「組織における内部不正防止ガイドライン」第3版の主な改訂内容

2015年3月
独立行政法人　情報処理推進機構

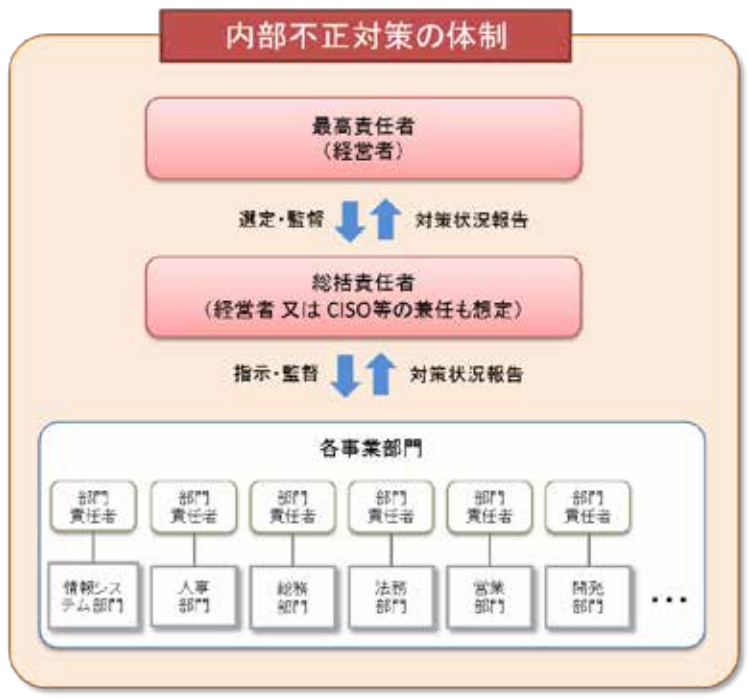
1.改訂概要

組織における内部不正防止ガイドライン（以下、本ガイドライン）をより使い易くし、広く活用してもらうため、本ガイドラインを利用する企業等からの要望を反映し、利用のためのリファレンスを追加するとともに、情報セキュリティに関する最新の標準規格及び指針へ対応しました。主な改訂のポインは以下の通りです。

①企業等からの要望への対応
　具体策の例示や必須対策と強化対策の明確化等
②情報セキュリティに関する最新の標準規格及び指針へ対応
　ISMSの規格改訂（JIS Q 27001:2014）及び営業秘密管理指針の全部改訂に対応し関連箇所を更新
③利用のためのリファレンスを追加
　内部不正を防止するための基本原則及び、企業のおかれている環境や懸念される不正行為別に分類した対策一覧を追加

2．新旧対応一覧

①企業等からの要望への対応□

項目	第2版	第3版
2-4-4. 図2	図2　内部不正対策の体制図 	図2　内部不正対策の体制図 
2-4-4.	・部門責任者：	・部門責任者（部門規模が大きい場合）：
3-1.	(2) 内部者 役員、従業員及び契約社員等の従業員に準ずるもの（以下、総称して「役職員」という。）	(2) 内部者 役員、従業員（契約社員を含む）及び派遣社員等の従業員に準ずる者（以下、総称して「役職員」という。）
	-	(5) 業務委託 業務の一部を、業務委託契約(準委任契約、または請負契約)を結び委託すること。本ガイドラインでは、契約社員及び労働者派遣業法で定義する労働者派遣、は含みません。
	-	(6) 委託先 業務委託される側の組織。
	-	(7)「望ましい」、「望まれます」 文末が「ねばならない」「します」「必要です」は、必須と考えられる対策を示しています。「望ましい」「望まれます」という表現になっている対策は、より対策を強化したい場合を想定しています。ただし、「例えば」で始まる文章は、どちらも規定していません。
	-	(8) 情報機器 通信機能を持つ、PCやサーバ、ノートPCやスマートデバイス等のモバイル機器等。
4-2-2.	(5) 情報システムにおける利用者のアクセス管理 4. 利用者ID及びアクセス権の登録･変更･削除の手続きに漏れがないように、人事異動に関連する人事手続き等と連携した運用とすることが望まれます 。	(5) 情報システムにおける利用者のアクセス管理 4. 利用者ID及びアクセス権の登録･変更･削除の手続きに漏れがないように、人事異動に関連する人事手続き等と連携した運用とします 。
4-3.	(8) 物理的な保護と入退管理 1. セキュリティを強化すべき物理的領域を定め、･･･します。例えば、サーバルームへの入室の際にICカードによる認証を行うようにします。	(8) 物理的な保護と入退管理 1. セキュリティを強化すべき物理的領域を定め、･･･します。例えば、サーバルームへの入室の際にICカードやバイオメトリックスによる認証を行うようにします。

