経済産業省委託事業

営業秘密に関する欧米の法制度調査

2022 年 3 月

独立行政法人　日本貿易振興機構
ニューヨーク事務所

目次

我が国が先進国に数えられるようになって以来、営業秘密は、経済社会で活動を行っている個人、法人の重要な資産であり続けている。高機能の製品やサービスを生み出すためには、これからも、あるいは、これまで以上に、営業秘密の創出、管理、及び、保護が欠かせないことは、疑問の余地がない。

医薬品、無人乗用車、無線通信、AI 関連発明など、競争の激しい産業分野では、技術の安定で確実な製品化、そのスピードが勝敗を決することが多い。従って、これらの分野で事業を行う者には、特に、営業秘密の管理が企業の存続と発展に不可欠となってきている。こうした状況は、Innovator 企業の営業秘密をターゲットとする、国際産業スパイによる盗取、詐取事件の報道や、技術開発部門担当者や営業部社員からライバル企業への漏洩事件の発覚が増えるにつれて、適切な対応が急がれる事項の一つとなり、深刻な問題として認識されるようになってきた。

また、センサーの高性能化、情報通信の加速化、ネットワークの万能化は、ありとあらゆる事象を、データとして捉えることを可能にし、営業秘密は、数、価値ともに増えていくものと考えられる。これに加え、巨大な情報のクラウド保存により、厳密な情報管理は、費用的に困難なこともわかっており、営業秘密の保護に、これまでにない挑戦を与えている。さらに、新型コロナウィルスの世界的拡大とそれに伴うリモートワークの普及により企業外部での就業機会が世界的に拡大する中で、サイバー攻撃は大幅に増え、企業の技術的弱点につけこむ手口も巧妙化しつつある。

他方で、巨大データの蓄積、技術標準化等を通じて、限られた企業が複数のマーケットで支配的地位を獲得している状況は問題視されている。更に、構造的不況の持続、及び、必要とされる技術力の変化から、雇用の不安定化や被用者の雇用を求める権利保護が課題となっている。営業秘密の適切かつ実効的に保護するための仕組みの確立と、技術情報や雇用機会への平等なアクセス、透明性の確保も無視できないと考えられる。

以上のような状況は、諸外国でも同様にみられている。米国では、州レベルでは、1971 年に発表された「統一営業秘密法」あるいは（及び）「不法行為法リステートメント」に基づき、保護が付与されていたところであるが、連邦レベルでも、1996 年施行された「産業スパイ法」、さらに、2016 年に制定された「営業秘密保護法」を活用して、営業秘密の保護が可能となっている。共和党のトランプ前大統領は、中国政府、中国企業による知的財産権や国家機密の不正取得を厳しく摘発し、訴追を行っているが、その傾向は、民主党に政権が移行しても継続している。

ヨーロッパ全域での営業秘密保護の主要な歩みとして、ヨーロッパ連合で、2017 年に、各

加盟国での制度整備を求める「営業秘密指令」が成立した。これを受け、各国で法改正がなされ、上記の問題に対応すべき措置も幾つか明文で講じられた。英国は、EU を脱退したが、脱退前に、前述の指令に基づいた営業秘密法が誕生しており、従前のコモンローに基づく保護が補強された。

こうした状況を踏まえ、本事業では、米国、英国、EU、及びドイツにおける、営業秘密保護の実態や動向を調査し、立法、司法制度の状況を調査し、米国、英国、EU、及びドイツにおける、情報管理体制を整備する方法、規程や契約、具体的な管理体制・枠組み(営業秘密の保護)のあり方を検討するためのマニュアルを作成した。

本マニュアルが、米国、英国、EU、及びドイツで事業を行う日系企業の営業秘密保護のために、何らか役立つものとなれば幸いである。

米国

第 1 章　営業秘密の定義

米国は、英国と同様にコモンローの国であるところ、営業秘密の保護は、民事法体系では、判例法に基づく不法行為法、不正競争防止法が主に関連しており、長年にわたり発達してきた[1]。1979 年に、統一法委員会（ULC）がモデルの営業秘密法（UTSA）を作成し、現在までに、ニューヨーク州を除く全州が UTSA を採用し、営業秘密保護法を立法化して保護を与えている[2]。

また、米国刑事法では、州レベルで、長年に亘って窃盗罪等（対象となる無体物に含める、あるいは営業秘密を条文に明記する）として処罰されてきたところ、UTSA 作成後に、UTSA に沿った内容に改正されるなどされている。さらに、1996 年の連邦経済スパイ法により、営業秘密侵害を連邦法上の重犯罪として扱うことができるようになった。

さらに、2016 年、連邦法として営業秘密保護法（DTSA）が制定されて以降、営業秘密保有者は、営業秘密侵害の事実に関して、州の裁判所だけでなく、連邦裁判所においても、民事上の法的救済を求められるようになった[3]。DTSA は、連邦裁判所での救済の付与以外にも、(1)営業秘密法の統一、(2)外国人、外国法人による営業秘密侵害に対する救済の実効化、(3)一方的証拠品押収手続(ex parte seizure)による立証方法の容易化を目指していた。DTSA のこれらの立法目的のうち、連邦裁判所へのアクセスを与えるという目的、(2)外国人、外国法人による侵害への救済付与との目的は、同法施行により実現されているとされるが、(1)営業秘密法の統一、(3)一方的証拠品押収手続の点については、実現あるいは利用が進んでいないとの見方が強い[4]。

1　判例法/UTSA/DTSA による定義

(1)　判例法による定義

---

[1] 契約上の義務不履行を除く請求、即ち、不法行為、不当利得、守秘義務違背、営業秘密の窃取といった契約に基づかない請求は、営業秘密侵害に関するコモンローの判例法が適用になるとされる。Restatement (First) of Torts, § 757, cmt. b (1939)、Restatement (Third) of Unfair Competition, §§ 39, 40 cmt. a (1995), Penalty Kick Management Ltd. v, Coca Cola Co. 318 F.3d 1284 (2003).

[2] 営業秘密、法律情報所 (最終アクセス日 2022 年 2 月 18 日), https://www.law.cornell.edu/wex/trade_secret.

[3] 法律情報所、脚注 2

[4] Mark Klapow, et al. How 5-Year-Old Trade Secrets Act Has Met Its Goals, Law360 (2021).

従前の判例に基づく定義によると、情報のうち、下記の要素を考慮して、営業秘密として認めるべきものを言うと判断されており、実体が掴みづらい定義となっていた[5]。

a. 保有者の事業以外で、情報が知られている程度
b. 事業に携わる従業員や、その他の人々に、どの程度知られているか
c. 情報の秘密を守るために、保有者が講じた措置の程度
d. 保有者の事業と、その競合他社にとっての、情報の価値
e. 情報を開発するために企業が費やした労力又は金銭の量
f. 情報が、他者によって、適切に取得、若しくは、複製される可能性の容易さ、又は、困難さ

(2) UTSA による定義

UTSA は、下記のように営業秘密を定義しており、TRIPS 協定第 39 条第 2 項の開示されていない情報（営業秘密）の定義と合致したものとなっている[6]。

> 製法（方式）、パターン、集積、プログラム、装置、方法、技術、又はプロセスを含む、次のような情報。
>
> a. その開示、又は、使用から、経済的価値を得られる他者により、一般的に知られていない、かつ、適法な手段によって容易に確認できないことから、実際の、又は、潜在的な、独立した経済的価値を導き出す
> b. その秘密性を維持するため、当該状況下で、合理的な努力の対象となっている

(3) DTSA による定義

DTSA は、営業秘密を、下記のように定義する[7]。

> 秘密性を維持するために合理的な措置が取られていた情報で、その開示、又は、使用から経済的価値を得られる他者に一般に知られておらず、かつ、適法な手段により容易に知ることができないことから、独立した経済的価値を導き出すもの

この定義は、UTSA の定義とほぼ同様であり、UTSA を採用した州法の営業秘密の定義と概ね同様であると理解されている[8]。

---

[5] Restatement (First) of Torts、脚注 1
[6] 1985 年の改変を含んだ統一営業秘密法、統一州法委員全国会議（1985）（「UTSA」）https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=e19b2528-e0b1-0054-23c4-8069701a4b62.
[7] 18 U.S.C. § 1839(3).
[8] Klapow、脚注 4 参照。

2　秘密性保護の措置

DTSA における「合理的な秘密性保持の措置」及び UTSA における「秘密性維持のための合理的な努力の対象」に関して、各裁判所の解釈は相当分かれているとの見解が強い[9]。裁判所において、下記のように、営業秘密に対する保護措置が取られていない可能性があると判断する、あるいは示唆することがある。

a. 秘密保持義務を課さずに、顧客あるいは顧客となりうる者に情報をシェアしたこと[10]
b. 従業員に、会社業務専用の携帯、コンピューター等、通信・処理装置を与えていなかったこと（又は、私用の携帯の使用を許可した）[11]
c. 機密情報の定義が限定的で、範囲が狭すぎたこと[12]
d. 秘密保護義務を課す契約前に情報を開示したこと[13]
e. 明示的に「機密情報」と告げる等、指定をしなかったこと[14]
f. 「機密情報」とのラベルの欠如[15]
g. 従業員の秘密保護義務への署名拒否の事実[16]

したがって、裁判所は、次のような事実の有無を重要視することは、明らかである。

i. 情報は、割り当てられた仕事を実行するため、少なくとも潜在的にアクセスを必要とする人にのみ開示されている（「知る必要があるベース」）、
ii. 情報が開示される人は、秘密保持義務に拘束され、情報に関して、この秘密保持義務を負っていることを認識している。

特に、裁判所は、一定の機密性保持の努力に関して（従業員が、会社から貸与されたハードウェアではなく、自分のハードウェアにファイルを保存することを阻止しなかったこと等）、同種の業界で、機密情報の保護に必要な場合に、通常取られている措置がとられていないことは、「合理的な秘密性保護の措置が存在した」事実を否定する、一種の抗弁となる

[9] Joseph W. Hammell, Protection of Employers' Trade Secrets and Confidential Information, Practical Law Practice Note 5-501-1473 (Westlaw 2021)
[10] Yellowfin Yachts, Inc. v. Barker Boatworks, LLC, 898 F.3d 1279, 1299-1301 (11th Cir. 2018)、Madison Oslin v. Interstate Res., No. MJG-12-3041, 2015 U.S. Dist. LEXIS 37587 (D. Md. Mar. 25, 2015)、Prostar Wireless Group v. Domino's Pizza, 360 F. Supp. 3d 994 (N.D. Cal. 2018)
[11] Encompass Services, PLLC v. Maser Consulting, P.A. and Hilsman, 2019 NCBC 66 (J. McGuire).
[12] 機密情報として、ソフトウェアのソースコード、その構造、アルゴリズムとのみ指定していた。Broker Genius v. Zalta, 280 F. Supp. 3d 495 (S.D.N.Y. 2017)
[13] Smart & Assocs. v. Indep. Liquor (NZ) Ltd., 226 F. Supp. 3d 828 (W.D. Ky. 2016)
[14] Big Vision Private v. E.I. Dupont De Nemours & Co., 1 F. Supp. 3d 224 (S.D.N.Y. 2014)
[15] Yellowfin Yachts, Inc. v. Barker Boatworks, LLC, 898 F.3d 1279, 1299-1301 (11th Cir. 2018)
[16] Yellowfin Yachts, Inc. v. Barker Boatworks, LLC, 898 F.3d 1279, 1299-1301 (11th Cir. 2018)

と考えているようにも解釈できる。

3　州法の定義の DTSA による影響

州法による営業秘密の定義は若干差異があるため、ある州で営業秘密として認められたとしても、別の州が反対の結論に達する可能性があり、こうした状況は DTSA 制定によっても変わっていないと理解されている[17]。

ただし、以下のような情報は、大体の州で、営業秘密として保護されている。

- マーケティング計画
- 商業図面
- 食品等のレシピ
- 販売データ
- 製造プロセス
- 化学式
- 顧客に関する、詳細情報。

後述の第 4 章「営業秘密事件の実務」で、DTSA 制定後、DTSA の営業秘密の定義等についての裁判例を紹介し、むしろ、州法の定義が DTSA に影響を与えるという、本来の立法目的と逆の現象が見られていることに言及する。

第 2 章　営業秘密侵害行為の定義

1　判例法における営業秘密侵害行為

従来より、コモンローの下で、請求の基礎として営業秘密の侵害行為、すなわち、不正な使用・開示、又は違法な取得がされたことが、必要であった[18]。具体的に、違法な取得、又は、不正な使用・開示を構成する行為は、不正な方法でなされるか、若しくは、守秘義務に違背してなされる場合とされてきた[19]。

(1)　UTSA（州法）による営業秘密侵害行為

UTSA において、つまり殆どの州では、下記の行為が違法な侵害行為とされている[20]。

---

[17] Farmers' Edge Inc. v. Farmobile, LLC, 970 F.3d 1027, 1033 (8th Cir. 2020)
[18] 法律情報所、脚注 2
[19] Restatement (First) of Torts, § 757(1939)、Restatement (Third) of Unfair Competition, § 39 (1995)
[20] UTSA 第 1 条 オハイオ州の営業秘密法は、UTSA をほぼそのまま制定法化したものである。Allied Erecting & Dismantling Co. v. Genesis Equip. & Mfg., Inc., 649 F. Supp. 2d 702, 711–12 (N.D. Ohio 2009)

a. 他人の営業秘密が、不正な方法で取得されたことを認識しているか、認識すべきであった者による、当該営業秘密の取得。
b. 以下の者による、明示、若しくは、黙示の同意なき、他人の営業秘密の開示、又は、使用。
   i. 当該営業秘密を不正な方法を用いて取得
   ii. 開示、若しくは、使用のときに、自己の営業秘密に関する知識が、
      a) 営業秘密を不正な方法を用いて取得した者に由来して、又は、その者を介して得られた、
      b) 秘密性を保持すべき、あるいは、使用を制限すべき義務を負うと考えられる状況で得られた、又は、
      c) 救済請求者に、秘密性を保持すべき、あるいは、使用を制限すべき義務を負っていた者に由来して、又は、その者を介して得られた、
      ことを認識していたか、認識すべきであった。
   iii. 重大な状況の変化が生じる前に、得た知識が、他人の営業秘密で、偶然、あるいは、ミスで得られたことを認識していたか、認識すべきであった。

(2) 第三者の行為

判例法、UTSA にならって制定された州法のもとでも、契約関係に立つ者以外の者が、故意もしくは過失により、営業秘密の不正な開示、取得、使用をした場合においても、民事的救済を受けることが可能であった[21]。例えば、不正に取得された営業秘密を使用している製品やサービスを作出、販売、輸出入、市場に提供する者の行為を対象として、民事的救済措置（金銭的損害賠償を含む）を求めることができていた[22]。

例えば、製造委託の注文に際し、他人によって営業秘密侵害との訴えを起こされているにもかかわらず、不正に取得した営業秘密を、受託者たる製造者に対して提供し、営業秘密保有者からのライセンスがある旨、信用性に乏しい説明をしていた場合、受託者が、そのような説明を鵜呑みにするのは、事情を「認識すべきであった」ので、侵害にあたるとされる[23]。

[21] UTSA や各州法の定義では、不正な取得、不正な開示、又は、使用とは、その状況下で、営業秘密が、不正に取得等された事実を知っていたか、知るべきであった場合には、営業秘密の侵害となるとされている。UTSA 第 1 条
[22] Restatement (First) of Torts, § 757(1939)、Restatement (Third) of Unfair Competition, § 39 (1995)、UTSA 第 1 条
[23] Cognis Corp. v. CHEMCENTRAL Corp., 430 F. Supp. 2d 806, 812–13 (N.D. Ill. 2006)

2　DTSA における営業秘密侵害行為

(1)　DTSA の侵害行為の定義[24]

DTSA は、UTSA をほぼ踏襲して、営業秘密侵害行為を次のように定めている。

a. 他人の営業秘密が、不正な方法で取得されたことを認識しているか、認識すべきであった者による、当該営業秘密の取得

b. 以下に該当する、明示、若しくは、黙示の同意の無い、他人の営業秘密の開示、又は、使用:

i. 当該営業秘密を不正な方法を用いて取得

ii. 開示、若しくは、使用のときに、自己の知識が、

a) 営業秘密を不正な方法を用いて取得した者に由来して、又は、その者を介して得られた、

b) 秘密性を保持すべき、あるいは、使用を制限すべき義務を負うと考えられる状況で得られた、又は、

c) 救済請求者に、秘密性を保持すべき、あるいは、使用を制限すべき義務を負っていた者に由来して、又は、その者を介して得られた、

ことを認識していたか、認識すべきであった

iii. 重大な状況の変化が生じる前に、得た知識が、他人の営業秘密で、偶然、あるいは、ミスで得られたことを認識していたか、認識すべきであった。

(2)　第三者の行為[25]

DTSA も、UTSA、即ち、判例法と同様、契約関係に立つ者以外の者が、過失により営業秘密の不正な開示、取得、使用をした場合においても、民事的救済を受けることが可能であるとする。例えば、不正に取得された営業秘密を使用している製品やサービスを作出、販売、輸出入、市場に提供する者の行為を対象として、民事的救済措置(金銭的損害賠償を含む)を求めることができる[26]。

3　ミスによる営業秘密の取得

上記の通り、判例法上も、DTSA でも、重大な状況の変化が生じる前に、営業秘密であると

[24] 18 U.S.C. § 1839(5)

[25] UTSA や各州法の定義では、不正な取得、不正な開示、又は、使用とは、その状況下で、営業秘密が、不正に取得等された事実を知っていたか、知るべきであった場合には、営業秘密の侵害となるとされている。

[26] 18 U.S.C. § 1839(5)

認識できた者が（従前から取引していた同業者や内部関係者等）、たまたま情報を受け取ってしまった場合（E メールを誤って送られた場合等）、その情報を勝手に開示したり、使用したりした場合には、営業秘密侵害行為となる[27]。すなわち、営業秘密保有者によるそのようなミスにもかかわらず、「秘密性保持の合理的措置」に欠けると判断されず、営業秘密は保護されたままである。もちろん、そのミスの後の是正措置が秘密性の保護手段として相当であったかが争点となる。

4　主観的要件と救済

UTSA 第 1 条、DTSA 定義規定によると、不正な使用又は開示にあたるのは、行為者が、所定の事情の存在下に[28]、自分が「営業秘密の知識を」得たことを認識していたか、認識すべきであった場合である[29]。これを、文言通りに解釈すると、所定の事情について、故意あるいは過失を有していたことが必要で、かつ、「営業秘密」についての知識（ないしは認識）が、必要であるかのようにも読める。しかし、裁判例は、これを広義に解し、営業秘密の具体的内容を直接に知っていないような第三者にも、自分の情報元が、当該情報について守秘義務を負っているような状況、あるいは、侵害にあたりうる行為により取得したことを、知っているか、知るべきであった事実があれば、「営業秘密の知識を」得たと認定している[30]。

その他、主観的要件が救済内容に影響を与えることは、後述のとおりである[31]。

5　除外規定

(1)　判例法

判例法では、以下の場合には、「不正」取得、開示、使用にはあたらないと解されてきた[32]。

- 保有者と独立して営業秘密を取得した場合
- 既に適正に知られていた情報・物件を、リバースエンジニアリングして取得し

[27] UTSA 第 1 条、18 U.S.C. § 1839(5).
[28] 所定の事情とは、UTSA では、(i)営業秘密を不正な方法を用いて取得した者に由来して、又は、その者を介して、(ii)秘密性保持、あるいは、使用制限の義務を負う状況において、又は、(iii)救済を求める者に、秘密性保持、あるいは、使用制限義務を負っていた者に由来して、又は、その者を介して、
[29] UTSA 第 2 条、18 U.S.C. § 1839(5)
[30] Penalty Kick Mgmt. Ltd. v. Coca Cola Co., 318 F.3d 1284, 1292 (11th Cir. 2003) (applying Georgia law); Cognis Corp. v. ChemCentral Corp., 430 F. Supp. 2d 806, 812 (N.D. Ill. 2006); PMC, Inc. v. Kadisha, 93 Cal. Rptr. 2d 663, 673 (Cal. Ct. App. 2000)
[31] 下記「差止命令」「損害賠償」を参照
[32] Restatement of Torts, Section 757, Comment (f)

た場合

- 保有者から、それを許可するライセンスを受けている場合[33]
- 公に使用、又は、公衆に供覧されている営業秘密を観察して取得した場合

(2) DTSA

①適正な行為の除外

DTSA は、判例法と同様に、営業秘密の取得、使用又は開示行為が「不正」ではない場合として、以下を規定している[34]。特に、

- 保有者と独立して営業秘密を取得した場合
- 既に適正に知られていた情報・物件を、リバースエンジニアリングして取得した場合
- その他の適正な取得

②公益目的の除外

さらに、DTSA は、下記の行為は同法により禁止されず、また、同法による民事救済の付与から除外されると規定する[35]。

1) 連邦政府、州政府又はその下部機関により、合法的になされた場合
2) 連邦政府、州政府、地方公共団体、又は弁護士に対して、違法行為を通告する、あるいは、捜査する目的だけのために開示され、開示が封印の下にされている場合
3) 雇用主による報復行為を裁判で訴えている従業員が、弁護士に対して開示、あるいは、裁判所手続で使用した場合

なお、上記 2）及び 3）は、州法に基づく営業秘密侵害の訴えにおいても、侵害にはあたらない理由として主張できるとする。

③雇用主の通知義務

雇用主は、従業員に秘密保持義務あるいは守秘義務を負わせるような契約を締結させたり、合意させたりする場合には、上記の 3）の免責規定を従業員に通知しなければならない。この通知を怠ると、懲罰的賠償や弁護士費用を請求することや補償を受け

[33] 注意として、ライセンスには、明示のライセンスの他に、黙示のライセンスが存在することであり、これらについては、州法の規律するところによる。
[34] 18 U.S.C. § 1839(6)
[35] 18 U.S.C. § 1833(b)

ることができない。

6　恒久的差止命令等の救済措置における利益調整

UTSA の第 2 条は、営業秘密の侵害が現に行われているか又は差し迫っていると考えられる場合に、差止命令が発せられると規定する[36]。相手方は、営業秘密が存在しなくなったという事情があれば、命令の取り消しを求めることができる[37]。

また、同条(b)は、例外的な場合、差止命令に代えて、合理的なロイヤルティの支払いを命じることができるとする。例えば、取得の際には、営業秘密であることや、営業秘密の不正な取得について善意で、認識を欠いていたのに、後に事情を知るに至った場合、その者の使用をすべて禁止するのは、不測の損失を招いてしまい、公平と言い難い。そこで、営業秘密取得時に善意の者に対して、差止命令を発令しないという判断をしうるとしている[38]。

DTSA は、営業秘密の侵害が現に行われているか、又は、差し迫っていると考えられる場合に、妥当と考えられる内容の、侵害を禁止する差止命令が発せられる、と規定する[39]。相手方が労働者である場合には、雇用の機会を奪う結果となる差止命令は発令できず、営業秘密を侵害する蓋然性、予想される侵害行為等を勘案して、必要かつ合理的な内容の命令でなければならない。他方で、営業秘密保護のための積極的な措置も命ずることができる。

また、衡平の観点から、例外的な場合に、差止命令に代えて、保護が妥当な期間について、合理的なロイヤルティの支払いを命じることができるとする[40]。

7　損害賠償における利益調整

UTSA では、営業秘密取得前の侵害者の立場の変化などを考慮して、衡平に反するという事情の無い限り、営業秘密保有者は、侵害者に対して損害賠償を請求できるとする。

その範囲は、侵害により実際に受けた損失の額、及び、同額に反映されていない侵害者が不当に享受した利益である[41]。損害の額は、合理的なロイヤルティの額により算定することもできる[42]。なお、意図的な、又は、悪意の侵害者に対しては、こうして決せられた損害額の 2 倍を超えない額を懲罰的損害賠償として課しうる[43]。

---

[36] UTSA 第 2 条
[37] UTSA 第 2 条（しかし、侵害者が侵害により利益を受ける Lead time の間は、継続させる）
[38] UTSA 第 2 条 cmt.
[39] 18 U.S.C. § 1836(b)(3)(A)
[40] 18 U.S.C. § 1836(b)(3)(A)
[41] UTSA 第 3 条
[42] UTSA 第 3 条(a)
[43] UTSA 第 3 条(b)

DTSA でも、営業秘密保有者は、侵害者に対して損害賠償を請求でき、その範囲は、侵害により実際に受けた損失の額、及び、同額に反映されていない、侵害者が不当に享受した利益である[44]。損害の額は、合理的なロイヤルティの額により算定することもできる[45]。また、意図的な、又は、悪意の営業秘密侵害者に対しては、こうして決せられた損害額の 2 倍を超えない額を懲罰的損害賠償として課しうる[46]。

加えて、営業秘密侵害の訴えを誤用・悪用した者、差止命令に対して不当に取消申立てをした者、及び、意図的又は悪意で営業秘密を侵害した者には、弁護士費用を負担させうる[47]。

8　時効

UTSA も DTSA も、営業秘密保有者の請求の時効は、3 年間である[48]。

第 3 章　営業秘密侵害に関連する法律、規制の概要(判例法/UTSA/DTSA 以外)

1　1930 年関税法[49]

(1)　規定対象

関税法には、米国知的財産権の保護や公正な競争確保を目的とする規定として、米国へ輸入される物品については、物品の米国内への輸入、又は、その販売に、不公正な競争方法及び不公正な行為が存在しており、それが米国市場に影響を与える、又は、与える恐れがある場合に、国際貿易委員会（ITC）が調査、決定のプロセスを得て、適当な措置を取ることができると定められている。

従って、営業秘密侵害品が輸入されている旨、又は、輸入が予定されている旨の訴えがあり、そのような事実が認められれば、ITC による行政措置の発動が行われ、ひいては、税関により、侵害品の押収が行われることになる。

(2)　捜査と裁判

ITC は、行政府の一部でありつつも、独立した準司法的機関でもあり、行政法判事（ALJ）による審判手続が行われている[50]。調査の申請あるいは職権により調査開始決定がなされ、通知が公告された後、12 か月から 15 か月以内に手続を完結するのが基本である

---

[44] 18 U.S.C. § 1836(b)(3)
[45] 18 U.S.C. § 1836(b)(3)(B)
[46] 18 U.S.C. § 1836(b)(3)(C)
[47] 18 U.S.C. § 1836(b)(3)(D)
[48] UTSA 第 6 条、18 U.S.C. § 1836(d)
[49] Tariff Act §337(a)(1)(A), 19 U.S.C.A. §1337(a)(1)
[50] 第 337 条、米国国際貿易委員会 (最終アクセス日 2022 年 2 月 18 日)
https://www.usitc.gov/intellectual_property/about_section_337.htm.

[51]。主張（争点）の整理、証拠開示手続は、裁判所で実施されているものと比べると、ずっと迅速に行われる。調査対象となる当事者にとっては、証拠開示がより広範囲にわたりうるため、対応だけでも大変な費用と労力を要するものであり、営業にも支障が生じる。

ITC は、関税法違反行為として調査を行い、違反行為を認める場合には、物品の輸入に対して次のような措置を取ることができる[52]。

- 物品の輸入の排除
- 暫定的な物品の輸入の排除
- 違反行為の停止
- 手続と証拠開示の濫用に対する制裁
- 物品の押収と没収

2　連邦経済スパイ法[53]

1996 年に制定された連邦経済スパイ法は、海外の政府や機関を利する、営業秘密の取得、開示、使用する行為を連邦犯罪とし、違反行為に対する懲役、罰金の法定刑を規定する。連邦政府の刑事訴追の根拠となり、また、司法省が、違反行為の差止命令を、民事事件として求めることもできることも規定されている。

(1)　スパイ目的の営業秘密侵害[54]

a. 犯罪が外国政府、外国の機関又は外国の代理人に利益をもたらすことを意図して、あるいは、それを知る者が、故意に

i. 盗む、若しくは、許可なく、流用する、取得する、持ち去る、あるいは、隠す、又は、偽り、欺き、又は、欺瞞によって、営業秘密を取得する

ii. 許可なく、営業秘密のコピー、複製、スケッチ、描画、撮影、ダウンロード、アップロード、変更、破棄、複写、模造、送信、配信、送付、郵送、通信、又は伝達する

iii. 営業秘密を、それが、盗まれ、若しくは、許可なく流用、取得、あるいは、変換されたことを知って、受取り、購入、所持する。

iv. 上記第（a）項から（c）項のいずれかに記載されている違反を犯そうとす

[51] 第 337 条調査の質問と回答、米国国際貿易委員会 (最終アクセス日 2022 年 2 月 18 日) https://www.usitc.gov/intellectual_property/documents/337_faqs.pdf.
[52] 米国内において、下記危害やその恐れが起こることが必要である。（i）米国の産業を破壊、又は、実質的に損なうこと、（ii）そのような産業の確立を防げる、（iii）米国の貿易、および、商取引を制限、又は、独占する
[53] 18 U.S.C. §§ 1831,1832
[54] 18 U.S.C. § 1831

る

v. 上記第（a）項から（c）項のいずれかに記載されている罪を犯すために、1 人以上の他者と共謀し、その 1 人以上が、共謀の目的を達成するために、行為を行う場合には、次項（b）の場合を除き、500 万ドル以下の罰金、15 年以下の懲役、又は、その両方を科す。

b. 第 1 項(上記の a）に違反した組織には、1,000 万ドル、又は、営業秘密の研究、デザイン、その他必要となる費用の回避分を含む、盗まれた営業秘密の価値の 3 倍を超えない額のいずれか高い金額で罰金を科す。

(2) 非スパイ目的（産業スパイ）の営業秘密侵害[55]

a. 営業秘密を領得する目的で、州間取引若しくは外国取引で使用される、又は、使用予定である、製品、若しくは、サービスに関連して、その所有者以外の者の経済的利益に、営業秘密の所有者に不利益を与えることを、意図し、あるいは、知りながら、故意に、前条の行為を犯す場合に、罰金、10 年以下の懲役、又は、その両方を科す。

b. 第 1 項(上記の a)に違反した組織には、500 万ドル、又は、営業秘密の研究、デザイン、その他必要となる費用の回避分を含む、盗まれた営業秘密の価値の 3 倍を超えない額のいずれか高い金額で罰金を科す。

(3) 没収規定

連邦経済スパイ法は、侵害品の没収、破壊、被害者への返還ができることを規定する[56]。

(4) 時効

連邦経済スパイ法違反の時効は、5 年間とされている[57]。

(5) 州刑事法との関係

連邦経済スパイ法は、州間の取引、国際取引に関わる製品やサービスに適用される[58]。この条件自体は充たされることは少なくないと考えられる（営業秘密の侵害に関係する製品やサービスが一つの州だけにとどまっているのは少ない）が、連邦経済スパイ法の処罰の対象は上述のとおり、故意による所定の営業秘密の取得、開示、及び、使用に限られている。

[55] 18 U.S.C. § 1832
[56] 18 U.S.C. § 1834
[57] 18 U.S.C. § 3282
[58] 18 U.S.C. §§ 1831, 1832

3　州刑事法

営業秘密侵害を刑事犯罪として処罰する州は少なくはない[59]。そして、懲役刑や罰金刑が法定刑として規定され、実際に刑事処罰が行われた歴史を有している。以下詳しく述べる。

(1)　営業秘密の定義

州法の営業秘密の定義は統一されていないが、カリフォルニア州を含め、かなりの州は、ニュージャージー州の定義と類似した定義を採用している[60]。他方、近年になって営業秘密侵害を犯罪化した州では、UTSA に沿った定義を採用している[61]。ニュージャージー州の定義は、科学的情報、又は、技術的な情報を保護対象とするが、顧客情報や財務情報は含まないと考えられており、UTSA より狭くなっている。

(2)　侵害行為

侵害行為としては、殆どの州で、窃盗罪の構成要件とほぼ同じ行為を犯罪とする。特に、主観的要件として、営業秘密保有者から、その財物を奪取する意図を要求するものが殆どである。

(3)　重罪化

幾つかの州で、軽犯罪ではなく、重罪（通常の刑事犯罪）となるために、取得された営業秘密の価値が、一定額以上であることを必要とする。例えば、アラスカ州、アイオワ州、ノースダコタ州、オレゴン州、サウスダコタ州では、通常の刑事事件として立件されるためには、営業秘密の価値が 1,000 ドル以上であることが証明されなければならない[62]。

(4)　法定刑

州により、最高の懲役や罰金の多寡は違っている。厳罰化が見られるミズーリ州では、最高 15 年の懲役、5,000 ドル、又は、侵害者の利益の 2 倍までの罰金を課しうるとされ、デラウェア州では、最高 25 年の懲役、妥当な場合には罰金、それに被害者への犯罪収益の返還を命じうる[63]。

---

[59] 50 年を超える歴史を有する州もある。Kurt M. Saunders & Michelle Evans, A Review of State Criminal Trade Secret Theft Statutes, 21 UCLA J.L. & Tech. 1, 2−3 (2017)
[60] 多くは、次のように定義する。秘密であることで価値のある、科学的又は技術的な情報、設計、プロセス、手順、公式又は改善。そして、限られた目的のためにアクセスできる、指定された人以外の人が利用できるようになることを防止する措置を、所有者が講じる場合、営業秘密は、秘密であると推定される。Saunders & Evans,7−8
[61] Saunders & Evans,7−8
[62] Saunders & Evans,7−8
[63] Saunders & Evans,7−8

4 秘密保持条項違反

(1) 一般原則

労働契約などで、侵害者が秘密保持義務を負うとの合意が存在し、契約上の義務違反として、営業秘密又は機密情報保持義務違反を訴える場合、各州の判例法によらなければならない。

各州の裁判例は、企業間での秘密保持条項と労働者との秘密保持条項とで、異なったアプローチを取る。前者では、契約条項をなるべく忠実に解釈するのに対して、後者では、従業員であった者の自由な市場参加への拘束が、非合理な市場取引の制限にあたらないか精査される[64]。具体的には、退職した労働者が機密情報や営業秘密を使用することを制限する条項に、「合理性」があることを必要とする[65]。

事案により異なるものの、条項があまりに広すぎる場合には、(1)秘密保持義務が課されるのは、営業秘密に該当するような、機密性の高い情報にのみであるとして、問題の情報は、秘密保持義務の範囲外であったとしたり、(2)差止命令を狭い範囲でのみ発令する、という措置をとる[66]。あるいは、(3)秘密保持条項は、不公正な取引にあたるとして、法的拘束力を否定することもある[67]。したがって、広い情報を「機密情報」としてカバーしうる定義を設けることは、保有者にとって重要であるが[68]、あまりに無制限に含めるのは逆効果である。

(2) 必然的開示の原則

ペンシルバニア州、イリノイ州、アイオワ州、ニューハンプシャー州など、幾つかの州で、前雇用主の重要な機密情報に接することのできた従業員が、競合相手の営業上重要な地位に転職してしまうことを、「営業秘密を必然的に開示してしまう」と推定し、禁止することを認めている[69]。個別の事案によるが、元従業員の労働の自由を制限する可能性はあり、州が判例を変更する内容の労働者保護法を定めることがある[70]。

(3) 差止命令による救済

元従業員等、秘密保持義務を負う者が、営業秘密を開示あるいは使用してしまう可能性が

---

[64] North Pacific Lbr. Co. v. Moore, 275 Or. 359 (1976)、Ticor Title Ins. Co. v. Cohen, 173 F.3d 63 (2d Cir. 1999)
[65] BDO Seidman v. Hirshberg, 93 N.Y.2d 382 (1999); Eldridge v. Johnston, 195 Or. 379 (1952)
[66] 雇用後も、営業秘密に対する秘密保持義務を負うが、仕事から得られたスキルや知識は、含まれない。広すぎる条項は、過剰な義務を課す部分を、無効化して解釈されることがある。BDO Seidman v. Hirshberg, 93 N.Y.2d 382 (1999)
[67] Geloff v. R.C. Hemm's Glass Shops, Inc., 167 N.E.3d 1095 (Ohio Ct. App. 2021)
[68] Synthes, Inc. v. Emerhe Med. Inc., 25 F. Supp. 3d 617 (E.D. Pa. 2014)
[69] PepsiCo, Inc. v. Redmond, 54 F.3d 1262 (7th Cir. 1995)
[70] マサチューセッツ、イリノイ州など。

ある場合には、差止命令が発令されうるが、裁判所は、営業秘密侵害事件に比較して、その妥当性や範囲につき、慎重に判断する傾向がある[71]。

(4) 競業避止義務違反

秘密保持義務と同様、あまりに広い内容の競業避止義務は「合理性」を欠くため、全部又は一部が無効となる。その他にも、判例により形成されてきた法理あるいは原則が存在し（競業避止義務を課すべき必要性や合理性がないとする事情がある）、一定の場合に、条項が無効とされることがある[72]。

5 通信関連機器に関する刑事法

(1) コンピューター犯罪取締法（1986）

類型と法定刑		
犯罪となる行為	法定刑	コメント
国家機密を取得する(a)(1)	10年	
不正アクセスし情報を取得する(a)(2)	原則1年、一定の加重事由あれば5年	1030(a)(2)(C)は、意図的に、権限なく、あるいは権限を超えて、保護されたコンピューターにアクセスし、保護されたコンピューターから、情報を取得した場合、州間又は外国の通信が含まれる場合は、違反する。
政府コンピューターへの侵入(a)(3)	1年	
詐欺又は利益取得目的でのアクセス(a)(4)	5年	コンピューターの使用自体は詐取あるいは利益取得に含まれず、利益取得が1年に5,000ドルを超えない場合には、該当しない。なお、詐欺の目的は、不法領得のみならず、不誠実を示す主観的要素で足りるとする裁判例がある。[73]
情報送信を故意に行うことで、保護されたコンピューターへ意図的に危害を与える(a)(5)(A)	1年か10年	送信するのは、プログラム、情報、コードなど。営業秘密の送信が、コンピューターのデータの整合性の破壊とい

[71] Cabela's LLC v. Highby, 362 F. Supp. 3d 208 (D. Del. 2019), aff'd, 801 F. App'x 48 (3d Cir. 2020)
[72] Rector-Phillips-Morse, Inc. v. Vroman, 253 Ark. 750 (1973)
[73] Shurgard Storage Centers, Inc v. Safeguard Self Storage, Inc 119 F. Supp. 2d 1121 (WD Wash. 2000)

		う損害にあたるとする裁判例もある。[74]
故意に保護されたコンピューターにアクセスし、無謀に((a)(5)(B))又は、過失で危害を与える(同(C))	原則1年、一定の加重事由あれば5年	
パスワードの取引(a)(6)	1年	
コンピューターに関する脅迫 (a)(7)	5年	
上記の未遂や共謀(b)	10年	

米国連邦法として、コンピューター犯罪取締法が制定されており、第三者の管理するコンピューターにアクセス権限が無い、又は、アクセス権限を超えてアクセスすることを禁止する[75]。犯罪として捜査、告訴されることがあるが、民事訴訟を提起し、（1）法の規定する犯罪類型に該当する行為の存在、（2）損害又は損失を被ったことを主張、立証して、損害賠償請求をすることも可能である[76]。なお、「保護された」コンピューターという概念が重要であり、情報自体が営業秘密として保護されていたかどうかは、犯罪の成否に影響しない。

(2)　電信詐欺法・郵便詐欺法[77]

電信機器、ラジオ、テレビ等を用いた組織的な詐欺、及び、郵便を用いた組織的な詐欺は、連邦犯罪として、それぞれ懲役20年、懲役30年の法定刑が規定されている。

6　営業秘密事件の審理と措置

(1)　一時的抑制命令[78]

[74] Shurgard Storage Centers, Inc v. Safeguard Self Storage, Inc 119 F. Supp. 2d 1121 (WD Wash. 2000)
[75] 18 U.S.C. § 1030
[76] 18 U.S.C. § 1030(g)　18 U.S.C. § 1030(a)(5)(B)(i),(ii),(iii),(iv),又は(v)に記載されている要因の1つが、行為に含まれる場合にのみ可能であり、（i）は経済的損害に限定される。
[77] 18 U.S.C. §§ 1341,1343
[78] 連邦民事訴訟規則第65条(b)
カリフォルニア州では、証拠により、以下の要件が充たされれば、営業秘密の侵害に対する一時的抑制命令あるいは暫定的差止命令を発令する。Whyte v. Schlage Lock Co., 101 Cal. App. 4th 1443, 1463–64 (2002); Prime Tech Staffing v. Mickelsen, 2005 WL 775688, *3+ (2005)　ニューヨーク州でも、同等の要件である。N.Y. C.P.L.R. 6301

- 申立人が、本案で勝訴する可能性（これに関して、営業秘密の特定や、合理的な秘密性保持の措置が問われる）
- 命令が認められない場合、申立人に生じる取り返しのつかない損害(侵害が行われる切迫性)
- 上記の2要素のバランスー命令が認められた場合に侵害者に与えると予測される損害に比較して、命令が認められない場合に生じると予測される申立人の損害の超越

営業秘密保有者は、裁判所に対し、一時的抑制命令を申し立てることができ、侵害行為の停止や侵害品等の証拠の保全を命じるように、請求することができる[79]。

一時的抑制命令は、侵害者の関与なく、申立人のみが関与する一方的な手続を経て、発せられることもできる。その場合、申立人は以下を主張・立証する必要がある[80]。

a. 営業秘密侵害の本案で勝訴する相当な蓋然性、
b. 命令が認められない場合、申立人に生じる取り返しのつかない損害
c. 命令が認められた場合に侵害者に与える損害に比較し、命令が認められない場合に生じる申立人の損害が上回ること、
d. 公共の利益

一時的抑制命令は、被申立人に生じうる損害を補償するための保証金を、申立人が提供しなければ発せられない[81]。

また、一時的抑制命令は、最大で 14 日間のみ存続する。被申立人に通知することなく発せられた場合は、被申立人が参加する暫定的差止命令審尋期日を予定しなければならない。

(2) 暫定的差止命令[82]

営業秘密保有者は、裁判所に対し、暫定的差止命令を申し立てることができ、侵害行為の停止や証拠の保全、侵害品等の差押え、物品の中立した第三者による保管を命じるように、請求することができる[83]。

暫定的差止命令は、申立人が被申立人に通知し、被申立人が関与する審尋手続を経て発せられることが原則である。その場合、申立人は、以下を主張・立証する必要がある[84]。

a. 営業秘密侵害の本案で勝訴する相当な可能性、
b. 命令が認められた場合に侵害者に与える損害に比して、命令が認められない場合に生じる申立人の損害が上回ること
c. 命令が認められない場合、申立人に生じる取り返しのつかない損害
d. 公共の利益

---

[79] Schiavo ex rel. Schindler v. Schiavo, 403 F.3d 1223, 1225–26 (11th Cir. 2005).
[80] Schiavo ex rel. Schindler v. Schiavo, 403 F.3d 1223, 1225–26 (11th Cir. 2005).
[81] 連邦民事訴訟規則第 65 条(c)
[82] 連邦民事訴訟規則第 65 条(a)
[83] 連邦民事訴訟規則第 65 条(a)
[84] Beacon Theatres, Inc. v. Westover, 359 U.S. 500, 506–07 (1959)、Winter v. Nat. Res. Def. Council, Inc, 555 U.S. 7 (2008)
ニューヨーク州では、明白で説得力のある証拠により、以下が立証されると、暫定的差止命令を発令する。N.Y. C.P.L.R. 6301;Arthur J. Gallagher & Co. v. Marchese, 946 N.Y.S.2d 243, 244 (2d Dep't 2012).

- 申立人が、本案で勝訴する可能性（これに関して、営業秘密の特定や、合理的な秘密性保持の措置が問われる）
- 命令が認められない場合、申立人に生じる取り返しのつかない損害(侵害が行われる切迫性)
- 衡平の観点から、申立人の利益が被申立人の利益を超越

暫定的差止命令は、被申立人に生じうる損害を補償するための保証金を、申立人が提供しなければ、発せられない[85]。

(3) 本案前証人尋問請求[86]

訴訟を提起する前にも、証拠が逸失してしまいかねない場合には、証人から証言を得る手続を裁判所に申立て、証言を保全することができる。これは、相手方に通知することを要し、下記を示さなければならない。

- 申立人が訴訟提起を予定しているが、現在それを提起することはできないこと
- 予定される訴訟の本質及びそれに対する申立人の利害
- 証言が示すと予想される事実とその取得を望む理由
- 予想される不利な当事者の名前と住所
- 証言録取される者の名前と住所及び予想される証言内容

(4) 連邦裁判所に対する証拠品、侵害品の差押えの申立て[87]

DTSA において、営業秘密保有者は、連邦裁判所に対して、相手方に対する通知を得ない申立てを行い、相手方の財産を差し押さえる命令を得ることができる。この一方的な差押申立手続は、本案訴訟の証拠を保存するため、又は、営業秘密の伝播又は拡散がされないようにするために利用される。申立人が、以下の事実を証拠で証明した場合に、裁判所は、相手方からの証拠を差押え、移動して保管することができる。

a. 相手方が回避するか、従わない可能性が高いため、一時的抑制命令では不十分である
b. 申立てが認められない場合、即時で回復不可能な損害が、申立人に発生する
c. 申立てを否定することによる申立人への損害は、申立てが認められて、命令を受ける者の正当な利益を上回り、および、命令によって影響を受ける可能性のある第三者への損害を有意に上回る
d. 営業秘密が存在する
e. 相手方が、営業秘密を侵害しているか、若しくは、侵害の恐れがあり、あるいは、これらを企図している
f. 営業秘密と差押対象とされる物を、相手方が所持している
g. 差し押えられる対象とその場所を合理的に特定している
h. 相手方、及び、相手方に加担している者は、申立手続の通知を受けると、対象物を破壊、移動、隠匿するか、さもなければそれに裁判所がアクセスできないようにする
i. 申立人は、要求する差押を公表していない

以上の要件は、一時的抑止命令（同様に、一方的な手続きで発令されうる）に比して、非常に厳格であり、これらを十分に証明することは、多くの場合に難しいと思われる[88]。

[85] 連邦民事訴訟規則第 65 条(c)
[86] 連邦民事訴訟規則第 27 条
[87] 18 U.S.C. § 1836(b)(2)
[88] Klapow, et al. 脚注 4

(5)　訴訟手続における証拠開示、営業秘密の保護

米国では、民事事件の本案が提起され、最初の被告の答弁あるいは訴訟却下の申立てがされた後、証拠開示に関する当事者間のやりとりが始まる[89]。したがって、営業秘密保有者としては、訴状の作成、裁判所への提出の段階では通常、相手方たる私人から、公的な経路で情報を入手することはできない[90]。

証拠開示にあたり、営業秘密保有者は、裁判所の保護命令を求めることができる[91]。保護命令申立てには、営業秘密の保護以外も、保護を求める理由とすることができ、当事者又は個人を、支障、困惑、抑圧、又は、過度の負担、若しくは、費用から保護するため、保護命令が必要とする正当な理由があることを主張し、証明する[92]。裁判所は、以下を命じうる。

a. 開示又は見分を禁止する。
b. 開示又は見分のために、時間と場所又は費用の配分を含む条件を指定する。
c. 開示を求める当事者によって選択された方法以外の方法を指示する。
d. 特定の事項についての調査を禁止又は開示、若しくは、見分の範囲を特定の事項に限定する。
e. 見分が行われている間に、立ち会う可能性のある人物を指定する。
f. 裁判所の命令があった場合にのみ、証言録取書を封印して、開封することを要求する。
g. 営業秘密又はその他の機密の研究、開発、又は商業情報が開示されないこと、又は特定の方法でのみ開示されることを要求する。
h. 裁判所の指示に従って開封するために、当事者が指定された文書又は情報を、封印された封筒で同時に提出することを要求する。

保護命令が発せられると、保有者は、自己の主張・立証にあたり、保護命令が指定する、営業秘密や機密情報の開示の方法、アクセス制限に従って、関連する書面やデータに、営業秘密、又は機密情報が含まれていないか確認し、もし含まれていれば、その旨を特定、説明等することとなる。

争いが生じれば、裁判所は、イン・カメラ手続（公衆の傍聴できる公開廷でなく、当事者と裁判官のみで、秘密性を判断する手続）を用いて、実際の証拠等に機密情報等が存在するかを判断することもできる[93]。

---

[89] 連邦裁判所の事件の場合、連邦民事訴訟規則第 26 条
[90] 相手方に原告の代理人が非公式に接触することもあるが、営業秘密侵害事件での、このような交渉の行われる割合は、不明である。
[91] 連邦民事訴訟規則第 26 条　実務では、各裁判所及び裁判官が、定形の規則として、保護命令に等しい内容を含む命令を予め作成して、当事者に適用しているのが通常である。
[92] 連邦民事訴訟規則第 26 条
[93] UTSA 第 5 条

DTSA はこうした判例法の用意する秘密保護のシステムに加え、裁判所が、積極的に営業秘密保有者が営業秘密と主張する情報を、十分に保護する措置を採用しなければならないと規定する[94]。

(6) 恒久的差止命令

① 判例法[95]

UTSA が規定するように、営業秘密が侵害されている、又は、侵害の恐れがあると認められる場合、裁判所は、恒久的差止命令を命じることができる[96]。そして、例外的な状況があれば、差止めの認められ得る期間を超えない期間について、被告による合理的なロイヤルティの支払いを命じることもできる[97]。

判例法上、原告が本案（主な手続き）の請求を基礎づける事実の立証に成功すれば、*eBay* 判決の示した要件に基づき、営業秘密保有者たる原告への救済手段として、以下を命じることができる[98]。

a. 営業秘密の開示、利用の禁止、
b. 営業秘密を含む、若しくは、具体化する、侵害者が所持、若しくは、所有する文書、物件、材料、物質、又は電子ファイルの破壊、又は所有者への返還
c. 侵害品のリコール、破壊、流通経路からの侵害製品の除去
d. 侵害者の関連業務における営業秘密の混入、使用の防止のために必要なあらゆる措置、必要な場合、特定の従業員の隔離、誓約、監視、検証の措置

② DTSA[99]

DTSA では、以下に記載する要件と制限の下に、民事救済として、恒久的差止命令を命じることができると規定する。

a. 実際の、又は、恐れのある営業秘密侵害を防止するために、裁判所が合理的であるとみなす条件を、下記に従って課す
    i. 被告が、雇用関係に入るのを防ぐことなく、また、雇用に課せられる条件が、被告が知っているとする情報だけでなく、侵害事実を示す証拠に基づいている
    ii. 上記以外の場合は、合法的な職業、取引又はビジネスに対する制約を禁止する、適用州法に反しない

---

[94] 18 U.S.C. § 1835
[95] 上記 3.6「恒久的差止命令等、救済措置における利益調整」を参照
[96] UTSA 第 2 条
[97] UTSA 第 2 条(b)
[98] Marine Turbo Engineering, Ltd. v. Turbocharger Services Worldwide, LLC, No. 11-60621-CIV, 2012 WL 13005811 (S.D. Fla. July 23, 2012)
[99] 18 U.S.C. § 1836(b)(3)(A)

b. 裁判所によって適切と判断された場合、営業秘密を保護するために、積極的な措置を講じることを要求する

ただし、例外的な状況があれば、救済措置の認められ得る期間を超えない期間について、合理的なロイヤルティの支払いを命じることもできることについては、上述したとおりである。

7 損害賠償

(1) 判例法

UTSA では、営業秘密保有者は、侵害者に対して、侵害により実際に受けた損失の額、及び、同額に反映されていない、侵害者が不当に享受した利益を、侵害者に対して請求することができる[100]。損害は、合理的なロイヤルティの額により、算定することもできる[101]。

(2) DTSA

DTSA では、営業秘密保有者は、侵害者に対して、侵害により実際に受けた損失の額、及び、同額に反映されていない、侵害者が不当に享受した利益を、侵害者に対して請求することができる[102]。損害は、合理的なロイヤルティの額により算定することもできる[103]。

第 4 章 営業秘密事件の実務

1 保護される営業秘密

営業秘密の定義に関して、多くの裁判例を鑑みると、DTSA の定義が、UTSA の定義と同様であることを重視して、UTSA を採用して制定された、各州営業秘密法に基づく各州の判例は不変であり、過去の判例を引き継ぐものと理解されている[104]。

営業秘密を具現化した製品が写真で公表されたり、一部の情報は特許として保護されていたりしても、それ自体で営業秘密を消失させるわけではないため、被告としては注意が必要である[105]。

---

[100] UTSA 第 3 条
[101] UTSA 第 3 条(a)
[102] 18 U.S.C. § 1836(b)(2)(C)
[103] 18 U.S.C. § 1836(b)(2)(C)
[104] Midwest Sign & Screen Printing Supply Co. v. Dalpe, 386 F. Supp. 3d 1037, 1053 (D. Minn. 2019);Kuryakyn Holdings, LLC v. Ciro, LLC, 242 F. Supp. 3d 789, 797-98 (W.D. Wisc. 2017); Earthbound Corp. v. MiTek USA, Inc., 2016 WL 4418013, at *10 (W.D. Wash. Aug. 19, 2016)
[105] T-Mobile USA, Inc. v. Huawei Device USA, Inc., 115 F. Supp. 3d 1184, 1193 (W.D. Wash. 2015)

実務上最も問題となるのは、原告が、証拠開示を経ていない訴訟提起段階で、どの程度詳細に被告が侵害したとする営業秘密を特定しなければならないかである。被告が、具体的にどのようにして取得したか、どのように使用しているかについては殆ど分からないが、ある程度、被告がアクセスできた情報について原告で推測がついている場合には、営業秘密を広く定義しても、訴訟が却下されないことが多い[106]。しかし、広範すぎることによって、主張立証の対象が定まらない場合には、請求が却下されてしまう[107]。

侵害の対象である営業秘密の範囲について、ニューヨーク州は、訴状の記載において、被告に対して、何の侵害で訴えられたかを知らせるに足りる十分な特定性を要求し[108]、カリフォルニア州では、合理的な特定性を要求する。このように、表現上の違いはあるが、技術分野によっても、原告と被告の関係によって、裁判所のアプローチは異なっていると考えられ、実務上の差異は明らかではない[109]。

2　営業秘密侵害行為の認定

(1)　違法な「使用」の範囲：原告との契約内容、被告の侵害品

違法な「使用」にあたるかは、もし契約関係が存在する場合には、原告と被告（又は被告関連会社）との契約内容、被告の提供する（予定の）侵害品の性状が、重要な判断要素となる。

テキサス州最高裁は、保有者に不利益となりうる営業秘密の商業的利用である限り、「使用」として、侵害行為を構成すると判示した[110]。これに準じ、第5連邦巡回控訴裁判所も、ライセンス切れとなったコンピューターを解析、使用して、自社の製品を作るという、侵害品の製造行為は、研究・開発上の使用、情報を利用した新規顧客開拓と並んで、違法な「使用」と考えられると判断した[111]。ニューヨーク州の連邦破産裁判所も、契約上の守秘義務、

---

[106] 原告の顧客リスト、顧客の価格設定、過去の販売実績等は十分に特定されているとした判例、Brocade Commc'ns Sys., Inc. v. A10 Networks, Inc., 873 F. Supp. 2d 1192 (N.D. Cal. 2012), on reconsideration in part, No. C 10-3428 PSG, 2012 WL 12925716 (N.D. Cal. July 8, 2012)

[107] 原告が、6頁にわたり、行間なく、内部機密情報の項目を羅列した場合、AMP Inc. v. Fleischhacker, 823 F.2d 1199, 1203 (7th Cir. 1987)に許可したり、数千もの営業秘密のうち、問題となっている情報を大まかに特定した場合、Litton Sys., Inc. v. Sundstrand Corp.,750 F.2d 952, 954, (Fed. Cir. 1984)、原告が54頁に103件の営業秘密を列挙した場合、Struthers Scientific & Int'l Corp. v. General Foods Corp., 51 F.R.D. 149,151-52 (D. Del. 1970) .

