【参考資料２】

秘密情報の保護ハンドブック

～企業価値向上に向けて～

平成２８年２月

（最終改訂：令和~~４~~６年~~５~~●月）

経済産業省

はじめに

企業は、自社が持つ様々な営業情報や技術情報を用いて、他社との差別化を図り、自社の競争力を向上させています。事業活動で用いられる情報の中には、秘密とすることでその価値を発揮する情報も存在します。そのような、営業秘密をはじめとする秘密情報の保護は、自社の競争力強化の観点とともに、ひとたび秘密情報の漏えいが起こると、研究開発投資の回収機会を失ったり、社会的な信用の低下により顧客を失ったりと、甚大な損失を被るといった観点からも、欠かすことのできないものとなっています。

そして、秘密情報の漏えいは、従業員等の企業の内部者、発注元や委託先等の取引先、不正アクセス行為者等の外部者など、様々な経路により生ずるおそれがあります。さらに、ＩＴの高度化・多様化も相まって、秘密情報の漏えいは、その情報を漏らそうとする者にとってはより容易に、その防止策を講ずる企業にとってはより複雑・困難になりつつあると言えます。

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む中、情報の利用・アクセス場所がこれまでの企業内中心から、従業員の自宅や実家、サテライト施設など企業外部からの情報利用・アクセスが浸透・常態化しつつあり、情報管理・利用のあり方が変容しつつあります。

加えて、情報管理・利用のあり方は絶えず変化しており、ＡＩ（人工知能）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、おり、これらを活用することで業務の効率化、新たなビジネスの創出など事業者・企業に有益なものとしてその普及・利用の拡大が期待される。一方で、例えばＡＩ開発におけるデータ学習時や外部の生成ＡＩへの情報の不用意な入力を通じて、意図しない情報漏えいにつながる懸念も皆無ではなく、情報漏えいへの対策を講じながら新たなツールの効果的な利用を進めつつ、情報漏えいへの対策を両立させることも重要といえます。

さらに、企業・産業界にとって競争力の源泉である技術情報について、国内での不正取得や開示といった漏えい事案だけでなく、海外の企業・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が発生するなど、競争力の維持の観点や経済安全保障の観点からも、企業が保有する技術情報・重要情報の流出の防止は、重要な課題となってきています。

こうした状況の中で、経済産業省では、まず、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要件の考え方を、平成２７年１月に改訂した「営業秘密管理指針」（最終改訂：平成３１年１月）に示しました。また、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」の制度を導入するとともに、法的保護を受けるために必要な要件の考え方を平成３１年１月に「限定提供データに関する指針」（令和４年５月改訂）として示しました。

その後、令和５年には不正競争防止法が改正され、限定提供データの保護範囲の見直し（「秘密管理されている」情報であっても、営業秘密に該当しないものについては限定提供データとして保護を受けることが可能となるように保護を拡充）とともに、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が日本国外において使用等された場合における訴訟手続（国際裁判管轄・適用範囲）の明確化等を含む制度整備が行われ、本ハンドブックを含めて関係する啓発資料の見直しも図りました。

本書では、不正競争防止法に基づく営業秘密として法的保護を受けられる水準を越えて、秘密情報の漏えいを未然に防止するための対策を講じたい企業の方々にも参考としていただけるよう、様々な対策例を集めて紹介しました。なお、本書が対象とする秘密情報としては、典型例として営業秘密が想起されますが、必ずしもこれにとどまるものではなく、個人情報保護法の対象となる個人情報、外為法の対象となるような重要な技術の情報、特許出願前の技術情報のほか、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といった企業等において秘密として管理する必要がある様々な情報も該当する可能性があります。したがって、各社の事業規模や取り扱う情報の性質などに応じて取捨選択し、情報漏えいの防止に取り組んでいただきたいと考えます。このような見地から、本書では「営業秘密」という言葉ではなく、より広い意味として「秘密情報」という言葉を用いています。

また、外国から狙われる企業の重要情報・秘密情報の実態については、その危険性に比して不透明なところがありましたが、警察庁からの協力・情報提供を受けて、具体的な事例を整理し、漏えいを未然に防止するための対策を講じたい企業の方々にも参考としていただけるよう、様々な対策を集めて紹介しました。

加えて、企業が有する秘密情報は、あくまで事業活動の中で有効利用されてこそ存在意義があります。必要以上に厳格な管理をし「金庫」の中にしまったままでは、企業価値向上のための秘密情報という本来あるべき姿が失われてしまいますので、情報の管理と有効利用との適正なバランスを考慮いただくことも重要です。

本書が、企業における創意工夫を促し、秘密情報の適切な管理、そして、その有効利用を通じて、企業価値の継続的な向上が果たされることを期待しています。

目　　次

参考資料

その他

第１章　目的及び全体構成

１－１　目的及び留意点等

（秘密情報の重要性）

○　企業が有する「情報資産」は、商品の生産、販売、サービスの提供などの様々な企業活動の価値や効率性を高めています。「情報資産」と一口に言っても、顧客情報、発明情報、ビジネスモデル、取引情報、人事・財務情報など多種多様であり、製品やサービスが均質化しつつある近年において、他者との差別化を図り、競争力を高めていくために、「情報資産」の保護・活用は、ますますその重要性を増しています。

○　そのような「情報資産」の中には、他者に対して秘密とすることでその価値を発揮する情報（秘密情報）が存在します。そのような秘密情報は、一度でも漏えいすれば、たちまち情報の資産としての価値が失われてしまい、その回復は非常に困難なものです。企業の経営に致命的な悪影響を与える場合もあるでしょう。

（本書の目的）

○　経営者は、企業の価値・競争力の源泉となる秘密情報を含めた「情報資産」を企業活動の中でどのように有効に活用しつつ、企業価値・競争力の毀損につながるその漏えいリスクにどのように対処していくかを、リーダーシップを持って判断していかなければなりません。そこで、本書では、秘密情報を決定する際の考え方や、その漏えい防止のために講ずるべき対策例、万が一情報が漏えいした場合の対応方法等を、近年の情報漏えいの具体的事例を交えて示しており、それによって、経営者をはじめとする企業の方々に、自社における秘密情報の管理を適切に実施していく際の参考としていただくことを目的としています。

（本書と営業秘密管理指針との関係）

○　平成３１年１月に改訂した営業秘密管理指針[1]には、不正競争防止法における「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[2]の対策を示して

---

[1] https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31ts.pdf

[2] 不正競争防止法に規定する「営業秘密」と認められるためには、その情報が、①秘密として管理されていること（秘密管理性）、②事業活動にとって有用であること（有用性）、③公然と知られていないことの３要件を満たす必要があります。①の秘密管理性が認められるためには、企業の「特定の情報を秘密として管理しようとする意思」が、具体的状況に応じた経済合理的な秘密管理措置によって、従業員に明確に示され、結果として、従業員がその意思を容易に認識できる（「認識可能性」が確保される）必要があります。

います。

○　一方、本書は、営業秘密としての法的保護を受けられる水準を超えて、秘密情報の漏えいを未然に防止するための対策を講じたい企業の方々にも参考としていただけるよう、情報漏えい対策として有効と考えられる対策をできる限り収集して包括的に紹介しています。企業の方々が漏えい対策を検討・実施する際に、会社の規模、業態、保有する情報の性質などに応じて適切な漏えい対策を選択いただけるように工夫しております。

○　したがって、本書で紹介する対策の全てを実施しなければ、不正競争防止法の「営業秘密」として法的保護が受けられないというものではありません。そこで、本書では「営業秘密」という言葉ではなく、より広い意味として「秘密情報」という言葉を用いています。

（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。

~~**（参考）限定提供データ・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４年５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に必要となる最低限の水準の対策を示しています。~~

- ~~不正競争防止法に規定する「限定提供データ」と認められるためには、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、秘密として管理されてい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。~~

（秘密情報の管理の効用）

○　適切な秘密情報の管理を実施することにより、企業の価値・競争力の毀損といった企業にとって致命的な悪影響を及ぼすおそれもある情報漏えいのリスクを減らすという安全・安心の面だけでなく、実効的な情報管理により、業務の効率性、企業への信用・信頼、業績等が上がり、ひいては、企業価値の向上につながることを期待できます。また、退職者との関係で自社の秘密情報の対象範囲・内容を明確にすることは、転職・独立・起業に当たってのトラブルを防止し、働く方々の自由な職場選択・キャリアアップを可能とする環境の整備につながるとともに、企業にとっても、転職者の受け入れに伴う紛争の予防になり、人材の流動性の向上を通じて多様な人材確保が可能となります。さらに、我が国企業の秘密情報の管理のレベルが底上げされることは、共同研究・開発における情報漏えいリスクを低減させ、オープンイノベーション[3]を更に進展させます。

[3] 企業の内部と外部のリソースを有機的に結合させ、新しい価値を創造すること（産学連携や企業間連携による共同研究など）

○　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、ＡＩ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ＡＩ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ＡＩ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。

（参考）「秘密情報の保護」の視点からのＡＩ利用

近年の生成ＡＩの進展に伴い、あまりＡＩを利用してこなかった多くの企業や組織においてもＡＩ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ＡＩですが、大きくクローズアップされた利便性の傍ら、ＡＩ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「ＡＩ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ＡＩ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ＡＩ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、ＡＩ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ＡＩ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ＡＩ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ＡＩを利用し、営業秘密にあたる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

[4] 「AI 原則実践のためのガバナンス・ガイドライン」 https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20220128_1.pdf ~~https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/20220128_report.html~~

ＡＩ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にあたる情報が漏えいした。

③　ＡＩの悪用による情報漏えいリスク

ＡＩ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、営業秘密にあたる情報が漏えいした。

ＡＩ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、ＡＩ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ＡＩの処理は何が想定されるのか、そうした処理に関するＡＩ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。ＡＩ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ＡＩ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、ＡＩを直接利用しないとしても、ＡＩ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。

ＡＩ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ＡＩを利活用することが望まれます。

○　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。

○　このように、秘密情報の管理を実施することには、個別の企業や働く方々にとっても、社会全体にとっても、その実施に係るコストを上回る効用があると言えます。したがって、経営者・情報管理責任者の方々は、この点を踏まえ、一時的な秘密情

[5] 経済安全保障推進法については、内閣府ＨＰにおいて情報が公開されている。
https://www.cao.go.jp/keizai_anzen_hosho/index.html

報の管理に係る手間・コストなどを嫌うことなく、秘密情報の漏えい事故は、企業価値の毀損につながる深刻なリスクである点を認識し、情報の適切な管理・取扱いを求める法令への受け身的な対応に終始するのではなく、企業価値の維持・向上にとっての深刻なリスクを回避し、むしろ企業価値・競争力の維持・向上に積極的・能動的に務めることも含めて、法令遵守の観点から、その実施に適切に取り組んでいただきたく思います。

（本書の留意点）

○　本書は、前述のとおり、企業の有する秘密情報の漏えいを防止するという観点からの様々な対策を示すものですが、情報管理に当たっては、本書で示すもの以外にも、情報を不正に改ざんさせないための対策（完全性の確保）や、システムダウンや災害時等にも情報が失われないようにするための対策（可用性の確保）なども重要となります。

○　また、秘密情報の漏えいの中には、従業員のミスによるものなど、漏えい者が意図しない形での漏えいも含まれますが、本書では、基本的に、意図的な秘密情報の漏えい防止を目的とした対策を紹介しています。ただし、本書において紹介する対策を実施することによって、意図的でない情報漏えいの防止にも相当程度の効果があるものと考えられます。

○　なお、本書では、本書策定の時点で有効であると考えられる対策を紹介しており、様々な技術の進展により、情報漏えいの手口やその対策が高度化・多様化するなどの状況の変化が生じた場合には、対策も、適時に見直されるべきものです。

（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、十分あ当てはまり、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。

１－２　本書の全体構成

（本書の全体構成）

○　第２章では、まずは自社が保有する情報の全体像を把握し、それを評価した上で、その中から秘密として保持すべき情報（秘密情報）を決定する際の考え方を説明します。

○　第３章では、秘密情報を同様の情報漏えい対策を講ずるものごとに分類する際の考え方と、具体的に講ずるべき対策等を示します。

○　第４章では、本書で示す様々な秘密情報の管理に係る方策をより実効的なものとするための社内体制のあり方を示します。

○　第５章では、他社の秘密情報に係る紛争に巻き込まれないため、又は万が一巻き込まれてしまったとしても正当にその立場を守るための対策を紹介します。

○　第６章では、自社の秘密情報が漏えいしてしまった場合の対応について説明します。

○　また、参考資料として、「各種契約書等の参考例」や「各種相談窓口」、「秘密情報管理に関する各種ガイドライン等について」、「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」、「競業避止義務契約の有効性について」を添付しています。

（情報漏えい対策の流れ）

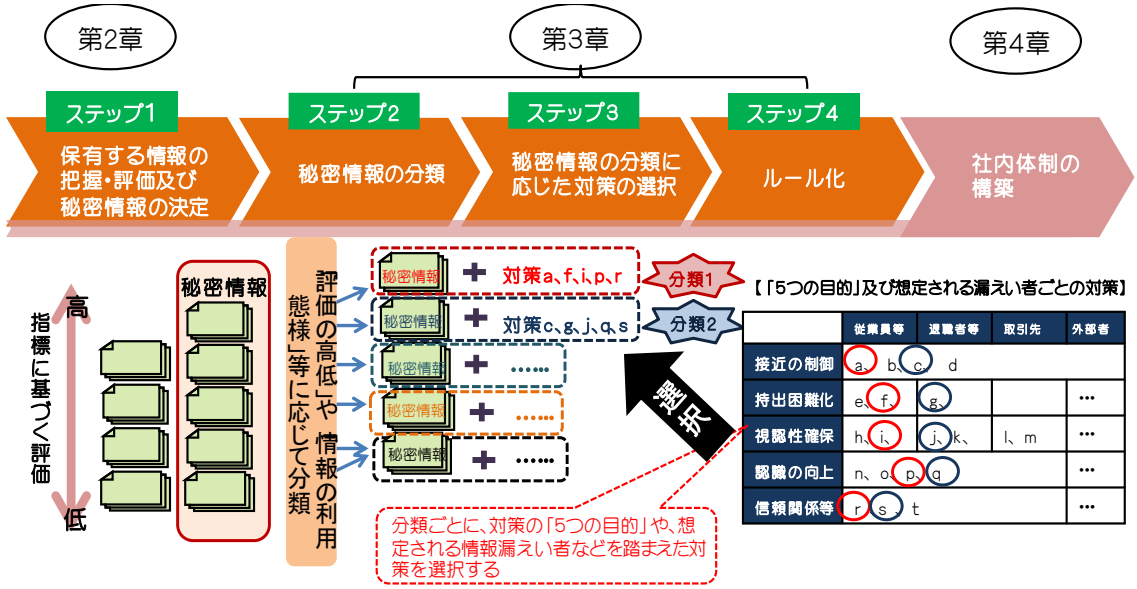
○　前述のとおり、第２章から第４章にかけては、

・　自社が保有する情報を把握・評価した上で、秘密情報を決定・分類して、実施する情報漏えい対策を選択する。

・　その内容について、社内においてルール化し、様々な状況の変化に応じて必要な見直しを行う

という情報漏えい対策の一連の流れとなっております。その流れを意識した上で第２章から第４章までを参照いただくと、より理解がしやすいものと考えられます。

図表１（１）情報漏えい対策の流れ



１－３　本書の使い方

○　本書では、様々な秘密情報の管理に係る方策を、本章１－２のとおりの順番で示していますが、各企業においては、必ずしも本書に記載された全てを、記載された順番に沿って実施しなければならないものではありません。また、企業における取組みの状況や企業の規模・業種・業態等により、できる範囲に絞り込んで着手するということが有効といえる場合も考えられますが、その場合であっても、措置されない部分についてのリスクを把握し、そのリスクを受容できるものかどうかも分析しておくことが必要です。

○　したがって、本書を読む時点で、どの程度の秘密情報の管理を既に実施しているかは企業によって大きく異なると考えられることから、例えば、次のコラムのように自社にとって特に参考となると考えられる箇所から読み始めていただいても構いません。

コラム①

本書をどのように使えばいいの？

情報漏えい対策を一から検討し直す必要がある？

既に、平成２７年改訂前の営業秘密管理指針やＩＳＭＳ（情報セキュリティマネジメントシステム）などの考え方を参考に、秘密情報の漏えい対策を実施しているが、このハンドブックに基づき、改めて一から情報漏えい対策を検討し直す必要があるのか知りたい。

→　本書は、基本的に、改訂前の営業秘密管理指針等に記載された対策を、犯罪学などの考え方を参考に整理して紹介するものです。そのため、既に対策を実施されている場合には、その全てを一から検討し直す必要はないと考えられますが、対策の更なる水準の向上や、対策の遺漏のチェックなどを行う際に、本書をお役立てください。

秘密情報の管理に関心はあるものの、自社は人員が少なく、費用もほとんどかけることができないが、そのような場合は秘密情報の管理は諦めるしかないのか。

→　第３章３－４において、具体的な対策例を多数紹介しています。その中には、必ずしも多くの費用が必要でない対策もありますので、本書も参照いただきながら、まずは、自社で行うことができる範囲内で対策の検討を始めていただくことをお薦めします。

保有する情報を漏れなく把握したい

自社の保有する情報にどのようなものがあるか、ある程度、把握できていると考えているが、重要な情報を見落としていないか、漏れがないか、改めて確認したい。

→　第２章２－１において、自社が保有する情報の把握方法の例や、把握に当たっての留意点などを記載していますので参照ください（ｐ１３４９～）。

秘密情報を決定するための社内基準をつくりたい

既に情報管理規程を策定しており、その規程に基づき、各部門において秘密情報の決定を行っているが、その決定が適切に行われるよう、指定に係る社内基準を定めたい。

秘密情報の分類が適切か確認したい

→　第２章２－２において、秘密として保持すべき情報か否かを判断する際に参考となる考え方を紹介していますので参照ください（ｐ１８４～）。

既に情報管理規程を策定しており、「極秘」、「社外秘」といった形で、自社の情報を

分類しているが、その分類の仕方が適切か改めて確認したい。
→　第３章３－１において、自社の秘密情報を分類するに当たっての考え方を紹介していますので参照ください（ｐ２１~~１７~~～）。

第２章　保有する情報の把握・評価、秘密情報の決定

- 企業が保有する情報は、その一つ一つの情報ごとに、その経済的な価値や漏えいしたときに生ずる損失、情報の性質・内容・存在形態等が異なっています。
- その違いを踏まえずに、闇雲に情報管理策を実施してしまうと、費用と手間がかさむ割には情報漏えい防止の効果が乏しくなったり、本当に必要なときに情報を利用できなくなるなど、業務効率の低下につながったりするおそれもあります。いたずらに秘密情報の対象範囲が広がることによって埋没してしまい、かえって、真に重要な情報をいざというときに守ることができないという状況も招きかねません。
- また、企業が保有する情報の中には、特許権などの権利を取得することによって、法的保護の下で公開しつつ活用すべきものや、個人情報のように法令の規定に基づいて必要かつ適切な安全管理措置を講じること~~外部への漏えいは一切許してはならず厳格な管理~~が求められるもの、さらに営業秘密や限定提供データのように法律による保護を受けるために相応の管理措置が講じられているもののように、多様な情報があります。よって、自社が保有する情報のうち、どの情報を公開し、どの情報を秘密情報とするのか（あるいは、法令又は契約に基づき~~より~~秘密情報として取り扱わ~~にし~~なければならないのか）を、自らの意思を持って適切に判断して組み合わせ、収益の最大化を図っていく必要があります。
- なお、情報の把握については、企業によって「有益・必要な情報」の洗い出しという観点だけでなく、その情報が存在することが有害な「不要情報」（例：他社から受け取った秘密情報のうちその保有権限を失ったものや、今後使用の見込みがなく、保有する意義が不明瞭な情報等）についても、企業や従業員等の情報機器や情報システムの中に残ったままではないか洗い出し、不要情報が紛れ込んでいた場合には消去・廃棄する必要があります。
- 本章では、まず自社が保有する情報全体を把握した上で、その評価を行い、それらの情報の中から秘密情報を決定するというステップ（図表１（１）で示したステップ１）の具体的方法について、順を追って紹介します。

（本章で紹介する方法について）

○　本章では、これから初めて秘密情報の管理を開始しようとしている企業を念頭に、自社が保有する情報[6]から秘密情報を決定するまでのステップを紹介しています。一方で、本書を参照する企業の中には、既に、保有する情報の全体像の把握、その

[6] ここでいう「自社が保有する情報」とは、事実上自社内に存在するあらゆる情報を対象としています。

評価、秘密情報の決定、秘密情報の取扱いに関する社内規程の整備など、取組みがある程度進んでいる企業も存在すると考えられます。

○　そのような場合には、本章で示す手順にこだわらず、自社の取組みの進捗状況に応じて、例えば、

- ２－２で示す観点を参考としながら、秘密情報とすべき情報に不足がないかどうかの検証として、漏えいした場合に甚大な悪影響がある、いわば「虎の子の情報」や「独自のノウハウ」等を、部署ごとに探し出し、それを報告させる
- 本章で示す評価・秘密情報の決定に係る観点を参考としながら、社内規程に基づき既に各部署において実施している秘密情報の指定が適切に行われているか否か、その社内規程自体が適切な内容となっているか否かなどを確認する

といった形で、本章で紹介する方法を参照いただくことが考えられます。どのような形であれ、自社が保有する情報の全体像が把握され、それらが適切に評価された上で、秘密情報とすべき情報が適切に決定されている状況となっていることが重要です。

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

○　秘密情報の管理のファーストステップは、自社の保有する情報を把握して、経済的価値や漏えい時の損失の程度といった指標に基づいて評価することです。このステップを通じて、企業は、単に秘密情報を決定するだけではなく、自社の持つ強みやその源泉を再確認して、今後の更なる競争力強化の可能性の検討につなげることができます。

（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═やＰＣ、ＵＳＢ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、Ｆ１品種の親系統となる植物、水産物[7]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共有・活用することの促進にもつながります。

○ なお、個々の企業における製品やサービスが変化するなど、企業活動、そしてそれを取り巻く環境は常に変化し、それに伴い技術情報や顧客情報、取引情報などの企業が取り扱う情報の種類や重要性も変化することがあります。したがって、必要に応じてその変化に対応した追加的な情報の把握や更新をすることも重要です。

（保有する情報の把握方法）

○ 保有する情報の把握に当たっては、個別の担当者の感覚によって、その判断にばらつきが生じないようにするため、事業規模や扱う情報の多寡等に応じて、社内で統一的な判断が可能となるような情報の把握方法を取ることが望ましいでしょう。例えば、具体的方法としては、以下のような方法が考えられます[8]。

① 経営者等の責任者が社内の各部署や担当者に対して直接ヒアリング等を実施することにより把握する方法

② 秘密情報の管理を統括する部署が統一的な基準を示しつつサポートしながら、各部署や個別の担当者に、その基準に則してそれぞれが有する情報を経営者等の責任者に報告させ、情報を集約することにより把握する方法

○ なお、自社が保有する情報を把握する際に、特に他社との差別化要因となっている（自社の強みとなっている）情報を漏れなく把握するためには、競合他社との製品・サービス等の差異を分析することが有効です。例えば、他社と比較して競争力が強い製品やサービス、高い売上げに結びつく特徴的な性質を持つものをピックアップし、その個性や特徴を生み出している要因を分析することで、自社が把握すべき情

---

7 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。

8 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。

報が見えてくるでしょう[9]。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の情報、プラントのレイアウトや試作品などの「物」自体の情報については、紙媒体や電子データ等の形の情報に比べて、その把握が難しい場合が多いと考えられるため、特にこのような考え方が有効です。

（把握に当たっての留意点）

○　保有する情報の全体像の把握といっても、自社内に現在存在する書類や電子データ等の一つ一つを網羅的に確認するということではありません。「○△製品の設計内容に係る情報」など、情報の種類を、一定程度、一般化・抽象化した形で把握することが必要となります。そのように把握することで、日々の業務の中、新たに生成されたり、入手したり、不要になるといった情報のライフサイクル等に伴い、常に変動する情報の全体像や取り扱う情報を適切に把握でき、後述の対策も立てやすくなります。

○　そして、その一般化・抽象化した形での情報の把握に当たっては、その後の情報の評価や分類といった作業を見据えて、情報にアクセスできる者の範囲や、重要度の大きく異なる情報が混在することのない一般化・抽象化の程度について、一定程度念頭に置いた上で行うことが望ましいでしょう。

（良い例）○△製品の設計内容に係る情報

（悪い例）○△業務に関する情報・・・情報の対象範囲が広すぎて具体的でないため、アクセス範囲を限定すべき非常に重要な情報と、アクセスを特に限定しなくてもよい一般情報が混在してしまいます。その結果、この後の情報の評価や分類が適切になされないおそれがあります。

○　なお、情報の把握については、企業によって「有益・必要な情報」の洗い出しという観点だけでなく、その情報が存在することが有害な「不要情報」（例：他社から受け取った秘密情報のうちその保有権限を失ったものや、今後使用の見込みがなく、保有する意義が不明瞭な情報等）についても、企業や従業員等の情報機器や情報システムの中に残ったままではないか洗い出し、不要情報が紛れ込んでいた場合には消去・廃棄する必要があります。このような取組みについても定期的・継続的に行うことにより、外部からの攻撃や従業員・退職者等による持ち出しを介した想定外の情報漏えい事故のリスクとともに、企業が保有し、管理を要する情報の総量を適

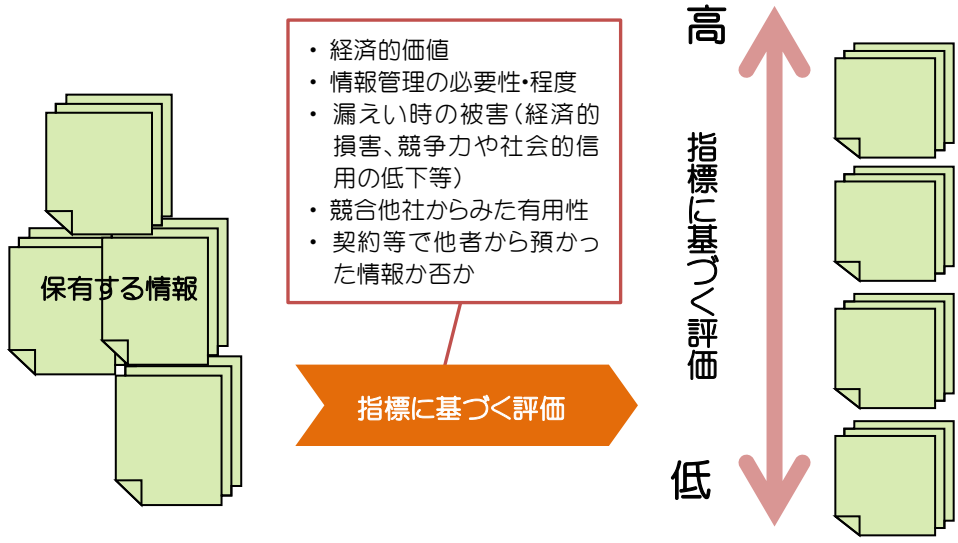
[9] 例えば、自社の主力製品が高い売上げを達成している理由として、その製品等が高い技術水準を有しているために他社の製品等と比べて競争力がある場合は、まずその技術自体が「自社の強み」といえ、その技術水準の実現を基礎付けている「製造ライン情報」、「人材育成プログラム」、「報酬体系情報」なども「自社の強み」と判断できます。

正化することによる情報管理のコストを減らすことにつながると考えられます。

（２）保有する情報の評価

○　次に、前述（１）の作業で把握した情報について、情報が生み出す経済的価値、情報管理の必要性・程度（法令や取引先との契約により強い管理が求められているのか、企業の判断により管理の要否・程度を選択できるのか）、他社に利用されたり、漏えいしてしまった場合の自社の損失の大きさ（どの程度競争力や社会的信用が低下してしまうのか等[10]）、競合他社にとって有用か否か、悪用されるような性格の情報か否か、契約等に基づき他社から預かった情報か否か等、以下の観点を参考に評価を行い、その評価結果に応じて情報を階層化します。なお、本書は秘密情報の保護を目的としていますので、ここで実施する評価の対象は非公表の情報や未公開の情報等を前提としています。

図表２（１）評価のイメージ



【評価に当たって考慮すべき観点の例】

- 情報の経済的価値（その情報によって生み出される現在の価値、及びその分野における技術革新のスピードや代替技術の有無等を加味した将来的な価値）
- 情報管理の必要性・程度（法令や取引先との契約により強い管理が求められているのか、企業の判断により管理の要否・程度を選択できるのか。
- 情報漏えい行為等によって被る損失の程度

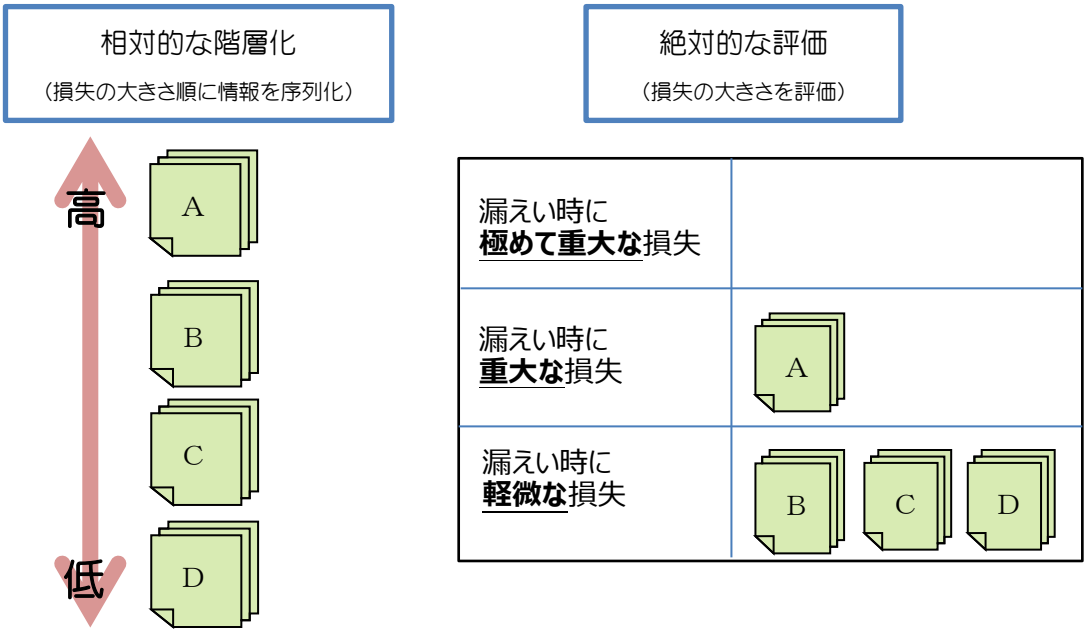
[10] 取引先の情報や顧客情報などについては、その漏えいによって、自社に対して損害賠償請求がなされる場合も考えられます。

- **取引先など他社に与える損失の程度（例えば、情報が漏えいした場合、その情報を使用して製造した部品を納めた取引先に生ずる損失の程度）**
- **競合他社にとっての有用性（情報が他社に渡った場合の他社のコスト削減及び他社製品の価格などへの影響の程度）**
- **情報漏えい時の社会的信用低下（顧客減少等）による損失の程度**
- **情報漏えい時の契約違反や法令違反に基づく制裁の程度**

等

※第３章において、同様の対策を講ずるものごとに秘密情報を分類することを見据えて、ここでは、評価の高低によって、情報を相対的に階層化することに主眼を置いています。しかし、自社の対策全体としてどの程度厳格な対策を講ずるかを判断するためには、それぞれの情報が漏えいした際の実際の損失の程度、情報管理の必要性・程度等を念頭に置いておく必要があります。そのため、情報の相対的な階層化に加えて、その情報が絶対的にどの程度の評価がなされるものかを意識しておくことも重要です（例えば、自社の情報のうち最も評価の高いものであっても、漏えいしたときの損失がそれほど大きくないという場合には、全体としてそれほど厳格な対策を講じなくても良い場合もあり得ます）。

図表２（２）相対的な階層化と絶対的な評価のイメージ
－情報を損失で評価した場合－



○　前述（１）（２）の作業により、自社が保有する情報にはどのようなものがあるのか、そのうち自社の競争力の源泉となるような価値の高い情報は何かを認識（再認識）することができます。価値の高い情報を「見える化」して自社の財産として位置づけられれば、今後の事業展開に役立てるとともに、企業価値・競争力の向上にもつなげることができます。

２－２　秘密情報の決定

○　次に、それぞれの情報の評価の高低を基準に、保護に値するものかどうかを判断します。保護に値するものであっても、その情報をより効果的に活用するための方法を、情報の性格に照らして検討することが重要です。

○　技術情報については、特許権など権利化して他社にライセンス[11]を行ったり、標準化を行うことを通じて、他社にも自社技術を広く使用させ自社技術の市場を拡大させるという活用方法もある一方で、他社との差別化を図るために情報を独占することによって、自社の技術的優位性を高めるという活用方法もあります。自社で独占する場合については、権利化した上で独占使用する方法や秘密として保持する方法が考えられますが、権利化する場合は情報が公開されることになりますので、情報の性質なども考慮し、その情報の価値が最大限高められる活用方法を慎重に選択することが重要です。

○　顧客情報については、権利化、標準化の対象とならない性格のものでもあり、秘密として保持する方が適切と考えられます。

○　商品として広く提供されるデータやコンソーシアム内で共有されるデータなど限定提供データに該当しうる情報については、企業間で複数者に提供や共有されることで、新たな事業の創出やサービス製品の付加価値の向上など、その利活用が期待されるデータであることから、そのデータがどのような価値を持つのかを十分考慮し、適切な法的保護を受けられるような形態で保持・提供することが重要です[12]。

○　保護を要するものかどうかを判断する際には、想定される管理コスト、訴訟コスト

11 他社へのライセンスについては、営業秘密などの権利化しないノウハウや、限定提供データが対象となる場合もあります。

12 限定提供データとして保護される情報についても、意図せざる利用・流通への対策や法的保護を受ける前提として相応の管理が必要であり、この意味で管理が必要な重要情報と評価可能であることから、秘密情報に並びうるものとして取り上げています。

（証拠収集等のための労力、費用、訴訟期間等）等のコスト、漏えいによって被るおそれのある損失、保護により得られる利益（損害賠償請求や侵害差止請求により取り戻すことが容易か否か）の総合考慮という観点から保護する意義がどの程度あるか、法令や他社との契約による特別の管理を求められる情報か否かという視点での判断が必要となる場合もあると考えられます。また、Ｓｏｃｉｅｔｙ５．０においては、重要な情報・データを組織外から大量に取得する機会や外部と共同して利活用する機会が増えていくものと考えられることから、外部から取得・入手した重要な情報・データを、組織内において、取得時の条件を遵守して取扱い、コンプライアンスを確保することが今まで以上に重要になると考えられます。

○　そのなかで、秘密として保持することを決定した情報が、自社の秘密情報となります。

○　以下では、真に秘密として保持するべき情報を判断し、自社の秘密情報を決定する際に参考となる観点を紹介します。

（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

○　自社独自の情報であり、それが漏えいした場合、自社の競争力が低下する情報か否か

（取引価格や取引先に関する情報、接客マニュアル、公表前のデザイン　等）

○　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、受託契約~~や~~・ライセンス契約~~、~~・Ｍ＆Ａ~~における~~交渉における~~（事前協議を含む。）~~ＮＤＡ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）

②技術情報

○　市場に流通する自社の製品等を分析することによって容易にその製品に用いられている技術が判明してしまい、他社がすぐに追いつくことができる技術に関する情報か否か

→　容易に判明する情報であれば、特許権などの知的財産権として権利化した方が活用しやすい可能性があります。

（部品の組合せ方法、新規素材の成分　等）

○　**権利化した場合であっても、権利侵害の探知や立証が難しい情報か否か**

→　権利侵害の探知等が難しいものは、権利化のコストに見合う権利行使ができない可能性があるため、秘密情報とする方が良い可能性があります。

（製造ノウハウ　等）

○　**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**

（受託契約・~~や~~ライセンス契約・~~、~~M＆A~~における~~交渉における~~（事前協議を含む。）~~ＮＤＡ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）

○　**通信技術や試験方法などの社会基盤や技術標準となる技術であり、自社利益の最大化のためには当該技術の市場の拡大が求められる情報か否か**

→　将来的な市場拡大が見込めるので、秘密情報とするのではなく、権利化・標準化した方が良い可能性があります。

※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。

※情報の評価の結果、情報漏えいの際の損失がほぼ生じず、侵害企業との訴訟に係る費用や管理コストのほうが確実に被害額を上回ると考えられる場合には、その情報については、積極的には公開しないものの、コストをかけて秘密として保持するための対策は行わないこともあり得ます。

○　**以上の観点等により検証した結果、秘密として保持すべきと判断される情報を自社における秘密情報として決定し、第３章における情報漏えい対策の対象とします。**

第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

- 秘密情報の活用の促進、管理コストの適正化等の観点から、秘密情報の評価等に応じたメリハリのある情報漏えい対策を講ずることが重要です。そのためには、自社の秘密情報を、その評価の高低や情報の利用態様等に応じて、同様の管理水準であると考えられるものごとに分類した上で、その分類ごとに適切な対策を選択することが必要です。
- 本章では、そのような「秘密情報の分類」に係る考え方や、講ずる対策を選択する際に参考となる具体例等を紹介します。（図表１（１）で示したステップ２、ステップ３）
- 本章では、比較的簡易な管理方法から高度な管理方法まで様々な具体的対策例を提示していますが、その全てを実施しなければ情報漏えい対策として不十分ということではありません。本章で提示する対策を参考に、各社の企業規模、業種、秘密情報の内容・性質・存在形態、対策にかけることができる費用の多寡等の様々な状況に応じて、合理的かつ効果的と考えられる対策を適切に取捨選択・工夫して実施することが重要です。
- また、分類や対策は一度決めたら終わりではなく、情報のライフサイクル（生成→利用→保存→廃棄）における各ステージや様々な技術の進展等を考慮しつつ適宜見直していくことも重要です[13]。
- さらに、ここで記載する一連の流れを実効的にするためには、その内容を社内ルール化して社内で共有化しておくことも重要です。
- なお、第１章で述べたとおり、本章で示す対策を実施することは、秘密情報の漏えいを防ぐだけでなく、人材の流動性の向上を通じた多様な人材確保やオープンイノベーションの更なる進展にも寄与します。

３－１　秘密情報の分類

（分類の必要性）

[13] 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（https://www.jnsa.org/ikusei/01/02-02.html~~http://www.jnsa.org/ikusei/01/02-02.html)、http://www.jnsa.org/ikusei/01/02-02.html)~~、IPA「中小企業の情報セキュリティ対策ガイドライン」（https://www.ipa.go.jp/security/guide/sme/about.html）~~https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html)~~ 参照

○　第２章において、自社における「秘密として保持すべき情報」（秘密情報）が決定されることとなりますが、秘密情報は日々の業務の中で活用されてこそ価値を発揮するものであることを踏まえると、すべての秘密情報に一律に厳格な管理を行うことは、円滑な業務の実施に支障を及ぼし、また管理コストの無用な増大を招く結果となります。例えば、企業活動に不可欠な情報であっても、漏えいをおそれるあまり、金庫のように常時鍵を掛けて誰も開けてはならない場所に保管して事業活動に一切使わないのでは、その情報は活用されず、資産としては無価値なものとなります。情報の活用と管理のバランスを考慮した適正な管理方法を検討していくことが重要です。

○　そのためには、各企業で取り扱う秘密情報の内容・性質やその評価の高低、その利用態様、企業において採用することが可能な管理措置等の事情に応じ、秘密情報を同様の管理水準であると考えられるものごとに分類した上で、その分類ごとに必要な対策をメリハリをつけて選択することが重要です。

○　なお、分類の数については、各企業において適正と考えられる分類数は異なるものと考えられますが、あまりに多くの分類数としてしまうと、情報管理が煩雑となり対策が徹底されなくなってしまうなど、対策の有効性・効率性を低減してしまうおそれがあることに留意します。

（分類に当たっての考え方）

○　秘密情報の分類においては、まず、第２章２－１において行った情報の評価の結果を考慮し、評価の高い情報ほど厳格な対策を行うことが考えられます。

○　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ＰＣ、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」、「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。

【情報の利用態様として考慮すべき観点の例】
- 個々の従業員が手軽に閲覧・持出し・利用等をできるようにしておかなければ日々の業務遂行が困難となる情報か否か（例：従業員が営業を行うに当たって頻繁に用いる顧客情報）
- 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
- 情報に対するアクセス権者の範囲が広くならざるを得ない性質のものか否か（例：世界各地の研究拠点と共有する実験データ）
- その情報を活用する従業員の職務は何か
- 外部ネットワークに接続されたＰＣ、クラウドなどの外部サービス等に保管されることが多い情報か否か
- 顧客や取引先に開示することが多い情報か否か
- サプライチェーンで共有する必要がある情報か否か
- 日々更新される情報か否か（開発情報、顧客情報など）

※「同程度の評価の情報でも異なる対策を講ずる場合」とは、例えば、個々の従業員が手軽に閲覧・持出し・利用等をできるようにしておくべき情報については、他の情報に比べ簡易な管理を行うことが望ましいといったような場合や、情報に対するアクセス権者の範囲が広くならざるを得ない情報については、５つの「対策の目的」（後述）のうち、「接近の制御」に係る対策よりも、「視認性の確保」に係る対策を重点的に選択することが有効であるといったような場合を指します。

○　また、個人情報保護法に基づく取扱い管理が求められる個人情報や、他社から秘密保持義務を負った状態で受領した情報（営業秘密、限定提供データのほか、契約・信義則に基づく秘密保持義務を負っている情報）など、「法令や他社との契約に基づく特別の管理」を求められる情報については別の対策を講ずる分類とすべき場合もあります。

○　このように、情報の評価の高低の観点に加えて、「情報の利用態様」や「法令や他社との契約による特別の管理」の観点から、別の対策を講ずる分類を設けることも考えられます。

※社内の統一的なルールでは、情報の評価の観点からの分類のみ設けておき、例えば、各

部門の管理責任者が行う「分類の指定」等の運用の段階において、「情報の利用態様」や「法令や他社との契約に基づく特別の管理」の観点を考慮するといったことも考えられます。

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）

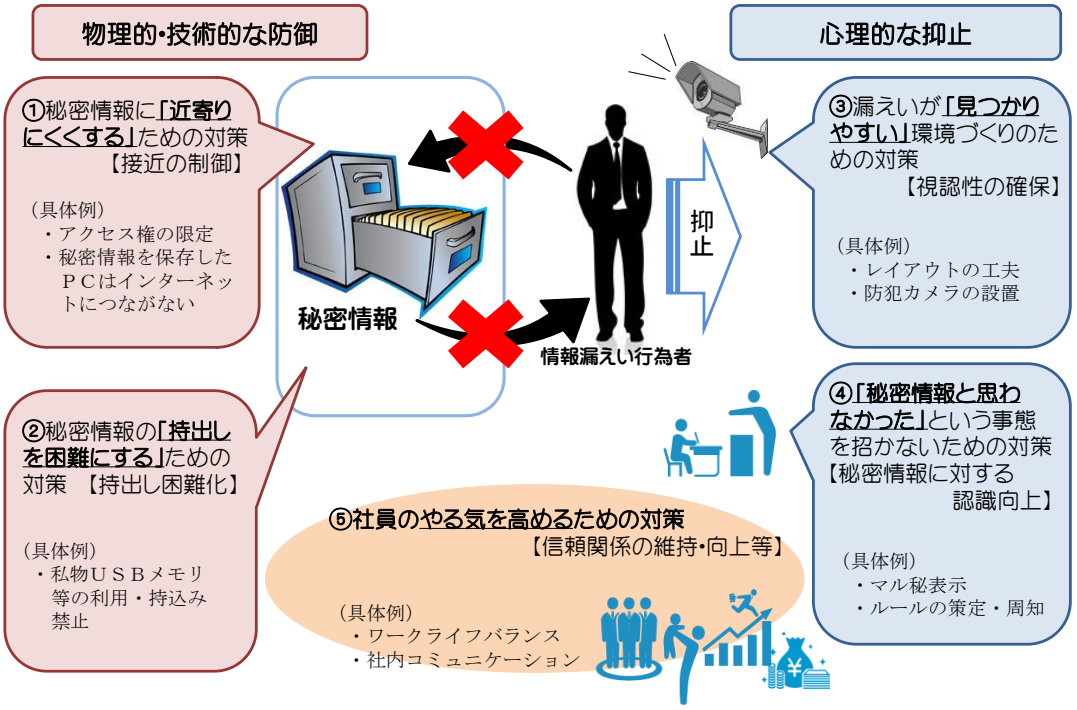
○　本章３－１において設定した秘密情報の分類ごとに、具体的にどのような情報漏えい対策を講ずるのかを選択します。その際には、誰に対して対策を行うのか（従業員、退職者、取引先、外部者）、どのような形で秘密情報が存在しているのか（情報にネットワークを介してアクセスすることができるか、工場ライン等の物件自体が秘密情報である場合か否か等）、漏えいの手口やその動機がいかなるものであるかといった状況によって効果的な対策は異なることに留意する必要があります。加えて、転職者の増加や、様々な契約形態に基づく人事やグローバル人材の登用、テレワークの導入・実施状況や個人端末による情報利用の可否、生成ＡＩなどの利用（生成ＡＩなどに、自社が保有している情報を入力すること）の可否など、各社の事情に応じた対策を選択することが有効です。

（５つの「対策の目的」）

○　情報漏えい対策は、目的を考えずに闇雲に実施してしまうと、業務への過度な制限や、無駄なコストが発生しかねません。したがって、情報漏えいに対し、それぞれの対策がどのような効果を発揮するのかといった目的を意識し、効果的・効率的な対策を選択することが望まれます。

○　そこで、本章においては、場所・状況・環境に潜む「機会」が犯罪を誘発するという犯罪学の考え方なども参考としながら、秘密情報の漏えい要因となる事情を考慮し、以下の５つの「対策の目的」を設定した上で、それぞれに係る対策を提示しています。

図表３（１）５つの対策の目的



【５つの「対策の目的」】

（１）接近の制御

秘密情報を閲覧・利用等することができる者（アクセス権者）の範囲を適切に設定した上で、施錠管理・入退室制限等といった区域制限（ゾーニング）等により自らが権限を有しない秘密情報に現実にアクセスできないようにすることで、アクセス権限を有しない者を対象情報に近づけないようにすることを目的としています。

なお、「接近の制御」に係る対策のポイントは、まず、アクセス権を有する者が、本当にその情報について知るべき者かという観点から適切に限定されることであり「接近の制御」に係る対策を講ずる前提として、まずは社内の規程等により、アクセス権設定に係るルールを策定することが必要となります。

また、今後、さらに普及・常態化するテレワークにおいては、外部からの情報へのアクセスをよりきめ細かい単位で制御することが求められるようになるため、細かいアクセス権限管理に対応できるアクセス管理基盤の整備、雇用関係の終了や契約の終了に伴い速やかなテレワークでのアクセス権限の削除が望まれます。

（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ＰＣ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ＵＳＢ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、ＰＣ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ＶＰＮ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ＡＩ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、これらの利用の当否を判断する、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。

（３）視認性の確保

職場のレイアウトの工夫、資料・ファイルの通し番号管理、録画機能付き防犯カメラの設置、入退室の記録、ＰＣのログ確認等により、秘密情報に正当に又は不当に接触する者の行動が記録されたり、他人に目撃されたり、事後的に検知されたりしやすい環境を整えることによって、秘密情報の漏えいを行ったとしても見つかってしまう可能性が高い状態であると認識するような状況を作り出すことを目的としています。近年は、ＡＩ等の最新技術を組み入れた高度な内部不正モニタリングシステムの開発も進んでおり、これを活用することが有効と考えられます。このほか、可視性を強化してセキュリティコントロールのレベルを維持する努力[14]も行うことも有効と考えられます。

また、ここでの対策は、従業員等の行為の正当性（身の潔白）を証明

14 例えば、ＥＤＲ（Endpoint Detection and Response）の導入が考えられます。これは、ＰＣ、サーバ等のエンドポイント上で、長期間イベント（ファイル作成・削除、プロセスの実行・停止、ネットワークアクセス、ログオン・ログオフ等）の内容を記録し、エンドポイントにおける不審な挙動や異常を検知し、管理者に通報して早期の対応を支援するソリューションで、組織内外のエンドポイントに侵入された場合には、検知された異常に対して素早い対応ができるようにすることで、被害の拡大の抑止につながります。

する手段としても有効であり、このような従業員をモニタリングすることの目的が従業員の保護であることを就業規則等に明記して従業員に周知徹底するとともに、従業員の理解を得た上で、適切な運用を行うことが必要です。

さらに、現実に監視するというだけでなく、例えば、職場の整理整頓や従業員等に文書管理責任を分担させて情報管理に関する当事者意識を持たせたりすることで、職場を管理の行き届いた状態にすることにより心理的に漏えいしにくい状況を作ることも含まれます。

なお、情報漏えい行為の状況などを記録する対策等は、情報漏えいが生じた場合の行為者に対する責任追及の際に必要となる証拠の確保手段としての意義もあります。

特に、テレワークの実施との関係では、自宅、サテライトオフィスなど職場と同レベルでの視認性を確保することが困難となることが想定されることから、テレワークに伴う秘密情報・重要情報へのアクセス履歴、操作履歴（Ｗｅｂへのアクセスログやメールの送受信履歴など）等のログ・認証を記録し、一定の期間に安全に保存することが視認性の確保のための対策としても有効であると考えられます。

（４）秘密情報に対する認識向上（不正行為者[15]の言い逃れの排除）

秘密情報の取扱い方法等に関するルールの周知、秘密情報の記録された媒体へ秘密情報である旨の表示を行うこと等により、従業員等の秘密情報に対する認識を向上させることを目的としています。これにより、同時に、不正に情報漏えいを行う者が「秘密情報であることを知らなかった」、「社外に持ち出してはいけない資料だと知らなかった」、「自身が秘密を保持する義務を負っている情報だとは思わなかった」といった言い逃れができないようになります。

また、企業と退職予定の従業員との関係によっては、退職予定者が秘密保持誓約書の提出を拒否することがあり得ることから、退職時だけでなく、入社時や配属先の異動時、重要プロジェクトへの配属時・転出時・終了時にも、秘密保持契約を取り交わすことが秘密情報に対する認識向上のための対策として有効であると考えられます。

（５）信頼関係の維持・向上等

従業員等に情報漏えいとその結果に関する事例を周知することで、秘

15 ここでいう不正行為者とは、実際に不正に情報漏えいを行う者を意味し、従業員等を不正行為を行う可能性のある者としてみだりに疑う趣旨ではありません。

密情報の管理に関する意識を向上させます。また、働きやすい職場環境の整備や適正な評価等によって企業への帰属意識を醸成したり、仕事へのモチベーションを向上させます。これらの取組みによって、職場のモラルや従業員等との信頼関係を維持・向上することを目的とします。

従業員等との信頼関係を維持・向上するための取組みは、企業の生産性向上や効率的な経営の実現などの観点からも重要なポイントであるため、企業においては既に創意工夫を凝らしながら様々な取組みが実施されているところですが、これらの取組みが、情報漏えい対策としても有効であると考えられます。

また、テレワークの実施との関係では、テレワーク実施中の従業員等は疎外感や不安感に悩むことが多いだけでなく、不審な挙動がすぐには見つからない状況にあることや外部の脅威者からのアプローチを受けやすいと考えられます。そこで、対策として悩みに対して相談・助言を提供する窓口の設置やコミュニケーションツールの整備、定期的なアンケートによる疎外感・不安感を感じている従業員等の可視化、オンライン会議での定期的な職場コミュニケーションの実施、定期的な出勤日の設定等を通じて、過度な干渉にならない程度の良好で十分なコミュニケーション機会を確保することは、従業員等の不安感・疎外感の払拭につながる上、信頼関係の維持・向上のための対策としても有効であると考えられます。

○ なお、ここで紹介する対策のうち、「接近の制御」、「持出し困難化」、「視認性の確保」、「秘密情報に対する認識向上」に資する対策の中には、不正競争防止法上の「営業秘密」の要件である「秘密管理性」を満たすために必要な「認識可能性（第１章１－１参照）」の確保につながるものや、従業員のミスによる漏えいの防止につながるものもあります。

（対策の選択の方法）

○ 本章冒頭で述べたとおり、本章では、比較的簡易な管理方法や、より高度な管理方法など、様々な難易の対策を提示していますが、そのすべての対策を実施しなければ、情報漏えい対策として不十分ということではありません。本章で提示する対策を参考に、各社の企業規模や業種、秘密情報の評価や利用態様、対策にかけることができる費用の多寡等の様々な状況に応じて、合理的かつ効果的と考えられる対策を適切に取捨選択・工夫して実施することが重要です。

○　また、５つの「対策の目的」を考慮しながら、バランス良くそれぞれの目的に応じた対策を選択していくことが重要です。企業の規模、保有する情報の性質、その情報をどのような利用態様で活用するのかといった事情を考慮して、重視すべき「対策の目的」を選択して、ムリ、ムダ、ムラの無い形で対策を講じていくことが考えられます。

３－３　秘密情報の取扱い方法等に関するルール化

（１）ルール化の必要性とその方法

○　本章に記載するステップを通じて、決定された対策を実効的に講じていくためには、その内容を社内でルール化することが必要です。

○　ルール化の方法としては、就業規則、情報管理規程といった社内の規程を策定することが一般的です。いずれの場合においても、従業員等が、秘密情報の管理を適切に行うことができるよう、秘密として保持すべき情報、その取扱い方法について理解できる内容としておくことが重要です。

※ルール策定に当たっては、従業員とのコミュニケーションを十分に取りながら進めることが、透明性確保・従業員の認識の向上を図るために重要です。

○　近年、テレワークが普及し、常態化しつつありますが、秘密情報のレベルに応じたアクセス制限やＰＣ等への格納の制限を行わないと、企業の管理下にない個人所有のＰＣ等に秘密情報を格納したり、従業員等関係者以外の者が秘密情報にアクセスしたりする可能性があります。このため、テレワークでクラウドサービスを利用する場合に、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取り扱い、当該情報をクラウド上に置く際のアクセス権限を適切に設定すること等[16]で、秘密情報の漏えい防止に効果があるため、テレワーク中に従業員が遵守すべきルールを社内ルールの中で定めることが必要です（就業規則や情報管理規定といった既存の規定に追加する、またはテレワークに特化したルールを別途作成するなど、方法は各社の事情に応じて対応を進めることが望ましいと考えられます。）。

○　さらに、近年、ＡＩ技術の進展を踏まえて、外部の生成ＡＩ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ＡＩ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当否を判断する、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ＡＩなどを利用する場合には、予め許可された生成ＡＩ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

[16] これらのほかにも、多要素認証を採用するなどといった認証の強化、不要なアカウント権限の削除、定期的な設定のチェックなどが秘密情報の漏えい防止に効果があります。

成ＡＩ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。

（２）秘密情報の取扱い等に関する社内の規程の策定

○　秘密情報の管理について社内の規程を策定することは、秘密情報の取扱い等に関するルールを社内に広く周知するための手段として効果的です。

○　従業員等が秘密情報の取扱いや、秘密情報に関して秘密保持義務が課されていること等について、十分理解できるようにするため、社内の規程には以下の内容を盛り込んでおきます。

（社内の規程に盛り込んでおくとよい条項）
※条項によっては、その詳細が規程に基づいて別途作成される細則や別紙等に記載される場合もあります[17]。

①適用範囲
：役員、従業員、派遣労働者、委託先従業員（自社内において勤務する場合）等、本規程を守らなければならない者を明確にします。
②秘密情報の定義
：本規程の対象となる情報の定義を明確化します。
③秘密情報の分類
：分類の名称（例えば、「役員外秘」、「部外秘」、「社外秘」）及び各分類の対象となる秘密情報について説明します。
④秘密情報の分類ごとの対策
：「秘密情報が記録された媒体に分類ごとの表示をする」、「アクセス権者の範囲の設定」、「秘密情報が記録された書類を保管する書棚を施錠管理して持出しを禁止する」、「私物のＵＳＢメモリの持込みを制限し複製を禁止する」など、分類ごとに講ずる対策を記載します[18]。
⑤管理責任者
：秘密情報の管理を統括する者（例えば、担当役員）を規定します。
⑥秘密情報及びアクセス権の指定に関する責任者
：分類ごとの秘密情報の指定やその秘密情報についてのアクセス権の付与

17 秘密情報の取扱い等に関する社内規程の参考例については、参考資料２の「第２　秘密情報管理規程の例」を参照。
18 秘密情報の分類毎の対策に関する規定の参考例については、参考資料２の第２　２．における「秘密情報管理基準（例）」を参照。

を実施する責任者（例えば、部門責任者、プロジェクト責任者）について規定します。

⑦秘密保持義務

：秘密情報をアクセス権者以外の者に開示してはならない旨などを規定します。

⑧罰則

：従業員等が秘密情報を漏えいした場合の罰則を定めておきます。

○　なお、社内の規程を周知して、従業員等の秘密情報の取扱い等についての理解を深めることは、それ自体が「秘密情報に対する認識向上」に資する対策となります。

○　また、テレワークの実施に際しては、企業組織の外で業務を行う中で秘密情報を取り扱う可能性があり、秘密情報の漏えいリスクが高まると考えられることから、秘密情報の漏えい対策の強化が求められます。詳細については、総務省「テレワークセキュリティ対策第５版（令和３年５月）」[19]、ＩＰＡ「組織における内部不正防止ガイドライン（第５版。令和４年４月）」[20]をご覧ください。社内の規程を周知して、従業員等の秘密情報の取扱い等についての理解を深めることは、それ自体が「秘密情報に対する認識向上」に資する対策となります。

【テレワークなど企業組織の外での業務における秘密情報の保護のための対策のポイントの例】[21]

- 電車内やカフェ等では画面を覗き込まれないように注意する。また、秘密情報について大声で会話し、漏えいが発生しないように注意する。
- 不特定多数の利用者が利用するネットワーク（例：ホテルの有線ＬＡＮ・無線ＬＡＮ、公衆無線ＬＡＮ）の接続を許可するかどうかを判断する。また、許可されたネットワーク環境から企業のネットワークに接続する際には、秘密情報を暗号化したり、ＶＰＮ等を用いて通信を暗号化する。
- 外部から企業ネットワークに接続する場合、テレワークで用いるＰＣ等には電子データを可能な限り保存しないことが望まれる。
- 採用するテレワークの方式によっては、その特性に応じた情報漏えいの対策の強化が求められることがある。（例：テレワーク用ＰＣ上にデータ

19 https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

20 組織外部での業務における重要情報の保護についてどのようなリスクがあるか、どのような対策かを講じるべきかにいては、ＩＰＡ『組織における内部不正防止ガイドライン』（https://www.ipa.go.jp/security/guide/insider.html~~https://www.ipa.go.jp/security/fy24/reports/insider/~~）を参照。

21 ＩＰＡ『組織における内部不正防止ガイドライン』ｐ６１－６４を参照。

の保存が可能な場合、端末の内蔵記憶装置の暗号化やデータのリモートワイプの対策強化）

- これらの対策を前提として、組織外での業務（テレワーク）を認めるにあたり、従業員遵守すべき事項を定め、従業員の服務規律として就業規則等の内部規定でその遵守を求める。また、定めた内部規定について、定期的に実施状況を把握し、改善を図ることも必要。
- 企業の外部での共同作業（テレワーク等）でクラウドサービスを利用する場合、利用する情報がクラウドサービスで取り扱って良い情報かどうかの判断基準を定めて遵守を求めるとともに、セキュリティ確保のためのルール（多要素認証の設定、パスワードの使いまわしを避ける、データの共有範囲の設定、不要なアカウント・権限の削除等~~クラウドサービスで用いるパスワードについて他の用務で用いるパスワードとの共用を避けるなどの厳格な管理、データの共有範囲の限定等~~）を定めて、対象となる従業員に教育を通じて徹底を図る。
- 海外からのテレワークは、インシデント発生時の自社からの対応が困難であること、外国政府による監視の可能性・リスク、データの管理・取り扱いに対する現地の法制度への配慮が必要であることなどからリスクが高く、特別な情報漏えい対策を検討する必要がある。

コラム②

秘密情報が漏えいしてしまうと会社が大きな損失を被る、といっても、具体的にどのような損失が生ずるのでしょうか。ここでは、秘密情報の漏えいにまつわる事例も参照しながら、秘密情報の漏えいが、企業活動にとっての大きな脅威となることを、改めて確認していただければと思います。

こんなに怖い、秘密情報の漏えい

秘密情報は、競合他社に対して秘密であることで、自社の競争力の源泉となっており、それが漏えいしてしまうと、秘密情報の経済的価値が損なわれてしまうこととなります。

秘密情報の価値が失われてしまう！

製鉄業を営む大企業の元従業員が、韓国の競合企業に製鉄プロセス・製鉄設備の設計図などを漏えいした事案では、約 1000 億円の損害を被ったとして、その賠償などを求める訴訟が提起されました。この技術情報は、開発までに 20 年以上の期間がかかりましたが、情報漏えい先企業は、そのような投資コストを払うことなく、その技術を使用した製品を販売し、多額の売上げにつなげていました。また、この事案では、その韓国企業から、さらに別の中国の競合企業にも再漏えいがあったとされており、一度起こった情報漏えいの被害は、想像を超えて拡大するおそれも含んでいるといえるでしょう。

また、電気機械器具製造業を営む大企業の、NAND 型フラッシュメモリに関する仕様や検査方法が、業務提携先に勤める元従業員を通じて、韓国の競合企業に漏えいしてしまった事案でも、約 1100 億円の損害賠償請求がなされました。

社会的信用も低下してしまうおそれ

顧客情報などの秘密情報が漏えいしてしまった場合、競合他社に顧客が奪われてしまうリスクが生ずるだけでなく、その顧客対応に多くのコストがかかってしまうことに加え、情報を漏えいさせてしまった事実が、企業の社会的信用を低下させてしまうおそれもあります。

教育サービス業を営む大企業の顧客名簿が、業務再委託先の従業員を通じて漏えいしてしまった事案では、名簿を取り扱う業者なども介在して、その顧客名簿が約 500 社に拡散されたと言われています。お詫びの書状等の送付など、漏えいした名簿に記載された顧客への対応だけでも、多額の費用が必要となったことに加え、顧客情報を漏えいさせてしまったとして個人情報保護法に基づく監督省庁からの行政措置を受けることとなりました。

逆に訴えられる顧客からの訴訟

また、それだけに留まらず、インターネット接続サービス業を営む企業の会員情報が、ア

カウント管理の抜け穴を突いた不正なアクセスにより漏えいしてしまった事案においては、一部の会員から、その企業に対して慰謝料を求める民事訴訟が提起されました。このように、情報漏えいの被害者であったはずが、情報管理の不備があったとして、情報漏えいの加害者として逆に訴えられてしまうこともあるのです。共同・受託研究など、取引先と互いの秘密情報を共有したり、転職者の受入れに際して、転職元企業の秘密情報が図らずも自社に紛れ込んだりするといった場面においても、情報管理が不十分である場合、秘密情報を漏えいした加害者として訴えられてしまうリスクがあるといえるでしょう。

さらに、上記の事例から分かることは、秘密情報の漏えいは、会社の従業員等の内部者だけでなく、退職者、委託先、不正アクセス者などの外部者も含めて、様々な経路から起こり得るということです。秘密情報の漏えい対策を講ずるに当たっては、そのような経路の違いを意識することで、より実効的で効率的な対策を実施できるでしょう。

秘密情報の漏えいの経路を意識

本書では、第３章３－４において、「従業員等」、「退職者等」、「取引先」、「外部者」のそれぞれに向けた対策を紹介していますので、参考にしてください。

コラム③

外国から狙われる企業の秘密情報

企業が保有する秘密情報は、意図的に窃取されるリスクにさらされています。

自社の従業員が秘密情報を持ち出して競合他社へ転職してこれを漏えいさせてしまったり、自社の秘密情報を共有・開示した取引先が悪意でこれを競合他社に渡してしまったり･･･こうしたライバル企業との競争の中で行われる秘密情報の窃取は、かねてから秘密情報の漏えいをめぐる問題として捉えられてきましたが、問題となるのはこのようなケースだけではありません。

