IPA Better Life with IT

組織における内部不正防止対策

独立行政法人 情報処理推進機構
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

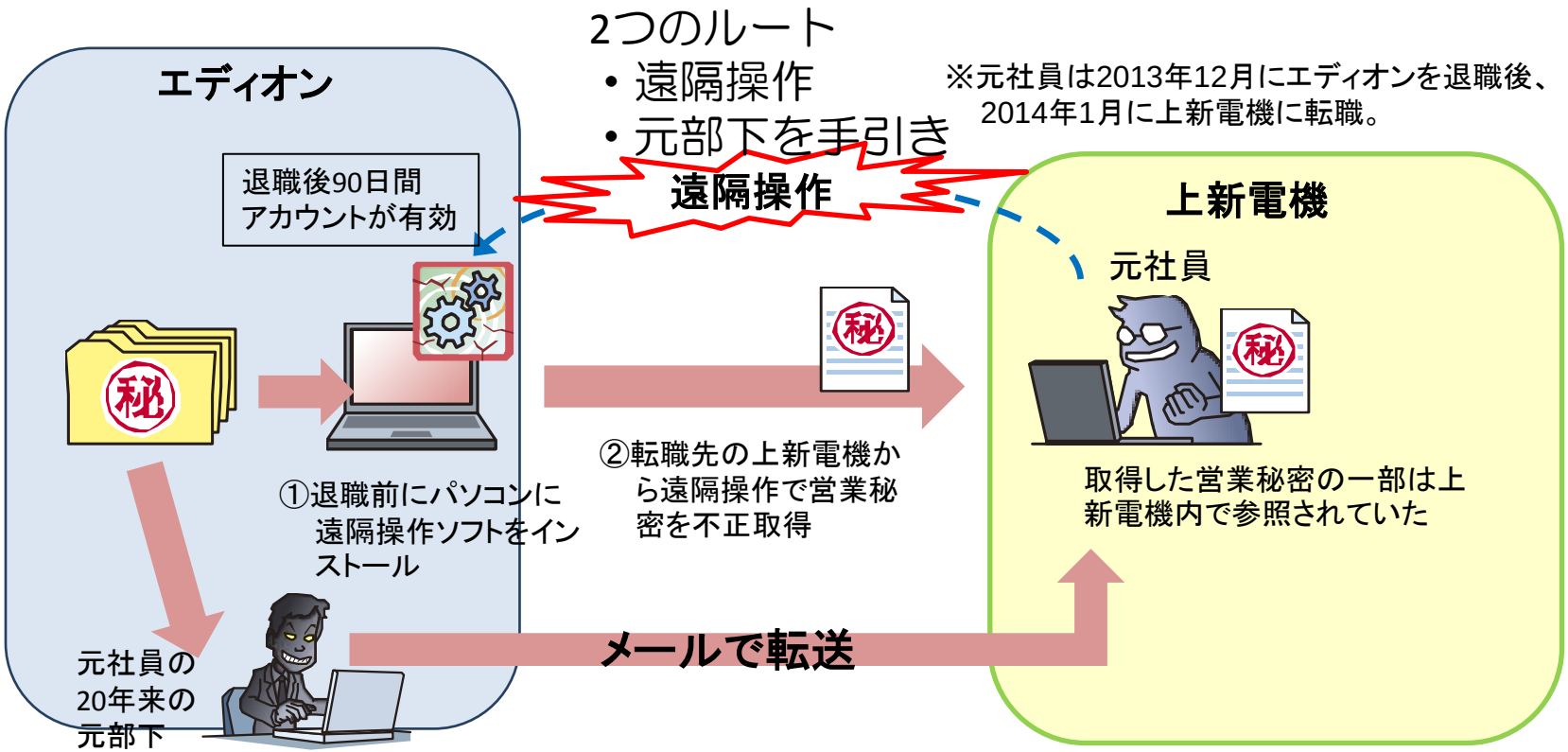
1. 内部不正インシデントの状況
   - 内部不正事例
   - 内部不正の状況
   - 内部不正の特徴
2. 内部不正を防ぐ
   - 内部不正者への対策方針
   - トップの関与・体制整備
   - 内部者対策
   - 内部不正に強い組織の構築
3. ガイドライン
   - 不正競争防止法（営業秘密保護）、内部不正防止ガイドライン

1(1)　相次ぐ内部不正事件

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の取得したとして**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	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	金融関連の保守管理業務を委託している会社の元社員が、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　元社員による営業秘密不正取得
～外部攻撃（遠隔操作）と内部者不正の組み合わせ～

2015年1月、家電量販店エディオンの元社員が退職前に事務所のパソコンに遠隔操作ソフトをインストールし、転職先の上新電機の業務用パソコンから遠隔操作ソフトを通じて不正に営業秘密にあたる情報を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。



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。

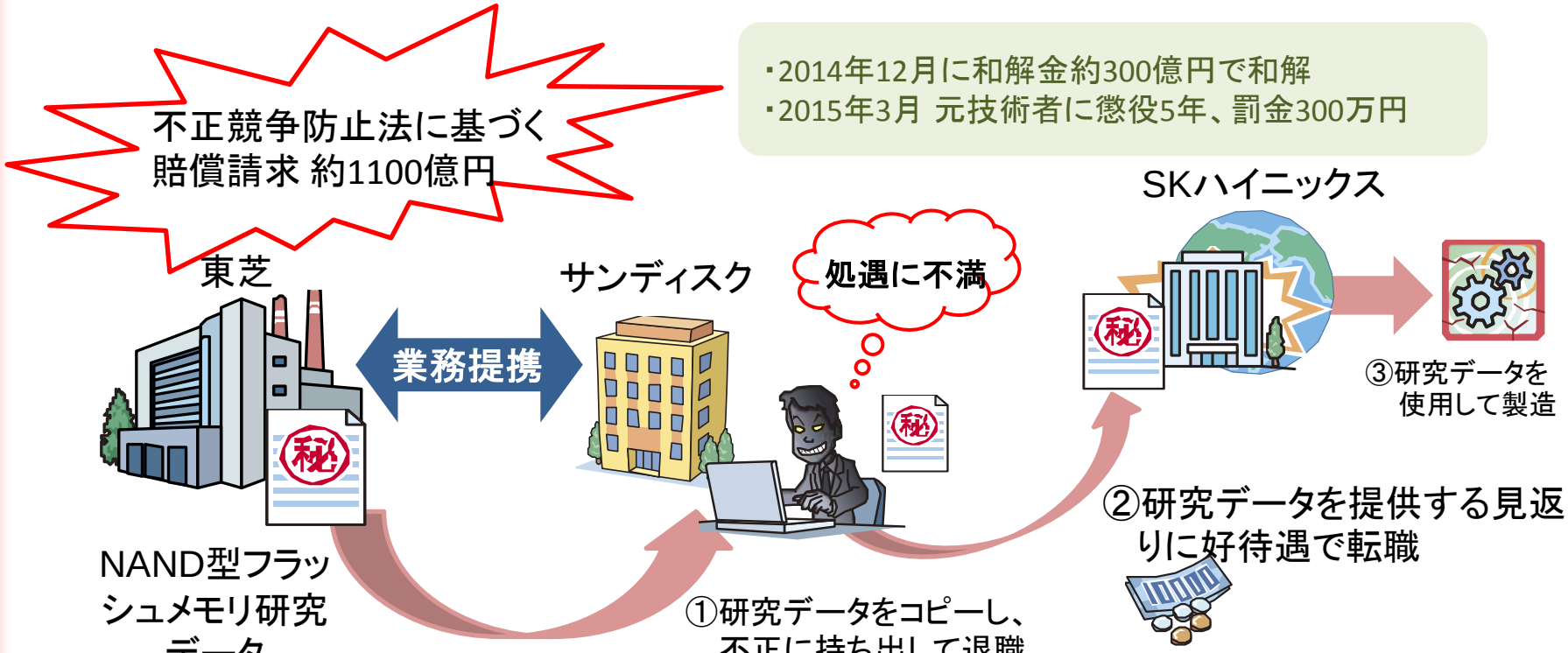
2014年9月25日時点で報道より得られた情報を元に記載

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

事例3　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。



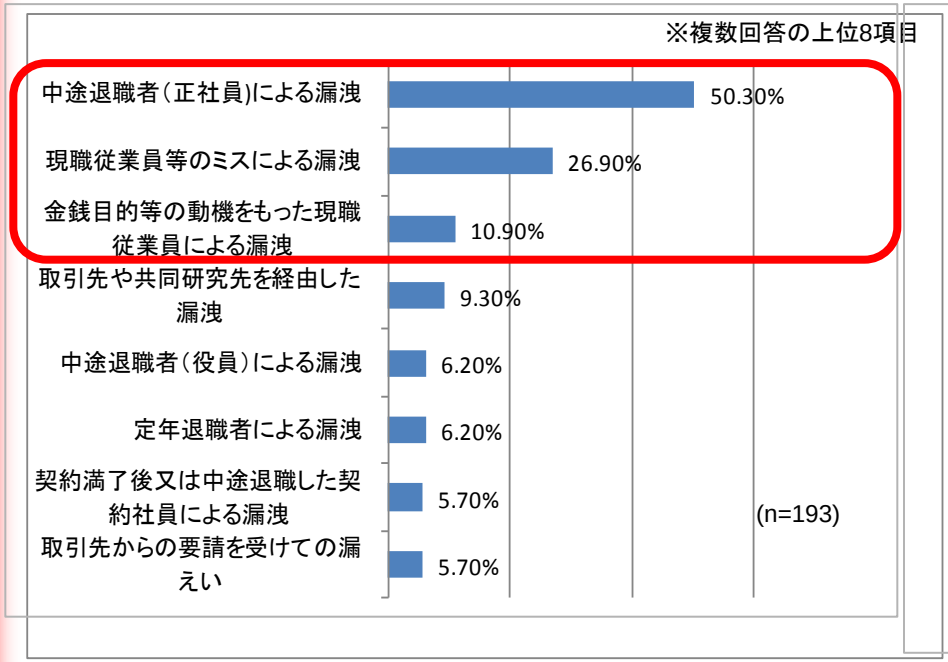
(2)内部不正の状況

- インシデントの発生源として最も多いと挙げられたのは現従業員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
- 半数以上の企業が「内部犯行による情報漏洩リスク」を重視　[JIPDEC:企業IT利活用動向調査2015]
- 情報漏えいの“敵”は社内にあり「内部犯行」「うっかりミス」に懸念　[TechTargetジャパン:企業の情報漏えい対策に関する読者調査]
- 漏洩の疑い、過去5年間で企業の1割が経験 ～ 漏洩防止への取り組みは5割にとどまる～　[帝国データバンク]
- 営業秘密の流出者は、中途退職者が最も多く、流出先は国内競合他社が多い　[METI:「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）]

