技術等情報管理に関する研修素材

技術等情報管理の重要性

技術等情報管理がなぜ重要か、具体的な漏えい事例を含め解説します。

技術等情報管理に必要な対策

技術等情報を守るために必要な対策を解説します。

自社の対策状況チェック

自社の技術等情報管理の対策状況を「チェックリスト形式」・「クイズ形式」で確認できます。

参考情報

技術等情報管理認証制度やセルフチェックシート、監査ガイドライン等技術等情報管理に関する情報を紹介します。

技術等情報管理の重要性

- 技術等情報は、企業の重要な経営資源の1つです。
- 情報管理が不十分で情報漏えいや紛失を起こすと自社の業務や売上に影響が出るだけでなく、取引先からの信頼低下、取引停止につながる可能性があります。
- 自社及び取引先から預かった**技術等情報を適切に管理・活用することは、企業が事業活動を継続し、競争力を強化していくための第一歩**です。

技術等情報の漏えい事例

情報漏えい事例	概要	想定される原因	有効と想定される対策
A社 （個人情報流出）	• グループ企業勤務の派遣社員が顧客情報を持出し名簿業者に売却。 • 情報流出した**顧客に対する補償金の支払いや顧客の流出等の影響が発生**。	• 外部委託先の管理不備 • 外部記憶媒体の管理不備	人的アクセス制限（外部委託先のアクセス権） 情報の電子的保管（外部記憶媒体の管理）
B社 （転職時の技術情報持出）	• 元従業員が競合他社に**転職する際に設計図の情報を持出**。 • 元従業員は有罪判決。	• 情報へのアクセス権設定の不備	人的アクセス制限（必要な情報のみアクセス権設定）
C社 （海外企業への情報持出）	• 業務提携先の元社員が**研究データを不正に持出。転職先の海外企業へ提供**。 • 元社員は有罪判決を受け、転職先の海外企業とは和解金の支払いで合意。	• 外部記憶媒体の管理不備	情報の電子的保管（外部記憶媒体の管理）

情報を適切に管理できず、技術等情報が漏えいすると、
- **売上減、企業の競争力低下**
- **顧客や取引先からの信頼低下**

が発生する可能性

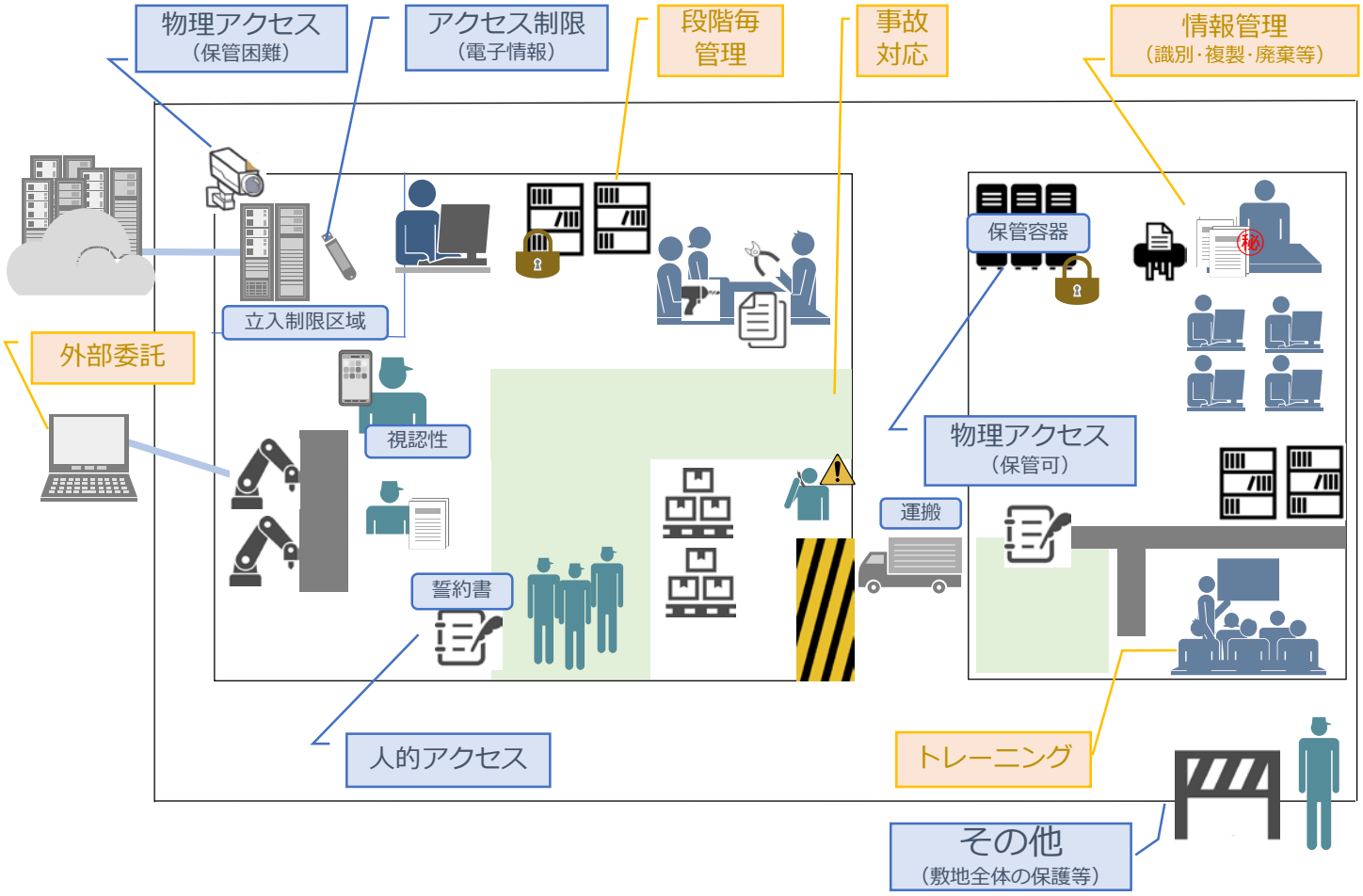
トップに戻る

技術等情報管理に必要な対策

技術等情報管理の必要最低限の取組を対策を進めるための事前準備と、情報の保管方法や従業員教育等の個別の対策があります。
これから対策を検討される方は事前準備から確認することをおすすめします。
すでに対策を進められている方は、自社の対策が不十分な箇所、気になる箇所から学ぶこともできます。