近年、地政学上のリスクがクローズアップされ、国際的な産業競争も激しくなる中、日本の企業や研究機関が保有する高度な技術情報をはじめとする秘密情報は、これら情報を入手して自国の産業の地位を高めたり、軍事技術に転用したりしようとする外国からも狙われるようになっているのです。

外国のスパイ活動といえば、国の機関を対象に行われるイメージがあるかもしれませんが、最近では企業や研究機関で働く人々にも及ぶようになっています。これを受け、米国や英国などでは、普段は公に発信することの少ない防諜・治安機関が、積極的に企業等に対する情報提供活動（アウトリーチ活動）を展開し、企業等における秘密情報の保護の取組に貢献しています。日本でも、企業や研究機関に対し、スパイの手口や対策のノウハウを情報提供し、対策に役立ててもらうためのアウトリーチ活動が警察において積極的に進められています。

外国から企業等の秘密情報が狙われるリスクのパターンについて、警察などが把握した事例を基に大まかに分類すると、以下のとおり整理することができます。

① サイバー攻撃による秘密情報の窃取
② スパイ~~となる者を仕立てた~~工作による秘密情報の窃取
③ ~~通常の~~経済・学術活動~~に見せかけた~~を通じた秘密情報の窃取

企業等の秘密情報を確実に守るためには、「自社には狙われるような情報はない」と~~考えず~~思い込むことなく、想定される様々なリスクを認識し、これに応じた具体的な対策を講じることが必要となります。以下に掲げたそれぞれのリスクの内容と留意すべき点をまずはしっかりと認識し、本書で掲げた具体的対策（３－４参照）を講じる際の参考としてください。

① サイバー攻撃による秘密情報の窃取！

国内外で政府機関や重要インフラ事業者等を標的としたサイバー攻撃が激しさを増していますが、あらゆる産業でＤＸ（デジタルトランスフォーメーション）が進むにつれ、企

業等がサイバー攻撃や不正アクセスによって、直接的に秘密情報を窃取される危険性も増しています。

こうしたリスクに対応するためには、まず、各企業において、特に経営者のリーダーシップの下、サイバー攻撃に対する認識を深め、企業等にとって本当に守らなければならない情報を特定（２－２参照）するとともに、本書で掲げた対策（コラム④、コラム⑤参照）とあわせて、以下に掲げる基本的対策を講じることが効果的だと考えられます。

1　リスク低減のための措置

○　パスワードが単純でないかの確認、アクセス権限の確認・多要素認証の利用・不要なアカウントの削除等により、本人認証を強化する。

○　IoT 機器を含む情報資産の保有状況を把握する。特に VPN 装置やゲートウェイ等、インターネットとの接続を制御する装置の脆弱性は、攻撃に悪用されることが多いことから、セキュリティパッチ（最新のファームウェアや更新プログラム等）を迅速に適用する。

○　端末のセキュリティ機能の活用や、セキュリティ対策ソフトの導入を行う。

○　ソフトウェア及び機器のリストを管理し、不要と判断するものは排除する。また役割等に基づいてネットワークを分割する。

○　メールの添付ファイルを不用意に開かない、URL を不用意にクリックしない、連絡・相談を迅速に行うこと等について、組織内に周知する。

○　近年のランサムウエアの流行に対抗するため~~には、、~~情報窃取被害によるリスク低減を図る観点から自組織で保管する重要データ~~の~~を暗号化するが~~必要となると考えられます~~。

