IPA Information-technology Promotion Agency, Japan

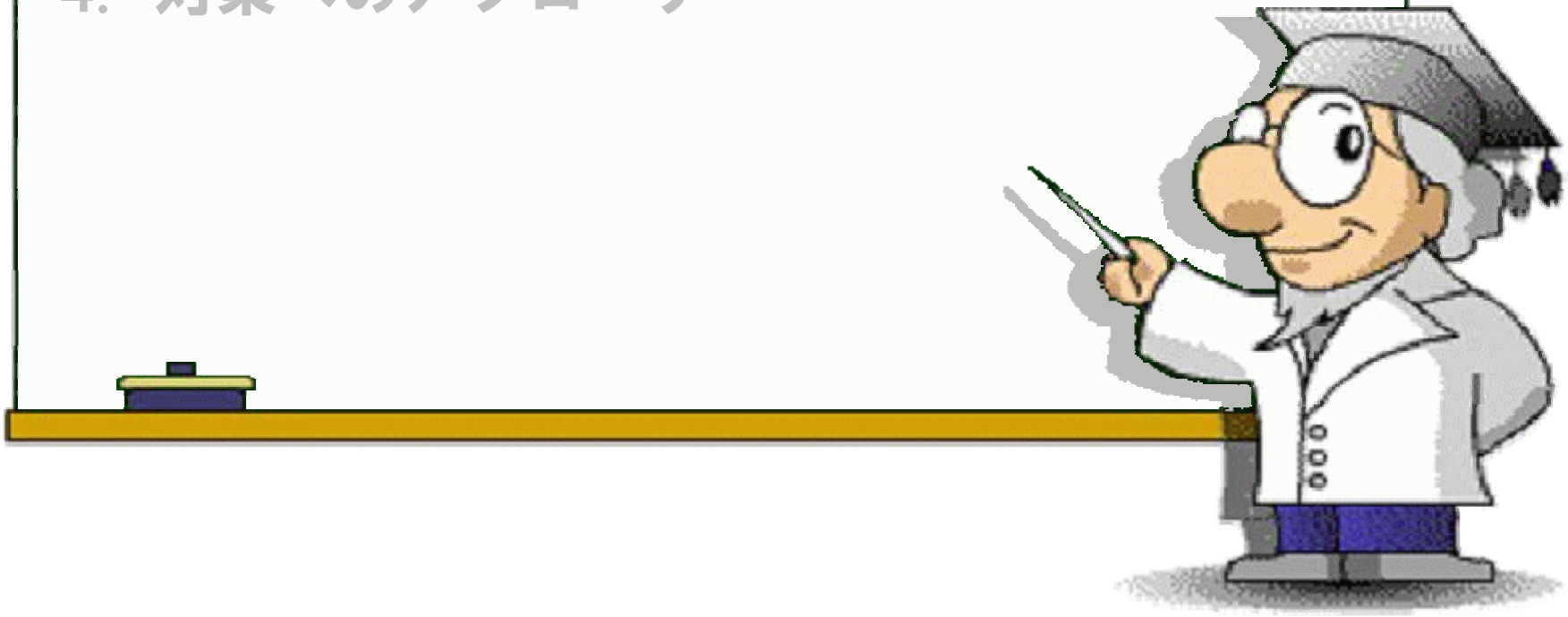
# 標的型攻撃の脅威とセキュリティ対策
## ～サイバー攻撃のデモ実演～

2012年11月17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
研究員　渡辺 貴仁

# 目次

1. サイバー攻撃について
2. 標的型攻撃（新しいタイプの攻撃）とは
3. 新しいタイプの攻撃のモデル
4. 対策へのアプローチ



# サイバー攻撃報道事例

| 時期 | 報道 |
|---|---|
| 2011/5 | 韓国の農協でシステム障害（読売新聞等） |
| 2011/4-5 | ソニーにサイバー攻撃、個人情報流出1億件超（朝日新聞等） |
| 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） |
| 2011/9 | IHIにもサイバー攻撃　日本の防衛・原発産業に狙いか（産経新聞等） |
| 2011/10 | 衆院にサイバー攻撃　議員のパスワード盗まれる（朝日新聞等） |
| 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） |
| 2012/1 | JAXA：職員のパソコン感染、無人補給機情報など流出か（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） |
| 2012/2 | 特許庁、トロイの木馬型感染…メール情報流出か（読売新聞等） |
| 2012/3 | 国際協力銀行の顧客220社とのメール流出（毎日新聞等） |
| 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） |
| 2012/10 | 不審メール:内閣府を名乗り、県に　／徳島（毎日新聞） |

# サイバー攻撃の発生事例①

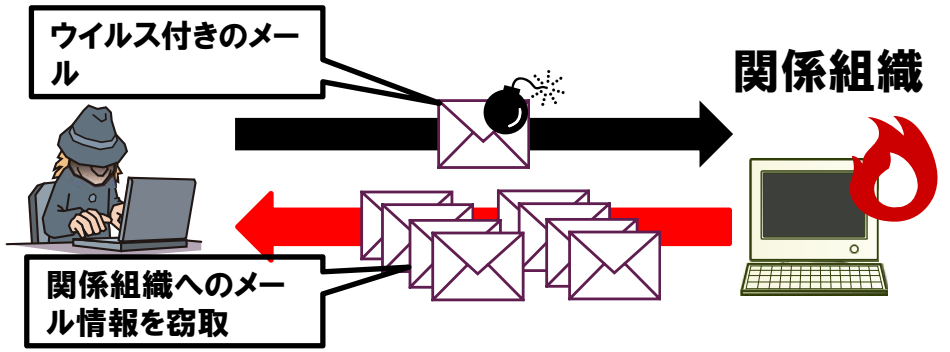
## ～防衛産業に対する標的型攻撃～

IPA

## ■ 国内の大手総合重機メーカに対する標的型攻撃（2011年9月）

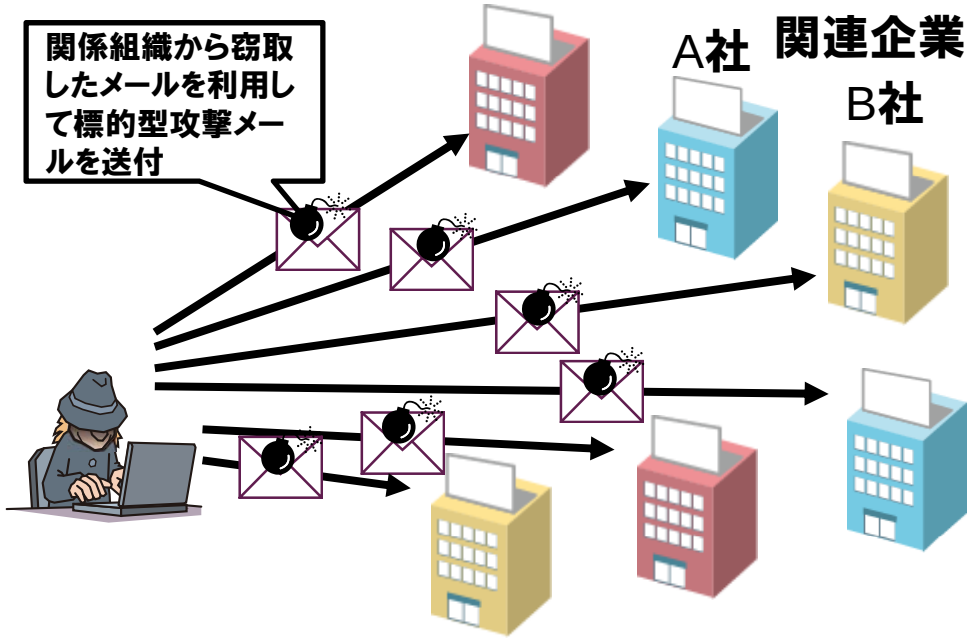
**■ 攻撃①**

**関係組織の職員のPCがウイルスに感染させ、大手総合重機メーカとのやりとりメールを盗んだ。**




**■ 攻撃②**

**攻撃①の10時間後、関連企業に対し、盗んだメールを利用した標的型攻撃メールを送付した。**






※複数の報道から導き出したシナリオです。

# サイバー攻撃の発生事例①

## ～防衛産業に対する標的型攻撃～

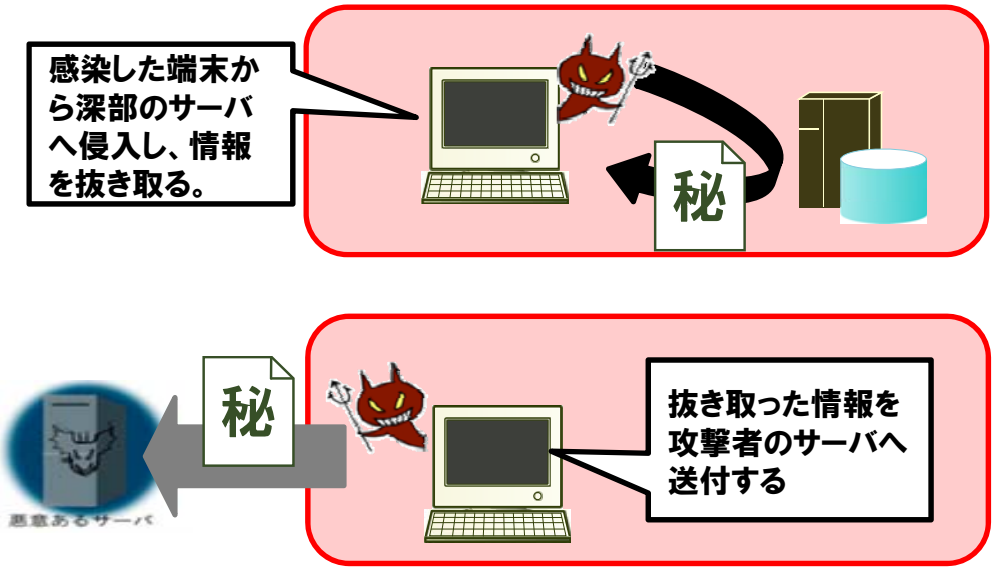
IPA

■ 被害

事象：ウイルスは広域に社内拡散

事業所数11拠点
感染数：83台のPCやサーバ
外部通信を行う

端末に感染したウイルスが**内部サーバに侵入**し、**原発・防衛関連情報**を**攻撃者（米国サーバ）へ送付**する。




同社の愛知の拠点のサーバへ情報が集約され送付された

※複数の報道から導き出したシナリオです。

組織内に巧妙なルートで侵入され、
- 組織内拡散
- 組織内調査
- 重要サーバへの不正アクセス

による・・・

**組織の重要情報（知的財産、顧客情報等）を狙われる事件**が顕在化

# サイバー攻撃の発生事例②

## ～攻撃された後、外部への攻撃に使われたと思われるケース～

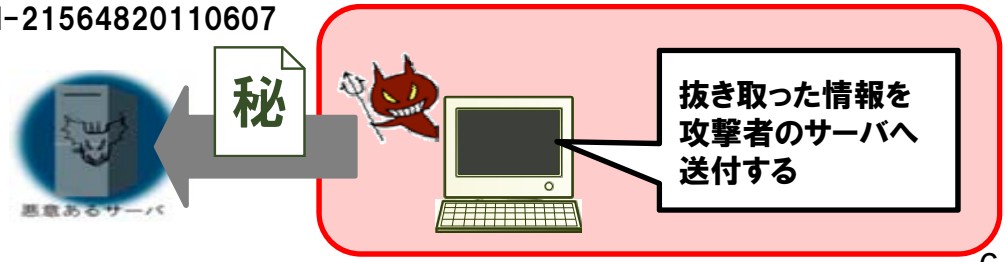
■ EMC Corporationのセキュリティ事業部門であるRSAのSecurIDに関する情報が盗まれたケース

「Anatomy of an Attack」
http://blogs.rsa.com/rivner/anatomy-of-an-attack/

① 従業員宛に標的型攻撃メールを送付
② 添付ファイルはExcelのゼロデイの脆弱性を狙うウイルス
③ 従業員がクリックして感染し、**バックドア**を作成される
④ ネットワーク情報を収集し、更に権限の高いアカウント情報を取得
⑤ 収集したアカウント情報を利用し、ターゲットのサーバへ侵入
⑥ サーバから機密情報(RSA SecurIDの製品情報と言われている)を取得
⑦ ⑥の情報を外部サーバ(侵入されたホスティング業者のサーバ)へ送付
⑧ 攻撃者が情報を取得後、外部サーバから痕跡を消去

● また、ロイター通信の報道によると、RSAから盗んだ情報を利用しロッキード・マーチンへの攻撃に使われたと報道されている
http://jp.reuters.com/article/topNews/idJPJAPAN-21564820110607

※RSA SecurID:
EMC Corporationのセキュリティ事業部門であるRSAの展開しているサービスであるワンタイムパスワードシステム。



# サイバー攻撃の発生事例③

■ 韓国農協(金融業務)が攻撃を受ける(2011年4月)

- 攻撃経路:
  - ウェブハードサイト(ウェブ経由のファイル共有サイト)
    - 農協ネットワークシステムの外部委託業者がウェブサイト経由でマルウェアに感染
- 攻撃の結果:
  - 電算ネットワークのデータが大量に破壊され、数日にわたって業務不能状態へ。
    - 農協のバックアップされたデータも削除
    - 一部のデータは復旧不可能な状況へ

# サイバー攻撃の変遷

## ～ 攻撃手法の巧妙化だけでなく攻撃者像も変化 ～

IPA

### ■ 攻撃者の狙い

いたずら目的<br>顕示欲の誇示 → 金銭目的（犯罪）<br>サービス妨害（嫌がらせ） → スパイ・諜報活動<br>機密情報の窃取

### ■ 攻撃者像

攻撃者1人<br>セキュリティ技術者 → グループ<br>犯罪者 → 国家？・Hacktivist・<br>犯罪プロ集団

### ■ 攻撃手法

不正侵入 → Botnet<br>Spamメール → 標的型・シーケンシャル<br>マルウェア

※ソーシャルエンジニアリングによる、ウェブ、メール、USB等経由の攻撃へ

### ■ ビジネスインパクト

- 個人情報流出 ⇒ 企業の社会的責任
- 知的財産情報の窃取 ⇒ 企業の競争力低下、国家の危機管理問題へ
- 制御機器やシステム停止 ⇒ 企業の競争力低下、サプライチェーンの崩壊、社会インフラの混乱、国家の危機管理問題へ

