NTT DATA
Trusted Global Innovator

IPA「組織における内部不正防止ガイドライン」の改訂に係る調査等業務　概要説明資料

2022年4月6日

作成：株式会社エヌ・ティ・ティ・データ経営研究所

目次

はじめに

企業が保有する秘密情報の保護は、近年益々その重要性を増している。個人情報の保護はもとより、重要技術情報の保護に対する要請が強まり、保護目的の構造変革が進んでいる。

秘密情報の保護に関して、独立行政法人情報処理推進機構（以下、「IPA」）では、内部不正防止のために「組織における内部不正防止ガイドライン」（2013年初版、2017年第4版改訂）を公表、啓発を実施してきた。経済産業省でも、2016年に「秘密情報の保護ハンドブック」を公表、秘密情報の保護・管理に関する啓発を行っている。

「組織における内部不正防止ガイドライン」、「秘密情報の保護ハンドブック」ともに前回の改訂から時間が経過し、最近の社会環境・動向の変化や、セキュリティ関連技術の変遷に則した改訂が必要な状況になっている。改訂を踏まえた啓発の強化も急務であると言える。

今回、IPAの「組織における内部不正防止ガイドライン」の改訂を行うとともに、同ガイドラインと内容が不可分である「秘密情報の保護ハンドブック」の改訂に役立つ情報整理を実施した。
本資料ではその実施内容の概要について説明する。

エグゼクティブサマリー　～調査方法

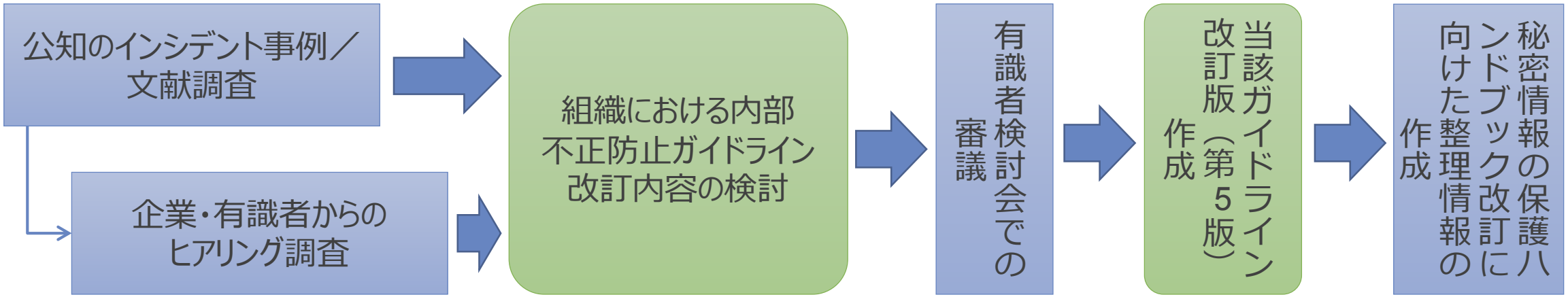
本調査・改訂の実施方法は以下の通り。

①まず文献／事例調査及びこれを受けたヒアリング調査を実施
②その結果を踏まえてIPA「組織における内部不正防止ガイドライン」の改訂内容を検討
③有識者検討会でこの改訂内容を議論した上で有識者等から得たご意見・コメントに基づいて修正
④ガイドライン改訂版（第5版）を作成

---

⑤修正内容を踏まえ、経済産業省「秘密情報の保護ハンドブック」の改訂に向けた整理情報を作成

【本調査・改訂の実施方法・プロセス】



エグゼクティブサマリー　～「組織における内部不正防止ガイドライン」改訂のポイント

今回の「組織における内部不正防止ガイドライン」では、国家戦略や事業／社会環境の変革、サイバーセキュリティ技術（攻撃・防御）の急速な進展を踏まえ、以下のポイントに沿い改訂した。

【IPA「組織における内部不正防止ガイドライン」改訂のポイント】　（注）「」内にガイドラインの見出しを示す。

1. **経営者に向けたメッセージを強化**
   - ●内部不正による営業秘密、とりわけ重要技術情報の漏えいが事業経営に及ぼすリスクが増大していることへの危機感を提示・警告（「１．　背景」、「4-1 基本方針」等）
   - ●最近の法改正に伴う重要な注意点について注意喚起（「３．　用語の定義と関連する法律」）
2. **テレワークに代表される働き方改革の広がりと常態化によって増大するリスクを低減できる対策を追記・増補**
   - ●社外における秘密情報の取扱増加に伴い必要となる人的・技術的・組織的対策の増補・強化（「4-4 技術・運用管理」、「4-5 原因究明と証拠確保」、「4-6 人的管理」、「4-8 職場管理」、「4-10 組織の管理」等）
3. **雇用の流動化による退職者増加がもたらすリスクを低減できる対策を追記**
   - ●人的管理の強化（「4-6 人的管理」等）
4. **セキュリティ技術の急速な進展と個人情報に配慮した運用の在り方**
   （「4-4 技術・運用管理」、「4-6 人的管理」等）
5. **重要な法改正に伴う必要な対策の増補・強化**
   （「4-1 基本方針」、「4-4 技術・運用管理」等）

１．文献調査

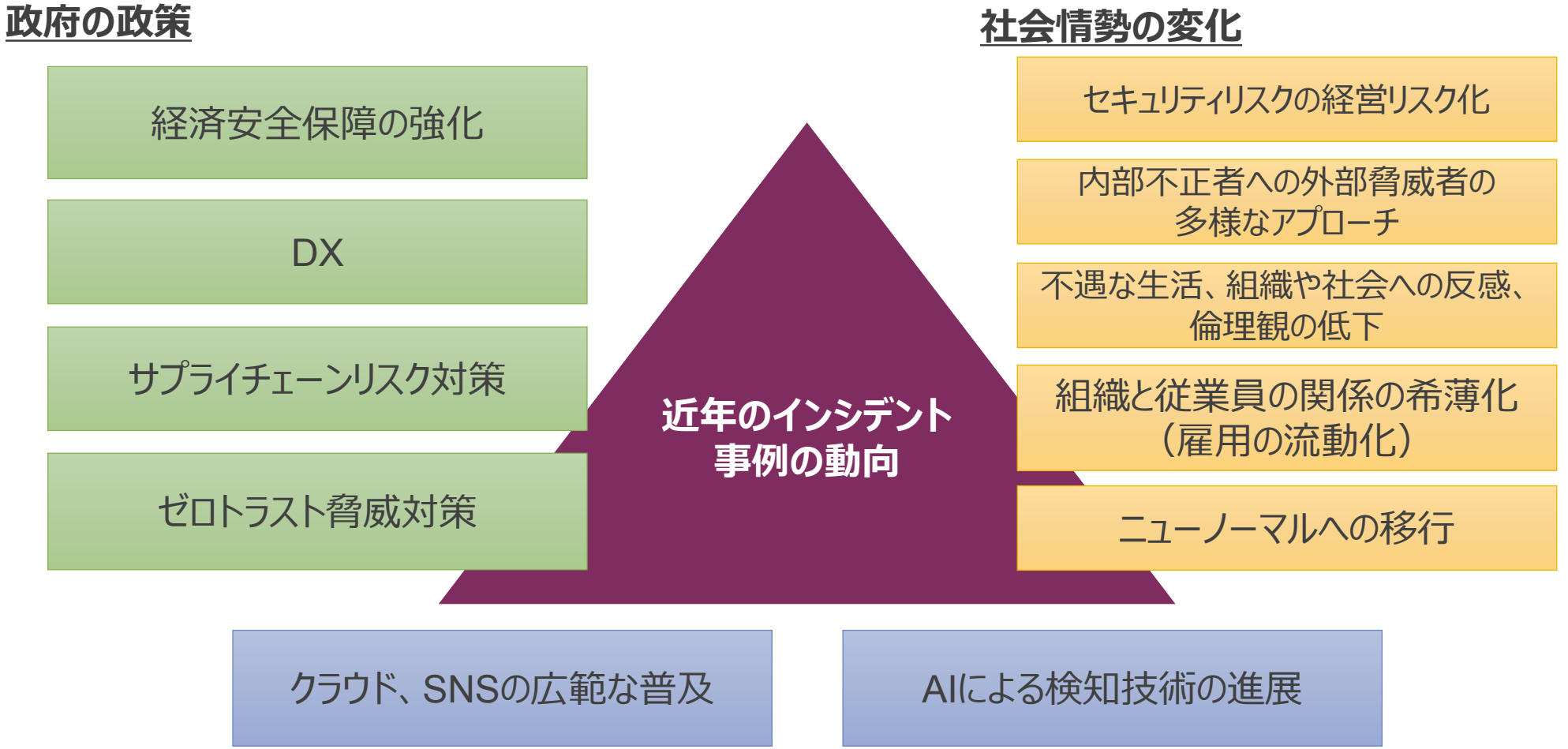
1．文献調査

国内外における直近の**内部不正によるインシデント事例の事実関係**、
文献に記載された**対策／ベストプラクティス**等から、新たに求められる対策の在り方を抽出して検討。

	調査種類	調査概要
文献調査	インシデント事例調査	• 国内・海外の内部不正によるインシデント事例調査
	国内外の文献調査	• 内部不正対策、及び秘密情報の保護や管理に関する国内や海外の文献調査
	関連法令、Q&A集等の調査	• NISCサイバーセキュリティ関連法令Q&Aハンドブックの調査

1-1. インシデント事例調査

ITに係る政府の政策、社会情勢の変化、サービス・技術の進歩などを現在着目すべき**３つの環境条件**として捉え、これらと相関する事例を抽出、ガイドラインの事例集に追加。



