IPA Better Life with IT

2014.9.5　第1回　技術情報防衛シンポジウム

企業における内部不正の現状と内部不正防止ガイドラインの紹介

独立行政法人　情報処理推進機構
セキュリティセンター　情報セキュリティ分析ラボラトリー
ラボラトリー長　小松文子

目次

1. 2014年に相次ぐ内部不正事件

報道月	事件の概要	不正行為者	動機
7月	株式会社ベネッセコーポレーションの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元社員が、大量の個人情報を流出させたとして不正競争防止法違反の疑いで逮捕された。	委託先社員 SE	金銭の取得
5月	国立国会図書館のネットワークシステム保守管理の委託を受けている株式会社日立製作所の社員が、システムにアクセスできる権限を悪用して　国会図書館が発注した入札情報などを不正に入手し、営業担当の社員に送付していた。	委託先社員 SE	受注活動を有利にしたかった
5月	日産自動車株式会社の元社員が退職する直前、同社のサーバにアクセスし、販売計画など営業上の秘密を不正に得ていたとして不正競争防止法違反の疑いで逮捕された。	退職者	金銭の取得？（容疑否認）
3月	株式会社東芝の業務提携先であるサンディスク社の元社員が、東芝の機密情報を不正に持ち出し、転職先の韓国SKハイニックス社に提供したとして、不正競争防止法違反の容疑で逮捕された	退職者,技術者	処遇（給与等）の不満
2月	株式会社横浜銀行のATMの保守管理業務を委託している富士通フロンテック株式会社の元社員が、ATMの取引データから顧客のカード情報を不正に取得し、偽造キャッシュカードを作成・所持していた容疑で逮捕された。	委託先社員、技術者	金銭の取得

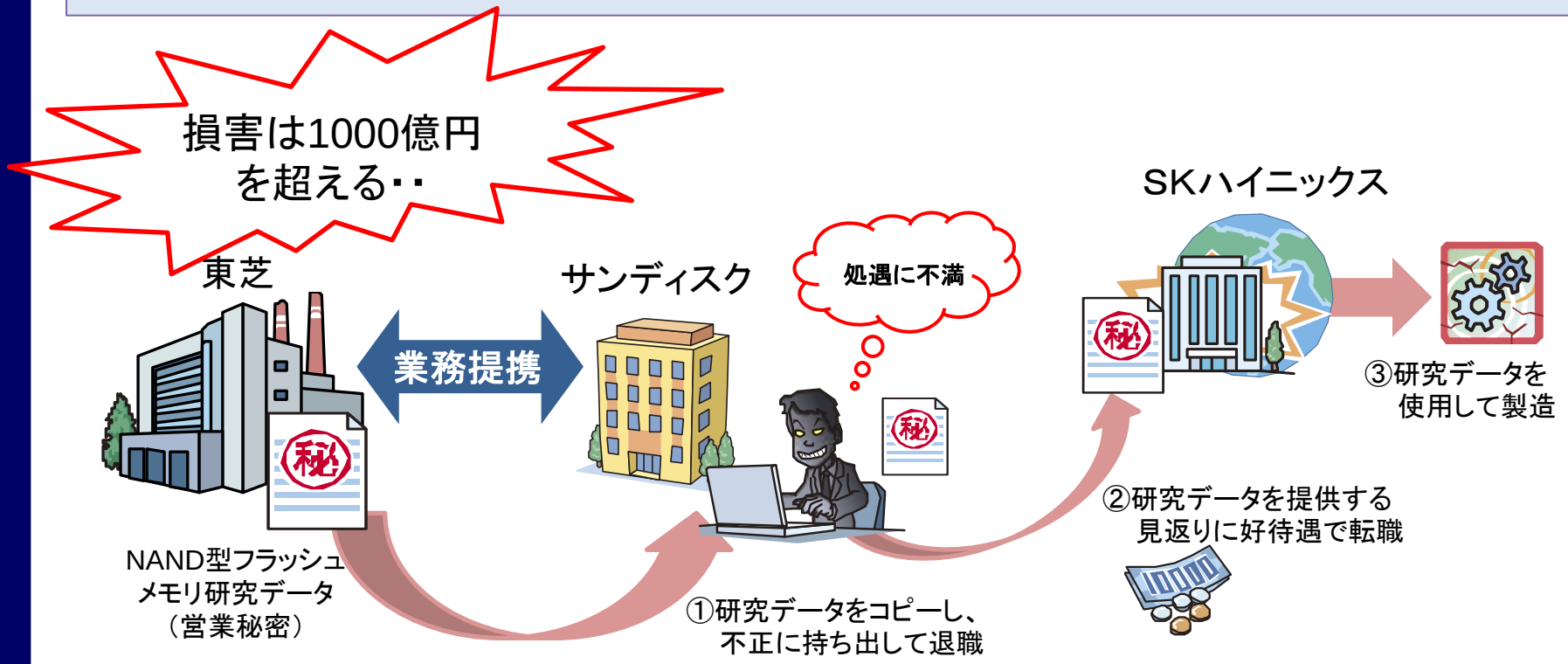
事例2

事例1

（報道により公表された事例をIPAがまとめたもの）

事例1　海外競合企業への技術情報の流出

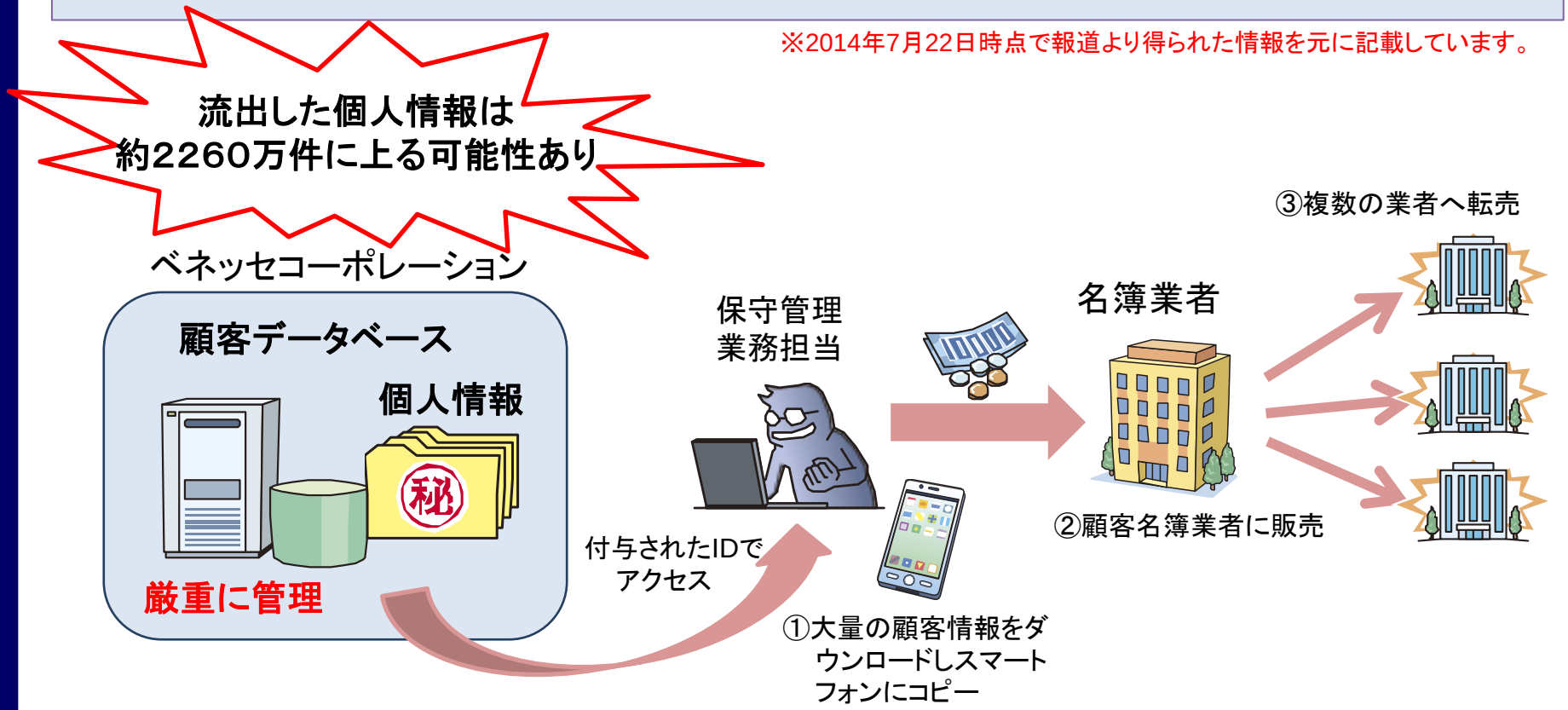
2014年3月、東芝のフラッシュメモリーの研究データを不正に持ち出し、転職先である韓国の半導体大手ＳＫハイニックスに提供したとして、東芝と業務提携していた半導体メーカー サンディスクの元技術者が、不正競争防止法違反（営業秘密開示）容疑で逮捕された。



事例2　委託SEによる個人情報漏えい

2014年7月、株式会社ベネッセコーポレーションの顧客データベースを保守管理するグループ会社（株式会社シンフォーム）の委託先の元社員が、顧客の個人情報を名簿業者へ売り渡す目的で、記憶媒体にコピーし流出させたとして不正競争防止法違反の疑いで逮捕された。

※2014年7月22日時点で報道より得られた情報を元に記載しています。



2. 内部不正対策を海外に学ぶ：米国における先進的な取り組み

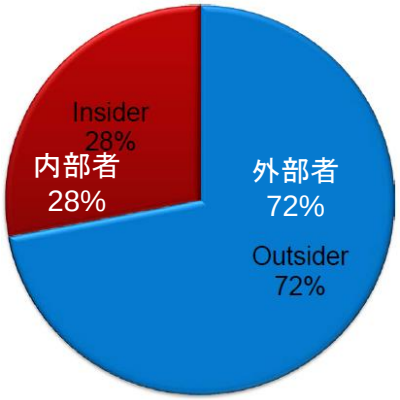
- 2014 US State of Cybercrime Survey
  - PWC, CERT®, CSO Magazine, US Secret Service
  - 回答者：557エグゼクティブ（従業員5000人以上28%,500～5000人:29%,500人以下:43%）

- CERT®/内部脅威センターによる事例収集と分析
  - 2000年、国防省（DOD：Department of Defense)がスポンサーとなり「内部者の脅威プログラム」が開始
  - カーネギーメロン大学ソフトウエア工学研究所（SEI）に設置
  - 政府機関等がスポンサーとなり、2014年2月現在、850の事例を収集・分析し内部不正対策を推進

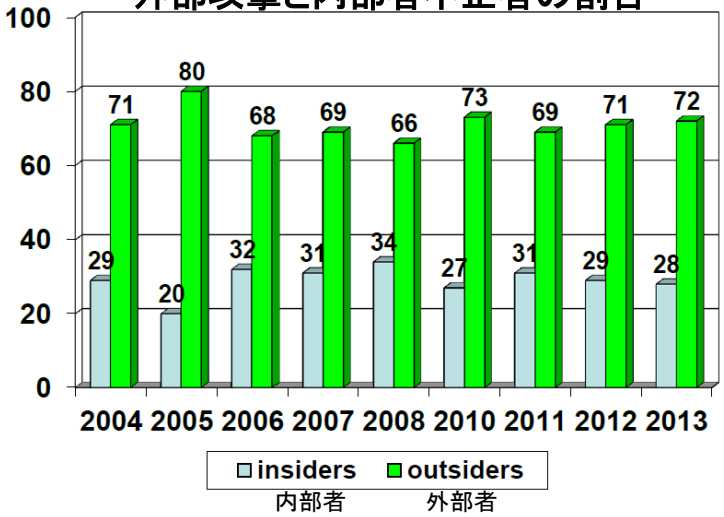
米国：企業の37%が内部者による事故を経験し、サイバー犯罪の犯行者は外部が7割弱、被害額はほぼ同じ

- 37%：Insider Incident（内部者による事故）を経験
- よくある内部不正
  - 82%　個人または機微情報の意図しない漏えい
  - 76%　機密情報が不正アクセス/不正使用された　または盗まれた
  - 71%　顧客情報が不正アクセス/不正使用された　または盗まれた
  - 63%　従業員情報が不正アクセス/不正使用された または盗まれた

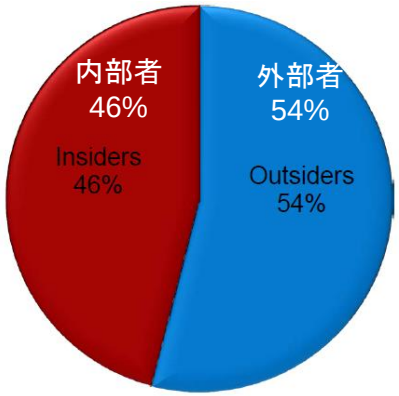
サイバー犯罪（eCrime）の犯行者の内訳



外部攻撃と内部者不正者の割合

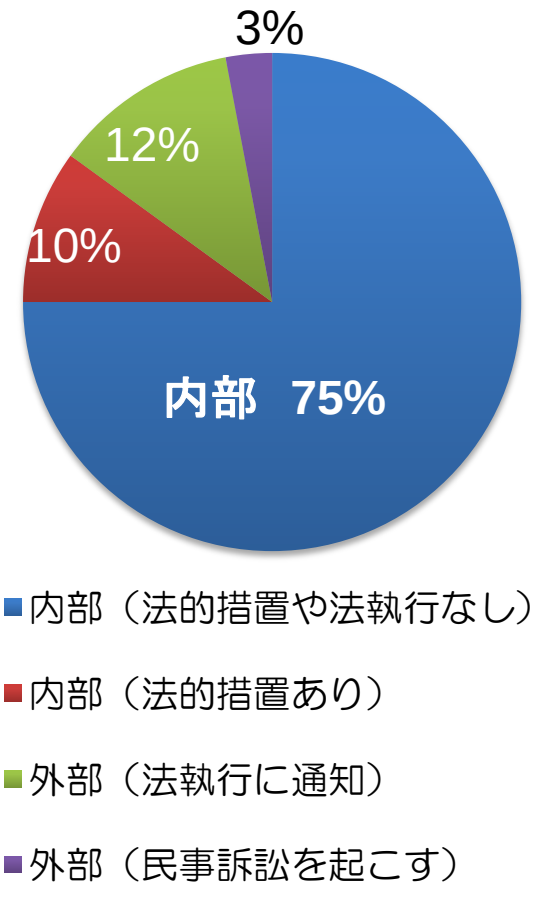


どちらの事件がより被害が大きかいと思うか：内部脅威と外部脅威はほぼ同じ



出典：2014 US State of Cybercrime Survey、2014.4（PWC, CERT, CSO Magazine, US Secret Serviceによる）

米国：75%が法的措置を取らず内部で処理 その理由は被害の状況を十分把握できなかったから



サイバー犯罪に対し法的措置を取らなかった理由	2013 %	2012 %	2011 %
被害の程度が起訴を保証するのに十分でない	34	36	40
起訴するのに、証拠がない／情報が不足している	36	36	34
犯罪を犯した個人を特定できなかった	37	32	37
ネガティブな公開（評判）を懸念	12	9	14
（自社の？）信頼を懸念	8	7	9
競合他社がこの事故で優位になることを懸念	7	6	7
法執行機関より事前にネガティブな回答を受けた	8	5	6
この事故を報告できるかわからない	6	5	4
法執行機関より、自己が国家安全保障に関連するとされた	3	4	4
その他	8	12	11
わからない	21	28	20

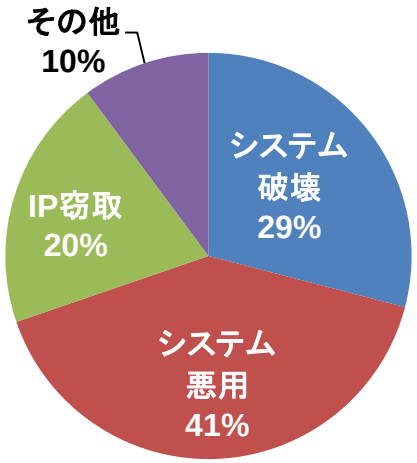
出典：2014 US State of Cybercrime Survey、2014.4（PWC、CERT, CSO Magazine, US Secret Serviceによる）

米国：内部不正のうち、システム悪用が41%, 破壊が29%, 知的財産窃取（20%）

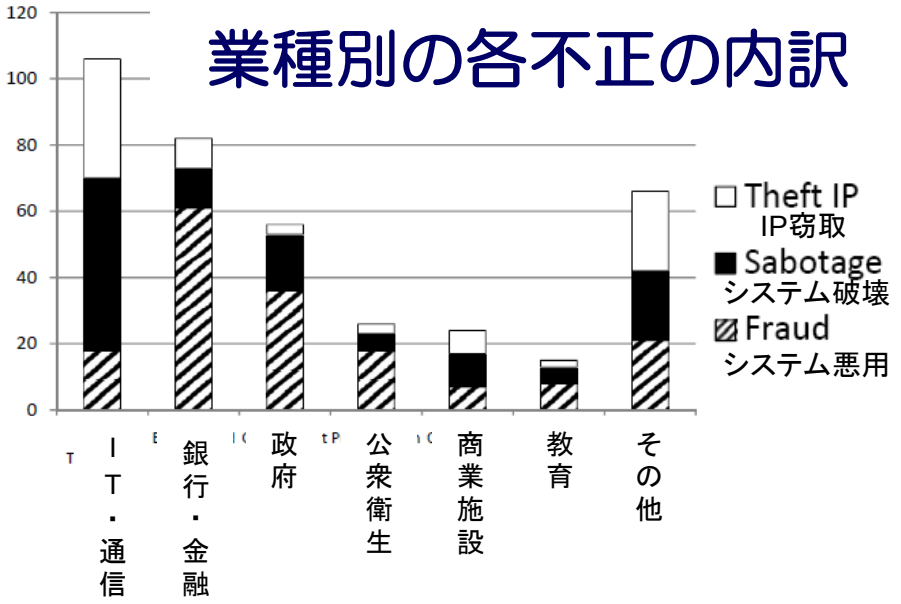
- システム悪用: (Fraud)
  - システムを悪用し、組織のデータを改ざん・削除、アカウントなどを窃取
- システム破壊: (Sabotage)
  - プログラムやシステムを不正プログラムなどによって攻撃し、破壊すること
- 知財（IP）窃取
  - 知財の窃盗

