IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

「2012年版 10大脅威」
～変化・増大する脅威！～

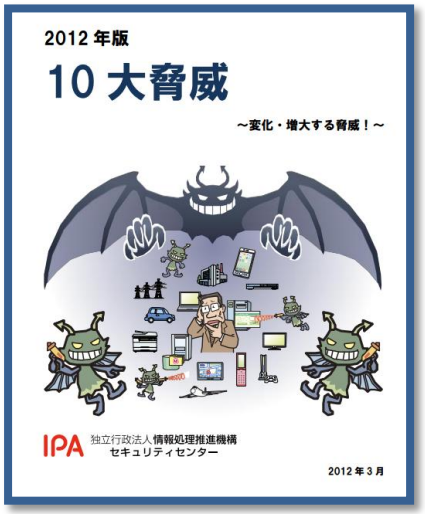
独立行政法人情報処理推進機構（IPA）
技術本部 セキュリティセンター

2012年版「10大脅威の概要」

http://www.ipa.go.jp/security/vuln/documents/10threats2012.pdf

2012年版10大脅威は、2011年に発生したセキュリティインシデントや攻撃情報などの一般報道を基にして、情報セキュリティ分野の研究者や実務担当者123名で構成する「10大脅威執筆者会」でまとめています。

第1章	・情報セキュリティを取巻く環境の変化
第2章	・10の脅威について概要と影響の解説
第3章	・今後対策が重要となる脅威



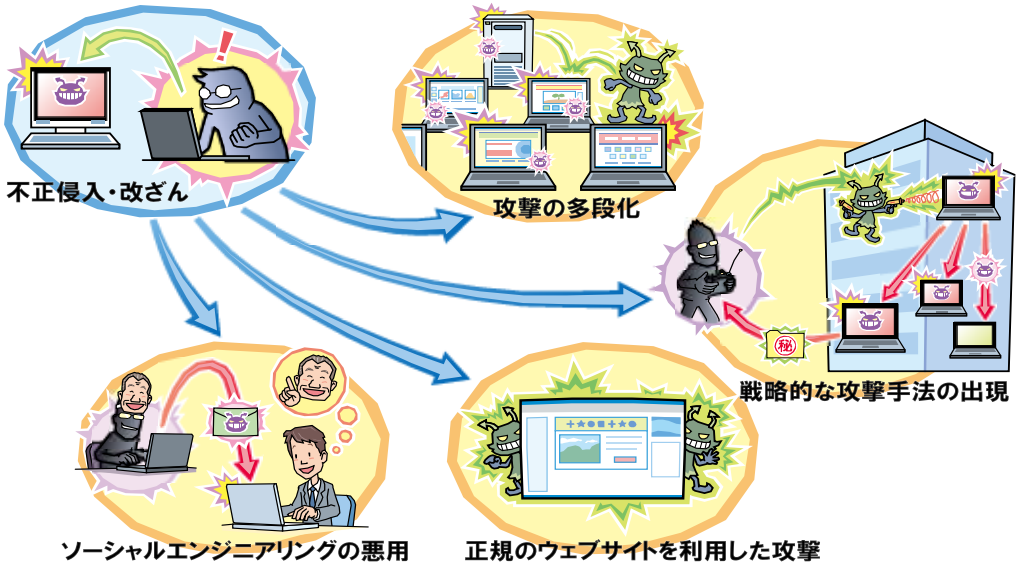
情報セキュリティを取り巻く状況の理解やセキュリティ対策の参考に、本書をご活用ください。 内部への教育資料に

目次

- 1章「情報セキュリティを取巻く環境の変化」
  ～攻撃手法、システム環境、攻撃者像、攻撃時のインパクトの変化について ～
- 2章「2012年版 10大脅威」
  ～セキュリティ専門家が選ぶ2011年に起こった10の脅威について～
- 3章「今後対策が必要となる脅威」
  ～今後、国内で顕在化しそうな脅威の概要と傾向～

1．攻撃手法の変化

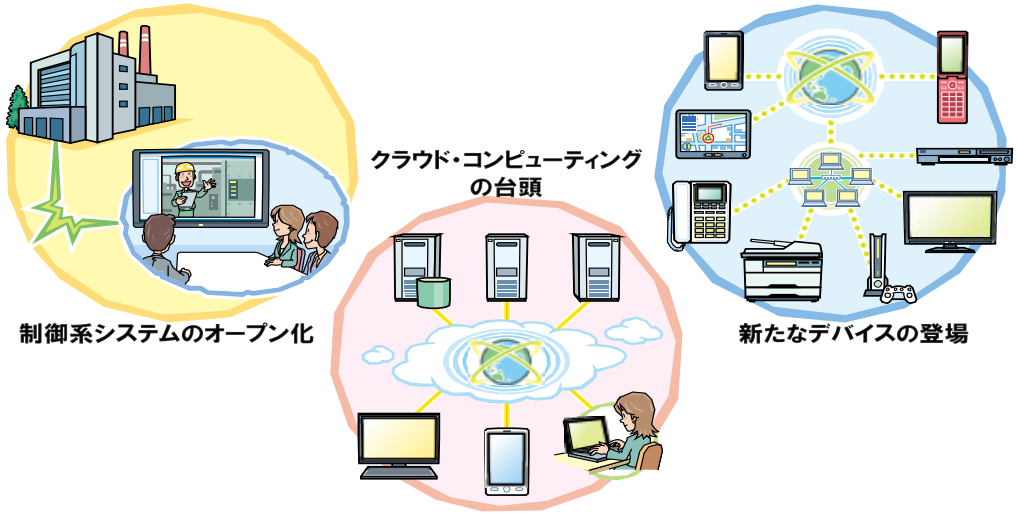
～「１つの脆弱性＝１つの攻撃」から人を騙すテクニックや洗練した手法の登場～



- 近年の傾向
  - 複数の攻撃を駆使した多段型の攻撃に変化
  - 正規のウェブサイトを踏み台に使った攻撃の出現
  - 人の心理面をつくソーシャルエンジニアリングの出現
  - 複数の攻撃を戦略的に使う攻撃手法の出現

