IPA Better Life with IT

組織における内部不正対策
～内部不正防止ガイドライン（第3版）について～

2015年7月１４日

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

講演内容

1. 内部不正インシデントの状況
2. 内部不正の要因と対策
3. 内部不正防止ガイドライン

1. 内部不正インシデントの状況
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4月	A社の元社員が、営業秘密である包装機械の設計図を不正に取得したとして**不正競争防止法違反で逮捕**された。2013年に退職後、競合他社へ転職している。	退職者	不明（容疑否認）
2月	B社の元社員がサーバから在職中にモーターショーに関するデータ等計8件のファイルを不正に取得し、自分のハードディスクに複製したとして**不正競争防止法違反で逮捕**された。退職後は中国の自動車会社に転職。	退職者	転職先での利益取得
1月	家電量販店C社の元社員が、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	転職先で役立てたかった
2014年10月	D社の社員が顧客の個人情報を数回に渡り第三者に売却していたことが警察からの情報提供で発覚し、**懲戒解雇**となった。**不正競争防止法違反で告訴**予定	社員	金銭の取得
10月	医療関係者向け転職情報サイトを運営するE社の元社員、役員宛メールを自分のメールアドレスに自動転送されるようにサーバを設定、受信し盗み見たとして**私電磁的記録不正作出、同供用の疑いで逮捕**。	社員（システム管理）	不明
7月	F社の顧客データベースを保守管理するグループ会社G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	H機関のネットワークシステム保守管理の委託先であるI社の社員が、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、懲戒解雇**となった。	委託先社員SE	受注活動を有利にしたかった

（報道により公表された事例をIPAがまとめたもの）

組織への影響

事例１　F社

- 特別損失　260億円（情報セキュリティ対策、お客様への対応等）
- 新規営業活動の一時停止
- 役員2名（代表取締役副会長、取締役）の引責辞任

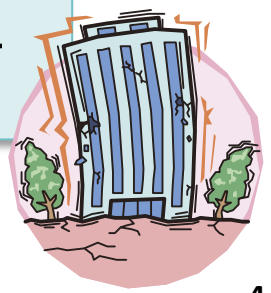
事例２　I社

- 応札辞退
- 指名停止：I社 6ヶ月、子会社5社 3カ月
- 役員3名（執行役副社長1名、執行役常2名）減俸30%（1カ月）

事例３　K社

（C社から営業秘密を持ち出したとして逮捕された元従業員の転職先）

- 不正競争防止法の両罰規定（業務主体たる法人にも罰金刑）により書類送検　→　不起訴（2015/5/22）

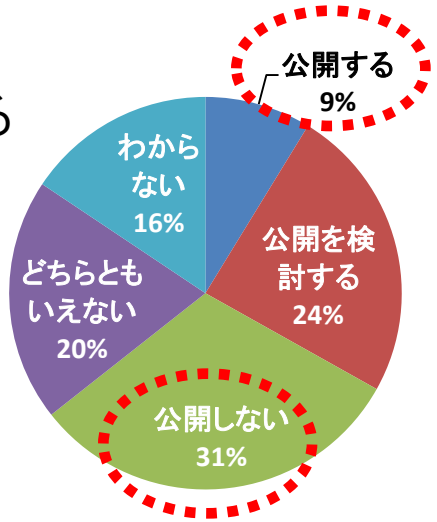


公表されないことが多い

- 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）

5

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%

[PwC:グローバル情報セキュリティ調査®2015]

- 過半の企業が「内部犯行による情報漏えいリスク」を重視

[JIPDEC,ITR: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]

- 漏えいの疑い、過去5年間で企業の1割が経験
  ～ 漏えい防止への取り組みは5割にとどまる ～

[帝国データバンク:営業秘密に関する企業の意識調査]

