経済産業省委託事業

営業秘密に関する欧州法制度の概要

２０２６年２月

独立行政法人　日本貿易振興機構
デュッセルドルフ事務所

目　　次

EU……1

第 1 章　営業秘密漏えいの実態……1

第 2 章　営業秘密の保護体系……2

1　EU 営業秘密指令の概要と位置付け……2
2　EU 営業秘密指令以外の営業秘密に関連する法令の概要と位置付け……3
3　まとめ……7

第 3 章　営業秘密の定義……7

1　EU 営業秘密指令における営業秘密の定義……7
2　営業秘密の各要件の意義……8
3　日本法との比較……8
4　まとめ……9

第 4 章　営業秘密侵害行為の定義……9

1　EU 営業秘密指令における営業秘密侵害行為……9
2　営業秘密侵害行為に対する救済措置等の適用に関する例外……11
3　日本法との比較……11
4　まとめ……12

第 5 章　民事措置……13

1　民事的救済措置の付与義務と救済措置の内容……13
2　暫定的措置及び予防的措置（第 10 条）……14
3　本案判断から生じる措置……14
4　まとめ……16

第 6 章　刑事措置……17

第 7 章　行政措置……18

第 8 章　適用範囲……18

1　EU 営業秘密指令の要求事項……18
2　EU 営業秘密指令により影響を受けない事項……18
3　まとめ……18

第 9 章　訴訟手続に関する諸制度……19

1　立証責任に関する規定・制度・運用……19
2　証拠収集に関する規定・制度・運用……19

3　訴訟の証拠収集等における営業秘密の保護に関する規定・制度・運用 …… 19
4　まとめ …… 20

第 10 章　営業秘密侵害事件の動向 …… 21

1　EU の営業秘密侵害事件の統計情報 …… 21
2　参考になる裁判例 …… 22
3　まとめ …… 24

第 11 章　EU の法律・制度・運用を踏まえた、営業秘密漏えい対策を実施するにあたってのポイント …… 24

1　EU において営業秘密漏えい対策を実施するにあたってのポイント・留意点 …… 24
2　ライセンス、生産委託、合弁会社設立で気をつけるべきポイント …… 27
3　まとめ …… 28

ドイツ …… 30

第 1 章　営業秘密の保護体系 …… 30

1　保護体系の概要 …… 30
2　営業秘密関連の法改正の動き …… 31
3　その他営業秘密・技術流出に関する法律 …… 31
4　サイバーセキュリティ政策 …… 32
5　まとめ …… 34

第 2 章　営業秘密の定義 …… 34

1　総論 …… 34
2　GeschGehG による定義 …… 35
3　日本法との比較 …… 37
4　まとめ …… 38

第 3 章　営業秘密侵害行為の定義 …… 39

1　営業秘密侵害行為 …… 39
2　許容される行為 …… 40
3　営業秘密侵害行為の例外 …… 41
4　日本法との比較 …… 41
5　まとめ …… 42

第 4 章　民事措置 …… 43

1　総論 …… 43

2　除去及び差止請求権（GeschGehG 第 6 条）……43
3　廃棄、引渡し、回収並びに市場からの除去及び撤去を請求する権利（GeschGehG 第 7 条）……44
4　情報提供請求権（GeschGehG 第 8 条）……44
5　損害賠償請求権（GeschGehG 第 10 条）……45
6　まとめ……46
第 5 章　刑事措置……46
1　GeschGehG……46
2　刑法……47
3　まとめ……48
第 6 章　行政措置……48
第 7 章　適用範囲……49
1　営業秘密の保護に関する公法上の規定の優先……49
2　GeschGehG により影響を受けない事項……49
3　まとめ……49
第 8 章　訴訟手続に関する諸制度……50
1　民事訴訟……50
2　刑事訴訟……52
3　まとめ……53
第 9 章　営業秘密侵害事件の動向……53
1　ドイツの営業秘密侵害事件の統計情報……53
2　参考になる裁判例……54
3　まとめ……56
第 10 章　ドイツの法律・制度・運用を踏まえた、営業秘密漏えい対策を実施するにあたってのポイント……56
1　ドイツにおいて営業秘密漏えい対策を実施するにあたってのポイント・留意点……56
2　ライセンス、生産委託、合弁会社設立で気をつけるべきポイント……57
3　まとめ……59
英国……60
第 1 章　営業秘密の保護体系……60
1　営業秘密に関する制度の概要……60

2　秘密情報・営業秘密保護の並存 …… 61
3　まとめ …… 61

第 2 章　営業秘密の定義 …… 61

1　UK TS 規則による定義 …… 62
2　判例法による定義 …… 62
3　NSA 2023 による定義 …… 63
4　日本法との比較 …… 63
5　まとめ …… 64

第 3 章　営業秘密の侵害行為 …… 65

1　UK TS 規則による営業秘密侵害行為の定義：営業秘密不正取得・開示・使用 …… 65
2　契約で定めた秘密保持義務の不履行：秘密情報の不正開示・使用 …… 65
3　判例法による秘密保持義務違反：秘密情報の不正開示・使用 …… 66
4　NSA 2023 による営業秘密侵害行為の定義：営業秘密不正取得、複製、記録、保持、開示、アクセス提供 …… 67
5　日本法との比較 …… 67
6　まとめ …… 68

第 4 章　民事措置 …… 68

1　救済手段 …… 68
2　権利・救済手段の期間制限 …… 71
3　まとめ …… 71

第 5 章　刑事措置 …… 72

1　NSA 2023 …… 72
2　コンピュータ不正使用法 …… 72
3　その他刑事罰 …… 75
4　日本法との比較 …… 75
5　まとめ …… 75

第 6 章　行政措置 …… 76

第 7 章　適用範囲 …… 76

1　UK TS 規則 …… 76
2　NSA 2023 …… 77
3　コンピュータ不正使用法 …… 77
4　まとめ …… 78

第 8 章　訴訟手続に関する諸制度 …… 78

1　訴訟手続中の営業秘密の保護 …… 78
2　訴訟手続における情報の開示・証拠収集 …… 80
3　まとめ …… 82

第 9 章　営業秘密侵害事件の動向 …… 83

1　英国における営業秘密侵害事件 …… 83
2　参考になる裁判例 …… 83
3　まとめ …… 84

第 10 章　英国の法律・制度・運用を踏まえた、営業秘密漏えい対策を実施するにあたってのポイント …… 84

1　英国における営業秘密管理の留意点 …… 84
2　ライセンス、生産委託、合弁会社設立で気をつけるべきポイント …… 85
3　まとめ …… 88

【条文】 …… 89

EU　89

DIRECTIVE (EU) 2016/943 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL …… 89

ドイツ　112

Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) …… 112

英国　130

1　The Trade Secrets (Enforcement, etc.) Regulations 2018 …… 130
2　National Security Act 2023 …… 155
3　Computer Misuse Act 1990 …… 164

【参考書式】 …… 193

ドイツ　193

1　就業規則における秘密保護関連規定の例 …… 193
2　従業員との秘密保持契約書の例 …… 223
3　退職後の競業避止契約書の例 …… 228
4　取引先との秘密保持契約書の例 …… 233
5　来訪者受付表 …… 249

英国　251

1　従業員ハンドブックにおける秘密保護関連規定の例 ……251
2　従業員との秘密保持契約書の例 ……269
3　退職後の競業避止契約書の例 ……278
4　取引先との秘密保持契約書の例 ……286
5　来訪者受付表 ……297

EU

第 1 章　営業秘密漏えいの実態

EUにおける営業秘密をめぐるリスクは、企業活動のグローバル化とデジタル化の進展に伴って顕在化・拡大している。2023 年 6 月 28 日に、欧州連合知的財産庁（European Union Intellectual Property Office。以下「EUIPO」という）により公表された報告書「EU における営業秘密侵害事件の動向」（TRADE SECRETS LITIGATION TRENDS IN THE EU（以下「2023 年 EU 報告書」という））[1]によれば、2017 年 1 月 1 日から 2022 年 10 月 31 日までの期間で、EU 加盟国全体から収集された公表済みの営業秘密侵害事件は民事事件・刑事事件・行政事件あわせて 695 件に上る[2]。また、2022 年 7 月に欧州委員会により公表された研究調査書「データ経済の文脈における営業秘密の法的保護に関する研究」（STUDY ON THE LEGAL PROTECTION OF TRADE SECRETS IN THE CONTEXT OF THE DATA ECONOMY（以下「2022 年 EU 研究調査書」という））[3]の実証データによれば、企業にとって大きな懸念事項は、従業員又は元従業員による営業秘密の漏えいであることが明らかとされており、これは、営業秘密の保有者（前職の雇用主）のみならず、新たな雇用主が意図せず新規従業員が前職から持ち込んだ営業秘密にアクセスして利用してしまうおそれがある点でも重大な懸念とされている[4]。日本企業も関係した営業秘密の侵害事案として、フランスのタイヤメーカーの元従業員が、同社の重タイヤ製造プロセスに関する機密情報を日本のタイヤメーカーに売り込もうとし、当該元従業員は有罪となり、罰金及び 2 年の禁固刑が言い渡された事件がある[5]。当該事件では日本のタイヤメーカーによる営業秘密の侵害が問題となったわけではないものの、上記のとおり、日本企業にとって、自社の従業員や元従業員が自社の営業秘密を漏えいする場合だけでなく、自社の従業員が第三者の営業秘密の利用に関与する可能性があることにも留意する必要がある。また、EU におい

1　2023 年 EU 報告書は、EU 営業秘密指令第 18 条に定められた報告義務に基づき、EU における営業秘密侵害事件の動向を分析したものである。2023 年 EU 報告書の分析対象期間は、2017 年 1 月 1 日から 2022 年 10 月 31 日までであり、2018 年に公表された『EU 加盟国における営業秘密侵害事件のベースライン』（Baseline of Trade Secrets Litigation in the EU Member States）を補完するものである（2023 年報告書 9 頁）。EUIPO, “TRADE SECRETS LITIGATION TRENDS IN THE EU”, 28 June 2023, <https://www.euipo.europa.eu/en/publications/trade-secrets-litigation-trends-in-the-eu>.

2　2023 年 EU 報告書 19 頁。

3　2022 年 EU 研究調査書は、①企業間・組織間で共有されるデータに対して EU の営業秘密保護の法的枠組みがどの程度適用されるのか、そして②欧州企業による営業秘密の実務運用状況を分析するものである。European Commission, “STUDY ON THE LEGAL PROTECTION OF TRADE SECRETS IN THE CONTEXT OF THE DATA ECONOMY (GRO/SME/20/F/206)”, July 2022, <https://op.europa.eu/en/publication-detail/-/publication/c0335fd8-33db-11ed-8b77-01aa75ed71a1/language-en>.

4　2022 年 EU 研究調査書 81 頁。

5　日本弁理士会令和 2 年度不正競争防止法委員会第 1 部会「欧米における営業秘密保護に関する質問および回答」（2021）8 頁＜https://jpaa-patent.info/patent/viewPdf/3891＞。

ては人材の流動性が高い状況が続いており[6][7]、サプライチェーンの複雑化に加え、AI の飛躍的な進歩及び社会実装[8]により、営業秘密が外部に流出するリスクが日々増しつつあるといえる。加えて、サイバー攻撃や産業スパイにより、情報漏えいが起こる可能性も考慮する必要がある[9]。さらには、2020 年の欧州データ戦略の一環として制定された EU データ法のもとで導入された IoT 製品により生み出されたデータについての強制データ開放の枠組みにおいて、一部の類型のデータについては営業秘密もデータ開放の対象とされている（第 2 章において詳述する）ことから、営業秘密をより意識的に特定及び管理する必要性も生じている。このような現況に照らすと、EU においても、営業秘密の保護を単なる「法務・知財の課題」にとどめるのではなく、戦略的な「経営課題」として位置付ける必要性が高まっているといえる。以下では、EU 営業秘密指令の体系や運用などを踏まえた上、営業秘密漏えい対策を実施するにあたってのポイントを説明する。

第 2 章　営業秘密の保護体系

1　EU 営業秘密指令の概要と位置付け

「非開示のノウハウ及び事業上の情報（営業秘密）の違法な取得、使用及び開示に対する保護に関する指令(EU)2016/943」（以下「EU 営業秘密指令」という）[10]は、2016 年に成立した EU レベルでの営業秘密の保護の水準について定める指令である。EU 営業秘密指令は、指令であるがゆえに、直接に事業者に適用されるわけではなく、各加盟国にその内容に従った国内法の制定を義務づけている。

営業秘密は、容易に窃取され又は違法に取得されうる情報であるところ、加盟国によって法的保護の水準に相違があることで、EU 域内市場の断片化及び営業秘密に関する規則の効果が希釈化するとともに、営業秘密の利用を伴うイノベーションに繋がる経済活動を、国境を超えて行うインセンティブが阻害され、EU 域内におけるイノ

6　European Commission, Annual report on intra-EU labor mobility 2024 published, <https://employment-social-affairs.ec.europa.eu/news/annual-report-intra-eu-labour-mobility-2024-published-2025-02-07_en>.

7　従業員がその企業の業務の詳細を熟知したまま退職することに伴うリスクは、経済環境の変化（人材の流動性の増加や、経済における情報の価値の上昇）により一層高まっていることが指摘されている。Magdalena Kolasa, “Trade Secrets and Employ Mobility, January 2018, p.2, <https://api.pageplace.de/preview/DT0400.9781108337496_A32337385/preview-9781108337496_A32337385.pdf>.

8　例えば、営業秘密を保有する企業の従業員が、生成 AI ツール（ChatGPT など）に誤って営業秘密を含む情報を入力し、営業秘密が競合他社や第三者へ漏えいするリスクが指摘されている。CAMILLA A. HRDY, “Trade Secrecy Meets Generative AI”, 01. February 2025, p.317, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5121745&>.

9　Thomas Hoeren, “The New EU Directive on the Protection of Trade Secrets and Its Implementation” 2020, p.209, <https://www.itm.nrw/wp-content/uploads/214_10.1007_978-981-15-1350-3.pdf>.

10　Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, <https://eur-lex.europa.eu/eli/dir/2016/943/oj/eng>.

ベーションが生まれにくくなる。さらには、営業秘密の保護が十分でない加盟国や第三国において不正に取得された営業秘密を活用して生み出された製品を EU 域内に流通させることが容易になることで、EU 域内の適切な機能が阻害されるおそれがある（EU 営業秘密指令前文(8)(9)）ことから、EU 営業秘密指令は、EU 域内市場における十分かつ一貫性のある水準の民事上の救済を確保すべく、営業秘密の違法な取得、使用及び開示からの保護に関するルールを EU レベルで定めている（EU 営業秘密指令第 1 条第 1 項、前文(10)）。

EU 営業秘密指令は、営業秘密の違法な取得、使用又は開示に対し、民事上の救済を規定するにとどまる。刑事罰、行政措置、公共調達、その他の政府・公共機関での国内手続における営業秘密の使用に関しては、加盟国の国内法で定めることが可能である。

各加盟国は、2018 年 6 月 9 日までに、EU 営業秘密指令を国内法化する義務が課されていた（EU 営業秘密指令第 19 条第 1 項）が、現在、全ての加盟国において、EU 営業秘密指令は国内法への移行が完了している[11]。

2 EU 営業秘密指令以外の営業秘密に関連する法令の概要と位置付け

(1) EU データ法

一部の規定を除き、2025 年 9 月 12 日に適用開始された EU データ法[12]は、個人データの保護を確保しつつデータへの公正なアクセスと利用者の権利を強調して、EU 域内においてデータがもたらす諸課題に対応し、データがもたらす可能性を解放するための包括的な取組である[13]。具体的には、IoT 製品が生成するデータへの利用者のアクセス・移転の権利を規定する B2B・B2C データ共有（EU データ法第 2 章。IoT データ条項とも呼ばれる）、IoT データ条項のもとでのデータ共有のみならず、EU 法及び国内法のもとでデータの強制開放を義務づけられる場合の共通のルールを定める条項（EU データ法第 3 章。水平条項とも呼ばれる）、事業者間のデータ関連契約についての規制（EU データ法第 4 章）、民間事業者が保有するデータを公的機関が公益目的のために利用可能とする B2G データ共有（EU データ法第 5 章）、データ処理サービス（典型的には、IaaS、PaaS、SaaS といったクラウドサービスやエッジサービスを指す（EU データ法前文(78)(81)）におけるスイッチング促進及び第三国による非個人データへの違法なガバメントアクセスを防ぐための措置（EU データ法第 6 章・第 7 章）

---

11 European Union, “Document 32016L0943 – National transposition”, <https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=CELEX:32016L0943>.

12 Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on Harmonised Rules on Fair Access to and Use of Data and Amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act), <https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng>.

13 European Commission, “Data Act”, <https://digital-strategy.ec.europa.eu/en/policies/data-act>.

等について規定する。

このうち、IoT データ条項は、コネクテッド製品[14]及び関連サービス[15]の利用者に対してコネクテッド製品の利用により生成されたデータ等へのアクセス及び第三者への共有を行う権利を付与している（EU データ法第 3 条第 1 項、第 4 条第 1 項、第 5 条第 1 項）。IoT データ条項の適用対象となる製品データ及び関連サービスデータは、①生データ（追加の形式の処理を行うことなく自動的に生成されるデータポイントを参照するソース又は一次データとしても知られる生の形式のデータ）、②前処理データ（後続の処理と分析の前に、理解しやすく、使いやすくする目的で前処理されたデータ）（EU データ法前文(15)）、③メタデータ（データの発見又は利用を容易にする、データの内容又は利用に関する構造化された記述）（EU データ法第 2 条第 2 号）に限定されるが、営業秘密がこれらのカテゴリーに含まれれば、利用者の要求に応じて利用者又は第三者に対して営業秘密にアクセスさせる必要がある。

EU データ法では、営業秘密の保護を維持するためのフレームワーク（営業秘密ハンドブレーキと呼ばれる[16]）が設けられている。具体的には、データ保有者は、利用者からアクセス（又は、第三者への移転）の要求を受けたデータに営業秘密が含まれている場合には、営業秘密として保護されているデータを特定のうえ、利用者（又は、第三者）との間でデータの秘密性を保全するために必要な相応の技術的及び組織的措置を合意するものとされている（EU データ法第 4 条第 6 項、第 5 条第 9 項）。ただし、必要な措置が合意されない場合、又は、利用者（第三者）が合意した措置を実施しない場合、若しくは営業秘密の秘密性を侵害する場合には、データ保有者は営業秘密として特定されたデータの共有を撤回又は中止できる。データ保有者の決定は適切になされたうえで、不当な遅滞なく書面で利用者（又は、第三者）に通知しなければならない。また、データ共有が撤

---

14 利用又は環境に関するデータを取得、生成又は収集する製品であって、電子通信サービス、物理的接続又はデバイス上のアクセスを通じて製品データを通信することが可能なもの（ただし、その主な機能が、利用者以外の者のためにデータを保存、処理又は送信するものを除く）を意味する（EU データ法第 2 条第 5 号）。例えば、インフラ、車両、健康・ライフスタイル器具、船、飛行機、家庭用品及び消費財、医療及び健康機器、農耕機械及び産業機械（EU データ法前文(14)）、さらには、消費者向け製品としてコネクテッドカー、健康管理器具及びスマートホーム端末が、その他の製品として飛行機、ロボット及び産業機械が挙げられる（European Commission, Data Act Explained, <https://digital-strategy.ec.europa.eu/en/factpages/data-act-explained>）。

15 電子通信サービス以外のデジタルサービス（ソフトウェアを含む）であって、①そのデジタルサービスがない場合にコネクテッド製品が 1 つ以上の機能を実行しなくなるような態様で、購入、レンタル又はリースの時点で製品に接続されているか、②コネクテッド製品の機能を追加、更新又は適応させるために、製造者又は第三者によってその後製品に接続されるものを意味する（EU データ法第 2 条第 6 号）。例えば、IoT 家電のアプリケーションサービスが挙げられる。

16 European Commission, Frequently Asked Questions Data Act (Version 1.3), <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act>. 23 番。

回等されたことについては、データ保有者より管轄当局[17]にも通知がなされなければならない（EU データ法第 4 条第 7 項、第 5 条第 10 項）。

さらに、営業秘密の保有者であるデータ保有者が、技術的及び組織的措置を講じてもなお営業秘密の開示によって深刻な経済的損害[18]を被る可能性が高い旨を立証することができた例外的な場面においては、データ保有者は、特定のデータへのアクセス等の要求を拒絶できるとされている。この立証は、第三国における営業秘密保護の執行可能性、要求されたデータの性質及び機密性の水準、コネクテッド製品の独自性及び新規性等の客観的な要素に基づいて行わなければならない。データ保有者は、アクセス要求を拒絶する場合には利用者に、また、移転要求を拒絶する場合にはデータの移転先の第三者に、不合理な遅滞なく書面でその拒絶の理由を伝える必要がある。さらに、いずれの場合もデータ保有者は管轄当局に拒絶の旨を通知する必要がある（EU データ法第 4 条第 8 項、第 5 条第 11 項）[19]。

なお、2025 年 11 月 19 日に欧州委員会より提案された Digital Omnibus 法案[20]第 1 条第 3 項及び第 4 項は、上記の EU データ法第 4 条第 8 項及び第 5 条第 11 項の修正を行うものである。具体的には、EU 域内と営業秘密保護法制の水準が同等ではない第三国の事業体又はその直接若しくは間接の支配下にある EU 域内に拠点を有する事業体[21]にデータを共有する場合も、データ共有の拒絶事由として明記する提案がなされている。この営業秘密保護法制の水準の同等性については、理論上第三国の法的枠組みが堅固であるか、EU のルールを上回るものであったとしても、実際には適切な執行に欠ける場合をも対象とするとされている（デジ

17 各加盟国において、1 つ以上の監督当局が指定される(EU データ法第 37 条第 1 項）。複数指定された場合には、当局間の協力を容易にするための data coordinator が指定される（同条第 2 項）。

18 深刻な経済的損害は、深刻かつ取り返しのつかない経済的損害を意味し、ケースバイケースで判断される必要がある（EU データ法前文(31)）。

19 この点を論じたものとして、石川智也「EU データ法のもとでのデータへのアクセス権と営業秘密保護の調和および日本のデータ利活用法制への示唆」情報ネットワーク・ローレビュー第 24 巻（2025）45 頁～65 頁。

20 *Proposal for a Regulation of the European Parliament and of the Council Amending Regulations (EU) 2016/679, (EU) 2018/1724, (EU) 2018/1725, (EU) 2023/2854 and Directives 2002/58/EC, (EU) 2022/2555 and (EU) 2022/2557 as Regards the Simplification of the Digital Legislative framework, and Repealing Regulations (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868, and Directive (EU) 2019/1024 (Digital Omnibus), COM(2025) 837 final (Nov. 19, 2025).*

21 資本又は議決権の保有、財務的参加、契約上の取決め、仲介企業等を通じて、事業体の経営又は戦略的決定に対して決定的又は支配的な影響力を行使する能力があるかによって判断され、支配は、過半数でなくとも、直接又はその他の手段を通じて行使される可能性があるとされる。データ保有者は、適切な非侵襲性を確保しつつ、公的登録簿の検索や利用者等への直接請求等の方法で関連情報の取得に最善の努力を払うべきとされている（デジタルオムニバス法案前文(13)）。

タルオムニバス法案前文(11)）[22]。開示を拒否する根拠の立証にあたっては、データ保有者は、不十分又は不適切な法的基準、不十分又は恣意的な執行、過去の侵害事例、EU 法と抵触する外国開示義務、EU 域内事業体に対する法的救済手段の制限、競合他社を弱体化させるための手続的戦術の戦略的悪用、不当な政治的影響力等の要素を考慮しうるとされている。また、第三国又は第三国に所在する事業体の営業秘密の保護水準に関する全面的な分析又は実証を要求されるべきではないとされる一方で、第三国全体に対して体系的又は一般化して適用されるべきではなく、各事例の具体的な状況に応じて明確で比例的かつ個別に対応すべきとされている（デジタルオムニバス法案前文(12)）。

データ処理サービス（クラウドサービス等）のスイッチングに関する規律は、顧客によるクラウドサービス等の切替えを促進するために、クラウドサービス等の提供者に対して、スイッチングを妨げない義務、契約条項での所定の事項の合意、スイッチングを容易にするための技術的措置の確保等を求める規律である。もっとも、エクスポート可能なデータ（EU データ法第 2 条第 38 号）及びデジタル資産（EU データ法第 2 条第 32 号）がスイッチングの対象とされているところ、エクスポート可能なデータからデータ処理サービス提供者又は第三者の営業秘密は除外されており、営業秘密を構成するデジタル資産の移転を要しないものとすると規定されている（EU データ法第 30 条第 6 項）ため、顧客がクラウドサービス等を切り替えるにあたって、クラウドサービス等の提供者が自ら又は第三者の営業秘密を移転する必要はないといえる。

(2) EU AI 法

EU AI 法[23]は、EU における人々の健康、安全その他の基本権、民主主義及び法の支配に対する潜在的なリスクを抑えつつ、AI によるイノベーション促進を目的とした包括的な AI に関する法的枠組みであり、2025 年 2 月 2 日から段階的に適用開始されている。EU AI 法は、リスクベースアプローチを採用し、AI システムについては AI システムの持つリスクを①許容できないリスク、②ハイリス

---

22 デジタルオムニバス法案のスタッフワーキング文書（*COMMISSION STAFF WORKING DOCUMENT Accompanying the documents Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL*, SWD (2025) 836 final (Nov. 19, 2025)）脚注 36 で引用されている、2025 年 5 月 22 日公表のスタッフワーキング文書（*COMMISSION STAFF WORKING DOCUMENT Report on the protection and enforcement of intellectual property rights in third countries*, SWD (2025) 131 final (May 22, 2025)）5 頁では、中国やインドをはじめとする多くの国々において、営業秘密の保護が不十分であり、その執行に課題のあることが、EU の企業に回復不能な損害をもたらしているとの指摘がなされている。

23 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), <https://digital-strategy.ec.europa.eu/en/policies/data-act>.

ク、③透明性に関するリスク、④最小限のリスクに分け、汎用目的 AI モデルについてはシステミックリスクを有する汎用目的 AI モデルとそれ以外の汎用目的 AI モデルに分けており、いずれもリスク水準に応じた規制を設けている。

EU AI 法においても、営業秘密の保護に配慮した規定があり、例えば、欧州委員会、市場監視当局及び認定適合性評価機関等は、EU 法又は国内法に従い、それらの任務及び活動の遂行にあたって取得される情報及びデータ（システミックリスクの有無を問わず汎用目的 AI モデルに関して作成し AI Office に提出されたものを含む（EU AI 法第 53 条第 1 項(b)及び第 7 項、第 55 条第 3 項））の機密性を、営業秘密等を保護するような方法により確保しなければならない旨が規定されている（EU AI 法第 78 条）。また、汎用目的 AI モデルの提供者は、モデルを AI システムに組み込む AI システムの提供者に対して当該汎用目的 AI モデルの能力及び限界を十分に理解できるように情報及び文書を作成及び提供しなければならない（EU AI 法第 53 条第 1 項(b)）ものの、これは営業秘密等の保護には抵触しない範囲で求められるにとどまる（EU AI 法第 53 条第 1 項(b)）。

3　まとめ

EU 営業秘密指令は、加盟国間で異なっていた営業秘密保護の水準を調和し、営業秘密の違法な取得、使用又は開示に対する民事上の救済を確保するために制定された。同指令は民事上の救済に限って規律するものであるが、刑事措置や行政措置については、各加盟国が国内法で独自に定めることができる。なお、現時点では、全ての加盟国で国内法化が完了している。また、EU データ法や EU AI 法といった近時成立したデジタル法制においては、データ共有義務や AI システム・モデルに関する情報提供義務の履行に際して営業秘密との抵触が生じうるものの、営業秘密の価値が毀損されるリスクを回避するための仕組みが設けられており、EU 営業秘密指令の内容だけでなくこれらの法令との関係性及びそれに伴う管理上の影響を適切に理解する必要がある。

第 3 章　営業秘密の定義

1　EU 営業秘密指令における営業秘密の定義

営業秘密とは、次の要件を全て満たす情報を意味する（EU 営業秘密指令第 2 条第 1 号）。

① 単体として、又は、その構成要素の正確な構成と組み立てにおいて、当該種別の情報を通常取り扱う者の間で、一般に知られておらず、又は容易にアクセスできない、という意味で秘密であること（秘密性）。

② 秘密性ゆえに、商業的価値を有していること（商業的価値）。

③ 情報を秘密に保つために、合法的に情報を管理している者によって、当該状況下

で、合理的な措置が講じられていること（合理的な措置）。

これは、知的財産権の貿易関連の側面に関して定めた条約である TRIPS 協定[24]第 39 条第 2 項で規定される非公開情報（Undisclosed information）の要件に沿った内容である。

2　営業秘密の各要件の意義

営業秘密の定義は、不正利用から保護される対象を限定することなく、均質な定義を定めることが重要であるため、ノウハウ、事業情報及び技術情報のうち、それらを秘密として保持する正当な利益が存在し、かつ、その秘密性が維持されるとの正当な期待が認められるものを包含するように解釈されるべきであるとされる（EU 営業秘密指令前文(14)）。

前記 1①の要件との関係では、従業員が通常の職務の過程で得た経験及び技能、その種の情報を通常取り扱う者の間で、一般に知られている、又は容易にアクセス可能な情報は、営業秘密の定義から除外される（EU 営業秘密指令前文(14)）。

前記 1②の要件との関係では、ノウハウ又は情報は、実際の価値か潜在的な価値かを問わず、商業的価値を有するべきとされる。例えば、その違法な取得、使用又は開示が、その者の科学的・技術的潜在能力、事業上若しくは財務上の利益、戦略的地位、又は競争力を損なうという点において、これを適法に管理する者の利益を害するおそれがある場合には、商業的価値を有するものとみなされるべきとされる（EU 営業秘密指令前文(14)）。

前記 1③の要件との関係では、EU 営業秘密指令上、明確に説明されているわけではないが、「合理的な措置」という概念は、その情報が特別な取扱いを必要とし、法的保護を受けることを第三者に通知する機能を有していることを踏まえて、明確な秘密管理措置と明示的な合意という二つの事実上の態様の双方を含むと指摘するものがある。具体的な方法としては、契約条項を通じて情報へのアクセスを制限することが挙げられ、その他にも暗号化等の措置も合理的な措置となりうるが、リバースエンジニアリングを十分困難にしており、第三者にとって情報が秘密として扱われることが明白である場合に限るとの指摘もあり[25]、秘密情報であることに疑義が生じないような管理を行うべきである。

3　日本法との比較

日本の不正競争防止法において、「営業秘密」は、次の 3 要件を満たすものと定義

24　World Trade Organization, “Agreement on Trade-Related Aspects of Intellectual Property Rights”, <https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm>.

25　Ulla-Maija Mylly, “Preserving the Public Domain: Limits on Overlapping Copyright and Trade Secret Protection of Software”, *IIC - International Review of Intellectual Property and Competition Law*, Vol. 52 (2021), 1314, pp.1329-1330, <https://link.springer.com/article/10.1007/s40319-021-01120-3>.

される（不正競争防止法第 2 条第 6 項）。

① 秘密として管理されていること（秘密管理性）

② 事業活動に有用な技術上又は営業上の情報であること（有用性）

③ 公然と知られていないこと（非公知性）

①秘密管理性は、EU 営業秘密指令第 2 条第 1 号(c)の③「合理的な措置」と文言は異なるものの、①は、情報自体が無形で、その保有・管理態様が様々であり、特許権などのように公示を前提にできず、営業秘密であることが容易に知り得ないため、企業が秘密として管理しようとする対象を従業員や取引先に対して明確化する[26]ことを目的としていることを踏まえると、EU 営業秘密指令第 2 条第 1 号(c)の③「合理的な措置」に対応するものであると考えられる。②有用性は、EU 営業秘密指令第 2 条第 1 号(b)の②「商業的価値」と対応する関係にあるが、②はその情報が客観的にみて、事業活動にとって有用であることが必要とされる[27]にとどまり、「秘密性ゆえに」有用であることは求められていない点で、文言上は、EU 営業秘密指令第 2 条第 1 号(b)の②「商業的価値」の方が要件を満たすハードルが高いように思われる。③非公知性は、一般的には知られておらず、又は容易に知ることができないことが必要であるとされており[28]、営業秘密指令第 2 条第 1 号(a)の①「秘密性」と対応関係にあるといえる。

4 まとめ

EU 営業秘密指令において、「営業秘密」は、秘密性、商業的価値及び合理的な措置の 3 つの要件から成る。同指令の各要件は、日本の不正競争防止法における「営業秘密」の 3 要件（秘密管理性、有用性及び非公知性）と概ね対応するものの、商業的価値の要件に関しては、日本の不正競争防止法上の定義には含まれていない要素（商業的価値が秘密であることにより生じていること）が求められている。保護したい情報の EU 営業秘密指令の各加盟国の国内法における営業秘密該当性の判断や営業秘密として保護するための情報管理の方法を検討する前提として、EU 営業秘密指令の「営業秘密」の定義を理解しておくことは有益である。

第 4 章 営業秘密侵害行為の定義

1 EU 営業秘密指令における営業秘密侵害行為

(1) 侵害行為

EU 営業秘密指令第 2 条第 3 号において、侵害者は、違法に営業秘密を取得、

---

26 経済産業省「営業秘密管理指針」（2025 年 3 月 31 日改訂）7 頁。

27 同上 20 頁。

28 同上 22 頁。

使用又は開示する自然人又は法人をいうと定義されている。そして、EU 営業秘密指令第 4 条において、具体的には以下の行為が営業秘密を違法に取得、使用及び開示する行為にあたると規定されている。

ア　営業秘密の違法取得

営業秘密の保有者の同意なく、以下の行為により行われた営業秘密の取得は違法取得とみなされる（EU 営業秘密指令第 4 条第 2 項）。

① 営業秘密の保有者の適法な管理下にあり、営業秘密を含む、又はその営業秘密を推知することができる、文書、物品、材料、物質、又は電子ファイルへの無権限でのアクセス、使用又はコピー

② 行為時の状況下で、誠実な商慣習に反すると考えられるその他の行為

イ　営業秘密の違法使用又は開示

営業秘密の保有者の同意なく、以下の者により行われた営業秘密の使用又は開示は違法な使用又は開示とみなされる（EU 営業秘密指令第 4 条第 3 項）。

① 営業秘密を違法に取得した者

② 秘密保持契約又は営業秘密を開示しないその他の義務に違反した者

③ 営業秘密の使用を制限する契約上の義務又はその他の義務に違反した者

ウ　違法使用又は開示の介在を知りながらする取得、使用又は開示

営業秘密が、違法に使用又は開示した（上記イにあたる行為）者から、直接又は間接に取得されたものであることを知っていた（又はその状況下において知るべきであった）場合にも違法取得、使用又は開示とみなされる（EU 営業秘密指令第 4 条第 4 項）。

エ　侵害品を製造、提供、上市、輸出、輸入又は保管する者

侵害品の製造、提供若しくは上市又はこれらの目的での輸入、輸出若しくは保管は、その行為を行う者が、当該営業秘密について違法に使用されたことを知っていた（又はその状況下において知るべきであった）場合にも、当該営業秘密の違法使用とみなされる（EU 営業秘密指令第 4 条第 5 項）。

(2) 適法な営業秘密の取得、使用及び開示

営業秘密が次のいずれかの手段により取得された場合、「適法」とみなされる（EU 営業秘密指令第 3 条第 1 項）。

① 独自の発見又は創造

② 公衆に利用可能とされた製品若しくは物品、又は、営業秘密の取得を制限する法的に有効な義務を負っていない情報の取得者が適法に保有する製品若しくは物品の、観察、研究、解体又は検査

③ EU 法及び加盟国の法令及び実務に則った、労働者又は労働者代表の情報提

供及び協議の権利行使

④　行為時の状況下で、誠実な商慣習に合致するその他の実務上の行為

また、営業秘密の取得、使用又は開示は、EU 法又は国内法により要求され、又は認められている範囲内においては、適法とみなされる（EU 営業秘密指令第 3 条第 2 項）。

なお、適法に取得された製品のリバースエンジニアリングは、契約で別段の合意がある場合を除き、適法な手段とみなされるべきとされる（EU 営業秘密指令前文(16)）。また、営業秘密の取得、使用又は開示が、法律によって義務づけられる場合、又は認められる場合、EU 営業秘密指令の目的に照らして適法と取り扱われるべきであるが、EU 法又は国内法がその情報の受領者又は取得者に対して営業秘密に関する秘密保持義務又は営業秘密の使用に関する制限を課すことを妨げてはならないとされる（EU 営業秘密指令前文(18)）。

2　営業秘密侵害行為に対する救済措置等の適用に関する例外

EU 営業秘密指令第 5 条は、以下のいずれかの場合に行われた営業秘密の取得、使用又は開示については、加盟国が EU 営業秘密指令に規定された措置、手続及び救済の適用対象から除外されることを確保しなければならない旨を規定している。

①　メディアの報道の自由及び多元主義を含む、欧州基本権憲章に定める表現及び情報伝達の自由の権利行使

②　公共の利益を保護する目的での、不正行為又は違法行為の暴露

③　労働者代表が、EU 法又は国内法に従い、その正当な職務遂行の一環として、その職務遂行に必要がある場合に、労働者から開示を受けること

④　EU 法又は国内法により認められた正当な利益を保護する目的での行為

3　日本法との比較

日本においては、不正競争防止法第 2 条第 1 項に、営業秘密に係る不正行為の行為類型が規定されており、大きく分けると以下のパターンに分類される[29]。

(1)　不正取得類型（第 2 条第 1 項第 4 号）

営業秘密の保有者から不正な手段で営業秘密を取得し、その取得した営業秘密を使用、開示する行為

(2)　信義則違反類型（第 2 条第 1 項第 7 号）

営業秘密の保有者から正当に示された営業秘密を不正に使用、開示する行為

(3)　転得類型（第 2 条第 1 項第 5 号、第 6 号、第 8 号、第 9 号）

ア　取得時悪意転得類型

①　第 2 条第 1 項第 4 号の営業秘密不正取得行為の介在について知って（悪

29　経済産業省-知的財産政策室「逐条解説・不正競争防止法」第 3 版（2024 年）97 頁～98 頁。

意）又は重過失により知らないで営業秘密を取得し、その取得した営業秘密を使用、開示する行為（第 2 条第 1 項第 5 号）

② 第 2 条第 1 項第 7 号の営業秘密不正開示行為の介在等について悪意又は重過失で営業秘密を取得し、その取得した営業秘密を使用、開示する行為（第 2 条第 1 項第 8 号）

イ 取得時善意転得類型

① 営業秘密を取得した後に、営業秘密不正取得行為（第 2 条第 1 項第 4 号）の介在について悪意又は重過失で当該営業秘密を使用、開示する行為（第 2 条第 1 項第 6 号）

② 営業秘密を取得した後に、営業秘密不正開示行為（第 2 条第 1 項第 7 号）の介在等について悪意又は重過失で当該営業秘密を使用、開示する行為（第 2 条第 1 項第 9 号）

(4) 営業秘密侵害品譲渡等類型（第 2 条第 1 項第 10 号）

(1)～(3)の不正使用行為により生じた物を譲渡等する行為

上記(1)不正取得類型及び(2)信義則違反類型は、営業秘密の取得（EU 営業秘密指令第 4 条第 2 項）及び営業秘密の使用又は開示（EU 営業秘密指令第 4 条第 3 項）と対応関係にある。また、上記(3)転得類型は、EU 営業秘密指令における第三者を通じた取得、使用又は開示（EU 営業秘密指令第 4 条第 4 項）と対応関係にある。(4)営業秘密侵害品譲渡等類型は、EU 営業秘密指令第 4 条第 5 項に類似しているものの、主に以下の点において異なっていると述べる指摘がある[30]。

① 営業秘密侵害品の範囲について、日本では技術上の秘密を使用した物に限定されているが、EU 営業秘密指令ではそのような限定はなく、かつ、そのデザイン、特徴、機能、生産方法又はマーケティングが違法に取得、使用又は開示された営業秘密によって著しく利益を受けている製品と規定されている（EU 営業秘密指令第 2 条第 4 号）ため、EU 営業秘密指令の方が広く定義されている。

② EU 営業秘密指令における主観的要件は実質上故意又は過失といえるところ、これは不正競争法防止法の場合（故意又は重過失）よりも緩やかである。

③ 不正競争防止法は、図利加害目的で営業秘密侵害品の譲渡などを行う行為（譲受時に営業秘密侵害品であることについて故意である場合に限る）につき、罰則を設けている（不正競争法防止法第 21 条第 1 項第 5 号、同条第 2 項第 5 号）のに対し、EU 営業秘密指令は、刑事罰については特段の規定を置いていない。

4 まとめ

EU 営業秘密指令は、営業秘密の違法取得、使用又は開示の類型を定めており、具

30 鈴木將文「営業秘密の保護の国際的側面に関する覚書」『特許研究 PATENT STUDIES』No.69（2020 年）59 頁、65 頁＜https://www.inpit.go.jp/content/100870234.pdf＞。

体的には、無権限のアクセスや契約違反、第三者による悪意の転得、侵害品の流通などの行為を侵害行為として規律する。他方で、独自の発見や適法に取得された製品のリバースエンジニアリングなど一定の行為は適法な取得として定めている。また、公共の利益を保護する目的での、不正行為又は違法行為の暴露など、特定の場面では営業秘密の侵害に対する救済措置の適用が除外される。このような EU 営業秘密指令の侵害行為の類型や例外の規律について把握することは、EU 営業秘密指令の各加盟国の国内法を理解するうえで有益である。日本の不正競争防止法と比較すると、行為類型に一定の対応関係があるものの、侵害品の範囲、主観的要件、刑事罰の有無などに相違がある点にも留意する必要がある。

第 5 章　民事措置

1　民事的救済措置の付与義務と救済措置の内容

(1) 概要（第 6 条）

① 加盟国は、違法な営業秘密侵害に対して、民事的救済を確保するために必要な手段、手続及び救済手段を定めなければならない（EU 営業秘密指令第 6 条第 1 項）。

② 上記の手段、手続及び救済手段は、以下を満たさなければならない（EU 営業秘密指令第 6 条第 2 項）。

a. 公正かつ衡平であること

b. 不必要に複雑、若しくは高額な、又は不合理な時間的制約若しくは不当な遅延を伴うものでないこと

c. 効果的かつ抑止効果があること

(2) 比例性と手続濫用（第 7 条）

① 上記の手段、手続、救済手段は、以下のように実施される必要がある（EU 営業秘密指令第 7 条第 1 項）。

a. 比例的であること

b. EU 域内市場での正当な取引の障害とならないこと

c. 濫用に対する保護措置が講じられていること

② 加盟国は、営業秘密の違法な取得、使用又は開示に関する申立てが明らかに根拠を欠き、かつ、申立人が手続を濫用的に、又は悪意をもって開始したと認められる場合に、管轄司法機関が、被告／被申立人の求めに応じて、被告／被申立人への損害賠償、申立人への制裁などの適当な措置を命ずることができるようにしなければならない。上記の措置は、別の法的手続で処理することができる（EU 営業秘密指令第 7 条第 2 項）。

(3) 時効期間（第 8 条）

① 加盟国は、営業秘密侵害に対する手段、手続及び救済手段の適用に関する実体的請求及び訴訟に適用される時効期間に関する規則を定めなければならない（EU 営業秘密指令第 8 条第 1 項）。

② 時効期間は、6 年を超えてはならない（EU 営業秘密指令第 8 条第 2 項）。

2 暫定的措置及び予防的措置（第 10 条）

① 加盟国は、営業秘密の保有者の申立てにより、管轄司法機関が、侵害が疑われる者に対し、以下の暫定的又は予防的措置のいずれかを命ずることができるよう確保しなければならない。

a. 暫定的に、営業秘密の使用若しくは開示の停止、又は必要に応じてその禁止

b. 侵害品の製造、提供、上市、若しくは使用の禁止、又は、これらの目的のための侵害品の輸入、輸出、若しくは保管の禁止

c. 市場への参入又は流通を防止するため、輸入品を含む侵害の疑いのある物品の差押え又は引渡し

② 加盟国は、管轄司法機関が、上記①の措置に代えて、営業秘密の保有者に対する補償を確保するための保証金の預託を条件として、営業秘密の違法な使用の継続を認めることができるよう確保しなければならない。保証金の預託と引き換えに営業秘密を開示することは認められない。

3 本案判断から生じる措置

(1) 差止命令及び是正措置（第 12 条）

① 加盟国は、本案に関する司法判断において、営業秘密の違法な取得、使用、又は開示があったと認定された場合、管轄司法機関が、申立人の申立てに基づき、以下の一以上の措置を命じることができるようにしなければならない（EU 営業秘密指令第 12 条第 1 項）。

a. 営業秘密の使用若しくは開示の停止又は必要に応じてこれらの禁止

b. 侵害品の製造、提供、上市若しくは使用の禁止、又はこれらを目的とする侵害品の輸入、輸出若しくは保管の禁止

c. 侵害品に関する適切な是正措置の実施

d. 営業秘密を含む又はこれを具体化する文書、物品、材料、物質、電子ファイルの全部若しくは一部の破棄、又は、適切な場合には申立人への引渡し

② 上記の①c.に記載の是正措置には、以下を含む（EU 営業秘密指令第 12 条第 2 項）。

a. 市場からの侵害品の回収

b. 侵害品の侵害性の除去

c. 侵害品の破棄、又は適切な場合、市場からの回収。ただし、その回収によって、当該営業秘密の保護を損なわないことを要する

③ 加盟国は、管轄司法機関が市場からの侵害品の回収を命じるとき、営業秘密の保有者の要求に応じて、その侵害品を、保有者、又は慈善団体に引き渡すように命じられる旨を規定できる（EU 営業秘密指令第 12 条第 3 項）。

④ 特段の事情がない限り、上記①c.及び d.の費用は、侵害者が負担する（EU 営業秘密指令第 12 条第 4 項）。

⑤ 管轄司法機関が、EU 営業秘密指令第 12 条に基づく措置に従わない者に対し、効果的、比例的かつ抑止効果のある制裁（反復的な罰金の支払い（recurring penalty payments））を課すことができる（EU 営業秘密指令第 16 条）。

(2) 申立要件、保護措置、代替措置（第 13 条）

① 加盟国は、EU 営業秘密指令第 12 条の差止命令及び是正措置の申立てを審理し、その比例性を評価する際に、管轄司法機関が、当該事件の具体的状況を考慮に入れることを義務づけるものとし、これには、適切な場合、以下を含むものとする（EU 営業秘密指令第 13 条第 1 項）。

a. 営業秘密の価値又はその他の特徴
b. 営業秘密を保護するために講じられた措置
c. 営業秘密を取得、使用又は開示する際の侵害者の行為
d. 営業秘密の違法な使用又は開示の影響
e. 当事者の正当な利益及び措置の許否が当事者に与え得た影響
f. 第三者の正当な利益
g. 公共の利益
h. 基本的権利の保護

管轄司法機関が、第 12 条第 1 項 a.及び b.の停止・禁止期間を限定する場合、侵害者が営業秘密の違法な取得、使用又は開示により得た可能性のある商業的又は経済的利益を失わせるのに、十分な期間としなければならない。

② 加盟国は、当該情報が、被申立人の責に帰すことができない理由により営業秘密としての要件（EU 営業秘密指令第 2 条第 1 号）を満たさなくなった場合、被申立人の申立てにより、第 12 条第 1 項 a.及び b.の措置を取り消させるか、又は失効させるものとする（EU 営業秘密指令第 13 条第 2 項）。

③ 加盟国は、以下の全ての条件が満たされる場合、EU 営業秘密指令第 12 条に定める措置の被申立人（侵害者）の申立てにより、管轄司法機関は、当該措置に代えて、被申立人から申立人（被害者）への金銭的補償（pecuniary compensation）の支払いを命ずることができる旨を定めなければならない（EU 営業秘密指令第 13 条第 3 項）。

a. 被申立人が営業秘密の使用・開示時点で当該営業秘密が、当該情報を違法使用又は開示した者から入手されたものであることを知らずかつ知るべき理由もなかったこと。
b. 措置の実施が、被申立人に不相当な不利益をもたらす可能性があること。
c. 被申立人から申立人への金銭的補償により、合理的に、損失を補償できること。

(3) 損害賠償（第 14 条）

① 加盟国は、管轄司法機関が、被害者の申立てに基づき、故意又は過失により営業秘密の違法な取得、使用又は開示をした者に対し、営業秘密の保有者が営業秘密の違法な取得、使用又は開示によって被った、実際の損害を補償するのに適切な損害賠償金の支払いを命ずることを確保しなければならない。加盟国は、従業員の故意によらない、雇用主の営業秘密の、違法な取得、使用又は開示に対する従業員の損害賠償責任を制限できる（EU 営業秘密指令第 14 条第 1 項）。

② 損害額を算定する際、管轄司法機関は、被害者が被った経済的損失（逸失利益を含む）、侵害者の得た不当利得、適切な場合には、経済的要素以外の事項（違法な取得、使用又は開示によって営業秘密の保有者に生じた精神的損害等）を考慮に入れるものとする（EU 営業秘密指令第 14 条第 2 項）。

③ 管轄司法機関は、適切な場合には、侵害者が、当該営業秘密の使用許諾を受けたとすれば支払われるべきであったロイヤルティ等を基礎として、損害賠償額を算定できる（EU 営業秘密指令第 14 条第 2 項）。

4 まとめ

EU 営業秘密指令は、営業秘密の違法取得、使用又は開示に対して、民事上の救済措置を加盟国に規定するよう義務づけている。救済措置には、暫定的措置・予防的措置（使用停止・禁止等）、本案での差止命令・是正措置、及び故意・過失に基づく損害賠償が含まれる。場合によっては、管轄司法機関が、差止命令や是正措置に代えて金銭的補償を命じることも認められている。なお、時効期間は最長 6 年とされ、手続濫用に対する制裁も規定されている。自社の営業秘密が侵害されている疑いが生じた場合には、立証が必要となる事由を考慮しながらどのような救済措置を求めるかを検討する必要がある。

第 6 章　刑事措置

EU 営業秘密指令は、刑事措置について規定していない[31]ものの、指令の目的が、営業秘密の侵害に対する民事上の救済措置についての十分かつ一貫した水準の確保にあることに鑑み、加盟国は、指令の保護措置を尊重する限りにおいて、これを超える範囲の保護を導入することも可能である（前文(10)）ため、各加盟国は、営業秘密侵害に対する刑事責任について規定できるとされる[32]。実際、2018 年 5 月時点においては、アイルランドを除く各加盟国が、営業秘密の保護に関する刑事措置を規定する法律を有しているとされ[33]、アイルランドにおいても、2018 年 6 月に適用が開始された EU 営業秘密指令の国内実施法[34]第 18 条において、刑事罰に関する規定が設けられている。もっとも、EUIPO によれば、営業秘密侵害に関する刑事訴追は依然として非常に稀で例外的なものであり、2023 年に実施された調査においては、少なくとも 14 の加盟国で 1 件以上の刑事訴訟が確認されるにとどまった[35]。

また、営業秘密侵害に対する刑事責任は EU 営業秘密指令の適用範囲外であるため、刑事措置について、必ずしも加盟国間で一致するとは限らない。例えば、スペインの判例では、刑事上の有罪判決を下す際に、必ずしも EU 営業秘密指令第 2 条で定義される意味での「営業秘密」の該当性を分析する必要はない、すなわち、刑法は EU 営業秘密指令第 2 条に定められた保護対象となる情報の定義に必ずしも拘束されるものではないと判示された[36]。

---

31 World Intellectual Property Organization, “OVERVIEW OF NATIONAL AND REGIONAL TRADE SECRET SYSTEMS - EUROPEAN UNION”, p.3, <https://www.wipo.int/documents/d/trade-secrets/docs-overview-country-sheets-eu-final.pdf#:~:text=6,trade%20secrets%20in%20judicial%20proceedings>.

32 EUIPO, “TRADE SECRETS LITIGATION TRENDS IN THE EU”, 2023, p.83, <https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2023_Trade_Secrets_Litigation_Trends_in_the_EU/2023_Trade_Secrets_Litigation_Trends_Study_FullR_en.pdf#:~:text=75,Presumed%20Acquisition%2C%2019%20February%202019>.

33 EUIPO, “THE BASELINE OF TRADE SECRETS LITIGATION IN THE EU MEMBER STATES”, 2018, p.415, <https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2018_Baseline_of_Trade_Secrets_Litigations_in_EU_Member_States/2018_Baseline_of_Trade_Secrets_Litigations_in_EU_Member_States_EN.pdf>.

34 S.I. No. 188/2018 - European Union (Protection of Trade Secrets) Regulations 2018.

35 EUIPO, “TRADE SECRETS LITIGATION TRENDS IN THE EU”, 2023, p.83, <https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2023_Trade_Secrets_Litigation_Trends_in_the_EU/2023_Trade_Secrets_Litigation_Trends_Study_FullR_en.pdf#:~:text=75,Presumed%20Acquisition%2C%2019%20February%202019>.

36 Tradingall Electronic S.L./Aplicaciones Electronicas y De Radiofrecuencia S.L: SAP BA 187/2019 (19 February 2019).

第 7 章　行政措置

EU 営業秘密指令は、行政措置を規定していない。なお、EU 営業秘密指令は、営業秘密の保有者に対し、公益上の理由から営業秘密を含む情報を行政機関等に開示することを求める EU 法又は国内法の適用に影響を及ぼすものではない（EU 営業秘密指令第 1 条第 2 項(b)）。

第 8 章　適用範囲

1　EU 営業秘密指令の要求事項

EU 営業秘密指令は、EU 域内の加盟国に対し、営業秘密の違法な取得、使用及び開示からの保護に関して同指令に沿った国内の法制度を整備する義務を課すものである（EU 営業秘密指令第 1 条第 1 項、第 19 条）。また、EU 営業秘密指令第 1 条第 1 項は、加盟国が国内法で必ず確保すべき最低限の調和水準を定めつつ、加盟国がより広範な保護措置を採用することを認めている[37]。そのため、各加盟国が、国内法の適用範囲を拡充することは許容されると考えられる。

2　EU 営業秘密指令により影響を受けない事項

EU 営業秘密指令は以下の事項に影響を及ぼさないと規定される（EU 営業秘密指令第 1 条第 2 項）。

① メディアの報道の自由及び多元主義を含む、欧州基本権憲章に定める表現及び情報伝達の自由の権利行使

② 公益上の理由から、営業秘密を含む情報を公衆又は行政当局若しくは司法当局に対して、それらの機関の業務遂行のために開示することを営業秘密の保有者に求める又は開示を義務づける、EU 法又は国内法の適用

③ EU 法又は国内法に定められた義務及び特権に従い、事業者から提出された情報を保持する EU の機関及び団体又は国内の公的機関が、当該情報を開示することを要求又は許容する、EU 法又は国内法の適用

④ EU 法並びに国内法及び慣行に従った、社会的パートナーの自律性及びそれらが労働協約を締結する権利

3　まとめ

EU 営業秘密指令は、営業秘密の違法な取得、使用及び開示からの保護について、加盟国に最低限の共通ルールを整備する義務を課しつつ、各加盟国がより幅広い保護

37　Davide Arcidiacono, “The Trade Secrets Directive in the International Legal Framework”, 2016, p.1078, <https://www.europeanpapers.eu/system/files/pdf_version/EP_EF_2016_I_038_Davide_Arcidiacono_00083.pdf>.

措置を講じることも認めているため、各加盟国の国内法の適用範囲の相違にも留意するべきである。一方で、同指令は、報道の自由、公益上の理由に基づく当局に対する法令上の情報提供義務、公的機関による法令に基づく情報開示、労働者団体の自律といった領域には影響を及ぼさない旨を明確にしている。

第 9 章　訴訟手続に関する諸制度

1　立証責任に関する規定・制度・運用

暫定的措置及び予防的措置（EU 営業秘密指令第 10 条）、差止命令及び是正命令（第 12 条）、損害賠償（EU 営業秘密指令第 14 条）のいずれも当事者の申立てが要求されている。

立証責任の転換については、EU 営業秘密指令において規定されていないが、営業秘密の違法な取得を推認したスペインの裁判例があり、2023 年 EU 報告書においても重要な裁判例として紹介されている。具体的には、複雑な電子機器とその組込みソフトウェアの模倣が争われた事案において、両製品が高度に複雑であるにもかかわらずほぼ同一であるという顕著な類似性は偶然では説明できないとして、直接証拠がなくても営業秘密の違法な取得を合理的に推定しうると判断された[38]。

2　証拠収集に関する規定・制度・運用

加盟国は、管轄司法機関が、EU 営業秘密指令第 10 条に定める措置（暫定的措置及び予防的措置）に関し、申立人に対し、十分な確実性をもって次の事項について確認するために、合理的に利用可能と考えられる証拠の提出を求める権限を有することを確保しなければならない（EU 営業秘密指令第 11 条第 1 項）。

① 営業秘密が存在すること
② 申立人がその営業秘密の保有者であること
③ その営業秘密が違法に取得された又は違法に使用若しくは開示されている、又は営業秘密の違法な取得、使用若しくは開示が差し迫っていること

3　訴訟の証拠収集等における営業秘密の保護に関する規定・制度・運用

① 加盟国は、営業秘密の違法な取得、使用又は開示に関する訴訟手続において、当事者、その弁護士若しくはその他の代理人、裁判所職員、証人、専門家、及び当該訴訟手続に関与するその他の者、又は当該訴訟手続の一部を構成する文書にアクセスできる者が、利害関係人の正当な理由付けのある申立てに基づき管轄司法機関が秘密と認定した営業秘密又は営業秘密であると主張される情報について、

38　Tradingall Electronic S.L./Aplicaciones Electronicas y De Radiofrecuencia S.L: SAP BA 187/2019 (19 February 2019).

当該手続への参加又は文書へのアクセスによって知り得た内容を使用し又は開示することを禁止する措置を確保しなければならない。加えて、加盟国は、管轄司法機関が、職権でこれらの措置を講じることを認めることもできる（EU 営業秘密指令第 9 条第 1 項）。

上述の守秘義務は、訴訟手続が終了した後も、引き続き有効に存在するが、以下のいずれかの場合に消滅する（EU 営業秘密指令第 9 条第 1 項）。

a. 終局判決により、営業秘密が、EU 営業秘密指令第 2 条第 1 号に定められた営業秘密の要件を満たさないことが判明した場合

b. 当該営業秘密が、通常その種の情報を扱う業界内部者の間で、一般的に知られるようになるか、容易にアクセスできるようになった場合

② 加盟国は、管轄司法機関が、申立て又は職権により、営業秘密の侵害に関する訴訟手続で使用又は参照された営業秘密の秘密性を保護するために必要な特定の措置を講じることができるよう確保しなければならない。秘密保持措置には、少なくとも以下が含まれる（EU 営業秘密指令第 9 条第 2 項）。

a. 当事者、又は第三者によって提出された、営業秘密を含む文書について、その全部又は一部へのアクセスを、限定された人数に制限すること

b. 営業秘密が開示される可能性がある審理及びその記録等へのアクセスを、限定された人数に制限すること

c. a.及び b.にいう限定された人数以外の者に対しては、営業秘密を含む部分が削除又はマスキングされた非機密版の判決文にアクセスできるようにすること

③ なお、上記②a.及び b.にいう限定された人数は、実効的救済及び公正な司法手続を受ける各当事者の権利を確保するために必要な最小限度を超えてはならず、少なくとも各当事者につき少なくとも 1 名の自然人と、その弁護士又はその他の代理人を含めなければならない（EU 営業秘密指令第 9 条第 2 項）。

④ 加盟国は、第 9 条に基づき採用された措置に従わない、又は従うことを拒否する者に対し、管轄司法機関が制裁を科すことができるよう確保しなければならない（EU 営業秘密指令第 16 条）。

4 まとめ

EU 営業秘密指令には立証責任を定める規定は設けられていない。暫定的措置・予防的措置の申立てに際しては、営業秘密の存在・保有・侵害の蓋然性について合理的に利用可能な証拠の提出が求められる。また、訴訟段階での営業秘密の漏えいを防ぐため、文書・審理へのアクセス制限など、秘密保持措置が義務づけられている。このような EU 営業秘密指令の規律を把握することは、各加盟国の営業秘密侵害事件における訴訟手続を理解するうえで有益である。

第 10 章　営業秘密侵害事件の動向

1　EU の営業秘密侵害事件の統計情報

2023 年 EU 報告書によると、2017 年 1 月 1 日から 2022 年 10 月 31 日までに公表された判決として、合計 695 件の営業秘密侵害事件に関する報告を EU 加盟の 27 か国から受けたとされ、EU の営業秘密侵害事件の動向について以下のように報告されている[39]。

報告された訴訟件数	695 件
上訴率	46%
侵害請求の勝訴率（侵害認定に至った請求の割合）	27%

(1)　訴訟の分類[40]

ほとんどの事件は民事事件と分類され（89%）、行政事件（5%）及び刑事事件（5%）と分類されるものは少数にとどまった。

(2)　技術情報・商業情報の動向[41]

営業秘密のうち、33%は技術情報、62%は商業情報として分類された。訴訟において最も取り上げられた技術情報の種類は、「製造プロセス／ノウハウ」（19%）であった。「試作品／未公開の製品設計」と分類された情報は、手続全体のわずか 3%にとどまった。他方、訴訟において、最も取り上げられた商業情報の種類は、「下流情報（流通方法、広告戦略、マーケティングデータ、顧客リスト）」（31%）及び「財務情報（価格設定モデル、会計データ）」（13%）であった。

(3)　訴訟手続[42]

最も多く確認された侵害請求は、「無断使用／開示：秘密保持契約違反」（29%）及び「無断使用／開示：無断取得に基づくもの」（23%）であった。次いで確認された侵害請求は、「許容された取得（直接アクセス又はその他の不公正な手段によるもの）」（20%）及び「無断使用／開示：契約上の制約違反」（14%）であった。一方、「第三者による違法取得を知りつつ取得・使用・開示した」との請求は比較的少数で、報告された侵害請求のわずか 4%にとどまった。

被告側の主張のうち最も多く主張された反論は、「主張された情報は一般に知

39　2023 年 EU 報告書 19 頁、25 頁。

40　2023 年 EU 報告書 24 頁。

41　2023 年 EU 報告書 30 頁。

42　2023 年 EU 報告書 33 頁～35 頁。

られているため、営業秘密は存在しない」というものであった。2 番目に多かった反論は、「情報が開示されないようにするために必要な合理的措置を原告が講じていなかったため、営業秘密は存在しない」というものであった。営業秘密指令第 5 条に基づく例外（例：表現及び情報の自由の行使に関するもの）が抗弁として主張されることは非常に稀であった。

(4) 訴訟結果に関する動向[43]

全体の申立ての認容率は 27%であり、これは、侵害について実質的な判断が示された手続の 73%において、被告側に有利な判断が下されたことを意味する。ただし、この結果が必ずしも被告側の主張した反論の成功に起因するとは限らない。原告は、手続的な理由[44]やその他の理由で敗訴する可能性があるほか、被告が明示的に主張していない反論を裁判所が判断に用いる場合もある[45]。

本案において最も認められた措置は、敗訴した被告による営業秘密の使用の停止及び／又は禁止を命じるものであった。侵害品の回収、撤去、変更又は破棄を明示的に命じる措置は比較的稀であり、確認されたのはわずか 15 件にとどまった。合計 107 件の手続で損害賠償が認められており、その根拠として最も一般的であった根拠は、原告が被った経済的不利益であった。損害賠償額を正確に把握できたのは60件のみであったところ、下記のとおり、認容された損害賠償額には大きなばらつきがみられた。

指標	金額（ユーロ）
最大値	7,852,123.50
最小値	1,000.00
平均値	410,680.72
中央値	32,711.18
標準偏差	1,236,095.52

2 参考になる裁判例

(1) 前提

EU 営業秘密指令は「規則」とは異なり加盟国に対して国内法を指令が求める水準に整備する義務を課すにとどまる。また、同指令の実施が不完全な場合であっても、その規定から私人間の権利義務は直接生じないと解されている。したがって、EU 営業秘密指令第 10 条、第 12 条及び第 14 条以下に定められた各種の

43 2023 年 EU 報告書 39 頁～40 頁。

44 原文に沿って説明しているが、侵害に関する実質的な判断が示された事案において被告側に有利な判断が行われた理由として手続的な理由を挙げている趣旨については、各国の訴訟実務を踏まえた検討が必要になると考えられるため精査していない。

45 2023 年 EU 報告書 34 頁。

請求権に係る規定が私人間の紛争において直接適用されることはない[46]。

もっとも、直接適用が否定されるとしても、これによって指令が国内法秩序に影響を及ぼさないわけではない。EU 機能条約[47]第 288 条第 3 文、欧州連合条約[48]第 4 条第 3 項に基づき、国内実施法は指令の文言及び目的に可能な限り整合的に解釈されるべきものとされている[49]。

以下では、EU 営業秘密指令の中心的な概念の一つである「営業秘密」について加盟国の裁判所がどのように解釈したのか概観する趣旨で、2023 年 EU 報告書でも重要な判決と指摘される[50]下記オーストリア最高裁判所判決を紹介する。

(2) オーストリア最高裁判所　事件番号 4Ob188/20f（2021 年 1 月 26 日）[51]

ア　事案

原告企業の元従業員である被告 2 及び被告 3 は、在職中に原告の機密設計データを収集・コピーし、退職後に有限責任会社である被告 1 を設立して利用した。被告らはデザイナーに原告の図面をテンプレートとして使用させ、約 25 時間分の設計作業を節約した。

原告はこれを営業秘密の違法取得・違法使用として民事訴訟を提起した。

イ　判断

被告らは、原告のデータは一般に知られ、第三者が容易に把握できる技術水準に属するため、営業秘密ではないと主張した。

下級審は、当該データは公知ではなく、適切な秘密保持措置の対象にもなっていたものの、平均的な能力を有するデザイナーであれば問題となる設計の作成に要する時間はおよそ 40 ないし 50 時間であるところ、図面使用で節約されたのは約 25 時間にすぎず、EU 営業秘密指令がいう商業的価値を有しないとして請求を棄却した。

最高裁も、営業秘密の各概念を検討したうえで、営業秘密の保護にあたり、当事者間の競争関係や競争への特別な影響は要件ではないことを指摘し、下級審の判断を支持した。

本判決は、特に、営業秘密の違法使用が、営業秘密の保有者の商業的利益や戦略的地位を損なうほど広範なものでない場合には、「商業的価値」の要

46 Trebeck/Schulte-Wissermann,“Die Geheimnisschutzrichtlinie und deren Anwendbarkeit”, 2018, Rn. 1176.

47 Treaty on the Functioning of the European Union.

48 Treaty on European Union.

49 Trebeck/Schulte-Wissermann,“Die Geheimnisschutzrichtlinie und deren Anwendbarkeit”, 2018, Rn. 1176.

50 2023 年 EU 報告書 103 頁～105 頁。

51 OGH 4Ob188/20f (RS0133480).

件は充足しないと示した点が重要であるとされる[52]。

3　まとめ

EU では 2017 年～2022 年の間に 695 件の営業秘密侵害事件が報告されており、その大半が民事事件で、商業情報を巡る紛争が多かった。侵害請求としては、秘密保持契約の違反や無断取得に基づく使用が中心であり、これに対して被告が主張する典型的な抗弁は「情報が公知であること」及び「合理的措置が講じられていないこと」の 2 点であった。原告の勝訴率は 27%にとどまり、主要な救済は営業秘密の使用の停止・禁止命令であり、侵害品の回収・撤去等を命じる措置は比較的少なかった。損害賠償は 107 件で認められたものの、その金額には大きな幅があり、中央値は約 3.3 万ユーロであった。このように、営業秘密侵害を主張する原告の主張立証は必ずしも容易ではないため、営業秘密の管理体制の整備や従業員及び取引先との契約内容の検討は、裁判での営業秘密該当性や侵害行為の主張立証を見据えながら慎重に行うべきである。

第 11 章　EU の法律・制度・運用を踏まえた、営業秘密漏えい対策を実施するにあたってのポイント

1　EU において営業秘密漏えい対策を実施するにあたってのポイント・留意点

EU における営業秘密漏えい対策としては、営業秘密の保護及び管理のポイントについて説明する欧州知財ヘルプデスクによるガイダンス[53]が参考になる。同ガイダンスにおいて示される営業秘密漏えい対策のポイント・留意点は以下のとおりである。

(1)　営業秘密及びその保有者であることの特定

営業秘密が保護されるためには、まず当該情報を適切に特定するべきでる。これは、企業が自社の資産を慎重に精査し、保有する営業秘密を特定することを意味する。そのうえで、誰がその情報にアクセスできるかを明確に定めるべきである。

また、将来的に法的紛争が生じうる場合に備え、問題となる営業秘密を保有している証跡を確保しておくことも有用である。なお文書等の作成日を取得する手段として、例えば以下の手段が含まれる。

①　文書への公証人の公証印
②　公的機関による証明
③　証人による証言書

52　2023 年 EU 報告書 105 頁。

53　European IP Helpdesk, “Trade Secrets: Managing Confidential Business Information”, April 2021, p.7-10, <https://op.europa.eu/en/publication-detail/-/publication/5f1c6d8a-f015-11eb-a71c-01aa75ed71a1/language-en>.

④ 知財当局が提供する日付証明メカニズムの利用（envelope Soleau、i-DEPOT、WIPO Proof など）

(2) 技術的保護措置

営業秘密を、許可を受けた者のみがアクセスできる場所（アーカイブ、金庫など）に安全に保管するとともに、情報にアクセスできるのは、業務上その情報を知る必要のある者に限定すべきである。

電子的に保存された情報には、パスワード管理やアクセス履歴を追跡できる監視機能など、最低限の技術的保護措置を講ずるべきである。さらに、最新の OS やウイルス対策ソフトの利用、定期的なバックアップ、バックアップメディアの施錠設備での保管も重要である。

営業秘密の不正取得リスクは、現従業員、元従業員、競合企業、サプライヤーなど多様な主体から発生しうるため、外部及び内部双方の脅威に備え、クリーンデスクポリシー、入退室管理、ファイル・フォルダ・コンピュータを保護するパスワード使用、シュレッダー・施錠措置等の基本的な対策も併せて講じるべきである。

(3) 秘密保持条項及び秘密保持契約（NDA）

企業は従業員及び取引先との契約に秘密保持条項を盛り込む、又は秘密保持契約（Non-Disclosure Agreement、いわゆる「NDA」）を締結することを検討すべきである。また、営業上の重要な情報は、新たなビジネス関係の開始を検討する相手方にとって決定的な要素になりうることから、交渉段階で価値のある情報を開示する前に NDA を締結することが有益となる。

(4) 競業避止条項及び競業避止契約

競業避止条項及び競業避止契約は、従業員や取引先が企業の機密文書にアクセスすることで相当なノウハウを取得しうる場合に、当該従業員や取引先との関係を規律するうえで特に有用である。具体的には、退職する従業員や取引先が競合他社のために働くことが禁止される期間を定めることにより、情報の流出防止に資する。

競業避止の規定は、雇用契約や業務提携契約に盛り込むことができるほか、当事者間で別途契約として締結することもできる。

従業員や退職者の競業避止義務に制限を課す法的枠組みは、EU 域内の加盟国

間において異なっており、例えばドイツ[54]やベルギーでは、競業避止条項が有効となるために従業員への金銭的補償が要件とされているのに対し、オランダでは、競業避止条項の有効性は裁判で争いうるものの、法定の成立要件としては、書面による作成及び成人の従業員による署名が求められているにとどまる[55]。

(5) 勧誘禁止条項及び勧誘禁止契約

勧誘禁止契約とは、従業員が退職後に企業の顧客を自ら又は競合他社の利益のために勧誘しないことを約するものであり、別途契約として締結できるほか、雇用契約に条項として盛り込むこともできる。特に、顧客層が限定されている業態、例えば専門的な営業分野などでは、有用な手段となる。

また、競合企業同士が、互いの従業員を勧誘しないことを明示的に合意する目的で勧誘禁止契約を締結する場合もある。なお、2025 年 6 月 2 日、欧州委員会は EEA 域内における食品及びその他の製品のオンライン注文・配送分野における引抜禁止協定（相互に相手方の従業員を引き抜かないことに関する合意又は協調的行為）を締結していた大手フードデリバリー企業 2 社に対し、合計約 3 億 2,900 万ユーロの制裁金を賦課する決定を公表した[56]。これまで、雇用市場は競争法上の問題としてあまり意識されてこなかったが、今後は競争法の観点からも十分な留意が必要である。

(6) 文書のマーキング

文書のマーキングは、当該文書が適切に取り扱われ、秘密保持義務が確実に履行されることを担保するために必要な措置である。文書には、例えば次のような表示を付すことができる。

① 機密
② 第三者機密
③ 複写禁止
④ 配布先限定

---

54 販売事業を行う事業者（法人、自然人を問わない）（Handlungsgehilfe）については競業避止義務についての法令上の規制がある（Handelsgesetzbuch (HGB) 第 60 条、第 74 条）ところ、従業員及び元従業員に対する競業避止義務の有効性は、販売事業者に対して課される競業避止義務に関する規律が裁判例上参照され、(1)雇用者に正当なビジネス上の利益があること、(2)競業避止が不合理なものでないこと、(3)期間が 2 年を超えないこと、(4)退職後の競業避止義務については雇用者が相当の補償金（直近の報酬の 50%程度）を支払うこと等を考慮の上、個別具体的に判断されている。

55 Zekic Nuna, “Non-compete clauses and worker mobility in the EU”, November 2022, p.3, <https://repository.tilburguniversity.edu/server/api/core/bitstreams/2af0a187-20e1-4441-84be-3128b88a8024/content>.

56 European Commission, “Commission fines Delivery Hero and Glovo €329 million for participation in online food delivery cartel”, June 2025, <https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1356>.

⑤　NDA 対象

これらの各分類は、さらに CRITICAL（最重要）、MAXIMUM（高）、MEDIUM（中）、MINIMUM（低）といったレベルに細分化することも可能である。

(7)　従業員の教育及び監督

従業員に対しては、企業の営業秘密方針及び機密情報の取扱方法について周知徹底するための教育を行うべきである（特に会社外の行動について）。情報セキュリティ監査を実施し、現従業員の機密保持規程への遵守状況を確認するとともに、義務違反を行った退職者に対して必要な対応をとるなどの従業員の行動を監督することも効果的な手段である。

2　ライセンス、生産委託、合弁会社設立で気をつけるべきポイント

ライセンス、生産委託、合弁会社設立を行うにあたっては、当事者間で秘密情報のやりとりが見込まれるため、営業秘密としての保護を維持するために秘密保持義務を明記すべきである。契約の準拠法は各契約において定められる国の法令となるところ、これらの契約は営業秘密その他の知的財産権や有形資産といった自社の競争力の源泉となるアセットを利用させる重要な契約となることが多いため、社内にノウハウが蓄積していない場合にはそもそも関係国の現地法弁護士に相談すべき性質の契約ではあるが、営業秘密の保護という観点でも慎重な検討を要する。以下では、EU において一般的に留意すべきと考えられているポイントを説明する。

(1)　ライセンス契約

特許権のライセンスに加え、その実施、製造、運用などに不可欠な特許化されていない技術情報（ノウハウ）も併せてライセンスの対象とすることが有益である場合がある。もっとも、ノウハウがライセンスの対象となり相手方に提供される場合においても営業秘密として法的保護を維持するためには、当該情報が、「営業秘密」（EU 営業秘密指令第 2 条第 1 号）の定義、すなわち、秘密性・商業的価値・合理的な措置の 3 要件を充足し続ける必要がある。そのため、ノウハウをライセンスの対象に含める契約においては、ノウハウの使用・開示方法をできる限り明確に定めるとともに、ライセンシーやその関係者（例えば、ライセンシーの従業員や委託先など）に対してライセンサーが営業秘密を保護するために設定した水準と同等以上に厳格な秘密保持義務を課すことが重要である。また、契約期間に関しては、特許とその他のノウハウを合わせてライセンスする場合、特許権のライセンス期間は特許権の存続期間内に限定される一方で、ノウハウライセンス部分は、営業秘密としての性質が維持される限りにおいて、特許権の存続期間を超えて存続させることも可能であるため、両者を明確に区別して規定す

べきである[57]。

(2) 生産委託契約

(1)に列挙した注意点は、生産委託契約にもあてはまる。

委託者としては、受託者の生産ラインの運営状況、生産品の数量などの確認体制、保存・管理状況を十分確認することが、特に重要である。そこで、契約書にも、これらの事項について、受託者に報告、保証、あるいは誓約をするよう義務づけることを検討すべきである。

また、生産委託契約では、受託者が第三者の機密情報、営業秘密情報を保有していて、委託者の製品の製造に使用してしまった場合、第三者から、機密情報・営業秘密の違法使用、開示にあたるとして法的請求を受ける可能性がある。委託者自身が当該事実を認識していない場合であっても、受託者に対する差止命令その他の法的措置により、結果として製品の製造や供給に重大な支障をきたす可能性がある。そこで、生産された製品が、受託者と取引関係のある、他社の機密情報・営業秘密の侵害をしないことを誓約する、保証を要求することを検討すべきである。

さらに、機密情報、営業秘密へのアクセス、使用目的、使用方法の限定に関して、受託者から第三者への再委託を禁止することも考慮すべきである。

(3) 合弁契約

合弁会社は、参加当事者が提供した、あるいは、合弁会社自身が調達した人材、技術、データ、施設及び資材を使用して、事業を行うことが多い。参加者の様々な機密情報、営業秘密が提供されることもある。

したがって、合弁会社が研究や開発をして得られる成果物に対して、どの者に所有権あるいは管理権が帰属するのかを契約で明確化しておくことが、特に重要になる。

3 まとめ

EU で営業秘密を保護するためには、情報の特定、アクセス管理、証跡確保を行い、物理的・技術的措置と NDA 等の契約管理を組み合わせた多層的な保護体制を構築すべきである。また、文書のマーキングや従業員教育を通じて、内部・外部双方の漏えいリスクに備えることも重要である。さらに、営業秘密の提供を伴う契約上、秘密保持義務は汎用的に重要となるが、ライセンス契約ではノウハウの使用・開示方法の明確化、生産委託契約では第三者権利侵害防止の保証や再委託の禁止、合弁契約で

57 European IP Helpdesk, “Europe - Frequently Asked Questions (FAQ) - Trade Secret - What is a “patent and know-how licence” and when is it useful?”, <https://intellectual-property-helpdesk.ec.europa.eu/regional-helpdesks/european-ip-helpdesk/europe-frequently-asked-questions_en#Licences>.

