IPA Information-technology Promotion Agency, Japan

標的型攻撃／新しいタイプの攻撃 の 実態と対策

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

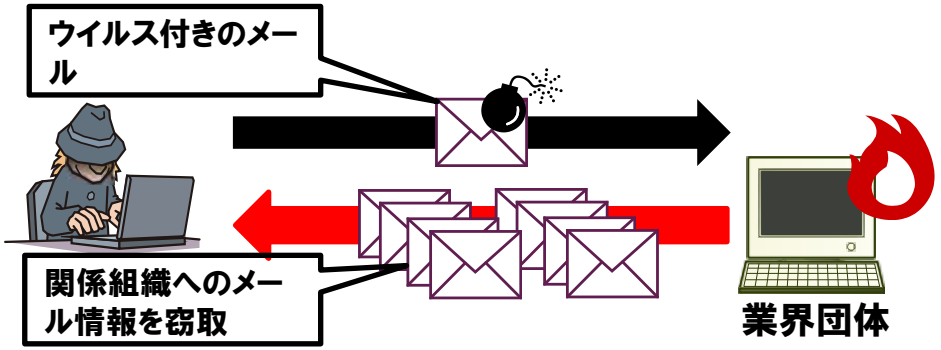
目次

某重工業企業へのサイバー攻撃
何が起こっていたのか？（1）～報道ベース～

IPA

某重工業企業へのサイバー攻撃で起こっていたこと

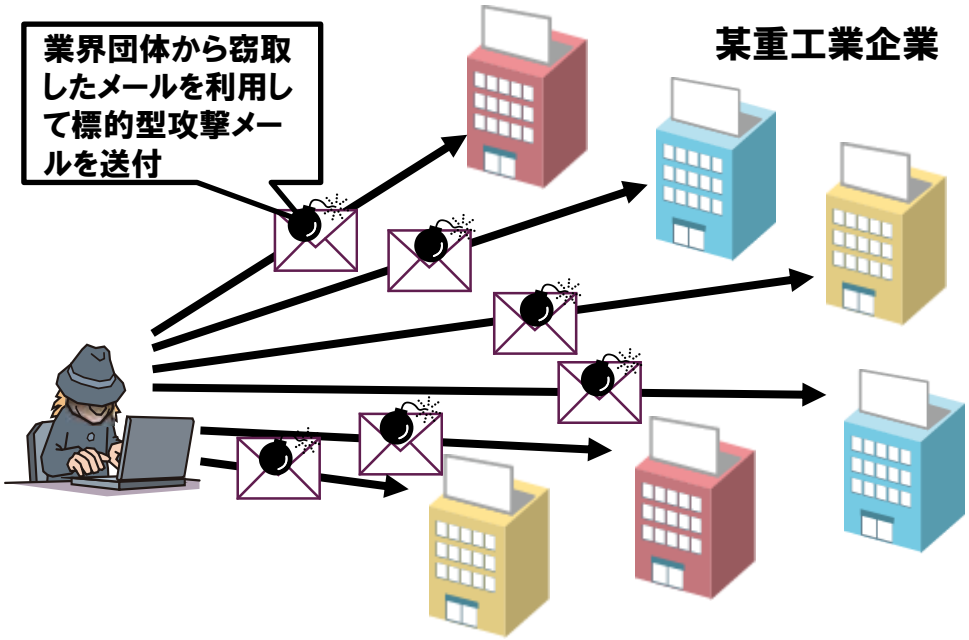
①
重工関係企業が所属する業界団体の職員のPCがウイルスに感染し、**関係企業とやり取りしていたメール情報**が盗まれた。



②
盗まれたメールを使用され、
関係企業に対して
標的型攻撃メールを送付された。
正規メール送付の約10時間後

その関係企業の中に、某重工業企業等が含まれていた。

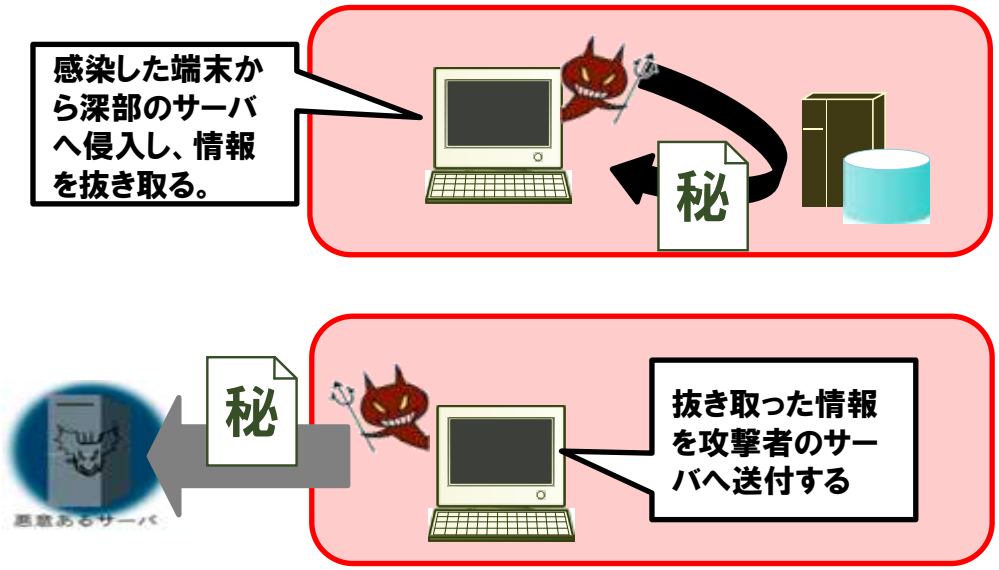
※複数の報道から導き出したシナリオです。



某重工業企業へのサイバー攻撃
何が起こっていたのか？（2）～報道ベース～

（某重工業企業の場合の被害）
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
- 外部通信を行われる

端末に感染したウイルスにより**内部サーバへ侵入され、一部の情報を抜き取られた可能性がある。**
抜き取られた情報を攻撃者のサーバ（米国サーバ）へ送付された模様。
機密情報の流出は確認されていない。



ある拠点のサーバへ情報が集約され送付された可能性

※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

今回の事件の教訓

（１）標的型攻撃は、攻撃目標に関係する組織も狙っている
- 関係が深く、セキュリティ対策の弱い組織や団体など。
- 信頼感のある（安心してメールを開いてしまう）組織や団体など。

（２）組織関係や業界団体活動に大きな支障を生じる可能性大
- 業界団体としての存立基盤である信頼関係が損なわれる。
- メールによる業務情報のやり取りが阻害される。

（３）セキュリティ対応があまいと、関係する組織にも大きな脅威となる。

- 各組織が社会的責任として充分なセキュリティ対策をとる。
- 業界が一丸となってセキュリティレベルの向上を図る。

脅威の動向
～このような事件が世界中で起こっている～

■ 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

これらの不正侵入は、金銭的な対価では無く、**企業や政府の機密情報や知的財産そのものを入手することを目的**に実行されるという特徴があります。そして過去5～6年間に、厳重に保護された**国家機密、ソースコード、バグデータベース、メールアーカイブ、交渉計画、新規油田・ガス田開発の入札に関する詳細な調査結果、ドキュメントストア、契約書、SCADAの構成図、設計図面**など、多くのデータが主として欧米の企業から不正に取得されているのが実態です。

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

脅威の動向
～巧妙な標的型攻撃の実例～

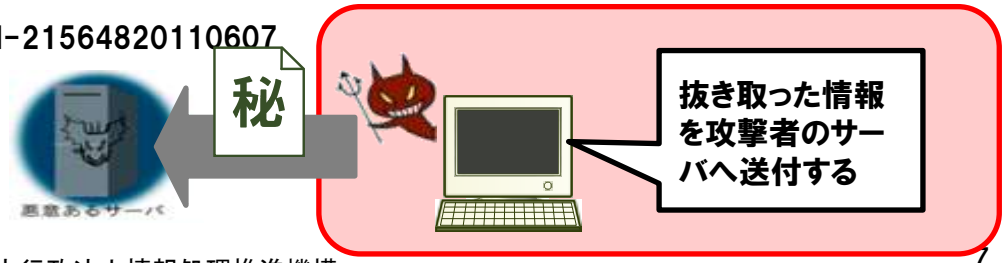
■ EMC Corporationのセキュリティ事業部門であるRSAのSecurIDに関する情報を盗まれたケース

「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。



目次

「標的型攻撃メール」とは

『標的型攻撃メール』の定義(IPA):
情報窃取を目的として特定の組織に送られるウイルスメール(*)。

注(*)ウイルスメールとは、ウイルスファイルを添付したり、ウイルスに感染するサイトに誘導する仕掛けをしたメールである。不特定多数に大量に送られ、感染すると、そのパソコンから更にウイルスメールをばら撒くマスメール型ウイルスメールと、少数の標的にだけ送られる標的型攻撃メールがある。