対策を進めるための事前準備

- 守る情報の決定
- 守る情報の識別・対策整理
- 管理者選任



トップに戻る

守る情報の決定

トップに戻る

- 技術等情報管理の取組を進めるには、**守る情報（管理対象情報）の特定が必要**です。
- 守る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：その技術等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、その技術等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。

技術等情報の例

【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

【セルフチェックシートの項目】

X.X	追加予定

守る情報の識別・対策整理

トップに戻る

- 特定した守る情報（管理対象情報）は、**<u>他の技術等情報と区別して識別できるように表示</u>**しましょう。表示方法は以下のようなものがあります。
  - 紙の場合　　：「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　　：ファイル名に記録し、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等、守る情報であることを表示
- 特定した守る情報（管理対象情報）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。

紙の場合

【社外秘】設計図.doc

【関係者限り】試作品イメージ.ppt

電子情報の場合

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

【セルフチェックシートの項目】

X.X	追加予定

管理者選任

トップに戻る

- 経営層は、管理対象情報を守るための**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管理対象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
情報管理プロセスの確立
人的アクセスの制限・管理、従業員教育
情報を守るために必要な対策の実施と状況把握
情報漏えい等事故の把握や対応
各種対策について記録を取得・一定期間保管

【基準該当箇所】

Ⅰ　共通事項	第三　管理者の選任

【セルフチェックシートの項目】

共通事項　整理番号1

情報管理プロセス

トップに戻る

- 管理対象情報を適切に管理するために、**管理対象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。
- 管理対象情報については、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。

各プロセスで検討する内容の例

プロセス	検討内容例
作成	• 作成された情報が管理対象情報の場合、識別できるようにする手順を検討
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検討
複製	• 管理対象情報の複製を認める際の基準や承認手順等を検討
廃棄	• 管理対象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検討

さらに取組を強化する場合・・・

管理対象情報は**段階別に管理**しましょう。
（価値の高い情報は、アクセス者を限定、対策を組合せて強化　等）

敷地全体を保護しましょう。
（外周の金網、監視カメラ等の侵入防止、監視・駆けつけ体制　等）

外部委託先を管理しましょう。
（情報は全体像がわからないよう渡す、情報蓄積による漏えいを防止する契約）

【基準該当箇所】

Ⅰ　共通事項	第四　管理対象情報の管理等

【セルフチェックシートの項目】

共通事項　整理番号2－19

従業員教育

トップに戻る

- 技術等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効果的**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**しましょう。

以下の内容等の従業員教育を定期的に実施

- 管理対象情報を適切に管理することの重要性や意義
- 情報管理に関する社内規程やルール
- 情報漏えい等が発生したときの報告ルール　　等

【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

【セルフチェックシートの項目】

共通事項　整理番号20－22

情報漏えい等事故発生時の報告ルール

トップに戻る

- 管理対象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。

報告を求める事象の例

私有のUSB等への管理対象情報の複製・持出

競合他社等との頻繁な接触・情報提供

【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

【セルフチェックシートの項目】

共通事項　整理番号23－32

人的アクセス制限

トップに戻る

- 管理対象情報を適切に管理するために、必要な人のみが管理対象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。

人的アクセス制限・管理する際のポイント
管理対象情報にアクセスできる人が必要最小限の範囲となっているか
アクセス権の定期的な見直しの実施（プロジェクトの終了時や、異動・退職時等）
管理対象情報へのアクセス権を設定した人への責任明確化（秘密保持の制約等）
一時的な訪問者（見学者等）を受け入れる場合のルール（誓約書面の取得、立ち会い等）

【基準該当箇所】

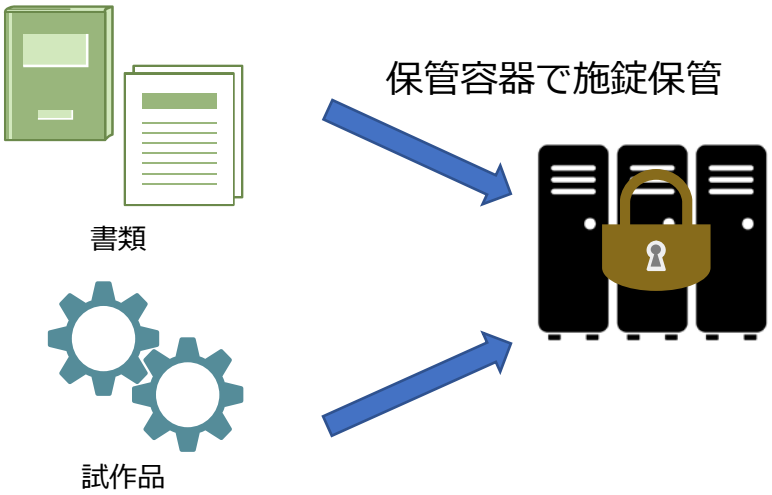
Ⅱ　管理対象情報への人的アクセスの制限

【セルフチェックシートの項目】

共通事項　整理番号33－57

情報の物理的保管

- 管理対象情報が保管容器（金庫等）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
- 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



