IPA Better Life with IT

企業の内部不正はいかにして起こるのか ～実例とその対策～

独立行政法人 情報処理推進機構
技術本部 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

目次

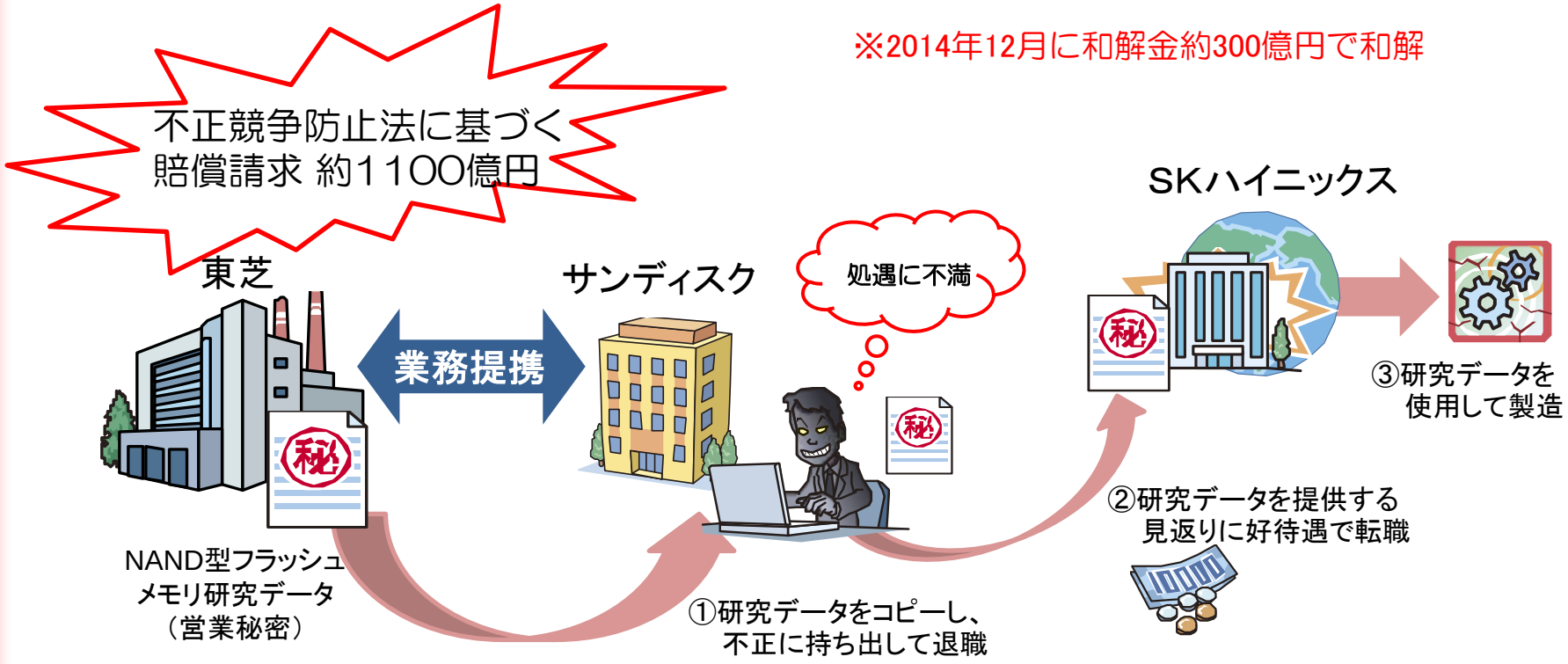
１．内部不正に関する状況

(1)　相次ぐ内部不正事件　～　2014年以降

報道月	事件の概要	不正行為者	動機
2015年1月	家電量販店エディオンの元社員が、販売戦略に関する営業秘密を不正に取得したとして**不正競争防止法違反（営業秘密の不正取得）**の容疑で逮捕された。	退職者 現社員	転職先で役立てたかった
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先である株式会社日立製作所の社員が、権限を悪用し入札情報等を不正に入手し、自社の入札活動に利用したとして**公契約関係競売等妨害の容疑で刑事告発され、懲戒処分**となった。	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9月25日時点で報道より得られた情報を元に記載

流出した個人情報は
約３５０４万件

業務被害
- 特別損失 260億円（2014年度第1四半期）
- 役員2名が辞任

(2)　内部不正の状況：海外　1/2

- 「グローバル情報セキュリティ調査®」 2015
  - Managing cyber risks in an interconnected world : Key findings from The Global State of Information Security Survey 2015, Sept.2014

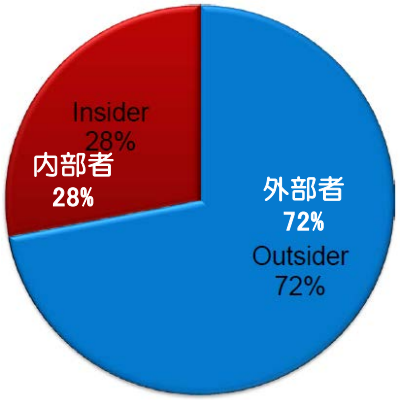
- 2014 US State of Cybercrime Survey
  - PWC, CERT®, CSO Magazine, US Secret Service
  - 回答者：557エグゼクティブ（従業員5000人以上 : 28%,500～5000人 : 29%,500人以下 : 43%）

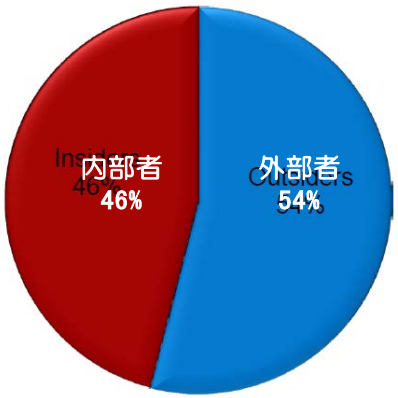
- CERT®/内部脅威センターによる事例収集と分析
  - 2000年、国防省（DOD：Department of Defense）がスポンサーとなり「内部者の脅威プログラム」が開始
  - カーネギーメロン大学ソフトウエア工学研究所（SEI）に設置
  - 政府機関等がスポンサーとなり、2014年2月現在、850の事例を収集・分析し内部不正対策を推進

(2)　内部不正の状況：海外　2/2

- インシデントの発生源として最も多く挙げられたのは「従業員」
  - 現従業員35%　元従業員30%　ハッカー24%
  - グローバル情報セキュリティ調査2015
- 企業の37%が内部者による事故を経験
- サイバー犯罪の3割は内部犯行者であるが、被害額はほぼ同じ（内部46%・外部54%）
  - US　Cyber Crime Survey2014

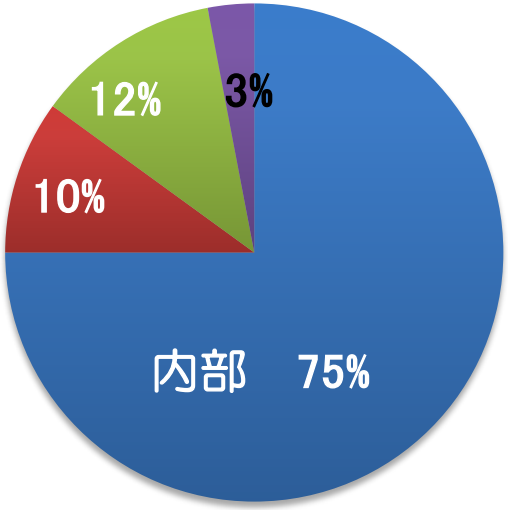
サイバー犯罪(eCrime)の犯行者の内訳





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

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



- 内部（法的措置や法執行なし）
- 内部（法的措置あり）
- 外部（法執行に通知）
- 外部（民事訴訟を起こす）

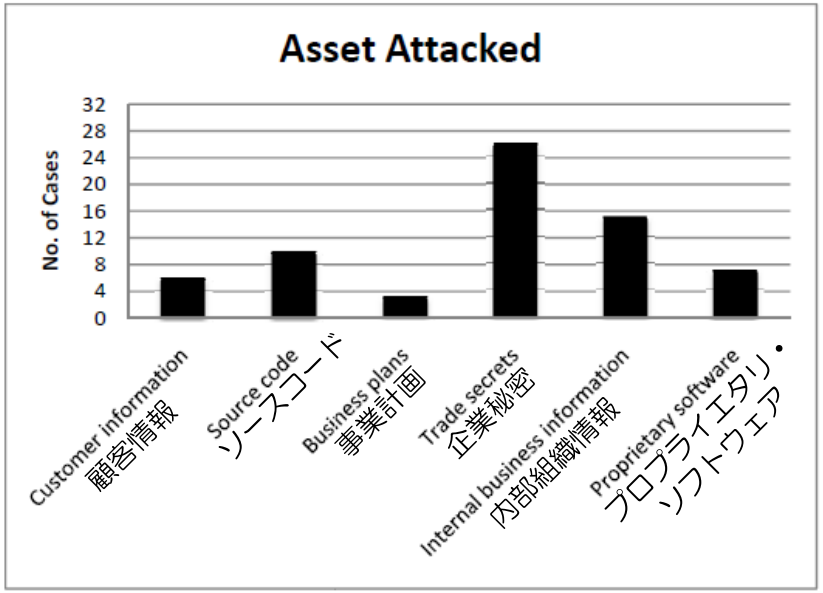
出典：2014 US State of Cybercrime Survey、2014.4（PWC, CERT, CSO Magazine, US Secret Serviceによる）

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、事故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

