NISA主催「中小企業のためのサイバーセキュリティ・セミナー」

（サイバーセキュリティを含む）

「経済安全保障」と「技術等情報の管理」

令和3年7月

長崎県　企画部／産業労働部
政策監　三上　建治
（前・経済産業省 製造産業局 技術戦略室長）

「技術等情報」とは何か？

〇外部に漏れると、**自社の競争力に重大な影響**がある内容
〇**他社から**契約等により得た情報等で、外部に漏れると、**自社の信用や、他社との信頼関係等に重大な影響**がある内容

守るべき「技術等情報」
（電子情報だけとは限らない）

※紙、物体、設備、知識

金型・試作品

製造装置・製造プロセス情報

研究情報

製造設計図・CAD

顧客情報・仕入先情報

業務マニュアル・
製造、業務ノウハウ

攻撃側
（悪人）

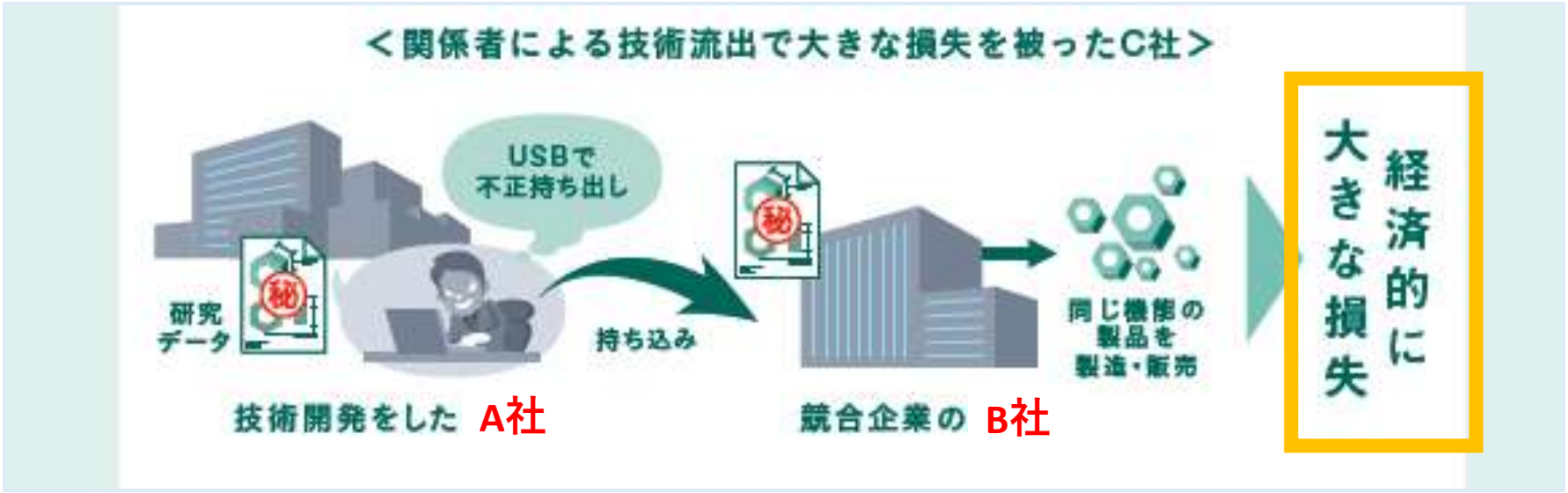
電子的通信
・クラウド

業務・
取引等
（善人）

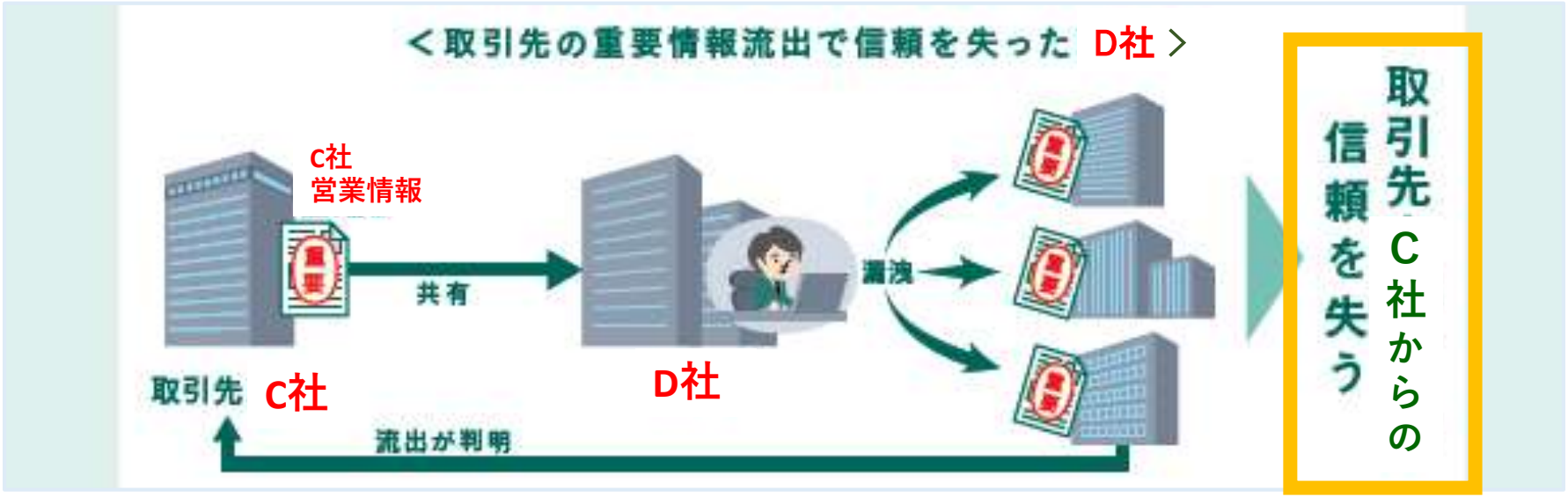
（参考）経済産業省「技術等管理認証制度の研修素材」を元に追加

情報漏えい・紛失による被害イメージ

＜自社情報の漏洩＞



＜他社情報の漏洩＞



（引用）経済産業省「技術等情報管理認証制度」パンフレット

技術等情報の管理の重要性

〇技術等情報漏洩の事例（イメージ）

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）

他にも「インターンの留学生が・・・」など

＜企業側＞
適切に管理できず、情報が漏洩すれば、