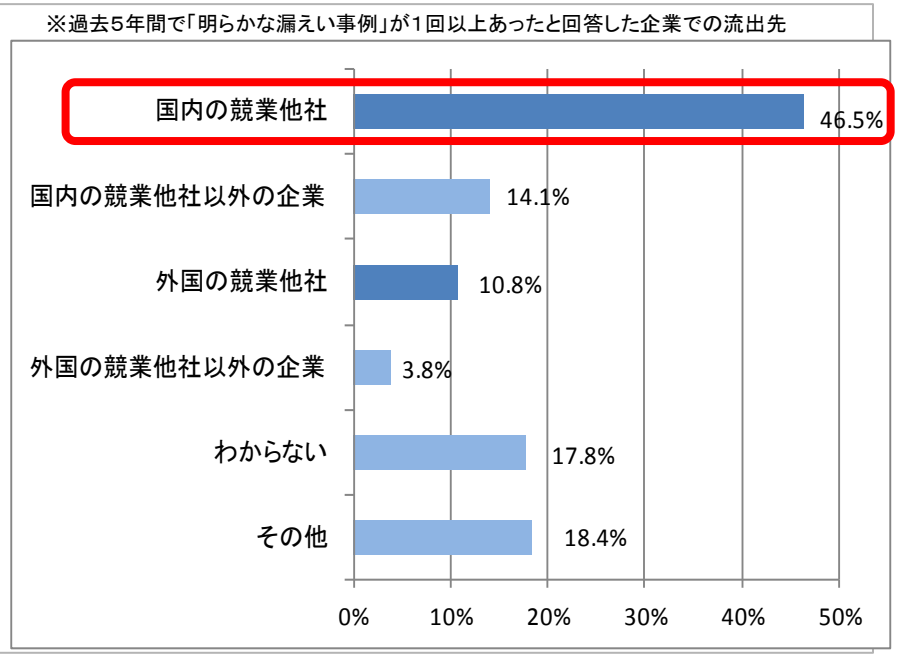
(2)内部不正の状況
内部者による技術情報流出の実態

- 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い
- 流出ルートは、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

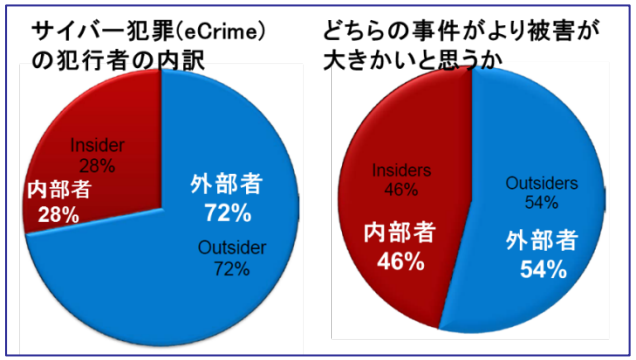


（出典）経済産業省:「人材を通じた技術流出に関する調査研究報告書（2013年3月）」

(2) 内部不正の状況
被害額と平均解決日数

- サイバー攻撃の年間平均被害額では内部不正が最も高い
  - 内部不正　約21.4万ドル　[2014 Global Report on the Cost of Cyber Crime]
  - DoS攻撃　約16.6万ドル,Webベースの攻撃　約11.6万ドル

- サイバー犯罪の犯行者の内訳は、外部者が72%であるが、被害の大きさは、外部は54%、内部者によるものは46%と拮抗 [US Cyber Crime Survey2014]

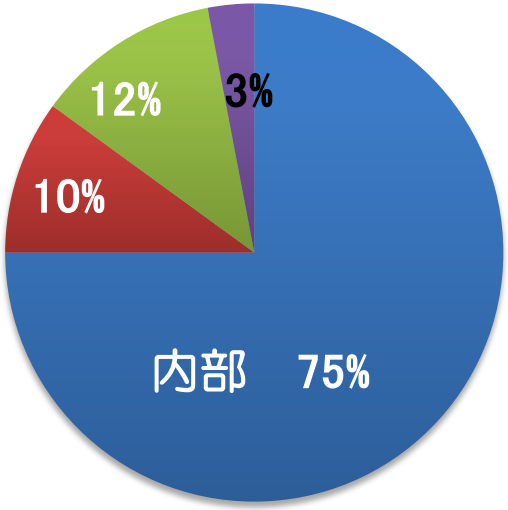


- サイバー攻撃の解決に要する平均日数は、内部不正が最長で、58.5日、最短はウィルス/ワーム/トロイの木馬で1.2日

項目	海外（7カ国275社）	日本（31社）
サイバー攻撃の平均解決日数（解決にかかる1日当たりの平均費用）	31日（約2万ドル/日	25日（約2百万/日）
内部不正の平均解決日数	58.5日	39.5日

(2)内部不正の状況：75%が法的措置を取らず その理由は被害の状況を十分把握できなかったから

2014 US State of Cybercrime Survey



- 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）

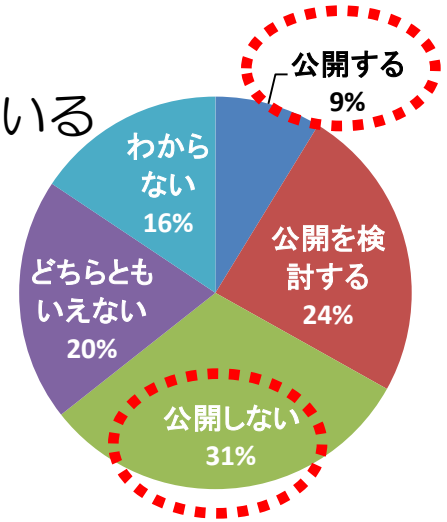
サイバー犯罪に対し法的措置を取らなかった理由	2013 %	2012 %	2011 %
被害の程度が起訴を保証するのに十分でない	34	36	40
起訴するのに、証拠がない／情報が不足している	36	36	34
犯罪を犯した個人を特定できなかった	37	32	37
ネガティブな公開（評判）を懸念	12	9	14
（自社の？）信頼を懸念	8	7	9
競合他社がこの事故で優位になることを懸念	7	6	7
法執行機関より事前にネガティブな回答を受けた	8	5	6
この事故を報告できるかわからない	6	5	4
法執行機関より、事故が国家安全保障に関連するとされた	3	4	4
その他	8	12	11
わ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

(2)内部不正の状況
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）

(3)内部不正の特徴のまとめ

- 不正者（内部者）
  - 職員、退職者、委託先等職員

  →権限を付与された者の内部不正を防ぐ
- 動機　→　抑止対策
  - 金銭や転職
  - 心理的なもの（恨み、あてつけ等）
- 悪意の無い不正

  →守れるルール
- 組織　→　インセンティブ
  - 自ら発見することが少ない、公表しない

2　内部不正を防ぐ：内部不正者への対策方針

- 内部不正発生に対する環境整備
  - 動機：犯罪心理学を援用（抑止効果）
    - 不正のトライアングル
    - 状況的犯罪防止
  - 職場環境の整備