標的型攻撃メールの特徴

- 送信者名として、実在する信頼できそうな組織名や個人名を詐称
- 受信者の業務に関係の深い話題や、詐称した送信者が扱っていそうな話題
- ウイルス対策ソフトを使っていてもウイルスが検知されない場合が多い
- メールが海外のIPアドレスから発信される場合が多い
- 感染しても、パソコンが重たくなるとか変なメッセージが表示されることは余りない
- 外部の指令サーバ(C&Cサーバ)と通信
- 長期間にわたって標的となる組織に送り続けられる(内容は毎回異なる)

メール受信者が不信感をいだかないように、色々な「だましのテクニック」を駆使している

国内における標的型攻撃メールの歴史

年月	事象
2005年10月	実在の外務省職員を詐称して、ウイルスを埋め込んだMS Wordファイルが添付された日本語メールが複数の官公庁に届いた。
2006年5月	新聞社を詐称して、ウイルスを埋め込んだMS Wordファイルが添付された日本語メールが民間企業に届いた。
2007年7月	未修正の一太郎の脆弱性を悪用したウイルスメールが発見された。（ゼロデイ攻撃）
2007年10月	Adobe Readerの脆弱性を悪用してPDFファイルにウイルスを埋め込んだウイルスメールが発見された。
2008年11月	標的型攻撃メールに関する組織内の注意喚起メールを加工して、多数の従業員に標的型攻撃メールが届いた。
2009年7月	添付ファイルのない標的型攻撃メールが発見された。
2011年3月	地震や原発事故を話題にした標的型攻撃メール多発。
2011年7月	おれおれ詐欺を模倣した標的型攻撃メールが発見された。
2011年9月	防衛、重工関連企業などで標的型攻撃の被害発生。

ウイルスメールの形態の変化

マスメール型ウイルスメール → 標的型攻撃メール

	マスメール型	標的型攻撃
ターゲット	セキュリティ対策の不十分なPC	特定の組織の情報
宛先	不特定多数	少数の組織
送信者	知らない人	信頼できそうな組織や人物
ウイルス対策ソフト	大半は検知	ほとんど検知不可
話題	誰にでも関係のある話題	受信者に関係が深い話題
記述言語	ほとんど英語	日本語など受信者が通常使う言語
添付ファイル	実行形式（exe）	pdf や doc などの文書ファイル
感染拡大	感染したPC内から自身をメール再発信	再発信せず
感染後の症状	何らかの異常な症状	特に気付くような症状なし

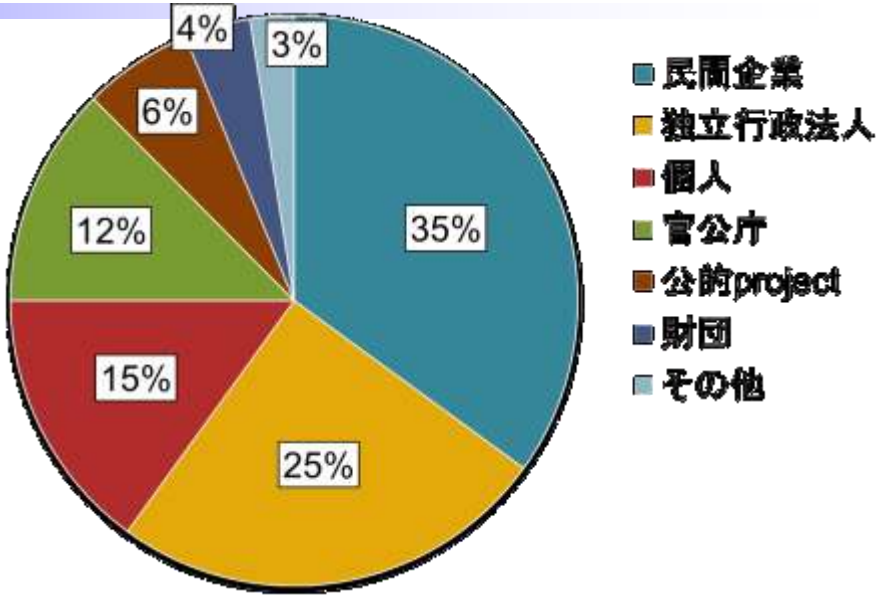
標的型攻撃メールに騙される場合と気付く場合

- ウェブ等で公表されている情報を加工
  - メール受信者が信頼しそうな組織がウェブで公開している情報をそのままコピーして使うので、内容や表現が適切に見えた為、添付ファイルを開く。
    - 普段そのようなメールを送ってくる人からではないので、不審に感じて気付く。
- 組織内の業務連絡メールを加工
  - 関係者のPCから、業務連絡メールを盗み、それを元にウイルスメールを作成する為、メール受信者にとって、ほとんど疑う余地のない正規のメールに思えて開く。
    - 添付ファイルを使うことが不自然に感じて気付く。
- 添付ファイルのないウイルスメール
  - 添付ファイルがなければ危険ではないと思い込んでリンクをクリックする。
    - 接続先のURLが不適切と気付く。
- おれおれ詐欺を模倣
  - 知らない人の名前で添付ファイルやURLリンクの書いてない普通のメールを何回かやりとりし、不信感がなくなった頃、写真を見ろと添付ファイルが送られ、開く。
    - 添付ファイルを開く前に、メールを送ってきた人が本当に信頼できるのか自問することで不審に気付く。

IPAに届けられた標的型攻撃メールの分析（１）

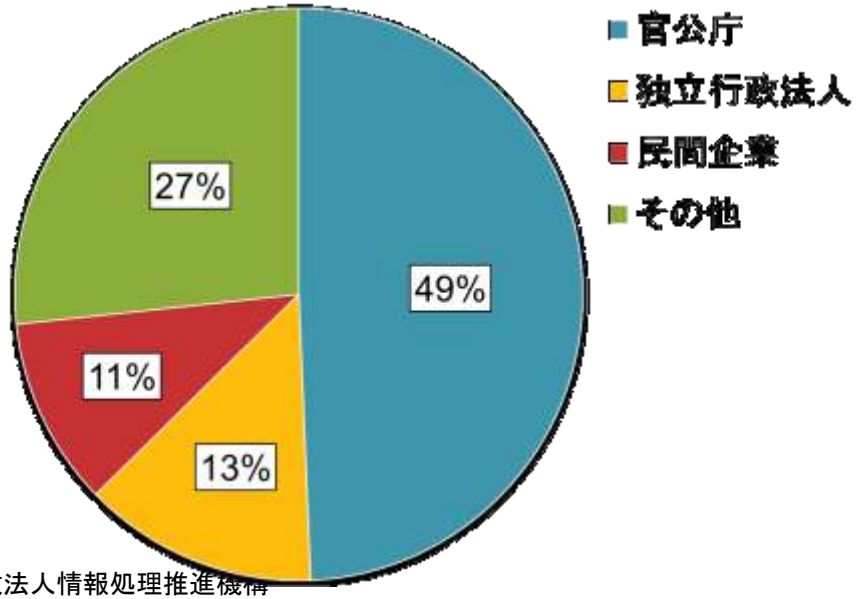
(1) 標的型攻撃メールの送信先

- **民間企業、独立行政法人、個人**の順に多くなっています。
- 官公庁が少ないのは、官公庁に届く標的型攻撃メールの情報は、内閣官房情報セキュリティセンター（NISC）で集約しているためと推察します。
- 個人は、組織と無関係なプライベートなメールアドレスに届いたということですが、その個人が所属する組織や、関係者を標的にしていると思われます。



(2) 標的型攻撃メールが詐称する送信元

- 標的型攻撃メールの多くは、**官公庁や独立行政法人のような公的機関を詐称**していることが多いです。公的機関の組織名をかたることで、**メール受信者の不信感を減らそうとしている**と思われます。
- その他は、メール受信者に関係のある団体名などです。



IPAに届けられた標的型攻撃メールの分析（２）

(3) 標的型攻撃メールの記載内容の傾向

- 標的型攻撃メールのタイトルや本文の内容を「イベント」「報告書」「ニュース・注意喚起」という項目で分類してみましたが、**特に傾向はない**ようです。

- メールの内容から、単なる「公開情報」の紹介か、「組織内限定」の業務連絡か、組織を横断した「関係者限定情報」かで分類してみると、「関係者限定情報」を扱っているメールが半分以上ありました。**「関係者限定情報」だと、自分にそれほど関係なくても自分に届くことに不信をもたずに開いてしまう心理をついている**と思われます。