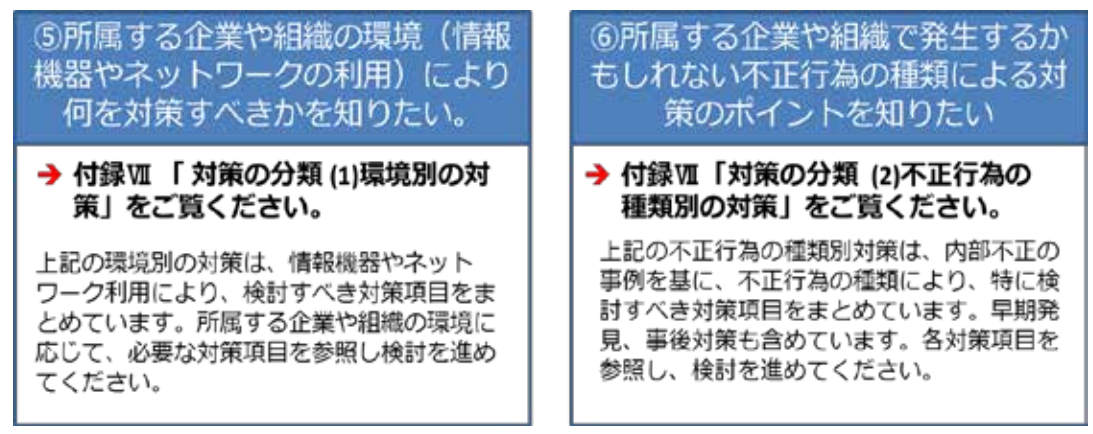
	(9) 情報機器及び記録媒体の資産管理及び物理的な保護 4.情報機器及び記録媒体を処分する際は、･･･します。さらに、CD-ROM、DVD-ROM、HDD等の記録媒体は破砕機等を用いて物理的に破壊することが望まれます。	(9) 情報機器及び記録媒体の資産管理及び物理的な保護 4.情報機器及び記録媒体を処分する際は、･･･します。さらに、CD-R、DVD-R等の記録媒体は破砕機[28]等を用いて物理的に破壊することが必要です。 28 シュレッダー等に搭載されています。
	(10) 情報機器及び記録媒体の持出管理及び監視	(10) 情報機器及び記録媒体の持出管理
	(11) 個人の情報機器及び記録媒体の業務利用及び持込の制限 3. 個人の情報機器を組織ネットワークへ接続することを許可する場合には、許可された業務システム及び業務サービスのみに接続可能とするように制限することが望まれます。	(11) 個人の情報機器及び記録媒体の業務利用及び持込の制限 3. 個人の情報機器を組織ネットワークへ接続する場合には、(12)で示す情報セキュリティ対策を実施した機器のみ許可します。その場合、許可された業務システム及び業務サービスのみに接続可能とするように制限することが望まれます。
	8. スマートデバイス等のモバイル機器や携帯可能なUSBメモリ等の外部記録媒体の利用を制限するソフトウェアを導入することで、個人の情報機器及び記録媒体による情報漏えいの対策を講じることが望まれます。	8. スマートデバイス等のモバイル機器や携帯可能なUSBメモリ等の外部記録媒体の利用を制限するソフトウェア[30]を導入することで、個人の情報機器及び記録媒体による情報漏えいの対策を講じることが望まれます。 30 ハードウェア対策としては、USBの差込口のないものやUSBの差込口が無効となっている端末の使用が挙げられます。
4-4.	(12) ネットワーク利用のための安全管理 3.電子メールに関しては･･･････望まれます。また、外部宛のメール送信を再確認する機能や、添付ファイル等が暗号化されていないと送信できないメールシステム等	(12) ネットワーク利用のための安全管理 3.電子メールに関しては･･･････望まれます。また、外部宛のメール送信を再確認する機能や上司に承認を要求する機能、及び添付ファイル等が暗号化されていないと送信できないメールシステム等
	(15) 組織外部での業務における重要情報の保護 ■どのようなリスクがあるのか？ 公共の場で････恐れがあります。	(15) 組織外部での業務における重要情報の保護 ■どのようなリスクがあるのか？ 公共の場で････恐れがあります。在宅勤務では、重要情報の機密レベルに応じたアクセス制限やPC等への格納の制限をしないと、組織の管理下にない個人所有のPC等へ重要情報が格納したり、本人以外（家族や訪問者など）がそれらの重要情報へアクセスする可能性があり、重要情報が漏えいするリスクが高まります。
	■対策のポイント 2. ホテルの有線LAN･無線LANや公衆無線LAN等の不特定の利用者が共有するネットワークの接続を許可するかどうかを判断します。	■対策のポイント 2. ホテルの有線LAN･無線LANや公衆無線LAN等の不特定の利用者が共有するネットワークの接続を許可するかどうかを判断します[33]。 33 重要情報の機密レベルによっては、ID及びパスワードによる利用者認証に加え、物理アドレスを利用した端末認証を行うといった認証の多重化や、組織外部からの接続を禁止することが望まれます。組織内においても同様に利用を制限することが望まれます。
	3. 許可されたネットワーク環境から組織ネットワークに接続する際には、VPN等を用いて通信を暗号化する必要があります。	3. 許可されたネットワーク環境から組織ネットワークに接続する際には、重要情報を暗号化したり、VPN等を用いて通信を暗号化する[34]ことが必要です。 34 組織内であっても、重要情報の機密レベルや外部関係者より判断し、必要に応じて暗号化することが望まれます。
	-	4. 組織外部から組織ネットワークに接続する場合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ます[35]。組織内の重要情報にアクセスさせる場合は、アクセス権限の割り当てをより細かく設定するなどして、必要な情報以外へのアクセスを防ぎます。 35 デスクトップの仮想化などが挙げられます。デスクトップの仮想化では、組織外部から組織内ネットワークに接続し、組織内の電子データをローカルPC（あるいはクライアントPC）等に保存することなく、閲覧や編集を行うことができ、情報のPC等への残留を防ぐことができます。
	(16) 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） 1. 業務を委託する場合、･･･、必要に応じて、委託先の体制や規程等の点検、実地検査等を実施し、その結果について、総括責任者または部門責任者等が適切に評価することが望まれます。	(16) 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） 1. 業務を委託する場合、･･･、委託先の体制や規程等の点検、委託後の監査が可能かどうかの確認、必要に応じて実地調査等を実施し、その結果について、総括責任者または部門責任者等が適切に評価することが望まれます。
4-5.	(17) 情報システムにおけるログ･証跡 の記録と保存 ■どのようなリスクがあるのか？ ログ･証跡を記録していないと、ログ･証跡から不正行為の前兆となる行為を知ることができないため、発見の遅れや、発見時に被害が大きくなっているといった恐れがあります。	(17) 情報システムにおけるログ･証跡 の記録と保存 ■どのようなリスクがあるのか？ ログ･証跡を記録し、定期的に確認していないと、ログ･証跡から不正行為の前兆となる行為を知ることができないため、発見の遅れや、発見時に被害が大きくなっているといった恐れがあります。

