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、秘密情報の性質、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[9]。
- 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）

○　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

[9] 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（http://www.jnsa.org/ikusei/01/02-02.html）参照

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性質やその評価の高低、その利用態様等の事情に応じ、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等に保管すべき情報か否か」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）
- 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

➢　**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）

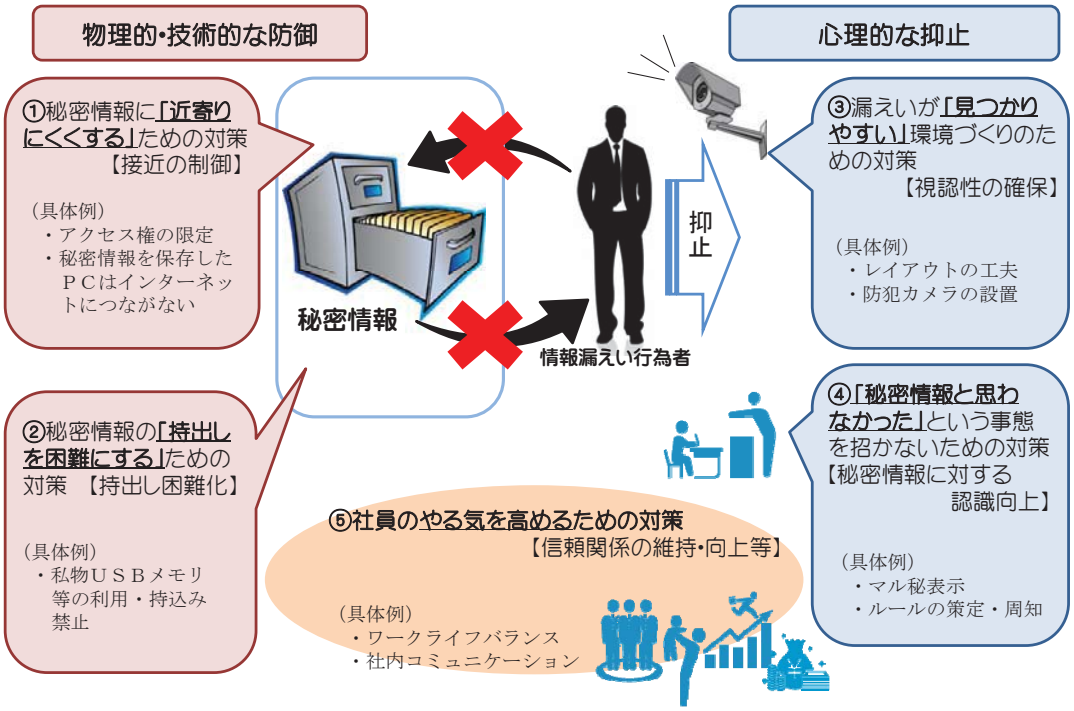
○　本章３－１において設定した秘密情報の分類ごとに、具体的にどのような情報漏えい対策を講ずるのかを選択します。その際には、誰に対して対策を行うのか（従業員、退職者、取引先、外部者）、どのような形で秘密情報が存在しているのか（情報にネットワークを介してアクセスすることができるか、工場ライン等の物件自体が秘密情報である場合か否か等）、漏えいの手口やその動機がいかなるものであるかといった状況によって効果的な対策は異なることに留意する必要があります。加えて、転職者の増加や、様々な契約形態に基づく人事やグローバル人材の登用など、各社の事情に応じた対策を選択することが有効です。

（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。

（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、事業者が保有するノートＰＣの固定、記録媒体の複製制限、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。

（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。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。

（４）秘密情報に対する認識向上（不正行為者[10]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。

（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

10 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。

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。

○ 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。

（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[11]。

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

11 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　情報管理規程の例」を参照。

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[12]。
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。

[12] 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（＊５）における「情報管理基準（例）」を参照。

コラム② こんなに怖い、秘密情報の漏えい

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。

秘密情報の価値が失われてしまう！

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。

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。

逆に訴えられてしまうかも！？

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。

秘密情報の漏えいの経路は様々！

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。

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。

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、自社内の実習生や派遣労働者、委託先従業員であって自社内において勤務する者なども含みます。

（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。

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、その秘密情報の内容・性質等を踏まえて、「知るべき者だけが知っている（ need to know　）」という状態が実現するようにすることが重要です。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ります。