[108] PaySys Int'l, Inc. v. Atos Se, No. 14-CV-10105, 2016 WL 7116132 (S.D.N.Y. Dec. 5, 2016)

[109] Cal. Civ. Proc. Code §2019.210

[110] Computer Assocs. Int'l v. Altai, Inc., 918 S.W.2d 453, 455 (Tex.1996)

[111] Gen. Universal Sys., Inc. v. HAL, Inc., 500 F.3d 444, 450–51 (5th Cir. 2007)

秘密保持義務が、不正「使用」に該当するかどうかの判断で、吟味されると判示した[112]。

第 11 連邦巡回控訴裁判所も、「使用」「開示」を広義に解釈して、(i)第三者が営業秘密を知ることを可能にする情報を提供することは、「開示」であり、(ii)営業秘密の「相当な部分」を使用して、営業秘密から「相当に由来した」改善、若しくは、修正を作成する行為は、「使用」であり、他方、営業秘密から「わずかな」貢献のみで、具体化されたとされる物品を製造した場合、使用の責任を負わないと判示した。このように、侵害品の性状と営業秘密の性状・内容の比較をスライディング・スケールで行い、不正な「使用」かどうかを判断する意見が多い。

カリフォルニア州第 6 地区控訴裁判所は、原告が、自己のソフトウェア製品に関する特定の技術情報、Cookie のバッファリング、セッションの維持、セッションの破棄、負荷分散などのソフトウェアに関する技術的に詳細な事項を、被告の質問に回答する形で開示していた場合、被告が自己の事業に密かに応用、改良していた場合には、「使用」に当たるとした[113]。反対に、原告が、機密保持契約下に、健康保険の窓口の事務が一般にどのように機能するのかを説明したり、自己のデータ入力、出力がどうなっているのかを見せたりするだけでは、被告が後に自社製品を開発したとしても、違法な「使用」の内容とはならないと判断した[114]。

(2) DTSA による営業秘密侵害行為の拡大

DTSA に関しての判決は、以下の点で、新法が侵害行為の範囲を広げると考えることもできる。

① 「不正使用を達成させる行為」

DTSA の営業秘密侵害の定義には、営業秘密の不正使用を「達成させる」行為が含まれる。この点について、裁判所は、用語が意味する行為は、犯罪行為の計画が開始されてから、犯罪完了に至るまでの、犯罪が遂行中であることを明らかにする如何なる行為も含めて解釈されるべきと判断した。そこで、被告が、多くの国内展示会で、不

[112] In re Collins, 540 B.R. 54, 63 (Bankr. E.D.N.Y. 2015)

[113] 原告は、機密保持契約に従って、ソフトウェア製品を被告に販売する過程で、ソフトウェアに関する、個別化された、非常に具体的な事実を、被告に開示し、追加の内容を含む、技術バインダーを被告に提供した。原告のソフトウェア製品に関する特定の技術情報として「Cookie のバッファリング」、「セッションの維持」、「セッションの破棄」、「負荷分散」、「その他の事項」などのソフトウェアに関する技術的な質問に回答した。Ajaxo, Inc. v. E*Trade, Inc., 135 Cal.App.4th 21, 37 Cal.Rptr.3d 221,227–229(6th Dist.2006)

[114] Agency Solutions.Com, LLC v. TriZetto Grp., Inc., 819 F. Supp. 2d 1001, 1029–30 (E.D. Cal. 2011)

正取得されたとされる、営業秘密を具体化した製品を宣伝、促進、販売してきた以上、「不正使用」がされたと認定した[115]。しかし、この DTSA の「達成させる」行為には、他者の営業秘密の侵害行為を幇助する行為は含まれていないとする下級審レベルの判決も存在している[116]。

即ち、現在のところ、DTSA に関する裁判例で、侵害行為を広義に解釈する判決が下されてきているものの、具体的な事案の事実関係により判断が分かれると予想され、今後の裁判例の発展を見極める必要がある。

② 不法な使用、開示、取得の行為地

海外法人である被告が、米国法人である原告の営業秘密を、原告の海外子会社の従業員から取得し、米国内のトレードショーで侵害品を展示した事件で、イリノイ州の連邦裁判所は、DTSA が、被告らの行為に適用される根拠として、DTSA の域外適用に関する 1837 条は、RICO 規定と異なり、行為と米国との結合性を要求しておらず、また、DTSA は、不正取得が DTSA の施行前の場合でも適用されるので、不正使用が施行後である以上、不正使用により生じた損害賠償の請求や不当利得の返還を求めることができると判断した。即ち、域外での使用行為についても、損害賠償を可能とすると解釈した[117]。

3 訴訟提起及び証拠収集段階における営業秘密の保護

米国の民事訴訟法は、訴訟提起段階では、厳格な請求の原因の特定を要求しないが、ディスカバリー（証拠開示）が不当に広範にならない程度の「営業秘密」の限定が必要であり、侵害されたと主張する「営業秘密」の内容を次々と変更することは、心証形成に悪影響を与えかねない[118]。ビデオのクラウドに関連する技術を保有していた原告が、ビデオのクラウドのアーキテクチャ及び技術を利益化する手法が営業秘密であったとして、被告を訴えた事件で、個別の要素（コンポーネント）がどう機能するかは示したものの、それが一体としてどのように作動するか等を示せなかった場合に、営業秘密の特定はなかったと判断した裁判例がある[119]。

---

[115] Motorola Sols., Inc. v. Hytera Commc'ns Corp., 436 F. Supp. 3d 1150, 1164–65 (N.D. Ill. 2020)
[116] Power Home Solar, LLC v. Sigora Solar, LLC, No. 3:20-CV-00042, 2021 WL 3856459, at *10 (W.D. Va. Aug. 30, 2021)
[117] Motorola Sols., Inc. v. Hytera Commc'ns Corp., 436 F. Supp. 3d 1150, 1162 (N.D. Ill. 2020)
[118] Next Commc'ns, Inc. v. Viber Media, Inc., 758 F. App'x 46, 49 (2d Cir. 2018)
[119] Next Commc'ns, Inc. v. Viber Media, Inc., 758 F. App'x 46, 49 (2d Cir. 2018)

この裁判例では、被告との間に、機密情報を非常に広く定義する秘密保持契約が存在したが、同契約は、特に営業秘密の存在の立証に有益な要素とはならなかった。

訴状を、機密情報を含めたものを「封印下に」提出することもでき、営業秘密保護のために、多くの事件で利用されているようである[120]。

連邦第6巡回控訴裁判所は、DTSAの規定に基づき、機密性の保護に利用される封印について、封印されて提出された資料が、控訴審で利用される場合でも、封印されたままの状態が維持される旨を判示した。この事件では、従前に特許侵害訴訟を提起し、被告会社と和解した営業秘密保有者が、被告会社と弁護士が和解契約の秘密保持義務に違反して、営業秘密を被告会社の従業員に開示したと主張し、一時的抑制命令を得たが、その後の審理で命令が取り消されたため、控訴したというものである[121](McKeague, J.)。

元従業員が競争会社に転職した後、元従業員と競争会社による営業秘密侵害の疑いを持ち、訴訟提起のための情報を得るために、連邦民事訴訟規則27条（訴訟前の証拠開示）に基づいて、元従業員らから、競争会社の機密情報となっているPortfolioDefenseというソフトの開示を求めようとしたところ、裁判所は、当該情報は、テキサス州証拠法507条で保護される営業秘密にあたるとして、申立てを却下した[122]。即ち、州法レベルでの秘密情報の保護規定で、営業秘密侵害訴訟に関する証拠収集を排除した。

4　救済手段、営業秘密保護の現状

前述のとおり、営業秘密侵害行為の被害者である保有者に認められる救済手段としては、従来より、金銭的賠償、不当利得返還、恒久的差止命令、暫定的差止命令、一時的抑止命令が認められてきた[123]。

(1)　差止命令

営業秘密保持者は、侵害品の破壊、侵害品の引渡し、侵害者からの営業秘密の返還や消去を、差止めで求めなければならない事情を証明できれば、侵害行為を実効的に阻止することができる。

他方で、救済を与えるにあたり、他の法益とのバランスが重要であり、UTSAでも、DTSAでも、侵害者が、当初は、営業秘密の侵害の事実について善意であった場合などは、差止命令に代えて、合理的なロイヤルティの支払いを命じうるとしている。

---

[120] 即ち、秘密部分は、黒塗りされ、一般が閲覧できない。T-Mobile USA, Inc. v. Huawei Device USA, Inc., 115 F. Supp. 3d 1184, 1193 (W.D. Wash. 2015)
[121] Magnesium Machine, LLC v. Terves, LLC, Case No. 20-3779 (6th Cir. Dec. 10, 2020)
[122] In re PrairieSmarts LLC, 421 S.W.3d 296, 307 (Tex. App. 2014)
[123] 前記「営業秘密事件の審理と措置」参照

幾つかの州では、裁判例を踏まえると、営業秘密の侵害の事実が認定された際には、反証は可能であるもの、差止命令の要件である「取り返しのつかない（回復不可能な）損害の発生」という要件を充足すると推定される[124]。例えば、イリノイ州の連邦地裁は、DTSA とイリノイ営業秘密保護法の事件で、反証可能な推定を適用した[125]。オハイオ州や、カリフォルニア州の判決にも、同様のものがみられる[126]。

これに対して、他の多くの州で、反証可能な推定を適用しないとするものが見られる[127]。

(2) 金銭的賠償

米国の不法行為の損害賠償の一般規則に従い、損害賠償は、違反行為と事実的因果関係のある、かつ、相当因果関係のある損害に関してのみ認められる。そして、侵害行為がなければ、原告が有していたであろう元の地位に回復するのに必要な程度で付与される。

実際の事件で、営業秘密の侵害による損害を立証するのは容易ではないことが多い[128]。この相当因果関係の立証の困難性を明確に示した判決が、連邦第 9 巡回控訴裁判所により下された[129]。

原告は、営業秘密の不正使用と不当利得を理由に、元従業員とその新雇用主である被告会社に対して訴訟を起こしたが、地方裁判所は、被告らの申立てに基づき、請求を却下する略式判決を下した。第 9 巡回区控訴裁判所はこれを認容した。

営業秘密の不正使用に基づいた、被告に対する損害賠償の請求について、裁判所は、まず、原告が主張する、営業秘密の不正取得、使用が十分に立証されていないと指摘した。その上で、営業秘密の喪失により、1,600 万ドルを超える価値をもつ営業秘密の損害が原告に生じているので、同額の賠償が発生しているとする専門家の報告書は、被告が侵害した事実を前提としており、採用できないと結論づけた。

---

[124] Brightview Grp., LP v. Teeters, 441 F. Supp. 3d 115, 138 (D. Md. 2020)
[125] Vendavo, Inc. v. Long, 397 F. Supp. 3d 1115, 1143-44 (N.D. Ill. 2019)
[126] Allied Erecting & Dismantling Co. v. Genesis Equip. & Mfg., Inc., No. 4:06CF114, 2010 WL 3370286, at *2 (N.D. Ohio Aug. 26, 2010)
[127] 例えば、DTSA に基づく営業秘密侵害事件で、連邦第 10 巡回控訴裁判所は、DTSA は、差止命令を許可するだけであり、強いるものではないと、結論した。First W. Capital Mgmt. Co. v. Malamed, 874 F.3d 1136, 1142-44 (10th Cir. 2017) 連邦第 3 巡回控訴裁判所も、今後起きる可能性がある開示行為は、差し止められるべき対象だが、既に開示された情報を差し止める必要がないとして、差止命令の付与を否定した。Campbell Soup Co. v. ConAgra, Inc., 977 F.2d 86, 91-93 (3d Cir. 1992)
[128] T-Mobile USA, Inc. v. Huawei Device USA, Inc., 115 F. Supp. 3d 1184, 1193 (W.D. Wash. 2015)
[129] Joshua David Mellberg LLC v. Will, No. 20-16215, 2021 WL 4480840, at *1 (9th Cir. Sept. 30, 2021)

裁判所は、原告の不当利得の請求についても、地方裁判所の判断を是認した。原告が、営業秘密の開発に数百万ドルを費やしたと主張し、財務書類を開示し、証言も提出したが、裁判所は、提出された証言を「一般者の意見」および「一般的な主張」として、判断の参考にしなかった。裁判所は、不当利得の理論に関して、原告が開発費に関する宣誓書を補足として提出したことについて、時期に遅れたものとして排除した。そこで、損害額計算を必要とする、連邦民事訴訟規則 26a(1)(A)(iii)を満たさなかったと認定した。

営業秘密保有者は、損害の立証をする代わりに、侵害者によって得られた利益の引渡し、ライセンスした場合に支払われるべきロイヤルティの支払いを求めることもできるので、合理的ロイヤルティの率が入手可能であれば、資料を提出することができる。

UTSA も DTSA も、懲罰的損害賠償を採用し、侵害行為が故意か過失かによって額を増加させることができる。

DTSA は、裁判所が、営業秘密侵害の訴えを濫用的に起こした原告、差止命令取消しを正当な理由なく求めた被告、意図的で故意に営業秘密を侵害した被告に対し、弁護士費用を負担させうるとしており、原告としても、不合理な請求をすることはできない。

5　内部告発と営業秘密の使用・開示

前記の通り、DTSA は、一定の内部告発行為を、適正な営業秘密の使用であるとして、違法な侵害行為から除外する。この規定に関して、連邦オハイオ州地方裁判所は、正当な公益目的の営業秘密開示を免責する点に着目し、免責規定の適用を緩やかに認めた[130]。

問題となった従業員は、その代理人を通じて、会社の違法行為を告発するために、営業秘密を開示したのであり、(1)情報使用の意図が違法行為の内部告発の目的「だけ」と考えても良いこと、(2)多少、自己の職責を超えて、会社の情報にアクセスしたとしても、その営業秘密へのアクセスだけを、営業秘密の使用から切り離して捉えて、不正であったとすることは、立法の目的、文言に反していることを理由として、従業員の主張を採用した。そこで、従業員の営業秘密開示は、情報のアクセスと一体として捉えられ、免責された。

第 5 章　準拠法・域外適用

1　判例法での準拠法

営業秘密侵害に関して、海外で不正に取得された米国法人の営業秘密の侵害には、特に保

[130] FirstEnergy Corp. v. Pircio,524 F.Supp.3d 732

護法益と関連のある州の判例が適用されてきた。幾つかの州は、侵害行為が行われた地域、又は、被告が侵害行為による利益を受けた地域の法律を適用するとしているため、侵害行為がカリフォルニア州で行われる場合の他にも、侵害行為による利益を受ける地域が米国カリフォルニア州であれば、取得行為や使用行為が国外であっても、カリフォルニア州法が適用となる[131]。

また、多数の州で、原告の本店所在地の法律を適用する[132]。したがって、米国テキサス法人の保有する営業秘密の侵害では、被告の営業秘密の取得行為、又は開示行為が国外でなされても、テキサス法の適用となる。このように記載すると、判例法では、無制限な適用があったかのように思われてしまうが、実際には、「不正な」使用、開示、取得に限定されており、原告あるいは被告に関係が深い州の法を適用した。あるいは、侵害品は、州に持ち込まれて、宣伝や販売の促進に使われていた事実がみられる事件が殆どであった[133]。

2　侵害品の輸入と米国関税法の適用

関税法は連邦法であり、域外適用の問題が生じる[134]。営業秘密侵害品が米国内に輸入されることになると、関税法第 337 条に基づいて、輸入についての不公正な競争手段、又は、不正な行為に対する ITC による調査と決定がなされ得る。その場合、ITC は、営業秘密の不正使用の調査の過程で、国内市場での不公正な競争から生じる不利益から国内産業を保護する必要がある限り、中国でなされる行為にも、調査と検討を加えることができるとされる[135]。

3　DTSA 下の侵害行為と域外適用

イリノイ州の連邦地方裁判所は、被告である海外法人が、第三者により不正に取得された

---

131 カリフォルニア州法の営業秘密について、不正な開示を州内で存在したことを根拠に適用する判例に Meggitt (San Juan Capistrano), Inc. v. Yongzhong, No. SACV130239DOCMLGX, 2013 WL 12120067, at *2 (C.D. Cal. Sept. 26, 2013), *aff'd in part, dismissed in part sub nom*. Meggitt San Juan Capistrano, Inc. v. Yongzhong, 575 F. App'x 801 (9th Cir. 2014)、被告の活動中心の州で、被告が不正な利益を受けることを根拠に、被告拠点地法の適用があると示唆する判例に Mergenthaler Linotype Co. v. Leonard Storch Enterprises, Inc., 66 Ill.App.3d 789, 23 Ill.Dec. 352, 383 N.E.2d 1379, 1389–90 (1978); Goldberg v. Medtronic, Inc., 686 F.2d 1219, 1225 (7th Cir.1982); Smith v. Dravo Corp., 203 F.2d 369, 373 (7th Cir.1953); SIL–FLO, Inc. v. SFHC, Inc., 917 F.2d 1507, 1511–12 (10th Cir.1990).

132 FMC Corp. v. Capital Cities/ABC, Inc., 915 F.2d 300, 302 (7th Cir.1990); Restatement (Second) Conflict of Laws § 145, comment e (1971).

133 原告と、（被告や、被告に営業秘密を漏洩した者が）積極的に契約関係に入っていたことが原因となっている場合など、州と接点がないとは言えない事情があった。Salton, Inc. v. Philips Domestic Appliances & Pers. Care B.V., 391 F.3d 871, 877–80 (7th Cir. 2004)

134 *See* WesternGeco LLC . ION Geophysical Corp., 138 S. Ct. 2129, 2135 (2018)

135 TianRui Group Co. Ltd. v. International Trade Commission, 661 F.3d 1322 (Fed. Cir. 2011)

営業秘密を海外で使用している場合に、侵害行為は海外なので、DTSA の適用はないと被告が主張したのに対し、侵害品が米国内に持ち込まれて、展示や見本として使用されている以上、米国内の「不正な使用」があると考えられ、域外適用の問題は生じない可能性があることを述べた[136]。したがって、域外適用の問題が本当に生じるのかどうかも検討する必要がある。

DTSA は、以下の場合に、米国外行為にも DTSA が適用されることを規定する[137]。

a. 侵害者が、米国の市民、若しくは、永住外国人である自然人、又は、米国、州若しくはその政治的区分の法律下で、組織された団体である。

b. 米国で犯罪を達成させる行為が行われた。

イリノイ州の地方裁判所により、明文による域外適用は重要であるが、それだけでなく、「米国内の」不正な使用が緩やかに決定される可能性が示された[138]。

第 6 章　営業秘密侵害の事件数

1　訴訟数の概観

2017 年以降、およそ年間 1,300 件ほどの営業秘密侵害事件が提起されている。ことに、営業秘密侵害事件の連邦裁判所への提起は、DTSA 判例の誕生した 2016 年から 2017 年に 30%増加し、その後は特に増減がない[139]。

2020 年の営業秘密侵害事件の 72.9%、 2019 年の営業秘密侵害事件の 72.5%で、DTSA に基づいた請求が含まれていた。

営業秘密の訴訟が頻繁に提起される裁判地としては、以下の州がある:

- カリフォルニア州;
- イリノイ州;
- ニューヨーク州

2　訴訟結果

2017 年から 2020 年の間での事件の終局は下記のとおりであった。

- 67% の事件は、本案に関する判決前に和解
- 74% の本案終局判決に至った事件で、恒久的差止命令を発令

---

[136] Philips Med. Sys. (Cleveland), Inc. v. Buan, No. 19-CV-02648, 2021 WL 3187709, at *10 (N.D. Ill. July 28, 2021)
[137] 18 U.S.C. § 1837
[138] Motorola Sols., Inc. v. Hytera Commc'ns Corp., 436 F. Supp. 3d 1150, 1162 (N.D. Ill. 2020)
[139] LexMachina 調査結果。この結果には、DTSA に基づく請求、UTSA（州法）に基づく請求、刑事訴追、行政的措置のすべてが含まれる。

- 54% の本案終局判決に至った事件で、暫定的差止命令を発令
- 65% の本案終局判決に至った事件で、一時的抑止命令を発令

全体で、12 億 9400 万ドルの金銭的賠償が認められた（2020 年一年では、5 億 4100 万ドル）。これには、以下を含む:

- 現実の損失;
- 懲罰的賠償;
- 合理的ロイヤルティ
- その他の損害;
- 判決前の利息;
- 弁護士費用

2019 年と比較して、裁判所は、2020 年の一年で、営業秘密事件一件あたりで、より高額の金銭的賠償を認めた。

3　解決の期間

2017 年から 2020 年の間での事件解決に要した平均時間:

- 略式判決まで:　617 日
- 審判まで:　795 日
- その他：　259 日（和解を含む）

4　連邦経済スパイ法

米国司法省（DOJ）は、外国人又は外国法人による営業秘密侵害事件の捜査、対中国の経済スパイ法事件の訴追を主に手掛けてきた機関である。DOJ が扱った事件としては、非常に大幅なコンピューターシステムへの侵入、および、営業秘密の不正取得に対する外国の軍関係者の起訴、外国の政府及び外国の企業に代わって営業秘密の不正取得を敢行した個人及び企業体の起訴、並びに、多数の外国人による営業秘密の窃取事例の訴追がある[140]。

18 U.S.C. § 1831（スパイ目的による営業秘密の侵害行為を刑事処罰する規定）が、裁判所の意見（中間的判断含む）で引用された事件は、同法が制定された 1996 年以降全 188 件あり、2021 年 11 月 27 日までの 5 年間で 129 件、2021 年 11 月 27 日までの 3 年間で 80 件であった。他方、18 U.S.C. § 1832（非スパイ目的による営業秘密の侵害行為を刑事処罰する規定）が、裁判所の意見（中間的判断含む）で引用された事件は、1996 年以降全 282 件であり、2021 年 11

[140] 米国司法省, Report to Congress Pursuant to the Defend Trade Secrets Act https://www.justice.gov/criminal-ccips/page/file/1101901/download (最終アクセス日 2022 年 2 月 18 日).

月 27 日までの 5 年間で 142 件、2021 年 11 月 27 日までの 3 年間で 86 件であった。このことからも、同法違反として事件となる刑事事件又は民事事件は、特にこの 3 年間で増加していると理解される。

FBI の年間報告によると、連邦経済スパイ法の立件数は、ここ数年で増加している。（括弧内は、年間知財犯罪件数中の割合）

- 2019　Economic Espionage Act Economic espionage, 18 U.S.C. § 1831 2 (3%)
  Theft of trade secrets, 18 U.S.C. § 1832 14 (22%)
- 2018　Economic Espionage Act Economic espionage, 18 U.S.C. § 1831 1 (2%)
  Theft of trade secrets, 18 U.S.C. § 1832 10 (14.7%)
- 2017　Economic Espionage Act Economic espionage, 18 U.S.C. § 1831 2 (3%)
  Theft of trade secrets, 18 U.S.C. § 1832 9 (11%)
- 2016　Economic Espionage Act Economic espionage, 18 U.S.C. § 1831 1 (1%)
  Theft of trade secrets, 18 U.S.C. § 1832 5 (6%)

第 7 章　営業秘密関連の法改正の動き

1　営業秘密法

DTSA 成立以来、連邦法の改正は現在までなされていない。2021 年春には、米国の核心的技術に関わる技術に関して、外国人による営業秘密の侵害を覚知した場合に、省庁間での連絡を確立し、関税、輸入、証券・金融取引、知的財産保護等に対する制裁を加えることを可能とする法案が、上院議員の Graham Lindsey 氏により提案された[141]。

州営業秘密法の改正の動向は、発表がない。

2　サイバーセキュリティ政策

前政権から重点が置かれている、対中国対策、サイバー犯罪による国家機密情報の漏洩対策については、規制が引き続き強化されている。

(1)　輸出規制

2021 年 10 月 21 日、米国商務省産業安全保障局は、重要な暫定最終規則（暫定規則）を発表した[142]。暫定規則は、サイバーセキュリティとランサムウェアの問題に対する、政府全

---

[141] 「中国による営業秘密盗取との戦闘法」と第する法案を提案しているが、進行がみられない。S1245−CCP Trade Secrets Act, https://www.congress.gov/bill/117th-congress/senate-bill/1245/text.

[142] 米国商務省、商務省は、民間人の監視およびその他悪意のあるサイバー活動で使用される品目の輸出管理を強化（最終アクセス日 2022 年 2 月 28 日）
https://www.commerce.gov/news/press-releases/2021/10/commerce-tightens-export-controls-items-used-surveillance-private.

体の重点化を反映し、悪意のあるサイバー活動に使用できる、侵入ソフトウェア、ネットワーク監視機器、及び、関連技術などの「サイバーセキュリティアイテム」の新しい輸出管理を確立する。この規則には、新しい輸出管理分類番号、新しく定義された用語、及び新ライセンス例外「輸出許可されたサイバーセキュリティ」（ライセンス例外 Ace）が組み込まれている。パブリックコメントに基づいて、変更が加えられなければ、2022 年 1 月 19 日（公開から 90 日以内）に発効する予定である。

暫定規則は、「正当なサイバーセキュリティ活動」を妨げないように「適切に調整」されることを目的とする。しかし、国グループ D の国（中華人民共和国など）のユーザーとビジネスを行う、サイバーセキュリティ分野で事業を行っている企業は、サイバーセキュリティアイテムのエンドユーザーが、「政府のエンドユーザー」か「非政府のエンドユーザー」であるか、評価が必要になる。前者では、ライセンス例外 Ace が利用不可能である。提案された新しいフレームワークでは、追加のデューデリジェンスが必要になりうることに注意すべきである。

(2)　5G 等の通信環境

2021 年 11 月 11 日、バイデン大統領は、2021 年安全設備法に署名した[143]。これにより、連邦通信委員会は、同委員会の「対象リスト」に記載の機器及びサービスについて、以後は承認を審査しないか、又は、承認しないことを明確にしなければならなくなった。2021 年 3 月 12 日に最初に公開されたリストには、米国政府が以前、国家安全保障上のリスクとして特定した、中国の電気通信、及び、セキュリティカメラ会社が含まれている。既存の制限は、政府の調達と、助成金の文脈で、そのような指定項目の採用を制限する。安全設備法は、これに加え、連邦通信委員会に、米国内の誰もが、特定の中国の技術を使用することを禁止する規則を制定するように促すものであり、著しい効果の増加が予定される。

現在、対象リストには、(1)Huawei Technologies 社、(2) ZTE Corporation、(3) Hytera Communications Corporation、(4) Hangzhou Hikvision Digital Technology Company、(5) Dahua Technology Company 、及び、それらの子会社や関連会社が含まれている。

(3)　通商法第 301 条による調査

トランプ大統領は、2017 年に改正された 1974 年通商法（貿易法）の第 301 条に基づく、

[143] ホワイトハウス、法案へ署名：H.R.3919（Nov. 11, 2021)
https://www.whitehouse.gov/briefing-room/statements-releases/2021/11/11/bill-signed-h-r-3919/#:~:text=signed%20into%20law%3A-,H.R.,unacceptable%20risk%20to%20national%20security.

中国による不正な貿易慣行に関する調査を行うよう命じた[144]。第 301 条は、潜在的に対応可能な外国の行為、方針、又は、慣行の、以下の 3 つのカテゴリーを定めている。

i. 貿易協定違反

ii. 不当（米国の国際的な法的権利と矛盾するもの）で、米国の商取引に負担をかける、又は、制限する行為、ポリシー若しくは慣行

iii. 不合理又は差別的であり、米国商取引に負担をかけたり、制限したりする行為、方針、又は慣行。

このうち、第 3 のカテゴリーの行為が、2017 年の調査に最も関連していた。

調査の結果、中国は、合弁事業の要件、外国投資の制限及び行政審査とライセンス供与のプロセスを使用して、米国企業からの技術移転を要求又は圧力をかけており、米国企業からのライセンス供与やその他の技術関連の交渉において、市場ベースの条件を設定する能力を奪っていること、加えて、中国は、大規模な技術移転を生み出すために、米国の企業や資産へ、体系的な投資と買収を指示し、不当に促進していると結論づけた。そして、USTR は、2018 年 7 月から、対中国向けの 25%の従価税を行うことと決定した。

導入された中国物品に対する追加関税賦課は、除外の申請の許可を受けることができれば、これを免れることができるようになっていたが、2020 年末に失効した[145]。バイデン政権は、国内製造業の部品不足等の状況を踏まえ、2021 年 10 月に、一度失効した除外を復活させる予定であると公表しており、今後、除外の復活が見込まれている。

第 8 章　国際協力・他国との連携状況

前述のとおり、経済スパイ法は、域外適用規定を設けるなど、米国捜査・訴追機関が、国際的な営業秘密事件で、幅広く管轄権を掌握することを目指すものと理解されるが、実際には、対人管轄、事物管轄から、捜査・訴追権限には、地理的な制限がある。海外に所在する外国人が、海外に位置している間に行った行為に関しては、米国の捜査機関、司法機関の権能は限定あるいは否定されてしまうのが通常で、更に、関連する営業秘密が米国内にない場

---

144 同条は、貿易相手のさまざまな不公正な行為、政策、慣行に対処するために使用できる、米国の主要な規制手段である。USTR, 974 年通商法第 301 条に基づく技術移転、知的財産、およびイノベーションに関連する中国の行為、方針、および慣行に関する調査の結果（March 22, 2018)

145 USTR, USTR は、第 301 条の関税の対象となる中国製品の潜在的除外について、コロナウィルス関係の物品については、除外の復活を 11 月に決定した 。米国 USTR、「製品除外の延長に関する通知：技術移転、知的財産、およびイノベーションに関連する中国の法律、方針、および慣行」86 Fed. Reg. 63438 (2021 年 11 月 16 日)https://ustr.gov/about-us/policy-offices/press-office/press-releases/2021/october/ustr-requests-comments-reinstatement-targeted-potential-exclusions-products-china-subject-section.

合、管轄が否定されかねない[146]。

しかし、経済スパイ法は、（1）犯罪者が、米国市民あるいは永住外国人である、若しくは、米国法に基づいて組織された法人である、営業秘密の侵害、又は、（2）犯罪を達成させる行為が米国内で行われているものに、米国の捜査機関に管轄権を与える[147]。

DOJ の Computer Crime and Intellectual Property Section (CCIPS), Office of International Affairs in the Criminal Division (OIA) が、これまでに DOJ が訴追した国際的営業秘密事件の捜査を手掛けてきた[148]。CCIPS はサイバーラボというグループを有し、ハッキングを伴うコンピューター利用による侵害で、証拠の収集、解析を行うことができる。

犯人が米国内にいない場合などは、海外の捜査機関・司法機関から協力を得て事件を捜査・訴追することが重要となる。DOJ 内のリソースだけでなく、海外の捜査機関に対して、捜査協力を求める場合、米国が外国と締結している刑事共助条約を通じて、犯人の捜索、証拠収集の要請がなされる。例えば、証人の召喚、証拠の提出、捜索令状の発行に関する権限を米国検察官に与えるものであるが、実際に権限を行使するためには現地の捜査機関の執行が不可欠となる。

これに加えて、広域な組織的犯罪の場合には、インターポール、ユーロポールを通じて国際犯罪への捜査協力を、複数国に申請することがなされる。

米国の連邦捜査局（FBI）は、世界中の法執行機関、諜報機関、および、セキュリティサービスとの関係を構築しており、自国民や自国企業を保護するために、特別捜査官やその他の要員を 63 の海外支所に配置している[149]。したがって、海外拠点を通して、迅速かつ継続的な情報交換が可能となっている。FBI は、捜査対象に、組織的犯罪、サイバー犯罪（サイバー部門が担当する）を含むため、知的財産権事件や営業秘密侵害事件（民間企業の事件は、犯罪捜査部門の知的財産権プログラムが扱う）も、捜査を行うことができる。

米国は、TRIPS 協定に基づいた知的財産権保護制度の強化を WTO に訴えるなどして、他国に要求してきた。また、USTR は、ASEAN 諸国に対しても、かねてより、国際的な知的財産権保護の協調について、合意・協定の交渉を重ねてきた。例えば、2016 年 11 月には、ペルーのリマで開催されたアジア太平洋経済協力（APEC）の指導者と大臣による、「営業秘密の保護と侵害に対する執行の最善の慣行」の合意に至った[150]。

---

146 上記「準拠法・域外適用」を参照。
147 上記「準拠法・域外適用」を参照。
148 米国司法省、脚注 140
149 FBI、海外支所 (最終アクセス日 2022 年 2 月 18 日) https://www.fbi.gov/contact-us/legal-attache-offices.
150 営業秘密の保護と侵害に対する執行の最善の慣行(2016)

第 9 章　仲裁の利用

上記のとおり、営業秘密侵害事件における、比較的多額の認容額、高率の恒久的差止命令は、裁判所における訴訟を選択する、極めて重要な動機となっている。

しかし、裁判所における審理では、少なくとも、営業秘密の内容や、自社の技術の内容について主張、立証しなければならず、措置をとらない限り公開されてしまう結果となり、自社の機密情報を、競争相手に知られて（推察されて）しまいかねない。また、カリフォルニア州では、原告が、訴えの最初から、合理的な特定性をもって営業秘密を特定しなければならないという要求が存在する。

これに対して、仲裁手続では、仲裁自体の存在も秘密にでき、パブリシティの悪影響を防ぎえるうえ、仲裁手続で交わされた当事者の主張、提出された証拠について、より秘密性が確保される。したがって、営業秘密の侵害事件を、裁判を介さず、仲裁手続きで解決することは、当事者にとって有益な場合が多くある。それに、裁判手続きは、長期に及び、費用も多額となりやすい。

一般商事事件での仲裁手続き利用が定着してきた米国では、営業秘密事件の仲裁手続きの利用も、珍しいことではないとされる[151]。

第 10 章　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

第一に、営業秘密には、「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」ことが要件とされているため、機密情報や営業秘密を、秘密保持義務への合意のないまま、第三者に提供することは、それらの「機密性」を失わせる結果となりかねない[152]。

次に、営業秘密の合理的な特定性が、州法上要求されるのと同様に、契約においても、何が営業秘密か、当事者にとって明確であるように定義する必要がある。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）を明文で盛り込むのが賢明であり、必要性が高い。

ライセンスを受けるなどして、機密情報あるいは営業秘密を保持する者が、「秘密性を保持するための合理的な措置」を取っているか否かは、以後の営業秘密の保護に重要な事実として関わってくる[153]。このため、秘密保持義務の内容を秘密保持契約書内に盛り込むことが重要であると推奨される。

---

[151] Jeremy Cohen, et al., Preparing for Trade Secret and Restrictive Covenant Litigation While the Court Near You is Closed, Seyfarth Shaw (Apr. 14, 2020) https://www.jdsupra.com/legalnews/preparing-for-trade-secret-and-40528/.

[152] 第 1 章「営業秘密の定義」を参照

[153] UTSA 第 1 条、18 U.S.C. § 1839(3).

裁判所の述べたように、

- 自社あるいはライセンシーの従業員が、自己の情報通信機器を使用できないようにするか、それを許す場合は、アクセスと使用のコントロールのための厳格な制限を課すこと、
- パスワードによる保護なく、コンピューターのアクセスや、ファイルを保存や読み出しすることができないこと、
- ライセンシーにおいて、機密情報、営業秘密を、機密性に関する程度でラベルすること、
- ライセンシー従業員の機密性保持の言明、
- 情報が、業務を実行するため少なくとも潜在的にアクセスを必要とする人にのみ開示されている（「知る必要があるベース」）、
- 情報の開示を受ける者は、秘密保持義務に拘束され、情報に関して、この秘密保持義務を負っていることを認識していることの確認

は、プラスの要素となるため、含めることが推奨される[154]。

本報告書に添付の書式は、こうした重要な要素を含んだ保護措置が取られるように、ライセンシーに義務付けている。ライセンシーの中の誰が機密情報に触れうるかについての特定は、添付文書の形で行われるのが現実的と考えられる。また、相手会社の機密情報を取り扱う者と個別に、同様の秘密保持契約を締結することも勧められる。

ライセンス、生産委託、合弁会社設立の際に、当事者間で契約書がかわされる場合、契約書に機密保持条項を盛り込むのは通常なされるが、米国法が準拠法である場合には、以下の問題が起こりうるので注意し、米国弁護士に相談することが推奨される。

1　ライセンス契約

(1) 機密情報、営業秘密の特定

あまりに広範囲で網羅的な条項は、機密性保持の実施が困難であり、実務的ではない。あまりに秘密保持義務が広範な契約は、無効とされたり、法的拘束力を否定されることもある。また、雇用関係に関連する場合は、被用者の労働の自由が考慮される。

実際には、情報の機密性のラベルが有意義と考えられる。機密情報とすべき必要性があること、実際に機密情報として扱われていることが、後に立証できるよう確認すべきである。

一方、相手会社が、機密情報や営業秘密を利用して生み出すデータや情報を、機密情報や営業秘密に含めることは、多くの場合に、不可能ではないと考えられる。

---

[154] 第１章「営業秘密の定義」を参照

(2) 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

契約条項を作成する場合、何が許されるか、そして、何が不正取得、使用、又は、開示になるかを明確にすることは、ライセンシー及びライセンサーの利益を守り、また、有効な関係を維持するためにも大切である。例えば、ライセンシー側で、パスワード等アクセス制限を設定すること、アクセスできる者を一定の被用者、関係会社の被用者、専門家、監査人等に制限すること、アクセスの目的と使用方法を制限することなどが、考えられる。

侵害行為者が、営業秘密の不正使用、開示、取得にあたる事実を認識していたことや、認識すべきであったことが、営業秘密侵害の前提とされており、許可事項と不許可事項を分別することが意味を持つと考えられる。

営業秘密保有者において、機密性を保つ合理的な措置をとっていたかに関連して、電子機器使用時のパスワード要求、不用意な紙媒体での処理のないことは必須と考えられる。

(3) 契約終了後の情報の返却あるいはデータ削除義務

秘密保持義務の内容として、提供された機密情報や営業秘密は、契約関係終了時に保有者に返却すること、また、バックアップも含めて、保存されたデータから削除するように要求すること、それを確認することを明記することが必要である。これは、前記の、機密性を保つ合理的な措置の認定にも、プラスの要素として働くと考えられる。

(4) 補償条項

相手方の秘密保持義務違反の結果生じた損害について、相手方に補償の義務を負わせることは、多くの場合に行われている。秘密保持義務条項の有効性が認められる場合、こうした補償条項の効力も同様に認められるであろう。

(5) 損害額

機密情報・営業秘密保有者は、不正取得、使用、あるいは、開示により生じた損害に対する賠償として、特約がない場合、自分の被った損害を立証して、その填補を求めることができる。この損害の立証は困難となることも考えられるので、損害額の算定について、事前に合意しておくことも考えられる。

(6) 仲裁合意

裁判による紛争解決と比較し、仲裁は、営業秘密、機密情報の保護に適し、手続きで提出あるいは開示された情報の秘密性が保たれやすいと考えられている。そこで、ライセンス契約にあたっても、仲裁条項を挿入して、仲裁により契約の紛争を解決し、ライセンサーの機密情報や営業秘密の保護を図ることは、積極的に検討されるべきである。

2　生産委託契約

上記に列挙した注意点は、生産委託契約にも当てはまる。委託者としては、受託者の生産ラ

インの運営状況、生産品の数量等の確認体制、保存・管理状況を十分確認することが、特に重要となると考えられる。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は検討されるべきである。

生産委託契約では、受託者が、第三者の機密情報、営業秘密情報をたまたま持っていて、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、請求を起こされてしまう可能性がある。委託者自身が知り得ない場合、委託者に対する請求は成功しないとしても、暫定措置により、生産に対する影響が起こりうる。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は、検討されるべきである。

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は、特に重要となる。

欧州

第 1 章　営業秘密の定義

1　EU 指令の制定と主要加盟国の国内法移行

2016 年、欧州連合で制定された「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、開示に対する保護に関する指令（EU）2016/943」（以下「EU 指令」という。）は、事業に関して利用されている価値ある情報が、競争相手に盗用されたり、無断で使用、あるいは、開示されてしまうことにより、企業や個人主が築いた市場競争力を奪取されてしまう事態が起こらないように、不公正な競争を防ぐ観点で、各加盟国で制定されている法律を強化し、調和させることを目的とした、法的文書である。EU 指令自体には、直接的に対私人的な法的効力を及ぼすものでないものの、各加盟国は、2018 年 6 月 9 日までに、EU 指令を国内法に移行する措置をとる義務を負った。その結果、第 3 章「営業秘密侵害に関連する法律、規制の概要」で説明するように、各加盟国で国内法制定が実現している。

EU 指令は、営業秘密の違法な取得、使用、開示に対し、民事上の救済を規定するにとどまる。刑事制裁、行政措置、公共調達、その他の政府・公共機関での国内手続きにおける営業秘密の使用に関しては、EU 加盟国の国内法に委ねられている。EU 指令以外に、EU 内市場における、企業による消費者への不公正な商慣行に関する指令が存在し[155]、不公正な競争に対して、不公正商慣習指令が、EU 指令に加えて適用される場合がある。

2　EU 指令による「営業秘密」の定義

EU 指令の第 2 条によると、「営業秘密」とは次のような情報を意味する[156]。これは、知的所有権の貿易関連の側面に関する協定(TRIPS 協定)に含まれる定義に基づいており、米国や日本で一般に受け入れられている「営業秘密」の概念と、定義上は、ほぼ等しいものとなった[157]。

(1) 第 2 条の規定内容

営業秘密の定義は、ノウハウ、ビジネス、及び技術情報を網羅するように解釈されるべき

---

[155] 2005/29 / EC（不公正商慣習指令）

[156] EU 指令第 2 条

[157] 世界貿易機関の知的所有権の貿易関連側面に関する協定（1994 年 4 月 15 日）第 39 条の定義規定。EU 指令は、世界貿易機関（WTO）加盟国が遵守すべき、TRIPS による統一された定義に従い、それを欧州連合に正式に導入したものである。

とされ、それらの秘密性を保持することに、正当な利益があり、秘密として保持されることが期待されるものを意味する[158]。これにより、従業員が、通常の雇用過程で得られた経験やスキルだけでなく、業界内部者が、各自容易に作成することが可能な情報も、定義から除外されることが予想される。

a. 単体として、又は、そのコンポーネントの正確な構成と組み立てにおいて、その種の情報を扱う業界内関係者の間で、通常、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。
b. それが秘密であることから、商業的価値がある。
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。

EU 指令では、具体的にどの程度の秘密性保持のための措置が「合理的」とみなされるか、及び、どのような状況下で、問題となった情報が「容易にアクセスできない」情報であるかについて、特別な規定が置かれていない。今後、これらの用語の解釈（殊に、秘密性保持の措置の要求）に関し、各加盟国の国内法の規定や判例法により、解釈のばらつきが生じうる。

上記の要件のうち、秘密性のために「商業的価値がある」について、実際の金銭的な価値には限定されておらず、潜在的に有益なものであれば、要件は満たされると捉えられる[159]。例えば、保有者により営業秘密として扱われ、実際に開示が厳しく制限されてきた情報は、反証が無い限り、商業的価値があると見なされるべき、とするアプローチは、EU 指令によって排斥されていない。また、保有者が受ける利益は、科学的新規性、技術的優越性だけでなく、ビジネス的効率性、経済的有利性、戦略的優越性、競争力が含まれるため、保有者の債務額や財務諸表に存する情報、顧客のクレジットカード情報も含まれうる。

EU 指令第 2 条の解釈に争いが生じれば、最終的には、欧州連合司法裁判所（CJEU）が判断することになる。

(2) EU 指令による「保有者」の定義

EU 指令には、「保有者」とは、営業秘密を合法的に管理する自然人又は法人を意味すると規定されている[160]。これには、営業秘密を発明した者のみならず、発明者の雇用主、関連会社、ライセンシーが含まれる。

(3) EU 指令による「侵害者」の定義

[158] EU 指令序文
[159] EU 指令序文
[160] EU 指令第 2 条

侵害者とは、営業秘密を、違法に取得、使用又は開示した自然人、若しくは、法人を意味する[161]。したがって、侵害者は必ずしも、営業秘密保有者と直接的な契約関係がある者や、事実上の競争、取引関係にある者に限られない。しかし、「違法に」との限定があることから、適用される法律で、取得、使用、又は開示が、違法と判断されることが前提となる。

(4) EU 指令による「侵害品」の定義

侵害品とは、違法に取得、使用、又は、開示された営業秘密に、相当に利益を受けるデザイン、機能、製造プロセス、マーケティング、又は、特性を持つ物品を言う、と定義している。侵害品と認定するには「相当に利益を受ける」ことが必要となるため、立証は容易ではない可能性が高い。更に、各加盟国の裁判所が異なった解釈をする可能性もあろう。

第 2 章　営業秘密侵害行為の定義

1　EU 指令における営業秘密侵害行為

(1) 第 3 条による侵害行為からの除外

EU 指令第 2 条は、上記の通り、侵害者とは、違法に営業秘密を取得、使用、若しくは、開示する者を言う、と定義し、侵害行為は、「違法に取得、使用、又は開示」することであることを明らかにしている。この点で、第 3 条は、「違法」ではない場合を例示的に列挙するが、これらの行為のうち最初の 2 つの類型は、他の国々でも、殆ど営業秘密侵害行為とはみなされていない[162]。下記 c 及び d の類型は、管轄により違法とみなされている可能性がある。

a. 独立した発見や創造
b. 一般公衆が入手可能であった、若しくは、営業秘密の取得に法的制約を課されていなかった入手者が所持していた、製品や物品の観察、研究、解体、検査
c. 連合法や法令、慣習に則った、情報及び諮問を得られる、労働者あるいは労働組合の権利の行使
d. その他、行為時の状況下で、誠実な商慣習に合致した行動

(2) 第 4 条の規定

EU 指令は、更に、第 4 条において、どのような範囲の行為が、「違法な取得、使用、又は開示」に該当しうるか、行為者の保有者に対する関係、立場に応じて、具体的な侵害行為

[161] EU 指令第 2 条
[162] 日本でも、リバースエンジニア等で得られた情報、公開情報から察することができた情報については、不公正な競争とは言えず、営業秘密侵害とは考えられていない。

を例示的に列挙している[163]。

① 営業秘密の取得者

営業秘密保有者の同意なく、以下のいずれかの行為を行った場合、侵害行為に該当する。

a. 保有者の管理下にある、営業秘密を含んだ、若しくは、営業秘密を取り出しうる、文書、物件、材料、物質、又は、電子ファイルへのアクセス、使用、若しくは、コピー

b. 行為時の状況下で、誠実な商慣習に反するその他の行動

前半部分は、同意なく営業秘密を含んだ有体物や無体物にアクセスする行為を、侵害行為とする。したがって、目的は必要でないことはもちろん、故意や過失を問わないように読める[164]。

以上のように、EU 指令は、「誠実な商慣習に反する」行為という、漠然とした内容の行為を、営業秘密の違法な取得に含めている。例えば、営業秘密保有者の同意が欺罔により得られた場合、同意が撤回された、若しくは、効力を失ったことが明らかな場合には、「誠実な商慣習に反する」に該当すると考えられる。同じ定義を国内法に有する、加盟国の裁判例の今後の動向を注意する必要がある。

② 営業秘密の開示者、使用者

営業秘密保有者の同意なく、以下のいずれかの行為を行った場合、侵害行為に該当する。

a. 営業秘密を違法に取得（上記(1)の規定にあたる行為）

b. 秘密保持義務、又は、営業秘密を開示しない義務に違反

c. 契約上の義務、又は、営業秘密の使用を制限すべき義務に違反

以上のように、営業秘密の違法な取得者以外にも、守秘義務を負う被用者、会社役員、アドバイサー、会社買収の交渉相手等、営業秘密の開示、使用に関して制限を受ける者も、開示や使用ができない。

③ 営業秘密の取得者、使用者、開示者

営業秘密が、違法に使用あるいは開示していた（上記②や本項にあたる行為）者から、直接的、若しくは、間接的に得られた事実を、認識していたか、その行為時の状況下で、認識すべきであった場合

④ 侵害品の製造者、提供者、市場展開者、輸出者、輸入者、若しくは保管者

---

[163] EU 指令第 4 条

[164] ICC, Protecting Trade Secrets-Recent EU and US Reforms (2019) 16, *available at* https://iccwbo.org/publication/trade-secrets-report/.

