技術情報管理　自己チェックリスト　活用ガイド

自己チェックリストにおいて、対策ができているか判断に迷ったときは、この活用ガイドをご確認ください。

ファーストステップ　（経営の視点）

ファーストステップは、情報漏えいを防ぐための基礎的な確認事項です。
経営上も重要な情報漏えいを防ぐための取組の方針ですので、全ての事項を確認しましょう。

1　経営者とともに、守るべき情報を特定している。

守るべき情報とは、その情報が漏えいした場合に、
・自組織の競争力に大きな影響を与えるもの
・自組織の信用や顧客等との信頼関係に大きな影響を与えるもの（顧客等から預けられた情報など）
のことを言います。

理由	守るべき情報を明確にしないと、組織において情報の管理ができません。経営者が関わり、自組織の経営の観点から、どの情報を守るべきかを決める必要があります。
対策例	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・仕入れ先情報、業務マニュアル・製造/業務ノウハウなど、自社が持つ情報を洗い出し、経営者がその価値を判断して、守るべきかどうかを決めます。

2　守るべき情報が、紙情報、電子情報、試作品・製造装置などの物自体のどれに当たるかを分け、保管場所を記録している。

理由	守るべき情報の形態に合った保管を行わないと、情報漏えいを起こす恐れがあります。また、保管場所を明らかにしないと、情報が盗み出された場合にすぐに気づくことができず、被害が拡大する恐れがあります。
対策例	紙情報の場合はキャビネット、電子情報の場合はサーバ・PC・クラウド、試作品など小さな物は保管庫・金庫、製造装置など大きな物は設置された拠点・工場に保管します。

3　守るべき情報には、一目でほかの情報と区別できるよう、目印をつけている。

理由	守るべき情報だと思われないと、適切に管理されません。
対策例	紙情報の場合：情報が記載された紙に管理対象情報であること（社外秘等の表示）を記載します。 電子情報の場合：ファイル名に管理対象情報であることを記録します。 試作品・製造装置などの物の場合：当該物そのもの又はその保管容器に表示します。

4　取引先などから預けられた情報は、その取引先などの意向を聞いて、対策方法を定めている。

理由	自社だけで対策方法を定めると、顧客が求める対策と異なることで、対策が行われていないと判断される恐れがあります。
対策例	取引先の意向で示された情報の取り扱いに関する条件に従って、対策を行います。

5　経営層が、以下の取組に責任を持つ管理者を定めている。

（1）情報セキュリティのルールを作る。
（2）情報に触れる職員を制限・管理して、トレーニングする。
（3）情報セキュリティのルールを実行する。
（4）情報漏えいが起きそうになっていないかをいつも確認し、漏えいが起きたら対応する。
（5）（2）～（4）の取組状況を記録する。

理由	管理者を定めないと、役割や責任をもって情報管理を進められません。 また、組織における管理者の業務として正式に定めることで、管理者が情報管理に取り組む時間を確保するとともに、その成果を人事評価に反映することができます。
対策例	管理者として総務部門の責任者、情報システム部門の責任者、品質管理部門の責任者、製造部門の責任者などを定めます。

6	情報セキュリティの責任者が誰なのか、全従業員がしっかり分かるようにしている。
理由	責任者が認識されないと、従業員が管理者の指示に従わない恐れがあります。 責任者が認識されることで、従業員が報告や相談をしやすくなります。
対策例	責任者を社内のイントラネットに掲載します。

7	守るべき情報を作ってから廃棄するまでの全期間、しっかり管理するための取組を従業員が実践している。
理由	情報の作成から廃棄まで一貫して対策を行わないと、対策が不十分なところから情報漏えいを起こす恐れがあります。
対策例	守るべき情報の管理簿を作成し、守るべき情報には、情報に接することができる人のみに伝えられる、閲覧できるような手順を定めます。また、守るべき情報の複製や廃棄の手順を定めます。