は成果物の権利帰属の明確化など、契約類型に応じた内容を規定する必要がある。

ドイツ

第 1 章　営業秘密の保護体系

1　保護体系の概要

EU 第 2 章 1.に記載したとおり、EU 営業秘密指令は、加盟国に対して営業秘密の違法な取得、利用及び開示に対する民事法上の救済を確保するよう義務づけている（EU 営業秘密指令第 6 条第 1 項）。ドイツにおいては、従来、主として不正競争防止法（Gesetz gegen den unlauteren Wettbewerb（以下「UWG」という））[58]第 17 条から第 19 条までの刑事罰に係る規定及びドイツ民法（Bürgerliches Gesetzbuch（以下「BGB」という））[59]により保護されてきたものの、営業秘密保護法の立法資料（以下「ホワイトペーパー」という）[60]において、EU 営業秘密指令により求められる水準を十分に実現するものではないと評価され、2019 年 4 月に営業秘密保護法（Gesetz zum Schutz von Geschäftsgeheimnissen。以下「GeschGehG」という）[61]が施行された。

GeschGehG の構成は以下のとおりである[62]。

① 第 1 章：一般規定

a. 営業秘密の定義を規定する（GeschGehG 第 2 条第 1 号）とともに、営業秘密を保護するための禁止事項を定めており（GeschGehG 第 4 条）、これに違反した場合には営業秘密の違法な取得、使用又は開示が成立するものとされる。

b. GeschGehG 第 5 条は、個別の事案において GeschGehG 第 4 条の違反が正当化されうる例外規定を定めている。

② 第 2 章：侵害時の請求権

a. 営業秘密の違法な取得、使用又は開示があった場合において、営業秘密の保有者が侵害者に対して請求できる権利が規定されている。

b. これには、消去及び差止請求権（GeschGehG 第 6 条）、廃棄、引渡し、回収、撤去及び撤退請求権（GeschGehG 第 7 条）、情報提供を求める権利（GeschGehG 第 8 条）、並びに故意又は過失による侵害に対する損害賠償請

---

58 Gesetz gegen den unlauteren Wettbewerb (UWG), <https://www.gesetze-im-internet.de/uwg_2004/BJNR141400004.html>.

59 Bürgerliches Gesetzbuch, <https://www.gesetze-im-internet.de/bgb/>.

60 Bundestag, “Drucksache 19/4724”, 04 October 2018, p.1, <https://dserver.bundestag.de/btd/19/047/1904724.pdf>.

61 Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG), <https://www.gesetze-im-internet.de/geschgehg/BJNR046610019.html>. 英語訳 <https://www.gesetze-im-internet.de/englisch_geschgehg/>.

62 ホワイトペーパー1 頁～2 頁。

求権（GeschGehG 第 10 条）が含まれる。

③ 第 3 章：営業秘密紛争における訴訟手続

a. 営業秘密の侵害に関する訴訟手続について規定されている。

b. 特に、GeschGehG 第 16 条から第 20 条までにおいては、裁判手続における秘密保持に関する規定が設けられている。

④ 第 4 章　刑事規定

a. 削除された UWG 第 17 条から第 19 条までの営業秘密保護のための刑事規定が GeschGehG 第 23 条に規定されている[63]。

2 営業秘密関連の法改正の動き

GeschGehG は、施行以来、2026 年 1 月末時点まで改正されていない。なお、2024 年 10 月、民事訴訟法（Zivilprozessordnung）[64]を改正し、新たに民事訴訟法第 273a 条が追加された[65]ことにより、裁判所は、当事者の申立てに基づき、争点となっている情報が GeschGehG 第 2 条第 1 号に定める営業秘密に該当しうる場合には、当該情報の全部又は一部を秘密として取り扱うべき情報と分類できるようになった。この場合、GeschGehG 第 16 条から第 20 条までの規定が準用される。詳細については、第 8 章「訴訟手続に関する諸制度」で説明する。

3 その他営業秘密・技術流出に関する法律

(1) 不正競争防止法（UWG）

UWG[66]は、競争事業者、消費者その他の市場参加者を不正な取引行為から保護すると同時に、健全な競争に関する公共の利益を保護することを目的（UWG 第 1 条）として、不正な取引行為を禁止する法律であるところ、従来、UWG の第 17 条から第 19 条までに営業秘密を侵害した場合における刑事罰の規定が存在していた[67]。もっとも、前記のとおり、UWG 第 17 条から第 19 条までは、GeschGehG の施行により GeschGehG 第 23 条に置き換えられたことに伴い、削除

---

63 山田雄大「ドイツ営業秘密保護法罰則について」（2022 年）42 頁＜https://www.jstage.jst.go.jp/article/takahogaku/41/0/41_39/_pdf/-char/ja＞。

64 Zivilprozessordnung, <https://www.gesetze-im-internet.de/zpo/index.html#BJNR005330950BJNE169500125>.

65 Bundesministerium der Justiz und für Verbraucherschutz, “Gesetz zur Stärkung des Justizstandortes Deutschland durch Einführung von Commercial Courts und der Gerichtssprache Englisch in der Zivilgerichtsbarkeit (Justizstandort-Stärkungsgesetz)”, 10 Octorber 2024, <https://www.recht.bund.de/bgbl/1/2024/302/VO.html>.

66 邦語の参考訳として、中田邦博＝カライスコス アントニオス＝古谷貴之「ドイツ不正競争防止法の意義と条文訳（2020 年改正版）」がある＜https://opac.ryukoku.ac.jp/iwjs0005opc/bdyview.do?bodyid=TD32161914&elmid=Body&fname=ssk-np_51_017.pdf&loginflg=on&once=true＞。

67 Thomas Hoeren, “The New EU Directive on the Protection of Trade Secrets and Its Implementation”, p.209.

された。

(2) 刑法

ドイツ刑法は、第 202a 条、第 203 条、第 204 条、第 355 条に基づいて営業秘密の保護を規定する。詳細については、第 5 章「刑事措置」で検討する。

(3) データ保護法制

連邦データ保護法（Bundesdatenschutzgesetz。以下「BDSG」という）[68]は、ドイツの公的機関（一部の領域に関しては、州の公的機関を含む）の個人データの処理に適用される規律、民間事業者の個人データの処理に適用される一般データ保護規則[69]（以下「GDPR」という）を補完する規律、及び欧州刑事司法指令[70]の国内法を主に規定する。BDSG には個人データに係る情報が営業秘密を含む場合に営業秘密を保護する規定が設けられており、具体的には、法令又は性質上秘密として保持しなければならない情報（特に第三者の正当な利益が優越する場合）が開示されることとなるときは、GDPR 上の第三者から取得した個人データに関する情報提供義務（GDPR 第 14 条）やアクセス権（GDPR 第 15 条）、データ主体に対するデータ侵害通知義務（GDPR 第 34 条）は適用されない（BDSG 第 29 条第 1 項）。但し、データ主体に対するデータ侵害通知義務は、損害のおそれ等を考慮してデータ主体の利益が秘密保持の利益を上回る場合には、適用されることとなる。

4 サイバーセキュリティ政策

2021 年 9 月 8 日、ドイツ連邦内閣（Bundeskabinett）は、今後 5 年間のサイバーセキュリティの枠組みとして、公式戦略文書「ドイツのサイバーセキュリティ戦略 2021」（Cyber-Sicherheitsstrategie für Deutschland 2021、以下「2021 年戦略」という）

---

68 Bundesdatenschutzgesetz (BDSG) vom 30.Juni 2017 (BGBl. I S.2097), <https://www.gesetze-im-internet.de/bdsg_2018/>.

69 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>.

70 Directive (EU) 2016/680 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, <https://eur-lex.europa.eu/eli/dir/2016/680/oj/eng>.

を採択した[71]。2021 年戦略において、「社会」「経済」「国家」「EU／国際」の四つの行動分野に焦点をあてると同時に各分野において 44 の戦略目標が示された[72]。

① 第 1 の行動分野「デジタル化された環境における安全かつ自律的な行動」（Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung）では、市民すなわち社会全体が中心に据えられている。当該分野における 10 の戦略目標は、市民がデジタル技術の利点を活用しつつ、デジタル環境において安全かつ自律的に行動できるようにすることを目的とする。

② 第 2 の行動分野は「国家と経済の共同任務」（Gemeinsamer Auftrag von Staat und Wirtschaft）を標題とする。当該分野における 13 の戦略目標は、経済全体におけるサイバーセキュリティを強化すると同時に重要インフラにも焦点を当てる。

③ 第 3 の行動分野「効率的かつ持続可能な国家全体のサイバーセキュリティ・アーキテクチャ」（Leistungsfähige und nachhaltige gesamtstaatliche Cybersicherheitsarchitektur）では、サイバーセキュリティに関与する国家の主体及びこの分野において必要とされる発展が焦点とされる。当該分野における 14 の戦略目標は、とりわけ当局間の効果的な協力を妨げる障壁を除去するとともに、サイバー空間において不断に変化する要請を明確化し、それに対応するため当局が十分な能力と権限を備えることを目的としている。

④ 第 4 の行動分野「欧州及び国際的なサイバーセキュリティ政策におけるドイツの積極的関与」（aktive Positionierung Deutschlands in der europäischen und internationalen Cybersicherheitspolitik）は、EU 及び NATO におけるドイツの取組に焦点を当てる。当該分野における 7 つの戦略目標は、これらの機関におけるサイバーセキュリティ政策の基盤及び手段の更なる発展を目的としている。

2025 年 8 月 31 日、ドイツ連邦内務省（Bundesministerium des Innern）は、2021 年戦略について評価する「2021 年ドイツ・サイバーセキュリティ戦略の評価」（Evaluierung der Cybersicherheitsstrategie für Deutschland 2021）を公表した[73]。評価結果によれば、2021 年戦略における施策の大部分は既に実施が完了しているか、少なくとも実施段階にあることが明らかとなった。最も多く施策の実施が完了していると評価された行動分野は、第 2 の行動分野である（35%が実施済みとされる）が、当該行動

---

71 Bundesministerium des Innern, “Cybersicherheits-strategie für Deutschland 2021 beschlossen”, 08 September 2021, <https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2021/09/cybersicherheitsstrategie-2021.html>.

72 Bundesministerium des Innern, für Bau und Heimat, “Cybersicherheitsstrategie für Deutschland 2021”, 08 September 2021, p. 6-7, <https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/2021/09/cybersicherheitsstrategie-2021.pdf?__blob=publicationFile&v=3>.

73 Bundesministerium des Innern, “Evaluierung der Cybersicherheitsstrategie 2021”, 31 August 2025, <https://www.publikationen-bundesregierung.de/pp-en/search-for-publications/cybersicherheitsstrategie-2021-2383352#:~:text=Date%20of%20publication%3A%2031.2025>.

分野において、国内認証（nationalen Zertifizierungen）、中小企業の十分な参画の欠如及び国家サイバーセキュリティ評議会（Nationale Cyber-Sicherheitsrat）の役割については、批判的に評価されている。第 3 の行動分野における多くの施策は、依然として初期段階にあり、38%は計画中、46%は実施過程にあるとされる。これは、連邦と州との協力強化を目的として検討されていた基本法の改正が実現できず、また議会構成のもとではもはや実施が不可能であるため、代替策を模索していることに起因すると考えられている。注目すべきは、一部の施策、特に第 1 の行動分野において、所管省庁の評価と関係ステークホルダーの認識との間に乖離が見られる点であるとされ、これには、テレマティクス・インフラの発展や脆弱性への対応などに関わる施策が含まれる[74]。

5　まとめ

EU 営業秘密指令の実施に伴い、ドイツでは、従来の UWG や BGB による保護では同指令の求める水準を満たしていないと判断され、2019 年に GeschGehG が制定された。GeschGehG は、営業秘密の定義、侵害時の請求権、訴訟手続、刑事措置を体系的に規律している。また、訴訟手続の局面において、2024 年には民事訴訟法が改正され、訴訟における営業秘密の取扱いに関する保護が拡充された。さらに、サイバーセキュリティに関して、2021 年に採択された国家戦略の評価が 2025 年に実施された。営業秘密に関する法制度の理解や具体的な営業秘密の管理方法及び侵害事案への対応の検討に際して、このように GeschGehG の制定の経緯や、民事訴訟法を含めた改正動向を合わせて把握しておくことは有益である。

第 2 章　営業秘密の定義

1　総論

従来、UWG 第 17 条から第 19 条までに営業秘密侵害の刑事罰に関する規定が置かれていたが、営業秘密を定義する規定は設けられていなかった[75]。そのため、営業秘密の定義は、裁判所により個別に判断されており[76]、営業秘密の概念については、決定的といいうる定義を見出し得なかったが[77]、例えば下記の要件を満たす情報について営業秘密としての保護を認めた裁判例がある[78]。

74　*Ibid*., p.2.

75　山田雄大「ドイツ営業秘密保護法罰則について」（2022 年）42 頁＜https://www.jstage.jst.go.jp/article/takahogaku/41/0/41_39/_pdf/-char/ja＞。

76　Ansgar Ohly, “The German Trade Secrets Protection Act of 2019”, 12 September 2019, p.2, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3578381>.

77　小野昌延「営業秘密の保護【増補】」（2013 年）103 頁。

78　BGH, Urt. v. 27. 4. 2006 - I ZR 126/03, GRUR 2006, 1044[1046].

① 事業に関連する情報であること
② 厳格に制限された範囲の者のみに知られていること
③ 秘密保有者が秘密保持の意思を有していること
④ 秘密保持に経済的利益が存すること

しかしながら、EU 営業秘密指令のドイツにおける国内実施法である GeschGehG の制定により、営業秘密の定義が条文上明文化されるに至った。

2 GeschGehG による定義

GeschGehG 第 2 条は、営業秘密を、以下のような情報と定義する。

① 当該情報が、全体において、又はそのコンポーネントの正確な構成と組み合わせにおいて、その種の情報を通常扱う業界内関係者の間で一般に知られておらず、又は容易にアクセス可能でなく、そのことにより経済的価値を有すること（第 1 号 a）
② 当該情報を適法に管理する者によって、その状況に応じて秘密として保持するための合理的な措置が講じられていること（第 1 号 b）
③ 秘密性を保持することについて、正当な利益が存在すること（第 1 号 c）

(1) 一般に知られていない、又は容易にアクセス可能でない情報

一般に知られていない、又は容易にアクセス可能でない情報（以下「秘密情報」という）は、特許法における「新規性」（Neuheitsbegriff）のような絶対的な概念とは異なり、相対的な概念と解されている。すなわち、ある特定の関係者にとって当該情報にアクセス可能であったか否かが秘密情報の該当性の判断にあたって重要となる[79]。ある情報が、情報の保有者及び守秘義務を負う者のみに知られている場合、たとえその範囲が広範であったとしても、当該情報は「一般に知られている」ものとは評価されない（例えば、生産設備内における業務上の事実が、当該施設で勤務する従業員に知られることがあったとしても、一般的にはそのことにより秘密性が失われるとはみなされない）[80]。また、典型的には、製造方法、顧客・仕入先リスト、原価情報、事業戦略、企業データ、市場分析、試作品、数式やレシピなどが保護対象に含まれるとされる[81]。

(2) 経済的価値

情報が経済的価値を有するとは、その情報の取得、利用又は開示が、情報保有

---

79 Ansgar Ohly, “The German Trade Secrets Protection Act of 2019”, 12 September 2019, p.3, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3578381>.

80 BGH GRUR 2018, 1161 para 38.

81 ホワイトペーパー24 頁。

者の科学的及び技術的ポテンシャル、事業上又は財産上の利益、戦略的地位又は競争力に対し、これを適法に管理する保有者の利益を毀損するおそれがある場合をいい（EU 営業秘密指令前文(14)参照）、商業化していない大学の研究成果も保護の対象になるとされる[82]。

(3) 合理的な秘密保持措置

どのような秘密保持措置（Geheimhaltungsmaßnahmen）が必要かは営業秘密の種類及び利用の具体的事情に依存するとされるが、具体的な対応として、物理的なアクセス制限、設備上の対策や契約上の保護などが挙げられる。また、秘密を保持すべき全ての情報に個別の表示を付す必要はなく、原則として特定の情報カテゴリーに対して技術的なアクセス制限などの措置を講じることや、社内規則・雇用契約書にこれを規定することが可能であるとされる[83]。

もっとも、裁判例の中には、契約上の秘密保持義務の規定のみを根拠として秘密保持措置の存在が主張された事案において、業務の過程で知り得た全ての事項や出来事を一括して秘密保持義務の対象とし、その中に営業秘密に該当しない事項も含めてしまうような契約上の取決めのみでは、秘密保持措置として十分とは認められないと判示した裁判例[84]がある点には留意する必要がある。

また、秘密保持措置の合理性を評価する際には以下のような要素が特に考慮される場合があるとされており[85]、実際に同様の基準に従って秘密保持措置の合理性を判断した裁判例[86]もあるため、これらの要素を勘案しながら営業秘密を管理すべきである。

① 営業秘密の価値及びその開発コスト(der Wert des Geschäftsgeheimnisses und dessen Entwicklungskosten)
② 情報の性質（die Natur der Informationen）
③ 企業にとっての重要性（die Bedeutung für das Unternehmen）
④ 企業の規模（die Größe des Unternehmens）
⑤ その企業における一般的な秘密保持措置（die üblichen Geheimhaltungsmaßnahmen in dem Unternehmen）
⑥ 情報の表示方法（die Art der Kennzeichnung der Informationen）
⑦ 従業員や取引先との契約上の規定（vereinbarte vertragliche Regelungen mit Arbeitnehmern und Geschäftspartnern）

---

82 ホワイトペーパー24 頁。

83 ホワイトペーパー24 頁。

84 LAG Düsseldorf, Urt. v. 3. 6. 2020－ 12 SaGa 4/20, 1(80).

85 ホワイトペーパー24 頁～25 頁。

86 OLG Stuttgart , Urt. v. 19.11.2020 – 2 U 575/19, 1(169).

(4) 正当な利益

正当な利益（berechtige Interesse）という要件の解釈を巡っては、「企業内の違法行為や不正行為に関する情報が営業秘密として保護の対象となりうるか」や「経済的価値の要件との関係性」などについて議論がなされているが、個々の事案において利益衡量を行う余地を残したものであるとの指摘もある[87]。また、裁判例には、正当な利益という要件には、特段の重要性はなく、単に軽微なケース（reine Bagatellfälle）を GeschGehG の保護対象から除外する機能を果たすと判示したものがある[88]。

3 日本法との比較

日本の不正競争防止法において、「営業秘密」は、次の 3 要件を満たすものと定義される（不正競争防止法第 2 条第 6 項）。

① 秘密として管理されていること（秘密管理性）

② 事業活動に有用な技術上又は営業上の情報であること（有用性）

③ 公然と知られていないこと（非公知性）

①秘密管理性は、GeschGehG 第 2 条第 1 号の合理的な秘密保持措置と対応関係にあるといえる。①秘密管理性は、保有者が実施する具体的状況に応じた経済合理的な秘密管理措置によって従業員等に明確に示され、当該秘密管理意思に対する従業員等の認識可能性が確保される必要がある。そして、どの程度の秘密管理措置が必要になるかについて、過去の裁判例においても、情報の性質、保有形態、情報を保有する企業等の規模等の諸般の事情を総合考慮し、合理性のある秘密管理措置が実施されていたか否かという観点から判断が行われてきた[89]。GeschGehG 第 2 条第 1 号 a の合理的な秘密保持措置は、保有者が立証責任を負う客観的な要件とされており、前記 2(3)で挙げたその判断要素は日本における秘密管理性の判断にあたって考慮されてきた要素と類似しているため、大きな差異はないように思われる。

②有用性は、GeschGehG 第 2 条第 1 号の経済的価値や正当な利益と対応関係にあるといえる。②有用性の要件は、公序良俗に反する内容の情報（脱税や有害物質の垂れ流しなどの反社会的な情報）など、秘密として法律上保護されることに正当な利益が乏しい情報を営業秘密の範囲から除外したうえで、広い意味で商業的価値が認められる情報を保護することに主眼がある[90]。他方、GeschGehG 第 2 条第 1 号 a の経済的価

87 Harte-Bavendamm/Ohly/Kalbfus, Harte-Bavendamm, “GeschGehG”, 2. Aufl., 2024, GeschGehG § 2 Begriffsbestimmungen Rn. 69a.

88 OLG Schleswig, Urt. V. 28.04.2022 – 6 U 39/21, 1(91).

89 経済産業省-知的財産政策室「逐条解説・不正競争防止法」第 3 版（2024 年）46 頁～47 頁。

90 同上 49 頁。

値は、前記 2(2)のとおり、開示により保有者の利益が害されるおそれがあれば肯定されるため、広く認められると考えられる[91]が、同号 a では EU 営業秘密指令の要件に沿って、一般に知られていない、又は容易にアクセス可能でないがゆえに経済的価値を有することが求められているため、この点は日本法上の有用性の要件とは異なる。

③非公知性は、GeschGehG 第 2 条第 1 項の秘密情報の概念と対応関係にあるといえる。③非公知性は、具体的には、当該情報が合理的な努力の範囲内で入手可能な刊行物に記載されていないなど、営業秘密の保有者の管理下以外では一般的に入手することができない状態をいい、特定の者が事実上秘密を維持していれば、なお非公知と考えられる場合がある[92]。これは、GeschGehG 第 2 条第 1 号 a の「一般に知られていない、又は容易にアクセス可能でない」という要件が、前記 2(1)のとおり、ある特定の関係者にとってアクセス可能か否か相対的に判断されるのと共通している。なお、（販売されている製品の）リバースエンジニアリングによって得られる情報の③非公知性については、日本の裁判上は、その困難性によって該否が判断されており、非公知性を認めた裁判例もある[93]ところ、同様に、ドイツの GeschGehG 第 2 条第 1 号の営業秘密の概念においても、製品の特徴が容易に認識できるようなものである場合を除き、リバースエンジニアリングが行われたとしても、その知識が他者に開示されていなければ秘密性が直ちに失われるわけではないとされる[94]。

4 まとめ

ドイツでは、従来、営業秘密について、明確な法律上の定義がなく、裁判例により個別に判断されていたが、GeschGehG の制定により、営業秘密は秘密性・経済的価値・合理的秘密保持措置・正当な利益を要件として法定された。同法は秘密性を相対的概念として捉え、製造方法や顧客リストなど多様な情報が対象となるほか、合理的秘密保持措置については様々な客観的な要素に基づいて評価される。また、日本の不正競争防止法における「営業秘密」の 3 要件（秘密管理性・有用性・非公知性）とも概ね対応関係が見られる。これらを踏まえて、保護したい情報がドイツにおいて営業秘密に該当するか検討する必要がある。

---

91 Ansgar Ohly, “The German Trade Secrets Protection Act of 2019”, 12 September 2019, p.4, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3578381>.

92 経済産業省-知的財産政策室「逐条解説・不正競争防止法」第 3 版（2024 年）50 頁～51 頁。

93 大阪地判平成 15 年 2 月 27 日最高裁 HP 参照（平成 13(ワ)10308）。

94 Harte-Bavendamm/Ohly/Kalbfus, Harte-Bavendamm, “GeschGehG”, 2. Aufl., 2024, GeschGehG § 2 Begriffsbestimmungen Rn. 33.

第 3 章　営業秘密侵害行為の定義

1　営業秘密侵害行為

(1)　総論

GeschGehG は、行為の時間的な連鎖に沿って同法上禁止される侵害行為を規定する（GeschGehG 第 4 条）。具体的には、①取得、②使用又は開示、③第三者を通じた取得、使用又は開示、④侵害品の流通という連鎖である[95]。

なお、③④のみ主観的要件を必要とする。他方で、営業秘密の侵害に基づく金銭的損害賠償は、故意又は過失による侵害行為を要件とする（GeschGehG 第 10 条第 1 項）ことには留意する必要がある。

(2)　営業秘密の取得

営業秘密の取得とは、営業秘密の保有者の適法な管理下にあり、営業秘密を含む若しくは営業秘密を推測できる文書、物、原料、材料、若しくは電磁的情報への無権限のアクセス（Zugang）、領得（Aneignung）若しくは複製（Kopieren）、又はその都度の状況下において、公正な商慣習を考慮して、信義誠実の原則に反するあらゆる行為をいう（GeschGehG 第 4 条第 1 項）。

行為者が当該営業秘密について正当なアクセス権限等を有している場合（例えば、雇用契約等に基づいて営業秘密にアクセスする権限を持つ従業員）には、その取得行為自体は違法とならないとされる。ただし、このように取得された営業秘密を使用又は開示する行為については、GeschGehG 第 4 条第 2 項に基づき違法な使用又は開示と評価される場合がある[96]。

(3)　営業秘密の使用又は開示

営業秘密の使用又は開示とは、次に該当する者による、営業秘密の使用又は開示行為をいう（GeschGehG 第 4 条第 2 項）。

① 前項の規定によって営業秘密を自ら取得した者
② 営業秘密の使用制限義務に違反した者
③ 営業秘密の不開示義務に違反した者

「使用」とは、第三者に開示することを除いたあらゆる営業秘密の利用行為をいう。また、「開示」とは、第三者に対して営業秘密の内容を知らしめる行為を意味し、その対象が必ずしも不特定多数であることを要しない[97]。

95　Ansgar Ohly, “The German Trade Secrets Protection Act of 2019”, 12 September 2019, p.6, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3578381>.

96　ホワイトペーパー27 頁。

97　ホワイトペーパー27 頁。

(4) 第三者を通じた取得、使用（侵害品の流通）又は開示

第三者を通じた取得、使用又は開示とは、第三者を通じて営業秘密を取得した者が、当該営業秘密の取得、使用又は開示の時点で、当該第三者がGeschGehG第4条第2項に違反して営業秘密を使用又は開示したことを知っていた又は知るべきであった場合における取得、使用又は開示行為をいう（GeschGehG第4条第3項第1文）。

第三者を通じた使用には、侵害品の製造、提供、上市又はこれらの目的での輸出入若しくは保管を含む（GeschGehG第4条第3項第2文）。

GeschGehG第4条第3項は、当該営業秘密を取得、使用又は開示した者自身が自らはGeschGehG第4条第2項に違反していない場合、例えば第三者から当該営業秘密を取得したような状況を対象としている[98]。

2 許容される行為

GeschGehGは、EU営業秘密指令に従い、許容される行為を明確に定義している。

(1) 許容される営業秘密の取得

営業秘密は、特に以下の方法により取得できる（GeschGehG第3条第1項）。

① 独自の発見又は創作をすること（GeschGehG第3条第1項第1号）。

② 以下のいずれかの条件を満たす製品又は物品の観察、研究、分解又は試験を行うこと（GeschGehG第3条第1項第2号）。

a. 一般に公開されている。

b. 観察者、研究者、分解者又は試験者が適法に保有しており、かつ営業秘密の取得を制限する義務を負っていない。

③ 労働者の情報及び協議に関する権利、又は労働者代表の参加及び共同決定に関する権利を行使すること（GeschGehG第3条第1項第3号）。

GeschGehG第3条第1項第1号は、営業秘密に基づく排他的権利の創設を否定する立法意思を反映している。GeschGehG第3条第1項第2号は、製品自体から営業秘密を分解又は解析する行為（いわゆるリバースエンジニアリング）を原則として適法と位置付けている。ただし、これに対しては、依然として、知的財産法上又は不正競争防止法上の制限[99]が適用されうる点に留意する必要がある[100]。

GeschGehG第3条第1項第3号は、営業秘密の存在を理由として、労働者代表

98 ホワイトペーパー28頁。

99 ホワイトペーパーは、当該制限の具体例として、GeschGehG第3条第1項第2号aに関して、UWG第4条第3号に基づく商品・役務の出所の混同（Herkunftstäuschung）又は評価の不当利用（Rufausbeutung）に対する保護を挙げている（ホワイトペーパー26頁）。

100 ホワイトペーパー25頁～26頁。

（Arbeitnehmervertretungen）の参加権を制限できないことを確認する規定であるが、労働法上の守秘義務を別途課すことはできる[101]。

(2) 許容される営業秘密の取得、使用又は開示

営業秘密は、法律によって、法律に基づいて又は法律行為により、取得、使用又は開示できる（GeschGehG 第 3 条第 2 項）。ここでいう法律には、直接適用される EU 法も含まれるとされる[102]。

3 営業秘密侵害行為の例外

営業秘密の取得、使用又は開示が、以下などの正当な利益の保護のために行われた場合、第 4 条の禁止規定に該当しないものとする（GeschGehG 第 5 条）。

① 言論及び情報の自由の権利行使（メディアの自由及び多元主義の尊重を含む）

② 取得、使用又は開示が一般的な公共の利益の保護に資する場合における、違法行為又は不正行為の暴露

③ 労働者代表がその任務を果たしうるのに必要とされる場合に労働者代表に対する労働者による開示

4 日本法との比較

日本においては、不正競争防止法第 2 条第 1 項に、営業秘密に係る不正行為の行為類型が列挙されており、大きく分けると以下のパターンに分類される[103]。

(1) 不正取得類型（第 2 条第 1 項第 4 号）

営業秘密の保有者から不正な手段で営業秘密を取得し、その取得した営業秘密を使用、開示する行為

(2) 信義則違反類型（第 2 条第 1 項第 7 号）

営業秘密の保有者から正当に示された営業秘密を不正に使用、開示する行為

(3) 転得類型（第 2 条第 1 項第 5 号、第 6 号、第 8 号、第 9 号）

ア 取得時悪意転得類型

① 第 2 条第 1 項第 4 号の営業秘密不正取得行為の介在について知って（悪意）又は重過失により知らないで営業秘密を取得し、その取得した営業秘密を使用、開示する行為（第 2 条第 1 項第 5 号）

② 第 2 条第 1 項第 7 号の営業秘密不正開示行為の介在等について悪意又は重過失で営業秘密を取得し、その取得した営業秘密を使用、開示する行為（第 2 条第 1 項第 8 号）

---

101 ホワイトペーパー26 頁。

102 ホワイトペーパー26 頁。

103 経済産業省-知的財産政策室「逐条解説・不正競争防止法」第 3 版（2024 年）97 頁～98 頁。

イ　取得時善意転得類型

① 営業秘密を取得した後に、営業秘密不正取得行為（第 2 条第 1 項第 4 号）の介在について悪意又は重過失で当該営業秘密を使用、開示する行為（第 2 条第 1 項第 6 号）

② 営業秘密を取得した後に、営業秘密不正開示行為（第 2 条第 1 項第 7 号）の介在等について悪意又は重過失で当該営業秘密を使用、開示する行為（第 2 条第 1 項第 9 号）

(4) 営業秘密侵害品譲渡等類型（第 2 条第 1 項第 10 号）

(1)～(3)の不正使用行為により生じた物を譲渡等する行為

(1)不正取得類型及び(2)信義則違反類型は、営業秘密の取得（GeschGehG 第 4 条第 1 項）及び営業秘密の使用・開示（GeschGehG 第 4 条第 2 項）と対応関係にある。また、GeschGehG における第三者を通じた取得、使用又は開示（GeschGehG 第 4 条第 3 項）と、不正競争防止法における転得類型（不正競争防止法第 2 条第 1 項第 5 号、第 6 号、第 8 号、第 9 号）は過失か、重過失かの違いはあるものの一応の対応関係にある。

また、不正競争防止法においては、営業秘密の善意取得者保護のために、取引によって営業秘密を取得した者（その取得した時にその営業秘密について営業秘密不正開示行為であること又はその営業秘密について営業秘密不正取得行為若しくは営業秘密不正開示行為が介在したことを知らず、かつ、知らないことにつき重大な過失がない者に限る）がその取引によって取得した権原の範囲内においてその営業秘密を使用し、又は開示する行為（不正競争防止法第 19 条第 1 項第 7 号）や、継続的な不正使用行為の消滅時効期間が経過した後に当該使用に基づいて生じた営業秘密侵害品の譲渡等の適用除外規定（不正競争防止法第 19 条第 1 項第 8 号）が設けられているが、営業秘密の侵害にあたる不正競争行為の一部の類型について適用除外と定めるにとどまっている。GeschGehG で営業秘密の侵害行為にはあたらないと規定される一部の行為類型（独自の発見又は創作など）は不正競争防止法上も営業秘密の侵害には該当しないものの、言論及び情報の自由の権利行使（メディアの自由及び多元主義の尊重を含む）や、取得、使用又は開示が一般的な公共の利益の保護に資する場合における、違法行為又は不正行為の暴露といった行為類型が GeschGehG では営業秘密の侵害行為から類型的に除外されている点は日本法の建付けとは異なる。

5　まとめ

GeschGehG は、概ね EU 営業秘密指令に従い、営業秘密の侵害行為を①取得、②使用又は開示、③第三者を通じた取得、使用又は開示、④侵害品の流通という行為類型に沿って規律している。また、独自の発見又は創作やリバースエンジニアリングなど、適法と評価される取得、使用又は開示の類型も規定するとともに、公共の利益を目的とする内部告発など、一定の例外も認めている。日本の不正競争防止法との比較

では、行為類型に一応の対応関係が見られる一方、適法な行為や例外として許容される行為の範囲の間で相違が見られる。営業秘密の管理方法や契約条項の検討に際しては、これらの侵害行為の類型や例外について留意しておく必要がある。

第4章　民事措置

1　総論

GeschGehG において、営業秘密の保有者が侵害者に対して請求できる権利が規定されているところ、これには、除去及び差止請求権（GeschGehG 第 6 条）、廃棄、引渡し、回収、撤去及び撤退請求権（GeschGehG 第 7 条）、情報提供請求権（GeschGehG 第 8 条）、並びに故意又は過失による侵害に対する損害賠償請求権（GeschGehG 第 10 条）が含まれる[104]。以下では、それぞれの請求権について説明する。

2　除去及び差止請求権（GeschGehG 第 6 条）

営業秘密の保有者は、侵害者に対して当該侵害の除去を請求する権利を有し、再発のおそれがある場合又は侵害のおそれが初めて生じる場合には、差止を請求する権利を有する（GeschGehG 第 6 条）。侵害者が企業の従業員又は代表者である場合、営業秘密の保有者は、除去及び差止請求権を事業主（Inhaber des Unternehmens）に対しても行使できる（GeschGehG 第 12 条）。ここにいう事業主とは、その名及び責任において事業を営む者をいい、法人（juristische Person）、権利能力を有する人的会社（rechtsfähige Personengesellschaft、BGB 第 14 条第 2 項）、個人商人（Einzelkaufmann）がこれに該当する一方で、会社の機関（Organ einer Gesellschaft）はここにいう事業主には含まれない[105]。

除去及び差止請求権を行使することが、個々の事案において、①営業秘密の価値その他の特定の性質、②秘匿を維持するために講じられた措置、③営業秘密を取得、使用又は開示する際の侵害者の行為、④営業秘密の違法な使用又は開示の結果、⑤営業秘密の保有者及び侵害者の正当な利益並びに請求の履行が双方に及ぼしうる影響、⑥第三者の正当な利益、又は⑦公益といった要素を勘案して、不均衡となる場合には、当該請求権の行使は認められない（GeschGehG 第 9 条）。

除去請求権は、既発生の継続している侵害の排除を目的とする。除去の方法は侵害行為の性質次第であるものの、除去請求は、EU 営業秘密指令第 12 条第 2 項(b)に従い、侵害品から侵害の原因となる特定の構成要素を取り除くことによっても充足できるため、GeschGehG 第 7 条に基づく侵害品の廃棄や回収請求に比して軽微な救済手段

104　ホワイトペーパー1 頁～2 頁。

105　Harte-Bavendamm/Ohly/Kalbfus, Ohly, “GeschGehG”, 2. Aufl., 2024, GeschGehG § 12 Haftung des Inhabers eines Unternehmens Rn. 15.

であるとされる[106]。

差止請求権は、侵害（再発又は初めていずれも含む）のおそれがある場合に認められる。再度の侵害のおそれは、一般的には既に行われた侵害行為により証明されるが、侵害者が違約金付き差止宣言（strafbewehrte Unterlassungserklärung）を申し立てた場合には、その証明が覆されうる[107]。違約金の額は、相当であることが求められるところ、債務者に将来の侵害回避を十分に促す水準に設定される必要がある一方で、再度の侵害が生じた場合に債権者が被る損害と不均衡であってはならない。この判断に際しては、個別事案の事情、特に企業規模、売上高、侵害の重大性及び繰り返しの危険の程度が重要であるとされる[108]。

3　廃棄、引渡し、回収並びに市場からの除去及び撤去を請求する権利（GeschGehG 第 7 条）

営業秘密の保有者は、侵害者に対し、廃棄、引渡し、回収、並びに市場からの除去及び撤去を請求する権利を有する（GeschGehG 第 7 条）。侵害者が企業の従業員又は代表者である場合、営業秘密の保有者は、廃棄、引渡し、回収並びに市場からの除去及び撤去を請求する権利を事業主（Inhaber des Unternehmens）に対しても行使できる（GeschGehG 第 12 条）。

廃棄、引渡し、回収並びに市場からの除去及び撤去を請求する権利についても、個々の事案において、前記 2 に記載した要素を勘案しつつ、比例原則の観点から不均衡となる場合には、当該請求権の行使は認められない（GeschGehG 第 9 条）。

4　情報提供請求権（GeschGehG 第 8 条）

営業秘密の保有者は、侵害者に対し、侵害品等に関する情報の提供を請求できる（GeschGehG 第 8 条第 1 項）。また、侵害者が、故意又は重大な過失により当該情報を提供しない場合、又は遅滞、不正確若しくは不完全な形で当該情報を提供した場合、侵害者は、その結果生じた損害について、営業秘密の保有者に対して損害賠償義務を負う（GeschGehG 第 8 条第 2 項）。侵害者が企業の従業員又は代表者である場合、営業秘密の保有者は、情報提供請求権及び情報提供義務違反に基づく損害賠償請求権を事業主（Inhaber des Unternehmens）に対しても行使できるが、事業主に対する情報提供義務違反に基づく損害賠償請求権（GeschGehG 第 8 条第 2 項）の行使は、事業主が故意又は重大な過失により当該情報を提供しない場合、又は遅滞、不正確若しくは不完全な形で当該情報を提供した場合に限り認められる（GeschGehG 第 12 条）。

106　ホワイトペーパー29 頁～30 頁。

107　ホワイトペーパー30 頁。

108　Harte-Bavendamm/Ohly/Kalbfus, Ohly,“GeschGehG”, 2. Aufl., 2024, GeschGehG § 6 Beseitigung und Unterlassung Rn. 35.

情報提供請求権についても、個々の事案において、前記 2 に記載した要素を勘案しつつ、比例原則の観点から不均衡となる場合には、当該請求権の行使は認められない（GeschGehG 第 9 条）。

5　損害賠償請求権（GeschGehG 第 10 条）

GeschGehG 第 10 条は、財産的損害に対する賠償請求権（GeschGehG 第 10 条第 1 項及び第 2 項）及び非財産的損害に対する金銭補償請求権（GeschGehG 第 10 条第 1 項及び第 3 項）を規定している[109]。

財産的損害に対する損害賠償請求権における損害額の算定方法については、原告に対して以下の 3 つの方式の中から選択する権利を認めている[110]。

① 原告が自己の被った損害を詳細に算定して主張する方式
この方式は一般的な民事訴訟において通常の方法であるが、知的財産法においては侵害と財産的損害との間の因果関係を立証することが困難であるため、しばしば実効性を欠き、営業秘密の事案においても同様の問題がしばしば生じる（GeschGehG 第 10 条第 1 項）。

② 侵害者が侵害によって得た利益を基準として損害額を算定する方式
原告は GeschGehG 第 8 条に基づく情報提供請求権を行使することで、これを立証できる（GeschGehG 第 10 条第 2 項第 1 文）。

③ 侵害者が営業秘密の取得、利用又は開示につき営業秘密の保有者の承諾を得て適法に行ったとすれば支払わなければならなかったであろう仮のライセンス料に相当する額を損害額とする方式（GeschGehG 第 10 条第 2 項第 2 文）
この場合、適用されるべきは通常のライセンス料率であり、それは営業秘密の保有者自身が通常設定しているライセンス料率、又は当該市場において一般的に通用しているライセンス料率である[111]。

この点に関し、算定方法次第で結果が異なりうるところ、ある方式に基づいて算定された請求額が、別の方式で算定された請求額を大きく上回るという理由だけで直ちに否認されるものではないとした裁判例がある[112]。

非財産的損害に対する金銭的補償請求における損害額は、衡平の要件（Voraussetzung der Billigkeit）に照らして判断される[113]。金銭的損失の補償が衡平であ

---

109 Fuhlrott/Hiéramente, Spieker, “BeckOK GeschGehG”, 26. Edition, GeschGehG § 10 Haftung des Rechtsverletzers Rn.1.

110 Ansgar Ohly, “The German Trade Secrets Protection Act of 2019”, 12 September 2019, p.12, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3578381>.

111 Fuhlrott/Hiéramente, Spieker, “BeckOK GeschGehG”, 26. Edition, GeschGehG § 10 Haftung des Rechtsverletzers Rn.5.

112 OLG Düsseldorf, Urt. v. 14. 10. 2003 - 20 U 40/03 Gewinnherausgabeanspruch, 53 (54).

113 ホワイトペーパー33 頁。

るか否かは、ドイツ民法第 242 条の信義則の一般原則（allgemeinen Grundsätzen von Treu und Glauben）に従い、営業秘密侵害の事案における具体的事情、すなわち営業秘密の性質及び重要性、侵害者の行為態様、侵害の影響の持続性、侵害の内容、過失の程度等を総合的に考慮して判断される[114]。

6　まとめ

GeschGehG は、営業秘密侵害に対して、除去・差止め（第 6 条）、廃棄・回収等（第 7 条）、情報提供（第 8 条）、損害賠償請求（第 10 条）といった民事上の救済措置を規定している。このうち、除去・差止め（第 6 条）、廃棄・回収等（第 7 条）、情報提供（第 8 条）の請求権については侵害者に対して行使できるだけでなく、一定の場合には事業主に対しても行使しうる。また、これらの請求権は比例原則による制限を受ける。損害賠償請求については、営業秘密侵害を主張する者は、3 つの算定方式（営業秘密の保有者が被った損害、侵害者が得た利益、ライセンス料に相当する額）のいずれかから選択することができ、さらに、衡平の観点から非財産的損害についても金銭補償が認められている。自社の営業秘密が侵害されている疑いが生じた場合には、立証が必要となる事由を考慮しながらどのような救済措置を求めるかを検討する必要がある。

第 5 章　刑事措置

1　GeschGehG

(1)　刑事罰の対象となる行為

GeschGehG 第 4 条に規定される営業秘密の侵害行為のうち一定の場合には、刑事罰の対象となりうる（GeschGehG 第 23 条）。すなわち、①GeschGehG 第 4 条第 1 項第 1 号に違反して営業秘密を取得する行為、②GeschGehG 第 4 条第 2 項第 1 号(a)に違反して営業秘密を使用若しくは開示する行為、又は③GeschGehG 第 4 条第 2 項第 3 号に違反して、従業員が雇用関係の枠組みに基づいてアクセスした営業秘密を雇用関係の有効期間内に開示する行為は刑事罰の対象となる（GeschGehG 第 23 条第 1 項）。また、自己又は第三者の競争を促進するため、自己又は第三者の利益のため、又は事業主を害する意図をもって、②又は③の第三者の行為によって取得した営業秘密を使用又は開示する行為を行った者も処罰対象となる（GeschGehG 第 23 条第 2 項）。そして、未遂も処罰対象となる（GeschGehG 第 23 条第 5 項）ほか、刑事訴追機関が刑事訴追について特別な公の利益があるために職権による介入を必要と考える場合を除き、営業秘密の保有

114　Fuhlrott/Hiéramente, Spieker, “BeckOK GeschGehG”, 26. Edition, GeschGehG § 10 Haftung des Rechtsverletzers Rn.4.

者（法益侵害を受けた者）による告訴を必要とする親告罪である（GeschGehG 第 23 条第 8 項）。

以上で述べた GeschGehG 第 4 条の営業秘密の侵害行為と GeschGehG 第 23 条の罰則規定の対応関係を表で示すと以下のとおりである[115]。

行為類型	第 4 条（禁止規定）	第 23 条（罰則規定）
営業秘密を取得すること	第 4 条第 1 項第 1 号	第 23 条第 1 項第 1 号
	第 4 条第 1 項第 2 号	なし
営業秘密を使用・開示すること	第 4 条第 2 項第 1 号(a)	第 23 条第 1 項第 2 号
	第 4 条第 2 項第 1 号(b)	なし
	第 4 条第 2 項第 2 号	第 23 条第 3 項
	第 4 条第 2 項第 3 号	第 23 条第 1 項第 3 号及び第 3 項

(2) 加重類型

上記行為類型に該当する違反に対しては、3 年以下の自由刑又は罰金が科されるところ、以下の行為類型の違反に対しては、5 年以下の自由刑又は罰金が科される（GeschGehG 第 23 条第 4 項）。

① GeschGehG 第 23 条第 1 項又は第 2 項の場合に商業活動として行った者

② GeschGehG 第 23 条第 1 項第 2 号若しくは第 3 号又は第 23 条第 2 項の場合に国外において使用されることを知って開示した者

③ GeschGehG 第 23 条第 1 項第 2 号又は第 2 項の場合に営業秘密を国外で使用した者

2 刑法

ドイツ刑法においても、以下の態様でのデータや情報の取得、使用又は開示が刑事罰の対象として規定されている。

① 行為者のために予定されたものではなく、かつ不正なアクセスに対して特に安全措置が講じられているデータに対し、アクセス防止措置を乗り越えて、権限なく、自らアクセスし又は他人にアクセスさせた者は、3 年以下の自由刑又は罰金が科される（ドイツ刑法第 202 条 a）。

② 専門家（医師、歯科医、心理学者、弁護士又は弁理士等）としての立場で、他人の事業秘密又は営業秘密を違法に開示した者は、1 年以下の自由刑又は罰金に処する（ドイツ刑法第 203 条第 1 項）。

115 山田雄大「ドイツ営業秘密保護法罰則について」（2022 年）47 頁＜https://www.jstage.jst.go.jp/article/takahogaku/41/0/41_39/_pdf/-char/ja＞。

③　正当な権限なく、他人の秘密、特に第 203 条に基づき守秘義務を負う事業秘密又は営業秘密を利用した者は、2 年以下の自由刑又は罰金に処する（ドイツ刑法第 204 条第 1 項）。

④　権限なく、職務上知り得た他人の事業秘密又は営業秘密を開示又は使用した公務員は、2 年以下の自由刑又は罰金に処する（ドイツ刑法第 355 条第 1 項第 2 号）。

なお、ドイツ刑法に法人に刑罰を科す制度はない[116]。また、これらの犯罪に未遂犯を処罰する規定は設けられていない[117]。

上記の他、従業員であっても、立ち入りの許されていない施設に立ち入る等した場合には、不法侵入罪（ドイツ刑法第 123 条）が成立し、違法に自ら領得し又は第三者に領得させる目的で、他人の書類や物品の持ち出しがあるのであれば、窃盗罪（ドイツ刑法第 242 条、第 243 条）が成立しうる（なお、ドイツ刑法第 242 条第 2 項により窃盗の未遂犯は処罰される。）。

3　まとめ

GeschGehG 第 4 条に規定される営業秘密の侵害行為の一部は第 23 条において刑事罰の対象として規定されており、競争目的、私益目的、第三者の利益目的など、特定の主観的要件を満たす場合に処罰される。また、他人の違法行為により取得した営業秘密の使用又は開示も処罰の対象となり、未遂も罰せられる。さらに、商業活動として行った場合や、国外で使用されることを知りつつ開示した場合などの加重類型では、より重い刑罰が科される。加えて、ドイツ刑法においても、専門職に課される守秘義務違反や、不正アクセスによる秘密取得などが処罰対象とされている。従業員への教育において、刑事罰があることも周知しつつ、従業員の営業秘密の取扱いに関する意識を高めることが重要である。なお、GeschGehG 第 23 条に規定される刑事責任に関する規定は、法人には適用されない。

第 6 章　行政措置

GeschGehG において、行政措置は規定されていないが、法人の代表者が GeschGehG 第 23 条に規定される刑事責任を負い、又は違反行為を防ぐ監督義務に違反し、その結果として法人が利益を獲得した又は獲得し得た場合には、当該法人に行政法上の制裁金が課されうる（秩序違反法（Gesetz über Ordnungswidrigkeiten）[118]第 30 条、第 130 条）。

116　ローター・クーレン（岡上雅美訳）「ドイツにおけるコンプライアンスと刑法」（2013 年）166 頁＜https://www.waseda.jp/folaw/icl/assets/uploads/2014/05/A04408055-00-0470301651.pdf＞。

117　各犯罪を規定する条文には、未遂犯を処罰される旨が規定されていない。

118　Gesetz über Ordnungswidrigkeiten (OWiG), <https://www.gesetze-im-internet.de/owig_1968/index.html#BJNR004810968BJNE000393123>.

第 7 章　適用範囲

1　営業秘密の保護に関する公法上の規定の優先

営業秘密の秘匿、取得、利用又は開示に関する公法上の要件は、GeschGehG の規定に優先する（GeschGehG 第 1 条第 2 項）。したがって、GeschGehG は、例えば国家機関に対する情報請求権（Informationsansprüche gegen staatliche Stellen）、営業秘密の秘匿に関する公法上の規定（öffentlich-rechtliche Vorschriften zur Geheimhaltung von Geschäftsgeheimnissen）又は公務員の守秘義務（Verschwiegenheitspflichten für Angehörige des öffentlichen Dienstes）には適用されない（EU 営業秘密指令前文(11)及び(18)参照）[119]。

また、ドイツにおいて環境情報へのアクセスに関する規定[120]が適用される範囲において、GeschGehG の適用は除外される（EU 営業秘密指令第 1 条第 2 項(c)参照）[121]。

2　GeschGehG により影響を受けない事項

以下の事項は、GeschGehG により影響を受けない（GeschGehG 第 1 条第 3 項柱書）。

① ドイツ刑法第 203 条により不正な開示が処罰対象となる営業秘密についての職業上の法的保護及び刑事法上の保護（GeschGehG 第 1 条第 3 項第 1 号）[122]

② 言論及び情報の自由（メディアの自由及び多元主義の尊重を含む）の権利行使（GeschGehG 第 1 条第 3 項第 2 号）

③ 社会的パートナー（Sozialpartner）の自律及び既存の EU 法及び国内法に基づく労働協約を締結する権利（GeschGehG 第 1 条第 3 項第 3 号）

④ 雇用関係から生じる権利義務及び労働者代表の権利（GeschGehG 第 1 条第 3 項第 4 号）。

3　まとめ

GeschGehG は、秘密情報の取得、利用又は開示を行う公法上の義務や、環境情報へのアクセス制度などの特別法が適用される領域には及ばず、また、言論の自由や既存の EU 法及び国内法に基づく労働者代表の権利を制限するものでもない。

119　ホワイトペーパー23 頁。

120　環境情報へのアクセスに関する規定（環境情報指令（Directive 2003/4/EC）の国内法）は、営業秘密を含む環境情報の提供義務を負う公的機関及び私的機関がそれを開示すべき場合、又は開示を拒否できる場合を最終的に定めている（ホワイトペーパー23 頁）。

121　ホワイトペーパー23 頁。

122　GeschGehG は営業秘密の保護を規律するが、個人のプライバシーの保護や、病気・法律問題に関する支援を行う職業の守秘義務など、その他の義務については影響を与えない（ホワイトペーパー23 頁）。

第 8 章　訴訟手続に関する諸制度

1　民事訴訟

(1)　立証責任に関する規定・制度・運用

実体法の適用が問題となる場合、立証責任（Beweislast）に関する規律は実体法に従う[123]。具体的には、請求権者は全ての「権利を基礎づける事実（rechtsbegründende Tatsachen）」について立証責任を負い、これに対し相手方は「権利を妨げる事実（rechtshindernde Tatsachen）」「権利を消滅させる事実（rechtsvernichtende Tatsachen）」「権利の行使を阻止する事実（rechtshemmende Tatsachen）」について立証責任を負う[124]。

例えば、営業秘密の保有者が状況に応じて講じるべき合理的な秘密保持措置は、営業秘密の客観的構成要件にあたる（GeschGehG 第 2 条第 1 号）ところ、この点についての証明責任は営業秘密の保有者に帰属する[125]。

(2)　証拠収集に関する規定・制度・運用

ドイツ民事訴訟法は下記の 5 種類の証拠を認めている（ドイツ民事訴訟法第 371 条から第 455 条まで）。

① 現物検証による証拠（ドイツ民事訴訟法第 371 条以下）
② 証人尋問による証拠（ドイツ民事訴訟法第 373 条以下）
③ 鑑定人による証拠（ドイツ民事訴訟法第 402 条以下）
④ 書類・記録による証拠（ドイツ民事訴訟法第 415 条以下）
⑤ 当事者尋問による証拠（ドイツ民事訴訟法第 445 条以下）

ドイツ法には一般にディスクロージャーやディスカバリーの制度が存在しないため、営業秘密侵害の主張を裏付けるために必要な証拠を入手することは、営業秘密の保有者にとって多くの場合、大きな問題となる。これは、特許訴訟とは異なり、GeschGehG に基づく請求においては、単に情報が使用されているという事実だけでは足りず、その情報が違法に取得されたことを営業秘密の保有者が証明しなければならないためである[126]。

---

123 BGH, Urt. V. 3. 4. 2001 - XI ZR 120/00.

124 Vorwerk/Wolf, Bacher, “BeckOK ZPO”, 57. Edition, ZPO § 284 Beweisaufnahme Rn.72.

125 Fuhlrott, Fuhlrott/Hiéramente“BeckOK GeschGehG, 26. Edition, GeschGehG § 2 Begriffsbestimmungen Rn.66.

126 Thomas Nägele, Simon Apel, Jonathan Drescher and Alexander Stolz, “Trade Secrets 2025 - Germany”, Chambers and Partners, 24 April 2025, 5.7, <https://practiceguides.chambers.com/practice-guides/trade-secrets-2025/germany>.

(3) 訴訟の証拠収集等における営業秘密の保護に関する規定・制度・運用

ア GeschGehG 第 16 条から第 20 条まで及びドイツ民事訴訟法第 273a 条

裁判所は、営業秘密侵害事件において、当事者の申立てにより、事件に関連する情報が営業秘密である可能性がある場合、その情報の全部又は一部を秘密情報と指定できる（GeschGehG 第 16 条第 1 項）。その結果、全ての訴訟関係人は、訴訟手続外で把握した情報を除き、秘密情報の訴訟外での使用又は開示を禁止される（GeschGehG 第 16 条第 2 項）。この義務は、営業秘密の存在を否定する確定判決が出された場合や、当該情報を通常取り扱う者の間で一般的に知られ又は容易に利用可能となった場合を除き、訴訟終了後も存続する（GeschGehG 第 18 条）。さらに、裁判所は、当事者の求めに応じ、公判や当事者又は第三者の提出文書などのアクセス制限といった追加の制約を命じることができる（GeschGehG 第 19 条）。秘密保持義務に違反した場合、最高 10 万ユーロの秩序金（Ordnungsgeld）又は最長 6 か月の秩序拘禁（Ordnungshaft）が課される可能性がある（GeschGehG 第 17 条）。こうした命令を裁判所が発する前提として、申立人は当該情報が営業秘密であることを疎明（Glaubhaftmachung）しなければならない（GeschGehG 第 20 条第 3 項）。

しかし、この規定には、法律の明文上、営業秘密そのものが訴訟上の争点である場合にしか適用されないという重大な欠点があった[127]。このような欠点を改善するために、2025 年 4 月 1 日から施行されたドイツ民事訴訟法第 273a 条により、争点となる情報が GeschGehG の意味における営業秘密に該当する可能性がある場合には、原則として全ての民事訴訟に GeschGehG 第 16 条から第 20 条までが適用されることとなった[128]。ドイツ民事訴訟法第 273a 条の手続においては、当事者の申立てが必要であり、その際、申立人は要件事実を全て主張し、かつ疎明しなければならない。裁判所の判断は決定（Beschluss）により、通常は相手方の意見を確認することなく行われる。裁判所が情報を秘密保持すべきものと認定した場合、その後の手続及び法的効果は GeschGehG 第 16 条から第 20 条までに基づき規定される[129]。

イ 公開原則とその例外

公開原則に関する規定は、ドイツ法上、裁判所構成法

127 Prütting, “Münchener Kommentar zur ZPO”, 7. Aufl., 2025,ZPO § 273a Geheimhaltung Rn. 7.

128 Thomas Nägele, Simon Apel, Jonathan Drescher and Alexander Stolz, “Trade Secrets 2025 - Germany”, Chambers and Partners, 24 April 2025, 5.8.

129 Prütting, “Münchener Kommentar zur ZPO”, 7. Aufl., 2025,ZPO § 273a Geheimhaltung Rn. 8.

（Gerichtsverfassungsgesetz）[130]第169条に置かれている。裁判所構成法第169条第1項第1文によれば、判決裁判所における審理及び判決の言渡しは公開でなされる。また、欧州人権条約（European Convention on Human Rights）[131]第6条第1項により、ドイツを含む締約国は公開原則の保障が要請されている[132]。

他方、ドイツ法上、公開原則の例外も認められている。重要な営業秘密が取り上げられ、その公開の議論により、優越する正当に保護された利益が侵害されるおそれがある場合には、裁判所は審理を非公開とすることができる（裁判所構成法第172条第2号）。また、民事訴訟については、ドイツ民事訴訟法第128条第2項が、当事者双方が同意をした場合に、裁判所が書面による審理を行うことを認めているところ、ドイツ法上、第三者の訴訟記録の閲覧は、閲覧に法律上の利益がある場合に限定されている（ドイツ民事訴訟法第299条第2項）ことを勘案すると、書面審理によることとなると、事実上の完全非公開審理となる[133]。なお、欧州人権条約において、ドイツを含む締約国は、①民主的社会における道徳、公の秩序、若しくは国家安全保障の利益のため、②未成年者の利益や当事者の私生活の保護が必要な場合、又は、③公開が司法の利益を害する特別な事情において裁判所が厳格に必要と認める場合、公開原則を制限しうるとされる（欧州人権条約第6条第1項）。

2　刑事訴訟

(1)　立証責任に関する規定・制度・運用

検察当局が全ての構成要件を立証しなければならない。ただし、検察は被疑者の施設を捜索し、差押えを命じることができる。このような手段によって、被疑者が第三者の営業秘密を保有していることを立証できる場合も多い。しかし、被疑者が「不正な手段で秘密を入手したわけではない」又は「少なくとも不正な取得であることを認識していなかった」と主張する場合、反駁が困難となる場合が多い[134]。

130　Gerichtsverfassungsgesetz, <https://www.gesetze-im-internet.de/gvg/index.html#BJNR005130950BJNE019404125>.

131　European Convention on Human Rights, <https://www.echr.coe.int/documents/d/echr/Convention_ENG>.

132　本間学「当事者の合意に基づく民事訴訟の公開の排除？―ドイツにおける議論からの示唆」（2025年）238頁＜https://www.ritsumei.ac.jp/acd/cg/law/lex/24-56/011honma.pdf＞。

133　同上238頁～239頁。

134　Thomas Nägele, Simon Apel, Jonathan Drescher and Alexander Stolz, “Trade Secrets 2025 - Germany”, Chambers and Partners, 24 April 2025, 9.1.

(2) 証拠収集に関する規定・制度・運用

ドイツ刑事訴訟法は、下記の 4 種類の証拠を認めている。

① 証人（ドイツ刑事訴訟法第 48 条以下）

② 鑑定人（ドイツ刑事訴訟法第 72 条以下）

③ 書面（ドイツ刑事訴訟法第 249 条以下）

④ 検証（ドイツ刑事訴訟法第 86 条以下）

ドイツの刑事手続において、被害者の立場は比較的弱いとされる。捜査段階では、事件の調査は専ら所轄の法執行当局の責務であり、被害者にできる協力は証言の提供にほぼ限られる。また、被害者は（少なくとも原則として）捜査記録の閲覧を求める権利を有している（ドイツ刑事訴訟法第 406e 条）が、秘密保持違反の疑いがあり、記録に被疑者側の営業秘密が含まれる場合には、被疑者の秘密保持利益を理由に閲覧が認められないことが多い[135]。

(3) 訴訟の証拠収集等における営業秘密の保護に関する規定・制度・運用

刑事訴訟においても公開原則が適用される（裁判所構成法第 169 条第 1 項第 1 文）。もっとも、重要な営業秘密が取り上げられ、その公開の議論により、優越する正当に保護された利益が侵害されるおそれがある場合には、裁判所は審理を非公開とすることができる（裁判所構成法第 172 条第 2 号）。

3 まとめ

ドイツでは、民事訴訟における立証責任は一般原則のとおり、営業秘密の客観的要件（合理的秘密保持措置など）については営業秘密の保有者が証明責任を負う。また、GeschGehG 第 16 条から第 20 条まで及び改正民事訴訟法第 273a 条により、訴訟上の営業秘密保護（秘密情報の指定、アクセス制限、違反に対する秩序罰金など）が制度化されている。刑事手続では、検察が全ての事実を立証しなければならず、被害者の関与は限定的で、被害者の記録閲覧も被疑者側の営業秘密との関係で制限されうる。民事・刑事いずれも重要な営業秘密が争点となる場合には公開原則の例外として非公開審理が認められる。

第 9 章 営業秘密侵害事件の動向

1 ドイツの営業秘密侵害事件の統計情報

2023 年 EU 報告書によると、2017 年 1 月 1 日から 2022 年 10 月 31 日までに公表されたドイツの営業秘密侵害事件の判決の動向について、以下のように報告されている

135 Thomas Nägele, Simon Apel, Jonathan Drescher and Alexander Stolz,“Trade Secrets 2025 - Germany”, Chambers and Partners, 24 April 2025, 9.1.

[136]。

報告された訴訟件数	39 件
上訴率	53%
侵害請求の勝訴率	19%

(1) 訴訟の分類

ほとんどの事件は民事事件と分類され、行政事件はなく、刑事事件は 1 件のみであった。

(2) 技術情報・商業情報の動向

営業秘密のうち、37%は技術情報、60%は商業情報として分類された。最も取り上げられた情報の種類は、製造プロセス（22%）と商業上の下流情報（25%）であった。訴訟に関与した商業分野では製造業が圧倒的多数（53%）を占め、次いで専門的・科学的サービス（17%）であった。

(3) 訴訟手続

侵害請求の大半は、非公開情報の使用に関する契約上の制約違反（51%）に関するものであり、次いで無権限の取得に基づく使用（23%）であった。

被告側が主張した抗弁は多様であり、最も一般的なものは「合理的な措置が取られていないため営業秘密が存在しない」とするものや「労働者の権利行使」であった。注目すべき点として、リバースエンジニアリングや独自の発見を抗弁として持ち出した事例も少数ながら存在した。

(4) 訴訟結果に関する動向

本案において最も一般的に認められた処分は、情報の使用停止命令であった。注目すべき点として、文書の破棄命令が 2 件認められている。損害賠償は 5 件で認められ、そのうち金額が明示的に報告されたのは 1 件（166,677.36 ユーロ）のみであった。

2 参考になる裁判例

2023 年 EU 報告書において、重要なドイツの裁判例として以下の 2 つの判決が取り上げられている。

(1) デュッセルドルフ高等地方裁判所　事件番号 15 U 6/20（2021 年 3 月 11 日）[137]

ア　事案

原告企業と被告企業は機械・装置の製造・保守を行う競合企業であった。被告企業の取締役は原告企業の元従業員であったところ、被告企業は入札の

136 2023 年 EU 報告書 45 頁～47 頁。

137 OLG Düsseldorf, Urt. V. 11.3.2021 – 15 U 6/20.

際に遠心分離機ドラムの CAD 図面を提出した。原告企業は、これらの図面は被告企業の取締役が在職中に不正に入手して持ち出した営業秘密であり、それによって被告企業が低価格かつ迅速な提案を可能にし、落札につながったと主張した。他方、被告企業は、リバースエンジニアリングによる適法な取得や情報の公知性、原告企業の秘密保持措置の不備、情報の不使用、さらには原告適格の欠如を主張して争った。

イ　判断

デュッセルドルフ高等地方裁判所は、CAD 図面を営業秘密と認定し、被告企業の抗弁を退けた。裁判所は、図面自体に商業的価値があり、既存のドラムの測定では寸法程度の情報しか得られず、図面に含まれるその他の技術情報を再現できないため、リバースエンジニアリングの抗弁は成立しないと判断した。また、原告企業の技術的・組織的・契約的な措置は「合理的な秘密保持措置」にあたり、理想的な保護又は極端な安全性までは不要とした。さらに、被告企業の取締役は原告企業に在職中に秘密を取得したものであり、その取得には法的根拠がないと認定された。侵害行為は GeschGehG 施行前に発生していたが、旧法に基づく差止請求は認められるとした。結果として、同裁判所は営業秘密侵害を認定し、差止命令、情報提供命令、損害賠償請求を認めた。

(2) デュッセルドルフ地方労働裁判所　事件番号 12 SaGa 4/20（2020 年 6 月 3 日）[138]

ア　事案

被告は原告の元従業員であり、その後、原告の競合企業に雇用された。原告は、被告が雇用関係終了後も、顧客、販売額、収益及び製品種類に関する 3 種類の文書、並びに顧客関係に関する個人的なメモ（会議録を含む）を受領・使用していたと主張した。これに対し被告は、記憶していた情報を合法的に使用したにすぎず、原告が主張するようなファイルを新しい雇用主の業務で使用してはいないと反論した。

イ　判断

第一審は仮処分の申立てを却下したが、控訴審は一部認容し、被告に対し、個人的メモの使用の差止を命じた。他方で、3 種類の文書に関しては第一審の却下を維持した。裁判所は、個人的メモの内容は営業秘密に該当しうるとし、返還義務を定めた契約条項が秘密保持の「合理的措置」として十分であると認定した。他方、1 種類の文書については一般的な秘密保持条項し

138　LAG Düsseldorf, Urt. v. 3.6.2020 – 12 SaGa 4/20.

かなく具体性を欠くため「合理的措置」の要件を満たさないと判断され、営業秘密性が否定された。また、残る 2 種類の文書については被告が所持していたとの立証が不十分であると判断された。

3　まとめ

2023 年 EU 報告書によれば、2017 年 1 月 1 日から 2022 年 10 月 31 日までに公表されたドイツにおける営業秘密侵害事件の判決は 39 件であり、勝訴率は 19%にとどまっている。対象となる情報は、技術情報・商業情報の双方に及ぶが、侵害請求の多くは、秘密保持契約の違反や無権限取得に基づく使用に関するものである。これに対し、被告側は抗弁として、秘密保持措置の不備や労働者の権利行使を主張するほか、リバースエンジニアリングなどを抗弁として主張する事例もみられる。救済措置としては、使用停止命令が最も一般的である一方、損害賠償が認められた事例は限られている。したがって、最新の動向にも留意しつつ、訴訟での立証に耐えうるような営業秘密の管理体制を構築することが重要である。

第 10 章　ドイツの法律・制度・運用を踏まえた、営業秘密漏えい対策を実施するにあたってのポイント

1　ドイツにおいて営業秘密漏えい対策を実施するにあたってのポイント・留意点

ドイツにおける営業秘密漏えい対策としては、ドイツの各地域の商工会議所（IHK）が公開するガイダンス[139]が参考になる。かかるガイダンスにおいて示される営業秘密漏えい対策の実施上のポイント・留意点は以下のとおりである。

(1)　一般論

企業にとって、営業秘密が重要であればあるほど、より厳格な保護措置を講じる必要がある。

(2)　実務上の重要な対応策の例

①　IT セキュリティ対策
②　秘密情報の取扱いに関する従業員のトレーニング
③　定期的な監査・チェック
④　契約上の規定（秘密保持契約など）

139　ドイツの各地域の商工会議所がガイダンスを公表しているところ、本報告書においては、具体的なポイントが豊富に示されているカッセル・マールブルク商工会議所のガイダンスを参照している。Industrie- und Handelskammer Kassel-Marburg, “Geschäftsgeheimnisse richtig schützen”, December 2023, <https://www.ihk.de/kassel-marburg/beratung-service/recht/wirtschaftsrecht/gesellschaftsrecht/geschaeftsgeheimnisse-richtig-schuetzen-442413>.

⑤　文書化・記録化
⑥　緊急時対応システム（秘密漏えい時の対応マニュアル）

(3)　企業が取るべきステップ
①　保護すべき情報の棚卸し・把握
②　秘密保護計画における重要度に応じた分類
③　適切な保護措置の決定と文書化

(4)　契約上の課題
①　秘密保持条項や利用制限条項のみでは不十分とされる可能性
②　契約上、違反時の違約金（Vertragsstrafe）の有無が重要視される傾向
③　新規採用時には「前職の秘密情報は持ち込まない」旨を説明し、契約書や記録に残すことが望ましい

(5)　秘密保持契約

秘密保持契約（non-disclosure agreement、いわゆる「NDA」）は、秘密保護のための重要な手段である。一般的に通用する定型的な条項は存在せず、個別事案に応じて調整すべきである。契約内容には、秘密の特定、契約目的、禁止行為、保護期間、サービスプロバイダーへの情報提供に関する規定、違反時の違約金を盛り込むべきである。これらの条項は通常、普通取引約款規制（Recht über Allgemeinen Geschäftsbedingungen）の適用対象となるため、専門家による法的助言が推奨される。

(6)　リバースエンジニアリングに対する対応

市場に流通した製品から営業秘密を導き出す「リバースエンジニアリング」は、GeschGehG により原則として許容される。リバースエンジニアリングにより営業秘密が導き出されるのを防止するために、製品に技術的保護措置を組み込む、又は契約上の「禁止条項」を設ける必要が生じうる。

2　ライセンス、生産委託、合弁会社設立で気をつけるべきポイント

(1)　前提

GeschGehG 第 2 条に規定されるとおり、情報を適法に管理する者によって、当該状況下で秘密性を保持するための合理的な措置がとられていることが営業秘密の要件となるため、営業秘密を秘密保持の合意のないまま第三者に提供することは、それらの秘密性を失わせる結果となりかねない。そのため、ライセンス、生産委託、合弁会社設立の際に、法律関係を明確化し、将来の紛争を防ぐためにも、以下の点に留意しつつ、秘密保持契約を締結し、又はこれらの契約において

秘密保持義務を明文で盛り込む必要がある。これらの契約は営業秘密その他の知的財産権や有形資産といった自社の競争力の源泉となるアセットを利用させる重要な契約となることが多いため、社内でノウハウが蓄積していない場合にはドイツ法弁護士に相談すべき性質の契約ではあるが、営業秘密の保護という観点でも慎重な検討を要する。

(2) ライセンス契約

ノウハウのライセンス契約を締結する場合には、営業秘密が開示されることになる。そのため、営業秘密としての保護を確保するために、前記 1 において秘密保持契約の要素として述べた内容やホワイトペーパーで示された要素に従って営業秘密の該当性を判断した裁判例[140]の判示も考慮すると、開示される秘密の特定、契約の目的、ライセンシーの禁止行為、ライセンシーにおいて営業秘密を機密性に関する程度でラベルすること、ライセンシーの従業員の機密性保持の誓約、業務を実行するために少なくとも潜在的に情報にアクセスすることを必要とする者のみがアクセスできること[141]、情報の開示を受ける者は秘密保持義務に拘束され、当該情報に関して秘密保持義務を負っていることを認識していること、秘密保持義務に違反した場合の違約金などをライセンシーとの契約に含めることが考えられる。

(3) 生産委託契約

(2)にライセンス契約で列挙した注意点は、生産委託契約にもあてはまる。また、委託者としては、受託者の生産ラインの運営状況、生産品の数量などの確認体制、保存・管理状況を十分確認することが特に重要である。そこで、契約書にもこれらの事項について、受託者に報告、保証、あるいは誓約をするよう義務づけることを検討すべきである。

また、生産委託契約では、受託者が、第三者の機密情報、営業秘密情報を保有していて、委託者の製品の製造に使用してしまった場合、第三者から、機密情報・営業秘密の不正使用、開示にあたるとして、法的請求を受ける可能性がある。委託者自身が当該事実を認識していない場合であっても、受託者に対する差止命令その他の法的措置により、結果として製品の製造や供給に重大な支障をきたす可能性がある。そこで、生産された製品が、受託者と取引関係のある他社の機密情報・営業秘密の侵害をしないことを誓約する、非侵害保証を要求することを検討すべきである。

---

140 OLG Stuttgart , Urt. v. 19.11.2020 – 2 U 575/19, 1(169).

141 Harte-Bavendamm/Ohly/Kalbfus, Harte-Bavendamm, “GeschGehG”, 2. Aufl., 2024, GeschGehG § 2 Begriffsbestimmungen Rn. 64.

さらに、機密情報、営業秘密へのアクセス、使用目的、使用方法の限定に関して、受託者から第三者への再委託を禁止することも考慮すべきである。

(4) 合弁契約

合弁会社は、参加当事者が提供した、あるいは、合弁会社自身が調達した人材、技術、データ、施設、及び、資材を使用して、事業を行うことが多い。参加者の様々な機密情報、営業秘密が提供されることもある。したがって、合弁会社が研究や開発をして得られる成果物に対して、どの者に所有権あるいは管理権が帰属するのかを契約で明確化しておくことが、特に重要となる。

3 まとめ

営業秘密としての保護には合理的な措置の実施が求められるため、1 に挙げた要素を参考に技術的及び組織的な体制の整備を進めるべきである。また、ライセンスや生産委託など、外部の事業者に営業秘密を提供する局面においては、提供される秘密の内容を特定しつつ、提供先の利用方法、アクセス範囲、秘密保持義務に違反した場合の違約金の設定といった内容を規定することで契約上の防御を図るべきである。

英国

第 1 章　営業秘密の保護体系

1　営業秘密に関する制度の概要

英国において、営業秘密は、民事上、①「秘密情報（confidential information[142]）」を保護する判例法（コモンロー及び衡平法）並びに②EU 営業秘密指令を国内法化した The Trade Secrets (Enforcement, etc.) Regulation 2018 (SI 2018/597)（以下「UK TS 規則」という）により保護されている。③雇用契約や秘密保持契約等の契約により保護されることもある。

刑事上の保護としては、④National Security Act 2023（以下「NSA 2023」という）が国家安全保障上脅威を伴う事案に対する刑事責任を定めている。また、営業秘密について定める法令ではないが、個別の事案によっては、⑤Computer Misuse Act 1990（以下「コンピュータ不正使用法」という）や⑥Theft Act 1968（以下「窃盗法」という）が適用される場合もある。

英国における営業秘密の保護は、秘密情報の保護に関する判例法に端を発している。英国における秘密情報の保護は、17 世紀の裁判例にまで遡ることができ、雇用法（employment law）・特許法（patents）・契約法（contract）・著作権法（copyright）・刑法（criminal law）・衡平法（equity）等、多様な法理が用いられてきたという[143]。現在、判例法による秘密情報の保護は、秘密保持義務が生じる状況のもとで伝達された秘密性を有する情報を、情報提供者に不利益を与える形で無断使用することを禁じる衡平法上の法理に基づく秘密保持義務違反による保護が中心となっている。

その後、2018 年に UK TS 規則が制定された。当時 EU の加盟国であった英国は、2017 年 3 月に EU 脱退の正式通知を行い、2019 年 3 月にその脱退（いわゆる Brexit）が予定されていたが、2016 年に制定された EU 営業秘密指令に基づき、2018 年 6 月 9 日、UK TS 規則を制定した。現在は EU を脱退しているため、EU 営業秘密指令が英国裁判所を直接に拘束する効力は持たないが、UK TS 規則は、英国の国内法であるため、その適用は、英国の EU 脱退の影響を受けない[144]。

このように、営業秘密の不正使用等については、従前民事救済により対処されてき

142　裁判例において、営業秘密は、保護される秘密情報のうち特に秘密性の高い情報を指すと考えられてきた。Faccenda Chicken Ltd v. Fowler, Fowler v. Faccenda Chicken Ltd. [1986] 1 All ER 617.

143　Tanya Aplin and Richard Arnold, “UK implementation of the Trade Secrets Directive”,The Harmonization and Protection of Trade Secrets in the EU, 2020, p.65-p.70.