2. システム環境の変化

～システム環境の変化により、新たな脅威が生じる～



- **システム環境の変化により下記のような脅威が発生**
  - **ネットワークに接続する新たなデバイスの登場により**
    - 外部から攻撃を受ける脅威に晒される状態
    - 個人に紐づく情報を保持するスマートフォンは、攻撃への影響が大きい
  - **制御系システムのオープン化により**
    - クローズド⇒オープン化　になったことにより情報システムと同様になった
    - 攻撃者にとって攻撃しやすい環境になってきた
  - **クラウドの台頭により、データ管理の考え方の変化**

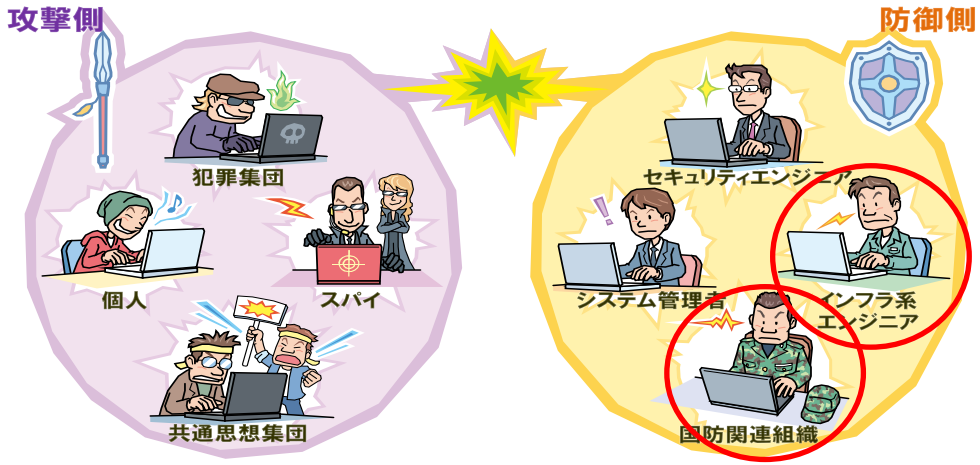
3. 情報セキュリティを取巻く構図の変化

～金銭目的から「諜報活動」「主張型攻撃」を目的とした攻撃者の出現～

- **攻撃者側の構図の変化**
  - **スパイ活動や社会インフラを狙う集団の出現**
    - 国防関連、エネルギー関連、企業の知的財産情報の窃取を狙った攻撃の発生
    - 製造・制御ラインを狙った攻撃の発生
    - 攻撃者は膨大な資金と技術を持った大きな組織であると考えられている
  - **共通思想集団の存在**
    - 「Hacker」+「Activist」=「Hactivist（ハクティビスト）」 新用語の登場
    - 自分たちの主張に敵対する国家や企業のサーバなどへ攻撃を加える
    - インターネット上で攻撃予告、攻撃成果をネット上に公開することで、主張を誇示

3．情報セキュリティを取巻く構図の変化

～企業の情報セキュリティ対策からナショナルセキュリティへ～



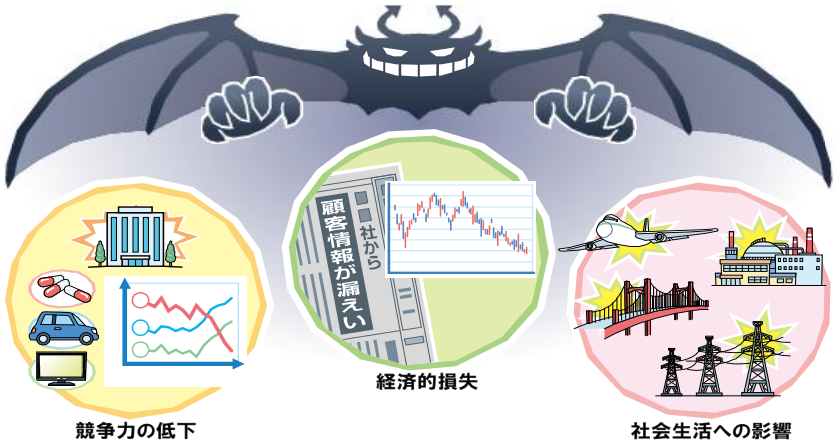
- **防御側の構図の変化**
  - **制御系・組込み系システムへの拡大**
    - 制御・組込系システムが攻撃対象の拡大
    - **制御系エンジニアにも、セキュリティ対策が求められるようになった**
  - **ナショナルセキュリティとしての対応**
    - 米国国防省は、サイバー空間を陸、海、空、宇宙に次ぐ第5の新たな戦場と宣言
    - 政府機関や軍需関連産業まで巻き込んだ防衛体制となりつつある
    - **サイバー攻撃が軍事行動、経済活動の一端を担う意味合いに変化**

4. 攻撃によるインパクトの変化

～一企業の不祥事だった問題が社会的問題に～

- **インシデントが発生した際の組織に与えるインパクトも増大している**
  - **機密情報が窃取されることで・・・。**
    - **知的財産の場合・・・模倣品出現⇒市場での競争力の低下⇒企業収益の低下**
    - **国家機密情報の場合・・・外交上のアドバンテージを奪われる⇒国益に影響**
    - **将来の利益や国益が奪われる大きな問題**
  - **情報の大量流出（メガリーク）することで・・・。**
    - **大手ゲームメーカーの例では、1ヶ月近くサービスを停止せざるをえない状況**
    - **ブランドイメージの大幅な低下、営業利益にも影響**
    - **一企業の不祥事的な扱いから社会的な問題に**

4. 攻撃によるインパクトの変化



- インシデントが発生した際の組織に与えるインパクトも増大している
  - 社会インフラが狙われることで・・・。
    - 海外では、工場プラントや鉄道システムが攻撃により一時停止した事例がある
    - 社会インフラが攻撃を受けた場合、我々の社会生活にも大きく影響する
      ex.電力供給停止、鉄道停止、工場停止 etc

今後、求められる対応とは？

- システムトータルでの対策
  - セキュリティ製品の適切な配置と設定、情報資産の管理、攻撃を受けても実害を防ぐためのネットワーク設計など視点を広げた対策が必要
  - システム管理部門、ユーザ部門、さらには、企画部門や経営陣などが連携してシステムトータルで対策検討
- 情報共有の仕組み
  - 近年の攻撃は被害に気付きにくく、特定の組織に対する攻撃のため、攻撃情報が表に出ない傾向にある
  - １つの組織・機関だけの対応には限界が見えてきており、情報共有の枠組みが求められている
- 組織毎の脅威の見極め
  - 攻撃を受けた際の損失を見極めた上で、組織の運用形態や現状の対策状況に合わせて対策を講じることが重要

