日本システム監査人協会 近畿支部　定例研究会

標的型攻撃をはじめとするサイバー攻撃の現状と対策

2015年11月20日

植垣 雅則

システム監査技術者、公認内部監査人 (CIA)

※本セミナー資料における意見にわたる部分は、講演者の個人的見解であり、所属する法人や団体の公式見解ではありません。

目次

【講演概要】
日本年金機構を狙った標的型メール攻撃により大量の個人情報が流出する事案が発生するなど、サイバー攻撃による情報セキュリティの脅威は どんどん高まっています。サイバー攻撃の手口がますます巧妙化･複雑化する中、組織としてサイバー攻撃に備えるには、管理面･技術面の両方から情報セキュリティ対策を高度化する必要があります。
本講演では最近の発生事案を例にとり、課題を整理するとともに、どのような対策が考えられるかについて解説します。
また、システム監査人として、どのような役割を果たせるかについて考察します。

1．標的型メール攻撃

1.標的型メール攻撃
はじめに

- 大手メーカーや政府機関が「標的型攻撃メール」により被害を受けたことを公表するなど、「標的型攻撃メール」による機密情報の窃取等は2011年度以降、社会的な課題となっています。当攻撃の特徴はメールを本物らしく偽装して、受信者にクリック等の操作をさせ、さらにパソコンに脆弱性（ソフトの問題点）が残っていれば、それを悪用してウイルスに感染させるとの手口です。さらに、感染しても以前のウイルスのように目立った変化がなく、感染していることに長期間気付かないこともあります。
- 攻撃者は金銭的な利得のため、個人情報や製品開発情報などの機密情報を密かに盗み出すことを狙っており、以前のイタズラ目的のウイルス感染とは異なっています。攻撃者は、重要情報を保有している企業・団体に狙いを定め、マルウェアに感染させるために巧妙なメールを送るなどの攻撃を執拗に行ってきます。
- このように「標的型攻撃メール」は従来とは異なる特徴を持っており、従来型の対策だけでは防ぎきれない可能性もあります。このため、社員一人一人がその特徴を理解・認識し、不審なメールに騙されないように備えることが重要です。
- 当パートでは、「標的型攻撃メール」の特徴を理解・認識していただくとともに、それに対する対策を理解し、各社各機関において実践していただくことを狙いとしています。

1. 標的型メール攻撃

1-1. 標的型攻撃の事例
1-2. 標的型攻撃の対象組織は？
1-3. 標的型攻撃について
1-4. 標的型攻撃メールの特徴
1-5. 標的型攻撃メール例
1-6. 攻撃に利用するコンピュータウイルスの高度化
1-7. ゼロデイ脆弱性を狙った攻撃
1-8. 攻撃手法及び対策の推移のまとめ
1-9. 標的型攻撃メールの訓練事例
1-10. 標的型攻撃メールに対する対策

1.標的型メール攻撃

1-1. 標的型攻撃の事例 (1/2)

- Stuxnetのウラン濃縮施設への攻撃　【標的型攻撃】
  - 2010年6月に独シーメンス社の制御システムの脆弱性を利用したウイルスが発見される
  - 後に、イランのウラン濃縮施設の遠心分離機が停止させられた
- 米RSA社のSecurIDに関する情報漏洩　【標的型攻撃】
  - 2011年3月にRSAのセキュリティ関連部門がAnonymous (攻撃グループの名称) によってサイバー攻撃を受け、同社のセキュリティ製品であるSecurIDに関する情報が漏えいした
- 米国大手証券への攻撃　【標的型攻撃】
  - 米国モルガンスタンレー証券が2009年にAurora攻撃 (下記参照) の被害を受けていたことが、2011年3月の上記RSA社の事件を通じて発覚
  - Aurora攻撃とはInternet Explorerのゼロデイ脆弱性を悪用したAPT攻撃 (後述) であり、Googleが被害をブログで公表したことで知られている
- 衆参両院への攻撃　【標的型攻撃】
  - 2011年7月に、衆議院の議員のパソコンやサーバーがウイルスに感染した
  - 2011年8月に、参議院のサーバのうち2台がウイルスに感染した
- 大手重工メーカーへの攻撃　【標的型攻撃】
  - 2011年8月に、大手重工メーカーの社内情報システムが攻撃によりウイルスに感染

公共施設･重要施設への攻撃、公共性の高いサービスを狙った攻撃が世界的に頻発

1.標的型メール攻撃
1-1. 標的型攻撃の事例 (2/2)

■ **大手重工メーカーでの被害事例**

- **標的型攻撃メールが送信され、内部ネットワーク内で添付ファイルが開かれた可能性あり**
  - **添付ファイルを開くことでウイルスに感染**
  - **利用された脆弱性は**Adobe Reader/Flash Player**の脆弱性**(CVE-2011-0611)
  - 2011年4月に修正プログラムが公開されていた
- **ウイルスに感染することにより攻撃者が外部から端末を制御できるようになる**
  - **新しいウイルスのダウンロード**(8種類以上)
  - **他のシステムへの感染**(11拠点、83台)
  - **攻撃の見えない化**
  - **情報探査**
- **会社の機密情報を盗み出すことが攻撃の目的と見られている**
- **あるサーバがウイルスによって異常な動作をすることから本件が発覚した**
  (見つかってラッキーとも言える)

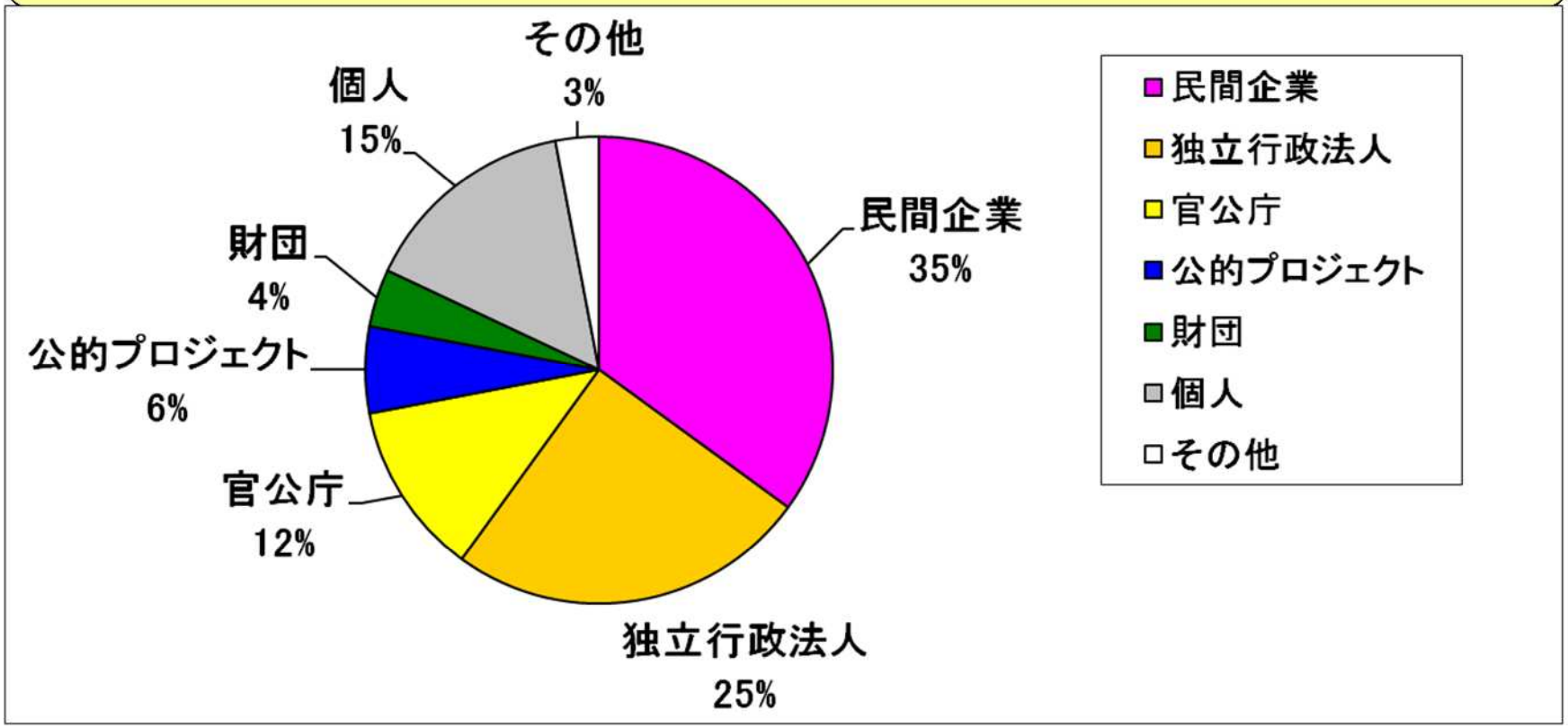
参考：情報処理推進機構（IPA）セキュリティセンターのWebサイト「標的型サイバー攻撃の事例分析と対策レポート」

機密情報を有していれば、会社の規模には関係なく、狙われる可能性が常にある

1.標的型メール攻撃

1-2. 標的型攻撃の対象組織は？

標的型攻撃メール送信先

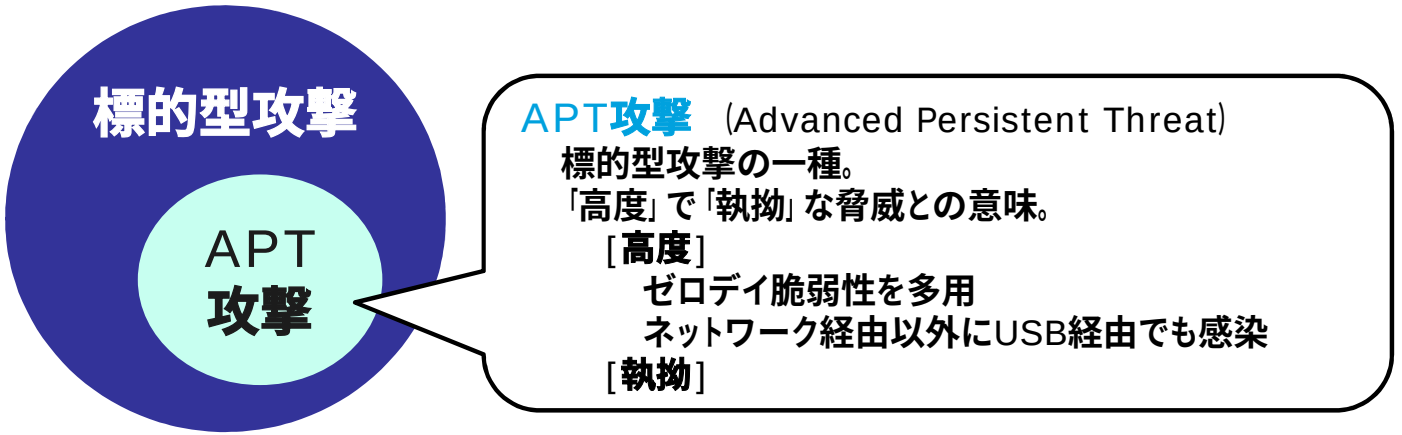


参考：独立行政法人 情報処理推進機構（IPA） 2011/10/3公表「IPAテクニカルウォッチ　標的型攻撃メールの分析に関するレポート」

攻撃対象は、公的機関が合計では一番多いが、民間企業も1／3超を占めている

1-3. 標的型攻撃について (1) 標的型攻撃とは

- **ここ最近のサイバー攻撃のキーワードである「標的型攻撃」とは？**
  - **特定の個人や組織に向けて関係者になりすましてメールを送信し、悪意の添付ファイルを開かせたり、悪意のサイトへ誘導することで、不正なプログラムを実行させる攻撃**
  - **一度不正なプログラムが実行されると、攻撃を受けたPCが自ら攻撃者の用意した新たなプログラムをダウンロードして実行する**
  - **これによって攻撃を受けたPCが外部の攻撃者から操作できたり、情報を搾取できる状態になり、機密情報が外部に漏えいしてしまう**
  - **メールで侵入してくるため、ファイアウォールでは防げず、亜種や新種も多いことからウイルス対策ソフト等により侵入時点で100%の駆除をすることは難しい**
  - **メールの添付ファイルに潜むウイルスはウイルス対策ソフトで検出しにくい**
  - **既知の脆弱性を狙うものからゼロデイ脆弱性を利用するものもある**
  - **標的型攻撃のうち、特徴的な攻撃を持つものを特にAPT攻撃と呼ぶ**