1-1. インシデント事例調査

公知情報に基づくインシデント事例調査の結果、抽出した事例を以下に示す。

#	事件の概要
1	電子製品を製造する企業において、元社員が、企業の産業用ロボットの設計図や生産ラインのレイアウト図などの営業秘密データ59件を不正にハードディスクに複製していた事例
2	大手総合製造メーカーにおいて、元社員が、企業のタッチセンサー技術の情報を不正に私用のハードディスクに複製し、競合企業の従業員にデータの画像を送信していた事例
3	大手靴製造メーカーにおいて、元社員が、同社が開発した靴の画像や性能データを含む約3万6000点の営業秘密情報を社員用メールに添付し、個人用アドレスへ送信した事例
4	精密部品製造メーカーにおいて、社員（中国籍）が、同社のサーバーに不正アクセスを実行。サーバー内から製品のドリルなどの同社製品の設計情報やマニュアルなどを自身のUSBメモリーに転送した事例
5	複数の小売電気事業者の委託先などが、顧客になりすまして他社のウェブサイト上から既契約関連情報を取得し、不正な申し込みや営業に利用していた事例
6	某市役所において、関係ない職員が人事課が管理するデータを不正に閲覧し、自身のパソコンに保存していた事例
7	某市立幼稚園の元職員が業務以外の目的で保護者の連絡先を入手し、メールを送信していた事例
8	某大規模公的病院において、事務職の職員が同機構の患者情報約14万人分の個人情報が保存されたパソコンを持ち出し、職員家族が廃棄事業者に処分を依頼し、同事業者よりパソコンを買い取った人物がインターネットオークションに出品した事例
9	大手インターネット証券会社において、システム開発や運用を委託した会社の従業員が顧客情報を不正に取得し、約2億円の顧客資産を売却して現金を引き出していた事例
１０	某国立大学において、元職員がウェブシステムのマニュアルとともに機密情報である助成事業の申請情報を外部に持ち出し、転職先である他大学のウェブサーバに流出した事例
１１	某県立小学校教職員が、保護者の個人情報を私的に利用し、保護者に精神的苦痛を与えた事例
１２	某市役所において、総務部人事課の職員が当時所属していた教育委員会のパソコンから同市の職員2747人分の個人情報含むファイルを入手し、外部に流出させた事例
１３	国立大学の著名な某研究所において、非常勤職員が教授宛てのメールを盗み見たり、機密文書をスキャンして持ち出したほか、教授室を盗撮した事例
１４	某市民病院にて、職員が、不正に電子カルテを閲覧し、患者情報を取得していた事例
１５	トレーディングカードゲームを扱う大手通信販売サイトを運営する企業において、従業員が、Twitter上に顧客情報を書き込んでいた事例
１６	某市の市議が、当選前の職員当時に個人情報を持ち出し、自身の選挙活動に利用した事例
１７	某地方銀行の元職員が同行をすでに退職済みだった知人へ顧客情報を不正に提供した事例
１８	某大手樹脂加工メーカーにおいて、当時社員だった男性が中国企業に営業秘密にあたる技術情報を漏えいした事例

1-1. インシデント事例調査

公知情報に基づくインシデント事例調査の結果、抽出した事例を以下に示す。

#	事件の概要
１９	大手モバイルキャリア企業に勤務していた男性が、在籍期間中に5Gなどの技術情報を持ち出し、転職先の他のモバイルキャリア企業に漏えいした事例
２０	大手マンション管理企業の元従業員が、社内システムに保存していた顧客の個人情報約5000件を不正に外部の法人へ持ち出した事例
２１	大手新興IT企業に勤務していた元従業員が8名分の顧客情報を不正に持ち出し、うち6名分についてカードローンに申し込んだ事例
２２	金融機関を中心とした法人顧客275社に関する上場投資信託の取引内容などが、同社従業員を通じて他の証券会社に漏洩していた事例
２３	2020年3月初旬に解雇された医療機器包装会社の元従業員が偽のユーザーアカウントを使用して、約115,581件の記録を編集し、約2,371件の記録を削除した事例
２４	グローバル大手重電メーカーでの長期間にわたる従業員による貴重な独占的データと企業秘密の窃取が、2020年7月に発覚した事例
２５	大手ITソリューション企業による2億5000万人の顧客記録が、14年間にわたってパスワード保護なしにオンライン上で誰でもアクセスできる状態となっていた事例
２６	コロナ禍の発生以来、フィッシング攻撃とスピアフィッシング攻撃が急増していた事例
２７	2020年7月、大手SNSのIT管理者になりすまして在宅勤務の主要な管理者ににせの電話をかけ、一部の従業員を巧みにだましてアカウントの資格情報を開示させ、約130の著名なアカウントのパスワードを変更し、それらを使用してビットコイン詐欺を実行した事例
２８	グローバル大手通信機器メーカーの元従業員が会社のクラウドインフラストラクチャに不正アクセスし、悪意のあるコードを展開して、シスコのWebExアプリケーションで使用されている456台の仮想マシンを削除した事例
２９	グローバル大手飲料メーカーの従業員による人的資源の記録を含むハードドライブの盗難により、約8,000人の従業員にデータ侵害通知書を発行することを余儀なくされた事例
３０	2020年10月末、不特定多数の大手ECサイトの顧客に、自身の名前とメールアドレスが “同ECサイトの従業員によって第三者に開示された ”という内容のメールが届いた事例
３１	2020年9月、ネバダ州の裁判所がロシア国籍の容疑者をコンピューターに意図的に損害を与えた共謀罪で起訴した事例
３２	2018年、大手新興自動車メーカーの不満を持つ従業員がデータを盗み出した事例
３３	2018年、ある男性が100GBの顧客データを元雇用者の競合他社に4,000ドルのバーゲン価格で売ろうとしていて、ウクライナの警察が摘発した事例
３４	人事部の誰かが誤って上級幹部のチームにメールを送信したことで、某国の国民保健サービスの従業員24人の個人情報が流出した事例
３５	某国国民保健サービスのコロナウイルス感染者追跡アプリの詳細（個々人のコロナウイルスの健康状態及び正確な位置データ）が、誰でも閲覧できる状態でGoogle Driveに保存され、流出した事例
３６	2019年、大手金融機関が使用していたグローバル大手クラウドサービスの元ソフトウェアエンジニアが、誤って構成されたWebアプリケーションファイアウォールを悪用し、1億件を超える顧客のアカウントとクレジットカード情報に不正にアクセスした事例

1-1. インシデント事例調査

公知情報に基づくインシデント事例調査の結果、抽出した事例を以下に示す。

#	事件の概要
３７	2020年1月、グローバル大手ホテルグループが顧客サービスを提供するために使用していた第三者のアプリケーションをハッカーが悪用し、520万件の記録にアクセスされた事例
３８	大手IT機器リース会社とのリース契約終了後に回収されたサーバのハードディスクが、同社が消去を委託していた会社の従業員によってインターネット上で売却された事例
３９	某地方銀行において、従業員が顧客の求めに応じて別の顧客の情報を提供していた事例
４０	国営放送において、受信料収納業務の委託先から受信契約者の個人情報が漏洩し、委託先社長自らキャッシュカードをだまし取る窃盗事件に関与した事例
４１	某大手セキュリティ製品メーカーにおいて、従業員が同社内の顧客サポートのデータベースに不正アクセスして情報を入手して第三者に提供、第三者は入手した情報を悪用してサポート詐欺犯罪を行っていた事例
４２	某電子部品メーカーにおいて、会計システムの更新を委託していたITサービス大手の再委託先である同社中国法人の社員が、約7万2000件の情報を不正に取得していた事例
４３	風力タービン会社のエンジニアが重要な知的財産を盗み、競合他社である中国企業に転職した事例
４４	大手インターネットサービス企業の自動運転車プロジェクトに関わっていたエンジニアが同社から営業秘密を盗んだ事例
４５	2018年4月、某銀行の従業員が顧客の連絡先リストを盗み、150万人もの顧客の口座が侵害された事例
４６	某有力州立大学でGoogle ClassroomのサイトとZoomミーティングのパスワードが公開された事例
４７	某有名大学のオリジナルのコロナ・ワールド・マップをコピーしユーザー名、パスワード、クレジットカード番号などの重要な情報を盗み出すように設計され、地図をナビゲートしようとすると、AZORultと呼ばれるマルウェアが起動し、情報が漏えいした事例
４８	攻撃者が某大学病院を攻撃し30台のサーバを感染させ、これにより同病院のITシステムはクラッシュし、緊急治療を必要とする患者が20マイル離れた別の病院に転送された事例
４９	1973年に大手防衛・宇宙産業企業に入社し、1996年に他の大手防衛・宇宙産業企業に買収されるまで防衛・宇宙部門に在籍していた社員が、スペースシャトル計画およびデルタIVロケットに関する情報を含むアクセス制限された技術および同社の企業秘密を盗み、国外に漏えいさせた事例
５０	中国国家安全部の工作員が、経済スパイ行為を共謀・企図し、米国の複数の航空・宇宙関連企業から企業秘密を盗んだ事例
５１	元政府機関職員が、某国のミサイルシステムの極秘情報を含む電子メールを8人に送信し、「敵対的」な外国の国々とも共有した事例
５２	某国運輸局が、別の某国にある大手ITサービス企業のクラウドサービス上に保存した機密情報が漏えいした事例
５３	病院施設において、夜間勤務の元警備員が、暖房・換気・空調（HVAC）用のコンピュータや、すべてのコンピュータに接続され医療記録や患者の請求情報などが保存されているナースステーションのコンピュータに不正にアクセスし、パスワードクラッキングプログラムやボットネットなどで攻撃した事例

1-1. インシデント事例調査

公知情報に基づくインシデント事例調査の結果、抽出した事例を以下に示す。

#	事件の概要
５４	簿記係であった元社員が個人的な費用を支払うために会社の口座から70枚以上の小切手を振り出し、約20万ドルを横領した事例
５５	元社員が、辞める前の4ヶ月間に、会社のサーバーにアクセスし、営業秘密を含む15,000以上のPDFファイルと20,000以上の抄録にアクセスしダウンロードした事例
５６	政府機関においてソフトウェアエンジニアであった元職員が、退職前にソースコードをリムーバブルメディアにコピーし、退職時に提出した自分のノートパソコンからソースコードを削除した事例
５７	海運・倉庫業の大手企業において、元役員が、自分の部署への請求書の金額を膨らませ、支払いの一部を回収していた事例
５８	製造会社の営業担当であった元社員が会社への不満から競合他社へ転職し、転職元会社の顧客記録を持ち出した事例
５９	住宅ローン会社の元契約社員が会社への不満から、サーバー上のバックアップデータを含むすべてのデータを消去するように設計されたスクリプトを仕掛けた事例
６０	業績不振を理由に解雇された元契約社員が元勤務先のユーザーアカウントにリモートアクセスし、約130万ドル相当の企業秘密が保存されている13のシステムにアクセスしていた事例
６１	企業が元社員のアクセス権を剥奪する前に、元社員が別のユーザーアカウントを作成するとともに、顧客のファイルを削除した事例
６２	大手通信会社において、ヘルプデスク技術者であった元社員が、会社から支給されたコンピュータにハッキングツールをインストールし、他の従業員の認証情報を盗み、外部の共犯者に渡した事例
６３	金融機関の元社員が、毎週日曜日に出勤し、2万件の住宅ローン申請者の記録をUSBフラッシュドライブにダウンロードし、販売していた事例
６４	自動車管理局において、元事務員と共謀者3名が、5年以上にわたり、移民に1,000件以上の不正な運転免許証を発行し、1件あたり800～1600ドルの報酬を得ていた事例
６５	小売企業において、ネットワークエンジニアとして勤務していた元社員が、解雇1か月後にIT部門に偽名のトークンの有効化を依頼、その後、元社員は、有効化されたトークンを使ってネットワークにアクセスし、仮想マシンの削除、SANの停止、メールボックスの削除などを行った事例
６６	投資銀行において、コンピュータのスペシャリストとして勤務していた元社員が会社への不満からリスク評価プログラムに取引のリスクを少しずつ増加させるようプログラムを改ざんした事例
６７	飲料メーカーにおいて、幹部のアシスタントとして勤務していた元社員が、外部の共犯者と共に企業秘密文書のコピーや秘密プロジェクトの1つに関する幹部の電子メールのコピーを印刷し、盗み出そうとした事例
６８	化学製造会社において、上級研究員として勤務していた元社員（在住外国人）が、退職を表明した翌月、化学物質の手順を詳細に記したMicrosoft Wordの文書を他企業の自身の電子メールアカウントに電子メールで送信した事例
６９	米国の電力会社において元社員が退職した夜、有効なままであった電子キーカードを使って、会社の安全な施設にアクセスし2人の上級管理職のコンピュータを使用して、900万ドルの着服を行った事例
７０	営業担当者であった元社員が会社への不満から、転職を上司に伏せた上で、1ヶ月間に亘り顧客の機密情報が閲覧可能となるネットワークにアクセスするためのパスワードや、自身が開発に携わったコンピュータプログラムの情報を含む100通以上の機密メールを自宅のコンピュータに転送した事例

