

「秘密情報の保護ハンドブック」の改訂 (改訂方針と改訂内容一覧)

令和5年11月

経済産業省知的財産政策室

1. 「秘密情報の保護ハンドブック」の改訂方針

<改訂の基本方針>

- 直近改訂（令和4年5月）以降の社会経済情勢の変化・関係法令の進展等を踏まえて改訂を検討。
- 一方、啓発資料として産業界・関係団体に行き渡っていることから、構成・基本的内容については、現行版を踏襲しつつ、以下の観点を踏まえて、ハンドブックの内容を補強・追記する方針で改訂を進める。

□ 関連する「法制度の見直し・ガイドラインの改訂」に伴う修正

- ・ 直近改訂以降の進展、例えば、「法制度の見直し」に伴う修正として、令和5年の不競法改正で見直された①「限定提供データ」の保護範囲、②使用等の推定規定の拡充、③国際的な営業秘密侵害に係る手続等に関する記載を追加するほか、この間に発出された「各種ガイドライン」（例：「水産分野における優良系統の保護等に関するガイドライン」・「養殖業における営業秘密の保護ガイドライン」（水産庁））等を反映。

□ 営業秘密・秘密情報を取りまく「環境の変化」に伴う修正

- ・ AIの利活用が進展などの環境変化に合わせて、意図しない情報漏えいインシデントを防ぐ上での留意点・流出リスクについて記載の見直しを図る。
- ・ 海外への重要な技術情報の流出への懸念が高まっている中、外国から日本企業が保有する秘密情報が狙われるリスクについて、過去の漏えい事件を踏まえ、啓発コラムの見直しを図る。

□ 巻末の「参考資料」の修正

- ・ 関連情報・参考情報として巻末に添付されている「参考資料」について、直近の情報に対応して所要の修正・更新。

等

◆ 「従業員向け」啓発資料の作成

- ・ 従来作成・公表した資料（「営業秘密管理指針」・「秘密情報の保護ハンドブック」・「ハンドブックのてびき」）は主として企業において営業秘密管理を担う経営層・担当者向けの内容から構成されているが、実際に営業秘密に接する従業員等にとって、どのような行為が不正競争防止法違反となるのか（刑事・民事の責任が発生するのか）、営業秘密以外にもどのような情報に注意が必要なのかといった従業員目線で留意事項が理解できる啓発資料を作成する。

(参考)「秘密情報の保護ハンドブック」の位置づけ・「営業秘密管理指針」との関係

- 「営業秘密管理指針」は、不正競争防止法により「営業秘密」として法的保護を受けるために必要となる最低限の水準の対策を示すもの。 (平成15年1月策定、27年1月全面改定、31年1月最終改訂)
- 「秘密情報の保護ハンドブック」は、企業が保有する「秘密情報」について、法的保護レベルを超えて、情報漏えい対策として有効と考えられる対策や推奨される包括的対策等を包括的に紹介するもの。 (平成28年2月策定、令和4年5月改訂)

営業秘密管理指針について

- 法的保護を受けるために必要となる**最低限の水準の対策**を示すものとして平成27年1月に策定。
- その後、第四次産業革命を背景とした情報活用形態の多様化を踏まえて**平成31年1月に改訂**※。

※ 外部クラウドを利用して営業秘密を保管・管理する場合も、秘密として管理されていれば秘密管理性が失われるわけではない旨等を追記。

秘密情報の保護ハンドブックについて

- 法的保護レベルを超えて、**情報漏えい対策として有効と考えられる対策**や、漏えい時に推奨される**包括的対策等**をできる限り収集して**包括的に紹介するもの**として平成28年に作成。
- より良い漏えい対策を講じたい企業の方々に、企業の実情に応じて対策を取捨選択したり、参考としていただけるよう、**様々な対策を網羅的に掲載**。
- 簡易版「**秘密情報の保護ハンドブックのてびき**」も公表。

秘密情報の保護ハンドブック
(漏えい防止レベル)

営業秘密管理指針
(法的保護レベル)

1章	目的及び全体構成
2章	保有する情報の把握・評価、秘密情報の決定
3章	秘密情報の分類、情報漏えい対策の選択及びそのルール化
4章	秘密情報の管理に係る社内体制のあり方
5章	他社の秘密情報に係る紛争への備え
6章	漏えい事案への対応
参考資料	各種契約書・規程等の参考例、各種相談窓口等の連絡先、営業秘密侵害罪にかかる刑事訴訟手続、競争禁止義務契約の有効性について等を掲載

(追記参考例) ①法制度の見直し・ガイドラインの改訂に伴う修正点の追記例

限定提供データの追記例

【第1章 (1-1)】

(本書の限定提供データに関する指針との関係)

(本書と限定提供データに関する指針との関係)