2.　内部不正者への対策：動機を抑止

不正のトライアングル

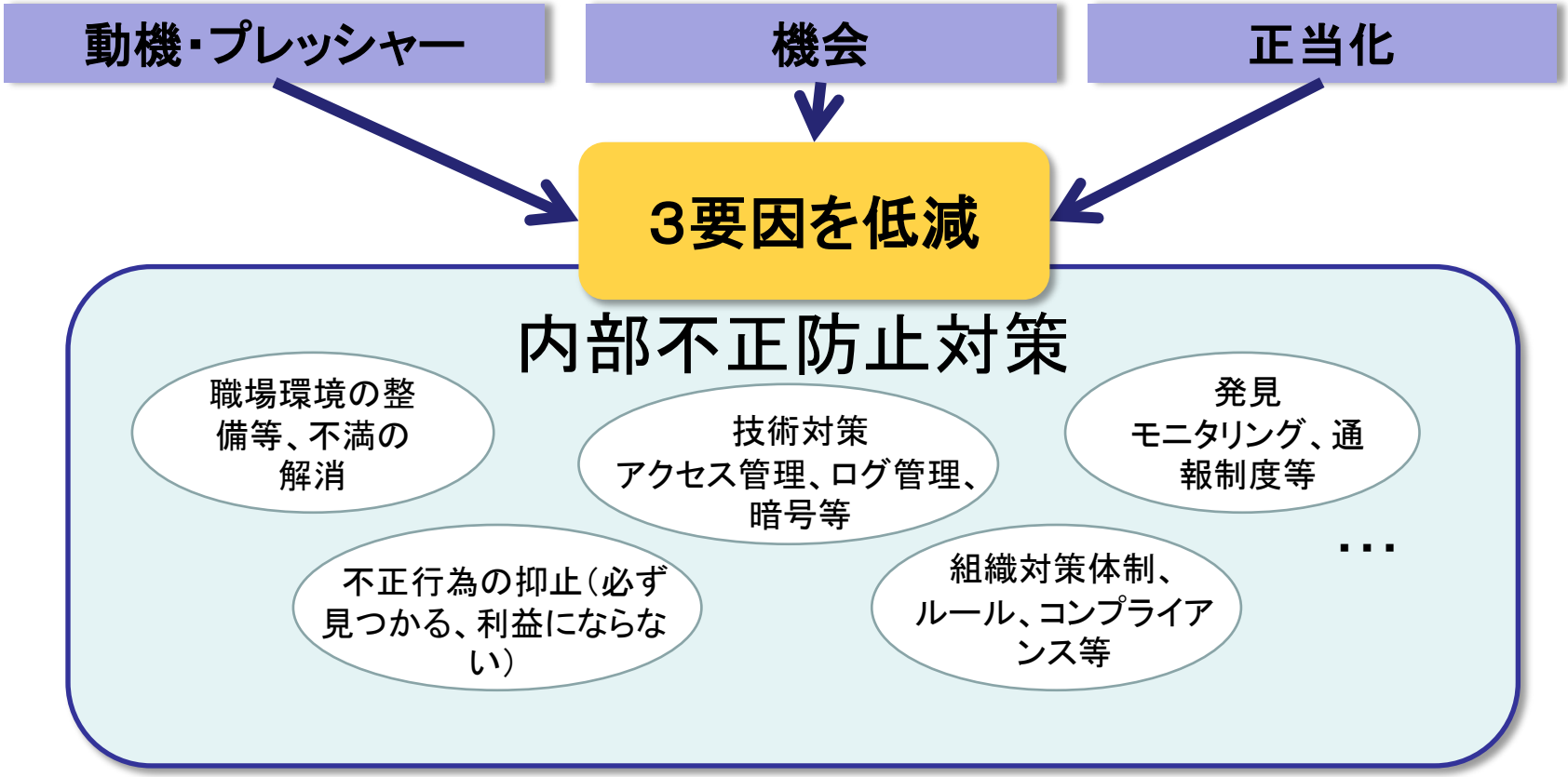
- 「動機・プレッシャー」「機会」「正当化」の３要因が揃った時に発生

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。
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。

※ドナルド・R・クレッシー（米国の組織犯罪研究者）による

2.　内部不正者への対策
内部不正防止対策は３要因の低減

- 組織の対策は、「動機・プレッシャー」と「機会」の低減を図る。



2.内部不正者への対策: 状況的犯罪予防の考え

IPA

都市空間における犯罪予防の理論。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で、犯罪機会・動機を低減する犯罪予防策。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む（Cornish & Clarke,2003）

1. **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
2. **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
3. **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
4. **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

「機会」の低減

5. **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

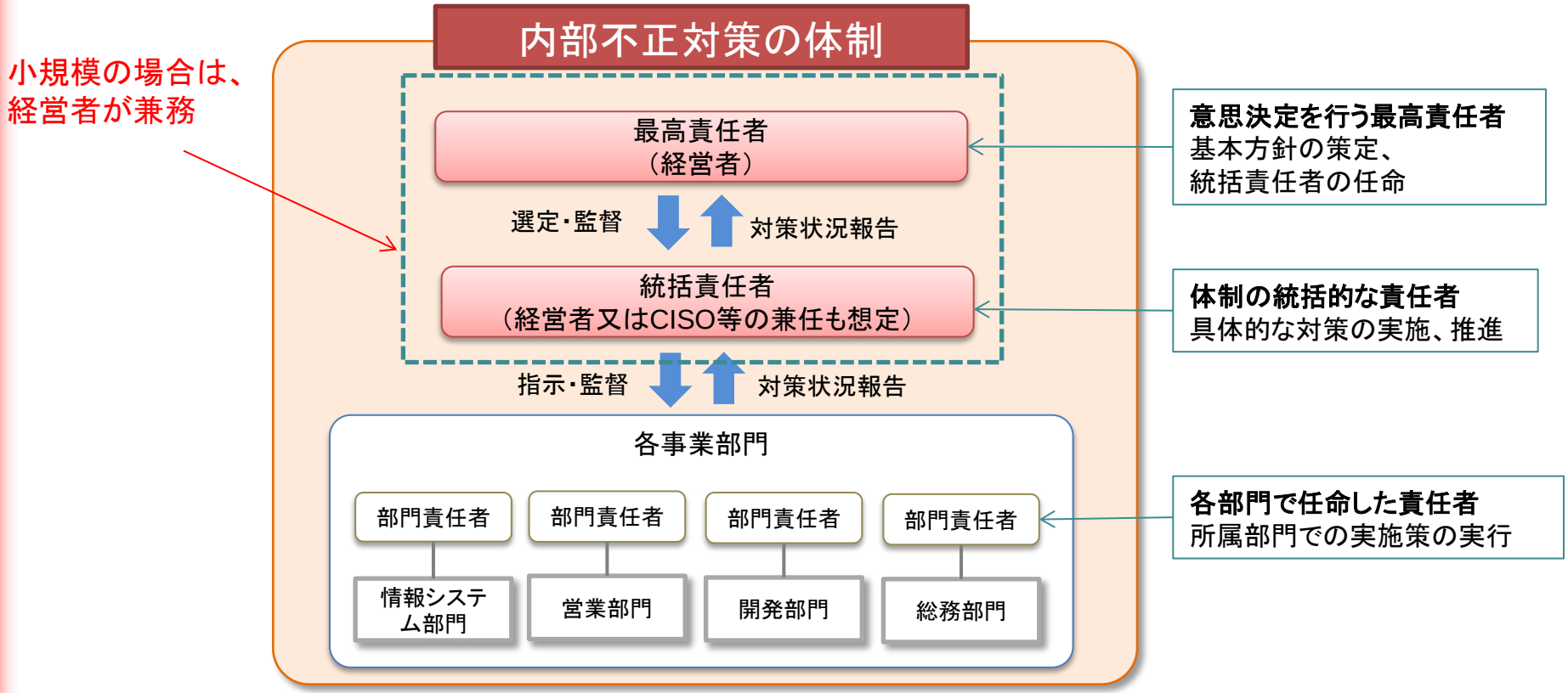
正当化の低減

3. 内部不正対策

1. トップの関与
2. これだけはやってほしい基本対策
3. 内部者（退職者、管理者）の管理
4. 委託先の管理
5. 職場環境の整備
6. 早期発見
7. 悪意のない情報漏えい
8. 事後対応

3.1　トップの関与
内部不正対策の管理体制

- 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



3.2　これだけはやってほしい基本対策　1/2

- 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）

※営業秘密として不正競争防止法の法的保護を受けるためにも重要

技術やノウハウ等の情報が「営業秘密」として不正競争防止法で保護されるためには、秘密管理性、有用性、非公知性の３要件を満たすことが必要。

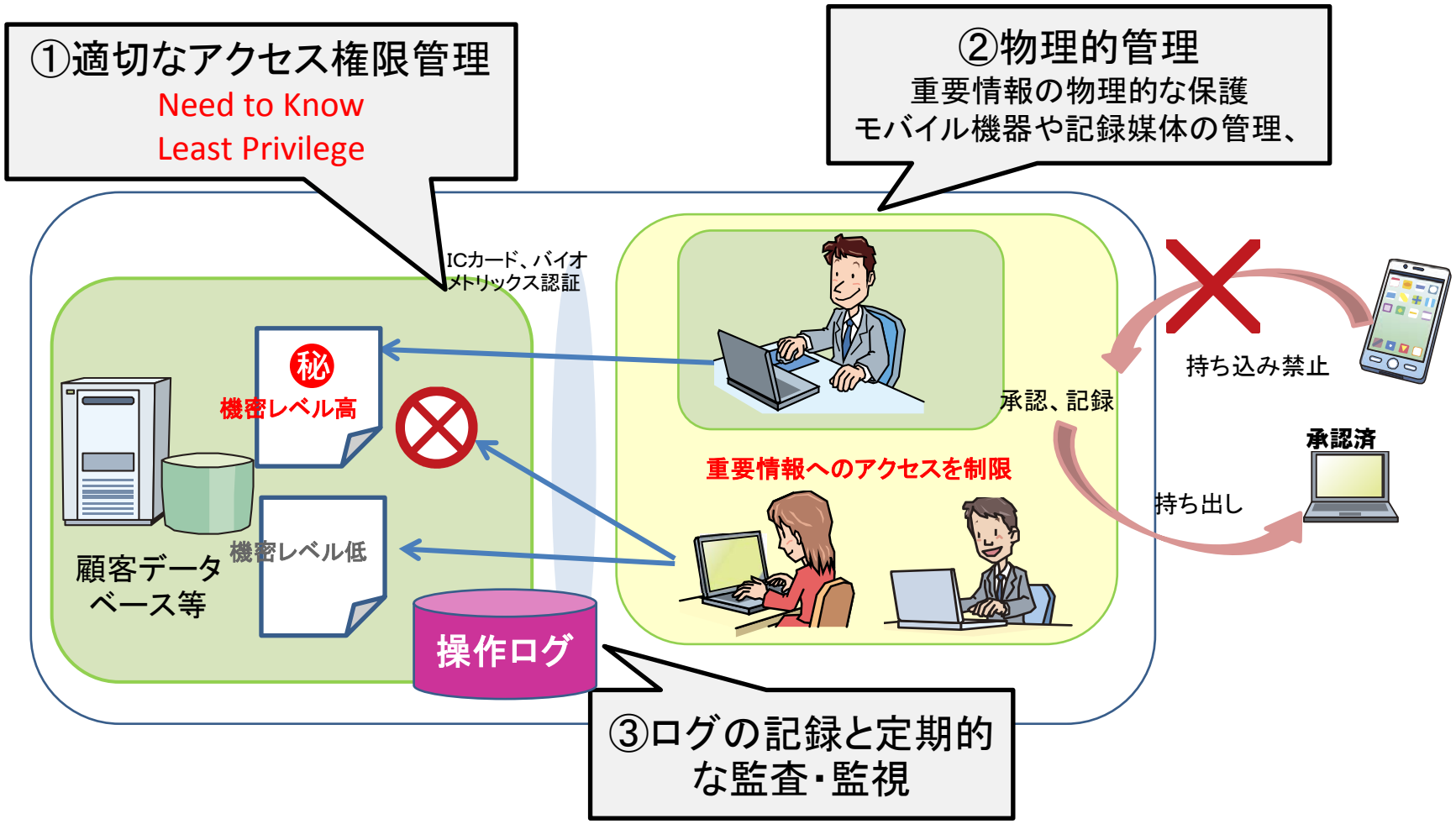
営業秘密管理指針

秘密管理性の要件の趣旨は、なにが営業秘密かを社員に明らかにすることで、不足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年1月　全部改訂

