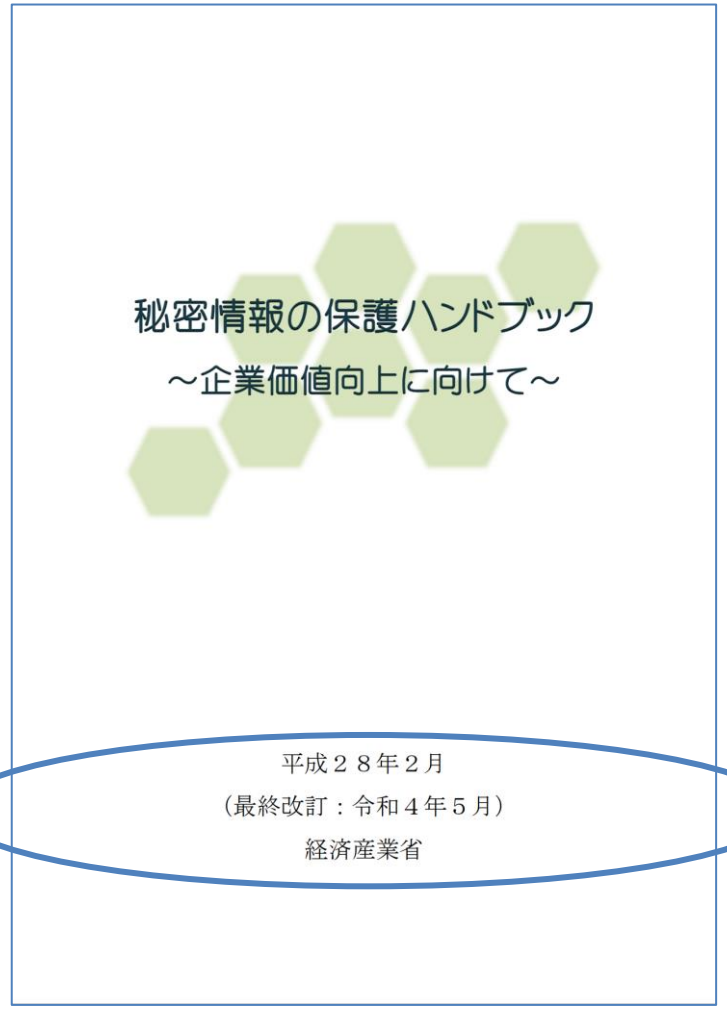
「秘密情報の保護ハンドブック」改訂の背景・狙い・重要ポイントと改訂内容の解説

２０２２年　９月　９日

営業秘密保護推進研究会　事務局長
株式会社NTTデータ経営研究所　三笠　武則

APPTraS

秘密情報の保護ハンドブック（以後、「ハンドブック」という。）の最新版は、産業構造審議会 知的財産分科会 不正競争防止小委員会のWebサイトで公開されています。



https://www.meti.go.jp/shingikai/sankoshin/chiteki_zaisan/fusei_kyoso/20220517_report.html

目次

1. ハンドブックの狙い、初版公開時期、営業秘密管理指針との関係
2. ハンドブックの概要
3. 改訂の背景とポイント
4. 外国から日本企業が保有する秘密情報が狙われる典型的なパターン
5. ハンドブック改訂に係る詳しい解説
    a. 法制度の見直し、ガイドラインの改訂に伴って追記された事項
    b. テレワークと外部サービス利用の常態化に伴って追記された事項
    c. 技術の進展と従業員のプライバシー保護のバランスについて追記された事項
    d. 雇用の流動化を踏まえて追記された事項
    e. サプライチェーン間での情報開示・共有の範囲拡大に伴う対策について
    f. 重要情報の多様化（技術情報、限定提供データ、機微情報）
    g. 国家の競争力維持（経済安全保障）への認識の高まり（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）への言及について
6. 参考資料の改訂について

ハンドブックの狙い、初版公開時期、営業秘密管理指針との関係

ハンドブックの狙い、初版公開時期

【ハンドブック策定の狙い】
経営者を始めとする企業の皆様に、自社における秘密情報の管理を適切に実施していく際の参考としていただくこと

このために：
1. 企業の価値・競争力の源泉となる秘密情報を決定する際の考え方を示すこと
2. 秘密情報を適切に分類し、分類に応じた情報漏えい対策を選択し、秘密情報の取扱い等をルール化するためのフレームワークを示すこと
3. 情報漏えい防止のために講じるべき対策と、万一情報が漏えいした場合の対処方法を具体例に基づいて示すこと
4. 上記を実践できる社内体制の考え方について示すこと
5. 他社の秘密情報に係る紛争に備える方法を具体例に基づいて示すこと

【初版の公開】
ハンドブックの初版は平成28年2月に公開されました。
今回、初版公開後約6年を経て、大規模な改訂が行われました。

営業秘密管理指針との関係

■ 営業秘密管理指針は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
■ ハンドブックは、有効と考えられ、推奨される対策等を、事例に基づき網羅的に紹介するもの

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…

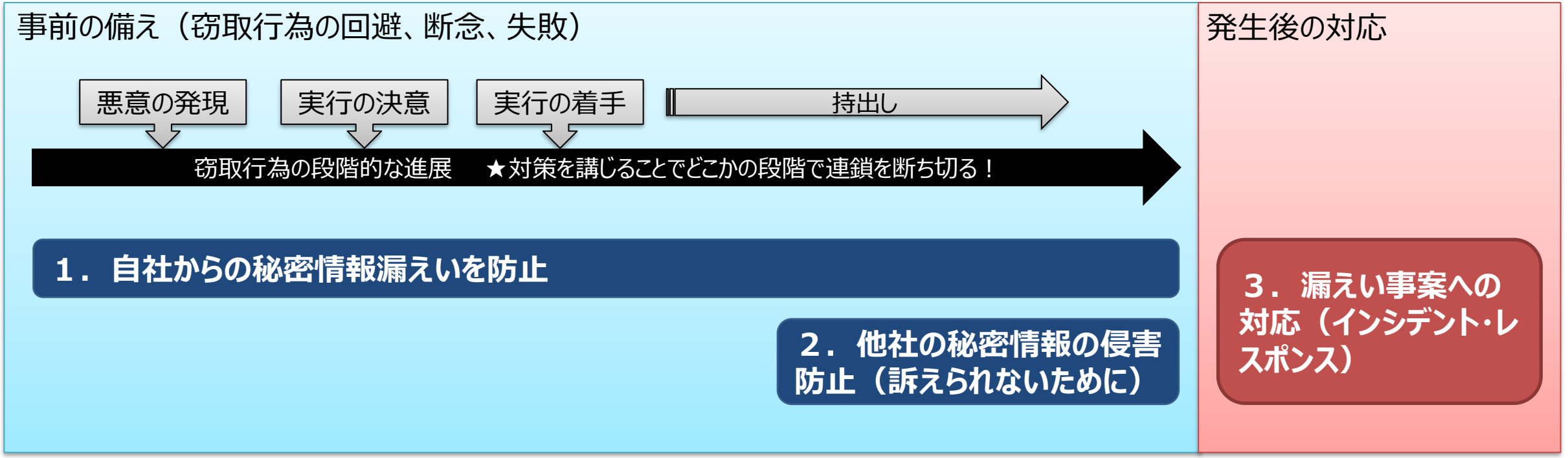
簡易版の「ハンドブックのてびき」では、イラスト付きで秘密情報管理の基本となる考え方を解説しています。
ハンドブックへの導入・理解を助ける資料となっていますので、ぜひご活用ください。
http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/hbtebiki.pdf

（出典）経済産業省知的財産政策室「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４年5月）

秘密情報の保護ハンドブックの概要

情報漏えいに関する３つの重要なシーン

ハンドブックは、①窃取行為を回避・断念・失敗させるための事前の備え、②他社の秘密情報の侵害防止、③漏えい発生後の事案への対応 の３つのシーンに重点を置き、具体的な事例に基づいて望ましい対策・対応を推奨しています。事前の備えは、悪意を持たせない、実行を決意させない、実行させない、持ち出させないという４つの「段階」で構成されています。



４つの典型的な漏えいルートと対策の５つの目的

ハンドブックでは、秘密情報の典型的な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（サイバー攻撃）の４つに焦点を当てています。また、防止対策の目的として、a.接近の制御、b.持出し困難化、c.視認性の確保、d.秘密情報に対する認識向上、e.信頼関係の維持・向上等に着目しています。

