

秘密情報の保護ハンドブック ～企業価値向上に向けて～

令和6年 2月

経済産業省 知的財産政策室



本資料でできること

本資料では、「秘密情報の保護ハンドブック」をお読みになる方に向けて、以下のポイントについて簡単にご紹介しております。

- ✓ ハンドブックと、営業秘密管理指針との違い
- ✓ ハンドブックの特徴や全体構成
- ✓ 情報漏えい対策の全体像と気を付けるべきポイント
- ✓ ハンドブック令和6年2月改訂で追加された内容
- ✓ 秘密情報漏えいの事例と対策
- ✓ 企業における秘密情報管理のための実際の取組

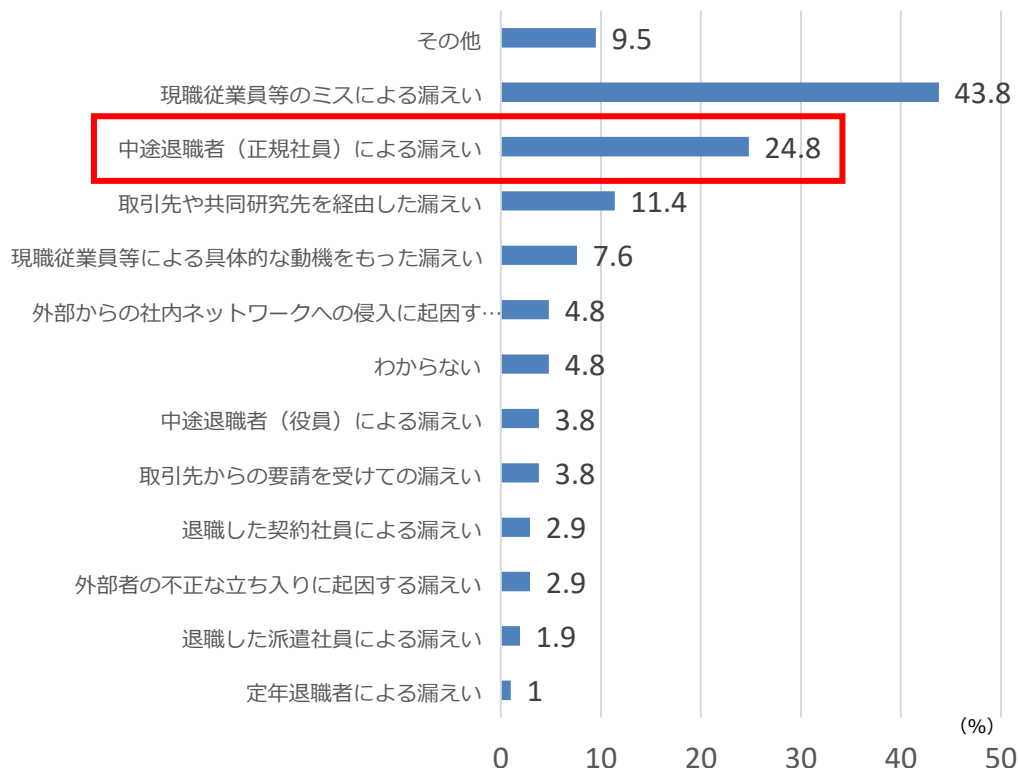
資料一覧

1. 情報の漏えいレートと近年増加するサイバー攻撃
2. 「秘密情報の保護ハンドブック」の位置づけ・「営業秘密管理指針」との関係
3. 「秘密情報の保護ハンドブックの特徴」
(参考) ハンドブックの全体構成
4. 「秘密情報の保護ハンドブック」情報漏えい対策 ～全体像～
5. 「秘密情報の保護ハンドブック」のポイント
(参考) 「営業秘密」の概要(営業秘密の3要件)
6. 「秘密情報の保護ハンドブック」情報漏えい対策
～効率よく講じるための5つの「対策の目的」～
(参考) 秘密情報の漏えい対策の5つの目的～犯行の段階に応じた対策の選択～
7. 「秘密情報の保護ハンドブック」の改訂について【令和6年2月】
8. 実際にあった?! 事例と対策とそのポイント(ケース1～6)
9. 企業における秘密情報の管理の事例(①～⑩)

1. 情報の漏えいルートとサイバー攻撃の現状

- 情報の漏えいルートは様々ですが、**従業員のミスに次いで、「中途退職者による漏えい」が多いのが現状です。**
- また、外部からの攻撃も続いている中で、近年は**ランサムウェア被害が急増**。様々な局面に情報漏えいリスクが潜んでいます。

情報漏えいルート

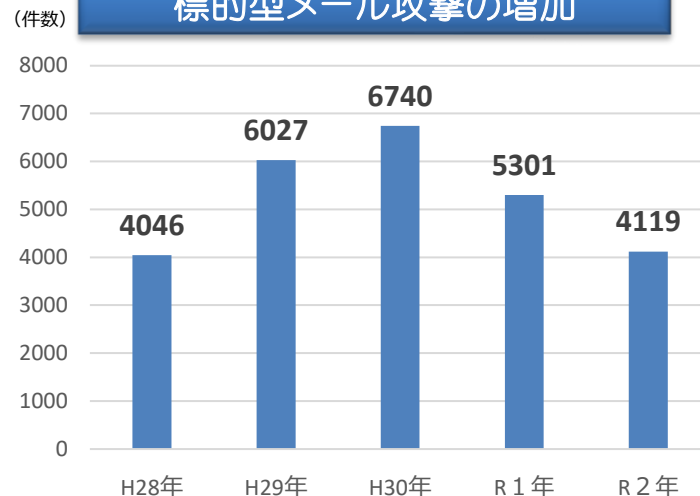


（出典）IPA『令和2年度 「企業における営業秘密管理に関する実態調査」報告書（回答約105社）』

企業の秘密情報は、
内部からも外部からも漏えいする恐れがあり、
それぞれに適切な対策を講じる必要があります。

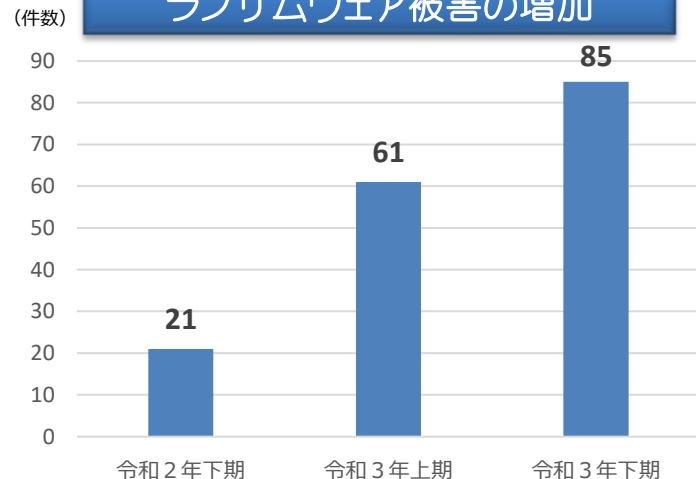


標的型メール攻撃の増加



（出典）警察庁 サイバー空間をめぐる脅威の情勢について

ランサムウェア被害の増加



（出典）警察庁 令和3年におけるサイバー空間をめぐる脅威の情勢等について（速報版）

2. 「秘密情報の保護ハンドブック」の位置づけ・「営業秘密管理指針」との関係

- 当室では営業秘密に関する様々な資料を公表していますが、代表的な2冊の違いは以下のとおりです。
- 「指針」と比べて網羅性を重視した「ハンドブック」は分量も多いため、必ずしも全てを読みこむ必要はありません。自社の実情を踏まえて、必要な対策を取捨選択・検討するための辞書のようにお使いください。

営業秘密管理指針について

<https://www.meti.go.jp/policy/economy/chizai/chiteki/guideline/h31ts.pdf>

- 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**を示すものとして平成27年1月に策定。
- その後、第四次産業革命を背景とした情報活用形態の多様化を踏まえて**平成31年1月に改訂**※。

※ 外部クラウドを利用して営業秘密を保管・管理する場合も、秘密として管理されていれば秘密管理性が失われるわけではない旨等を追記。

秘密情報の保護ハンドブック
(漏えい防止レベル)

営業秘密管理指針
(法的保護レベル)

秘密情報の保護ハンドブックについて

- 法的保護レベルを超えて、**情報漏えい対策として有効と考えられる対策**や、漏えい時に推奨される**包括的対策等**をできる限り収集して**網羅的に紹介するもの**として平成28年2月に作成。
- より良い漏えい対策を講じたい企業の方々に、企業の実情に応じて対策を取捨選択したり、参考としていただけるよう、**様々な対策を網羅的に掲載**。

!