3.2 これだけはやってほしい基本対策 2/2



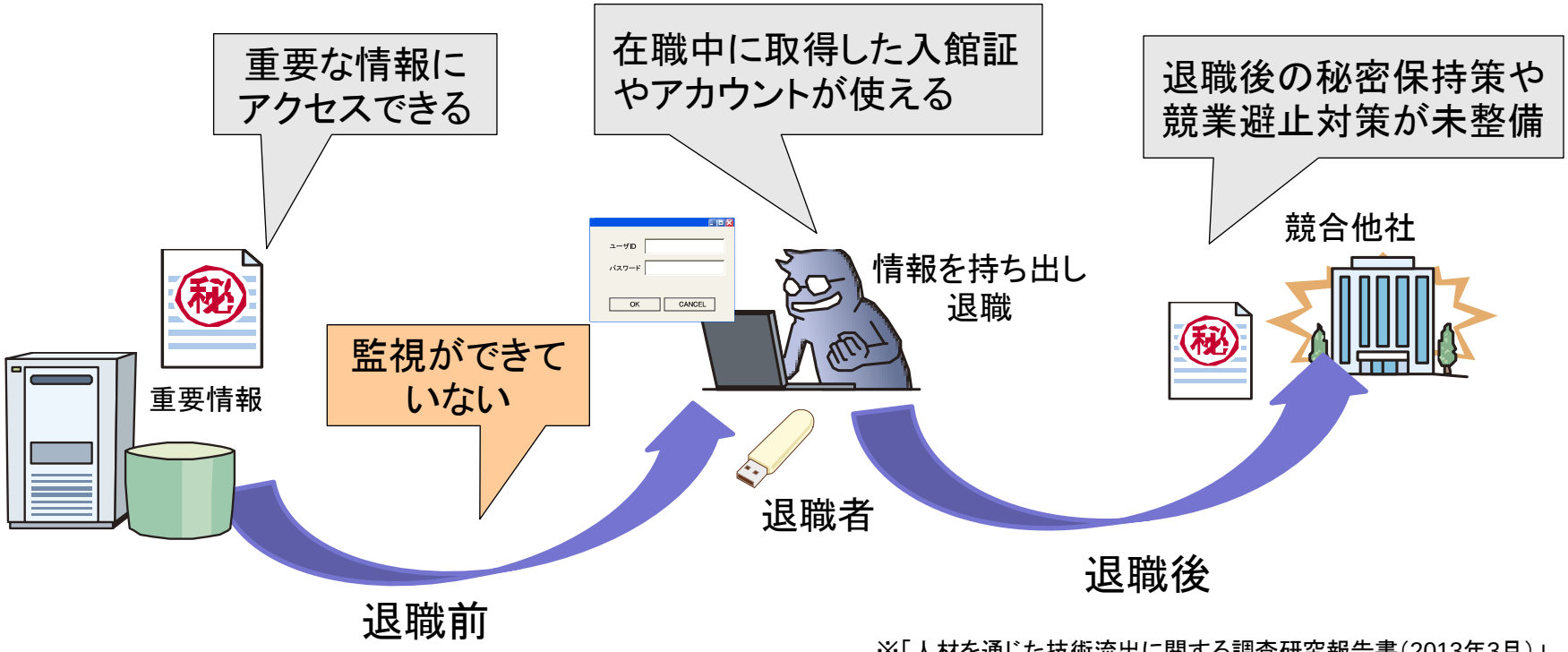
④内部不正対策の継続した見直し、改善

3.3　内部者対策：退職者

対策ポイント：　①退職前の監視強化と②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

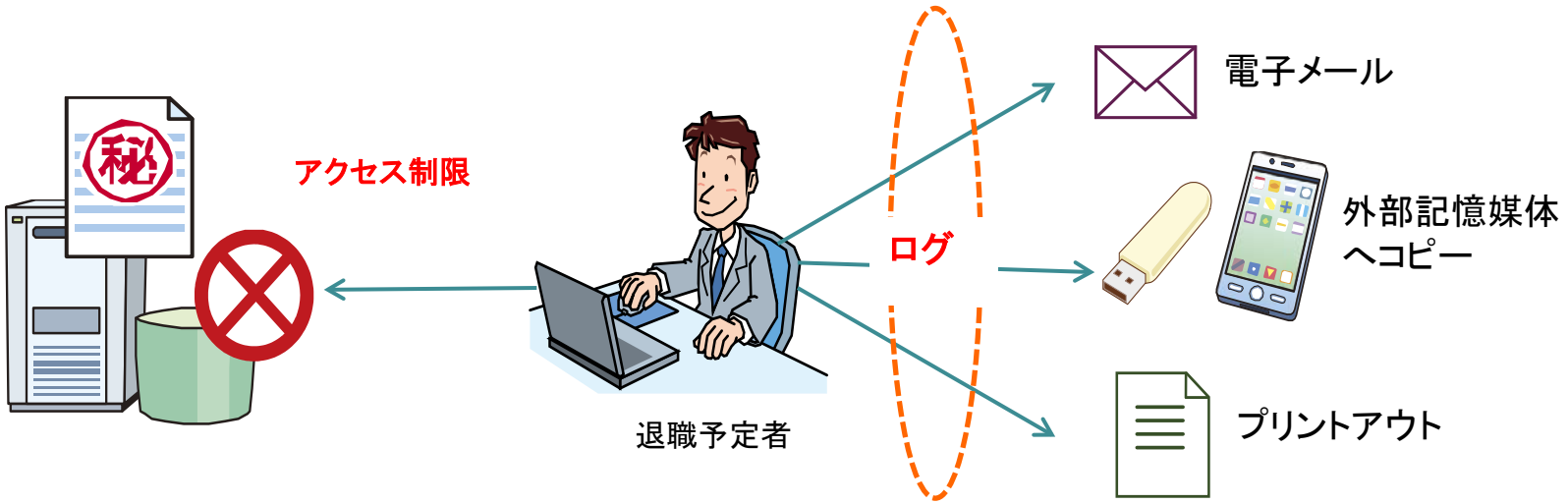


※「人材を通じた技術流出に関する調査研究報告書（2013年3月）」

3.3　内部者対策：退職者
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。

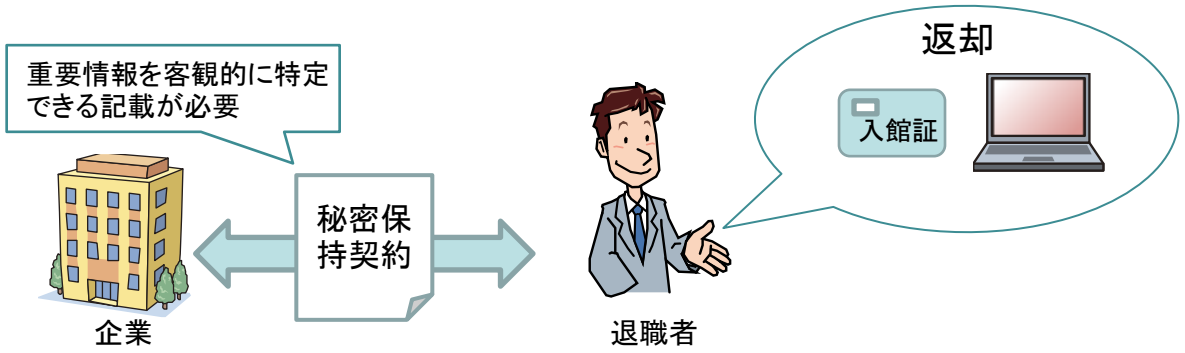


3.3　内部者対策：退職者
②退職時の手続き

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、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。

