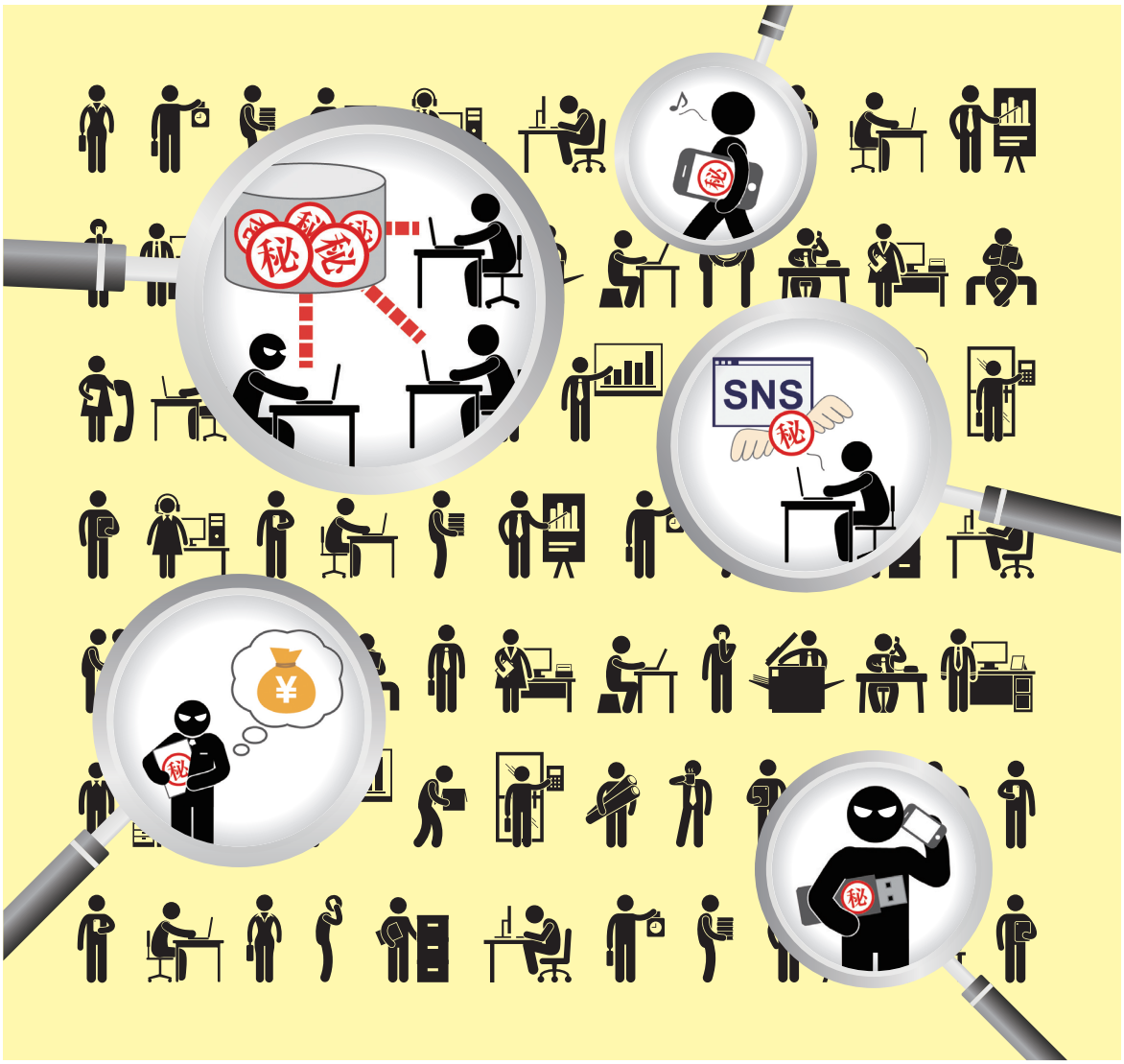
IPA

組織における
内部不正防止ガイドライン



独立行政法人 情報処理推進機構

目 次

1. 背景

近年、企業やその他の組織において、内部不正による情報セキュリティ事故が原因で事業の根幹を脅かすようなケースが目立つようになってきました。その典型例としては、社員や職員等によって顧客情報が不正に売られたことによる個人情報の大量漏えいや、製品情報が退職の際に不正に持ち出されたことによる技術情報の漏えい等が挙げられます。他にも、悪意はないにしても、自宅で業務を行うために社内情報を無断で持ち出し、自宅 PC から漏えいさせてしまう例も見られます。これら内部不正に関わる情報セキュリティ事故が毎年変わらず発生していることは、広く報道されています。

内部不正に関わる事故については、JNSA（特定非営利活動法人 日本ネットワークセキュリティ協会）の調査報告[1]によれば、2005 年～2010 年の内部犯罪・内部不正行為による個人情報漏えいの発生件数は全体のわずか 1%程度であるのに対して、漏えいした個人情報の数は約 25%程度（全体の 1/4 近く）となっています。このように外部からの攻撃よりも 1 件あたりの被害が大きい場合が少なくないことから、ひとたび発生してしまうと事業に大きな影響があることを覚悟しなければなりません。また、経済産業省の調査[2]において、営業秘密の漏えいがあった企業では漏えい経路が「中途退職者(正規社員)による漏えい（50.3%)」、「現職従業員等のミスによる漏えい（26.9%)」、「金銭目的等の動機をもった現職従業員等による漏えい（10.9%)」と報告されています。このように、競争力につながる価値ある営業情報の漏えいは、内部の関係者によるものが多くを占めます。このため、内部不正は、組織における脅威の一つと位置づけられるので、経営課題として経営者・経営陣が真摯に取り組まなければなりません。

内部不正に関わる事故は、風評被害が発生する恐れがあることや、関係者との調整がつかない等の理由から組織内部で処理されてしまう傾向にあり、組織の外部に知られることは稀です。したがって、報道や判例で公開された事故以外にも、裁判に至らない事故や内部規程違反の未公表の事件が多く存在することは想像に難くありません。このように組織間で内部不正に関する情報が共有されていないため、社会での実態を把握するのが困難です。それに

---

[1] JNSA の「情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～」

[2] 経済産業省の「営業秘密の管理実態に関するアンケート」調査結果（確報版）
URL: http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/121211HP.pdf

加えて、内部不正の発生する要因や効果的な対策等について組織を越えた検討も困難な状況にあります。現状、組織を越えた検討ができないため、それぞれの組織が経験等をもとに個別の対策を講じているのが実情です。また、独立行政法人情報処理推進機構（以下、IPA と言います）のインタビュー調査[3]において、リスクを小さく捉えて対策を講じていなかったために、事故を発生させてしまった企業が見られました。こうした軽視は内部不正に関わる情報が共有されておらず、脅威への認識不足が影響しているとも考えられます。これらの企業では、「自社では内部不正は発生しないだろう」「自社の従業員に不正行為をするものはいない」と考えて、リスクを軽視していました。このように、組織内部だけの検討で対策を進めると、そもそも対策の必要性に気づかないということも起こり得るのです。

内部不正対策を講じていないと、事故発生を防止できない可能性があるのはもちろん、事故発生に気づかないために被害が拡大し関係者に迷惑が及んで初めて発覚するようなケースや、原因不明で事故を解明できないケース等、事後対策に支障をきたすこともあります。さらに、不正行為を行った者を特定できたとしても、注意義務を怠っていたとして、懲戒処分が無効になってしまったり、訴訟が困難になってしまうケースさえ考えられます。

IPA は、組織における内部不正防止ガイドライン（以降、本ガイドラインと言います）を作成・公開して、組織における内部不正の防止を推進します。本ガイドラインにより、これまで内部不正対策について「考えてこなかった」「何をすればよいかわからなかった」という企業（特に中小企業に重きをおいて）であっても、効果的な内部不正対策を整備できます。

2014 年 9 月の改訂（2.0 版）にあたって

2014 年前半、退職者による海外への技術流出や従業員による不正な情報の窃取など、内部者の不正行為によるセキュリティ事故が相次いで報道され、さらに教育関係事業者において委託先の従業員により極めて大量の顧客情報が漏えいするという事故が発生しました。これらの事例を分析し得られた効果的な対策を本ガイドラインに反映しました。

2.0 版の主な改訂ポイントは次の 3 点です。

・経営層によるリーダーシップの強化

[3] 組織内部者の不正行為によるインシデント調査報告書（2012 年 7 月）
URL: https://www.ipa.go.jp/security/fy23/reports/insider/

・情報システム管理運用の委託における監督強化
・高度化する情報通信技術への対応

また、上記の対策強化に伴い内部不正チェックシートの改訂、および内部不正事例集への事例追加、個人情報の保護に関連する本ガイドラインの対策項目一覧の追加を行いました。

2015 年 3 月の改訂（第 3 版）

本ガイドラインを使い易くし、より広く活用していただくため、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。

第 3 版の主な改訂ポイントは次の 3 点です。
・本ガイドラインに対する企業等からの要望への対応
・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への対応
・本ガイドライン利用の参考となる基本原則及び対策分類の追加

2017 年 1 月の改訂（第 4 版）

新たな法制度の施行や情報セキュリティに関連した新たなガイドライン等に対応するとともに、IPA が実施した内部不正に関する調査結果[4]及び本ガイドラインに対する要望を反映しました。

第 4 版の主な改訂ポイントは次の 3 点です。
・新たな法制度及び情報セキュリティに関連したガイドライン等への対応
・内部不正事例、コラムの追加
・本ガイドラインに対する企業等からの要望への対応

[4] 内部不正による情報セキュリティインシデント実態調査報告書（2016 年 3 月）
URL: https://www.ipa.go.jp/security/fy27/reports/insider/

2. 概要

本ガイドラインは、組織における内部不正の防止を主眼としています。なお、内部不正が発生してしまうことも考慮し、その後の早期発見と拡大防止も視野に入れています。

内部不正から保護する対象は、組織が管理する情報及び情報システムとしており、情報の記録媒体としての紙は対象外とします。ただし、情報システム内の情報を紙にプリントアウトする行為は含みます。

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[5]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[6]。

- **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

---

[5] 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。

[6] 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.本ガイドラインの構成と活用方法

本ガイドラインは以下の構成となっており、前半の「1 章 背景」「2 章 概要」と後半の「3 章 用語の定義と関連する法律」「4 章 内部不正を防ぐための管理のあり方」の大きく 2 つに分かれています。

表 1 本ガイドラインの構成と想定読者

本ガイドラインの構成	想定読者	
	経営者	対策実施者
1 章 背景	○	○
2 章 概要	○	○
3 章 用語の定義と関連する法律	○	○
4 章 内部不正を防ぐための管理のあり方	○※1	○
付録Ⅰ：内部不正事例集	–	②
付録Ⅱ：内部不正チェックシート	–	① ④
付録Ⅲ：Q&A 集	–	○
付録Ⅳ：他のガイドライン等との関係	–	③
付録Ⅴ：基本方針の記述例	○	○
付録Ⅵ：内部不正の基本 5 原則と 25 分類	○	○
付録Ⅶ：対策の分類	–	⑤ ⑥

※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。

1 章、2 章は、本ガイドラインの位置づけ及び利用方法を示すもので、すべての読者に読んでいただくべき内容となっています。対策の実施者のみでなく、経営者（経営陣）[7]を想定読者としており、内部不正防止の重要性や、本ガイドラインの概要と活用方法について述べています。情報セキュリティに関わる内部不正の脅威については、「付録Ⅰ：内部不正事例集」を読むと、対策の重要性をより深く理解できます。

[7] 会社の規模や運営方針、及び形態によって異なるため、本ガイドラインでは、主要な取締役を指すものとします。

４章は、経営者（経営陣）から対策を任された対策の実施者が、具体的な対策を策定するための内容となっています。ただし、経営者は組織での役割の把握のために「4 章 4-1.基本方針」に目を通してください。対策の実施者は、はじめに付録Ⅱのチェックシートによって、組織の内部不正対策について状況を把握してください。もし、チェックシートの結果から対策が不十分な項目があれば、「4. 内部不正を防ぐための管理のあり方」及び「付録Ⅲ：Q&A 集」を参考にして、具体的な対策を検討してください。図１に、検討内容に合わせた本ガイドラインの利用方法を示しますので、合わせて参照ください。

図 1　検討内容ごとの本ガイドラインの利用方法

2-3.内部不正対策の体制構築の重要性

本ガイドラインを活用して効果的・効率的に内部不正対策をするためには、経営者が内部不正対策に関して組織の内外に責任を持ち、積極的に関与し推進していくことが必要です。経営者の関与は、組織内における内部不正対策に関わる意識の向上を図る上でも、実施策の周知徹底を図る上でも重要な役割を果たします。

また、具体的な実施策の策定及び周知徹底には、組織全体での取り組みが不可欠です。内部不正防止の対策は複数の関係者（関係部門）の業務に及ぶため、これら関係者で協力して実施策を策定することが必要です。情報資産の保護に関する実施策を策定することからすれば、少なくとも、情報システム担当者／部門、事務担当者／部門、人事担当者／部門が関係するものと考えられます。例えば、情報システムを扱う業務を変更する場合には、情報システム部門やその業務の主管部門のみによる措置だけでなく、変更内容について人事担当者／部門が教育することが必要です。また、法務部門による法的な確認も必要となることがあります。このように、実施策の周知徹底や教育等にあたっては、組織内において対策漏れがないように、指示が組織全体に伝わり、実施状況が集約されて経営者が把握できるような体制作りが必要です。

2-4.内部不正対策の体制

内部不正対策の体制では、2-2 で述べたように組織内に関係する様々な部門が存在しており、それら部門を統括・仲介する「最高責任者」「総括責任者」の役割が重要です。

内部不正対策は、会社法[8]や金融商品取引法[9]で求められている内部統制と、リスク管理の面から密接な関係があり、体制の面でも重なる部分があります。このため、既存の内部統制の体制を利用することで効率的かつ効果的な体制構築が可能となります。

以下では、内部不正対策の体制構築について、内部統制の体制を参照して説明します。説明では、体制のポイントとなる「最高責任者」、「総括責任者」、「各部門／担当者」の役割の観点から述べます。図 2 に内部不正対策の体制例を示しますので、合わせて参照してください。

---

[8] 会社法では、内部統制システムの構築に関する重要な規則及び体制等の基本方針は取締役会での決議事項とされています（会社法第 348 条第 3 項第 4 号、第 362 条第 4 項第 6 号、第 416 条第 1 項第 1 号ホ）。なお、本ガイドラインでは、企業に取締役会が存在しない場合は、取締役が決定する事項としています。

[9] 米国の企業改革法（SOX 法、Sarbanes-Oxley Act of 2002）及び日本版 SOX 法（J-SOX 法）においても同様に内部統制の構築が求められます。

2-4-1.最高責任者

内部不正対策においても内部統制と同様に、最高責任者等の役割を定めることが必要です。内部不正対策には、予算や人事権が必要であり、責任をもってそれらの権限を実施する責任者が必要です。本ガイドラインでは、この役割を担う者を最高責任者とします。最高責任者は、内部不正対策の基本方針を策定し、これを取締役会の決議で決定します。また、最高責任者は、企業等の経営を理解し、具体的な対策を実施・推進する役割である総括責任者を任命します。

2-4-2.総括責任者

内部不正対策を具体的に推進する役割を定めます。本ガイドラインでは、この役割を担う者を「総括責任者」とします。総括責任者は、組織全体の具体的な対策を実施及び確認するとともに、各事業部門と経営者を仲介する役割を担います。この仲介という役割は内部統制における内部統制委員会等の役割でもあります。そこで、組織に内部統制委員会等が存在する場合には、体制構築の手間を小さくするために、委員会の委員が総括責任者を兼任することが望ましいと言えます。

2-4-3.総括責任者の任命について

内部不正対策のために、すべての企業や組織で内部統制委員会等の体制を構築しなければならないわけではありません。小規模な企業の場合は、内部統制に関する体制が十分でなく、内部統制委員会等が設置されていないことがあります。このような場合にも、内部不正対策の総括責任者を新たに置けば、委員会を設置しなくても、内部不正対策の体制を整えることが可能です。

総括責任者は、企業の規模や形態によって、CISO[10]や CPO[11]が兼任する場合や、経営者（最高責任者）が兼任する場合も考えられます。例えば、企業の規模が比較的小規模である場合は、大規模な企業に比べ経営者の目が組織全体に届くため、経営者自らが内部不正対策に取り組むことで、素早く効果的な対策を講じることが可能です。このような場合は、経営

---

[10] CISO（Chief Information Security Officer）は、経営層から任命される最高情報セキュリティ責任者であり、企業や組織において情報セキュリティの全体の責任を担います。本書では、このような役割を CISO として説明を行います。

[11] CPO（Chief Privacy Officer）は、経営層から任命される個人情報保護管理者であり、企業や組織において個人データの安全管理に関する責任及び権限を有します。本書では、このような役割を CPO として説明を行います。

者が最高責任者と総括責任者を兼任し、体制を整備・構築することも考えられます。詳細は、「Q&A1」及び「付録Ⅴ：基本方針の記述例」を参照してください。

2-4-4.各部門／担当者の参画及び協力体制

本ガイドラインで扱う内部不正対策の取り組みは、内部統制の中でも特に、「IT に係る全般統制」に関係しますが、IT の専門的な知見を有する情報システム部門だけが参加すればよいというものではありません。内部不正対策においては、例えば、総務部門における職場環境の整備、人事部門における教育及び各種内部規程の整備のように、多くの部門が関係する総合的な対策が求められるため、様々な部門や担当者の積極的な参画・協力が必要です。また、これらの部門の規模が大きい場合には、部門ごとの責任者の参画も必要です。

