経営の重要課題としての情報セキュリティ対策

独立行政法人 情報処理推進機構

理事　立石譲二

IPA（情報処理推進機構）のご紹介

- 日本のIT国家戦略を技術面、人材面から支えるために設立された、経済産業省所管の独立行政法人。
- 誰もが安心してITのメリットを実感できる**“ 頼れるIT社会”**の実現を目指しています。

①情報セキュリティ

・ウイルス、不正アクセス等の届出機関。及び、調査研究、情報セキュリティの普及啓発活動。
・いち早く対策方法を広く国民に向けて発信

②情報処理システムの信頼性向上

・重要インフラを支える情報処理システムの信頼性向上に向けた取り組み

③IT人材育成

・国家試験「情報処理技術者試験」の実施機関
・IT人材の育成や発掘などの促進。また、若手人材の育成やIT人材に必要なスキルの明確化に向けた取り組み

IPA　検索

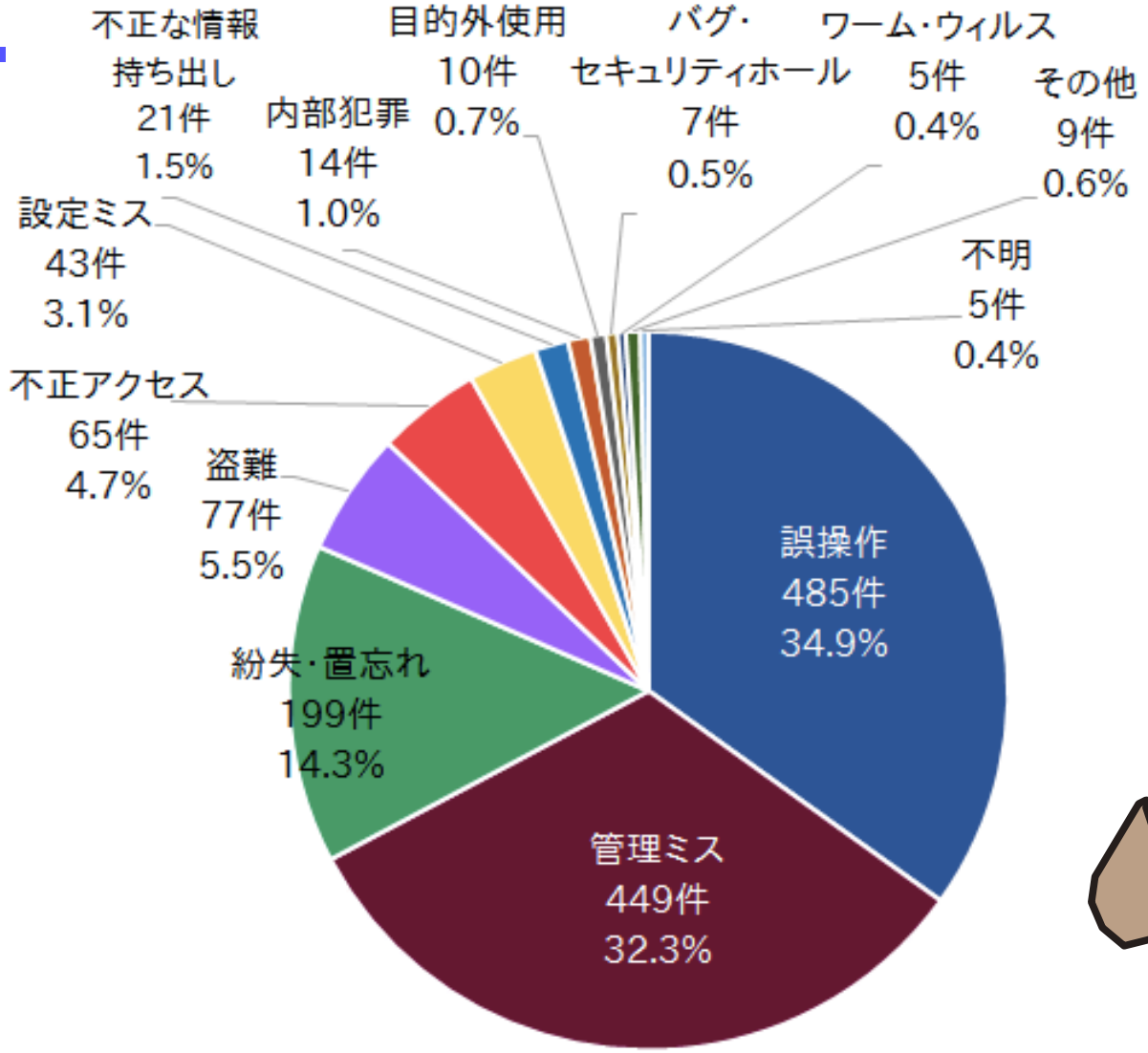
本日のアジェンダ

- リスクマネジメントの本質
- 情報セキュリティはどこまでやれば良いのか
- 内部不正の対策
- 外部からの脅威への対策

～標的型攻撃メールを例として～

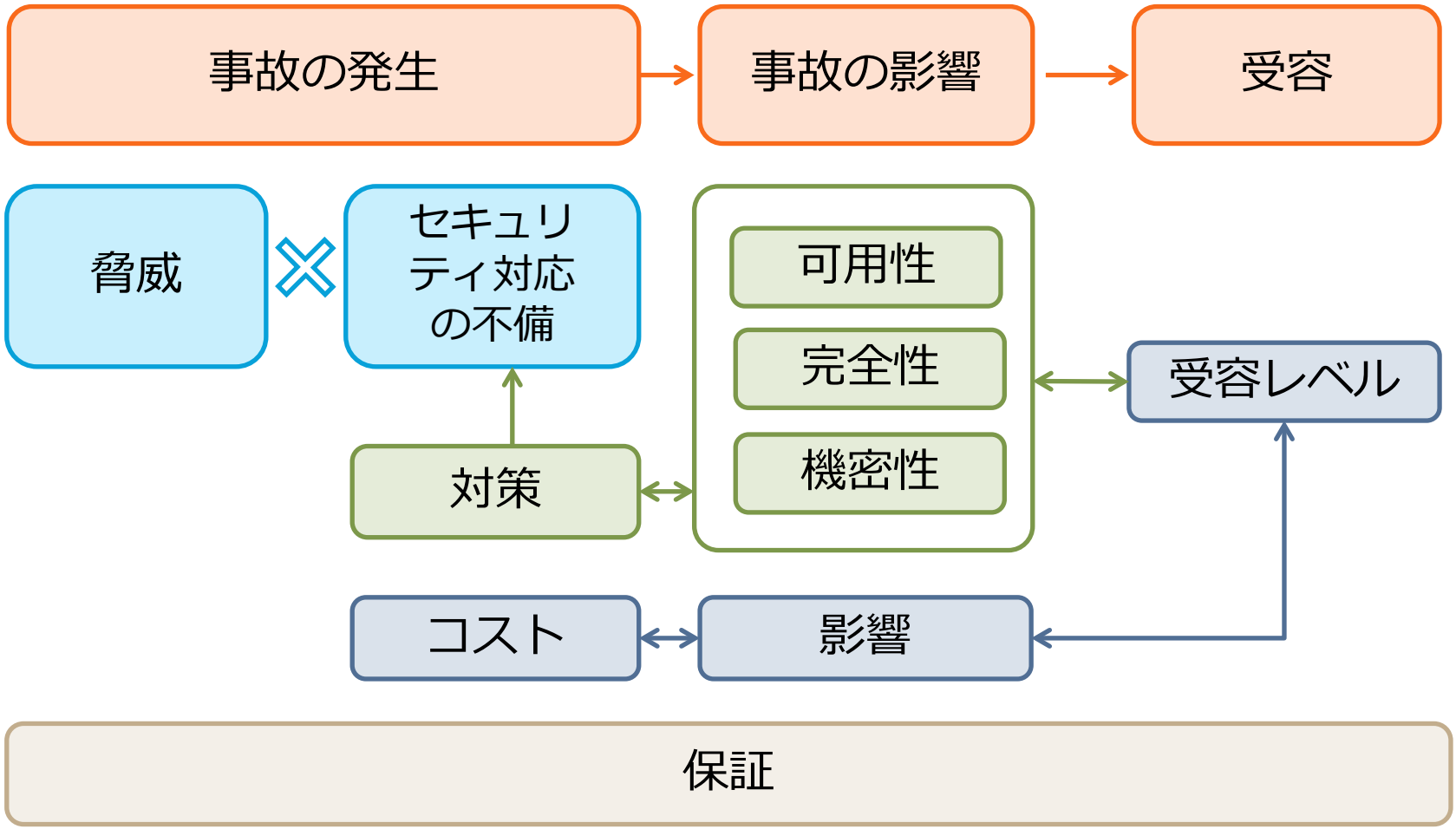
リスクマネジメントの本質

情報漏えいの原因比率（件数）



（出典）JNSA「2013年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～」

リスクマネジメントの本質



影響度を基盤にしたリスク管理

- **情報セキュリティの３つ項目と影響の関係**
  - 可用性・・・情報が使えない時の影響
  - 完全性・・・情報が壊れたり、改ざんされた時
  - 機密性・・・情報が漏れてしまった場合の影響
- **重要度よりも影響度を考える**
  - 重要度は主観的であることが多く、定量化できない
  - 情報資産そのものの価値よりも、それをとりまく環境のほうが重要な判断要素となることが多い