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

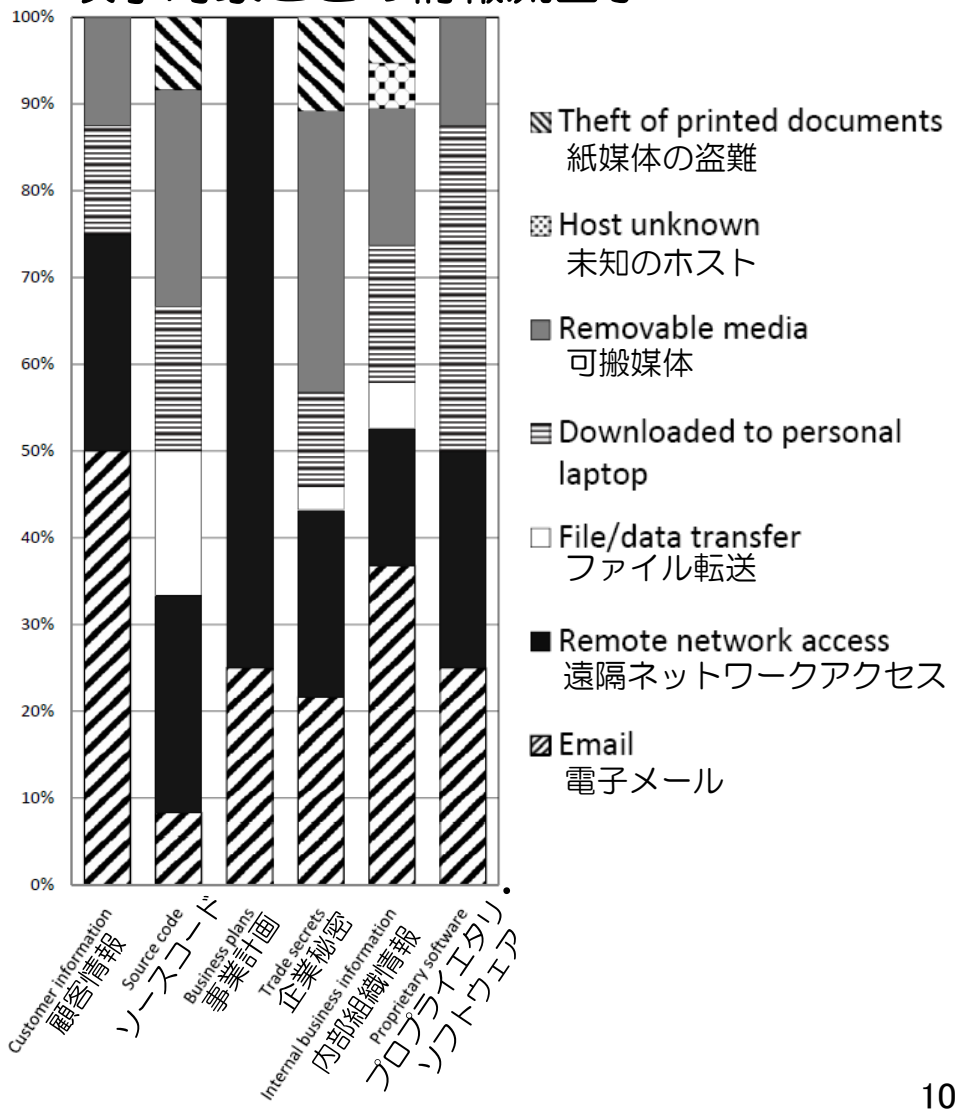
攻撃対象資産



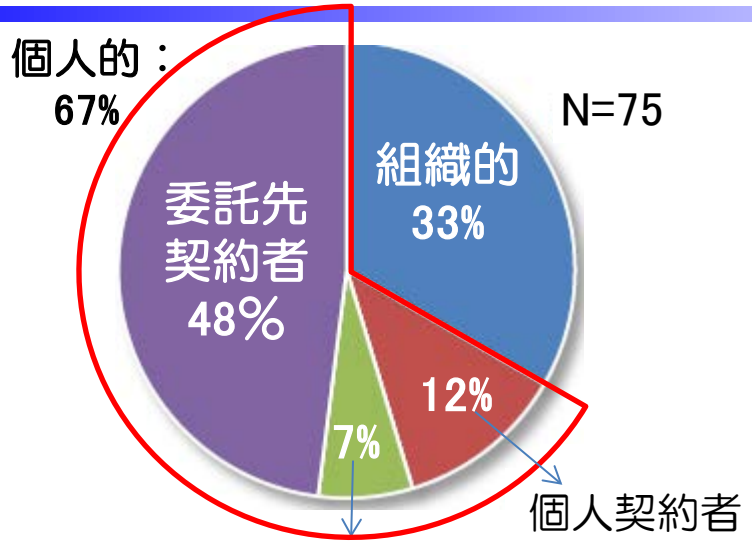
内部者に攻撃された資産の種類

＊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。

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

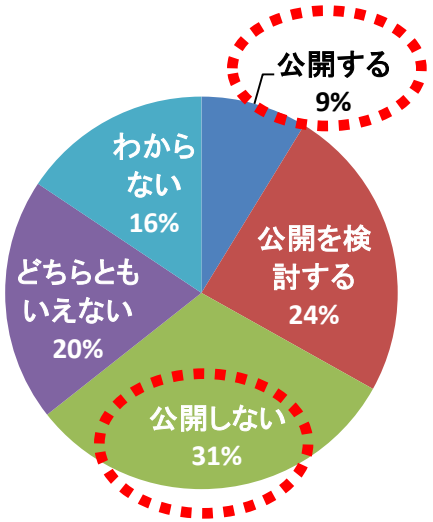
75事例における割合（%）	委託先などのビジネスパートナ		通常の内部者
	組織的	個人的	
職種			
技術職	45	80	39
非技術職	55	20	61
許可されたアクセス（範囲）			
権限あり	44	36	48
権限なし	26	36	23
場所			
組織内	81	60	73
遠隔（リモート）	19	40	27
雇用者　状況			
現職	90	69	76
前職	10	31	24
不正の種類			
システム悪用	64	23	54
IP窃取	28	18	19
システム破壊	8	59	27
動機（かっこ）内は順位			
経済的利益	59(1)	28(2)	53(1)
報復	0(5)	46(1)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

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まれ
  （**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

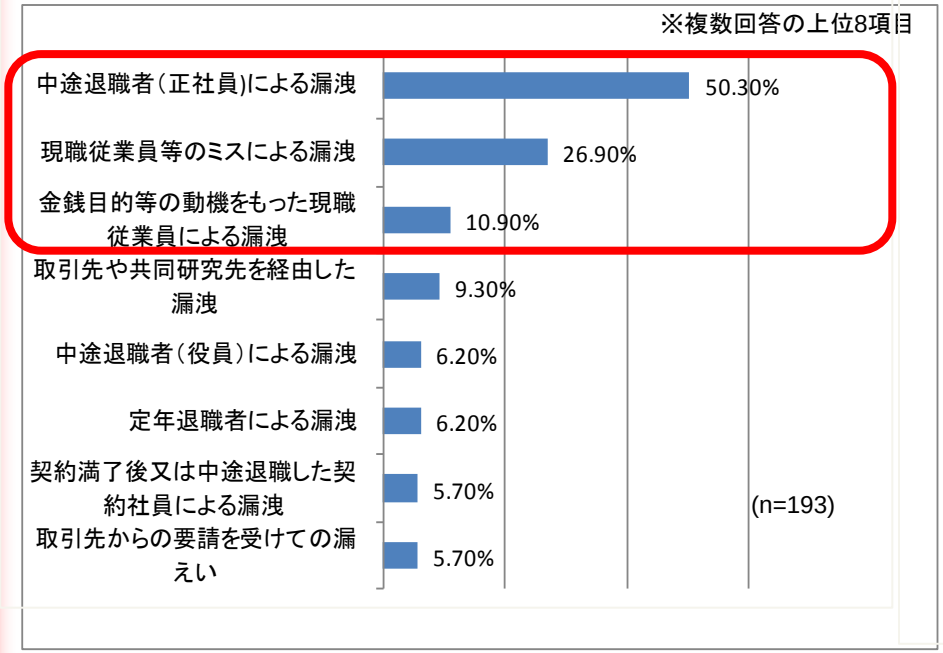


（経営者、管理者を対象としたIPAのアンケート調査より）

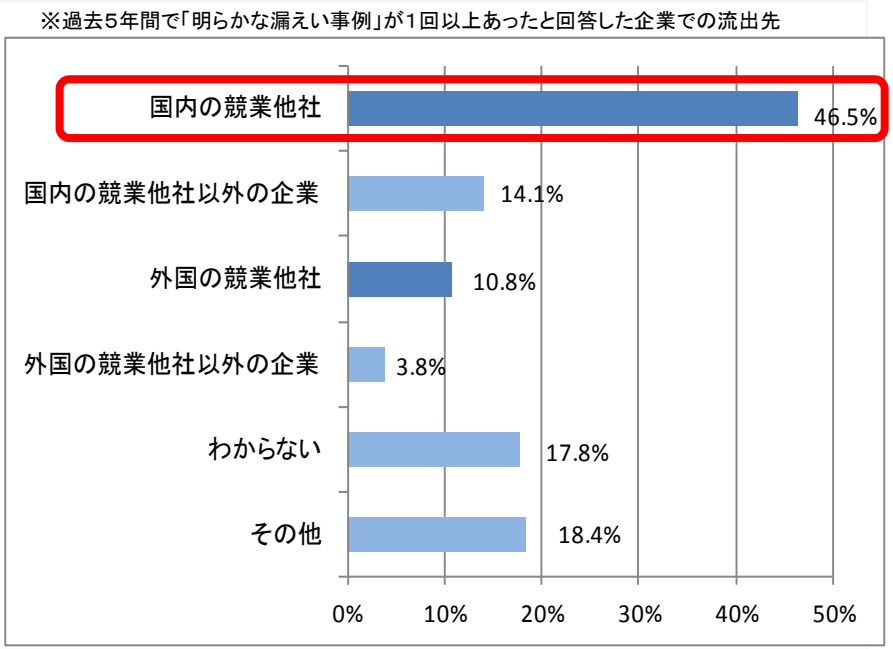
(3)　内部不正の状況：国内　1/3
企業における情報漏えいの実態

- 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、従業員によるものが多くを占める。
- 流出ルートでは、退職者による漏えいが最も多い。
- 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）」

(3)　内部不正の状況：国内　2/3
現状の対策と従業員の意識

- 対策状況は、アカウント管理、アクセス制御関連が中心（経営者向けアンケート）
- 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）

（社員:n=3,000　経営者・管理者:n=110）

(3)　内部不正の状況：国内　3/3
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）

2．内部不正の起きる要因と対策

内部不正はなぜ発生するのか
不正のトライアングル

- 「動機・プレッシャー」「機会」「正当化」の３つの要因が揃った時に発生(ドナルド・R・クレッシー)

動機・プレッシャー		機会		正当化
不正行為に至るきっかけ、原因。処遇への不満やプレッシャー（業務量、ノルマ等）など。	×	不正行為の実行を可能、または容易にする環境。IT技術や物理的な環境及び組織のルールなど。	×	自分勝手な理由づけ、倫理観の欠如。都合の良い解釈や他人への責任転嫁など。

例.

