技術情報管理認証制度

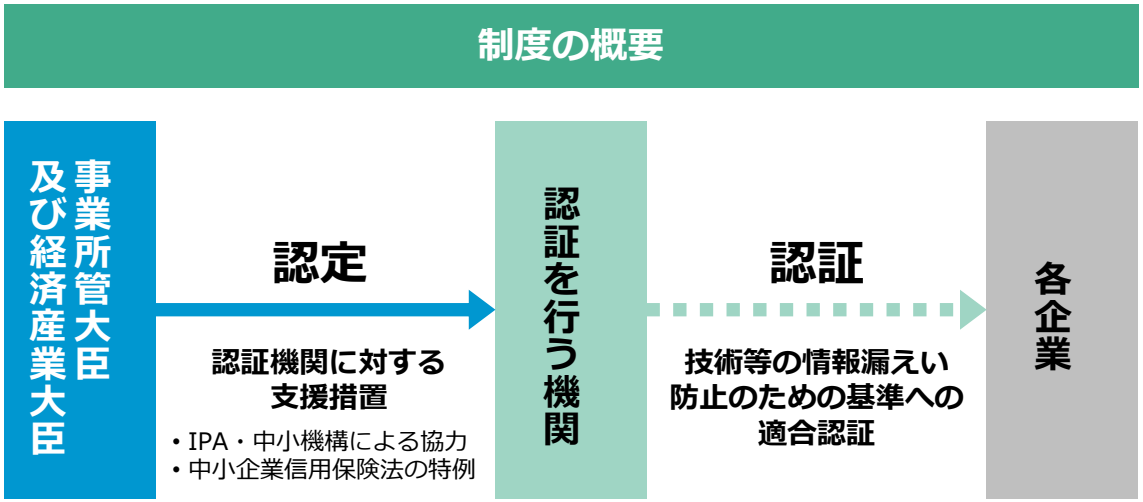
技術情報管理に関する研修素材

【本資料の使い方】

- 本資料は、「技術情報管理認証制度」で定められる基準を元に、技術情報管理に関して、より具体的な管理方法の例や様式サンプルを示したものです。
- 本資料は、以下の方々にご活用いただけます。
  - **情報管理を進める事業者、研究機関等の皆様**
    → 情報管理を進める際の具体的な方法として参照できます。
    → 内部監査を行う際に、管理方法についての妥当性を判断する参考にできます。
  - **助言を行う組織や専門家の皆様**
    → 事業者、研究機関等への助言の参考として活用できます。

技術情報管理認証制度とは

- 産業競争力強化法に基づき、事業者（企業や研究機関等）の技術等の情報の管理について、国で示した「守り方」に即して守られているかどうかを、国の認定を受けた機関による認証を受けられる制度（平成30年9月25日開始）

