経済産業省

資料３－１

「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

経済産業省知的財産政策室

１．「秘密情報の保護ハンドブック」の改訂について

＜改訂の基本方針＞

- 平成２８年の策定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・追記する方針で編集。

□ 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

- ハンドブック策定後の進展、例えば、**「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年の個人情報保護法の改正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」**（「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）等）を反映。

□ 営業秘密・秘密情報をとりまく「環境の変化」に伴う修正

- **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。

□ 「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

- ハンドブックが対象とする「秘密情報」について、営業秘密のほか、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。
- 近年、特に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）。

等

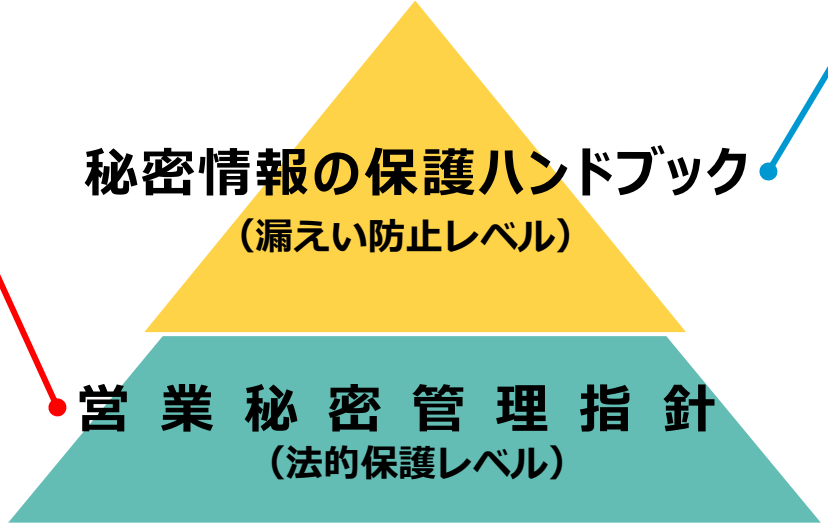
（参考）「秘密情報の保護ハンドブック」の位置づけ・「営業秘密管理指針」との関係

- 「営業秘密管理指針」は、不正競争防止法により「営業秘密」として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。　（平成１５年１月策定、２７年１月全面改定、３１年１月最終改訂）
- 「秘密情報の保護ハンドブック」は、企業が保有する「秘密情報」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推奨される包括的対策等を包括的に紹介するもの。（平成２８年２月策定）

営業秘密管理指針について

- 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**包括的に紹介するもの**として平成28年に作成。
- 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**。
- 簡易版**「秘密情報の保護ハンドブックのてびき」**も公表。

1章	・目的及び全体構成
2章	・保有する情報の把握・評価、秘密情報の決定
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
4章	・秘密情報の管理に係る社内体制のあり方
5章	・他社の秘密情報に係る紛争への備え
6章	・漏えい事案への対応
参考資料	・各種契約書・規程等の参考例、各種相談窓口等の連絡先、営業秘密侵害罪にかかる刑事訴訟手続、競業避止義務契約の有効性について　等を掲載

（追記参考例）①法制度の見直し・ガイドラインの改訂に伴う修正点の追記例

限定提供データの追記例

【第１章（1-1）】

（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

- 平成３０年には、付加価値の源泉となるデータの利活用を活発化し、安心してデータの提供・利用ができる環境を整備すべく不正競争防止法を改正し「限定提供データ」の制度が導入されました。令和４年●月に改訂した「限定提供データに関する指針」には、不正競争防止法における「限定提供データ」として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しています。
- 不正競争防止法に規定する「限定提供データ」と認められるためには、その情報が、①業として特定の者に提供する（限定提供性）、②電磁的方法により相当量蓄積され（相当蓄積性）、③電磁的方法により管理され（電磁的管理性）との３要件を満たす必要があります（ただし、オープンなデータと同一のもの、秘密として管理されているものは除外されます。）。
- 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。