営業秘密が、違法に使用されていた（上記②、③にあたる行為）事実を、認識していたか、その行為時の状況下で、認識すべきであった場合

具体的にどのような行為が営業秘密侵害行為となるかは、各加盟国が国内移行で行う制定法の規定、及び、裁判所の解釈に依存することは否めず、実務上、相当な幅が生じるのではないか、と考えられる[165]。

2　営業秘密侵害行為に対する例外

EU 指令は、第一次的には、欧州連合内での営業秘密保護を強化するための原点として制定されたが、中には、情報のような無体物が財産として保護されてよいか、といった保護の拡大、強化に対する懸念も存在した[166]。これに対し EU 指令は、営業秘密の定義において、「合理的」な秘密性保持措置を要求し、「違法性」についての限定する規定を盛り込んだほか、侵害行為に関し、下記のような例外規定を設けた。

a. メディアの報道の自由、多様性を含む、表現、及び、情報の自由の権利行使
b. 公共の利益を保護する目的での、違法行為、不正行為、又は不法行為の暴露
c. 連合法や国内法に則った、組合代表の機能の正当な権利行使としてなされる、労働者から組合代表への開示で、必要があるもの
d. 連合法や国内法に認められた正当な利益を保護する目的での行為

EU 指令は、比例性と濫用に関する保護措置に基づくだけでなく、内部告発や、第三者の犯罪や違法行為に関する情報提供を、営業秘密侵害から除外することで、保護を与えている[167]。すなわち、「営業秘密」の定義には、違法又は不正な商慣行に関連する情報（例えば、過去の違反に関する情報で、規制省庁へ届け出ていないもの）も含まれてしまうところ、そのような情報は法的保護を与えるべき意義に乏しいと考えられ、また、公益を促進する、違法行為に関する通報が、不正行為を隠匿する事業主により妨げられるのは不合理である。そこで、EU 指令は、違法行為、不正行為、又は不法行為を明らかにする目的の例外規定を設け、開示を正当化することができることとした。

第 3 章　営業秘密侵害に関連する法律、規制の概要

1　EU 指令の国内法移行

例えば、ドイツの新しい営業秘密法は、最小調和の程度で、EU 指令を実施することを目的

165 過失、故意等の主観的要件、及び、転得者はどうか、等。
166 EU 指令序文
167 EU 指令第 5 条

として制定されたが、営業秘密の定義の変更を無理なくされた。その他、ドイツで強固に貫かれていた、訴訟手続の公開制度との関係から、営業秘密を公開から保護する手続について導入し、今後の知的財産権訴訟における、重要なステップとなることが期待される[168]。

英国の新しい営業秘密法は、英国が欧州連合から脱退する前に制定され、EU 指令の立法目的を充足するような内容の規定となっている[169]。特に、営業秘密の定義の面で、かつての営業秘密の概念を変更するものと予想される[170]。一方、コモンローの下で発展した、従前より存在する機密情報に対する法的保護は、併存することが示唆され、新法下の保護に関し、今後の裁判例の展開が待たれるところである[171]。

フランスでは、商事法の中に、EU 指令を実施することを目的として条文が新設された[172]。民事事件として、営業秘密所有者が、損害賠償請求、差止請求等を求めることができ[173]、また、侵害者の悪質性の程度に応じて、損害額の増額がなされるように規定されている。但し、濫用的な訴訟を起こした原告に対しての制裁手段が置かれていることが、他に見られない特徴となっている[174]。

チェコ共和国は、知的財産権の救済に関する 1 つの条項を修正するだけで EU 指令を移行した[175]。

ポルトガルでは、営業秘密保有者は、情報を秘密に保つために必要なすべての措置を講じる必要があるとの規定となっている。これには、秘密性を維持するための合理的な措置を超えた措置が、必要になる可能性があると思われる。

このように、EU 指令自体は、営業秘密という財産権を取り出して、統一した定義を用意、確立し、欧州連合全体で均一な最低限の保護基準を確立したという点では重要であるが、各国間での法制度や保護の内容は異なったままである。すなわち、EU 加盟国は、EU 指令に定められた、特定の責任除外規定、及び、自由保障措置の遵守を条件として[176]、より広範囲の営業秘密保護を提供できる。

---

168 本書「ドイツ」編
169 Mr. Williams 氏インタビュー
170 Mr. Williams 氏インタビュー
171 Mr. Williams 氏インタビュー；本書「英国」編を参照
172 フランス商事法第 L. 151–7 条
173 第 L. 152–３条
174 第 L. 152–6 条
175 Rogier de Vrey, EU: Trade Secret Law Reforms, CMS (最終アクセス日 2022 年 2 月 18 日) https://cms.law/en/int/publication/eu-trade-secret-law-reforms.
176 EU 指令には、内部告発者の保護、表現の自由、雇用者の権利の保護に関する規定が設けられた。

2　営業秘密侵害に対する刑事処罰

(1) 刑事根拠法規

オーストリア、ベルギー、キプロス、デンマーク、エストニア、フィンランド、フランス、ドイツ、ギリシャ、ハンガリー、イタリア、ラトビア、リトアニア、ルクセンブルグ、マルタ、オランダ、ポルトガル、ルーマニア、スロバキア、スペイン、スウェーデンにおいては、営業秘密侵害が刑事処罰されうる刑事法の規定が制定された[177]。

オーストリア、キプロス、チェコ共和国、デンマーク、フィンランド、ドイツ、ギリシャ、ポーランド、ルーマニアでは、不正競争防止法として、営業秘密侵害が処罰される立法がされている[178]。

スウェーデンは、特別法で営業秘密侵害の刑事処罰規定を設けた[179]。

このほか、EU 加盟国ではないが、スイスでも、営業秘密侵害が刑事処罰されうるとの規定が同国の不正競争防止法に規定されている。

(2) 親告罪

11 カ国で、親告罪として、処罰されている[180]。

(3) 主観的要件

ベルギー、エストニア、フランスでは、過失による営業秘密侵害に、刑事処罰が適用可能とされてきた[181]。デンマークでは、一定の例外的場合（秘密が広範囲に流布されたなど）には、過失のみで足りるとされている[182]。ハンガリー、イタリア、スウェーデンでは、故意が必要とされているが、目的犯とはされていない[183]。

(4) 関連犯罪

フランスでは、外国権力に秘密情報を提供する行為については、最大 15 年の懲役刑が課される等、厳罰化が規定されている。

より多くの国が、コンピューター犯罪に関して、刑事処罰する規定を置いており、営業秘

---

177 競争会社間での価格設定の合意など、明らかな独占禁止法の違反となる行為は、規制されると考えられている。欧州委員会、欧州内の営業秘密と機密事業情報の調査（2013）（「欧州委員会調査」) 55
https://ec.europa.eu/docsroom/documents/14838/attachments/1/translations/en/renditions/pdf
178 欧州委員会調査 55
179 欧州委員会調査 55
180 欧州委員会調査 75
181 欧州委員会調査 57
182 欧州委員会調査 57
183 欧州委員会調査 58

密侵害に関連して、コンピューター犯罪としても取締りが可能となっている[184]。

(5) 訴追状況

営業秘密事件が、刑事事件として訴追されることは少ない。その理由として、刑事有罪判決に前提とされる、より高度の確実性（心証）を形成するための立証が難しいこと、合理的な秘密性保持の措置が採られていたことの立証が難しいことがあげられる[185]。

(6) 保全的措置

殆どの国で、刑事事件に付随した処分として、証拠保全のための、コンピューターや場所の捜索、差押、被告人の捜索、逮捕、侵害差止命令が、裁判所により発せられることが可能とされている[186]。

(7) 刑事罰

① 侵害者個人：大半の国では、懲役刑と罰金とが併科される（15 国）。次いで、懲役刑のみが法定されている国もある（10 国）、6 ヶ月から 3 年の法定刑とされているが、侵害者と営業秘密保有者との関係、侵害者の心理状態、その他の要素で刑が異なることが多い[187]。

② 法人罰：従業員や役員の行為について、法人が罰せられることも、オーストリア、ベルギー、キプロス、デンマーク、エストニア、フィンランド、フランス、ハンガリー、ラトビア、ルクセンブルグ、オランダ、ポーランド、ルーマニア、スロベニア、スペイン、英国でみられる[188]。

また、スペインや、幾つかの東欧諸国では、法人の解散、事業停止等、厳しい処置が行いうることとなっている[189]。

このほか、スイスにおいても法人罰の規定があり、最高 410 万ユーロまで罰金を課すことができるとされている。

(8) 民事救済との関係

多くの国で、民事的な損害賠償の訴えが、刑事事件手続内で扱われているとされる[190]。

---

184 ベルギー等の加盟国にコンピュータ犯罪処罰規定がある。欧州委員会調査 57-61

185 そのほか、故意や目的といった主観的要素の立証の困難性、多くの国で親告罪であり、民事で和解されると、刑事の進行に影響が出ることも、原因としてある。欧州委員会調査 77

186 欧州委員会調査 77

187 欧州委員会調査 61-66

188 欧州委員会調査 78

189 欧州委員会調査 79-81

190 欧州委員会調査 76

第 4 章 営業秘密事件の実務

1　民事的救済措置の付与義務と救済措置の内容（EU 指令第 3 章第 1 節）

(1) 概要（第 6 条）[191]

① 加盟国が、違法な営業秘密侵害に対して、民事救済を可能とするために要される、手段、手続き、是正措置を用意しなければならない。

② 上記の手段、手続き、是正措置は、以下を充たす。

- 公正で衡平である
- 不必要に煩雑、あるいは、高額な、又は、不合理な時間的制約や不当な遅延に服するものでない
- 効果的で阻止力を有する

(2) 比例性と手続濫用（第 7 条）[192]

① 上記の手段、手続き、是正措置は、以下のように実施される必要がある。

- 比例性を有し
- 欧州連合内市場での正当な取引へ障害を設けることがない
- 濫用に対する予防策を用意する

② 加盟国は、司法機関が、被告/被申立人の申立てにより、営業秘密侵害が存在するとは到底認められない、又は、申立人が手続きを悪意で利用、若しくは、濫用している場合に、被告/被申立人への損害賠償や、申立人への制裁を含む適当な措置を命ずることができるようにする。上記の措置は、本案とは別の手続きとすることができる。

(3) 時効期間（第 8 条）[193]

① 加盟国は、営業秘密侵害に対する手段、手続、是正措置が、実体法上、又は、手続法上、利用可能な期間を一定期間に限定する。

② その期間は、6 年を超えてはならない。

(4) 法的手続中の営業秘密の秘密性の保持（第 9 条）[194]

① 関係者による正当な理由ある申立てに応じ、管轄権ある司法機関が、当事者、その訴訟代理人弁護士、若しくは、その他の代表者、裁判所職員、証人、専門家、及び、そ

[191] EU 指令第 6 条
[192] EU 指令第 7 条
[193] EU 指令第 8 条
[194] EU 指令第 9 条

の他の営業秘密の違法な取得、使用若しくは開示に関連する法的手続に参加している者、又は、これらの法的手続の一部を構成する文書にアクセスできる者が、手続参加、若しくは、アクセスの結果知ることとなった、営業秘密、若しくは、争いのある営業秘密を、秘密であると特定し、使用又は開示することを禁止することを、加盟国は保証しなければならない。加えて、加盟国は、管轄権ある司法機関が、職権で行動することを許すこともできる。

上述の守秘義務は、法的手続きが終了した後も、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。

- 最終決定により、営業秘密が、第 2 条に定められた要件を満たさないことが判明した場合
- 時間の経過とともに、情報が、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、管轄権のある司法当局が、当事者による正当な理由ある申立てに基づいて、営業秘密の違法な取得、使用若しくは開示についての法的手続で使用された、あるいは言及された営業秘密、若しくは、争いある営業秘密の、機密性を保持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にしなければならない。加えて、加盟国は、管轄権ある司法機関が職権でそのような措置を講じることを許すこともできる。

本項の措置は、少なくとも以下が利用可能とされなければならない。

- 当事者、又は第三者によって提出された、営業秘密、あるいは、争いある営業秘密を含む文書へのアクセスを、全体的若しくは部分的に、限られた数の者に制限すること。
- 営業秘密、若しくは、争いある営業秘密が、開示される可能性がある場合、公開法廷へのアクセスを制限すること、及び、それら訴訟手続に関する記録、あるいは写しへのアクセスを限られた数の者に限定すること。
- 上記限られた数の者に含まれる者以外の者が、営業秘密を含む文章が、削除、又は、編集された、司法判断の非秘密版を利用できるようにすること。

③ 前項の措置を決定し、それらの比例性を評価する場合、管轄権のある司法機関は、効果的な救済、並びに、公正な裁判を受ける権利、当事者の、並びに、適切な場合には、第三者の正当な利益、及び、前項の措置の許可、又は、拒否に起因して生じる、いずれかの当事者の、適切な場合は、第三者の、被りうる潜在的危害を考慮するものとする。

2　暫定的措置及び予防的措置（EU 指令第 3 章第 2 節）

(1) 暫定的措置及び予防的措置（第 10 条）[195]

① 加盟国は、管轄権を有する司法機関が、営業秘密保有者の申立てに応じ、侵害者に対し、以下の暫定的、並びに、予防的措置のいずれかを、命じることができることを保証する。

- 営業秘密の暫定的使用又は開示の停止、又は、事情によっては、それらの禁止
- 侵害品の製造、提供、市場展開、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
- 輸入品を含む、侵害の疑いのある物品の押収、若しくは、送付により、市場への流入、又は、市場内流通の防止

② 加盟国は、司法機関が、上記①に代えて、仮想的な営業秘密保有者への損害賠償を充足するに見合う保証金の預託を命じ、営業秘密の使用を許可することができる。

(2) 申立要件と保全策（第 11 条）[196]

① 加盟国は、管轄権ある司法機関が、第 10 条記載の措置に関し、次の事項について、満足できる程度に確実に示すことのできる、提出可能と合理的に見なされる証拠を、提出するよう、申立人に求める権限を有するものとする。

- 営業秘密が存在する
- 申立人が営業秘密の保有者である
- 営業秘密が違法に取得されたか、違法に使用、又は、開示されているか、営業秘密の違法な取得、使用、又は、開示が差し迫っている

② 加盟国は、管轄権ある司法機関が、申立ての許可、又は、却下の決定で、比例性を検討するに際して、必要に応じ、以下を含む当該事件の特殊な状況を、考慮に入れるようにする。

- 営業秘密の価値、及び、その他の特徴
- 営業秘密を保護するために講じられた措置
- 営業秘密を取得、使用、又は、開示する際の、被申立人の行為
- 営業秘密の違法な使用、又は、開示の影響
- 当事者の正当な利益、及び、措置の付与又は拒否が、当事者に与える可能性のある影響

[195] EU 指令第 10 条
[196] EU 指令第 11 条

- 第三者の正当な利益
- 公共の利益
- 基本的権利の保護

③ 加盟国は、管轄権ある司法機関が、下記の場合には、被申立人の申立てにより、措置の取り消し、効力の停止が行われるようにしなければならない。

- 申立人が、措置を命じる司法機関によって決定された合理的な期間内に、又は、20 営業日、若しくは、31 暦日のいずれか長い方を超えない期間内に、事件の実体的審理に至る法的手続を開始しなかった場合
- 当該情報が、被申立人に帰することができない事由により、第 2 条の営業秘密の要件を満たさなくなった場合。

④ 加盟国は、司法機関が、被申立人やその他の第三者に生じうる損失を、補償する保証金の預託を、申立人に命じることができるようにする。

3　本案判断から生じる措置（EU 指令第 3 章第 3 節）

(1) 差止命令及び是正措置（第 12 条）[197]

① 加盟国は、事件の実体について下された司法的判断が、営業秘密の違法な取得、使用、又は開示があったとした場合、管轄権ある司法機関が、申立人の求めに応じて、1 つ又は複数の、侵害者に対する以下の措置を命じうるものする[198]。

a. 営業秘密の使用、若しくは、開示の停止、又は、場合によっては、禁止
b. 侵害品の製造、提供、市場展開、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. 侵害品に関する適切な是正措置の採用
d. 営業秘密を含む、又は、具体化する文書、物件、材料、物質、若しくは、電子ファイルの全部、あるいは一部の破壊、又は、適切な場合、それらの文書、物件、材料、物質、若しくは、電子ファイルの全部、あるいは一部の、申立人への送付

② 上記の c. に記載の是正措置には、以下を含む。

- 市場からの侵害品の回収。
- 権利を侵害している物品から、権利を侵害している特徴を奪うこと。
- 権利を侵害している物品の破壊、又は、適切な場合は、市場からの撤退。但

[197] EU 指令第 12 条
[198] 損害賠償と異なり、故意、過失を問わない。第 14 条を参照。

し、その撤退によって、問題の営業秘密の保護が損なわれることはないことを要する。

③ 加盟国は、以下を規定することができる。

市場からの侵害品の撤退を命じるとき、管轄権のある司法機関は、営業秘密の保有者の要求に応じて、その商品を、保有者、又は、慈善団体に送付するように命じることができる。

④ 司法機関は、特段の事情がない限り、上記①c. 及び d. の措置は、侵害者の費用により執行されるよう命じることとする。

(2) 申立要件、保全策、代替措置（第 13 条）[199]

① 加盟国は、第 12 条の差止命令及び是正措置の申立てを検討し、それらの比例性を評価する際に、管轄権を有する司法機関が、以下を含む、事件の特殊な事情を考慮に入れることを要求するものとする：

- 営業秘密の価値、又は、その他の特徴
- 営業秘密を保護するために講じられた措置
- 営業秘密を取得、使用、又は、開示する際の、侵害者の行為
- 営業秘密の違法な使用、又は、開示の影響
- 当事者の正当な利益、及び、措置の付与又は拒否が、当事者に与える可能性のある影響
- 第三者の正当な利益
- 公共の利益
- 基本的権利の保護

管轄権を有する司法機関が、上記（第 12 条）第①項 a. 及び b. の措置の期間を制限する場合、侵害者が営業秘密の違法な取得、使用、又は、開示から得た可能性のある、商業的、若しくは、経済的利益を払拭するのに、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、被申立人に直接的又は間接的に帰することができない理由のための第 2 条第① 記載の要件をもはや満たさない場合、被申立人の要求に応じ、上記（第 12 条）第① 項 a. 及び b. の措置が取り消されるか、又は、効力を失うものとする。

③ 加盟国は、第 12 条の措置を命じるにあたり、次の条件が充たされる場合、措置の対象者の申立てにより、金銭的賠償をもって代えうることを規定する。

[199] EU 指令第 13 条

- 使用、又は、開示の時点で、申立人は、その状況下で、営業秘密を違法に使用、又は、開示している他の者から、営業秘密が取得されたことを知らなかったし、知りうべきではなかった。
- 措置の執行が、申立人に不相当な危害をもたらす。
- 原告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。

(3) 金銭的賠償（第 14 条）[200]

① 加盟国は、管轄権のある司法機関が、損失を被った当事者の申立てに応じて、営業秘密の違法な取得、使用、又は、開示に従事していることを知っている、又は知るべきであった侵害者に、営業秘密の違法な取得、使用、又は開示の結果として被った、営業秘密保有者の実際の不利益を補償するのに適切な損害賠償支払いを命じるものとする。加盟国は、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、制限することができる。

② 前項の損害賠償を算定する場合、管轄権のある司法機関は、被侵害者が被った利益の損失、侵害者による不当な利得、経済への悪影響など、すべての適切な要素を考慮に入れるものとし、さらに、営業秘密の違法な取得、使用、又は開示によって、営業秘密の保有者に引き起こされた道徳的偏見など、経済的要因以外の要素も、妥当と判断される限り、考慮されるものとする。

③ 司法機関は、適切な場合には、侵害者が、営業秘密を使用するライセンスを求めた場合に支払われるべき、最低限のロイヤルティ、若しくは、手数料額等の要素に基づいて、損害賠償を一括支払額として算定することができる。

(4) 制裁（第 16 条）[201]

EU 指令第 9 条、第 10 条、及び第 12 条の措置に従わない者に対しては、司法機関による制裁を課すことができるようにするものとする。また、第 10 条、第 12 条の不遵守に対しては、定期的な違反金の支払を命じることができるものとする。

4 行政措置

(1) 欧州連合

欧州連合では、不正競争に関し、欧州委員会が捜査、訴追する権限を有する。しかし、営業秘密の不正取得、使用を不正競争とした事例は見当たらず、むしろ、営業秘密を他社にシ

[200] EU 指令第 14 条
[201] EU 指令第 16 条

ェアすることを拒否した行為、競争者間での共同での使用を、不正競争防止に関して問題としたことがある[202]。技術移転ブロック除外規制[203] と 研究開発ブロック除外規制[204]は、営業秘密の取り扱いについて言及しているが、ライセンスはむしろ競争促進的であると考えられている[205]。

これに対し、秘密保持契約については、その競争阻害的側面が問題となりうる。もともと、英国、ギリシャ、イタリア、スロベニアでは、規制当局が特に、独占的、又は、寡占的地位にある者が、情報を秘匿し、秘密保持契約に存在する反競争法的問題を規制してきたとされている[206]。

2018 年 5 月に制定されたヨーロッパの一般データ保護規則（GDPR）は、ヨーロッパ市民に関するデータを扱う企業が、市民のプライバシーに関わるデータを収集、保存、移転する場合に、様々な保護措置等を課すべきことを定めており、情報が収集されている市民に対して、どのような収集がされているかの適切な開示がない場合に、制裁を課すことができるものとなっている[207]。Google に対して、フランスの情報保護当局が、5000 万ユーロの罰金を課した事実は有名である[208]。即ち、情報が個人のプライバシーに関わる場合には、開示が強制されることがあり、営業秘密保護を一定程度制限する。

更に、現在立法化が検討されている The Digital Markets Act（DMA）では、Google などのサーチエンジン、SNS などプラットフォームの運営者に対して、データのシェアを義務づけることで、情報の独占を防止しようとする[209]。

(2) 加盟国当局の規制

ヨーロッパ全体で、営業秘密の不正取得等に関し、不正競争法違反として訴訟が提起され

---

[202] 例えば、Case T-201/04, Microsoft Corp. v. Comm'n, 2004 O.J. (C 179) 36; Case T313/05, Microsoft Corp. v. Comm'n, 2005 O.J. (C 257) 31. Katarzyna A. Czapracka, Antitrust and Trade Secrets: The U.S. and the EU Approach, 24 Santa Clara High Tech J. 207, 209 (2008)
競争会社間での価格設定の合意など、明らかな独占禁止法の違反となる行為は、規制されると考えられている。欧州委員会調査、脚注 177、9-10 頁
https://ec.europa.eu/docsroom/documents/14838/attachments/1/translations/en/renditions/pdf

[203] The Transfer of Technology Block Exemption Regulation EC/772/2004

[204] The Research and Development Block Exemption Regulation EC/1217/2010

[205] 欧州委員会調査、脚注 177、9 頁

[206] 欧州委員会調査、脚注 177、50 頁

[207] General Data Protection Regulation、規則(EU) 2016/679

[208] Adam Satariano, Google Is Fined $57 Million Under Europe’s Data Privacy Law, The N.Y. Times (Jan. 21, 2019) https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html.

[209] 第 7 章「営業秘密関連の法改正」を参照

ることは稀であり、営業秘密の利用が反競争的とされることも稀とされる[210]。ベルギーでは、競争当局や財務省が職権で、営業秘密事件の捜査を行うことがある。中産階級大臣の要請、公共団体その他の特定の公的機関、若しくは、自然人又は法人の苦情の後、競争に対する危害が発生した場合にも、捜査や訴追がなされることがある[211]。ブルガリアでも、競争企業間で営業秘密の不正取得等がなされた場合に、行政的措置が行われる事が可能となっている[212]。

第 5 章　域外適用

EU 指令は、欧州連合内の加盟国に対する拘束力を持つ文書であるところ、同指令が対象とする侵害行為、侵害者について、地域的、地理的な制限、あるいは、国籍上の制限は明記されていない[213]。また、「侵害品」の輸出入が侵害行為に含まれており[214]、営業秘密の不正取得が、裁判地内で起きたことを厳格に必要としないようにも読める。

しかし、EU 指令は、準拠法や管轄権の問題について、明確に扱うことは企図しておらず、欧州連合の既存の法律で決定されることとなることを前提としている[215]。したがって、各加盟国で保護される営業秘密について、準拠法、域外適用についても、各国の判例法、欧州連合の関係する法律により決定される。

第 6 章　営業秘密侵害の事件数

営業秘密の本案訴訟事件、あるいは、暫定的措置申立事件の処理について、全事件数、処理状況を公開しない加盟国が多く、公開された全事件数として把握することはできない。

なお、欧州連合が行った調査で、営業秘密侵害の被害を受けた（又は、未遂事件があった）と返答した、 140 社のうち、わずか 57 社（40.7%）が、裁判所における救済を求めたと回答している。救済を求めなかったと回答した者のうち、その理由としては、証拠収集が困難で

---

[210] 欧州連合知的財産権局、営業秘密訴訟のベースライン（2018）（「ベースライン」）、47,48 頁
[211] ベースライン、24 頁
[212] ベースライン、34,35 頁
[213] EU 指令第 1 条
[214] EU 指令第 4 条
[215] EU 指令序文第 37 段落「この指令は、司法協力、管轄権、民事及び商事に関する判決の承認と執行のための調和のとれた規則を確立すること、又は、準拠法に対処することを、目的としていない。そのような問題を一般に扱う、他の文書が、原則として、この指令の対象分野に、等しく適用され続けるべきである。」
しかし、違法とはならない情報開示行為等について、「連合法又は国内法にしたがって」と限定が加えられていることなど、地理的な要素が関係する場面は否定できない。EU 指令第 5 条

あったこととした者が最多であった[216]。裁判所において救済を求めた者のうち、以下のとおりに、救済が得られた[217]。

- 証拠の捜索と確保の保全措置(32%)；
- 損害賠償等の金銭的賠償（32%)；
- 侵害者に対する刑事制裁(30%)；
- 侵害行為を禁止する差止命令(28%)；
- 決定の刊行物への公開(15.8%)；
- 侵害品の破壊(10.5%)；
- 税関で侵害品を没収するとの命令(3.5%)；
- 上記のいずれも得られず(17.5%)。

第 7 章　営業秘密関連の法改正

営業秘密自体ではないが、一部大企業のデータ収集と使用に関係し、個人情報保護のほか、競争を実効化し、消費者を保護しようとする法律の制定が予定されている。欧州委員会は 2020 年 12 月、使用・運営の自由を原則としてきたインターネットに、大幅に変化をもたらす、インターネットを利用する消費者、中小企業のアクセスの自由の実質的保障、競争阻害の防止を目的とした 2 つの法案を提出し、現在も立法化が進んでいる。

1　営業秘密法

EU 指令が 2016 年に策定された後、新たな法制度改正は現在までなされていない。改正の動きは未だない。

2　デジタル化競争政策

2020 年以来、The Digital Markets Act（DMA)、The Digital Service Act（DSA)の立法化が進んでいる。[218]DMA は、欧州連合市場内での、インターネット上のプラットフォームの運営と使用に関連しており、市場競争の促進を目的とする[219]。他方、DSA は、プラットフォームに

---

[216] 欧州委員会調査、脚注 177、143 頁
[217] 欧州委員会調査、脚注 177、144 頁
[218] 欧州議会、立法電車スケジュール（DMA 経過) (最終アクセス日 2022 年 2 月 18 日) https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-digital-markets-act. 欧州議会、立法電車スケジュール（DSA 経過) (最終アクセス日 2022 年 2 月 18 日) https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-digital-services-act.
[219] DMA 序文

アクセスするユーザーに対して、情報管理システム、実態の透明化、ユーザーの安全確保、誤用や濫用に対する責任の所在の明確化を目的とする[220]。

欧州委員会は、３つのオプション（規制対象者や規制内容が固定されたものから、可動性ある、柔軟な仕組みまで）のうち、第２の部分的に柔軟な仕組みを採用することとし、規制対象者は指定されるものの、規制内容については逐次変更ができるようにした。IoT の急速な発展に合致した、柔軟な規制という点で特徴がある。

DMA と DSA は、企業が欧州内に営業所を置かない場合にも、規制対象とするものであり、域外適用とは言えないが、欧州連合内の法益が脅かされるのであれば、対象者に対する管轄権を緩和・拡張して及ぼす点で、GDPR と同様である。

(1) 規制対象者：ゲートキーパー

① 以下で「コアプラットフォームサービス」とは、下記のいずれかを意味する[221]。

a. オンライン媒介サービス
b. オンライン検索エンジン
c. オンラインソーシャルネットワーキングサービス
d. ビデオ共有プラットフォームサービス
e. 番号に依らない対人コミュニケーションサービス
f. オペレーティングシステム
g. クラウドコンピューティングサービス

② ゲートキーパーは、以下の条件を充たす、コアプラットフォームを意味する[222]。

a. 連合内市場に重大な影響を及ぼす（みなし規定があり、少なくとも 3 つの EU 加盟国でのコアプラットフォーム活動[223]があること、及び、例えば、資本時価総額が 650 億ユーロ以上と考えられる場合、本要件に該当する）。
b. ビジネスユーザーがエンドユーザーに到達するための、重要なゲートウェイとして機能する、コアプラットフォームサービスを運用する（少なくとも月間 4500 万人のアクティブなエンドユーザーを有し、年間 1 万人のアクティブなビジネスユーザーがいる、という閾値をみたすことで、本要件を充たすことが、当初法案で

[220] DSA 序文
[221] DMA 第 2 条（2）
[222] あるいは、欧州委員会の調査により、適用可能であると判断される場合。DMA 経過、脚注 218
[223] 2021 年 9 月に提出された、欧州議会内、市民の自由、正義、内務に関する委員会意見は、媒介サービスを拡大し、例えば、金融機関でウェブサービスを行う者も含めるべき、とした。DMA 経過、脚注 218

規定されている）。

c. その運用において、固定した、持続性のある地位を享受する、若しくは、近い将来にそうした地位を享受すると予期される（過去 3 年間で、上記 b. が充たされた場合には、本要件に該当するとされる）。[224]

なお、欧州連合議会の主要な政党は、2021 年 11 月 17 日、市場の売上高が 800 億ユーロ以上、少なくとも一つのインターネットサービスの提供を行う者を規制対象とすることに合意した（Reuter 報道による）[225]。

(2) 規制内容

① ゲートキーパーの義務

第 3 条（7）に従って特定された、コアプラットフォームサービスのそれぞれに、ゲートキーパーは、以下の義務を負うと規定する[226]。

i. これらのコアプラットフォームサービスから供された個人データを、ゲートキーパーが提供するその他のサービスから得た個人データ、若しくは、第三者のサービスから得た個人データと結合させ、又は、個人データを組み合わせるため、他のゲートキーパーが提供するサービスへ、エンドユーザーをサインインさせることは、エンドユーザーに、特別に当該選択肢を提示し、同意を受けていない限り、やめなければならない。

ii. ビジネスユーザーが、エンドユーザーに、ゲートキーパーのオンライン媒介サービスを通じて提供される、製品又はサービスを、当該価格とは異なる価格又は条件で、第三者のオンライン媒介サービスを通じて、提供することができるようにしなければならない。

iii. ビジネスユーザーが、コアプラットフォームを介して取得したエンドユーザーに、サービスオファーを宣伝できること、ビジネスユーザーが、そのためにゲートキーパーのコアプラットフォームサービスを使用するかどうかに関係なく、これらのエンドユーザーとの契約を締結できること、及び、ゲートキーパーのコアプラットフォームサービスを介した、ビジネスユーザーのソフトウェアアプリケーションを使用して、エンドユーザーが、ゲートキーパーのコアプラットフォームを使用しない形で、ビジネスユーザーから取得した、コンテンツ、サブスクリプション、機能、又は、

[224] DMA 序文
[225] Reuter, EU lawmakers agree on rules to target big tech- FT (Nov. 17, 2021)
[226] DMA 第 5 条

その他のアイテムを、アクセス、若しくは、使用すること、を可能としなければならない。

iv. ビジネスユーザーが、ゲートキーパーの事業に関連する公的監督機関に、問題を提起することを防止、又は、制限することは、やめなければならない。

v. ゲートキーパーのコアプラットフォームを介して、ビジネスユーザーが提供するサービスに際して、ゲートキーパーの識別サービスを、使用、提供、相互操作するように、ビジネスユーザーに要求することは、やめなければならない。

vi. 本条に規定されたゲートキーパーのコアプラットフォームサービスに、アクセス、加入、登録するための条件として、ゲートキーパーのその他の第3条規定のコアプラットフォームサービスサービスに、若しくは、第3条(2)(b)の閾値を充たすものに、参加、登録をすることを、ビジネスユーザー、あるいはエンドユーザーに、要求してはならない。

vii. 広告サービスを供している広告主、及び、掲載者に対し、その求めに応じて、ゲートキーパーによって提供される、特定の広告の公開、及び、関連する広告サービスのそれぞれについて、掲載者に支払われた金額又は報酬に加え、広告主及び出版社が支払った価格に関する情報を提供しなければならない。

② 特に指定されたゲートキーパーの義務

ゲートキーパーは、第3条(7)規定に従い、コアプラットフォームサービスのそれぞれについて、下記義務を負う[227]。

i. コアプラットフォームサービスのビジネスユーザーの活動を通じて、あるいは、ビジネスユーザーのエンドユーザーの活動を通じて、生成され、利用可能となった非公開のデータ、及び、コアプラットフォームサービスのビジネスユーザーによって提供される、若しくは、これらのビジネスユーザーのエンドユーザーにより提供される、非公開のデータを、ビジネスユーザーと競争して使用することは、やめなければならない。

ii. 技術的に、第三者によってスタンドアロンベースで提供することのできない、オペレーティングシステム、又は、デバイスの機能に不可欠なソフトウェアアプリケーションに関連し、ゲートキーパーが制限する可能性を損

[227] DMA 第6条

なうことなく、エンドユーザーが、コアプラットフォームサービスにプリインストールされているソフトウェアアプリケーションを、アンインストールできるようにしなければならない。

iii. 当該ゲートキーパーのオペレーティングシステムを使用、若しくは、相互運用している、第三者のソフトウェアアプリケーション、又は、ソフトウェアアプリケーションストアのインストールと、効果的な使用を、許さなければならない。これらのソフトウェアアプリケーション又はソフトウェアアプリケーションストアが、ゲートキーパーのコアプラットフォームサービス以外の手段で、アクセスされることを許さないとならない。ゲートキーパーが提供するハードウェア、又は、オペレーティングシステムの万全性を危険にさらすことがないように、第三者のソフトウェアアプリケーション、ソフトウェアアプリケーションストアを確実にするための、相当な措置を、ゲートキーパーがとることを妨げてはならない。

iv. ゲートキーパー自体、又は、同じ事業に属する第三者によって提供されるサービスや製品を、第三者の同様のサービス又は製品と比較し、ランク付けにおいてより有利に扱うべきでない。そのようなランキングには、公正かつ無差別の条件を適用しなければならない。

v. エンドユーザー向けのインターネットアクセスプロバイダーを含め、ゲートキーパーのオペレーティングシステムを使用してアクセスする、さまざまなソフトウェアアプリケーションとサービスに、エンドユーザーが切り替え、又は、参加する機能を技術的に制限してはならない。

vi. 利用可能な、又は、ゲートキーパーによる付帯サービスの提供で使用されている、同じオペレーティングシステム、ハードウェア、又は、ソフトウェア機能を、ビジネスユーザーと付帯サービスのプロバイダーが、アクセスをしたり、相互運用性を持つように許さなければならない。

vii. ゲートキーパーのパフォーマンス測定ツール、及び、広告主と出版社が独自に広告枠を独立して検証するために必要な情報を、広告主とサイト運営者に対し、それらの申請に応じて、無料で提供しなければならない。

viii. ビジネスユーザー、若しくは、エンドユーザーの活動を通じて生成されたデータの、効果的な移行性を提供しなければならない。継続的、リアルタイムのアクセスの提供を含め、特に、エンドユーザーが、EU 2016/679 規則に準拠して、データ移行性を行使することを、促進するツールを提供しなければならない。

ix. ビジネスユーザー、並びに、それが提供する製品又はサービスを受けるエンドユーザーによる、関連コアプラットフォームサービス使用のコンテキストで、提供、若しくは、生成される、集約データ又は非集約データを、ビジネスユーザー又はビジネスユーザーが承認する第三者に、効果的、高品質、継続的、かつリアルタイムの、アクセス、ないしは使用を無料で許さなければならない。個人データについては、関連するコアプラットフォームサービスを通じて、関連するビジネスユーザーによって提供される、サービス、若しくは、製品に関して、エンドユーザーによってなされた使用に直接に関連する場合のみ、かつ、エンドユーザーが、規則（EU）2016/679 の意味で、その共有を選択する旨の同意（オプト・イン）したときに限り、アクセス、ないしは使用を許すことができる。

x. オンライン検索エンジンの第三者プロバイダーに、その申請により、ゲートキーパーのオンライン検索エンジンで、エンドユーザーに生成された、無料検索と有料検索に関連するデータのランキング、検索、クリックと表示に対するアクセスを、公正、合理的、非差別的な条件で、また、個人データを構成する、検索、及び、クリックと表示は、匿名化の上、提供しなければならない。

xi. 第 3 条に従って指定されたソフトウェアアプリケーションストアへの、ビジネスユーザーのアクセスの、公正で差別のない一般的条件を適用しなければならない。

③ 義務の例外的停止[228]

第 32 条（4）の諮問手続に従って、ゲートキーパーは、特定の義務の遵守が、ゲートキーパーの責に帰すことができない、例外的な事情により、ゲートキーパーの欧州連合内事業の経済的存続可能性を危うくすることを理由として、そのような存続可能性の危険に対処するために必要な範囲でのみ、特定の義務の停止を求めることができる。

④ 義務の免除[229]

第 32 条（4）の諮問手続に従って、欧州委員会の職権により、又は、ゲートキーパーの申請により、全体的又は部分的に、第 3 条（7）に従い特定された個々のコアプラットフォームサービスに関連して、第 5 条及び第 6 条に規定の義務から免除するこ

[228] DMA 第 8 条
[229] DMA 第 9 条

とができる。

(3) 規制の実施

DMA では第 5 章以下に、事業者が義務に違反している場合に対する規制執行手続が、具体的に記載されている。欧州連合レベルでは、通信ネットワーク、コンテンツ、テクノロジー総指令局が、DMA, DSA の 2 法の所轄官庁となる。新たに創設が提案されている、欧州デジタルサービス委員会（EBDS）は、独立した諮問グループとして機能し、各国の規制当局を補助するとされる。

第 26 条では、第 25 条に基づく違反決定に際して、年間売上高の 10%を超えない罰金を課しうるとしている[230]。このような欧州委員会の決定は、CJEU により審査される。

(4) 立法化に対する加盟国の対応、経済社会的影響の予測

ドイツ、フランス、オランダは、DMA が、各加盟国の競争法当局に、より柔軟に規制を行う権限、拡張された規制手段を付与するよう求めている。加盟国の競争法当局は、一致して、競争法当局の権限の拡大を考慮するように声明を出している[231]。

また、もし DMA が成立すれば、米国に拠点を置く、Google 他の情報通信関連主要 5 社に対して、プラットフォーム上で運営しているユーザーが生成したデータに、ユーザーがアクセスできるようにし、第三者がそのようなプラットフォーム運営者のサービスに互作動性を持つサービスを提供できるように要求するというものである。 現在のところ、そのようなプラットフォームの運営主体である Google、Apple、Amazon、Facebook、Microsoft、Alibaba Group、Bookings.com に適用されるとされる[232]。

3 デジタルサービス適正化

DSA は、近年問題となっている、オンラインでの偽造品、悪意のある表現（ヘイトスピーチ）、偽情報の広がり等、オンラインを利用した違法な取引、違法なコンテンツ配信、その他の危害を及ぼす行為に対して規制し、利用者を保護することを目的とする。即ち、プラットフォームに対し、コンテンツの適正化、プラットフォーム運営の透明化、ユーザーの安全確保、誤用や濫用に対する責任の所在の明確化を求めるもので、2000 年に制定された e-

[230] DMA 第 26 条
[231] 欧州議会、立法電車スケジュール（DMA 経過) (最終アクセス日 2022 年 2 月 18 日) https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-digital-markets-act.
[232] Reuter, 脚注 225;Makenzie Holland, EU's Digital Markets Act could affect US job growth, TechTarget (Nov. 5, 2021), https://searchcio.techtarget.com/news/252509188/EUs-Digital-Markets-Act-could-impact-US-job-growth.

Commerce Directive の改正を伴う。

企業が欧州内に営業所を置かない場合にも規制対象とするものであり、欧州連合内の法益が脅かされるのであれば、対象者に対する管轄権を緩和・拡張して及ぼす[233]。

(1) 規制対象者

オンライン媒介サービスに適用があり、オンラインでの役割、規模、オンラインエコシステムへの影響に応じて、オンライン媒介業者のカテゴリーを設け、異なる義務を課す[234]。

① ネットワーク基盤プロバイダーによって提供される媒介サービス：コンジットサービス」（例：インターネットアクセス）及び「キャッチサービス」（例：情報の中間的、及び、一時的な自動保存）；

② 情報を保存および配布するプロバイダーによって公衆に提供されるホスティングサービス（クラウドやウェブホスティングサービスなどの）

③ 売り手と消費者を結びつけるプロバイダーによるオンラインプラットフォームサービス。オンラインマーケットプレイス、アプリストア、共同経済プラットフォーム、ソーシャルメディアプラットフォーム;

④ 非常に大規模なオンラインプラットフォーム（又は VLOP）は、月間アクティブユーザー数が 4500 万人を超えるプラットフォームで、特に、経済と社会に特定の影響を与え、違法なコンテンツや社会的危害の流布にリスクを含むため、特定のルールが設定されている。

(2) 規制内容

① DSA の範囲内にあるオンライン媒介サービスの、すべてプロバイダーに適用可能な基本的な義務として、サービスの透明性と基本的権利保護する義務が含まれる。これには、そのサービス使用に対し、課す可能性のあるすべての制限を明記する義務が含まれる。

② アルゴリズムによる意思決定レビューなど、コンテンツのモデレーションの目的で使用されるツールの使用を含む、これらの制限を適用、及び、実施するにあたり、責任を持って行動することが要求される[235]。

③ 違法なコンテンツと見なされる、又はプロバイダーの利用規約に違反した情報の削除と無効化について報告する必要がある[236]。

[233] DSA 第 1 条
[234] DSA 第 2 条
[235] DSA 第 12 条
[236] DSA 第 13 条

④ 最後に、すべての媒介者は、加盟国の当局、及び、その他の管轄当局との直接のコミュニケーションを容易にする単一の連絡先を届け出[237]、欧州連合外のものは、欧州連合内の法定代理人を指名する[238]

（加算義務）	媒介サービス	ホスティングサービス	オンラインプラットフォーム	特大プラットフォーム
透明性報告	●	●	●	●
基本的権利によるサービス条件の制約	●	●	●	●
命令後の加盟国当局との協調	●	●	●	●
連絡先、必要な場合は法定代理人	●	●	●	●
通知と行動、 利用者への情報提供義務		●	●	●
訴えと是正、裁判外解決			●	●
信頼された警告			●	●
濫用的通知と対抗的通知への措置			●	●
取引相手の信用調査			●	●
オンライン広告の利用者向け透明性			●	●
犯罪通報			●	●
リスク管理義務と遵守担当役員				●

[237] DSA 第 10 条
[238] DSA 第 11 条

外的リスク監督と公共への説明義務				●
推薦システム透明化と情報アクセスへの利用者選択				●
監督庁や研究者とのデータシェア				●
行動規範				●
緊急事態対応協力				●

(3) 規制の実施

所轄は、国内の規制実施に対して責任を負うデジタルサービスコーディネーター、及び消費者保護委員会（IMCO）となる予定である。DSA の内容とする義務が果たされているかは、当該プロバイダーの主な営業拠点が置かれている加盟国により監督される[239]。また、各加盟国は、規制違反に対して、効果的で比例した、抑止的な罰金を用意する[240]。

(4) サイバーセキュリティ政策

増えつつあるサイバー犯罪による機密情報の漏洩については、特に、米国で規制が強化されているが、欧州連合においても、重点的に安全性を強化する政策が近年拡充してきている。

第 8 章　国際協力・他国との連携状況

EU 指令は、欧州連合加盟国内で、一貫した保護が営業秘密保有者に付与されることを目的としているので、加盟国内の連携を勧奨し、指令の発効後、定期的に調査報告書が作成されて、欧州委員会に検討されるように予定している。

また、EU 加盟国間の司法、内務関係協力は、欧州連合条約第 6 編に包含されており、同条約は、「共通の関心事項」に関して協力活動が行われうること、具体的な分野として、民事司法、刑事司法での共助が含まれることを規定する[241]。現在の EU の司法共助・内務協力の活動は、1995 年 12 月に採択されたマドリッド欧州理事会による指針に基づいて行われている

[239] DSA 第 40 条
[240] DSA 第 42 条
[241] 欧州連合を設立する条約

[242]。

EU 加盟国間での捜査共助を調整する機関として知られているユーロポールは、1995 年 7 月に署名されたユーロポール設立条約を根拠に、1998 年 10 月 1 日に正式発足した組織であり、設立後、現在まで機能している。各加盟国は、中央当局からユーロポールを通じて、他の加盟国に対して刑事事件の捜査等へ国際共助を要請することが可能となる。ユーロポールは、EU 他加盟国へ、重大な犯罪への捜査協力の目的で捜査、訴追の協力の要請をする中継機関、情報収集機関となっている[243]。中でも、犯罪による収益を追跡し、犯罪物品を没収する機能があるとされ、仮に、国際共助を得られれば、国際的経済犯罪に、捜査、訴追だけでなく、犯罪収益の被害者への還元に有用な手段が得られ、重要な犯罪阻止につながる情報を収集できる可能性がある[244]。

日本は、EU との間で犯罪捜査に相互に協力するための条約を締結しており、上記のような、欧州内での国際犯罪捜査、訴追の協力に匹敵した協力要請を行いうる[245]。例えば、犯罪者の所在地の特定、物件の取得や引渡し等が想定されている[246]。国際司法共助の中で、最も迅速、効果的に協力が得られることが可能と期待されるのは刑事事件であるものの、欧州加盟国内では、営業秘密の不正な取得等を、刑事事件として捜査、訴追する実務は殆どなく（ドイツで存在するも、非常に少数である）、営業秘密の刑事事件に関する司法共助を、欧州から十分に得られるかには、不明な点が多い[247]。

この点、EU 指令が制定され、各加盟国で新法が制定、施行されたこと、営業秘密に対する欧州連合内の法的枠組みが相当程度統一され、また、救済が強化されたことは、重要な意味を持つ。最低限の営業秘密保護を与え、侵害に対する民事的な救済措置を整備する結果、欧州連合内に十分な営業秘密の民事的保護のない国が無くなり、欧州連合内の隣接国で侵害行為を行うことで、少なくとも、法の網の目をくぐって営業秘密を不正取得するなどし、民事責任を免れることはできなくなった[248]。

EU 指令により、著作権、商標権、特許権などの知的財産権に比較しうる保護が受けられる

---

242 千田恵介、EU の司法・内務協力の現状（1999）
243 千田恵介、EU の司法・内務協力の現状（1999）
244 千田恵介、EU の司法・内務協力の現状（1999）
245 刑事に関する共助に関する日本国と欧州連合との間の協定（外務省の HP に情報がまとめられている。https://www.mofa.go.jp/mofaj/gaiko/treaty/shomei_47.html）
246 刑事に関する共助に関する日本国と欧州連合との間の協定
247 下記「英国の営業秘密制度」を参照（英国では、営業秘密侵害自体を、刑事処罰する法令がない）
248 従前より、保護の強い国へ、営業秘密侵害行為により可能となった製品を輸出する行為について、法的権利を行使することは、共犯者とみなされうるような例外的な場合に、一部の国で可能と考えられたものの、非常に困難であった。本書「ドイツ」「英国」編を参照。

ようになった反面、大半の加盟国で、営業秘密は依然として、「知的財産」権には含まれていない[249]。したがって、営業秘密の保有者が水際で侵害品を摘発し、差し押さえたりなどすることは、EU 法に基づいた形態では不可能である。その結果、営業秘密は、国境において税関職員が侵害品を摘発するといった形で行政的に権利を実現する手段を有しない。但し、水際の救済策は、加盟国の国内法で付与することは不可能ではないので、加盟国ごとに検討がなされる必要がある[250]。

第 9 章　仲裁の利用

公開された事件数は見当たらなかったが、営業秘密事件を仲裁手続で解決することは増加していると思料される[251]。

第 10 章　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

EU 指令により、営業秘密は、「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」と定義され[252]、「情報を合法的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」ことが要件となったため、各加盟国法上も、機密情報や営業秘密を、秘密保持義務への合意のないまま、第三者に提供することは、それらの「機密性」を失わせる結果となりかねない[253]。具体的な当事者間の事実関係によらず、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）を明文で盛り込む必要がある。

ライセンスを受けるなどして、機密情報あるいは営業秘密を保持する者が、「秘密性を保持するための合理的な措置」を取っているか否かは、以後の営業秘密の保護に重要な事実として関わってくる。EU 指令では、具体的にどの程度の秘密性保持のための措置が「合理的」とみなされるか、及び、どのような状況下で、問題となった情報が「容易にアクセスできない」情報であるかについて、明らかにされていない。秘密保持義務の内容は、各加盟国の裁判例に応じ、決定される必要があり、そのうち、重要な事項は、秘密保持契約書内に明記さ

[249] EU 執行指令（知的財産権の執行指令 2004/48 / EC ）、EU 関税執行規則（知的財産権の関税執行に関する規則（EU）No608/2013）
イタリア、ポルトガルは明文で知的財産権に含めており、フィンランドでは、判例上含められ、フランスでは、製法の営業秘密だけを含めている。Intellectual Property Office of European Union, Baseline of Trade Secrets Litigations in EU Member States (2018)
[250] Mr. Williams 氏インタビュー
[251] 英国の営業秘密保護、第 9 章「仲裁の利用」を参照。
[252] EU 指令第 2 条
[253] 第 1 章「営業秘密の定義」を参照。

れるべきである[254]。

（1）ライセンシーにおいて、機密情報、営業秘密を、機密性の程度に応じたラベルをすること、（2）ライセンシー従業員の機密性保持の指導、（3）情報が、業務を実行するため少なくとも潜在的にアクセスを必要とする人にのみ開示されている（「知る必要があるベース」）、（4）情報の開示を受ける者は、秘密保持義務に拘束され、情報に関して、この秘密保持義務を負っていることを認識していることの確認、などが、プラスの要素となるため、ライセンス契約の記載に含めることが推奨される。

ドイツのライセンス契約に含まれる秘密保持契約の参考例は、他の加盟国でもある程度参考となる。ライセンス、生産委託、合弁会社設立の際に、当事者間で契約書がかわされる場合、機密保持条項は、通常含まれている。なお、契約の準拠法を決定する場合には、営業秘密保有者の利益が保護されるべき地域と、相手方の事業地域と合わせて検討されることになると考えられる[255]。

1　ライセンス契約

(1) 機密情報、営業秘密の特定

ライセンス契約で秘密保持義務を定める場合、機密情報、営業秘密を特定しておくことは重要である。また、EU 指令は、以下の情報を営業秘密から除外している。

a. 独立した発見や創造
b. 一般公衆が入手可能であった、若しくは、営業秘密の取得に法的制約を課されていなかった入手者が所持していた、製品や物品の観察、研究、解体、又は、検査
c. 連合法や法令、慣習に則った、情報及び諮問を得られる、労働者あるいは労働組合の権利の行使
d. その他、行為時の状況下で、誠実な商慣習に合致した行動

特に、上記 d. に該当する情報が何かが不明確であるところ、契約条項で、適用になる範囲が明確な形で、機密情報、営業秘密が定義され、それが保護されるべきと通常考えられるものであれば、そのような情報を許可なく（権限なく）取得、開示、使用することは「誠実な商慣習に合致」したとは言い難いと考えられる。

したがって、明確で、保護の必要性とバランスのとれた定義とすることが、最終的には、価値ある営業秘密の実効的保護を実現すると言える。また、広範囲すぎる、不明確な条項は、履行が困難であり、現実的でもない。情報の機密性のラベルは、明確化に資し、可能であれ

[254] Stuttgart Court of Appeal, Judgement of 19 November 2020 – 2 U 575/19, GRUR-RS 2020, 35613
[255] 第 5 章「域外適用」の記述を参照。

ば、採用されるべきと考えられる。

(2) 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

契約条項を作成する場合、何が許されるか、そして、何が不正取得、使用、又は、開示になるかを明確にすることは、ライセンシー及びライセンサーの利益を守り、また、有効な関係を維持するためにも大切である。例えば、ライセンシー側で、パスワード等アクセス制限を設定すること、アクセスできる者を、一定の被用者、関係会社の被用者、専門家、監査人等に制限すること、アクセスの目的と使用方法を制限することなどが考えられる。

侵害行為者が、営業秘密の不正使用、開示、取得にあたる事実を認識していたことや、認識すべきであったことが、営業秘密侵害の前提とされており、許可事項と不許可事項を分別することが意味を持つと考えられる。

(3) 契約終了後の情報の返却あるいはデータ削除義務

秘密保持義務の内容として、提供された機密情報、営業秘密は、契約関係終了時に保有者に返却すること、また、バックアップも含めて、保存されたデータから削除するように要求すること、それを確認することの 2 点を明記することが必要である。これは前記の、機密性を保つ合理的な措置の認定にも、プラスの要素として働くと考えられる。

(4) 補償条項

相手方の秘密保持義務違反の結果生じた損害について、相手方に補償の義務を負わせることは、契約に含められることが少なくない。

(5) 損害額

機密情報・営業秘密保有者は、不正取得、使用、あるいは、開示により生じた損害に対する賠償として、特約がない場合、自分の被った損害を立証して、その填補を求めることができる。この損害の立証は、裁判上困難となることも考えられるので、損害額の算定について、事前に合意しておくことも考えられる。

(6) 仲裁合意

裁判による紛争解決と比較し、仲裁は、営業秘密、機密情報の保護に適していると一般に考えられている。この理由として、営業秘密保有者が主張した内容、提出あるいは開示した情報の秘密性が保たれることが、通常あげられる。そこで、ライセンス契約にあたっても、仲裁条項を挿入して、仲裁により契約の紛争を解決し、ライセンサーとライセンシーの双方の機密情報や営業秘密の保護を図ることは、積極的に検討されるべきである。

2　生産委託契約

上記に列挙した注意点は、生産委託契約にも当てはまる。

委託者としては、受託者の生産ラインの運営状況、生産品の数量等確認体制、保存・管理状況を十分確認することが、特に重要となると考えられる。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は検討されるべきである。

生産委託契約では、受託者が、第三者の機密情報、営業秘密情報をたまたま持っていて、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請求をおこされてしまう可能性がある。委託者自身が知り得ない場合、受託者に対して差止命令などが発されたり、発令された措置により生産に対する影響が起こりうる。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は検討されるべきである。

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は特に重要となる。

ドイツ

第 1 章　営業秘密の定義

ドイツは EU 加盟国であるため、EU の指令や規制に従って国内法の整備・改正がなされる。ドイツにおける営業秘密の保護に関する法律は、2016 年 6 月 9 日 EU 指令[256]の国内実施のために制定され、2019 年 4 月 18 日に発効した[257]。2019 年まで、ドイツではさまざまな法律や規制が、営業秘密の保護に適用されてきた。この中には、ドイツ不正競争法（UWG）、ドイツ刑法、ドイツ財政法、ドイツ民法（BGB）、ドイツ株式会社法、ドイツ競争制限法（ARC）が含まれる。1896 年から 2019 年まで、主に営業秘密保護に適用された法律は不正競争法（UWG）[258]で、UWG に関する刑事事件や民事事件の判決によって、営業秘密の保護がなされてきた[259]。したがって、新法 GeschGehG に営業秘密の定義規定を置き、規制・救済の対象となる不正な営業秘密の取得、使用、開示行為を明確化した[260]。新法が UWG を置き換えたこととなる。

そこで、本報告書では、ドイツ法における営業秘密の定義について、かつての UWG（第 17 条～第 19 条）に関する判例法で示された考え方と、EU 指令を受けて 2019 年に発効した営業秘密の保護に関する法律（GeschGehG）が規定している定義内容について紹介する。

1　判例法による定義

従前の UWG の第 17 条～第 19 条に関して発展した判例法では、下記の要件を満たすものについて営業秘密としての保護を認めていた。

a.　非公知で、容易に入手できない、限られた数の者にのみ知られており、

---

[256] EU Directive 2016/943 (Directive)

[257] Gesetzzum Schutzvon Geschäftsgeheimnissen(略称「GeschGehG」)

[258] Gesetzgegen den unlauteren Wettbewerb：UWG 第 17 条から第 19 条

[259] ドイツの不正競争法（UWG）には、特定の不正流用行為に対する営業秘密の保護に焦点を当てた、第 17 条、第 18 条、第 19 条が規定されていた。従業員による営業秘密の第三者への違法な開示を禁止しているだけでなく、第 19 条は共犯者の行為を処罰し、更に、産業スパイ、つまり、従業員、若しくは、第三者による技術的手段の適用による、営業秘密の不正使用も禁止されていた。新法がこれらの規定を置き換えることとなる。Thomas Nagele, et al., Trade Secrets 2021, Chambers And Partners (Apr. 28, 2021), https://practiceguides.chambers.com/practice-guides/trade-secrets-2021/germany/trends-and-developments

[260] GeschGehG 第 4 条。経済産業省「諸外国における営業秘密保護制度に関する調査研究報告書」（2014）、特許庁「人材の移動による技術流出に係る知的財産の在り方に関する調査研究報告書」（2011）、経済産業省「諸外国の訴訟手続きにおける営業秘密保護の在り方等に関する調査研究報告」（2010）がある。

b. 特定の事業にかかわる、
c. 技術的又は非技術的情報で、
d. 情報を保有する者の意図によって秘密とされている[261]。

このように、営業秘密の存在に関して客観的な事実から認定できる秘密性の存在を明確に要求してこなかった[262]。このため、営業秘密保有者が主観的に秘密であると判断し、実際に商業的価値がある情報については、営業秘密保有者がどのようにして秘密性を保持していたかが詳細に審理されることはなかった[263]。

2 GeschGehG による定義[264]

GeschGehG 第 2 条は、EU 指令の内容を取り込んだものとなっており、何が営業秘密となるかについて、以下のとおり定義している。

a. 集合体として、又は、その正確な構成や要素の組立てに関して、当該情報と同種の情報を通常扱う業界の内部者で、一般に知られておらず、又は、容易にアクセスすることができない点において、秘密にされている。
b. 情報を合法的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。
c. 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

GeschGehG の定義では、秘密性確保のための合理的な措置が採られていたことを要件としている。また、「秘密性保持に関する、正当な利益の存在」が必要となる。「正当な」という限定が付されていることからして、営業秘密保有者自身の私的な利益を超えて、公的に見ても、保護に値する情報であるかが問われる可能性がある。この点について英国 TS 規則で採用された定義と比較すると、商業的価値の有無を格別に問題としていない点で異なる[265]。

(1) 秘密性保護の措置

従前、営業秘密の存在を認めるために、裁判所は、最適の保護措置がとられている必要はなく、個別の事件の事実関係に即して、相当性の観点から判断する、とのみ述べていた[266]。一方で、裁判所の中には、個々の営業秘密に対する保護措置が採られている必要があると述

[261] 連邦裁判所は、営業秘密の存在に関して、事実の発見が、秘密の所有者に経済的損害を引き起こす可能性があるため、所有者が、秘密性確保に正当な利益を持っていることを要求した。Maria von Tippelskirch 氏インタビュー
[262] 前掲 Nagele, et al.
[263] 前掲 Nagele, et al.
[264] GeschGehG 第 2 条
[265] 営業秘密規則第 2 条
[266] Dusseldorf Regional Labor Court, Judgment of 3 June 2020 – 12 SaGa 4/20

べたものもあり、混乱が生じていた。

このような中、シュトゥットガルト控訴裁判所は[267]、「情報を秘密に保つための合理的な措置」の最低基準に関する判例を確立しようとした。同裁判所は、下記を考慮することを判示した。

a. 営業秘密の性質と価値
b. 当該事業にとっての営業秘密の重要性
c. 研究と開発に要した費用
d. 事業の規模
e. 事業において通常にとられている安全策
f. 情報のラベルの仕方
g. 従業員や取引先との契約中での言明

また、同裁判所は、次のような事実の有無を重要視することを明らかとした。

i. 情報は、割り当てられた仕事を実行するため、少なくとも潜在的にアクセスを必要とする人にのみ開示されている（「知る必要があるベース」）、
ii. 情報が開示される人は、秘密保持義務に拘束され、情報に関して、この秘密保持義務を負っていることを認識している。

その上で、同裁判所は、所有者に秘密保護の不備がある場合は、所有者が追加の保護措置をとったかどうかに関係なく、適切なレベルの秘密の保護がない状況と認定される結果につながる可能性があると判断した。特に、従業員が、パスワードによる保護なしで、自分のハードウェアにファイルを保存することを容認することで、「データ漏洩」の危険にさらす、または、紙の文書が関係している場合は、無許可の者が、紙の文書を閲覧しうる状態にあったなど、保護に不備があることによって、通常、秘密の適切なレベルの保護を否定する場合がある。

(2) 新法と旧法の差異

以上のとおり、新法の定義では、秘密性を保つための合理的な措置がとられていることを明確に要件としていることから、旧法において営業秘密とされていた情報が、営業秘密にあたらなくなる可能性はある。

この点に関連して、シュトゥットガルト控訴裁判所の示した要件は重要と考えられ、営業秘密を知る必要がある関係者間のみでシェアされていたか、秘密保持義務が課せられていたか、パスワード管理がされていたか、記載された有体物の管理が厳格にされていたか、は営

[267] Stuttgart Court of Appeal, Judgement of 19 November 2020 – 2 U 575/19, GRUR-RS 2020, 35613

業秘密該当性を判断する上で、検討されることになると思われる。

第2章　営業秘密侵害行為の定義

1　従前の判例法における営業秘密侵害行為

UWG第17条から第19条では、侵害行為となるのは、基本的には、従業員が、故意又は過失により、営業秘密を不正に開示、取得又は使用した場合であり、従業員以外の者については、教唆等の積極的な意図・意欲（単に、営業秘密であるという認識、故意だけでなく）が伴っていることを要求していた[268]。

2　新法における営業秘密侵害行為

(1) GeschGehG第4条によると、次の行為を営業秘密の侵害行為と規定している。

a. 営業秘密の保有者の合法的な管理下にあり、営業秘密を含む、又は、営業秘密を取り出しうる文書、物件、材料、物質、又は、電子ファイルへの許可を得ないアクセス、使用、若しくは、コピー、又は、当該状況下において、誠実な商慣行を考慮して、信義誠実の原則に反するその他の行為。
b. 次に該当する者による、営業秘密の使用または開示する行為。
   i. 前項の規定により営業秘密を自ら取得した者
   ii. 営業秘密の使用制限義務に違反している者
   iii. 営業秘密を開示しない義務に違反している者
c. 他人を通じて営業秘密を取得し、その取得、使用又は開示の時点で、他人が前項に反して、営業秘密を使用又は開示していた事実を、認識していたか、若しくはその行為時の状況下で、認識すべきであった場合。これは、使用が、これらの目的のための、侵害品の生産、提供、市場展開、輸入、輸出、又は、保管からなる場合に、特に適用される。

(2) 第三者の行為

GeschGehG第4条により、侵害行為は、広げられた概念で決められるようになり、従業員以外の者について、積極的な意図・意欲のみならず、過失により営業秘密の不正な開示、取得、使用をした場合においても、民事的救済を受けることが可能となった[269]。このため、例

---

[268] 前掲 Nagele, et al.