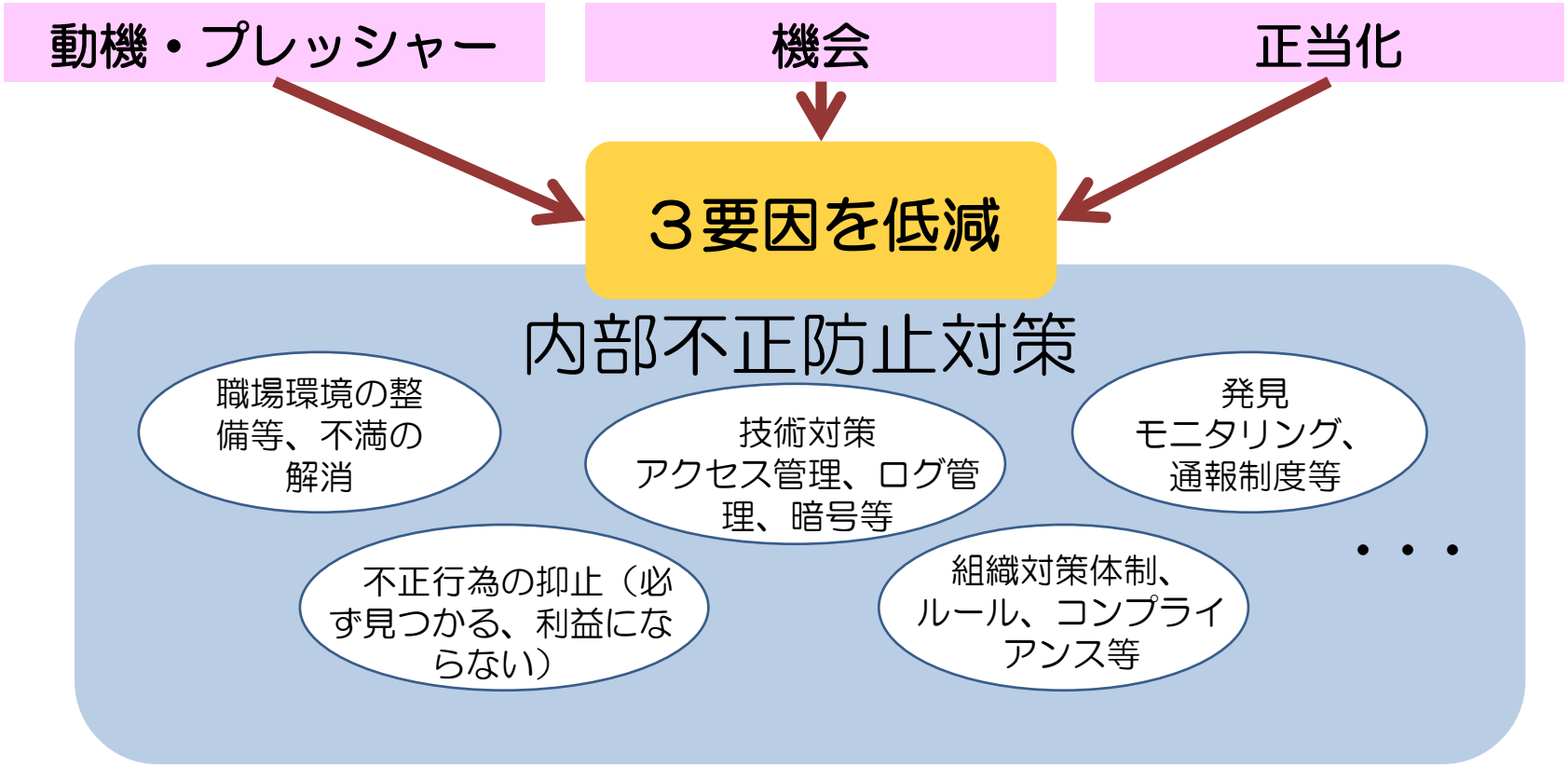
人事に不満がある 金銭問題を抱えている	×	システム管理者権限 持ち出し可能な環境	×	• 正当に評価がされないから • 情報窃取を繰り返しても気づかれない。

※米国の組織犯罪研究者

犯罪対策として、「状況的犯罪予防」による予防策についても効果があると言われている。この分類は付録参照

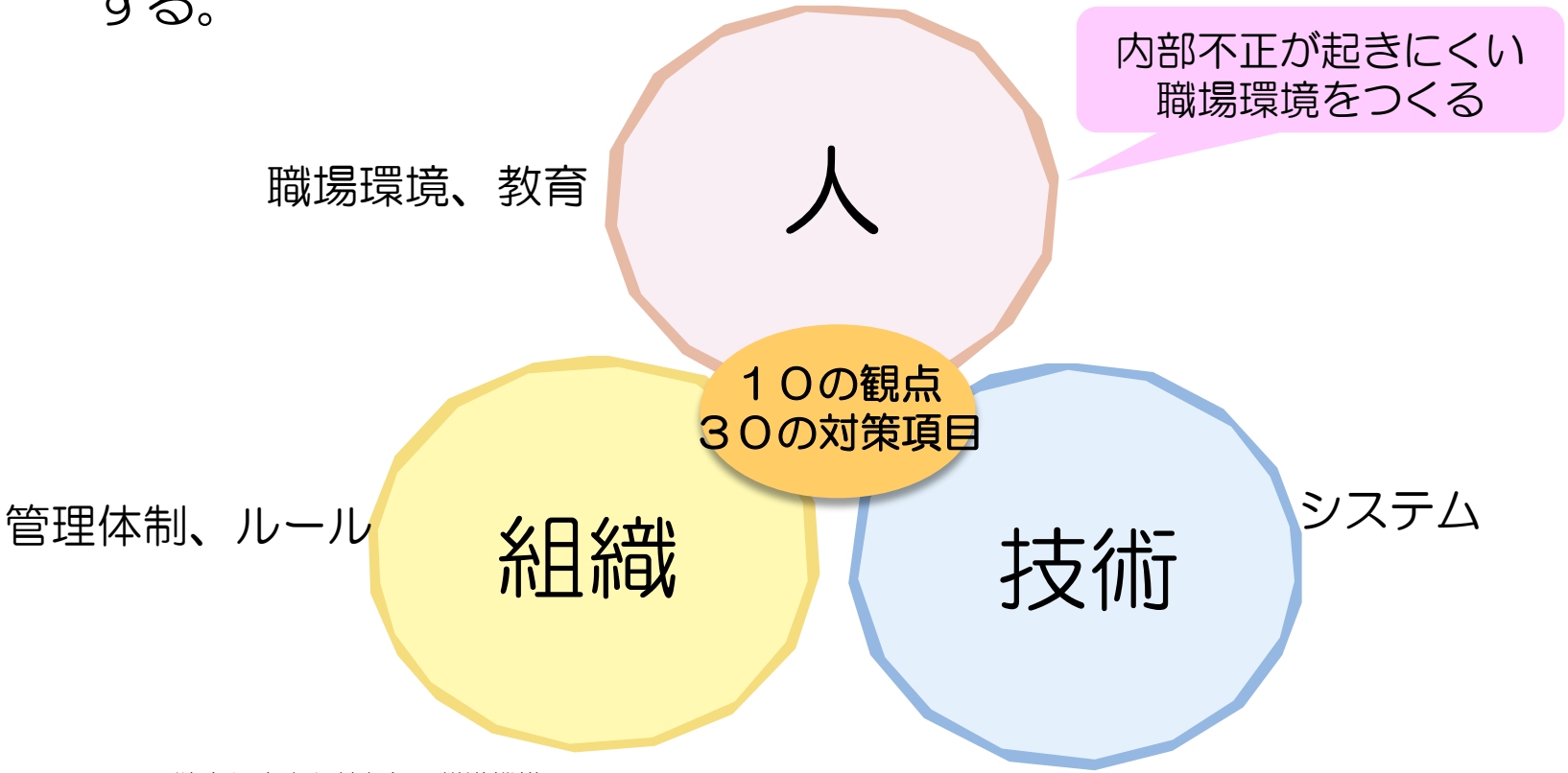
内部不正防止対策は３要因の低減

- 組織が対策できるのは、
  「動機・プレッシャー」と「機会」の低減



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
- 不正トライアングルの３要因（特に、動機・プレッシャーと機会）の低減に向け、「人」、「組織」、「技術」の面から、対策を検討する。