○　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」[13]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[14]等を設定しておきます。**

※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見当をつけら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。

○ **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ー等）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

[13] 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』ｐ２９を参照）。

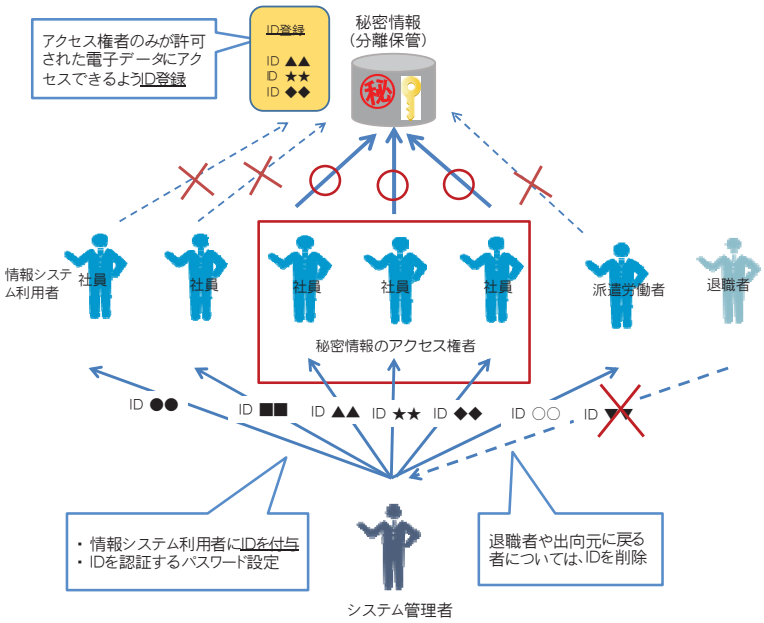
[14] ＩＰＡ『チョコっとプラスパスワード』(http://www.ipa.go.jp/chocotto/pw.html）に、パスワードの安全性を高めるための管理方法が分かり易く説明されています。

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。

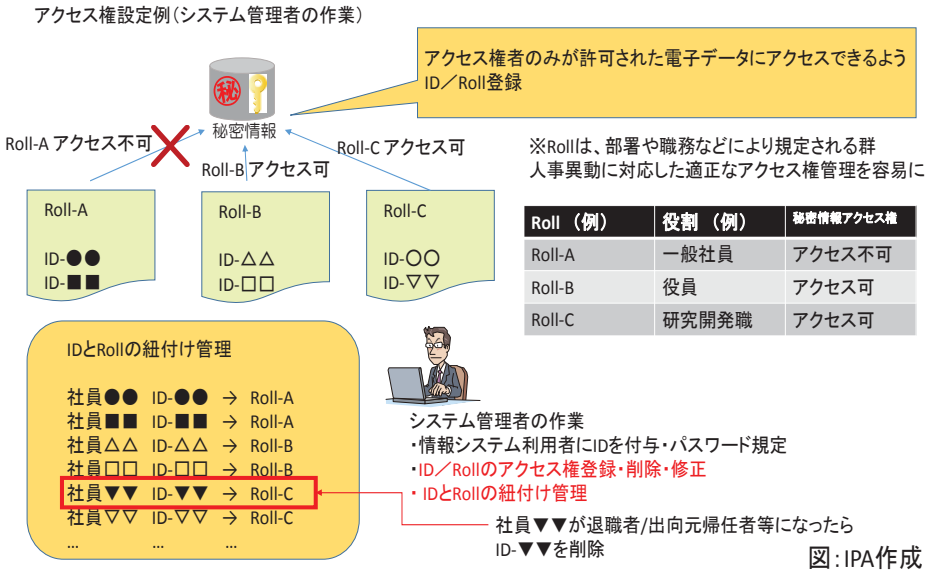
※情報システム上のＩＤ登録作業は、複数人のシステム管理者で行うことで、適正な実施を確保することができます。

※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[15]。

図表３（２）情報システム上のアクセス権設定の流れ



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）



Roll（例）	役割（例）	秘密情報アクセス権
Roll-A	一般社員	アクセス不可
Roll-B	役員	アクセス可
Roll-C	研究開発職	アクセス可

図：IPA作成

[15] ＩＰＡ『組織における内部不正ガイドライン』ｐ３０,３１,４８を参照。

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ー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、サーバーにアクセスできない状態とする等）。