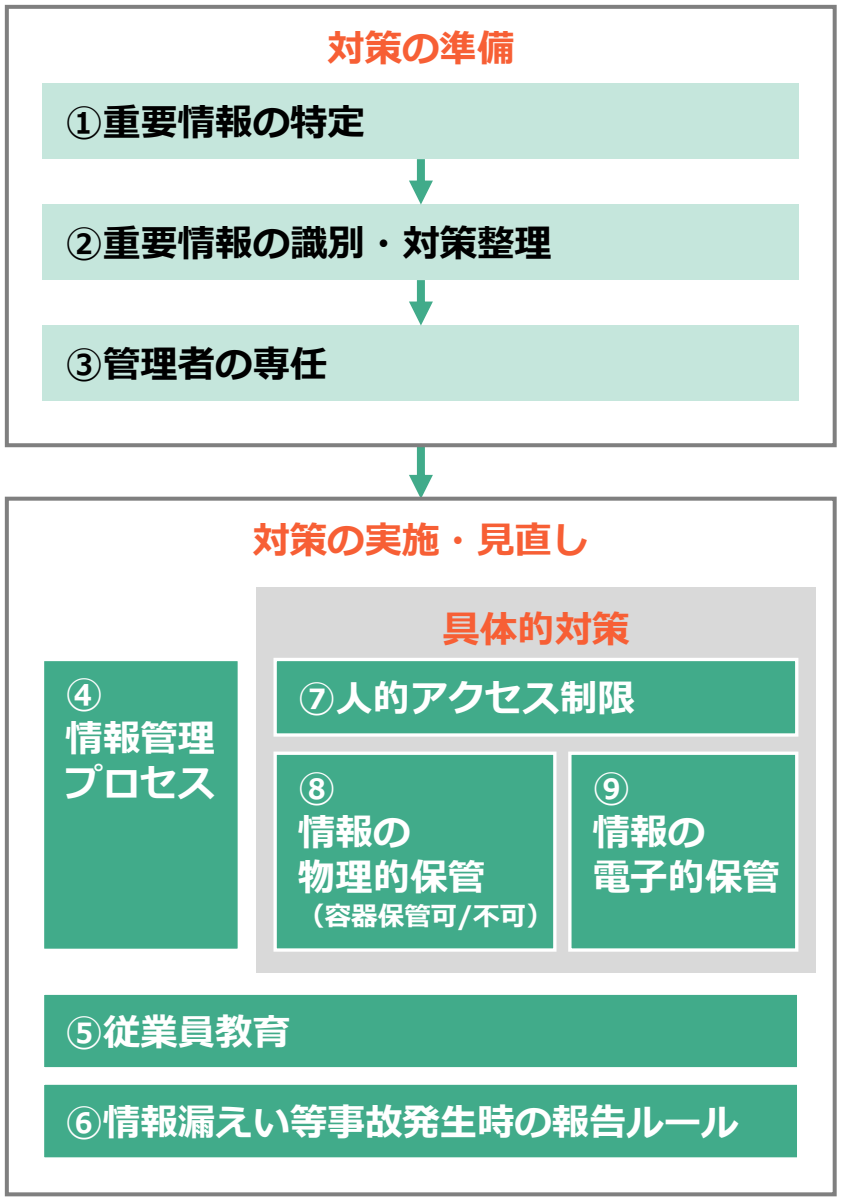


認証制度の特徴

1. 組織の**「強み」となる情報に絞った**管理状況が認証できます
2. **専門家の助言**を得ながら情報管理を進められます
3. 自組織の状況や情報の重要性により、**簡単な対策から**始め、**段階的にレベルアップ**できます

技術情報管理認証制度における情報管理の進め方

- 技術情報管理の取組を進めるには、**対策の準備**として以下を行います。
  - ① **重要情報の特定**
  - ② **重要情報の識別・対策整理**
  - ③ **管理者の責任**
- その後、実際の**対策の実施**として以下を行います。対策は、重要な情報の活用の仕方の変化や、従業員の管理状況などを踏まえて、必要に応じて**見直し**ます。
  - ④ **情報管理プロセス**の策定
  - ⑤ **従業員教育**
  - ⑥ **情報漏えい等事故発生時の報告ルール**の策定
- 情報管理における**具体的な対策**は、情報の態様（物理的な情報か電子情報か、保管容器に保管できるかできないか）を踏まえて以下の事項を実施します。
  - ⑦ **人的アクセス制限**
  - ⑧ **情報の物理的保管**
  - ⑨ **情報の電子的保管**
- 技術情報管理認証制度では、これらの①～⑨を必須の実施事項として定めています。これらを行うことにより、**重要情報の管理を包括的に進める**ことができます。



注）技術情報管理認証制度では、守るべき情報を「管理対象情報」としていますが、本資料ではわかりやすさのために「重要情報」と表現しています。

① 重要情報の特定

- 技術情報管理の取組を進めるには、**重要情報の特定が必要**です。
- 重要情報を特定する際は**経営層も関与し**、以下のポイントを考慮しましょう。
  ポイント1：その情報が漏えいすると、**自社の競争力に重大な影響**を与えますか。
  ポイント2：他社から契約等に基づき預けられた情報等で、その情報が漏えいした場合、**自社の信用や、他社との信頼関係等に重大な影響**を与えますか。
- 特定した情報は、必要に応じて保管場所等を記録した目録を作成し、保管しましょう。

守るべき情報（例）

「守るべき情報」とは、例えば以下のようなものが挙げられます。

目録（例）※1

業務分類	情報資産名称	備考	利用者範囲	管理部署	媒体・保存先	個人情報の種類			保存期限	登録日
						個人情報	要配慮個人情報	特定個人情報		
営業	製品カタログ	現役製品カタログ一式	営業部	営業部	書類					2016/7/1
営業	製品カタログ	現役製品カタログ一式	営業部	営業部	可搬電子媒体					2016/7/1
❶技術	❷製品設計図	❸現役製品の設計図	❹開発部	❺開発部	❻書類	❼			❾	❿2016/7/1

※1 情報処理推進機構「中小企業の情報セキュリティ対策ガイドライン 第3版 付録7 リスク分析シート「台帳記入例」」から抜粋

参考：「営業秘密」と認められる要件※2

「営業秘密管理指針」では、「営業秘密」として法的保護を受けるために必要となる最低限の水準の対策を示しています。

「秘密管理性」を満たすためには、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必要があります。

秘密管理性
①情報に**アクセスできる者を制限**していること
②情報にアクセスした者がそれが**秘密であると認識**できること

有用性
事業活動等に使用されることで、経費の節約、経営効率の改善等に役立つものであること

非公知性
情報の保有者の管理下以外では、一般に入手できないこと

※2 経済産業省「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）を元に作成

基準該当箇所 Ⅰ 共通事項　第一　適切な管理をする必要がある技術等情報の特定

② 重要情報の識別

- 重要情報は、**他の技術情報と区別して識別できるように表示**しましょう。
- 特定した重要情報については、情報の価値や種類等に応じて、必要な対策を決める必要があります。
- 他社から預けられた情報の場合は、契約内容等他社が求める対策を考慮して、必要な対策を検討する必要があります。