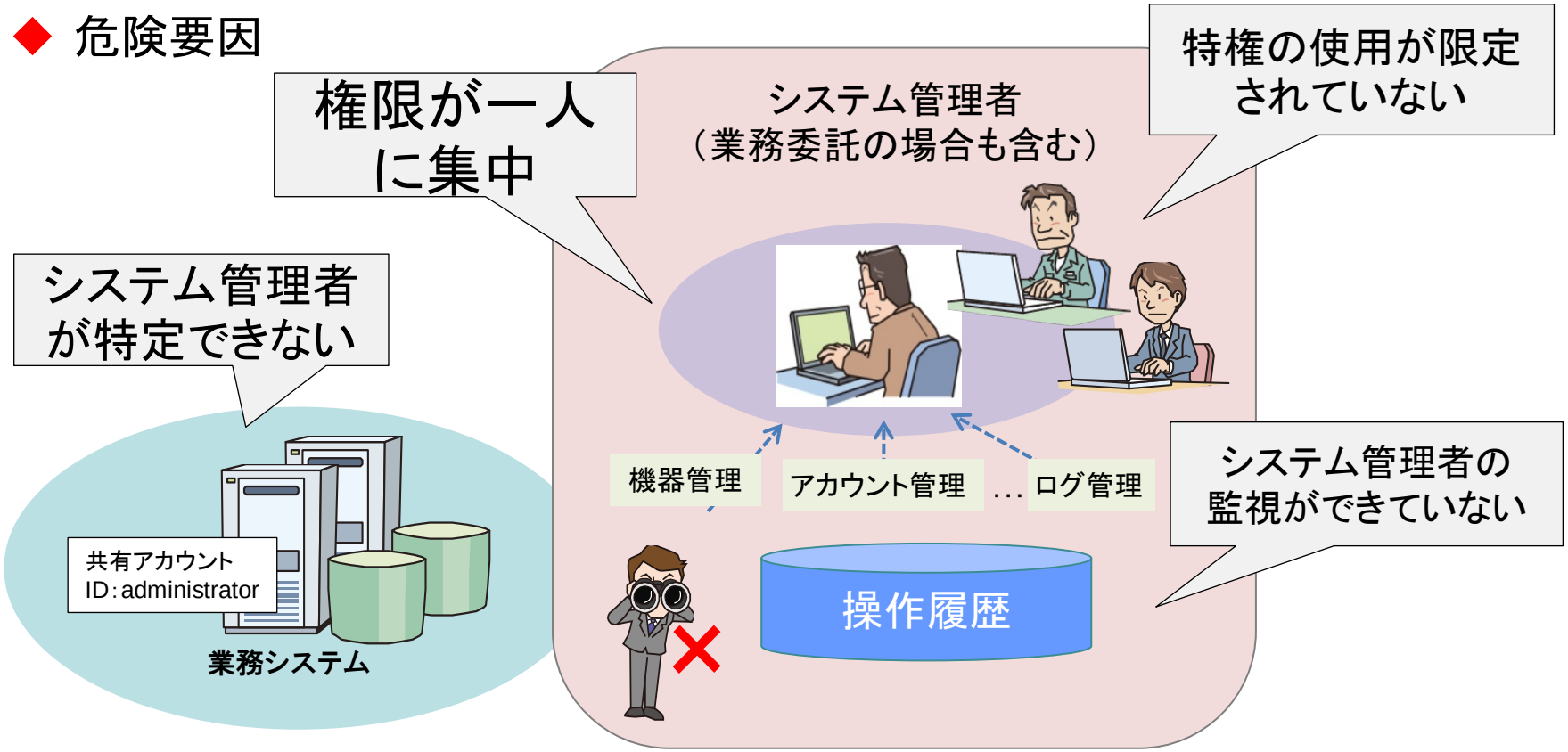


3.3　内部者対策：システム管理者

対策ポイント：　①適切な権限管理と②システム管理者の監視

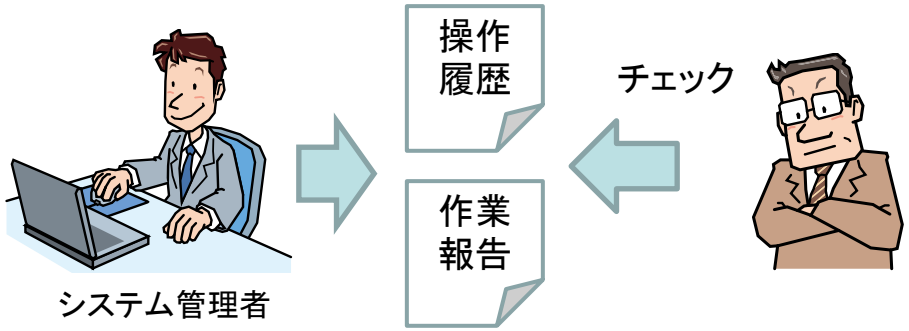
システム管理者は多くの権限を持つため、不正行為を働こうとすると重大な事故を引き起こしかねない。

◆ 危険要因



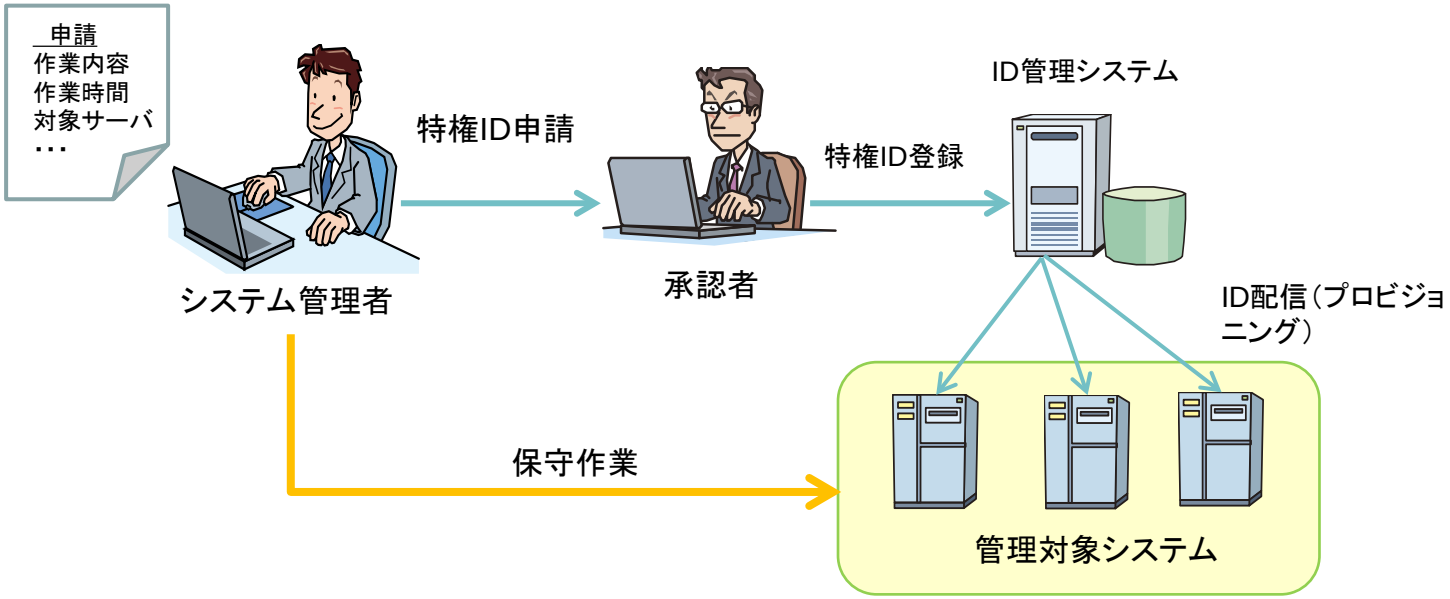
3.3　内部者対策：システム管理者 ①適切な権限管理（ルール・運用）

- 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。
- 付与する権限は必要最小限とする。
  - ✓ 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する。また、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期間に限って行う。
  - ✓ アクセス権限は定期的に見直す。
- 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。



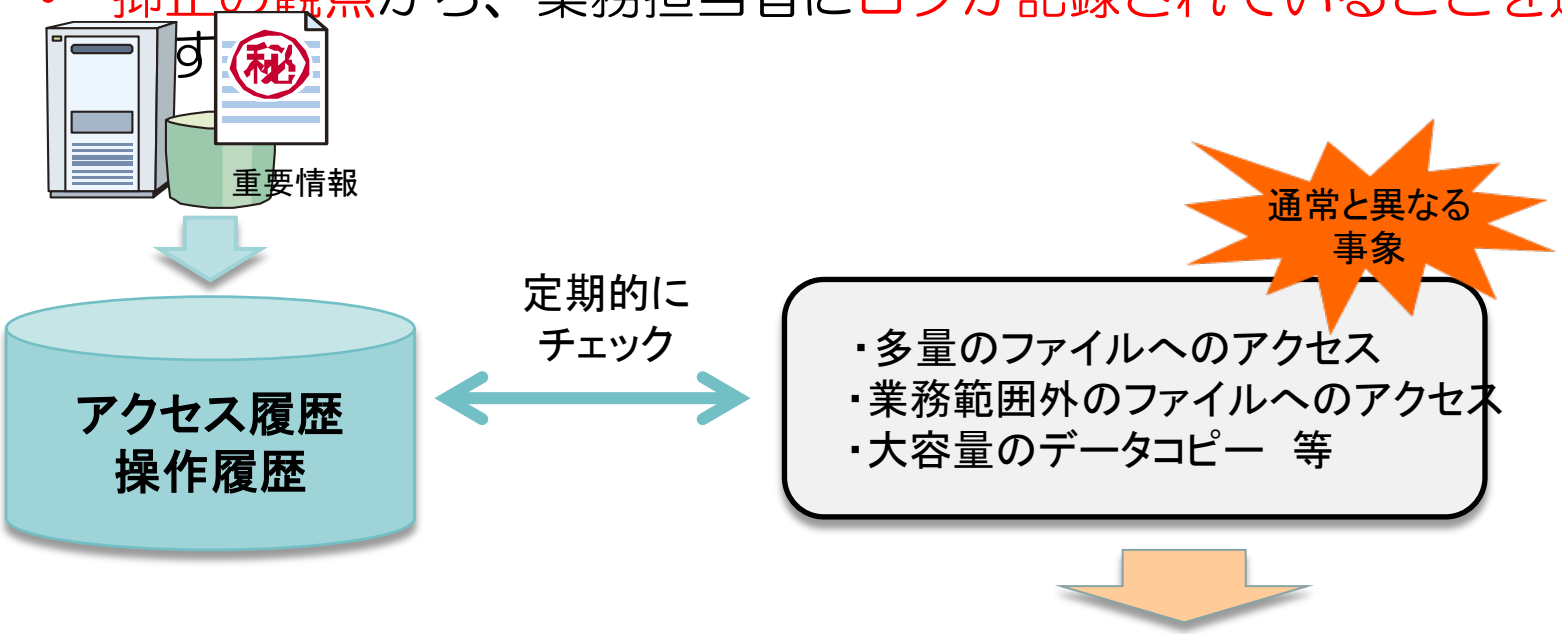
3.3　内部者対策：システム管理者 ①適切な権限管理（システム）

- システム管理者ごとにIDを割り当て、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特権を用いて操作できないようにする。



3.3　内部者対策：システム管理者
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、システム管理者以外のものが定期的に監査し異常な事象の発見に努める。
  - ✓ 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す



3.4　委託先管理

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

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

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

重要情報

業務委託

委託先

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

3.4　委託先管理
①重要情報の取扱いに関する合意

委託元

- 委託前、委託先の体制や規定の点検等により、重要情報の取扱いについて確認する。
- 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、安全管理が十分かを定期・不定期に確認する。
- 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。
- 事後対策の連携を契約等で明確化しておく。