IPとは、特許、著作権、商標、意匠、科学的公式、ソースコードの一部であり、顧客に関する機密情報を含む独自の創造的な発想などをさす。

内部不正の種類



業種別の各不正の内訳



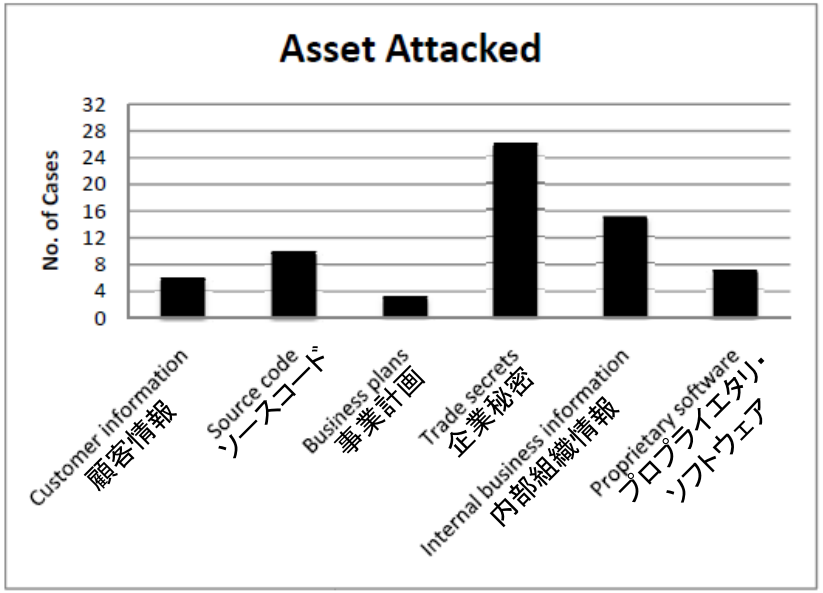
収集した550のケースのうち、国家スパイを除く413の内訳（2011 年現在）

出典： An Analysis of Technical Observations in Insider Theft of Intellectual Property Cases, 2011

米国：知財窃取の攻撃対象と情報流出手口

出典An Analysis of Technical Observations in Insider Theft of Intellectual Property Cases, 2011

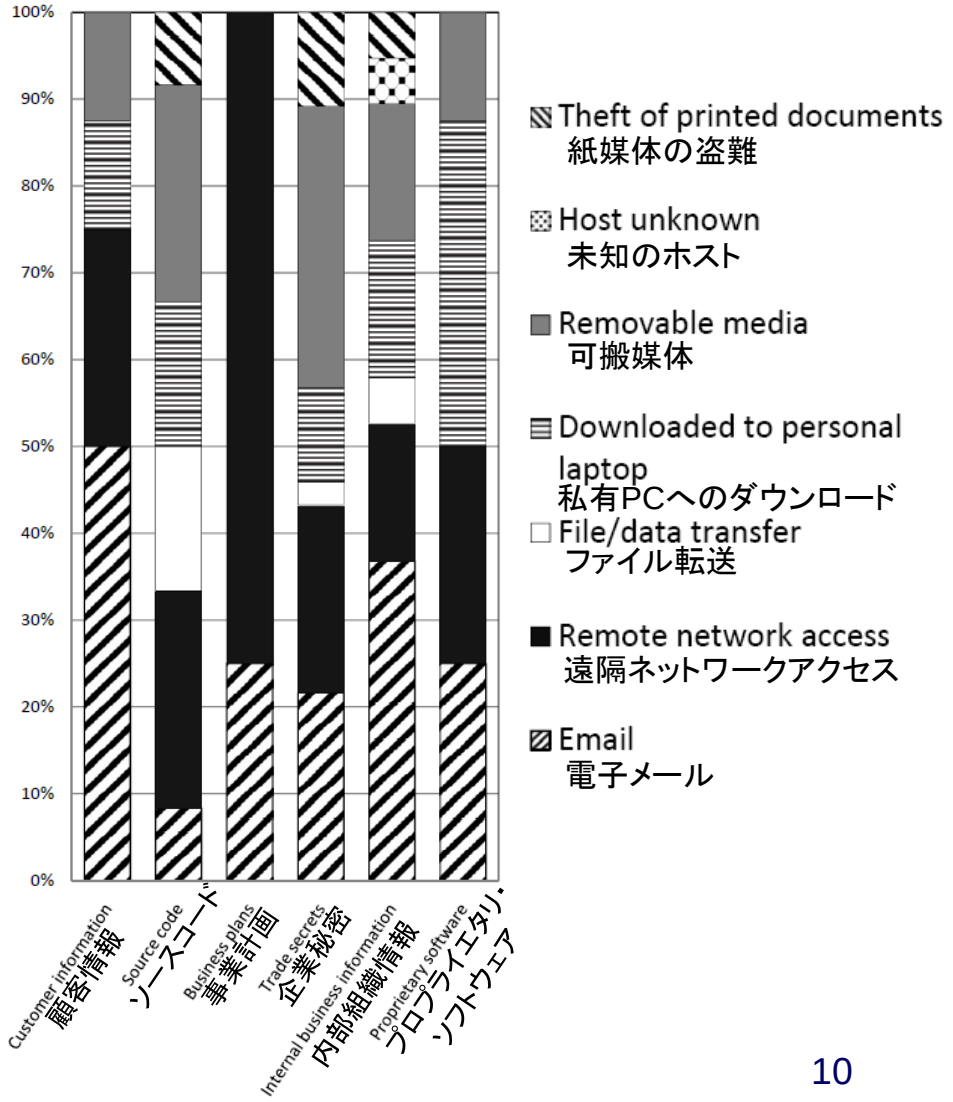
攻撃対象資産



内部者に攻撃された資産の種類

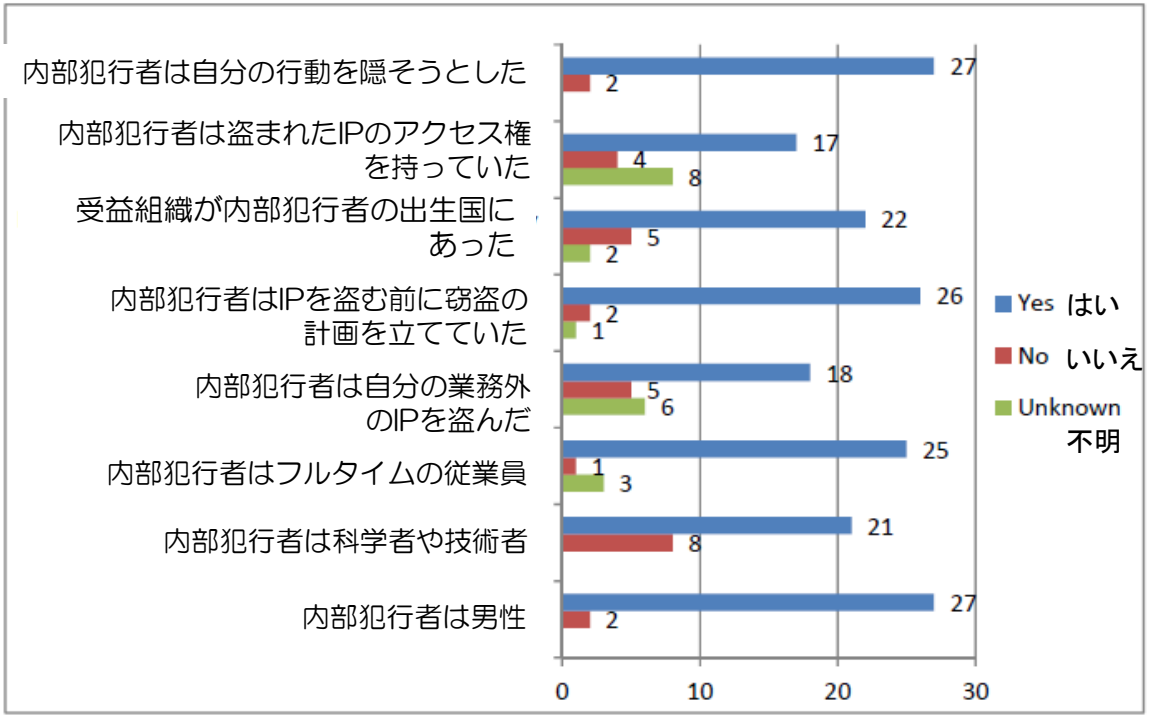
＊顧客情報には、アカウント（ID）を含まない

攻撃対象ごとの情報流出手口

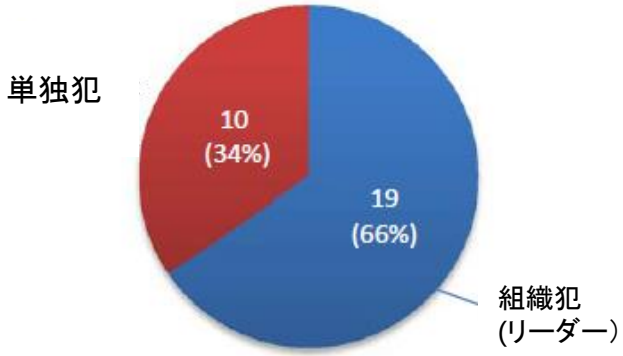


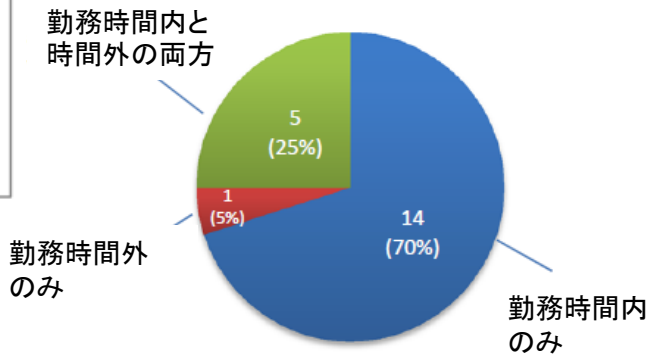
米国：外国政府および企業に関連した米国内知的財産（IP）の内部者による窃取

- **外国政府や企業が関連した29のIP窃取の状況**



外国政府または企業に関連したIP窃取



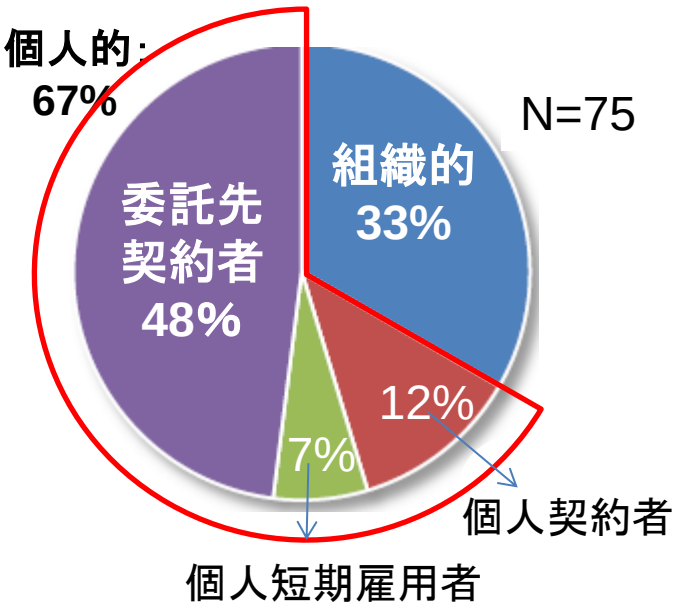


出典：Spotlight On: Insider Theft of Intellectual Property Inside the United States Involving Foreign Governments or Organizations, May 2013, CERT®

参考：外国政府・企業に関連したインサイダーを防ぐための7つの推奨　（CERT®による）

- 推奨 1: 雇用者の退職に際するプロセスを確立する
- 推奨 2: IP ネットワークを経由するIPを監視する.
- 推奨 3: 適切な物理セキュリティを維持
- 推奨 4: 最少権限のアクセスを考慮する
- 推奨 5: 競合他社との通信を監視
- 推奨 6: 海外渡航に関する 研究所のポリシーとベストプラクティス
- 推奨 7: 監査者が異常者（ anomalies）を検知する努力

米国：外部委託先などビジネスパートナーによる内部脅威の状況



組織的		サービスごとアウトソースしている。ヘルプデスク業務など
個人的	個人契約	個人で当該組織と契約しサービスを提供。コンサルタントなど
	個人短期雇用	短期雇用者
	委託先契約者	委託先と契約しており、（被害）企業にはフルタイムの勤務者

注：一部の内部者には複数の動機があるため、カテゴリは内部者の種類ごとに合計が100%を超えています。

75事例における割合（%）	委託先などのビジネスパートナ		通常の内部者
	組織的	個人的	
職種			
技術職	45	80	39
非技術職	55	20	61
許可されたアクセス（範囲）			
権限あり	44	36	48
権限なし	26	36	23
場所			
組織内	81	60	73
遠隔（リモート）	19	40	27
雇用者　状況			
現職	90	69	76
前職	10	31	24
不正の種類			
システム悪用	64	23	54
IP窃取	28	18	19
システム破壊	8	59	27
動機（かっこ）内は順位			
経済的利益	59(1)	28(2)	53(1)
報復	0(5)	46(1)	21(3)
ビジネス優位	15(3)	22(3)	35(2)
イデオロギー、興味	19(2)	18(4)	8(5)
その他	15(3)	14(5)	10(4)

出典：Spotlight On: Insider Threat from Trusted Business Partners　Version 2: Updated and Revised, October 2012、CER®T

3. 国内の状況：過去の調査報告、事例調査、判例調査-内部不正にフォーカスした調査は少ない

- 「情報セキュリティにおける人的脅威に関する調査研究報告書」（2010年3月、公益財団法人　日工組社会安全財団）
  - 警察機関における調書を対象としたアンケートにより内部犯行者を統計的に４つのモデルに分類した。
  - 企業風土・文化、個人の資質などと動機とを分析
- 「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 IPA）
  - インタビューによる事例調査、判例調査
  - 従業員、経営者へのアンケート調査
- 経済産業省:「人材を通じた技術流出に関する調査研究報告書（2013年3月）」
- NPO日本ネットワークセキュリティ協会（JNSA）
  - 組織で働く人間が引き起こす不正・事故対応WG　2013年発足　IPAのガイドラインに沿ったソリューションガイドを公表。2014年度は、ベストプラクティスを収集し公開予定。

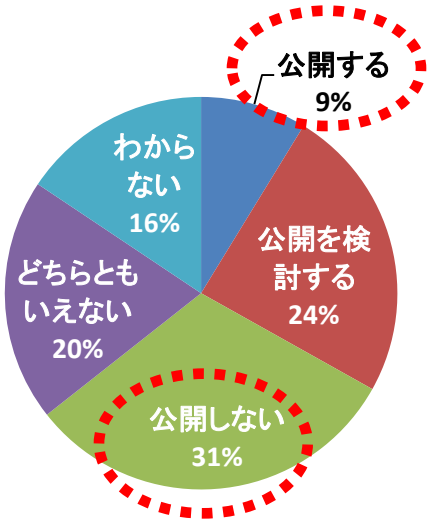
国内の状況：内部不正に関する事件は公表されないことが多い

- 組織の**事業の根幹を脅かす**事件が報道されている。
  しかし、公開されている事件は**氷山の一角**
  - 裁判に至らないものや内部規定違反等の事件も多く存在する
- 組織内部で処理され、外部に公開されることは稀（**情報を公開したくない**）
  - 会社の信用に関わる、風評被害が発生する恐れがある
  - 関係者との調整がつかない
- 他の組織との情報共有が困難
  - 自らの経験をもとに独自の対策を実施している

Q 有益な対策を検討する事例として情報を公開する可能性はありますか？

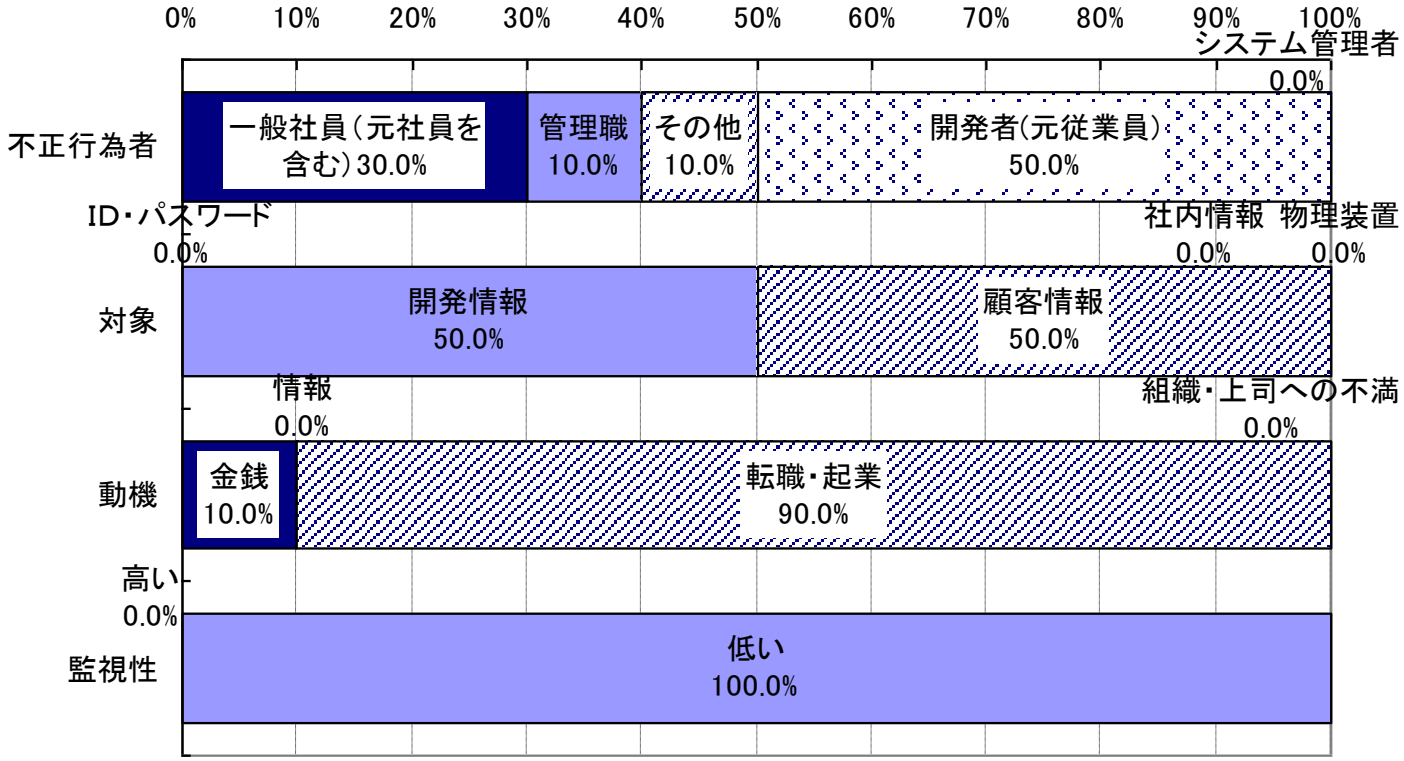
届出を行う公的または**中立的な機関**が「個人や企業名等が特定できない状態での公開」をすることで**関係者から合意が得られた**場合