144　なお、英国の EU 脱退後も、European Union (Withdrawal) Act 2018 により、英国下級裁判所には EU 脱退前の欧州司法裁判所の判例法が引き続き適用される（同法 6(1)・(4)）。EU 脱退後の欧州司法裁判所の決定は英国裁判所を拘束しないが、英国裁判所は、説得力のある裁判例として、EU 脱退後の欧州司法裁判所の決定を参照できる（同法 6(2)）。

たところ、英国では、2023 年に、国家安全保障の強化を目的とし、外国勢力によるスパイ行為、妨害工作、選挙干渉等に対する刑事罰を新設したNSA 2023 が制定された。NSA 2023 は、第 2 条において、外国勢力のために営業秘密を不正に取得・複製・記録・保持・開示する行為を犯罪と定め、当該行為を外国勢力のため、又はその指示・利益のために行った場合、最大 14 年の拘禁刑を科すと定めている。

2　秘密情報・営業秘密保護の並存

UK TS 規則第 3 条は、「営業秘密の不正取得、使用又は開示に関して、本規則よりも広範な保護を営業秘密の保有者に提供する」等の要件を満たす場合、営業秘密の保有者は、UK TS 規則に基づく措置、手続及び救済に代えて、又は加えて、秘密保持義務違反に関する訴訟において救済を求めることができると定めており、UK TS 規則は判例法を排除するものではない。

また、Trailfinders Ltd. v. Travel Counsellors Ltd.[145]において、EU 営業秘密指令（及び同指令と共通の営業秘密の定義を持つ UK TS 規則）は従前の契約解釈や判例法を排除しないと示された。当該裁判例は、被告が持ち出した顧客情報を、無断に取得し、転職先で利用したという事実について、①当該情報は、EU 営業秘密指令（及び UK TS 規則）にいう営業秘密に該当し、被告の行為はその不正取得、使用と認められると判じた。また、②当該情報は、判例法上の秘密情報にも該当し、その利用は秘密保持義務違反にも該当すると述べた。さらに、③元従業員である被告は、雇用契約や秘密保持契約に基づく義務にも違反したと認定している。裁判所は、これらの重畳適用を認めている。

3　まとめ

英国における営業秘密の保護制度は、17 世紀以降判例の積み重ねにより、衡平法上の法理に基づくものとして形成されてきた。2016 年、当該判例法に加え、UK TS 規則が制定され、明文で営業秘密が保護されるようになった。もっとも、UK TS 規則は判例法を排除するものではない。加えて、2023 年には国家安全保障の強化を目的とし、外国勢力によるスパイ行為、妨害工作、選挙干渉等に対する刑事罰を新設したNSA2023 も制定された。

第 2 章　営業秘密の定義

本章では、現行の営業秘密関連法における営業秘密の定義を説明する。

145　Trailfinders Ltd. v. Travel Counsellors Ltd. [2020] EWHC 591.

1　UK TS 規則による定義

UK TS 規則第 2 条では、「営業秘密」を以下の要件を満たす情報と定義している。

A-1　当該情報全体として、又はその構成要素の正確な組合せ及び集積として、当該種別の情報を通常取り扱う者の間において一般に知られておらず、又は容易に入手可能でもないこと。

A-2　当該情報が秘密であることにより商業的価値を有すること。

A-3　当該情報を適法に管理する者によって、状況に応じて合理的と考えられる、情報を秘密に保つための措置が講じられていること。

2　判例法による定義

英国判例法の衡平法に基づく秘密保持義務違反の法理では、関係者間の信頼関係の性状や内容に着目して、秘密情報（営業秘密を含む）が保護されてきた[146]。裁判例は、秘密とする義務を生じさせる状況で情報が伝えられ、信用関係に由来する情報が、秘密情報の保有者にとって不利益に使用され、又は使用されるおそれがある場合に、そのような行為を信用に違背する不法な行為としてきた。

Coco v AN Clark (Engineering) Ltd.判決では、秘密保持義務違反の法理により保護されるためには、以下の 3 つの要件が必要とされている[147]。

B-1　情報自体が「必要な秘密性」を有していること。

B-2　当該情報が、秘密保持義務が生じる状況のもとで伝達されていること。

B-3　当該情報が無断で使用され、情報提供者に不利益が生じていること。

B-1 の秘密性は、情報が公知でないことを意味する。公知とは、専門家ではなく、一般大衆に知られていることを指すとされる。Thomas Marshall (Exports) Ltd v. Guinle 事件では、どのような情報が秘密情報にあたるかの判断要素として以下が挙げられた。秘密性の要件として、厳密な秘密管理性は要求されていない[148]。

①　当該情報の開示が、情報の保有者を害するか又は競合者等にとって有利になると保有者が確信していること。

②　当該情報が依然として秘密である（公知になっていない）と保有者が確信していること。

③　上記 2 点に関する保有者の確信が合理的であること。

④　関連する特定の産業又は取引の慣行に照らして、当該情報が秘密情報として保護されるべきものであると判断されること。

B-2 の秘密保持義務の存否につき、Coco v AN Clark (Engineers) Ltd 判決は、情報の受領者が合理的な根拠に基づき、情報が秘密として提供されていると認識するかどうか

146　Trailfinders Ltd. v. Travel Counsellors Ltd. [2020] EWHC 591.

147　Coco v A.H. Clark (Engineering) Ltd. [1969] RPC 41, Judge Megarry, J. para11-14.

148　Thomas Marshall (Exports) Ltd v. Guinle[1979] Ch 227, [1978] IRLR 174, [1978] ICR 905.

という客観的基準で判断されるとした。

B-3 の無断使用につき、Coco v AN Clark (Engineers) Ltd 判決は、上記のように「無断使用」とそれによる「不利益」の発生を要件としているが、「不利益」を要件とすることに反対する見解もある[149]。

3　NSA 2023 による定義

NSA 2023 第 2 条第 2 項は、「営業秘密」とは、以下の要件を全て満たす情報、文書その他の物をいうと定義している。

C-1　当該情報等が、関連分野の知識若しくは専門性を有する者に一般に知られていない、又は利用不可能であること。

C-2　当該情報等が、実際又は潜在的な産業的、経済的又は商業的価値を有し、関連分野の知識若しくは専門性を有する者に一般に知られ又は利用可能となった場合、その価値が損なわれるおそれが実際に又は合理的に予想されること。

C-3　当該情報等が、関連分野の知識若しくは専門性を有する者に一般に知られ、又は利用可能となることを防止するための措置が取られることが合理的に想定されること（実際にそのような措置が取られているか否かを問わない）。

4　日本法との比較

日本の不正競争防止法において、「営業秘密」は以下の 3 要件を満たすものと定義される（不正競争防止法第 2 条第 6 項）。

①　秘密として管理されていること（秘密管理性）。

②　事業活動に有用な技術上又は営業上の情報であること（有用性）。

③　公然と知られていないこと（非公知性）。

不正競争防止法の①秘密管理性については、UK TS 規則の A-3「秘密保持措置」や NSA 2023 の C-3「秘密保持措置」に対応しうる。不正競争防止法及び UK TS 規則においては、営業秘密に該当するためには、当該情報について秘密保持措置が実際に講じられていることが必要であるが、NSA 2023 では合理的に秘密保持措置が講じられると期待されることで足りる。一方で、英国の判例法においては、秘密情報（営業秘密）について、秘密保持措置を要件としていない。ただし、UK TS 規則の「秘密保持措置」が講じられたことの証明は、英国判例法の B-2「秘密保持義務」の立証に資する可能性が高いとの指摘がある[150]。

不正競争防止法の②有用性については、UK TS 規則の A-2「価値」や NSA 2023 の C-2「価値」に対応しうる。UK TS 規則は情報が商業的価値を持つことを、営業秘密

149　Coco v A.H. Clark (Engineering) Ltd. [1969] R.P.C. 41, Judge Megarry, J. para 14.

150　Kirkland & Ellis International LLP, “Trade Secrets 2025”, 24 April 2025, <https://practiceguides.chambers.com/practice-guides/trade-secrets-2025/uk>.

に該当するための要件としている一方で、NSA 2023 では潜在的価値も含むとされている。不正競争防止法における有用性については、直接事業活動に活用されている情報に限らず、潜在的な価値がある場合も含まれるため[151]、この点においては、NSA 2023 に近しいと思われる。英国判例法においては、「不利益」を要件と捉える場合においては、「価値」要件はその判断の前提として考慮されうるものと考えられる。

不正競争防止法の③非公知性については、UK TS 規則の A-1「秘密性」、英国判例法の B-1「秘密性」、NSA 2023 の C-1「秘密性」に対応する。UK TS 規則では「当該情報と同種の情報を通常扱う業界内の人々の間で一般に知られておらず、又は、そのような人々が容易にアクセスすることができない」ことが基準とされ、NSA2023 では「関連分野の知識若しくは専門性を有する者に一般に知られていない、又は利用不可能であること」が基準とされている。これらはいずれも当業者基準であるのに対し、不正競争防止法上や判例法においては、文言上、一般に知られていないことが基準とされている点で差異がある。

英国判例法における、B-2「秘密保持義務」や B-3「無断使用（・不利益）」の要件については、英国判例法が、秘密保持義務違反の法理の要件として挙げている要件である。そのため、不正競争防止法の要件とは位置づけが異なる。　上記について表にまとめると以下のとおりである。なお、英国の表内の各要件の末尾に、日本法の要件との対応関係を、①から③の番号にて記載している。

	日本	英国		
根拠法	不正競争防止法	UK TS 規則	判例法	NSA 2023
定義	①　秘密管理性 ②　有用性 ③　非公知性	A-1　秘密性（③） A-2　価値（②） A-3　秘密保持措置（①）	B-1　秘密性（③） B-2　秘密保持義務 B-3　無断使用（・不利益）	C-1　秘密性（③） C-2　価値（②） C-3　秘密保持措置（①）
要件①：秘密管理性	✓実際の管理措置が必要	✓実際の管理措置が必要	-（不要） ただし、B-2 と立証は共通しうる	✓管理措置が期待されることが必要
要件②：価値性、有用性	✓事業上有用	✓商業的価値	-（不要）	✓潜在的価値でも可
要件③：秘密性	✓一般基準	✓当業者基準	✓一般基準	✓当業者基準
日本法にない要件	-	-	✓秘密保持義務 無断使用（不利益）	-

5　まとめ

英国では、営業秘密について、判例法、UK TS 規則、及び NSA 2023 それぞれで異なる定義が用いられている。もっとも、判例法は秘密保持義務違反の法理に基づき①秘密性、②秘密保持義務、③無断使用（・不利益）を営業秘密に該当するための要件とする一方で、UK TS 規則及び NSA 2023 は各要件の詳細は異なるものの、どちらも

151　経済産業省「営業秘密管理指針」（2025 年 3 月 31 日改訂）20 頁。

①秘密性、②価値、③秘密保持措置を要件とするという大枠では共通しており、これらは日本の不正競争防止法における「営業秘密」の 3 要件（秘密管理性・有用性・非公知性）とも概ね対応関係が見られる。

第 3 章　営業秘密の侵害行為

UK TS 規則における営業秘密の「侵害」、判例法における秘密保持義務違反、日本の不正競争防止法における不正競争行為は、定義や建付けに差異はあるが、行為類型としては共通する部分が多い。以下では当該行為類型について概説する。

1　UK TS 規則による営業秘密侵害行為の定義：営業秘密不正取得・開示・使用

UK TS 規則の第 2 条は、以下の用語について、定義している。

- 「侵害者」とは、営業秘密を不正取得、使用又は開示した者をいう。
- 「侵害品」とは、営業秘密の不正取得、使用又は開示によって、その設計、機能、製造工程、販売促進、又は特性が、大きな利益を得ている物品をいう。

UK TS 規則第 3 条第 1 項は、営業秘密の取得、開示、使用は、秘密情報に対する守秘義務の違反となる場合に、違法とされる旨定めている。UK TS 規則の Explanatory Note（注釈）は、その解釈は、判例法で確立された理論（the law of confidence）に依拠して決定される旨を示しており、判例法を参照することが重要である[152]。

2　契約で定めた秘密保持義務の不履行：秘密情報の不正開示・使用

(1)　明示的に規定された秘密保持義務違反

当事者間に、明示に秘密保持契約（あるいは守秘義務条項を含む契約）が締結されていれば、それを根拠として、損害賠償等の請求が可能である。Marathon Asset Management LLP v. Seddon では、従業員の雇用契約に明示的な秘密保持義務が含まれていたことを認定し、当該義務違反があったと判示している[153]。

(2)　黙示的な忠実義務違反

また、雇用契約には、従業員が忠実かつ誠実に職務を遂行する義務が黙示的に含まれており、この忠実義務には、従業員が雇用主の秘密情報を雇用関係の目的のみに使用し、それ以外の目的で使用しない義務が含まれる。前掲 Marathon Asset Management LLP v. Seddon では、雇用契約における明示的な秘密保持義務の違反に加え、黙示の忠実義務違反も認定された[154]。

152　UK TS 規則 Explanatory Note。

153　Marathon Asset Management LLP v. Seddon [2017] EWHC 300 (Comm) para 111,142.

154　Marathon Asset Management LLP v. Seddon [2017] EWHC 300 (Comm) para 111,142.

Faccenda Chicken Ltd v. Fowler 事件は、明示の秘密保持契約がない事案であり、その第一審判決は、雇用契約上黙示的に認められる忠実義務に基づいて、雇用主の利益以外の使用が禁じられるべき雇用主の情報を分類して検討している。すなわち、従業員が退職後も忠実義務に従い秘密保持義務を負うべき情報は営業秘密や秘密性の高い情報に限られ、業務上知り得たが従業員のスキル・知識となった情報は、雇用期間中は秘密保持義務の対象となるが、退職後は元従業員が自由に利用できる場合が多いとした[155]。同事件控訴審は、第一審判決の情報の分類を踏まえた上で、退職後も秘密保持義務の対象となるべき営業秘密や秘密性の高い情報に該当するかの判断に際しては、以下の要素を考慮すべきであるとした。

① 雇用の性質。秘密情報を日常的に扱う職種であれば、従業員はその情報の機微をより強く認識できるため、守秘義務の範囲は広くなる。一方、秘密情報にたまにしか触れない職種の場合は、義務の範囲は限定される。

② 情報自体の性質。当該情報が、営業秘密又は営業秘密と同等の重要性や要保護性を有するか。

③ 雇用主がどれだけ秘密性を強調したか。雇用主が単に当該情報が「秘密だ」と伝えるだけでは十分ではなく、雇用主がどのように情報を管理し、秘密性を強調していたか。

④ 秘密情報の分離可能性。秘密情報が、秘密でない情報と容易に分離できるか[156]。

3 判例法による秘密保持義務違反：秘密情報の不正開示・使用

前述のとおり、英国判例法上、一定の場合において秘密情報を取得した者は秘密情報を漏えいしてはならないという秘密保持義務違反（breach of confidence）の法理により、秘密情報（営業秘密）の保護が図られてきた。

Saltman Engineering Co Ltd v. Campbell Engineering Co Ltd では、契約がなくても秘密保持義務が認められ[157]、Seager v. Copydex Ltd では、秘密情報の保護が衡平法に基づくと示された[158]。

Ocular Sciences Ltd v Aspect Vision Care Ltd では、衡平法上の救済を与えるか否かについて、秘密情報の性質・重要性、被告の事業や第三者への影響、原告・被告双方の訴訟態度や誠実性、救済の実効性・相当性等が考慮されている[159]。

155 Faccenda Chicken Ltd v. Fowler [1985] FSR 105.

156 Faccenda Chicken Ltd v. Fowler [1987] Ch 117.

157 Saltman Engineering Co Ltd v Campbell Engineering Co Ltd [1849] 1 Mac & G 25, 41 ER 1171.

158 Seager v Copydex Ltd [1967] RPC 349, 368 (Lord Denning MR).

159 Ocular Sciences Ltd v Aspect Vision Care Ltd (No.2) [1997] RPC 289.

4　NSA 2023 による営業秘密侵害行為の定義：営業秘密不正取得、複製、記録、保持、開示、アクセス提供

NSA 2023 第 2 条第 1 項では、以下の全ての要件を満たす、当該行為者の行為は犯罪を構成するものとされている。

① 次に掲げる行為のいずれかを行ったこと。
   a. 営業秘密を取得し、複製し、記録し、又は保持する行為。
   b. 営業秘密を開示し、又は第三者に対し、これに対する利用を許す行為。
② 当該行為が無権限であること。
③ 当該行為者が、当該行為が無権限であることを知っているか、又は知っている他の事情を踏まえれば合理的に知っているべきであること。
④ 当該行為に関して外国勢力要件（NSA 2023 第 31 条参照）が満たされていること。

5　日本法との比較

日本の不正競争防止法第 2 条第 1 項に規定されている、営業秘密に関する不正競争行為は、前記ドイツ第 3 章 4 のとおり、①営業秘密不正取得類型（第 4 号）、②信義則違反類型（第 7 号）、③転得類型（取得時悪意転得類型：第 5 号、第 8 号、取得時善意転得類型：第 6 号、第 9 号）、④営業秘密侵害品譲渡等類型（第 10 号）に分類できる。

前述のとおり、UK TS 規則は、不正取得、使用又は開示行為を「侵害」としているが、その解釈については、判例法の法的枠組みに依拠している。

契約に基づく黙示的義務や衡平法による救済について、英国の裁判例では、保有者が当該情報を秘密性のある情報として保持し、信用を寄せていた者に当該情報にアクセスさせていたことが明らかな場合に、秘密保持義務が認められているが、秘密保持義務の対象となるべき営業秘密や秘密性の高い情報に該当するかの判断に際しては、上記のとおり雇用や情報の性質、情報の管理方法等の個別的事情が総合的に考慮されている。日本の不正競争防止法と英国の契約又は判例法に基づく秘密情報の保護は、想定する営業秘密侵害行為において重複するところもあるが、後者については、営業秘密侵害行為類型が条文で明確化されておらず、個別判断がなされている点に違いがある。

刑事罰について、日本の不正競争防止法第 21 条は、営業秘密の各種の不正競争行為に関する罰則を規定しているところ、同条第 1 項第 1 号から第 5 号まで、同条第 2 項第 1 号から第 5 号まではいずれも主観的要件として図利加害目的が規定されている。その一方で、NSA 2023 は、詳細な行為類型を設けず包括的な「unauthorised conduct」を要件としている。また、NSA 2023 は、主観的要件としては図利加害目的まで求めず、無権限の認識で足りるとしているが、「foreign power condition」という国家安全保障上の要件を明示的に含んでいる点で、不正競争防止法と NSA 2023 の立法目的の

違いがあらわれている。

	日本	英国		
根拠法	不正競争防止法	UK TS 規則	判例法	NSA2023
侵害行為類型（民事）	✓条文で明記 ① 不正取得類型 ② 信義則違反類型 ③ 転得類型 ④ 営業秘密侵害品譲渡等類型	・判例法の判断枠組みに従う	✓個別判断 ・明示又は黙示の契約義務違反 ・衡平法に基づく信任義務違反	－
侵害行為類型（刑事）	・第21条第1項第1～5号、同条第2項第1～5号 ・主観的要件としては図利加害目的	－	－	・行為類型について unauthorised conduct という包括的な記載 ・主観的要件として無権限の認識 ・国家安全保障上の要件

6　まとめ

UK TS 規則は、営業秘密の取得、開示、使用は、秘密情報に対する守秘義務の違反となる場合に、違法とされる旨定めているが、その解釈を、判例法で確立された理論（the law of confidence）に委ねている。英国の契約法や判例法では、明示の秘密保持契約違反だけでなく、従業員の黙示の忠実義務違反、さらには契約がなくても成立する衡平法上の秘密保持義務違反が認められ、状況に応じて柔軟に保護範囲が決まる。NSA 2023 は、安全保障を背景として、無権限での営業秘密の不正取得、複製、記録、保持、開示、アクセス提供等の広い行為が侵害行為として規定されており、外国勢力要件を設ける点で、上記の民事上の保護とは性質が異なる。日本の不正競争防止法は、営業秘密の不正競争行為について明確に規定している一方で、英国では判例法中心の個別事案ごとの柔軟な判断がなされる傾向がある点で差異がある。

第4章　民事措置

1　救済手段

UK TS 規則において、営業秘密の侵害行為があった場合、以下の手段が認められている。

(1)　恒久的差止命令

①　裁判所が、本案において、営業秘密の不正取得、使用又は開示があったと認定した場合、裁判所は、営業秘密の保有者の申立てに基づき、侵害者に対し

て、以下の一つ又は複数の措置を命ずることができる[160]。

a. 営業秘密の使用又は開示の停止、又は場合により、禁止。

b. 侵害品の製造、提供、市場への流通若しくは使用、又は当該目的のための侵害品の輸入、輸出若しくは保管の禁止。

c. 侵害品に関する是正措置の採用（必要に応じて以下を含む）

ⅰ. 侵害品の市場からの回収。

ⅱ. 侵害品から侵害する特徴を失わせること。

ⅲ. 侵害品の破棄又は市場からの撤去（ただし、撤去が当該営業秘密の保護を損なわない場合に限る）。

d. 営業秘密を含む又は具現化した文書、物品、資料、物質若しくは電子ファイルの全部若しくは一部の破棄、又は必要に応じて、これらの全部若しくは一部の申立人への引渡し。

② 上記の命令の申立てを審理し、当該命令の比例性を評価するにあたり、裁判所は事案の具体的事情を考慮しなければならず、必要に応じて以下を含む要素を考慮するものとする[161]。

a. 営業秘密の価値その他の特性。

b. 営業秘密を保護するために講じられた措置。

c. 侵害者による営業秘密の取得、使用又は開示の態様。

d. 営業秘密の不正使用又は開示の影響。

e. 当事者の正当な利益及び当該措置の採否が当事者に及ぼす影響。

f. 第三者の正当な利益。

g. 公共の利益。

h. 基本的権利の保護。

③ 上記命令の対象となる者は、申立てにより、上記命令に代えて損害賠償の支払いを命じる命令を求めることができ、裁判所は、以下の各号のいずれにも該当する場合に、当該命令を発することができる[162]。

a. 使用又は開示の時点において、その者が、営業秘密を不正使用又は開示している他者から取得されたものであることを知らず、又は知るべきものでもなかった場合。

b. 当該命令に基づく措置の実施が、その対象者にとって過度な不利益をもたらす場合。

c. 損害を受けた者に対して損害賠償を支払うことが合理的に妥当である場合。

---

160 UK TS 規則第 14 条。

161 UK TS 規則第 15 条。

162 UK TS 規則第 16 条。

(2) 損害賠償

裁判所は、損害を被った当事者の申立てに基づき、営業秘密の不正取得、使用又は開示が行われていることを知っていた、又は知るべきであった侵害者に対し、営業秘密の保有者に対する当該不正取得、使用又は開示により実際に被った損害に相当する損害賠償の支払いを命じなければならない。損害算定規定に基づき、損害を算定する場合、特に以下を含む、全ての適切な要素を考慮しなければならない[163]。

① 営業秘密の保有者が被った経済的損害（逸失利益を含む）及び侵害者が得た不当な利益。

② 営業秘密の不正取得、使用又は開示によって営業秘密の保有者に生じた精神的損害を含む、経済的要素以外の要素。

また、裁判所は、必要に応じて、侵害者が当該営業秘密の使用について使用許諾を取得していたと仮定した場合に支払うべき使用許諾料又は料金に基づいて損害賠償を命じることができる。

(3) 暫定的措置（保全措置）[164]

① 裁判所は、営業秘密の保有者の申立てに基づき、営業秘密であると主張される情報の侵害者に対して、以下のいずれかの措置を命ずることができる。

a. 営業秘密の使用又は開示の停止、又は場合により、禁止。

b. 侵害品の製造、提供、市場への流通若しくは使用、又は当該目的のための侵害品の輸入、輸出若しくは保管の禁止。

c. 侵害が疑われる物品（輸入品を含む）が市場に流通することを防ぐための、当該物品の差押え又は引渡し。

② 上記命令の可否につき、裁判所は、「審理すべき重大な争点」の存在を確認しなければならず、申立人の保護の必要性は、被申立人が自身の権利行使を妨げられることによる損害（これも損害賠償で十分に救済されない場合がある）とのバランスで考慮されなければならない[165]。そして、上記命令を発するか否かを判断し、当該命令の比例性を評価するにあたり、裁判所は、事案の具体的状況を考慮し、必要に応じて以下の事項を含めて検討しなければならない[166]。

a. 営業秘密の価値及びその他特性。

---

163 UK TS 規則第 17 条。

164 UK TS 規則第 11 条。

165 American Cyanamid Co v. Ethicon Ltd [1975] FSR p101,106-108.

166 UK TS 規則第 12 条第 2 項。

b. 営業秘密を保護するために講じられた措置。
c. 営業秘密を取得、使用又は開示する際の被疑侵害者の行為。
d. 営業秘密の不正使用又は開示の影響。
e. 当事者の正当な利益及び当該措置の許可又は却下が当事者に与える影響。
f. 第三者の正当な利益。
g. 公共の利益。
h. 基本的権利の保護。

③ 上記命令を発する前に、裁判所は、営業秘密の保有者に対して、以下の各号の事項について、裁判所が十分な確実性をもって認定できると合理的に考えうる証拠の提示を求めることができる[167]。
a. 営業秘密が存在すること。
b. 営業秘密の保有者が申立てを行っていること。
c. 被疑侵害者が以下のいずれかに該当すること。
i. 営業秘密を不正取得したこと。
ii. 営業秘密を不正使用又は開示していること。
iii. 営業秘密を不正使用又は開示しようとしていること。

2 権利・救済手段の期間制限[168]

イングランド及びウェールズ並びに北アイルランドにおける出訴期間（limitation period）は 6 年、スコットランドにおける時効期間（prescriptive period）は 5 年である。両期間の起算点は、(a)当該請求の対象となる不正取得、使用若しくは開示が終了した日、又は(b)営業秘密の保有者が知った日（営業秘密の保有者が、(i)侵害者の行為の存在、(ii)当該行為が営業秘密の不正取得、使用若しくは開示に該当すること、及び(iii)侵害者の身元の全てを初めて知り、若しくは合理的に知り得たとみなされる日をいう）のいずれか後の日をいうとされている。

3 まとめ

UK TS 規則は、営業秘密侵害に対して、恒久的差止命令、損害賠償、及び暫定的措置（保全措置）といった民事上の救済措置を規定している。恒久的差止命令には、営業秘密の使用又は開示の停止命令又は禁止命令だけでなく、侵害品の製造等の禁止命令、市場からの回収等の是正措置命令、関連文書の破棄命令等も含まれる。損害賠償請求については、営業秘密の保有者が被った逸失利益を含む経済的損害、精神的損害、侵害者が得た不当な利益等全ての適切な要素を考慮の上損害額が算定される。裁

167 UK TS 規則第 12 条第 1 項。

168 UK TS 規則第 5 条、第 6 条。

判所は、侵害者が当該営業秘密の使用について使用許諾を取得していたと仮定した場合に支払うべき使用許諾料又は料金に基づいて損害賠償も可能である。

第 5 章　刑事措置

1　NSA 2023

NSA 2023 は、スパイ活動、破壊工作、及び外国勢力の指示を受けた者による国家安全保障への脅威に関する規定を定める法律である（NSA 2023 前文）。

NSA 2023 における営業秘密の定義は第 2 章 3、営業秘密侵害行為の定義は第 3 章 4 記載のとおりである。以下の各号をいずれも満たす場合、犯罪が成立し、14 年以下の拘禁若しくは罰金又はその両方に処せられる（NSA 2023 第 2 条第 1 項、第 8 項）。

① 当該行為者が次に掲げる行為のいずれかを行ったこと。
   a. 営業秘密を取得し、複製し、記録し、又は保持する行為。
   b. 営業秘密を開示し、又は第三者に対しこれに対する利用を許す行為。
② 当該行為が無権限であること。
③ 当該行為者がその行為が無権限であることを知っているか、又はその者が知っている他の事情を踏まえて合理的に知っているべきであること。
④ 当該行為について外国勢力要件（第 31 条参照）が満たされていること。

2　コンピュータ不正使用法

営業秘密の不正取得等が、コンピュータ不正使用法に基づいて処罰対象となる場合もある。コンピュータ不正使用法は、下記を犯罪と定める。

(1) 第 1 条：コンピュータ装置への不正アクセス

以下の要件を全て満たす場合、その者は罪を犯したものとされている。

① コンピュータに何らかの機能を実行させることにより、他のコンピュータに保存されているプログラム若しくはデータへの無権限のアクセスをうること、又はそのような無権限のアクセスを可能にすることを意図すること。
② 行為者が取得しようとする、又は可能にしようとするアクセスが無権限であること。
③ 当該コンピュータに当該機能を実行させる時点で、行為者が、当該アクセスが無権限であることを知っていること。

なお、①の「コンピュータに何らかの機能を実行させることにより、他のコンピュータに保存されているプログラム又はデータへの無権限のアクセスをうる」場合とは、以下のいずれかをいう[169]。

169　コンピュータ不正使用法第 17 条第 2 項。

a. プログラム又はデータを変更又は消去する場合。
b. プログラム又はデータを、保存されている記憶媒体以外の記憶媒体にコピー若しくは移動する場合、又は保存されている記憶媒体内の別の位置にコピー若しくは移動する場合。
c. プログラム又はデータを使用する場合。
d. プログラム又はデータを、保存されているコンピュータから出力させる場合（表示させる場合又はその他の方法による場合も含む）。

当該罪を犯した者は、以下の刑に処される。

① イングランド及びウェールズの略式裁判の場合、略式裁判の法定上限以下の拘禁若しくは罰金又はその両方。
② スコットランドの略式裁判の場合、12 か月を超えない拘禁若しくは法定上限以下の罰金又はその両方。
③ 公判による有罪判決の場合、2 年以下の拘禁若しくは罰金又はその両方。

(2) 第 2 条：他の犯罪の実行又はその実行を容易にする目的での無権限アクセス

法律で刑期が定められている犯罪又は 21 歳に達した者（イングランド及びウェールズでは 18 歳に達した者）で前科のない者が、5 年以上の拘禁刑が科されうる犯罪（イングランド及びウェールズにおいては、1980 年治安判事裁判所法（Magistrates' Courts Act）第 33 条による制限がなければ科されうる犯罪）について、①当該犯罪を実行する意図、又は②当該犯罪の実行を幇助する意図を有して、第 1 条に規定する犯罪が行われた場合、本罪に該当する。

当該罪を犯した者は、以下の刑に処される。

① イングランド及びウェールズの略式裁判の場合、略式裁判の法定上限以下の拘禁若しくは罰金又はその両方。
② スコットランドの略式裁判の場合、12 か月を超えない拘禁若しくは法定上限以下の罰金又はその両方。
③ 公判による有罪判決の場合、5 年以下の拘禁若しくは罰金又はその両方。

(3) 第 3 条：コンピュータの運用等を妨害する意図又は妨害する危険性を認識しながら行う不正行為

以下の要件を全て満たす場合、その者は本罪を犯したものとされる。

① コンピュータに対して権限なき行為を行ったこと。
② 当該行為を行う時点で、行為者が、当該行為が無権限であることを知っていること。
③ 以下の a.又は b.のいずれかに該当すること。
a. 以下のいずれかの意図で当該行為を行った場合。
i. コンピュータの運用を妨害すること。

ii. コンピュータに保存されているプログラム若しくはデータへのアクセスを妨げ、又は阻害すること。

iii. プログラムの運用又はデータの信頼性を損なうこと。

iv. 上記（i）から（iii）に掲げる行為のいずれかを可能にすること。

b. 行為者が、当該行為により上記 a.記載の結果が生じる可能性があると認識している場合。

当該罪を犯した者は、以下の刑に処される。

① イングランド及びウェールズの略式裁判の場合、略式裁判の法定上限以下の拘禁若しくは罰金又はその両方。

② スコットランドの略式裁判の場合、12 か月を超えない拘禁若しくは法定上限以下の罰金又はその両方。

③ 公判による有罪判決の場合、10 年以下の拘禁若しくは罰金又はその両方。

(4) 第 3ZA 条：重大な損害を生じさせ、又はその危険を生じさせる不正行為

以下の要件を全て満たす場合、その者は本罪を犯したものとされる。

① コンピュータに対して権限なき行為を行ったこと。

② 当該行為を行う時点で、行為者が、当該行為が無権限であることを知っていること。

③ 当該行為が実質的に重大な損害を生じさせること、又はそのような損害を生じさせる重大な危険を生じさせること。

④ 行為者が、当該行為により重大な損害を生じさせる意図を有している、又はそのような損害が発生する危険性を認識していること。

「重大な損害」とは、以下のいずれかに該当するものをいう。

① 人の福祉に対する損害（損害の生じる場所を問わない）。

② 環境に対する損害（損害の生じる場所を問わない）。

③ 国家経済に対する損害（損害の生じる国を問わない）。

④ 国家安全保障に対する損害（損害の生じる国を問わない）。

当該罪が、以下のいずれかを引き起こした場合又はその危険性を生じさせた場合、その者は、公判で有罪判決を下された場合、無期拘禁若しくは罰金又はその両方に処される。

① 人の福祉に対する損害又は人の福祉に対する重大な損害。

② 国家安全保障に対する重大な損害。

また、当該罪を犯した者は、上記の場合を除き、公判による有罪判決の場合、14 年以下の拘禁若しくは罰金又はその両方に処される。

3　その他刑事罰

上記の他、例えば、従業員であっても、立ち入りの許されていない施設に立ち入る等した場合には、不法侵入に関する犯罪が成立し[170]、自己の支配下にない書類や物品の持ち出しがあるのであれば、窃盗法第 1 条が適用となり、その法定刑は 7 年である（窃盗法第 7 条）。

4　日本法との比較

日本において、上記 1 記載の NSA 2023 のように国家安全保障への脅威に対抗するための法律としては、特定秘密の保護に関する法律（平成 25 年法律第 108 号）が存在し、政府が特定秘密として指定した情報（同法第 3 条）に限り、外国の利益を図る目的等で取得等一定の行為を行った場合に罪が成立する（同法第 24 条）。加えて、日本の不正競争防止法における刑事罰については、第 3 章 5 記載のとおりである。

また、上記 2 記載のコンピュータ不正使用法については、情報に対する不正な手段から当該情報を保護する点で、不正競争防止法の不正取得類型（第 2 条第 1 項第 4 号）と共通する側面がある。一方で、コンピュータ不正使用法は、営業秘密に限定せず、プログラムやデータ等を保護対象にしている点で相違する。なお、営業秘密に関連する法規から離れると、刑法の不正指令電磁的記録取得等罪（刑法第 168 条の 2、第 168 条の 3）も、コンピュータ不正使用法と同じくサイバー犯罪を規制するものであるが、当該罪は主にコンピュータウイルス等の不正指令電磁的記録に焦点をあてている点が相違する。また、日本の「不正アクセス行為の禁止等に関する法律」は、不正アクセス等を規制する点でコンピュータ不正使用法と近しいが、当該法律は「アクセス制御機能」（同法第 2 条第 3 項）の突破行為である「不正アクセス」（同法第 2 条第 4 項）等を禁止し（同法第 3 条～第 7 条）、処罰する（同法第 11 条～第 14 条）という位置づけがコンピュータ不正使用法と異なる。

上記 3 との比較では、同様のケースでは、日本においても刑法上の住居侵入等罪（刑法第 130 条）や窃盗罪（刑法第 235 条）が成立しうる。

5　まとめ

NSA 2023 は、国家安全保障に対する脅威を規制する包括的な法律であり、営業秘密の不正取得・使用・開示についても刑事罰を設けている。一方、営業秘密の不正取得等がサイバー手段で行われる場合には、コンピュータ不正使用法が適用されうる。同法においては、コンピュータ装置への不正アクセス（第 1 条）やコンピュータの運用等を妨害する意図又は妨害する危険性を認識しながら行う不正行為（第 3 条）が刑事罰の対象とされており、加えて、重大な損害を生じさせ、又はその危険を生じさせる不正行為（3ZA 条）については、より重い刑罰が科される。さらに、行為態様によっ

170　Criminal Justice and Public Order Act 1994, Section 68.

ては不法侵入に関する犯罪や窃盗罪等も成立しうる。NSA 2023 と比較すると日本の特定秘密保護法が対象とする情報は極めて限定的である。また、コンピュータ不正使用法と比較すると日本の刑法における不正指令電磁的記録取得等罪や不正アクセス禁止法はその対象となる行為はより限定的である。

第 6 章　行政措置

英国において営業秘密侵害に対する行政措置はない[171]。

第 7 章　適用範囲

1　UK TS 規則

UK TS 規則の適用範囲は条文上明確ではない。この点に関し、Celgard, LLC v. Shenzhen Senior Technology Material Co.[172]は、抵触法に従い、損害発生地が英国の場合に、UK TS 規則が準拠法として適用されると判示した。

当該裁判例は、営業秘密の取得及び営業秘密を使用した製品の製造が中国でなされ、当該製品が英国に輸入された事案である。原告は、被告らの秘密保持義務違反により受けた損害は、輸入先である英国で発生しており、英国での不正な競争に関して生じる請求が問題となっているので、英国法が適用されると主張し、被告は、中国法が適用されると反論した。

第一審は、抵触法につき、EU レベルでの不法行為等に係る抵触法の規律を定めた Rome Ⅱ規則（Regulation (EC) No 864/2007 on the law applicable to non-contractual obligations）が適用され[173]、不法行為に基づく非契約債務に適用される法が決定されるため、損害発生地の法律が適用されると述べた。その上で、営業秘密を不正利用して製造された製品の輸入や販売が英国で行われ、それが原告の英国顧客に対する販売能力に損害を与えるため、損害発生地は英国であると判断した。

また、裁判所は、UK TS 規則の立法趣旨からも、UK TS 規則の適用が認められると判断した。すなわち、UK TS 規則の解釈として、その前身となる EU 営業秘密指令は前文(4)(9)(28)において、海外で営業秘密を不正利用されて製造された製品が加盟国に輸入されることを問題視していることを指摘し、本件のように営業秘密を不正利用されて製造された製品を英国に輸入する行為は、UK TS 規則が英国で発生する可能性が

171　Carpmaels & Ransford LLP, “Q&A: enforcement proceedings for trade secrets in United Kingdom – Lexology”, 2 October 2025, .<https://www.lexology.com/library/detail.aspx?g=a6e15da0-23ea-4e44-8f72-adc537acd4a3>.

172　Celgard, LLC v. Shenzhen Senior Technology Material Co Ltd [2020] EWHC 2072.

173　当該裁判例は EU 脱退前のものであるが、英国は Rome II規則を国内法化しているため（Law Applicable to Contractual Obligations and Non-Contractual Obligations (Amendment etc.) (EU Exit) Regulations 2019 (SI 2019/834)）、EU 脱退後も同様の判断がなされうる。

あると想定している行為であると述べている。

以上により、当該事案においてUK TS規則が準拠法とされた。当該結論は、控訴審でも支持されている[174]。

2　NSA 2023

NSA 2023第2条第4項は、同条第1項は同項が定める行為が英国国外で行われた場合であっても適用されると定める。また、同条第5項は、同条第1項が定める行為が全て英国国外で行われた場合、当該営業秘密が「英国人（UK person）」（同条第6項で定義）の所有又は管理下にある場合に限り、犯罪となると定める。

3　コンピュータ不正使用法

コンピュータ不正使用法第4条は、犯罪行為が英国で行われたかどうか及び被告人が行為時点で英国にいたかどうかは犯罪の成否に影響しない（同条第1項）が、犯罪が成立するためには、少なくとも1つは英国との「重要な関連性」がなくてはならない（同条第2項）としている。同法第5条は、以下の場合に重要な関連性が認められると定める。

① 第1条、第3条、第3ZA条、又は第3A条に基づく犯罪に関し、被告人が当該犯罪行為時に英国国外に所在していた場合であっても、当該犯罪の有罪判決を確定するために証明が必要な行為又はその他事実が、「本国」（①イングランド及びウェールズに同法を適用する場合、イングランド及びウェールズ、②スコットランドに適用する場合、スコットランド、③北アイルランドに適用する場合、北アイルランドを指す。同法第4条第6項）で発生した場合には、本国の管轄権と重要な関連性が認められる。

② 第1条に基づく犯罪について、以下のいずれかに該当する場合にも「重要な関連性」が認められる。

a. 被告人が、コンピュータに機能を実行させる行為を行った時点で本国に所在していたとき。

b. 被告人が、当該行為により、無権限のアクセスを確保し、若しくは確保しようと意図した、又は無権限のアクセスを可能にし、若しくは可能にしようと意図したプログラム若しくはデータを含むコンピュータが、その時点で本国に所在していたとき。

③ 第3条に規定される犯罪に関して、以下のいずれかに該当する場合にも「重要な関連性」が認められる。

a. 被告人が、無権限の行為を行った（又は行わせた）時点で本国に所在していたとき。

174　Shenzhen Senior Technology Material Co Ltd v Celgard, LLC (Rev 1) [2020] EWCA Civ 1293.

b. 当該無権限の行為が、本国に所在するコンピュータに対して行われたとき。

④ 第 3ZA 条に規定される犯罪に関して、以下のいずれかに該当する場合にも「重要な関連性」が認められる。

a. 被告人が無権限の行為を行った（又は行わせた）時点で本国に所在していたとき。

b. 当該無権限の行為が、本国に所在するコンピュータに対して行われたとき。

c. 当該無権限の行為が、本国において（本条に定める）重大な損害を生じさせたとき、又はそのような損害を生じさせる重大な危険を生じさせたとき。

4 まとめ

UK TS 規則の適用範囲は条文上明確ではないが、裁判例において、損害発生地が英国の場合には、UK TS 規則が準拠法として適用されると判示されている。NSA 2023 及びコンピュータ不正使用法は、行為が英国国外で行われた場合であっても適用されるが、処罰の対象となる行為は、英国と一定の関係性を有する行為である必要がある。

第 8 章 訴訟手続に関する諸制度

1 訴訟手続中の営業秘密の保護

(1) 公開原則

民事裁判手続における公開の原則は判例法上認められている[175]。また、国内法化された欧州人権条約第 6 条第 1 項及び民事訴訟規則（Civil Procedure Rules）第 39.2 条第 1 項でも、公開の原則が認められており、判例法の原則を補強している。

(2) 公開原則の例外

ア 営業秘密に関する公開原則の例外

UK TS 規則では、営業秘密等に関する、公開原則の例外として、以下の定めがある。

訴訟手続の参加者又は訴訟手続の一部を構成する文書を利用する参加者は、以下の営業秘密又は営業秘密であると主張されている情報を使用又は開示してはならない（第 10 条第 1 項）。

① 利害関係人による正当な理由を示した申立て又は裁判所の職権に基づ

175 Scott v Scott ([1913] AC 417)

き、裁判所が命令により秘密であると認定し、

② 参加者が訴訟手続への参加又は利用の結果として、知るに至ったもの。

上記義務は、訴訟手続が終了した後も、裁判所が最終的な判断により、営業秘密であると主張された情報が営業秘密の要件を満たさないと認定した場合、又は当該情報が、時の経過により、通常その種の情報を取り扱う者の間で一般に知られ、又は容易に入手可能となった場合を除き、存続する（第10条第2項、第3項）。

また、裁判所は、文書へのアクセス、審理の立会い、又は訴訟記録閲覧を限られた人数の者に制限し（いわゆるconfidentiality club）、それ以外の者に対しては、裁判所判断のうち営業秘密を含む部分を削除又は編集する措置を採ることができる（第10条第5項）。当該措置の採否、又はどの措置を命ずるか、及び当該措置の比例性を判断する際には、以下の事項を考慮しなければならない（第10条第7項）。

① 実効的な救済及び公正な裁判を受ける権利を確保する必要性。

② 当事者の正当な利益。

③ 当事者に対する潜在的な不利益。

イ その他、一般的な公開原則の例外

なお、その他の公開原則の例外については、以下の定めがある。

① 民事訴訟規則

審理の全部又は一部は、以下のいずれかに該当し、かつ「適正な司法の実現を確保するために非公開で行うことが必要」であると裁判所が確信する場合に限り、非公開で行わなければならない（第39.2条第3項）。

a. 公開により審理の目的が損なわれる場合。

b. 国家安全保障に関する事項に関わる場合。

c. 秘密情報（個人の資産に関する情報を含む）を扱い、公開によりその秘密性が損なわれる場合。

d. 子又は保護対象者の利益を守るために非公開が必要な場合。

e. 事前通知なしの申立てに関する審理で、公開が被申立人に不当な不利益を与える場合。

f. 信託財産の管理又は被相続人の財産管理に関する非訟事項に関連する場合。

g. その他、裁判所が適正な司法の実現を確保するために必要と判断する場合。

② 欧州人権条約[176]

公開の原則は、①民主的社会における道徳、公の秩序、若しくは国家安全保障の利益のため、②未成年者の利益や当事者の私生活の保護が必要な場合、又は、③公開が司法の利益を害する特別な事情において裁判所が厳格に必要と認める場合、制限されうる（第6条第1項）。

③ 裁判例（Scott v Scott 事件）

Scott v Scott 事件において、裁判所は、司法の運営は、事件の審理に関する限り、後述する極めて限定的な例外を除き、公開法廷で行われなければならないとの原則を述べた上で、例外についても「司法の最も根本的な目的が“正義の実現”であるという、より根本的な原則から生じる」とした。そして、例外が認められる場合として、「被後見人や精神病者の二つの事案において、裁判所は主として被後見人や精神病者の利益を保護するために裁判を行っている」という場合と「秘密の製造方法（secret process）等が争点となる訴訟であり、公開によって訴訟の目的物自体が失われる場合」をあげた。これらの場合について「正義の実現が常に最優先の目的である以上、公開原則という一般的なルールも、結局はその手段にすぎず、この最優先の目的の前には譲歩しなければならない」と述べられている。

2 訴訟手続における情報の開示・証拠収集

証拠収集手段又は開示制限について、UK TS 規則は営業秘密に関する特別な規律を設けていない。そのため、この点は民事訴訟規則等の一般法に委ねられる。

(1) 証拠収集手段

ア 民事訴訟規則第 18.1 条：更なる情報提供の要求（obtaining further information）

裁判所は、当事者に対して、訴訟で争点となっている事項について明確化を求める又は追加情報の提供を求める命令を発することができる（第18.1条(1)）。

裁判所は命令を発するにあたって、条件を付すことや、命令又は条件に従わなかった場合の制裁を明示することができる（第3.1条(3)）。

イ 民事訴訟規則第 31 条：文書の開示及び閲覧（disclosure and inspection of

176 1998 年人権法（Human Rights Act 1998）第1条により国内的効力を付与されている。

documents）

文書開示（disclosure）とは、当事者が文書が存在すること又は存在していたことを明らかにすることである（第 31.2 条）。標準的な開示（standard disclosure）では、当事者は以下の文書のみを開示することが求められる（第 31.6 条）。

① 自己が依拠する文書。
② 以下のいずれかに該当する文書。
   a. 自己の主張に不利となる文書。
   b. 他の当事者の主張に不利となる文書。
   c. 他の当事者の主張を支持する文書。
③ 関連する実務指針により開示が求められる文書。

標準的な開示の手続として、当事者は、他の当事者に対して文書のリスト（list of documents）を送達することによって開示を行う（第 31.10 条第 1 項）。

裁判所は、特定開示命令（specific disclosure）又は特定閲覧命令（specific inspection）を出すことができる。特定開示命令とは、当事者に対して以下のいずれか又は複数を行うことを命じるものである。

① 命令で指定された文書又は文書の種類の開示。
② 命令で定められた範囲における探索。
③ 当該探索の結果見つかった文書の開示。

特定閲覧命令とは、当事者に対し、相手方が「不相応」を理由に閲覧を拒否した文書についても、文書の閲覧を許可することを命じるものである（第 31.12 条）。

開示対象となる電子文書には、メール、カレンダー、テキストメッセージ、ボイスメール、音声・映像記録、チャットや SNS のメッセージ、写真、設計図や図面等に加え、削除済みの電子文書やメタデータも含まれる。また、自らの管理下にある文書だけでなく、過去に管理下にあった文書も開示しなければならない。そして、文書の保存義務は、一般に訴訟の提起ではなく、訴訟の提起が想定できるようになった時点で発生するため、即時対応として、①ルーチンの破棄（バックアップ削除等）の停止、②記録管理担当者（第三者委託先を含む）への通知、③関連文書を保有・作成しうる全従業員への通知、④メタデータの保存（容易に変更されるため）等の対応を行い、上記の開示対象文書を保存する必要がある[177]。

---

177 Hogan Lovells, “Disclosure of documents in civil proceedings in England and Wales”, November 2023. <https://www.hoganlovells.com/-/media/project/english-site/our-thinking/publication-embedded-media/pdfs/2023/disclosure-of-d1-.pdf?sc_lang=en&hash=9D52279F9E2228BE56E771B1C2DA7AE6>.

(2) 資料の開示制限

ア 民事訴訟規則第 5.4C 条：第三者の書面の閲覧制限

原則として、訴訟当事者ではない第三者も、主張書面や判決等の訴訟書面の交付を受けることができる（第 5.4C 条(1)）。また、当事者の提出したその他の文書や裁判所と当事者との間のやり取りについても、裁判所が許可すれば、取得可能である（第 5.4C 条(2)）。これに対し、訴訟当事者又は訴訟書面上特定される者の申立てにより、裁判所は、第三者に訴訟書面の写しを取得させない、訴訟書面の写しを取得することができる第三者を制限する、裁判所の指示に従って編集された場合に限って訴訟書面の写しを取得できるようにする、その他裁判所が適切と認める命令を発することができる（第 5.4C 条(4)）。

イ 民事訴訟規則第 18.2 条：更なる情報の利用制限

裁判所は、当事者が他の当事者に提供した情報（自発的に提供された場合も、第 18.1 条に基づく命令に従って提供された場合も含む）について、当該情報が提供された訴訟手続以外の目的で使用してはならないと指示することができる。

ウ 民事訴訟規則第 31.22 条：開示文書のその後の利用

文書の開示を受けた当事者は、①当該文書が公開法廷において陳述又は引用された場合、②裁判所の許可があった場合、③開示当事者が同意した場合を除いて、当該訴訟手続の目的のためにのみ当該文書を使用できる（第 31.22 条(1)）。

公開法廷において陳述又は引用された文書であっても、訴訟当事者又は当該文書の所有者の申立てにより、裁判所は文書使用を制限又は禁止する命令を発することができる（第 31.22 条(2)、(3)）。

3 まとめ

UK TS 規則は、訴訟手続に関し、営業秘密の秘密保持を確保するための措置として、裁判所が必要に応じて秘密保持のための措置を命じることができることを定めている。具体的には、裁判所は、訴訟手続の参加者又は訴訟手続の一部を構成する文書を利用する参加者に対し、営業秘密又は営業秘密であると主張されている情報の使用又は開示を制限することができる。また、文書へのアクセス、審理の立会い、又は訴訟記録閲覧について、限られた人数の者に制限しうる。

第 9 章　営業秘密侵害事件の動向

1　英国における営業秘密侵害事件

英国における営業秘密侵害事件の統計資料等は見あたっていない。なお、英国の Intellectual Property Office（以下「UK IPO」という）が 2021 年 4 月に公表したレポート[178]では、営業秘密は特許等他の知的財産権と比較してコストが低く、迅速に導入できる点が評価され、英国のイノベーティブな企業の約 70%が、製品やプロセスのイノベーションを営業秘密で保護している一方で、デジタル化やリモートワークの普及により、営業秘密の流出リスクや侵害リスクが高まっているため、営業秘密に基づくイノベーションエコシステムの保護が英国企業にとって重要性を増していると述べられている。

2　参考になる裁判例

営業秘密の管理等に関して、以下の 2 つの 2020 年の裁判例では、法解釈が示されており参考となりうる。

(1)　秘密情報保護の暫定的措置の期間設定、賠償額算定の基礎

C Wzrd Ltd & Anor v. Kortan & Anor[179]において、裁判所は、暫定的措置を採るべきかという判断において考慮される損害は、金銭的に算定可能な部分と、算定困難な部分に分かれ、後者については暫定的措置の段階では具体的な額や内容の認定は行われず、本案審理で状況証拠や推計に基づいて算定されるとした。また、暫定的措置は、被告の違法行為によって生じた不当な競争上の優位を中和し、原告を本来あるべき競争状態に戻すために限定的に発令すべきと述べた。

本裁判例は、仮想通貨領域でオンライン教育・解析プラットフォームを運営する原告が、対立の後会員データベースをダウンロードし、競合会社を設立して競業準備・勧誘・返金促進・毀損的投稿等を行った元共同創業者に関して、暫定的措置を含む救済を申し立てた事案である。

裁判所は、被告が会員に返金請求を促したことで、原告は実際に返金対応を余儀なくされ、売上やキャッシュフローが減少したと認定し、当該返金請求による損害は算定可能であるが、SNS 等での批判や誹謗中傷によって会社のブランドイメージが損なわれ、将来的な新規顧客獲得が難しくなったという損害については

178　Intellectual Property Office, “The economic and innovation impacts of trade secrets - GOV.UK”, 19 April 2021, <https://www.gov.uk/government/publications/economic-and-innovation-impacts-of-trade-secrets/the-economic-and-innovation-impacts-of-trade-secrets>.

179　C Wzrd Ltd & Anor v. Kortan & Anor [2020] EWHC 1360 (Ch).

本案で判断されると判じた。

また、被告によるデータベースや顧客情報の不正使用を禁止する暫定的措置について、原告は 6 か月間の競業禁止を求めたが、裁判所は原告が本来の競争状態に回復するために必要最小限の長さでなければならず、適切な期間は 3 か月であると述べた。

(2) 秘密保持契約の効力を否定した裁判例

Quilter Private Client Advisers Ltd v. Falconer & Anor では、被用者との雇用契約内に秘密保持義務の規定が存在したが、当該規定は、秘密情報を網羅的に下記のように定義していた[180]。

「秘密情報とは、秘密情報と明記されているか否かにかかわらず、（1）当社が秘密情報と考える当社の経営、顧客、製品、事務、及び、財務に関する（経営展開プラン、価格設定、研究や解析結果を含むが、それに限らない）情報、並びに、（2）当社の経営、及び、供給者、顧客、代理人（中略）のいずれかに関する技術的データ、ノウハウを含めた営業秘密をいう。」

「あなたは、雇用に伴い、秘密情報にアクセスできます。あなたは、雇用中又は雇用終了後、自分の職務の適切な遂行以外に、秘密情報を使用、又は、いかなる人、会社、他の団体にも開示しないことに同意するものとする。」

裁判所は、このような限定のない条項は自由と競争の不当な制限にあたり、法的拘束力を持たないと、傍論で述べた。

3 まとめ

直近の英国における営業秘密に関する参考裁判例として、2020 年の、①暫定的措置について、考慮される損害のうち算定困難な部分については暫定的措置の段階では具体的な額や内容の認定は行われず、その範囲は不当な競争上の優位を中和し、原告を本来あるべき競争状態に戻すために限定的とすべきであることとした裁判例、及び、②雇用契約内の秘密情報を網羅的に記載した秘密保持義務の規定は、自由と競争の不当な制限にあたり、法的拘束力を持たないとした裁判例が存在する。

第 10 章 英国の法律・制度・運用を踏まえた、営業秘密漏えい対策を実施するにあたってのポイント

1 英国における営業秘密管理の留意点

英国政府は、2023 年 4 月「Guide to Managing Intellectual Property and Confidentiality」

---

180 Quilter Private Client Advisers Ltd v. Falconer & Anor [2020] EWHC 3294.para 15, 210-212.

という資料を公開している[181]。当該資料においては、「合理的な措置」を講じていることが法的保護の前提となるため、形式的なラベル付けだけでなく、実効性のある管理体制・教育・契約・技術的対策が求められると述べられ、営業秘密管理に関する実務的なポイントとして、以下のポイントが指摘されている。

① 秘密情報の特定と分類
　どの情報が秘密情報又は営業秘密であるかを特定し、最新のリストを作成・維持すること。
② アクセス管理
　営業秘密へのアクセスは知る必要がある者に限定し、物理的及び電子的な管理手段を用いて保護すること。
③ 契約・通知の徹底
　従業員、契約業者、ビジネスパートナーとは秘密保持契約（NDA）を締結し、全員が自らの責任を理解していることを確認すること。
④ 情報のマーキング
　秘密文書には「Confidential」等のラベルを付し、秘密性を明示すること。
⑤ 従業員教育
　秘密保持の重要性や違反時のリスクについて、定期的な教育・研修を実施すること。
⑥ 退職・契約終了時の対応
　従業員の退職や契約終了時には、秘密情報の返還又は安全な破棄を徹底し、継続する義務について本人に再確認させること。

2　ライセンス、生産委託、合弁会社設立で気をつけるべきポイント

　ライセンス、生産委託、合弁会社設立においては、情報の共有を伴う場合があるため、第三者提供によって、営業秘密の「秘密性」が失われるおそれがある。

　契約上、明示的な守秘義務の定めがない場合であっても、当事者間の契約関係に由来して、黙示の（秘密情報及び営業秘密の）守秘義務を生じさせることがあることは上述のとおりであるが、ライセンス契約はそのような守秘義務を生じさせる契約関係として捉えられていない。また、衡平法の原理に基づく守秘義務は、具体的な事実関係に依存し、どのような状況で生じるかはっきりしないことが多いので、当事者間の法律関係を明確化し、将来の紛争を防ぐためにも、秘密保持義務（守秘義務）を明示すべきである。その他、英国法が準拠法である場合には、以下のポイントに留意し、

181　Government Office for Technology Transfer, “Guide to Managing Intellectual Property and Confidentiality”, April 2023.
<https://assets.publishing.service.gov.uk/media/6489e0be5f7bb700127faa59/Guide_to_Managing_Intellectual_Property_and_Confidentiality.pdf>.

必要に応じて英国法弁護士に相談すべきである。

(1) ライセンス契約

UK IPO が 2014 年 12 月に公開した知的財産のライセンスに関するガイダンス[182]の中で示されているチェックリスト[183]では、以下がポイントとされている。

① 営業秘密の特定と明確化

ライセンス契約締結時には、どの情報が営業秘密に該当するかを明確に特定する。契約書において「秘密情報」や「ノウハウ」の範囲を具体的に定義する。

② 秘密保持義務（Confidentiality）

契約には秘密保持義務が含まれているか。その義務はどのくらいの期間続くか。契約終了後も存続するか。

③ 使用範囲・目的の限定

営業秘密の利用目的や使用範囲（例：特定の製品・プロセス・地域等）を契約で明確に限定する。

④ 再開示・第三者提供の制限

ライセンシーにサブライセンスや譲渡を認めるか。第三者への開示に制限があるか。

⑤ 契約終了時の対応

契約終了時に営業秘密や関連資料を返還・破棄させる義務を明記する。

⑥ 違反時の救済措置

営業秘密の不正利用や漏えいがあった場合、どのような救済措置（禁令・損害賠償等）をとれるか。

(2) 生産委託契約

英国内閣府は、「The Sourcing Playbook」という公共調達や外部委託に関する政府向けガイドラインを 2021 年 5 月に公表しており、最新版は 2023 年 6 月に公表された版となっている[184]。公共調達等に関する契約向けのガイドラインであるものの、以下のように民間企業にも参考となる記載が含まれている。

① 自社データの確保・維持

必要な時に適切な判断を行うため、自社の資産およびサービスに関する十

182 GOV.UK, “Licensing intellectual property”, 12 December 2024. <https://www.gov.uk/guidance/licensing-intellectual-property>.

183 Intellectual Property Office, “Licensing Intellectual Property – Checklist”. <https://assets.publishing.service.gov.uk/media/5a7db323ed915d2ac884d066/licensingchecklist.pdf>.

184 HM Government, “The Sourcing Playbook”, June 2023. <https://assets.publishing.service.gov.uk/media/64901fcc5f7bb700127fac5e/Sourcing_Playbook_Final.pdf>.

分なデータおよび情報を収集・維持する必要がある。サプライヤーは、良質なデータがなければ、サービスの提供モデルや価格構造が実行可能で持続可能かどうかを判断できない。

② 契約時のデータ提供

関連するデータについて、適切な範囲で共有すべきである。サプライヤーが事前にデューデリジェンスを完了できない状況において、データの誤りについてサプライヤーに責任を負わせるべきではない。

③ データに誤りがある場合の対応

データが誤っていることが後に判明した場合、誤りを反映して対応するための契約上の措置を設ける必要がある。

④ 契約終了・プロジェクト終了時の対応

契約終了時、サプライヤーの委託者に対する秘密情報及び営業秘密の返還又は安全な破棄がなされるよう契約で定めておくべきである。いかなる状況においても新たな契約体制へ円滑に移行できるよう、事前に十分な検討を行っておく必要がある。

(3) 合弁契約

合弁会社は、参加当事者が提供した、あるいは、合弁会社自身が調達した人材、技術、データ、施設、及び、資材を使用して、事業を行うことが多い。参加者の様々な秘密情報、営業秘密が提供されることもある。したがって、合弁会社が研究や開発をして得られる成果物に対して、どの者に所有権あるいは管理権が帰属するのかを契約で明確化しておくことが、特に重要となる。

英国内閣府が 2010 年 3 月に公開した公的セクターが民間企業等と JV を組成する際のガイダンス[185]では、以下が指摘されている。

① 秘密情報・営業秘密の保護

JV 契約及び関連契約には、各当事者の秘密情報及び営業秘密を保護するための適切な秘密保持条項を盛り込むことが重要である。

② 情報共有の範囲と制限

契約には、秘密情報の取扱方法、誰がその情報にアクセスできるか、JV 終了時にその情報がどのように扱われるかを明記すべきである。

③ 知的財産・ノウハウの管理

当事者は、JV に提供又は JV で開発された秘密情報や営業秘密を含む知的財産及びノウハウの所有権、利用、保護について合意しておくべきである。

185 HM TREASURY, “Joint Ventures: a guidance note for public sector bodies forming joint ventures with the private sector”, March 2010. <https://assets.publishing.service.gov.uk/media/5a7b9d82ed915d1311060652/06_joint_venture_guidance.pdf>.

3　まとめ

英国で営業秘密を管理・活用する際は、第三者との取引や共同事業の場面における情報コントロールや契約の取り決めを含め、実効性のある管理体制や教育・技術的対策を徹底することが必要となる。上記は日本法における望ましい営業秘密の管理体制と大きく異なるものではないが、前提となる英国法や裁判例を踏まえ、必要に応じて現地専門家の助言も活用しながら、営業秘密の保護体制を構築すべきである。

【条文】

EU

Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure

（原文）

CHAPTER I
Subject matter and scope

Article 1
Subject matter and scope

1. This Directive lays down rules on the protection against the unlawful acquisition, use and disclosure of trade secrets.

   Member States may, in compliance with the provisions of the TFEU, provide for more far-reaching protection against the unlawful acquisition, use or disclosure of trade secrets than that required by this Directive, provided that compliance with Articles 3, 5, 6, Article 7(1), Article 8, the second subparagraph of Article 9(1), Article 9(3) and (4), Article 10(2), Articles 11, 13 and Article 15(3) is ensured.

2. This Directive shall not affect:
   (a) the exercise of the right to freedom of expression and information as set out in the Charter, including respect for the freedom and pluralism of the media;
   (b) the application of Union or national rules requiring trade secret holders to disclose, for reasons of public interest, information, including trade secrets, to the public or to administrative or judicial authorities for the performance of the duties of those authorities;
   (c) the application of Union or national rules requiring or allowing Union institutions and bodies or national public authorities to disclose information submitted by businesses which those institutions, bodies or authorities hold pursuant to, and in compliance with, the obligations and prerogatives set out in Union or national law;
   (d) the autonomy of social partners and their right to enter into collective agreements, in accordance with Union law and national laws and practices.

3. Nothing in this Directive shall be understood to offer any ground for restricting the mobility of employees. In particular, in relation to the exercise of such mobility, this Directive shall not offer any ground for:
   (a) limiting employees' use of information that does not constitute a trade secret as defined in point (1) of Article 2;
   (b) limiting employees' use of experience and skills honestly acquired in the normal course of their employment;
   (c) imposing any additional restrictions on employees in their employment contracts other than restrictions imposed in accordance with Union or national law.

Article 2
Definitions

For the purposes of this Directive, the following definitions apply:

(1) 'trade secret' means information which meets all of the following requirements:

   (a) it is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;

   (b) it has commercial value because it is secret;

   (c) it has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret;

(2) 'trade secret holder' means any natural or legal person lawfully controlling a trade secret;

(3) 'infringer' means any natural or legal person who has unlawfully acquired, used or disclosed a trade secret;

(4) 'infringing goods' means goods, the design, characteristics, functioning, production process or marketing of which significantly benefits from trade secrets unlawfully acquired, used or disclosed.

CHAPTER II
Acquisition, use and disclosure of trade secrets

Article 3
Lawful acquisition, use and disclosure of trade secrets

1. The acquisition of a trade secret shall be considered lawful when the trade secret is obtained by any of the following means:

   (a) independent discovery or creation;

   (b) observation, study, disassembly or testing of a product or object that has been made available to the public or that is lawfully in the possession of the acquirer of the information who is free from any legally valid duty to limit the acquisition of the trade secret;

   (c) exercise of the right of workers or workers' representatives to information and consultation in accordance with Union law and national laws and practices;

   (d) any other practice which, under the circumstances, is in conformity with honest commercial practices.

2. The acquisition, use or disclosure of a trade secret shall be considered lawful to the extent that such acquisition, use or disclosure is required or allowed by Union or national law.

Article 4
Unlawful acquisition, use and disclosure of trade secrets

1. Member States shall ensure that trade secret holders are entitled to apply for the measures, procedures and remedies provided for in this Directive in order to prevent, or obtain redress for, the unlawful acquisition, use or disclosure of their trade secret.

2. The acquisition of a trade secret without the consent of the trade secret holder shall be considered unlawful, whenever carried out by:

   (a) unauthorised access to, appropriation of, or copying of any documents, objects, materials,

substances or electronic files, lawfully under the control of the trade secret holder, containing the trade secret or from which the trade secret can be deduced;

(b) any other conduct which, under the circumstances, is considered contrary to honest commercial practices.

3. The use or disclosure of a trade secret shall be considered unlawful whenever carried out, without the consent of the trade secret holder, by a person who is found to meet any of the following conditions:

(a) having acquired the trade secret unlawfully;

(b) being in breach of a confidentiality agreement or any other duty not to disclose the trade secret;

(c) being in breach of a contractual or any other duty to limit the use of the trade secret.

4. The acquisition, use or disclosure of a trade secret shall also be considered unlawful whenever a person, at the time of the acquisition, use or disclosure, knew or ought, under the circumstances, to have known that the trade secret had been obtained directly or indirectly from another person who was using or disclosing the trade secret unlawfully within the meaning of paragraph 3.

5. The production, offering or placing on the market of infringing goods, or the importation, export or storage of infringing goods for those purposes, shall also be considered an unlawful use of a trade secret where the person carrying out such activities knew, or ought, under the circumstances, to have known that the trade secret was used unlawfully within the meaning of paragraph 3.

Article 5
Exceptions

Member States shall ensure that an application for the measures, procedures and remedies provided for in this Directive is dismissed where the alleged acquisition, use or disclosure of the trade secret was carried out in any of the following cases:

(a) for exercising the right to freedom of expression and information as set out in the Charter, including respect for the freedom and pluralism of the media;

(b) for revealing misconduct, wrongdoing or illegal activity, provided that the respondent acted for the purpose of protecting the general public interest;

(c) disclosure by workers to their representatives as part of the legitimate exercise by those representatives of their functions in accordance with Union or national law, provided that such disclosure was necessary for that exercise;

(d) for the purpose of protecting a legitimate interest recognised by Union or national law.

CHAPTER III
Measures, procedures and remedies

Section 1
General provisions

Article 6
General obligation

1. Member States shall provide for the measures, procedures and remedies necessary to ensure the availability of civil redress against the unlawful acquisition, use and disclosure of trade secrets.

2. The measures, procedures and remedies referred to in paragraph 1 shall:

   (a) be fair and equitable;

   (b) not be unnecessarily complicated or costly, or entail unreasonable time-limits or unwarranted delays; and

   (c) be effective and dissuasive.

Article 7
Proportionality and abuse of process

1. The measures, procedures and remedies provided for in this Directive shall be applied in a manner that:

   (a) is proportionate;

   (b) avoids the creation of barriers to legitimate trade in the internal market; and

   (c) provides for safeguards against their abuse.

2. Member States shall ensure that competent judicial authorities may, upon the request of the respondent, apply appropriate measures as provided for in national law, where an application concerning the unlawful acquisition, use or disclosure of a trade secret is manifestly unfounded and the applicant is found to have initiated the legal proceedings abusively or in bad faith. Such measures may, as appropriate, include awarding damages to the respondent, imposing sanctions on the applicant or ordering the dissemination of information concerning a decision as referred to in Article 15.
   Member States may provide that measures as referred to in the first subparagraph are dealt with in separate legal proceedings.

Article 8
Limitation period

1. Member States shall, in accordance with this Article, lay down rules on the limitation periods applicable to substantive claims and actions for the application of the measures, procedures and remedies provided for in this Directive.
   The rules referred to in the first subparagraph shall determine when the limitation period begins to run, the duration of the limitation period and the circumstances under which the limitation period is interrupted or suspended.

2. The duration of the limitation period shall not exceed 6 years.

Article 9
Preservation of confidentiality of trade secrets in the course of legal proceedings

1. Member States shall ensure that the parties, their lawyers or other representatives, court officials, witnesses, experts and any other person participating in legal proceedings relating to the unlawful acquisition, use or disclosure of a trade secret, or who has access to documents which form part of those legal proceedings, are not permitted to use or disclose any trade secret or alleged trade secret which the competent judicial authorities have, in response to a duly reasoned application by an interested party, identified as confidential and of which they have become aware as a result of such participation or access. In that regard, Member States may also allow competent judicial authorities to act on their own initiative.
   The obligation referred to in the first subparagraph shall remain in force after the legal proceedings have ended. However, such obligation shall cease to exist in any of the following circumstances:

(a) where the alleged trade secret is found, by a final decision, not to meet the requirements set out in point (1) of Article 2; or

(b) where over time, the information in question becomes generally known among or readily accessible to persons within the circles that normally deal with that kind of information.

2. Member States shall also ensure that the competent judicial authorities may, on a duly reasoned application by a party, take specific measures necessary to preserve the confidentiality of any trade secret or alleged trade secret used or referred to in the course of legal proceedings relating to the unlawful acquisition, use or disclosure of a trade secret. Member States may also allow competent judicial authorities to take such measures on their own initiative.
The measures referred to in the first subparagraph shall at least include the possibility:

(a) of restricting access to any document containing trade secrets or alleged trade secrets submitted by the parties or third parties, in whole or in part, to a limited number of persons;

(b) of restricting access to hearings, when trade secrets or alleged trade secrets may be disclosed, and the corresponding record or transcript of those hearings to a limited number of persons;

(c) of making available to any person other than those comprised in the limited number of persons referred to in points (a) and (b) a non-confidential version of any judicial decision, in which the passages containing trade secrets have been removed or redacted.

The number of persons referred to in points (a) and (b) of the second subparagraph shall be no greater than necessary in order to ensure compliance with the right of the parties to the legal proceedings to an effective remedy and to a fair trial, and shall include, at least, one natural person from each party and the respective lawyers or other representatives of those parties to the legal proceedings.

3. When deciding on the measures referred to in paragraph 2 and assessing their proportionality, the competent judicial authorities shall take into account the need to ensure the right to an effective remedy and to a fair trial, the legitimate interests of the parties and, where appropriate, of third parties, and any potential harm for either of the parties, and, where appropriate, for third parties, resulting from the granting or rejection of such measures.

4. Any processing of personal data pursuant to paragraphs 1, 2 or 3 shall be carried out in accordance with Directive 95/46/EC.

Section 2
Provisional and precautionary measures

Article 10
Provisional and precautionary measures

1. Member States shall ensure that the competent judicial authorities may, at the request of the trade secret holder, order any of the following provisional and precautionary measures against the alleged infringer:

(a) the cessation of or, as the case may be, the prohibition of the use or disclosure of the trade secret on a provisional basis;

(b) the prohibition of the production, offering, placing on the market or use of infringing goods, or the importation, export or storage of infringing goods for those purposes;

(c) the seizure or delivery up of the suspected infringing goods, including imported goods, so as to prevent their entry into, or circulation on, the market.

2. Member States shall ensure that the judicial authorities may, as an alternative to the measures referred to in paragraph 1, make the continuation of the alleged unlawful use of a trade secret subject to the lodging of guarantees intended to ensure the compensation of the trade secret holder. Disclosure of a trade secret in return for the lodging of guarantees shall not be allowed.

Article 11
Conditions of application and safeguards

1. Member States shall ensure that the competent judicial authorities have, in respect of the measures referred to in Article 10, the authority to require the applicant to provide evidence that may reasonably be considered available in order to satisfy themselves with a sufficient degree of certainty that:

   (a) a trade secret exists;

   (b) the applicant is the trade secret holder; and

   (c) the trade secret has been acquired unlawfully, is being unlawfully used or disclosed, or unlawful acquisition, use or disclosure of the trade secret is imminent.

2. Member States shall ensure that in deciding on the granting or rejection of the application and assessing its proportionality, the competent judicial authorities shall be required to take into account the specific circumstances of the case, including, where appropriate:

   (a) the value and other specific features of the trade secret;

   (b) the measures taken to protect the trade secret;

   (c) the conduct of the respondent in acquiring, using or disclosing the trade secret;

   (d) the impact of the unlawful use or disclosure of the trade secret;

   (e) the legitimate interests of the parties and the impact which the granting or rejection of the measures could have on the parties;

   (f) the legitimate interests of third parties;

   (g) the public interest; and

   (h) the safeguard of fundamental rights.

3. Member States shall ensure that the measures referred to in Article 10 are revoked or otherwise cease to have effect, upon the request of the respondent, if:

   (a) the applicant does not institute legal proceedings leading to a decision on the merits of the case before the competent judicial authority, within a reasonable period determined by the judicial authority ordering the measures where the law of a Member State so permits or, in the absence of such determination, within a period not exceeding 20 working days or 31 calendar days, whichever is the longer; or

   (b) the information in question no longer meets the requirements of point (1) of Article 2, for reasons that cannot be attributed to the respondent.

4. Member States shall ensure that the competent judicial authorities may make the measures referred to in Article 10 subject to the lodging by the applicant of adequate security or an equivalent assurance intended to ensure compensation for any prejudice suffered by the respondent and, where appropriate, by any other person affected by the measures.

5. Where the measures referred to in Article 10 are revoked on the basis of point (a) of paragraph 3 of this Article, where they lapse due to any act or omission by the applicant, or where it is

subsequently found that there has been no unlawful acquisition, use or disclosure of the trade secret or threat of such conduct, the competent judicial authorities shall have the authority to order the applicant, upon the request of the respondent or of an injured third party, to provide the respondent, or the injured third party, appropriate compensation for any injury caused by those measures.

Member States may provide that the request for compensation referred to in the first subparagraph is dealt with in separate legal proceedings.

***Sect*ion 3**
Measures r*esulting from a decision on the merits of the case*

Article 12
Injunctions and corrective measures

1. Member States shall ensure that, where a judicial decision taken on the merits of the case finds that there has been unlawful acquisition, use or disclosure of a trade secret, the competent judicial authorities may, at the request of the applicant, order one or more of the following measures against the infringer:

   (a) the cessation of or, as the case may be, the prohibition of the use or disclosure of the trade secret;

   (b) the prohibition of the production, offering, placing on the market or use of infringing goods, or the importation, export or storage of infringing goods for those purposes;

   (c) the adoption of the appropriate corrective measures with regard to the infringing goods;

   (d) the destruction of all or part of any document, object, material, substance or electronic file containing or embodying the trade secret or, where appropriate, the delivery up to the applicant of all or part of those documents, objects, materials, substances or electronic files.

2. The corrective measures referred to in point (c) of paragraph 1 shall include:

   (a) recall of the infringing goods from the market;

   (b) depriving the infringing goods of their infringing quality;

   (c) destruction of the infringing goods or, where appropriate, their withdrawal from the market, provided that the withdrawal does not undermine the protection of the trade secret in question.

3. Member States may provide that, when ordering the withdrawal of the infringing goods from the market, their competent judicial authorities may order, at the request of the trade secret holder, that the goods be delivered up to the holder or to charitable organisations.

4. The competent judicial authorities shall order that the measures referred to in points (c) and (d) of paragraph 1 be carried out at the expense of the infringer, unless there are particular reasons for not doing so. Those measures shall be without prejudice to any damages that may be due to the trade secret holder by reason of the unlawful acquisition, use or disclosure of the trade secret.

Article 13
Conditions of application, safeguards and alternative measures

1. Member States shall ensure that, in considering an application for the adoption of the injunctions and corrective measures provided for in Article 12 and assessing their proportionality, the competent judicial authorities shall be required to take into account the specific circumstances of the case, including, where appropriate:

(a) the value or other specific features of the trade secret;

(b) the measures taken to protect the trade secret;

(c) the conduct of the infringer in acquiring, using or disclosing the trade secret;

(d) the impact of the unlawful use or disclosure of the trade secret;

(e) the legitimate interests of the parties and the impact which the granting or rejection of the measures could have on the parties;

(f) the legitimate interests of third parties;

(g) the public interest; and

(h) the safeguard of fundamental rights.

Where the competent judicial authorities limit the duration of the measures referred to in points (a) and (b) of Article 12(1), such duration shall be sufficient to eliminate any commercial or economic advantage that the infringer could have derived from the unlawful acquisition, use or disclosure of the trade secret.

2. Member States shall ensure that the measures referred to in points (a) and (b) of Article 12(1) are revoked or otherwise cease to have effect, upon the request of the respondent, if the information in question no longer meets the requirements of point (1) of Article 2 for reasons that cannot be attributed directly or indirectly to the respondent.

3. Member States shall provide that, at the request of the person liable to be subject to the measures provided for in Article 12, the competent judicial authority may order pecuniary compensation to be paid to the injured party instead of applying those measures if all the following conditions are met:

(a) the person concerned at the time of use or disclosure neither knew nor ought, under the circumstances, to have known that the trade secret was obtained from another person who was using or disclosing the trade secret unlawfully;

(b) execution of the measures in question would cause that person disproportionate harm; and

(c) pecuniary compensation to the injured party appears reasonably satisfactory.

Where pecuniary compensation is ordered instead of the measures referred to in points (a) and (b) of Article 12(1), it shall not exceed the amount of royalties or fees which would have been due, had that person requested authorisation to use the trade secret in question, for the period of time for which use of the trade secret could have been prohibited.

Article 14
Damages

1. Member States shall ensure that the competent judicial authorities, upon the request of the injured party, order an infringer who knew or ought to have known that he, she or it was engaging in unlawful acquisition, use or disclosure of a trade secret, to pay the trade secret holder damages appropriate to the actual prejudice suffered as a result of the unlawful acquisition, use or disclosure of the trade secret.