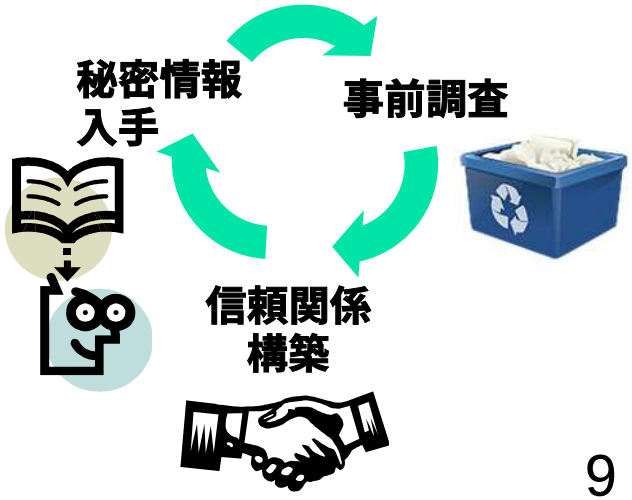
1-3. 標的型攻撃について (2) 標的型攻撃のサイクル

- **標的型攻撃では目標とする情報を入手できるまで、次の3ステップが繰り返される**

➢ **事前調査**
- 組織などが公開している公開情報や財務情報、新聞、業界雑誌、Webサイト、ソーシャルメディア、場合によってはゴミ箱等々から情報を入手
- または攻撃対象の組織と関係のある別の組織を攻撃し、信頼関係が築ける情報を入手

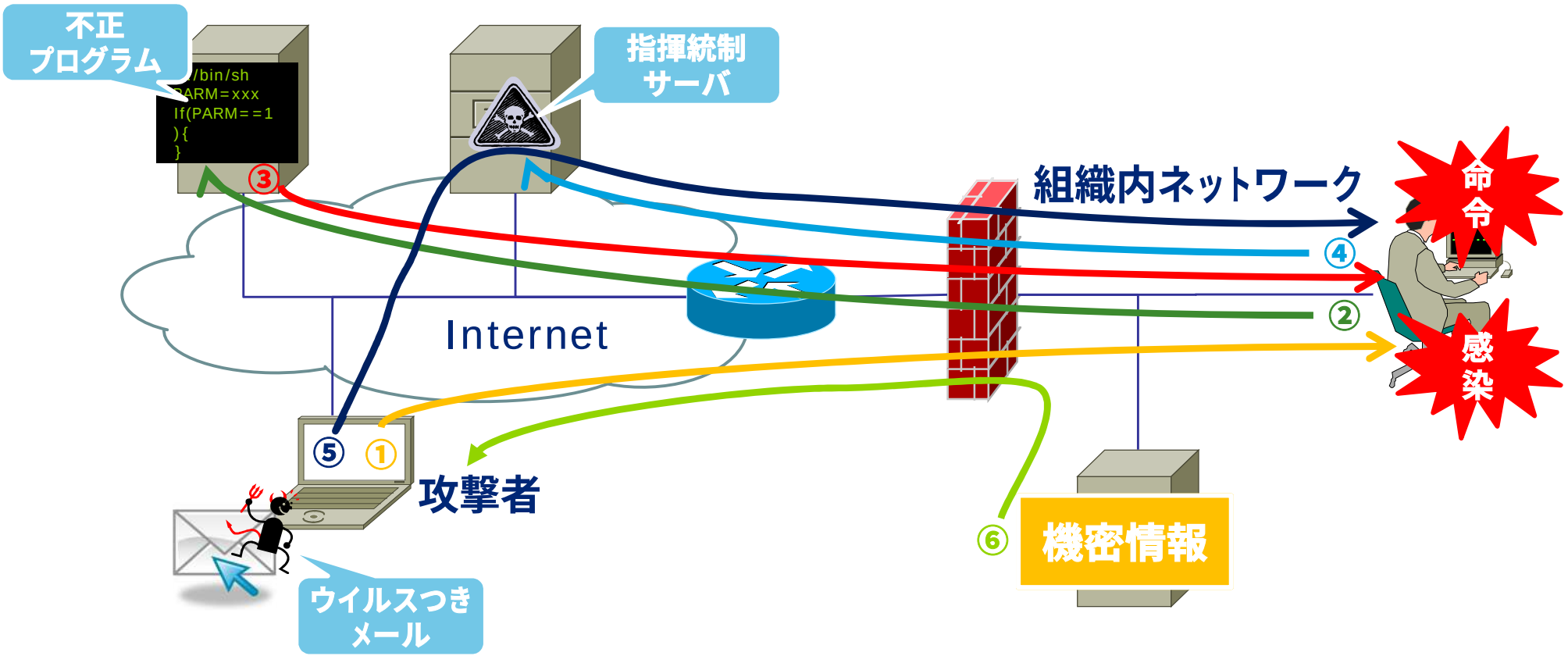
➢ **信頼関係構築**
- 内部情報を知っていることを誇示し、内部の人間であると思わせる
- 助けを求める、権威をちらつかせる等々のアプローチもある

➢ **秘密情報入手**
- 様々な手口を駆使し、攻撃対象の組織から情報を入手
- 入手した情報を利用して更なる侵入を繰り返す



1.標的型メール攻撃

1-3. 標的型攻撃について (3) 標的型攻撃メールの流れ



①攻撃者から標的者に標的型攻撃メール送信
②行動やPCに問題があるとウイルスに感染し、不正プログラムを要求
③不正プログラムを自動的に秘密裏にダウンロード
④攻撃者の用意した外部サーバ（指揮統制サーバ・C&Cサーバ）と接続
⑤攻撃者から外部サーバ経由で不正な指令が送信される
⑥組織内の機密情報等が攻撃者に秘密裏に送信されてしまう

1.標的型メール攻撃

1-4. 標的型攻撃メールの特徴

	特徴の比較（傾向）	攻撃者の目的	感染数	検体収集	言語	件名	本文	送信者	添付ファイル	感染後のPCの症状
従来型	マスメール型ウイルスメール	・社会騒乱 ・多数のPCを操りたい	多い	容易	主に英語	一般的な用件	・一般 ・勧誘 ・指示：添付ファイルを開封 等	・個人名 ・不明組織	実行形式	・重くなる ・PCダウン
最近	標的型攻撃メール	・特定の組織の情報窃取 ・システムの妨害	少ない	困難	日本語	自分に関係ありそうな用件	・関心事 ・用件の説明が適切	（詐称） ・官公庁 ・大企業	文書形式	特に変わらず

※全てが上記のように区分できるわけではないが、大枠の特徴と傾向を表していると理解して下さい。

参考：独立行政法人 情報処理推進機構（IPA） 2011/10/3公表「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」

従来の意識・知識のままでは、標的型攻撃メールに引っかかってしまう可能性が高い！

1.標的型メール攻撃

1-4. 標的型攻撃メールの特徴 －メール記載内容－

■テーマによる分類

分類	割合	テーマ事例
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、会議資料、情報セキュリティ調査、ウイルス・不正アクセス届出状況
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

※メール受信者が関係する／興味を持ちそうな仕事関係のテーマが多い。

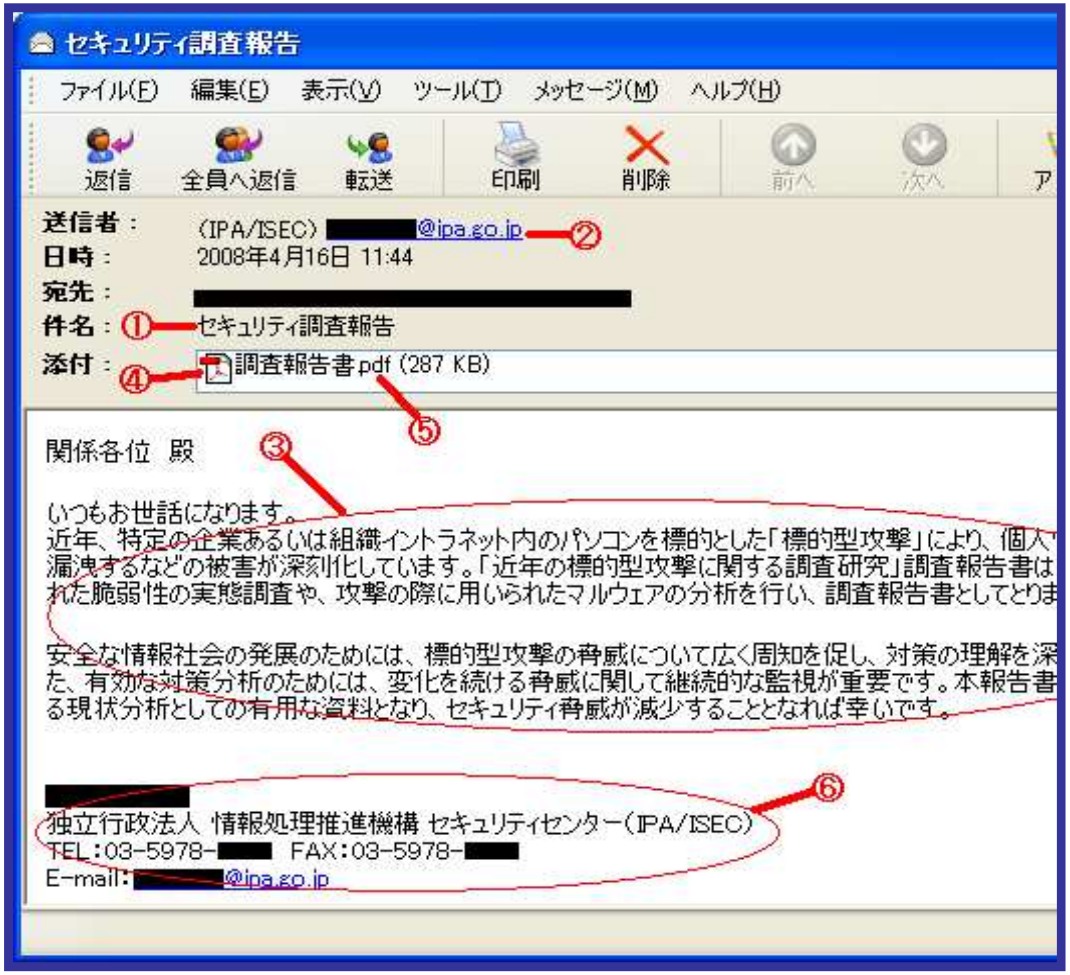
※セキュリティ関連の連絡・注意喚起を装った攻撃メールもあるので、騙されないように特に注意が必要である。

参考：独立行政法人 情報処理推進機構（IPA） 2011/10/3公表「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」

標的型攻撃メールの内容・特徴を理解しておくことは、防御のために重要！

1.標的型メール攻撃
1-5. 標的型攻撃メール例 (1/2) －PDFファイルの添付－

- 右は情報処理推進機構 セキュリティセンター(IPA/ISEC)を装ったメールで、実際に政府機関あてに送付されたもの
- 信頼させるための工夫が以下のとおり施されている
  - ① メールの受信者が興味を持つと思われる件名
  - ② 送信者のメールアドレスが信頼できそうな組織のアドレス
  - ③ 件名に関わる本文
  - ④ 本文の内容に合った添付ファイル名
  - ⑤ 添付ファイルがPDFファイルやワープロ文書など
  - ⑥ ②に対応した組織名や個人名などを含む署名
- 添付のPDFファイルに問題があり、開くとウイルスに感染する可能性があった。

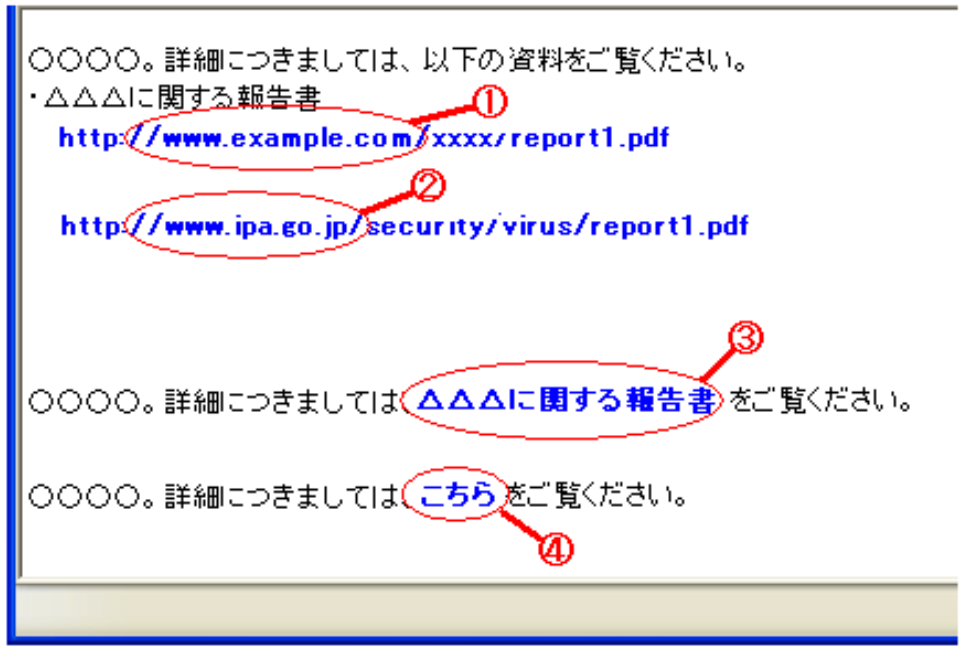


参考：情報処理推進機構 (IPA) セキュリティセンターのWebサイト
「2008年4月16日に、IPAをかたって政府関係組織に送られたメール例」
http://www.ipa.go.jp/security/virus/fushin110.html