○　保有するアプリケーション・システムに対する定期的な脆弱性診断やペネトレーションテストを実施する。

2　インシデントの早期検知

○　サーバ~~ー~~や PC、ネットワーク機器等における各種ログを確認する。

○　通信の監視・分析やアクセスコントロールを再点検する。

3　インシデント発生時の適切な対処・回復への備え

○　データ消失等に備えて、データのバックアップの実施及び復旧手順を確認する。

○　インシデント発生時に備えて、インシデントを認知した際の対処手順を確認し、対外応答や社内連絡体制等を準備する。

また、ここ数年、サイバー攻撃による外国への秘密情報の流出リスクはより顕著なものとなっています。以下に、ここ数年で確認された事例の概要と対策の留意点を紹介しま

すので、秘密情報の流出防止策を講じる上での参考としてください。

＜事例１＞

（概要）

- ~~日本の防衛関連産業の国内拠点システムが、外国にある同社の海外拠点システムを経由して不正アクセスを受けた。この事例では、外国の攻撃者が、同国にある日本の防衛関連産業の海外拠点システムに対し、ウイルス対策管理サーバーの脆弱性を突いた攻撃を実施した。~~外国のサイバー攻撃グループが 2010 年頃から日本を含む東アジアや米国の政府、産業、技術、メディア、エレクトロニクス及び電気通信分野を標的とし、情報窃取を目的としたサイバー攻撃を行っていることが確認された。この事例では、海外子会社等のルーターの脆弱性を悪用してバックドアを設置し、そこから標的の企業の本社のネットワーク等に侵入などが行われている。
- ~~~~

（留意点）

- ~~海外拠点を経由したサイバー攻撃があり得ることを念頭に、国内拠点のセキュリティ対策を実施する必要がある。海外拠点を含めて脆弱性への対応状況の確認を徹底するほか、海外拠点から国内拠点が保有する機微な情報へのアクセスを完全に遮断するなどの対策を検討することも効果的。~~この手口では、信頼された内部ネットワークからの攻撃となり検知が困難になる場合がある。また、この事例では、侵入が発見されないようにルーターのログ記録の無効化等が実施されていた。ネットワークの脆弱な点の解消を常に行うほか、境界防御が突破された場合の被害を軽減するための措置を講ずることが重要。

＜事例２＞

（概要）

- 外国に進出した日本企業の現地法人において、公的に導入が義務付けられている税務ソフトウェアをインストールした後、自動的にマルウェアがダウンロードされた。この事例では、現地法人の秘密情報が窃取される可能性が生じていた。

（留意点）

- 公的に導入が義務付けられているソフトウェアだからといって必ずしも安全なものとは限らないことを認識する必要がある。海外現地法人が用いるソフトウェアにセキュリティ上の懸念がないか常に情報収集し、不審な通信の検知・遮断措置を講じることが必要。
- 例えば、セキュリティ上の懸念が払拭できないソフトウェアを使用する端末を、他の業務で使用するネットワークから分離しておくなど、いざというときの被害を最小化するための対策

を講じておく。

サイバー上のリスクだけではなく、人を通じた秘密情報の窃取にも備えなければなりません。人を通じた秘密情報の窃取といえば、退職者が不正に持ち出した秘密情報を競合他社へ漏えいさせるといったケースや、競合他社の社員が、取引や従業員等を介して自社製品・サービスに関する秘密情報を盗むといったケースのような「産業スパイ」によって引き起こされるものをイメージするのではないでしょうか？

② スパイとなる者を仕立てた工作による秘密情報の窃取！

もちろんこうしたいわば典型的なリスクにも引き続き対応を講じていく必要がありますが、前述のとおり、日本の企業等が保有する秘密情報は外国からも狙われているということをしっかりと認識しておく必要があります。こうしたケースでは、外国側が企業等の秘密情報にアクセスしやすくなるよう、スパイとなる者を仕立てて秘密情報を盗ませるといった形態に注意しなくてはなりません。

実際に、日本において、外国政府職員からスパイ活動をするよう工作を受け、営業秘密を漏えいしてしまったという事例がありました。

通信関連会社の社員が、ある日道端で、外国の政府職員~~を名乗る~~とみられる外国人から飲食店の場所を尋ねられ、食事に誘われます。ここから二人の関係が始まり、以後、継続的に食事をする間柄となりますが、この社員はこの外国人に唆され、自社の営業秘密を不正に取得するようになり、最終的に不正競争防止法違反（営業秘密の領得）で逮捕されてしまいます。

逮捕に至るまで、この社員は、外国人から巧妙なスパイ工作を受けていました。まず、外国人は、社員に公開情報を提供させ少額の報酬を渡します。これを繰り返すことで情報提供に対する心理的な抵抗を弱めていきました。

やがて、この外国人は、社員の感覚が麻痺したところで、社外秘の営業秘密を持ち出すよう要求します。同時に情報の漏えい発覚を防ぐための具体的な方法を伝授し、発覚を恐れる気持ちを和らげます。最後には、社員に「あなたの自宅を知っている」などと伝えることで恐怖心を煽り、この関係からは抜け出せないという意識を植え付けていくのです。

危険をもたらす出会いはリアルな空間だけでなく、ＳＮＳ上でも生じます。例えば、こんな事例がありました。

ＳＮＳを通じて外国企業の社員と知り合った日本の化学メーカー社員が、自社の営業秘密をこの外国企業に流出させ、不正競争防止法違反（営業秘密侵害）で逮捕検挙されました。

この事例でターゲットとなった日本人社員はビジネスパーソン向けのＳＮＳを使用しており、

外国企業の社員は、そこに書かれている個人情報に着目して接近したとみられます。「業務に関して質問がある」などと伝えて接触し、技術指導を依頼したり、報酬や転職の打診を含めた働き掛けを行ったりしていました。また、言葉巧みに日本人社員を外国に招待するなどして深い関係を築いていきました。

醸成された関係を背景に、日本人社員は、最終的には自社のコンピュータにアクセスして営業秘密を不正に取得し、電子メールを使用して外国企業に提供し~~てしまい~~ました。

【対策の留意点】

企業等の内部にいる人間がスパイに仕立てられ、こうした者を通じて秘密情報が狙われるリスクは、現実空間にもインターネット上にも存在し、その手口も様々です。悪意を持った者が自分たちの秘密情報を狙って接近してくるという危険性については、身近な危険として考えにくく、ともすれば、「自分たちには関係ない」という意識に押しやられ、当事者意識をもった対策が講じられにくい側面があります。

しかしながら、企業等の秘密情報を確実に守るには、こうしたリスクが現実のものとなっていることを、経営者やセキュリティ担当者だけでなく、社員一人ひとりに認識してもらうことが必要です。さらに、社員の誰かが不審なアプローチを受けた際に、セキュリティ担当者や上司への相談・報告を行い、組織内で共有した上で、このリスクを排除し、再度のアプローチが行われることを防ぐ・備えるという取組を徹底することが重要です。

③ ~~通常の経済・学術活動に見せかけた~~を通じた秘密情報の窃取！

経済活動がグローバル化し、また、研究活動のオープン化、国際化が進展する中で、合弁や企業の買収、共同研究など、それ自体は合法な経済・学術活動についても、自由で開かれたシステムが悪用され、これを隠れ蓑にすることにより、秘密情報が狙われるリスクが存在します。

また、技術革新により民生技術と軍事技術の境界があいまいとなり、民生技術の軍事転用の危険性が増す中で、こうした活動によって外国へ移転した技術情報が軍事転用され、日本の安全保障上のリスクとなる可能性についても考慮しておく必要があります。

近年、合弁や買収をめぐってこうしたリスクが確認された事例としては以下のものがあります。

○　合弁

- 日本企業が外国で投資や事業を行うためには合弁会社を設立しなければならない場合も多々ありますが、ある日本企業が協定に基づき合弁の相手である外国企業に提供した技術が、当該国において軍事転用される懸念が発生するなどのケースも確認されて

います。

○　買収

●　先端技術を保有する日本の中小企業が、外国企業に買収された又は買収を持ち掛けられたという複数のケースについて、その背景に外国政府機関による技術獲得の意向がうかがえるものや、軍事転用のリスクが懸念されるものも確認されています。

また、共同研究をめぐっては、日本でこのような事例が確認されています。

○　共同研究

●　とある国の経済制裁対象となっていた外国企業の日本法人が、先端技術の研究を行う日本の複数の大学や研究機関に対し、共同研究の働き掛けを行っていました。
この背景には、経済制裁の対象となったことにより、調達が困難となった物資の自社製造を行うため、日本の先端技術の情報を獲得しようという意向があったと考えられます。
この法人は、ある大学に共同研究を持ち掛け難色を示された際に、代替案として、自社の名前が出ないよう、他の日本企業とのタイアップによる共同研究という形態を提案し、説得を試みていました。

【対策の留意点】

重要なのは、こうした活動を抑制することではなく、背景に存在するかもしれない情報窃取のリスクを認識しておくことです。これらの活動により、意図していない又は想定していた範囲を超えた秘密情報の移転が発生したり、自社の技術が外国で軍事転用されてしまうなど予想していなかった結果を招いたりすることを防止しなければなりません。

そのためには、合法的な活動により、情報の移転をめぐって意図していなかった結果を招いてしまうリスクが存在するということをまずはしっかりと認識し、その上で企業等の意思決定を行うことが必要です。

また、近年、安全保障上の観点から、企業、研究機関における技術情報をはじめとする秘密情報の管理はより強化されつつありますが、共同研究の事例からも分かるように、こうした管理が及びにくくなるような「工夫」を施して働き掛けが行われるということも合わせて認識しておく必要があります。

このほか、共同研究を行うに当たっての具体的な対策として、英国が行っている対策も参考となります。~~ＣＰＮＩ~~ＮＰＳＡ（英国国家~~インフラ保護センター~~保護安全保障局）では、国際的な共同研究の公正性を守るため、研究機関を対象として、共同研究のパートナーとして信頼できる研究機関かどうかを判断する基準等を盛り込んだガ

イダンスを公表しています[22]。そこには、研究内容を守る方法として、研究パートナーの適合性（米国のエンティティ・リスト、国連制裁リスト、国の腐敗認識指数、英国の輸出制限、人間の自由度指数等が例示されています）を判断するための情報収集、アクセス制限、不正アクセスの監視及び防止、サイバーセキュリティ基準の確認などが示されています。

なお、経済産業省では、技術情報や生産ノウハウを有する製造業を対象として、国境を越えた意図せざる技術流出を防止するための指針[23]を定めていますが、その他の業種にとっても参考となる基本的な対策、留意事項が盛り込まれていることから、本書と合わせて参照してください。

[22] https://www.npsa.gov.uk/trusted-research-academia~~https://www.cpnipsa.gov.uk/trusted-research-guidance-academia~~

[23] 技術流出防止指針～意図せざる技術流出防止のために～
https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/030314guideline2.pdf

３－４　具体的な情報漏えい対策例

○　ここでは、従業員等、退職者等、取引先、外部者それぞれごとに、５つの「対策の目的」に応じて有効と考えられる対策例を提示します。

（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~~自社内の実習生~~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。

（留意点）

なお、自社が直接雇用する者以外に対しては、「⑤信頼関係の維持・向上等」の観点からの対策は効果が乏しい場合もあるため、それ以外の「対策の目的」の観点からの対策を着実に実施していくことが重要です。

①「接近の制御」に資する対策

ここで紹介する対策は、

ａ．ルールに基づく適切なアクセス権の付与・管理

を実施して、秘密情報を閲覧・利用等することができる者（アクセス権者）の範囲を適切に設定した上で、

ｂ．情報システムにおけるアクセス権者のＩＤ登録

ｃ．分離保管による秘密情報へのアクセスの制限

ｄ．ペーパーレス化

ｅ．秘密情報の復元が困難な廃棄・消去方法の選択

といった対策を講ずることで、秘密情報に対するアクセス権（秘密情報を閲覧・利用等することができる権限）を有しない者を秘密情報に近づけないようにすることを目的としています。

なお、今後、さらに普及・常態化するテレワークにおいては、外部からの情報へのアクセスをよりきめ細かい単位で制御することが求められるようになるため、細かいアクセス権限管理に対応できるアクセス管理基盤の整備、雇用関係の終了や契約の終了に伴い速やかなテレワークでのアクセス権限の削除が望まれます。

ａ．ルールに基づく適切なアクセス権の付与・管理

○　社内規程等において、秘密情報の分類ごとに、アクセス権の設定に関するルール（どのような手続きで誰が設定するのかなど）を明確にした上で、当該ルールに基づき、適切にアクセス権の範囲を設定します。

○　アクセス権の範囲については、その秘密情報を知る必要がない者にまでアクセス権を付与してしまうと、情報漏えいリスクを不必要に高めてしまうこととなるため、当該秘密情報の内容・性質等を踏まえて、「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、その秘密情報へのアクセス権限を付与する者を必要最小限にすることが重要です。また、権限を付与する期間も必要な時期に限って行うことが考えられます。なお、今後、さらに普及・常態化するテレワーク等においては、企業の外部から秘密情報へのアクセスを細かい単位で制御することが求められるようになるため、きめ細かいアクセス権限管理に対応できるアクセス管理基盤の整備を行うことが考えられます。

○　人事部門との情報共有を円滑にすること等により、異動等に伴うアクセス権の変更を迅速に実施して、常に、アクセス権者の範囲が適正に設定されているようにすることも考えられます。

○　例えば、人事異動、プロジェクト終了時などについては、アクセス権の範囲を適切に変更することが重要です。また、出向等によって他組織に就業する者についても一時的にアクセス権を停止する等の対応を行うことが考えられます。

（漏えいリスクを低減するためのアクセス権設定の具体例）

- 工場の作業ライン等について、作業の一連の流れを複数人で分担するなど、工程全体の情報を１人の作業員が把握できないようにアクセス権の範囲を設定する。実習生に開示する情報の範囲についても注意する。
- 従業員等の個人ではなく、業務や役職に基づきアクセス権を設定することで、人事異動等に伴って適切にアクセス権が設定・変更されるようにする。

※特に情報システムにおいては、「ロールベースアクセス制御」[24]に対応したアクセス制御システムを導入して、アクセス権の範囲を業務にひも付して、人事異動に対応して適切にアクセス権が設定・変更されるように設定することも有効です。

アクセス権設定の事例

◆　**印刷業・大規模企業の事例**
～事前調査により適正なアクセス権設定を実施～

顧客情報や企業情報等の機密性の高い情報についてアクセス権を付与する場合は、必要に応じて、事前に、従業員が当該秘密情報をほしがる事情を有していないかなどの調査を行っている。また、アクセス権設定後もアクセス権者の名簿を作成して必要に応じて社員の調査を行うようにしている。

ｂ．情報システムにおけるアクセス権者のＩＤ登録

○　予め、従業員等に対して情報システム上のＩＤを付与し、そのＩＤを認証する（ＩＤを使用する者が本人であることを確認する）ためのパスワード[25]等を設

[24] 情報システムにおいて個人ではなく職務（役割）に対してアクセス権限を割り当てること（ＩＰＡ（独立行政法人情報処理推進機構）『組織における内部不正防止ガイドライン』ｐ４０を参照）。

[25] ＩＰＡ『チョコっとプラスパスワード』（https://www.ipa.go.jp/security/chocotto/index.html~~http://www.ipa.go.jp/chocotto/pw.html~~）に、パスワードの安全性を高めるための管理方法が分かり易く説明されています。

定しておきます。

※ＩＤ・パスワードは複数の従業員間で同じものを使い回さないことが重要です。

※パスワードの設定に当たっては推測されやすいパスワードは避けることが重要です。また、パスワードに有効期限を設定し、長期間にわたり同一のパスワードを使用しないことも有効です。

※なお、アクセス権限の確認については、ＩＤ・パスワードの設定で十分だと安心せず、多要素認証の利用・不要なアカウントの削除等により、本人認証を強化することも重要です。

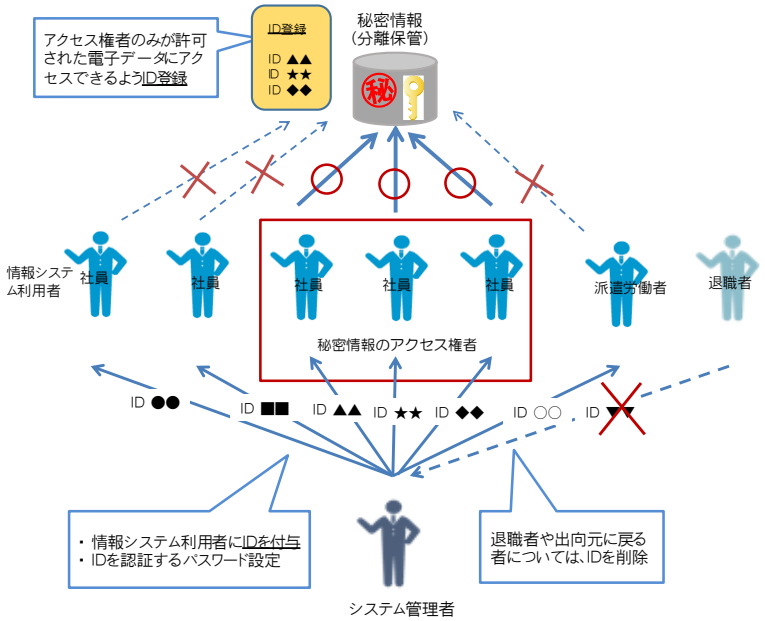
○　ａ．により決定されたアクセス権者だけが、利用することが許可された電子データ等（ｃ．に記載の電子データ、分離されたフォルダやサーバ等）にアクセスできるように、ＩＤを登録します。

※電子データやフォルダへアクセスするためのＩＤを情報システムに登録した上で、登録されたＩＤに限定して電子データや分離されたフォルダにアクセスすることができるよう、最もよく使われているＯＳの機能を活用して設定することができます。

※情報システム管理者は大きな権限を有しているので、情報システム上のＩＤ登録作業は、複数人のシステム管理者で行うことで、権限の集中による内部不正や情報システムの破壊などの業務妨害活動を防止することが可能となり、適正な実施を確保することができます。

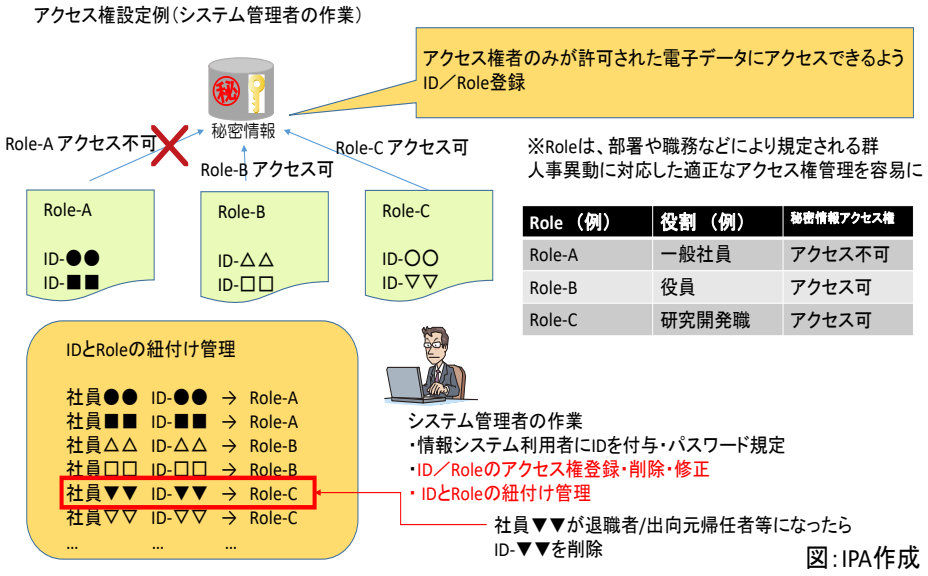
※情報システム管理者に対する情報漏えい対策も重要です[26]。

図表３（２）情報システム上のアクセス権設定の流れ



[26] ＩＰＡ『組織における内部不正ガイドライン』ｐ４０、４２、６８を参照。

図表３（３）ロールベースアクセス権の設定例（システム管理者の作業）



図：IPA作成

ｃ．分離保管による秘密情報へのアクセスの制限

○　秘密情報が記録された書類・ファイルや記録媒体（ＵＳＢメモリ等）については、保管する書棚や区域（倉庫、部屋など）を分離し、電子データについては格納するサーバ═やフォルダを分離した上で、アクセス権を有しない者が、その秘密情報を保管する領域にアクセスできないようにします（秘密情報が保管された部屋に入室できない、保管庫を開扉できない、サーバ═にアクセスできない状態とする等）。

○　なお、全ての秘密情報について、厳格なアクセス制限を講ずることが難しい場合も考えられますので、秘密情報の評価の高低や利用態様に応じて、対策を選択していくことが重要です。

（具体的な管理方法）

➢　書類・ファイル、記録媒体を書棚や区域（倉庫、部屋など）に保管し施錠管理。

ex）　業務時間のみ解錠する（同時に、業務時間中についてはアクセス権を有しない者が入室・閲覧しないように視線を配るなど、視認性

を高めておくことが重要）。

ex）管理者が鍵を管理し、入退室の際の鍵の貸出しは許可制にする。

ex）重要度の高い情報等については、認証システム導入による入退室管理を実施する。

※認証システムとしては、ＩＣカード認証、生体認証（指紋認証、こう彩認証、静脈認証等）、ワンタイムパスワード（時刻同期方式、イベント同期方式、チャレンジレスポンス方式等）、ＰＩＮ入力の付与等があり、アンチパスバック機能[27]も併用できる。なお、これらのシステムのうち、製品によっては、入退出者や入退出時刻等を記録する機能を持つものもあるが、その記録を保存することは「視認性の確保」にもつながる。

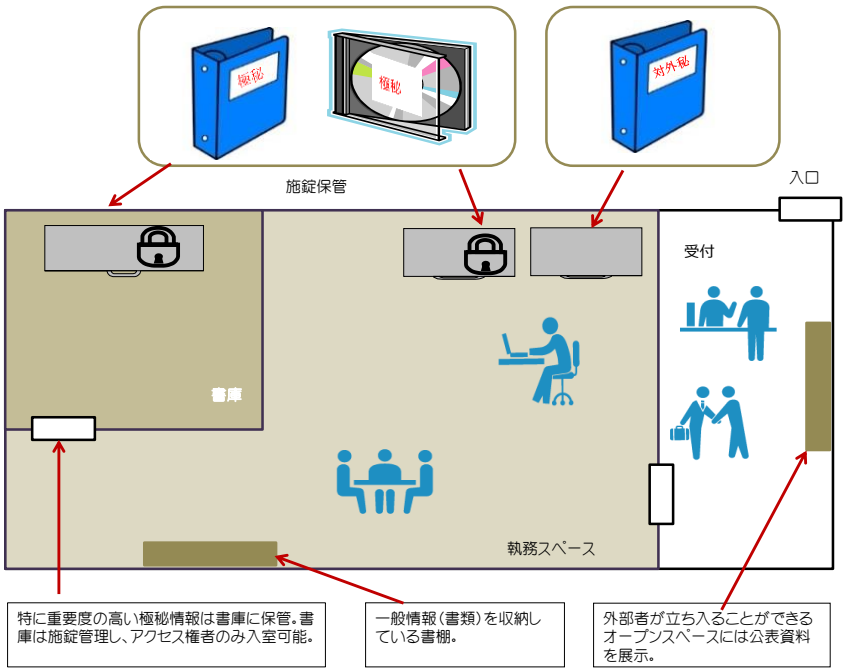
ex）重要度の高い情報等については、警備システムの導入、警備員の配
置

➢ **屋外に存在する植物等**

ex）屋外のほ場で栽培されている植物等については、見学者等が立ち入る区画を限定する、果実が実っていて、外観上品種の判別がされやすい時期などは、見学者等を立ち入らせないことにより管理。

図表３（４）秘密情報の分離保管の例（書類等）

[27] 入室していないＩＤでは退室できず、退室していないＩＤでは入室できない等、同じＩＤで続けて入退室できないようにする機能。



➢　**電子データの管理**

以下のような方策で秘密情報が記録された情報の分離等を行った上で、アクセス権を有する者のＩＤからのみアクセスできるようにする。

※フォルダや電子データについて、アクセスに必要なパスワードを設定して管理する方法も考えられるが、個別ＩＤ付与を行わないままに共通パスワードのみで管理する場合、万一情報漏えいが発生した場合に追跡が困難になるケースがあることに注意。また、人事異動や退職等によってアクセス権を失った者が、その後も、そのフォルダや電子データにアクセスできることがないよう、その都度パスワードを変更することが重要。

ex）**秘密情報をネットワークにつながっているＰＣに保存しない**

※秘密情報をネットワークに接続しない特定のＰＣに保存する場合は、当該ＰＣを施錠管理する区域に保管し、アクセス権者のみが作業できるようにすることも考えられる（区域における施錠管理）。

ex）**アクセス権を有する者のＩＤでログインしたＰＣ等からのみその電子データを閲覧できる状態にする。**

ex）**フォルダの分離**

ex）**サーバ═の物理的分離（複数台のサーバ═に分離）、サーバ═の仮想化による論理的分離（1 台のサーバ═を複数の仮想**

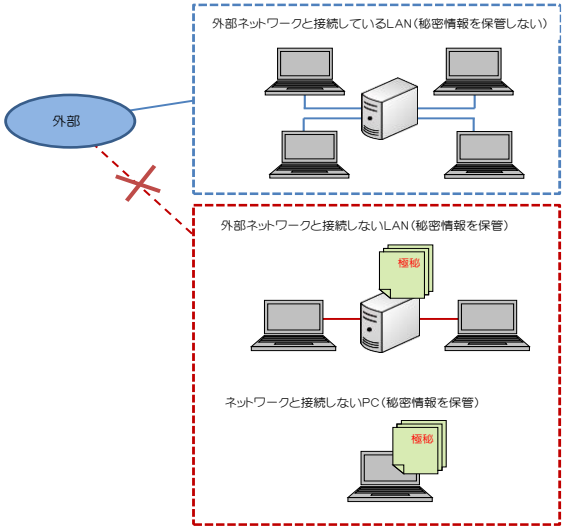
サーバ═に分割）

ex）ネットワークの分離（複数のＬＡＮを構築）

※上記方策は、組み合わせて利用することも考えられる。

※重要度の高い情報の場合は、ＰＣ、サーバ═等へのアクセスに当たって、ＩＣカードによる認証システム（前述）を導入することも考えられる。

図表３（５）秘密情報の分離保管の例（電子データ）



➢ プラントのレイアウト、金型、試作品等

ex）プラントのレイアウト等、その「物」自体が秘密情報であるものが置かれた工場等を施錠管理。

施設内の分離保管の事例

◆ **電機機器製造業・大規模企業の事例**
～動線の工夫等でアクセス制限強化～

執務スペースのゾーニングを行い、社外の人は特定の会議スペースなどしか立ち入れないようにしている。社内の人間でもアクセス権のない社員であれば研究所に入れないといった施設の区分管理を行っている。区分管理を徹底するため、施設への経路についてはいわゆる裏道をなくし、動線を1つに制限するなどの工夫を行っている。

◆ **印刷業・大規模企業の事例**
～複数の領域設定でアクセス制御～

オフィスを以下の4つの領域に区分することでアクセス制御を徹底。

領域1　訪問客が入室可能なエリア
領域2　一般的なオフィスエリアで、オフィスカードを持つ社員は全員入室可能
領域3　氏名、住所等一般的な個人情報を扱う部署であり、当該部署に所属する者のみ入室可能。監視カメラを導入。
領域4　未公表情報等の機密性の特に高い情報を保管。指紋認証や生体認証による入退室管理を実施。

秘密情報の分離管理とそのアクセス範囲の設定の事例

◆ **建設業・大規模企業の事例**
～フォルダごとの管理で適正な情報管理～

秘密情報を含む電子データ（ファイル）を、特定のフォルダに保存し、フォルダごとに開示範囲を設定し、適正な情報の分離とアクセス権設定を行っている。

◆ **出版業・大規模企業の事例**
～文書管理システムを活用した効率向上～

秘密情報（電子データ）のアクセス権の範囲設定や印刷の権限設定を文書管理システム上で一元管理。これにより秘密情報の管理が容易になり、業務効率アップにもつながった。

ｄ．ペーパーレス化

○　自社内の秘密情報をペーパーレスにして、アクセス権を有しない者が秘密情報に接する機会を少なくします。加えて、電子化された秘密情報について、印刷やコピーができない措置を施せば、更に持出し困難化にも資することになります。

○　例えば、ペーパーレス化し、情報を社内共通のデータベースといった形で活用することにより、日々更新される情報の最新の状態について、従業員間での共有化が促進されることになります。更に、従業員が相互にアイディアを出し合うなどの活動が利便となることにより、共有知識の更なる高付加価値化や作業の効率化にも役立ちます。

○　なお、完全なペーパーレス化を実施することが難しい場合でも、電子化された秘密情報について、印刷できるデータの内容や、印刷できる者、印刷の目的等を限定するというルールを設け、併せてその印刷物の廃棄方法にも留意することで、同様の効果が得られます（廃棄方法については ｅ．に記載）。

ペーパーレス化の事例

◆　**金型製造業･小規模企業の事例**
～情報の整理整頓によって業務効率アップ～

情報の整理･整頓活動として、不要な情報の廃棄、必要な情報の電子化･データベース化等を実施し、できる限り紙媒体は保有しないよう徹底。これにより、情報セキュリティの向上が図られ、さらに、文書検索の時間短縮による迅速な顧客対応が可能となり、売上げ向上にも貢献。

ｅ．秘密情報の復元が困難な廃棄・消去方法の選択

○　秘密情報が記録された書類・ファイルや記録媒体等の廃棄、秘密情報が記録された電子データの消去を行う場合、アクセス権を有しない従業員等が、廃棄・消去された情報を復元して、その情報にアクセスすることができないように、以下のように復元不可能な形にして廃棄・消去します。

（具体的な廃棄・消去方法）
- 書類の廃棄方法

ex）シュレッダーにより裁断し、廃棄。

※秘密情報の重要度に応じて、より復元を困難とするため、クロスカット（縦方向と横方向の両方から裁断する）方式のシュレッダーを利用するなど、かけることができる費用の多寡も踏まえながら、シュレッダーの機能性について検討することも重要。

ex）秘密情報を廃棄するゴミ箱は、廃棄後取り出すことができない鍵付きゴミ箱に限定。

ex）重要度の高い情報等については、信頼できる専門処理業者に依頼して焼却・溶解処分。場合によっては、その証明書を発行してもらう。

- 秘密情報を保存していた記録媒体（ＵＳＢメモリ等）、ＰＣ、サーバの廃棄方法

ex）市販されている完全消去するソフトや、磁気記録方式のハードディスク磁気破壊サービス等を利用してデータを消去の上、その記録媒体等を物理的に破壊（記録媒体からデータを消去しただけでは復元されるおそれがあるため）。

②「持出し困難化」に資する対策

ここで紹介する対策は、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ＰＣ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ＵＳＢ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、持ち出したりすることを物理的、技術的に阻止することを目的としています。

具体的には、どのような形で情報が持ち出されるのかといった持ち出しの態様（【書類、記録媒体、物自体等の持出しを困難にする措置】、【電子データの外部送信による持出しを困難にする措置】、【秘密情報の複製を困難にする措置】、【アクセス権変更に伴いアクセス権を有しなくなった者に対する措置】）に応じて、対策を整理して記載しています。

なお、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、ＰＣ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ＶＰＮ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ＡＩ等の利用にあたっては、社外に情報が流出・公開等されてしまう可能性があるものの利用を組織として避ける、生成ＡＩを利用する際に、秘密情報の入力を避ける等の対策を講じることが重要となります。

【書類、記録媒体、物自体等の持出しを困難にする措置】

ａ．秘密情報が記された会議資料等の適切な回収

○　アクセス権を有する従業員等であっても、個別には資料を所持させないこととした上で、会議等で資料を配布した場合には、終了後、回収します（資料に、通し番号を付すことで遺漏なく回収することが可能です。）。従業員等の手元に資料を残させないことにより、資料を持ち出すことができない状態にします。

※テレワークの普及を背景に、オンライン会議についても浸透しつつあります。秘密情報を紙・電子データで直接に配布・送信することが避けることが可能な一方で、会議中に画面上で秘密情報を共有・表示こともあるかもしれませんが、このようなときには、会議画面が録画・撮影される可能性も考慮して、オンライン会議の画面上で共有する情報についても事前に精査する、発表前に録画機能が用いられていないかどうか確認するといった点に注意を払うことが考えられます。

ｂ．秘密情報の社外持出しを物理的に阻止する措置

○　ノートＰＣ等を持ち出せないようセキュリティワイヤーで固定したり、使用者の不在時にノートＰＣ等を机の引出しやロッカー等に格納・施錠することが考えられます。

○　退社時の荷物検査や、セキュリティタグによる退社時の情報持出しのチェック等の対策を講ずることも考えられます。

※例えば、秘密情報が記載・記録された紙や記録媒体、それ自体が秘密情報である物件に検知タグを取付けた上で、出入口に検知ゲートを設置し、不正な持出しの場合に警報が鳴るようなシステムを導入することが考えられます。

ｃ．電子データの暗号化による閲覧制限等

○　電子データを暗号化しておくことで、アクセス権がない従業員等が当該データを入手することができたとしても、閲覧ができないようにします[28][29]。

○　電子データのアクセス権を有するＩＤでログインしたＰＣ等からのみ当該電子データを閲覧できるようにします。

ｄ．遠隔操作によるデータ消去機能を有するＰＣ・電子データの利用

○　ＰＣ等が盗難された場合などに備えて、以下の市販のツールを利用することが考えられます。

（消去機能の例）

- 遠隔操作によりＰＣ内のデータを消去できるツール。
- 情報機器について、パスワードロックで、一定の回数認証に失敗すると重要情報を消去するツール。
- 一定期間、管理サーバとのやり取りがなされない状態が続いた場合に指定したデータが自動的に消去されるサービス。
- 電子データそのものに遠隔操作による消去機能を備えさせるツール。

[28] 電子データの持出しにつながる操作は閲覧だけではなく、印刷やコピー＆ペーストなども同様です。したがって、暗号化による閲覧制限だけではなく、閲覧権を持つ従業員等に対してもデータ単位で閲覧、編集、印刷、コピー＆ペースト等の利用権限を設定し、最小の権限でデータを利用させるようにすることが望ましいです。また、この暗号化した電子データを参照するためには管理サーバによる認証を受けることが必要となるシステムが望ましいです。

[29] ＩＰＡ「対策のしおりシリーズ」（http://www.ipa.go.jp/security/antivirus/shiori.html）に暗号化の概要、注意事項が記載されています。

【電子データの外部送信による持出しを困難にする措置】

ｅ．社外へのメール送信・Ｗｅｂアクセスの制限

○　電子データについて、メールに添付できない設定としたり、メールの送信容量を制限したりすることで、秘密情報である電子データを、メール送信によって外部に持ち出すことを防止・困難化します。

○　コンテンツフィルタを導入して、企業が禁止しているＳＮＳ、アップローダー、Ｗｅｂメールサイト及び掲示板等へのアクセスを制限し、Ｗｅｂアクセスによる持出しを防止・困難化します。

○　ＰＣ等の情報機器では、企業内で許可されたソフトウェア以外のものを利用してインストールすることや、企業が許可した以外のオンラインストレージや生成ＡＩ等を利用することを禁止し、企業内ネットワークから情報を外部に持ち出すことを防止・困難化します。

ｆ．電子データの暗号化による閲覧制限等（再掲）

○　電子データを暗号化したり、登録されたＩＤでログインしたＰＣからしか閲覧できないような設定にしておくことで、外部に秘密情報が記録された電子データを、無断で、メールに添付して送信しても、閲覧ができないようにします。

ｇ.遠隔操作によるデータ消去機能を有するＰＣ・電子データの利用（再掲）

○　電子データそのものに遠隔操作による消去機能を備えておくことで、無断で外部にデータが送信された場合に消去することができます。

【秘密情報の複製を困難にする措置】

ｈ．コピー防止用紙やコピーガード付の記録媒体・電子データ等により秘密情報を保管

○　秘密情報が記載された書類について、市販のコピー偽造防止用紙（コピーできないものや浮き出し文字によって不正コピーであることを明らかにするもの等）を使用することで、不完全な複製物しか作成できないようにします。

○　電子化された秘密情報について、印刷、コピー＆ペースト、ドラッグ＆ドロップ、ＵＳＢメモリへの書込みができない設定としたり、コピーガード付きのＵＳＢメモリやＣＤ－Ｒ等に保存することで、秘密情報の複製を制限します。

※テレワークの普及を背景に、オンライン会議についても浸透しつつあります。秘密情報を紙・電子データで直接に配布・送信することが避けることが可能な一方で、会議中に画面上で秘密情報を共有・表示こともあるかもしれませんが、このようなときには、会議画面が録画・撮影される可能性も考慮して、オンライン会議の画面上で共有する情報についても事前に精査する、発表前に録画機能が用いられていないかどうか確認するといった点に注意を払うことが考えられます。（再掲）

電子データの複製、持出しを予防している事例

◆　**化学品製造業・大規模企業の事例**
～書込みを制限してデータの複製、持出しを予防～

社内のパソコンはUSBメモリ等の外部記録媒体への書込みができない設定にし、書込みが必要な場合は、事前申請をして特定の場所に設置された書込み可能なパソコンを使用することにしている。この対策により社内の電子データの無断複製・持出しを予防している。

ｉ．コピー機の使用制限

○　従業員等のＩＤカードとコピー機を連動させ、同一のＩＤカードで１日当たりに印刷できる枚数を制限することにより、一度に資料全体の複製物を作成することを困難にします。

ｊ．私物のＵＳＢメモリや情報機器、カメラ等の記録媒体・撮影機器の業務利用・持込みの制限

○　社内におけるＰＣやＵＳＢメモリ等の記録媒体の利用は会社貸与品のみとし

た上で、私物の記録媒体の持込みを制限して、秘密情報の私物記録媒体への複製ができないようにします。この対策を徹底するために、ＵＳＢの差込口のないものやＵＳＢの差込口を無効化したり、物理的にふさぐ部品を取り付けたＰＣを利用することが考えられます。

○　合わせて、私物のＵＳＢメモリ等の持込みや業務での利用がなされていないかを確認することも重要です。

※私物の記録媒体等の業務利用を認める場合には、利用できる業務範囲や利用に当たって遵守すべき事項等のルールを定めることが重要です[30、31]。

○　私物のスマートフォンについて、重要な秘密情報が保管されている書庫や区域など、特に情報漏えい対策を厳格に行うべき区域に限って、持込みを制限することが考えられます。

○　無線ＬＡＮの利用に関しては、役職員の私用のスマートフォンによるテザリングや工事の要らない無線ＬＡＮアクセスポイントなどで、許可なく企業の外部に接続することを禁止して、情報の持出し・漏えいを困難にすることが考えられます。

○　テレワークを実施する場合には、テレワークで用いるＰＣ等には電子データを可能な限り保存しない、秘密情報を暗号化したり、ＶＰＮ等を用いて通信を暗号化するといったシステムや機器の利用制限を行うことのほか、ＥＤＲ（Endpoint Detection and Response）やＮＤＲ（Network Detection and Response）等の導入~~で社内ネットワーク全体の不審な挙動や異常を検知しなどするなど内部不正モニタリングシステムを活用し~~、操作・送信履歴を確保するなどの視認性を高める取組みと組み合わせることで、情報の持出し・漏えいを困難にすることが考えられます。

○　生産ラインのレイアウトなどについては、その工場へのカメラ等の撮影機器の持込みを制限し、写真撮影を通じた情報の持出しを困難にします。

30　ＩＰＡ『組織における内部不正防止ガイドライン』ｐ３６、ｐ４７を参照

31　私物端末の業務利用の際のリスクやセキュリティ対策等については、『私物端末の業務利用におけるセキュリティ要件の考え方（平成２５年３月　各府省情報化統括責任者（ＣＩＯ）補佐官等連絡会議ワーキンググループ報告）』が参考になります。
（~~https://www.kantei.go.jp/jp/singi/it2/cio/hosakan/wg_report/byod.pdf~~https://warp.ndl.go.jp/info:ndljp/pid/12187388/www.kantei.go.jp/jp/singi/it2/cio/hosakan/wg_report/byod.pdf）。

私物を持ち込ませないために工夫している事例

◆ **印刷業･大規模企業の事例**

～工場内への私物の持込みを防止する対策～

以下の対策を講ずることで工場内に私物を持ち込ませないように工夫している。

- 工場内の私物（パソコン、携帯電話、鞄、カメラなど）の持込みを禁止。さらに、私物はロッカーに入れ、ポケットの無い作業着を着用の上、勤務エリアに入室することを義務付け。
- 外部からの来訪者が工場内に立ち入る際も、同様に作業着の着用を義務付け。

◆ **コールセンター業･中規模企業の事例**

～私物持込み防止対策が社員の潔白の証明に～

顧客情報をなどの機密性の高い情報を扱うエリアについては、鞄や私物をロッカーに入れ、身の回りの必要最低限の持ち物だけを透明バッグにいれて入室するようにしている。この対策は、社員の身の潔白を証明する手段にもなっている。

【アクセス権変更に伴いアクセス権を有しなくなった者に対する措置】

ｋ．秘密情報の消去・返還

○　プロジェクトに参加する従業員等に秘密情報を示す際に、秘密保持契約を入社時や退社時に結ぶ場合や就業規則等において秘密保持義務が規定されている場合であっても、個別の秘密保持契約等において、可能であれば対象となる秘密情報を明確化した上で、プロジェクト終了時の秘密情報の消去・返還について定めておきます。これに基づき、プロジェクト終了時には、当該従業員等が有している秘密情報が記録された書類や記録媒体等を返還させ、秘密情報である電子データを消去させます[32]。

※記録媒体等の返却時には、その記録媒体や内部に記録されたデータに対して、利用者が設定したパスワードも提出させるようにします。

○　この措置の実効性を確保するためには、前述の「ｈ．コピー防止用紙やコピーガード付の記録媒体・電子データ等により秘密情報を保管」で紹介したような、複製のできない形で秘密情報を共有しておくことが必要となります。

[32] プロジェクト参加時の秘密保持契約書の参考例については、参考資料２の第３における「２従業員等のプロジェクト参加時」を参照。

③「視認性の確保」に資する対策

ここで紹介する対策は、職場のレイアウト変更、録画機能付き防犯カメラの設置といった、情報漏えい行為が【目につきやすい状況を作りだす対策】、入退室の記録、情報システムにおけるログの記録・保存といった、情報漏えい行為が【事後的に検知されやすい状況を作り出す対策】により、秘密情報の漏えいを行ったとしても見つかってしまう可能性が高い状態であると認識させるような状況を作り出すことを目的としています。特に、近年は、ＡＩ等の最新技術を組み入れた高度な内部不正モニタリングシステムの開発も進んでおり、【目につきやすい状況を作り出す対策】、【事後的に検知されやすい状況を作り出す対策】の実効性を補完し高める観点から、これを活用することが有効と考えられます。

また、ここでの対策は、従業員等の行為の正当性（身の潔白）を証明する手段としても有効であり、このような従業員をモニタリングすることの目的が従業員の保護であることを就業規則等に明記して従業員に周知徹底するとともに、従業員の理解を得た上で、適切な運用を行うことが必要です。

さらに、現実に監視するというだけでなく、例えば、職場の整理整頓や従業員等に文書管理責任を分担させて情報管理に関する当事者意識を持たせるなど、【管理の行き届いた職場環境を整える対策】により、情報管理に関心の高い職場であると認識させ、心理的に漏えいしにくい状況を作ることも含まれます。

なお、情報漏えい行為の状況などを記録する対策等は、情報漏えいが生じた場合の行為者に対する責任追及の際に必要となる証拠の確保手段としての意義もあります。

このほか、テレワークの実施との関係では、自宅、サテライトオフィスなど職場と同レベルでの視認性を確保することが困難となることが想定されることから、テレワークに伴う秘密情報・重要情報へのアクセス履歴、操作履歴（Ｗｅｂへのアクセスログやメールの送受信履歴など）等のログ・認証を記録し、一定の期間に安全に保存することが視認性の確保のための対策としても有効であると考えられます。

【管理の行き届いた職場環境を整える対策】

ａ．職場の整理整頓（不要な書類等の廃棄、書棚の整理等）

○　不要となった書類が廃棄されておらず、様々な資料が乱雑に積まれ、整理がなされていない状態となっていると、職場全体が情報管理に対して無関心であるとか、無責任であることを情報漏えい者に連想させ、情報漏えいを行ったとしても発覚しないと思わせることになってしまいます。

○　書類等の必要性を適切に判断した上で不要なものは廃棄するとともに、書棚の

整理や、職場の清掃等を実施することで、情報漏えいを行おうとする者に対して、情報管理に係る関心が高く、管理が行き届いた職場であると認識させることにつながります。

○　加えて、従業員による整理整頓を促進して自社情報が整理されることにより、情報検索が容易になり、業務効率が向上することも期待できます。

ｂ．秘密情報の管理に関する責任の分担

○　従業員等のそれぞれが、秘密情報の管理についての責任を分担し、分担体制をリスト化する等して明確化することで、情報管理に対する当事者意識を高めます。

ｃ．「写真撮影禁止」、「関係者以外立入り禁止」の表示

○　秘密情報が保管されている書庫や区域（倉庫、部屋など）の出入口に「写真撮影禁止」、「関係者以外立入り禁止」といった掲示を行うことにより、情報管理に係る関心が高く、管理が行き届いた職場であると認識させるようにします。

※なお、工場内での重要な設備機材や各種機械の配置・生産ライン、屋外に存在するＦ１品種の親系統（植物）等の情報によっては、安易にこれらの表示を行ってしまうと、かえって注目を集める結果となってしまうこともあり得ることから、秘密情報の存在に着目させない工夫を検討すべき場合もあります 。

【目につきやすい状況を作り出す対策】

ｄ．職場の座席配置・レイアウトの設定、業務体制の構築

○　従業員同士で互いの業務態度が目に入ったり、背後から上司等の目につきやすくするような座席配置としたり、秘密情報が記録された資料が保管された書棚等が従業員等からの死角とならないようにレイアウトを工夫します。

※なお、取り扱う情報によっては、アクセス権のない従業員等から画面を容易に見られることによって秘密情報が漏えいしてしまうことを防ぐために、座席配置・レイアウトを検討すべき場合もあります 。

○　また、秘密情報を取り扱う作業については、可能な限り複数人で作業を行う体制を整えます。単独作業を実施する場合には、各部門の責任者等が事前に単独作業の必要性、事後には作業内容を確認するようにします。

ｅ．従業員等の名札着用の徹底

○　従業員等に社員証や名札の着用を徹底させ、他者から自己の氏名や所属部署が確認でき、情報漏えい行為を目撃された場合に、すぐさま自己の氏名等が特定されてしまう状況とすることにより、「見えやすさ」を確保します。

ｆ．防犯カメラの設置等

○　秘密情報が記録された書類・電子媒体が保管された書庫や区域など、秘密情報の不正な取得や複製の現場となり得る場所に防犯カメラを設置して、情報漏えい行為を行おうとする者に「見られている」という認識を持たせるようにします。合わせて、当該場所から会社の外へと向かう動線に対しても防犯カメラが向けられていると、より効果的です。

○　この対策は、秘密情報の保管区域にアクセス権者のＩＣカードでのみ入室を可能としている場合に、アクセス権を持たない者がアクセス権者のＩＣカードを使用して入室したり、アクセス権を持たない者がアクセス権者と一緒に入退室することを防止するなど、アクセス権者とＩＣカードの使用者の同一性を担保し、①「接近の制御」に資する対策を補完する効果もあります。

○　視認性の効果を高めるためには、見えやすいところに防犯カメラを設置するとともに、そのそばに「防犯カメラ作動中」といった掲示をすることが考えられます。

※この掲示は、本対策の効果を高めるとともに、従業員等が知らない間に撮影されていたということがないようにする意味でも重要です。

○　抑止力の観点からは、必ずしも全時間帯の映像を記録しておく必要はないものの、情報漏えい行為者に対する責任追及の際に必要となる証拠の確保の観点からは、より多くの時間帯で映像が記録されていることが望ましいと考えられます。

防犯カメラ設置の事例

◆　**衣類メンテナンス業・中規模企業の事例**
～カメラ設置により従業員のスキルアップへ～

顧客対応、洗浄、アイロンがけなどのすべての工程をカメラで撮影・録画している。作業の録画をクレーム対応（従業員保護）、従業員自身のスキルチェックに活用することで、高付加価値サービスの実現に貢献。

ｇ．秘密情報が記録された廃棄予定の書類等の保管

○　秘密情報が記録された廃棄予定の書類等についても、実際に廃棄するまでの間は、引き続き秘密情報としての管理を実施することが重要であり、廃棄場所は、複数の従業員等の目の届く場所に設置します。

ｈ．外部へ送信するメールのチェック

○　外部へのメール送信の際に、その全てのメール又は一部のメールについて、上司の承認を必要とするシステムを使用したり、自動的に上司等にもＣＣメールが送信されるよう設定したり、従業員のメールの送受信内容を必要に応じて閲読する場合があることを周知したりするなど、外部とのメールでのやり取りが上司等に把握される可能性があると認識させることで、メールでの情報漏えい行為を行いにくい状況を作ります。

※上司の承認を必要とするシステムを使用する対策は、秘密情報の送付先の間違いを防止する効果もあります。

※本対策を講ずる前提として、「社内メールの業務目的以外の使用を禁止していること」、「メールのやりとりをモニタリングする可能性があること」を予め就業規則等の規程に盛り込んでおく[33]等して社内に周知し、従業員等のメールが知らない間にチェックされていたということがないようにすることが重要です[34]。

※直接、「視認性の確保」につながるわけではないものの、そもそも一定以上の役職の従業員でなければ外部へとメールを送信できないよう設定するということも考えられます（「持出し困難化」につながる対策）。

ｉ．内部通報窓口の設置

○　従業員等が、他の従業員等の情報漏えい行為と思わしき行為を確認した場合の通報窓口を設置し、窓口が設置された旨を周知します。

○　また、内部通報を無用に躊躇することがないよう、匿名での私書箱等を設置するなど通報者の匿名性を確保する工夫を行います。この場合、内部通報者に不

---

33 就業規則における規定例については、参考資料２の「第１　秘密情報管理に関する就業規則（抄）の例」を参照。

34 従業者のモニタリングを実施する上での留意点については、「個人情報の保護に関する法律についてのガイドライン」及び「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」に関する Q&A の Q5-7 等が参考になります。（https://www.ppc.go.jp/all_faq_index/）~~「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」（https://www.ppc.go.jp/files/pdf/iinkaikokuzi01.pdf）に関する Q&A　Q４―Q６が参考になります。（https://www.ppc.go.jp/personalinfo/faq/2009_APPI_QA/https://www.ppc.go.jp/all_faq_index/#sec17）~~

利益を及ぼさないように配慮することも重要です。

○ なお、自己の属する部門以外の部門へと通報することが可能となるよう、複数部門において窓口を設置することが考えられます。

【事後的に検知されやすい状況を作り出す対策】

ｊ．秘密情報が記録された媒体の管理等

○ 秘密情報が記録された書類、ファイル、記録媒体（ＵＳＢメモリ等）を、共有して書庫等に保管するとともに、それらの複製を禁止した上で、保管する媒体等に通し番号を付けて管理します。これによって資料の不足や欠損が生じた場合にすぐに把握できるようにします。

○ さらに、共有保管された書類、ファイル、記録媒体を貸し出す場合やテレワークの実施のために自宅等に持ち帰る場合には、誰にどの記録媒体を貸し出しているかわかるように、貸出し時及び返却時に、その日時、氏名、貸し出した資料名等を記録して管理します。資料の重要性によっては、貸出しを許可制としたり、利用期間を設定して、期間経過後に返却を促す通知を行うことも考えられます。

ｋ．コピー機やプリンター等における利用者記録・枚数管理機能の導入

○ 従業員等のＩＤカードとコピー機やプリンター等とを連動させることによって、ＩＤカードによる認証がなければ印刷ができないように設定した上で、コピー機やプリンター等を、誰が、いつ利用したか、どのような資料を何枚印刷したか等を記録します。

ｌ．印刷者の氏名等の「透かし」が印字される設定の導入

○ 秘密情報が記載された電子データを印刷した場合に、強制的に印刷者の氏名やＩＤの「透かし」が印字されるように設定することにより、印刷物の外観から、誰が印刷したものかがすぐ分かるようにします。

ｍ．秘密情報の保管区域等への入退室の記録・保存とその周知

○ 秘密情報が記録された媒体等を分離保管している区域への入退室について記録を取る（台帳管理、ＩＣカードや生体認証等）とともに、その旨を周知します。

※職場の出社・退社時間の記録をとることも考えられます。

ｎ．不自然なデータアクセス状況の通知

○　深夜帯や休日に、複数分野の業務にわたる様々なデータにアクセスし、大量のダウンロードがなされているなど、不自然な時間帯・アクセス数・ダウンロード量を検知した場合に上司等に通知がなされるようにした上で、その旨を社内に周知します。

ｏ．ＰＣやネットワーク等の情報システムにおけるログの記録・保存とその周知

○　ＰＣやネットワーク等において、誰が（利用者ＩＤの記録）、どの端末から、いつ、どの秘密情報にアクセスされたか（アクセス履歴）、どのような操作をしたか（Ｗｅｂページへのアクセス履歴や、メールの送受信履歴等）といったログを取得し、保存します。加えて、ログを記録・保存していることについては事前に社内に周知しておきます。

※ログの収集・記録にあたり、利用者のプライバシー人権を保護するため、「社内ＰＣの業務目的以外の使用を禁止していること」、「アクセスログをモニタリングする可能性があること」を、予め就業規則等の規程に盛り込んでおく[35]等して社内に周知することが考えられます。この事前の周知は、従業員等のアクセスログが知らない間にチェックされていたということがないようにする意味でも、また、経営者が内部不正者でない従業員の無実を証明するためにログを活用し、プライバシー・人権を保護する姿勢を示すことで、従業員にも組織から守られているという意識を共有してもらうことにもつながり重要です。

○　ログの保存期限については、情報漏えいのリスクの高い情報に関するログか否か、ログの保存にかけられるコストはどの程度かといった観点を踏まえて決定することとなります。

○　なお、ログの確認を定期的に実施することで、情報漏えいにつながり得る兆候が把握できる場合があります。（詳細は第６章）

○　また、高度なモニタリングシステムの導入・活用という観点からは、クラウドプロキシを導入し、これに含まれている接続・操作ログを取得・分析する機能、マルウェア対策機能、不正サイトへの接続をブロックする機能等を利用することや、ＥＤＲやＮＤＲ等のを~~の~~導入で社内ネットワーク全体の~~し、エンドポイ~~

[35] 就業規則における規定例については、参考資料２の「第１　秘密情報管理に関する就業規則（抄）の例」を参照。

~~ントにおける~~不審な挙動や異常を検知し、管理者に通報して早期の対応を支援するソリューションを活用するなど可視性を強化してセキュリティコントロールのレベルを維持する努力を講じる事も考えられます。

○　さらに、テレワークの場合、企業内での場合と異なり物理的な視認性の確保が困難なことから、テレワークに伴うログをＰＣ管理ツール等を活用して記録して、安全に保存及び収集するようにします。このログには、秘密情報へのアクセス履歴、利用者の操作履歴（Ｗｅｂのアクセスやメールの送受信履歴など）、ＶＰＮ装置へのアクセス履歴、テレワーク関連機器やクラウドサービスにログインした際の認証・操作履歴、テレワーク端末の操作履歴等についても取得します。

ｐ．秘密情報の管理の実施状況や情報漏えい行為の有無等に関する定期・不定期での監査

○　内部監査等を実施する際に、秘密情報の管理が適切に実施されているかを監査するとともに、資料の不足・欠損、不審な情報システムログ等の情報漏えい行為につながり得る兆候がないかを監査するとともに、監査が実施されている旨を周知します。

※監査の実施は、従業員等の秘密情報の取扱い方法等に関する認識を高めることにもつながります（秘密情報に対する認識向上（不正行為者の言い逃れの排除））。

④「秘密情報に対する認識向上（不正行為者の言い逃れの排除）」に資する対策

ここで紹介する対策は、

ａ．秘密情報の取扱い方法等に関するルールの周知

ｂ．秘密保持契約等（誓約書を含む）の締結

ｃ．秘密情報であることの表示

を行うことで、従業員等の秘密情報の対象範囲や取扱いについての認識を深めることを目的としています。これにより、同時に、不正に情報漏えいを行う者が「秘密情報であることを知らなかった」、「社外へ持ち出してはいけない情報だとは思わなかった」、「秘密を保持する義務を負っている情報だと思わなかった」といった言い逃れができないようにします。

また、企業と退職予定の従業員との関係によっては、退職予定者が秘密保持誓約書の提出を拒否することがあり得ることから、退職時だけでなく、入社時や配属先の異動時、重要プロジェクトへの配属時・転出時・終了時にも、必要に応じて秘密保持契約を取り交わすことが秘密情報に対する認識向上（不正行為者の言い逃れの排除）に資する対策として有効であると考えられます。

ａ．秘密情報の取扱い方法等に関するルールの周知

○　秘密情報の取扱い方法等に関する社内の規程等（本章３－３に記載）は、社内に周知しなければ、それを守るべき従業員等にその内容を認識させることはできません。そのため、社内の規程等の内容について、従業員等が認識できるよう、継続的に研修等を実施することが重要です。その際には、規程の内容のみならず、情報管理の徹底が自社の発展に貢献した事例や、社内で起こった秘密情報の漏えいとその結果に関する事例（「信頼関係の維持・向上等」に資する対策）といった具体的事例を取り上げながら、説明することも効果的です。

（本対策に必要な社内規程の条項）

- 社内規程の適用範囲
  ：役員、従業員、派遣労働者、委託先従業員（自社内において勤務する場合）等、本規程を守らなければならない者を明確にします。
- 秘密情報の定義
  ：本規程の対象となる情報の定義を明確化します。
- 秘密情報の分類
  ：分類の名称（例えば、「役員外秘」、「部外秘」、「社外秘」）及び各分類の対象となる秘密情報について説明します。
- 秘密情報の分類ごとの対策
  ：「秘密情報が記録された媒体に分類の名称の表示をする」、「アクセ

ス権者の範囲の設定」、「秘密情報が記録された書類を保管する書棚を施錠管理して持出しを禁止する」、「私物のＵＳＢメモリの持込みを制限し複製を禁止する」など、分類ごとに講じられる対策を記載します。

- 秘密情報及びアクセス権の指定に関する責任者
  ：分類ごとの秘密情報の指定やその秘密情報についてのアクセス権の付与を実施する責任者（例えば、部門責任者、プロジェクト責任者）について規定します。
- 秘密保持義務
  ：秘密情報をアクセス権者以外の者に開示してはならない旨などを規定します。

○　研修等については、以下のような方法が考えられます。

（研修等の内容の例）

- 「秘密情報の管理の重要性」、「秘密情報の分類」、「秘密情報の具体的取扱い方法」を盛り込んだ資料を作成する。なお、社内規程等の変更があった場合にはそれを盛り込む。併せて、④「秘密情報に対する認識向上（不正行為者の言い逃れの排除）」に直接資する対策ではないものの、「秘密情報の管理の実践例」、「秘密情報の漏えいとその結果に関する事例」、「関係法令の内容・改正状況」、海外からの情報窃取の動向（コラム「外国から狙われる企業の秘密」（ｐ３７~~１~~）を参照）、標的型攻撃メール（コラム「標的型攻撃メールってどんなもの？」（ｐ１２００~~０６~~）を参照）などの警戒すべき手口とその対処方法等を盛り込んだ説明資料を作成しておくと効果的。

（研修等の実施の例）

- 定例の会議等での説明資料の配布、社内電子掲示板等への掲示、電子メールでの送付。
- 定期的に行われる朝礼や課内会議等での、秘密情報の取扱いに関する注意喚起・意識の共有。
- 入社時、昇進時等、定期的に実施される研修の講義内容として盛り込む。
- 守るべきルールの変更（関係法令や社内規程の改正等）に伴う研修の実施。
- 秘密情報の管理に関する研修会を実施（情報漏えいリスクや責務に応

じた部門や役職ごとの研修会等の実施も効果的)。

- 従業員等がいつでも受講できるよう、e-ラーニングを導入。理解度確認付 e-ラーニング等の従業員等全員の受講が確認できる教育プログラムの実施。

教育訓練が情報漏えいの防止につながった事例

◆ **機械製造業･大規模企業の事例**
～標的型攻撃メールに対する訓練によって情報漏えいを防止～

過去、特定の部署に所属する従業員らの社用メールアドレス宛てに、実在する取引先の名前を用いた「なりすましメール」が複数送信された。これらのメールは取引の連絡のように見せかけて、添付ファイルを開封させようと巧妙に仕組まれたものであったが、日頃から教育･訓練を通じて、不用意に添付ファイルを開封しないこと、不審なメールが送信された場合や万が一不審なメールのファイルを開封してしまった場合には、すぐに情報セキュリティ担当に通報することを、社員に周知徹底していたため、実際の漏えいにはつながらなかった。

○　研修等を実施した後に、例えば、「研修内容について理解したので、今後の情報の取扱いには注意します」といった誓約書を取ることは、従業員等の認識を更に深める対策として有効です。

中小企業の周知事例

◆ **金型製造業･小規模企業の事例**
～改善策提案型会議で情報管理の重要性を周知～

一方的に情報管理について説明するのではなく、全社員が参加する会議において、情報管理策を提案しあうことによって、情報管理の重要性について共有するようにしている。これにより、従業員にも、当事者意識が芽生え、効果的な対策実行につながっている。

ｂ．秘密保持契約等（誓約書を含む）の締結

○　従業員等に、自社の秘密情報の範囲等について認識させる方策として、社内の規程等に加え、又は規程に代えて、秘密情報を取り扱う従業員等と秘密保持に関する契約を締結したり、従業員等に対して誓約書の提出を要請することが考えられます。

※規程等に加えて秘密保持契約を締結する場合は、秘密保持契約において、その規程の内容を引用し、規程を遵守することを義務として盛り込むという方法もあります。

○　秘密保持契約等は、従業員等個人が契約等の当事者になるため、その従業員等の秘密情報の管理に対する認識をより確実なものとする効果があります。

○　契約等に盛り込む内容として、「秘密を守る」という内容のみ規定した場合、退職時に社内資料を自宅に持ち帰ったまま返還しない、個人メールアドレスにメールを送信する等の行為は該当しないといった言い逃れを許すおそれがありますので、「持出禁止（持出が認められる場合はその条件）」、「返還、廃棄・消去（必要があればその確認）」といった取扱いの内容も定めておくことも考えられます。

○　秘密保持契約等を締結するタイミングとしては、入社・採用時、退職・契約終了時、在職中（部署の異動時、出向時、プロジェクト参加時、昇進時等の取り扱う情報の種類や範囲が大きく変更されるタイミング）等が考えられます。入社時の契約では、秘密保持義務の対象となる情報の特定は難しい場合が多いですが、在職中（特に、部署の異動時・出向時、プロジェクト参加時・終了時）、退職時には、対象となる情報の範囲の特定が徐々に容易になりますので、対象範囲をできる限り明確化した上で、秘密保持契約等を締結します[36]。なお、対象範囲の明確化については、単に特定の程度が高いほど良いということではなく、双方の認識が一致する程度に特定されているか否かがポイントとなります。

具体例

- 概括的な概念による特定：
  「～に関するデータ」、「～についての手順」というように、情報カテゴリーを示すことにより特定する方法。
  ex）「新技術Ａを利用して製造した試作品Ｂの強度に関する検査データ」
  ex）「Ｂの製造におけるＣ工程で使用される添加剤及び調合の手順」
  ex）「新築マンションＤに関する顧客情報」
- 媒体や保管場所等による特定：
  秘密情報が記録された媒体の名称や番号等により、情報を特定する方法。
  ex）「「極秘」と表示された情報」

[36] 秘密保持契約書の参考例については、参考資料２の「第３　秘密保持誓約書の例」を参照。

ex）「ラボノートＶに記載された情報」
ex）「書庫Ｗで施錠管理されている情報」
ex）「Ｘ社から提供されたファイルＹのうちｐ〇〇に記載された情報」
※「新技術Ａを利用して製造した試作品Ｂの強度に関するラボノートＶに記載された検査データ」のように、「概括的な概念による特定」と「媒体や保管場所等による特定」の方法を組み合わせて特定性を高めることも考えられる。

○　また、「ａ．秘密情報の取扱い方法等に関するルールの周知」における研修等の実施の後に、「研修内容について理解したので、今後の情報の取扱いには注意します」といった誓約書を従業員等から取る等、定期的に誓約書を取得することも、秘密情報の管理に係る認識を向上する対策として有効です。

ｃ．秘密情報であることの表示

ⅰ）秘密情報が記載された媒体への表示

○　社内の規程に基づいて、秘密情報が記録された媒体等（書類、書類を綴じたファイル、ＵＳＢメモリ、電子文書そのもの、電子文書のファイル名、電子メール等）に、自社の秘密情報であることが分かるように表示を行います。

○　表示は、社内の規程で定めた「秘密情報の分類」の名称を表示することが考えられます。その際、その表示を見た者が、その表示が付されている情報が、自社における秘密情報であることに加えて、アクセスできる者の範囲（例えば、「役員限り」等）や、どのような取扱い方法（例えば、「持出し禁止」、「返還、廃棄・消去」等）が求められている秘密情報であるのかも認識できるような表示とするとより効果的です。

○　また、秘密情報が記録された媒体等を保管する書庫や区域（倉庫、部屋など）に「無断持出し禁止」といった掲示を行うことも考えられます。

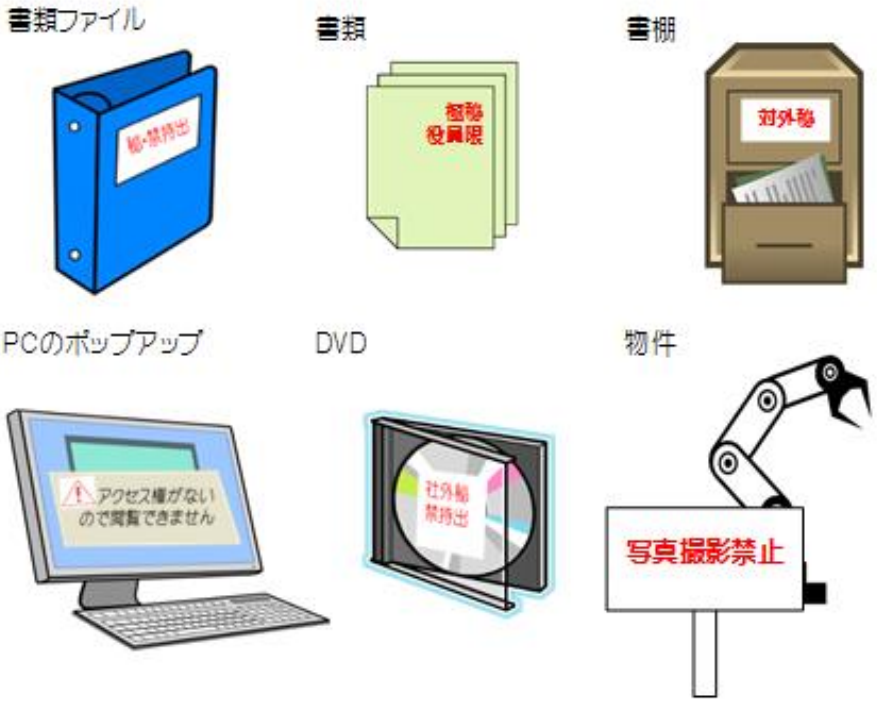
ⅱ）直接表示することが困難な物件等

○　工場の生産ラインのレイアウトや金型等、それ自体に秘密情報であることの表示が困難なものについては、自社の秘密情報に当たる物件が保管されている場所に「無断持出し禁止」、「写真撮影禁止」といった掲示をしたり、物件リストを作成して、従業員等へ周知するといった方法が考えられます。

※秘密情報の窃取を企図するアクセス権のない者に対しては、上記の掲示によって

これらの物件そのものが秘密情報であることを分かりやすくしてしまうという懸念がありますが、当該対策を通じて従業員等の秘密情報に対する認識を向上させることは、重要な情報漏えい対策であり、やはり表示していた方が望ましいと考えられます。

図表３（６）秘密表示の事例



⑤「信頼関係の維持・向上等」に資する対策

ここで紹介する対策は、従業員等に情報漏えいとその結果に関する事例を周知することで、秘密情報の管理に関する意識を向上させます。また、働きやすい職場環境の整備や適正な評価等によって企業への帰属意識を醸成したり、仕事へのモチベーションを向上させます。これらの取組みによって、職場のモラルや従業員等との信頼関係を維持・向上することを目的としています。

従業員等との信頼関係を維持・向上するための取組みは、企業の生産性向上や効率的な経営の実現などの観点からも重要なポイントであるため、企業においては既に創意工夫を凝らしながら様々な取組みが実施されているところですが、これらの取組みが、情報漏えい対策としても有効であると考えられます。

また、テレワーク実施中の従業員等は疎外感や不安感に悩むことが多いだけでなく、不審な挙動がすぐには見つからない状況にあることや外部の脅威者からのアプローチを受けやすいといった恐れがあります。このため、悩みに対して相談・助言を提供する窓口の設置やコミュニケーションツールの整備等を通じて、良好で十分なコミュニケーション機会を確保することは、従業員等の不安感・疎外感の払拭につながり、信頼関係の維持・向上のための対策としても有効であると考えられます。

【秘密情報の管理に関する従業員等の意識向上】

従業員等の、秘密情報の管理の重要性に関する理解を深め、漏えいに対する危機意識を高めることを目的とします。

ａ．秘密情報の管理の実践例の周知

○　秘密情報の管理等に係る研修等において、秘密情報の管理の徹底が、企業の発展・業績向上などに貢献したという事例を紹介して、秘密情報の管理の重要性に関する理解を深めます。

ｂ．情報漏えいの事例の周知

○　秘密情報の管理等に係る研修等において、秘密情報の漏えいが企業に多大な損害を与え得るものであることについて、自社内外の具体的な漏えいとその結果に関する事例等[37]をまとめた資料や映像等を準備し紹介します。

ｃ．情報漏えい事案に対する社内処分の周知

○　秘密情報の管理に係る研修等において、情報漏えい事案に対して、社内においてどのような処分がなされるのかについて、予め従業員等に説明しておくこと

[37] ＩＰＡ『組織における内部不正防止ガイドライン』に内部不正事例が紹介されています（ｐ９６~~６４~~参照）。

で、従業員等の情報漏えい行為を未然に防止します。ｂ.「情報漏えいの事例の周知」とともに説明するとより効果的と考えられます。

※社内処分については従業員等に対して過度な萎縮とならないような配慮が必要です。

【企業への帰属意識の醸成・従業員等の仕事へのモチベーション向上】

ｄ．働きやすい職場環境の整備

○　例えば、ワーク・ライフ・バランスの推進の観点から、長時間労働の抑制（適正な業務配分等）や年次休暇取得促進のための体制構築（労働時間の適正化、多様な休み方の提案等）、福利厚生の充実などを実施することにより、従業員等が働きやすい職場環境を整えて、企業への帰属意識を高めます[38、39]。

○　また、上司と部下、同僚同士がコミュニケーションを取りやすい職場環境を整えることも、企業への帰属意識を高めることに貢献します[40]。

○　なお、テレワーク実施中の従業員等は疎外感や不安感に悩むことが多いだけでなく、不審な挙動がすぐには見つからない状況にあることや外部の脅威者からのアプローチを受けやすいと考えられます。そこで、対策として、悩みに対して相談・助言を提供する窓口の設置やコミュニケーションツールの整備、定期的なアンケートによる疎外感・不安感を感じている従業員等の可視化、オンライン会議での定期的な職場コミュニケーションの実施、定期的な出勤日の設定等を通じて、過度な干渉にならない程度の良好で十分なコミュニケーション機会を確保することは、従業員等の不安感・疎外感の払拭につながる上、信頼関係の維持・向上のための対策としても有効であると考えられます。

ｅ．透明性が高く公平な人事評価制度の構築・周知

○　従業員等の業務範囲、責任を明確にし、業務への貢献を多面的に評価するなど

38　「働き方・休み方改善ポータルサイト」（厚生労働省：http://work-holiday.mhlw.go.jp/index.html）では企業の先進的取組み等が紹介されています。また、『ワーク・ライフ・バランスの実現に向けた　「３つの心構え」と「１０の実践」』（内閣府：http://wwwa.cao.go.jp/wlb/research/kouritsu/pdf/3point10jissen-1.pdf）では、ワーク・ライフ・バランスに係る基本的な実践方法や事例等が紹介されています。

39　日本労働組合総連合会では、「働くことを軸とする安全社会の実現」（https://www.jtuc-rengo.or.jp/activity/seisaku_jitsugen/data/201107_teigen.pdf?39）へのアプローチとして「ディーセントワークの実現（経済的・社会的に自立できる質の高い雇用とワーク・ライフ・バランスの実現）」の重要性を挙げています。

40　「あかるい職場応援団」（厚生労働省：https://www.no-harassment.mhlw.go.jp/）では、良好なコミュニケーションとその前提となるディスコミュニケーションの解消に参考となる様々な情報が紹介されています。

納得感の高い人事評価制度を構築して、従業員等の就労継続や昇進意欲を向上させることは、従業員等の仕事へのモチベーション向上につながります。

○ 従業員等の能力や希望等を踏まえて配属等の適正な判断を行うことも仕事への満足度やモチベーション向上につながります。

○ 新商品開発や生産効率化に資する発明、業務にかかるコスト削減への取組み、日々の業務の改善など、創意工夫を行って企業に貢献した者などに対する表彰制度や報奨制度[41]を導入することも、モチベーション向上に貢献します。

従業員のモチベーション向上事例

◆ **機器メンテナンス業・中規模企業の事例**
～工夫を発案した社員へのリスペクトにより従業員のやる気向上～

プレス機械のカタログ・図面データ（4000機種以上）を収集・利用し、経年劣化した機械の現状データ・修理ノウハウを独自に文章化して、知的資産として共有。作業ノウハウを文章化する際、アイディアを提案した社員名を明記・登録することで、「自分も会社の知的財産を作り出している」と従業員に当事者意識が芽生え、やる気が向上している。