識別のための主な表示方法

紙の場合　　：紙そのものや、ファイル、書類棚等に「社外秘」等を表示し、守る情報であることを表示

電子情報の場合　　：ファイル名やフォルダ名に、守る情報であることを表示

試作品・製造装置の場合：保管容器にラベルを貼る、傍に看板を立てる等、守る情報であることを表示

紙の場合

電子情報の場合

【社外秘】設計図.doc

【関係者限り】試作品イメージ.ppt

モノの場合

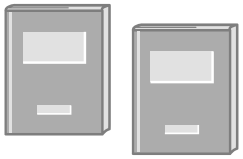
基準該当箇所　Ⅰ 共通事項　　第二　管理対象情報の識別と必要な措置の整理

③ 管理者の選任

- 経営層は、重要情報を守るための**対策推進に責任を持つ管理者を選任**する必要があります。
- 従業員数が多い場合や重要情報が複数の事業部門に関係する場合は、誰が管理者か従業員等が認識できるように、社内規程や社内掲示で周知しましょう。
- 従業員数が少人数の場合は、経営層が管理者を兼務する等、組織の規模に応じて適切な管理者を選任しましょう。

管理者の役割

（1）情報管理の**手順を確立**する。



（2）情報を取り扱う者の制限・管理、**従業員へのトレーニング**を行う。

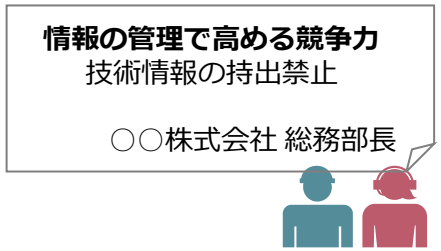
（3）情報漏えい防止**対策を実施**し、その実施状況を把握する。

（4）情報漏えいの兆候・事実の把握に努め、**事象発生時に必要な対応**を行う。

（5）（2）-（4）の**記録を取得し、保管**する。

周知の方法

- 「情報管理規程」にて、情報管理責任者を定め、社内研修にて周知する。
- 社内のポスター・標語で周知する。
- 朝礼等で適時に周知する。



Point
責任者を選任することで、対策を一元的に進めたり、組織としての意思決定を迅速に行うことができます。

基準該当箇所	Ⅰ 共通事項　　第三　管理者の選任

④ 情報管理プロセス（1/3）

- 重要情報を適切に管理するために、**重要情報の作成から廃棄までの情報管理プロセスを作成**する必要があります。
- 重要情報については、管理簿を作成し、情報の持出や複製・廃棄等の状況がわかるようにしましょう。
- さらに、情報管理プロセスは、従業員に周知し、情報管理の取組が習慣化するようにしましょう。

各プロセスの検討内容（例）

プロセス	検討内容例
作成	• 作成された情報が重要情報の場合、識別できるようにする手順を定める。
内容の伝達	• 情報へのアクセスが認められている従業員から、アクセスが認められていない従業員へ情報を伝える際の手順等を定める。
複製	• 重要情報の複製を認める際の基準や承認手順等を定める。
廃棄	• 重要情報を復元不可能な方法（細断や焼却等）で廃棄するための手順等を定める。

管理簿（例）

No.	対象情報	目的	媒体	取扱区分（収集・作成、保管、複製、利用、提供及び廃棄）	保管・持出場所	開始時			終了時			備考
						日付	担当者	承認者	日付	担当者	承認者	
1												
2												
3												
4												
5												
6												

基準該当箇所　Ⅰ 共通事項　　第四　管理対象情報の管理等

④ 情報管理プロセス（2/3）

情報管理規程の記載事項（例）

章	条	項目	内容
第1章 総則	第1条	目的	規程の目的
	第2条	適用範囲	規程の適用範囲
	第3条	定義	「秘密情報」等定義
	第4条	秘密情報の分類	「極秘」等分類
第2章 秘密情報の管理体制	第5条	管理責任者	管理責任者設置
	第6条	情報管理委員会	基準策定の委員会設置
	第7条	指定	秘密情報の指定、アクセス権者の範囲設定 等
	第8条	秘密情報の取扱い	規程及び基準の準拠
第3章 従業員等	第9条	申告	秘密情報取得時の申告
	第10条	秘密保持義務	秘密保持義務
	第11条	誓約書等	秘密保持誓約書の提出
	第12条	退職者	秘密保持契約の遵守 等
	第13条	教育	教育実施
	第14条	監査	監査実施・報告
第4章 社外対応	第15条	秘密情報の開示を伴う契約等	委託時の秘密保持義務
	第16条	第三者の情報の取扱い	秘密かどうかの確認、制約条件の明確化 等
	第17条	外来者・見学	運用手続の定め
第5章 雑則	第18条	罰則	違反時の罰則措置