各種ガイドライン追記例

【第３章（3-3）】

○ 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）」[14]、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。

【第３章（3-4）】

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。

○ なお、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」[43]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（脚注）】

[46] 特定個人情報の取扱いに関しては、『お役立ちツール（※中小企業向け特定個人情報の適正な取扱いに関するガイドライン（事業者編））』（特定個人情報保護委員会）~~ｐ４７以下~~において、中小規模事業者における対応方法等が記載されています。
（https://www.ppc.go.jp/personalinfo/legal/-
~~http://www.ppc.go.jp/files/pdf/261211guideline2.pdf~~）

（追記参考例）②営業秘密・秘密情報をとりまく「環境の変化」に伴う修正点の追記例

テレワークに関する追記例

【第３章（3－2）】

【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）持ち出し困難化

・・・・・・・

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。

（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

⋮

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。

技術の進展と新たな漏洩対策に関する追記例

【【第３章（3－2）】

【５つの「対策の目的」】

（１）接近の制御

・・・・・・・

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[12]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。

サプライチェーン間での情報の開示・共有に関する追記例

【【第３章（3－4）】

３－４　具体的な情報漏えい対策例

（３）取引先に向けた対策

○　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。

（追記参考例）③「重要な秘密情報の多様性」への考慮に係る啓発に関する追記例

秘密情報の外縁の明確化

【第１章（1－1）】

○　さらに、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。また、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２章（冒頭）】

・　また、企業が保有する情報の中には、特許権などの権利を取得することによって、法的保護の下で公開しつつ活用すべきものや、個人情報のように法令の規定に基づいて外部への漏えいは一切許してはならず厳格な管理が求められるものない、さらに営業秘密や限定提供データのように法律による保護を受けるために相応の管理措置が講じられているもののように、多様な情報がもあります。よって、自社が保有する情報のうち、どの情報を公開し、どの情報を秘密情報とするのか（あるいは、しなければならないのか）を、自らの意思を持って適切に判断して組み合わせ、収益の最大化を図っていく必要があります。↵

海外への情報漏えいに関するコラムの追加

【第３章（コラム③＜追加＞）】

近年、地政学上のリスクがクローズアップされ、国際的な産業競争も激しくなる中、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のです。↵

外国のスパイ活動といえば、国の機関を対象に行われるイメージがあるかもしれませんが、最近では企業や研究機関で働く人々にも及ぶようになっています。これを受け、米国や英国などでは、普段は公に発信することの少ない防諜・治安機関が、積極的に企業等に対する情報提供活動（アウトリーチ活動）を展開し、企業等における秘密情報の保護の取組に貢献しています。日本でも、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し、対策に役立ててもらうためのアウトリーチ活動が警察において積極的に進められています。↵

↵

外国から企業等の秘密情報が狙われるリスクのパターンについて、警察などが把握した事例を基に大まかに分類すると、以下のとおり整理することができます。↵

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↵

↵

企業等の秘密情報を確実に守るためには、「自社には狙われるような情報はない」と考えず、想定される様々なリスクを認識し、これに応じた具体的な対策を講じることが必要となります。以下に掲げたそれぞれのリスクの内容と留意すべき点をまずはしっかりと認識し、本書で掲げた具体的対策（３－４参照）を講じる際の参考としてください。↵