皆さんの会社の全員が騙されない (添付ファイルを開かない) と言い切れますか？

1-5. 標的型攻撃メール例 (2/2) －悪意のURLリンク－

- メールに添付ファイルを付けずに、本文の中で、「詳細につきましては、こちらをご覧ください」のように記載して、ウイルスに感染する仕掛けをしたウェブサイトに誘導することで、ウイルスに感染させる例もある。
- 悪意のあるウェブサイトに誘導するメールであるが故の怪しい点
  - ① テキストメールで送信者のドメインと異なるURLが見える例
  - ② HTMLメールで、表示のURLとリンクのURLが異なる例
  - ③、④ HTMLメールで、URLを表示しない例
- 上記の③や④のリンクをクリックすると、悪意のあるウェブサイトに接続し、ウイルスに感染する可能性があった。



参考：情報処理推進機構（IPA） セキュリティセンターのWebサイト
「2008年4月16日に、IPAをかたって政府関係組織に送られたメール例」
http://www.ipa.go.jp/security/virus/fushin110.html

皆さんの会社の全員が騙されない（メール内リンクをクリックしない）と言い切れますか？

1.標的型メール攻撃
1-6.攻撃に利用するコンピュータウイルスの高度化

標的型攻撃メールでは、様々な工夫でウイルス（不正なプログラム）に感染させることを狙うが、ウイルス全般が高度化する中で、特に以下のような特徴を有する

ウイルスの特徴の変遷
- データの破壊、サービスの停止 ⇒ 情報の窃取
- 既知の脆弱性 ⇒ ゼロデイ脆弱性
- OSの脆弱性 ⇒ アプリケーションの脆弱性

ウイルス対策ソフトがあるから安全 ⇒？

ファイアウォールがあるから安全 ⇒？

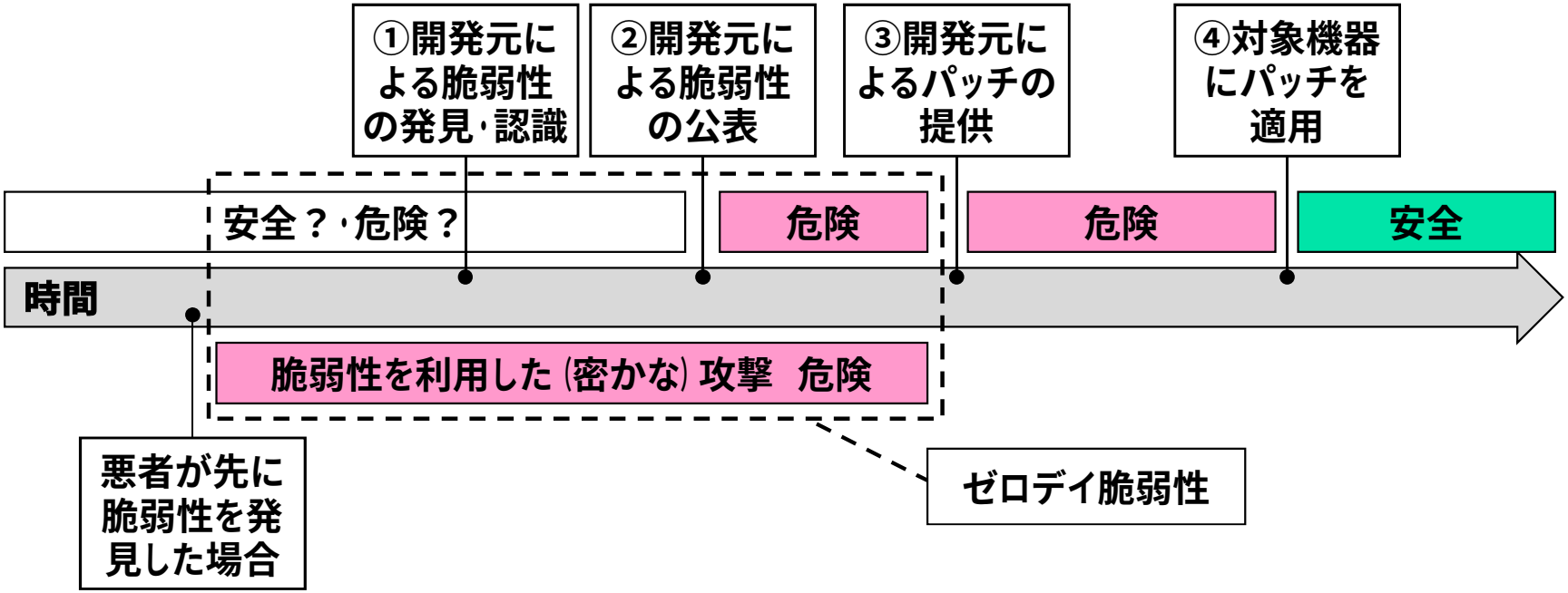
インターネットに接続していないから安全 ⇒？

（参考）過去の主なコンピュータウイルスの変遷

攻撃に利用するコンピュータウイルスは高度化し、見つからないように潜伏する傾向

1-7. ゼロデイ脆弱性を狙った攻撃

- **ゼロデイ脆弱性とは？**
  - ソフトウェアの脆弱性（セキュリティ上の問題）のうち、その存在が認識されているが、それに対するセキュリティパッチがソフトウェア開発元から提供されていない状態のもの
  - 悪意あるプログラムでその脆弱性を狙うことにより、コンピュータに対する不正を行う
  - OS（Windows）だけでなく、アプリケーション（Adobe製品等）にも当脆弱性がある。



  - 未知のゼロデイ脆弱性は悪者（攻撃者）にとってお金になる。ヤミ市場での売買もあり。

Windowsのセキュリティパッチをタイムリーに適用するだけで、安心してはいけない！

1.標的型メール攻撃

1-8.攻撃手法及び対策の推移のまとめ

主な攻撃手法	主な（技術的）対策
コンピュータウイルスの登場	ウイルス対策ソフトの導入
サーバの公開サービスに対する 不正アクセス（安易なパスワード等）	パスワード管理の徹底 ファイアウォールの導入
電子メールを利用した クライアントPCへの攻撃（従来型）	ユーザ教育 （不審なファイル / サイトは開かない）
サーバの公開サービスに対する 脆弱性を利用した攻撃	サーバOS等への修正プログラムの適用 IDP（侵入検知防御システム）の設置
クライアントPCのサービスに対する 脆弱性を利用した攻撃	クライアントOS等への修正プログラムの適用 パーソナルファイアウォールの導入
USBメモリ等媒体を通じた攻撃	Autorun無効化 デバイス制御
Webアプリケーションに対する 攻撃（SQLインジェクション等）	Webアプリの設計・プログラムの見直し WAF（Web Application Firewall）の導入
偽装メール＋クライアントPCのアプリケーション の脆弱性（ゼロデイ含む）を利用した攻撃	アプリ（Adobe製品等）の修正プログラムの適用 アウトバウンド（内部からの不正な通信）監視

標的型攻撃

従来からの対策も含めて、
総合的に実施することが重要！！

1.標的型メール攻撃
1-9. 標的型攻撃メールの訓練事例(1) －訓練概要－

■ **政府機関における標的型不審メール攻撃訓練**

➢ **情報セキュリティ対策の一環として、標的型メール攻撃に対する訓練を行った。**

■実施主体：内閣官房情報セキュリティセンター（NISC）

■訓練期間：2011年10月～12月

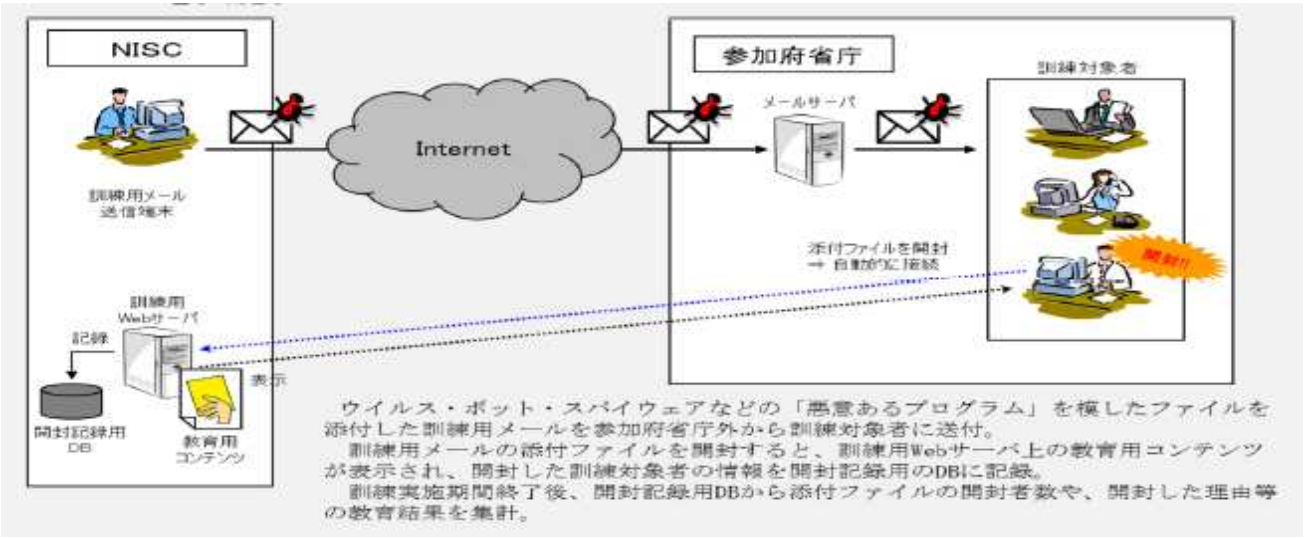
■訓練対象：内閣官房等12の政府機関約6万名

■訓練内容：①訓練対象者に対して事前教育の実施。

②訓練対象者に対して標的型不審メールを模擬したメールを2回送付。

③模擬メール中の添付ファイルを開封もしくは、URLをクリックするなど不適切な扱いをした場合は、教育コンテンツに誘導。

④参加府庁省に個別の訓練結果を通知し、各府庁省内において適切な事後教育指導を実施。



その結果は？

参考：内閣官房情報セキュリティセンター（NISC）の平成24年1月19日付報道資料：「政府機関における情報セキュリティ対策の取組状況について」

1.標的型メール攻撃

1-9. 標的型攻撃メールの訓練事例(1) －訓練結果－

■ **政府機関における標的型不審メール攻撃訓練の結果（中間報告）**

■訓練結果：今回の訓練における不審メールの開封率は以下のとおり。

◆1回目（添付メール）　10．1%

（組織により1．1%～23．8%）　※約6万名のうち**約6，000名**

◆2回目（リンクメール）　3．1%

（組織により0．4%～　6．1%）　※約6万名のうち**約1，800名**

■結果分析：①1回目の訓練と比べ2回目の結果が良くなっていることから、標的型不審メールに対するセキュリティ意識は向上したものと想定される。

②ただし、この効果は一時的なものであり、時間の経過とともに意識レベルは低下するものと想定されるため、今後も訓練を継続していくことが重要である。

■課題　：不審メールを開封した事例のほか、以下の検討を要する事例が見られた。

①不審メールの送信元に対し、メールを返信する方法で差出人の確認をしているケース

②メールの自動返信機能を設定することにより、攻撃者に対し、不在通知が自動発信されたケース

これらの事例では、組織で使用している有効なアドレスを攻撃者に通知してしまうことになり、攻撃者に次ぎの攻撃に資する組織内の情報を提供したことになる。

したがって、これらについても対策が必要となる。対策としては、以下のような例が考えられる。

①差出人の確認については、電話等により行うこと

②自動返信の範囲を組織内に限定すること

事前教育を受けても、約10%の人が不審メールに反応したことをどう思いますか？

1-9. 標的型攻撃メールの訓練事例(2)

■民間会社で2015年度に実施した標的型攻撃メールを想定した訓練

■対象者：メールアドレスを保有する全役職員

1回目（全体状況）

訓練対象者数	開封者数	割合
781名	171名	22％

開封者の内訳

メール種別	差出人	開封率
URLリンク型	架空の外部機関	1％
添付ファイル型	社内部署を偽装	39％
URLリンク型	社内部署を偽装	30％
添付ファイル型	社内部署を偽装	17％

2回目（全体状況）

訓練対象者数	開封者数	割合
775名	81名	1％

開封者の内訳

メール種別	差出人	開封率
添付ファイル型	架空の外部機関	1％
URLリンク型	架空の外部機関	1％

1-10. 標的型攻撃メールに対する対策

標的型攻撃メール

防御

運用管理面での対策	＋	技術面での対策
メール受信者の情報リテラシー向上や受信メールの取扱いが非常に重要である。		メールは人間が操作するものであり、またメール受信者を信用させる様々なだましのテクニックを駆使していることから、うっかり添付ファイルを開いてしまうリスクの対策も不可欠。