テーマ事例は、実際の文言ではなく、抽象化してあります。

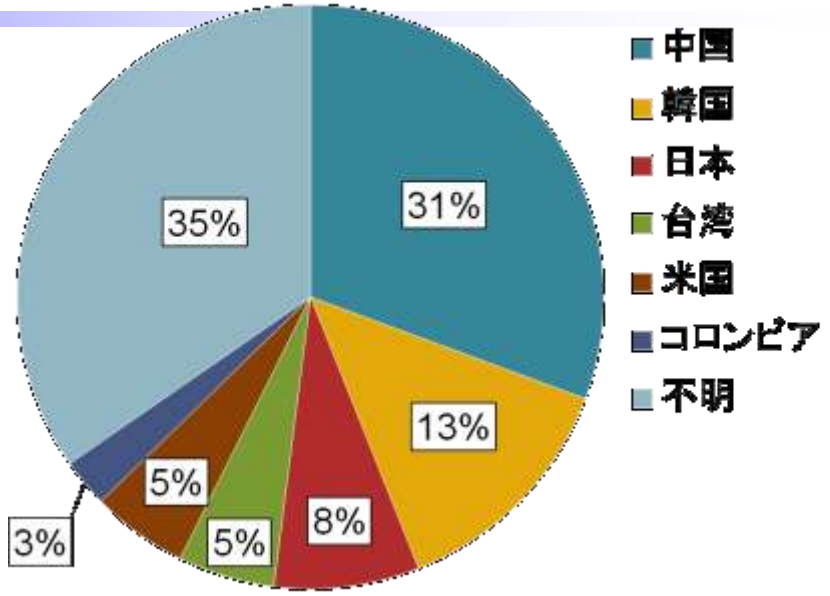
分類	割合	テーマ事例（抽象化済）
イベント	38%	国際会議、シンポジウム、研修会、選挙、法令改正、VIP会合日程、役員人事異動、来訪者情報、社内ウイルス調査
報告書	32%	外交機密文書、国際情勢、海外資源、政府部局報告書、情報セキュリティ調査、ウイルス・不正アクセス届出状況、会議資料
ニュース注意喚起	30%	東日本震災、金融情勢、国際情勢、外交情報、政府予算、製品事故、情報セキュリティ注意喚起、新型インフルエンザ

分類	割合	テーマ事例（抽象化済）
関係者限定情報	53%	選挙、演説原稿、法令改定、外交情報、法人実態調査、海外資源、来訪者情報、VIP会合日程、国際会議、政府部局報告書、情報流出事故
公開情報	38%	東日本震災、新型インフルエンザ、情報セキュリティ注意喚起、情報セキュリティ調査報告、国際情勢、シンポジウム、金融情勢、経済外交、政府予算、製品事故、経済成長戦略
組織内限定	9%	不審メールの注意喚起、社内ウイルス調査、組織内業務連絡、役員人事異動

IPAに届けられた標的型攻撃メールの分析（３）

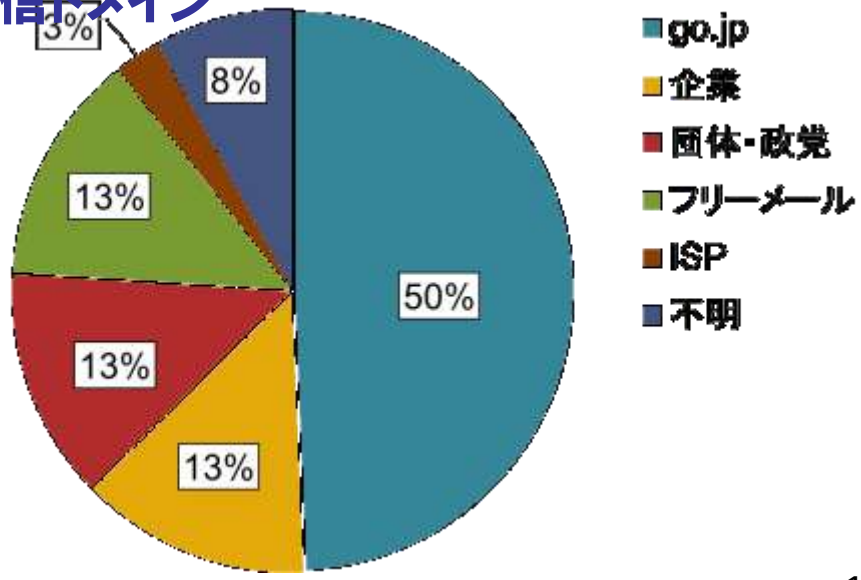
(4) 標的型攻撃メール発信元のIPアドレス

- メールヘッダに記録されている、メールを発信したIPアドレスを調べると、中国が30%以上を占めています。
- ほとんどは、**日本の組織をかたっています**が、**日本のIPアドレスから発信される場合は少ないです**。
- 不明は、IPAに御提供いただいた検体にメールヘッダが含まれていないためです。



(5) 標的型攻撃メールの(詐称している)発信ドメイン

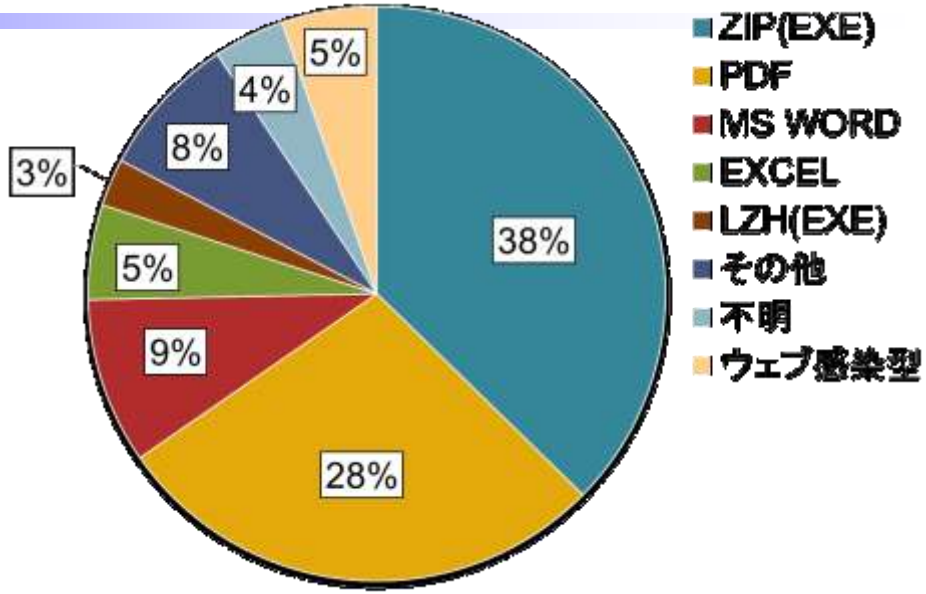
- **メールヘッダの From: を詐称することは容易**であり、官公庁や独立行政法人などが使用している、**go.jpというドメインのメールアドレスが約半分**を占めます。
- 標的型攻撃メールの多くは、攻撃者と無関係な第三者のパソコンを踏み台にして発信していると推察されますが、メールサーバを詐称して送るとメールを受信しないメールサーバが増えているため、YahooやGmailのようなフリーメールアドレスを使うことがあります。



IPAに届けられた標的型攻撃メールの分析（４）

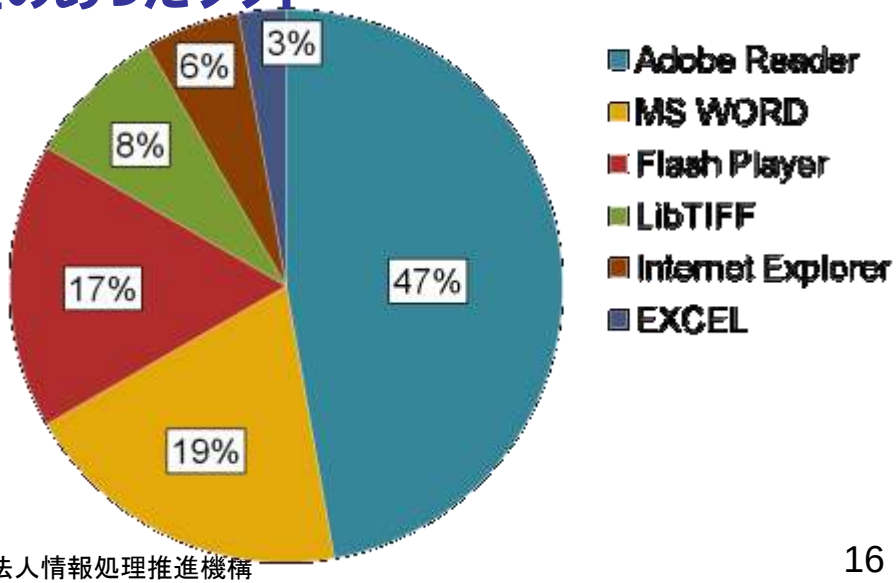
(6) 標的型攻撃メールの添付ファイル

- メールの添付ファイルとしては、**最初の頃は、MS word や Excel の脆弱性を悪用しウイルスを埋め込む例**が多かったです。
- その後、**Adobe Readerの脆弱性を悪用してPDFファイルにウイルスを埋め込む例**が増えました。
- 最近は、アイコンやファイル名をMS Word の文書ファイルように偽装した exe ファイルが増えています。