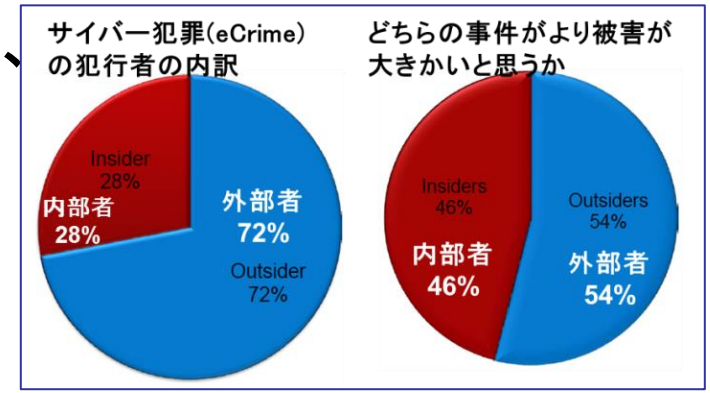
被害額と平均解決日数

- サイバー攻撃の年間平均被害額では内部不正が最も大きい
  - **内部不正　約21.4万ドル**
  - **DoS攻撃　約16.6万ドル、Webベースの攻撃　約11.6万ドル**

[Ponemon：2014 Global Report on the Cost of Cyber Crime]　提供：HP Enterprise Security

- サイバー犯罪の犯行者の内外内訳は、
  外部者が72%と多数派だが：
  被害の大きさ評価では外部は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

[Ponemon：2014 Global Report on the Cost of Cyber Crime]　提供：HP Enterprise Security