8	全ての従業員に対して、情報セキュリティに関する意識を高めるためのトレーニング機会を設けている。
	トレーニングにおいて以下のうち必要なものを含みます。 (1) 技術等の情報と守るべき情報の違い (2) 守るべき情報を適切に管理することの重要性、意識 (3) 守るべき情報を含む技術等情報の漏えいとその結果の事例 (4) 関係法令の内容 (5) マニュアル、重要情報の適切な管理に係る文書の内容 (6) 関係法令等に違反した場合の処分等 (7) 重要情報の漏えいの事故等発生時の報告手続 (8) 標的型メール等の手口・ウィルス、感染防止の対策、感染した場合の対処の手順
理由	全ての従業員が情報セキュリティに対する意識を高めないと、従業員の対策の不備から情報漏えいを起こす恐れがあります。また、情報漏えいの兆候や事故が発生した際の従業員からの報告が遅れ、被害が拡大する恐れがあります。 情報セキュリティの意識が高い職場は、情報漏えいを起こしにくくなります。
対策例	全従業員に対して、情報の取扱いに関するe-learningを1年に1回実施します。週に1回、朝礼で情報の取扱いに関する注意喚起を行います。

9	守るべき情報の漏えいや不正な取扱いに気づいた場合の報告先を決めて、全従業員に知らせている。
理由	情報漏えい事故や不正な取扱いを見つけた場合の報告先がわからないと、報告が遅れ、情報漏えいの被害が拡大する恐れがあります。
対策例	情報漏えい事故や不正な取扱いに関する報告先を、e-learningで周知します。

10	守るべき情報の漏えいや不正な取扱いが発生した場合の対応手順を定めている。
理由	情報漏えい事故が発生した場合の対応手順を定めていないと、事故発生時に迅速に対応することができません。
対策例	責任者が情報漏えいの報告を受けた場合に、証拠を集めたり、事実を確認する手順や、対応を検討するための社内体制を定めます。

アイコンは、各項目がチェックリストで示されるレーダーチャートのどの項目に対応しているかを示しています。

ルール作り	ルールの実践	人的対策	設備的対策
サイバー対策	漏えいを起こさない	漏えい後の被害を抑える	取引先との関係

セカンドステップ （実務の視点）

セカンドステップは情報の漏えいを防ぐための具体的な対策です。
実務に沿って守るべき情報の種類を確認し、それぞれ必要な対策を実施しましょう。

11	守るべき情報を外部委託先などに渡す場合には、守るべき情報の第三者への開示の禁止を含む、秘密保持契約を締結している。
理由	外部委託先の情報セキュリティを契約で定めていないと、外部委託先等が情報を適切に管理せず、情報漏えい事故を起こす恐れがあります。また、外部委託先等が情報漏えい事故を起こした際に、責任を問えなくなる恐れがあります。
対策例	外部委託先等が、自組織からの情報の取扱いに関する指示に対応できるかどうか事前に確認し、秘密保持契約を交わした後に、情報を引き渡します。

12	守るべき情報に接することができる人を定め、その人以外が守るべき情報に接することがないよう制限している。
理由	情報に接することができる人の制限がなされていないと、守るべき情報に接することができる人以外が情報を盗み出す恐れがあります。
対策例	守るべき情報に接することができる人のみが、その情報を扱えるような手順を定めます。 守るべき情報に接することができる人の範囲を、定期的に見直します。 退職等により必要がなくなった従業員については、守るべき情報に接することができる権利を直ちに失効させます。 守るべき情報に接することができる人との秘密保持契約を交わします。

管理対象情報が金庫等の保管容器に保管できる場合（例えば、書類・試作品等）

13	守るべき情報を保管容器に施錠して保管している。
理由	情報に接することができる人以外が、守るべき情報に近づきやすい、あるいは持ち出しやすいと、情報漏えいを起こす恐れがあります。
対策例	守るべき情報を保管する金庫などを、施錠して管理します。 保管容器は、近づく者を確認することができる場所（カメラや人感センサーの設置、視認できるレイアウト）に設置します。