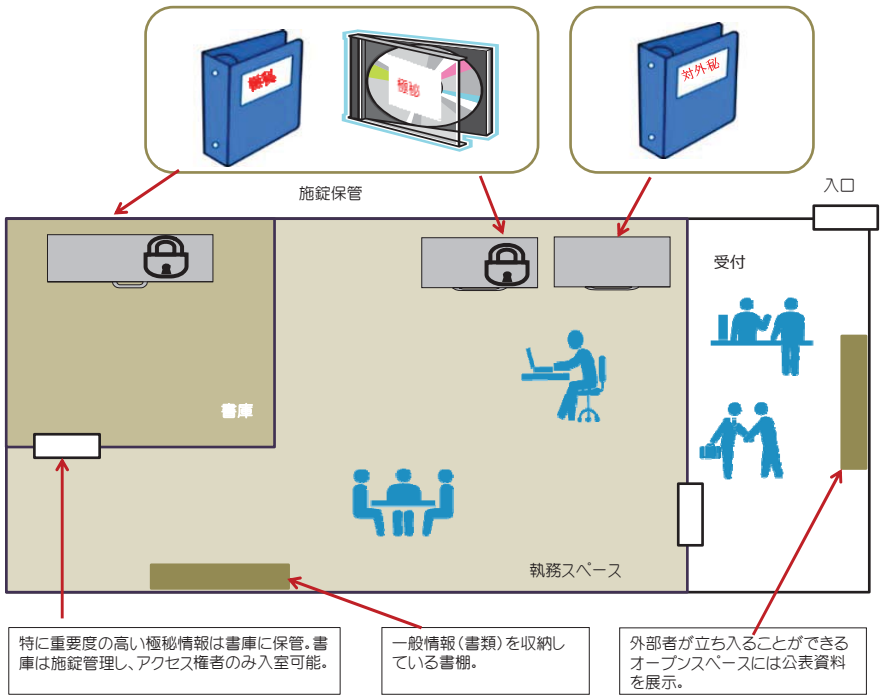
○ なお、全ての秘密情報について、厳格なアクセス制限を講ずることが難しい場合も考えられますので、秘密情報の評価の高低や利用態様に応じて、対策を選択していくことが重要です。

（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[16]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

[16] 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。

図表３（４）秘密情報の分離保管の例（書類等）



➢　**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）**サーバーの物理的分離（複数台のサーバーに分離）、**

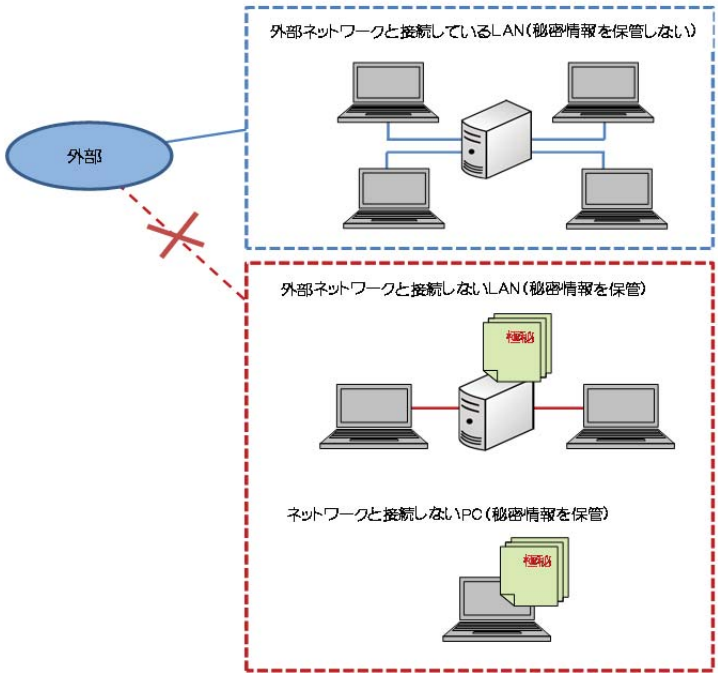
サーバーの仮想化による論理的分離（1 台のサーバーを複数の仮想サーバーに分割）

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、サーバー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、サーバーの廃棄方法

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、従業員の私物ＵＳＢ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。