（経営者、管理者を対象としたIPAのアンケート調査より）



内部不正の状況
(1)判例調査：判例DBの1376件から抽出

- 10件の判例のうち，9件が金銭目的，1件は心理的満足
- 動機は転職・起業が90%
- 監視性は低い環境

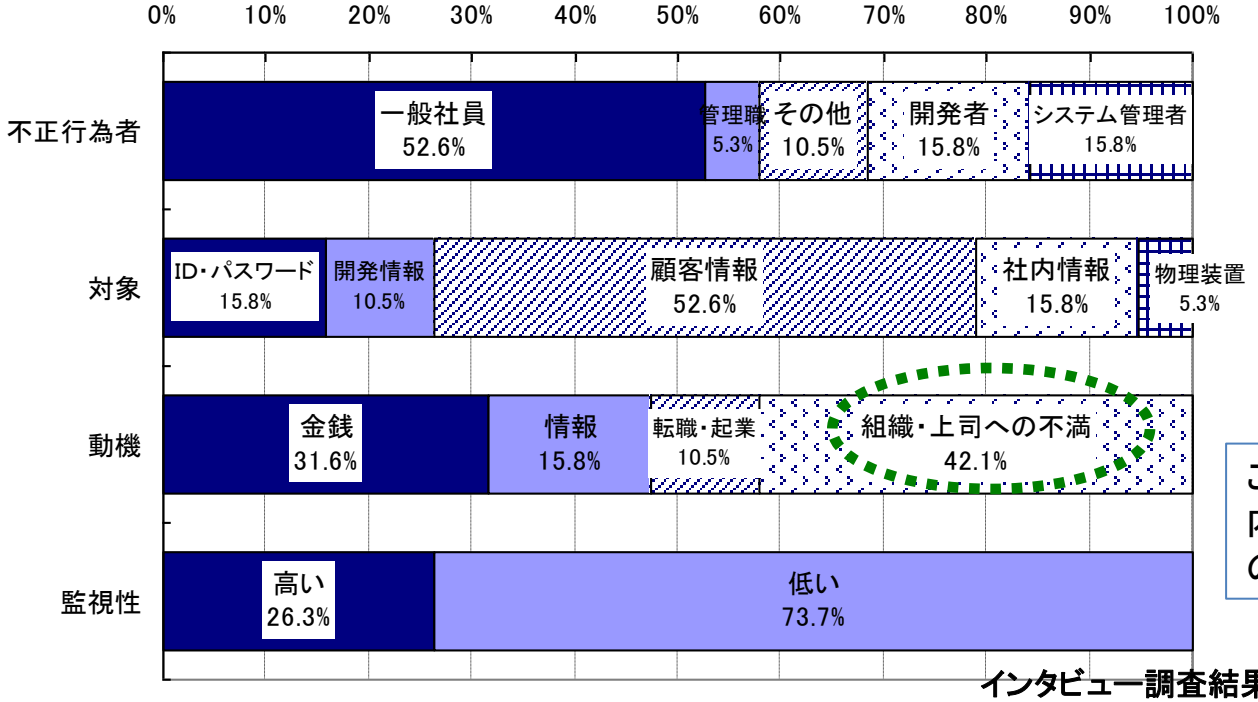


出典：IPA調査、2012.7

内部不正の状況：(2)企業のIT部門・フォレンジック専門家・法律家へのインタビュー調査

- 裁判に至らない事例も含むインタビュー調査による実態
  - 情報持ち出しでは**金銭目的以外の項目も発生**している
  - 動機として、**組織・上司への不満**の割合が高い

	システム悪用	情報持ち出し（金銭目的）	情報持ち出し（心理的満足）	破壊行為	不明
判例調査	0件	10件	1件	0件	0件
インタビュー調査	1件	9件	6件	1件	2件



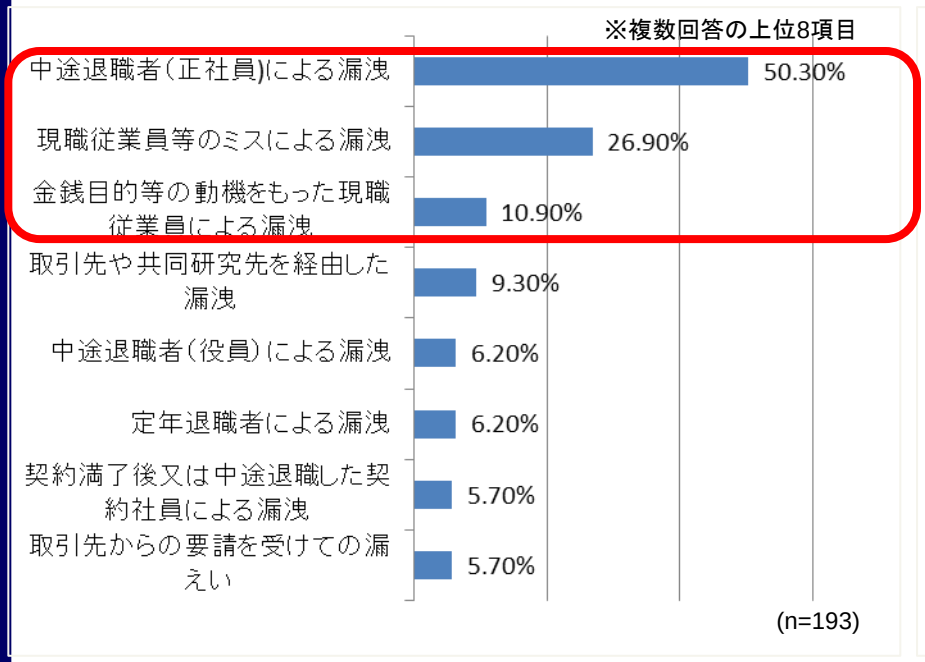
これらの事例は、
内部不正防止ガイドラインの付録Ⅰに抽象化し記載

インタビュー調査結果の詳細分類（n=19）

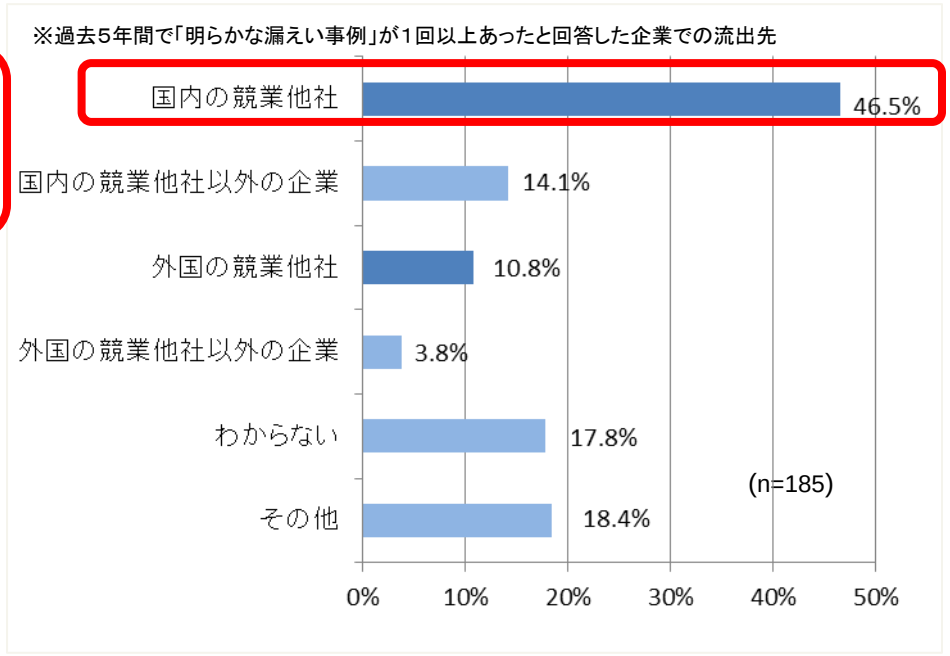
内部不正に関する企業の実態
(1) 情報漏えいの実態

- ビジネス上有用なノウハウや技術等の営業秘密の流出は、<u>従業員によるものが多く</u>を占める。
- 流出ルートでは、<u>退職者による漏えいが最も多い</u>。
- 国内外の競業他社へ漏えいしている恐れがある。

営業秘密の漏えい者



営業秘密の漏えい先



（出典）経済産業省:「人材を通じた技術流出に関する調査研究報告書（2013年3月）」を基にIPAが作成

内部不正に関する企業の実態
(2) 現状の対策と従業員の意識

- 対策状況は、IDパスワード等のアカウント管理、アクセス制御関連が中心（経営者が回答）
- 従業員にとって、最も抑止力が高い対策は「社内システムの操作の証拠が残る（54%）」。しかし、この項目は経営者、システム管理者では19位。
- 内部不正の対策に、社員と管理者の意識のギャップが見られた。

→ 経営者が講じる対策が必ずしも効果的に機能していない可能性がある

対策の実施状況

順位	対策	割合
1	社内システムにログインするための**IDやパスワードの管理**が徹底されている	31.9%
2	開発物（ソースコード）や顧客情報などの重要情報は**特定の職員のみアクセス**できるようになっている	29.4%
3	**退職者のアカウント**は、即日、削除される	27.5%
4	職務上で作成・開発した成果物は、企業に帰属することを研修で周知徹底する	26.9%
5	情報システムの管理者以外に、**情報システムへのアクセス管理**を操作できない	24.4%

内部不正への気持ちが低下する対策

社員		内容	経営者・管理者の結果	
順位	割合		順位	割合
1位	54.2%	社内システムの操作の証拠が残る	19 位	0.0%
2位	37.5%	顧客情報などの重要な情報にアクセスした人が監視される（アクセスログの監視等含む）	5 位	7.3%
3位	36.2%	これまでに同僚が行ったルール違反が発覚し、処罰されたことがある	10位	2.7%
4位	31.6%	社内システムにログインするためのIDやパスワードの管理を徹底する	3位	11.8%
5位	31.4%	顧客情報などの重要な情報を持ち出した場合の罰則規定を強化する	10 位	2.7%

（出典）IPA：組織内部者の不正行為によるインシデント調査　調査報告書（2012年7月）

内部不正に関する企業の実態
(3) 内部不正が発生する要因

- 不正行為を働く動機を高める要因は、処遇面の不満に関する項目が上位３つを占めた（社員向けアンケート）

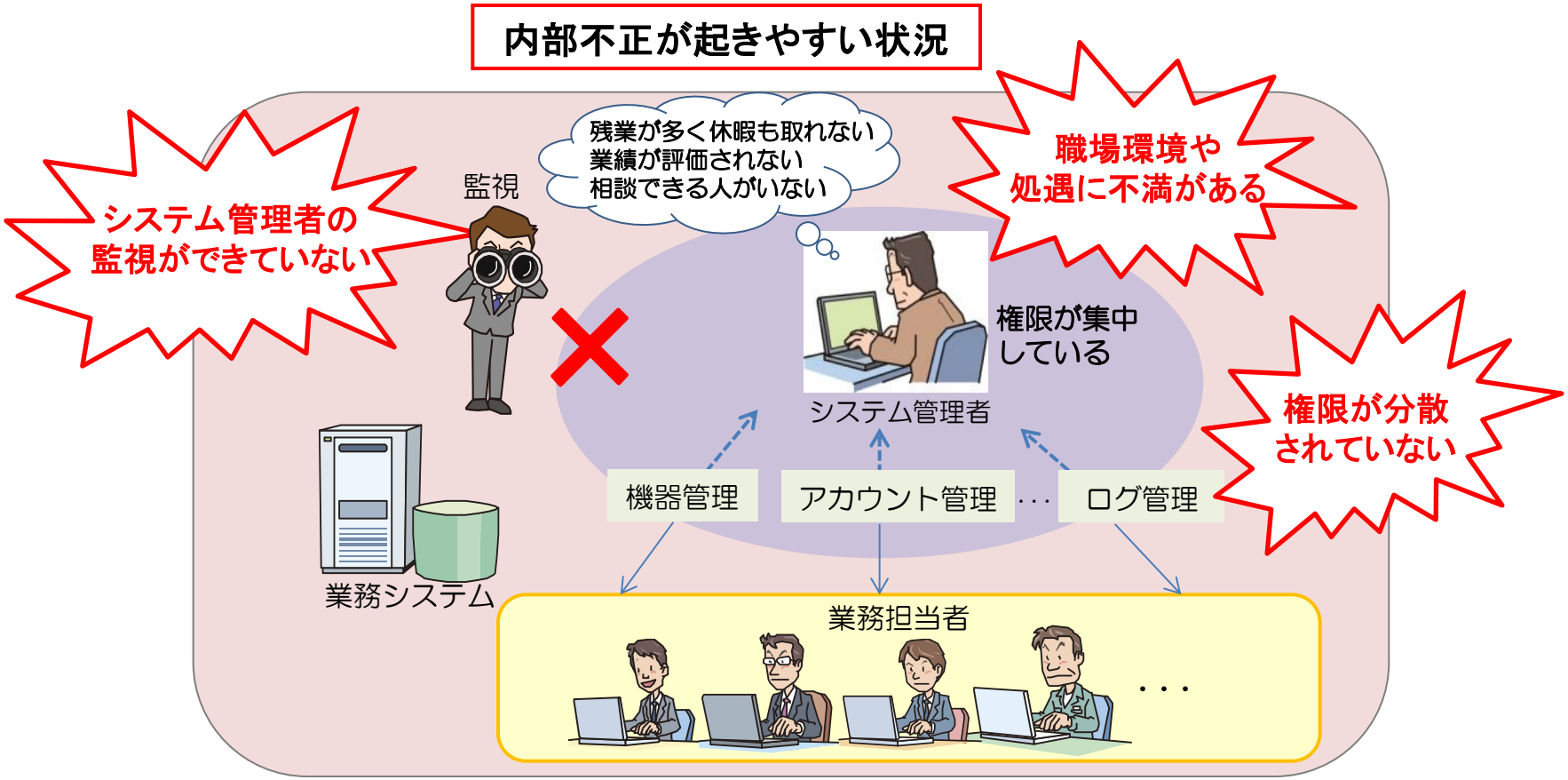
不正行為への気持ちを高める要因

順位	内容	割合
1	不当だと思う解雇通告を受けた	34.2%
2	給与や賞与に不満がある	23.2%
3	社内の人事評価に不満がある	22.7%
4	職場で頻繁にルール違反が繰り返されている	20.8%
5	システム管理がずさんで顧客情報を簡単に持ち出せることを知っている	20.1%
6	社内ルールや規則に違反した際、罰則がない	18.7%
7	上司の仕事の取り組み方や上司の人間性に不満がある	18.3%
8	職場で人間関係のトラブルがある	17.8%
9	社内のだれにも知られずに、顧客情報などの重要な情報を持ち出せる方法を知っている	16.4%
10	かつて同僚がルール違反を行ったことが発覚したが、社内で処罰されなかった	16.1%

（出典）IPA：組織内部者の不正行為によるインシデント調査　調査報告書（2012年7月）

4．内部の不正行為への対策の難しさ

- 不正者が、正規のアクセス権限を持つ内部者であるため、技術的な対策だけでは防ぐことが困難



Ⅱ部　組織における内部不正防止ガイドラインの紹介

１．「組織における内部不正防止ガイドライン」の概要

２．　内部不正対策例

（緊急呼びかけ）内部不正による情報漏えい

ケース１　退職にともなう情報漏えい
ケース２　システム管理者による不正行為
ケース３　委託先からの情報漏えい等
ケース４　職場環境に起因する不正行為
ケース５　従業員による悪意のない不正行為
ケース６　早期発見
ケース７　内部不正発生時の対応

1.内部不正防止ガイドライン 策定の背景

内部不正の現状

- 近年、従業員や委託先社員による内部不正事件が発生。
  ひとたび発生すると事業に大きな影響をもたらす。
- 信頼や評判が損なわれるといった負の影響を懸念し、公表されることは稀。

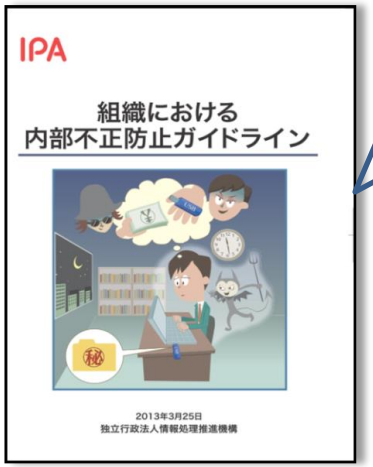
内部不正対策に関する状況

- 自らの経験をもとに独自の対策を実施
- 組織を超えた検討が困難
- コストによる制約等から効率的、効果的な対策が必要（特に中小企業）

組織における内部不正防止ガイドライン

内部不正防止ガイドライン：目的

- 組織において内部不正を防止するための環境整備に役立てる
- これまで 内部不正対策を 「考えてこなかった」 「何をすればよいかわからない」という企業も考慮した内容　（特に中小企業に重きをおいている）
- 防止対策だけでなく、早期発見・拡大防止にも対応



【目次】
1章 背景
2章 概要
3章 用語の定義と関連する法律
4章 内部不正防止のための管理の在り方
付録Ⅰ 内部不正事例集
付録Ⅱ チェックシート
付録Ⅲ Q&A集
付録Ⅳ 他のガイドライン等との関係
付録Ⅴ 基本方針の記述例

・内部不正の知見を有する様々な分野の有識者6名から成る「組織における内部不正防止ガイドライン検討委員会」を設置（2012年7月）

・内部不正行為についての調査「組織内部者の不正行為によるインシデント調査」を基に検討

「組織における内部不正防止ガイドライン」 ※日本語版、英語版

内部不正防止ガイドラインの位置づけ

- 営業秘密管理指針（経済産業省 知的財産政策室）
  - 知的財産やノウハウ等の営業秘密の保護を目的とした指針
  「不正競争防止法」で定められている営業秘密の３要件
  - ➢ 秘密管理性
  - ➢ 有用性
  - ➢ 非公知性

- 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（経済産業省）
  - 組織が管理する個人情報を保護する場合は、「個人情報保護法」で求められる安全管理措置義務関連の規定への対応が必要
  - ➢ 安全管理措置（法第２０条関連）

内部不正防止ガイドラインの位置づけ

ガイドライン（付録Ⅳ） P68~P71

- 情報セキュリティマネジメントシステム（ISMS）
  JIS Q 27001　付属書Aの管理策

JIS Q 27001：2006 とガイドラインの対応一覧 （付録Ⅳ抜粋）

大項目		項目名	JIS Q 27001 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情報セキュリティ基本方針 A.6.1内部組織 A.6.2外部組織
		(2) 総括責任者の任命と組織横断的な体制構築	A.5.1情報セキュリティ基本方針 A.6.1内部組織 A.6.2外部組織
資産管理	秘密指定	(3)情報の格付け	A.7.1資産に対する責任 A.7.2情報の分類 A.11.1 アクセス制御に対する業務上の要求事項
⋮			
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.13.1情報セキュリティの事象及び弱点の報告 A.13.2情報セキュリティインシデントの管理及びその改善 A.14.1事業継続管理における情報セキュリティの側面

ISMSの管理策に対応する項目無し

内部不正にはトップダウンで、組織横断の取組みを！

- **経営者（経営陣）**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
  - 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や実施策の周知徹底を図る上で重要
- 効果的な実施策の策定、及びその実施策の周知徹底には、**組織横断での取り組みが不可欠**
  - 内部不正対策の検討では複数の部門が関係するため、これら関係部門が協力して実施策を策定することが必要
  - 実施策の周知徹底のために、組織内で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体制作りが必要