安全管理のための原則

- **情報資産が増えると、管理コストが増える**
  - 紙文書と電子化文書のメリット、デメリットを考慮した安全管理を徹底する。
  - 紙文書と電子化文書も出来る限りコピーを増やさない。
  - 必ず保管場所と公開範囲を取り決める。

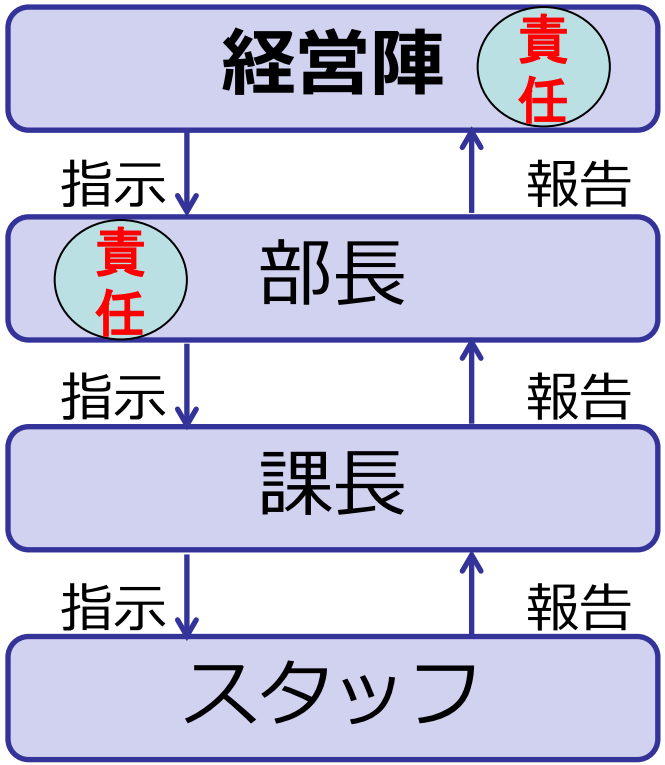
	紙文書	電子化文書
メリット	• 電子媒体を用いず見ることが可能 • 改ざんの痕跡が残る • 鍵などを用いて物理的に保管することができる	• 膨大な情報を保管し、容易に検索ができる • 共有、複製が簡単にできる • 暗号化やアクセス制御等で保護することができる
デメリット	• 保管場所が必須 • 目視のため、検索に時間がかかる • 変色や虫食いなどにより劣化・破損等することがある	• 電子媒体がないと利用できない • 不注意などで不特定多数に情報を漏洩することがある • セキュリティー対策は重要で大変な問題点である

情報セキュリティはどこまでやればよいのか

不祥事が発生した時に備えて

- **情報セキュリティに限らず、不祥事が発生した場合に十分な情報を持っておく**
  - 不祥事が発生した場合の対応において、十分な情報がないことで被害が大きくなることがある
  - 情報が十分になかったために、対応が遅れてしまったり、間違った対応をしてしまい、対応のコストが莫大になってしまうことがある
- **事故に備えて、いつでも情報が上がってくる体制を作っておくことが重要です**

トップがすべての責任を負う

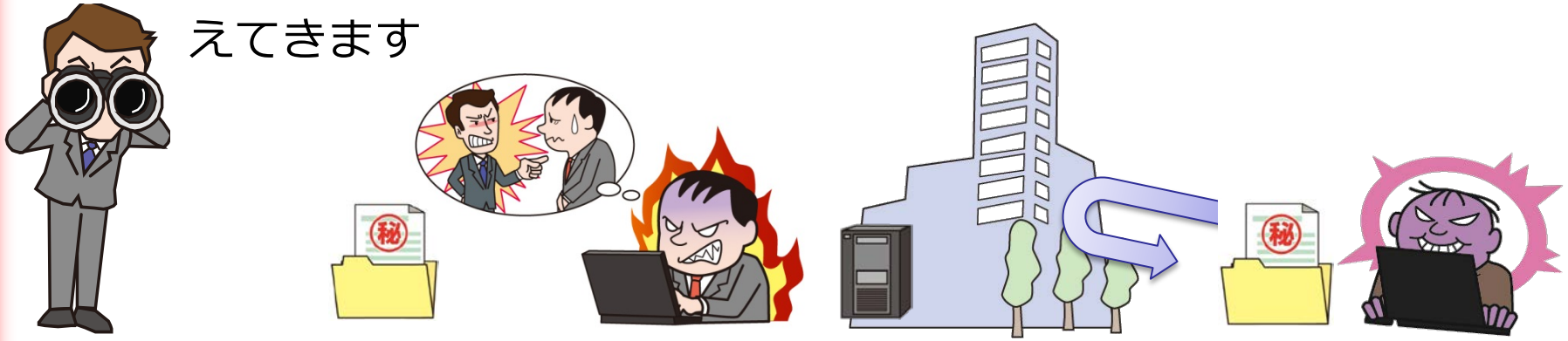


- **指示と報告による組織づくりと責任の明確化**
  - 上司は部下に指示をし、部下はそれが完了したことを報告する。もしも問題がある場合は相談や連絡を行う
- **最終責任は経営陣**
  - ITに関する指示は経営陣が行う
  - それに応えて組織はすべての報告（情報）が経営陣に集まるようにする

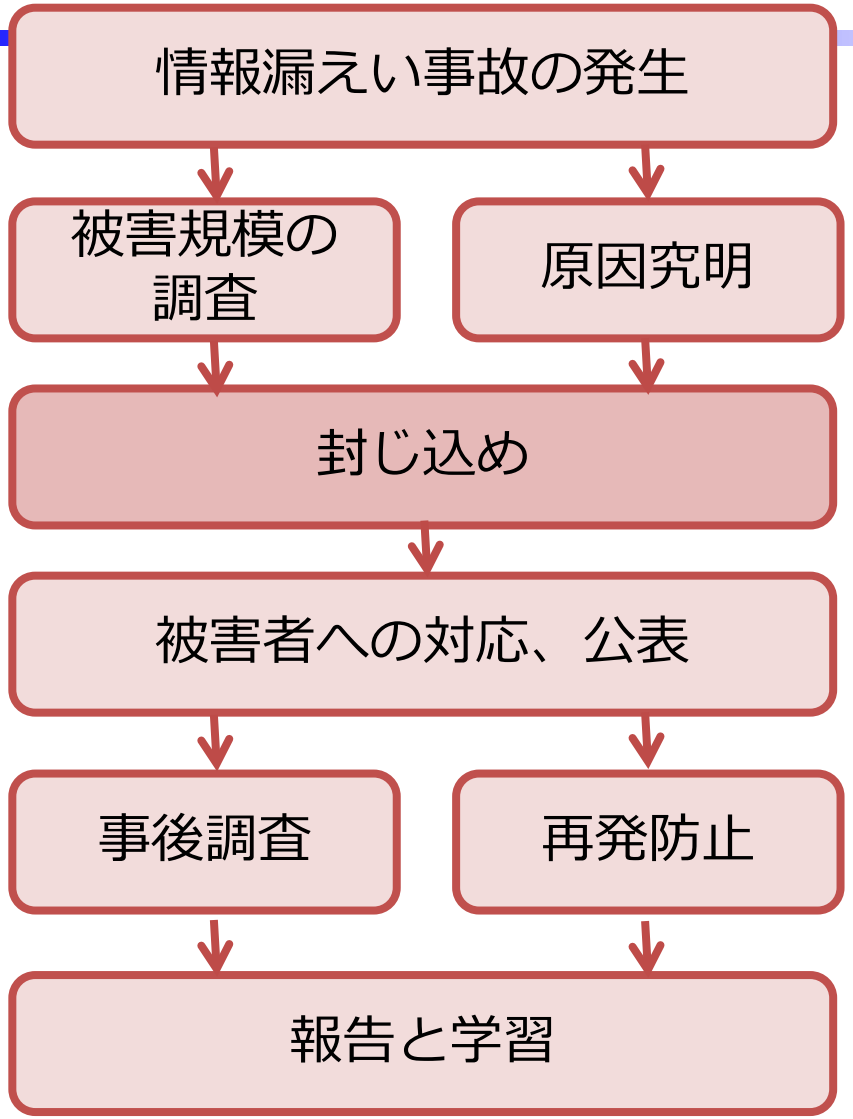
特別損失計上の事態になれば経営を任せたステークホルダー（株主）に対して責任を果たせない！