情報管理基準の記載事項（例）

項目	小項目	内容
1.極秘情報の取扱い	(1)表示	「極秘」「○○限り」の表示
	(2)保管	区別した保管、暗号化・分離保管、施錠
	(3)複製	管理責任者のみ複製可、電子媒体やファイルの複製不可設定
	(4)閲覧	外部者への閲覧不可、要管理責任者許可、閲覧記録
	(5)配布	通し番号付与、会議後回収
	(6)社外への持出し	要管理責任者許可、暗号化・自らの携行・保管庫への保管
	(7)第三者への提供	要管理責任者許可・管理責任者下での開示・管理
	(8)廃棄	管理責任者管理下、読取不可形式での廃棄
2.対外秘情報の取扱い	(1)表示	「対外秘」の表示
	(2)保管	区別した保管、暗号化・分離保管
	(3)複製	複製の原則禁止、完了後の即座回収
	(4)閲覧	外部者への閲覧不可、画面表示注意
	(5)配布	「対外秘」表示、取扱方法説明　等
	(6)社外への持出し	暗号化・自らの携行・保管庫への保管
	(7)第三者への提供	要管理責任者許可・管理責任者下での開示・管理
	(8)廃棄	読取不可形式での廃棄

経済産業省「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）を元に作成

基準該当箇所　Ⅰ 共通事項　　第四　管理対象情報の管理等

④ 情報管理プロセス（3/3）

情報セキュリティポリシーの記載事項（例）

章	項目
1 組織的対策	1.情報セキュリティのための組織
	2.情報セキュリティ取組みの**監査・点検/点検**
	3.情報セキュリティに関する情報共有
2 人的対策	1.雇用条件
	2.従業員の責務
	3.雇用の終了
	4.情報セキュリティ教育
	5.人材育成
3 情報資産管理	1.情報資産の管理
	2.情報資産の社外持ち出し
	3.媒体の処分
	4.バックアップ
4 アクセス制御及び認証	1.アクセス制御方針
	2.利用者の認証
	3.利用者アカウントの登録
	4.利用者アカウントの管理
	5.パスワードの設定
	6.従業員以外の者に対する利用者アカウントの発行
	7.機器の識別による認証
	8.端末のタイムアウト機能
	9.標準設定等

章	項目
5 物理的対策	1.セキュリティ領域の設定
	2.関連設備の管理
	3.セキュリティ領域内注意事項
	4.搬入物の受け渡し
6 IT機器利用	1.ソフトウェアの利用
	2.IT機器の利用
	3.クリアデスク・クリアスクリーン
	4.インターネットの利用
	5.私有IT機器・電子媒体の利用
	6.標準等
7 IT基盤運用管理	1.管理体制
	2.IT基盤の情報セキュリティ対策
	3.IT基盤の運用
	4.クラウドサービスの導入
	5.脅威や攻撃に関する情報の収集
	6.廃棄・返却・譲渡
	7.IT基盤標準
8 システム開発及び保守	1.新規システム開発・改修
	2.脆弱性への対処
	3.情報システムの開発環境
	4.情報システムの保守
	5.情報システムの変更

章	項目
9 委託管理	1.委託先評価基準
	2.委託先の選定
	3.委託契約の締結
	4.委託先の評価
	5.再委託
10 情報セキュリティインシデント対応ならびに事業継続管理	1.対応体制
	2.情報セキュリティインシデントの影響範囲と対応者
	3.インシデントの連絡及び報告
	4.対応手順
	5.情報セキュリティインシデントによる事業中断と事業継続管理
11 個人番号及び特定個人情報の取り扱い	（個人番号及び特定個人情報の適正な取り扱いに関する基本方針）
	（個人番号及び特定個人情報取扱規程）

情報処理推進機構「中小企業の情報セキュリティ対策ガイドライン 第3版 付録5情報セキュリティ関連規程（サンプル）」を元に作成

基準該当箇所	Ⅰ 共通事項　　第四　管理対象情報の管理等

⑤ 従業員教育

- 重要情報の適切な管理の取組を進めるうえでは、**従業員等に対策を周知し情報管理に対する意識を高めるために、従業員教育を行うことが必要**です。
- 従業員教育の方法としては、社内会議での実施やe-learning等があります。
- 従業員教育は、1回実施するだけではなく、**定期的に実施**することが望ましいです。