【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

【セルフチェックシートの項目】

「適切な管理をすべき技術の情報」が紙情報の場合　整理番号1－47
「適切な管理をすべき技術の情報」が試作品や製造装置等の物の場合　整理番号1－79

情報の電子的保管

トップに戻る

- 管理対象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、管理対象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、管理対象情報を適切に管理しましょう。

情報システムの管理対策の例
パソコンへ等のウイルス対策ソフトをインストールし、定期的に更新・スキャンする
OS等を最新の状態に更新する
ファイヤーウォールやIDS/IPS等を導入する
アクセスログを取得し定期的に確認する
不要なネットワークポートやUSBポート等を使用不能にする

【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

【セルフチェックシートの項目】

「適切な管理をすべき技術の情報」が電子情報の場合　整理番号1－92

■ 情報管理を進める際の具体的な対策について、実際に企業で対策を進める担当者の立場で考え、クイズ形式で確認しましょう。

<ストーリー>

Xさんは、大手自動車メーカ向けに部品を製造する中小企業A社に勤務しています。

最近、主な取引先であるB自動車から、B自動車の製造にかかわる情報の徹底管理を求める指示が来ました。

B自動車の指示を受けたA社の社長は、情報管理の取組を強化することを決定し、Xさんをリーダーに指名し対策を検討するよう指示しました。

リーダーに指名されたXさんは取組の検討を開始しました。

ストーリー1	ストーリー2	ストーリー3	ストーリー4
対策開始	対策の考え方・社員教育	具体的な対策実施	情報漏えいの発生
■ 技術等情報の特定・識別・管理者の選任までの内容に関するクイズ	■ 作成から廃棄までの管理プロセス、保管形態別の対策、社員教育に関するクイズ	■ 事故発生時の報告ルールと人的アクセスに関するクイズ	■ 事故発生時の報告ルールと人的アクセスに関するクイズ
情報管理に初めて取り組む企業が最初に実施する事項		情報管理の具体的な対策	事故発生時の対応、必要な対策

【ストーリー1-1　対策開始（技術等情報の特定）】
リーダーに指名されたXさんは情報管理の取組を進めるにあたり、最初に自社が保有する情報を調べることにしました。

そこで、Xさんは各事業部門の協力を得て、情報の一覧を作成しました。

一覧を基に、Xさんは、社長と共に自社が守るべき情報を決めることにしました

＜クイズ1-1＞
あなたが、Xさんの場合、どのように守る情報を決めますか。

１．各事業部門から提出された情報をすべて守る必要がある情報と判断する

２．B自動車に関する情報だけが守る必要がある情報と判断する

３．自社の競争力や他社からの信用への影響等を考慮し判断する

＜解答＞
　すべて正解

＜解説＞
守る必要がある情報を決める際は、自社への競争力への影響等の基準を基に判断する必要があります。
何れの選択肢も判断基準を基に守る必要がある情報を特定しているため、すべてが正解となります。

ただし、「1．各事業部門から提出された情報をすべて守る必要がある情報と判断する」のようにすべての情報を守る必要があると判断し、同じレベルの対策を実施した場合、業務に支障がでる可能性があります。

技術等情報管理の対策を進めるうえでは、利便性も考慮することが必要です。

【ストーリー1-2　対策開始（技術等情報の識別）】
自社で守るべき情報を特定した結果、A社では部品の設計図（電子と紙媒体で保管）と部品そのものが、守るべき情報でした。

Xさんは、守るべき情報を適切に守るためには、どの情報が守るべき情報かを社員が一目で認識し、わかるように表示する必要があると考えました。

そこで、まず、電子情報について対策を考えることにしました。

＜クイズ1-2＞
あなたが、Xさんの場合、どのような工夫を実施しますか。

１．電子情報も自社の守るべき情報であることを従業員に周知し理解してもらう

２．電子情報は、管理対象情報以外もすべて守るべき情報として「社外秘」の表示を入れるルールとし、認識してもらう

３．電子情報を守るべき情報の対象から外し、識別不要とする

＜解答＞
１．電子情報も自社の守るべき情報であることを従業員に周知し理解してもらう

＜解説＞
守るべき情報を適切に守るためには、他の情報と識別できるようにすることが重要です。
守るべき情報が何かを従業員に周知し理解してもらうことも重要です。

「２．電子情報は、管理対象情報以外もすべて守るべき情報として「社外秘」の表示を入れるルールとし、認識してもらう」

この場合、管理対象情報以外の電子情報すべてに「社外秘」を入れた場合、本来の管理対象情報が不明確になってしまいます。

「３．電子情報を守るべき情報の対象から外し、識別不要とする」

この場合、従業員が守るべき情報等を認識できず、適切な管理が行われない可能性があります。そのため、情報漏えい等のリスクが高まります。

【ストーリー1-3　対策開始（管理者の選任）】
自社が守るべき情報（部品の設計図（電子と紙媒体で保管）と部品そのもの）を特定したことにより、Xさんは今後具体的な対策を検討・実施していく必要があると考えました。

対策を推進していくためには、対策の責任者を決める必要があるとXさんは考え、社長に相談することにしました。

社長と相談した結果、3人の候補が挙がりました。

候補者①：B自動車向け部品を製造する部署の責任者

候補者②：社内の情報システムを管理する情報システム部門の責任者

候補者③：経営者である社長

＜クイズ1-3＞
あなたが、Xさんの場合、どのメンバーが最適だと考えますか。

1．候補者①：B自動車向け部品を製造する部署の責任者

2．候補者②：社内の情報システムを管理する情報システム部門の責任者

3．候補者③：経営者である社長

＜解答＞
3．候補者③：経営者である社長

＜解説＞
管理者を選任するに際には、守るべき情報の種類や関係する部署等を考慮する必要があります。
A社の守るべき情報はB自動車向けの情報だけではなく、電子情報だけでもありません。
このことから、全社を広く見ることができる社長が適任と考えられます。