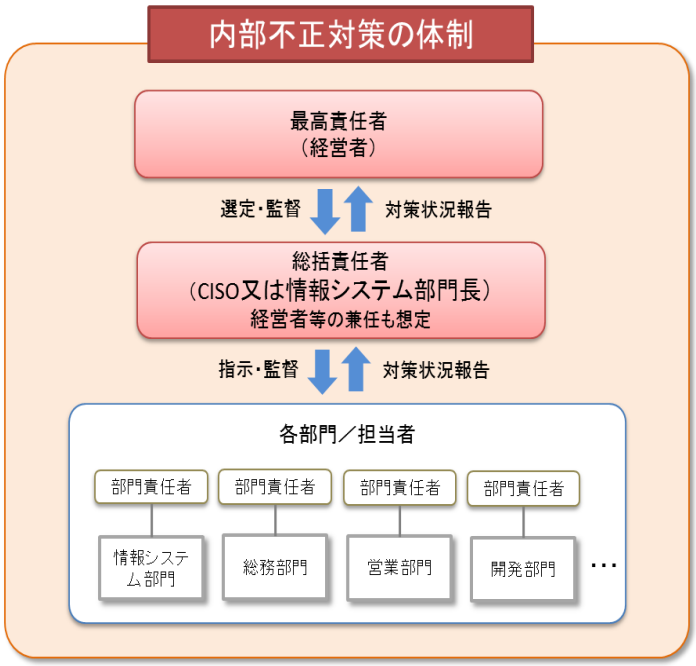


図 2　内部不正対策の体制図

・最高責任者：経営者であり、会社法等の法令及び取締役会決議に従い、内部不正対策に関して意思決定を行う最高責任を負います。

・総括責任者：内部不正対策の体制の総括的な責任者であり、会社法等の法令に従い、経営者により任命されます。経営者の基本方針に基づき組織全体の具体的な管理策の作成及び管理策に基づいた対策を実施し、対策状況を確認するとともに、見直しを行います。

・部門責任者（部門規模が大きい場合）：各部門から当該部門の責任者として任命されます。総括責任者の指示のもと、自らが担当する部門における対策を実施し、対策状況を確認するとともに、見直しを行います。

3. 用語の定義と関連する法律

ここでは､本ガイドラインにおいて用いる用語の定義及び関連する法律の概要について述べます。

3-1.用語

(1) 組織

企業、地方公共団体等の法人その他団体とします。

(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。）又は、役職員であった者のうち、以下の 2 つのどちらかでも満たした者とします。

・組織の情報システムや情報（ネットワーク、システム、データ）に対して直接又はネットワークを介したアクセス権限を有する者
・物理的にアクセスしうる職務についている者（清掃員や警備員等を除く）

(3) 内部不正

本ガイドラインでは、違法行為だけでなく、情報セキュリティに関する内部規程違反等の違法とまではいえない不正行為も内部不正に含めます。内部不正の行為としては、重要情報や情報システム等の情報資産の窃取、持ち出し、漏えい、消去・破壊等を対象とします。また、内部者が退職後に在職中に得ていた情報を漏えいする行為等についても、内部不正として取り扱います。

(4) 重要情報

組織が活用する情報のうち、以下の特徴を持ったものをいう。

その情報に対する内部不正により事業に影響を及ぼす可能性があるもので､企業や組織は､情報が重要情報か否かを適切に判断します。また、重要情報には、格付けによって重要度を付与し、重要度ごとに取り扱いを定めます（(3) 情報の格付け区分を参照)。

(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。

3-2.関連する法律

本ガイドラインに関連する法律を以下に概説します。ここに記載した関連する法律等を網羅的に検討して対策するためには、法務部門担当者及び人事部門、総務部門と検討することが必要です。

(1) 個人情報の保護に関する法律（個人情報保護法）

個人情報の漏えいや不正利用等から、個人の権利利益を保護するために、個人情報を取り扱う事業者の順守すべき義務（安全管理措置や従業員と委託先の監督義務等）を規定しています。この義務規定に事業者が違反し、不適切な個人情報の取り扱いを行っている場合には、事業を所管する主務大臣が事業者に対し勧告、命令等の措置をとることができます。命令に従わなかった場合には、罰則の対象になります。

■重要情報に「個人情報」としての保護が必要な場合

企業や組織が管理する個人情報を内部不正から保護することを目的として本ガイドラインを利用する場合は、「個人情報の保護に関する法律についてのガイドライン（通則編）（法第 2 条関連、法第 20 条関連から法第 22 条関連等）」もご確認ください。

本ガイドラインとの関係については、「付録Ⅳ：他ガイドライン等との関係」の(3)を参照願います。

(2) 行政手続における特定の個人を識別するための番号の利用等に関する法律（マイナンバー法）

マイナンバー法では、マイナンバーをその内容に含む個人情報（以下、特定個人情報という）の利用範囲を限定する等、一般の個人情報よりも厳格な保護措置を定めています。正当な理由なく特定個人情報を提供したり、業務で知りえたマイナンバーを不正な利益を図る目的で第三者に提供・盗用した場合等の不正行為に対し、直接罰（行政命令等を経ることなく直ちに個人や組織に、刑事罰が適用されるもの）が設けられています。マイナンバーを取り扱う事業者には、マイナンバー及び特定個人情報の漏えいや不正利用を防ぐため、必要かつ適切な安全管理措置や従業者に対する監督が求められています。

■重要情報に「特定個人情報」としての保護が必要な場合

企業や組織が管理する特定個人情報を内部不正から保護することを目的として本ガイドラインを利用する場合は、個人情報保護委員会の「特定個人情報の適正な取扱いに関するガイドライン」もご確認ください。

本ガイドラインとの関係については「付録Ⅳ：他ガイドライン等との関係」の(4)を参照願います。

(3) 不正競争防止法

不正競争防止法では「営業秘密」の保護に関する規定が置かれており、内部者等が営業秘密を不正に使用・開示等を行うことに対して、民事上の差止請求等が認められているとともに、違法性の高い侵害行為については刑事罰も適用されます。ただし、営業秘密として認められるには、その情報が有用かつ公然と知られておらず、秘密として管理されていることが必要です。

本ガイドラインは、営業秘密を含む重要な情報の取扱方法等を示しており、営業秘密を保護するために有益な情報が記載されていると考えています。一方で、営業秘密としての保護（を求めるための管理措置）という観点からは、本ガイドラインで示す全ての対策が求められるわけではありません。

■保有する重要情報に「営業秘密」としての保護が必要な場合

ノウハウ等の営業秘密を内部不正者から保護することを目的として本ガイドラインを利用する場合は、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。

本ガイドラインとの関係については、「付録Ⅳ：他ガイドライン等との関係」の(2)を参照願います。

(4) 労働契約法

従業員が在職中に漏えい等の内部不正を起こした場合に、従業員が労働契約に違反していることで、解雇・懲戒処分、損害賠償請求等を行う場合に関係します。ただし、具体的な解

雇等の懲戒処分の効力は、労働法上の判断枠組みに基づいて判断されることになります。さらに、従業員の内部不正によって会社に損害が生じた場合に、その従業員は労働契約上の債務不履行若しくは不法行為に基づく損害賠償請求の対象となることもあります。

(5) 労働者派遣法

従業員は、労働契約に付随する義務として秘密保持義務を負いますが、派遣先企業と派遣労働者との間には労働契約が存在しません。派遣先企業は、派遣労働者に秘密保持義務を直接負わせることはできないため、企業を介して派遣労働者に秘密保持をさせるためには、労働者派遣法への考慮が必要です[12]。

(6) その他

内部者による不正行為に関連する法制度としては、上記以外にも刑法（例えば窃盗罪、横領罪、背任罪等）や民法（例えば契約責任、不法行為責任等）、労働法理（例えば秘密保持義務違反、競業避止義務違反等）、公益通報者保護法も存在します。

[12] 詳細は（２３）を参照してください。

4. 内部不正を防ぐための管理のあり方

本節では、組織内において具体的な内部不正対策を講じるために、以下の 10 の観点から必要な対策をできる限り網羅的に示します。

4-1. 基本方針
4-2. 資産管理
4-3. 物理的管理
4-4. 技術・運用管理
4-5. 証拠確保
4-6. 人的管理
4-7. コンプライアンス
4-8. 職場環境
4-9. 事後対策
4-10. 組織の管理

これら 10 の観点のもと 30 項目の対策を示しています。ただし、複数の内部不正を想定して示しているため、特定の内部不正のみを対象とする場合には、全ての対策を実施すると必要以上の対策となることもある点に注意してください。

次に、30 項目の対策に関する検討の流れについて説明します。対策の検討にあたっては、リスク（事業に与える影響）を許容できるかどうかの検討が必要です。例えば、あるリスクを許容すれば、そのリスクに関係するすべての項目の対策を講じる必要がないこともあり得ます。ただし、内部不正が発生した場合の事後の法的手続きを考慮すると、「4-2. 資産管理」「4-6. 人的管理」「4-7. コンプライアンス」のリスクを許容することは望ましくありません。これらの項目は、組織ではなく内部不正者に非があることを示すために必要なものだからです。

30 項目の各対策は、図 3 のように以下の 3 点から構成されています。

・「対策の指針」:

必要な対策を枠で囲み示しています。チェックシートの項目[13]でもあります。ここで対策の概要を掴んでください。

・「どのようなリスクがあるか」:

対策をとらなかった場合にどのようなリスクがあるかを示しています。対策の必要性を理解してください。

・「対策のポイント」:

リスクに対する具体的な対策を立案するためのヒントとしてください。

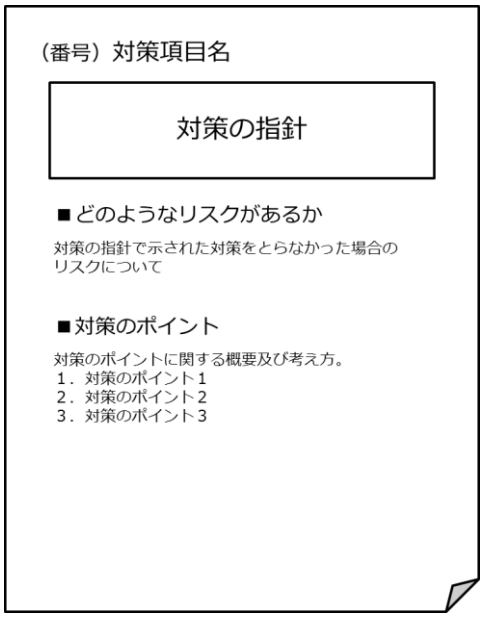


図 3　各対策の構成概要

以下のように、「対策の指針」から「対策のポイント」へと順番に読み進めながら具体的な対策を検討してください。項目によっては複数の関係者（関係部門）に関連するものがあるため、これらの関係者の参画が必要です。各項目の関係者（関係部門）は、「付録Ⅱ：チェックシート」に記載されているので参照してください。

[13] 本ガイドラインでは「対策の方針」をまとめ、内部不正対策の状況を確認するための「チェックシート」を付録Ⅱに付帯しています。また、チェックシートは以下の Web ページでも公開しております。
URL: https://www.ipa.go.jp/security/fy24/reports/insider/

(1)「対策の指針」を読んで、対策の概要を捉えてください。

(2)「どのようなリスクがあるか」を読んで、「対策の指針」で示された対策をとらなかった場合のリスクを理解してください。ここで、情報セキュリティの事故が発生した場合に、事業に与える影響を考えてください。事業に与える影響が小さく、リスクを許容できると判断した場合は、必ずしも対策を講じる必要はありません。

(3) (2)の事業に与える影響を踏まえ、「対策のポイント」を参考にコストやリソース等を考慮して具体的な実施策を立案します。補足のために、「付録Ⅲ：Q&A 集」や「付録Ⅳ：他のガイドラインとの関係」を付けています。これらの付録も参考にして、具体的な実施策を立案してください。

社会背景や企業規模等によって、(2)の許容可能なリスクが変化することから、(3)で立案した具体的な実施策を定期的に見直すことが望ましいと言えます。また、本ガイドラインも、社会背景や IT の発展とともに改訂されていくと想定されるため、本ガイドライン改訂のタイミングでの見直しも効果的です。

4-1.基本方針（経営者の責任、ガバナンス）

組織における内部不正防止では、組織全体において効果的な対策を推進する上で経営者の関与が非常に重要であり、経営者のリーダーシップによる基本方針の策定及び組織的な管理体制の構築が必要です[14]。経営者は経営課題の１つとして、内部不正対策を捉えなければなりません。その際には、情報資産に関わる機密性[15]、完全性[16]、可用性[17]の観点からリスク管理の一環として、内部不正対策を検討することが重要です。

経営者が主導する形で、内部不正対策の体制と仕組みを構築し、運用させることで内部不正防止に対する意識や取り組みを組織内に徹底させることが可能となります。そして、結果的に個人情報保護及び内部統制強化、企業に対する法的要請等にも対応できることになります。

---

[14] 経済産業省「サイバーセキュリティ経営ガイドライン」では、経営者のリーダーシップによってサイバーセキュリティ対策を推進するため、サイバー攻撃から企業を守る観点より、経営者が認識すべき３原則と、経営者がセキュリティの担当幹部（CISO 等）に指示をすべき重要１０項目をまとめています。

[15] 情報へのアクセスを許可された人だけが情報を使うことができるようにすること。例えば、情報を漏えいしないことです。

[16] 情報及び情報の処理方法が正確であり、権限のない者による情報の改変がないこと。例えば、情報を改ざんされないことです。

[17] 情報へのアクセスを許可された利用者が、必要なときはいつでも情報や情報システムにアクセスできるようにすること。例えば、システム障害が発生し、情報や情報システムが利用できない状態にならないことです。

（１） 経営者の責任の明確化

①内部不正対策は経営者の責任であり、経営者は基本となる方針を組織内外に示す「基本方針」を策定し、役職員に周知徹底しなければならない。

②経営者は、「基本方針」に基づき対策の実施のためのリソースが確保されるよう、必要な決定、指示を行わなければならない。

■どのようなリスクがあるのか？

経営者が、内部不正対策は自らの責任で行うことの強い意識を持ち、組織の経営戦略または経営方針に照らして、内部不正がもたらす組織運営への影響の把握を行わないと、組織が内部不正対策を行うにあたっての基本方針を定めることが困難となります。

そして、経営者がリーダーシップをとり、「基本方針」を策定しないと、社内外における経営責任の所在があいまいになり、実効性のある管理体制の整備が困難となります。「基本方針」は経営者の内部不正防止に向けた意志を伝えるものでもあり、策定しないと経営者の意志が役職員に伝わらず、具体的な対策を立てることや役職員に内部不正対策を周知徹底することが困難になります。

さらに、経営者が、「基本方針」に基づく対策の実施のために必要なリソース確保のための決定、指示を行わないと、やはり、実効性のある管理体制の整備が困難となります。

■対策のポイント

経営者は、経営戦略または経営方針に照らして、内部不正に起因する組織運営への負の影響を把握した上で、内部不正対策の大枠となる基本方針を策定し、内部不正対策の方向づけを行わなければなりません[18]。経営者は対策を実効性のあるものとするために、リソース確保のために必要な決定、指示を行い、さらに、実施状況をモニタリング[19]、評価することによって基本方針や組織内リソース配置を定期的に見直していきます。

---

[18] なお、持株会社を中心として、複数の企業によりグループを形成し、重要情報に係る業務上の連携が密接である場合等においては、グループ全体におけるコーポレートガバナンスのデザインに基づいて、内部不正対策についても、グループ全体で立案することが必要です。この場合、グループ内の企業間の連携体制や責任体制を文書化し、明確化しておくことが必要です。

[19] 定期的な報告によって継続的に状況を把握していること。

これらについて、経営者は自ら以下の対策を把握し、組織内において責任を持ちます。また、対外的な説明責任を持ちます。

1. 経営戦略または経営方針に照らして、内部不正がもたらす組織運営への影響を把握します[20]。
2. 本ガイドライン等を参考にし、基本方針を策定(Q&A1:P74)します。
3. 策定した基本方針を実行するために必要な人材や予算等のリソース確保のための決定を行い、指示します。
4. 策定した基本方針に照らし合わせ、役職員に内部不正対策を教育等によって周知徹底します。
5. モニタリング及び評価の結果をもとに、基本方針や組織内のリソース配分を定期的に見直します。
6. 重要情報とそれ以外の情報を区別します(Q&A2:P75)。さらに、重要情報を事業上の重要度等を考慮していくつかに分類することが望まれます（Q&A3:P75)。
7. 重要情報の区別及び分類は、社会背景や事業環境等とともに変化するため、定期的に見直します。

[20] 近年、情報の活用が組織運営の様々な局面においてますます重要となる中、内部不正は組織活動自体の停止や、社会的信頼の失墜を招く可能性も十分にあることを念頭に、影響を検討することが必要です。

（２）　総括責任者の任命と組織横断的な体制構築

①経営者が総括責任者の任命、並びに、管理体制及び実施策の承認を行い、経営者主導の取り組みであることを組織全体に示さなければならない。②総括責任者は、基本方針に則り組織横断的な管理体制を構築しなければならない。また、実施策を策定しなければならない。

ただし、経営者が組織全体に目が届く組織であれば、自ら内部不正対策の実施にあたり、管理体制を必ずしも構築する必要はない。

■どのようなリスクがあるのか？

経営者が総括責任者の任命及び実施する対策を承認しないと、必要な予算や人事を割り当てることが難しいことから、実効的な管理体制の構築が困難になります。

内部不正の対象となる重要情報は組織内の多岐にわたる部門に存在するため、組織横断的な管理体制が構築できないと、組織として効果的・効率的な対策や情報管理ができないだけでなく、対策や情報管理が徹底されない恐れがあります。対策や情報管理が徹底されていないと、内部不正が発生してしまう危険が高まります。