[269] 第４条は、取得、開示、または、使用する時点で、その状況下で、営業秘密が、違法に開示あるいは使用していた者から、直接または間接に取得された事実を知っていたか、知るべきであった場合には、営業秘密の侵害となるとする。なお、EU指令では、当初は営業秘密であることを知らず、後に不正に開示された営業秘密であったことを認識した場合も、侵害行為とし

えば、不正に取得された営業秘密を使用している製品やサービスを、作出、販売、輸出入、市場に提供する者の行為を対象として、民事的救済措置（金銭的損害賠償を含む）を求めることができるようになった[270]。

(3) 侵害における主観的要件

EU 指令の第 14 条（1）によると、加盟国は、被用者が、雇用主の営業秘密を、違法に取得、使用、または開示した場合に、故意を欠くときには、その法的責任を緩和することができることとなっている。この点に関して、ドイツではこのオプションは適用されていない[271]。他方で、営業秘密の侵害に基づく金銭的損害賠償は、GeschGehG の第 10 条（1）に従って、侵害者が少なくとも過失で行動したことが必要となる。ただし、これまでのところ、この GeschGehG の第 10 条に関連する公開された裁判所の決定は見あたらない。

(4) 除外規定

GeschGehG 第 5 条は、どのような営業秘密の取得、使用又は開示行為が例外的に許されるか規定している。内部告発のための情報の開示など、公共の利益を目的とした行為を、侵害行為から除外している[272]。

a. メディアの報道の自由、多様性を含む、表現、及び、情報の自由の権利行使。
b. 取得、使用、又は、開示が、違法行為、不正、その他の不法行為を明らかにするのに役立つなど、一般の公益を保護するのに適している場合（内部告発者システムの組織において、法第 5 条第 2 項の規定に加えて、まもなく発効する連合法違反を報告する者の保護に関する指令（EU 2018/0106）の規定）を考慮に入れる必要がある。
c. 従業員代表が、その職務を遂行できるようにするために必要な場合、従業員が、従業員代表へ、秘密とされる情報の開示をする場合（法第 5 条第 3 項）。これには、例えば、従業員の代表が差し迫った人員削減について通知した場合など、合法的なグループの利益の追求が含まれる可能性がある。

3　新法と判例法の差異

新法により、営業秘密侵害行為の範囲は、営業秘密保有者と直接の取引関係がない第三者（いわゆる転得者）の行為にまで及ぶようになった。したがって、営業秘密侵害の故意が通常無いような転得者が、侵害品を製造したり、販売したり、輸入した場合であっても、侵害

てカバーする。ドイツにおいては、行為者のとった行為（開示や使用）の時点での心理的内容を問題としている。
270 前掲 Nagele, et al.
271 第 11 条
272 同法第 5 条

している事実について、知るべきであった（過失があった）と立証できる限り、そのような第三者に対して民事的救済を請求することもできるようになった。

第3章　営業秘密侵害に関連する法律、規制の概要

1　GeschGehG

(1) 証拠収集／保全措置[273]

営業秘密保有者は、侵害者に対して、次の情報を請求する権利がある。

a. 侵害製品の生産者、供給者、並びに、他の以前の所有者、及び、意図された顧客と販売店の名前と住所
b. 製造、注文、配送、又は、受領した侵害品の数量と購入価格
c. 営業秘密を含む、若しくは、具体化する、侵害者が所有、又は、保有する文書、物件、材料、物質、または電子ファイル
d. 営業秘密を入手したであろう者、営業秘密を開示した相手

(2)　救済

GeschGehGは、営業秘密保有者は、侵害者に対して、次の救済を受ける権利がある可能性があることを明確にしている。

- 侵害排除措置（第6条）
- 侵害品の破壊、リコールなどの特別措置（第7条）及び
- 会計情報と補償（第8条）

つまり、第6条で、営業秘密保持者の申立てに応じて、裁判所は、暫定的措置として、営業秘密の使用、若しくは、開示の禁止、並びに、停止、及び、文書、物件、材料、物質、又は、電子ファイルの差押えを命じることができる。

また、第7条の規定により、本案（主な手続き）に関して下される裁判所の決定では、以下を命じることができる。

a. 営業秘密を含む、若しくは、具体化する、侵害者が所持、若しくは、所有する文書、物件、材料、物質、又は電子ファイルの破壊または没収
b. 侵害品のリコール
c. 流通経路からの侵害製品の永久的な除去
d. 権利を侵害している製品の破壊
e. 営業秘密の保護に影響がない場合は、侵害品の市場からの撤退
f. 損害賠償[274]

---

[273] 同法第8条

[274] (1) 第11条は、故意、若しくは、過失のいずれもみたさない侵害者が、侵害者が、請求の履行により過剰な不利益を被る場合、かつ、金銭による補償が適切であると思われる場合、第6

(3) 訴訟手続

恒久的措置や暫定的措置の発令にあたり、裁判所は、裁量により、口頭での審理なし、完全に対審なし、又は、口頭審理後に決定する、のいずれかを選ぶことができる。原則として、差止命令と差押えとが双方同時に申し立てられた場合、口頭審理も、侵害者の審尋も開かれない。そうしないと、警告によって、侵害の事実を隠匿するリスクがあるためである。そのような事情が確実に証明され、権利が明確である場合、事前に被告の意見を聞く理由はないとされる。

(4) 時効

民事上の請求権については、3 年間の通常の時効の対象となる[275]。ただし、特別規定として、第 13 条では、侵害者が、特別な状況下では、損害賠償請求権の時効による消滅後であっても、取得した商品を放棄する義務があることを規定している。これは、6 年の除斥期間に服する。

(5) 刑事罰

競争上の利益を図るため、自己の利益のため、第三者の利益のため、または、営業秘密保有者に損害を与える目的で、(i)不正使用、開示、取得した者、もしくは、(ii)他人を通じて取得した営業秘密を使用、開示した者には、最高 3 年の懲役または罰金が科せられ、競争上の利益を図るため、または、自己の利益のために、取引の過程で業務上委託された技術的性質の秘密文書または規則である営業秘密を使用、開示した者は、最高 2 年の懲役または罰金が科せられる[276]。

産業スパイ、営業秘密の海外利用事案については、最高 5 年の懲役または罰金が科せられる[277]。

条または第 7 条に基づく請求を回避するために、営業秘密の所有者に金銭賠償することができると規定する。
(2) 賠償金額は、ライセンスを契約上付与する場合に、適切と考えられる額に基づく。営業秘密の保有者は、差止命令を受けられる期間以上の期間に対して、補償を求めることができない。
(3) 損害定量化は、3 つの方法から選択できるとされている。実際に発生した損害の賠償を要求するか、侵害者が行った利益の返還を要求するか、または、営業秘密を取得、使用、または開示することに同意を得た場合に侵害者が支払わなければならなかったであろう適切なロイヤルティに基づいて損害を計算することができる。

[275] BGB 第 195 条、第 199 条
[276] GeschGehG 第 23 条第 1 項から第 3 項
[277] 同条第 4 項

未遂犯も罰せられる[278]。

訴追にあたっては、原則として、被害者の申告が必要とされる[279]。

2　刑法

ドイツ刑法は、営業秘密の取得、使用、あるいは、開示行為を、犯罪として処罰する[280]。

a. 第 203 条は、専門家（医師、歯科医、心理学者、弁護士又は弁理士）としての立場で、他人の事業秘密または営業秘密を不法に開示した者に対して、最高 1 年の懲役または罰金を科す。
b. 第 204 条は、第 203 条に従って秘密を保持する義務がある者が、他人の秘密、特に、事業秘密または営業秘密を違法に使用した場合の、2 年以下の懲役または罰金の賦課を規定する。第 202a 条（データスパイ）は、不正アクセスから保護されており、直接に他人に認識されえない、又は、送信されない方法で保存されたデータを許可なく取得する行為を犯罪とする。これには、秘密の取引データ、及び、事業データが含まれる。罰則は、最高 3 年の懲役又は罰金とされている。
c. 第 355 条（1）　2 は、公務員が、営業秘密、事業秘密を違法に開示、又は、使用した場合に対する罰則として、2 年以下の懲役または罰金を定める。
d. ドイツでは、刑事責任は法人には適用されない。
e. 未遂犯は罰せられない。

3　民法

(1)　従業員は、BGB 第 242 条の一般的な誠実な履行条項に従って、雇用主の営業秘密、及び、事業秘密を秘密に保つ義務がある。従業員は慣習を考慮し、信義誠実の原則に従って履行する義務がある。

雇用中、守秘義務違反が発生した場合、雇用主は通知なしに従業員を解雇し、損害賠償を請求することができる。

しかし、雇用主の特別な利益によって正当化されない、従業員に対する過度の義務を課す条項は無効とされる。

従業員は、雇用後も営業秘密に対する守秘義務を負うが、仕事から得られたスキルや知識は、守秘義務に含まれない。

(2)　取引関係を意図して交渉を行う企業は、営業秘密を含む可能性のある機密情報を互いに

278 同条第 5 項
279 同条第 8 項
280 ドイツ刑法は、第 203 条、第 204 条、第 202（a）条、および第 355 条（1）に基づいて営業秘密の保護を規定しており、それぞれ、個人秘密の侵害、他者の秘密の悪用、データスパイ、および税務秘密の違反を処罰する。

共有することがよくある。BGB は、第 311 条及び第 241（2）条に基づいて、相手方の権利および法的利益を保護しなければならないと規定している。

4　商法

ドイツ商法第 164 条により、機密保持条項と競業避止条項は、元従業員が合意された競業避止義務に対して、一定の報酬を受け取った場合にのみ有効であるとする。また、競業避止条項についての法定の上限期間（制限）は 2 年である。

5　その他関連法改正

(1)　特許法

GeschGehG の制定に伴い、ドイツ国内で、営業秘密保護強化に付随する制定法の改正作業がみられている。例えば、ドイツの特許法（「Patentgesetz」、略称：「PatG」）は、2021 年 8 月 18 日に改正された。この改正では、営業秘密や機密情報保護の強化を受けたもので、PatG への新しい第 145a 条の追加が含まれる。この PatG の第 145a 条に従い、GeschGehG の第 16 条から第 20 条が特許訴訟に適用されるようになったことが重要である。つまり、GeschGehG の第 16 条から第 20 条は、裁判所が「訴訟の対象となる情報」の機密扱いを義務付けているので、今後の特許侵害訴訟においては、当事者の機密情報や営業秘密が、不必要に開示あるいは不正に使用されないように対策が講じられる。ただし、この「訴訟の対象となる情報」という概念について、学術文献ではかなり曖昧であると指摘されている[281]。

上記に関連して、PatG の第 145a 条は、「訴訟の対象となる情報」という用語を「原告または被告によって係属中の訴訟に投入された情報」と定義しており、おそらく、PatG の第 145a 条の定義は、GeschGehG の第 16 条の同じ用語の解釈に直接影響を与えないと解されるが、PatG の第 145a 条の定義が、少なくとも判例法によって、最終的に GeschGehG 第 16 条に導入されると考えられるところである。

(2)　実用新案法

前掲(1)で紹介した特許法と同じことが、ドイツの実用新案法（「Gebrauchsmustergesetz」、略称：「GebrMG」）の新しい第 26a 条にも当てはまる。同条は第 145a 条 PatG と同様の規定を置くものであり、2021 年 8 月 18 日に発効した。

[281] Alexander in：Köhler/ Bornkamm / Federsen、UWG、第 39 版 2021、及び、GeschGehG 第 16 条欄外 25 を参照

第 4 章　営業秘密事件の実務

1　知的財産権訴訟の訴訟提起および証拠収集段階における営業秘密の保護

ドイツの民事訴訟法は、米国のように、ディスカバリーを特徴・制度の一つとして有していない。それでも、営業秘密の保有者が営業秘密侵害を主張したい場合に、秘密を開示等してしまう危険は内在する。

初めに、EU 指令に基づき、営業秘密は、実際に秘密である場合に限られる。つまり、関連する業界内で広く知られていない場合、ドイツ法下で保護される。この点、すべての情報が保護されるわけではない（一定範囲でしか保護されない）ことを理解しなければならない。次に、営業秘密の違法な使用、取得等を実証するには、営業秘密の具体的な記載が必要であることも重要である。したがって、所有者が、必要に応じて、営業秘密を「開示する」必要がある。それによって、営業秘密が、相手方に知られる危険にさらされる。このリスクを軽減することが、上記の GeschGehG の第 16 条から第 20 条の主な目的である。

営業秘密訴訟において営業秘密を保護するメカニズムは、GeschGehG の第 16 条から第 20 条に含まれている。その詳細は、次のとおりである。当事者による申請により、裁判所は、特定の情報が機密情報であることを確定できる。この場合、訴訟に関与する者、例えば、当事者、その代理人、証人、専門家が、訴訟の目的を超えて、訴訟手続において提示された機密情報を使用、または、開示することが禁止される。また、第三者のファイルにアクセスする場合、機密情報は記録から省略される。

(1)　Dusseldorf Court of Appeal, Judgment of 11 January 2021 - 20 W 68/20, GRUR-RS 2021, 7875 ff

この決定は、ドイツの著作権法第 87a 条以降の規定に基づく、データベースの保護に関係するものである。原告は、問題となっているデータベースについて、アクセスを被告に提供すべきものではないことを理由として、データベースの内容について、決定することを拒否した。その代わり、原告は、GeschGehG の第 16 条に基づく措置を申請した。

デュッセルドルフ控訴裁判所は、GeschGehG 第 16 条以降は、営業秘密に関係のない手続に適用はされないと判断した。デュッセルドルフ控訴裁判所は、GeschGehG 制定の公式資料から、機密保持に関する規則は、営業秘密に関する（BT-Drs。19/ 4724、34 を参照）訴訟にのみ適用される、という立法者の声明を確認し、同判断に至る理由とした。このような GeschGehG 第 16 条以降の制限的な適用は、同法制定以来、ドイツの法律学者によって批判

されていたところである[282]。

なお、本論点に関しては、2020 年 10 月 28 日のカールスルーエ控訴裁判所の判決でも、結論が下されないままとなっていた[283]。

本決定で、デュッセルドルフ裁判所が同条の適用範囲を制限したことが、新しく PatG の第 145a 条、および、26aGebrMG が制定されることとなった理由である[284]。

(2) Stuttgart Court of Appeal, Judgment of 19 November 2020 - 2 U 575/19, GRUR-RS2020, 35613

実質的に、また、機能的にも、GeschGehG は、UWG の第 17 条から第 19 条を書き換える。UWG の第 17 条は、GeschGehG が発効した日に廃止された。しかし、GeschGehG には移行規定は含まれていない。したがって、営業秘密侵害時に該当する UWG 第 17 条が法的に有効であった場合、営業秘密保有者が、そうした過去の侵害に基づいて、侵害者に対して営業秘密訴訟を開始し、GeschGehG を遡及的に適用することも考えられる。これが、シュトゥットガルト控訴裁判所が判断をした事件において問題となった。裁判所は、当事者による最初の行動が、GeschGehG ではなく、UWG 第 17 条によって規律されていたとしても、当事者が GeschGehG の規定に基づいて申し立てれば、第 16 条以降の守秘義務を課す措置を適用することは可能とした。

(3) Hamm Court of Appeal, Judgment of 27 January 2021 - 20 W 48/20, BeckRS 2021, 14668

ハム控訴裁判所は、通常、営業秘密と見なすことができる情報が、訴訟中に守秘義務の命令なく、提出物として裁判所に提出されることで、一般に知られるようになるとは限らず、営業秘密としてのステータスと保護を、必ずしもそれで失うことにはつながらないと述べた。それは、裁判所の訴訟手続中に提出物へのアクセスが許可されるのは、通常限られた何人かのグループの者であり、情報が一般に知られるようになることにつながらないと考えたためである。更に、裁判所は、複数の訴訟手続きの提出物として情報を提出することさえ、守秘義務を課さなくても、情報を一般に知らしめることにつながるとは限らないとした。

2 救済手段、営業秘密保護の現状

ドイツ民法下では、不法行為の被害者に認められる救済手段として、従来、金銭的賠償、不

[282] GeschGehG（Hauck in：GRUR-Prax 2019、223、225、Semrau-Brandt in：GRURPrax 2019、127、128; Schregle in：GRUR 209、912、913 を参照）
[283] 6 W 35/20、BeckRS 2020、90799
[284] 上記第 3 章 5「その他関連法改正」を参照

当利得返還、侵害製品の破壊が認められてきた[285]。営業秘密保有者は、差止めによる救済、金銭的賠償、保護された情報の返却又は破棄、損害賠償を計算する基礎とする利益に関する情報の提供、捜索命令、特定の文書提出命令、暫定的措置等の救済を利用できる。

ただし、裁判所が救済を与えるにあたり、他の法益とのバランスが重要とされており、被用者に対して、労働の自由を不必要に制限することとなる場合には、秘密保持義務はその効力を否定されてしまうことがある。また、雇用期間終了後に、被用者に課される制約（例えば、取引先を自らの顧客として勧誘したり、他の従業員を従業員等として勧誘したりすることの禁止）は、従前の 3 年間の平均給与のおよそ 50%の支払をする場合にのみ有効であるとされている[286]。

これらの救済措置は、GeschGehG の発効後、GeschGehG で許可されている上記救済策と並行して、引き続き有効に存続し、利用することが可能である。

(1) 本案判決による作為又は不作為義務を課す命令

① 排除措置命令および差止命令

ドイツの法律では、権利がすでにあることについて争いがない場合、権利侵害された時点で、繰り返しのリスクがあるため、被告が、すでに権利を侵害しているかどうかによって、侵害の危険性の認定に差異が生じる。被告は、契約上のペナルティによってサポートされる、侵害の中止と中止の宣言によってのみ、排除措置命令や差止命令を回避できる。また、過去に被告の侵害がなかったが、初めて侵害の危険性が生じている場合には、侵害に該当する行為はしないという、被告の拘束力のない宣言によって、命令を回避することができる。

シュトゥットガルト控訴裁判所は、営業秘密の侵害は単一の現象ではないが、3 つの個別のタイプの侵害（違法な取得、使用、開示）は個別に扱われなければならないと認定した[287]。その結果、違法な営業秘密の取得は、違法な取得に関して繰り返されるリスクを生み出すだけとされた。そこで、違法に取得した営業秘密の使用・開示については、最初の侵害の危険性が生じているのみであり、不法に取得した侵害者が、侵害行為をしない旨の拘束力のない宣言を行うことにより、取得した営業秘密の使用と開示に関する差止命令を免れることができる[288]。

---

[285] Germany, Practical Law UK Practice Note (2020 Westlaw)
[286] Germany, Practical Law UK Practice Note (2020 Westlaw)
[287] Stuttgart Court of Appeal, Court order of 27 November 2020 – 6 W 113/20, GRURRR 2021, 229
[288] Stuttgart Court of Appeal, Court order of 27 November 2020 – 6 W 113/20, GRURRR 2021, 229

② 事業を所有していないとの宣言

シュトゥットガルト労働裁判所は、第三者が、不法に取得された営業秘密について、第三者の宣誓の代わりに、もはや事業を所有していないと宣言することを認めた[289]。

(2) 損害賠償

ドイツ民法の一般規則に従い、損害賠償は、違反行為がなかったかのように、当事者を元の立場に置くために必要な程度で付与される。民法第 249 条に同様の規定が存在している。営業秘密保有者は、営業秘密の侵害から生じた損害を証明するが、計算方法として、失われた利益の補償、侵害者によって得られた利益の引渡し、ライセンスした場合に支払われるべきロイヤルティの支払いが存在する。

なお、ドイツでは、懲罰的損害賠償は採用されておらず、侵害行為が故意か過失かによって額を調整していない。

(3) 暫定的措置

排除措置命令および差止命令は、暫定的措置としても得られる。これらは、UWG の第 8 条に基づき、（ドイツの法律では常にそうであるように）過失又は故意を必要としない。通常、数営業日以内に付与され、一方的な申立手続を経て、暫定的差止命令によって救済を受けうる。

3 公務員による秘密の不正流用

国営企業の従業員が、改修プロジェクトの積算根拠と想定される最大費用に関する情報を漏らした事件に関して、連邦裁判所は、「営業秘密」という用語は、公開入札中に受け取ったオファーにも適用されると判断した[290]。

4 内部告発と営業秘密の使用・開示

ドイツの脱税事件に関連して、銀行が顧客に関して保有するデータが営業秘密として保護されるかどうか、そのような情報を漏らした銀行員と、そのような情報を使用する税務調査官の両

[289] Stuttgart Labour Court of Appeal, Judgment of 18 August 2021 – 4 SaGa 1/21, BeckRS 2021, 26156

[290] この特定のケースでは、ドイツの米陸軍地域契約事務所が建設工事契約の公開入札を行っていたとき、一部の米陸軍当局者が、他の競合他社が行ったオファー価格を競合他社に漏らし、それに応じて自分のオファーを調整することができた。5 StR 152/13 (dated 09/04/2013)

方が、UWG 第 17 条に基づいて罰せられるべきかどうかが議論された。同論点は、連邦裁判所によって決定されなかった。

GeschGehG 第 5 条は、違法行為を明らかにするのに役立つ取得、使用、又は、開示が、一般の公益を保護するのに適している場合、取得、使用、又は、開示を、侵害行為から除外する。内部告発は、第 5 条、及び、連合法違反を報告する者の保護に関する指令（EU 2018/0106）の規定に基づき、公益に役立つ限り、刑事責任から免除される可能性がある。

第 5 章　準拠法・域外適用

刑事法の適用に関して、犯罪者がドイツで行動した場合、又は、営業秘密、及び、事業秘密を侵害された企業が物理的にドイツに所在する場合は、ドイツ刑法が適用されうる。

不法行為法の適用に関しては、損害の発生が国内の場合にドイツ法適用がありうる。

GeschGehG の域外適用の可能性に関連する公開された裁判所の決定は見つからなかった。

第 6 章　営業秘密侵害の事件数

営業秘密刑事事件の受理は、フランクフルト支局で、年間およそ 2 桁台前半と報告されているが、公訴や実際の刑事裁判所の判決は殆どない。営業秘密侵害は、詐欺罪等の刑事事件として告発、告訴されるが、捜査、訴追はめったに行われていないとのことである[291]。2015 年の一年間に、営業秘密侵害の刑事事件は 396 件の受理がされたと報告されている。GeschGehG が施行された後、2020 年の一年間で、ドイツ国内の捜査当局に、新法に基づく営業秘密刑事事件として受理されたものは 136 件あったが、訴追は未だ一件もなされていないとのことである[292]。

その理由としては、刑事事件として要求される証明の程度が高く、有罪となる見込が少ないと判断されること、証拠収集に時間がかかること、民事で解決されると刑事事件を進行させる意味が失われること、があげられる[293]。

なお、ドイツの裁判所による判決や決定は一般的には公開されていない。代わりに、裁判所、又は、いずれかの当事者が、法的に十分に価値がある、又は、公共の利益の観点で重要と見なした場合にのみ公開される。したがって、特定のトピックに関して、公開された判決や決定の数は必ずしも、特定の時間内に下された裁判や決定の総数に対応するわけではな

[291] Professor Esser インタビュー、Maria von Tippelskirch 氏インタビュー
[292] Professor Esser インタビュー
[293] Professor Esser インタビュー

い。また、ドイツの最高裁判所による統計はないようであり、民事事件の総数については不明であった[294]。

第 7 章　営業秘密関連の法改正の動き

1　営業秘密法

成立以来、GeschGehG に関する改正は、現在までなされていない。成立した GeschGehG の改正の動きは未だない。

2　デジタル化政策

ドイツ産業連盟が自認するとおり、Digitalization（デジタル化）の分野では、ドイツは EU の先導者としての地位に立てていない。特に、超高速ブロードバンド接続では、遅れがみられる。早急に対応が必要な、サイバーセキュリティとデータ保護に向けて、新しいデジタル技術が産業界に浸透することを目指す必要があることも確認されている。

以上から、ドイツの業界は、企業がデジタル化の可能性を最大限に活用できる環境を開発することを、国内およびヨーロッパの規制当局の両方に奨励している[295]。

3　サイバーセキュリティ政策

一方、増えつつあるサイバー犯罪による機密情報の漏洩については規制が強化され、基本的な重点化政策が 2021 年に成立している。2021 年 9 月 8 日、連邦内閣は、連邦内務省、建築およびコミュニティ省（Bundesministerium des Inneren、fürBauundHeimat、BMI）によって提示された、新しいドイツのサイバーセキュリティ戦略（2021）、を採用した[296]。新しいドイツのサイバーセキュリティ戦略は、2016 年のドイツのサイバーセキュリティ戦略に代わるものであり、今後 5 年間の連邦政府のサイバーセキュリティポリシーの基本的な方向性を説明している。

サイバーセキュリティの新戦略の目標は、市民がデジタルテクノロジーを安全に、自由に、そして自己決定的に、使い続けることを可能にすることである。この目標は、特に、高レベルのサイバーセキュリティを通じて、国家、経済、科学、社会のデジタル主権を強化すること、つまり、「個人や機関がデジタル世界で、自己決定的かつ安全に、独立して役割を果たす能力と可能性」を保障することである。

---

[294] Mr. Kuhne 報告
[295] Digitalization, BDI. https://english.bdi.eu/topics/germany/digitalisation/.
[296] Cybersicherheitsstrategie für Deutschland 2021, Kapitel 3 (S. 8).

第 1 行動分野は、社会の「サイバーセキュリティ能力」を高めるという目標を設定している。たとえば、IT セキュリティソリューションの使いやすさを向上さ、デジタル消費者保護サービスを拡張し、電子 ID と電子通信をより適切に保護する。AI を IT セキュリティに貢献するツールとして使用することも含めているのが興味深い点である。

第 2 行動分野は、サイバーセキュリティの分野における、国家、企業、科学、市民社会間の協力の改善によって、国家サイバーセキュリティ評議会の強化、及び、ドイツのデジタル経済とドイツ企業の保護を目指す。

第 3 行動分野は、危険を回避するための、連邦政府の立法能力と、連邦情報セキュリティ局（Bundesamt für Sicherheitinder Informationstechnik、BSI）と州との間の協力を拡大することを意図する。サイバースペースでの法執行も強化され、セキュリティ当局による、暗号化された通信へのアクセスが作成される。

第 4 行動分野は、デジタル世代のための EU のサイバーセキュリティ戦略やネットワークと情報システムに関する指令など、合意された最低基準を導入および実施することを内容とする[297]。

4　5G 環境の整備

大きな注目を呼んだドイツの 5G のプロバイダー制限に関して、2021 年 5 月 7 日、連邦議会は、2021 年 4 月 23 日に連邦議会で可決された、IT セキュリティ法 2.0（ ″IT-SiG 2.0″）を可決した[298]。連邦議会は、米国のように特定の外国企業を情報通信関係のインフラから排斥する結果となる、排除的な体制を採用することなく、IT-SiG 2.0 法案を通過させ、かつ、サイバーセキュリティを含めた国家安全の向上を、重大な政策として遂行する同法を成立させた[299]。

(1) BSI の権限

連邦情報セキュリティ局（「BSI」）は現在、政府各局と協議し、IT セキュリティに関する拘束力のある最低基準を確立する役割を担っている。現行の IT の脆弱性に関する情報を受け取り、影響を受ける IT メーカーに報告する、BSI の権限が拡大されると同時に、BSI が

---

297 これらに伴い、４つのガイドラインの策定が行われており、以下をその内容とする。（1）国家、ビジネス、科学、社会の共同タスクとしてサイバーセキュリティの確立、（2）国家、経済、科学、社会のデジタル主権強化、（3）デジタル化の安全な達成、（4）目標の測定可能化、かつ透明化

298 ドイツ連邦政府, 提出された「IT セキュリティ法 2.0」の草案 (2021 年 1 月 27 日) https://www.bundestag.de/presse/hib/819040-819040.

299 ドイツ連邦政府, 提出された「IT セキュリティ法 2.0」の草案 (2021 年 1 月 27 日) https://www.bundestag.de/presse/hib/819040-819040.

情報の受け取りを拒否する権利がないことが明らかになった。

(2) データ保護

IT-SiG 2.0は、安全性に関わる保存データの保管要件を簡素化した。連邦通信技術の障害、若しくはエラー、または、連邦情報技術への攻撃を、特定、区別、排除するために必要な限りで、ログデータ等が蓄積、収集、および自動的に評価される点には変更がない。 IT-SiG 2.0は、連邦情報セキュリティ局法(BSIG)第5条によるデータの保存期間の制限を、自動評価に必要な期間を超えて、現行のバージョンで規定されている最大3か月から最大18か月に延長した。ただし、BSIG第5条（3）に従って悪意のあるプログラムが使用されている疑いが確認された際に、悪意のあるプログラムによる危険を回避するために必要な場合、または、他の悪意のあるプログラムを検出して情報技術を保護するため、このデータが使用される実際の蓋然性がある場合にのみ、そのデータ保管が許可される点が、制限として課される。

(3) 製品関連の規制

IT-SiG 2.0により、BSIには、ITセキュリティの技術ガイドラインを作成するだけではなく、説明する責任があり、同時に、関連する当事者（メーカー、開発者、ビジネス）を含めた、国際標準と標準を考慮に入れ、採用することが明確になった。

2021年1月25日のIT-SiG2.0のバージョンと比較して、ITセキュリティラベル自体に変更はない。ITセキュリティラベルは、1）製造元の確認、および、2）BSI Webサイトでアクセスできる製品に関する動的セキュリティ情報（リンクまたは電子パッケージ挿入物としてのQRコードを介して）の2つの要素で構成される。

ただし、ITセキュリティラベルに関連して、IT-SiG 2.0は、BSIが、ITセキュリティ要件を満たすために、製造元が準拠する必要のある、製品カテゴリーに応じた基準、標準、またはITセキュリティ仕様を、命令で規定することとした。そのような規制がない場合、製造業者は、製品カテゴリーに応じて、BSIによって発行された技術ガイドラインの仕様に準拠する必要があることとなる。

(4)「特別公益事業」

IT-SiG 2.0の政府草案は、特別な安全性を必要とする新しいカテゴリーの事業、いわゆる「特別公益事業」を定義した。この例としては、兵器部門の企業のみならず、ドイツ経済にとって重要なものであれば、他の産業、事業も含まれる[300]。すなわち、サプライチェーン内の事業でも、「独自のセールスポイントのため、公益性の高い事業のサプライヤーとして

[300] この点について、草案に関する議論の中で、主管する連邦内務大臣のホルスト・ゼーホーファーは、ドイツの自動車メーカーに言及している。

本質的に重要である」場合、特別公益事業に該当することとなった。

つまり、これらの事業は、重大なインフラストラクチャと同様の、保護および義務の体制の対象となる。これには、特に、登録、IT 認証、監査、保護対策を含む、2 年ごとの自主的な誓約、および、障害と情報の開示の場合の即時報告が含まれる。

一般に公益性の高い事業に製品やサービスを供給する、サプライチェーンの事業が、特別公益に含まれうることになったので、相当に規制範囲が広がった。以上のように、ドイツの特別公益事業へのサプライヤーは、その直接あるいは間接の提供先が、兵器産業や自動車等の事業にあたるのであれば、高度な IT セキュリティの要件を満たし、文書化し、BSI に報告する義務を負うので、今後の対策が必須となる。

(5) 重大なコンポーネント

IT-SiG 2.0 で、「使用がドイツ連邦共和国の治安や治安を損なう可能性がある場合」重要なコンポーネントの使用を禁止できることとされた。 そこで、重大なコンポーネントの製造元が、他国の政府によって管理されているか、あるいは、ドイツ連邦共和国、若しくは、他の EU 加盟国の治安や安全に悪影響を及ぼしうる活動にすでに関与しているかどうか、確認されることとなった。5G のサイバーリスクに対処するための、欧州委員会の EU5G ツールボックスのコア要件が考慮される。

5G 通信装置も、この重大なコンポーネントではあり、リスク判定をクリアーしなければならない。外務省を含む連邦関係省庁が、製造会社の情報を集め、高リスクの会社については、連邦政府による 5G ネットワークからの排除を可能とする。連邦内務省は、重大なコンポーネントの検討にあたり、使用の潜在的な禁止（事前禁止）を求めることができ、これまでより多くの時間を調査に費やすことができるようになった。

第 8 章　国際協力・他国との連携状況

ドイツは、知的財産権保護制度では EU を主導する加盟国であるが、上記のとおり、ドイツ国内でも営業秘密侵害に関する民事事件はこれまでも存在してきたものの、新法の制定から斬新な変化が見られたわけでなく、また、事件数が急激に増えているとはいえない[301]。

他方、メルケル前首相を継いだオラフ・ショルツ首相は、中国との関係が強いと言われる一方、知的財産権に関しては、自国産業の権利強化を目指すのではないかと見られ、今後の知

[301] ドイツは、コロナウィルスのワクチンの生産、販売に関して、World Trade Organization's (WTO) intellectual property rules の Waiver をしないことを、他国の求めを拒否して、反対した。

財政策の動向が注目されている[302]。

第 9 章　仲裁の利用

ドイツ国内では、一般事件での仲裁手続の利用も、知的財産権紛争での仲裁手続きの利用も、他の EU 諸国に比較すると少なく、進んでいない[303]。一方で、特許裁判の利用が圧倒的である。

第 10 章　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

第一に、EU 指令の内容を取り込んだ GeschGehG 第 2 条が営業秘密として定義するように、「情報を合法的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」ことが要件となったため、機密情報や営業秘密を、秘密保持義務への合意のないまま、第三者に提供することは、それらの「機密性」を失わせる結果となりかねない[304]。具体的な当事者間の事実関係によらず、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）を明文で盛り込むことが必要である。

ライセンスを受けるなどして、機密情報あるいは営業秘密を保持する者が、「秘密性を保持するための合理的な措置」を取っているか否かは、以後の営業秘密の保護に重要な事実として関わってくる。秘密保持義務の内容を秘密保持契約書内に盛り込むことも推奨され、契約書に含めるべき項目としては、シュトゥットガルト控訴裁判所が触れた重要な要素がある[305]。

裁判所の述べたように、必須事項として、従業員が、パスワードによる保護なく自分のハードウェアにファイルを保存することができないことを義務付けているか、また、文書に情報が記載される場合には、無許可の担当者による紙の文書のアクセスを許すなど、秘密情報の管理に失敗することが無いように、（1）ライセンシーにおいて、機密情報、営業秘密を、機密性に関する程度でラベルすること、（2）ライセンシーの従業員の機密性保持の誓約、（3）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にのみ

---

[302] Alan Crawford, For Germany's likely new leader Olaf Scholz, Hamburg is at the centre of a growing dilemma over China, Bloomberg (Oct. 23, 2021), https://www.bloomberg.com/news/features/2021-10-23/germany-s-growing-dilemma-over-china-puts-hamburg-in-spotlight.

[303] German Arbitration Institute (DIS)での 2020 年の年間仲裁事件数は、165 件であった。うち、外国当事者が関与する事件は半分程度である。https://www.disarb.org/en/about-us/our-work-in-numbers.

[304] 第 1 章「営業秘密の定義」を参照。

[305] Stuttgart Court of Appeal, Judgement of 19 November 2020 – 2 U 575/19, GRUR-RS 2020, 35613

開示されていること（「知る必要があるベース」）、（4）情報の開示を受ける者は、秘密保持義務に拘束され、情報に関して、この秘密保持義務を負っていることを認識していることを認識していること、などが、プラスの要素となるため、これらの規定を契約書や社内規則等に含めることが推奨される。

本報告書に添付の書式は、前記の重要な要素を含んだ保護措置が採られるように、ライセンシーに義務付けている。ライセンシーの中の誰が機密情報に触れうるかについての特定は、添付文書の形で行われるのが現実的と考えられる。また、相手会社の機密情報を取り扱う者から、個別に、同様の秘密保持契約を取ることも勧められる。

ライセンス、生産委託、合弁会社設立の際に、当事者間で契約書がかわされる場合、契約書に機密保持条項を盛り込むことは通常なされるが、ドイツ法が準拠法である場合には、以下の問題が起こりうるので注意し、ドイツ弁護士に相談するなどすべきである。

1　ライセンス契約

(1) 機密情報、営業秘密の特定

あまりに広範囲で網羅的な条項は、機密性保持の実施が困難であり、実務的ではない。また、技術（に関わる情報）の取引を広げるという、EU の理念とする公共の利益が害されないかが問題とされ得ること、さらに、雇用関係に関連する場合には、被用者の労働の自由が考慮されることも注意するべきである。

実際上は、情報の機密性を示すラベルが有意義と考えられる。機密情報とすべき必要性があること、実際に、機密情報として扱われていることが、後に立証できるよう確認すべきである。

一方、相手会社が、機密情報や営業秘密を利用して生み出すデータや情報を、機密情報や営業秘密に含めることは、多くの場合に、不可能ではないと考えられる。

(2) 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

契約条項を作成する場合、何が許されるか、そして、何が不正取得、使用、または、開示になるかを明確にすることは、ライセンシー及びライセンサーの利益を守り、また、有効な関係を維持するためにも大切である。例えば、ライセンシー側で、パスワード等アクセス制限を設定すること、アクセスできる者を、一定の被用者、関係会社の被用者、専門家、監査人等に制限すること、アクセスの目的と使用方法を制限することなどが、考えられる。

侵害行為者が、営業秘密の不正使用、開示、取得にあたる事実を認識していたか、認識すべきであったことが、営業秘密侵害の前提とされており、許可事項と不許可事項を分別することが意味を持つと考えられる。

営業秘密保有者において、機密性を保つ合理的な措置をとっていたかどうかを要件として

新たに導入した[306]。上記のシュトゥットガルト控訴裁判所の判示内容に注意し、パスワード要求、不用意な紙媒体での処理のないことは必須と考えられる。

(3) 契約終了後の情報の返却あるいはデータ削除義務

秘密保持義務の内容として、提供された機密情報、営業秘密は、契約関係終了時に、保有者に返却すること、また、バックアップも含めて、保存されたデータから削除するように要求すること、それを確認すること、を明記することが必要である。これは、前記の機密性を保つ合理的な措置の認定にもプラスの要素として働くと考えられる。

(4) 補償条項

相手方の秘密保持義務違反の結果生じた損害について、相手方に補償の義務を負わせることは、ドイツでも多くの場合に行われている。秘密保持義務条項の有効性が認められる場合、こうした補償条項の効力も同様に認められるであろう。

(5) 損害額

機密情報・営業秘密の保有者は、不正取得、使用、あるいは、開示により生じた損害に対する賠償として、特約がない場合、自分の被った損害を立証して、その填補を求めることができる。ただし、この損害の立証は困難となることが考えられるので、損害額の算定について、事前に合意しておくことも考えられる。

(6) 仲裁合意

裁判による紛争解決と比較し、仲裁は、営業秘密、機密情報の保護に適し、その手続で提出あるいは開示された情報の秘密性が保たれやすいと考えられている。そこで、ライセンス契約にあたっても、仲裁条項を挿入して、仲裁により契約を巡る紛争を解決し、ライセンサーの機密情報や営業秘密の保護を図ることは積極的に検討されるべきである。

なお、仲裁条項は、紛争となった場合の権利保護に対して重要な影響を与える。そこで、疑問のある場合には、国際弁護士に相談することが勧められる。

2　生産委託契約

前掲１ライセンス契約で列挙した注意点は、生産委託契約にも当てはまる。委託者としては、受託者の生産ラインの運営状況、生産品の数量等確認体制、保存・管理状況を十分確認することが特に重要となると考えられる。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は検討されるべきである。

また、生産委託契約では、受託者が、第三者の機密情報、営業秘密情報をたまたま持っていて、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

[306] GeschGehG 第 2 条

使用、開示にあたるとして、請求を起こされてしまう可能性がある。委託者自身が知り得ない場合、委託者に対する請求が認められることはないとしても、暫定措置により生産に対する影響が起こりうる。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は、検討されるべきである。

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は、特に重要となる。

英国

英国と米国は共にコモンローの国であるが、法制度上及び実務上、下記のように営業秘密保護に関して顕著な差異が見られる。

第1章　営業秘密の定義

本章では、現行の営業秘密関連法での営業秘密の定義を、新たに制定された法と判例法のコモンローを比較しつつ説明する。

1　新法による定義

欧州連合議会が、2016年にDirective（EU）2016/943（“EU指令”）を制定したことから、当時欧州連合の加盟国であった英国も、EU指令の保護内容に応じて、営業秘密の保護を現代化、成文化する作業を開始し、2018年6月9日、The Trade Secrets（Enforcement, etc.）Regulation 2018（SI 2018/597）（“UK TS規則”）の制定に至った。ただしUK TS規則は、すでに存在する判例法のコモンローにより、EU指令よりも広範囲、あるいは、強力な保護が存在していた場合、営業秘密の保有者は、UK TS規則の下で付与される保護よりも、コモンローによる拡大された保護を受けられることを明確に記載している[307]。

UK TS規則では、営業秘密を次のように定義している[308]。

a. 単体として、又は、その正確な構成や要素の組立てに関して、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点において、秘密にされている。
b. 秘密であるために、商業的価値がある。
c. 当該情報を合法的に管理している者により、特定の状況下で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。

2　判例法による定義

英国コモンローの衡平法に基づく守秘義務では、関係者間の信頼関係の性状や内容に着目し

[307] Robert Williams & Will Smith, Bird & Bird & Trade Secrets (last visited Nov. 21, 2021) https://www.twobirds.com/~/media/pdfs/trade-secrets-article-points-to-note-article-series---sweden---may-2021.pdf.
[308] Trade Secrets (Enforcement, etc.) Regulation 2018 (SI 2018/597) (「UK TS規則」) 第2条.

て、秘密（営業秘密を含む）が保護されてきた[309]。裁判例は、情報を秘密とする義務を生じさせる状況で伝えられ、信用関係に由来する情報が、機密情報の保有者にとって不利益に使用され、又は使用の恐れがある場合に、そうした行為を信用に違背する不法行為としてきた[310]。

これに加えて、黙示の信任義務としての守秘義務、忠実義務として守秘義務、明示の守秘義務が生じることがある。

衡平法上の守秘義務で保護を受ける機密情報の内容について、Thomas Marshall (Exports) Ltd v. Guinle 事件では、どのような情報が機密情報にあたるかの判断要素として、以下が挙げられた[311]。

a. 情報は、関係する業界の使用と慣行に照らして、
b. 行為時に、情報が公開されると、保有者にとって有害である又はライバルにとって有利になる、と保有者が合理的に信じていたか、
c. 保有者が、情報がまだ公に開示されていないと合理的に信じていたか。

3　新法と判例法の差異

UK TS 規則で規定された営業秘密は、コモンローの衡平法の原理に基づく守秘義務で保護された機密情報の中に含まれると考えられており、保護範囲を拡大するものではないと理解されている[312]。

実際上、英国裁判所は、第 2 章及び第 4 章で述べるように、不正開示、使用、取得行為の判断をするにあたり、事案に応じて、どのような情報をどの程度保護するのか決めている。例えば、当事者間に契約関係が存在し、それが雇用関係の場合、被用者は、雇用者に対して誠実義務や忠実義務を負うことから、雇用者の有する情報を、機密でない情報、機密情報、営業秘密の 3 つの分類に分け（このうち第 3 グループの情報が営業秘密と考えられている）、それぞれについて、違法な行為を検討してきた。営業秘密に該当する情報については、契約関係を前提とする忠実義務、誠実義務を前提とすることなく侵害行為が存在しうるので、私的な雇用者の財産的価値の保護、あるいは、不誠実な取引関係の抑止という法益を強化することとなる。

---

309 詳しく述べると、営業秘密は、保護される秘密情報のうちの特に機密性の高い情報をさすものとして、裁判例は考えてきたようである。Fraccenda Chicken Ltd v. Fowler [1985] FSR 105.
310 Coco v A. N. Clark [1969] RPC 41, 及び Attorney-General v Guardian Newspapers (No 2) [1990] 1 AC 109.
311 Thomas Marshall (Exports) Ltd v. Guinle[1979] 1 Ch 227
312 Clémence Lapotre,Trade Secret Directive Becomes Directly Effective: Growling (June 7, 2018)　https://gowlingwlg.com/en/insights-resources/articles/2018/trade-secrets-directive-becomes-directly-effective/

第4章で紹介する裁判例において一部説明されているが、コモンローの黙示の守秘義務や衡平の理念に基づく機密情報の保護と、新法による保護は併存するため、実務上、UK TS規則が大きな変化をもたらすとは期待されていない。しかし、営業秘密法の域外適用の可能性についてUK TS規則がこれを肯定しており、判例法に基づく保護を超えるのではないか、という解釈も現れており、注目されている。

第2章 営業秘密侵害行為

以下で、営業秘密の侵害行為の定義を概説する。

1 新法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

(1) 第2条：営業秘密侵害者、営業秘密侵害物件

UK TS規則の第2条は、「侵害者」とは、営業秘密を違法に取得、開示又は使用した者をいう、と定義している。同条は、「侵害品」とは、営業秘密を違法に取得、使用又は開示した、商品、デザイン、機能、製造プロセス、マーケティング、又は、違法に取得、使用、開示された営業秘密に起因するこれらの有利な特性をいう、と定義している。

他の条文でも、何が「違法に取得、使用又は開示」に該当するかについて、特別に規定していない。したがって、どのような行為が営業秘密侵害行為となるかは、新法は明らかにしていない。

(2) 第3条：保護の拡大

UK TS規則のExplanatory Note（注釈）は、第3条第(1)項が、どのような営業秘密の取得、開示、使用が違法な取得、開示又は使用となるかは、コモンローの判例法で確立された理論に依拠して決定されることを示している、と注記している[313]。

(3) まとめ

以上のとおり、営業秘密の侵害行為に関して、新法は、「侵害品」の定義を与えている点で、注目されている。即ち、UK TS規則が、侵害品自体に対する救済措置を、営業秘密保有者に対して付与しているとの解釈も可能である。しかし、判例法を積極的に変更するような規定は存在しない。

[313] UK TS規則のExplanatory Note.