全ての従業員等への教育内容（例）

以下のうち必要な項目について教育を実施します。

- 技術等情報（一般的な情報）と重要情報の違い
- 重要情報を適切に管理することの重要性、意識
- 重要情報を含む技術等情報の漏えいとその結果の事例
- 関係法令の内容
- マニュアル、技術等情報の適切な管理に係る文書の内容、関係法令等に違反した場合の処分等
- 重要情報の漏えいの事故等（重要情報の紛失の事故及び改ざん又は破壊がされた事実を含む）が発生したことを発見した場合の報告手続
- 標的型メール等の警戒すべき手口、標的型メール等による情報システムが提供する機能を妨害するウィルス、スパイウェア等の感染を防止するための対策、感染した場合の対処手順

アクセス権を有する者への教育内容（例）

以下のうち必要な項目について教育を実施します。

- Need to Knowの原則（情報は必要のある人のみ（情報へのアクセスは必要な人のみ）に伝え、知る必要のない人に伝えない（情報へのアクセスが必要ではない人にはアクセスを認めない。）という原則）を守ることの重要性（勤務において留意すべき事項を含む。）
- 重要情報の取扱手続の詳細
- 情報の漏えい等の兆候及び端緒のケーススタディ（私生活において注意すべき事項を含む。）

Point
教育は1年に1回以上定期的に行うことが効果的です。入社時、昇格・昇進の機会の研修や、朝礼など、定期的な会議の時間を使って資料配布、周知・注意喚起を行うことで、従業員の意識を高めることもできます。

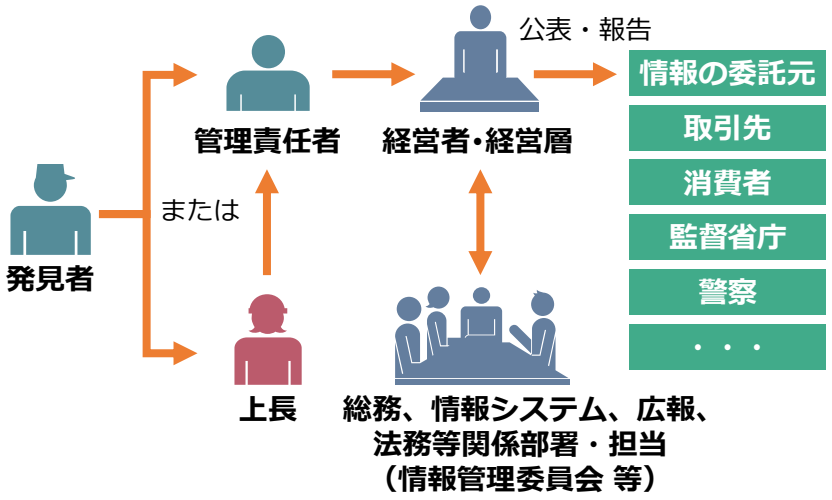
基準該当箇所　Ⅰ 共通事項　　第五　管理対象情報の適切な管理をするためのトレーニング

⑥ 情報漏えい等事故発生時の報告ルール（1/3）

- 重要情報の漏えいが疑われるような事故が発生した際に、被害の未然防止や拡大を防ぐために、**事故等発生時の報告ルールを策定し、従業員等に周知**する必要があります。
- 報告ルールには、どのような事象を発見したときに報告してほしいか、報告先は誰か等を整理しましょう。
  - 情報漏えいを完全に防ぐことは不可能です。
    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に備えておくことが重要です。
  - 対応にあたっては、以下に留意することが必要です。
    - 漏えいの疑いを確実・迅速に把握すること
    - 情報漏えいの損失を最小限に抑えるとともに、原因究明や証拠保全の措置を迅速に実施すること
    - 損失の回復と将来的な再発防止のための責任追及を実施すること

情報漏えい等事故発生時の報告ルート・対応体制

- 兆候を発見した者は、上長または管理責任者に報告します。
- 管理責任者は、速やかに経営者・経営層に報告を行います。
- 対応を行う人員は、組織内での情報拡散を防止するために、必要最小限の人数で構成します。
- 取り扱う内容については秘密保持を徹底します。