1-1. インシデント事例調査

調査した事例のうち、以下を**「組織における内部不正防止ガイドライン」付録Ⅰ：内部不正事例集**に追加。

不正内容に着目したタグと概要		本ガイドラインの関連項目（旧番号）	元事例（事例一覧番号）
技術情報（営業秘密）の外部への漏えい	企業において、防衛・宇宙部門に在籍していた従業員が、防衛・宇宙関連の営業秘密にあたる技術情報を海外政府に提供した。 【主な原因】 従業員の出身国であった海外政府からのアプローチを受けた。	(17)情報システムにおけるログ・証跡の記録と保存	No49米防衛・宇宙産業企業の事件
個人情報の暴露	自治体において、職員が、所属していた部署から貸し出されたパソコンから同自治体職員の個人情報含むファイルを入手し、新聞社にファイル添付したメールを送信した。 【主な原因】 部署から貸し出されたパソコンの中に、個人情報を含むファイルがゴミ箱内に残されていた。待遇への不満や、自治体での情報管理についてマスコミに告発することで認められたいといった自己顕示的な発想があった。	(12)ネットワーク利用のための安全管理 (13)組織外部での業務における重要情報の保護	No12某市役所の事例
システム/プログラムの破壊	企業において、従業員が、退職前に開発中のシステムのソースコードを自分のノートパソコンから削除した。 【主な原因】 処遇に不満があった。変更管理プログラムマネージャーにソースコードを提出することを義務付けていなかった。	(4)格付け区分の適用とラベル付け (14)情報機器や記録媒体の持ち出しの保護 (17)情報システムにおけるログ・証跡の記録と保存 (20)雇用終了の際の人事手続き (21)雇用終了及び契約終了による情報資産等の返却 (24)公平な人事評価の整備	No56政府機関事例
営業秘密の持ち出し	企業において、従業員が、退職後に企業のシステム内の機密情報に不正アクセスしていた。 【主な原因】 業績不振を理由に解雇されることに不満があった。退職後に共有アカウントのパスワードが変更されていなかった。	(5)情報システムにおける利用者のアクセス管理 (7)情報システムにおける利用者の識別と認証 (20)雇用終了の際の人事手続き	No60事例

1-1. インシデント事例調査

不正内容に着目したタグと概要		本ガイドラインの関連項目（旧番号）	元事例（事例一覧番号）
システム/プログラムの改ざん	金融機関において、従業員が、債券売買のためのリスク評価プログラムの取引のリスクを少しずつ増加させるようプログラムを改ざんした。 【主な原因】 経営陣に不満を抱いていた。プログラミング実施者以外の者によるプログラム変更管理がなされていなかった。システムのベースラインやファイルのハッシュ値を比較するツールの定期的な使用がなされていなかった。	(17)情報システムにおけるログ・証跡の記録と保存	No66投資銀行事例
システム/プログラムの改ざん	企業において、従業員が会社から支給されたコンピュータにハッキングツールをインストールし、他の従業員の認証情報を盗み、外部の共犯者に渡した。共犯者は会社のWebサイトにその認証情報を用いて不正アクセスし、Webサイトを改ざんした。 【主な原因】会社から支給されたコンピュータにハッキングツールをインストールすることが可能であった。	(12)ネットワーク利用のための安全管理	No62大手通信会社事例
顧客情報（営業秘密）・個人情報の持ち出し	企業において、共同開発先として委託した自社の海外現地法人の従業員が業務用パソコンへ取引先情報および個人情報を含むデータを許可なくダウンロードし、海外のクラウドストレージサービスの個人アカウントへアップロードした。 【主な原因】 海外現地法人の従業員に対する教育による内部不正対策の周知徹底が十分でなかった。	(16)業務委託時の確認 (27)事後対策に求められる体制の整備	No42某大手電子部品メーカーから中国再委託に情報が漏えいした事例
システム/プログラムの破壊	病院施設において、ハッキンググループのリーダーでもあった夜間勤務の警備員が、医療機関のコンピュータに不正にアクセスし、プログラムに攻撃を行った。 【主な原因】 コンピュータは鍵のかかった部屋に設置していたものの、警備員のセキュリティキーを使って物理的にアクセスしていた。	(3)情報の格付け区分 (4)格付け区分の適用とラベル付け (8)物理的な保護と入退管理 (17)情報システムにおけるログ・証跡の記録と保存	No53病院施設事例
金銭の着服	企業において、元役員が、退職日の夜、有効なままであった電子キーカードを使ってアクセスコードを入手し、上級管理職2人のコンピュータを使用して、海外口座に電子送金を行い、国外逃亡した。 【主な原因】 退職日の夜に電子キーカードが有効な状態であった。	(5)情報システムにおける利用者のアクセス管理	No69米国の電力会社事例

1-2. 国内外文献調査　～文献調査の実施方法

法令・指針・ガイドライン・レポート・記事等30個の公知文献を選定し、調査を実施。
テレワーク・雇用流動化等の環境変化、サイバーセキュリティ技術の進展等に伴う新しい対策等を抽出、現在のガイドラインの構造に紐づけてガイドライン改訂の方針とした。

文献調査の実施プロセス

対象文献の調査

調査対象文献については：

1. 内部不正との関わりが深い法令・指針の制定・改正等
2. 海外公的機関の内部不正防止ガイドライン・レポート等
3. 国内外のテレワークセキュリティガイドライン等
4. 国内外民間の内部不正防止対策に関するレポート、記事、白書、書籍等

から30個の公知文献を選定
（次頁参照）

ガイドライン改訂に資する対策・指針等の抜粋

現在のガイドライン構造との紐づけ

抜粋した対策・指針等を現在のガイドラインの関係箇所と紐づけ。

整理にあたり、

1. 指針レベルで新たに柱を立てるか
2. 対策のポイントを追記することで指針に厚みを持たせるか

のどちらの方針を採用するかを検討。

ガイドラインの改訂方針の検討

検討結果に基づき、予め立てておいた仮説も勘案、
ガイドライン改訂方針を検討

1-2. 国内外文献調査　～文献調査の対象一覧(1/3)

調査対象の国内外30件の公知文献を以下に示す。

#	種別	執筆時期	タイトル	著者	URL
1	国内の関連法改正／施行	2021年	令和３年 改正個人情報保護法について（官民を通じた個人情報保護制度の見直し）	個人情報保護委員会	https://www.ppc.go.jp/personalinfo/minaoshi/
2		2020年	令和２年 改正個人情報保護法について	個人情報保護委員会	https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/
3		2018年	技術等情報漏えい防止措置の実施の促進に関する法令 産業競争力強化法、施行令、産業競争力強化法に基づく認定技術等情報漏えい防止措置認証機関に関する命令、技術等情報漏えい防止措置認証業務の実施の方法、技術及びこれに関する研究開発の成果、生産方法その他の事業活動に有用な情報の漏えいを防止するために必要な措置に関する基準	経済産業省貿易管理部安全保障貿易課	https://www.meti.go.jp/policy/mono_info_service/mono/technology_management/index.html
4	技術情報管理認証制度に係る指針	2018年	技術等情報漏えい防止措置の実施の促進に関する指針	経済産業省貿易管理部安全保障貿易課	同上
5	国内公的機関のテレワークに関わるセキュリティガイドライン等	2020年5月	テレワーク時における秘密情報管理のポイント（Q&A解説）	経済産業省知的財産政策室	https://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/teleworkqa_20200507.pdf
6		2021年1月	緊急事態宣言(2021 年 1 月 7 日)を踏まえたテレワーク実施にかかる注意喚起 （これまでに発出した注意喚起を含む）	NISC	https://www.nisc.go.jp/pdf/press/20210108_caution_press.pdf
7			テレワークにおけるセキュリティ確保（ポータルサイトで各種ガイドラインを公表）	総務省	https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/
8		2020年7月	家庭内で安全快適に在宅勤務を行うためのレファレンスガイド	ICT-ISAC	https://www.ict-isac.jp/news/remote%20work%20reference%20guide.pdf
9	海外の公的機関による内部不正対策に関するガイドライン、レポート等	2020年11月	Insider Threat Mitigation Guide	米国CISA	https://www.cisa.gov/sites/default/files/publications/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf
10			INSIDER THREAT MITIGATION（公的なWebポータルサイト）	米国CISA	https://www.cisa.gov/insider-threat-mitigation
11		2021年3月	Insider Threat Mitigation for U.S. Critical Infrastructure Entities: Guidelines from an Intelligence Perspective	英国NCSC	https://www.dni.gov/files/NCSC/documents/news/20210319-Insider-Threat-Mitigation-for-US-Critical-Infrastru-March-2021.pdf
12		2020年	ENISA Threat Landscape 2020 - Insider Threat	ENISA	https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-insider-threat

1-2. 国内外文献調査　～文献調査の対象一覧(2/3)