目次

- 1章「情報セキュリティを取巻く環境の変化」
  ～攻撃手法、システム環境、攻撃者像、被害時のインパクトの変化について ～
- **2章「2012年版 10大脅威」**
  ～セキュリティ専門家が選ぶ2011年に起こった10の脅威について～
- 3章「今後対策が必要となる脅威」
  ～今後、国内で顕在化しそうな脅威の概要と傾向～

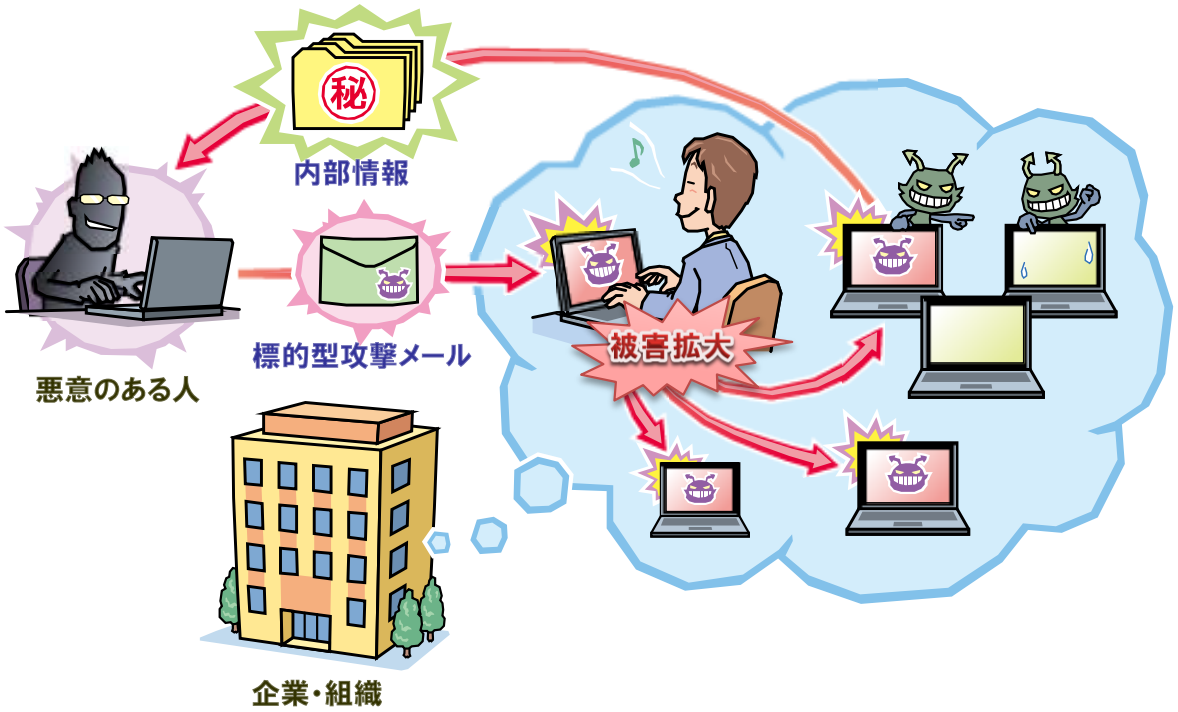
2012年版
執筆者会が選んだ10大脅威と脅威の変遷

IPA

	2012年版10大脅威	2011年	2010年	2009年	2008年	2007年
1位	機密情報が盗まれる!? 新しいタイプの攻撃（標的型攻撃） 定番	5位	6位	3位	4位	2位
2位	予測不能の災害発生！ 引き起こされた業務停止 New	–	–	–	–	–
3位	特定できぬ、共通思想集団による攻撃 New	–	–	–	–	–
4位	更新忘れのクライアントソフトを狙った攻撃 定番	3位	2位	–	8位	–
5位	ウェブサイトを狙った攻撃 定番	2位	1位	2位	5位	9位
6位	スマートフォンやタブレットを狙った攻撃	4位	–	–	–	–
7位	大丈夫 !? 電子証明書に思わぬ落し穴 New	–	–	–	–	–
8位	身近に潜む魔の手・あなた職場は大丈夫？（内部犯行・情報漏洩の脅威） 定番	1位	5位	5位	3位	7位
9位	危ない！ アカウントの使まわしが被害を拡大 定番	–	8位	4位	–	8位
10位	利用者情報の不適切な取扱いによる信用失墜（プライバシーに係る問題） New	–	–	–	–	–

長い間、脅威と認識されながらも解消されない脅威の存在を無視できない。継続的に対策を行うことが組織に求められる

【1位】機密情報が盗まれる!? 新しいタイプの攻撃



- 脅威
  - 組織の機密情報が窃取されてしまう
  - 攻撃に気付けない。有効な対策方法がない

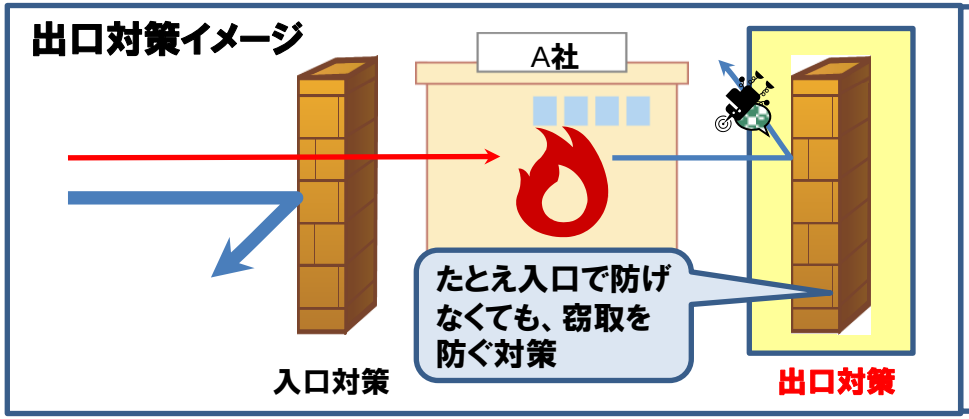
【1位】機密情報が盗まれる。新しいタイプの攻撃

- **事例1：衆議院への攻撃**
  - 衆議院議員1人のパソコンで、ウイルス付きのファイルを開いたことでウイルスに感染
  - ネットワークを経由して感染範囲が拡大しサーバとパソコン計32台がウイルスに感染した。
  - 全議員約480人のIDとパスワードが流出し、最大15日間にわたってメールが攻撃者に見られていた可能性