参考：独立行政法人 情報処理推進機構（IPA） 2011/10/3公表「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」

1-10. 標的型攻撃メールに対する対策

運用管理面での対策

(1) **従業員の情報リテラシーの向上（意識向上）**

少なくとも、次の知識と対応を身につけておくことが必要である。

- ウイルス対策ソフトを導入していても、ウイルスを100%防げるわけではない。
- 件名、本文、添付ファイル名などが日本語のウイルスメールも増えている。
- 差出人のメールアドレスは簡単に詐称できる。
- 原則として、実行形式の添付ファイルを開いてはいけない。
- PDFファイルやワープロ文書など実行形式でない文書データファイルから感染するウイルスもあるので、少しでも怪しいと感じたら、添付ファイルを開いてはいけない。
- ウイルスに感染しても、目に見える異常な症状が出るとは限らない。
- 脆弱性の修正プログラムが公開されたら、原則として、すぐに適用する。

(2) **標的型攻撃メールに関する情報集約と情報共有**

- 不審なメールが届いた場合の連絡体制を整備しておくこと。
- 不審メールの連絡を受けた場合は、速やかに・具体的に、組織内での注意喚起を行い、従業員が不審メールに気付かずに不適切な行為（添付ファイルを開く、リンクをクリックする）を行わないようにすること。

参考：独立行政法人 情報処理推進機構（IPA） 2011/10/3公表「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」

1-10. 標的型攻撃メールに対する対策

技術面での対策

※一つの技術的対策で全てを防御することはできないので、
複数の対策を組み合わせることが重要

(1) **ウイルス対策ソフトの適切な運用**

①常時監視機能を用いてファイルを開く前に自動的にチェックする
②定期的に最新のウイルス定義情報を用いてコンピュータ内の全ファイルをスキャンする

(2) OS**のセキュリティパッチの速やかな適用**

・インターネットに接続しているパソコンはWindows Updateを利用するなどして、OSのセキュリティパッチを速やかに適用すること。

(3) **アプリのセキュリティパッチの速やかな適用**

・Windows Updateの対象外のソフトウェアも多数あり、特に以下のソフトウェアは脆弱性を狙われやすいので、適時のバージョンアップまたはセキュリティパッチ適用を行うこと。
Adobe Reader（PDF用ソフト）、Adobe Flash Player（動画表示ソフト）、Java Runtime 等

(4) **ファイアウォール等によるネットワーク防御・監視**

・ファイアウォールにより外部からの攻撃を防御したり、IDP（Intrusion Detection and Prevention：侵入検知防御システム）により侵入を防御したりといった対策も検討すること。
・また、アウトバウンド監視機能（内部からの不正な通信を監視するもの）をもった製品も登場していますので、ネットワークの増強や更改といった機会に導入を検討すること。

参考：独立行政法人 情報処理推進機構（IPA） 2011/10/3公表「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」

2．日本年金機構の不正アクセス事案

2.日本年金機構の不正アクセス事案
はじめに

- 前パートで見たように、標的型メール攻撃は2011年頃から徐々に増加し、様々な企業・団体が狙われ、ニュースになっている事案も多く生じています。
  そのような社会環境のもと、今年5月に日本年金機構が標的型メール攻撃によって狙われ、一部の端末がウイルスに感染し、気付かない間に、約125万件もの大量の個人情報がインターネットを通じて外部に流出するという重大事案が発生しました。
- 一人がふとした不注意から問題のあるメールに添付されたファイルを開いてしまうと、気付かないうちにマルウェアに感染し、最悪の場合には社内の機密情報が攻撃者に勝手に送信されてしまいます。このようにメールに対する一人の不注意が、企業の存続を危うくする事態を引き起こすおそれがあります。
- 日本年金機構では、事案の発生を受けて調査委員会を設置し、その結果を8月に公表しました。当パートでは、その調査結果を参考にして、標的型攻撃メールに対してどのように備えればよいかをご説明いたします。

2．日本年金機構の不正アクセス事案

2-1. 不正アクセスによる個人情報流出事案の概要
2-2. 個人情報流出に関するお客様対応
2-3. 標的型メール攻撃を受けた際の対応の課題
2-4. 共有ファイルサーバの取扱いに関する課題
2-5. 標的型メールに関する職員向け注意喚起の課題
2-6. 標的型メール攻撃に適切に対応できなかった原因
2-7. 再発防止に向けた今後の取組
2-8. まとめ

2.日本年金機構の不正アクセス事案

2-1. 不正アクセスによる個人情報流出事案（概要）

- **日本年金機構の不正アクセスによる個人情報流出事案**
  - 2015年5月8日（金）～　標的型メールを計124通受信。　うち5名が添付ファイル等を開封。
  - 31台のPCがウイルスに感染
  - 2015年5月21日（木）～23日（土）　約125万件（対象者は約101万人）の個人情報が流出
    ※感染PC及び共有ファイルサーバにある個人情報がウイルスにより外部に送信された（次ページ参照）
  - 2015年6月1日（月）　事案公表
- **流出した個人情報の内訳**
  - 4情報（基礎年金番号、氏名、生年月日、住所）　⇒　約　5.2万件
  - 3情報（基礎年金番号、氏名、生年月日）　⇒　約116.7万件
  - 2情報（基礎年金番号、氏名）　⇒　約　3.1万件

  ※約55万件のデータについては、パスワード未設定
- **基幹システムへの侵入及び基幹システムからの情報漏えいは確認されていない**

日本年金機構 不正アクセスによる情報流出事案に関する調査委員会「不正アクセスによる情報流出事案に関する調査結果報告」（平成27年8月20日）を基に作成

2.日本年金機構の不正アクセス事案

2-1. 不正アクセスによる個人情報流出事案（詳細）

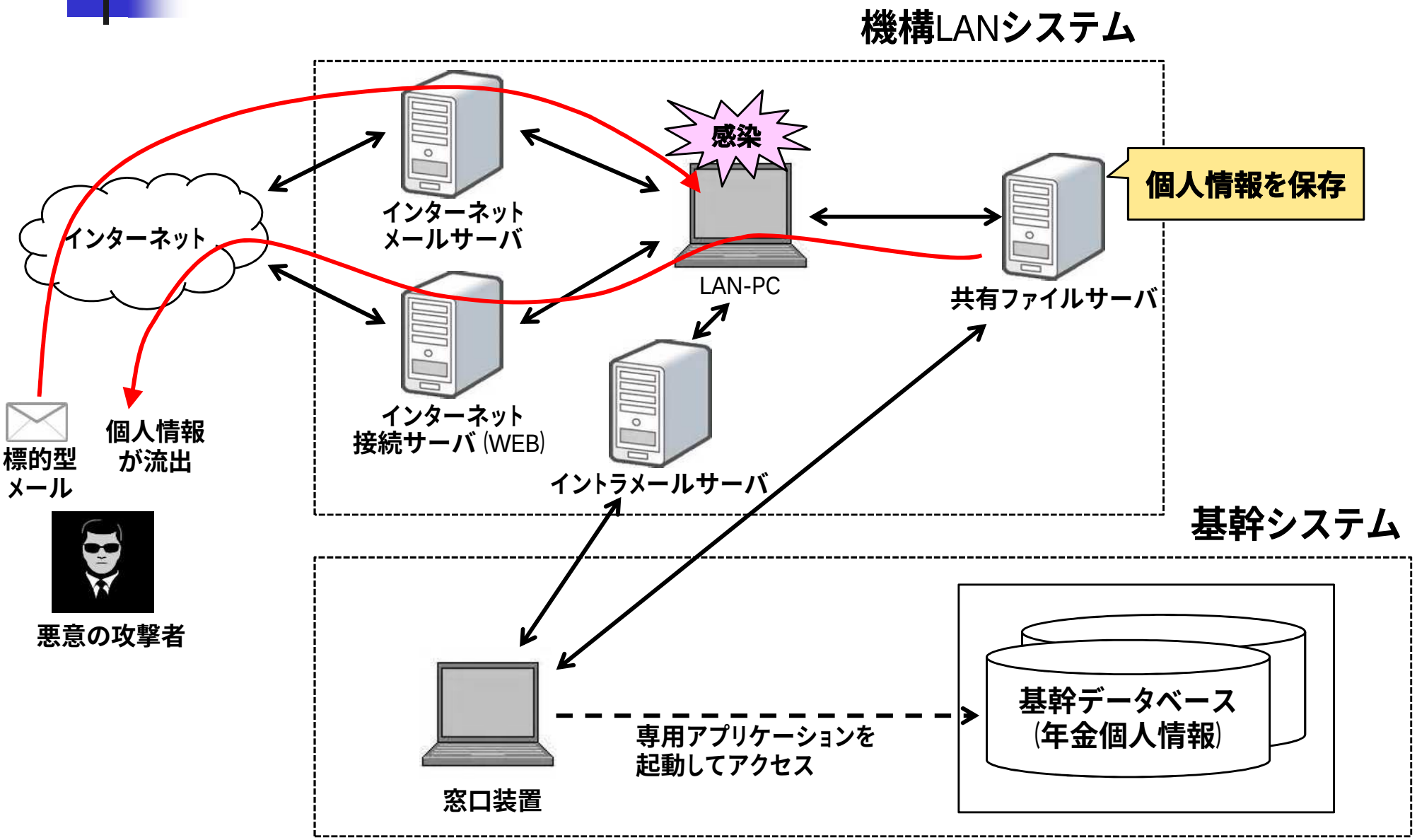
日付	経過日数	事象
5月8日（金）	1日目	「不審な通信を検知」と通報（NISC *1⇒厚労省⇒機構）。 該当端末を特定し、LANケーブル抜線
5月15日（金）	8日目	運用委託会社が「新種ウイルスは、外部に情報を漏洩するタイプではない」との解析結果を機構に報告。　機構は問題が一旦収束したと判断。
5月18日（月）	11日目	不審メール受信（99通）
5月19日（火）	12日目	警察に相談・捜査依頼。　不審メール受信（20通）
5月20日（水）	13日目	不審メール受信（3通）
5月21日（木）	14日目	個人情報流出が始まる
5月22日（金）	15日目	「不審な通信を検知」と通報（NISC⇒厚労省⇒機構） 該当端末を特定し、LANケーブル抜線。　該当拠点のインターネット接続を遮断。
5月23日（土）	16日目	「不審な通信を検知」と連絡（運用委託会社⇒機構） 該当端末を特定し、LANケーブル抜線。　該当拠点のインターネット接続を遮断。 個人情報流出が止まる。
5月28日（木）	21日目	「機構から流出したと考えられるデータを発見した」との連絡（警察⇒機構）
5月29日（金）	22日目	機構全体のインターネット接続を遮断。
6月1日（月）	25日目	事案公表
6月4日（木）	28日目	メール送受信用外部回線を遮断

*1) NISC：内閣サイバーセキュリティセンター
　　サイバーセキュリティ対策の一環として政府機関に対する攻撃の情報収集・分析等を行っている。

日本年金機構 不正アクセスによる情報流出事案に関する調査委員会「不正アクセスによる情報流出事案に関する調査結果報告」（平成27年8月20日）を基に作成

2.日本年金機構の不正アクセス事案

(参考) 日本年金機構のシステムイメージ



日本年金機構 不正アクセスによる情報流出事案に関する調査委員会「不正アクセスによる情報流出事案に関する調査結果報告」(平成27年8月20日) を基に作成

2.日本年金機構の不正アクセス事案
(参考) 不審メールの例

■ 不審なメールが届いた場合は開封せず削除するよう注意喚起メールを発信しており、その中で実際に受信した不審メールの例を紹介していた。

不審メール例1

差出人：■■■■■■＜xxxx@yahoo.co.jp＞
件名：給付研究委員会オープンセミナーのご案内
添付ファイル：給付研究委員会オープンセミナーのご案内.lzh

○○　○○様

平成27年5月に横浜国立大学と企年協が共同で実施いたしました企業年金アンケート結果の報告会と意見交換会を下記のとおり実施いたします。
アンケートの集計結果に基づく報告会は、今後の企業年金の方向性を考えるうえでも、基金関係者にとって大いに参考になると思います。

会員の皆様の積極的な参加をお願い申し上げます。

お申し込みは添付資料をクリックしてください。

■■■■■■

不審メール例2

差出人：■■■■■■＜xxxx@yahoo.co.jp＞
件名：「厚生年金基金制度の見直しについて（試案）に関する意見」

○○　○○様

5月1日に開催された厚労省「厚生年金基金制度に関する専門委員会」最終回では、厚生年金基金制度廃止の方向性を是とする内容が提出されました。これを受けて、企年協では、「厚生年金基金制度の見直しについて（試案）に関する意見」を、5月5日に厚労省年金局企業年金国民年金基金の渡辺課長に提出いたしました。
添付ファイルをご覧ください。
＊＊
URL：＿＿＿＿＿＿＿＿＿＿＿＿