・・・以下、①～③の具体的な事例と対策、インシデント発生時の対処等について解説。

２．「秘密情報の保護ハンドブック」の主な改訂内容　～巻末・参考資料の修正～

＜改訂の基本方針＞

- 関連情報・参考情報として、巻末に「参考資料」が添付されているところ、以下のとおり整理・拡充。

□ 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

（参考）
「秘密情報の保護ハンドブック」の改訂箇所一覧

（参考）秘密情報の保護ハンドブックの改訂内容

章	節	項目	主な改訂内容
はじめに	―	―	■ テレワークの普及、働き方の多様化・柔軟化と、それに伴う企業外部からの情報利用・アクセスの常態化など、情報管理・利用の在り方の変容について追加 ■ 秘密情報・重要情報に対する（特に海外からの巧妙な接触を通じた）漏えい事案の発生、事例に基づく対策等の紹介（コラム欄の追加）について追加 ■ 不競法平成30年改正「限定提供データ」の導入について追加 ■ 企業が管理・保有する、秘密情報・重要情報について、営業秘密以外にも、個人情報保護法、外為法の対象となる情報など多様であることを追加
第１章 目的及び全体構成	1-1 目的及び留意点等	―	**（本書の目的）** ■ 情報の価値と漏えいリスクについて、「企業価値・競争力の源泉とその既存」でである点を追記 **（本書と営業秘密管理指針との関係）** ■ （参考）として限定提供データ・指針と本ハンドブックとの関係について追加 **（秘密情報の管理の効用）** ■ 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について追加 ■ 情報管理の背景として競争力の維持の他、経済安全保障の視点も加わりつつあること、企業が管理すべき情報が多様化・多義化していること、海外への情報漏えい事案に伴う懸念を追加 ■ 情報漏えいのリスクへの対応について、法令遵守（情報の管理義務と企業価値の維持・向上）の観点から積極的な対応が望まれる旨を追記
	1-2 本書の全体構成	―	―
	1-3 本書の使い方	―	■ 秘密情報の管理について、できる範囲に絞り込んでの着手が有効といえる場合もあること、その際は措置されない部分のリスクを把握し、そのリスクを受容できるものかどうかも分析しておく必要があることを追加
第２章 保有する情報の把握・評価、秘密情報の決定	冒頭（枠囲み）	―	■ 企業が保有し、管理が必要な情報の種類の多様化と具体例について追記 ■ 保有情報を把握する際には、「不要情報」（保有権限を失った情報、保有意義が不明瞭な情報等）が残っていないかの洗い出しと、消去・廃棄が必要であることを追加
	2-1 企業が保有する情報の評価	(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）** ■ 情報の存在形態（クラウド等に記録されたデータ）、非製造業における現物での営業秘密の例（Ｆ１系統の親品種）を追記 ■ 保有情報を把握する際には、「不要情報」（保有権限を失った情報、保有意義が不明瞭な情報等）が残っていないかの洗い出しと、消去・廃棄が必要であることを追加
		(2) 保有する情報の評価	**【評価に当たって考慮すべき観点の例】** ■ 情報管理の評価指標の例として、「秘密管理の必要性・程度」を追記 ■ 情報管理の意義として、「企業価値・競争力の向上」を追記
	2-2 秘密情報の決定	冒頭	■ 限定提供データに対する、本書の利用可能性（情報の管理面での有用性）について追加 ■ Society5.0におけるデータ利活用機会の増加と情報管理・漏えい対策の意義について追加
		(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	■ 契約に基づき限定的に開示された情報の例として、限定提供データを追加 ■ 漏えいが法令違反になる情報の例として、安全保障貿易に関わる技術・製品に関する情報を追加