	■対策のポイント 内部不正の早期発見及び事後対策の観点から、以下のようにログ・証跡を記録して安全に保存します。	■対策のポイント 内部不正の早期発見及び事後対策の観点から、以下のようにログ[38]・証跡を記録して安全に保存します。 38 サーバのログだけでなく、クライアントのログ（Q&A10:P74）(Q&A11:P74)についても必要かどうか検討します。 付録III：Q&A集 対策のヒントとなるQ&A10 Q-10クライアントのログとして何をどのように採取すればいいかわかりません。（4-5（17）） A-10少なくとも、利用者の操作の日時、内容（ログオン、ログオフ）とその結果（失敗）がわかるイベントログを採取します。Windowsの場合、管理ツールで収集することが可能です。 対策のヒントとなるQ&A11 Q-11内部不正の対策として、クライアントのログに関する設定で留意するべきことは何ですか？（4-5（17）） A-11クライアントの基本ソフトウェア（特にWindows）における初期値のログ設定は、すべての動作ログを記録する設定にはなっていません。そのため、特に重要情報を保存するクライアントにおいては、Windowsの場合、セキュリティ監査を有効にすることで、ほぼすべての動作を記録することが望まれます。
	6. ログ・証跡の保存期間は、リスクとコストのバランスによって決定します。保存期間は、内部不正の抑止の観点から内部者に知らせないことが望まれます[39]。 39 ログの保存期間は、・・・存在します。	6. ログ・証跡の保存期間は、リスクとコストのバランスによって決定します。保存期間は、内部不正の抑止の観点から内部者に知らせないことが望まれます[39]。 39 組織内のシステム開発や運用の面で知らせる必要がある場合を除きます。ログの保存期間は、・・・存在します。
	（18）システム管理者のログ・証跡 の確認 ■対策のポイント 1. 情報システムの設定変更や運用に関する作業をログに記録し、定期的にその作業のログの内容をシステム管理者の上司または総括責任者41が確認します。	（18）システム管理者のログ・証跡 の確認 ■対策のポイント 1. 情報システムの設定変更や運用に関する作業をログに記録し[40]、定期的にその作業のログの内容をシステム管理者の上司または総括責任者[41]が確認します。 40 システム管理者が取得及び保存すべきログには、少なくとも、ネットワーク境界に位置する機器（ファイアーウォール、ルータ、検知システム等）の通信に関するログや、各種サーバ（Web、プロキシ、データベース、DHCP等）におけるアクセス記録及び各サーバ特有の機能が動作したことを示す記録（認証、処理、割り当て等）などがあります。
4-6.	（19）教育による内部不正対策の周知徹底 1. 内部者に順守すべき事項や背景等に関する教育をします(Q&A12:P75)。教育内容を忘れないように、教育を毎年繰り返し実施することが望まれます。 ・対策のヒントとなるQ&A10 ① 内部不正によって組織にどのような影響があるのかについて具体的事例を説明します。	（19）教育による内部不正対策の周知徹底 1. 内部者に順守すべき事項や背景等に関する教育をします(Q&A12:P75)。教育内容を忘れないように、教育を毎年繰り返し実施することが望まれます。 ・対策のヒントとなるQ&A10 ① 内部不正によって組織にどのような影響があるのかについて、自組織で発生した不正行為などを含め、具体的事例を説明します。
4-10.	（29）内部不正に関する通報制度の整備	（29）内部不正に関する通報制度の整備 2.社外から重要情報に関わる問い合わせや通報があった場合には、速やかに調査を開始するため（27）で述べた体制を整える必要があります。