41 特許法３５条の職務発明に関する発明者へのインセンティブ（報奨）付与については、特許法第 35 条第 6 項の指針（ガイドライン）（https://www.jpo.go.jp/system/patent/shutugan/shokumu/shokumu_guideline.html）が参考になります。

（２）退職者等に向けた対策

（退職者等とは）

自社を定年退職・中途退職した者（本人の意思に基づかない退職も含む）が典型的ですが、契約期間や実習期間が満了した派遣労働者や実習生など、自社内での勤務を終了した者を広く含みます。また、ここでは、退職の申出があってから実際に退職するまでの間の者など（退職予定者等）も含みます。

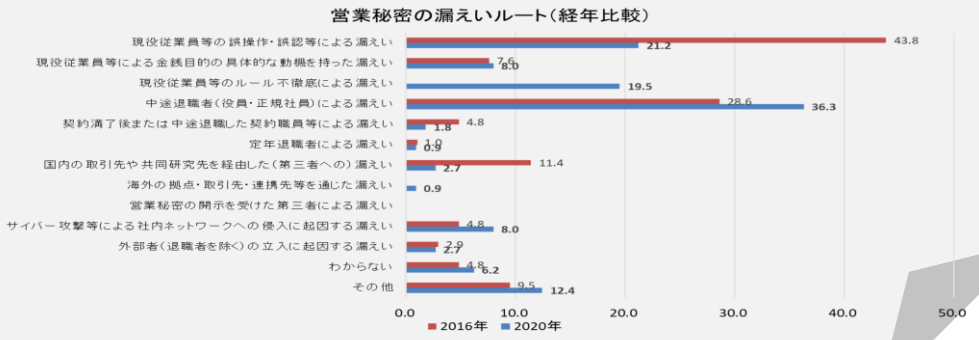
退職者等は、元々は従業員等であることから、退職予定者等に対しては、従業員等に向けた対策を、必要に応じて一部の対策を強化しつつ実施し、実際に退職した後については、転職先等での行動（営業や研究開発などの活動状況）や転職先の企業の動向（商品販売の状況、研究開発の動向）を把握するといった特有の対策を実施することが考えられます。

また、退職者との関係も常に円満な形での退職となるわけではなく、退職に際して秘密保持義務契約等の締結を拒否されるような事態に備えて、日頃から技術的・物理的な対策、通常時からの秘密保持契約書の締結等を組み合わせて備えておくことが重要と考えられます。

退職者に向けた対策の必要性

～情報漏えいの約半数は中途退職者に由来～

令和2年度にIPAが実施した調査によれば、企業における営業秘密の漏えいは、従業員・役員（現職・退職者）を通じたものが8割超に達している。また、中途退職者による漏えいは約4割で最多を占めており（前回4年前の調査と比較しても増加）、転職・独立など人材の流動化が進む中で、退職者を通じた情報の漏えい対策の重要性が高まっている。



①「接近の制御」に資する対策

ここで紹介する対策は、定年退職の場合は、しかるべきタイミングで、そして、中途退職の場合は申出を受けた後速やかに、秘密情報へのアクセス権を削除する等の対策を講ずることで退職までの間、秘密情報に近づけないようにすることを目的としています。

ａ．適切なタイミングでのアクセス権の制限

○　退職時には、遅滞なく、その退職者の情報システムの利用者ＩＤやアクセス権限（テレワークのための権限を含む）を削除します。加えて、確実にＩＤカードや会社への入館証を回収するとともに、当該ＩＤカード等では施錠された区域への解錠ができなくなっていることを確認します。

○　従事している業務内容によっては、退職予定者等について、しかるべきタイミングで、秘密情報へのアクセス権（テレワークのための権限を含む）を適切に制限することも考えられます。

②「持出し困難化」に資する対策

ここで紹介する対策は、退職予定者等について、従業員等に向けた対策に加え、その一部の対策をより厳格化したり、追加的な対策を実施する等して、秘密情報が記録された媒体等を社外へ持ち出す行為を物理的、技術的に阻止することを目的としています。

また、退職した従業員等が海外において秘密情報を不正に開示・使用するような事態に備えて、退職前の事前対策を十分に講じることが必要です。例えば、秘密情報を安易に海外に持ち出さないように警告するとともに、技術的・物理的な情報漏えい対策をしっかりと講じることが考えられます。

【従業員等に向けた対策（再掲）】

（書類、記録媒体、物自体等の持出しを困難にする措置）

ａ．秘密情報が記された会議資料等の適切な回収

ｂ．秘密情報の社外持出しを物理的に阻止する措置

ｃ．電子データの暗号化による閲覧制限等

ｄ．遠隔操作によるデータ消去機能を有するＰＣ・電子データの利用

（電子データの外部送信による持出しを困難にする措置）

ｅ．社外へのメール送信・Ｗｅｂアクセスの制限

ｆ．電子データの暗号化による閲覧制限等

ｇ．遠隔操作によるデータ消去機能を有するＰＣ・電子データの利用

（秘密情報の複製を困難にする措置）

ｈ．コピー防止用紙やコピーガード付の記録媒体・電子データ等により秘密情報を保管

ｉ．コピー機の使用制限

ｊ．私物のＵＳＢメモリや情報機器、カメラ等の記録媒体・撮影機器の業務利用・持込みの制限

【退職予定者等に対する特有の措置】

ｋ．社内貸与の記録媒体、情報機器等の返却

○　定年退職が近い者の場合は、従事させる業務内容も踏まえた適切なタイミングで、中途退職者については、退職の申出を受けてから速やかに会社貸与の記録媒体や情報機器を返却させます。

※記録媒体、情報機器等の返却時には、その記録媒体や内部に保管された電子データ等に対して、利用者が設定したパスワードも提出させるようにします。

○　必要に応じて、在職中に使用していたＰＣは回収し、実際に退職するまでは初

期化されたＰＣを新たに貸与して残務に従事させるということも考えられます。

③「視認性の確保」に資する対策

ここで紹介する対策は、退職予定者等については、従業員等に向けた対策に加え、その一部の対策をより厳格化する、追加的な対策を実施する等して視認性を高め、秘密情報の漏えいを行ったとしても見つかってしまう可能性が高い状態であることを認識させるようすることを目的としています。

また、退職者については、可能な範囲で転職先での行動（営業や研究開発などの活動状況）や転職先の企業の動向（商品販売の状況、研究開発の動向）等を把握するような対策を講ずることが考えられます。

【従業員等に向けた対策（再掲）】

（管理の行き届いた職場環境を整える対策）

- **ａ．職場の整理整頓（不要な書類等の廃棄、書棚の整理等）**
- **ｂ．秘密情報の管理に関する責任の分担**
- **ｃ．「写真撮影禁止」、「関係者以外立入り禁止」の表示**

（目につきやすい状況を作り出す対策）

- **ｄ．職場の座席配置・レイアウトの設定、業務体制の構築**
- **ｅ．従業員等の名札着用の徹底**
- **ｆ．防犯カメラの設置等**
- **ｇ．秘密情報が記録された廃棄予定の書類等の保管**
- **ｈ．外部へ送信するメールのチェック**
- **ｉ．内部通報窓口の設置**

（事後的に検知されやすい状況を作り出す対策）

- **ｊ．秘密情報が記録された媒体の管理等**
- **ｋ．コピー機やプリンター等における利用者記録・枚数管理機能の導入**
- **ｌ．印刷者の氏名等の「透かし」が印字される設定の導入**
- **ｍ．秘密情報の保管区域等への入退室の記録・保存とその周知**
- **ｎ．不自然なデータアクセス状況の通知**
- **ｏ．ＰＣやネットワーク等の情報システムにおけるログの記録・保存とその周知**

  ※ただし、モニタリングすることの目的が従業員等の保護であることを就業規則等に明記して従業員等に周知徹底するとともに、従業員等の理解を得た上で、適切な運用を行うことが必要。

- **ｐ．秘密情報の管理の実施状況や情報漏えい行為の有無等に関する定期・不定期での監査**

【退職予定者等に対する特有の措置】

ｑ．退職をきっかけとした対策の厳格化とその旨の周知

○　現職の従業員等に向けた「視認性の確保」に資する対策について、退職の申出等をきっかけとして、必要に応じて、例えば、以下のような形で厳格化します。

（厳格化する対策の例）

- 「ｏ．ＰＣやネットワーク等の情報システムにおけるログの記録・保存とその周知」について、退職の申出があった後だけでなく、以前のものも含めて、ログを集中的に確認する。
- 「ｏ．ＰＣやネットワーク等の情報システムにおけるログの記録・保存とその周知」について、視認性の確保が困難になるテレワークについて、退職の申出があった後にはテレワークに伴う履歴やクラウドサービスログイン時の認証・操作ログの確認など、一般の従業員と比べて高度な確認を行う。

退職者予定者に対する措置の事例

◆　**自動車製造業･大規模企業の事例**

～退職の申出後すぐに対応して情報漏えい防止を強化～

従業員から退職の申出があった後は、すぐに、過去にさかのぼって当該従業員の過去のログの確認を行うとともに、会社PCの持出しと会社PCからインターネットへの接続を全面的に禁止して、退職者による情報漏えい防止の強化を図っている。

ｒ．ＯＢ会の開催等

○　例えば、ＯＢ名簿や中途退職者名簿の作成・定期的な更新を行ったり、ＯＢ会の開催を通じて退職者との定期・不定期の交流機会を持ったりすることで、退職者の動向の把握に努めていることを認識させることが考えられます。その他、同期会などにおいて中途退職者の近況について情報が得られる可能性もあります。

○　一方で、ＯＢ会に現役社員も参加する場合には、ＯＢが現役社員から最新の情報を得る良い機会になってしまうこともありますので、参加する現役社員への予めの注意喚起が重要です。

退職者の状況把握の事例

◆ **鉄鋼業･大規模企業の事例**

～OB会を通じてゆるやかに状況把握～

従業員から退職の申出があった後は、速やかに個別に面談を実施し、当該従業員が接していた秘密情報である文書や図面を確認して再度の秘密保持契約を締結している。さらに、定期的に OB 会を開催して、緩やかに退職者の退職後の近況を把握するようにしている。

④「秘密情報に対する認識向上（不正行為者の言い逃れの排除）」に資する対策

ここで紹介する対策は、退職予定者等に、漏えいしてはいけない自社の秘密情報について、再度確認等することでその認識を高めることを目的としています。これにより、同時に、退職時に情報漏えいを行った者が「秘密情報であることを知らなかった」等の言い逃れができないようにすることを目的としています。

また、退職者との関係も、常に円満な形での退職となるわけではなく、退職に際して秘密保持義務契約等の締結を拒否されるような事態に備えて、日頃からその他の対策（技術的・物理的な対策、通常時からの秘密保持契約書の締結等）とあわせて備えておくことが重要と考えられます。

ａ．秘密保持契約等の締結

○　特に退職後時には、改めて明確な注意喚起を行うべく、就業規則等による一般的な秘密保持義務に係る規程の有無にかかわらず、退職者と、個別に秘密保持契約等を締結することが重要です[42]。

○　秘密保持契約等の締結に当たっては、退職予定者等との面談等を通じて、在職中にアクセスした秘密情報を確認し、それらが秘密保持義務の対象に含まれるように秘密保持義務を設定します（加えて、その面談の内容を客観的な形で記録を残すことも考えられます）。

※なお、退職時に突然契約の話をされると、退職者が当惑する可能性があることから、退職時に秘密保持契約を締結する場合があることを事前に周知しておくと、よりスムーズに契約締結の手続を進められるでしょう。

ｂ．競業避止義務契約の締結

○　退職者のうち、例えば、重要なプロジェクトにおけるキーパーソンなど、自社の利益を守るために秘密保持義務をより実効的にすることが必要だと考えられる場合、競業避止義務契約を締結することも考えられます。

○　しかし、競業避止義務契約は、秘密保持契約と異なり、より直接的に「職業選択の自由」を制限するおそれがありますので、労使相互において、その必要性や内容の十分な理解を図るとともに、義務範囲を合理的なものとすることが重要です[43]。

42　退職時の秘密保持誓約書の例については、参考資料２の第３における「３　従業員等の退職時」を参照。

43　競業避止義務契約の有効性については、参考資料５「競業避止義務契約の有効性について」を参照。

※なお、退職時に特有の契約の一つとして、ここで競業避止義務について紹介していますが、競業避止義務契約は、秘密保持義務をより実効的にするものであるため、この契約自体が直接的に「秘密情報に対する認識向上（不正行為者の言い逃れの排除）」に資する対策ではないことに留意が必要です。

ｃ．秘密情報を返還・消去すべき義務が生ずる場合の明確化等

○　退職時に締結する秘密保持契約において、秘密保持義務の対象となる情報が記録された資料や記録媒体を返還するとともに、電子データについては消去し、その情報を自ら一切保有しないことを確認するといった契約条項を盛り込みます。

○　この対策により、退職者等が、返還・消去すべき情報を認識できるようにします。また、返還・消去義務に違反した者が、「返還・消去すべき情報だとは思わなかった」、「返還・消去したと言った覚えはない」といった言い逃れをすることを防ぐことも可能となります。

⑤「信頼関係の維持・向上等」に資する対策

ここで紹介する対策は、適切な退職金の支払い等により、退職時まで退職者等との信頼関係を持続させること等を目的としています。また、こうした対策は、退職後においても退職者等との良好な関係を維持することにもつながり得ます。

なお、これらの対策は、通常、情報漏えいの防止を主たる目的として実施されるものではありませんが、これらの取組みを通じて退職者等との信頼関係が継続されることによって、自社の秘密情報の漏えいを防ぐ効果もあると考えられます。

ａ．適切な退職金支払い

○　退職金制度を設けている場合には、法令に従い、就業規則等により、適用される従業員等の範囲や退職手当の計算方法、支払い方法、支払い時期等を予め明確にしておき、それに基づいた適切な退職金の支払いを実施することにより、円満な退職を促し、退職時まで退職者等との信頼関係を持続するようにします。

○　キーパーソンについては、一旦退職した後も、改めて秘密保持義務契約を締結した上で、アドバイスやコンサルティングを行う「非常勤顧問」として再雇用することも考えられます。

ｂ．退職金の減額などの社内処分の実施

○　競業避止義務契約に反して競合他社に再就職する等、退職後において情報漏えいを行う可能性が高いと認められる場合には、退職金の減額処分や返還請求などが実施されることを予め社内に知らせておき、それを現実に実施することで、退職者の漏えいに対する危機意識を高めます[44]。

[44] 競業避止義務契約の有効性については、参考資料５「競業避止義務契約の有効性」を参照。

（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における交渉~~（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。

（ここで紹介する対策）

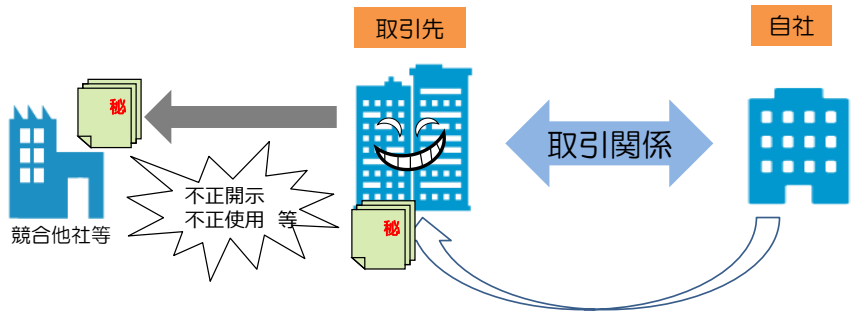
○ 取引先を通じた情報漏えいの中には、大別して、以下の２つのパターンが考えられます。

（ⅰ）取引先自体が主体となり悪意で情報の不正使用や不正開示を行う場合

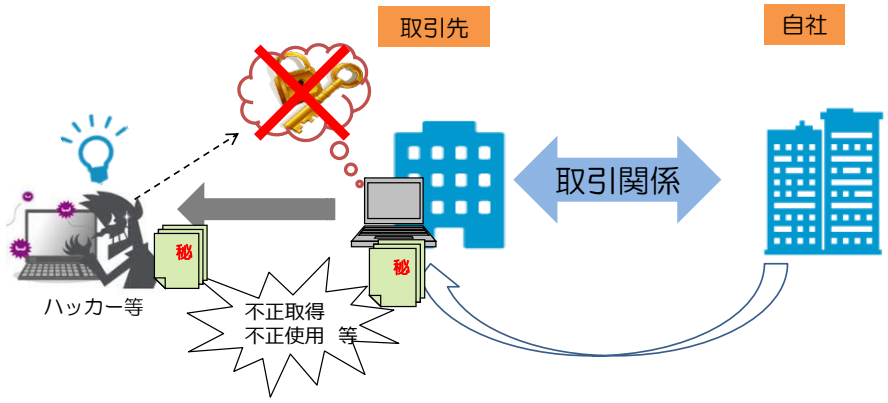
（ⅱ）取引先の情報管理が不十分であったことに起因して、相手方従業員、退職者、再委託者や外部者等を通じて情報漏えいしてしまう場合

図表３（７）取引先を通じた情報漏えいのパターン

（ｉ）取引先自体が主体となる情報漏えい



（ii）取引先の管理不十分による情報漏えい



○　（ｉ）に関しては、取引先に対して自社が直接情報漏えい対策を実施する必要があり、（ii）に関しては、取引先の社内での情報漏えい対策の実施を、当該取引先に対して要請することが考えられます。

○　ここでは（ｉ）に係る対策を中心に紹介しています。（ii）については、自社内で実施する対策の水準等を参考に、必要と考えられる対策を取引先に実施させるという観点から、契約内容等を検討することが重要です。

（取引を開始する前に留意すべき点）

○　取引先への対策を検討する前提として以下の２点について留意することが重要です。

➢　秘密情報を取り扱う業務を不用意に委託しない

秘密情報を取り扱う業務について委託等を検討する場合、予め、その委託等により生ずるリスクを考慮し、真に必要な取引であるかを検討する必要があります。例えば、コストを安く抑えられるからという理由だけで海外の取引先に不用意に秘密情報を取り扱う業務を委託してしまうと、物理的に管理が行き届かないばか

りでなく、法律や商慣行の違い等により漏えいリスクが高まる可能性もあります。

➢　取引先の管理能力の事前確認

取引先の決定に当たっては、当該相手方が秘密情報を適切に管理し、かつ、自社からの情報管理に係る要請に適切に対応できる能力を有するか否かを、事前調査や、ＩＳＭＳ（情報セキュリティマネジメントシステム）などの基準・認証・資格などを参考としつつ、事前に確認することが重要です[45]。

○　以上の２点を踏まえ、取引先に秘密情報を共有することを決定した場合、取引先に向けた対策として、以下を検討します。

[45] 委託先の情報管理能力を確認する際に参考となる基準としては、ＩＳＭＳが代表ですが、その他には、例えば、内閣サイバーセキュリティセンター（ＮＩＳＣ）が政府機関向けに策定している『政府機関の情報セキュリティ対策のための統一基準群（~~令和３年度版~~令和５年度版）』の中の「政府機関等のサイバーセキュリティ対策のための統一基準（令和５年度版）」（~~https://www.nisc.go.jp/active/general/kijunr3.html~~https://www.nisc.go.jp/pdf/policy/general/kijyunr5.pdf）のｐ~~２６~~１４２以降に、政府機関が外部委託する場合のセキュリティ基準が掲載されているので参考になるでしょう。また、今後は委託先の業務従事者の中に「情報処理安全確保支援士」（https://www.ipa.go.jp/jinzai/riss/index.html）など~~「情報セキュリティマネジメント試験」（https://www.jitec.ipa.go.jp/sg/）（平成２８年度春期から開始）~~の有資格者がいるかどうかといった観点も参考になるでしょう。

取引先の選定時の確認事例

◆ **医薬品製造業・大規模企業の事例**

～事前・事後のダブルチェック、再委託先にも同様の確認を～

委託先と個人情報を共有する場合、情報の預託前に訪問して情報セキュリティ体制について調査を行う。ISMS認証取得事業者やプライバシーマーク付与事業者の場合には特段の事情がない限り契約前調査のみで済ませるが、そうでない事業者の場合、契約後にも定期的な監査を実施している。また、委託先から再委託という形で別の事業者が関与する場合にも、同様の事前確認を実施する。

①「接近の制御」に資する対策

ここで紹介する対策は、取引先において、極力、秘密情報に接触する者を少なくし、権限のない者を秘密情報に近づきにくくすることを目的としています。

ａ．取引先に開示する情報の厳選

○　取引先に秘密情報を開示して事業を遂行することを決定した場合には、取引契約の前後に関わらず、それぞれの秘密情報について、開示の必要性を慎重に判断し、開示する秘密情報を必要最低限に厳選することが重要です。なお、秘密情報の開示に当たっては、事前に秘密保持契約を締結することが有効です[46]。

具体例

- 契約前の商談等の場においては、秘密情報が記載された資料は渡さず、その場で回収したり、コアな情報は伝えないよう徹底する。また、オンラインでの打合せの場合には、オンライン会議の画面上で共有する情報についても事前に精査する、発表前に録画機能が用いられていないかどうか確認する。
- コア技術に係る特に重要な秘密情報は取引先に開示せず、周辺技術のみ開示し、その範囲のみでの業務委託にする。
- 複数の委託先に業務を分担させた上で情報を渡す事で、特定の取引先に情報が集中しないように配慮する。
- 取引先が自社に来訪する場合でも、書庫や工場等への不必要な立入りをさせないようにする。
- 契約の範囲外の情報を渡さないよう徹底する。

[46] 取引先との秘密保持契約の参考例については、参考資料２の「第４　業務提携の検討における秘密保持契約書の例」以下を参照。

取引先に渡す情報を厳選している事例

◆ **機械部品製造業･中規模企業の事例**
～過去の失敗を踏まえ、工程サンプルは渡さない～

過去に、工程サンプルを渡して契約交渉中だった取引先が、その工程サンプルを海外の競合他社に渡し、同じ製品を作られてしまったことがあった。それ以来、工程サンプルは絶対に渡さないようにしている。さらに、取引先に見積書を出す段階で、見積書の中に「自社のノウハウ（図面、工程サンプル）は、財産であり、提供しない」と明記している。

ｂ．取引先での秘密情報の取扱者の限定

○　取引先において、秘密情報の取扱者が不必要に増えると、その分管理が行き届きにくくなり、漏えいのリスクが高まると考えられます。したがって、取引先において秘密情報を取り扱う者を限定することが重要です。

具体例

- 契約書等において、取引先における秘密情報の取扱者を指定する。その際、取扱者を変更する場合には、自社の許可が必要である旨契約書に規定する。
- 契約後の秘密情報のアクセスについては自社サーバ═を利用することとし、そのアクセス権限を自社で管理する。（その際、サーバ═へのアクセスログを記録・確認することは、③「視認性の確保」にも資するものと考えられる。）

○　サプライチェーン間での秘密情報の受け渡しの機会が増えていることから、秘密情報の受け渡しに関しては、重要度に合わせた組織内部での管理・取扱いの手順を定めるとともに、委託先等の取引先の関係者にこれを遵守させる必要があります。対策が脆弱な取引先から秘密情報が漏えいしないように、その対策状況を踏まえて提供する秘密情報の範囲を制限する、委託その他の契約時に合意した基準・規定に基づいて提供先（取引先）における遵守状況を監査できるようにするといったサプライチェーン対策を講じることが重要です。

②「持出し困難化」に資する対策

取引先に秘密情報を共有・開示する場合には、自社サーバ═の利用等を除き、既に秘密情報を物理的に自社外に出しているため直接の管理が及ばず、不正な持出しを困難にする対策は基本的に考えられません。したがって、①「接近の制御」に記載した対策を中心に、その他の目的に資する対策を確実に実施することが重要です。

ａ．秘密情報の消去・返還と複製できない媒体での開示

○　契約満了時や契約解除時に取引先が自社の秘密情報をそのまま持ち続けてしまうことのないよう、委託契約や秘密保持契約等に、秘密情報の返還義務や消去義務を設けることが重要です。特に秘密情報を電子データで取引先に開示した場合には、消去義務に併せて、消去した旨の報告義務や消去の証明義務を設けることが有効と考えられます。

○　この実効性を確保するためには、複製ができない媒体（コピー防止用紙やコピーガード付のＵＳＢメモリ、ＣＤ－Ｒ等）や、文書作成ソフトの一般的な機能などを活用し、コピー・印刷や記録媒体への記録を禁止する設定を施した電子データを用いることも考えられます。

○　業務の委託等に当たり、取引先に対して自社が直接管理できるサーバ═を使用させた場合、そのサーバ═内のデータのダウンロードや印刷等を禁止する設定とするなど、取引先が実施できる操作を必要最低限にすることが有効です。

ｂ．遠隔操作によるデータ消去機能を有するＰＣ・電子データの利用

○　アクセス権者の頻繁な変更を自社で直接コントロールしたり、契約満了後等に、万一ＰＣやデータが取引先に残った場合に備え、以下の市販のツールやサービスを利用することも考えられます。

具体例

- 遠隔操作によりＰＣ内のデータを消去できるツール。
- 情報機器について、パスワードロックで、一定回数、認証に失敗すると重要情報を消去するツール。
- 一定期間、管理サーバ═とのやり取りがなされない状態が続いた場合に指定したデータが自動的に消去されるサービス。
- 電子データそのものに遠隔操作による消去機能を備えさせるツール。

③「視認性の確保」に資する対策

ここで紹介する対策は、取引先について視認性を強化し、秘密情報を漏えいしたとしても見つかってしまう可能性が高い状態であることを認識させることを目的とします。また、こうした取組みを強化することにより、互いの状況をよく把握できるようになり、情報漏えいの疑いが生じた場合等にも、客観的事実に基づいて判断できるため、無用なトラブルを避けることにもつながります。

ａ．秘密情報の管理に係る報告の確認、定期・不定期での監査の実施

○　取引先に対し、秘密情報の管理に係る義務の履行状況を報告させ、その内容が契約内容に沿うものか否かを確認したり、定期・不定期に秘密情報の管理状況の監査を実施することにより、その管理を確実なものとするとともに、不正行為をしたとしても見つかってしまう可能性が高い状態であることを認識させることができます。

具体例

- 契約等に、秘密情報を管理していることを定期的に報告する義務を定め、その報告が契約内容に沿うものか否かを確認する。
- 契約等に、定期的に秘密情報へのアクセスログを提出させる義務を定め、アクセス者やその閲覧頻度等が契約内容に沿ったものか否か確認する。
- 契約等に秘密情報の管理状況について監査を実施する旨を規定し、定期・不定期に情報管理体制やその履行状況の監査を実施する。

ｂ．取引先に自社サーバ═を使用させてログの保全・確認を実施

○　~~個人情報など、~~漏えいした場合に他者に被害を与えるような情報の場合や、多数の者により管理・活用される情報など、特に取引先の視認性を確保する必要があると考えられる場合には、自社が直接管理できるサーバ═を使用することを条件とした委託契約等を締結し、そのログを確認することが考えられます。なお、その際、当該サーバ═は、一定のセキュリティレベルが保たれていることが前提です。

④「秘密情報の認識向上（不正行為者の言い逃れの排除）」に資する対策

ここで紹介する対策は、取引先に対し、漏えいしてはいけない秘密情報を明示し、その認識を深めることを目的としています。また、それにより取引先が情報漏えいを行った際に「秘密情報であることを知らなかった」等の言い逃れができないようにすることも目的としています。

ａ．取引先に対する秘密保持義務条項

○　取引先に対し、自社が開示する情報が秘密情報であり、取引先にとって秘密保持の対象になるということを示すため、取引開始時に、秘密保持の対象となる情報をできる限り明確化した秘密保持契約等を締結することが重要です[47]。

○　たとえば、秘密保持契約の締結に当たり、その対象を「○○で開示されたすべての情報」などとしてしまうと、事業を実施する中で、公知情報等を混在して開示してしまうこと等により、秘密保持の対象が不明確になる懸念があるため、以下の具体例を参考に、その対象を明確化することが重要です。なお、当該契約は、必要や状況に応じて見直すことも考えられます。

具体例

- 契約等において、秘密保持の対象を「基本契約又は個別契約により知り得た相手方の営業上又は技術上の情報のうち、相手方が秘密である旨明示したもの」とし、実際の秘密情報の受渡しに際して秘密であることを明示する。
- 契約書等において、「甲が乙に秘密である旨指定して開示する情報は、別紙のとおりである。なお、別紙は甲乙協力し、常に最新の状態を保つべく適切に更新するものとする」旨記載し、双方協議の上、秘密保持の対象情報を別紙としてリスト化し、リストは常に最新の状態を保つよう更新する。
- 委託契約等の事業開始後に事前の契約等において指定した情報の範囲を超えるものを口頭で開示した場合には、開示した側が、情報の開示後一定期間内に当該情報の内容を文書化し、当該文書を秘密保持義務の対象とすることとするなど、予め、口頭で開示した情報の取扱いに関する規定を設ける。

ｂ．秘密情報であることの表示

[47] 取引先との秘密保持契約の参考例については、参考資料２の「第４　業務提携の検討における秘密保持契約書の例」以下を参照。

○　実際に秘密情報に接する取引先の従業員の認識をより確実にするためには、取引先に開示する紙媒体の資料やファイル、ＵＳＢメモリ、ＣＤ－Ｒ等の記録媒体、電子データ等に「秘密情報」であることの表示をすることが重要です。

ｃ．具体的な秘密情報取扱い等についての確認

○　取引先の従業員等が、秘密情報について不適切な取扱いをすることのないよう、取引先が実施する秘密情報の具体的管理方法や契約終了後の取扱いを事前に確認した上で、それを契約書に定めることが有効です。

具体的な秘密情報取扱い等についての確認事例

◆　**電気機械器具製造業･大規模企業の事例**

～取引先と一体となって情報管理を実施～

取引先選定条件の一つとして「重要情報の機密保持」を掲げ、取引先と相互に秘密情報の適正な管理･活用･廃棄を推進する体制を構築している。

具体的には、取引先との契約締結前に、自社で作成した「情報セキュリティ基準」と「情報セキュリティ基準チェックシート」を提示して、取引先における情報セキュリティの体制を確認している。契約後においても、定期的に情報セキュリティの実施状況を確認している。

ｄ．取引先に対する秘密情報の管理方法に関する研修等

○　取引先での秘密情報の認識を確実にするため、契約における具体的な秘密情報の対象やその管理方法について研修等を実施することが有効です。なお、④「秘密情報の認識向上（不正行為者の言い逃れの排除）」に直接資する対策ではないものの、標的型攻撃メールなどの警戒すべき手口とその対処方法についても、併せて研修や訓練を実施することで、取引先に対する外部者からの不正アクセス行為等を通じて、自社の情報が漏えいしてしまうことを防ぎます[48]。

具体例

[48] 取引先従業員の教育研修にあたっては、ＩＰＡが公開している各種動画を従業員に視聴させるといった取組みも有効です。その他にも、ＩＰＡでは研修に用いることのできる各種素材を公表しています。

＜映像で知る情報セキュリティ＞

https://www.ipa.go.jp/security/videos/list.html~~https://www.ipa.go.jp/security/keihatsu/videos/~~

＜情報セキュリティ啓発＞

https://www.ipa.go.jp/security/keihatsu/features.html

- 重要な秘密情報を開示する場合には、取引先との秘密保持契約において、取引先における秘密保持に関する従業員への教育の実施を規定する。

ｅ．取引先とのやりとりの議事録等の保存

○　取引先に対し、秘密情報を開示するに当たり確認した事項や決定した内容について、それを記録として残すことは、取引先に秘密情報を授受したことを認識させるために有効です。

具体例

- 秘密情報の特定に当たって行う協議等のやりとりは、双方合意の上議事録を作成する。
- 秘密情報の授受に当たり、それを台帳で共有管理する（秘密情報の内容、授受の日時、保管場所、提供先等）。
- メールで秘密情報の授受を実施した場合にはそのメールでのやり取りを保存しておく。

⑤「信頼関係の維持・向上等」に資する対策

ここで紹介する対策は、取引先と自社との信頼関係を向上させることを目的としています。

なお、これらの対策は、通常、情報漏えいの防止を主たる目的として実施されるものではありませんが、これらの取組みを通じて取引先との信頼関係を維持・向上させることによって、取引先による秘密情報の漏えいを防ぐ効果もあると考えられます。

ａ．適正な対価の支払い等

○　関係法令や各種ガイドライン等を遵守し、取引を適正化して取引先と公正で円満な関係を築くことは、取引先が不正を起こすきっかけとなり得る環境を作らないための基本的な前提となります。

具体例

- 親事業者と下請事業者の関係の場合には、「下請適正取引等の推進のためのガイドライン」[49]を参考にして、価格協議を頻繁に実施して原材料価格等の高騰分を適切に取引価格に反映するなどの対応をする。
- コンプライアンス宣言等を作成・公表し、それに基づいて相手との関係を構築する。
- 公平な取引を推進するため、自社従業員に向けた倫理研修を実施する。

ｂ．契約書等における損害賠償や法的措置の記載

○　取引における契約書等において、秘密保持義務の違反時における損害賠償の責任を規定したり、契約時に、秘密情報の漏えい等に対して法的措置等の厳正な処置をとることを明記した自社のポリシーを通知すること等は、取引先による情報漏えいを牽制する効果があります。

ｃ．委託先に下請代金支払遅延等防止法が適用される場合の助言・支援

○　業務を委託する場合、秘密情報の取扱いについて必要なセキュリティ対策（委託先がテレワークを実施している場合は、テレワークセキュリティを含む）が確実に実施されることを契約に先立って確認するために、委託業務の内容に沿って、委託先の体制や規定等の点検、個人情報漏えい事故発生時に委託

[49]「下請適正取引等の推進のためのガイドライン」　業種別一覧
https://www.chusho.meti.go.jp/keiei/torihiki/guideline.htm

先が委託元の調査に協力する義務を負うことの確認、予め合意した規定等に基づいて委託後の監査に協力することが可能かどうかの確認等を実施し、その結果について適切に評価することが望まれます。

○　なお、委託先が下請代金支払遅延等防止法を適用される場合には、下請中小企業振興法に基づく「振興基準」[50]第３の~~５~~２（２）にあるように、委託先に対してセキュリティ対策の助言・支援を行うこととされています。また、セキュリティ対策に資する特定の物やサービスの購入を強制することは禁じられています。

情報管理を徹底して取引先の信頼を向上した事例

◆　**電子機器製造業･中規模企業の事例**

～「接近の制御」に資する対策を徹底して取引先の信頼も向上～

自社及び他社から預かった情報について、以下の対策を徹底して実施することで、取引先からの信頼も向上させた。

－工場の入口は二重の扉を設置。内側の扉は内部からのみ解錠可能とし、外部者の入構を制限。

－第三者に特別に入室を許可する場合、カメラは持込み禁止、携帯やスマホのカメラもレンズにシールを貼ってもらう。その上、取引先等から預かっている情報や部品等は、当事者以外の部品等は目に触れないよう、覆いを掛けて目隠し管理。

---

50 下請中小企業振興法は、親事業者の協力のもとに、下請中小企業の体質を強化し、下請性を脱した独立性のある企業への成長を促すことを目的としており、その柱の一つとして、下請中小企業の振興のための下請事業者、親事業者のよるべき振興基準の策定とそれに定める事項についての指導及び助言が含まれており、同法に基づき、下請事業者及び親事業者のよるべき一般的な基準として「振興基準」が定められています。

この中（第３　下請事業者の施設又は設備の導入、技術の向上及び事業の共同化に関する事項２　情報化への積極的対応）で、「⑵ 親事業者は、~~前号~~(1)の下請事業者による取組を~~の~~支援する~~の~~ため、下請事業者の要請に応じ、管理能力の向上についての指導、標準的なコンピュータ~~や~~、ソフトウェア~~、~~及びデータベースの提供、オペレータの研修、セキュリティ対策の助言及び~~・~~支援~~及び~~並びに国~~・~~及び地方公共団体~~自治体~~による情報化支援策の情報提供等の協力を行うものとする。」とされています。

「振興基準」　~~https://www.chusho.meti.go.jp/keiei/torihiki/shinkoukijyun.htm~~ https://www.chusho.meti.go.jp/keiei/torihiki/shinkoukijyun/zenbun.pdf

（４）外部者に向けた対策

（外部者とは）

基本的には前述の（１）従業員等、（２）退職者等、（３）取引先以外の者をいいます。例えば、工場への不法侵入者やサーバ═への不正アクセス行為者が該当します。また、そのような悪質性の高い者だけでなく、自社への来訪者（各種渉外販売員、工場見学者等）、各種メンテナンス業者など自社への立入りが許されている外部者も含まれます。

（留意点）

外部者に対しては、基本的に「⑤信頼関係の維持・向上等」に係る対策は有効ではなく、また、「④秘密情報の認識向上（不正行為者の言い逃れの排除）」に係る対策も有効でない場合が多いと考えられます。したがって、特にそれ以外の「①接近の制御」、「②持出し困難化」、「③視認性の確保」の対策を中心に対策を検討することが重要です。

特に、各種機器メンテナンス等、外部の事業者が自社の秘密情報に接する可能性のある業務を外注等する場合には、（３）取引先に向けた対策~~での留意点~~（ｐ８９~~０~~）での留意点と同様に、まずはその外注等の必要性をよく検討し、事業者を選定するに当たっては、当該事業者の秘密情報の取扱い体制について、事前に確認することが重要です。

（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~~秘密情報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考えられますので、不要な秘密情報が含まれないようにするなど、文書・書類の内容を確認し、何を提出するのか十分吟味・検討する必要があります。
- また、訴訟手続において開示された営業秘密の漏えいを防止する制度として、訴訟記録の閲覧等の制限（民事訴訟法第９２条第１項第２号）や秘密保持命令（法第１０条）などの制度があります。どのような手段を活用することが営業秘密の漏えい防止に効果的であるのか、弁護士等の専門家に十分に相談するなどしながら検討する必要があります。
- なお、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（ｐ８９）での留意点と同様に、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。

①「接近の制御」に資する対策

ここで紹介する対策は、外部者を秘密情報に極力近づけないことを目的としています。外部者に対しては、この「接近の制御」に資する対策を確実に行うことが最も重要です。

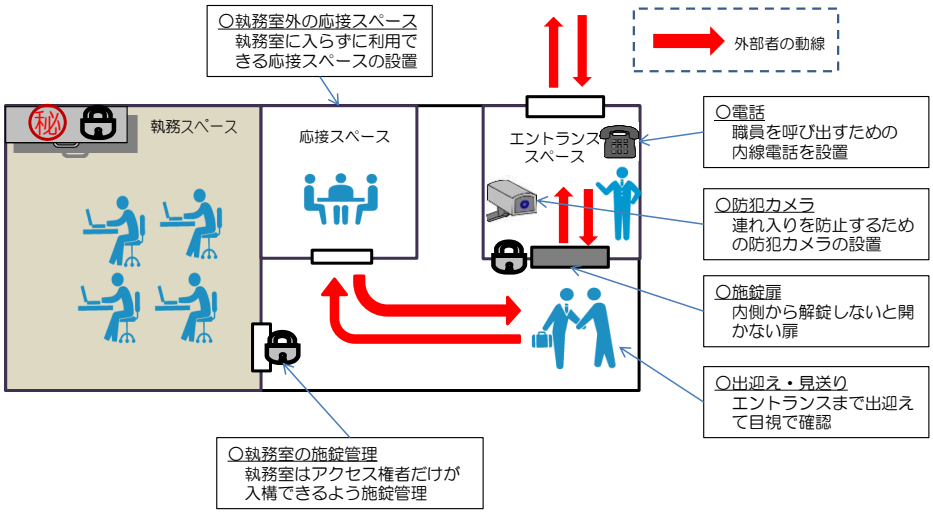
ａ．秘密情報を保管する建物や部屋の入場制限、書棚や媒体等のアクセス制限

○　秘密情報を保管する建物や部屋等については、許可された者以外は入場、入室等できないよう制限することが重要です。

具体例

- 秘密情報を保管する社屋の施錠管理（アクセス権を持たない者がアクセス権者と一緒に入構することを防止する観点から、防犯カメラの併設が望ましい）。
  ex）執務室には近づけないオフィスの設計（来訪者は玄関に設置された内線電話により、従業員を呼び出し内側から解錠してもらわなければ入構できない工夫、執務スペースを通らなくても応接スペースを利用できるようなレイアウトの工夫等）。
- 敷地入口での警備員による身分確認。
- 入構ゲートを設置し、ＩＤ認証での入構制限。
- 書類・ファイル、記録機器・媒体を保管する区域（書庫、サーバールームなど）を施錠管理し、入退室を制限。

図表３（８）オフィスのレイアウト例



○　各種メンテナンス業者等、物理的に社屋内等で活動する外部者に対しては、社屋への入構は一般的に許可されているため、入室できる場所を限定したり、秘密情報を管理する書棚やＰＣ、ＵＳＢメモリ等の記録媒体自体に制限をかけることが有効です。それらは、持ち出されてしまった場合にも有効な取組み（持出し困難化）であることがあります。

具体例
- 秘密情報を保管した書棚の施錠管理。
- ＩＤ、パスワードによるＰＣの認証管理。
- ＵＳＢメモリ等の記録媒体のパスワード管理。

ｂ．外部者の構内ルートの制限

○　工場の視察や見学など、外部者を受け入れる際には、そのルートを適正に限定し、従業員が同行の上、秘密情報が保管されたエリアや部屋には近づけないようにすることが有効です。

具体例
- それ自体が秘密情報である製造機械等はルートに含まない。
- 外部者の通るルート沿いにある机上やプリンタ、コピー機等に秘密情報を放置しない。
  - ex）外部者が通るルートに設置したＰＣはフィルム等を貼って画面をのぞかれないようにする。
  - ex）秘密情報が表示された物件にカバーをかける。
  - ex）秘密情報が保管されたサーバールームや書庫等については、フロアマップや部屋の表札等にはそれと分かる記載をしない。

ｃ．ペーパーレス化

○　自社内の秘密情報をペーパーレスにすることは、オフィスへの来訪者等が秘密情報に接する機会を少なくするため、外部者の秘密情報への接近の制御に有効です。その際、併せて電子化された秘密情報へのアクセス制限を実施することが望まれます。加えて、電子化された秘密情報について、印刷やコピーができない措置を施すことで②「持出し困難化」にも資することになります。なお、完全なペーパーレス化を実施することが難しい場合でも、電子化された秘密情報について、印刷できるデータの内容や、印刷できる者、印刷の目的等を限定するというルールを設け、併せてその印刷物の廃棄方法にも留意することで、同様の効果が得られます（廃棄方法についてはｄ．に記載）。

ｄ．秘密情報の復元が困難な廃棄・消去方法の選択

○　秘密情報が記録された書類・ファイルや記録媒体等の廃棄、秘密情報が記録された電子データの消去を行う場合、外部者が、廃棄・消去された情報を復元して、その情報にアクセスすることができないように、以下のように復元不可能な形にして廃棄・消去します。

（具体的な廃棄・消去方法）

- 書類の廃棄方法

ex）シュレッダーにより裁断し、廃棄。

※秘密情報の重要度に応じて、より復元を困難とするため、クロスカット（縦方向と横方向の両方から裁断する）方式のシュレッダーを利用するなど、かけることができる費用の多寡も踏まえながら、シュレッダーの機能性について検討することも重要。

ex）秘密情報を廃棄するゴミ箱は、廃棄後取り出すことができない鍵付きゴミ箱に限定。

ex）重要度の高い情報等については、信頼できる専門処理業者に依頼して焼却・溶解処分。場合によっては、その証明書を発行してもらう。

- 秘密情報を保存していた記録媒体（ＵＳＢメモリ等）、ＰＣ、サーバ═の廃棄方法

ex）市販されているデータ完全消去ソフトや、磁気記録方式のハードディスク磁気破壊サービス等を利用してデータを消去の上、その記録媒体等を物理的に破壊（記録媒体からデータを消去しただけでは復元されるおそれがあるため）。

ｅ．外部ネットワークにつながない機器に秘密情報を保存する

○　不正アクセス等に備え、ネットワークに接続された機器で利用・保管する必要性のない秘密情報については、その利用態様を踏まえ、外部ネットワークにつながない機器に保存することが有効です。

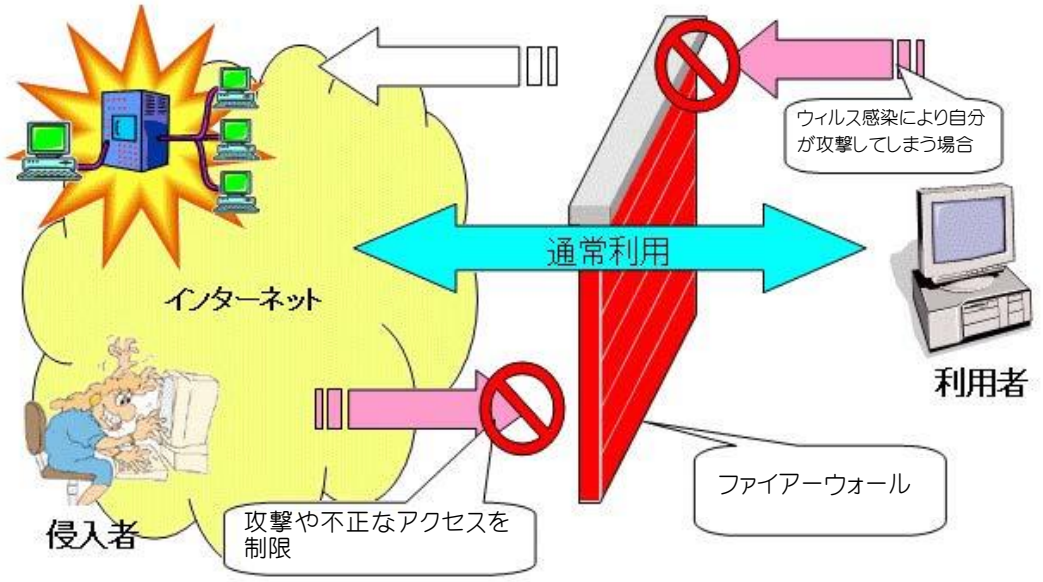
ｆ．ファイアーウォール、アンチウィルスソフトの導入、ソフトウェアのアップデート

○　ネットワークにつながったＰＣ等の機器に保管されている秘密情報を不正アクセス等から守るためには、ファイアーウォールの導入や、ウィルスに感染させないためのアンチウィルスソフトなどのセキュリティソフトの導入、各種ソフトウェアの適時のアップデートが重要です。さらに不正侵入防御シス

テムの導入等により防御することも有効と考えられます。

○　外部者からの標的型攻撃メールなどによる情報窃取活動への対抗手段として、まずは社内における秘密情報へのアクセス権者を最小限にする対策が有効となります。したがって、本章３－４　（１）　従業員等に向けた対策　①「接近の制御」　を確実に実施することが重要です。

図表３（９）ファイアーウォールとは

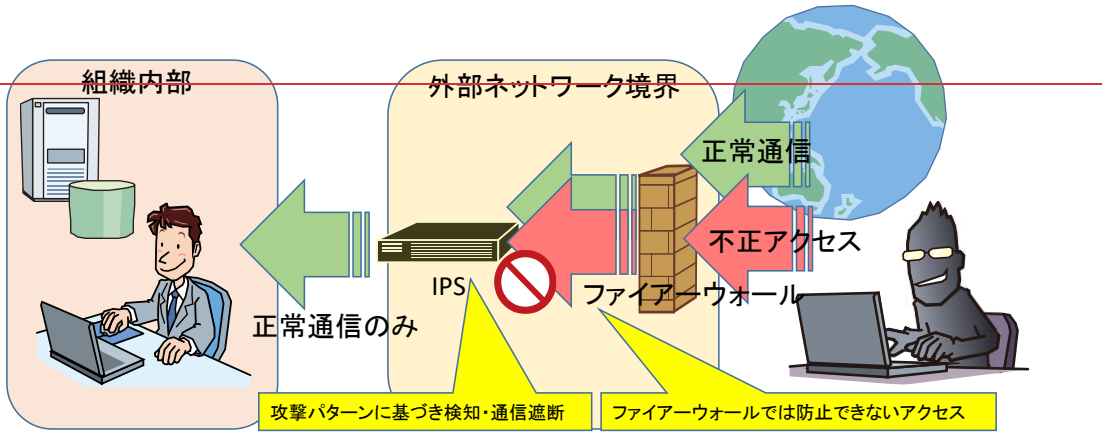


（ＩＰＡ『不正アクセス対策のしおり』より引用）

図表３（１０）不正侵入防御システムとは

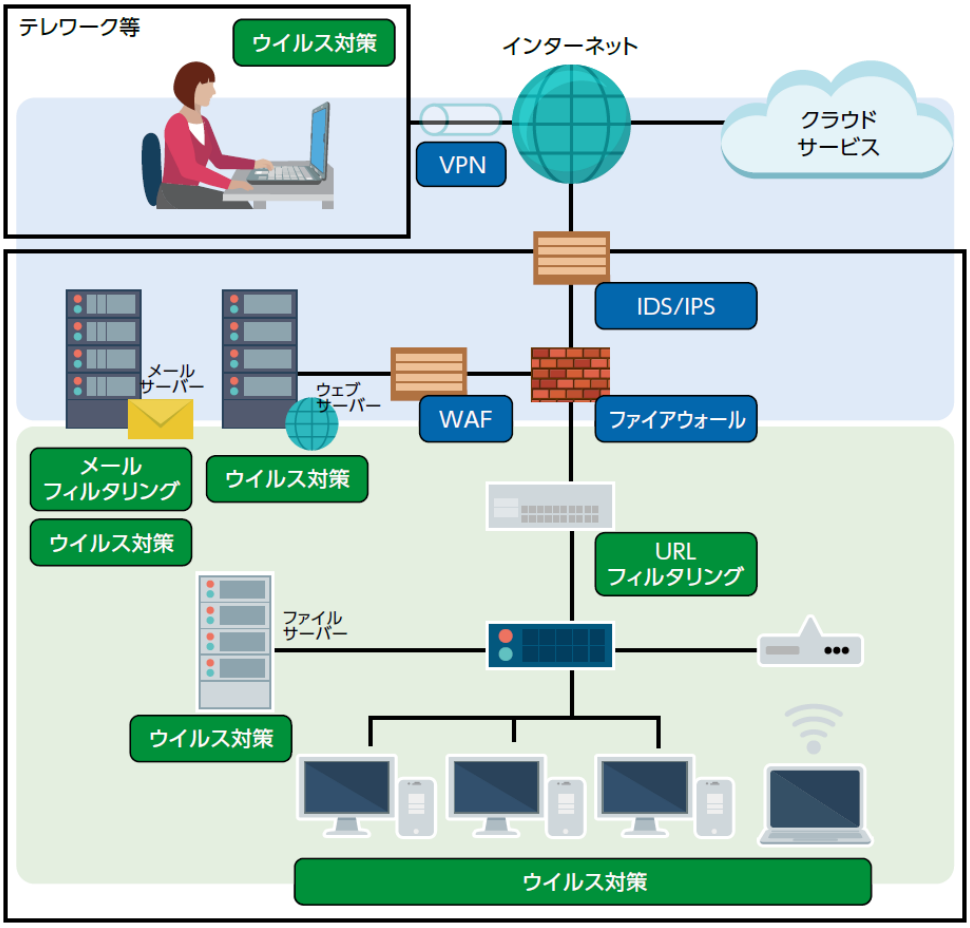
不正侵入防御システムとは

不正侵入防御システムとは、不正な侵入を検出したうえで、その攻撃を防御する機能を備えたシステムで、IPS（Intrusion Prevention System）と呼ばれます。攻撃パターンのデータベースを参照することで不正アクセスなどの有害な通信を検出し、遮断する機能を持ちます。



（図：ＩＰＡ作成）

図表３（９）技術的対策例



コンピュータやインターネットを利用するときに施すネットワーク関連の技術的対策例です。

・ファイアーウォール

通信をさせるかどうかを判断し許可する、または拒否する技術。例えば、インターネットと社内 LAN との間に設置して、外部からの不正なアクセスを社内のネットワークに侵入させないようにできます。

・IDS（Intrusion Detection System：侵入検知システム）

システムやネットワークに対する不正なアクセスなどを検知して管理者に通知する技術。例えば、インターネットとファイアーウォールの間に設置することで、不正アクセスと思われる通信を検知して管理者に通知できます。

・IPS（Intrusion Prevention System：侵入防御システム）

システムやネットワークに対する不正なアクセスなどを検知して自動的に遮断する技術。例えば、インターネットとファイアーウォールの間に設置することで、不正アクセスと思われる通信を検知して管理者に通知するとともに通信を遮断できます。

・WAF（Web Application Firewall）

ウェブアプリケーションの脆弱性を悪用した攻撃からウェブアプリケーションを

保護する技術。例えばファイアーウォールや IDS/IPS とウェブサーバの間に設置することで、ウェブアプリケーションがやり取りするデータを監視して攻撃を検出できます。

・VPN（Virtual Private Network）

インターネットのような公衆ネットワーク上で、保護された仮想的な専用線環境を構築する技術。例えば、テレワーク勤務者が職場との間で機密性の高い電子データをやり取りする際に、VPN を利用することで暗号化による安全な通信ができます。

（ＩＰＡ「中小企業の情報セキュリティ対策ガイドライン」[51]より引用）

ｇ．ネットワークの分離（複数のＬＡＮを構築）

○　ネットワークを分離することで、１つのネットワークに不正アクセス等があった場合でも、その他のネットワークに保管される秘密情報へは直接アクセスできないため、接近の制御の強化とともにウィルス等に感染した場合でも被害の拡散防止にもなります[52]。

51　「中小企業の情報セキュリティ対策ガイドライン」（https://www.ipa.go.jp/security/guide/sme/about.html）参照

~~52　VPN（バーチャルプライベートネットワーク）を適切に活用することで、安全性を担保しつつネットワーク構築に柔軟性を持たせることができるようになります。~~

②「持出し困難化」に資する対策

ここで紹介する対策は、外部者が仮に秘密情報にアクセスしたとしても、それを持ち出す行為を物理的、技術的に阻止することを目的としています。

ａ．外部者の保有する情報端末、記録媒体の持込み・使用等の制限

○　各種メンテナンス業者や見学者等が秘密情報を保管する場所に入場する場合には、秘密情報を記録等できる機器（ＰＣやＵＳＢメモリ等）や撮影機器（カメラ、スマートフォン等）の持込みを制限することが有効です。その際、荷物を預かったり、実際の見学に自社の担当者が付き添う等の取組みを併せて行うことで、より実効性が向上すると考えられます。

○　不正侵入者等による不正な複製等を制限するためには、ＰＣ等の機器に対する記録媒体の使用制限を実施することが有効です。

具体例

- ＵＳＢメモリの差込口がないものや、ＵＳＢメモリの差込口を無効化したり、物理的にふさぐ部品を取り付けたＰＣを利用する。
- 許可された会社貸与のＵＳＢメモリ以外は、ＰＣが認識しないよう設定する。

ｂ．ＰＣのシンクライアント化

○　データの保存といった機能をＰＣから切り離してサーバ＝に集中させ、ＰＣ自体には秘密情報を保管しない（ＰＣをシンクライアント化する）ことで、万が一ＰＣが盗難されたり紛失した場合にも秘密情報は持ち出すことができなくなります。

ｃ．秘密情報が記載された電子データの暗号化

○　秘密情報が記載された電子データを暗号化しておくことによって、たとえ電子データが不正に持ち出されてしまっても、複合のためのキー（パスワードなど）がなければ解読できない状態とします。

ｄ．遠隔操作によるデータ消去機能を有するＰＣ・電子データの利用

○　万一、ＰＣやデータが盗難された場合に備え、以下の市販のツールやサービスを利用することも考えられます。

具体例

- 遠隔操作によりＰＣやスマートフォン等の端末内のデータを消去できるツール。
- 情報機器について、パスワードロックで、一定回数、認証に失敗すると重要情報を消去するツール。
- 一定期間、管理サーバ═とのやり取りがなされない状態が続いた場合に指定したデータが自動的に消去されるサービス。
- 電子データそのものに遠隔操作による消去機能を備えさせるツール。

③「視認性の確保」に資する対策

ここで紹介する対策は、外部者に対する視認性を強化し、秘密情報の漏えいを行ったとしても見つかってしまう可能性が高い状態であることを認識させるようにすることを目的とします。

ａ．「関係者以外立入り禁止」や「写真撮影禁止」の張り紙等

○　秘密情報が保管されている書棚や区域（倉庫、部屋など）に、「関係者以外立入り禁止」等の張り紙や看板を設置することで、外部者の出入りに対する従業員等の関心が高まるとともに、外部者に対して情報管理に係る関心が高く、管理が行き届いた職場であると認識させることで、不正な立入りや情報漏えい行為を心理的に抑止する効果が期待できます。

※なお、「関係者以外立入り禁止」等の掲示の際には、同時に「入室に関する問合わせ先」も記入しておかないと、「立入り禁止とは分かっていたけれど、担当者を探して入室してしまった」といった言い逃れを許してしまいかねないことから、より心理的な抑止効果を高めるため、「関係者以外立入り禁止」の看板には、管理者の連絡先も併記することが有効です。

ｂ．秘密情報を保管する建物・区域の監視

○　秘密情報が記録された書類・記録媒体が保管・蔵置された建物や区域（倉庫、部屋など）、書棚、秘密情報の廃棄場所など、秘密情報の不正な取得や複製の現場となり得る場所について、以下のような方法により、不正行為が「目撃されやすい」状況とします。

具体例

- 秘密情報が保管された場所やその出入口が、従業員等の死角とならないようにレイアウトを工夫する。その上で、出入口の扉の開閉時にはチャイムやブザーがなるよう設定し、人の出入りが人目に立つ状態にする。
- 出入口での守衛による入退状況のチェック。
- 防犯カメラの設置。
- 入退室をＩＤカード等により制限し、その入退室のログを保存、確認。

○　不正アクセス等に備え、ＰＣやネットワーク等の情報システムにおけるログを記録・保存、確認することも重要です[53]。

[53] ~~特に近年その巧妙さを増す標的型攻撃への対策の際に参考となるものとして、自社のシステ~~

具体例

- ファイアーウォールのログなどの外部からの通信に係るログ（ファイアーウォールの透過や拒否のログなど）や、ＰＣ等のアクセス履歴に係るログ等を記録・保存し、定期的に確認（さらに、組織内から外部に向けた通信ログも保存して定期的に確認をすれば、万が一標的型攻撃メール等によりウィルスに感染し、社内の秘密情報が外部に送信された場合にも、速やかに発見することが可能）。

○　特に、各種メンテナンス業者等、外部業者などの、一定の社内における活動を許された者に対しては、それぞれの業者の担当者を決め、外部業者の活動内容や人員の配置等について定期的に報告させ、把握していない活動を実施していないか確認します（従業員の誰も何も知らないという状況で外部者が作業している状態をなくします）。なお、これらの取組みは、事案が発生した場合の客観的な証拠となり得るため、取引先に対する無用な疑いを避けることにもつながります。

具体例

- 入構の事前届出をさせたり、社内活動に係る日報等を提出させる。
- 機器のメンテナンス事業者が来室する際には、必ずそのメンテナンス作業に立ち会う。
- 外部業者であることが外見上明らかな状態にするため、社内では制服を着用することを契約において規定。
- 機器メンテナンス事業者等には、業務専用の一時的なＩＤを付与し、作業終了後は権限を無効化するとともに、ＰＣ等の作業画面の録画や操作ログを記録する。

○　また、秘密情報が保管される執務室等に外部業者などが立ち入る際には、執務室にいる従業員に対してそれを知らせることにより、秘密情報を放置したり、不用意に秘密情報を口にしてしまうことを防ぐことができます。

具体例

- 従業員への一斉メールで外部者の入室スケジュールを事前に周知する。

~~ム内部に深く侵入してくる高度な標的型攻撃を対象に、システム内部での攻撃プロセスの分析と内部対策をまとめたＩＰＡ『「高度標的型攻撃」対策に向けたシステム設計ガイド』があります。（https://www.ipa.go.jp/security/vuln/newattack.html）~~

- 外部者が入室した場合にアラートやチャイムが鳴ったり、赤色灯が回るようにする。

ｃ．来訪者カードの記入、来訪者バッジ等の着用

○　自社の従業員でない者が執務室等に立ち入る場合には、入口にて来訪者カード等を準備し、氏名や訪問先を記入してもらい、アポイントの有無を確認することなどにより、来訪者に対し、情報管理に係る関心が高く、管理が行き届いた職場であると認識させ、不正行為を心理的に抑制します。また、来訪者の入構時には、当該来訪者と実際に面識のある従業員が直接入口に出迎えることによって、来訪者のなりすましを防ぎます。

○　入構の際に、来訪者用のバッジ等を渡して着用してもらうことで、その者が来訪者であるということが外見上明らかとなり、従業員等の意識的又は無意識的な関心を集め、不正行為に対して心理的な抑止効果が期待できます。その際、来訪目的先ごとに色分けしたバッジ等を配布し、来訪目的の場所以外に立ち入った場合に人目に立つ状態にして、従業員が声掛けをすることも有効です（同時に、従業員等の社員証着用を徹底させ、社員証やバッジ等を「何も着用していない」ことが人目に立つ状態とすることにより、バッジ等を外されてしまう事態に備えることが考えられます）。

④「秘密情報の認識向上（不正行為者の言い逃れの排除）」に資する対策

ここで紹介する対策は、外部者が情報漏えいした際に「秘密情報であるとは気がつかなかった」等の言い逃れをできないようにすることを目的としています。ただし、外部者のうち、不法侵入者や不正アクセス行為者など、悪質性の高い者に対しては、基本的にはこれらの対策は効果が乏しい場合が多いと考えられますので、それらの者に向けた対策は、特に「①接近の制御」、「②持出し困難化」、「③視認性の確保」に資する対策を強化することが重要と考えられます。

ａ．「関係者以外立入り禁止」や「写真撮影禁止」の張り紙等（再掲）

○　不正行為者の言い逃れを排除する観点からは、特に各種メンテナンス業者等のように、何らかの契約に基づき執務スペースに立ち入ることができる者や、アポイントメントや渉外活動で立ち入る者に対しては、秘密情報が保管されている場所の入口、書棚、作業場等に「写真撮影禁止」、や「関係者以外立入り禁止」「無断持出し禁止」等の張り紙や看板を設置することが有効です。

※なお、「関係者以外立入り禁止」の看板を掲げる時には、同時に連絡先も記入しておかないと、「立入り禁止とは分かっていたけれど、担当者を探して入室してしまった」という言い逃れを許してしまいかねないため、「関係者以外立入り禁止」の看板には、管理者の連絡先も併記することが必要です。

ｂ．秘密情報であることの表示

○　外部者以外への対策と同様、実際に秘密情報に接した者が、その情報が秘密情報であることを認識できるようにするため、外部者が接する可能性のある紙媒体の資料・ファイル、ＵＳＢメモリ、ＣＤ－Ｒ等の記録媒体、電子データ等には、秘密情報であることを表示することが望ましいと考えられます。

※秘密情報の窃取を企図して不法侵入や不正アクセスなどを行う外部者に対しては、秘密情報であることを表示することによって、かえってそれと分かりやすくなってしまうという懸念もありますが、従業員等に向けた対策として重要な対策であることや、来訪者や見学者等の悪意のない外部者が秘密情報と分からず、うっかり持ち出してしまう懸念を考慮すれば、やはり表示しておいた方が望ましいと考えられます。その上で、不法侵入者等に対しては、「①接近の制御」、「②持出し困難化」、「③視認性の確保」などの取組みを着実に行うことが重要でしょう。

ｃ．契約等による秘密保持義務条項

○　各種メンテナンス業者等、一定の許可の下に、秘密情報に接する可能性のある事業者に対しては、「業務中に接する一切の情報を漏えいしてはならない」旨を業務委託契約等に盛り込むこと等が重要です。

⑤「信頼関係の維持・向上等」に資する対策

不法侵入や不正アクセスを企図する外部者に対しては、「信頼関係の維持・向上等」に資する有効な対策は考えにくいですが、一定の契約関係のある外部者に対しては、（３）取引先に向けた対策 ⑤「信頼関係の維持・向上等」の対策が有効な場合が考えられますので、そちらを参考に対策することが望まれます。

コラム④

近年、標的型攻撃メールの増加や巧妙化が問題となっていますが、実際、その手口はどのようなもので、どのような注意を払えばいいのでしょうか。

標的型攻撃メールってどんなもの？

標的型攻撃メールは、広くばらまかれる迷惑メールとは違い、情報窃取等を目的として、ごく少数または多数ながら特定された範囲のみに対して送られる、利用者の PC をマルウェアに感染させることを目的とした~~狙った相手の秘密情報などを盗むことを目的として、関係者などになりすまし、あたかも業務に関係しそうな偽のメールを、ウィルスを仕込んだ添付ファイルと一緒に送信してくる~~ものです。

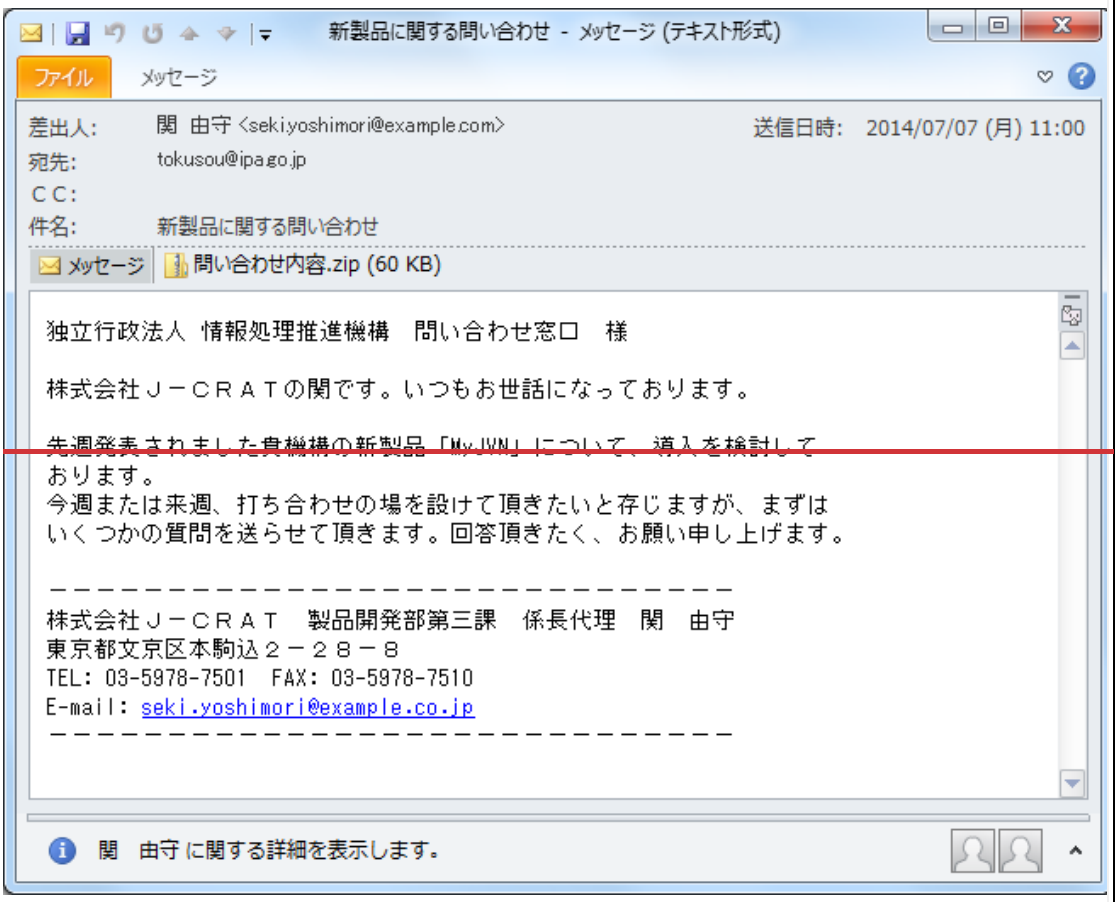
具体的には、以下のような特徴があります~~メールが報告されています~~。

- メールの受信者に関係がありそうな送信者を詐称する。
- 添付ファイルや本文中の URL リンクを開かせるため、件名・本文・添付ファイルに細工が施されている。
（業務に関係するメールを装ったり、興味を惹かせる内容や、添付ファイルの拡張子を偽装したりするなど）
- ウィルス対策ソフトで検知しにくいマルウェアが使われる。

一般には次のような件名、本文から構成される事例が多く見られます。

- 社内の連絡メールを装うもの（ファイルサーバのリンクを模すケースを含む）
- 関係省庁や、政府機関からの情報展開を模すもの（連絡先、体制、会見発表内容など）
- メディアリリース
- 合併や買収情報
- ビジネスレポート/在庫レポート/財務諸表
- 契約関連
- 技術革新情報
- 国際取引
- 攻撃者に関する情報
- 自然災害
- ウェブなど公開情報を引用したもの
- 政府/業界イベント
- 政府または産業における作業停止
- 国際的または政治的なイベント

（ＩＰＡ「標的型攻撃メールの見分け方」より引用）



~~一見、何ら問題のない普通のメールのように見えますが、上記メールが標的型攻撃メールであると気がつくためには、どこに注意すればいいのでしょうか。~~

~~IPAでは、以下のとおりその着眼点をまとめています。~~

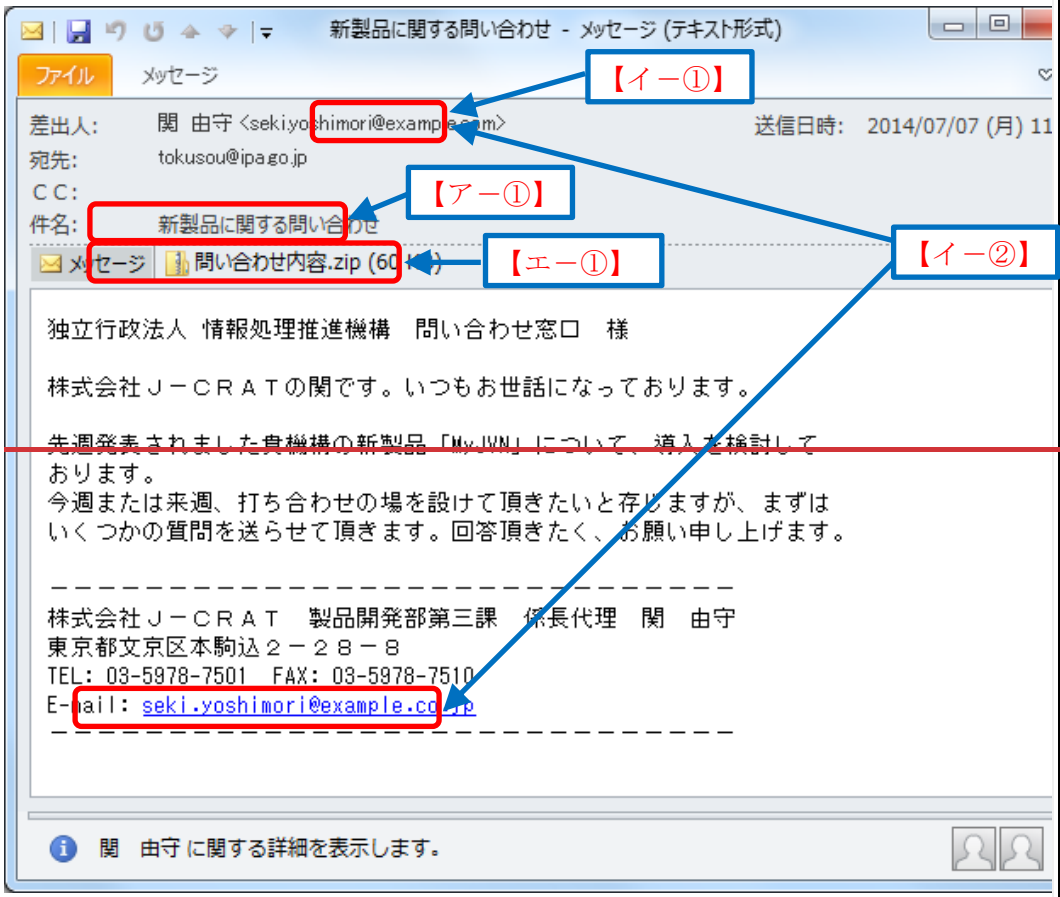
~~◆標的型攻撃メールの着眼点（特徴）~~

~~(ア) メールのテーマ~~	~~① 知らない人からのメールだが、メール本文のURLや添付ファイルを開かざるを得ない内容~~ ~~(例1) 新聞社や出版社からの取材申込や講演依頼~~ ~~(例2) 就職活動に関する問い合わせや履歴書送付~~ ~~(例3) 製品やサービスに関する問い合わせ、クレーム~~ ~~(例4) アンケート調査~~
	~~② 心当たりのないメールだが、興味をそそられる内容~~ ~~(例1) 議事録、演説原稿などの内部文書送付~~ ~~(例2) VIP 訪問に関する情報~~
	~~③ これまで届いたことがない公的機関からのお知らせ~~ ~~(例1) 情報セキュリティに関する注意喚起~~ ~~(例2) インフルエンザや新型コロナウイルス等の感染症流行情報~~ ~~(例3) 災害情報~~

	④ 組織全体への案内 （例 1）人事情報 （例 2）新年度の事業方針 （例 3）資料の再送、差替え
	⑤ 心当たりのない、決裁や配送通知（英文の場合が多い） （例 1）航空券の予約確認 （例 2）荷物の配達通知
	⑥ ID やパスワードなどの入力を要求するメール （例 1）メールボックスの容量オーバーの警告 （例 2）銀行からの登録情報確認
（イ） 差出人の メールアドレス	① フリーメールアドレスから送信されている
	② 差出人のメールアドレスとメール本文の署名に記載されたメールアドレスが異なる
（ウ） メールの本文	① 日本語の言い回しが不自然である
	② 日本語では使用されない漢字（繁体字、簡体字）が使われている
	③ 実在する名称を一部に含む URL が記載されている
	④ 表示されている URL（アンカーテキスト）と実際のリンク先の URL が異なる（HTML メールの場合）
	⑤ 署名の内容が誤っている （例 1）組織名や電話番号が実在しない （例 2）電話番号が FAX 番号として記載されている
（エ） 添付ファイル	① ファイルが添付されている
	② 実行形式ファイル（ exe / scr / cpl など）が添付されている
	③ ショートカットファイル（ lnk など）が添付されている
	④ アイコンが偽装されている （例 1）実行形式ファイルなのに文書ファイルやフォルダのアイコンとなっている
	⑤ ファイル拡張子が偽装されている （例 1）二重拡張子となっている （例 2）ファイル拡張子の前に大量の空白文字が挿入されている （例 3）ファイル名に RLO（「Right-to-Left Override」と呼ばれる文字の表示上の並びを左右逆にする制御文字。）が使用されている

（ＩＰＡテクニカルウォッチ『標的型メールの例と見分け方』より編集）

上記を踏まえ、注意深くメールを見てみると、以下の着眼点に気がつきます。



・製品に関する問い合わせ【アー①】を装った標的型攻撃メールの例。

・本文中に、実際の製品名やサービス名が記載されている場合が多い。

・フリーメールアドレス（図中では@example.com）を利用している点【イ－①】だけでは不審と判断できないが、差出人のメールアドレスと署名のメールアドレスが異なる点【イ－②】が不審である。

・また、zip 圧縮ファイルが添付されている【エ－①】ため、慎重に対応する必要がある。

被害に遭わないためには、このようにポイントに注意し、標的型攻撃メールを“嗅ぎ分けることか”が非常に重要になります。最近では標的型攻撃からランサムウェアに感染して企業組織が身代金を要求されたり、秘密情報を曝露すると脅迫される事例も増加しています。IPAから公開されている各種資料を利用するなどして、従業員のみならず、取引先等も含めた教育・研修を実施することが望まれます。

（参考）IPAで公開している各種学習素材

＜IPAテクニカルウォッチ『標的型メールの例と見分け方』＞

https://www.ipa.go.jp/files/000043331.pdf

＜J-CRAT 標的型サイバー攻撃特別相談窓口「標的型メールの見分け方」＞

https://www.ipa.go.jp/security/todokede/tokubetsu.html

＜ビジネスメール詐欺（BEC）対策特設ページ＞

https://www.ipa.go.jp/security/bec/about.html

＜映像で知る情報セキュリティ＞

https://www.ipa.go.jp/security/keihatsu/videos/

~~＜高度標的型攻撃」対策に向けたシステム設計ガイド＞~~

~~https://www.ipa.go.jp/files/000046236.pdf~~

コラム⑤

最低限のサイバーセキュリティって？

多くの企業にとっては、いきなり本格的な対策を開始するのは大変なことだと思います。IPAでは、企業の規模に関わらず、最低限実行すべき重要な対策を5か条にまとめています。

インターネットの普及に伴い様々な脅威が現れ、攻撃者の手口は年々巧妙かつ悪質になっていますが、対策には共通する部分があります。本5か条は、共通する基本的な対策をまとめたものですので、必ず実行しましょう。

~~標的型攻撃メールや不正アクセスなどが怖いと聞くけれど、何から対策を始めていいのか分からない…という方もいらっしゃるでしょう。本書における他の対策と同様、行うべき対策やその程度については、各企業組織での事業活動でのインターネットの利用状況や、使用している電子機器、守るべき情報等によって異なります。したがって、各企業組織において、本書や、IPAが公開している各冊子などを参考に各々に応じた対策を適時実施することが必要です。~~

~~ここでは、「事業活動において、請求書や納品書のやり取りなどにメールを利用しているけれど、セキュリティ対策まではまだ手が付けられていない」というような事業者の方が、"まず"何から始めればよいか、という観点で、以下3点（いざという時に備えてプラス1）を最低限のサイバーセキュリティ対策としてご紹介いたします。~~

①OS やソフトウェアは常に最新の状態にしよう！~~ソフトウェアは、常に最新版にアップデートしましょう。~~

OS やソフトウェアを古いまま放置していると、セキュリティ上の問題点が解決されず、それを悪用したウィルスに感染してしまう危険性があります。お使いの OS やソフトウェアには、修正プログラムを適用する、もしくは最新版を利用するようにしましょう。~~標的型攻撃メールに仕込まれたウィルスは、ＰＣの脆弱性を狙ってくる傾向にあります。したがって、ＰＣ利用時の脆弱性を解消することが重要です。そのためには、Windows や Mac に代表されるＯＳ（基本ソフトウェア）や、Adobe Reader、Word、Excel、一太郎などといったアプリケーションソフトウェアについては、常に最新の状態で利用しましょう。~~

②ウィルス対策ソフトを導入しよう！~~ウィルス対策ソフトを導入しましょう。~~

~~重要なセキュリティ情報をいち早く入手する方法については、ＩＰＡのサイバーセキュリティ注意喚起サービス「icat for JSON」等を利用することも一案です。~~

~~https://www.ipa.go.jp/security/vuln/icat.html~~

ID・パスワードを盗んだり、遠隔操作を行ったり、ファイルを勝手に暗号化するウイルスウィルス

が増えています。ウィルス対策ソフトを導入し、ウィルス定義ファイル（パターンファイル）は常に最新の状態になるようにしましょう。怪しいWebサイトや、不審なメールを介したウィルスを検知して、ウィルス感染を未然に防ぐため、ＰＣにはウィルス対策ソフトを導入しましょう。お使いのＰＣの環境に適していないウィルス対策ソフトや、ウィルス対策ソフトを騙るウィルス等もありますので、ウィルス対策ソフトの選定にあたって不安がある場合は、ＰＣの購入元等にも相談されるといいでしょう（※）。

なお、ウィルス対策ソフトについても、常にアップデートして、最新のウィルスを検知できるようにしておくことが重要です。

（※）ウィルス対策ソフト製品は購入後一定期間（1年間等）のみアップデートできるようになっていることが多く、有効期限が切れていないか確認することも重要です。

③パスワードを強化しよう！ファイアーウォールを設定しましょう。

パスワードが推測や解析されたり、ウェブサービスから流出したID・パスワードが悪用されたりすることで、不正にログインされる被害が増えています。パスワードは「長く」「複雑に」「使い回さない」ようにして強化しましょう。不正アクセスを遮断するため、ファイアーウォールを設定しましょう。ファイアーウォールには、ソフトウェアとしてＰＣやサーバーに導入するものや、専用の通信機器としてネットワークに設置するものなどがあります。前者では、WindowsなどのＯＳに内蔵されているファイアーウォール機能もありますので、新しいソフトウェアの導入や機器の設置が難しい場合には、まずはこの機能をOSの設定から有効にすることで対応しましょう。

④共有設定を見直そう！

データ保管などのウェブサービスやネットワーク接続した複合機の設定を間違ったために、無関係な人に情報を覗き見られるトラブルが増えています。無関係な人が、ウェブサービスや機器を使うことができるようお設定になっていないことを確認しましょう。

⑤脅威や攻撃の手口を知ろう！

取引先や関係者と偽ってウィルス付きのメールを送ってきたり、正規のウェブサイトに似せた偽サイトを立ち上げたりしてID・パスワードを盗もうとする巧妙な手口が増えています。脅威や攻撃の手口を知って対策をとりましょう。

ファイアーウォールを専用の通信機器として導入する意義については、標的型攻撃対策を説明するIPAの「『標的型メール攻撃』対策に向けたシステム設計ガイド」の1-9頁以降にその一例が紹介されています。
https://www.ipa.go.jp/files/000033897.pdf

少なくとも上記３つの取組を確実に実施して、被害を未然に防ぐことが重要ですが、

実際に標的型攻撃メール等の被害にあった場合には、いかに迅速に適切に対処して被害を最小限にするかが重要です。

そこで、以下では、上記３つの取組にプラス１として、実際に被害に遭った場合に備えて実施しておいた方がよい取組をご紹介します。

いざという時に備えて

流出等の事態が発生した時、原因究明・調査のため、システムのログ（履歴・記録）が重要になりますが、予め準備しておかないと、いざという時の役に立たないこともあります。以下の点に注意して設定を確認しておきましょう。

・サーバや機器のシステム時刻を合わせる

→時刻が合っていないと、いざというときにいつ何があったか分かりません！

・ログが記録・保存できる期間に注意する

→どのくらいの期間や容量を記録・保存できるのか確認し、適切にチェックされるような体制を！

近年急速に増加している標的型攻撃メールや不正アクセスを念頭に、まず実施すべきと考えられる対策を３つ（プラス１）に絞ってご紹介しましたが、これで足りるというものではありません。以下の参考資料などにより、自社のインターネットの利用状況等を踏まえて、最適な対策を実施して下さい。

（参考）

中小企業の情報セキュリティ対策ガイドライン
https://www.ipa.go.jp/security/guide/sme/about.html
中小企業向け情報セキュリティ対策
https://www.ipa.go.jp/security/sme/list.html
IPA　対策のしおり　シリーズ
https://www.ipa.go.jp/security/antivirus/shiori.html
IPA　ここからセキュリティ
http://www.ipa.go.jp/security/kokokara/
NISC　国民を守る情報セキュリティサイト
http://www.nisc.go.jp/security-site/trouble/material.html
NISC　政府機関における情報システムのログ取得・管理の在り方の検討に係る調査報告書
http://www.nisc.go.jp/inquiry/pdf/log_shutoku.pdf

JPCERT/CC　高度サイバー攻撃への対処におけるログの活用と分析方法

https://www.jpcert.or.jp/research/apt-loganalysis.html

第４章　秘密情報の管理に係る社内体制のあり方

- 秘密情報漏えいの対策の実施（第２章、第３章）や、他社の秘密情報に係る紛争への備え（第５章）、秘密情報の漏えい事案への対応（第６章）といった、本書で紹介する取組み全般を、真に実効的なものとするためには、それらの対策が一時的なものとならないようにする必要があります。
