資料５

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
セキュリティセンター

IPA Better Life with IT

組織における内部不正防止ガイドライン

- 組織の情報漏えいに関する内部不正対策に特化したガイドライン
- 2022年4月に改訂第5版発行

1. 背景
2. 概要
3. 用語の定義と関連する法律
4. 内部不正を防ぐための管理のあり方
   - 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 原因究明と証拠確保
   - 4-6 人的管理
   - 4-7 コンプライアンス
   - 4-8 職場管理
   - 4-9 事後対策
   - 4-10 組織の管理

付録Ⅰ～Ⅷ

内部不正の3要因 「不正のトライアングル」

内部不正は「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*

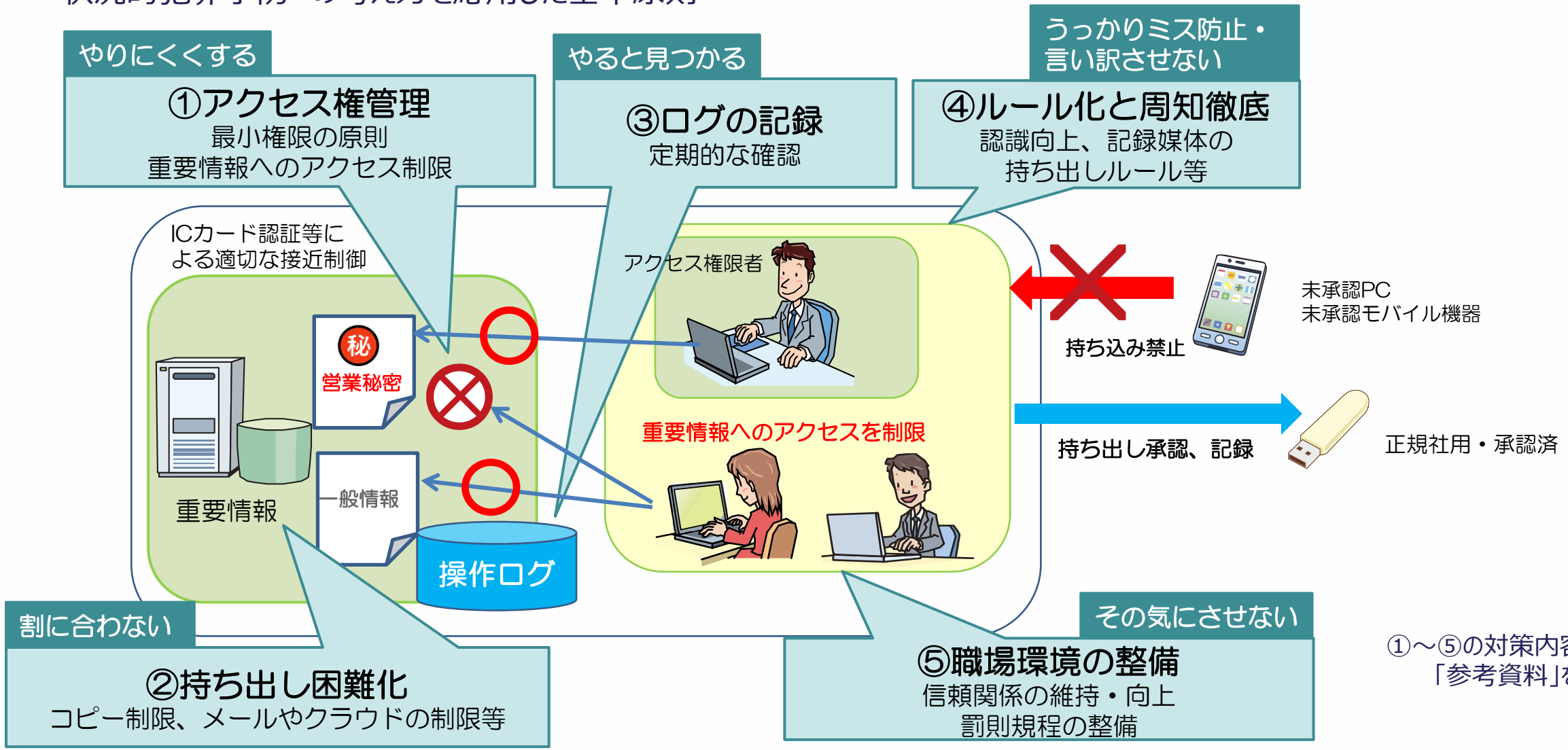
内部不正の3要因

動機・プレッシャー	機会	正当化
不正を働こうと考える きっかけ、心理的原因： ・処遇への不満 ・日常業務のプレッシャー	不正行為の実行を 可能・容易にする環境 ・ITや物理環境の不備 ・組織のルール不備等	自分勝手な理由づけや 倫理観の欠如： ・都合の良い解釈 ・他人への責任転嫁等
・人事に不満 ・金銭問題を抱えている ・高いノルマを課されている	**・強力なシステム管理権限 ・持ち出し可能な環境 ・同じ業務を長期間担当**	**・正当に評価がされない ・サービス残業 ・会社へのうらみ**
低減・抑制策		
・ 職場環境整備 ・ 不満の解消等	**・ 技術対策** ・ アクセス管理、ログ管理、暗号化等 **・ モニタリング、通報制度等 ・ 監視による不正抑止 ・ 組織対策体制** ・ 内部統制・法令遵守強化等	**・ 契約 ・ 誓約書署名等**

*Donald Ray Cressey（米国の組織犯罪研究者）による

内部不正防止対策の勘所

状況的犯罪予防*の考え方を応用した基本原則



①～⑤の対策内容の詳細は
「参考資料」を参照

＊状況的犯罪予防（Situational Crime Prevention）：都市空間における犯罪予防の理論 [Cornish & Clarke, 2003]

10の観点・33の対策項目

- 対策項目各々のリスク、対策のポイントについて整理