#	種別	執筆時期	タイトル	著者	URL
13	講演資料	2021年6月	境界防御をさらに困難にする「外部脅威者が巧妙に仕掛けるインサイダー攻撃」	名和利男	https://sbbit.jp/eventinfo/63142/
14	動画アーカイブ	2020年11月	NCD Insightオンラインセミナーシリーズ 対談「内部犯行の脅威と対策」 （パネリスト） 日本サイバーディフェンス株式会社、Dr. Susanna Berry、名和 利男	Nihon Cyber Defence社	https://www.twx-threatintel.com/threat-intelligence/%E3%82%A6%E3%82%A7%E3%83%93%E3%83%8A%E3%83%BC%E3%81%AA%E3%81%A9%E3%81%AE%E5%8B%95%E7%94%BB/20210407/ncd-seminar/
15	レポート		CERT Insider Threat Center(Webポータルサイト伝統的なポータル)	カーネギーメロン大学	https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=91513
16	Webポータルサイト		Address rising insider threats with zero trust	IBM社	https://www.ibm.com/blogs/digital-transformation/in-en/blog/addressing-rising-insider-threats-with-zero-trust/
17	Web記事	2021年6月	5 Steps to Navigating Insider Risk in the Post-Pandemic World	Mark Wojtasiak	https://www.darkreading.com/vulnerabilities---threats/5-steps-to-navigating-insider-risk-in-the-post-pandemic-world/d/d-id/1341202
18	書籍	2020年9月	Why Insider Risk Is the Biggest Cyber Threat You Can’t Ignore	Joe Payne（著), Jadee Hanson（著), Mark Wojtasiak（著), George Kurtz (はしがき)	https://www.amazon.co.jp/Inside-Jobs-Insider-Biggest-Threat/dp/1510764488
19	レポート		2021 Data Exposure Report -Insider Risk is a Data Protection Problem	CODE 42	https://www.code42.com/resources/report-2021-data-exposure/
20	White Paper		A Step-by-Step Guide to Automating Workflows to Protect Data	CODE 42	https://www.code42.com/resources/white-paper-a-step-by-step-guide-to-automating-workflows-to-protect-data/
21	書籍	2019年	Insider Threats A Business Leader's Guide to Managing Employees and Cyber Security	Cedric Leighton, Amy Love Leighton	
22	White Paper	2021年5月	Securing C-Suite Collaboration in an Era of Insider Risk	Diligent	https://www.infosecurity-magazine.com/white-papers/secure-csuite-collab-insider-risk/
23	公的なWebポータルサイト		Insider Risk Mitigation Framework	英国CPNI	https://www.cpni.gov.uk/insider-risks/insider-risk-mitigation-framework
24			HoMER(Holistic Management of Employee Risk)	英国CPNI	https://www.cpni.gov.uk/resources/holistic-management-employee-risk-homer-guidance

1-2. 国内外文献調査　～文献調査の対象一覧(3/3)

#	種別	執筆時期	タイトル	著者	URL
25	公的なWebポータルサイト		Personnel Security Maturity Model	英国CPNI	https://www.cpni.gov.uk/personnel-security-maturity-model
26	公的なWebポータルサイト		SeCURE 4(Assessing Security Culture)	英国CPNI	https://www.cpni.gov.uk/secure-4-assessing-security-culture
27	公的なWebポータルサイト		The employment practice code	英国ICO (英国個人情報保護監督機関)	https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf
28	レポート		Global Fraud and Risk Report 2019/20	クロール社	https://www.kroll.com/en/insights/publications/global-fraud-and-risk-report-2019
29	レポート	2018年12月	Common Sense Guide to Mitigating Insider Threats, Sixth Edition	CERT National Insider Threat Center	https://resources.sei.cmu.edu/asset_files/TechnicalReport/2019_005_001_540647.pdf
30	レポート		HUMAN RESOURCES' ROLE IN PREVENTING INSIDER THREATS	CISA	https://www.cisa.gov/sites/default/files/publications/HRs%20Role%20in%20Preventing%20Insider%20Threats%20Fact%20Sheet_508.pdf

1-2. 国内外文献調査　文献調査から得られた重要な示唆(1/2)

国内外文献調査から、最近の環境変化等に関連したリスク低減に繋がる**多くの具体的な示唆**が得られた。
ガイドラインの改訂にあたり、これらの示唆を参考にして検討を実施。

#	着目すべき環境変化	重要な示唆の導出
1	営業秘密の漏えい、とりわけ重要技術情報の漏えいに対する社会的な危機感の拡大	• 技術等情報のうち管理対象情報の特定に当たっては、事業者の経営層も関与した上で、以下の事項を考慮する。 １．その技術が漏えいした場合に、自らの競争力に重大な影響を与えるか否か ２．他者から契約等に基づき預けられた情報であること等により、その技術等情報が漏えいした場合自らの信用、他者との信頼関係等に対して重大な影響を与えるか否か
2	内部不正が事業経営に及ぼすリスクの増大	• 技術等情報のうち管理対象情報の特定に当たっては、事業者の経営層も関与した上で、以下の事項を考慮する。 １．その技術が漏えいした場合に、自らの競争力に重大な影響を与えるか否か ２．他者から契約等に基づき預けられた情報であること等により、その技術等情報が漏えいした場合自らの信用、他者との信頼関係等に対して重大な影響を与えるか否か
3	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	• テレワークにおける社外からの秘密情報へのアクセスについて、従業員の予見可能性を確保 • テレワークを前提とした秘密情報の持ち出しについて現行の働き方との差に則して管理の態様や諸規定を見直し周知徹底 • 一時的または恒久的に海外でのテレワークを希望する従業員は、例外的に個別にリスク評価を実施。海外でアクセスする資料の機密性、ハードコピーの将来的セキュリティ、現地の雇用法、保護監視等を考慮すべき • セキュリティポリシーやテレワークのための情報セキュリティ関連規程につき、定期的に実施状況を把握・改善 • オフィスネットワーク上の共有フォルダやクラウドサービスに対するアクセス権限設定、ファイアウォール設定等により、機密情報を閲覧・編集する必要のないテレワーク端末やテレワーク勤務者からのアクセスを制御 • VPN機器や個人の無線LANルーターのソフトウェアアップデートに関した要求 • 社内システムやクラウドサービスへのアクセス時の利用者認証機能として、可能な限り多要素認証を強制 • テレワーク端末がオフィスネットワークやクラウドサービスに接続する際は証明書認証を要求
4	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	• 管理対象情報を委託先に渡す際の秘密保持契約締結を要求 • クラウド／データセンター利用時の秘密保持契約締結 • 組織は、クラウドサービスプロバイダーのあらゆる側面を慎重に検討し、サービスプロバイダーが組織のセキュリティ慣行を満たしているか、または上回っていることを確認する

1-2. 国内外文献調査　文献調査から得られた重要な示唆(2/2)

#	着目すべき環境変化	重要な示唆の導出
5	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）の急速な進展と個人情報に配慮した運用	• アクセス権設定等の特別な権限を持つ管理者等管理情報システムの維持に責任を有する者の管理情報システムへのログインに対して、二つの認証機能（パスワード、生体認証、電子証明書等）を組み合わせた二要素認証を要求する • 特権ユーザーまたはシステム管理者のアカウントに多要素認証を要求することで、管理者が組織を去った後にユーザーが特権的なアクセスを悪用するリスクを低減することができる • インサイダー脅威による被害や混乱が発生する前に、積極的（プロアクティブ）に検知して即時対処を伴う「モニタリング」の仕組みを導入し、「 最新のモニタリングツールの多くに実装されている『ユーザー（人間）とエンティティ（デバイスなど）の振る舞い解析』」などを利用 • 従業員とITネットワークの両方に対し、通常行動のベースラインを設定し、重大な変化を特定できるようにする • SIEMにインサイダー脅威の検知ルールを導入する。継続的にログを確認し、監視リストを確実に更新する • 監視ツールを使用して、一定期間、ネットワークと従業員の活動を監視し、通常の動作と傾向の基礎を確立する • セキュリティチームは、適切なデータセキュリティ技術の導入によって、データ活動のコンテキストを可視化できる。これらのインサイダーリスク指標を用いて、ソースコードの流出、疑わしいファイルタイプの不一致、個人用クラウドストレージへの同期、従業員の離職など、特定のタイプのリスクを重要度の低いイベントよりも優先させる
6	雇用の流動化による退職者（転職者）の急増	• 退職時に知的財産権/秘密保持契約を確立する • 従業員や契約社員が組織から離脱する際には、VPNサービス、アプリケーションサーバー、電子メール、ネットワークインフラ機器、リモート管理ソフトウェアへのアクセスを必ず無効にする
7	法改正等（個人情報保護法、不正競争防止法等）：個人情報漏えいの通報義務、重要データ保護等の観点	• 限定提供データ取扱に関する内部不正（アクセス権のない限定提供データの取得・使用・開示、アクセス権を持つ限定提供データの違法な使用・開示、不正な経緯を知って転得した限定提供データの使用・開示等） • 管理対象情報を委託先に引き渡す場合は、可能な限り分割して引き渡すことを要求 • 内部から外部への通信について、ログを取得し監視することを要求 • 管理対象情報の適切な管理をするためのトレーニングや意識の啓発を図るためのトレーニングを受講させる機会を定期的に設け、管理対象情報を含む技術等情報に係る認識向上による不正行為者の言い逃れの排除等に資するよう取組を行うことを求めている • AIを活用する等の高度な内部不正検知システムの適用のトレンドとプライバシー／人権保護との兼ね合い • 内部不正防止の観点から法的に問題が生じない範囲でストレスチェック結果などの情報を適正に取り扱いながら活用

2．インタビュー調査

2．インタビュー調査

	調査種類	調査概要
インタビュー調査	国内企業インタビュー	• 国内企業へのインタビューを通じて、内部不正対策の現状や考え方を調査
	国内外有識者インタビュー	• 国内外有識者へのインタビューを通じて、専門的見地から内部不正対策の現状や事例についての知見及び今後のあるべき姿に関する考え方を調査

2-1. 国内企業

国内企業7社に対し、インタビュー調査を実施。**テレワークを積極的に推進**している企業を中心に、**内部不正対策の知見・経験**を有していると目される企業等を選定。

#	時期	業種・業態	セキュリティ管理成熟度	テレワーク先進性	クラウドとの関わり	内部不正対策との関わり	期待される成果・有効性
1	第1回	警備業	高い	あまり進んでいない	他社のクラウドサービスとの提携を積極的に推進	他社の内部不正対策への取組など、豊富な経験を持つ	テレワークが進んでいない大企業として、テレワーク時代の情報漏えい対策をどのように捉えているかを把握でき、他のテレワークが進んでいる企業との対比が可能。 内部不正対策については、顧客事例から得た豊富な知見の提供にも期待できる。
2		セキュリティサービス	高い	積極推進	クラウドサービスを利用	セキュリティに関するコンサルティングを実施	ガイドラインの利用企業として、ガイドライン改訂について有益な知見をいただくことが期待できる。
3		製造業ITサービス	高い	製造業として先進的な取組	クラウドサービスを積極的に提供		製造業においても積極的にテレワークに取り組む企業として、ニューノーマルの情報漏えい対策について、高い知見と経験に基づく回答を期待できる。
4	第2回	樹脂加工	高い	積極推進	AWSやAzureを積極的に活用	最近、営業秘密侵害事件を経験	最近営業秘密侵害事件を経験した企業としての内部不正対策への課題やあるべき姿の考え方を聴取して参考にすることができる。
5		リスクマネジメント	高い	「テレワーク東京ルール」実践企業宣言を行う	クラウドサービスのセキュリティ診断を事業化	リスクマネジメントの観点から内部不正にも詳しい	リスクマネジメントサービスを提供する企業として、幅広い視野でニューノーマル時代の内部不正を捉えていると考えられるため、その知見をガイドライン検討に活かすことができる。
6	第3回	大手SIer	高い	特に積極的にテレワークを推進する大企業	クラウドサービスの提供も利用も先進的	成熟した運用を実施	成熟度の高い総合的な取組について伺うことができるとともに、ガイドライン改訂についても高い見地から有益なレビューをしていただくことが期待できる。
7		ITサービス	高い	テレワーク先進企業の定評あり	クラウドサービスを積極的に提供	内部不正対策への取組は先進的	成熟度の高い総合的な取組について伺うことができるとともに、ガイドライン改訂についても高い見地から有益なレビューをしていただくことが期待できる。