日本年金機構 不正アクセスによる情報流出事案に関する調査委員会「不正アクセスによる情報流出事案に関する調査結果報告」（平成27年8月20日）を基に作成

2.日本年金機構の不正アクセス事案

2-2. 個人情報流出に関するお客様対応

■ 約125万件（対象者は約101万人）の個人情報が流出したことを6月1日（月）に公表

■ お客様へのお詫びと問い合わせ対応

- お詫びとお願いの文書送付（6/3～4：約1.5万人　6/22～29：約100万人）
- 未送達者への対応（7月～）
- 専用コールセンターの開設（6月～：約1000人体制）
- 年金事務所の土日開所（6～7月：全国312事務所　8月：59事務所）

■ お客様の被害防止に向けた取組

- お詫びとお願いの文書送付（6/3～4：約1.5万人　6/22～29：約100万人）
- 基礎年金番号の変更のお知らせ文書の送付（8月下旬～：約96万人）
- 住所変更・金融機関変更の手続者への対応（6月上旬～：対象者への戸別訪問等）
- 不審電話への対応（6月～：通報者への戸別訪問等）
- ホームページによる情報提供等（6月～：不審電話に対する注意喚起、具体的な事例等を掲載）
- 関係機関と連携した広報（6月～：消費者庁、国民生活センター、警察庁、市町村等と連携）

※上記対応過程で説明の誤りがあり、さらに、誤りに関する国民への公表、厚労省への報告も遅れた。

※上記の対応費用は2015/8/20時点で約6億円。　以降、約4億円の追加費用を見込む。

日本年金機構 不正アクセスによる情報流出事案に関する調査委員会「不正アクセスによる情報流出事案に関する調査結果報告」（平成27年8月20日）を基に作成

2.日本年金機構の不正アクセス事案

2-3. 標的型メール攻撃を受けた際の対応の課題

標的型メールを受信した際に対応すべきであったと考えられる重要ポイント

① 送信元メールアドレスの受信拒否の設定を行わなかった

※同じ送信元から多数のメールアドレス宛に送信されていることの認識が薄かった

②標的型メール攻撃ではないかとの疑いが組織として共有されなかった

※担当者は疑いを持ったが、組織としては共有されなかった

③標的型メール受信者全員に個別に添付ファイルの開封の有無を確認しなかった

※情報セキュリティ担当部署では、職員が添付ファイルを開封したことを把握していなかった

④解析結果に基づくフィルタリングを行わなかった

※怪しい通信先を特定し、フィルタリング（不審URLへの通信の遮断）することの想定がなかった

⑤機構内すべての統合ネットワークを通じたインターネット接続の遮断を行わなかった

※事態の重大性を認識するに至らず、適時にインターネット接続を遮断しなかった

上記の対策を実施していれば、個人情報流出を防止できたかもしれない。。。

日本年金機構 不正アクセスによる情報流出事案に関する調査委員会「不正アクセスによる情報流出事案に関する調査結果報告」（平成27年8月20日）を基に作成

2.日本年金機構の不正アクセス事案

2-4. 共有ファイルサーバの取扱いに関する課題

① ルール軽視･無視

- 「共有フォルダ運用要領」は作成されていた。
  - ルール1：個人情報等の重要情報は共有ファイルサーバに原則として保管しない。
  - ルール2：例外的に保管する場合は、パスワード設定などのセキュリティ措置を行うこと。
- 上記ルールの徹底が図られていなかった。 **運用ルール自体が有名無実化**
- 運用ルールが全拠点で本当に実行されているかなどの点検･確認が行われていなかった。

② リスク認識の甘さ･欠如

- インターネット接続下にある共有ファイルサーバに個人情報を置くことの**リスク認識が甘かった**。
- 最初の攻撃があった時に、外部流出の危険性を認識せず、役員が対策を検討しなかった。
- 個人情報をインターネット接続環境下に置く、という問題を持ったシステム設計を改善しておらず、役員はもとより組織全体として**サイバーセキュリティの危機意識に欠けていた**。

2.日本年金機構の不正アクセス事案

2-5. 標的型メールに関する職員向け注意喚起の課題

① 日頃の注意喚起が不十分

- 標的型メール攻撃に対する日頃からの継続的な**注意喚起が不十分であった**。
- 職員研修などでは、万一開封してしまった際に対応するノウハウが徹底されていなかった。
- インターネットの閲覧規制を行っていた。業務上の理由がある職員には、規制を解除していたが、情報セキュリティ担当部署などから標的型メール攻撃に関する注意喚起はされなかった。
- これらの結果として、
  - ✓ 5名の職員が標的型メールの添付ファイルを開封した。
  - ✓ うち4名は不審メールを受信したことを情報セキュリティ担当部署に報告しなかった。

② 攻撃発覚後の注意喚起が不十分

- 今回の攻撃発生後、注意喚起のために全職員にメールが送られた。
- しかし、その内容は、不審メールの削除指示に限られていた。
- 誤って添付ファイルを開封した場合の具体的対処方法や、情報セキュリティ担当部署に連絡することなどの記載はなかった。

日本年金機構 不正アクセスによる情報流出事案に関する調査委員会「不正アクセスによる情報流出事案に関する調査結果報告」（平成27年8月20日）を基に作成

2.日本年金機構の不正アクセス事案

2-6. 標的型メール攻撃に適切に対応できなかった原因

情報セキュリティ対策全般に係る事項

① 情報セキュリティポリシーの課題

- インシデント対応の必要性が規定されていたが、その具体化はリスク管理一般の規定等に委ねられていた。
- このため、標的型メール攻撃に対応できるような**具体的なルールは定められていなかった**。
- リスク分析と対応方針の策定ができていなかった。

② ガバナンス・組織体制上の課題

- **基本的対応は担当者任せとなっていた。**
- 役員はリスク認識に欠けていた。（年金個人情報を守るという組織として一貫した方針の欠如）
- CIO（システム部門担当理事）や情報セキュリティ担当部長は具体的な指示を行わなかった。
- 理事長・最高情報セキュリティ責任者（副理事長）への報告が適時適切でなかった。
- 情報セキュリティ担当部署に情報セキュリティに関する専門的な知識や経験を有する者が配置されていなかった。
- 上位組織（厚生労働省）との情報共有について、具体的なルールが定められていなかったため、担当者レベルに止まっていた。

日本年金機構 不正アクセスによる情報流出事案に関する調査委員会「不正アクセスによる情報流出事案に関する調査結果報告」（平成27年8月20日）を基に作成

2.日本年金機構の不正アクセス事案

2-7. 再発防止に向けた今後の取組

① 今後の機構システム全体のあり方

- 基幹システム・個人情報等重要情報を扱うシステムはインターネット接続環境から完全に遮断
- （当面の対応）既存のLANシステムとは物理的に独立したインターネット環境の構築を検討

② 情報セキュリティ体制の強化

- 標的型メール攻撃等への多層防御体制の整備（入口対策、内部対策、出口対策の強化）。
- 情報セキュリティ専門家の招聘 or 専門機関との契約

③ 職員研修・内部監査

- 情報セキュリティ研修の充実、標的型メール攻撃等の対する訓練
- リスクを考慮した内部監査の実施（共有ファイルサーバの点検状況等の監査）

④ ガバナンス・組織風土のゼロベースからの抜本改革

- 理事長をトップとした改革（実態を踏まえたルール設定、人事評価制度の見直し、など）
- 厚労省との的確かつ緊密な情報共有体制の構築

日本年金機構 不正アクセスによる情報流出事案に関する調査委員会「不正アクセスによる情報流出事案に関する調査結果報告」（平成27年8月20日）を基に作成

2.日本年金機構の不正アクセス事案
2-8. まとめ

自社のシステム環境、利用状況を踏まえ、以下の項目を確認・検討することを推奨します。

① 標的型メール攻撃に対する注意喚起・訓練

- インターネット閲覧や電子メールを使用している役職員向けに、標的型メール攻撃の概要・リスクをきちんと説明し、注意喚起をすること。
- 標的型メール攻撃を想定した実機訓練を実施すること。

② 重要情報の取扱いに対する注意喚起・徹底

- 重要情報を扱う情報システムはインターネット接続環境と分離すること。
- 重要情報を保存・送信等する際には、適切なパスワード設定を徹底すること。

③ インターネット接続環境のセキュリティ対策状況のチェック

- インターネット接続しているサーバ・パソコンについて、OSやミドルウェアのセキュリティパッチの適用状況、ウイルス対策の状況等を再確認すること。

④ 情報セキュリティ対策・個人情報保護対策の点検

- 重要情報の取扱いが適切に確保されているかとの観点から、取扱ルール自体の定期的な見直し、取扱ルールに沿った業務遂行状況の点検を行うこと。
  (対策は継続的に実施する必要があり、形骸化しないように注意が必要)

⑤ インシデント(情報セキュリティ事故)に備えた体制整備

- 問題(兆候含む)が発生した場合の連絡ルート、対応体制を具体的に定めること。
- 発生事象とその影響を洗い出し、最悪のシナリオを想定した対応策を具体的に検討すること。

3．ウェブサイトに対する攻撃

3.ウェブサイトに対する攻撃

はじめに

- 最近、ウェブサイトに対する不正アクセスが多発しており、ウェブサイトにアクセスしたお客様がウイルス感染する事例やウェブサイト全体の閉鎖を余儀なくされ会社の売上やお客様からの信頼を損なうような事例も発生しています。
- 背景には、ソフトウェアの脆弱性が起因していますが、ウェブサイトへの不正アクセスに対する会社の発見や対応の遅延が被害を拡大しているものもあります。
- 当パートでは、ウェブサイトに関連するセキュリティ対応について、実際のトラブル事例を通じて、各社各機関で求められる対応策をご紹介します。