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	（20）教育による内部不正対策の周知徹底 （21）従業員モニタリングの目的等の就業規則での周知 （22）派遣労働者による守秘義務の遵守 （23）雇用終了の際の人事手続き （24）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： 秘密指定とアクセス管理	（3）情報の格付け区分 （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 やりにくくする	7	コンプライアンス	（25）法的手続きの整備 （26）誓約書の要請 うっかりミス防止・言い訳させない
3	物理的管理	（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 （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	8	職場環境	（27）公平な人事評価の整備 （28）適正な労働環境及びコミュニケーションの推進 （29）職場環境におけるマネジメント
4	技術・運用管理	（12）内部不正モニタリングシステムの適用 （13）ネットワーク利用のための安全管理 （14）重要情報の受渡し保護 （15）情報機器や記録媒体の持ち出しの保護 （16）組織外部での業務における重要情報の保護 （17）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） 割に合わない	9	事後対策	（30）事後対策に求められる体制の整備 （31）処罰等の検討及び再発防止 その気にさせない
5	原因究明と証拠確保	（18） 情報システムにおけるログ・証跡の記録と保存 （19） システム管理者のログ・証跡の確認 やると見つかる	10	組織の管理	（32）内部不正に関する通報制度の整備 （33）内部不正防止の観点を含んだ確認の実施

使い勝手を考慮し付したガイドライン付録群

- 付録Ⅰ　内部不正事例集
  企業・組織にとっての「他山の石」用途
- 付録Ⅱ　内部不正簡易チェックシート
  対策導入支援用。対策の指針をまとめ、組織横断的な担当俯瞰も目指す
- 付録Ⅲ　Ｑ＆Ａ集
- 付録Ⅳ　他ガイドライン等との関係
  JIS Q 27001、営業秘密管理指針/秘密情報の保護ハンドブック、個人情報保護ガイドライン等
- 付録Ⅴ　基本方針の記述例
- 付録Ⅵ　内部不正防止の基本5原則と25分類
- 付録Ⅶ　対策の分類
  企業や組織の環境別対策、不正行為の種類別対策
- 付録Ⅷ　テレワークに係る対策一覧