「１．候補者①：B自動車向け部品を製造する部署の責任者」
A社の守るべき情報は「部品の設計図（電子と紙媒体で保管）と部品そのもの」で、B自動車向けの情報だけではありません。そのため、B自動車向け部品を製造する部署の責任者では、守るべき情報のすべてを見ることができません。

「２．候補者②：社内の情報システムを管理する情報システム部門の責任者」
A社の守るべき情報は「部品の設計図（電子と紙媒体で保管）と部品そのもの」 で電子情報だけではなく、紙情報やものがあります。そのため、情報市捨て部門の責任者では、守るべき情報のすべてを見ることができません。

【ストーリー2-1　対策の考え方・社員教育（管理プロセスの決定）】
任命された責任者のもと、Xさんは具体的対策を進めていくことにし、取組のはじめとして、情報の作成から廃棄までの情報管理プロセスを整備することにしました。

A社ではこれまで全社統一の情報管理プロセスはなく、情報管理の取組は各部署に任されていました。

Xさんは情報を守るためには全社統一の情報管理プロセスを作成したほうがよいと考え、作成することにしました。

＜クイズ2-1＞
あなたがXさんの場合、情報管理プロセスを作成する際どのようなことを実施しますか。

１．各部署の既存の情報管理プロセスを確認し、全社統一のものを作成する際の参考にする

２．自社で作成した情報のみを管理対象とし、プロセスを作成する

３．管理プロセスを詳細に作成し、例外は認めない運用とする

＜解答＞

１．各部署の既存の情報管理プロセスを確認し、全社統一のものを作成する際の参考にする

＜解説＞

情報管理プロセス（作成から廃棄まで）を検討する際は、既存のプロセスを参考にすることで、従業員の負担軽減やルールが順守されやすくなります。また、自社で保有している情報だけではなく、顧客から提供を受けている情報の管理方法も検討する必要があります。

「２．自社で作成した情報のみを管理対象とし、プロセスを作成する」

A社ではB自動車向けの部品を作成するにあたり、B自動車から設計情報等様々な情報の提供を受けている可能性があります。自社で作成した情報のみを対象とした場合、顧客から提供を受けた情報を適切に管理できない可能性があります。

「３．管理プロセスを詳細に作成し、例外は認めない運用とする」

事業を進めていく中では、管理プロセス策定当初は想定していなかった事例等が発生する可能性があります。例外を認めない運用とした場合、想定外の事例に対応できないため、想定外の事例が発生したときどのように対応するかを検討していくことが望ましいです。

【ストーリー2-2　対策の考え方・社員教育（形態別の保管ルール）】
自社で守るべき情報を特定した結果、A社では部品の設計図（電子と紙媒体で保管）と部品そのものが、守るべき情報でした。

そこで、Xさんは物理的対策と電子情報への対策を検討し、必要な対策を整理しました。

必要な対策を整理したXさんは、対策を実施するにあたり、各部署の責任者に対策内容の説明し意見を受け付けることにしました。すると、各部署の責任者から以下のような意見が出ました。

- 部品を保管容器で保管する等物理的な対策はわかるが、電子情報の対策はこれまで実施した経験がなくどのように実施すればよいかわからない
- 対策内容が、現場の業務実態とかけ離れており、業務が回らなくなる可能性がある

各部署の意見を基に、Xさんは対策を再度検討することにしました。

＜クイズ2-2＞
あなたが、Xさんの場合どのように対策を見直しますか。

1．各部署の意見は理解したが、情報を守ることを優先し対策は変更しない

2．現場の業務実態を確認し、情報を守ることと業務遂行のバランスが取れるようにする

3．対策実施が難しい部署については、適宜サポートする

＜解答＞
　すべて正解

＜解説＞
情報管理の取組を進める上では、各部署の協力が必要不可欠です。
各部署の意見を踏まえつつ、情報を守ることと業務遂行のバランスが取れる対策を検討することが望ましいです。

「１．各部署の意見は理解したが、情報を守ることを優先し対策は変更しない」
適切な情報管理を進めるために、情報管理に十分な知識やノウハウを持つ部署/担当者が検討した対策を変更しないことも方法としては考えられます。一方、現場の理解が得られないまま対策を推進しようとした場合、情報管理に関するルールや対策が守られず、取組が形骸化する可能性もあります。

「２．現場の業務実態を確認し、情報を守ることと業務遂行のバランスが取れるようにする」
情報を守ることと業務遂行のバランスが取れるような対策の検討は、セキュリティを確保しながら事業推進を進める上で重要です。

「３．対策実施が難しい部署については、適宜サポートする」
対策実施を依頼する部署に十分なノウハウや知識が不足している場合は、適宜サポートし対策を進めてもらうことが望ましいです。

【ストーリー2-3　対策の考え方・社員教育（社員教育）】
全社統一の管理プロセス、保管形態別の対策を決めたXさんは、新たなルールを従業員に周知する必要があると考え、情報管理に関する従業員教育を実施することにしました。

A社ではこれまで、従業員教育を実施してきましたが以下のような課題が明らかになっています。

- 入社時等に研修は行っているが、定期的・継続的な研修ができていない
- 社内ルールを周知するために研修を行っているが、現場の業務が忙しいため参加率が低い
- 正社員は教育できているが、短期契約等非正規の従業員教育ができていない