2　判例法による守秘義務違背の原理：機密情報の不正取得・開示・使用

(1) 伝統的な守秘義務違背：雇用関係に黙示に含まれる守秘義務

英国コモンローの下では、被用者は、雇用者に対して、忠実義務と誠実義務を負うとされている。これらの義務は、雇用契約に伴う黙示の条件であり、契約関係上の義務と理解されている。したがって被用者は、雇用者の秘密を誤用してはならない義務を負う[314]。英国の裁判例では、以下のように、被用者の忠実義務・誠実義務が説明されている。

「法は、被用者が雇用者に対して、忠実にかつ誠実に行動する義務を負うことを、雇用関係に含まれるものとして理解する。被用者は、雇用者が秘密としていることを、業務を行うのに必要とする場合に限りで使用するが、他の目的に使用することはできないという誠実義務を負っていることは、長年に亘って、裁判で支持されている[315]。」

(2) 情報の分類化

現在も英国裁判所によって参考とされる Goulding 裁判官の判決では、問題となった情報の種類に応じて、秘密の使用を３分類に区別し、被用者の情報の使用が、守秘義務に反するかどうか判断すべきと判示した。即ち、従業員がアクセスした可能性のある情報のうち、(i) 最初のグループの情報は、機密ではない情報であり、(ii) 第 2 のグループは、通常の雇用過程で取得された機密情報であり、従業員の頭の中に残り、彼自身の経験とスキルの一部になる。(iii) 第 3 のグループは、特定の営業秘密の形式で存在する機密の情報である[316]。第 2 及び第 3 のグループの情報は、被用者が、雇用期間中に、雇用されている業務に関係する以外で使用することができない義務を負う。しかし、雇用契約の終了に伴い、第 2 のグループの情報は、このような守秘義務の対象から外れ、被用者は、第 3 のグループの情報についてのみ、雇用の終了後も開示等してはならないという守秘義務を負う[317]。

(3) 被用者の守秘義務の要素

前記の裁判の上訴審で Neill 裁判官は、従業員が雇用に留まっている間は、被用者の黙示の義務として、誠実義務又は忠実義務が課され、従業員の守秘義務もその条件に含まれることを再確認しつつ、次のことに注意を促した[318]。(a) 誠実義務の範囲は、雇用契約の性質によって異なり[319]、(b) 被用者が、雇用終了後に使用するために、まだ雇用されている間に雇用主の顧客のリストを作成したり、コピーした場合、又は、そのような顧客リストを故

[314] Marathon Asset Management LLP v. Seddon [2017] EWHC 300 (Comm).
[315] Coco v A. N. Clark [1969] RPC 41
[316] Fraccenda Chicken Ltd v. Fowler [1985] FSR 105
[317] Fraccenda Chicken Ltd v. Fowler [1985] FSR 105.
[318] [1987] Ch 117
[319] Vokes Ltd. v. Heather, 62 R.P.C. 135.

意に記憶した場合、守秘義務違反となるが、特別な状況を除いて、元従業員が、以前の雇用主の顧客を訪問したり、顧客と取引したりすることについて、一般的に制限はされていない[320]。したがって、被用者は、営業秘密に至らないような機密情報については、自分の頭の中にある場合、雇用終了後に開示したり、使用したりしても、忠実義務や誠実義務違反とはならない[321]。

よって、雇用関係終了後の被用者について、開示、使用が違法な忠実義務、誠実義務違反となるかについては、下記要素を考慮に入れて判断することになる。

a. 雇用の性質。機密資料が習慣的に取り扱われる地位への雇用は、従業員が、その機密性を認識することが期待できるため、高い機密保持義務を課される。
b. 情報自体の性質。第 3 グループの情報（営業秘密）の明らかな例として、製造方法の秘密が含まれる。特定の情報が、限られた人数の者にのみ、限定して配布されているという事実は、情報の性質、その機密性の程度に、重要な示唆を与える。
c. 雇用主が、情報の重要性、機密性について、従業員に強い認識を植え付けたかどうか。雇用主は、特定の情報について、機密であると従業員に伝えるだけでは、一切の使用又は開示を違法とする営業秘密に位置づけられないが、情報に対する自身の態度が、その情報が第 3 グループの情報に含まれるのかどうか、判断するのに役立つ場合がある。
d. 情報を、従業員が自由に使用又は開示できる他の情報から、簡単に分離できるかどうか[322]。

以上のとおり、情報の 3 分類化、及び、上述の 4 要素を考慮するというアプローチは、被用者が、雇用契約終了後に別の雇用機会を探し求め、労働に従事する自由を享受することができるという、公共の利益に配慮した判断をするために重要となる[323]。

(4) 被用者の不正取得、使用、開示に関する故意・過失

黙示の契約上の忠実義務、信実義務は、被用者が、情報が機密であることを知っている場合、又は、被用者の立場にある合理的な行為者が知り得た場合にのみ、従業員を拘束するとされている。

[320] Robb v. Green [1895] 2 QB 315 and Wessex Dairies Ltd. v. Smith [1935] 2 K.B. 80
[321] Roger Bullivant Ltd v Ellis [1987] FSR 172
[322] Lancashire Fires Ltd v S.A. Lyons & Co Ltd [1996] FSR 629 (CA), at 668-9.
[323] Vestergaard Frandsen A/S v Bestnet Europe Ltd [2013] UKSC 31; [2013] 1 WLR 1556.

(5) 非公知性、非容易取得性

情報が既に公知となっている場合には、機密情報も、営業秘密も存在しない。

しかし、英国裁判例では、原告から機密情報を不正取得した被告が、当該情報を、他から製品を合法的に入手することで、リバースエンジニアリングで発見する、もしくは、突き止めることができたはずであることと主張しても、機密情報がなかったとすることにはならない。つまり、原告から直接に入手することで、情報を構築するのに雇用者が費やした労働、費用、技術的な困難の克服を省くことができたことで、機密情報の存在を肯定することができるとされてきた[324]。

一部が公開された情報で、他の部分が非公開の機密情報である場合、被用者は、パブリックドメインにある資料のみを使用するように、特別な注意を払う必要がある。つまり、被用者は、公的な情報源から得た場合よりも、有利な立場にあってはならず、雇用者の信用を得て受け取った情報を使って、他人を有利な競争的地位に置くべきでない。ただし、秘密情報に起因する時間と手間を省き、得た価値の多寡によって、差止命令をすることは妥当でなく、損害賠償だけが許される場合も多くあると考えられている[325]。

(6) 伝統的な営業秘密侵害行為：衡平法の原理に基づく守秘義務

雇用関係という契約関係に基づく黙示の守秘義務とは別に、衡平法で、信頼関係に由来する信用を基礎として、守秘義務が課せられることがある。つまり、営業秘密などの機密情報を、機密性を保つことに同意した、又は、機密性を認識したか、認識すべきであった状況で受け取った被告が、その機密性と矛盾して使用する場合に、被告による信用の違背と認められる[326]。

裁判例では、機密性を認識し得たはずの被告に対して、差止命令を発令することも可能と判断されている[327]。

衡平法に基づく守秘義務の場合、契約に基づく守秘義務と異なり、前述の 3 分類の情報のうち、第 2 グループの情報については、雇用関係の終了により守秘義務が終わらない。なぜなら、衡平法は、契約関係とは独立して、当事者間の信義、誠実、公平等の観点から、裁判所が義務の有無を決定するものだからである。

(7) 伝統的な営業秘密侵害行為：故意・過失がある第三者による不正取得・使用・開示

---

[324] Force India Formula One Team Ltd v Aerolab Srl [2013] EWCA Civ 780; [2013] RPC 36
[325] Seager v Copydex (No. 1) [1967] 1 WLR 923
[326] Attorney General v Guardian Newspapers Ltd (No 2) [1990] 1 AC 109 , 281.
[327] Primary Group (UK) Ltd v The Royal Bank of Scotland plc [2014] EWHC 1082 (Ch); [2014] RPC 26

原告が、営業秘密等の機密情報を有している場合、競争関係にある被告が、原告の情報を不正に取得したり、使用したりした場合、被告は、原告に対して、衡平法により、直接自己の行為に対する責任を負う。すなわち、被告が、取得した情報が、原告の機密情報で、信用を置いていた者に限定してシェアされていたにもかかわらず、信用違背の結果取得されたことを認識していたか、被告が置かれていた特定の状況下で、合理的な者であればそう認識すべきであった場合には、自己が不正に取得、使用、開示した結果生じた原告の損害について責任を負う[328]。

(8) 伝統的な営業秘密侵害行為：新雇用主による不正取得・使用・開示

被告が、原告と契約関係にない場合でも、原告に雇用されていた元従業員を雇用して、原告の営業秘密を巧みに活用することで自己の製品の改良などをした場合、元従業員の違法な守秘義務違背に対して、間接的に責任を負うと判断されてきた[329]。被告が、自己の営業に関連して、元原告従業員の不正取得、使用によって利益を受けられたことから、間接的責任である代位責任を負うことになる[330]。

あるいは、共同不法行為責任を問えると示唆する見解もある[331]。

3 新法と判例法の差異

前述のとおり、UK TS 規則は、不正開示、使用、取得行為について、特別に規定しておらず、従来の判例法の法的枠組みが引き続き適用されることとなっている。EU 指令では、営業秘密侵害を認定するための前提として、そもそも営業秘密が存在していたか、さらに、その客観的要件として、保有者が機密性を保つために合理的な措置をとっていたかを独立した要件と打ち立てている。従来の英国裁判例では、機密性の保持のための合理的な措置の存在を独立して考察せず、侵害者が、保有者が当該情報を機密性ある情報として保持し、信用を寄せていた者にのみ当該情報にアクセスさせていたことが明らかな場合に、不正開示、使用、取得を認めていた。UK TS 規則に基づく営業秘密侵害の案件では、これまでのコモンロー下での機密情報の不正開示、使用、取得の案件とは異なり、合理的な措置があったかどうかを、一つの独立した争点として審理する可能性が否定できない。

---

328 Vestergaard Frandsen A/S & Ors v Bestnet Europe Ltd & Ors [2013] UKSC 31 (22 May 2013)
329 Vestergaard Frandsen A/S & Ors v Bestnet Europe Ltd & Ors [2013] UKSC 31 (22 May 2013)
330 Ocular Sciences Ltd v Aspect Vision Care Ltd (No.2) [1997] RPC 289
331 Growling、脚注 312

第 3 章　営業秘密侵害に関連する法律、規制の概要

1　営業秘密侵害行為に関する EU 指令及び UK TS 規則

英国が、EU を脱退したことで、EU 指令が、英国裁判所を直接に拘束する効力を持ち続けることはない。他方、UK TS 規則は、EU 指令を英国内法に移行するために誕生したので、営業秘密侵害について規律する UK TS 規則の適用は続く。また、UK TS 規則の適用と解釈にあたって、EU 指令の立法目的、規律内容等が参考とされうる。

(1) 定義規定[332]

前述のとおり、UK TS 規則では、何が営業秘密か、何が営業秘密侵害行為となるかについて定義している。「侵害品」とはデザイン、機能、製造プロセス、マーケティング又は、これらの特性が、不正に取得、使用、又は開示された営業秘密から看過できない程の利益を受けている製品とされている。営業秘密保有者とは、営業秘密を合法的に管理、所持する者を言うことから、ライセンシーも該当することとなる。

(2) 権利・救済手段の期間制限[333]

除斥期間は 6 年とされ、権利の法定期間は 5 年とされている。期間の起算点は、(a) 請求の対象となる違法な取得、使用又は開示が終了する日、(b) 営業秘密保持者が侵害を認識した日のいずれか後の日をいうとされている。

(3) 訴訟（手続）中の営業秘密の保護

関係者又は、手続きの一部を構成する文書にアクセスできる者は、次の要件を充たす営業秘密、又は、営業秘密とされる対象物を、使用又は開示してはならない。

① 利害関係者による正当な理由のある申請、又は、裁判所自身の職権により、命令で、裁判所が機密事項として特定し、

② 手続きへの参加、又は、アクセスの結果として、参加者が知るに至ったもの[334]。

また、裁判所は、文書へのアクセスを手続関係者や第三者のうちの一部にのみ限定したり、審理の傍聴・立会いや訴訟記録閲覧を特定の関係者に制限したり、営業秘密を省いたり、塗り潰す等した後の記録を閲覧可能にするといった措置も採ることができる[335]。

[332] UK TS 規則 第 2 条
[333] 第 5 条
[334] 第 10 条
[335] 第 10 条

(4) 恒久的差止命令

① 裁判所は、本案の審理により、営業秘密の侵害があったと認めた場合、営業秘密の保有者による申立てに応じて、以下の措置の 1 つ又は複数を命じる恒久的差止命令を発令することができる[336]。

a. 営業秘密の使用、又は、開示の停止、又は（場合によっては）禁止。

b. 侵害品の製造、提供、市場への進出、使用の禁止、又はこれらの目的での侵害品の輸入、輸出、保管の禁止。

c. 権利を侵害している製品に関する是正措置の採用（適切な場合を含む）-

i. 市場からの侵害品の回収。

ii. 侵害品から侵害する特徴を失わせること。

iii. 権利を侵害している製品の破壊、又は、市場からの撤退。ただし、撤回によって、問題の企業秘密の保護が損なわれないことを条件とする。

d. 営業秘密を含む、又は、それを具体化する文書、オブジェクト、資料、実物、又は電子ファイルの全部又は一部の破壊、又は、適切な場合、その文書、オブジェクト、資料、実物、又は電子ファイルの全部又は一部の、申立人への送付。

② 裁判所は、上記の恒久的な差止命令について、下記の要素を考慮しなければならない[337]。

a. 営業秘密の価値及びその他の特定できる特徴、

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を取得、使用、又は、開示する行為、

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、暫定措置の付与又は拒否が、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、及び

h. 基本的権利の保護

③ 差止命令を課された侵害者は、以下の場合には、裁判所に対し、差止命令の代わりに、金銭的賠償をすることを申し立てることができる[338]。

a. 申立人が、使用、又は、開示の時点で、違法に使用、又は、開示していた他者から、営業秘密が取得されたことを知らなかった、又は、当該状況下で、知りうるべきではなかった場合、

[336] 第 14 条
[337] 第 15 条
[338] 第 16 条

b. 当該差止処分の実施が、命令を受けた者に、不釣り合いな損害をもたらす場合、及び

c. 被害を受けた当事者に賠償することが、合理的に十分できると考えられる場合。

(5) 損害賠償

裁判所は、営業秘密保有者の申立てにより、営業秘密の不正開示、使用、又は、取得が行われていることを知っていた、若しくは、知っているはずであった侵害者に対して、営業秘密の違法な取得、使用、又は開示の結果として被った、実際の損害の賠償を命じる必要がある。裁判所は、a. 又は b. のいずれかに基づいて、損害賠償を与える[339]。

① 本項に基づいて損害賠償を与える場合、裁判所は、以下を含むすべての適切な要素を考慮に入れる。

a. 営業秘密保有者が被った逸失利益、侵害者に生じた不当な利益を含む、引き起こされた経営的影響、及び

b. 営業秘密の違法な取得、使用、又は、開示によって、営業秘密の保有者に引き起こされた道徳的偏見を含む、経済的要因以外の要素。

② 本項に基づいて損害賠償を与える場合、裁判所は、必要に応じて、侵害者が、交渉によりライセンスを取得した場合に、支払うべきロイヤルティ、又は、手数料に基づいて、損害賠償を与えることができる。

(6) 暫定措置(保全措置)[340]

① 営業秘密保持者の申請により、裁判所は、侵害者とされる者に対して、以下の措置のいずれかを命じることができる[341]。

a. 暫定的に、営業秘密の使用、若しくは、開示の停止、又は禁止、

b. 侵害品の製造、提供、市場への進出、使用の禁止、又は、これらの目的での侵害品の輸入、輸出、保管の禁止、

c. 市場に展開し、若しくは、流通するのを防ぐことができるように、輸入品を含む、侵害の疑いのある製品の押収又は送付。

---

339 第 17 条

340 第 11 条

341裁判所は、暫定措置の代わりに、侵害者に、損害額の担保を提供するように命じうる。暫定措置が発令された場合、営業秘密保有者は、裁判所が定めた期間内に本案訴訟を提起しなければならない（提起がされない場合、暫定措置命令を取り消しうるとされる）。第 11 条、第 13 条

② 裁判所は、暫定措置を発令するかどうかの判断にあたり、下記について十分な確信を抱かせることが可能と合理的に見なされる証拠を提供するよう、営業秘密保有者に命じうる[342]。

a. 企業秘密が存在する、

b. 営業秘密保持者が申請を行っており、

c. 侵害者とされる者が

i. 企業秘密を不法に取得した。

ii. 営業秘密を違法に使用、又は、開示している、又は

iii. 企業秘密を違法に使用、又は、開示しようとしている。

③ 裁判所は、暫定措置の発令をすべきか、及び、その相当性について、恒久的差止命令と同様の要素を考慮しなければならない。

(7) 判決公開における営業秘密を守るための措置[343]

営業秘密の違法な取得、使用、又は、開示の訴訟手続において、裁判所は、営業秘密保有者の申立てに基づき、侵害者の費用負担で、判決情報の発信のため、全体的又は部分的公表を含む、適切な措置を命じることができる。裁判所が採る措置は、第 10 条に規定されている営業秘密の機密性を、保持する必要がある。

2 契約関係を基礎とする守秘義務違背

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、損害賠償等の請求を行う事が可能である[344]。他方で、そうした守秘義務を課す契約や条項が、不合理な自由の制約にあたると考えられると、秘密保持契約も条項も、法的拘束力を否定されてしまう[345]。

明示の守秘義務の他に、第 2 章で述べたように、雇用関係などの法的関係を基礎として、あるいは、コモンローで、黙示の契約上の忠実義務、誠実義務の一内容として、守秘義務が課される場合があり、被用者や会社役員、その他誠実義務の一内容[346]として生じることがあ

[342] 第 12 条
[343] 第 18 条
[344] Marathon Asset Management LLP v. Seddon [2017] EWHC 300 (Comm)
[345] Marathon Asset Management LLP v. Seddon [2017] EWHC 300 (Comm)
[346] QBE Management Services (UK) Ltd v Dymoke and others [2012] EWHC 80 (QB)

る。

3　衡平法下における守秘義務違背

コモンローでは、契約に基づく守秘義務とは別に、衡平法に基づいても、守秘義務が課される。これは、同業者等、保有者と契約関係にないが、保有者の機密情報であると合理的に理解できるような場合に、機密情報を不正に取得した者から買い入れて使用する場合に問題となる[347]。

4　コンピューター不正使用法

英国裁判所が、1990 年のコンピューター不正使用法（Computer Misuse Act 1990）を適用できる犯罪は、下記のような事実、事情がある場合である[348]。

(1) 第 1 条：コンピューター装置への不正アクセス

自分のコンピューターを含むコンピューターに、アクセスを確立する目的で機能を実行させる行為。ただし、コンピューターとの単なる物理的接触（操作に至らない行為）、及び、コンピュータープログラムと接触なくデータを閲覧する、あるいは、誰かの出力データを取得する行為は除外されている。したがって、機密情報出力の読み取り、画面に表示されたデータの読み取り、又は、「コンピューターの盗み聴き」（機密情報が表示されている画面を、知りながら敢えて見る）は、いずれも対象外となる。

なお、行為者において、自己にアクセス権がないという認識を有している必要がある。判決で、一部のデータにアクセスできる被用者が、それ以外のデータにアクセスした場合には、本罪が成立するとしたものがある[349]。

起訴されれば、犯罪に対する罰則は最大 2 年の懲役とされている。なお、第 1 条と第 2 条は、第 17 条の解釈の条文と併せて検討される必要がある。

(2) 第 2 条：犯罪遂行目的でのコンピューター装置への不正アクセス

行為者が、さらなる犯罪の実行又は促進を目的として、第 1 条に基づく不正アクセス罪を実行する場合には、第 2 条の構成要件に合致し、同条の適用がある。ただし、行為者が意図

[347] 前記「営業秘密侵害行為」に掲載の判決を参照。
[348] Computer Misuse Act 1990
[349] R v Bow Street Magistrates' Court and Allison (AP) Ex Parte Government of the United States of America (Allison) [2002] 2 AC 216,

した、さらなる犯罪が実際に行われたことを証明する必要はない。

例えば、銀行のコンピューターに不正にアクセスして、電子送金の過程にある資金を、自身の銀行口座、又は共犯者の銀行口座に移行する、窃取の目的で、不正アクセスを取得することが、第2条に該当すると考えられる。又は、情報が関係する人物を恐喝する目的で、コンピューターに保持されている機密情報へ不正アクセスする場合も該当すると考えられている。

第2条の行為に課しうる最大の刑罰は、5年の懲役とされている。

(3) 第3条：コンピューターを誤作動させる目的で、あるいは、誤作動を起こさせるかについて無謀な状況での、コンピューター装置への不正アクセス

第 3 条（2）項に記載のいずれかを実行することを意図して、コンピューターアクセスが許可されていないことを知って、コンピューター不正アクセスを行うこと、又は、その行為を行うことによって、第 3 条（2）項に記載の 1 つが起きるかどうかについて無謀である場合は、本罪に該当する。

例として、意図的又は無謀なコンピューター作動の障害、正当なユーザーによるコンピューター装置へのアクセスの防止又は妨害、又は、コンピューターに保存されている資料の操作又は信頼性を障害することが該当する。行為者は、行為が許可されていないことを認識している必要がある。分散型サービス拒否攻撃（DDoS）を伴う場合、特に、コンピューターの作動、保存内容の改変が起きなくても充足はされ、作動障害は一時的なもので足りる可能性がある[350]。

DDoSは、さまざまなソースから発信されたトラフィックを使用し、アクセスを集中させることで、インターネットに接続されたホストのサービスを一時的又は無期限に中断し、本来のユーザーが、装置又はネットワークリソースを利用できないようにする一種のサイバー攻撃であり、被害者が、1 つのソースだけをブロックすることで攻撃を阻止することができなくする。群衆が事業所の入り口を塞いで、合法的な顧客がアクセスすることを不可能にし、それによって営業を混乱させる手口に例えられてきた。

実際には行為者からのアクセスであるにもかかわらず、別人からのものかのようにコンピューターに情報を記録させた場合、それは明らかにコンピューターの信頼性に影響を及ぼす。したがって、そのような行為は、コンピューターの操作信頼性を損なう第 3 条（2）項（c）に該当する[351]。

[350] DPP v Lennon（2006）170 JP 532

[351] Zezev and Yarimaka v. Governor of H.M. Prison Brixton [2002] EWHC 589 (Admin).

ただし、コンピューター上のコンテンツ内容を変更しただけでは、1971 年刑事損害法第 10 条の意味における刑事損害とはみなされない[352]。

(4) 第 3ZA 条：重大な損害を与える、又は、そうした危険性を持つコンピューター装置への不正アクセス

不正アクセスをした結果、被害者に重大な損害を与えた場合、行為者は第 3ZA 条により処罰されることになる。特に、人命あるいは国家的安全に影響を与える危険性がある場合、重大犯罪とみなされ、厳しい刑罰が科されることになる。

本罪が適用される場合、最大で 14 年の懲役が科されるが、第 3 条 (a) (b)項にあたる場合には、無期懲役の法定刑が定められている。

(5) 域外適用の有無

第 1、3、3ZA 条違反の刑事責任は、母国（イングランドとウェールズ）と、少なくとも 1 つの「重要なリンク」があることの証明が必要とされる。重要なリンクには次のものが含まれる。

a. 被告人が、犯罪時に母国にいる。
b. 犯罪の標的は母国にある。
c. 犯罪を助長した技術活動は、母国に拠点を置くサーバーを通過した可能性がある。

5 競争法

競争法は、機密情報や営業秘密を保有する者に救済を与えるというのではないが、機密情報がライバル会社へ提供されることに対して制裁を課すという点では、営業秘密法に無関係なわけではない。

EU の機能に関する条約第 101 条は、EU 内の自由な人的物的移動を保護する規定であるが、反競争的な合意、取決め、協調的行動、慣行を禁止する。また、同条約第 102 条は、市場における支配的地位の濫用を禁止する[353]。英国では、1998 年競争法が制定され、同法により、市場取引に影響を与える反競争的協定及び支配的地位の濫用が禁止されている[354]。

したがって、製品の価格設定や取引業者の選定、あるいは製品の互作動性に関わる技術標準

[352] Cox v Riley (QBD) 1986.
[353] The Treaty on the Functioning of the European Union.
[354] Competition Act 1998

の決定など、市場における競争に影響を与える可能性のある情報が、その市場に参加している同業者同士で交換される場合、1998 年競争法の第 1 章及び第 101 条（1）TFEU に該当し、違法となりうる。競合会社間での機密情報の交換が、それ自体が、市場の運営に関して不確実性を軽減又は除去した場合には違法となりえる。なぜなら、市場参加者間の情報交換は、不確実性を低減又は除去することができ、価格競争や技術競争を減殺してしまうからである。

6　刑事営業秘密法

英国では、営業秘密の不正開示、使用、取得自体が犯罪となる旨の特別な刑事法は制定されていない。上述のように、例えば外部者が、営業秘密保有者から許可を受けた者にのみアクセスが許されている、営業秘密を保存しているコンピューターに侵入して、データを盗取した場合には、コンピューター装置不正アクセス法の適用がありうる。

さらに、従業員でも、立ち入りの許されていない施設に立ち入るなどした場合には、不法侵入に関する犯罪が成立し、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 条が適用になる[355]。

7　重複する知的財産権侵害に基づく請求

また、以下のような情報の持ち出しがされ、不法にコピーされて配布されている場合には、著作権法、特許法、意匠法の侵害が問題となることもある[356]。

a. 機械工学的デザイン
b. 製造デザインやモデル
c. デザインの仕様書
d. 詳細な技術的情報
e. 技術的図面
f. データシート
g. 操作マニュアル
h. 説明図や写真
i. 報告書や見積書
j. 価格設定表

[355] 1968 年窃盗法
[356] TBD(Owen Holland) Ltd v Simons & Ors [2020] EWHC 30

1　EU 指令/UK TS 規則による営業秘密保護とコモンローの機密情報保護との関係を問題とした判例

UK TS 規則は、第 3 条において、UK TS 規則の発効後も、コモンローで衡平の原理に基づいて認められてきた守秘義務違背を請求原因とする請求を行うことができ、それは、UK TS 規則下の営業秘密侵害行為の請求に代えて、あるいは、加えて請求することができる規定としている。

Trailfinders Ltd. v. Travel Counsellors Ltd. において、Hacon 裁判官は、これまでに発達した英国の機密情報保護に関する判例法は影響を受けないと判示した[357]。したがって、Hacon 裁判官は、機密情報及び営業秘密の保護は、市場における競争の促進や被用者の権利など公共の利益とのバランスに配慮する必要があると述べた上、*Faccenda Chicken* が採用した３分類のアプローチにならって、被用者が持ち出した情報がどのような情報にあたるかを吟味し、第２の機密情報にあたると結論し、機密情報に関わる過去の判例を適用した。

Hacon 裁判官は、機密情報保有者である原告が主張した、元従業員らによる黙示の守秘義務違反、及び、衡平法の守秘義務違反を認定した。更に、被告元従業員らを雇用していた被告会社に対しては、衡平法の原理に基づく守秘義務違反を認定した。他方で、Hacon 裁判官は、被告元従業員らの責任についての被告会社の代位責任は否定した。

2　EU 指令/UK TS 規則による営業秘密保護とコモンローの機密情報保護と両者を取り扱った判例

Celgard, LLC v. Shenzhen Senior Technology Material CO, Ltd では、リチウムイオンバッテリーの生産者で、製法の営業秘密を有している原告が、元従業員であった科学者が被告会社に転職して、営業秘密に該当する技術を取得、使用したとして、被告元従業員に対しては、コモンローの守秘義務違背を主張し、被告会社に対しては、営業秘密法違反を主張した[358]。なお、*Celgard* 事件では、被告会社が中国の会社であったため、英国で提起された民事事件の被告となった中国会社に対して、相当時間を要する正式な送達によらず、代替的な送達で訴状を送達しうるか、また、英国内で事件を審理することが妥当であるかについて、争われたことから、これらの点へ判断を示した。

被告会社は、被告の製品は被告自身の技術で製造されたもので、原告の営業秘密とは関係ないとし、特に、原告が主張する「営業秘密」があまりに曖昧であり、請求は不合理であり、審理を開始すべきでないと主張した。原告は、自己が営業秘密と考える製法の内容をあまり特定し

[357] Trailfinders Ltd. v. Travel Counsellors Ltd. [2020] EWHC 591
[358] Celgard, LLC v. Shenzhen Senior Technology Material CO, Ltd [2020] EWHC 2072

てないことは認めつつ、被告元従業員が被告会社に転職後、被告会社の商品ラインが増加し、商品の製法に基づくと考えられる性能が向上し、市場シェアが増加していることなどの状況証拠に依存し、不正使用があると主張した。裁判所は、原告が主張する営業秘密の特定自体は不十分であるにもかかわらず、状況証拠に鑑み、営業秘密の不正使用の蓋然性は否定できないとした[359]。

送達に関しての管轄権の有無について、裁判所は、差止命令により禁止される被告の行為が英国内の行為を想定していること、原告が英国内で損害を受けていること等から肯定した。

また、英国で審理することが妥当であるか（Forum Non Conveniens)については、事件で原告の行う請求原因事実だけに限らず、紛争の全体を考慮し、英国外では受けられない救済がないかを考慮しなければならない[360]と述べて、被告従業員は、米国で雇用されていた後、中国において被告会社に勤務している場合でも、英国内への被告会社商品の流入、英国の顧客の奪取の観点を無視できないことやその他の事情から、英国で審理することは可能であるとした[361]。裁判所は、その判断の中で、準拠法についても検討し、原告が被告らの守秘義務違背により受けた損害は英国で発生していることから、英国法が適用されるとした。

3　機密情報保護の暫定的措置の期間設定、賠償額算定の基礎

デジタルコインのプラットフォームを運営する原告が、退職後に原告を中傷する元ディレクターの被告に対して、機密情報を不正に使用している、あるいは、原告の知名度を不正に使用してなりすましている（Passing-off）などと主張し、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を得ていた[362]。裁判所は、原告が金銭的賠償を既に請求していること、金銭的損害は、被告の侵害行為がなければ、原告が享受しえたであろう経済的利益を、原告に回復させることを目的としていること、暫定的措置も同様に、原告の損害を填補、回復する目的で付与されることを確認した。争点となった暫定措置の期間について、裁判所は、被告が原告に対して、役員として法律に基づいて信任義務を負っていたことから、一定期間中は原告の機密情報を原告にとって不利になるように使用すべきでないことを肯定したものの、原告が保有していたデータベースや顧客リストを、不正に使用したことがないことを認め、機密情報を不正使用するような被告の意図が明らかでないことを重視し、全体で６ヶ月に限定した。

[359] 原告は、証拠保全命令を得たり、コンピューター映像化、検証命令を受けたり、捜索命令を活用したり、文書提出命令を求めることができる。
[360] Re Harrods Buenos Aires Ltd [1992] Ch 72
[361] 被告会社の商品は、中国で製造されている可能性は、裁判所も認識していた。
[362] C Wzrd Ltd & Anor v. Kortan & Anor [2020] EWHC 1360 (Ch).

4　秘密保持契約の効力を否定した例

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、その規定が、機密情報を網羅的に下記のように定義していた[363]。

> 機密情報とは、機密情報と明記されているか否かにかかわらず、（1）当社が機密情報と考える当社の経営、顧客、製品、事務、並びに、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、及び、（2）当社の経営、並びに、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、機密情報にアクセスすることがある。あなたは、雇用中と雇用終了後も、自分の職務の適切な遂行以外に、機密情報を使用、若しくは、いかなる人、会社、他の団体にも開示しないことを合意する。

裁判所は、このような限定のない条項は不当な自由と競争の制限にあたり、法的拘束力を持たないと、傍論で結論した。

5　暫定措置の内容を複数の期間に分割して、異なった内容の秘密保持措置を命じ、擬制信託を否定し、秘密保有者の「汚い手」について言及した例

従前より、雇用者等の営業秘密保有者が、以下で説明するような、製造や販売等の差止命令、証拠提出命令、収支の報告命令、被告の営業利益の擬制信託への吸収等、強力な（暫定又は恒久的）措置を、競争相手や元従業員に対して発動し、決定的なダメージを与えることができることの問題は認識されてきた。そこで、既に現状維持のための差止命令が発令されている場合には、それに加えて、被告の製品を原告や中立的な保管者へ送付すべきとする命令は不要、と結論する裁判例が存する[364]。

擬制信託とは、当事者間に信託契約が無いにもかかわらず、自己の違法な（大抵の場合には、原告の信頼を裏切るような形でなされる）行為に直接的に由来して、利益を得ている被告に対し、あたかも信託の受託者の忠実・誠実義務を負っているかのように考えて、被告の営業活動の内容について、原告に報告させるとともに、収益を自己の財産とは分離して、確実に管理さ

[363] Quilter Private Client Advisers Ltd v. Falconer & Anor [2020] EWHC 3294.
[364] Ocular Sciences Ltd v Aspect Vision Care Ltd (No.2) [1997] RPC 289

せるという措置を課すものである[365]。英国の裁判例で認めたものもあるが、積極的に擬制信託を課すことは妥当ではないのではないか、という意見が強い[366]。

また、営業秘密保有者が自己の顧客に対して、裁判所が実際に与えた救済措置以上に命令があるかのように誤導するなどして、不正な行為を行った場合には、そのような行為が救済の否定につながることを示唆した。具体的には、既に存在する暫定措置による制約で守られる利益が十分なことも考慮しつつ、営業秘密保有者が求めうる内容を制限的にのみ認容した[367]。

6　暫定的措置

(1) 一方的申立て（非対審式）

暫定的申立ての多くが、まずは営業秘密保有者が一方的な(ex parte)暫定的措置の発動を求めることから始まるため、機密情報や営業秘密を侵害するような被申立人の行為の差し止めを求め、被申立人が参加せず、対審構造をとらない手続で決定に至ることが多い[368]。これには、営業秘密保有者にとって非常に迅速な救済が得られるというメリットがある反面、制度が濫用される恐れがある。一つの対策として、申立人は、被申立人が被る可能性のある損害を担保するため、担保を預託しなければならないとされている。

以上とは別に、より幅広い、あるいは、より強力な暫定的措置の申立てに関しては、被申立人の参加を許した後に決定に至るという段階を得て発せられる[369]。

(2) 暫定的差止命令の要件

裁判所は、暫定的差止命令申立において、下記の事項を考慮して、措置を命じるかどうか決定する[370]。

a. 本案で審理されるべき重要な問題がある（申立人が勝訴する合理的な可能性がある）
b. 本案が解決するまで待てない緊急の必要性を申立人が有する（金銭的賠償に代えられない利益）
c. 申立人と被申立人の被る困窮度の比較
d. 現状が維持されなければならないとする要素の存在[371]

[365] Ocular Sciences Ltd v Aspect Vision Care Ltd (No.2) [1997] RPC 289、Spycatcher case [1990] AC 109 参照。
[366] Ocular Sciences Ltd v Aspect Vision Care Ltd (No.2)
[367] Fortescue Metals Group Ltd & Anor v. Argus Media Ltd & Anor [2020] EWHC 1304 (Ch).
[368] Huw Evans, et al., Trade Secret Protection: the regimes in key jurisdictions (2017)
[369] Forse and others v Secarma Ltd and others [2019] EWCA Civ 215
[370] Forse and others v Secarma Ltd and others [2019] EWCA Civ 215
[371] American Cyanamid Co v. Ethicon Ltd [1975] AC 396

(3) 暫定措置の内容

暫定措置の内容として最も基本的なのは、被申立人による機密情報の不正な使用、開示、取得（譲渡しと譲受け）の禁止である。この他にも、下記のようなことを命じる決定がなされうる。

① 捜索と押収命令

1975年、*Anton Piller KG v Manufacturing Processes Ltd & Ors*事件において、英国裁判所は、申立人が被申立人の事業敷地内に赴いて、不正取得、使用の決定的証拠となる文書の捜索と押収ができる旨の命令を下した[372]。申立人であるAnton Piller KGは、被申立人が機密情報を不正に開示しており、技術的図面及び手順書を著作権を侵害してコピーしていると主張した。申立人は、一方的な審理手続きで、被申立人の敷地に立ち入り、関連文書を検証し、押収することを許可するよう裁判所の命令を求めた。下級審は却下したが、上級審のOmrod裁判官は、次の要件下に、申立てを認めることとした。

a. 申立原因事実について、格別に強固な立証があること、
b. 予測される、又は、現実の損害が、申立人にとって、非常に重大であること、
c. 被申立人が、その手中に、侵害の事実を明らかにする文書や物体を所持しており、もし、被申立人に手続きへ参加させる審理をすると、それら資料を破壊する現実的恐れがあることを明白に示す証拠がある。

この捜索と押収命令は、被申立人に通知をしないで、決定を得られる点で、営業秘密を保有する申立人に有利であるため、頻繁に利用されるようになった。他国でも（オーストラリア、カナダ、香港、インド、アイルランド、イスラエル、ニュージーランド、南アフリカ）裁判所は、この方式を採用した。さらに、捜索と押収命令は、機密情報たる物やデータそのものが被申立人の管理下にある場合、これら機密情報を取り戻すためにも使用されている[373]。

② 資産凍結命令

侵害者が、比較的弱小な法人で、経営状況が不安定である場合、若しくは、資産隠しをする可能性がある場合など、申立人は、被申立人の財産が処分又は変動しないようにする、資産凍結の命令を求めることができる[374]。要件としては、

a. 申立原因事実について、一応の立証がある、

[372] Anton Piller KG v Manufacturing Processes Ltd & Ors, [1976] 1 All ER 779, [1975] EWCA Civ 12, [1976] Ch 55.
[373] Yousif v Salama and Another [1980] 1 WLR 1540
[374] Huw Evans、脚注368

b. 資産が減少する恐れがある、

c. 被申立人が、裁判所の管轄地内に、資産を有している。

本命令も、被申立人にとって致命的な打撃を与える可能性があるため、より緩やかな手段で目的を達成できないかを検討する。

③ 証拠保全命令

証人審問が終了するまで、証拠を滅失させたり、変造したり、性質を変えるなどを禁止する[375]。

④ 送付命令

被申立人に対し、いくつかのカテゴリーの情報を申立人に提供させることを命じる。被申立人は、申立人がコンピューターフォレンジックを用いて情報を解析できるような形態で、これを提供しなければならない[376]。

また、被申立人に対し、機密情報の侵害（不正な取得、開示、又は、使用）の結果により作られたと疑われる製品を、申立人が吟味できるように、申立人の指定する場所へ送付すべきことを命じることも可能な場合がある。

⑤ 報告命令

被申立人が機密情報を不正に使用して、申立人の技術を実装した製品を製造したり、顧客を得ている疑いのある場合、被申立人の関連する事業の収支について報告させるものである。

第5章 域外適用

以下は、営業秘密保護法の域外適用についてであるが、英国の欧州連合離脱を念頭として、法制度、裁判例を説明する。

上述のように、コンピューター不正使用法UK TS規則は、EU指令を英国内法に移行、実施するために、第2条において、「営業秘密」、「侵害行為」、「侵害品」に関して定義を設けた[377]。そこで、機密情報の不正な開示、取得、使用に対するコモンローの保護とは異なる地理的保護範囲を議論する余地が生じた。

EU指令/UK TS規則の域外適用を問題とした裁判例には、*Celgard, LLC v. Shenzhen Senior Technology Material Co.*があり[378]、下記のように、重要な判示がなされた。営業秘密の実際

[375] Huw Evans、脚注368
[376] Huw Evans、脚注368
[377] UK TS規則第2条
[378] Celgard, LLC v. Shenzhen Senior Technology Material Co Ltd [2020] EWHC 2072

の取得や営業秘密を使用した商品の製造は、英国外でなされている。

原告は、被告らの守秘義務違背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。下級審は、原告の求める、被告会社製品の英国内への輸入の差し止め等の請求に、中国の裁判所が中国法を適用する可能性は低いと、専門家証人が結論していることから、英国法が適用されると認めた。

上級審(Arnold LJ, Popplewell LJ と Davis LJ が同意）は、EU 指令第 4(5)条の解釈を議論し、下級審の結論を支持した[379]。

第 6 章 営業秘密、機密情報の事件数（本案裁判例）

営業秘密事件の民事事件数の概要、刑事責任訴追状況を述べる。

1 刑事

営業秘密侵害罪がないため、刑事事件は存在しない。

2 民事

民事事件については、EU 指令を受けて UK TS 規則が制定され、営業秘密侵害自体を保護する法律が誕生したことから、事件数は今後増加していくのではないかと考えられる。しかし、UK TS 規則施行後の、公開されている裁判例では、営業秘密を扱った民事事件 (2020 年 1 年間）は、全英国で 14 件、機密情報で 20 件に過ぎなかった[380]。これは、UK TS 規則施行直後であることが関係している可能性がある。

しかし英国では、これまでも、本案訴訟となる営業秘密事件も機密情報事件も非常に少なかった。それには、以下のような理由が考えられる[381]。

まず、機密情報も営業秘密も、知的財産権とは認められておらず、契約に基づく関係や衡平法などの、当事者間の関係と切り離して考えることは難しいことから、契約にまつわる事実や当事者のインタラクションが紛争の鍵となり、かつ、請求の原因となる。

---

379 とりわけ、パラグラフ 3 が、「営業秘密を違法に取得した」と規定し、取得が「違法」であったかどうかの問題にどの法律を適用すべきかという問題を未解決のままにしていると認めた。したがって、これはやがて CJEU が回答する必要があることを認めた。Shenzhen Senior Technology Material Co Ltd v Celgard, LLC (Rev 1) [2020] EWCA Civ 1293.

380 Bailii ウェブサイトの事件検索結果 https://www.bailii.org/form/search_cases.html.

381 Mr. Williams 氏のインタビュー

また、申立てにより、侵害者に対する暫定的措置が発せられた場合、かなり多くの場合で紛争は解決するので、本案事件の提起も必要がない。

よって、比較的訴訟数の少なかった英国での、営業秘密を含む機密情報に関連する法はこれから進展する可能性がある。刑事罰の立法化も、全く可能性がないとは言えないが、表面化はしていない。

第 7 章　営業秘密関連の法改正

営業秘密に関連した法改正の動向であるが、上記のように、営業秘密に関する新法である UK TS 規則は、2018 年に誕生しており、現時点では、さらなる国内法改正の動きがない。

なお、Brexit 後の UK-EU 間の知的財産権関連の条約締結の動きであるが、House of Lords による調査報告では、Draft の条約では、営業秘密の保護は特に変更が無いであろうとされている[382]。

第 8 章 国際協力・他国との連携状況

以下で、英国政府による、営業秘密保護のための他国との連携について述べる。

英国は、EU を脱退しているが、EU 指令 に基づいた国内法を制定しているため、EU 諸国の営業秘密保護と同レベルの保護は確保されている、という認識が一般である。英国の Customs & Border における営業秘密侵害品の押収は、他の EU 諸国と同様に、非常に難しいとされている[383]。これは、営業秘密侵害品に限らず、特許侵害品についても同様である。なぜなら、税関職員には、侵害品であるかどうかを容易に判断する能力がないためである。したがって、営業秘密保有者が税関職員に請求するなどして、侵害品の押収を委託することは期待できないと考えられている。

前述のとおり、英国の裁判所は、米国で不正に取得され、中国等で不正に使用されている営業秘密の侵害事件について、英国に輸入されようとしている場合に、機密情報の侵害行為に対する管轄を肯定した[384]。また、米国で本案が係属している事件について、たまたま侵害者が英国内に資産を有していた場合、被告の資産を凍結する命令を出した事件もある[385]。

---

[382] Professor Phillip Johnson, Professor of Commercial Law, Cardiff University (PBS0013) (June 22, 2020) https://committees.parliament.uk/writtenevidence/7567/default/.
[383] Professor Phillip Johnson、脚注 382
[384] Celgard, LLC v. Shenzhen Senior Technology Material CO, Ltd [2020] EWHC 2072
[385] Motorola v. EWHC

第 9 章　仲裁の利用

一般に、仲裁手続は、裁判所における訴訟と比して、当事者が有する営業秘密や機密情報の秘密性が保たれると言われる。確かに、英国の仲裁機関で仲裁を行う場合、当事者も仲裁人も、仲裁の内容について口外しないという秘密保持の義務を負うと理解されている[386]。したがって、仲裁合意がある限り、営業秘密が問題となる事件では仲裁の利用が望ましいとも考えられる[387]。

WIPO の事務局によると、営業秘密関係事件の仲裁事件は、近時増加の傾向が見られるとのことであった[388]。これは、営業秘密を会社の知的財産権の一部あるいは周辺に位置づける実務にも由来するであろう。他の英国内の仲裁機関では、営業秘密事件数は公表されていない。

第 10 章　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

以下、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を説明する。

第一に、機密情報や営業秘密を、秘密保持義務への合意のないまま第三者に提供することは、それらの「機密性」を失わせる結果となりかねない[389]。当事者間の契約関係に由来して、黙示の（機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以上に見たとおりであるが、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）を明文で盛り込む必要がある。

ライセンス、生産委託、合弁会社設立の際に、当事者間で契約書がかわされる場合、契約書に機密保持条項を盛り込むことは通常なされるが、英国法が準拠法である場合には、以下 1.～3. のポイントに注意し、必要に応じて英国弁護士に相談するなどすべきである。

---

386 Nikki O'Sullivan, *Keeping it under wraps: the limits on confidentiality in arbitration* (2017), http://arbitrationblog.practicallaw.com/keeping-it-under-wraps-the-limits-on-confidentiality-in-arbitration/.

387 しかし、秘密保持は全能ではない。仲裁判断は、後に裁判所で争われることがあるためである。O'Sullivan、脚注 386

388 WIPO, Symposium "Thinking Internationally About IP and ADR: What Every Lawyer & Corporate Counsel Should Know Virtual Seminar" hosted by the University of Illinois System (Aug. 19, 2021).

389 前記「営業秘密の定義」を参照。

1　ライセンス契約

(1) 機密情報、営業秘密の区別

上述のとおり、英国では、機密情報と営業秘密は区別され、例えば、自己商品に内在する不具合に関して集められた情報は、機密性ある情報とは言えようが、営業秘密には該当しないと判断される可能性もある。ライセンス交渉にあたり、何が営業秘密にあたりうるかは十分に検討する必要がある。

(2) 機密情報、営業秘密の特定

第 4 章で紹介した判例のように、あまりに広範囲で網羅的な条項は、効力を否定されることがある（公正な競争の保持という公共の利益が、害されないかが問題とされる。また、当該事例のように、雇用関係に関連する場合、特に、被用者の労働の自由が考慮される）[390]。

実際に、ライセンシーにおいて機密情報が一体何なのか判別できない状況で、ライセンサーから情報を受け取っても、十分に保護のしようがない。機密情報とすべき必要性があることと、実際に機密情報として扱われていることが、後に争点となり、審査されるのであり、機密情報・営業秘密を明確に特定し、秘密性に配慮した受渡しをすることが非常に重要となる。

(3) 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

契約条項を作成する場合、何が許されるか、そして、何が不正取得、使用、又は、開示になるかを明確にすることは、ライセンシー及びライセンサーの利益を守り、また、有効な関係を維持するためにも大切である。例えば、ライセンシー側で、パスワード等アクセス制限を設定すること、アクセスできる者を制限すること、アクセスの目的と使用方法を制限することなどが考えられる。

衡平法上の守秘義務違背には、行為者が機密情報の不正使用にあたることを認識していたか、認識すべきであったことが、前提とされており、許可事項と不許可事項を分別することが意味を持つと考えられる。

また、新法である UK TS 規則は、営業秘密保有者において、機密性を保つ合理的な措置をとっていたかを要件として導入した。[391]未だ判例法として確立はしていないものの、ライセンサー内部で機密性保持がどのように実施されるべきかは逐次検討し、不十分な点は是正すべきである。

---

[390] Quilter Private Client Advisers Ltd v. Falconer & Anor [2020] EWHC 3294.
[391] UK TS 規則第 2 条

(4) 契約終了後の情報の返却あるいはデータ削除義務

秘密保持義務の内容として、提供された機密情報、営業秘密は契約関係終了時に、保有者に返却すること、また、バックアップも含めて、保存されたデータから削除するように要求すること、それを確認すること、を明記することが必要である。これは、前記の、機密性を保つ合理的な措置の認定にも、プラスの要素として働くと考えられる。

(5) 損害額

機密情報・営業秘密保有者は、不正取得、使用、あるいは、開示により生じた損害に対する賠償として、特約がない場合、自分の被った損害を立証して、その填補を求めることができる。この損害の立証は、営業秘密侵害行為の立証や損害の特定と関連して、困難となることも考えられるので、損害額の算定について、事前に合意しておくことも考えられる。

(6) 仲裁合意

裁判による紛争解決と比較し、仲裁は、営業秘密、機密情報の保護に適し、手続きで提出あるいは開示された情報の秘密性が保たれやすいと考えられている。そこで、ライセンス契約にあたっても、仲裁条項を挿入して、仲裁により契約の紛争を解決し、ライセンサーの機密情報や営業秘密の保護を図ることは、積極的に検討されるべきである。

2 生産委託契約

上記に列挙した注意点は、生産委託契約にも当てはまる。

委託者としては、受託者の生産ラインの運営状況、生産品の数量等確認体制、保存・管理状況を十分確認することが特に重要となると考えられる。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は検討されるべきである。

生産委託契約では、受託者が、第三者の機密情報、営業秘密をたまたま持っていて、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、請求を起こされてしまう可能性がある。委託者としては知り得ない場合にも、「侵害品」に対する救済は与えられているので、影響を受けることとなる。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は、検討されるべきである。

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は特に重要となる。

参考書式　目次

1　就業規則における秘密保護関連規定の例

Trade Secret Policy

Scope

This policy sets forth procedures and measures to protect information identified as trade secrets owned by Company entities that shall affect all Company employees (herein, employee includes part and full time; temporary and permanent) and contractors.

Policy

1. Trade Secret Definition

A trade secret is information that is kept secret and provides economic value or a competitive advantage to Company because of its status as secret. Examples of information that could be considered a trade secret include information such as, but not limited to, formula, pattern, algorithm, compilation, program, method, technique, customer lists, data sets or compilations, product road maps, pricing schedules, failed experimentation, or manufacturing processes.

Information qualifying as a trade secret shall be identified as such by Company's Intellectual Property (IP) committee and those employee(s) authorized to access the trade secret shall be responsible for maintaining its secrecy.

Factors that weigh into the consideration as to whether information should be considered a trade secret or Company confidential information or alternatively protected under other forms of IP are as follows:

- extent the information is known outside the business
- extent the information is known inside the business
- extent of measures that are used to guard the secrecy of the information
- ease or difficulty to reverse engineer
- value of the information to company and competitors
- effort/cost to develop information

In certain jurisdictions, the trade secret needs to be continuously used in the business.

2. On-Boarding Acknowledgement and Employment Agreements

a. At some point during the on-boarding process, an employee or contractor shall acknowledge that they will not use or disclose the trade secrets, inventions, and other proprietary and confidential information belonging to third parties. An acknowledgement form regarding third party trade secrets and proprietary information will be provided.
b. Before the employer/employee or employer/contractor relationship begins or meaningfully changes (e.g., by a promotion or assignment change) and before any trade

secrets are disclosed, the employee or contractor shall sign an agreement that includes at least the following:

i. **IP Assignment**: Every employee or contractor shall sign an IP assignment. The agreement shall include a present assignment expressly transferring to the Company as the owner of IP, IP including trade secrets, developed by the employee during and in connection with his or her employment. A similar assignment also shall be signed by consultants, licensees, or other third parties where applicable.
ii. **Confidentiality Provision**: Every employee or contractor shall sign a Confidentiality Agreement acknowledging their duty of confidentiality with respect to Company's information and trade secrets. A similar agreement also shall be signed by consultants, licensees, or other third parties.
iii. **Non-Compete/Non-solicitation:** To the extent permitted by law, the agreement shall contain provisions prohibiting an employee or contractor from accepting employment or performing services for a competitor or competing with Company or soliciting a former employer's customers or employees.

For additional information, please consult the *Employee Handbook* and/or Human Resources (HR).

3. Third Party Agreement

Prior to entering a contractual relationship with a third party, a non-disclosure agreement (NDA) or agreement containing confidentiality provisions shall be executed before any Company confidential information -particularly trade secret information- is shared. **If trade secrets are to be shared with third parties, kindly alert the Legal Department so additional contractual provisions may be included in the NDA or other agreement for added protection.**

4. Physical Security Measures

a. **Facility Security Measures**: Access into and out of the facility shall be controlled and monitored with visitor sign-in logs with picture ID required, visitor non-disclosure agreements (NDA's), pre-approval of all visitors, and surveillance cameras. All visitors shall be accompanied by an escort while on-site and are prohibited from on-site use of any device with recording capability (e.g., camera, video-camera, stop-watch or smart-phone with any of those functions).
b. **Restricted Access**: Access to the building shall be restricted through locked doors requiring badge entry issued to only authorized employees and contractors. All physical embodiments of a trade secret, whether a prototype, working model or actual embodiment in use, shall be maintained in a restricted area that is under lock and key and out of view. Employees or contractors shall put working materials or files containing trade secrets in a locked desk or filing cabinet when not in use (see *Clean Desk Policy*).

5. Marking

A trade secret shall be conspicuously marked as strictly confidential per our Global Marking Policy. This marking shall differentiate the trade secret information from other Company confidential

information. Accordingly, for trade secret information all physical documents and digital files shall include "Company Strictly Confidential" either in the form of a header, footer or watermark. In any instance where trade secret information can be copied or downloaded, such copying of such document or digital files is tracked, monitored, and destroyed after use.

6. Trade Secret Storage

a. **Identification and Description of Trade Secret**: Once information has been identified as trade secret, the Company IP attorney will prepare a brief description of the trade secret.
b. **Protective Measures:** Trade secrets will be maintained and protected in a manner that is greater than that of Company confidential information. All trade secrets shall be stored in a trade secret database on a Company controlled network that is password protected where the password is known only to Authorized Persons (defined in Section 7 herein). Additional encryption measures may be used where appropriate. The database shall be maintained by a Company IP attorney and/or Information Technology (IT) where access is granted. Trade secrets shall be segregated from other Company confidential information and only accessible through a Company-controlled network and not through any other network, cloud storage, or the internet except via the Company Internal Private Network (VPN). Old hardware, such as laptops or hard drives containing trade secret information, should be physically destroyed rather than being thrown away or recycled.