- **事例2：大手重工業へのサイバー攻撃**
  - 外部からの標的型攻撃メールにより、システム内部に侵入されたと言われている
  - 本社のほか工場、研究所など国内11拠点にあるサーバ45台と従業員が使用していたパソコン38台の感染が確認された

【1位】機密情報が盗まれる。新しいタイプの攻撃

- 対策
  - 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」

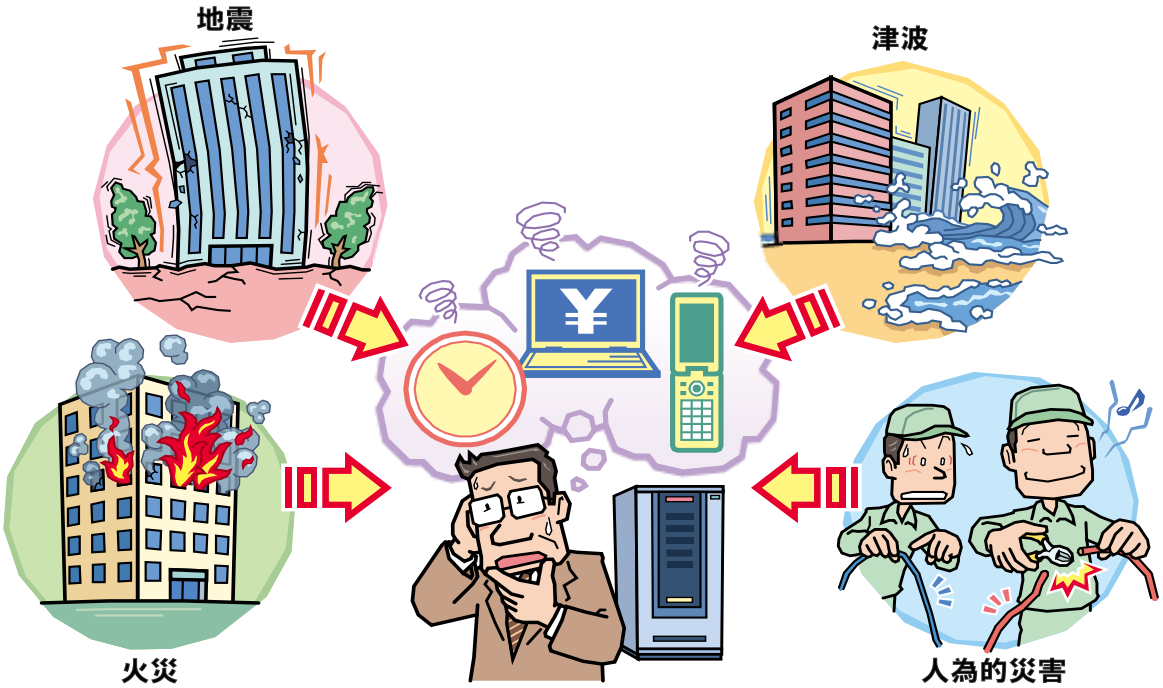


出口対策によりたとえ攻撃されても、組織への影響を回避することが重要

詳細はこちら

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

【2位】予測不能の災害発生！ 引き起こされた業務停止



- 脅威
  - 3.11の震災に伴い、様々な事象が連鎖した
    - 地震によるサーバ障害、津波による戸籍データ消失
    - サービスの中断、収入の途絶、顧客からの信用低下

【2位】予測不能の災害発生！ 引き起こされた業務停止

- **事例1：東北地方太平洋沖地震**
  - **直接被害**：地震によるサーバ障害や津波による戸籍データの消失
  - **間接被害**：計画停電により38％企業が事業に何らかの影響を受けた
  - **間接被害**：義援金の振り込みが殺到し10日間におよぶシステム障害

- **事例2：作業ミスによる事業停止**
  - **人災**：データセンターにおいて、業者が誤って回線を切断してしまい、中核事業が一時的に停止した

直接的な被害ばかりが目立つが、災害発生後の人災や間接被害も見過ごせない

【2位】予測不能の災害発生！ 引き起こされた業務停止

- 対策：行動計画、BCP（事業継続計画）の策定・運用
  - 事業に優先度をつける
  - 事業に不可欠な資源を把握する
  - 資源の代替策を用意、検討する
  - 許容可能な停止期間を決める
  - 事業が影響を受ける災害を洗い出す
  - 復旧計画を立てる
  - BCP発動前の事前対策を検討する

緊急事態に備え、事業継続および早期復旧を可能にするための行動計画を立てることが重要

【3位】特定できぬ、共通思想集団による攻撃

- 脅威
  - 自分たちの主義・主張に反する政府機関や企業を攻撃する集団の出現
  - ソーシャルメディアを活用することで手広く仲間を募り、攻撃を呼び掛ける
  - 自らの主張を認めさせるために、攻撃を予告し、攻撃対象組織が主張を見直すように要求。要求が却下されれば、攻撃を実施

    攻撃例：DDoS,機密情報の暴露、ウェブサイトの改竄

【3位】特定できぬ、共通思想集団による攻撃

- **事例1：ソニー株式会社へのDDoS攻撃**
  - ソニー株式会社が運営する複数のサイトに「Anonymous（アノニマス）」と呼ばれる集団による、DDoS攻撃の実施
  - 複数のサイトが継続的にダウンするなど、サービスの提供が困難な状況に陥った

- **事例2：任天堂株式会社への暴露攻撃**
  - 「LulzSec」と呼ばれる集団が、任天堂の米国サーバの脆弱性を悪用した不正アクセスを行い、ウェブサーバの設定ファイルを公開
  - Lulzsecの要望は、任天堂がサーバの脆弱性を修正することであった
  - 共通的思想を持つ集団が組織の機微な情報を暴露した攻撃の一つであると考えられる