②情報セキュリティに関する最新の標準規格及び指針へ対応

項目	第2版	第3版
3-2.	（2）不正競争防止法 ・・・ ■保有する重要な情報に「営業秘密」としての保護を求める場合 ノウハウ等を営業秘密として内部不正者から保護することを目的とされる場合は、経済産業省のホームページに掲載されている「営業秘密管理指針」等も参照してください。「営業秘密管理指針」の参照資料1では、・・・把握することができます。	（2） 不正競争防止法 ・・・ ■保有する重要な情報に「営業秘密」としての保護を求める場合 ノウハウ等を営業秘密として内部不正者から保護することを目的とされる場合は、経済産業省のホームページに掲載されている「営業秘密管理指針」等も参照してください。
付録IV	（1）JIS Q 27001　付属書　A	（1）JIS Q 27001　付属書　A →　※　別紙1　置換
	（2）営業秘密管理指針 営業秘密管理指針では、・・・すべてに対応する必要はありません。 （表）	（2）営業秘密管理指針 営業秘密管理指針では、不正競争防止法によって差し止め等の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が示されています。漏えい防止及び漏えい時の包括的な対策は、別途「営業秘密保護マニュアル（仮称）」に示される予定です。

③利用のためのリファレンス

項目	第2版	第3版
2-1.	-	2-1. 内部不正防止の基本原則 本ガイドラインは、状況的犯罪予防[4] の考え方を内部不正防止に応用し、以下の5つを基本原則としています[5]。 ・**犯行を難しくする**（やりにくくする）： 対策を強化することで犯罪行為を難しくする ・**捕まるリスクを高める**（やると見つかる）： 管理や監視を強化することで捕まるリスクを高める ・**犯行の見返りを減らす**（割に合わない）： 標的を隠したり、排除したり、利益を得にくくすることで犯行を防ぐ ・**犯行の誘因を減らす**（その気にさせない）： 犯罪を行う気持ちにさせないことで犯行を抑止する ・**犯罪の弁明をさせない**（言い訳させない）： 犯行者による自らの行為の正当化理由を排除する 4 犯罪学者のCornish & Clarke（2003）が提唱した都市空間における犯罪予防の理論。犯罪予防対策を実施すべき5つに分類し、更に25の犯罪予防技術に細分化しています。監視者の設置などによって外部からのコントロールが可能な「環境」を適切に定めることを主眼として、犯罪機会・動機を低減し、予防する犯罪予防策であり、直接的に犯罪を防止する対策及び間接的に犯罪を防止及び抑止する対策を含んでいます。 5 付録VIに、基本原則を更に各々5つに細分化し、その対策例と関連する本ガイドラインの対策項目をまとめていますので、ご参照ください。
2-2. 表1	表 1 本ガイドラインの構成と想定読者 ・・・・ ①～④については、図1をご覧ください。	表 1 本ガイドラインの構成と想定読者 （付録VI、付録VII追加） <table><tr><td>付録Ⅵ：内部不正の基本 5 原則と 25 分類</td><td>○</td><td>○</td></tr><tr><td>付録Ⅶ：対策の分類</td><td>－</td><td>⑤⑥</td></tr></table> ※1：「4-1.基本方針」迄をご覧ください。 ①～⑥については、図1をご覧ください。
2-2. 図1	図1 検討内容ごとの本ガイドラインの利用方法	図1 検討内容ごとの本ガイドラインの利用方法 （⑤、⑥を追加） 
付録VI	-	付録VI：内部不正の基本5原則と25分類 → ※別紙2 追加
付録VII	-	付録VII：対策の分類 → ※別紙3 追加