Member States may limit the liability for damages of employees towards their employers for the unlawful acquisition, use or disclosure of a trade secret of the employer where they act without intent.

2. When setting the damages referred to in paragraph 1, the competent judicial authorities shall take into account all appropriate factors, such as the negative economic consequences, including lost profits, which the injured party has suffered, any unfair profits made by the infringer and, in

appropriate cases, elements other than economic factors, such as the moral prejudice caused to the trade secret holder by the unlawful acquisition, use or disclosure of the trade secret.
Alternatively, the competent judicial authorities may, in appropriate cases, set the damages as a lump sum on the basis of elements such as, at a minimum, the amount of royalties or fees which would have been due had the infringer requested authorisation to use the trade secret in question.

Article 15
Publication of judicial decisions

1. Member States shall ensure that, in legal proceedings instituted for the unlawful acquisition, use or disclosure of a trade secret, the competent judicial authorities may order, at the request of the applicant and at the expense of the infringer, appropriate measures for the dissemination of the information concerning the decision, including publishing it in full or in part.

2. Any measure referred to in paragraph 1 of this Article shall preserve the confidentiality of trade secrets as provided for in Article 9.

3. In deciding whether to order a measure referred to in paragraph 1 and when assessing its proportionality, the competent judicial authorities shall take into account, where appropriate, the value of the trade secret, the conduct of the infringer in acquiring, using or disclosing the trade secret, the impact of the unlawful use or disclosure of the trade secret, and the likelihood of further unlawful use or disclosure of the trade secret by the infringer.

   The competent judicial authorities shall also take into account whether the information on the infringer would be such as to allow a natural person to be identified and, if so, whether publication of that information would be justified, in particular in the light of the possible harm that such measure may cause to the privacy and reputation of the infringer.

CHAPTER IV
Sanctions, reporting and final provisions

Article 16
Sanctions for non-compliance with this Directive

Member States shall ensure that the competent judicial authorities may impose sanctions on any person who fails or refuses to comply with any measure adopted pursuant to Articles 9, 10 and 12.

The sanctions provided for shall include the possibility of imposing recurring penalty payments in the event of non-compliance with a measure adopted pursuant to Articles 10 and 12.
The sanctions provided for shall be effective, proportionate and dissuasive.

Article 17
Exchange of information and correspondents

For the purpose of promoting cooperation, including the exchange of information, among Member States and between Member States and the Commission, each Member State shall designate one or more national correspondents for any question relating to the implementation of the measures provided for by this Directive. It shall communicate the details of the national correspondent or correspondents to the other Member States and the Commission.

Article 18
Reports

1. By 9 June 2021, the European Union Intellectual Property Office, in the context of the activities of the European Observatory on Infringements of Intellectual Property Rights, shall prepare an initial report on the litigation trends regarding the unlawful acquisition, use or disclosure of trade

secrets pursuant to the application of this Directive.

2. By 9 June 2022, the Commission shall draw up an intermediate report on the application of this Directive, and shall submit it to the European Parliament and to the Council. That report shall take due account of the report referred to in paragraph 1.

   The intermediate report shall examine, in particular, the possible effects of the application of this Directive on research and innovation, the mobility of employees and on the exercise of the right to freedom of expression and information.

3. By 9 June 2026, the Commission shall carry out an evaluation of the impact of this Directive and submit a report to the European Parliament and to the Council.

Article 19
Transposition

1. Member States shall bring into force the laws, regulations and administrative provisions necessary to comply with this Directive by 9 June 2018. They shall immediately communicate the text of those measures to the Commission.
   When Member States adopt those measures, they shall contain a reference to this Directive or be accompanied by such a reference on the occasion of their official publication. Member States shall determine how such reference is to be made.

2. Member States shall communicate to the Commission the text of the main provisions of national law which they adopt in the field covered by this Directive.

Article 20
Entry into force

This Directive shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union.

Article 21
Addressees

This Directive is addressed to the Member States.

Done at Strasbourg, 8 June 2016.

（参考和訳）

2016 年 6 月 8 日付の未公開ノウハウ及び事業情報（営業秘密）の違法取得、使用又は開示に対する保護に関する欧州議会及び理事会指令（EU）2016/943

第 I 章
目的及び適用範囲

第 1 条
目的及び適用範囲

1. 本指令は、営業秘密の違法な取得、使用又は開示に対する保護に関する規定を定めるものである。
   加盟国は、TFEU（欧州連合機能条約）の規定に従う限りにおいて、本指令が要求する水準を上回る、営業秘密の違法な取得、使用又は開示に対するより広範な保護を規定することができる。ただし、その場合においても、第 3 条、第 5 条、第 6 条、第 7 条第 1 項、第 8 条、第 9 条第 1 項第 2 段落、第 9 条第 3 項及び第 4 項、第 10 条第 2 項、第 11 条、第 13 条並びに第 15 条第 3 項の遵守が確保されなければならない。

2. 本指令は、以下の事項に影響を及ぼすものではない。
   (a) メディア報道の自由及び多元主義を含め、欧州基本権憲章に定める表現及び情報伝達の自由の権利行使。
   (b) 公益上の理由から、営業秘密を含む情報を公衆又は行政当局若しくは司法当局に対して、それらの機関の業務遂行のために開示することを営業秘密の保有者に求める又は開示を義務づける、EU 法又は国内法の適用。
   (c) EU 法又は国内法に定められた義務及び特権に従い、事業者から提出された情報を保持する EU の機関及び団体又は国内の公的機関が、当該情報を開示することを要求又は許容する、EU 法又は国内法の適用。
   (d) EU 法並びに国内法及び実務に従った、社会パートナーの自律性及び社会パートナーが労働協約を締結する権利。

3. 本指令のいかなる規定も、労働者の移動の自由を制限する根拠として解されてはならない。特に、当該移動の自由の行使に関連して、本指令は以下の事項の根拠となるものではない。
   (a) 第 2 条第 1 号に定義される営業秘密に該当しない情報について、労働者がこれを使用を制限すること。
   (b) 労働者が通常の雇用過程において正当に取得した経験及び技能の使用を制限する

こと。

(c) EU 法又は加盟国法に従って課される制限を除き、労働者の雇用契約に追加的な制限を課すこと。

第 2 条
定義

本指令においては、以下の定義を適用する。

(1) 「営業秘密」とは、次の全ての要件を満たす情報をいう。

(a) 当該情報が、単体として、又はその構成要素の正確な構成と組み立てにおいて、当該種別の情報を通常取り扱う者の間で一般に知られておらず、又は容易にアクセスできないという意味で秘密であること。

(b) 秘密性ゆえに、商業的価値を有していること。

(c) 情報を秘密に保つために、合法的に情報を管理している者によって、当該状況下で、合理的な措置が講じられていること。

(2) 「営業秘密の保有者」とは、営業秘密を適法に管理する自然人又は法人をいう。

(3) 「侵害者」とは、営業秘密を違法に取得、使用、又は開示する自然人又は法人をいう。

(4) 「侵害品」とは、そのデザイン、特性、機能、生産工程又は販売が、違法に取得、使用又は開示された営業秘密から実質的に利益を得ている製品をいう。

第 II 章
営業秘密の取得、使用及び開示

第 3 条
営業秘密の適法な取得、使用及び開示

1. 営業秘密の取得は、以下の方法により当該営業秘密が取得された場合には、適法なものとみなされる。

(a) 独自の発見又は創作。

(b) 公衆に提供された、又は情報取得者が適法に保有し、かつ営業秘密の取得を制限する法的に有効な義務を負っていない製品又は物について、その観察、研究、分解又は試験を行うこと。

(c) EU 法及び加盟国法並びに国内慣行に従って、労働者又は労働者代表が有する情

報及び協議を受ける権利の行使。

(d) 当該状況において誠実な商慣行に適合するその他の行為。

2. 営業秘密の取得、使用又は開示が、EU法又は加盟国法により要求され、又は認められる限りにおいては、当該取得、使用又は開示が適法なものとみなされる。

第4条
営業秘密の違法な取得、使用及び開示

1. 加盟国は、営業秘密の保有者が、その営業秘密の違法な取得、使用又は開示を防止し、又はこれに対する救済を得るために、本指令に定める措置、手続及び救済を申立てる権利を有することを確保しなければならない。

2. 営業秘密の保有者の同意なく営業秘密を取得する行為は、以下のいずれかによって行われた場合には、違法なものとみなされる。

(a) 営業秘密を含む、又はそこから営業秘密を推知することができる文書、物品、材料、物質若しくは電子ファイルであって、営業秘密の保有者の適法な管理下にあるものついて、無権限のアクセス、占有又は複製を行うこと。

(b) 当該状況において誠実な商慣行に反すると考えられるその他の行為。

3. 営業秘密の使用又は開示は、営業秘密の保有者の同意なく、かつ次のいずれかの条件に該当する者により行われた場合には、違法なものとみなされる。

(a) 営業秘密を違法に取得した者。

(b) 秘密保持契約又は営業秘密を開示しないその他の義務に違反した者。

(c) 営業秘密の使用を制限する契約上の義務又はその他の義務に違反した者。

4. 営業秘密の取得、使用又は開示は、当該取得、使用又は開示の時点において、当該者が、営業秘密が第 3 項の意味において違法に使用又は開示している別の者から直接又は間接に取得されたものであることを知っている、又は当該状況において知るべきである場合にも、違法なものとみなされる。

5. 侵害品の製造、提供、上市、又はそのための輸入、輸出若しくは保管は、当該行為者が、当該営業秘密が第 3 項の意味において違法に使用されたものであることを知っている、又は当該状況において知るべきである場合には、営業秘密の違法な使用とみなされる。

第 5 条
例外

加盟国は、当該営業秘密の取得、使用又は開示が、以下のいずれかの場合に該当する場合には、本指令に定める措置、手続及び救済の申立てが却下されることを確保しなければならない。

(a) メディアの報道の自由及び多元主義を含む、欧州基本権憲章に定める表現及び情報伝達の自由の権利行使。
(b) 公共の利益を保護する目的での、不正行為又は違法行為・活動の暴露。
(c) 労働者代表が、EU 法又は国内法に従い、その正当な職務遂行の一環として、その職務遂行に必要がある場合に、労働者から開示を受けること。
(d) EU 法又は国内法により認められた正当な利益を保護する目的での行為。

第 III 章
措置、手続及び救済

第 1 節
一般規定

第 6 条
一般的義務

1. 加盟国は、営業秘密の違法な取得、使用及び開示に対して民事上の救済を行使できるようにするために必要な措置、手続及び救済を定めなければならない。

2. 第 1 項に定める措置、手続及び救済は、以下の要件を満たさなければならない。
   (a) 公正かつ衡平であること。
   (b) 不必要に複雑、若しくは高額な、又は不合理な時間的制約若しくは不当な遅延を伴うものでないこと。
   (c) 効果的かつ抑止効果があること。

第 7 条
比例原則及び手続濫用

1. 本指令に定める措置、手続及び是正措置は、以下のように実施される必要がある。
   (a) 比例的であること。
   (b) EU 域内市場での正当な取引の障害とならないこと。

(c) 濫用に対する保護措置が講じられていること。

2. 加盟国は、営業秘密の違法な取得、使用又は開示に関する申立てが明らかに根拠を欠き、かつ申立人が濫用的又は不誠実により法的手続を開始したと認められる場合には、被申立人の申立てに基づき、加盟国法に定める適切な措置を管轄司法機関が適用できることを確保しなければならない。
当該措置には、必要に応じて、被申立人に対する損害賠償の付与、申立人に対する制裁、又は第 15 条にいう決定に関する情報の公表命令などが含まれうる。
加盟国は、第 1 段落にいう措置について、本案とは別の手続とすることができる。

第 8 条
時効期間

1. 加盟国は、本条に従い、本指令に基づく手段、手続及び是正措置の適用に関する実体的請求及び訴訟に適用される時効期間に関する規則を定めなければならない。
第 1 段落にいう規則は、時効期間の起算点、時効期間の長さ、及び時効期間が中断又は停止する事由を定めるものとする。

2. 時効期間は、6 年を超えてはならない。

第 9 条
訴訟手続における営業秘密の秘密保持

1. 加盟国は、営業秘密の違法な取得、使用又は開示に関する訴訟手続において、当事者、その弁護士その他代理人、裁判所職員、証人、専門家、及び当該訴訟手続に関与するその他の者、又は当該訴訟手続の一部を構成する文書にアクセスできる者が、利害関係人の正当な理由付けのある申立てに基づき管轄司法機関が秘密と認定した営業秘密又は営業秘密であると主張される情報について、当該手続への参加又は文書へのアクセスによって知り得た内容を使用し又は開示することを禁止する措置を確保しなければならない。
この点に関し、加盟国は、管轄司法機関が職権でこれらの措置を講じることを認めることもできる。
第 1 段落にいう義務は、訴訟手続が終了した後も、引き続き有効に存在するが、以下のいずれかの場合に消滅する。
(a) 終局判決により、営業秘密が、EU 営業秘密指令第 2 条第 1 号に定められた営業秘密の要件を満たさないことが判明した場合。
(b) 当該営業秘密が、通常その種の情報を扱う業界内部者の間で、一般的に知られる

ようになるか、容易にアクセスできるようになった場合。

2. 加盟国は、管轄司法機関が、申立て又は職権により、営業秘密の侵害に関する訴訟手続で使用又は参照された営業秘密の秘密性を保護するために必要な特定の措置を講じることができるよう確保しなければならない。
第 1 段落に定める措置には、少なくとも以下が含まれるものとする。
(a) 当事者、又は第三者によって提出された、営業秘密を含む文書について、その全部又は一部へのアクセスを、限定された人数に制限すること。
(b) 営業秘密が、開示される可能性がある審理及びその記録等へのアクセスを、限定された人数に制限すること。
(c) (a)及び(b)にいう限定された人数以外の者に対しては、営業秘密を含む部分が削除又はマスキングされた非機密版の判決文にアクセスできるようにすること。
第 2 段落(a)及び(b)にいうにいう限定された人数は、実効的救済及び公正な司法手続を受ける各当事者の権利を確保するために必要な最小限度を超えてはならず、少なくとも，各当事者につき少なくとも 1 名の自然人と、その弁護士又はその他の代理人を含めなければならない。

3. 第 2 項に規定する措置を決定し、かつその比例性の判断にあたっては、管轄司法機関は、実効的な救済及び公正な裁判を受ける権利を確保する必要性、当事者及び必要に応じて第三者の正当な利益、並びに当該措置の採否により当事者及び必要に応じて第三者に生じうる損害を考慮しなければならない。

4. 第 1 項、第 2 項又は第 3 項に基づいて行われる個人データの処理は、指令 95/46/EC に従って行われなければならない。

第 2 節
暫定的措置及び予防的措置

第 10 条
暫定的措置及び予防的措置

1. 加盟国は、営業秘密の保有者の申立てにより、管轄司法機関が、侵害が疑われる者に対して、以下の暫定的又は予防的措置のいずれかを命ずることができるよう確保しなければならない。
(a) 暫定的に、営業秘密の使用若しくは開示の停止、又は必要に応じてそれらの禁止。
(b) 侵害品の製造、提供、上市若しくは使用の禁止、又はそれらの目的のための侵害

品の輸入、輸出若しくは保管の禁止。

(c) 輸入品を含む、侵害の疑いのある物品について、その市場への参入又は流通を防止するための差押え又は引渡し。

2. 加盟国は、管轄司法機関が、第 1 項に規定する措置に代えて、営業秘密の違法な使用が疑われる行為を続けることを、営業秘密の保有者に対する補償を確保するための保証金の預託を条件として認めることができるよう確保しなければならない。なお、営業秘密の開示を、保証金の預託と引換えに認めることはできない。

第 11 条
申立ての条件及び保護措置

1. 加盟国は、第 10 条に規定する措置に関して、管轄司法機関が、申立人に対し、次の事項につき、十分な確実性をもって確認するために、合理的に利用可能と考えられる証拠の提出を求める権限を有することを確保しなければならない。

(a) 営業秘密が存在すること。

(b) 申立人が営業秘密の保有者であること。

(c) 当該営業秘密が違法に取得、使用又は開示されていること、又はその違法な取得、使用又は開示が差し迫っていること。

2. 加盟国は、当該申立ての認容又は却下について決定、並びにその比例性を判断するにあたり、管轄司法機関が、当該事件の具体的事情を考慮しなければならないことを確保しなければならない。その具体的事情には、必要に応じて、次の事項を含むものとする。

(a) 営業秘密の価値又はその他の特性。

(b) 営業秘密を保護するために講じられた措置。

(c) 営業秘密を取得、使用又は開示する際の被申立人の行為。

(d) 営業秘密の違法な使用又は開示の影響。

(e) 当事者の正当な利益及び措置の許否が、当事者に与える可能性のある影響。

(f) 第三者の正当な利益。

(g) 公共の公益。

(h) 基本的権利の保護。

3. 加盟国は、第 10 条に規定する措置が、以下のいずれかに該当する場合には、被申立人の申立てにより取り消される、又は効力を失うことを確保しなければならない。

(a) 申立人が、当該措置を命じた司法機関が加盟国法に基づき相当な期間内に管轄司法機関が定める合理的期間内に、又はそのような定めがない場合には 20 営業日又

は31暦日いずれか長い期間を超えない期間内に、当該事件の本案判断に至る法的手続を開始しない場合。

(b) 当該情報が、第2条第1号の要件が、被申立人に起因しない理由により満たさなくなった場合。

4. 加盟国は、管轄司法機関が、第10条に規定する措置を、被申立人及び必要に応じて当該措置の影響を受けるその他の者に対する損害の補償を確保することを目的として、申立人による十分な保証の提供又はこれと同等の担保を条件とすることができるよう確保しなければならない。

5. 第10条に定める措置が、第3項(a)に基づき取り消された場合、又は申立人の行為若しくは不作為により失効した場合、又は後に営業秘密の違法な取得、使用又は開示若しくはそのおそれが存在しなかったことが判明した場合には、管轄司法機関は、被申立人又は損害を被った第三者の申立てにより、申立人に対し、当該措置により生じた一切の損害について適切な補償を行うよう命ずる権限を有するものとする。
加盟国は、第1段落の補償の申立てを別個の法的手続で取り扱うことを定めることができる。

第3節
事件の本案に基づく措置

第12条
差止め及び是正措置

1. 加盟国は、事案の本案に関する司法判断において、営業秘密の違法な取得、使用又は開示があったと認定された場合、管轄司法機関が申立人の申立てに基づき、侵害者に対し以下の一以上の措置を命じることができるようにしなければならない。
(a) 営業秘密の使用若しくは開示の停止、又は必要に応じてその禁止。
(b) 侵害品の製造、提供、上市若しくは使用の禁止、又はこれらを目的とする侵害品の輸入、輸出若しくは保管の禁止。
(c) 侵害品に関する適切な是正措置の実施。
(d) 営業秘密を含む又はこれを具体化する文書、物品、材料、物質、電子ファイルの全部又は一部の破棄、又は、適切な場合には申立人への引渡し。

2. 第1項(c)に規定する是正措置には、以下の措置が含まれるものとする。
(a) 市場からの侵害品の回収。
(b) 侵害品の侵害性の除去。

(c) 侵害品の破棄、又は適切な場合、市場からの回収。ただし、その回収によって、当該営業秘密の保護を損なわないことを要する。

3. 加盟国は、市場からの侵害品の回収を命じるとき、管轄司法機関は、営業秘密の保有者の要求に応じて、その製品を、保有者、又は慈善団体に引渡すように命じることができる。

4. 管轄司法機関は、第 1 項(c)及び(d)に規定する措置を、特段の事情がない限り、侵害者の負担において実施するものとする。
これらの措置は、営業秘密の違法な取得、使用又は開示に起因して営業秘密の保有者に支払うべき損害賠償請求を妨げるものではない。

第 13 条
申立ての条件、保護措置及び代替措置

1. 加盟国は、第 12 条に規定する差止め及び是正措置の採用に関する申立てを審理し、その比例性を判断するにあたり、管轄司法機関が、当該事件の具体的状況を考慮に入れることを義務づけるものとし、これには、適切な場合、以下を含むものとする。
(a) 営業秘密の価値又はその他の特性。
(b) 営業秘密を保護するために講じられた措置。
(c) 営業秘密を取得、使用又は開示する際の侵害者の行為。
(d) 営業秘密の違法な使用又は開示の影響。
(e) 当事者の正当な利益及び措置の認否が、当事者に与える可能性のある影響。
(f) 第三者の正当な利益。
(g) 公共の公益。
(h) 基本的権利の保護。
管轄司法機関が、第 12 条第 1 項(a)及び(b)に規定する措置の期間を限定する場合、当該期間は、侵害者が営業秘密の違法な取得、使用又は開示により得た商業的又は経済的利益を失わせるのに、十分な期間でなければならない。

2. 加盟国は、第 12 条第 1 項(a)及び(b)に規定する措置について、当該情報が被申立人に直接又は間接に責に帰すことができない理由により第 2 条第 1 号の要件を満たさなくなった場合には、被申立人の申立てにより取消されるか、又は失効させるものとする。

3. 加盟国は、第 12 条に規定する措置の対象となる可能性のある者の申立てにより、次の各条件が全て満たされる場合には、管轄司法機関が、当該措置に代えて、被申立人か

ら申立人（被害者）への金銭的補償（pecuniary compensation）の支払いを命ずることができる旨を定めなければならない。

(a) 当該者は、使用又は開示の時点で、当該営業秘密が、違法に営業秘密を使用又は開示した者から入手されたものであることを知らずかつ知るべき理由もなかったこと。

(b) 措置の実施が、被申立人に不相当な不利益をもたらす可能性があること。

(c) 被申立人から申立人への金銭的補償により、合理的に、損失を補償することができること。

第12条第1項(a)及び(b)の措置に代えて金銭的補償が命じられる場合、当該補償額は、当該者が当該営業秘密の使用について許諾を求めた場合に支払うべきであったロイヤルティ又は料金を基礎として算定される額を上限とし、営業秘密の使用が禁止されうる期間分を相当するものとする。

第14条
損害賠償

1. 加盟国は、管轄司法機関が、被害者の申立てにより、営業秘密の違法な取得、使用又は開示を行っていたことを知っていた、又は当該状況下で知り得たはずである侵害者に対し、営業秘密の保有者が営業秘密の違法な取得、使用又は開示によって被った、実際の損害を補償するのに適切な損害賠償金の支払いを命じずることを確保しなければならない。

   加盟国は、従業員が故意によらず、雇用主の営業秘密の、違法な取得、使用又は開示に対する従業員の損害賠償責任を制限することができる。

2. 第 1 項の損害賠償額を算定するにあたり、管轄司法機関は、被害者が被った経済的損失（逸失利益を含む）、侵害者の得た不当利得、適切な場合には、経済的要素以外の事項、すなわち違法な取得、使用又は開示によって営業秘密の保有者に生じた精神的損害等を考慮に入れるものとする。

   管轄司法機関は、適切な場合には、侵害者が、当該営業秘密の使用許諾を受けたとすれば支払われるべきであったロイヤルティ等を基礎として、損害賠償額を算定し、損害賠償を命ずることができる。

第15条
司法の決定に関する公表

1. 加盟国は、営業秘密の違法な取得、使用又は開示において提起された法的手続において、申立人の申立てに基づき、かつ侵害者の費用負担により、当該決定に関する情報

の公表のための適切な措置（決定全文又はその一部の公表を含む）を命ずることが、管轄司法当局において可能となるよう確保しなければならない。

2. 第 1 項に規定する措置は、第 9 条に従って営業秘密の機密性を保持しなければならない。

3. 第 1 項に規定する措置を命ずるか否かの判断及びその比例性を評価するにあたり、管轄司法機関は、必要に応じて、営業秘密の価値、侵害者の行為、営業秘密の違法な使用又は開示が及ぼす影響、及び侵害者による将来の違法使用若しくは開示の可能性を考慮しなければならない。
また、管轄司法機関は、侵害者に関する情報が自然人を識別できるものであるかどうか、そしてその場合に、当該情報の公表が正当化されるかどうかを考慮しなければならない。特に、その措置が侵害者のプライバシー及び名誉に与えうる損害を考慮するものとする。

第 IV 章
制裁、報告及び最終規定

第 16 条
本指令違反に対する制裁

加盟国は、第 9 条、第 10 条及び第 12 条に基づき採用された措置に従わない、又は従うことを拒否する者に対し、管轄司法機関が制裁を科すことができるよう確保しなければならない。
当該制裁には、第 10 条及び第 12 条に基づき採用された措置に従わなかった場合に、再犯制裁金（recurring penalty payments）を課す可能性を含めるものとする。
制裁は、実効性、比例性及び抑止力を有するものでなければならない。

第 17 条
情報交換及び連絡担当者

加盟国間、及び加盟国と欧州委員会との間における情報交換を含む協力を促進する目的で、加盟国は、本指令により規定された措置の実施に関するあらゆる事項に対応するため、1 名以上の国内連絡担当者を指定指名するものとする。
各加盟国は、当該国内連絡担当者の詳細を、他の加盟国及び欧州委員会に通知しなければならない。

第 18 条
報告

1. 欧州連合知的財産庁は、知的財産権侵害に関する欧州オブザーバトリーの活動の一環として、2016 年 6 月 9 日までに、本指令の適用に基づく営業秘密の違法な取得、使用又は開示に関する訴訟の動向について、初期報告書を作成するものとする。

2. 欧州委員会は、2022 年 6 月 9 日までに、本指令の適用に関する中間報告書を作成し、これを欧州議会及び理事会に提出するものとする。当該報告書は、第 1 項にいう報告書を十分に考慮に入れるものとする。
中間報告書は、特に、本指令の適用が研究及びイノベーション、労働者の流動性、並びに表現及び情報の自由の行使に及ぼしうる影響を検討するものとする。

3. 欧州委員会は、2026 年 6 月 9 日までに、本指令の影響に関する評価を実施し、その報告書を欧州議会及び理事会に提出するものとする。

第 19 条
国内法への移行措置

1. 加盟国は、本指令を遵守するために必要な法律、規則及び行政上の規定を、2018 年 6 月 9 日までに施行しなければならない。加盟国は、これらの規定の文面を直ちに欧州委員会に通知するものとする。
加盟国がこれらの規定を採択する際には、当該規定には本指令への参照を含めるか、又はその公式公布の際にそのような参照を付さなければならない。加盟国は、当該参照の方法を定めるものとする。

2. 加盟国は、本指令の対象分野において制定した主要な国内法規定の文面を欧州委員会に通知しなければならない。

第 20 条
施行日

本指令は、欧州連合官報に公布された日の翌日から起算して 20 日目に発効する。

第 21 条
名宛人

本指令は、加盟国を名宛人とする。

ドイツ

Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG)

（原文）

Abschnitt 1

Allgemeines

§ 1 Anwendungsbereich

(1) Dieses Gesetz dient dem Schutz von Geschäftsgeheimnissen vor unerlaubter Erlangung, Nutzung und Offenlegung.

(2) Öffentlich-rechtliche Vorschriften zur Geheimhaltung, Erlangung, Nutzung oder Offenlegung von Geschäftsgeheimnissen gehen vor.

(3) Es bleiben unberührt:

1. der berufs- und strafrechtliche Schutz von Geschäftsgeheimnissen, deren unbefugte Offenbarung von § 203 des Strafgesetzbuches erfasst wird,
2. die Ausübung des Rechts der freien Meinungsäußerung und der Informationsfreiheit nach der Charta der Grundrechte der Europäischen Union (ABl. C 202 vom 7.6.2016, S. 389), einschließlich der Achtung der Freiheit und der Pluralität der Medien,
3. die Autonomie der Sozialpartner und ihr Recht, Kollektivverträge nach den bestehenden europäischen und nationalen Vorschriften abzuschließen,
4. die Rechte und Pflichten aus dem Arbeitsverhältnis und die Rechte der Arbeitnehmervertretungen.

§ 2 Begriffsbestimmungen

Im Sinne dieses Gesetzes ist

1. Geschäftsgeheimnis

   eine Information

   a) die weder insgesamt noch in der genauen Anordnung und Zusammensetzung ihrer Bestandteile den Personen in den Kreisen, die üblicherweise mit dieser Art von Informationen umgehen, allgemein bekannt oder ohne Weiteres zugänglich ist und daher von wirtschaftlichem Wert ist und

   b) die Gegenstand von den Umständen nach angemessenen Geheimhaltungsmaßnahmen durch ihren rechtmäßigen Inhaber ist und

   c) bei der ein berechtigtes Interesse an der Geheimhaltung besteht;

2. Inhaber eines Geschäftsgeheimnisses

   jede natürliche oder juristische Person, die die rechtmäßige Kontrolle über ein Geschäftsgeheimnis hat;

3. Rechtsverletzer

   jede natürliche oder juristische Person, die entgegen § 4 ein Geschäftsgeheimnis

rechtswidrig erlangt, nutzt oder offenlegt; Rechtsverletzer ist nicht, wer sich auf eine Ausnahme nach § 5 berufen kann;

4. rechtsverletzendes Produkt

   ein Produkt, dessen Konzeption, Merkmale, Funktionsweise, Herstellungsprozess oder Marketing in erheblichem Umfang auf einem rechtswidrig erlangten, genutzten oder offengelegten Geschäftsgeheimnis beruht.

§ 3 Erlaubte Handlungen

(1) Ein Geschäftsgeheimnis darf insbesondere erlangt werden durch

1. eine eigenständige Entdeckung oder Schöpfung;

2. ein Beobachten, Untersuchen, Rückbauen oder Testen eines Produkts oder Gegenstands, das oder der

   a) öffentlich verfügbar gemacht wurde oder

   b) sich im rechtmäßigen Besitz des Beobachtenden, Untersuchenden, Rückbauenden oder Testenden befindet und dieser keiner Pflicht zur Beschränkung der Erlangung des Geschäftsgeheimnisses unterliegt;

3. ein Ausüben von Informations- und Anhörungsrechten der Arbeitnehmer oder Mitwirkungs- und Mitbestimmungsrechte der Arbeitnehmervertretung.

(2) Ein Geschäftsgeheimnis darf erlangt, genutzt oder offengelegt werden, wenn dies durch Gesetz, aufgrund eines Gesetzes oder durch Rechtsgeschäft gestattet ist.

§ 4 Handlungsverbote

(1) Ein Geschäftsgeheimnis darf nicht erlangt werden durch

1. unbefugten Zugang zu, unbefugte Aneignung oder unbefugtes Kopieren von Dokumenten, Gegenständen, Materialien, Stoffen oder elektronischen Dateien, die der rechtmäßigen Kontrolle des Inhabers des Geschäftsgeheimnisses unterliegen und die das Geschäftsgeheimnis enthalten oder aus denen sich das Geschäftsgeheimnis ableiten lässt, oder

2. jedes sonstige Verhalten, das unter den jeweiligen Umständen nicht dem Grundsatz von Treu und Glauben unter Berücksichtigung der anständigen Marktgepflogenheit entspricht.

(2) Ein Geschäftsgeheimnis darf nicht nutzen oder offenlegen, wer

1. das Geschäftsgeheimnis durch eine eigene Handlung nach Absatz 1

   a) Nummer 1 oder

   b) Nummer 2

   erlangt hat,

2. gegen eine Verpflichtung zur Beschränkung der Nutzung des Geschäftsgeheimnisses verstößt oder

3. gegen eine Verpflichtung verstößt, das Geschäftsgeheimnis nicht offenzulegen.

(3) Ein Geschäftsgeheimnis darf nicht erlangen, nutzen oder offenlegen, wer das Geschäftsgeheimnis über eine andere Person erlangt hat und zum Zeitpunkt der Erlangung, Nutzung oder Offenlegung weiß oder wissen müsste, dass diese das Geschäftsgeheimnis

entgegen Absatz 2 genutzt oder offengelegt hat. Das gilt insbesondere, wenn die Nutzung in der Herstellung, dem Anbieten, dem Inverkehrbringen oder der Einfuhr, der Ausfuhr oder der Lagerung für diese Zwecke von rechtsverletzenden Produkten besteht.

§ 5 Ausnahmen

Die Erlangung, die Nutzung oder die Offenlegung eines Geschäftsgeheimnisses fällt nicht unter die Verbote des § 4, wenn dies zum Schutz eines berechtigten Interesses erfolgt, insbesondere

1. zur Ausübung des Rechts der freien Meinungsäußerung und der Informationsfreiheit, einschließlich der Achtung der Freiheit und der Pluralität der Medien;
2. zur Aufdeckung einer rechtswidrigen Handlung oder eines beruflichen oder sonstigen Fehlverhaltens, wenn die Erlangung, Nutzung oder Offenlegung geeignet ist, das allgemeine öffentliche Interesse zu schützen;
3. im Rahmen der Offenlegung durch Arbeitnehmer gegenüber der Arbeitnehmervertretung, wenn dies erforderlich ist, damit die Arbeitnehmervertretung ihre Aufgaben erfüllen kann.

Abschnitt 2

Ansprüche bei Rechtsverletzungen

§ 6 Beseitigung und Unterlassung

Der Inhaber des Geschäftsgeheimnisses kann den Rechtsverletzer auf Beseitigung der Beeinträchtigung und bei Wiederholungsgefahr auch auf Unterlassung in Anspruch nehmen. Der Anspruch auf Unterlassung besteht auch dann, wenn eine Rechtsverletzung erstmalig droht.

§ 7 Vernichtung; Herausgabe; Rückruf; Entfernung und Rücknahme vom Markt

Der Inhaber des Geschäftsgeheimnisses kann den Rechtsverletzer auch in Anspruch nehmen auf

1. Vernichtung oder Herausgabe der im Besitz oder Eigentum des Rechtsverletzers stehenden Dokumente, Gegenstände, Materialien, Stoffe oder elektronischen Dateien, die das Geschäftsgeheimnis enthalten oder verkörpern,
2. Rückruf des rechtsverletzenden Produkts,
3. dauerhafte Entfernung der rechtsverletzenden Produkte aus den Vertriebswegen,
4. Vernichtung der rechtsverletzenden Produkte oder
5. Rücknahme der rechtsverletzenden Produkte vom Markt, wenn der Schutz des Geschäftsgeheimnisses hierdurch nicht beeinträchtigt wird.

§ 8 Auskunft über rechtsverletzende Produkte; Schadensersatz bei Verletzung der Auskunftspflicht

(1) Der Inhaber des Geschäftsgeheimnisses kann vom Rechtsverletzer Auskunft über Folgendes verlangen:

1. Name und Anschrift der Hersteller, Lieferanten und anderer Vorbesitzer der rechtsverletzenden Produkte sowie der gewerblichen Abnehmer und Verkaufsstellen, für die sie bestimmt waren,

2. die Menge der hergestellten, bestellten, ausgelieferten oder erhaltenen rechtsverletzenden Produkte sowie über die Kaufpreise,

3. diejenigen im Besitz oder Eigentum des Rechtsverletzers stehenden Dokumente, Gegenstände, Materialien, Stoffe oder elektronischen Dateien, die das Geschäftsgeheimnis enthalten oder verkörpern, und

4. die Person, von der sie das Geschäftsgeheimnis erlangt haben und der gegenüber sie es offenbart haben.

(2) Erteilt der Rechtsverletzer vorsätzlich oder grob fahrlässig die Auskunft nicht, verspätet, falsch oder unvollständig, ist er dem Inhaber des Geschäftsgeheimnisses zum Ersatz des daraus entstehenden Schadens verpflichtet.

§ 9 Anspruchsausschluss bei Unverhältnismäßigkeit

Die Ansprüche nach den §§ 6 bis 8 Absatz 1 sind ausgeschlossen, wenn die Erfüllung im Einzelfall unverhältnismäßig wäre, unter Berücksichtigung insbesondere

1. des Wertes oder eines anderen spezifischen Merkmals des Geschäftsgeheimnisses,

2. der getroffenen Geheimhaltungsmaßnahmen,

3. des Verhaltens des Rechtsverletzers bei Erlangung, Nutzung oder Offenlegung des Geschäftsgeheimnisses,

4. der Folgen der rechtswidrigen Nutzung oder Offenlegung des Geschäftsgeheimnisses,

5. der berechtigten Interessen des Inhabers des Geschäftsgeheimnisses und des Rechtsverletzers sowie der Auswirkungen, die die Erfüllung der Ansprüche für beide haben könnte,

6. der berechtigten Interessen Dritter oder

7. des öffentlichen Interesses.

§ 10 Haftung des Rechtsverletzers

(1) Ein Rechtsverletzer, der vorsätzlich oder fahrlässig handelt, ist dem Inhaber des Geschäftsgeheimnisses zum Ersatz des daraus entstehenden Schadens verpflichtet. § 619a des Bürgerlichen Gesetzbuchs bleibt unberührt.

(2) Bei der Bemessung des Schadensersatzes kann auch der Gewinn, den der Rechtsverletzer durch die Verletzung des Rechts erzielt hat, berücksichtigt werden. Der Schadensersatzanspruch kann auch auf der Grundlage des Betrages bestimmt werden, den der Rechtsverletzer als angemessene Vergütung hätte entrichten müssen, wenn er die Zustimmung zur Erlangung, Nutzung oder Offenlegung des Geschäftsgeheimnisses eingeholt hätte.

(3) Der Inhaber des Geschäftsgeheimnisses kann auch wegen des Schadens, der nicht Vermögensschaden ist, von dem Rechtsverletzer eine Entschädigung in Geld verlangen, soweit dies der Billigkeit entspricht.

§ 11 Abfindung in Geld

(1) Ein Rechtsverletzer, der weder vorsätzlich noch fahrlässig gehandelt hat, kann zur Abwendung der Ansprüche nach den §§ 6 oder 7 den Inhaber des Geschäftsgeheimnisses in Geld abfinden, wenn dem Rechtsverletzer durch die Erfüllung der Ansprüche ein unverhältnismäßig großer Nachteil entstehen würde und wenn die Abfindung in Geld als angemessen erscheint.

(2) Die Höhe der Abfindung in Geld bemisst sich nach der Vergütung, die im Falle einer

vertraglichen Einräumung des Nutzungsrechts angemessen wäre. Sie darf den Betrag nicht übersteigen, der einer Vergütung im Sinne von Satz 1 für die Länge des Zeitraums entspricht, in dem dem Inhaber des Geschäftsgeheimnisses ein Unterlassungsanspruch zusteht.

§ 12 Haftung des Inhabers eines Unternehmens

Ist der Rechtsverletzer Beschäftigter oder Beauftragter eines Unternehmens, so hat der Inhaber des Geschäftsgeheimnisses die Ansprüche nach den §§ 6 bis 8 auch gegen den Inhaber des Unternehmens. Für den Anspruch nach § 8 Absatz 2 gilt dies nur, wenn der Inhaber des Unternehmens vorsätzlich oder grob fahrlässig die Auskunft nicht, verspätet, falsch oder unvollständig erteilt hat.

§ 13 Herausgabeanspruch nach Eintritt der Verjährung

Hat der Rechtsverletzer ein Geschäftsgeheimnis vorsätzlich oder fahrlässig erlangt, offengelegt oder genutzt und durch diese Verletzung eines Geschäftsgeheimnisses auf Kosten des Inhabers des Geschäftsgeheimnisses etwas erlangt, so ist er auch nach Eintritt der Verjährung des Schadensersatzanspruchs nach § 10 zur Herausgabe nach den Vorschriften des Bürgerlichen Gesetzbuchs über die Herausgabe einer ungerechtfertigten Bereicherung verpflichtet. Dieser Anspruch verjährt sechs Jahre nach seiner Entstehung.

§ 14 Missbrauchsverbot

Die Geltendmachung der Ansprüche nach diesem Gesetz ist unzulässig, wenn sie unter Berücksichtigung der gesamten Umstände missbräuchlich ist. Bei missbräuchlicher Geltendmachung kann der Anspruchsgegner Ersatz der für seine Rechtsverteidigung erforderlichen Aufwendungen verlangen. Weitergehende Ersatzansprüche bleiben unberührt.

Abschnitt 3

Verfahren in Geschäftsgeheimnisstreitsachen

§ 15 Sachliche und örtliche Zuständigkeit; Verordnungsermächtigung

(1) Für Klagen vor den ordentlichen Gerichten, durch die Ansprüche nach diesem Gesetz geltend gemacht werden, sind die Landgerichte ohne Rücksicht auf den Streitwert ausschließlich zuständig.

(2) Für Klagen nach Absatz 1 ist das Gericht ausschließlich zuständig, in dessen Bezirk der Beklagte seinen allgemeinen Gerichtsstand hat. Hat der Beklagte im Inland keinen allgemeinen Gerichtsstand, ist nur das Gericht zuständig, in dessen Bezirk die Handlung begangen worden ist.

(3) Die Landesregierungen werden ermächtigt, durch Rechtsverordnung einem Landgericht die Klagen nach Absatz 1 der Bezirke mehrerer Landgerichte zuzuweisen. Die Landesregierungen können diese Ermächtigung durch Rechtsverordnung auf die Landesjustizverwaltungen übertragen. Die Länder können außerdem durch Vereinbarung die den Gerichten eines Landes obliegenden Klagen nach Absatz 1 insgesamt oder teilweise dem zuständigen Gericht eines anderen Landes übertragen.

§ 16 Geheimhaltung

(1) Bei Klagen, durch die Ansprüche nach diesem Gesetz geltend gemacht werden (Geschäftsgeheimnisstreitsachen) kann das Gericht der Hauptsache auf Antrag einer Partei

streitgegenständliche Informationen ganz oder teilweise als geheimhaltungsbedürftig einstufen, wenn diese ein Geschäftsgeheimnis sein können.

(2) Die Parteien, ihre Prozessvertreter, Zeugen, Sachverständige, sonstige Vertreter und alle sonstigen Personen, die an Geschäftsgeheimnisstreitsachen beteiligt sind oder die Zugang zu Dokumenten eines solchen Verfahrens haben, müssen als geheimhaltungsbedürftig eingestufte Informationen vertraulich behandeln und dürfen diese außerhalb eines gerichtlichen Verfahrens nicht nutzen oder offenlegen, es sei denn, dass sie von diesen außerhalb des Verfahrens Kenntnis erlangt haben.

(3) Wenn das Gericht eine Entscheidung nach Absatz 1 trifft, darf Dritten, die ein Recht auf Akteneinsicht haben, nur ein Akteninhalt zur Verfügung gestellt werden, in dem die Geschäftsgeheimnisse enthaltenden Ausführungen unkenntlich gemacht wurden.

§ 17 Ordnungsmittel

Das Gericht der Hauptsache kann auf Antrag einer Partei bei Zuwiderhandlungen gegen die Verpflichtungen nach § 16 Absatz 2 ein Ordnungsgeld bis zu 100 000 Euro oder Ordnungshaft bis zu sechs Monaten festsetzen und sofort vollstrecken. Bei der Festsetzung von Ordnungsgeld ist zugleich für den Fall, dass dieses nicht beigetrieben werden kann, zu bestimmen, in welchem Maße Ordnungshaft an seine Stelle tritt. Die Beschwerde gegen ein nach Satz 1 verhängtes Ordnungsmittel entfaltet aufschiebende Wirkung.

§ 18 Geheimhaltung nach Abschluss des Verfahrens

Die Verpflichtungen nach § 16 Absatz 2 bestehen auch nach Abschluss des gerichtlichen Verfahrens fort. Dies gilt nicht, wenn das Gericht der Hauptsache das Vorliegen des streitgegenständlichen Geschäftsgeheimnisses durch rechtskräftiges Urteil verneint hat oder sobald die streitgegenständlichen Informationen für Personen in den Kreisen, die üblicherweise mit solchen Informationen umgehen, bekannt oder ohne Weiteres zugänglich werden.

Nichtamtliches Inhaltsverzeichnis

§ 19 Weitere gerichtliche Beschränkungen

(1) Zusätzlich zu § 16 Absatz 1 beschränkt das Gericht der Hauptsache zur Wahrung von Geschäftsgeheimnissen auf Antrag einer Partei den Zugang ganz oder teilweise auf eine bestimmte Anzahl von zuverlässigen Personen

1. zu von den Parteien oder Dritten eingereichten oder vorgelegten Dokumenten, die Geschäftsgeheimnisse enthalten können, oder
2. zur mündlichen Verhandlung, bei der Geschäftsgeheimnisse offengelegt werden könnten, und zu der Aufzeichnung oder dem Protokoll der mündlichen Verhandlung.

Dies gilt nur, soweit nach Abwägung aller Umstände das Geheimhaltungsinteresse das Recht der Beteiligten auf rechtliches Gehör auch unter Beachtung ihres Rechts auf effektiven Rechtsschutz und ein faires Verfahren übersteigt. Es ist jeweils mindestens einer natürlichen Person jeder Partei und ihren Prozessvertretern oder sonstigen Vertretern Zugang zu gewähren. Im Übrigen bestimmt das Gericht nach freiem Ermessen, welche Anordnungen zur Erreichung des Zwecks erforderlich sind.

(2) Wenn das Gericht Beschränkungen nach Absatz 1 Satz 1 trifft,

1. kann die Öffentlichkeit auf Antrag von der mündlichen Verhandlung ausgeschlossen werden und
2. gilt § 16 Absatz 3 für nicht zugelassene Personen.

(3) Die §§ 16 bis 19 Absatz 1 und 2 gelten entsprechend im Verfahren der Zwangsvollstreckung, wenn das Gericht der Hauptsache Informationen nach § 16 Absatz 1 als geheimhaltungsbedürftig eingestuft oder zusätzliche Beschränkungen nach Absatz 1 Satz 1 getroffen hat.

§ 20 Verfahren bei Maßnahmen nach den §§ 16 bis 19

(1) Das Gericht der Hauptsache kann eine Beschränkung nach § 16 Absatz 1 und § 19 Absatz 1 ab Anhängigkeit des Rechtsstreits anordnen.

(2) Die andere Partei ist spätestens nach Anordnung der Maßnahme vom Gericht zu hören. Das Gericht kann die Maßnahmen nach Anhörung der Parteien aufheben oder abändern.

(3) Die den Antrag nach § 16 Absatz 1 oder § 19 Absatz 1 stellende Partei muss glaubhaft machen, dass es sich bei der streitgegenständlichen Information um ein Geschäftsgeheimnis handelt.

(4) Werden mit dem Antrag oder nach einer Anordnung nach § 16 Absatz 1 oder einer Anordnung nach § 19 Absatz 1 Satz 1 Nummer 1 Schriftstücke und sonstige Unterlagen eingereicht oder vorgelegt, muss die den Antrag stellende Partei diejenigen Ausführungen kennzeichnen, die nach ihrem Vorbringen Geschäftsgeheimnisse enthalten. Im Fall des § 19 Absatz 1 Satz 1 Nummer 1 muss sie zusätzlich eine Fassung ohne Preisgabe von Geschäftsgeheimnissen vorlegen, die eingesehen werden kann. Wird keine solche um die Geschäftsgeheimnisse reduzierte Fassung vorgelegt, kann das Gericht von der Zustimmung zur Einsichtnahme ausgehen, es sei denn, ihm sind besondere Umstände bekannt, die eine solche Vermutung nicht rechtfertigen.

(5) Das Gericht entscheidet über den Antrag durch Beschluss. Gibt es dem Antrag statt, hat es die Beteiligten auf die Wirkung der Anordnung nach § 16 Absatz 2 und § 18 und Folgen der Zuwiderhandlung nach § 17 hinzuweisen. Beabsichtigt das Gericht die Zurückweisung des Antrags, hat es die den Antrag stellende Partei darauf und auf die Gründe hierfür hinzuweisen und ihr binnen einer zu bestimmenden Frist Gelegenheit zur Stellungnahme zu geben. Die Einstufung als geheimhaltungsbedürftig nach § 16 Absatz 1 und die Anordnung der Beschränkung nach § 19 Absatz 1 können nur gemeinsam mit dem Rechtsmittel in der Hauptsache angefochten werden. Im Übrigen findet die sofortige Beschwerde statt.

(6) Gericht der Hauptsache im Sinne dieses Abschnitts ist

1. das Gericht des ersten Rechtszuges oder
2. das Berufungsgericht, wenn die Hauptsache in der Berufungsinstanz anhängig ist.

§ 21 Bekanntmachung des Urteils

(1) Der obsiegenden Partei einer Geschäftsgeheimnisstreitsache kann auf Antrag in der Urteilsformel die Befugnis zugesprochen werden, das Urteil oder Informationen über das Urteil auf Kosten der unterliegenden Partei öffentlich bekannt zu machen, wenn die obsiegende Partei hierfür ein berechtigtes Interesse darlegt. Form und Umfang der öffentlichen Bekanntmachung werden unter Berücksichtigung der berechtigten Interessen der im Urteil genannten Personen in der Urteilsformel bestimmt.

(2) Bei den Entscheidungen über die öffentliche Bekanntmachung nach Absatz 1 Satz 1 ist insbesondere zu berücksichtigen:

1. der Wert des Geschäftsgeheimnisses,
2. das Verhalten des Rechtsverletzers bei Erlangung, Nutzung oder Offenlegung des Geschäftsgeheimnisses,
3. die Folgen der rechtswidrigen Nutzung oder Offenlegung des Geschäftsgeheimnisses und

4. die Wahrscheinlichkeit einer weiteren rechtswidrigen Nutzung oder Offenlegung des Geschäftsgeheimnisses durch den Rechtsverletzer.

(3) Das Urteil darf erst nach Rechtskraft bekannt gemacht werden, es sei denn, das Gericht bestimmt etwas anderes.

§ 22 Streitwertbegünstigung

(1) Macht bei Geschäftsgeheimnisstreitsachen eine Partei glaubhaft, dass die Belastung mit den Prozesskosten nach dem vollen Streitwert ihre wirtschaftliche Lage erheblich gefährden würde, so kann das Gericht auf ihren Antrag anordnen, dass die Verpflichtung dieser Partei zur Zahlung von Gerichtskosten sich nach dem ihrer Wirtschaftslage angepassten Teil des Streitwerts bemisst.

(2) Die Anordnung nach Absatz 1 bewirkt auch, dass

1. die begünstigte Partei die Gebühren ihres Rechtsanwalts ebenfalls nur nach diesem Teil des Streitwerts zu entrichten hat,
2. die begünstigte Partei, soweit ihr Kosten des Rechtsstreits auferlegt werden oder soweit sie diese übernimmt, die von dem Gegner entrichteten Gerichtsgebühren und die Gebühren seines Rechtsanwalts nur nach diesem Teil des Streitwerts zu erstatten hat und
3. der Rechtsanwalt der begünstigten Partei seine Gebühren von dem Gegner nach dem für diesen geltenden Streitwert beitreiben kann, soweit die außergerichtlichen Kosten dem Gegner auferlegt oder von ihm übernommen werden.

(3) Der Antrag nach Absatz 1 ist vor der Verhandlung zur Hauptsache zu stellen. Danach ist er nur zulässig, wenn der angenommene oder festgesetzte Streitwert durch das Gericht heraufgesetzt wird. Der Antrag kann vor der Geschäftsstelle des Gerichts zur Niederschrift erklärt werden. Vor der Entscheidung über den Antrag ist der Gegner zu hören.

Abschnitt 4

Strafvorschriften

§ 23 Verletzung von Geschäftsgeheimnissen

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber eines Unternehmens Schaden zuzufügen,

1. entgegen § 4 Absatz 1 Nummer 1 ein Geschäftsgeheimnis erlangt,
2. entgegen § 4 Absatz 2 Nummer 1 Buchstabe a ein Geschäftsgeheimnis nutzt oder offenlegt oder
3. entgegen § 4 Absatz 2 Nummer 3 als eine bei einem Unternehmen beschäftigte Person ein Geschäftsgeheimnis, das ihr im Rahmen des Beschäftigungsverhältnisses anvertraut worden oder zugänglich geworden ist, während der Geltungsdauer des Beschäftigungsverhältnisses offenlegt.

(2) Ebenso wird bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs, aus Eigennutz, zugunsten eines Dritten oder in der Absicht, dem Inhaber eines Unternehmens Schaden zuzufügen, ein Geschäftsgeheimnis nutzt oder offenlegt, das er durch eine fremde Handlung nach Absatz 1 Nummer 2 oder Nummer 3 erlangt hat.

(3) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer zur Förderung des eigenen oder fremden Wettbewerbs oder aus Eigennutz entgegen § 4 Absatz 2 Nummer 2 oder

Nummer 3 ein Geschäftsgeheimnis, das eine ihm im geschäftlichen Verkehr anvertraute geheime Vorlage oder Vorschrift technischer Art ist, nutzt oder offenlegt.

(4) Mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe wird bestraft, wer

1. in den Fälle d n des Absatzes 1 oder des Absatzes 2 gewerbsmäßig handelt,
2. in den Fällen des Absatzes 1 Nummer 2 oder Nummer 3 oder des Absatzes 2 bei der Offenlegung weiß, dass das Geschäftsgeheimnis im Ausland genutzt werden soll, oder
3. in den Fällen des Absatzes 1 Nummer 2 oder des Absatzes 2 das Geschäftsgeheimnis im Ausland nutzt.

(5) Der Versuch ist strafbar.

(6) Beihilfehandlungen einer in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Person sind nicht rechtswidrig, wenn sie sich auf die Entgegennahme, Auswertung oder Veröffentlichung des Geschäftsgeheimnisses beschränken.

(7) § 5 Nummer 7 des Strafgesetzbuches gilt entsprechend. Die §§ 30 und 31 des Strafgesetzbuches gelten entsprechend, wenn der Täter zur Förderung des eigenen oder fremden Wettbewerbs oder aus Eigennutz handelt.

(8) Die Tat wird nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

（参考和訳）

第 1 節 総則

第 1 条 適用範囲

(1) 本法は、営業秘密の不正な取得、使用及び開示に関する保護を目的とする。

(2) 営業秘密の秘密保持、取得、使用又は開示に関する公法上の規定を優先する。

(3) 次の事項は影響を受けない。

1. ドイツ刑法第 203 条により不正な開示が処罰対象となる営業秘密についての職業上の法的保護及び刑事法上の保護
2. 欧州連合基本権憲章（OJ C 202、2016 年 6 月 7 日、389 頁）に基づく言論及び情報の自由（メディアの自由及び多元主義の尊重を含む）の権利行使
3. 社会パートナー（Sozialpartner）の自律及び既存の EU 法及び国内法に基づく労働協約を締結する権利
4. 雇用関係から生じる権利義務及び労働者代表の権利

第 2 条 定義

本法において、

1. 営業秘密とは、
   （次の要件を充足する）情報をいう
   a) 全体において、又はそのコンポーネントの正確な構成及び組み合わせにおいて、この種の情報を通常扱う者にとって一般に知られておらず、又は容易にアクセス可能でなく、そのことにより経済的価値を有するもの
   b) 当該情報を適法に管理する者によって、その状況に応じて秘密として保持するための合理的な措置が講じられているもの
   c) 秘密性を保持することについて、正当な利益があるもの
2. 営業秘密の保有者とは、
   営業秘密を適法に管理している自然人又は法人をいう
3. 侵害者とは、
   第4条に違反して営業秘密を違法に取得、利用又は開示する自然人又は法人をいう。第5条の例外を主張できる者は、侵害者とはみなされない。
4. 侵害品とは、
   その設計、特徴、機能、製造プロセス又はマーケティングが、違法に取得、使用又は開示された営業秘密から実質的な利益を得ている物品をいう

第 3 条 許容される行為

(1) 営業秘密は、特に次の方法によって取得することができる。

1. 独自の発見又は創作
2. 製品又は物品の観察、研究、分解又は試験
   a) 一般に公開されたもの、若しくは
   b) 観察者、研究者、分解者又は試験者が適法に保有しており、かつ営業秘密の取得を制限する義務を負っていない場合
3. 労働者の情報及び協議に関する権利、又は労働者代表の参加及び共同決定に関する権利の行使

(2) 営業秘密は、法律によって、法律に基づいて又は法律行為により許可されている場合、取得、使用又は開示することができる。

第 4 条 禁止される行為

(1) 営業秘密は、次の方法によって取得してはならない

1. 営業秘密の保有者の適法な管理下にあり、営業秘密を含む、又は営業秘密が引き出される文書、物、原料、材料又は電磁的情報への無権限のアクセス、領得又は複製すること
2. その都度の状況下において、公正な商慣習を考慮して、信義誠実の原則に反するあらゆる行為

(2) 次のいずれかに該当する者は、営業秘密を使用又は開示してはならない。

1. 自己の行為により、第 1 項
   a) 第 1 号又は
   b) 第 2 号によって
   営業秘密を取得する場合
2. 営業秘密の使用を制限する義務に違反する場合
3. 営業秘密を開示しない義務に違反する場合

(3) 第三者を通じて営業秘密を取得した者は、その取得、使用又は開示の時点で、当該第三者が第 2 項に違反して営業秘密を使用又は開示したことを知っていた、又は知るべきであった場合には、営業秘密を取得、使用又は開示してはならない。これは、特にその使用が、侵害品の製造、提供、上市又はこれらの目的での輸出入若しくは保管を内容とする場合に適用される。

第 5 条 例外

営業秘密の取得、使用又は開示が、正当な利益を保護する目的で行われる場合には、第4条の禁止規定の適用を受けない。特に、次の場合がこれに該当する。

1. 言論及び情報の自由の権利行使（メディアの自由及び多元主義の尊重を含む）

2. 取得、使用又は開示が一般的な公共の利益の保護に資する場合における、違法行為又は不正行為の暴露
3. 労働者代表がその任務を果たしうるのに必要とされる場合に労働者代表に対する労働者による開示

第 2 節 権利侵害に関する請求

第 6 条 侵害の除去及び差止

営業秘密の保有者は、侵害者に対し侵害の除去を請求する権利を有し、再発のおそれがある場合又は侵害のおそれが初めて生じる場合には、差止を請求する権利を有する。

第 7 条 破棄、引渡し、回収、市場からの除去・撤去

営業秘密の保有者は、侵害者に対して、次の事項を請求する権利を有する。

1. 侵害者が占有又は所有する営業秘密を含む、又は営業秘密を反映する文書、物品、資料、素材、電子ファイルの破棄又は引渡し
2. 侵害品の回収
3. 販売経路からの侵害品の恒久的な除去
4. 侵害品の廃棄
5. 営業秘密の保護がこれにより侵害されない場合に限り、侵害品の市場からの撤去

第 8 条 侵害品に関する情報提供及び情報提供義務違反に対する損害賠償

(1) 営業秘密の保有者は、侵害者に対して、次の事項についての情報の提供を請求することができる。
   1. 侵害品の製造者、供給者、その他の前保有者の名称及び住所、並びに当該侵害品の供給先として予定されていた商業上の顧客及び販売先の名称及び住所
   2. 製造、注文、供給又は受領された侵害品の数量及び購入価格
   3. 侵害者が占有又は所有している営業秘密を含む、又は営業秘密を反映する文書、物品、材料、物質、電子ファイル
   4. 侵害者が営業秘密を取得した相手方及び当該営業秘密を開示した相手方
(2) 侵害者が故意又は重大な過失により、情報を提供しない場合、又は情報の提供を遅延させる、誤った情報を提供する、若しくは不完全な情報を提供する場合、侵害者は、営業秘密の保有者に対し、その結果生じた損害について賠償する義務を負う。

第 9 条 不均衡の場合における請求の除外

第6条から第8条第1項に基づく請求は、個々の事案においてその履行が不均衡となる場合には、行使することができない。この判断にあたっては、特に次の事項を考慮するものとする。

1. 営業秘密の価値又はその他の特定の性質
2. 秘密保持のために講じられた措置
3. 営業秘密の取得、使用又は開示に際する侵害者の行為
4. 営業秘密の違法な使用又は開示の結果
5. 営業秘密の保有者及び侵害者の正当な利益並びに請求の履行が双方に及ぼしうる影響
6. 第三者の正当な利益
7. 公益

第 10 条 権利侵害者の責任

(1) 故意又は過失により権利を侵害した者は、営業秘密の保有者に、その侵害によって生じた損害について賠償する義務を負う。ドイツ民法第 619a 条の規定は、これによって影響を受けない。

(2) 損害額の算定にあたっては、侵害者が権利侵害によって得た利益も考慮に入れることができる。損害賠償の請求額は、侵害者が営業秘密の取得、使用又は開示について同意を得ていた場合に支払うべきであった適切な対価の額に基づいて定めることもできる。

(3) 営業秘密の保有者は、財産的損害以外の損害についても、衡平に照らして相当と認められる場合には、侵害者に対して金銭による補償を請求することができる。

第 11 条 金銭による補償

(1) 故意又は過失による行為ではない侵害者は、第 6 条又は第 7 条に基づく請求を回避するために、当該請求の履行により不均衡な不利益を被るおそれがあり、かつ金銭による補償が相当と認められる場合には、営業秘密の保有者に金銭による補償を行うことができる。

(2) 金銭による補償の額は、契約上の使用権が付与された場合に相当と認められる対価の額に基づいて算定するものとする。その額は、営業秘密の保有者が差止請求権を有する期間に相当する、第 1 項の意味における報酬の額を超えてはならない。

第 12 条 事業主の責任

侵害者が企業の従業員又は代表者である場合、営業秘密の保有者は、第6条から 第8条に基づく請求を事業主に対しても行うことができる。第8条第2項に基づく請求については、

事業主が故意又は重大な過失により、情報を提供しない場合、又は情報の提供を遅延させる、誤った情報を提供する、若しくは不完全な情報を提供する場合にのみ、これが適用される。

第 13 条 時効完成後の返還請求

侵害者が故意又は過失により営業秘密を取得、使用又は開示し、その結果、営業秘密の保有者の犠牲の上に何らかの利益を得た場合には、当該侵害者は、第10条に基づき、ドイツ民法の規定に従って、不当利得の返還義務を負う。この義務は、損害賠償請求権が時効により消滅した後であっても存続する。当該返還請求権は、その発生から6年で時効にかかる。

第 14 条 濫用の禁止

本法に基づく権利行使が、全ての状況を考慮して権利の濫用であると認められる場合には、その行使は認められない。権利が濫用的に行使された場合、被告は、その法的防御のために要した必要費用の償還を請求することができる。これを超える範囲の償還請求権は、影響を受けない。

第 3 節 営業秘密紛争に関する手続

第 15 条 実体的及び地理的管轄、政令による委任

(1) 本法に基づく請求を通常の裁判所において提起する場合、請求の価額にかかわらず、地方裁判所が専属的管轄権を有する。
(2) 第 1 項に基づく訴訟については、被告の普通裁判籍が所在する管轄区域内の裁判所が専属的管轄権を有する。被告が国内に裁判籍を有しない場合、その行為が行われた管轄区域内の裁判所のみが管轄権を有する。
(3) 州政府は、政令により、複数の地方裁判所の管轄区域の訴訟を、第 1 項に基づく地方裁判所に割り当てる権限を有する。州政府は、政令により、この権限を州司法省に委任することができる。また、各州は、合意により、第 1 項に基づく州裁判所が管轄する訴訟を、他の州の管轄裁判所に全体又は一部移送することができる。

第 16 条 秘密保持

(1) 本法に基づく請求を提起する訴訟（営業秘密に関する紛争）において、当事者の申立てにより、当該訴訟の本案を審理する裁判所は、係争中の情報が営業秘密である可能性がある場合、その情報の一部又は全部を機微情報として指定することができる。
(2) 当事者、その訴訟代理人、証人、専門家、その他の代理人、並びに営業秘密紛争

に関与する、又は当該訴訟の文書にアクセスできるその他全ての者は、機微情報として指定された情報を秘密として取扱い、訴訟手続以外では、これを使用又は開示してはならない。ただし、当該情報を訴訟以外で既に知り得た場合は、この限りでない。

(3) 裁判所が第 1 項に基づく決定を行った場合、記録の閲覧権を有する第三者には、営業秘密を含む記述が判読不能にされた記録の内容のみを提供することができる。

第 17 条 秩序措置

本案を審理する裁判所は、第16条第2項に基づく義務に違反した場合、当事者の申立てにより、10万ユーロ以下の秩序金又は6ヶ月以下の秩序拘禁を直ちに科すことができる。秩序金を科す場合、その秩序金が徴収できない場合に備えて、その代わりに秩序拘禁をどの程度科すかを同時に決定しなければならない。第1項に基づいて科された秩序措置に対する不服申立ては、執行停止の効力を有する。

第 18 条 訴訟終了後の秘密保持

第16条第2項に基づく義務は、裁判手続の終了後も引き続き存続する。ただし、本案を審理する裁判所が、訴訟の対象となった営業秘密の存在を確定判決により否定した場合、又はその情報が、通常そのような情報を扱う立場にある者にとって一般的に知られ、若しくは容易に入手可能となった場合は、この限りではない。

第 19 条 その他の司法上の制限

(1) 第 16 条第 1 項に加え、本案を審理する裁判所は、当事者の申立てにより、営業秘密を保護するため、次の事項に関し、アクセスの全部又は一部について、特定の信頼できる人物に限定することができる。

1. 当事者又は第三者によって提出又は提示された、営業秘密を含む可能性のある文書
2. 営業秘密が開示される可能性のある口頭弁論、並びにその記録又は議事録。

これは、あらゆる状況を考慮した上で、秘密保持の利益が、効果的な法的保護及び公正な手続を受ける権利も考慮した上で、当事者の聴聞権を上回る場合にのみ適用される。各当事者の少なくとも 1 人の自然人及びその訴訟代理人又はその他の代理人には、それぞれアクセスを許可しなければならない。その他、裁判所は、その目的を達成するために必要な命令を自由裁量で決定する。

(2) 裁判所が第 1 項第 1 文に基づく制限を行った場合、

1. 申立てにより、口頭弁論から一般の傍聴人を排除することができ、
2. 第 16 条第 3 項は、許可された者には適用されない

(3) 第 16 条から第 19 条第 1 項及び第 2 項は、本案を審理する裁判所が第 16 条第 1 項に基づき情報を機微情報として指定した場合、又は第 1 項第 1 文に基づき追加の制限を設けた場合、強制執行手続においても準用する。

第 20 条 第 16 条から第 19 条に基づく措置の手続

(1) 本案裁判所は、紛争係属中に限り、第 16 条第 1 項及び第 19 条第 1 項に基づく制限を命ずることができる。

(2) 相手方当事者は、遅くとも当該措置の命令後に裁判所の聴聞を受けなければならない。裁判所は、当事者を聴聞した後、当該措置を撤回又は変更することができる。

(3) 第 16 条第 1 項又は第 19 条第 1 項に基づく申立てを行う当事者は、争点とされている情報が営業秘密であることを疎明しなければならない。

(4) もし、書面その他資料が、第 16 条第 1 項に基づく申立て若しくは命令、又は第 19 条第 1 項第 1 文第 1 号に基づく命令に従い提出される場合、申立当事者は、当該当事者の主張に従い営業秘密を含むと主張する記述部分を特定しなければならない。

第 19 条第 1 項第 1 文第 1 号の場合には、営業秘密を開示することなく閲覧可能なバージョンも提出しなければならない。

当該営業秘密部分を削除したバージョンが提出されなかった場合、裁判所は、特段の事情が認められない限り、閲覧に同意があるものと推定することができる。

(5) 裁判所は、申立てについて決定をもって判断する。

申立てを認容する場合、裁判所は、第 16 条第 2 項及び第 18 条に基づく命令の効果並びに第 17 条に定める違反の結果について、関係人に告知しなければならない。

裁判所が申立てを却下しようとする場合、申立人に対しその旨及びその理由を示し、裁判所が定める期間内に意見を述べる機会を付与しなければならない。

第 16 条第 1 項に基づく機微性の分類及び第 19 条第 1 項に基づく制限命令は、本案における不服申立てと併せてのみ争うことができる。

これ以外については即時抗告が認められる。

(6) 本節にいう「本案裁判所」とは、

1. 第一審裁判所、又は
2. 本案が控訴審で係属している場合の控訴裁判所をいう。

第 21 条 判決の公表

(1) 営業秘密に関する訴訟において勝訴した当事者は、申立てにより、判決主文において、敗訴当事者の費用負担で判決又は判決に関する情報を公表する権限の付与を受けることができる。ただし、勝訴当事者がそのための正当な利益を示した場合に限る。

公表の方法及び範囲は、判決に記載された者の正当な利益を考慮して、判決主文において定められる。

(2) 第 1 項第 1 文に基づく公表に関する判断にあたっては、特に以下の事項を考慮するものとする。

1. 営業秘密の価値
2. 営業秘密の取得、使用又は開示に関する侵害者の行為。
3. 営業秘密の違法な使用又は開示による結果
4. 侵害者による更なる違法な使用又は開示の蓋然性

(3) 判決は、裁判所が別段の定めをしない限り、確定後に限り公表することができる

第 22 条 訴額の減額

(1) 営業秘密に関する訴訟において、当事者が訴額の全額に基づいて算定された訴訟費用の負担がその経済状況を著しく危険にさらすことを疎明した場合には、裁判所は、当事者の申立てにより、その当事者の裁判費用支払義務を、その経済状況に応じて調整された訴額一部に基づいて算定されるものとする旨を命ずることができる。

(2) 第 1 項の命令は、次の効力も有するものとする。

1. 恩恵を受ける当事者は、その弁護士費用についても、当該調整後の訴額部分に基づいてのみ支払えば足りること
2. 恩恵を受ける当事者が、訴訟費用の負担を命じられる、又は任意に負担する場合には、相手方が支払った裁判費用及び弁護士費用についても、当該調整後の訴額部分に基づいてのみ償還義務を負うこと
3. 訴訟外費用が相手方に課され、又は相手方がこれを負担する場合には、恩恵を受ける当事者の弁護士は、相手方に対し、相手方に適用される訴額に基づいて、その弁護士費用を相手方から徴収することができること

(3) 第 1 項の申立ては、本案の口頭弁論に先立って行わなければならない。
その後においては、裁判所が定め、又は認定された訴額が引き上げられた場合に限り、申立てを行うことができる。
申立ては、裁判所の書記官室において申述し、記録にとどめることができる。
申立てについて裁判所が決定をする前に、相手方を聴聞しなければならない。

第 4 節 罰則

第 23 条 営業秘密の侵害

(1) 自己若しくは他者の競争を促進する目的、自己若しくは第三者利益を図る目的、又は事業主に損害を与える意図をもって、次の各号のいずれかに該当する行為を行った者は、3 年以下の自由刑又は罰金刑に処する。

1. 第 4 条第 1 項第 1 号に違反して営業秘密を取得した者
2. 第 4 条第 2 項第 1 号(a)に違反して営業秘密を使用又は開示した者
3. 第 4 条第 2 項第 3 号に違反して、企業に雇用されている者が、雇用関係において委託された、又は入手可能となった営業秘密を、雇用関係の有効期間中に開示した者

(2) 自己若しくは他者の競争を促進する目的、自己若しくは第三者利益を図る目的、又は事業主に損害を与える意図をもって、第 1 項第 2 号又は第 3 号に定める第三者の行為によって取得した営業秘密を使用又は開示した者も、同様に処する。

(3) 自己若しくは他者の競争を促進する目的、又は自己の利益を図る目的で、第 4 条第 2 項第 2 号又は第 3 号に違反して、業務上委託された秘密の原型若しくは技術的性質の指示である営業秘密を使用又は開示した者は、2 年以下の自由刑又は罰金に処する。

(4) 次のいずれかに該当する者は、5 年以下の自由刑又は罰金に処する。
1. 第 1 項又は第 2 項の場合において、商業活動として行った者
2. 第 1 項第 2 号若しくは第 3 号、又は第 2 項の場合において、開示の際に、その営業秘密が国外で使用されるべきものであることを知っていた者
3. 第 1 項第 2 号又は第 2 項の場合において、その営業秘密を国外で使用した者

(5) 未遂は罰する。

(6) ドイツ刑事訴訟法第 53 条第 1 項第 1 文第 5 号に規定される者の幇助行為は、営業秘密の受領、評価又は公表に限定される場合、違法ではない。

(7) ドイツ刑法第 5 条第 7 項の規定がこれを準用する。ドイツ刑法第 30 条及び第 31 条の規定は、行為者が自己若しくは他者の競争を促進する目的、又は自己の利益を図る目的で行為した場合に準用される。

(8) 本罪は、検察当局が刑事訴追に特別な公益上の利益があると判断して職権による介入が必要であると認めた場合を除き、告訴があった場合にのみ訴追される。

英国

1 The Trade Secrets (Enforcement, etc.) Regulations 2018

（原文）

5 2018 No. 597
Intellectual Property
The Trade Secrets (Enforcement, etc.) Regulations 2018

Made
15th May 2018

Laid before Parliament
18th May 2018

Coming into force
9th June 2018

The Secretary of State is a Minister designated for the purposes of section 2(2) of the European Communities Act 1972 in relation to intellectual property (including both registered and unregistered rights).

The Secretary of State, in exercise of the powers conferred by section 2(2) of that Act, makes the following Regulations.

1 Citation, commencement and extent

(1) These Regulations may be cited as the Trade Secrets (Enforcement, etc.) Regulations 2018 and come into force on 9th June 2018.

(2) These Regulations extend to England and Wales, Scotland and Northern Ireland.

2. Interpretation

For the purposes of these Regulations—"court" means—

(a) in England and Wales, a County Court hearing centre where there is also a Chancery District Registry or the High Court (as provided for in rule 63.13 of the Civil Procedure Rules 1998),

(b) in Scotland, the sheriff or the Court of Session, and

(c) in Northern Ireland, a county court or the High Court;

"infringer" means a person who has unlawfully acquired, used or disclosed a trade secret;

"infringing goods" means goods, the design, functioning, production process, marketing or a characteristic of which significantly benefits from a trade secret unlawfully acquired, used or disclosed;

"trade secret" means information which—

(a) is secret in the sense that it is not, as a body or in the precise configuration and

assembly of its components, generally known among, or readily accessible to, persons within the circles that normally deal with the kind of information in question,

(b) has commercial value because it is secret, and

(c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret;

"trade secret holder" means any person lawfully controlling a trade secret.

3 Wider protection

(1) The acquisition, use or disclosure of a trade secret is unlawful where the acquisition, use or disclosure constitutes a breach of confidence in confidential information.

(2) A trade secret holder may apply for and a court may grant measures, procedures, and remedies available in an action for breach of confidence where the measures, procedures and remedies—

(a) provide wider protection to the trade secret holder than that provided under these Regulations in respect of the unlawful acquisition, use or disclosure of a trade secret, and

(b) comply with the safeguards referred to in Article 1 of Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

(3) A trade secret holder may apply for and a court may grant the measures, procedures and remedies referred to in paragraph (2) in addition, or as an alternative, to the measures procedures and remedies provided for in these Regulations in respect of the unlawful acquisition, use or disclosure of a trade secret.

4. Time limits for bringing proceedings

(1) Proceedings may not be brought before a court in respect of a claim for the unlawful acquisition, use or disclosure of a trade secret and for the application of measures, procedures and remedies provided for under these Regulations—

(a) in England and Wales and Northern Ireland, after the end of the limitation period for the claim, and

(b) in Scotland, after the end of the prescriptive period for the claim, except where the subsistence of the obligation in relation to which the claim is made was relevantly acknowledged before the end of that period.

(2) The limitation period referred to in paragraph 1(a) is to be determined in accordance with this regulation and regulations 5 to 7 and 9.

(3) Section 36 of the Limitation Act 1980 (equitable jurisdiction and remedies) does not apply in relation to proceedings in respect of a claim for the unlawful acquisition, use or disclosure of a trade secret.

(4) The prescriptive period referred to in paragraph 1(b) is to be determined in accordance with this regulation and regulations 5, 6 and 8.

(5) Section 6 of the Prescription and Limitation (Scotland) Act 1973 (extinction of obligations by prescriptive periods of five years) does not apply in relation to an obligation arising from

a claim for the unlawful acquisition, use or disclosure of a trade secret.

(6) The following provisions of the Prescription and Limitation (Scotland) Act 1973 apply for the purposes of, or in relation to, paragraph (1)(b) as they apply for the purposes of, or in relation to, section 6 of that Act—

(a) section 10 (relevant acknowledgment);

(b) section 13 (prohibition of contracting out);

(c) section 14(1)(c) and (d) (computation of prescriptive periods).

5. Length of limitation or prescriptive period

(1) The limitation period is six years.

(2) The prescriptive period is five years.

(3) The limitation or prescriptive period begins with the day specified in regulation 6.

6. Beginning of limitation or prescriptive period

(1) The limitation or prescriptive period for a claim for the unlawful acquisition, use or disclosure of a trade secret against an infringer begins with the later of—

(a) the day on which the unlawful acquisition, use or disclosure that is the subject of the claim ceases, and

(b) the day of knowledge of the trade secret holder.

(2) In paragraph (1)(b), "the day of knowledge of the trade secret holder" is the day on which the trade secret holder first knows or could reasonably be expected to know—

(a) of the infringer's activity,

(b) that the activity constitutes an unlawful acquisition, use or disclosure of a trade secret, and

(c) the identity of the infringer.

(3) The reference in paragraph (2) to the trade secret holder knowing something is to the trade secret holder having sufficient knowledge of it to bring a claim for the unlawful acquisition, use or disclosure of a trade secret.

(4) Where a person has acquired the liability of an infringer from another person (whether by operation of law or otherwise)—

(a) the reference to an infringer in paragraph (1) is to be read as a reference to the person who has acquired the liability, but

(b) the references to the infringer in paragraph (2) are to be read as references to the original infringer.

(5) This regulation has effect subject to—

(a) regulation 7 in relation to the limitation period, and

(b) regulation 8 in relation to the prescriptive period.

7 Effect of disability on limitation period

(1) If, in relation to a claim in England and Wales and Northern Ireland for the unlawful acquisition, use or disclosure of a trade secret, the trade secret holder is under a disability during the whole or any part of the limitation period, the limitation period for the claim begins with the earlier of—

(a) the day on which the trade secret holder ceases to be under a disability, and

(b) the day on which the trade secret holder dies.

(2) In England and Wales, references in paragraph (1) to a person being "under a disability" have the same meaning as in section 38(2) of the Limitation Act 1980 (interpretation).

(3) In Northern Ireland, references in paragraph (1) to a person being "under a disability" have the same meaning as in article 47 of the Limitation (Northern Ireland) Order 1989 (persons under a disability).