14	守るべき情報を書庫、金庫などから持ち出した場合に取り扱ってよい場所を定めている。
理由	情報に接することができる人以外が、守るべき情報に近づき、情報漏えいを起こす恐れがあります。 持ち出した際の取扱い場所を明らかにしないと、情報が盗み出された場合に気づくことができず、また気づいた後も状況の把握や原因の調査が難しくなることで、漏えいの被害が拡大する恐れがあります。
対策例	守るべき情報に接することができる人が、情報を金庫から持ち出し、取扱いをする場所を限定する手順を定めます。 守るべき情報の運搬時の持ち出し、取り扱う場所への運搬、保管容器への保存について、情報に接することができる人に限るための手順を定めます。

管理対象情報が金庫等の保管容器に保管できない場合（例えば、製造装置等）

15	守るべき情報が置かれる場所を立入制限区域とし、守るべき情報に接することができる人以外が立ち入らないよう制限している。
理由	情報に接することができる人以外が、守るべき情報に近づきやすい、あるいは持ち出しやすいと、情報漏えいを起こす恐れがあります。
対策例	守るべき情報が管理される立入制限区域の入退室管理を行います。 守るべき情報が管理される立入制限区域に不正に侵入する者の監視（カメラやセンサーの設置）を行います。 守るべき情報が管理される立入制限区域に不正に侵入する者が検知された場合の警備員等の駆け付け体制を整備します。

16	守るべき情報を他社の事業所等で取り扱う場合に、秘密保持契約を結び、施錠、巡回監視などを依頼している。
理由	他社に求める情報管理の取組を契約で定めていないと、他社が情報を適切に管理せず、情報漏えい事故を起こす恐れがあります。他社が情報漏えい事故を起こした際に、責任を問えなくなる恐れがあります。
対策例	守るべき情報を取り扱う他社が、建物の施錠・巡回監視を依頼し、契約を交わします。

管理対象情報が電子情報の場合

17	守るべき情報が保存されたPCや記録媒体の持ち出しを管理するなど、守るべき情報に接することができる人以外に情報を見られないよう制限している。
理由	情報に接することができる人以外が、守るべき情報に近づきやすい、あるいは持ち出しやすいと、情報漏えいを起こす恐れがあります。
対策例	守るべき情報が保存されたPCや記録媒体の持ち出し手順を定めます。 守るべき情報を取り扱うデスクは常に整理整頓し、守るべき情報が万一持ち出されてもすぐに気づくようにします。

18	電子ファイルにパスワードを設定するなど、守るべき情報に接することができる人以外に情報を見られないよう制限している。
理由	情報に接することができる人以外が、守るべき情報に近づきやすい、あるいは持ち出しやすいと、情報漏えいを起こす恐れがあります。
対策例	PCにログインするために、一人にひとつ、別々のIDを割り当てます。 IDを割り振られた人が、それぞれの業務に合わせて、電子ファイルを見られる範囲を定めます。

19	守るべき情報をクラウドサービスなどに保存するときは、信頼性を確認して保存先を決め、秘密保持契約を結んでいる。
理由	外部事業者に求める情報管理を契約で定めていないと、外部事業者が情報を適切に管理せず、情報漏えい事故を起こす恐れがあります。また、外部事業者が情報漏えい事故を起こした際に、責任を問えなくなる恐れがあります。
対策例	クラウド等を管理する者の信頼性を示す、ＩＳＯ／ＩＥＣ２７０１７の認証、日本セキュリティ監査協会クラウドセキュリティ推進協議会によるＣＳマークの取得の状況等を確認します。

情報セキュリティ対策に関する助言を受けたり、対策が十分かどうか第三者機関による審査が受けられる「技術情報管理認証」の取得もご検討ください。

技術情報管理認証制度

- 情報セキュリティの取組をマークで対外的に示せます
- 国が主導する制度のため、お客様や取引先の信頼につながります
- 国の一部の補助事業の審査で加点が受けられます

取組手順

専門家の助言や第三者による認証を受けたい方

国認定の認証機関に申込 → 情報管理に関する専門家の助言※ → 国の基準を満たすか審査 → 認証（国の基準を満たせば）

※ 希望する場合のみ助言を受けられます。
助言を行わない認証機関もありますので、詳細は認証機関にお尋ねください。

国の基準に則った対策を自組織で進めたい方

自己チェックリストで自己点検 → 研修素材を見ながら取組実施 → 自己チェックリストに何度でも再挑戦

技術情報管理認証制度　検索