- そのためには、秘密情報の管理の実施状況を定期的にチェックするとともに、状況の変化に応じた見直しを行うことができる社内体制を整えることが重要です。
- 秘密情報の漏えい対策に取り組む企業は、規模も業種も様々であることから、本章では、そのような社内体制の整備における基本的な考え方を示しつつ、考えられる社内体制の参考例を提示しています。

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）

○ 秘密情報の管理は一旦対策を講ずれば完結するというものではなく、それが継続して実施され、状況の変化に応じて適切に見直しが行われるようにしていかなければなりません。

○ 秘密情報の管理に割くことができる費用や人員が限られている中で、網羅的な対策を実施することが困難である場合は、必ずしもその全てを実施しなければならないというものでもありません。守るべき情報の種類や企業規模等を踏まえて、適切と考えられる対策を選択して実施していくことが重要です。

○ いかなる対策を選択するかは、どの秘密情報が自社の経営戦略上重要性が高いのか、どの程度の費用・人員を割いて対策を実施するかといった経営判断によるべき問題であり、個々の部門で独自に判断することが望ましくない場合が多いと考えられます。

○ 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ＡＩを含む新たなツールの特性を理解した上での対応（利用の当否、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。

○ 加えて、秘密情報の漏えいが、その情報の経済的な価値を失わせるのみならず、企業の社会的信用の低下や他社からの訴訟リスクなど、様々な損失を生じさせるおそれがあることを踏まえると、秘密情報・重要情報について法令の定める管理義務を果たすことに加えて、企業価値の維持・向上を図ることの両面でンプライアンスの観点からも、経営層が、率先して社内体制の構築に関与していくという意識を持つ必要があるでしょう。したがって、経営層が、自社内外に向けて、秘密情報の管理に取り組む姿勢（ポリシー）を明確に示し、自社内の個々人すべてが、秘密情報の管理の当事者であるという意識を持って、継続的に対策を講ずることができる体制を整えることが重要となります。

○ どのような社内体制が望ましいのかは、事業の規模や性質によって異なりますが、経営層の積極的な関与の下、以下の例を参考に、体制が単に形式的なものにならないように留意しながら、秘密情報の管理が継続的に実施され、状況の変化に応じた適切な見直しを行うことができる責任者と責任部署を中心にした一元的な体制とすることがポイントです。

（小規模な企業における社内体制の具体例）

○ 小規模な企業であれば、以下のように特別の組織や会議体を設置するという形での体制整備よりも、例えば、

- 定例の社内会議等において、経営層も含めた全社員により、秘密情報の管理の実施状況の報告・確認や見直しを行う
- 社内において情報漏えい防止のために「これだけはやってはいけない」というような最低限の禁止事項を定め、周知徹底するとともにその実施状況を確認する

というような柔軟な体制のほうが、より実効的かつ効率的となる場合もあり得ます[54]。

~~54 特定個人情報の取扱いに関しては、『お役立ちツール（※中小企業向け）』（個人情報保護委員会）において、中小規模事業者における対応方法等が記載されています。（https://www.ppc.go.jp/personalinfo/legal/）~~

小規模な企業における社内体制

◆　**金型製造業･小規模企業の事例**
～従業員全員で話し合い、当事者意識も向上～

従業員が十数名であることから、定期的に、社長も含めた全従業員で、秘密情報の管理に関する研究会を行っている。その研究会において、社内ルールの内容や運用の改善などについて議論し、現場の実情に即応した取組の見直しや取組の徹底を可能とするとともに、個々の従業員の当事者意識の向上にもつながっている。

◆　**工場設備製造業･小規模企業の事例**
～社長が責任者として見回り、情報管理を徹底～

従業員が20名程度と小規模であることから、あまり詳細なルールは策定していないが、社長が情報管理の責任者として、本社･工場を含めた3拠点に頻繁に足を運び状況確認を行うことで、情報管理の徹底を図っている。

（事業規模が大きな企業における社内体制の具体例）

○　**事業の規模が大きくなると、より組織的な体制を整えておく必要が生ずることから、例えば、担当取締役を決定の上、当該取締役を長として、秘密情報の管理の実施について様々な部門や担当者の参画・協力を一元的に統括し、リーダーシップを取る部門横断的な組織とその責任者を設置することが考えられます（以下、部門横断的な組織について、便宜上「秘密情報管理委員会」という。）。秘密情報の管理に係る判断は、重要な経営判断と密接に関連する場合もあるほか、仮に情報漏えいが起こった場合には会社としての迅速な判断が求められることから、そのような判断が円滑に、かつ適切に行われるようにするため、日頃からの取締役の関与が必要となるからです。**

※必ずしも「秘密情報管理委員会」を新たに設置する必要はなく、情報資産の管理を統括する「情報セキュリティ委員会」や、様々な経営リスクを管理することを目的とした「リスク管理委員会」、法令等の遵守一般を担当する「コンプライアンス委員会」といった社内に既に存在している別の組織に、同様の機能を担わせることも考えられます。

○　**また、「秘密情報管理委員会」は、経営企画、総務、法務、情報システム、営業、**

技術、製造、人事・労務、経理、知的財産、貿易・輸出管理など、情報漏えい対策に関連し得る社内の部門を広く巻き込む形で、各部門の責任者をもって構成することが望まれます（特に、「情報漏えい対策」とは関連性が薄いとの誤解がなされやすい人事・労務部門が抜け落ちないように留意）。加えて、「秘密情報管理委員会」の下に事務局を設置し、様々な社内規程案の作成や、部門間調整、「秘密情報管理委員会」の運営などの業務を担わせます。

○　なお、秘密情報管理委員会の運営にあたる事務局には、自社の経営戦略、ガバナンス、複数部門にわたるマネジメントなど多岐にわたる機能が求められます。よって、担当の取締役が、トップマネジメントとして、事務局に配属させるのに適切な人材を任命することも考えられます（必要に応じて、専門知識を有する者を参画させることも考えられます）。

（部門横断的な組織と各部門の役割分担）

○　一方で、事業規模が大きくなるにつれて、全社的に情報を集約して統一的に対策を検討し、その徹底を図ることや、適切な対策の見直しが困難になってくる場合もあります。そのような場合には、例えば、

・　全社的には基本的な方針のみを決定し、それ以外の秘密情報の管理の一部について、相当の規模の部門単位（例えば、２０～３０人程度の規模）に権限を降ろすという対応

・　相当の規模の部門単位ごとに、所属する部門単位（特に、営業、技術、製造部門）における秘密情報の管理の推進を担う責任者を任命し、その責任者を通じて、秘密情報の指定や分類の決定、対策の実施などの秘密情報の管理を徹底させるという対応[55]

など、事業規模等の各社の状況に応じて、部門横断的な組織と、各部門において、適切な役割分担を行うことがあり得ます。ただし、その場合でも、どの程度まで各部門に権限や責任を降ろすか等については、全社的な秘密情報の管理にばらつきが生じることのないように慎重に検討すべきでしょう。

【「秘密情報管理委員会」が担う役割（全社統一的に実施すべき対策）】

➢　社内規程の整備・見直し

秘密情報の管理方法等に関して社内においてルール化しておくべきことを社内規程とします。（参考資料２「第２　情報管理規程の例」を参照）

[55]　この対応の一環として、例えば、部門横断的に一定期間発足するプロジェクトの推進に当たって、そのプロジェクト独自で、秘密情報の管理の責任者の任命・対策の実施を行うことも考えられます。

例えば、

- 第２章で紹介した「保有情報の評価及び秘密情報の決定」及び第３章で紹介した「秘密情報の分類、情報漏えい対策の選択」を実施し、その内容をルール化
- 第３章で紹介した対策のうち、「アクセス権の範囲の適切な設定」や「秘密情報の表示」、「社外持ち出しルールや廃棄方法等のルール化」など、特に社内ルール化しておくべき対策のルール化

などを実施します。

- なお、ルール化にあたっては、必ずしも秘密情報の管理に係る独立したルールでなくとも良く、その他の保有情報を含めた情報管理全体のルールや、諸々のリスク対応に係るルールと統合された形も考えられます。

➢ 各部門の役割分担の決定

第３章において選択した「情報漏えい対策」や第６章において紹介する事後対応に係る対応等について、自社内のどの部門に、どのような対策を担わせるかを決定します。対策の中には、サイバーセキュリティのための情報システムの構築のように、専門的な部門にその実施を一定程度集中させたほうが良い場合や、社外持出しの許可のように、個別の部門ごとに実施させても良い場合もあり得るでしょう。

役割分担の一例については、「本章４－２　各部門の役割分担の例」を参照。

➢ 情報収集体制の確立

日頃から、秘密情報の管理に係る情報が社内において適切に共有されるような体制を整えます。例えば、人事部門が退職予定者を把握した場合に、情報セキュリティ部門が、当該退職予定者のアクセスログのチェックを強化するなどの対応が可能となるような体制を検討します。

具体的には、各部門の担当者の情報共有の場を定期的に設けたり、情報共有のタイミングやその内容、情報共有ルート等について社内ルール化しておいたりすることが考えられるでしょう。

➢ 情報漏えい事案対応に係るルール（マニュアル等）の策定

実際に情報漏えいが疑われる場合の対応について、誰が情報漏えいの兆候をチェックするのか、情報漏えいを検知した場合、どのような基準で、どのようなルートで、誰まで報告を行うのか、情報漏えいに対する初動対応や責

任追及をどのように実施するのか等を、マニュアル等において事前に明文化します。また、実際に情報漏えいが生じた場合を想定して、そのマニュアル等に沿う形で、部門間での情報共有、対策チームの招集、初動対応の手順、報道対応などを確認するための全社的な訓練（机上訓練・実地訓練）を行うことも重要です。このような訓練対応を通じて、そのマニュアル等自体の改善点が把握できることもあります。

その具体的に内容については、第６章を参照。

- 秘密情報の管理のチェック・見直し

秘密情報の管理に係る情報共有や内部監査、事後対応等を通じて自社の秘密情報の管理の実施状況を定期・不定期にチェックします。その結果、秘密情報の分類が不適切となっていたり、廃棄・消去すべき情報が残存しているなど実施する対策が不十分となっていたりする場合には、必要に応じて、対策の実施を再徹底したり、その実施内容や、実施に当たっての社内体制・社内規程等について見直しを行います。

※内部監査等の実施に当たっては、毎回同一の観点からの監査を繰り返すだけでは効果が乏しくなるおそれもあるため、情報漏えいの手口の高度化・多様化の状況などを踏まえつつ、必要に応じて、内部監査等におけるチェックポイントなどを見直すことも重要。

- 周知徹底、教育、意識啓発

自社の秘密情報の定義や、秘密情報をどのように取り扱うべきかといったような秘密情報の管理に係る社内ルールについて、部門間で異なる理解や運用がなされないよう統一的な研修等を実施します。その際、必ずしも全従業員を対象とした周知、教育ばかりでなく、職務ごとの情報漏えいリスク・責務に応じた周知、教育を行うことも考えられます。なお、秘密情報の管理に係る社内表彰の実施や、情報漏えい者に対する懲戒処分の内容の周知（必要に応じて懲戒処分の内容に関する担当部門への事前の意見を行うこともあり得ます）なども、従業員等への意識啓発のために有効である場合があります。

部門横断的な組織と各部門の役割分担の事例

◆ **製造業・大規模の事例**

～全社的なモデルとその例外とのバランスがとれた仕組み～

部門・拠点が多いことから、中心的な部門において、秘密情報の管理についての原則的な方針を定めて、各拠点・各部門に示し、実際の運用の多くは各拠点・各部門の責任者を任命して行わせている。例えば、中心的な部門において、「極秘情報」、「秘情報」といった秘密情報の分類の方法や、「どのような情報を、どの分類として指定すべきか」といった考え方や事例についてのモデルを作成する。各拠点・各部門においては、そのモデルを基に、責任者が運用を行っているが、そのモデルとは異なったルールで情報管理を行いたいと考える場合には、各拠点・各部門から、その理由も合わせて中心的な部門へと伝え、それを許可するという仕組みとすることにより、全社的な統一と、各拠点・各部門の実情に沿った柔軟性のバランスを図っている。

（子会社・委託先等を含めた秘密情報の管理体制の構築）

○ 一定程度の事業規模を有する企業の場合、国内外を問わず、子会社や各地の支社を有しており、自社の秘密情報が共有する場合がありますが、当該子会社や支社においても、自社の秘密情報の管理に係るルールや対策が徹底されるようにすることが重要です。

※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続が明確化され、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保存~~蔵置~~されている営業秘密についても、海外での侵害行為（海外に所在する物理サーバや仮想サーバからの取得行為等）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保存~~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。

○ また、委託先やサプライチェーンに関わる複数の企業など、他社に自社の秘密情報を共有する必要性がある場合、当該他社との関係で、秘密情報の対象やアクセス権者等の範囲を明確化し、共有化することや、当該他社における情報漏えい対策及びその実施体制の構築等を確保することが重要となります。

○ 具体的には、そのような観点から、当該他社との契約内容等を検討する必要があります。また、自社において統一的な対応がなされるよう、委託先等における秘密情報の管理体制の構築に係る当該他社との契約のあり方について、自社内でルール化しておくことも重要です。

パートナー企業やグループ企業を含めた管理体制の事例

◆ **電気機械器具製造業・大規模の事例**

～自社作成のチェックシートを共有し、取引先の情報管理水準を向上～

委託先企業や再委託先にも一定の情報管理水準が保たれるよう、委託契約の内容として、実施すべき情報管理策を具体的に盛り込んでいる。その一環として、自社が作成した情報セキュリティに係る基準やチェックシートを共有し、それらに基づく対策を講ずるよう求めている。同時に、委託先・再委託先も含めた情報セキュリティ研修を実施して徹底を図っている。

◆ **海外・電気機械器具製造業・大規模の事例**

～グループ全体で秘密情報保護ポリシーを共有～

外国拠点も含めたグループ全体で、統一化された秘密情報保護ポリシーを策定している。その際、各地域の法制度・ガイドライン・慣習などを検証し、最も情報漏えいリスクが高い地域を特定した上で、その地域を念頭に置いたポリシーを策定している。

４－２　各部門の役割分担の例

各部門がいかなる対策に責任を持つこととするかを分担することが、効率的かつ実効的であると考えられます。当然、このような役割分担でなければならないわけではありませんが、以下では、その役割分担の際の参考となるよう分担の一例を示します。

■　部門横断的な組織の事務局担当

（「保有する情報の把握・評価、秘密情報の決定」に関する役割）

- 「保有する情報の把握・評価、秘密情報の決定」の作業方針の決定などの全体取りまとめ

（情報漏えい対策に関する役割）

- 情報管理規程などの社内規程等の原案・見直し案の作成
- 秘密情報の管理に関する研修内容や実施方法の検討
- 部門横断的な組織（秘密情報管理委員会など）の事務運営
- 秘密情報の管理の実施状況の確認

（情報漏えい事案への対応に関する役割）

- 情報漏えい事案対応の際の全体調整（対策チーム等の招集・運営等）
- 「情報漏えい事案対応に係るルール・マニュアルの原案・見直し案の作成

■　法務担当

（情報漏えい対策に関する役割）

- 情報漏えいに関する訴訟対応の観点からの就業規則・情報管理規程等の確認
- 秘密保持契約・誓約書、委託契約等の各種契約の確認・ひな形の作成

  ※加えて、特に秘密保持義務契約書の管理（どのような情報について、いつまで、誰が、秘密保持義務を負っているのかといった情報の管理）も重要。

  ※新たに進みつつあるデータ利活用型ビジネスを進める上では、情報の保護、円滑な利活用・提供を可能にする自社の戦略に沿った契約、規約等の検討・策定が重要になるため、法務部門・担当の役割が重要。

（「他社の秘密情報に係る紛争への備え」に関する役割）

- 転職者の受入れ、共同研究開発の場合等における法的リスク低減に関する相談
- 秘密保持契約・誓約書、共同研究開発契約等の各種契約の確認・ひな形の作成

※新たに進みつつあるデータ利活用型ビジネスを進める上では、情報の保護、円滑な利活用・提供を可能にする自社の戦略に沿った契約、規約等の検討・策定が重要になるため、法務部門・担当の役割が重要。（再掲）

- 他社からの警告書を受けた場合の対応の検討

（情報漏えい事案への対応に関する役割）

- 民事訴訟を提起する場合の訴訟対応の全体とりまとめ
- 刑事告訴をする場合の警察当局との窓口対応

■　人事・労務担当

（情報漏えい対策に関する役割）

- 法務担当との連携の下、就職時・退職時・異動時における適切な誓約書等の取得
- 部門横断的組織の事務局や法務担当との連携の下、情報漏えい防止の観点からの就業規則の見直し
- 教育・研修等の運営

  ※その内容や方法についても、部門横断的な組織の事務局のサポートを得ながら人事・労務担当が検討することとしてもよい
- 秘密情報漏えいに対する社内処分の実施・その内容の周知
- 働きやすい職場環境の整備に係る検討・実施や透明性が高く公平な人事評価制度の構築等
- テレワークや雇用の流動化など社会環境や事業環境が変化する中での従業員のメンタルヘルスケアの支援等
- 秘密情報の管理に係る意識共有、企業への帰属意識や働きがいを高める取組みの実施、防犯カメラの設置やログ取得、諸々の社内規程の整備に当たっての、労働組合との協議や取り決めの対応
- 退職者等の動向の把握

（「他社の秘密情報に係る紛争への備え」に関する役割）

- 法務担当との連携の下、適切な転職者の受入れの実施

（情報漏えい事案への対応に関する役割）

- 秘密情報漏えい者に対する懲戒等の実施

■情報システム担当（セキュリティ担当、ＩＴ担当）

（情報漏えい対策に関する役割）

- 社内規程等に沿ったＰＣ等へのアクセス権限の設定・変更等の実施
- 社内規程等に沿った情報システムの構築

  ※電子データの暗号化に係る設定、電子データ等の印刷・複製禁止に係る設定、私物ＵＳＢ等の使用禁止の設定、不許諾ソフトウェアのインストール禁止に係る設定、外部メールのチェックに係る設定、文書作成時の「マル秘」表示の自動的付加に係る設定、印刷者の氏名等の「透かし」の自動的付加に係る設定など
- 必要なログの取得・保管
- 不正アクセス等に対する防護システムの導入・運用、ＡＩを活用した最新の対策技術・不正検知技術等の導入の検討・運用

（「他社の秘密情報に係る紛争への備え」に関する役割）

- 他社情報を自社情報のサーバ═等と別に保管する場合のサーバ═の分離・仮想化（一台のサーバ═を複数に分割して利用すること）に係る設定

（情報漏えい事案への対応に関する役割）

- 情報漏えいの兆候の把握や、その疑いの検知のためのログ確認等の実施
- 被害の拡大防止の観点からのネットワーク遮断の実施
- 証拠保全の観点から、ログ等の保全

■　経営企画・分析担当

（「保有する情報の把握・評価、秘密情報の決定」に関する役割）

- 経営戦略の観点からの情報の評価、秘密情報の決定時における助言

（情報漏えい対策に関する役割）

- 従業員等への周知を見据えた秘密情報の管理の企業の業務効率化等に対する貢献度の分析

（「他社の秘密情報に係る紛争への備え」に関する役割）

- 他社から受領する秘密情報を厳選する際の、経営戦略的観点からの助言

■　総務担当

（情報漏えい対策に関する役割）

- 部門横断的組織の事務局や法務担当との連携の下、情報漏えい防止の観点からの情報管理規程の見直し
- 来訪者受付・来訪者証の発行などの対応
- 工場見学等のマニュアルの作成・そのマニュアルに基づく対応
- 防犯カメラの設置
- コピー機やプリンター等における利用者記録・枚数管理機能の導入
- 施錠された部屋・保管庫等の鍵の管理
- 清掃業者、メンテナンス業者等との契約・各業者への対応

■　広報担当

（情報漏えい事案への対応に関する役割）

- 情報漏えいの事実の公表などに係るマスコミ対応の窓口

■　監査担当（内部統制担当）

（情報漏えい対策に関する役割）

- 秘密情報の管理の観点からの定期・不定期での内部監査の実施。その結果の部門横断的組織の事務局へのフィードバック（監査結果に基づく改善指導、社内規程の改定に係る提言等）
- 情報漏えいに関する内部通報窓口の設置・運用

■　知的財産担当

（「保有する情報の把握・評価、秘密情報の決定」に関する役割）

- オープン＆クローズ戦略等の知的財産戦略の観点からの情報の評価、秘密情報の決定時における助言

※新たに進みつつあるデータ利活用型ビジネスを進める上では、情報の保護、円滑な利活用・提供を可能にする自社の戦略に沿った契約、規約等の検討・策定が重要になるため、多岐にわたり、改正も多い知的財産法に精通した知的財産担当の役割が重要。

コラム⑥

技術情報管理認証制度（TICS）について

サイバー攻撃や情報漏えいのニュースが多い昨今、企業が持つ強みである技術やノウハウなどを外部に漏らさないために、情報セキュリティ対策を講じること~~内部での流出防止対策~~が重要です。経済産業省では、事業者が保有する重要な技術情報等の適切な情報セキュリティ~~内部管理~~体制に対し、国が認定した機関（以下、「認証機関」という。）から認証を受けることができる、産業競争力強化法に基づく技術情報管理認証制度（以下、「認証制度」という。）を平成３０年９月に創設し、運用しています。

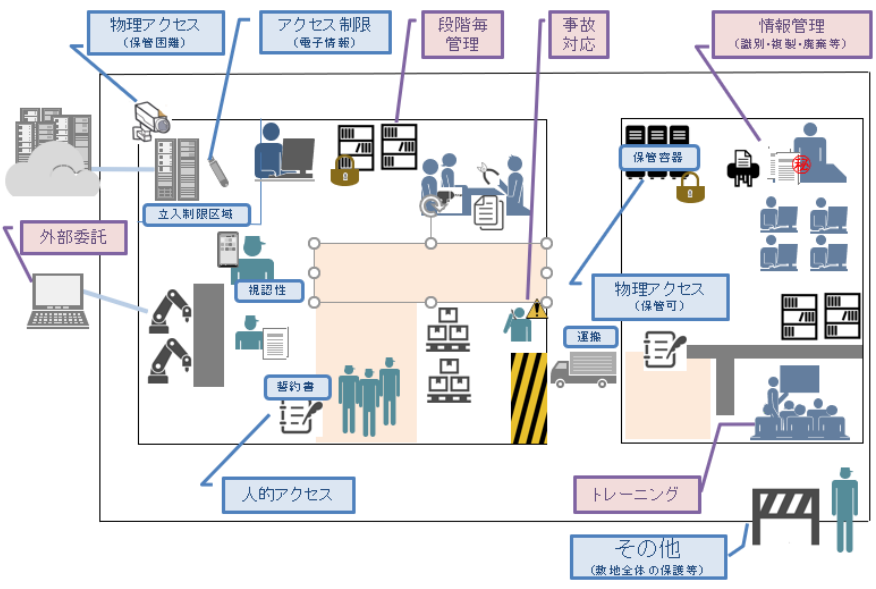
認証制度とは、どういう制度でしょうか？

認証制度では、事業者が自ら保有又は他者から預けられた情報~~技術等~~のうち守るべき重要な情報を特定し、当該情報の態様・価値等に応じて取り組むべき情報セキュリティ対策~~流出・漏えい防止策~~を決定し、~~内部管理~~情報セキュリティ体制を整備~~した後で、認証機関に認証を取得するための申請書を提出~~します。このとき、この制度の特徴として事業者は、認証機関の専門家から体制整備のための指導・助言を受けることができます。最終的に~~その後~~、認証機関が事業者の整備した情報セキュリティ~~内部管理~~体制の審査を行い、国が定めた~~認証制度の~~基準を満たせば認証を付与します。

漏えい防止策は何があるでしょうか？

事業者が取り組むべき情報セキュリティ対策~~漏えい防止策~~として、認証制度では基準を２００項目以上定めており、その中から必要な項目を選択して取り組むこととなります。例としては、①守る情報の決定、②守る情報の識別・対策整理を行った上で、③管理者選任、④情報管理プロセスの設定、⑤従業員への対策周知や教育、⑥情報漏えい等の事故発生時の報告ルールの設定、⑦守る~~管理対象~~情報へのアクセス権の設定、⑧金庫等による物理的情報の管理、⑨ID 等設定による電子情報の管理、があります。

（イメージ図）

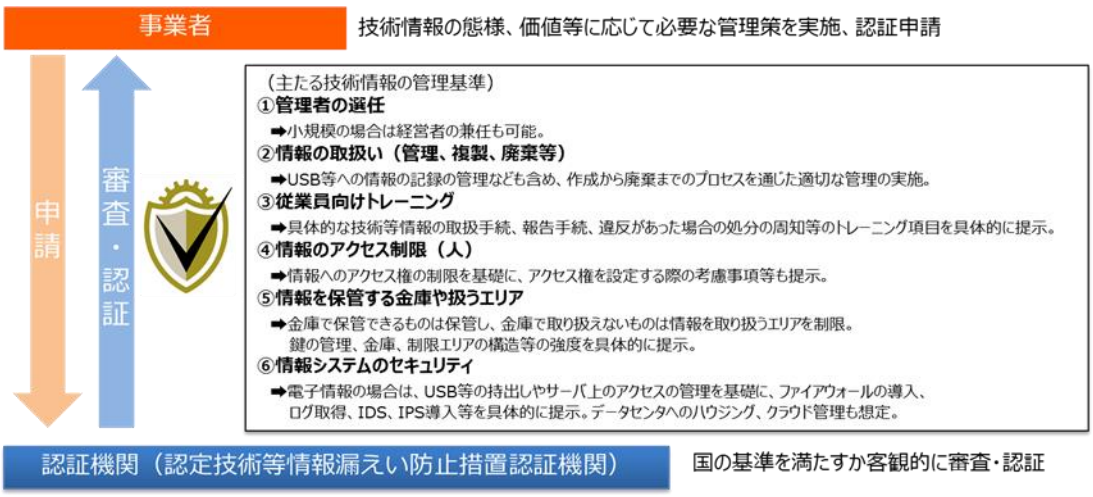


認証取得のメリットは何でしょうか？

認証を取得することで、事業者は~~重要な技術情報等の内部管理~~情報セキュリティ体制を適切に整備していることを取引先に示すことができるため、認証の取得は取引先からの信頼の獲得を後押しし、その後の情報交換や事業遂行を円滑にするといったメリットがあるほか、社内の~~同事業者内で重要な技術情報を適切に管理する~~情報セキュリティへの意識~~の~~向上につなげることも可能と考えております。

経済産業省ホームページにおいては、情報セキュリティ対策を何から始めていいかわからない事業者の方や自社の状況を把握したい方のために、専門知識がなくても自社の情報セキュリティ対策の状況を自ら確認し、必要な対策を把握することが可能な認証~~制度の普及促進を含め、事業者が保有する重要な技術情報等の適切な管理を支援するために、パンフレットや研修素材、事業者自身が重要な技術情報等を守る管理体制を構築できているか否かを簡単にチェックするためのセルフ~~自己チェックリストと活用ガイド~~シート等~~を公表していますので、ご活用いただけますと幸いです。

■技術情報管理　自己チェックリスト（METI/経済産業省）
https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/page03.html#checklist



第５章　他社の秘密情報に係る紛争への備え

・　他社の秘密情報に係る紛争に巻き込まれてしまった場合に備えて、各企業においては、平時より適切な対策を講じておくことが重要です。
・　本章では、健全に事業活動を行っている企業が、図らずも紛争に巻き込まれてしまった場合に、正当にその立場を守ることができるようにするため、自社の保有する情報が真に独自のものであると立証できるようにしておくための日頃からの管理手法や、他社の秘密情報を意図せず侵害しないための予防策を紹介します（後者については、他社情報の意図しない侵害が起こりやすい場面ごとに紹介します）。特に、転職者の受入れや共同・受託研究開発における対策は、第１章で述べたとおり、人材の流動性の向上を通じた多様な人材確保やオープンイノベーションの更なる進展にも寄与するものと考えられます。
・　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。

５－１　自社情報の独自性の立証

○　秘密情報の侵害を行ったとして、他社から不正競争防止法違反や契約違反等を理由とした損害賠償請求訴訟や差止請求訴訟を提起された場合等に、問題となっている情報が自社の独自情報であることを客観的に立証し、正当に自社の立場を守ることができるようにするため、平時より対策をしておくことが重要です。

○　こういった訴訟が提起されるリスクは、健全に事業活動を行っている企業であっても存在することに留意が必要です。例えば、自社製品と同じ機能・性能を持った製品を製造・販売している競合他社から提訴される、ライバル企業から嫌がらせ目的で提訴される、といったケースがあり得るところです[56]。

[56] なお、転職者の受入れのケースにおいて、転職元企業の秘密情報を参照することなく、転職先企業において独自開発した情報が、結果的に転職元企業の秘密情報と合致した場合の当該独自情報や、業界内では公知となっている情報、転職者が転職元企業において身につけた技能やノウハウ等については、基本的に利用は制約されませんが、そういったことも含め、自社の正当な立場を立証できるようにしておくことがこの章の主眼です。

具体例

（基本的な考え方）

- 情報の作成・取得過程、更新履歴、可能であれば消去された日時・内容のログ等について、関係する資料（電子メール、検討文書、メモ、議事録等）を保管する。その際、ファイルの履歴管理機能や履歴管理機能を持った情報管理システムの活用等も有用。

  ※なお、事後的にフォレンジック技術を活用することによる情報復元の手段もあり得るが、その前提として、事前に、前述のように履歴等の記録が取られていることが不可欠。

（保存しておくべき記録の内容）

- 技術情報については、当該技術が生まれるまでの実験過程等を記載したラボノートを作成・保存。ラボノートについては、その信用力の向上の観点から、定期的に、プロジェクトに参加していない従業員による日付等の確認を行うことも考えられる。

- 営業情報、例えば、顧客名簿については、顧客になるに至った経緯の記録（どの広告を見てどのようなアクセスがあったのかの記録、会員加入申込書等の原本等）、取引情報については、その作成経緯の記録として、取引経緯を記録した書面（取引伝票等の原本等）、接客マニュアルは、それらの作成に至る会議の議事録などを保存する。

（記録の信用力の向上）

- また、これらの資料について、必要に応じて、公正証書化することによって、信用力を高めることが考えられる。同様に、電子文書（例えば、細かい技術仕様についての大量のデータ）については、認証タイムスタンプや電子公証を利用し、特定の日時にその秘密情報を保有していたことと、それ以降その秘密情報が改ざんされていないことを客観的に証明できるようにすることも考えられる。

５－２　他社の秘密情報の意図しない侵害の防止

○　他社の秘密情報を意図せず侵害することを防ぐためには、自社で保有している情報の作成過程や入手経路に不正がないかどうかを事前に確認した上で、自社にと

っての必要性の観点から、他社から受け取る秘密情報を厳選し、受領した他社の秘密情報は、自社情報と徹底的に分離して管理することがポイントとなります。

○　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。

○　また、この対策を真に実効性のあるものにしていくためには、現場の従業員による他社情報の意図しない侵害のリスクを正しく理解することが必要であり、例えば、社内研修等を通じて周知徹底を行うことも重要です。

○　さらに、内部監査等を通じて、自社における対策が、実際に正しく実施されているか定期的に確認を行うことも重要です。

○　なお、特に留意すべきなのは、他社から営業秘密の開示を受けた場合等に、それが不正な開示であることを知らなかったとしても、知らないことにつき「重大な過失」（取引上の注意義務の著しい違反）があると評価されるときには、不正競争防止法上、その営業秘密を使用したり、更に別の他社に開示したりする行為等が損害賠償請求や差止請求の対象となり得る点です（不正競争防止法第２条第１項第５号等）。

○　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、ここでいう「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きいて「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。

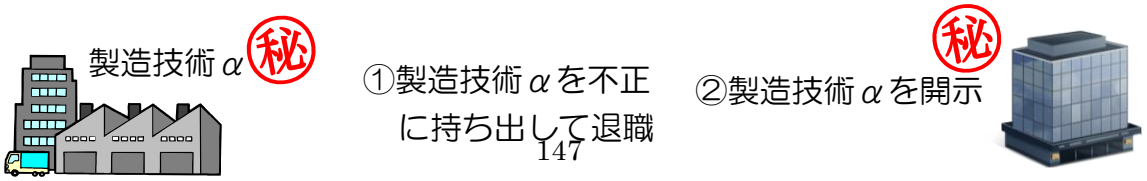
※「重大な過失」とは、我が国企業に求められるべき取引上の注意義務に照らし、営業秘密の取得時の客観的状況から、他社の営業秘密を侵害するおそれが大きいことが容易に予期できたにもかかわらず、その疑いを払拭するための合理的努力を怠ったこと、すなわち悪意と同視し得るほど、取引上の注意義務に著しく違反したことを意味します。

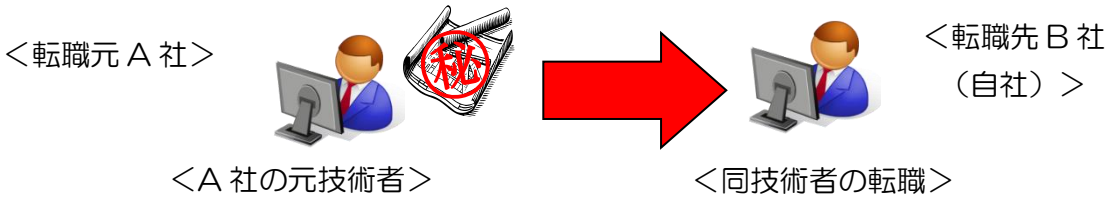
※以下の対応策は、そのような「重大な過失」がないとされるために有効と考えられる取組みですが、これらの取組みにより、常に「重大な過失」がないとされたり、これらの取組みをしていなかったからといって「重大な過失」があったとされたりするものではないことに留意が必要です。

（１）転職者の受入れ

○　他社の秘密情報の不正取得、不正使用等を前提とした採用・営業活動を行わないことは当然ですが、他社から転職者を受け入れる場合、その転職者が持ち込む情報の中に、転職元の秘密情報が存在する場合があるなど、意図せぬ形で他社の秘密情報を取得してしまうリスクが生じ得ます。なお、出向していた従業員が、自社に戻ってきた場合にも、以下と同様の対応策が必要となる場合があります。

図表５（１）転職者による情報持込みのイメージ





○　特に、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、知らなかったことに「重大な過失」がある場合には、不正競争防止法に基づく損害賠償請求や差止請求の対象となり得るため注意が必要です。

○　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。特に同業他社からの転職者、特別な技術・技能を有する転職者を受け入れた際には、他社の情報が自社内に不必要に混入することの防止を意識した対応が重要です。

○　なお、自社が受け入れようとしている転職者について、転職元企業の中核部署にいたことがあったかどうか、極めて高い評価を受けていたかどうかといった観点から、その転職者の立場を確認することも考えられるでしょう。転職元企業におけるキーパーソンと呼べるような人物である場合には、特に~~慎重に~~他社の情報が自社内に不必要に混入することの防止を意識して以下の対応策を講ずることが重要です。

○　以下では、①転職者の契約関係の確認、②転職者採用時における誓約書の取得等、③採用後の管理、の場面に分けて対応策を紹介します。必ずしもこのうち、いずれか１つの場面への対応で足りるということはなく、状況に応じ、必要な対策を採ることが重要となります。

①転職者の契約関係の確認

○　転職者の受入れに当たっては、まずはその転職者が、転職元との関係で負っている「特定の情報を外部に持ち出してはいけない」（秘密保持義務）、「競合他社に転職してはならない」（競業避止義務）といった義務の有無やその内容を確認するこ

とが必要です。これによって、不要なトラブルなく転職者の能力を活かした適切な配属ができ、転職してきた者が自社内において転職元の秘密情報を開示・使用していないかをより着実に確認することにつながります。

○　実際には、転職元企業からの警告書面を受領し、その中に契約内容の一部が記載されて初めて転職者の負っている義務内容の一部が明らかになるようなケースもあることから、まず転職者本人との間で、面接での記憶喚起等を通じた事実確認をしっかり行うことが重要です。

○　なお、仮に転職者の義務の内容を確定的に確認できなかったとしても、転職者が転職元企業との関係で秘密保持義務等を負っている可能性はゼロではなく、そのリスクは容易に無視し得ないものである以上、必要に応じて下記②、③の取組みを検討することが重要です。

具体例

- 転職元の就業規則や、退職時に交わしている契約書や誓約書などを確認し、特定の情報を外部に持ち出してはいけないといった義務（秘密保持義務）や、退職後に競業に就いてはいけないといった義務（競業避止義務）等の有無や内容を面接やアンケートなど合理的な方法を通じて確認する。
- 転職者が、そのような契約書や誓約書等の写しを転職元から交付されていなかったり、その内容が「すべての情報を持ちだしてはならない」といったものであるなど、転職者が負っている義務の範囲が漠然としている場合であっても、転職者本人に対する記憶喚起やインタビュー等を通じて、できるだけ義務の範囲を特定するよう努める。
- 転職者が義務を負っているかどうかに関わらず、②で後述するような「誓約書の取得」などの取組みも着実に実施することが望ましい。なお、転職元において中核的な役割を担っていた転職者を受け入れる際には、当該技術情報の性質や当該転職者の従前の職務内容等に応じ、当該転職者が転職元企業との間で秘密保持義務や競業避止義務を負っている可能性が高いことに留意した、より慎重な対応を行うことが考えられる。
- 以上の対応を行ったことを、採用時の議事録やレポート等の書面の形で記録・保存しておく。

②転職者採用時における誓約書の取得等

○　転職者に、転職元での秘密情報を自社内に持ち込ませないよう注意を喚起するとともに、不正競争防止法上の「重大な過失」が無いとの主張の一つの根拠とするために、転職者の採用時に書面での確約を取っておくことが有効です。

具体例

- 以下の内容（特に一点目が重要）を含む誓約書を転職者から取得する。

  ex）Ａ社が、Ｂ社からの転職者Ｃを採用する場合におけるＣからＡ社へ差し入れる誓約書の内容。

  - 「第三者の秘密情報を含んだ媒体（データ、資料）を一切持ち出していない」
  - 「Ａ社の業務に従事するに当たり、Ｂ社の情報を用いない」
  - 「第三者が保有するあらゆる秘密情報を持ち込まない」
  - 「Ａ社で就業するにあたり不都合が生ずる競業避止義務がない」
  - 「第三者の完成させた職務発明等をＡ社名義で出願しない」
  - 「Ｂ社の製造プロセスに関する情報を知っているが、Ａ社の設備の内容及び仕様等に照らして、当該情報を転用できるような状況にはない」

    ※最後の点については、従事させる業務の具体的内容に応じて、採用後に約させることも考えられる。

- これらの誓約書の内容を補強する材料の一つとして、転職者の採用の経緯や理由として、どのような能力や経験等に積極的に着目し、どのような環境でそれらを発揮することを期待しているか等を社内文書として残しておく。

③　採用後の管理

○　転職者から採用時に誓約書を取得しただけでは、必ずしも他社情報の侵害のリスクを完全に回避できるものではありません。採用後もそのようなリスクに配慮し、転職者の負う秘密保持義務等の内容を踏まえつつ、以下のような対応を行うことが考えられます。

○　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。

具体例

- 転職者が従事する業務内容を定期的に確認する（私物のＵＳＢメモリ等の記録媒体の業務利用や持込みを禁止するといった取組みも有効）。

（２）共同・受託研究開発

○ 他社（大学等の研究機関も含む）との共同研究開発や他社から委託を受けた研究開発（受託研究開発）に際しては、自社においても同種の独自研究開発を行っている場合も多いところ、他社が独自に進めていた研究開発成果等の秘密情報の開示を受けることもあることから、独自研究開発のみを行っている場合に比べて、他社の情報と自社の情報が紛れやすい状況にあります。この場合、当該研究開発の分野に関連する情報を不用意に使用・開示してしまった場合には、他社との間の契約違反となるおそれがあり、その場合には損害賠償請求等がなされてしまう可能性があります（不正の利益を得る目的又は当該他社に損害を加える目的で、営業秘密に該当する秘密情報を使用・開示する行為は不正競争防止法違反にもなり得ます）。

図表５（２）共同開発による情報混在のイメージ

○ なお、共同研究先が、自社だけでなく競合他社とも並行して研究を行っている場合には、当該研究先を通じた競合他社の秘密情報の意図しない侵害のリスクも生じ得るため、必要に応じて、下記の対応策とは別途、共同研究先に対しても複数の共同研究情報を意図せず侵害しないように注意を促すことが考えられます。

○ 以下では、共同研究開発や受託研究開発の場面において、①他社から得る情報の厳選、②秘密情報に該当する情報の明確化、③他社の秘密情報の分離管理、④自社の独自研究・開発からの他社の秘密情報の排除、の４つの視点に分けて対応策

を紹介します。必ずしもこのうち、いずれか１つの場面への対応で足りるということはなく、具体的な状況に応じ、必要な対策を採ることが重要です。

○　なお、同時に、研究開発の開始前に保有していた自社の独自情報については、本章５－１で記載したような措置を講ずることにより、独自性を立証することができるようにしておくことも重要です。

①他社から得る情報の厳選

他社情報の意図しない侵害のリスクを低減するためには、他社の秘密情報を得ること自体が自社の事業遂行上のリスクを抱えることになり得るという認識の下、他社から得る秘密情報を厳選することが重要です。他社から秘密情報を得る場合には「当該情報を共同研究開発目的以外で使用しない」旨の契約が結ばれることが通常であるところ、そのような契約に合意することは、将来的に自社の独自研究開発や別の他社との共同研究開発を行う際の紛争リスクを高めることになるからです。

具体例

- 他社の情報を得る前に、将来自社において関連する独自の研究開発を行う可能性を検討する。
- その可能性を踏まえた上で、他社の情報を得ることにより、自社の事業遂行に与えるリスクを具体的に検討する。
- 他社の情報を得る場合の「当該情報を共同研究開発目的以外で使用しない」旨の契約については、「〇〇年経過後は使用できる」といった、より細かな契約条件を検討することも考えられる。

②秘密情報に該当する情報の明確化

他社から秘密情報を得ることとした場合には、共同・受託研究開発の進捗状況等に応じ、秘密情報に該当する情報をできる限り明確化することが重要です。これは、秘密情報に該当する情報が明確となっていなければ、どの情報に対する意図しない侵害を防止するべきかという対策が立てられず、かえってそのリスクを高め、無用な対策コストを支払う必要が生じるおそれがあるからです。

具体例

- 秘密保持契約を締結する際に、できる限りその対象となる情報を契約書内で明確に示す（特に技術内容等に係る情報などは、将来の自社の独自研究開発に与える影響が大きくなることが考えられるため、社内での秘密情報の決定の場合や従業員の秘密保持義務の対象を決定する場合に比較して、より具体的・限定的に決定することが望ましい）。
  ex）秘密保持契約書内に、相手方から開示を受け、かつ開示の際に相手方から秘密である旨の明示のあった情報についてのみ秘密情報とする旨を規定する。
  ex）秘密保持契約書内に、相手方から受領した情報について、既に知っている情報であった場合には、その根拠とともに、その旨を申し出る義務を規定する（申し出た場合には当該情報は秘密保持の対象とならない）。
  ex）研究開発の過程で事前に想定していた範囲や書面で合意していた範囲を超えて、事後的に口頭で秘密情報が共有される事態が考えられる場合には、それに備え、「口頭での情報開示後、一定期間内にその旨を文書化した場合に限り、秘密保持義務の対象とする」旨の規定を設ける。
- 研究開発の過程で実際にいつどのような情報を授受したかについて記録する。相手方に授受の確認のサインをもらうことも考えられる。

③他社の秘密情報の分離管理

他社から実際に得た秘密情報については、自社情報と分離して管理します。自社情報と、他社情報が混在してしまうと、他社から訴えられたときに「他社の秘密情報を使っていないこと」を立証することが極めて困難となるため、情報が混在しないための管理をしっかり行っていたことを立証できるようにしておくことが重要です。

具体例

- 他社から情報を得る窓口を設定し、その窓口以外では他社から秘密情報を受け取らないようにする（専用のメールアドレスを設定することも有効）。また、その窓口では、取得した情報の内容、取得した日時、取得の経緯等を記録する。
- 他社の秘密情報を含む電子データは、自社情報とは別のフォルダにおいて管理する。場合によっては、そのフォルダには関係者以外がアクセスできないようにＩＤ・パスワード等でアクセス制限を行い、アクセスログを記録する。

- 化合物や試作品のように物それ自体が秘密情報に該当する場合は、特別のキャビネットや倉庫等において、自社情報と分離して保管する（施錠した上で、その鍵の貸出し記録や、その物の持出し記録を作成することも考えられる）。
- 自社における共同・受託研究開発の関係者（他社の秘密情報に接する必要のある従業員等）を特定し（必要に応じてリスト化して特定の手続でのみ当該リストを変更可能なものとすることも考えられる）、その全員から「当該情報を共同・受託研究開発の関係者以外に開示しない」、「当該情報を共同・受託研究開発目的以外で使用しない」旨の誓約書を取得する。
- 共同研究開発終了後に、確認書を取得し、誓約が遵守されたことを改めて確認する。

④自社の独自研究・開発からの他社の秘密情報の排除

自社において独自に、他社の共同研究・開発と内容的に類似する研究・開発等を実施する場合には、当該他社から秘密情報を取得ないし使用したとして訴えられるリスクを低減するため、自社独自の研究・開発に使用する情報の中に、当該他社から得た秘密情報が紛れ込んでしまうことを防止する措置を講ずる必要があります。

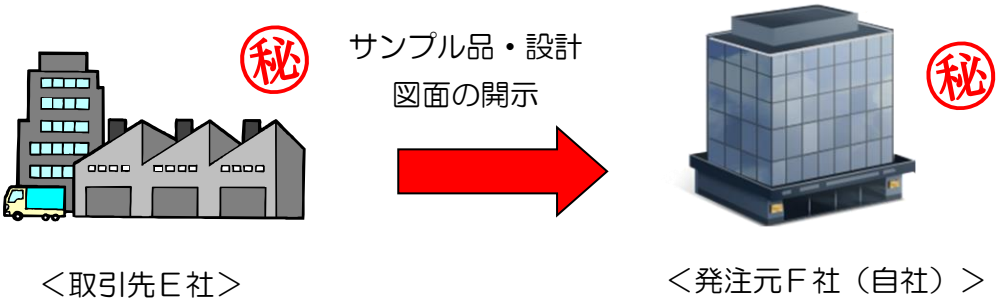
具体例

- 自社の独自研究開発の関係者を特定し、その全員から「当該他社の秘密情報に接触しない」又はその者が共同・受託研究開発にも携わる必要がある場合には「当該他社の秘密情報を自社の研究開発現場に持ち込まない」旨の誓約書を取得する。
- 自社の独自研究開発を開始するときに、その研究開発に使用する情報の中に、共同・受託研究開発に関する情報が含まれていないかを厳重に確認する。自社の独自研究開発に途中から参加する従業員がいる場合には、その従業員のＰＣ等もチェックする。また、共同・委託研究開発には専用の初期化されたＰＣを別途貸与することも考えられる。
- 前述のように情報を分離することに加えて、自社開発を行う者の中に、共同研究開発に携わる者を含めない（自社開発と共同研究開発の担当者を分ける）ことが望ましいが、人員との関係で難しい場合には、①自社開発で使用する情報を明確化する、②自社の研究開発現場と共同研究開発現場を物理的に別部屋とする、③それぞれの開発経緯を詳細に記録する等、更に厳格に情報を分離する対策を実施することが考えられる。

（３）取引の中での秘密情報の授受

○　日常的に行っている取引の中で、取引先から秘密情報を取得することは少なくありません。例えば、委託契約や請負契約等において、相手方から秘密情報の開示を受けることがあります。

図表５（３）取引先の情報混在のイメージ



○　このうち、特に留意すべき点としては、①委託者や注文者からではなく、受託者や請負人、下請企業等から秘密情報が開示される場面も想定されますが、これらの場面では委託者や注文者から秘密情報が開示される場面に比して、その情報の適切な管理の必要性について気づきにくい可能性があります。

○　特に、②商品サンプル等それ自体が秘密情報である物の受領の場面については、発注者である自社が、不正な利益を得たり、取引先に損害を加えたりする意図で当該商品サンプル等を使用・開示しないことは当然のことです（その場合には不正競争防止法上の民事・刑事責任（※）を問われてしまいます）が、そのような意図がないとしても、秘密表示が付された書類等に比べて、取引先の秘密情報を受領しているという意識が低くなることもあり得ます。

※平成２７年不正競争防止法改正により、営業秘密侵害罪が非親告罪となり、当該取引先の意思によらず、刑事訴追される可能性もあることに留意が必要です。

○　したがって、これらの場面においては提供された秘密情報の意図しない侵害のリスクが高まる可能性があり（このケースについても、（２）共同・受託研究開発のケースと同様、契約違反に基づく損害賠償請求や差止請求がなされることが考えられる）、意識的に対応策を講ずることが考えられます。

具体例

- 社内研修などを通じて、日常的な取引における秘密情報の授受の可能性や、商品サンプルや試作品等は、それ自体が他社の秘密情報に該当し得る旨を従業員に対して周知する。
- 秘密情報の開示や商品サンプル・試作品等の受領が、口頭やメールでのやり取りに留まって行われた場合であっても、秘密保持契約が成立していたとして提訴されるリスクが存在することから、取引先の秘密情報の内容や、使用目的の制限、秘密保持の期間などについて、書面により確認をすることが望ましい。
- 当該商品サンプルや試作品等を含む秘密情報を取り扱う自社従業員を限定した上で、「当該取引以外の目的で当該情報を使用・開示しない」といった誓約書を取得したり、特別のキャビネットや倉庫等において、自社情報と分離して保管したりするなど、（２）共同・受託研究開発のケースと同様の取組みが有効である。

（４）技術情報・営業情報の売込み

○　外部の研究者等が独自研究したものとして技術情報を売込みに来たり、何者かが顧客名簿等の営業情報を売込みに来たりした場合、実はその売り込まれた情報が他社の公開前特許等の秘密情報であったり、盗まれた顧客名簿であることもあり得ることから、当該情報の意図しない侵害のリスクが生じます。

○　特に、前述したとおり、売り込まれた情報が他社の営業秘密に該当する場合には、その事実について知らなかったとしても、知らなかったことに「重大な過失」がある場合には、不正競争防止法に基づく損害賠償請求や差止請求の対象となり得るため注意が必要です。

具体例

- 売り込まれた情報の出所や、どのようにしてその情報を取得したのか等を売込みに来た者に確認し、「当該情報は〇〇（出所）から正当に取得したものである」旨の誓約書等を取得することが望ましい。また、情報を売込みに来た者から確認した事実について、可能な範囲で関係者に事実関係を聴取することなども有効。
- その確認した内容等を踏まえてなお、他社の秘密情報の不正な売込みである疑いが相当程度残る場合には、その売込みには応じないことが重要。

５－３　営業秘密侵害品に係る紛争の未然防止

○　平成２７年不正競争防止法改正により、営業秘密を不正に使用することによって生じた物（営業秘密侵害品）の譲渡・輸出入等の行為が、民事措置（損害賠償請求・差止請求）及び刑事措置の対象に含まれることとなりました。

○　これは、営業秘密を不正使用した張本人（例えば、他社の営業秘密にあたる技術情報を不正に入手し、それを用いて製品を製造したメーカー）でなくとも、それが営業秘密侵害品であることを知って、又は知らないことについて「重大な過失」がある状態で、その営業秘密侵害品を譲り受けた者が、その営業秘密侵害品を譲渡・輸出入等する行為（例えば、営業秘密を侵害して作った製品であることを知っている小売業者による販売行為や商社による輸出行為）は民事措置の対象となるということです。

○　また、これらの行為のうち、営業秘密侵害品であることについて、それを譲り受けたときに認識した上で、意図的に譲渡・輸出入等を行った場合には、民事措置のみならず、刑事措置の対象にもなり得ます。

○　よって、他社との間で製品の売買等の取引をする場合には、そのような「重大な過失」があると判断されてしまうことのないように特に注意を払う必要があります。

○　ただし、この「重大な過失」とは我が国企業に求められるべき取引上の注意義務に照らし、営業秘密の取得時の客観的状況から、他社の営業秘密を侵害するおそれが大きいことが容易に予期できたにもかかわらず、その疑いを払拭するための合理的努力を怠ったこと、つまり悪意と同視し得るほど、取引上の注意義務に著しく違反したことを意味し、通常の企業活動を行っている場合にはこの「重大な過失」があるとされることは極めて限定的であることが想定されます。すなわち、実際に、自社の取引するすべての製品に対して、取引の都度、営業秘密侵害品であるか否かの確認を行うことは現実的ではないことから、基本的には、他社から「営業秘密侵害品である」との警告書を受領したり、取引相手が営業秘密侵害を行っている疑いがあるとの情報が業界内で広がっているといった「疑わしい状況」が生じている場合に、相当の注意を払ったということが証明できる程度の対策を行うことが肝要です。

具体例

- 自社が取引する製品について、「営業秘密侵害品である」との警告書を他社から受けた場合、まずはその書面が、侵害された営業秘密の内容や、どのような経緯で侵害がなされたか、いかなる理由で侵害の事実を確信したか、といった具体的な内容を伴うものであるか否かを確認する。
- 具体的な内容を伴う警告書である場合には、その内容について取引先などの関係者にその真偽を確認する。それを踏まえて、取引する製品が営業秘密侵害品であるとの疑いが相当程度残る場合には、それ以降の製品の取引は一旦中止することが望ましい。一方、取引を継続する場合には、取引先などの関係者から「営業秘密を侵害して生産したものではない」旨の誓約書を取得する。

  ※なお、警告書が電子メールで送付されることもあり得るところ、警告書を装った標的型攻撃メール等には十分に留意して対処することが必要。
- 例えば、「営業秘密の侵害事案について報道がなされた」、「自社の販売する商品と同じメーカーが製造する同一ラインナップの商品について差止請求訴訟が認容された」、「取引相手が営業秘密侵害を行っている疑いがあるとの情報が業界内で広がっている」といった「疑わしい状況」が生じた場合にも、前述と同様の確認を行う。

複数の委託契約における秘密保持の状況を
データベースで一元管理している事例

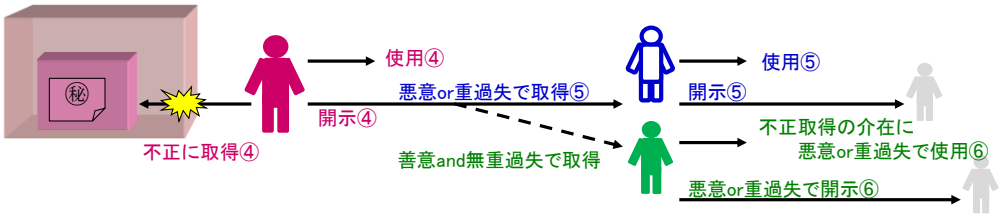
◆ **製造業・大規模企業の事例**

～契約管理データベースを活用して自社の義務違反を防ぐ～

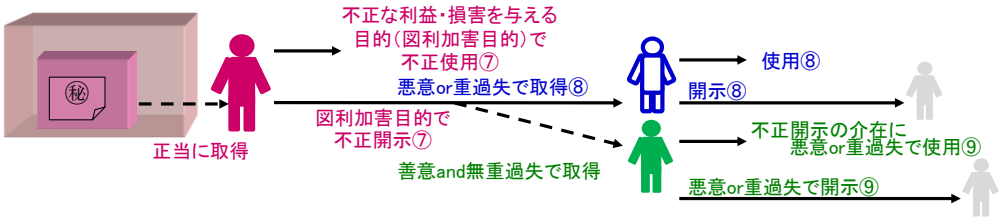
秘密保持契約を締結する相手方が多岐にわたり、様々な部門において独自に契約を締結すると、秘密保持を負っているという認識をしていない従業員が知らず知らずのうちに秘密保持義務違反を犯してしまう可能性がある。そこで、契約管理データベースを導入し、自社が交わした契約をすべて入力。それにより、従業員が、どの取引先に対してどのような秘密保持義務を負っているのかといった点を常に確認し、自社の義務違反を防ぐようにしている。

図表５（４）不正競争防止法上の営業秘密侵害行為類型（民事）

〇不正取得の類型



〇正当取得の類型

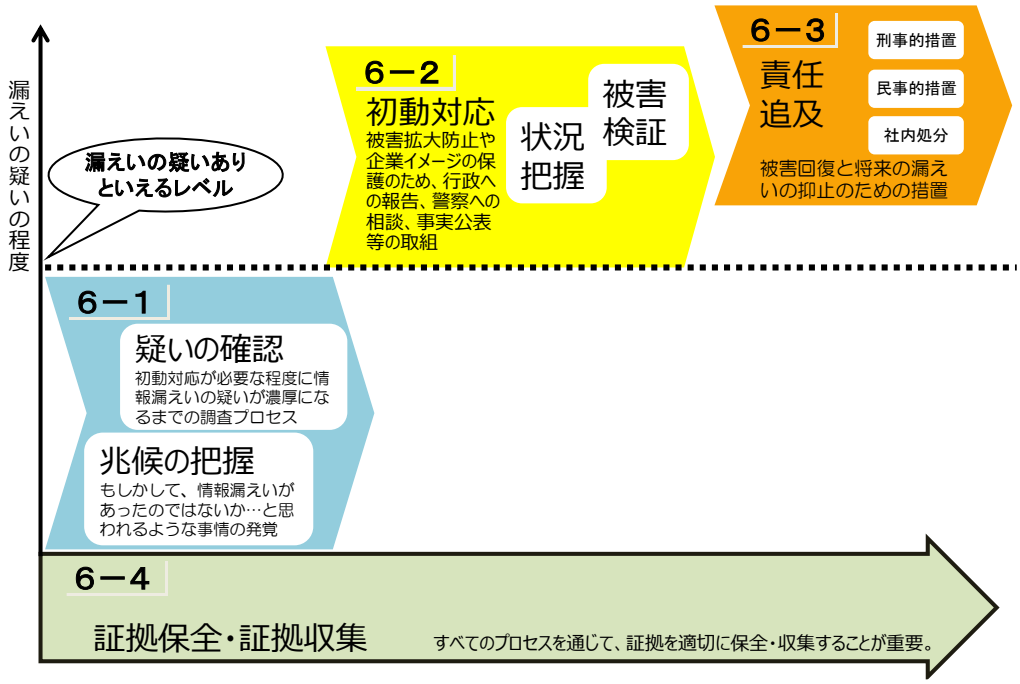


※　〇囲いの数字は、不正競争防止法第2条第1項各号の該当号数
※　悪意or重過失＝当該行為があったことを知っている、あるいは重大な過失により知らない
※　善意and無重過失＝当該行為があったことを、重大な過失なく知らない

第６章　漏えい事案への対応

- 企業が情報管理をどれだけ徹底したとしても、昨今のサイバー攻撃をはじめとする情報漏えい手口の高度化等を踏まえると、情報漏えいを完全に防ぎ切ることは困難であり、万が一情報漏えいが起こった場合に迅速に対応できるよう備えておくことが重要です。
- 対策に当たっては、（１）情報漏えいの疑いを確実・迅速に確認できるようにすること、（２）情報漏えいが起こってしまったと思われる場合に、その損失を最小限に抑え、また原因究明・責任追及に係る証拠を保全するための応急措置を迅速に実施すること、（３）損失回復（損害賠償・差止）と将来的な再発抑止のための徹底的な責任追及を実施すること、の３点がポイントとなります。
- なお、漏えい時に適切な対応をするためには、第２章及び第３章の漏えい防止対策を講ずるとともに、第４章の社内体制を整え、また万が一紛争に発展してしまった場合を見据えた第５章に記載する事前の備えをしていることなど、漏えい後の対応だけではなく、日頃からの備えをしておくことが重要となります。

図表６（１）本章における各項目の関係



６－１　漏えいの兆候の把握及び疑いの確認方法

○　企業の重要な情報が漏えいした場合、多くの場合、その被害は時間の経過とともに拡大します。速やかに情報漏えいに対処し、その被害を最小限に抑えるためには、事前に情報漏えいにつながり得る兆候を把握（以下（１））し、その兆候を確認すること等を通じて、漏えいの疑いを確認し（以下（２））、速やかに対処することができる体制・社内ルールを構築したうえで、インシデント発生時の活動内容を事前に定め、訓練等で確認しておくことも必要です（第４章も参照）。これらの取組みは、第３章で示した「視認性の確保」等にも資する場合が多いことから、同時に情報漏えいを未然に防止することにもつながると考えられます。

（１）漏えいの兆候の把握

○　ここでは、漏えいの主体に応じて、情報漏えいにつながり得る兆候と考えられる具体例を記載します。具体的には、①従業員等、②退職者等、③取引先、④外部者ごとに記載をしています（それぞれの定義は第３章に記載）。

○　以下のような兆候を適切に発見するためには、日頃から自社の通常の業務や取引の実態を把握しておくことが重要です。例えば、以下①に記載の「業務量に比べて異様に長い残業時間」や以下③に記載の「取引先からの異様に詳細な情報照会」といっても、各企業・各部署の状況に応じて、どの程度の時間の残業が「異様」と言えるのか、取引の実態に照らしてどの程度の情報開示が通常と言えるのかは異なります。

○　具体的には、例えば、自社の従業員の勤務状況等について、タイムカードによる業務時間の把握や、部署内での報告、定期的な面談による業務量の確認等を通じて、どのような状態が「異様」と言えるのかを意識しておかないと、従業員の残業が情報漏えいにつながり得る兆候に当たるのかどうかの判断が難しいでしょう。

○　漏えいの兆候の把握にあたっては、ＡＩ等の最新技術を組み入れたモニタリングシステムの活用が考えられますが、従業員保護のための適切な設定ができるものを選定し、~~プライバシー・人権を保護するための個人情報保護法等の法的要求を満足できる~~組織体制を構築することが必要です。また、監視効能の有効性、従業員の通常行動を学習し、行動に重要な変化が生じた場合に特定できる機能等の有効性を評価・確認します。

①従業員等の兆候

従業員等の情報漏えいの兆候としては、例えば、以下のものが考えられます。

- （業務上の必要性の有無に関わらず）秘密情報を保管しているサーバ═や記録媒体へのアクセス回数の大幅な増加
- 業務上必要性のないアクセス行為
  ex）担当業務外の情報が保存されたサーバ═やフォルダへの不必要なアクセス
  ex）不必要な秘密情報の大量ダウンロード
  ex）私物の記録媒体等の不必要な持込みや使用
- 業務量に比べて異様に長い残業時間や不必要な休日出勤（残業中・休日中に情報漏えいの準備等を行う従業者が多いことから兆候となり得る）
- 業務量としては余裕がある中での休暇取得の拒否（休暇中のＰＣチェック等による発覚を恐れるため兆候となり得る）
- 経済的、社会的に極めて不審な言動
  ex）給与に不満を持っているにも関わらず急激な浪費をし始めた
  ex）頻繁に特定の競合他社と接触している

②退職者等の兆候

退職者等の漏えいの兆候としては、例えば、以下のものが考えられます。特に、中核的な業務に携わっていた者など、キーパーソンといえる元従業員についてはその退職前後を通じた動き（転職先企業の業務内容を含む）の把握が重要となります。

- 退職前の社内トラブルの存在
- 在職時の他社との関係
  ex）競合他社から転職の勧誘を受けていた
- 同僚内の会話やＯＢ会等で話題になっている、元従業員の不審な言動
  ex）競合他社に転職して、前職と同じ分野の研究開発を実施しているとの取引先からの情報提供
- 退職者の転職先企業が製造・販売を開始した商品の品質や機能が、特に転職後、自社商品と同水準となった

③取引先の兆候

取引先の漏えいの兆候としては、例えば、以下のものが考えられます。

- 取引先からの突然の取引の打切り
  ex）自社しか製造できないはずの特別な部品について、発注元からの部品発注が途絶えた
- インターネット上での取引先に関する噂
  ex）インターネット掲示板、ＳＮＳ、ＨＰ等において、自社の非公開情報や自社製品との類似品が取り沙汰されている
- 取引先からの、取引内容との関係では必ずしも必要でないはずの業務資料のリクエストや通常の取引に比べて異様に詳細な情報照会
- 自社の秘密情報と関連する取引先企業の商品の品質の急激な向上
- 自社の秘密情報と関連する分野での取引先の顧客・シェアの急拡大

④外部者の兆候

外部者の漏えいの兆候としては、例えば、以下のものが考えられます。

なお、不正アクセスなどのサイバー攻撃については、その兆候を把握しにくく、実際に情報漏えいの被害が発覚したときが最初の兆候となる場合も多いため、その兆候をいち早く把握するための日常的な管理体制の構築が特に重要と考えられます。

- 自社における事件の発生
  ex）社員証・パスワードなどの流出事件の発生
  ※流出の態様としては、典型的には盗難行為であるが、巧みな話術による聞出し、盗み聞き・盗み見等を通じた流出があり得ることにも留意
  ex）社員の机上の物など、オフィスにおける盗難事件の発生
- 自社会議室における偵察機器（盗聴器など）の発見
- 競合他社等での秘密情報漏えい、不法侵入等の事案発生（類似の技術を持つ自社の情報についても狙われやすいと考えられるため兆候となり得る）
- ウィルス対策ソフト、セキュリティ対策機器による警報
- 自社の秘密情報それ自体ではないが、それと不可分一体のはずの情報が漏えいしていること
- 電話、メール等を受信した関係者からの通報
  ex）自社の顧客名簿に記載された者が、競合他社から営業の電話を受けたが、その競合他社に連絡先を教えた覚えがないため、不審に思ってその旨連絡をしてきた

ex）他所における侵害を調査していたセキュリティ調査機関が、侵害されたサーバ═において自社の情報を発見したと連絡してきた

（２）漏えいの疑いの確認

○　前述（１）により情報漏えいにつながり得る兆候を把握した場合には、その兆候を放っておくことなく、情報漏えいが発生した疑いが高いものとして初動対応を開始する必要がないかを確認する必要があります。いかなる者による情報漏えいの兆候であったかにより、有効な確認方法が異なることから、兆候が生じた者に応じた確認方法を取ることが必要であると考えられます。したがって、以下では前述（１）の分類に応じて、その漏えいの疑いを確認するための対応策として考えられる具体例取組みを示します。

○　テレワークの場合、企業内での場合と異なり物理的な視認性の確保が困難なことから、テレワークに伴うログを記録して、安全に保存するようにします。このログには、秘密情報へのアクセス履歴、利用者の操作履歴（Ｗｅｂのアクセスやメールの送受信履歴など）、ＶＰＮ装置へのアクセス履歴、テレワーク関連機器やクラウドサービスにログインした際の認証・操作履歴、テレワーク端末の操作履歴等についても取得します。

○　また、モニタリングシステムの開発も進んでおり、これを活用することが有効と考えられますが、その導入に当たっては、従業員保護のための適切な設定ができるものを選定し、~~プライバシー・人権を保護するための個人情報保護法等の法的要求を満足できる~~組織体制を構築することが必要です。さらに、このような従業員をモニタリングすることは従業員等の行為の正当性（身の潔白）を証明する手段としても有効であり、その目的が従業員の保護であることを就業規則等に明記して従業員に周知徹底するとともに、従業員の理解を得た上で、適切な運用を行うことが望まれます。

○　なお、以下の取組みを実施するにあたっては、兆候のあった直近の時点だけではなく、ある程度過去に遡って、事実や状況の確認を行う必要がある場合があるという点に留意してください。

①従業員等による漏えいの疑いの確認

従業員等による漏えいの疑いを確認するための取組みとしては、例えば、以下のものが考えられます。なお、メールのモニタリングや社内ＰＣのログ確認について

は、そのような措置を行うことがあり得ること等を事前に就業規則[57]で定めておくなどすると、手続的な問題は起こりにくくなるでしょう。

具体例

- 文書管理台帳等による情報保有状況の確認
  ex）紙媒体の資料やＵＳＢメモリ等の記録媒体のリスト管理により、漏えいの兆候のある者による重要情報の不正な持出しがないかを精査する
- 漏えいの兆候のある者の社内ＰＣについて、ＵＳＢメモリ等の記録媒体の接続ログの確認
- 漏えいの兆候のある者の社内ＰＣのログ等の保存・確認や、メール送信、インターネット利用履歴のモニタリング（場合によっては社内ＰＣを没収して調べることも考えられる）
  ex）業務メール、インターネット上でのメール、外部ストレージ（クラウドサービス等）へのアップロードなどを通じた不正なデータ送信の確認
  ex）漏えいの兆候のある者の社内サーバ、フォルダ、電子データへのアクセスに関するログの詳細な確認
  ※一定以上の量のダウンロードがあった場合に自動でアラートの鳴るシステムを導入することなどは、速やかに漏えいの疑いの確認に取りかかることを可能とするという観点から有効。
- 秘密情報を含む幹部宛のメールが、漏えいの兆候のある者の個人アドレスへと自動転送されるような不正な設定がなされていないか確認
- 社内規程等に基づく監査の実施

[57] 参考資料２の「第１　秘密情報管理に関する就業規則（抄）の例」参照。

②退職者等による漏えいの疑いの確認

退職者等に関して、退職予定者等による漏えいの疑いの確認については、前述①と同様の取組みを行うことが考えられますが、退職後に特有の確認としては、退職者の転職先把握が特に重要です。仮に競合他社への転職の事実が確認できた場合には、速やかに本章６－２以降に記載の初動対応の開始を検討することが考えられます。

具体的な取組みとしては、例えば、以下のものが考えられます。

具体例

- 漏えいの兆候のある退職者等の転職先企業及びその業務内容について、元同僚らへの事情聴取、ＯＢ会等、内部通報窓口、新聞紙面上の会社人事情報といった様々なルートでの情報収集
- 漏えいの兆候のある退職者について、退職前後での資料の大幅な減少の有無の確認
- 社内資料のリスト管理等による、漏えいの兆候のある退職者等の未返却物の確認
- 漏えいの兆候のある退職者等の退職前一定期間のダウンロードデータの内容チェック
- 漏えいの兆候のある退職者等の退職前一定期間のメール等の通信記録のモニタリング

③取引先による漏えいの疑いの確認

取引先による漏えいには、第３章で記載したとおり、大別して、

（ｉ）取引先自体が主体となり悪意で情報の不正使用や不正開示を行う場合

（ii）取引先の情報管理が不十分であったことに起因して、相手方従業員、退職者、再委託者や外部者等を通じて情報漏えいしてしまう場合

の２通りの場合があり得ます。

（ii）の場合は委託先等の社内において、本項①、②、④の取組みを実施することを契約等で確保するといった取組みが考えられます。以下では、（ｉ）の場合について有効と考えられる取組みの例を掲載します。

具体例

- 漏えいの兆候のある取引先等が製造・販売している商品のチェック
  ex）取引先が製造・販売する商品の品質や機能が、兆候を把握した時期の前後において、自社商品と同水準となった
- （顧客名簿等に意図的に入れた）トラップ情報の使用の確認

ex）顧客情報の中に意図的に自社や協力会社の住所を利用したダミー情報を入れておいたところ、そのダミーの宛先に郵送物が届いた場合

- 漏えいの兆候のある取引先に自社のサーバ＝を使わせていた場合には、そのアクセスやダウンロードの履歴をチェック

④外部者による漏えいの疑いの確認

外部者については、例えば、以下の取組みを行うことが考えられます。

具体例

- 競合製品・類似商品のチェック

  ex）他社が製造・販売する商品の品質や機能が、兆候を把握した時期の前後において、自社商品と同水準となった

- （顧客名簿等に意図的に入れた）トラップ情報の使用の確認

  ex）顧客情報の中に意図的に自社や協力会社の住所を利用したダミー情報を入れておいたところ、そのダミーの宛先に郵送物等が届いた場合

- パスワードの流出した端末に対する不正アクセスの有無の確認
- 自社内への不法侵入等がないかどうか、監視カメラの記録映像を確認
- 社内資料のリスト管理による、書類や記録媒体等の持出しの有無の確認
- ウィルス対策ソフト、セキュリティ対策機器等を用いて、不正アクセスやサイバー攻撃の有無を確認

６－２　初動対応

○　情報漏えいの疑いを確認し、対応の必要があると判断した場合、被害の拡大防止や企業イメージの保護、迅速かつ適切な法的措置のために、適切な初動をとることが重要です。

○　スムーズな対応を行うためには、日頃から連絡体制や対処要領を準備しておくことが考えられます[58]。

58　ＩＰＡ『組織における内部不正防止ガイドライン』ｐ８９～ｐ９１、『対策の~~情報漏えい発生時の対応~~ポイント~~集~~』も参照。コンピュータセキュリティのインシデント対応体制については、日本シーサート協議会の HP『CSIRT 構築に役立つ参考ドキュメント類』も参照。
http://www.nca.gr.jp/activity/build-wg-document.html

具体例

- 有事における組織体制や、レポートラインの確保につき、事前に社内マニュアル等で明文化しておく（第４章も参照）。
- 平時から、情報漏えいを見据えた取組みを実施する。
  ex）情報漏えいが実際に起こったと仮定して、社内での対処（部門間での情報共有、対策チームの招集、初動対応の手順、報道対応等）を訓練（机上訓練・実地訓練）する
  ex）実際に社内システムを攻撃し、侵入できないという事実によってその安全性を確認する（ペネトレーションテストの実施）

（１）社内調査・状況の正確な把握・原因究明

情報漏えいの状況を正確に把握し、将来的な再発防止に資するため、まずは以下の観点から、現時点で把握できていること、できていないことについて書面等を用いて社内で明らかにします。

いつ：いつ漏れたか。一度だけか。数回に分けて漏れたか。漏えいを把握するまでの時系列は。

だれが：誰が漏らしたか。社員か、委託先か。その者はどのような権限を持っていたか。外部者の場合、自社とどのような関わりがある者か。

なにを：漏えいした情報の内容は何か。どのくらいの量の情報が漏れたか。どのような形で保存されていた情報か。

どのように：どのような方法・原因で漏えいしたか。ネットワークを通じたものか。どのようにセキュリティが破られたか。

（２）被害の検証

前述（１）で明らかになった事実を元に、自社、取引先、消費者等に対して、どのような損失（間接的な損失や信用の低下を含む）が予測されるか、最悪の事態を想定して検証を行います。この検証を通じて、更に対応を進める必要があると判断される場合には、以下のような対応を進めていきます。

（３）初動対応の観点

以下に示す取組みが主なものとして考えられますが、情報は素早く拡散してしまうことや秘密情報の漏えいによる損失は回復が困難であること等に鑑みると、全体

として、迅速な対処をすることが肝要です。特に、コンピュータウィルス等による被害の場面では、表面的に発覚したウィルス被害にのみ対処するのではなく、探知が困難な形でより深刻なウィルスが埋め込まれている場合もあるため、技術的専門家[59]に相談することが望まれます。

○更なる拡散の防止

具体例

- 自社情報端末のネットワークからの遮断（主にサイバー攻撃による漏えいの場合）
- 漏えいしたと疑われる者等に対する警告書の発出
- ＨＰ等に漏えいした情報が開示された場合、当該情報のインターネット上からの削除要請

○法律に基づく手続

具体例

- 個人情報の場合、個人情報保護委員会への報告及び本人への通知~~法に基づき、業種に応じた主務官庁に対する報告等~~の対応が必要
- 特に、一定の個人データの漏えい等の事態が発生した場合、事態を知った時点から概ね３～５日以内に「速報」として、また３０日以内（不正な目的で行われたおそれがある場合は６０日以内）を「確報」として個人情報保護委員会に報告しなければならない。また、当該事態が生じた旨を本人に通知しなければならない。~~故意の内部不正によって個人データが漏えいした場合は、遅滞なく、個人情報保護委員会及び本人（漏えいしたデータの保有者）への報告を実施。また、事態の発生を認識した後速やかに報告するとともに、６０日以内に確報を行う。~~