# サイバー攻撃の種類（攻撃者像から）

## 1.諜報活動をする者？

**目的**
情報窃取が主な目的
（情報破壊等もあり得る）

**手法**
標的型攻撃メール
組織内ネットワークへ侵入

**事例**
大手重工関連企業
衆議院・参議院

## 2.共通思想集団（Hacktivist）

**目的**
独自の主義主張

**手法**
サーバへのDDoS攻撃
サーバから情報窃取
SNSで勢力拡大

**事例**
Anonymous, Lulzsec
ゲーム会社への攻撃

## 3.詐欺集団（従来からの攻撃の1つ）

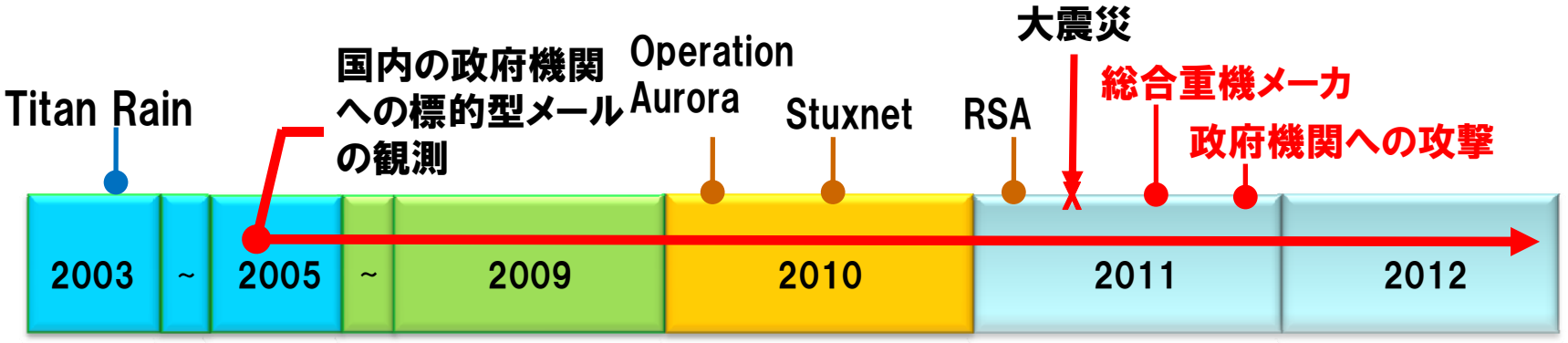
**目的**
金銭目的

**手法**
フィッシング詐欺
マルウェア感染
（クレジットカード番号取得等）

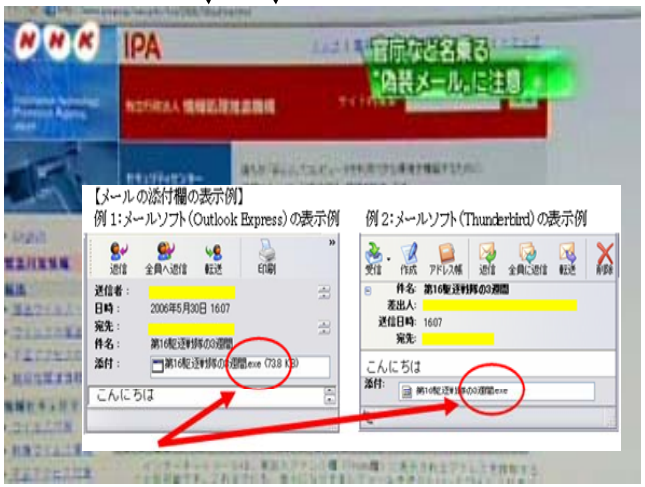
**事例**
一般ユーザのウイルス感染
決済サイトへの攻撃
ショッピングサイトへの攻撃

# 標的型攻撃メールはいつからあった？

## ～10年前から行われている攻撃～



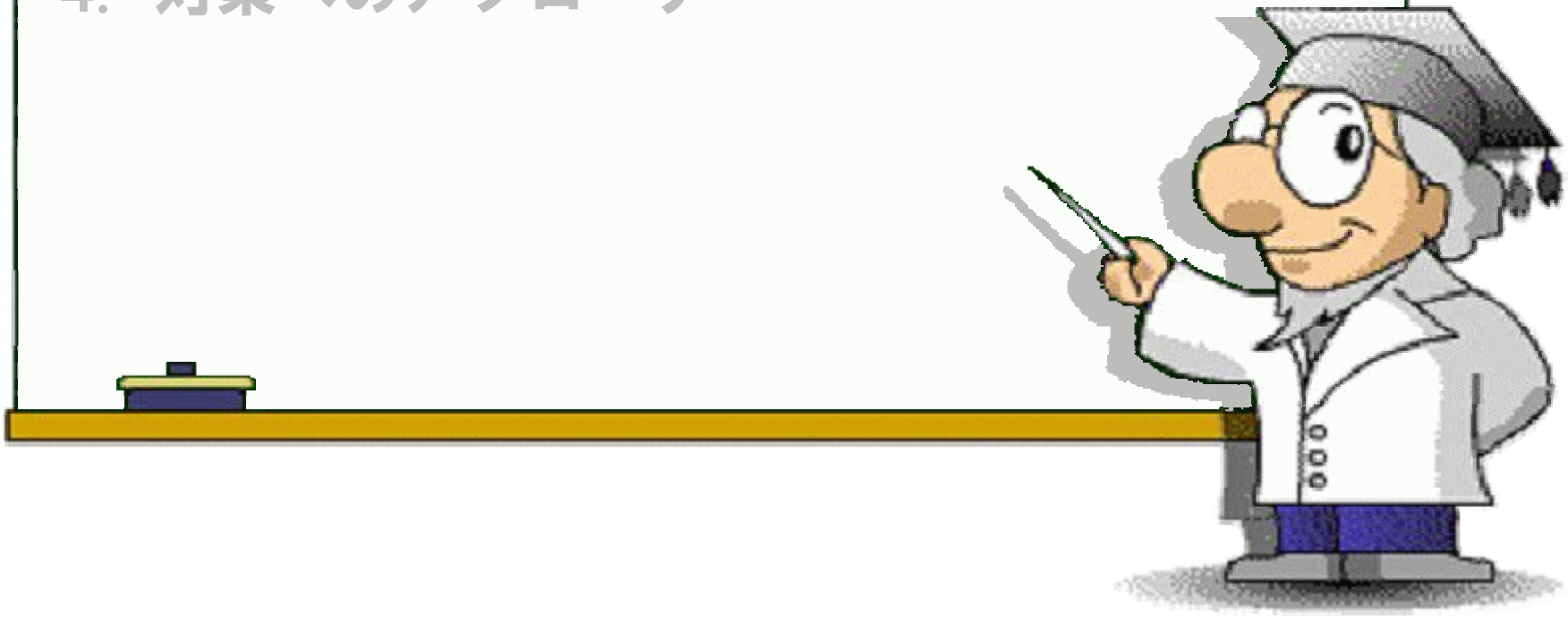

2006/5/30




- 10年間攻撃が続いており、被害が食止められていない現実
- ここ2年間で攻撃による被害が顕在化してきた

# 目次

1. サイバー攻撃について
2. **標的型攻撃（新しいタイプの攻撃）とは**
3. 新しいタイプの攻撃のモデル
4. 対策へのアプローチ



# 『標的型攻撃』とは？

IPA

## ■標的型攻撃の特徴

- ■巧妙（ソーシャルエンジニアリング）
- ■とにかくしつこい（執拗）
  - ■1回の攻撃で終わりではない。何度も何度もやってくる。
  - ■組織のネットワークに忍び込んでいる。（何か月から何年の単位で徐々に攻撃を行う）
- ■組織の活動に被害をもたらしかねない情報を窃取される（もしくは破壊される）

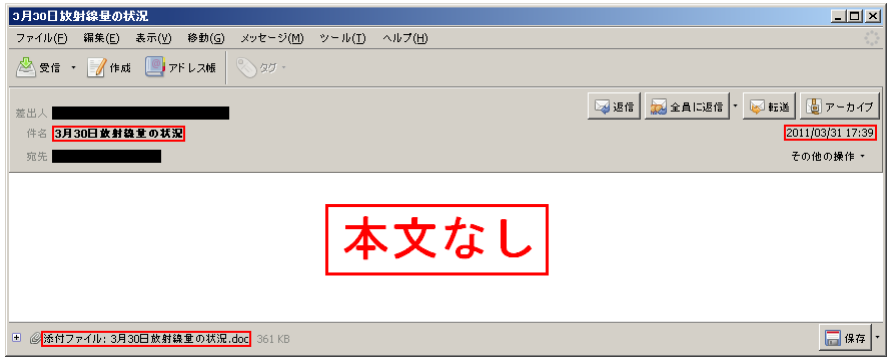
- ■ 海外での呼び方
  - ■ APT（Advanced Persistent Threat：先進的でしつこい脅威）
  - ■ Cyber Espionage：サイバー空間におけるスパイ活動
- ■ 色々な日本語訳もあります
  - ■ 標的型攻撃（標的型サイバー攻撃）
  - ■ 持続的標的型攻撃
  - ■ 新しいタイプの攻撃（IPA）

# 『標的型攻撃』の実際のメール文面

## ● 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月で
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

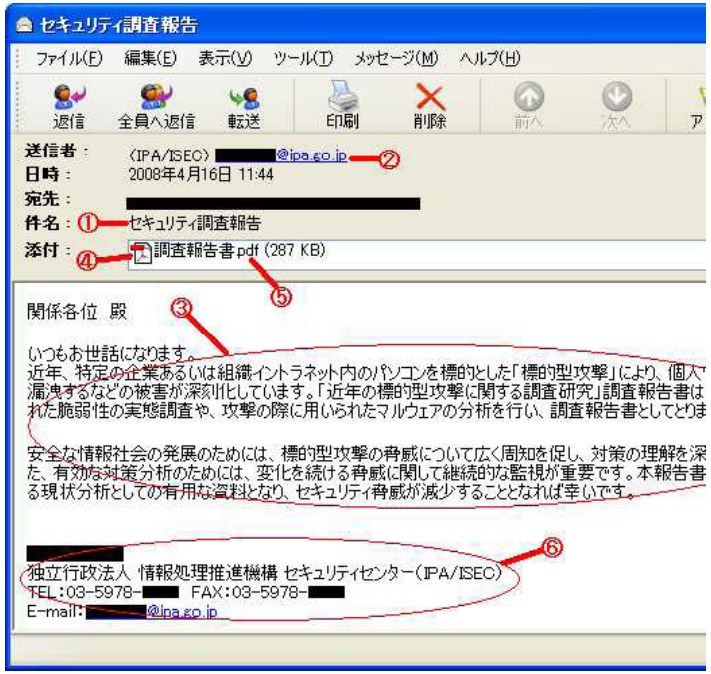



## ● IPAを騙ったメールの場合

◇(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
および、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。



# 巧妙な添付ファイル

## ～メール本文で受信者の興味を引き、既知の脆弱性を悪用～

IPA

## ■ メールに添付されていたドキュメント・ファイルの一例

| 検知日 | 添付ファイル名 | 悪用する脆弱性 |
|---|---|---|
| 2012年01月04日 | 平成22年7月.pdf | Adobe Readerの脆弱性 (CVE-2010-2883) |
| 2012年01月22日 | 梅花exel.xls | Adobe Flash Playerの脆弱性 (CVE-2011-0611) |
| 2012年02月13日 | 扶養親族届.pdf | Adobe Readerの脆弱性 (CVE-2010-0188) |
| 2012年02月13日 | 子ども手当.pdf | Adobe Readerの脆弱性 (CVE-2010-0188) |
| 2012年02月26日 | 本人確認書類001.pdf | Adobe Readerの脆弱性 (CVE-2010-0188) |
| 2012年03月28日 | インフルエンザの予防等基礎知識.doc | Adobe Flash Playerの脆弱性 (CVE-2012-0753) |
| 2012年04月17日 | 大飯原発の再稼働に反対する署名用紙.doc | Windows コモン コントロールの脆弱性 (MS12-027 : CVE-2012-0158) |
| 2012年04月17日 | 献金を受け取る機構及び人のリスト.doc | Windows コモン コントロールの脆弱性 (MS12-027 : CVE-2012-0158) |
| 2012年04月19日 | 日本が尖閣問題にこだわる6つの理由.doc | Windows コモン コントロールの脆弱性 (MS12-027 : CVE-2012-0158) |
| 2012年04月24日 | 履歴書.doc | Windows コモン コントロールの脆弱性 (MS12-027 : CVE-2012-0158) |
| 2012年04月26日 | 201204名簿(更新).doc | Windows コモン コントロールの脆弱性 (MS12-027 : CVE-2012-0158) |
| 2012年05月22日 | 計画停電スケジュール.doc | Windows コモン コントロールの脆弱性 (MS12-027 : CVE-2012-0158) |

出展：IBM Security Services「2012 上半期 Tokyo SOC 情報分析レポート」
http://www-935.ibm.com/services/jp/its/pdf/tokyo_soc_report2012_h1.pdf

# 脆弱性とは

## ■ 脆弱性：

**1．脆弱性の定義**
**脆弱性とは、ソフトウエア製品やウェブアプリケーション等において、コンピュータ不正アクセスやコンピュータウイルス等の攻撃により、その機能や性能を損なう原因となり得るセキュリティ上の問題箇所です。**

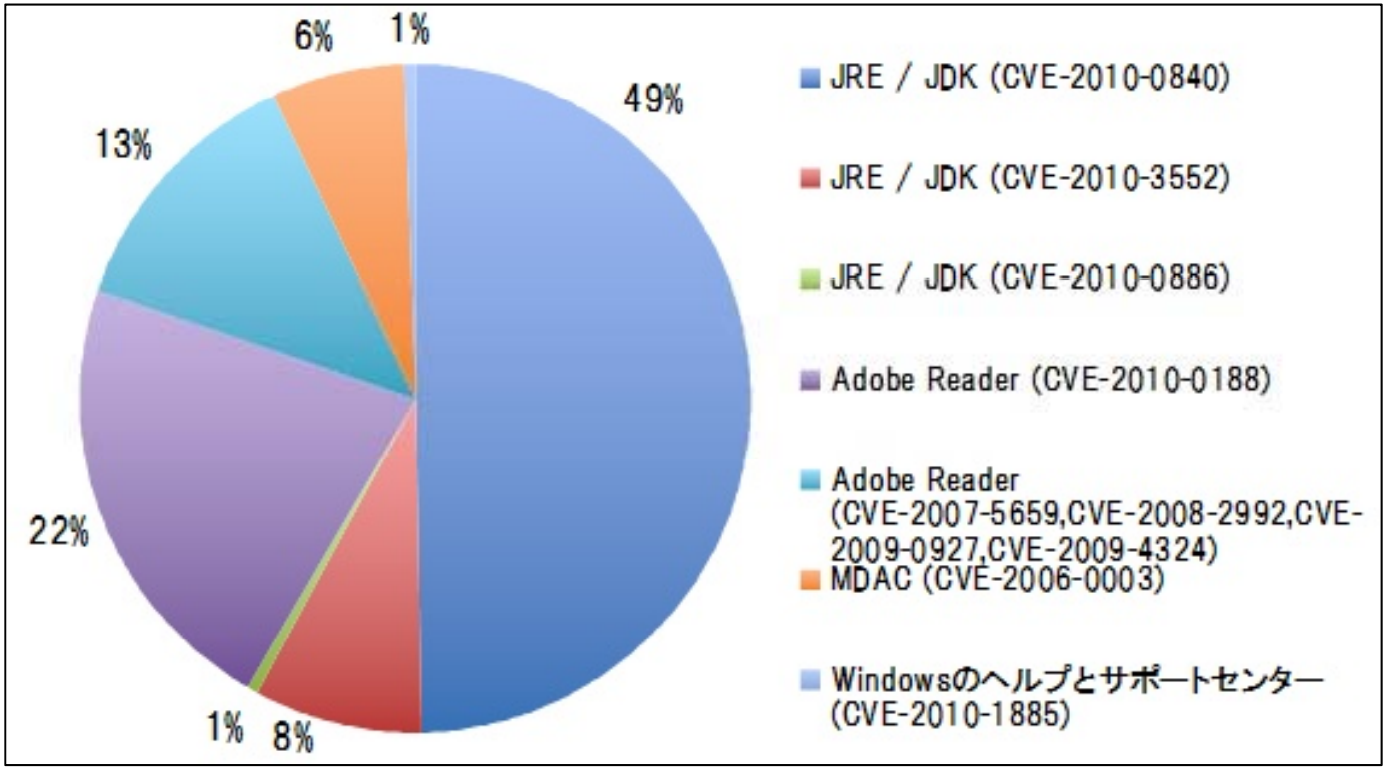
情報セキュリティ早期警戒パートナーシップガイドラインより
http://www.ipa.go.jp/security/ciadr/partnership_guide.pdf