【４つの典型的な漏えいルート】

今回改訂の重点 → **従業員等**

今回改訂の重点 → **退職者等**

サプライチェーンの観点での改訂 → **取引先**

外部者

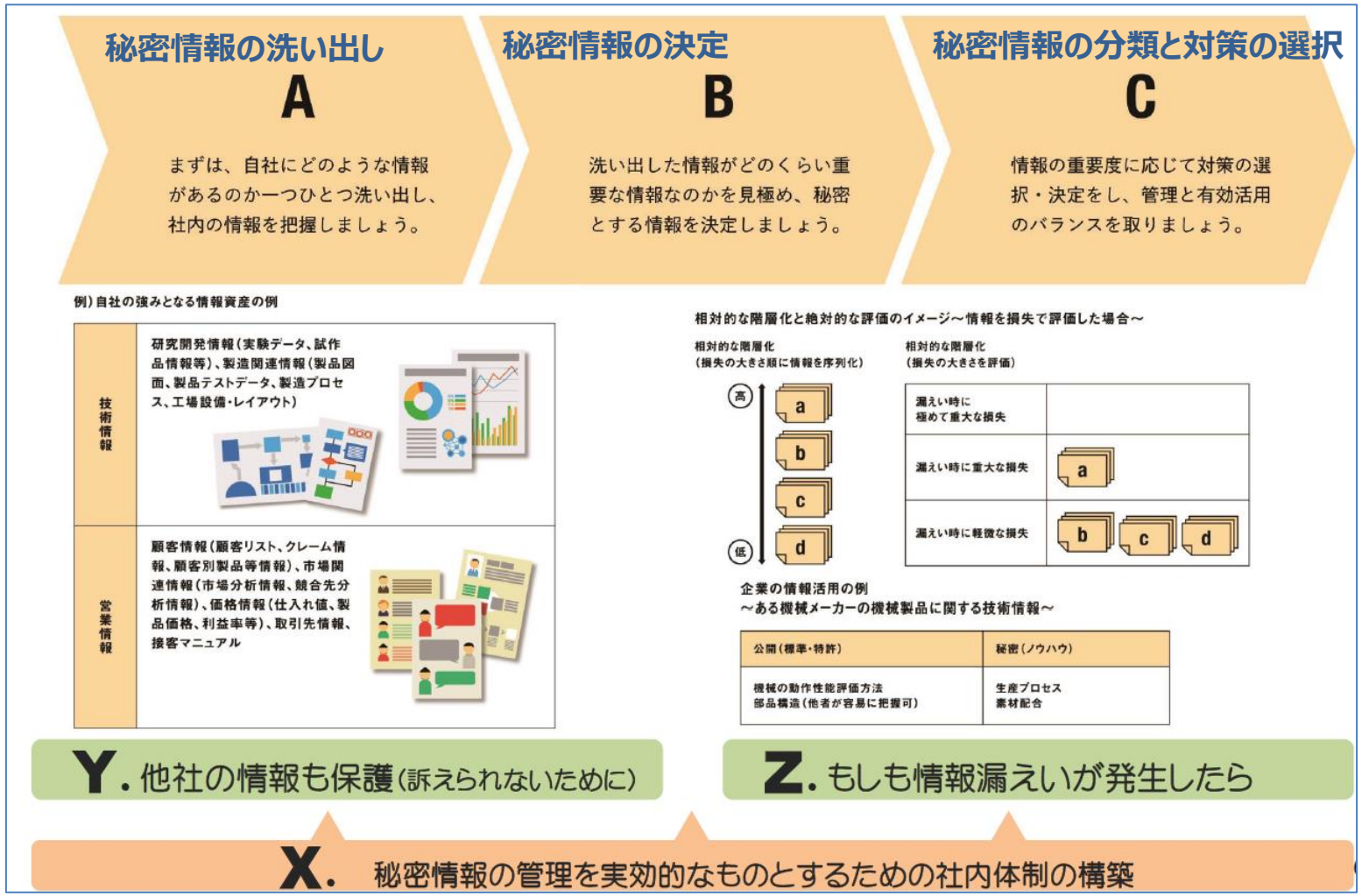
【対策の５つの目的】

	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
	 1	 2	 3	 4	 5
	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

（出典）経済産業省知的財産政策室「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４年5月）

ハンドブックの情報漏えい防止対策の全体像

ハンドブックでは、情報漏えい防止対策を、秘密情報の洗い出し、決定、分類と対策の選択の順に紹介しています。
さらに、漏えい防止体制、他社の秘密情報の保護や事後対策についても推奨をしています。



（出典）経済産業省知的財産政策室「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４年5月）

（参考）ハンドブックの目次構成

APPTraS 営業秘密保護推進研究会

ハンドブック本文の構成

1. 目的及び全体構成
2. 保有する情報の把握・評価、秘密情報の決定
3. 秘密情報の分類、情報漏えい対策の選択及びそのルール化
   ★漏えい主要４ルート×対策の５つの目的
4. 秘密情報の管理に係る社内体制のあり方
5. 他社の秘密情報に係る紛争への備え
6. 漏えい事案への対応

参考資料の構成

参考資料１　秘密情報漏えい対策一覧
参考資料２　各種契約書等の参考例
参考資料３　各種窓口一覧
参考資料４　秘密情報管理に関する各種ガイドライン等について
参考資料５　協業避止契約の有効性について
参考資料６　営業秘密侵害罪における刑事訴訟手続における被害企業の対応のあり方について

ハンドブック改訂の背景とポイント

初版公開後6年間に生じた変化によって顕在化した新たな７つの重要課題

ハンドブック改訂にあたり、初版公開後6年間に生じた変化によって顕在化した７つの重要課題に焦点を当てています。
これらは大きくは、「法制度・ガイドライン関連」「環境変化」「重要情報の多様化」という３つの視点で分類できます。

【関連する法制度の見直し・ガイドラインの改訂への対応】

1. 法制度見直し（不正競争防止法、個人情報保護法）、各種ガイドラインの公開・改訂（テレワークセキュリティ、中小企業の知的財産取引、組織の内部不正防止等）への対応の観点

【環境変化に伴う新たな対策や対策強化の必要性】

2. テレワークに代表される働き方の変化、及びその常態化に伴う情報漏えいの拡大
3. オンラインストレージやクラウド等の外部サービスの利用拡大
4. セキュリティ技術（特にエンドポイントセキュリティやモニタリング技術）の急速な進展と従業員のプライバシーに配慮した運用
5. 雇用の流動化による退職者（転職者）、中途採用者の急増
6. 内部不正やサプライチェーン間での情報開示・共有が事業経営に及ぼすリスクの増大

【重要な秘密情報の多様性への対応】

7. 秘密として管理される重要な技術情報、機微情報（外為法）の漏えいに対する社会的な危機感の急拡大、事業経営に与える損失・インパクトに対する認識の急増。国家の競争力維持（経済安全保障）への認識の高まり（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）。Society5.0におけるデータ漏えいに対する意識の高まり。

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（全体俯瞰）

APPTraS 営業秘密保護推進研究会

「法制度見直し」に伴う修正として、①平成30年の不競法改正で追加された「限定提供データ」の保護、②令和２、３年の個人情報保護法の改正等に関する記載を追加、（この間に発出・改訂された「各種ガイドライン」（「テレワークセキュリティガイドライン」（総務省）、「知的財産取引に関するガイドライン」（中小企業庁）、「組織における内部不正防止ガイドライン」（ＩＰＡ）等）を反映）

【ハンドブックの主な改訂箇所（全体俯瞰）】

1. 目的及び全体構成
   - 限定提供データ
   - 機微情報（外為法）
2. 保有情報の把握 → 保有情報の評価 → 秘密情報の決定
3. 秘密情報の分類 → 分類に応じた情報漏えい対策の選択 → ルール化と社内規程の策定
   - 他社から受領した秘密、限定提供データの扱い
   - 技術情報管理認証制度のコラム
   - 具体的な情報漏えい対策例

従業員等	a.接近の制御 b.持出し困難化 c.視認性の確保 d.秘密情報に対する認識向上 e.信頼関係の維持・向上等
退職者等	a.接近の制御 b.持出し困難化 c.視認性の確保 d.秘密情報に対する認識向上 e.信頼関係の維持・向上等
取引先	a.接近の制御　b.持出し困難化 c.視認性の確保 d.秘密情報に対する認識向上 e.信頼関係の維持・向上等
外部者	a.接近の制御　b.持出し　c.視認性の確保 d.秘密情報に対する認識　頼関係の維持・向上等

4. 秘密情報の管理に係る社内体制
5. 不競法営業秘密の不正使用行為を推定する規定
   - 自社情報の独自性の立証
   - 他社の秘密情報の意図しない侵害防止
     - a.転職者受入れ
     - b. 共同・受託研究開発
     - c. 取引での秘密情報授受
     - d. 技術・営業情報の売込み
   - 営業秘密侵害品に対する紛争の未然防止
6. 個人データ漏えい時の報告義務
   - 漏えいの兆候把握及び疑いの確認方法
   - 初動対応（状況把握・原因究明、被害の検証、対応、体制）
   - 責任追及（刑事・民事）
   - 証拠の保全・収集
   - デジタルフォレンジック情報のインサイダー取引への悪用