■対策のポイント

経営者が主導となり内部不正対策を組織内に徹底させるための体制を構築・運用します。具体的には以下のような対策を定めて運用します。

1. 総括責任者には、事業を考慮した実効的で効果的な内部不正対策を実現するために情報セキュリティと経営を理解できる者(Q&A1:P74)を任命します。
2. 総括責任者は、組織横断的な管理体制や関連部門の役割を具体化、明文化し、その役割を徹底させます。責任部門は総括責任者とともに組織全体での内部不正対策の実施策と実施体制を構築します（事業の規模等に応じ、重要情報の取り扱いに関する専門部署や委員会を設置する等(Q&A4:P75)）。また、想定する関連部門の重要情報・役割の概要については図４を参照してください。
3. 組織横断的な管理体制の構築では、総括責任者が対策実施の管理・運営の要員として各部門の部門責任者や担当者等を任命します。

4. 内部不正対策を組織内に徹底させるための体制の構築にあたっては、部門責任者、担当者等に求められる能力を明確化します。構築した体制において能力の不足が認められる場合には、責任者、担当者等の能力向上に向けた取り組みの実施や、組織外からの専門家の採用を検討します。また、責任者、担当者等が、役割に応じた必要な知識、ノウハウの習得を図れるように、総括責任者はそれを支援します。
5. 組織内で、内部不正防止の管理体制の他、プライバシー保護、コンプライアンス対策、危機管理対策等の関連の体制を構築する際には、経営者が主導し、それらの間の役割分担や連携の在り方を明確にします。
6. 重要情報の取り扱いに係る業務が業務委託先にまで及ぶ際には、必要に応じて、業務委託先までを含んだ連携体制を構築します（（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）を参照）。なお、一般的に、情報の取り扱いに係る業務の外部委託においては、専門的組織に業務を担わせることによる効率化等のメリットが考えられます。その一方で、内部不正対策の実施においては、リスクが増大する可能性も考えられます[21]。このため、情報の取り扱いに係る業務については、組織内部で行う場合と委託で行う場合のいずれが適切かを効率とリスクのバランスを考えた上で検討していくことが必要です。

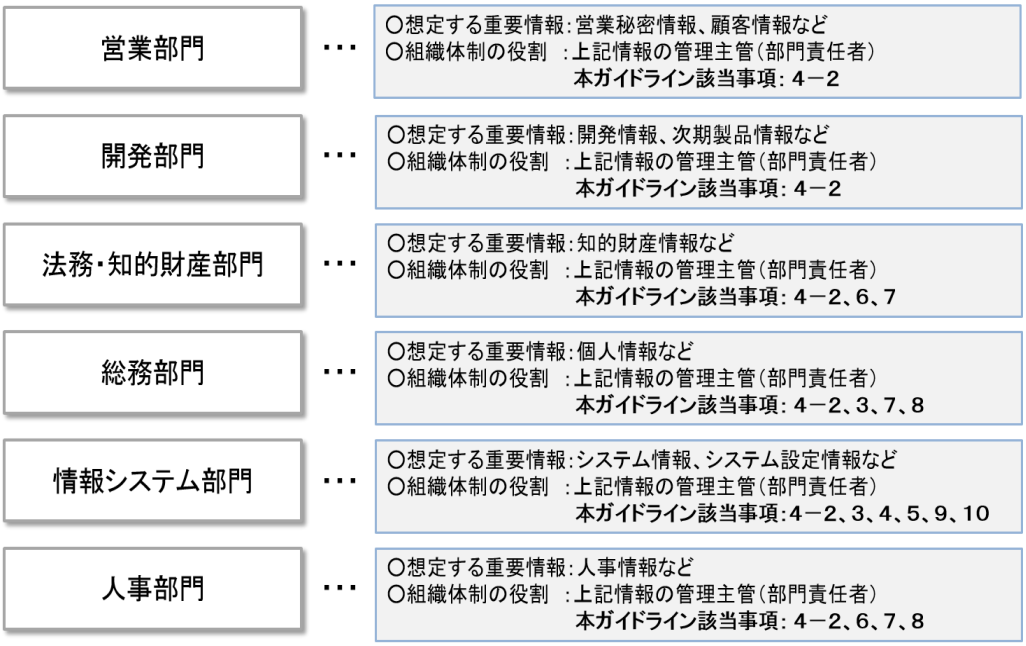


図 4　想定する関連部門と重要情報・役割の概要

[21] リスクが増大する例としては、内部不正対策の実施について間接的な監督になることや、自組織と委託先では基本方針が必ずしも一致しない等が挙げられます。

4-2.資産管理（秘密指定、アクセス権指定、アクセス管理等）

情報資産一覧化等の取り扱いや検討事項に関するフローの概要は図 5 を参照してください。

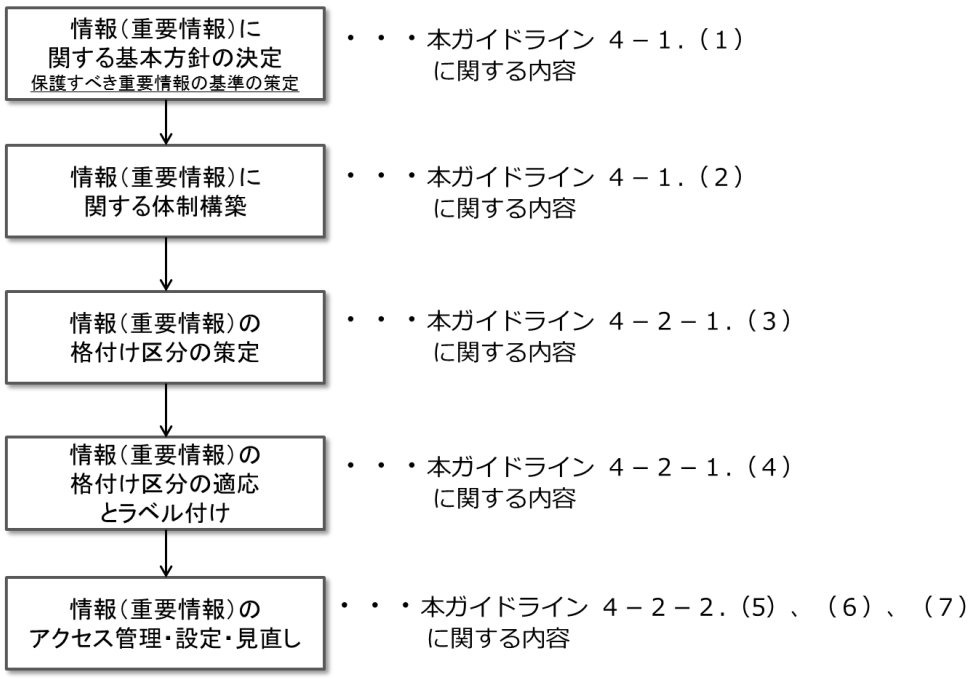


図 5　情報(重要情報)の取り扱いや検討事項に関するフロー図

4-2-1.秘密指定

（３） 情報の格付け区分

重要情報を把握して重要度に合わせて格付け区分し、その区分に応じて取り扱い可能な役職員の範囲（例：職位、職種等）を定めなければならない。

■どのようなリスクがあるのか？

顧客名簿や技術ノウハウ等の重要情報とそれ以外の情報を区別しないと、役職員は保護する必要のある重要情報が分からず、重要情報を知らずに漏らしてしまう恐れがあります。また、重要情報を格付け区分して区分に応じた適切な管理をしないと、対策が不十分であったり、対策にコストをかけすぎたりしてしまいます。

これらの管理ができていないと、不正を犯した内部者の責任を追及できないことがあります。また、企業や団体の管理責任を問われることもあります。

■対策のポイント

重要情報を把握し、適切に管理するために、以下のことを定めます。

1. 重要情報の取り扱いを定めます。3 つ以上に重要度を格付け区分した場合は、重要度ごとに取り扱いを定めます。定めた重要情報の取り扱いは、定期的に見直します。
2. 重要情報の管理者を定めます。例えば、部門責任者又は部門責任者から割り当てられた担当者を管理者とします。また、大規模な組織では、部門ごとに管理者を定めます。

（4） 格付け区分の適用とラベル付け

①重要情報の取扱範囲を限定するために、重要情報の作成者が（3）で定めた格付け区分を選択し、その選択について重要情報の管理者に確認を得なければならない。
②また、重要情報を含む電子文書や電子データには、役職員に格付け区分が分かるように機密マーク等の表示をしなければならない。

■どのようなリスクがあるのか？

重要情報の格付け区分を定めないと情報の取扱範囲が定まらず、重要情報を取り扱う必要のない役職員がアクセス可能となり、より多くの役職員が重要情報を知ることができてしまい漏えいの可能性が高まります。重要情報を知り得る役職員が多くなるほど、内部不正が見つかりにくい環境となり、内部不正が発生しやすく、発生後の内部不正者も見つけづらくなります。

重要情報の管理者（例：部門責任者等）を定めないと、重要情報の適切な管理が徹底されず、PC 等の情報資産の許可のない持ち出しや紛失等が発生することによって、重要情報が漏えいしてしまう恐れがあります。

また、重要度に応じたラベルの表示[22]を設定しないと、役職員が重要情報と知らずに持ち出してしまい、漏えいさせてしまう恐れがあります。

■対策のポイント

重要情報の取扱範囲を限定し、その重要情報の取り扱いが分かるように以下のことを定めて運用します。

1. 重要情報の取扱範囲は業務上取り扱う必要のある役職員のみとします。取扱範囲は、重要情報の不正使用の危険性を低減するために、職位・職務、役割や責任範囲、雇用形態等を踏まえて決定します。
2. 重要情報の作成者が（3）で定めた格付け区分を選択するとともに、その選択については、必ず上司等の重要情報の管理者に確認を得ることが必要です。また、既に作成し、保管されている重要情報についても同様に格付けされた区分に適用することが必要です。

[22] ツールによってはファイルのプロパティで指定できるものがあります。

3. 重要情報を含む電子文書には、役職員に分かるように格付け区分を示す機密マーク（秘密等の文字が表示される透かしや秘密を表す図形データ、スタンプ等）の表示を付けることが必要です。重要情報を含む電子文書等には、重要情報の有効期間を指定して上記の機密マークとともに記載することが望まれます。有効期間は定期的に見直します。重要情報の取扱期間が終了したら、廃棄等の取り扱いに従って処理します。
4. 重要情報のレベルにより消去方法のレベルを決めて、PC 等の情報機器の媒体から重要情報を消去します[23] 。

[23] 極めて重要な情報を扱う業務から役職員が外れる場合には、その役職員の情報機器の記録媒体から重要情報を完全消去します。完全消去には OS レベルでのフォーマットからツールによるランダム情報の書き込み等の消去のレベルがあります。

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

①情報システムでは、（４）で定めた取扱範囲（例：職位、職種等）によって限定された利用者のみが重要情報にアクセスできるように、利用者 ID 及びアクセス権の登録・変更・削除等の設定について手順を定めて運用しなければならない。②また、異動又は退職により不要となった利用者 ID 及びアクセス権は、ただちに削除しなければならない[24]。

■どのようなリスクがあるのか？

情報システムにおいて利用者 ID やアクセス権が適切に設定されないと、本来アクセス権のない役職員に重要情報のアクセスを許してしまい、重要情報を不正に利用される恐れがあります。また、逆に業務上アクセス権を必要とする役職員が権限のないために業務を遂行できなくなります。

異動又は退職によって不要となった利用者 ID が削除されていないと、役職員及び元役職員によって不正に利用されて、重要情報にアクセスされる恐れがあります。

これらの管理ができていないと、不正を犯した役職員及び元役職員の責任を追及できないことがあります。また、企業や団体の管理責任を問われることもあります。

■対策のポイント

情報システムにおいて、利用者 ID 及びアクセス権を誤りなく設定するために、以下の対策を実施します。

1. 利用者 ID 及びアクセス権の登録・変更・削除に関する承認手順や設定終了報告等の手続きを定めて運用します。
2. 情報システムには、（４）で定めた取扱範囲に基づいて重要情報へのアクセス権が利用者 ID に設定されるようにします。もし、（４）で定めた取扱範囲によるアクセス権の設定ができない場合は、（４）の見直し又は情報システムの機能変更を行って対処します。

[24] 利用者 ID を消去したときにアクセス記録などが消去されるような場合には、利用者 ID をロックしてアクセス出来ないような状態としてログを保全することが必要となります。

3. 重要情報へのアクセス権限を付与すべき者を必要最小限とします。また、アクセス権限を持つ者に付与する権限を必要最小限とし、権限を付与する期間も必要な時期に限って行うこととします。特に、委託先の従業員等に権限を付与する場合は、(16)で示す契約上の措置が必要です[25]。
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[26]。
5. 利用者 ID 及びアクセス権が適切に付与されているかを確認するために、定期的にアクセス権の要件を見直します。例えば、人事異動の時期に一斉に見直す等を行うことが望まれます。特に、アクセス権限が集中している者に対しては、適切性を確認し、不必要なアクセス権限は削除を行います。
6. 重要情報を格納している情報システムでは、時間及びアクセス数・量等のアクセス条件による制御を行うことが望まれます。例えば、時間であれば夜間に重要情報にアクセスすることを制限します。また、アクセス数・量であれば重要情報を一括してダウンロードすると上司等に通知されるようにします[27]。

[25] 例えば、委託先の従業員の異動や退職によりアカウントの削除漏れ等が発生しないように、体制に変更が生じた場合は変更内容を委託元に報告する等が挙げられます。

[26] 個人ではなく、職務（役割）に対してアクセス権限を割り当てる「ロールベースアクセス制御」に対応したアクセス制御システムを導入することも考えられます（Q&A5:P75）。

[27] 通知等によりモニタリングを行う場合には、通知内容を確認して適切に対処することが必要です（Q&A6:P76）。なお、対策を回避されないために、基準値については職員等に秘匿しておくことが必要です。

（6） システム管理者の権限管理

システム管理者が複数人いる場合は、システム管理者 ID ごとに適切な権限範囲を割り当てシステム管理者が相互に監視できるようにしなければならない。

■どのようなリスクがあるのか？

権限範囲を適切に割り当てていないと、例えば、利用者 ID の不正登録及び削除が起こることで、不正登録による重要情報の不正使用や、不正な削除による業務妨害等の恐れがあります。一人の管理者に権限が集中している場合は、情報システムの破壊及び重要情報の削除等の妨害によって事業継続が不可能となる恐れがあります[28]。

■対策のポイント

システム管理者による内部不正を防止するために、以下のようにシステム管理者 ID ごとに適切な範囲の権限を割り当て、運用されていることを確認します。

1. システム管理者を決める際には、高い規範意識等の適性を満たす者を任命します。複数の管理者を任命し、相互に監視[29]できることが望まれます。
2. 一人のシステム管理者に権限が集中しないように権限を分散します。
3. 相互に監視するために、作業内容や作業日時等が記載された作業報告を作成して残します。この作業報告を別のシステム管理者が確認することが望まれます。
4. システム管理者は、特権を必要とする操作以外では特権を用いて操作を行わないようにします。

[28] システム管理者が一人しかいない場合には、リスクを権限分散によって回避できません。そのため、（17）のような情報システム管理の操作履歴等をシステム管理者以外の者が確認するといった代替手段でリスクを低減させます。

[29] 複数のシステム管理者を設定することで、情報システムの設定作業者が自ら作業内容を確認するだけではなく、その設定作業が正しく実施されたかを他のシステム管理者が確認することで相互に監視することができます。また、相互に監視する方法以外として複数人の立会による作業も検討できます。複数人の立会作業としては、鍵の分散や分割等を用いることが考えられます。

（7） 情報システムにおける利用者の識別と認証

情報システムでは、利用者（情報システムを利用する内部者）及びシステム管理者（情報システムを管理する内部者）の識別において、共有 ID 及び共有のパスワード・IC カード等を使用せず、個々の利用者 ID 又はシステム管理者 ID を個別のパスワード・IC カード等で認証しなければならない。

■どのようなリスクがあるのか？

情報システムで共有 ID 及び共有のパスワード・IC カード等を使用していると、内部不正発生の際に重要情報にアクセスした利用者が識別できないため、内部不正者の特定が困難となります。また、内部不正者の特定が困難なことから心理的に重要情報を持ち出しやすい環境となります。

これらの管理がされていないと、不正を犯した内部者の責任を追及できないことがあります。また、企業や団体の管理責任を問われることもあります。

■対策のポイント

情報システムでは、利用者の識別と認証を適切に行うために、以下のように利用者 ID やシステム管理者 ID を管理する規程を整備し、運用することが必要です。

1. 利用者とシステム管理者を識別するために、利用者ごと、システム管理者ごとに利用者 ID、システム管理者 ID を割当てます。そして、利用者 ID 及びシステム管理者 ID はパスワード等で認証します。
2. 利用者自身の利用者 ID を他の利用者に不正使用されないように、パスワードについては、単純な文字列を設定しないこと及びできれば定期的に変更すること等の管理事項(Q&A7:P76)を定めて利用者に実施させます。
3. 他の利用者に ID 及びパスワード・IC カード等を貸与することを禁止します。

4-3.物理的管理

（８） 物理的な保護と入退管理

許可された者以外の重要情報の格納場所や取り扱う領域等への侵入等を物理的に保護する境界を定めて、重要情報や情報システムを壁や入退管理策によって保護しなければならない。