- 各種業法などの法令上、監督官庁等との間で、要求されている手続を実施

○企業イメージを含む損失の最小化

具体例

[59] IPA では、「情報セキュリティ安心相談窓口」を開設し、一般的な情報セキュリティ（主にウイルスや不正アクセス）に関する技術的な相談に対してアドバイスを提供しています。（https://www.ipa.go.jp/security/anshin/index.html~~http://www.ipa.go.jp/security/anshin/~~）

- 把握している事実につき、速やかな対外公表（事実経緯、漏えいした情報の内容、漏えいの原因、再犯防止策、問い合わせ窓口等について）の実施
- 顧客名簿流出時の被害者対応・マスコミ対応
  ex）被害者が特定できている場合等には被害者への事実の連絡及び謝罪
  ex）被害者が不特定多数であって今後の被害拡大の可能性が高い場合には、個別の謝罪に先だって公表
- 刑事事件に発展する可能性のある場合には、証拠隠滅や逃走を防止するためにも、警察に事実公表のタイミングや内容について早期に相談することが有効な場合もある。
- 共同研究の成果の漏えいなど、他社の情報が併せて流出しているおそれのある場合には、当該他社に対して対応を相談することが望ましい。

（４）初動対応の体制

○　以上の初動対応については、様々な部署が関係部署として想定されるところ、関係部署が綿密に連携して、適切かつ迅速に対処する必要があります。比較的小規模な企業の場合には、経営層が全体を統括しながら対応を進めていくことが考えられます。

○　一方で、企業規模によっては、役員をヘッドとした組織（対策チーム）を設置することが考えられます。この対策チームには、必要に応じて外部の専門家を含めることも考えられます。ただし、対策チームの人員は、社内での情報拡散を防止する観点から、必要最小限の人数で構成し、かつ扱っている内容については秘密保持を徹底することが考えられます。

○　場合によっては、第４章で紹介した「秘密情報管理委員会」の枠組みを利用して、対策チームの機能を行わせることも考えられます。ただし、この場合にも、「秘密情報管理委員会」の構成員のうち、必要最小限の範囲で情報を共有することが望まれます。

６－３　責任追及

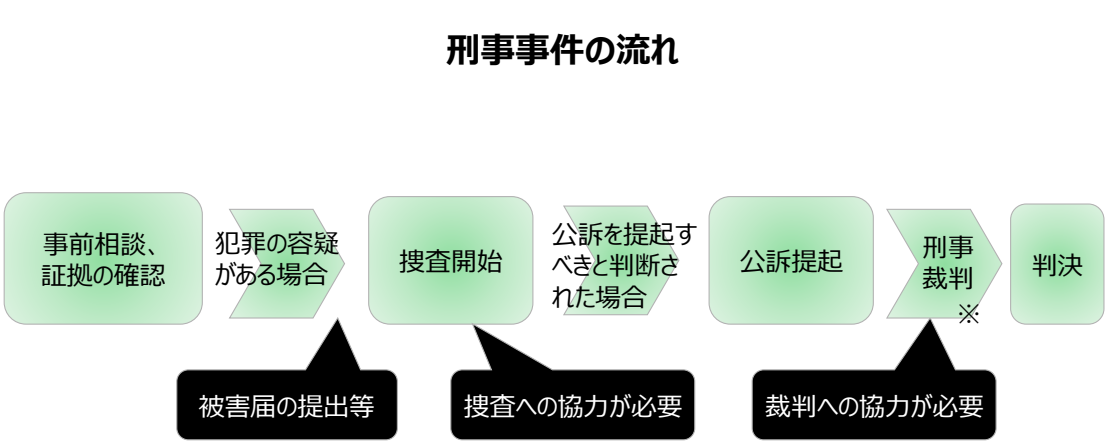
○　自社における被害回復と将来的な漏えいの抑止のため、徹底的な責任追及を実施します。

○　その前提として、責任追及の確実性と証拠収集の効率性を見据えて、どの情報を不正競争防止法上の責任追及に係る「営業秘密」又は「限定提供データ」とするのかを明確にするという点にも留意します。

○　なお、刑事と民事でいずれの措置（又は双方の措置）を採るかについては、相互に関係はなく、警察や弁護士等の専門家に相談しつつ、具体的事情に応じて臨機応変に決定すべきと考えられます。

（１）刑事的措置

図表６（２）刑事事件の流れ



※刑事訴訟手続の流れに関しては、参考資料「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」参照。

○　秘密情報の漏えいの事案では、当該情報が営業秘密に該当した場合に不正競争防止法上の営業秘密侵害罪（同法第２１条等）に該当し得るだけではなく、不正アクセス行為の禁止等に関する法律違反の罪（同法第１１条等）、電子計算機使用詐欺罪（刑法第２４６条の２）、背任罪（同法第２４７条）、横領罪（同法第２５２条）、個人情報データベース等不正提供罪（個人情報保護法第１７９~~８４~~条）等に該当する可能性もあります。

○　こういった罪に対する刑事責任の追及には、警察の関与が不可欠であるため、まず近場の都道府県警察本部の担当課[60]に相談に行くことが考えられます。その際には、会社の方針や社内調査の結果等を説明できる担当者が相談に行くことが好ましいと考えられます。

相談時に持参することが望ましいと考えられる資料

- 企業の概要がわかるもの（履歴事項全部証明書、組織図、パンフレット等）
- 侵害された営業秘密がわかるもの（データ印字、簿冊のコピー等）
- 漏えいが疑われる従業員（以下「被疑者」という。）を特定する資料（履歴書、人事記録等）
- 被疑者の勤務場所がわかるもの（事務所配置図、配席図等）
- 被疑者の出退社状況がわかるもの（タイムカード、営業日誌等）

※６－４（２）「営業秘密の要件該当性（特に秘密管理性）の証明に有効な資料例」及び「不正競争防止法違反の要件該当性の判断に有効な資料例」も併せて参照。

※その他、コンピュータシステムの概要、職場配置図など、侵害態様の解明に役立つ資料を持参することも有用と思われる。

○　場合によっては、必要書類が整うのを待たずして、前述６－２（３）の初動対応の一環で早急に警察へ相談するという選択肢もあり得ます（いかなる資料を、どのように確保すれば良いかといった証拠保全等について、警察から指導を受けられる場合もあるため）。ただし、この段階では情報の漏えいに関する資料（持ち出したことを示す証拠等）が不足していることから捜査が開始できない場合もあり得ることに留意が必要です。

○　また、刑事事件記録の民事裁判における活用についても、弁護士に早めに相談することが考えられます。

○　捜査開始後は、多数の関係者からの事情聴取、社内の実況見分等について、警察と連携・協力していくことが重要です。

（２）民事的措置

○　民事責任の追及の手段としては、当事者間の交渉による解決の他、民事裁判を提起して損害賠償請求権の行使等を行うことが考えられますが、それに先立って、民事保全手続で裁判前に権利の確保を求めることができます。

60　参考資料３「各種窓口一覧」参照。

○　また、知的財産権に関する調停手続（知財調停）、ＡＤＲ（裁判外紛争解決手続）の活用により、非公開の手続での柔軟な紛争解決手段を検討することも考えられます。紛争の存在自体をオープンにすることに抵抗があり、かつ、任意の交渉では話合いがまとまらないときなどに利用することが考えられます。

○　具体的にどのようなタイミングで、いかなる手段によって民事責任を追及するべきかはケースバイケースの判断であり、適切な損失回復のためにも、弁護士等の専門家と十分協議の上、決定することが望まれます。

裁判外の交渉

【内容】

- 当事者間で行う、紛争解決のための話合い全般をいう。

【特色】

- 法律の要件やルールにとらわれずに、当事者の任意で柔軟な解決手法を採ることが可能。

【留意点】

- 裁判所等の第三者の関与がないため、話がまとまらないおそれがある。

民事保全手続

【内容】

- 裁判を起こす前に、将来の権利を保護するため、仮の権利状態を確保しておくための手続。
- 営業秘密侵害や限定提供データ侵害が疑われるケースでは、営業秘密や限定提供データの開示・使用の仮の差止めや、競合他社への就職の仮の差止め等が考えられる。
- 裁判官との面接（当事者双方が出席する審尋期日を含む）を複数回行い、差止め等の可否を決定する。
- あくまで仮の手続であり、その後に正式な民事裁判をし、勝訴するまでの間のみ差止め等を目指すもの。

【特色】

- 手続は非公開。
- 裁判手続等に比べて迅速な対応が可能（事案によっては裁判手続と同程度の期間を要する場合もある）。

- 手続費用は低廉（申立人、被申立人一人ずつの場合、一件 2000 円。なお、別途郵便切手も必要[61]）。ただし、仮の差止めが認められるためには、本体の訴訟で判断が覆った場合に備えた担保（担保の有無や額は裁判所が決定）が必要[62]。

【留意点】

- 差止め等を認めてもらうためには、実務上は民事裁判手続と同程度の証拠が必要である（民事保全手続は仮の差止めを求めるものにせよ、営業秘密の使用等を一定期間止められるという効果は、事実上民事裁判に勝訴したときと類似するため）。

民事裁判手続

【内容】

- 営業秘密・限定提供データの使用の差止請求、営業秘密・限定提供データの漏えいによる損害賠償請求等を求める裁判手続。
- 例えば、自社従業員が競合他社へ転職した際に営業秘密を漏えいした事例では、その営業秘密の使用の差止め、その営業秘密の廃棄、その営業秘密の使用により生じた生産物の廃棄などを請求することが可能。同時に、自社従業員が競合他社へ転職した事例では、既に当該従業員に対して退職金の支給を行っていた場合、当該退職金の返還を求める裁判などが考えられる。

【特色】

- 手続は公開。ただし、営業秘密に該当するものについて当事者が尋問を受ける場合に、裁判所の決定により、尋問を公開しないで行うことができる（~~不競法~~不正競争防止法第１３条）。
- 手続費用は民事保全手続に比べて高額であり、その具体的金額は請求内容（差止請求の有無、損害賠償請求額）に応じて変動する。

【留意点】

- 裁判手続はその終結までの間に年単位での期間を要する場合も多い。

知財調停[63]

【内容】

61 http://www.courts.go.jp/tokyo-s/saiban/l3/l4/Vcms4_00000355.html
62 http://www.courts.go.jp/tokyo-s/saiban/l3/l4/Vcms4_00000354.html
63 東京地方裁判所ホームページリンク
（https://www.courts.go.jp/tokyo/saiban/minzi_section29_40_46_47/tizaityoutei/index.html）
大阪地方裁判所ホームページリンク
（https://www.courts.go.jp/osaka/saiban/tetuzuki_ip/index.html）

➢　ビジネスの過程で生じた知的財産権をめぐる紛争について、東京地裁又は大阪地裁知財部の裁判官及び知財事件の経験が豊富な弁護士・弁理士から構成された調停委員会の助言や見解を得て、原則として、３回程度の話合いにより簡易・迅速な解決を図る手続。

【特色】

➢　申立ての有無を含め手続はすべて非公開で行われるため、営業秘密の不正取得に関する紛争事例などにおいて、紛争の存在自体を第三者に知られることなく、迅速に紛争の解決を図ることができる。

➢　ウェブ会議を利用することで、東京や大阪以外の地域からも利用可能。

【留意点】

➢　管轄裁判所を東京地裁又は大阪地裁とする管轄合意が必要。ただし、令和８年５月２４日までに施行される「民事関係手続等における情報通信技術の活用等の推進を図るための関係法律の整備に関する法律」により、知的財産の紛争に関する調停事件について、簡易裁判所に加え、東京地方裁判所及び大阪地方裁判所にも管轄が認められることとなるので、その施行後は管轄合意が不要となる。

ＡＤＲ（裁判外紛争解決手続）

【内容】

➢　裁判によらず公正中立な第三者が当事者間に入り、話合いを通じて解決を図る手続。仲裁（中立な第三者による一定の判断が下されるもの）、調停・あっせん（いずれも中立な第三者の仲介による解決合意）など様々なものが存在。

【特色】

➢　手続は非公開であるため、係争の事実等が明るみに出ないで済む。

➢　ニーズに応じて仲裁、調停、あっせんを選択できるなど、裁判外紛争解決手続の利用の促進に関する法律の枠内で、比較的柔軟な対応が可能。

【留意点】

➢　相手方がＡＤＲ手続の開始に同意しないと、手続を行うことができない。

（３）社内処分

以上の刑事責任や民事責任の追及の他、従業員による漏えいに対しては、社内での処分（懲戒免職、降格等）を行うことが考えられます。そのためには、日頃か

ら、漏えい事案に適正に対処できるような社内規程になっているか、確認しておくことも重要です。

※ただし、従業員に対し過度な萎縮を及ばさないように配慮が必要です。

６－４　証拠の保全・収集

○　本章６－１から６－３までに記載した、漏えいの兆候の把握及び疑いの確認、初動対応、責任追及の全ての過程を通じて、各過程で必要となる範囲で、段階的に、かつ、着実に、漏えいの事実を裏付ける証拠を積み上げることが重要です。

○　その際に重要なのは、証拠の入手・生成方法を明らかにしておくことによって、証拠の保全・収集の正当性（改ざん等をしていないこと）を担保することや、事後的に共犯者が発覚した場合等に備えて得た情報を一定期間保存しておくことによって、保全・収集した証拠をきちんと利活用することができるようにしておくことです。

○　ここでは、責任追及のための準備段階（漏えいの兆候の把握、疑いの確認、初動対応）（以下（１））と、実際に責任追及を行っていく段階（以下（２））とに分けて、証拠保全・証拠収集に関する具体的取組みとして考えられるものを紹介します。

（１）証拠の保全

○　証拠の中には、特に電子情報など、時間の経過とともに失われやすく、時宜を逃すと証拠を確保することができなくなってしまうものが存在するため、そのような情報については、迅速な証拠の保全が求められます。

○　まず、早期に社内のネットワークやセキュリティの担当者と連携することが重要になります。

○　ただし、専門家を通さず自社だけで闇雲に保全を行おうとすると、場合によっては情報が壊れてしまったり、改ざんを疑われて事後的に証拠価値が失われる場合もあり得ますので留意が必要です。警察に即座に通報する、専門業者（フォレンジック等）を活用するといった、専門的な知見を持った者と適宜連携することが安全な場合が多いと考えられます。

○　なお、デジタルフォレンジックの活用にあたっては、システム管理者、インシデント対応担当者、デジタルフォレンジック担当者、弁護士、内部監査担当者等と連携することが必要です。サービスを受ける場合には、必要となる情報を迅速に提供できるように事前に伝達内容や方法を取り決めておくことが望まれます。さらに、漏えいした秘密情報にインサイダー情報が含まれる場合は、外部のデジタルフォレンジック解析を支援する担当者等に厳正な秘密保護・管理を求め、インサイダー取引につながらないようにします。

○　また、まだ漏えいの証拠が十分に確保できておらず、漠然と漏えいが疑われるに留まる段階で、当該漏えい行為をしたと考えられる従業員に接触する（不用意に事情聴取を行う）など拙速な対応をすることは、かえって証拠隠滅を助長するおそれなどがあるため避けるべきです。自社従業員からの漏えいが疑われる場合には、その漏えいの疑いに関する事情について対策チーム等の関係者限りとするなど、慎重に対応して証拠の隠滅・散逸等を防ぐことが重要です。実際にいかなる対応をすべきかは、警察や弁護士等と相談することが望まれます。

○　この他、民事訴訟法に基づく証拠保全手続が有効なケース（漏えいの疑われる者の自宅に所在する書類に対する証拠保全手続等）も考えられる。

○　以下は、本章６－１（２）における漏えいの疑いの確認のための具体的方策に加えて、特に証拠の保全の観点から重要と考えられる取組みとなります。

具体例
- 社内ネットワークのアクセスログや、監視カメラ等の記録を保存
- 漏えいが疑われる従業員のＰＣ等のバックアップ・通信記録保存・解析
- 漏えいの疑われる者から携帯電話やＰＣ等の通信記録の開示を受けることに成功した場合は、写真撮影等による証拠化

（２）証拠の収集

○　実際に責任追及を行っていく段階に用いる証拠を収集するにあたっては、特に営業秘密に該当すると思われる情報に関して、不正競争防止法に違反する事実を証明することを意識することが重要です。

○　すなわち、まず、漏えいされた秘密情報が同法で定義される営業秘密に該当するための要件として、①秘密管理性、②有用性、③非公知性が挙げられます（同法

第２条第６項）。また、それに加え、営業秘密侵害による刑事責任を問うためには同法第２１条第１項、民事責任を問うためには同法第２条第１項第４号から第１０号までの要件等をそれぞれ充たす必要があります。

○　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。

○　以下では、同法に規定される不正競争行為があったことの証拠となり得るものとして考えられる具体的な資料の例を掲載します。なお、これらの例は全てがそろっていないと裁判上十分な証拠とならないものではなく、あくまで有効と考えられる資料を列挙したものです。

○　いずれにせよ、証拠を収集するに当たっては、警察や弁護士等の専門家に相談した上で適切かつ迅速に責任追及の準備を進めることが望まれます。

※なお、秘密情報の侵害行為が、不正競争防止法に違反すると同時に、不正アクセス禁止法等の他の法令に抵触するケースもあり得ます。

営業秘密の要件該当性（特に秘密管理性）の証明に有効な資料例

- 情報の管理水準が分かる資料（就業規則、情報管理規程、管理状況に関する社内文書等）
- 漏えいが疑われる者と自社との間で交わされた秘密保持誓約書
- 情報の取扱いに関する社内研修等の実施状況に関する社内記録
- 特定の情報に対するマル秘マークの付記、アクセス制限、施錠等の情報の管理状況に関する社内記録（教育マニュアル等）
- 漏えいが疑われる者が、漏えいに係る情報が秘密であることを認識できたことを裏付ける陳述書（社内における実際の管理状況、口頭での情報管理に係る注意喚起の状況、示談文書等）

※　第３章参照

不正競争防止法違反のその他の要件該当性の判断に有効な資料例

- 漏えいが疑われる者の立場（アクセス権の保有者であったか、会議等で資料を配付された者であったか、外部者であるか）に関する社内記録

- 漏えいが疑われる者が自社従業員である場合には、どのような秘密保持に係る任務を負っていたかが分かる就業規則、秘密保持誓約書
- 漏えいが疑われる者が委託先である場合、委任契約書、秘密保持契約書
- 情報持出しの具体的行為態様が分かるアクセスログ、メールログ、入退室記録、複製のログ
- 漏えいが疑われる者の行為目的が窺える他社とのメールや金銭のやりとりに関する書面
- 情報漏えいの発覚の経緯を、社内調査等に基づき時系列的にまとめた文書

※　第３章参照

参考資料１

情報漏えい対策一覧

第３章３－４で紹介した情報漏えい対策の一覧表を作成しました。
講ずる対策を検討する際等にご活用下さい。

1. 従業員等に向けた対策

①「接近の制御」

ページ

a. ルールに基づく適切なアクセス権の付与・管理	~~38~~45
b. 情報システムにおけるアクセス権者のＩＤ登録	~~39~~46
c. 分離保管による秘密情報へのアクセス制限	~~41~~48
d. ペーパーレス化	~~45~~53
e. 秘密情報の復元が困難な廃棄・消去方法の選択	~~45~~53

②「持出し困難化」

【書類、記録媒体、物自体等の持出しを困難にする措置】

a. 秘密情報が記された会議資料等の適切な回収	~~47~~55
b. 秘密情報の社外持出しを物理的に阻止する措置	~~47~~56
c. 電子データの暗号化による閲覧制限等	~~48~~56
d. 遠隔操作によるデータ消去機能を有するＰＣ・電子データの利用	~~48~~56

【電子データの外部送信による持出しを困難にする措置】

e. 社外へのメール送信・Ｗｅｂアクセスの制限	~~48~~56
f. 電子データの暗号化による閲覧制限等（再掲）	~~49~~57
g. 遠隔操作によるデータ消去機能を有するＰＣ・電子データの利用（再掲）	~~49~~57

【秘密情報の複製を困難にする措置】

h. コピー防止用紙やコピーガード付の記録媒体・電子データ等により秘密情報を保管	~~50~~58
i. コピー機の使用制限	~~50~~58
j. 私物のＵＳＢメモリや情報機器、カメラ等の記録媒体・撮影機器の業務利用・持込みの制限	~~50~~58

【アクセス権変更に伴いアクセス権を有しなくなった者に対する措置】

k. 秘密情報の消去・返還	~~53~~61

③「視認性の確保」

【管理の行き届いた職場環境を整える対策】

a. 職場の整理整頓（不要な書類等の廃棄、書棚の整理等）	~~54~~62
b. 秘密情報の管理に関する責任の分担	~~55~~63
c. 「写真撮影禁止」、「関係者以外立入り禁止」の表示	~~55~~63

【目につきやすい状況を作り出す対策】

d. 職場の座席配置・レイアウトの設定、業務体制の構築	~~55~~63
e. 従業員等の名札着用の徹底	~~55~~63
f. 防犯カメラの設置等	~~56~~64
g. 秘密情報が記録された廃棄予定の書類等の保管	~~56~~65
h. 外部へ送信するメールのチェック	~~57~~65
i. 内部通報窓口の設置	~~57~~65

【事後的に検知されやすい状況を作り出す対策】

j. 秘密情報が記録された媒体の管理等	~~58~~66
k. コピー機やプリンター等における利用者記録・枚数管理機能の導入	~~58~~66
l. 印刷者の氏名等の「透かし」が印字される設定の導入	~~58~~66
m. 秘密情報の保管区域等への入退室の記録・保存とその周知	~~58~~66
n. 不自然なデータアクセス状況の通知	~~58~~66
o. ＰＣやネットワーク等の情報システムにおけるログの記録・保存とその周知	~~59~~67
p. 秘密情報の管理の実施状況や情報漏えい行為の有無等に関する定期・不定期での監査	~~60~~68

④「秘密情報に対する認識向上（不正行為者の言い逃れの排除）」

a. 秘密情報の取扱い方法等に関するルールの周知	~~61~~69
b. 秘密保持契約等（誓約書を含む）の締結	~~64~~72
c. 秘密情報であることの表示	~~66~~74

⑤「信頼関係の維持・向上等」

【秘密情報の管理に関する従業員等の意識向上】

a. 秘密情報の管理の実践例の周知	~~68~~76

b. 情報漏えいの事例の周知	~~68~~76
c. 情報漏えい事案に対する社内処分の周知	~~68~~76

【企業への帰属意識の醸成・従業員等の仕事へのモチベーション向上】

d. 働きやすい職場環境の整備	~~69~~77
e. 透明性が高く公平な人事評価制度の構築・周知	~~70~~77

2. 退職者等に向けた対策

①「接近の制御」

a. 適切なタイミングでのアクセス権の制限	~~72~~80

②「持出し困難化」

【退職予定者に対する特有の措置】

k. 社内貸与の記録媒体、情報機器等の返却	~~73~~81

【従業員等に向けた対策のうち退職者にも有効な措置（再掲　☞1. ②参照）】

（書類、記録媒体、物自体等の持出しを困難にする措置）

a. 秘密情報が記された会議資料等の適切な回収	~~47~~55
b. 秘密情報の社外持出しを物理的に阻止する措置	~~47~~56
c. 電子データの暗号化による閲覧制限等	~~48~~56
d. 遠隔操作によるデータ消去機能を有するＰＣ・電子データの利用	~~48~~56

（電子データの外部送信による持出しを困難にする措置）

e. 社外へのメール送信・Ｗｅｂアクセスの制限	~~48~~56
f. 電子データの暗号化による閲覧制限等（再掲）	~~49~~57
g. 遠隔操作によるデータ消去機能を有するＰＣ・電子データの利用（再掲）	~~49~~57

（秘密情報の複製を困難にする措置）

h. コピー防止用紙やコピーガード付の記録媒体・電子データ等により秘密情報を保管	~~50~~58
i. コピー機の使用制限	~~50~~58
j. 私物のＵＳＢメモリや情報機器、カメラ等の記録媒体・撮影機器の業務利用・持込みの制限	~~50~~58

③「視認性の確保」

【退職予定者に対する特有の措置】

q. 退職をきっかけとした対策の厳格化とその旨の周知	~~76~~84
r. ＯＢ会の開催等	~~76~~84

【従業員等に向けた対策のうち退職者にも有効な措置（再掲　☞1. ③参照）】

（管理の行き届いた職場環境を整える対策）

a. 職場の整理整頓（不要な書類等の廃棄、書棚の整理等）	~~54~~62
b. 秘密情報の管理に関する責任の分担	~~55~~63
c. 「写真撮影禁止」、「関係者以外立入り禁止」の表示	~~55~~63

（目につきやすい状況を作り出す対策）

d. 職場の座席配置・レイアウトの設定、業務体制の構築	~~55~~63
e. 従業員等の名札着用の徹底	~~55~~63
f. 防犯カメラの設置等	~~56~~64
g. 秘密情報が記録された廃棄予定の書類等の保管	~~56~~65
h. 外部へ送信するメールのチェック	~~57~~65
i. 内部通報窓口の設置	~~57~~65

（事後的に検知されやすい状況を作り出す対策）

j. 秘密情報が記録された媒体の管理等	~~58~~66
k. コピー機やプリンター等における利用者記録・枚数管理機能の導入	~~58~~66
l. 印刷者の氏名等の「透かし」が印字される設定の導入	~~58~~66
m. 秘密情報の保管区域等への入退室の記録・保存とその周知	~~58~~66
n. 不自然なデータアクセス状況の通知	~~58~~66
o. ＰＣやネットワーク等の情報システムにおけるログの記録・保存とその周知	~~59~~67
p. 秘密情報の管理の実施状況や情報漏えい行為の有無等に関する定期・不定期での監査	~~60~~68

④「秘密情報に対する認識向上（不正行為者の言い逃れの排除）」

a. 秘密保持契約等の締結	~~78~~86
b. 競業避止義務契約の締結	~~78~~86
c. 秘密情報を返還・消去すべき義務が生ずる場合の明確化等	~~79~~87

⑤「信頼関係の維持・向上等」

a. 適切な退職金支払い	~~80~~88
b. 退職金の減額などの社内処分の実施	~~80~~88

3. 取引先に向けた対策

①「接近の制御」

a. 取引先に開示する情報の厳選	~~84~~93
b. 取引先での秘密情報の取扱者の限定	~~86~~95

②「持出し困難化」

a. 秘密情報の消去・返還と複製できない媒体での開示	~~87~~96
b. 遠隔操作によるデータ消去機能を有するＰＣ・電子データの利用	~~87~~96

③「視認性の確保」

a. 秘密情報の管理に係る報告の確認、定期・不定期での監査の実施	~~88~~98
b. 取引先に自社サーバ═を使用させてログの保全・確認を実施	~~88~~98

④「秘密情報に対する認識向上（不正行為者の言い逃れの排除）」

a. 取引先に対する秘密保持義務条項	~~89~~99
b. 秘密情報であることの表示	~~90~~99
c. 具体的な秘密情報の取扱い等についての確認	~~90~~100
d. 取引先に対する秘密情報の管理方法に関する研修等	~~90~~100
e. 取引先とのやりとりの議事録等の保存	~~91~~101

⑤「信頼関係の維持・向上等」

a. 適正な対価の支払い等	~~92~~102
b. 契約書等における損害賠償や法的措置の記載	~~92~~102
c. 委託先に下請代金支払遅延等防止法が適用される場合の助言・支援	~~92~~102

4. 外部者に向けた対策

①「接近の制御」

a. 秘密情報を保管する建物や部屋の入場制限、書棚や媒体等のアクセス制限	~~95~~106
b. 外部者の構内ルートの制限	~~96~~107
c. ペーパーレス化	~~96~~107
d. 秘密情報の復元が困難な廃棄・消去方法の選択	~~97~~108
e. 外部ネットワークにつながない機器に秘密情報を保存する	~~97~~108
f. ファイアーウォール、アンチウィルスソフトの導入、ソフトウェアのアップデート	~~97~~108
g. ネットワークの分離（複数のＬＡＮを構築）	~~100~~112

②「持出し困難化」

a. 外部者の保有する情報端末、記録媒体の持込み・使用等の制限	~~101~~113
b. ＰＣのシンクライアント化	~~101~~113
c. 秘密情報が記載された電子データの暗号化	~~101~~113
d. 遠隔操作によるデータ消去機能を有するＰＣ・電子データの利用	~~101~~113

③「視認性の確保」

a. 「関係者以外立入り禁止」や「写真撮影禁止」の張り紙等	~~103~~115
b. 秘密情報を保管する建物・区域の監視	~~103~~115
c. 来訪者カードの記入、来訪者バッジ等の着用	~~105~~117

④「秘密情報に対する認識向上（不正行為者の言い逃れの排除）」

a. 「関係者以外立入り禁止」や「写真撮影禁止」の張り紙等（再掲）	~~106~~118
b. 秘密情報であることの表示	~~106~~118
c. 契約等による秘密保持義務条項	~~106~~118

参考資料２

各種契約書等の参考例

＜内容＞

各企業における秘密情報の管理・活用において参考となる各種契約書等の参考例を以下に例示しています。

一番重要なことは、就業規則や各種契約書等の**条項の内容（書きぶり）は、個別具体的事情を踏まえた上で書き分ける必要がある**ということです。

すなわち、以下はあくまで参考例の一つにすぎず、実際に社内向けの各種規定（就業規則や情報管理規程等）を策定したり、秘密保持誓約書や契約書等を作成したりする際には、業務の内容、実態、秘密情報の範囲や利用態様など個別具体的事情に応じ、自社にとってどのような規律を設けることが必要であるかとともに、負担となることはないかの観点から適切であるかについても十分な検討を行った上で、適宜、条項の取捨選択や内容の変更を継続的に行うことが必要です。

また、提示している参考例は書面作成を前提としていますが、デジタル化の進展に伴い、オンライン（ＰＤＦ、電子メールの提出・交換等）を活用して合意・意思確認をとり交わすことも考えられます。

さらに、企業間・企業内で取り交わされる場合以外にも、研究機関、大学等においても利用されることが考えられることから、当事者（差出人や宛先等）についても個別具体の状況に応じて適宜見直してとり交わすことが必要です。

なお、就業規則や情報管理規程等を策定する際には、労働基準法を始めとする労働関係法規や公益通報者保護法の趣旨等に反しないよう留意するとともに、秘密情報の利用形態を把握した上で、当該規程等が確実に履行可能なものとなるよう、労働者と協議するなどしてコンセンサスを形成することが有効です。

＜参考＞紹介する各規定・誓約書等の位置づけ

●企業等の内部関係に関する規定類

	採用 ⟶ 退職
就業期間中継続的かつ全員に関係	・秘密情報管理に関する就業規則（☞第１） ・秘密情報管理規程／秘密情報管理基準（☞第２）
特定の時期に取り交わすもの	・入社時の秘密保持誓約書（☞第３の 1.） ・プロジェクト参加時の秘密保持誓約書（☞第３の 2.） ・退職時の秘密保持誓約書（☞第３の 3.）

●外部見学の受入時に取り交わす秘密保持誓約書
他社による工場見学（☞第３の 4.）

●企業等が外部の取引先等と業務提携・委託等を行う場合（事前の協議時を含む）に取り交わす秘密保持誓約書等

事前の協議・検討の段階	本格的な（正式の）業務提携・委託等の段階
・業務提携の検討における秘密保持契約書（☞第４）	・取引基本契約書（製造請負契約）（☞第５） ・業務委託契約書（☞第６） ・共同研究開発契約書（☞第７）

第１　秘密情報管理に関する就業規則（抄）の例

第○条（服務規律）
１．従業員は、職場の秩序を保持し、業務の正常な運営を守るため、職務を遂行するにあたり、次の各号に定める事項を守らなければならない。
○　会社の施設、設備、製品、材料、電子化情報等を大切に取り扱い保管するとともに、会社の許可なく私的に使用しないこと。
○　（以下略）
２．従業員は、入退場に関し、次の各号に定める事項を守らなければならない。
○　警備員から所持品の検査を求められたときは、応じること。
○　会社の許可なく、書類や社品を会社外に持ち出さないこと。
○　会社の指示する手続を経て入退場すること。
○　日常携帯品以外の物品を携帯して入場しないこと。ただし、特に必要な場合は、会社の指示する手続をとること。
○　（以下略）
３．従業員は、従業員証を常時携帯し、入場のとき又は求められたときは、直ちに提示しなければならない。

第○条（入場制限・退場命令）（＊１）
従業員が次の各号の一に該当すると会社が認めた場合は、入場させず、又は退場させることがある。
○　入退場手続を行わないとき。
○　従業員証を所持していないとき。
○　警備員による所持品の検査に応じないとき。
○　業務外の事由で入場しようとするとき、又は終業後退場しようとしないとき。
○　（以下略）

第○条（遵守事項）
従業員は、次の各号に定める事項を守らなければならない。
○　従業員は、秘密情報管理規程に従い、秘密情報の取扱いを遵守しなければならない。
○　会社の内外を問わず、在職中、又は退職若しくは解雇によりその資格を失った後も、会社の秘密情報（＊２）を、不正に開示したり、不正に使用したりしないこと。
○　従業員は、在職中及び退職後【六ヶ月間／一年間／二年間】、会社と競合する他社に就職し、また競合する事業を営まないこと。（＊３）
○　退職時に、会社から貸与されたパソコンや携帯電話等、会社から交付を受けた資料（紙、電子データ及びそれらが保存されている一切の媒体を含む）を全て会社に返却すること。
○　会社の諸規則に違反する出版、又は講演などを行わないこと。
○　会社の許可なく、立入禁止区域に立ち入り、又は業務外の事由で自己の職場以外に立ち入り、若しくは会社の施設・敷地を利用しないこと。
○　会社の許可なく、会社の秘密情報を無断で社外に持ち出さないこと。（＊４）
○　業務上知った会社の秘密情報を使用し、在職中又は退職後においてその公表前に直接若しくは間接的に関連株式の売買を行わないこと。（＊４）
○　（以下略）

第○条（電子メール・インターネット等の適正利用）
１．従業員は、会社の電子メール、イントラネット及びインターネット（以下、総じて「インターネット等」という。）の利用に関し、次の事項を遵守して、パソコン、スマートフォン、携帯電話その他の情報通信機器（以下、総じて「端末」という。）を使用し、適切な情報ネットワーク環境の維持並びに社内情報の毀損及び漏えいの防止に努めなければならない。
○　会社が従業員に貸与した端末を業務以外の目的で使用しないこと。
○　私物の端末を会社の許可なく業務目的で使用しないこと。
○　会社が指定したウィルス対策ソフトを適正に運用、使用すること。
○　会社の内外を問わず、業務に使用する端末において、ファイル交換ソフトその他の情

報管理上問題が発生する可能性があるソフトウェア等又は業務に関係のないソフトウェア等をインストールしないこと。
○　会社の許可なく、私物のＵＳＢメモリ、ハードディスク等の記録媒体又は私物の端末を、業務に利用する端末に接続しないこと。
○　前項の許可を得て接続する場合は、アクセス権限のない者が操作できないようにパスワード設定をすること。
○　業務に関係のないウエッブサイトにアクセスしないこと。
○　（以下略）
２．会社は、インターネット等の利用の適正化を図るため、及び会社の秘密情報の管理を図るため、次の各号に定める事項その他必要と認める事項を講ずることができる。（＊５）（＊６）
○　必要に応じて、会社が従業員に貸与した端末若しくは会社のサーバ＝に保存されているデータを閲覧し、又は、情報を解析し、従業員ごとのインターネット等の利用履歴を確認すること。
○　必要に応じて、従業員が送受信した社用電子メールの内容を閲覧すること。
○　ウィルス感染等を予防するため、特定のウエッブサイトへのアクセスを制限すること。

第○条（防犯カメラの設置等）（＊７）
１．会社は、会社の防犯及び秘密情報の管理のため、次の各号に定める場所その他必要と認める場所に、防犯カメラを設置し、撮影することができる。
○　敷地出入口
○　サーバ＝ルーム出入口及び同ルーム内
○　（以下略）
２．会社は、次の各号に定める場合その他必要と認める場合には、防犯カメラにより撮影された画像又は動画の閲覧、保存等を行うことができる。
○　不法侵入者のあった場合
○　（以下略）

※なお、常時１０人以上の従業員を使用する使用者は、労働基準法（昭和２２年法律第４９号）第８９条の規定により、就業規則を作成し、所轄の労働基準監督署長に届け出なければならないとされています。就業規則を変更する場合も同様に、所轄の労働基準監督署長に届け出なければなりません。

（＊１）実効性の確保の観点から、このような条項を設けることが考えられますが、企業等の実態を踏まえて要否について検討することが望ましいでしょう。

（＊２）秘密情報のうち、特に営業秘密に属するものの範囲については、不正競争防止法上、営業秘密の要件の一つである秘密管理性の趣旨が、企業が秘密として管理しようとする対象（情報の範囲）が従業員等に対して明確化されることによって、従業員等の予見可能性、ひいては、経済活動の安定性を確保することにあることから、後掲の秘密情報管理規程等の中で、別途指定をする旨を就業規則内に定めることも考えられます。

（＊３）競業避止義務については、「ただし、会社が従業員と個別に競業避止義務について契約を締結した場合には、当該契約によるものとすること。」などとした上で、別途退職時に誓約書等で個別合意をすることが望ましいでしょう。（☞競業避止義務契約については、「参考資料５」を参照。）

（＊４）このような規定を入れる場合、秘密情報の具体的な情報取扱い方法については、情報管理規程でより詳細に定めることが考えられます。（☞「情報管理規定」については、第２を参照。）

（＊５）本項を社内規定に導入するにあたっても、案を策定し、事前に社内に徹底することが必要です。
~~詳細は、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（平成２６年１２月１２日厚生労働省・経済産業省告示第４号）」をご覧ください。~~
~~http://www.meti.go.jp/policy/it_policy/privacy/downloadfiles/1212guideline.pdf~~

（＊６）就業規則以外で定めを置く場合を含め、本項に定めるような事項を実施するにあたっては、あらかじめ従業員に通知し、必要に応じて協議を行うことが望ましいと考えられます。また、その実施に当たっての責任者及びその権限も定めておくことが重要です。加えて、実施が適正に行われているかを監査又は確認することも重要です。

（＊７）本項に定めるような防犯カメラに関する事項ついては、あらかじめ従業員に通知し、必要に応じて協議を行った上で、このような条項を入れることが考えられます。また、実際に防犯カメラを設置している場所に、「防犯カメラ作動中」という標識等を立てることも考えられます。また、防犯カメラの設置等の責任者及びその権限も定めておくことが重要です。加えて、防犯カメラの設置等が適正に行われているかを監査又は確認することも重要です。

第２　秘密情報管理規程・秘密情報管理基準の例

（第３章３－３（２）参照）

１．秘密情報管理規程の例

第１章　総則

第１条（目的）

この規程は、情報の管理に関して必要な事項を定め、もって秘密情報の適正な管理及び活用を図ることを目的とする。

第２条（適用範囲）

この規程は、役員及び従業員（以下「従業員等」という。）に適用されるものとする。（＊１）

第３条（定義）

この規程において各用語の定義は、次に定めるところによる。

① 「秘密情報」とは、会社が保有する情報のうち、第七条の規定により、秘密として保持すべきと決定した情報、又は同条の規定による秘密として保持すべきと決定をしていない情報であって、当該情報の内容、性質及び管理態様等から会社が秘密であることを認識できるもので不正競争防止法第２条第６項に規定する営業秘密に該当する情報をいう。（＊２）

② 「文書等」とは、文書、図画、写真、ストレージ（フラッシュメモリ（ＳＳＤ、ＵＳＢメモリ、ＳＤカードなど）、光学ディスク（ＣＤ、ＤＶＤ、ブルーレイディスクなど）、磁気ディスク（ハードディスクなど以下「ストレージ」という。）等の記録媒体に情報を記載又は記録したものをいう。

③ 「電子化情報」とは、ストレージやオンラインストレージ（クラウドサービス等）に電磁的に記録される情報であって、情報システムによって処理が可能な形態にあるものをいう。

④ 「物件」とは、物品、製品、設備その他の文書等以外のものをいう。

第４条（秘密情報の分類）

秘密情報として管理するため、次のとおり分類を定める。（＊３）

① 極秘　　これを他に漏らすことにより会社が極めて重大な損失若しくは不利益を受ける、又はそのおそれがある秘密情報であり、原則として指定された者以外には開示してはならないもの。

② 社外秘　　極秘以外の秘密情報であり、原則として社内の者以外には開示してはならないもの。

③ （以下略）

第２章　秘密情報の管理体制

第５条（管理責任者）

１．会社の秘密情報の管理を統括するため、秘密情報の管理に係る統括責任者（以下「統括責任者」という。）を置く。統括責任者は、役員の中から取締役会の指名により決定する。

２．各部門長及び各部門内の業務分掌単位の長は、それぞれ秘密情報管理責任者（以下「管理責任者」という。）として、本規程に定めるところにより、所管する部門及び業務分掌単位における秘密情報の管理の任にあたる。

第６条（秘密情報管理委員会）

１．本規程の改定並びに第四条に規定する秘密情報の分類に応じた情報漏えい対策を定める規程（以下「秘密情報管理基準」という。）の策定及び改定を行うため（＊４）、秘密情報管理委員会（以下「委員会」という。）を設ける。

２．委員会は、統括責任者を委員長とし、各部門長を委員とする。

３．委員会は、第十四条に定める監査結果を受け、本規程及び秘密情報管理基準の改定の必要性について検討を行い、その結果をふまえて必要な措置を講じるものとする。

４．委員会の運用に関する細則（以下、「委員会運用細則」という。）は、別途定める（＊５）。

第７条（指定）
１．管理責任者は、別途定めるところにより、会社が保有する情報について、秘密情報として指定するとともにその秘密情報の分類を指定し、その秘密保持期間及びアクセスすることができる者（以下「アクセス権者」という。）の範囲を特定するものとする。
２．管理責任者は、前項により指定された情報を含む文書等、電子化情報及び物件に、秘密情報である旨を明示する。
３．管理責任者は、第一項により指定された情報について、日時の経過等により秘密性が低くなり、又は秘密性がなくなった場合においては、その都度、秘密情報の分類の変更又は秘密情報の指定の解除を行うものとする。

第８条（秘密情報の取扱い）
従業員等は、本規程及び秘密情報管理基準に従い秘密情報を取り扱わなければならない。（＊６）

第３章　従業員等

第９条（申告）
従業員等は、業務の過程で秘密情報として指定された情報の範囲に含まれるものを取得し、又は創出した場合は、遅滞なくその内容を管理責任者に申告するものとし、管理責任者は第七条第一項に従い秘密情報の分類を指定するものとする。

第１０条（秘密保持義務）
１．従業員等は、管理責任者の許可なく、秘密情報をアクセス権者以外の者に開示してはならない。
２．従業員等は、管理責任者の許可なく、秘密情報を指定された業務以外の目的で使用してはならない。

第１１条（誓約書等）
１．従業員等は、秘密情報管理基準に定める様式により、秘密保持を誓約する書面を管理責任者に提出するものとする。
２．入社前に他の職場において第三者の秘密情報に接していたと判断される従業員等は、配属先の管理責任者が必要と認めるときは、入社時に管理責任者又は統括責任者による面接を受け、個別の誓約書その他秘密情報管理基準に定める書面を会社に提出するものとする。

第１２条（退職者）
１．従業員等は、その身分を失った後においても、第十条第一項に定める秘密保持義務を遵守しなければならない。
２．管理責任者は、従業員等が退職する際、当該従業員等が在職中に知り得た秘密情報を特定するなど、当該従業員等が負う秘密保持義務等の内容を確認するものとする。
３．従業員等は、退職時に、文書等又は物件を社外に持ち出してはならず、また自己の保管する文書等又は物件をすべて会社に返還しなければならない。
４．従業員等は、退職時に、自己の文書等に記録等された秘密情報を消去するとともに、消去した旨の誓約書（自己の文書等に秘密情報が記録等されていないときは、その旨の誓約書）を管理責任者に提出しなければならない。
５．従業員等は、退職後において、前二項に定める文書等、物件、又は秘密情報のうちで、過失により返還又は消去していないものを発見した場合には、速やかに前二項に定める措置を講じるものとする。

第１３条（教育）
管理責任者は、従業員等に対してこの規程の内容を周知徹底させるため適切な教育を行い、従業員等の秘密情報の管理に関する意識の高揚、維持に努めるものとする。

第１４条（監査）
１．管理責任者は、本規程を遵守し、秘密情報を管理するため、所管する部門や業務分掌単位における監査を行い、その結果を統括責任者に報告するものとする。

２．従業員等は、前項の監査に誠実に協力しなければならない。

第４章　社外対応

第１５条（秘密情報の開示を伴う契約等）

アクセス権者は、人材派遣会社、委託加工業者、請負業者等の第三者に対し、会社の業務に係る製造委託、業務委託等をする場合、又は、実施許諾、共同開発その他の秘密情報の開示を伴う取引等を行う場合、当該会社との契約において相手方に秘密保持義務を課すほか、秘密保持に十分留意するものとする。

第１６条（第三者の情報の取扱い）

１．従業員等は、第三者から情報の開示を受ける場合、当該情報を秘密として取り扱うべきか否か、及び当該情報の開示につき、当該第三者が正当な権限を有することの確認をしなければならない。

２．前項に定める場合において、従業員等は、当該第三者が正当な権限を有しないとき又は正当な権限を有するか否かにつき疑義のあるときには、当該情報の開示を受けてはならない。

３．従業員等は、第一項により開示を受ける情報については、当該第三者との間で、その使用又は開示に関して会社が受ける制約条件を明確にしなければならない。

４．第一項により開示を受けた情報を使用又は開示する場合は、前項の会社が受ける制約条件に従うものとし、当該情報は会社の秘密情報と同等に取り扱うものとする。

第１７条（外来者・見学）

事業場長は、必要に応じ、統括責任者の同意を得て、外来者への応対、施設の見学等に関する運用手続（秘密保持契約の締結、立入禁止区域の設定その他の秘密保持のための措置に関する記載を含む。）を定めるものとする。

第５章　雑則

第１８条（罰則）

従業員等が故意又は重大な過失により、この規程に違反し、就業規則に定める各種懲戒に該当する場合は、同規則により措置される。

（＊１）自社に派遣されている派遣労働者や自社内において勤務する委託先の労働者については、自社との間に、雇用契約等直接の契約関係が存在しないので、第１５条に例示したように、派遣元企業や委託先企業との間で、秘密保持契約等を締結し、派遣元企業や委託先企業を介して、自社における秘密情報の取扱いを遵守してもらう形になります。

（＊２）本規定の対象となる秘密情報について、原則的には第７条の規定に基づいて管理責任者により指定されたものが該当することになるものの、管理責任者が指定をし忘れた場合に備えて、客観的に会社が秘密管理しようとしている情報と認識可能な不正競争防止法の営業秘密に該当するような情報についても、秘密情報に含まれうることを明らかにする観点から、「又は」以下の記載を入れています。この点について、対象範囲についてシンプルに判断できるように、指定された情報のみを対象としたい場合には、この部分は削除することも考えられます。

（＊３）「役員外秘」、「部外秘」、「社外秘」等の、アクセスできる者の範囲が認識できるような名称の分類とすることも考えられます。もしくは、秘密情報が記録された媒体等に、アクセスできる者の範囲や当該情報の取扱い方法等とともに、秘密情報の分類の名称を表示することも考えられます。

（＊４）対策の詳細については、「３－４　具体的な情報漏えい対策例」をご参照ください。

（＊５）委員会の運用細則において、誰が情報の評価を行い、誰がどのような観点から情報の利用態様を分析するか、どのようにして秘密情報を分類するか等の決定手続を定めることが考えられます。

（＊６）秘密情報管理基準の詳細については、「２．秘密情報管理基準の例」を参考にしてください。

２．秘密情報管理基準の例

※情報管理基準は、各社が選択した漏えい対策等を踏まえて定めることになります。情報管理基準のイメージ（例）は以下の通りです。

※なお、この例では、秘密情報が「極秘」と「対外秘」の２分類あり、「極秘」は社内でアクセスできる者を限定して、情報を施錠管理し、複製や社外への持出しを原則的に禁止する情報、「対外秘」は対外的に秘密として保持する情報であり、複製や社外への持出しは必要最低限にすることが求められる情報と想定し、本基準例を作成しています。

※本基準例の用語は、前掲の秘密情報管理規程の例に則っています。

秘密情報管理基準（例）

１．極秘情報の取扱い

極秘情報を含む文書等、電子化情報及び物件の取扱いは、次のとおりとする。

(1) 表示

・ 極秘情報が記録された文書等には、「極秘」及びアクセス権の範囲（例えば、「役員限り」、「製造部限り」等）を表示する。
・ 電子化情報自体が極秘情報である場合は、電子文書そのもの及びファイル名に「極秘」及びアクセス権の範囲を表示する。
・ 物件自体が極秘情報である場合は、管理責任者が物件リストを作成してアクセス権者において共有し、当該物件の保管場所に「極秘」及び「無断持出禁止」の表示を行う。

(2) 保管

・ 極秘情報が記録された文書等を保管する場合には、他の文書等と区別して、保管庫に施錠して保管する。当該保管庫の鍵は、管理責任者が管理する。
・ 電子化情報自体が極秘情報である場合に、当該電子化情報をＰＣ等の情報システム機器に保管する場合には、暗号化し、外部ネットワークに接続しないＰＣ等に保管する。当該ＰＣ等を保管する区域は施錠管理する。当該区域の鍵は管理責任者が管理する。

(3) 複製

・ 極秘情報の複製・印刷は、管理責任者以外はすることができない。
・ 電子化情報自体が極秘情報である場合は、当該電子化情報を保管するＰＣ等が設置された区域には私物の電子媒体（ＵＳＢメモリ等）、カメラ、スマートフォン等の機器の持込みを禁止する。また当該電子化情報を保管するＰＣはＵＳＢ等の差込口を無効化したものを使用する。
・ 極秘情報である電子化情報の全部又は一部については、印刷、転記、ＵＳＢメモリ等の記録媒体への書込み及びメールへの添付ができない設定とする。

(4) 閲覧

・ 極秘情報が記録された文書等をアクセス権者以外の者に閲覧させてはならない。
・ 極秘情報が記録された文書等を他のアクセス権者に閲覧させるにあたっては、管理責任者の許可を得なければならない。
・ 極秘情報である電子化情報へのアクセスはアクセス権者のＩＤからのみ可能とする。閲覧の際は他者に読み取られないように注意する。
・ 管理責任者は、閲覧者氏名、日時、閲覧した情報の内容等を記録する。
・ テレワークの実施に際して、会社の外で極秘情報を閲覧する場合にも、この基準の内容に留意し、周囲の環境に十分に注意して対応するものとする。

(5) 配布

・ 極秘情報が記録された文書等を会議等で資料として配布する場合は、通し番号を付し、会議後回収する。

(6) 社外への持出し

・ 極秘情報が記録された文書等、電子化情報及び物件を持ち出すに当たっては、管理責

任者の許可を得なければならない。
・ 管理責任者の許可を得て文書等を社外に持ち出す場合（テレワーク等の正当な業務の実施のため持ち出す場合を含む。）には（電子化情報は暗号化するなどの措置を講じた上で）取扱者自らが携行し、滞在先では保管庫に保管する等紛失しないよう適切な措置を講ずる。
・ 管理責任者の許可を得て電子化情報を外部に電子メール等で送信する場合には、暗号化等の適切な措置を行う。
(7) 第三者への提供
・ 原則として極秘情報の提供は認めない。
・ ただし、取引先等の第三者に対し、極秘情報を開示する必要が生じた場合は、管理責任者の許可を得なければならない。極秘情報の開示、提供した極秘情報の管理等については、管理責任者の指示の下で行う。
(8) 廃棄
・ 極秘情報の利用者は、無断で、極秘情報が記録された文書等及び物件の廃棄並びに電子化情報の消去をすることができない。
・ 極秘情報が記録された文書等及び物件の廃棄並びに電子化情報の消去にあたっては、管理責任者の管理の下行う。
・ 管理責任者は、電子化情報をフォルダ等から消去する際は、第三者が残留情報を読みとることができないように情報を消去しなければならない。
・ 管理責任者は、極秘情報が記録された文書等及び物件を廃棄する際は、裁断、焼却、溶解等、第三者が残留情報を読みとることができないよう適切な方法により廃棄が行われるようにしなければならない。文書等が電子媒体(ＵＳＢメモリ、ＰＣ等)である場合には、第三者が残留情報を読み取ることができないよう電子化情報を消去した上で廃棄しなければならない。

２．対外秘情報の取扱い
対外秘情報を含む文書等、電子化情報及び物件の取扱いは、次のとおりとする。
(1) 表示
・ 対外秘情報が記録された文書等には、「対外秘」と表示する。
・ 電子化情報自体が対外秘情報である場合には、電子文書そのもの及びファイル名に「対外秘」と表示する。
・ 物件自体が対外秘情報である場合は、管理責任者が物件リストを作成して社内で共有し、その物件の保管場所に「対外秘」及び「無断持出禁止」の表示を行う。
(2) 保管
・ 対外秘情報が記録された文書等を保管する場合には、他の文書等と区別して保管する。
・ 電子化情報自体が対外秘情報である場合に、当該電子化情報をＰＣ等の情報システム機器に保管する場合には、暗号化し、分離されたフォルダ等に保管する。
・ 対外秘情報をＵＳＢメモリ等の記録媒体等に保管する場合には、暗号化する。
(3) 複製
・ 対外秘情報の複製・印刷・撮影は、業務上やむを得ない場合を除いて、行ってはならない。
・ 対外秘情報の複製・印刷は、外部者に読み取られないよう使用後ただちに回収する。
(4) 閲覧
・ 対外秘情報が記録された文書等を外部者に閲覧させてはならない。
・ 対外秘情報である電子化情報の画面表示は、外部者に読み取られないように注意する。
・ テレワークの実施に際して、会社の外で対外秘情報を閲覧する場合にも、この基準の内に留意し、周囲の環境に十分注意して対応するものとする。
(5) 配布
・ 対外秘情報が記録された文書等の配布・送付に当たっては、文書への「対外秘」表示、取扱い方法についての説明、資料の回収等、社外に対外秘情報が漏えいしないよう、必要な措置を講ずる。
・ 対外秘情報である電子化情報をメールで送信する場合には、暗号化した上で送信する。
(6) 社外への持出し

・　対外秘情報の記録された文書等及び物件を持ち出す必要がある場合には（電子化情報は暗号化するなどの措置を講じた上で）取扱者自らが携行し、滞在先では保管庫に保管する等紛失しないよう適切な措置を講ずる。
・　対外秘情報が記録された文書等のうち、ＰＣやＵＳＢメモリ等の電子媒体を持出す場合（テレワーク等の正当な業務の実施のため持ち出す場合を含む。）には、保管された電子化情報を暗号化する。
・　対外秘情報である電子化情報を外部に電子メール等で送付する場合には、暗号化等の適切な措置を行う。

(7) 第三者への提供

・　取引先等の第三者に対し、対外秘情報を開示する必要が生じた場合は、必要最小限の開示内容を精査し、対外秘情報であることを示す表示をして、管理責任者の許可を得なければならない。従業員は、当該取引先等の第三者による秘密保持誓約署の提出がなされたもとで、対外秘情報の開示、提供を行う。また、開示・提供した対外秘情報の管理等については、管理責任者の指示の下で行い、開示・提供の必要性がなくなった場合又は開示する取引先等の第三者が交代した場合は、全ての回収を確認するとともに、経緯を管理責任者に提出する。

(8) 廃棄

・　対外秘情報である電子化情報をフォルダ等から消去する際は、管理責任者が指定した方法により、第三者が残留情報を読みとることができないように情報を消去しなければならない。
・　対外秘情報が記録された文書等及び物件を廃棄する際は、管理責任者によって指定された場所に持込まなければならない。文書等が電子媒体である場合には、第三者が残留情報を読み取ることができないよう電子化情報を消去した上で指定された場所に持ち込まなければならない。
・　管理責任者は、指定された場所に持込まれた文書等及び物件を廃棄する際は、裁断、焼却、溶解等、第三者が残留情報を読みとることができないよう適切な方法により廃棄が行われるようにしなければならない。文書等が電子媒体である場合には、対外秘情報が消去されていることを確認の上、適切な廃棄が行われるようにしなければならない。

第３　秘密保持誓約書の例

※秘密保持誓約書（契約）といっても様々なものが存在します。以下では、契約の相手方（従業員等の内部関係者向け、取引相手・見学者等の外部の関係者向け）や秘密保持契約締結のタイミング（入社時・プロジェクト開始／参加時・退職時、見学受け入れ時、契約の事前協議段階、契約締結時）に応じて、いくつかの例を掲載します。

１．従業員等の入社時

秘密保持に関する誓約書

この度、私は、貴社に採用されるにあたり、下記事項を遵守することを誓約いたします。

記

第１条（在職時の秘密保持）
貴社就業規則及び貴社秘密情報管理規程を遵守し、次に示される貴社の秘密情報（＊１）について、貴社の許可なく、不正に開示又は不正に使用しないことを約束いたします。
① 製品開発に関する技術資料、製造原価及び販売における価格決定等の貴社製品に関する情報
② （以下略）

第２条（退職後の秘密保持）
前条各号の秘密情報については、貴社を退職した後においても、不正に開示又は不正に使用しないことを約束いたします。退職時に、貴社との間で秘密保持誓約書を作成することに同意いたします。

第３条（損害賠償）
前二条に違反して、第一条各号の秘密情報を不正に開示又は不正に使用した場合、法的な責任を負担するものであることを確認し、これにより貴社が被った一切の被害を賠償することを約束いたします。

第４条（第三者の秘密情報）（＊２）
１．第三者の秘密情報を含んだ媒体（文書、図画、写真、ＵＳＢメモリ、ＤＶＤ、ハードディスクドライブその他情報を記載又は記録するものをいう。）を一切保有しておらず、また今後も保有しないことを約束いたします。
２．貴社の業務に従事するにあたり、第三者が保有するあらゆる秘密情報を、当該第三者の事前の書面による承諾なくして貴社に開示し、又は使用若しくは出願（以下「使用等」という。）させない、貴社が使用等するように仕向けない、又は貴社が使用等しているとみなされるような行為を貴社にとらせないことを約束いたします。

第５条（第三者に対する守秘義務等の遵守）（＊２）
貴社に入社する前に第三者に対して守秘義務又は競業避止義務を負っている場合は、必要な都度その旨を上司に報告し、当該守秘義務及び競業避止義務を守ることを約束いたします。

第６条（創出等した情報の報告及び帰属）（＊３）
１．貴社により秘密情報として指定された情報の範囲に含まれるものについて、その創出又は取得に関わった場合には、遅滞なくその内容を貴社に報告します。
２．前項の情報については、私がその創出又は取得に携わった場合であっても、貴社業務上作成したものであることを確認し、当該情報の帰属が貴社にあることを確認いたします。また当該情報について私に帰属する一切の権利を貴社に譲渡し、その権利が私に帰

属する旨の主張をいたしません。

以上

令和　　年　　月　　日
株式会社＿＿＿＿＿＿
代表取締役（社長）＿＿＿＿＿＿殿

住　所　＿＿＿＿＿＿＿＿＿＿＿＿
＿＿＿＿＿＿＿＿＿＿＿＿
氏　名　＿＿＿＿＿＿＿＿＿＿＿＿

（＊１）情報管理規程等において、別途秘密情報の範囲が指定されている場合には、第１条各号に代わり、当該規程等を用いることも考えられます。

（＊２）特に転職者の入社時などに、他社が保有する重要情報を意図せず侵害することを防止するという観点から、従前の勤務先で課せられた秘密保持義務（や競業避止義務）の内容について採用の過程で十分に確認をするとともに、入社に際して確認を図る観点から、このような条項を設けることが望ましいでしょう。

（＊３）秘密情報の帰属については様々な考え方がありますが、このような条項を設けることも考えられます。ただし、本誓約書について秘密保持に関係する事項に特化させたい場合、就業規則やプロジェクトごとに作成される職務発明や職務著作などの成果の帰属・取扱いに関する取り決めが作成されるような場合は、必ずしも本誓約書に規定する必要はありません。

２．従業員等のプロジェクト参加時

秘密保持に関する誓約書

年　　月　　日

＿＿＿＿＿株式会社
＿＿＿＿＿工場
＿＿＿＿＿殿

プロジェクト名　＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

現 住 所　＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿
氏　　名　＿＿＿＿＿＿＿＿＿＿
生年月日　＿＿＿＿年＿＿月＿＿日生

私は、上記プロジェクト（以下「本プロジェクト」という。）に参画するにあたり、秘密情報の取扱いに関し、就業規則、情報管理規程、及びすでに提出した誓約書（ただし、これらのうち私に適用されないものがある場合はそれを除く。）に基づく義務を負うことを確認し、加えて以下を誓約いたします。

記

第１条（秘密保持の誓約）
会社の許可なく、本プロジェクトに関して会社が秘密情報として指定した情報（以下「対象秘密情報」という。）を、本プロジェクトの参画者以外の者に対し開示し、又は本プロジェクト遂行の目的以外に使用しないことを約束いたします。（＊１）

第２条（プロジェクト終了後の秘密保持等）
１．対象秘密情報を、公知になったものを除き、本プロジェクト終了後（退職後も含む。）も、不正に開示又は不正に使用しないことを約束いたします。
２．本プロジェクトを終了するとき、本プロジェクトを担当しなくなったとき、又は会社による要求があるときには、対象秘密情報が記録等された会社の文書等（文書、図画、写真、ＵＳＢメモリ、ＤＶＤ、ハードディスクドライブその他の情報を記載又は記録するものをいう。以下同じ。）又は物件であって自己の保管するものを、遅滞なくすべて会社に返還し、その旨書面にて報告いたします。
３．前項に定める場合において、対象秘密情報が自己の文書等に記録等されているときには、当該情報を消去するとともに、消去した旨（自己の文書等に対象秘密事項が記録等されていないときは、その旨）、書面にて報告いたします。

第３条（第三者に対する守秘義務の遵守）
第三者に対して守秘義務を負っている情報については、本プロジェクトにおいて知り得たかそれ以前から知っていたかにかかわらず、その守秘義務を遵守することを約束いたします。

第４条（情報の帰属）（＊２）
本プロジェクトの業務の成果である情報は会社に帰属することを確認し、異議を述べません。

以上

（＊１）秘密保持の対象として指定すべき情報については、プロジェクトの進行等に伴い、その範囲や内容がより特定することが考えられることから、プロジェクトの進行途中又は終了時において、適宜情報の範囲・内容の特定をより具体化することが望ましいです。

（＊２）秘密情報の帰属に関し、このような条項を設けることも考えられます。ただし、本誓約書について秘密保持に関係する事項に特化させたい場合、就業規則やプロジェクトごとに作成される成果の帰属・取扱いに関する取り決めが作成されるような場合は、本誓約書に規定する必要はありません。

３．従業員等の退職時

秘密保持誓約書

私は、令和　　年　　月　　日付にて、一身上の都合により、貴社を退職いたしますが、貴社秘密情報に関して、下記の事項を遵守することを誓約いたします。

記

第１条（秘密保持の確認）
私は貴社を退職するにあたり、次に示される貴社の秘密情報に関する一切の資料、媒体等（文書、図画、写真、ＵＳＢメモリ、ＤＶＤ、ハードディスクドライブその他情報を記載又は記録するものをいう。）について、原本はもちろん、そのコピー及び関係資料等を、直ちに貴社に返還、消去又は廃棄し、その情報を自ら保有していないことを確認いたします。
①　製品開発に関する技術資料、製造原価及び販売における価格決定等の貴社製品に関する情報
②　（以下略）

第２条（退職後の秘密保持の誓約）
貴社に対して誓約した入社時の「秘密保持に関する誓約書」に記載された事項及び就業規則その他の貴社の諸規則に定めのある事項のうち、退職後も義務を負う事項についてはこれを正しく認識し、退職後も誠実に遵守すること。特に、前条各号に掲げる貴社の秘密情報を、貴社退職後においても、不正に開示又は不正に使用しないことを約束いたします。

第３条（秘密情報の帰属）（＊１）
第一条各号の秘密情報は貴社に帰属することを確認いたします。また当該秘密情報に関し、私に帰属する一切の権利を貴社に譲渡し、貴社に対し当該秘密情報が私に属している旨の主張を行いません。

第４条（契約の期間、終了）
本契約は、○○年間有効とします。ただし、第一条各号の秘密情報が公知となった場合は、その時点をもって、当該公知となった秘密情報についての本契約第二条の義務は終了することとします。

（＊２）

以上

令和　　年　　月　　日
株式会社＿＿＿＿＿＿
代表取締役（社長）＿＿＿＿＿＿殿

住　所　＿＿＿＿＿＿＿＿＿＿
＿＿＿＿＿＿＿＿＿＿
氏　名　＿＿＿＿＿＿＿＿＿＿

（＊１）秘密情報の帰属に関して、このような条項を設けることも考えられます。ただし、本誓約書について秘密保持に関係する事項に特化させたい場合、就業規則やプロジェクトごとに作成される成果の帰属・取扱いに関する取り決めが作成されるような場合は、必ずしも本誓約書に規定する必要はありません。

（＊２）競業避止義務に関して、個別の誓約書・同意書等を取り交わすことのほか、秘密保持義務誓約書の中で以下のような規定（▲）を設けることも考えられます。ただし、退職後の競業避止義務については、その有効性が認められるためには、企業側の守るべき利益の存在を前提として、退職する従業員の地位、地域的限定、競業避止義務の存続期間、禁止される競業行為の範囲、代償措置等について、具体的事情の下で合理的なものとなるように考慮する必要があるものと考えられます。

また、競業避止義務を課す場合に補償手当を支給するときには、以下のような規定（■）を設けることも考えられます。

第▲条(競業避止義務の確認)
貴社を退職するにあたり、退職後【六ヶ月間／一年間】、貴社からの許諾がない限り、次の行為をしないことを誓約いたします。
① 貴社で従事した○○の開発に係る職務を通じて得た経験や知見が貴社にとって重要な企業秘密及びノウハウであることに鑑み、当該開発及びこれに類する開発に係る職務を、貴社の競合他社（競業する新会社を設立した場合にはこれを含む。以下同じ。）において行うこと
② 貴社で従事した○○に係る開発及びこれに類する開発に係る職務を、貴社の競合他社から契約の形態を問わず、受注又は請け負うこと

第■条（補償手当）
私は、本誓約書の遵守のため、貴社給与及び退職金のほか、補償手当○○○円の交付を受けたことを確認いたします。

４．他社による工場見学時

（製造業者が、自社の工場を他社の従業員に見学させる際に用いる誓約書の例）

秘密保持誓約書

令和＿＿年＿＿月＿＿日

＿＿＿＿＿＿株式会社
＿＿＿＿＿＿工場
＿＿＿＿＿＿殿

株式会社＿＿＿＿＿＿
代表取締役＿＿＿＿＿＿

この度、当社の従業員＿＿＿＿＿＿が令和＿＿年＿＿月＿＿日、貴社○○工場における工程を見学させていただくにあたり、下記の事項を厳守することを誓約いたします。

記

第１条（秘密保持の誓約）
当社は、貴工場の見学に際し、貴社が当社に開示し、かつ開示の際に秘密である旨明示した一切の情報（以下「秘密情報」といいます。）（＊１）について、厳に秘密を保持するものとし、事前に貴社の書面による承諾を得た場合を除き、第三者に秘密情報を開示いたしません。ただし、当社が書面によってその根拠を立証できる場合に限り、以下の情報は秘密情報の対象外とさせていただきます。
① 貴社から開示を受けたときに既に当社が保有していた情報
② 貴社から開示を受けたときに既に公知であった情報
③ 貴社から開示を受けた後、当社の責めに帰し得ない事由により公知となった情報

第２条（承諾を得ない使用の禁止）
当社は、貴社から開示された秘密情報を、貴社の事前の書面による承諾を得た場合を除き、使用いたしません。

第３条（従業員に対する開示）
工場見学で得た情報を当社内で開示する場合には、必要最小限の範囲に留めます。この場合、当社は、秘密情報を知り得た当社の従業員（貴工場を見学した従業員も含む。）について、その在職中及び退職後○年間は、本誓約書と同趣旨の義務を課すこととさせていただきます。

第４条（損害賠償）
当社、当社の従業員又は当社の元従業員が、本誓約書に記載する事項のいずれかに違反したことにより、貴社に損害が生じた場合には、当社が一切の責任を負うものとし、貴社の被った一切の損害を賠償いたします。

以上

（＊１）秘密保持の対象とする情報の定義と呼称（例えば、「企業秘密」、「秘密情報」など。）については、当該開示の趣旨や取引慣行等に応じて様々なものが考えられます。なお、上記では「一切の情報」と書いていますが、秘密保持の対象となる情報の特定ができる場合には、別紙でその内容をリスト化するなど、できる限り具体的に行うことが重要です。

第４　業務提携・業務委託等の事前検討・交渉段階における秘密保持契約書の例

（他社との業務提携・業務委託等の取引を本格化させるに際して、その事前検討にあたり、当該企業同士が交渉で秘密情報を取り交わす際に用いる秘密保持契約書の例（＊１））

秘密保持契約書

＿＿＿＿株式会社（以下「甲」という。）と＿＿＿＿株式会社（以下「乙」という。）とは、＿＿＿＿について検討するにあたり（以下「本取引」という。）、甲又は乙が相手方に開示する秘密情報の取扱いについて、以下のとおりの秘密保持契約（以下「本契約」という。）を締結する。

第１条（秘密情報）（＊２）（＊３）

１．本契約における「秘密情報」とは、甲又は乙が相手方に開示し、かつ開示の際に秘密である旨を明示した技術上又は営業上の情報、本契約の存在及び内容その他一切の情報をいう。ただし、開示を受けた当事者が書面によってその根拠を立証できる場合に限り、以下の情報は秘密情報の対象外とするものとする。

①　開示を受けたときに既に保有していた情報

②　開示を受けた後、秘密保持義務を負うことなく第三者から正当に入手した情報

③　開示を受けた後、相手方から開示を受けた情報に関係なく独自に取得し、又は創出した情報

④　開示を受けたときに既に公知であった情報

⑤　開示を受けた後、自己の責めに帰し得ない事由により公知となった情報

２．前項本文の情報のうち、甲が乙に秘密である旨を指定して開示する情報は別紙１を、また乙が甲に秘密である旨を指定して開示する情報は別紙２を含むものとする。なお、別紙１及び別紙２は甲と乙とが協力し、常に最新の状態を保つべく適切に更新するものとする。（＊４）

３．甲又は乙が口頭により相手方から開示を受けた情報については、改めて相手方から当該事項について記載した書面の交付を受けた場合に限り、相手方に対し本規程に定める義務を負うものとする。（＊５）

４．口頭、映像その他その性質上秘密である旨の表示が困難な形態又は媒体により開示、提供された情報については、開示者が相手方に対し、秘密である旨を開示時に伝達し、かつ、当該開示後〇日以内に当該秘密情報を記載した書面を秘密である旨の表示をして交付することにより、秘密情報とみなされるものとする。（＊５）

第２条（秘密情報等の取扱い）

１．甲又は乙は、相手方から開示を受けた秘密情報及び秘密情報を含む記録媒体若しくは物件（複写物及び複製物を含む。以下「秘密情報等」という。）の取扱いについて、次の各号に定める事項を遵守するものとする。