- 平成30年には、付加価値の源泉となるデータの利活用を活発化し、安心してデータの提供・利用ができる環境を整備すべく不正競争防止法を改正し「限定提供データ」の制度が導入されました。令和6年●月に改訂した「限定提供データに関する指針」には、不正競争防止法における「限定提供データ」として法的保護を受けるための要件等についてひとつの考え方を示しています。
- 「限定提供データ」として法的保護が受けられるためには、その情報が、①「業として特定の者に提供する」(限定提供性)、②「電磁的方法により相当量蓄積され」(相当蓄積性)、③「電磁的方法により管理され」(電磁的管理性)との3要件を満たす必要があります(ただし、オープンなデータと同一のもの、「営業秘密」に該当するものは除外されます。)
- 本書は、企業が保有する重要な情報について、その漏えい対策のための秘密管理について対象とするものであることから、必ずしも限定提供データに対して全ての内容があてはまるわけではありませんが、企業が保有する価値ある情報のひとつとして、情報の把握・評価(第2章)、情報の漏えい対策の選択(第3章)、紛争への備え(第5章)など限定提供データにも活用可能な内容も含まれており、その管理について参考になるものと考えられます。

【第6章 (6-4)】

(2) 証拠の収集

- また、漏えいされた秘密情報が同法で定義される限定提供データに該当するための要件として、①限定提供性、②相当蓄積性、③電磁的管理性が挙げられるとともに、営業秘密を除くとされています(同法第2条第7項)。また、それに加え、限定提供データ侵害による民事責任を問うためには同法第2条第1項第11号から第16号までの要件等を満たす必要があります。

19条の2、19条の3の追記例

【第4章 (4-1)】

(子会社・委託先等を含めた秘密情報の管理体制の構築)

※令和5年の不正競争防止法改正において、国際的な営業秘密侵害事案における民事訴訟の手續が明確化され、日本国内において事業を行う営業秘密保有者の営業秘密であって、日本国内において管理されているものに関する民事訴訟であれば、海外での侵害行為(不正な取得・使用・開示)も日本の裁判所に訴訟を提起することができ、その際に日本の不正競争防止法が適用されると規定されました(国際裁判管轄について第19条の2、適用範囲(準拠法)について第19条の3。)
これにより、日本国内において保有・管理されている営業秘密だけでなく、海外に所在するサーバに蔵置されている営業秘密についても、海外での侵害行為に対し日本の不正競争防止法に基づいて保護を受けることが可能となりましたが、この保護を受ける上で、日本国内で管理体制を敷いていること(例:ID・パスワードの設定など)が必要なことから、営業秘密を海外に所在するサーバに蔵置している場合には、これらを意識して取り組むことが重要となります。

(追記参考例) ①法制度の見直し・ガイドラインの改訂に伴う修正点の追記例

5 条の 2 の追記例

【第 5 章（冒頭）】

- また、平成 27 年不正競争防止法改正により、新たに導入され、令和 5 年改正によりその適用範囲が拡充された営業秘密の不正使用行為を推定する規定（同法第 5 条の 2）及び平成 27 年不正競争防止法改正により新たに規制対象となった営業秘密侵害品の取引（同法第 2 条第 1 項第 10 号）について、紛争を防止するための方策も紹介します。

【第 5 章（5-2）】

- 加えて、平成 27 年不正競争防止法改正により、営業秘密の不正使用行為を推定する規定（同法第 5 条の 2）が導入され、「生産方法の営業秘密」を違法に取得して、その生産方法により生産することができる製品を生産している場合には、違法に取得した営業秘密を不正使用したものと推定されることとなりました。また、平成 30 年の不正競争防止法施行令において、「情報の評価又は分析の方法（生産方法に該当するものを除く。）の営業秘密」がこの推定規定の対象として追加され（第 1 条）、これを違法に取得し、使用して評価し、又は分析する役務を提供している場合には、違法に取得した営業秘密を不正使用したものと推定されることとなりました。なお、ここでの「違法な取得」には、平成 27 年の制度導入当初は、①産業スパイなど営業秘密を不正手段で取得した者（第 2 条第 1 項第 4 号）、②不正取得・開示が介在した営業秘密であることを知った上での取得した者（第 2 条第 1 項第 5 号・第 8 号）を対象としていました（第 5 条の 2 第 1 項）が、令和 5 年不正競争防止法改正により、③従業員・元従業員・取引先関係者など営業秘密の保有者からその営業秘密を示された者であって（第 2 条第 1 項第 7 号）、それを領得した者（第 5 条の 3 第 3 項）、④不正な経緯等を知らずに転得したが、警告書を受け取ること等によりその経緯等を事後的に知った者であって（第 2 条第 1 項第 6 号・第 9 号）、不正な経緯等を事後的に知ったにもかかわらず、記録媒体等を削除等しなかった場合（第 5 条の 2 第 4 項）も対象となりました。不正開示等であることを知らないことについて「重大な過失」がある状態で営業秘密を取得する場合も含まれることから、特に「重大な過失」とされてしまうこと等のないような適切な対応をすることが重要です。また、取得時に重大な過失がなかったとしても、取得後に重大な過失がある状態となり、その後に記録媒体等を削除しない場合等も含まれることから、廃棄・削除等の適切な対応をすることが重要です。

【第 5 章（5-2）】

（1）転職者の受け入れ

- また、前述のとおり、転職者の持ち込んだ情報が他社の営業秘密であると知らなかったとしても、警告書を受け取ること等により営業秘密の不正取得・不正開示に関する経緯を事後的に知った場合であって、そのような経緯を事後的に知ったにもかかわらず、入手した記録媒体等を削除等しなかった場合にも、営業秘密の不正使用に係る推定規定の対象となり得るため注意が必要です。