【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。

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[17]。

---

[17] ＩＰＡ『暗号化による＜情報漏えい＞対策のしおり』（https://www.ipa.go.jp/security/keihatsu/announce20140320_2.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、管理サーバー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。

【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。

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。

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[18、19]。

○　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。

○　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。

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。

18　ＩＰＡ『組織における内部不正防止ガイドライン』ｐ３６を参照
19　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）。

【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、秘密保持契約等において、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[20]。

※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。

[20] 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、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】、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。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。

【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。

【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[21]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[22]。

※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。

---

21 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。

22 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経済産業分野を対象とするガイドライン』ｐ４０が参考になります。
（http://www.meti.go.jp/policy/it_policy/privacy/downloadfiles/1212guideline.pdf）

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。

※「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[23]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

[23] 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。

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）

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。

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」、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？」（ｐ８９）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）」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、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[24]。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」
  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」

[24] 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。

※「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。

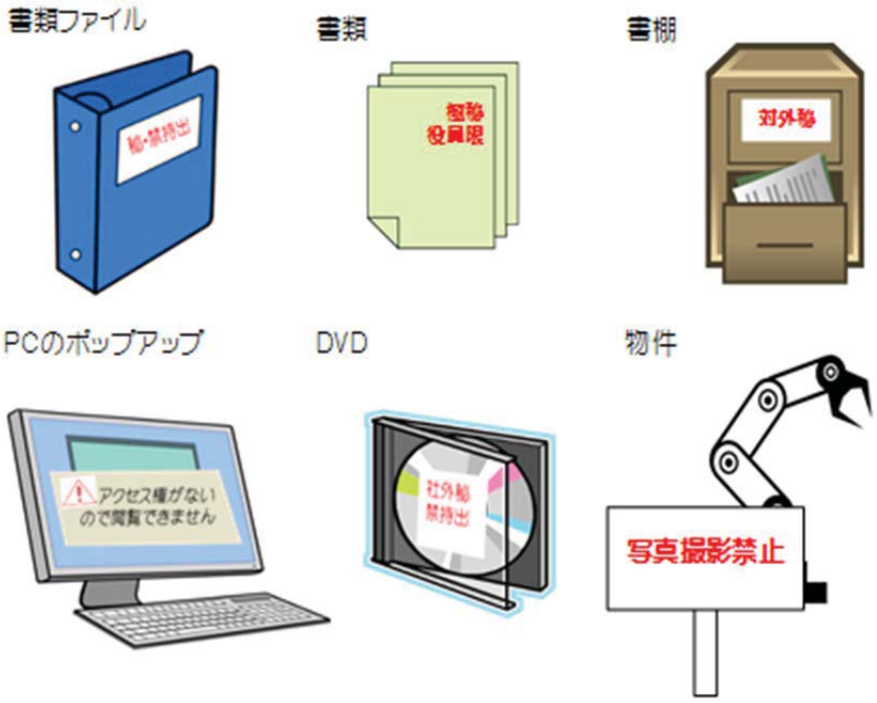
○　また、秘密情報が記録された媒体等を保管する書庫や区域（倉庫、部屋など）に「無断持出し禁止」といった掲示を行うことも考えられます。

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。

【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[25]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。

[25] 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（ｐ６４参照）。

【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[26、27]。

○　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[28]。

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[29]を導入することも、モチベーション向上に貢献します。

26　「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。

27　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」（http://www.jtuc-rengo.or.jp/kurashi/anshin_shakai/data/201507digest.pdf）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。

28　「あかるい職場応援団」（厚生労働省：http://no-pawahara.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。

29　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、職務発明に関する指針（ガイドライン）（http://www.jpo.go.jp/seido/shokumu/pdf/shokumu/06.pdf）が参考になります。

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。

（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。

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。

【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
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。