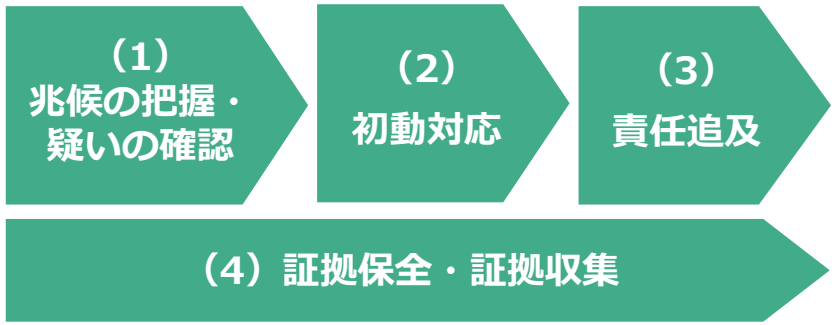


Point
発見者が日頃から上長や管理責任者に報告しやすいような風通しのよい風土を構築しておくことも有効です。

基準該当箇所	Ⅰ 共通事項　　第六　管理対象情報の漏えいの事故等の発生時等の報告

⑥ 情報漏えい等事故発生時の報告ルール（2/3）

事故発生時の対応フロー



Point

「異変」や「異常」に気づくためには、
「通常」の状態を把握しておかなければなりません。

- 日頃の従業員の業務の様子
  （業務時間、PCや情報の利用状況、業務場所等）
- 取引先とのやり取り（情報照会等の要求 等）
- 物品（機器、メディア 等）の設置場所

従業員からの報告や面談等を通じて上長や管理責任者が認識しておくことが必要です。

（1）兆候の把握、疑いの確認

- 情報漏えいの兆候が報告された場合、その状況が正しいかどうかの確認を行います。

（2）初動対応

- 現状を正しく把握します。（時系列で、いつ、誰、何、どのようにを把握）
- 自社、取引先、情報が漏えいした顧客、一般消費者等の関係者に対して、どのような被害・影響があるかを検証します。
- 被害防止・最小化の観点で、更なる拡散の防止、法律に基づく監督省庁等への報告、対外公表等を行います。

（3）責任追及

- 情報漏えいの際には、不正競争防止法上の営業秘密侵害罪（同法第21条等）、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）等に該当する可能性があることから、都道府県警察への相談も検討します。

（4）証拠保全・証拠収集

- 各過程において、漏えいの事実を裏付ける証拠を収集します。

経済産業省「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）を元に作成

基準該当箇所	Ⅰ 共通事項　　第六　管理対象情報の漏えいの事故等の発生時等の報告

⑥ 情報漏えい等事故発生時の報告ルール（3/3）

報告を求める事象（例）

対象	兆候
従業員等の兆候	• （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ー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 • 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
退職者等の兆候	• 退職前の社内トラブルの存在 • 在職時の他社との関係 • 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 • 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
取引先の兆候	• 取引先からの突然の取引の打切り • インターネット上での取引先に関する噂 • 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
外部者の兆候	• 自社における事件の発生 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

経済産業省「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）より抜粋

基準該当箇所	Ⅰ 共通事項　　第六　管理対象情報の漏えいの事故等の発生時等の報告

⑦ 人的アクセス制限（1/4）

- 重要情報を適切に管理するために、必要な人のみが重要情報にアクセスできるように、**適切なアクセス権の設定**を行いましょう。
- **アクセス権の設定状況は、定期的に確認・見直し**を行う必要があります。特に、従業員の異動時や退職時等は気を付けましょう。
- また、従業員による情報漏えいを防ぐために、守秘義務の厳守や退職後に業務中に知り得た情報を不正に使用しないよう、秘密保持の誓約書を締結することも有効です。

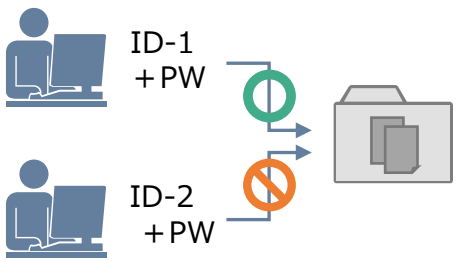
アクセス権の設定に関する考え方

- アクセス権を設定された者のみが重要情報を取り扱い得ることを明らかにします。
- アクセス権を設定する際には、以下を考慮します。
  - Need to Knowの原則に照らし、必要最小限の範囲となっているか否か
  - 情報の取扱いに係る社内規程への違反履歴
  - 退職、派遣元への復帰等、近い将来に自組織の直接の管理対象から外れる可能性
- アクセス権設定を一人の管理者が行っている場合には、アクセス権の設定に係る監査を他の者が行う仕組みを設けます。

Point
IDの登録作業は、複数の管理者が行うことで、適正な実施を確保できます。

アクセス権の管理方法

- アクセス権を設定された者の範囲は、定期的に、あるいはアクセス権の設定が必要となった業務の終了時点等の適切な時点で見直します。
- 退職等により必要のなくなった従業員等のアクセス権は、直ちに失効させます。
- アクセス権を設定された者の氏名、役職、アクセス権の設定年月日、トレーニングの受講の状況等、アクセス権を設定された者の状況を記録した管理簿を作成し、保管します。