【第 5 章（5-2）】

（1）③採用後の管理

- 転職者として受け入れた者が転職前に勤務していた企業から、転職者により営業秘密の持ち出し等を理由とする警告や訴えの提起等がなされた場合には、同人が社内に持ち込んだ情報について、内容や保有状況の確認を行い、その内容によっては当該情報を削除するとともにその経緯を記録に残す、同一の情報を別途保有している場合には、その作成・入手の経緯について整理するといった対応を行うことが考えられます。

(追記参考例) ①法制度の見直し・ガイドラインの改訂に伴う修正点の追記例

水産庁ガイドライン追記例

【第2章(2-1)】 (企業が保有する情報とは)

- まずは、自社において「どういった情報を保有しているのか」を全体的に把握することから始まります。その際、情報は、紙に記載されていたり、サーバー~~＝~~やP C、U S Bメモリ等の機器・媒体や、クラウドなどの外部サービスに記録された電子データ等のような形で存在するだけではありません。その他にも、従業員が業務の中で記憶した製造ノウハウなど文章化されず目に見えない形で存在する場合や、プラントのレイアウト、金型、試作品、F 1品種の親系統となる植物、水産物⁶などの「物」自体が把握すべき情報である場合もあるので留意する必要があります。こうした情報も含めて、自社が保有する情報を把握することは、秘密情報の管理の一環であるだけでなく、自社の財産としての情報資産を認識することでもあり、これまで活用されていなかった情報資産を社内でも共有・活用することの促進にもつながります。

⁶ これまで、営業秘密については、製品の製造方法・原材料構成、顧客リストのように製造業、サービス業等において認識されることが多かったものの、近年、農林水産業(養殖業を含む)など非製造業においても、営業秘密によるノウハウ等の保護・活用への関心が高まってきています。このため、非製造業における営業秘密、とりわけ書面化されていないものの例についても紹介しています。

⁷ 社内の一定の技術情報については、各部署が全社共通の技術情報データベースに登録するシステムとしておくなど、情報の把握に資する取組みを日々の業務に組み入れるといった方法も考えられます。なお、この場合には、「知るべきものだけが知っている (need to know)」の原則に基づいて、システムのセキュリティを適正に強化し、必要に応じてアクセス権限の階層化を行います。

【参考資料4(第6章)】

その他 特定の分野・領域の特性を踏まえた対応

■ 水産分野における優良系統の保護等に関するガイドライン及び養殖業における営業秘密の保護ガイドライン(水産庁)

<https://www.jfa.maff.go.jp/j/saibai/yousyoku/youuryou.html>

水産分野における優良系統の保護等に関するガイドラインは、水産物の優良系統の保護の必要性に関する現状を整理するとともに、保護すべき対象、不正競争防止法の営業秘密の枠組み等の既存の知的財産制度上における対応の整理、優良系統の保護に資する対応等についてまとめたものです。

また、養殖業における営業秘密の保護ガイドラインは、養殖現場における飼育、選抜等による優れた生産技術やノウハウ、その他の技術上の情報について、不正競争防止法の営業秘密の枠組みを活用した保護に取り組む際の留意点等をわかりやすくまとめたものです。

(追記参考例) ②営業秘密・秘密情報を取りまく「環境の変化」に伴う修正点の追記例

A I の普及・利活用に関連する追記例

【第1章 (1-1)】 (秘密情報の管理の効用)

- また、近年の情報通信機器・技術の普及・進展、働き方の多様化・柔軟化の流れとともに、大規模な感染症や各種防災への対応・対策の関係上、企業におけるテレワークの取組みが急速に進んでいます。このような中、情報の利用・アクセスがこれまでの企業内から、自宅やサテライト施設など外部からの情報利用・アクセスが常態化しつつあります。さらに、A I を活用した新たな情報利用・創出の場面が増えてきている中で、例えばA I を作成・学習の段階で様々なデータを利用する、情報分析のために生成A I を利用するといった新たなツールの利活用も進んできつつあります。したがって、このような流れを踏まえた秘密情報の管理・利用のあり方を検討し、取り入れることも、経営者や情報管理責任者にとって必要となってきています。

【第1章 (1-1)】 (参考)

(参考)「秘密情報の保護」の視点からのA I 利用

近年の生成A I の進展に伴い、あまりA I を利用してこなかった多くの企業や組織においてもA I のビジネスへの活用がこれまで以上に意識され、広い範囲で実際に業務への適用が始まっています。様々な業種の業務効率化を始め、利用の仕方によってはこれまでになかった新しい事業も期待できるA I ですが、大きくクローズアップされた利便性の傍ら、A I を利用する際には留意しなければならない様々なリスクが存在します。活用するケースや環境ごとにどのようなリスクがあるのかについては、経済産業省から公開されている「A I 原則実践のためのガバナンス・ガイドライン」⁴等に、リスクを洗い出す分析に関する指針について述べられています。

そうしたリスクには、情報漏えいに直結するものもあります。機械学習に基づくA I は大量のデータを学習して入力データの分類・判定を行いますし、生成A I は質問（プロンプト）により利用者が様々なデータを入力しながら利用します。例えば以下のようなシナリオを考慮してみると、A I による情報漏えいのリスクをイメージしやすくなるかもしれません。