3.　内部不正防止対策事例

内部不正防止の基本対策
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

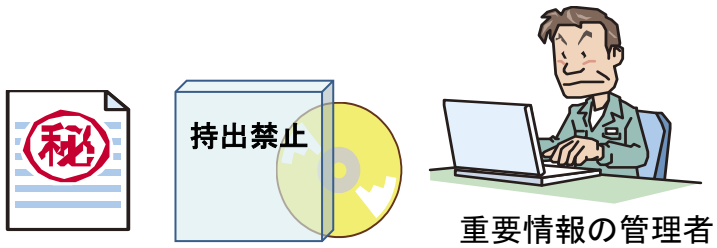
内部不正防止の基本対策　1/3

a. 営業秘密として不正競争防止法の法的保護を受けるために必要な対策

- 重要情報の特定
  - ✓ 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、定期的に見直す。（取扱範囲、消去方法等）
  - ✓ 従業員にわかるように目立つ場所に「機密情報」等を表示する。（ラベル付け）

営業秘密管理指針
秘密管理性の要件の趣旨は、秘密であることを社員に明示し、不測の嫌疑を回避すること。企業が特定の情報を秘密として管理していることを社員が容易に認識できる**「認識可能性」**がポイント。

2015.1 全部改訂

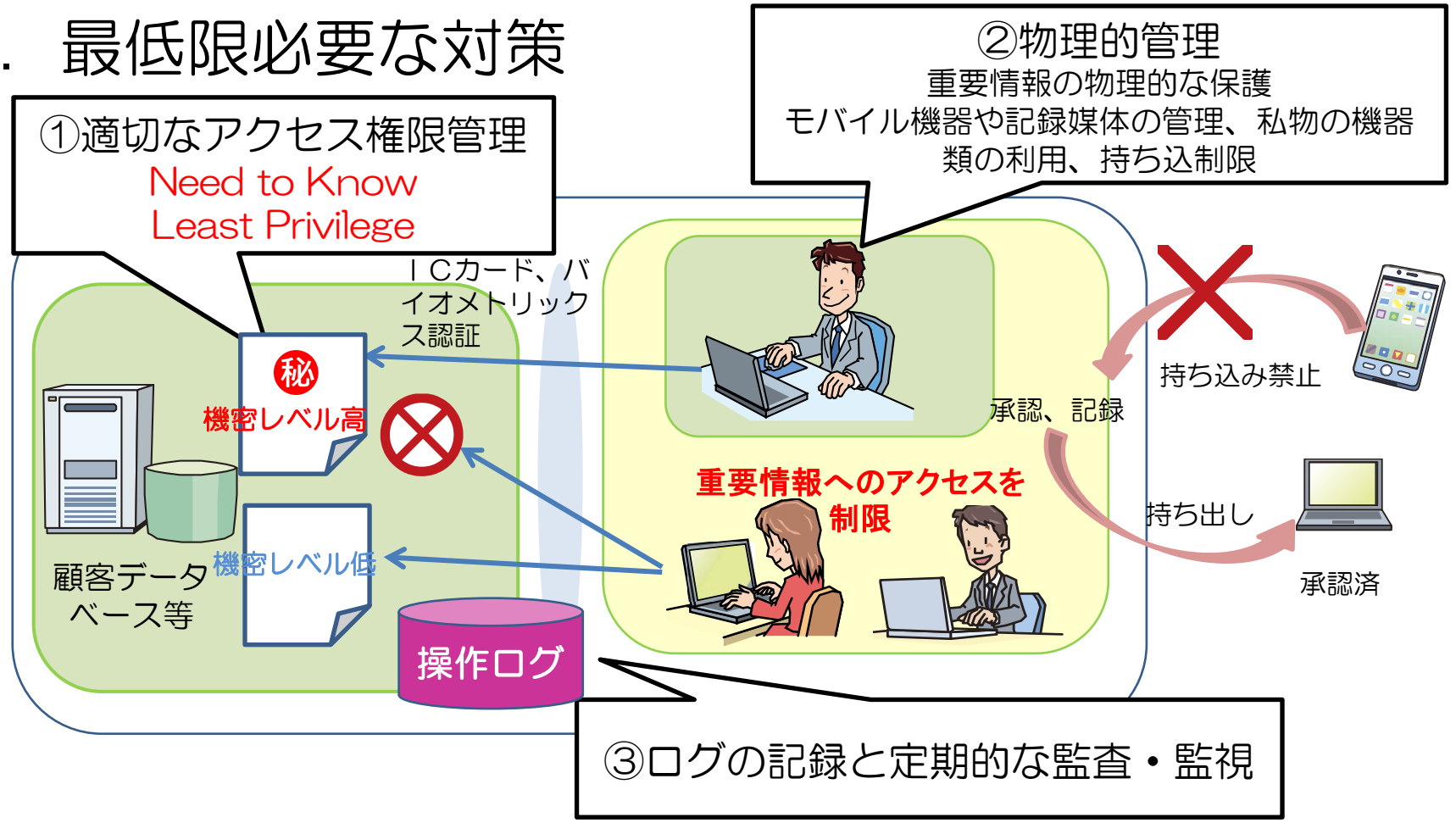


「秘」などの表示

重要情報の管理者
（部門責任者等）

内部不正防止の基本対策　2/3

b.　最低限必要な対策



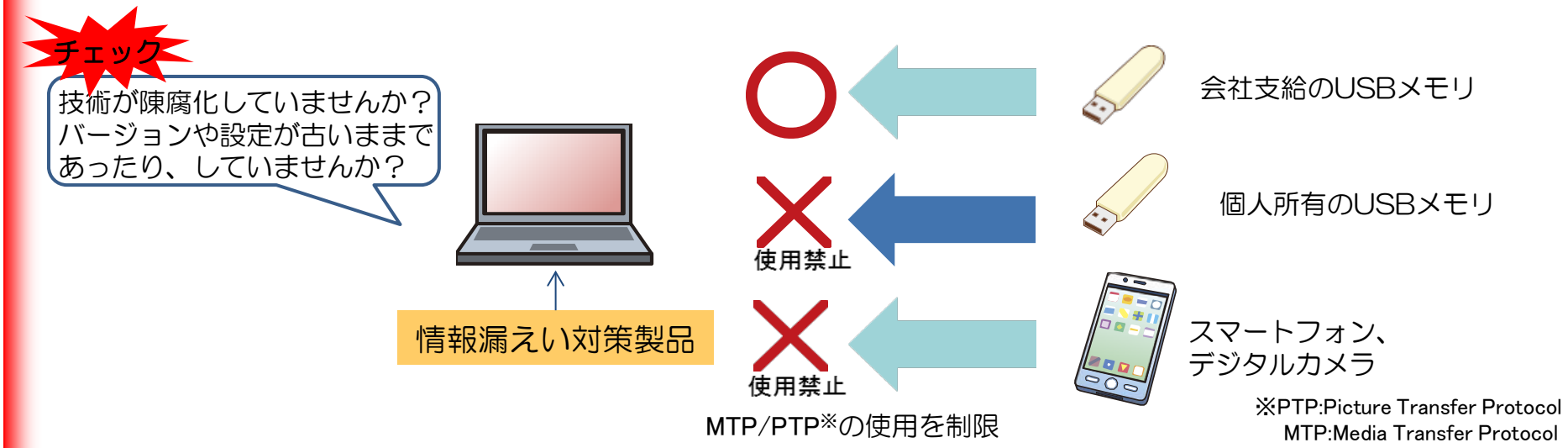
④内部不正対策の継続した見直し、改善

内部不正防止の基本対策　3/3

対策例：モバイル機器等の業務利用及び持ち込み制限

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。
  （サーバルーム、重要情報を取り扱う業務フロア等）
- ✓ 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