何を知っておくべきか

- **情報セキュリティにおいては、事故の兆候が把握できるようになることが重要です**
  - 事故が起きる前にはいつもと違ったことが起きていることがほとんどです。事故であっても、犯罪であっても、準備段階で気づくことができれば被害は最小限に収まります
- **日常の監視による把握が重要です**
  - 監視対象が増えると管理が大変になり、管理できない情報が増えてきます



事故対応のスキーム



- **被害の極小化**
  - 事故が発生した時にもっとも重要な事は被害を最小限に抑えること
- **封じ込め・再発防止**
  - まずは被害が大きくならないようにできることを検討する
  - 再発防止のためには十分な情報が必要になる

内部不正の対策

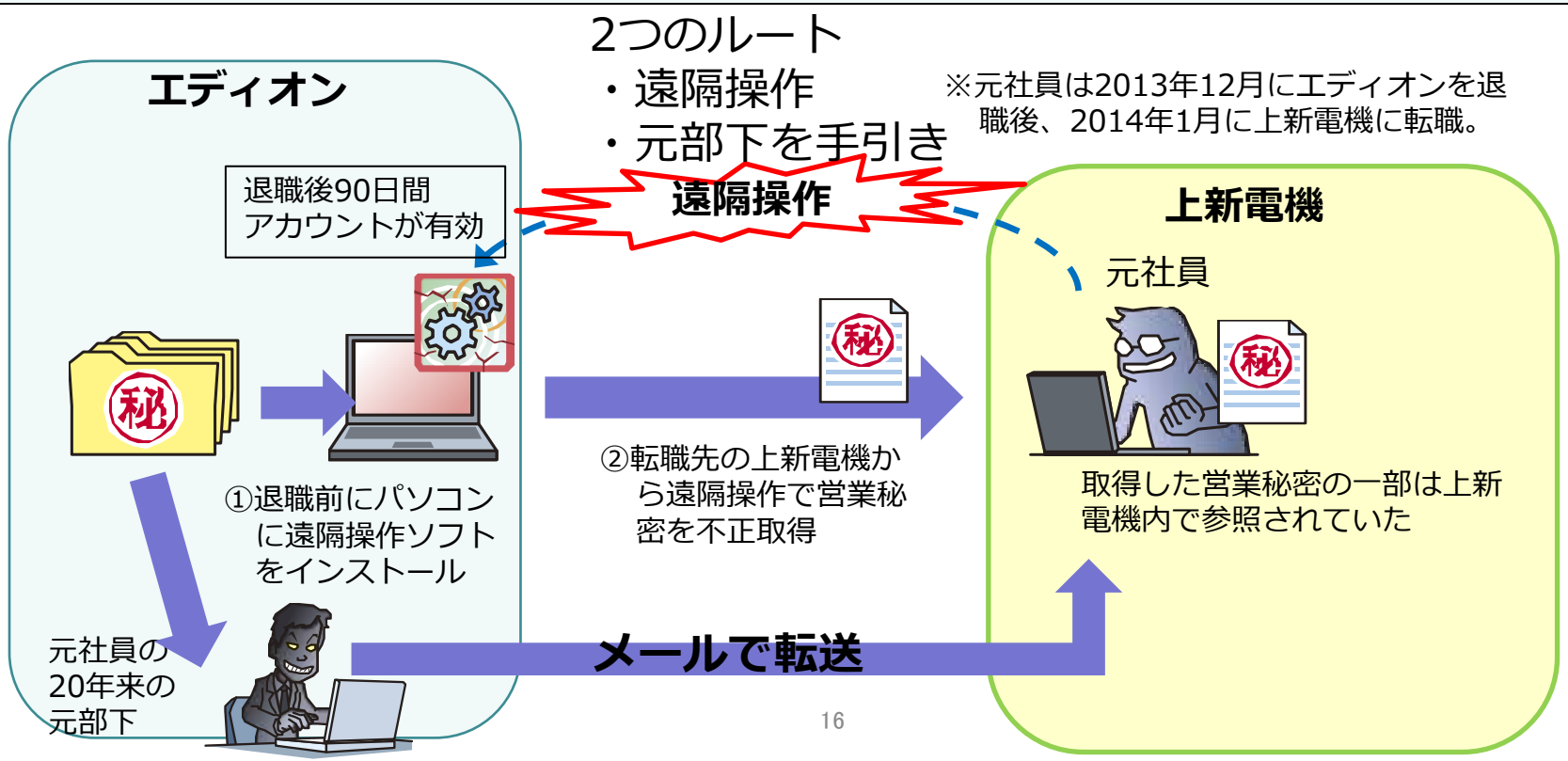
相次ぐ内部不正事件

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～

IPA

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。

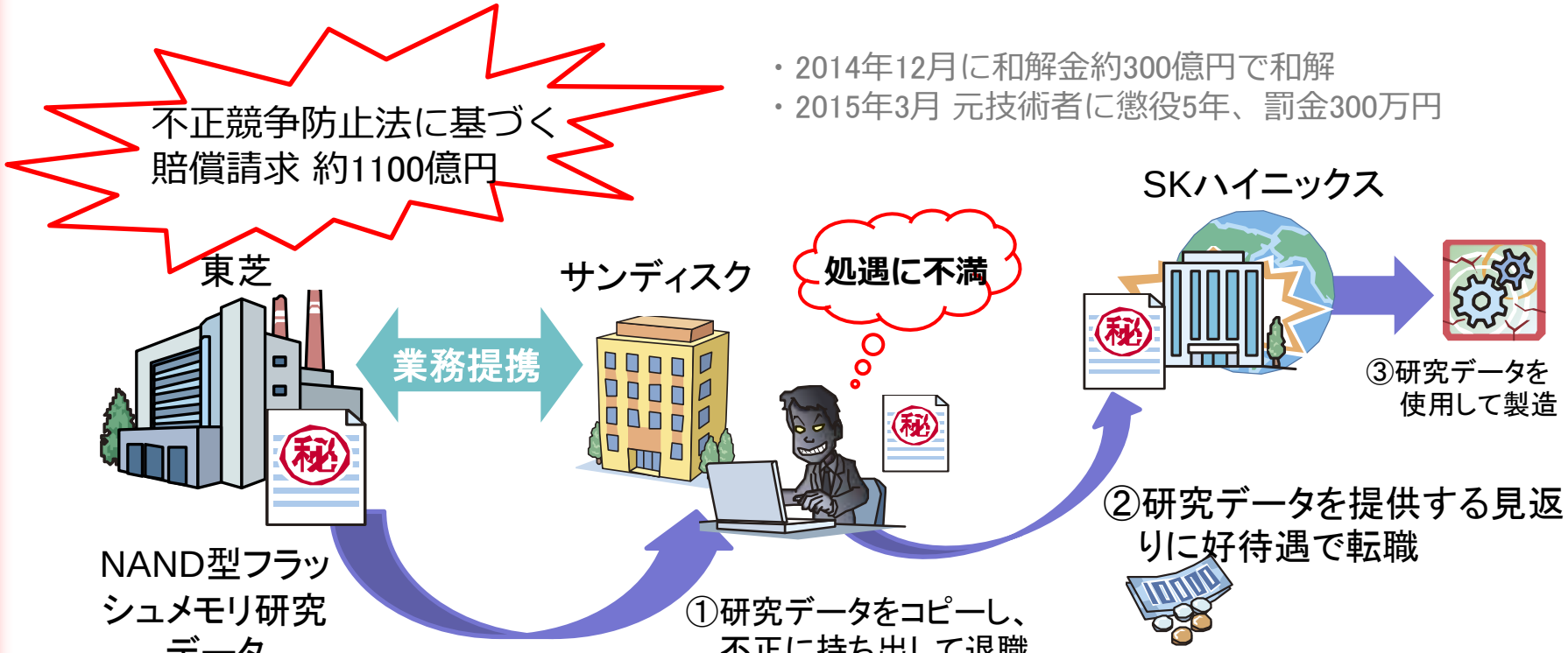
2014年9月25日時点で報道より得られた情報を元に記載

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

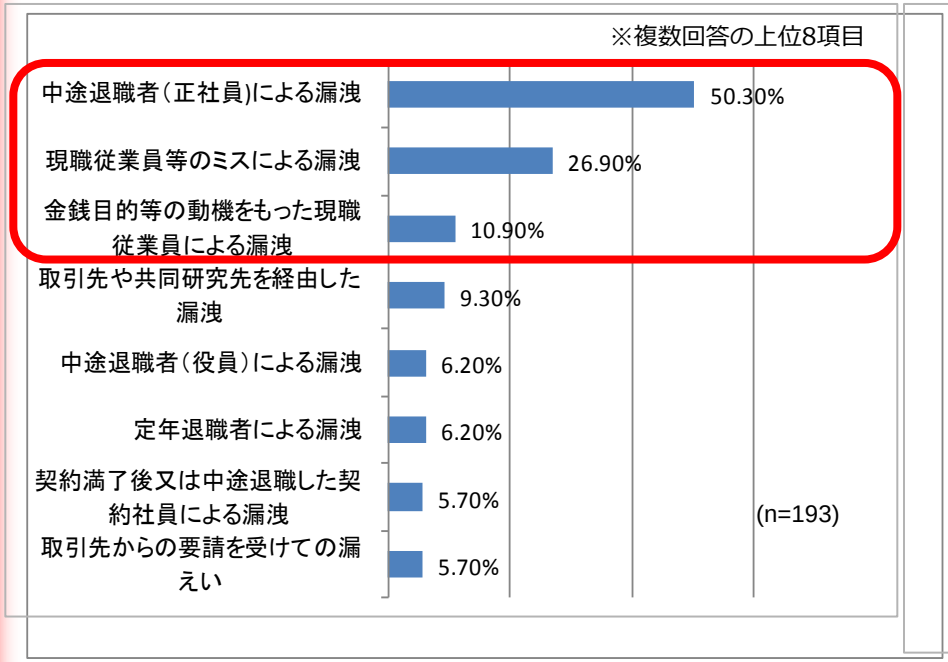