① 生成A I 利用における組織のルール不備による情報漏えいリスク

組織における生成A I 利用のルール化とその周知が遅れ、職員が個人で秘密情報保護に関する契約に不備がある生成A I を利用し、営業秘密情報を学習させてしまった。

② サプライチェーン（委託先）での情報漏えいリスク

A I による情報分析を委託する企業で、分析データの管理不備があり、分析を委託した営業秘密情報が漏えいした。

③ A I の悪用による情報漏えいリスク

A I の悪用によりフィッシングメールのなりすましが巧妙化して職員がだまされ、営業秘密情報が漏えいした。

A I の利活用が日々の業務により一層密接に関わってくる潮流の中、A I を利用する際は、「こうしたリスクがある」という前提に基づき、自組織における営業秘密に関するA I の処理は何が想定されるのか、そうした処理に関するA I 利用ルールやデータ管理ルールはどうなっているのか等の確認が必要です。A I を自社の業務やサービスに導入していない場合でも、個人が生成A I を利用する場合のルールは重要です。自分のPCで営業秘密に関する質問をする、等の使い方は避けるべきでしょう。さらに、A I を直接利用しないとしても、A I を悪用したフェイクコンテンツやなりすましによる営業秘密窃取のリスクが生じています。

A I の導入はさらに加速することが予想されますが、そのリスクについて最新の情報を収集し、組織のルールを作りながら効果的にA I を利活用することが望まれます。

(追記参考例) ②営業秘密・秘密情報を取りまく「環境の変化」に伴う修正点の追記例

A I の普及・利活用に関連する追記例 (続き)

【第3章 (3-1)】 (分類に当たっての考え方)

○ 一方で、同程度の評価の秘密情報であっても、以下のような「情報の利用態様」に応じて、異なる対策を講ずる場合もあります。

※「情報の利用態様」は予め定められたものではなく、自社の事業規模や業種、取り扱う情報の内容・性質等を踏まえた上で、望ましい「情報の利用態様」とは何かを自主的に判断することが重要です。

例えば、その秘密情報は、「従業員各々に個別に資料を所持させるべきものなのか、共有資料のみとするのか」や、「ネットワークに接続されたP C、クラウドなどの外部サービス等に保管すべき情報か否か」、「テレワークなど社外からのアクセスや個人所有のデバイスを用いたアクセスに際して使用を認めるべき情報か否か」、「生成A Iなどの利用に際して使用(入力)を認めるべき情報か否か」、「サプライチェーンで共有する必要がある情報か否か」といったことを今一度検討してみることが有効です。

【第3章 (3-2)】 (5つの「対策の目的」)

(2) 持出し困難化

秘密情報が記載された会議資料等の回収やテレワーク・オンライン会議でのアクセス(投影等)の制限、事業者が保有するノートP Cの固定や持ち出しの制限、記録媒体への複製制限や組織が許可した以外のオンラインストレージの利用制限、従業員の私物U S Bメモリ等の携帯メモリの持込み・利用を制限すること等によって、当該秘密情報を無断で複製したり持ち出すことを物理的、技術的に阻止することを目的としています。

特に、テレワークの実施との関係では、重要情報のレベルに応じたアクセス制限、P C等への格納制限、実施を認める場所の吟味(自宅等の周囲の目から遮断が可能・容易な環境か、電車やカフェ等の周囲の目がある環境か)、画面の覗き込み防止フィルムを用いる、オンラインで会議を行う際は大声での会話を避ける、組織ネットワークに接続する際にはV P N等を用いて暗号化する等の対策を講じることが重要となります。また、生成A Iなどをビジネスで利用する場合には、入力した情報が社外に流出・公開等されてしまう可能性があるのかどうかを踏まえて、これらの利用の可否を判断する、これらの利用に当たっては社外に流出等されてしまったら困る情報は使用(入力)しないといった対応を講じることが重要となります。

(追記参考例) ②営業秘密・秘密情報を取りまく「環境の変化」に伴う修正点の追記例

A I の普及・利活用に関連する追記例 (続き)

【第3章 (3-3)】

(1) ルールの必要性とその方法

○ さらに、近年、A I 技術の進展を踏まえて、外部の生成A Iなどを事業・業務の中で利活用する動きが増えていますが、利用しようとする生成A Iなどの情報管理の状況、すなわち入力した情報が社外に流出・公開等されてしまう可能性があるのかどうかを踏まえてこれらの利用の可否を判断する、これらの利用に当たっては社外に流出されてしまったら困る情報は使用(入力)しないといった対応を講じないと、秘密情報が社外に流出等してしまう可能性があります。このため、生成A Iなどを利用する場合には、予め許可された生成A Iを用いるようにするとともに、適切に定められた基準に基づいて予め許可された情報のみを使用(入力)するようにすること等とするルールを定めることは、秘密情報の漏えい防止に効果があるため、生成A Iなどの利用に際して従業員が遵守すべきルールを定めることが必要です。

【第4章 (4-1)】

(経営層の関与の必要性)

○ また、秘密情報は全ての部門に存在することが考えられ、かつ、その漏えい対策は、知的財産、貿易・輸出管理、人事・労務、情報セキュリティ、法務といった従来から対策に関与していた部門のほか、テレワークの導入・浸透に伴う新たな課題への対応に伴うテレワークに対応した相談窓口や外部メンタルヘルスケアの支援、生成A Iを含む新たなツールの特性を理解した上での対応(利用の可否、利用時の留意点の検討)などの多様な観点からの対策を必要とすることから、自社内の個々の部門が、それぞれ独自に対策を行い、全体としての調整を欠いたままでは十分な対策を講ずることはできません。その一方で、情報管理規程等の社内ルールの整備など、本来的に全社的に検討しなければならない対策も存在します。