3．ウェブサイトに対する攻撃

3-1.　ウェブサイトに関する攻撃の種類（まとめ）

3-1-1. 攻撃①：ウェブサイトの改ん

3-1-1. 攻撃①：Open SSLの脆弱性を狙った攻撃

3-1-2. 攻撃②：水飲み場型攻撃（標的型攻撃の一種）

3-1-3. 攻撃③：パスワードリスト攻撃（攻撃手法と事例）

3-2.　ウェブサイトに関する攻撃への対策（まとめ）

3-2-1. 対策①：ウェブサイトに関する対策

3-2-2. 対策②：標的型攻撃に対する対策

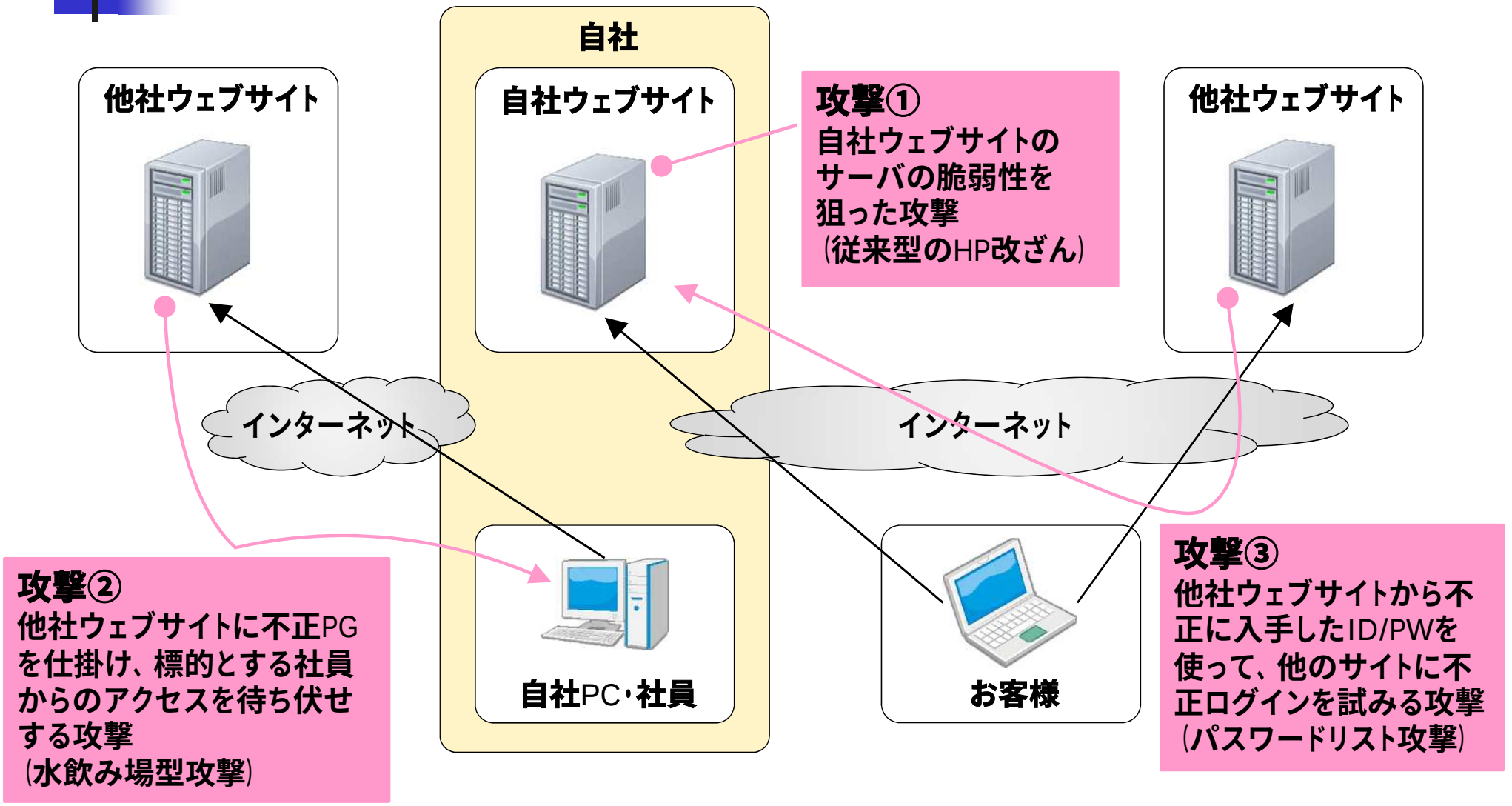
3-2-3. 対策③：パスワードリスト攻撃への対策

3-2-4.（参考）セキュリティパッチ適用の必要性

3-2-5.（参考）ビデオを活用した社員研修の事例

3.ウェブサイトに対する攻撃

3-1. ウェブサイトに関する攻撃の種類（まとめ）



ウェブサイトに関する攻撃の種類は複雑・多様化している

3.ウェブサイトに対する攻撃

3-1-1. 攻撃①：ウェブサイトの改ざん

概要・経緯	• 2014年3月28日（金）：外部からの指摘により、ウェブサイトの一部改ざんが判明。 • 同日17:30に**関連サイトをすべて閉鎖**し、詳細調査を開始。 • 3月31日（月）：HPに「お詫びとお知らせ」を掲載。問い合わせ対応の特別窓口を設置。 • 4月8日（火）：調査状況とウェブサイト再開に向けた予定を公表。 ➢ ウェブサイトの改ざんは3月10日から行われていた。（※**発覚まで日数を要した**） ➢ 改ざんされたウェブサイトにアクセスした場合、不正なプログラムが実行され、第三者の不正なサイトに誘導されるおそれがあった。（※実被害の報告は無い模様） • 4月23日（水）：サーバのセキュリティを強化した上で、一部のウェブサイトを再開 • 4月30日（水）：通販サイトを含む大半のサイトを順次再開。 全サイトの再開は5月16日。
影響（自社）	• 4月30日の復旧までの**約1ヶ月間、HPを通じた情報発信不可、ネット販売停止**、等
影響（外部）	• お客様からのグループ全体に対する信用の毀損 ※顧客情報の流出やウイルス感染といった被害報告は無かった模様
原因	• サーバの脆弱性を狙ってウェブサイトを改ざんしたものだが、詳細は非公表のため不明

ウェブサイトで取り扱う情報・機能の拡大とともに、その重要性は高まり、リスクも大きくなっている

3.ウェブサイトに対する攻撃

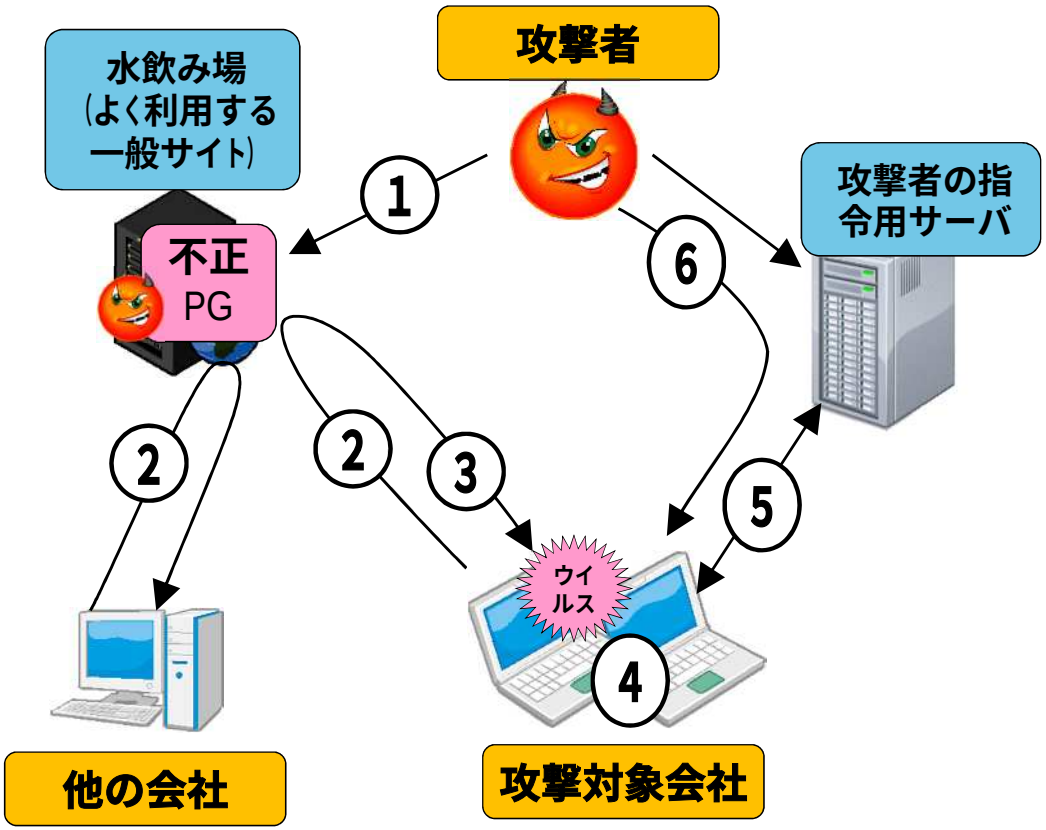
3-1-1. 攻撃①：Open SSLの脆弱性を狙った攻撃

概要・経緯	• 2014年4月11日（金）：多数の不審なアクセスを検知したことから、会員専用ウェブサービスを停止。 • 4月12日（土）：停止したウェブサービスを再開。 • 4月18日（金）：不正アクセスに関する内容を公表。 ➢ 不正アクセスにより不正閲覧された顧客：894名 ➢ 不正閲覧された情報：氏名、住所、カード番号（一部非表示）、有効期限、等 ➢ 暗号化ソフト（Open SSL(*1)）の脆弱性を狙った不正アクセス ➢ Open SSLのバージョンアップなどを4月12日に図った上で、ウェブサービスを再開 (*1)Open SSL：インターネットで暗号化通信を実現するためのソフトウェア。無料で利用できることから全世界で多数のOpen SSLが利用されている。
影響（外部）	• 不正閲覧の対象顧客に個別にメール/手紙/電話により連絡 ※クレジットカードの不正使用や個人情報悪用の被害は報告されていない。
原因	• 暗号化ソフト（Open SSL）の脆弱性を狙った不正アクセス ※当脆弱性は4月7日に公表され、注意喚起がされていたもの

サーバOSだけでなくサーバ関連の様々なソフトの脆弱性にも注意が必要

3.ウェブサイトに対する攻撃

3-1-2. 攻撃②：水飲み場型攻撃（標的型攻撃の一種）



① 攻撃者が攻撃対象会社の社員が利用しそうな一般ウェブサイトに対して、サーバOS等の脆弱性を狙って不正なプログラムを仕掛ける。

② 通常のウェブサイトへのアクセス

③ 多数の利用者のうち、攻撃対象会社の社員（例：IPアドレスから識別）に対して、不正なプログラム（ウイルス）を送り込むように攻撃する。

④ 攻撃対象会社の社員のパソコンにOSやブラウザの脆弱性があると、それを利用して不正プログラム（ウイルス）に感染する。

⑤ 不正プログラム（ウイルス）と攻撃者が用意した指令用サーバとの通信が密かに確立してしまう。

⑥ 攻撃者は社員に気付かれずに、社員のPCを操作して、攻撃対象会社内の情報にアクセスし、機密情報の不正持ち出しを行うことが可能となる。

標的型攻撃の種類・手口はどんどん高度化・複雑化している

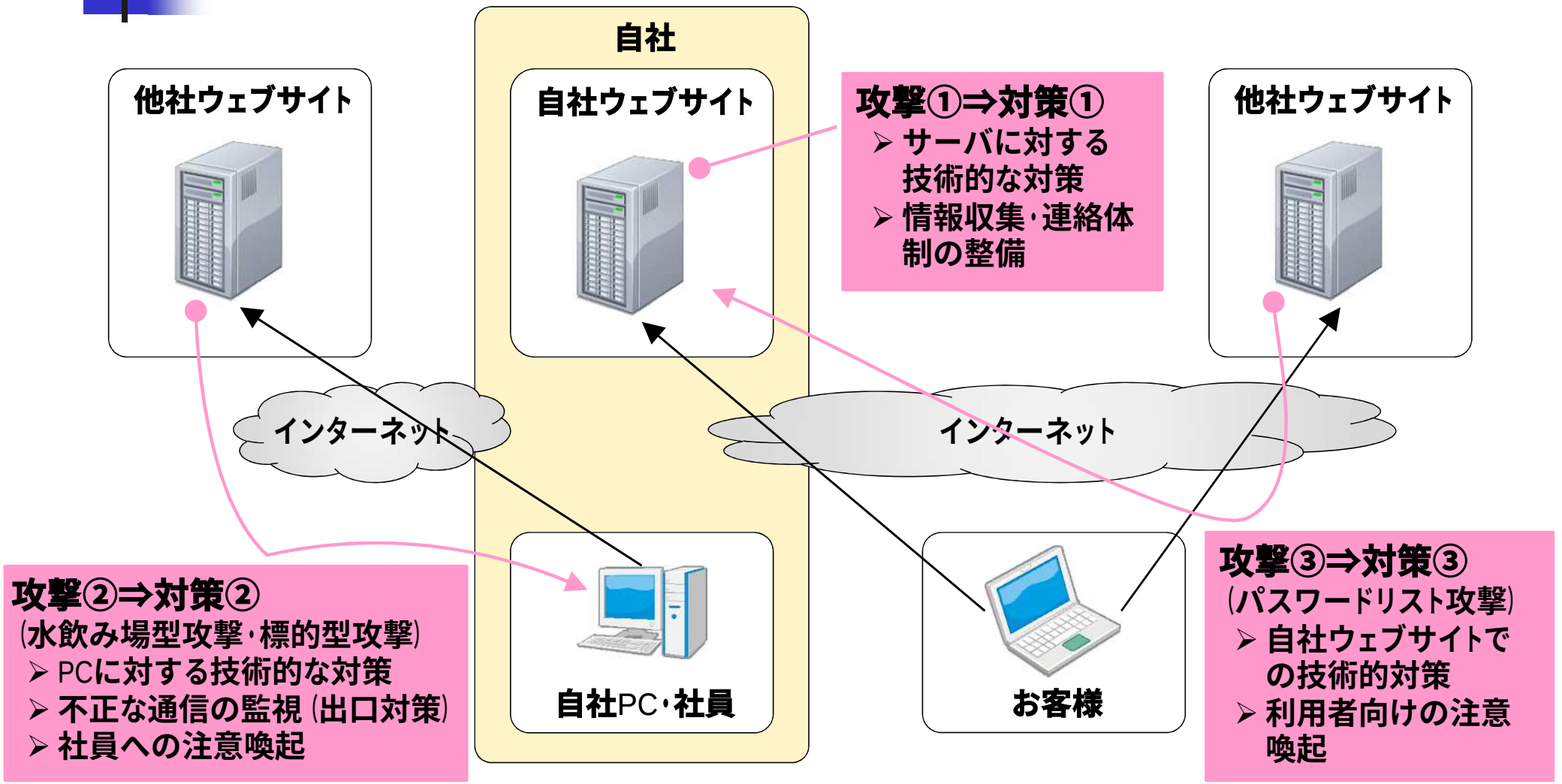
3.ウェブサイトに対する攻撃

3-1-3. 攻撃③：パスワードリスト攻撃（攻撃手法と事例）

攻撃手法	• 攻撃者は、「脆弱なウェブサイトへの攻撃」や「闇サイトを通じた売買」等により、IDとPW（パスワード）の組み合わせリストを入手する。 • 入手したID/PWのリストを利用して一般ウェブサイトへのログインを機械的に試み、IDとPWが一致すれば（ID/PWを使い回していれば）ログインできてしまう。
事例（1） **概要・経緯**	• 3月18日：A社の会員サイトに外部からの不正なログインがあったことを公表 ➢ 3月17日に不正ログインの形跡を認識し、サービスを一旦停止し、調査開始 ➢ 不正ログイン試行対象期間：2014年3月16日～3月17日 ➢ 合計約92万件の不特定多数のIPアドレスから断続的・機械的な不正ログイン試行 ➢ 不正ログイン対象者には個別にメール等で連絡 • 3月26日：ウェブサイトを通じたサービスの全面再開を公表
事例（2） **概要・経緯**	• 4月23日：B社の会員サイトに外部からの不正なログインがあったことを公表 ➢ 4月18日に不正ログインの形跡を認識し、調査開始　（※認識までに日数を要した） ➢ 不正ログイン試行対象期間：2014年3月23日～4月21日 ➢ 合計460万件超の不特定多数のIPアドレスから断続的・機械的な不正ログイン試行 ➢ うち78,361件で不正ログイン（氏名、住所等の個人情報が閲覧されたおそれ） ➢ 対象アカウントでのログインを不可とする措置、パスワード変更依頼をメールで通知