**2．脆弱性とは**
**組織の情報資産は、多くの脅威にさらされています。**
**脆弱性とは、組織の情報セキュリティ体制上、これらの脅威に対する攻撃に弱い状態のことを指します。**
**第三者が脅威となる行為(システムの乗っ取りや機密情報の漏洩など)を行うことができる欠陥や仕様上の問題点といったシステム上の問題点や、機密情報の管理体制が整っていないなどといった人間の振る舞いに関する問題点も脆弱性となり得ます。**

脅威と脆弱性とリスクの関係より
http://www.ts-ism.com/materials/archives/55.html

# 狙われるソフトウェアの脆弱性

- Black Hole Exploit Kit(攻撃ツール)が攻撃対象とする脆弱性:
  - 93%が3rdパーティ製の既知の脆弱性を使う

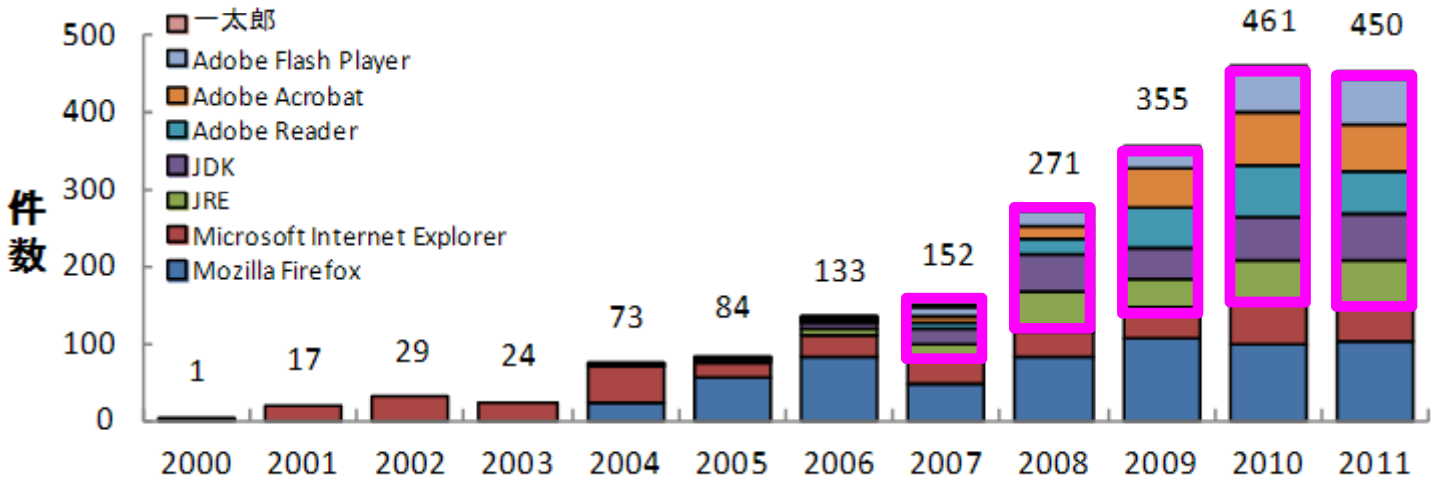



**いま一番危ない脆弱性は何だ? ～2011年版～**
http://itpro.nikkeibp.co.jp/article/COLUMN/20110904/368103/

# 脆弱性を狙った攻撃
## ～製品ベンダー側も日々対策を行っている～

IPA

- 主要クライアントソフトのセキュリティ対策情報公開の推移




  - Adobe Reader, JRE, Adobe Flash Playerにおいて発見される脆弱性が増えている

- **統計情報：利用者のセキュリティパッチ／アップデート状況**
  - 「Windows OS のセキュリティパッチ」の更新を行っている　・・・70%
  - 「Adobe Readerのバージョンアップ」 を行っている　・・・55.8%

☞ **OSに比べて、クライアントソフトの定期的な更新作業が定着していない実情**

# ゼロデイ攻撃とは

IPA

## ■ ゼロデイ攻撃：

OSやアプリケーションの脆弱性を修正するパッチが開発ベンダより提供されるより前に行われる、その脆弱性を突いた攻撃のこと

### ゼロデイ攻撃に利用された脆弱性：

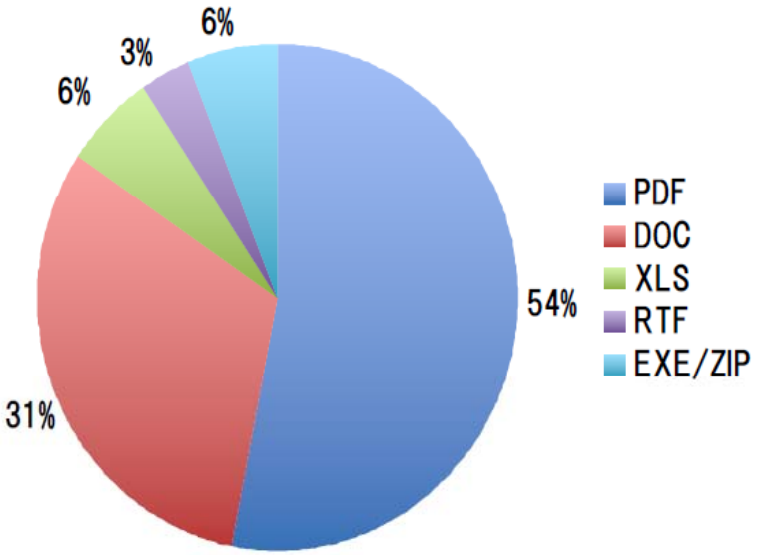
| CVE番号 | 脆弱性名 | ベンダー対応時期 |
|---|---|---|
| CVE-2011-2462 | Adobe Reader および Acrobat における任意のコードを実行される脆弱性 | 2011/12 |
| CVE-2012-0767 | Adobe Flash Player におけるクロスサイトスクリプティングの脆弱性 | 2012/2 |
| CVE-2012-0779 | Adobe Flash Player における任意のコードを実行される脆弱性 | 2012/5 |
| CVE-2012-1535 | Adobe Flash Player における任意のコードを実行される脆弱性 | 2012/8 |
| CVE-2012-4681 | Oracle Java 7 に脆弱性 | 2012/8 |
| CVE-2012-4969 | Internet Explorer に任意のコードが実行される脆弱性 | 2012/9 |

# 標的型攻撃メールの傾向

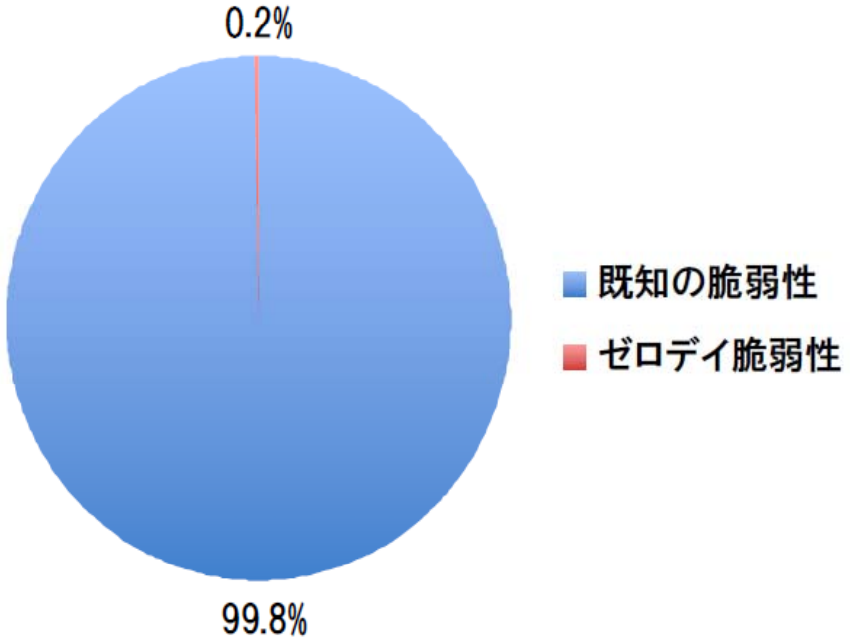
## ～99%以上が既知の脆弱性が悪用されている～

IPA

## ■ 攻撃に使われたファイル種別と脆弱性種別




メールに添付されていた不正なファイルの拡張子




ドキュメント・ファイルの悪用する脆弱性の割合

出展：IBM Security Services「2012 上半期 Tokyo SOC 情報分析レポート」
http://www-935.ibm.com/services/jp/its/pdf/tokyo_soc_report2012_h1.pdf

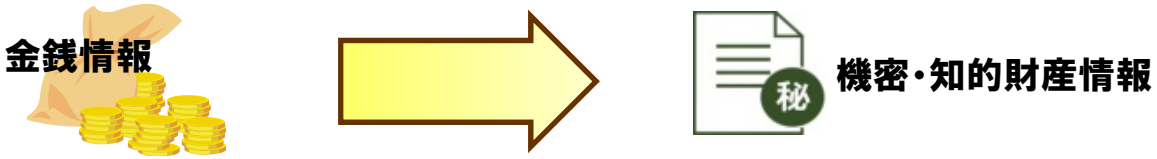
**脆弱性対策をタイムリーに行っていれば、攻撃を防げる可能性は高まる**

# 『標的型攻撃』の状況

## ～攻撃者が狙う情報や地域は多岐にわたっている～

■ McAfee社が、2011年8月に公表した資料
「世界14カ国、72組織をターゲットにしたOperation Shady RAT （McAfee）」
http://www.mcafee.com/japan/security/mcafee_labs/blog/content.asp?id=1275

**国家機密情報、ソースコード、メールアーカイブ、交渉計画、新規油田・ガス田開発に関する詳細な調査結果、ドキュメントストア、契約書、システム設計図面**などが窃取




2006年から2010年までの攻撃対象国

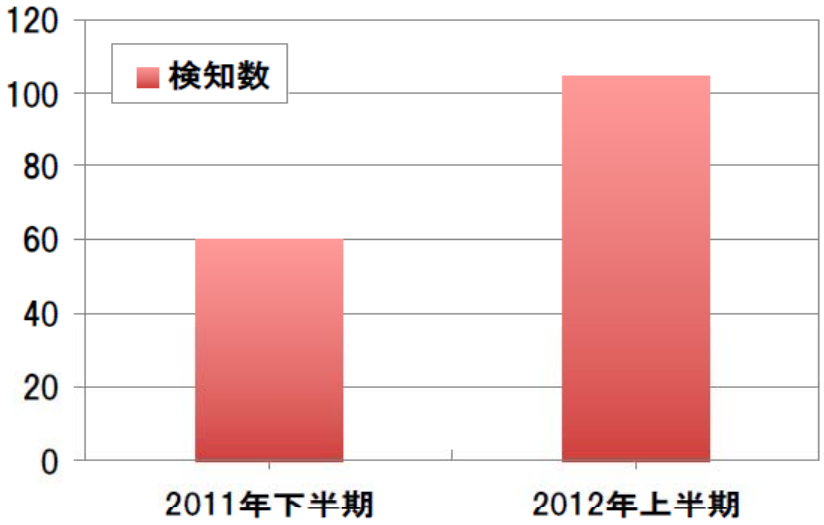
| 国 | 攻撃数 | 国 | 攻撃数 |
|---|---|---|---|
| 米国 | 49 | インドネシア | 1 |
| カナダ | 4 | ベトナム | 1 |
| 韓国 | 3 | デンマーク | 1 |
| 台湾 | 3 | シンガポール | 1 |
| 日本 | 2 | 香港 | 1 |
| スイス | 2 | ドイツ | 1 |
| 英国 | 2 | インド | 1 |

| 業種 | 攻撃数 |
|---|---|
| 政府・行政機関 | 22組織 |
| 工業関連 | 6組織 |
| 通信関連 | 13組織 |
| 軍需関連 | 13組織 |
| 金融関連 | 4組織 |
| その他 | 12組織 |

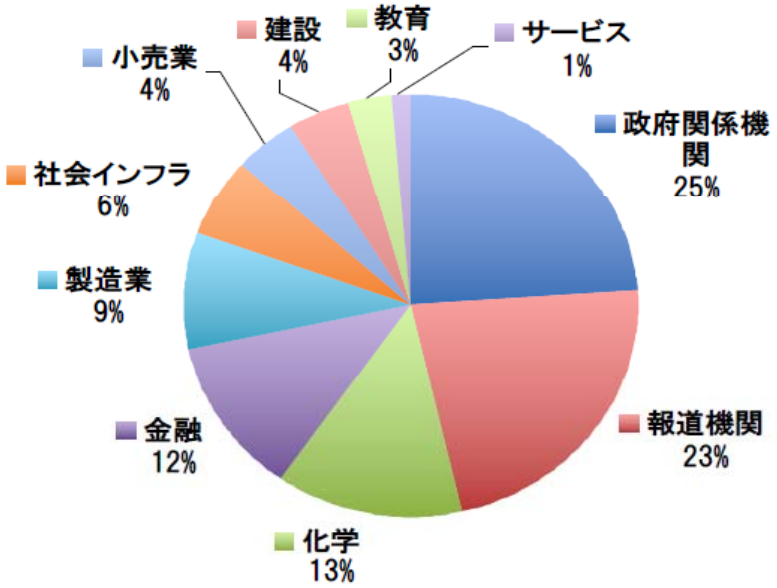
# 標的型攻撃メールの傾向
## ～前年度より2倍に検知件数が増加～

IPA

## ■ 標的型攻撃メールの件数と業種別割合




標的型メール攻撃の検知件数比較



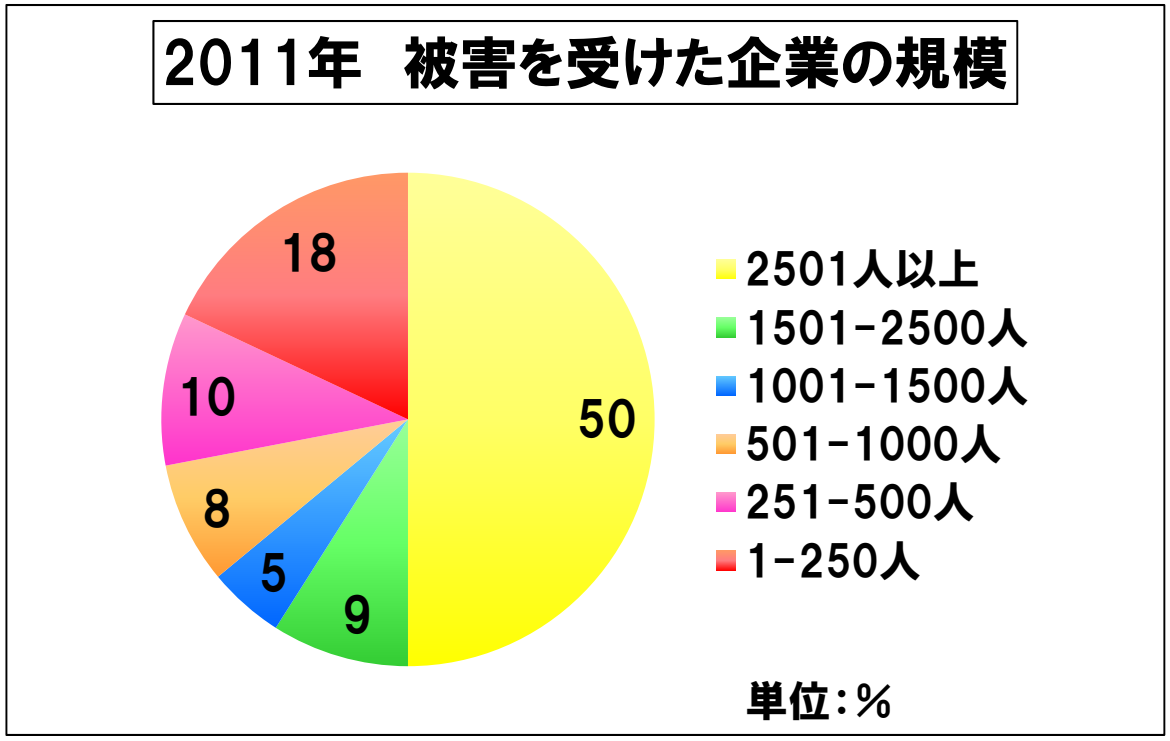

標的型メール攻撃のターゲットとなった組織の業種別割合

出展：IBM Security Services「2012 上半期 Tokyo SOC 情報分析レポート」
http://www-935.ibm.com/services/jp/its/pdf/tokyo_soc_report2012_h1.pdf