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。

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[30]。

○　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[31]。

※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。

---

30 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。

31 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。

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[32]。

[32] 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）

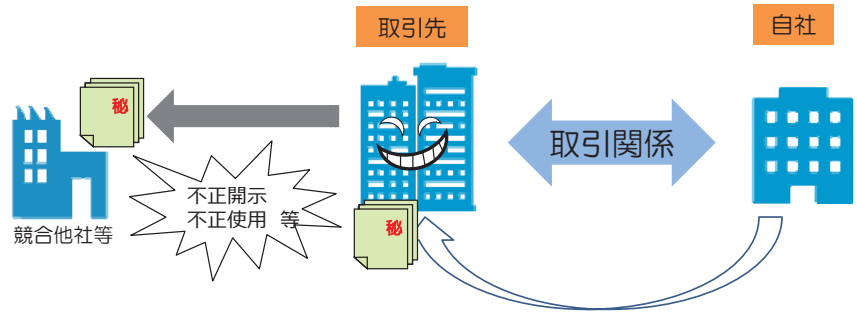
○ 取引先を通じた情報漏えいの中には、大別して、以下の２つのパターンが考えられます。

（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

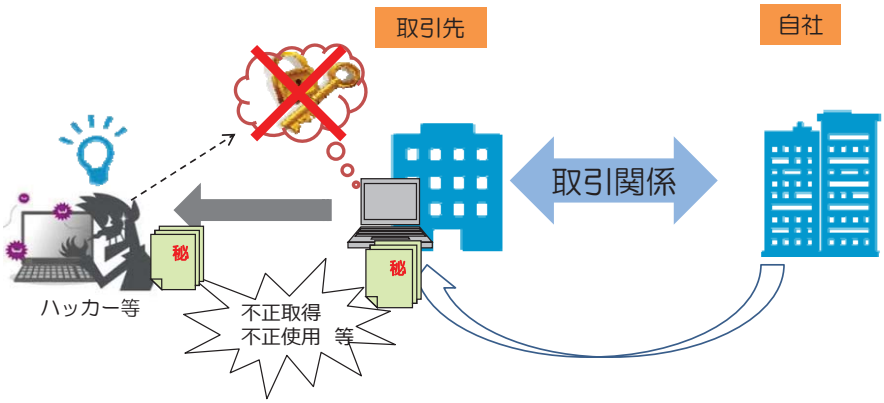
（ii）取引先の情報管理が不十分であったことに起因して、相手方従業員、退職者、再委託者や外部者等を通じて情報漏えいしてしまう場合

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[33]。

○　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。

---

33 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（平成２６年度版）』（http://www.nisc.go.jp/active/general/pdf/kijyun26.pdf）のｐ２３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[34]。

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。
- 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。

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。

[34] 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。

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ー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、サーバー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。）

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、自社サーバーの利用等を除き、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。特に秘密情報を相手方に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ーを使用させた場合、そのサーバー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、管理サーバー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ー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ー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、当該サーバーは、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[35]。

○　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。

35 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。

ｂ．秘密情報であることの表示

○　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[36]。

---

[36] 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/keihatsu/videos/
＜情報セキュリティ啓発＞
https://www.ipa.go.jp/security/keihatsu/features.html

具体例

- 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」[37]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。

[37]「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
http://www.chusho.meti.go.jp/keiei/torihiki/ShitaukeGuideLineGyoushu.htm

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。

（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ー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（ｐ６４）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。

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。

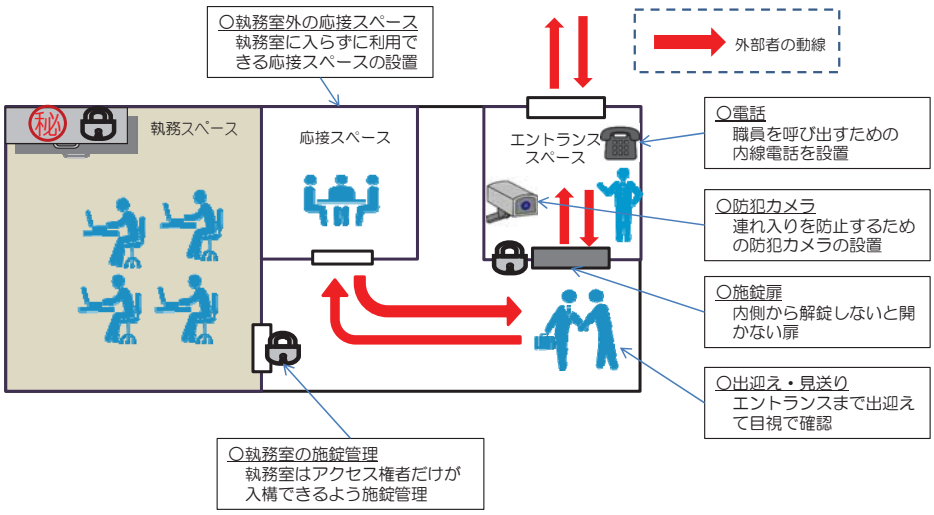
ａ．秘密情報を保管する建物や部屋の入場制限、書棚や媒体等のアクセス制限

○　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、サーバーの廃棄方法
  - 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。