8. Suspension of prescriptive period during period of disability

(1) If, in relation to a claim in Scotland for the unlawful acquisition, use or disclosure of a trade secret, the trade secret holder is under legal disability for a period at any time, the period during which the trade secret holder is under legal disability—

(a) is not to be counted when calculating whether the prescriptive period for the claim has expired, and

(b) is not to be regarded as separating the time immediately before it from the time immediately after it.

(2) In paragraph (1), "legal disability" has the same meaning as in section 15(1) of the Prescription and Limitation (Scotland) Act 1973 (interpretation).

9. New claims in pending actions: England and Wales and Northern Ireland

For the purposes of regulations 4 to 7—

(a) section 35 of the Limitation Act 1980 (new claims in pending action) applies in relation to a claim for the unlawful acquisition, use or disclosure of a trade secret that is a new claim and to proceedings for the unlawful acquisition, use or disclosure of a trade secret as it applies in relation to new claims and proceedings for the purposes of that Act; and

(b) Article 73 of the Limitation (Northern Ireland) Order 1989 (new claims in pending actions) applies in relation to a claim for the unlawful acquisition, use or disclosure of a trade secret that is a new claim and to proceedings for the unlawful acquisition, use or disclosure of a trade secret as it applies in relation to new claims and proceedings for the purposes of that Order.

10. Preservation of confidentiality of trade secrets in the course of proceedings

(1) A participant, or a participant who has access to documents which form part of the proceedings, must not use or disclose any trade secret or alleged trade secret—

(a) which, on a duly reasoned application by an interested party or on a court's own initiative, a court by order identifies as confidential, and

(b) of which a participant has become aware as a result of participation in the proceedings or the access.

(2) The obligation referred to in paragraph (1) remains in force after the proceedings have ended, subject to paragraph (3).

(3) The obligation in paragraph (1) ceases to exist—

(a) where a court, by final decision, finds that the alleged trade secret does not meet the requirements of a trade secret, or

(b) where over time the information in question becomes generally known among, or readily accessible to, persons within the circles that normally deal with that kind of information.

(4) On a duly reasoned application by a party or on a court's own initiative, a court may order any of the measures set out in paragraph (5) as may be necessary to preserve the confidentiality of any trade secret or alleged trade secret used or referred to in the course of proceedings.

(5) A court may—

(a) restrict access to any document containing a trade secret or alleged trade secret submitted by the parties or third parties, in whole or in part, to a limited number of persons,

(b) restrict access to hearings, when trade secrets or alleged trade secrets may be disclosed, and to the record or transcript of those hearings to a limited number of persons, and

(c) make available to a person, who is not one of the limited number of persons referred to in sub-paragraph (a) or (b), a non-confidential version of any judicial decision, in which the passages containing trade secrets have been removed or redacted.

(6) The number of persons referred to in paragraph 5(a) or (b) must be no greater than necessary to ensure compliance with the right of the parties to the legal proceedings to an effective remedy and to a fair trial, and must include, at least, one individual from each party and the lawyers or other representatives of those parties to the proceedings.

(7) In deciding whether or not to grant the measures in paragraph (5) in accordance with paragraphs (4) and (6) and which of the measures to order and in assessing the proportionality of the measures, a court must take into account—

(a) the need to ensure the right to an effective remedy and to a fair trial,

(b) the legitimate interests of the parties, and

(c) any potential harm for the parties.

(8) In this regulation—

"participant" means a party, a lawyer or other representative of a party, a court official, a witness, an expert or any other person participating in proceedings;

"parties", in paragraph (7), includes, where appropriate, third parties;

"proceedings" means legal proceedings relating to the unlawful acquisition, use or disclosure of a trade secret.

11 Interim measures

(1) On the application of a trade secret holder, a court may order any of the following measures against the alleged infringer—

(a) the cessation of, or (as the case may be) the prohibition of, the use or disclosure of the trade secret on a provisional basis;

(b) the prohibition of the production, offering, placing on the market or use of infringing goods, or the importation, export or storage of infringing goods for those purposes;

(c) the seizure or delivery up of the suspected infringing goods, including imported goods, so as to prevent the goods entering into, or circulating on, the market.

(2) A person to whom the suspected infringing goods are delivered up under paragraph (1)(c) must retain the infringing goods pending a decision to make or not to make an order under regulation 14(2).

(3) A court making an order under paragraph (1) may set a reasonable period within which a trade secret holder must bring proceedings for a decision on the merits of the case before a court.

(4) Where no period is set under paragraph (3), a trade secret holder must bring proceedings before a court within a period not exceeding 20 working days or 31 calendar days after the day on which the order under paragraph (1) has been made, whichever is the longer.

(5) For the purposes of paragraph (4)—

(a) if the period of 20 working days ends on a day other than a working day, the proceedings are in time if they are brought on the next working day, and

(b) "working day" means any day except a Saturday or Sunday, Christmas Day, Good Friday or a day which is a bank holiday in any part of the United Kingdom under section 1 of the Banking and Financial Dealings Act 1971 (bank holidays).

(6) As an alternative to the measures referred to in paragraph (1), a court may make an order making the continuation of the alleged unlawful use conditional upon the lodging by the alleged infringer of guarantees intended to ensure the compensation of the trade secret holder.

(7) An order under paragraph (6) must not permit disclosure of a trade secret in return for the lodging of guarantees.

(8) A court may make an order under paragraph (1) or (6) conditional upon the lodging by the trade secret holder of adequate security or an equivalent assurance intended to ensure compensation for any prejudice suffered by the alleged infringer and, where appropriate, by any other person affected by the order.

12. Matters to be considered before making an order under regulation 11(1)

(1) Before making an order under regulation 11(1), a court may require the trade secret holder to provide evidence that may reasonably be considered available to satisfy the court with a sufficient degree of certainty that—

(a) a trade secret exists,

(b) the trade secret holder is making the application, and

(c) the alleged infringer—

(i) has acquired the trade secret unlawfully,

(ii) is unlawfully using or disclosing the trade secret, or

(iii) is about to unlawfully use or disclose the trade secret.

(2) In considering whether to make an order under regulation 11(1) and in assessing the proportionality of such an order, a court must take into account the specific circumstances of the case, including where appropriate—

(a) the value and other specific features of the trade secret,

(b) the measures taken to protect the trade secret,

(c) the conduct of the alleged infringer in acquiring, using or disclosing the trade secret,

(d) the impact of the unlawful use or disclosure of the trade secret,

(e) the legitimate interests of the parties and the impact which the granting or rejection of the measures could have on the parties,

(f) the legitimate interests of third parties,

(g) the public interest, and

(h) the safeguard of fundamental rights.

13. Revocation of order under regulation 11(1)

(1) Where a court makes an order under regulation 11(1), the court may, on the application of the alleged infringer, revoke the order—

(a) if the trade secret holder does not bring proceedings leading to a decision on the merits of the case before a court within the period set under regulation 11(3) or in regulation 11(4), or

(b) if the information in question is no longer a trade secret for reasons that cannot be attributed to the alleged infringer.

(2) A court may, on the application of the alleged infringer or an injured third party, order the trade secret holder to provide the alleged infringer, or the injured third party, appropriate compensation for any injury caused by a measure ordered under regulation 11(1)—

(a) where a court revokes an order under paragraph (1)(a),

(b) where the measure lapses due to any act or omission by the trade secret holder, or

(c) where it is subsequently found that there has been no unlawful acquisition, use or disclosure of a trade secret or threat of such conduct.

14 Injunctions or interdicts and corrective measures

(1) Where a court finds on the merits of the case that there has been an unlawful acquisition, use or disclosure of a trade secret, the court may, on application by the trade secret holder, order one or more of the following measures against the infringer—

(a) the cessation of, or (as the case may be) the prohibition of, the use or disclosure of the trade secret;

(b) the prohibition of the production, offering, placing on the market or use of infringing goods, or the importation, export or storage of infringing goods for those purposes;

(c) the adoption of corrective measures with regard to the infringing goods, including where appropriate—

(i) recall of the infringing goods from the market;

(ii) depriving the infringing goods of their infringing quality;

(iii) destruction of the infringing goods or their withdrawal from the market, provided that the withdrawal does not undermine the protection of the trade secret in question;

(d) the destruction of all or part of any document, object, material, substance or electronic file containing or embodying the trade secret, or where appropriate, the delivery up to the applicant of all or part of that document, object, material, substance or electronic file.

(2) Where a court orders that infringing goods be withdrawn from the market, the court may order, on the application of the trade secret holder, that the infringing goods be delivered up and forfeited to the trade secret holder together with all or part of any document, object, material, substance or electronic file containing or embodying the trade secret.

(3) Where a court makes an order for a measure under paragraph (1)(c) or (d) or paragraph (2), the court must—

(a) order that the measure be carried out at the expense of the infringer, unless there are particular reasons for not doing so, and

(b) ensure the measure is without prejudice to any damages that may be due to the trade secret holder by reason of the unlawful acquisition, use or disclosure of the trade secret.

15 Matters to be considered when making an order under regulation 14

(1) In considering an application for an order under regulation 14 and assessing the proportionality of such an order, the court must take into account the specific circumstances of the case, including where appropriate—

(a) the value or other specific features of the trade secret,

(b) the measures taken to protect the trade secret,

(c) the conduct of the infringer in acquiring, using or disclosing the trade secret,

(d) the impact of the unlawful use or disclosure of the trade secret,

(e) the legitimate interests of the parties and the impact which the granting or rejection of the measures could have on the parties,

(f) the legitimate interests of third parties,

(g) the public interest, and

(h) the safeguard of fundamental rights.

(2) Where a court makes an order limiting the duration of a measure ordered under regulation 14(1)(a) or (b), the duration must be sufficient to eliminate any commercial or economic advantage that the infringer could have derived from the unlawful acquisition, use or disclosure of the trade secret.

(3) On the application of the defendant, the court must revoke a measure ordered under regulation 14(1)(a) or (b) if the information in question no longer constitutes a trade secret for reasons that cannot be attributed directly or indirectly to the defendant.

(4) In the application of paragraph (3) to Scotland, "defendant" means defender.

16 Compensation instead of order under regulation 14

(1) A person liable to the imposition of an order under regulation 14 may apply for, and a court may make, an order for compensation to be paid to the injured party instead of an order under regulation 14—

(a) if at the time of use or disclosure the person neither knew nor ought, under the circumstances, to have known that the trade secret was obtained from another person who was using or disclosing the trade secret unlawfully,

(b) if the execution of the measures in question would cause disproportionate harm to the person liable to the measures, and

(c) if it appears reasonably satisfactory to pay compensation to the injured party.

(2) Where a court makes an order for the payment of compensation instead of an order under regulation 14(1)(a) or (b), the compensation must not exceed the amount of royalties or fees which would have been due, had that person obtained a licence to use the trade secret in question, for the period for which use of the trade secret could have been prohibited.

17 Assessment of damages

(1) On the application of an injured party, a court must order an infringer, who knew or ought to have known that unlawful acquisition, use or disclosure of a trade secret was being engaged in, to pay the trade secret holder damages appropriate to the actual prejudice suffered as a result of the unlawful acquisition, use or disclosure of the trade secret.

(2) A court may award damages under paragraph (1) on the basis of either paragraph (3) or (4).

(3) When awarding damages under paragraph (1) on the basis of this paragraph, a court must take into account all appropriate factors, including in particular—

(i) the negative economic consequences, including any lost profits, which the trade secret holder has suffered, and any unfair profits made by the infringer, and

(ii) elements other than economic factors, including the moral prejudice caused to the trade secret holder by the unlawful acquisition, use or disclosure of the trade secret.

(4) When awarding damages under paragraph (1) on the basis of this paragraph, a court may, where appropriate, award damages on the basis of the royalties or fees which would have been due had the infringer obtained a licence to use the trade secret in question.

18 Publication of judicial decisions

(1) In proceedings for the unlawful acquisition, use or disclosure of a trade secret, a court may order, on the application of the trade secret holder and at the expense of the infringer, appropriate measures for the dissemination of information concerning the judgment, including its publication in whole or in part.

(2) Any measure a court may order under paragraph (1) must preserve the confidentiality of trade secrets as provided for in regulation 10.

(3) In deciding whether to order a measure under paragraph (1) and when assessing whether such measure is proportionate, the court must take into account where appropriate—

(a) the value of the trade secret,

(b) the conduct of the infringer in acquiring, using or disclosing the trade secret,

(c) the impact of the unlawful use or disclosure of the trade secret,

(d) the likelihood of further unlawful use, or disclosure of the trade secret by the infringer, and

(e) whether the information on the infringer would be such as to allow an individual to be identified and, if so, whether publication of that information would be justified, in particular in the light of the possible harm that such measure may cause to the privacy and reputation of the infringer.

19 Proceedings to which these Regulations apply

These Regulations apply only to proceedings—

(a) brought before a court after the coming into force of these Regulations,

(b) in respect a claim for the unlawful acquisition, use or disclosure of a trade secret, and

(c) for the application of measures, procedures and remedies provided for under these Regulations.

Sam Gyimah
Minister of State
Department for Business, Energy and Industrial Strategy
15th May 2018

EXPLANATORY NOTE

(This note is not part of the Regulations)

These Regulations implement provisions of Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure (OJ L157, 15.6.2017, p.1) ("the Directive"). A number of the provisions of the Directive, in particular the provisions in Chapter II and Articles 6, 7 and 16, have been implemented in the United Kingdom by the principles of common law and equity relating to breach of confidence in confidential information, and by statute and court rules. These Regulations address those areas where gaps occur or where the implementation of the provisions of the Directive in the United Kingdom, across its jurisdictions, may be made more transparent and coherent.

Regulation 2 defines the terms "infringer", "infringing goods", "trade secret" and "trade secret holder" in accordance with Article 2 of the Directive and adds a definition of "court".

Regulation 3(1) makes clear that the issue of whether the acquisition, use or disclosure of a trade secret is unlawful is determined by reference to the principles of the law of confidence. Where the measures, procedures and remedies available in an action for breach of confidence offer wider protection to a trade secret holder than that offered under the Regulations, the trade secret holder may apply for, and a court may grant, them provided they comply with the safeguards referred to in Article 1 of the Directive (Regulation 3(2)). The measures, procedures and remedies referred to in regulation 3(2) are in addition, or an alternative, to the measures, procedures and remedies provided under these Regulations in respect of the unlawful acquisition, use or disclosure of a trade secret (Regulation 3(3)).

Regulations 4 to 9 make provision for limitation and prescriptive periods applicable to proceedings for claims for the unlawful acquisition, use or disclosure of a trade secret and for the application of measures, procedures and remedies under these Regulations. Regulations 4 to 9 implement Article 8 of the Directive. A limitation period of six years is set for England and Wales and Northern Ireland. A prescriptive period of five years is set for Scotland. Provision is made for determining when the limitation or prescriptive period begins to run and for suspending the limitation or prescriptive period on account of disability.

Regulation 10 provides for the preservation of confidentiality of trade secrets in the course of legal proceedings in implementation of Article 9(1) to (3) of the Directive.

Regulation 11 provides for interim measures against an alleged infringer in implementation of Article 10 of the Directive. Where an interim order for delivery up is made, a trade secret holder must retain the infringing goods until an order is made under regulation 14(2) that the goods be forfeited to the trade secret holder or destroyed. A time limit is set within which a claim must be brought after an interim order has been made. As an alternative to interim measures, a court may require guarantees to be lodged by the alleged infringer to compensate the trade secret holder. A court may also require a trade secret holder to provide adequate security to compensate an alleged infringer for any prejudice suffered.

Regulation 12 provides for the matters a court needs to consider before making an interim order under regulation 11(1). Regulation 12 implements Article 11(1) and (2) of the Directive.

Regulation 13 provides for revocation of an order made under regulation 11(1) where a trade secret

holder does not bring proceedings before a court within the specified period or in certain other circumstances. Where a measure ordered is revoked, a court may order payment of appropriate compensation to the alleged infringer or injured third party. Regulation 13 implements Article 11(3) and (5) of the Directive.

Regulation 14 provides for injunctions, or interdicts in Scotland, and corrective measures which may be imposed on an infringer. These measures include requiring an infringer, at his expense, to recall the infringing goods from the market, to deprive them of their infringing quality, to destroy the infringing goods or to withdraw them from the market. When ordering the withdrawal of the goods from the market, a court may require the goods to be delivered up and forfeited to the trade secret holder. Regulation 14 implements Article 12 of the Directive.

Regulation 15 sets out the matters to be considered when making an order under regulation 14 and implements Article 13(1) and (2) of the Directive.

Regulation 16 enables a court to order compensation instead of an order under regulation 14 under certain conditions. This implements Article 13(3) of the Directive.

Regulation 17 sets out the factors that need to be taken into account when making an award of damages for the unlawful acquisition, use or disclosure of a trade secret. This implements Article 14 of the Directive.

Regulation 18 makes provision for the publication of information relating to judicial decisions in proceedings for the unlawful acquisition, use or disclosure of a trade secret. This implements Article 15 of the Directive.

Regulation 19 makes clear that the Regulations apply only to proceedings brought before a court after the coming into force of these Regulations in respect of a claim for the unlawful acquisition, use or disclosure of a trade secret and for the application of measures, procedures and remedies provided for under these Regulations.

A full impact assessment has not been produced for this instrument as no, or no significant, impact on the private, voluntary or public sector is foreseen. A transposition note is available from the Intellectual Property Office, Concept House, Cardiff Road, Newport NP10 8QQ and is available with the explanatory memorandum alongside this instrument on the Legislation UK website at www.legislation.gov.uk. Copies have also been placed in the libraries of both Houses of Parliament.

（参考和訳）

2018 年 第 597 号
知的財産
2018 年 営業秘密（執行等）規則

制定日
2018 年 5 月 15 日

議会提出日
2018 年 5 月 18 日

施行日
2018 年 6 月 9 日

国務大臣は、1972 年欧州共同体法第 2 条第 2 項の目的に関して、
知的財産（登録・未登録の権利を含む）に関して指定された大臣である。
国務大臣は、同法第 2 条第 2 項に基づく権限を行使して、以下の規則を制定する。

1　題名、施行日及び適用範囲

(1) 本規則は「2018 年営業秘密（執行等）規則」と称し、2018 年 6 月 9 日に施行される。

(2) 本規則は、イングランド及びウェールズ、スコットランド及び北アイルランドに適用する。

2　定義

本規則において、以下の各号に掲げる用語は、当該各号に定める意味を有する。

「裁判所」とは、以下をいう。

(a) イングランド及びウェールズにおいては、1998 年民事訴訟規則第 63.13 条に定める、チャンセリー地方登記所を併設するカウンティ・コートの審理センター又は高等法院（High Court）

(b) スコットランドにおいては、シェリフ又はセッション裁判所（Court of Session）

(c) 北アイルランドにおいては、カウンティ・コート又は高等法院

「侵害者」とは、営業秘密を不正取得、使用、又は開示した者をいう。

「侵害品」とは、営業秘密の不正取得、使用、又は開示によって、その設計、機能、製造工程、販売促進、又は特性が、大きな利益を得ている物品をいう。

「営業秘密」とは、以下の要件を満たす情報をいう。

(a) 当該情報全体として、又はその構成要素の正確な組合せ及び集積として、当該種別の情報を通常取り扱う者の間において一般に知られておらず、又は容易に入手可能でもないこと

(b) 当該情報が秘密であることにより商業的価値を有すること

(c) 当該情報を適法に管理する者によって、状況に応じて合理的と考えられる、情報を秘密に保つための措置が講じられていること

「営業秘密の保有者」とは、営業秘密を適法に管理する者をいう。

3 より広範な保護

(1) 営業秘密の取得、使用又は開示が、秘密保持義務違反（breach of confidence）を構成する場合、当該取得、使用又は開示は不法とする。

(2) 営業秘密の保有者は、秘密保持義務違反に関する訴訟において利用可能な措置、手続及び救済であって、以下の要件を満たすものを裁判所に申立てることができ、裁判所はこれを認めることができる。

(a) 営業秘密の不正取得、使用又は開示に関して、本規則に基づく保護よりも、営業秘密の保有者に対して広範な保護を与えるものであること

(b) 2016 年 6 月 8 日付欧州議会及び理事会指令（EU）2016/943「不法な取得、使用及び開示に対する未公開ノウハウ及び事業情報（営業秘密）の保護に関する指令」第 1 条に言及される保護措置に適合すること

(3) 営業秘密の保有者は、前項に定める措置、手続及び救済を、本規則に基づく営業秘密の不正取得、使用又は開示に関して認められる措置、手続及び救済に加えて、又はそれらに代えて、裁判所に申立てることができ、裁判所はこれを認めることができる。

4 訴訟提起の期間制限

(1) 営業秘密の不正取得、使用又は開示に関する請求及び本規則に基づく措置、手続及び救済の申立てに関しては、以下の期間経過後は裁判所に提起することができない。

(a) イングランド、ウェールズ及び北アイルランドにおいては、当該請求に係る出訴期間（limitation period）の経過後

(b) スコットランドにおいては、当該請求に係る時効期間（prescriptive period）の経過後。但し、当該期間の経過前に、当該請求に係る義務の存続が適切に承認された場合を除く

(2) 第 1 項(a)にいう出訴期間は、本条、第 5 条から第 7 条及び第 9 条に従って定めるものとする。

(3) 1980 年出訴期間法（Limitation Act 1980）第 36 条（衡平法上の管轄及び救済）は、営業秘密の不正取得、使用又は開示に関する請求に係る訴訟手続には適用しない。

(4) 第 1 項(b)にいう時効期間は、本条、第 5 条、第 6 条及び第 8 条に従って定めるも

のとする。

(5) 1973 年スコットランド時効及び出訴期間法（Prescription and Limitation (Scotland) Act 1973）第 6 条（5 年の時効期間による義務の消滅）は、営業秘密の不正取得、使用又は開示に関する請求から生じる義務については適用しない。

(6) 1973 年スコットランド時効及び出訴期間法の以下の規定は、第 1 項(b)に関し、又はこれに関連して、同法第 6 条に関し、又はこれに関連して適用されるのと同様に適用される。

(a) 第 10 条（適切な承認）

(b) 第 13 条（契約による適用除外の禁止）

(c) 第 14 条第 1 項(c)及び(d)（時効期間の算定）

5 出訴期間又は時効期間の長さ

(1) 出訴期間は 6 年とする。

(2) 時効期間は 5 年とする。

(3) 出訴期間又は時効期間は、第 6 条に定める日から起算する。

6 出訴期間又は時効期間の起算日

(1) 侵害者に対する営業秘密の不正取得、使用又は開示に関する請求についての出訴期間又は時効期間は、以下のいずれか遅い日から開始する。

(a) 当該請求の対象となる不正取得、使用又は開示が終了した日

(b) 営業秘密の保有者が知った日

(2) 第 1 項(b)にいう「営業秘密の保有者が知った日」とは、営業秘密の保有者が以下に掲げる事項を初めて知った、又は合理的に知り得たとみなされる日をいう。

(a) 侵害者の行為の存在

(b) 当該行為が営業秘密の不正取得、使用又は開示に該当すること

(c) 侵害者の身元

(3) 第 2 項において営業秘密の保有者が何かを「知る」とは、営業秘密の不正取得、使用又は開示に関する請求を行うのに十分な程度の認識を有することをいう。

(4) ある者が他の者から（法律の効力その他の方法により）侵害者としての責任を承継した場合、

(a) 第 1 項の「侵害者」との言及は、当該責任を承継した者を指すものとし、

(b) 第 2 項の「侵害者」との言及は、元の侵害者を指すものとする

(5) 本条は、以下の規定に従うものとする。

(a) 出訴期間については第 7 条

(b) 時効期間については第 8 条

7 出訴期間に対する無能力の影響

(1) イングランド、ウェールズ及び北アイルランドにおける営業秘密の不正取得、使用又は開示に関する請求について、営業秘密の保有者が出訴期間の全部又は一部の間無能力状態にある場合には、当該請求に係る出訴期間は、以下のいずれか早

い日から開始する。

(a) 営業秘密の保有者が無能力状態でなくなった日

(b) 営業秘密の保有者が死亡した日

(2) イングランド及びウェールズにおいて、第 1 項にいう「無能力状態にある」とは、1980 年出訴期間法第 38 条第 2 項（解釈）に定める意味を有するものとする。

(3) 北アイルランドにおいて、第 1 項にいう「無能力状態にある」とは、1989 年出訴期間（北アイルランド）命令第 47 条（無能力状態にある者）に定める意味を有するものとする。

8 無能力期間中の消滅時効期間の停止

(1) スコットランドにおける営業秘密の不正取得、使用又は開示に関する請求について、営業秘密の保有者がある期間にわたり法律上の無能力状態にある場合、当該無能力状態にある期間については、以下のとおりとする。

(a) 当該請求に係る時効期間の満了を計算する際に算入しない

(b) 当該期間の直前の時点と直後の時点を分断するものとはみなさない

(2) 第 1 項にいう「法律上の無能力状態」とは、1973 年スコットランド時効及び出訴期間法第 15 条第 1 項（解釈）に定める意味を有するものとする。

9 係属中の訴訟における新たな請求：イングランド、ウェールズ及び北アイルランド

本規則第 4 条から第 7 条の目的のため、以下のとおりとする。

(a) 1980 年出訴期間法第 35 条（係属中の訴訟における新たな請求）は、営業秘密の不正取得、使用又は開示に関する新たな請求及び営業秘密の不正取得、使用又は開示に関する訴訟手続について、同法に基づく新たな請求及び訴訟手続に関して適用されるのと同様に適用される。

(b) 1989 年出訴期間（北アイルランド）命令第 73 条（係属中の訴訟における新たな請求）は、営業秘密の不正取得、使用又は開示に関する新たな請求及び営業秘密の不正取得、使用又は開示に関する訴訟手続について、当該命令に基づく新たな請求及び訴訟手続に関して適用されるのと同様に適用される。

10 訴訟手続における営業秘密の秘密保持

(1) 訴訟手続の参加者又は訴訟手続の一部を構成する文書を利用する参加者は、以下の営業秘密又は営業秘密であると主張されている情報を使用又は開示してはならない。

(a) 利害関係人による正当な理由を示した申立て又は裁判所の職権に基づき、裁判所が命令により秘密であると認定し、

(b) 参加者が訴訟手続への参加又は利用の結果として、知るに至ったもの

(2) 第 1 項にいう義務は、当該訴訟手続が終了した後も、第 3 項に従い存続する。

(3) 第 1 項の義務は、以下の場合には消滅する。

(a) 裁判所が最終的な判断により、営業秘密であると主張された情報が営業秘密

の要件を満たさないと認定したとき

(b) 当該情報が、時の経過により、通常その種の情報を取り扱う者の間で一般に知られ、又は容易に入手可能となったとき

(4) 利害関係人の正当な理由を示した申立て又は裁判所の職権に基づき、裁判所は、訴訟手続において使用された、又は言及された営業秘密若しくは営業秘密であると主張される情報の秘密を保持するために必要な限度で、第 5 項に定める措置を命ずることができる。

(5) 裁判所は、以下の措置を命ずることができる。

(a) 当事者又は第三者が提出した営業秘密又は営業秘密であると主張される情報を含む文書の利用を、全部又は一部について、限定された人数の者に制限すること

(b) 営業秘密又は営業秘密であると主張される情報が開示されうる審理への立会い及び当該審理の記録又は議事録の利用を、限定された人数の者に制限すること

(c) 第(a)又は(b)に定める限定された人数の者に含まれない者に対して、営業秘密を含む部分を削除又は編集した非秘密版の裁判所の判断を提供すること

(6) 第 5 項(a)又は(b)に定める限定された人数は、訴訟当事者の実効的な救済及び公正な裁判を受ける権利を確保するために必要な限度を超えてはならず、少なくとも各当事者の代表者 1 名及び当該当事者の弁護士その他の代理人を含まなければならない。

(7) 裁判所は、第 4 項及び第 6 項に従い第 5 項に定める措置を認めるか否か、又はどの措置を命ずるか、及び当該措置の比例性を判断する際には、以下の事項を考慮しなければならない。

(a) 実効的な救済及び公正な裁判を受ける権利を確保する必要性

(b) 当事者の正当な利益

(c) 当事者に対する潜在的な不利益

(8) 本規則において、

「参加者」とは、当事者、当事者の弁護士その他の代理人、裁判所職員、証人、専門家その他訴訟手続に参加する者をいう。

「当事者」とは、第 7 項において、必要に応じ第三者を含む。

「訴訟手続」とは、営業秘密の不正取得、使用又は開示に関する法的手続をいう。

11 暫定的措置

(1) 裁判所は、営業秘密の保有者の申立てに基づき、営業秘密であると主張される情報の侵害者に対して、以下のいずれかの措置を命ずることができる。

(a) 営業秘密の使用又は開示の停止、又は場合により、禁止

(b) 侵害品の製造、提供、市場への流通若しくは使用、又は当該目的のための侵

害品の輸入、輸出若しくは保管の禁止

(c) 侵害が疑われる物品（輸入品を含む）が市場に流通することを防ぐための、当該物品の差押え又は引渡し

(2) 第 1 項(c)に基づき侵害が疑われる物品の引渡しを受けた者は、第 14 条第 2 項に基づく命令を下すか否かの決定がなされるまで、当該物品を保管しなければならない。

(3) 第 1 項に基づく命令を下す裁判所は、営業秘密の保有者が本案の申立てを行うべき合理的な期間を定めることができる。

(4) 第 3 項に基づく期間が定められていない場合、営業秘密の保有者は、第 1 項に基づく命令が発せられた日から 20 営業日又は 31 暦日（いずれか長い方）以内に裁判所に訴訟を提起しなければならない。

(5) 第 4 項の適用において、以下のとおりとする。

(a) 20 営業日の期間が営業日以外の日に終了する場合、翌営業日に訴訟を提起すれば期限内とみなされる

(b) 「営業日」とは、土曜日、日曜日、クリスマス、聖金曜日又は 1971 年銀行及び金融取引法第 1 条に基づく英国各地の銀行休日を除く日をいう

(6) 第 1 項に掲げる措置に代えて、裁判所は、被疑侵害者が営業秘密の保有者への補償を確保するための保証金等を供託することを条件として、当該不正使用の継続を認める命令を下すことができる。

(7) 第 6 項に基づく命令は、保証金等の供託と引き換えに営業秘密の開示を認めてはならない。

(8) 裁判所は、第 1 項又は第 6 項に基づく命令を、被疑侵害者及び必要に応じてその他命令の影響を受ける者が被る損害を補償するための十分な担保を提供すること又は同等の保証を営業秘密の保有者が供託することを条件として下すことができる。

12 第 11 条第 1 項に基づく命令を行う前に考慮すべき事項

(1) 第 11 条第 1 項に基づく命令を発する前に、裁判所は、営業秘密の保有者に対して、以下の各号の事項について、裁判所が十分な確実性をもって認定できると合理的に考えうる証拠の提示を求めることができる。

(a) 営業秘密が存在すること

(b) 営業秘密の保有者が申立てを行っていること

(c) 被疑侵害者が以下のいずれかに該当すること

(i) 営業秘密を不正取得したこと

(ii) 営業秘密を不正使用又は開示していること

(iii) 営業秘密を不正使用又は開示しようとしていること

(2) 第 11 条第 1 項に基づく命令を発するか否かを判断し、当該命令の比例性を評価するにあたり、裁判所は、事案の具体的状況を考慮し、必要に応じて以下の事項

を含めて検討しなければならない。

(a) 営業秘密の価値及びその他特性

(b) 営業秘密を保護するために講じられた措置

(c) 営業秘密を取得、使用又は開示する際の被疑侵害者の行為

(d) 営業秘密の不正使用又は開示の影響

(e) 当事者の正当な利益及び当該措置の許可又は却下が当事者に与える影響

(f) 第三者の正当な利益

(g) 公共の利益

(h) 基本的権利の保護

13 第 11 条第 1 項に基づく命令の取り消し

(1) 裁判所が第 11 条第 1 項に基づく命令を発した場合、裁判所は、被疑侵害者の申立てに基づき、以下の場合には裁判所は当該命令を取り消すことができる。

(a) 営業秘密の保有者が、第 11 条第 3 項又は第 11 条第 4 項に定める期間内に、本案の判決をうるための訴訟を提起しない場合

(b) 当該情報が、被疑侵害者に起因しない理由により、もはや営業秘密でなくなった場合

(2) 裁判所は、被疑侵害者又は損害を被った第三者の申立てに基づき、営業秘密の保有者に対し、第 11 条第 1 項に基づく措置により生じた損害について、被疑侵害者又は損害を被った第三者に適切な賠償を行うことを命ずることができる。

(a) 裁判所が第 1 項(a)に基づき命令を取り消した場合

(b) 営業秘密の保有者の行為又は不作為により当該措置が失効した場合

(c) その後、営業秘密の不正取得、使用又は開示、又はそのおそれがなかったことが判明した場合

14 差止命令及び是正措置

(1) 裁判所が、本案において、営業秘密の不正取得、使用又は開示があったと認定した場合、裁判所は、営業秘密の保有者の申立てに基づき、裁判所は侵害者に対して、以下の一つ又は複数の措置を命ずることができる。

(a) 営業秘密の使用又は開示の停止、又は場合により、禁止

(b) 侵害品の製造、提供、市場への流通若しくは使用、又は当該目的のための侵害品の輸入、輸出若しくは保管の禁止

(c) 侵害品に関する是正措置の採用（必要に応じて以下を含む）

(i) 侵害品の市場からの回収

(ii) 侵害品から侵害する特徴を失わせること

(iii) 侵害品の破棄又は市場からの撤去（ただし、撤去が当該営業秘密の保護を損なわない場合に限る）

(d) 営業秘密を含む又は具現化した文書、物品、資料、物質若しくは電子ファイルの全部若しくは一部の破棄、又は必要に応じて、これらの全部若しくは一

部の申立人への引渡し

(2) 裁判所が侵害品の市場からの撤去を命じる場合、裁判所は、営業秘密の保有者の申立てに基づき、当該侵害品を営業秘密の保有者に引き渡し、かつ没収すること、及び営業秘密を含む又は具現化する文書、物品、資料、物質又は電子ファイルの全部又は一部を営業秘密の保有者に引き渡すことを命ずることができる。

(3) 裁判所が第 1 項(c)若しくは(d)又は第 2 項に基づく措置を命ずる場合、以下の事項を行わなければならない。

(a) 特段の事情がない限り、当該措置が侵害者の費用負担で実施されることを命じること

(b) 当該措置は、営業秘密の不正取得、使用又は開示により営業秘密の保有者に生じうる損害賠償請求権を害さないことを確保すること

15 第 14 条に基づく命令を行う際に考慮すべき事項

(1) 第 14 条に基づく命令の申立てを審理し、当該命令の比例性を評価するにあたり、裁判所は事案の具体的事情を考慮しなければならず、必要に応じて以下を含む要素を考慮するものとする。

(a) 営業秘密の価値その他の特性

(b) 営業秘密を保護するために講じられた措置

(c) 侵害者による営業秘密の取得、使用又は開示の態様

(d) 営業秘密の不正使用又は開示の影響

(e) 当事者の正当な利益及び当該措置の採否が当事者に及ぼす影響

(f) 第三者の正当な利益

(g) 公共の利益

(h) 基本的権利の保護

(2) 裁判所が第 14 条第 1 項(a)又は(b)に基づき命じる措置の期間を制限する場合、当該期間は、侵害者が営業秘密の不正取得、使用又は開示から得た可能性のある商業的又は経済的利益を排除するのに十分なものでなければならない。

(3) 被告の申立てに基づき、裁判所は、当該情報が被告に直接的又は間接的に起因しない理由で営業秘密に該当しなくなった場合には、第 14 条第 1 項(a)又は(b)に基づき命じた措置を取り消さなければならない。

(4) 第 3 項をスコットランドに適用する場合、「defendant」は「defender」を意味する。

16 第 14 条に基づく命令の代わりの損害賠償

(1) 第 14 条に基づく命令の対象となる者は、申立てにより、第 14 条に基づく命令に代えて損害賠償の支払いを命じる命令を求めることができ、裁判所は、以下の各号のいずれにも該当する場合に、当該命令を発することができる。

(a) 使用又は開示の時点において、その者が、営業秘密を不正使用又は開示している他者から取得されたものであることを知らず、又は知るべきものでもな

かった場合

(b) 当該命令に基づく措置の実施が、その対象者にとって過度な不利益をもたらす場合

(c) 損害を受けた者に対して損害賠償を支払うことが合理的に妥当である場合

(2) 裁判所が、第 14 条第 1 項(a)又は(b)に基づく命令の代わりに損害賠償の支払いを命じる場合、当該賠償額は、その者が当該営業秘密の使用について実施権を取得していたと仮定した場合に、営業秘密の使用を禁止できた期間について支払われるべき使用許諾料又は料金の額を超えてはならない。

17 損害賠償の算定

(1) 裁判所は、損害を被った当事者の申立てに基づき、営業秘密の不正取得、使用又は開示が行われていることを知っていた、又は知るべきであった侵害者に対し、営業秘密の保有者に対する当該不正取得、使用又は開示により実際に被った損害に相当する損害賠償の支払いを命じなければならない。

(2) 裁判所は、第 1 項に基づく損害賠償額を、第 3 項又は第 4 項のいずれかに基づき算定することができる。

(3) 裁判所が第 1 項に基づく損害賠償額を本項に基づき算定する場合、特に以下を含む、適切な要素を総合的に考慮しなければならない。

(i) 営業秘密の保有者が被った経済的損害（逸失利益を含む）及び侵害者が得た不当な利益

(ii) 営業秘密の不正取得、使用又は開示によって営業秘密の保有者に生じた精神的損害を含む、経済的要素以外の要素

(4) 裁判所が第 1 項に基づく損害賠償額を本項に基づき算定する場合、必要に応じて、侵害者が当該営業秘密の使用について実施権を取得していたと仮定した場合に支払うべき使用許諾料又は料金に基づいて損害賠償を命じることができる。

18 裁判所判決の公表

(1) 営業秘密の不正取得、使用又は開示に関する訴訟において、裁判所は、営業秘密の保有者の申立てに基づき、侵害者の費用負担で、判決に関する情報の周知を図るための適切な措置（判決の全部又は一部の公表を含む）を命じることができる。

(2) 裁判所が第 1 項に基づき命じる措置は、第 10 条に定める営業秘密の秘密保持を確保しなければならない。

(3) 裁判所が第 1 項に基づく措置を命じるか否かを判断し、当該措置の比例性を評価する際には、必要に応じて以下の事項を考慮しなければならない。

(a) 営業秘密の価値

(b) 営業秘密を取得、使用又は開示する際の侵害者の行為

(c) 営業秘密の不正使用又は開示の影響

(d) 侵害者による営業秘密のさらなる不正使用又は開示の可能性

(e) 侵害者に関する情報が個人を特定できるものであるか否か、及び個人を特定しうる場合、当該情報の公表が正当化されるか否か。特に当該措置が侵害者のプライバシー及び名誉に与える可能性のある損害を考慮するものとする

19 本規則の適用を受ける手続

本規則は、以下の要件を満たす手続にのみ適用される。

(a) 本規則の施行後に裁判所に提起されたもの

(b) 営業秘密の不正取得、使用又は開示に関する請求に係るもの

(c) 本規則に定める措置、手続及び救済の適用を求めるもの

サム・ギマ
国務大臣
ビジネス・エネルギー・産業戦略省
2018 年 5 月 15 日

解説書

（この解説書は本規則の一部ではありません）

本規則は、欧州議会及び理事会による 2016 年 6 月 8 日付け指令（EU）2016/943（営業秘密の不正取得、使用及び開示に関する未公開ノウハウ及び事業情報（営業秘密）の保護に関する指令）（OJ L157, 2017 年 6 月 15 日, p.1）（以下「指令」という）の規定を実施するものである。
指令の規定のうち、特に第 II 章及び第 6 条、第 7 条、第 16 条の規定は、英国において、秘密情報保持義務違反（breach of confidence）に関するコモンロー及び衡平法の原則及び法令及び裁判所規則によって既に実施されている。
本規則は、従来の取扱いにおいて欠落が生じている領域、又は英国の各法域における指令の規定の実施を、より透明かつ整合的にすることができる領域を対象とするものである。

規則第 2 条は、指令第 2 条に従って「侵害者」「侵害品」「営業秘密」「営業秘密の保有者」の用語を定義し、さらに「裁判所」の定義を追加する。

規則第 3 条第 1 項は、営業秘密の取得、使用又は開示が不正であるか否かの判断は、秘密保持義務（law of confidence）の原則に基づいて行われることを明確にしている。
秘密保持義務違反に関する訴訟において利用可能な措置、手続及び救済が、本規則に基づくものより広範な保護を営業秘密の保有者に提供する場合、営業秘密の保有者はそれらを申立てることができ、裁判所は、指令第 1 条に言及される保護措置に適合する限り、これを認めることができる（規則第 3 条第 2 項）。
規則第 3 条第 2 項で言及される措置、手続及び救済は、営業秘密の不正取得、使用又は開示に関して、本規則に基づき提供される措置、手続及び救済に追加して、又は代替として提供される（規則第 3 条第 3 項）。

規則第 4 条から第 9 条は、営業秘密の不正取得、使用又は開示に関する請求に係る訴訟手続及び本規則に基づく措置、手続及び救済の適用に関して、適用される出訴期間及び時効を規定する。
規則第 4 条から第 9 条は、指令第 8 条を実施するものである。
イングランド、ウェールズ及び北アイルランドには 6 年の出訴期間が定められている。

スコットランドには 5 年の時効が定められている。
出訴期間又は時効の起算日の決定、及び無能力を理由とする出訴期間又は時効の停止に関する規定が設けられている。

規則第 10 条は、指令第 9 条第 1 項から第 3 項の実施として、訴訟手続における営業秘密の秘密保持を確保することを規定する。

規則第 11 条は、指令第 10 条の実施として、申立てられた侵害者に対する暫定措置について規定している。
引渡しを命じる暫定命令が発せられた場合、営業秘密の保有者は、規則第 14 条第 2 項に基づき当該侵害品が営業秘密の保有者に没収される、又は破壊される命令が発せられるまで、当該侵害品を保持しなければならない。
暫定命令が出された後に請求を提起すべき期間の制限が定められている。
暫定措置に代えて、裁判所は、営業秘密の保有者に対する補償を確保するために、申立てられた侵害者に保証の提供を求めることができる。
また、裁判所は、営業秘密の保有者に対し、申立てられた侵害者が被った損害を補償するための十分な担保を提供するよう求めることもできる。

規則第 12 条は、裁判所が規則第 11 条第 1 項に基づく暫定命令を発する前に考慮すべき事項を規定する。
規則第 12 条は、指令第 11 条第 1 項及び第 2 項を実施するものである。

規則第 13 条は、営業秘密の保有者が定められた期間内に裁判所に訴訟を提起しない場合又はその他一定の状況において、規則第 11 条第 1 項に基づき発せられた命令の取消について規定する。
命じられた措置が取り消された場合、裁判所は、申立てられた侵害者又は損害を被った第三者に対して、適切な補償の支払いを命じることができる。
規則第 13 条は、指令第 11 条第 3 項及び第 5 項を実施するものである。

規則第 14 条は、差止命令又はスコットランドにおける禁止命令（interdict）及び侵害者に課すことができる是正措置について規定する。
これらの措置には、侵害者に対し、自己の費用で侵害品を市場から回収すること、侵害品の侵害性を除去すること、侵害品を破壊すること、又は市場から撤去することが含まれる。
裁判所が当該侵害品の市場からの撤去を命じる場合、当該侵害品を営業秘密の保有者に引き渡し、没収することを命じることができる。
規則第 14 条は、指令第 12 条を実施するものである。

規則第 15 条は、規則第 14 条に基づく命令を発する際に考慮すべき事項を規定し、指令第 13 条第 1 項及び第 2 項を実施するものである。

規則第 16 条は、一定の条件のもとで、裁判所が規則第 14 条に基づく命令に代えて損害賠償の支払いを命じることを可能にする。
これは、指令第 13 条第 3 項を実施するものである。

規則第 17 条は、営業秘密の不正取得、使用又は開示に関する損害賠償を認定する際に考慮すべき要素を定めている。
これは、指令第 14 条を実施するものである。

規則第 18 条は、営業秘密の不正取得、使用又は開示に関する訴訟において、裁判所の判断に関する情報の公表について規定する。
これは、指令第 15 条を実施するものである。

規則第 19 条は、本規則が、本規則施行後に裁判所に提起された、営業秘密の不正取得、使用又は開示に関する請求及び本規則に定める措置、手続及び救済の適用を求める訴訟にのみ適用されることを明確に規定する。

本規則については、民間、任意団体、又は公共部門に対して影響がない、あるいは重大な影響がないと予想されるため、完全な影響評価書は作成されていない。
移行に関する注記（transposition note）は、知的財産庁、（Concept House, Cardiff Road, Newport NP10 8QQ ）で入手可能であり、本規則に付随する注記とともに Legislation UK のウェブサイト（www.legislation.gov.uk） にも掲載される。
また、両院の図書館にも写しが置かれている。

（原文）

National Security Act 2023

1 Obtaining or disclosing protected information

(1) A person commits an offence if—

(a) the person—

(i) obtains, copies, records or retains protected information, or

(ii) discloses or provides access to protected information,

(b) the person's conduct is for a purpose that they know, or having regard to other matters known to them ought reasonably to know, is prejudicial to the safety or interests of the United Kingdom, and

(c) the foreign power condition is met in relation to the person's conduct (see section 31).

(2) In this section "protected information" means any information, document or other article where, for the purpose of protecting the safety or interests of the United Kingdom—

(a) access to the information, document or other article is restricted in any way, or

(b) it is reasonable to expect that access to the information, document or other article would be restricted in any way.

(3) Subsection (1) applies whether the person's conduct takes place in the United Kingdom or elsewhere.

(4) A person who commits an offence under this section is liable on conviction on indictment to imprisonment for life or a fine (or both).

(5) For the purposes of this section—

(a) a person retains protected information if the person retains it in their possession or under their control;

(b) disclosure includes parting with possession.

2 Obtaining or disclosing trade secrets

(1) A person commits an offence if—

(a) the person—

(i) obtains, copies, records or retains a trade secret, or

(ii) discloses or provides access to a trade secret,

(b) the person's conduct is unauthorised,

(c) the person knows, or having regard to other matters known to them ought reasonably to know, that their conduct is unauthorised, and

(d) the foreign power condition is met in relation to the person's conduct (see section 31).

(2) A "trade secret" means any information, document or other article which—

(a) is not generally known by, or available to, persons with knowledge of or expertise in

the field to which it relates,

(b) has actual or potential industrial, economic or commercial value which would be, or could reasonably be expected to be, adversely affected if it became generally known by, or available to, such persons, and

(c) could reasonably be expected to be subject to measures to prevent it becoming generally known by, or available to, such persons (whether or not it is actually subject to such measures).

(3) A person's conduct is unauthorised if the person—

(a) is not entitled to determine whether they may engage in the conduct, and

(b) does not have consent to engage in the conduct from a person who is so entitled.

(4) Subsection (1) applies whether the person's conduct takes place in the United Kingdom or elsewhere (but see subsection (5)).

(5) Conduct within subsection (1) which takes place wholly outside the United Kingdom constitutes an offence only if the trade secret is in the possession or under the control of a UK person.

(6) A "UK person" means—

(a) a United Kingdom national;

(b) an individual who lives in the United Kingdom;

(c) a body incorporated under the law of a part of the United Kingdom;

(d) an unincorporated association formed under the law of a part of the United Kingdom.

(7) A "United Kingdom national" is an individual who is—

(a) a British citizen, a British overseas territories citizen, a British National (Overseas) or a British Overseas citizen,

(b) a person who under the British Nationality Act 1981 is a British subject, or

(c) a British protected person within the meaning of that Act.

(8) A person who commits an offence under this section is liable on conviction on indictment to imprisonment for a term not exceeding 14 years or a fine (or both).

(9) For the purposes of this section—

(a) a person retains a trade secret if they retain it in their possession or under their control;

(b) disclosure includes parting with possession.

31 The foreign power condition

(1) For the purposes of this Part the foreign power condition is met in relation to a person's conduct if—

(a) the conduct in question, or a course of conduct of which it forms part, is carried out for or on behalf of a foreign power, and

(b) the person knows, or having regard to other matters known to them ought reasonably to know, that to be the case.

(2) The conduct in question, or a course of conduct of which it forms part, is in particular to be treated as carried out for or on behalf of a foreign power if—

(a) it is instigated by a foreign power,

(b) it is under the direction or control of a foreign power,

(c) it is carried out with financial or other assistance provided by a foreign power for that purpose, or

(d) it is carried out in collaboration with, or with the agreement of, a foreign power.

(3) Subsections (1)(a) and (2) may be satisfied by a direct or indirect relationship between the conduct, or the course of conduct, and the foreign power (for example, there may be an indirect relationship through one or more companies).

(4) A person's conduct may form part of a course of conduct engaged in by the person alone, or by the person and one or more other persons.

(5) The foreign power condition is also met in relation to a person's conduct if the person intends the conduct in question to benefit a foreign power.

(6) For the purposes of subsection (5) it is not necessary to identify a particular foreign power.

(7) The foreign power condition may be met in relation to the conduct of a person who holds office in or under, or is an employee or other member of staff of, a foreign power, as it may be met in relation to the conduct of any other person.

35 Offences by bodies corporate etc

(1) If an offence under this Part is committed by a body—

(a) with the consent or connivance of an officer of the body, or

(b) due to any neglect on the part of such an officer,

the officer, as well as the body, is guilty of the offence and liable to be proceeded against and punished accordingly.

(2) In this section—

- "body" means a body corporate, a partnership or an unincorporated association other than a partnership;
- "officer of a body"—

(a) in relation to a body corporate, means a director, member of the committee of management, chief executive, manager, secretary or other similar officer of the body, or a person purporting to act in any such capacity;

(b) in relation to a partnership, means a partner or person purporting to act as a partner;

(c) in relation to an unincorporated association other than a partnership, means a person who is concerned in the management or control of the body or purports to act in the capacity of a person so concerned.

(3) In subsection (2) "director" includes—

(a) a person occupying in relation to a body corporate the position of a director (by whatever name called),

(b) a person in accordance with whose directions or instructions (not being advice given in a professional capacity) the directors of that body are accustomed to act, and

(c) a person who has an interest or right in, or in relation to, the body corporate that (whether alone or together with other interests or rights held by the person) enables the person materially to influence the policy of the body corporate.

(4) If the affairs of a body corporate are managed by its members, subsection (1) applies in relation to the acts and defaults of a member in connection with the member's functions of

management as if the member were a director of the body.

(5) The Secretary of State may by regulations provide for the modification of any provision of this section in its application to a body corporate or unincorporated association formed or recognised under the law of a country or territory outside the United Kingdom.

36 Offences committed outside the United Kingdom

(1) Where an offence under this Part may be committed by conduct taking place outside the United Kingdom, it may be so committed—

(a) in the case of conduct by an individual, whatever the nationality of the individual, and

(b) in the case of conduct by a person other than an individual, regardless of whether the body corporate or unincorporated association is formed or recognised under the law of a country or territory outside the United Kingdom.

(2) Subsection (1) is subject to sections 3(6) and 17(6) (commission of offences under sections 3 and 17 by conduct outside the United Kingdom).

(3) Where an offence under this Part is committed outside the United Kingdom—

(a) proceedings for the offence may be taken at any place in the United Kingdom, and

(b) the offence may for all incidental purposes be treated as having been committed at any such place.

(4) In the application of subsection (3) to Scotland, any such proceedings against a person may be taken—

(a) in any sheriff court district in which the person is apprehended or is in custody, or

(b) in such sheriff court district as the Lord Advocate may determine.

(5) "Sheriff court district" is to be read in accordance with the Criminal Procedure (Scotland) Act 1995 (see section 307(1) of that Act).

38 Power to exclude the public from proceedings

If it is necessary in the interests of national security, a court may exclude the public from—

(a) any part of proceedings for an offence under this Part, or

(b) any part of proceedings relating to section 69A of the Sentencing Act 2020 (as inserted by section 19) or to section 20 or 21,

except for the passing of sentence.

（参考和訳）

国家安全保障法 2023 年

1　保護情報の取得又は開示

(1) 以下の各号をいずれも満たす場合、その者は罪を犯したものとする。

(a) その者が次に掲げる行為のいずれかを行ったとき。

(i) 保護秘密を取得し、複製し、記録し、又は保持する行為。

(ii) 保護秘密を開示し、又は第三者に対し、これに対する利用を許す行為。

(b) その者の行為が、英国の安全又は利益を害する目的であることを、その者が知っている又はその者が知っている他の事情を踏まえて合理的に知るべきとき。

(c) 当該行為に関して外国勢力要件（第 31 条参照）が満たされているとき。

(2) 本条において「保護情報」とは、英国の安全又は利益を保護する目的で、以下の各号いずれかに該当する情報、文書又はその他の物をいう。

(a) 当該情報、文書又はその他の物への利用が何らかの方法で制限されているもの。

(b) 当該情報、文書又はその他の物への利用が何らかの方法で制限されることが合理的に予想されるもの。

(3) 第 1 項の規定は、英国国内で行われた行為のみならず、国外で行われた行為にも適用される。

(4) 第 1 項の罪を犯した者は、公判において有罪とされた場合、無期拘禁若しくは罰金又はその両方に処せられる。

(5) 本条の適用においては、以下の各号に定めるところによる。

(a) 「保護情報を保持する」とは、保護情報を自己の占有又は支配下に置くことをいう。

(b) 「開示」には、当該情報の占有を放棄することを含む。

2　営業秘密の取得又は開示

(1) 以下の各号をいずれも満たす場合、その者は罪を犯したものとする。

(a) その者が次に掲げる行為のいずれかを行ったとき。

(i) 営業秘密を取得し、複製し、記録し、又は保持する行為。

(ii) 営業秘密を開示し、又は第三者に対しこれに対する利用を許す行為。

(b) その者の行為が無権限であるとき。

(c) その者が、その行為が無権限であることを知っている又はその者が知っている他の事情を踏まえて合理的に知るべきとき。

(d) 当該行為に関して外国勢力要件（第 31 条参照）が満たされているとき

(2) 本条において「営業秘密」とは、以下の各号の要件を全て満たす情報、文書又はその他の物をいう。

(a) 当該情報等が、関連分野の知識若しくは専門性を有する者に一般に知られていない、又は利用不可能であること。

(b) 当該情報等が、実際又は潜在的な産業的、経済的又は商業的価値を有し、関連分野の知識若しくは専門性を有する者に一般に知られ又は利用可能となった場合、その価値が損なわれるおそれが実際に又は合理的に予想されること。

(c) 当該情報等が、関連分野の知識若しくは専門性を有する者に一般に知られ、又は利用可能となることを防止するための措置が取られることが合理的に想定されること（実際にそのような措置が取られているか否かを問わない）。

(3) 本条において「無権限」とは、以下の各号いずれにも該当する場合をいう。

(a) その者が当該行為を行うか否かを決定する権限を有しないとき。

(b) その者が当該行為を行う権限を有する者から当該行為を行う同意を得ていないとき。

(4) 第 1 項の規定は、英国国内で行われた行為のみならず、国外で行われた行為にも適用される。但し、次項の要件を満たす場合に限る。

(5) 第 1 項に規定する行為が全て英国国外で行われた場合、当該営業秘密が英国人の占有又は支配下にあるときに限り、犯罪が成立する。

(6) 本条において「英国人」とは、次に掲げる者をいう。

(a) 英国国民

(b) 英国に居住する個人

(c) 英国法に基づき設立された法人

(d) 英国法に基づき設立された非法人団体

(7) 本条において「英国国民」とは、次に掲げる者をいう。

(a) 英国市民、英国海外領土市民、英国国民（海外）又は英国海外市民

(b) 1981 年英国国籍法に規定される英国臣民

(c) 同法に規定される英国保護対象者

(8) 本条の罪を犯した者は、公判において有罪とされた場合、十四年以下の拘禁若しくは罰金又はその両方に処せられる。

(9) 本条の適用においては、以下の各号に定めるところによる。

(a) 「営業秘密を保持する」とは、営業秘密を自己の占有又は支配下に置くことをいう。

(b) 「開示」には、営業秘密の占有を放棄することを含む。

31　外国勢力要件

(1)　本編の適用において、以下の各号をいずれも満たす場合、当該行為に関して外国勢力要件が満たされるものとする。

(a)　当該行為又はその一連の行為が、外国勢力のため又は外国勢力に代わって行われる場合。

(b)　その者が、その事実を知っている又はその者が知っている他の事情を踏まえて合理的に知るべきとき。

(2)　当該行為又はその一連の行為は、特に以下の場合、外国勢力のため又は外国勢力に代わって行われたものとみなす。

(a)　外国勢力に唆されて行われたとき。

(b)　外国勢力の指揮又は管理下で行われたとき。

(c)　外国勢力から資金又はその他の援助を受けて行われたとき。

(d)　外国勢力との協力又は同意のもとで行われたとき。

(3)　第 1 条(a)及び第 2 項の要件は、当該行為又はその一連の行為と外国勢力との間に、直接的又は間接的な関係がある場合にも満たされうる（一社又は複数の会社を介した間接的関係がある場合等）。

(4)　当該行為は、単独で行われたものと、二人以上の者が共同で行ったものとを問わない。

(5)　外国勢力要件は、行為者が当該行為を外国勢力の利益のためにする意図を有する場合にも満たされる。

(6)　第 5 項の適用においては、どの外国勢力であるかを特定することを要しない。

(7)　外国勢力要件は、外国勢力のもとで職に就いている者、又はその職員・従業員・スタッフである者の行為に関しても、その他の者の行為と同様に適用される。

35　法人等による犯罪

(1)　本編に規定する犯罪が法人等の団体によって行われた場合において、次のいずれかに該当するときは、当該団体の役員もまた当該犯罪について団体と同様に責任を負い、起訴及び処罰される。

(a)　当該団体の役員の同意又は黙認により当該犯罪が行われたとき。

(b)　当該団体の役員の注意義務違反により当該犯罪が行われたとき。

(2)　本条において、

「団体」とは、法人、パートナーシップ又はパートナーシップ以外の非法人団体をいう。

「団体の役員」とは、次のいずれかに該当する者をいう。

(a)　法人の場合は、取締役、経営委員会の構成員、最高経営責任者、管理者、秘書その他これに類する役員、又はその地位にあるかのように振る舞う者

(b)　パートナーシップの場合は、パートナー又はパートナーであるかのように振

る舞う者

(c) パートナーシップ以外の非法人団体の場合は、当該団体の管理若しくは運営に関与する者、又はそのような地位にあるかのように振る舞う者

(3) 前項における「取締役」には、次に掲げる者を含む。

(a) 名称の如何を問わず、法人において取締役の地位にある者

(b) 当該法人の取締役を、その指示又は命令（専門的助言を除く）に従わせている者

(c) 当該法人に対して実質的に影響力を行使できるほどの利害関係や権利を有している者（単独に限らず、他の権利や利害と合わせた場合も含む）

(4) 法人の業務がその構成員によって運営される場合、当該構成員が管理機能に関連して行った行為又は不作為について、当該構成員を取締役とみなして、第 1 項の規定を適用する。

(5) 国務大臣は、英国国外の国又は地域の法の下に設立され若しくは認められた法人又は非法人団体への本条の適用に関し、本条の規定を修正する規則を制定することができる。

36 英国外で行われた犯罪

(1) 本編に規定する犯罪が英国国外で行われた行為によって成立しうる場合、以下のとおりとする。

(a) 個人による行為である場合、その者の国籍を問わない。

(b) 個人以外の者による行為である場合、当該法人又は非法人団体が英国以外の国又は地域の法の下に設立され又は認められているか否かを問わない。

(2) 前項の規定は、第 3 条第 6 項及び第 17 条第 6 項（英国国外で行われた行為による第 3 条及び第 17 条の犯罪の成立）に従う。

(3) 本編に規定する犯罪が英国国外で行われた場合には、以下のとおりとする。

(a) 当該犯罪に係る訴追手続は、英国国内のいずれの地においても行うことができる。

(b) 当該犯罪は、付随的な目的において、英国国内のいずれの場所で行われたものとしてみなすことができる。

(4) 前項の規定をスコットランドに適用する場合においては、当該行為者に対する訴追手続は、次のいずれかの地において行うことができる。

(a) 当該行為者が逮捕され、又は拘禁されているシェリフ裁判所管轄区

(b) 法務官が定めるシェリフ裁判所管轄区

(5) 本条における「シェリフ裁判所管轄区（sheriff court district）」は、1995 年刑事手続（スコットランド）法第 307 条第 1 項の規定に従って解されるものとする。

38　手続の非公開

国家安全保障の利益のために必要がある場合、裁判所は、次に掲げる手続の一部から、一般の者を排除することができる。但し、判決の言渡しについては、この限りでない。

(a)　本編に規定する犯罪に係る手続の一部

(b)　2020 年量刑法第 69A 条（第 19 条により挿入されたもの）又は第 20 条若しくは第 21 条に関する手続の一部

3 Computer Misuse Act 1990

（原文）

Computer Misuse Act 1990
1990 CHAPTER 18

An Act to make provision for securing computer material against unauthorised access or modification; and for connected purposes.

[29th June 1990]

Be it enacted by the Queen's most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same, as follows:—

Computer misuse offences

1 Unauthorised access to computer material.

(1) A person is guilty of an offence if—

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer , or to enable any such access to be secured;

(b) the access he intends to secure , or to enable to be secured, is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at—

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

(3) A person guilty of an offence under this section shall be liable—

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding the general limit in a magistrates' court or to a fine not exceeding the statutory maximum or to both;

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding F512 months or to a fine not exceeding the statutory maximum or to both;

(c) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both.

2 Unauthorised access with intent to commit or facilitate commission of further offences.

(1) A person is guilty of an offence under this section if he commits an offence under section 1 above ("the unauthorised access offence") with intent—

(a) to commit an offence to which this section applies; or

(b) to facilitate the commission of such an offence (whether by himself or by any other person);

and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

(2) This section applies to offences—

(a) for which the sentence is fixed by law; or

(b) for which a person who has attained the age of twenty-one years (eighteen in relation to England and Wales) and has no previous convictions may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the M1Magistrates' Courts Act 1980).

(3) It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.

(4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.

(5) A person guilty of an offence under this section shall be liable—

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding the general limit in a magistrates' court or to a fine not exceeding the statutory maximum or to both;

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(c) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

3 Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.

(1) A person is guilty of an offence if—

(a) he does any unauthorised act in relation to a computer;

(b) at the time when he does the act he knows that it is unauthorised; and

(c) either subsection (2) or subsection (3) below applies.

(2) This subsection applies if the person intends by doing the act—

(a) to impair the operation of any computer;

(b) to prevent or hinder access to any program or data held in any computer; or

(c) to impair the operation of any such program or the reliability of any such data; or

(d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done.

(3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (c) of subsection (2) above.

(4) The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to—

(a) any particular computer;

(b) any particular program or data; or

(c) a program or data of any particular kind.

(5) In this section—

(a) a reference to doing an act includes a reference to causing an act to be done;

(b) "act" includes a series of acts;

(c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily.

(6) A person guilty of an offence under this section shall be liable—

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding the general limit in a magistrates' court or to a fine not exceeding the statutory maximum or to both;

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(c) on conviction on indictment, to imprisonment for a term not exceeding ten years or to a fine or to both.

3ZA Unauthorised acts causing, or creating risk of, serious damage

(1) A person is guilty of an offence if—

(a) the person does any unauthorised act in relation to a computer;

(b) at the time of doing the act the person knows that it is unauthorised;

(c) the act causes, or creates a significant risk of, serious damage of a material kind; and

(d) the person intends by doing the act to cause serious damage of a material kind or is reckless as to whether such damage is caused.

(2) Damage is of a "material kind" for the purposes of this section if it is—

(a) damage to human welfare in any place;

(b) damage to the environment of any place;

(c) damage to the economy of any country; or

(d) damage to the national security of any country.

(3) For the purposes of subsection (2)(a) an act causes damage to human welfare only if it causes—

(a) loss to human life;

(b) human illness or injury;

(c) disruption of a supply of money, food, water, energy or fuel;

(d) disruption of a system of communication;

(e) disruption of facilities for transport; or

(f) disruption of services relating to health.

(4) It is immaterial for the purposes of subsection (2) whether or not an act causing damage—

(a) does so directly;

(b) is the only or main cause of the damage.

(5) In this section—

(a) a reference to doing an act includes a reference to causing an act to be done;

(b) "act" includes a series of acts;

(c) a reference to a country includes a reference to a territory, and to any place in, or part or region of, a country or territory.

(6) A person guilty of an offence under this section is (unless subsection (7) applies) liable, on conviction on indictment, to imprisonment for a term not exceeding 14 years, or to a fine, or to both.

(7) Where an offence under this section is committed as a result of an act causing or creating a significant risk of—

(a) serious damage to human welfare of the kind mentioned in subsection (3)(a) or (3)(b), or

(b) serious damage to national security,

a person guilty of the offence is liable, on conviction on indictment, to imprisonment for life, or to a fine, or to both.

3A Making, supplying or obtaining articles for use in offence under section 1, 3 or 3ZA

(1) A person is guilty of an offence if he makes, adapts, supplies or offers to supply any article intending it to be used to commit, or to assist in the commission of, an offence under section 1, 3 or 3ZA.

(2) A person is guilty of an offence if he supplies or offers to supply any article believing that it is likely to be used to commit, or to assist in the commission of, an offence under section 1, 3 or 3ZA.

(3) A person is guilty of an offence if he obtains any article—

(a) intending to use it to commit, or to assist in the commission of, an offence under section 1, 3 or 3ZA, or

(b) with a view to

its being supplied for use to commit, or to assist in the commission of, an offence under section 1, 3 or 3ZA.

(4) In this section " article " includes any program or data held in electronic form.

(5) A person guilty of an offence under this section shall be liable—

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding the general limit in a magistrates' court or to a fine not exceeding the statutory maximum or to both;

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(c) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both.

4 Territorial scope of offences under this Act.

(1) Except as provided below in this section, it is immaterial for the purposes of any offence under section 1, 3 or 3ZA above—

(a) whether any act or other event proof of which is required for conviction of the offence occurred in the home country concerned; or

(b) whether the accused was in the home country concerned at the time of any such act or event.

(2) Subject to subsection (3) below, in the case of such an offence at least one significant link with domestic jurisdiction must exist in the circumstances of the case for the offence to be committed.

(3) There is no need for any such link to exist for the commission of an offence under section 1 above to be established in proof of an allegation to that effect in proceedings for an offence under section 2 above.

(4) Subject to section 8 below, where—

(a) any such link does in fact exist in the case of an offence under section 1 above; and

(b) commission of that offence is alleged in proceedings for an offence under section 2 above;

section 2 above shall apply as if anything the accused intended to do or facilitate in any place outside the home country concerned which would be an offence to which section 2 applies if it took place in the home country concerned were the offence in question.

(4A) It is immaterial for the purposes of an offence under section 3A whether the accused was in the home country concerned at the time of any act or other event proof of which is required for conviction of the offence if there is a significant link with domestic jurisdiction in relation to the offence.

(5) This section is without prejudice to any jurisdiction exercisable by a court in Scotland apart from this section.

(6) References in this Act to the home country concerned are references—

(a)in the application of this Act to England and Wales, to England and Wales;

(b)in the application of this Act to Scotland, to Scotland; and

(c)in the application of this Act to Northern Ireland, to Northern Ireland.

5 Significant links with domestic jurisdiction.

(1) The following provisions of this section apply for the interpretation of section 4 above.

(1A) In relation to an offence under section 1, 3, 3ZA or 3A, where the accused was in a country outside the United Kingdom at the time of the act constituting the offence there is a significant link with domestic jurisdiction if—

(a) the accused was a United Kingdom national at that time; and

(b) the act constituted an offence under the law of the country in which it occurred.

(1B) In subsection (1A)—

"country" includes territory;
"United Kingdom national" means an individual who is—

(a) a British citizen, a British overseas territories citizen, a British National (Overseas) or a British Overseas citizen;

(b) a person who under the British Nationality Act 1981 is a British subject; or

(c) a British protected person within the meaning of that Act.

(2) In relation to an offence under section 1, either of the following is a significant link with domestic jurisdiction—

(a) that the accused was in the home country concerned at the time when he did the act which caused the computer to perform the function; or

(b) that any computer containing any program or data to which the accused by doing that act secured or intended to secure unauthorised access, or enabled or intended to enable unauthorised access to be secured, was in the home country concerned at that time.

(3) In relation to an offence under section 3, either of the following is a significant link with domestic jurisdiction—

(a) that the accused was in the home country concerned at the time when he did the unauthorised act (or caused it to be done) ; or

(b) that the unauthorised act was done in relation to a computer in the home country concerned.

(3A) In relation to an offence under section 3ZA, any of the following is also a significant link with domestic jurisdiction—

(a) that the accused was in the home country concerned at the time when he did the unauthorised act (or caused it to be done);

(b) that the unauthorised act was done in relation to a computer in the home country concerned;

(c) that the unauthorised act caused, or created a significant risk of, serious damage of a material kind (within the meaning of that section) in the home country concerned.

6 Territorial scope of inchoate offences related to offences under this Act.

(1) On a charge of conspiracy to commit an offence under this Act the following questions are immaterial to the accused's guilt—

(a) the question where any person became a party to the conspiracy; and

(b) the question whether any act, omission or other event occurred in the home country concerned.

(2) On a charge of attempting to commit an offence under this Act the following questions are immaterial to the accused's guilt—

(a) the question where the attempt was made; and

(b) the question whether it had an effect in the home country concerned.

(3) . . . . . .

(4) This section does not extend to Scotland.

7 Territorial scope of inchoate offences related to offences under external law corresponding to offences under sections 1 to 3.

(1) . . . . . .

(2) . . . . . .

(3) The following subsections shall be inserted after section 1(1) of the M2Criminal Attempts Act 1981—

"(1A)Subject to section 8 of the Computer Misuse Act 1990 (relevance of external law), if this subsection applies to an act, what the person doing it had in view shall be treated as an offence to which this section applies.

(1B) Subsection (1A) above applies to an act if—

(a) it is done in England and Wales; and

(b) it would fall within subsection (1) above as more than merely preparatory to the commission of an offence under section 3 of the Computer Misuse Act 1990 but for the fact that the offence, if completed, would not be an offence triable in England and Wales."

(4) . . . . . .

8 Relevance of external law.

(1) A person is guilty of an offence triable by virtue of section 4(4) above only if what he intended to do or facilitate would involve the commission of an offence under the law in force where the whole or any part of it was intended to take place.

(2) . . . . . .

(3) A person is guilty of an offence triable by virtue of section 1(1A) of the M3Criminal Attempts Act 1981 . . . only if what he had in view would involve the commission of an offence under the law in force where the whole or any part of it was intended to take place.

(4) Conduct punishable under the law in force in any place is an offence under that law for the purposes of this section, however it is described in that law.

(5) Subject to subsection (7) below, a condition specified in subsection (1) or (3) above shall be taken to be satisfied unless not later than rules of court may provide the defence serve on the prosecution a notice—

(a) stating that, on the facts as alleged with respect to the relevant conduct, the condition is not in their opinion satisfied;

(b) showing their grounds for that opinion; and

(c) requiring the prosecution to show that it is satisfied.

(6) In subsection (5) above "the relevant conduct" means—

(a) where the condition in subsection (1) above is in question, what the accused intended to do or facilitate;

(b) . . . . . .

(c) where the condition in subsection (3) above is in question, what the accused had in view.

(7) The court, if it thinks fit, may permit the defence to require the prosecution to show that the condition is satisfied without the prior service of a notice under subsection (5) above.

(8) If by virtue of subsection (7) above a court of solemn jurisdiction in Scotland permits the defence to require the prosecution to show that the condition is satisfied, it shall be competent for the prosecution for that purpose to examine any witness or to put in evidence any production not included in the lists lodged by it.

(9) In the Crown Court the question whether the condition is satisfied shall be decided by the judge alone.

(10) In the High Court of Justiciary and in the sheriff court the question whether the condition is satisfied shall be decided by the judge or, as the case may be, the sheriff alone.

9 British citizenship immaterial.

(1) Except as provided by section 5(1A),In any proceedings brought in England and Wales in respect of any offence to which this section applies it is immaterial to guilt whether or not the accused was a British citizen at the time of any act, omission or other event proof of which is required for conviction of the offence.

(2) This section applies to the following offences—

(a) any offence under this Act ;

(b) . . . . . .

(c) any attempt to commit an offence under this Act; and

(d) . . . . . .

Miscellaneous and general

10 Savings

Sections 1 to 3A have effect without prejudice to the operation—

(a) in England and Wales of any enactment relating to powers of inspection, search or seizureor of any other enactment by virtue of which the conduct in question is authorised or required; and

(b) in Scotland of any enactment or rule of law relating to powers of examination, search or seizureor of any other enactment or rule of law by virtue of which the conduct in question is authorised or required

and nothing designed to indicate a withholding of consent to access to any program or data from persons as enforcement officers shall have effect to make access unauthorised for the purposes of any of those sections.In this section—“ enactment ” means any enactment, whenever passed or made, contained in—

(a) an Act of Parliament;

(b) an Act of the Scottish Parliament;

(c) a Measure or Act of the National Assembly for Wales;

(d) an instrument made under any such Act or Measure;

(e) any other subordinate legislation (within the meaning of the Interpretation Act 1978);

" enforcement officer " means a constable or other person charged with the duty of investigating offences; and withholding consent from a person "as" an enforcement officer of any description includes the operation, by the person entitled to control access, of rules whereby enforcement officers of that description are, as such, disqualified from membership of a class of persons who are authorised to have access.

11 Proceedings for offences under section 1.

. . . . . .

12 Conviction of an offence under section 1 in proceedings for an offence under section 2 or 3.

. . . . . .

13 Proceedings in Scotland.

(1) A sheriff shall have jurisdiction in respect of an offence under section 1 or 2 above if—

(a) the accused was in the sheriffdom at the time when he did the act which caused the computer to perform the function; or

(b) any computer containing any program or data to which the accused by doing that act secured or intended to secure unauthorised access, or enabled or intended to enable unauthorised access to be secured, was in the sheriffdom at that time.

(2) A sheriff shall have jurisdiction in respect of an offence under section 3 above if—

(a) the accused was in the sheriffdom at the time when he did the unauthorised act (or caused it to be done) ; or

(b) the unauthorised act was done in relation to a computer in the sheriffdom.

(2A) A sheriff shall have jurisdiction in respect of an offence under section 3ZA above if—

(a) the accused was in the sheriffdom at the time when he did the unauthorised act (or caused it to be done), or

(b) the computer in relation to which the unauthorised act was done was in the sheriffdom at that time.

(2B) A sheriff shall have jurisdiction in respect of an offence under section 3A above if—

(a) the accused was in the sheriffdom at the time when—

(i) he made, adapted, supplied or offered to supply the article intending it to be used as mentioned in subsection (1) of that section,

(ii) he supplied or offered to supply the article believing that it would be used as mentioned in subsection (2) of that section, or

(iii) he obtained the article intending to use it, or with a view to its being supplied for use, as mentioned in subsection (3) of that section; or

(b) the offence related to the commission of an offence under section 1, 3 or 3ZA above (in the way described in subsections (1) to (3) of section 3A above) and any computer as mentioned in subsection (1)(b), (2)(b) or (2A)(b) of this section was in the sheriffdom at the time the accused carried out the act constituting the offence under section 3A above.

(3) . . . . . .

(4) . . . . . .

(5) . . . . . .

(6) . . . . . .

(7) . . . . . .

(8) In proceedings in which a person is charged with an offence under section 2 or 3 above and is found not guilty or is acquitted of that charge, he may be found guilty of an offence under section 1 above if on the facts shown he could have been found guilty of that offence in proceedings for that offence . . . .

(9) Subsection (8) above shall apply whether or not an offence under section 1 above has been libelled in the complaint or indictment.

(10) A person found guilty of an offence under section 1 above by virtue of subsection (8) above shall be liable, in respect of that offence, only to the penalties set out in section 1.

(10A) Where an offence under section 1, 3, 3ZA or 3A above is committed outside Scotland, the person committing the offence may be prosecuted, tried and punished for the offence—

(a) in any sheriff court district in Scotland in which the person is apprehended or is in custody, or

(b) in such sheriff court district as the Lord Advocate may direct,

as if the offence had been committed in that district; and the offence is, for all purposes incidental to or consequential on the trial or punishment, deemed to have been committed in that district.

(11) This section extends to Scotland only.

14 Search warrants for offences under section 1.

. . . . . .

15 Extradition where Schedule 1 to the Extradition Act 1989 applies.

. . . . . .

16 Application to Northern Ireland.

(1) The following provisions of this section have effect for applying this Act in relation to Northern Ireland with the modifications there mentioned.

(1A) In section 1(3)(a)—

(a) the reference to England and Wales shall be read as a reference to Northern Ireland; and

(b) the reference to the general limit in a magistrates' court shall be read as a reference to six months.

(2) In section 2(2)(b)—

(a) the reference to England and Wales shall be read as a reference to Northern Ireland; and

(b) the reference to section 33 of the M4Magistrates' Courts Act 1980 shall be read as a reference to Article 46(4) of the M5Magistrates' Courts (Northern Ireland) Order 1981.

(2A) In section 2(5)(a)—

(a) the reference to England and Wales shall be read as a reference to Northern Ireland; and

(b) the reference to the general limit in a magistrates' court shall be read as a reference to six months.

(3) . . . . . .

(3A) In section 3(6)(a)—

(a) the reference to England and Wales shall be read as a reference to Northern Ireland; and

(b) the reference to the general limit in a magistrates' court shall be read as a reference to six months.

(3B) In section 3A(5)(a)—

(a) the reference to England and Wales shall be read as a reference to Northern Ireland; and

(b) the reference to the general limit in a magistrates' court shall be read as a reference to six months.