①　情報取扱管理者を定め、相手方から開示された秘密情報等を、善良なる管理者としての注意義務をもって厳重に保管、管理する。

②　秘密情報等は、本取引の目的以外には使用しないものとする。

③　秘密情報等を複製する場合には、本取引の目的の範囲内に限って行うものとし、その複製物は、原本と同等の保管、管理をする。また、複製物を作成した場合には、複製の時期、複製された記録媒体又は物件の名称を別紙のとおり記録し、相手方の求めに応じて、当該記録を開示する。（＊６）

④　漏えい、紛失、盗難、盗用等の事態が発生し、又はそのおそれがあることを知った場合は、直ちにその旨を相手方に書面をもって通知する。

⑤　秘密情報の管理について、取扱責任者を定め、書面をもって取扱責任者の氏名及び連絡先を相手方に通知する。（＊７）

２．甲又は乙は、次項に定める場合を除き、秘密情報等を第三者に開示する場合には、書面により相手方の事前承諾を得なければならない。この場合、甲又は乙は、当該第三者との間で本契約書と同等の義務を負わせ、これを遵守させる義務を負うものとする。

３．甲又は乙は、法令に基づき秘密情報等の開示が義務づけられた場合には、事前に相手方

に通知し、開示につき可能な限り相手方の指示に従うものとする。

第３条（返還義務等）
１．本契約に基づき相手方から開示を受けた秘密情報を含む記録媒体、物件及びその複製物（以下「記録媒体等」という。）は、不要となった場合又は相手方の請求がある場合には、直ちに相手方に返還するものとする。
２．前項に定める場合において、秘密情報が自己の記録媒体等に含まれているときは、当該秘密情報を消去するとともに、消去した旨（自己の記録媒体等に秘密情報が含まれていないときは、その旨）を相手方に書面にて報告するものとする。

第４条（損害賠償等）
甲若しくは乙、甲若しくは乙の従業員若しくは元従業員又は第二条第二項の第三者が相手方の秘密情報等を開示するなど本契約の条項に違反した場合には、甲又は乙は、相手方が必要と認める措置を直ちに講ずるとともに、相手方に生じた損害を賠償しなければならない。

第５条（有効期限）
本契約の有効期限は、本契約の締結日から起算し、満〇年間とする。期間満了後の〇ヵ月前までに甲又は乙のいずれからも相手方に対する書面の通知がなければ、本契約は同一条件でさらに〇年間継続するものとし、以後も同様とする。

第６条（協議事項）
本契約に定めのない事項について又は本契約に疑義が生じた場合は、協議の上解決する。

第７条（管轄）
本契約に関する紛争については〇〇地方（簡易）裁判所を第一審の専属管轄裁判所とする。

本契約締結の証として、本書を二通作成し、両者署名又は記名捺印の上、各自一通を保有する。

令和＿＿年＿＿月＿＿日

（甲）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

（乙）＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

別紙１

開示情報一覧（甲から乙に開示）

提供年月日	情報の件名・概要	提供方法	その他
	ファイル名・文書のタイトルその他提供した情報を特定できる記載	CD、紙資料、メール等	

（＊１）業務提携・業務委託等の事前検討・協議に際して秘密保持契約書を締結する場合のほか、その後の業務提携・業務委託に係る契約の中で上記の例のような秘密保持条項を盛り込む場合も考えられます。なお、本例のように、業務提携・業務委託に係る契約とは別に、事前の協議段階での秘密保持契約を締結する場合には、業務提携・業務委託に係る契約書において、別途、秘密保持契約書を締結している旨を明示し、それぞれが何に関連する秘密保持契約であるのか等、契約関係を明確にすることが有効です。

（＊２）この他、業務提携・業務委託等に向けた検討の事実それ自体が秘密情報に含まれると定めることもあります。その場合、業務提携・業務委託の検討の事実については、第５条に定める有効期限は他の秘密情報と比べて相対的に短く、自動更新条項は置かずに６か月～２年程度となることが一般的です。また、業務提携・業務委託を合意した時点での当該業務提携・業務委託の事実についての公表は、事前に双方同意のもとで行う旨を併せて規定することも考えられます。

（＊３）秘密保持の対象とする情報の定義と呼称（例えば、「企業秘密」、「秘密情報」など。）については、当該開示の趣旨や取引慣行等に応じて様々なものが考えられます。なお、上記では「一切の情報」と書いていますが、秘密保持の対象となる情報の特定ができる場合には、別紙でその内容をリスト化するなど（☞＊４（第２項）を参照）、できる限り具体的に行うことが重要です。

（＊４）秘密情報の対象をより明確化するためには、秘密保持の対象情報を別紙でリスト化し、随時更新することも考えられ、その場合にはこのような規定を追加することも考えられます。

（＊５）口頭や映像等で情報が開示される場合に備え、このような規定を追加することも考えられます。

（＊６）複製を行うことについては、事前の書面による承諾を求めると、受領者において情報の円滑な活用が阻害される可能性が懸念されます。そこで、また～以下のような規定を設け、いつどのような複製物を作成したかをリスト化し、返還・消去の対象を明確化することも考えられます。

（＊７）取扱責任者等、秘密情報の授受を行う窓口を決定し、当該窓口経由でのみ秘密情報の開示を行う場合も考えられます。

第５　取引基本契約書（製造請負契約）（抄）の例

（(金型）製造業者（乙）が、取引先（甲）から試作品・金型及びこれに付帯する製品の製作、改造又は修理を請け負う場合の基本契約書の条項の例）

第○条（仕様書、図面の確認等）
　甲又は乙は、相手方から交付された図面、仕様書その他の指示について疑義がある場合は相手方に申出るものとし、相手方はこれに対し、書面により指示等を行うものとする。

第○条（目的物の価格）
１．甲又は乙は、設計仕様、金型製作仕様、品質、納期、納入方法、支払方法、材料費、労務費、諸経費、検査方法、市場の動向などの諸要素を考慮した合理的な算定方式に基づき、見積書等により協議の上、目的物の価格を定めるものとする。
２．個別契約成立後、価格決定の基礎となった条件が変更される場合は、価格について協議するものとする。

第○条（秘密保持）
１．甲又は乙は、基本契約又は個別契約により知り得た相手方の営業上又は技術上の情報のうちで、相手方が秘密である旨を明示したもの（以下「秘密情報」という。）（＊１）を、第５項に定める場合を除き、相手方の承諾を得ない限り、第三者に開示若しくは漏えい、又は本契約の目的以外に使用してはならない。ただし、開示を受けた当事者が、書面によってその根拠を立証できる場合に限り、以下の情報は秘密情報の対象外とするものとする。
　①　開示を受けたときに既に保有していた情報
　②　開示を受けた後、秘密保持義務を負うことなく第三者から正当に入手した情報
　③　開示を受けた後、相手方から開示を受けた情報に関係なく独自に取得し、又は創出した情報
　④　開示を受けたときに既に公知であった情報
　⑤　開示を受けた後、自己の責めに帰し得ない事由により公知となった情報
２．前項本文の情報のうち、甲が乙に秘密である旨を指定して開示する情報は別紙１を、また乙が甲に秘密である旨を指定して開示する情報は別紙２を含むものとする。なお、別紙１及び別紙２は甲と乙とが協力し、常に最新の状態を保つべく適切に更新するものとする。（＊２）
３．甲又は乙が口頭により相手方から開示を受けた情報については、改めて相手方から当該事項について記載した書面の交付を受けた場合に限り、相手方に対し本規程に定める義務を負うものとする。（＊３）
４．口頭、映像その他その性質上秘密である旨の表示が困難な形態又は媒体により開示、提供された情報については、開示者が相手方に対し、秘密である旨を開示時に伝達し、かつ、当該開示後○日以内に当該秘密情報を記載した書面を秘密である旨の表示をして交付することにより、秘密情報とみなされるものとする。（＊３）
５．甲又は乙は、法令に基づき前項に規定する秘密情報の開示が義務づけられた場合には、事前に相手方に通知し、開示につき可能な限り相手方の指示に従うものとする。

第○条（図面等の管理）
１．甲又は乙は、相手方が貸与し又は提出した図面、仕様書等の保管管理については、厳重にこれを行うものとし、相手方の承諾がない限り、第三者に開示してはならない。
２．甲又は乙は、本契約又は個別契約に基づき開示を受けた秘密情報を含む図面及び仕様書並びにその複製物（以下「図面等」という。）について、不要となった場合又は相手方の請求がある場合には、直ちに相手方に返還するものとする。
３．前項に定める場合において、秘密情報が自己の図面等に含まれているときは、当該秘密情報を消去するとともに、消去した旨（自己の図面等に秘密情報が含まれていないときは、その旨)、相手方に書面にて報告するものとする。

第○条（知的財産権等）
１．甲と乙との共同研究により取得した知的財産権の帰属は、甲と乙とが協議して定めるも

のとする。
２．目的物の製作に関する設計上の考案、設計図面、又は製作情報に関する知的財産権は、原則として乙に帰属する。（＊４）
３．甲又は乙は、相手方の図面若しくは仕様書により製作された目的物又はその製作方法に関連し知的財産権の出願を行う場合には、事前にその旨を相手方に申出て書面による承諾を得なければならない。この場合、知的財産権の帰属等に関しては、その貢献度に応じて甲と乙とが協議して定める。
４．甲又は乙は、目的物に関わる知的財産権を第三者に譲渡又は実施権設定の許諾を行う場合は、相手方の書面による承諾を得るものとする。
５．甲又は乙は、目的物につき第三者との間に知的財産権上の権利侵害等の紛争が生じたときは、相手方に書面で通知し、甲及び乙のうちその責めに帰すべき者が、その負担と責任において処理・解決するものとする。

第○条（目的物等に化体された秘密情報の帰属等）（＊４）
１．目的物及び成果物に化体された秘密情報は、乙に帰属する。
２．甲は、乙から示された前項の秘密情報の秘密性を保全し、○○において自ら○○の製造に用いるためにのみ使用することができる。
３．甲は、第一項の秘密情報（これが化体した目的物又は成果物を含む。）を第三者に開示する場合又はその複製を作成する場合には、書面により乙の事前の承諾を得るものとする。
４．その他当該秘密情報の取扱いについて疑義が生じた場合には、甲と乙とが協議するものとする。

第○条（製作・販売の禁止）
甲又は乙は、相手方の書面による事前の承諾を得ない限り、第三者に対し相手方の図面、又は仕様書による製作又は販売を行ってはならない。

第○条（損害賠償等）（＊４）
甲若しくは乙、甲若しくは乙の従業員若しくは元従業員又は甲若しくは乙の許諾により開示を受けた第三者が相手方の秘密情報等を開示するなど本契約の条項に違反した場合には、甲又は乙は、相手方が必要と認める措置を直ちに講ずるとともに、相手方に生じた損害を賠償しなければならない。

別紙１

開示情報一覧（甲から乙に開示）

提供年月日	情報の件名・概要	提供方法	その他
	ファイル名・文書のタイトルその他提供した情報を特定できる記載	CD、紙資料、メール等	

（＊１）秘密保持の対象とする情報の定義と呼称（例えば、「企業秘密」、「秘密情報」など。）については、当該開示の趣旨や取引慣行等に応じて様々なものが考えられます。なお、上記では特に限定を付していませんが、秘密保持の対象となる情報の特定ができる場合には、別紙でその内容をリスト化するなど（☞＊２（第２項）を参照）、できる限り具体的に行うことが重要です。

（＊２）秘密情報の対象をより明確化するためには、秘密保持の対象情報を別紙でリスト化し、随時更新することも考えられ、その場合にはこのような規定を追加することも考えられます。

（＊３）口頭や映像等で情報が開示される場合に備え、このような規定を追加することも考えられます。

（＊４）目的物等の価格に乙が業務の過程において創出等した情報の対価を含めたり、甲から製造方法に関する情報や図面などが提供されることによって情報の創出に対する甲の寄与度が著しく高いと考

えられたりする等の事情により、乙が業務の過程において創出等した情報を甲に帰属させることについて合意がなされている場合においては上記の「知的財産権等」、第二項及び「目的物等に化体された秘密情報の帰属等」の規定に代わり、以下の内容を定めることも考えられます。

第〇条（知的財産権の帰属等）
２．目的物の製作に関する設計上の考案、設計図面、又は製作情報に関する知的財産権は、甲に帰属する。

第〇条（目的物等に化体された秘密情報の帰属等）
目的物及び成果物に化体された秘密情報は、甲に帰属する。

（＊５）秘密保持義務の違反時における損害賠償の責任を規定することは、情報漏えいを抑止する効果があります。

第６　業務委託契約書（抄）の例

（企業（甲）が、自己の特定の業務についてこれを他社（乙）に委託する場合であって、甲のみが秘密情報を開示する場合の契約書の条項の例）

※各種メンテナンス業者等、一定の許可の下に、自社の秘密情報に接する可能性のある事業者に対しては、業務中に接する自社情報の漏えいの防止のため、業務委託契約の中で秘密保持を合意する必要があります。

第〇条（秘密保持）
１．乙は、本契約の履行にあたり、甲が秘密である旨を明示して開示する情報及び本契約の履行により生じる情報（以下「秘密情報」という。）（＊１）を秘密として取り扱い、次に定める場合を除き、甲の事前の書面による承諾なく第三者に開示してはならない。ただし、乙が書面によってその根拠を立証できる場合に限り、以下の情報は秘密情報の対象外とするものとする。
①　開示を受けたときに既に乙が保有していた情報
②　開示を受けた後、秘密保持義務を負うことなく第三者から正当に入手した情報
③　開示を受けた後、相手方から開示を受けた情報に関係なく乙が独自に取得し、又は創出した情報
④　開示を受けたときに既に公知であった情報
⑤　開示を受けた後、乙の責めに帰し得ない事由により公知となった情報
２．甲が乙に秘密である旨指定して開示する情報は、別紙の通りである。なお、別紙は甲と乙とが協力し常に最新の状態を保つべく適切に更新するものとする。（＊２）
３．乙が口頭により相手方から開示を受けた情報については、改めて相手方から当該事項について記載した書面の交付を受けた場合に限り、相手方に対し本規程に定める義務を負うものとする。（＊３）
４．口頭、映像その他その性質上秘密である旨の表示が困難な形態又は媒体により開示、提供された情報については、開示者が相手方に対し、秘密である旨を開示時に伝達し、かつ、当該開示後〇日以内に当該秘密情報を記載した書面を秘密である旨の表示をして交付することにより、秘密情報とみなされるものとする。（＊３）
５．乙は、甲より開示された秘密情報の管理につき、乙が保有する他の情報や記録媒体等と明確に区別して適切に管理するとともに、以下の事項（＊４）を遵守する。（＊５）（＊６）
①　秘密情報は本契約の目的の範囲内でのみ使用する。
②　委託期間満了時又は本契約の解除時には、秘密情報が記録等された記録媒体又は物件（複写物、複製物を含む。）を甲に返却、又は自己で廃棄の上、廃棄した旨の誓約書を甲に提出する。
③　前号に関わらず、甲から返却また廃棄を求められたときは、秘密情報（第五号に基づく複写物及び複製物を含む。）を甲に返却、又は自己で廃棄の上、廃棄した旨の誓約書を甲に提出する。
④　前二号に定める場合において、秘密情報が自己の記録媒体又は物件に記録等されているときは、当該秘密情報を消去するとともに、消去した旨（自己の記録媒体等に秘密情報が記録等されていないときは、その旨）、書面にて甲に報告する。
６．乙は、法令に基づき前項に規定する秘密情報の開示が義務づけられた場合には、事前に甲に通知し、開示につき甲の指示に従うものとする。

第〇条（再委託）
１．乙は、甲の事前の書面による承諾を得ずに、本業務の全部又は一部を第三者へ再委託してはならない。
２．前項の事前の書面による承諾に基づき本業務を再委託する場合には、乙は自己が負う義務と同等の義務を再委託先に対して書面にて課すとともに、甲に対して再委託先に当該義務を課した旨を書面により報告し、かつ乙は当該秘密情報の開示に伴う責任を負うものとする。
３．前項に加え、乙は再委託先から次の各号の承諾を得なければならない。また、乙は、当

該承諾を得た旨を甲に書面で報告する。
① 事故発生時には直ちに甲に対しても通知すること
② 事故再発防止策を協議する際には甲の参加も認めること
③ 再委託先における秘密情報の具体的管理状況の報告は、甲の閲覧も認めること

第○条（損害賠償等）（＊７）
乙若しくは乙の従業員若しくは元従業員又は甲の許諾により乙から開示を受けた第三者が甲の秘密情報等を開示するなど本契約の条項に違反した場合には、乙は、甲が必要と認める措置を直ちに講ずるとともに、甲に生じた損害を賠償しなければならない。

別紙

開示情報一覧

提供年月日	情報の件名・概要	提供方法	その他
	ファイル名・文書のタイトルその他提供した情報を特定できる記載	CD、紙資料、メール等	

（＊１）秘密保持の対象とする情報の定義と呼称（例えば、「企業秘密」、「秘密情報」など。）については、当該開示の趣旨や取引慣行等に応じて様々なものが考えられる。なお、上記では特に限定を付していませんが、秘密保持の対象となる情報の特定ができる場合には、別紙でその内容をリスト化するなど（☞＊２（第４項）を参照）、できる限り具体的に行うことが重要です。

（＊２）秘密情報の対象をより明確化するためには、秘密保持の対象情報を別紙でリスト化し、随時更新することも考えられ、その場合にはこのような規定を追加することも考えられます。

（＊３）口頭や映像等で情報が開示される場合に備え、このような規定を追加することも考えられます。

（＊４）上記の他、開示された秘密情報の具体的管理方法につき、以下のように定める例もあります。

① 秘密情報の管理責任者及び保管場所を定め、善良なる管理責任者の注意をもって保管管理する。
② 秘密情報を取り扱う従業員を必要最小限にとどめ、上記保管場所以外へ持ち出さない。
③ 秘密情報の管理責任者名、秘密情報を取り扱う従業員の氏名及び秘密情報の保管場所を、○年○月○日までに甲に報告する。また、報告内容に変更が生じた場合には、変更が生じた月に提出する第十一号の具体的管理状況の報告において、当該変更内容を甲に報告する。
④ 前号にて報告した秘密情報を取り扱う従業員に対して本契約の内容を周知徹底させ、秘密情報の漏えい、紛失、破壊、改ざん等を未然に防止するための措置を取る。
⑤ 甲の書面による承諾を得た場合を除き、秘密情報を複写、複製しない。
⑥ 事故発生時には直ちに甲に対して通知し、事故再発防止策の協議には甲の参加を認める。
⑦ 乙は、甲に対して、秘密情報の以下の具体的管理状況を毎月末に報告する。乙は、甲が乙の事務所における秘密情報の管理状況を確認するために、乙の事務所への立入検査を希望する場合には、当該検査に協力するものとする。また、甲は乙に対して是正措置を求めることができ、乙はこれを実施するものとする。
(a) 委託契約範囲外の加工、利用の禁止の遵守
(b) 委託契約範囲外の複写、複製の禁止の遵守
(c) 安全管理措置状況

（＊５）なお、委託業務の履行に伴い、乙から甲に開示がなされる乙の秘密情報がある場合には、乙の秘密情報の取扱いについての定めについても設ける必要があります。

（＊６）本契約の履行を通じ、乙の創意により新たに作成された情報の帰属について、以下のような定めを設ける例もあります。

> 第〇条（乙が創出した秘密情報の帰属）
> １．本契約の履行にあたり、甲が開示した秘密情報に基づかずに、乙が創出した秘密情報は、乙に帰属する。
> ２．甲は、当該示された秘密情報の秘密性を保全し、〇〇に用いるためにのみ使用することができる。
> ３．甲は、当該秘密情報を第三者へ開示する場合又はその複製を作成する場合には、乙の事前の承諾を得るものとする。
> ４．その他当該秘密情報の取扱いについて疑義が生じた場合には、甲と乙とが協議することとする。

（＊７）秘密保持義務の違反時における損害賠償の責任を規定することは、情報漏えいを抑止する効果があります。

第７　共同研究開発契約書（抄）の例

（企業（甲）が、他社（乙）との間で特定の製品等の研究開発活動を分担する際の契約書の条項の例）

第○条（定義）
本契約書において、次に掲げる用語は次の定義によるものとする。
①　「研究成果」とは、本契約に基づき行われた本共同研究の遂行の過程で得られた発明、考案、意匠、著作物、ノウハウ等の技術的成果をいう。
②　「知的財産権」とは、次に掲げるものをいう。
イ　特許法、実用新案法、意匠法、商標法、半導体集積回路の回路配置に関する法律、種苗法、著作権法に規定する各権利、及び外国における当該権利に相当する権利
ロ　秘密とすることが可能な技術情報であって、かつ、財産的価値のあるものの中から甲と乙とが協議の上、特に指定するもの

第○条（資料等提供）
１．甲又は乙は、本共同研究の実施のために必要な情報、資材及び資料（以下「資料等」という。）を相互に無償で提供又は開示するものとする。ただし、第三者との契約により秘密保持義務を負っているものについては、この限りではない。
２．甲又は乙は、本共同研究完了後又は本共同研究中止後、相手方から提供された資料等（それに基づき新たに作成された資料等であって、甲と乙とが協議して指定したものを含む。）について、直ちに相手方に返還するものとする。
３．前項に定める場合において、自己の資料等に相手方の技術上又は営業上の情報が含まれているときは、甲又は乙は、当該情報を消去するとともに、消去した旨（自己の資料等に当該情報が含まれていないときは、その旨）、相手方に書面にて報告するものとする。

第○条（秘密保持）
１．甲又は乙は、本共同研究の実施にあたり、相手方より開示を受け、又は知り得た技術上若しくは営業上の一切の情報のうち、相手方が秘密である旨を明示したもの（以下「秘密情報」という。）（＊１）について、本条第六項に定める場合を除き、第三者に開示又は漏えいしてはならない。ただし、開示を受けた当事者が書面によってその根拠を立証できる場合に限り、以下の情報は秘密情報の対象外とするものとする。
①　開示を受け又は知得したときに既に保有していた情報
②　開示を受け又は知得した後、秘密保持義務を負うことなく第三者から正当に入手した情報
③　開示を受け又は知得した後、相手方から開示を受けた情報に関係なく独自に取得し、又は創出した情報
④　開示を受け又は知得したときに既に公知であった情報
⑤　開示を受け又は知得した後、自己の責めに帰さない事由により公知となった情報
２．前項本文の情報のうち、甲が乙に秘密である旨を指定して開示する情報は別紙１を、また乙が甲に秘密である旨を指定して開示する情報は別紙２を含むものとする。なお、別紙１及び別紙２は甲と乙とが協力し、常に最新の状態を保つべく適切に更新するものとする。（＊２）
３．甲又は乙が口頭により相手方から開示を受けた情報については、改めて相手方から当該事項について記載した書面の交付を受けた場合に限り、相手方に対し本規程に定める義務を負うものとする。（＊３）
４．口頭、映像その他その性質上秘密である旨の表示が困難な形態又は媒体により開示、提供された情報については、開示者が相手方に対し、秘密である旨を開示時に伝達し、かつ、当該開示後○日以内に当該秘密情報を記載した書面を秘密である旨の表示をして交付することにより、秘密情報とみなされるものとする。（＊３）
５．甲又は乙は、第一項に規定する秘密情報を本共同研究以外の目的に使用してはならない。ただし、書面により事前に相手方の承諾を得た場合はこの限りではない。
６．甲又は乙は、法令に基づき第一項に規定する秘密情報の開示が義務づけられた場合には、事前に相手方に通知し、開示につき可能な限り相手方の指示に従うものとする。

第〇条（第三者との共同研究の禁止）
　甲又は乙は、相手方の事前の書面による承諾なしに、第三者との間で本共同研究と同一の目的となる研究を行ってはならない。

第〇条（知的財産権の出願等）（＊４）
１．甲又は乙は、本契約の有効期間中及びその失効後〇年間において、本共同研究により研究成果が生じた場合は、速やかに相手方に通知しなければならない。
２．甲又は乙は、前項に規定する研究成果に係る知的財産権については、原則として、甲乙双方の共有とし、その持分は原則として折半とするものとする。
３．甲又は乙は、前項に規定する研究成果に係る知的財産権の出願又は設定登録の申請（以下「出願等」という。）を行う場合には、共同で出願等するものとする。
４．甲又は乙は、前項に規定する知的財産権の出願等の手続及びその権利保全に要する一切の費用について、原則として、折半して負担するものとする。
５．甲又は乙は、前項に規定する費用を負担しないときは、当該知的財産権に係る自己の持ち分を相手方に譲渡するものとする。譲渡に必要な事項は、別途、甲と乙とが協議して定めるものとする。
６．甲又は乙は、外国において知的財産権を出願等する場合には、別途甲と乙とが協議して、これを定めるものとする。

第〇条（研究成果の公表等）
　甲又は乙は、本契約の有効期間中及び契約終了後〇年間は、本共同研究によって得られた研究成果を公表又は第三者に開示しようとする場合には、その内容、時期、方法等について、書面により事前に相手方の承諾を受けるものとする。

第〇条（研究成果の実施）（＊５）（＊６）
１．本共同研究の研究成果及び第〇条（知的財産権の出願等）の規定による共有の知的財産権について甲又は乙以外の第三者（それぞれの子会社を含む。）に実施させる場合には、予め甲と乙とで協議し、実施の可否及びその条件等を定めるものとする。
２．前項の規定に基づき、共有の知的財産権を第三者に実施させた場合の実施許諾料は、当該知的財産権に係る甲及び乙の持分に応じて、それぞれに配分するものとする。

第〇条（持分の譲渡）
　甲又は乙は、本共同研究の結果生じた知的財産権の持分を第三者に譲渡する場合には、書面により事前に相手方の承諾を受けるものとする。

第〇条（利用発明等）（＊７）
１．甲又は乙は、第〇条（知的財産権の出願等）に規定する発明の利用発明又は改良発明（以下「利用発明等」という。）をし、これらについて知的財産権の出願等をしようとするときは、その内容を相手方に書面で事前に通知しなければならない。
２．甲又は乙は、前項による通知があったときは、甲と乙とで協議し、当該利用発明等の取扱いについて決定する。

第〇条（有効期限）
　本契約の有効期限は、本共同研究の実施期間とする（令和〇年〇月〇日から令和〇年〇月〇日まで）。ただし、第〇条（知的財産権の出願等）及び第〇条（研究成果の公表等）の規定は当該条項が定める期間、第〇条（研究成果の実施）、第〇条（持分の譲渡）、及び第〇条（利用発明等）の規定は第〇条（知的財産権の出願等）に規定する知的財産権の存続する期間中、第〇条（秘密保持）の規定は本契約の有効期間満了後もなお〇年間有効に存続するものとする。

第〇条（損害賠償等）（＊８）
　甲若しくは乙、甲若しくは乙の従業員若しくは元従業員又は甲若しくは乙の許諾により開示を受けた第三者が相手方の秘密情報等を開示するなど本契約の条項に違反した場合には、甲又は乙は、相手方が必要と認める措置を直ちに講ずるとともに、相手方に生じた損害を賠償しなければならない。

別紙１

開示情報一覧（甲から乙に開示）

提供年月日	情報の件名・概要	提供方法	その他
	ファイル名・文書のタイトルその他提供した情報を特定できる記載	CD、紙資料、メール等	

（＊１）秘密保持の対象とする情報の定義と呼称（例えば、「企業秘密」、「秘密情報」など。）については、当該開示の趣旨や取引慣行等に応じて様々なものが考えられる。なお、上記では特に限定を付していませんが、秘密保持の対象となる情報の特定ができる場合には、別紙でその内容をリスト化するなど（☞＊２（第２項）を参照）、できる限り具体的に行うことが重要です。

（＊２）秘密情報の対象をより明確化するためには、秘密保持の対象情報を別紙でリスト化し、随時更新することも考えられ、その場合にはこのような規定を追加することも考えられます。

（＊３）口頭や映像等で情報が開示される場合に備え、このような規定を追加することも考えられます。

（＊４）当該共同研究の目的や契約当事者の分担業務等に応じ、例えば、相手方から情報提供や援助等は無く単独で開発した研究成果の帰属について当該開発者の単独とすること等を定めることも考えられます。

（＊５）当該研究の目的や契約当事者の事業分野等に応じて、研究成果の実施については、例えば次のように、その実施の在り方について具体的に定めることなども考えられます。

第○条（研究成果の実施）
１．本共同研究の研究成果の実施については、次のとおりとする。
　①　甲がＸＸＸ（製品名）の製造を行い、乙が同ＸＸＸ（製品名）を搭載したＹＹＹ（製品名）の販売を行う。
　②　（省略）
２．前項に定めるほかは、甲と乙との協議により、その実施者と条件を定めるものとする。

（＊６）本条項は、甲及び乙それぞれが研究成果を実施する場合を前提としているが、例えば甲が研究成果を実施しない場合には次のような条項となることが考えられます。

第○条（研究成果の実施）
１．乙が本共同研究の研究成果を実施しようとする場合には、その旨を事前に文書により甲に通知しなければならない。
２．乙の実施に際して、甲は自己実施をしないことから、乙は、甲と乙とが別途定める実施契約に基づき実施料を甲に支払わなければならない。

（＊７）共同研究開発の目的や研究成果に含まれる事項の性質等から、一定の利用発明や改良発明がなされることが予想され、そうした利用発明や改良発明を独自に実施することが企図されているような場合等においては、当該利用発明や改良発明の出願等については協議を要することなく、単独で行うことができる旨を定めることなども考えられます。

（＊８）秘密保持義務の違反時における損害賠償の責任を規定することは、情報漏えいを抑止する効果があります。

※今後、最新情報に更新の可能性あり

参考資料３

各種窓口一覧

本書に関連してご利用いただけると考えられる窓口をまとめました。
各窓口の詳細については、それぞれの URL 等をご確認下さい。

各種窓口一覧

＜全般（情報漏えい対策、知的財産戦略等）＞

営業秘密・知財戦略相談窓口（営業秘密 110 番）【INPIT】	
特許としての権利化、営業秘密としての秘匿化を含むオープン・クローズ戦略等の具体的な知的財産戦略に加え、秘匿化を選択した際の営業秘密の管理手法、また営業秘密の漏えい・流出等に関する相談に対応します。 また、近畿地域の企業を対象とした「関西知財戦略支援専門窓口」も設置しております。	営業秘密・知財戦略相談窓口 ＜URL＞ https://faq.inpit.go.jp/tradesecret/service/ ＜電話＞ 03-3581-1101（内線　3844） ＜メール＞ trade-secret@inpit.go.jp 関西知財戦略支援専門窓口 ＜URL＞ https://www.inpit.go.jp/kinki/senmon_madoguchi/index.html ＜電話＞ 06-6486-9122 ＜メール＞ ip-js01@inpit.go.jp
知財総合支援窓口　【特許庁/INPIT】	

中小企業等が抱える経営課題について、自社のアイデアや技術などの「知的財産」の側面から解決を図る支援窓口です。経験豊富な窓口相談担当者が支援します（全国 47 都道府県に設置）。より専門的な内容の相談は、専門家や関係支援機関と連携して支援を行います。	＜URL＞ https://chizai-portal.inpit.go.jp/ ＜全国共通ナビダイヤル＞ 0570-082100 ※お近くの支援窓口につながります。
弁護士知財ネット　【弁護士知財ネット】	
弁護士知財ネットでは、社内の秘密管理体制、他社との秘密保持契約等の各種契約、漏えい洩時の民事刑事の対応等の法律相談を受け付けています（有料）。 Web 上の「相談依頼」フォーマットに記載の上送信し、担当者からのお返事をお待ちください。 または、各地域会連絡窓口担当弁護士に電話でご連絡ください。	＜URL＞ http://www.iplaw-net.com/ ＜相談依頼フォーマット＞ https://iplaw-net.com/consultation ＜電話＞ http://www.iplaw-net.com/telephone （地域別の連絡窓口一覧）
ひまわりほっとダイヤル　【日本弁護士連合会】	
「ひまわりほっとダイヤル」は、中小企業や個人事業主のみなさまを対象に、日本弁護士連合会及び全国 52 の弁護士会が提供する、弁護士との面談予約が可能なサービスです。全国共通電話番号または WEB の申込みフォームから、地域の弁護士会につながります。一部の地域を除き、初回相談 30 分が無料です。 法律の専門家である弁護士が、経営上の問題・悩みについて、裁判まで見通したアドバイスを行います。	＜URL＞ https://www.nichibenren.or.jp/ja/sme/index.html~~※上記 web からのお申し込みも可能です。~~ ＜電話＞ 0570-001(おおい)-240(ちゅーしょー)（全国共通「ひまわりほっとダイヤル」） ＜WEB 申込みフォーム＞ https://form.qooker.jp/Q/auto/ja/chusho2015/online/

弁理士知財キャラバン　【日本弁理士会】	
日本弁理士会では、特許、デザイン、ブランド、コンテンツ、製造ノウハウなどの知的財産を上手に活用して、さらに上を目指す中小企業を応援するため、「弁理士知財キャラバン」事業を実施しています。 知財経営コンサルティングのスキルを持った弁理士が直接企業を訪問して、共に課題を解決していきます。	＜URL＞ https://www.jpaa.or.jp/activity/caravan/ ※申請方法については、上記 web ページをご確認下さい。
常設知的財産相談室　【日本弁理士会】	
特許・実用新案・意匠・商標の出願手続、調査、鑑定、異議申立、訴訟はもちろん、諸外国の制度や知的財産権全般について弁理士が無料で相談に応じています。	＜URL＞ https://www.jpaa.or.jp/free_consultation/ ~~http://www.jpaa.or.jp/?cat=774~~ （相談を受け付けている支部の所在地と電話番号一覧） ※最寄りの窓口をご確認の上、電話による事前予約をお願いいたします。

＜情報セキュリティ＞

情報セキュリティ安心相談窓口　【IPA】	
一般的な情報セキュリティ（主にコンピュータウイルスや不正アクセス）に関する技術的な相談に対してアドバイスを提供しています。	＜URL＞ https://www.ipa.go.jp/security/anshin/index.html ＜電話＞ 03-5978-7509 ＜メール＞ anshin@ipa.go.jp
インシデント報告窓口　【JPCERT/CC】	
インターネットを介して発生する情報流出、フィッシングサイト、Web 改ざん、マルウエア感染、サーバへの侵入やDos(DDos)等の不正アクセス等に関する技術的な対応依頼、ご相談、ご報告を受け付けます。	＜URL＞ https://www.jpcert.or.jp/form/ <Web フォーム> https://www.jpcert.or.jp/form/ <メール> info@jpcert.or.jp

＜漏えいが疑われるとき＞

営業秘密・知財戦略相談窓口（営業秘密 110 番）　【INPIT】（再掲）	
営業秘密の漏えい・流出等に関する相談に対応します。社内調査の仕方や、証拠の集め方、警察に相談する際のポイント等をアドバイスするとともに、必要に応じてＩＰＡとの連携や、警察庁を通じた都道府県警察のご紹介を行います。 また、近畿地域の企業を対象とした「関西知財戦略支援専門窓口」も設置しております。	営業秘密・知財戦略相談窓口 ＜URL＞ https://faq.inpit.go.jp/tradesecret/service/ ＜電話＞ 03-3581-1101（内線　3844） ＜メール＞ trade-secret@inpit.go.jp 関西知財戦略支援専門窓口 ＜URL＞ https://www.inpit.go.jp/kinki/senmon_madoguchi/index.html

	＜電話＞ 06-6486-9122 ＜メール＞ ip-js01@inpit.go.jp

＜漏えいが疑われるとき＞

警察　【都道府県警察本部(営業秘密侵害事犯担当)】

被害の御相談を受け付けます。下表から、最寄りの窓口をご確認下さい。	下表参照

＜営業秘密侵害事犯　窓口連絡先一覧＞

警察名	代表電話
北海道警察本部生活経済課	011-251-0110
北海道函館方面本部生活安全課	0138-31-0110
北海道旭川方面本部生活安全課	0166-35-0110
北海道釧路方面本部生活安全課	0154-25-0110
北海道北見方面本部生活安全課	0157-24-0110
青森県警察本部保安課	017-723-4211
岩手県警察本部生活環境課	019-653-0110
宮城県警察本部生活環境課	022-221-7171
秋田県警察本部生活環境課	018-863-1111
山形県警察本部生活環境課	023-626-0110
福島県警察本部生活環境課	024-522-2151
警視庁生活経済課	03-3581-4321
茨城県警察本部生活環境課	029-301-0110
栃木県警察本部生活環境課	028-621-0110
群馬県警察本部生活環境課	027-243-0110
埼玉県警察本部生活経済課	048-832-0110
千葉県警察本部生活経済課	043-201-0110
神奈川県警察本部生活経済課	045-211-1212
新潟県警察本部生活保安課	025-285-0110
山梨県警察本部生活安全捜査課	055-235-2121
長野県警察本部生活環境課	026-233-0110
静岡県警察本部生活保安課	054-271-0110
富山県警察本部生活環境課	076-441-2211
石川県警察本部生活安全捜査課	076-225-0110
福井県警察本部生活環境課	0776-22-2880
岐阜県警察本部生活環境課	058-271-2424

警察名	代表電話
愛知県警察本部生活経済課	052-951-1611
三重県警察本部生活環境課	059-222-0110
滋賀県警察本部生活環境課	077-522-1231
京都府警察本部生活保安課	075-451-9111
大阪府警察本部生活経済課	06-6943-1234
兵庫県警察本部生活経済課	078-341-7441
奈良県警察本部生活環境課	0742-23-0110
和歌山県警察本部生活環境課	073-423-0110
鳥取県警察本部生活安全企画課	0857-23-0110
島根県警察本部生活環境課	0852-26-0110
岡山県警察本部生活安全捜査課	086-234-0110
広島県警察本部生活環境課	082-228-0110
山口県警察本部生活環境課	083-933-0110
徳島県警察本部生活安全企画環	088-622-3101
香川県警察本部生活環境安全捜	087-833-0110
愛媛県警察本部生活環境課	089-934-0110
高知県警察本部生活環境安全企	088-826-0110
福岡県警察本部生活保安課	092-641-4141
佐賀県警察本部生活安全企画課	0952-24-1111
長崎県警察本部生活環境課	095-820-0110
熊本県警察本部生活環境課	096-381-0110
大分県警察本部保安課	097-536-2131
宮崎県警察本部生活環境課	0985-31-0110
鹿児島県警察本部生活環境課	099-206-0110
沖縄県警察本部生活保安課	098-862-0110

~~標的型サイバー攻撃特別相談窓口（IPA）~~	
~~標的型攻撃メールを受信した場合の、専門窓口として「標的型サイバー攻撃特別相談窓口」を設置し、相談を受け付けています。~~ ~~※新型コロナウイルス感染防止策の徹底のため、電話相談等を一時的に停止している場合がありますので、ウェブサイトをご確認下さい。~~	~~＜URL＞~~ ~~http://www.ipa.go.jp/security/tokubetsu/index.html~~ ~~＜メール＞~~ ~~tokusou@ipa.go.jp~~ ~~＜電話＞~~ ~~03-5978-7599~~
弁護士知財ネット　【弁護士知財ネット】（再掲）	
弁護士知財ネットでは、社内の秘密管理体制、他社との秘密保持契約等の各種契約、漏えい洩時の民事刑事の対応等の法律相談を受け付けています（有料）。 Web 上の「相談依頼」フォーマットに記載の上送信し、担当者からのお返事をお待ちください。または、各地域会相談窓口担当弁護士に電話でご連絡ください。	＜URL＞ http://www.iplaw-net.com/ ※相談依頼フォーマットはこちらから ＜電話＞ http://www.iplaw-net.com/telephone （地域別の連絡窓口一覧）
ひまわりほっとダイヤル　【日本弁護士連合会】（再掲）	
「ひまわりほっとダイヤル」は、中小企業や個人事業主のみなさまを対象に、日本弁護士連合会及び全国 52 の弁護士会が提供する、弁護士との面談予約が可能なサービスです。全国共通電話番号または WEB の申込みフォームから、地域の弁護士会につながります。一部の地域都道府県を除き、初回面談相談 30 分が無料~~相談を実施中~~です。 法律の専門家である弁護士が、経営上の問題・悩みについて、裁判まで見通したアドバイスを行います。	＜URL＞ https://www.nichibenren.or.jp/ja/sme/index.html ＜電話＞ 0570-001-240（全国共通「ひまわりほっとダイヤル」） ＜WEB 申込みフォーム＞ https://form.qooker.jp/Q/auto/ja/chusho2015/online/ ~~※上記 web からのお申し込みも可能です。~~
日本知的財産仲裁センター（ADR）（※）　【日本知的財産仲裁センター】	
日本知的財産仲裁センターでは、弁護士もしくは弁理士 1 名、又は弁護士及び弁理士各 1 名による知的財産紛争に関連する相談を受け付けています（有料）。	＜URL＞ https://www.ip-adr.gr.jp/ ＜FAX＞ 03-3500-3839 ＜E-maill＞

	info@ip-adr.gr.jp

（※）日本知的財産仲裁センターは、ADR 法の基準をクリアしたものとして、法務大臣の認証を受けた民間ADR事業者「かいけつサポート」です。「かいけつサポート」一覧は、以下URLで確認できます。
~~https://www.moj.go.jp/KANBOU/ADR/jigyousya/ninsyou_index.html~~
https://www.adr.go.jp/jigyousha/

＜その他＞

公証役場　【法務局】	
確定日付で私書証書の存在した日を証明できます。相談は無料です。いつでも気軽にご相談ください。	＜URL＞ 公証役場一覧 https://www.koshonin.gr.jp/list （全国の公証役場所在地・電話番号・メールアドレス等）

※今後、最新情報に更新の可能性あり

参考資料４

秘密情報管理に関する各種ガイドライン等について

各章ごとに参考になるガイドライン等を紹介します。

【各章横断　テレワークの導入・実施に伴う情報管理への対応】

■テレワークの導入・実施に伴う対策

https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

(1) テレワークセキュリティガイドライン（総務省）

企業等がテレワークを実施する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するために、テレワークの導入に当たってのセキュリティ対策についての考え方や対策例を示したガイドライン。

(2) 中小企業等担当者向けテレワークセキュリティの手引き（チェックリスト）（総務省）

セキュリティの専任担当がいないような中小企業等におけるシステム管理担当者（専門用語について仕組みの詳細まではわからないが、利用シーンがイメージできるレベルの方）を対象として、テレワークを実施する際に最低限のセキュリティを確実に確保してもらうための手引き（チェックリスト）。

また、テレワークを導入・実施する場合を含めて、無線 LAN（Wi-Fi）の導入、情報システムの暗号化機能・電子署名機能の導入といった情報管理に対応する上で有益なガイドラインとして、以下のものもあります。

■無線 LAN（Wi-Fi）の導入・実施に伴う情報管理への対応

https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/

(1) Wi-Fi 利用者向け 簡易マニュアル（総務省）

Wi-Fi の利用者に対し、安全な Wi-Fi の利用のために必要なセキュリティ対策等に関する理解を深めていただくことを目的としたガイドライン。

(2) Wi-Fi 提供者向け セキュリティ対策の手引き（総務省）

Wi-Fi の提供者に対し、安全な Wi-Fi の提供のために必要なセキュリティ対策等に関する理解を深めていただくことを目的としたガイドライン。

■情報システムの暗号化機能・電子署名機能の導入への対応

https://www.cryptrec.go.jp/list.html

CRYPTREC 暗号リスト

総務省及び経済産業省は、CRYPTREC の活動を通して電子政府で利用される暗号技術の評価を行っており、2013 年 3 月に 「電子政府における調達

のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」を策定。政府機関等における情報システムの調達及び利用において本リストが利用されています。

【第２章　保有する情報の把握・評価、秘密情報の決定】

■知的財産の利用に関する独占禁止法上の指針（公正取引委員会）

https://www.jftc.go.jp/dk/guideline/unyoukijun/chitekizaisan.html

知的財産のうち技術に関するものを対象として、技術の利用に係る制限行為に対する独占禁止法の適用に関する考え方を包括的に明らかにした指針。本書第２章２－２「秘密情報の決定」における技術情報の活用方法を検討する際に参考になります。

■個人情報の保護に関する法律についてのガイドライン（通則編）（個人情報保護委員会）

https://www.ppc.go.jp/files/pdf/210101_guidlines01.pdf

事業者が個人情報の保護に関する法律に基づき、個人情報の適切な取扱いの確保に関して行う活動を支援し、この支援により事業者が講ずる措置が適切かつ有効に実施されることを目的として、事業者の理解を助ける具体的な指針として定められています。このほか、~~（なお、従来、公表されていた「個人情報の保護に関する事業分野ごとのガイドライン」に代えて、~~金融、~~信用、債権回収業、~~医療、~~郵便分野~~情報通信等の特定分野ガイドラインが~~公表さ~~定められ~~ています。）。

本書第２章２－２「秘密情報の決定」を検討する際に参考になるほか、本ガイドラインの「（別添）講ずべき安全管理措置の内容」は、第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」及び第４章「秘密情報管理に係る社内体制のあり方」を検討する際に参考になります。

■特定個人情報の適正な取扱いに関するガイドライン（事業者編）（個人情報保護委員会）

~~https://www.ppc.go.jp/files/pdf/my_number_guideline_jigyosha.pdf~~https://www.ppc.go.jp/files/pdf/2307_my_number_guideline_jigyosha.pdf

行政手続における特定の個人を識別するための番号の利用等に関する法律に基づき、より厳格な管理が求められる個人番号（いわゆるマイナンバー）をその内容に含む個人情報（特定個人情報）の適正な取扱いを確保するための具

体的な指針として定められています。
　前掲の「個人情報の保護に関する法律についてのガイドライン（通則編）」とともに、本書を検討する際に参考になります。

【第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】

■情報セキュリティ関係

(1) 組織における内部不正防止ガイドライン
（独立行政法人情報処理推進機構（ＩＰＡ））

https://www.ipa.go.jp/security/guide/insider.html

　組織において、内部不正による情報セキュリティ事故を防止するためのガイドライン。第３章３－４「具体的な情報漏えい対策例」の情報システム関連の対策については、本ガイドラインも参考にしています。

(2) ＩＳＭＳ関係（JISQ27001、JISQ27002）

①JISQ27001

　情報セキュリティマネジメントシステム（ISMS）は、組織のマネジメントとして情報の機密性、完全性、可用性を維持することを目的としており、JISQ27001 は、ISMS を実施する際の要求事項等を定めたものです。情報セキュリティマネジメントの観点から情報漏えい対策を検討する場合や、取引先の漏えい対策の状況を確認する際に参考になります。
　また、ISMS の認証を行う ISMS 適合性評価制度が運用されており、一般社団法人マネジメントシステム認定センター（ISMS-AC）から認定された「認証機関」に申請することで認証を受けることができます。

ISMS 適合性評価制度（ISMS-AC）
https:/isms.jp/isms.html

②情報セキュリティ管理基準（経済産業省）、情報セキュリティ監査制度

　JIS Q 27001 のほかに「情報セキュリティ管理策の実施のための規範（ベストプラクティス）」として、JIS Q 27002 が策定されています。これらに基づいて、マネジメント基準や技術基準など具体的な管理策をまとめた「情報セキュリティ管理基準」が経済産業省より公開されており、ISMS 認証取得を目指している組織、独自に情報セキュリティマネジメントの確立を検討している組織、情報セキュリティ監査を実施する組織等幅広い利用者を想定して情報セキ

ュリティマネジメントの基本的な枠組みと具体的な管理項目を規定。

情報セキュリティ監査制度、情報セキュリティ管理基準（経済産業省）
http://www.meti.go.jp/policy/netsecurity/index.html

~~(3) ＩＰＡ対策のしおりシリーズ（ＩＰＡ）~~
~~http://www.ipa.go.jp/security/antivirus/shiori.html~~
~~一般のご家庭や企業・組織の方々を対象に、情報セキュリティ上の様々な脅威への対策をテーマ別（ウィルス対策、不正アクセス対策、情報漏えい対策、インターネット利用時の危険対策、標的型攻撃メール対策、暗号化による対策等）に分かり易く説明した小冊子シリーズ。情報セキュリティ上の対策を検討する際に参考になります。~~

(43) 映像で知る情報セキュリティ（ＩＰＡ）
脅威や対策を学ぶための映像コンテンツを ~~YouTube の「IPA channel(ipa.jp)」で~~公開しています。
https://www.ipa.go.jp/security/videos/list.html
情報漏えいに関する映像は次の 2 点です。
① 情報を漏らしたのは誰だ？　～内部不正と情報漏えい対策～(11 分)
https://www.youtube.com/watch?v=5Z_10h2aA8c
② 3 つのかばん　～新入社員が知るべき情報漏えいの脅威～（11 分）
https://www.youtube.com/watch?v=FljLaQA-cRU

(54) 中小企業の情報セキュリティ対策ガイドライン（ＩＰＡ）
https://www.ipa.go.jp/security/keihatsu/sme/guideline/index.html
情報セキュリティ対策に取り組む際の、(1)経営者が実施すべき指針、(2)社内において対策を実践する際の手順や手法をまとめたガイドラインです。経営者編と実践編から構成され、個人事業主・小規模事業者を含む中小企業の利用を想定しています。

(65) サイバーセキュリティお助け隊サービス制度（ＩＰＡ）
https://www.ipa.go.jp/security/sme/otasuketai-about.html
~~https://www.ipa.go.jp/security/keihatsu/sme/otasuketai/index.html~~
中小企業に対するサイバー攻撃への対処支援サービスに不可欠なサービスを要件としてまとめた~~向けのセキュリティサービスが満たすべき基準~~「サイバーセキュリティお助け隊サービス基準」を示し、基準を満たす民間の~~セキ~~

~~ュリティ~~サービスを登録・公表する制度です。中小企業において、（~~5~~ 4）等を参考にしながら、外部サービスの活用を含めた対応をご検討される際には、こちらのセキュリティサービスの活用もご検討ください。
（ユーザー向けウェブサイト）https://www.ipa.go.jp/security/otasuketai-pr/

【第４章　秘密情報の管理に係る社内体制のあり方】

■サイバーセキュリティ経営ガイドライン（経済産業省、ＩＰＡ）

https://www.meti.go.jp/policy/netsecurity/mng_guide.html

情報システムの専門部署を持ち、IT を利活用する企業の経営者を対象として、サイバー攻撃から企業を守る観点で、経営者が認識する必要がある「３原則」及び経営者が担当幹部（ＣＩＳＯ等）に指示すべき「重要１０項目」をまとめたもの。秘密情報の管理に係る社内体制を検討する際に参考になります。

■サイバーセキュリティ経営可視化ツール（ＩＰＡ）

https://www.ipa.go.jp/security/economics/checktool.html

サイバーセキュリティ対策の実践状況をセルフチェックするためのツール（ウェブサービス）です。「サイバーセキュリティ経営ガイドライン Ver2.0」をベースにしており、自社の対策状況を定量的に可視化することができます。

■技術情報管理認証制度（ＴＩＣＳ）（経済産業省）

https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/index.html

産業競争力の源泉となる技術情報等の適切な内部管理体制の構築及び適切な管理下での技術情報等の取引の活性化を目的に、事業者の保有する重要な技術情報等の管理体制について、国が認定した第三者機関が認証する制度（平成３０年改正産業競争力強化法により創設）。

事業者の保有する技術等（デジタル情報、金型や完成品などの物自体、製造プロセスやノウハウ、研究開発の成果等を含みます。）のうち適切に管理するべ

き重要なものを特定した上で、その管理方法や内部管理体制等を、第三者機関が審査し認証~~認定~~を付与します。

【第５章　他社の秘密情報に係る紛争への備え】

■先使用権制度の円滑な活用に向けて－戦略的なノウハウ管理のために－（第２版）（特許庁）

~~https://www.jpo.go.jp/shiryou/s_sonota/senshiyouken.htm~~https://www.jpo.go.jp/system/patent/gaiyo/senshiyo/document/index/senshiyouken_2han.pdf

先使用権制度の明確化と先使用権の立証手段の具体化を図り、先使用権制度がより円滑に活用されることを目的に、有識者による委員会での議論の結果を踏まえて、特許庁が作成し公表したもの。

第三章中の「証拠力を高めるための具体的な手法の紹介」では、公証制度、タイムスタンプが紹介されており、本書第５章５－１「自社情報の独自性の立証」を検討する際に参考になります。

■知的財産取引に関するガイドライン・契約書のひな形（中小企業庁）

https://www.chusho.meti.go.jp/keiei/torihiki/chizai_guideline.html

大企業と中小企業との適正な知的財産取引を推進し両者の共存共栄を図るため、有識者による検討会での議論を踏まえ、中小企業庁が作成し公表したもの。知的財産取引における問題事例やあるべき姿が、取引の段階に応じ示されている。

また、知的財産取引を行うに当たり注意すべきポイントをまとめたものとして、ガイドラインとあわせて契約書のひな形も公表されている。秘密保持契約を含め４種類のひな形が示されており、秘密保持義務を中心に紹介している「参考資料２　各種契約書等の参考例」とあわせて、契約の内容を検討する上で参考になります。

【第６章　漏えい事案への対応】

■高度サイバー攻撃への対処におけるログの活用と分析方法

（一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC））

https://www.jpcert.or.jp/research/apt-loganalysis.html

企業の情報セキュリティにおけるインシデントの対処に対して、情報漏えい事案の調査や、解析に資するログの活用と分析方法について解説したも

の。情報漏えい事案に対応する調査分析方法等を検討する際に参考になります。

■侵入型ランサムウェア攻撃を受けたら読む FAQ（一般社団法人 JPCERT/CC）

https://www.jpcert.or.jp/magazine/security/ransom-faq.html

企業や組織の内部ネットワークに攻撃者が「侵入」した後、情報窃取やランサムウェアを用いたファイルの暗号化などを行う攻撃の被害に遭った場合の対応のポイントや留意点などを FAQ 形式で記載したもの。ランサムウェアの分類や攻撃者による情報の扱われ方について参考になります。

■CSIRT マテリアル（一般社団法人 JPCERT/CC）

https://www.jpcert.or.jp/csirt_material/

企業の情報セキュリティにおけるインシデントに対して迅速に対応する CSIRT(Computer Security Incident Response Team)=「コンピューターセキュリティインシデントに対応するチーム」の構築について解説したもの。情報漏えい事案に対応する組織構築を検討する際に参考になります。

【その他　特定の分野・領域の特性を踏まえた対応】

■農業分野における営業秘密の保護ガイドライン
（公益社団法人農林水産・食品産業技術振興協会（JATAFF））

https://pvp-conso.org/842/

農業分野における優れた栽培・飼養技術やその他のノウハウ等（以下、「技術・ノウハウ等」）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んでいただく際の留意点等をわかりやすくまとめたもの。

ガイドラインの中では、農業の現場において実際に技術・ノウハウ等を営業秘密として保護するために具体的に何をしたらよいかを簡単に確認できるマニュアルに加え、農業分野の特殊性を踏まえた理論的な整理や参考となる取組事例も掲載しています。

■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/yuuryou.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。

参考資料５

競業避止義務契約の有効性について

１．　はじめに

本参考資料は、平成２４年度経済産業省委託調査「人材を通じた技術流出に関する調査研究」の有識者による委員会において、関連する５０以上の判例をもとに討議を行い、とりまとめられた報告書をもとにしたものである。

同報告書では、競業避止義務契約のみならず退職金や年金の支給制限についても、判例をもとに分析･検討を行っている。

このうち、競業避止義務契約の有効性の判断について記載された章（本編　Ⅳ．競業避止義務契約が有効であると判断される基準）を抜粋し、参考資料として紹介する。

なお、報告書全文については下記アドレスにて公開しているので、参照されたい。

「平成２４年度　人材を通じた技術流出に関する調査研究」本編

http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/honpen.pdf

また、同報告書が公表後から今日に至るまでの間にも、競業避止義務（就業規則･契約祖･誓約書）に関する判例は存在しており、特に、営業秘密侵害を巡る争いの中（２２件）のうち競業避止義務についても判断されたもの（５件）について、令和２年度ＩＰＡ調査「企業における営業秘密管理に関する実態調査２０２０」報告書の裁判例調査が記載された箇所（２．実態調査の概要　２．５．２　裁判例に関する調査結果一覧）に~~一覧として~~とりまとめられている。

この報告書全文については下記アドレスにて公開されているので、あわせて参照されたい。

「企業における営業秘密管理に関する実態調査２０２０」報告書

https://www.ipa.go.jp/security/reports/economics/ts-kanri/20210318.html

２．　競業避止義務契約が有効であると判断される基準

在職中の競業行為が認められないことはもちろんだが、退職後について競業避止義務を課すことについては、職業選択の自由を侵害し得ること等から、制限的に解されていることは事実である。この点、古い判例ながら今日においてもしばしば参照されている判例（奈良地判 S45.10.23）は競業避止義務契約について、「債権者の利益、債務者の不利益及び社会的利害に立って、制限期間、場所的職種的範囲、代償の有無を検討し、合理的範囲において有効」であるとしている。

このように競業避止義務契約の有効性について争いとなった判例においては、多面的な観点から競業避止義務契約を締結することの合理性や契約内容の妥当性等を判断しており、近年の判例における判断のポイントについて理解しておくことは、競業避止義務契約の導入・見直しを検討する上で重要である[64]。

（１）競業避止義務契約の有効性判断

- 競業避止義務契約が労働契約として、適法に成立していることが必要。
- 判例上、競業避止義務契約の有効性を判断する際にポイントとなるのは、①守るべき企業の利益があるかどうか、①を踏まえつつ、競業避止義務契約の内容が目的に照らして合理的な範囲に留まっているかという観点から、②従業員の地位、③地域的な限定があるか、④競業避止義務の存続期間や⑤禁止される競業行為の範囲について必要な制限が掛けられているか、⑥代償措置が講じられているか、といった項目である。

ここでは、退職後の競業避止義務契約について具体的な検討、判断を行っている判例のうち、競業避止義務契約の具体的な内容について判断を行なっている判例について整理を行なった。

判例は、①守るべき企業の利益があるかどうか、①を前提として競業避止義務契約の内容が目的に照らして合理的な範囲に留まっているかという観点から、②従業員の地位が、競業避止義務を課す必要性が認められる立場にあるものといえるか、③地域的な限定があるか、④競業避止義務の存続期間や⑤禁止される競業行為の範囲について必要な制限が掛けられているか、⑥代償措置が講じられているか、といった項目について判断を行なっており、規定自体の評価及び当該競業避止義務契約の有効性判断を行なっている。

[64] もっとも判例自体は個別性が強いため、どのような規定ぶりであれば競業避止義務契約が有効となるか、については一概に言えない点には留意を要する。

企業側に守るべき利益があることを前提として、競業避止義務契約が過度に職業選択の自由を制約しないための配慮を行い、企業側の守るべき利益を保全するために必要最小限度の制約を従業員に課すものであれば、当該競業避止義務契約の有効性自体は認められると考えられる。

【競業避止義務契約の具体的な内容について判断を行なっている判例】

	競業避止義務契約の形態	有効性判断のポイント						⑦有効性の判断	備考
		①企業の利益	②従業員の地位	③地域的限定	④期間	⑤禁止行為の範囲	⑥代償措置		
東京高判 H24.6.13 ☆	誓約書（在職時）	●	●		●	●	●	●	
東京地判 H24.1.13 ☆		△	●	●	● 2年	●	●	●	目的に一応の正当性が認められるものの、本事案の事情のもとでは目的の正当性を過大視することはできないとされた。
大阪地判 H24.3.15	就業規則		●	●	● 2年	●	●	●	6ヶ月は場所的制限なし。6ヶ月～2年は場所的制限あり。
東京地判 H24.3.13	就業規則＆誓約書（入社時）	●	－		－	－	●	●	労働者が元使用者の業務上の秘密を使用する立場になく競業禁止の前提を欠くこと及び代償措置が無いことをもって効力を否定。
東京地判 H24.1.23	誓約書（退職時）	○	○	●	● 5年	●	●	●	
大阪地判 H23.3.4 ☆	就業規則				● 1年	－	●	●	
大阪地決 H21.10.23	就業規則	○			○ 1年	○	○	○	
東京地判 H22.10.27	誓約書（退職時）	○	○		○ 3年	－	／	○	

東京高判 H22.4.27 ☆	就業規則	△			－	△	●	△	限定解釈により限定的に有効とした上で、問題となった行為については限定された範囲を外れているとして違反を否定（控訴審）。
東京地判 H21.11.9 ☆	就業規則	●		●	○ 1年	●	●	●	
東京地判 H20.11.18[65]	誓約書（退職時）	○	○				○	○	独立支援制度の存在と厚遇措置が代償措置として認められた。
東京地判 H19.4.24	誓約書（退職時）	○	○	○	○ 1年	○	●	○	
東京高判 H15.12.25	誓約書（締結時期不明）	○			○ 6月		○	○	
東京地判 H14.8.30	就業規則＆誓約書（在職時）	○		○	○ 2年	○	●	○	
大阪地判 H8.12.25		△		－	－	－	●	●	規定の適用範囲を限定的して義務違反を否定した事案。
東京高判 H12.7.12	誓約書（入社時）	○			○ 6月	○		○	義務違反は認められたが義務違反と因果関係のある損害が認められず請求棄却。
東京地判 H11.10.29	誓約書（入社時）	○			○ 6月	○		○	同上
東京地判 H.6.9.29	誓約書（退職時）				○ 1年	○	／	○	

※○：肯定的に判断、●：否定的に判断、△：判断が実質的になされていない又は不明確

－：規定は存在するが判例中に判断なし

／：代償措置の定めはないが、その点について特段の言及なし

空欄：そもそも規定なし又は不明

※☆：退職金減額又は不支給が争われる中で、競業避止義務の定めの効力が問題となっている事案

なお、競業避止義務については就業規則に規定を設けている事例と、個別の誓約書において規定を設けている例があるが、就業規則に規定を設け、かつ、規定した内容と異なる内容の個別の誓約書を結ぶことについては、就業規則に定める基準に達しない労働条件

[65] なお、本件の控訴審判決である東京高判 H21.5.27 では、「退職する従業員の職業選択の自由、営業の自由の点をも斟酌すると、〔本件競業避止義務契約において、利用して事業を営むことが禁止される〕機密事項には、被控訴人（注：元使用者）以外の者からも容易に得られるような知識又は情報は……含まれないと解するのが相当である」ところ、本件における元使用者の技術等は、このような機密事項に該当すると認められないため、競業避止義務契約の有効性について判断するまでもなく、同義務の違反は認められないとの判断がなされている。

を定める契約の効果を無効とする労働契約法 12 条との関係が問題となる。もっとも実務上は、就業規則には「従業員は在職中及び退職後 6 ヶ月間、会社と競合する他社に就職及び競合する事業を営むことを禁止する」というような原則的な規定を設けておき、加えて、就業規則に、例えば「ただし、会社が従業員と個別に競業避止義務について契約を締結した場合には、当該契約によるものとする」というように、個別合意をした場合には個別合意を優先する旨規定しておけば、労働契約法 12 条の問題は生じず、規則の周知効果を狙うという観点からも記載をしておくべきであると考えられる。

就業規則の規定例

（競業避止義務）

第○○条

従業員は在職中及び退職後 6 ヶ月間、会社と競合する他社に就職及び競合する事業を営むことを禁止する。ただし、会社が従業員と個別に競業避止義務について契約を締結した場合には、当該契約によるものとする。

個別合意の例（誓約書の例）

貴社を退職するにあたり、退職後 1 年間、貴社からの許諾がない限り、次の行為をしないことを誓約いたします。

1）貴社で従事した○○の開発に係る職務を通じて得た経験や知見が貴社にとって重要な企業秘密ないしノウハウであることに鑑み、当該開発及びこれに類する開発に係る職務を、貴社の競合他社（競業する新会社を設立した場合にはこれを含む。以下、同じ。）において行いません。

2）貴社で従事した○○に係る開発及びこれに類する開発に係る職務を、貴社の競合他社から契約の形態を問わず、受注ないし請け負うことはいたしません。

（２）競業避止義務契約の判断ポイント

① 企業側の守るべき利益

- ■ 企業側の守るべき利益は、不正競争防止法上の「営業秘密」に限定されない。
- ■ 営業秘密に準じるほどの価値を有する営業方法や指導方法等に係る独自のノウハウについては、営業秘密として管理することが難しいものの、競業避止によって守るべき企業側の利益があると判断されやすい傾向がある。

企業側の守るべき利益については、不正競争防止法によって明確に法的保護の対象と

される「営業秘密」はもちろんだが、個別の判断においてこれに準じて取り扱うことが妥当な情報やノウハウについては、競業避止義務契約等を導入してでも守るべき企業側の利益と判断している。

判例の中で争われた事例を見ると、技術的な秘密や、営業上のノウハウ等に係る秘密（教授法など顧客に対するサービスの手法も含む）、顧客との人的関係等について、企業の利益の有無が判断されている。

本報告書で紹介している判例の中には、技術的な秘密について企業の利益の有無が判断されているものは少ないが、めっき加工や金属表面処理加工について、めっき技術訓練学校の教科書の記述やめっき事業者各社のホームページの記載等と比較して、法的保護に値する独自のノウハウが存することを主張して、一応の疎明がなされていると判断された事案がある（大阪地決 H21.10.23）[66]。

営業秘密に準じるほどの価値を有する営業方法や指導方法等に係る独自のノウハウについては、営業秘密として管理することが難しいものの、競業避止によって守るべき企業側の利益があると判断されやすい傾向がある（例えばヴォイストレーニングを行うための指導方法・指導内容及び集客方法・生徒管理体制についてのノウハウ、デントリペア及びインテリアリペアの各技術の内容及びこれをフランチャイズ化したノウハウ、店舗における販売方法や人事管理のあり方等について企業側の利益があると判断した判例が見られる）。

また判例の中には顧客との人的関係等について判断を行なったものも見られ、多数回にわたる訪問説明、長期間の地道な営業活動を要するような場合であって、人的関係の構築が当該企業の信用や業務としてなされたものである場合には、企業側の利益があると判断されやすい。