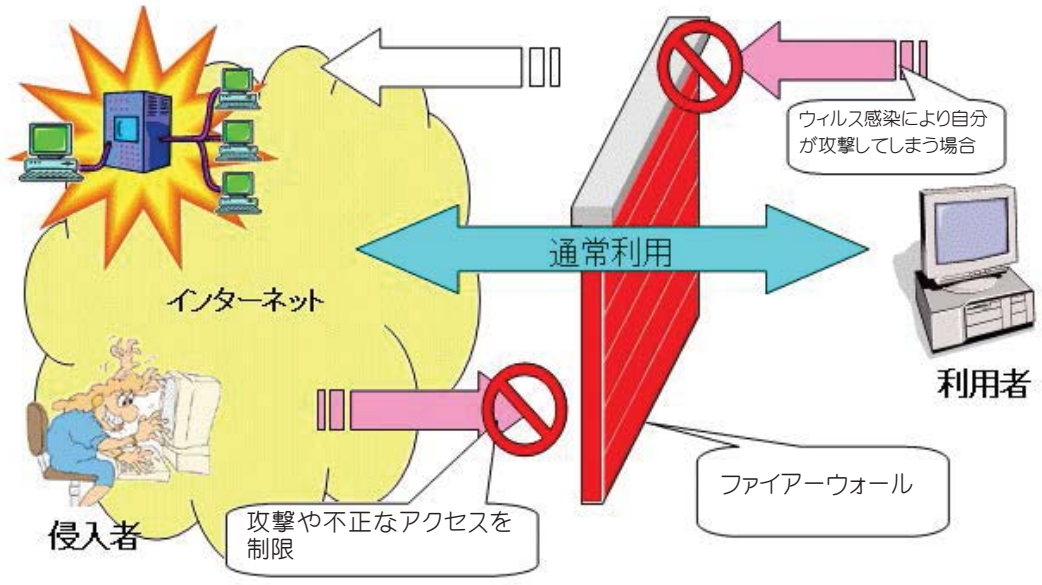
ｆ．ファイアーウォール、アンチウィルスソフトの導入、ソフトウェアのアップデート

○　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

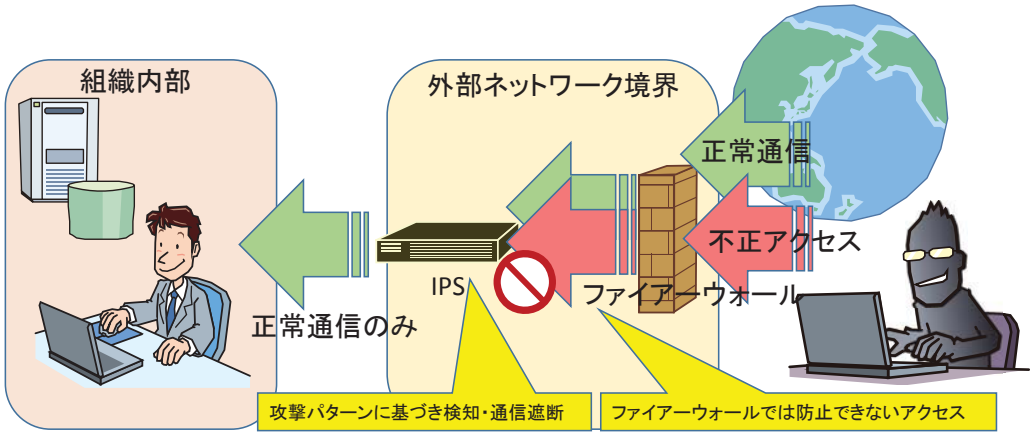


（ＩＰＡ『不正アクセス対策のしおり』より引用）

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）

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[38]。

[38]　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ーに集中させ、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、管理サーバー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[39]。