＜クイズ2-3＞
A社の上記のような状況の場合、あなたはどのように従業員教育を行いますか。

１．新たな情報管理ルールについて、誰もが目にできるよう社内掲示する

２．情報管理に関する研修を定期的に開催する

３．短時間で確認できるよう、ルールのポイントをまとめた資料を作成し配布する

＜解答＞
　すべて正解

＜解説＞
情報管理に関するルールは策定しただけではなく、従業員に認知・理解してもらうことが取組の実効性を高める上で重要です。
様々な方法で周知するとともに、定期的に研修や情報発信をし、従業員の情報管理に対する意識を維持・向上させましょう。

【ストーリー3-1　具体的な対策実施（情報管理（作成・識別･複製･廃棄等））】
Xさんは、情報は作成から廃棄までのプロセスを通じて管理する必要があると理解し、それぞれのプロセスについて具体的な手順を定めることにしました。

Xさんは、社長と相談の上、A社において守るべき情報は、部品に関する紙の設計図、電子情報の設計データ、ものである試作品と定義しました。

＜クイズ3-1＞
あなたがXさんの場合、守るべき情報を作成する際には、どうしたらよいと思いますか。

1．管理すべき情報であると誰もがわかるよう、紙に「㊙」と記載する、電子情報のファイル名に「●●限り」を含める等、情報の識別を行う

2．管理すべき情報であると気づかれないよう、秘密であることは明示せず、取扱者だけに周知する

3．管理すべき情報の管理簿を作成し、状況が常にわかるようにしておく

＜解答＞

１．管理すべき情報であると誰もがわかるよう、紙に「㊙」と記載する、電子情報のファイル名に「●●限り」を含める等、情報の識別を行う

３．管理すべき情報の管理簿を作成し、状況が常にわかるようにしておく

＜解説＞

守るべき情報を作成した際は、その情報が守るべき情報であることがわかるように識別すること、管理簿を作成することが適切な管理に必要です。

「２．管理すべき情報であると気づかれないよう、秘密であることは明示せず、取扱者だけに周知する」

秘密であることを明示せず、取扱者だけに周知して守る方法も考えられます。ただし、この方法では、適切なアクセス権の管理をしていないと、取扱者以外の従業員が情報を閲覧したり、管理すべき情報として考えず、適切に管理しない可能性があります。

【ストーリー3-2　具体的な対策実施（情報管理（作成・識別･複製･廃棄等））】
Xさんは、A社において守るべき情報は、部品に関する紙の設計図、電子情報の設計データ、ものである試作品と定義しました。

Xさんは、情報管理のプロセス全体において適切に管理をするためには、利用終了後の廃棄まで対策を行う必要があると考えました。

＜クイズ3-2＞
あなたがXさんの場合、守るべき情報を廃棄する際には、どうしたらよいと思いますか。

1．紙はゴミ箱に捨て、電子情報はサーバやPCから削除する

2．ものについては、粉砕・破壊など、復元ができないようにして廃棄する

3．お客様から預かった情報は、お客様との取り決めに基づいて廃棄する

＜解答＞
２．ものについては、粉砕・破壊など、復元ができないようにして廃棄する
３．お客様から預かった情報は、お客様との取り決めに基づいて廃棄する

＜解説＞
情報を廃棄する際は、復元できない形で廃棄することが重要です。
お客様から預かっている情報は、お客様との取り決めに基づいて返却や廃棄する必要があります。

「１．紙はゴミ箱に捨て、電子情報はサーバやPCから削除する」
紙情報をゴミ箱に捨てただけでは、内容を読むことができるため情報漏えいにつながるリスクがあります。紙情報を廃棄する際には、シュレッダーでの細断や焼却等により復元不可能な方法で廃棄する必要があります。また、電子情報をサーバやPCから削除する際にも、完全消去や難読化等復元不可能な処理をする必要があります。

【ストーリー3-3　具体的な対策実施（人的アクセス制限（1））】
A社の工場には、工場で勤務する人だけではなく、オフィスの事務所にいる社員や、外部委託の事業者の方が機器の保守などで工場に入る場合があります。

Xさんは、工場にいる人が、立ち入りを認められている人かどうか区別する必要があると考えました。

＜クイズ3-3＞
あなたがXさんの場合、工場に立ち入りを認められている人とそうでない人を区別するためには、どうしたらよいと思いますか。

1．工場で勤務する人が工場に入る場合は、必ず決められた作業着を着用する

2．工場に入る場合は、社員も外部委託の事業者も、入口で必ず名前を記載する

3．工場で勤務しない社員が工場に入る場合は、管理者に立ち入り許可をもらい、
許可を示すタグなどを身につける

＜解答＞

１．工場で勤務する人が工場に入る場合は、必ず決められた作業着を着用する

３．工場で勤務しない社員が工場に入る場合は、管理者に立ち入り許可をもらい、
許可を示すタグなどを身につける

＜解説＞

立入制限区域内に立ち入ることが許可されている人と許可されていない人を確認できるよう、決められた作業着やタグ等の標識を着用してもらい、視認性を高める必要があります。

「２．工場に入る場合は、社員も外部委託の事業者も、入口で必ず名前を記載する」

工場に入る場合に、名前を記載してもらうことは、工場への入退室の記録を取るうえでは有効な対策です。ただし、この方法では工場へ立ち入りを認められている人とそうでない人を区別することはできないため、区別できるよう標識（腕章やストラップ等）の着用等の対策を組み合わせる必要があります。

【ストーリー3-4　具体的な対策実施（人的アクセス制限（2））】
Xさんは、勤務者や外部委託の事業者だけではなく、工場見学等で立入制限区域である工場に訪れる訪問者からの情報漏えいを防ぐ必要があると考えました。