2. 内部不正の要因と対策

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する

動機・プレッシャー
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。

×

機会
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。

×

正当化
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
高いノルマを設定された

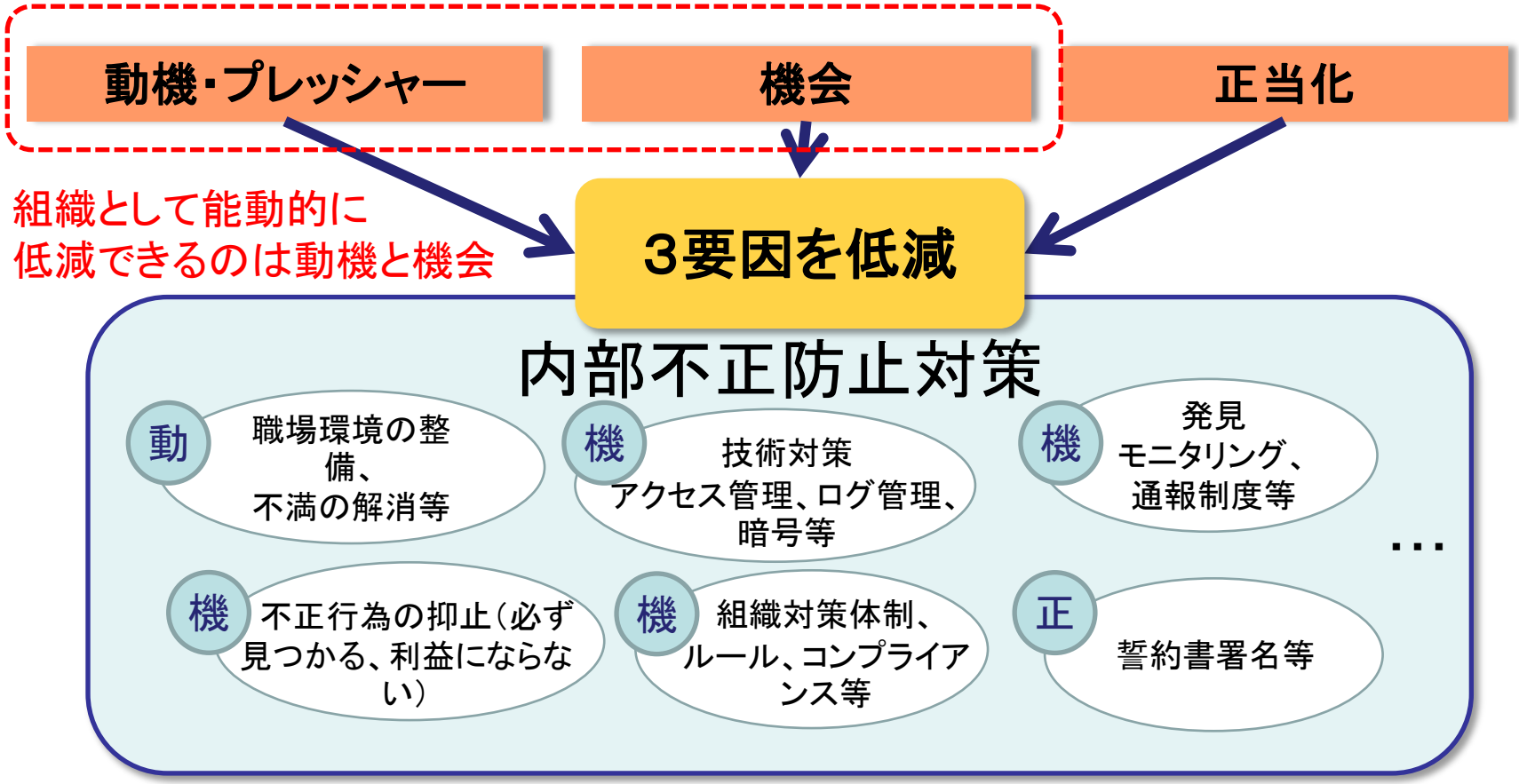
システム管理者権限
持ち出し可能な環境
同じ業務を長期間担当

・正当に評価がされないから
・サービス残業を強いられているから

※ドナルド・R・クレッシー（米国の組織犯罪研究者）による

内部不正防止対策は３要因の低減

- 組織対策として重要なこと＝
  「動機・プレッシャー」と「機会」の低減



3. 内部不正防止ガイドライン 第3版

- 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**

【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
付録Ⅵ 基本5原則と25分類の対策例 *New!*
付録Ⅶ 対策の分類 *New!*

改訂概要

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

※日本語版、英語版

内部不正防止の基本5原則 *New!*

状況的犯罪予防※の考え方を内部不正防止に応用した5原則

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

「機会」の低減

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
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

「動機・プレッシャー」の低減

「正当化」の低減

※犯罪学者のCornish & Clarke（2003）が提唱した都市空間における犯罪予防の理論。監視者の設置などによって外部からのコントロールが可能な「環境」を適切に定めることを主眼として、犯罪機会・動機を低減し、予防する犯罪予防策。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。

例えば…調査報告：内部不正への気持ちが低下する対策

やると見つかる

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）

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
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

チェックシートで現状を把握 する

30の対策項目に対応

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？	□	[ ]			

各項目に関係する部門を示している

New!