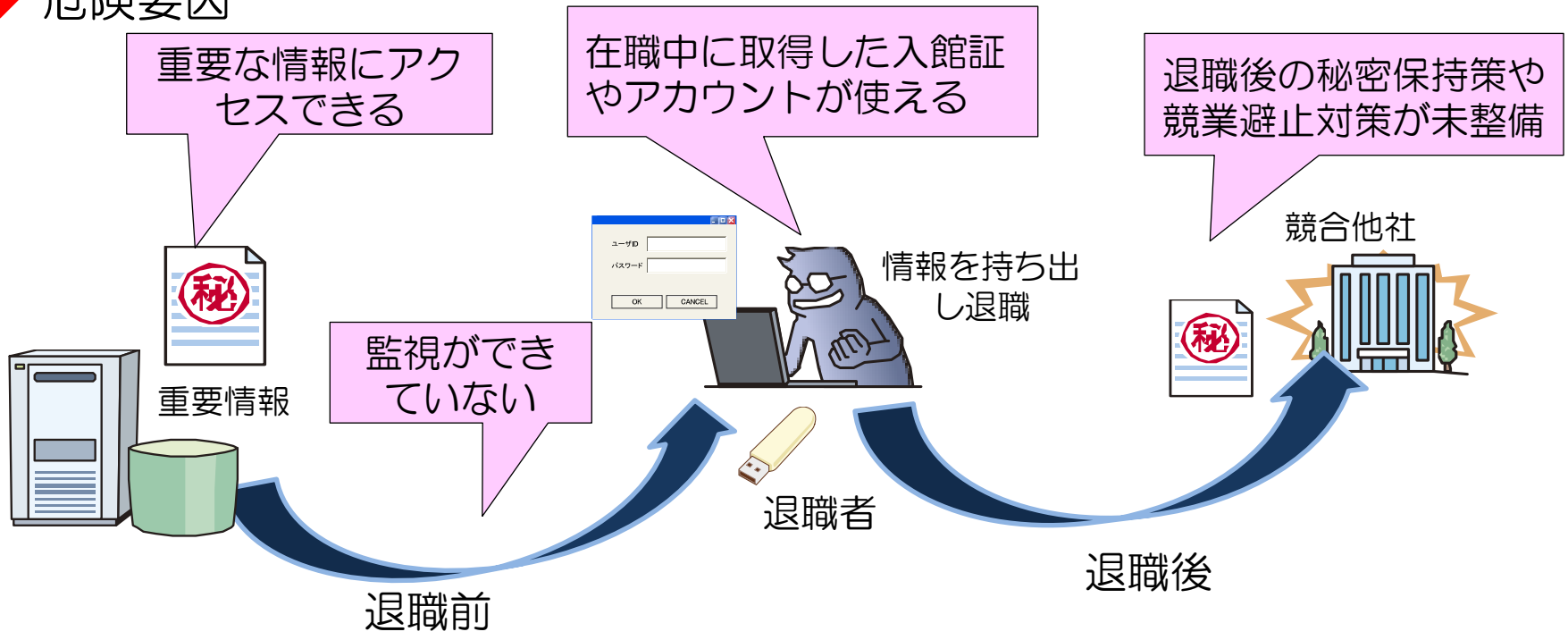
ＩＴの技術進歩や新たな脅威の出現等に応じて、継続的に対策を見直し改善する。

ケース1　退職にともなう情報漏えい

ポイント：　退職前の監視強化と退職時の手続き

- 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



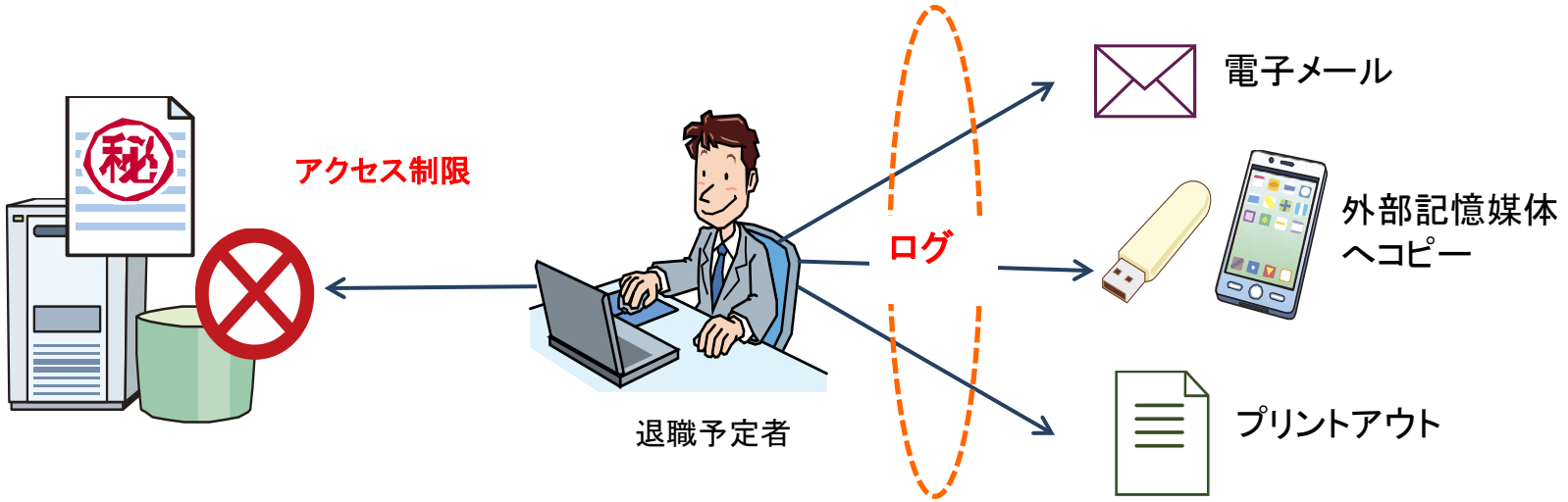
※経済産業省：人材を通じた技術流出に関する調査研究

退職にともなう情報漏えいへの対策

①退職前の監視強化

- 退職の数週間前から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。

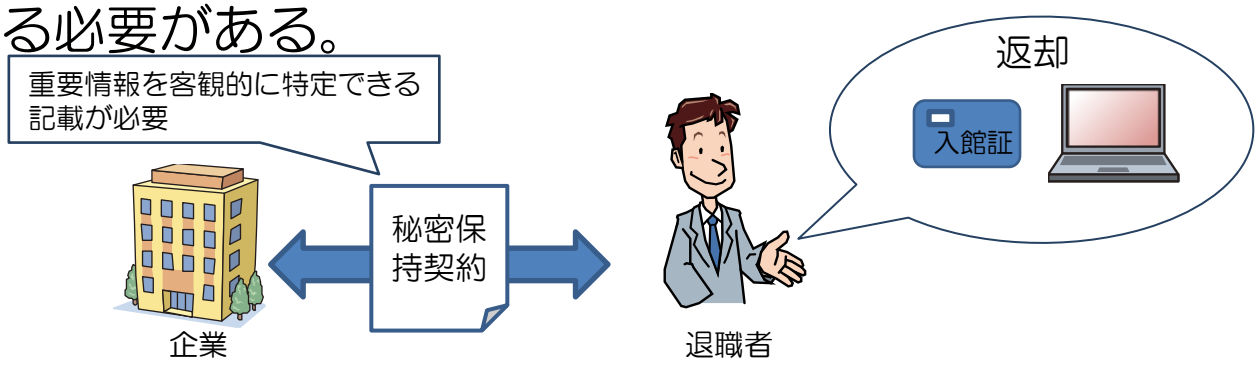
  ✓ 退職する従業員の電子メールのやりとりや、USBメモリへのコピー、プリントアウト等による情報の持ち出しを、操作ログをとり監視する。
  ✓ 重要な情報へのアクセスやUSBメモリの利用を制限する。



②退職時の手続き

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。

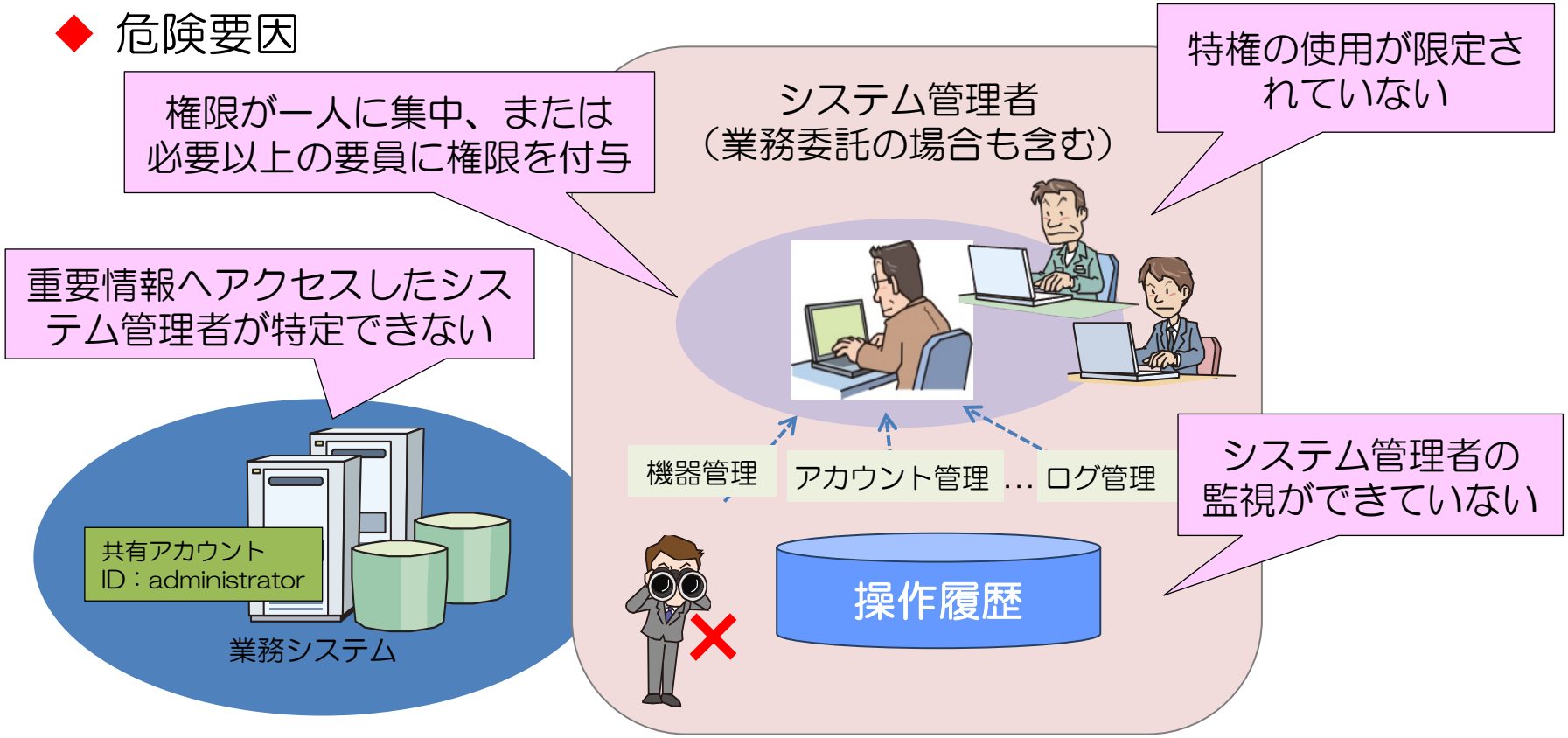
- 入館証の回収、貸出機器の返却
- 速やかな情報システムのアカウント削除
  - ✓ アカウント削除漏れがないよう、人事システムと連携して実施することが望ましい。
- 退職後に重要情報が競合他社に渡らないよう秘密保持契約（誓約書を含む）を結ぶことが望ましい。さらに、非常に重要な情報を扱っていた従業員が競合相手に転職しないよう、協業避止義務契約を締結する。ただし、職業選択の自由を侵害しないよう適切な範囲に設定する必要がある。