従業員等に対して情報システム上のIDを付与し、そのIDを認証するパスワード（PW）等を設定します。

アクセス権を設定された者だけが、許可された電子データ等にアクセスできるように、IDを登録します。

⑦ 人的アクセス制限（2/4）

従業員の秘密保持について

- アクセス権を設定された者としての責任を明確にするため、アクセス権を設定された者から、以下のうち必要な事項を確保する秘密保持契約または誓約書を得ます。
  - 第三者に対する守秘義務を厳守すること。
  - アクセス権の設定の解除の後（退職後も含む） も アクセス権が設定されている間に知り得た重要情報について、公知になったものを除き、不正に開示したり、使用しないこと。
  - マニュアルその情報の取扱いに関する社内規程を遵守すること。
  - 重要情報の漏えいにつがなり得る事象等を発見した場合、指定された者に報告を行うとともに、重要情報の漏えいの事故等が発生した場合に必要な対応を行うこと。
  - 重要情報へのアクセスのログ等をアクセス権の設定を行った者等から確認されること。
  - 重要情報に接する必要がなくなった場合は、速やかに返却等の対応が求められること。

Point

従業員から秘密保持誓約書を得るタイミングは、入社・採用時、退職・契約終了時、在職中の取扱う情報が変更されるタイミング（昇進時等）が考えられますが、退職時にトラブル等が発生している場合は誓約書を得ることが難しいことがあります。
入社時に退職時も含めた誓約書を取得するとともに、在職中に研修と合わせる等して定期的に誓約を取得することで、適時な取得が可能になるとともに、従業員の意識を高める効果も期待できます。

⑦ 人的アクセス制限（3/4）

従業員の秘密保持契約・誓約書（例）　<入社時>

秘密保持誓約書

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情報管理規程を遵守し、次に示される貴社の秘密情報について、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契約を締結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）
１．第三者の秘密情報を含んだ媒体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）
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。

以上

平成____年____月____日
株式会社_____
代表取締役社長_____ 殿

住 所_____
氏 名_____ 印

経済産業省「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）より抜粋

基準該当箇所　Ⅱ　管理対象情報への人的アクセスの制限

⑦ 人的アクセス制限（4/4）

従業員以外（訪問者等）の秘密保持について

- アクセス権を設定された者以外の従業員等や、従業員等以外の者等（訪問者：（例）立入制限区域にある製造設備の見学者等）のように一時的なアクセスについて、以下の対応を行います。
  - 訪問者がNeed to Knowの原則を満たすものであるかを評価する。
  - 訪問者から、その訪問により得られた重要情報を第三者等に開示しないこと等を誓約する書面を得る。
  - アクセス権を設定された者の立会い等、重要情報を保護するために適切な措置を講ずる。

従業員以外（訪問者等）の秘密保持誓約書（例）<工場見学時>

秘密保持誓約書

____年____月____日

_____株式会社
_____殿

（所属/住所・名前）

この度、__年__月__日、貴社____工場を見学させていただくにあたり、私は、貴社が秘密である旨を明示し開示した一切の情報（以下「秘密情報」といいます。）について、厳に秘密を保持するものとし、第三者に秘密情報を開示しません。

以上

左：経済産業省「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）を元に作成

⑧ 情報の物理的保管（1/2）

- 重要情報が保管容器（金庫、キャビネット等）で保管できる（紙情報や試作品等）の場合、施錠して保管できる**保管容器を用いて保管し、物理的アクセスを制限**しましょう。
  - 鍵の適切な管理（鍵の貸出し管理簿作成、文字盤鍵の鍵番号の年1回以上変更　等）
- 保管容器から**情報を持ち出して取扱う場合や運搬する場合は、取扱のルール**を決めて、運用しましょう。
  - 運搬時の封筒の封印、受領証の受け取り、外部事業者との秘密保持契約締結　等

保管容器に求められる要件

- 施錠することができる保管容器を用いる。
- 保管容器の鍵の管理を行う。
  - 差込み式の鍵は、鍵の貸出し
  - 文字盤鍵の場合は、鍵番号の設定
- 鍵の管理手順を定める。
- 鍵の貸出し、鍵番号の共有を管理するための管理簿を作成し、保管する。
- 文字盤鍵の鍵番号は、年に1回以上変更する。
- 文字盤鍵の鍵番号は、以下のような事象が生じた都度、変更する。
  - 購入後の備え付け時、使用場所変更時
  - 管理者やアクセス権者が替わった場合
  - 鍵番号の漏えい（または恐れがある）時