組織における内部不正防止ガイドライン
各項目の紹介

基本方針：経営層が関与した管理体制整備

- 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（ポリシー）」を策定
- 経営者による意思決定を組織全体に周知徹底
- **組織横断的な実施状況が把握できる管理体制**を企業の規模や実情に応じ構築

内部不正防止対策の10の観点（分類）と関連部門

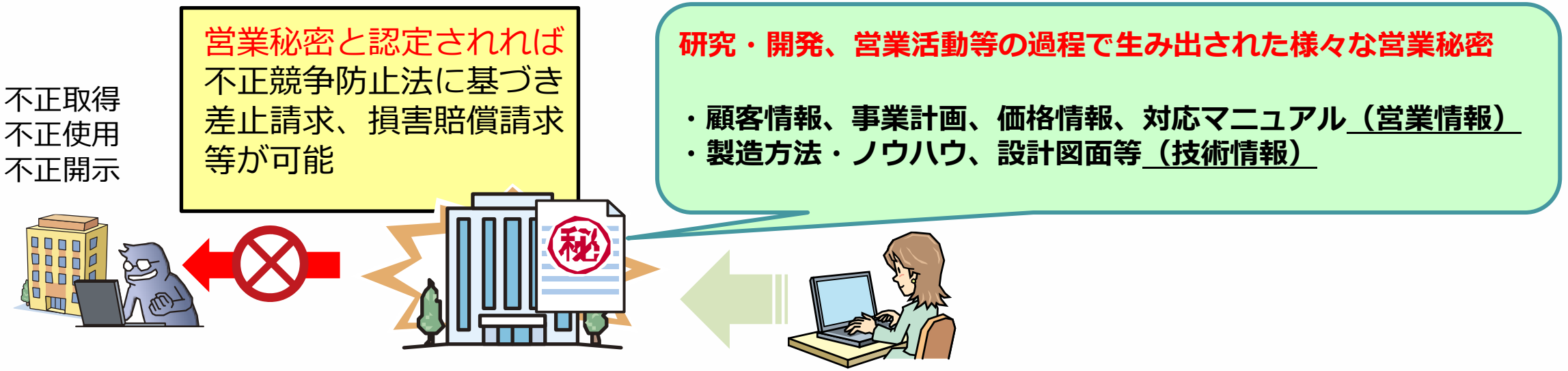
観点（分類）	経営者	情報システム部	総務部	人事部	法務・知財部	営業・開発等の各部門
1.基本方針	○					
2.資産管理		○				○
3.物理的管理		○	○			○
4.技術的管理		○				○
5.証拠確保		○				○
6.人的管理			○	○	○	○
7.コンプライアンス			○	○	○	○
8.職場環境			○	○		○
9.事後対策		○				○
10.組織の管理		○				○

資産管理：重要情報の特定と格付け区分

重要情報の特定（明確化）

- 少なくとも**重要情報と一般情報**の2つに分けて管理（情報の格付け区分）
- **重要度ごとに取扱いルール**を定め、**定期的に見直す**（取扱範囲、廃却方法等）
- 従業員にわかるように「機密情報」等を**表示**（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



資産管理：アクセス管理の導入・適用

やりにくくする

- 情報システムにおける利用者のアクセス管理
  - 誰がどのデータにどのようにアクセスできるかを決める
  - 決めた通りのアクセスだけを許す仕組みを作る
  - 退職などに伴う更新を徹底する
- システム管理者の権限管理
  - システム管理者のふるまいに透明性を確保する
- 情報システムにおける利用者の識別と認証
  - パスワード等を共有せず利用者をひとりひとり見分けるようにする

物理的管理：モノの動きの制限・監視

割に合わない

- 物理的な保護と入退管理
  - 大事な情報を囲う場所を作って出入りを制限する
- 情報機器及び記録媒体の資産管理及び物理的な保護
  - 情報の持ち運び手段を把握して外に出ないよう管理する
  - 必要に応じてそれらの手段を無効化する
- 情報機器及び記録媒体の持出管理
  - 持ち出しが必要な場合にはしっかりと記録・追跡する
- 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
  - 外からの持ち込みも制限・記録・追跡する