2014年3月、東芝のフラッシュメモリーの研究データを不正に持ち出し、転職先である韓国の半導体大手SKハイニックスに提供したとして、東芝と業務提携していた半導体メーカー サンディスクの元技術者が、不正競争防止法違反（営業秘密開示）容疑で逮捕された。



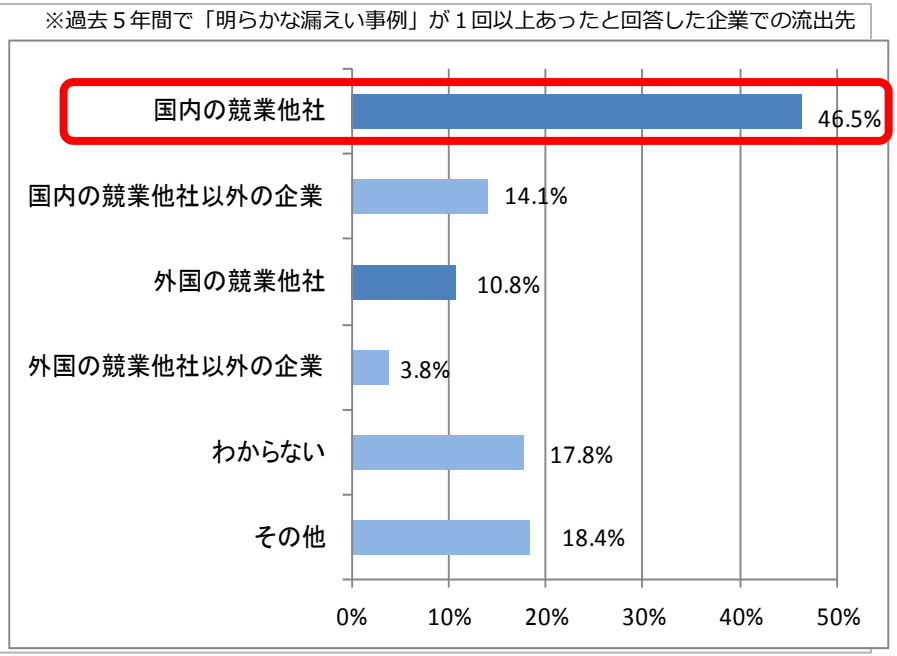
内部不正の状況：
内部者による技術情報流出の実態

- 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）」

内部不正の状況：公表されないことが多い

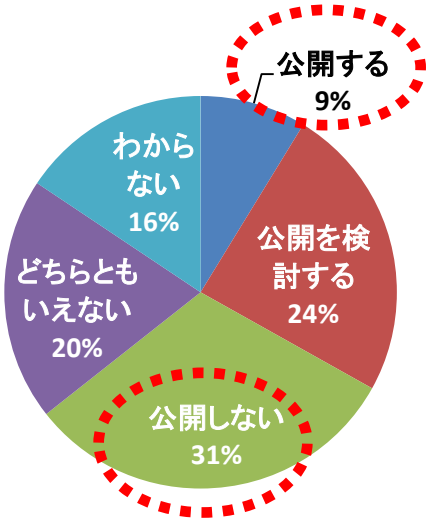
- 組織の**事業の根幹を脅かす**事件が報道されている。
  しかし、公開されている事件は**氷山の一角**
  - 裁判に至らないものや内部規定違反等の事件も多く存在する
- 組織内部で処理され、外部に公開されることは稀

（**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）

内部不正に関する企業の実態：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）

内部不正を防ぐ：
内部不正者への対策方針

- 内部不正を防ぐ**環境**を整備する
  - 動機への抑止効果
    - 犯罪心理学を援用
      - 不正のトライアングル
      - 状況的犯罪防止
  - 職場環境の整備