ハンドブックを初めてお読みになる前に…



簡易版の「ハンドブックのてびき」では、イラスト付きで**秘密情報管理の基本となる考え方**を解説しています。

ハンドブックへの導入・理解を助ける資料となっていますので、ぜひご活用ください。

https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/170607_hbtebiki.pdf

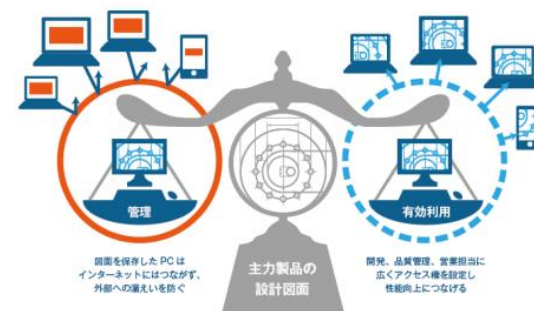
3. 「秘密情報の保護ハンドブック」の特徴

漏えいルートごとの対応策を掲載

- 典型的な情報漏えいルートとして、①従業員等、②退職者等、③取引先、④外部者と整理。漏えいルートごとに対応策を講じることが重要です。

情報漏えいの対策を講じる企業の拠り所となる考え方を紹介

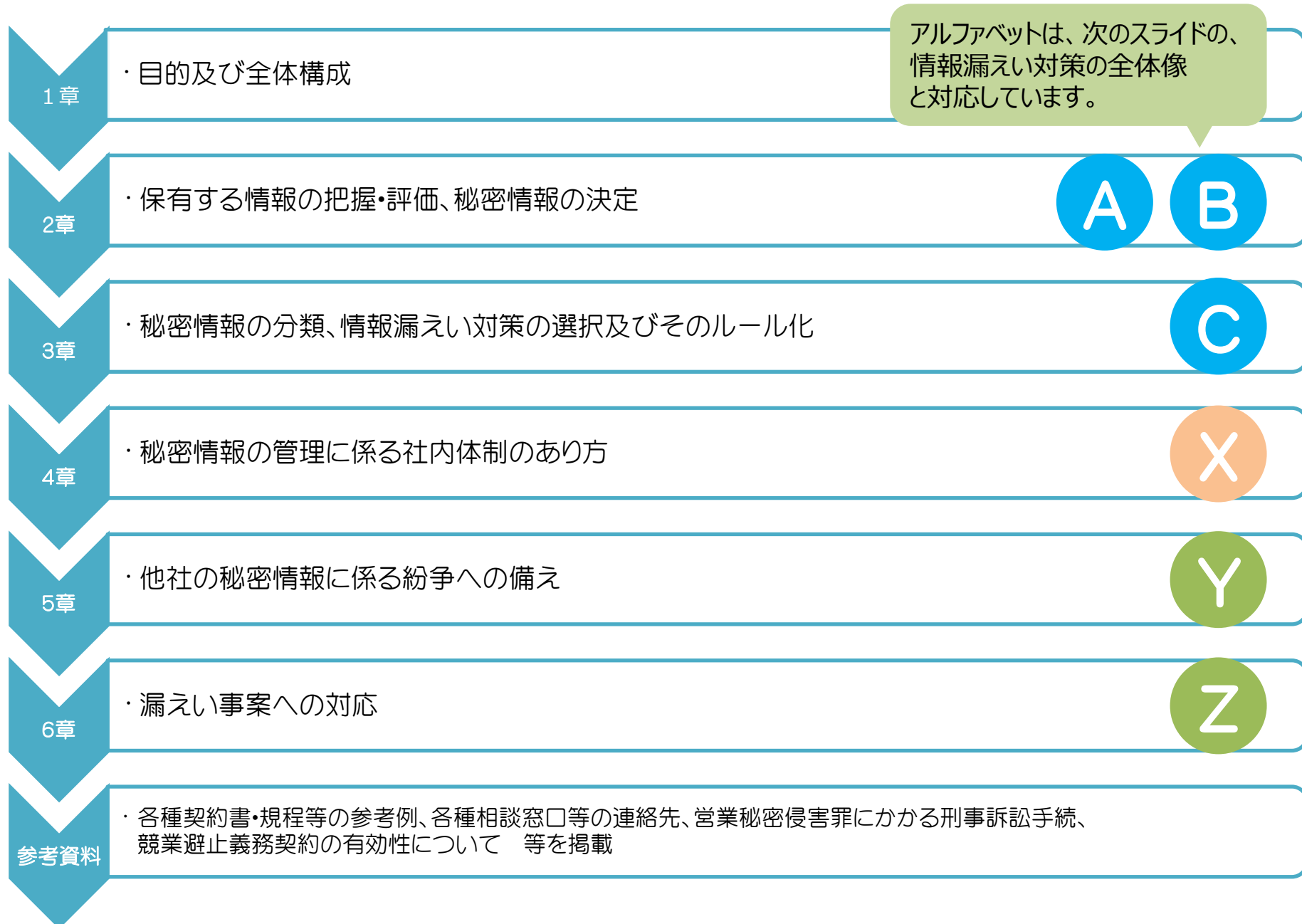
- 秘密情報の「管理」と「有効利用」のバランス
 - ☞ 企業にとって管理が必要な情報として、営業秘密の他、個人情報、機微技術情報、限定提供データなど、多様な情報が含まれることを想定して解説。
- 効率よく講じるための「5つの対策の目的」の設定
- 社内体制構築時の参考情報（各部門の役割分担例、部門横断的な管理体制等）



実際に漏えいしてしまった時の対応を紹介

- 他社からの訴えに対する備え
- 有事における対応

(参考) ハンドブックの全体構成



4. 「秘密情報の保護ハンドブック」情報漏えい対策 ～全体像～

A

まずは、自社にどのような情報があるのか一つひとつ洗い出し、社内の情報を把握しましょう。

B

洗い出した情報がどのくらい重要な情報なのかを見極め、秘密とする情報を決定しましょう。

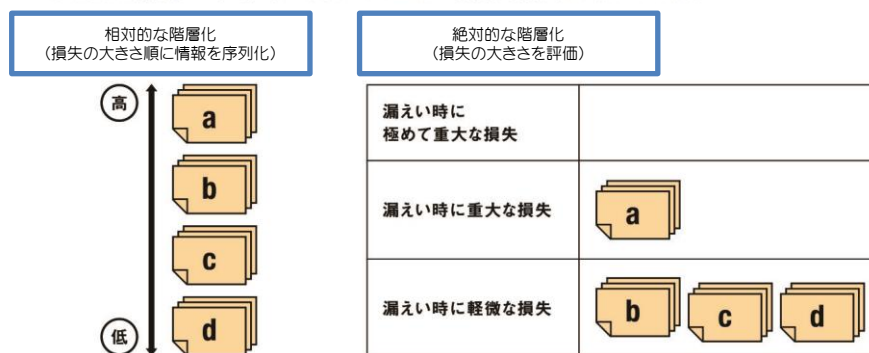
C

情報の重要度に応じて対策の選択・決定をし、管理と有効活用とのバランスを取りましょう。

例) 自社の強みとなる情報資産の例

技術情報	研究開発情報(実験データ、試作品情報等)、製造関連情報(製品図面、製品テストデータ、製造プロセス、工場設備・レイアウト) 
営業情報	顧客情報(顧客リスト、クレーム情報、顧客別製品等情報)、市場関連情報(市場分析情報、競合先分析情報)、価格情報(仕入れ値、製品価格、利益率等)、取引先情報、接客マニュアル 

相対的な階層化と絶対的な評価のイメージ～情報を損失で評価した場合～



企業の情報活用の例
～ある機械メーカーの機械製品に関する技術情報～

公開(標準・特許)	秘密(ノウハウ)
機械の動作性能評価方法 部品構造(他者が容易に把握可)	生産プロセス 素材配合

Y. 他社の情報も保護(訴えられないために)

Z. もしも情報漏えいが発生したら

X. 秘密情報の管理を実効的なものとするための社内体制の構築

5. 「秘密情報の保護ハンドブック」のポイント ①他社の情報も保護（訴えられないために）

- 紛争を未然に防止するとともに、意図せずに争いに巻き込まれてしまった場合への備えを紹介。
- こうした取組は、他社からの信頼向上、多様な人材の獲得にもつながる。

Y.