当攻撃は2013年頃から有名な会員サイト等を狙って多数発生

3-2. ウェブサイトに関する攻撃への対策（まとめ）



攻撃の種類に応じて、技術的対策・管理的対策を検討・実行することが重要

3.ウェブサイトに対する攻撃

3-2-1. 対策①：ウェブサイトに関する対策

技術的対策	• サーバOSのパッチ適用、バージョンアップ • サーバOS以外のソフトウェアへのパッチ適用、バージョンアップ ➢ データベースソフト（Oracle、SQL Server等） ➢ 暗号化通信ソフト（Open SSL） ➢ ウェブサイト開発用ソフト（Apache Struts：アパッチ ストラッツ） 等々 • 特権ID（Administrator、root）の適切な管理
管理的対策	• 問題発生に備えた社内連絡体制の整備 • 問題発生時に迅速かつ適切な行動を取れるようにするための机上訓練・実地訓練 • ウェブサイト担当ベンダーとの連絡体制の確認 • ウェブサイトに関連するセキュリティ情報の収集 ➢ 当事務局発信のメルマガの活用 ➢ 公的機関・有名機関等からの公表ニュースの収集 ➢ 担当ベンダーからの情報提供

ウェブサイト（インターネット接続サーバ）については、技術的対策の着実な実施が重要

3.ウェブサイトに対する攻撃

3-2-2. 対策②：標的型攻撃に対する対策

技術的対策 PCに対する 基本的な対策	• OSに対するパッチ適用 • アプリケーションに対するパッチ適用 ➢ ブラウザ、MS-Office、Adobe Reader/Flash、JAVA　等 • ウイルス対策ソフトの導入＆パターンファイルの定期更新
技術的対策 ネットワーク等 に対する対策	• 外部からの不審なアクセスを防御する仕組み ➢ FW（ファイアウォール）、WAF（Webアプリケーション用FW） ➢ IDS/IPS（IDS：侵入検知システム、IPS：侵入防御システム） • 内部からインターネットへの不正な通信の監視 ※出口対策（攻撃＆感染を前提に、情報の外部流出を検知・防止する仕組み）
管理的対策	• 標的型攻撃（標的型メール攻撃、水飲み場型攻撃）といった新たな攻撃についての説明 • ウェブサイトや電子メール利用に際しての社員への注意喚起 ➢ 不審なサイトにはアクセスしない ➢ 不審なメールは開かない、不審な添付ファイルは開かない

インターネットを通じた攻撃手法が高度化・巧妙化しているので、対策の強化が必要

3.ウェブサイトに対する攻撃

3-2-3. 対策③：パスワードリスト攻撃への対策

技術的対策 **自社ウェブサイトでの対策**	• 機械的・連続的なログイン要求を発見・遮断する仕組みの導入（攻撃者の特定） ➢ 当機能を備えたFW（ファイアウォール）等の専用機器 ➢ 監視用機器・アクセスログの適時適切なチェック • 機械的・連続的なログイン要求を防止する仕組みの導入（個々のIDを防御） ➢ ログイン画面に画像認識機能を追加 ➢ ログイン失敗が一定回数を超えると当該IDをロック
管理的対策	• 利用者向けの注意喚起 ➢ 他のウェブサイト、サービスで使用しているID/パスワードを使用しない ➢ パスワードは定期的に変更する ➢ 過去に使用したパスワードは再使用しない ➢ 第三者が容易に推測できるパスワードは使用しない ※サイト利用者個人としては、ウェブサイト毎にID/PWを変更することが困難な場合でも、少なくとも重要なウェブサイト（個人情報を多数登録するなど）と単純なウェブサイトでIDやパスワードを同一にすることは避けましょう！

IDを利用するウェブサイトについては、攻撃されることを前提に事前対策を考えることが必要

3.ウェブサイトに対する攻撃

3-2-4. (参考) セキュリティパッチ適用の必要性(1/2)

Windows等のOS

- Windows等のOSは改良が加えられているものの、新たな脆弱性 (問題点、セキュリティホール) も次々と見つかっている。 以下はWindowsの脆弱性の例。
  - ✓ 細工が施されたWebページにInternet Explorerでアクセスし、F1キーを押してヘルプファイルを呼び出した場合、悪意のあるプログラムを勝手に実行されてしまう。
  - ✓ 特別に細工された AVI ファイル (ビデオ) を開いた場合、悪意のあるプログラムを勝手に実行されてしまう。
  - ✓ 特別な細工がされたメディア コンテンツ (音楽、ビデオ等) をMedia Playerで開いた場合、悪意のあるプログラムを勝手に実行されてしまう。

※悪意のあるプログラムを勝手に実行されてしまうと、メールやファイル等を盗み見られたり、勝手に削除されたり、あるいは、IDやパスワードを盗まれたり、ウイルスやスパイウェアを埋め込まれたりと、何をされるか分からないことになり、非常に危険な状態となる。

パソコンやサーバを安全に使うためには、
OSに対する最新のセキュリティパッチを適時に適用し続けることが必要

特に不特定多数が利用するインターネットに接続している場合は、
悪意のある者がいろんなワナ・攻撃を仕掛ける可能性があり、セキュリティパッチの適用は必須

3-2-4. (参考) セキュリティパッチ適用の必要性(2/2)

OS以外の各種ソフトウェア

- 前ページではWindows等のOSを例にとり、セキュリティ上の脆弱性を紹介したが、OS以外のソフトウェアであっても、以下のような脆弱性事例が発生している。
  - ✓Microsoft Excel
    - 特別な細工がされたExcelファイルを開いた場合、悪意のあるプログラムを勝手に実行されてしまう。
  - ✓Adobe Reader (PDFファイルの参照に利用)
    - 特別な細工がされたPDFファイルを開いた場合、悪意のあるプログラムを勝手に実行されてしまう。
  - ✓Adobe Flash Player (Webページのアニメーションやグラフィックス再生に利用)
    - 特別な細工がされたWebページにアクセスし、Flash Playerで表示した場合、悪意のあるプログラムを勝手に実行されてしまう。

※悪意のあるプログラムを勝手に実行されてしまった場合の被害はOSでの例と同じであり、場合によっては非常に危険な状態となる。

OS以外の各種ソフトウェアについても、セキュリティパッチの発行状況を確認し、最新のセキュリティパッチを適時に適用し続けることが必要

3.ウェブサイトに対する攻撃

3-2-5. (参考) ビデオを活用した社員研修の事例(1/2)

- IPAでは情報セキュリティに関する啓発用の映像コンテンツを公開している。

  http://www.ipa.go.jp/security/keihatsu/videos/index.html

  - 2012年5月から取り組み始め、2015年11月現在で15編のビデオを公開
  - 各編が約10分で簡潔にまとめてある
  - YouTubeを利用しているので、インターネットに接続可能な
    パソコン等があれば簡単に視聴可能
  - IPAに申し込めば、基礎知識DVD-ROM (10編の映像も含む) が
    企業あたり1枚に限り無償で提供してもらえる
    ※DVDの利用は、社内研修等、営利を目的としない用途に限る
    ※具体的な申込方法等は、IPAサイトを参照
  - 組織内で利用する場合は、DVD内のコンテンツを媒体やサーバにコピーし、利用することも可能

	**あなたの組織が狙われている！** **-標的型攻撃 その脅威と対策- (約10分)** 2012/05/08**公開** 標的型攻撃メールをうっかり開いてしまい、情報漏えい事件を起こしてしまった会社員の主人公。ナビゲーターの解説を通じて、標的型攻撃の実態と対策について学べます。
	**ウイルスはあなたのビジネスもプライベートも狙っている！(約10分)** 2013/01/30**公開** ウイルスの中にはパソコン利用者に気づかれないように密かに情報の抜き取りや乗っ取りやWebカメラによる盗撮を行うものがあります。ドラマを交えた本映像を通じて攻撃者の狙いを知り、被害に遭わないための対策を理解していただきたいと思います。

3-2-5. (参考) ビデオを活用した社員研修の事例(2/2)

IPAビデオの解説シートを作成

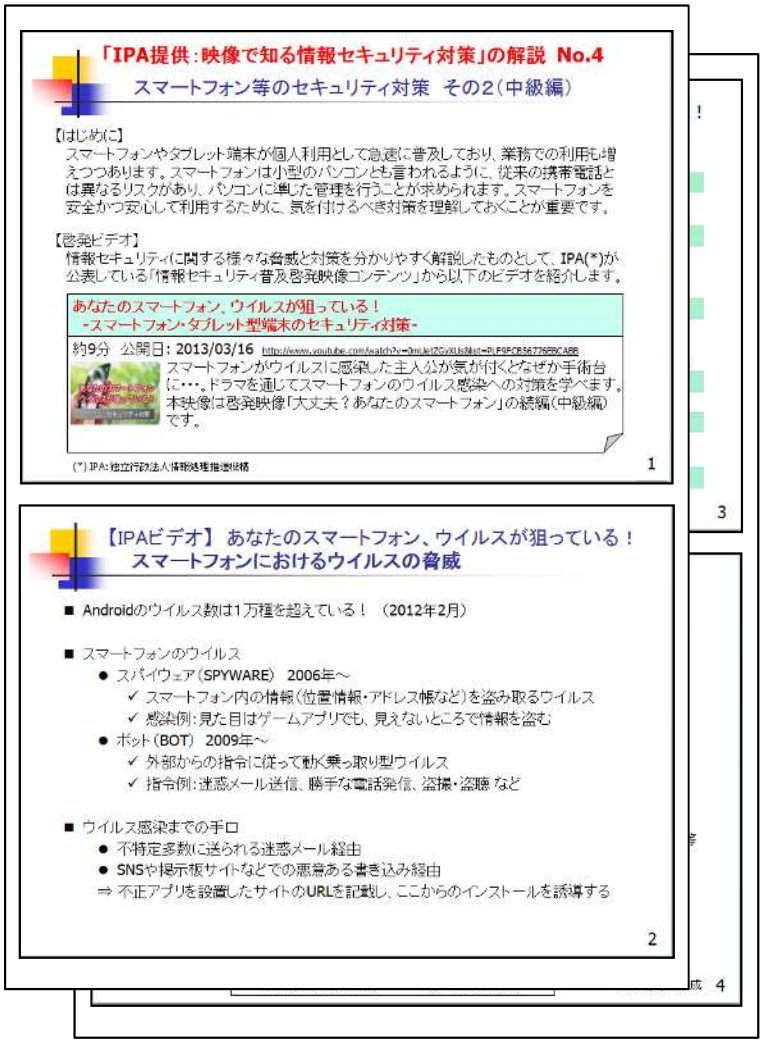
【解説シートの概要】

- 前ページにあるIPAビデオの理解を深めるために各ビデオの内容をまとめた解説シートを作成
- 解説シートは4ページで以下の構成
  - P1：はじめに & 啓発ビデオ紹介
  - P2,3：ビデオ内の表示内容、説明内容のまとめ
  - P4：関連する当社の取組 (規程、GL等) の紹介

【各社での活用方法】

- 社内研修でのビデオ放映に合わせて、解説シートを配布し、理解を深めてもらうようにしている。

解説シート



4．ウェブサイトのセキュリティ対策状況点検事例

4.ウェブサイトのセキュリティ対策状況 点検事例
はじめに

- 前パートでみたようにウェブサイトに対する脅威は様々なものがあります。セキュリティ対策に関する情報は多数公表されていますが、単に情報収集するだけでは不十分で、実際に自己点検（チェック）をすることが重要です。自己点検を通じて、自らの弱いところが把握でき、適切な対策の検討・実現にも繋がると言えます。
- 当パートでは、IPAのチェックリストを活用した点検事例について、ご紹介いたします。あくまでも一企業の結果ですので、対策レベルの善し悪しではなく、全体的な状況・傾向を理解するのに参考にしていただければと思います。