別紙 1

付録IV：他ガイドライン等との関係

（1）JIS Q 27001　附属書 A

本ガイドラインでは、組織が内部不正から情報資産を守る対策を示しています。情報セキュリティマネジメントは、組織が保護すべき情報資産について機密性、完全性、可用性を維持するものであり、情報資産を保護するという観点から関連する項目が多く存在します。そこで、情報セキュリティマネジメントの観点から本ガイドラインを読む方の参考として、本ガイドラインの管理策に関連する JIS Q 27001 附属書 A の管理策を以下に示します。なお、本ガイドラインの「職場環境」に対応する、JIS Q 27001 の管理策は存在しません。

大項目		項目名	JIS Q 27001:2014 附属書 A 関連項目
基本方針		（1）経営者の責任の明確化	A.5.1　情報セキュリティのための経営陣の方向性 A.7.2　雇用期間中
		（2）総括責任者の任命と組織横断的な体制構築	A.6.1　内部組織
資産管理	秘密指定	（3）情報の格付け	A.8.1　資産に対する責任 A.8.2　情報分類 A.9.1　アクセス制御に対する業務上の要求事項
		（4）格付け区分の適用とラベル付け	A.8.1　資産に対する責任 A.8.2　情報分類 A.9.1　アクセス制御に対する業務上の要求事項
	アクセス権指定	（5）情報システムにおける利用者のアクセス管理	A.8.1　資産に対する責任 A.8.2　情報分類 A.9.1　アクセス制御に対する業務上の要求事項 A.9.2　利用者アクセスの管理
		（6）システム管理者の権限管理	A.8.1　資産に対する責任 A.8.2　情報分類 A.9.1　アクセス制御に対する業務上の要求事項 A.9.2　利用者アクセスの管理
		（7）情報システムにおける利用者の識別と認証	A.8.1　資産に対する責任 A.8.2　情報分類 A.9.2　利用者アクセスの管理 A.9.3　利用者の責任
物理的管理		（8）物理的な保護と入退管理策	A.11.1 セキュリティを保つべき領域 A.12.1 運用の手順及び責任
		（9）情報機器及び記録媒体の資産管理及び物理的な保護	A.8.3　媒体の取扱い A.11.2 装置
		（１０）情報機器及び記録媒体の持出管理	A.8.3　媒体の取扱い A.11.2 装置 A.12.1 運用の手順及び責任

大項目	項目名	JIS Q 27001:2014 附属書A 関連項目
	（１１）個人の情報機器及び記録媒体の業務利用及び持込の制限	A.6.2　モバイル機器及びテレワーキング A.8.3　媒体の取扱い A.12.1 運用の手順及び責任
技術･運用管理	（１２）ネットワーク利用のための安全管理	A.6.2　モバイル機器及びテレワーキング A.12.2 マルウェアからの保護 A.12.6 技術的ぜい弱性管理 A.13.1 ネットワークセキュリティ管理 A.14.1 情報システムのセキュリティ要求事項
	（１３）重要情報の受渡し保護	A.8.3　媒体の取扱い A.13.2 情報の転送 A.14.1 情報システムのセキュリティ要求事項 A.10.1 暗号による管理策 A.12.1 運用の手順及び責任
	（１４）情報機器や記録媒体の持ち出しの保護	A.6.2　モバイル機器及びテレワーキング A.8.3　媒体の取扱い A.9.4　システム及びアプリケーションのアクセス制御 A.10.1 暗号による管理策 A.12.1 運用の手順及び責任
	（１５）組織外部での業務における重要情報の保護	A.6.2　モバイル機器及びテレワーキング A.8.3　媒体の取扱い A.9.4　システム及びアプリケーションのアクセス制御 A.11.2 装置 A.10.1 暗号による管理策
	（１６）業務委託の確認（第三者が提供するサービス利用時を含む）	A.7.1　雇用前 A.7.2　雇用期間中 A.7.3　雇用の終了及び変更 A.13.1 ネットワークセキュリティ管理 A.15.1 供給者関係における情報セキュリティ A.15.2 供給者のサービス提供の管理
証拠確保	（１７）情報システムにおけるログ・証跡の記録と保存	A.12.4 ログ取得及び監視 A.12.7 情報システムの監査に対する考慮事項
	（１８）システム管理者のログ・証跡の確認	A.12.4 ログ取得及び監視 A.12.7 情報システムの監査に対する考慮事項
人的管理	（１９）教育による内部不正対策の周知徹底	A.7.2　雇用期間中
	（２０）雇用終了の際の人事手続き	A.7.3　雇用の終了及び変更 A.18.1 法的及び契約上の要求事項の順守
	（２１）雇用終了及び契約終了による情報資産等の返却	A.8.1　資産に対する責任 A.18.1 法的及び契約上の要求事項の順守
コンプライアンス	（２２）法的手続きの整備	A.7.1　雇用前 A.7.2　雇用期間中 A.7.3　雇用の終了及び変更 A.18.1 法的及び契約上の要求事項の順守
	（２３）誓約書の要請	A.7.1　雇用前 A.7.3　雇用の終了及び変更 A.13.2 情報の転送 A.18.1 法的及び契約上の要求事項の順守