＜クイズ3-4＞
あなたがXさんの場合、工場への訪問者の方からの情報漏えいを防ぐためには、どうしたらよいと思いますか。

1．訪問者が工場に入る場合、常に社員が立ち会うようにする

2．訪問者が工場に入る際に、管理対象情報を第三者等に開示しないことなどを誓約する書面を得る

3．訪問者が工場で知りうる情報は、必要最低限となるように立入場所、見学内容を決定する

＜解答＞
　すべて正解

＜解説＞
外部からの訪問者等による情報漏えいを防ぐためにも、社員の立会や誓約書の提出等を求めることが効果的な対策です。

【ストーリー3-5　具体的な対策実施（物理アクセス制限）】
Xさんは紙の設計図の保管方法について考えることにしました。

紙の設計図は、設計部門・開発部門のメンバーが日々、頻繁に利用していますが、各部門には、複数の部品の担当者がいて、他の担当の部品の設計図は双方が見られないように管理する必要があります。

＜クイズ3-5＞
あなたがXさんの場合、紙の設計図はどのように保管したらよいと思いますか。

１．設計図は部門毎のロッカーに保管して毎日施錠する

２．設計図は部品毎にロッカーに保管して毎日施錠する

３．設計図は部門・部品毎にロッカーに保管して、利用の度に施錠する

＜解答＞
　すべて正解

＜解説＞
どの方法でも、守るべき情報である設計図を守ることができますが、運用方法により追加の管理方法が必要な場合や業務に支障をきたす可能性があります。
対策を検討する際には、情報を守ることと業務遂行のバランスをとることが望ましいです。

「１．設計図は部門毎のロッカーに保管して毎日施錠する」
各部門のメンバーが他の部門の設計図を見ることが難しくなり、部門間での情報管理は実現されます。一方で、部門内のメンバーが他の担当の部品の設計図を見ることができる可能性があり、部門内での管理方法を別途考える必要があります。

「２．設計図は部品毎にロッカーに保管して毎日施錠する」
部品ごとにロッカーに保管することにより、各部品の担当者が他の部品の設計図を見ることが難しくなり、設計図ごとの情報管理は実現されます。

「３．設計図は部門・部品毎にロッカーに保管して、利用の度に施錠する」
利用のたびに施錠する運用は情報管理の観点からは有効な対策ですが、A社ではメンバーが頻繁に利用していることから、利用の度に施錠する運用では、現場の業務を阻害する可能性もあります。

【ストーリー3-6　具体的な対策実施（アクセス制限（電子情報））】
Xさんは電子情報の設計データの保管方法について考えることにしました。

設計データは社内のサーバ上に保管され、社員はPCにインストールされた専用のソフトウェアを用いて都度設計データを利用します。PCは設計データを利用する複数の社員が共有しています。

＜クイズ3-6＞
あなたがXさんの場合、設計データが利用可能なPCにおいて、専用ソフトウェアの利用時にはどのように管理したらよいと思いますか。

1．専用ソフトウェアを利用する社員のみに対して、共通のID・PWを設定する

2．専用ソフトウェアを利用する社員のみに対して、それぞれ別々のID・PWを設定する

3．専用ソフトウェアを利用する際のPWは推測されにくいものとする

＜解答＞
２．専用ソフトウェアを利用する社員のみに対して、それぞれ別々のID・PWを設定する
３．専用ソフトウェアを利用する際のPWは推測されにくいものとする

＜解説＞
セキュリティを確保するために、共通のID・PWを設定しないこと、PWは推測されにくいものにすることが重要です。

「１．専用ソフトウェアを利用する社員のみに対して、共通のID・PWを設定する」
共通のID・PWの設定は、運用上便利ではありますが、内部不正等で情報漏えいが発生した際に、誰がログインし情報を持ち出したのかを特定することが困難になる等、セキュリティ上のリスクがあります。

【ストーリー3-7　具体的な対策実施（アクセス制限（電子情報））】
Xさんは電子情報の設計データの管理についても気になりました。

設計データを取り扱うPCはインターネットに接続しておらず、メールやWeb閲覧はできませんが、プリンタやUSBメモリを利用することは可能です。また、PCが設置された工場内には、メールやWeb閲覧ができる事務用のPCは別に複数あります。

＜クイズ3-7＞
あなたがXさんの場合、設計データが利用可能なPCにおいて、設計データはどのように管理したらよいと思いますか。

1．USBは業務で利用するため、会社が用意したUSBのみ自由に使えるようにする

2．設計データは必要な場合のみプ印刷することとし、印刷した場合は「㊙」を記載する

3．業務上支障がない場合は、ソフトウェア上で、印刷ができない設定や社外でファイルを開けない設定を行う

＜解答＞

２．設計データは必要な場合のみプ印刷することとし、印刷した場合は「㊙」を記載する

３．業務上支障がない場合は、ソフトウェア上で、印刷ができない設定や社外でファイルを開けない設定を行う

＜解説＞

情報漏えいを防ぐためにも、業務上不要な印刷や持出をしないようにすることが重要です。
印刷や持出が業務上必要な場合は、そのためのルールを決めましょう。

「１．USBは業務で利用するため、会社が用意したUSBのみ自由に使えるようにする」

会社が用意したUSBのみを利用できるようにすることは、私用のUSB等を利用した情報持出を防止するためには効果的な対策です。ただし、自由に使えるようにするのではなく、USB等の記録媒体で情報を持ち出す場合のルールを定める必要があります。

【ストーリー3-8　具体的な対策実施（物理アクセス（保管困難））】
Xさんは電子情報の設計データの保管方法について考えることにしました。

設計データは社内のサーバ上に保管され、社員はPCにインストールされた専用のソフトウェアを用いて都度データを利用しています。また、PCを利用する社員には、それぞれ別々のID・PWを定めています。