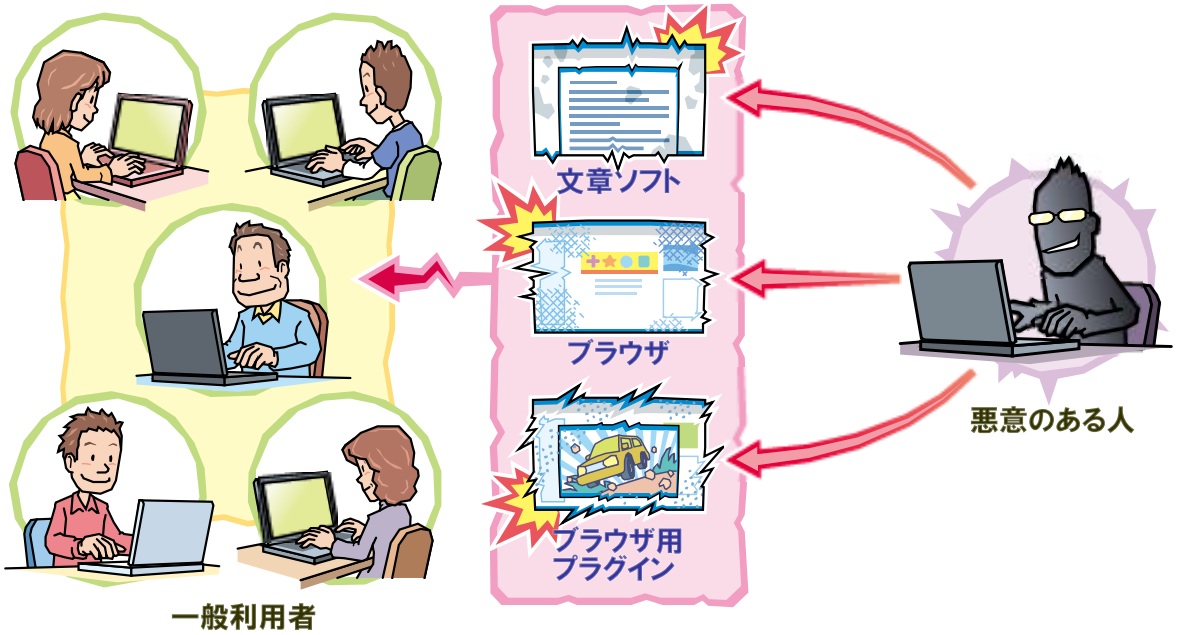
【3位】特定できぬ、共通思想集団による攻撃

- **対策1：定期的なセキュリティ対策**
  - 公開サーバの脆弱性対策等の日ごろからのセキュリティ対策の実施
  - 機密情報の取り扱いに関する内部ルールの制定と定期的な見直し

- **対策2：利用者の意見に耳を傾ける**
  - 対立する問題に対して、適切に対応することにより、問題の発生を未然に防げる可能性がある
  - 対決姿勢を煽らない対応も重要である

公開サーバ（サービス）に対して、日頃からセキュリティ点検と対策を行うことが重要

【4位】今もどこかで…更新忘れのクライアントソフトを狙った攻撃



- 脅威
  - Adobe Reader,Flash Player,Java等の脆弱性を突いた継続的な攻撃の発生
  - OSの脆弱性よりもクライアントソフトの脆弱性が狙われる傾向にある
  - クライアントソフトの脆弱性は、標的型攻撃におけるシステム侵入手段やウイルス感染などに悪用されることが多く、情報窃取に繋がる危険性がある

【4位】今もどこかで…更新忘れのクライアントソフトを狙った攻撃

- **統計1：クライアントの脆弱性を狙った攻撃傾向**
  - マルウェアダウンロードの原因となった脆弱性のうち58%はJava
  - 2011年上半期に発生した攻撃でJavaの脆弱性を狙ったものが最も多い