- 政府機関、報道機関、製造事業者などにメールが送付
- 添付ファイルを開くことで、マルウェアが感染する攻撃手法

# 誰を標的にしている？

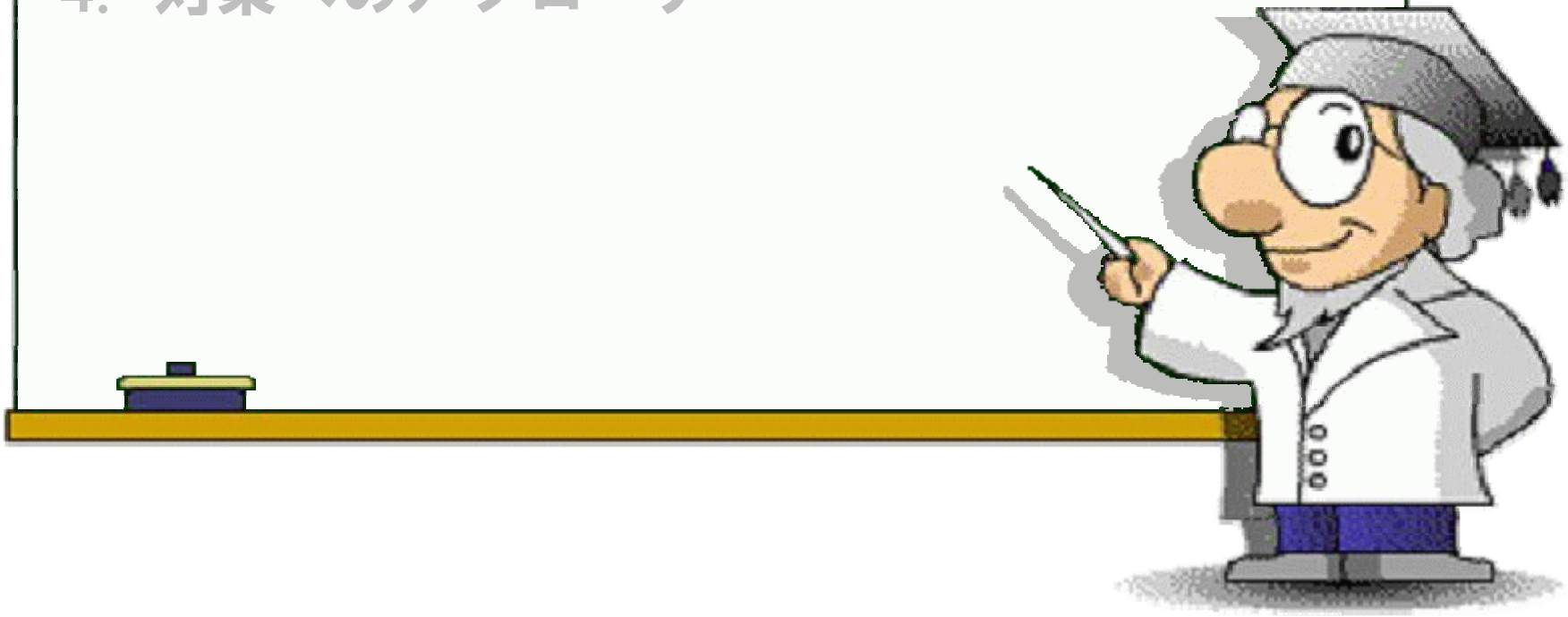
- 報道では大企業や官公庁が狙われているものが取り上げられる。
  - 中小企業は対象外？




インターネットセキュリティ脅威レポート 2011年の傾向より
http://www.symantec.com/content/ja/jp/enterprise/white_papers/istr17_wp_201207.pdf

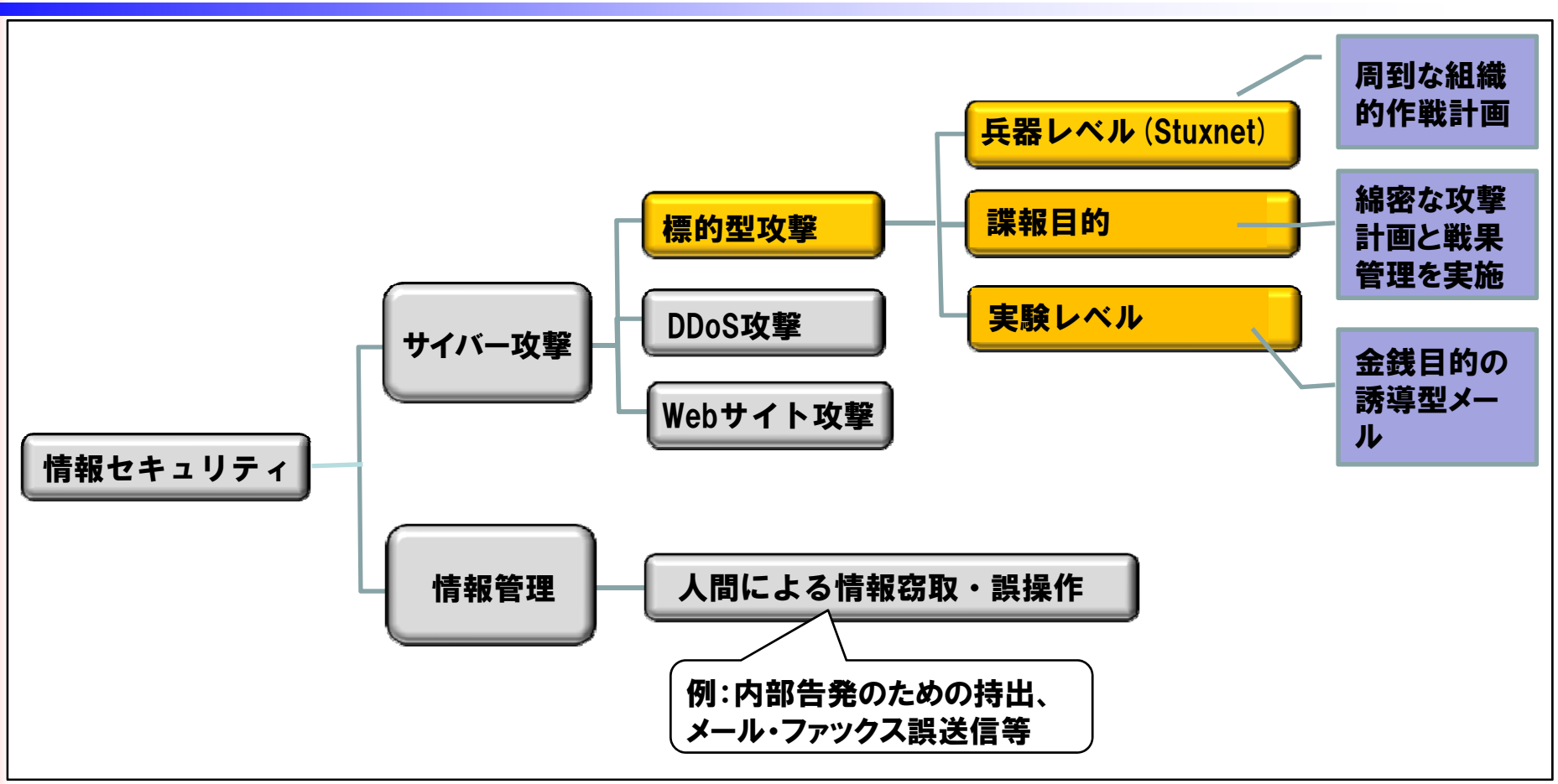
# 目次

1. サイバー攻撃について
2. 標的型攻撃（新しいタイプの攻撃）とは
3. **新しいタイプの攻撃のモデル**
4. 対策へのアプローチ



# 情報セキュリティにおける攻撃の分類

## ～ 新たな対策を検討する段階へ～




**一口に標的型攻撃といっても、高度なものから低度なレベルまで様々存在する**

# 「新しいタイプの攻撃」の流れ

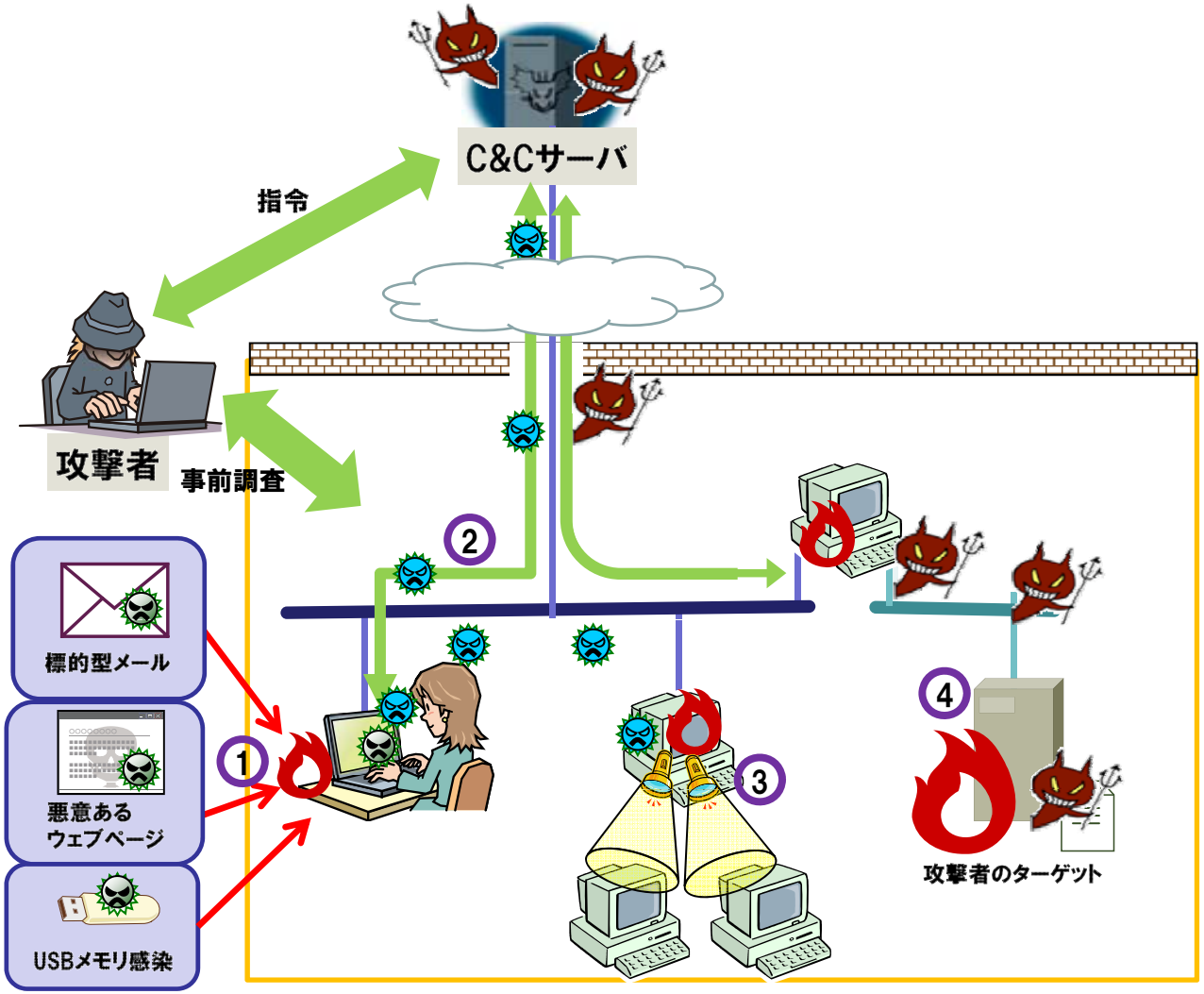
⓪[事前調査]
ターゲットとなる組織を攻撃する為の情報を収集

①[初期潜入段階]
標的型メールやUSBメモリ、ウェブサイト閲覧を通してウイルスに感染する。

②[攻撃基盤構築段階]
侵入したPC内でバックドアを作成し、外部のC&Cサーバと通信を行い、新たなウイルスをダウンロードする

③[システム調査段階]
情報の存在箇所特定や情報の取得を行う。攻撃者は取得情報を基に新たな攻撃を仕掛ける

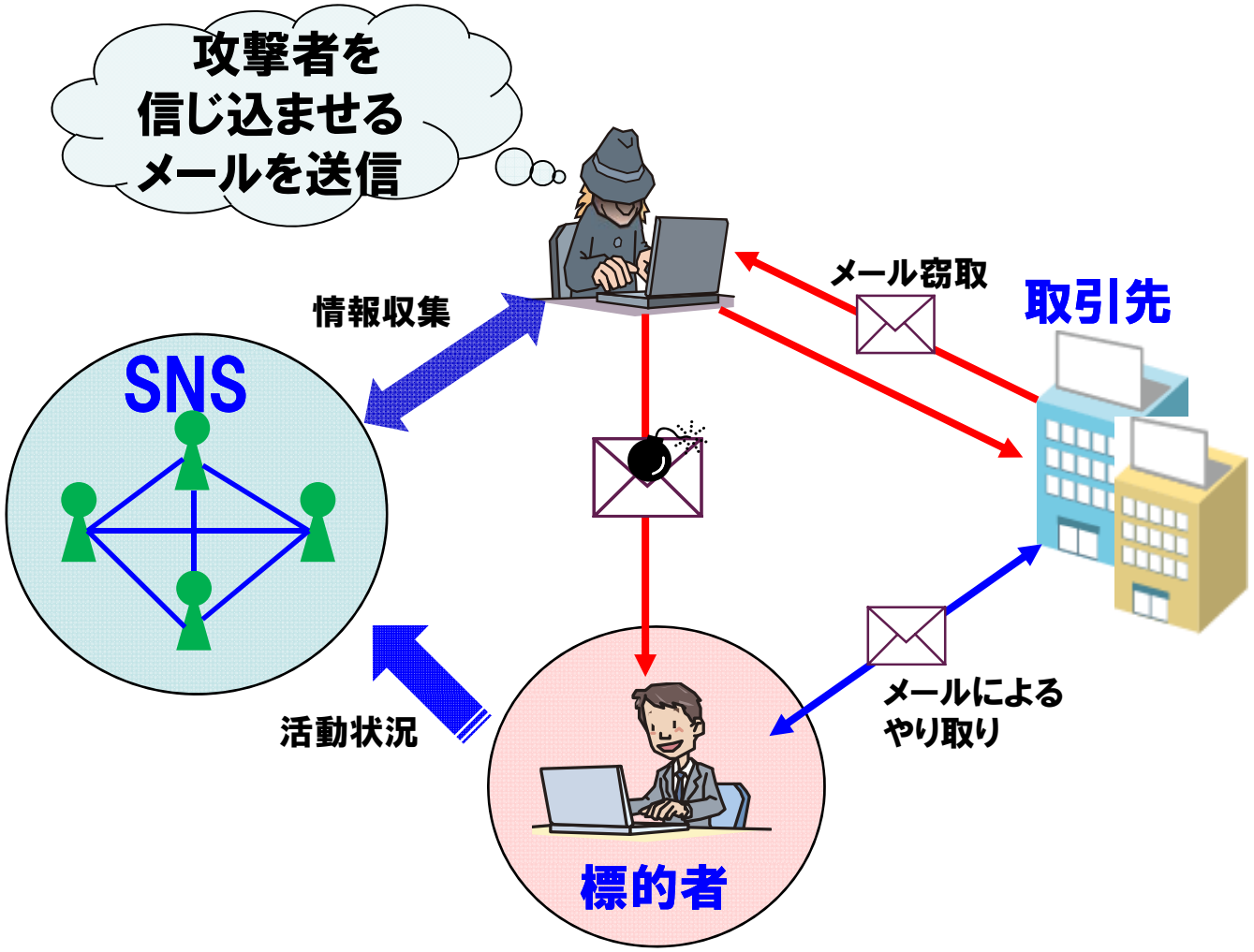
④[攻撃最終目的の遂行段階]
攻撃専用のウイルスをダウンロードして、攻撃を遂行する