自社情報の独自性の立証

他社から秘密情報の侵害を理由に訴訟を提起された場合には、それが自社の独自情報であることを客観的に立証できるよう、日頃から備えておくことが重要。
（例：経緯書類の保存）

他社の秘密情報の侵害の防止

(1) 転職者の受入れ
（例：転職者の前職での契約関係確認）

(2) 共同・受託研究開発
（例：他社の秘密情報の分離保管）

(3) 取引の中での秘密情報の授受
（例：サンプル等の受領時の書面確認）

(4) 秘密情報の売込み
（例：情報の出所の誓約書での確認）

営業秘密侵害品に係る紛争の未然防止

疑わしい状況が生じている場合に相当の注意を払ったということが証明できる程度の対策が必要。

5. 「秘密情報の保護ハンドブック」のポイント ②もしも情報漏えいが発生したら

- 情報管理を徹底しても、情報漏えいを完全に防ぐことは困難。
- 万が一情報漏えいが発生した場合に迅速に対応できるよう、その手順を紹介。

2.

兆候の把握及びその確認

- (1) 漏えいにつながる兆候の把握
- (2) 漏えいの疑いの確認

初動対応

- (1) 社内調査・状況の正確な把握・原因究明
- (2) 被害の検証
- (3) 初動対応の観点
- (4) 対策チームの設置等

責任追及

- (1) 刑事的措置 (2) 民事的措置 (3) 社内処分

証拠の保全・収集



（参考）「営業秘密」の概要（営業秘密の3要件）

【不競法第2条第6項】この法律において「営業秘密」とは、秘密として管理されている生産方法、販売方法その他事業活動に有用な技術上又は営業上の情報であって、公然と知られていないものをいう。

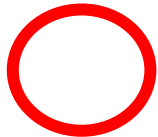
技術やノウハウ等の情報が「営業秘密」として不競法で保護されるためには、以下の3要件を**全て**満たすことが必要です。

【秘密管理性】秘密として管理されていること

営業秘密保有企業の秘密管理意思が、秘密管理措置によって従業員等に対して明確に示され、**当該秘密管理意思に対する従業員等の認識可能性が確保される必要**があります。

【有用性】有用な営業上又は技術上の情報であること

当該情報自体が客観的に事業活動に利用されていたり、利用されることによって、経費の節約、経営効率の改善等に役立つものであること。現実に利用されていなくてもかまいません。



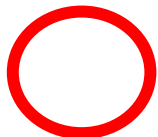
- ・設計図、製法、製造ノウハウ
- ・顧客名簿、仕入先リスト
- ・販売マニュアル



- ・有害物質の垂れ流し、脱税等の反社会的な活動についての情報は、法が保護すべき正当な事業活動ではないため、有用性があるとはいえない。

【非公知性】公然と知られていないこと

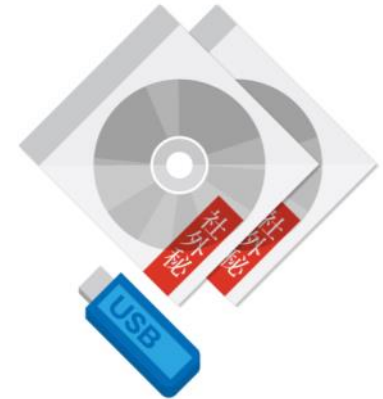
保有者の管理下以外では一般に入手できないこと。



- ・第三者が偶然同じ情報を開発して保有していた場合でも、当該第三者も当該情報を秘密として管理していれば、非公知といえる。



- ・刊行物等に記載された情報
- ・特許として公開



6. 「秘密情報の保護ハンドブック」情報漏えい対策 ～効率よく講じるための5つの「対策の目的」～

- 漏えい要因を考慮した5つの「対策の目的」を設定。
- 各社の状況に応じ、ルートごと、目的ごとにムリ・ムダ・ムラの無い形で対策を取捨選択。

物理的・技術的な防御

心理的な抑止

働きやすい環境の整備

接近の制御

持ち出し困難化

視認性の確保

秘密情報に対する認識向上

信頼関係の維持・向上等



秘密情報に近寄りにくく
するための対策



秘密情報の持ち出しを
困難にするための対策



漏えいが見つかりやすい
環境づくりのための対策



秘密情報だと思わなかった！
という事態を
招かないための対策



社員のやる気を高め、
秘密情報を持ち出そうという
考えを起こさせないための対策

- 対策の具体例
- アクセス権の設定
 - 秘密情報を保存したPCを不必要にネットに繋がらない
 - 構内ルートの制限
 - 施錠管理
 - フォルダ分離
 - ペーパーレス化
 - ファイアーウォールの導入 等

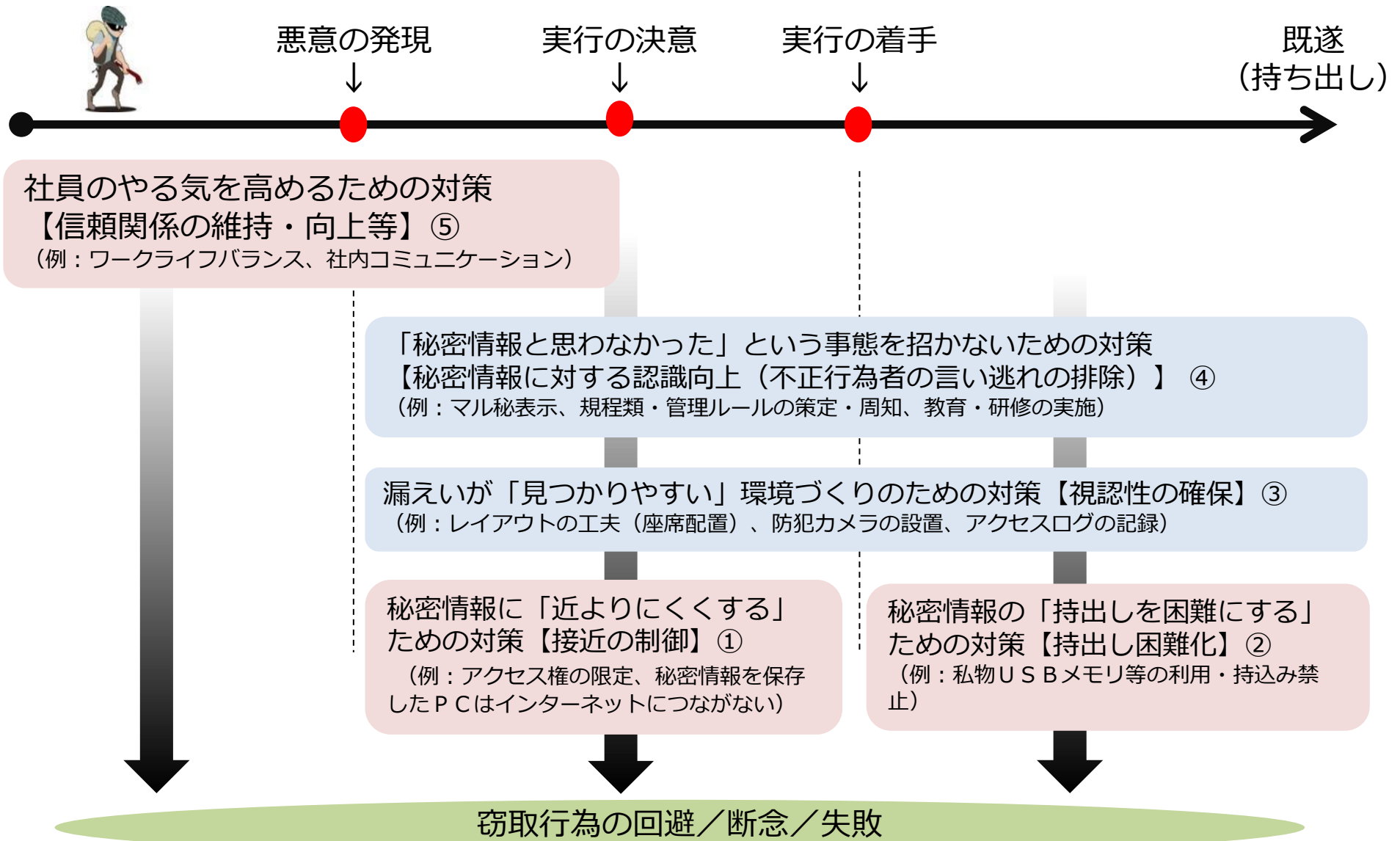
- 私用USBメモリの利用・持込み禁止
- 会議資料等の回収
- 電子データの暗号化
- 外部へのアップロード制限 等