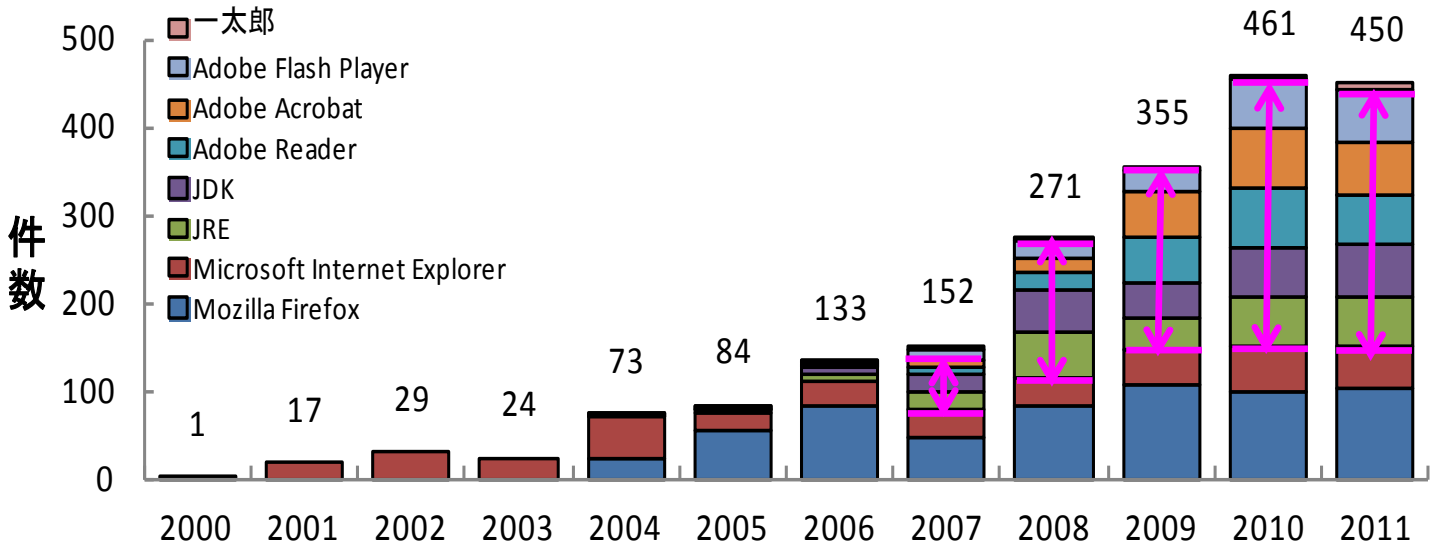
  ⇒クライアントソフトの既知の脆弱性が狙われている

- **統計2：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

【4位】今もどこかで…更新忘れのクライアントソフトを狙った攻撃

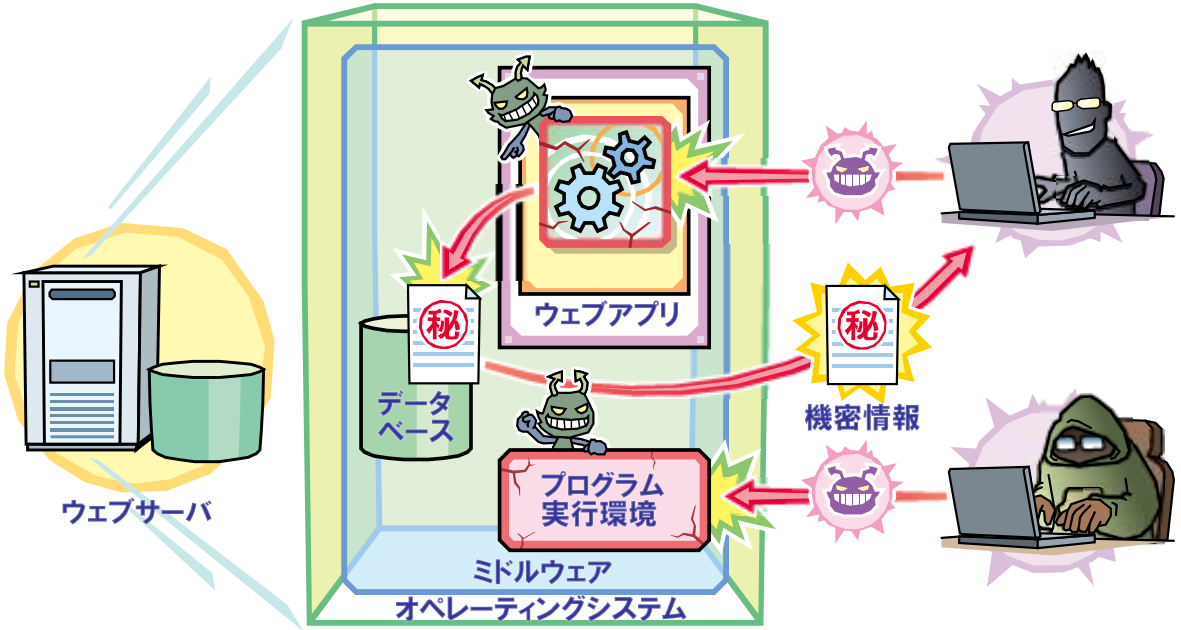
- 対策：修正プログラムの適用



（出典）IPA：脆弱性対策情報データベースJVN iPediaの登録状況 2011第4四半期

- Adobe Reader,JRE,Adobe Flash Playerにおいて発見される脆弱性が増えている
- 世の中の99%の攻撃は既知の脆弱性を悪用していると言われており修正プログラムを適用することが、PCを守る基本となる

【5位】止まらない！ ウェブサイトを狙った攻撃



- 脅威
  - ウェブサイトを狙った攻撃が継続して続いている
  - ミドルウェア、ウェブアプリケーションの脆弱性を狙った攻撃の発生
  - 内部情報などが漏えいしてしまう脅威

【5位】止まらない！ ウェブサイトを狙った攻撃

- 事例1：SQLインジェクション攻撃「LizaMoon」
  - 「大規模なSQLインジェクション攻撃」が22万6000以上のURLに対して仕掛けられた
  - 悪意のあるウェブサイトへ転送されるコードが仕組まれており、ユーザを偽ウイルス対策ソフトの配布サイトに転送する仕掛けになっていた
- 事例2：OSS「osCommerce」を狙った攻撃
  - 「osCommerce」を利用したオンラインショッピングサイトに対する大規模なIFRAMEインジェクション攻撃の発生
  - 日本国内を含む90,000以上のウェブサイトの感染が確認

【5位】止まらない！ ウェブサイトを狙った攻撃

- **対策1：脆弱性を作りこまない**
  - IPAで公開している「安全なウェブサイトの作り方」や「セキュア・プログラミング講座」を参考に、ウェブサイトの安全向上に努めることが重要
    - 「安全なウェブサイトの作り方」：http://www.ipa.go.jp/security/vuln/websecurity.html
    - 「セキュアプログラミング」：http://www.ipa.go.jp/security/awareness/vendor/programming
- **対策2：定期的な脆弱性診断**
  - 脆弱性情報は、日々発見されている為、定期的な脆弱性診断が重要
- **対策3：ソフトウェアアップデート**
  - OS、ミドルウェア、アプリケーションなど、組込んでいるソフトウェアをアップデートし、脆弱性の無い状態にしておくことが重要

【6位】続々発覚、スマートフォンやタブレットを狙った攻撃

- **脅威**
  - スマートフォンは、**パソコンに携帯機能が付加したもの**と考える必要あり
  - 「盗難・紛失」「ウイルス・不正なアプリケーション」「フィッシング・詐欺」などPCと同様の脅威が広がってきている
  - 信頼できないアプリケーションをインストールすることで、利用者情報の窃取や詐欺等の被害に遭う危険性

【6位】続々発覚、スマートフォンやタブレットを狙った攻撃

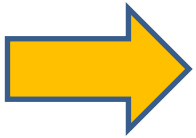
- **統計1：スマートフォンの脆弱性を悪用したウイルス数の増加**
  - 「Android Market」の**厳格な審査がない点が**、ウイルス増加の要因と言われている
  - アプリケーション配布サイトを使ってウイルスを展開する手法が定着