# 第0段階～第1段階

## ～用意周到な準備を経て攻撃が行われる～

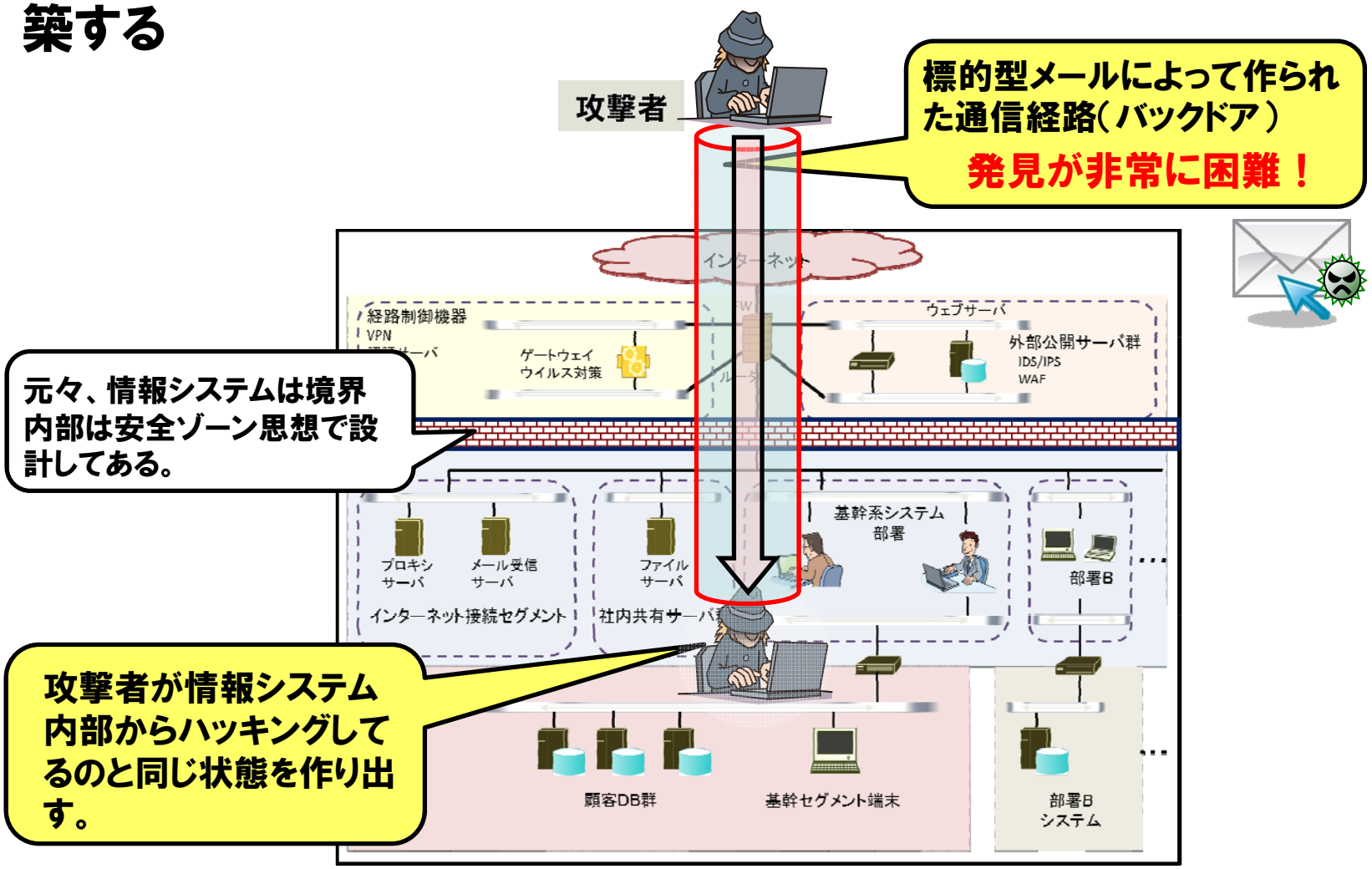
■ 攻撃者は、標的の身辺を偵察した後に攻撃を仕掛ける



# 第１段階～第２段階
## ～標的型メールを使った内部ハッキング～

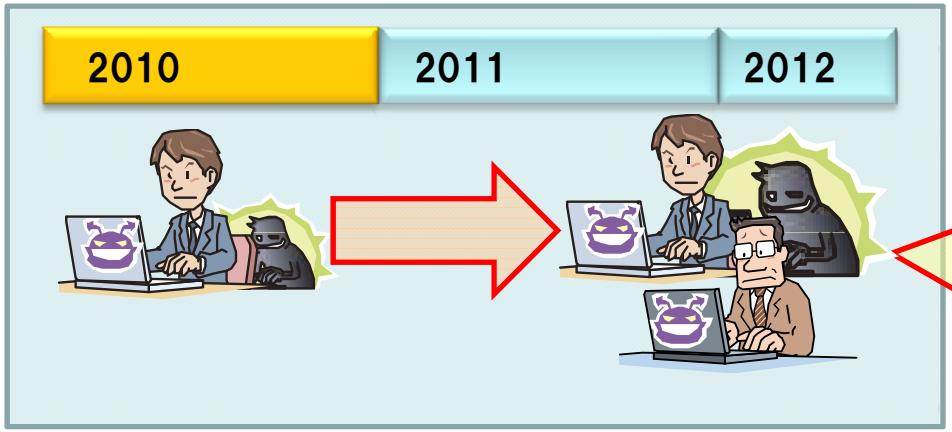
IPA

- 標的型メールによって内部ハッキングをするためのバックドアを構築する



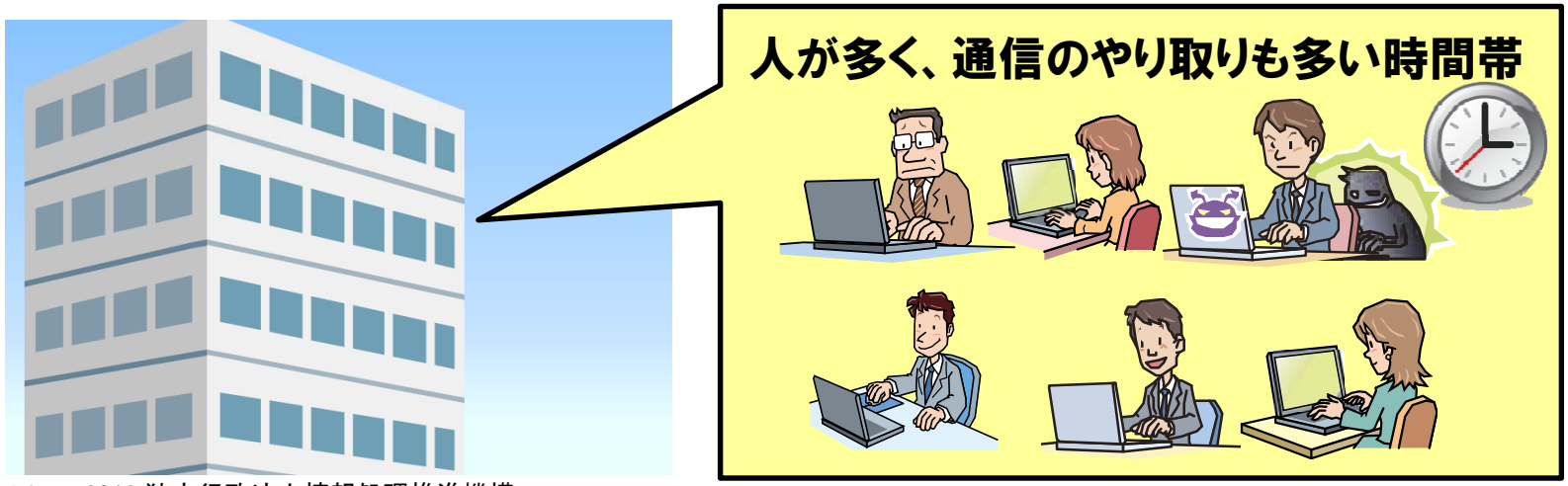
# 第2段階～第3段階
## ～長期間発見されないように潜伏して情報を窃取～

- 数か月～数年単位で潜伏する




この間に
・必要な情報を取得
・ウイルスの機能アップデート
・組織内への拡散
等を行う

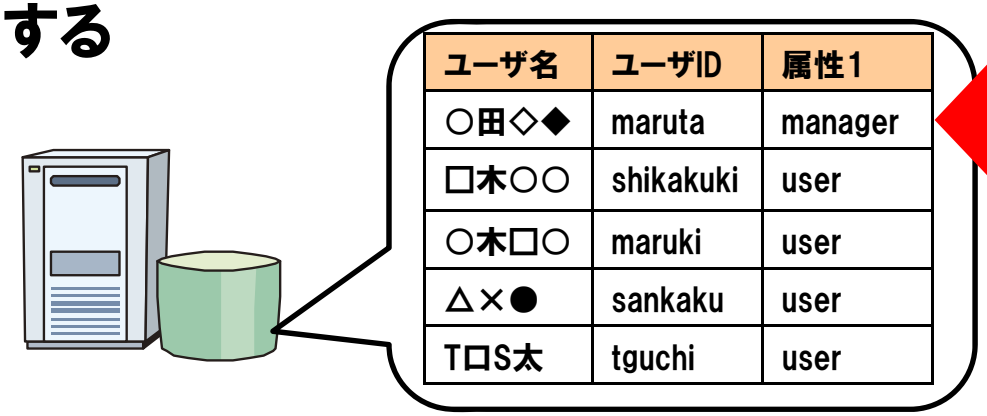
- 攻撃者がバックドア通信を行うのは業務時間帯。通常の通信の中に紛れて発見しづらいように行われる



# 第3段階～第4段階
## ～狙われるディレクトリサーバ～

IPA

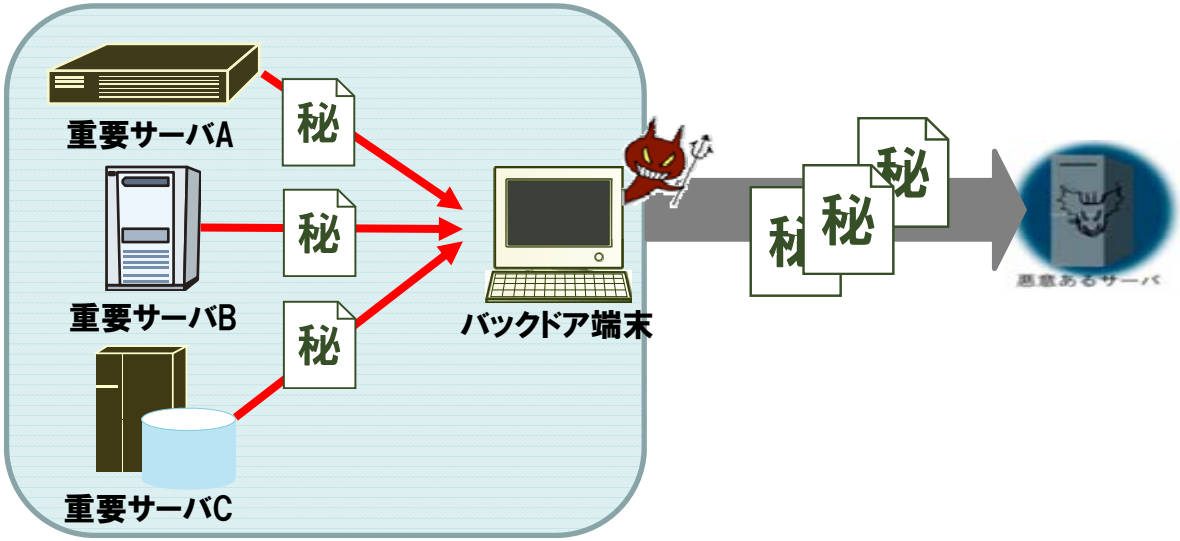
- 社員のユーザ管理をするディレクトリサーバを攻撃し、特権のIDを取得する



| ユーザ名 | ユーザID | 属性1 |
|---|---|---|
| ○田◇◆ | maruta | manager |
| □木○○ | shikakuki | user |
| ○木□○ | maruki | user |
| △×● | sankaku | user |
| T□S太 | tguchi | user |