大項目	項目名	JIS Q 27001:2014 附属書A 関連項目
職場環境	（２４）公平な人事評価の整備	－
	（２５）適正な労働環境及びコミュニケーションの推進	－
	（２６）職場環境におけるマネジメント	－
事後対策	（２７）事後対策に求められる体制の整備	A.6.1　内部組織 A.15.1 供給者関係における情報セキュリティ A.16.1 情報セキュリティインシデントの管理及びその改善 A.17.1 情報セキュリティ継続
	（２８）処罰等の検討及び再発防止	A.7.2　雇用期間中 A.16.1 情報セキュリティインシデントの管理及びその改善
組織の管理	（２９）内部不正に関する通報制度の整備	A.7.2　雇用期間中 A.16.1 情報セキュリティインシデントの管理及びその改善
	（３０）内部不正防止の観点を含んだ確認の実施	A.5.1　情報セキュリティのための経営陣の方向性 A.12.6 技術的ぜい弱性管理 A.12.7 情報システムの監査に対する考慮事項 A.16.1 情報セキュリティインシデントの管理及びその改善 A.17.1 情報セキュリティ継続 A.18.2 情報セキュリティのレビュー

別紙２

付録VI：内部不正の基本 5 原則と 25 分類

状況的犯罪予防に基づく、内部不正防止の基本 5 原則と 25 分類、及び各々の対策例、関連する本ガイドラインの対策項目を以下に示します。「主な対策項目」は、本ガイドラインの対策項目の番号を表しています。

(出典)5 カテゴリ 25 分類は、社会安全研究財団：「環境犯罪学と犯罪分析」　P191 を参考とし、IPA が作成

基本 5 原則と 25 分類		対策例※	主な対策項目
犯行を難しくする(やりにくくする)：対策を強化することで犯罪行為を難しくする			
	対象の防御策を強化する	アクセス制御、パスワードポリシーの設定、退職者の ID 削除、セキュリティワイヤーによる PC 固定	(5)(6)(7)(9)(14)(21)
	施設への出入りを制限する	外部者の立ち入り制限、入退出管理	(8)
	出口で検査する	ノート PC 等の持ち出し検査、メールやネットの監視	(8)(10)(17)(18)
	犯罪者をそらす	物理レベルに応じた入退制限	(8)
	情報機器やネットワークを制限する	未許可の PC/USB メモリの持ち込み禁止､SNS の利用制限、ホテル及び公衆の無線 LAN の利用制限	(11)(12)(15)
捕まるリスクを高める（やると見つかる）：管理や監視を強化することで捕まるリスクを高める			
	監視を強化する	アクセスログの監視、複数人での作業環境、情報機器の棚卸し、モバイル機器の持出管理、入退室記録の監査	(6)(8)(9)(10)(17)(18)(30)
	自然監視を支援する	通報制度の整備	(29)
	匿名性を減らす	ID 管理、共有アカウント廃止、台帳による持出し管理	(7)(9)(10)
	現場管理者を利用する	単独作業の制限	(26)
	物理的な監視体制を強化する	監視カメラの設置、機械警備システムの導入	(8)
犯行の見返りを減らす（割に合わない）：標的を隠す/排除する、利益をなくすことで犯行を防ぐ			
	標的を隠す（存在がわからない）	アクセス権限の設定、モバイル機器等の施錠保管、覗き見防止フィルムの貼付	(5)(6)(9)(15)
	対象を排除する（存在をなくす）	データの完全消去、記録媒体等の物理的な破壊、関係者に開示した情報の廃棄・消去	(4)(9)(13)(21)
	所有物を特定する	情報機器及び記録媒体の資産管理	(9)
	市場を阻止する	警察への迅速な届出、（法制度対応）	(27)
	利益を得にくくする	電子ファイル・ハードディスク・通信の暗号化	(12)(13)(14)(15)
犯行の誘因を減らす（その気にさせない）：犯罪を行う気持ちにさせないことで犯行を抑止する			
	欲求不満やストレスを減らす	公正な人事評価、適正な労働環境、円滑なコミュニケーションの推進	(24)(25)
	対立（紛争）を避ける	公正な人事評価、適正な労働環境、円滑なコミュニケーションの推進	(24)(25)（29)
	感情の高ぶりを抑える	公正な人事評価、適正な労働環境、円滑なコミュニケーションの推進	(24)(25)
	仲間からの圧力を緩和する	公正な人事評価、適正な労働環境、円滑なコミュニケーションの推進	(25)
	模倣犯を阻止する	再発防止策、(インシデントの手口の公表を慎重にする)	(28)
犯罪の弁明をさせない（言い訳させない）：犯行者による自らの行為の正当化理由を排除する			
	規則を決める	基本方針の策定、管理・運用策の策定、業務委託契約、就業規則、	(1)(2)(16)(20)(22)(27)
	指示を掲示する	基本方針の組織内外への掲示、教育による周知徹底、	(1)(2)(19)
	良心に警告する	管理レベルの表示、誓約書へのサイン、持ち込禁止のポスター	(3)(4)(11)(19)(20)(23)
	コンプライアンスを支援する	順守事項や関連法などの教育	(19)(22)(23)
	薬物・アルコールを規制する	（職場での飲酒禁止、重要情報保持時の飲酒制限）	-