(7) 標的型攻撃メールで悪用された脆弱性のあったソフト

- PDF ファイルや MS Word, Excel ファイルのような文書ファイルにウイルスを埋め込む場合、その文書ファイルを開くアプリケーションの脆弱性を悪用して、内部のウイルスを起動する必要があります。
- 最近は、Adobe Reader の脆弱性を悪用する例が増えています。



標的型攻撃メール対策

標的型攻撃メールの見分け方

- 普段メールをやりとりしていない人から、添付ファイル付きのメールが届いた
- そのメールを何故自分に送ってきたのか心当たりがない
- ファイル拡張子が exe のような実行形式（圧縮ファイルの場合は、その中身）
- ファイル名が文字化けしている

標的型攻撃メールが届いた場合の対応

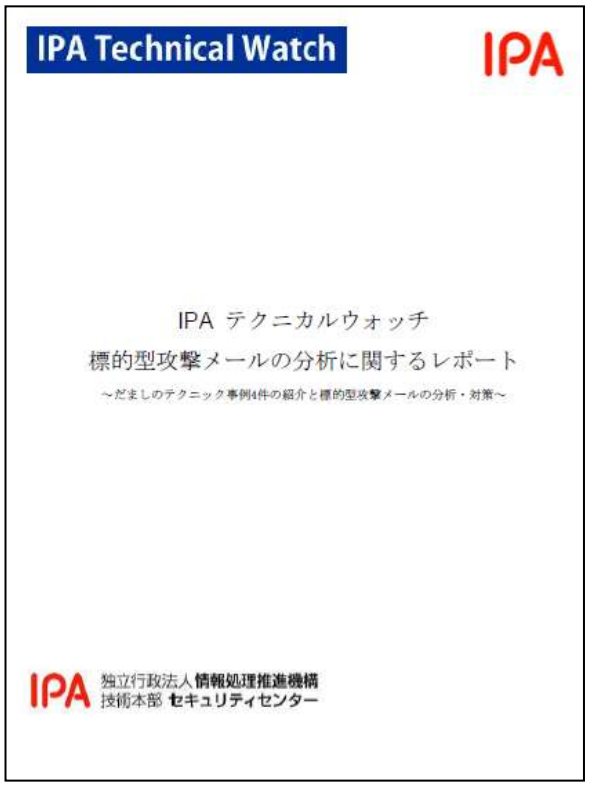
- 電話番号案内（104）やウェブから、メール送信者の連絡先を調べ、そのメールを送ったか直接確認する。
- メール送信者がなりすましと判明した場合、組織内の情報システム部門などセキュリティ対策部門に報告し、指示を仰ぐ。
- 組織内のセキュリティ対策部門は、当該メールにウイルス感染の仕掛けがあるか調べるとともに、同様の攻撃メールが他の人に届いていないか調査し、注意喚起する。

関係機関への届出

- 同じ攻撃者から他の組織に対して同様の攻撃メールが届いている可能性があるので、IPAの相談窓口に連絡する。 => 第5章「IPAの取組」を参照。

標的型攻撃メールの分析レポートの公開

■IPA テクニカルウォッチ
『標的型攻撃メールの分析』に関するレポート　2011/10/3 リリース
～だましのテクニックの事例4件の紹介と標的型攻撃メールの分析・対策～
http://www.ipa.go.jp/about/technicalwatch/20111003.html



＜目次＞

目次

「新しいタイプの攻撃」とは

『新しいタイプの攻撃』の定義(IPA):
ソフトウェアの脆弱性を悪用し、複数の既存攻撃を組み合わせ、ソーシャル・エンジニアリングにより特定企業や個人を狙った攻撃の総称。

攻撃の特徴の一例

- ソーシャルエンジニアリングの活用による巧妙なアプローチ(侵入)
- ゼロデイの脆弱性の利用
- ネットワーク/USBデバイスによる拡散
- 外部の指令サーバ(C&Cサーバ)との通信
- 個別システムに特化した攻撃

個々の攻撃が防御システムを回避するように巧みに組合わさり、攻撃目標に合わせて設計されている

「新しいタイプの攻撃」の事例

- Google、Yahoo! を狙った攻撃 (Operation Aurora)
  - Google,Yahoo!,Symantec,Adobe System など30余りの企業を標的とした攻撃
  - ソフトウェア構成管理(SCM: Software Configuration Management)などの知的財産を詐取する(攻撃者の狙い)
  - Googleの中国撤退騒動など、国際的な問題にまで発展
- イランの原子力施設を狙った攻撃の発生 (Stuxnet)
  - 原子力施設の制御システムが攻撃のターゲットになったことで世界的に注目
  - ドイツ・シーメンス社の制御装置の動作に異常をきたすことに特化したウイルスであった
- 日本を含めた某重工業企業への攻撃
- 米国セキュリティ関連企業を狙った攻撃