テレワーク中に遵守するルールの策定

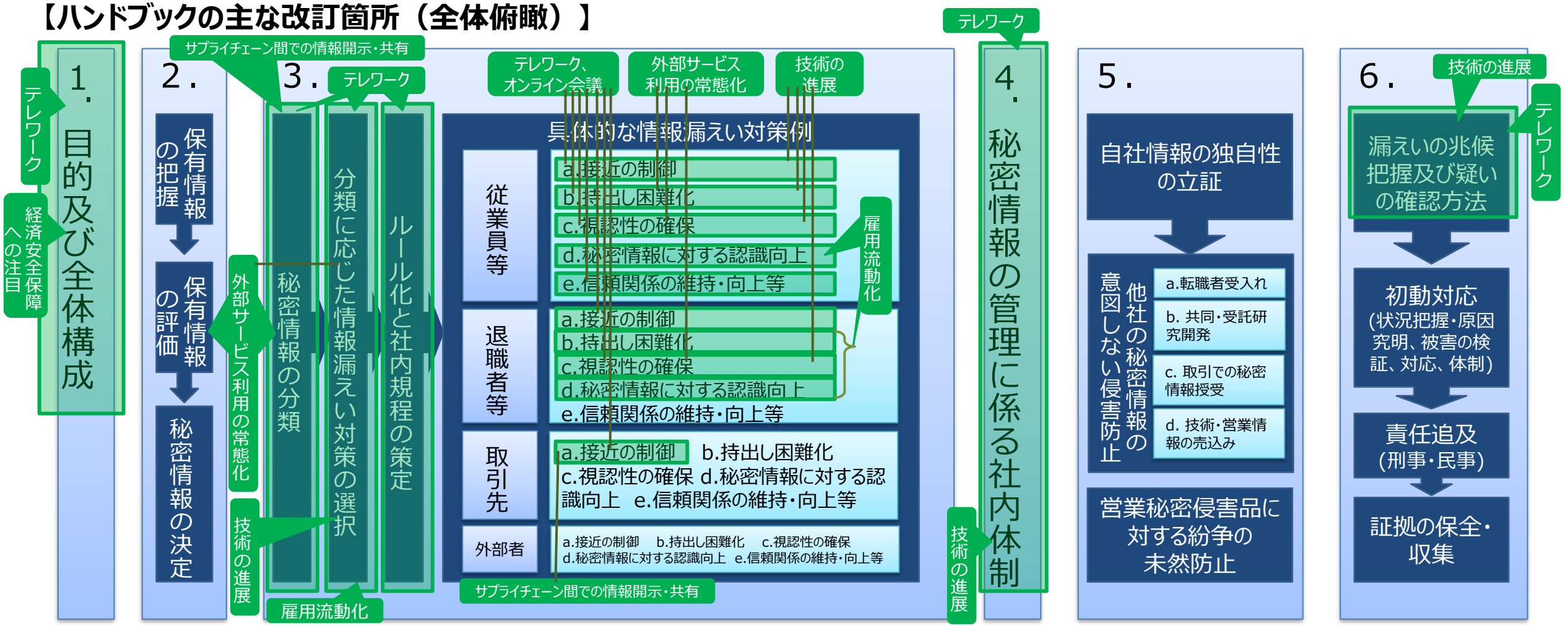
委託先に下請法が適用される場合のセキュリティ対策の助言・支援

限定提供データ、個人情報データベース等不正提供罪

営業秘密・秘密情報をとりまく「環境の変化」に伴う修正（全体俯瞰）

テレワークの普及、雇用の流動化（転出元企業における雇用期間中・退職時の留意点、受入先企業における転職者の受入時の留意点）等の環境変化に合わせた情報漏えい・流出リスクについて記載の見直しを図るとともに、**技術の進展を含む新たな対策**や**サプライチェーン間での情報の開示・共有**に係る記載を追加

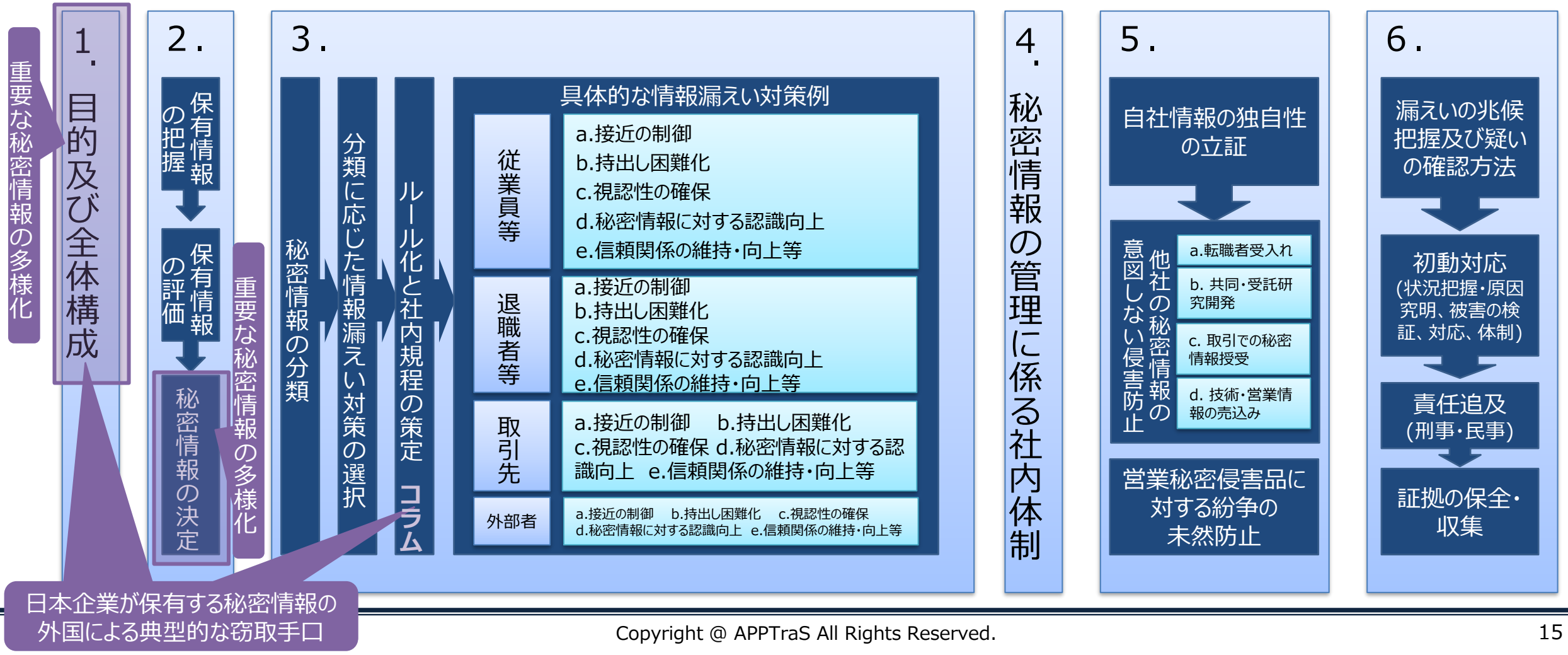
【ハンドブックの主な改訂箇所（全体俯瞰）】



「重要な秘密情報の多様性」への考慮に係る啓発に係る修正・明確化（全体俯瞰）

営業秘密のほか、限定提供データ、個人情報（個人情報保護法）、機微情報（外為法）等具体例を盛り込むことによって、対象の明確化・具体化を実施。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、過去の漏洩事件を踏まえ、典型的なパターンに整理して紹介（警察庁からの提供情報に基づきコラムを追加）。

【ハンドブックの主な改訂箇所（全体俯瞰）】



外国から日本企業が保有する秘密情報が狙われる典型的なパターンとその対策について

～新たに追記された、コラム③「外国から狙われる企業の秘密情報」における重要な注意喚起について～

【警察庁からの注意喚起】外国から日本企業の秘密情報が狙われている！

ハンドブックに新たに追記された『コラム③　外国から狙われる企業の秘密情報』では、

「日本の企業や研究機関が保有する高度な技術情報をはじめとする秘密情報は、これら情報を入手して自国の産業の地位を高めたり、軍事技術に転用したりしようとする外国からも狙われるようになっている」

と警告されています。

＜ハンドブックが指摘する、認識を新たにすべき重要ポイント＞

- **外国のスパイ活動**は、最近では**企業や研究機関で働く人々にも及んでいる**
- あらゆる産業でDXが進展し、秘密情報のデジタル化とIT利用が拡大している
- 技術革新により民生技術と軍事技術の境界があいまいとなり、**盗まれた民生技術が外国で軍事転用**され、我が国の安全保障上のリスクとなる懸念が高まっている
- 英米の防諜・治安機関のグッド・プラクティスに倣い、我が国でも**警察が企業や研究機関に対し、スパイの手口や対策のノウハウを情報提供**するアウトリーチ活動に積極的に取り組んでいる

日本企業が保有する秘密情報が狙われる典型的な手口とは？

ハンドブックに新たに追記された『コラム③　外国から狙われる企業の秘密情報』では、日本企業が保有する秘密情報が窃取される典型的な手口として、下記の３つを挙げている。

海外拠点を踏み台としたサイバー攻撃

＜ハンドブックに掲載された事例＞

- 外国の攻撃者が、同国にある日本の防衛関連産業の海外拠点システムに対し、ウイルス対策管理サーバーの脆弱性を突いた攻撃を実施し、これを踏み台として国内侵入
- 外国に進出した日本企業の現地法人において、公的に導入が義務付けられている税務ソフトウェアをインストールした後、自動的にマルウェアがダウンロードされた

外国政府職員等がスパイとなる内通者を唆す／脅すことによる窃取

＜ハンドブックに掲載された事例＞

- 通信関連会社の社員が外国政府職員を名乗る外国人のアプローチを受け、そそのかされて秘密情報を提供しはじめ、自宅や家族への危害で脅されて足抜けできなくなった
- SNSの個人情報で狙いを付けられて外国企業社員のアプローチを受け、言葉巧みにそそのかされて、不正に取得した秘密情報を電子メールで外国企業に提供

外国政府の息がかかった外国企業による合弁・買収・共同研究

＜ハンドブックに掲載された事例＞

- 日本企業が協定に基づき合弁の相手である外国企業に提供した技術が、当該国政府に渡り、軍事転用される
- 外国企業が先端技術を保有する日本の中小企業を買収し、獲得した技術を軍事転用する
- とある国の経済制裁対象となっていた外国企業の日本法人が、その名前が出ないように、他の日本企業とのタイアップによる共同研究という架空形態を国内の複数大学に提案し、隠れ蓑としようとした

ハンドブックが示す対策の留意点

【海外拠点を踏み台としたサイバー攻撃】

＜ハンドブックが示す対策の留意点＞

■ **海外拠点を経由したサイバー攻撃があり得ることを念頭**に、国内拠点のセキュリティ対策を実施することが必要。海外拠点を含めて脆弱性への対応状況の確認を徹底するほか、**海外拠点から国内拠点が保有する機微な情報へのアクセスを完全に遮断するなどの対策を検討することも効果的**。

■ **公的に導入が義務付けられているソフトウェアだからといって必ずしも安全なものとは限らない**ことを認識することが必要。**海外現地法人が用いるソフトウェアにセキュリティ上の懸念がないか常に情報収集**し、不審な通信の検知・遮断措置を講じることが必要。