【有効性が認められたもの】

- めっき技術訓練校の教科書の記述やめっき事業者各社のホームページの記載等からすると、「債

[66] 本訴では、めっき加工を業とする会社が複数存在し、同種の製品を加工等していること、具体的な技術内容等に関する基本的な事項については、書籍等で広く流布されていること、各製品に関する情報をノートに記載しているものの、その内容が被告企業の指揮命令に基づくものではないこと、当該ノートの記載事項によらなくても基本的な教科書の記載に沿って作業することが可能であること、当該ノートの保管方法や取扱いについて特段注意等がなかったこと、簡単な品物については外注していたこと、等から独自のノウハウが秘密保持契約によって保護されるべき対象とならないと判断している（大阪地判 23.3.4）。しかし、逆に書籍等によって広く流布されていない技術・ノウハウであって、一般的に流布している情報では再現出来ないこと、指揮命令に基づいて技術・ノウハウの要点を書面にまとめ、これを秘密として管理していること、これを独自の技術・ノウハウとして外注先等に開示していないこと、等の要件が満たされている場合には、企業の利益があると判断される可能性が高い。

権者については、めっき加工や金属表面処理加工について、法的保護に値する独自のノウハウが存し、競業避止を必要とする正当な利益が存在することについて、一応の疎明がなされていると認められる。」と判示。（大阪地決 H21.10.23）

- 「ヴォイストレーニングを行うための指導方法・指導内容及び集客方法・生徒管理体制についてのノウハウ」は、原告の代表者によって「長期間にわたって確立されたもので独自かつ有用性が高い」と判断。（東京地判 H.22.10.27）
- 「デントリペア及びインテリアリペアの各技術の内容及びこれをフランチャイズ化したところに原告の独自性があるということができ」、これらは不正競争防止法上の営業秘密には厳密にはあたらないが、「それに準じる程度には保護に値するということができ」、「競業禁止によって守られる利益は、要保護性の高いものである」と判断。（東京地判 H20.11.18）
- 「店舗における販売方法や人事管理の在り方」や「全社的な営業方針、経営戦略等」の「知識及び経験を有する従業員が、（原告を）退職した後直ちに、（原告の）直接の競争相手である家電量販店チェーンを展開する会社に転職した場合には、その会社は当該従業員の知識及び経験を活用して利益を得られるが」、「その反面、（原告が）相対的に不利益を受けることは容易に予想されるから、これを未然に防ぐことを目的として被告のような地位にあった従業員に対して競業避止義務を課することは不合理でない」と判断。（東京地判 H19.4.24）
- 「商店会等に対する街路灯の営業は、成約までに長時間を要し、契約を取るためには、その間に営業担当の従業員が商店会等の役員等をたびたび訪問して、その信頼を得ることが重要であること、そのため、この種の営業においては、長期間経費をかけて営業してはじめて利益を得ることができるから、このような営業形態を採っている（元使用者）においては、従業員に退職後の競業避止義務を課する必要性が存する」と判断。（東京高判 H12.7.12、東京地判 H11.10.29）
- 秘密保持義務契約の効力判断中で、原告の「『顧客の名簿及び取引内容に関わる事項』並びに『製品の製造過程、価格等に関わる事項』」は、個別レンタル契約を経営基盤の一つにおいている原告にとって、経営の根幹に関わる重要な情報であると判断し、結論としても契約の効力を肯定した上で、「退職後の競業避止義務は、秘密保護の必要性が当該労働者が秘密を開示する場合のみならず、これを使用する場合にも存することから、秘密保持義務を担保するものとして容認できる場合がある」と肯定的に評価した。（東京地判 H14.8.30）

【有効性が否定されたもの】

- 「ここでいうノウハウとは、不正競争防止法上の営業秘密に限らず、原告が被告業務を遂行する過程において得た人脈、交渉術、業務上の視点、手法等であるとされているところ、これらは、原告がその能力と努力によって獲得したものであり、一般的に、労働者が転職する場合には、多かれ少なかれ転職先でも使用されるノウハウであって、かかる程度のノウハウの流出を禁止しようとすることは、正当な目的であるとはいえない。」「顧客情報の流出防止を、競合他社への転職自体を禁止することで達成しようとすることは、目的に対して、手段が過大であ

る」とした。（東京地判 H24.1.13、東京高判 H24.6.13）

- 秘密保持義務を定める就業規則や個別の合意で同義務の対象となる業務上の秘密の内容が具体的に定められていなかった事案において、このような場合には同義務の対象となる秘密事項については少なくとも秘密管理性と非公知性の要件が求められるところ、本件で問題となった廃プラスチックの仕入れ先等に関する情報は秘密管理性を欠き、秘密保持義務の対象に当たらないので同義務違反は成立しないとの判断をした上で、競業避止義務契約の効力について、上記で判断したところによれば、被告（労働者）らは原告での業務遂行過程において業務上の秘密を使用する立場にあったわけではないため、そもそも競業を禁ずべき前提条件を欠くと判断した。（東京地判 H24.3.13）
- 一般に、使用者にとって獲得した顧客との人的関係を維持することは競業避止義務契約の設定における正当な目的の一つといえるが、本件においては、被告 H2 が原告入社に当たって入社以前に自己の顧客となった者の一部を引き継いできたこともあって、原告における 3 次元ＣＡＤ業務の売り上げが被告の入社後に飛躍的に伸びていること等から、同業務の受注には被告と「顧客との個人的信頼関係が大きく影響したものと推認される」とする一方、「顧客の開拓がもっぱら原告の投下資本によるものと認めるに足りる証拠は見当たらない」として、競業避止義務契約設定の目的には一応の正当性が認められるものの、本件ではこれを過大視することは出来ないとした。（東京地判 H24.1.23）
- もっぱら特定の企業への転職を禁止することを目的とした競業避止義務契約を締結していたケースにおいて、守るべき企業の利益が営業秘密であったとしても、他の企業への転職が禁止されていないことからみて、当該情報は原告会社にとってそれほど要保護性の高いものではないといわざるを得ないと判断した。（東京地判 H21.11.9）
- 「退職した従業員に対し、一定期間競業避止義務を課すことは、従来の取引先の維持という点で意味がある。しかし、このような従業員と取引先との信頼関係は、従業員が業務を遂行する中で形成されていくもので、従業員が個人として獲得したものであるから、営業秘密といえるような性質のものではない。また、このような従業員と取引先との個人的信頼関係が業務の受注に大きな影響を与える以上、使用者としても、各種手当を支給するなどして、従業員の退職を防止すべきである」とした上で、本件では、十分な代償措置が講じられていないこと、退職した従業員によって営業上の秘密が他の企業に漏れたわけではないこと等からすれば、競業避止義務規定は本件における退職従業員には適用されないと判断した。（大阪地判 H8.12.25）

② 従業員の地位

■ 合理的な理由なく、従業員すべてを対象にした規定はもとより、特定の職位にある者全てを対象としているだけの規定は合理性が認められにくい。
■ 形式的な職位ではなく、具体的な業務内容の重要性、特に使用者が守るべき利益との関わりが判断されている。

従業員の地位について判断を行なった判例では、形式的に特定の地位にあることをもって競業避止義務の有効性が認められるというよりも、企業が守るべき利益を保護するために、競業避止義務を課すことが必要な従業員であったかどうかが判断されていると考えられる。例えば、形式的には執行役員という比較的高い地位にある者を対象とした競業避止義務であっても、企業が守るべき秘密情報に接していなければ否定的な判断を行っている判例もある。

【有効性が認められたもの】

- 原告は、「指導方法及び指導内容等についてノウハウを伝授されたのであるから、本件競業避止合意を適用して原告の上記ノウハウを守る必要があることは明らかであり、被告が週 1 回のアルバイト従業員であったことは上記判断〔競業避止義務契約の合理性、有効性が認められること〕を左右するものではない」と判断。（東京地判 H22.10.27）
- 「被告の従業員としての地位も、インストラクターとして秘密の内容を十分に知っており、かつ、原告が多額の営業費用や多くの手間を要して上記技術を取得させたもので、秘密を守るべき高度の義務を負うものとすることが衡平に適うといえる。」と判断。（東京地判 H20.11.18）
- （地区部長、母店長、店長、理事を経験し、原告の全社的な営業方針、経営戦略等を知ることができた被告につき）「（被告のような）地位にあった従業員に対して競業避止義務を課することは不合理でない」と判断。（東京地判 H19.4.24）

【有効性が否定されたもの】

- 従業員数 6,000 人の日本支店において 20 人しかいない執行役員で役員会の構成員である高い地位にあったが、「保険商品の営業事業はそもそも透明性が高く秘密性に乏しいし、また、役員会においては、被告の経営上に影響がでるような重要事項については、例えば決算情報が 3 週間部外秘とされるといった時限性のある秘密情報はあるが、原告が、それ以上の機密性のある情報に触れる立場にあったものとは認められない」と判断（東京地判 H24.1.13）。控訴審でも職務の実態は取締役に類する権限や信認を付与されるものではなかったという判断をしている。（東京高判 H24.6.13）

③ 地域的限定

■ 地域的限定については、使用者の事業内容や、職業選択の自由に対する制約の程度、特に禁止行為の範囲との関係を意識した判例が見られる。
■ 地理的な制限がないことのみをもって競業避止義務契約の有効性が否定されている訳ではない。

地域的限定について判断を行なっている判例は少ないが、争われている場合には業務の性質等に照らして合理的な絞込みがなされているかどうかという点が問題とされている。地域的な限定がされていない場合については、他の要素と併せて否定的な判断がなされている例が散見されるが、地理的な制限が規定されていない場合であっても、使用者の事業内容（特に事業展開地域）や、職業選択の自由に対する制約の程度、特に禁止行為の範囲との関係等と総合考慮して競業避止義務契約の有効性が認められている場合もあり、判例は地理的な制限がないことのみをもって競業避止義務契約の有効性を否定しない傾向があるといえる。

【有効性が認められたもの】

- 「地理的な制限がないが、（原告が）全国的に家電量販店チェーンを展開する会社であることからすると、禁止範囲が過度に広範であるということもない」と判断。（東京地判 H19.4.24）
- 誓約書による退職後の競業避止義務の負担は「在職時に担当したことのある営業地域（都道府県）並びにその隣接地域（都道府県）に在する同業他社（支店、営業所を含む）という限定された区域におけるものである（隣接都道府県を超えた大口の顧客も存在しうることからすると、やむを得ない限定の方法であり、また「隣接地域」という限定が付されているのであるから、無限定とまではいえない）」と判断。（東京地判 H14.8.30）

【有効性が否定されたもの】

- 「本件誓約書における競業避止義務においては、退職後 6 か月間は場所的制限がなく、また 2 年間は在職中の勤務地又は『何らかの形で関係した顧客その他会社の取引先が所在する都道府県』における競業及び役務提供を禁止しているところ、原告在職中に九州及び関東地区の営業マネージメントに関与していた被告Ｂについては、少なくとも退職後 2 年間にわたり、九州地方及び関東地方全域において、原告と同種の業務を営み、又は、同業他社に対する役務提供ができないことになり、被告Ｂの職業選択の自由の制約の程度は極めて強い」と判断。（東京地判 H24.3.15）
- 地域の限定がない。（東京地判 H24.1.23）

④ 競業避止義務期間

■ 1年以内の期間については肯定的に捉えられている例が多い。
■ 近年は、2年の競業避止義務期間について否定的に捉えている判例が見られる。

退職後、競業避止義務の存続する期間についても、形式的に何年以内であれば認められるという訳ではなく、労働者の不利益の程度を考慮した上で、業種の特徴や企業の守るべき利益を保護する手段としての合理性等が判断されているものと考えられる。

概して1年以内の期間については肯定的に捉えられている[67]が、特に近時の事案においては、2年の競業避止義務期間については、否定的な判断がなされる例が見られる[68]。

【有効性が認められたもの】

- めっき加工業における事案で、1年間という期間につき仮処分決定に際しては「期間を1年間と限定しており、一応、合理的範囲に限定されている」と判断。（大阪地決 H21.10.23）
- ヴォイストレーニングに係る教育支援業における事案で、指導方法・指導内容及び集客方法・生徒管理体制についてのノウハウは、長期間にわたって確立されたもので独自かつ有用性が高いと判断しており、そのために退職後3年間の競合行為禁止期間も、目的を達成するための必要かつ合理的な制限であると判断。（東京地判 H22.10.27）
- 家電量販店に係る事案で、「知識及び経験を有する従業員が、（原告を）退職した後直ちに、（原告の）直接の競争相手である家電量販店チェーンを展開する会社に転職した場合には、その会社は当該従業員の知識及び経験を活用して利益を得られるが」、「その反面、（原告が）相対的に不利益を受けることは容易に予想される」という競合禁止目的に係る判断を前提として、退職後1年という期間は、目的に照らし、「不相当に長いものではない」と判断。（東京地判 H19.4.24）
- 街路灯販売業に係る事案で、守るべき企業の利益が、形成に長期間の地道な営業活動を要する顧客関係であることを前提として、「競業禁止期間6ヶ月と比較的短期間である」と判断。（東京高判 H15.12.25 の原審（DB の収録なし）における判断）
- 訪問型レンタル業に係る事案で、「退職後2年間という比較的短い期間」と判断。（東京地判 H14.8.30）
- 街路灯販売業に係る事案で、「競業禁止の期間は6ヶ月と決して長くない」と判断。（東京地

[67] 近時の判例では、禁止行為の範囲が抽象的であるとして、競業避止義務期間が1年である点を考慮しても、競業避止義務契約の有効性が否定されているものもある（大阪地判 H24.3.9）が、多くはない。

[68] 過去には、2年間の競業避止期間でも有効性が認められているものも多い（東京地判 H14.8.30 など）。

判 H11.10.29）

- コンサル業に係る事案（競業避止義務期間は 1 年）で、「その禁止期間、業務の範囲等に鑑み公序良俗に反すると認めるほどに過度に制約するものではない」と判断。（東京地判 H6.9.29）

【有効性が否定されたもの】

- 保険業における事案で、「保険商品については、近時新しい商品が次々と設計され販売されているころであり（公知の事実）、保険業界において、転職禁止期間を 2 年間とすることは、経験の価値を陳腐化するといえるから（原告本人）、期間の長さとして相当とは言い難い」と判断。（東京地判 H24.1.13、東京高判 H24.6.13）
- 人材派遣業における事案で、「本件誓約書における競業避止義務においては、退職後 6 か月間は場所的制限がなく、また 2 年間は在職中の勤務地又は『何らかの形で関係した顧客その他会社の取引先が所在する都道府県』における競業及び役務提供を禁止しているところ、原告在職中に九州及び関東地区の営業マネージメントに関与していた被告Ｂについては、少なくとも退職後 2 年間にわたり、九州地方及び関東地方全域において、原告と同種の業務を営み、又は、同業他社に対する役務提供ができないことになり、被告Ｂの職業選択の自由の制約の程度は極めて強いものと言わざるをえない」と判断。（大阪地判 H24.3.15）
- 建築資材製造・販売・リース業における事案で「同条項は、１年間という制限はあるものの、一般的抽象的に被告の競業・競合会社（同概念も抽象的一般的であると評価できる。）への入社を禁止しており、被告を退職した従業員に対して過大な制約を強いるものであるといわざるを得ない」と判断。（大阪地判 H24.3.9）[69]
- ソフトウェアの販売・導入支援事業における事案で「禁止期間は 5 年間と長期」と判断。（東京地判 H24.1.23）
- ビル管理業に係る事案で、原審で（１年という）「期間こそ比較的短い」という判断を行なった。（東京地判 H21.11.9）なお、控訴審は期間の長さの妥当性については個別に判断せず、代償措置がないことなどを強調して規定自体が職業選択の自由に対する重大な制約となると判断。（東京高判 H22.4.27）

⑤ 禁止行為の範囲

- ■ 業界事情にもよるが、競業企業への転職を一般的・抽象的に禁止するだけでは合理性が認められないことが多い。
- ■ 業務内容や職種等について限定をした規定については、肯定的に捉えられている。

禁止される競業行為の範囲についても、企業側の守るべき利益との整合性が判断されている。競業行為の定義については競業避止義務契約において定めがあれば、原則としてそれに従うことになるが、契約上、一般的・抽象的にしか定められていない場合には、当

[69] 結論として有効性が否定されているが、競業避止義務期間が１年であること自体は肯定的に評価されている。

該企業と競業関係に立つ企業に就職したり、競合関係に立つ事業を開業したりすることといった一般的な定義に従って考えることとなる。一般的・抽象的に競業企業への転職を禁止するような規定は合理性が認められないことが多い一方で、禁止対象となる活動内容（たとえば在職中担当した顧客への営業活動）や従事する職種等が限定されている場合には、有効性判断において肯定的に捉えられることが多くなる。このような禁止対象となる活動内容や職種を限定する場合においては、必ずしも個別具体的に禁止される業務内容や取り扱う情報を特定することまでは求められていないものと考えられる。例えば在職中に担当していた業務や在職中に担当した顧客に対する競業行為を禁止するというレベルの限定であっても、肯定的な判断をしている判例もある。

【有効性が認められたもの】

- 「競業をしたり、在職中に知り得た顧客との取引を禁じるに留まり、就業の自由を一般的に奪ったりするような内容とはなっていない」と判断。（大阪地決 H21.10.23）
- 「本件競業避止条項の対象となる同業者の範囲は、家電量販店チェーンを展開するという（原告の）業務内容に照らし、自らこれと同種の家電量販店に限定されると解釈することができる」と判断。（東京地判 H19.4.24）
- 「禁じられる職種は、原告と同じマット・モップ類のレンタル事業というものであり、特殊技術こそ要しないが契約獲得・継続のための労力・資本投下が不可欠であり、（訴外会社が）市場を支配しているため、新規開拓には相応の費用を要するという事情がある」。また、「禁じられているのは顧客奪取行為であり、それ以外は禁じられていない」と判断。（東京地判 H14.8.30）
- 競業（営業活動）禁止の対象は「原告在職中に原告の営業として訪問した得意先に限られており、競業一般を禁止するものではない」と判断。（東京高判 H12.7.12、東京地判 H11.10.29）
- 「教育、コンサルティングを担当もしくは勧誘した相手に対し、原告と競合して教育、コンサルティングないしその勧誘をしない」との誓約書につき「その禁止期間、業務の範囲等に鑑み、公序良俗に反すると認めるべきほどに被告の営業活動を過度に制約するものとはいえない」と判断。（東京地判 H6.9.29）

【有効性が否定されたもの】

- 原告が在職中に得たノウハウはバンクインシュアランス業務の営業に関するものであり、「バンクアシュアランス業務の営業にとどまらず、同業務を行う生命保険会社への転職自体を禁止することは、それまで生命保険会社において勤務してきた原告への転職制限として、広範にすぎる」とした。（東京地判 H24.1.13、東京高判 H24.6.13）
- 「本件誓約書における競業避止義務においては、退職後 6 か月間は場所的制限がなく、また 2 年間は在職中の勤務地又は『何らかの形で関係した顧客その他会社の取引先が所在する都道府

県』における競業及び役務提供を禁止しているところ、原告在職中に九州及び関東地区の営業マネージメントに関与していた被告Ｂについては、少なくとも退職後 2 年間にわたり、九州地方及び関東地方全域において、原告と同種の業務を営み、又は、同業他社に対する役務提供ができないことになり、被告Ｂの職業選択の自由の制約の程度は極めて強い」と判断。（大阪地判 H24.3.15）

- 「一般的抽象的に被告の競業・競合会社（同概念も抽象的一般的であると評価できる）への入社を禁止しており、被告を退職した従業員に対して過大な制約を強いるものであるといわざるを得ない」と判断。（東京地判 H24.3.9）
- 被告が長年携わってきた 3 次元ＣＡＤ等の事業について、退職後の被告が自己の顧客又は第三者から業務依頼がなされたときには必ず原告（元使用者）を紹介しなければならず、この場合、紹介に基づく業務で得た粗利益の 20％を紹介料として原告が被告に支払うとの契約〔注：裁判所は「競業避止義務を課したものと解される」と判断〕について、「事実上、原告の顧客のみならず新たに獲得される顧客から生じる利益（の 8 割）まで原告が獲得しようとする目的に出たもの」と否定的に判断。（東京地判 H24.1.23）
- 「対象行為も競合他社への就職を広範に禁じており顧客奪取行為等に限定するものではない」と判断。（東京地判 H21.11.9）控訴審では、競業する事業を行うこと及び競業他社への就職を禁止することは職業選択の自由に重大な制約を加えるものとした。（東京高判 H22.4.27）

⑥ 代償措置

- ■ 代償措置と呼べるものが何も無い場合には、有効性を否定されることが多い。
- ■ もっとも必ずしも競業避止義務を課すことの対価として明確に定義された代償措置でなくても、代償措置（みなし代償措置も含め）と呼べるものが存在することについて、肯定的に判断されている。

代償措置については、他の要素と比較して判断により直接的な影響を与えていると思われる事案も少なくなく、裁判所が重視していると思われる要素である。もっとも裁判例を見る限り、複数の要因を総合的に考慮する考え方が主流であり、代償措置の有無のみをもって有効性の判断が行われている訳ではない。

代償措置と呼べるものが存在しないとされた事案では、そのことを理由の一つに挙げて競業避止義務契約の効力が否定されることが多いが、代償措置以外の点で、効力を肯定する方向で考慮される要素が多いときには、結論として効力が肯定される場合もある。

なお、裁判例に現れた事案に置いては、競業避止義務を課すことの対価として明確に定

義された代償措置が存在する例は少ないが、このように明確に定義された措置でなくても、代償措置（みなし代償措置も含め）と呼べるものが存在することについて、肯定的に判断されているケースも少なくない。

このような例として、判例の中には賃金が高額であれば代償措置があったとみなしている例がある[70]。もっとも、その一方で、大手生命保険会社における執行役員の競業避止が問題となった事案（東京地判 H24.1.13、東京高判 H24.6.13）のように、比較的高額な報酬を受け取っていた場合であっても、競業避止義務が課せられた前後で賃金の差がないことなどから競業避止義務に対しての代償措置があったとはいえないと判断している例もある。

【代償措置は不十分であるものの、有効性が認められたもの】

- 「独立支援制度としてフランチャイジーとなる途があること、被告が営業していることを発見した後、原告の担当者が、被告に対し、フランチャイジーの待遇については、相談に応じ通常よりもかなり好条件とする趣旨を述べたこと、が認められ、必ずしも代償措置として不十分とはいえない」として退職後の独立支援制度及び厚遇措置を代償措置として認めた。（東京地判 H20.11.18）
- 「代償措置については、（原告が）役職者誓約書の提出を求められるフロアー長以上の従業員に対し、それ以外の従業員に対し、それ以外の従業員に比して高額の基本給、諸手当を支給しているとは認められるものの、これが競業避止義務を課せられたことによる不利益を補償するに足りるものであるかどうかについては、十分な立証があるとはいいがたい。しかし、代償措置に不十分なところがあるとしても、この点は違反があった場合の損害額の算定に当たり考慮することができるから、このことを持って本件競業避止条項の有効性が失われることはない」と判断。（東京地判 H19.4.24）
- 「代償措置（説明会等、業務進捗の節目毎の奨励金の支給）がある」ことを理由の一つに挙げて競業避止義務を負うことを認めた。（東京高判 H15.12.25）
- 「本件誓約書の定める競業避止義務を被告が負担することに対する代償措置を講じていない」が、「本件誓約書の定める競業避止義務の負担による被告の職業選択の自由を制限する程度はかなり小さいといえ、代償措置が講じられていないことのみで本件誓約書の定める競業避止義務の合理性が失われることにはならない」と判断。（東京地判 H14.8.30）

[70] ここで整理の対象としている判例ではないが、例えば、執行役員の地位にあって相当の厚遇（就任後 5 年間の収入は、2,330 万円～4,790 万円）を受けていたことについて、全てを労働の対価とみなすことは出来ず、競業避止条項に対する代償としての性格もあったと一応認められると判断した例（東京地決 H22.9.30）、報酬は決して安くない額（3 年間の年収は 1,490 万円、1,620 万円、1,400 万円）であること、競業禁止が重要な要素の 1 つであることを明示した雇用契約書を取り交わしていることから、支給した報酬の中には退職後の競業禁止に対する代償も含まれている判断した例（東京地決 H18.5.24）等がある。

【代償措置が不十分であるとして、有効性が否定されたもの】

- 月給 131 万円（別途賞与）が支払われていた事案で「原告の賃金は、相当高額であったものの、本件競業避止条項を定めた前後において、賃金額の差はほとんどないのであるから、原告の賃金額をもって、本件競業避止条項の代償措置として十分なものが与えられていたということは困難である。また、前記認定のとおり、被告においては、金融法人本部の本部長である原告の部下たる者の中に、相当数のより高額な給与の者がいたところ、それらの原告の部下については、特段競業避止義務の定めはないのであるから（証人Ｘ３）、やはり、原告の代償措置が十分であったということは困難である。」と判断。（東京地判 H24.1.13、東京高判 H24.6.13）
- 「競業避止義務等を課される対価として受領したものと認められるに足りるのは月額 3000 円の守秘義務手当のみである」として否定的に判断。（東京地判 H24.3.15）

【代償措置がなく、有効性が否定されたもの】

- 被告らは、「原告での業務遂行過程において、業務上の秘密を使用する立場にあったわけではないから、そもそも競業を禁ずべき前提条件を欠くものであるし、原告は、被告らに対し、何らの代償措置も講じていないのであるから、上記競業避止条項ないし特約は、民法 90 条により無効と認めざるを得ない」と判断。（東京地判 H24.3.13）
- 「制約に見合う代替措置（退職慰労金の支払等）が設けられていたとは認められない」ことを否定的に判断。（東京地判 H24.3.9）
- 「競業避止義務を設定するに当たり、退職金等の支払いはなく（中略）何らかの代償措置が図られた事実は見当たらない」と判断した他、入社時の報酬（月額 30 万円の給与及び成果に応じた賞与）の支払いを受けていた事実及び退職年度の報酬（月額 40 万円の給与及び賞与年間 284 万円）の支払いを受けていた事実も原告における売上の推移から推認される被告の貢献度を考慮すると代償措置とみなすことはできないとも判断。（東京地判 H24.1.23）
- 「確かに、原告らの年収は、比較的高額なものであると認められる」としながらも、年収だけでなく「退職金は支給されるものの、その額は競業避止義務を課すことに比して十分な額であるか疑問がないとはいえない」と判断。（大阪地判 H23.3.4）
- 仮処分では、「年収 660 万以上と低賃金と言い難い」点を持って一応の疎明がなされていると判断された。（大阪地決 21.10.23）
- 代償措置は何ら講じられていない。（東京地判 H21.11.9、東京高判 H22.4.27）
- 「このような従業員と取引先との個人的信頼関係が業務の受注に大きな影響を与える以上、使用者としても、各種手当を支給するなどして、従業員の退職を防止すべきであるが、前記で認定したように、被告」「は、従業員が恒常的に時間外労働に従事していたにもかかわらず、一定額の勤務手当を支給しただけで、労働時間に応じた時間外手当を支給していなかったのであ

るから、十分な代償措置を講じていたとは言えない」。（大阪地判 H8.12.25）

（３）競業避止義務契約の有効性に係るまとめ

上記の検討を踏まえると、競業避止義務契約締結に際して最初に考慮すべきポイント、競業避止義務契約の有効性が認められる可能性が高い規定のポイント、有効性が認められない可能性が高い規定のポイントは次のとおりである。また、手続き上の観点から、労働法との関係におけるポイントについても整理を行なった。

競業避止義務契約締結に際して最初に考慮すべきポイント：

- 企業側に営業秘密等の守るべき利益が存在する。
- 上記守るべき利益に関係していた業務を行っていた従業員等特定の者が対象。

競業避止義務契約の有効性が認められる可能性が高い規定のポイント：

- 競業避止義務期間が 1 年以内となっている。
- 禁止行為の範囲につき、業務内容や職種等によって限定を行っている。
- 代償措置（高額な賃金など「みなし代償措置」といえるものを含む）が設定されている。

有効性が認められない可能性が高い規定のポイント：

- 業務内容等から競業避止義務が不要である従業員と契約している。
- 職業選択の自由を阻害するような広汎な地理的制限をかけている。
- 競業避止義務期間が 2 年超となっている。
- 禁止行為の範囲が、一般的・抽象的な文言となっている。
- 代償措置が設定されていない。

労働法との関係におけるポイント：

- 就業規則に規定する場合については、個別契約による場合がある旨を規定しておく。
- 当該就業規則について、入社時の「就業規則を遵守します」等といった誓約書を通じて従業員の包括同意を得るとともに、十分な周知を行う。

参考資料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

１．はじめに

営業秘密侵害罪に係る刑事訴訟手続において、裁判所等が、営業秘密の内容を秘匿するための措置を実効的かつ適切に講じるためは、秘匿の対象となる営業秘密を保有する被害企業から、検察官に対し十分な協力がなされることが前提となる。

被害企業としても、公訴を提起し公判に立会する検察官との間で協力関係を適切に構築することにより、自らの保有する営業秘密、これに基づく事業活動を守ることができる。

そこで、被害企業が、いつ、どのような協力をすることが役立つかについてイメージしやすいよう、秘匿措置を講じる場合の刑事訴訟手続の一連の流れや秘匿の申出書等の記載例を示すこととする。

営業秘密侵害罪に係る刑事訴訟手続を通じて営業秘密が公となってしまうことを防止するため、不正競争防止法においては、刑事訴訟手続の中で、営業秘密の内容を秘匿するための措置が導入されている。

【不正競争防止法における措置の内容】

① 秘匿決定（第 23 条第 1 項～第 3 項）

裁判所は、被害企業等の申出に応じて、営業秘密の内容を特定させることとなる事項を公開の法廷で明らかにしない旨の決定をすることができる。

なお、第 1 項に基づき被害企業等が当該事件に係る営業秘密について申出を行う場合は、検察官を通じて行わなければならない。

② 呼称等の決定（第 23 条第 4 項）

裁判所は、秘匿決定をした場合には、秘匿決定の対象となった営業秘密の内容を特定させることとなる事項（営業秘密構成情報特定事項）に係る名称等に代わる呼称等を定めることができる。

例えば、営業秘密の内容が、化学反応を起こす温度である「1300℃」である場合には、「1300℃」に代えて、公開の法廷で用いるべき「X℃」といった呼称を定めることができる。

③ 尋問等の制限（第 25 条）

裁判長は、秘匿決定があった場合において、訴訟関係人のする尋問等が営業秘密構成情報特定事項にわたるときは、これを制限することができる。

④ 公判期日外の証人尋問等（第 26 条）

裁判所は、秘匿決定をした場合において、一定の要件が認められるときは、公判期日外において証人等の尋問又は被告人質問を行うことができる。

⑤ 要領記載書面の提示命令（第 27 条）

裁判所は、呼称等の決定や、公判期日外の証人尋問等をするに当たり、検察官

及び被告人又は弁護人に対し、訴訟関係人のすべき尋問等に係る事項の要領を記載した書面の提示を命ずることができる。

⑥　証拠書類の朗読（第 28 条）

秘匿決定があった場合、証拠書類を朗読する際には、営業秘密構成情報特定事項を明らかにしない方法で行わなければならない。

⑥　証拠開示の際の営業秘密の秘匿要請（第 30 条）

検察官又は弁護人は、取調べを請求した証拠書類等を相手方に開示するに当たり、その相手方に対し、営業秘密の内容を特定させることとなる事項を、被告人を含む関係者に知られないようにすることを求めることができる。

上記制度が実効的かつ適切に機能するためには、秘匿措置を講じる裁判所等が、どのような事柄を秘匿する必要があるのか（秘匿すべき範囲）について、十分に把握する必要がある。

しかしながら、当該事件を担当する裁判官等が、秘匿対象たる営業秘密に係る技術分野に精通しているとは限らないことから、裁判所等が秘匿すべき範囲を迅速かつ的確に把握するためには、当該営業秘密の保有者であってその秘匿を希望する被害企業から、できる限り早い段階で、十分かつ適切な情報提供がなされることが望ましい。むしろ、本制度は、被害企業からそのような情報提供がなされることを前提としているということができる。

もっとも、被害企業は、当該事件の被害者であるとはいえ、刑事訴訟手続の当事者ではないこと等から、例えば、秘匿の申出は検察官を通じて行うこととされており、その他の裁判所に対する協力も、実際の手続は検察官と連携しつつ、検察官を通じて行うこととなる。

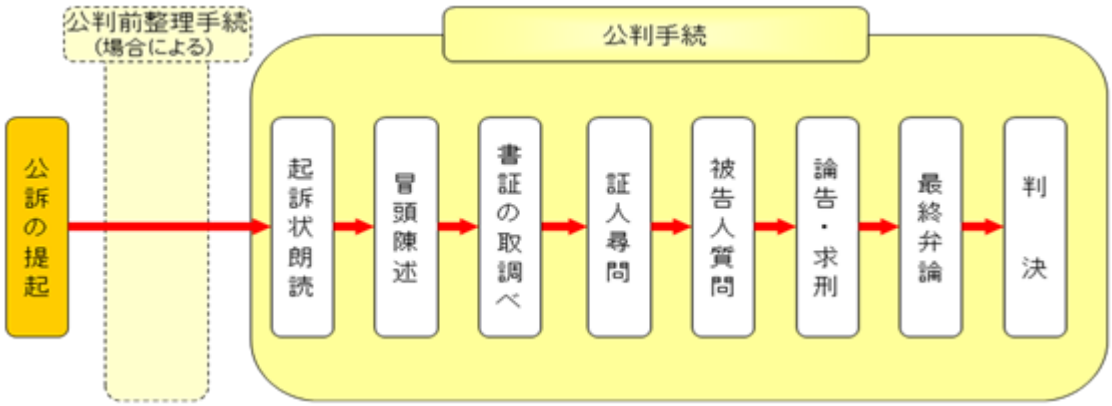
そこで、被害企業がこのような協力を迅速、適切かつ円滑に行えるよう、以下、本制度の概要を説明した上で、被害企業等による秘匿の申出、情報提供等の協力のあり方について、具体的な事例に沿って、秘匿の申出書等の記載例とともに説明することとする。

２．営業秘密侵害罪に係る刑事訴訟手続の流れ

（１）概要

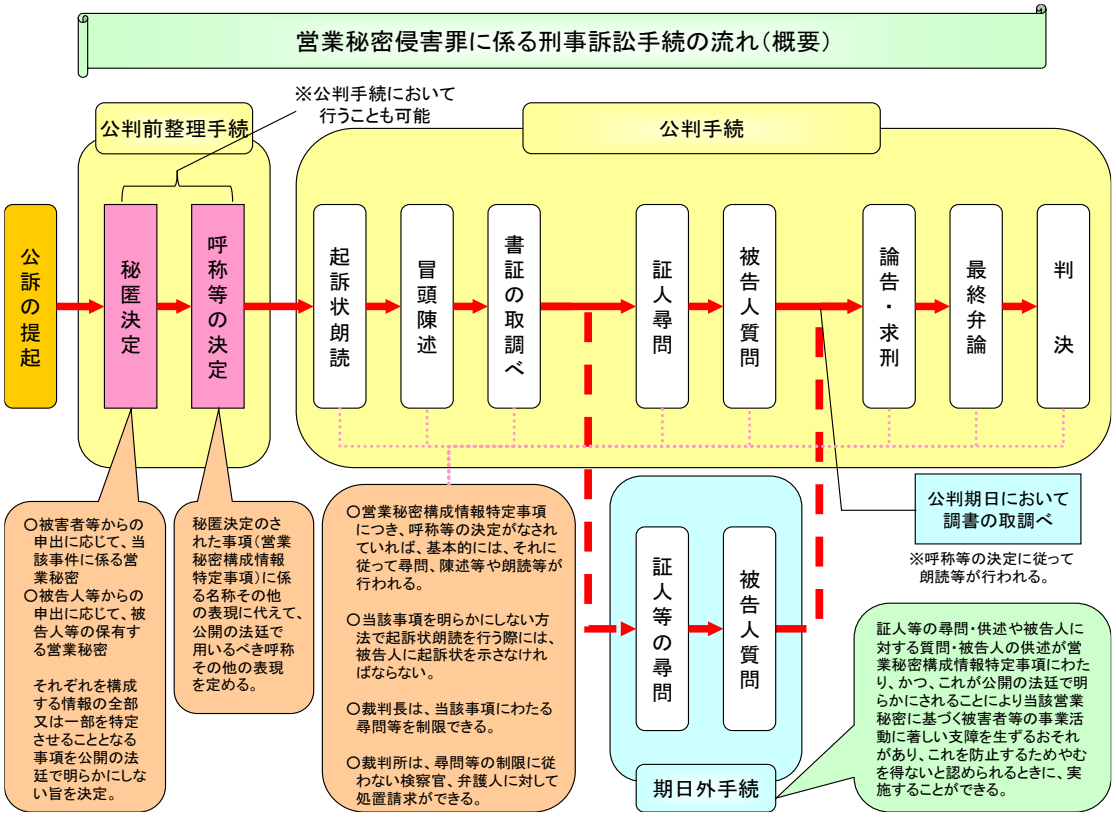
一般的な刑事訴訟手続の流れは、以下のとおりである。

【一般的な刑事訴訟手続の流れ】



営業秘密侵害罪に係る刑事訴訟手続において、営業秘密の内容を秘匿するための措置を講じる場合には、通常、以下のような流れとなることが想定される。

【秘匿措置を講じる場合の刑事訴訟手続の流れ】



（２）具体的な事例に沿って

営業秘密侵害罪に係る刑事訴訟手続において、営業秘密を秘匿するための手続の運用がどのように行われるのかについて、次の事例に沿って紹介する。

第１　事案の概要

被告人は、株式会社Ｘの技術部長Ｗのパソコンに不正にアクセスし、株式会社Ｘの営業秘密である製品Ａの製造方法に関するデータを電子メールで自己所有のパソコンに送信して、営業秘密を取得した（不正競争防止法第２１第１項第１号）。

この営業秘密は、ニッケル・クロム・モリブデン鋼を３０００度で１０分加熱した上で、成型前処理剤「プリ・トリートメント」を混ぜた後、型に入れて成型するという方法により製品Ａを製造するというものである（この事案における「営業秘密」、「営業秘密を構成する情報」、「営業秘密を構成する情報を特定させることとなる事項」、「名称その他の表現」及び（裁判所により定められる）「呼称その他の表現」の関係については、次頁を参照。）。

なお、製品Ａを製造するための公知技術としては、ニッケル・クロム・モリブデン鋼を２０００度で２０分加熱し、薬品Ｐを混ぜることにより強度を増すという方法があるが、この営業秘密に係る方法においては、高価な薬品Ｐに代えて、安価な成型前処理剤「プリ・トリートメント」を用いることにより、強度が高い製品を製造することができる。

【本事例における「営業秘密」、「営業秘密を構成する情報」、「営業秘密を構成する情報を特定させることとなる事項」、「名称その他の表現」及び（裁判所により定められる）「呼称その他の表現」の関係】

<table>
<tr><td colspan="2">営業秘密の概要</td><td colspan="3">ニッケル・クロム・モリブデン鋼を３０００度で１０分加熱した上で、
成型前処理剤「プリ・トリートメント」を混ぜた後、型に入れて成型するという製品Ａの製造方法</td></tr>
<tr><td colspan="2">上記営業秘密を構成する情報</td><td>成型前処理剤が「プリ・トリートメント」であること</td><td>ニッケル・クロム・モリブデン鋼を加熱する温度が３０００度であること</td><td>・・・（その他）</td></tr>
<tr><td colspan="2">上記情報を特定させることとなる事項</td><td>・成型前処理剤が「プリ・トリートメント」であること
・（成型前処理剤「プリ・トリートメント」が）日本では、経済産業株式会社が独占的に製造・販売しているものであること
等</td><td>・ニッケル・クロム・モリブデン鋼を加熱する温度が３０００度であること
等</td><td>・・・</td></tr>
<tr><td></td><td>当該事項に係る名称その他の表現</td><td>・成型前処理剤「プリ・トリートメント」という名称
・「経済産業株式会社」という名称
等</td><td>・「３０００度」という表現
等</td><td>・・・</td></tr>
<tr><td></td><td>呼称その他の表現
※名称その他の表現の言い換えであり、裁判所により定められる</td><td>・「本件薬品」
・「α株式会社」
等</td><td>・「本件加工温度」
等</td><td>・・・</td></tr>
</table>

第２　手続の流れ

１　公訴提起

公訴事実の概要は、次のとおりである。

被告人は、不正の利益を得る目的で、平成○年○月○日ころ、株式会社Ｘの技術部長Ｗのパソコンに不正アクセス行為をし、同パソコンから製品Ａの製造方法の営業秘密を取得した。

２　公訴提起に引き続く被害者等の申出

被害者である株式会社Ｘは、公訴事実に係る営業秘密を構成する情報を特定させることとなる事項を公開の法廷で明らかにされたくない旨を検察官に対し、書面により申し出た。

３　検察官による意見を付した通知

検察官は、被害者からの申出の内容及び公訴事実に係る営業秘密を構成する情報を特定させることとなる事項を公開の法廷で明らかにしない旨の決定をすることが相当である旨の意見を付して、裁判所に通知した。

４　公判前整理手続

(1) 被告人側の争い方

被告人側は、

例①　公訴事実を認める

例②　データの入手行為を否認し、被告人は、製品Ａと同じものを製造しているが、その製造方法は独自に開発したものである旨主張する

との方針を示した。

(2) 秘匿決定に関する被告人側の意見等

被告人側は、

例①　しかるべく

例②　製品Ａの製造方法のうち、ニッケル・クロム・モリブデン鋼を用いることは公知のものであり、これについてまで秘匿決定をするのは相当でない

旨の意見を述べた。

（なお、例②において、検察官は、被告人側の意見を受けて、被害者との事前の相談に基づき、ニッケル・クロム・モリブデン鋼を用いることについては、製品Ａを調べればすぐに明らかとなる情報であること等から、秘匿決定をしないことは問題ないとの意見を述べた。）

(3) 秘匿決定

これを受けて、裁判所は、次の秘匿決定を行った。

例①　本件営業秘密である製品Ａの製造方法を構成する情報を特定させることとなる事項を公開の法廷で明らかにしない。

例②　本件営業秘密である製品Ａの製造方法を構成する情報のうち、以下の各情報を特定させることとなる事項を公開の法廷で明らかにしない（※）。

・　ニッケル・クロム・モリブデン鋼を加熱する温度

・　ニッケル・クロム・モリブデン鋼を加熱する時間

・　加工に用いる薬品

※　裁判所は、弁護人及び検察官の意見を踏まえ、ニッケル・クロム・モリブデン鋼を用いることについては、秘匿の必要がないと判断し、その部分を除いて秘匿決定をすることとした。

(4) 呼称等の決定

裁判所は、

例①　呼称等の決定を行わなかった。

例②　「３０００度」を「本件加工温度」（ア）

「１０分」を「本件加工時間」（イ）

成型前処理剤「プリ・トリートメント」を「本件薬品」（ウ）

とする呼称等の決定を行った（※）。

※　裁判所は、呼称等の決定を行うに当たり、検察官及び弁護人に尋問等に係る事項の要領を記載した書面の提示を命じ、検察官及び弁護人が提示した同書面によれば、上記（ア）から（ウ）までの呼称等を定めることにより、営業秘密構成情報特定事項を公開の法廷で明らかにすることなく必要な尋問等を行うことができるものと考えられる。

(5) 公判期日外の被告人質問を行う旨の決定

例①　－

例②　裁判所は、被告人質問は公判期日外においてする旨を決定した（※）。

※　被告人質問については、弁護人からの尋問等に係る事項の要領を記載した書面の提示を受け、また、検察官からは、相当詳細な質問を行うことになること、その場合には、被告人の供述が営業秘密構成情報特定事項にわたる蓋然性が非常に高いと考えられる旨の指摘があった。これを受けて、弁護人・検察官から、被告人質問については公判期日外で行ってほしいとの申出があった。

5　起訴状の朗読

例①、②　起訴状には「製品Ａの製造方法」の具体的な内容までは明示されておらず、営業秘密構成情報特定事項に係る名称等は記載されていなかったことから、そのまま朗読された。

（以下、例②について）

6　検察官・弁護人の冒頭陳述

上記４(4)の呼称等の定め[71]に従って行われた。

7　技術部長Wの証人尋問

上記４(4)の呼称等の定めに従って行われた。

8　被告人質問

被告人質問は公判期日外において行われた。

その手続の中で、被告人は、

71　法第２３条第４項の規定に基づき裁判所が決定で定めた、営業秘密構成情報特定事項に係る名称その他の表現に代わる具体的な呼称その他の表現を意味する場合には、「呼称等の定め」と表記することとする。

・「技術部長Wのパソコンから製品Ａの製造方法のデータを不正に持ち出したことはありません。」
・「様々な実験を繰り返した結果、ニッケル・クロム・モリブデン鋼を３０００度で加熱する方法で加熱時間を１０分とすればある程度の強度を確保できることが判明し、さらに、加える薬品をいろいろと試していく中で、薬品Ｐよりもずっと安い薬品であって、国内では経済産業株式会社のみが製造している成型前処理剤「プリ・トリートメント」にたどりつき、これを用いた場合には、ニッケル・クロム・モリブデン鋼の通常の加工方法で薬品Ｐを用いた場合と同程度の強度の製品を製造することができることが分かりました。」

などと供述した。

9　呼称等の定めの追加

検察官から、成型前処理剤「プリ・トリートメント」の入手先である「経済産業株式会社」については、成型前処理剤「プリ・トリートメント」を特定させることとなることから、「α株式会社」という呼称等を定めるべきであるとの意見が示され、これに対し、弁護人も「しかるべく」との意見を述べたため、裁判所は、それらの意見を踏まえて、

「経済産業株式会社」を「α株式会社」

とする呼称等の決定を行った。

10　公判廷における期日外の被告人の供述調書の取調べ

上記４(4)及び９の呼称等の定めに従って、次のとおり朗読した。

・「技術部長Wのパソコンから製品Ａの製造方法のデータを不正に持ち出したことはありません。」
・「様々な実験を繰り返した結果、ニッケル・クロム・モリブデン鋼を本件加工温度で加熱する方法で加熱時間を本件加工時間とすればある程度の強度を確保できることが判明し、さらに、加える薬品をいろいろと試していく中で、薬品Ｐよりもずっと安い薬品であって、国内ではα株式会社のみが製造している本件薬品にたどりつき、これを用いた場合には、ニッケル・クロム・モリブデン鋼の通常の加工方法で薬品Ｐを用いた場合と同程度の強度の製品を製造することができることが分かりました。」

11　論告・弁論・最終陳述から判決まで

上記４(4)及び９の呼称等の定めに従って行われた。

※　証拠調べ後、論告・弁論・最終意見陳述のため、呼称等の定めを追加することも可能である。

３．被害企業の協力のあり方

（１）秘匿の申出

①秘匿決定

秘匿決定は、被害者等から申出があるときにすることができる。

秘匿決定は、「営業秘密を構成する情報の全部又は一部を特定させることとなる事項」を公開の法廷で明らかにしない旨の決定である。

②秘匿の申出

秘匿の申出をする被害企業としては、検察官と事前に打ち合わせを行い、「営業秘密を構成する情報」のうち、いずれの情報について秘匿を希望するかを検討した上で、秘匿の申出をすることが想定される。

ｉ）申出の方式

申出は、「不正競争防止法第２３条第１項に規定する事件に係る刑事訴訟手続の特例に関する規則」（平成２３年最高裁判所規則第４号）（以下、「最高裁規則」という。）で規定された以下の事項を明らかにして、検察官に対して行う。

営業秘密は、専門的・技術的な内容を含み、また、それを構成する情報は複雑多岐にわたることも予想されることから、申出の内容が正確に検察官及び裁判所に伝わるよう申出は、原則として書面でしなければならないとされている（最高裁規則第２条第２項本文)。

なお、この申出の際に提出した書面は、検察官から裁判所に提出されることとなる（最高裁規則第２条第５項)。

万が一、審理開始の直前になって、急遽秘匿の必要が生じた場合など、書面による申出を行う時間的な余裕がないといったやむを得ない事情があるときは、口頭で申出を行なうことも許されている（最高裁規則第２条第２項ただし書)。その場合であっても、その後速やかに、口頭にて申し出た内容を、検察官に対して書面で提出することが望ましい。

【被害企業が、法第２３条第１項の申出をする際に明らかにすべき事項（最高裁規則第２条第１項各号)】

ア）申出人の氏名又は名称及び住所

申出人が法人の場合は、事務所の所在地を住所として明らかにする。

イ）申出に係る事件を特定するに足りる事項

事件番号まで明らかであれば望ましいが、「被告人○○に対する不正競争防止法違反被告事件」などという程度でも問題ないと考えられる。

ウ）申出人が申出をすることができる者であることの基礎となるべき事実

申出人が被害者であるときは「被害者本人」であることを、被害者の法定代理人であるときはその旨を、それぞれ明らかにすれば足りる。また、申出人が被害者又は当該被

害者の法定代理人から委託を受けた弁護士であるときは、申出人が弁護士であることのほか、被害者又は当該被害者の法定代理人から申出をすることについて委託があることを明らかにしなければならない。

エ）上記イ）の事件に係る営業秘密を構成する情報のうち、秘匿決定の対象とすべき事項に係るもの

営業秘密を構成する情報のうち、それを特定させることとなる事項を公開の法廷で明らかにされたくないもの（情報） を、なるべく具体的に明らかにするよう留意する。

オ）秘匿決定を必要とする事情

申出に係る営業秘密を構成する情報を特定させることとなる事項が公開の法廷で明らかにされた場合の弊害等、秘匿の必要性に係る事情（申出に係る情報の全部を秘匿する必要性等、範囲の相当性に関する事情も含む。）について、具体的に明らかにするよう留意する。

ⅱ）申出の時期

申出の時期については、個々の事案にもよるが、できるだけ早い段階で、検察官に対し、秘匿の申出をする予定である旨を伝えた上で、検察官との間で、申出書の記載内容や提出時期について相談しておくことが望ましい。

この点、侵害の対象とされる営業秘密が不正競争防止法上の「営業秘密」に該当するか否かにつき被害企業から十分な情報・資料の提供を受ける必要があることが想定され、通常は、起訴に至るまでに、被害企業と捜査機関との間には相当程度の接触があると考えられる。このため、あらかじめ、捜査段階において、秘匿の申出につき検察官に相談しておき、公訴提起に至った段階で、迅速かつ円滑に秘匿の申出をすることができるよう、検察官と連携し、十分に準備しておくことが有用である。

（２）具体的な措置（呼称等の定め、尋問等の制限、公判期日外の証人尋問等）に向けた被害企業の協力

①具体的な措置（呼称等の定め、尋問等の制限、公判期日外の証人尋問等）

秘匿決定がなされた後、具体的な措置（呼称等の定め、尋問等の制限、公判期日外の証人尋問等）が適切に講じられることにより、秘匿決定の対象とされた事項（営業秘密構成情報特定事項）の秘匿を如何に図っていくかが重要となる。

これら措置が適切に講じられる前提としては、訴訟関係人が尋問・陳述・被告人質問（以下、「尋問等」という。）において言及しようとする事項が営業秘密構成情報特定事項に該当するか否か、どのような内容の主張立証を行う場合に営業秘密構成情報特定事項にわたる尋問等がなされるおそれがあるか、といった判断が適切になされる必要がある。

②具体的な措置に向けた協力

ところで、刑事訴訟手続に関与する当事者は検察官、被告人等であって、被害企業は当事者ではない。したがって、被害企業としては、あらかじめ秘匿の申出の際又はできる限り早い時期

に、検察官に対し、公開の法廷で明らかにされるおそれのある営業秘密構成情報特定事項を具体的に列挙して情報提供しておくことが望ましい。検察官は、これら被害企業から提供を受けた情報に基づき、秘匿決定があった場合において事件の性質、審理の状況その他の事情を考慮して、営業秘密構成情報特定事項のうち公開の法廷で明らかにされる可能性があると思料するものがあるときは、裁判所及び被告人又は弁護人に対して、これを通知する（最高裁規則第４条第１項）。

また、裁判所は、呼称等の決定に際して、対象とすべき営業秘密構成情報特定事項に係る名称その他の表現等について、検察官に書面の提出を求めることができるものとされている（最高裁規則第５条第１項）。よって、その実効的かつ円滑な運用に資するよう、被害企業は、あらかじめ、検察官に対し呼称等の候補を積極的に提案することが望ましい。これは、例えば、ある物質の名称について呼称を定める場合において、当該物質が金属であること自体が営業秘密構成情報特定事項に該当するときは、「金属Ａ」といった呼称ではなく「物質Ａ」といった呼称を定める必要があるように、呼称等の定め方は秘匿の実効性に影響を及ぼし得るからである。

また、公判期日外の証人尋問等に関しては、いかなる証人等に対して尋問等が行われる可能性があるか、当該証人等の尋問、供述等が営業秘密構成情報特定事項にわたる可能性があるか等について、適宜、検察官と連携しつつ、必要な情報提供等の協力をすることが望ましい。

さらに、公判期日外の証人尋問等が行われた後も、当該証人尋問等の結果を記載した書面（尋問調書等）を公判期日において朗読等する必要があり、必要に応じて追加の呼称等の定めが行われることになる。このため、当該証人等の尋問、供述等のうちのいずれの部分が営業秘密構成情報特定事項に該当するのか等につき、適宜、検察官と連携しつつ、必要な情報提供等の協力をすることが望ましい。

なお、公判期日外の証人尋問等を行うには、「当該営業秘密に基づく被害者、被告人その他の者の事業活動に著しい支障を生ずるおそれ」が要件とされていることなどを踏まえ、被害企業としては、あらかじめ秘匿の申出の際等に、検察官に対し、当該営業秘密の要保護性に関する情報・資料等を提供しておくことが望ましい。

※　裁判所は、呼称等の決定をし、又は公判期日外の証人尋問等の実施を決定する際には、必要に応じて、検察官・弁護人等に対し、尋問等に係る事項の要領を記載した書面の提示を命ずることができるため、被害企業は検察官を通じて、提示命令を受けて情報提供をすることもできるものの、常にこの提示命令がなされるとは限らない。

また、裁判所は、呼称等の決定に際して、検察官に対して、その対象とすべき営業秘密構成情報特定事項に係る名称その他の表現や、これに代わるべき呼称その他の表現等を記載した書面の提出を求めることができるものの（最高裁規則第５条第１項）、常にこの求めがなされるとは限らない。

したがって、検察官に対する情報提供については、その時期に制限があるわけではないことを踏まえ、検察官が適時に裁判所に対して有用な情報を伝達できるよう、秘匿決定がなされた後、又は審理手続がある程度進行した後であっても、なお公開の法廷で明らかにされるおそれのある営業秘密構成情報特定事項があると判断される場合には、その旨及び当該事項に係る名称その他の表現に代えて定めるべき呼称その他の表現等について、随時、追加的に検察官に情報提供をしていくことが有益であろう。

（３）証拠開示の際の営業秘密の秘匿要請に関する協力

①証拠開示の際の秘匿要請

検察官から弁護人に開示する証拠書類又は証拠物に、「営業秘密を構成する情報の全部又は一部を特定させることとなる事項」が記載等されている場合には、検察官は、弁護人に対し、当該事項がみだりに関係者に知られないようにすることを求めること（秘匿要請）ができる。

その場合、弁護人に対して秘匿要請に係る義務を適切に課すためには、当該証拠に記載等されている事項のうち、いかなる事項が秘匿要請の対象となっているのかを明らかにする必要がある。

※　秘匿要請がなされる事件では、すでに被害企業から秘匿の申出がなされていることもあると考えられ、その場合には、すでに検察官に対して上記（１）又は（２）に係る情報提供がなされているものと考えられる。もっとも、これらの情報提供は、公開の法廷で明らかにされるおそれのある営業秘密構成情報特定事項についてなされるものである。

これに対し、証拠開示の際に弁護人に開示される証拠には、公開の法廷で言及されるおそれのある内容よりも更に詳細かつ広範な内容が記載等されていることが想定され、当該証拠のいずれの部分が「営業秘密を構成する情報の全部又は一部を特定させることとなる事項」に該当するかの判断については、被害企業からの検察官に対する更なる情報提供が必要となることが少なくないものと考えられる。

②証拠開示の際の秘匿要請に関する協力

したがって、被害企業としては、捜査段階において検察官に対して、被害企業が提出した資料等のいずれの部分が「営業秘密を構成する情報の全部又は一部を特定させることとなる事項」に該当するかにつき具体的に情報提供をするとともに、起訴後においても、検察官が取調べを請求する予定の証拠について、「営業秘密を構成する情報の全部又は一部を特定させることとなる事項」が記載等されている可能性がある場合には、あらかじめ、検察官の秘匿要請に係る判断に資するよう、情報提供をすることが望ましい。

また、秘匿要請は、「営業秘密を構成する情報の全部又は一部を特定させることとなる事項」が明らかにされることにより「当該営業秘密に基づく被害者、被告人その他の者の事業活動に著しい支障を生ずるおそれ」がある場合に行うことができるため、この点についても情報提供する必要があるが、上記（２）の協力と併せて、秘匿の申出の際に行っておくことが望ましい。

※　証拠開示は、起訴後早期の段階で行われることもあるため、できる限り早い段階で、上記の協力を行っておく必要がある。

この点、捜査段階で捜査機関に対して自ら提出した資料や捜査機関からの事情聴取に応じて作成された供述調書等に関しては、上記の協力に向けた準備をしておくことは比較的容易である。

他方、捜査機関が独自に入手した情報が記載された書面や被告人（被疑者）の供述調書等に関しては、適宜、検察官と連携しながら、弁護人に対する秘匿要請が適切になされるようにする必要があるため、できるだけ早い段階で検察官に相談しておくべきである。

（４）事件終結後の訴訟記録の閲覧制限に関する情報提供

①事件終結後の訴訟記録の閲覧

刑事裁判が終結した後の訴訟記録については、当該記録を保管する検察官（保管検察官）に対して閲覧請求がなされた場合、当該検察官が、刑事確定訴訟記録法に基づき、閲覧を許可するか否かを判断することとなる。

保管検察官において、当該記録を閲覧させることにより当該記録に記載等されている営業秘密に基づく被害企業等の事業活動に著しい支障を生ずるおそれがあると認められるものなどについては、刑事確定訴訟記録法の定める一定の事由がある場合を除き、閲覧を不許可としたり、又は一部を不許可としてその該当部分をマスキングした記録のみを閲覧させたりする等の措置をとることが可能である。

②事件終結後の訴訟記録の閲覧制限に関する情報提供

このため、被害企業としては、当該記録に含まれる公判調書、証拠書類等に、自己の保有する営業秘密の内容が明らかとなるような記載等があり、又はそのおそれがあると考えられる場合には、あらかじめ、検察官に対し、その旨を伝えた上で、裁判確定後の保管検察官の当該記録の閲覧に係る判断に資するよう、必要に応じて、当該記録を閲覧させることによる影響等に関する情報提供をしておくことが望ましい。

※　訴訟記録は、訴訟終結後、第一審裁判所に対応する検察庁の検察官に送付され、以後、刑事確定訴訟記録法に基づく閲覧の対象となる。このため、被害企業としては、できるだけ早い段階で、確定訴訟記録の保管検察官に、当該記録を閲覧させることによる影響等に関する情報提供をしておくことが望ましい。さらにいえば、捜査段階においては、捜査担当検察官、公判段階においては、公判担当検察官に、同様の情報提供をしておくことが望ましいと考えられる。

なお、当該事件において秘匿決定がなされている場合には、保管検察官において、当該秘匿決定、上記（１）ないし（３）の協力に係る情報提供やこれを踏まえた呼称等の定め等を踏まえて、当該記録の閲覧の許否を適切に判断することとなるものと考えられるが、例えば、被告人側の請求証拠等に係る訴訟記録に関しては、なお当該記録のうちのいずれの部分が営業秘密の内容に係るものであるのか等につき必ずしも明らかではなく、時間の経過とともに要保護性に変化が生じることも考えられることから、確定訴訟記録の閲覧請求段階で、改めて協力が必要となることに留意する必要がある。

４．　秘匿の申出書等の記載例

（１）営業秘密の秘匿の申出書（第２３条第１項に基づく申出）

営業秘密の秘匿の申出書

〇年〇月〇日

〇〇検察庁
検察官　検事　〇〇　殿

〇〇株式会社　（被害者本人）
代表取締役社長　〇〇
（事務所の所在地・連絡先）　〇〇

被告人〇〇に対する不正競争防止法違反（営業秘密侵害）被告事件について、下記のとおり、当該事件に係る営業秘密を構成する情報の全部又は一部を特定させることとなる事項を公開の法廷で明らかにされたくない旨、同法第２３条第１項の規定に基づき申し出ます。

記

１　申出をすることができる者であることの基礎となるべき事実

２　営業秘密を構成する情報のうち、秘匿決定の対象とすべき事項に係るもの

別添１記載のとおり

３　秘匿決定を必要とする事情

本営業秘密は、弊社の主力商品である製品Ａの製造方法を内容とするものであり、本営業秘密が公開の法廷で明らかにされることにより、〇〇社や〇〇社といった競争事業者の知るところとなった場合に弊社に生じ得る支障・損害は甚大であると考えられる。・・

４　上記２の事項のうち、公開の法廷で明らかにされるおそれがあると思料するもの、当該事項に係る名称その他の表現に代わる呼称その他の表現として相当であると思料するもの及びその他呼称等の決定をするに当たり参考となるべき事項

別添２記載のとおり

５　備考

その他本営業秘密に関し留意すべき事項等については、別紙を御参照ください。

以上

注　なお、公訴事実に掲げられた営業秘密の内容を示す文書等の写しを引用する方法により「営業秘密を構成する情報」を明らかにすることも考えられる。

（別添１）

営業秘密を構成する情報のうち、秘匿決定の対象とすべき事項に係るもの

秘匿すべき情報①	成型前処理剤「プリ・トリートメント」
秘匿すべき情報②	ニッケル・クロム・モリブデン鋼を加熱する温度が３０００度であること
秘匿すべき情報③	ニッケル・クロム・モリブデン鋼を加熱する時間が１０分であること

（別添２）

別添１の各対象情報を特定させることとなる事項のうち、公開の法廷で明らかにされるおそれがあると思料するもの及び当該事項に係る名称その他の表現に代わる呼称等その他の表現として相当であると思料するものについて

秘匿すべき情報①		
成型前処理剤「プリ・トリートメント」		
上記情報を特定させることとなる事項であって、公開の法廷で明らかにされるおそれがあると思料するもの		当該事項に係る名称その他の表現に代わる呼称その他の表現
「成型前処理剤『プリ・トリートメント』」	⇒	「本件薬品」
（成型前処理剤「プリ・トリートメント」を独占的に販売している）「経済産業株式会社」	⇒	「α株式会社」
	⇒	

秘匿すべき情報②		
ニッケル・クロム・モリブデン鋼を加熱する温度が３０００度であること		
上記情報を特定させることとなる事項 であって、公開の法廷で明らかにされる おそれがあると思料するもの		当該事項に係る 名称その他の表現に代わる 呼称その他の表現
「（ニッケル・クロム・モリブデン鋼を加熱する温度である）３０００度」	⇒	「本件加工温度」
	⇒	
	⇒	

（別紙）

その他本営業秘密に関し留意すべき事項について

製品Ａを製造するための公知技術としては、ニッケル・クロム・モリブデン鋼を２０００度で２０分加熱し、薬品Ｐを混ぜることにより強度を増すという方法があるが、本営業秘密に係る方法においては、薬品Ｐよりも安価な成型前処理剤「プリ・トリートメント」を用いて、強度が高い製品を製造することができる。・・・

成型前処理剤「プリ・トリートメント」によっても強度を増すことができる原理は、・・・

（２）証拠開示の際の営業秘密の秘匿要請に関する協力をする際の記載例

証拠開示の際の営業秘密の秘匿要請について

○年○月○日

○○検察庁
検察官　検事　○○　殿

○○株式会社
代表取締役社長　○○

被告人○○に対する不正競争防止法違反（営業秘密侵害）被告事件について、貴職が、弁護人に証拠書類又は証拠物を閲覧する機会（又は、閲覧し、かつ、謄写する機会）を与えるに当たっては、下記のとおり、営業秘密を構成する情報の全部又は一部を特定させることとなる事項が明らかにされることにより当該営業秘密に基づく弊社の事業活動に著しい支障を生ずるおそれがあるため、弁護人に対し、その旨を告げ、当該事項が、関係者（被告人を含む。）に知られないようにすることを求めていただきたくお願い申し上げます。

記

記載例１

１　営業秘密

製品Ａの製造方法

２　証拠書類又は証拠物の中に含まれる上記営業秘密を構成する情報の全部又は一部を特定させることとなる事項

別添「営業秘密目録」記載のとおり

３　上記２の事項が明らかにされることにより当該営業秘密に基づく弊社の事業活動に生ずるおそれのある著しい支障の内容その他当該求めを必要とする事情

別紙のとおり

以上

（別添）

営業秘密目録

本営業秘密の概要	ニッケル・クロム・モリブデン鋼を３０００度で１０分加熱した上で、成型前処理剤「プリ・トリートメント」を混ぜた後、型に入れて成型するという方法
本営業秘密を構成する情報①	成型前処理剤「プリ・トリートメント」
本営業秘密を構成する情報②	３０００度
本営業秘密を構成する情報③	１０分

※　従前に司法警察員○○に対して○年○月○日に提出した、弊社○○部○○作成に係る○年○月○日付け「○○」と題する書面も参照いただきたい。

（１）本営業秘密を構成する情報①を特定させることとなる事項であって、証拠書類等に記載等されているおそれがあると思料するもの

○成型前処理剤「プリ・トリートメント」
○（成型前処理剤「プリ・トリートメント」を独占的に製造・販売している）「経済産業株式会社」
○・・・

（２）本営業秘密を構成する情報②を特定させることとなる事項であって、証拠書類等に記載等されているおそれがあると思料するもの

○・・・
○・・・
○・・・

（３）事件終結後の訴訟記録の閲覧制限に関する情報を提供する際の記載例

保管記録の閲覧について

○年○月○日

○○検察庁　検察官　殿

○○株式会社
代表取締役社長　○○

下記事件の保管記録（以下、「本件記録」という。）については、下記のとおり、営業秘密を構成する情報の全部又は一部を特定させることとなる事項が明らかにされることにより当該営業秘密に基づく弊社の事業活動に著しい支障を生ずるおそれがあるため、閲覧に際して配慮願います。

なお、当該営業秘密については、上記事件において、秘匿決定（○○地方裁判所平成○年○月○日決定）がなされております。

記

１　被告事件

（１）裁判を受けた者の氏名　○○

（２）罪名　不正競争防止法違反

（３）第一審　○年○月○日　○○裁判所
控訴審　○年○月○日　○○高等裁判所
上告審　○年○月○日　最高裁判所

（４）確定年月日　○年○月○日

２　本件記録を閲覧させることにより明らかにされる営業秘密を構成する情報の全部又は一部を特定させることとなる事項

本件においてなされた秘匿決定（○○地方裁判所○年○月○日決定）の対象となった営業秘密構成情報を特定させることとなる事項及び別紙１の事項

３　上記２の事項が明らかにされることにより弊社の事業活動に生じるおそれのある著しい支障の内容及びその理由

別紙２のとおり

以上

※令和６年の本書改訂にあたり、以下の委員会で御議論いただきました。

産業構造審議会　知的財産分科会

不正競争防止小委員会

委員名簿

◎岡村 久道	国立情報学研究所 客員教授
	京都大学大学院 医学研究科 講師、弁護士
河野 智子	ソニーグループ株式会社 知的財産・技術標準化部門
	スタンダード＆パートナーシップ部 著作権政策室
	国内渉外担当
小松 文子	ノートルダム清心女子大学 特別招聘教授
下川原 郁子	日本知的財産協会 理事長
	株式会社東芝 技術企画部 エキスパート
末吉 亙	ＫＴＳ法律事務所 弁護士
杉村 純子	プロメテ国際特許事務所 代表弁理士
田村 善之	東京大学大学院 法学政治学研究科 教授
冨田 珠代	日本労働組合総連合会 総合政策推進局 総合局長
長谷川 正憲	日本経済団体連合会 知的財産委員会・企画部会 委員
	キヤノン株式会社 知的財産法務本部 知的財産渉外第三部 部長
畠山 一成	日本商工会議所 常務理事
水野 正則	知的財産高等裁判所 判事

敬称略（５０音順）

※◎：委員長

オブザーバー

内閣府知的財産戦略推進事務局
法務省民事局
法務省刑事局

※令和４年の本書改訂にあたり、以下の委員会で御議論いただきました。

産業構造審議会　知的財産分科会

不正競争防止小委員会

委員名簿

淺井 俊雄	日本知的財産協会 副理事長 日本電気株式会社 知的財産本部 上席主幹
◎岡村 久道	京都大学大学院 医学研究科 講師、弁護士
小川 暁	東京地方裁判所 判事
久貝 卓	日本商工会議所 常務理事
河野 智子	ソニーグループ株式会社 知的財産・技術標準化部門 スタンダード＆パートナーシップ部 著作権政策室 著作権政策担当部長
小松 文子	長崎県立大学 副学長
近藤 健治	トヨタ自動車株式会社 知的財産部 主査
末吉 亙	ＫＴＳ法律事務所 弁護士
杉村 純子	日本弁理士会 会長 プロメテ国際特許事務所 代表弁理士
田村 善之	東京大学大学院 法学政治学研究科 教授
冨田 珠代	日本労働組合総連合会 総合政策推進局長
長谷川 正憲	日本経済団体連合会 知的財産委員会・企画部会 委員 キヤノン株式会社 知的財産法務本部 知的財産渉外第三部長
林 いづみ	桜坂法律事務所 弁護士
山本 和彦	一橋大学大学院 法学研究科 教授

敬称略（５０音順）

※◎：委員長

オブザーバー

内閣府知的財産戦略推進事務局
法務省民事局
法務省刑事局

※平成２８年の本書策定にあたり、以下の委員会、研究会で御議論いただきました。

産業構造審議会　知的財産分科会

営業秘密の保護・活用に関する小委員会

委員名簿

	相澤　英孝	一橋大学大学院国際企業戦略研究科教授
	飯田　圭	日本弁理士会不正競争防止法委員会・貿易円滑化対策委員会委員 弁護士・弁理士
	池村　治	日本経済団体連合会知的財産委員会企画部会委員 味の素株式会社　知的財産部長
	石井　夏生利	筑波大学図書館メディア系准教授
	伊藤　眞	日本大学大学院法務研究科客員教授
	岡村　久道	英知法律事務所　弁護士
	久貝　卓	日本商工会議所常務理事
	久慈　直登	日本知的財産協会専務理事
◎	後藤　晃	政策研究大学院大学教授
	齋藤　憲道	経営法友会評議員
	末吉　亙	潮見坂綜合法律事務所　弁護士
	鈴木　千帆	東京地方裁判所判事
	髙山　佳奈子	京都大学大学院法学研究科教授
	長澤　健一	キヤノン株式会社取締役・知的財産法務本部長
	野口　祐子	グーグル株式会社法務部長　弁護士
	林　いづみ	桜坂法律事務所　弁護士
	春田　雄一	日本労働組合総連合会経済政策局長
	三原　秀子	帝人株式会社　非常勤顧問
	宮島　香澄	日本テレビ報道局解説委員
	横山　久芳	学習院大学法学部教授

敬称略（５０音順）

※◎：委員長

オブザーバー

法務省民事局付　沖本　尚紀

法務省刑事局付　煙山　明

企業の機密情報の管理手法等に係る
マニュアルの策定に向けた研究会
委員名簿

	上原　哲太郎	立命館大学　情報理工学部　教授
◎	岡村　久道	英知法律事務所　弁護士
		国立情報学研究所　客員教授
	木全　政弘	日本経済団体連合会　知的財産委員会企画部会　委員
		三菱電機株式会社　知的財産センター長
	小松　文子	独立行政法人情報処理推進機構
		情報セキュリティ分析ラボラトリー　ラボラトリー長
	小宮　信夫	立正大学　文学部社会学科　教授
	島田　まどか	西村あさひ法律事務所　弁護士
	田中　勇気	アンダーソン・毛利・友常法律事務所　弁護士
	春田　雄一	日本労働組合総連合会　経済政策局長
	平井　真以子	日本製薬工業協会　知的財産委員会　運営委員
		武田薬品工業株式会社　知的財産主席部員

敬称略（５０音順）

※◎：座長

オブザーバー

産業構造審議会　知的財産分科会　営業秘密の保護・活用に関する小委員会
委員長　後藤　晃　（政策研究大学院大学　教授）
委　員　久慈　直登（一般社団法人日本知的財産協会　専務理事）

JPCERT コーディネーションセンター
理事／分析センター長　真鍋　敬士

警　察　庁　生活安全局　生活経済対策管理官付
内 閣 官 房　知的財産戦略推進事務局
特　許　庁　企画調査課
経済産業省　産業技術環境局　大学連携推進室
商務情報政策局　情報セキュリティ政策室

秘密情報の保護ハンドブック　～企業価値向上に向けて～

初　版　２０１６年２月８日
第２版　２０１７年９月１日
第３版　２０１８年９月１日
第４版~~改訂版~~　２０２２年５月１７日
改訂版　２０２４年●月●日

編　著　経済産業省経済産業政策局知的財産政策室
〒　１００－８９０１　東京都千代田区霞が関１丁目３番１号