内部不正者への対策：動機を抑止
不正のトライアングル

IPA

・「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。

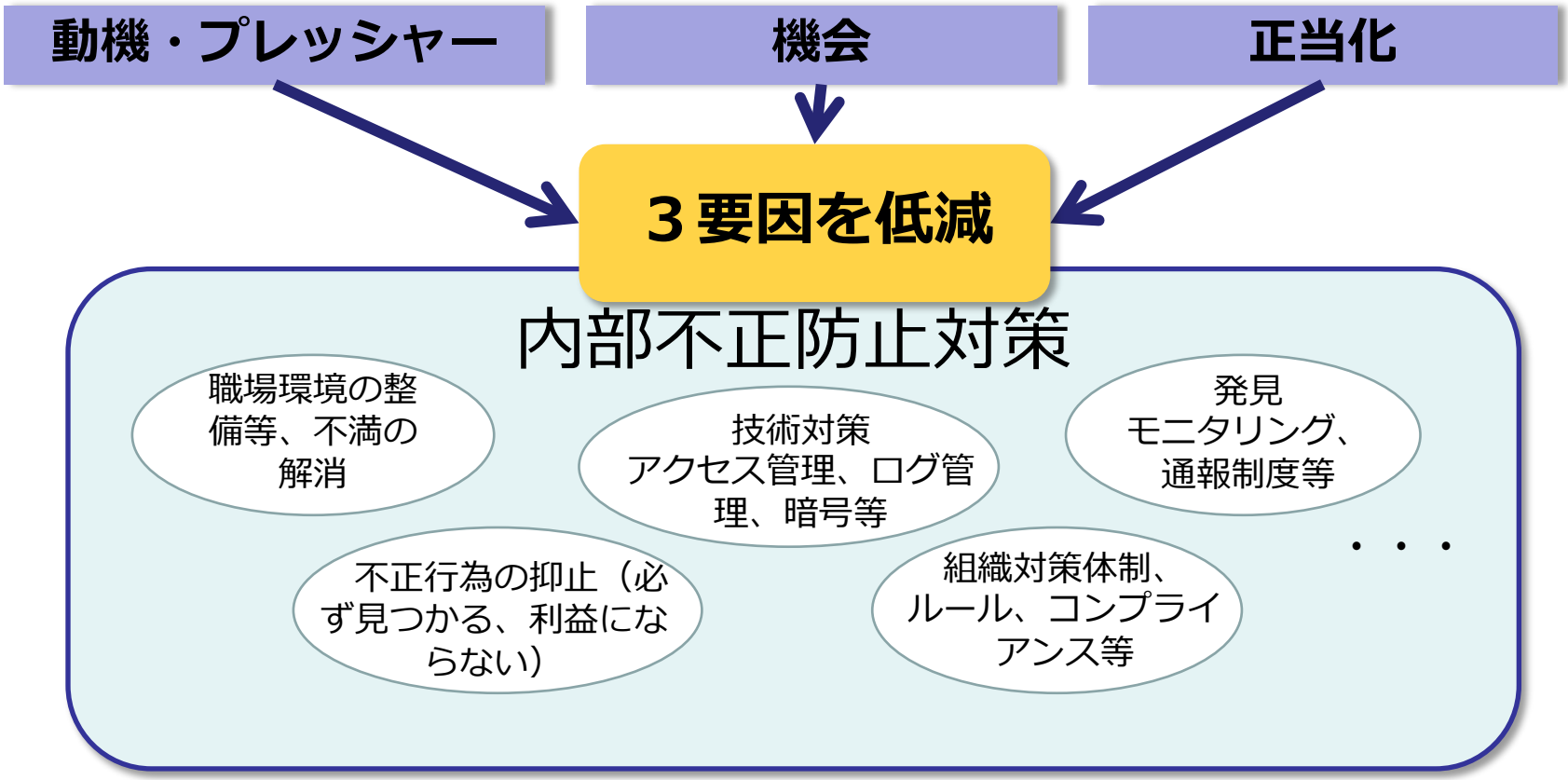
例.

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。**

※ 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。



内部不正防止ガイドライン
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

（付録）「内部不正チェックシート」

※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

外部からの脅威への対策
～標的型攻撃メールを例に～

サイバー攻撃報道事例

不正アクセスといわれている攻撃

標的型といわれている攻撃

IPA

時期	報道
2011/9	三菱重にサイバー攻撃、８０台感染…防衛関連も　（読売新聞等）
2011/11	サイバー攻撃：参院会館のＰＣ、ウイルス感染は数十台に　（毎日新聞等）
2012/2	農水省に標的型メール攻撃、情報流出狙う？　（読売新聞等）
2012/6	パソコン５台、ウイルス感染か＝外部サイトと通信－原子力安全基盤機構（時事通信）
2012/7	財務省ＰＣ数か月情報流出か…トロイの木馬型　（読売新聞等）
2012/9	「中国紅客連盟」の標的か…総務省統計局サイト（読売新聞等）
2012/11	ＪＡＸＡ、ロケット設計情報流出か　ＰＣがウイルス感染　（朝日新聞等）
2012/12	三菱重工もウイルス感染　宇宙関連の情報流出か（産経新聞）
2012/12	原子力機構ＰＣウイルス感染…告発情報漏えい？（読売新聞）
2013/1	農水機密、サイバー攻撃…ＴＰＰ情報など流出か（読売新聞）
2013/2	米マイクロソフトも感染、アップルと似た攻撃（読売新聞）
2013/5	大分空港HP、ウイルス感染させるよう改ざん（読売新聞）
2013/7	朝日新聞記者を装うウイルスメール　国会議員２人に届く（朝日新聞）
2013/10	セブン通販サイトに不正アクセス　１５万人の情報流出か（朝日新聞）
2014/1	「角川」サイト改ざん　閲覧でウイルス感染の恐れ（朝日新聞）
2014/9	法務省に不正アクセス　情報流出の可能性（日経新聞）
2014/10	JALの情報漏洩、4131件を特定　増える可能性も（日経新聞）
2015/1	朝日新聞社でPC17台がウイルス感染、外部サーバー通じ1カ月以上情報が漏洩（日経）
2015/3	成田空港:ホームページ改ざんされ閉鎖（毎日新聞）
2015/4	富山県運営ＨＰ改ざん　個人情報入力画面に誘導（産経新聞）
2015/6	不正アクセスで年金情報１２５万件が流出か（NHK）
2015/6	標的型メール、東商も被害…１万件超情報流出か（読売新聞）

日本年金機構の情報漏えい事件(2015.6)

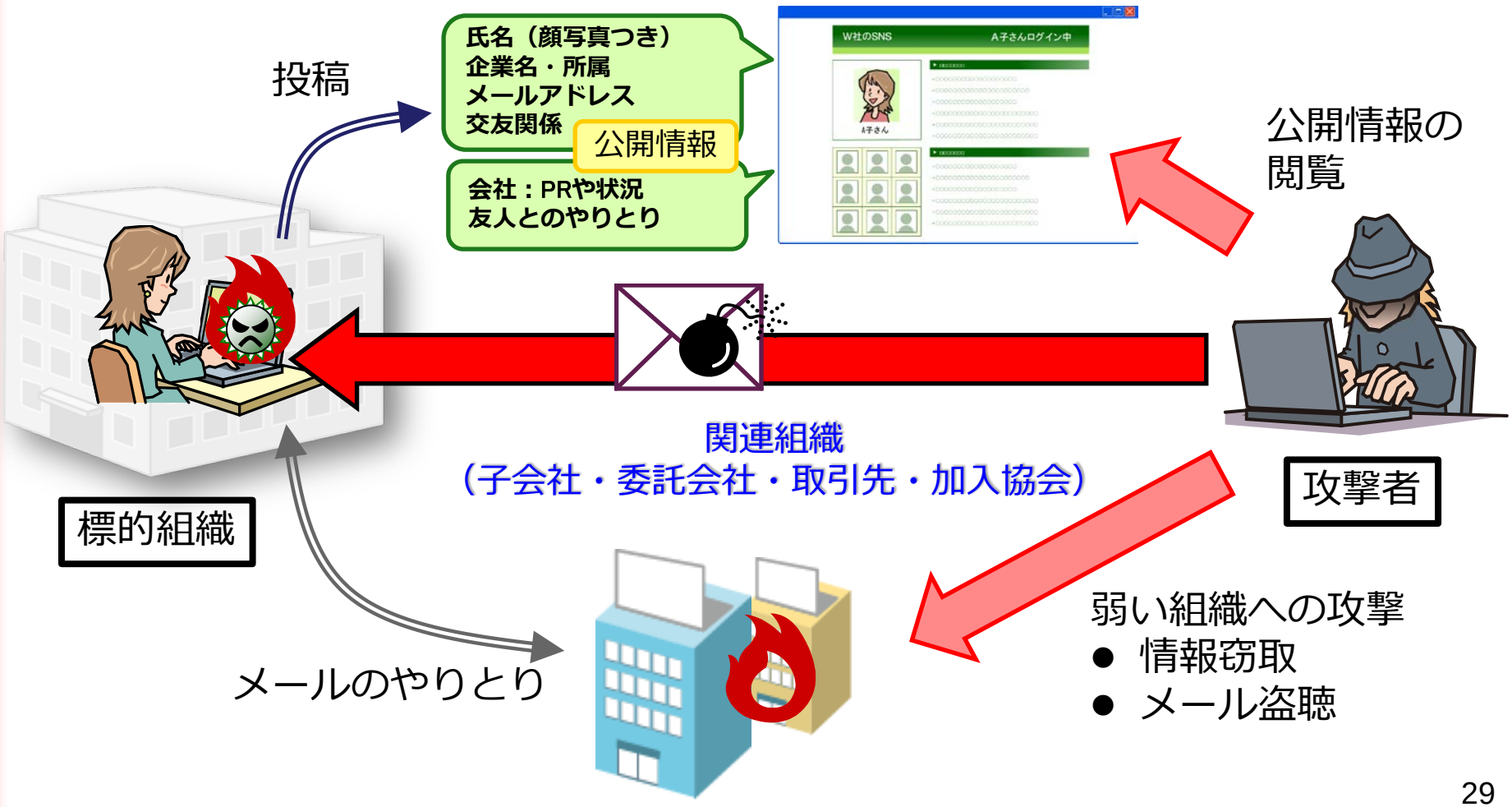
- ウイルス感染により年金情報などが窃取
- セキュリティ上の課題
  - 認証サーバの脆弱性対策が不十分
  - すべての端末においてローカル管理者権限のID・パスワードが同一であった
  - インシデント発生時に責任者への報告がなされていなかった
  - 情報系ネットワークの多重防御の取り組みが不十分