2-1. 国内企業のインタビュー結果（1/2）

経営者の意識向上、ふるまい解析とプライバシ／人権への配慮、テレワークのログ等の記録、退職予定者の権限・ログ管理、テレワーク時のケア、テレワークの内部不正対策のレビュー等の企業の実態を聴取。

#	ヒアリングのポイント	国内企業の回答
1	経営陣に責任を自覚してもらうために、どのような工夫をすれば良いか	■ テレワークの普及により情報が分散することで内部不正を含めたリスクが増大していることを意識していただくことが必要 ■ 現在の様々な脅威について、一度手を打ったから大丈夫という感覚を持っていただきたくない ■ 自分が経営層からどうやってみられているのかを知ることができるように、公平な形でのメールの発信、雑談の会議等、内部不正が起きないような環境づくりに取り組んでいただきたい
2	a. 内部不正対策としてのふるまい解析等は、プライバシー／人権保護の観点から、どこまでやったらプライバシー／人権侵害になるのか。 b. 他方で、システム管理者が監視・検知の対策実施に萎縮しないようにするためにはどのような工夫が必要か。	■ ふるまい検知等のシステムについては当然に事前の合意が必要。権限者による検知状況の閲覧につき、正当な手続きを整備することが必要 ■ 悪事を取り締まるという観点ではなく、何もしていない人を守るために監視をするという伝え方が必要 ■ 会社から貸与されたPCやスマホ（携帯）等を使う限りは、一定の監視があるという暗黙の了解がある ■ 業種/職種によってまちまちでルール化が必要 ■ 過度な締め付けを行うと、抜け道を悪用する不正行為を誘発しやすい
3	プライバシー／人権保護の観点からどのような点に留意しているか。	■ 人事部門から指示があれば動くという方式を採用 ■ 監視は、従業員のあらを探すためではなく、従業員を守るためだと、社内規程に記載 ■ メール・ログ等の監査は誓約書やポリシーで規定して従業員に周知して実施 ■ 次のようなことをガイドラインに記載すべき： ✓ 技術の進歩とこれに偏重した導入によって従業員の反発等を受ける危惧があり、これへの注意喚起が必要 ✓ 人事部門が監視結果を、テレワーク時のパフォーマンス評価等の目的で使ってしまう恐れがある。こうした目的外使用が認められないことを周知すべき ✓ 就職・異動の際に誓約書等でふるまい解析等の情報の利用目的を周知徹底することが重要
4	従業員のテレワークに伴うログ・証跡（VPN装置やVDI機器等へのアクセスログ、テレワーク関連機器やクラウドサービスにログイン時の認証ログやログイン後の操作ログ、テレワーク端末の操作ログやイベントログ等）の記録・保存を行っているか。	■ 会社貸与PCはツールにより監視。BYODのログは取得しない ■ 従業員のテレワークに伴うログ・証跡の記録・保存を実施。ランサムウェア等による問題発生時に操作ログ等を保存しておくことは重要 ■ 基本的にログ・証跡が残っているが、あくまでも「こういうところに不審なアクセスがあった」程度の管理であり、今後もその強化を考えていない

2-1. 国内企業のインタビュー結果（2/2）

#	ヒアリングのポイント	国内企業の回答
5	a. 退職予定者の秘密情報へのアクセスや、テレワーク利用の権限を、どの段階で無効にしているか／するべきか。 b. 退職後の情報漏えいに対し、どのような抑止力を駆使すべきか。 c. 退職予定者のログ分析をどのように行っているか／おこなうべきか。	■ 人事システムで、退職日を迎えるとその時点で（実質的に、退職翌日）ログイン権限をはく奪 ■ アカウントは全社アカウント管理システムと紐づいており、退職時にすべての権限を自動的にはく奪（テレワークも同様） ■ 退職した方の訴求ログ分析はしていないが、人事からの指示があれば対応 ■ 退職予定者に対し、Webアクセス状況やメールの確認を行っている事例あり ■ 従業員の退職が決まったら監視を強化する、数か月前にまで遡ってログを分析する等の対策を実施している会社もあるようだ
6	テレワークを行う従業員の疎外感、不公平感を緩和し、日常と異なる行動を早期に見出すため、従業員との日常のコミュニケーションをどのようにして確保しているか。	■ テレワークという働き方は、心と身体の健康、ケアと改善が必要と認識 ■ 遠隔会議システムを社員に開放し、これを使ったコミュニケーションや、実際の出社を週1で実施したりして対応 ■ 人事部門の施策ではあるが、テレワーク時には日報を書いて上司とコミュニケーションをとるという規則がある ■ 各部署の裁量で、毎週決まった曜日・時間にチームミーティングを実施。チームミーティングはWeb会議であり、管理職は、メンバーの顔色、声のトーンを業務連絡や雑談をしながら確認 ■ 定期的に社員にアンケートをとって孤独感を感じている社員を可視化し、チームで週1回対面会議を実施したり、毎朝チームで顔見せ朝会したりする等の取り組みを実施
7	テレワークを行う従業員の内部不正対策について、企業はどのようなレビューや内部監査を実施しているか／実施すべきか。	■ 内部統制の一環として内部不正のリスクアセスメントを実施するのがやりやすい ■ 月単位で不審行動をレポートにし、内部不正リーダー、管理者に報告。「能動的に監視」ではなく「通常からの逸脱を見守り」として対処すべき ■ 不正対策と併行して、従業員の悩みを吸い上げる等、週1の定期的な会議で確認を実施。このくらいの頻度が妥当と考える

2-2. 国内及び海外の有識者

有識者へのインタビュー調査については、技術面と法的実務の両方を重視し、**技術に精通する専門家2名**と**セキュリティ分野で知見が豊富な弁護士2名**にインタビューを実施。

さらに、内部不正対策で世界をリードしている**英国の経験豊富なサイバーセキュリティ専門家**（元政府職員、2名）に対してオンラインでインタビューを実施、海外の最先端の知見の収集に努めた。

#	国内／海外	インタビューを実施した有識者の概要	備考
1	国内	サイバーセキュリティ分野で知見が豊富な弁護士	
2	国内	同	
3	国内	サイバーセキュリティ技術に精通するコンサルタント	
4	国内	サイバーセキュリティ技術に精通するプロフェッショナル（2回）	専門的知見に関する情報の事前提供を受け、ヒアリングを行い議論
5	英国	同（3回）	2名

2-2. 国内及び海外の有識者のインタビュー結果（1/3）

国内及び海外の有識者のインタビューでは、**技術的観点と法的実務の観点**から多くの有意義な示唆あり。
これらを参考にして、組織における内部不正防止ガイドラインの関係各所に追記・修正を実施。

#	ヒアリングのポイント	有識者（法律関係者）の回答
1	a. 経営者が社内で内部不正防止ガイドラインを実行に移すにあたり、納得感を持って現場にその内容を伝えられるようにするためには、ガイドラインをどのような書き方にすれば良いか。 b. 経営陣に責任を自覚してもらうために、どのような工夫を施しているのか。	■ 情報漏えいに関して、令和4年に令和2年個人情報保護改正を受けて個人情報保護委員会に対する報告の義務化の実施がされる予定であり、記載した方が良いと考えられる。 ■ 経営者が一番に読むだろう冒頭部分に証拠保全の体制整備の必要性について記載頂きたい。 ■ 重要なのは証拠確保であり、証拠保全の観点から技術的な環境や技術的証拠保全に対して理解を求めたい。経営者には、問題が起こった際に無駄にシステムに触らないことや、証拠が残るような体制を組んでいて欲しい。 ■ 経営陣はサイバーセキュリティのリスクがどの程度の事業リスクかイメージできない点がリスクだと考える。ガイドラインで、事業リスクを前提として、経営陣にメッセージを伝えてもよい。「御社の事業にどういうダメージを与えるのか」という観点がないと自分事として捉えられない。経営陣にそういうスイッチが入ると、ヒト・モノ・カネを動かし、情シスより積極的に対策をする傾向がある。
2	内部不正対策に取り組む社内体制の構造（骨格）について、可能な範囲で（またはあるべき姿のお考えを）ご教示いただきたい。	■ メインはリスク管理部門が中心になると考える。何か起こった場合にはシステム等を確認するのはセキュリティ部門、働き方等人事部等が携わるがそのとりまとめはリスク管理部門ではないか。 ■ 小規模企業においては特に、コンプライアンスについて総務が兼務している場合があるため、どうしたら機能するか考えている。 ■ 内部統制が不十分な会社では、外部監査役を活用するとよい。
3	a. 内部不正対策としてのふるまい検知等は、プライバシー／人権保護の観点から、どこまでシステムとして自動化できるか。逆にどこまでやったらプライバシー／人権侵害になるのか。 b. 他方で、システム管理者が監視・検知の対策実施に萎縮しないような書きぶりとするためにはどのような工夫が必要か。	■ ふるまい解析等のモニタリングの重要性等が進歩しEDR等のエンドポイントソリューションも増加してきており、プライバシー/人権保護との観点からもう少し議論されるべきところである。但し、その線引きは難しい。ふるまい解析をセキュリティ以外の目的に利用するのは問題であるが、目的を不正対策に限定すれば、現状、ある程度許容内であると考えている。 ■ 自分が知っている限りにおいて、EDR等のツール利用が人権侵害であるというクレームが従業員から入った事例はない。 ■ EDRの一環として不審なふるまいをモニタリングし、目的は従業員保護とした方がよい。 例えば、社内規定に記載し従業員がモニタリングを認識していても従業員の業績評価等を実施してしまうと過剰であるため、目的をセキュリティ対策と限定することで紛争リスクを低減できるのではないかと考える。 ■ AIを上手く活用して全て対応するなら問題ないが、人の手が入る状態になるとプライバシー侵害度合が上がり問題になることも想定できる。