・売上減、企業の競争力低下
・顧客や取引先からの信頼低下

→　さらに、企業の「重要な情報」の流出は、国家としての安全保障の面でも、リスクになる可能性大（半導体、ソフトウェア、インフラ）

「経済安全保障」とは？

○　我が国から技術・データが流出した場合、**大量破壊兵器等の研究・開発に転用されるおそれ**や、**企業に対する信頼の低下**、**我が国企業や大学等における技術的優位の喪失に伴う国際的な競争力の低下にもつながり**かねない。

→　国益を守る規制、取締り強化の動き：　**「経済安全保障」**

外国において発生した経済安全保障に関連した事象（↓我が国も事象あり）

2018年

航空宇宙

▶米国当局は、同国航空宇宙関連企業から秘密情報を窃取しようとした容疑で中国情報機関員の身柄を拘束したと発表。容疑者はベルギーで逮捕され、身柄は米国に引渡し。

▶オーストラリア当局は、ニッケル合金をイランに不正輸出した容疑でオーストラリア在住の男女（女はイラン人）を起訴。同人らは、当該ニッケル合金は、オランダ企業のフランス工場で使用するためのものと説明していた模様。

新合金

2019年

▶米国カリフォルニア州上級裁判所は、オランダの半導体製造企業の米国子会社から同社元従業員の中国人らに秘密情報を窃取させたなどとして、中国などから出資された米国企業に対し、8億4,500万ドルの支払いを命令。

半導体

2020年

▶米国当局は、中国の人材招致計画に参加して金銭を受領していたにもかかわらず、米国において研究費を受領する際に、同人材招致計画に参加したことを秘匿して虚偽の申告をしたとして、同国大学教授を逮捕・起訴。