7. Limited, Need-to-Know Access

a. **Responsible Employee**: Employee(s), as designated by a Company US IP attorney or the Company IP committee, shall be responsible for maintaining the secrecy of each trade secret by ensuring that the requirements of this policy are met for that trade secret.
b. **Authorized Persons Only**: Access or use of a trade secret by an authorized person is authorized only if, and only to the extent, he or she needs to access or use the trade secret to perform his or her job responsibilities. An authorized person may copy a trade secret, or a portion of a trade secret, only if necessary, to perform his or her job responsibilities. All such copies shall be promptly destroyed, i.e. rendered indecipherable and unable to be reconstructed once they are no longer needed.
c. Visitors must sign acknowledgments prohibiting disclosure of information viewed or accessed during a visit, preventing them from bringing recording devices (e.g., cameras, cell phones, USB drives) into restricted areas, and requiring that they be accompanied by employees while in locations where they may access sensitive information.
d. **Electronic Information Management**:
    i. Access to trade secrets shall be limited to only authorized persons and through only authorized means.
    ii. If information relating to a trade secret must be shared between authorized persons, it shall be done through secure transfer means, i.e. via encrypted email or a secure file transfer.
    iii. A list of the persons authorized to access a trade secret shall be maintained by the Responsible Employee for each trade secret and/or the Company IP Attorney.

8. Protected Networks and Mobile Devices

a. **Network and Device Security**: Network and device security solutions shall be maintained by Company's IT department as in the normal course of business.
b. **Personal Devices**: Employees and contractors shall follow Company's policies regarding use of company devices that precludes employers and contractors from using personal devices for work related matters unless he or she has complied with Company's *Bring Your Own Device (BYOD) Policy*. **Downloading or use of trade secret information on personal devices is prohibited.**
c. **Portable Device or Drives:** Portable devices or drives are not allowed for use on Company computers.

9. Proprietary Data Control

All presentations, articles, and research papers that are to be publicly disclosed, or otherwise disclosed to non-employees, shall be reviewed by a Company IP attorney prior to the disclosure, so that trade secrets and any other Company confidential information are not disclosed.

10. Employee Training

Employees and contractors shall receive IP training as a part of Company's New Hire Orientation, as applicable. The IP training portion shall include the topics of trade secrets and Company's trade secret policy. Thereafter, employees and contractors shall have periodic certifications and policy acknowledgements of IP and Trade Secret Policy training.

11. Off-Boarding Process

Exit interviews shall be conducted for all employees and contractors who have been terminated or are otherwise departing Company. During the exit interview, at least the following steps will be performed:

a. Upon resignation or termination, Company IT shall be alerted, and the departing employee or contractor shall have their e-mail access and network access disabled. All employee or contractor passwords shall be terminated. Any laptops, phones, or other company provided devices will be retrieved by IT, and employee or contractor shall sign an acknowledgment that all company-provided laptops, documents, etc. have been returned.
b. The employee or contractor shall be provided with a copy of the agreements from Section 2 herein, including the Confidentiality Agreement which references the employee's or contractor's continuing duty to keep trade secrets (and other Company confidential information) confidential. The employee or contractor will be reminded of their continuing duty with respect to Company confidential information and trade secrets and shall sign an acknowledgement of such reminder.
c. Access keys, keys to desks or cabinets, company credit card, and/or key cards shall be returned to Building Security and/or Human Resources (HR).
d. Any laboratory or engineering notebooks shall be retrieved and inventoried by the Company IP department. The Company IP attorney shall remove the employee from any authorization lists.
e. If a personal device was used for work related duties, it shall be cleansed of any sensitive company information.

f. Request IT to monitor any downloads of Company information via portable devices by departing employee and/or e-mails to employee personal e-mail or out of Company network account.

An Exit Interview Form (to be completed prior to employee or contractor departure) should be used as part of the off-boarding process. For additional information, please consult the *Employee Handbook* and/or Human Resources (HR).

12. Remedies for Trade Secret Misappropriation

Trade secret misappropriation is governed by State (or in Canada Provincial) and Federal laws. Remedies for trade secret misappropriation may include injunctive relief, monetary damages, attorneys' fees, litigation costs, and in some cases, criminal sanctions including fines and imprisonment.

13. Whistleblower Immunity Notice under the Defend Trade Secrets Act of 2016

An employee or contractor will be immune from an action that would otherwise count as trade secret misappropriation if the disclosure is made (i) in confidence to a Federal, State, or local government official, either directly or indirectly, or to an attorney; and (ii) solely for the purpose of reporting or investigating a suspected violation of law; or is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal. (18 U.S.C. 1833(b)).

This notice shall be included in Confidentiality or Non-Disclosure Agreements and NDAs entered by Company described in Section 2 herein.

Related Policies:
Employee Handbook
Clean Desk Policy
Bring Your Own Device (BYOD)
Global Marking Policy – Confidential Information

（参考和訳）就業規則における秘密保護関連規定の例

営業秘密方針

範囲

このポリシーは、企業が所有する、企業秘密として識別される、情報を保護するための、企業の全従業員（従業員は、パートタイムとフルタイム、一時的および永続的を指す）及び請負業者に当てはまる、手順と対策を定める。

ポリシー

1. 営業秘密の定義

営業秘密とは、秘密にされており、その秘密としての地位のために、経済的価値又は競争上の優位性を、企業に与える情報である。営業秘密と見なすことができる情報の例には、方式、パターン、アルゴリズム、編集、プログラム、方法、技術、顧客リスト、データセット又は編集、製品ロードマップ、価格設定スケジュール、失敗した実験、製造方法などが含まれるが、これらに限定されない。

営業秘密に該当する情報は、企業の知的財産（IP）委員会によって、そのように特定され、営業秘密へのアクセスを許可された従業員は、その秘密性を維持する責任を負う。

情報を営業秘密又は企業の機密情報と見なすか、あるいは、他の形式の IP で保護するかを検討する際の要素は、次のとおりである。

1) 情報がビジネス外で知られている範囲
2) 情報がビジネス内で知られている範囲
3) 情報の秘密を守るために使用される措置の範囲
4) リバースエンジニアリングの容易さ又は難しさ
5) 企業や競合他社にとっての情報の価値
6) 情報を開発するための努力/コスト

特定の法管轄域では、営業秘密を、ビジネスで継続的に使用する必要がある。

2. 入社時の確認および雇用契約

a. 入社手続のある時点で、従業員又は請負業者は、第三者に属する営業秘密、発明、その他の所有情報及び機密情報を、使用又は開示しないことを確認する。第三者の営業秘密および所有情報に関する確認書が提出される。
b. 雇用主/従業員又は雇用主/請負業者の関係が始まる前、若しくは、意味のある変更（昇進や配属の変更など）の前、および何らかの営業秘密が開示される前に、従業員又は請負業者は、少なくとも以下を含む契約に署名する必要がある。

i. IP 譲渡：すべての従業員又は請負業者は、IP 譲渡に署名する必要がある。契約には、従業員が、明示的に、雇用中、及び、雇用に関連して開発した、営業秘密を含む IP を、所有者として企業に譲渡する現在の譲渡が含まれる。同様の譲渡は、該当する場合は、コンサルタント、ライセンシー、又は他の第三者によっても署名されるものとする。

ii. 機密保持義務条項：すべての従業員または請負業者は、企業の情報及び営業秘密に関する機密保持義務を認める契約に署名する。同様の契約は、コンサルタント、ライセンシー、又は他の第三者によっても署名されるものとする。

iii. 非競争/非勧誘：法律で許されている範囲で、契約には、従業員又は請負業者が、競合他社との間で雇用受入れ、又はサービス提供、企業との競争、若しくは、元雇用主の顧客または従業員の勧誘を、禁止する条項が含まれる。

詳細は、就業規則及び/又は人事課にて、参照すること。

3. 第三者との契約

第三者と契約関係を結ぶ前に、企業の機密情報（特に営業秘密情報）を共有するより先に、機密保持契約（NDA）または機密保持条項を含む契約を締結しなければならない。営業秘密を第三者と共有する場合は、法務部に警告し、追加の保護を与えるため、NDA 中の追加の契約条項、又は、その他の契約を含めることができるようする。

4. 物理的な安全性措置

a. 施設のセキュリティ対策：施設への出入りは、写真付き ID が必要な訪問者のサインイン記録、訪問者の機密保持契約（NDA）、すべての訪問者の事前承認、及び、監視カメラにより、管理並びに監視されなければならない。すべての訪問者は、現場付添いを要するものとし、記録機能を備えたデバイス（カメラ、ビデオカメラ、ストップウォッチ、またはこれらの機能を備えたスマートフォンなど）を現場で使用することは禁じられている。

b. アクセスの制限：建物へのアクセスは、許可された従業員と請負業者にのみ発行される、バッジを必要とする、施錠されたドアによって制限される。営業秘密のすべての物理的実施形態は、プロトタイプ、開発中モデル、又は、実際に使用されている実施例かにかかわらず、施錠され、視界に入らない、制限領域に維持されるものとする。従業員又は請負業者は、使用していないときは、営業秘密を含む作業資料又はファイルを、施錠された机またはファイリングキャビネットに入れなければならない（整頓された机ポリシーを参照）。

5. マーキング

営業秘密は、当社のグローバルマーキングポリシーに従って、厳重に機密として目立つようにマークされる。このマーキングは、営業秘密情報を、他の企業の機密情報と区別する。したがって、営業秘密情報の場合、すべての物理的文書およびデジタルファイルには、ヘッダー、フッター、または、透かしのいずれかの形式で「社内厳重機密」を含める必要がある。営業秘密情報を、コピー又はダウンロードできる場合は、そのような文書又はデジタルファイルのコピーは、常に追跡、監視され、使用後に破棄される。

6. 営業秘密の保管

a. 営業秘密の特定と説明: 情報が営業秘密として特定されると、企業の知的財産弁護士が営業秘密の簡単な説明を作成する。
b. 保護措置：営業秘密は、企業の機密情報より厳重な方法で、維持および保護される。すべての営業秘密は、パスワードで保護された、企業が管理するネットワーク上の営業秘密データベースに保存され、パスワードは、被許可者（第 7 条で定義）のみが知っているものとする。必要に応じて、追加の暗号化手段を使用できる。データベースは、アクセスが許可されている、企業の IP 弁護士及び/または情報技術（IT）課によって、保持される。営業秘密は、他の企業の機密情報から分離され、企業が管理するネットワークを介してのみアクセス可能で、企業の内部プライベートネットワーク（VPN）を介する場合を除き、他のネットワーク、クラウドストレージ、またはインターネットを介してアクセスすることはできない。営業秘密情報を含むラップトップやハードドライブなどの古いハードウェアは、廃棄、リサイクルするのではなく、物理的に破壊する必要がある。

7. 限られた、知る必要のあるアクセス

a. **責任ある従業員**：企業の米国 IP 弁護士又は IP 委員会によって指定された従業員は、このポリシーの要件が、その営業秘密について満たされていることを確認することで、各営業秘密の秘密性を維持する責任を負う。
b. **被許可者に限定**：許可された者による営業秘密へのアクセス又は使用は、その者が職務を遂行するために、営業秘密にアクセス又は使用する必要がある場合にのみ許可される。許可された者は、必要な場合に限り、営業秘密又は営業秘密の一部をコピーし、職務を遂行することができる。そのようなコピーはすべて、必要がなくなると、すぐに破棄、即ち、解読、再構築できないようにされる。
c. 訪問者は、訪問中に閲覧又はアクセスされた情報の開示、並びに、記録装置（カメラ、携帯電話、USB ドライブなど）の制限区域内持込みが、いずれも禁止され、企業機密情報にアクセスする可能性のある場所では、従業員の同伴を要する旨を確認する書面に署名する必要がある。
d. **電子情報管理**：
    i. 営業秘密へのアクセスは、許可された人物のみ、かつ、許可された手段のみを介するよう、制限される。

ii. 営業秘密に関連する情報が許可された者の間で共有する必要がある場合、それは安全な転送手段、つまり暗号化された電子メール又は安全なファイル転送を介して行われる。
iii. 営業秘密へのアクセスを許可された者のリストは、各営業秘密の責任ある従業員及び/又は企業の IP 弁護士によって維持される。

8. 保護されたネットワーク及び携帯

a. **ネットワークとデバイスのセキュリティ**：ネットワークとデバイスのセキュリティソリューションは、通常の業務と同様に、企業の IT 部門によって維持される。
b. **個人用デバイス**：従業員と請負業者は、企業の個人所有デバイス持参（BYOD）ポリシーに準拠していない限り、仕事関連の問題での個人用デバイス使用を禁止している、企業のデバイス使用に関するポリシーに従う。これにより、雇用主と請負業者は、営業秘密情報を、個人のデバイス上にダウンロード、又は、それで使用することが、禁止される。
c. **ポータブルデバイスまたはドライブ**：企業のコンピューターでのポータブルデバイス又はドライブの使用は許可されない。

9. 所有データ管理

公に開示される、又は、その他非従業員に開示される、すべてのプレゼンテーション、記事、及び研究論文は、営業秘密及びその他企業の機密情報が開示されないように、開示前に、企業の IP 弁護士によってレビューされる。

10. 従業員研修

従業員と請負業者は、必要に応じて、企業の新入社員オリエンテーションの一環として、IP トレーニングを受ける。 IP トレーニングの部分には、営業秘密および企業の営業秘密ポリシーのトピックが含まれる。その後も、従業員と請負業者は、IP および営業秘密ポリシートレーニングの定期的な認証とポリシー確認を得る必要がある。

11. 退職時手順

退職面接は、解雇された、又は、企業を辞めた全従業員及び請負業者に対して、実施される。終了時面接では、少なくとも次の手順が実行される。

a. 辞任または退職すると、企業の IT に警告が発せられ、退職した従業員または請負業者の、電子メールアクセスとネットワークアクセスを無効にする必要がある。すべての従業員又は請負業者のパスワードは終了する。ラップトップ、電話、その他の企業が提供するデバイスは、IT によって取り返され、従業員又は請負業者は、企業が提供するすべてのラップトップ、ドキュメントなどが、返却されたことの確認書に署名する必要がある。
b. 従業員または請負業者には、従業員または請負業者の、営業秘密（およびその他の企業の機密情報）の機密性を保持する継続的な義務に言及する、機密保持契約

を含む、本契約第 2 条以降のコピーが提供される。従業員または請負業者は、企業の機密情報および営業秘密に関する、継続的な義務について注意喚起され、その確認書に署名する。

c. アクセスキー、デスクまたはキャビネットへのキー、企業のクレジットカード、および/またはキーカードは、施設セキュリティ課および/又は人事課（HR）に返却する。
d. 実験室ノートブックまたはエンジニアリングノートブックは、企業の IP 部門が取得して、インベントリを作成する必要がある。企業の IP 弁護士は、許可リストから従業員を削除する。
e. 個人のデバイスが仕事関連の職務に使用された場合は、企業の機密性ある情報をすべて削除しなければならない。

f. 退職する従業員による、ポータブルデバイスを介した、及び/又は、企業のネットワークアカウントから従業員の個人的な電子メール宛電子メールの送信による、企業情報のダウンロードを監視するよう IT に要求する。　.

退職手続の一環として、終了面接フォーム（従業員又は請負業者の出発前に記入する必要がある）を使用する必要がある。詳細は、従業員ハンドブック及び/又は人事課（HR）にて参照すること。

12. 営業秘密侵害への救済

営業秘密の侵害は、州法（またはカナダ州法）及び連邦法が適用になる。営業秘密の侵害に対する救済には、差止めによる救済、金銭的損害賠償、弁護士費用、訴訟費用、場合によっては、罰金や懲役などの刑事制裁が含まれる場合がある。

13. 2016 年営業秘密保護法による内部告発者免責

もし、開示が（i）直接あるいは間接に、連邦、州、又は地方政府公務員に、又は、弁護士に、内密になされている、（ii）法律違反の疑いを報告または調査することのみを目的としている場合、または、訴訟その他の手続きで提出された、訴状又はその他の文書で行われ、そのような提出が封印されている場合は、従業員または請負業者は、営業秘密の侵害と見なされる行為から免責される。(18 U.S.C. 1833(b))

この通知は、本第 2 条に記載されている、企業が締結した、機密保持または非開示契約、及び NDA に、含まれる。

関連トピック：

就業規則
整頓された机ポリシー
個人所有デバイス持参(BYOD)ポリシー
グローバルマーキングポリシー - 機密情報

2　従業員との秘密保持契約書の例

Confidentiality and Proprietary Rights Agreement (CA)

This Employee Confidentiality and Proprietary Rights Agreement ("**Agreement**") is entered into by and between [ ], a California [ ], (the "**Employer**") and [ ] (the "**Employee**") (the Employer and the Employee are collectively referred to herein as the "**Parties**") as of [ ], 2021 (the "**Effective Date**").

In consideration of the Employee's employment by the Employer, which the Employee acknowledges to be good and valuable consideration for her obligations hereunder, the Employer and the Employee hereby agree as follows:

1. Confidentiality and Security.

(a) Confidential Information. The Employee understands and acknowledges that during the course of employment by the Employer, she will have access to and learn about confidential, secret and proprietary documents, materials, data, and other information, in tangible and intangible form, of and relating to the Employer and its businesses and existing and prospective customers, suppliers, investors and other associated third parties ("**Confidential Information**"). The Employee further understands and acknowledges that this Confidential Information and the Employer's ability to reserve it for the exclusive knowledge and use of the Employer is of great competitive importance and commercial value to the Employer, and that improper use or disclosure of the Confidential Information by the Employee might cause the Employer to incur financial costs, loss of business advantage, liability under confidentiality agreements with third parties, civil damages and criminal penalties.

For purposes of this Agreement, Confidential Information includes, but is not limited to, all information not generally known to the public, in spoken, printed, electronic or any other form or medium, relating to: business processes, practices, research, operations, services, strategies, techniques, contracts, negotiations, know-how, trade secrets, work-in-process, databases, accounting records, legal information, marketing information, and customer lists of the Employer or its businesses or any existing or prospective customer, supplier, investor or other associated third party, or of any other person or entity that has entrusted information to the Employer in confidence.

The Employee understands that the above list is not exhaustive, and that Confidential Information also includes other information that is marked or otherwise identified as confidential or proprietary, or that would otherwise appear to a reasonable person to be confidential or proprietary in the context and circumstances in which the information is known or used.

The Employee understands and agrees that Confidential Information developed by her in the course of her employment by the Employer shall be subject to the terms and conditions of this Agreement as if the Employer furnished the same Confidential Information to the Employee in the first instance. Confidential Information shall not include information that is generally available to and known by the public at the

time of disclosure to the Employee, provided that such disclosure is through no direct or indirect fault of the Employee or person(s) acting on the Employee's behalf.

(b) Disclosure and Use Restrictions. The Employee agrees and covenants:

(i) Employee covenants:

(A) to treat all Confidential Information as strictly confidential;

(B) not to directly or indirectly disclose, publish, communicate, or make available Confidential Information, or allow it to be disclosed, published, communicated or made available, in whole or part, to any third party not having a need to know and authority to know and to use the Confidential Information in connection with the business of the Employer and, in any event, not to anyone outside of the direct employ of the Employer, except as required in the performance of any of the Employee's authorized employment duties to the Employer or with the prior consent of an authorized officer acting on behalf of the Employer in each instance (and then, such disclosure shall be made only within the limits and to the extent of such duties or consent); and

(C) not to access or use any Confidential Information, and not to copy any documents, records, files, media, or other resources containing any Confidential Information, or remove any such documents, records, files, media or other resources from the premises or control of the Employer, except as required in the performance of any of the Employee's authorized employment duties to the Employer or with the prior consent of an authorized officer acting on behalf of the Employer in each instance (and then, such access and use shall only be within the limits and to the extent of such duties or consent). The Employee understands and acknowledges that the Employee's obligations under this Agreement regarding any particular Confidential Information begin immediately and shall continue during and after the Employee's employment by the Employer until the Confidential Information has become public knowledge other than as a result of the Employee's breach of this Agreement or a breach by those acting in concert with the Employee or on the Employee's behalf.

(ii) Permitted disclosures. Nothing in this Agreement shall be construed to prevent disclosure of Confidential Information as may be required by applicable law or regulation, or pursuant to the valid order of a court of competent jurisdiction or an authorized government agency, provided that the disclosure does not exceed the extent of disclosure required by such law, regulation, or order. The Employee shall promptly provide written notice of any such order to an authorized officer of the Employer.

(iii) Nothing in this Agreement prohibits or restricts the Employee (or Employee's attorney) from initiating communications directly with, responding to an inquiry from, or providing testimony before the Securities and Exchange Commission (SEC), the Financial Industry Regulatory Authority (FINRA), any other self-regulatory organization, or any other federal or state regulatory authority regarding a possible securities law violation.

(iv) Nothing in this Agreement in any way prohibits or is intended to restrict or impede the Employee from discussing the terms and conditions of her employment with co-workers or union representatives, exercising her rights under Section 7 of the National Labor Relations Act, exercising protected rights to the extent that such rights cannot be waived by agreement, or otherwise disclosing information as permitted by law.

(v) Notice of Immunity Under the Economic Espionage Act of 1996, as amended by the Defend Trade Secrets Act of 2016. Notwithstanding any other provision of this Agreement:

(A) This Employee will not be held criminally or civilly liable under any federal or state trade secret law for any disclosure of a trade secret that is made: (1) in confidence to a federal, state, or local government official, either directly or indirectly, or to an attorney and solely for the purpose of reporting or investigating a suspected violation of law; or (2) in a complaint or other document that is filed under seal in a lawsuit or other proceeding.

(B) If the Employee files a lawsuit for retaliation by the Employer for reporting a suspected violation of law, the Employee may disclose the Employer’s trade secrets to the Employee’s attorney and use the trade secret information in the court proceeding if the Employee (1) files any document containing the trade secret under seal; and (2) does not disclose the trade secret, except pursuant to court order.

(vi) Duration of Confidentiality Obligations. The Employee understands and acknowledges that her obligations under this Agreement with regard to any particular Confidential Information shall commence immediately upon the Employee first having access to such Confidential Information (whether before or after she begins employment by the Employer) and shall continue during and after her employment by the Employer until such time as such Confidential Information has become public knowledge other than as a result of the Employee's breach of this Agreement or breach by those acting in concert with the Employee or on the Employee's behalf.

IN WITNESS WHEREOF, the Parties have executed this Agreement as of the Effective Date above.

(参考和訳)従業員との秘密保持契約書の例

機密保持義務契約

この従業員の機密保持義務（「本契約」）は、カリフォルニア州の[　　]である[　　]（「雇用主」）と[　　]（「従業員」）（雇用者と従業員を総称して「当事者」と言う。）との間で 2021 年 月 日（「発効日」）に締結される。

雇用主による従業員の雇用を考慮し、従業員は、本契約に基づく義務に対する、十分かつ価値のある対価と認め、雇用主と従業員は、以下のとおり合意する。

1. 機密性と安全性.

(a) 機密情報。従業員は、雇用主による雇用の過程で、雇用主、その事業、既存および将来の顧客、サプライヤー、投資家、その他の関連する第三者に関連する、有形及び無形の機密、秘密、及び所有される、文書、資料、データ、その他の情報（「機密情報」）にアクセスし、それを知ることがあることを、理解し、確認する。従業員はさらに、この機密情報、及び、雇用主が、独占的な知識と使用のために、それを留保することができる能力が、雇用主の競争上非常に重要で、商業的価値があること、並びに、従業員は、従業員による機密情報の不正使用又は開示が、金銭的費用、ビジネス上の優位性の喪失、第三者との機密保持契約に基づく責任、民事上の損害賠償、及び刑事罰を、雇用主に負わせる可能性があることを理解し、確認する。

本契約の目的上、機密情報には、雇用主とその事業、既存又は将来の顧客、サプライヤー、投資家、その他の関連する第三者、若しくは、情報を雇用主に秘密裏に委託したその他の個人又は団体についての、ビジネスプロセス、慣行、調査、運用、サービス、戦略、技術、契約、交渉、ノウハウ、営業秘密、開発品、データベース、会計記録、法的情報、マーケティング情報、顧客リストに関する、一般に知られていない、口頭、印字、電子、その他の形式又は媒体中の、全情報を含み、これに限られない。

従業員は、上記のリストが網羅的ではなく、機密情報には、機密又は所有された情報、としてマーク、あるいは他の方法で識別された情報、若しくは、情報が知られた、又は、使用された文脈や状況で、合理的な者にとり、機密情報又は所有情報と考えられる、その他の情報も含まれることを理解する。

従業員は、雇用主による雇用の過程で、自身が作成した機密情報は、雇用主が、同じ機密情報を従業員に提供したかのように扱われ、本契約の条件に従うべきことを理解し、同意する。機密情報には、従業員又は従業員に代わって行動する人物の、直接的又は間接的な過失によるものでない限り、従業員への開示時に、一般に利用可能か、一般に知られている情報は含まれない。

(b)　開示と使用の制約。従業員は、以下に同意し、合意する:

(i)　従業員は、下記のように、誓約する:

(A)　全機密情報を厳に機密として扱う;

(B)　機密情報を、直接的又は間接的に開示、公開、伝達、又は、利用可能にしない、知る必要がなく、知る権限を持たない第三者に、その全部又は一部を開示、公開、伝達、又は、利用可能にしない、雇用主の事業に関連して、機密情報を使用する、いかなる場合でも、雇用主に対する、従業員の許可された職務の履行に必要な場合、又は、雇用主を代理する権限のある役員の事前の同意を得た場合以外、雇用主から直接に雇用された者以外には開示しない（以後、開示は、そのような義務又は同意の範囲内でのみ行われる）;

(C)　雇用主に対する、従業員の許可された職務の履行に必要な場合、又は、雇用主を代理する権限のある役員の事前の同意を得た場合以外、機密情報にアクセス又は使用したり、機密情報を含む文書、記録、ファイル、メディア、その他の資料をコピーしたり、そのような文書、記録、ファイル、メディア、その他の資料を雇用主の施設又は管理から持ち出したりしない。（以後、アクセスと使用は、そのような義務又は同意の範囲内でのみ行われる）。従業員は、特定の機密情報に関する本契約に基づく従業員の義務は、直ちに施行され、雇用主による従業員の雇用中および雇用後も、従業員による、あるいは、従業員と協力して、又は従業員に代わって行動する者による、機密保持義務の違反の結果として以外に、機密情報が公に知られるようになるまで、継続することを理解し、確認する。

(ii)　許可される開示。本契約のいかなる条項も、適用される法律又は規制によって、若しくは、管轄裁判所又は政府機関の有効な命令に従って要求される場合、開示が、それら法律、規制、又は命令によって要求される開示の範囲を超えない限り、機密情報の開示を妨げるとは解釈されない。従業員は、雇用主を代表する権限のある役員に、そのような命令についての書面による通知を、迅速に提供する。

(iii)　本契約のいかなる条項も、従業員（又は従業員の弁護士）が、証券取引法違反の可能性に関して、証券取引委員会（SEC）、金融業界規制当局（FINRA）、その他の自主規制機関、その他の連邦又は州の規制当局と、直接に会話を開始したり、問い合わせに応答したり、証言を提供したりすることを禁止又は制限するものではない。

(iv)　本契約のいかなる条項も、従業員が、同僚又は組合の代表者と、雇用条件について話し合い、全国労働関係法第 7 条に基づく権利を行使し、保護された権利を、そのような権利が合意によって放棄できない範囲で行使し、又は、法律が許可するように情報を開示することを、禁止するものでなく、制限又は妨害することをを意図しない。

(v)　2016 年連邦営業秘密保護法によって改正された、1996 年経済スパイ活動法に基づく、免責の通知。

本契約の他の規定にもかかわらず

(A)　従業員は、次のような営業秘密の開示について、連邦又は州の営業秘密法に基づいて、刑事上又は民事上の責任を負わない: (1) 直接又は間接に、連邦、州又は地方政府の公務員に対し、若しくは、弁護士を介して、内密に、法律違反の疑いを報告、又は、調査することのみを目的とする場合、又は、(2) 訴訟又はその他の手続きで、封印されて提出された訴状又はその他の文書中の場合.

(B)　従業員が法律違反の疑いを報告したとして、雇用主による報復訴訟が提起された場合、従業員が (1) 営業秘密を含む文書を封印下に提出し; (2) 裁判所の命令に基づく場合を除き、営業秘密を開示しない場合には、従業員は、雇用主の営業秘密を従業員の弁護士に開示し、裁判所の手続きで企業の秘密情報を使用することができる。

(vi)　機密保持義務の期間。従業員は、特定の機密情報に関する本契約に基づく義務は、従業員がそのような機密情報に最初にアクセスした時点に直ちに開始し（雇用主による雇用を開始する前か後かにかかわらず）、雇用主による雇用の間、及び、その後も、従業員による、若しくは、従業員と協力している、又は、従業員に代わって行動する者による、本契約の違反以外の結果、そのような機密情報が公に知られるようになるまで、継続することを理解し、確認する。

本契約の証として、当事者は、発効日に、本契約を署名捺印した。

3　退職後の競業避止契約書の例

NON-COMPETITION AGREEMENT

SECTION 1. Definition.

(a) Competitive Business means any corporation, partnership, association, or other person or entity, including but not limited to Executive, (i) which competes directly, or is planning to compete directly, with the Company with respect to the design, development, manufacture, remanufacture, assembly, marketing, sales, or service of [ ], or any other business of the Company, that was related to Executive's work, practice, customer relationship, planning, operation, marketing, purchasing, or sales responsibility, or that Executive received any Confidential Information or Trade Secrets about, at any time within eighteen (18) months prior to termination of Executive's employment with the Company or any of its subsidiaries, and (ii) which engages or plans to engage in such competition in the demographic regions that the Company sold or distributed, or actively attempts to sell or distribute, such products or services within eighteen (18) months prior to termination of Executive's employment with the Company or any of its subsidiaries.

(b) Confidential Information shall mean information, not generally known in the trade or industry, which Executive learns or creates during the course of Executive's employment with the Company or any of its subsidiaries, which may include but is not limited to product specifications, manufacturing procedures, methods, equipment, compositions, data compilations, technologies, formulas, know-hows, research and development programs, sales methods, customer lists, customer information, computer programs and other confidential technical or business information and data. Confidential Information shall not include any information that (A) is or becomes generally available to the public other than as a result of a disclosure by Executive in violation of this Non-Competition Agreement or (B) becomes available to Executive on a non-confidential basis from a source other than the Company or its affiliates which is not prohibited from disclosing such information to Executive by a legal, contractual or fiduciary obligation to the Company or any other person.

(c) Trade Secret(s) means information, including a formula, pattern, compilation, program, device, method, technique or process, that derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons in the same business circle or industry, and that is the subject of efforts to maintain its secrecy that are reasonable under the circumstances.

SECTION 2. Non-Competition; Non-Solicitation.

(a) Noncompetition. During the term of Executive's employment with the Company or any of its subsidiaries and for eighteen (18) months following the termination of such employment for any reason, Executive shall not, directly or indirectly, participate in, consult with, be employed by, or assist with the organization, planning, ownership, financing, management, operation or control of any Competitive Business in any capacity in which, in the absence of this Agreement, Confidential Information, Trade Secrets or goodwill of the Company would reasonably be considered useful.

(b) Nonsolicitation. During the term of Executive's employment with the Company or any of its subsidiaries and for eighteen (18) months following the termination of such employment for any reason, Executive shall not, directly or indirectly, on behalf of any Competitive Business, either by himself or by providing substantial assistance to others, solicit to terminate employment with the Company or any of its subsidiaries, or to accept or begin employment with or service to any Competitive Business, any employee of the Company whom Executive supervised or about whom Executive gained Confidential Information at any time during the last eighteen (18) months of Executive's employment with the Company or any of its subsidiaries.

SECTION 3. No Right to Continued Employment.

Nothing in this Non-Competition Agreement shall confer upon Executive any right to continue in the employ of the Company or shall interfere with or restrict in any way the rights of the Company, which are hereby reserved, to discharge Executive at any time for any reason whatsoever, with or without cause.

SECTION 4. No Conflicting Agreements.

Executive warrants that Executive is not bound by the terms of a confidentiality agreement, non-competition or other agreement with a third party that would conflict with Executive's obligations hereunder.

SECTION 5. Remedies.

(a) In the event of breach or threatened breach by Executive of any provision hereof, the Company shall be entitled to seek temporary or preliminary injunctive relief or other equitable relief to which either of them may be entitled, without the posting of any bond or other security.

(b) The period of time during which the restrictions set forth in Section 2(a) hereof will be in effect will be extended by the length of time during which Executive is in breach of the terms of those provisions as finally determined by an arbitrator or any court of competent jurisdiction.

SECTION 6. Successors and Assigns.

This Non-Competition Agreement shall be binding upon Executive and Executive's heirs, assigns and representatives and inure to the benefit of the Company and its successors and assigns, including without limitation any entity to which substantially all of the assets or the business of either of the Company are sold or transferred. The obligations of Executive are personal to Executive and shall not be assigned by Executive.

SECTION 7. Severability.

It is expressly agreed that if any restrictions set forth in this Non-Competition Agreement are found by any court having jurisdiction to be unreasonable because they are too broad in any respect, then and in each such case, the remaining provisions herein contained shall, to the greatest extent permitted under applicable law, nevertheless, remain effective, and this Non-Competition Agreement, or any portion hereof, shall, to the extent permitted by applicable law, be considered to be amended, so as to be

considered reasonable and enforceable by such court, and the court shall specifically have the right to restrict the time period or the business or geographical scope of such restrictions to any portion of the time period, business or geographic areas to the extent the court deems such restriction to be necessary to cause the covenants to be enforceable and, in such event, the covenants shall be enforced to the extent so permitted and the remaining provisions shall be unaffected thereby. In such event, the parties hereto agree to execute all documents necessary to evidence such amendment so as to eliminate or modify any such unreasonable provision in order to carry out the intent of this Non-Competition Agreement insofar as possible and to render this Non-Competition Agreement enforceable in all respects as so modified. The covenants contained in this Section 7 shall be construed to extend to separate jurisdictions or sub-jurisdictions of the United States in which the Company, during the term of Executive's employment, have been or are engaged in business, and to the extent that any such covenant shall be illegal and/or unenforceable with respect to any jurisdiction, said covenant shall not be affected thereby with respect to each other jurisdiction, such covenants with respect to each jurisdiction being construed as severable and independent. The restrictive covenant provisions of this Non-Competition Agreement shall govern to the extent there is any conflict between their terms and the terms of any other agreement or understanding with the Company.

(参考和訳)退職後の競業避止契約書の例

競業避止合意

第 1 条. 定義.

(a) 競合ビジネスとは、貴殿を含むが限定されない、以下の条件を充たす、企業、組合、協会、その他の個人又は団体を意味する。(i)[ ]の製造、再製造、組立て、マーケティング、販売、又はサービスに関して、若しくは、(1)貴殿の仕事、慣行、顧客関係、計画、運用、マーケティング、購入、又は販売の責任に関連した、又は、(2)貴殿が、当社またはその子会社との雇用が終了する前の 18 か月以内のいずれかの時点で、関連した機密情報または営業秘密を受け取った、当社の他の事業に関して、直接に当社と競合する、又は、競合する予定である、(ii) 貴殿の当社又はその子会社との雇用が終了する前の 18 か月以内に、当社が、そのような製品またはサービスを販売または配布した、若しくは、積極的に販売または配布を試みた地域において、当社と競争する、あるいは、競争を予定する。

(b) 機密情報とは、当社またはその子会社と貴殿間の雇用の過程で、貴殿が知る、又は、作成する、取引界、業界で一般的に知られていない情報を意味する。これには、製品の仕様、製造手順、方法、機器、構成、データ編集、技術、方式、ノウハウ、研究開発プログラム、販売方法、顧客リスト、顧客情報、コンピュータープログラム、その他の機密の技術情報又はビジネス情報及びデータが含まれるが、これらに限定されない。機密情報には、(A) この競業避止合意に違反する貴殿による開示による結果を除いて、一般に利用可能である、又は、一般に利用可能となる情報、若しくは、(B) 当社その他の者に対する法的、契約上、又は受託者責任により、貴殿への情報開示が禁止されない、当社またはその関連会社以外の情報源から、内密でない状況で、貴殿に利用可能となった情報は、含まれない。

(c) 営業秘密とは、方式、パターン、編集、プログラム、デバイス、方法、技術、またはプロセスを含む情報を意味し、一般に知られていないこと、及び、同じ業界または産業の他者により、適正な方法で容易に確認できないことから、現実の、又は、潜在的な独立した経済的価値を導き出し、その状況下で、秘密性を維持するための合理的な努力の対象となっている。

第 2 条. 競業避止; 勧誘避止.

(a) 競業避止 当社又はその子会社と貴殿との雇用期間中、及び、いずれかの事由による雇用終了後 18 か月間、貴殿は、競合ビジネスの組織、計画、所有、資金調達、管理、運営または支配へ、本契約のない場合に、当社の機密情報、営業秘密、又は、当社ののれんが、それに合理的に有用と見なされうる地位において、直接的または間接的に、参加、諮問、就業又は支援をしない。

(b) 勧誘避止 当社又はその子会社と貴殿との雇用期間中、及び、いずれかの事由による雇用終了後 18 か月間、貴殿は、直接的または間接的に、競合ビジネスに代

わって、自身で、あるいは、他者に相当な支援を提供することで、貴殿が当社又はその子会社との雇用から最終 18 か月間の任意の時点で、貴殿が監督した、又は、貴殿がその者に関する機密情報を入手した、当社の従業員に対し、当社又はその子会社との雇用の終了、若しくは、競合ビジネスとの間の雇用関係又はサービスの、受諾又は開始を唆してはならない。

第 3 条. 継続雇用の権利の不存在

この競業避止合意のいかなる条項も、当社との雇用を継続する権利を貴殿に付与するものではなく、また、理由の有無、如何を問わず、いつでも貴殿を解雇する当社の権利を、それは留保されているが、妨害または制限するものではない。

第 4 条. 矛盾する合意の不存在.

貴殿は、本契約に基づく貴殿の義務と矛盾する、機密保持契約、競業避止義務、又は、第三者とのその他の契約に、拘束されないことを保証する。

第 5 条. **救済**.

(a) 本契約のいずれかの条項の貴殿による違反または違反の恐れがある場合、当社は、保証金その他の担保なく、いずれか享受することのできる、一時的又は暫定的差止命令その他の衡平法上の救済を受けることができる。

(b) 本契約の第 2 条 (a) に規定された制限が有効である期間は、仲裁人または管轄権を有する裁判所によって、最終的に決定された、これらの規定条項違反の期間によって延長される。

第 6 条. **承継と譲渡**.

この競業避止契約は、貴殿及び貴殿の相続人、譲受人、代理人を拘束し、当社、その後継者、及び譲受人（当社の実質的に全資産又は事業が売却又は譲渡された会社が含まれるが、これに限定されない。）の利益のために、効力を生じる。貴殿の義務は、貴殿に個人的なものであり、貴殿によって移転されることはできない。

第 7 条. **分離可能性**.

管轄権を有する裁判所によって、この競業避止契約に定められた制限が、いずれかの事由で、広範すぎるために不合理であると判断された場合、本合意に含まれる残りの条項は、それにかかわらず、適用される法令の下で認められる最大の限度で、引き続き有効であり、この競業避止合意またはその一部は、適用される法令によって認められる範囲で、裁判所が、合理的かつ執行可能であると考えられるように、修正されたと見なされ、かつ、裁判所が、当該制限の期間、事業、又は地理的な範囲を、当該制限が法的拘束力を有するために必要な程度で、期間、事業、又は地理的の範囲を限定する権利を、特に有するものとする。そのような場合、

本合意は、許可された範囲で法的に執行され、残りの条項は、そこで影響を受けないものとする。そのような場合、当事者は、この競業避止合意の目的を可能な限り実行し、本合意を全ての点で修正後に執行可能となるように、不合理な条項を削除又は変更する旨の、修正を証明するために必要な、全ての文書を署名することに同意する。この第 7 条に含まれる規定は、貴殿の雇用期間中に、当社が事業を行った、又は、行っている米国内の各別の管轄区域又は準管轄区域にまで及ぶものと解釈される。本合意の制約が、いずれかの管轄域で、違法及び/又は執行不能であるものとされた程度で、当該制約は、他の管轄域では影響を受けないものとし、各管轄域に関して、当該制約は、分離可能かつ独立であると解釈される。本競業避止契約の制約条項は、その条件と当社の他の契約または合意の条件との間で矛盾がある場合、優先して適用される。

4　取引先との秘密保持契約書の例

NON-DISCLOSURE AGREEMENT

This Non-Disclosure Agreement ("Agreement") dated _____, 20___ (the "Effective Date"), between _____, a _____corporation ("Party A") with offices at _____ and _____, a _____corporation located at _____ ("Party B").

1. Background. Party A and Party B (the "parties") intend to engage in discussions and negotiations concerning a possible transaction or business relationship between them. In the course of such discussions and negotiations and in the course of any such transaction or business relationship, it is anticipated that each party will disclose or deliver to the other party and to the other party's directors, officers, employees, agents or advisors (including, without limitation, attorneys, accountants, consultants, bankers, financial advisors and members of advisory boards) (collectively, "Representatives") certain of its trade secrets or confidential or proprietary information for the purposes of enabling the other party to evaluate the feasibility of such transaction or business relationship and to perform its obligations and exercise its rights under any such transaction or business relationship that is agreed to between the parties (the "Purposes"). The parties have entered into this Agreement in order to assure the confidentiality of such trade secrets and confidential or proprietary information in accordance with the terms of this Agreement. As used in this Agreement, the party disclosing Proprietary Information (as defined below) is referred to as the "Disclosing Party"; the party receiving such Proprietary Information is referred to as the "Recipient".

2. Proprietary Information. As used in this Agreement, the term "Proprietary Information" shall mean all trade secrets or confidential or proprietary information designated as such in writing by the Disclosing Party, whether by letter or by the use of an appropriate proprietary stamp or legend, prior to or at the time any such trade secret or confidential or proprietary information is disclosed by the Disclosing Party to the Recipient. Notwithstanding the foregoing, information which is orally or visually disclosed to the Recipient by the Disclosing Party, or is disclosed in writing without an appropriate letter, proprietary stamp or legend, shall constitute Proprietary Information if it would be apparent to a reasonable person, familiar with the Disclosing Party's business and the industry in which it operates, that such information is of a confidential or proprietary nature the maintenance of which is important to the Disclosing Party. In addition, the term "Proprietary Information" shall be deemed to include: (a) any notes, analyses, compilations, studies, interpretations, memoranda or other documents prepared by the Recipient or its Representatives which contain, reflect or are based upon, in whole or in part, any Proprietary Information furnished to the Recipient or its Representatives pursuant hereto; and (b) the existence or status of, and any information concerning, the discussions between the parties concerning the possible transaction or business relationship.

3. Use and Disclosure of Proprietary Information. The Recipient and its Representatives shall use the Proprietary Information of the Disclosing Party only for the Purposes and such Proprietary Information shall not be used for any other purpose without the prior written consent of the Disclosing Party. The Recipient and its Representatives shall hold in confidence, and shall not disclose any Proprietary Information of the Disclosing Party; provided. however, that (i) the Recipient may make any disclosure of such information to which the Disclosing Party gives its prior written consent; and (ii) any

of the Proprietary Information may be disclosed by the Recipient to its Representatives who need to know such information in connection with the Purposes and who are informed of the confidential nature of such information and of the terms of this Agreement. In any event, the Recipient shall be responsible for any breach of this Agreement by any of its Representatives, and agrees, at its sole expense, to take reasonable measures to restrain its Representatives from prohibited or unauthorized disclosure or use of the Proprietary Information, Notwithstanding anything contained in this Agreement to the contrary, this Agreement shall not prohibit the Recipient from disclosing Proprietary Information of the Disclosing Party to the extent required in order for the Recipient to comply with applicable laws and regulations, provided that the Recipient provides prior written notice of such required disclosure to the Disclosing Party and takes reasonable and lawful actions to avoid and/or minimize the extent of such disclosure.

4. Limitation on Obligations. The obligations of the Recipient specified in Section 3 above shall not apply, and the Recipient shall have no further obligations, with respect to any Proprietary Information to the extent that such Proprietary Information:

(a) is generally known to the public at the time of disclosure or becomes generally known without Recipient or its Representatives violating this Agreement;

(b) is in the Recipient's possession at the time of disclosure;

(c) becomes known to the Recipient through disclosure by sources other than the Disclosing Party without such sources violating any confidentiality obligations to the Disclosing Party; or

(d) is independently developed by the Recipient without reference to or reliance upon the Disclosing Party's Proprietary Information.

5. Ownership of Proprietary Information. The Recipient agrees that it shall not receive any right, title or interest in, or any license or right to use, the Disclosing Party's Proprietary Information or any patent, copyright, trade secret, trademark or other intellectual property rights therein, by implication or otherwise. Each of the parties hereto represents, warrants and covenants that the trade secrets which it discloses to the other party pursuant to this Agreement have not been stolen, appropriated, obtained or converted without authorization.

6. Return of Proprietary Information. The Recipient shall, upon the written request of the Disclosing Party, return to the Disclosing Party all Proprietary Information received by the Recipient or its Representatives from the Disclosing Party (and all copies and reproductions thereof). In addition, the Recipient shall destroy: (i) any notes, reports or other documents prepared by the Recipient which contain Proprietary Information of the Disclosing Party; and (ii) any Proprietary Information of the Disclosing Party (and all copies and reproductions thereof) which is in electronic form or cannot otherwise be returned to the Disclosing Party. Alternatively, upon written request of the Disclosing Party, the Recipient shall destroy all Proprietary Information received by the Recipient or its Representatives from the Disclosing Party (and all copies and reproduction thereof) and any notes, reports or other documents prepared by the Recipient which contain Proprietary Information of the Disclosing Party. Notwithstanding the return or destruction of the Proprietary Information, the Recipient and its

Representatives will continue to be bound by their obligations of confidentiality and other obligations hereunder.

7. Securities. Recipient represents that it is aware, and will advise its representatives who are informed of the matters that are the subject of this Agreement, of the restrictions imposed by the applicable federal and state securities laws on the purchase or sale of securities by any person who has received material, non-public information regarding a company with publicly traded securities, as well as the restrictions making it unlawful to communicate such information to any other person when it is reasonably foreseeable that such other person is likely to purchase or sell securities in reliance upon such information.

8. Non-Solicitation of Employees Covenant. Each party agrees that during the term of this Agreement and for the period of two (2) years after the termination of this Agreement, it will not, either directly or through others solicit or attempt to solicit any employee of the other party with whom such party came into contact with during the evaluation of a possible transaction between the parties to become an employee, consultant or independent contractor to or for itself or any of its affiliates; provided,- however, that nothing contained herein shall be deemed to prohibit any party, either directly or through others, from (i) conducting any general solicitation not specifically targeted at any such employee, and, for the avoidance of doubt, the hiring or engagement by a party of any employee of the other party who responds to such general advertising or who approaches such party or any of its affiliates without any solicitation or inducement to leave the employ of the other party or any of its affiliates shall not be deemed a breach of this Section 8, or (ii) soliciting for employment or hiring any employee of the other party or any of its affiliates who was terminated by the other party or any of its affiliates; each subject to such employee's restrictive covenants

9. Miscellaneous.

(a) This Agreement supersedes all prior agreements, written or oral, between the parties relating to the subject matter of this Agreement. This Agreement may not be modified, changed or discharged, in whole or in part, except by an agreement in writing signed by the parties.

(b) This Agreement will be binding upon and inure to the benefit of the parties hereto and their respective heirs, successors and assigns.

(c) This Agreement shall be construed and interpreted in accordance with the internal laws of the Commonwealth of Massachusetts, without giving effect to the principles of conflicts of law thereof.

(d) The provisions of this Agreement are necessary for the protection of the business and goodwill of the parties and are considered by the parties to be reasonable for such purpose. The Recipient agrees that any breach of this Agreement will cause the Disclosing Party substantial and irreparable injury and, therefore, in the event of any such breach, in addition to other remedies which may be available, the Disclosing Party shall have the right to specific performance and other injunctive and equitable relief.

(e) The confidentiality obligations imposed by this Agreement shall continue with respect to a particular item of Proprietary Information until the fifth anniversary of the disclosure of such Proprietary Information to Recipient pursuant to this Agreement; provided, however, that the confidentiality

obligations imposed by this Agreement with respect to source code included in the Proprietary Information shall continue in perpetuity.

(f) For the convenience of the parties, this Agreement may be executed by facsimile and in counterparts, each of which shall be deemed to be an original, and both of which taken together, shall constitute one agreement binding on both parties.

EXECUTED as a sealed instrument as of the day and year first set forth above.

(参考和訳)取引先との秘密保持契約書の例

機密保持契約

_____で設立され、事業所を _____に置く、 _____（“X”）と、 _____で設立され、事業所を _____に置く、 _____（“Y”)は、20___ 年_____日, （「契約日」),以下のとおり本機密保持契約（“本契約”）を締結した 。

1. 背景　当事者 X 及び当事者 Y（「当事者」）は、両者間の可能な取引又はビジネス関係に関する、議論及び交渉に従事することを意図する。そのような話し合いや交渉の過程、並びに、そのような取引や取引関係の過程で、各当事者は、相手方が、そのような取引又はビジネス関係の実現可能性を評価できるようにするため、及び、当事者間で合意されたそのような取引又はビジネス関係（「目的」）の下で、その義務を履行し、その権利を行使するため、相手方及び相手方の取締役、役員、従業員、代理人、又は顧問（ 、弁護士、会計士、コンサルタント、銀行家、財務顧問及び諮問委員会のメンバー）（総称して「代理人」）に、特定の営業秘密、機密情報、又は保有情報を、開示あるいは提供することを予定している。両当事者は、本契約の条項に従って、このような営業秘密、機密情報、又は保有情報の機密性を保証するために、本契約を締結した。本契約で、保有情報（以下に定義）を開示する当事者は、「開示当事者」と呼ばれる。そのような保有情報を受け取る当事者は、「受領者」と呼ばれる。

2. 情報保有情報　本契約で使用される、「保有情報」という用語は、そのような営業秘密、機密情報、又は保有情報が開示当事者から受領者に開示される時点、若しくは、それ以前に、開示当事者によって、書簡、適切な専有スタンプ、又は、説明文のいずれによるかを問わず、書面で指定された、すべての営業秘密、機密情報、又は保有情報を意味する。上記にかかわらず、開示当事者によって受領者に口頭又は視覚的に開示された情報、若しくは、適切な書簡、専有スタンプ、又は、説明文なく、書面で開示された情報は、開示当事者の事業及びその属する業界に通じた合理的な者に、当該情報が、機密、あるいは、保有される性質のもので、その維持が、開示当事者にとって重要であると明らかである場合、保有情報を構成する。さらに、「保有情報」という用語には、次のものが含まれると想定されている：(a)本契約に従って受領者又はその代理人に提供される保有情報の、全体又は部分を含む、反映する、若しくは、基礎とする、受領者又はその代理人が用意した、ノート、解析、編集、調査、解釈、メモ、又は、他の書面、（b）取引又はビジネス関係の可能性に関する、当事者間の話し合いの存在又は状況、及び、それらに関する情報。

3. 保有情報の使用及び開示　受領者及びその代理人は、開示当事者の保有情報を本目的にのみ使用するものとし、かかる保有情報は、開示当事者の事前の書面による同意なしに、他の目的に使用できない。受領者とその代理人は、秘密性を保持し、開示当事者の保有情報を開示しない。ただし、（i）受領者は、開示当事者が事前に書面で同意した情報を開示することができ、（ii）保有情報のいずれかは、本目的に関連して、そのような情報を知る必要があり、当該情報の機密性、及び本契約の条項について知らされている代理人に、受領者によって開示される。いずれにせよ、受領者は、その代理人による本契約の違反に対して責任を負い、その代理人による、禁止される、又は、許可の無い、保有情報の開示、若しくは使用を制限するため、合理的な措置を自己の費用で講

じることに同意する。本契約中のこれに反する規定にもかかわらず、本契約は、受領者が、適用法及び規制を遵守するために必要な範囲で、事前に開示当事者に、必要な開示を書面で通知し、かつ、そのような開示を回避、及び/又は、範囲を最小化するために、適法な合理的行動を取ることを条件として、開示当事者の保有情報を開示することを禁じない。

4. 制限及び義務　下記に該当する保有情報に関しては、その限りで、前掲第 3 条で指定された受領者の義務が適用されず、受領者は、それ以上の義務を負わないものとする。

(a) 開示の時点で一般に知られている、若しくは、受領者又はその代理人が、本契約に違反することなく、一般に知られるようになる。

(b) 開示の時点で、受領者が所有している。

(c) 開示当事者以外の情報源からの開示で、受領者に知られるようになり、当該情報源が、開示当事者に対する秘密保持義務に違反していない。

(d) 開示当事者の所有情報を参照したり、依存したりすることなく、受領者が独自に開発した。

5. 保有情報の保有　受領者は、黙示的又はその他の方法により、開示当事者の保有情報、若しくは、その中の特許、著作権、営業秘密、商標、その他の知的財産権に対する権利、権原、利益、又は、ライセンスや使用権を、取得しないことに同意する 。本契約の各当事者は、本契約に従って相手方当事者に開示する営業秘密が、許可なく盗取、侵害、取得、又は転換されていないことを、表明、保証、かつ、誓約する。

6. 保有情報の返却　受領者は、開示当事者の書面による要求に応じて、受領者又はその代理人が開示当事者から受け取った、すべての保有情報（及び、そのすべてのコピーと複製）を開示当事者に返却する。さらに、受領者は以下を破棄する:（i）開示当事者の保有情報を含む、受領者が作成したメモ、レポート、又はその他の文書;（ii）電子形式であるか、その他、開示当事者に返却することができない、開示当事者の保有情報（及び、そのすべてのコピーと複製）。あるいは、開示当事者の書面による要求に応じて、受領者は、受領者又はその代理人が開示当事者から受け取ったすべての保有情報（及び、そのすべてのコピーと複製）、並びに、開示当事者の保有情報を含む受領者が作成したメモ、レポート、又はその他の文書を、破棄する。保有情報の返却又は破棄にかかわらず、受領者及びその代理人は、引き続き、秘密保持義務、及び、本契約に基づくその他の義務に拘束される。

7. 証券　受領者は、適用される連邦及び州の証券法により、上場証券を保有する会社に関する重要な非公開情報を受領した者に、証券の購入又は売却について課された制限、並びに、当該情報を受領すると、それに依り、証券の購入又は売却することが、合理的に予測できる他人に、そのような情報を伝達することを違法にする制限を、自己が認識していること、そして、本契約の対象となる事項を知らされる代理人に忠告することを、表明する。

8. 従業員の非勧誘　各当事者は、本契約の期間中、及び、本契約の終了後 2 年間、直接又は他者を介して、当事者間で潜在的取引の評価中に接触した、相手方の従業員を、自身又はその関連会社の、従業員、コンサルタント、又は独立請負業者になるように、勧誘したり、勧誘しようとしたりしない。ただし、ここに含まれる規定は、各従業員の制限合意に準拠するものの、直接又は他者を介して、（i）そのような従業員を特に対象としない、一般的な勧誘を行うことを、禁止するものではない。疑義を避ける目的で記載すると、そのような一般的な広告に応答する、若しくは、他の当事者又はその関連会社の雇用を辞めるため、勧誘又は誘因なしに、そのような当事者又はその関連会社に近づく、他の当事者の従業員を、雇用又は採用することは、本条違反とはみなされない。（ii）相手方又はその関連会社によって解雇された、相手方又はその関連会社の従業員を、雇用又は雇用に勧誘することを、禁止するものではない。

9. その他.