ディレクトリサーバ内の特権ユーザ情報を窃取し、様々なシステムへアクセスできるように

- そして、目的の機密情報の窃取へ



# 「新しいタイプの攻撃」の分析

■「新しいタイプの攻撃」の流れを分析してみると**共通的な攻撃手法**があることが分かった

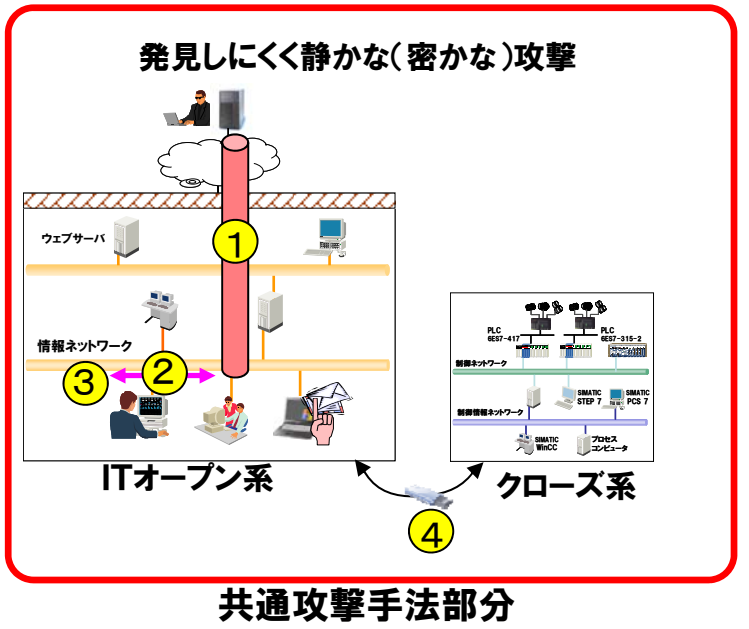
| 段階 | 攻撃内容 | 特徴 |
|---|---|---|
| 第0段階<br>［事前調査段階］ | （1）攻撃戦略の検討<br>・攻撃ターゲットの環境調査<br>・関係機関に対する情報窃取活動 | 第1段階の初期潜入を確実に行うための関係者しか知らない情報が狙い |
| 第1段階<br>［初期潜入段階］ | （1）各種初期攻撃<br>・標的型攻撃メール添付ウイルス<br>・ウェブ改ざんによるダウンロードサーバ誘導<br>・外部メディア（USB等）介在ウイルス<br>など | 入口の対策をすり抜け、システム深部に潜入<br>素早く次の段階へ移行。<br>攻撃手法は使い捨て |
| 第2段階<br>［攻撃基盤構築段階］ | （1）バックドア（裏口）を使った攻撃基盤構築<br>・ウイルスのダウンロードと動作指示<br>・ウイルスの拡張機能追加 | 構築した攻撃基盤は発見されない。<br>構築した攻撃基盤は再利用される。 |
| 第3段階<br>［システム調査段階］ | （1）組織のシステムにおける情報の取得<br>（2）情報の存在箇所特定 | 時間をかけて何度もしつこく行う。 |
| 第4段階<br>［攻撃最終目的の遂行段階］ | （1）組織の重要情報（知財・個人情報等）の窃取<br>（2）組織情報（アカウント等）と基に、目標を再設定 | 何度も攻撃を行うための情報窃取。<br>組織への影響を与える情報窃取。 |

共通攻撃手法

# 共通攻撃手法の分析

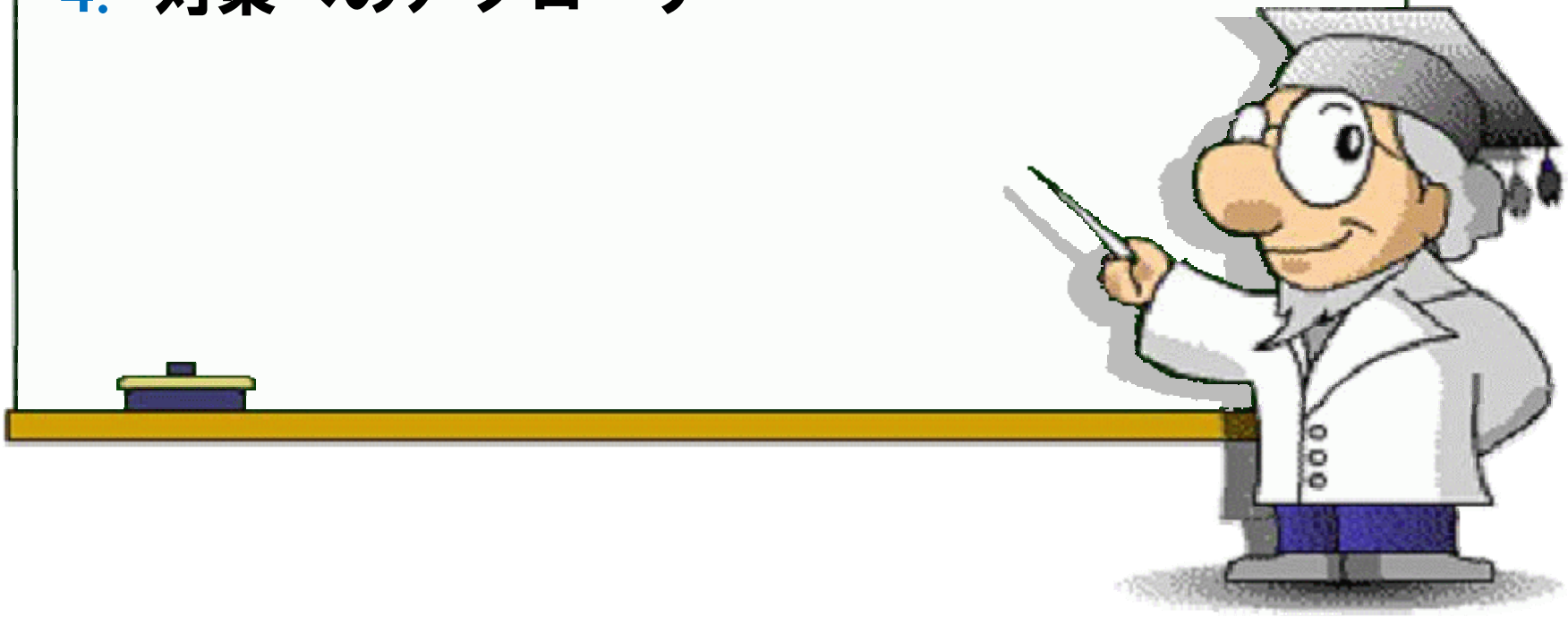
## ■ 共通攻撃手法を更に見ていくと4つの機能が存在する

| 番号 | 共通攻撃手法機能 | 役割 |
|---|---|---|
| ① | httpバックドア通信機能 | ウイルスと攻撃者のサーバとの通信を確立 |
| ② | システム内拡散機能 | システム内の情報窃取の効率化のため、多くの端末に感染させる |
| ③ | 一斉バージョンアップ機能 | システム内のウイルスに効果的な攻撃を行わせる機能を持たせるようにする |
| ④ | USB利用型情報収集機能 | クローズ系システムの情報を収集するためUSB等にそのような機能のウイルスを入れ込む |



# 目次

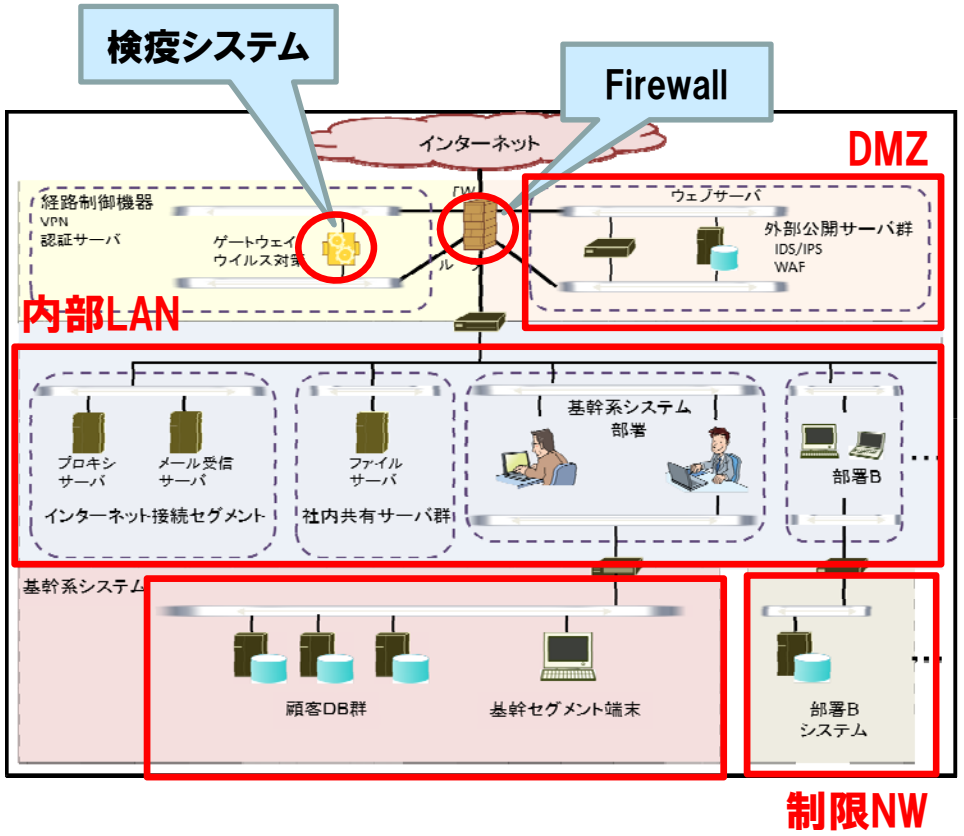
1. サイバー攻撃について
2. 標的型攻撃（新しいタイプの攻撃）とは
3. 新しいタイプの攻撃のモデル
4. **対策へのアプローチ**



# セキュリティ対策の特徴と弱点（1）

## ～境界防御の概念でシステムができている～

- 不正侵入を阻止
  - FireWall
    - 許可された通信のみ通過
    - 通信内容は関知しない
  - IDS(IPS)
    - 攻撃を行う通信を検知
    - 未知の攻撃の阻止は難しい
  - Anti-Virus
    - マルウェアの侵入を阻止
    - 見逃しの可能性
- 端末でのセキュリティ対策
  - 端末レベルで侵入を阻止
  - 脆弱性対策
- 基本的に外→内への侵入に備える

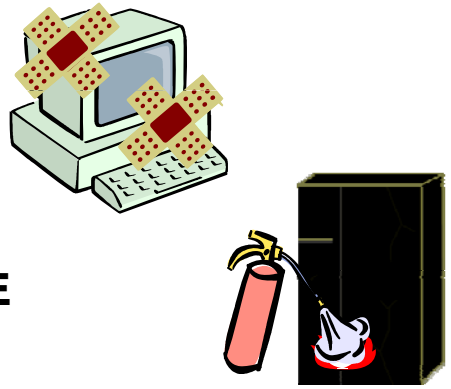


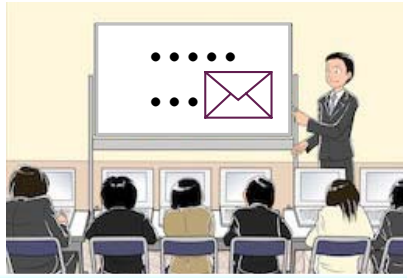
# セキュリティ対策の特徴と弱点（2）

## ～個人のスキルやエンドポイントセキュリティ～

IPA

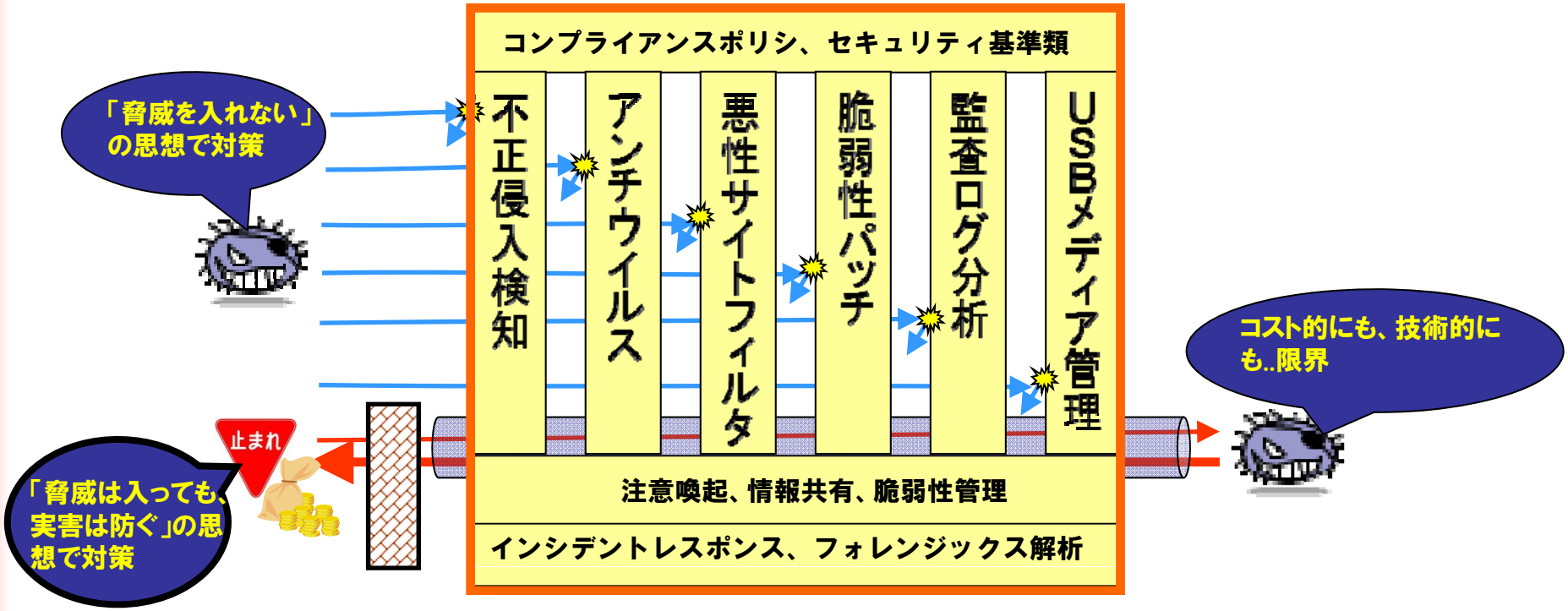
- 脆弱性対策（セキュリティパッチ適用）
  - エンドポイント（PC）へのパッチ適用
    - セキュリティ対策の基本であり、効果大
    - 全端末に適用することを前提
    - エンドユーザ主導による対策の為、漏れの可能性
  - サーバ機器等へのパッチ適用
    - 互換性の問題で適用できないケースの問題
    - システム停止が許容できない運用上の事情
- 啓発活動による対策
  - 不審メールを開かない個人や組織への啓発
    - 組織内での注意力・対策熱が上がる
    - 1人でも感染すれば組織内に侵入
    - マルウェア開封率0%が必須条件
  - ルールによる制限
    - USBメディアの持込禁止
    - 業務に支障をきたす可能性