■どのようなリスクがあるのか？

重要情報を格納する装置や重要情報を扱う PC 等の情報機器に許可のない者が触れることができると、それら情報機器が破壊されて業務を妨害されたり、重要情報が盗まれて漏えいしたりする恐れがあります。また、それらの情報機器を操作されることで重要情報の漏えい又は消去の恐れがあります。

特に、重要情報の格納装置及び記録媒体は、破壊されると業務が継続できなくなる恐れがあるため、入退室管理が厳しいサーバルーム等で厳重に保護することが必要です。

■対策のポイント

例えば、図 6 のように重要情報の格納場所や取り扱う領域等を明確にし、これらの領域に入ることができる役職員や運送業者等の外部者を制限するために、物理的に保護することが必要です。

1. セキュリティを強化すべき物理的領域を定め、領域ごとに管理する情報資産の重要性に応じて順守すべきセキュリティ上の規程を整備(Q&A8:P76)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。
2. 役職員や運送業者等の外部者によって、重要情報が不正に持ち出されないように出入り可能な領域を決めて領域ごとに入退出管理をします。例えば、運送業者はロビーまで、取引先は応接室まで、役職員は共用エリアと業務フロアまでというようなセキュリティポリシーを策定します。また、サーバルーム等への入室はシステム管理担当者等の資格のある者だけが必要な場合のみ、サーバルームの管理者（責任者等を含む）の許可を事前に得て入室するものとします。
3. 各入退出管理ポイント（各管理エリアの境界）では、内部不正の防止及び発生後の犯人追跡のために、入退出の記録を取ることが必要です。また、入退出の証跡を残

すことを目的とし、顔写真等の「個人を特定するための記録」を取ることで、より高い内部不正抑止効果が期待できます。この場合、「入退出の記録」と「個人を特定するための記録」は、定期・不定期に監査を行って照合するようにします。

4. 重要情報にアクセス可能な物理的領域については、無人時における不正侵入も考慮することが必要です。例えば、機械警備システムや監視カメラを導入し、建物の開錠（最初入場時）・閉錠（最終退出時）における警備システム操作者の記録については、顔写真等の個人を特定するための記録も取ることが望まれます。
5. 重要情報を格納する装置は、必要に応じてネットワークから隔離された環境を用意する等も考慮することが必要です。

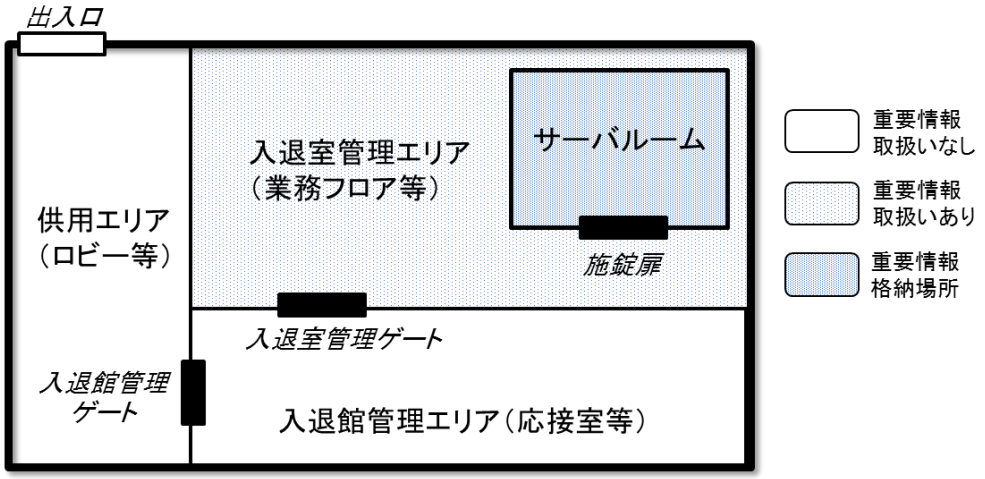


図 6　物理的に保護する領域の参考例

（９）　情報機器及び記録媒体の資産管理及び物理的な保護

①PC 等の情報機器及び携帯可能な外部記録媒体[30]は、盗難や紛失等がないように管理・保護しなければならない。②また、不要になった情報機器や記録媒体を処分する際には重要情報が完全消去されていることを確認しなければならない。

■どのようなリスクがあるのか？

情報機器及び記録媒体が管理されていないと、盗難や紛失をしやすい環境であるだけでなく、盗難や紛失を発見できません。また、情報機器を物理的に保護していないと、盗難によって重要情報が漏えいしてしまう恐れがあります。

また、情報機器及び記録媒体に重要情報が記録され、不十分な削除のまま処分すると、その重要情報が漏えいする恐れがあります。

■対策のポイント

保護すべき重要情報を扱う情報機器及び記録媒体に求められる対策を規定し、情報機器及び記録媒体の盗難及び紛失、並びに、処分を考慮して管理・保護することが必要です。

1. 情報機器の紛失等を発見できるようにするために、台帳等で設置場所や使用者を管理し、定期的に棚卸（資産の有無の確認）を実施します。
2. 盗難や不正持ち出しがないように、情報機器はセキュリティワイヤー等で机等に固定することが望まれます。また、ノート PC やスマートデバイス等の携帯可能なモバイル機器や、USB メモリ等の携帯可能な記録媒体は棚や机等に施錠保管します。
3. 重要情報の格納サーバやアクセス管理サーバ等の情報機器は、管理者以外が触れられないように、入退出管理が厳しいサーバルーム等の場所に設置します。
4. 情報機器及び記録媒体を処分する際は、HDD や USB メモリ等の記録媒体から重要情報を復元できないように完全消去します。さらに、CD-R、DVD-R 等の記録媒体は破砕機[31]等を用いて物理的に破壊することが必要です。

[30] USB メモリ、ポータブル HDD 等

[31] 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

持ち出し可能なノートPC及びスマートデバイス等のモバイル機器並びに携帯可能なUSB メモリ及び CD-R 等の記録媒体を（８）の物理的に保護された場所から外に持ち出す場合、持ち出しの承認及び記録等の管理をしなければならない[32]。

■どのようなリスクがあるのか？

モバイル機器及び記録媒体の持ち出しの承認がされていないと、許可なく重要情報を持ち出されて、重要情報が漏えいしてしまう恐れがあります。また、持出記録を付けていないと、内部不正が発生したときの調査が困難になる可能性があります。

■対策のポイント

モバイル機器及び記録媒体の持ち出し管理では、以下のことを定めて運用しなければなりません。

1. モバイル機器及び記録媒体を持ち出す際に、部門管理者等の承認を得てから持ち出すことが必要です。
2. モバイル機器及び記録媒体を持ち出す際に、持ち出した情報資産及び、日時、担当者等を記録して管理することが必要です。

[32] （８）の物理的に保護された場所の外においての携帯可能な情報機器及び USB メモリ内の重要情報の保護に関しては（１４）を参照してください。

（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

個人のノート PC やスマートデバイス等のモバイル機器及び携帯可能な USB メモリ等の外部記録媒体の業務利用及び持込を適切に制限しなければならない。

■どのようなリスクがあるのか？

個人の情報機器及び記録媒体を業務利用すると、個人の情報機器及び記録媒体の組織による管理が困難であることや、個人と組織の情報がともに扱われることから、ウイルス感染や操作ミス等によって重要情報が漏えいする可能性が高くなります。また、内部不正の発生後の調査において、個人の情報機器及び記録媒体の提供を承諾してもらえずに、調査が困難になる場合があります。

重要情報を取り扱う業務フロア等の領域に個人の情報機器及び記録媒体を持ち込まれると、個人の情報機器や記録媒体に重要情報を格納して持ち出される恐れがあります。また、カメラ付きの情報機器であれば、重要情報を写真に撮って持ち出される恐れもあります。通信可能な情報機器であれば、重要情報を外部に送信される恐れもあります。

■対策のポイント

個人の情報機器及び記録媒体の業務利用及び持込を制限する場合、その場所で扱う重要情報の重要度及び情報システムの設置場所等を考慮することが必要です。具体的には、以下の内容を定めて運用します。

1. 個人の情報機器及び記録媒体の業務利用を許可するか検討します。
2. 業務利用を許可する場合には、利用する業務範囲及び順守事項等のルールを整備します。利用する業務範囲が広くなれば、扱う重要情報が増えて管理が難しくなることに注意することが必要です。また、業務利用にあたって順守事項等の承諾書をとっておくことが望まれます。
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、(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。

4. 個人の情報機器において重要度の高い情報を扱う場合には、必要に応じて個人の情報機器上でも重要情報を管理できるソフトウェア等を導入して組織側で重要情報を管理できることが望まれます。
5. 重要情報の重要度により重要情報格納サーバやアクセス管理サーバ等が設置されているサーバルーム、及び重要情報を取り扱う業務フロア等には、個人所有のノート PC やタブレット端末、スマートデバイス等のモバイル機器、その他の携帯可能な情報機器の持込・利用を厳しく制限します。
6. 情報機器の持込を禁止する場所では、持込禁止のポスター等を貼って警告することが望まれます。
7. 個人所有の USB メモリ等の携帯可能な記録媒体等の持込を制限します。記録媒体等の利用は会社貸与品のみとします。
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[33]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。

[33] 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.技術・運用管理

（１２）ネットワーク利用のための安全管理

組織のネットワーク利用では、PC 等の情報機器から重要情報が漏えいしないように、ファイル共有ソフト及びソーシャル・ネットワーク・サービス(SNS)、外部のオンラインストレージ等の使用を制限して安全なネットワーク環境を整えなければならない。

■どのようなリスクがあるのか？

情報機器にファイル共有ソフトがインストールされていると、PC 内の重要情報が外部に意図せずに漏えいしてしまう恐れがあります。ファイル共有ソフトで取得した外部のファイルを実行することでマルウェア感染を起こし、組織内の他の情報機器に感染を広げてしまう恐れもあります。

また、SNS 及び外部のオンラインストレージの利用並びに掲示版の書き込みが許可されていると、重要情報がアップロードされたり、書き込まれたりして漏えいする恐れがあります。

■対策のポイント

組織のネットワークから外部に重要情報が漏えいしないように、情報機器において対策を講じることが必要です。

1. PC 等の情報機器には、組織内で許可されたソフトウェア以外のもの（例えば、ファイル共有ソフト等）をインストールして利用することを禁止します。利用を許可するソフトウェアは、組織内で決定します。利用者から新たに利用申請があったソフトウェアは、利用させてもよいか判断することが必要です。
2. Web アクセスに関しては、コンテンツフィルタを導入して、SNS 及びアップローダー、掲示版等へのアクセスを制限することが望まれます。
3. 電子メールに関しては、業務のメールを個人のメールアドレスに転送する設定になっていないかを確認することが望まれます。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を導入することで、誤送信による情報漏えいの対策を講じることが望まれます。

4. PC 等の情報機器を守るために、ウイルス対策ソフトの導入やパッチ適用等の一般的なセキュリティ対策を実施します。

COLUMN

「電子データのパスワード管理」の危険

重要情報を保護するには、以下の二点が重要です。
①重要情報は、通常の情報と区別を明確にする。
②アクセス権を有する使用者からのみアクセスできるようにする。

利用者単位でアクセスを制限する他、電子データ（フォルダや個別のファイル）単位で重要情報に共通パスワードを設定する方法も考えられます。例えばWindowsでも、そのような機能を簡単に実現するソフトウェアが存在します。

ただし、その場合、重要情報へのアクセスを許可された者は、共通でパスワードを利用するため、人事異動や退職等により、ひとりでも権限変更すると、その都度、共通のパスワードを変更しなければならないなど、細心の注意が必要です。

（１３）重要情報の受渡し保護

①委託先等の関係者への重要情報の受渡しでは、受渡しから廃棄までが適切に管理されていなければならない。②インターネットを用いた送信や組織外を介する記録媒体等を用いた重要情報の受渡しでは、誤って重要情報が関係者以外に渡ってしまうことも考慮して暗号化等で重要情報を保護しなければならない。

■どのようなリスクがあるのか？

電子メールや記録媒体等での重要情報の受渡しでは、重要情報を必要時以外に持ち出しできないようにしないと、内部者が不正に重要情報を持ち出してしまう恐れがあります。また、受け渡す重要情報を保護していないと、電子メールの誤送信や記録媒体の盗難・紛失によって重要情報が漏えいしてしまう恐れがあります。

■対策のポイント

関係者への重要情報の受渡しから関係者による重要情報の廃棄までを以下のように管理します。

1. 重要情報の受渡しに関しては、重要度に合わせた組織内部での手順(Q&A9:P77)及び承認手続きを定めるとともに、委託先等の関係者にも順守させます。
2. 関係者への重要情報の受渡しに関し記録します。
3. 関係者へのインターネットを用いた送信及び記録媒体を用いた手渡しによる重要情報の受渡しについて暗号化します。
4. 関係者に開示した重要情報の廃棄・消去に関する記録を関係者から取得します。
5. 上記の取り決めについては、委託先までではなく、それ以降の再委託先にも順守させることが必要です[34]。

[34] 個人情報の保護に関する法律の第 22 条では、委託先の監督として、「個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。」ことが定められています。

（１４）情報機器や記録媒体の持ち出しの保護

ノート PC 及びスマートフォン等のモバイル機器並びに USB メモリ及び CD-R 等の携帯可能な記録媒体に重要情報を格納して（８）の物理的に保護された場所の外に持ち出す場合に、技術的な対策によって重要情報が適切に保護されていなければならない。

■どのようなリスクがあるのか？

重要情報が格納された情報機器や記録媒体を暗号化やパスワードロック等の技術的な対策を施さずに持ち出すと、盗難や紛失に会った際に重要情報が漏えいする恐れがあります。

■対策のポイント

重要情報が格納されたノート PC、スマートフォン等のモバイル機器や USB メモリ等の記録媒体を組織外に持ち出す場合に、適切な対策を行うことが必要です。

1. 情報機器を利用する際に利用者 ID とパスワード等による認証をするように設定をします。また、ノート PC では BIOS パスワード、HDD パスワードを設定することが望まれます[35]。さらに、重要情報を保護するために暗号化ソフトを導入することが望まれます(Q&A10:P77)。
2. 重要情報が記録されている情報機器の紛失を想定し、リモートから情報機器内の重要情報を消去できるツール又はサービスを利用することが望まれます。また、パスワードロックの認証で一定の回数認証に失敗すると重要情報を消去するツールを利用することも望まれます。

[35] 重要情報にアクセス可能な情報機器として、その組織の標準的な機器以外（例えば、スマートフォンやタブレット PC 等）が存在する場合は、扱う情報の重要度に合わせ、同じレベルのセキュリティ対策を実施することが必要です。

（１５）組織外部での業務における重要情報の保護

（８）の物理的に保護された場所の外で重要情報を用いて業務を行う際に、周囲の環境やネットワーク環境等を考慮し、適切に重要情報を保護しなければならない。

■どのようなリスクがあるのか？

公共の場で業務を行っている際に、覗き込まれることで重要情報が漏えいする恐れがあります。また、公衆の有線 LAN や無線 LAN に接続して、通信を保護せずに組織のネットワークに接続すると、ネットワーク上で重要情報を盗聴される可能性があり、重要情報が漏えいする恐れがあります。テレワーク[36]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

組織外部においての重要情報を扱う業務では、利用環境において画面を覗かれないように適切に保護し、接続許可されたネットワーク環境のみに接続することが必要です。

1. 電車の車内やカフェ等では、画面が覗き込まれないように注意します。また、画面に覗き見防止フィルムを貼り、覗き込まれないようにすることが望まれます。
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[37]。
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[38]ことが必要です。

---

[36] テレワークとは、情報通信技術を活用した、場所や時間にとらわれない多様な就労・作業形態です。テレワークの形態としては、例えば、在宅勤務、モバイルワーク、サテライトオフィスやスポットオフィス等を利用した勤務等の形態があります。

[37] 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。

[38] 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[39]。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。
5. 組織外部での共同作業（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もよい情報であるか判断するとともに、セキュリティ確保のためのルール[40]を定め、作業対象となる従業員に対し、教育等を通じ徹底することが必要です。

COLUMN

情報の持ち出し手段の最多はUSBメモリ

内部不正を行ったことのある経験者への調査によると、情報の持ち出し手段としては、USBメモリが最多でした。USBメモリ等の外部記録媒体に関する利用ルールの徹底、利用制限が、内部不正対策として有効です。

内部情報の持ち出し手段

	1位	2位	3位
内部不正経験者すべて (n=200)	USBメモリ 43.6%	電子メール 34.3%	パソコン 25.5%
故意の内部不正経験者のみ (n=98)	USBメモリ 53.0%	電子メール 28.9%	紙媒体 18.8%

（複数回答）

出典：「内部不正による情報セキュリティインシデント実態調査」（2016年3月3日）

[39] 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。

[40] クラウドサービスで用いるパスワードの厳格な管理（パスワードは一定強度以上とし、他の用途で用いるパスワードとの共用を避ける等）、データの共有範囲の限定（必要とする利用者の間でのみ共有）等。

（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）

委託する業務内容と重要情報の重要度に応じて、セキュリティ対策を事前に確認・合意してから契約し、委託先が契約通りに情報セキュリティ対策を実施しているか定期的及び不定期に確認しなければならない。

■どのようなリスクがあるのか？

委託する業務内容と重要情報の重要度に応じて必要なセキュリティ対策を確認せずに契約すると、委託先のセキュリティ対策の不備によって重要情報が漏えいする可能性があります。また、契約内容によっては重要情報の漏えいによる損害を補償されない場合があります。