(a) 本契約は、本契約の主題に関連する、書面又は口頭による、当事者間の以前の全合意を置き換える。本契約は、当事者が署名した書面での合意による場合を除き、全体又は一部を、変更、改正、又は解除することはできない。

(b) 本契約は、本契約の当事者、及び、それぞれの相続人、後継者、譲受人の利益を拘束し、効力を生じる。

(c) 本契約は、準拠法の原則に影響を与えることなく、マサチューセッツ州内法に従って、解釈及び理解される。

(d) 本契約の規定は、当事者の事業及びのれんの保護に必要であり、当事者は、そのような目的のために、合理的であると見なす。受領者は、本契約の違反が、開示当事者に重大かつ取り返しのつかない損害をもたらすことに同意し、したがって、違反が発生した場合、利用可能な他の救済策に加えて、開示当事者は、特定の義務履行、その他、差止命令及び衡平法上の救済を求める権利を有する。

(e) 本契約によって課される秘密保持義務は、本契約に従って受領者に保有情報を開示してから５年間、保有情報の特定の項目に関して、継続する。ただし、保有情報に含まれるソースコードに関して、本契約により課せられる守秘義務は、永続的に継続するものとする。

(f) 当事者の便宜のために、本契約は、ファクシミリで締結することができ、契約書(2 部)は、それぞれが原本と見なされ、一体として、両方の当事者を拘束する 1 つの契約を構成するものとする。

上記の年月日に、封印された書面として署名完了。

5　来訪者受付表

Visitor List

From [　　/　　/　　] to [　　/　　/　　]
Located at [　　]
Attended by [　　]
Reviewed by [　　]

No.	Name	ID checked	Contact details	Affiliation	Arrival	Departure	Accepted by

(参考和訳)来訪者受付表

訪問者リスト

[　　/　　/　　] から [　　/　　/　　]まで

所在地 [　　]

確認者 [　　]

監督者 [　　]

No.	氏名	本人確認	連絡先	所属組織	到着時刻	出発時刻	受入対応者 （受入先）

第 2 章　ドイツにおける参考書式

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). 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/Communications Policy

1. About Policy

1.1 Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

2. Equipment Security

2.1 You are responsible for the security of the equipment allocated to or used by you, and you must not allow it to be used by anyone other than in accordance with this policy. You should use passwords on all IT equipment, particularly items that you take out of the office. You should keep your passwords confidential and change them regularly.

2.2 You may use the equipment allocated to you only to serve our business goals. You may not use the equipment for anything that does not support or augment our business.

2.3 You must only log on to our systems using your own username and password. You must not use another person's username and password or allow anyone else to log on using your username and password.

2.4 If you are away from your desk you should log out or lock your computer. You must log out and shut down your computer at the end of each working day.

3. Systems/Programs/Infrastructures

3.1 You should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of your duties).

3.2 You must not download or install software from external sources without authorisation from [POSITION]. Downloading unauthorised software may interfere with our systems and may introduce viruses or other malware.

3.3 You must not attach any device or equipment including mobile phones, tablet computers or USB storage devices to our systems without authorisation from [POSITION].

3.4 We monitor all e-mails passing through our system for viruses. You should exercise particular caution when opening unsolicited e-mails from unknown sources. If an e-mail looks suspicious do not reply to it, open any attachments or click any links in it.

3.5 Inform [POSITION] immediately if you suspect your computer may have a virus.

4. E-mail Communication

4.1 Adopt a professional tone and observe appropriate etiquette when communicating with third parties by e-mail. [You should also include our standard e-mail signature and disclaimer.]

4.2 Remember that e-mails can be used in legal proceedings and that even deleted e-mails may remain on the system and be capable of being retrieved.

4.3 You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate e-mails.

4.4 You should not:

(a) send or forward private e-mails at work which 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 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.

4.5 Do not use your own personal e-mail account to send or receive e-mail for the purposes of our business. Only use the e-mail account we have provided for you.

4.6 [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.]

5. Internet

5.1 Internet access is provided solely for business purposes. [Occasional personal use may be permitted as set out in paragraph 6.]

5.2 You should not access any web page or download any image or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content that is legal in Germany may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

5.3 We may block or restrict access to some websites at our discretion.

6. Monitoring

6.1 Our systems enable us to monitor telephone, e-mail, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations in our role as an employer, your use of our systems including the telephone and computer systems (including any personal use) may be continually monitored by automated software or otherwise.

6.2 We reserve the right to retrieve the contents of e-mail messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):

(a) to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy;

(b) to find lost messages or to retrieve messages lost due to computer failure;

(c) to assist in the investigation of alleged wrongdoing; or

(d) to comply with any legal obligation.

7. Prohibited Acts

7.1 Misuse of our telephone or e-mail system or inappropriate internet use will be dealt with Disciplinary Procedure. Misuse of the internet can in some cases be a criminal offence.

7.2 Creating, viewing, accessing, transmitting or downloading any of the following material will usually amount to gross misconduct (this list is not exhaustive):

(a) pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

(b) offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients;

(c) a false and defamatory statement about any person or organisation;

(d) material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities Policy or our Anti-harassment and Bullying Policy);

(e) confidential information about us or any of our staff or clients (except as authorised in the proper performance of your duties);

(f) unauthorised software;

(g) any other statement which is likely to create any criminal or civil liability (for you or us); or

(h) music or video files or other material in breach of copyright.

(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、主要な方針や手続きを示す。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、すべ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、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すべ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 及び通信システム方針

1.　本方針

1.1　この方針の違反は、懲戒手続で対応される可能性があり、深刻な場合には、即時解雇につながる重大な逸脱行為として扱われる可能性がある。

2.　機器の安全性

2.1　あなたは、あなたに割り当てられた、または、あなたが使用する機器の安全性に責任を負い、この方針に服する者以外の者による使用を許可してはならない。すべての IT 機器、特に、オフィスから持ち出す品目には、パスワードを使用しなければならない。パスワードは、内密にし、定期的に変更する必要がある。

2.2　割り当てられた機器は、当社のビジネス目標を達成するためにのみ、使用できる。当社の事業の支持または発展以外の目的で、機器を使用してはならない。

2.3　自分のユーザー名及びパスワードを使用してのみ、システムにログオンしなければならない。他人のユーザー名及びパスワードを使用したり、他人に、自分のユーザー名及びパスワードを使用してログオンさせたりしてはならない。

2.4　端末から離れている場合は、ログアウトするか、コンピューターをロックする。終業時には、ログアウトして、コンピューターをシャットダウンしなければならない。

3.　システム/プログラム/基盤

3.1　既存のシステム、プログラム、情報若しくはデータを、削除、破棄、又は変更してはならない（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　[　　]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、システムに影響を与え、ウイルスやその他のマルウェアを導入する可能性がある。

3.3　[　　]の許可なしに、携帯電話、タブレットコンピューター、USB ストレージデバイス等のデバイスを、システムに接続してはならない。

3.4　システムを通過する、すべての電子メールを、そのウイルス感染について監視する。送信元不明の迷惑メールを開く場合は、特に注意すること。電子メールが疑わしいと考える場合には、返信、添付ファイル開封、及びその中のリンクをクリック、をいずれもしてはならない。

3.5　コンピュータにウイルスまたはマルウェアが含まれている可能性がある場合は、直ちに[　　]に通知する。

4. E-mail

4.1 電子メールで第三者とコミュニケーションをとるときは、業務上の口調を採用し、適切なエチケットに沿ったものとする。[標準の電子メール署名と、免責事項も含める必要がある。]

4.2 電子メールは、法的手続で使用でき、削除された電子メールもシステムに残り、取り寄せできる可能性があることに注意する。

4.3 虐待的、わいせつな、差別的、人種差別的、嫌がらせの、侮蔑的、中傷的、性的表現の、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 以下は禁止される：

(a) 第三者に読まれたくない、職場の内密な電子メールを送信、又は転送する。

(b) チェーンメール、ジャンクメール、漫画、ジョーク、ゴシップを、送信、又は転送する。

(c) 些細なメッセージを送信したり、実際に受信する必要のない他者に、電子メールを不必要にコピー、又は転送したりすることで、システム混雑に加担する。

(d) 他者の電子メールアドレス（許可されていない場合）又は仮名で、メッセージを送信する。

4.5 当社の業務目的で電子メールを送受信するために、あなた自身の個人的な電子メールアカウントを使用してはならない。提供された電子メールアカウントのみを使用しなければならない。

4.6 [追加のセキュリティリスクのため、Gmail や Hotmail などの Web ベースの個人用電子メールへのアクセスをコンピューターシステムでいつでも許可していない。]

5. インターネット

5.1 インターネットへのアクセスは、業務目的のみに付与されている。 [時折の個人使用は、第 6 項に記載のように、許される。]

5.2 違法、攻撃的、悪趣味、又は不道徳と見なされる可能性のある、Web ページにアクセスしたり、インターネットから画像や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。ドイツ内で合法である Web コンテンツであっても、この禁止事項に該当する程度に悪趣味である可能性が存在する。原則として、（ページを表示することを意図しているかどうかにかかわらず）誰かがページのコンテンツに当惑する可能性がある場合、又は、当社のソフトウェアが、ページまたはファイルにアクセスしたという事実が公開された場合、問題となる可能性がある場合、当該表示が、この方針違反となる。

5.3 当社の裁量で、いくつかのウェブサイトをブロックしたり、アクセス制限したりすることがある。

6. 監視

6.1 当社のシステムは、電話、電子メール、ボイスメール、インターネット、その他の通信を監視することができる。業務上の理由から、また、雇用主としての当社の役割から、法的義務を遂行するために、電話及びコンピューターシステムを含む、当社のシステムの使用（個人的な使用を含む。）は、自動ソフトウェア又はその他の方法で、継続的に監視される場合がある。

6.2 当社は、以下の目的を含め、業務上の利益のために合理的に必要な場合、電子メールメッセージの内容を取り寄せしたり、インターネットの使用状況（アクセスしたページや行われた検索を含む。）を確認したりする権利を留保する（このリストは網羅的ではない。）。

(a) 電子メールシステムまたはインターネットの使用が合法であり、このポリシーに準拠しているかどうかを監視するため。

(b) 失われたメッセージを検索するため、又は、コンピューターの障害のために失われたメッセージを取得するため。

(c) 申し立てられた不正行為の調査を支援するため。

(d) 法的義務を遵守するため。

7. 禁止事項

7.1 当社の電話又は電子メールシステムの誤用、若しくは、不適切なインターネットの使用は、懲戒手続で対応する。インターネットの誤用は、場合によっては、犯罪となる可能性がある。

7.2 次の資料の作成、表示、アクセス、送信、又はダウンロードは、通常、重大な逸脱行為となる（このリストは網羅的ではない。）。

(a) ポルノ素材（つまり、性的に露骨または興奮する性質の文章、写真、映画、ビデオクリップ）；

(b) 攻撃的、わいせつ、又は犯罪的な内容、若しくは、当社又はクライアントに当惑を引き起こす可能性のある内容。

(c) 個人又は組織に関する、虚偽の名誉毀損の声明。

(d) 差別的、攻撃的、侮蔑的、又は他者を当惑させる可能性のある資料（機会均等ポリシー、ハラスメント防止、及びいじめに関するポリシーに違反する資料を含む）。

(e) 当社、当社のスタッフ又はクライアントに関する機密情報（職務の適切な遂行において許可されている場合を除く。）。

(f) 許可されていないソフトウェア。

(g) （あなた又は当社にとって）刑事または民事責任を引き起こす可能性のあるその他の声明。

(h) 著作権を侵害する音楽、ビデオファイル又はその他の素材。

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) 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.

(2) Bei Beendigung des Arbeitsverhältnisses oder bei Freistellung wird der Arbeitnehmer dem 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.

(3) 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.

§ 1 Confidentiality and Return of Documents

(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) The Employee shall, upon termination of the employment or in the event of the Employee being 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).

(3) 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.

(4) 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.)

(4) 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 Datenträger 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 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.

(4) The employer shall ensure that the employee works in a secured working environment for the respective task, i.e. appropriate programmes and 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、雇用主とすべての関係会社の機密事項と事業秘密および営業秘密のすべて（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、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、所有しているすべ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。

(3) 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。

(4) 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。

(5)［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すべて、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

§ 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.

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.

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 dem Übergang seiner Rechte aus dieser Vereinbarung einverstanden.

§ 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.

§ 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すべての分野に、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、すべ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§§ 74 ff 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

§ 1 Zusammenarbeit

(1) [Beschreibung der Geschäftsbeziehung der Parteien] (die „Zusammenarbeit“)

(2) Mit der vorliegenden Vereinbarung erhält jeder Vertragspartner Schutz für die Informationen, die im Rahmen dieser Zusammenarbeit schon weitergegeben wurden und noch weitergegeben werden.

§ 2 Vertrauliche Informationen

(1) Vertrauliche Informationen im Sinne dieser Vereinbarung sind alle Informationen, die

a) seitens eines Vertragspartners ausdrücklich und schriftlich als vertraulich bezeichnet wurden;

b) zu den nach §§ 17, 18 UWG geschützten Informationen gehören, insbesondere Know-how;

c) durch gewerbliche und andere Schutzrechte geschützt sind, zB Entwurfsmaterial für Software (vgl. § 69a Abs. 1 UrhG);

d) unter das Bankgeheimnis oder den Datenschutz oder eine ähnliche Geheimhaltungspflicht fallen oder von ähnlicher Natur wie die durch Bankgeheimnis oder Datenschutz geschützten Informationen sind

e) bei denen sich das Geheimhaltungsinteresse des offenbarenden Vertragspartners aus der Natur der Information ergibt. „Information“ meint sowohl die Daten als auch die mit den Daten versehenen Datenträger.

§ 1 Cooperation

(1) [Description of business relationship between the parties] (the “Cooperation”).

(2) With the present agreement, each contracting party receives protection for the information that has already been passed on and will still be passed on within the framework of this Cooperation.

§ 2 Confidential Information

(1) Confidential information within the meaning of this agreement is all information which

a) has been expressly designated in writing as confidential by a contractual partner;

b) belongs to information protected under §§ 17, 18 UWG, in particular knowhow;

c) is protected by industrial and other property rights, e.g. design material for software (cf. section 69a para. 1 UrhG);

d) is subject to banking secrecy or data protection or a similar obligation of secrecy or is of a similar nature as the information protected by banking secrecy or data protection

(e) where the disclosing party's interest in secrecy arises from the nature of the information. "Information" means both the data and the data carriers containing the data.

(2) Die Einbeziehung unter die vertraulichen Informationen entfällt oder endet, wenn

a) die Information öffentlich bekannt ist;

b) der offenbarende Vertragspartner schriftlich auf den Schutz verzichtet oder

c) die Information dem empfangenden Vertragspartner auf anderem Wege als durch den offenbarenden Vertragspartner bekannt wurde und hierbei durch niemanden eine Geheimhaltungspflicht verletzt wurde.
Wer sich auf eine dieser Ausnahmen beruft, hat ihr Vorliegen zu beweisen.

(2) Inclusion among the confidential information shall cease or terminate if

a) the information is in the public domain

b) the disclosing contracting party waives protection in writing; or

c) the information became known to the receiving contracting party by means other than through the disclosing contracting party and no obligation of secrecy was breached by anyone in the process.
Whoever invokes one of these exceptions must prove its existence.

§ 3 Gestattete Vorgänge

(1) Der empfangende Vertragspartner darf die Information in der Weise und in dem Maße handhaben (auch kopieren), wie dies zur Durchführung der Zusammenarbeit zweckmäßig und üblich ist.

(2) Der empfangende Vertragspartner darf die Information nur denjenigen seiner angestellten Mitarbeiter zur Verfügung stellen, die in die Zusammenarbeit einbezogen sind, und zwar in dem Maße, wie dies der Aufgabenstellung des Mitarbeiters im Rahmen der Zusammenarbeit entspricht. In diesem Maße darf er die Informationen auch seinen externen Beratern zur Verfügung stellen.

§ 3 Permitted Actions

(1) The receiving contracting partner may handle (including copy) the information in the manner and to the extent that this is expedient and customary for the performance of the Cooperation.

(2) The receiving contracting party may only make the information available to those of its employed staff who are involved in the Cooperation, and to the extent that this corresponds to the task of the employee within the framework of the Cooperation. To this extent, he may also make the information available to his external consultants.

(3) The receiving contractual partner may transfer the information to third

(3) Der empfangende Vertragspartner darf die Information Dritten überlassen, wenn der übertragende Vertragspartner dem zuvor schriftlich zugestimmt hat. Wenn der Dritte ein mit dem empfangenden Vertragspartner nach § 15 AktG verbundenes Unternehmen ist und seine Kenntnisnahme für das gemeinsame Ziel (vgl. § 1) nützlich ist, darf der offenbarende Vertragspartner die Zustimmung nicht ohne nachvollziehbaren Grund verweigern.

parties if the transferring contractual partner has agreed to this in writing in advance. If the third party is a company affiliated with the receiving contracting party pursuant to section 15 of the German Stock Corporation Act (AktG) and its knowledge is useful for the common objective (cf. section 1), the disclosing contracting party may not refuse consent without comprehensible reason.

(4) Der empfangende Vertragspartner darf die Information offenbaren, soweit er hierzu gesetzlich oder behördlich verpflichtet ist. Er beachtet hierbei § 4 Abs. 4

(4) The receiving contracting party may disclose the information insofar as it is obliged to do so by law or by the authorities. In doing so, he/she shall observe § 4 para. 4

§ 4 Pflichten

§ 4 Duties

(1) Der empfangende Vertragspartner schützt und sichert die vertraulichen Informationen mit der erforderlichen Sorgfalt, zumindest mit der Sorgfalt, mit welcher er eigene vergleichbare Informationen schützt. Informationen werden so verwahrt und gesichert, dass Missbrauch und unbefugte Kenntnisnahme ausgeschlossen sind.

(1) The receiving contracting party shall protect and secure the confidential information with the necessary care, at least with the care with which it protects its own comparable information. Information shall be stored and secured in such a way that misuse and unauthorised access are excluded.

(2) In Bezug auf Informationen nach § 2 Abs. 1 (d) kann der überlassende Vertragspartner verlangen, dass kenntnisnehmende Personen schriftlich zur Verschwiegenheit nach Maßgabe dieser Vereinbarung verpflichtet werden (vgl. § 53 BDSG) und dass dies dem überlassenden Vertragspartner im Voraus nachgewiesen wird.

(2) With regard to information according to § 2 para. 1 (d), the providing contracting party may demand that persons having knowledge are obliged in writing to maintain confidentiality in accordance with this agreement (cf. § 53 BDSG) and that this is proven to the providing contracting party in advance.

(3) Der empfangende Vertragspartner unterrichtet den überlassenden Vertragspartner unverzüglich und schriftlich, wenner Kenntnis oder Verdacht von einer bevorstehenden oder stattgefundenen Verletzung der Geheimhaltungsinteressen des überlassenden Vertragspartners hat.

(3) The receiving contractual partner shall inform the assigning contractual partner immediately and in writing if it has knowledge or suspicion of an imminent or actual breach of the confidentiality interests of the assigningcontractual partner.

Geschützt hierbei sind die Geheimhaltungsinteressen des überlassenden Vertragspartners gegenüber jedermann.

The confidentiality interests of the transferring contractual partner vis-à-vis everyone are protected in this respect.

(4) Der empfangende Vertragspartner unterrichtet den überlassenden Vertragspartner unverzüglich und im Voraus von einer Weitergabe der Informationen nach § 3 Abs. 4.

(4) The receiving contracting party shall inform the transferring contracting party without delay and in advance of any disclosure of information pursuant to Article 3 (4).

§ 5 Unerlaubte Vorgänge

§ 5 Unauthorised Actions

(1) Der empfangende Vertragspartner darf (soweit in § 3 oder in anderer Weise nichts anderes ausdrücklich schriftlich gestattet ist) Schutzrechte an den vertraulichen Informationen (insbesondere urheberrechtliche Befugnisse) nicht nutzen. Er darf auch sonst die Informationen (auch wenn sie nicht unter ein gesetzliches Schutzrecht fallen) in keiner Weise nutzen oder verwerten.

(1) The receiving contracting party may not (unless otherwise expressly provided in writing in § 3 or otherwise) use industrial property rights to the confidential information (in particular copyright rights). Nor may it otherwise use or exploit the information (even if it is not covered by a statutory property right) in any way.

(2) Kein Vertragspartner darf angestellten Mitarbeitern des anderen Vertragspartners das Angebot machen, ihn während der Dauer dieser Vereinbarung und bis zum Ablauf zweier Kalenderjahre danach einzustellen (Abwerbeverbot). Das Abwerbeverbot verpflichtet auch verbundene Unternehmen des einen Vertragspartners und schützt auch im Sinne eines Vertrages zugunsten Dritter verbundene Unternehmen des anderen Vertragspartners in Bezug auf deren Mitarbeiter; die Vertragspartner stehen insofern hiermit für die Handlungen der mit ihnen jeweils verbundenen Unternehmen ein. Einem solchen Arbeitsvertrag stehen andere Angebote und Vereinbarungen gleich, aufgrund derer die Arbeitskraft des Mitarbeiters nicht mehr dem bislang anstellenden Unternehmen zugutekommt, sondern ganz oder teilweise dem Vertragspartner.

(2) No contractual partner may make an offer to employed staff of the other contractual partner to employ him during the term of this agreement and until the expiry of two calendar years thereafter (non-solicitation). The non-solicitation clause also obliges affiliated companies of one contracting party and also protects, in the sense of a contract for the benefit of third parties, affiliated companies of the other contracting party with regard to their employees; the contracting parties are hereby liable for the actions of their respective affiliated companies. Other offers and agreements on the basis of which the employee's labour no longer benefits the previously employing enterprise but the contracting party in whole or in part are equivalent to such an employment contract.

§ 6 Vertragsstrafe

(1) Ein Vertragspartner, der Pflichten nach § 3, § 4 oder § 5 verletzt (Schuldner), hat dem anderen Vertragspartner (Gläubiger) für jeden Pflichtverstoß unter Verzicht auf die Einrede des Fortsetzungszusammenhangs eine Vertragsstrafe zu bezahlen. Die Vertragsstrafe beträgt für Verstöße gegen § 3, § 4, § 5 Abs. 1 zwischen EUR [•] und EUR [•] Sie hat in diesem Rahmen billigem Ermessen zu entsprechen. Maßgeblich hierfür sind die Bedeutung der verletzten Pflicht, der Nachteil des Gläubigers (auch der immaterielle Nachteil) und der Grad der Pflichtverletzung und des Verschuldens des Schuldners. Einigen sich die Vertragspartner hierüber nicht, so entscheidet hierüber verbindlich als Schiedsgutachter ein vom Präsidenten des Oberlandesgerichtes [•] benannter Richter dieses Oberlandesgerichtes nach (auch nur schriftlicher) Anhörung der Vertragspartner.

(2) Für den Fall eines Verstoßes gegen § 5 Abs. 2 beträgt die Vertragsstrafe drei Bruttomonatsgehälter, wie der Mitarbeiter sie zuletzt zu bekommen hatte (bei variabler Vergütung bezogen auf die letzten 12 vollen Kalendermonate). Bei erfolgreicher Abwerbung beträgt die Vertragsstrafe das Doppelte.

§ 7 Dauer der Verpflichtung

Soweit nichts anderes vereinbart ist, gelten die Verpflichtungen aus der vorliegenden Vereinbarung auf Dauer.

§ 6 Contractual penalty

(1) A contracting party who breaches obligations under § 3, § 4 or § 5 (debtor) shall pay the other contracting party (creditor) a contractual penalty for each breach of obligation, waiving the defence of continuation of the contract. The contractual penalty for breaches of § 3, § 4, § 5 para. 1 shall be between EUR [•] and EUR [•] and shall be in accordance with reasonable discretion. The decisive factors are the significance of the breached obligation, the disadvantage to the creditor (including the immaterial disadvantage) and the degree of the breach of obligation and the fault of the debtor. If the parties to the contract do not agree on this, a judge of this Higher Regional Court appointed by the President of the Higher Regional Court [•] shall make a binding decision on this as an arbitrator after hearing the parties to the contract (even if only in writing).

(2) In the event of a breach of section 5 subsection 2, the contractual penalty shall amount to three gross monthly salaries as the employee last received them (in the case of variable remuneration based on the last 12 full calendar months). In the event of a successful enticement, the contractual penalty shall be twice that amount.

§ 7 Duration of the obligation

Unless otherwise agreed, the obligations under this Agreement shall be perpetual.

§ 8 Vertragsdauer

(1) Die Vereinbarung kann von jedem Vertragspartner jederzeit gekündigt werden, jedoch frühestens auf einen Zeitpunkt, zu welchem die in § 1 Abs. 1 genannte Zusammenarbeit endet.

(2) Die Vereinbarung endet in jedem Fall mit Ablauf eines vollen Kalenderquartals nach Ende der Zusammenarbeit.

§ 8 Term of the agreement

(1) The agreement may be terminated by either contracting party at any time, but not earlier than the date on which the Cooperation referred to in Article 1(1) ends.

(2) The agreement shall end in any case at the end of a full calendar quarter after the end of the Cooperation.

§ 9 Schlussbestimmungen

(1) Die für Vorgänge bei der Durchführung der Vereinbarung angeordnete Schriftform wird auch durch Telefax und E-Mail eingehalten und auch, wenn die Festlegung in einem Protokoll über eine Besprechung zwischen den Vertragspartnern niedergelegt ist, das Protokoll allen Vertragspartnern vorliegt und binnen zwei Wochen kein schriftlicher Widerspruch erfolgt.

(2) [Schlussklauseln über anwendbares Recht, Gerichtsstand und Schriftform]

§ 9 Final Provisions

(1) The written form prescribed for transactions in the execution of the agreement shall also be complied with by fax and e-mail and also if the stipulation is laid down in a record of a discussion between the contracting parties, the record is available to all contracting parties and no written objection is made within two weeks.

(2) [Final clauses on applicable law, place of jurisdiction and written form].

(参考書式)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

§1　協力

(1)［当事者間取引関係の説明］(「本協力」又は「本合意」)

(2) 現在の合意の下で、各契約当事者は、本協力の枠組みの中で、すでに渡されている情報、並びに、引き続き渡される情報について、保護を享受する。

§2　機密情報

(1) 本合意内の「機密情報」とは、以下に該当するような、すべての情報である。

a) 契約当事者によって、機密として、書面で明示的に指定されている。

b) UWG§§17、18 で保護されている情報、特にノウハウに属している。

c) 産業財産権並びにその他財産権によって保護されている。例：ソフトウェアのデザイン素材

(UrhG 第 69a 条第 1 段落を参照)

d) 銀行秘密またはデータ保護の対象となっているか、同様の機密保持義務を生じさせるもの、又は、情報が、銀行秘密又はデータ保護で守られるために、銀行秘密によって保護される情報と同様の性質のもの。

e) 開示する当事者の機密性に関する利益が、情報の性質から生じるもの。

「情報」とは、データ及びデータを内蔵するデータキャリアをいう。

(2) 機密情報への内包は、次の場合に中止または終了する。

a) 情報はパブリックドメインにある。

b) 開示する契約当事者が、書面により保護を免除する。

c) 情報が、開示を受ける当事者に、開示する契約当事者から受けとる以外の手段で、秘密保持義務の違反の状況のない状態で、知られるようになった。

これらの例外の 1 つを主張する者は、誰でも、その存在を証明する必要がある。

§3　許可される行為

(1) 受領する契約当事者は、本協力の履行のために、効率的で、慣習的に行われうる方法および範囲で、情報を処理（コピーを含む）できる。

(2) 受領する当事者は、情報を利用できるようにするだけ

本協力に関与している、雇用されたスタッフにのみ、そしてこれが本協力の枠組内で職務を行う限りで、従業員に情報利用できるようにする。この限定内で、外部コンサルタントにも、情報を利用できるようにすることができる。

(3) 受領する当事者は、情報を与える当事者が、書面でこれに同意する場合、情報を第三者に転送することができる。第三者が、ドイツ株式法（AktG）第 15 条に基づき、受領当事者の関連会社の場合、及び、その知識が、共通の目的に有益である（§1 を参照）場合には、開示する契約当事者は、理解しうる理由なく、同意を拒否することはできません。

(4) 受領当事者は、法律または規制当局による義務がある場合、情報を開示することができる。但し、受領当事者は、§4 第 4 段落を遵守しなければならない。

§4　義務

(1) 受領当事者は、必要な注意をもって、少なくとも、自己が同種の情報を保護するために払う注意と比較可能な程度に、機密情報を保護及び防御するものとする。情報は、誤用や無許可のアクセスが除外されるように、保護及び防御されるものとする。

(2) 提供する契約当事者は、§2 第 1 段落(d)の情報について、知識を有する者が、本合意（BDSG§53 を参照）に従って、機密性を維持することが義務付けられていること、並びに、これが、提供する契約当事者に証明されていることを、書面で要求することができる。

(3) 受領する契約当事者は、提供する契約当事者の機密性の利益への、差し迫った、若しくは、現実の違背についての認識又は疑いがある際には、直ちに、提供する契約当事者に、書面で通知するものとする。

(4) 受領締約国は、第 3 条(4)に基づく情報の開示に先立って、かつ、遅滞なく、提供する契約者に通知する。

§5　許されない行為

(1) 受領する当事者は、（§3 に基づく、又は、その他の書面で明記されていない限り）機密情報に対する産業所有権を、特に著作権を、使用することはできない。また、（法定財産権の対象外であっても）情報を使用又は搾取することはできない。

(2) 契約当事者は、他の契約当事者の雇用されたスタッフに、本契約期間及びその後 2 暦年の間、雇用するために、雇用の申し出をしてはならない（非勧誘）。非勧誘条項は、契約当事者の関連会社をも同様に義務づけ、更に、第三者の利益のための契約の意味で、相手方契約当事者の関連会社の従業員に関しても、保護の対象とする。契約当事者は、これにより、それぞれの関連会社の行動に対して責任を負う。契約又は申出のうち、従業員の労働が、全体または一部で、以前の雇用主である契約当事者に利益をもたらさなくなり、他の契約当事者に利益となるものは、勧誘の雇用契約に相当する。

§6　契約上の罰金

(1) §3、§4、又は§5 に基づく義務に違反する契約当事者（債務者）は、契約継続の抗弁を放棄し、他の契約当事者（債権者）に、それぞれの義務違反に、契約上の罰金を支払う。 §3、§4、及び、§5 第 1 項の義務違反に対する契約上の罰金は、EUR [·]と EUR [·]の間の額であり、合理的な裁量に従う。決定的な要因は、違反された義務の重要性、債権者への不利益（重要でない不利益を含む）、違反の程度、及び債務者の過失である。もしも、契約当事者間に同意が得られない場合、当事者双方の主張立証を聞いた後（書面のみであっても）、当該地域の高等裁判所裁判長によって任命された高等地方裁判所の裁判官を仲裁人とした仲裁により、拘束力のある決定で解決されることに同意する。

(2) §5 第 2 項の違反が発生した場合、契約上の罰金は、従業員が最後に受取した月給総額の 3 倍になる。（変動報酬の場合、過去 12 全暦月に基づく）。勧誘が成功した場合、契約上の罰金は、この 2 倍の額になる。

§7　義務の存続期間

別段の合意がない限り、本契約に基づく義務は永続的である。

§8　本契約の期間

(1) 本契約は、いつでも、どちらかの契約当事者により終了する場合がある。しかし、第1条(1)で言及されている、本協力日終了日より前でない。

(2) 本契約は、いかなる場合でも、本協力の終了後、完全な暦四半期で終了するものとする。

§9 終局的規定

(1) 本契約締結時の取引について定められた書面は、ファックスと電子メールでも交わされるものとする。もし、本契約の定めが、契約当事者の協議の記録に記載された場合、すべての契約当事者がその記録を利用でき、2週間以内に書面による異議申立てが行われないことを要する。

(2) [準拠法、管轄地、及び、本契約書面の方式についての、最終的な条項]。

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:

* * *

（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

１　就業規則における秘密保護関連規定の例

Staff handbook

6. Introduction

6.1 [GENERAL DETAILS ABOUT THE EMPLOYER AND ITS BUSINESS.]

6.2 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.

7. Using the Staff Handbook

7.1 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.

7.2 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). They do **not** form part of the terms of your contract with us, which are provided to you separately.

8. Responsibility for the Staff Handbook

8.1 The HR Manager has overall responsibility for this Staff Handbook and for ensuring that its policies and procedures comply with our legal obligations.

8.2 The Staff Handbook is reviewed regularly to ensure that its provisions continue to meet our legal obligations and reflect best practice.

8.3 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.

9. Personal data

9.1 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 intranet for further information.

10. Emergency contact details

10.1 The Human Resources Department is responsible for maintaining up-to-date details of your home address and the emergency contact telephone numbers of the 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 will periodically be asked to confirm that these are up to dat]. This information is held in confidence and will only be used when needed.

Schedule 1 Dress code

1. About this policy

1.1 We encourage everyone to maintain an appropriate standard of dress and personal appearance at work. The purpose of our dress code is to establish basic guidelines on appropriate clothing and appearance at our workplace, so that we:

(a) promote a positive and professional image;

(b) respect the needs of men and women from all cultures and religions;

(c) make any adjustments that may be needed because of disability;

(d) take account of health and safety requirements; and

(e) help staff and managers decide what clothing it is appropriate to wear to work.

1.2 Managers are responsible for ensuring that this dress code is observed and that a common sense approach is taken to any issues that may arise. Any enquiries regarding the operation of our dress code (including whether an article of clothing is suitable to wear to work) should be made to your line manager or the Human Resources Department.

1.3 Failure to comply with the dress code may result in action under our Disciplinary Procedure.

1.4 We will review our dress code periodically to ensure that it reflects appropriate standards and continues to meet our needs.

1.5 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. Appearance

2.1 While working for us you represent us with customers and the public. Your appearance contributes to our reputation and the development of our business.

2.2 It is important that you appear clean and smart at all times when at work, particularly when you may be in contact with clients, other business contacts or the general public.

2.3 [Different departments may have specific clothing requirements, for example, because their work is customer-facing or raises particular health and safety concerns. It is important that you dress in a manner appropriate to your working environment and the type of work you do.]

2.4 All employees in customer facing roles should wear smart business attire.

2.5 Employees in certain roles may be asked to cover up visible tattoos or to remove or cover up visible body piercings.

2.6 Footwear must be safe and clean and take account of health and safety considerations. Trainers, stilettos and flip-flops are not acceptable.

2.7 Where we provide safety clothing and equipment, including protective footwear, it should be worn or used as appropriate and directed.

3. Religious and cultural dress

3.1 You may wear appropriate religious and cultural dress (including clerical collars, head scarves, skullcaps and turbans) unless it creates a health and safety risk to you or any other person or otherwise breaches this policy.

3.2 Where necessary the Human Resources Department can give further information and guidance on cultural and religious dress in the workplace.

3.3 Priority is at all times given to health and safety requirements. Where necessary, advice will be taken from the Health and Safety Officer.

Schedule 2 Expenses policy

1. About this policy

1.1 This policy deals with claims for reimbursement of expenses, including travel, accommodation and hospitality.

1.2 This policy does not form part of any employee's contract of employment and we may amend it 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 voice whistleblowing concerns openly under this policy. Completely anonymous disclosures are difficult to investigate. If you want to raise your concern confidentially, we will make every effort to keep your identity secret and only reveal it where necessary to those involved in investigating your concern.

2. External disclosures

2.1 The aim of this policy is to provide an internal mechanism for reporting, investigating and remedying any wrongdoing in the workplace. In most cases you should not find it necessary to alert anyone externally.

2.2 The law recognises that in some circumstances it may be appropriate for you to report your concerns to an external body such as a regulator. We strongly encourage you to seek advice before reporting a concern to anyone external. Protect operates a confidential helpline. Their contact details are at the end of this policy.

3. Protection and support for whistleblowers

3.1 We aim to encourage openness and will support whistleblowers who raise genuine concerns under this policy, even if they turn out 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 suffered any such treatment, you should inform [the Whistleblowing Officer **OR** [POSITION]] immediately. [If the matter is not remedied you should raise it formally using our Grievance Procedure.]

3.3 You must not threaten or retaliate against whistleblowers in any way. If you are involved in such conduct you may be subject to disciplinary action. [In some cases the whistleblower could have a right to sue you personally for compensation in an employment tribunal.]

3.4 However, if we conclude that a whistleblower has made false allegations maliciously, the whistleblower may be subject to disciplinary action.

3.5 Protect 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 procedure

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

1. About this policy

1.1 This flexible working policy gives eligible employees an opportunity to request a change to their working pattern.

1.2 We will deal with flexible working requests in a reasonable manner and within a reasonable time. In any event the time between making a request and notifying you of a final decision (including the outcome of any appeal) will be less than three months unless we have agreed a longer period with you.

1.3 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. Eligibility

2.1 To be eligible to make a flexible working request, you must:

(a) be an employee;

(b) have worked for us continuously for at least 26 weeks at the date your request is made; and

(c) not have made a flexible working request during the last 12 months (even if you withdrew that request).

3. What is a flexible working request?

3.1 A flexible working request under this policy means a request to do any or all of the following:

(a) to reduce or vary your working hours;

(b) to reduce or vary the days you work;

(c) to work from a different location (for example, from home).

4. Making a flexible working request

4.1 Your flexible working request should be submitted to [us **OR** [POSITION]] in writing and dated. It should:

(a) state that it is a flexible working request;

(b) explain the change being requested and propose a start date;

(c) identify the impact the change would have on the business and how that might be dealt with; and

(d) state whether you have made any previous flexible working requests.

5. Meeting

5.1 We will arrange a meeting at a convenient time and place to discuss your request. You may be accompanied at the meeting by a colleague of your choice. They will be entitled to speak and confer privately with you, but may not answer questions on your behalf.

5.2 We may decide to grant your request in full without a meeting, in which case we will write to you with our decision.

6. Decision

6.1 We will inform you in writing of our decision as soon as possible after the meeting.

6.2 If your request is accepted, we will write to you with details of the new working arrangements and the date on which they will commence. You will be asked to sign and return a copy of the letter.

6.3 If we cannot immediately accept your request we may require you to undertake a trial period before reaching a final decision on your request.

6.4 Unless otherwise agreed, changes to your terms of employment will be permanent.

6.5 We may reject your request for one or more of the following business reasons:

(a) the burden of additional costs;

(b) detrimental effect on ability to meet customer demand;

(c) inability to reorganise work among existing staff;

(d) inability to recruit additional staff;

(e) detrimental impact on quality;

(f) detrimental impact on performance;

(g) insufficiency of work during the periods that you propose to work; or

(h) planned changes.

6.6 If we are unable to agree to your request, we will write to tell you which of those reasons applies in your case. We will also set out the appeal procedure.

7. Appeal

7.1 You may appeal in writing within 14 days of receiving our written decision. [This includes a decision following a trial period.]

7.2 Your appeal must be dated and must set out the grounds on which you are appealing.

7.3 We will hold a meeting with you to discuss your appeal. You may bring a colleague to the meeting.

7.4 We will tell you in writing of our final decision as soon as possible after the appeal meeting, including reasons. There is no further right of appeal.

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 intended to promote effective communication and working practices. This policy outlines the standards you must observe when using these systems, when we will monitor their use, and the action we will take if you breach these standards.

1.2 [POSITION] has overall responsibility for this policy, including keeping it under review.

1.3 Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

1.4 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. Equipment security and passwords

2.1 You are responsible for the security of the equipment allocated to or used by you, and you must not allow it to be used by anyone other than in accordance with this policy. You should use passwords on all IT equipment, particularly items that you take out of the office. You should keep your passwords confidential and change them regularly.

2.2 You may use the equipment allocated to you only to serve our business goals. You may not use the equipment for anything that does not support or augment our business.

2.3 You must only log on to our systems using your own username and password. You must not use another person's username and password or allow anyone else to log on using your username and password.

2.4 If you are away from your desk you should log out or lock your computer. You must log out and shut down your computer at the end of each working day.

3. Systems and data security

3.1 You should not delete, destroy or modify existing systems, programs, information or data (except specifically authorised in the proper performance of your duties).

3.2 You must obtain a permission from your supervisor and our security manager for accessing, obtaining, retaining, transferring, copying, disclosing, communicating, or altering technical and operational information about existing our computer systems, networks, and IT infrastructures.

3.3 You must obtain a permission from your supervisor and our data security manager for transferring, copying, uploading, disclosing, communicating, or altering information and data that you have access to in connection with performance of your work and is not shared with outside people or other staff who are not given access to such information and data by our security manager.

3.4 You must not download or install software from external sources without authorisation from [POSITION]. Downloading unauthorised software may interfere with our systems and may introduce viruses or other malware.

3.5 You must not attach any device or equipment including mobile phones, tablet computers or USB storage devices to our systems without authorisation from [POSITION].

3.6 We monitor all e-mails passing through our system for viruses. You should exercise particular caution when opening unsolicited e-mails from unknown sources. If an e-mail looks suspicious do not reply to it, open any attachments or click any links in it.

3.7 Inform [POSITION] immediately if you suspect your computer may have a virus or malware.

3.8 Upon termination of your employment, you must return all the equipment allocated to or used by you as they should be.

4. E-mail

4.1 Adopt a professional tone and observe appropriate etiquette when communicating with third parties by e-mail. [You should also include our standard e-mail signature and disclaimer.]

4.2 Remember that e-mails can be used in legal proceedings and that even deleted e-mails may remain on the system and be capable of being retrieved.

4.3 You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate e-mails.

4.4 You should not:

(a) send or forward private e-mails at work which 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 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.

4.5 Do not use your own personal e-mail account to send or receive e-mail for the purposes of our business. Only use the e-mail account we have provided for you.

4.6 [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.]

5. Using the internet

5.1 Internet access is provided solely for business purposes.

5.2 You should not access any web page or download any image or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content that is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

5.3 We may block or restrict access to some websites at our discretion.

6. Personal use of our systems

7. Monitoring

7.1 Our systems enable us to monitor telephone, e-mail, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations in our role as an employer, your use of our systems including the telephone and computer systems (including any personal use) may be continually monitored by automated software or otherwise.

7.2 We reserve the right to retrieve the contents of e-mail messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the business, including for the following purposes (this list is not exhaustive):

(a) to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy;

(b) to find lost messages or to retrieve messages lost due to computer failure;

(c) to assist in the investigation of alleged wrongdoing; or

(d) to comply with any legal obligation.

8. Prohibited use of our systems

8.1 Misuse or excessive personal use of our telephone or e-mail system or inappropriate internet use will be dealt with under our Disciplinary Procedure. Misuse of the internet can in some cases be a criminal offence.

8.2 Creating, viewing, accessing, transmitting or downloading any of the following material will usually amount to gross misconduct (this list is not exhaustive):

(a) pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

(b) offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients;

(c) a false and defamatory statement about any person or organisation;

(d) material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities Policy or our Anti-harassment and Bullying Policy);

(e) confidential information about us or any of our staff or clients (except as authorised in the proper performance of your duties);

(f) unauthorised software;

(g) any other statement which is likely to create any criminal or civil liability (for you or us); or

(h) music or video files or other material in breach of copyright.

Schedule 27 Social media policy

1. About this policy

1.1 This policy is in place to minimise the risks to our business through use of social media.

1.2 This policy deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Google+, Wikipedia [, Whisper] [, Instagram] [, Tumblr] and all other social networking sites, internet postings and blogs. It applies to use of social media for business purposes as well as personal use that may affect our business in any way.

1.3 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. Personal use of social media

2.1 [Personal use of social media is never permitted during working hours or by means of our computers, networks and other IT resources and communications systems.

OR

Occasional personal use of social media during working hours is permitted so long as it does not involve unprofessional or inappropriate content, does not interfere with your employment responsibilities or productivity and complies with this policy.]

3. Prohibited use

3.1 You must avoid making any social media communications that could damage our business interests or reputation, even 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 against staff or third parties; 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. You may be required to undergo training in order to obtain such authorisation.

3.4 You must not post comments about sensitive business-related topics, such as our performance, or do anything to jeopardise our trade secrets, confidential information and intellectual property. You must not include our logos or other trademarks in any social media posting or in your profile on any social media.

3.5 [You are not permitted to add business contacts made during the course of your employment to personal social networking accounts.

OR

The contact details of business contacts made during the course of your employment are our confidential information. On termination of employment you must provide us with a copy of all such information, delete all such information from your personal social networking accounts and destroy any further copies of such information that you may have.]

3.6 Any misuse of social media should be reported to [POSITION].

4. Guidelines for responsible use of social media

4.1 You should make it clear in social media postings, or in your personal profile, that you are speaking on your own behalf. Write in the first person and use a personal e-mail address.

4.2 Be respectful to others when making any statement on social media and be aware that you are personally responsible for all communications which will be published on the internet for anyone to see.

4.3 If you disclose your affiliation with us on your profile or in any social media postings, you must state that your views 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 are consistent with the professional image you present to clients and colleagues.

4.4 If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with your manager.

4.5 If you see social media content that disparages or reflects poorly on us, you should contact [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 committing a breach of this policy will be required to co-operate with our investigation.

5.2 You may be required to remove any social media content that we consider to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

(参考和訳)就業規則における秘密保護関連規定の例

就業規則

1. 初めに

1.1 ［雇用主とその事業に関する一般的記載］

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. 就業規則の使用について

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、主要な方針や手続きを示す。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、すべ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、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。

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、その趣旨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、行動がその要件を下回ったときに、確実に対処しなければならない。

4. 個人情報

4.1 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、合法的な理由がある場合にのみ、処

理される。当社は、あなたにデータの使用目的を通知する。詳細については、イントラネットのプライバシー通知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　ドレスコード

1.　この方針について

1.1　私たちは、すべての者が、職場における、適切な服装と個人的な外見の基準を、維持することを勧奨する。ドレスコードの目的は、職場での適切な服装と外見に関する、基本的なガイドラインを確立することにあり、そうして：

(a)　ポジティブでプロフェッショナルなイメージを促進する。

(b)　すべての文化と宗教の、男性と女性のニーズを尊重する。

(c)　障害のために必要となる可能性のある調整を行う。

(d)　健康と安全の要求を考慮に入れる。

(e)　スタッフと管理者が、仕事に着るのに適切な服を、決める助けとなる。

1.2　管理者は、このドレスコードが遵守され、発生する可能性のある問題に対して、常識的なアプローチが取られるようにする責任がある。ドレスコードの運用に関する問い合わせ（衣服が仕事に適しているかどうかを含む）は、ラインマネージャーまたは人事部に連絡すること。

1.3　ドレスコードに従わない場合は、懲戒手続きに基づく措置が取られる可能性がある。

1.4　ドレスコードは、定期的に見直され、適切な基準を反映し、ニーズを依然として満たしているかが確認される。

1.5　この方針は、従業員の雇用契約の一部を構成するものではなく、いつでも修正することができる。

2.　外見

2.1　私たちのために働いている間、あなたは、顧客や一般の人々に、私たちを代表する。あなたの外見は、私たちの評判と、私たちのビジネスの発展に、貢献する。

2.2　仕事中、特に、顧客、他のビジネス上の連絡先、または、一般の人々と接触している可能性があるとき、常に、清潔で、賢明に見えることが重要となる。

2.3　[たとえば、部門ごとに、特定の衣服の要求がある場合がある。たとえば、仕事が顧客と接するため、または、特定の健康と安全上の問題を引き起こしうるためであり、作業環境や、作業の種類に適した服装をする、ことが重要である。]

2.4　顧客対応の役割を担う従業員は、全て、賢実なビジネス服を着る必要がある。

2.5　特定の役割の従業員は、目に見える入れ墨を隠すか、目に見えるボディピアスを取り除くか、隠すように、求められる場合がある。

2.6　履物は、安全で清潔でなければならず、健康と安全のための考慮事項を、検討しなければならない。トレーナー、ハイヒール、フリップフロップは、着用できない。

2.7　保護靴を含む、安全服および装備を提供する場合は、必要に応じて、若しくは、指示に従って、着用、又は、使用する必要がある。

3.　宗教的、文化的衣服

3.1　あなたや他者への健康、安全上のリスクを生んだり、他の規則に違反しない限り、あなたは、適切な、宗教的、並びに、文化的な衣服（僧の襟、頭巾、帽子、ターバンを含む）を身につけることができる。.