■ セキュリティ上の懸念が払拭できないソフトウェアを使用する端末を、他の業務で使用するネットワークから分離しておくなど、**いざというときの被害を最小化するための対策を講じておくこと**。

【外国政府職員等がスパイとなる内通者をそそのかす／脅すことによる窃取】

＜ハンドブックが示す対策の留意点＞

■ **企業等の内部にいる人間がスパイに仕立てられ、こうした者を通じて秘密情報が狙われるリスクは、現実空間にもインターネット上にも存在し、その手口も様々。**

■ **悪意を持った者が自分たちの秘密情報を狙って接近してくるという危険性については**、身近な危険として考えにくく、ともすれば、「自分たちには関係ない」という意識に押しやられ、**当事者意識をもった対策が講じられにくい側面がある**ことに注意。しかし、企業等の秘密情報を確実に守るには、**こうしたリスクが現実のものとなっていることを、経営者やセキュリティ担当者だけでなく、社員一人ひとりに認識してもらうことが必要**。

■ さらに、社員の誰かが**不審なアプローチを受けた際に**、セキュリティ担当者や上司への**相談・報告を行い、組織内で共有した上で**、このリスクを排除し、**再度のアプローチが行われることを防ぐ・備えるという取組を徹底することが重要**。

【外国政府の息がかかった外国企業による合弁・買収・共同研究による獲得】

＜ハンドブックが示す対策の留意点＞

■ 重要なのは、合弁・買収・共同研究といった**通常の経済・学術活動を抑制することではなく、背景に存在するかもしれない情報窃取のリスクを認識しておくこと。合法的な活動により、情報の移転をめぐって意図していなかった結果**（意図していない又は想定していた範囲を超えた秘密情報の移転、自社の技術が外国で軍事転用等）**を招いてしまうリスクが存在するということをまずはしっかりと認識**し、その上で企業等の意思決定を行うことが必要。

■ 秘密情報の管理が及びにくくなるような、**隠れ蓑とできる「工夫」を施して働き掛けが行われる**ことも認識しておくべき。

ハンドブック改訂に関する解説

（注意）
この区画において、赤字下線は今回のハンドブックの追記・修正を意味していません。
今回の追記・修正の意図をご理解いただくにあたり、強調しておきたいポイントに赤字下線を付しています。

本資料で解説するハンドブック改訂の視点

本資料では７つの視点からハンドブックの改訂内容を整理して解説します。

a. 法制度の見直し、ガイドラインの改訂に伴って追記された事項

b. テレワークと外部サービス利用の常態化に伴って追記された事項

c. 技術の進展と従業員のプライバシー保護のバランスについて追記された事項

d. 雇用の流動化を踏まえて追記された事項

e. サプライチェーン間での情報開示・共有の範囲拡大に伴う対策について

f. 重要情報の多様化（技術情報、限定提供データ、機微情報）

g. 国家の競争力維持（経済安全保障）への認識の高まり（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）への言及について

a. 法制度の見直し、ガイドラインの改訂に伴って追記された事項

不正競争防止法については、「限定提供データ」（平成30年度改正）、営業秘密の不正使用行為を推定する規定（不競法第5条の3）についての記載（27年法改正及び30年政令改正の内容）が追記されています。

＜限定提供データについて＞

第1章　目的及び全体構成
１－１　目的及び留意点等
（本書と営業秘密管理指針との関係）
（参考）限定提供データ・限定提供データに関する指針との関係
・・・
本書は、企業が保有する重要な情報について、その漏えい対策のための秘密管理について対象とするものであることから、**必ずしも限定提供データに対して全ての内容があてはまるわけではありませんが、企業が保有する価値ある情報のひとつとして**、情報の把握・評価（第２章）、情報の漏えい対策の選択（第３章）紛争への備え、（第５章）など限定提供データにも活用可能な内容も含まれており、その管理について参考になるものと考えられます。・・・

第2章　保有する情報の把握・評価、秘密情報の決定
２－２　秘密情報の決定
・・・
商品として広く提供されるデータやコンソーシアム内で共有されるデータなど限定提供データに該当しうる情報については、企業間で複数者に提供や共有されることで、新たな事業の創出やサービス製品の付加価値の向上など、その利活用が期待されるデータであることから、**そのデータがどのような価値を持つのかを十分考慮し、適切な法的保護を受けられるような形態で保持・提供することが重要**です。
・・・
Ｓｏｃｉｅｔｙ５．０においては、**重要な情報・データを組織外から大量に取得する機会や外部と共同して利活用する機会が増えていく**ものと考えられることから、外部から取得・入手した重要な情報・データを、組織内において、**取得時の条件を遵守して取扱い、コンプライアンスを確保することが今まで以上に重要**になると考えられます。
・・・
第3章　秘密情報の分類、情報漏えい対策の選択及びそのルール化
３－１　秘密の分類
・・・
また、個人情報保護法に基づく管理が求められる個人情報や、他社から秘密保持義務を負った状態で受領した情報（営業秘密、**限定提供データのほか、契約・信義則に基づく秘密保持義務を負っている情報**）など、**「法令や他社との契約に基づく特別の管理」を求められる情報については別の対策を講ずる分類とすべき場合もあります**。・・・

第6章　漏えい事案への対応
６－３　責任追及
・・・その前提として、責任追及の確実性と証拠収集の効率性を見据えて、**どの情報を不正競争防止法上の責任追及に係る**「営業秘密」又は**「限定提供データ」とするのかを明確にする**という点にも留意します。・・・

（２）民事的措置
民事保全手続：営業秘密侵害や**限定提供データ侵害が疑われるケースでは**、営業秘密や**限定提供データの開示・使用の仮の差止めや、競合他社への就職の仮の差止め等が考えられる**。
民事裁判手続：営業秘密・**限定提供データの使用の差止請求、**営業秘密・**限定提供データの漏えいによる損害賠償請求等を求める裁判手続**。

a. 法制度の見直し、ガイドラインの改訂に伴って追記された事項

（続き）

＜営業秘密の不正使用行為を推定する規定の対象拡大等について＞

第5章　他社の秘密情報に係る紛争への備え
（前文）
・・・
また、平成２７年不正競争防止法改正により、新たに導入された**営業秘密の不正使用行為を推定する規定（同法第５条の２）**及び新たに規制対象となった営業秘密侵害品の取引（同法第２条第１項第１０号）について、紛争を防止するための方策も紹介します。

５－２　他社の秘密情報の意図しない侵害の防止
・・・
加えて、**平成２７年不正競争防止法改正**により、営業秘密の不正使用行為を推定する規定（同法第５条の２）が導入され、**「生産方法の営業秘密」を違法に取得して、その生産方法により生産することができる製品を生産している場合には、違法に取得した営業秘密を不正使用したものと推定される**こととなりました。また、**平成３０年の不正競争防止法施行令**において、**「情報の評価又は分析の方法（生産方法に該当するものを除く。）の営業秘密」がこの推定規定の対象として追加**され（第１条）、これを違法に取得し、使用して評価し、又は分析する役務を提供している場合には、違法に取得した営業秘密を不正使用したものと推定されることとなりました。なお、ここでいう「違法な取得」には、不正開示であることを知らないことにつき「重大な過失」がある状態で営業秘密を取得する場合も含まれることから、特に「重大な過失」とされてしまうことのないような対応をすることが重要です。

a. 法制度の見直し、ガイドラインの改訂に伴って追記された事項

個人情報保護法については、「個人データ漏えい時の報告義務」（令和2年改正）、「個人情報データベース等不正提供罪」（平成29年5月適用）についての記載が追記されています。

第６章　漏えい事案への対応
６－２　初動対応
（３）初動対応の観点
〇法律に基づく手続　[具体例]
・・・
特に、**故意の内部不正によって個人データが漏えいした場合は、遅滞なく、個人情報保護委員会及び本人**（漏えいしたデータの保有者）**への報告を実施**。また、**事態の発生を認識した後速やかに報告**するとともに、**６０日以内に確報**を行う。
・・・

６－３　責任追及
（１）刑事的措置
秘密情報の漏えいの事案では、当該情報が営業秘密に該当した場合に不正競争防止法上の営業秘密侵害罪（同法第２１条等）に該当し得るだけではなく、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）、**個人情報データベース等不正提供罪（個人情報保護法第８４条）等に該当する可能性もあります**。

a. 法制度の見直し、ガイドラインの改訂に伴って追記された事項

不正競争防止法、個人情報保護法以外では、ハンドブックは、外為法の機微情報、委託先に下請代金支払遅延等防止法が適用される場合の助言・支援、産業競争力強化法に基づく「技術情報管理認証制度」、デジタルフォレンジック調査におけるインサイダー取引規制への留意等について追記しています。

第２章　保有する情報の把握・評価、秘密情報の決定
（１）秘密情報の決定に当たって考慮すべき観点のイメージ
②技術情報
・・・
その漏えいにより、法令違反や他社との契約違反等となり、当該他社との信頼関係を毀損させる情報か否か
（受託やライセンス等の他社との契約等により限定的に開示された技術情報、**安全保障貿易管理に関わる製品に関する技術情報**等）

第3章　秘密情報の分類、情報漏えい対策の選択及びルール化
３－４　具体的な情報漏えい対策例
（３）取引先に向けた対策
⑤「信頼関係の維持・向上等」に資する対策
c.委託先に下請代金支払遅延等防止法が適用される場合の助言・支援
・・・
委託先が下請代金支払遅延等防止法を適用される場合には、下請中小企業振興法に基づく「振興基準」46第３の５（２）にあるように、委託先に対してセキュリティ対策の助言・支援を行うこととされています。また、セキュリティ対策に資する特定の物やサービスの購入を強制することは禁じられています。