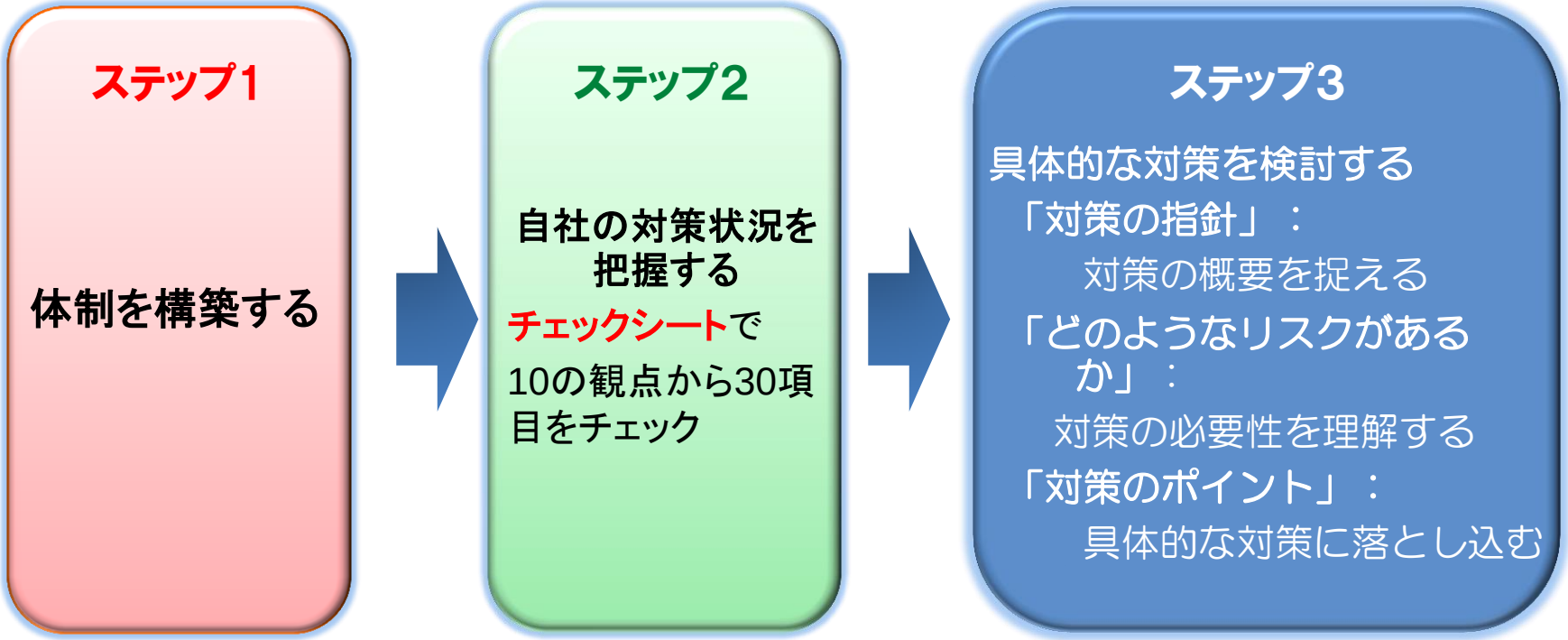
内部不正防止対策10分類と関連部門

	経営者	情報システム部	総務部	人事部	法務・知財部	営業・開発等の各部門
1.基本方針	○					
2.資産管理		○				○
3.物理的管理		○	○			○
4.技術的管理		○				○
5.証拠確保		○				○
6.人的管理			○	○	○	○
7.コンプライアンス			○	○	○	○
8.職場環境			○	○		○
9.事後対策		○				○
10.組織の管理		○				○

ガイドラインを活用した内部不正対策の進め方

ステップ１. 管理体制を構築する。**組織横断での実施体制**を確保。
ステップ２. 現状の対策状況をチェックする。
ステップ３. インシデントが発生した場合の事業に与える影響から、各対策の必要性を検討し、具体策を立案する。事業に与える影響は小さく、リスクを許容できると判断すれば必ずしも対策する必要はない。

IPA 「組織における内部不正防止ガイドライン」を利用した進め方

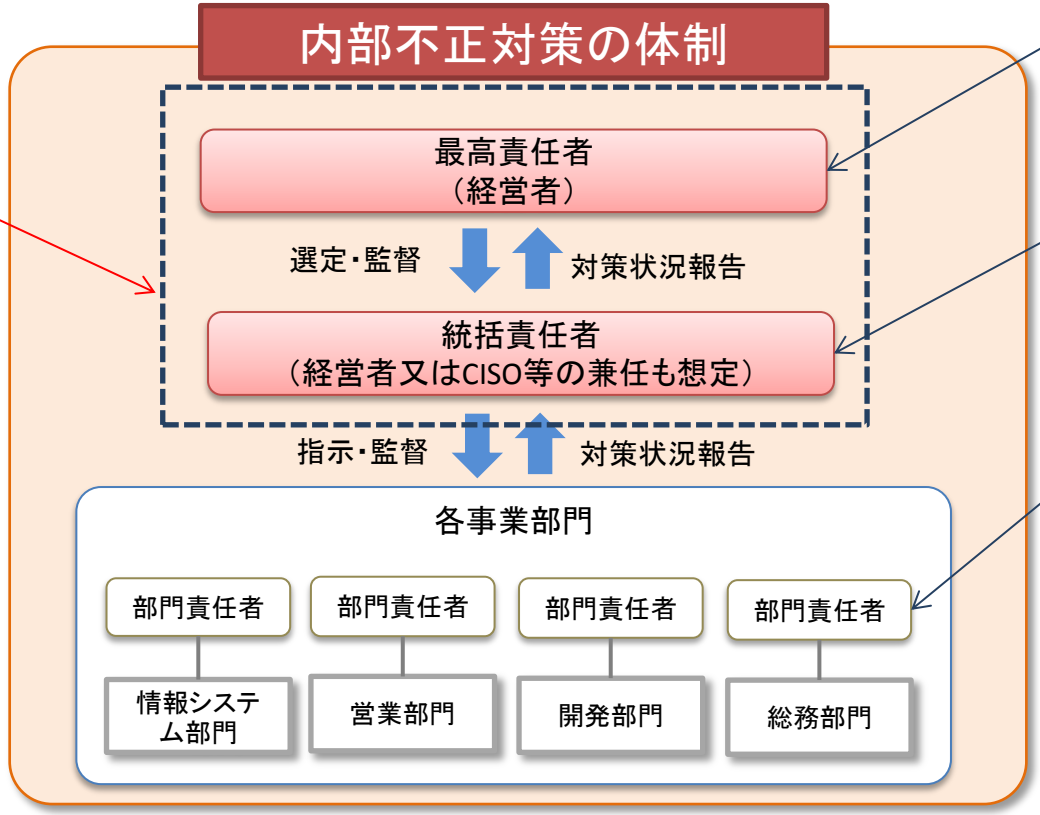


ステップ1　体制を構築する
～　内部不正防止対策の管理体制～

ガイドライン　P10~11

- 経営者による意思決定が会社全体に伝わり、実施状況が把握できる管理体制を構築する。
- 企業の規模により体制は柔軟に検討する

小規模の場合は、
経営者が兼務



意思決定を行う最高責任者
基本方針の策定、
統括責任者の任命

体制の統括的な責任者
具体的な対策の実施、推進

各部門で任命した責任者
所属部門での実施策の実行

ステップ2　現状の対策状況を把握する
～チェックシートで現状を把握～

ガイドライン　P60~63

※ □：主担当/実施部門、[ ]：サポート/実施補助・確認部門

No	内容	チェック欄
4-1．基本方針		
(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）
(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）
	⋮	
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)	内部者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？	□

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
		[ ]	[ ]	[ ]
		[ ]	[ ]	[ ]

30の対策項目に対応

各項目に関係する部門を示している

ステップ2
10の観点での30の対策項目

ガイドライン　P18~P56

番号	観点（分類）	対策項目	番号	観点（分類）	対策項目
1	基本方針	(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	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
2	資産管理	（3）情報の格付け （4）格付け区分の適用とラベル付け （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	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
3	物理的管理	（8）物理的な保護と入退管理策 （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及び監視 （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	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	技術的管理	（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 （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 （16）第三者が提供するサービス利用の確認（クラウドコンピューティングを含む）	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
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	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

（特徴）
アンケート調査から分析

ステップ3　具体的な対策を検討する
～対策のポイントを理解し実施策を立案～

①対策の指針、ポイントを理解
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する

組織における内部不正防止ガイドライン

②具体的な実施策を立案する
製品・ソリューション利用等を検討

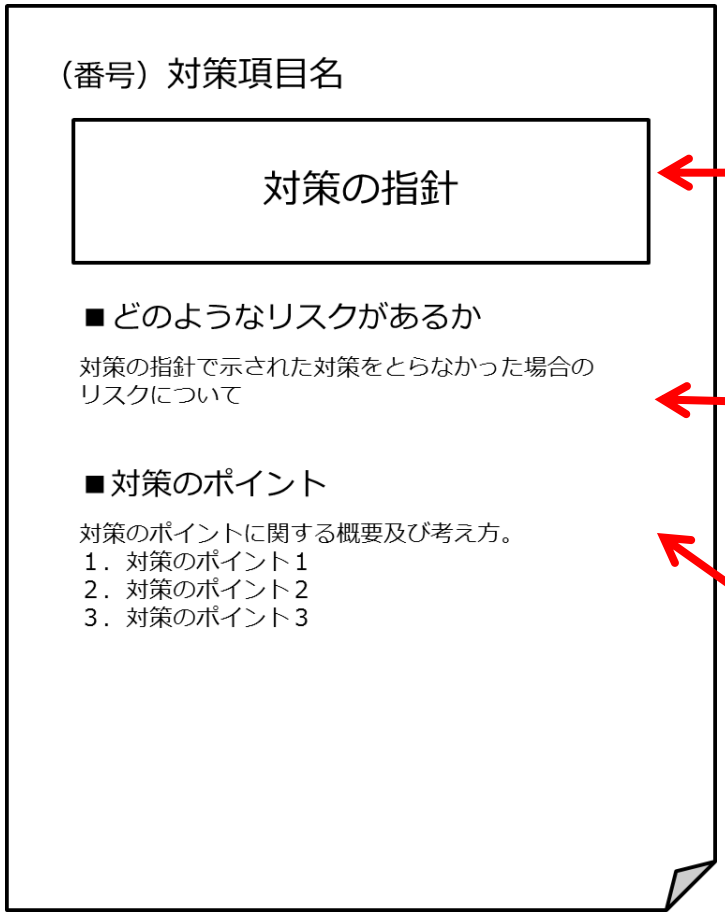
JNSA※内部不正対策ソリューションガイド

ガイドラインの各対策を実現するための製品やサービスをまとめたソリューションガイド。30の対策項目にマッピング。

製品・ソリューション
掲載企業数：16社
掲載製品数：156品
（2014年8月現在）

※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

ステップ3　具体的な対策を検討する
～対策のポイントを理解し実施策を立案～



①**「対策の指針」を読んで、対策の概要を捉える。**

②**「どのようなリスクがあるか」を読んで、対策しない場合のリスクを知る。**
インシデントが発生した場合の事業に与える影響を考える。
事業に与える影響が小さく、リスクを許容できると判断すれば、必ずしも対策する必要はない。

③ **②の事業に与える影響から、「対策のポイント」を読んでコストやリソース等を考慮し具体的な実施策を立案する。**
「付録Ⅲ：Q&A集」や「付録Ⅳ：他のガイドラインとの関係」**JNSAソリューションガイド**を参考。

※ 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。

ステップ3　対策例　（1）経営者の責任の明確化

ガイドライン　P18

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。　←①対策の指針

■どのようなリスクがあるか？　←②どのようなリスクがあるか

経営者のリーダーシップにより「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。また、「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。

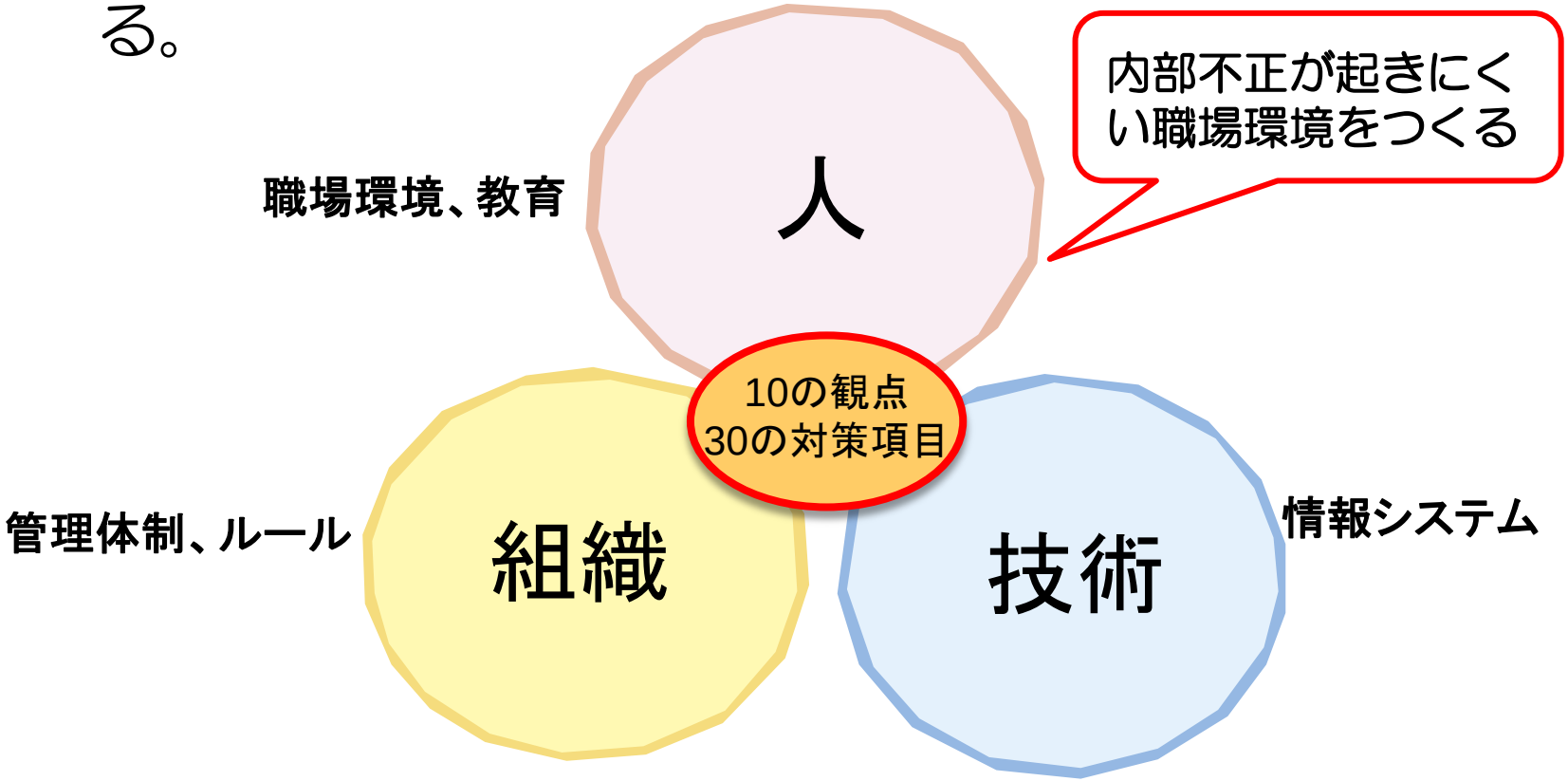
■対策のポイント　←③対策のポイント

経営者は、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。経営者は対策を実効性のあるものとするために実施状況をモニタリング 、評価することによって基本方針を定期的に見直していきます。

1. 経営者が内部不正対策の方向づけ、モニタリング、評価に関与して組織内外において責任を持ちます。
2. 本ガイドライン等を参考にし、基本方針を策定（Q&A1:P65）します。
3. 組織が保護すべき重要な情報（重要情報）を定めます。
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

内部不正へは「人」的対策を

- 正規のアクセス権限を持つ内部者による不正行為は技術的な対策だけでは防ぐことが困難
- 「人」・「組織」・「技術」の面から、対策を検討する。



2. 内部不正対策例

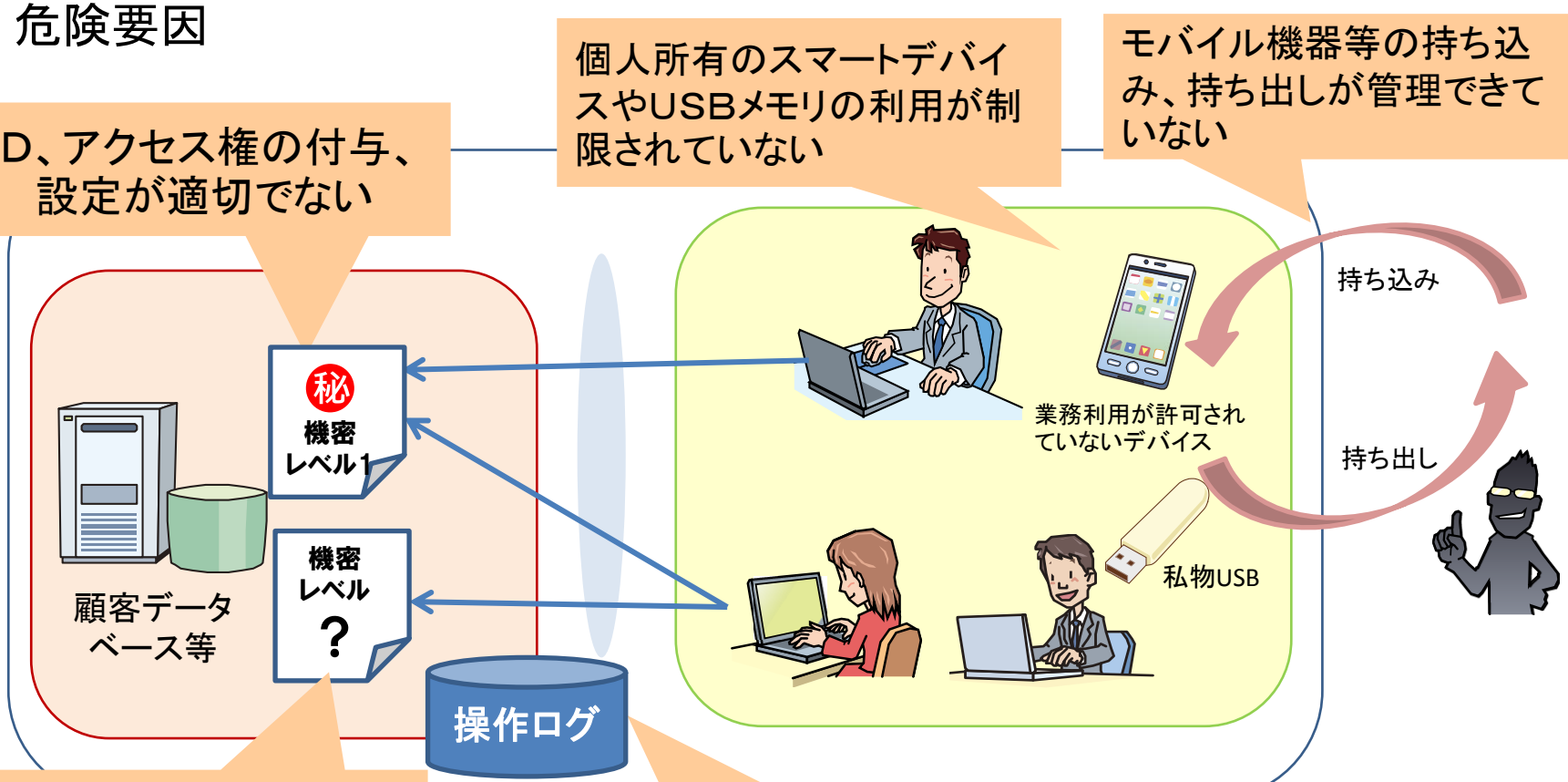
（緊急呼びかけ）内部不正による情報漏えい

ケース1　退職にともなう情報漏えい
ケース2　システム管理者による不正行為
ケース3　委託先からの情報漏えい等
ケース4　従業員による悪意のない不正行為
ケース5　職場環境に起因する不正行為
ケース6　早期発見
ケース7　内部不正発生時の対応