3.2　必要な場合、人事部は、職場の文化的、及び、宗教的服装について、更に情報やガイダンスを提供する。

3.3　健康、安全の要求が常に優先される。必要な場合、健康安全役員からアドバイスを得られる。

Schedule 2　**内部告発方針**

1.　**機密性**

1.1　この方針の下で、スタッフが、内部者の不正の懸念を公然と表明できるようになることを願う。完全に匿名の開示を、調査することは困難である。あなたが、秘密裏に懸念を提起したい場合、私たちは、あなたの身元を秘密に保つために、あらゆる努力をし、あなたの懸念の調査に関与する人々に必要な場合にのみ、それを明らかにする。

2.　**外部への開示**

2.1　このポリシーの目的は、職場での不正行為を報告、調査及び是正するための内部メカニズムを提供することである。ほとんどの場合、外部の者に警告する必要はない。

2.2　法律は、状況によっては、規制当局などの外部機関に、懸念を報告することが適切な場合があることを認める。外部者に懸念を報告する前に、アドバイスを求めることを強く勧める。［機関の名前］は、機密のヘルプラインを運営している。その連絡先の詳細は、このポリシーの最後に記載されている。

3.　**内部告発者の保護と支持**

3.1　当社は、開放性を励まし、この方針下に真摯に懸念を表明する内部告発者に、たとえ間違っていたとしても、サポートを与える。

3.2　内部告発者は、真摯な懸念を表明した結果として、不当な扱いを受けてはならない。そのような扱いを受けたと思われる場合は、直ちに[内部告発責任者[　　]に]申告する必要がある。[問題が解決されない場合は、異議申立手続を使用して、正式に問題提起する必要がある。]

3.3　内部告発者に対して、いかなる方法でも、脅迫したり、報復したりしてはならない。あなたが、そのような行為に関与している場合、あなたは懲戒処分の対象となる可能性がある。[場合によっては、内部告発者は、雇用審判所で、損害賠償請求のために、あなたを個人的に訴えることがある。]

3.4　しかし、もし、当社で、内部告発者が、虚偽の主張を悪意で行ったと認めた場合には、内部告発者は、懲戒処分の対象となりうる。

3.5　[機関の名前]は、機密のヘルプラインを運営している。この方針の最後に、その連絡先がある。

4. **連絡先**

内部告発役員	[名前] [電話] [E-MAIL]
[業務執行員［又は、他の信用される個人]]	[名前] [電話] [E-MAIL]
[機関の名前／Protect] (独立した公益機関)	Helpline: 0203 117 2520 E-mail: Website:

Schedule 3　**IT 及び通信システム方針**

1.　この方針について

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作業慣行を促進することを目的としている。この方針は、これらのシステムを使用するときに遵守しなければならない基準、それらの使用を監視する時期、及びこれらの基準に違反した場合に実行する行動の概要を示している。

1.2　[　　]は、この方針の見直しの継続を含め、この方針に対して、全体的に責任を負う。

1.3　この方針の違反は、懲戒手続で対応される可能性があり、深刻な場合には、即時解雇につながる重大な逸脱行為として扱われる可能性がある。

1.4　この方針は、従業員の雇用契約の一部を形成するものではなく、当社において、随時改変することができる。

2.　機器の安全性及びパスワード

2.1　あなたは、あなたに割り当てられた、または、あなたが使用する機器の安全性に責任を負い、この方針に服する者以外の者による使用を許可してはならない。すべての IT 機器、特に、オフィスから持ち出す品目には、パスワードを使用しなければならない。パスワードは、内密にし、定期的に変更する必要がある。

2.2　割り当てられた機器は、当社のビジネス目標を達成するためにのみ、使用できる。当社の事業の支持または発展以外の目的で、機器を使用してはならない。

2.3　自分のユーザー名及びパスワードを使用してのみ、システムにログオンしなければならない。他人のユーザー名及びパスワードを使用したり、他人に、自分のユーザー名及びパスワードを使用してログオンさせたりしてはならない。

2.4　端末から離れている場合は、ログアウトするか、コンピューターをロックする。終業時には、ログアウトして、コンピューターを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安全性

3.1　既存のシステム、プログラム、情報若しくはデータを、削除、破棄、又は変更してはならない（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　既存のコンピューターシステム、ネットワーク並びに IT 基盤に関する技術情報及び運用情報にアクセス、取得、保持、転送、コピー、開示、通信、又は変更するには、上司及び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　業務の遂行に関連してアクセスでき、外部者、並びに、当社のセキュリティマネージャーから、そのような情報やデータへのアクセスを許可されていないスタッフと、共有されていない情報及びデータを、転送、コピー、アップロード、開示、伝達、又は変更するには、上司及びデータセキュリティマネージャーから、許可を得る必要がある。

3.4　[　　]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、システムに影響を与え、ウイルスやその他のマルウェアを導入する可能性がある。

3.5　[　　]の許可なしに、携帯電話、タブレットコンピューター、USB ストレージデバイス等のデバイスを、システムに接続してはならない。

3.6　システムを通過する、すべての電子メールを、ウイルス感染について監視する。送信元不明の迷惑メールを開く場合は、特に注意すること。電子メールが疑わしいと考える場合には、返信、添付ファイル開封、及びその中のリンクをクリック、をいずれもしてはならない。

3.7　コンピュータにウイルスまたはマルウェアが含まれている可能性がある場合は、直ちに[　　]に通知する。

3.8　雇用終了時に、割り当てられた、または使用された、すべての機器を本来あるべき状態で返却する必要がある。

4.　E-mail

4.1　電子メールで第三者とコミュニケーションをとるときは、業務上の口調を採用し、適切なエチケットに沿ったものとする。[標準の電子メール署名と、免責事項も含める必要がある。]

4.2　電子メールは、法的手続で使用でき、削除された電子メールもシステムに残り、取得できる可能性があることに注意する。

4.3　虐待的、わいせつな、差別的、人種差別的、嫌がらせの、侮蔑的、中傷的、性的表現の、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　以下は禁止される：

(a)　第三者に読まれたくない、職場の内密な電子メールを送信、又は転送する。

(b)　チェーンメール、ジャンクメール、漫画、ジョーク、ゴシップを、送信、又は転送する。

(c)　些細なメッセージを送信したり、実際に受信する必要のない他者に、電子メールを不必要にコピー、又は転送したりすることで、システム混雑に加担する。

(d)　他者の電子メールアドレス（許可されていない場合）又は仮名で、メッセージを送信する。

4.5　当社の業務目的で電子メールを送受信するために、あなた自身の個人的な電子メールアカウントを使用してはならない。提供された電子メールアカウントのみを使用しなければならない。

4.6　[追加のセキュリティリスクのため、Gmail や Hotmail などの Web ベースの個人用電子メールへのアクセスをコンピューターシステムでいつでも許可していない。]

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、業務目的のみに付与されている。

5.2　違法、攻撃的、悪趣味、又は不道徳と見なされる可能性のある、Web ページにアクセスしたり、インターネットから画像や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。英国内で合法である Web コンテンツであっても、この禁止事項に該当する程度に悪趣味である可能性が存在する。原則として、（ページを表示することを意図しているかどうかにかかわらず）誰かがページのコンテンツに当惑する可能性がある場合、又は、当社のソフトウェアが、ページまたはファイルにアクセスしたという事実が公開された場合、問題となる可能性がある場合、当該表示が、この方針違反となる。

5.3　当社の裁量で、いくつかのウェブサイトをブロックしたり、アクセス制限したりすることがある。

6.　当社システムの個人使用

[個人メールのチェックなど、許されるものがある場合には、許可内容を記載]

7.　監視

7.1　当社のシステムは、電話、電子メール、ボイスメール、インターネット、その他の通信を監視することができる。業務上の理由から、また、雇用主としての当社の役割から、法的義務を遂行するために、電話及びコンピューターシステムを含む、当社のシステムの使用（個人的な使用を含む。）は、自動ソフトウェア又はその他の方法で、継続的に監視される場合がある。

7.2　当社は、以下の目的を含め、業務上の利益のために合理的に必要な場合、電子メールメッセージの内容を取得したり、インターネットの使用状況（アクセスしたページや行われた検索を含む。）を確認したりする権利を留保する（このリストは網羅的ではない。）。

(a)　電子メールシステムまたはインターネットの使用が合法であり、このポリシーに準拠しているかどうかを監視するため。

(b)　失われたメッセージを検索するため、又は、コンピューターの障害のために失われたメッセージを取得するため。

(c)　申し立てられた不正行為の調査を支援するため。

(d)　法的義務を遵守するため。

8.　当社システムの禁止される使用

8.1　当社の電話又は電子メールシステムの誤用、過度の個人的使用、若しくは、不適切なインターネットの使用は、懲戒手続で対応する。インターネットの誤用は、場合によっては、犯罪となる可能性がある。

8.2　次の資料の作成、表示、アクセス、送信、又はダウンロードは、通常、重大な逸脱行為となる（このリストは網羅的ではない）。

(a)　ポルノ素材（つまり、性的に露骨または興奮する性質の文章、写真、映画、ビデオクリップ）；

(b)　攻撃的、わいせつ、又は犯罪的な内容、若しくは、当社又はクライアントに当惑を引き起こす可能性のある内容。

(c)　個人又は組織に関する、虚偽の名誉毀損の声明。

(d)　差別的、攻撃的、侮蔑的、又は他者を当惑させる可能性のある資料（機会均等ポリシー、ハラスメント防止、及びいじめに関するポリシーに違反する資料を含む。）。

(e)　当社、当社のスタッフ又はクライアントに関する機密情報（職務の適切な遂行において許可されている場合を除く。）。

(f)　許可されていないソフトウェア。

(g)（あなた又は当社にとって）刑事または民事責任を引き起こす可能性のあるその他の声明。

(h)　著作権を侵害する音楽、ビデオファイル又はその他の素材。

Schedule 4　ソーシャルメディア方針

1.　この方針について

1.1　このポリシーは、ソーシャルメディアの使用を通じて、当社のビジネスへのリスクを最小限に抑えるために実施されている。

1.2　このポリシーは、Facebook、LinkedIn、Twitter、Google+、Wikipedia [、Whisper] [、Instagram] [、Tumblr]、その他のすべてのソーシャルネットワーキングサイト、インターネット投稿、ブログなど、あらゆる形態のソーシャルメディアの使用を対象としている。これは、ビジネス目的でのソーシャルメディアの使用、及び当社のビジネスに何らかの影響を与える可能性のある個人的な使用に、適用される。

1.3　この方針は、従業員の雇用契約の一部を構成するものではなく、いつでも変更することができる。

2.　ソーシャルメディアの個人利用

2.1　[ソーシャルメディアの個人的な使用は、勤務時間中である場合、若しくは、当社のコンピューター、ネットワーク、その他の IT リソース、及び通信システムを使用する場合、許可されない。]

または

[勤務時間中のソーシャルメディアの時折の個人的な使用は、それが非専門的、又は不適切なコンテンツを含まず、あなたの職責又は生産性を妨げず、このポリシーに合致している限り、許可される。]

3.　禁止される使用

3.1　間接的であっても、当社のビジネス上の利益や評判を損なう可能性のある、ソーシャルメディアコミュニケーションを行わないようにしなければならない。

3.2　当社、当社のスタッフ又は第三者を、名誉毀損したり、誹謗中傷するため、スタッフや第三者に対して、嫌がらせ、いじめ、又は不法な差別をするため、虚偽または誤解を招く発言をするため、若しくは、同僚や第三者になりすますため、ソーシャルメディアを使用してはならない。

3.3　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を介して、当社に代わって意見を表明してはならない。そのような許可を取得するために、トレーニングを受ける必要がある。

3.4　当社の業績など、ビジネスに関連する機密性あるトピックについて、コメントを投稿したり、営業秘密、機密情報、知的財産を危険にさらすような行為を行ったりしてはならない。ソーシャルメディアへの投稿や、ソーシャルメディアのプロフィールに、当社のロゴやその他の商標を含めてはならない。

3.5　[雇用の過程で作成されたビジネス上の連絡先を、個人のソーシャルネットワーキングアカウントに追加することは、許されない。]

または

[あなたの雇用の過程で取得されたビジネス上の取引先の連絡先の詳細は、当社の機密情報にあたる。雇用終了時に、あなたは、そのようなすべての情報のコピーを、当社に提供し、あなたの個人的なソーシャルネットワーキングアカウントから、そのようなすべての情報を削除し、あなたが持っているかもしれない、そのような情報のさらなるコピーを破棄しなければならない。]

3.6　ソーシャルメディアの誤用は、[　　]に報告しなければならない。

4.　ソーシャルメディアの合理的な使用のためのガイドライン

4.1　ソーシャルメディアの投稿または個人のプロフィールで、自分個人について話していることを明確にする必要がある。一人称で書いて、個人のメールアドレスを使用することとする。

4.2　ソーシャルメディアで発言するときは、他者に敬意を払い、インターネット上で、誰でも見ることができるように公開されるすべてのコミュニケーションについて、あなたが個人的に責任を負うことに注意しなければならない。

4.3　あなたが、あなたのプロフィール、又はソーシャルメディアの投稿で、当社との関係を開示する場合、あなたは、あなたの見解が、あなたの雇用主の見解を表していないことを表明しなければならない（3.3 に規定のように、当社に代わって話すことを許可されていない限り。）。また、プロフィールと投稿するコンテンツが、クライアントや同僚に提示する、職業上のイメージと一致していることを確認する必要がある。

4.4　あなたの意見や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、上司と話し合うまで投稿を控えなければならない。

4.5　当社を誹謗中傷したり、当社を悪く提示するソーシャルメディアコンテンツを見つけた場合は、[あなたのマネージャーまたは[部門]]に連絡する必要がある。

5. 本方針の違反

5.1 本方針の違反は、解雇を含む懲戒処分となりうる。[本方針の違反をしていると疑われるスタッフの者は、当社の調査に協力する必要がある。]

5.2 本方針に違反すると考えられるソーシャルメディアの内容を取り除くように求められることがある。除去の要求への不服従は、懲戒処分の対象になることがある。

2　従業員との秘密保持契約書の例

Confidentiality Clause in Employment Agreement

11. Confidential Information

11.1 The Confidential Information means all confidential information relating to Employer [and its Group Company] that Employee obtain knowledge of, during the exercise of, or in connection with, Employee's duties owed to Employer [or its Group Company][, before, on or after the date of this agreement]. This includes:

(a) all confidential or proprietary information relating to:

(i) the research and development plan, the business operation, the labor and employment, the marketing and advertising, the finance, submitted or received documents from regulatory authorities and other business partners, the past, present, and potential customers and clients, the affairs with customers and business affiliates [, OR or] plans and prospects[, intentions, or market opportunities] of Employer [or of the Employer's Group Company] that are not publicly known and not readily ascertainable by someone in the same or similar business circle; and

(ii) (the operations, processes, product information, know-how, technical information, designs, trade secrets, or software of Employer[, or of Employer's Group Company] that are indicated as proprietary information by Employer or its representative or its Group Company;

(b) any information, findings, data or analysis derived from the Confidential Information; [and]

(c) any other information that is identified by Employer or its Representatives [or its Group Company, or their Representatives] as being of a confidential or proprietary nature[; and OR .]

(d) [any information detailed in Exhibit A]

but excludes any information referred to in clause 11.2.

11.2 Information is not the **Confidential Information** if:

(a) it is, or becomes, generally available to the public other than as a direct or indirect result of the information being disclosed by Employee or its Representatives in breach of this agreement [(except that any compilation of otherwise public information in a form not publicly known shall still be treated as the 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 person who, to Employee's knowledge, is not under any confidentiality obligation in respect of that information;

(d) it was lawfully in the possession of Employee before the information was disclosed 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.

12. Confidential Obligations

12.1 Either during this agreement or at any time during [number] years after the termination of this agreement Employee shall:

(a) keep the Confidential Information secret and confidential;

(b) use the Confidential Information only during the exercise of Employee's duties owed to Employer;

(c) maintain the label and classification of the Confidential Information as confidential in a manner that anyone who is exposed to the Confidential Information can understand the confidentiality of the Confidential Information all the time;

(d) protect the Confidential Information with necessary care so that no one can misuse or access to the Confidential Information without authorization;

(e) take security measures as set forth in Exhibit B;

(f) not 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 as expressly permitted by, and only necessary to perform Employee's duties, in accordance with this agreement;

(g) not copy, reduce to writing or otherwise record the Confidential Information except as strictly necessary for the performance of Employee's duties. Any such copies, reductions to writing and records shall be the property of Employer[; and OR .];

(h) not convey, disclose, or implicitly provide information about Employer's products and services and Employee's work in a lecture or a publication without obtaining a prior authorization 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 any other unauthorized use by any person including Permitted Disclosure and Mandatory Disclosure;

(j) not obtain or attempt to obtain intellectual property rights on the Confidential Information

(k) [[INCLUDE ANY OTHER SPECIFIC REQUIREMENTS.]]

13. Permitted Disclosure

13.1 Employee may disclose the Confidential Information to its Representatives on the basis that it:

(a) informs Employer's business affiliates, employees, and customers, of the confidential nature of the Confidential Information before it is disclosed; and

(b) procures that those persons or entities comply with the confidentiality obligations in clause 12.1

14. Mandatory Disclosure

14.1 Subject to the provisions of this clause, Employee may disclose the Confidential Information to the minimum extent required by:

(a) an order of any court of competent jurisdiction or any regulatory, judicial, governmental or similar body or any taxation authority of competent jurisdiction;

(b) the laws or regulations of any country to which Employer [or its Group Company] is subject.

14.2 Before Employee discloses any Confidential Information pursuant to clause 14.1 Employee shall, to the extent permitted by law, use all reasonable endeavours to give Employer as much notice of this disclosure as possible.

15. Return or destruction of the Confidential Information

15.1 (1) Upon completion or termination of the employment, or (2) upon Employer's request at any time in writing to Employee, Employee shall:

(a) return to Employer all documents, data, and materials [and any copies thereof] containing, reflecting, incorporating or based on Employer's Confidential Information;

(b) return to Employer all documents, devices, data, and materials [and any copies thereof] which relate to Employer or its Group Company including notes, reports, memos, records, files, drawings, protocols, and other similar documents;

(c) certify in writing to Employer that items listed in 5.1.(b) are the sole property of Employer and its Group Company and that Employee has complied with the requirements of this clause 15.1.

16. Reservation of rights and acknowledgment

16.1 Except as expressly stated in this agreement, Employer makes any express or implied warranty or representation concerning its Confidential Information, including but not limited to the accuracy or completeness of the Confidential Information.

16.2 The disclosure of the Confidential Information by Employer shall not form any offer by, or representation or warranty on the part of, Employer to enter into any further agreement with Employee.

17. Rights and remedies

17.1 Except as expressly provided in this agreement, the rights and remedies provided under this agreement are in addition to, and not exclusive of, any rights or remedies provided by law.

17.2 [Without prejudice to any other rights or remedies that each party may have, each party acknowledges and agrees that damages alone would not be an adequate remedy for any breach of the terms of this agreement by the other party. Accordingly, each party shall be entitled to the remedies of injunctions, specific performance or other equitable relief for any threatened or actual breach of this agreement.]

Exhibit A Designated Confidential Information

Exhibit B Minimum Security Measures

1. Protection and non-sharing of an ID, a badge, a key, a password, or any other form of authentication information that allows a holder's access to Employer's premises or log in to a device or equipment that may display or provide access to Confidential Information.
2. Locking of a device or equipment that may display or provide access to Confidential Information.
3. Limitation of printing on paper or other tangible medium for display, sharing, conveyance, retention, recording, saving, or any other types of use of Confidential Information
4. Prohibition of transferring, storing, saving, copying, recording, photographing, and duplicating of Confidential Information except authorized by Employer
5. Prohibition of a device and/or a means that possesses the functionality of copying, photographing, recording, transmitting, sharing, conveying, saving, or storing Confidential Information in premises and buildings where Employee uses or affords access to Confidential Information
6. Prohibition of use of Employee's own device and equipment for accessing or using Confidential Information
7. . . .

(参考和訳)従業員との秘密保持契約書の例

英国：雇用契約中の機密保持条項

1. 機密情報

1.1 機密情報とは、従業員が、自己の雇用主［及びそのグループ会社］に対して負う職責を遂行する間に、又は、遂行に関連して、［本合意の締結前、締結日、あるいは締結以降］知ることとなった、雇用主［及びそのグループ会社］に関する機密性ある情報を意味する。これには、以下を含む。:

a. 下記に関連するすべての機密情報、あるいは、保有情報:

(i) 公に知られておらず、同じか類似の業界の者が、容易に確認できない、雇用主[、又は雇用主のグループ会社]の、研究・開発計画、事業運営、労働及び雇用、マーケティング及び広告、財務、規制当局並びにその他のビジネスパートナーに提出された、若しくは受領した文書、過去、現在並びに将来の顧客及び取引相手、顧客並びに事業関連会社との関係[、又は]計画、及び、見通し[、意図、若しくは、市場機会];

(ii) (雇用主、その代表者、又は、そのグループ会社によって保有情報として示される、雇用主[、又は、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);

b. 機密情報に由来する情報、発見、データ、又は、解析;［及び］

c. 雇用主[、その代表者、又は、そのグループ会社]によって、それが秘密で所有されることを指定された、その他の情報[; または]

d. ［Exhibit A に記載の情報］

が、次項1.2.に言及された情報を除く。

1.2 次の情報は、機密情報にあたらない:

a. ［(公知の情報の、公に知られていない形態への編集が、機密情報として扱われるべきことを除き。)］、従業員、又は、その代理人が、この合意に反して開示したことの、直接、あるいは、間接の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;

b. 雇用主から開示されるより前に、従業員が、機密保持義務なく入手可能であった;

c. 従業員が知る限り、当該情報について機密保持義務を負わない人物から、従業員が、機密保持義務なく、入手が可能となった、可能である、又は、可能となる;

d. 雇用主から開示される前に、従業員に合法に所持されていた；[又は]

e. [雇用主から開示された情報と独立して、従業員により、又は、従業員のために開発された；又は]

f. 当事者が、書面で、情報が機密情報ではないと合意した.

2. 機密保持義務

2.1 本契約中、又は、本契約の終了後[ ]年間、如何なる時点でも、従業員は:

a. 機密情報を秘密にして機密性を保持する；

b. 雇用主に対して負う職責を遂行する間にのみ、機密情報を使用する；

c. 機密情報に接する者が、機密情報の機密性を常に理解できるように、機密情報のラベル及び分類を、機密として維持する；

d. 誰も、機密情報を権限なく不正使用、又は、違法にアクセスできないように、必要な注意をもって、機密情報を保護する；

e. Exhibit B に指定のセキュリティ対策を実施する；

f. 本契約に従い、従業員の職責を遂行するのに必要な限度で、かつ、明示的に許可を得ている場合を除き、いずれの者に対しても、直接又は間接に、機密情報の全部又はその一部を、開示、利用可能化、又は、開示若しくは利用可能化の試みを行わない；

g. 従業員の職責を遂行するのに厳密に必要な場合以外、機密情報のコピー、文書化、あるいは記録化を行わない。作成されたコピー、文書、及び、記録は、いずれも雇用主の財産となる[；そして]；

h. 事前に雇用主から許可を得ることなく、講義や発表にて、雇用主の製品やサービス、及び、従業員の仕事に係る情報を、伝播、開示、又は、暗黙の提供を行わない；

i. (1) 現実の、又は、差し迫った、従業員による疑われる機密保持義務違反, (2) 許される開示及び強制的開示を含む、現実の、又は、差し迫った、何者かによる開示、安全性の侵害、不正使用、侵害、又は、その他の無許可の使用について、雇用主に直ぐに通知する；

j. 機密情報に関して、知的財産権を取得ないしは得ようとしない

k. [[その他の必要事項を含める]]

3. 許される開示

3.1 従業員は、以下の条件で、自己の代理人に対して、機密情報を開示することができる:

a. 機密情報が開示される前に、雇用主の関連会社、従業員及び顧客に、機密情報の機密性を通知

b. それらの個人又は団体が、2.1の機密保持義務を遵守することの取り付け

4. 強制的開示

4.1 本条項の規定するところにより、従業員は、要求された最小限度で、機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、規制庁、司法機関、行政庁若しくは他の同様の機関、又は管轄権を有する税務当局の命令;

b. 雇用主[、又はそのグループ会社]が服する法律、又は規制

4.2 4.1項に従い、従業員が機密情報を開示する前に、従業員は、法律で許される限度で、雇用主に、当該開示に関してできるだけ通知するよう、合理的な努力をしなければならない。

5. 機密情報の返還、又は、消去

5.1 (1) 雇用の完了、若しくは、終了に際して、 又は、(2)何時でも、雇用主の、書面による従業員への要請により、従業員は:

a. 雇用主の機密情報を含んだ、反映した、取り込んだ、あるいは、基礎とする、全ての書面、データ、資料[、及び、それらのコピー]を、雇用主に返還することとする;

b. 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を含む、雇用主、又は、そのグループ会社に関連する、すべての文書、装置、データ、並びに、資料[、及び、それらのコピー]を、雇用主に返却する;

c. 従業員は、5.1.b の項目が、雇用主とそのグループ会社のみの財産であり、従業員が 5.1.の要件を充足したことを、雇用主に書面で確証する

6. 権利の保留及び確認

6.1 本合意で明示に規定されている場合を除き、雇用主は、機密情報の正確性、あるいは完全性に限られないが、それを含めて、機密情報に関する明示、若しくは、黙示の保証、又は、表明を行わない。

6.2 雇用主の機密情報の開示は、従業員とのさらなる合意を締結する、雇用主による申出、又は、雇用主の表明、若しくは、保証を構成しない。

7. 権利と救済

7.1 本合意で明示的に規定されている場合を除き、本合意に基づいて付与される権利、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 [各当事者が持つ可能性のある、他の権利又は救済を妨げることなく、各当事者は、損害賠償だけでは、他の当事者による本合意内容の違反に対する適切な救済ではないことを認め、同意する。したがって、各当事者は、恐れのある、若しくは、現実の違反に対する差止命令、特定義務の履行、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　　指定機密情報

Exhibit B　　最小安全性措置

1. その保有者が、雇用主の施設にアクセスしたり、機密情報を表示、若しくは、アクセスすることのできる装置や機器に、ログインしたりすることを許す、ID、バッジ、キー、パスワード、又は、その他の形式の認証情報の、保護と非共有。
2. 機密情報を表示、又は、それにアクセスを付与する、装置、若しくは、機器の施錠・暗号化。
3. 機密情報の展示、共有、移転、保持、記録、保存、又は、その他の種類の使用のために利用される、紙やその他の有体媒体への印刷の制限。
4. 雇用主の許可がない限り、機密情報の転送、貯蔵、保存、コピー、記録、写真撮影、及び、複製の禁止。
5. 従業員が、機密情報を使用、若しくは、アクセスできる、施設、並びに建物での、機密情報のコピー、写真撮影、記録、送信、共有、伝達、保存、又は、貯蔵の機能を備えた装置、及び/又は、手段の禁止
6. 機密情報にアクセスする、又は使用するために、従業員個人の装置又は機器を使用することの禁止
7. . . .

3 退職後の競業避止契約書の例

UK Employee Non-compete Agreement

1. Interpretation

The definitions and rules of interpretation in this clause apply in this agreement.

a. **Board**: the board of directors of the Company (including any committee of the board duly appointed by it).
b. **Capacity**: as 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) which is not in the public domain relating to [our **OR** any Group Company's] business, products, affairs and finances for the time being 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 (by way of illustration only and without limitation) [EXAMPLES].
d. **Garden Leave**: any period during which we have [exercised our rights under clause [NUMBER] **OR** required you not to do any work or contact 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 from time to time.]
f. **Restricted Business**: those parts of [our **OR** any Group Company's] business with which you were involved to a material extent in the [PERIOD] months before Termination.
g. **Restricted Customer**: any firm, company or person who, during the [PERIOD] months before Termination, was [a customer or prospective customer of **OR** in the habit of dealing with] [the Company **OR** any Group Company] with whom you had contact [or about whom you became aware or 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 concern which competes with any Restricted Business] and with whom you dealt in the [PERIOD] months before Termination in the course of your employment.
i. **[Subsidiary and Holding Company**: in relation to a company mean "subsidiary" and "holding company" as defined in section 1159 of the Companies Act 2006 [and a company shall be treated, for the purposes only of the membership requirement contained in subsections 1159(1)(b) and (c), 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 termination of your employment with us howsoever 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 the your employment by 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 by us and for [PERIOD] months after Termination, solicit or endeavour to entice away from [us **OR** any Group Company] the business or custom of a Restricted Customer with a view to providing goods or services to that Restricted Customer in competition with any Restricted Business;

b. [during your employment by us and for [PERIOD] months after Termination [in the course of any business concern which is in competition with any Restricted Business], offer to employ or engage or otherwise endeavour to entice away from [us **OR** any Group Company] any Restricted Person;]

c. [during your employment by us and for [PERIOD] months after 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 by us and for [PERIOD] months after Termination, be involved in any Capacity with any business concern which is (or intends to be) in competition with any Restricted Business;

e. for [PERIOD] months after Termination, be involved with the provision of goods or services to (or otherwise have any 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 after Termination, represent yourself as 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 by us,

(i) disclose or use, or attempt to disclose or use, Confidential Information or trade secrets that you have access to, without written authorization, or allow directly or indirectly, an unauthorized third party to obtain or use Confidential Information or trade secrets;

(ii) pursue or attempt to pursue economic or social interest of any business concern other than us; or

h. during your employment by us, without written authorization,

(i) provide goods or services of, or carry out business activities (including consultation, financing, management, operation, and marketing) of, or engage in preparatory activities for the launch of,

(ii) assume a Capacity in,

(iii) assist employing or engaging an employee by, or

(iv) represent yourself as holding any Capacity in, or as connected with,

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 not more than [5]% of the total issued share capital of any company, whether or not it is listed or dealt in on a recognised stock exchange; [or]
b. being engaged or concerned in any business concern insofar as your duties or work shall relate solely to geographical areas where the business concern is not in competition with any Restricted Business[; or **OR** .]
c. [being engaged or concerned in any business concern, provided that your duties or work shall relate solely to services or activities of a kind with which you were not concerned to a material extent in the [PERIOD] months before 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 before Termination.

2.5 If, during the your employment by 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 which competes with any part or parts of [our OR any Group Company's] business with which you are or have been involved to a material extent during the your employment by 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 the approach or offer as soon as possible; [and]
b. [if requested, provide a copy of any written offer as soon as possible; and]
c. give the person making the offer a copy of this clause 2 within [seven days] of the offer being made.

The obligations contained in this clause 2.5 are continuing obligations and shall also apply if, at any time subsequent to the relevant approach or offer being made but before the expiry of the last of the covenants in this clause 2, the business making the offer or approach so competes with [our OR any Group Company's] business.

2.6 [If, at any time during your employment, [two] or more Restricted Persons have left their employment, appointment or engagement with us to carry out services for a business concern which competes with, or is intended to compete with any Restricted Business, you will not at any time 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 way with that business concern.]

2.7 The parties entered into the restrictions in this clause 2 having been separately legally advised.

2.8 Each of the restrictions in this clause 2 is intended to be separate and severable. If any of the restrictions shall be held to be void but would be valid if part of their wording were deleted, such restriction shall apply with such deletion as may be necessary to make it valid or effective.

2.9 If your employment is transferred to any firm, company, person or entity other than a Group Company (the "New Employer") pursuant to the Transfer of Undertakings (Protection of Employment) Regulations 2006, you will, if required, enter into an agreement with the New Employer containing post-termination restrictions corresponding to those restrictions in this clause 2, protecting the [confidential information], trade secrets and business connections of the New Employer.

2.10 [You will, 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 restrictions 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

従業員の競業避止条項

1. 解釈

本条項における定義と解釈の規則は、本契約に適用される。

a. **取締役会**：当社の取締役会（正式に任命された、取締役会の委員会を含む。）。

b. **地位**：エージェント、コンサルタント、ディレクター、従業員、労働者、所有者、パートナー、又は株主として。

c. **機密情報**：[当社又はグループ会社の]事業、製品、商務及び財務に関連する、パブリックドメインにない情報（文書形式で記録されているかどうか、及び、磁気又は光学ディスク、若しくは、メモリに保存されているかどうかにかかわらず。）で、[当社又はグループ会社に、]期間中機密であるもの、並びに、営業秘密（[当社又はグループ会社]の事業に関連する技術データ及びノウハウ、若しくは、当社の[その]事業の連絡先を含むがこれらに限定されない。）、特に（説明のためのみで、制限されない。）[例]。

d. **ガーデンリーブ**：当社が、[第[数字]条に基づいて権利を行使した、若しくは、就労、又は、当社の従業員やビジネスの連絡先との連絡をやめるよう要求した]、期間。

e. [**グループ会社**：会社、その子会社、又は持ち株会社、及び、持ち株会社の子会社。]

f. **制限ビジネス：**退職前の[期間]ヶ月間に重要な範囲で関与した[当社又はグループ会社の]ビジネスの部分。

g. **制限顧客：**解雇前の[期間]ヶ月間に、[当社又はグループ会社][の顧客又は潜在的顧客であった、又は、と取引慣行にあった]、貴殿が、貴殿の雇用の過程で、コンタクトを取った、[若しくは、貴殿が知るようになった、又は、知らされた]事業所、会社、又は、個人。

h. **制限対象者：**[当社又はグループ会社]によって[[地位]以上のレベルで雇用[又は従事]され、制限ビジネスと競合する事業主に、いかなる役割であっても関与する場合には、[当社又はグループ会社]の利益に重大な損害を与える可能性のあり]、かつ、貴殿が、雇用の過程で、退職の[期間]ヶ月内にやりとりした者。

i. **[子会社及び持ち株会社：**会社に関連して、2006 年会社法の第 1159 条で定義されている、「子会社」および「持ち株会社」を意味する。[そして、会社は、第 1159 条第(1)(b)及び(c)に含まれる、メンバーシップ要件の目的でのみ、他の会社のメンバーとして扱われる。それは、他の会社の株式が(a)証券によるか、又は、証券を獲得することに関連してかにかかわらず、他者（又はその被指名人）の名前で、若しくは、(b)被指名人の名前で、登録されている場合でも当てはまる。]

j. **退職：**いかなる原因であれ、当社と貴殿との間の雇用の終了。

2. 制約

2.1 雇用の結果として貴殿がアクセスできる機密情報及び[当社又はグループ会社の]ビジネス上のつながりを保護するために、以下の行為に及ばないことを、当社に合意する[（当社自身のため、各グループ会社の受託者及び代理人として）]:

a. 退職後[期間]の期間、制限ビジネスと競合する商品又はサービスを提供する目的で、制限顧客を勧誘をして、[当社又はグループ会社]から、制限顧客のビジネス又は取引慣行を、奪い取る、又は、奪い取るように努めること。

b. [退職後[期間]の期間 、[制限ビジネスと競合する事業主の関連で]、制限対象者を雇用又は採用するか、その他の方法で、[当社又はグループ会社]から、引き抜こうと努めること。]

c. [退職後[期間] 、[制限ビジネスと競合する事業主の関連で]、制限対象者が、雇用又は採用されることで、契約違反となるかどうかにかかわらず、制限対象者を雇用又は採用するか、若しくは、雇用又は採用を援助すること。

d. 退職後から[期間]ヶ月間、制限ビジネスと競合している（又は競合する予定の）事業主で、地位に就くこと。

e. 退職後[期間]の期間、制限ビジネスと競合する事業主の関連で、制限顧客への商品又はサービスの提供に関与する（、若しくは、その他の方法で、ビジネスを行う）こと。

f. 退職後いつでも、元従業員以外の何らかの地位で、[当社又はグループ会社と]関係があることを表明するか、[当社又はグループ会社]に関連する登録名称又は商号を使用すること。

g. 雇用中、

(i) 貴殿がアクセスできる機密情報又は営業秘密を、当社の書面による許可なく、開示又は使用、若しくは、開示又は使用の試みをする、あるいは、直接又は間接に、当社により許可を受けていない第三者が、機密情報又は営業秘密を取得あるいは使用できるようにすること、

(ii) 当社以外の事業主の経済的又は社会的利益を追求する、若しくは、追求しようとすること。

h. 雇用中、当社の書面による許可なく、当社以外の他の事業主の、

(i) 商品又はサービスの提供に関与する、若しくは、そのビジネス活動（顧問、ファイナンス、経営、運営、及び、販売促進を含む）又は開業準備を行うこと、

(ii)地位に就くこと、

(iii)従業員の雇用又は採用を援助すること、

(iv)地位に就いている、又は、関係があると表明すること。

2.2　前項 2.1 の制限は、以下を妨げない。

a.　公認の証券取引所に上場又は取引されているかどうかにかかわらず、会社の発行済み株式資本合計の[5]%以下の株式又はその他の証券による投資を保有すること。

b.　職責又は仕事が、制限ビジネス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する、あるいは、関与する[;又は]

c.　[貴殿の義務又は仕事が、終了前の[期間]月間に重要な範囲で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、事業主の事業に従事する、又は関与すること。]

2.3　第 2 条による制限は、貴殿の下記行動に適用される：

a.　直接的、又は、間接的;

b.　貴殿個人、事業所、会社、又は、他者のために、若しくは、それらと連携して

2.4　前 2.1 項の制限が適用される期間は、退職直前にガーデンリーブに服した間だけ、短縮される。

2.5　雇用中、又は、第 2 条の規定の各制約が最後に満了する前に、貴殿が雇用中に重要な範囲で関与している、又は関与したことがある、[当社又はグループ会社の]事業の一部又は複数の部分と競合する、事業の地位に貴殿が就くかという、接触又は申出を受け取った場合、以下をしなければならない:

a.　[当社又は取締役会]に、[書面で]、接触又は申出の事実と、接触又は申出を行った者の身元を、できるだけ直ぐに通知する。

b.　[要求に応じて、書面による申出のコピーを、できるだけ直ぐに提供する。]

c.　申出をした者に、申出が行われてから[7 日]以内に、この第 2 条のコピーを渡す。

第 2.5 項に含まれる義務は、継続的な義務であり、関連する接触又は申出が行われた後で、第 2 条の各制約が最後に満了する前に、申出又は接触を行う事業主が、 [当社又はグループ会社]の事業と競合する場合に、適用される。

2.6　[貴殿の雇用中の任意の時点で、[2]人以上の制限対象者が、制限ビジネスと競合する、又は競合することを企図する事業主の、サービス実現のために、雇用される、任命される、又は、採用を離れる場合、これら制限対象者のいずれかが、当社によって雇用又は採用された最後の日から 6 か月間、貴殿は、その事業主に、何らかの形で雇用される、若しくは、従事してはならない。]

2.7　両当事者は、独立した法的助言を受けた上で、第 2 条の制限に合意した。

2.8　第 2 条の各制限は、別個で、分離できることを意図している。制限のいずれかが無効とみなされても、それらの文言の一部が削除されると有効である場合、当該制限は、それを有効化する、又は、効力をもたせる必要な削除とともに適用される。

2.9　2006 年事業譲渡（雇用の保護）規則に従って、グループ会社以外の事業所、会社、個人、又は団体（「新規雇用主」という。）に雇用が譲渡された場合、[機密情報]、営業秘密、及び、新規雇用主のビジネス上のつながりを保護するため、第 2 条の制限に対応する退職後の制限を含め、必要に応じて、新規雇用主と合意する。

2.10　[当社の求めに応じて、当社の費用で、グループ会社に対して、別個に、この第 2 条の規定する制限に対応した制限（又は、その中で適切と考えられるな制限）に拘束されることに同意する。]

4 取引先との秘密保持契約書の例

Confidentiality Clause in Transactional Agreements

18. Confidential Information

18.1 The Confidential Information means all confidential information relating to the Purpose which Discloser or its Representatives [or its Group Company, or their Representatives] directly or indirectly provides to Recipient or its Representatives [or its Group Company, or their Representatives][, 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) the research and development, the business operations, the finance, the past, present, and potential customers and clients, the affairs with customers and business affiliates[, OR] plans[, intentions, or market opportunities] of Discloser [or of Discloser's Group Company] that are not publicly known and not readily ascertainable by someone in the same or similar business circle; and

(ii) (the operations, processes, product information, know-how, technical information, designs, trade secrets or software of Discloser[, or of Discloser's Group Company] that are indicated as proprietary information by Discloser or its representative or its Group Company;

(d) any information, findings, data or analysis derived from the Confidential Information; [and]

(e) any other information that is identified by Discloser or its Representatives [or its Group Company, or their Representatives] as being of a confidential or proprietary nature[; and OR .]

(f) [any information detailed in Exhibit A]

but excludes any information referred to in clause 11.2.

18.2 Information is not the **Confidential Information** if:

(a) it is, or becomes, generally available to the public other than as a direct or indirect result of the information being disclosed by Recipient or its Representatives in breach of this agreement [(except that any compilation of otherwise public information in a form not publicly known shall still be treated as the 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 person who, to Recipient's knowledge, is not under any confidentiality obligation in respect of that information;

(d) it was lawfully in the possession of Recipient before the information was disclosed 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.

19. Confidential Obligations

19.1 In return for Discloser making the Confidential Information available to Recipient, Recipient undertakes to Discloser that it shall:

(a) keep the Confidential Information secret and confidential;

(b) not use the Confidential Information except when it is necessary to realize the Purpose;

(c) label and classify the Confidential Information as confidential in a manner that anyone who is exposed to the Confidential Information can understand the confidentiality of the Confidential Information all the time;

(d) protect the Confidential Information with necessary care so that no one can misuse or access to the Confidential Information without authorization;

(e) take security measures as set forth in Exhibit B;

(f) not 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 as expressly permitted by, and only necessary to realize the Purpose, in accordance with this agreement;

(g) obtain a valid confidentiality agreement in writing from any employee, officer, expert, business affiliate, and person who are expected to receive or be exposed to the Confidential Information and legally bind such employee, officer, expert, business affiliate, and person with duty of confidentiality identical to Recipient’s duty of confidentiality under this agreement;

(h) obtain written consent from Discloser to any contractual or statutory transfer of Recipient’s contractual rights and/or duties under this agreement, prior to transfer of such rights and/or duties;

(i) not copy, reduce to writing or otherwise record the Confidential Information except as strictly necessary for the Purpose. Any such copies, reductions to writing and records shall be the property of Discloser[; and OR .];

(j) immediately notify Discloser of (1) any suspected actual or imminent breach of confidentiality by Recipient or its employee, officer, expert, business affiliate, and other person who are expected to receive or be exposed to the Confidential Information, (2) any actual or imminent disclosure, security breach, misuse, misappropriation, or any other unauthorized use by any person including Permitted Disclosure and Mandatory Disclosure;

(k) not obtain or attempt to obtain intellectual property rights on the Confidential Information

(l) [[INCLUDE ANY OTHER SPECIFIC REQUIREMENTS.]]

20. Permitted Disclosure

20.1 Recipient may disclose the Confidential Information to its Representatives on the basis that it:

(a) informs those Representatives of the confidential nature of the Confidential Information before it is disclosed; and

(b) procures that those Representatives comply with the confidentiality obligations in clause 12.1 as if they were Recipient.

20.2 Recipient shall be liable for the actions or omissions of the Representatives in relation to the Confidential Information as if they were the actions or omissions of Recipient.

21. Mandatory Disclosure

21.1 Subject to the provisions of this clause, a party may disclose the Confidential Information to the minimum extent required by:

(a) an order of any court of competent jurisdiction or any regulatory, judicial, governmental or similar body or any taxation authority 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) the laws or regulations of any country to which its affairs [or those of its Group Company] are subject.

21.2 Before a party discloses any Confidential Information pursuant to clause 14.1 it shall, to the extent permitted by law, use all reasonable endeavours to give the other party as much notice of this disclosure as possible. [Where notice of such disclosure is not prohibited and is given in accordance with clause 14.2, that party shall take into account the reasonable requests of the other party in relation to the content of this disclosure.]

21.3 If a party is unable to inform the other party before the Confidential Information is disclosed pursuant to clause 14.1 it shall, to the extent permitted by law, inform the other party of the full

circumstances of the disclosure and the information that has been disclosed as soon as reasonably practicable after such disclosure has been made.

22. Return or destruction of the Confidential Information

22.1 (1) Upon completion or termination of the Purpose and (2) upon Discloser's request at any time in writing to Recipient, Recipient shall:

(a) destroy [or return to Discloser] all documents and materials [(and any copies)] containing, reflecting, incorporating or based on Discloser's Confidential Information;

(b) erase all Discloser's Confidential Information from its computer and communications systems and devices used by it, or which is stored in electronic form; [and]

(c) [[to the extent technically and legally practicable,] erase all Discloser's Confidential Information which is 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 15.1.

22.2 Nothing in clause 15.1 shall require Recipient to return or destroy any documents and materials containing or based on Discloser's Confidential Information that Recipient is required to retain by applicable law, or to satisfy the requirements of a regulatory authority or body of competent jurisdiction or 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 documents and materials retained by Recipient pursuant to this clause 22.2.

23. Reservation of rights and acknowledgment

23.1 The disclosure of the Confidential Information by one party does not give the other party or any other person any licence or other right in respect of any Confidential Information beyond the rights expressly set out in this agreement.

23.2 Except as expressly stated in this agreement, Discloser makes any express or implied warranty or representation concerning its Confidential Information, including but not limited to the accuracy or completeness of the Confidential Information.

23.3 The disclosure of the Confidential Information by the parties shall not form any offer by, or representation or warranty on the part of, that party to enter into any further agreement with the other party [in relation to the Purpose].

24. Rights and remedies

24.1 Except as expressly provided in this agreement, the rights and remedies provided under this agreement are in addition to, and not exclusive of, any rights or remedies provided by law.

24.2 [Without prejudice to any other rights or remedies that each party may have, each party acknowledges and agrees that damages alone would not be an adequate remedy for any breach of the terms of this agreement by the other party. Accordingly, each party shall be entitled to the remedies of injunctions, specific performance or other equitable relief for any threatened or actual breach of this agreement.]

25. No obligation to continue discussions

Nothing in this agreement shall impose an obligation on either party to continue discussions or negotiations in connection with the Purpose, or an obligation on each party[, or its Group Company] to disclose any information (whether the Confidential Information or otherwise) to the other party.

26. Ending Discussions and duration of confidentiality obligations

26.1 If either party decides not to continue to be involved in the Purpose with the other party, it shall notify that other party in writing immediately.

26.2 Notwithstanding the end of discussions between the parties in relation to the Purpose pursuant to clause 26.1, each party's obligations under this agreement shall continue in full force and effect for a period of [two] years from the date of this agreement.

26.3 The end of discussions relating to the Purpose shall not affect any accrued rights or remedies to which either party is entitled.

Exhibit A Designated Confidential Information

Exhibit B Minimum Security Measures

8. Password requirement for logging into a device that may display or provide access to Confidential Information to a user of the device.
9. Limitation of printing on paper or other tangible medium for display, sharing, conveyance, retention, recording, saving, or any other types of use of Confidential Information
10. Limitation of access to premises and buildings where Recipient uses or affords access to Confidential Information to only those who owe duty of confidentiality to Recipient
11. Prohibition of a device and/or a means that possesses the functionality of copying, photographing, recording, transmitting, sharing, conveying, saving, or storing Confidential Information in premises and buildings where Recipient uses or affords access to Confidential Information
12. . . .

(参考和訳)取引先との秘密保持契約書の例

英国：取引関係相手との機密保持条項

1. 機密情報

1.1 機密情報とは、開示者若しくはその代表者[又はそのグループ会社若しくはその代表者]が、受領者若しくはその代表者[又はそのグループ会社若しくはその代表者] に[本件契約前、締結時、又は締結以降]、直接又は間接的に提供する、すべての機密情報を意味する：

(a) 本件契約の話し合い及び交渉が、その目的と現況に関して、行われているという事実；

(b) [本件契約の[存在及び]条件;]

(c) 以下に関連するすべての機密情報、又は保有情報:

(i) 公に知られておらず、同じか類似の業界の何者かが、容易に確認できない、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、過去、現在、並びに、将来の顧客とクライアント、顧客並びにビジネスアフィリエイトとの関係[、又は]計画[、意図、又は市場機会];

(ii) 開示者、その代表者、又はそのグループ会社によって保有情報として示される、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;

(d) 機密情報に由来する情報、発見、データ、又は、解析;[そして]

(e) 開示者、その代表者[、そのグループ会社、又はその代表者]によって、それが機密であるか、保有されることが、指定された、その他の情報

[; そして]

(f) [Exhibit A に記載の情報]

が、次項 1.2. に言及された情報を除く。

1.2 次の情報は、機密情報にあたらない:

(a) [(公知の情報が公に知られていない形態への編集が機密情報として扱われるべきことを除き。)]、受領者、又は、その代理人が、この合意に反して開示したことの、直接、あるいは、間接の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;

(b) 開示者から開示されるより前に、受領者が、機密保持義務なく入手可能であった;

(c) 受領者が知る限り、当該情報について機密保持義務を負わない人物から、受領者が、機密保持義務なく、入手が可能となった、可能である、又は、可能となる;

(d) 開示者から開示される前に、受領者に合法に所持されていた;[又は]

(e) [開示者から開示された情報と独立して、受領者により、又は、受領者のために開発された; 又は]

(f) 当事者が、書面で、情報が機密情報ではないと合意した.

2. 機密保持義務

2.1 開示者が、機密情報を受領者が利用できるようにするのと引き換えに、受領者は、開示者に対して、以下を誓約する:

(a) 機密情報を秘密にして機密性を保持する;

(b) 目的を実現する必要がある場合を除き、機密情報を使用しない ;

(c) 機密情報に接する者が、機密情報の機密性を常に理解できるように、機密情報のラベル、及び、分類を、機密として維持する;

(d) 誰も、機密情報を権限なく不正使用、若しくは、違法にアクセスできないように、必要な注意をもって、機密情報を保護する ;

(e) 別紙 B に記載されているセキュリティ対策を講じる ;

(f) 本契約に従い、目的の実現に必要な限度で、かつ、明示の許可を得ている場合を除き、いずれの者に対しても、直接若しくは間接に、機密情報の全部若しくはその一部を、開示、利用可能化、又は、開示や利用可能化の試みを行わない ;

(g) 従業員、役員、専門家、ビジネスアフィリエイト、及び、機密情報を受信又は接することが予想される人物から、本契約に基づく受領者の機密保持義務と同一の機密保持義務をそのような人物に課す有効な機密保持契約を書面で取得する ;

(h) 本契約に基づく、受領者の契約上の権利及び/若しくは義務の、契約上又は法定の譲渡について、そのような権利及び/若しくは義務の譲渡の前に、開示者から書面による同意を得る ;

(i) 目的のために厳密に必要な場合を除き、機密情報をコピー、文書化、その他の記録化を行わない。作成されたコピー、文書、及び、記録は、いずれも開示者の財産となる[;そして] ;

(j) (1) 現実の、若しくは、差し迫った、受領者、その従業員、役員、専門家、ビジネスアフィリエイト、及び、機密情報を受け取るか、又は、機密情報に接することが予想されるその他の人物による、機密保持義務違反の疑い，(2) 許される開示、並びに、強制的開示を含む、現実の、若しくは、差し迫った、何者かによる開示、安全性の侵害、不正使用、侵害、又は、その他の無許可の使用について、開示者に直ちに通知する；

(k) 機密情報に関して、知的財産権を取得、ないしは、得ようとしない

(l) [[その他の必要事項を含める]]

3. 許される開示

3.1 受領者は、以下の条件で、自己の代理人に対して、機密情報を開示することができる:

1) 機密情報が開示される前に、それら代理人に、機密情報の機密性を通知
2) それらの代理人が、受領者のように、2.1 の機密保持義務を遵守することの取り付け

3.2 受領者は、機密情報に関連する、代理人の作為又は不作為について、あたかも受領者自身の作為又は不作為であるかのように、責任を負う。

4. 強制的開示

4.1 本条項の規定するところにより、当事者は、要求された最小限度で、機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、規制庁、司法機関、行政庁、若しくは、他の同様の機関、又は、管轄権を有する税務当局の命令;

(b) その株式（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；

(c) その業務（又はそのグループ会社の業務）が適用される国の法律又は規制

4.2 4.1 に従い、当事者が機密情報を開示する前に、法律で許される限度で、相手当事者に、当該開示に関してできるだけ通知するよう、合理的な努力をしなければならない。[そのような開示の通知が禁止されておらず、4.2 項に従って行われる場合、その当事者は、この開示の内容に関する相手当事者の合理的な要求を、考慮に入れる。]

4.3　4.1 項に従って機密情報が開示される前に、当事者が相手当事者に通知できない場合、法律で許可されている範囲で、その開示が行われた後、合理的に可能な限り直ぐに、開示の全状況及び開示された情報を、相手当事者に通知する。

5.　機密情報の返還、又は、消去

5.1　(1)目的の完了、若しくは、終了に際して、又は、(2)何時でも、開示者の、書面による受領者への要請により、受領者は:

(a)　開示者の機密情報を含んだ、反映した、取り込んだ、あるいは、基礎とする、全ての書面及び資料[、及び、それらのコピー]を、破棄[、又は、開示者に返還]することとする;

(b)　自己のコンピュータと通信システム、及び、自己が使用するデバイスに存在する、又は電子形式で保存されている、すべての開示者の機密情報を消去する ;

(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ストレージサービスに電子形式で保存されている、開示者の全機密情報を消去する ;

(d)　この条項 5.1 の要件に適合していることを、開示者に書面で確証する。

5.2　第 5.1 項のいかなる規定も、適用される法により、受領者が保持する必要がある、あるいは、規制当局又は管轄機関の要求、若しくは、対象となる上場当局又は証券取引所の規則を満たす必要のある、開示者の機密情報を含む、又は、それに基づく、文書及び資料を返却又は破棄することを、受領者に要求するものではない。本契約の規定は、本項 5.2 に従って受領者が保持する、すべての文書及び資料に、引き続き適用されるものとする。

6.　権利の保留及び確認

6.1　一方の当事者による機密情報の開示は、本契約で明示的に定められた権利を超えて、他方の当事者又は他者に、機密情報に関するライセンス又はその他の権利を与えるものではない。

6.2　本合意で明示に規定されている場合を除き、開示者は、機密情報の正確性又は完全性に限られないが、それを含めて、機密情報に関する、明示、若しくは、黙示の保証、又は、表明を行わない。

6.3　当事者の機密情報の開示は、[目的に関して、]相手当事者とのさらなる合意を締結する、当事者による申出、又は、当事者の表明、若しくは、保証を構成しない。

7. 権利及び救済

7.1 本合意で明示的に規定されている場合を除き、本合意に基づいて付与される権利、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 [各当事者が持つ可能性のある、他の権利又は救済を妨げることなく、各当事者は、損害賠償だけでは、他の当事者による本合意内容の違反に対する、適切な救済ではないことを認め、同意する。したがって、各当事者は、恐れのある、若しくは、現実の違反に対する差止命令、特定義務の履行、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. 話し合いを続ける義務の不存在

本契約のいかなる条項も、いずれかの当事者に、目的に関連して話し合い、若しくは、交渉を継続する義務を課すことはなく、各当事者[又はそのグループ会社]に情報（機密情報又はその他）を他方当事者に開示する義務を課すことはない。

9. 話合いの終了及び守秘義務の期間

9.1 いずれかの当事者が、他方の当事者との目的に関与し続けないと決めた場合、直ちに、書面で、他方当事者に通知するものとする。

9.2 9.1 項に基づく、目的に関した当事者間の話し合いの終了にもかかわらず、本契約に基づく各当事者の義務は、本契約の日付から[2]年間、完全に効力を持ち続ける。

9.3 目的に関した話し合いの終了は、いずれかの当事者が有する、未払いの権利又は救済に影響を与えない。

Exhibit A　　指定機密情報

Exhibit B　　最小安全性措置

1. ユーザーに、機密情報を表示、又は、機密情報へのアクセスを提供する可能性のある装置にログインするためのパスワードの要求。
2. 機密情報の展示、共有、移転、保持、記録、保存、又は、その他の種類の使用のために利用される、紙やその他の有体媒体への印刷の制限。
3. 受領者が機密情報を使用する、又は、機密情報へのアクセスを許可する、施設及び建物へのアクセスを、受領者に機密保持義務を負っている者のみに制限。
4. 受領者が、機密情報を使用、若しくは、機密情報へのアクセスを提供する、施設、並びに建物での、機密情報のコピー、写真撮影、記録、送信、共有、伝達、保存、又は、貯蔵の機能を備えた装置、及び/又は、手段の禁止
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	本人確認	連絡先	所属団体	到着日 時	出発日 時	受入対応者 （受入先）

報告書の利用についての注意・免責事項

本報告書は、日本貿易振興機構（ジェトロ）が現地調査会社に委託し作成したものであり、調査後の法律改正などによって情報が変わる場合があります。掲載した情報・コメントは調査委託先の判断によるものであり、情報の正確性や一般的な解釈がこのとおりであることを保証するものではありません。また、本報告書はあくまでも参考情報の提供を目的としており、法的助言を構成するものではなく、法的助言として依拠すべきものではありません。本報告書にてご提供する情報等に基づいて行為をされる場合には、必ず個別の事案に沿った具体的な法的助言を別途お求め下さい。

ジェトロおよび調査委託先は、本報告書の記載内容に関して生じた直接的、間接的、派生的、特別の、付随的、あるいは懲罰的な損害および利益の喪失について、それが契約、不法行為、無過失責任、あるいはその他の原因に基づき生じたかにかかわらず、一切の責任を負いません。これは、たとえジェトロまたは調査委託先が係る損害等の可能性を知らされていても同様とします。

[調査受託]

Brundidge & Stanger, P.C.

独立行政法人　日本貿易振興機構　ニューヨーク事務所

2022 年 3 月

禁無断転載

本報告書の作成においては、できるだけ正確な情報の提供を心がけておりますが、本報告書で提供している情報は、調査時点で入手・判明し得たものであり、ご利用に際してはこの点をご留意の上、ご活用ください。