技術・運用管理：アクセス管理境界の管理

割に合わない

- 内部不正モニタリングシステムの適用
  - 異常事態の発生をなるべく自動的に検知する仕組みを設ける（プライバシーに対する配慮を忘れずに）
- ネットワーク利用のための安全管理
  - 直接管理外のサービスやソフトウェアの利用を管理する
- 重要情報の受け渡し保護
  - 委託先を含む重要情報の内外の行き来を把握・保護する
- 情報機器や記録媒体の持ち出しの保護
  - 機器や媒体上の重要情報そのものを暗号化等で保護する

技術・運用管理：アクセス管理境界の管理

割に合わない

- 組織外部での業務における重要情報の保護
  - テレワークや出先業務での情報漏えいを防止する

- 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
  - 業務委託先でも十分に情報管理が行われていることを確認し
    その継続的順守を契約条件の中に盛り込む

原因究明と証拠確保：漏れのない状況把握

やると見つかる

- 情報システムにおけるログ・証跡の記録と保存
  - 誰がいつどのように重要情報にアクセスしたかを記録する
- システム管理者のログ・証跡の確認
  - 収集したアクセス記録を元に不適切なアクセスを検知する

アクセス管理の仕組みを作っただけで安心しない

人的管理：不正行為に対する認識の確立

うっかりミス防止・
言い訳させない

- 教育による内部不正対策の周知徹底
  - 正しいことと不正とに対する理解を広め浸透させる
- 従業員モニタリングの目的等の就業規則での周知
  - 従業員のプライバシーを守ることで信頼を培う
- 派遣労働者による守秘義務の遵守
  - 従業員だけを対策の対象としない
- 雇用終了の際の人事手続き
- 雇用終了及び契約終了による情報資産等の返却
  - 雇用関係の終了後にも重要情報が漏えいしないよう取り計らう

コンプライアンス：法の保護を得るための準備

うっかりミス防止・
言い訳させない

- 法的手続きの整備
  - 就業規則等の内部規定を整備して懲戒処分を可能にする
- 誓約書の要請
  - 内部者が守らなければならない事柄を確実に認識させる

コンプライアンス：法の保護を得るための準備

うっかりミス防止・
言い訳させない

- 法的手続きの整備
  - 就業規則等の内部規定を整備して懲戒処分を可能にする
- 誓約書の要請
  - 内部者が守らなければならない事柄を確実に認識させる

職場環境：快適なチームワークの維持

その気にさせない

- 公平な人事評価の整備
  - 不平や不満を生まない人事評価を心がける
  - 適時の配置転換等を交えることで特定業務の属人化を避ける
- 適正な労働環境及びコミュニケーションの推進
  - 過剰なストレスを生まない職場環境を心がける
  - 打ち解けやすく悩みを相談できるコミュニケーションを保つ
- 職場環境におけるマネジメント
  - 従業員との距離を緊密に保つ（目の届かない仕事をさせない）

事後対策：快適なチームワークの維持

その気にさせない

- 事後対策に求められる体制の整備
  - 実際の問題に応じた迅速な対応内容を事前に洗い出し準備する
  - 何があったかを把握・分析し着実に限定・復旧する仕組みを整える
  - 内部不正発生時には自分たちが加害者になる恐れもあると自覚する

- 処罰等の検討及び再発防止
  - 不正行為が高くつくものであることをはっきりと示す
  - 発生した内部不正を隠さず内部で共有し引き締めを図る

組織の管理：対策の着実な有効化

やると見つかる

- 内部不正に関する通報制度の整備
  - 実際に安心して利用できる匿名通報制を充実させる
  - ためらいなく利用できるよう教育と周知を徹底する

- 内部不正防止の観点を含んだ確認の実施
  - 内部不正防止の対策が着実・継続的に機能するよう点検を怠らない

内部不正のない組織を着実に維持・運営する