身分詐称

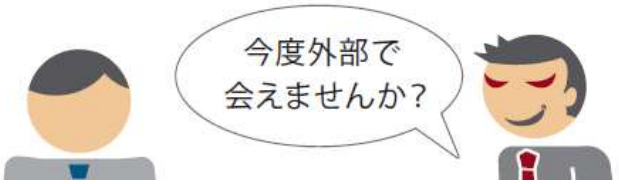
（引用）公安調査庁パンフ「経済安全保障の確保に向けて～技術・データの流出防止～」（2021年度版）を基に編集

世の中、「悪意」多し

未然・防止へ注意を

サイバー攻撃
～企業や大学等が保有する秘密情報の窃取～

不審なアプローチ
～従業員との1対1の関係構築～



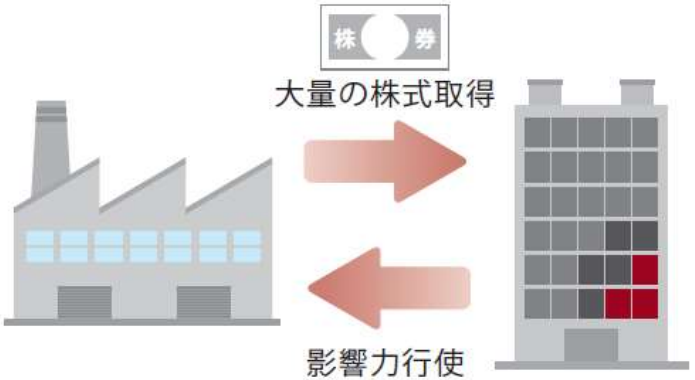
共同研究・事業
～技術・データの持ち出し～

経歴偽装による在籍
～留学生・研究者等の送り込み～

警戒心を持たれることを回避

人材リクルート
～技術に精通している従業員の引抜き～

投資・買収・合併
～影響力を行使して意思決定に関与～



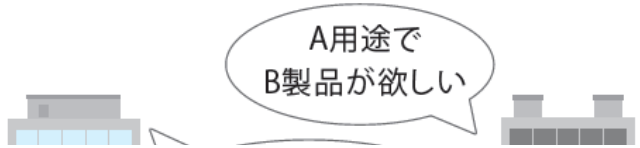
（引用）公安調査庁パンフ「経済安全保障の確保に向けて～技術・データの流出防止～」（2021年度版）を基に編集