第4章　秘密情報の管理に係る社内体制のあり方
コラム⑥　技術情報管理認証制度について
認証制度とは、どういう制度でしょうか？　　漏えい防止策は何があるでしょうか？　　認証取得のメリットは何でしょうか？

第6章　漏えい事案への対応
６－４　証拠の保全・収集
（１）証拠の保全
・・・
なお、デジタルフォレンジックの活用にあたっては、・・・**漏えいした秘密情報にインサイダー情報が含まれる場合は、外部のデジタルフォレンジック解析を支援する担当者等に厳正な秘密保護・管理を求め、インサイダー取引につながらないようにします**。

b. テレワークと外部サービス利用の常態化に伴って追記された事項

今回のハンドブック改訂では、テレワークに関する追記・修正が最も多くなっています。外部サービス利用の常態化も併せると、5章以外の全ての章で追記・修正が行われています。

テレワークに関する追記・修正を整理すると、概ね次のような事項となっています。

- 概観：テレワークの普及・進展、働き方の多様化を踏まえた情報管理のあり方の変化
- テレワークと外部サービス利用の常態化に伴い、重要情報が社外にも分散することへの対応（事前対策、事後対応）
  より細かい単位でのアクセス制御が可能なアクセス権限管理基盤の整備推進
  個人端末利用（BYOD）の制限
  利用できるソフトウェア／オンラインサービスの制限
  VPN等の導入
  オンライン会議で資料表示した情報の漏えい対策
  エンドポイントセキュリティ対策による視認性の向上（テレワーク端末のログ取得等）を活かした、テレワーク者からの情報漏えい対策の強化
- テレワーク中のコミュニケーション改善
- 退職者のテレワーク権限の削除、一般の従業員より高度なログ確認
- 退職予定者との間の秘密保持義務契約に係る課題とその改善

  等

b. テレワークと外部サービス利用の常態化に伴って追記された事項

第１章　目的及び全体構成
１－１　目的及び留意点等
（秘密情報の管理の効用）
・・・
また、近年の情報通信機器・技術の普及・進展、働き方の多様化・柔軟化の流れとともに、大規模な感染症や各種防災への対応・対策の関係上、**企業におけるテレワークの取組みが急速に進んでいます**。このような中、情報の利用・アクセスがこれまでの企業内から、**自宅やサテライト施設など外部からの情報利用・アクセスが常態化しつつあり、このような流れを踏まえた秘密情報の管理・利用のあり方を検討し、取り入れることも、経営者や情報管理責任者にとって必要**となってきています。

第2章　保有する情報の把握・評価・秘密情報の決定
２－１企業が保有する情報の全体像の把握
（企業が保有する情報とは）
まずは、自社において「どういった情報を保有しているのか」を全体的に把握することから始まります。その際、情報は、紙に記載されていたり、サーバーやＰＣ、ＵＳＢメモリ等の機器・媒体や、**クラウドなどの外部サービスに記録された電子データ等のような形で存在**するだけではありません。その他にも、従業員が業務の中で記憶した製造ノウハウなど文章化されず目に見えない形で存在する場合や、プラントのレイアウト、金型、試作品、Ｆ１系統の親品種となる植物などの「物」自体が把握すべき情報である場合もあるので留意する必要があります。

第3章　秘密情報の分類、情報漏えい対策の選択及びそのルール化
３－１　秘密情報の分類
（分類に当たっての考え方）
・・・
一方で、同程度の評価の秘密情報であっても、**以下のような「情報の利用態様」に応じて、異なる対策を講ずる場合もあります**。
※「情報の利用態様」は予め定められたものではなく、**自社の事業規模や業種、取り扱う情報の内容・性質等を踏まえた上で、望ましい「情報の利用態様」とは何かを自主的に判断**することが重要です。
例えば、その秘密情報は、「従業員各々に個別に資料を所持させるべきものなのか、共有資料のみとするのか」や、**「ネットワークに接続されたＰＣ、クラウドなどの外部サービス等に保管すべき情報か否か」**、**「テレワークなど社外からのアクセスや個人所有のデバイスを用いたアクセスに際して使用を認めるべき情報か否か**」、「サプライチェーンで共有する必要がある情報か否か」といったことを**今一度検討してみる**ことが有効です。

【情報の利用態様として考慮すべき観点の例】
・・・
テレワークなど**社外からのアクセスや個人所有のデバイスを用いたアクセスに際して使用を認めるべき情報か**否か
・・・
外部ネットワークに接続されたＰＣ、クラウドなどの外部サービス等に保管されることが多い情報か否か　・・・

b. テレワークと外部サービス利用の常態化に伴って追記された事項

（続き）

３－２　分類に応じた情報漏えい対策の選択
（対策の選択に当たっての考え方）
本章３－１において設定した秘密情報の分類ごとに、具体的にどのような情報漏えい対策を講ずるのかを選択します。・・・加えて、転職者の増加や、様々な契約形態に基づく人事やグローバル人材の登用、**テレワークの導入・実施状況や個人端末による情報利用の可否**など、各社の事情**に応じた対策を選択することが有効**です。

【５つの「対策の目的」】
（１）接近の制御
・・・
また、今後、**さらに普及・常態化するテレワークにおいては**、外部からの情報へのアクセスをよりきめ細かい単位で制御することが求められるようになるため、**細かいアクセス権限管理に対応できるアクセス管理基盤の整備、雇用関係の終了や契約の終了に伴い速やかなテレワークでのアクセス権限の削除が望まれます**。

（２）持出し困難化
秘密情報が記載された会議資料等の回収や**テレワーク・オンライン会議でのアクセス（投影等）の制限**、事業者が保有するノートＰＣの固定や持ち出しの制限、記録媒体への複製制限や**組織が許可した以外のオンラインストレージの利用制限**、従業員の私物ＵＳＢメモリ等の携帯メモリの持込み・利用を制限すること等によって、当該秘密情報を無断で複製したり持ち出すことを物理的、技術的に阻止することを目的としています。
特に、**テレワークの実施との関係では、重要情報のレベルに応じたアクセス制限、ＰＣ等への格納制限、実施を認める場所**の吟味（自宅等の周囲の目から遮断が可能・容易な環境か、電車やカフェ等の周囲の目がある環境か）**、画面の覗き込み防止フィルムを用いる、オンラインで会議を行う際は大声での会話を避ける、組織ネットワークに接続する際にはＶＰＮ等を用いて暗号化する等の対策を講じる**ことが重要となります。

（３）視認性の確保
・・・
特に、**テレワークの実施との関係では**、自宅、サテライトオフィスなど職場と同レベルでの視認性を確保することが困難となることが想定されることから、**テレワークに伴う秘密情報・重要情報へのアクセス履歴、操作履歴**（Ｗｅｂへのアクセスログやメールの送受信履歴など）**等のログ・認証を記録し、一定の期間に安全に保存**することが視認性の確保のための対策としても有効であると考えられます。

（５）信頼関係の維持・向上等
・・・
また、テレワークの実施との関係では、**テレワーク実施中の従業員等**は疎外感や不安感に悩むことが多いだけでなく、不審な挙動がすぐには見つからない状況にあることや外部の脅威者からのアプローチを受けやすいと考えられます。そこで、対策として**悩みに対して相談・助言を提供する窓口の設置やコミュニケーションツールの整備、定期的なアンケートによる疎外感・不安感を感じている従業員等の可視化、オンライン会議での定期的な職場コミュニケーションの実施、定期的な出勤日の設定等を通じて、過度な干渉にならない程度の良好で十分なコミュニケーション機会を確保することは、従業員等の不安感・疎外感の払拭につながる上、信頼関係の維持・向上のための対策としても有効**であると考えられます。

b. テレワークと外部サービス利用の常態化に伴って追記された事項

（続き）

３－３　秘密情報の取扱い方法等に関するルール化

（１）ルール化の必要性とその方法

・・・

近年、テレワークが普及し、常態化しつつありますが、秘密情報のレベルに応じたアクセス制限やＰＣ等への格納の制限を行わないと、企業の管理下にない個人所有のＰＣ等に秘密情報を格納したり、従業員等関係者以外の者が秘密情報にアクセスしたりする可能性があります。このため、**テレワークでクラウドサービスを利用する場合に、適切に定められた基準に基づいて予め許可された情報のみを取り扱い、当該情報をクラウド上に置く際のアクセス権限を適切に設定すること等で、秘密情報の漏えい防止に効果があるため、テレワーク中に従業員が遵守すべきルールを社内ルールの中で定めることが必要**です（**就業規則や情報管理規定といった既存の規定に追加する、またはテレワークに特化したルールを別途作成する**など、方法は各社の事情に応じて対応を進めることが望ましいと考えられます。）。

（２）秘密情報の取扱い等に関する社内の規定の策定

・・・

また、**テレワークの実施に際しては、企業の外で業務を行う中で秘密情報を取り扱う可能性があり、秘密情報の漏えいリスクが高まると考えられることから、秘密情報の漏えい対策の強化が求められます**。詳細については、総務省「テレワークセキュリティ対策第５版（令和３年５月）」、ＩＰＡ「組織における内部不正防止ガイドライン」をご覧ください。社内の規程を周知して、従業員等の秘密情報の取扱い等についての理解を深めることは、それ自体が「秘密情報に対する認識向上」に資する対策となります。