**セキュリティ対策には
一長一短があり、
完全な対策は難しい**

# 新しい発想による対策




**従来の対策**

「脅威を入れない」対策

**侵入されることを前提とした対応**

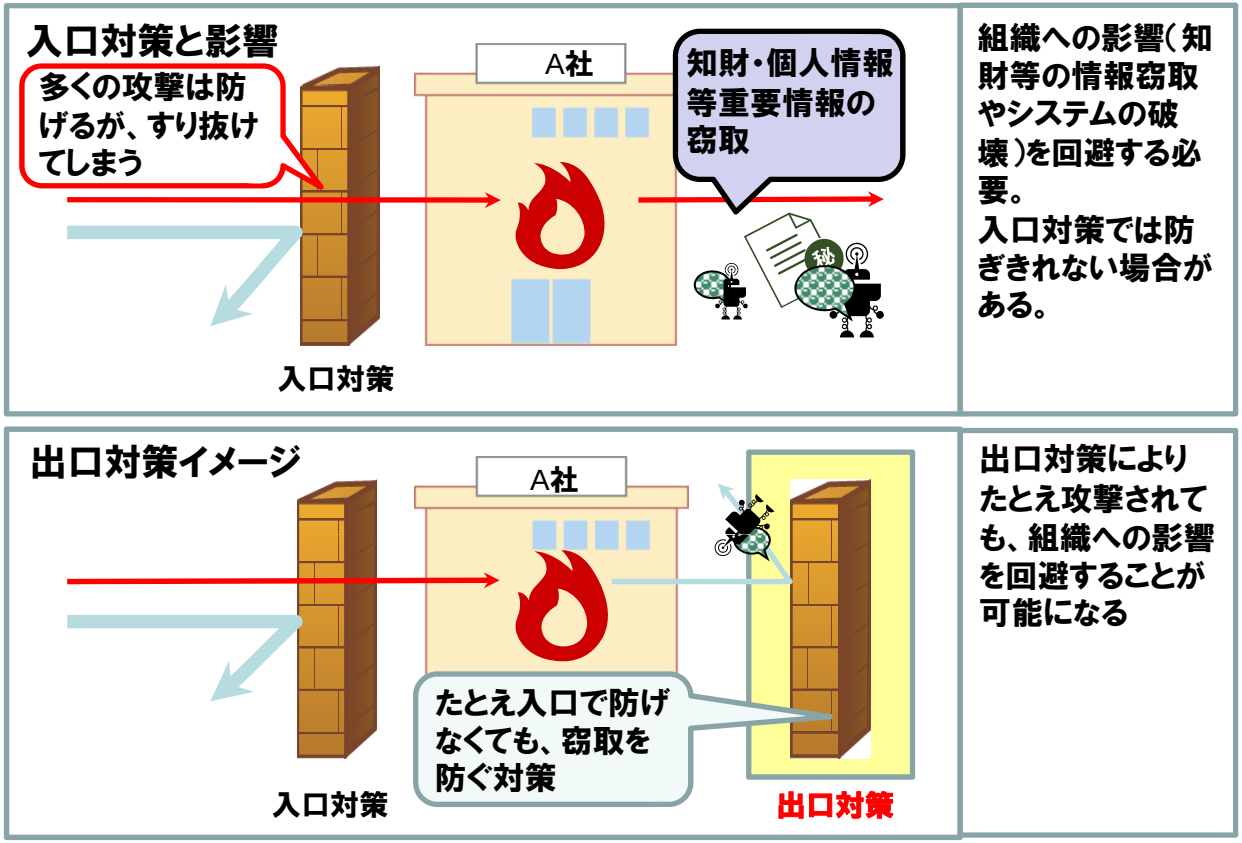
**新しい発想の対策**

「実害を防ぐ」対策

# 新しい発想による対策

- 入口と出口に二重のセキュリティ対策を
  - 外部からの脅威をブロックする「入口対策」
  - 情報が外部に持出されない為の「出口対策」

## 組織への影響と入口対策・出口対策

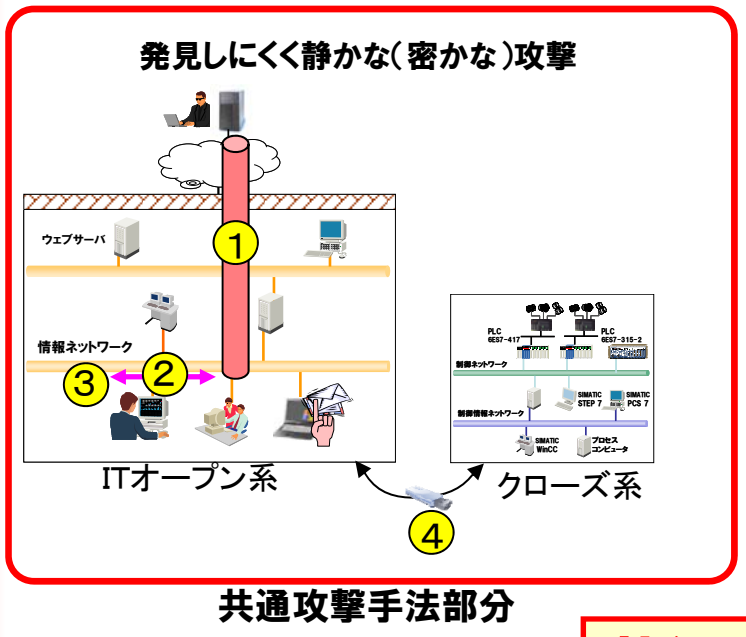


# 攻撃の分析
## ～共通的な攻撃手法と対策ポイント～

IPA

### ■ 設計対策のポイント

- 外部通信の検知と遮断することによる**攻撃基盤構築の阻止**
- ウイルスのシステム内拡散防止による**攻撃の最終目的への到達回避**

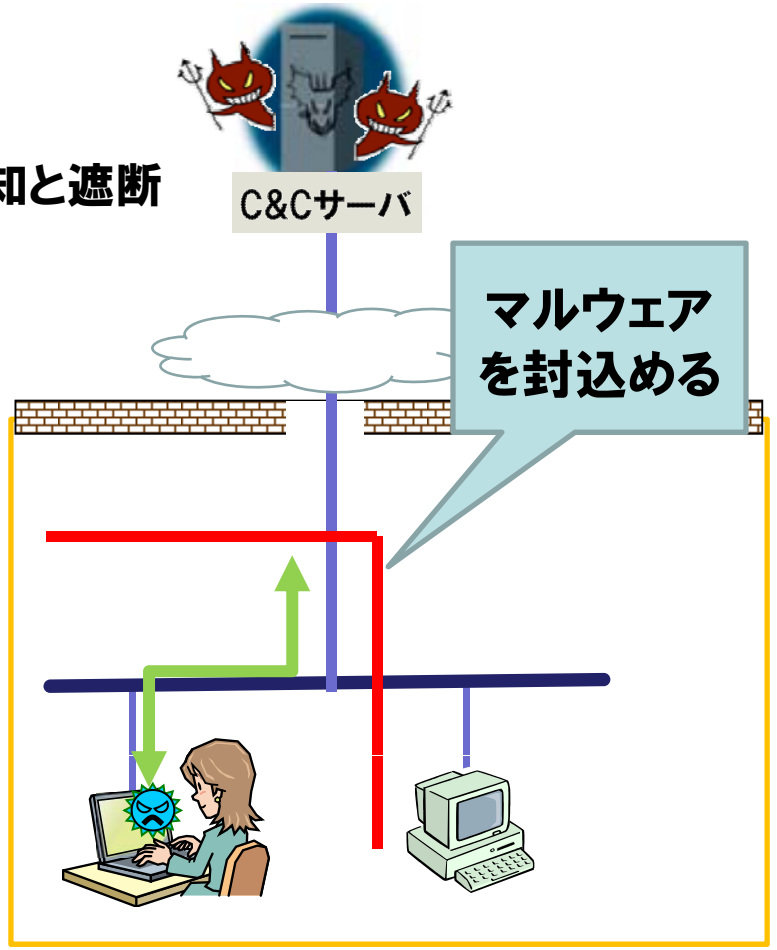



| 番号 | 共通攻撃手法機能 | 役割 |
|---|---|---|
| ① | httpバックドア通信機能 | ウイルスと攻撃者のサーバとの通信を確立 |
| ② | システム内拡散機能 | システム内の情報窃取の効率化のため、多くの端末に感染させる |
| ③ | 一斉バージョンアップ機能 | システム内のウイルスに効果的な攻撃を行わせる機能を持たせるようにする |
| ④ | USB利用型情報収集機能 | クローズ系システムの情報を収集するためUSB等にそのような機能のウイルスを入れ込む |

**共通攻撃手法を止める対策（出口対策）を**

# 出口対策 考え方
## ～マルウェアの活動を制限する為のネットワーク設計～

- バックドア通信の検知と抑止
  - プロキシサーバとFWの設定
    - 正常な通信の流れを作る
    - ルール外の通信を試みるマルウェアの検知と遮断
- 感染予防策
  - アクセス区画の整理
    - VLANを構築
    - VLAN間の通信を制限
    - マルウェアの偵察行為を阻止
  - 浸食予防
    - VLAN毎に通信の監視
    - 感染発覚時は、VLANを切り離す
- 早期発見のために
  - ログの監視



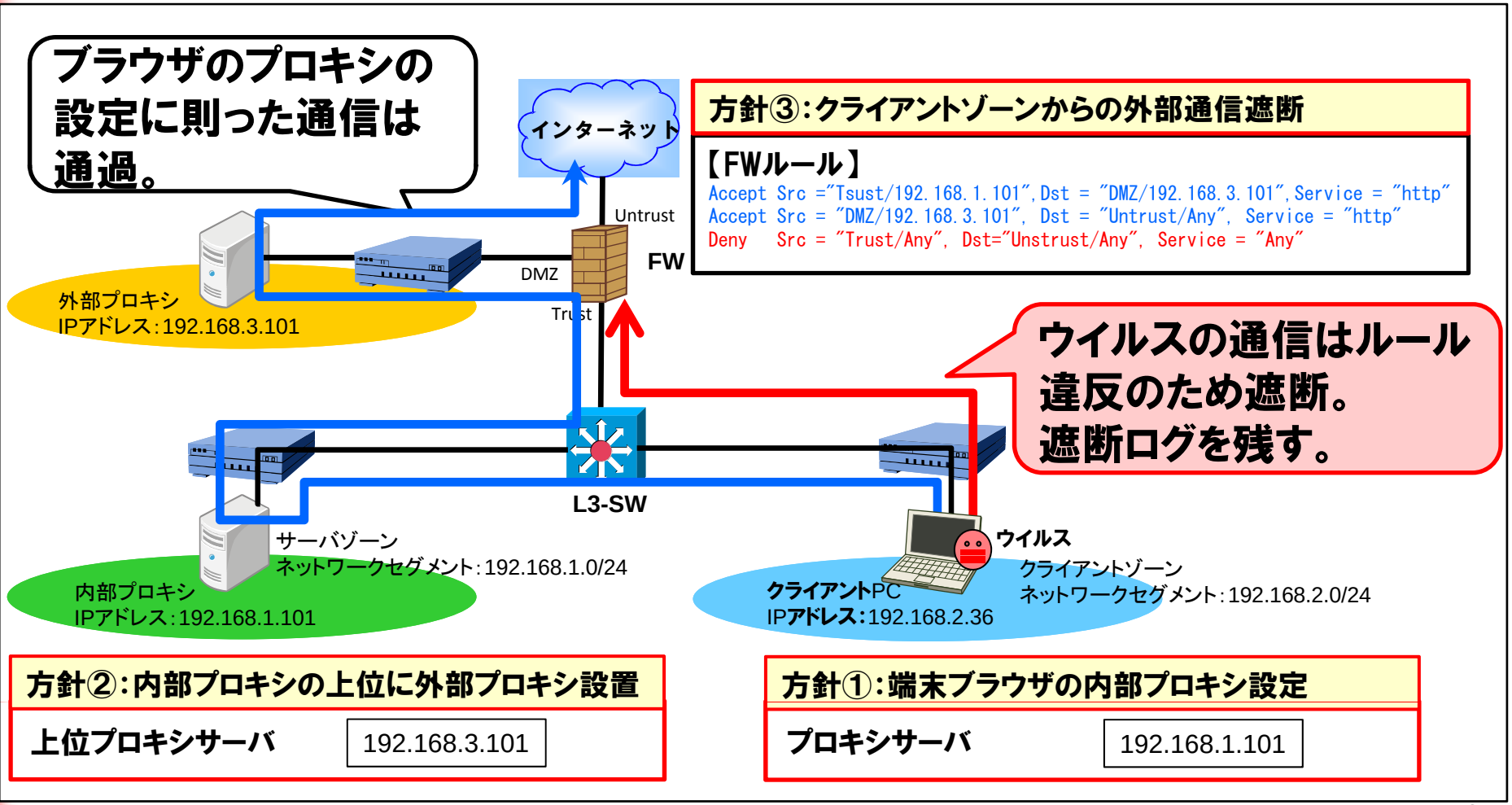
# 8つの出口対策（設計対策）

（黄色）はバックドア通信を止める対策
（青色）はシステム内拡散等を止める対策

| 対策 | 実装手法 | 区分 |
|---|---|---|
| ① サービス通信経路設計 | 1.ファイアウォールの外向き通信の遮断ルール設定<br>2.ファイアウォールの遮断ログ監視 | A.保守等作業ですぐできる対策 |
| ② ブラウザ通信パターンを模倣するhttp通信検知機能の設計 | 1.httpメソッド利用バックドア通信の遮断 | B.システム設計時に見直すべき対策 |
| ③ RATの内部proxy通信（CONNECT接続）の検知遮断設計 | 1.RATのCONNECT確立通信の特徴を利用した、内部proxyログでの監視 | B.システム設計時に見直すべき対策 |
| ④ 最重要部のインターネット直接接続の分離設計 | 最重要部がインターネットへ直接接続しないようにVLAN等で設計 | B.システム設計時に見直すべき対策 |
| ⑤ 重要攻撃目標サーバの防護 | 1.ADを管理する管理セグメントを防護する。<br>2.利用者から見えるADのサービスに対するパッチ当て。 | B.システム設計時に見直すべき対策 |
| ⑥ SW等でのVLANネットワーク分離設計 | 利用者セグメントと管理セグメントを分離設計する等 | B.システム設計時に見直すべき対策 |
| ⑦ 容量負荷監視による感染活動の検出 | スイッチ等の負荷やログ容量等における異常検知を行い、セキュリティ部門と連携する | B.システム設計時に見直すべき対策 |
| ⑧ P2P到達範囲の限定設計 | ③④の対策に加え、不要なRPC通信の排除を目的としたネットワーク設計 | B.システム設計時に見直すべき対策 |

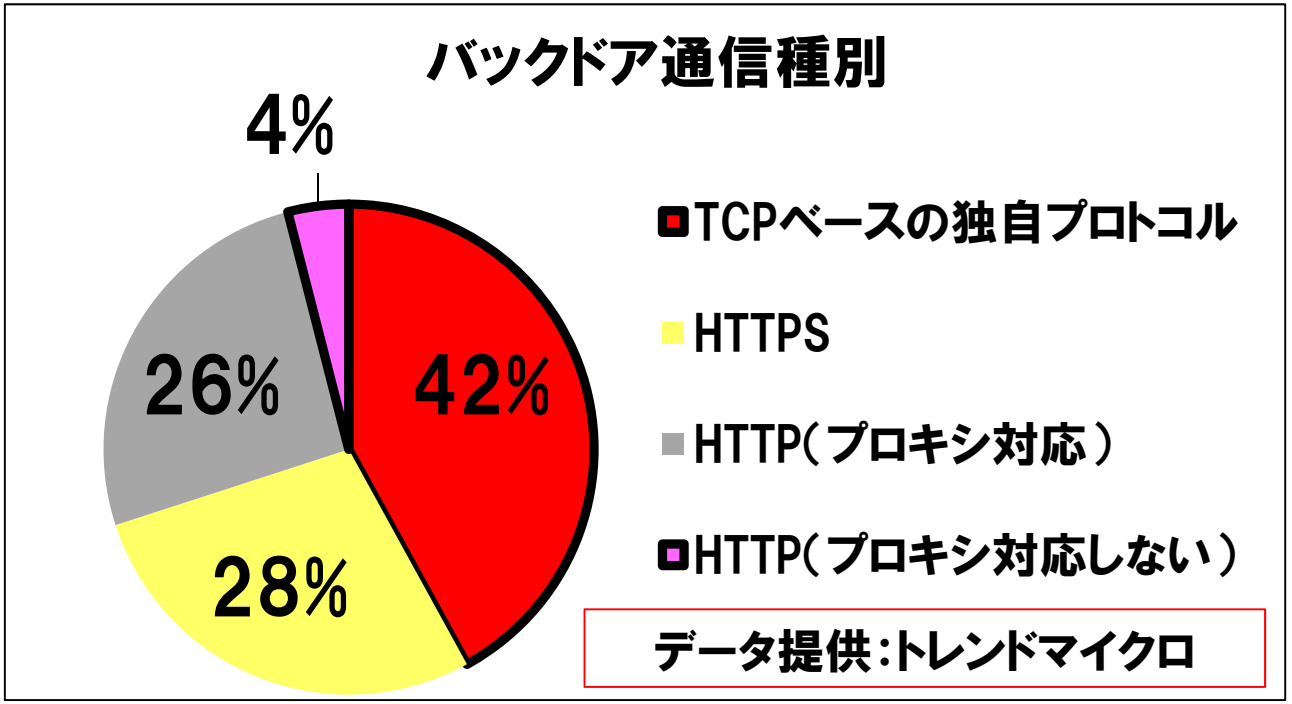
# 【参考】設計対策:サービス経路設計

- プロキシサーバを経由して正常通信の流れを作る
- FWのログから攻撃の有無を把握する



# 【参考】設計対策:サービス経路設計

- FWでプロキシ経由以外の通信を遮断することで・・・
  - TCPベースの独自プロトコルとHTTP(プロキシ対応しない)通信の46%のバックドア通信を遮断可能。