ケース2　システム管理者による不正行為

ポイント：　適切な権限管理とシステム管理者の監視

◆ 危険要因

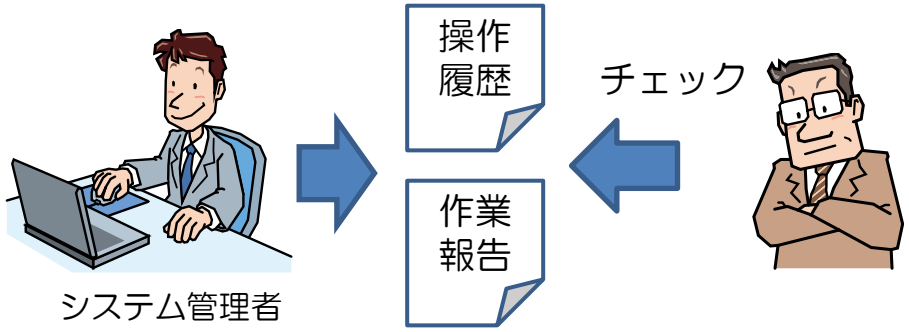


システム管理者は多くの権限を持つため、不正行為を働こうとすると重大な事故を引き起こしかねない。

①適切な権限管理

（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。

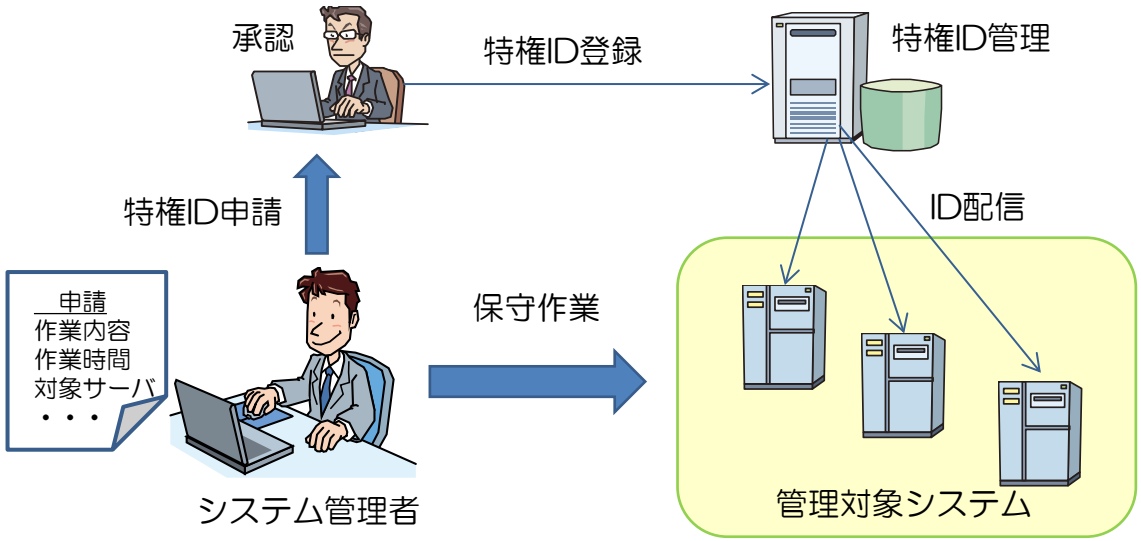


システム管理者による不正行為への対策

①適切な権限管理

- 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

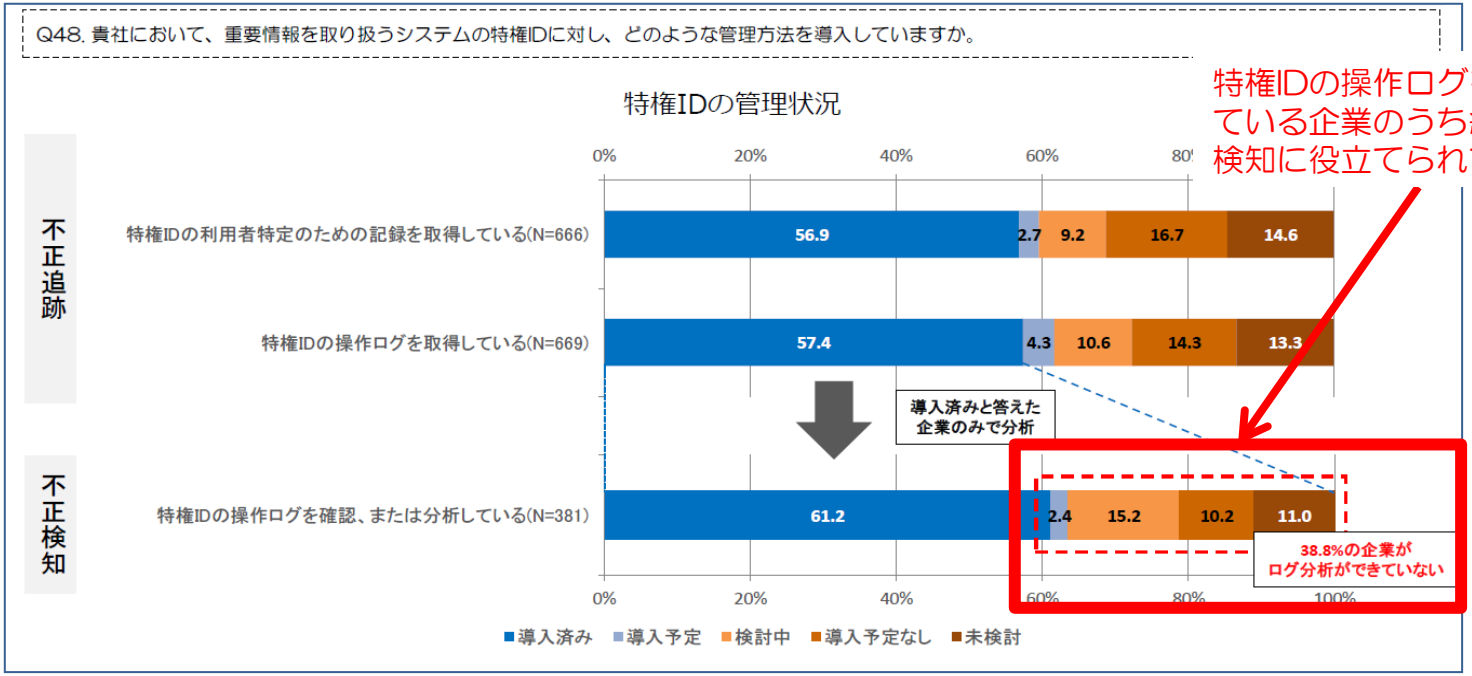
- 特権を用いた操作を限定する。
  - ✓ 一時的な特権IDの払い出しや、作業の申請・承認プロセスの厳密化等特権を必要とする作業以外はできるだけ操作できないようにする。



システム管理者による不正行為への対策

②システム管理者の監視

- システム管理者のアクセス履歴や操作履歴を記録し、システム管理者意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
- 抑止の観点から、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

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

◆ 危険要因

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。

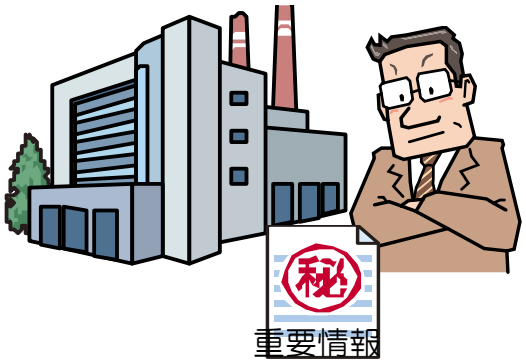
重要情報の安全管理に必要な事項が契約に盛り込まれていない

セキュリティ管理策
サービスレベル
ログの提供　等

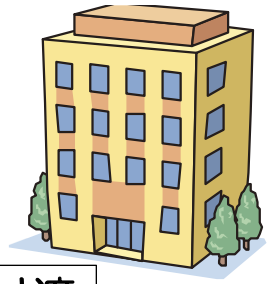
クラウドサービス

第三者が提供するサービス利用

委託元



業務委託



委託先

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

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。

①重要情報の取扱いに関する委託先管理

- 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

委託先による情報漏えい等への対策

①重要情報の取扱いに関する委託先管理

委託元

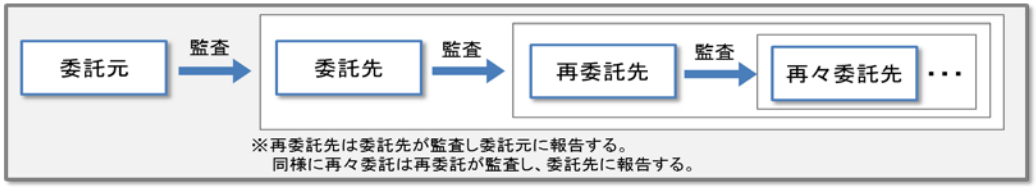
- 委託前、委託先の体制や規定の点検等により、重要情報の取扱いを確認する。
- 委託契約では、必要かつ適切なセキュリティ対策ついて、委託先と同意した内容を具体化し委託契約を締結する。
- 契約期間中、契約内容について定期・不定期に遵守されていることを確認する。
- 再委託時、委託元への事前承認を必要とする。また、契約期間中の確認や監査の実施体制を明確にする。