章	節	項目	主な改訂内容
第３章 秘密情報の分類、情報漏えい対策の選択及びのルール化	冒頭（枠囲み）	–	■ 情報管理の対策の選択判断の指標の例として、「秘密管理の必要性・程度」を追記
	3-1秘密情報の分類	–	（分類の必要性） ■ 軽微な修正（趣旨の明確化のための追記）
			（分類に当たっての考え方） ■ 情報の分類・評価において、クラウドなど外部サービスの利用、テレワークにおける個人デバイス・外部サービスの使用、サプライチェーンでの情報共有といった点の考慮が必要である旨を追加 ■ 他社から受領した秘密保持義務を負っている情報の例（営業秘密、限定提供データ、その他の情報）について追記
	3-2 分類に応じた情報漏えい対策の選択	–	【冒頭】 ■ テレワークの導入、個人端末の利用について追記 【５つの対策の目的】 (1)接近の制御 ■ アクセス権限管理の粒度を細かくするためのアクセス管理基盤整備や、雇用終了時等にテレワークのための権限を削除を追加 (2)持出し困難化 ■ テレワークやオンライン会議でのアクセス（投影）制限、許可の無いオンラインストレージの利用制限を追加 ■ テレワークにおける持ち出し困難化の観点からの留意点について追記 (3)視認性の確保 ■ 視認性の向上に向けて「高度なモニタリングシステムの適用」、「セキュリティコントロールレベルを維持する努力（ＥＤＲの導入など）」が重要である点を追加 ■ 従業員へのモニタリングの目的が、従業員保護であることを周知徹底するとともに人権・個人情報保護に係るコンプライアンスの確保の必要性について追記 ■ 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・操作ログの確認への言及を追加 (4)秘密情報に対する認識向上 ■ 退職予定者が秘密保持契約や誓約書の提出を拒否したときの対策について追加 (5)信頼関係の維持・向上等 ■ テレワーク中のコミュニケーションの改善（相談等口の設置等）を追加
	3-3 秘密情報の取扱い方法等に関するルール	(1) ルール化の必要性とその方法	■ テレワーク中に従業員が遵守するルールを定めることが必要である旨を追加
		(2) 秘密情報の取扱い等に関する社内規程の策定	■ 企業の外で情報を扱うテレワークの実施により漏えいリスクが高まるので、セキュリティ対策が必要である旨及び参考資料（有益情報）の紹介に関する記載を追加 ■ 「テレワーク等企業の組織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具体例」を追加

章	節	項目	主な改訂内容
第３章 秘密情報の分類、情報漏えい対策の選択及びのルール化	3-3 秘密情報の取扱い方法等に関するルール	コラム③　外国から狙われる企業の秘密情報　＜新規＞	■「外国から狙われる企業の秘密情報」を追加し、外国から企業等の秘密情報が狙われるリスクのパターンや具体的な事例とともに、リスク低減のための措置と対策の留意点を紹介
	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** ■　（冒頭）テレワークにおける権限設定の細かい制御、契約終了に伴う権限の早期削除について追加 ■ a. アクセス権の設定の最小化と、テレワークでの細かい単位での制御の必要性、これを可能にするアクセス権限管理基盤の整備について追記 ■ b. 情報システム管理者の意義とともに不正・事故防止のための複数人チェックの必要性を追記 **②「持出し困難化」に資する対策** ■　（冒頭）対策の目的を具体化・追記し、テレワーク、オンライン会議での注意点を追加 ■ a. h. テレワーク、オンライン会議での資料表示（共有）における留意点をへの言及を追加 ■ e. 許可されていないソフトウエア、ストレージのインストール・利用の禁止について追加 ■ h. 無線LAN・テザリングの利用制限を通じた情報の持ち出し・漏えい困難化について追加 ■ j. ＶＰＮの利用、ＥＤＲの導入等によるテレワーク中の持ち出し困難化を追加 ■ k. 秘密保持契約の締結の重要性を追記 **③「視認性の確保」に資する対策** ■　（冒頭）AI 等の最新技術を組み入れた内部不正モニタリングシステム活用の有効性、モニタリングの目的が従業員保護であることの周知を徹底する点を追加 ■　（冒頭）テレワークにおける履歴の記録やクラウドサービスログイン時の認証・操作ログの確認の視認性の確保への有効性について追加 ■ o. ログの収集・記録における利用者のプライバシー保護の必要性、従業員への配慮について追記 ■ o. 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（EDR の導入・クラウドプロキシの適用等）を追加 **④「秘密情報に対する認識の向上」に資する対策** ■　（冒頭）プロジェクト配属時・転出時・終了時の秘密保持契約締結の重要性について追加 **⑤「信頼関係の維持・向上等」に資する対策** ■　（冒頭）テレワーク中のコミュニケーション面での支援・体制整備等の必要性について追加 ■ d. テレワーク中のコミュニケーションの改善について追加