(4) Subsection (7) below shall apply in substitution for subsection (3) of section 7; . . . .

(5) . . . . . .

(6) . . . . . .

(7) The following paragraphs shall be inserted after Article 3(1) of that Order—

"(1A)Subject to section 8 of the Computer Misuse Act 1990 (relevance of external law), if this paragraph applies to an act, what the person doing it had in view shall be treated as an offence to which this Article applies.

(1B) Paragraph (1A) above applies to an act if—

(a) it is done in Northern Ireland; and

(b) it would fall within paragraph (1) as more than merely preparatory to the commission of an offence under section 3 of the Computer Misuse Act 1990 but for the fact that the offence, if completed, would not be an offence triable in Northern Ireland.".

(8) In section 8—

(a) . . . . . .

(b) the reference in subsection (3) to section 1(1A) of the M6Criminal Attempts Act 1981 shall be read as a reference to Article 3(1A) of that Order.

(9) The references in sections 9(1) and 10 to England and Wales shall be read as references to Northern Ireland.

(9A) In section 10 the definition of "enactment" shall be read as including a reference to an enactment, whenever passed or made, contained in Northern Ireland legislation or in an instrument made under such legislation.

(10) . . . . . .

16A Northern Ireland: search warrants for offences under section 1

(1) Where a county court judge is satisfied by information on oath given by a constable that there are reasonable grounds for believing—

(a) that an offence under section 1 above has been or is about to be committed in any premises, and

(b) that evidence that such an offence has been or is about to be committed is in those premises,

he may issue a warrant authorising a constable to enter and search the premises, using such reasonable force as is necessary.

(2) The power conferred by subsection (1) above does not extend to authorising a search for material of the kinds mentioned in Article 11(2) of the Police and Criminal Evidence (Northern Ireland) Order 1989 (privileged, excluded and special procedure material).

(3) A warrant under this section—

(a) may authorise persons to accompany any constable executing the warrant; and

(b) remains in force for twenty-eight days from the date of its issue.

(4) In exercising a warrant issued under this section a constable may seize an article if he reasonably believes that it is evidence that an offence under section 1 above has been or is about to be committed.

(5) In this section " premises " includes land, buildings, movable structures, vehicles, vessels, aircraft and hovercraft.

(6) This section extends only to Northern Ireland.

17 Interpretation.

(1) The following provisions of this section apply for the interpretation of this Act.

(2) A person secures access to any program or data held in a computer if by causing a computer to perform any function he—

(a) alters or erases the program or data;

(b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

(c) uses it; or

(d)has it output from the computer in which it is held (whether by having it displayed or in any other manner);

and references to access to a program or data (and to an intent to secure such access or to enable such access to be secured) shall be read accordingly.

(3) For the purposes of subsection (2)(c) above a person uses a program if the function he causes the computer to perform—

(a) causes the program to be executed; or

(b) is itself a function of the program.

(4) For the purposes of subsection (2)(d) above—

(a) a program is output if the instructions of which it consists are output; and

(b) the form in which any such instructions or any other data is output (and in particular whether or not it represents a form in which, in the case of instructions, they are capable of being executed or, in the case of data, it is capable of being processed by a computer) is immaterial.

(5) Access of any kind by any person to any program or data held in a computer is unauthorised if—

(a) he is not himself entitled to control access of the kind in question to the program or data; and

(b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled but this subsection is subject to section 10.

(6) References to any program or data held in a computer include references to any program or data held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing any program or data held in any such medium.

(7). . . . . .

(8) An act done in relation to a computer is unauthorised if the person doing the act (or causing it to be done)—

(a) is not himself a person who has responsibility for the computer and is entitled to determine whether the act may be done; and

(b) does not have consent to the act from any such person.

In this subsection " act " includes a series of acts.

(9) References to the home country concerned shall be read in accordance with section 4(6) above.

(10) References to a program include references to part of a program.

18 Citation, commencement etc.

(1) This Act may be cited as the Computer Misuse Act 1990.

(2) This Act shall come into force at the end of the period of two months beginning with the day on which it is passed.

(3) An offence is not committed under this Act unless every act or other event proof of which is required for conviction of the offence takes place after this Act comes into force.

（参考和訳）

1990 年コンピュータ不正使用防止法

(Computer Misuse Act 1990)

1990 年第 18 章

コンピュータ上の資料を不正なアクセス又は改ざんから保護するための規定を設けること、及びその他関連する事項を定めるための法律。

[1990 年 6 月 29 日]

女王陛下の勅命により、聖職貴族院・世俗貴族院及び庶民院の助言と同意を得て、次のとおり制定する。

コンピュータ不正使用に関する犯罪

1　コンピュータ資料への不正アクセス

(1)　以下の要件を全て満たす場合、その者は罪を犯したものとする。

(a)　コンピュータに何らかの機能を実行させることにより、他のコンピュータに保存されているプログラム若しくはデータへの無権限のアクセスをうること、又はそのような無権限のアクセスを可能にすることを意図すること。

(b)　行為者が取得しようとする、又は可能にしようとするアクセスが無権限であること。

(c)　当該コンピュータに当該機能を実行させる時点で、行為者が当該アクセスが無権限であることを知っていること。

(2)　本条に規定される罪を犯すために必要な故意は、以下のいずれも特定する必要はない。

(a)　特定のプログラム又はデータを対象とすること。

(b)　特定の種類のプログラム又はデータを対象とすること。

(c)　特定のコンピュータに保存されているプログラム又はデータを対象とすること。

(3)　本条に規定される罪を犯した者は、以下の刑に処する。

(a)　イングランド及びウェールズの略式裁判の場合、略式裁判の法定上限以下の拘禁若しくは罰金又はその両方。

(b)　スコットランドの略式裁判の場合、12 か月を超えない拘禁若しくは法定上限以下の罰金又はその両方。

(c)　公判による有罪判決の場合、2 年以下の拘禁若しくは罰金又はその両方。

2　他の犯罪の実行又はその実行を容易にする目的での無権限アクセス

(1) 以下のいずれかの意図を有して第 1 条に規定する罪（「不正アクセス罪」）を犯した場合、本条に規定される罪が成立する。

(a) 本条が適用される犯罪を実行する意図

(b) 当該犯罪の実行を幇助する意図（自己又は第三者が行う場合を問わない）

当該行為者が実行又は幇助しようとする罪を、以下「関連犯罪」という。

(2) 本条が適用される犯罪は、次のとおりとする。

(a) 法律で刑期が定められている犯罪

(b) 21 歳に達した者（イングランド及びウェールズでは 18 歳に達した者）で前科のない者が、5 年以上の拘禁刑が科されうる犯罪（イングランド及びウェールズにおいては、1980 年治安判事裁判所法（Magistrates' Courts Act）第 33 条による制限がなければ科されうる犯罪）

(3) 本条の適用において、関連犯罪が不正アクセス罪と同一機会に実行されるか、将来の機会に実行されるかは問わない。

(4) 「関連犯罪」の実行が事実上不可能な場合であっても、本条に規定する罪を犯しうる。

(5) 本条に規定する罪を犯した者は、以下の刑に処する。

(a) イングランド及びウェールズの略式裁判の場合、略式裁判の法定上限以下の拘禁若しくは罰金又はその両方。

(b) スコットランドの略式裁判の場合、12 か月を超えない拘禁若しくは法定上限以下の罰金又はその両方。

(c) 公判による有罪判決の場合、5 年以下の拘禁若しくは罰金又はその両方。

3　コンピュータの運用等を妨害する意図又は妨害する危険性を認識しながら行う不正行為

(1) 以下の要件を全て満たす場合、その者は罪を犯したものとする。

(a) コンピュータに対して権限なき行為を行ったこと。

(b) 当該行為を行う時点で、行為者が、当該行為が無権限であることを知っていること。

(c) 以下の第 2 項又は第 3 項のいずれかに該当すること。

(2) 以下のいずれかの意図で当該行為を行った場合、本項が適用される。

(a) コンピュータの運用を妨害すること。

(b) コンピュータに保存されているプログラム若しくはデータへのアクセスを妨げ、又は阻害すること。

(c) プログラムの運用又はデータの信頼性を損なうこと。

(d) 上記(a)から(c)に掲げる行為のいずれかを可能にすること。

(3) 行為者が、当該行為により第 2 項各号の結果が生じる可能性があることを認識している場合、本項が適用される。

(4) 第 2 項の意図又は第 3 項の認識は、以下のいずれも特定する必要はない。

(a) 特定のコンピュータを対象とすること。

(b) 特定のプログラムやデータを対象とすること。

(c) 特定の種類のプログラム又はデータを対象とすること。

(5) 本条において

(a) 「行為を行う」には、第三者に行為を行わせることを含む。

(b) 「行為」には、一連の行為を含む。

(c) 「損なう」、「妨げる」又は「阻害する」には、一時的にこれを行うことを含む。

(6) 本条に規定される罪を犯した者は、以下の刑に処す。

(a) イングランド及びウェールズの略式裁判の場合、略式裁判の法定上限以下の拘禁若しくは罰金又はその両方。

(b) スコットランドの略式裁判の場合、12 か月を超えない拘禁若しくは法定上限以下の罰金又はその両方。

(c) 公判による有罪判決の場合、10 年以下の拘禁若しくは罰金又はその両方。

3ZA 重大な損害を生じさせ、又はその危険を生じさせる不正行為

(1) 以下の要件を全て満たす場合、その者は罪を犯したものとする。

(a) コンピュータに対して権限なき行為を行ったこと。

(b) 当該行為を行う時点で、行為者が、当該行為が無権限であることを知っていること。

(c) 当該行為が実質的に重大な損害を生じさせること、又はそのような損害を生じさせる重大な危険を生じさせること。

(d) 行為者が、当該行為により重大な損害を生じさせる意図を有していること、又はそのような損害が発生する危険性を認識していること。

(2) 本条における「重大な損害」とは、以下のいずれかに該当するものをいう。

(a) 人の福祉に対する損害（損害の生じる場所を問わない）

(b) 環境に対する損害（損害の生じる場所を問わない）

(c) 国家経済に対する損害（損害の生じる国を問わない）

(d) 国家安全保障に対する損害（損害の生じる国を問わない）

(3) 第 2 項(a)における「人間の福祉に対する損害」とは、以下のいずれかに限る。

(a) 人命の喪失

(b) 人の疾病又は傷害

(c) 金銭、食料、水、エネルギー又は燃料の供給の途絶

(d) 通信システムの途絶

(e) 輸送施設の途絶

(f) 保健サービスの途絶

(4) 第 2 項の適用において、損害を生じさせる行為が以下のいずれかであるかは問わない。

(a) 直接的か否か。

(b) 当該行為が唯一又は主要な原因であるか否か。

(5) 本条において

(a) 「行為を行う」には、行為を行わせることを含む。

(b) 「行為」には、一連の行為を含む。

(c) 「国」には、領土及び国又は領土のいかなる場所、部分、地域を含む。

(6) 本条に定める罪を犯した者は、第 7 項が適用される場合を除き、公判による有罪判決の場合、14 年以下の拘禁若しくは罰金又はその両方を科す。

(7) 本条に規定する罪が、以下のいずれかを引き起こした場合又はその危険性を生じさせた場合、その者は、公判で有罪判決を下された場合、無期拘禁若しくは罰金又はその両方に処する。

(a) 第 3 項(a)又は(b)に規定する人の福祉に対する重大な損害

(b) 国家安全保障に対する重大な損害

3A 第 1 条、第 3 条又は第 3ZA 条に基づく罪に使用する物品の製造、供給又は取得

(1) 第 1 条、第 3 条、又は第 3ZA 条に基づく犯罪の実行又は幇助に使用されることを意図して、何らかの物品を製造、改変、供給、又は供給の申出を行った場合、その者は罪を犯したものとする。

(2) 何らかの物品を供給又は供給を申し出るに際して、その物品が第 1 条、第 3 条、又は第 3ZA 条に基づく犯罪の実行又は幇助に使用されるおそれがあると信じて、当該物品の供給又は供給の申出を行った場合も、その者は罪を犯したものとする。

(3) 以下のいずれかの意図で何らかの物品を取得した場合も罪を犯したものする。

(a) 第 1 条、第 3 条、又は第 3ZA 条に規定する罪の実行又は幇助のために、当該物品を使用する意図

(b) 当該物品を供給し、第 1 条、第 3 条、又は第 3ZA 条に基づく犯罪の実行又は幇助のために当該物品が使用される目的

(4) 本条において「物品」には、電子形式で保存されるプログラム又はデータを含む。

(5) 本条に規定される罪を犯した者は、以下の刑に処する。

(a) イングランド及びウェールズの略式裁判の場合、略式裁判の法定上限以下の拘禁若しくは罰金又はその両方。

(b) スコットランドの略式裁判の場合、12 か月を超えない拘禁若しくは法定上

限以下の罰金又はその両方。

(c) 公判による有罪判決の場合、2 年以下の拘禁若しくは罰金又はその両方。

管轄権

4 ［本法上の犯罪に関する］域外適用範囲

(1) 以下に定める場合を除き、第 1 条、第 3 条又は第 3ZA 条に規定する犯罪に関して、以下を問わない。

(a) 当該犯罪の有罪判決を確定するために証明が必要な行為又はその他事実が、本国で発生したか否か。

(b) 被告人が当該行為又は事実の発生時に本国に所在していたか否か。

(2) 第 3 項に規定される場合を除き、犯罪が成立するためには、当該犯罪が行われた状況において、本国の管轄権との間に少なくとも 1 つの重要な関連性が存在していなければならない。

(3) 第 2 条に規定される犯罪の訴追において、第 1 条に基づく犯罪の成立を立証する場合、当該関連性が存在する必要はない。

(4) 第 8 条で規定する場合を除き、以下の場合、第 2 条が適用される。被告人が本国以外の場所での行為、又は容易にしようと意図した行為が、本国で行われた場合に第 2 条が適用される犯罪に該当するものであれば、その行為は犯罪とみなす。

(a) 第 1 条に規定する犯罪に関して、本国との重要な関連性が事実上存在する場合。

(b) 第 2 条に基づく犯罪の訴追において、その犯罪の実行が主張される場合。

(4A) 第 3A 条に基づく犯罪に関して、当該犯罪について本国の管轄権と重要な関連性が存在する場合、被告人が当該行為時又は事実の発生時に本国に所在していたか否かは問わない。

(5) 本条は、スコットランドの裁判所が本条以外の規定に基づき行使する管轄権に影響を及ぼさない。

(6) 本法において「本国」とは以下を指す。

(a) 本法をイングランド及びウェールズに適用する場合、イングランド及びウェールズ。

(b) 本法をスコットランドに適用する場合、スコットランド。

(c) 本法を北アイルランドに適用する場合、北アイルランド。

5 本国の管轄権との重要な関連性

(1) 本条の以下の規定は、第 4 条の解釈に適用される。

(1A) 第 1 条、第 3 条、第 3ZA 条、又は第 3A 条に基づく犯罪に関し、被告人が当該犯罪行為時に英国国外に所在していた場合、以下の要件を満たす場合は本国の管轄

権と重要な関連性が認められる。

(a) 被告人が当時英国国民であったこと。

(b) 当該行為がその発生した国の法律において犯罪を構成する行為であったこと。

(1B) 第 1A 項において

「国」には領土を含む。

「英国国民」とは、以下のいずれかに該当する個人をいう。

(a) 英国市民、英国海外領土市民、英国海外国民、又は英国海外市民

(b) 1981 年英国国籍法に基づき英国臣民である者

(c) 1981 年英国国籍法に規定される英国保護対象者

(2) 第 1 条に規定される犯罪に関して、以下のいずれかに該当する場合、本国の管轄権と重要な関連性があるものとする。

(a) 被告人が、コンピュータに機能を実行させる行為を行った時点で本国に所在していたとき。

(b) 被告人が、当該行為により、無権限のアクセスを確保し、若しくは確保しようと意図した、又は無権限のアクセスを可能にし、若しくは可能にしようと意図したプログラム若しくはデータを含むコンピュータが、その時点で本国に所在していたこと。

(3) 第 3 条に規定される犯罪に関して、以下のいずかに該当する場合、本国の管轄権との重要な関連性があるものとする。

(a) 被告人が、無権限の行為を行った（又は行わせた）時点で本国に所在していたとき。

(b) 当該無権限の行為が、本国に所在するコンピュータに対して行われたとき。

(3A) 第 3ZA 条に規定される犯罪に関して、以下のいずれかに該当する場合、本国の管轄権との重要な関連性があるものとする。

(a) 被告人が無権限の行為を行った（又は行わせた）時点で本国に所在していたとき。

(b) 当該無権限の行為が、本国に所在するコンピュータに対して行われたとき。

(c) 当該無権限の行為が、本国において（本条に定める）重大な損害を生じさせたとき、又はそのような損害を生じさせる重大な危険を生じさせたとき。

6 本法に基づく犯罪に関する未遂罪等の域外適用範囲

(1) 本法に規定する犯罪の共謀罪に関する訴追において、被告人の有罪を判断する上で以下の事項は問わない。

(a) 共謀に参加した者が共謀に加わった場所。

(b) 有罪判決に必要な行為、不作為又はその他の事実が本国で発生したか否か。

(2) 本法に規定する罪の未遂罪に関する訴追において、被告人の有罪を判断する上で以下の事項は問わない。

(a) 未遂が行われた場所。

(b) 当該未遂が本国に効果を及ぼしたか否か。

(3) ［削除］

(4) 本条はスコットランドにおいては適用されない。

7 外部法上の犯罪に関する未遂罪の域外適用範囲

(1) ［削除］

(2) ［削除］

(3) 1981 年刑事未遂法(Criminal Attempts Act 1981)第 1 条第 1 項の後に、以下の各項を挿入するものとする。

(1A) 1990 年コンピュータ不正使用法第 8 条（外国法の関連性）に従い、この項が適用される場合、当該行為者が意図したことは、本条が適用される犯罪とみなされる。

(1B) 第 1A 項は、以下の場合に適用される。

(a) 当該行為がイングランド及びウェールズにおいて行われた場合。

(b) 当該行為が完遂された場合に、イングランド及びウェールズで審理されえない犯罪であるという事実を除けば、1990 年コンピュータ不正使用法第 3 条に基づく犯罪の実行に向けた単なる準備行為以上の行為として第 1 項に該当するものである場合。

(4) ［削除］

8 外部法の関連性

(1) 第 4 条第 4 項に基づき審理される犯罪に関して、被告人が意図した行為又は容易にしようとした行為が、当該行為の全部又は一部が行われることを意図した場所において現行法上犯罪を構成する場合に限り、犯罪が成立するものとする。

(2) ［削除］

(3) 1981 年刑事未遂法第 1 条第 1A 項に基づき審理される犯罪に関して、被告人が意図した事項が、当該行為の全部又は一部が行われることを意図した場所において現行法上犯罪を構成する場合に限り、犯罪が成立するものとする。

(4) いかなる場所においても、そこの現行法上処罰可能な行為は、当該法における記載を問わず、本条の目的においては犯罪とみなされる。

(5) 第 7 項に従う場合、第 1 項又は第 3 項に規定する条件は、裁判規則で定める期限までに、弁護側が検察に対して以下の事項を記載した通知を送達しない限り、満たされたものとみなす。

(a) 関連行為に関して主張される事実に基づき、当該条件が満たされていないと

考える旨を記載すること。

(b) その意見の根拠を示すこと。

(c) 検察に対して、当該条件が満たされていることを立証するよう求めること。

(6) 第 5 項における「関連行為」とは、以下をいう。

(a) 第 1 項の要件が問題となる場合、被告が意図した行為又は容易にしようとした行為。

(b) ［削除］

(c) 第 3 項の要件が問題となる場合、被告人が意図した事項。

(7) 裁判所は、適当と判断する場合、弁護側が第 5 項に基づく通知を事前に送達することなく、検察に当該条件が満たされていることを立証させることを許可することができる。

(8) スコットランドの正式裁判所において、第 7 項に基づき、弁護側に検察に当該条件の立証を要求することを裁判所が許可した場合、検察はその目的のため、提出済みの証拠目録に含まれていない証人の尋問又は証拠物の提出を行うことができる。

(9) クラウンコートにおいては、当該条件が満たされているか否かの判断は裁判官のみが行う。

(10) 高等裁判所及びシェリフ裁判所においては、当該条件が満たされているか否かの判断は、裁判官又は場合に応じてシェリフのみが行うものとする。

9 英国市民権の影響の無さ

(1) 第 5 条第 1A 項に定める場合を除き、本条が適用される犯罪に関するイングランド及びウェールズでの訴追手続においては、有罪の判断において、被告人が有罪判決に必要な行為、不作為、又はその他の事実の発生時に英国市民であったか否かは問わない。

(2) 本条は、以下の犯罪に適用される。

(a) 本法に基づく全ての犯罪

(b) ［削除］

(c) 本法に基づく犯罪の未遂罪

(d) ［削除］

10 保存条項

第 1 条から第 3A 条は、以下の効力を損なわない。

(a) イングランド及びウェールズにおける、検査、捜索又は差押えに関するいかなる制定法又は当該行為が許可又は要求される根拠となるその他制定法。

(b) スコットランドにおける、調査、捜索又は差押えに関するいかなる制定法及び法理又は当該行為が許可又は要求される根拠となるその他の制定法又は法

理。

また、執行官に対してプログラム又はデータへのアクセスに関する同意を留保することを示すいかなる措置も、これらの各条の適用に関して、当該アクセスを無権限とする効力を有しない。

本条において「制定法」とは、いつ成立又は制定されたかを問わず、以下を含む。

(a) 議会制定法

(b) スコットランド議会制定法

(c) ウェールズ国民議会の措置法(Measure)又は法(Act)

(d) 上記の法(Act)又は措置法(Measure)に基づき制定された命令

(e) 1978 年解釈法にいうその他の下位立法

「執行官」とは、犯罪の捜査の職務を負う警察官又はその他の者をいう。

また、執行官に対して同意を留保することには、アクセス権を管理する権限を有する者が、当該執行官を、アクセス権を有する者の範囲から除外する規則を運用することを含む。

11 第 1 条違反に関する手続

［削除］

12 第 2 条又は第 3 条違反に関する手続における第 1 条違反の有罪判決

［削除］

13 スコットランドにおける手続

(1) シェリフは、第 1 条又は第 2 条に基づく犯罪に関して、以下のいずれかの場合に管轄権を有する。

(a) 被告人が、コンピュータに機能を実行させる行為を行った時点でシェリフ管轄区域内に所在していた場合。

(b) 被告人が当該行為により、無権限のアクセスを確保し若しくは確保することを意図した又は無権限のアクセスを可能にし若しくは可能にしようと意図したプログラム又はデータを含むコンピュータが、その時点でシェリフ管轄区域内に所在していた場合。

(2) シェリフは、第 3 条に基づく犯罪に関して、以下のいずれかの場合に管轄権を有する。

(a) 被告人が無権限の行為を行った（又は行わせた）時点でシェリフ管轄区域内に所在していた場合。

(b) 当該無権限の行為がシェリフ管轄区域内のコンピュータに関して行われた場合。

(2A) シェリフは、第 3ZA 条に基づく犯罪に関して、以下のいずれかの場合に管轄権を

有する。

(a) 被告人が無権限の行為を行った（又は行わせた）時点でシェリフ管轄区域内に所在していた場合。

(b) 当該無権限の行為が行われたコンピュータが、その時点でシェリフ管轄区域内に所在していた場合。

(2B) シェリフは、第 3A 条に基づく犯罪に関して、以下の場合に管轄権を有する。

(a) 被告人が、以下のいずれかの行為を行った時点でシェリフ管轄区域内に所在していた場合。

(i) 第 3A 条第 1 項にいう、当該物品を使用する意図をもって製造、改造、供給又は供給を申し出た場合。

(ii) 第 3A 条第 2 項にいう、当該物品が使用されると信じて供給又は供給を申し出た場合。

(iii) 第 3A 条第 3 項にいう、当該物品を使用する意図又は供給する目的をもって取得した場合。

(b) 当該犯罪が第 1 条、第 3 条又は第 3ZA 条に基づく犯罪の実行に関連するものであり（第 3A 条第 1 項から第 3 項に記載される方法による）、本条第 1 項(b)、第 2 項(b)又は第 2A 項(b)にいうコンピュータが、被告人が第 3A 条に基づく犯罪を構成する行為を行った時点で保安官管轄区域内に所在していた場合。

(3) ［削除］

(4) ［削除］

(5) ［削除］

(6) ［削除］

(7) ［削除］

(8) 第 2 条又は第 3 条に基づく犯罪で起訴され、無罪又は免訴となった者は、提示された事実に基づき、第 1 条に基づく犯罪で有罪とされうる場合には、当該犯罪で有罪とされうる。［削除］

(9) 第 8 項は、第 1 条に基づく犯罪が訴状又は起訴状に記載されているか否かを問わず適用される。

(10) 第 8 項に基づき第 1 条に基づく犯罪で有罪とされた者は、その犯罪に関して、第 1 条に定める刑罰のみを科される。

(10A)第 1 条、第 3 条、第 3ZA 条、又は第 3A 条に基づく犯罪がスコットランド国外で行われた場合、当該犯罪を行った者は、以下のいずれかのスコットランドのシェリフ裁判所地区で起訴、審理及び処罰されうる。

(a) 当該違反者が逮捕又は拘留されているシェリフ裁判所地区

(b) ロード・アドボケイトが指定するシェリフ裁判所地区、

この場合、当該犯罪は、審理又は処罰に付随又は結果として生じる全ての目的におい

て、その管轄区域で行われたものとみなされる。

(11) 本条はスコットランドにのみ適用される。

14　第 1 条違反に対する捜索令状

［削除］

15　1989 年引渡し法附則 1 が適用される場合の引渡し

［削除］

16　北アイルランドへの適用

(1)　本条の以下の規定は、本法を北アイルランドに適用する場合において、そこに記載された修正を加えた上で効力を有する。

(1A) 第 1 条第 3 項(a)において

(a)　「イングランド及びウェールズ」は「北アイルランド」と読み替えるものとする。

(b)　「治安判事裁判所における一般上限」は「6 か月」と読み替えるものとする。

(2)　第 2 条第 2 項(b)において

(a)　「イングランド及びウェールズ」は「北アイルランド」と読み替えるものとする。

(b)　「1980 年治安判事裁判所法第 33 条」は「1981 年治安判事裁判所（北アイルランド）命令第 46 条第 4 項」と読み替えるものとする。

(2A) 第 2 条第 5 項(a)において

(a)　「イングランド及びウェールズ」は「北アイルランド」と読み替えるものとする。

(b)　「治安判事裁判所における一般上限」は「6 か月」と読み替えるものとする。

(3)　［削除］

(3A) 第 3 条第 6 項(a)において

(a)　「イングランド及びウェールズ」は「北アイルランド」と読み替えるものとする。

(b)　「治安判事裁判所における一般上限」は「6 か月」と読み替えるものとする。

(3B) 第 3A 条第 5 項(a)において

(a)　「イングランド及びウェールズ」は「北アイルランド」と読み替えるものとする。

(b) 「治安判事裁判所における一般上限」は「6 か月」と読み替えるものとする。

(4) 第 7 条第 3 項に代えて、第 7 項を適用する。［削除］

(5) ［削除］

(6) ［削除］

(7) 第 3 条第 1 項の後に以下の各項を挿入するものとする。

(1A) 1990 年コンピュータ不正使用法第 8 条（外国法の関連性）に従い、この項が適用される場合、当該行為者が意図したことは、本条が適用される犯罪とみなされる。

(1B) 上記(1A)項は、以下の全ての行為に適用される。

(a) 当該行為が北アイルランドで行われた場合。

(b) 当該行為が、完遂された場合に北アイルランドで審理されえない犯罪であるという事実を除けば、1990 年コンピュータ不正使用法第 3 条に基づく犯罪の実行に向けた単なる準備以上の行為として第 1 項に該当するものである場合。

(8) 第 8 条において

(a) ［削除］

(b) 第 3 項における「1981 年刑事未遂法第 1 条第 1A 項」は、「当該命令第 3 条第 1A 項」と読み替えるものとする。

(9) 第 9 条第 1 項及び第 10 条における「イングランド及びウェールズ」は「北アイルランド」と読み替えるものとする。

(9A) 第 10 条における「制定法」の定義は、北アイルランドの立法又は当該立法に基づき制定された命令等を含むものと読み替える。

(10) ［削除］

(11) ［削除］

(12) ［削除］

16A 北アイルランド：第 1 条に基づく犯罪に関する捜索令状

(1) 治安判事裁判所の判事が、警察官による宣誓供述に基づき、以下の事実を信じるに足る合理的な理由があると認めた場合、令状を発付することができる。

(a) 第 1 条に基づく犯罪が、当該場所で既に行われた、又は行われようとしていること。

(b) 当該犯罪が既に行われたか、又は行われようとしていることを示す証拠が、その場所に存在すること。

この場合、判事は、警察官に対し、必要な合理的な有形力を用いて当該場所に立ち入り、捜索することを認める令状を発付することができる。

(2) 第 1 項により付与される権限は、1989 年北アイルランド警察・刑事証拠令(Police

and Criminal Evidence (Northern Ireland) Order 1989)第 11 条第 2 項に記載される種類の資料（特権資料、除外資料及び特別手続資料）を捜索する権限を付与するものではない。

(3) 本条に基づく令状は、以下の効力を有する。

(a)令状を執行する警察官に他者を同行させることを許可することができる。

(b) 発行日から 28 日間有効とする。

(4) 本条に基づく令状を行使する場合、警察官は、当該物品が第 1 条に基づく犯罪が既に行われたか、又は行われようとしていることを示す証拠であると合理的に信じる場合、その物品を押収することができる。

(5) 本条における「場所」には、土地、建物、可動構造物、車両、船舶、航空機及びホバークラフトを含む。

(6) 本条は北アイルランドにのみ適用される。

17 定義

(1) 本条の以下の規定は、本法の解釈のために適用される。

(2) コンピュータに何らかの機能を実行させることをもって、他のコンピュータに保存されているプログラム又はデータへの無権限のアクセスを取得する場合とは、以下のいずれかをいう。

(a) プログラム又はデータを変更又は消去する場合。

(b) プログラム又はデータを、保存されている記憶媒体以外の記憶媒体にコピー若しくは移動する場合、又は保存されている記憶媒体内の別の位置にコピー又は移動する場合。

(c) プログラム又はデータを使用する場合。

(d) プログラム又はデータを、保存されているコンピュータから出力させる場合（表示させる場合又はその他の方法による場合も含む）。

プログラム又はデータへのアクセス及び当該アクセスを確保する意図［又は当該アクセスを可能にする意図］に関する記載は、これに従って解釈されるものとする。

(3) 第 2 項(c)の目的において、プログラムを使用する場合とは、以下の場合をいう。

(a) 行為者がコンピュータに実行させる機能が、プログラムを実行させる場合。

(b) 当該機能自体がプログラムの機能である場合。

(4) 第 2 項(d)の目的において

(a) プログラムは、その構成要素である命令が出力される場合に出力されたものとする。

(b) 当該命令又はその他のデータが出力される形式（特に、命令の場合にそれが実行可能な形式であるか、又はデータの場合にコンピュータによって処理可能な形式であるか）は問わない。

(5) コンピュータに保存されているプログラム又はデータに対するいかなる種類のア

クセスも、以下を満たす場合には無権限とみなす。

(a) 行為者が、当該プログラム又はデータへの当該種類のアクセスを制御する権限を有していない場合。

(b) 行為者が、当該種類のアクセスを制御する権限を有する者から、当該種類のアクセスに関して同意を得ていない場合［ただし、本項は第 10 条に従う］。

(6) コンピュータに保存されているプログラム又はデータの記載には、当該コンピュータ内に一時的に挿入されているリムーバブル記憶媒体に保存されているプログラム又はデータも含まれる。また、コンピュータは、当該媒体に保存されているいかなるプログラム又はデータも含んでいるものとみなされる。

(7) ［削除］

(8) コンピュータに関して行われる行為は、以下の場合には無権限とする。

(a) その行為を行う者（又は行わせる者）が、コンピュータに関する責任を負い、当該行為を行うことができるか否かを決定する権限を有する者ではない場合。

(b) その者が、当該権限を有する者から当該行為に関して同意を得ていない場合。

本項において「行為」には一連の行為を含む。

(9) 「本国」は、第 4 条第 6 項に従って解釈される。

(10) プログラムへの言及には、プログラムの一部分に関する記載を含む。

18 名称、施行等

(1) 本法は「1990 年コンピュータ不正使用法(Computer Misuse Act 1990)」と称する。

(2) 本法は、成立の日から起算して 2 か月目の末日に施行される。

(3) 本法に基づく犯罪は、本法施行後に、当該犯罪の有罪判決のために立証が必要な全ての行為又はその他の事象が発生した場合にのみ成立する。

【参考書式】

ドイツ

1　就業規則における秘密保護関連規定の例

German Staff Handbook

DATED

[EMPLOYER'S NAME]

STAFF HANDBOOK

Staff handbook

1. Introduction

1.1 [GENERAL DETAILS ABOUT THE EMPLOYER AND ITS BUSINESS.]

1.2 We are an equal opportunities employer and do not discriminate on the grounds of gender, sexual orientation, marital or civil partner status, pregnancy or maternity, gender reassignment, race, colour, nationality, ethnic or national origin, religion or belief, disability or age.

2. Using the Staff Handbook

2.1 This Staff Handbook sets out the main policies and procedures that you will need to be aware of while working for us. You should familiarise yourself with it and comply with it at all times. Any questions you may have with regard to its contents or what you have to do to comply with it should be referred to the Human Resources Department.

2.2 The policies and procedures set out in this handbook apply to all employees unless otherwise indicated. They therefore apply to managers, officers, directors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff and volunteers (collectively referred to as staff in this handbook). Unless stated explicitly otherwise, they do not form part of the terms of your contract with us, which are provided to you separately.

2.3 Our policies and procedures have been agreed with the TRADE UNION OR WORKS COUNCIL.

3. Responsibility for the Staff Handbook

3.1 The HR Manager has overall responsibility for this Staff Handbook and for ensuring that its policies and procedures comply with our legal obligations.

3.2 The Staff Handbook is reviewed regularly to ensure that its provisions continue to meet our legal obligations and reflect best practice.

3.3 Everyone should ensure that they take the time to read and understand the content of this handbook and act in accordance with its aims and objectives. Managers must ensure all staff understand the standards of behaviour expected of them and to take action when behaviour falls below those requirements.

4. Personal data

Whenever we process personal data about you in connection with our policies, we will process it in accordance with our Data Protection Policy. We will only process your personal data if we have a lawful basis for doing so. We will notify you of the purpose or purposes for which we use it. Please see the Privacy Notice on the intranet for further information.

5. Emergency contact details

The Human Resources Department is responsible for maintaining up-to-date details of your home address and the emergency contact telephone numbers of the person or persons you would like us to contact in the event of an emergency, for example if you have an accident. This information will be requested by the Human Resources Department when you start work and you

should advise us of any changes straight away. This information is held in confidence and will only be used when needed.

Schedule 1 Disciplinary and Capability Procedure

1. About Procedure

1.1 This procedure is intended to help maintain standards of conduct and performance and to ensure fairness and consistency when dealing with allegations of misconduct or poor performance.

1.2 Minor conduct or performance issues can usually be resolved informally with your line manager. This procedure sets out formal steps to be taken if the matter is more serious or cannot be resolved informally.

1.3 This procedure applies to all employees regardless of length of service. It does not apply to agency workers or self-employed contractors.

1.4 This procedure does not form part of any employee's contract of employment and we may amend it at any time.

2. Investigations

2.1 Before any disciplinary hearing is held, the matter will be investigated. Any meetings and discussions as part of an investigation are solely for the purpose of fact-finding and no disciplinary action will be taken without a disciplinary hearing.

2.2 In some cases of alleged misconduct, we may need to suspend you from work while we carry out the investigation or disciplinary procedure (or both). [While suspended, you should not visit our premises or contact any of our clients, customers, suppliers, contractors or staff, unless authorised to do so.] Suspension is not considered to be disciplinary action.

3. Hearing

3.1 We will give you written notice of the hearing, including sufficient information about the alleged misconduct or poor performance and its possible consequences to enable you to prepare. You will normally be given copies of relevant documents and witness statements.

3.2 You may be accompanied at the hearing by a trade union representative or a colleague, who will be allowed reasonable paid time off to act as your companion.

3.3 You should let us know as early as possible if there are any relevant witnesses you would like to attend the hearing or any documents or other evidence you wish to be considered.

3.4 We will inform you in writing of our decision, usually within one week of the hearing.

4. Disciplinary Action and Dismissal

4.1 The usual penalties for misconduct or poor performance are:

(a) Stage 1: First written warning [or improvement note]. Where there are no other active written warnings [or improvement notes] on your disciplinary record, you will usually receive a first written warning [or improvement note]. It will usually remain active for six months.

(b) Stage 2: Final written warning. In case of further misconduct or failure to improve where there is an active first written warning [or improvement note] on your record, you will usually receive a final written warning. This may also be used without a first

written warning [or improvement note] for serious cases of misconduct or poor performance. The warning will usually remain active for 12 months.

(c) Stage 3: Dismissal or other action. You may be dismissed for further misconduct or failure to improve where there is an active final written warning on your record, or for any act of gross misconduct. Examples of gross misconduct are given below (paragraph 6). You may also be dismissed without a warning for any act of misconduct or unsatisfactory performance during your probationary period.

(d) We may consider other sanctions short of dismissal, including demotion or redeployment to another role (where permitted by your contract), and/or extension of a final written warning with a further review period.

5. Appeals

5.1 You may appeal in writing within three weeks of being told of the decision.

5.2 The appeal hearing will, where possible, be held by someone other than the person who held the original hearing. You may bring a colleague or trade union representative with you to the appeal hearing.

5.3 We will inform you in writing of our final decision as soon as possible, usually within one week of the appeal hearing. There is no further right of appeal.

6. Gross Misconduct

6.1 Gross misconduct will usually result in dismissal without warning, with no notice or payment in lieu of notice (summary dismissal).

6.2 Gross misconduct is a serious breach of contract and includes misconduct which, in our opinion, is likely to prejudice our business or reputation or irreparably damage the working relationship and trust between us. This may include misconduct committed outside of work. The following are examples of matters that are normally regarded as gross misconduct:

(a) theft or fraud;

(b) physical violence or bullying;

(c) deliberate and serious damage to property;

(d) serious misuse of the organisation's property or name;

(e) deliberately accessing internet sites containing pornographic, offensive or obscene material;

(f) serious insubordination;

(g) unlawful discrimination, victimisation or harassment;

(h) bringing the organisation into serious disrepute;

(i) serious incapability at work brought on by alcohol or illegal drugs;

(j) causing loss, damage or injury through serious negligence;

(k) a serious breach of health and safety rules;

(l) a serious breach of confidence.

This list is intended as a guide and is not exhaustive.

Schedule 2 Grievance Procedure

1. Step 1: Written Grievance

1.1 You should put your grievance in writing and submit it to your line manager. If your grievance concerns your line manager you may submit it to [POSITION].

1.2 The written grievance should set out the nature of the complaint, including any relevant facts, dates, and names of individuals involved so that we can investigate it.

2. Step 2: Meeting

2.1 We will arrange a grievance meeting, normally within [one week] of receiving your written grievance. You should make every effort to attend.

2.2 We may adjourn the meeting if we need to carry out further investigations, after which the meeting will usually be reconvened.

2.3 We will, usually within two weeks of the last grievance meeting, issue our decision and notify you of any further action that we intend to take to resolve the grievance. We will also advise you of your right of appeal.

3. Step 3: Appeals

3.1 You may appeal in writing to us, stating your grounds of appeal, within three weeks of the date on which the decision was sent or given to you.

3.2 We will hold an appeal meeting, normally within four weeks of receiving the appeal. This will be dealt with impartially by three managers who have not previously been involved in the case.

3.3 We will confirm our final decision in writing, usually within two weeks of the appeal hearing. There is no further right of appeal.

Schedule 3 IT Policy

1. Gegenstand und Geltungsbereich	**1. Subject matter and scope**
Diese Richtlinie regelt den Einsatz und die Nutzung der IT-Infrastruktur des Unternehmens durch die Mitarbeiter und umfasst insbesondere: • Einsatz und Nutzung der E-Mail-Systeme des Unternehmens, • Einsatz und Nutzung des Internets am Arbeitsplatz, • Nutzung des betrieblichen Intranets, • Einsatz und Nutzung vom Unternehmen bereitgestellter Computeranlagen (PC, Laptops zur Nutzung außerhalb der Geschäftsräume sowie sämtliche Hard- und Software), • –Einsatz und Nutzung vom Unternehmen bereitgestellter Kommunikationsmittel (Telefon und Fax, Mobiltelefone und mobile Geräte zum Empfangen und Versenden von E-Mails). Die Richtlinie gilt für alle Mitarbeiter, die die IT-Infrastruktur des Unternehmens nutzen.	This policy governs the use of the company's IT infrastructure by employees and covers in particular: • Use of the company's e-mail systems, • Use of the internet at work, • Use of the company intranet, • Use and utilisation of computer equipment provided by the company (PCs, laptops for use outside the business premises and all hardware and software), • Use and utilisation of communication tools provided by the company (telephone and fax, mobile phones and mobile devices for receiving and sending e-mails). The policy applies to all employees who use the company's IT infrastructure.
2. Nutzung der IT-Infrastruktur	**2. Use of the IT infrastructure**
Die IT-Infrastruktur des Unternehmens dient der Verbesserung der externen und internen Kommunikation, der Erzielung einer höheren Effizienz und der Beschleunigung der Informationsbeschaffung und der Arbeitsprozesse. Die IT-Infrastruktur steht den Mitarbeitern deshalb grundsätzlich nur im Rahmen ihrer dienstlichen Aufgabenerfüllung zur Verfügung. Nach Maßgabe der folgenden Regelungen und Einschränkungen steht die IT-Infrastruktur in angemessenem Umfang auch zur privaten Nutzung zur Verfügung, soweit dadurch die dienstliche Aufgabenerfüllung und die Verfügbarkeit der IT-Infrastruktur nicht beeinträchtigt wird und keine Unternehmensinteressen entgegenstehen. Soweit diese Richtlinie die Möglichkeit zur privaten Nutzung vorsieht, ist dies eine freiwillige, vom Unternehmen jederzeit widerrufbare Leistung.	The company's IT infrastructure serves to improve external and internal communication, achieve greater efficiency and accelerate information retrieval and work processes. The IT infrastructure is therefore only available to employees for the purpose of performing their work duties. Subject to the following rules and restrictions, the IT infrastructure is also available for private use to a reasonable extent, provided that this does not impair the performance of work duties or the availability of the IT infrastructure and does not conflict with the company's interests. Insofar as this policy provides for the possibility of private use, this is a voluntary service that can be revoked by the company at any time.

3. Allgemeine Regelungen für die Nutzung der IT-Infrastruktur	**3. General rules for the use of the IT infrastructure**
Die Mitarbeiter sind verpflichtet bei der Nutzung der IT-Infrastruktur geltende, einschlägige Gesetze und interne Regelungen einzuhalten. Eine Nutzung der IT-Infrastruktur, die geeignet ist, das Ansehen oder die Sicherheit der IT-Infrastruktur des Unternehmens zu beeinträchtigen ist untersagt. Das gilt insbesondere für: • das Anbieten, Abrufen, Speichern oder Verbreiten von Inhalten, die gegen Persönlichkeitsrechte, urheberrechtliche oder strafrechtliche Bestimmungen verstoßen; • das Anbieten, Abrufen, Speichern oder Verbreiten von weltanschaulicher oder politischer Werbung; • das Anbieten, Abrufen, Speichern oder Verbreiten von pornographischen, rassistischen, gewaltverherrlichenden, verfassungsfeindlichen, terroristischen sowie sonstigen rechtswidrigen Inhalten; • die Nutzung von Chat-Seiten und File-Sharing-Netzwerken.	Employees are obliged to comply with applicable laws and internal regulations when using the IT infrastructure. Any use of the IT infrastructure that is likely to damage the reputation or security of the company's IT infrastructure is prohibited. This applies in particular to: • offering, accessing, storing or distributing contents that violate personal rights, copyright or criminal law provisions; • offering, accessing, storing or distributing ideological or political advertising; • offering, accessing, storing or distributing pornographic, racist, violence-glorifying, anti-constitutional, terrorist or other illegal content; • using chat sites and file-sharing networks.
4. Nutzung der betrieblichen E-Mailsysteme, des Intranets und des Internets	**4. Use of company email systems, the intranet and the internet**
4.1 Nutzung der E-Mailsysteme Die private Nutzung der E-Mail-Systeme des Unternehmens ist untersagt. Eingehende private E-Mails sind nach Kenntnisnahme zu löschen. Absender privater E-Mails sind von den Adressaten darauf hinzuweisen, dass die E-Mail-Adresse nur für dienstliche Zwecke genutzt werden darf. Privater E-Mail-Verkehr darf nur über kostenlose Web-Mail-Dienste erfolgen. Aufgrund zusätzlicher Sicherheitsrisiken gestatten wir zu keiner Zeit den Zugriff auf webbasierte private E-Mail-Konten wie Gmail oder Hotmail auf unseren Computersystemen. Eine zeitnahe dienstliche Korrespondenz ist zu gewährleisten. Deshalb bestimmt jeder Mitarbeiter einen Vertreter für den Fall der Abwesenheit und	**4.1 Use of email systems** Private use of the company's email systems is prohibited. Incoming private emails must be deleted after reading. Senders of private emails must be informed by the recipients that the email address may only be used for business purposes. Private email correspondence may only be conducted via free webmail services. We do not permit access to web-based personal e-mail such as Gmail or Hotmail on our computer systems at any time due to additional security risks. Timely business correspondence must be ensured. For this reason, each employee shall designate a representative in the event of absence and grant them access rights to the business email account.

räumt diesem Zugriffsrechte auf den dienstlichen E-Mail-Account ein. Im Falle einer vorhersehbaren Abwesenheit ist der Absender mittels einer „Auto-Reply“-Funktion über die Dauer der Abwesenheit zu informieren. Im Falle einer unvorhersehbaren Abwesenheit wird das Einrichten dieser Funktion durch den benannten Vertreter veranlasst. Das Unternehmen hält die Möglichkeit vor, E-Mail-Korrespondenz mit einer elektronischen Signatur zu versehen oder zu verschlüsseln. Vorgesetzte des Mitarbeiters sind berechtigt anzuordnen, dass E-Mails mit bestimmtem Inhalt mit elektronischer Signatur und/oder Verschlüsselung zu versenden sind. Mitarbeiter dürfen keine beleidigenden, obszönen, diskriminierenden, rassistischen, belästigenden, herabwürdigenden, diffamierenden, pornografischen oder anderweitig unangemessenen E-Mails versenden. Darüber hinaus sollen Mitarbeiter insbesondere nicht: (a) private E-Mails am Arbeitsplatz versenden oder weiterleiten, von denen der Mitarbeiter nicht möchte, dass Dritte sie lesen; (b) Kettenbriefe, Junk-Mails, Cartoons, Witze oder Klatsch versenden oder weiterleiten; (c) durch das Versenden trivialer Nachrichten oder das unnötige Kopieren oder Weiterleiten von E-Mails an andere, die keinen wirklichen Bedarf haben, diese zu erhalten, zur Überlastung des Systems beitragen; oder (d) Nachrichten von der E-Mail-Adresse einer anderen Person (sofern nicht autorisiert) oder unter einem falschen Namen versenden.	In the event of a foreseeable absence, the sender shall be informed of the duration of the absence by means of an ‘auto-reply’ function. In the event of an unforeseeable absence, the designated representative shall arrange for this function to be set up. The company reserves the right to add an electronic signature to or encrypt email correspondence. The employee's superiors are entitled to instruct that emails with certain content be sent with an electronic signature and/or encryption. Employees must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate e-mails. Furthermore, Employees should in particular not: (a) send or forward private e-mails at work which the Employee would not want a third party to read; (b) send or forward chain mail, junk mail, cartoons, jokes or gossip; (c) contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to others who do not have a real need to receive them; or (d) send messages from another person's e-mail address (unless authorised) or under an assumed name.
4.2 Nutzung des Intranets Die private Nutzung des Intranets des Unternehmens ist untersagt. Inhalte dürfen durch die Mitarbeiter nur mit der Zustimmung der jeweils zuständigen Vorgesetzten eingestellt werden.	**4.2 Use of the intranet** Private use of the company's intranet is prohibited. Employees may only post content with the consent of their respective supervisors.
4.3 Nutzung des Internets Die private Nutzung des Internets steht unter dem Vorbehalt, dass der Mitarbeiter seine schriftliche Einwilligungserklärung unterzeichnet, die dem	**4.3 Use of the internet** Private use of the internet is subject to the employee signing a written declaration of consent, which grants the company the

Unternehmen im Folgenden näher bezeichnete Möglichkeiten zur Kontrolle der Einhaltung der Bestimmungen dieser Richtlinie einräumt. Es steht jedem Mitarbeiter frei, ob er diese Einwilligung unterzeichnet. Soweit der Mitarbeiter keine Einwilligung erteilt, oder diese widerruft, so ist ihm die private Nutzung des Internets untersagt. Das Internet darf privat genutzt werden, wenn der zeitliche Aufwand der privaten Nutzung von untergeordneter Bedeutung ist und unter Einbringung der jeweiligen Pausenzeiten des Mitarbeiters erfolgt. Der Zeitaufwand darf dabei eine Stunde pro Woche nicht überschreiten. Der Arbeitgeber kann nach eigenem Ermessen den Zugriff auf bestimmte Websites sperren oder einschränken.	options described in more detail below for monitoring compliance with the provisions of this policy. Every employee is free to decide whether to sign this declaration of consent. If the employee does not give his/her consent or revokes it, his/her is prohibited from using the internet for private purposes. The Internet may be used privately if the time spent on private use is of minor importance and takes place during the employee's respective break times. The time spent may not exceed one hour per week. The Employer may block or restrict access to certain websites at its discretion.
4.4 Ausnahmen Von den in diesem Abschnitt beschriebenen Verboten ausgenommen sind allein die betrieblich veranlasste Privatnutzung und die Privatnutzung in Notfällen.	**4.4 Exceptions** The only exceptions to the prohibitions described in this section are private use for business purposes and private use in emergencies.
4.5 Kontrollen Die Verbindungsdaten für den Internetzugang werden in anonymisierter oder pseudonymisierter Form mit Angabe von Zeitpunkt des Zugriffs, Zieladresse und übertragener Datenmenge protokolliert, mit dem Zweck, technische Fehler zu analysieren und zu korrigieren, die Systemleistung und Systemsicherheit zu gewährleisten und zu optimieren, das Gesamtvolumen der Nutzung zu ermitteln, und zur Durchführung von Stichproben zur Missbrauchskontrolle. Eine Unterscheidung von dienstlicher und privater Nutzung des Internet-Zugangs auf technischem Weg erfolgt nicht. Die so gewonnenen Protokolle werden stichprobenhaft und nicht personenbezogen ausgewertet. Ergibt sich bei der Auswertung der Verdacht einer Straftat oder einer schwerwiegenden Pflichtverletzung, insbesondere der Pflichten aus dieser Richtlinie, dürfen die Daten unter Hinzuziehung des Datenschutzbeauftragten personalisiert werden.	**4.5 Controls** The connection data for Internet access is logged in anonymised or pseudonymised form, stating the time of access, destination address and amount of data transferred, for the purpose of analysing and correcting technical errors, ensuring and optimising system performance and system security, determining the total volume of use, and carrying out random checks to control misuse. No technical distinction is made between business and private use of Internet access. The logs obtained in this way are evaluated on a random basis and are not personalised. If the evaluation gives rise to suspicion of a criminal offence or a serious breach of duty, in particular of the duties arising from this policy, the data may be personalised with the involvement of the data protection officer.

5. Sicherheitsmaßnahmen und Geheimhaltung	5. Security measures and confidentiality
5.1 Passwörter Der folgende Abschnitt regelt die Gestaltung und Handhabung von Passwörtern, die zur Authentifizierung berechtigter Mitarbeiter eingesetzt werden. Die Bestimmungen sind auf alle IT-Systeme des Unternehmens anzuwenden, die durch Passwörter vor unberechtigtem Zugriff und missbräuchlicher Verwendung oder Veränderung geschützt werden. • Passwörter sind geheim zu halten und nicht an Dritte weiterzugeben. Sie sind verdeckt einzugeben und dürfen insbesondere nicht auf Funktionstasten hinterlegt oder unverschlüsselt auf Rechnern gespeichert werden. Passwörter von Dritten dürfen nicht verwendet werden. • Das Passwort darf nicht leicht zu erraten sein. Trivialpasswörter, wie Namen, Kfz-Kennzeichen, Geburtsdatum, sind nicht zu verwenden. • Innerhalb des Passwortes ist mindestens ein Sonderzeichen oder eine Zahl zu verwenden. Um ein systematisches Ausspähen von Passwörtern zu vermeiden, müssen diese technisch so komplex wie möglich zusammengesetzt sein (Groß- und Kleinbuchstaben, Ziffern, Sonderzeichen). • Das Passwort muss mindestens 6 Zeichen lang sein. Bei wiederholter Fehleingabe wird der Zugang gesperrt. • Das Passwort ist unverzüglich zu wechseln, wenn das Passwort unautorisierten Personen bekannt geworden ist oder der Verdacht besteht, dass das Passwort unautorisierten Personen bekannt geworden ist.	**5.1 Passwords** The following section regulates the creation and handling of passwords used to authenticate authorised employees. The provisions apply to all of the company's IT systems that are protected by passwords against unauthorised access, misuse or modification. • Passwords must be kept secret and not disclosed to third parties. They must be entered covertly and, in particular, must not be stored on function keys or stored unencrypted on computers. Passwords belonging to third parties must not be used. • The password must not be easy to guess. Trivial passwords, such as names, vehicle registration numbers or dates of birth, must not be used. • The password must contain at least one special character or one number. To prevent systematic password spying, passwords must be as complex as possible (upper and lower case letters, numbers, special characters). • The password must be at least 6 characters long. Repeated incorrect entries will result in access being blocked. • The password must be changed immediately if it has become known to unauthorised persons or if there is suspicion that it has become known to unauthorised persons.
5.2 Kopier- und Installationsverbote Nur durch die IT-Abteilung des Unternehmens freigegebene Software darf auf den IT-Systemen verwendet werden. Das Herunterladen von Programmen und die Installation von Software darf	**5.2 Prohibitions on copying and installation** Only software approved by the company's IT department may be used on the IT systems. Programmes may only be downloaded and software may only be installed by the IT department, which checks the programmes

jeweils nur durch die IT-Abteilung erfolgen, welche die Programme auf IT-Kompatibilität, Freiheit von Viren und Trojanern und lizenzrechtliche Bestimmungen prüft. Auf IT-Systemen der Mitarbeiter aufgespielte Software darf nicht verändert werden. Die Kopie dieser Software auf private Rechner oder sonstige private Speichermedien ist untersagt. Die Benutzung privater Hard- und Software (private Mobiltelefone, PDAs, Kameras oder Memory-Sticks) zu dienstlichen Zwecken ist ohne Genehmigung durch die IT-Abteilung nicht zulässig, ein Anschluss an die IT-Systeme des Unternehmens ist untersagt. Änderungen an den Systemeinstellungen (Installation, Deinstallation, Änderungen an der Konfiguration etc.) dürfen nur durch die IT-Abteilung vorgenommen werden.	for IT compatibility, freedom from viruses and Trojans, and licensing requirements. Software installed on employees' IT systems may not be modified. Copying this software to private computers or other private storage media is prohibited. The use of private hardware and software (private mobile phones, PDAs, cameras or memory sticks) for business purposes is not permitted without the approval of the IT department; connection to the company's IT systems is prohibited. Changes to the system settings (installation, deinstallation, changes to the configuration, etc.) may only be made by the IT department.
5.3 Schutz vor schädlichen Inhalten und SPAM Die IT-Systeme des Unternehmens werden durch Mechanismen geschützt, die schädliche Inhalte wie Viren, Würmer und Trojaner herausfiltern. E-Mail-Anhänge sind durch den Mitarbeiter beim Empfang auf schädliche Inhalte zu überprüfen. Die vorgegebenen Schutzmechanismen dürfen nicht deaktiviert werden. Alle verdächtigen Ereignisse sind unverzüglich an die in Ziffer 5.5 genannte Stelle zu melden. Zum Schutz vor unerwünschten E-Mails hält das Unternehmen entsprechende Filtersysteme vor. Der Einsatz dieser Systeme ist optional. Um zu verhindern, dass eine vermeintlich als SPAM erkannte E-Mail gelöscht wird, werden diese E-Mails nicht automatisch gelöscht, sondern in einen separaten Ordner verschoben.	**5.3 Protection against harmful content and SPAM** The company's IT systems are protected by mechanisms that filter out harmful content such as viruses, worms and Trojans. Employees must check email attachments for harmful content upon receipt. The specified protection mechanisms must not be deactivated. All suspicious events must be reported immediately to the department specified in section 5.5. The company maintains appropriate filter systems to protect against unwanted emails. The use of these systems is optional. To prevent emails that are suspected of being spam from being deleted, these emails are not automatically deleted but moved to a separate folder.
5.4 Verfügbarkeit der Daten Daten sind so aufzubewahren, dass sie problemlos wiedergefunden werden können. Um das Risiko eines Datenverlusts zu reduzieren, sind regelmäßig Datensicherungen durchzuführen.	**5.4 Availability of data** Data must be stored in such a way that it can be easily retrieved. To reduce the risk of data loss, regular data backups must be performed.
5.5 Weitere Sicherheitsmaßnahmen Alle Mitarbeiter haben sicherzustellen, dass ihr Arbeitsplatz so eingerichtet ist, dass Unbefugten	**5.5 Additional security measures** All employees must ensure that their workplace is set up in such a way that

kein Zugriff auf Informationen und IT-Anwendungen möglich ist: • IT-Geräte sind bei längerem Verlassen des Arbeitsplatzes auszuschalten. Es ist außerdem eine passwortgeschützte Bildschirmsperre zu verwenden. Diese muss bei jedem Verlassen des Arbeitsplatzrechners manuell oder nach 5 Minuten automatisch aktiviert werden. • In Bereichen mit Publikumsverkehr sind Monitore, Drucker und Faxgeräte so aufzustellen, dass das Risiko der Einsichtnahme Dritter möglichst ausgeschlossen wird. • Ausdrucke auf zentralen Druckern und Kopierern sind unverzüglich abzuholen, Kopiervorlagen zu entfernen. • Mobile Datenträger sind so aufzubewahren, dass nur berechtigte Benutzer darauf zugreifen können. Das Gleiche gilt für mobil genutzte IT-Systeme.	unauthorised persons cannot access information and IT applications: • IT devices must be switched off when leaving the workplace for a longer period of time. A password-protected screen lock must also be used. This must be activated manually each time the workstation is left or automatically after 5 minutes. • In areas open to the public, monitors, printers and fax machines must be positioned in such a way that the risk of third parties viewing them is eliminated as far as possible. • Printouts from central printers and copiers must be collected immediately and copy templates removed. • Mobile data carriers must be stored in such a way that only authorised users can access them. The same applies to mobile IT systems.
5.6 Verhalten bei Sicherheitsvorfällen Sicherheitsvorfälle sind alle Ereignisse, die Relevanz für die Sicherheit und Integrität der IT-Systeme des Unternehmens haben, insbesondere Fehler, die zum Zugriff auf vertrauliche Daten durch unberechtigte Dritte, zum Verlust der Integrität schutzbedürftiger Daten oder zu Datenverlusten führen, Sicherheitslücken in Hard- oder Softwarekomponenten durch inhärente Fehler, Auftreten von Schadprogrammen oder kriminellen Handlungen (etwa Hacking von Internet-Servern, Einbruch in IT-Systeme, Diebstahl von Daten). Beim Auftreten von Sicherheitsvorfällen haben alle Beteiligten Ruhe zu bewahren und keine übereilten Maßnahmen zu ergreifen. Gegenmaßnahmen sind erst nach der Aufforderung durch die im folgenden Meldeplan genannten Berechtigten zu ergreifen. Im Umgang mit Sicherheitsvorfällen sind Ehrlichkeit und Kooperationsbereitschaft besonders wichtig. Sicherheitsvorfälle sind unverzüglich an die im Folgenden genannten Stellen zu melden. Alle Begleitumstände sind	**5.6 Conduct in the event of security incidents** Security incidents are all events that are relevant to the security and integrity of the company's IT systems, in particular errors that lead to unauthorised third parties accessing confidential data, to the loss of integrity of data requiring protection, or to data loss, security gaps in hardware or software components due to inherent errors, the occurrence of malware or criminal acts (such as hacking of Internet servers, intrusion into IT systems, theft of data). When security incidents occur, all parties involved must remain calm and refrain from taking any hasty measures. Countermeasures may only be taken after a request has been made by the authorised persons named in the following reporting plan. Honesty and a willingness to cooperate are particularly important when dealing with security incidents. Security incidents must be reported immediately to the departments listed below. All accompanying circumstances must be explained by those

durch die Betroffenen ungeschönt, offen und transparent zu erläutern, um damit zur Schadensminderung beizutragen. Meldeplan für Sicherheitsvorfälle:	affected in an unvarnished, open and transparent manner in order to help minimise damage. Reporting plan for security incidents:

Ereignis:	Stelle:
Verdacht des Zugriffs auf vertrauliche Daten durch unberechtigte Dritte; Verdacht der Offenlegung vertraulicher Daten an unberechtigte Dritte; Sicherheitslücken in Hard- oder Softwarekomponenten; kriminelle Handlungen; und sonstige Fälle	Sicherheitsbeauftragter
Fehler oder Ausfall der Funktionalität des IT-Systems	IT-Administrator
Verdacht auf Schadprogramme	Virenschutzbeauftragter

Event:	Authority
Suspicion of access to confidential data by unauthorised third parties; Suspicion of disclosure of confidential data to unauthorised third parties; Security gaps in hardware or software components; Criminal acts; and other cases	Security officer
Errors or failure of the IT system's functionality	IT administrator
Suspected malware	Virus protection officer

6. Inkrafttreten Diese Richtlinie wurde zuletzt am [...] aktualisiert.	**6. Effective date** This policy was last updated on [...].
Mit meiner Unterschrift bestätige ich, dass mir eine Kopie dieser IT-Richtlinie ausgehändigt wurde.	By signing, I confirm that I have received a copy of this IT policy.

（参考和訳）就業規則における秘密保護関連規定の例

ドイツ 就業規則

日付

[雇用主の名前]

就業規則

就業規則

1. 序文

1.1 [雇用主とその事業に関する概括的な説明]

1.2 当社は、機会均等を目指す雇用主であり、性別、性的指向、婚姻若しくは市民権のパートナーの地位、妊娠若しくは出産、性別の再割当て、人種、肌の色、国籍、民族、若しくは、出身国、宗教若しくは信念、障害、又は、年齢を理由に、差別しない。

2. 就業規則の使用

2.1 本就業規則は、あなたが、当社のために働いている間、あなたが知っておく必要がある、主要な方針や手続を示す。あなたは、これに精通し、常に、従わないとならない。こ の内容、あるいは、これを遵守するためにあなたがしなければならないことに関して、あなたが持つ疑問については、人事部に照会されるべきである。

2.2 このハンドブックに記載されている方針及び手順は、特に明記されていない限り、全ての従業員に適用される。したがって、これらは、マネージャー、役員、取締役、従業員、コンサルタント、請負業者、研修生、在宅勤務者、パートタイム、並びに、有期労働者、臨時スタッフ、並びに、代理店のスタッフ、及び、ボランティア（このハンドブックでは、まとめて「従業員」と呼ぶ）に適用される。これらは、特に明示されていない限り、別途提供される、当社との契約条件の一部を構成するものではない。

2.3 この方針及び手順は、労働組合[または労使協議会]と合意されている。

3. 就業規則への責任

3.1 人事部長は、この従業員ハンドブックに対して、全体的な責任を負い、その方針及び手順が、当社の法的義務に準拠していることを確認する。

3.2 スタッフハンドブックは定期的に見直され、その規定が、引き続き当社の法的義務を果たし、ベストプラクティスを反映しているか、確認される。

3.3 各従業員は、時間をかけ、このハンドブックの内容を読んで理解し、その目標と目的に従って行動する。管理者は、全従業員が、彼らに期待される行動の基準を理解し、行動がその基準を下回ったときに、確実に対処しなければならない。

4. 個人情報

当社の方針に関連して、あなたの個人データを処理する場合は、常に、データ保護ポリシーに従って処理される。あなたの個人データは、法的基礎がある場合にのみ、処理され、あなたに当社の使用目的が知らされる。詳細については、イントラネットのプライバシー通告を参照するものとする。

5. 緊急連絡先

人事部は、自宅の住所、及び、事故などの緊急時に、当社に連絡を取らせたい緊急連絡先の電話番号の、最新情報の詳細を維持する責任がある。これらの情報は、あなた

が職務を開始するときに、人事部から要求され、定期的に、これらが最新であることを確認するように求められる。この情報は機密情報として保持され、必要な場合にのみ使用される。

Schedule 1　　懲戒手続及び職能手続

1.　手順について

1.1　この手順は、行動及びパフォーマンスの基準を維持し、不正行為や業績の低下の申立てに対処する際の、公平性及び一貫性を確保することを目的とする。

1.2　軽微な行動やパフォーマンスの問題は、通常、ラインマネージャーと非公式に解決できる。この手順は、問題がより深刻であるか、非公式に解決できない場合に取られるべき正式な手順を示している。

1.3　この手順は、勤続期間に関係なく全ての従業員に適用されます。派遣労働者や自営業の請負業者には適用されません。

1.4　この手順は、従業員の雇用契約の一部を構成するものではなく、当社はいつでも改変することができる。

2.　調査

2.1　懲戒審問が開かれる前に、問題が調査されます。当該調査の一環としての会議や話し合いは、事実を明らかにすることのみを目的としており、審問が行われることなく懲戒処分が行われることはない。

2.2　逸脱行為が疑われる場合、調査または懲戒手続（あるいはその両方）の間、あなたは業務を中止しなければならない可能性がある。[停職中は、許可されていない限り、当社施設を訪問したり、クライアント、顧客、納入業者、請負業者、スタッフに連絡してはならない。]停職は、懲戒処分とは見なされない。

3.　審問

3.1　審問は、申し立てられた逸脱行為又は業績の低下、及び、考えられる結果に関して、準備を可能にする十分な情報を含めて、当社があなたに書面で通知する。通常、関連する書類及び証人陳述書のコピーが渡される。

3.2　審問には、労働組合の代表者又は同僚が、あなたに同席することができる。同僚は、あなたの同伴者として行動するために、合理的な有給休暇を与えられる。

3.3　審問に出席させたい関連する証人、または検討したい文書やその他の証拠がある場合は、できるだけ早くお知らせください。

3.4　決定は、審問から通常 1 週間以内に書面で通知される。

4.　懲戒処分と解雇

4.1　逸脱行為又は業績低下に対する通常の罰則は、以下のとおりである:

(a)　第 1 段階: 第一警告状[又は、改善通告].他の有効な警告状[又は、改善通告]があなたの懲戒記録に無い場合、あなたは、通常第一警告状[又は、改善通告]を受け取る。それは、6 ヶ月間有効に存続する。

(b) 第 2 段階: 最終警告状. 有効な第一警告状[又は、改善通告]があなたの懲戒記録に存在し、さらなる逸脱行動又は改善の欠如がある場合、あなたは、通常最終警告状を受け取る。重大な逸脱行為又は業績不良の場合には、第一警告状[又は、改善通告]なく、これが使用されても良い。この警告状は、12 ヶ月間有効に存続する。

(c) 第 3 段階: 解雇又は他の処分. 最終警告状があなたの懲戒記録に存在し、さらなる逸脱行動又は改善の欠如がある場合、又は、重大な逸脱行動がある場合、あなたは、解雇となりうる。重大な逸脱行為の例は、以下(6)がある。また、試用期間中の逸脱行為や不満足な業績について、警告なしに解雇されうる。

(d) 降格または別の役割への再配置（契約で許可されている場合）、及び/又は、さらなる見直し期間を伴う、最終的な書面による警告の延長を含む、解雇に至らない他の制裁を検討する場合がある。

5. 不服申立て

5.1 決定を受けてより 3 週間以内に、不服申立てをすることができる。

5.2 不服申立ての審問は、可能であれば、原審問に関与した者以外の者によって、行われる。同僚又は労働組合の代表者を、不服申立ての審問に、連れて行くことができる。

5.3 最終決定については、できるだけ早く、通常は、不服申立審理から、1 週間以内に書面で通知される。それ以上に、不服申立てを行う権利はない。

6. 重大な逸脱行為

6.1 重大な逸脱行為は通常、警告なしに解雇され、通告、又は、通告の代わりの支払いが行われない（要約解雇）。

6.2 重大な逸脱行為は、重大な契約違反であり、私たちの意見では、私たちのビジネスや評判を損なうか、当社の仕事上の関係や信頼を、取り返しのつかないほど損なう可能性のある逸脱行為が含まれる。これには、仕事以外で行われた逸脱行為が含まれうる。以下が、通常、重大な逸脱行為と見なされる件の例である。:

(a) 窃盗または詐欺;

(b) 身体的暴力またはいじめ;

(c) 財物への故意かつ重大な損傷;

(d) 組織の財物または名前の重大な誤用;

(e) ポルノ、攻撃的、又は、わいせつな素材を含むインターネットサイトに故意にアクセスすること;

(f) 深刻な不服従;

(g) 違法な差別、危害、嫌がらせ;

(h) 組織を深刻な不評に陥れること;

(i) アルコールまたは違法薬物によって引き起こされた、職場での深刻な能力欠如;

(j) 重大な過失により損失、損傷、又は傷害を引き起こすこと;

(k) 健康と安全に関する規則の重大な違反;

(l) 重大な守秘義務違背;

このリストは、ガイドとして意図されており、網羅的なものでない。

Schedule 2　　苦情処理

1.　Step 1: 書面による苦情

1.1　苦情を書面で提出し、ラインマネージャーに提出する必要がある。あなたの苦情があなたのラインマネージャーに関係しているなら、あなたはそれを[　　]に提出することができる。

1.2　書面による苦情は、調査できるように、関連する事実、日付、関係者の名前など、苦情の性質を記載する必要がある。

2.　Step 2: 会議

2.1　苦情処理会議は、通常、書面による苦情を受け取ってから[1 週間]以内に、開催される。あなたが出席できるよう、あらゆる努力をしなければならない。

2.2　会議は、更に調査を行う必要がある場合、延期されることがある。その後、会議は、通常再開される。

2.3　通常、最後の苦情処理会議から 2 週間以内に、決定を下し、苦情を解決するために取られる、さらなる措置について通知する。また、不服申立権についても通知される。

3.　Step 3: 不服申立て

3.1　あなたは、決定があなたに送られた、または与えられた日から 3 週間以内に、あなたの不服の理由を書面で訴えることができる。

3.2　通常、不服申立てを受けてから、4 週間以内に、不服申立会議を開催する。これは、それまで事件に関与したことのない 3 人のマネージャーによって、公平に処理される。

3.3　最終決定は、書面で確認する。通常、不服申立審理から 2 週間以内になされる。それ以上の不服申立権はない。

Schedule 3　　IT ポリシー

1.　対象及び適用範囲

本ポリシーは、従業員による当社 IT インフラストラクチャの利用を規律するものであり、特に以下を対象とする。

- 当社の電子メールシステムの利用
- 業務におけるインターネットの利用
- 当社イントラネットの利用
- 当社が提供するコンピュータ機器（PC、事業所外で使用するノート PC、その他全てのハードウェア及びソフトウェア）の使用及び活用
- 当社が提供するコミュニケーション手段（電話・FAX、携帯電話、電子メールの送受信用モバイル機器）の使用及び活用

本ポリシーは、当社の IT インフラストラクチャを利用する全ての従業員に適用される。

2.　IT インフラストラクチャの利用

当社の IT インフラストラクチャは、社内外のコミュニケーションの向上、業務効率の向上、情報取得及び作業プロセスの迅速化を目的として提供されるものです。したがって、IT インフラストラクチャは、従業員が業務を遂行する目的に限り利用することができる。

以下の規定及び制限に従うことを条件として、業務遂行や IT インフラストラクチャの可用性を損なわず、かつ当社の利益に反しない範囲に限り、従業員による一定の私的利用も認められる。

本ポリシーにおいて私的利用が認められている場合であっても、これは当社が任意に提供するものであり、当社はいつでもこれを撤回することができる。

3.　IT インフラストラクチャ利用に関する一般規則

従業員は、IT インフラストラクチャを利用するにあたり、適用される法令及び社内規程を遵守しなければならない。

当社の名誉又は IT インフラストラクチャの安全性を損なうおそれのある利用をしてはならない。

特に、以下の行為を禁止するものとする。

- 人格権、著作権又は刑事法令に違反する内容の提供、閲覧、保存又は配布
- イデオロギー的又は政治的広告の提供、閲覧、保存又は配布
- わいせつ、差別、暴力賛美、反憲法的、テロ関連その他違法な内容の提供、閲覧、保存又は配布
- チャットサイト及びファイル共有ネットワークの利用

4. 当社電子メールシステム、イントラネット及びインターネットの利用

4.1 電子メールシステムの利用

当社の電子メールシステムの私的利用は禁止される。受信した私的電子メールは、閲読後速やかに削除しなければならない。私的電子メールの送信者に対しては、当該メールアドレスは業務目的のみに使用されるべきである旨を受信者が通知しなければならない。私的な電子メールのやり取りは、無料のウェブメールサービスを通じてのみ行うことができる。

【当社では、追加的なセキュリティリスクに鑑み、Gmail や Hotmail 等のウェブベースの個人用メールへのアクセスを当社のコンピュータシステム上で一切許可しない。】

迅速な業務連絡を確保するため、各従業員は不在時の代理者を指定し、当該代理者に業務用メールアカウントへのアクセス権を付与しなければならない。

予見可能な不在の場合、従業員は「自動返信」機能により不在期間を送信者に通知しなければならない。予見不可能な不在の場合には、指定された代理者が当該機能の設定を行うものとする。

当社は、電子メールに電子署名を付与し、又は暗号化を行う権利を留保する。上司は、特定の内容を含むメールについて、電子署名及び／又は暗号化を施して送信するよう指示することができる。

従業員は、侮辱的、猥褻、差別的、人種差別的、嫌がらせ的、誹謗的、中傷的、ポルノ的又はその他不適切な電子メールを送信してはならない。

さらに、従業員は特に以下の行為を行ってはならない。

(a) 職場において、第三者に読まれたくないような私的な電子メールを送信・転送すること
(b) チェーンメール、迷惑メール、漫画、ジョーク又は噂話を送信又は転送すること
(c) 些細なメッセージを送信すること、又は受領の必要性が認められない者を宛先に不必要に追加し若しくはその者に転送することにより、システムに負荷を生じさせること
(d) （許可がある場合を除き）他人のメールアドレスから、又は偽名を用いてメッセージを送信すること

4.2 イントラネットの利用

当社イントラネットの私的利用は禁止する。従業員は、自らの上司の承認を得た場合に限り、コンテンツを掲載することができる。

4.3　インターネットの利用

インターネットの私的利用は、本ポリシーの遵守状況を監視するために必要な以下の措置について、従業員が書面による同意を行った場合に限り認められるものとする。従業員は、当該同意書に署名するか否かについて自由に決定することができる。同意しない場合、又は同意を撤回した場合には、従業員によるインターネットの私的利用は禁止される。

インターネットは、私的利用に要する時間が軽微であり、かつ従業員の休憩時間中に限り、私的に利用することができるものとする。利用時間は1週間あたり 1時間を超えてはならない。

使用者は、アクセス可能な特定のウェブサイトを裁量によりブロック又は制限することができる。

4.4　例外

本セクションに定める禁止事項の例外は、業務上の必要に伴う私的利用及び緊急時における私的利用に限られる。

4.5　コントロール

インターネットアクセスに関する接続データは、アクセス時刻、接続先アドレス及びデータ転送量を記録した上で、匿名化又は仮名化された形式で保存されるものとし、技術的障害の分析・修正、システム性能・システムセキュリティの確保・最適化、利用総量の把握、又は不正利用に対する抜き打ち検査を行うことを目的として使用される。

業務利用と私的利用の技術的区別は行わないものとする。

取得されたログは抜き打ち的に評価され、評価自体は個人識別不可能な形で行われる。

評価の結果、犯罪行為または重大な義務違反、特に本ポリシーに基づく義務違反の疑いが生じた場合には、データ保護責任者の関与のもと、当該データを個人と結びつけることができる。

5.　セキュリティ対策および機密保持

5.1　パスワード

本項は、認証された従業員を認証するために使用されるパスワードの作成及び取扱いについて定めるものである。本規定は、無断アクセス、不正使用又は変更から保護するためにパスワードで保護されている当社の全ての IT システムに適用される。

- パスワードは秘密として保持し、第三者に開示してはならない。パスワードは他人に見られないように入力し、特に、ファンクションキーへの登録又はコン

ピュータ上への平文での保存をしてはならない。第三者に属するパスワードを使用してはならない。

- パスワードは推測されやすいものであってはならない。氏名、車両番号、誕生日等の安易なパスワードを使用してはならない。
- パスワードには、少なくとも 1 つの記号又は数字を含めなければならない。体系的なパスワード推測を防止するため、パスワードは可能な限り複雑でなければならない（大文字・小文字・数字・記号の組合せ）。
- パスワードは 6 文字以上でなければならない。複数回の誤入力が行われた場合、アクセスは自動的にブロックされるものとする。
- パスワードが無権限者に知られた場合、又はその疑いが生じた場合には、直ちに変更しなければならない。

5.2 コピー及びインストールの禁止

当社 IT システムにおいて使用することができるソフトウェアは、当社 IT 部門が承認したものに限られるものとする。。プログラムのダウンロード及びソフトウェアのインストールは IT 部門のみが行うことができ、同部門が IT との互換性、ウイルス・トロイの木馬等の有害要素の有無、ライセンス条件を確認するものとする。