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

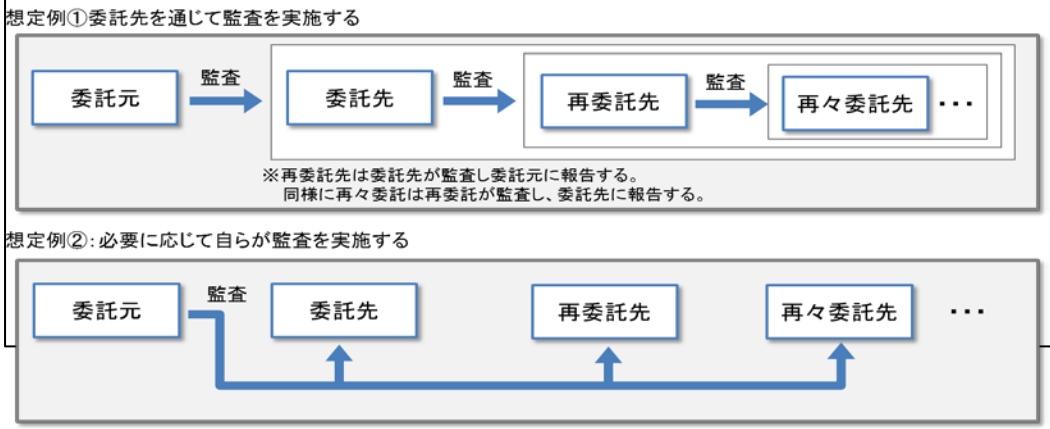
3.4　委託先管理
参考. 外部委託先の監督方法

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

委託先の監査体制



必要に応じて自らが確認や監査を実施する

3.4　委託先管理
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。

SLA構成要素

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		

ログの取得
セキュリティ（不正アクセス）ログ及びバックアップ取得結果ログを、要望に応じて提供する。

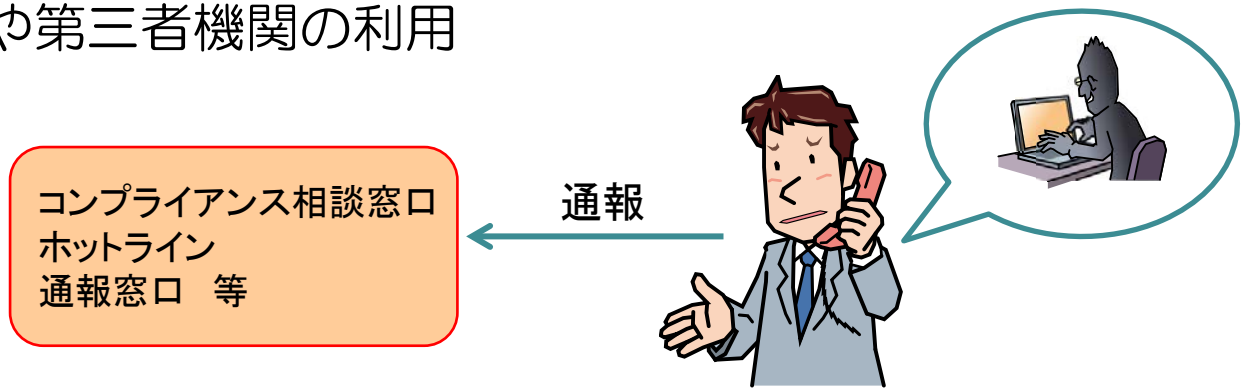
情報取扱者の制限
情報取扱環境
通信の暗号化レベル
ウイルス対策管理
公的認証取
サービスに関する第三者評価　等

（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
→ 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

3.5　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



3.6　職場環境の整備　1/2

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

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

3.6　職場環境の整備　2/2

公平な人事評価の整備

- ✓ 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。

上司

同僚

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。

良好なコミュニケーション

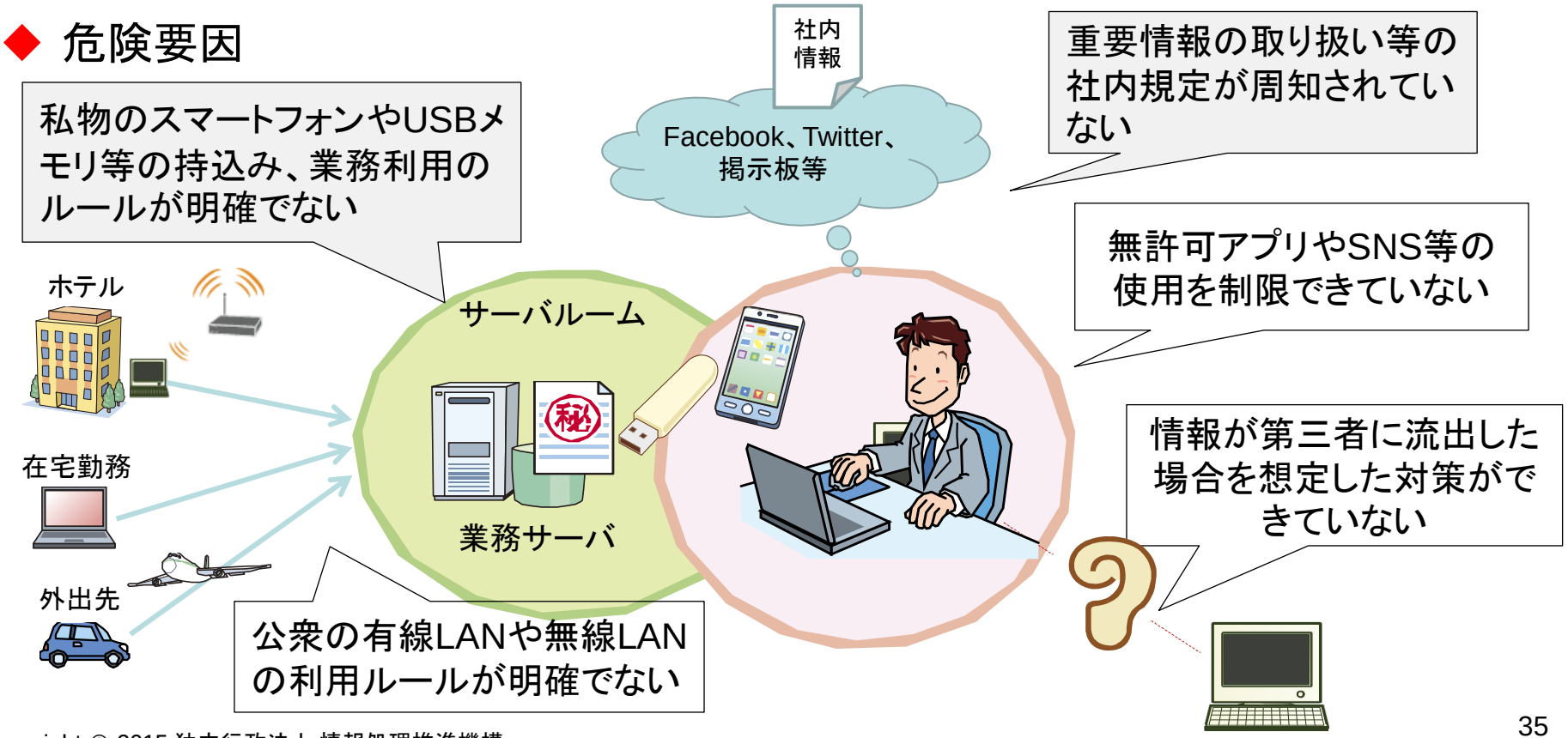
- ✓ 相談しやすい環境を整備し、業務の支援や上司や同僚との良好なコミュニケーションがとれる職場環境づくりを推進する。

3.7　悪意のない内部不正：ルール不徹底に起因する不正行為

①教育による周知徹底と②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、SNSや掲示板への安易な書き込みなど。

◆ 危険要因



3.7　悪意のない内部不正
①教育による周知徹底

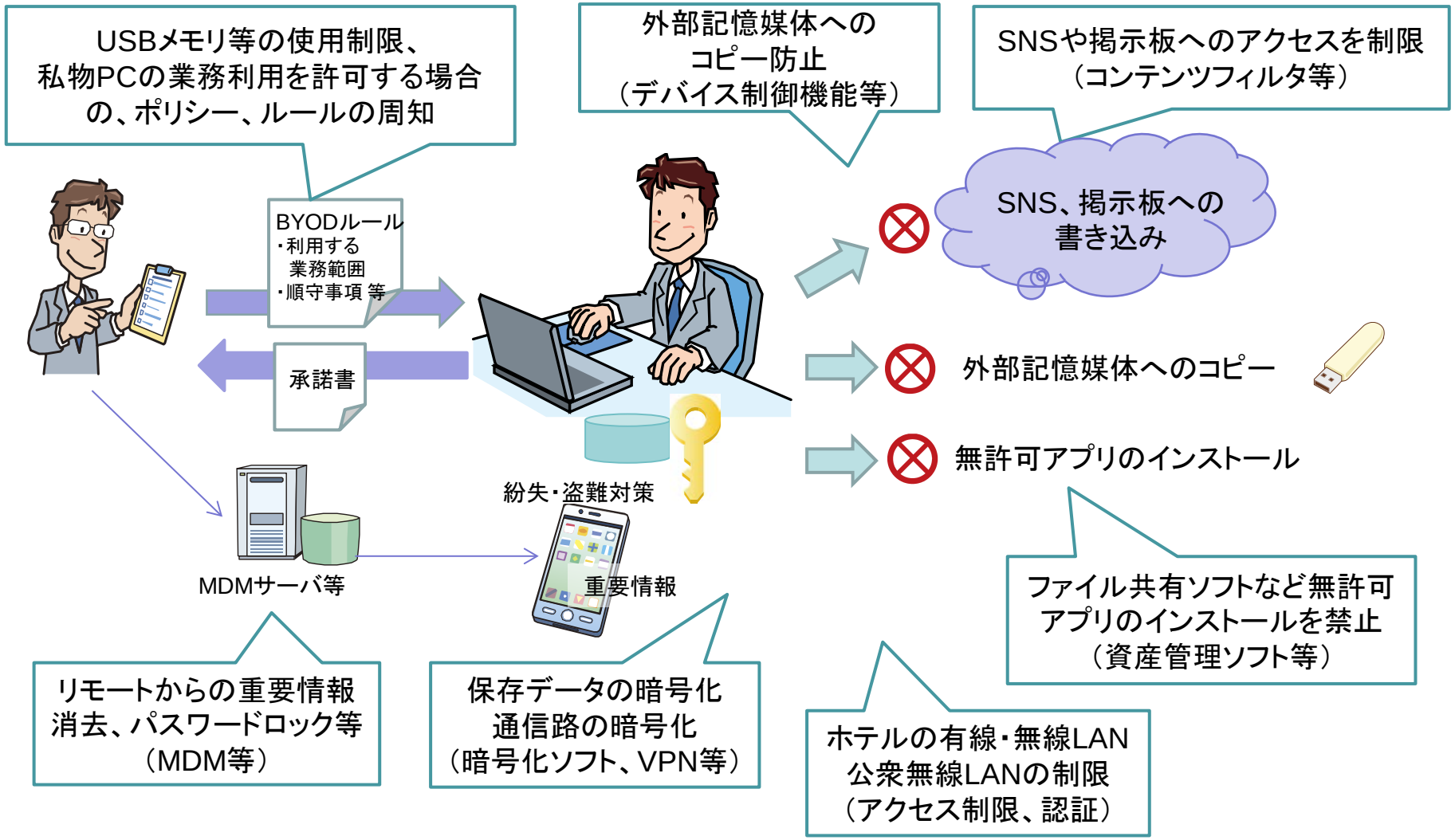
社内教育を通し、情報の無断持ち出しが不正行為であること、ルールに違反すると社内規定で罰せられることを認識させる。