リスク管理においてサイバー攻撃を想定した
具体的な対応について、明確化されていない

（出展）サイバーセキュリティ戦略本部「日本年金機構における個人情報流出事案に関する原因究明調査結果」

サイバー攻撃に向けた標的の調査

攻撃者は、標的の身辺を事前に調査し攻撃を仕掛ける

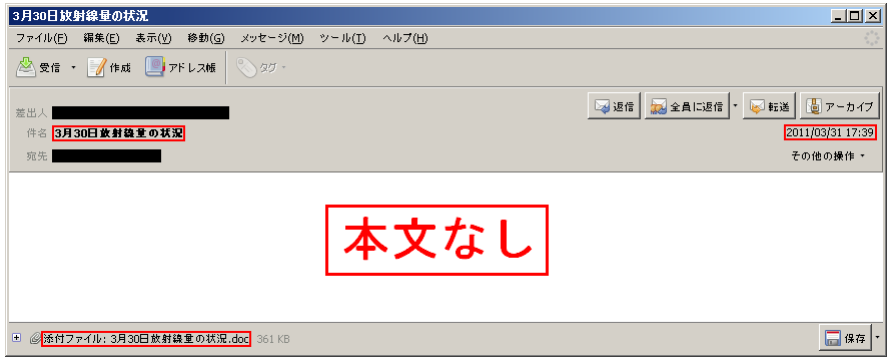


標的型メール攻撃　実際のメール文面

- IPAに届出のあったメールの場合

◇メールタイトル：3月30日放射線量の状況
◇メール本文内容：<本文なし>
◇添付ファイル名：3月30日放射線量の状況.doc

送信時期：2011年4月
興味の持たれそうなタイトルやファイル名を
使っていた

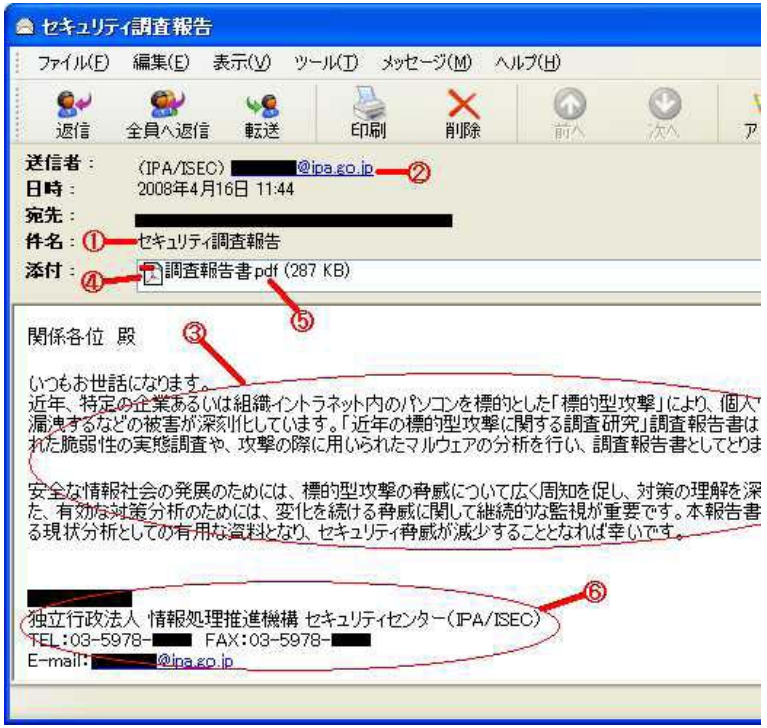


- IPAを騙ったメールの場合

◇（偽装された）差出人：IPAのメーリングリスト
◇メール本文内容：
　・実際にIPAがウェブ等で発表した内容
　・実際の職員の名前
◇添付ファイル名：調査報告書概要