※対策例の( )は、本ガイドラインの対策項目以外の例です。

別紙３

付録Ⅶ：対策の分類

（1）環境別の対策

企業や組織のおかれている環境（情報機器やネットワークの利用）別に、検討すべき対策項目を示します[1]。

①情報機器の利用やネットワーク環境に関わらず、どのような組織でも検討すべき対策

②組織内に、情報機器はあるが、ネットワークは存在しない（ただし、通信事業者が提供するメールサービスの利用など、外部との接続はある）場合に検討すべき対策

③組織内にネットワークが存在し、外部との接続もある場合に検討すべき対策

①どのような組織でも検討すべき対策内容

大項目	項目名
4-1 基本方針(経営者の責任、ガバナンス)	(1)経営者の責任の明確化
	(2)総括責任者の任命と組織横断的な体制構築
4-2 資産管理(秘密指定、アクセス権指定、アクセス管理等) 4-2-1 秘密指定	(3)情報の格付け区分
	(4)格付け区分の適用とラベル付け
4-3 物理的管理	(8)物理的な保護と入退管理
4-4 技術･運用管理	(13)重要情報の受渡し保護※1
	(16)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）※2
4-6 人的管理	(19)教育による内部不正対策の周知徹底
	(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
4-7 コンプライアンス	(22)法的手続きの整備
	(23)誓約書の要請
4-8 職場環境	(24)公平な人事評価の整備
	(25)適正な労働環境及びコミュニケーションの推進
	(26)職場環境におけるマネジメント
4-9 事後対策	(27)事後対策に求められる体制の整備
	(28)処罰等の検討及び再発防止
4-10 組織の管理	(29)内部不正に関する通報制度の整備
	(30)内部不正防止の観点を含んだ確認の実施

※1 ただし、「対策のポイント」の 3 (インターネット経由の場合) は除く

※2 ただし、「対策のポイント」の 5 (クラウドサービスを利用) は除く

[1] **本ガイドラインは、情報システムの利用によるセキュリティ対策を主眼においているため、情報機器やネットワークを利用しない組織の対策については、参考として検討してください。**

②組織内に情報機器が存在する場合

大項目	項目名
4-3 物理的管理	(9)情報機器及び記録媒体の資産管理及び物理的な保護
	(10)情報機器及び記録媒体の持出管理
	(11)個人の情報機器及び記録媒体の業務利用及び持込の制限
4-4 技術･運用管理	(12)ネットワーク利用のための安全管理
	(14)情報機器や記録媒体の持ち出しの保護
	(15)組織外部での業務における重要情報の保護

③組織内にネットワークが存在する場合

大項目	項目名
4-2-2 アクセス権指定	(5)情報システムにおける利用者のアクセス管理
	(6)システム管理者の権限管理
	(7)情報システムにおける利用者の識別と認証
4-4 技術･運用管理	(12)ネットワーク利用のための安全管理
	(13)重要情報の受渡し保護※1
	(16)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）※2
4-5 証拠確保	(17)情報システムにおけるログ・証跡の記録と保存
	(18)システム管理者のログ・証跡の確認

※1 「対策のポイント」の 3 (インターネット経由の場合)

※2 「対策のポイント」の 5 (クラウドサービスを利用)