[39] 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

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）

る。
- 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

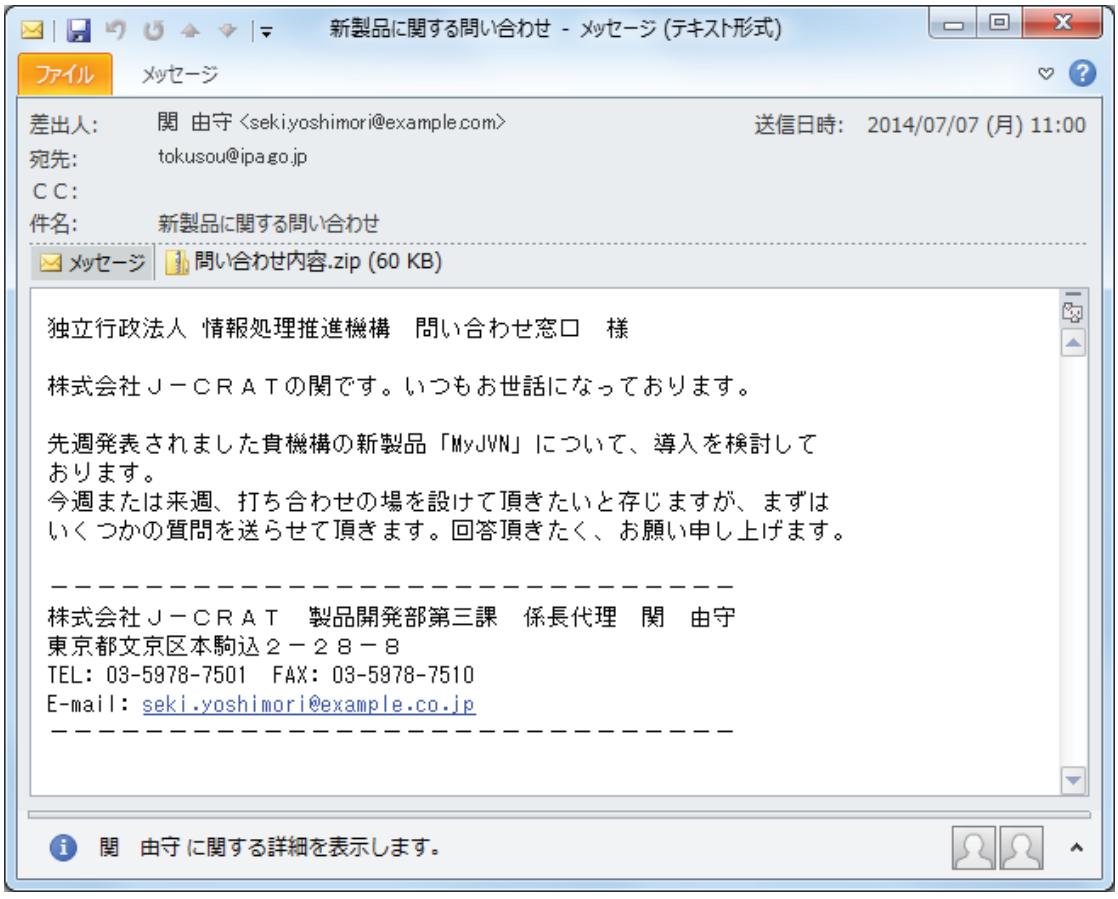
不法侵入や不正アクセスを企図する外部者に対しては、「信頼関係の維持・向上等」に資する有効な対策は考えにくいですが、一定の契約関係のある外部者に対しては、（３）取引先に向けた対策 ⑤「信頼関係の維持・向上等」の対策が有効な場合が考えられますので、そちらを参考に対策することが望まれます。

コラム③ 標的型攻撃メールってどんなもの？

近年、標的型攻撃メールの増加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。

標的型攻撃メールは、ただの迷惑メールとは違い、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、以下のようなメールが報告されています。