通常取引にすらリスクも
（軍事転用の恐れも）

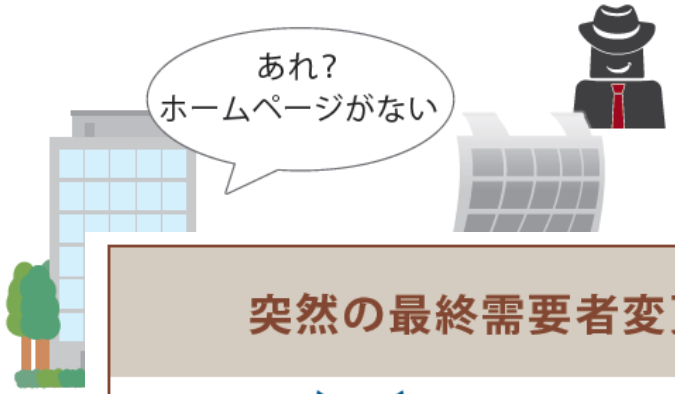
貴社に兆候はないか？

同一製品について同時期に複数の引き合い

用途と製品スペックの不釣り合い



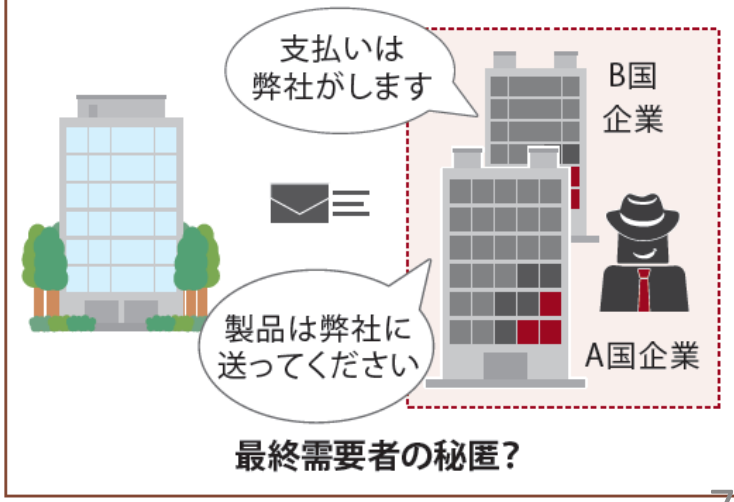
引き合い元企業のWEBサイトが存在しない



異なる企業の連絡先が同一

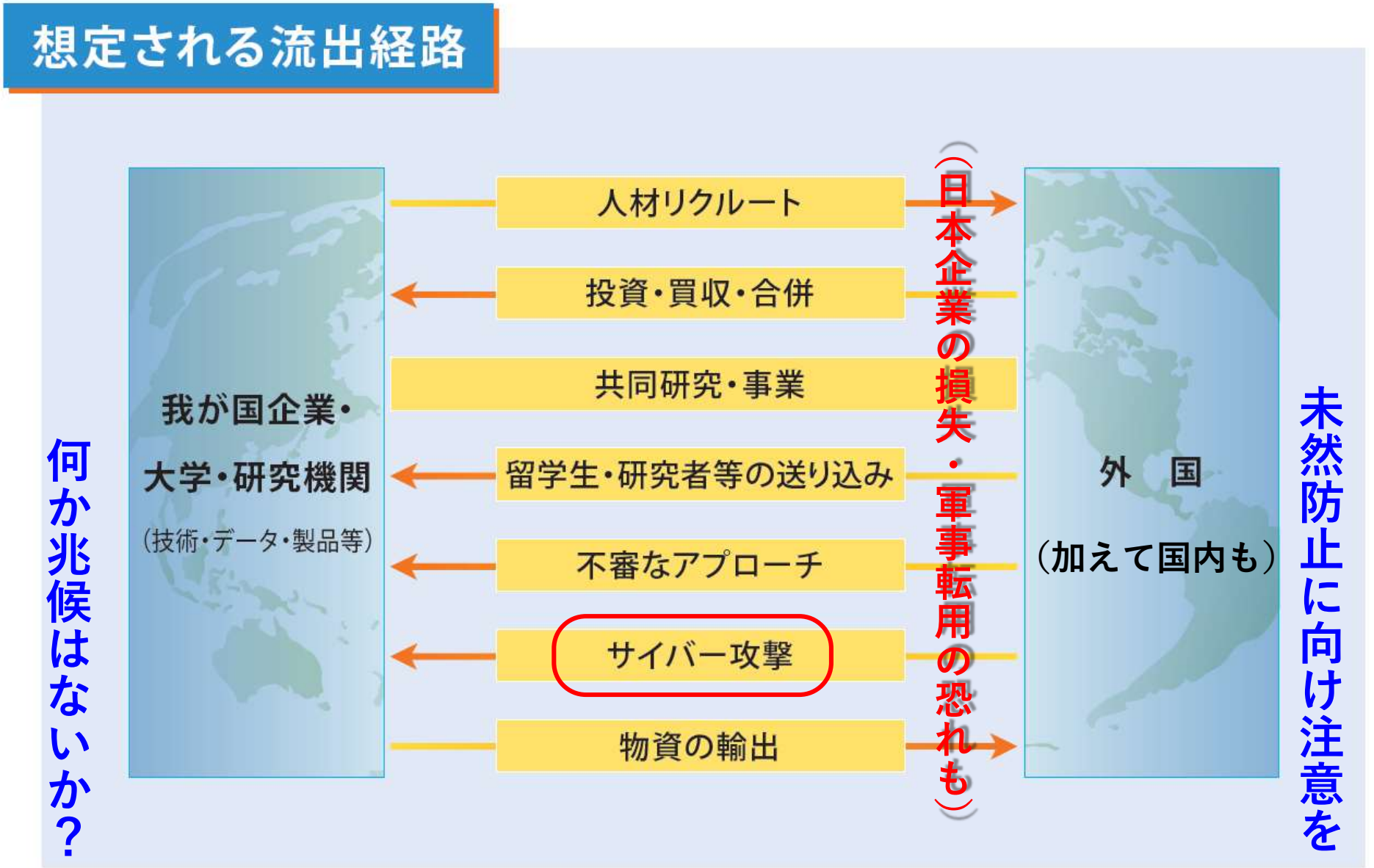
突然の最終需要者変更

受注先と支払い元の不一致



（引用）公安調査庁パンフ「経済安全保障の確保に向けて～技術・データの流出防止～」（2021年度版）を基に編集

結論：　気を付けるべきは「サイバーセキュリティ」だけではない