【テレワークなど企業組織の外での業務における秘密情報の保護のための対策のポイントの例】

- 電車内やカフェ等では画面を覗き込まれないように注意する。また、秘密情報について大声で会話し、漏えいが発生しないように注意する。
- 不特定多数の利用者が利用するネットワーク（例：ホテルの有線ＬＡＮ・無線ＬＡＮ、公衆無線ＬＡＮ）の接続を許可するかどうかを判断する。また、**許可されたネットワーク環境から企業のネットワークに接続する際には、秘密情報を暗号化したり、ＶＰＮ等を用いて通信を暗号化**する。
- 外部から企業ネットワークに接続する場合、**テレワークで用いるＰＣ等には電子データを可能な限り保存しない**ことが望まれる。
- 採用するテレワークの方式によっては、その特性に応じた情報漏えいの対策の強化が求められることがある。（例：テレワーク用ＰＣ上にデータの保存が可能な場合、端末の内蔵記憶装置の号化やデータのリモートワイプの対策強化）
- これらの対策を前提として、**組織外での業務（テレワーク）を認めるにあたり、従業員遵守すべき事項を定め、従業員の服務規律として就業規則等の内部規定でその遵守を求める**。また、定めた内部規定について、定期的に実施状況を把握し、改善を図ることも必要。
- 企業の外部での共同作業（**テレワーク等**）**でクラウドサービスを利用する場合、利用する情報がクラウドサービスで取り扱って良い情報かどうかの判断基準を定めて遵守を求めるとともに、セキュリティ確保のためのルール**（クラウドサービスで用いるパスワードについて他の用務で用いるパスワードとの共用を避けるなどの厳格な管理、データの共有範囲の限定等）**を定めて、対象となる従業員に教育を通じて徹底を図る**。
- **海外からのテレワークは、インシデント発生時の自社からの対応が困難であること、外国政府による監視の可能性・リスク、データの管理・取り扱いに対する現地の法制度への配慮が必要であることなどからリスクが高く、特別な情報漏えい対策を検討する必要**がある。

b. テレワークと外部サービス利用の常態化に伴って追記された事項

（続き）

３－４　具体的な情報漏えい対策例
（１）従業員に向けた対策
①「接近の制御」に資する対策
・・・
なお、今後、さらに**普及・常態化するテレワークにおいては**、外部からの情報へのアクセスをよりきめ細かい単位で制御することが求められるようになるため、**細かいアクセス権限管理に対応できるアクセス管理基盤の整備、雇用関係の終了や契約の終了に伴い速やかなテレワークでのアクセス権限の削除が望まれます**。

a. ルールに基づく適切なアクセス権の付与・管理
・・・なお、今後、さらに**普及・常態化するテレワーク等においては**、企業の外部から秘密情報へのアクセスを細かい単位で制御することが求められるようになるため、**きめ細かいアクセス権限管理に対応できるアクセス管理基盤の整備を行う**ことが考えられます。
・・・

②「持出し困難化」に資する対策
（略）
a. 秘密情報が記された会議資料等の適切な回収
・・・　※テレワークの普及を背景に、オンライン会議についても浸透しつつあります。秘密情報を紙・電子データで直接に配布・送信することが避けることが可能な一方で、会議中に画面上で秘密情報を共有・表示こともあるかもしれませんが、このようなときには、**会議画面が録画・撮影される可能性も考慮して、オンライン会議の画面上で共有する情報についても事前に精査する、発表前に録画機能が用いられていないかどうか確認するといった点に注意を払う**ことが考えられます※i。

e. 社外へのメール送信・Webアクセスの制限
・・・
ＰＣ等の情報機器では、企業内で許可されたソフトウェア以外のものを利用してインストールすることや、**企業が許可した以外のオンラインストレージを利用することを禁止**し、企業内ネットワークから情報を外部に持ち出すことを防止・困難化します。

h. コピー防止用紙やコピーガード付の記録媒体・電子データ等により秘密情報を保管
・・・
※iの再掲

j. 私物のＵＳＢメモリや情報機器、カメラ等の記録媒体・撮影機器の業務利用・持込みの制限
・・・
テレワークを実施する場合には、**テレワークで用いるＰＣ等には電子データを可能な限り保存しない、秘密情報を暗号化したり、ＶＰＮ等を用いて通信を暗号化するといったシステムや機器の利用制限を行うことのほか、ＥＤＲ（Endpoint Detection and Response）の導入などするなど内部不正モニタリングシステムを活用し、操作・送信履歴を確保するなどの視認性を高める取組みと組み合わせることで、情報の持出し・漏えいを困難にする**ことが考えられます。

b. テレワークと外部サービス利用の常態化に伴って追記された事項

（続き）

（１）従業員に向けた対策

③「視認性の確保」に資する対策

・・・

このほか、テレワークの実施との関係では、自宅、サテライトオフィスなど職場と同レベルでの視認性を確保することが困難となることが想定されることから、**テレワークに伴う**秘密情報・重要情報へのアクセス履歴、操作履歴（Ｗｅｂへのアクセスログやメールの送受信履歴など）等の**ログ・認証を記録し、一定の期間に安全に保存することが視認性の確保のための対策としても有効**であると考えられます。

j. 秘密情報が記録された媒体の管理等

・・・

さらに、**共有保管された書類、ファイル、記録媒体を**貸し出す場合や**テレワークの実施のために自宅等に持ち帰る場合には**、誰にどの記録媒体を貸し出しているかわかるように、**貸出し時及び返却時に、その日時、氏名、貸し出した資料名等を記録して管理**します。・・・

o. PCやネットワーク等の情報システムにおけるログの記録・保存とその周知

・・・

さらに、テレワークの場合、企業内での場合と異なり物理的な視認性の確保が困難なことから、**テレワークに伴うログを記録して、安全に保存するようにします**（講演者注：こうした記録はテレワーク端末にEDRを導入するなどで取得することができるようになります）。このログには、秘密情報へのアクセス履歴、利用者の操作履歴（Ｗｅｂのアクセスやメールの送受信履歴など）、ＶＰＮ装置へのアクセス履歴、テレワーク関連機器やクラウドサービスにログインした際の認証・操作履歴、テレワーク端末の操作履歴等についても取得します。

⑤「信頼関係の維持・向上」に資する対策」

・・・

また、テレワーク実施中の従業員等は疎外感や不安感に悩むことが多いだけでなく、不審な挙動がすぐには見つからない状況にあることや外部の脅威者からのアプローチを受けやすいといった恐れがあります。このため、**悩みに対して相談・助言を提供する窓口の設置やコミュニケーションツールの整備等を通じて、良好で十分なコミュニケーション機会を確保することは、従業員等の不安感・疎外感の払拭につながり、信頼関係の維持・向上のための対策としても有効**であると考えられます。

d. 働きやすい職場環境の整備

・・・

なお、テレワーク実施中の従業員等は疎外感や不安感に悩むことが多いだけでなく、不審な挙動がすぐには見つからない状況にあることや外部の脅威者からのアプローチを受けやすいと考えられます。そこで、対策として、**悩みに対して相談・助言を提供する窓口の設置やコミュニケーションツールの整備、定期的なアンケートによる疎外感・不安感を感じている従業員等の可視化、オンライン会議での定期的な職場コミュニケーションの実施、定期的な出勤日の設定等を通じて、過度な干渉にならない程度の良好で十分なコミュニケーション機会を確保することは、従業員等の不安感・疎外感の払拭につながる上、信頼関係の維持・向上のための対策としても有効**であると考えられます。

b. テレワークと外部サービス利用の常態化に伴って追記された事項

（続き）

（２）退職者等に向けた対策
①「接近の制御」に資する対策
退職時には、遅滞なく、その退職者の情報システムの利用者ＩＤやアクセス権限（**テレワークのための権限**を含む）**を削除します**。・・・
従事している業務内容によっては、退職予定者等について、しかるべきタイミングで、秘密情報へのアクセス権（**テレワークのための権限**を含む）**を適切に制限する**ことも考えられます。

③「視認性の確保」に資する対策
q. 退職をきっかけとした対策の厳格化とその旨の通知
（厳格化する対策の例）
・・・
「ｏ.ＰＣやネットワーク等の情報システムにおけるログの記録・保存とその周知」について、視認性の確保が困難になるテレワークについて、**退職の申出があった後にはテレワークに伴う履歴やクラウドサービスログイン時の認証・操作ログの確認など、一般の従業員と比べて高度な確認を行う**。

（３）取引先に向けた対策
①「接近の制御」に資する対策
a. 取引先に開示する情報の厳選
（具体例）
・・・オンラインでの打合せの場合には、**オンライン会議の画面上で共有する情報についても事前に精査**する、発表前に録画機能が用いられていないかどうか確認する。

⑤「信頼関係の維持・向上等」に資する対策
c. 委託先に下請代金支払遅延等防止法が適用される場合の助言・支援
業務を委託する場合、秘密情報の取扱いについて必要なセキュリティ対策（委託先がテレワークを実施している場合は、**テレワークセキュリティ**を含む）**が確実に実施されることを契約に先立って確認するために、委託業務の内容に沿って、委託先の体制や規定等の点検、個人情報漏えい事故発生時に委託先が委託元の調査に協力する義務を負うことの確認、予め合意した規定等に基づいて委託後の監査に協力することが可能かどうかの確認等を実施し、その結果について適切に評価**することが望まれます。
・・・

b. テレワークと外部サービス利用の常態化に伴って追記された事項

（続き）

第４章　秘密情報の管理に係る社内体制のあり方
４－１　社内体制構築に当たっての基本的な考え方
（経営層の関与の必要性）
・・・
また、秘密情報は全ての部門に存在することが考えられ、かつ、その漏えい対策は、知的財産、人事・労務、情報セキュリティ、法務といった従来から対策に関与していた部門のほか、**テレワークの導入・浸透に伴う新たな課題への対応に伴うテレワークに対応した相談窓口**や外部メンタルヘルスケアの支援などの多様な観点からの対策を必要とすることから、自社内の個々の部門が、それぞれ**独自に対策を行い、全体としての調整を欠いたままでは十分な対策を講ずることはできません**。・・・