大学等の情報漏えいに関連する追記例

【第1章 (1-1)】

(秘密情報の管理の効用)

(参考) 大学・研究機関など企業以外の組織における情報管理との関係

- 貴重な研究成果は、大学・研究機関にとって民間企業におけるものと同様に虎の子の財産であり、秘密情報として価値を有しています。ひとたび秘密ではなくなった情報は、再び秘密に戻ることはないことから、漏えいの防止や予防が重要であるとともに、それに加え、漏えいが発生した場合への備えを講じることも重要になります。
- 不正競争防止法については、「事業者」として大学が対象に含まれることを前提とした裁判例も存在しており、営業秘密についてもあてはまると考えられます。
- したがって、本書では、「企業」、「従業員」といった民間企業を念頭に置いた記載となっていますが、その内容は大学・研究機関における情報管理においても、十分当てはまり、参考になるものと思われます。
- また、大学や研究機関が保有する情報については、外部に有償提供するオリジナルの試験・試薬の製造方法、技術指導や性能検査を外部から受託する際の元となる独自の技術(検査方法など)、研究開発・実験データで、特許出願するか検討中の情報といった自ら創出した価値のある情報のほか、共同研究の相手先の民間企業から提供を受けた相手先の秘密情報などがあり、これらは不正競争防止法が対象とする「営業秘密」に該当する情報です。そのため、大学や研究機関が「営業秘密」を保有することは十分にあり得ます。

(追記参考例) ②営業秘密・秘密情報を取りまく「環境の変化」に伴う修正点の追記例

大学等の情報漏えいに関連する追記例 (続き)

【第3章 (3-4)】 (1) 従業員等に向けた対策

(従業員等とは)

従業員等とは、典型的には~~役員~~や自社が雇用する従業員が該当しますが、役員自社の実習生や派遣労働者、委託先従業員、実習生などであって、自社内において勤務する者などをも含みます。

なお、企業だけでなく、大学・研究機関といった組織にも、実験・研究データなど秘密情報が存在し、営業秘密や限定提供データとして不正競争防止法による保護を受けることが可能な情報があると考えられます。このため、大学・研究機関もこれらの情報の保有者になり得ることから、このような保有者との関係では、大学・研究機関に勤務している教員・研究者などが本ハンドブックでいう従業員等に相当することになります。

経済安全保障に関連する追記例

【第1章 (1-1)】 (秘密情報の管理の効用)

- さらに、企業にとって管理が必要とされる情報の種類も、企業の競争力の源泉として、法的保護を受ける前提として適切な管理が必要とされているものの管理の要否・内容について保有企業の判断に委ねられている営業秘密や限定提供データ（不正競争防止法）のほか、法律により保有企業に一定の管理が必要とされる個人情報（個人情報保護法）や安全保障貿易管理に関する技術情報（外為法）、経済安全保障推進法のもとで保全指定され特許出願の公開が留保された発明に関する情報⁵など多様化してきています。また、先端的な技術情報については、国内での競合企業による不正取得や退職者を通じた開示といった漏えい事案だけではなく、海外の企業や政府機関の関係者からの巧妙な接触を通じた漏えい事案も発生しており、競争力の維持の観点だけでなく、個々の企業の枠組みを超えた経済安全保障の視点からも、企業が保有する秘密情報・重要情報の意図しない流出を防止することは、重要な課題となってきています。

【第2章 (2-2)】 (1) ②技術情報

※権利化する場合であっても、出願公開までは一定期間秘密情報とすべき場合や、権利化する技術実施に当たってのノウハウは秘密情報とすべき場合もあります。また、経済安全保障推進法のもとで保全指定され特許出願の公開が留保された発明に関する情報については、保全指定が解除され、特許権が付与されたあとの侵害行為については特許法による対応が可能であるが、それ以前の段階における当該情報の不正取得・開示・使用等の侵害行為が行われた場合には、不正競争防止法の営業秘密に基づく救済（差止請求・損害賠償請求等）が対応手段になるものと考えられることから、営業秘密として保護を受けるための管理を行う必要があると考えられます。

(追記参考例) ②営業秘密・秘密情報を取りまく「環境の変化」に伴う修正点の追記例

M & Aに関連する追記例

【第2章 (2-2)】

(1) ①営業情報

- その漏えいにより、法令違反や他社との契約違反等となり、自社の社会的信用の低下を招いたり、他社との信頼関係を毀損させる情報か否か
(顧客の個人情報、受託やライセンス、M&Aにおける交渉等の他社との契約等により限定的に開示された営業情報・限定提供データ 等)

【第2章 (2-2)】

(1) ②技術情報

- その漏えいにより、法令違反や他社との契約違反等となり、当該他社との信頼関係を毀損させる情報か否か
(受託やライセンス、M&Aにおける交渉等の他社との契約等により限定的に開示された技術情報、安全保障貿易管理に関わる製品に関する技術情報、経済安全保障推進法のもとで保全指定され特許出願の公開が留保された発明に関する情報 等)