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

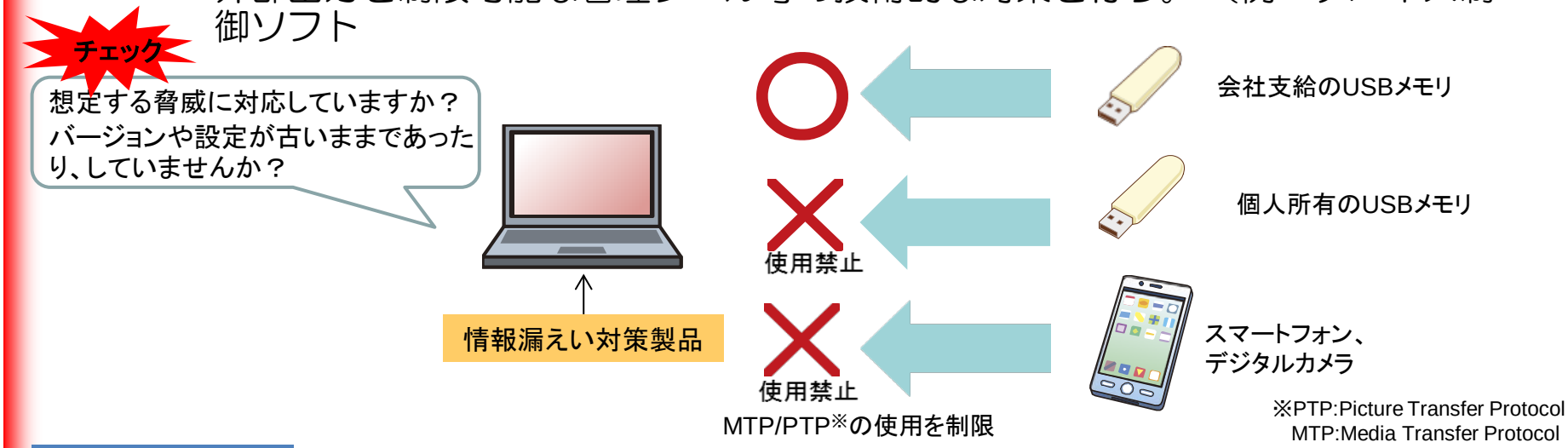
3.7　悪意のない内部不正
②情報漏えい対策



3.7　悪意のない内部不正
②情報漏えい対策

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



対策項目：(30)

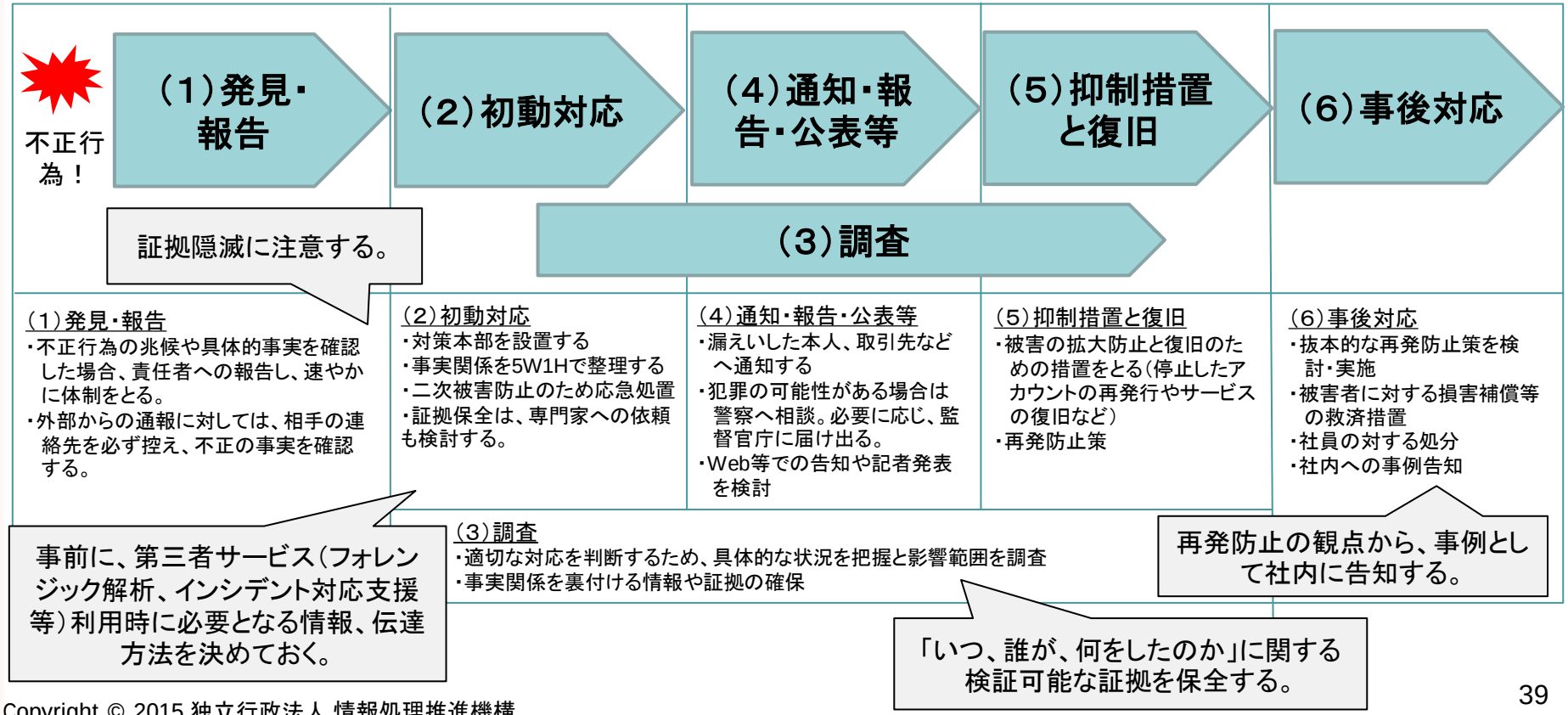
ITの技術進歩や新たな脅威の出現等に応じて、継続的に対策を見直し改善する。

3.8：内部不正発生時の事後対応

自社及び関係者（顧客、取引先など）の直接的・間接的被害を最小限に抑えるため、事後対策を実施する。

- 対応手順や報告手順を事前に取り決めておく。
- 業務を委託している場合は、委託先と協力して体制を整備する。

参考） 情報漏えい発生時の対応ポイント集（IPA）



ガイドライン

1. 営業秘密管理指針
   - 司法により参考とされ、一定の強制力あり
   - 経済産業省
2. 組織における内部不正防止ガイドライン
   - IPA　（独）情報処理推進機構
   - 強制力はない

1.営業秘密管理指針

- 「営業秘密管理指針（全部改訂）」
  - 改訂前の指針は、営業秘密に関する不正競争防止法の解釈のみならず、営業秘密管理に関するベストプラクティス及び普及啓発的事項をも含んでいた。

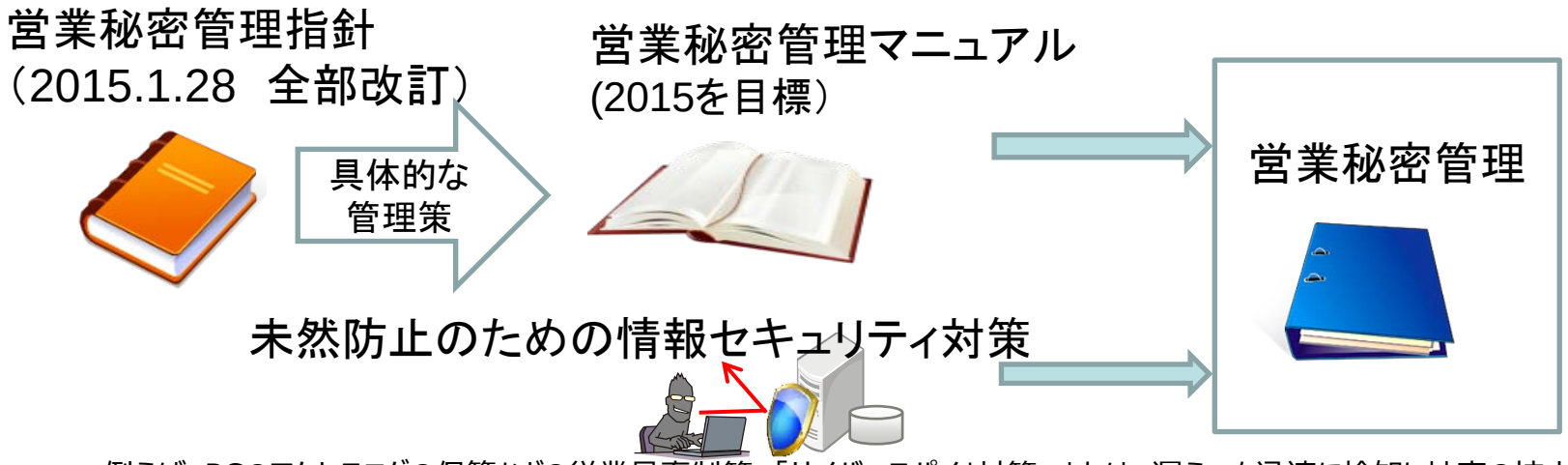
産業構造審議会　知的財産分科会　営業秘密の保護・活用に関する小委員会にて検討

ページ数は営業秘密管理指針（全部改訂案）による。

1. 営業秘密管理指針 指針で示す管理水準(p.2)