- **事例1：ワンクリック請求サイト**
  - PCサイト同様に、クリックしただけで料金を請求されるワンクリック請求サイトも確認されている

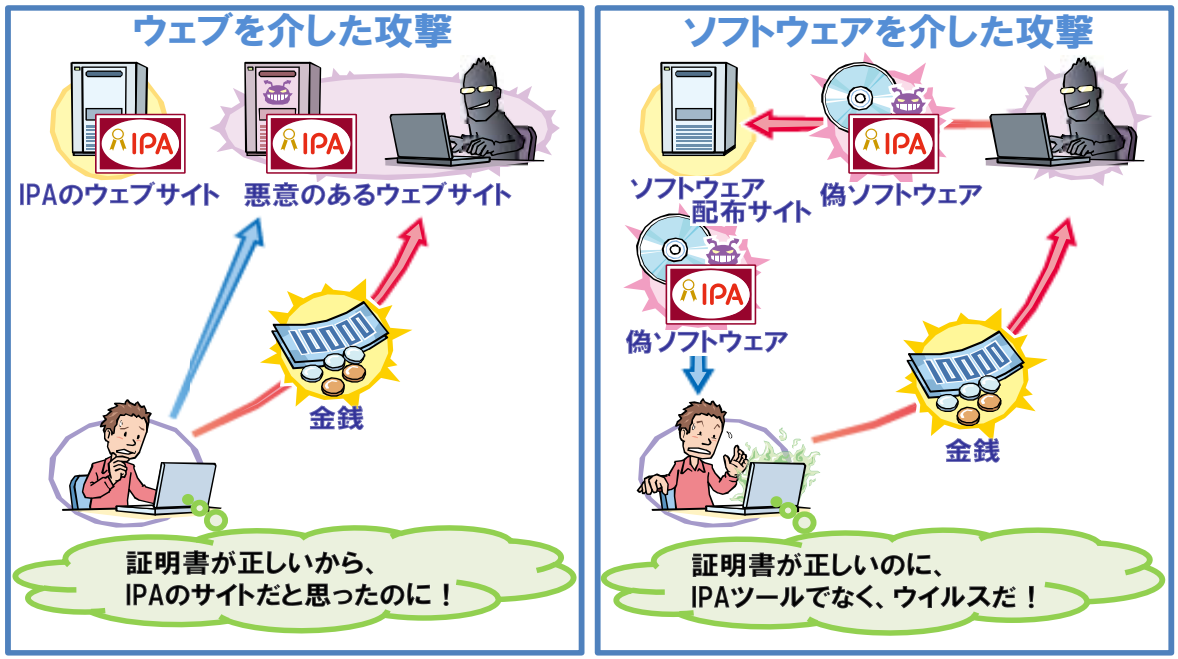
- **事例2：信頼できないアプリケーションによる被害事例**
  - 利用者が騙されて悪意あるアプリケーションをインストールしてしまうと、頻繁に請求画面が表示されたり、電話番号やメールアドレスが窃取される事例もあり

【6位】続々発覚、スマートフォンやタブレットを狙った攻撃

- 対策１：スマートフォンのアップデート実施
- 対策２：改造行為を行わない
- 対策３：信頼できる場所からのアプリケーションインストール
- 対策４：アプリケーションインストール前のアクセス許可確認
- 対策５：セキュリティソフトの導入
- 対策６：パソコンと同様の管理を実施

詳細はこちら  http://www.ipa.go.jp/security/txt/2011/08outline.html#5

【7位】大丈夫!?
電子証明書に思わぬ落し穴



- **脅威**
  - 電子証明書は、第三者である認証局を通してウェブサイトやソフトウェアの信憑性を証明するもの
  - 認証局や政府機関が攻撃を受け、不正に証明書が発行されたり、窃取される事件が発生
  - ソフトウェアやウェブサイトの信憑性が一時的に確認できなくなる事態に

【7位】大丈夫!?
電子証明書に思わぬ落し穴

- **事例1：電子証明書が不正に発行されてしまう**
  - 外部からの攻撃により、不正に電子証明書を発行される事件が発生
  - 攻撃により不正に発行された電子証明書は、500以上となる
  - ブラウザベンダは、当該認証局の証明書を失効する処置を取った

  ⇒偽の証明書を使用した罠サイトが構築されても、アプリケーションで正規サイトとして判断されてしまう

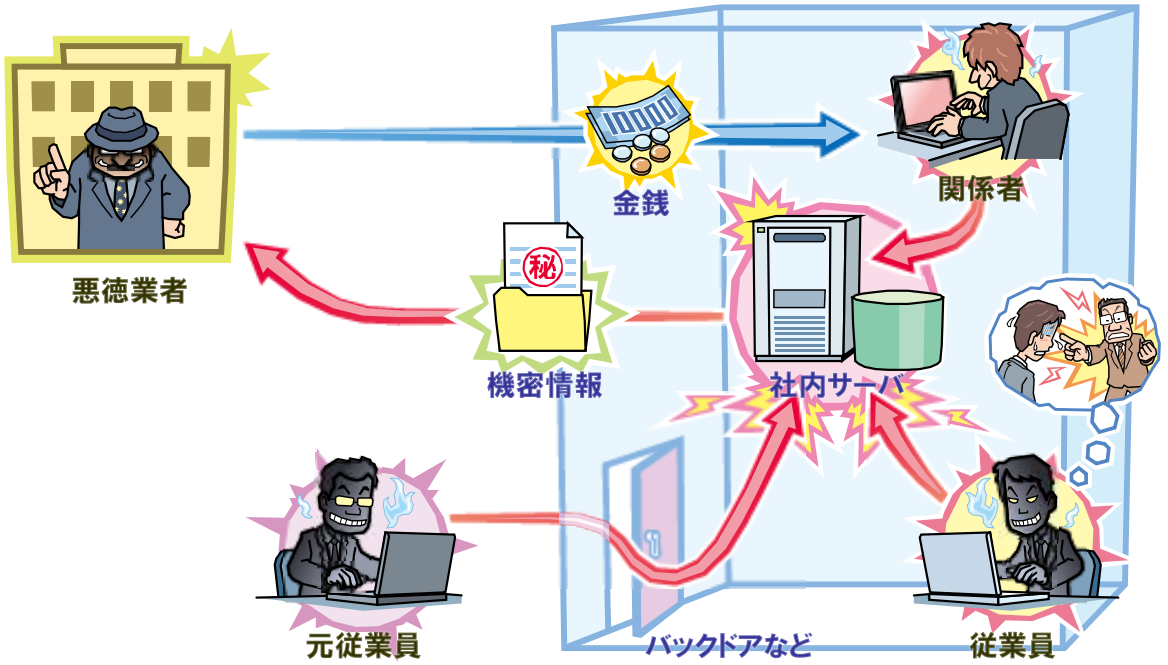
- **事例2：盗まれた証明書のマルウェアへの利用**
  - マレーシアの政府機関から盗まれた証明書を用いて署名されたマルウェアが発見された
  - Windowsでは署名のないアプリケーションをダウンロードしようとすると警告メッセージが表示されるが、正規の署名が施されている為、警告メッセージが表示されず、ユーザーが危険にさらされる恐れがある