これらの攻撃は、海外では「APT (advanced persistent threat:高度かつ継続的な脅威)」とも呼ばれる攻撃手法である

「新しいタイプの攻撃」の分析

IPA

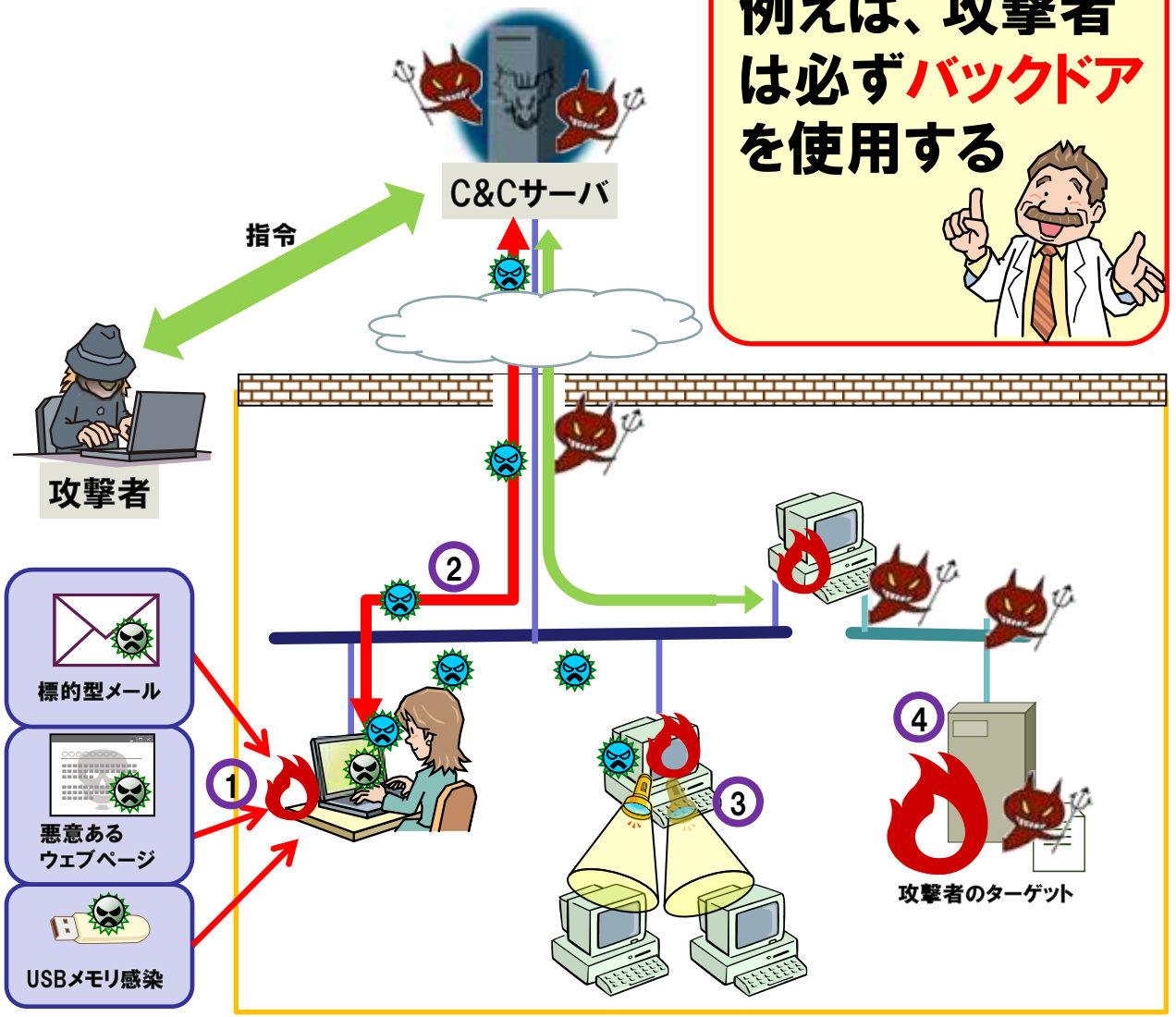
⓪ **[事前調査]**
ターゲットとなる組織を攻撃する為の情報を収集

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

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



例えば、攻撃者は必ずバックドアを使用する

「新しいタイプの攻撃」の分析

- 標的型攻撃メールにおいても次のような流れで攻撃が侵攻する
- この流れにおいては、**共通的な攻撃手法**を使用している

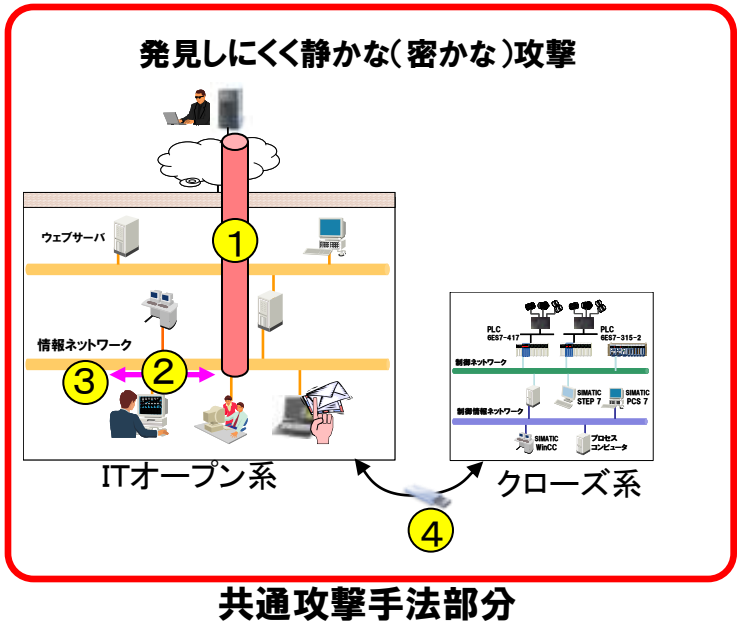
段階	攻撃内容	特徴
第1段階 ［初期潜入段階］	（1）各種初期攻撃 ・標的型攻撃メール添付ウイルス ・ウェブ改ざんによるダウンロードサーバ誘導 ・外部メディア（USB等）介在ウイルス など	入口の対策をすり抜け、システム深部に潜入 素早く次の段階へ移行。 攻撃手法は使い捨て
第2段階 ［攻撃基盤構築段階］	（1）バックドア（裏口）を使った攻撃基盤構築 ・ウイルスのダウンロードと動作指示 ・ウイルスの拡張機能追加	構築した攻撃基盤は発見されない。 構築した攻撃基盤は再利用される。
第3段階 ［システム調査段階］	（1）組織のシステムにおける情報の取得 （2）情報の存在箇所特定	時間をかけて何度もしつこく行う。
第4段階 ［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 （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。 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

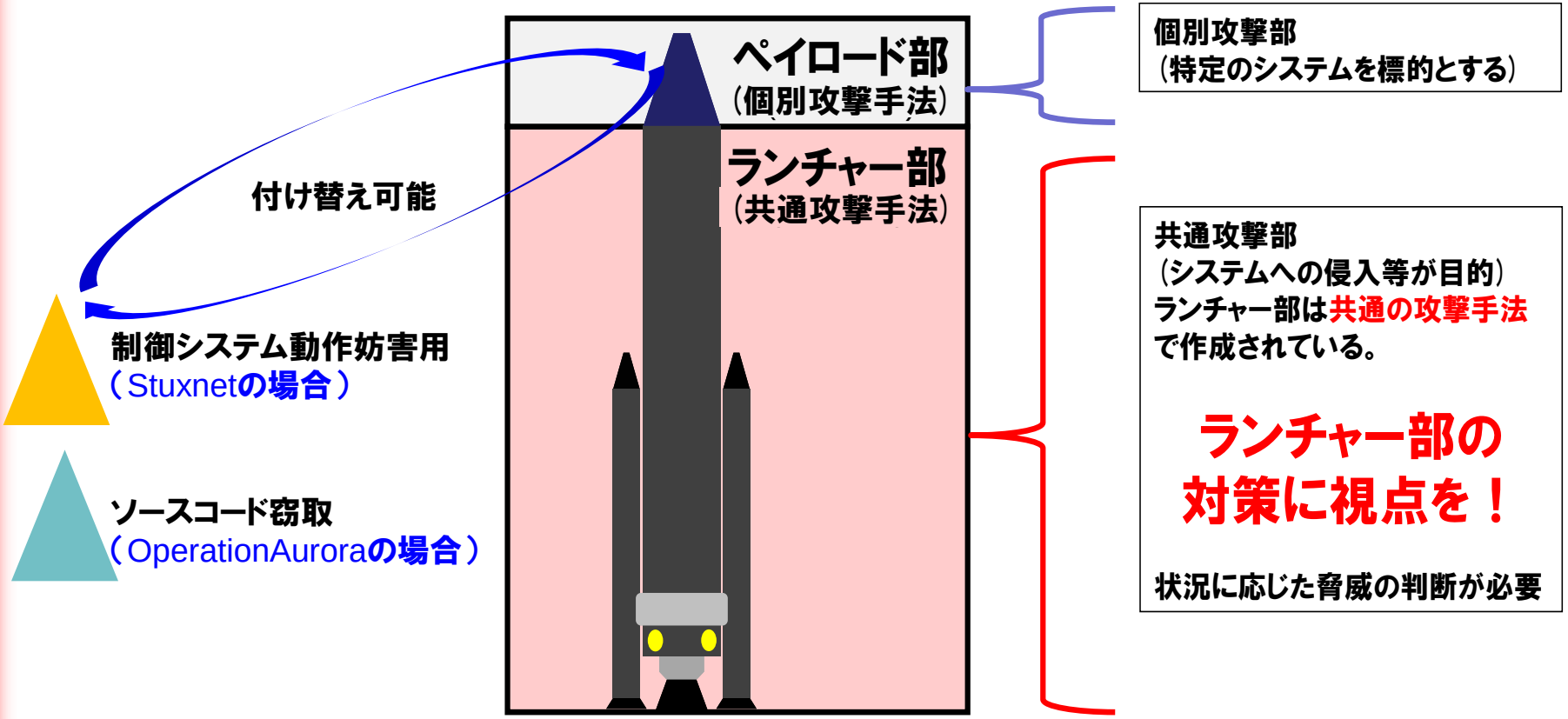
番号	共通攻撃手法機能	役割
①	httpバックドア通信機能	ウイルスと攻撃者のサーバとの通信を確立
②	システム内拡散機能	システム内の情報窃取の効率化のため、多くの端末に感染させる
③	一斉バージョンアップ機能	システム内のウイルスに効果的な攻撃を行わせる機能を持たせるようにする
④	USB利用型情報収集機能	クローズ系システムの情報を収集するためUSB等にそのような機能のウイルスを入れ込む



共通攻撃手法部分

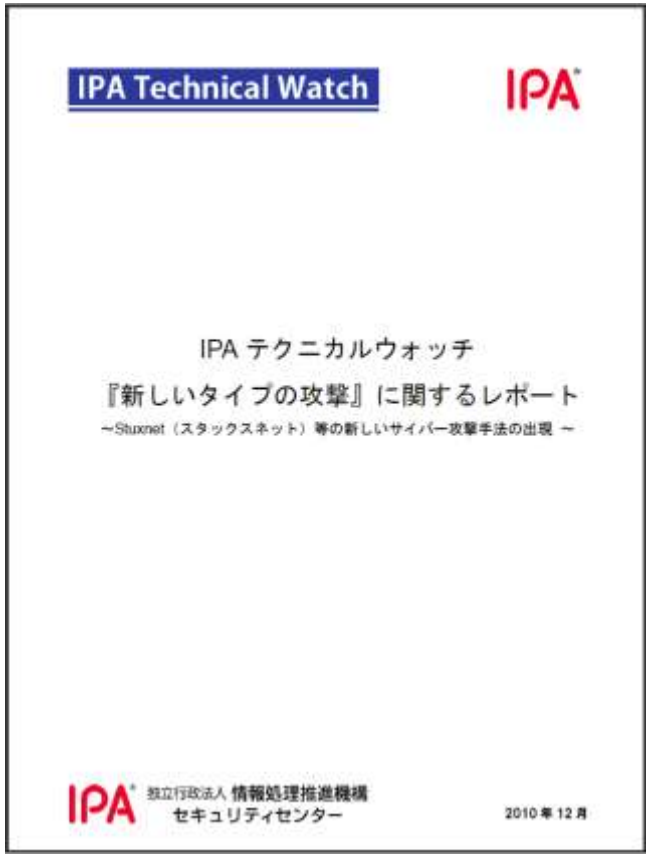
「新しいタイプの攻撃」のイメージ

『新しいタイプの攻撃』をロケットの例で考えてみると、システムへの攻撃に特化したペイロード部と特定のシステムに侵入する為の共通仕様部分のランチャー部に分けることができる。