（2）不正行為の種類別の対策

不正行為の種類別に、検討すべき対策項目を示します。合わせて、早期発見、事後対策に関する対策項目を示します。

①組織として検討すべき基本対策

②不正行為の種類別に検討すべき対策

③不正行為の兆候の把握や早期発見のための対策

④内部不正が発生した際の対策

①基本対策

危険要因	対策	項目名
従業員が重要情報かどうか認識できない	①重要情報の特定	(3)情報の格付け (4)格付け区分の適用とラベル付け
組織横断的な管理体制が構築されていない 新たな脅威や法律等に対し、対策の改善、見直しができていない	②経営者主導による組織横断の取り組み	(1)経営者の責任の明確化 (2)総括責任者の任命と組織横断的な体制構築 (30)内部不正防止の観点を含んだ確認の実施
重要情報が保管されているフロアに容易に入れる 個人が特定できる入退室の記録が取られていない 情報機器等の棚卸ができていない	③物理的な管理	(8)物理的な管理と入退管理 (9)情報機器及び記録媒体の試算管理及び物理的な保護
業務に必要な範囲を超えてアクセス権を付与している	④適切なアクセス権限管理(Need to Know、Least Privilege)	(5)情報システムにおける利用者のアクセス管理 (6)システム管理の権限管理
操作履歴(ログ)を採取していない 採取したログの定期監査をしていない	⑤定期的な操作履歴の監視、監査	(17)情報システムにおけるログ・証跡の記録と保存 (18)システム管理者のログ・証跡の確認
重要情報の取り扱い等の社内ルールが周知されていない 社内での管理方法(ログ監視等)、不正発覚時の懲戒処分を知らない	⑥教育による周知徹底	(19)教育による内部不正対策の周知徹底
重要情報を保護する義務があることを理解していない	⑦コンプライアンスの意識付け	(23)誓約書の要請

②不正行為の種類別の対策

a.退職にともなう情報漏えい

危険要因	対策	項目名
従業員(退職予定者含む)の監視ができていない	①退職前の監視強化	(10)情報機器及び記録媒体の持出管理 (17)情報システムにおけるログ・証跡の記録と保存 (21)雇用終了及び契約終了による情報資産等の返却
重要な情報にアクセスできる		
在職中に取得した入館証やアカウントが使える	②退職時の手続き	(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
退職後の秘密保持策や競業避止対策が未整備		

b.システム管理者による不正行為

危険要因	対策	項目名
権限が集中している 必要以上の要員に権限が付与されている	① 切な権限管理 （権限最小化､権限分散、相互監視）	(6)システム管理の権限管理 (7)情報システムにおける利用者の識別と認証
特権の使用が限定されていない		
重要情報にアクセスしたシステム管理者が特定できない		
システム管理者の監視ができていない	②システム管理者の監視	(18)システム管理者のログ・証跡の確認

c.委託先からの情報漏えい等

危険要因	対策	項目名
契約前及び契約期間中、委託先の体制やセキュリティ対策をチェックできていない	①重要情報の取り扱いに関する委託先管理	(2)総括責任者の任命と組織横断的な体制構築 (16)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) (27)事後対策に求められる体制の整備
重要情報の安全管理に必要な事項が契約に盛り込まれていない※	②契約への安全管理事項の盛り込み	
委託先との重要情報の受け渡し、廃棄・削除の手続きが定められていない	③重要情報の受け渡し保護	(13)重要情報の受渡し保護 (21)雇用終了及び契約終了による情報資産等の返却

※クラウドサービス利用時を含む

d.職場環境に起因する不正行為

危険要因	対策	項目名
人事評価に納得しておらず、不満がある	①公平な人事評価	(24)公平な人事評価の整備 (25)適正な労働環境及びコミュニケーションの推進 (26)職場環境におけるマネジメント
ある社員が、特定の業務を長期間担当している	②適切な労働環境	
特定の社員の業務量が過大になっている		
業務の悩みを誰にも相談できない、孤立している	③良好なコミュニケーション	
単独作業が多い		

e.ルール不徹底に起因する不正行為

危険要因	対策	項目名
重要情報の取り扱い等の社内ルールが周知されていない	①教育による周知徹底	(19)教育による内部不正対策の周知徹底
私物のスマートフォンやUSBメモリ等の持込み、業務利用が制限されていない ルールが明確でない	②情報漏えい対策	(10)情報機器及び記録媒体の持出管理 (11)個人の情報機器及び記録媒体の業務利用及び持込の制限
無許可アプリやSNS等の使用を制限できていない		(12)ネットワーク利用のための安全管理
情報が第三者に流出した場合を想定した対策ができていない		(14)情報機器や記録媒体の持ち出しの保護 (15)組織外部での業務における重要情報の保護

③早期発見

危険要因	対策	項目名
疑わしい行為を見つけたが、どこに相談したらいいかわからない	①通報制度の整備	(29)内部不正に関する通報制度の整備
ログの定期監査をしていない	②定期的な操作履歴の監視、監査	(17)情報システムにおけるログ・証跡の記録と保存 (18)システム管理者のログ・証跡の確認

④事後対策

危険要因	対策	項目名
内部不正が発生した際の対応がわからない 自社及び顧客、取引先などの被害を最小限に抑えたい	①対応手順、報告手順の事前の取り決め	(27)事後対策に求められる体制の整備
内部不正の再発を防止したい	②処罰の検討と再発防止	(22)法的手続きの整備 (28)処罰等の検討及び再発防止