従業員の IT システムにインストールされたソフトウェアを改変してはならない。また、当該ソフトウェアを私物のコンピュータや私的な記録媒体にコピーすることも禁止される。

私物のハードウェア及びソフトウェア（私物の携帯電話、PDA、カメラ、USB メモリ等）を業務目的で使用することは、IT 部門の承認がない限り許可されない。これらを当社の IT システムに接続することも禁止される。

システム設定の変更（インストール、アンインストール、構成変更等）は、IT 部門のみが行うことができる。

5.3 有害コンテンツ及びスパムからの保護

当社の IT システムには、ウイルス、ワーム、トロイの木馬等の有害コンテンツを除去するためのフィルタリング機能によって保護されている。従業員は、受信した電子メールの添付ファイルに有害コンテンツが含まれていないか必ず確認しなければならない。指定された保護機能を無効化してはならない。疑わしい事象を発見した場合には、直ちに、第 5.5 条に定める担当部署に報告しなければならない。

当社は、迷惑メールから保護するための適切なフィルタシステムを運用している。これらのシステムの使用は任意とする。スパムと疑われるメールが誤って削除されることを防ぐため、当該メールは自動削除されることなく、別フォルダに移動されるものとする。

5.4 データの可用性

データは容易に検索できるように保存しなければならない。

データ損失のリスクを軽減するため、定期的なデータバックアップを実施する必要がある。

5.5 追加のセキュリティ対策

従業員は、無権限者が情報や IT アプリケーションにアクセスできないよう、職場環境を適切に整える義務がある。

- 長時間職場を離れる際には、IT 機器を必ず電源オフにしなければならない。また、パスワード保護された画面ロックを使用しなければならない。画面ロックは、職場を離れる際に手動で作動させるか、又は 5 分後に自動的に作動するよう設定する必要がある。
- 公共エリアでは、モニター、プリンター、FAX 等を第三者による閲覧のリスクを可能な限り排除できる位置に配置しなければならない。
- 中央プリンター及びコピー機で出力された資料は速やかに回収し、原稿は必ず取り除かなければならない。
- モバイル記録媒体は、権限を有する者のみがアクセスできるよう保管しなければならない。モバイル IT 機器についても同様である。

5.6 セキュリティインシデント発生時の対応

セキュリティインシデントとは、当社 IT システムの安全性及び完全性に関連する一切の事象を指す。これには、無権限の第三者による機密データへのアクセスを生じさせるエラー、保護すべきデータの完全性の損失若しくはデータ喪失をもたらす事象、ハードウェア・ソフトウェアの固有の欠陥によるセキュリティホール、マルウェアの発生又は犯罪行為（インターネットサーバーのハッキング、IT システムの侵入、データ窃盗等）が含まれるものとする。

セキュリティインシデントが発生した場合、関係者は冷静を保ち、軽率な措置は避けなければならない。対処措置は、以下の報告プランに記載された権限者からの要請後に限り実施することができるものとする。

セキュリティインシデントへの対応にあたっては、誠実さ及び協力の意思が特に重要である。セキュリティインシデントは、直ちに以下に記載の担当部署へ報告しなければならない。影響を受けた者は、被害最小化のため、関連する状況を漏れなく、かつ事実に即して報告しなければならない。

セキュリティインシデントの報告プラン：

事象	報告先
機密データへの無権限第三者によるアクセスの疑い 機密データが無権限第三者に開示された疑い ハードウェア又はソフトウェアのセキュリティホール 犯罪行為 その他の事案	セキュリティ担当者

IT システムの機能に関するエラー又は障害	IT 管理者
マルウェアの疑い	ウイルス対策担当者

6. 施行日

本ポリシーは、［…］に最終更新された。

私は、本 IT ポリシーの写しを受領したことを署名により確認する。

2　従業員との秘密保持契約書の例

Annex 2 – Confidentiality Clause in Employment Contract

§1 Geheimhaltung und Rückgabe von Unterlagen	§1 Confidentiality and Return of Documents
(1) Der Arbeitnehmer ist verpflichtet, insbesondere auch während der Zeit nach Beendigung dieses Arbeitsvertrages alle vertraulichen Angelegenheiten, Betriebs- und Geschäftsgeheimnisse des Arbeitgebers und verbundener Unternehmen, welche ihm bei Ausübung seiner Tätigkeiten für den Arbeitgeber zur Kenntnis gelangen (insbesondere Verfahren, Daten, Know-how, Marketing-Pläne, Geschäftsplanungen, unveröffentlichte Bilanzen, Budgets, Lizenzen, Preise, Kosten und Kunden- und Lieferantenlisten) oder die vom Arbeitgeber als vertraulich bezeichnet werden, streng geheim zu halten.	(1) During and after the term of this Employment Agreement, the Employee shall treat as strictly confidential all confidential matters and trade and business secrets of the Employer and all Affiliated Companies, of which he/she obtains knowledge during the exercise of his/her duties for the Employer (including procedures, data, know-how, marketing plans, business planning, unpublished balance sheets, budgets, licenses, pricing, costs and customer and supplier lists) or which are designated as confidential by the Employer.
(2) Sowohl während der Dauer des Arbeitsvertrags als auch nach seiner Beendigung wird der/die Arbeitnehmer/in alle ihm/ihr während der Vertragsdauer bekannt gewordenen Geschäftsgeheimnisse im Sinne des Geschäftsgeheimnisschutzgesetzes streng geheim halten, auch gegenüber anderen Mitarbeitern des Arbeitgebers, die mit diesem Sachverhalt nicht befasst sind.	(2) Both during the term of this Employment Agreement and after its termination, the Employee shall keep all business secrets within the meaning of the Trade Secrets Protection Act that become known to him/her during the term of the contract strictly confidential, even towards other employees of the Employer who are not involved in this matter.
(3) Die Geheimhaltungspflicht gilt nicht hinsichtlich solcher Tatsachen, die jedermann zugänglich oder öffentlich bekannt sind oder deren Weitergabe zur Erfüllung der Aufgaben des Arbeitnehmers erforderlich ist. Im Zweifelsfall hat der Arbeitnehmer eine Weisung des Arbeitgebers zur Vertraulichkeit bestimmter Tatsachen oder Umstände einzuholen. Ferner gilt die Geheimhaltungspflicht nicht, wenn der Arbeitnehmer gesetzlich oder aufgrund einer gerichtlichen oder behördlichen Entscheidung verpflichtet ist, vertrauliche Informationen offenzulegen. In diesem Fall wird der Arbeitnehmer gegenüber dem Arbeitgeber vor der Offenlegung die bevorstehende Pflicht zur Offenlegung unverzüglich anzeigen Die Geheimhaltungspflicht gilt nicht in den Fällen des § 5 GeschGehG.	(3) The duty of confidentiality shall not apply to facts that are accessible to everyone or publicly known, or whose disclosure is necessary for the Employee to perform their duties. In case of doubt, the Employee shall seek instructions from the Employer regarding the confidentiality of certain facts or circumstances. Furthermore, the duty of confidentiality shall not apply if the Employee is obliged by law or by a court or official decision to disclose confidential information. In this case, the employee shall immediately notify the Employer of the impending obligation to disclose before disclosure. The duty of confidentiality shall not apply in the cases specified in § 5 GeschGehG.
(4) Bei Beendigung des Arbeitsverhältnisses oder bei Freistellung wird der Arbeitnehmer dem	(4) The Employee shall, upon termination of the employment or in the event of the Employee being

Arbeitgeber unaufgefordert, während des Bestehens seines Arbeitsverhältnisses auf Anforderung, alle in seinem Besitz befindlichen, den Arbeitgeber oder die Verbundenen Unternehmen betreffenden Unterlagen und Datenträger, insbesondere alle Notizen, Berichte, Memoranden, Aufzeichnungen, Akten, Zeichnungen, Protokolle und andere ähnliche Dokumente (sowie Kopien oder sonstige Reproduktionen hiervon) zurückgeben.	released from his/her duties, without being asked, and during the existence of his/her employment, upon request, return to the Employer all documents and data carriers in his/her possession which relate to the Employer or to any Affiliated Company including notes, reports, memoranda, records, files, drawings, protocols and other similar documents (as well as copies or other reproductions thereof).
(5) Der Arbeitnehmer erkennt an, dass die vorgenannten Unterlagen alleiniges Eigentum des Arbeitgebers oder der Verbundenen Unternehmen sind. Der Arbeitnehmer hat an den genannten Unterlagen kein Zurückbehaltungsrecht.	(5) The Employee acknowledges that the documents referred to above are the sole property of the Employer or any Affiliated Company. The Employee has no right of retention regarding these documents.
(6) Veröffentlichungen und Vorträge des Arbeitnehmers während der Dauer des Arbeitsverhältnisses bedürfen der vorherigen Zustimmung des Arbeitgebers, soweit diese die Branche, Erzeugnisse oder Dienstleistungen des Arbeitgebers betreffen. Die Zustimmung ist zu erteilen, wenn keine gemäß Absatz (1) geheimhaltungsbedürftigen Tatsachen mitgeteilt und auch ansonsten keine schützenswerten Interessen des Arbeitgebers verletzt werden. (alternativ: Dem Arbeitnehmer ist es gestattet, Fachvorträge zu halten und unter eigenem Namen zu veröffentlichen. Die Verschwiegenheitspflicht gemäß Absatz (1) bleibt unberührt.)	(6) Any publications and lectures of the Employee during the term of the employment require the prior consent of the Employer in so far as such publications and lectures concern the branch, products or services of the Employer. The Employer shall grant such consent if no information required to be kept confidential as described in para. (1) will be disclosed, and no other interests of the Employer which deserve protection are disregarded. (alternatively: The Employee may give professional lectures and publish under his/her own name. The confidentiality obligation pursuant to para. (1) remains unaffected.)
§2 Datensicherheit	§2 Data Security
(1) Das Kopieren von Daten und/oder Software auf mobile Datentrüber ist verboten, soweit nicht in Textform durch den Arbeitgeber gestattet. Der Arbeitnehmer hat ist verpflichtet, bei Verlassen seines Arbeitsplatzes seinen Computer gegen unbefugte Zugriffe zu sperren.	(1) The copying of data and/or software to mobile data carriers is prohibited unless permitted in text form by the employer. The employee is obliged to lock his computer against unauthorised access when leaving his workplace.
(2) Der Arbeitnehmer ist verpflichtet, alle betriebsbezogenen Daten nur auf dem vom Arbeitgeber zugewiesenen Serververzeichnis abzulegen. Die Speicherung von Daten auf Desktoprechnern ist aus Schutz- und Sicherheitsgründen vermieden werden.	(2) The employee is obliged to store all company-related data only on the server directory assigned by the employer. The storage of data on desktop computers shall be avoided for reasons of protection and security.
(3) Der Arbeitnehmer ist im Rahmen der allgemeinen Sorgfaltspflichten für den Schutz der auf einem dezentralen Rechner befindlichen Daten verantwortlich. Dies gilt insbesondere für Daten auf Notebooks.	(3) Within the general duties of care, the employee shall be responsible for the protection of data located on a decentralised computer. This applies in particular to data on notebooks.
(4) Der Arbeitgeber stellt sicher, dass der Arbeitnehmer in einer für die jeweilige Aufgabenstellung gesicherten Arbeitsumgebung	(4) The employer shall ensure that the employee works in a secured working environment for the respective task, i.e. appropriate programmes and

arbeitet, also entsprechende Programme und Geräte zur Verschlüsselung bzw. Sicherung werden zur Verfügung gestellt. Der Arbeitnehmer ist verpflichtet, die zur Verfügung gestellten Sicherungsmittel zu nutzen.	devices for encryption or backup shall be provided. The employee is obliged to make use of the security devices provided.
(5) Die Verwendung privater Geräte und Speicher für betriebsgezogene Tätigkeiten ist unzulässig. Sofern der Arbeitgeber mobile Gerate und Speicher (z.B. USB- Sticks) ausgibt, sind ausschließlich diese zulässig und dürfen ausschließlich mit betrieblichen Computern verwendet werden.	(5) The use of private devices and storage devices for business-related activities is not permitted. If the employer issues mobile devices and storage devices (e.g. USB drives), only these are permitted and may only be used with company computers.

（参考和訳）従業員との秘密保持契約書の例

雇用契約中の秘密保持義務

§1　機密保持と返還

(1) 本雇用契約の期間中及び終了後、従業員は、自己の職責を遂行する際に知ることとなった、又は、雇用主から機密情報として指定されている、雇用主と全ての関係会社の機密事項と事業秘密および営業秘密の全て（手順、データ、ノウハウ、マーケティング計画、事業計画、未発表の貸借対照表、予算、ライセンス、価格設定、コスト、顧客、および納入者リストを含む）を、機密として厳格に扱う。

(2) 従業員は、本雇用契約期間中に知り得た営業秘密保護法（GeschGehG）の意味におけるの一切の営業秘密について、契約期間中及び終了後を問わず、当該事項に関与しない他の従業員に対しても厳格な秘密保持義務を負うものとする。

(3) 秘密保持義務は、事実が一般にアクセス可能であるか公知となっている場合、又は従業員が自己の職務を遂行するために当該事実の開示が必要である場合には適用されない。疑義がある場合には、従業員は、特定の事実又は状況が秘密情報に該当するか否かについて、雇用主に指示を求めなければならない。

また、従業員が法令、裁判所の決定又は行政機関の命令により機密情報の開示を義務づけられる場合にも、秘密保持義務は適用されないものとする。この場合、従業員は、開示に先立ち、開示義務が生じる旨を直ちにに雇用主に通知しなければならない。

さらに、秘密保持義務は営業秘密保護法（GeschGehG）第 5 条に定める場合にも適用されないものとする。

(4) 従業員は、雇用終了時又は離職の求めの際、要請されるまでもなく、及び、雇用中、要請に応じて、雇用主または関連会社に関連する、所有している全ての文書及びデータ伝送手段（ノート、レポート、メモ、記録、ファイル、図面、プロトコル、及び、その他の同様の文書、並びに、そのコピーや複製も含む）を雇用主に返還する。

(5) 従業員は、上記の文書は、雇用主または関連会社だけの財産であり、従業員が、これら文書に関して保持する権利はないことを認める。

(6) 従業員が、雇用期間中に行う発表や講演には、そのような発表や講義が、雇用主の支部、製品又はサービスに関係する限り、雇用主の事前の同意が必要となる。雇用主は、前(1)項に記載されたような機密とすべき情報が、開示されることがなく、保護に値する雇用主の他の利益が損なわれることがない場合、そのような同意を与えるものとする。（従業員は、自己の名前で専門的な講義を行い、発表することができる。但し、従業員の、前(1)項の守秘義務は、変更がない）

§2　データ安全性

(1) 雇用主によって文書で許可されていない限り、モバイルデータキャリアへ、データ及び/またはソフトウェアのコピーは禁止される。従業員は、職場を離れるとき、不正アクセスに対応し、コンピューターをロックする義務を負う。

(2) 従業員は、会社関連のデータは全て、雇用主によって割り当てられたサーバーディレクトリへ保管する義務を負う。デスクトップコンピューターへのデータの保存は、保護及びセキュリティの理由から、避けるようにする。

(3) 従業員は、分散型コンピューターにあるデータの保護に、一般的な注意義務の範囲内で、責任を負う。これは、ノートブックのデータに、特に適用される。

(4) 雇用主は、従業員が、それぞれの作業のための安全な環境、すなわち、適切なプログラムと装置の暗号化又はバックアップの提供をするものとする。従業員は、提供されるセキュリティデバイスの使用をする義務がある。

(5) ビジネス関連の活動に、私的なモバイル装置や保存装置を使用することは許可されていない。雇用主が、モバイル装置と保存装置（USB ドライブなど）を提供する場合、これらのみが許可されており、会社のコンピューターに使用できる。

3　退職後の競業避止契約書の例

Annex 3 – Employer-employee non-compete agreement after resignation

§1 Für die Dauer von [•] Monaten nach Beendigung des Arbeitsverhältnisses ist es dem Arbeitnehmer untersagt, mit dem Arbeitgeber in Wettbewerb zu treten („Wettbewerbsverbot“).	§1 For a period of [•] months after termination of the employment relationship, the employee is prohibited from competing with the employer ("non-competition obligation").
§2 Das Wettbewerbsverbot bezieht sich - sachlich auf alle Bereiche, in denen der Arbeitgeber zu dem Zeitpunkt, in dem das Arbeitsverhältnis endet, tätig ist und - räumlich auf das gesamte Tätigkeitsgebiet des Arbeitgebers zu dem Zeitpunkt, in dem das Arbeitsverhältnis endet. Sachlicher und räumlicher Geltungsbereich des Wettbewerbsverbots werden zusammenfassend als „Geschäftsbereich“ bezeichnet.	§2 The non-competition obligation relates - materially to all areas in which the employer is active at the time the employment relationship ends and - territorially to the employer's entire area of activity at the time the employment relationship ends. The material and territorial scope of the non-competition obligation are collectively referred to as the "business area".
§3 Das Wettbewerbsverbot umfasst jegliche Wettbewerbstätigkeit im Geschäftsbereich des Arbeitgebers, sei es direkt oder indirekt, selbständig, als freier Mitarbeiter, arbeitnehmerähnlich oder als Arbeitnehmer/Angestellter, durch Errichtung eines oder Beteiligung an einem Wettbewerbsunternehmen, durch beratende Tätigkeiten oder auf sonstige Weise.	§3 The non-competition obligation includes any competitive activity in the employer's business area, whether directly or indirectly, self-employed, as a freelancer, quasi-employee or as an employee/ employee, through the establishment of or participation in a competitive company, through advisory activities or in any other way.
§4 Der Arbeitgeber verpflichtet sich, dem Arbeitnehmer für die Dauer des Wettbewerbsverbots eine Karenzentschädigung zu zahlen, die für jedes Jahr des Verbots die Hälfte der vom Arbeitnehmer zuletzt bezogenen vertragsmäßigen Leistungen erreicht. Anderweitigen Erwerb muss sich der Arbeitnehmer gemäß §74c HGB anrechnen lassen. Der Arbeitnehmer ist verpflichtet, unaufgefordert spätestens am Schluss eines jeden Kalendervierteljahres anzugeben, ob und in welcher Höhe er anderweitige Einkünfte bezieht. Auf Verlangen hat der Arbeitnehmer die Angaben zu belegen.	§4 The employer undertakes to pay the employee for the duration of the noncompetition obligation a waiting allowance equal to half of the contractual benefits last received by the employee for each year of the non-competition obligation. The employee must take into account any other earnings pursuant to section 74c HGB. The employee is obliged to declare, without being asked, at the latest at the end of each calendar quarter, whether and to what extent he receives other income. Upon request, the employee shall provide evidence of the information.
§5 Das Wettbewerbsverbot gilt auch mit einem Rechtsnachfolger des Betriebs, insbesondere geht es bei einer Veräußerung auf den Erwerber über. Der Arbeitnehmer ist mit	§5 The non-competition obligation shall also apply with a legal successor of the business, in particular it shall pass to the acquirer in the event of a sale. The employee agrees to the transfer of his rights under this agreement.

dem Übergang seiner Rechte aus dieser Vereinbarung einverstanden.	
§6 Der Arbeitgeber kann vor Beendigung des Arbeitsverhältnisses durch schriftliche Erklärung auf das Wettbewerbsverbot mit der Wirkung verzichten, dass er mit Ablauf eines Jahres seit der Erklärung von der Verpflichtung frei wird, die Karenzentschädigung zu zahlen.	§6 The employer may, before termination of the employment relationship, waive the non-competition obligation by written declaration with the effect that he shall be released from the obligation to pay the waiting compensation upon expiry of one year from the declaration.
§7 Das nachvertragliche Wettbewerbsverbot tritt nur in Kraft, wenn das Arbeitsverhältnis vom Arbeitgeber oder Arbeitnehmer nicht vor Ablauf der Probezeit gekündigt wird. Das nachvertragliche Wettbewerbsverbot tritt nicht in Kraft, wenn das Arbeitsverhältnis aufgrund Eintritts in den Ruhestand endet.	§7 The post-contractual non-competition obligation shall only enter into force if the employment relationship is not terminated by the employer or the employee before the end of the probationary period. The post-contractual non-competition obligation shall not enter into force if the employment relationship ends due to retirement.
§8 Verstößt der Arbeitnehmer schuldhaft gegen das Wettbewerbsverbot, ist er verpflichtet, eine Vertragsstrafe in Höhe des letzten Bruttomonatsgehalts zu zahlen.	§8 If the employee culpably violates the non-competition obligation, he shall be obliged to pay a contractual penalty in the amount of the last gross monthly salary.
Besteht die Verletzungshandlung in der kapitalmäßigen Beteiligung an einem Wettbewerbsunternehmen oder der Eingehung eines Dauerschuldverhältnisses (zB Arbeits-, Dienst-, Handelsvertreter oder Beraterverhältnis), wird die Vertragsstrafe für jeden angefangenen Monat, in dem die kapitalmäßige Beteiligung oder das Dauerschuldverhältnis besteht, neu verwirkt (Dauerverletzung). Mehrere Verletzungshandlungen lösen jeweils gesonderte Vertragsstrafen aus, gegebenenfalls auch mehrfach innerhalb eines Monats. Erfolgen dagegen einzelne Verletzungshandlungen im Rahmen einer Dauerverletzung, sind sie von der für die Dauerverletzung verwirkten Strafe mit umfasst. Werden mehrere Vertragsstrafen verwirkt, ist der Gesamtbetrag der zu zahlenden Vertragsstrafen auf das Sechsfache des letzten Bruttomonatsgehalts begrenzt.	If the act of violation consists of a capital participation in a competitor company or of entering into a continuing obligation (e.g. employment, service, commercial agent or consulting relationship), the contractual penalty shall be forfeited anew for each month or part thereof during which the capital participation or the continuing obligation exists (continuing violation). Several acts of infringement each trigger separate contractual penalties, if necessary also several times within one month. If, on the other hand, individual acts of infringement occur within the scope of a continuing infringement, they are included in the penalty forfeited for the continuing infringement. If several contractual penalties are forfeited, the total amount of the contractual penalties to be paid is limited to six times the last gross monthly salary.
Die Geltendmachung von Schäden, die über die verwirkte Vertragsstrafe hinausgehen, bleibt vorbehalten. Vorbehalten bleibt auch die Geltendmachung aller sonstigen gesetzlichen und vertraglichen Ansprüche und Rechtsfolgen aus einer Verletzung (zB Unterlassungsansprüche, Wegfall des Anspruchs auf Karenzentschädigung für die Dauer des Verstoßes usw).	The right to claim damages in excess of the forfeited contractual penalty is reserved. The right to assert all other statutory and contractual claims and legal consequences arising from a violation (e.g. injunctive relief, forfeiture of the right to compensation for waiting for the duration of the violation, etc.) is also reserved.

§9 Im Übrigen gelten die einschlägigen Vorschriften der §§74 ff HGB.	§9 In all other respects, the relevant provisions of §§74 ff HGB shall apply.

（参考和訳）退職後の競業避止契約書の例

雇用終了後の競業避止義務

§1　雇用関係の終了後[·]か月間、従業員は、雇用主と競争することを禁じられている（「競業避止義務」）。

§2　競業避止義務は、以下に関わる。

- 雇用関係が終了した時点で、雇用主が活動している全ての分野に、要素的に
- 雇用関係が終了した時点の、雇用主の活動領域全体に、地理的に

競業避止義務の要素と地理の範囲は、総して、「事業領域」と呼ばれる。

§3　競業避止義務には、直接または間接を問わず、自営業者、フリーランサー、準従業員、又は従業員/従業員として、競争相手の設立または参加を通じて、助言活動を通じて、若しくは、他の方法で、雇用主の事業領域で競争する行為を含む。

§4　雇用主は、非競争義務の期間中の従業員に、競業避止義務が課される毎年、当該従業員が最後に受け取った、契約上の利益の半分に等しい待機手当を支払うことを、約束する。

従業員は、HGB 第 74c 条に基づく、その他の収益を考慮に入れないとならない。従業員は、遅くとも各暦四半期の終わりに、質問されることなくとも、自己のその他の収益・収入を、受け取るかどうか、そしてどの程度受け取るか宣言する義務がある。従業員は、要求に応じて、情報の証拠を提供する。

§5　競業避止義務は、ビジネスの法的な後継者にも適用され、特に、それは、ビジネス売却の場合の取得者に移される。従業員は、本合意により、自分の権利の譲渡に同意する。

§6　雇用主は、雇用関係が終了する前に、競業避止義務を放棄する旨、そのような効果を伴う書面による宣言をして、宣言の 1 年経過から、待機中の補償を支払う義務から解放されることができる。

§7　契約後の競業避止義務は、試用期間が終了する前に、雇用者または従業員が雇用関係を終了しなかった場合にのみ、発効する。

契約後の競業避止義務は、退職により雇用関係が終了する場合、義務は発効しない。

§8　従業員が競業避止義務に有責に反した場合、最後の月給総額を、契約上の罰金として支払う義務がある。

違反行為が競合企業への資本参加または継続的な義務を伴う（雇用、サービス、商業代理店、コンサルティング関係など）合意の締結である場合、契約上の罰金は、資本参加または継続的な義務（継続的違反）が存在する毎月又はその一部について、新たに徴収される。いくつかの侵害行為は、必要な場合、1 か月内に数回、それぞれ個別の契約上の罰金をもたらす。

一方、個々の侵害行為が継続的侵害の範囲内で発生した場合、それらは継続的侵害に対して徴収される罰金に含まれる。複数の契約上の罰金が徴収された場合、支払われる契約上のペナルティの合計額は、最後の月給総額の 6 倍に制限される。

徴収された契約上の罰金を超える、損害賠償を請求する権利は留保される。他の、全ての法定および契約上の請求、並びに、違反から生じる、法的な権利主張（例：差止めによる救済、違反の期間について雇用待機に対する補償の権利の没収など）も留保される。

§9　その他の全ての点で、HGB§§74ff の規定が適用になる。

4　取引先との秘密保持契約書の例

Annex 4 – Confidentiality agreement with a business partner or customer

Präambel	**Preamble**
Zum Zwecke der Evaluierung von Möglichkeiten zur Eingehung einer Geschäftsbeziehung sowie ggf. zur Vorbereitung und Durchführung einer solchen beabsichtigen die Parteien, sich wechselseitig Zugang zu Informationen, Unterlagen, Zeichnungen und sonstigen Materialien, insbesondere Daten, zu gewähren, die vertrauliche Informationen und/oder Know-how der jeweils offenlegenden Partei enthalten.	For the purpose of evaluating the options of entering into a business relationship and, as the case may be, for the preparation and implementation of such relationship, the Parties intend to mutually disclose information, documents, drawings and other materials, including in particular data, containing confidential information and/or know-how of the disclosing Party.
Dies vorausgeschickt, verpflichten sich die Parteien gegenseitig zur Geheimhaltung Vertraulicher Informationen (wie nachfolgend definiert) der jeweils anderen Partei nach Maßgabe der folgenden Bestimmungen:	On this basis, the Parties mutually undertake to maintain confidentiality of the other Party's Confidential Information (as hereinafter defined) in accordance with the following provisions:
1. Definitionen und Auslegung	**1. Definition(s) and Interpretation**
(1) **Vertrauliche Informationen** im Sinne dieser Vereinbarung sind alle finanziellen, technischen, wirtschaftlichen, rechtlichen, steuerlichen und sonstigen in jedweder Form oder auf jedwedem Medium befindlichen Informationen (einschließlich Entwürfe, Fotografien, technische Zeichnungen, (Produkt-) Beschreibungen, Anleitungen, Software, Programme, Anweisungen, technisches, wissenschaftliches und betriebswirtschaftliches Know-how, Betriebsabläufe, Methoden, Bewertungsergebnisse, geschäftliche oder technische Pläne und Angebote, sonstige Daten), die der empfangenden Partei („**Empfänger**“) von der offenlegenden Partei („**Informationsgeber**“) zugänglich gemacht werden – und zwar gleich in welcher Form (sei es mündlich, schriftlich, elektronisch oder in sonstiger Form) und unabhängig von ihrer Qualität als Geschäftsgeheimnis im Sinne des § 2 Nr. 1 GeschGehG – oder dem Empfänger auf sonstige Weise zur Kenntnis gelangen und die als vertraulich oder in ähnlicher Weise bezeichnet oder gekennzeichnet sind oder deren vertraulicher Charakter aufgrund sonstiger Umstände erkennbar ist. Vertrauliche Informationen im Sinne dieser Vereinbarung schließen auch Verkörperungen, Kopien oder andere Reproduktionen oder Teile von Informationen ein. Eine vertrauliche Information	(1) **Confidential Information** within the meaning of this Agreement is all financial, technical, economical, legal, fiscal or other information in any form or medium (including drafts, photographs, technical drawings, (product-) descriptions, manuals, software, programmes, instructions, technical, scientific and economical know-how, operating procedures, methods, valuation results, business or technical plans and offers, other data) which is disclosed to the receiving Party ("**Recipient**") by the disclosing Party ("**Discloser**") – in any form whatsoever (orally, in writing, in electronic or other form) and independently from whether they are to be qualified as business secrets according to § 2 No. 1 of the German Business Secret Protection Act (GeschGehG) – or come to the Recipient's knowledge by other means and which are marked as confidential or whose confidential nature is evident due to other circumstances. Confidential Information within the meaning of this Agreement shall also include embodiments, copies or other reproductions or parts of information. Confidential Information within the meaning of this Agreement shall include the fact that Confidential Information has been disclosed to the Recipient, as well as the existence and the content of this Agreement.

im Sinne dieser Vereinbarung ist zudem die Tatsache, dass Vertrauliche Informationen dem Empfänger zur Kenntnis gebracht wurden, ebenso die Existenz und der Inhalt dieser Vereinbarung.	
(2) Vertrauliche Informationen im Sinne von vorstehender Ziff. 1.1 sind insbesondere auch jegliche Materialien, die Informationen beinhalten, die sich auf Technologien des Informationsgebers beziehen oder die Informationen mit Bezug zu derartigen Technologien oder zu den Finanzen, Geschäftsbeziehungen, dem Marketing und/oder der Forschung und Entwicklung des Informationsgebers enthalten. Dies gilt insbesondere auch für zukünftige Planungen und Prognosen in Bezug auf die Technologien des Informationsgebers.	(2) Confidential Information pursuant to Section 1.1 hereof includes in particular any materials containing information regarding the Discloser's technologies or materials containing information regarding such technologies, finance, business relationships, marketing and/or research and development of the Discloser. This shall apply in particular to plans and forecasts regarding the Discloser's technologies.
(3) Zu den Vertraulichen Informationen im hierin definierten Sinne gehören auch solche, die eine Partei der anderen vor Unterzeichnung dieser Vereinbarung offengelegt hat.	(3) Confidential Information as defined herein shall also include any information disclosed by either Party to the other before the signing of this Agreement.
(4) Der Informationsgeber wird dem Empfänger solche Informationen, die Geschäftsgeheimnisse Dritter enthalten, nur dann zugänglich machen, wenn er hierzu von dem bzw. den betreffenden Dritten ausdrücklich und schriftlich ermächtigt worden ist.	(4) The Discloser shall only make such information containing third party business secrets accessible to the Recipient if it has been expressly authorized to do so in writing by the third party or parties concerned.
2. Vertraulichkeitspflichten und Gebrauchsbeschränkungen	**2. Confidentiality Obligations and Restrictions of Use**
Unter Berücksichtigung der nachfolgenden Ziff. 3 wird der Empfänger nach Erhalt Vertraulicher Informationen vom Informationsgeber bzw., sofern nicht ein Ausnahmetatbestand gemäß nachfolgender Ziff. 3.4 vorliegt, nach Erhalt Vertraulicher Informationen, die erkennbar vom Informationsgeber stammen:	Subject to Section 3 below, upon receipt of the Confidential Information disclosed by the Discloser (or, unless the exception stipulated in Sect. 3.4 hereunder applies, where the Recipient has received Confidential Information from a third party which obviously originated from Discloser), the Recipient shall:
(1) die Vertraulichen Informationen streng vertraulich behandeln, die Vertraulichen Informationen nur für den Zweck, der mit dem Zugänglichmachen der Vertraulichen Informationen verfolgt wird, nutzen und diese Vertraulichen Informationen schützen, und zwar mit demselben Sorgfaltsmaßstab, mit dem der Empfänger regelmäßig seine eigenen Vertraulichen Informationen und Materialien schützt, mindestens jedoch mit der im Verkehr erforderlichen Sorgfalt; sofern die Vertraulichen	(1) hold the Confidential Information in strict confidence, use the Confidential Information only for the purpose which the Parties are attempting to achieve through disclosure and protect such Confidential Information by using the same degree of care as the Recipient uses to protect its own confidential information and materials of a similar nature, but not less than with the diligence required in the ordinary course of business; should Confidential Information contain personal data within the

Informationen personenbezogene Daten im Sinne der EU-Datenschutzgrundverordnung beinhalten, hat der Empfänger diese gemäß den in der EU geltenden Datenschutzvorgaben zu behandeln und zu speichern;	meaning of the European Union's Data Protection Regulations, the Recipient shall treat and store such data in full compliance with the rules and requirements of such data protection regulations;
(2) keine Vertraulichen Informationen oder Informationen, die diese Vertraulichen Informationen enthalten, offenlegen, veröffentlichen, verbreiten oder an Dritte weitergeben, mit Ausnahme der Weitergabe an Organmitglieder, Mitarbeiter und Berater des Empfängers, die a) diese Vertraulichen Informationen für den Zweck, der mit der Offenlegung der Vertraulichen Informationen verfolgt wird, kennen müssen, des Weiteren (b) darüber in Kenntnis gesetzt worden sind, dass die Vertraulichen Informationen den Bestimmungen dieser Vertraulichtkeitsvereinbarung unterliegen und c) mit dem Empfänger eine Anstellungs- oder eine anderweitige vertragliche Vereinbarung getroffen haben, die Vertraulichkeitsverpflichtungen enthält, die nicht weniger streng sind als die Vertraulichkeitsbestimmungen gemäß dieser Vereinbarung; der Informationsgeber darf Vertrauliche Informationen an Unterauftragnehmer, Lieferanten, Vertreter und andere nicht unter die oben in diesem Absatz (2) genannten Kategorien fallende Dritte nur mit vorheriger schriftlicher Genehmigung des Informationsgebers weitergeben.	(2) not disclose, publish or disseminate any such Confidential Information or any information incorporating such Confidential Information to any third party, except to its officers, employees and consultants of the Recipient who: (a) need to know such Confidential Information for the purpose which the parties are attempting to achieve through disclosure, (b) have been made aware that such Confidential Information is subject to the confidentiality obligations set forth in this Agreement, and (c) have entered into an employment contract or other agreement with the Recipient containing confidentiality obligations no less stringent than those contained in this Agreement; Recipient is permitted to disclose Confidential Information to his subcontractors, suppliers, agents and other external third parties not falling under the above categories of this subsection (2) only with Recipient's prior written consent;
(3) gegenüber dem Informationsgeber für jede Handlung oder Unterlassung der in vorstehender Ziff. (2) bezeichneten Dritten, die eine Verletzung von Vertraulichkeitspflichten darstellen, haftbar sein;	(3) be liable to Discloser for any act or failure to act by any of the individuals, entities or other third parties referred to in subsection (2) above;
(4) keine Kopie der Vertraulichen Informationen erstellen oder diese schriftlich zusammenzufassen oder durch Reverse Engineering verändern, sofern dies nicht für den Zweck, der mit dem Zugänglichmachen der Vertraulichen Informationen verfolgt wird, vernünftigerweise erforderlich ist. Alle Kopien oder Zusammenfassungen, die solchermaßen erstellt bzw. vorgenommen wurden, werden Eigentum (einschließlich aller darin enthaltenen Rechte am geistigen Eigentum) des Informationsgebers;	(4) not copy, reverse-engineer or reduce to writing any such Confidential Information, except as may be reasonably necessary for the purpose which the parties are attempting to achieve through disclosure; any copies or reductions so made become the property (including all intellectual property rights therein) of the Discloser;
(5) den Informationsgeber unverzüglich über jede Verletzung dieser Vereinbarung durch eines	(5) immediately inform the Discloser of any breach of this Agreement by any of its executive

seiner Organmitglieder, einen seiner Mitarbeiter und/oder Berater zu informieren und alle notwendigen Schritte einzuleiten, um jegliche negativen Wirkungen einer bestehenden Verletzung von Regelungen dieser Vereinbarung auszuschließen sowie künftige Verstöße gegen diese Vereinbarung zu vermeiden.	bodies, employees and/or consultants and shall take all steps needed to avoid negative effects of any current violation and to prevent future violations of this Agreement.
3. Ausnahmen	**3. Exceptions**
Der Begriff „Vertrauliche Informationen“ umfasst nicht solche Informationen, die:	The term “Confidential Information” does not include information which:
(1) sich bereits rechtmäßig und ohne Bestehen einer Vertraulichkeitspflicht im Besitz des Empfängers befunden haben, bevor der Empfänger die Informationen vom Informationsgeber erhielt;	(1) was already legitimately in the Recipient's possession and not subject to a duty of confidentiality, before the Recipient received the information from the Discloser;
(2) zum Zeitpunkt der Kenntniserlangung durch den Empfänger bereits öffentlich zugänglich waren oder es ohne Verschulden des Empfängers danach geworden sind;	(2) is/was in the public domain at the time the Recipient was provided with such information, or becomes part of the public domain without any culpable failure of the Recipient;
(3) vom Informationsgeber an Dritte weitergegeben wurden, ohne dass dem Dritten vom Informationsgeber eine Vertraulichkeitsverpflichtung bezüglich dieser Informationen auferlegt wurde;	(3) is disclosed by the Discloser to a third party without a duty of confidentiality placed on such third party;
(4) der Empfänger vor Abschluss dieser Vereinbarung von einem Dritten erlangt hat oder danach, jeweils ohne Verletzung dieser Vereinbarung, sofern der Dritte jeweils rechtmäßig in den Besitz der Informationen gelangt ist und durch die Weitergabe seinerseits gegen eine ihn bindende Vertraulichkeitsvereinbarung nicht verstößt;	(4) the Recipient received from a third party either before entering into this Agreement or afterwards without any violation of this Agreement, provided that the third party rightfully received the information and that by disclosing the information it does not infringe a non-disclosure agreement to which it is legally bound;
(5) der Empfänger eigenständig selbst entwickelt hat, ohne dass er auf die Vertraulichen Informationen des Informationsgebers zurückgegriffen oder darauf Bezug genommen hat;	(5) is independently developed by the Recipient without use or reference to the Discloser’s Confidential Information;
(6) die vom Empfänger mit vorheriger schriftlicher Zustimmung des Informationsgebers offengelegt werden. § 5 des Gesetzes zum Schutz von	(6) is disclosed by the Recipient with the Discloser's prior written approval. § 5 of the German Business Secret Protection Act (GeschGehG) remains unaffected.

Geschäftsgeheimnissen (GeschGehG) bleibt unberührt.	
4. Erlaubte Offenlegungen	**4. Permitted Disclosures**
Der Empfänger ist berechtigt, die Vertraulichen Informationen des Informationsgebers bzw. Teile davon offenzulegen, wenn und soweit der Informationsgeber dies vorab schriftlich gestattet hat oder wenn der Empfänger zur Offenlegung aufgrund der Anordnung eines zuständigen Gerichts oder einer Behörde oder aufgrund gesetzlicher Regelungen verpflichtet ist; er hat bei Vorliegen solcher Voraussetzungen, soweit rechtlich zulässig, rechtzeitig vor der Offenlegung den Informationsgeber über die Anordnung bzw. die gesetzlichen Regelungen und die dadurch betroffenen Vertraulichen Informationen schriftlich zu benachrichtigen und auf Aufforderung der offenlegenden Partei gegen die entsprechende Anordnung zur Offenlegung vernünftigerweise in Betracht kommende Rechtsmittel einzulegen.	The Recipient may disclose the Discloser's Confidential Information or parts thereof with the Discloser's prior written approval or if such disclosure is necessary in response to a valid order made by a court or other administrative body, or is otherwise required by law; in either of the foregoing cases, the Recipient is, unless prohibited by law, obliged to give written notice of the order or the legal basis and of the affected Confidential Information to the Discloser within due time before disclosure, and upon Discloser's request, he shall take reasonable efforts to object or appeal against any such court or administrative body order.
5. Eigentum und Rechte an Vertraulichen Informationen	**5. Ownership of and Rights in Confidential Information**
Der Informationsgeber behält jederzeit alle Rechte am geistigen Eigentum (einschließlich Patent-, Urheber- und Markenrechten) an den von ihm übermittelten Vertraulichen Informationen, keine Partei erhält durch diese Vereinbarung Rechte am geistigen Eigentum der anderen Partei. Es werden keine Rechte oder Lizenzen in oder an den Vertraulichen Informationen gewährt, mit Ausnahme der beschränkten Nutzungsrechte, die nach Maßgabe dieser Vereinbarung eingeräumt werden.	The Discloser shall, at all times, retain ownership of all intellectual property rights (including patents, copyrights and trademarks) in and to its Confidential Information, and neither Party acquires any intellectual property rights of the other Party under this Agreement. No rights or licenses in or to the Confidential Information are granted or implied other than the limited right to use such Confidential Information to the extent permitted by this Agreement.
6. Gewährleistungsausschluss, Haftung des Informationsgebers für Geschäftsgeheimnisse Dritter	**6. No Warranties, Discloser´s Liability for Third Parties´ Business Secrets**
(1) Der Empfänger akzeptiert die Vertraulichen Informationen ausdrücklich unter Ausschluss jeglicher Gewährleistung; der Informationsgeber gibt, soweit nichts anderes von ihm schriftlich bestätigt wird, keine Zusicherungen oder Gewährleistungen hinsichtlich der Vertraulichen Informationen, insbesondere ihrer Richtigkeit bzw. ihrer Fehlerfreiheit.	(1) The Recipient accepts the Confidential Information "AS IS"; unless otherwise declared in writing, the Discloser makes no representations or warranties with respect to the Confidential Information in particular not as regards their accuracy or faultlessness.

(2) Weder irgendeine Regelung in dieser Vereinbarung noch die Offenlegung von Vertraulichen Informationen darf im nachfolgenden Sinne ausgelegt werden:	(2) Nothing in this Agreement or in any disclosure of Confidential Information hereunder shall be construed as:
a) als Zusicherung oder als verbindliche Zusage in Bezug auf die Entwicklung oder die Verfügbarkeit von Produkten oder Dienstleistungen;	a) constituting or implying any representations or commitments as to the development or availability of products or services;
b) als Verpflichtung, irgendeine über diese Vereinbarung hinausgehende vertragliche Beziehung einzugehen, insbesondere nicht im Hinblick auf die Lieferung von Produkten oder die Erbringung von Dienstleistungen;	b) constituting an obligation to enter into any contractual relationship beyond this agreement, in particular not with regard to the delivery of Products or performance of Services;
c) als Verbot an den Empfänger, selbstständig Produkte oder Dienstleistungen zu entwickeln, die zu denen, die durch diese Vereinbarung umfasst sind, in Konkurrenz stehen (vorausgesetzt, dass solche Produkte oder Dienstleistungen nicht erst aufgrund des Erhaltes der Vertraulichen Informationen des Informationsgebers entwickelt werden);	c) prohibiting the Recipient from proceeding independently to develop products or services competitive with those involved herein (provided that, such products or services are not developed with the Discloser's Confidential Information provided hereunder); and/or
d) als Verbot zu Lasten einer Partei, sich mit Wettbewerbern der anderen Partei hinsichtlich Zwecken, die im Wesentlichen mit den von dieser Vereinbarung umfassten Zwecken ähnlich sind, zusammenzuarbeiten.	d) prohibiting either Party from cooperating with competitors of the other Party for purposes substantially similar to those provided for herein.
(3) Der Informationsgeber garantiert, dass er keine Geschäftsgeheimnisse Dritter an den Empfänger ohne deren bzw. dessen Zustimmung übermitteln wird bzw. übermittelt hat, es sei denn, diese Informationen sind ausdrücklich als Geschäftsgeheimnisse Dritter gekennzeichnet.	(3) The Discloser guarantees that it will not or has not transmitted any third-party business secrets to the Recipient without such third party´s consent, unless such information is expressly identified as third-party business secrets.
7. Schadenersatz- und Freistellungsansprüche, Vertragsstrafe	**7. Remedies, Indemnification, Penalty**
(1) Jede Partei erkennt an, dass die von ihr gemäß dieser Vereinbarung einzuhaltenden Pflichten notwendig und angemessen sind, um den Informationsgeber und sein Unternehmen zu schützen. Jede Partei erkennt darüber hinaus an, da wegen der Einzigartigkeit der Vertraulichen Informationen Schadenersatz in Form einer Geldzahlung unzureichend wäre, den Informationsgeber im Falle eines Verstoßes der anderen Partei für eine Verletzung der in dieser Vereinbarung enthaltenen Zusagen und Abmachungen zu entschädigen.	(1) Each Party acknowledges that its obligations set forth in this Agreement are necessary and reasonable in order to protect the Discloser and its business. Each Party furthermore expressly acknowledges that due to the unique nature of the Confidential Information, monetary damages would be insufficient to compensate the Discloser for any breach by the other Party of its covenants and agreements set forth in this Agreement. Accordingly, each Party agrees and acknowledges that any such violation or threat

Daher sind die Parteien sich übereinstimmend einig, dass eine jegliche tatsächliche oder auch nur drohende Verletzung für den Informationsgeber einen nicht wiedergutzumachenden Schaden bedeutet und dass deshalb zusätzlich zu allen gemäß anwendbarem Recht ohnehin bestehenden und unberührt bleibenden Rechtsbehelfen bzw. Ansprüchen der Informationsgeber	of violation shall cause irreparable injury to the Discloser and that, in addition to any other remedies that may be available on the basis of applicable law, the Discloser shall be entitled
a) das Recht hat, einstweiligen Rechtsschutz gegen eine drohende Verletzung dieser Vereinbarung bzw. gegen die Fortsetzung einer bereits eingetretenen Verletzung, die durch den Empfänger erfolgt oder ihm zuzurechnen ist, zu erwirken, ohne hierfür einen tatsächlich eingetretenen oder drohenden Schaden nachweisen zu müssen, und	a) to obtain injunctive relief against the threatened breach of this Agreement or the continuation of any such breach by or attributable to the Recipient, without the necessity of proving actual or impending damages, and
b) vom Empfänger die Freistellung bzw. den Ersatz von allen Schäden und Nachteilen (einschließlich des Ersatzes bzw. der Freistellung von Rechtsverfolgungskosten) verlangen kann, die ihm durch oder im Zusammenhang mit einer Verletzung der Verpflichtungen des Empfängers bzw. mit der Durchsetzung solcher Verpflichtungen bzw. der unerlaubten Offenlegung oder Verwendung seiner Vertraulichen Informationen durch den Empfänger selbst oder durch Dritte, denen der Empfänger Vertrauliche Informationen unzulässigerweise oder auch zulässigerweise überlassen hat, entstanden sind. Die unmittelbare Geltendmachung von Ansprüchen gegenüber Dritten wird durch die vorstehenden oder andere Regelungen in dieser Vereinbarung nicht eingeschränkt oder ausgeschlossen.	b) to be indemnified by the Recipient against any loss or harm, including but not limited to attorneys' and other legal fees, arising out of or in connection with any breach or enforcement of the Receiver's obligations under this Agreement or the unauthorized use or disclosure of the Discloser's Confidential Information by the Receiver or by third parties which have had access to the Confidential Information through act or failure to act by the Discloser, no matter if such access was permitted under this Agreement or not. Nothing in this Agreement shall be interpreted as to exclude or limit direct claims or legal action by Discloser against any third party.
(2) Für jeden Fall einer zurechenbaren Zuwiderhandlung gegen die Bestimmungen dieser Vereinbarung kann der Informationsgeber von dem Empfänger die Zahlung einer angemessenen Vertragsstrafe verlangen, die der Informationsgeber nach billigem Ermessen festlegen darf und deren Angemessenheit im Streitfall auf Antrag des Empfängers von einem zuständigen Gericht überprüft werden kann. Die Einrede des Fortsetzungszusammenhangs wird ausgeschlossen. Eine zu zahlende Vertragsstrafe ist auf etwaige Schadenersatzansprüche des Informationsgebers anzurechnen, wobei die Vertragsstrafe als Mindestschadensersatz anfällt.	(2) For each breach of any obligations committed by or attributable to the Recipient, the Discloser shall be entitled to demand payment of a penalty from the Recipient, the amount of which shall be determined by the Discloser in its equitable discretion, notwithstanding the Recipient's right to have a competent court of law decide on the appropriateness of such determination. The defense of continuation of an offense shall be excluded. Any penalty to be paid shall be deducted from Discloser's damages but shall always be regarded as minimum compensation.

(3) Der Informationsgeber hat unbeschadet eigener Schadenersatzansprüche den Empfänger von allen Ansprüchen, Forderungen und Haftungen Dritter (einschließlich angemessener Rechtsverteidigungskosten) sowie von etwaigen Strafgeldern und Bußgeldern freizustellen, die gegen den Empfänger aufgrund einer unberechtigten Offenlegung bzw. Weitergabe von Geschäftsgeheimnissen Dritter durch den Informationsgeber an den Empfänger geltend gemacht werden. Die vorstehenden Ansprüche bestehen nicht, sofern der Empfänger von der fehlenden Berechtigung des Informationsgebers Kenntnis hatte.	(3) Without prejudice to its own claims for damages, the Discloser shall indemnify the Recipient against all claims, demands and liabilities of third parties (including reasonable legal defense costs) as well as any penalties and fines asserted against the Recipient due to unauthorized disclosure or disclosure of third party trade secrets by the Discloser to the Recipient. The aforementioned claims do not exist if the Recipient was aware of the lack of authorization of the Discloser.
8. Laufzeit und Beendigung	**8. Term and Termination**
(1) Diese Vereinbarung tritt mit Unterzeichnung durch beide Parteien in Kraft und hat eine Laufzeit von 36 Monaten. Vertrauliche Informationen, die nach dem Ende der Laufzeit von einer Partei der anderen für den in der Präambel definierten Zweck offengelegt werden, fallen unter die Bestimmungen dieser Vereinbarung, als wären sie vor ihrer Beendigung offengelegt worden. Die Verpflichtungen zur Vertraulichkeit nach Ziffer 2 dieser Vereinbarung bestehen noch 5 Jahre nach Beendigung dieser Vereinbarung fort, sofern die Parteien keine abweichende schriftliche Vereinbarung treffen.	(1) This Agreement shall commence on the day it is signed by both Parties and remain in effect for 36 months. Any Confidential Information disclosed by either of the Parties to the other as regards the Purpose (as defined in the Preamble) after termination of this Agreement shall nevertheless be governed by its provisions as if it had been disclosed before termination. The confidentiality obligations pursuant to Section 2 of this Agreement shall survive for 5 years after the expiration of this Agreement unless the Parties agree otherwise in writing.
(2) Auf Verlangen des Informationsgebers hat der Empfänger unverzüglich alle oder Teile der Vertraulichen Informationen in jedweder Verkörperung, mit allen Kopien, Auszügen sowie daraus abgeleiteten Werken, dem Informationsgeber nach dessen Weisung zurückzugeben, zu vernichten und/oder endgültig aus seinen elektronischen und sonstigen Speichersystemen (einschließlich Clouds) zu löschen und dem Informationsgeber die Vernichtung oder Löschung unter Angabe von Ort, Zeit und Art und Weise der Vernichtung oder Löschung schriftlich zu bestätigen. Im Falle der Rückgabe Vertraulicher Informationen hat er schriftlich zu versichern, dass alle erhaltenen Vertraulichen Informationen einschließlich sämtlicher von ihm – auch auszugsweise – gefertigten Kopien vollständig zurückgegeben worden sind. Vertrauliche Informationen, die personenbezogene Daten enthalten, sind gemäß den Bestimmungen der EU-Datenschutzgrundverordnung auch ohne besondere Aufforderung des Informationsgebers	(2) Upon the Discloser's request, the Recipient shall promptly return or, at the Discloser's instruction, destroy and/or permanently erase or delete from its electronic and other information storage systems (including clouds), any and all Confidential Information and any and all copies, extracts and derivative works thereof, and shall certify in writing to the Discloser such destruction and/or permanent erasure or deletion and the details (place, time, method) thereof. In case of the return of Confidential Information, the Recipient shall confirm in writing that all Confidential Information received as well as all copies thereof (including fragments) have been returned in full. Confidential Information containing personal data shall, without the necessity of a request made by the Disclosing Party, be erased in accordance with the provisions of the EU General Data Protection Regulation once the purpose for storing them has lapsed.

zu löschen, sobald der Zweck für ihre Speicherung entfallen ist.	
9. Beschäftigungsverbot	**9. Non-Employment**
Keine Partei darf Mitarbeiter der anderen Vertragspartei während der Dauer dieser Vereinbarung oder in den nachfolgenden 24 Monaten einstellen oder in irgendeiner Weise, zB freiberuflich, beschäftigen, es sei denn, die andere Partei stimmt dem schriftlich zu. Einer Beschäftigung stehen andere Angebote und Vereinbarungen gleich, aufgrund derer die Arbeitskraft eines Mitarbeiters nicht mehr dem bislang anstellenden Unternehmen zugutekommt, sondern ganz oder teilweise der anderen Partei. Die Bestimmungen dieser Ziff. 9 verpflichten auch verbundene Unternehmen der Parteien und schützen auch im Sinne eines Vertrages zugunsten Dritter verbundene Unternehmen der anderen Partei in Bezug auf deren Mitarbeiter; die Parteien stehen insofern für die Handlungen der mit ihnen jeweils verbundenen Unternehmen ein.	During the term of this Agreement and for a period of twenty-four (24) months thereafter, neither Party shall employ or retain as an independent contractor any person who is an employee of the other Party, except with the other Party's written approval. Other offers and agreements, under which the work activities of an employee no longer benefit the employee's current employer, but are wholly or partly for the benefit of the other Party, shall also deemed employment within the meaning of this Section 9, the provisions of which shall also obligate affiliated companies of each Party and protect affiliated companies of the other Party with regard to their employees in the sense of a third party beneficiary; the Parties shall thus also be responsible for the actions of their respective affiliates.
10. Geltendes Recht und Gerichtsstand	**10. Governing Law and Jurisdiction**
Diese Vereinbarung unterliegt deutschem Recht unter Ausschluss des internationalen Privatrechts. Soweit dies zwischen den Parteien dieser Vereinbarung wirksam vereinbart werden kann, ist ausschließlicher Gerichtsstand für Streitigkeiten aus oder im Zusammenhang mit dieser Vereinbarung [Ort], Deutschland. Sollte der Informationsgeber gemäß Ziff. 7.1 (a) dieser Vereinbarung das Recht haben, einstweiligen Rechtsschutz zu beantragen, so kann er den entsprechenden Antrag bei jedem in der Sache oder für den Sitz des Empfängers zuständigen Gericht stellen.	This Agreement shall be governed by German law excluding its private international law provisions. [Place], Germany shall be the exclusive place of jurisdiction for all disputes arising from or in connection with this Agreement to the extent the Parties are legally able to agree on such a provision. In case Discloser is entitled to obtain injunctive relief as stipulated in Section 7.1 (a) hereof, he shall be entitled to apply for such injunctive relief before any court having jurisdiction over the Recipient or the subject matter hereof.
11. Sonstige Bestimmungen	**11. Miscellaneous**
(1) Keine der Parteien ist berechtigt, Rechte oder Verpflichtungen aus diesem Vertrag ohne vorherige schriftliche Zustimmung der anderen Partei auf Dritte zu übertragen.	(1) Neither Party shall assign any rights or delegate any obligations to third parties under this Agreement without the prior written consent of the other Party.
(2) Diese Vereinbarung ersetzt alle früheren zwischen den Parteien getroffenen Abreden zur Vertraulichkeit und ist zwischen den Parteien	(2) This Agreement supersedes all prior agreements between the Parties regarding the matter of confidentiality and governs all

hinsichtlich der Behandlung Vertraulicher Informationen abschließend.	confidentiality issues between the Parties conclusively.
(3) Diese Vereinbarung ist in deutscher und in englischer Sprache verfasst; im Falle von Unterschieden ist die [deutsche] Fassung maßgeblich. Da es sich hierbei um eine gegenseitige Geheimhaltungsvereinbarung handelt, gehen Zweifel bei der Auslegung nicht zu Lasten der Partei, die diese Vereinbarung vorgelegt oder entworfen hat.	(3) This Agreement is written in the German and in the English language. In case of any discrepancies, the [German] version shall prevail. This is a mutual non-disclosure agreement and any doubt arising as to its interpretation shall not be construed against the Party which presented or drafted it.
(4) Innerhalb dieser Vereinbarung enthält ein Verweis auf den Singular gleichzeitig einen Verweis auf den Plural und umgekehrt, wenn dies der Kontext erfordert.	(4) In this Agreement, a reference to the singular includes a reference to the plural and vice versa where required by the context.
(5) Die Überschriften dienen dem Zwecke der Orientierung und sind nicht zur Auslegung der jeweiligen Vorschrift, eines Abschnitts, einer Bestimmung oder dieser Vereinbarung heranzuziehen. Sofern es der Zusammenhang nicht zwingend anders erfordert, beziehen sich die Worte „hierin“, „hierunter“, „hier“ und Wörter ähnlicher Bedeutung auf diese Vereinbarung in ihrer Gesamtheit und nicht auf eine bestimmte Vorschrift, einen Abschnitt oder eine Regelung dieser Vereinbarung.	(5) The headings are for ease of reference and shall not affect the interpretation of the particular article, section, provision or this Agreement. Unless the context otherwise requires, the words “hereof,” “hereunder,” “herein” and words of similar meaning refer to this Agreement in its entirety, and not to any particular article, section or provision of this Agreement.
(6) Änderungen und Ergänzungen dieser Vereinbarung sowie jede unter Geltung dieser Vereinbarung abzugebende Erklärung bedürfen zu ihrer Wirksamkeit der Schriftform. Dies gilt auch für eine Abweichung von diesem Schriftformerfordernis sowie seine Abänderung.	(6) Changes and amendments to this Agreement as well as every notice given under this agreement must be in writing to be valid. This shall also apply to any variance or waiver of this written form requirement.
(7) Für den Fall, dass einzelne oder mehrere Bestimmungen dieser Vereinbarung unwirksam oder undurchführbar sind oder werden, wird dadurch die Wirksamkeit der übrigen Bestimmungen dieser Vereinbarung wie auch der Vereinbarung als solcher nicht berührt. Die unwirksame oder undurchführbare Bestimmung gilt als durch eine solche wirksame und durchführbare Bestimmung ersetzt, die den von den Parteien rechtlich und wirtschaftlich mit der unwirksamen bzw. undurchführbaren Klausel verfolgten Zielen am nächsten kommt.	(7) Where one or more provisions of this Agreement are or should become invalid or impracticable, the validity and effectiveness of the remaining provisions and this Agreement as such shall thereby not be affected. The invalid or impracticable provision shall be replaced by such valid and effective provision which from a legal and commercial point of view most closely approximates to that which the Parties intended to achieve when they agreed the invalid and/or impracticable provision.

（参考和訳）取引先との秘密保持契約書の例

取引相手との秘密保持義務条項

前文

当事者は、事業関係の締結可能性を評価し、必要に応じて当該関係の準備及び実施を行う目的のために、相互に、情報、文書、図面その他の資料、特にデータを開示する意図を有する。これらの資料には、開示当事者の機密情報及び／又はノウハウが含まれる場合がある。

この前提に基づき、当事者は、以下の規定に従い、相手方の「機密情報」（下記の定義による）を相互に秘密として保持する義務を負うものとする。

1. 定義及び解釈

(1) 本契約における**機密情報**とは、財務、技術、経済、法律、税務その他の一切の情報であり、その形態又は媒体を問わず、ドラフト、写真、技術図面、（製品）説明書、マニュアル、ソフトウェア、プログラム、指示書、技術的・科学的・経済的ノウハウ、運用手順、方法、評価結果、事業計画、技術計画、提案書、その他のデータを含む情報をいう。これらの情報は、開示当事者（以下「**開示者**」という）が受領当事者（以下「受領者」という）に対し、口頭、書面、電子手段その他いかなる方法によって開示した情報、又は受領者がその他の方法により知り得た情報であって、機密として表示されているもの、又はその機密性がその他の事情に照らして明らかであるものを含むものとし、これらは、当該情報がドイツ営業秘密保護法（GeschGehG）第 2 条第 1 号に定める営業秘密に該当するか否かを問わない。

本契約における機密情報には、当該情報の体現物、複製物、その他の再製物又はその一部も含まれるものとする。

さらに、本契約における機密情報には、受領者に対して機密情報が開示されたという事実、並びに本契約の存在及び内容も含まれるものとする。

(2) 第 1.1 条に定める機密情報には、特に、開示者の技術に関する情報を含む資料、又は当該技術、財務、事業関係、マーケティング、研究開発に関する情報を含む資料が含まれるものとする。これは、開示者の技術に関する計画及び予測についても同様とする。

(3) 本契約に定義する機密情報には、当事者のいずれかが本契約締結前に相手方に開示した情報も含まれるものとする。

(4) 開示者は、第三者の営業秘密を含む情報について、当該第三者から書面により明示的な承認を得た場合に限り、受領者がアクセスできるようにするものとする。

2. 秘密保持義務及び使用制限

以下の第 3 条の規定に従い、受領者は、開示者から開示された機密情報を受領した場合又は第 3.4 条の例外が適用されない場合において、受領者が第三者から受領した情報が明らかに開示者に由来する機密情報である場合には、以下の義務を負うものとする。

(1) 受領者は、機密情報を厳重に秘密として保持し、当事者が開示を通じて達成しようとしている目的のためにのみ機密情報を利用し、当該機密情報を、自らの同種の機密情報を保護する際と同等の注意をもって保護するものとする。ただし、その注意水準は通常の業務の過程において要求される相当の注意義務を下回らないものとする。

機密情報に GDPR において規定される個人データが含まれる場合、受領者は当該データを、当該データ保護規則の規定及び要件を完全に遵守して取り扱い、保管するものとする。

(2) 受領者は、かかる機密情報又は当該機密情報を含む一切の情報を、以下の要件を全て満たす受領者の役員、従業員及びコンサルタントを除き、第三者に開示、公表又は提供してはならない。

(a) 当事者が開示を通じて達成しようとしている目的のために当該機密情報を知る必要があること

(b) 当該機密情報が本契約に定める秘密保持義務の対象である旨を認識していること

(c) 本契約における秘密保持義務と同等以上の厳格な秘密保持義務を含む雇用契約又はその他の契約を受領者と締結していること

なお、受領者は、上記第(2)項に該当しない下請業者、供給業者、代理人その他の外部の第三者に対する機密情報の開示は、受領者が事前に書面により承諾を得た場合に限り、許可されるものとする。

(3) 受領者は、前第(2)項に規定される個人、法人又はその他の第三者の行為又は不作為について、開示者に対して責任を負うものとする。

(4) 受領者は、当事者が開示を通じて達成しようとしている目的において合理的に必要な場合を除き、機密情報を複製し、リバースエンジニアリングし、又は書面に書き起こしてはならない。合理的に必要な範囲で作成された複製物又は書面化された情報は、その全て（そこに含まれる知的財産権を含む）が開示者の所有に属するものとする。

(5) 受領者は、役員、従業員及び／又はコンサルタントによる本契約違反を認識した場合、直ちにその旨を開示者に通知し、現在生じている違反の悪影響を回避するために必要なあらゆる措置を講ずるとともに、将来の違反を防止するために必要な措置を講じなければならない。

3. 例外

本契約における「機密情報」には、以下の情報は含まれないものとする。

(1) 受領者が開示者から当該情報を受領する以前に、正当に保有しており、かつ秘密保持義務の対象となっていなかった情報。

(2) 受領者が当該情報を提供された時点で既に公知であった情報、又は受領者の責めに帰することなく公知となった情報。

(3) 開示者が第三者に対し、秘密保持義務を課すことなく開示した情報。

(4) 第三者が正当に取得し、かつ当該第三者が法的に拘束される秘密保持義務に違反することなく開示したものであって、受領者が本契約締結前又は締結後に第三者から受領した情報。

(5) 受領者が開示者の機密情報を一切使用せず、又は参照することなく独自に開発した情報。

(6) 受領者が開示者の事前の書面による承諾を得て開示した情報。

なお、ドイツ営業秘密保護法（GeschGehG）第 5 条の規定は影響を受けないものとする。

4. 許容される開示

受領者は、開示者の事前の書面による承諾を得た場合、裁判所その他の行政機関による有効な命令への対応として開示が必要な場合、又は法令により開示が要求される場合には、開示者の機密情報又はその一部を開示することができるものとする。

ただし、法令により禁止されていない限り、受領者は、当該命令又は開示義務の法的根拠及び対象となる機密情報について、開示の相当期間前に書面にて開示者に通知しなければならない。また、開示者の要請があるときは、当該裁判所又は行政機関の命令に対し、合理的な範囲で異議申立て又は不服申立てを行うための努力を尽くさなければならない。

5. 機密情報に関する所有権及び権利

開示者は、その機密情報に関する一切の知的財産権（特許権、著作権、商標権を含むがこれらに限られない）を、常に有するものとする。本契約に基づき、いずれの当事者も相手方の知的財産権を取得することはないものとする。

本契約により付与される権利は、当該機密情報を本契約により許容される範囲で使用する限定的な権利に限られ、それ以外の機密情報に関するいかなる権利又はライセンスも、明示的にも黙示的にも付与されるものではない。。

6. 保証の否認及び第三者営業秘密に関する開示者の責任

(1) 受領者は、機密情報を「現状のまま」受領するものとし、書面で別途定めがない限り、開示者は、当該機密情報に関して、特にその正確性又は完全性について、いかなる表明又は保証も行わないものとする。

(2) 本契約のいかなる規定、又は本契約に基づく機密情報の開示も、以下のいずれを意味し、又は構成するものと解釈してはならない。

a) 製品又はサービスの開発・提供可能性に関するいかなる表明又は約束を意味し、又はこれを暗示するもの

b) 本契約を超える契約関係、特に製品の供給又はサービスの提供に関する契約関係を締結する義務を構成するもの

c) 受領者が、本契約に基づき提供された開示者の機密情報を用いることなく、ここに関連するものと競合する製品又はサービスを独自に開発することを妨げるもの

d) いずれの当事者が、他方当事者の競合企業と、本契約の目的と実質的に類似する目的で協力することを妨げるもの

(3) 開示者は、第三者の営業秘密である旨を明示している場合を除き、当該第三者の同意なく第三者の営業秘密を受領者に提供することはなく、またこれまでに提供していないことを保証する。

7. 救済、補償、違約金

(1) 各当事者は、本契約に定める義務が開示者及びその事業を保護するために必要かつ合理的なものであることを認識する。さらに、各当事者は、機密情報が有する独自性に鑑み、他方当事者による本契約上の義務違反について、金銭賠償のみでは開示者に対する補償として不十分となる可能性があることを明示的に認識する。

したがって、各当事者は、当該違反又は違反のおそれが、開示者に回復困難な損害を生じさせることを認識するとともに、適用される法令に基づき利用可能なその他の救済に加えて、開示者が以下の救済を受ける権利を有することに同意し、これを確認する。

a) 実際の損害又は差し迫った損害を立証する必要なく、本契約の違反又はその継続に対する差止命令を取得する権利

b) 受領者による本契約違反又当該義務の履行確保に関連して生ずる損失又は損害、、並びに、受領者による開示者の機密情報の無断使用又は無断開示、若しくは、開示者の作為又は不作為により機密情報にアクセスした第三者による無断使用又は無断開示に起因し、又はこれに関連して生ずる損失若しくは損害について、（弁護士費用その他の法的費用を含む）受領者から補償を受ける権利

なお、本契約に基づくアクセスの許否を問わず、第三者の行為に対する開示者の直接請求権又は法的措置を排除又は制限するものとして解釈してはならない。

(2) 受領者により、又は受領者に帰責される義務違反が生じた場合、その都度、開示者は、受領者に対して違約金の支払いを請求する権利を有するものとし、当該違約金の額は、受領者が裁判所に対しその相当性の判断を求める権利を妨げないものとして、開示者が衡平の原則に従い決定するものとする。継続犯の抗弁は排除されるものとする。

支払われるべき違約金は、開示者が被った損害から控除されるものとするが、常に最低限の補償額として取り扱われるものとする。

(3) 開示者は、自己の損害賠償請求権を害することなく、第三者の営業秘密について、開示者が無権限に、又は第三者の同意なく受領者に開示したことに起因して受領者に対して第三者から主張される一切の請求、要求、責任（合理的な法的防御費用を

含む）、並びに受領者に科される一切の罰金・制裁金について、受領者を補償するものとする。

ただし、受領者が、開示者に当該第三者の権限がないことを認識していた場合には、この補償義務は生じないものとする。

8. 契約期間及び終了

(1) 本契約は、両当事者が署名した日に効力を生じ、36 か月間有効に存続するものとする。

いずれの当事者が、本契約終了後に、前文において定義する目的に関連して機密情報を開示した場合であっても、、当該機密情報は、契約終了前に開示されたものであるものとして本契約の規定が適用されるものとする。

第 2 条に基づく秘密保持義務は、当事者間で書面により別途合意がなされない限り、本契約終了後 5 年間存続するものとする。

(2) 受領者は、開示者から請求があった場合には、遅滞なくに、開示者の指示に従い、機密情報及びその一切の複製物、抜粋及び派生物を返還・破棄するとともに、必要に応じて電子媒体その他の情報保存システム（クラウドを含む）から恒久的に消去・削除するものとする。

さらに、受領者は、当該破棄及び／又は恒久的消去・削除を実施した旨、その詳細（場所、日時、方法）を、開示者に書面で証明しなければならない。

機密情報を返還する場合には、受領者は、受領した一切の機密情報及びその複製物（断片を含む）が完全に返還されたことを、書面により確認するものとする。

個人データを含む機密情報については、開示者からの要請を要することなく、当該データの保存目的が失われた時点で、GDPR の規定に従い消去しなければならない。

9. 就労禁止

本契約期間中及びその終了後 24 か月間、いずれの当事者も、相手方当事者の従業員を、相手方の書面による承諾なしに、雇用し、又は独立した請負人として業務委託してはならないものとする。

また、従業員の業務活動が現在の雇用主の利益とならず、全部又は一部が他方当事者の利益のために行われることとなる申込みその他の合意は、第 9 条の趣旨に照らし、雇用とみなされるものとする。

本条の規定は、各当事者の関連会社にも義務として適用され、他方当事者の関連会社を、その従業員に関し、第三者受益者の立場で保護するものとする。したがって、当事者は、自らの関連会社の行為についても責任を負うものとする。

10. 準拠法及び裁判管轄

本契約は、その国際私法規定を除き、ドイツ法を準拠法とする。

本契約から生じ、又はこれに関連する一切の紛争については、当事者がそのような合意を行うことが法的に可能な範囲において、ドイツ国［地名］を専属的合意管轄裁判所とするものとする。

なお、開示者が第 7.1 条(a)に定める差止命令を請求する権利を有する場合には、開示者は、受領者又は本件の対象に対して管轄権を有するいずれの裁判所に対しても、当該差止命令を申し立てることができるものとする。

11. 雑則

(1) 当事者は、他方当事者の事前の書面による承諾がない限り、本契約に基づくいかなる権利も第三者に譲渡し、又はいかなる義務を第三者に委任してはならないものとする。

(2) 本契約は、当事者間の秘密保持に関する従前の一切の合意に優先し、両当事者間の秘密保持に関する事項を最終的かつ包括的に規律するものとする。

(3) 本契約は、ドイツ語版及び英語版で作成されるものとする。両者の間に相違が生じた場合には、［ドイツ語］版を優先するものとする。本契約は両当事者間の秘密保持契約であり、その解釈について疑義が生じた場合であっても、本契約を提示し又は作成した当事者に不利益に解釈されるものではない。

(4) 文脈上必要とされる場合には、本契約において、単数形への言及は複数形を含み、複数形への言及は単数形を含むものとする。

(5) 見出しは便宜的なものであり、各条、各項その他の規定又は本契約の解釈に影響を及ぼすものではない。文脈上別段の定めがない限り、「hereof」「hereunder」「herein」その他これに類する語は、本契約全体を指し、特定の条、項又は規定を指すものではありません。

(6) 本契約の変更及び修正、並びに本契約に基づく一切の通知は、書面によって行われる場合に限り有効とする。この書面形式要件の改変又は放棄についても同様に書面によらなければならない。

(7) 本契約のいずれかの規定が無効となる若しくはなるべき場合、又は履行不能となる若しくなるべき場合であっても、本契約のその他の規定の有効性及び効力は、何ら影響を受けないものとする。無効又は履行不能となった規定は、当事者が当該規定により達成しようとした法的及び商業的目的に最も近い、有効かつ履行可能な規定に置き換えられるものとする。

5　来訪者受付表

Annex 5–Visitor list for a business site

Visitor Name	Visitor Address	Host	Time of Arrival	Time of Departure	Visitor Information Approved by:

*) Information regarding previous visitors should not be visible to subsequent visitors, e.g. by covering the respective parts of the table or using a digital system for registration.

* * *

（参考和訳）来訪者受付表

事業所の訪問客リスト

訪問客名	訪問客住所	ホスト	到着時刻	出発時刻	訪問客情報 許可者

※ 以前の来訪者に関する情報が、後の来訪者から見えることがないようにしなければならない。例えば、該当箇所を覆う、又はデジタルの登録システムを使用するなどの方法が考えられる。

英国

1　従業員ハンドブックにおける秘密保護関連規定の例

Staff handbook

1. Introduction

1.1 [GENERAL DETAILS ABOUT THE EMPLOYER AND ITS BUSINESS.]

1.2 We are an equal opportunities employer and do not discriminate on the grounds of gender, sexual orientation, marital or civil partnership status, pregnancy or maternity, gender reassignment, race, color, nationality, ethnic or national origin, religion or belief, disability or age.

2. Using the Staff Handbook

2.1 This Staff Handbook sets out the main policies and procedures that you will need to be aware of while working with us. You should familiarize yourself with its contents and comply with them at all times. Any questions regarding its provisions or how to comply should be directed to the Human Resources Department.

2.2 The policies and procedures set out in this handbook apply to all employees unless otherwise stated. This includes managers, officers, directors, employees, consultants, contractors, trainees, homeworkers, part-time and fixed-term employees, casual and agency staff and volunteers (collectively referred to as “staff” in this handbook). These policies do not form part of your contract with us, which is provided separately.

3. Responsibility for the Staff Handbook

3.1 The Human Resources Manager holds overall responsibility for this Staff Handbook and for ensuring that its policies and procedures comply with our legal obligations.

3.2 The Staff Handbook is reviewed regularly to ensure its provisions remain compliant with our legal obligations and reflect best practice.

3.3 All staff are expected to read and understand the contents of this handbook and act in accordance with its aims and objectives. Managers are responsible for ensuring that staff understand the standards of behavior expected of them and for taking action when those standards are not met.

4. Personal data

4.1 Whenever we process personal data about you in connection with our policies, we do so in accordance with our Data Protection Policy. We will only process your personal data where we have a lawful basis for doing so and will inform you of the purposes for which it is used. Please consult the intranet for further information.

5. Emergency contact details

5.1 The Human Resources Department is responsible for maintaining up-to-date details of your home address and the emergency contact telephone numbers of the persons you wish us to

contact in the event of an emergency, such as an accident. This information will be requested when you commence employment and you will be asked periodically to confirm its accuracy. This information is held in confidence and will only be used when needed.

Schedule 1 Dress code

Schedule 2 Expenses policy

1. About this policy

1.1 This policy outlines the procedures for claiming reimbursement of expenses, including those related to travel, accommodation and hospitality.

1.2 This policy does not form part of any employee's contract of employment and may be amended at any time.

2. Reimbursement of expenses

3. Travel expenses

4. Accommodation and other overnight expenses

5. Entertaining [clients OR customers]

Schedule 3 Equal opportunities policy

Schedule 4 Anti-harassment and bullying policy

Schedule 5 Anti-corruption and bribery policy

Schedule 6 Whistleblowing policy

1. Confidentiality

1.1 We hope that staff will feel able to raise whistleblowing concerns openly under this policy. Completely anonymous disclosures may be difficult to investigate. If you choose to raise your concern in confidence, we will make every effort to protect your identity and will only disclose it where strictly necessary to those involved in investigating the matter.

2. External disclosures

2.1 This policy is intended to provide an internal mechanism for reporting, investigating and addressing any wrongdoing in the workplace. In most cases, it should not be necessary to raise concerns externally.

2.2 However, the law acknowledges that in certain circumstances, it may be appropriate to report concerns to an external body, such as a regulator. We strongly encourage you to seek advice before doing so.

3. Protection and support for whistleblowers

3.1 We are committed to fostering a culture of openness and will support whistleblowers who raise genuine concerns under this policy, even if those concerns later prove to be mistaken.

3.2 Whistleblowers must not suffer any detrimental treatment as a result of raising a genuine concern. If you believe that you have experienced any such treatment, you should inform [the Whistleblowing Officer OR [POSITION]] immediately. [If the matter is not resolved, you may escalate it formally through our Grievance Procedure.]

3.3 Any form of threat or retaliation against whistleblowers is strictly prohibited. Individuals found to be engaging in such behavior may face disciplinary action. [In certain cases, the whistleblower may have the right to pursue a personal claim for compensation through an employment tribunal.]

3.4 However, if it is determined that a whistleblower has made false allegations that are malicious, vexatious, or frivolous, they may be subject to disciplinary action.

3.5 Protect (an independent whistleblowing charity, previously known as Public Concern at Work) operates a confidential helpline. Their contact details are at the end of this policy.