社内サーバには、システム管理者以外にアクセスする必要はないものの、専用のソフトウェアがインストールされたPCは、業務時間中、複数の社員が頻繁に利用しています。

＜クイズ3-8＞
あなたがXさんの場合、電子情報が保管されたサーバはどのように保管したらよいと思いますか。

1．サーバは立ち入り制限を行う区域に設置し、立入制限区域の入退室口は、業務時間中のみ解錠する

2．サーバは立ち入り制限を行う区域に設置し、立入制限区域の入退室口は、常に施錠することを基本とする

3．PC及びサーバは立ち入り制限を行う区域に設置し、立入制限区域の入退室口は、常に施錠することを基本とする

＜解答＞

２．サーバは立ち入り制限を行う区域に設置し、立入制限区域の入退室口は、常に施錠すること
を基本とする

＜解説＞

アクセスする必要な人だけが入れるよう立入制限区域の入退室ルールを検討する必要があります。
この場合、サーバにアクセスが必要なシステム管理者のみが入退室できるようにすることが重要です。

「１．サーバは立ち入り制限を行う区域に設置し、立入制限区域の入退室口は、業務時間中のみ解錠する」

サーバを立ち入り制限を行う区域に設置することは、不必要な人がアクセスできないようにするために効果的な対策です。立ち入り制限区域の入退室口を業務時間中のみでも開場していた場合、立ち入る必要がない人も入室できてしまします。

**「３．PC及びサーバは立ち入り制限を行う区域に設置し、立入制限区域の入退室口は、常に施錠
することを基本とする」**

社内サーバはシステム管理者以外アクセスする必要はありません。この場合、サーバへのアクセスが不要な社員が頻繁に出入りすることになります。

【ストーリー3-9　具体的な対策実施（運搬）】
Xさんはものである試作品の運搬についても、管理しなければならないと考えました。
A社の試作品は、主にA社の別の敷地にある別工場と、B事業者に運搬するケースがほとんどです。

＜クイズ3-9＞
あなたがXさんの場合、試作品の運搬の際に、どのような対策を行ったらよいと思いますか。

１．秘密保持契約や受領の確認書類が必要ない、大手の運送事業者に運搬を依頼する

２．中の試作品が見えないよう、梱包して封印した上で運搬を行う

３．試作品を引き渡した人、受け取った人、相互に、内容を確認する

＜解答＞
２．中の試作品が見えないよう、梱包して封印した上で運搬を行う
３．試作品を引き渡した人、受け取った人、相互に、内容を確認する

＜解説＞
守るべき情報を運搬する際は、情報漏えいを防ぐために、運搬中の紛失や第三者から見られないようにする等の対策が必要です。

「１．秘密保持契約や受領の確認書類が必要ない、大手の運送事業者に運搬を依頼する」
大手の運送事業者であっても、運搬を依頼する事業者が信頼できる事業者であるかの確認をする必要があります。運搬するものによっては、セキュリティの高い方法で運搬するサービスの利用も検討する必要があります。

【ストーリー3-10　具体的な対策実施（その他（敷地全体の保護））】
Xさんは、A社の敷地内には工場とオフィスがありますが、守るべき情報はいずれの建物にも存在しているため、敷地全体の保護が有効であると考えました。
現在、工場・オフィスとも、建物にセキュリティカメラは設置していません。

＜クイズ3-10＞
あなたがXさんの場合、敷地全体の保護を行う場合、どのような対策を行ったらよいと思いますか。

1．敷地の外周を金網等で囲う

2．不審者の侵入を検知するための赤外線警報装置やセキュリティカメラ等を導入する

3．不審者の侵入が検知された場合は、警備員が駆けつける等のサービスを契約する

＜解答＞
　すべて正解

＜解説＞

　何れの方法も敷地全体の保護を行う上では有効な対策です。
　対策を検討する際には、対策のレベルや予算等を考慮しましょう。

【ストーリー4　情報漏えいの発生】
ある日、B自動車からA社の競合であるC社に部品の調達先を切り替えるとの連絡が来ました。

理由を確認すると、C社がA社と同等以上の部品を低価格で提供できるためとのことでした。

C社の部品を調査したところ、A社の技術ノウハウが活用されている疑いがありました。社長は自社から情報が漏えいしたのではと疑い、Xさんに原因調査を指示しました。

【ストーリー4-1　情報漏えいの発生（事故発生時の報告ルール）】
調査にあたり、Xさんは、開発部門の従業員にヒアリングすることにしました。

開発部門では、最近、YさんがC社に転職しており、退職前の数ヶ月間、1人最後まで残業することが増えていたり、開発に携わっていない部品の設計図をコピーするなど、Yさんの行動に違和感を感じていた従業員が複数いることがわかりました。

しかし、怪しいとは思ってはいたものの、同じ部門の仲間でもあり、誰かに報告することをためらっていました。また、誰に話せばよいかわからなかったという声もありました。

A社では、職場の安全衛生の観点から事故やヒヤリハットの報告ルールはありましたが、情報の漏えいに関する報告ルールはありませんでした。そのため、未然に防ぐことができなかったとXさんは考えました。

＜クイズ3-1＞
Xさんは、情報漏えいに関する報告ルールを策定することにしました。あなたが、Xさんの場合どのように報告ルールの策定しますか。

１．情報漏えいが発生していると確認できた段階で報告してもらう

２．守るべき情報について、持ち出し等怪しい兆候を把握したときも報告してもらう

３．報告窓口を明確にし従業員に周知する

４．情報漏えいの予兆や発生を把握したが、報告しなかった従業員は社内処分の対象とする

＜解答＞
２．守るべき情報について、持ち出し等怪しい兆候を把握したときも報告してもらう
３．報告窓口を明確にし従業員に周知する

＜解説＞
情報漏えいを未然防止するためにも、事故の発生だけではなくヒヤリハットや予兆の段階から報告してもらうことが重要です。
従業員が報告しやすいよう報告窓口等の環境整備を行いましょう。