- 座席配置・レイアウトの工夫
- 防犯カメラの設置
- 職場の整理整頓
- 関係者以外立入禁止看板（窓口明確化）
- PCログの記録
- 作業の記録（録画等） 等

- マル秘表示
- ルールの策定・周知
- 秘密保持契約の締結
- 無断持出禁止の張り紙
- 研修の実施 等

- ワーク・ライフ・バランスの推進
- コミュニケーションの促進
- 社内表彰
- 漏えい事例の周知 等

(参考) 秘密情報の漏えい対策の5つの目的～犯行の段階に応じた対策の選択～



【対策の取捨選択の考え方】

- ・アクセス可能な者が多数に設定されている場合には、「視認性の確保」や「持出し困難化」が対策の中心。
- ・従業員の多様化の程度が大きいほど、「信頼関係の維持・向上等」の対策の困難度が増す。 など

7. 「秘密情報の保護ハンドブック」の改訂について【令和6年2月】

- 直近改訂（令和4年5月）以降の社会経済情勢の変化・関係法令の進展等を踏まえて改訂を検討。
- 一方、啓発資料として産業界・関係団体に行き渡っていることから、構成・基本的内容については、現行版を踏襲しつつ、以下の観点を踏まえて、ハンドブックの内容を補強・追記する方針で改訂を進める。

□ 関連する「法制度の見直し・ガイドラインの改訂」に伴う修正

- 直近改訂以降の進展、例えば、「法制度の見直し」に伴う修正として、令和5年の不競法改正で見直された①「限定提供データ」の保護範囲、②使用等の推定規定の拡充、③国際的な営業秘密侵害に係る手続等に関する記載を追加するほか、この間に発出された「各種ガイドライン」（例：「水産分野における優良系統の保護等に関するガイドライン」・「養殖業における営業秘密の保護ガイドライン」（水産庁））等を反映。

□ 営業秘密・秘密情報を取りまく「環境の変化」に伴う修正

- A I の利活用が進展などの環境変化に合わせて、意図しない情報漏えいインシデントを防ぐ上での留意点・流出リスクについて記載の見直しを図る。
- 海外への重要な技術情報の流出への懸念が高まっている中、外国から日本企業が保有する秘密情報が狙われるリスクについて、過去の漏えい事件を踏まえ、啓発コラムの見直しを図る。

□ 巻末の「参考資料」の修正

- 関連情報・参考情報として巻末に添付されている「参考資料」について、直近の情報に対応して所要の修正・更新。

等

8. 実際にあった?! 事例と対策とそのポイント

ケース1. 部品メーカーA社の例 【取引先向けの対策】 取引先から金型図面の提供を求められたが...

- A社が、精密機械メーカーB社に供給する部品aは、A社が独自に開発したもので、精巧な部品であると評判。
- ある日、B社から部品aの金型の図面を求められ、大口の取引先だからと泣く泣く提供した。
- その後、B社から部品aの発注が来なくなってしまった。どうやらB社がA社の部品aの金型図面を、A社の競合他社であるC社に渡し、安価で部品aをコピーした部品を製造させているようだ。
A社はどのような対策を講じておくべきだったのだろうか。

A社の秘密情報 : 部品aの金型図面



ケース 1. 部品メーカーA社の例【解説】

ポイント1 開示する情報は必要最低限にしましょう。

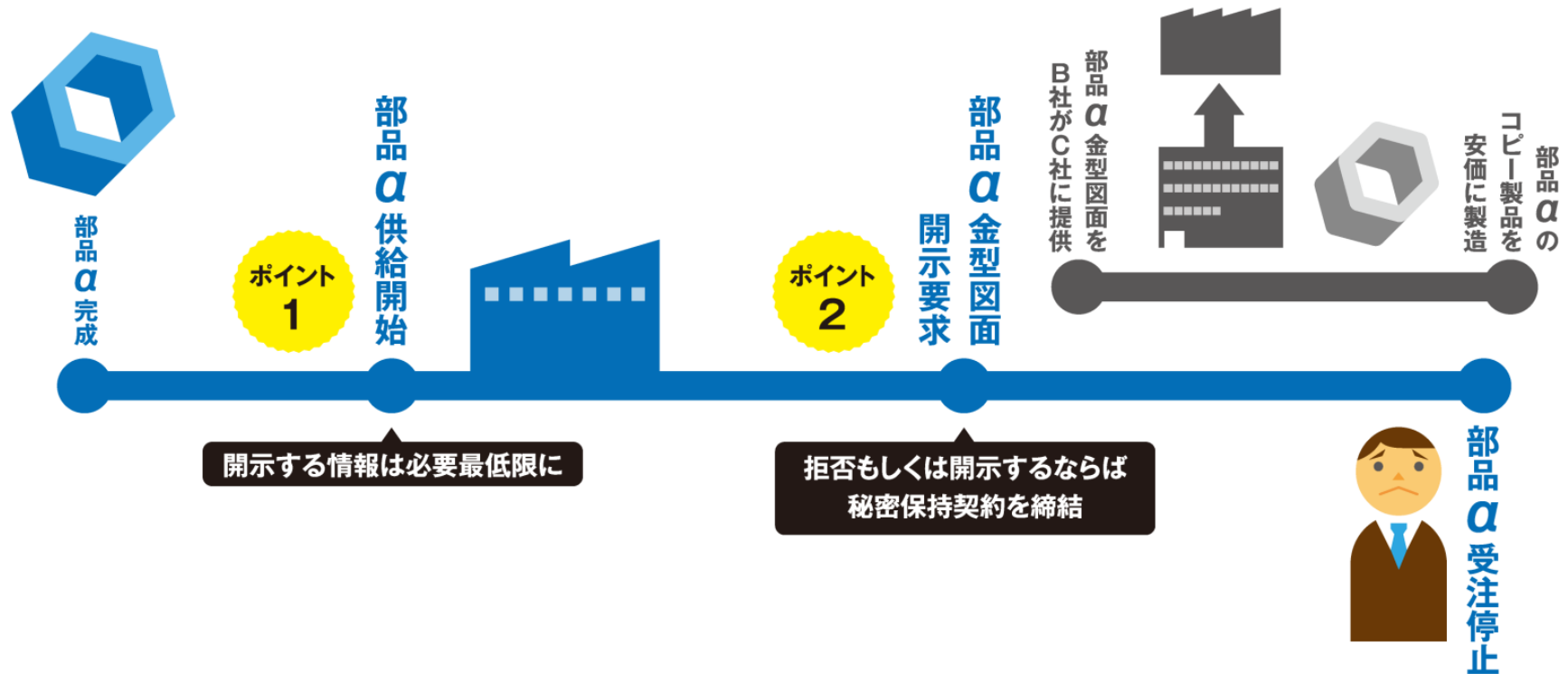
（接近の制御）【ハンドブック第3章3－4（3）①a】

- B社との取引で、金型図面の情報を開示する必要がなければ、開示を拒否することも大切です。
- 事前に、見積書や取引契約書に金型図面の開示はできない旨を書いておくことも効果的です。