どこから検討すべきかわからない場合の参考

所属する企業や組織の環境（情報機器やネットワークの利用）により何を対策すべきかを知りたい。

（1）環境別の対策からのアプローチ

①全ての組織で検討すべき対策
②情報機器はあるが、ネットワークは存在しない場合
③組織内にネットワークが存在する場合の対策

最近の事例を基に、企業で発生し得る内部不正のケース別に対策のポイントを知りたい。

（2）内部者による不正行為別のアプローチ

①組織として検討すべき基本対策
②不正行為別に検討すべき対策
③早期発見
④事後対策

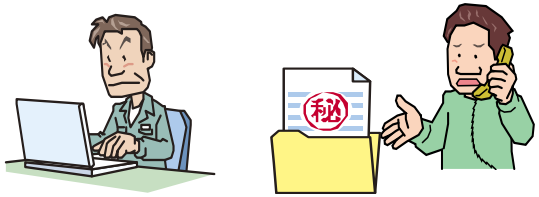
(1)環境別の対策からのアプローチ

①全ての組織で検討すべき対策

基本方針、秘密指定、物理的管理、人的管理、コンプライアンス、職場環境　等

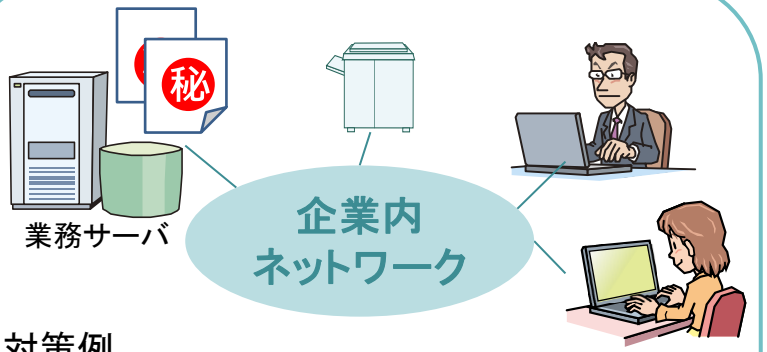
②情報機器はあるが、ネットワークが存在しない

（クラウドサービスの利用によるメール利用等の外部接続はある）



対策例
- 情報機器・記録媒体の管理、保護
- 電子メールやSNSによる情報漏えい対策
- 私物の情報機器等の業務利用、持込制限

③組織内にネットワークが存在する

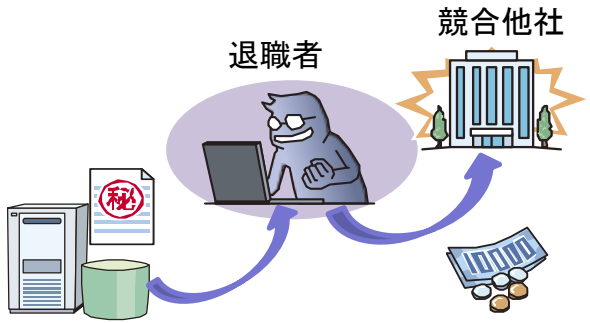


対策例
- 利用者の識別・認証、アクセス管理
- システム管理者の権限管理
- ネットワークによる重要情報の受け渡し保護
- 情報システムのログの記録と監査

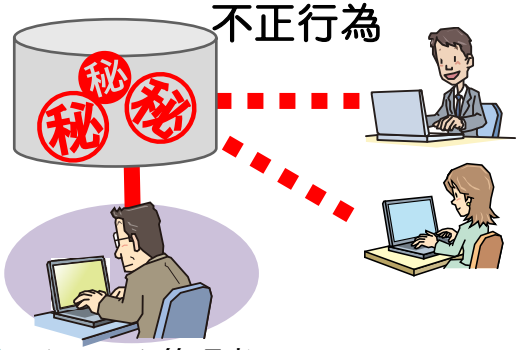
(2)内部者による不正行為別のアプローチ

組織で発生し得る内部不正

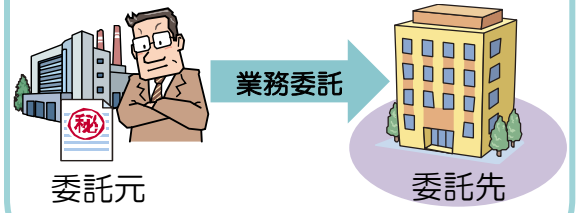
a.退職にともなう情報漏えい



b.システム管理者による不正行為



c. 委託先からの情報漏えい



d. 職場環境に起因する不正行為

e. ルール不徹底に起因する不正行為

さらに・・・
外部攻撃への対策にもなり得る

IPA