（緊急呼びかけ）内部不正による情報漏えい

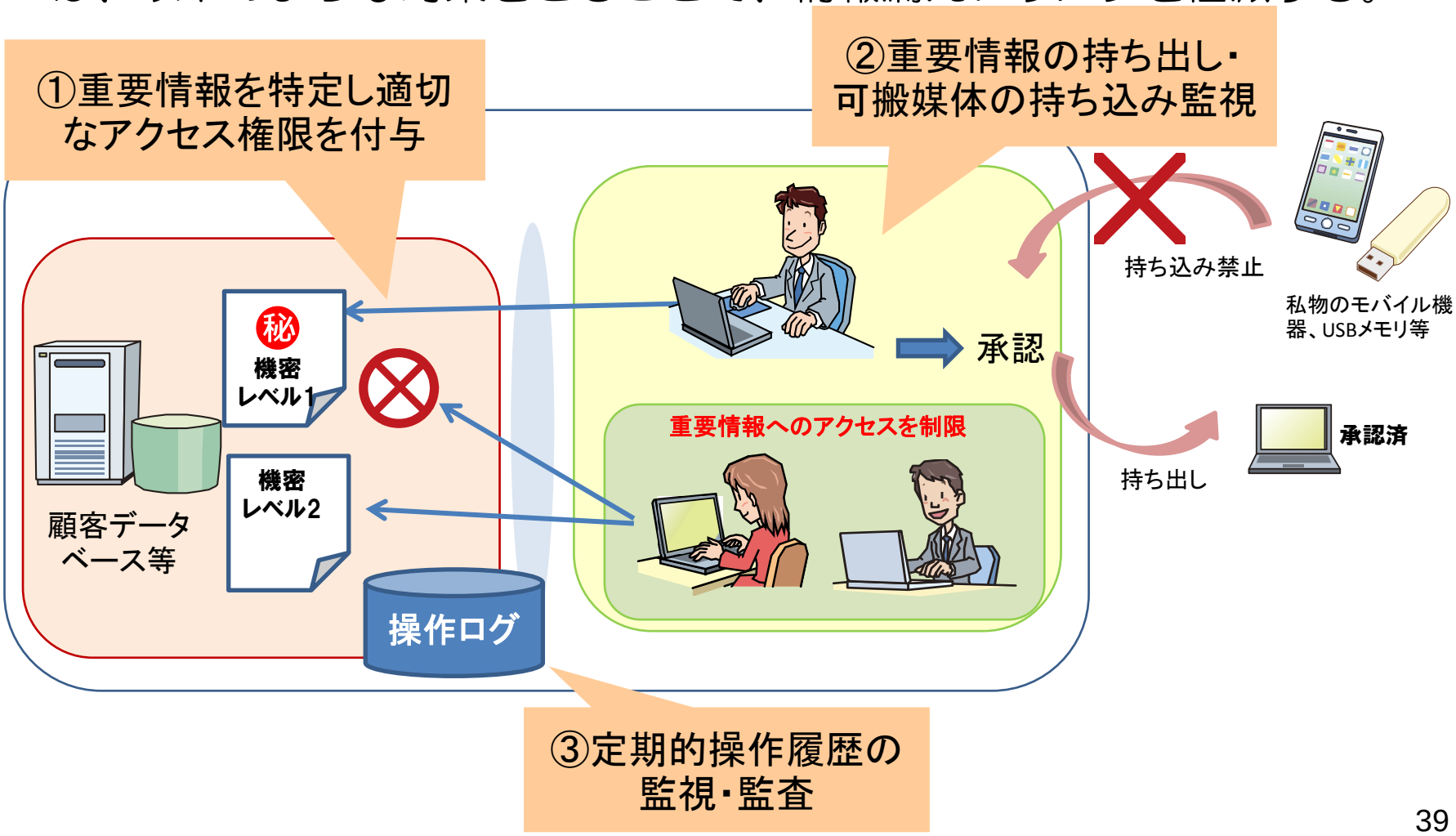
- 内部不正による情報漏えいを防止するため、セキュリティ対策の点検を！

◆ 危険要因



内部不正による情報漏えいのリスク低減策

- 特に重要な情報が保管されているファイルやデータベースについては、以下のような対策をとることで、情報漏えいリスクを低減する。



①重要情報を特定し適切なアクセス権限を付与

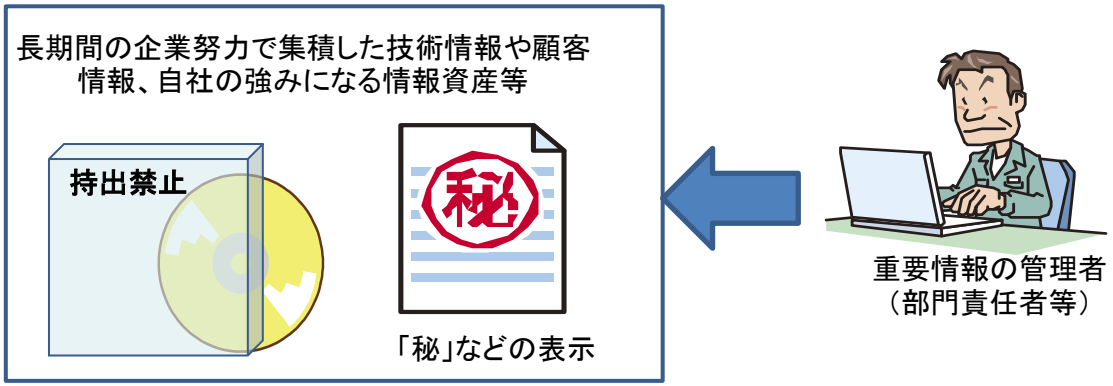
内部不正防止ガイドライン：（3）情報の格付け
（4）格付け区分の適用とラベル付け
（5）情報システムにおける利用者のアクセス管理

・重要情報を特定する。
- ✓ 少なくとも重要情報と一般情報の2つに分けて管理する。(情報の格付け区分)
- ✓ 重要度ごとに取扱いを定める。（取扱範囲、消去方法等）
- ✓ 従業員にわかるように電子文書の目立つ場所に「機密情報」等を表示する。（ラベル付け）

・適切なアクセス権限付与
- ✓ 重要情報へのアクセス権限を持つ操作員を最小とする。
- ✓ アクセス権限は定期的に見直す。
- ✓ 特に重要な情報は、時間及びアクセス数等のアクセス条件で制御する

※ 重要情報を特定し、安全に管理していないと不正競争防止法の保護対象にならない。
（詳細な要件は、経済産業省の「営業秘密管理指針」を参照。

重要度が高いほど、
アクセス権者を減らす



参考. 不正競争防止法で保護される営業秘密の３要件

技術やノウハウ等の情報が「営業秘密」として不競法で保護されるためには、以下の３要件を全て満たすことが必要です。

内部不正防止ガイドライン

➢ 秘密として管理されていること（秘密管理性）

①情報に触れることができる者を制限すること　（アクセス制限）

②情報に触れた者にそれが秘密であると認識できること　（客観的認識可能性）

➢ 有用な営業上又は技術上の情報であること（有用性）

当該情報自体が客観的に事業活動に利用されていたり、利用されることによって、経費の節約、経営効率の改善等に役立つものであること。現実に利用されていなくてもかまいません。

○
- 設計図、製法、製造ノウハウ
- 顧客名簿、仕入先リスト
- 販売マニュアル

×
- 有害物質の垂れ流し、脱税等の反社会的な活動についての情報は、法が保護すべき正当な事業活動ではないため、有用性があるとはいえない。

➢ 公然と知られていないこと（非公知性）

保有者の管理下以外では一般に入手できないこと。

○
- 第三者が偶然同じ情報を開発して保有していた場合でも、当該第三者も当該情報を秘密として管理していれば、非公知といえる。

×
- 刊行物等に記載された情報

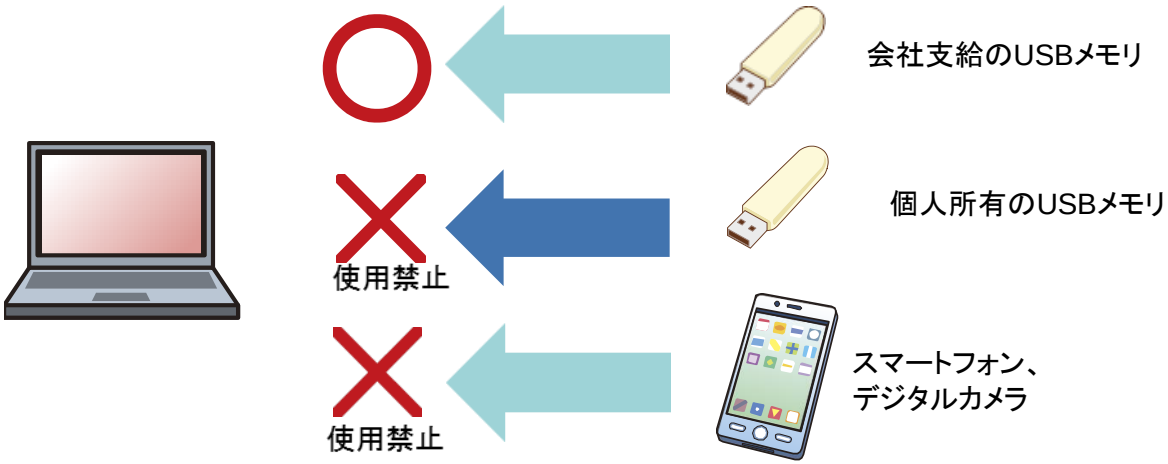
（出典）経済産業省「営業秘密管理指針 の概要」

②重要情報の持ち出し・可搬媒体の持ち込み監視

内部不正防止ガイドライン：（10）情報機器及び記録媒体の持ち出し管理及び監視
（11）個人の情報機器及び記録媒体の業務利用及び持ち込みの制限
（14）情報機器や記録媒体の持ち出しの保護

ノートPCやスマートデバイス等のモバイル機器および携帯可能なUSBメモリ等の記録媒体の管理を厳格にし、利用を制限する。

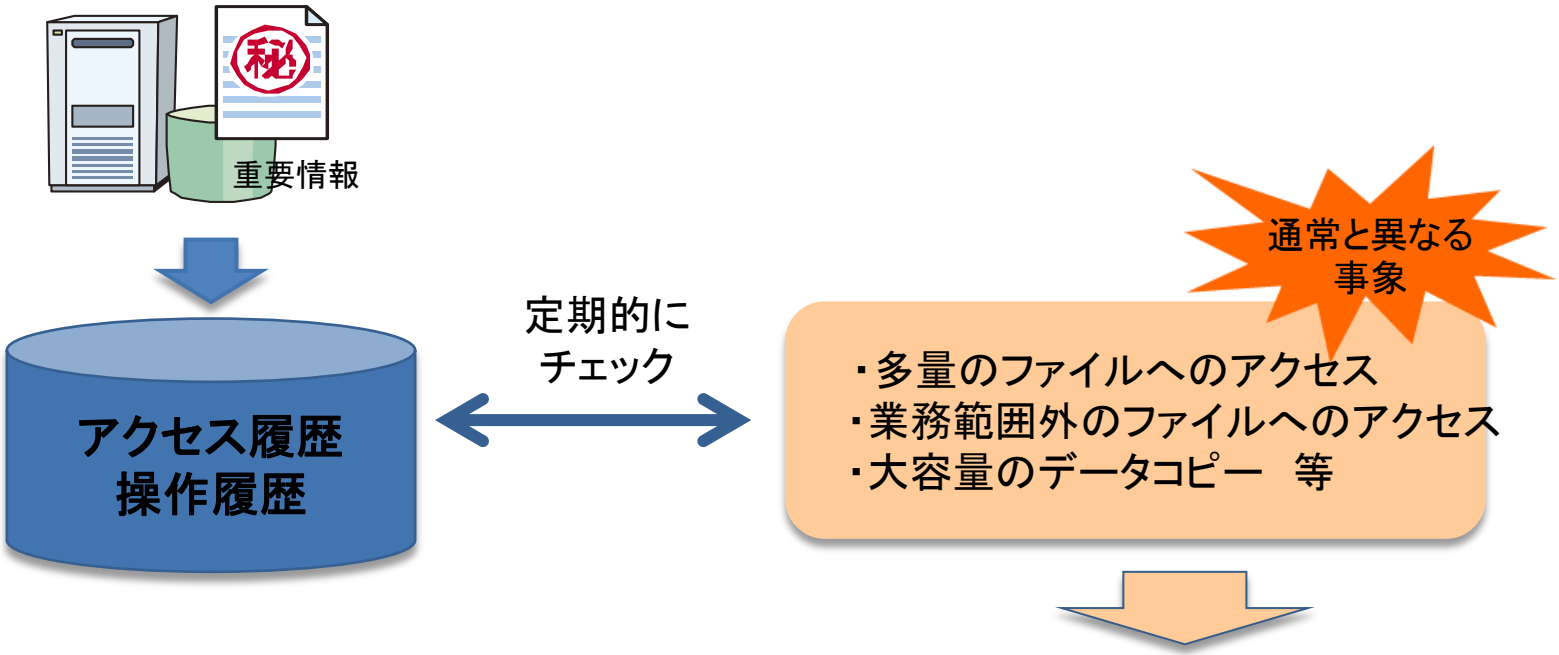
- ✓ 物理的に保護された場所からの持ち出しは、管理者の承認を必要とし、記録を取る。
- ✓ 個人所有のモバイル機器やUSBメモリの業務利用、持ち込みを制限する。
  特に、サーバルーム等への持ち込み、利用を厳しく制限する。
- ✓ 外部出力を制限可能な管理ツール等の技術的な対策を行う。（例　デバイス制御ソフト）



③定期的な操作履歴の監視・監査

内部不正防止ガイドライン：（17）情報システムにおけるログ・証跡の記録と保存

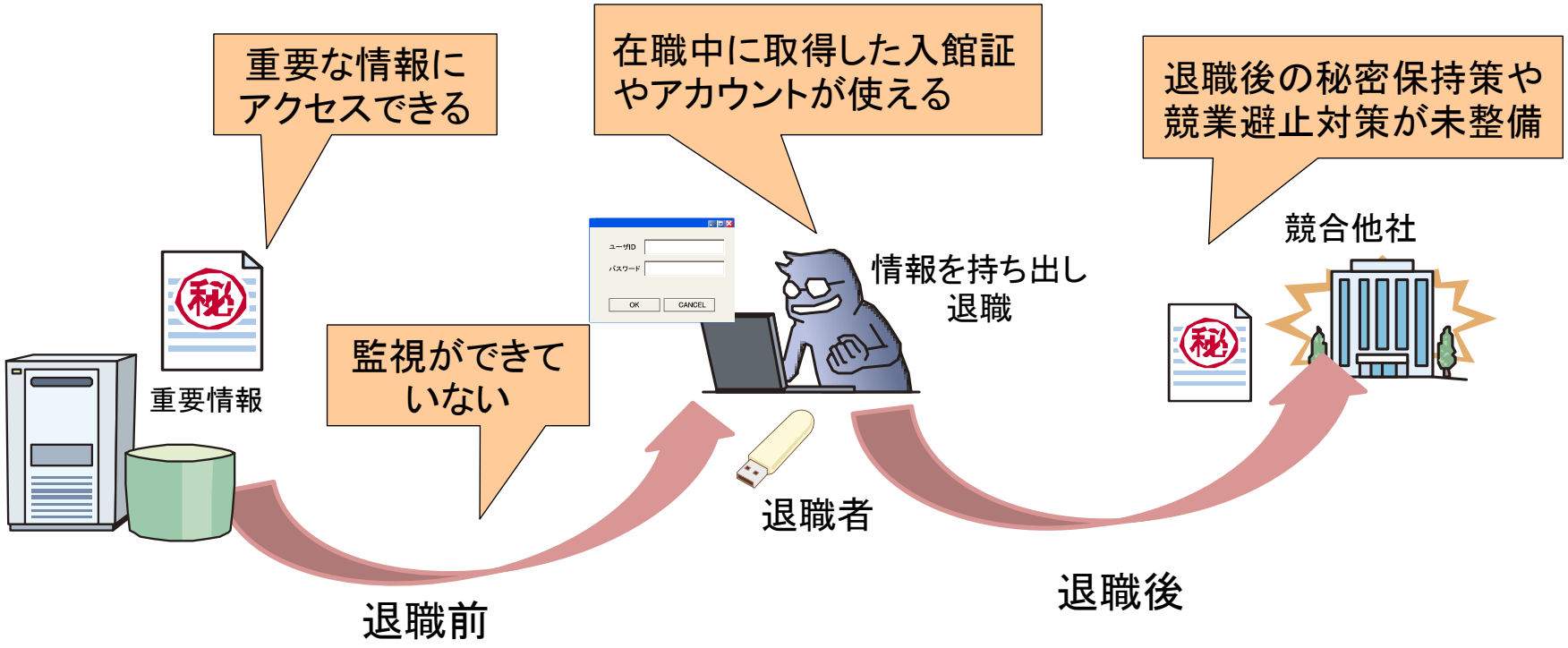
・内部不正の早期発見や事後対策の観点から、重要情報へのアクセス履歴、利用者の操作履歴等のログを記録する。
・ログを定期的に監査し、異常な事象の発見に努める。



ケース１　退職にともなう情報漏えい

- 経済産業省の調査※によると、営業秘密の漏えいは中途退職者が最も多い。
- 転職や契約期間の終了など従業員が退職するタイミングに特に注意が必要。

◆ 危険要因



※ 経済産業省:　人材を通じた技術流出に関する調査研究

退職にともなう情報漏えいへの対策

危険要因に対する対策（ガイドラインの参照箇所）

危険要因	対策	内部不正防止ガイドライン	ソリューション例※
監視ができていない 重要な情報に誰でもアクセスできる	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及び監視 （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	アクセス管理 情報資産管理 統合ログ管理
在職中に取得した入館証やアカウントが使える 退職後の秘密保持策や競業避止対策が未整備	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	入退室管理、監視， ID管理

※JNSA 内部不正対策ソリューションガイドを参考とした製品・サービス種別

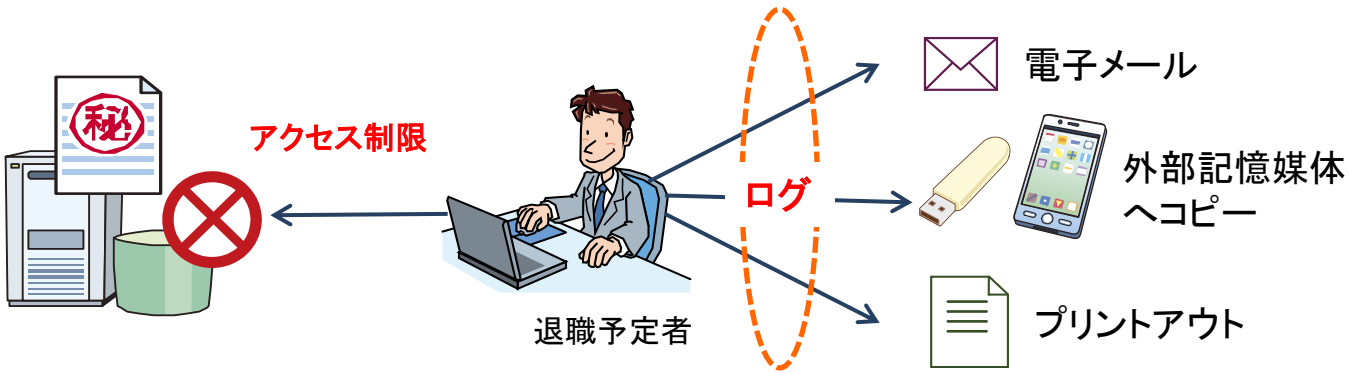
対策ポイント：　退職前の監視強化と退職時の手続き

①退職前の監視強化

内部不正防止ガイドライン：（10）情報機器及び記録媒体の持出管理及び監視
（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