【第3章 (3-4)】

(3) 取引先に向けた対策

(取引先とは)

- 自社の秘密情報を共有する相手方を指します。例えば、委託先や委託元、外注先や外注元、共同研究相手、M&A交渉(事前協議を含む。)の相手などが考えられます。
※自社内で業務を行う委託先従業員等については、(1) 従業員等に向けた対策の対象となります。

訴訟手続への情報提出に関連する追記例

【第3章 (3-4)】

(4) 外部に向けた対策

(参考) 訴訟手続における文書提出との関係

- 訴訟関係者(相手方の当事者・代理人など)について、例えば自己の主張や相手への反論、文書提出命令などにより営業秘密を含む保有する書類・データの提出を行うことがあり得ます。これらの関係者については、信義則上または法律上の守秘義務等が及ぶものの、当初の保有者の手を離れたところに情報が存在することとなり、情報漏えいや不正利用などのリスクがあり得ることから、慎重な対応が必要になると考えられます。
- 訴訟手続において秘密情報を提出する場合には、外部からの不正アクセス行為によるものでなく、秘密情報の保有者から提供されることから、(3) 取引先に向けた対策での留意点(p 80)と同様に、まずは秘密情報の提出の必要性をよく検討し、提出が真に必要な範囲について、十分に確認することが重要です。

【第5章 (5-2)】

- 以下では、特に他社情報の意図しない侵害が生じやすいと考えられる4つの場面((1) 転職者の受入れ、(2) 共同・受託研究開発、(3) 取引の中での秘密情報の授受、(4) 技術情報・営業情報の売込み)を想定し、それぞれの場面で有効と考えられる対策を紹介します。以下に示す対策を行うことは、業務効率等の観点で相応のコストがかかるものの、実際に秘密情報に関して紛争となってしまった場合、損害賠償や社会的信用の低下など、対策にかかるコストをはるかに上回る損失を被る場合が多いことを認識する必要があります。

※他社の秘密情報の混入やそれに伴う侵害については、訴訟手続を通じて、相手方から提出された文書・データに係る情報について生じることも考えられるところ、このような場合にも第5章の対策が参考になると考えられます。

(参 考)

「秘密情報の保護ハンドブック」の改訂箇所一覧

2. 「秘密情報の保護ハンドブック」の改訂内容一覧

章	節	項目	主な改訂内容
はじめに	—	—	■ A I を活用した新たな情報利用・創出の場面での効率的な利用と情報漏えいへの対策の両立の重要性を追加 ■ 令和 5 年不正競争防止法の改正（限定提供データの保護範囲の見直し、国際的な営業秘密侵害に関する手続の整備）に関連して、ハンドブックその他の啓発資料の見直しをする旨を追加 ■ 重要情報の例として、経済安全保障推進法のもと保全指定され特許出願の公開が留保された発明について追加
第 1 章 目的及び全 体構成	1-1 目的及び留意点等	—	（本書と営業秘密管理指針との関係） ■ （参考）コラムとして記載されていた「限定提供データ・指針と本ハンドブックとの関係」について、本文において（本書と限定提供データに関する指針との関係） として記載の位置づけを見直す （本書と限定提供データに関する指針との関係） ■ 参考から本文に記載位置づけを変更（再掲） ■ 令和 5 年改正に関連する記載（現地提供データの保護対象の見直し、限定提供データに関する指針の改訂）について内容を更新（その他の内容は、従来記載を踏襲） （秘密情報の管理の効用） ■ 「転職・独立」と追加 ■ A I を活用した情報の利活用（作成・学習の段階での利用や生成 A I の活用）を追加、解説として「（参考）「秘密情報の保護」の視点からの AI 利用」を追加及び脚注 4 として「A I 原則実践のためのガバナンス・ガイドライン」の U R L を追加 ■ 経済安全保障推進法のもとで保全指定され、特許出願の公開が留保された発明に関する情報などの多様化について追加及び脚注 5 として経済安全保障推進法について内閣府の H P の U R L を追加 （本書の留意点） ■ （参考）に大学・研究機関など企業以外の組織における情報管理との関係について追加
	1-2 本書の全体構成	—	■ なし
	1-3 本書の使い方	—	■ なし

章	節	項目	主な改訂内容
第2章 保有する情報の把握・ 評価、秘密情報の決定	冒頭（枠囲み）	—	■ 「法令又は契約により秘密に」を追加
	2-1 企業が保有する情報の 評価	(1) 企業が保有する情報の全体像 の把握	(企業が保有する情報とは) ■ 令和5年3月に水産分野、養殖業におけるガイドラインが策定・公表されたため、「物」による営業秘密の例として（F1品種の親系統となる植物に加えて）「水産物」を追加及び脚注7に「養殖業を含む。」を追加
		(2) 保有する情報の評価	■ なし
	2-2 秘密情報の決定	冒頭	■ 他社へのライセンスについて趣旨の明確化の観点から脚注11（旧脚注9）に「営業秘密などの権利化しないノウハウや」を追加
		(1) 秘密情報の決定に当たって考慮 すべき観点のイメージ	①営業情報 ■ 契約に基づく重要情報の開示例として、「M&Aにおける交渉」を追加 ②技術情報 ■ 契約に基づく重要情報の開示例として、「M&Aにおける交渉」を追加（①同様） ■ 漏えいにより法令違反の可能性ある技術情報の例として、「経済安全保障推進法のもとで保全指定され特許出願の公開が留保された発明に関する情報」を追加 ■ 経済安全保障推進法における非公開特許に関する情報を営業秘密として管理する意義・必要性について記載を追加