標的型攻撃のシナリオ

対策できない

ウイルス感染

人が行う不正アクセス

計画

①計画立案:
標的組織に関係する情報の収集

②攻撃準備:
攻撃に必要となる環境の準備
（メール、攻撃用サーバ）

③初期潜入:
標的型メールの送付

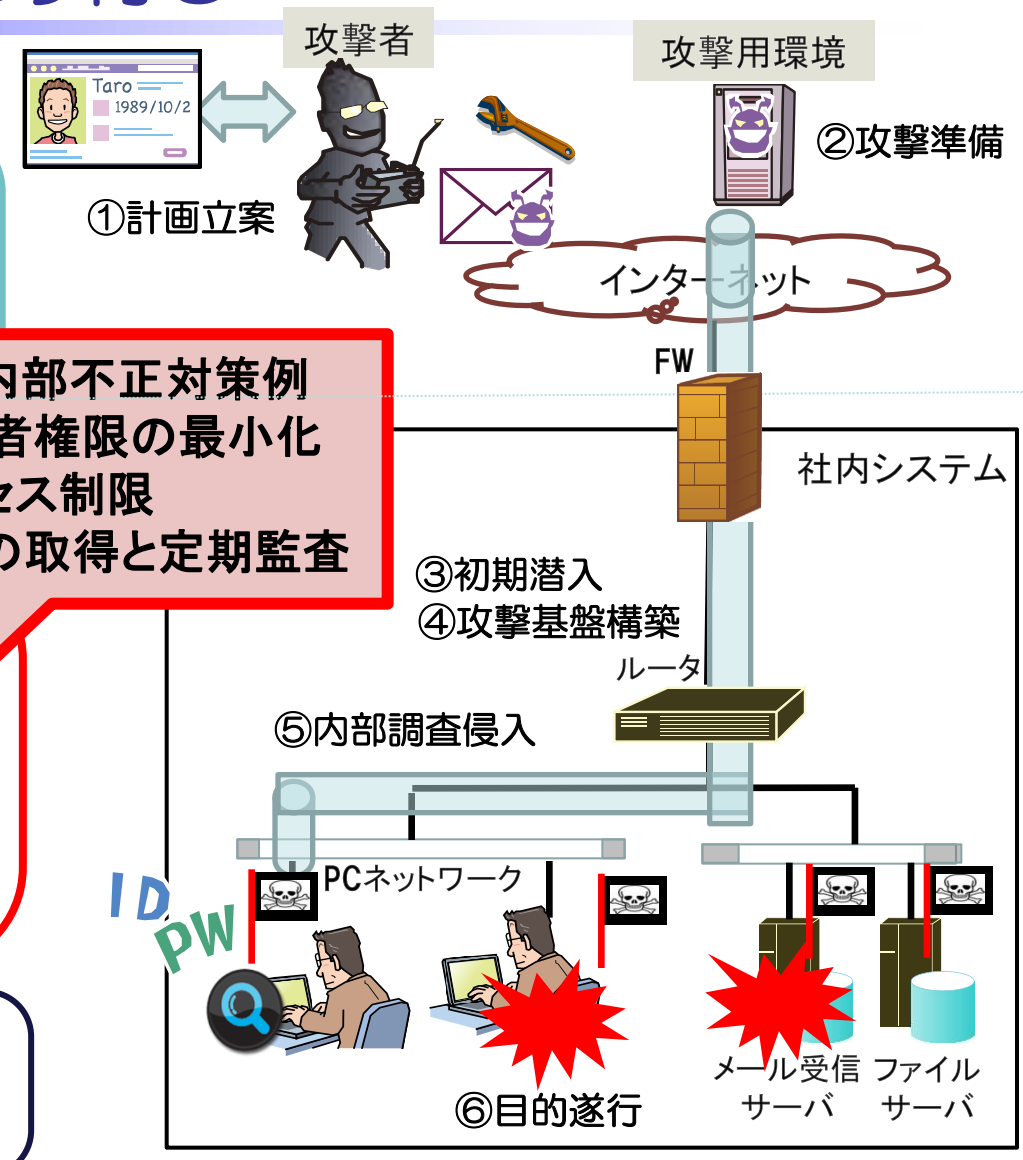
④攻撃基盤構築:
侵入端末を起点にして、ネットワ
およびサーバの位置情報等を収

⑤内部侵入・調査:
認証情報を窃取しながら、侵攻範囲を拡大
（管理端末乗っ取り、サーバ侵害等）

⑥目的遂行:
乗っ取ったサーバから機密情報を窃取、重要システムを破壊

対策は極めて困難

有効な内部不正対策例
- **管理者権限の最小化**
- **アクセス制限**
- **ログの取得と定期監査**



（参考）」対策にIPA「高度標的型攻撃向けたシステム設計ガイド」
https://www.ipa.go.jp/files/000046236.pdf

まとめ

- 内部者の不正行為に対する懸念が増大。
  内部不正による被害は甚大。

- 内部不正を防止するには、動機・プレッシャー、機会、正当化の3要因を低減することが必要。そのため、「人」、「組織」、「技術」の面から、対策を検討する。

- 内部不正防止ガイドラインを活用して内部不正防止のための環境整備を！どこから対策すべきかわからない場合は、条件別の対策分類が参考になります。

内部不正にはトップダウンで
組織横断の取り組み！

ご清聴ありがとうございました

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（IPA/ISEC）

〒113-6591
東京都文京区本駒込２－２８－８
　文京グリーンコート センターオフィス16階
TEL 03（5978）7508
FAX 03（5978）7518
電子メール　isec-info@ipa.go.jp
URL　http://www.ipa.go.jp/security/

内部不正対策 特設ページ：http://www.ipa.go.jp/security/insider/