・退職の数週間前からPC等をシステム管理部門等の管理化に置くことが望ましい。なんらかの形で監視されていると意識させることで不正行為を抑止する。

- ✓ 退職する従業員の電子メールのやりとりや、USBメモリへのコピー、プリントアウト等による情報の持ち出しを、操作ログをとり監視する。
- ✓ 重要な情報へのアクセスやUSBメモリの利用を制限する。



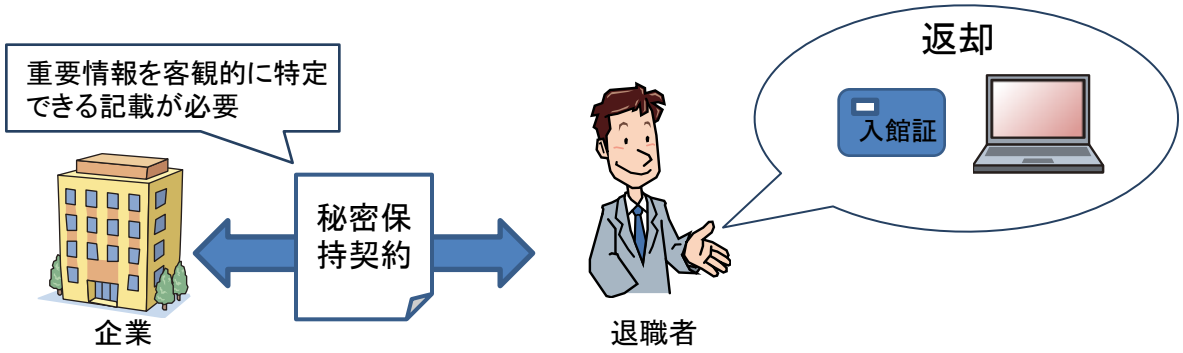
②退職時の手続き

内部不正防止ガイドライン：(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

従業員が退職後に重要情報を持ち出すことを防ぎ、知りえた重要情報が競合他社に渡らないようにするための措置を取る。

- 入館証の回収、貸出機器の返却
- 速やかな情報システムのアカウント削除
  - ✓ アカウント削除漏れがないよう、人事システムと連携して実施することが望ましい。

- 退職後に重要情報が競合他社に渡らないよう秘密保持契約(誓約書を含む)を結ぶことが望ましい。さらに、非常に重要な情報を扱っていた従業員が競合相手に転職しないよう、競業避止義務契約を締結する。ただし、職業選択の自由を侵害しないよう適切な範囲に設定する必要がある。



（参考）競業避止義務契約について

退職後の従業者等に対し、自社と競合する企業への就職や競合する事業を自ら行わない義務をかける契約。違反時に直接的に義務違反を主張できます。

職業選択の自由(憲法第２２条第１項)に対する制約となるため有効性の要件は厳格に判断されています。

○判例分析の結果による有効性が認められやすい規定のポイント(経済産業省委託調査※より)

- 営業秘密等の企業側の「守るべき利益」が存在する。
  ×具体的でない包括的なものは不可
- 基本的には、競業避止義務に見合う何らかの代償措置が設定されている。
- 対象をその「守るべき利益」に関与していた従業者に絞り込む。
  ×職位等の形式的な絞り込みは不可
- 業種にもよるが期間は１年以内。
  ※２年超が認められるのは例外的
- 禁止する競業行為の範囲について、「守るべき利益」と比較して絞り込む。
  ×一般的･抽象的なものは不可
- 競業禁止地域を、職業選択の自由を阻害するような広範なものとしない。
  ※基本的にはこれのみでは有効性を否定しない傾向だが・・

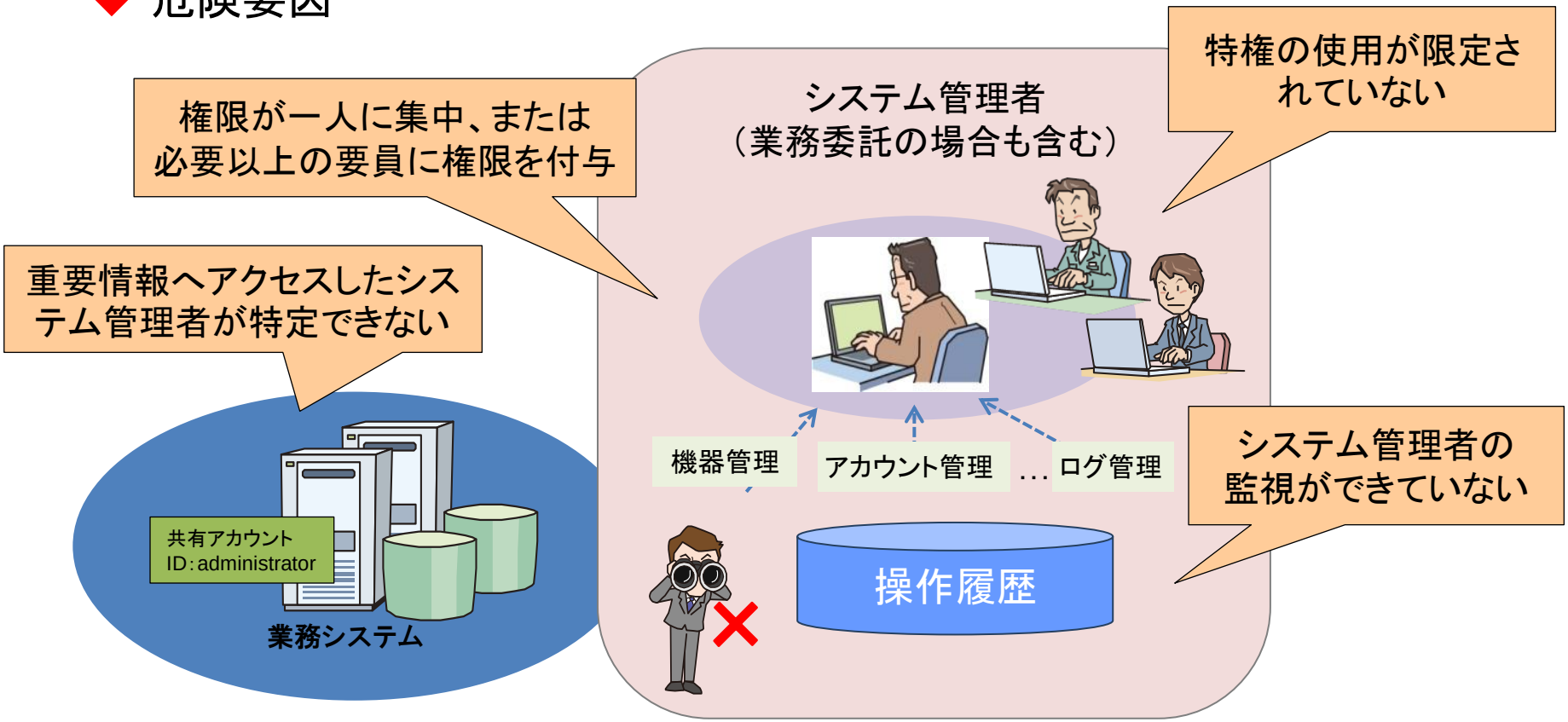
※規定ぶり、減額規定の考え方等の詳細は、平成24年度経済産業省委託調査「人材を通じた技術流出に関する調査研究報告書」を参照下さい。
http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/houkokusho130319.pdf

（出典）経済産業省「営業秘密管理（実践編）」

ケース２　システム管理者による不正行為

システム管理者は多くの権限を持つため、不正行為を働こうとすると重大な事故を引き起こしかねない。

◆ 危険要因



システム管理者による不正行為への対策

危険要因に対する対策（ガイドラインの参照箇所）

項目	対策	内部不正防止ガイドライン	ソリューション例※
権限が一人に集中 必要以上の要員に権限を付与	①適切な権限管理	（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ID管理 アクセス管理 セキュアOS
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	統合ログ管理

※JNSA 内部不正対策ソリューションガイドを参考とした製品・サービス種別

対策ポイント：　適切な権限管理とシステム管理者の監視

①適切な権限管理

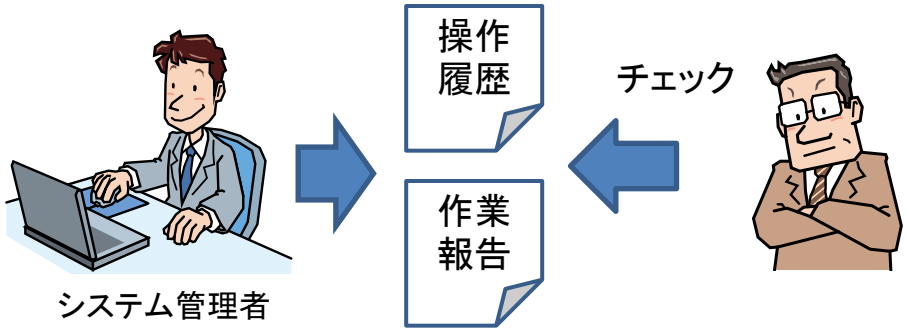
内部不正防止ガイドライン：(6)システム管理の権限管理
(7)情報システムにおける利用者の識別と認証

（ルール、運用）

・特定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する。
- ✓ システム管理者が一人の場合は、操作履歴をシステム管理者以外の者が確認するといった方法でリスクを低減させる。

・重要情報へのアクセス権限を持つ操作員を最小とする。
- ✓ 付与する権限も必要最小限とする。

・システム管理者が相互に監視し、不正を行うことが困難な環境を作る。
- ✓ 複数人で立会い作業する。
- ✓ 作業内容や作業日時等が記録された作業報告を別の管理者が確認する。

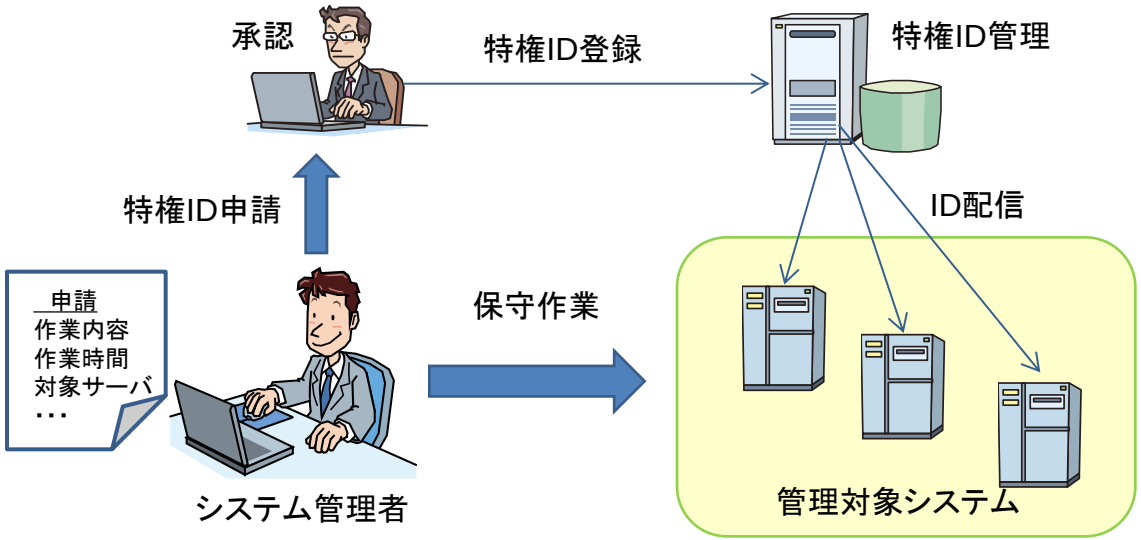


①適切な権限管理

内部不正防止ガイドライン：(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

・システム管理者ごとにIDを割り当て、内部不正行為の特定を可能とする。
- ✓ 共有アカウントの廃止

・特権を用いた操作を限定する。
- ✓ 一時的な特権IDの払い出しや、作業の申請・承認プロセスの厳密化等
  特権を必要とする作業以外ではできるだけ操作できないようにする。



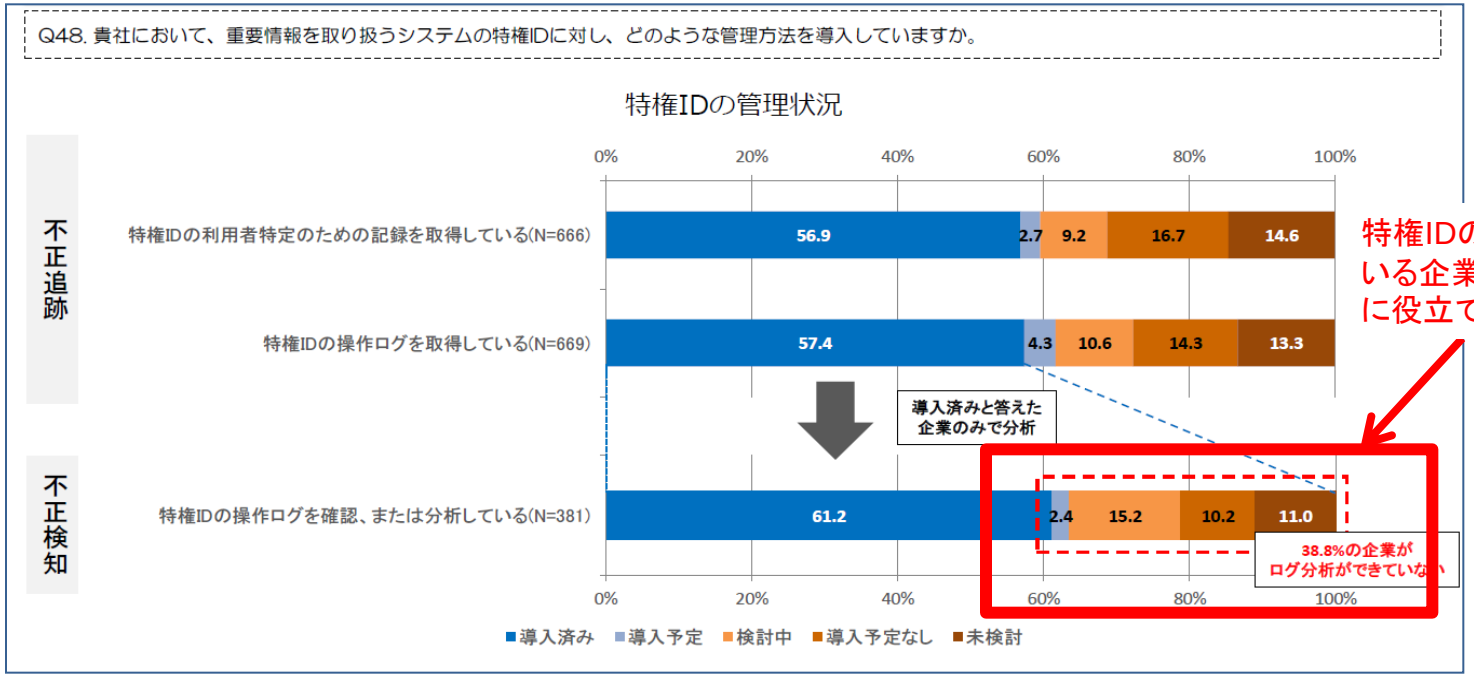
②システム管理者の監視

内部不正防止ガイドライン： （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を記録し、システム管理者以外のものが定期的に監査する。

- ✓ 総括責任者、委託元の責任者、システム管理者の上司などがチェック
- ✓ 作業申請外のアクセス、定期作業外の操作 等

・抑止の関連から、業務担当者にログが記録されていることを通知する。

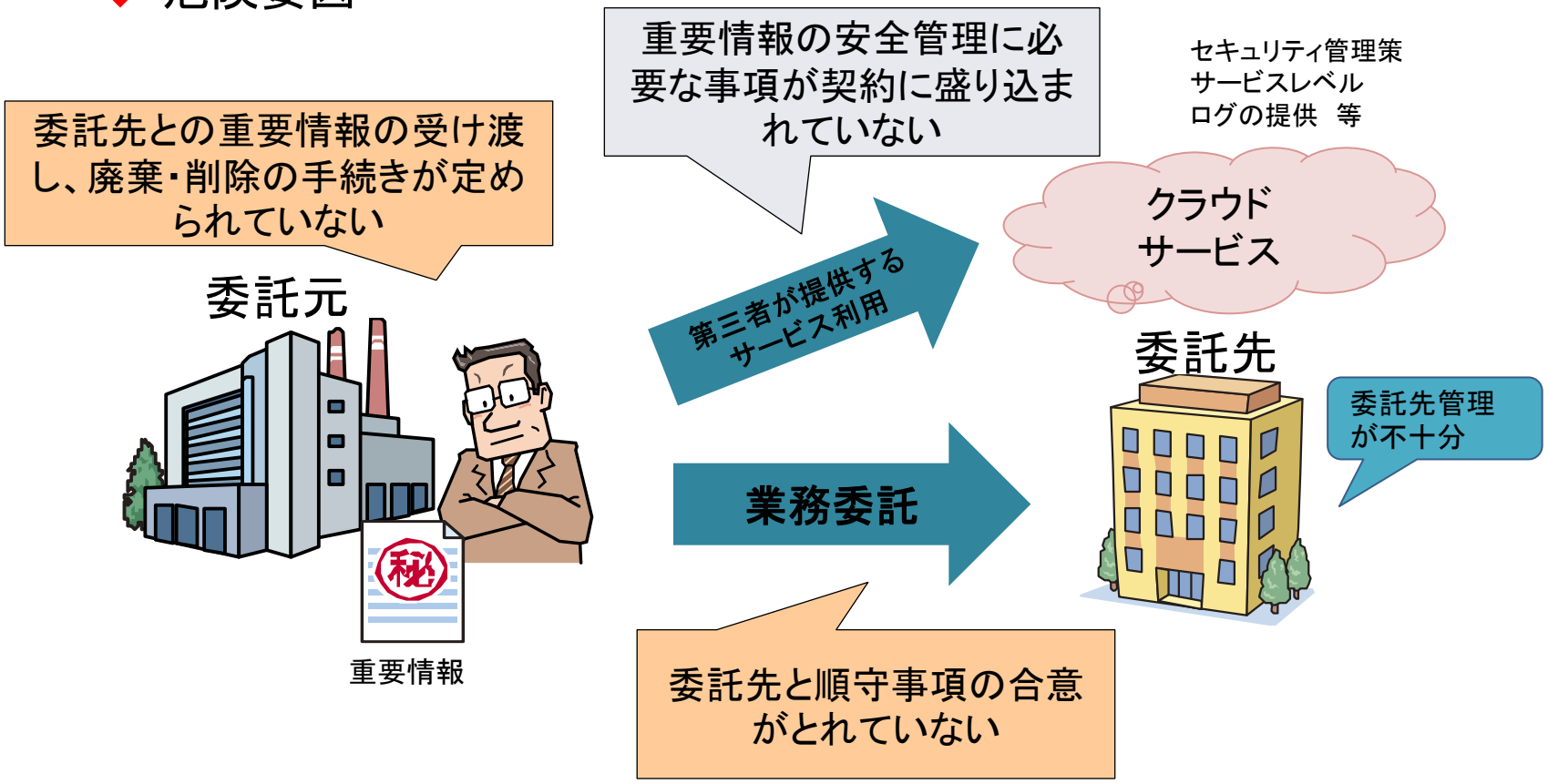


(出典)NRIセキュアテクノロジーズ：企業における情報セキュリティ実態調査2013第2版

ケース３　委託先による情報漏えい等

システム運用を外部に委託する企業が増加する中、委託先での管理体制や管理実態を把握できないケースもあり、委託先社員による事件も発生している。

◆ 危険要因



委託先による情報漏えい等への対策

危険要因に対する対策（ガイドラインの参照箇所）

危険要因	対策	対策（内部不正防止ガイドライン参照箇所）	対策ソリューション例※
順守事項について委託先と合意がとれていない	①重要情報の取扱いに関する委託先管理	（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	ファイル暗号・追跡 データー時保管サービス セキュアファイル転送
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			
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	（16）第三者が提供するサービス利用時の確認（クラウドコンピューティングを含む）	情報セキュリティマネジメントサービス