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

想定例①委託先を通じて監査を実施する



想定例②：必要に応じて自らが監査を実施する

委託先、再委託先に対する監査体制

委託先による情報漏えい等への対策

②契約への安全管理事項の盛り込み

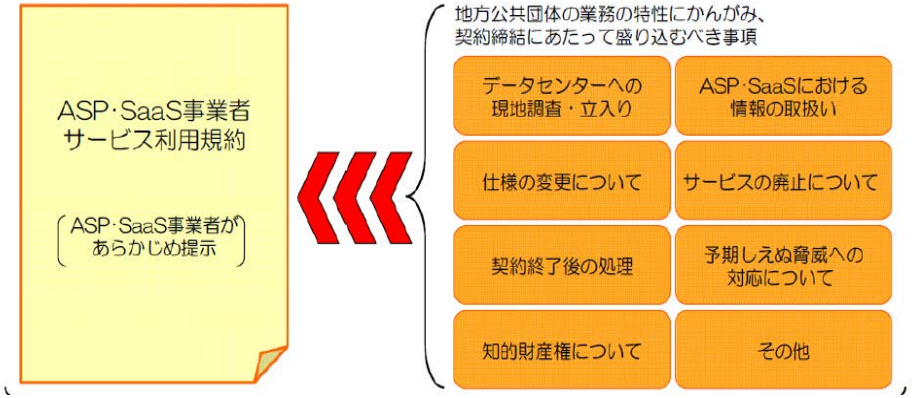
- 第三者が提供するサービスを利用する場合は、セキュリティ管理策、サービスレベル、ログの提供等を事前に確認し合意する。
  - ✓ クラウドサービスを利用する目的はなにか。（どのようなデータを預けるのか）
  - ✓ セキュリティ管理策が、重要情報を安全に管理するため十分か。
  - ✓ サービスレベル及び管理上の要求事項が、事業継続において適切か。
  - ✓ 内部不正が発生した際に、ログが提供されるか。

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

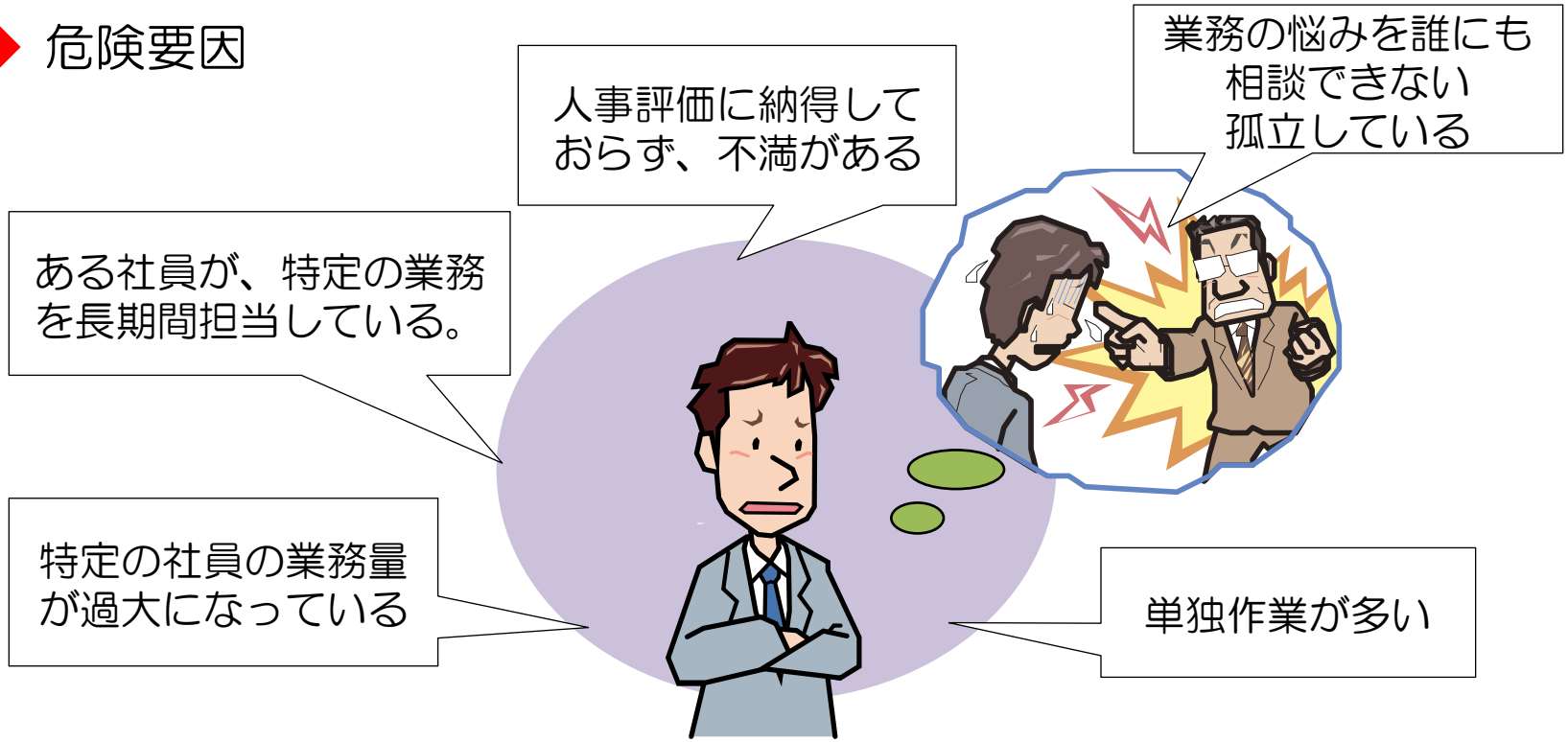


（出典）特定非営利活動法人 ASP・SaaS・クラウドコンソーシアム（ASPIC）:
クラウド・利用者の必要知識と関連ガイドライン等について

ケース4　職場環境に起因する不正行為

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

◆ 危険要因



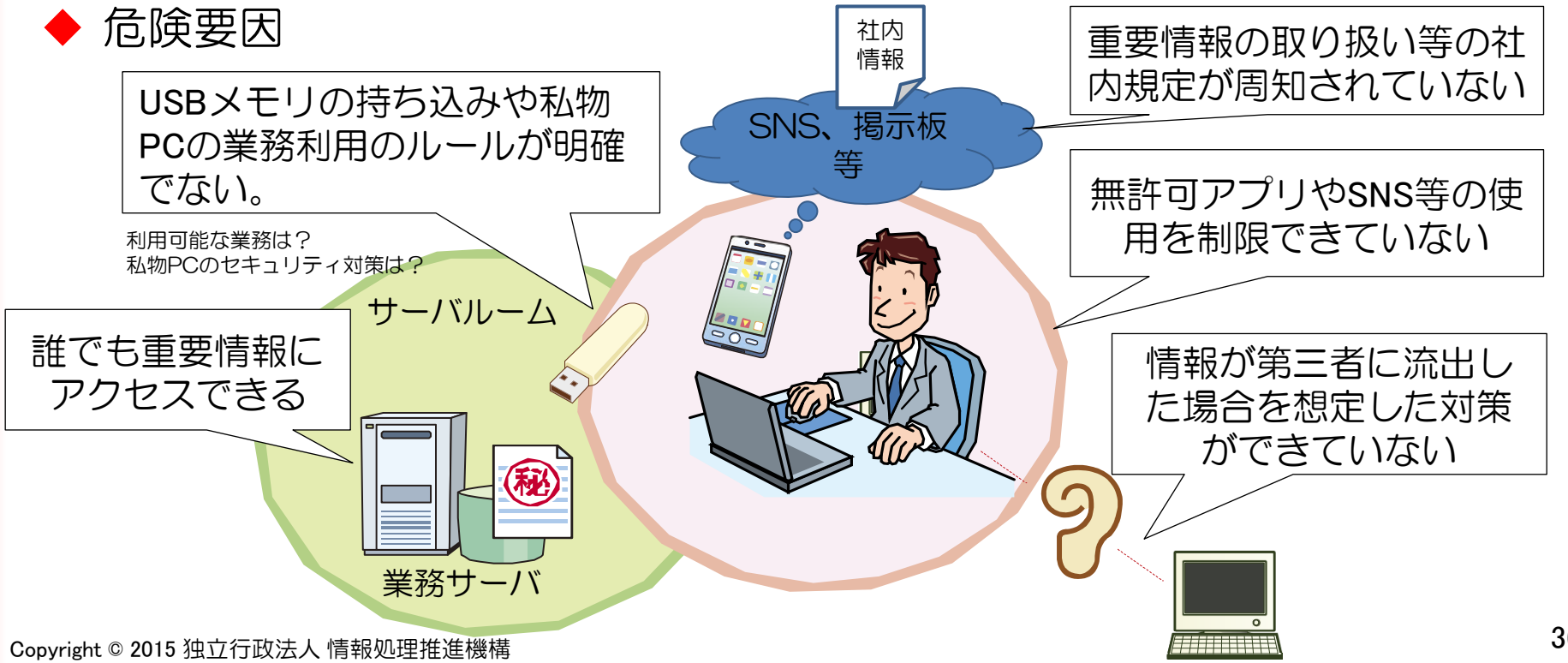
従業員に不正行為を踏みとどまらせる対策として、職場環境の整備が重要な役割を果たす。