契約期間中、委託先が契約通りにセキュリティ対策を実施していることを確認しないと、委託先の不備による情報漏えい等を防止できない可能性があります。また、契約書にログの提供を受けることを記載していないと、内部不正発生後の調査が困難になることがあります。

第三者が提供するサービス（クラウドサービスを含む）を利用する場合、第三者の提供するサービスで取り扱い可能な重要情報であるか判断しないと、第三者から事業に影響のある重要情報が漏えいした場合に事業が継続できなくなる可能性があります。

重要情報の重要度によっては、重要情報の取り扱いに係る業務が業務委託先にまで及ぶ際には、必要に応じて、業務委託先までを含んだ連携体制を構築します。なお、外部委託の検討にあたっては、効率化等のメリットと内部不正発生のリスクの増大とのバランスを考慮することが必要です。

■対策のポイント

業務を委託するにあたり、重要情報を安全に管理するために必要となる事項を事前に確認し、契約内容に盛り込みます。契約期間中は、契約通りにセキュリティ対策が実施されているか定期的及び不定期に確認することが必要です[41]。具体的には、（重要情報の重要度によっては、）以下の様な観点で内容を確認し、そのセキュリティ対策の内容を明確にすることが必要です。

[41] 業務委託先の監督方法については、経済産業省「個人情報の適正な保護に関する取組実践事例」報告書（平成 22 年 3 月）も参考となります。

1. 業務を委託する場合、重要情報の取り扱いについて必要なセキュリティ対策が確実に実施されることを事前に確認するために、委託する業務内容に沿って、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。
2. 委託先のセキュリティ対策が、安全に管理するために十分であるかを定期的及び不定期に確認します。その結果については、総括責任者または部門責任者等が、委託内容等の見直しを検討することを含め、適切に評価することが望まれます。
3. 再委託をする場合には、委託元は委託先から、再委託先の業務内容及び重要情報の取り扱い等について、事前報告または承認を求めることが望まれます。また、契約期間中は、委託先を通じて、または必要に応じて自らが、確認や監査を実施することが望まれます。確認や監査は定期的および不定期に実施します（Q&A11:P78）。
4. 委託先、再委託先との間では、内部不正が疑われた場合を想定して、ログが提供されることを、事前に確認し、契約上も明確化することが望まれます。
5. 第三者が提供するサービス（クラウドサービスを含む）を利用する場合、第三者が提供するサービスで取り扱ってもよい重要情報であるか判断します。また、そのサービスレベル及び管理上の要求事項が、事業継続において適切であるかを確認します。
6. 委託期間中、委託先や、その他第三者が提供するサービスにおいて、自組織の基本方針に照らし、適切な内部不正防止対策が確認できない場合には、契約先を切り替える、または組織外への委託を中止することも検討します。

4-5.証拠確保

（１７）情報システムにおけるログ・証跡[42]の記録と保存

内部不正の早期発見及び（２7）の事後対策の影響範囲の観点から、重要情報へのアクセス履歴及び利用者の操作履歴等のログ・証跡を記録し、定めた期間に安全に保存することが望ましい。

■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。

また、ログ・証跡が保存されていないと、内部不正が発生した場合に（２7）に述べる事後対応において、内部不正の原因特定及び内部不正者の追跡、影響範囲等の調査が困難になります。さらに、（２2）に述べる処罰等の根拠や、法的紛争や訴訟になった場合の証拠として認められない場合があります。

■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[43]・証跡を記録して安全に保存します。

1. ログは、重要情報へのアクセス履歴や、利用者の操作履歴（Web のアクセスログやメールの送受信履歴他）等を取得します。
2. 証跡は、設定したポリシーに応じて、上記のログ以外の日時、利用者、操作端末、操作内容、送受信の内容等の情報を取得します。
3. ログは定期的に確認します。多量なファイルへのアクセスや業務範囲外のファイルへのアクセス等の通常の業務と異なる事象が発見された者に対して、事象確認又は監視強化等の対策を行うことが望まれます。

---

[42] 組織のシステム及びネットワーク内で発生するイベント（事象）の記録です。本ガイドラインでは、「ログ」はシステム等で取られる作業ログであり、「証跡」は監査や監視のためにポリシーを決めて収集されるものです。

[43] サーバのログだけでなく、クライアントのログ（Q&A12:P78）（Q&A13:P78）についても必要かどうか検討します。

4. 利用者のプライバシー等を考慮して、ログ・証跡を収集することを労働組合等と合意をとることが望まれます。
5. ログ・証跡の保存を行っている事実を従業員に通知することは、内部不正の発生を抑止する上で効果的な方法と考えられるため、一般的には、通知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[44]。
7. ログ・証跡の確認には、改ざん及び削除防止並びに特定のシステム管理者からのみアクセス可能等の措置が取られていることが望まれます。確認をする際には、総括責任者またはシステム管理者から許可を得ることが望まれます。

[44] 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、ログ取得の対象となる情報の重要性やコスト、及び業種・業態等により様々な観点から検討することが必要です。関連する法令としては、例えば、刑事訴訟法の一部改正の(5)通信履歴の電磁的記録の保全要請の規定の整備では、「検察官・検察事務官・司法警察員は、差押え又は記録命令付差押えをするため必要があるときは、通信事業者等に対し、その業務上記録している通信履歴の電磁的記録のうち必要なものを特定し、30 日を超えない期間（特に必要があり、延長する場合には、通じて 60 日を超えない期間）を定めて、これを消去しないよう、書面で求めることができることとする。」等が存在します。

（１８）システム管理者のログ・証跡の確認

システム管理者のアクセス履歴や操作履歴等のログ・証跡を記録して保存し、(１７)で述べたログ・証跡とともに、システム管理者のログ・証跡の内容を定期的にシステム管理者以外が確認しなければならない。

■どのようなリスクがあるのか？

システム管理者は大きな権限を持つため、システム管理者以外の者が、システム管理者の作業報告を確認して監視をしていないと、作業の正当性及び真正性を確認することや、システム管理者の内部不正を検知することが困難になります。

■対策のポイント

情報システムのログは、通常取得されるエラーのログに加えて、日常のシステムに対する管理・運用作業の記録についても取得することが必要です。具体的には、以下のような内容を定め作業のログの取得と保護を実施します。

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[45]、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[46]が確認します。
2. 情報システムにおいて、ログ・証跡を収集できない場合には、システム管理者の作業内容をドキュメントに記録し、定期的にその作業内容をシステム管理者の上司または総括責任者が確認します。

[45] 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。

[46] 内部不正対策を行う企業や団体に内部監査体制が存在する場合には、内部監査の監査項目として確認、運用する方法も検討します。

4-6.人的管理

（１９）教育による内部不正対策の周知徹底

①すべての役職員に教育を実施し、組織の内部不正対策に関する方針及び重要情報の取り扱い等の手順を周知徹底させなければならない。②教育は繰り返して実施することが望ましい。また、教育内容を定期的に見直して更新し、更新内容を内部者に周知徹底させなければならない。

■どのようなリスクがあるのか？

すべての役職員に教育を実施しないと、役職員は適切な管理を行うことができません。また、教育内容を見直さないと、新たな脅威への対策を行えず、内部不正を発生させてしまう恐れがあります。

教育を実施していないと、不正行為を犯した内部者の責任を追及できないことがあります。さらに、企業や団体の管理責任を問われることもあります。

なお、重要情報を提示している契約相手に関して、その情報を直接取り扱う役職員に重要情報や重要情報の取り扱いについて十分周知されるようにしていないと、契約相手等から情報が流出するおそれがあります。

■対策のポイント

対象となる重要情報や重要情報の取り扱い等について周知し、内部不正対策への理解や意識を高め、内部者に対策を実施させるための教育が必要です。

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&A14:P78)。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。
2. 教育を実施した証拠として、受講者の受講状況及び理解度についての記録をとります。
3. 教育内容を定期的に見直して更新し、更新内容を周知徹底します。
4. 教育内容は、職位（管理職、非管理職等）及び契約形態（社員、派遣社員等）等の権限や職務に応じて適切なレベルや内容を実施することが望まれます。特にシステム管理者には規範意識を高める教育を実施することが望まれます。
5. 各部門責任者、担当者等は、情報通信技術の進歩や新たな脅威の出現、新しい法律の施行など技術的、社会的な変化に対応して、必要な知識の収集、能力の高度化を

図ることができるよう、組織外の情報源からの情報収集[47]や研修等に継続的に取り組むようにします。

COLUMN

効果的な内部不正対策～必ずしも経営者には理解されず～

内部不正を行ったことのある経験者と経営者・システム管理者では、有効と考える対策に違いがあります。特に顕著だったのは、罰則規定の強化と監視体制強化でした。不正行為を思いとどまらせるのに有効な対策を的確に把握し実施することが必要です。

内部不正経験者		対策	経営者・システム管理者	
順位	割合		順位	割合
1位	50.0%	ネットワークの利用制限（Webの閲覧、メールの送受信先等）	2位	30.3%
2位	46.5%	重要情報へのアクセス監視	4位	27.0%
3位	43.0%	重要情報へのアクセス制限	1位	43.9%
4位	25.0%	罰則規定の強化	12位	12.8%
5位	23.5%	社内の監視体制の強化	11位	13.1%

（内部不正経験者：n=200、経営者・システム管理者：n=1500）

出典：「内部不正による情報セキュリティインシデント実態調査」（2016年3月3日）

[47] 例えば、IPA の Web サイトにおいても、情報セキュリティ対策に係る最新の情報発信等を行っています。 URL: https://www.ipa.go.jp/

（２０）雇用終了の際の人事手続き

雇用終了により、退職後の元役職員による重要情報の漏えい等の不正行為が発生しないように、必要に応じて秘密保持義務を課す誓約書の提出を求めなければならない。

■どのようなリスクがあるのか？

雇用終了時に、秘密保持契約（誓約書を含む）を締結しないと、役職員が重要情報に関して認識がないまま退職してしまうことがありえます。この場合には、その元役職員が知り得た重要情報を公開してしまう可能性が高まり、さらに公開したことに対する損害賠償を請求した際にも請求が認められない可能性が高まります。なお、必要に応じて競業避止義務契約（誓約書を含む）を締結することもありえますが、その際には職業選択の自由を考慮することが必要です。

■対策のポイント

雇用終了の際に、役職員から秘密保持契約や競業避止義務契約を締結（誓約書の提出を含む）しておくことが望まれます。

1. 秘密保持契約には、秘密保持の対象となる重要情報を客観的に特定できる記載が必要です。
2. 競業避止義務を記載する場合には、職業選択の自由を侵害しないように、適切に範囲を設定することが必要です。

（２１）雇用終了及び契約終了による情報資産等の返却

役職員の雇用終了時及び請負等の契約先との契約終了時に、取り扱いを委託した情報資産のすべてを返却又は完全消去させなければならない。また、雇用者や契約先に与えていた情報システムの利用者 ID や権限を削除しなければならない。

■どのようなリスクがあるのか？

取り扱いを委託した情報資産（重要情報を含む）を返却又は完全消去させないと、重要情報が元役職員や元契約先から漏えいしてしまう恐れがあります。また、入館証や貸出機器の返却及び情報システムから権限の削除が行われていないと、建物に不正侵入されたり、ネットワークから情報システムに不正侵入されたりし、情報資産を持ち出される恐れがあります。

■対策のポイント

雇用終了時及び契約終了時には、以下のような対策を実施することが必要です。

1. 誓約書や契約書には、雇用終了時や契約終了時に情報資産の返却及び契約先所有のＰＣ等からの完全消去に関する記載が必要です。
2. 取り扱いを委託した情報資産及び入館証等の権限(Q&A15:P79) がすべて返却されたことを確認することが必要です。
3. 情報システムから元役職員の利用者 ID や権限が削除されたことを確認することが必要です。
4. 契約先所有の PC 等に保存されていたすべての重要情報を完全消去した旨の確証を契約先からとることが望まれます。
5. 雇用終了間際に情報の持ち出し等の内部不正が発生しやすいことから、雇用終了前の一定期間から、PC 等をシステム管理部門等の管理下に置くことが望まれます（例：アクセス範囲の限定、USB メモリの利用制限等）。

4-7.コンプライアンス

（２２）法的手続きの整備

内部不正を犯した内部者に対する解雇等の懲戒処分を考慮し、就業規則等の内部規程を整備して、正式な懲戒手続に備えなければならない。

■どのようなリスクがあるのか？

内部不正を犯した内部者に対する懲戒処分が就業規則等の内部規程に盛り込まれてない場合や正式な懲戒手続きが整備されていない場合には、内部者から不当処分の訴えにより懲戒処分が無効となる恐れがあります。

■対策のポイント

懲戒処分を行う場合には、内部規程において懲戒処分及び秘密保持義務に関する項目を定めておくことが必要です。

1. 内部規程には、懲戒処分の対象となる内部不正（例：営業秘密の侵害、個人情報の目的外利用等）に関する記載が必要です。
2. 内部規程には、秘密保持義務の対象となる重要情報を客観的に特定できる記載が必要です。
3. 解雇等の懲戒処分は、根拠となる内部規程に基づき、かつ労働法制を順守して処分をすることが必要です。
4. 適切な懲戒処分を決定するために、査問委員会等によって事実関係を明らかにすることが必要です。
5. 刑事告発及び民事訴訟の法的な手続きに関する内部規程を整備することが必要です。

（２３）誓約書の要請

役職員に対して重要情報を保護する義務があることを理解させるために「秘密保持誓約書」等の提出を要請しなければならない。

■どのようなリスクがあるのか？

役職員による誓約書の提出がないと、重要情報を保護する義務があることの意識付けができない恐れがあるだけでなく、内部不正を犯した役職員に対する解雇等の懲戒処分が、不当処分との訴えにより無効となる恐れもあります。

■対策のポイント

「秘密保持誓約書」に記載する重要情報は客観的に特定できなければなりません。また、「秘密保持誓約書」は、重要情報の保護を意識付けるために一度だけではなく特定の機会で何度も要請することが必要です。

1. 「秘密保持誓約書」には、秘密保持の対象となる重要情報を客観的に特定できる記載が必要です。
2. 「秘密保持誓約書」は、役職員に対して重要情報を保護する義務があることを理解させるために、入社時以外にも特定の機会（昇格、配置転換等による業務の変更やプロジェクトの終了時）に誓約書を要請することが望まれます[48]。

[48] 秘密保持誓約書を退職時に要請した場合には、要請に応じてもらえないこともあります。

4-8.職場環境

（２４）公平な人事評価の整備

公平で客観的な人事評価を整備するとともに、業績に対する評価を説明する機会を設ける等の人事評価や業績評価を整備することが望ましい。また、必要に応じて人員配置及び配置転換等を行い、適切な労働環境の整備を推進することが望ましい。

■どのようなリスクがあるのか？

役職員が、人事評価や業績評価の公平性や客観性が感じられない場合には、不平や不満を要因とした職場環境の低下を招き、内部不正を誘発する可能性があります。

ある役職員が特定の業務を長期間にわたって担当し続けると、その役職員のみが重要情報を扱う状態になり、重要情報を不正に利用される可能性が高まります。また、同種の重要情報の扱いが定常化することで、重要情報の取り扱いにおける緊張感が薄れ、うっかりミス及び誤操作による事故が発生する可能性が高まります。

■対策のポイント

人事評価や業績評価については、人事部門や人事担当者が主体となり、評価制度を整備することが必要です。また、適切な人員配置及び配置転換を行うことが必要です。

1. 昇進や昇格及び組織の給与体系については、公平かつ客観的に実施するとともに充分な透明性を保つことが重要です。必要に応じて、上司や部門長が人事評価や業績評価の評価内容を説明することが望まれます。
2. 評価制度を整備する一環として、業務で必要となる技術や知識に関する教育や研修の受講を推進することが望まれます。
3. ある役職員が特定の業務を長期間にわたり担当している場合には、このような状態を避けるために配置転換を検討することが望まれます。

（２５）適正な労働環境及びコミュニケーションの推進

業務量及び労働時間の適正化等の健全な労働環境を整備するとともに、業務支援を推進する体制や相談しやすい環境を整える等の職場内において良好なコミュニケーションがとれる環境を組織全体で推進することが望ましい。

■どのようなリスクがあるのか？

業務量及び労働時間が健全な労働環境が整備されていないと、特定の役職員の業務量が過大になり、それを解消するために負荷軽減や作業時間短縮を目的とする内部不正を行う可能性があります。また、業務遂行が困難になると役職員の不満が高まり、内部不正への誘因になりかねません。相談しやすい環境等の良好なコミュニケーションが十分でない場合には、業務への悩みやストレスを抱えた状態での作業が続くことにより、内部不正が発生する恐れもあります。

■対策のポイント

職場環境や労働環境の整備においては、総務部門や総務担当者が主体となり、業務量や労働時間等を適正化することが必要です。また、相談しやすい環境を整備し、職場の信頼関係に配慮するとともに、業務の支援や上司や同僚との良好なコミュニケーションがとれる環境を推進することが必要です。

1. 特定の役職員が休暇取得できない状態や長時間残業が継続している状態のように、極端に業務負荷が高い場合には、業務量や労働時間を適正な範囲にすることが必要です。
2. 業務は肉体的・精神的に健康を損ねない範囲とし、職場環境は安全で衛生的に保つことが必要です。
3. 上司や所属部門長は、部員や部下の能力を見極めて出来る限り適切な業務内容や業務量を割り当てることが必要です。
4. 上司や所属部門長は、業務や職務において助けが必要な部員や部下を出来る限り支援する体制や環境を考えておくことが必要です。
5. 仕事が遅れたり困ったりしているときにお互いに助け合う部員が存在する等、部員間の良好なチームワークを構築し維持することが必要です。