保管容器の取り扱い場所

- 重要情報を保管容器から持ち出して、取扱いをする場所を限定するための手順を定める。

保管容器の運搬

- 重要情報を保管容器から持ち出し運搬することを、アクセス権を設定された者に限定するための手順を定める。
- 運搬時、重要情報を外部から見ることができず、運搬中の不正が確認できるようにするための手順を定める。（封筒に入れ封印する等）
- 重要情報の運搬後、受領証を受け取り、管理者に提出する手順を定める。
- 重要情報の運搬時、情報を引き渡した者と引き渡された者が相互に内容についての確認を行うための手順を定める。
- 運搬を信頼できる輸送機関又は運搬事業者に行わせる手順を定める。
- 運搬を行う外部事業者の情報管理について評価し、秘密保持契約を締結しているかを確認するための手順を定める。

基準該当箇所	
	Ⅲ　管理対象情報が書類等の紙情報や試作品等の物であって、金庫等の保管容器に保管することができるものである場合の物理的アクセスの制限等 Ⅳ　管理対象情報が製造装置である場合等保管容器に保管することが困難な場合等の物理的アクセスの制限等

⑧ 情報の物理的保管（2/2）

■ 製造装置等保管容器に保管できない場合は、**製造装置等を設置している場所の立ち入り制限区域にする等、物理的アクセスを制限**しましょう。
- 入退口の施錠管理、受付簿による立入状況の記録、立入者として視認可能な標識の着用　等

立ち入り制限区域について

- 壁等の物理的な境界で他の区域と区分することができる区域であり、全ての入退室口を施錠（差込み式の鍵、文字盤鍵、 キーパッド式の鍵、認証システム等）できる区域を立入制限区域として設定する。
- 立入制限区域の入退室口を、原則として業務時間中のみ開錠する。
- 立入制限区域への全ての者の立入りの状況を記録し、保管する。（鍵の管理簿の作成、受付簿の管理、IDによる認証の導入、作業者以外の者による同行・確認等）

<より高いレベルで管理を行う場合>

- 立入制限区域への不審者の侵入に関して、視認性を高める。（赤外線警報装置、セキュリティカメラ等の警備システムの導入等）
- 立入制限区域の警備システムが作動した場合の警備員等の駆けつけ体制を確保する。
- 警備員等がモニターにより立入制限区域及びその周辺を常時監視する体制を確保する。
- 警備員等により立入制限区域及びその周辺を定期的に巡回監視を実施する体制を確保する。

立ち入り制限区域への立ち入りについて

- 全ての立入者について、他の者から視認できるよう、立ち入ることが許されていることがわかる標識の着用を求める。
- カメラ、携帯型の情報通信機器等の持込みを原則として禁止する。持ち込む場合には、予め管理者の承認を得る手順を定める。
- 立入制限区域内の製造設備等の重要情報は、持ち出せないようワイヤ等で固定する。

運搬について

- 重要情報の運搬時に、正しく発出されているかどうか、発出した情報が正しく到着しているか確認する。

基準該当箇所	
	Ⅲ　管理対象情報が書類等の紙情報や試作品等の物であって、金庫等の保管容器に保管することができるものである場合の物理的アクセスの制限等 Ⅳ　管理対象情報が製造装置である場合等保管容器に保管することが困難な場合等の物理的アクセスの制限等

⑨ 情報の電子的保管

- 重要情報が電子情報の場合は、**パソコン等の可搬式記録媒体の持出を管理**しましょう。
- 電子情報を自社のサーバ等で保管する場合は、**IDやパスワード等による認証を行い、適切なアクセス制限を行い、必要な対策を実施**し、重要情報を適切に管理しましょう。
- 自社サーバではなくクラウドやデータセンターに保管している場合は、**委託先事業者と秘密保持契約を締結した上で、自社で行える対策を実施**し、重要情報を適切に管理しましょう。

電子情報の保管について

- 管理対象情報が電子情報である場合には、可搬式記録媒体（PC、USBメモリ等）の持ち出しを管理する。
- 内部サーバ等で記録している場合は、ID・パスワード等によりアクセス制限を行い、必要な対策を行う。

<外部環境を利用している場合>

- クラウド等外部サーバ等で記録している場合は、クラウド事業者の信頼性を確認する。
- データセンターに自らのサーバ等を設置している場合は、データセンターの信頼性を確認する。
- クラウド事業者やデータセンター事業者との間で秘密保持契約を締結する。
- クラウドやデータセンターの対策を踏まえ、自組織で必要な情報管理を実施する。

電子情報に対する主な対策について

- セキュリティに配慮した利用者の操作手順書の作成
- ファイアウォールの導入
- ログの取得・保存
- 不正アクセス検知時の対応手順の策定
- 脆弱性情報管理
- システム構成要素の管理簿の作成・管理
- ウィルス対策ソフトウェア等の導入・定期的な更新
- ソフトウェアの導入管理
- バックアップ
- アクセス権管理（一意のID、適切な利用権限、パスワード管理）
- クリアデスク
- 持ち出し手順の作成
- 外部委託管理

基準該当箇所	Ⅴ　管理対象情報が電子情報である場合のアクセスの制限等