※JNSAの内部不正対策ソリューションガイドを参考とした製品・サービス種別

対策ポイント： 重要情報の取り扱いに関する委託先管理
契約への安全管理事項の盛り込み

①重要情報の取扱いに関する委託先管理

内部不正防止ガイドライン：（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

・重要度に合わせた取り扱い（受け渡しや廃棄）の手続きを定め、委託先、再委託先にも順守させる。
・関係者に開示した重要情報の廃棄・消去の記録を取得する。
  ✓ 契約終了時、取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させる。確証をとることが望ましい。

取扱いを委託した情報資産や与えた権限	
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-ROM/DVD-ROM、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

内部不正防止ガイドライン 付録Ⅲ:QA集　対策のヒントとなるQ&A6　参照

①重要情報の取扱いに関する委託先管理

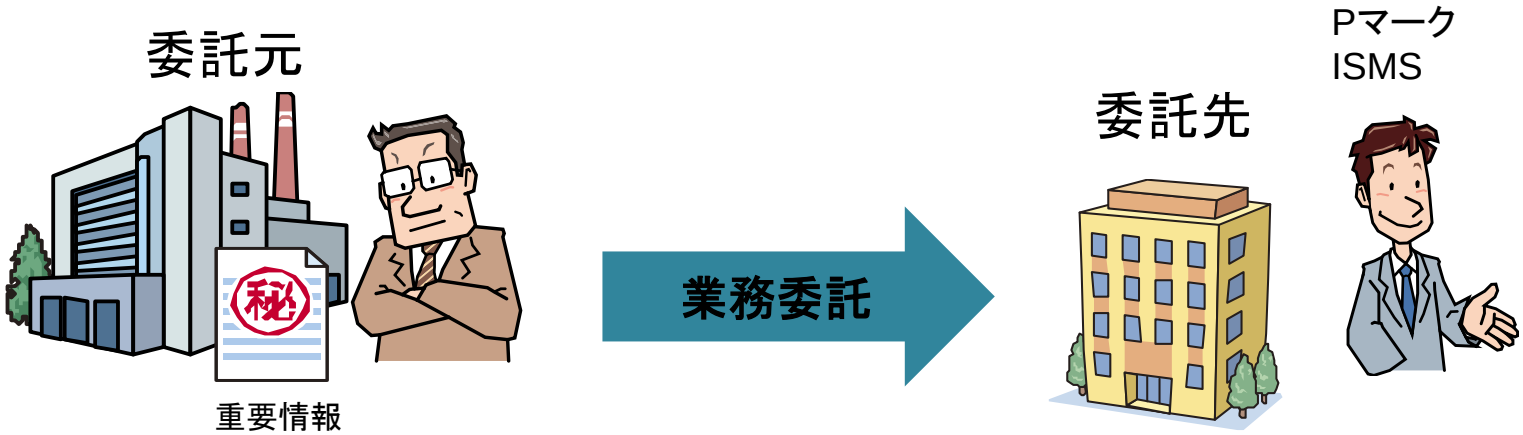
委託元

- 委託先にセキュリティポリシーや情報セキュリティ対策を理解してもらう
- 委託契約では、必要かつ適切な安全管理措置について、委託先と同意した内容を具体化し委託契約を締結する。
- 契約内容について、定期的に遵守されていることを確認する。

委託先（受託者）

- 重要情報を管理する仕組みをつくり対策を行う。
- 対外的なアピール材料
  - 外部のセキュリティ監査を定期的に実施し、監査結果を報告する
  - 情報セキュリティに関する第三者認証を取得する（プライバシーマーク、ISMS等）

（参考）経済産業省、JNSA：中小企業情報セキュリティ対策促進事業
http://www.jnsa.org/ikusei/rule/14_03.html



参考. 外部委託先の監督方法

取り組み事例

・独自のチェック、認定制度による委託先選定

・取扱情報、事業者規模に応じたチェックリストを作成し立ち入り検査を実施

・委託元部署だけでなく法務部が同行チェックし、委託元部署、委託先両社に意識づけ

・委託先へチェックシートを送付し、不備項目には改善計画の提出を求め、原則6ケ月以内に改善できなければ契約を終了

・契約前、契約締結時、契約中、契約後、それぞれチェック

・委託先を集めての合同勉強会開催

・社内点検時に委託先の担当者にも同行してもらい、自社の取り組み、チェックの厳しさを知ってもらう

・パートナー会社の経営層向け意識喚起の機会を設定

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）からの抜粋
http://www.meti.go.jp/policy/it_policy/privacy/061215kozinzyouhou.html

参考. 業務委託契約書の例

契約書に盛り込むべき事項

- 委託内容、範囲、責任の明確化
- 委託契約期間
- 秘密保持義務の取り決め
- 委託契約終了後の情報の取り決め（返還・消去・廃棄等）
- 再委託に関する取り決め
- 委託業者の情報セキュリティ管理に対する内容
- 契約内容を遵守していることの確認
- 契約内容を違反した場合の措置
- セキュリティ事件・事故が発生した場合の措置

業務委託契約書（抄）の例

（出典）経済産業省「営業秘密管理指針　参考資料2 各種契約書の参考例」から抜粋

第〇状（秘密保持）
：
第〇条（再委託）
１．乙は、甲の事前の書面による承諾を得ずに、本業務の全部又は一部を第三者へ再委託してはならない。
２．前項の事前の書面による承諾に基づき本業務を再委託する場合、乙は自己が負う義務と同等の義務を再委託先に対して書面にて課すとともに、甲に対して再委託先に当該義務を課した旨を書面により報告し、かつ乙は当該秘密情報の開示に伴う責任を負うものとする。
：
（具体的な管理方法）
〇．乙は、甲より開示された秘密情報の管理につき、乙が保有する他の情報や記録媒体等と明確に区別して適切に管理するとともに、以下の事項を遵守する。
①　秘密情報の管理責任者及び保管場所を定め、善良なる管理責任者の注意をもって保管管理する。
②　秘密情報を取り扱う従業者を必要最小限にとどめ、上記保管場所以外へ持ち出さない。
③　秘密情報の管理責任者名、秘密情報を取り扱う従業者の氏名及び秘密情報の保管場所を、〇年〇月〇日までに甲に報告する。また、報告内容に変更が生じた場合には、変更が生じた月に提出する第１１号の具体的管理状況の報告において、当該変更内容を甲に報告する。
④　前号にて報告した秘密情報を取り扱う従業者に対して本契約の内容を周知徹底させ、秘密情報の漏洩、紛失、破壊、改ざん等を未然に防止するための措置を取る。
⑤　甲の書面による承諾を得た場合を除き、秘密情報を複写、複製しない。
⑥　秘密情報は本契約の目的の範囲内でのみ使用する。
⑦　事故発生時には直ちに甲に対して通知し、事故再発防止策の協議には甲の参加を認める。
⑧　委託期間満了時又は本契約の解除時には、秘密情報が記録等された記録媒体又は物件（第５号に基づく複写物及び複製物を含む。）を甲に返却、又は自己で廃棄の上、廃棄した旨の誓約書を甲に提出する。

②契約への安全管理事項の盛り込み

内部不正防止ガイドライン：
（16）第三者が提供するサービス利用時の確認（クラウドコンピューティングを含む）

・第三者が提供するサービスを利用する場合は、セキュリティ管理策、サービスレベル、ログの提供等を事前に確認し合意する。

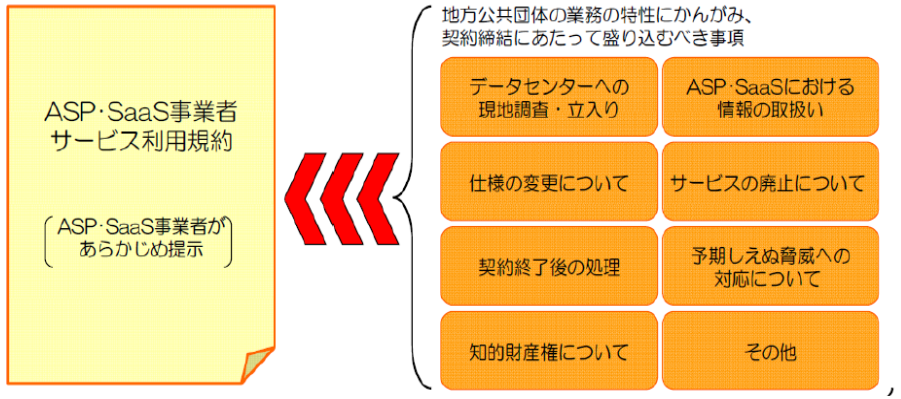
- ✓ クラウドサービスを利用する目的はなにか。（どのようなデータを預けるのか）
- ✓ セキュリティ管理策が、重要情報を安全に管理するため十分か。
- ✓ サービスレベル及び管理上の要求事項が、事業継続において適切か。
- ✓ 内部不正が発生した際に、ログが提供されるか

参考） 経済産業省：クラウドサービス利用のための情報セキュリティマネジメントガイドライン2013年度版
クラウドセキュリティガイドライン活用ガイドブック
→ クラウド契約時の契約書やサービスレベル合意書（SLA）を具体的に解説

①	前提条件	サービスレベルに影響を及ぼす業務上／システム上の前提条件		
②	委託範囲	合意された委託内容がカバーする範囲		
③	役割と責任	クラウド事業者と利用者の役割と責任を明確化した分担表		
④	サービスレベル項目		分類	分類項目の概要
		ア）	アプリケーション運用	システムの使い勝手に関わる項目（可用性／信頼性／性能／拡張性）
		イ）	サポート	障害対応や一般的問合せ対応に関わる項目
		ウ）	データ管理	データバックアップを含む利用者データの保証に関わる項目
		エ）	セキュリティ	公的認証や第三者評価（監査）を含むセキュリティに関わる項目
⑤	サービスレベル未達の場合の対応	サービスレベルが達成されなかった場合の対応方法（補償）		
⑥	運営ルール	クラウド事業者と利用者間のコミュニケーション（報告・連絡）のルール		

（出典）経済産業省：クラウドセキュリティガイドライン活用ガイドブック

契約に盛り込むべき事項の例



（出典）特定非営利活動法人 ASP・SaaS・クラウドコンソーシアム（ASPIC）：
クラウド・利用者の必要知識と関連ガイドライン等について

ケース４　職場環境に起因する不正行為

従業員に不正行為を踏みとどまらせる対策として、職場環境の整備が重要な役割を果たす。

◆ 危険要因

職場環境に起因する不正行為への対策

ガイドラインの参照箇所とソリューション例

危険要因	項目	内部不正防止ガイドライン参照箇所	対策ソリューション例※
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	・人事制度コンサルテーション ・職場診断 ・ヒューマンスキルコンサルテーション
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			

※JNSAの内部不正対策ソリューションガイドを参考とした製品・サービス種別

対策ポイント：　公平な人事評価、適正な労働環境、良好なコミュニケーション

職場環境の整備

内部不正防止ガイドライン：(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

公平な人事評価

- ✓ 公平で客観的な人事評価を整備し、従業員が評価内容を理解、納得できるよう、評価結果を説明する機会を設ける。
- ✓ 適切な人員配置及び配置転換をする。

適正な労働環境

- ✓ 業務量や勤務時間を適正化する。
- ✓ 特定の従業員の業務負荷が極端に高い状況を是正する。

上司

同僚

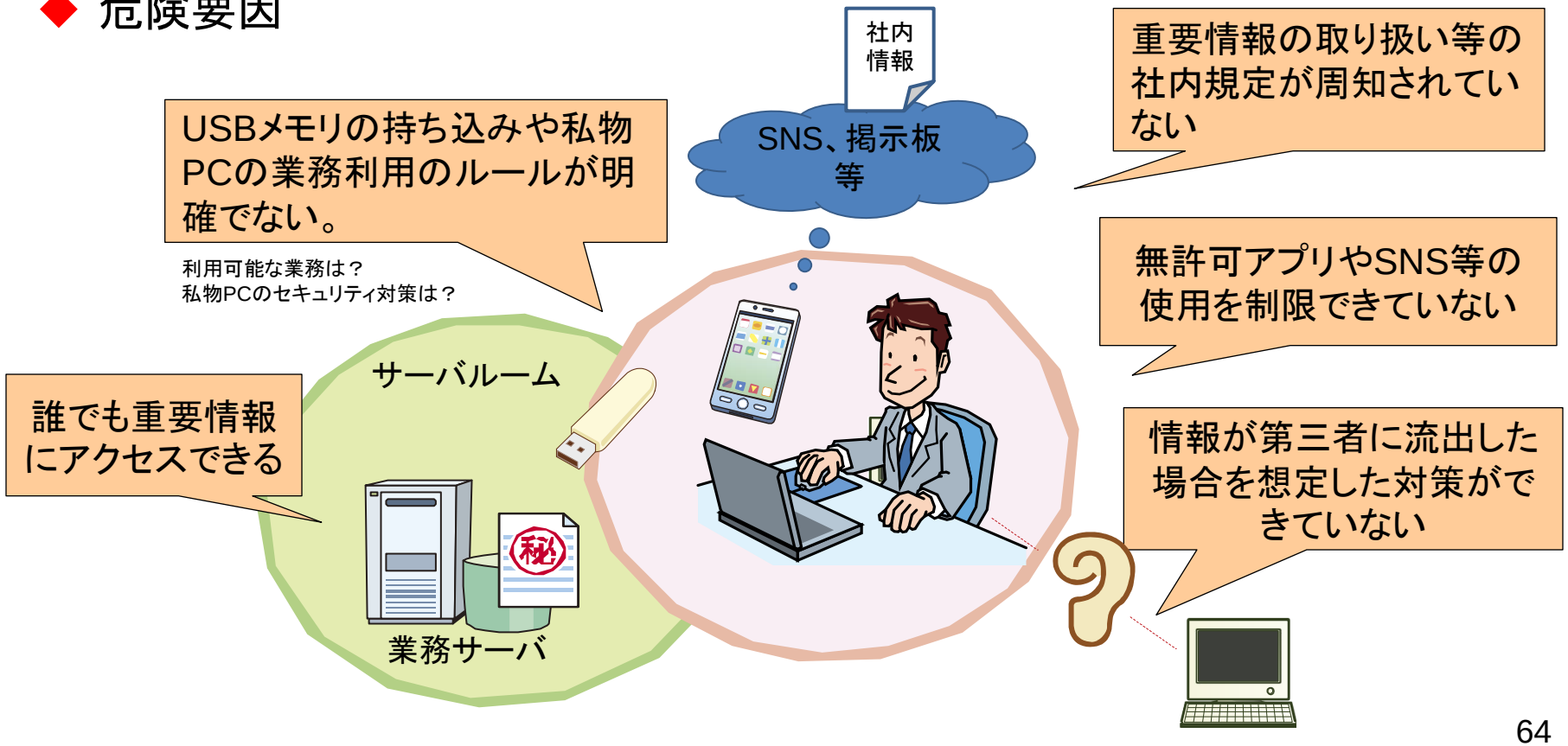
良好なコミュニケーション

- ✓ 相談しやすい環境を整備し、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職場環境づくりを推進する。

ケース5 従業員による悪意のない不正行為

- 企業で発生する内部不正は、明確な悪意を持った不正行為だけではなく、本人に悪気がなかった場合も多い。
- 自宅で作業するための社内情報の持ち出しや、PCの紛失や盗難、うっかりミスによるメールの誤送信、SNSや掲示板への安易な書き込みなど。

◆ 危険要因



従業員による悪意のない不正行為への対策

危険要因に対する対策（ガイドラインの参照箇所）

危険要因	対策	内部不正防止ガイドライン	ソリューション例※
重要情報の取り扱い等の社内規定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	人事育成コンサル、研修
UBSメモリの持ち込みや私物PCの業務利用のルールが明確でない。	②情報漏えい対策	（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	PC管理、検疫
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	コンテンツフィルタリング
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	暗号化
誰でも重要情報にアクセスできる		（5）情報システムにおける利用者のアクセス管理	アクセス管理、認証