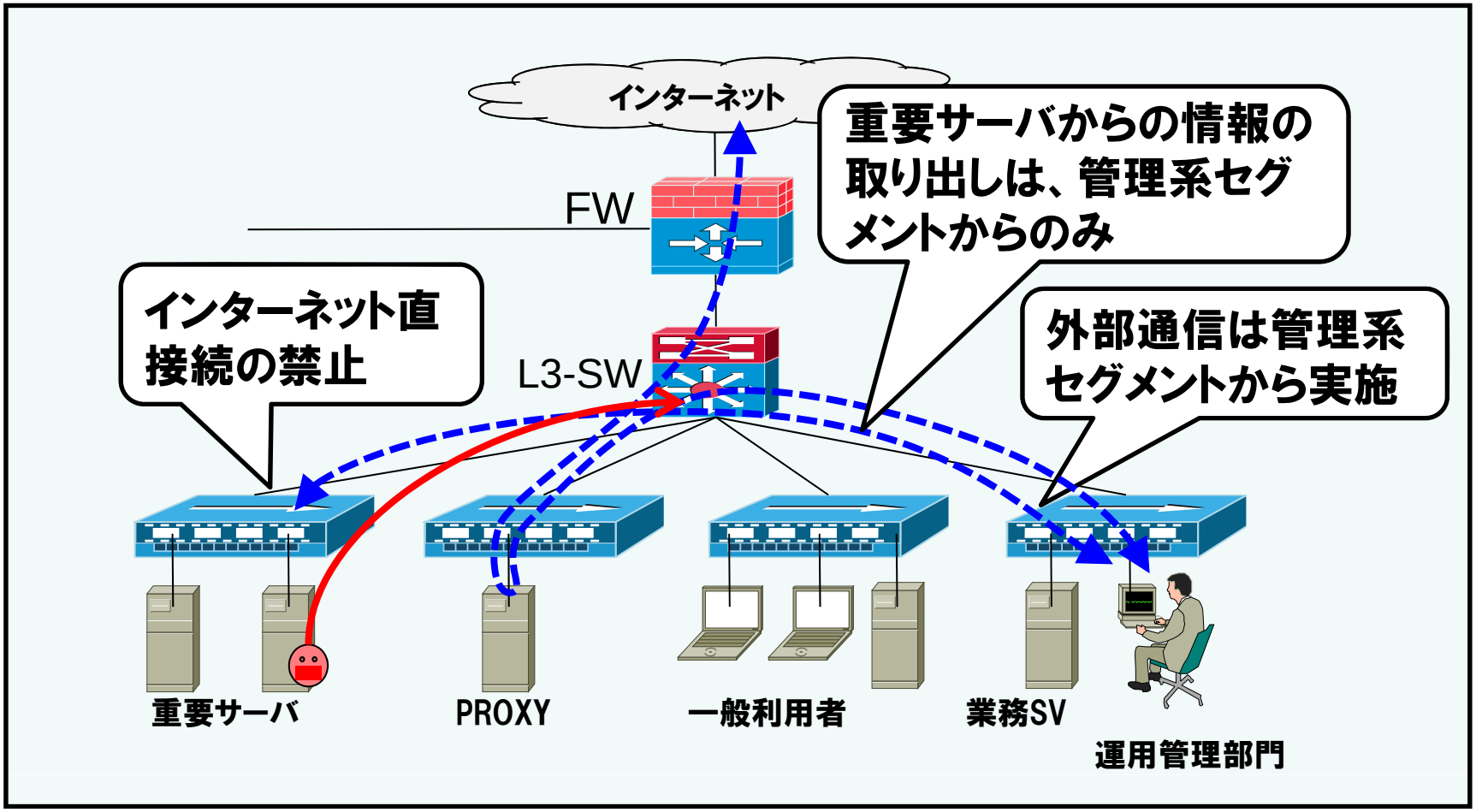



※2011年4月～10月国内で収集
標的型攻撃メールに添付されていたと思われるウイルス50個のバックドア通信サンプル

# 【参考】設計対策:最重要部の インターネット直接接続の分離設計

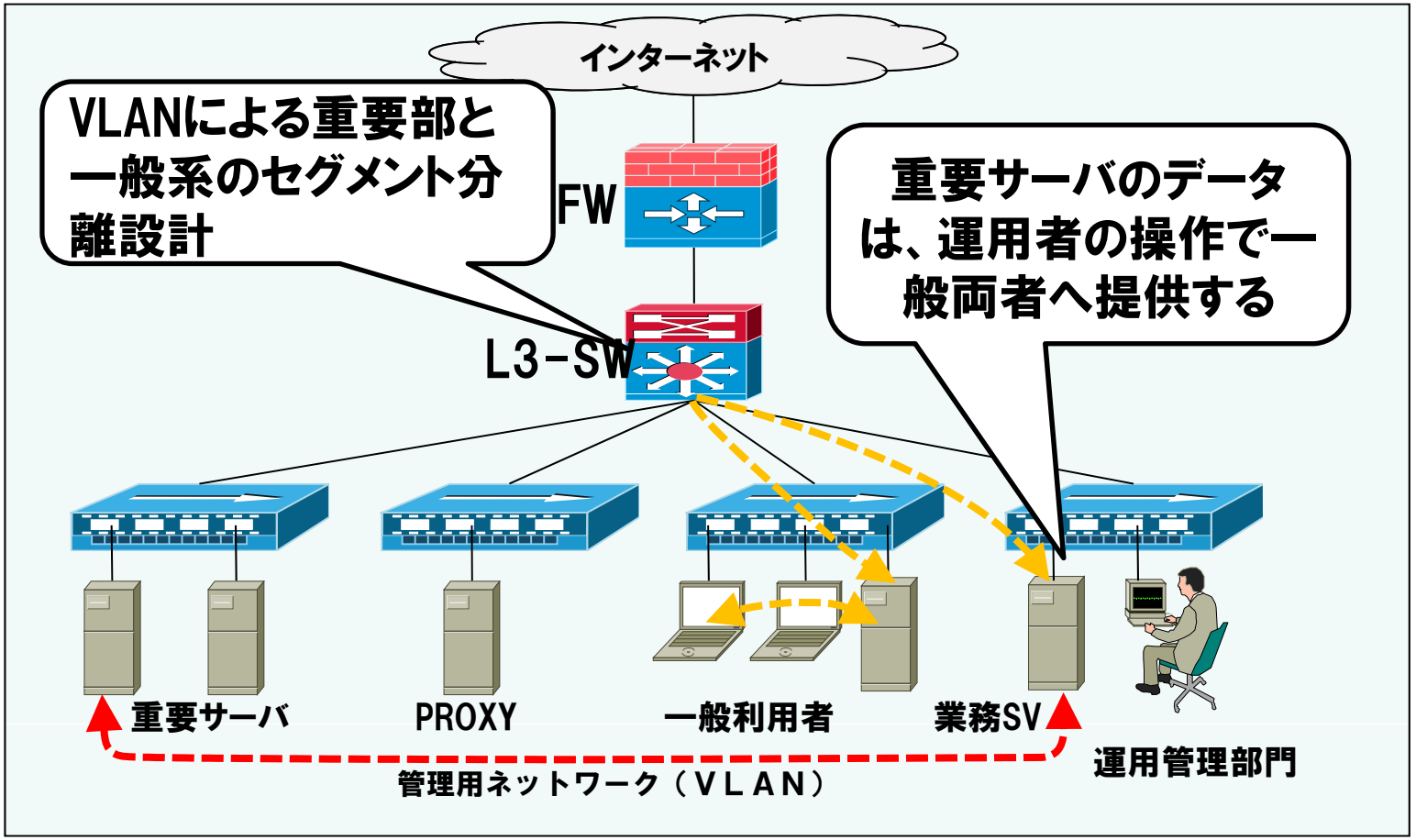
IPA

■ バックドアを仕掛けられても、重要な情報を窃取させない為の対策

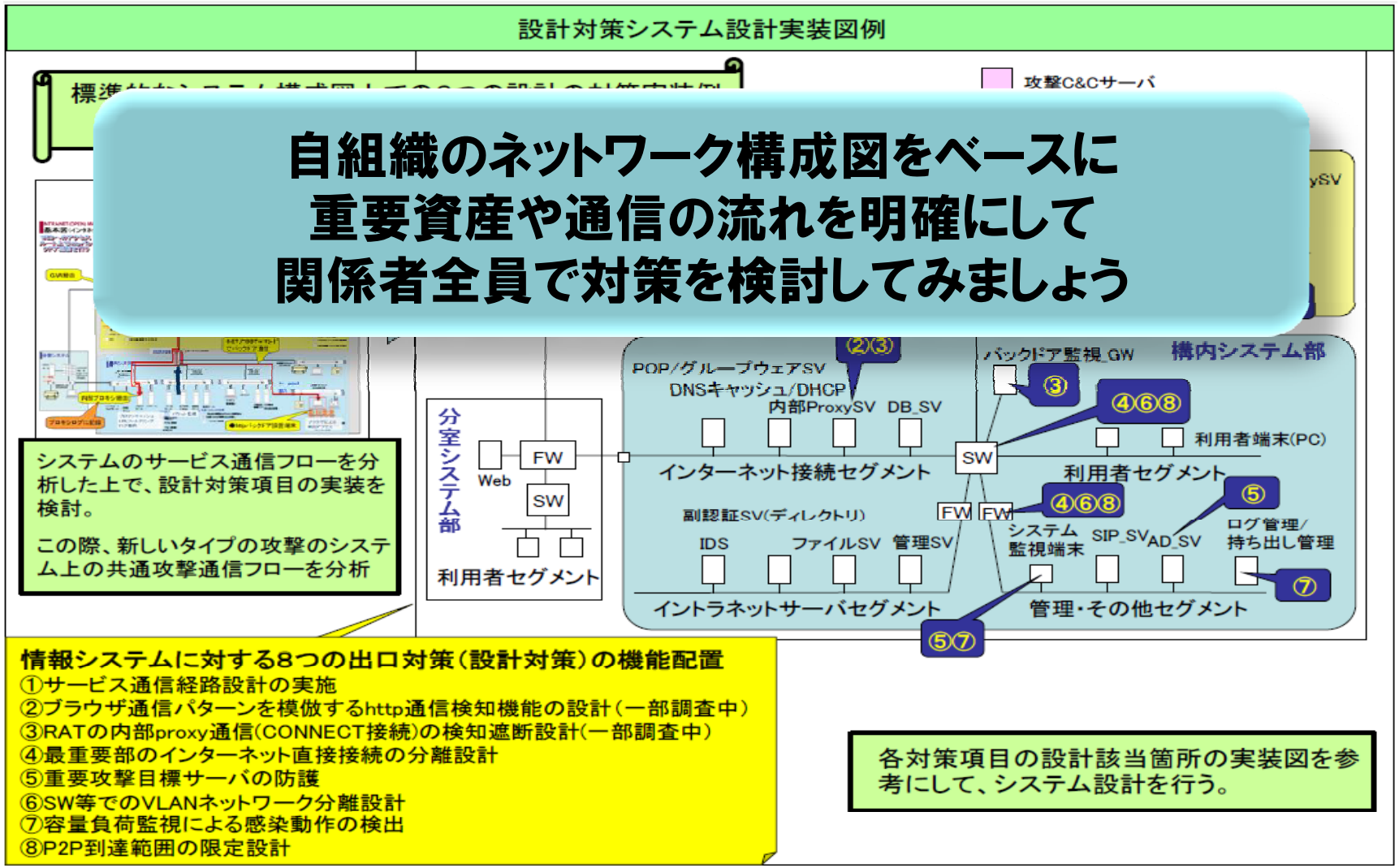


# 【参考】設計対策: VLANネットワーク分離設計

- ネットワークを分離することでウイルスの拡散を防止する
  - ウイルスが活動しづらいネットワーク環境を作る
  - 業務（通信）要件を整理し、不要なポートを開けない



# 【参考】設計実装図例



# 対策製品で何ができて何ができないか

- 対策製品を選定する上で重要なポイント
  - できることとできないことをしっかり見極める（聞く）
    - 100%防ぐことができればいいが・・・
      - 全てを防ぐことのできる万能製品は存在しないことを前提にする必要がある
    - ハコを置いただけで防げる攻撃は単純な攻撃だけ
      - 攻撃者は防御をすり抜けよう、と日々考えている！
      - そのような攻撃に対してハコを置いただけで守ることができるだろうか
  - 運用をしっかり考える
    - その製品を運用する場合、どの程度工数をかけなければならないかを真剣に考えなければならない。
      - 宝の持ち腐れどころか、結局機能しなくなる恐れも・・・

# 対策の考え方の整理

- 攻撃による組織への損失を見極めましょう
  - 何が発生すると組織にとって脅威なのか。ウイルス侵入ではなく、情報の窃取
  - 同じ攻撃であっても、環境や組織の形態によって脅威は変わってくる
- システム全体を見渡したトータルな対策
  - 一部分の対策では対策に漏れや、効率的・効果的な対策が行えなくなる
  - 入口対策に偏らず、出口対策にも視点を当てたバランスの取れた対策が重要


- 組織の運用形態に合った対策を
  - いくら万全のセキュリティ対策設備を整えても、運用ができなければ効果なし
  - 自分達で運用できることを念頭においた対策検討が重要

**他組織の脅威をそのまま自組織の脅威に当てはめて考えるのではなく、自組織の影響を分析して対策することが重要**

# 設計・運用ガイドについて

■『新しいタイプの攻撃』の対策に向けた設計・運用ガイド　2011/8/1 リリース
～Stuxnet(スタックスネット)をはじめとした新しいサイバー攻撃手法の出現～
http://www.ipa.go.jp/security/vuln/newattack.html


＜内容＞

- APT攻撃（新しいタイプの攻撃）の説明
- 攻撃仕様の分析
- 設計対策の考え方
- 対策補助資料の提供

# おわりに

IPAは、安心安全な情報システム、社会インフラの実現を目指します

## 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
http://www.ipa.go.jp/security/index.html
http://www.ipa.go.jp/security/vuln/index.html