2-2. 国内及び海外の有識者のインタビュー結果（2/3）

#	ヒアリングのポイント	有識者（法律関係者）の回答
4	高度なモニタリング技術はどのレベルまで到達しているか。	■ 相関分析とビックデータから導かれるパターンマッチングの行動予測が広義のAIとしてマーケティングされているが、昔と違う点としてパターンマッチングの分母数がかなり多くなっており、予測精度が高くなり、誤検知の数が少なくなっている点が挙げられる。ベンダー側も犯人側の手口を分析しており（最近のマルウェアを使わないタイプの攻撃（Powershell攻撃等のファイルレスマルウェア攻撃））、かなりハイレベルの対応をしている。 ■ EDR自身はクラウドコンソールに必要なログは吸い上げられており、かなりリアルタイムに近い形でモニタリングできる状態である。それをさらに専門のSIEMに吸い上げ、ふるまい解析（UEBA: User and Entity Behavior Analytics）等を導入している会社では、かなり見える化が進んでおり、内部不正の動き（進展プロセス）までも高精度で解析できる。 ■ 国内で、ふるまい解析を導入している会社は多いという段階までは到達していないが、広義な意味でUEBAを導入しようとしている企業は多い。第一段階はEDR導入の検討、次段階がクラウドプロキシ導入（脱VPNとクラウドに対してのリスクコントロール=インバウンド/アウトバウンドのインターネットへのアクセスコントロール）、第三段階としてバラバラにログを管理していたものをSIEMに集約して、それを「見える化」するためにUEBAを利用するという流れである。
5	テレワークを行う従業員の内部不正防止のために、従業員に定期的にどのような教育を実施しているか/実施する必要があるか。	■ テレワークを行う従業員の内部不正防止と抑止力発揮のために、ガイドラインにおいて、従業員に定期的に教育を受けさせることを求めていく考えである。特に、テレワーク固有の法的問題はないように思われる。労働法の関係で労務関係ではあると思われるが、情報の取り扱いでテレワーク固有の問題はほぼない。
6	テレワークを行う従業員の疎外感、不公平感を緩和し、日常と異なる行動を早期に見出すため、従業員との日常のコミュニケーションをどのようにして確保しているか。	■ このような記載はあった方がいいと思うが、人によっては過干渉になってしまうこともあるため人が嫌がらない範囲でやることが必要と考える。監視の意味合いが強くなり過ぎると問題となってくると考えられるため注意が必要である。 ■ 各チームリーダーが常日頃の朝会等のタイミングで声掛けをしていくのが絶対条件であると考える。これをやるかどうかでチームのコミュニケーション密度が全然違ってくる。雑談できないことがテレワークの一番の弊害であると考えている。組織として雑談が重要である。
7	テレワーク従事者の内部不正によるインシデントを想定した/あるいは対応するためのデジタルフォレンジックにどのように取り組んでいるか／取り組むべきか。	■ テレワーク時のログ取得については、端末はEDR（のログ取得）等を利用する対策及びその事前周知・従業員の合意という条件を求める。当初からEDRのログ取得を設計する等、デジタルフォレンジックの観点から証拠保全できる設計（Security by Design（「情報セキュリティを企画・設計段階から確保するための方策」））が必要である。VPNのログを取得しておらず侵入は判明したが、その後何が起こったのか不明という相談が増加しており、ログの重要性は高まっていると考えている。 ■ システム管理者が監視・検知の対策実施に萎縮しないようにするためには、ガイドラインにおいてプライバシー／人権保護に言及する際に、内部不正対策を実施しない方がリスクであり、従業員の同意をとるプロセスの必要性の高さと、その要件がさほど厳しくない点は記載してもよいかも知れない。個人情報保護法委員会Q&Aも「望ましい」といった書きぶりをしており、その目的を「従業員を守る」とした書きぶりもありえる。 ■ システム管理者が監視・検知の対策実施に萎縮しないようにするためには、ガイドラインにおいてプライバシー／人権保護に言及する際に、内部不正対策を実施しない方がリスクであり、従業員の同意をとるプロセスの必要性の高さと、その要件がさほど厳しくない点は記載してもよいかも知れない。

2-2. 国内及び海外の有識者のインタビュー結果（3/3）

#	ヒアリングのポイント	有識者（法律関係者）の回答
8	テレワークを行う従業員の内部不正対策について、企業はどのようなレビューや内部監査を実施しているか／実施すべきか。	■ テレワークを行う従業員の内部不正対策について、企業が行うべきレビュー（や内部監査）としては、モニタリングのログを見ていくしか対策がないと考えている。テレワーク以外の従業員と比較して特段の対策が必要であるとは思われない。 ■ テレワークが開始されて間もないため、私の知る限り労務管理上の一斉質問や上記のような内部監査対策としては聞いたことがないが、一般論として通用するのではないか。 ■ テレワークを行う従業員の内部不正対策について、実際は個々のリスクがあるから監査をしないといけないが、対策のポイントとして書きづらいと思っている。全社的に、形式的なアンケートをとってみるというのはどうか。 ■ その他技術的な話ではあるが、ネットワーク上の監視を実施して、テレワーク上の内部不正を技術的に検知するといったこともあるかもしれない。 ■ 企業インタビュー先としてAzure ADを使って技術的に検知するという企業もあり、これに関連して） PCを多層防御したりシンクライアントを活用したりする等、その物理的及び技術的監視は必要であると思う。
9	従業員のテレワークに伴うログ・証跡の記録や保存を行っているか。	■ モダンマルウェアは、基本的に活動を行ったらその場でログを消してしまうため、ローカルにログを残していては話にならない点に留意が必要である。
10	a. 退職予定者の秘密情報へのアクセスや、テレワーク利用の権限を、どの段階で無効にしているか／するべきか。 b. 退職後の情報漏えいに対し、どのような抑止力を駆使すべきか。 c. 退職予定者のログ分析をどのように行っているか／おこなうべきか。	■ 雇用終了及び契約終了による情報資産等の返却について、対策の強化方法として、お客様で内部不正のかなり大きな被害を受けているケースは年に数回あり、現場で経営陣と直接話す機会があるのだが、ログをとっておかないとその後の対策としてどうしようもないというのが企業を守る側の経営陣のスタンスである。 ■ 経営者の意図として、内部不正をやった人を罰するのではなく出来心を無くしたいという意図が多い。UEBAやSIEM等を導入し、その導入を従業員に周知することで、強い抑止力として使っている部分がある。

2-2. 国内及び海外の有識者
～国内外のサイバーセキュリティ技術に精通するプロフェッショナルへのインタビューから得られた示唆

経営陣へのメッセージの出し方、高度なモニタリング技術と従業員保護の周知、テレワーク時の内部不正対策・従業員教育・事後対応、退職時の内部不正対策強化等、日英の専門家から、実務に則した詳細な知見を得た。

関心がある主題	得られた回答の骨子
経営陣へのメッセージの出し方	■ 英国では、規制と政府指針を活用して、経営陣に責任を自覚してもらう取り組みがある。 （例） 上級役職員個人に対する責任を強化する規制枠組み：シニア・マネージャー・レジーム
モニタリングにあたっての従業員保護の周知	■ 企業が従業員に対して誠実さと透明性を持って接するよう努めるとともに、自社がそのような価値観を追求し、実践する企業であることを示す。 - なぜこのような対策が必要なのか、なぜ今行うのか - どんなリスクがあるのか、どんなメリットがあるのか（WIIFM原則 ）という観点から説明する。 ■ 経営陣は自社を守るためだけではなく、従業員を守るためであるというメッセージを強調することが有効 ■ 企業には顧客情報を保護する義務があり、顧客情報の保護は企業価値向上の重要な要素となり得る ■ 国内においては、内部不正対策ソリューションの市場が成熟していない現在の段階から、ガイドラインにおいて、「ふるまい解析等の導入においてはコンプライアンスに十分配慮のうえで検討すべき」ことを、注意喚起しておくことに意義がある。
AI等を活用した高度なモニタリング技術	■ 内部不正対策としての振る舞い検知等の一部の製品では、「教師なし機械学習と高度な相関関係の効率的な組み合わせ」を実現しているもので実用レベルになっている。特に、欧州GDPRや米国のプライバシー関連法に準拠した製品も多数存在見られることから、「プライバシー／人権保護の観点を考慮して運用上どこまでシステムとしてデータ収集・分析を実施するかを、組織の状況に合わせて適切に設定」できるレベルになっている。 ■ 教師あり機械学習はコストがかかる上に、個人の権利が強い国では教師データが少ないことが問題になる。
退職時の内部不正対策の強化	■ 「退職予定者のログ分析を行う」行為については、労働契約の締結時において、労働基準報に基づく「労働条件を書面などで明示」しておくとともに、労働契約法に基づく「使用者が、(1)合理的な内容の就業規則を(2)労働者に周知させている」ことが前提となる。したがって、「どのような、どこまで行うか」については、会社（使用者）と従業員（労働者）の合意形成（真の同意）により決定される。 ■ 退職予定者の監視は、一般の従業員の監視とは目的が異なっているため、個人情報の目的外使用にならないように、別途合意を形成する必要がある。内部不正防止が目的とストレートに書くと良くない可能性がある。 ■ 労務管理やセキュティ対策（EDR）等でログを容易に取得できるが、退職予定というだけで、従業員のシステム利用に係るログの分析がされるという行為は、「（1）合理的な内容に就業規則」であるとみなされない可能性がある。

2-2. 国内及び海外の有識者
～国内外のサイバーセキュリティ技術に精通するプロフェッショナルへのインタビューから得られた示唆

関心がある主題	得られた回答の骨子
テレワーク時の内部不正対策	■ テレワーク方式によって、クラウドプロキシやCASBの導入、テレワーク端末の内蔵記録装置（HDD・SSD等）の暗号化やデータの遠隔消去の対策を導入 ■ テレワーク端末とクラウドサービスのそれぞれに、どのような情報が保存されているかを管理 ■ クラウドサービスの設定不備や設定ミス等により意図せず情報を公開してしまわないよう十分に注意 ■ クラウドサービスへのアクセス権限に注意 ■ クラウドサービスへのアクセスログや操作ログを取得しそれらのログに異常がないか定期的に確認 ■ テレワーク端末についても必要なログを取得 ■ データのダウンロードができないクラウドサービスに限り使用許可等の対策を選択して適用 ■ 社員個人のPCやタブレットなどからクラウドを利用できることが見込まれ、システム管理者が実施しなければならない機器に対するセキュリティコントロールの対象が急増していることになるため、漏れ抜けの発生やヒューマンエラーが発生している可能性が高い。
海外からのテレワーク時の情報漏えい対策	■ 海外拠点や海外出張時で発生するセキュリティインシデントは、本社（本店）が持つセキュリティチームによる対処や調査に限界があるため、遠隔でも被害軽減や原因究明ができるように、海外で利用するPCには、遠隔からログや証跡を取得できる機能を組み込むか又は、クラウド等での作業を中心にするような仕組みにする。 ■ 最近では、海外で利用するPC内部でファイル処理することを少なくする「クラウドサービス方式」を取ることがほとんど、万が一のインシデント発生時には、クラウドに蓄積されているログや証跡で原因究明する。当該端末はリモートワイプする。 ■ したがって、「海外からのテレワークに対する情報漏えい対策」については、「PCで残さない形式、かつオフィスネットワークに接続しないクラウドサービス形式」を取るようにするなどの仕組みで工夫することが望ましい。
テレワークを行う従業員への教育	■ 最近の日本企業は、「ジョブ型」に移行しており、テレワークそのものが「ジョブ型」に最適なものとなっているため、それに適した内容にする必要がある。 ■ 従業員に対して、明確に定義された職務内容を実施していただくために、不明であると思われる領域に対する知識を積極的に提供する。例としては、「在宅勤務中の日常業務において、組織のデータを安全かつセキュアに使用、転送、保存する方法を徹底的な教訓・訓練を受けてもらう」となる。ただし、教育・訓練を受けることを命じるものではなく、教育・訓練サービスを提供し、それを受けるかは従業員の選択によるという位置づけにすることが重要。これは、ディール（取り引き）のようなもので、受けなければ職務内容の実施に当たり、支障をきたし、成果に影響することを十分に伝えることで、ほとんどの従業員が「徹底的に教育・訓練を受ける」ようになる。 ■ ジョブ型では、従業員自らが考えて理解して仕事をする行動様式が求められる。したがって、その行動様式に準じた教育方法を取る必要がある。また、社員には、明確に定義された職務内容を実施してもらっているため、彼らが自助として自分の利益を守るためのサービスとして、「被害に遭わないためのベストプラクティス」に係る教育・訓練サービスを提供する。
テレワークを行う従業員のログ・証跡の分析	■ テレワーク従事者による内部不正によるインシデントの調査の主な対象は、テレワーク従事者が利用していたPC、その周辺デバイス（スマートフォンを含む）、利用していたクラウドサービス（以下、PC等）となる。しかし、PC等に対して、事後に調査することを前提とした設計や設定にしていない場合、いざ調査を実施したとしても、証拠となるログや証跡を獲得することが困難になることが多い。テレワーク従事者が利用するPC等において、事後に調査することを前提にした設計や設定にすることを推奨する。具体的には、eディスカバリー準拠レベルであると説明すれば良い。既に大手の日本企業においても取り組んでいるため、納得しやすい。