『新しいタイプの攻撃』に関するレポート

■IPA テクニカルウォッチ
『新しいタイプの攻撃』に関するレポート　2010/12/17 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/about/technicalwatch/20101217.html



＜目次＞

目次

対策の考え方

組織の守るべき資産の明確化、リスクの評価に基づいて、一つの対策だけでなく、多層の防御が重要である。

① 脅威は極力上流で食い止める
　技術的対策だけでなく、標的型メールの取扱い規則も重要
② 侵入を阻止できなかった時の攻撃活動の抑止、被害の極小化を図るための対策を考えておく
③ 最後の砦となる守るべき情報の保護の強化
④ システム全体の監視と証跡の分析
⑤ 組織全体のセキュリティマネージメントやコンティンジェンシープランの整備

対策の全体像（１） ～入口対策～

IPA

（1）システムへの入口と経路での防御
- □ ファイアウォール
- □ 最新のウイルス対策ソフト（ネットワーク、サーバー、クライアント）
- □ 侵入検知システム／防止システム
- □ ネットワーク構造／設計（重要なサーバーに対するルート制御やネットからの隔離）

（2）脆弱性対策
- □ OSやサーバーソフトウェアの定期的な脆弱性診断
- □ ウェブサイトで使用しているOSやサーバーソフトウェアに関する脆弱性情報の、時期を逸しない収集とパッチの反映
- □ ウェブアプリケーションへの脆弱性の作り込みの回避
- □ ウェブアプリケーションファイアウォール（WAF）

（3） 標的型攻撃ルートでの対策
- □ スパムフィルター
- □ URLフィルター
- □ 外部メディア利用規則、強制利用抑止

対策の全体像（２）～出口対策、情報保護～

（4）ウイルス活動の阻害および抑止（出口対策）

- □ 端末間、他部署間のネットワーク通信の制限（ウイルスの組織内蔓延抑止）
- □ 組織の端末からの外部通信はプロキシを経由させる等の経路制御
- □ 組織内ネットワーク量の監視（異常さを早期に検知し、ウイルスの蔓延を早期に発見）
- □ 知財等のある重要なサーバーはインターネットから隔離

（5）アクセス制御

- □ ユーザ認証
- □ アクセスするプログラムの特定（ホワイトリスト化）

（6）情報の暗号化

- □ 通信路の暗号化（Virtual Private Networkなどの利用）
- □ ファイルの暗号化
- □ 暗号鍵管理

対策の全体像(３) ～監視、管理統制～

(7) システム監視、ログ分析

- □ ネットワークログ取得・分析
- □ サーバログ取得・分析
- □ アクセスログの監査(DB監査ツールなど含む)

(8) 管理統制およびコンテンジェンシープラン(事前準備・事後対応)

- □ セキュリティポリシー
- □ 海外を含むグループ会社間でのセキュリティガバナンス
- □ 危機対応体制の整備

上記(1)－(8)を現状対策のチエックリストに活用して下さい。
それぞれの組織において、
- ・現状把握
- ・リスク分析(脅威、資産、脆弱性)
- ・システムのライフサイクル(拡張や更改など)