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。

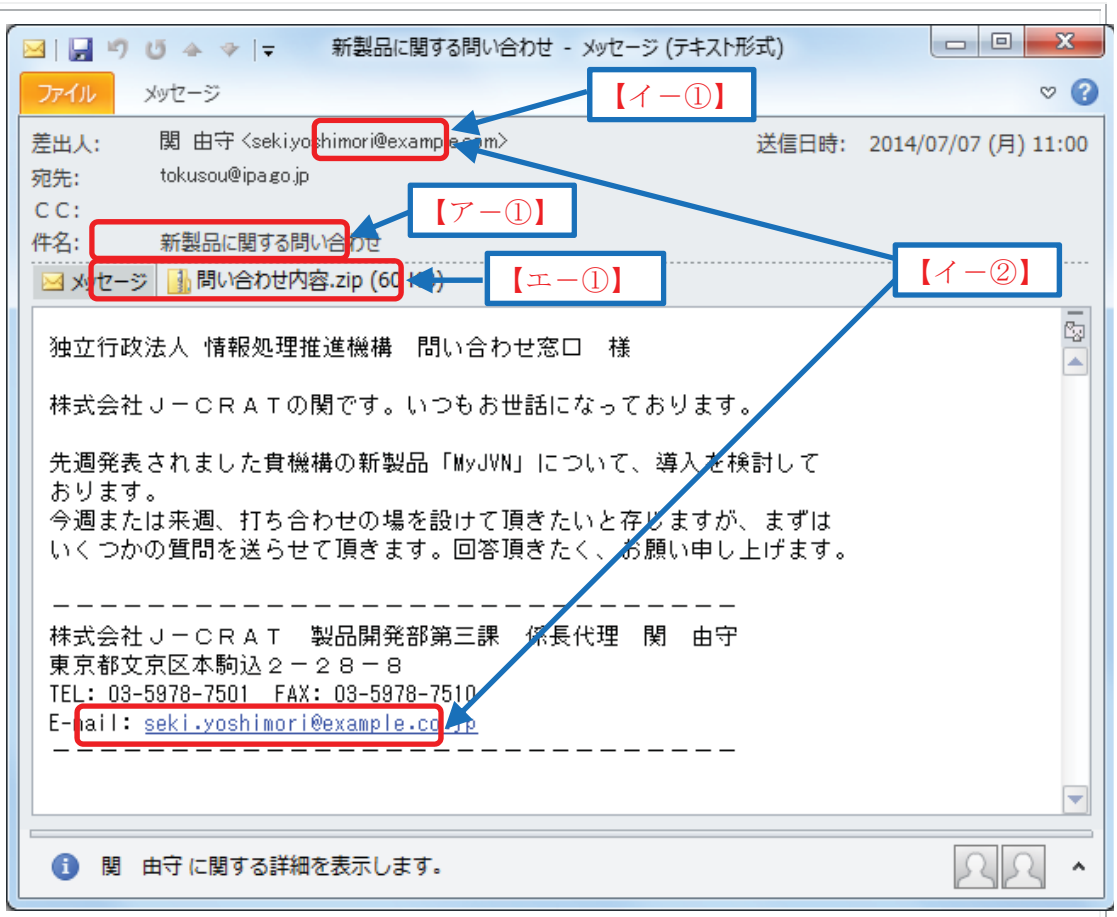
IPAでは、以下のとおりその着眼点をまとめています。

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』より抜粋）

上記を踏まえ、先程のメールを見てみると、以下のような着眼点に気がつきます。



・製品に関する問い合わせ【ア－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。

上記のように、被害に遭わないためには、標的型攻撃メールを“嗅ぎ分けられるか”が非常に重要になります。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

＜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④ 最低限のサイバーセキュリティって？

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、やるべき対策やその程度については、各企業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等によって異なります。したがって、各企業において、本書や、IPAが公開している各冊子などを参考に自社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。

①ソフトウェアは、常に最新版にアップデートしましょう。

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、Flash Player、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。

具体的な方法については、IPA対策のしおりシリーズ（10）『標的型攻撃メール<危険回避> 対策のしおり』の7頁以降に紹介されています。
https://www.ipa.go.jp/security/antivirus/documents/10_apt.pdf

②ウィルス対策ソフトを導入しましょう。

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の購入元や家電量販店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の多くは購入後一定期間（1年間等）使用できるようになっているため、有効期限が切れていないか確認することも重要です。

③ファイアーウォールを設定しましょう。

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自社PCやサーバーに導入するものや、ルーターなど、専用の通信機器として、設置するものなどがあります。前者では、Windows をはじめ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、まずはこの機能を有効にすることで対応しましょう。

以上の具体的な方法については、IPA対策のしおりシリーズ（4）『不正アクセス対策のしおり』の8頁以降に紹介されています。
https://www.ipa.go.jp/security/antivirus/documents/04_fusei.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

（プラス１）システムのログの設定を確認しましょう。

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。

- サーバー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）
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