今次調査の1．及び2．により得られた内部不正防止対策の主要ポイント

（１）テレワークの普及に伴う対策

- 重要情報の分散傾向に対応し、重要情報の棚卸し、保管状況の管理をルールやツールにより徹底
- クラウド活用の増加に対応し、クラウドプロキシやCASB（Cloud Access Security Broker）を導入
- テレワーク端末の内蔵記録装置（HDD・SSD等）の暗号化やデータの遠隔消去の対策を導入
- クラウドサービスのアクセス権限等の設定の漏れ・ミス等による意図しない相手への情報の曝露に注意
- クラウドサービスのアクセスログ・操作ログを取得し、不正アクセスがないかを定期的に確認
- テレワーク端末においても必要なログを取得
- テレワーク端末は可能な限り会社支給とし、EDR導入等で可視性を強化しセキュリティコントロールレベルを維持

（２）退職者関連対策

- システムのログ収集・解析を行うと同時に、雇用契約時等に合理的な内容の就業規則を就業者に周知
- 退職者が秘密保持契約や誓約を拒む事態を想定、入社時・重要プロジェクト配属時にも秘密保持契約を締結

（３）ふるまい検知等の新技術を活用する対策

- AIによる異常なふるまい検知等の新しい技術を内部不正対策として適用することを検討
- それらの活用と同時に従業員の人権・プライバシーに配慮した運用を行うことに留意

３．有識者検討会の運営

３．有識者検討会開催の趣旨

（１）「組織における内部不正防止ガイドライン」の改訂を検討する

（２）内容が同ガイドラインと不可分で整合性の調整が必要となる「秘密情報の保護ハンドブック」の改訂に役立つ情報を整理する

3．有識者検討会の運営　～委員構成～

有識者検討会の委員名簿を以下に示す。

＜有識者＞　（敬称略・五十音順）

	岡村　久道	英知法律事務所・京都大学大学院医学研究科　弁護士
	金子　啓子	大阪経済大学経営学部　ビジネス法学科　准教授
（委員長）	小松　文子	長崎県立大学　副学長
	高木　大資	東京大学大学院医学系研究科　講師
	西川　喜裕	三浦法律事務所　弁護士

＜オブザーバー＞

経済産業省　経済産業政策局　知的財産政策室

3．有識者検討会の運営　～運営実績～

本事業では、有識者検討会を4回開催し、組織における内部不正防止ガイドラインの改訂に係る審議を実施。
各回の検討会の運営実績と議事を以下に示す。

#	開催日時	議事
1	2020年9月30日（木） 15:00～16:30	1. 検討委員会の趣旨、運営方法 2. ニューノーマル移行／DX推進に伴う最近の情報漏えい等の環境変化の実態 3. 文献調査結果速報 4. ガイドライン改訂、ハンドブック改訂整理の検討方針
2	2021年11月8日（月） 13:00～15:00	1. ガイドライン改訂案の検討方法 2. 国内企業、国内外の有識者へのヒアリングについて 3. ガイドライン改訂案（骨子案）
3	2021年12月2日（木） 10:00～12:00	1. 第2回検討会及びその後のフォローアップで委員各位からいただいたご指摘について 2. 企業、有識者へのヒアリングについて（追加分） 3. ガイドライン改訂案及び付録の修正方針について
4	2022年1月21日（金） 13:00～15:00	1. 組織における内部不正防止ガイドライン改訂の最終案について 2. 秘密情報の保護ハンドブック改訂整理情報について 3. その他

４．組織における内部不正防止ガイドライン改訂の概要

４．組織における内部不正防止ガイドライン改訂の概要

調査結果、検討会での議論から、組織における内部不正防止ガイドラインの改訂にあたり、７つの環境変化に着目。また、検討会でのご指摘・議論を踏まえ、内部不正対策実施のための組織体制についても見直し。

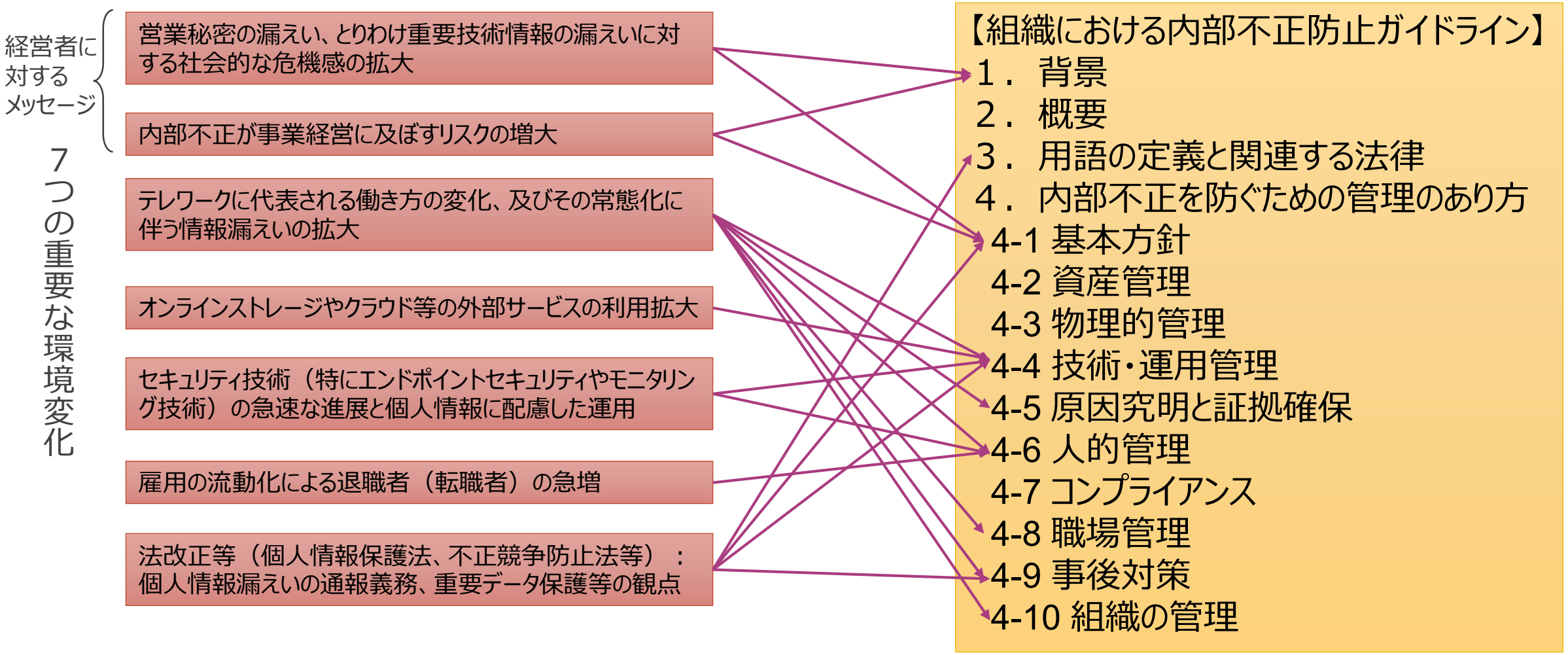
＜７つの環境変化＞

1. 営業秘密の漏えい、とりわけ重要技術情報の漏えいに対する社会的な危機感の拡大
2. 内部不正が事業経営に及ぼすリスクの増大
3. 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
4. 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
5. 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）の急速な進展と個人情報に配慮した運用
6. 雇用の流動化による退職者（転職者）の急増
7. 法改正等（個人情報保護法、不正競争防止法等）による個人情報漏えいの通報義務、重要データ保護等の観点

これらの７つの環境変化を重点項目ととらえ、内部不正事例調査、文献調査、企業／有識者ヒアリング、検討会議論等から関連事項を抽出、ガイドラインの修正・追記を行った。

4．組織における内部不正防止ガイドライン改訂の概要　～7つの重要な環境変化との関係

経営層へのメッセージとして「1 背景」や「4-1 基本方針」を加筆。技術の進歩から「4-4 技術・運用管理」に重点を置き改訂。モニタリングシステム適用時の従業員の人権・プライバシー保護の必要性から「4-6 人的管理」にも多く加筆。雇用の流動化について、退職時の対策を説明するために、「4-6 人的管理」に加筆・修正。



４．組織における内部不正防止ガイドライン改訂の概要　～テレワークに関する対策の追記

テレワークについては、幅広い対策の指針に対して改訂。
技術的な対策、人的管理と職場環境対策、さらに事後対策と証拠確保にも配慮する内容を修正・追記。

節・項目	対策の指針	関連する対策のポイント（要旨）
4-4.技術・運用管理	(13) ネットワーク利用のための安全管理	■ 組織外部で使用するPC等の対策強化 ■ ローカルブレイクアウト利用時の対策
	(16) 組織外部での業務における重要情報の保護	■ 重要情報と通信の暗号化 ■ テレワーク用PC等のローカル保存、組織内の重要情報への細かいアクセス制御 ■ 採用するテレワーク方式の特性に則した情報漏えい対策の強化 ■ テレワーク時の遵守ルール ■ クラウド等の外部サービス利用時のルール ■ クラウドサービス方式でテレワークを行う場合の対策 ■ 海外からのテレワーク ■ EDRやゼロトラストの概念の適用
	(17)業務委託時の確認（第三者が提供するサービス利用時を含む）	■ 委託先のテレワークセキュリティ対策の確認 ■ 個人情報漏えい事故発生時に委託先が負う義務
4-5.原因究明と証拠確保	(18)情報システムにおけるログ・証跡の記録と保存	■ テレワークに伴う履歴等の取得
4-6.人的管理	(20)教育による内部不正対策の周知徹底	■ テレワークを行う役職員等の実践的な教育・訓練 ■ 組織がテレワークを行う役職員を守ることの周知
4-8.職場環境	(27)公平な人事評価の整備	■ テレワークを行う従業員の公平な処遇
	(28)適正な労働環境及びコミュニケーションの推進	■ テレワークを行う役職員のコミュニケーションの確保
	(29)職場環境におけるマネジメント	■ テレワーク中の単独作業への対策
4-9.事後対策	(30)事後対策に求められる体制の整備	■ テレワーク中の内部不正に対応できるログ・証跡の取得