などに基づいて、緊急対策、計画的対策を組み合わせて、
セキュリティレベルの向上に努めて下さい。

目次

IPA「脅威と対策研究会」

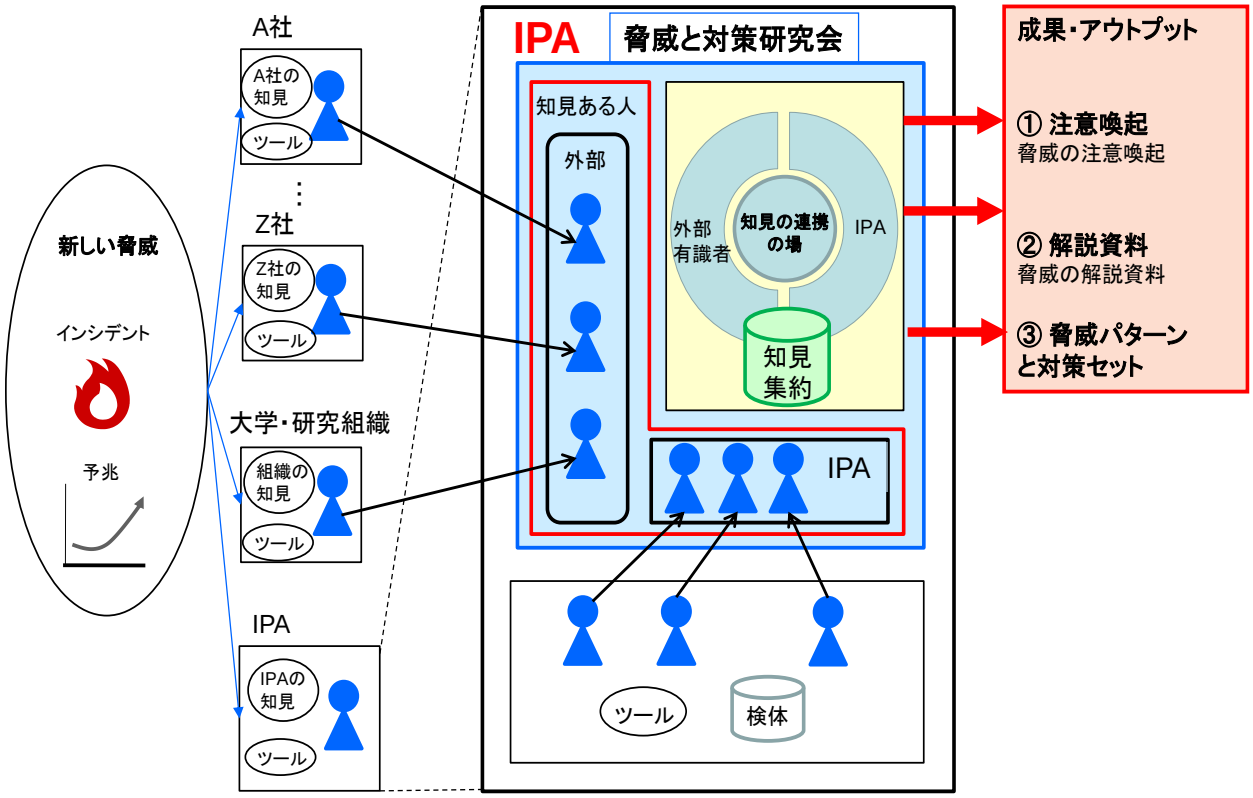
IPA「脅威と対策研究会」（2010.12 ～）

- SIベンダ、セキュリティベンダ、大学関連等の有識者で構成
- 「新しいタイプの攻撃」に関する攻撃の特徴の分析および対策の検討等を行う

研究会アウトプット

2010年12月公表：
IPA テクニカルウォッチ
『新しいタイプの攻撃』に関するレポート

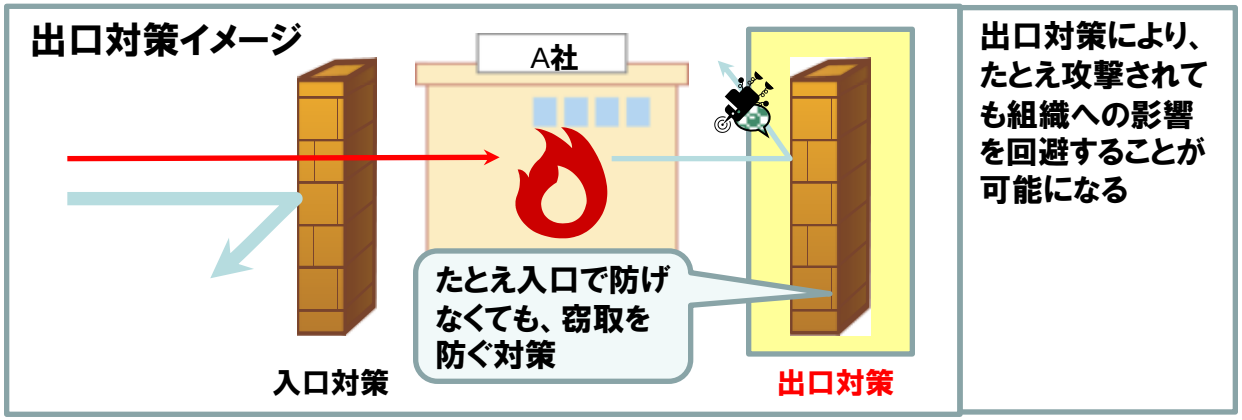
2011年8月公表：
「新しいタイプの攻撃」の対策に向けた設計・運用ガイド



「出口対策」とは

全体的なセキュリティの中で、「IPA脅威と対策研究会」で検討を実施している対策が「出口対策」である。

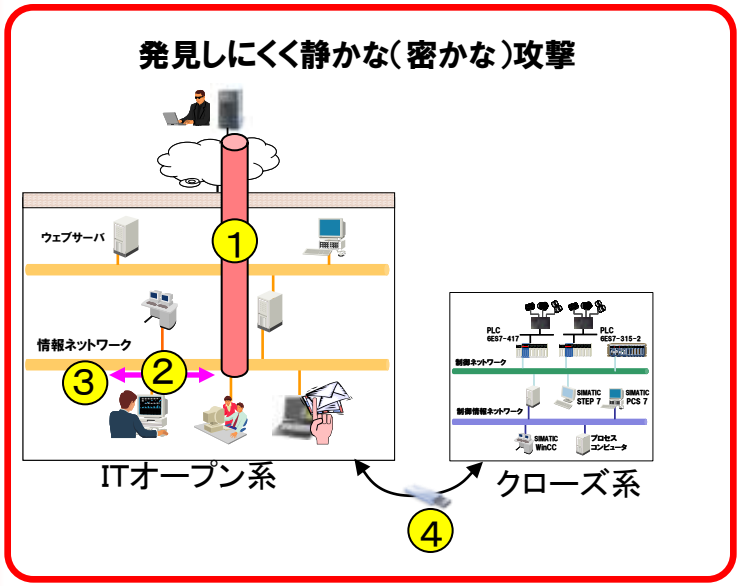
出口対策とは、たとえ入口対策をすり抜けた場合においても、**攻撃者に情報を窃取させないことや、重要システムを破壊させないことを目的**として、組織に入り込んだウイルスと攻撃者の通信を発生させないための対策



「出口対策」とは

■ 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

共通攻撃手法を止める6つの出口対策

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

対策	目的	手法
① サービス通信経路設計	httpバックドア通信の防止 ✓ 独自プロトコルの使用 ✓ システムプロキシ経由しない通信	1.ファイアウォールの外向き通信の遮断ルール設定 例）プロキシ経由以外の80番ポートを除外 2.ファイアウォールの遮断ログ監視
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	httpバックドア通信の防止 ✓ http通信を模倣した通信	httpメソッド利用バックドア通信の遮断 例）プロキシがウイルスには理解できない（ブラウザは理解できる）返答を返す
③ 最重要部のインターネット直接接続の分離設計	最重要部にバックドアを設置させないための対策	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
④ SW等でのVLANネットワーク分離設計	ウイルスの拡散範囲限定と検知	利用者セグメントと管理セグメントを分離設計する等
⑤ 容量負荷監視による感染活動の検出	ウイルスの拡散範囲限定と検知	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
⑥ P2P到達範囲の限定設計	ローカルセグメントに感染したウイルス間での一斉アップデート等の防止	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

出口対策の適用例

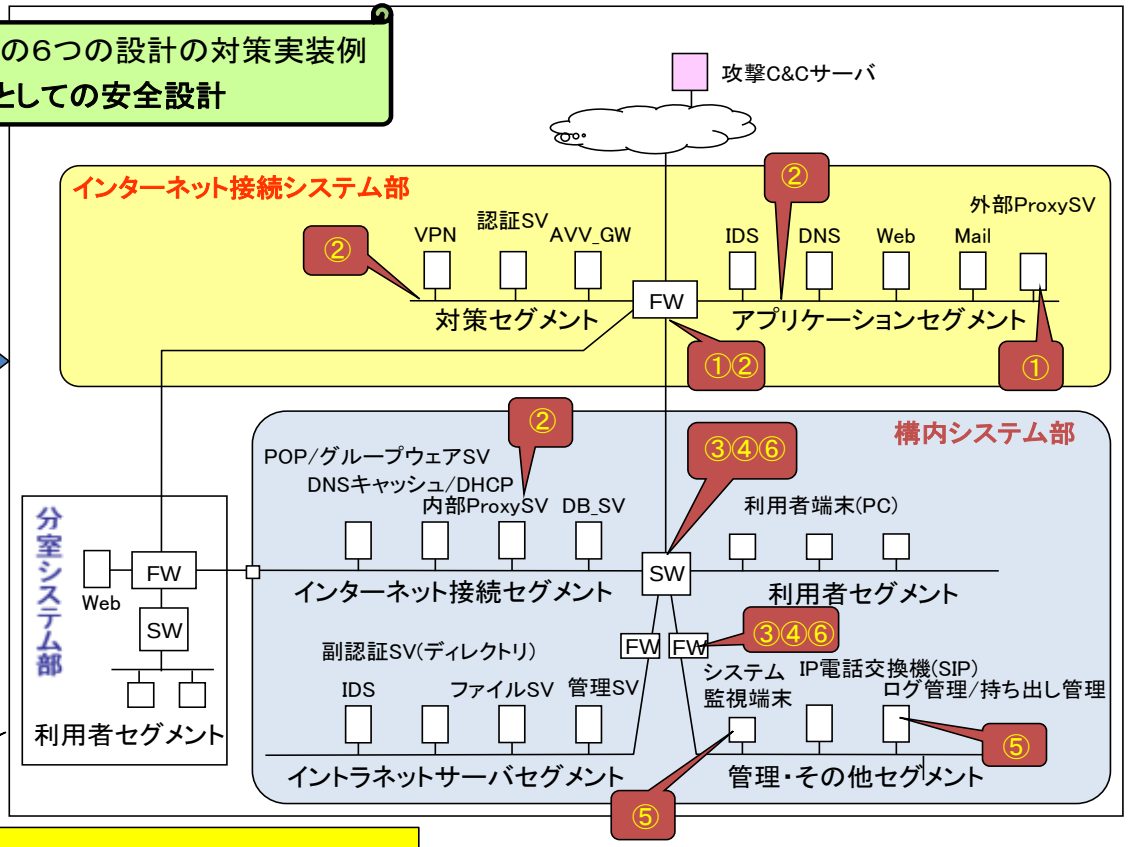
設計対策システム設計実装図例

標準的なシステム構成図上での6つの設計の対策実装例
システムの出口対策としての安全設計

システム基本図

システムのサービス通信フローを分析した上で、設計対策項目の実装を検討。

この際、新しいタイプの攻撃のシステム上の共通攻撃通信フローを分析



情報システムに対する6つの出口対策（設計対策）の機能配置
①サービス通信経路設計の実施
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（一部調査中）
③最重要部のインターネット直接接続の分離設計
④SW等でのVLANネットワーク分離設計
⑤容量負荷監視による感染動作の検出
⑥P2P到達範囲の限定設計

各対策項目の設計該当箇所の実装図を参考にして、システム設計を行う。

設計・運用ガイドの公開

■「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＞

- エグゼクティブサマリ（1章）
  経営層を対象として、「新しいタイプの攻撃」の解説とその対策における考え方を記載。

- 「新しいタイプの攻撃」の問題と背景（2章）
  「新しいタイプの攻撃」への対策の提案・指示等を行うプロジェクト管理者を対象として、「新しいタイプの攻撃」の概要の解説と、対策を行う際の設計における考え方を記載。

- 「新しいタイプの攻撃」への対策（3,4章）
  「新しいタイプの攻撃」への対策を実際に設計する方、実装する方を対象として、「新しいタイプの攻撃」を5つのパターンに分類し、それら5つのパターンに有効な6つの対策を提示。

目次

脆弱性のない安全なシステムの開発、運用に向けたIPAの取組み

IPA

セキュリティ対策

- 調査、動向把握、開発方針・体制整備（ビジネスインパクト分析含む）
- セキュアプログラミング
- ソースコード検査
- テスト（ファジング他）
- 脆弱性診断（ペネトレーション）
- 運用時対策
- 脆弱性対策