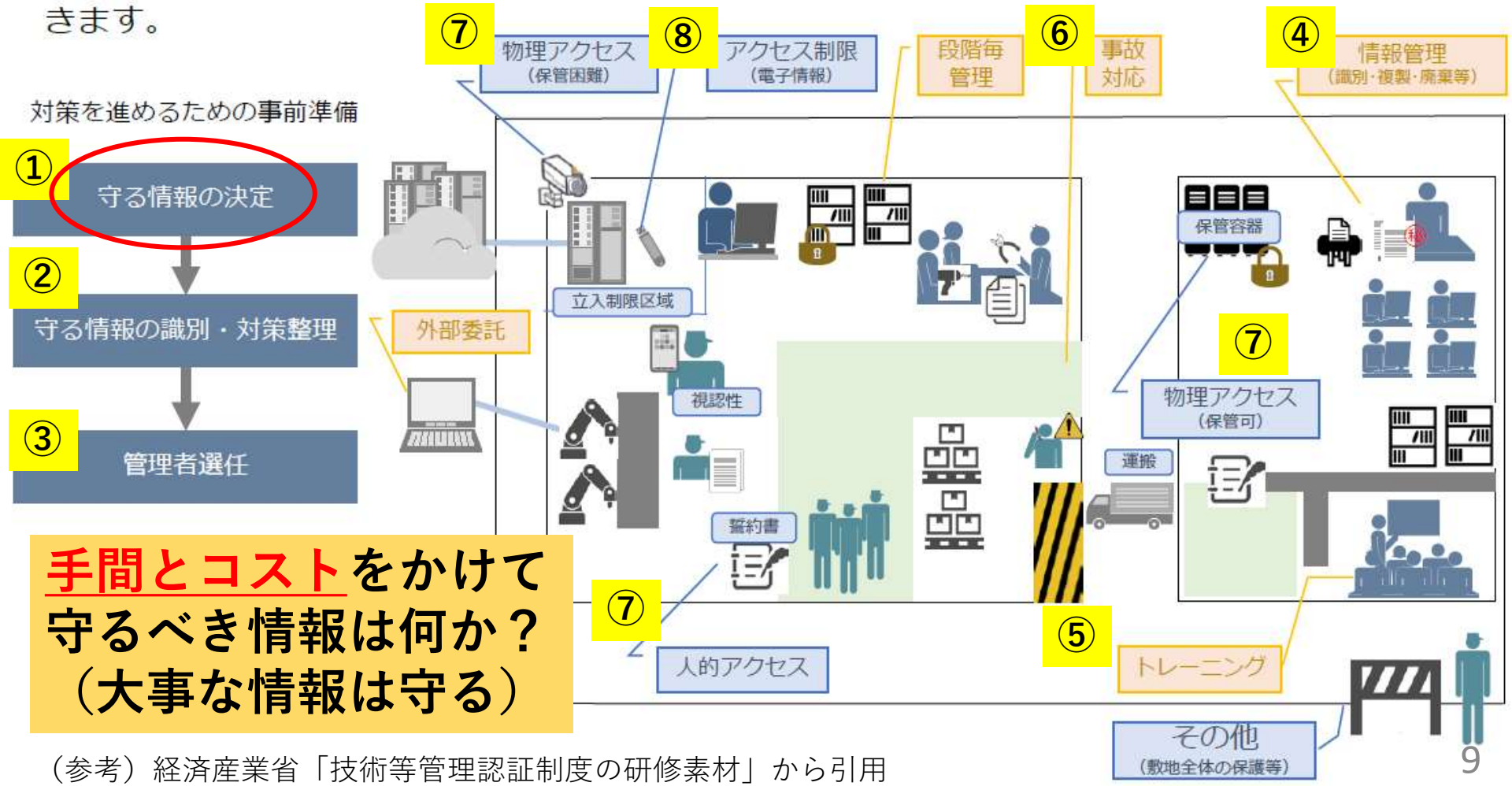


（引用）公安調査庁パンフ「経済安全保障の確保に向けて～技術・データの流出防止～」（2021年度版）を基に編集

その予防・対策は「サイバーセキュリティ」と似ている！

技術等情報管理に必要な対策（俯瞰図）

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。



<u>手間とコスト</u>をかけて守るべき情報は何か？（大事な情報は守る）

（参考）経済産業省「技術等管理認証制度の研修素材」から引用

（参考）経済産業省「技術等管理認証制度の研修素材」から

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

守る情報の決定 | 守る情報の識別・対策整理 | 管理者選任 | 情報管理プロセス | 従業員教育 | 情報漏えい等事故発生時の報告ルール | 人的アクセス制限 | 情報の物理的保管 | 情報の電子的保管

（参考）経済産業省「技術等管理認証制度の研修素材」から引用

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

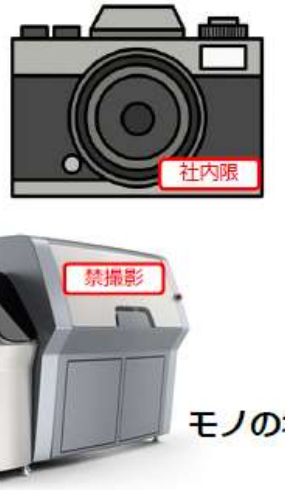
■ 特定した守る情報（管理対象情報）については、情報の価値や種類等に応じて、必要な対策を決める必要があります。他社から預けられた情報の場合は、契約内容等他社が求める対策を考慮して、必要な対策を検討する必要があります。