４．組織における内部不正防止ガイドライン改訂の概要　～各部分の改訂のポイント

「１．背景」では、経営者に向けたメッセージを示した。

「２．概要」では、内部不正体制における責任部門の必要性を示した。

「3-1. 用語の定義」では、今回のガイドライン改訂の重要ポイントである、重要情報のカバー範囲の拡大を定義した。「3-2. 関連する法律」では、個人情報保護法と不正競争防止法の改訂について示した。

節	項目	今回の改訂のポイント
１．背景	－	■ 技術・ノウハウ情報の漏えい対策の重要性 ■ 経済安全保障の観点
２．概要	2-4 内部不正対策の体制	■ 総括責任者の下に責任者と責任部門を置く一元的な体制を例示 ■ 重要情報の管理責任者の位置付けの明示
３．用語の定義と関連する法律	3-1 用語	■ 重要情報の定義に追記を行い、技術情報（営業秘密として管理される技術・ノウハウ情報、経済安全保障や安全保障貿易管理に関する重要技術情報）への意識付けを強めた
	3-2 関連する法律	■ 令和2年個人情報保護法改正（令和4年4月施行）において、個人の権利利益を害する恐れがある個人データ漏えい時の報告義務が規定された ■ 不正競争防止法に、限定提供データの保護規定が新たに追加された

4．組織における内部不正防止ガイドライン改訂の概要　～各部分の改訂のポイント

「4-1 基本方針」においては、経営者に向けたメッセージを強化。
秘密指定やアクセス管理について、テレワーク等による重要情報の広範分散傾向への対策を追加。

節・項目	対策の指針	今回の改訂のポイント
4-1 基本方針	本文	■ 経営者は内部不正を事業リスクとして捉えて対処すべき ■ 経営者自身が、行き過ぎた内部不正対策によって企業が活力を損なったり、情報の利活用が阻害されたりしないように、的確な意思決定を行うべき ■ 内部不正対策としてのモニタリングが強化される傾向の中で、経営者が主導して、モニタリングの目的が役職員の適正な保護であることを周知徹底すべき
	(1) 経営者の責任の明確化	■ 個人情報に加え、重要技術情報の漏えいリスクが高まっている ■ テレワーク等により重要情報が分散し、情報漏えいリスクが高まっている ■ 雇用の流動化に伴い、不満を持った転職者が増加する懸念があるため、経営者が率先して内部不正リスクの把握を進める ■ 情報漏えい時の事後対策としての証拠保全の重要性を、経営者がしっかり認識すべきこと ■ 事業経営において重要なデータの保護にも取り組むべき ■ 対策が脆弱な業務委託先・関連先等の内部不正によって重要情報が漏えいしないように、経営者が率先してサプライチェーン対策を強化すべき　等
4-2-1　秘密指定	(4) 格付け区分の適用とラベル付け	■ テレワーク等によって重要情報が細かい単位で広範囲に分散する傾向が強まるため、重要情報の棚卸しの重要性が高まっている
4-2-2　アクセス権設定	(5) 情報システムにおける利用者のアクセス管理	■ テレワーク等による重要情報の細かい単位での分散化に伴い、アクセス権限管理の粒度が細かくなっていくため、これに対応できるアクセス管理基盤を整備すべき

4．組織における内部不正防止ガイドライン改訂の概要　～各部分の改訂のポイント

「4-4 技術・運用管理」で近年の内部不正対策技術の進歩を踏まえた対策、テレワーク時の対策、委託先管理の強化、サプライチェーン対策の必要性等に言及。「4-5 原因究明と証拠確保」では、テレワーク時／クラウド等外部サービス利用時のログ・証跡取得の重要性、並びにログ・証跡取得とプライバシー保護の観点に言及。

節・項目	対策の指針	今回の改訂のポイント
4-4 技術・運用管理	(12) 内部不正モニタリングシステムの適用 **※新しく追加した指針**	■ モニタリングシステムが提供するAI監視機能等を内部不正対策として適用するにあたって必要な措置について記載
	(13) ネットワーク利用のための安全管理	■ 社外からネットワーク（SNS、オンラインストレージ、Webアクセス、電子メール）を利用するにあたり講じるべき対策
	(14) 重要情報の受渡し保護	■ 対策が脆弱な委託先等から重要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重要情報の範囲を制限する等のサプライチェーン対策を講じること
	(16) 組織外部での業務における重要情報の保護	■ テレワーク対策について幅広く追記 ■ 海外からのテレワークに関する技術的対策 ■ エンドポイントセキュリティ技術の適用 ■ ゼロトラストの概念の適用
	(17) 業務委託時の確認	■ 委託先・再委託先のセキュリティ対策の確認 ■ 情報漏えい事故発生時に委託先・再委託先が委託元の調査に協力する義務を負うことを事前・定期・不定期に確認 ■ 重要技術情報については、なりすましによる委託先への不審な問い合わせにも注意が必要であり、こうした事態に直面した場合は委託元に報告するルールを定めること ■ 委託先に下請法が適用される場合は、下請中小企業振興法の振興基準59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・支援を行うべき
4-5 原因究明と証拠確保	(18) 情報システムにおけるログ・証跡の記録と保存	■ テレワークに伴う履歴の取得 ■ アクセス等に失敗したログだけではなく、成功した（何に成功したかを含む）ログも取得しておくことで、分析や後日の確認・証拠保全等に役立つことを追記 ■ 利用者のプライバシー等を考慮し、ログ・証跡の収集について、「(21)従業員モニタリングの目的等の就業規則での周知」に基づいて必要な措置を講じるべき ■ クラウド等の外部サービスにログインした際の認証・操作等のログ・証跡による証拠保全が重要であることを追記 ■ ログ・証跡を別の社内サーバやクラウド等の外部サービスに集約すべき

4．組織における内部不正防止ガイドライン改訂の概要　～各部分の改訂のポイント

「4-6 人的管理」においては、テレワークに伴う対策、雇用終了時の対策の強化、従業員モニタリング時の人権・プライバシー保護対策に言及。
「4-7 コンプライアンス」では、雇用終了時に備えた秘密保持誓約書に関する対策を強化。
「4-8 職場環境」ではテレワーク時のコミュニケーション確保について示した。

節・項目	対策の指針	今回の改訂のポイント
4-6 人的管理	(20) 教育による内部不正対策の周知徹底	■ テレワークを巡る教育について示した
	(21) 従業員モニタリングの目的等の就業規則での周知 **※新しく追加した指針**	■ モニタリングシステムを用いて従業員の行動をモニタリングする場合の人権／プライバシー保護をどのように実践するかについて示した
	(22) 派遣労働者による守秘義務の遵守 **※新しく追加した指針**	■ 派遣労働者への秘密保持義務の課し方について示した
	(23) 雇用終了の際の人事手続き	■ 退職予定者が秘密保持契約や誓約書の提出を拒否することを想定した対策を推奨 ■ 退職した役職員が海外において重要情報を不正に開示するような事態に備えて、退職前の事前対策（重要情報を安易に海外に持ち出さないように警告、技術的・物理的な情報漏えい対策）を十分に講じること
	(24) 雇用終了及び契約終了による情報資産等の返却	■ テレワークを行うために付与した権限も削除すること
4-7 コンプライアンス	(26) 誓約書の要請	■ 「秘密保持誓約書」では、社内規程と重要情報の特定や運用によって、役職員が重要情報に対する企業の秘密管理意思を認識できるようにするために、秘密保持の対象となる重要情報について客観的に特定できるように記載されていること
4-8 職場環境	(28) 適正な労働環境及びコミュニケーションの推進	■ テレワーク中の内部不正の兆候を早期に発見し、内部不正を防止するために、テレワークを行う役職員が良好なコミュニケーションを保てる環境を整備すること

4．組織における内部不正防止ガイドライン改訂の概要　～各部分の改訂のポイント

「4-9 事後対策」では、テレワーク中の内部不正インシデントの事後対策について示し、故意の内部不正によって個人データ等が漏えいした場合の報告義務に言及した。さらに、民事訴訟・刑事告訴を目指す場合の対応を念頭に、事後対策を強化することを追記。
「4-10 組織の管理」では、テレワーク時の内部不正対策の実施状況確認について示した。

節・項目	対策の指針	今回の改訂のポイント
4-9 事後対策	(30) 事後対策に求められる体制の整備	■ テレワーク中の内部不正の事後対策について示した ■ 故意の内部不正によって個人データ等が漏えいした場合は報告義務があること ■ 個人情報データベース提供罪の適用が考えられる場合は、警察への相談、被害届提出、告訴等を早急に検討するとともに、原因究明・証拠保全を実施すること ■ 民事保全法による証拠保全、民事訴訟による仮処分、本訴（差止や損害賠償請求）、刑事告訴を行う場合は、過去の履歴等の電磁的記録をデジタル・フォレンジックで解析し、証拠として提出できるように、外部で解析を支援する専門家に協力を依頼すること
4-10 組織の管理	(33) 内部不正防止の観点を含んだ確認の実施	■ テレワーク時の役職員の内部不正対策やその他のセキュリティ対策の実施状況を確認すること

５．今後の課題

5．今後の課題

■技術的対策のキャッチアップ

エンドポイントセキュリティ技術に見られるように、内部不正対策に関連する技術はなお進展中であり、今後も技術的対策の観点をさらに深掘りし、技術への追従とそれらを活用した対策の強化に継続的に取り組む必要があると考えられる。

■社会的ニーズに適合した内部不正対策の普及・推進に必要な情報のキャッチアップ

今回、組織における内部不正防止ガイドラインがカバーする重要情報の範囲を、最新の環境条件変化に沿い、営業秘密・重要技術情報にまで大きく広げた。
このように今後も社会変化に伴い拡充が必要な事項を確認しつつ、内部不正対策として求められている課題に適宜対応する必要がある。そのためには社会環境条件が組織にどのような影響を与えているか、条件変化により何が必要となるかの継続的な調査・分析・把握が必要となると考えられる。

NTT DATA

Trusted Global Innovator