システムライフサイクル

1. 企画 → 2. 設計 → 3. 実装 → 4. テスト → 5. 運用／利用 → 6. 廃棄

- 脅威、動向：1. 企画
- 脆弱性：2. 設計、3. 実装、4. テスト
- 攻撃：5. 運用／利用

IPAの活動・成果物

- 10大脅威
- 情報セキュリティ白書
- 知っていますか？脆弱性

＜調査・ガイド類＞
- 組込みシステム向け
- 情報家電向け
- 制御システム向け
- 自動車向け
- 生体認証導入、運用ガイド

- 安全なWebサイトの作り方
- 安全なSQLの呼び出し方
- セキュアプログラミング講座
- 開発者向け脆弱性実習ツール：AppGoat
- 「ソースコード検査ツール
- 「新しいタイプの攻撃」の対策に向けた設計・運用ガイド

- TCP/IP脆弱性検証ツール
- SIP脆弱性検証ツール

- Web攻撃検出ツールiLogScanner
- WAF読本
- 安全なWebサイト運営入門
- 5分でできる！情報セキュリティポイント学習

【届出制度／脆弱性／ウイルス】
- 脆弱性届出制度（PP/Web）
- JVN, JVN iPedia, MyJVN
- ウイルス、不正アクセス届出制度
- 安心相談窓口

IPAの取組み（１） ～ウイルス・不正アクセス届出～

ウイルス・不正アクセス、標的型攻撃メールなどの届出をお願いします

■ ウイルス・不正アクセスの届出

IPAは、経済産業省の告示に基づき、コンピュータウイルス及び不正アクセスの届出を受付け、毎月国内の被害状況を統計データとして公表するとともに、被害の事例紹介や必要に応じて、注意喚起、緊急対策情報などを随時発信しています。

【届出】 http://www.ipa.go.jp/security/todoke/

【報告】 http://www.ipa.go.jp/security/txt/list.html

【注意喚起】 http://www.ipa.go.jp/security/announce/alert.html

■ 「情報セキュリティ安心相談窓口」の開設

IPAは、コンピュータウイルスをはじめとする不正なプログラム（マルウェア）や不正アクセスに関する総合的な相談窓口を開設しています。

http://www.ipa.go.jp/security/anshin/

電話：03-5978-7509 （平日 10:00～12:00、13:30～17:00）

FAX：03-5978-7518 e-mail：anshin@ipa.go.jp

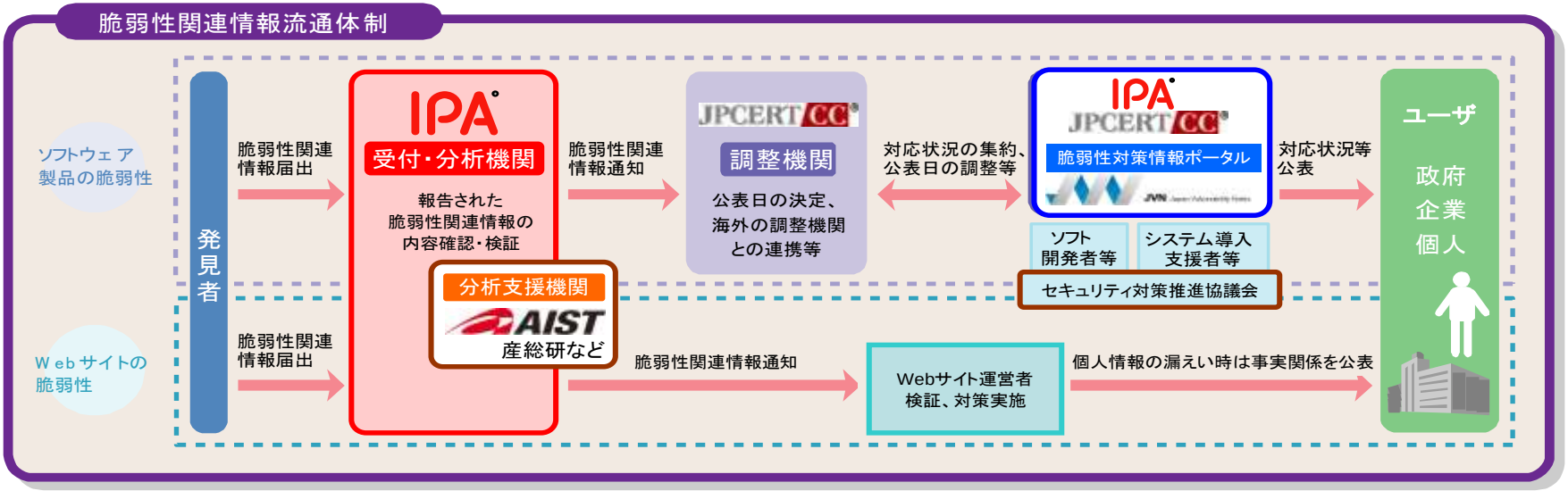
★ オペレータに、標的型攻撃メールと思われる不審メールを受け取ったと伝えてください

IPAの取組み（２）～脆弱性対策～

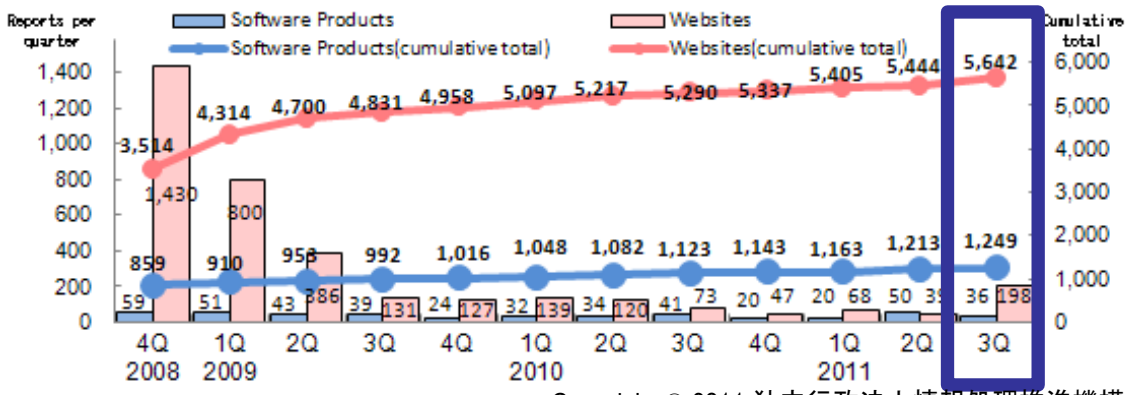
脆弱性関連情報の届出制度（情報セキュリティ早期警戒パートナーシップ）

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

2004年7月に経済産業省が「ソフトウエア等脆弱性関連情報取扱基準」（平成16年経済産業省告示第235号）を公示し、「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」に則り運用を行っている。



※JPCERT/CC：一般社団法人 JPCERT コーディネーションセンター、産総研：独立行政法人　産業技術総合研究所



2011 3Q(Jul-Sep)

分類	件数
ソフトウエア	1,249
ウェブサイト	5,642
累計	6,891

IPAの取組み（３）～脆弱性対策～

MyJVNバージョンチェッカ　http://jvndb.jvn.jp/apis/myjvn/

MyJVNを利用して、使っているソフトウェアが最新か、確認をして下さい。

- 利用者のPCにインストールされているソフトウェア製品のバージョンが最新であるかを、 簡単な操作で確認するツール
- チェックリストに基づき、バージョンが最新であるかどうかのチェックを手作業ではなく、ツールにより作業を自動化する。
- サーバーソフトやサーバOS (Win,Linux) でも動作可能　【2011年8月】

CPE common platform enumeration

OVAL oval.mitre.org

XCCDF

サイバー情報共有イニシアティブ（J-CSIP）における情報処理推進機構（IPA）の取り組み

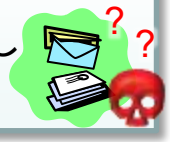
標的型サイバー攻撃に対しては、個別企業の利害関係を越えた情報共有が社会全体の観点での最大のメリット。IPAは公的機関として、NDA※の締結を前提に、メンバー企業間の信頼できる情報ハブ（集約点）の役割を担う。

※ NDA: Non-Disclosure Agreement、秘密保持契約

※ J-CSIP: サイバー情報共有イニシアティブ

1 「標的型サイバー攻撃特別相談窓口」の設置

ITユーザーが標的型攻撃を受けた際、駆け込み寺として、専門的知見を有する相談員による窓口を設置。



2 情報の匿名化 ＋ メンバー間での情報共有

標的型攻撃メールの内容や攻撃に使用されたウイルス等の分析結果を、信頼できる情報ハブを介して情報共有することにより、同様の標的型サイバー攻撃を未然に防止する。

※『標的型攻撃に関する情報共有枠組みのパイロットプロジェクト』と積極的に連携

3 標的型サイバー攻撃の実態調査

メンバー企業より提供された標的型攻撃メールを分析するとともに、IPAが特に「重大な攻撃が発生している」と判断する場合、対象メンバー企業の協力のもと、攻撃の実態調査を行う。

（例）・検出された不審なファイルの分析
・現地での一次調査