4. ウェブサイトのセキュリティ対策状況 点検事例

4-1. 参考にしたIPAのチェックリスト

4-2. セキュリティ対策点検の概要･ウェブサイト種別

4-3-1. 点検結果(1) CMSの安全確保

4-3-2. 点検結果(2) ウェブサイトの攻撃検知･防御

4-3-3. 点検結果(3) ペネトレーションテスト

4-3-4. 点検結果(4) セキュリティ教育･訓練

4-3-5. 点検結果(5) サーバソフトウェアの脆弱性解消

4-3-6. 点検結果(6) 改ざんの早期発見対応

4-3-7. 点検結果(7) 改ざん発生に備えた対応

4-3-8. 点検結果(8) ウェブアプリ開発時のセキュリティ

4.ウェブサイトのセキュリティ対策状況 点検事例
4-1. 参考にしたIPAのチェックリスト

IPAからウェブサイトのセキュリティ確保のため、各種の対策情報を公表

IPAテクニカルウォッチ
「ウェブサイト改ざんの脅威と対策」
～企業の信頼を守るために求められること～
2014/8/29**公表　全**22**ページ**
https://www.ipa.go.jp/security/technicalwatch/20140829.html

- **ウェブサイト改ざんの対策をまとめたもの**
- **ウェブサイトセキュリティ対策状況チェックリスト**

  社内の役割に応じたチェック項目を例示
  - ✓ **経営者層** (3**項目**)
  - ✓ **システム管理者** (9**項目**)
  - ✓ **ウェブサイト運営者** (5**項目**)
  - ✓ **ウェブアプリケーション開発者** (2**項目**)

主にウェブサイト開設後の運用チェック

「安全なウェブサイトの作り方 改訂第7**版」**
2015/3/26**改訂　全**115**ページ**
https://www.ipa.go.jp/security/vuln/websecurity.html

- SQL**インジェクションやクロスサイト・スクリプティング 等**11**種類の脆弱性とその対策を解説したもの**
- **ウェブアプリケーションの**
  セキュリティ実装 チェックリスト

  ※**上記の**11**種類の脆弱性毎に全約**50**のチェック項目を例示**

  ※**主にウェブアプリケーション開発者が留意すべき事項**

主にウェブサイト開発時の技術的チェック

※IPA 「ウェブサイト改ざんの脅威と対策　～企業の信頼を守るために求められること～」2014/8/29公表をもとに作成
※IPA 「安全なウェブサイトの作り方 改訂第7版」2015/3/26改訂公表をもとに作成

4.ウェブサイトのセキュリティ対策状況 点検事例

4-2. セキュリティ対策点検の概要・ウェブサイト種別

A社でのウェブサイトのセキュリティ対策チェックの事例

対象：グループの125社、202サイト
目的：運用中のウェブサイトを対象にセキュリティ対策状況の現状を把握し、課題を識別すること
方法：各ウェブサイトの管理者が回答　(必要に応じて外部委託先に問い合わせ)
　　前ページのIPAチェックリスト2種類を利用
　　全てのウェブサイトを対象に運用を調査
　　「ウェブサイトセキュリティ対策状況チェックリスト」をベースに調査項目を設定
　　ウェブサイトを以下の種別に区分し、開発の要素を含む②について開発を調査
　　「セキュリティ実装 チェックリスト」をそのまま利用　※開発ベンダーに回答を依頼することを想定

■ウェブサイトの種別

※％は総数に占める割合

総数			202	
	① 構成・運用がシンプルなサイト		44	22%
	② 一定の複雑性・重要性を有するサイト		158	78%
		②-1 コンテンツ管理ツール (CMS) を利用したサイト	124	61%
		②-2 お客様情報の入力フォームを有するサイト	118	58%
		②-3 お客様用マイページ (ログイン認証) のあるサイト	35	17%

4-3-1. 点検結果(1) CMSの安全性確保

■コンテンツ管理ツール（CMS）に対して安全なアクセスを確保するための対策

※％は各総数に占める回答割合

	総数	対応済（○）		未対応（×）	
① VPN,SSL等により通信内容を暗号化	144	83	58%	61	42%
② ファイアウォールによるIPアドレス制限	152	69	45%	83	55%
③ 二要素認証（*1）を使用	129	10	8%	119	92%

(*1) 二要素認証：ID/PWと他の要素（電子証明書、ICカード、ワンタイムパスワードなど）を組み合わせてログインのセキュリティレベルを高める方法

コンテンツ管理ツール（CMS）の脆弱性を狙った攻撃も発生しており、CMSが乗っ取られると、サーバが改ざん等されてしまいます。いずれかの対策を行うことが望まれます。

4-3-2. 点検結果(2) ウェブサイトの攻撃検知･防御

■ウェブサイトの攻撃検知･防御のための対策

※％は総数に占める回答割合

	総数	対応済（○）		未対応（×）	
IDS/IPS、WAFなどの攻撃を検知･防御する機器を導入	200	36	18%	164	82%

IDS (Intrusion Detection System)：侵入検知システム　「ネットワークなどへの不正なアクセスの兆候を検知し、ネットワーク管理者に通報する」機能を持つソフトウェア、またはハードウェアである。

IPS (Intrusion Prevention System)：侵入防止システム　異常を通知するだけでなく、通信遮断などのネットワーク防御を自動で行う機能を持つ。

WAF (Web Application Firewall)：ウェブアプリケーションファイアーウォール　Webアプリケーションのやり取りを把握･管理することによって不正侵入を防御することのできるファイアウォール。

従来のファイアーウォールだけの防御では不十分ですが、より高度な機器･システムの導入は途上にあります。ウェブサイトの特性に応じて、導入の検討が望まれます。

4.ウェブサイトのセキュリティ対策状況 点検事例
4-3-3. 点検結果(3) ペネトレーションテスト

■ウェブサイトのセキュリティ上の弱点を把握するための対策

※％は総数に占める回答割合

	総数	定期的に実施（○）		過去に実施（△）		未実施（×）	
ペネトレーションテスト（侵入テスト）の実施	206	14	7%	14	7%	178	86%

※ペネトレーションテスト（侵入テスト）：コンピュータやネットワークのセキュリティ上の弱点を発見するテスト手法の一つで、システムを実際に攻撃して侵入を試みる手法。

ペネトレーションテストにより脆弱性の発見に繋がる場合もありますので、重要なお客様情報を扱っているウェブサイトや古くに開発したウェブサイトでは、実施が望まれます。

4-3-4. 点検結果(4) セキュリティ教育・訓練

■定期的なセキュリティ教育・訓練の実施

※％は各総数に占める回答割合

	総数	定期的に実施（○）		過去に実施（△）		未実施（×）	
①標的型攻撃メールに対する定期的なセキュリティ教育	188	37	20%	114	61%	37	20%
②標的型攻撃メールに対する定期的な訓練	205	11	5%	25	12%	169	82%

標的型攻撃メールに対する教育は約8割で実施されているが、訓練の実施は2割弱に留まる。
実際の訓練を通じて気付くこともあるので、一度は実施することが望まれます。

4-3-5. 点検結果(5) サーバソフトウェアの脆弱性解消

■ウェブサイトのセキュリティ対策

※％は各総数に占める回答割合

	総数	適切に実施（○）		不適切な状況（×）		把握できていない（×）	
① セキュリティパッチの適用	207	172	83%	25	12%	10	5%
② ソフトウェアのバージョンアップ	206	162	79%	34	17%	10	5%

ウェブサイト用サーバにおいては、セキュリティパッチの適時適用は必須です。運用委託先と協議するなどして、確実に適用される環境を整える必要があります。

4-3-6. 点検結果(6) 改ざんの早期発見対応

■ウェブサイト改ざんの早期発見のための対策

※％は各総数に占める回答割合

	総数	両方あり（○）		前者のみ実施（△）		両方なし（×）	
①「コンテンツの定期的なチェック」と「改ざん検知機能」の組み込み状況	208	10	5%	41	20%	157	75%
②「アクセスログの管理」と「攻撃の痕跡確認」の実施状況	208	24	12%	161	77%	23	11%

対策状況はまだ途上ですが、IPAから「ウェブサイトの攻撃兆候検出ツール（iLog Scanner）が配布されているように、簡易なツールをまずは使ってみることも一案です。

4-3-7. 点検結果(7) 改ざん発生に備えた対応

■ウェブサイト改ざん発生に備えた対策

※％は各総数に占める回答割合

	総数	両方あり（○）		前者のみ実施（△）		両方なし（×）	
①「対応マニュアルを作成し、」「定期的に訓練も実施」	202	18	9%	38	19%	146	72%
②「バックアップを取得し、」「サイトの改ざん有無を確認」	205	29	14%	156	76%	20	10%

バックアップの取得は多くのウェブサイトでできていますが、インシデントに備えたマニュアル整備や訓練への対応は今後の課題です。

4-3-8. 点検結果(8) ウェブアプリ開発時のセキュリティ

■ウェブサイト開発時のセキュリティ対策

※％は各総数に占める回答割合

	総数	安全を確認（○）		一部に不備あり（×）		委託先からの回答なし（×）	
全体	144	98	68%	40	28%	6	4%
②-1 コンテンツ管理ツール（CMS）を利用したサイト	116	82	71%	30	26%	4	3%
②-2 お客様情報の入力フォームを有するサイト	92	66	72%	24	26%	2	2%
②-3 お客様用マイページ（ログイン認証）のあるサイト	32	22	69%	9	28%	1	3%

- ウェブサイト開発時にアプリケーション上の脆弱性を作らないよう、セキュア・プログラミングを行うことが大事であり、そのような開発委託先を選定することが必要です。
- ウェブサイトの見栄え（デザイン）と安全（セキュリティ）、両方とも大事です。

最後に

まとめ

- サイバー攻撃がますます複雑化･巧妙化する中で、自らが属する会社･機関が既に悪意ある攻撃者によって狙われているかもしれません。
- 組織のセキュリティレベルは平均点で表されるのではなく、最低点で決まります。
- このため、システム監査人は自社のサイバーセキュリティ対策が有効に機能しているかについて、管理面･技術面の両面からチェックすることが求められます。
  実際に他社で発生している事例や、IPA･NISC等の公的機関が公表する情報も収集し、両面から的確なチェックができるように日頃からの研鑽も必要になってきます。
- 一方で、技術面については、攻撃･対策ともに非常に高度になってきていますので、システム監査人が全てに対応することは現実的ではなくなりつつあります。
  自社のウェブサイトやネットワーク環境の特性によっては、外部の専門家を活用することも有効な対応と言えます。特に専門スキルを要するペネトレーションテストについて、システム部門か監査部門のいずれかが主体となって一度は実施することが望まれます。自社セキュリティ対策の全体像を見据えて、社内でよく協議することが重要です。
- システム監査･セキュリティ監査に対する経営陣からの期待はますます高まるものと推察されます。システム監査人として期待に応えられるように、日々精進に努めなければならないとあらためて決意し、結びとさせていただきます。

参考資料

■日本年金機構における不正アクセスによる情報流出事案に関する報告書

No	タイトル／URL／概要	頁数	発行元	発行時期
1	「不正アクセスによる情報流出事案に関する調査結果報告書」 http://www.nenkin.go.jp/files/kuUK4cuR6MEN2.pdf	49	日本年金機構	2015/8/20
2	「同」（概要版） http://www.nenkin.go.jp/files/e7wRRjRfiKiN1.pdf	17	同上	同上
3	「日本年金機構における不正アクセスによる情報流出事案検証委員会検証報告書」 http://www.nenkin.go.jp/files/XtYrbhaJKiEk4.pdf	43	厚生労働省	2015/8/21
4	「同」（要約版） http://www.nenkin.go.jp/files/GBWiTzeRPmtU3.pdf	27	同上	同上

■教育・研修用のツール等

No	タイトル／URL／概要	作成元
1	『標的型攻撃メールの分析に関するレポート』　2011年10月3日公表　全27ページ ※だましのテクニック事例4件の紹介と標的型攻撃メールの分析・対策を記したもの http://www.ipa.go.jp/about/technicalwatch/pdf/111003report.pdf	IPA （情報処理推進機構）
2	映像で知る情報セキュリティ ～映像コンテンツ一覧～ ※情報セキュリティ上の様々な脅威と対策を学べる約10分のビデオが全15本掲載。 https://www.ipa.go.jp/security/keihatsu/videos/	IPA （情報処理推進機構）

ご清聴ありがとうございました。

(参考) 発表者プロフィール

植垣 雅則

(うえがき　まさのり)

有限責任監査法人トーマツ
アドバイザリー事業本部
エンタープライズリスクサービス

シニアマネジャー

masanori.uegaki@tohmatsu.co.jp

- **公認内部監査人** (CIA)
- **情報処理技術者試験** (システム監査技術者, システムアナリスト, プロジェクトマネージャー, アプリケーションエンジニア, ネットワークスペシャリスト, データベーススペシャリスト, テクニカルエンジニア (システム管理), エンベデッドシステムスペシャリスト, テクニカルエンジニア (情報セキュリティ), 情報セキュリティアドミニストレータ, 上級システムアドミニストレータ　等　計13試験)
- **日本システム監査人協会　近畿支部　会員**
- **大手ベンダーでの地方銀行向け勘定系システム等の設計･開発･運用業務を経て、2002年より有限責任監査法人トーマツにて監査に従事。現在は主として金融機関向けのシステムリスク監査、システム統合リスク監査、IT統制監査、情報セキュリティ･個人情報保護に関するコンサルティング業務を多数手がける。**