6. 部員同士で仕事上の情報交換が活発で、業務以外の相談もできる環境を構築し維持することが必要です。
7. 業務が繁忙な時期及び不慣れな時期の部員には、業務の支援やサポートを推進することが望まれます。
8. 業務への悩みや人間関係に対するストレス等を発見して改善するために、組織では上司だけではなく、同僚も含めて相談しやすい環境を整備するとともに、職場で良好なコミュニケーションが保てる環境を組織の制度として推進することが望まれます。
9. 職場では、悩みを傾聴してくれる環境作りが望まれます。なお、職場で悩みを相談できない内容（例えば、直属上司に関係するもの）を考慮し、職場外の相談窓口から適切な上位の上司にフィードバックし、状況を改善するような環境を整備することが望まれます。相談者が安心できるように、相談内容に応じて相談者をできる限り匿名化し、上位上司にフィードバックした方がよい場合もあります。

（２６）職場環境におけるマネジメント

組織内では、他の役職員が不在で相互監視ができない環境における単独作業を制限することが望ましい。

■どのようなリスクがあるのか？

単独作業は相互監視のできない環境であり、内部不正が発生する可能性が高くなります。そして、内部不正が発生すると、発見や対応が遅れ、被害が拡大してしまう恐れがあります。また、単独作業が発生している場合には、「（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」が低下している可能性があります。

■対策のポイント

1. 単独作業は内部不正が発生しやすい作業環境であるため、その作業内容等の必要性を確認するとともに、作業内容を追跡できる手順を整備することが必要です。単独作業を実施するにあたっては、各部門の責任者等が、その作業を単独で行う必要性を確認した上で、事前承認する手続きを設けることが必要です。事前承認する内容は、「何故、その時期に、その作業をしなければいけないのか？」といった、理由及び時期／時間、作業内容について確認します。また、単独作業を避けるために、必要な支援を検討することが望まれます。
2. 単独作業は内部不正が発生する可能性があることから事後確認を行うことが必要です。事後確認する内容は、事前承認した内容と実際の単独作業内容のチェック及び単独作業時に扱った重要情報の有無と修正内容等を確認することが必要です。

4-9.事後対策

（２７）事後対策に求められる体制の整備

内部不正の影響範囲を特定するために、事象の具体的状況を把握するとともに、被害の最小化策や影響の拡大防止策を実施しなければならない。また、必要に応じて組織内外の関係者との連携体制を確保しなければならない。

■どのようなリスクがあるのか？

内部不正の影響範囲を特定できないと、迅速な事後対策が施せないだけではなく、法的処置等の対応を検討できなくなる可能性もあります。さらに、内部不正の調査や対処について第三者サービス（デジタル・フォレンジック[49]解析やインシデントレスポンス[50]支援等）を利用する際に必要となる情報や伝達方法を取り決めておかない場合には、適切なサービスを受けられない恐れがあります。

■対策のポイント

事後対策に求められる体制を構築するためには、以下のような内容を整備することが必要です。

1. 内部不正による被害の最小化、及び影響の拡大を防止するために、求められる対応手順や報告手順等を事前に取り決めておくことが必要です。内部不正の具体的な状況を把握し、影響範囲を調査するためには、「いつ、誰が、何をしたのか」に関する検証可能な証拠[51]を保全することが必要です。
2. 内部不正への対応については、システム管理者、インシデントレスポンス担当者（外部のインシデントレスポンス支援担当者を含む）、デジタル・フォレンジック解析担当者（外部支援担当者を含む）、弁護士、内部監査者等と連携することが必要です。

---

[49] コンピュータやネットワークの不正使用やサービス妨害等の行為や、法的紛争・訴訟に対し、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術。

[50] 悪意のある攻撃や、ウイルス感染、パソコンの盗難等の情報セキュリティの事件・事故が発生した後の被害を最小限にするための事後対応。

[51] デジタル・フォレンジック研究会発行の証拠保全ガイドラインの「証拠保全の一貫性（Chain of Custody）を証明できる書類」等を参照してください。

また、サービスを受ける場合には、必要となる情報を迅速に提供できるように事前に伝達内容や方法を取り決めておくことが望まれます。

3. 業務を委託している場合には、委託先と協力して体制を整備することが必要です。また、事後対策の連携体制について、あらかじめ契約等で明確化しておくことが望まれます。
4. 監督官庁への報告義務がある事案に関して、対応する体制を整えておくことが必要です。
5. 事業継続計画が存在する場合には、その計画との関係を考慮して内部不正対策の体制を構築することが必要です。

（２８）処罰等の検討及び再発防止

重大な不正を犯した内部不正者に対しては必ず組織としての処罰を検討しなければならない。また、必要に応じて、再発防止の措置を実施するとともに、再発防止の観点から内部不正の事例を組織の内部に告知することが望ましい。

■どのようなリスクがあるのか？

内部不正者に対する処罰を検討しない場合や再発防止策を実施しない場合には、同様の内部不正を再発させてしまう恐れがあります。また、再発防止の観点から内部不正の事例を組織の内部に告知･周知させない場合にも同様の内部不正を再発させてしまう恐れがあります。

■対策のポイント

内部不正者に対する処罰等の検討及び再発防止を検討するためには､以下のような内容を整備することが必要です。

1. 内部不正による影響を最小限にするために、求められる対応手順や報告手順等事業継続管理手順へ内部不正対策を組み込むことが必要です。内部不正者に対する処罰を検討するためには、本ガイドラインの（２2）法的手続きの整備で定めた内容を基に、人事担当者及び法務担当者、弁護士等で法的処置に関して検討することが必要です。
2. 内部不正の再発防止策を検討し、実施することが必要です。
3. 内部不正によるインシデントの具体的事象から学習し再発を防止するという観点から、発生した内部不正の事例を内部不正者に行われた処分も含めて組織の内部に告知することが望まれます。

4-10.組織の管理

（２９）内部不正に関する通報制度の整備

内部不正と思わしき事象が発生した場合についての通報制度を整備し各役職員が所属する部門以外の内部不正対策の関係者（総括責任者等）にも通報できる等、通報受付を複数設置し、必要に応じて通報者の匿名性を確保しなければならない。また、具体的な利用方法について教育を行うとともに周知徹底させなければならない。

■どのようなリスクがあるのか？

内部不正と思われる事象が発生した場合の通報制度を整備し、具体的な利用方法を教育していないと、内部不正の通報が機能せず、対応が遅れるだけではなく、内部不正の予兆を見逃してしまう恐れがあります。また、内部不正の通報受付を複数設置しない場合には、隠蔽行為によって問題が発生したと思われる部門から総括責任者等に情報が入らない(報告されない）恐れがあります。さらに、通報者の匿名性を確保しない場合には、周囲の人間関係等の影響から内部不正と思われる情報が得られない恐れがあります。

■対策のポイント

内部不正の通報制度については、以下のような内容を整備することが必要です。

1. 内部不正の通報に最低限必要となる以下の情報等を示すことが必要です。「受付窓口（連絡先と連絡方法)」、「対象となる情報や物理的資産」、「いつ、どのような状態（不正利用、破壊等）になったのか」、「事象をどのように知り得たのか」等
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ことが必要です。
3. 上記の内部不正の通報制度について教育を実施します。
4. 通報窓口（ホットライン等も含む）には、役職員が所属する部門長以外の窓口を設置することが望まれます。
5. 通報者が通報行為により不利益を受けないように匿名性を確保するため、匿名の私書箱や目安箱等を設置することや、第三者機関等の利用も検討することを考えます。

（３０）内部不正防止の観点を含んだ確認の実施

内部不正の防止及び抑止の観点から具体的な内部不正対策の項目を抽出し、定期的及び不定期に確認（内部監査等の監査を含む）を実施しなければならない。また、確認の結果については、総括責任者の確認のもと、経営者に報告するとともに、必要に応じて対策の見直しを実施しなければならない。

■どのようなリスクがあるのか？

（１）経営者の責任の明確化で記載したモニタリングを含め、定期的および不定期に確認や監査を実施しないと、内部不正対策の状況や組織の問題点が確認できず、効果的な対策の実施や見直しができない恐れがあります。

■対策のポイント

内部不正の防止や抑止の観点を盛り込んだ確認や監査（内部監査及び外部監査を含む）を行うためには、以下のような項目を検討し、計画を立てた上で、これに基づいて実施することが必要です。実施後には、改めてリスクの評価を行い、経営者のリーダーシップの下、対策やリソース配分の見直しを図ることが必要です。

1. 内部不正対策として特に実施することが望まれる項目（内部不正事例等で関連すると思われる事項）を参照し、具体的な対策の実施状況や整備状況等を確認し、経営者に報告することが必要です。
2. 各部門の業務内容や関係者との取り決めによって、同様の情報についても異なる管理や取り扱いが行われていないか等を確認することが必要です。
3. 内部不正と思われる事象や関連する事件・事故等の記録を確認し、それらの発生後に速やかに報告されているかを確認することが必要です。また、重要情報の管理手順や取扱方法に違反した事例の有無や、その後の対処方法等を確認することが必要です。
4. 内部不正の対策は、情報通信技術の進歩や、新たな脅威の出現、新しい法律の施行、など技術的・社会的な状況によっても見直すことが必要です。継続して、見直し、改善を図ります。

付録Ⅰ：内部不正事例集

IPA が実施した内部不正のインタビュー調査[52]、及び、「組織における内部不正防止ガイドライン検討委員会」の委員から得られた事例を以下に示します。

No	概要	本ガイドラインの関連項目
1	地方金融機関において、営業員が休眠口座の預金を着服した。 【主な原因】 営業成績のよい営業員を配置転換せずにいたこと及び相互に監視しない環境であったことから、不正行為が見つかりにくい環境であった。	(24)公平な人事評価の整備 (26)職場環境におけるマネジメント
2	中小企業において、システム管理者が社長の PC の設定を変更して社長宛のメールを自身のメールアカウントに転送して読んでいた。 【主な原因】 この企業には、システム管理者を担当する社員が１人しかおらず、内部不正を行っても見つかりにくい環境であった。また、この社員は、システム管理者に求められる規範意識が低かったことも考えられる。	(7)情報システムにおける利用者の識別と認証 (19)教育による内部不正対策の周知徹底
3	企業において、システム管理者の社員が、自宅で業務を行うために機密情報を持ち出し、Winny（ファイル交換ソフト）がインストールされた自宅の PC で業務を行ったことで機密情報を漏えいさせてしまった。 【主な原因】 機密情報を誰にも知られることなく持ち出せた。許可なく自宅で業務を行い、機密情報を漏えいさせた場合の処罰の重さを十分理解していなかったことも考えられる。	(12)ネットワーク利用のための安全管理 (19)教育による内部不正対策の周知徹底
4	ノート PC が机の上に山積み状態で長期間放置されていた環境で、ノート PC が知らぬ間に紛失していた。その後の調査によって、ノート PC が売却されていることが発覚したが、犯人は不明であった。 【主な原因】 ノートPCの管理がされておらず、フロアに入れるものであれば誰でも持っていくことができた。	(9)情報機器及び記録媒体の資産管理及び物理的な保護
5	企業において、社員が機密情報の入った CD-ROM を持ち出し、機密情報を換金していた。この社員は、情報システムから機密情報を取り出す際に、部下に仕事の一環と説明して正規の手続きで機密情報の入った CD-ROM を作らせて、隠蔽を図っていた。 【主な原因】 機密情報の入った CD-ROM の持ち出し管理がされていなかった。	(9)情報機器及び記録媒体の資産管理及び物理的な保護
6	企業において、開発者が「自身が開発したソース等は自分のもの」「他のプロジェクトでも役立ちそう」という認識から、開発ソース等を外部のオンラインストレージにアップロードして持ち出していた。	(12)ネットワーク利用のための安全管理 (19)教育による内

[52] 「組織内部者の不正行為によるインシデント調査」（2012 年 7 月）、「内部不正による情報セキュリティインシデント実態調査」（2016 年 3 月）
URL: https://www.ipa.go.jp/security/insider/

No	概要	本ガイドラインの関連項目
	【主な原因】 開発者は「開発物は企業の所有物である」との認識がなかった。また、外部のオンラインストレージ等の使用を制限していなかった。	部不正対策の周知徹底
7	企業において、システム管理者が機密情報を繰り返し持ち出して換金していた。繰り返す度に機密情報の持ち出し行為がエスカレートしていった。 【主な原因】 システム管理者の操作を監視することになっていたが、担当者が確認を怠っていたため、機密情報を繰り返し持ち出された。また、システム管理者の権限を分散せず、一人に権限が集中していたことも考えられる。	(6)システム管理者の権限管理 (18)システム管理者のログ・証跡の確認
8	企業において、在宅勤務の社員が、自宅の PC からインターネットを介して企業の情報システムに接続し、機密情報を取得して換金していた。在宅勤務は、監視の目が届きにくいことから、オフィスと比べて内部不正が発生しやすい環境である。 【主な原因】 在宅勤務等によるインターネットを介しての情報システム及び機密情報へのアクセスを制限していなかった。また、在宅勤務において必要な情報以外にもアクセスしていないかを監視していなかったことも考えられる。	(15)組織外部での業務における重要情報の保護 (17)情報システムにおけるログ・証跡の記録と保存
9	企業において、社員が転職先で利用する目的で退職時に開発物をまとめてダウンロードして持ち出した。 【主な原因】 開発物を持ち出して転職先で利用してはいけないという認識がなかった。また、多量なファイルへのアクセス等の通常の業務と異なる事象が発見された場合の確認や対策が実施されていなかった。	(5)情報システムにおける利用者のアクセス管理 (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
10	企業において、営業社員がリストラによって退職する際に、PC のパスワードを無断で変更し、変更したパスワードを忘れたとして通知しなかった。 【主な原因】 雇用終了前の一定期間から、PC の管理権限を企業側においていなかった。	(21)雇用終了及び契約終了による情報資産等の返却
11	企業において、ある部門の社員（複数名）が新会社立上げを考え一斉に退職する際に、顧客情報（営業秘密）を新会社で利用する目的で持ち出した。 【主な原因】 営業秘密を不正に持ち出して、使用する行為が、不正競争防止法違反にあたるという認識が乏しかった。	(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 (23)誓約書の要請
12	企業において、委託先のサイト構築・運営会社の従業員が不正行為と知りつつもその企業の顧客情報を他社に渡していた。その他社はその顧客情報を使って営業活動を行っていた。 【主な原因】 委託先のサイト構築・運営会社の情報セキュリティ対策が十分であることを確認できていなかったことが考えられる。	(13)重要情報の受渡し保護 (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）

No	概要	本ガイドラインの関連項目
13	製造販売メーカーにおいて、元従業員がこの製造販売メーカーの設計図面を利用して同業他社で同種の製品を製造して販売していた。 【主な原因】 退職時に重要情報の資産等の返却がしっかりと行われていなかった。	(21)雇用終了及び契約終了による情報資産等の返却
14	企業において、メンテナンス業務を委託した際に、渡した個人情報が再委託先のアルバイトによって複製され換金された。 【主な原因】 委託先の重要情報の管理体制を明確にし、再委託先までの管理ができていなかった。	(13)重要情報の受渡し保護 (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)
15	企業において、元従業員がインターネットから企業ネットワークへのリモートアクセス接続サービスを使って、機密情報を持ち出していた。 【主な原因】 企業ネットワークへのリモートアクセス接続サービスにおいて、元従業員のアカウントが削除されていなかった。	(5)情報システムにおける利用者のアクセス管理
16	教育機関において、先生が生徒の成績等の情報を USB メモリで持ち出した際に、盗難に遭い生徒の情報が漏えいしてしまった。 【主な原因】 生徒の情報を暗号化していなかった。	(15)組織外部での業務における重要情報の保護
17	教育機関において、個人のスマートフォンの業務利用を黙認されていた環境でスマートフォンが盗難に遭い、スマートフォン内の個人情報が漏えいした。 【主な原因】 個人のスマートフォンの業務利用を黙認し、適切な利用範囲を定めて運用していなかった。	(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
18	金融機関の ATM の保守管理業務を委託している企業の社員が、ATM の取引データから顧客のカード情報を不正に取得した。この情報から偽装キャッシュカードを作成・所持し、現金を引き出した。 【主な原因】 プロジェクト責任者であった元社員に権限が集中し、ひとりでカードの偽装が可能だった。また、相互に監視する体制も十分でなかった。	(6)システム管理者の権限管理
19	企業において、業務提携先の元社員が、企業の研究データを不正に持ち出し、転職先の海外企業に提供していた。 【主な原因】 待遇への不満が動機のひとつであった。また、退職前には情報の持ち出し等の内部不正が発生しやすいことから、記録媒体の利用制限、重要情報へのアクセス履歴等のログの記録により、監視する必要があった。	(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資産等の返却 (24)公平な人事評価の整備
20	企業において、顧客データベースを保守管理するグループ会社の業務委託先の社員が、販売目的で個人情報を不正に取得し、持ち出した。 【主な原因】 私物を持ち込むことが可能だった。また、業務用 PC には記録媒体を接続できないよう対策がされていたが、最新型のスマートフォンを接続した場合に記録媒体として認識されてしまい、データをコピーし持ち出すことが	(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 (16)業務委託時の確認(第三者が提