差出人をIPAとして実際に発表した内容を流用

これらのほかにもIPAでは実在の職員を詐称した
メールが届いたことも。



攻撃者「X」の概要 （１）

※ J-CSIP： IPAが運営している、国内重要産業の企業・組織間の情報共有体制

3年間のJ-CSIPの活動で、「標的型攻撃メール」と見なした数、939通

この情報を横断的に分析し、複数の観点で攻撃間の関連性を分析

同一の攻撃者によるものと推定する114通（全体の12%）のメールを抽出

攻撃者「X」

攻撃者「X」の概要 （2）

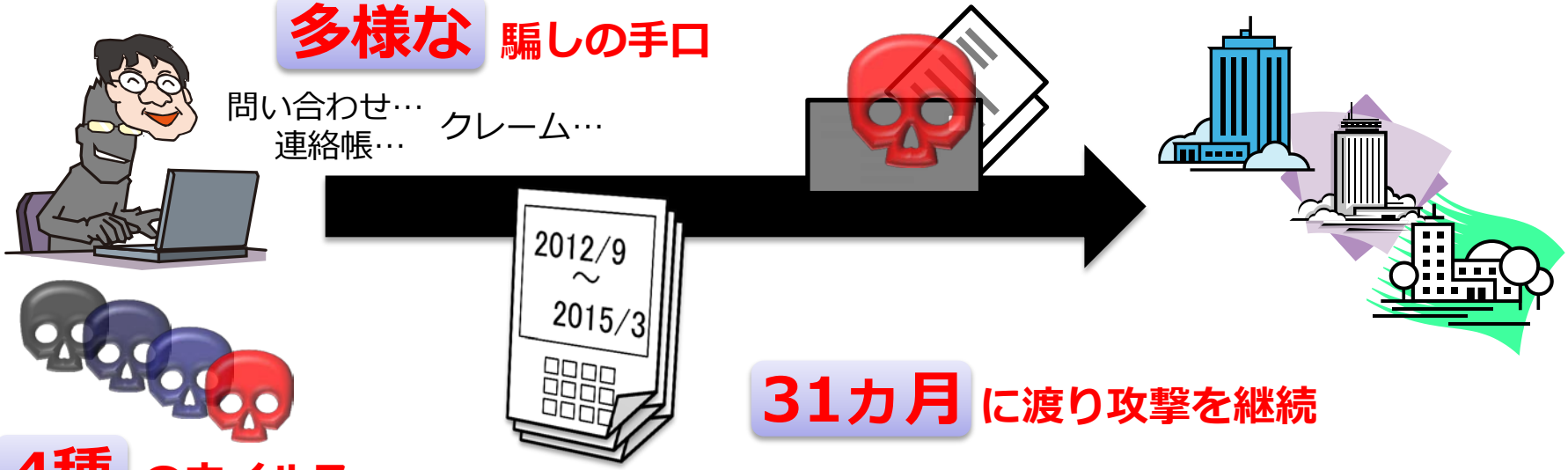
IPA

攻撃者「X」

114通 の攻撃メール

9組織 へ攻撃

多様な 騙しの手口



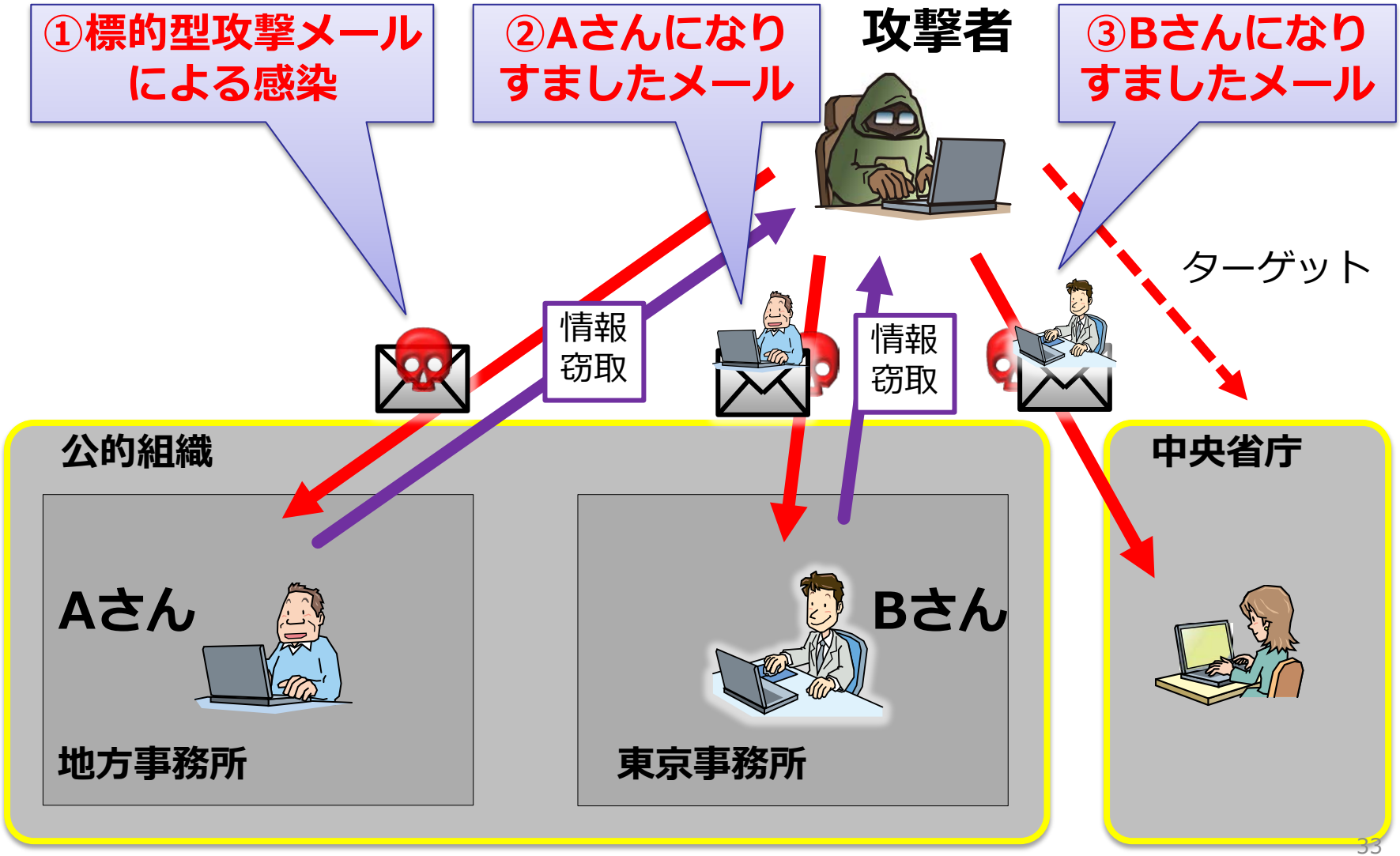
31カ月 に渡り攻撃を継続

4種 のウイルス

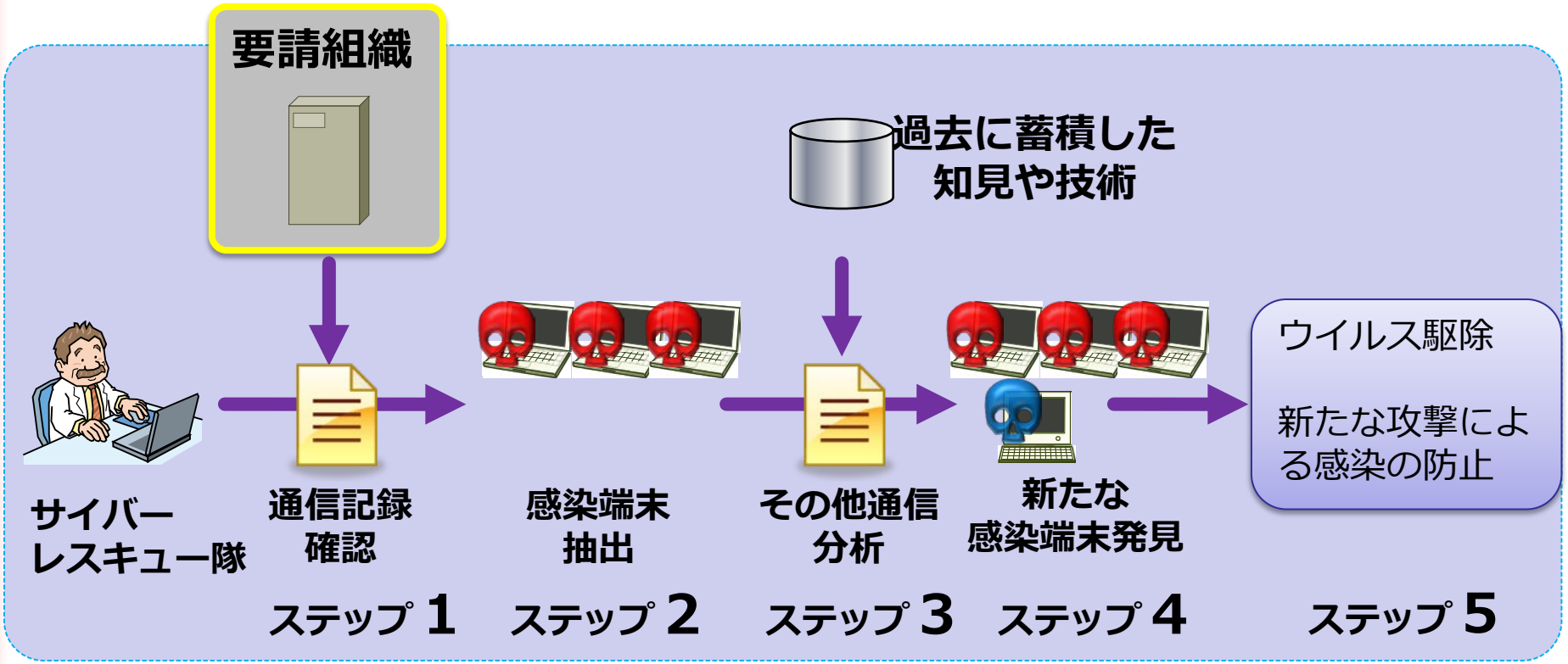
浮かび上がった執拗な攻撃者の存在

手を替え品を替えつつ長期に渡り確認されてきた114通の攻撃メールは、何らかの共通点によって互いに関係あり

サイバーレスキュー隊
が対応支援した攻撃事例



サイバーレスキュー隊(J-CRAT)
レスキューの流れ



出動

調査開始
感染確認等

分析
被害把握・証拠保全等

暫定対策
被害拡大防止

基本的な対策

- **怪しいメールではないか、常に注意を心掛ける**
- **ＯＳやアプリケーションは常に最新な状態にする**
  - ＯＳ：Windows や MacOS など
  - アプリケーション：Adobe Reader、Adobe Flash Player、JRE、プラグインソフトなど
- **ウイルス対策ソフトを利用**
  定義ファイルは最新化
  サポート期限切れの状態では使わない