章	節	項目	主な改訂内容
第３章 秘密情報の分類、情報漏えい対策の選択及びのルール化	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	（退職者とは） ■ 対策における留意点、秘密保持義務契約の締結が困難な場合への対応の必要について追記・追加し、営業秘密漏えいルートに関する令和２年度IPA調査結果（中途退職者による漏えいが４割超）を追加 ①「接近の制御」に資する対策 ■ a. 雇用終了時等にテレワークのための権限を削除する旨を追記 ②「持出し困難化」に資する対策 ■ （冒頭）退職従業員による情報の海外漏えいを防ぐために、秘密情報を安易に海外に持ち出さないように警告すること、技術的・物理的な情報漏えい対策との併用の重要性を追加 ③「視認性の確保」に資する対策 ■ （冒頭）退職者に対する対策の具体例を追記 ■ o. モニタリングシステムの導入において、モニタリングの目的が従業員の保護にあり、周知徹底・十分な理解を得た上で適切な運用が必要である点を追加 ■ q. 退職予定者が退職に際して重要情報を持ち出さないように、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より高度な確認を行うことを追加 ④「秘密情報に対する認識向上」に資する対策 ■ （冒頭）退職者との間で秘密保持義務契約の締結が困難な場合への対応の必要性について追加 ⑤「信頼関係の維持・向上等」に資する対策 ■ なし
		(3) 取引先に向けた対策	①「接近の制御」に資する対策 ■ a. オンライン会議における留意点の具体例（発表情報の画面共有）を追加 ■ b. サプライチェーン対策の観点から取引先に対する開示情報の制限の重要性を追加 ②「持出し困難化」に資する対策 ■ a. 軽微修正 ③「視認性の確保」に資する対策 ■ なし ④「秘密情報の認識向上」に資する対策 ■ なし ⑤「信頼関係の維持・向上等」に資する対策 ■ c. 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・支援の実施等（下請企業振興法に基づく「振興基準」）を追加
		(4) 外部者に向けた対策	■ なし
		コラム	■ 軽微修正（コラム番号の繰り下げ修正）

章	節	項目	■ 主な改訂内容
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）** ■ テレワークに対応した相談窓口の設置・外部専門家によるメンタルヘルスケア支援秘密情報の管理の効用（法律の定める管理義務の具備及び企業価値の向上）、責任者と責任部署を中心とした一元的な体制構築について追記 **（事業規模が大きな企業における社内体制の構築）** ■ 社内の各部門・担当者の参画・協力を一元的に統括する組織と責任者の設置について追記
	4-2 各部門の役割分担の例	–	**（冒頭枠内）** ■ 内部不正対策の体制における各部門の役割を追加（法務担当：データ利活用型ビジネスを進める際の契約等の検討、人事・労務担当：従業員のメンタルヘルスケア支援等、情報システム担当：不正アクセス対策・不正検知技術等の導入検討・運用、知財担当：データ利活用型ビジネスを進める際の助言等）
		コラム⑥　技術情報管理認証制度について　＜新規＞	■ 平成３０年９月から運用が開始した産業競争力強化法に基づく「技術情報管理認証制度」についての概要、制度のメリット等を紹介
第５章 他社の秘密情報に係る紛争への備え	冒頭（枠囲み）	–	■ 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２）についての記載（２７年法改正及び３０年政令改正の内容）を追記
	5-1 自社情報の独自性の立証	–	■ なし
	5-2 他社の秘密情報の意図しない侵害の防止	冒頭	■ 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２）についての記載（２７年法改正及び３０年政令改正の内容）を追記
		(1) 転職者の受入れ	■ なし
		(2) 共同・受託研究開発	■ なし
		(3) 取引の中での秘密情報の授受	■ なし
		(4) 技術情報・営業情報の売込み	■ なし
	5-3 営業秘密侵害品に係る紛争の未然防止	–	■ なし