ポイント2 開示する場合は、秘密保持契約を締結しておきましょう。

（秘密情報の認識向上）（持出し困難化）【ハンドブック第3章3－4（3）④a、②a】

- 金型図面に関する秘密保持契約には、秘密保持、目的外使用の禁止、契約終了時の金型図面の返還・消去義務等を定めておくといよいでしょう。



8. 実際にあった？！事例と対策とそのポイント

ケース2. 食品メーカーD社の例 【従業員・退職者向けの対策】従業員から退職の申出があったのだが・・・

- 即席めんを製造しているD社では、スープの配合レシピの情報が競争力の源泉である。
- 最近、ニュースで、「ある企業の退職者が転職先で営業秘密を不正使用して逮捕された」との報道を見たが、他人事ではない。最近、D社でも、スープ開発リーダーから、退職したいとの申出があった。転職先は競合他社のE社だという。大事な配合レシピを持ち出されないようにするためには、どのような対策を講じたら良いか。

D社の秘密情報 : スープの配合レシピ



ケース2. 食品メーカーD社の例【解説】

退職に伴う漏えいリスクを低減する対策を講じましょう。

ポイント1

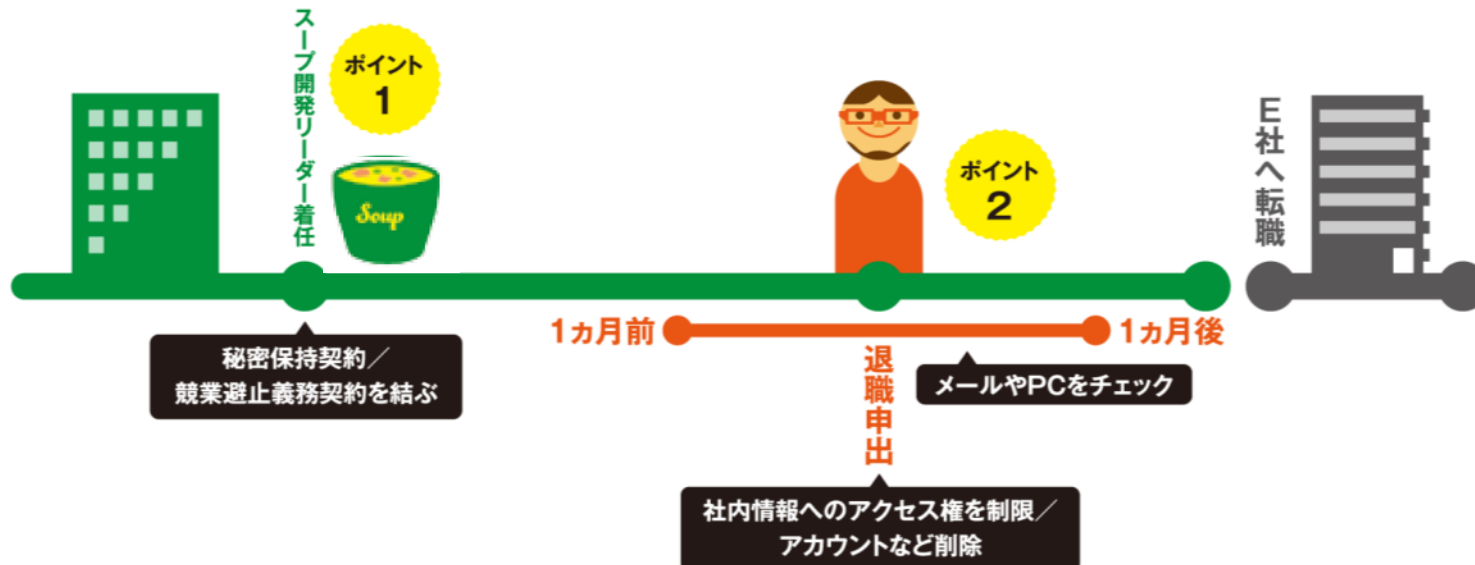
- 退職時だけでなく、入社時はもちろん、プロジェクト開始時にも秘密保持契約を締結。キーパーソンの場合は、競業避止義務契約を締結することも考えられます。（秘密情報に対する認識向上）【ハンドブック第3章3-4（2）④a、b】

ポイント2

- 退職の申出があったら、速やかに社内情報へのアクセス権を制限。退職時にはすぐにI D・アカウントを削除（I Dカード、入館証も回収）（接近の制御）【ハンドブック第3章3-4（2）①a】
- 退職申出前後のメールやP Cのログを集中的にチェック（視認性の確保）【ハンドブック第3章3-4（2）③q、r】
- 退職後もO B会の開催などで本人の近況を調査したり、転職先の商品情報をチェック

ポイント3

- 働きやすい職場環境や公平な人事評価制度を整備し、従業員の企業への愛着を高めておけば、貴重な人材を失わずに済み、漏えいリスクも低減します。（信頼性の維持・向上等）【第3章3-4（1）⑤】



8. 実際にあった？！事例と対策とそのポイント

ケース3. フィルムメーカーJ社の例 【従業員向けの対策】 製造ラインを新設したいのだが・・・

- J社は近々、耐熱性フィルムの製造ラインを新設する予定になっている。
- その新製造ラインでは、設備の改良や配置の工夫によって、他社に比べて高効率なフィルム製造システムが実現できる。そのため、製造ラインや工場のレイアウトといった情報が他社に漏れないようにしなければならない。対策として、どういったことができるだろうか。

J社の秘密情報 : 耐熱性フィルムの製造工程や工場レイアウト



ケース3. フィルムメーカーJ社の例【解説】

秘密情報の全体を把握できる人数を制限しましょう。

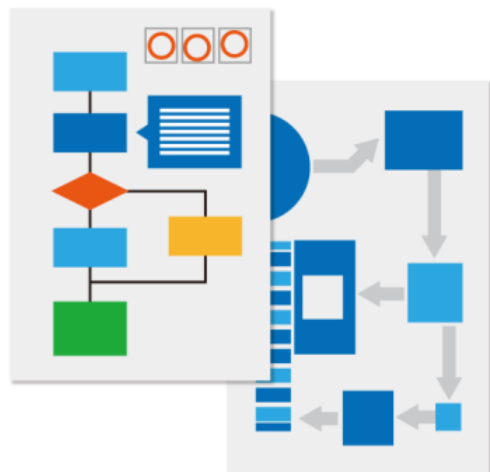
（接近の制御）【ハンドブック第3章3－4（1）①a】

- 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します。

情報に接する従業員が情報を持ち出しにくい対策を講じましょう。

（持出し困難化）【ハンドブック第3章3－4（1）②j】

- 工場内へのカメラ等の撮影機器の持込みを制限します。（ポケットのない作業着の着用の義務づけや、私物持込みは透明バッグに入れて入室するなどの工夫をすると効果的。）



8. 実際にあった？！事例と対策とそのポイント

ケース4. 繊維メーカーK社の例 【外部者向けの対策】 不審なメールが届いたが・・・

- K社は素材を仕入れて高機能繊維を製造し、顧客に販売する企業である。
- ある日、製造部門の従業員Lあてに、顧客を装ったメールが届いた。従業員Lがメールの内容に違和感を覚え、添付ファイルを開かずに社内セキュリティ部門に相談したところ、ウィルスが仕込まれた攻撃型メールであることがわかった。
- 今回は運良く従業員が不審に感じてファイルを開かなかったが、今後、このような攻撃を受けて誤って添付ファイルを開けば、K社の顧客情報や製造ノウハウといった情報のみならず、調達先から開示されている情報まで外部へ漏えいしてしまう恐れがある。
- 不正アクセスや、攻撃型メールの被害にあわないためにはどのような対策をしておけばよいか。

K社の秘密情報： K社情報（高機能繊維製造ノウハウ、顧客情報など）

調達先から開示された素材情報



ケース４． 繊維メーカーK社の例【解説】

ポイント１ できる限り外部への接続を切断しましょう。

（接近の制御）【第３章３－４（４）①e】

- 可能な限り外部ネットワークにつながらない機器に秘密情報を保存しましょう。

ポイント２ 不正アクセスや攻撃型メールの被害を最小限する対策を講じましょう。

（接近の制御）【第３章３－４（４）①f】

- 外部ネットワークにつながったＰＣ等に秘密情報を保管する場合は、ファイアーウォール、アンチウィルスソフトを導入し、ソフトウェアのアップデートをしっかりと行うことが大切です。