標的型攻撃対策の参考資料

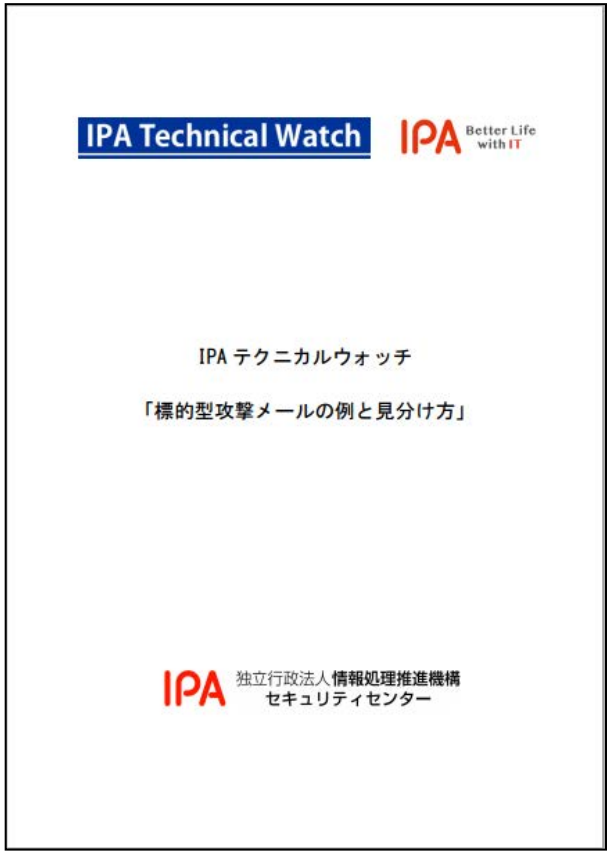
- **IPAテクニカルウォッチ**

「標的型攻撃メールの例と見分け方」

https://www.ipa.go.jp/security/technicalwatch/20150109.html

– メールの見分け方
  - 注意するときの着眼点
  - 標的型攻撃メールの例
  - 添付ファイルの種類と解説

６月以降、ダウンロードが急増！
累計10万件以上のダウンロード：
・組織での教育素材に
・個人のリテラシー向上に
ご活用下さい。



標的型攻撃対策の参考資料

- **『高度標的型攻撃』対策に向けたシステム設計ガイド**
  http://www.ipa.go.jp/security/vuln/newattack.html

  – 情報システム内部に深くに侵入してくる高度な標的型攻撃に対してシステム上の設計策を説明した資料。

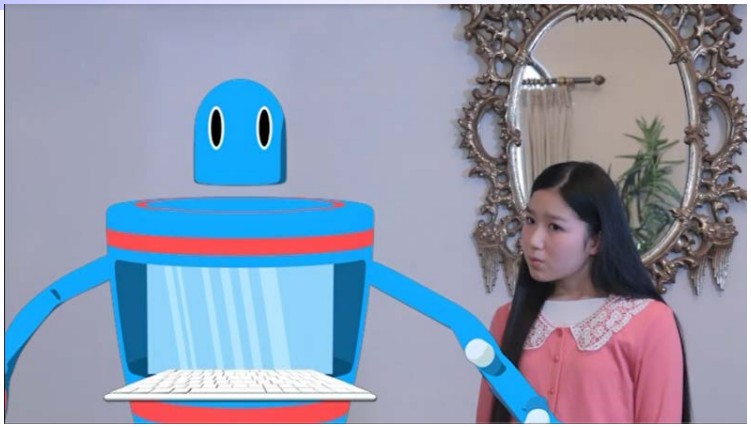
本日のまとめ

- 情報セキュリティにおける判断を経営陣が適切に行うことができるように、情報セキュリティに関する情報がトップまで上がるような仕組みづくりを心がけましょう
- また、事故にすぐに気がつくことで被害を極小化することが出来ます。事故が発生していること、事故が起きる兆候を感じ取ることができるようなモニタリングの仕組みを構築しましょう

映像で知る情報セキュリティ

～約10分間のドラマ・アニメ・ドキュメンタリー等を通して情報セキュリティを学べる～

情報を漏らしたのは誰だ?
～内部不正と情報漏えい対策～



陽だまり家族とパスワード
～自分を守る３つのポイント～

検証！
スマートフォンのワンクリック請求

情報セキュリティに関する脅威や対策などを学んで頂くための映像コンテンツを、YouTube内の「IPA Channel」を通じて公開しています。（全13作）
社内研修などでご活用下さい。
映像を収納したDVD-ROMでも配布しています。
（標的型/スマホ/SNS/新入社員向け等）

セキュリティ研修にご利用ください

そのままセキュリティ研修に使える情報が満載です。

http://www.ipa.go.jp/security/antivirus/shiori.html

Windows Server 2003のサポート終了に伴う注意喚起

Windows Server 2003のサポートが、2015年7月15日に終了しました。

サポート終了後は修正プログラムが提供されなくなり、脆弱性を悪用した攻撃が成功する可能性が高まります。

サポートが継続しているOSへの移行検討とOS移行に伴う周辺ソフトウェアの影響調査や改修等について計画的に迅速な対応をお願いします。

脆弱性を
悪用した攻撃

- 業務システム・サービスの停止・破壊
- 重要な情報の漏えい
- データ消去
- ホームページの改ざん
- 他のシステムへの攻撃に悪用

会社の事業に悪影響を及ぼす被害を受ける可能性があります

詳しくは　IPA　win2003　検索

またWindowsXPを利用されている方はサポートが継続しているOSへの移行検討をお願いします

情報セキュリティに関する新たな国家試験！

情報セキュリティマネジメント試験

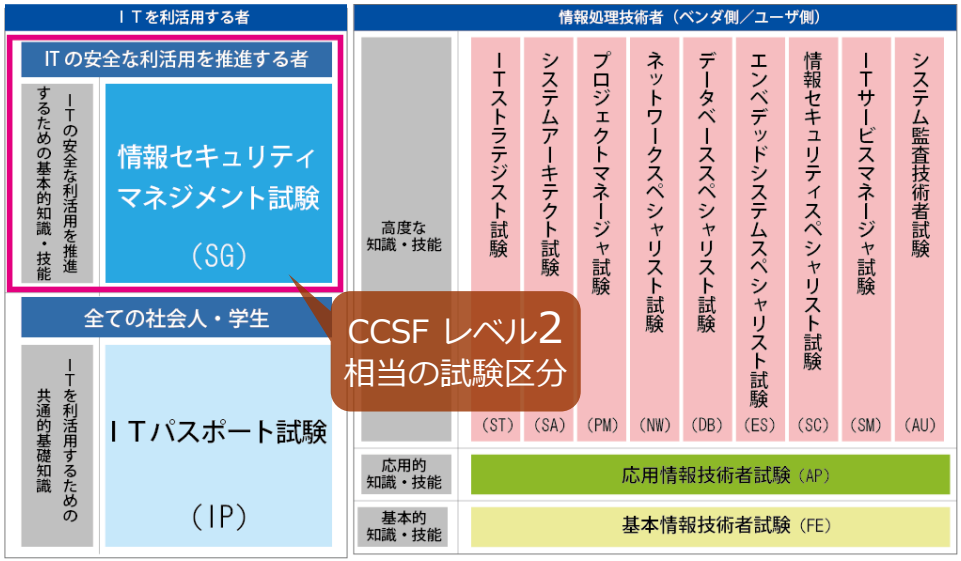
IPA

情報セキュリティマネジメント試験とは

情報セキュリティマネジメントの計画・運用・評価・改善を通して組織の情報セキュリティ確保に貢献し、脅威から継続的に組織を守るための基本的スキルを認定する試験

試験の位置づけ

経済産業省所管の国家試験である**「情報処理技術者試験」の新たな試験区分として創設。**



試験時間・出題形式

時間区分	試験時間	出題形式	出題数 解答数	基準点
午前	90分	多肢選択式 （四肢択一）	50問 50問	60点 （100点満点）
午後	90分	多肢選択式	3問 3問	60点 （100点満点）

更に詳しく知りたい方へ

新試験がわかるパンフレット

職場の情報セキュリティ管理者育成に！

職場の情報セキュリティ管理者のための**スキルアップガイド**

情報セキュリティ**スキルアップハンドブック**

新試験の対象者像を踏まえ作成

実施時期（予定）

- 開始：**H28年度春期**
  （申込受付：2016年1月中旬開始予定）
- 春期・秋期の**年2回**
  （春期：4月第3日曜、秋期：10月第3日曜）

IPA

ITパスポート試験

あなたのＩＴ力を証明する国家試験

ITパスポート公式キャラクター
上峰亜衣（うえみねあい）

【プロフィール：マンガ】 https://www3.jitec.ipa.go.jp/JitesCbt/html/uemine/profile.html

「ｉパス」は、ITを利活用するすべての社会人・学生が備えておくべきITに関する基礎的な知識が証明できる国家試験です。

お問い合せは

独立行政法人 情報処理推進機構
セキュリティセンター

〒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/