章	節	項目	主な改訂内容
第3章 秘密情報の 分類、情報 漏えい対策 の選択及び のルール化	冒頭（枠囲み）	－	■ 脚注13（旧脚注11）の特定非営利活動法人日本ネットワークセキュリティ協会「中小企業情報セキュリティ対策促進事業」ＨＰのＵＲＬを更新、IPA「中小企業の情報セキュリティ対策ガイドライン」のＵＲＬを追加
	3-1秘密情報の分類	－	（分類に当たっての考え方） ■ ＡＩ技術を活用した情報ツールとそれに伴う漏えいリスクとして、「生成ＡＩなどの利用に際して使用（入力）を認めるべき情報か否か」を追加 ■ 枠内：上記同様箇所あり
	3-2 分類に応じた情報漏えい対策の選択	－	（対策の選択に当たっての考え方） ■ 「生成ＡＩなどの利用（生成ＡＩなどに、自社が保有している情報を入力すること）の可否」を追加 （５つの対策の目的） (2)持出し困難化 ■ 生成ＡＩをビジネスで活用する場合、外部に流通したら困る情報は使用（入力）しないといった対応を講じることが重要な旨を追加
	3-3 秘密情報の取扱い方法等に関するルール	(1) ルール化の必要性とその方法	■ 生成ＡＩを事業・業務で利活用する際にルールを定めることが必要である旨を追加
		(2) 秘密情報の取扱い等に関する社内規程の策定	■ ＩＰＡ作成の組織における内部不正防止ガイドラインに「第５版。令和４年４月」を追加及び脚注19（旧脚注17）のＵＲＬを更新
		コラム② こんなに怖い、秘密情報の漏えい	■ なし
		コラム③ 外国から狙われる企業の秘密情報	■ サイバー攻撃に関する事例１を昨今の状況を踏まえた内容に修正。 ■ その他軽微修正

章	節	項目	主な改訂内容
第3章 秘密情報の 分類、情報 漏えい対策 の選択及び のルール化	3-4 具体的な情報漏えい対 策例	(1) 従業員等に向けた対策	(従業員等とは) ■ 「従業員等」について記載を整理 ■ 大学・研究機関向け啓発の観点から、「従業員等」の対象についての注意喚起を追加 ①「接近の制御」に資する対策 ■ b. 脚注24（旧脚注22）の I P A『チョコッとプラスパスワード』の U R L を更新 ■ c. 屋外に存在する植物等の管理方法について、農水省「農業分野における営業秘密の保護ガイドライン」の農業分野より具体的なアクセス制限の例示を抜粋・追加 ②「持出し困難化」に資する対策 ■ （冒頭）生成 A I 等を利用する際の注意点を追加 ■ c. 旧脚注25の I P A『対策のしおりシリーズ』の U R L を削除 ■ e. 「生成 A I 等」を追加 ■ j. 脚注27（旧脚注26）の参照先に「P 47」を追記 ③「視認性の確保」に資する対策 ■ c. 対策のための看板等の設置によるデメリットの（注意喚起を招く）可能性について追記 ■ h. 脚注31（旧脚注30）の「個人データの漏えい等の事案が発生した場合等の対応について」の U R L を更新 ④「秘密情報に対する認識向上」に資する対策 ■ なし ⑤「信頼関係の維持・向上等」に資する対策 ■ b. 脚注34（旧脚注33）の I P A『組織における内部不正防止ガイドライン』の記載ページを修正
		(2) 退職者等に向けた対策	■ なし

章	節	項目	主な改訂内容
第3章 秘密情報の 分類、情報 漏えい対策 の選択及び のルール化	3-4 具体的な情報漏えい対策例	(3) 取引先に向けた対策	(取引先とは) ■ 取引先関係者の例として、「M&A交渉（事前協議を含む。）の相手」を追加 (取引を開始する前に留意すべき点) ■ 脚注42（旧脚注41）に記載されているNISC作成の『政府機関の情報セキュリティ対策のための統一基準群』のURL等を更新 ①「接近の制御」に資する対策 ■ なし ②「持出し困難化」に資する対策 ■ なし ③「視認性の確保」に資する対策 ■ なし ④「秘密情報に対する認識向上」に資する対策 ■ d. の脚注45（旧脚注44）に記載されているIPAの〈映像で知る情報セキュリティ〉のURLを更新 ⑤「信頼関係の維持・向上等」に資する対策 ■ c. 各種ガイドライン等（振興基準）の改訂に伴い、本文、脚注47（旧脚注46）を修正
		(4) 外部者に向けた対策	(留意点) ■ （参考）訴訟手続きにおける情報提供する際の注意喚起を追加 ①「接近の制御」に資する対策 ■ f. 図表3（9）（10）、旧脚注47を削除し、最新の対策技術を紹介、脚注48として「中小企業の情報セキュリティガイドライン」のURLを追加 ②「持出し困難化」に資する対策 ■ なし ③「視認性の確保」に資する対策 ■ b. 各種ガイドライン等（高度標的型攻撃対策に向けたシステム設計ガイド）の公開終了に伴い、旧脚注48を削除 ④「秘密情報に対する認識向上」に資する対策 ■ なし ⑤「信頼関係の維持・向上等」に資する対策 ■ なし
		コラム④ 標的型攻撃メールってどんなもの？	■ 最新の公開情報を踏まえた記載の更新及び図表の削除
		コラム⑤ 最低限のサイバーセキュリティって？	■ 軽微修正（取組内容の変化等に伴う技術的修正）