（持出し困難化）【第３章３－４（４）②c】

- 秘密情報の電子データを暗号化することも効果的です。

※標的型メールの見分けるためのポイント等については、
ハンドブック１１２頁の「コラム④ 標的型攻撃メールって
どんなもの？」に掲載しています。



8. 実際にあった？！事例と対策とそのポイント

ケース5. 食品メーカーF社の例 【トラブルに巻き込まれないための対策】自社技術で作ったのに・・・

- 野菜のフリーズドライにより具だくさんの味噌汁を製造するF社では、日本の果物を使ったドライフルーツを新商品として開発中。
- ある日、商談会で名刺を交換した食品加工機器メーカーG社から、G社の保有するフリーズドライ技術を使った共同開発の提案を受けた。しかしコスト面で折り合わず、G社の申出は断ることに。
- その後F社は、自社技術を転用して新たなドライフルーツ商品βを開発し、販売を開始。すると突然、新商品βがG社の技術を用いて製造されたものであり、その製造・販売中止を求める警告状が送られてきた。
- しかしF社は、共同開発の打診を受けた際には、具体的なG社技術の開示は受けておらず、G社の秘密情報など使った覚えは一切ない。F社が、商品βは独自技術で開発したという潔白を示すには、どうしたらいいのだろうか。

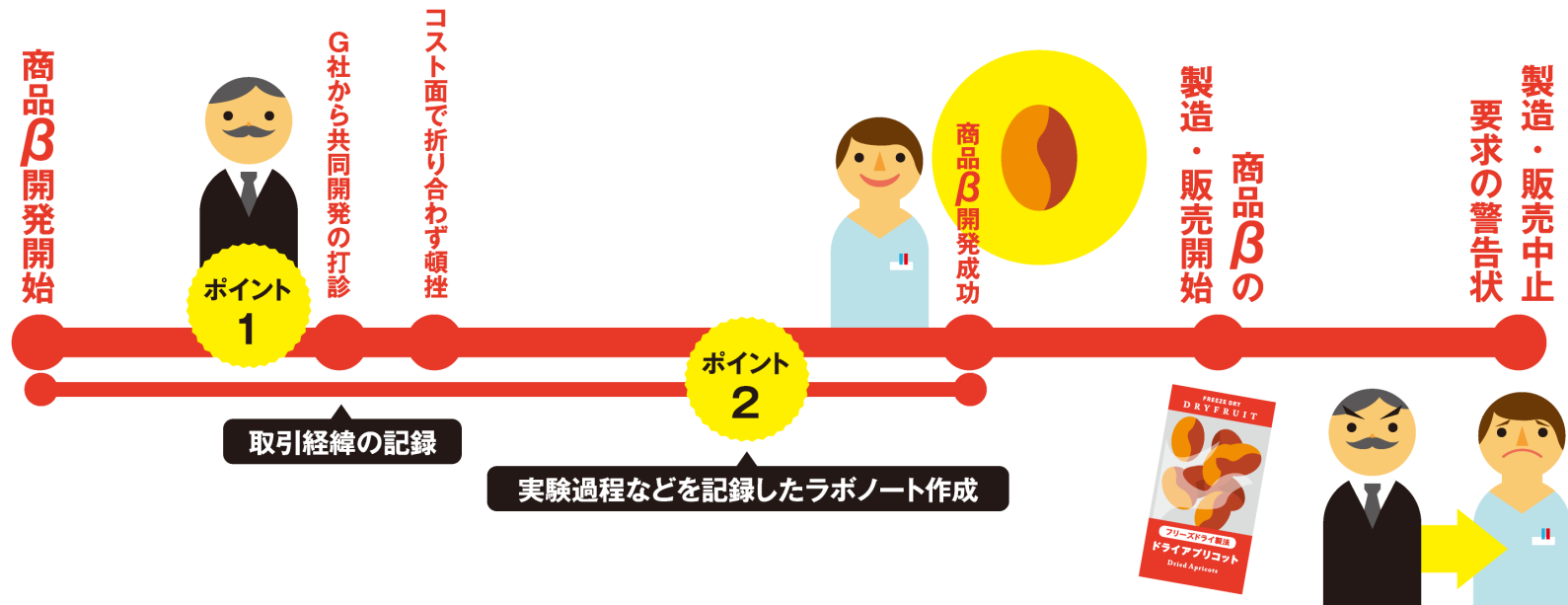


ケース5. 食品メーカーF社の例【解説】

ポイント1 他社の秘密情報は、できる限り受け取らないようにしましょう。

ポイント2 独自技術を証明できるように開発の内容や日時等を記録しておきましょう。【第5章5－1】

- 技術情報であれば、技術が生まれるまでの実験過程等を記録したラボノートの作成・保存
 - 日付確定のための公正証書（公証人が作成する公文書）等の利用
 - その他関連資料の保管（電子メール、検討文書、議事録等）
- 顧客名簿であれば、顧客になるに至った経緯の記録（来店・購入の履歴、会員登録時のWeb、申込書等）
 - 取引情報であれば、その取引経緯の記録（仕入や販売の際の価格や数量等が記載された伝票の原本等）



8. 実際にあった？！事例と対策とそのポイント

ケース6. 容器メーカーH社の例 【転職者向けの対策】転職者を受け入れて新製品を開発したら・・・

- H社は、軽量で強度の高い樹脂製の食品保存容器の開発に力を入れたいと考え、競合他社I社で容器開発経験のあるM氏を迎えた。
- M氏を開発部のリーダーとして開発を進めたところ、これまでになく軽量で強度の高い容器γの開発に成功し、販売を開始した。
- しかし、γを販売してから数か月後に、M氏の転職元であるI社から、「γはI社の秘密情報を不正使用して製造されたものであるため、販売を差し止めてほしい」との通知を受けた。これを受けてH社がM氏に確認したところ、I社の技術の一部を用いてγを開発したことを認めた。
- H社としては、M氏の採用にあたり、どのような対応をすべきだったのだろうか。



自社ノウハウは財産。他社の情報の管理も徹底し取引先からの信頼も向上

概要

高精度設備とIT化による最先端プレス技術で、金属の難加工形状品や微細加工品を提供。20年以上前に、取引先に、金型を作るノウハウである「工程サンプル」の提示を求められ、泣く泣く渡したところ、取引が打ち切られた経験（取引先はアジアの金型メーカーに情報を渡し、安く作らせたと推測）を踏まえ、**自社・他社の情報の管理の徹底を図り、取引先に対しても、その方針を示した。**こうした取組により、**取引先から信頼され、事業にも好影響が出ている。**

具体策

○「接近の制御」に資する対策【 C. ① 】

- － **工場の入口は内部からのみ解錠可能な扉**
- － **取引先の部品・金型**も、第三者に特別に入室を許可する場合、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（他社の情報もしっかり管理）**
- － 図面等の重要データは**インターネットに繋がっていないPCで管理**
- － 「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**」と取引先との**契約書に明記**

○「視認性の確保」に資する対策【 C. ③ 】

- － 金型やプレス機のある現場には**「立入禁止」、**
「撮影禁止」等の掲示

・自社と同レベルで取引先の情報管理を行うことで取引先からの信頼が向上

・業績にも好影響



従業員以外
立入禁止

ノウハウの見える化・ビッグデータの集積で知識集約型企业へ

概要

修理前よりも能率が向上すると評判の企業。社長自らが経営理念として「**知識集約型**」を掲げる。各工場を訪問し散在する**プレス機械のカatalog・図面データ**を、点検時に**経年劣化した機械の現状データ**を、**修理時に作業データを収集・蓄積**。このデータを活用し、**唯一無二のサービスを実現**。また、**社員の現場での工夫を作業マニュアル化**し、社内で共有。その際、**工夫を発案した社員の名前を明記・登録**し、「**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、やる気も向上**。

具体策

○保有する情報の洗い出し【 A 】

- ー市場製品の**Catalog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**

○信頼関係の維持・向上等【 C. ⑤ 】

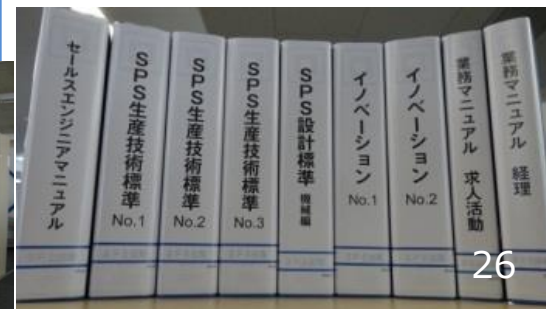
- ー**経営者自ら**が「**社員の知恵が我が社の財産**」と内外に発信
- ー作業ノウハウを文章化する際、アイデアを提案した**社員名を明記・登録**