４－２　各部門の役割分担の例
・・・
■人事・労務担当
（情報漏えい対策に関する役割）
・・・**テレワーク**や雇用の流動化など**社会環境や事業環境が変化する中での従業員のメンタルヘルスケアの支援等**

第６章　漏えい事案への対応
６－１　漏えいの兆候の把握及び疑いの確認方法
（２）漏えいの疑いの確認
・・・
テレワークの場合、企業内での場合と異なり物理的な視認性の確保が困難なことから、**テレワークに伴うログを記録して、安全に保存するようにします**（講演者注：テレワーク端末へのEDR導入が有効）。このログには、秘密情報へのアクセス履歴、利用者の操作履歴（Ｗｅｂのアクセスやメールの送受信履歴など）、ＶＰＮ装置へのアクセス履歴、テレワーク関連機器やクラウドサービスにログインした際の認証・操作履歴、テレワーク端末の操作履歴等についても取得します。

c. 技術の進展と従業員のプライバシー保護のバランスについて追記された事項

技術的には、接近の制御に関するアクセス管理基盤、視認性の向上に関する高度な従業員モニタリングシステム、高度なエンドポイントセキュリティ技術（EDRの導入等）、外部サービスの利用履歴取得のための高度なクラウドプロキシ技術等の実用化を念頭に、追記が行われています。
他方で、視認性の向上は従業員のプライバシー侵害に繋がりかねないため、これを防ぐ対策についても追記されています。

第３章　秘密情報の分類、情報漏えい対策の選択及びルール化
３－２　分類に応じた情報漏えい対策の選択
【５つの「対策の目的」】
（１）接近の制御
また、今後、さらに普及・常態化するテレワークにおいては、外部からの情報へのアクセスをよりきめ細かい単位で制御することが求められるようになるため、**細かいアクセス権限管理に対応できるアクセス管理基盤の整備**、雇用関係の終了や契約の終了に伴い速やかなテレワークでのアクセス権限の削除が望まれます※１。

（３）視認性の確保
近年は、**ＡＩ等の最新技術を組み入れた高度な内部不正モニタリングシステム**の開発も進んでおり、これ**を活用することが有効**と考えられます。このほか、**可視性を強化してセキュリティコントロールのレベルを維持する努力（講演者注：EDR等）も行うことも有効**と考えられます。
また、ここでの対策は、従業員等の行為の正当性（身の潔白）を証明する手段としても有効であり、このような**従業員をモニタリングすることの目的が従業員の保護であることを就業規則等に明記して従業員に周知徹底するとともに、従業員の理解を得た上で、適切な運用を行うことが必要**です。

３－４　具体的な情報漏えい対策例
（１）従業員等に向けた対策
①「接近の制御」に資する対策
・・・
※１と同じ追記

a. ルールに基づく適切なアクセス権の付与・管理
・・・
なお、今後、さらに普及・常態化するテレワーク等においては、企業の外部から秘密情報へのアクセスを細かい単位で制御することが求められるようになるため、**きめ細かいアクセス権限管理に対応できるアクセス管理基盤の整備を行う**ことが考えられます。

c. 技術の進展と従業員のプライバシー保護のバランスについて追記された事項

(続き)

３－４　具体的な情報漏えい対策例
（１）従業員等に向けた対策
②「持出し困難化」に資する対策
・・・
j.私物のＵＳＢメモリや情報機器、カメラ等の記録媒体・撮影機器の業務利用・持込みの制限
・・・
テレワークを実施する場合には、テレワークで用いるＰＣ等には電子データを可能な限り保存しない、秘密情報を暗号化したり、ＶＰＮ等を用いて通信を暗号化するといったシステムや機器の利用制限を行うことのほか、**ＥＤＲ（Endpoint Detection and Response）の導入などするなど内部不正モニタリングシステムを活用し、操作・送信履歴を確保するなどの視認性を高める取組みと組み合わせる**ことで、情報の持出し・漏えいを困難にすることが考えられます。

③「視認性の確保」に資する対策
・・・特に、近年は、**ＡＩ等の最新技術を組み入れた高度な内部不正モニタリングシステムの開発も進んでおり、【目につきやすい状況を作り出す対策】、【事後的に検知されやすい状況を作り出す対策】の実効性を補完し高める観点から、これを活用することが有効**と考えられます。
また、ここでの対策は、従業員等の行為の正当性（身の潔白）を証明する手段としても有効であり、このような**従業員をモニタリングすることの目的が従業員の保護であることを就業規則等に明記して従業員に周知徹底するとともに、従業員の理解を得た上で、適切な運用を行う**ことが必要です。
・・・
このほか、テレワークの実施との関係では、自宅、サテライトオフィスなど職場と同レベルでの視認性を確保することが困難となることが想定されることから、**テレワークに伴う秘密情報・重要情報へのアクセス履歴、操作履歴（Ｗｅｂへのアクセスログやメールの送受信履歴など）等のログ・認証を記録し、一定の期間に安全に保存することが視認性の確保のための対策としても有効**であると考えられます。（講演者注：こうした記録はテレワーク端末にEDRを導入するなどで取得することができるようになります。）

【事後に検知されやすい状況を作り出す対策】
ｏ．ＰＣやネットワーク等の情報システムにおけるログの記録・保存とその周知
・・・
また、高度なモニタリングシステムの導入・活用という観点からは、**クラウドプロキシを導入し、これに含まれている接続・操作ログを取得・分析する機能、マルウェア対策機能、不正サイトへの接続をブロックする機能等を利用**することや、**ＥＤＲの導入し、エンドポイントにおける不審な挙動や異常を検知し、管理者に通報して早期の対応を支援するソリューションを活用するなど可視性を強化してセキュリティコントロールのレベルを維持する努力を講じる**事も考えられます。（講演者注：特に後者の対策がいわゆる「ゼロトラスト」に繋がるものと理解して良い）
さらに、テレワークの場合、企業内での場合と異なり物理的な視認性の確保が困難なことから、**テレワークに伴うログを記録して、安全に保存するようにします**（講演者注：テレワーク端末へのEDR導入が有効）。このログには、秘密情報へのアクセス履歴、利用者の操作履歴（Ｗｅｂのアクセスやメールの送受信履歴など）、ＶＰＮ装置へのアクセス履歴、テレワーク関連機器やクラウドサービスにログインした際の認証・操作履歴、テレワーク端末の操作履歴等についても取得します。

ｃ．技術の進展と従業員のプライバシー保護のバランスについて追記された事項

(続き)

第4章　秘密情報の管理に係る社内体制のあり方
４－２　各部門の役割分担の例
・・・
■情報システム担当（セキュリティ担当、IT担当）
（情報漏えい対策に関する役割）
・・・
不正アクセス等に対する防護システムの導入・運用、**ＡＩを活用した最新の対策技術・不正検知技術等の導入の検討・運用**

第6章　漏えい事案への対応
６－１　漏えいの兆候の把握及び疑いの確認方法
（２）漏えいの疑いの確認
テレワークの場合、企業内での場合と異なり物理的な視認性の確保が困難なことから、**テレワークに伴うログを記録して、安全に保存するようにします**（講演者注：テレワーク端末へのEDR導入が有効）。このログには、秘密情報へのアクセス履歴、利用者の操作履歴（Ｗｅｂのアクセスやメールの送受信履歴など）、ＶＰＮ装置へのアクセス履歴、テレワーク関連機器やクラウドサービスにログインした際の認証・操作履歴、テレワーク端末の操作履歴等についても取得します。
また、**モニタリングシステムの**開発も進んでおり、これを活用することが有効と考えられますが、その**導入に当たっては、従業員保護のための適切な設定ができるものを選定し、プライバシー・人権を保護するための個人情報保護法等の法的要求を満足できる組織体制を構築することが必要**です。さらに、このような**従業員をモニタリングすることは従業員等の行為の正当性（身の潔白）を証明する手段としても有効であり、その目的が従業員の保護であることを就業規則等に明記して従業員に周知徹底するとともに、従業員の理解を得た上で、適切な運用を行う**ことが望まれます。

d. 雇用の流動化を踏まえて追記された事項

雇用の流動化を踏まえた対策強化については、２つの観点から追記されています。１つは、従業員として勤務している間から、昇格・異動・新プロジェクト参加等の適時に、「秘密情報に対する認識向上」の対策を講じていくことです。また２つめは、退職時の対策を「接近の制御」「持出し困難化」「視認性の確保」「秘密情報に対する認識向上」という４つの観点からさらに強化していくことです。

第３章　秘密情報の分類、情報漏えい対策の選択及びそのルール化
３－２　分類に応じた情報漏えい対策の選択
【５つの「対策の目的」】
（１）接近の制御
・・・
また、今後、さらに普及・常態化する**テレワークにおいては**、・・・**雇用関係の終了や契約の終了に伴い速やかなテレワークでのアクセス権限の削除**が望まれます。
・・・
（４）秘密情報に対する認識向上（不正行為者の言い逃れの排除）
・・・
また、企業と退職予定の従業員との関係によっては、**退職予定者が秘密保持誓約書の提出を拒否することがあり得ることから、退職時だけでなく、入社時や配属先の異動時、重要プロジェクトへの配属時・転出時・終了時にも、秘密保持契約を取り交わす**ことが秘密情報に対する認識向上のための対策として有効であると考えられます※a。