章	節	項目	■ 主な改訂内容
第4章 秘密情報の 管理に係る 社内体制 のあり方	4-1 社内体制構築に当たっ ての基本的な考え方	—	(経営層の関与の必要性) ■ 外為法関連情報を念頭に、関連部署の例示として、「貿易・輸出管理」を追加 ■ 「生成 A I を含む新たなツールの特性を理解した上での対応（利用の可否、利用時の留意点の検討）」を追加 (事業規模が大きな企業における社内体制の具体例) ■ 外為法関連情報を念頭に、関連部署の例示として、「貿易・輸出管理」を追加 (部門横断的な組織と各部門の役割分担) ■ （点線枠囲み）秘密情報の管理のチェック・見直しについて、積極面だけでなく不要情報の廃棄についても注意喚起の観点から「廃棄すべき情報が残存しているなど」を追加 (子会社・委託先等を含めた秘密情報の管理体制の構築) ■ 令和5年改正において国際的な営業秘密侵害に関する手続（裁判管轄・第19条の2、適用範囲・第19条の3）が新設されたことを踏まえて、営業秘密の所在を問わず、日本から適正な情報の管理がなされていることは、海外での侵害行為に対しても法的保護を求める上で重要となる旨を追加
	4-2 各部門の役割分担の例	コラム⑥ 技術情報管理認証制度について	■ 書きぶりが「内部での流出防止対策」から「情報セキュリティ対策」に修正。 ■ 技術情報管理自己チェックリストを追加。
第5章 他社の秘密 情報に係る 紛争への備 え	冒頭（枠囲み）	—	■ 令和5年度改正（第5条の2）を踏まえて記載を修正
	5-1 自社情報の独自性の立証	—	■ なし
	5-2 他社の秘密情報の意図しない侵害の防止	冒頭	■ 趣旨の明確化の観点から、「自社で保有している」を追記 ■ 訴訟手続での情報提出を通じた漏えいリスクについて、注意喚起のため※で記載を追加 ■ 令和5年改正において技術上の営業秘密の不正使用に係る推定（第5条2）の適用範囲が拡充されたこと踏まえて、保有情報の適正管理の必要性を追加
		(1) 転職者の受入れ	■ （冒頭・③）令和5年改正において技術上の営業秘密の不正使用に係る推定（第5条2）の適用範囲が拡充されたこと踏まえて、警告受取後等の情報の適正取扱いの必要性を追加
		(2)～(4)	■ なし
	5-3 営業秘密侵害品に係る紛争の未然防止	—	■ なし

章	節	項目	主な改訂内容
第6章 漏えい事案 への対応	6-1 漏えいの兆候の把握及 び疑いの確認方法	(1) 漏えいの兆候の把握	■ なし
		(2) 漏えいの疑いの確認	■ なし
	6-2 初動対応	冒頭	■ 各種ガイドライン等（組織における内部不正防止ガイドライン）に係る記載整理
		(1) 社内調査・状況の正確な把握・ 原因究明	■ なし
		(2) 被害の検証	■ なし
		(3) 初動対応の観点	■ 脚注54「情報セキュリティ安心相談窓口」のURLを更新
		(4) 初動対応の体制	■ なし
	6-3 責任追及	冒頭	■ なし
		(1) 刑事的措置	■ 表題を整理（「的」を削除）
		(2) 民事的措置	■ 表題を整理（「的」を削除）など軽微修正
		(3) 社内処分	■ なし
	6-4 証拠の保全・収集	(1) 証拠の保全	■ なし
		(2) 証拠の収集	■ （営業秘密の記載に並べて）限定提供データに責任追求に当たっての留意点を追記

章	節	項目	主な改訂内容
参考資料	1 情報漏えい対策一覧		■ 本編修正に合わせて形式的・軽微な修正（項目名・ページ番号の整理） ※パブコメまでに整理予定
	2 各種契約書等の参考例		■ なし
	3 各種窓口一覧		■ 現在掲載している窓口については、基本的には引き続き掲載しつつ、時点修正や廃止窓口の削除など軽微な修正 ※パブコメまでに整理予定
	4 秘密情報管理に関する各種ガイドライン等について		■ 現在掲載しているガイドライン等については、引き続き掲載しつつ、時点修正など軽微な修正 ■ このほか、新たに以下を追加 ■ その他 非製造業における営業秘密管理に関連して、水産庁の「水産分野における優良系統の保護等に関するガイドライン、及び「養殖業における営業秘密の保護ガイドライン」
	5 競業避止義務契約の有効性について		■ 公表資料のURL変更など軽微な修正
	6 営業秘密侵害罪に係る刑事訴訟手続における被害企業の対応のあり方について		■ なし

※その他、本誌のページの各箇所に記載されている「サーバー」を「サーバ」に統一し、今回の修正に伴う脚注やページ数の修正をおこなった。