章	節	項目	主な改訂内容
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	(1) 漏えいの兆候の把握	■ （冒頭）インシデントに速やかに対応できる体制・社内ルールのみならず、インシデント発生時の活用内容を事前に定め、訓練等で確認しておく必要性について追記 ■ ＡＩを組み入れたモニタリングシステムが提供する監視機能等（例：ふるまい解析）の有効性、モニタリングシステム活用時の従業員の人権・プライバシー保護に係るコンプライアンスの確保について追加
		(2) 漏えいの疑いの確認	■ テレワークにおける視認性確保のための各種のログの記録・保存の必要性を追加 ■ ＡＩを組み入れたモニタリングシステムが提供する監視機能等（例：ふるまい解析）の有効性、モニタリングシステム活用時の従業員の人権・プライバシー保護に係るコンプライアンスの確保について追加
	6-2 初動対応	(1) 社内調査・状況の正確な把握・原因究明	■ なし
		(2) 被害の検証	■ なし
		(3) 初動対応の観点	■ 故意の内部不正によって個人データが漏えいした場合の報告義務を追加（個人情報保護法改正内容の反映）
		(4) 初動対応の体制	■ なし
	6-3 責任追及	冒頭	■ 不競法の責任追及が可能な情報として「限定提供データ」を追記
		(1) 刑事的措置	■ 情報漏えいに係る罰則の例として、「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）を追記
		(2) 民事的措置	■ 民事手続の対象となる情報「限定提供データ」を追記 ■ 裁判公開原則の例外となる、民事裁判手続での当事者尋問の非公開について追加
		(3) 社内処分	■ なし
	6-4 証拠の保全・収集	(1) 証拠の保全	■ デジタル・フォレンジック活用時の留意点と、解析で開示する情報がインサイダー取引で悪用されない対策の必要性を追加
		(2) 証拠の収集	■ なし

章	節	項目	主な改訂内容
参考資料	1　情報漏えい対策一覧		■ 本編修正に合わせて形式的・軽微な修正
	2　各種契約書等の参考例		■ （冒頭）紹介している各種規程・誓約書等の全体像・相互の関係について、容易な把握を可能にすべく簡単な解説を追加 ■ 初めて契約業務に携わるケース等も想定し、各ひな形の前の導入を補足・追記 ■ 利用者の利便性を考慮し、これまで枠外で紹介されていたオプションとなる条項について、一部の例外（競業避止義務関係、権利の帰属関係）を除いて、各ひな形の中に取り込む形に整理（秘密保持義務と、これに関連する条項については網羅的に取り込み、利用者の判断で不要なものは適宜除外して活用してもらえるように整理）
	3　各種窓口一覧		■ 現在掲載している窓口については、引き続き掲載（時点修正など軽微な修正）
	4　秘密情報管理に関する各種ガイドライン等について		■ 現在掲載しているガイドライン等については、引き続き掲載・紹介予定（時点修正など軽微な修正） ■ このほか、冒頭に、「■テレワーク対応関係（各章横断）」の項目を追加し、総務省テレワークセキュリティガイドライン／中小企業担当者向けチェックリスト（令和３年５月）、「第５章（紛争への備え）関係」に、「中小企業庁知財取引検討会報告書（令和３年３月）、「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
	5　競業避止義務契約の有効性について		■ 前回ハンドブック改訂以降の営業秘密侵害事案（その中で、競業避止義務について争点となっているもの）の収集・整理が行われている、令和２年度にＩＰＡが実施した「企業における営業秘密管理に関する実態調査２０２０」について紹介
	6　営業秘密侵害罪に係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		■ なし