「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」

- 本指針は、**不正競争防止法によって差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を示すもの**である。営業秘密の漏えい防止ないし漏えい時に推奨される(高度なものを含めた)包括的対策は、別途策定する「営業秘密保護マニュアル」（仮称）によって対応する予定。



例えば、PCのアクセスログの保管などの従業員牽制策、「サイバースパイ」対策、または、漏えいを迅速に検知し被害の拡大を防止するための対策などは、より高度な営業秘密の漏えい防止策として必要となる場合もありうる。

1. 営業秘密管理指針と要件
必要な秘密管理措置の程度(p.6-9)

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。

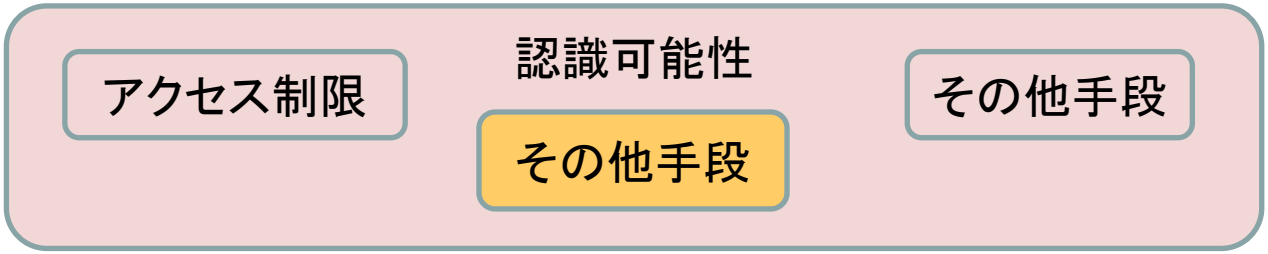
- 秘密管理性要件が満たされるためには、営業秘密保有企業が当該情報を秘密であると単に主観的に認識しているだけでは不十分。
  - 営業秘密保有企業の秘密管理意思：特定の情報を秘密として管理しようとする意思
  - 秘密管理措置：（後述）
  - 認識可能性の確保：情報にアクセスした者が秘密であると認識できる
  - 取引相手先に対する秘密管理意思の明示についても、基本的には、対従業員と同様に考えることが可能

1.　営業秘密管理指針と要件
秘密管理措置(p.6-9) － ①

- 秘密管理性要件は、従来、①情報にアクセスできる者が制限されていること(アクセス制限)、②**情報にアクセスした者に当該情報が営業秘密であることが認識できるようにされていること(認識可能性)**の2つが判断の要素になると説明されてきた。

アクセス制限　　認識可能性

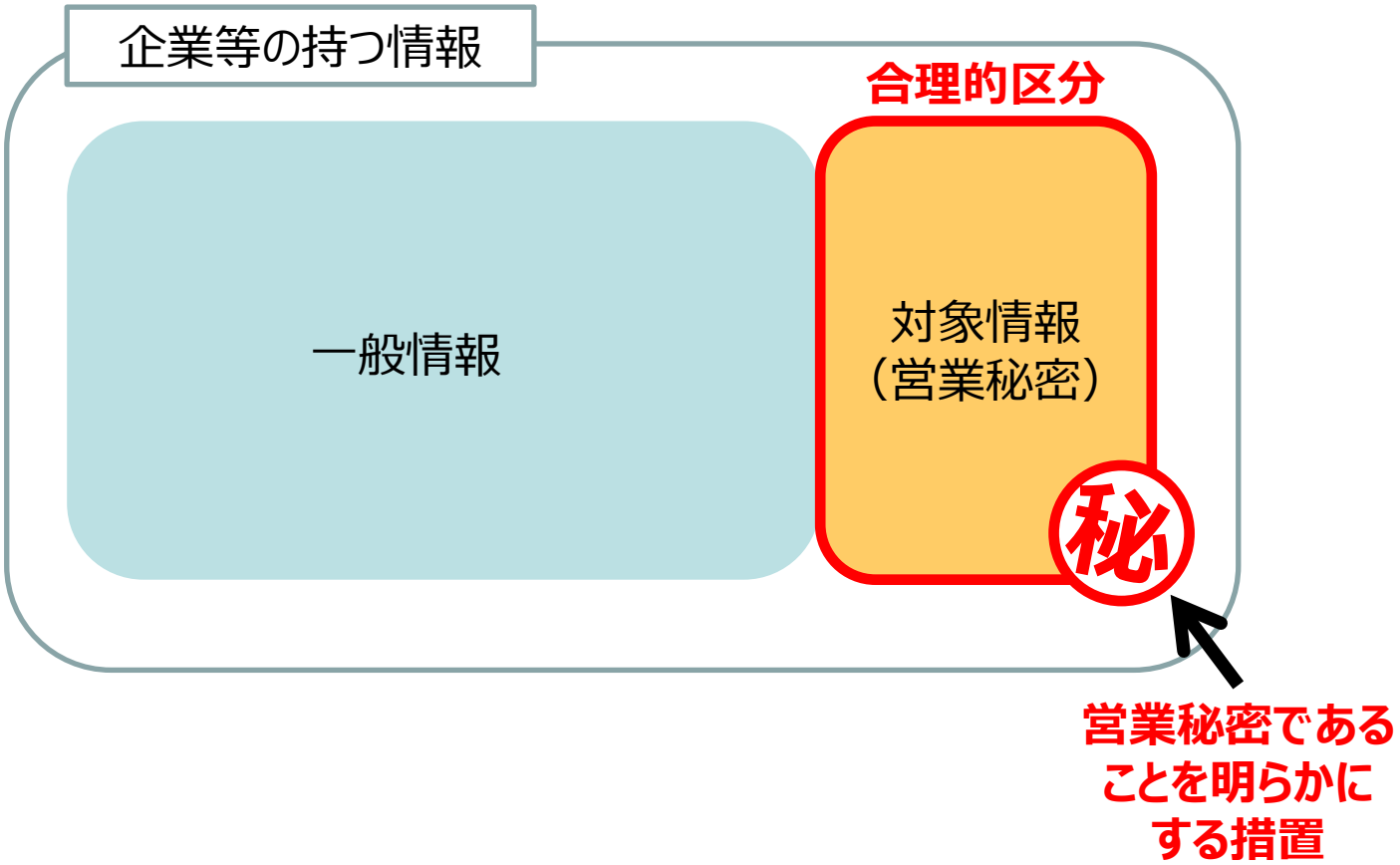
- 両者は秘密管理性の有無を判断する重要なファクターであるが、それぞれ別個独立した要件ではなく、**「アクセス制限」は、「認識可能性」を担保する一つの手段**であると考えられる。したがって、情報にアクセスした者が秘密であると認識できる(「認識可能性」を満たす)場合に、それ以上のアクセス制限がないことを根拠に秘密管理性が否定されることはない。



- 従業員がある情報について秘密情報であると現実に認識していれば、営業秘密保有企業による秘密管理措置が全く必要ではないということではない。

1. 営業秘密管理指針と要件
秘密管理措置(p. 6-9) - ②

- **秘密管理措置**は、対象情報(営業秘密)の一般情報(営業秘密ではない情報)からの**合理的区分**と当該対象情報について**営業秘密であることを明らかにする措置**で構成される。



1.　営業秘密管理指針
秘密管理措置の具体例(p.9-)

- 指針では、一例として媒体に対する典型的な秘密管理措置が紹介されている。

- **電子媒体の場合**
  - 一般情報からの合理的な区分を行った上で、次のような方法のいずれかによって、秘密管理性の観点から充分な秘密管理措置となり得る。
    - マル秘表示の貼付
      - 記録媒体/電子ファイル名・フォルダ名/記録媒体を保管するケース等
    - 営業秘密の電子ファイルを開いた場合に端末画面上にマル秘である旨が表示されるPC設定
      - 営業秘密の閲覧に要するパスワードの設定
      - 電子ファイルそのもの/当該電子ファイルを含むフォルダ

2.組織における内部不正防止ガイドライン（2014.9/2015.3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、2015年3月に改訂

版数	改訂日	主な改訂内容
第2版	2014.9	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。 ・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
第3版	2015.3	本ガイドラインを使い易くすることで、より広く活用していただけるよう強化 ・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

【目次】

第3版

※日本語版、英語版

2.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）

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
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

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・ソリューションの利用等を検討

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

まとめ

- 内部者の不正に対する懸念が増大
- 内部者の不正行為による被害は甚大
- 権限を持ち、悪意をもった内部者の不正を防ぐのは容易ではない
- 組織における内部不正対策
  - トップダウンによる、継続した対策見直し
  - 内部不正に見返りがない環境整備
  - 内部不正に強い組織の構築が重要
- （国内では）情報共有による事例分析が不足

参照情報

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/2011/04/20110401001/20110401001.html

参考：海外の調査および情報共有

- 「グローバル情報セキュリティ調査®」2015
  - PWC、CIO Magazine、CSO Magazine
  - 回答者：日本を含む世界154カ国の経営者や責任者
- 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%）
- 2014 Global Report on the Cost of Cyber Crime
  - Ponemon Institute, LLC
  - 回答者：日本を含む世界7カ国257社の経営者や責任者
- 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、2015年2月現在、700の事例を収集・分析し内部不正対策を推進