4. Contacts

Whistleblowing Officer	[NAME] [TELEPHONE] [E-MAIL]
[Managing Director [OR OTHER TRUSTED INDIVIDUAL]]	[NAME] [TELEPHONE] [E-MAIL]
Protect (Independent whistleblowing charity)	Helpline: 0203 117 2520 E-mail: Website:

Schedule 7 Holidays policy

Schedule 8 Disciplinary and capability procedures

Schedule 9 Grievance procedure

Schedule 10 Sickness absence policy

Schedule 11 Time off for antenatal appointments policy

Schedule 12 Time off for adoption appointments policy

Schedule 13 Maternity policy

Schedule 14 Adoption policy

Schedule 15 Paternity policy

Schedule 16 Shared parental leave (birth) policy

Schedule 17 Shared parental leave (adoption) policy

Schedule 18 Parental leave policy

Schedule 19 Time off for dependants policy

Schedule 20 Compassionate leave policy

Schedule 21 Parental bereavement leave policy

Schedule 22 Flexible working policy

Schedule 23 Time off for public duties policy

Schedule 24 Health and safety policy

Schedule 25 [Privacy Standard OR Data Protection Policy]

Schedule 26 IT and communications systems policy

1. About this policy

1.1 Our IT and communications systems are designed to promote effective communication and working practices. This policy sets out the standards you are expected to observe when using these systems, the circumstances under which we will monitor their use, and the actions we may take in response to any breach.

1.2 [POSITION] holds overall responsibility for this policy, including its ongoing review.

1.3 Breaches of this policy may be addressed under our Disciplinary Procedure and, in serious cases, may constitute gross misconduct, potentially resulting in summary dismissal.

1.4 This policy does not form part of any employee's contract of employment and may be amended at any time.

2. Equipment security and passwords

2.1 You are responsible for the security of any equipment allocated to or used by you, and you must not allow it to be used by others except in accordance with this policy. Passwords should be used on all IT equipment, particularly items taken outside of the office premises. Passwords must be kept confidential and changed regularly.

2.2 Equipment provided to you is to be used solely to support our business goals. You may not use it for any other purposes that do not support or augment our business.

2.3 You must only access our systems using your own username and password. You must not use another person's login credentials or allow others to use yours.

2.4 When away from your desk, you must log out or lock your computer. You must log out and shut down your device at the end of each working day.

3. Systems and data security

3.1 You must not delete, destroy, or modify existing systems, programs, information or data (unless specifically authorised to do so in the proper performance of your duties).

3.2 You must obtain permission from both your supervisor and our security manager before accessing, obtaining, retaining, transferring, copying, disclosing, communicating, or altering any technical or operational information relating to our computer systems, networks, or IT infrastructure.

3.3 You must obtain permission from your supervisor and our data security manager before transferring, copying, uploading, disclosing, communicating, or altering any information or data that you have access to in connection with your role, where such information is not intended to be shared externally or with staff who are not authorised to access such information and data by our security manager.

3.4 You must not download or install software from external sources without prior authorisation from [POSITION]. Downloading unauthorised software may interfere with our systems and may introduce viruses or other forms of malware.

3.5 You must not connect any external device or equipment including mobile phones, tablet computers or USB storage devices to our systems without prior authorisation from [POSITION].

3.6 All e-mails passing through our system are monitored for viruses. You should exercise particular caution when opening unsolicited e-mails from unknown sources. If an e-mail appears suspicious, do not reply, open any attachments or click any links.

3.7 If you suspect that your computer may be infected with a virus or malware, notify [POSITION] immediately.

3.8 Upon termination of your employment, all equipment allocated to or used by you must be returned in its original condition.

4. E-mail

4.1 Maintain a professional tone and observe appropriate etiquette when communicating with third parties via e-mail. [You should also include our standard e-mail signature and disclaimer.]

4.2 Be aware that e-mails may be used in legal proceedings and that deleted messages may still be retrievable from the system.

4.3 You must not send e-mails that are abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate.

4.4 You should not:

(a) send or forward private e-mails at work that you would not want a third party to read;

(b) send or forward chain mail, junk mail, cartoons, jokes or gossip;

(c) contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to recipients who do not need to receive them; or

(d) send messages from another person's e-mail address (unless authorised) or using an assumed name.

4.5 Do not use your own personal e-mail account for business-related communications. Only use the e-mail account we have provided to you.

4.6 [Access to web-based personal e-mail such as Gmail or Hotmail is not permitted on our computer systems at any time due to increased security risks.]

5. Using the internet

5.1 Internet access is provided solely for business-related purposes.

5.2 You must not access any website or download any image or file from the internet which could be considered illegal, offensive, inappropriate or immoral. Even content that is legal in the UK may still be deemed unacceptable under this policy. As a general rule, if the content of a webpage or file could reasonably offend someone (whether they are the intended viewer or not), or if accessing it could be a source of embarrassment if made public, then viewing it will constitute a breach of this policy.

5.3 We reserve the right to block or restrict access to certain websites at our discretion.

6. Personal use of our systems

6.1 We permit the incidental use of our internet, email and telephone systems to send personal emails, browse the internet and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not a right. It must not be overused or abused. We may withdraw permission for it at any time or restrict access at our discretion.

6.2 Personal use must meet the following conditions:

(a) use must be minimal and take place substantially out of normal working hours (that is, during lunch hours, before 9 am or after 6:00 pm);

(b) personal emails should be labelled "personal" in the subject header;

(c) use must not interfere with business or office commitments;

(d) use must not commit us to any marginal costs; and

(e) use must comply with this policy and our other policies [including [NAME OF POLICIES]].

7. Monitoring

7.1 Our systems allow us to monitor telephone, e-mail, voicemail, internet and other communications. For business purposes, and to meet our legal obligations as an employer, your use of these systems, including any personal use, may be subject to continuous monitoring through automated software or other means.

7.2 We reserve the right to retrieve email content and review internet usage (including websites visited and search history) where reasonably necessary for business purposes, including (but not limited to):

(a) monitoring that the use of the e-mail and internet systems is appropriate and in accordance with this policy;

(b) locating lost messages or retrieving messages lost due to system failure;

(c) assisting in the investigation of alleged misconduct; or

(d) complying with legal obligations.

8. Prohibited use of our systems

8.1 Misuse or excessive personal use of our telephone or e-mail systems, or inappropriate internet usage, will be addressed under our Disciplinary Procedure. In some instances, misuse of the internet may constitute a criminal offence.

8.2 The creation, viewing, access, transmission or downloading of any of the following types of material will generally be considered gross misconduct (this list is not exhaustive):

(a) pornographic material (including, written content, images, films or video clips of a sexually explicit or provocative nature);

(b) offensive, obscene, or criminal material or material that is likely to cause embarrassment to us or to our clients;

(c) false or defamatory statements about any individual or organisation;

(d) content that is discriminatory, offensive, derogatory or likely to cause embarrassment to others (including material that breaches our Equal Opportunities Policy or our Anti- harassment and Bullying Policy);

(e) confidential information about us, our staff, or clients (unless as authorised as part of your duties);

(f) unauthorised software;

(g) any statement or content which is likely to result in criminal or civil liability (for you or us); or

(h) music, video files or other material that infringe copyright.

Schedule 27 Social media policy

1. About this policy

1.1 This policy is designed to minimise the risks to our business arising from the use of social media.

1.2 This policy applies to all forms of social media, including Facebook, LinkedIn, X (formerly Twitter), Google+, Wikipedia [, Whisper] [, Instagram] [, Tumblr], and any other social networking platforms, internet postings, or blogs. It applies to both business-related use and personal use that may impact our business in any way.

1.3 This policy does not form part of any employee's contract of employment and may be amended at any time.

2. Personal use of social media

2.1 [Personal use of social media is not permitted during working hours or via our computers, networks and other IT resources and communications systems.

OR

Occasional personal use of social media during working hours is permitted provided it does not involve unprofessional or inappropriate content, does not interfere with your duties or productivity, and complies with this policy.]

3. Prohibited use

3.1 You must refrain from making any social media communications that could damage our business interests or reputation, whether directly or indirectly.

3.2 You must not use social media to defame or disparage us, our staff or any third party; to harass, bully or unlawfully discriminate; to make false or misleading statements; or to impersonate colleagues or third parties.

3.3 You must not express opinions on our behalf via social media, unless expressly authorised to do so by your manager. Authorisation may be subject to appropriate training .

3.4 You must not post comments on sensitive business matters, such as strategy, or disclose our trade secrets, confidential information or intellectual property. Our logos and trademarks must not be used in any social media post or profile.

3.5 [You are not permitted to add business contacts made during your employment to personal social networking accounts.

OR

Business contact details acquired during your employment are considered confidential. Upon termination of employment, you must provide us with a copy of all such information, delete it from your personal social networking accounts, and destroy any remaining copies.]

3.6 Any misuse of social media should be reported to [POSITION] immediately.

4. Guidelines for responsible use of social media

4.1 When posting on social media or on your personal profile, you should make it clear that you are speaking in a personal capacity. Use the first person and a personal e-mail address.

4.2 Always be respectful towards others when making statements on social media. Remember that you are personally responsible for all content you publish online, which may be visible to anyone .

4.3 If you disclose your affiliation with us in your profile or any social media postings, you must clearly state that your views are your own and do not represent those of your employer (unless you have been authorised to speak on our behalf as set out in paragraph 3.3). You should also ensure that your profile and any content you post reflect the professional image you present to clients and colleagues.

4.4 If you are unsure or concerned about the appropriateness of any statement or post, do not publish it until you have discussed it with your manager.

4.5 If you come accross social media content that is critical or reflects poorly on us, you should report it to [your manager OR [DEPARTMENT]].

5. Breach of this policy

5.1 Breach of this policy may result in disciplinary action, up to and including dismissal. [Any member of staff suspected of breaching this policy will be expected to co-operate fully with any investigation.

5.2 You may be required to remove any social media content that we consider to be in breach of this policy. Failure to comply with such a request may itself result in disciplinary action.

（参考和訳）従業員ハンドブックにおける秘密保護関連規定の例

従業員ハンドブック

1. 初めに

1.1 [雇用主及び事業に関する一般的記載]

1.2 当社は、平等に雇用機会を提供し、性別、性的指向、婚姻若しくはパートナーシップの状況、妊娠若しくは出産、性別変更、人種、肌の色、国籍、民族的若しくは国的出自、宗教若しくは信仰、障害、又は年齢を理由に、差別しない。

2. 本従業員ハンドブックの使用について

2.1 本従業員ハンドブックでは、あなたが、当社で勤務している間、把握しておくべき主要な方針や手続を定める。あなたは、この内容をよく理解し、常に遵守してください。本従業員ハンドブックの規定や遵守方法に関して疑問がある場合は、人事部にお問い合わせください。

2.2 本従業員ハンドブックに定められた方針及び手順は、別段の定めがない限り、全ての従業員に適用される。これには、管理職、役員、取締役、被雇用者、コンサルタント、契約社員、研修生、在宅勤務者、パートタイマー、有期労働者、臨時スタッフ、派遣社員、及び、ボランティアが含まれる（本従業員ハンドブックでは「スタッフ」と総称する）。本従業員ハンドブックは、別途提供される、あなたと当社との間の契約の一部を構成するものではなく、契約は別途提供される。

3. 本従業員ハンドブックについての責任

3.1 人事部長は、本従業員ハンドブック全体について責任を負うとともに、その方針及び手続が当社の法的義務に適合していることを確保する責任を負う。

3.2 本従業員ハンドブックは、その規定が、引き続き当社の法的義務への適合性を維持し、ベストプラクティスを反映するために、定期的に見直されるものとする。

3.3 全てのスタッフは、本従業員ハンドブックの内容を読んで理解し、その目的及び目標に従って行動することが期待される。管理職は、スタッフに、期待される行動基準を理解させ、かつ、当該基準が満たされない場合には対応する責任を負う。

4. 個人データ

4.1 当社が、当社の方針に関連して、あなたの個人データを処理する場合、当社の「データ保護ポリシー」に従って処理を行うものとする。当社は、正当な法的根拠がある場合に限り、あなたの個人データの処理を行い、あなたにそのデータの利用目的を通知する。詳細については、イントラネットをご参照ください。

5. 緊急連絡先の詳細

5.1 人事部は、あなたの自宅の住所、及び、あなたが事故等の緊急時に当社に連絡することを希望する人物の緊急連絡先電話番号の最新情報を管理する責任を負う。あなたは、雇用の開始時に、これらの情報の提供を求められ、その後定期的に、この情

報の正確性の確認を求められる。この情報は秘密情報として保持され、必要な場合にのみ使用される。

[中略]

Schedule 2　経費ポリシー

1. 本ポリシーについて

1.1 本ポリシーは、出張、宿泊、接待等に関連する経費の払い戻しを申請するための手続について定める。

1.2 本ポリシーは、いかなる従業員の雇用契約の一部を構成するものではなく、随時変更される可能性がある。

2. 経費の払い戻し

3. 出張費

4. 宿泊費及びその他の宿泊関連費

5. [顧客又は取引先の]接待費

[中略]

Schedule 6　内部告発ポリシー

1. 秘密保持

1.1 当社は、本ポリシーのもとで、スタッフが、率直に内部告発できることを望んでいる。完全に匿名の告発について調査することは困難である場合がある。あなたが、秘密裏に告発することを選択した場合、当社は、あなたの身元を保護するために、最大限努力し、当該問題の調査に関与する者にのみ、厳密に必要な場合に限り、あなたの身元を明らかにする。

2. 外部への告発

2.1 本ポリシーは、職場における不正行為について報告、調査及び対処するための内部メカニズムを構築することを目的とする。ほとんどの場合、外部に告発する必要はないはずである。

2.2 しかしながら、法律上は、特定の状況下において、規制当局などの外部機関に告発することが適切とされる場合がある。当社は、あなたに対し、そのような行動をとる前に、助言を求めることを強く推奨する。

3. 内部告発者の保護と支援

3.1 当社は、開放性の高い企業文化の醸成に取り組んでおり、たとえその告発が後に誤りであることが判明したとしても、本ポリシーのもとで真摯に内部告発を行った者を支援する。

3.2　内部告発者は、真摯に内部告発を行った結果として、不当な扱いを受けてはならない。もしあなたが、そのような扱いを受けたと考える場合は、直ちに[内部告発担当者又は[該当する役職の者]に]報告を行うものとする。[問題が解決されない場合は、あなたは、当社の苦情処理手続に従って正式に申立てを行うことができる。]

3.3　内部告発者に対する、いかなる形態の脅迫又は報復も、厳格に禁止される。そのような行為に関与した者は懲戒処分の対象となりうる。[一定の場合に、内部告発者は、雇用審判所を通じて、個人的に損害賠償請求を行う権利を有する可能性がある。]

3.4　しかしながら、内部告発者が、虚偽の内部告発を、悪意、嫌がらせ目的、又は軽率に行ったと判断された場合には、内部告発者は懲戒処分の対象となりうる。

3.5　Protect（旧名称を Public Concern at Work とする、独立の内部告発支援団体）は、秘密性の高い相談事業を運営している。その連絡先の詳細は、本ポリシーの末尾に記載されている。

4.　連絡先

内部告発担当者	[氏名] [電話番号] [メールアドレス]
[業務執行員 [、又はその他の信用できる個人]]	[氏名] [電話番号] [メールアドレス]
Protect （独立の内部告発支援団体）	電話番号: 0203 117 2520 メールアドレス: ウェブサイト:

[中略]

Schedule 26　IT 及び通信システムポリシー

1.　本ポリシーについて

1.1　当社の IT 及び通信システムは、効果的なコミュニケーション及び業務遂行を促進することを目的として設計されている。本ポリシーは、これらのシステムを使用する際にあなたが遵守すべき基準、当社がその使用状況を監視する場合、及び違反があった場合に当社が取りうる対応について定める。

1.2　[役職名]は、本ポリシーについて、継続的な見直しを含め、全体的な責任を負う。

1.3　本ポリシーに違反した場合、当社の懲戒手続に基づいて対処される可能性があり、違反が重大な場合には、重大な不正行為に該当し、即時解雇となる可能性がある。

1.4　本ポリシーは、いかなる従業員の雇用契約の一部を構成するものではなく、随時改訂される可能性がある。

2.　機器のセキュリティ及びパスワード

2.1　あなたは、あなたに割り当てられた、又は使用している機器のセキュリティに関して責任を負い、本ポリシーにより認められる場合を除き、他者に当該機器を使用させてはならない。全ての IT 機器には、パスワードを設定しなければならず、特に、オフィスから持ち出す機器には必要である。パスワードは、秘密として保持し、定期的に変更されなければならない。

2.2　あなたに提供された機器は、当社の業務目標を支援するためにのみ使用されるものとする。あなたは、当社の業務を支援又は強化しない目的で、機器を使用してはならない。

2.3　あなたは、あなたのユーザー名及びパスワードのみを使用して、当社のシステムにログインしなければならない。あなたは、他者のログイン情報を使用したり、他者にあなたのログイン情報を使用させたりしてはならない。

2.4　あなたが自席から離れる際には、あなたは、あなたのコンピュータからログアウトするか、これを操舵できない状態にしなければならない。あなたは、各勤務日の終業時には、あなたの機器をログアウトして、シャットダウンしなければならない。

3.　システム及びデータのセキュリティ

3.1　あなたは、既存のシステム、プログラム、情報又はデータを、削除、破棄、又は変更してはならない（あなたの職務の適切な遂行において、特別に許可されている場合を除く）。

3.2　あなたは、当社のコンピュータシステム、ネットワーク、又は IT インフラに関する技術情報又は運用情報について、アクセス、取得、保持、転送、コピー、開示、伝達、又は変更を行うに先立ち、あなたの上司及び当社のセキュリティマネージャーから許可を得なければならない。

3.3　あなたは、あなたの職務に関連してアクセスできる情報又はデータについて、当該情報を、外部者、又はデータセキュリティマネージャーにより当該情報及びデータへのアクセスが許可されていないスタッフと共有することが意図されていない場合、当該情報又はデータを転送、コピー、アップロード、開示、伝達、又は変更する前に、あなたの上司及びデータセキュリティマネージャーから許可を得なければならない。

3.4　あなたは、[役職名]の事前の許可なしに、外部ソースからソフトウェアをダウンロード、又はインストールしてはならない。許可されていないソフトウェアをダウンロードすると、当社のシステムに影響を与え、ウイルス又はその他のマルウェアを導入する可能性がある。

3.5　あなたは、携帯電話、タブレット型コンピュータ、USB 記憶装置を含む、いかなる外部機器又は装置も、[役職名]の事前の許可なしに、当社のシステムに接続してはならない。

3.6 当社のシステムを通過する全ての電子メールは、ウイルス感染をしていないか監視されている。送信元不明の未承諾の電子メールを開く際には、特に注意すること。電子メールが疑わしいと思われる場合には、返信、添付ファイルの開封、又はリンクのクリックをしてはならない。

3.7 あなたのコンピュータがウイルス又はマルウェアに感染している可能性があると疑う場合は、あなたは、直ちに[役職名]に報告すること。

3.8 あなたの雇用終了時には、あなたに割り当てられた、又はあなたが使用した、全ての機器を元の状態で返却されなければならない。

4. 電子メール

4.1 電子メールで第三者とコミュニケーションをとる際には、専門的な文体を維持し、適切なマナーを守らなければならない。[あなたは、当社の標準の電子メール署名及び免責事項も含めるものとする。]

4.2 電子メールは、法的手続で使用される可能性があること、及び削除されたメッセージであってもシステムから復元できる可能性があることを認識すること。

4.3 あなたは、侮辱的、わいせつ的、差別的、人種差別的、嫌がらせ的、侮蔑的、中傷的、ポルノ的、又はその他不適切な電子メールを送信してはならない。

4.4 あなたが以下の行為をすることは禁止される：

(a) 第三者に読まれたくない私的な電子メールを職場において送信又は転送すること

(b) チェーンメール、ジャンクメール、漫画、ジョーク、又はゴシップを、送信又は転送すること

(c) 些細なメッセージを送信したり、受信する必要のない者に不要に電子メールをコピー又は転送したりすることで、システムを混雑させること

(d) 他者の電子メールアドレスを用いてメッセージを送信すること（許可されている場合を除く）、又は偽名を使用すること

4.5 業務関連のやりとりであなたの個人用電子メールアカウントを使用してはならない。当社があなたに提供した電子メールアカウントのみを使用すること。

4.6 [当社のコンピュータシステムにおいて、Gmail や Hotmail などのウェブベースの個人用電子メールへアクセスすることは、より高いセキュリティリスクがあるため、いかなる時も許可されない。]

5. インターネットの使用

5.1 インターネットへのアクセスは、業務関連の目的のためのみに提供される。

5.2 あなたは、違法、攻撃的、不適切、又は不道徳と見なされる可能性のあるウェブサイトにアクセスしたり、インターネットから画像又はその他のファイルをダウンロードしたりしてはならない。英国において合法であるコンテンツであっても、本

ポリシーのもとでは不適切と見なされる可能性がある。原則として、ウェブページ又はファイルの内容が合理的に誰かを不快にさせうる場合（それが想定されていた閲覧者であるか否かを問わない）、又は、そのアクセスが公にされたら当人が当惑する原因となりうる場合、その閲覧は、本ポリシー違反となる。

5.3 当社は、裁量により、特定のウェブサイトへのアクセスをブロック又は制限する権利を留保する。

6. 当社システムの私的使用

6.1 当社は、以下に定める条件に従う場合に限り、当社のインターネット、電子メール及び電話システムを、私的な電子メールの送信、インターネットの閲覧、私的な電話の利用に限定的に使用することを認める。私的使用は権利ではなく特権である。過度な使用や、濫用をしてはならない。当社は、いつでも許可を撤回することができ、また、当社の裁量によりアクセスを制限することができる。

6.2 私的使用は、以下の条件を満たさなければならない。

(a) 使用は最小限であり、主として通常の勤務時間外に行われること（すなわち、昼休み、午前 9 時前又は午後 6 時以降）

(b) 私的な電子メールは、件名に「私用」と記載すること

(c) 使用が業務又はオフィスの義務に干渉しないこと

(d) 使用が当社に追加的な費用を発生させないこと

(e) 使用が本ポリシー及び当社の他のポリシー[[ポリシー名]を含む。]に従っていること

7. 監視

7.1 当社は、当社のシステムにより、電話、電子メール、ボイスメール、インターネット、及びその他の通信を監視することができる。業務上の目的及び雇用主としての法的義務を果たすために、あなたによるこれらのシステムの利用（個人的な利用を含む）状況は、自動化されたソフトウェア又はその他の方法により、継続的に監視される可能性がある。

7.2 当社は、業務上の目的のために合理的に必要な場合、電子メールの内容を取得したり、インターネットの利用状況（アクセスしたウェブサイト及び検索履歴を含む）を確認したりする権利を留保する。これには以下の目的が含まれるが、以下に限定されない。

(a) 電子メールシステム及びインターネットの利用が適切であり、本ポリシーに準拠しているかどうかを監視する目的

(b) 失われたメッセージを検索する目的、又はシステム障害のために失われたメッセージを復旧させる目的

(c) 告発された不正行為の調査を支援する目的

(d) 法的義務を遵守する目的

8. 当社システムの使用禁止事項

8.1 当社の電話又は電子メールシステムの不正使用、過度の私的使用、又は不適切なインターネット利用は、当社の懲戒手続に基づいて対処される。インターネットの不正利用は、場合によっては、犯罪行為に該当する可能性がある。

8.2 以下の種類の資料の作成、閲覧、アクセス、送信、又はダウンロードは、原則として重大な不正行為とみなされる（以下の行為に限られない）。

(a) ポルノ素材（性的に露骨又は興奮を生じさせる性質の文書、画像、映画、又はビデオクリップを含む）

(b) 攻撃的、わいせつ的、犯罪的な資料、又は、当社又は顧客を当惑させる可能性のある資料

(c) 個人又は組織に関する、虚偽又は名誉毀損的な記述

(d) 差別的、攻撃的、侮蔑的、又は他者を不快にさせる可能性のあるコンテンツ（当社の機会均等ポリシー又はハラスメント及びいじめ防止に関するポリシーに違反するコンテンツを含む）

(e) 当社、従業員又は顧客に関する秘密情報（あなたの職務の一環として許可された場合を除く）

(f) 許可されていないソフトウェア

(g) （あなた又は当社に）刑事又は民事責任を生じさせる可能性のある記述又は内容

(h) 著作権を侵害する音楽、ビデオファイル、又はその他の資料

Schedule 27 ソーシャルメディアポリシー

1. 本ポリシーについて

1.1 本ポリシーは、ソーシャルメディアの利用による当社の事業に対するリスクを最小限に抑えることを目的とする。

1.2 本ポリシーは、Facebook、LinkedIn、X（旧 Twitter）、Google+、Wikipedia [、Whisper] [、Instagram] [、Tumblr]、その他のソーシャルネットワーキングプラットフォーム、インターネット上の投稿、ブログを含む、あらゆる形態のソーシャルメディアに適用される。業務に関連する利用だけでなく、当社の事業に何らかの影響を及ぼす可能性のある私的利用にも、適用される。

1.3 本ポリシーは、従業員の雇用契約の一部を構成するものではなく、随時改訂される可能性がある。

2. ソーシャルメディアの私的利用

2.1 [勤務時間中、又は、当社のコンピュータ、ネットワーク、その他の IT リソース、若しくは通信システムを使用して行うソーシャルメディアの私的利用は、禁止される。

又は

勤務時間中にソーシャルメディアを時折、私的利用することは、それが非専門的又は不適切な内容を含まず、あなたの業務又は生産性を妨げず、本ポリシーに従っている限りで、許可される。]

3. 禁止される使用

3.1 あなたは、当社の事業上の利益又は評判を、直接的又は間接的に損なう可能性のある、ソーシャルメディア上の発信は行ってはならない。

3.2 あなたは、ソーシャルメディアを、当社、当社のスタッフ若しくは第三者を名誉毀損・誹謗中傷する目的、嫌がらせ・いじめ・不法な差別をする目的、虚偽若しくは誤解を招く発言をする目的、又は同僚若しくは第三者になりすます目的で、使用してはならない。

3.3 あなたは、あなたの上司から明示的に許可されていない限り、ソーシャルメディア上で当社を代表して意見を表明してはならない。許可は、適切な研修の受講を条件とする場合がある。

3.4 あなたは、戦略などの慎重な扱いを要する業務事項に関するコメントを投稿したり、当社の営業秘密、秘密情報又は知的財産を開示したりしてはならない。当社のロゴや商標は、ソーシャルメディアの投稿又はプロフィールに、使用されてはならない。

3.5 [あなたは、あなたの雇用期間中に得た業務上の連絡先を、個人のソーシャルネットワークアカウントに追加することは、許されていない。

又は

あなたの雇用期間中に取得した業務上の連絡先は当社の秘密情報とみなされる。雇用終了時に、あなたは、当該情報の全てのコピーを当社に提出し、あなたの個人的なソーシャルネットワークアカウントから削除し、残っているコピーも全て破棄しなければならない。]

3.6 ソーシャルメディアの不適切な使用は、[役職名]に直ちに報告しなければならない。

4. ソーシャルメディアの責任ある利用のためのガイドライン

4.1 ソーシャルメディア又はあなたの個人のプロフィールに投稿する際は、あなたは、あなたが個人の立場で発信していることを明確にしなければならない。一人称を使用し、個人のメールアドレスを使用すること。

4.2 ソーシャルメディアで発言するときは、常に他者に敬意を払うこと。あなたがオンライン上に公開する全ての内容は、誰にでも見られる可能性があり、あなたが個人的に責任を負うことを忘れないこと。

4.3 あなたは、プロフィール又はソーシャルメディアの投稿において、あなたが当社との関係を開示する場合は、あなたの見解が、あなたの個人的なものであり、あなたの雇用主の見解を代表するものでないことを明確に記載しなければならない（第3.3 項に定めるとおり、あなたが当社を代表して投稿することについて許可されている場合を除く）。また、あなたは、あなたのプロフィール及び投稿内容が、あなたが顧客や同僚に提示する、職業上のイメージと一致しているよう留意しなければならない。

4.4 あなたは、発言又は投稿の適切性について、確信が持てない、又は懸念がある場合は、あなたがあなたの上司と協議を終えるまで公開してはならない。

4.5 あなたが、当社を批判したり、当社に悪影響を及ぼす可能性のあるソーシャルメディアコンテンツを見つけたり場合は、あなたは、[あなたの上司又は[部門名]]に報告すること。

5. 本ポリシー違反

5.1 本ポリシーに対する違反は、解雇を含む懲戒処分の対象となりうる。[本ポリシーに違反した疑いのあるスタッフは、当社の調査に全面的に協力することが求められる。]

5.2 あなたは、当社が本ポリシーに違反すると判断したソーシャルメディア上のコンテンツは、削除を求められる場合がある。当該要求へ従わない場合、それ自体が懲戒処分の対象になる可能性がある。

2　従業員との秘密保持契約書の例
Confidentiality Clauses in Employment Agreement

1. Confidential Information

1.1 Confidential Information means all confidential information relating to Employer [and its Group Company] that Employee becomes aware of, during, or in connection with, the performance of their duties owed to Employer [or its Group Company][, whether before, on, or after the date of this agreement]. This includes:

(a) all confidential or proprietary information relating to:

(i) research and development plans, business operations, employment matters, marketing and advertising, financial data, documents submitted to or received from regulatory authorities and business partners, and information concerning past, present, or prospective customers and clients, relationship with customers and business affiliates [, OR or] future plans and prospects[, intentions, or market opportunities] of Employer [or of the Employer's Group Company] that are not publicly known or readily ascertainable by someone operating in the same or similar business sector; and

(ii) operations, processes, product information, know-how, technical data, designs, trade secrets, or software belonging to Employer[, or of Employer's Group Company] that are designated as proprietary by Employer or its Representatives or its Group Company;

(b) any information, findings, data or analysis derived from the Confidential Information; [and]

(c) any other information identified by Employer, its Representatives [or its Group Company, or their Representatives] as confidential or proprietary in nature[; and OR .]

(d) [any information detailed in Exhibit A] but excluding any information referred to in clause 1.2.

1.2 Information shall not be considered Confidential Information if:

(a) it is, or becomes, publicly available other than as a direct or indirect result of disclosure by Employee or its Representatives in breach of this agreement [(except that any compilation of publicly available information in a non-public format shall still be treated as Confidential Information)];

(b) it was available to Employee on a non-confidential basis prior to disclosure by Employer;

(c) it was, is, or becomes available to Employee on a non-confidential basis from a third party who, to Employee's knowledge, is not subject to any confidentiality obligation in respect of that information;

(d) it was lawfully in the Employee’s possession prior to disclosure by Employer; [or]

(e) [it is developed by or for Employee independently of the information disclosed by Employer; or]

(f) the parties agree in writing that the information is not confidential.

2. Confidentiality Obligations

2.1 During the term of this agreement and for a period of [number] years following its termination, Employee shall:

(a) keep all Confidential Information strictly secret and confidential;

(b) use the Confidential Information solely in the course of performing duties owed to Employer;

(c) ensure that Confidential Information is clearly labelled and classified as confidential, in a manner that allows anyone who is exposed to it to recognize and uphold its confidential nature at all times;

(d) protect the Confidential Information with appropriate care to prevent unauthorised access or misuse;

(e) implement the security measures set out in Exhibit B;

(f) not, whether directly or indirectly, disclose, make available, or attempt to disclose or make available, any Confidential Information, in whole or in part, to any person, except where expressly permitted, and strictly necessary for the performance of Employee's duties under this agreement;

(g) not copy, transcribe, or otherwise record the Confidential Information except where strictly necessary for the performance of Employee's duties. Any such copies, transcriptions, or records shall remain the property of Employer;

(h) not present, disclose, or otherwise, whether expressly or implicitly, communicate any information relating to Employer's products and services, or Employee's work in lectures or publications without prior written authorisation from Employer;

(i) immediately notify Employer of (1) any suspected actual or imminent breach of confidentiality by Employee, (2) any actual or imminent disclosure, security breach, misuse, misappropriation, or other unauthorised use by any person including where such events occur in the context of Permitted Disclosure and Mandatory Disclosure;

(j) not seek or attempt to obtain intellectual property rights over any Confidential Information; or

(k) [INCLUDE ANY OTHER SPECIFIC REQUIREMENTS.]

3. Permitted Disclosure

3.1 Employee may disclose Confidential Information to its Representatives, provided that it:

(a) informs Employer's business affiliates, employees, and customers, of the confidential nature of the Confidential Information prior to disclosure; and

(b) procures that such persons or entities comply with the confidentiality obligations in clause 2.1

4. Mandatory Disclosure

4.1 Subject to the provisions of this clause, Employee may disclose Confidential Information only to the minimum extent required by:

(a) an order of any court, regulatory, judicial, governmental or similar body, or any taxation authority, in each case of competent jurisdiction;

(b) applicable laws or regulations of any jurisdiction to which Employer [or its Group Company] is subject.

4.2 Before making any disclosure under clause 4.1, Employee shall, to the extent permitted by applicable law, use all reasonable endeavors to provide Employer with as much advance notice of the intended disclosure as possible.

5. Return or destruction of the Confidential Information

5.1 (1) Upon the completion or termination of employment, or (2) upon Employer's written request at any time, Employee shall:

(a) destroy [or return to Employer] all documents, data, and materials [including any copies] that contain, reflect, incorporate or are based on Employer's Confidential Information;

(b) destroy [or return to Employer] all documents, devices, data, and materials [including any copies] which relate to Employer or its Group Company, including notes, reports, memoranda, records, files, drawings, protocols, and similar documents;

(c) certify in writing to Employer that items listed in clause 5.1 are the sole property of Employer and its Group Company and that Employee has complied fully with the requirements of this clause 5.1.

6. No warranty and no representation

6.1 The disclosure of Confidential Information by Employer shall not constitute an offer, or representation or warranty by Employer to enter into any further agreement with Employee.

6.2 Except as expressly stated in this agreement, Employer makes no express or implied warranty or representation regarding its Confidential Information, including, without limitation, its accuracy or completeness.

7. Rights and remedies

7.1 Except as expressly provided in this agreement, the rights and remedies set out in this agreement are in addition to, and not exclusive of, any rights or remedies available at law.

7.2 [Without prejudice to any other rights or remedies available to either party, each party acknowledges and agrees that damages alone may not be an adequate remedy for any breach of this agreement. Accordingly, either party shall be entitled to seek injunctive relief, specific performance, or other equitable remedies in respect of any actual or threatened breach of this agreement.]

Exhibit A Designated Confidential Information

Exhibit B Minimum Security Measures

1. IDs, badges, keys, passwords, or other forms of identification or authentication information that grant access to Employer's premises or to any device or equipment capable of displaying or providing access to Confidential Information shall be protected and are prohibited from sharing.

2. Any device or equipment that may display or provide access to Confidential Information shall be locked when not in use or when unattended.

3. The printing of Confidential Information onto paper or any other tangible medium for purposes of display, sharing, transmission, retention, recording, storage, or any other form of use shall be restricted.

4. The transfer, storage, saving, copying, recording, photographing, or duplication of Confidential Information, except where authorised by Employer, shall be prohibited.

5. The use of any device and/or means capable of copying, photographing, recording, transmitting, sharing, conveying, saving, or storing Confidential Information shall be prohibited within the premises and buildings where Employee uses or affords access to such information.

6. The use of Employee's personal device or equipment to access or use Confidential Information shall be prohibited.

7. . . .

（参考和訳）従業員との秘密保持契約書の例

英国：雇用契約における秘密保持条項

1. 本秘密情報

1.1 本秘密情報とは、本従業員が、本雇用主[及びそのグループ会社]に対して負う職務の遂行中、又は、それに関連して、[本契約の締結前、締結日、又は締結後を問わず]知ることとなった、本雇用主[及びそのグループ会社]に関する全ての秘密性のある情報を意味する。これには、以下を含む。

(a) 以下に関する全ての秘密又は専有情報

(i) 本雇用主[、又は、本雇用主のグループ会社]の、研究開発計画、事業運営、雇用関連事項、マーケティング及び広告、財務データ、規制当局及びビジネスパートナーに提出又は受領した文書、過去・現在・将来の顧客及び取引相手に関する情報、顧客及び事業関連会社との関係[、又は]計画、見通し[、意図、又は市場機会]であって、同業又は類似業界の者にとって公知でなく、容易に知り得ないもの、及び

(ii) 本雇用主[、又は、本雇用主のグループ会社]の業務、プロセス、製品情報、ノウハウ、技術情報、デザイン、営業秘密、又はソフトウェアで、本雇用主、その代表者、又はそのグループ会社によって専有情報として指定されたもの

(b) 本秘密情報に由来するいかなる情報、発見、データ、又は解析結果[、及び]

(c) 本雇用主、その代表者[、又は、そのグループ会社、又はそれらの代表者]によって、秘密性又は専有性があると識別された、その他のいかなる情報[、又は]

(d) [別紙 A に記載の情報。]但し、第 1.2 条に定める情報を除く。

1.2 以下のいずれかに該当する情報は、本秘密情報にあたらない。

(a) 本従業員又はその代表者による本契約違反に該当する開示の、直接的又は間接的な結果としてではなく、一般に入手可能である、又は一般に入手可能となった情報[（但し、公知の情報を、非公開の形式で編集したものは、依然として本秘密情報として扱われる）]

(b) 本雇用主からの開示以前に、本従業員が、秘密保持義務なく入手していた情報

(c) 本従業員が知る限り、当該情報について秘密保持義務を負わない第三者から、本従業員が秘密保持義務なく入手した、又は入手可能となった情報

(d) 本雇用主からの開示以前に、本従業員が適法に所持していた情報[、又は]

(e) [本雇用主から開示された情報と無関係に、本従業員により開発された、又は、本従業員のために開発された情報、又は]

(f) 当事者間で書面により、秘密情報でないことに合意した情報

2. 秘密保持義務

2.1 本契約の有効期間中及びその終了後[年数]年間、本従業員は以下を遵守しなければならない。

(a) 全ての本秘密情報を厳格に秘密として保持すること

(b) 本雇用主に対して負う職務遂行の過程でのみ、本秘密情報を使用すること

(c) 本秘密情報に接する者が、常にその秘密性を認識し秘密保持できるように、当該情報を明確にラベル付けし、かつ、秘密として分類されていることを確保すること

(d) 本秘密情報の無断アクセス又は不正使用を防止するため、適切な注意をもって、本秘密情報を保護すること

(e) 別紙 B に定めるセキュリティ対策を実施すること

(f) 本契約に基づく本従業員の職務の遂行において、明示的に許可され、かつ厳密に必要とされる場合を除き、本秘密情報の全部又はその一部を、いかなる者に対しても、直接的又は間接的に、開示、提供、又は開示・提供を試みてはならないこと

(g) 本従業員の職務遂行に厳密に必要な場合を除き、本秘密情報のコピー、書き写し、又はその他の方法で記録しないこと。作成されたコピー、文書、及び、記録は、全て本雇用主の所有物とする

(h) 事前に本雇用主から書面による許可をうることなく、講演や出版物にて、本雇用主の製品やサービス、及び、本従業員の業務に関連する情報を、明示的又は黙示的に提示、開示、又はその他の方法で伝達しないこと

(i) 以下の事項について、直ちに本雇用主に直ちに通知すること。(1)実際に発生した、又は発生が差し迫った本従業員による秘密保持義務違反の疑い、(2)第三者による開示、セキュリティ侵害、不正使用、流用、又はその他の無許可の使用が、許可された開示及び義務的開示の状況において発生した場合を含め、実際に発生した、又は発生が差し迫っている場合

(j) 本秘密情報に関して、知的財産権を取得せず、取得を試みないこと

(k) [その他、特定の要件がある場合は、ここに記載する。]

3. 許可された開示

3.1 本従業員は、以下の条件を満たす場合に限り、その代表者に対して、本秘密情報を開示することができる。

(a) 本秘密情報が開示される前に、本雇用主の関連会社、従業員及び顧客に対し、本秘密情報の秘密性を通知すること

(b) 当該個人又は団体が、第 2.1 条の秘密保持義務を遵守することを確保すること

4. 義務的開示

4.1 本条の規定に従い、本従業員は、以下の場合に限り、必要最小限の範囲で、本秘密情報を開示することができる。

(a) 管轄権を有する裁判所、規制当局、司法機関、行政庁その他類する機関、又は税務当局の命令がなされた場合

(b) 本雇用主[、又は、そのグループ会社]が従うべき、適用される法律又は規制による場合

4.2 第 4.1 条に従い本秘密情報を開示する前に、本従業員は、適用法令で許される限度で、本雇用主に、当該開示に関してできるだけ事前に通知するよう、合理的な努力を尽くさなければならない。

5. 本秘密情報の返還又は破棄

5.1 (1)雇用の完了、若しくは、終了に際して、又は、(2)本雇用主の書面による要請があった場合、本従業員は以下を履行しなければならない。

(a) 本雇用主の本秘密情報を含み、反映し、取り込み、又は基づく、全ての文書、データ及び資料[それらのコピーを含む。]を、破棄[、又は、本雇用主に返還]すること

(b) メモ、報告書、覚書、記録、ファイル、図面、プロトコル、及び、その他類似の文書を含む、本雇用主、又はそのグループ会社に関連する、全ての文書、装置、データ、並びに、資料[、及び、それらのコピー]を、破棄[、又は、本雇用主に返還]すること

(c) 本従業員は、第 5.1 条 b 記載の項目が、本雇用主とそのグループ会社の単独の所有物であること、及び、本従業員が第 5.1 条の要件を充足したことを、本雇用主に対し書面で証明すること

6. 非保証及び表明の不存在

6.1 本雇用主による本秘密情報の開示は、本雇用主が本従業員とのさらなる契約を締結することについての、申込み、表明、保証を構成しない。

6.2 本契約で明示的に定める場合を除き、本雇用主は、本秘密情報の正確性又は完全性を含むが、これに限定されない、本秘密情報に関する明示又は黙示の表明又は保証を一切行わない。

7. 権利及び救済

7.1 本契約で明示的に定める場合を除き、本契約に規定された権利及び救済は、法律によって付与される権利及び救済に追加されるものであり、これを排除するものではない。

7.2 [各当事者が有する他の権利又は救済を妨げることなく、各当事者は、損害賠償のみでは、本契約違反に対する十分な救済とはならない場合があることを認め、同意する。したがって、各当事者は、本契約の実際の、又は差し迫った違反に関して、差止命令、特定義務の履行請求、又は、その他の衡平法上の救済を受ける権利を有するものとする。]

Exhibit A 指定秘密情報

Exhibit B 最低限のセキュリティ対策

1. 本雇用主の施設、又は本秘密情報を表示又は利用可能な機器・装置へのアクセスを許可する ID、バッジ、キー、パスワード、又はその他の形式の認証情報は、保護されなければならず、共有してはならない。

2. 本秘密情報を表示又はアクセスできる機器・装置は、使用していない場合、又は無人の場合は、施錠しなければならない。

3. 本秘密情報を表示、共有、送信、保持、記録、保存、又はその他の利用のために、紙その他の有体媒体に印刷することは制限される。

4. 本雇用主に許可されない限り、本秘密情報の転送、保管、保存、コピー、記録、写真撮影、及び、複写は禁止される。

5. 本従業員が、本秘密情報を使用又はアクセスできる施設・建物内で、本秘密情報のコピー、写真撮影、記録、送信、共有、伝達、保存、又は保管の機能を備えた機器又は手段の使用は禁止される。

6. 本秘密情報にアクセス又は利用するために、本従業員個人の機器又は装置を使用することは禁止される。

7. . . .

3　退職後の競業避止契約書の例
UK Employee Non-compete Agreement

1. Definitions and interpretation

The definitions and rules of interpretation in this clause apply throughout this agreement.

(a) **Board**: the board of directors of the Company (including any committee of the board duly appointed by it).

(b) **Capacity**: acting as an agent, consultant, director, employee, worker, owner, partner or shareholder.

(c) **Confidential Information**: information (whether or not recorded in documentary form, or stored on any magnetic or optical disk or memory) that is not in the public domain and relates to [our **OR** any Group Company's] business, products, affairs or finances, and which, at the time of disclosure, is confidential to [us **OR** any Group Company], and trade secrets, including, without limitation, technical data and know-how relating to [our **OR** any Group Company's] business or any of [our **OR** its] business contacts, including, in particular, without limitation, [EXAMPLES].

(d) **Garden Leave**: any period during which we have [exercised our rights under clause [NUMBER] **OR** required you not to carry out any work or to refrain from contacting our employees or business contacts].

(e) [**Group Company**: the Company, its Subsidiaries or Holding Companies from time to time, and any Subsidiary of any Holding Company.]

(f) **Restricted Business**: any part of [our **OR** any Group Company's] business in which you were materially involved during the [PERIOD] months prior to Termination.

(g) **Restricted Customer**: any firm, company or person who, during the [PERIOD] months prior to Termination, was [a customer or prospective customer of **OR** regularly dealt with] [the Company **OR** any Group Company], and with whom you had contact [or of whom you became aware or were informed] in the course of your employment.

(h) **Restricted Person**: anyone employed [or engaged] by [us **OR** any Group Company] [at the level of [POSITION] or above, and who could materially damage [our **OR** any Group Company's] interests if they were involved in any Capacity in any business which competes with any Restricted Business], and with whom you had dealings during the [PERIOD] months prior to Termination.

(i) [**Subsidiary and Holding Company**: in relation to a company, "subsidiary" and "holding company" have the meanings given in section 1159 of the Companies Act 2006. [For the purposes only of the membership requirement contained in subsections 1159(1)(b) and (c), a company shall be treated as a member of another company even if its shares in that other company are registered in the name of (a) another person (or its nominee), whether by way of security or in connection with the taking of security, or (b) a nominee].]

(j) **Termination**: the ending of your employment with us, however caused.

2. Restrictions

2.1 In order to protect the Confidential Information and [our **OR** any Group Company's] business connections to which you have access as a result of your employment with us, you covenant with us [(on our own behalf and as trustee and agent for each Group Company)] that you shall not:

(a) during your employment with us and for a period of [PERIOD] months following Termination, solicit or attempt to entice away from [us **OR** any Group Company] the business or custom of any Restricted Customer, with a view to providing goods or services to that Restricted Customer, in competition with any Restricted Business;

(b) [during your employment with us and for a period of [PERIOD] months following Termination [in the course of any business concern which is in competition with any Restricted Business], offer to employ, engage or otherwise attempt to entice away from [us **OR** any Group Company] any Restricted Person;]

(c) [during your employment with us and for a period of [PERIOD] months following Termination [in the course of any business concern which is in competition with any Restricted Business], employ or engage or otherwise facilitate the employment or engagement of any Restricted Person, whether or not such person would be in breach of contract as a result of such employment or engagement;]

(d) during your employment with us and for a period of [PERIOD] months following Termination, be involved in any Capacity with any business concern which is (or intends to be) in competition with any Restricted Business;

(e) for a period of [PERIOD] months following Termination, be involved in the provision of goods or services to (or otherwise have business dealings with) any Restricted Customer in the course of any business concern which is in competition with any Restricted Business;

(f) at any time following Termination, represent yourself as being connected with [us **OR** any Group Company] in any Capacity, other than as a former employee, or use any registered names or trading names associated with [us **OR** any Group Company];

(g) during your employment with us,

(i) disclose or use, or attempt to disclose or use, any Confidential Information or trade secrets that you have access to, without prior written authorisation, or allow directly or indirectly, any unauthorised third party to obtain or use Confidential Information or trade secrets;

(ii) pursue or attempt to pursue any economic or social interest in any business concern other than us; or

(h) during your employment with us, without prior written authorisation,

(i) provide goods or services for, or carryout business activities (including consulting, financing, management, operations, or marketing) for, or engage in preparatory activities for the launch of any business concern that competes with any Restricted Business,

(ii) assume a Capacity in […],

(iii) assist in the employment or engagement of any employee by […], or

(iv) represent yourself as holding any Capacity in, or as being connected with, any business concerns other than us.

2.2 None of the restrictions in clause 2.1 shall prevent you from:

(a) holding an investment, by way of shares or other securities, of no more than [5]% of the total issued share capital of any company, whether or not listed or dealt in on a recognized stock exchange; [or]

(b) being engaged or concerned in any business concern, provided that your duties or work relate solely to geographical areas where that business concern does not compete with any Restricted Business[; or **OR** .]

(c) [being engaged or concerned in any business concern, provided that your duties or work relate solely to services or activities of a kind with which you were not materially concerned during the [PERIOD] months prior to Termination.]

2.3 The restrictions imposed on you by this clause 2 apply to you acting:

(a) directly or indirectly; and

(b) on your own behalf or on behalf of, or in conjunction with, any firm, company or person.

2.4 The period[s] for which the restriction[s] in clause 2.1 apply shall be reduced by any period that you spend on Garden Leave immediately prior to Termination.

2.5 If, during your employment with us or before the expiry of the last of the covenants in this clause 2, you receive an approach or offer to be involved in any Capacity in a business that competes with any part or parts of [our OR any Group Company's] business in which you are or have been materially involved during your employment with us, you shall:

(a) notify [us OR the Board] [in writing] of the fact of the approach or offer and the identity of the person making it, as soon as possible; [and]

(b) [if requested, provide a copy of any written offer as soon as possible; and]

(c) provide the person making the offer with a copy of this clause 2 within [seven days] of the offer being made.

The obligations under this clause 2.5 are continuing obligations and shall also apply if, at any time after the relevant approach or offer is made, but before the expiry of the last of the covenants in this clause 2, the business making the offer or approach competes with [our OR any Group Company's] business.

2.6 [If, at any time during your employment, [two] or more Restricted Persons leave their employment, appointment or engagement with us to provide services to a business concern that competes with, or is intended to compete with any Restricted Business, you shall not, during the six months following the last date on which any of those Restricted Persons were employed or engaged by us, be employed or engaged in any capacity with that business concern.]

2.7 The parties confirm that they have entered into the restrictions in this clause 2 having received separate and independent legal advice.

2.8 Each of the restrictions in this clause 2 is intended to be separate and severable. If any restriction is held to be void but would be valid if part of its wording were deleted, that restriction shall apply with such deletion as may be necessary to render it valid and effective.

2.9 If your employment is transferred to any firm, company, person or entity other than a Group Company ("New Employer") pursuant to the Transfer of Undertakings (Protection of Employment) Regulations 2006, you shall, if required, enter into an agreement with New Employer containing post-termination restrictions corresponding to those in this clause 2, protecting the [confidential information], trade secrets and business connections of New Employer.

2.10 [You shall, at our request and expense, enter into a separate agreement with any Group Company in which you agree to be bound by restrictions corresponding to those in this clause 2 (or such of those restrictions as may be appropriate) in relation to that Group Company.]

（参考和訳）退職後の競業避止契約書の例

英国における従業員の競業避止契約

1. 定義及び解釈

本条に定める定義及び解釈は、本契約全体に適用される。

(a) **本取締役会**：当社の取締役会（取締役会により正式に任命された委員会を含む）。

(b) **資格**：代理人、コンサルタント、取締役、従業員、労働者、所有者、パートナー、又は株主として行動することをいう。

(c) **本秘密情報**：（文書形式で記録されているか否か、磁気ディスク、光学ディスク又はメモリに保存されているか否かを問わず）公知ではなく、[当社又は本グループ会社の]事業、製品、業務又は財務に関連し、開示時に、[当社又は本グループ会社にとって、]秘密である情報、及び、営業秘密をいう。これには、[当社又は本グループ会社]の事業又は[当社又はその]事業関係者に関連する技術データ及びノウハウを含むが、これらに限定されない。特に[例]を含むが、これに限定されない。

(d) **ガーデンリーブ**：当社が、[第[数字]条に基づく権利を行使した、又は、あなたに就労業務を行わないこと、当社の従業員若しくは事業関係者との接触を控えることを要求した]期間をいう。

(e) [**本グループ会社**：当社、その子会社、持ち株会社、及び、持株会社の子会社をいう。]

(f) **制限事業**：雇用関係終了前[期間]か月間に、あなたが実質的に関与していた[当社又は本グループ会社の]事業の一部をいう。

(g) **制限顧客**：雇用関係終了前[期間]か月間に、[当社又は本グループ会社の][顧客若しくは潜在的顧客であった、又は定期的に取引していた]企業、会社、又は個人であって、あなたがあなたの雇用期間中に接触した、[又はあなたが認識した若しくは知らされた]者をいう。

(h) **制限対象者**：[当社**又は**本グループ会社]に雇用され[又は契約している]者で、[職位が[ポジション]以上であり、制限事業と競合する事業においていかなる地位で関与したとしても、[当社**又は**本グループ会社]の利益に重大な損害を与える可能性がある者で]、あなたが雇用関係終了前[期間]か月内に業務上関与した者をいう。

(i) [**子会社及び持ち株会社**：会社に関して、2006 年会社法の第 1159 条で定義されている、「子会社」及び「持ち株会社」をいう。[同法第 1159 条第 1 項(b)及び(c)に定める会員要件を満たすためだけに、親会社の株式が子会社において、(a)他の者（又はその名義人）の名義で登録されている場合（担保のため、又は担保取得に関連している場合）、又は(b)名義人の名義で登録されている場合であっても、親会社は子会社の構成員とみなされるものとする。]

(j) **雇用関係終了**：原因を問わず、あなたと当社との間の雇用の終了をいう。

2. 制約

2.1 あなたがあなたと当社との雇用関係によりアクセスできる本秘密情報及び[当社又は本グループ会社の]事業上のつながりを保護するため、あなたは当社に対し[（当社自身のため、並びに各本グループ会社の受託者及び代理人として）]あなたが以下の行為に及ばないことを約する。

(a) あなたと当社との雇用期間中及び雇用関係終了後[期間]か月間、制限顧客に対して制限事業と競合する製品又はサービスを提供する目的で、[当社又は本グループ会社]との取引関係をやめさせ、又は当該制限顧客から新たな取引を誘致しようとすること

(b) [あなたと当社との雇用期間中及び雇用関係終了後[期間]か月間、[制限事業と競合する事業において]、[当社又は本グループ会社]から制限対象者を引き離そうとする目的で、雇用を申し出、契約を提案し、又はその他の方法で引き抜こうと試みること。]

(c) [あなたと当社との雇用期間中及び雇用関係終了後[期間]か月間、[制限事業と競合する事業において]、制限対象者を雇用し、契約し、又はその雇用若しくは契約を容易にすること（当該者がその雇用又は契約により契約違反となるか否かを問わない）。]

(d) あなたと当社との雇用期間中及び雇用関係終了後[期間]か月間、[制限事業と競合している（又は競合しようとしている）事業に、いかなる資格であっても関与すること。]

(e) [制限事業と競合する事業において、制限顧客に対する製品又はサービスの提供に関与し、又はその他の取引関係を持つこと。]

(f) 雇用関係終了後のいかなる時点においても、元従業員として以外のいかなる資格においても、あなたが[当社**又は**本グループ会社]と関係があると自己を称したり、[当社**又は**本グループ会社]に関連する登録名称又は商号を使用したりすること

(g) あなたと当社の雇用期間中、

(i) 事前の書面による承認なく、あなたがアクセスできる本秘密情報又は営業秘密を開示し、又は使用し、若しくは開示し、又は使用しようと試みること、又は直接的若しくは間接的に、権限のない第三者に本秘密情報又は営業秘密を取得、又は使用させること

(ii) 当社以外の事業において、経済的又は社会的利益を追求し、若しくは、追求しようとすること

(h) あなたと当社の雇用期間中、事前の書面による承認なく、

(i) 制限事業と競合する事業に対し、製品又はサービスを提供し、又は事業活動（コンサルティング、資金調達、経営、運営又はマーケ

ティングを含む）を行い、若しくはその事業の開始に向けた準備活動に従事すること

(ii) [ ]において資格に就くこと

(iii) [ ]による従業員の雇用又は契約を支援すること

(iv) 当社以外の事業において、あなた自身が何らかの資格に就いていると称し、又は、当該事業と関係があると称すること

2.2 第 2.1 条の制限は、あなたについて以下の事項を妨げない。

(a) 公認の証券取引所に上場又は取引されているか否かを問わず、会社の発行済株式資本の総額の[5]%以下の株式又はその他の証券を保有すること[又は]

(b) あなたの職務又は業務が、制限事業と競合しない地理的領域に限定される限りで、事業主の事業に従事又は関与すること[又は]

(c) [あなたの職務又は業務が、雇用関係終了前[期間]か月間にあなたが実質的に関与しなかった種類のサービス又は活動に限られることを条件として、事業に従事又は関与すること。]

2.3 あなたに課せられた本第 2 条による制限は、下記あなたの行動に適用される。

(a) 直接的又は間接的に行動する場合

(b) あなた自身のため、企業・会社・個人のため、又はそれらと連携して行動する場合

2.4 本第 2.1 条の制限が適用される期間は、雇用関係終了前にあなたがガーデンリーブに服した期間分、短縮される。

2.5 あなたの雇用期間中、又は本第 2 条に定める最後の誓約の期限が満了する前に、あなたが、[当社又は本グループ会社の]事業のうち、あなたがあなたと当社における雇用期間中に実質的に関与している又は関与していた部分と競合する事業において、何らかの資格で関与することについての働きかけ又は申出を受けた場合、あなたは以下をしなければならない。

(a) [当社又は本取締役会]に、[書面で]、当該働きかけ又は申出の事実及びそれをを行った者の身元を、可能な限り速やかに、通知すること

(b) [要求された場合、可能な限り速やかに、書面による申出の写しを提供すること。]

(c) 申出をした者に、申出がなされてから[7 日]以内に、本第 2 条の写しを交付すること

本第 2.5 条に基づく義務は、継続的な義務であり、関連する働きかけ、又は申出がなされた後、かつ本第 2 条に定める最後の誓約の期限が満了する前に、当該働きか

け、又は申出を行った事業が、[当社又は本グループ会社]の事業と競合する場合にも、適用される。

2.6 [あなたの雇用期間中に、[2]名以上の制限対象者が、当社との雇用、任命又は契約を終了し、制限事業と競合する、又は競合することを予定する事業にサービスを提供する場合、あなたは、その制限対象者のいずれかが雇用又は契約されていた最後の日から 6 か月間、当該事業において、いかなる資格でも雇用され、又は関与してはならない。]

2.7 両当事者は、独立した法的助言を受けた上で、本第 2 条に定める制限に合意したことを確認する。

2.8 本第 2 条の各制限は、別個かつ分離可能であることを意図している。制限のいずれかが無効と判断されても、その文言の一部を削除すれば有効となる場合、当該制限は、有効かつ効力を持つために必要な削除がなされた上で適用されるものとする。

2.9 2006 年事業譲渡（雇用保護）規則に従って、本グループ会社以外の企業、会社、個人、又は団体（以下、「新規雇用主」という）にあなたの雇用が移転された場合、あなたは、要求された場合、新規雇用主の[本秘密情報]、営業秘密、及び事業上のつながりを保護するため、本第 2 条に定める制限と同様の雇用契約終了後の制限を含む契約を新規雇用主と締結するものとする。

2.10 [あなたは、当社の求めに応じて、当社の費用で、本グループ会社との間で、別個に、本第 2 条に定める制限と同様の制限（、又はその中で適切と考えられる制限）に拘束されることにあなたが同意する契約を締結しなければならない。]

4　取引先との秘密保持契約書の例
Confidentiality Clauses in Transactional Agreements

1. Confidential Information

1.1 Confidential Information means all confidential information relating to the Purpose that Discloser or its Representatives [or any Group Company of Discloser, or their Representatives] directly or indirectly provides to Recipient or its Representatives [or any Group Company of Recipient, or their Representatives][, whether before, on or after the date of this agreement]. This includes:

(a) the fact that discussions and negotiations are taking place concerning the Purpose and the status of those discussions and negotiations;

(b) [the [existence and] terms of this agreement;]

(c) all confidential or proprietary information relating to:

(i) research and development plans, business operations, financial data, past, present, or prospective customers or clients, relationships with customers and business affiliates[, OR] future plans[, intentions, or market opportunities] of Discloser [or any Group Company of Discloser] that are not publicly known or readily ascertainable by someone operating in the same or similar business sector; and

(ii) operations, processes, product information, know-how, technical data, designs, trade secrets or software belonging to Discloser[, or any Group Company of Discloser], that are designated as proprietary by Discloser, its Representative or its Group Company;

(d) any information, findings, data or analysis derived from the Confidential Information; [and]

(e) any other information identified by Discloser or its Representatives [or any Group Company of Discloser, or their Representatives] as being confidential or proprietary in nature[; and OR .]

(f) [any information detailed in Exhibit A] but excludes any information referred to in clause 1.2.

1.2 Information shall not be considered Confidential Information if:

(a) it is, or becomes, publicly available other than as a direct or indirect result of disclosure by Recipient or its Representatives in breach of this agreement (except that any compilation of publicly available information in a non-public format shall still be treated as Confidential Information) ;

(b) it was available to Recipient on a non-confidential basis prior to disclosure by Discloser;

(c) it was, is, or becomes available to Recipient on a non-confidential basis from a third party who, to Recipient's knowledge, is not subject to any confidentiality obligation in respect of that information;

(d) it was lawfully in Recipient’s possession prior to disclosure by Discloser; [or]

(e) [it is developed by or for Recipient independently of the information disclosed by Discloser; or]

(f) the parties agree in writing that the information is not confidential.

2. Confidentiality Obligations

2.1 In return for Discloser making the Confidential Information available to Recipient, Recipient undertakes to Discloser that it shall:

(a) keep all Confidential Information strictly secret and confidential;

(b) not use the Confidential Information except as necessary to fulfil the Purpose;

(c) label and classify the Confidential Information as confidential in a manner that allows anyone who is exposed to it to recognize and uphold its confidential nature at all times;

(d) protect the Confidential Information with appropriate care to prevent unauthorised access or misuse;

(e) implement the security measures set out in Exhibit B;

(f) not, whether directly or indirectly, disclose, make available, or attempt to disclose or make available any Confidential Information, in whole or in part, to any person except where expressly permitted, and strictly necessary to fulfil the Purpose under this agreement;

(g) obtain a valid confidentiality agreement in writing from any employee, officer, expert, business affiliate, and other person who is expected to receive or be exposed to the Confidential Information, and to ensure that such individuals are legally bound by a duty of confidentiality identical to Recipient's duty under this agreement;

(h) obtain Discloser's prior written consent for any contractual or statutory transfer of Recipient's rights and/or obligations under this agreement;

(i) not copy, transcribe or otherwise record Confidential Information except where strictly necessary for the Purpose. Any such copies, written records, or other reproductions shall remain the property of Discloser;

(j) immediately notify Discloser of (1) any suspected actual or imminent breach of confidentiality by Recipient or any employee, officer, expert, business affiliate, or other person who is expected to receive or be exposed to the Confidential Information, (2) any actual or imminent disclosure, security breach, misuse, misappropriation, or other unauthorised use by any person, including where such events occur in the context of Permitted Disclosure or Mandatory Disclosure;

(k) not seek or attempt to obtain intellectual property rights in respect of the Confidential Information;

(l) [INCLUDE ANY OTHER SPECIFIC REQUIREMENTS.]

3. Permitted Disclosure

3.1 Recipient may disclose Confidential Information to its Representatives, provided that it:

(a) informs such Representatives of the confidential nature of the Confidential Information prior to disclosure; and

(b) procures that such Representatives comply with the confidentiality obligations in clause 2.1 as if they were Recipient.

3.2 Recipient shall be liable for any acts or omissions of its Representatives in relation to the Confidential Information as if such acts or omissions were its own.

4. Mandatory Disclosure

4.1 Subject to the provisions of this clause, a party may disclose Confidential Information only to the minimum extent required by:

(a) an order of any court, regulatory, judicial, governmental or similar body, or any taxation authority, in each case of competent jurisdiction;

(b) the rules of any listing authority or stock exchange on which its shares [or those of its Group Company] are listed or traded; or

(c) applicable laws or regulations of any jurisdiction to which its affairs [or those of its Group Company] are subject.

4.2 Before making any disclosure under clause 4.1, a party shall, to the extent permitted by applicable law, use all reasonable endeavors to provide the other party with as much advance notice of the intended disclosure as possible. [Where such notice is not prohibited and is given in accordance with this clause 4.2, the disclosing party shall take into account the reasonable requests made by the other party regarding the content of the disclosure.]

4.3 If a party is unable to inform the other party prior to disclosing Confidential Information pursuant to clause 4.1, it shall, to the extent permitted by applicable law, inform the other party of the full circumstances of the disclosure and the information disclosed as soon as reasonably practicable thereafter.

5. Return or destruction of the Confidential Information

5.1 (1) Upon the completion or termination of the Purpose or (2) upon Discloser's written request at any time , Recipient shall:

(a) destroy [or return to Discloser] all documents, data, and materials [(including any copies)] that contain, reflect, incorporate or are based on Discloser's Confidential Information;

(b) erase all of Discloser's Confidential Information from its computer and communications systems and devices used by it, or stored in electronic form; [and]

(c) [[to the extent technically and legally practicable,] erase all of Discloser's Confidential Information stored in electronic form on systems and data storage services provided by third parties; and]

(d) certify in writing to Discloser that it has complied with the requirements of this clause 5.1.

5.2 Nothing in clause 5.1 shall require Recipient to return or destroy any documents or materials containing or based on Discloser's Confidential Information that Recipient is required to retain

under applicable law, to satisfy the requirements of a regulatory authority or body of competent jurisdiction, or under the rules of any listing authority or stock exchange to which it is subject. The provisions of this agreement shall continue to apply to any such documents and materials retained by Recipient pursuant to this clause 5.2.

6. No warranty and no representation

6.1 The disclosure of Confidential Information by one party does not give the other party, or any other person, any license or other rights in respect of such Confidential Information beyond those expressly set out in this agreement.

6.2 Except as expressly stated in this agreement, Discloser makes no express or implied warranty or representation regarding its Confidential Information, including, without limitation, its accuracy or completeness.

6.3 The disclosure of the Confidential Information by either party shall not constitute an offer, representation or warranty by that party to enter into any further agreement with the other party [in relation to the Purpose].

7. Rights and remedies

7.1 Except as expressly provided in this agreement, the rights and remedies set out in this agreement are in addition to, and not exclusive of, any rights or remedies available at law.

7.2 [Without prejudice to any other rights or remedies available to either party, each party acknowledges and agrees that damages alone may not be an adequate remedy for any breach of this agreement. Accordingly, either party shall be entitled to seek injunctive relief, specific performance or other equitable remedies in respect of any actual or threatened breach of this agreement.]

8. No obligation to continue discussions

Nothing in this agreement shall impose any obligation on either party to continue discussions or negotiations in connection with the Purpose, nor shall it oblige either party[, or its Group Company] to disclose any information (whether Confidential Information or otherwise) to the other party.

9. Ending discussions and duration of confidentiality obligations

9.1 If either party decides not to continue its involvement in the Purpose with the other party, it shall notify that other party in writing without delay.

9.2 Notwithstanding the termination of discussions between the parties in relation to the Purpose pursuant to clause 9.1, each party's obligations under this agreement shall remain in full force and effect for a period of [two] years from the date of this agreement.

9.3 The termination of discussions relating to the Purpose shall not affect any accrued rights or remedies to which either party may be entitled.

Exhibit A Designated Confidential Information

Exhibit B Minimum Security Measures

1. A password shall be required to log into any device that may display or provide access to Confidential Information to a user of the device.

2. The printing of Confidential Information onto paper or any other tangible medium for purposes of display, sharing, transmission, retention, recording, storage, or any other form of use shall be restricted.

3. Access to premises and buildings where Recipient uses or provides access to Confidential Information shall be limited to individuals who are subject to a duty of confidentiality to Recipient.

4. The use of any device and/or a means capable of copying, photographing, recording, transmitting, sharing, conveying, saving, or storing Confidential Information shall be prohibited within the premises and buildings where Recipient uses or affords access to such information.

5. . . .

（参考和訳）取引先との秘密保持契約書の例

英国：取引契約における秘密保持条項

1. 本秘密情報

1.1 本秘密情報とは、開示者又はその代表者[又は開示者のグループ会社若しくはその代表者]が、目的に関連して、受領者又はその代表者[又は受領者のグループ会社若しくはその代表者]に[本契約締結前、締結日、又は締結後を問わず]、直接又は間接的に提供する、全ての秘密性を有する情報をいう。これには以下を含む。

(a) 目的に関する協議及び交渉が行われている事実並びにその協議及び交渉の状況

(b) [本契約の[存在及び]条件]

(c) 以下に関連する全ての秘密又は専有情報

(i) 開示者[、又は開示者のグループ会社]の、研究開発計画、事業運営、財務データ、過去・現在・将来の顧客又はクライアント、顧客及びビジネス提携先との関係[、又は]計画[、意図、又は市場機会]であって、同業又は類似業界の者にとって公知でなく、容易に知り得ないもの

(ii) 開示者[又は開示者のグループ会社]の業務、プロセス、製品情報、ノウハウ、技術情報、デザイン、営業秘密又はソフトウェアで、開示者、その代表者、又はそのグループ会社によって専有情報として指定されたもの

(d) 本秘密情報に由来する情報、発見、データ、又は解析結果[、及び]

(e) 開示者又はその代表者[又は開示者のグループ会社若しくはその代表者]によって、秘密性又は専有性があると識別された、その他の情報[、又は]

(f) [Exhibit A に記載の情報。]但し、第 1.2 条に定める情報を除く。

1.2 以下のいずれかに該当する情報は、本秘密情報にあたらない。

(a) 受領者又はその代表者による本契約違反に該当する開示の直接的又は間接的な結果としてではなく、一般に入手可能である、又は一般に入手可能となった情報（但し、公知の情報を非公開の形式で編集したものは、依然として本秘密情報として扱われる）

(b) 開示者による開示以前に、受領者が、秘密保持義務なく入手していた情報

(c) 受領者が知る限り、当該情報について秘密保持義務を負わない第三者から、受領者が秘密保持義務なく入手した、又は入手可能となった情報

(d) 開示者による開示以前に、受領者が適法に所持していた情報[又は]

(e) [開示者による開示情報と無関係に、受領者により独自に、又は受領者のために開発された情報、又は]

(f) 当事者間で書面により、秘密情報でないことに合意した情報

2. 秘密保持義務

2.1 開示者が、本秘密情報を受領者が利用できるようにすることと引き換えに、受領者は、開示者に対して、以下を誓約する。

(a) 全ての本秘密情報を厳格に秘密として保持すること

(b) 目的を達成するために必要な場合を除き、本秘密情報を使用しないこと

(c) 本秘密情報に接する者が、常にその秘密性を認識し秘密保持できるように、当該情報を秘密としてラベル付けし、分類すること

(d) 本秘密情報への無断アクセス又は不正使用を防止するため、適切な注意をもって本秘密情報を保護すること

(e) 別紙 B に定めるセキュリティ対策を実施すること

(f) 本契約に基づき明示的に許可され、かつ目的達成に厳密に必要な場合を除き、本秘密情報の全部又は一部を、直接的又は間接的に、いかなる者に対しても、開示、提供、又は開示・提供を試みないこと

(g) 本秘密情報を受領又は接することが予想される従業員、役員、専門家、事業関係者その他の者から、書面による有効な秘密保持契約を取得し、当該者が本契約に基づく受領者の義務と同一の秘密保持義務に法的に拘束されることを確保すること

(h) 本契約に基づく受領者の権利及び／又は義務の契約上又は法令上の譲渡について、事前に開示者の書面による同意をうること

(i) 目的達成に厳密に必要な場合を除き、本秘密情報を複写、書き写し、又はその他の方法で記録しないこと。作成されたコピー、書面記録、その他の複製物は全て開示者の所有物とすること

(j) 以下の事項について、直ちに開示者に通知すること。(1)受領者又は本秘密情報を受領又は接することが予想される従業員、役員、専門家、事業関係者その他の者による、秘密保持義務違反の疑いが実際に発生した、又は発生が差し迫っている場合、又は(2)第三者による開示、セキュリティ侵害、不正使用、流用、又はその他の無許可の使用が、許可された開示及び義務的開示の状況において発生した場合を含め、実際に発生した、又は発生が差し迫っている場合

(k) 本秘密情報に関して、知的財産権を取得せず、取得を試みないこと

(l) [その他、特定の要件がある場合は、ここに記載する。]

3. 許可された開示

3.1 受領者は、以下の条件を満たす場合に限り、その代表者に対して、本秘密情報を開示することができる。

(a) 本秘密情報が開示される前に、当該代表者に対し、本秘密情報の秘密性を通知すること

(b) 当該代表者が、第 2.1 条に定める秘密保持義務を、受領者と同様に遵守することを確保すること

3.2 受領者は、本秘密情報に関して、その代表者の行為又は不作為について、自己の行為又は不作為と同様に責任を負うものとする。

4. 義務的開示

4.1 本条の規定に従い、当事者は、以下の場合に限り、必要最小限の範囲で、本秘密情報を開示することができる。

(a) 管轄権を有する裁判所、規制当局、司法機関、行政庁その他類する機関、又は税務当局の命令がなされた場合

(b) 当事者[又はそのグループ会社の株式]が上場又は取引されている上場当局又は証券取引所の規則に従う場合

(c) 当事者[又はそのグループ会社]が従うべき、適用される法律又は規制による場合

4.2 第 4.1 条に従い本秘密情報を開示する前に、当事者は、適用法令で許される限度で、相手方当事者に対し、当該開示に関してできるだけ事前に通知するよう、合理的な努力を尽くさなければならない。[当該通知が禁止されておらず、第 4.2 条に従って通知が行われる場合、開示当事者は、開示内容に関して他方当事者からなされた合理的な要請を考慮しなければならない。]

4.3 第 4.1 条に従って本秘密情報を開示するに際し、当事者が事前に他方当事者に通知することができない場合、当事者は、適用法令で許される限度で、開示の状況及び開示された情報の全容を、可能な限り速やかに相手方当事者に通知しなければならない。

5. 本秘密情報の返還又は消去

5.1 (1)目的の完了若しくは終了時、又は(2)開示者からの書面による要請があった場合、受領者は以下を履行しなければならない。

(a) 開示者の本秘密情報を含み、反映し、取り込み、又は基づく全ての文書、データ及び資料[それらのコピーを含む。]を、破棄[又は開示者に返還]すること

(b) 開示者の本秘密情報を、受領者が使用するコンピュータ及び通信システム並びに機器から、又は電子形式で保存されている場合には、全て消去すること

(c) [[技術的及び法的に実行可能な範囲で]第三者が提供するシステム及びデータ保存サービスに電子形式で保存されている開示者の本秘密情報を全て消去すること]

(d) 第 5.1 条の要件を遵守したことを、開示者に対し書面で証明すること

5.2 第 5.1 条のいかなる規定も、受領者が、適用法令に基づき保持することを義務づけられている文書及び資料、管轄権を有する規制当局又は機関の要件を満たすために保持することを義務づけられている文書及び資料、又は当該受領者が従うべき上場当局又は証券取引所の規則に基づき保持することを義務づけられている文書及び資料を、返還又は破棄することを要求するものではない。受領者が第 5.2 条に従って保持する当該文書及び資料については、本契約の規定が引き続き適用されるものとする。

6. 非保証及び表明の不存在

6.1 一方当事者による本秘密情報の開示は、相手方当事者又は他者に対し、本契約で明示的に定められた範囲を超えて、当該本秘密情報に関するライセンス又はその他の権利を付与するものではない。

6.2 本契約で明示的に定める場合を除き、開示者は、本秘密情報の正確性又は完全性を含むが、これに限定されない、本秘密情報に関する明示又は黙示の表明又は保証を一切行わない。

6.3 当事者の本秘密情報の開示は、[目的に関して、]当該当事者が相手当事者とのさらなる契約を締結することについての申込み、表明又は保証を構成しない。

7. 権利及び救済

7.1 本契約で明示的に定める場合を除き、本契約に規定された権利及び救済は、法律によって付与される権利及び救済に追加されるものであり、これを排除するものではない。

7.2 [各当事者が有する他の権利又は救済を妨げることなく、各当事者は、損害賠償のみでは、本契約違反に対する十分な救済とならない場合があることを認め、同意する。したがって、各当事者は、本契約の実際の又は差し迫った違反に関して、差止命令、特定義務の履行請求、又はその他の衡平法上の救済を受ける権利を有するものとする。]

8. 協議を継続する義務の不存在

本契約のいかなる規定も、目的に関連して、いずれの当事者に対しても協議又は交渉を継続する義務を課すものではなく、各当事者[又はそのグループ会社]に、相手方当事者に対して、情報（本秘密情報か否かを問わない）を開示する義務を課すものではない。

9. 協議の終了及び守秘義務の期間

9.1 いずれかの当事者が、目的に関して他方当事者との関与を継続しないことを決定した場合、当該当事者は、遅滞なく書面により他方当事者に通知しなければならない。

9.2 第 9.1 条に従って目的に関する協議が終了した場合であっても、各当事者の本契約に基づく義務は、本契約の日から[2]年間、完全に効力を有するものとする。

9.3 目的に関する協議の終了は、いずれの当事者が有する既得の権利又は救済に影響を及ぼすものではない。

Exhibit A 指定秘密情報

Exhibit B 最低限のセキュリティ対策

1. 本秘密情報を表示又はアクセス可能な機器にログインするためには、パスワードを必須としなければならない。

2. 本秘密情報の表示、共有、送信、保持、記録、保存、又はその他の使用のために、紙その他の有体媒体に印刷することは制限される。

3. 受領者が本秘密情報を使用し、又はアクセスを提供する施設及び建物へのアクセスは、受領者に対して秘密保持義務を負う者に限定されなければならない。

4. 本秘密情報のコピー、写真撮影、記録、送信、共有、伝達、保存、又は保管が可能な機器及び／又は手段の使用は、受領者が当該情報を使用し、又はアクセスを提供する施設及び建物内において禁止される。

5. . . .

5　来訪者受付表
Visitor List

No.	Name	ID	Contact details	Company	Arrival	Departure	Accepted by

（参考和訳）来訪者受付表

訪問客リスト

No.	氏名	ID	連絡先	企業	到着日時	出発日時	受入対応者 （受入先）