No	概要	本ガイドラインの関連項目
	できた。さらに、企業は業務委託先以降のセキュリティ対策が不十分であることを確認していなかった。	供するサービス利用時を含む） (30)内部不正防止の観点を含んだ確認の実施
21	企業において、業務委託先の従業員が、顧客情報を不正に持ち出し、自宅に設置している個人所有の NAS(Network Attached Storage)に保存していた。NAS の認証機能の設定が不適切だったため、インターネット上に顧客情報が流出した。 【主な原因】 業務委託先のセキュリティ対策について、定期的な確認ができておらず、顧客情報の取扱いや管理体制の不備に気づけなかった。	（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)
22	企業において、従業員が、顧客から Web の問い合わせフォームに入力された内容を、個人のアドレスにも送信するよう設定し、問い合わせ内容を不正に入手していた。 【主な原因】 従業員であれば誰でも設定変更できる状態であった。また、漏えい疑義に際しては、ログの保管期間が短く、必要なログが残っていなかったため、原因究明調査に時間がかかった。	（5）情報システムにおける利用者のアクセス管理 （17）情報システムにおけるログ・証跡の記録と保存
23	企業において、従業員が、会社が貸与していたスマートフォンにインストールしたアプリを利用して、会社のパソコンに接続し、Wi-Fi 経由で機密情報を外部に持ちだした。 【主な原因】 許可されたソフトウェア以外のものをスマートフォンにインストールして利用した。また、会社のパソコンが、許可されていないアクセスポイント等と制限なく、Wi-Fi 接続できる状態であった。	（12）ネットワーク利用のための安全管理 (15)組織外部での業務における重要情報の保護
24	企業において、元従業員が、在職中に重要情報をメールに添付し、複数回に分けて自宅のアドレスに送っていたことが発覚した。 【主な原因】 個人のメールアドレスへの送信や外部宛てのメールに対するモニタリングや確認を行っていなかった。営業秘密を不正に取得し、転職先等で利用することは不正競争防止法違反にあたるという認識が不足していたと考えられる。	（12）ネットワーク利用のための安全管理 (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

付録Ⅱ：内部不正チェックシート

内部不正チェックシートは、本ガイドラインの第４章 対策の指針をまとめたものです。

※ □:主担当/実施部門[53]、[ ]:サポート/実施補助･確認部門[54]

No	内容	チェック欄
4-1. 基本方針		
(1)-①	内部不正の対策が経営者の責任であることを組織内外に示す「基本方針」を策定し、役職員に周知徹底していますか?	□:経営者(最高責任者)
(1)-②	「基本方針」に基づき対策を実施するためのリソースが確保されるよう、必要な決定、指示をしていますか?	□:経営者(最高責任者)
(2)-①	経営者は、内部不正対策の総括責任者の任命及び管理体制と実施策の承認を行っていますか? (ただし、経営者が組織全体に目が届く組織であれば、自ら内部不正対策の実施にあたり、管理体制を必ずしも構築する必要はありません。)	□:経営者(最高責任者)
(2)-②	総括責任者は、基本方針に則り組織横断的な管理体制を構築し、実施策を策定していますか?	□:総括責任者

No	内容	直接部門	関連部門			
			情報システム部門	総務部門	人事部門	法務･知財部門
4-2-1. 秘密指定						
(3)	重要情報を把握し、重要度に合わせて格付け区分し、取り扱い可能な内部者の範囲を定めていますか?	□				
(4)-①	重要情報の作成者は、定めた格付け区分を選択し、その選択について上司等に確認を得ていますか?	□				
(4)-②	重要情報を含む電子文書には、内部者が分かるように機密マーク等の表示をしていますか?	□				

[53] 業務の観点からチェックシートの対策項目を実施する上で適切と考えられる部門。

[54] 主担当部門/実施部門が、対策の策定や実施をする上で、連携すべきと考えられる部門。

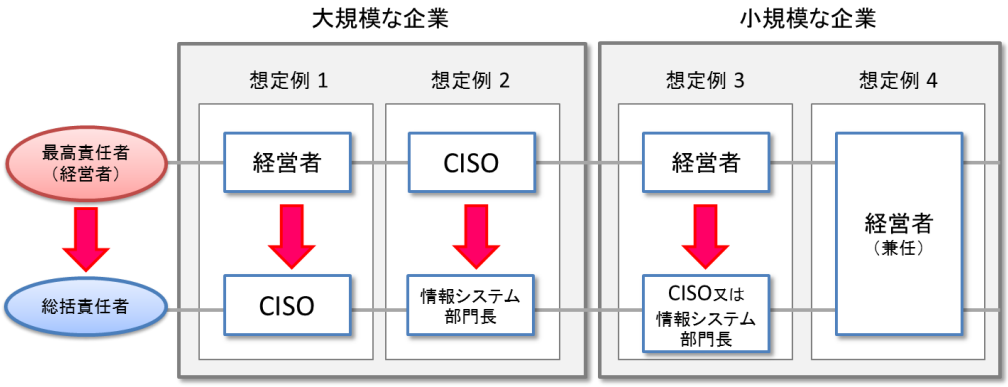
No	内容	直接部門	関連部門			
			情報システム部門	総務部門	人事部門	法務･知財部門
4-2-2. アクセス権指定						
(5)-①	情報システムを管理･運営する担当者は、利用者 ID 及びアクセス権の登録･変更･削除等の設定手順を定めて運用していますか?		□			
(5)-②	情報システムを管理･運営する担当者は、異動又は退職により不要となった利用者 ID 及びアクセス権を、ただちに削除していますか?		□			
(6)	複数のシステム管理者がいる場合は、情報システムの管理者 ID ごとに適切な権限範囲の割り当てを行い、相互に監視できるように設定していますか? また、システム管理者が一人の場合は、ログ等により監視していますか?	□	[ ]			
(7)	情報システムでは、共有 ID や共有のパスワード･IC カード等を使用せず、個々の利用者 ID を個別のパスワード･IC カード等で認証していますか?	[ ]	□			
4-3. 物理的管理						
(8)	重要情報の格納場所や取り扱う領域等を物理的に保護するために壁や入退管理策によって保護していますか?	□	[ ]	[ ]		
(9)-①	PC 等の情報機器や USB メモリ等の携帯可能な記録媒体は、盗難や不正持ち出し等がないように管理･保護していますか?	□	[ ]			
(9)-②	情報機器や記録媒体を処分する際には重要情報が完全消去されていることを確認していますか?	□	[ ]			
(10)	モバイル機器や携帯可能な記録媒体を外部に持ち出す場合には、持ち出しの承認及び記録等の管理をしていますか?	□	[ ]			
(11)	個人のモバイル機器及び記録媒体の業務利用及び持込を制限していますか?	[ ]	□			
4-4. 技術･運用管理						
(12)	組織のネットワークは、重要情報を不正に持ち出し可能なファイル共有ソフトや SNS、外部のオンラインストレージ等の使用を制限していますか?		□			
(13)-①	委託先等の関係者への重要情報の受渡しは、受渡しから廃棄迄を含めて管理していますか?	□	[ ]			
(13)-②	インターネット等の組織外を介す重要情報の受渡しでは、誤って関係者以外に渡ってしまうことも考慮し、暗号化等で保護していますか?	□	[ ]			

No	内容	直接部門	関連部門			
			情報システム部門	総務部門	人事部門	法務･知財部門
(14)	組織外部で利用･取り扱い可能な重要情報を限定し、重要情報や情報機器を保護していますか?	□	[ ]			
(15)	組織外で重要情報を用いた業務を行う際に、周囲の環境やネットワーク環境等を考慮して保護していますか?	□	[ ]			
(16)	委託する業務内容に応じたセキュリティ対策を契約前に確認･合意し、契約期間中にも契約通りにセキュリティ対策が実施されていることを確認していますか?	□	[ ]			[ ]
4-5. 証拠確保						
(17)	重要情報へのアクセス履歴及び利用者の操作履歴等のログ･証跡を定めた期間に従って安全に保護していますか?（推奨）	[ ]	□			
(18)	システム管理者のアクセス履歴や操作履歴等のログ･証跡を記録して保存するだけでなく、そのログ･証跡の内容を定期的にシステム管理者以外が確認していますか?		□			
4-6. 人的管理						
(19)-①	すべての役職員に教育を実施し、組織の内部不正対策に関する方針及び重要情報の取り扱い等の手順を周知徹底していますか?	□		[ ]	[ ]	
(19)-②	教育を定期的に繰り返して実施し、教育内容を定期的に見直して更新していますか?	□		[ ]	[ ]	
(20)	雇用の終了時に秘密保持義務を課す誓約書の提出を求めていますか?（推奨）	□		[ ]	[ ]	[ ]
(21)	役職員の雇用終了時および請負等の契約先との契約終了時に、取り扱いを委託した情報資産のすべてを返却または完全消去し、情報システムの利用者 ID や権限を削除していますか?	□		[ ]	[ ]	[ ]
4-7. コンプライアンス						
(22)	就業規則等の内部規程を整備し、正式な懲戒手続を備えていますか?	□		[ ]	[ ]	[ ]
(23)	役職員に対して重要情報を保護する義務があることを理解させるために「秘密保持誓約書」等を要請していますか?	□		[ ]	[ ]	[ ]

No	内容	直接部門	関連部門			
			情報システム部門	総務部門	人事部門	法務・知財部門
4-8. 職場環境						
(24)	公平で客観的な人事評価を整備するとともに、業績に対する評価を説明する機会を設ける等、人事評価や業績評価の整備を推進していますか？（推奨）			[ ]	□	
(25)	業務量及び労働時間の適正化等の適切な労働環境を整備するとともに、業務支援を推進する体制や相談しやすい環境を整える等職場内において良好なコミュニケーションを組織全体で推進していますか？（推奨）			□	[ ]	
(26)	相互監視ができない環境における単独作業を制限し、単独作業には事前承認、事後確認等の手続きを定めていますか？（推奨）	□		[ ]	[ ]	
4-9. 事後対策						
(27)	内部不正の影響範囲を特定するために、事象の具体的状況を把握するとともに、被害の最小化策や影響の拡大防止策を実施し、必要に応じて組織内外の関係者との連携体制を確保していますか？	□	[ ]			
(28)	内部不正者に対する処罰を検討し、内部不正の事例を内部に告知することを検討していますか？	□	[ ]			
4-10. 組織の管理						
(29)	内部不正と思わしき事象が発生した場合についての通報制度を整備し、通報受付を複数設置し、必要に応じて通報者の匿名性を確保していますか？	□	[ ]			
(30)	内部不正対策の項目を抽出し、定期的及び不定期に確認（内部監査等の監査を含む）し、確認した結果は、経営者に報告し、必要に応じて対策の見直しを実施していますか？	□	[ ]			

付録Ⅲ：Q&A 集

対策のヒントとなる Q&A1

Q-1 基本方針をどのように策定すればよいかわかりません。(4-1(1)、4-1(2))
A-1 本ガイドラインの示す基本方針は、既存の情報セキュリティ基本方針を利用すること想定しています。必要に応じて、内部不正対策に関する事項を追記します。 以下では、情報セキュリティ基本方針を策定していない組織を対象に最低限の内容を説明します。 基本方針では、社内での重要情報の保護・管理の徹底、及び社外への説明責任の観点から以下の 3 項目を最低限定めてください。 ①経営者は経営課題の一つとして、リスク管理を行う必要があることを認識し、その一環として内部不正を防止し、重要情報を保護・管理することの重要性を示します。 ②保護・管理すべき重要情報を識別し、その重要情報に関して事業上の重要性を示します。重要情報とは、企業及び団体の事業に大きな影響を与える情報です。例としては、戦略的な情報及び公開されていない知的財産を含む製造・開発情報や営業情報等です。また、秘密管理を行うことが義務付けされた関係者から得た共有情報等も含みます。 ③重要情報の保護・管理に関する実施体制を策定し、見直しを行いつつ継続的な活動であることを示します。実施体制には、内部不正対策を実施するにあたり、整備すべき体制を記載します。最低限責任者を示すことが必要です。また、継続的によりよい対策としていくための活動について示します。 詳しくは、付録Ⅴの基本方針の記述例を参照してください。 なお、基本方針で記載した体制は、大規模な企業と小規模な企業に分けて、各々2 種類の体制が想定されます。体制についての概要を以下の図を用いて説明します。    大規模な企業においては、経営者を最高責任者とし、CISO を総括責任者とした体制(想定 1)、CISO を最高責任者とし、情報システム部門長を総括責任者とした体制(想定 2)を想定しています。また、小規模な企業においては、経営者を最高責任者とし、CISO を総括責任者とした体制(想定 3)、経営者が最高責任者と総括責任者を兼任する体制(想定 4)を想定しています。

対策のヒントとなる Q&A2

Q-2 重要な情報をどのように区分すればよいかわかりません。(4-1(1))
A-2 まずは、保護対象の情報か否かの 2 つに区分するとよいでしょう。保護対象の情報は、組織内での取扱ルールを決めて管理しましょう。実際の業務の中で、保護対象の情報で重要度の違いによって取り扱いを変える必要がある場合に、区分を増やして管理すればよいでしょう。ただし、区分が増えすぎると管理が煩雑になるため、4 区分程度にすることが望まれます。

対策のヒントとなる Q&A3

Q-3 重要な情報(重要情報)にはどのような情報があるのかわかりません。(4-1(1))
A-3 重要情報は、各部門の業務内容や取り扱う情報によって異なります。例えば、営業部門であれば、顧客情報や関係者限りの営業情報等になります。また、開発部門であれば、開発物や設計書等が重要情報と考えられます。一般的には、組織の利益に影響を与える情報と考えられますが、重要情報を組織外の関係者と共有することで利益に結び付く場合もあり、主管部門の業務や状況によって様々な共有範囲や取り扱いが考えられます。さらに、ある時期までは重要度が高く、一定期間を経ると公知情報となる情報もあり、重要度は時間とともに変化する情報もあります。

対策のヒントとなる Q&A4

Q-4 専門部署や委員会とはどのようなものかわかりません。(4-1(2))
A-4 例えば、重要情報の取り扱いを総括する部署や、総括責任者等が代表者となり重要情報の取り扱いを監督する「管理委員会」を設置するなどです。参考として、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」(平成 28 年 12 月 28 日改正)では、組織的安全管理措置の望まれる手法として「個人データの取扱いを総括する専門部署の設置、及び個人情報保護管理者(CPO)が責任者となり、社内の個人データの取扱いを監督する「管理委員会」の設置」を挙げています。

対策のヒントとなる Q&A5

Q-5 重要情報へのアクセスを制限するために、できるだけコストを抑える方法を教えてください。(4-2-2(5))
A-5 例えば、Windows のセキュリティ機能を利用し、重要情報が保存されたフォルダのアクセス制限をすることができます。 Windows では、フォルダを右クリックして呼び出すプロパティの中で、共有設定とセキュリティ設定ができるようになっており、重要情報のアクセスを必要な個人やグループに限定する「アクセス権限」を指定できます。この時、「ロールベースアクセス制御」の考え方に基づき、重要情報へのアクセス権限を「役割(ロール)」毎に指定することもできます(役割とは、例えば、課長などの職務や人事部などの所属部署です)。役割による指定をすれば、権限者に異動があっても、重要情報へのアクセス権限の割り当てを見直すことなく運用管理ができます。 サーバを利用しない「ワークグループ環境」でも、情報を保存している PC で権限者のアカウントや役割グループを作成する方法があります。この方法を利用すると、アカウントが少ない小規模シス

テムであれば、重要情報を保護するアクセス制限を実現できます。ただし、サーバの台数が多い場合は、管理が煩雑になる場合があります。
さらに、多数のアカウントの制御をしなければならないシステムでは、サーバでユーザの属性情報を一元管理することができる「Active Directory」を利用すれば、適切なアクセス制限の運用が容易です（ただし、付加的なライセンス費用が必要です）。

対策のヒントとなる Q&A6

Q-6 アクセス数・量に伴う通知システムを導入し、モニタリングを行おうとしています。通知が行われるアクセス数・量の基準値をどのように設定すればよいかわかりません。（4-2-2（5））
A-6 通知システムを利用してモニタリングを行う場合、通知が行われる基準値が大きすぎる場合には、必要な通知が行われない一方で、小さすぎる場合は、通知が頻繁すぎることで不正を発見しづらくなるため、システム運用実態にあわせ基準値を設定し、見直していくことが重要です。

対策のヒントとなる Q&A7

Q-7 単純な文字列を設定しないよう、利用者が管理するパスワードの規約をどのように設定してよいかわかりません。（4-2-2（7））
A-7 単純な文字列とは、ID と同じパスワードの設定や、氏名や名前及び生年月日や、キーボード配列（例えば 12345678 や QWERTYU 等）です。これらの単純な文字列の設定を避けるため、例えば、英数大文字小文字を含め、8 桁以上等と規約を定めます。

対策のヒントとなる Q&A8

Q-8 重要情報を扱う物理的区画についてどのようにセキュリティを強化すべきかわかりません。（4-3（8））
A-8 重要情報を扱う物理的区画（敷地内及び建物、諸室等）に、入ることができる人を制限し、対象となる個人を識別できるようにします。又は、入退館（室）の履歴を個人単位で記録し、その記録を適切に管理し、定期・不定期に確認します。なお、これらの履歴を自動記録する機材の導入や設置が難しい場合には、入退館（室）の履歴を書面に残す形で記録し、その書面を適切に管理し、定期・不定期に確認します。この場合の入退館（室）履歴情報が記載された書面は、他の入退館者の目に触れることがないようにすることが重要です。重要情報を扱う区画、およびその場所の鍵や入場を許可する IC カード等については以下のような事項を検討することが必要です。 ① 鍵や IC カード等の運用・管理 ・ 役職員間の鍵や IC カードの貸借を原則禁止とし、責任者（重要情報を扱う区画の責任者）の確認のもと鍵、IC カードの貸出／返却記録を行います。 ・ ディンプルキー、カード等の容易には複製できない鍵、IC カードを使います。 ・ 異動／退職等で鍵、IC カードが必要なくなった場合には、確実に鍵を返却させます。 ・ 鍵、IC カードを紛失した場合に備え、鍵紛失時の諸手続を定める（マニュアルを作成する）とともに、紛失した鍵、IC カードを無効にする措置がすぐとれるようにします。 ・ 鍵、IC カード貸出者に対する定期・不定期（抜き打ち）の所持確認を行います。