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

（参考）経済産業省「技術等管理認証制度の研修素材」から引用

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

（参考）経済産業省「技術等管理認証制度の研修素材」から引用

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

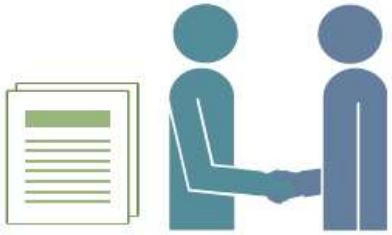
情報漏えい等事故発生時の報告ルール

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】

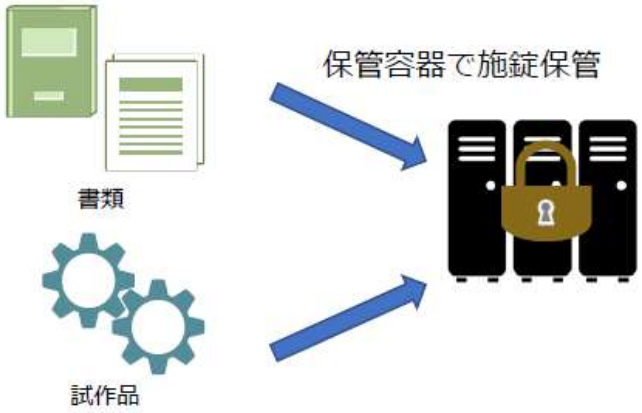
Ⅱ　管理対象情報への人的アクセスの制限

【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

技術等情報管理 研修素材中のクイズ例

トップに戻る

■ 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

技術等情報管理 研修素材中のクイズ例

【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。

<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。

技術等情報管理 研修素材中のクイズ例

【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。

<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。

普段・平時と**異なる何か**に気が付くか？

例：ある情報（物理、サーバ）へのアクセスが**普段より多い**（マイナーな案件なのに）

例：ある従業員の挙動が**不審**（業務ミス、ネット・メールの利用先、金遣い・借金）

物理的な保管庫へのアクセス

社内サーバへのアクセス

社内での業務状況（無気力、怯え、血気過ぎ）

プライベート（把握は難しいが）

まず、「普段・平常」を認知しているか？

→　モニタリングしかない（デジタルの活用）

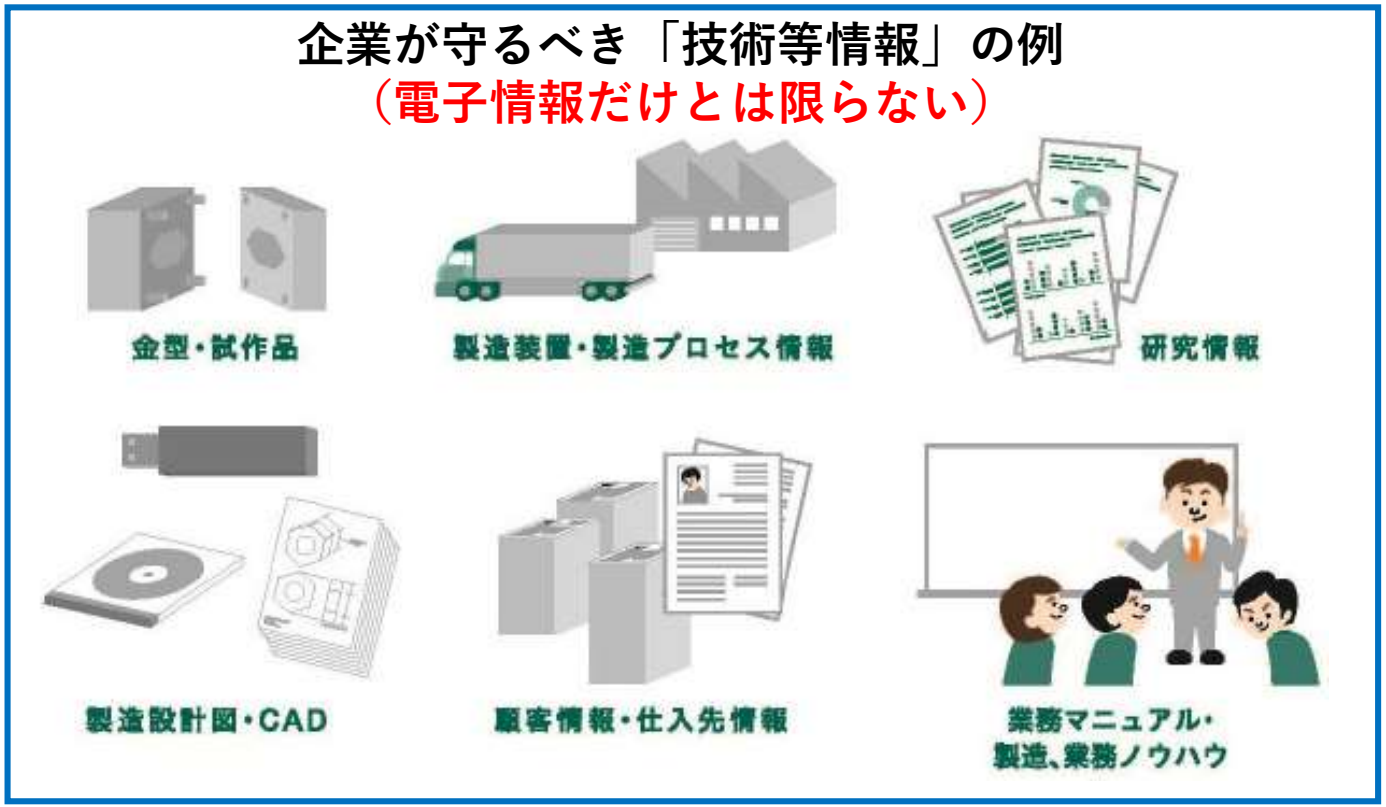
（まとめ）企業の大事な「技術等情報」を守る！

①**セルフチェック、自己監査**してみる　（IPA、経産省）

②**認証（第三者）**を取得して、示す　（IPA、ISMS、経産省）

③事案を**共有**し、**学び**、**備え**よう　（警察、公安、経産省）

→NEW ④「**万が一**」のことも考えよう　（セキュリティ保険）



（参考）経済産業省「技術等管理認証制度の研修素材」を元に追加

＜困ったことがあれば＞

【重要技術、輸出管理、知財・営業秘密】
→　**経済産業省、各経済産業局**

【犯罪】
→　**警察庁（各県警）**

【経済安全保障関連の調査・分析】
→　**法務省（公安調査庁）**

ご清聴

ありがとうございました