３－４　具体的な情報漏えい対策例
・・・
（１）従業員に向けた対策
④「秘密情報に対する認識向上（不正行為者の言い逃れの排除）」に資する対策
・・・
※aと同じ記載を追記
・・・
b. 秘密保持契約等（誓約書を含む）の締結　　（注）この部分は雇用の流動化を踏まえた追記・修正ではないが、退職時の対策に続く一連の備えを示しているため敢えて引用した
・・・
秘密保持契約等を締結するタイミングとしては、入社・採用時、**退職・契約終了時**、**在職中（部署の異動時、出向時、プロジェクト参加時、昇進時等の取り扱う情報の種類や範囲が大きく変更されるタイミング）**等が考えられます。入社時の契約では、秘密保持義務の対象となる情報の特定は難しい場合が多いですが、**在職中（特に、部署の異動時・出向時、プロジェクト参加時・終了時）、退職時には、対象となる情報の範囲の特定が徐々に容易になりますので、対象範囲をできる限り明確化した上で、秘密保持契約等を締結**します。なお、対象範囲の明確化については、単に特定の程度が高いほど良いということではなく、双方の認識が一致する程度に特定されているか否かがポイントとなります。

d. 雇用の流動化を踏まえて追記された事項

（続き）

３－４　具体的な情報漏えい対策例

・・・

（２）退職者等に向けた対策

（退職者等とは）

・・・

退職者等は、元々は従業員等であることから、退職予定者等に対しては、従業員等に向けた対策を、必要に応じて一部の対策を強化しつつ実施し、実際に退職した後については、**転職先等での行動（営業や研究開発などの活動状況）や転職先の企業の動向（商品販売の状況、研究開発の動向）を把握するといった特有の対策を実施**することが考えられます。
また、退職者との関係も常に円満な形での退職となるわけではなく、**退職に際して秘密保持義務契約等の締結を拒否されるような事態に備えて、日頃から技術的・物理的な対策、通常時からの秘密保持契約書の締結等を組み合わせて備えておくことが重要**と考えられます。

②「持出し困難化」に資する対策

・・・

また、**退職した従業員等が海外において秘密情報を不正に開示・使用するような事態に備えて**、退職前の事前対策を十分に講じることが必要です。例えば、**秘密情報を安易に海外に持ち出さないように警告するとともに、技術的・物理的な情報漏えい対策をしっかりと講じる**ことが考えられます。

③「視認性の確保」に資する対策

・・・

また、**退職者については、可能な範囲で転職先での行動（営業や研究開発などの活動状況）や転職先の企業の動向（商品販売の状況、研究開発の動向）等を把握**するような対策を講ずることが考えられます。

④「秘密情報に対する認識向上（不正行為者の言い逃れの排除）」に資する対策

・・・

また、退職者との関係も、常に円満な形での退職となるわけではなく、**退職に際して秘密保持義務契約等の締結を拒否されるような事態に備えて、日頃からその他の対策（技術的・物理的な対策、通常時からの秘密保持契約書の締結等）とあわせて備えておくことが重要**と考えられます。

e. サプライチェーン間での情報開示・共有の範囲拡大に伴う対策について

サプライチェーン間での情報開示・共有の範囲拡大については、秘密情報の分類においてその対象となる情報であるかを考慮すべきであることが追記されています。また、取引先に対する「a.接近の制御」の対策として、サプライチェーン間での情報開示・共有を制限すべき情報であるかの判断が重要であることが追記されました。

第３章　秘密情報の分類、情報漏えい対策の選択及びそのルール化
３－１　秘密情報の分類
（分類にあたっての考え方）
・・・
一方で、同程度の評価の秘密情報であっても、以下のような「情報の利用態様」に応じて、異なる対策を講ずる場合もあります。
※**「情報の利用態様」は**予め定められたものではなく、自社の事業規模や業種、**取り扱う情報の内容・性質等を踏まえた上で**、**望ましい「情報の利用態様」とは何かを自主的に判断することが重要**です。
例えば、**その秘密情報は**、「従業員各々に個別に資料を所持させるべきものなのか、共有資料のみとするのか」や、「ネットワークに接続されたＰＣ、クラウドなどの外部サービス等に保管すべき情報か否か」、「テレワークなど社外からのアクセスや個人所有のデバイスを用いたアクセスに際して使用を認めるべき情報か否か」、**「サプライチェーンで共有する必要がある情報か否か」**といったこと**を今一度検討してみることが有効です**。

３－４　具体的な情報漏えい対策例
（３）取引先に向けた対策
①「接近の制御」に資する対策
b. 取引先での秘密情報の取扱者の限定
・・・
サプライチェーン間での秘密情報の受け渡しの機会が増えていることから、**秘密情報の受け渡しに関しては、重要度に合わせた組織内部での管理・取扱いの手順を定めるとともに、委託先等の取引先の関係者にこれを遵守させる必要**があります。**対策が脆弱な取引先**から秘密情報が漏えいしないように、その対策状況を踏まえて**提供する秘密情報の範囲を制限する、委託その他の契約時に合意した基準・規定に基づいて提供先（取引先）における遵守状況を監査できるようにするといったサプライチェーン対策を講じることが重要**です。

f. 重要情報の多様化（技術情報、限定提供データ、機微情報）

重要情報として、個人情報に留まらず、重要な技術情報、限定して提供／受領されDXで利活用される重要データ、機微情報（外為法）等の多様な企業情報が、漏えいからの保護対象としてクローズアップされるようになりました。ハンドブックでは、これに対する注意喚起として、目的や秘密情報の決定において、その留意点を追記しています。

第1章　目的及び全体構成
１－１　目的及び留意点
（秘密情報の管理の効用）
・・・
○**企業にとって管理が必要とされる情報の種類も**、企業の競争力の源泉として、法的保護を受ける前提として適切な管理が必要とされているものの管理の要否・内容について保有企業の判断に委ねられている**営業秘密や限定提供データ（不正競争防止法）のほか**、**法律により保有企業に一定の管理が必要とされる個人情報**（個人情報保護法）や**安全保障貿易管理に関する技術情報（外為法）など多様化してきています**。・・・

第2章　保有する情報の把握・評価、秘密情報の決定
２－２　秘密情報の決定
（１）秘密情報の決定に当たって考慮すべき観点のイメージ
①営業情報
・・・
その漏えいにより、法令違反や他社との契約違反等となり、自社の社会的信用の低下を招いたり、**他社との信頼関係を毀損させる情報か**否か
（顧客の個人情報、**受託やライセンス等の他社との契約等により限定的に開示された**営業情報・**限定提供データ** 等）
②技術情報
・・・
その漏えいにより、法令違反や他社との契約違反等となり、**当該他社との信頼関係を毀損させる情報か**否か
（**受託やライセンス等の他社との契約等により限定的に開示された**技術情報、**安全保障貿易管理に関わる製品に関する技術情報** 等）

・・・

g. 国家の競争力維持への認識の高まりへの言及について

経済安全保障は、国家の競争力維持において民間企業の役割も重要であることを、改めて明確化したものと捉えることもできます。
日本企業が保有する秘密情報が外国から狙われるリスクをしっかりと意識するとともに、典型的な手口への対策強化が求められていることは、既に本資料で詳説したとおりです（スライド16～19参照）。

第1章　目的及び全体構成
１－１　目的及び留意点
（秘密情報の管理の効用）
・・・
・・・**先端的な技術情報については**、国内での競合企業による不正取得や退職者を通じた開示といった漏えい事案だけではなく、**海外の企業や政府機関の関係者からの巧妙な接触を通じた漏えい事案も発生**しており、競争力の維持の観点だけでなく、個々の企業の枠組みを超えた**経済安全保障の視点からも、企業が保有する秘密情報・重要情報の意図しない流出を防止することは、重要な課題**となってきています。

第３章　秘密情報の分類、情報漏えい対策の選択及びそのルール化
３－３　秘密情報の取扱方法等に関するルール化
コラム③　外国から狙われる企業の秘密情報
①サイバー攻撃による秘密情報の窃取！
②スパイとなる者を仕立てた秘密情報の窃取！
③通常の経済・学術活動に見せかけた秘密情報の窃取！

参考資料の改訂について

参考資料の改訂について

巻末の参考資料については、参考資料２、３、４、５に改訂が加えられています。

【参考資料２　各種契約書等の参考例】

- 取り上げている規定類（就業規則、秘密情報管理規定、秘密保持誓約書、各種契約書の秘密保持関連規定）について、相互の関係がわかるよう解説を追加
- 従来は、必須事項をひな形の本文に、選択的・任意的な事項を注記に記載していたが、利便性（そのまま使える）の観点から、秘密保持に関連する内容についてはひな形の本文に集約し、オプション的なものについてはその旨を注記して、利用者の選択で取り除けるように、構成を整理

  ※競合避止義務に関する規定、外部との関係（契約）における成果物の帰属については、これまでどおり注記のままとしている。

【参考資料３　各種窓口一覧】

- 所収の各種窓口の、取組みの内容、連絡先等の情報を更新

【参考資料４　秘密情報管理に関する各種ガイドライン等について】

- 「テレワークセキュリティガイドライン」（総務省）、「知財取引検討会報告書」（中小企業庁）、「技術認証管理制度」（経済産業省・産業競争力強化法）等を追加

【参考資料５　競業避止義務の有効性について】

- 営業秘密侵害事案（その中で競業避止義務について争点となっているものを含む）の収集・整理が行われているＩＰＡ「企業における営業秘密管理に関する実態調査」（令和３年公表）を紹介し、前回ハンドブックの公表以降の判例の状況についての情報を追加

出典：経済産業省知的財産政策室「「秘密情報の保護ハンドブック」の改訂（改訂方針と改訂ポイント）」（2022年3月）

本資料に関するお問い合わせ先

【お問合せ先】

株式会社NTTデータ経営研究所　エグゼクティブスペシャリスト　三笠武則（みかさたけのり）
（営業秘密保護推進研究会　事務局長）

E-mail: mikasat@nttdata-strategy.com　　TEL: 090-1459-0597