・ スペア鍵等が、どこの鍵か判る情報を照合できない状態で保管します。

・ ある鍵番号のスペア鍵が、どこの鍵か判る情報を「重要情報」として扱います。

② 入退室記録（履歴）の確認

・ 入退出記録（カメラ画像を含む）を定期・不定期に確認し、鍵の操作者(IC カード所持者)と実際の入退出者を照合します。

・ 入退出管理で得られた入室情報と退出情報は定期・不定期に照合し、不自然な点がないかどうかを確認します。

③ その他

・ 重要情報を扱う物理的区画内の行動についてはカメラ等で監視するとともに、監視している旨を伝えます。

・ 故意に解錠した窓等からの侵入も判るように機械警備システム等の導入を検討することも必要です。

・ 緊急の入室や一般的には入室が想定されていない経営者や特権所有者等の入室等の例外規定については別途定めることが望まれます。

対策のヒントとなる Q&A9

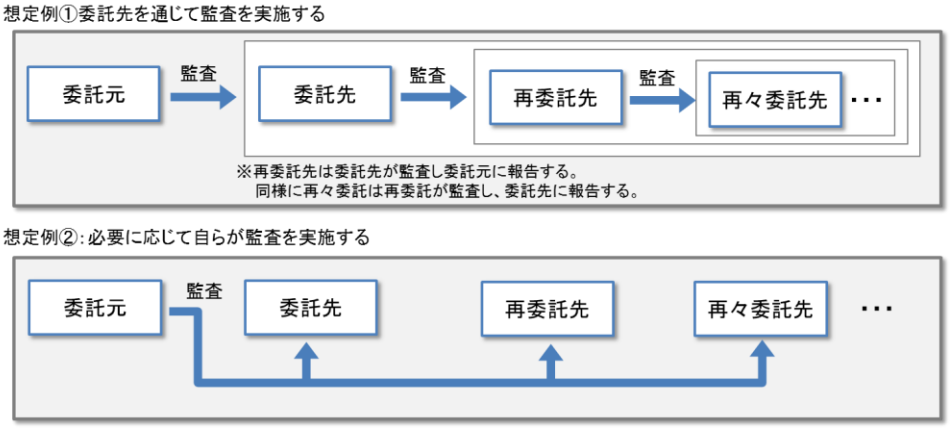
Q-9 重要情報の取り扱い（受け渡し）に関する手順をどのように設定してよいかわかりません。（4-4（13））
A-9 重要情報の取り扱い（受け渡し）に関する手順は、ネットワーク経由であれば、電子メールとオンラインストレージによって手順が異なります。 例えば、電子メールであれば、重要情報を添付して送付することを想定すると、「必ず重要情報を暗号化したものを添付する」や「復号するパスワードの伝達は電話等の電子メール以外の手段を用いる」等の規程を定めます。 オンラインストレージであれば、自社で用意したオンラインストレージのみの使用に限定するかを検討することが必要です。自社のオンラインストレージであれば、「ダウンロードの可能な期間」や「ダウンロード時のパスワードの受渡し」等の規程を定めます。また、インターネット上のオンラインストレージサービスを利用する場合には、誰もがダウンロードできてしまうサービスを使用しないことを前提として、「アップロードする重要情報を必ず暗号化する」や「ダウンロード先とパスワードを同じメールで送らない」等の規程を定めます。

対策のヒントとなる Q&A10

Q-10 重要情報を暗号化するために、できるだけコストを抑える方法を教えてください。(4-4(14))
A-10 例えば、Windows の機能（EFS）を利用し、フォルダやファイルを暗号化することができます。フォルダを右クリックして呼び出すプロパティの中の、「属性詳細設定」で暗号化の設定が可能です。重要情報を含むフォルダを暗号化し、ハードディスクの盗難などで持ち出された場合でも情報が読まれることを防ぐことができます。ログオンした正規のユーザは特に暗号化／復号を意識せずに情報の読み書きが可能です。ただし、暗号化した場合は、暗号化キーと証明書をバックアップして必ず安全な場所（情報を保存しているPCの外部等）に保管しておくといった注意が必要です。この暗号化機能は、Windows7 以降での使用を想定しています。Windows のバージョン、エデ

ィション、及びファイルシステムフォーマットによっては制約があり、確認が必要です。

対策のヒントとなる Q&A11

Q-11「委託先を通じて、または必要に応じて委託元が、監査を実施する」の意味がわかりません。(4-4(16))
A-11 以下の図の 2 つの方法いずれかを指しています。図では、①委託先を通じて監査する場合と、②必要に応じて自ら(委託元)が監査する場合を表しています。なお、再委託先が再々委託を実施する場合以降も同様です。 

対策のヒントとなる Q&A12

Q-12 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-12 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&A13

Q-13 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-13 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。

対策のヒントとなる Q&A14

Q-14 どのような内容を教育すればよいかわかりません。(4-6(19))
A-14 教育では、内部者の内部不正対策の理解や意識を高める内容を行うべきであり、具体的には以下のようなものが考えられます。 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。 ② 運用規程に示されている重要情報の分類や管理方法等に関する順守すべき事項を説明しま

す。例えば、機密情報が記された FAX、プリントアウトその他の書類が長時間放置されたままにならないようなルール、内部不正を発見したときの通報の手順等について説明します。

③ 社内規則等の内部規程に基づき内部不正が発覚した際の懲戒処分について説明します。例えば、具体的な事案を基に内部不正に対して懲戒処分の内容を説明すると効果的です。

④ 重要情報の管理方法を示すとともに対策を実施していることについて説明します。例えば、対策内容についてはメールのアーカイブ等の監視やモニタリング等を行っていることを説明すると効果的です。

⑤ 内部不正対策の理解を深めるために、運用規程の背景となる関連する法令等（不正競争防止法、個人情報保護法等）について説明することが望ましいです。

対策のヒントとなる Q&A15

Q-15 取り扱いを委託した情報資産や与えた権限としてどのようなものがありますか。（4-6（21））

A-15 以下のような情報等があります。

① 重要情報

- 顧客情報（仕入れや売上に関する購買・営業情報等一般に公開されていない情報も含む）
- プログラムソースや、設計図等の製造に関する情報
- 情報システムに関連する情報（情報システムの設定情報等）
- 企業が所有する公開されていない知的財産（特許）関連情報等

② ハードウェア

- PC（ノート PC 含む）、企業貸与のスマートフォン、CD-R/DVD-R、USB メモリ等

③ 与える権限

- 入館証
- 利用者 ID（と利用者 ID に対応したパスワード）
- 保管庫（金庫、ワゴン、キャビネット等）の施錠鍵

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）情報の格付け区分	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	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）業務委託時の確認（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

大項目	項目名	JIS Q 27001:2014 附属書 A 関連項目
		A.18.1 法的及び契約上の要求事項の順守
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

（2）営業秘密管理指針・秘密情報の保護ハンドブック

営業秘密管理指針では、不正競争防止法における「営業秘密」として、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。また、営業秘密として法的保護を受けられる水準を超えた、秘密情報の漏えい防止及び漏えい時の包括的な対策は、経済産業省「秘密情報の保護ハンドブック～企業価値向上に向けて～」に示されています。本ハンドブックは、秘密情報を内部不正等から守り、活用するための対策の参考としてご利用いただけます。

（3）個人情報の保護に関する法律についてのガイドライン（通則編）[55]

個人情報の保護に関する法律についてのガイドライン（通則編）では、個人情報保護法で求められる必要かつ適切な安全管理措置を示しています。個人情報保護の観点から、本ガイドラインを適用する場合、参考になる項目は、安全管理措置（法 20 条関連）の「講じなければならない事項」及び従業者の監督（法 21 条関連）、委託先の監督（法 22 条関連）です。以下に、対応する本ガイドラインの対策項目を示します。なお、社員による不正な個人情報の持ち出しに関して、本ガイドラインの「職場環境」は、個人情報の保護に関する法律についてのガイドライン（通則編）において存在しない項目です。「職場環境」の「対策のポイント」を参考にすることで、個人情報の不正な持ち出しの対策の強化に役立つと考えられます。

安全管理措置（法 20 条関連）		本ガイドラインの関連項目
基本方針の策定		(1) 経営者の責任の明確化
個人データの取扱いに係る規律の整備		―
組織的安全管理措置	(1) 組織体制の整備	(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 (27) 事後対策に求められる体制の整備 (29) 内部不正に関する通報制度の整備
	(2) 個人データの取扱いに係る規律に従った運用 (3) 個人データの取扱状況を確認する手段の整備	(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 (18) システム管理者のログ・証跡の確認 (21) 雇用終了及び契約終了による情報資産等の返却
	(4) 漏えい等の事案に対応する体制の整備	(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
	(5) 取扱状況の把握及び安全管理措置の見直し	(30) 内部不正防止の観点を含んだ確認の実施
人的安全管理措置	従業者の教育	(19) 教育による内部不正対策の周知徹底 (23) 誓約書の要請
物理的安全管理措置	(1) 個人データを取り扱う区域の管理	(8) 物理的な保護と入退管理
	(2) 機器及び電子媒体等の盗難等の防止	(9) 情報機器及び記録媒体の資産管理及び物理的な保護
	(3) 電子媒体等を持ち運ぶ場合の漏えい等の防止	(13) 重要情報の受渡し保護 (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

[55] 改正個人情報保護法（平成 27 年 9 月 9 日公布）の全面施行の日（平成 29 年 5 月 30 日）から施行。

安全管理措置(法 20 条関連)		本ガイドラインの関連項目
	(4) 個人データの削除及び機器、電子媒体等の廃棄	(4) 格付け区分の適用とラベル付け (9) 情報機器及び記録媒体の資産管理及び物理的な保護
技術的安全管理措置	(1) アクセス制御	(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
	(2) アクセス者の識別と認証	(7) 情報システムにおける利用者の識別と認証
	(3) 外部からの不正アクセス等の防止	(12) ネットワーク利用のための安全管理 (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) 情報システムの使用に伴う漏えい等の防止	(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 (30) 内部不正防止の観点を含んだ確認の実施

従業者の監督(法 21 条関連)	本ガイドラインの関連項目
個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たって、法第 20 条に基づく安全管理措置を遵守させるよう、当該従業者に対し必要かつ適切な監督をしなければならない。	(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

委託先の監督(法 22 条関連)	本ガイドラインの関連項目
(1) 適切な委託先の選定	(13) 重要情報の受渡し保護 (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) 委託契約の締結	
(3) 委託先における個人データ取扱状況の把握	

（4）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）[56]

特定個人情報の適正な取扱いに関するガイドラインでは、番号法第４条及び個人情報保護法第 51 条に基づき、事業者が特定個人情報の適正な取扱いを確保するための具体的な指針を示しています。特定個人情報の保護の観点から、本ガイドラインを適用する場合、参考になる項目は、委託の取扱い（法 10 条、11 条関連）、安全管理措置（法 12 条、33 条、34 条関連）です。以下に、対応する本ガイドラインの対策項目を示します。

委託の取扱い(法 10.11 条関連)	本ガイドラインの関連項目
委託先の監督 (委託先における安全管理措置、必要かつ適切な監督)	(13) 重要情報の受渡し保護 (16) 業務委託時の確認(第三者が提供するサービ

[56] 事業者のうち金融機関が行う金融業務に関しては、「(別冊) 金融業務における特定個人情報の適正な取扱いに関するガイドライン」が適用されます。

再委託(再委託の要件、再委託の効果、再委託先の監督)	ス利用時を含む)

安全管理措置(法 12.33.34 条関連)		本ガイドラインの関連項目
基本方針の策定		(1) 経営者の責任の明確化
取扱規程等の策定		―
組織的安全管理措置	a. 組織体制の整備	(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 (27) 事後対策に求められる体制の整備 (29) 内部不正に関する通報制度の整備
	b. 取扱規程等に基づく運用 c. 取扱状況を確認する手段の整備	(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 (18) システム管理者のログ・証跡の確認 (21) 雇用終了及び契約終了による情報資産等の返却
	d. 情報漏えい等事案に対応する体制の整備	(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
	e. 取扱状況の把握及び安全管理措置の見直し	(30) 内部不正防止の観点を含んだ確認の実施
人的安全管理措置	a. 事務取扱担当者の監督	―
	b. 事務取扱担当者の教育	(19) 教育による内部不正対策の周知徹底 (23) 誓約書の要請
物理的安全管理措置	a. 特定個人情報等を取り扱う区域の管理	(8) 物理的な保護と入退管理
	b. 機器及び電子媒体等の盗難等の防止	(9) 情報機器及び記録媒体の資産管理及び物理的な保護
	c. 電子媒体等を持ち出す場合の漏えい等の防止	(13) 重要情報の受渡し保護 (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
	d. 個人番号の削除、機器及び電子媒体等の廃棄	(4) 格付け区分の適用とラベル付け (9) 情報機器及び記録媒体の資産管理及び物理的な保護
技術的安全管理措置	a. アクセス制御	(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
	b. アクセス者の識別と認証	(7) 情報システムにおける利用者の識別と認証
	c. 外部からの不正アクセス等の防止	(12) ネットワーク利用のための安全管理 (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
	d. 情報漏えい等の防止	(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
従業者の監督		(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

付録Ⅴ：基本方針の記述例

以下に基本方針の例を示しますので、必要に応じて追記・修正を行って使用してください。

（基本方針の例）

1. 内部不正対策の意義

基本方針（以下「本方針」という）は、【○○○（例：独立行政法人情報処理推進機構）】（以下「本組織」という」において取り扱う重要情報及び情報システムを内部不正による脅威から保護し、事業において安全かつ有用に活用するための必要事項を定めることを目的に制定します。今後、内部不正対策を重要な経営課題のひとつと捉え、本組織で取り組むべく推進します。

2. 重要情報の保護

本方針では、本組織が保護すべき重要情報を【○○○、△△△、□□□（例：顧客情報）】と指定します。

・○○○は、…である。
・△△△は、…である。
・□□□は、…である。
・（例：開発情報は、製品の他社有意性を守るために重要な製造委託会社外に漏らしてはならない）

これらの重要情報に対して業務実態に応じた適切な対策を講じます。対策の実施は本組織において周知徹底します。

3. 実施体制

内部不正に対して組織的に対策する体制を確立するために、その役割と責任を定めます。

・最高責任者　・・・　【○○○（例：代表取締役等の経営陣）】
　内部不正対策に関して意思決定を行う最高責任者。
・総括責任者　・・・　【△△△（例：代表取締役等の経営陣）】
　内部不正対策に関する重要事項を決定し、対策状況の確認及び見直しを行い、
　内部不正が発生した場合の対応及び状況の確認を行う責任者。

※【○○○】と【△△△】は同じでもよい。

3-1. 最高責任者によるモニタリング

最高責任者は、内部不正対策の方針づけを行い、その方針に関する定期的な報告を総括責任者から継続的に受けて評価します。必要に応じて、実施体制や方針を見直します。

3-2. 総括責任者による対策実施と報告

総括責任者は、最高責任者の方針づけを基に具体的な対策を立案し、実施状況を定期的に最高責任者に報告します。

4. 基本方針の見直し

本方針は、効果的で効率的な内部不正対策を維持するために、定期的な見直しを行い、必要に応じて改訂します。

付録Ⅵ：内部不正防止の基本 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)
	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、利益を得にくくすることで犯行を防ぐ			
	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、持ち込み禁止のポスター	(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、重要情報所持時の飲酒制限)	-

※対策例の( )は、本ガイドラインの対策項目以外の例です。

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[57]。

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

[57] 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)情報の格付け区分 (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	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
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		
重要情報が保管されているフロアに容易に入れる	③物理的な管理	(8)物理的な保護と入退管理 (9)情報機器及び記録媒体の資産管理及び物理的な保護
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		
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)システム管理者の権限管理
操作履歴(ログ)を採取していない	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
採取したログの定期監査をしていない		
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	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
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		
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	①適切な権限管理 （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
必要以上の要員に権限が付与されている		
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、業務利用が制限されていない	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
ルールが明確でない		
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	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
自社及び顧客、取引先などの被害を最小限に抑えたい		
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

■ 改版履歴

・1.0 版（2013 年 3 月 25 日）

・1.1 版（2013 年 5 月 7 日）
編集上の用語や用語使いの間違い等を修正

・1.2 版（2013 年 8 月）
用語使いの間違い等を修正

・1.3 版（2014 年 8 月）
用語を修正

・2.0 版（2014 年 9 月 26 日）
事例に基づき対策項目等を更新

・第 3 版（2015 年 3 月）
利用者からの要望事項の反映、及び改訂された標準規格・指針の関係箇所を更新

・第 4 版（2017 年 1 月）
関連するガイドライン等の追加、内部不正事例・コラムの追加、利用者からの要望事項の反映

組織における内部不正防止ガイドライン
2017年1月 第4版発行

独立行政法人 情報処理推進機構
〒 113-6591
東京都文京区本駒込2丁目28番8号 文京グリーンコートセンターオフィス
URL　http://www.ipa.go.jp
電話　03-5978-7530　FAX　03-5978-7518
E-Mail isec-info@ipa.go.jp