・従業員のやる気、
当事者意識向上

・同業他社への転職
者無し

・顧客満足、信頼向上

・メンテサービスの
海外展開を実現



厳格な情報管理と作業の見える化で顧客の信頼向上、高付加価値サービスを実現

概要

蓄積した製品・作業のデータを活用し、通常では繊維を傷めるため水洗浄ができず水溶性の汚れを落とせない衣類の水洗浄を可能とする技術（特許技術とノウハウで管理）を生み出した。この技術と、データベースによる徹底した顧客管理・接客で、顧客ニーズに対応した世界唯一のケアメンテというクリーニングとは異なるサービスを実現。

具体策

- 保有する情報の洗い出し【 A 】
 - －取り扱った衣類の素材、ブランド、洗浄方法を全てデータ化
- 「接近の制御」に資する対策【 C. ① 】
 - －従業員ごとにアクセスできるデータを管理・制限
 - －従業員ごとに毎日更新されるパスワードを付与
 - －作業で使用する溶剤の性質等は従業員にも非開示
- 「持出し困難化」に資する対策【 C. ② 】
 - －作業場への携帯電話の持込み禁止
- 「視認性の確保」に資する対策【 C. ③ 】
 - －全ての作業工程をカメラで撮影・録画
- 信頼関係の維持・向上等【 C. ⑤ 】
 - －作業スキルを見える化。技能認定 & 昇給でやる気向上

- ・顧客の信頼向上
- ・高価格でも、満足度の高いサービスを提供
- ・従業員のやる気向上
- ・作業の録画を、クレーム対応(従業員保護)、従業員自身でのスキルチェックに活用



厳格な情報管理によりグローバルな生産体制を実現し、世界シェアトップ

概要

1993年に、明るさや残光時間において従来の蓄光顔料の約10倍の輝度を有しながら、放射性物質を全く含まない蓄光顔料（製品名：「ルミノーバ」）を世界に先駆けて開発し、各国で物質特許を取得。以来、同製品は、夜光時計の針や文字盤、避難誘導標識、安全標識など幅広く活用されている。社長自らが知財の重要性を謳い、社長の直下の法務・知財室が中心となり知財戦略を立案。ルミノーバは特許期間の満了を迎えたが、商標の登録、技術ノウハウの秘匿化などに戦略的に取り組み、高い競争力を維持。コア技術である製法や原材料情報は秘密情報として管理。海外の生産工場には調合済の原料を供給し、製法・原材料情報は社内であってもブラックボックスにして明らかにしないなど、生産現場での徹底した情報管理により、グローバルな生産体制を実現し、世界シェアトップを実現。

具体策

○「接近の制御」に資する対策【 C. ① 】

- － 海外の生産工場には調合済の原料を供給し、**製法や原材料情報は社内であっても開示しない**
- － 取引先・共同研究開発相手にも製法や原材料情報は開示しない
- － 社内で秘密情報を取り扱う**エリア・取扱い者を限定**
- － 電子データについては、社内においてもアクセス制限

○「視認性の確保」に資する対策【 C. ③ 】

- － 秘密情報が含まれる電子情報は**タイムスタンプで管理**し、不正なアクセスや複製を検知

○「信頼関係の維持向上等」に資する対策【 C. ⑤ 】

- － **ノウハウの発案に対しても特許取得と同様に社内報奨**

- ・グローバルで効率的な生産体制を実現
- ・世界シェアトップを実現
- ・従業員のやる気向上



チームでの話し合いにより発想力と意識を高め、他社情報も徹底的に管理

概要

従業員の自由な発想力と、チーム力を育む職場環境とで、自動車メーカー等の様々なニーズに的確に対応した高品質の部品設計を生み出す。部品設計のために顧客から提示される設計仕様、新車開発スケジュール等の秘密情報を、社内で厳格に管理。各部署のメンバーで構成される「機密管理実行委員会」の下、漏えい対策を統一的に進める。加えて、全社朝礼において従業員自らが経験したヒヤリハット事例を共有したり、従業員同士が定期的にアイデアを出し合って漏えい対策を提案・検討する仕組みを設けたりするなど、従業員の発想力とチーム力を活用し、きめ細かい情報管理体制を構築するとともに、意識の向上を実現している。こうした取組により、顧客からの信頼を獲得している。

具体策

○「接近の制御」に資する対策【 C. ① 】

- －設計に関する情報は、**限定されたプロジェクトメンバーのみがアクセス**
- －秘密情報が記録された書類は従業員が立ち会い、専門業者が焼却処分
- －顧客との電子データのやりとりは、**専用回線**を使用

○「持出困難化」に資する対策【 C. ② 】

- －社内での**カメラ付き携帯の持込みを禁止**
- －電子メールは、**秘密情報の送信時は暗号化**。全ての電子メールの文中に**情報取扱いに関するチェック項目を記載し、送信時に確認**

○「視認性の確保」に資する対策【 C. ③ 】

- －秘密情報を取り扱うエリアの出入口に**監視カメラを設け**入退管理

○「秘密情報に対する認識向上」に資する対策【 C. ④ 】

- －全社朝礼で、毎日、**情報管理対策の6項目を唱和**
- －従業員が自らの**ヒヤリハットの実経験を紹介・共有**。従業員同士がチームに分かれ**情報漏えい対策のアイデアコンテスト**を実施するなど、**従業員の意識を高めている**

・顧客の情報を徹底的に管理し、取引先の信頼を獲得



機密唱和（6項目）

- ・メール本文下にチェックシートを添付します。
- ・「添付資料有無」「暗号化しパスワード設定有無」「車名併記無」「転送・引用文有無」
- ・新規受入れ者の指導を必ず行います。
- ・違反が発覚したら即時に上司に報告します。
- ・カメラ付き携帯電話は持ち込みません。
- ・機密書類は持ち出しません。
- ・お客様の入退室記入を必ず行います。

技術情報の管理手法を使い分け、高付加価値の食品を開発

概要

北海道産の農産物だけを用いて、健康改善作用と美味しさを兼ね備えた食品（“コンディショニング食品”）として北海道食品機能性表示制度に基づく認定を受ける商品や、中小企業庁長官奨励賞（平成26年度）を受賞した商品等を開発・製造する。

戦略的に管理手法を使い分けることにより、協力・連携の拡大と、独自技術の保護・他社との差別化を実現。例えば玉ねぎの加工に関して、加熱処理方法と加工生成物質については、特許を取得している。加工委託先への生産工程の条件設定等については、営業秘密（技術ノウハウ）として秘密保持契約を結び情報を提供。また、設定条件の生成方法は社内でも限定した社員のみしか知らない。

一方で、ヤーコン（北海道産の根菜）については、地域活性化や生産者の収益増に向け、認知度の向上や食材の用途拡大を図るべく、自社の技術を無償公開。

具体策

○秘密とする情報の決定【 B 】

- － **技術の重要性・性質等に応じ**、①特許出願、②社内でもアクセス権を制限、③秘密保持契約を締結した上で他社に提供等の**管理手法を決定**

○接近の制御【 C. ① 】

- － **ノウハウの重要な部分**は社内でもアクセス限定（電子情報を**外づけハードディスクだけに保存し**、当該ディスクは**限定された社員しか知らない場所に保管**）

- ・管理手法の使い分けにより、協力・関係の拡大、独自技術保護・他社との差別化を実現
- ・技術の無償提供で、地元の経済活性化、農業生産者の収益増を目指す



知財を活用したブランディングにより資源循環型社会の構築に貢献

概要

“地球が喜ぶテクノロジー”という企業理念の下、炭づくりの匠の技を参考に、もみ殻、食品加工残渣といった廃材から高品質な炭を連続的に生み出す技術を開発。炭化処理の方法や炭化機基本構造については特許を取得する一方、装置自体は処理する廃材の種類や装置の設置現場の状況に応じた個別の設計が必要となることから、炭化機内の構造や配管を含む最適設計技術はノウハウとして秘密管理。
 また、炭化機から生み出される炭（油吸着材、調湿材など）自体でも、特許権と商標権を取得し、炭化機ユーザーに対し「SUMIX」の商標と品質評価結果の結果などをライセンス提供することにより、互いにWin-Winの関係での炭の品質確保とブランド構築がなされ、高品質な炭の市場を開拓。