「１．情報漏えいが発生していると確認できた段階で報告してもらう」
情報漏えいが発生した場合報告してもらうことが重要ですが、確認できた段階では対応が遅くなる可能性があります。確認が取れてなくても、情報漏えいの疑いの段階で報告してもらうことが、被害拡大等を防ぐうえで重要です。

「４．情報漏えいの予兆や発生を把握したが、報告しなかった従業員は社内処分の対象とする」
報告しなかった従業員を社内処分の対象とすると、従業員を委縮させ、報告が十分に上がらなくなる可能性があります。

【ストーリー4-2　情報漏えいの発生（人的アクセスの制限）】
Yさんが情報を持ち出した疑いが高まったことから、Xさんは重要な情報に必要な従業員のみがアクセスしているかどうかを調べる必要があると考えました。

Xさんは、情報システムにおける、Yさんのアクセス権限の設定状況と各種情報へのアクセスログを確認しようとしました。すると、開発部門では、従業員は自分が関わる製品のみならず、他の製品の情報にもアクセスできる状態にあることがわかりました。また、誰がどの情報にアクセスしたかどうかのログも取得できていませんでした。

A社では電子情報について、従業員のアクセス権の設定をしていましたが、開発部門では、開発の状況によってメンバーの配置を変更する場合があり、製品毎のアクセス権設定ができていませんでした。

＜クイズ3-2＞
上記のようなA社の状況の場合、今後どのような事態が生じると予想されますか。

1．Yさんが他の製品の情報も持ち出している可能性があり、C社からさらなる競合製品が発売される。

2．Yさんが情報を持ち出している事実を証明できず、法的に訴えることが難しい。

3．アクセス権の設定が適切でないことから、漏えいした情報が、企業として保護すべき情報と認められない場合がある。

＜解答＞
　すべて正解

＜解説＞

　適切な情報管理のための対策を実施していない場合、情報を持ち出されるだけではなく、十分な対策を実施していなかったことから、持ち出した従業員や競合他社を法的に訴えることが難しくなる可能性があります。

【ストーリー4-3　情報漏えいの発生（秘密保持契約の取得）】
Xさんは、Yさんを法的に訴えることを想定し、秘密保持契約書（NDA）の提出状況を確認することにしました。

しかし、確認したところ、Yさんが退職する前に、NDAを取得できていないことが発覚しました。

人事部に確認したところ、退職時のNDA提出はルールとして定められているものの、提出を拒んだり、忘れたりして提出をしないまま退社してしまう場合や、突然退社してしまう場合があり、NDA取得が難しいことがわかりました。

＜クイズ3-3＞
退社後も、自社の保護すべき情報を外部に不適切に漏らされることのないように、秘密保持契約（NDA）を確実に結ぶためには、どのような対策が取り得るでしょうか。

1．人事部にNDA取得の責任を持たせ、退職後も退職者を追いかけて確実にNDAを取得する

2．退職時に、NDAを結ぶことを、残った有給取得の消化やボーナス支給の条件にするなど、NDAを取得するための意欲を高める

3．入社時に、退職後の秘密保持を条項に含めたNDAを取得しておく

＜解答＞

３．入社時に、退職後の秘密保持を条項に含めたNDAを取得しておく

＜解説＞

在職中だけではなく退職後も、業務上知り得た情報を開示しないようにNDAを取得しておくことが望ましいです。入社時に取得することは、NDAを確実に取得するための有効な方法の1つです。

「１．人事部にNDA取得の責任を持たせ、退職後も退職者を追いかけて確実にNDAを取得する」

人事部にNDA取得の責任を持たせることにより、NDAを取得できる可能性は高まります。ただし、突然の退職等で退職者と連絡が取れないような場合は、NDAを取得できない可能性があります。

「２．退職時に、NDAを結ぶことを、残った有給取得の消化やボーナス支給の条件にするなど、NDAを取得するための意欲を高める」

NDAは、会社に一方的に有利な条件が含まれるケースがあるため、結ぶか結ばないかは従業員が選択できます。

技術等情報管理認証制度の概要

技術等情報管理認証制度は、企業の技術等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です。
技術等情報管理認証制度の詳細については、下記の経済産業省HP、パンフレットを参照してください。

経済産業省「重要技術マネジメント」
http://www.meti.go.jp/policy/mono_info_service/mono/technology_management/index.html

また、技術等情報管理認証制度は、認証取得を希望する企業向けに以下のサポートコンテンツがあります。

セルフチェックシート

- 自社の情報管理状況を自身で把握できるチェックシートです。告示の各項目について、確認時のポイント等をまとめてあります。

セルフチェックシートのイメージ及びURLを追加

監査ガイドライン

- 告示の各項目について、基準を満たしているかどうかを確認する際のガイドラインです。
- 主に認証機関の利用を想定したものですが、企業の方が認証取得に向けた準備や自己監査をする際に活用できます。

	概要
認証取得のために期待される到達レベルの考え方	• 監査ガイドラインに示した対策の考え方を示したものです。 • 対策を実施したり、内部監査を行う際、対策の目的や成果等について、より深く理解したいときに参照ください。
監査ガイドライン	• 認証取得時に、審査員が確認するポイントを示したものです。 • 対策を実施したり、認証取得時に審査員に対策状況を説明する際の参考として、ご覧ください。
監査の指針	• 認証取得に向け、内部監査を実施する際は、この指針に沿って実施してください。 • 外部の専門家に監査を依頼する際は、この指針に基づいているかを確認することが有効です。

監査ガイドラインのURLを追加

トップに戻る