対策ポイント：　教育による周知徹底と情報漏えい対策

①教育による周知徹底

内部不正防止ガイドライン：（19）教育による内部不正対策の周知徹底

社内教育を通し、情報の無断持ち出しが不正行為であること、ルールに違反すると社内規定で罰せられることを認識させる。

教育の内容

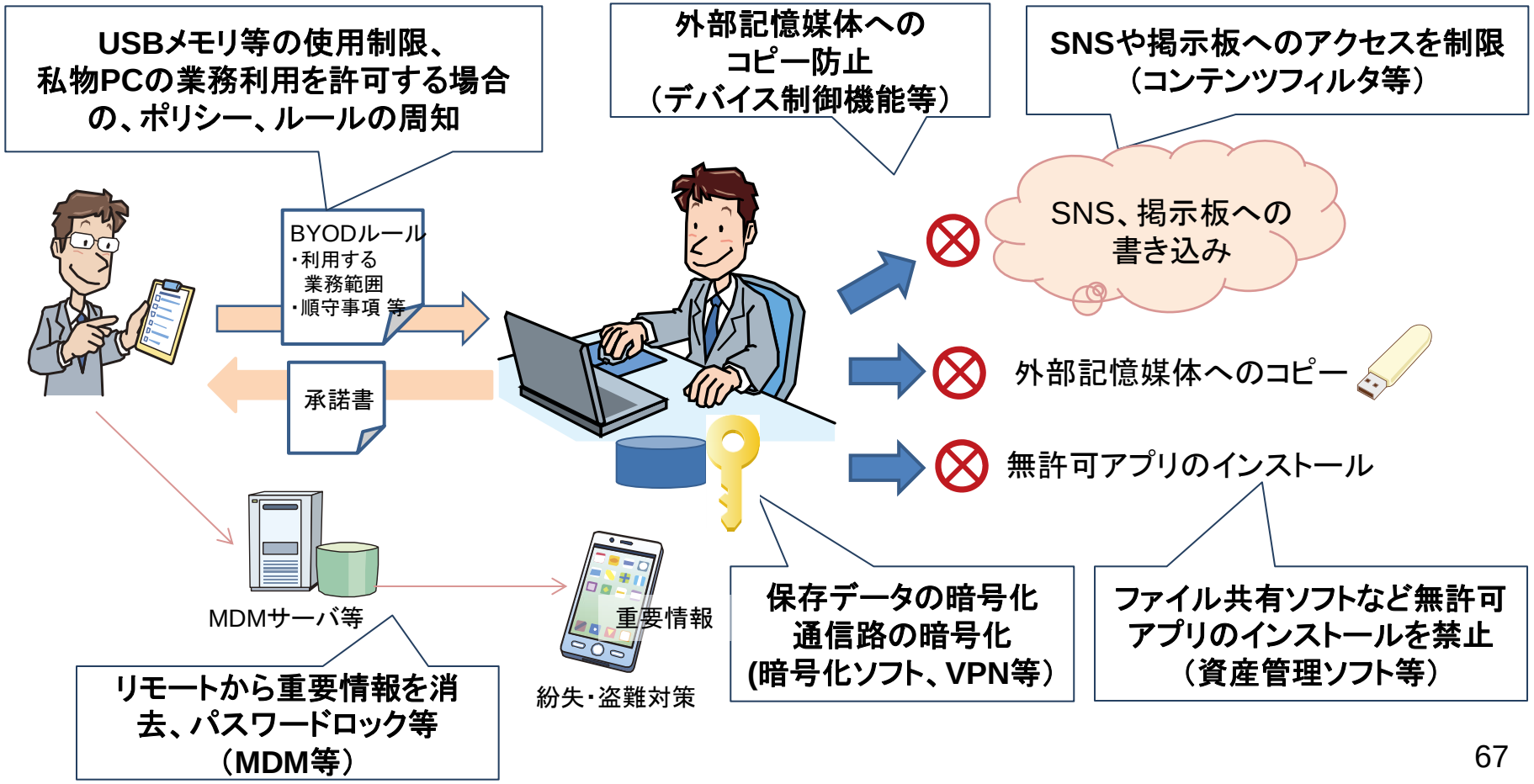
- 内部不正が組織にどのような影響を及ぼすかの具体的事例
- 重要情報の分類や管理方法等に関する順守すべき事項
  - ✓ 機密情報が記された FAX、プリントアウト等の書類が長時間放置されたままにならないようなルール
  - ✓ SNS等を利用した情報発信での注意事項
  - ✓ 内部不正を発見したときの通報の手順　等
- 内部不正が発覚した際の懲戒処分について
- 重要情報の管理方法と対策について
  - ✓ メールのアーカイブ等の監視やモニタリング等を行なっていることを説明する
- 内部不正対策の理解を深めるために、関連する法令等（不正競争防止法、個人情報保護法等）について説明することが望ましい。

ガイドライン 付録Ⅲ:QA集　対策のヒントとなるQ&A7　参照

②情報漏えい対策

内部不正防止ガイドライン：

（5）情報システムにおける利用者のアクセス管理
（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
（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しの保護
（15）組織外部での業務における重要情報の保護



ケース6　早期発見

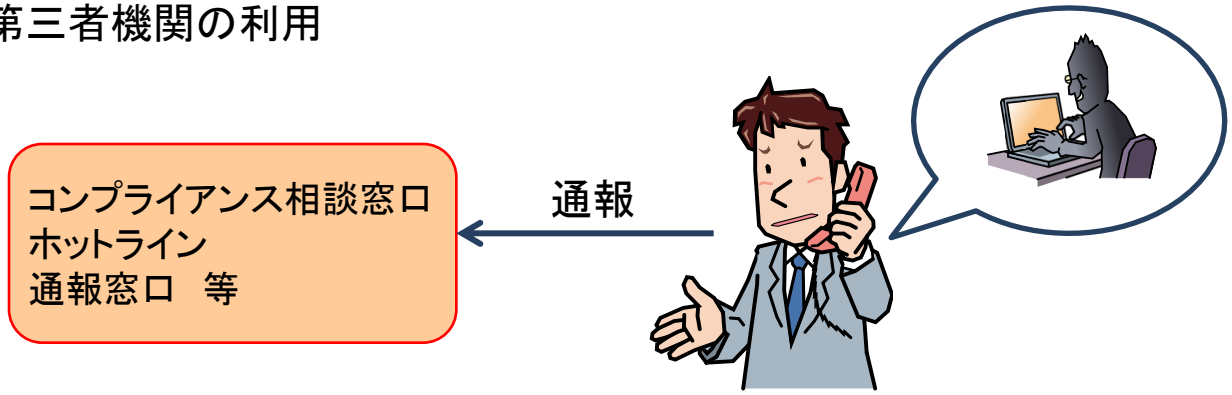
内部不正の予兆を見逃さず、早期対応を図るため、通報制度を整備する。

ガイドラインの参照箇所とソリューション例

項目	内部不正防止ガイドライン参照箇所	対策ソリューション例※
①通報制度の整備	（29）内部不正に関する通報制度の整備	情報セキュリティマネジメントサービス

※JNSAの内部不正対策ソリューションガイドを参考とした製品・サービス種別

・内部不正の通報窓口を設置し、具体的な利用方法を教育する。
・通報窓口（ホットライン等を含む）には、問題が発生した部門での隠蔽行為を防ぐため、複数設置する。
・通報者が通報行為により不利益を受けないよう匿名性を確保する。
　✓　匿名の私書箱や第三者機関の利用



ケース7 内部不正発生時の対応（事後対応）

直接的・間接的被害を最小限に抑えるため、事後対策を実施する。
（自社だけではなく、関係者（顧客、取引先など）の被害も最小限に抑える）

ガイドラインの参照箇所とソリューション例

項目	内部不正防止ガイドライン参照箇所	対策ソリューション例※
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	・フォレンジック ・情報セキュリティマネジメントサービス
②処罰を検討と再発防止策	（22）法的手続きの整備 （28）処罰等の検討及び再発防止	

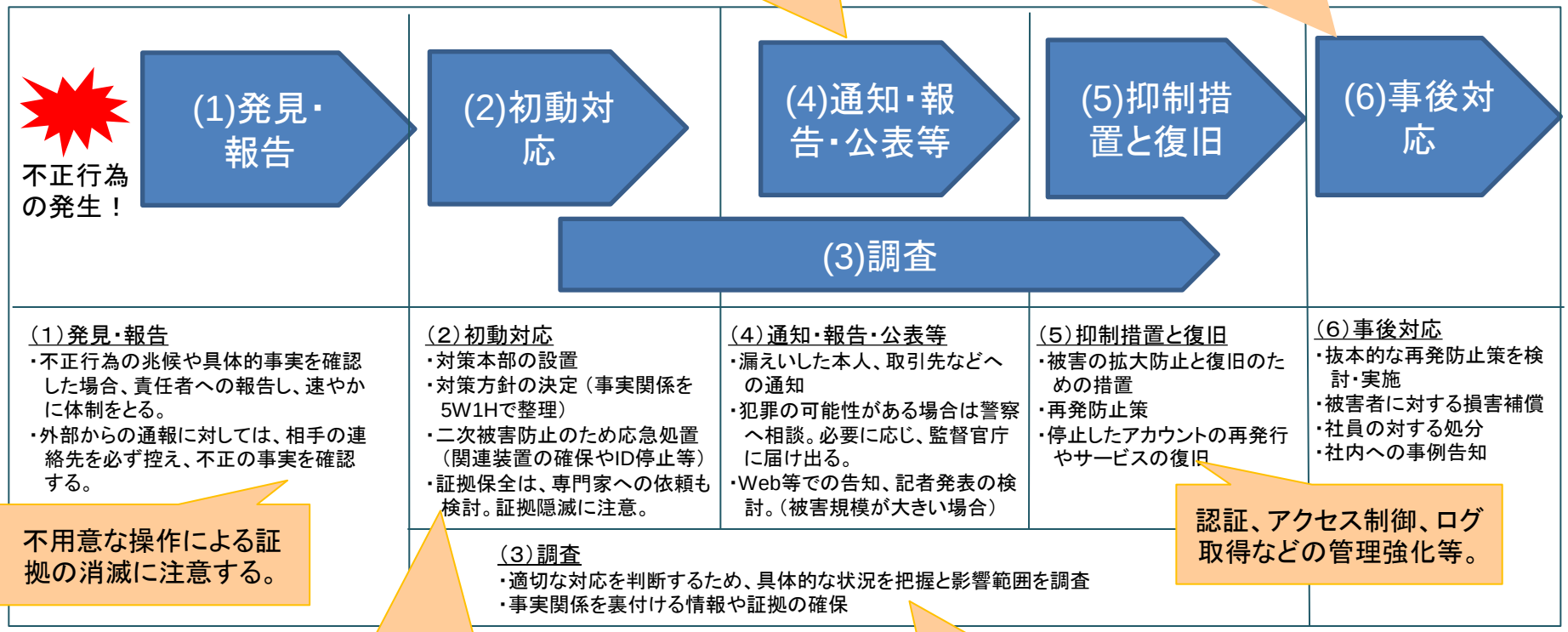
※JNSAの内部不正対策ソリューションガイドを参考とした製品・サービス種別

・対応手順や報告手順を事前に取り決めておく。

内部不正発生時の対応

例　情報漏えい時の対応

参考）情報漏えい発生時の対応ポイント集（IPA）



付録

- CERT®による19のプラクティス
- 米国CERT® Insider Threat Centerについて

内部脅威への19のベストプラクティス

IPA

CERT® Best Practices Against Insider Threats in All Nations

No.	項目
1	企業全体の**リスクアセスメント**で、インサイダーおよび取引先企業からの脅威を考慮する
2	文書化し、一貫したポリシと　コントロールを実行する
3	全従業員への定期的な**セキュリティ教育**にインサイダーの脅威に対する意識を組み込む
4	**雇用プロセス**から監視し、不審なまたは破壊的な行為へ対応する
5	職場環境に負の問題を予測し、管理する
6	資産を知る
7	厳格なパスワードとアカウント管理ポリシーの実装と実践
8	**職務分掌と特権の最小化**
9	クラウドサービスでの明示的なセキュリティ協定の定義、特にアクセス制限と監視機能
10	**特権ユーザに対する厳格なアクセス制御と監視ポリシー**
11	システム変更管理の実施
12	ログ相関エンジンや、セキュリティイベントや情報の管理システム(SIEM)を使い、**ログを採取、監視し、従業員の行動を監査する。**
13	モバイルデバイスを含むすべてのエンドポイントからの**リモートアクセスを監視し制御**する。
14	包括的な**従業員の終了（退職）手続き**の策定
15	セキュアなバックアップとリカバリ手続きの実装
16	インサイダー脅威対策（プログラム）を策定
17	通常のネットワークデバイス行為のベースライン（通常の振る舞い）を確立する
18	ソーシャルメディアに対して特に警戒する
19	**無許可のデータ脱出へのドアを閉める**

各プラクティスの詳細は付録を参照

CERTによる19のプラクティス

Best Practices Against Insider Threats in All Nations

No.	• 内容
1	• 企業全体のリスク評価を行う • 物理的、技術的制御として多重防御する • 組織は、全ての従業員、請負業者、信頼するビジネスパ-トナーに秘密保持契約（NDA）への署名を要求し、組織に合ったバックグラウンドチェックをする。
2	• 従業員は、雇用の際および定期的に、ポリシーを理解し、遵守することをコミットするためサインする。 • 組織は、ポリシーの中で、システムやデータの許可使用についてや、成果物の所有権、従業員の評価や不満の対処などを明確にしなければならない。
3	• 組織は、従業員に対しインサイダー脅威（不正コピーや不正アクセス、パスワード取得など）の行動を認識するため訓練を実施する。 • トレーニングは、不正な行動を報告するための手順を含む。従業員は組織のポリシーを理解するため、定期的にテストを行う。
4	• 組織は内定者、請負業者、ビジネスパートナーからの従業員のバックグラウンドチェック（身元調査）を行い、定期的に再調査をし、インサイダー個人、専門性、金融ストレス要因を確認する。内容は、犯罪歴、信用調査、職歴、能力評価など。 • 組織はリスクレベルを決定し、個人を調査する違反に対する処置（警告、処罰、EAP）を強化する。 EAP: Employee Assistance Program
5	• 組織は、キャリアや労働時間、紛争解決等を明確に伝え、期待を維持し、公正な職場環境を促進する。もし、ボーナスや昇給がない場合は事前通知する。 • セキュリティ担当者は、金融ストレスやダウンサイジングなどの影響を受けた個人を警戒する。
6	• 組織は、誰がアクセス許可され、どこにあるのか、すべての物理的情報資産を管理する • 組織は、データのタイプ、データが処理され、保存される場所を理解する • 組織は、資産のソフトウェア構成を文書化する。資産リストはタイムリーに更新する。
7	• 組織は、共有パスワードを禁止し、定期的にパスワードを変更する、強力なパスワードポリシと手続きを策定する。請負業者やベンダーを含むすべてのスタッフはこれに従わなければならない。 • 法的部門は、契約者に契約の終了をタイムリーに通知することを要求する。 • 組織は、共有アカウントを禁止し、定期的に監査し、すべてのアカウントの必要性を再調査する
8	• バックアップやリストアなどの場合の相互監視（2人ルール） • 最小特権の実装 • ロールベースのアクセス制御
9	• データ保護と監視要件は、組織の独自要件に適合する必要がある（データ保護については物理的・技術的のみでなく人的要件も含める） • プロバイダーは事前に従業員の身元調査を行い、雇用後の定期的な更新、トレーニング等を行う • 組織はプロバイダーの契約、SALを見直し、プロバイダーのポリシやその実施をレビューする。SLAは人的資源、監査や違反通知の要件を含む • 組織、第三者、またはプロバイダー自身が、監視、分析、監査する

CERTによる19のプラクティス

IPA

Best Practices Against Insider Threats in All Nations

No.	内容
10	・組織は、特権ユーザに対し、ユーザ協定や行動ルールを含む特権固有のポリシーへのサインを要求する。特権ユーザの職務分掌が重要。 ・組織は、職務終了時、完全にアクセス不可であることを確認する
11	・組織は、ハードウェア、ソフトウェアの構成をベースに識別し文書化する、変更を更新する。（許可しない変更、例えばバックドアの作成などを防ぐ） ・変更管理プロセスを管理する
12	・組織は、従業員の行動のベースラインと不規則な行動を把握し、モニタリングを調整するためSIMSを活用する ・法務、人事(HR)、情報保証（IA）などを含む、企業全体の協力が必要
13	・モバイルデバイスによるリスクを認識する ・組織はリモートアクセスのすべての処理のログを取得、監視し、ユーザが退職時にはアクセスを無効にする
14	・組織は、従業員の退職時のポリシを策定しそれに従う ・退職者の物理的、電子的アクセスが無効であることを保証するためのチェックリストを策定する ・疑わしい行動を検知するため、退職前の30日間のネットワーク行動を考慮する。
15	・組織はSLAの遵守を保証するため、安全でテストされたバックアップとリカバリのプロセスを持つ ・可能であれば、作業時、特権ユーザの権限分離を行う ・ログを改ざんできないよう保護する ・クラウドサービスの場合は9を参照
16	・インサイダー脅威対策は企業全体で実施し、役割と責任を明確化して、対応する ・組織は、インサイダー脅威を識別する基準、悪意のある振る舞いを防止するための技術的、非技術的対策を実行するめの手順等を策定する ・法的部門（弁護士）は、情報収集に関しすべての証拠が法的基準の従い収集、維持されているか確認する。また、従業員のプライバシー保護を保証する。
17	・ネットワーク上での異常な振る舞いを識別するため、ベースラインの挙動を捉える ・より広範囲なアプローチとして、非技術的な職場の行動も収集する ・できるだけ広く、企業、部、グループおよび個々のレベルで正常なネットワーク上の振る舞いを集める ・長くモニターするほど信頼できる
18	・組織はSNSに関するポリシと手続きだけでなく、トレーニングを行うべきである ・組織は、意図的と意図的でないもの両方について、SNSへの投稿を制限し、関係法に従いSNSのポリシ策定を検討する。
19	・重要な資産、アクセス許可されている人、実際にアクセスする人、資産の場所を識別する ・組織は重要資産をどのように削除、コピーするかを理解する。物理的、ワイヤレスで接続するすべての装置を考慮する ・課題は生産性とセキュリティのバランス

付録：米国CERT® Insider Threat Centerについて

年		主な活動テーマ
2000	初期の研究	米国国防省（DoD）の支援により、軍と国防を対象とした研究がされた。
2001	内部者の脅威の調査研究の開始	シークレットサービス、CERTの共同プロジェクトが開始された。DHS（Department of Homeland Security）が2003，2004年の予算措置の支援をした。金融分野、IT分野、政府分野、重要インフラ分野に焦点を当てた報告書を公表。
2001	内部者の脅威データベースの構築	上記のシークレットサービスとの共同研究の成果をデータベース化した。その後、維持には、カーネギーメロン大学（CMU）のCylabが支援した。2009年は、DHSのFNS（Federal Network Security)部門がこのデータベースのスポンサーになる。
2005	ベストプラクティスの提供	「内部不正の防止と検出の共通的なガイド」を発行（Cylabがスポンサー）した。 現在はDHS　FNSがスポンサーで、ベストプラクティスが提供されている。
2005	システムダイナミクスによりモデル化	内部脅威者のふるまいを、システムダイナミクスとしてとらえたMERIT（Management and Education of the Risk of Insider Threat）モデルを公表
2006	オンサイトワークショップの開催	内部者脅威の防止、リスク分析についてのワークショップを、組織などからの希望により、オンサイトで開催。
2006	双方向の仮想シュミレーションツール	MERITモデルの双方向シミュレーションツールを公表。
2007	内部脅威の分析	130分類4000の内部脅威分析項目を発表。 ITセキュリティ、HR（人事）、ソフトウエア開発、法律、データ保持者、物理セキュリティの分野における文書を公表。 2009年にDHS FNSがこの分析プロセスを評価し、スポンサーとなった。
2008	内部脅威　ラボ設立	CyLabによって“insider threat lab”が設立され、内部犯行を防ぐための技術対策の評価などが可能となった。DHS FNSがその環境を利用することを支援している。
2010	内部脅威　訓練	内部犯罪　防止のためのシュミレーション訓練を可能とする環境を設置した。現在政府や産業界にワークショップなどで提供されている。
2010	内部脅威　調査 金融セクター	DHS　S&T（Science & Technology）、シークレットサービス、DoT（Department of Treasury : 財務省）と共同で再度、金融・銀行領域の調査を開始。

参考情報

1. IPA:「組織における内部不正防止ガイドライン」
   http://www.ipa.go.jp/security/fy24/reports/insider/index.html
2. IPA：組織内部者の不正行為によるインシデト調査 調査報告書
   http://www.ipa.go.jp/files/000014169.pdf
3. IPA:情報漏えい発生時の対応ポイント集
   http://www.ipa.go.jp/security/awareness/johorouei/
4. 経済産業省:「人材を通じた技術流出に関する調査研究報告書(別冊) 営業秘密の管理実態に関するアンケート調査結果
   http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/H2503chousa.pdf
5. 経済産業省：営業秘密管理指針
   http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/111216hontai.pdf
6. 経済産業省：クラウドサービス利用のための情報セキュリティマネジメントガイドライン2013年度版 クラウドセキュリティガイドライン活用ガイドブック
   http://www.meti.go.jp/press/2011/04/20110401001/20110401001.html
7. NRIセキュアテクノロジーズ：企業における情報セキュリティ実態調査2013第2版
   http://www.nri-secure.co.jp/news/2014/0221_report.html

- ご清聴ありがとうございました