具体策

○「接近の制御」に資する対策【 C. ① 】

- － 最適設計のノウハウは社長のみが管理
- － 秘密情報が記載された紙媒体は施錠管理
- － 秘密情報は、メールでのやりとりを禁止

○「秘密情報に対する認識向上」に資する対策【 C. ③ 】

- － 秘密情報にはマル秘マークを表示
- － 入社時と退職時に秘密保持を契約
- － 装置の納入先や製造委託先とも秘密保持を契約



・コア技術の秘匿化により技術的優位性確保

・知財を活用しユーザーと共に高品質市場を構築

・知財を活用したブランディングにより資源循環型社会の構築に貢献



オープン・クローズ戦略の実践により、長期にわたり製品の競争力を確保

概要

配線用遮断器などのいわゆる“ブレーカー”を開発・製造するメーカーで、地元ではブレーカーが社名の「テンパール」の通称で呼ばれるほど親しまれている会社。1951年の創業当時から「会社の宝は技能と技術」とうたい、製品技術の特許を多数取得し、技術を知財で守ることをいち早く実践。1965年には、その当時10個の特許権を保有、特許は真珠のように大切なものとの思いから、10（テン）の真珠（パール）として、社名を変更した。

現在では、インフラを支える機器であり同型の製品が長く販売されるという特性にあわせて、リバース・エンジニアリングによって判明する技術は特許化する一方で、分からない技術については、ノウハウとして秘密管理を行いグループ企業であっても情報共有も最低限とするなど、オープン・クローズ戦略を実践し、技術流出に細心の注意を払っている。

具体策

○「秘密とする情報の決定」に資する対策【 B 】

- －製品寿命が長いため、代々の担当者間の情報の継承が確実に行えるよう、**製品ごとに関連情報を一元化して保管**

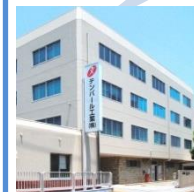
○「接近の制御」に資する対策【 C. ① 】

- －**開発**データは厳格な**アクセス制限（開発部へ立入禁止）**

○「秘密情報に対する認識向上」に資する対策【 C. ④ 】

- －グループ企業への情報共有であっても、**製造に必要な最低限の情報のみを提供**。開示した情報については**取引基本契約のなかで秘密保持を規定**

・特許と営業秘密とを組み合わせることにより、長期にわたる競争力の維持を実現



顧客から信頼される情報管理体制を構築し売上げを伸ばす

概要

経営層も含め社員全員が、情報管理の重要性や情報漏えいの損害を十分に認識し、リスクを徹底的に排除しながら、顧客の信頼を獲得し、成長を遂げてきたモバイルコンテンツの開発・配信会社。2008年に情報セキュリティマネジメントシステム国際標準規格（ISMS）の認証を取得し、顧客から要求されるセキュリティレベルへの迅速な対応が可能に。

また、社内の情報管理ルールを分かりやすくまとめた簡易マニュアルを作成。その中で、報道された他社の漏えい事案を示し、最悪のケースでは、経営陣の引責辞任、数百億円規模の損害賠償、顧客喪失などにつながることを紹介し、それを研修や社内テストにおいても確認し、社員全員が情報管理の認識を高めている。また、横断的な情報セキュリティ確保の体制や社外による監査体制などが構築されていることも、信頼を高め顧客の獲得につながっている。

具体策

- 継続的かつ適切に実施するための社内体制の構築【 X 】
 - －横断的な部署が参加する「情報セキュリティ委員会」の設置
 - －外部コンサルが参画する「監査委員会」の設置
 - －情報管理ルールの「簡易マニュアル」の作成
- 「秘密情報に対する認識向上」に資する対策【 C. ④ 】
 - －進行段階に応じ事業範囲に応じた情報の取扱いを規定
 - －情報管理の理解を確認するチェックテストや社内チームディスカッションを実施
 - －業務開始・終了時に自社・共同開発先の従業員との秘密保持を契約
 - －退職時に競業避止義務を契約



株式会社メディア・マジック
ISMSマニュアル 簡易版



- ISMS認証の取得により顧客からのセキュリティ要求にも迅速に対応し、売上げ1.5倍増

【設問】 会社で管理している個人情報外部へ流出してしまった場合、どのような問題が発生すると考えられるでしょうか。想定されるリスクを具体的に3つ以上記載してください。

【回答例】

- ・クライアントや社会的な信用の失墜
- ・取引停止、売上減少
- ・多額の損害賠償費用の発生
- ・会社の倒産 など

生産性向上のためのデジタル化により、サービスの質の向上・情報管理の強化を実現

概要

小型貫流ボイラに搭載したセンサで、顧客のボイラの運転状況をリアルタイムでモニタリングを行うことで、単に製品の販売を行うだけではなく、故障の予兆を検知し工場の稼働を停止することなく修理を行ったり、複数台のボイラの最適な運転管理による燃料消費の削減の提案などの顧客のニーズに応える付加価値の高いサービスも併せて提供することで、小型ボイラーの国内シェア6割以上を獲得。

また、自社のボイラの納入・稼働の台数が拡大しつつも、サービスの質を維持・向上させるため、顧客へのメンテナンスサービスや省エネの提案に必要な情報の最新版が客先からでも常に見られるように、客先からでも直接専門の技術社員と相談するために全社員の所属・連絡先の検索を可能とするように、情報・ノウハウの見える化・デジタル化を進めるとともに、タブレット等の情報端末を全サービススタッフに装備させた。こうした取組みにより、営業力の強化、一人あたりの生産性の大幅向上を実現している。

具体策

○「接近の制御」に資する対策【 C. ① 】

- ー 業種や役職に応じたアクセス権を設定。顧客情報は担当エリア内では共有しつつ、エリア外の情報についてはアクセス制限
- ー 情報へのアクセスは、ログをとり、その旨を社員へ周知

○「持ち出し困難化」に資する対策【 C. ② 】

- ー 会議資料は全て情報端末で閲覧、印刷不可。情報端末の紛失対策とし、一定時間が経過すると自動的にアクセスを遮断

○「秘密情報の認識向上」に資する対策【 C. ④ 】

- ー 社員が発案・作成した法令ハンドブック「法令の“ほ”」を頒布

○「社員のやる気向上」に資する対策【 C. ⑤ 】

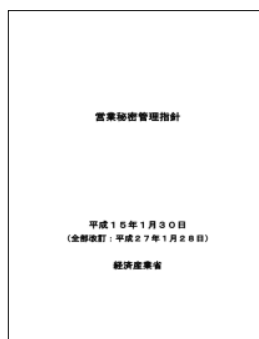
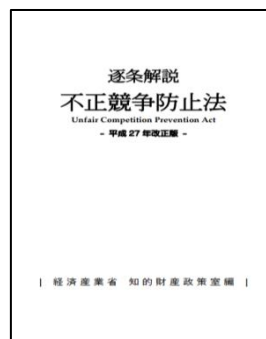
- ー 年2回、全国のメンテナンススタッフを愛媛県の本社で研修。
スキル向上により、生産性向上 & 給与UPを図っている

- 顧客のニーズに応え、現場の生産性の向上を図るために、情報のデジタル化を進めた結果、サービスの質の向上・情報管理の強化が実現され、業界シェア6割を獲得



最後までお読みいただきありがとうございました。

経済産業省HPでは、
「逐条解説」、「営業秘密管理指針」、「秘密情報の保護ハンドブック」、など、
不正競争防止法に関するさまざまな資料を掲載しております。



不正競争防止法 知的財産政策室

検索

<http://www.meti.go.jp/policy/economy/chizai/chiteki/>



不正競争防止法の解釈等に関するご質問はこちらまで

経済産業省 経済産業政策局 知的財産政策室

〒100-8901 東京都千代田区霞が関1丁目3番1号

TEL: 03-3501-1511 (内線2631)

E-mail: bz1-chitekizaisan@meti.go.jp

https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/170607_hbtebiki.pdf