ケース5　従業員による悪意のない不正行為

ポイント：　教育による周知徹底と情報漏えい対策

- 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

①教育による周知徹底

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。

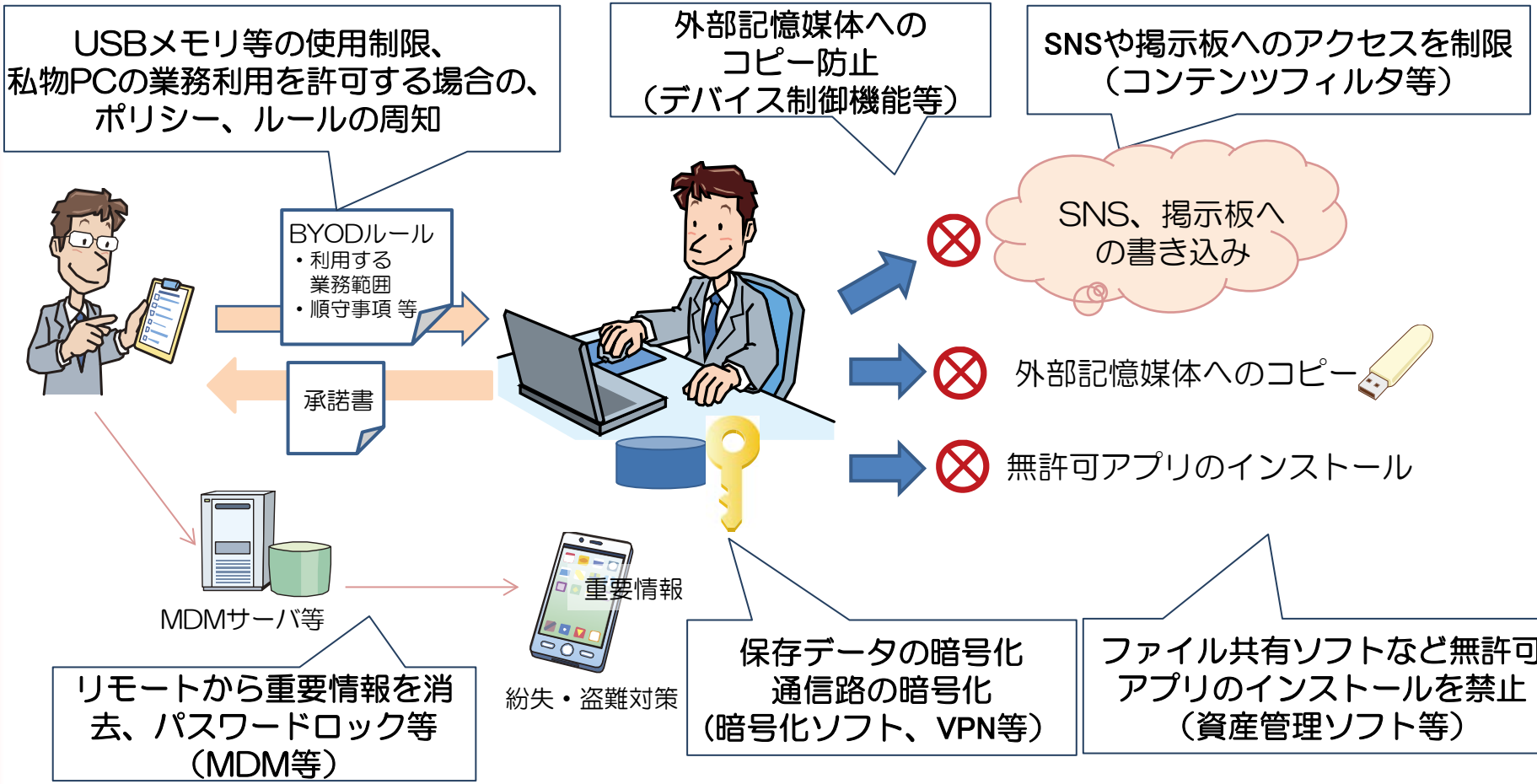
教育の内容

- 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

従業員による悪意のない不正行為への対策

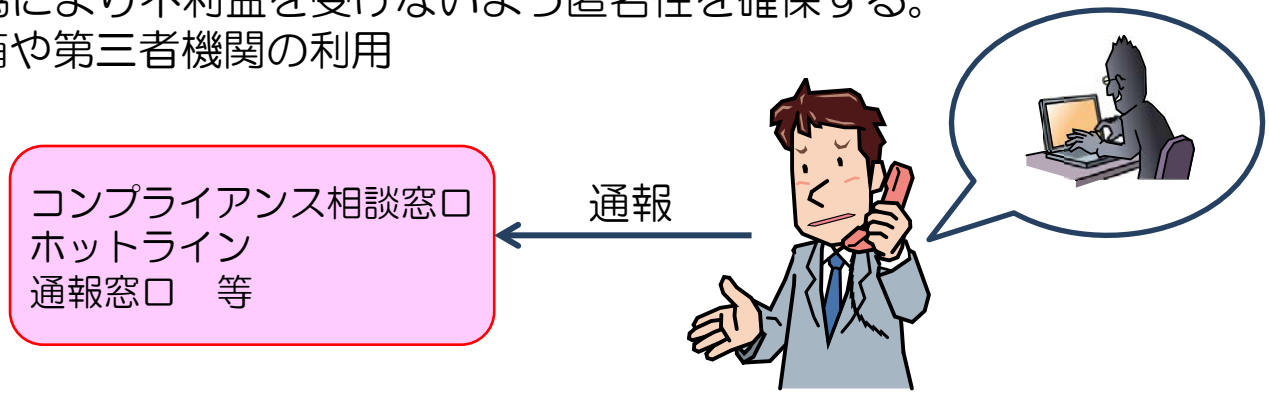
②情報漏えい対策



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。

- 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。
(自社だけでなく、関係者(顧客、取引先など)の被害も最小限に抑える)

４．IPA「組織における内部不正防止ガイドライン」の紹介

内部不正防止ガイドライン（2014.9改訂）

- 内部不正を防止するための環境整備に役立てて頂くためのガイドライン
- 防止対策だけでなく、発生してしまった際の早期発見・拡大防止にも対応
- 2014年9月改訂版では、経営者責任の明確化、必要な人材の確保など、経営者主導が不可欠な取組みを新たに追加。以下の３点を強調すべく加筆した。
  - ✓ 経営層によるリーダーシップの強化
  - ✓ 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

【目次】

「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20条関連）
    - 従業者の監督（法21条関連）
    - 委託先の監督（法22条関連）

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。

改訂前

➢ 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」

「営業秘密管理」の全部改訂

「営業秘密」の定義（不正競争防止法第2条第6項）
「秘密として管理されている[①秘密管理性]生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報[②有用性]であって、公然と知られていないもの[③非公知性]をいう」

①秘密管理性

秘密管理性要件が満たされるためには、**営業秘密保有企業の秘密管理意思**が**秘密管理措置**によって従業員等に対して明確に示され、当該秘密管理意思に対する**従業員等の認識可能性が確保される必要**がある。
具体的に必要な秘密管理措置の内容・程度は、企業の規模、業態、従業員の職務、情報の性質その他の事情の如何によって異なるものであり、企業における営業秘密の管理単位（本指針13ページ参照）における**従業員がそれを一般的に、かつ容易に認識できる程度のものである必要がある。**

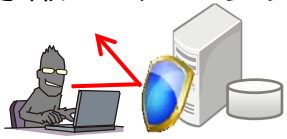
営業秘密管理指針
（2015.1.28 全部改訂）

具体的な管理策

営業秘密管理マニュアル
（2015.春を目標）

営業秘密管理

未然防止のための情報セキュリティ対策



内部不正防止ガイドラインの位置づけ

- 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

対応項目無し

内部不正防止ガイドラインの特徴①
１０の観点での３０の対策項目

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) 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）	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

内部不正防止ガイドラインの特徴②
チェックシートで現状を把握

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

組織における内部不正防止ガイドライン／付録Ⅱ：内部不正チェックシート（一部抜粋）

※□：主担当／実施部門（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）
※[ ]：サポート／実施補助・確認部門（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）

内容	チェック欄				
基本方針					
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）			
「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）			
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
物理的管理					
個人のモバイル機器および記録媒体の業務利用および持込を制限していますか？	[ ]	□			
技術・運用管理					
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？	□	[ ]			[ ]
人的管理					
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およ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？	□		[ ]	[ ]	
組織の管理					
内部不正対策の項目を抽出し、定期的および不定期に確認（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？	□	[ ]			

内部不正防止ガイドラインの特徴③
ソリューションガイドを活用した具体策の検討

①対策の指針、ポイントを理解する
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

②具体的な実施策を立案する
製品・ソリューションの利用等を検討

組織における内部不正防止ガイドライン

JNSA※内部不正対策ソリューションガイド

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ソリューションガイド（オンライン版）
内部不正防止・抑止サービス

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。

※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

最後に

① **内部不正にはトップダウンで組織横断の取り組みを！**
経営者は、経営戦略に則って内部不正対策の方向づけを行うとともに、対策実施のために必要な人材や予算等のリソース確保を！

② **職場環境を見直し、内部不正が発生しにくい環境を！**
ポイントは、「公正な人事評価」、「適切な労働環境」、「良好なコミュニケーション」。たとえ“穴”を見つけても不正行為の実行を思い止まらせるような根本的な防止対策を。

③ **ITの技術進歩や新たな脅威等に応じ、継続的に対策の見直しを！**
新しいITの採用やインフラのバージョンアップ時に要注意。導入済みの製品やソリューションも確認を！

③ **ログの監視で早期発見を！抑止効果も。**
ログを記録するだけでなく、定期監査や有効なチェックができていますか？ログのチェックで不正行為の早期発見を！抑止効果も。

参考情報

1. IPA:内部不正の防止には、経営層を含めた組織横断的防御を！（特設ページ）
   http://www.ipa.go.jp/security/insider/index.html
2. 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
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/20150128hontai.pdf
6. 経済産業省: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/2013/03/20140314004/20140314004.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

参考
「状況的犯罪予防」理論における犯罪予防策

1. **犯行を難しくする**
   技術的な対策を強化することで犯罪行為を難しくする
2. **捕まるリスクを高める**
   管理や監視を強化することで捕まるリスクを高める
3. **犯行の見返りを減らす**
   犯行を難しくするための技術的対策によって、犯行者から適切な目標物を遠ざけることや隠すことが困難な場合に適用
4. **犯行の挑発を減らす**
   外部からの挑発による犯罪行為を抑止
5. **犯罪を容認する言い訳を許さない**
   犯行者による自らの行為の正当化理由を排除する

※状況的犯罪予防：犯罪が発生する物的な環境や状況に着目した犯罪予防の手法