【7位】大丈夫!?
電子証明書に思わぬ落し穴

- **認証局側の対策：**
  - 不正アクセス等のセキュリティ対策を実施し、証明書に関するシステムの厳重な管理
  - 不正に電子証明書が発行された事実が確認された場合は、関連する証明書の失効処理を即座に行う

- **利用者側の対策：**
  - ベンダが提供する情報をもとに、即座に修正プログラムを適用する
  - 問題のある認証局の証明書を無効にする対策の実施

【8位】身近に潜む魔の手・・・ あなたの職場は大丈夫？



- 脅威
  - 組織内部の人による故意の情報流出や業務妨害
  - 関係者による犯行が行われた場合、影響範囲が大きい
  - 内部情報を知っている者による、人為的な犯行である為、完全な対策が難しい

【8位】身近に潜む魔の手・・・ あなたの職場は大丈夫？

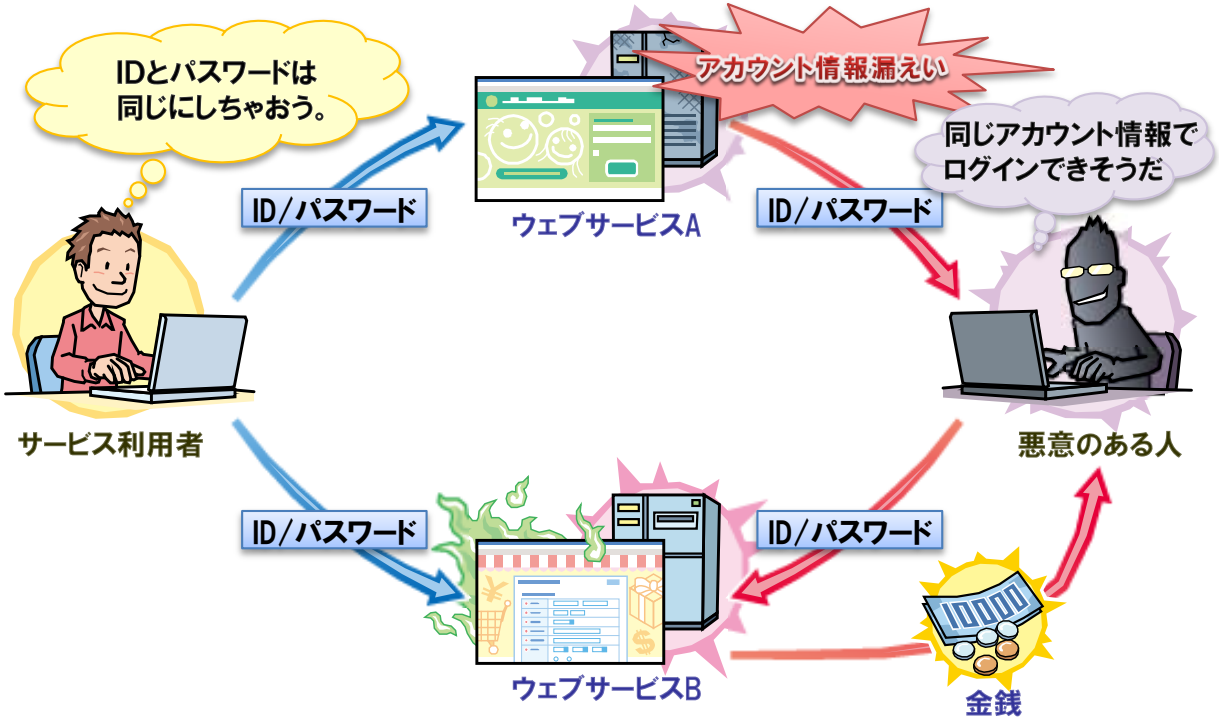
- **事例1：国内通信会社のデータ改ざんによる営業妨害**
  - 業務委託先の元社員により、基地局とネットワーク センターを結ぶ ATM 伝送装置の回線設定データが改ざんされる事件が発生
  - 携帯電話サービスが対象地域で利用しにくい状態になり、約7万2,700人の利用者が影響を受けた

- **事例2：ソーシャルゲームにおけるデータ改ざん**
  - ソーシャルゲームのサーバに元派遣社員が不正アクセスを行い、約130万人が利用するゲームのデータ改ざん
  - 元派遣社員は、任期満了で退社する際に、サーバ内に不正アクセス制限を解除できるプログラムを仕込んでいた
  - 約1,000万円の被害があったといわれている

【8位】身近に潜む魔の手・・・ あなたの職場は大丈夫？

- **対策１:「物理的対策」と「システム的対策」の実施**
  - 重要な情報が保存されている場所や作業場への入場を物理的に制限する
  - 重要システムへのアクセス制限の実施
- **対策２:職務権限の分離**
  - 作業実施者と承認者を分けることにより、不正をしづらくする環境構築
  - 承認されないと作業が行えない仕組みの導入
- **対策３:情報漏えい発生時の事後対応の計画**
  - 情報漏洩発生時に、適切な対応が行える体制や手順の準備
  - 問題発生時に、いかに早く通常業務に戻せるかが事後対応の鍵となる

【9位】危ない！アカウントの使いまわしが被害を拡大！



- 脅威
  - ID/PWを窃取するスパイウェアによる攻撃
  - 他のウェブサービスでもパスワードを使い回ししていることにより被害拡大
  - 8割弱の人が同じID/PWで複数のウェブサイトを利用している実態

【9位】危ない！アカウントの使いまわしが被害を拡大！

- **統計1：セキュリティの脅威に対する意識調査**
  - 8割弱の人が「各種インターネットサービスで用いるパスワードは、基本的に普段使うパスワードを使いまわしている」と回答
  - 適切なパスワードを設定していない、適切に管理されていないといったアカウント情報の管理不備の実態が明らかに

- **事例1：Facebookのログイン乗っ取り**
  - 1日当たり10億を超すFacebookへのログイン件数のうち、アカウント乗っ取りによるログインが0.06％を占めるという数字が公表された
  - 毎日60万件のアカウントが乗っ取られている計算

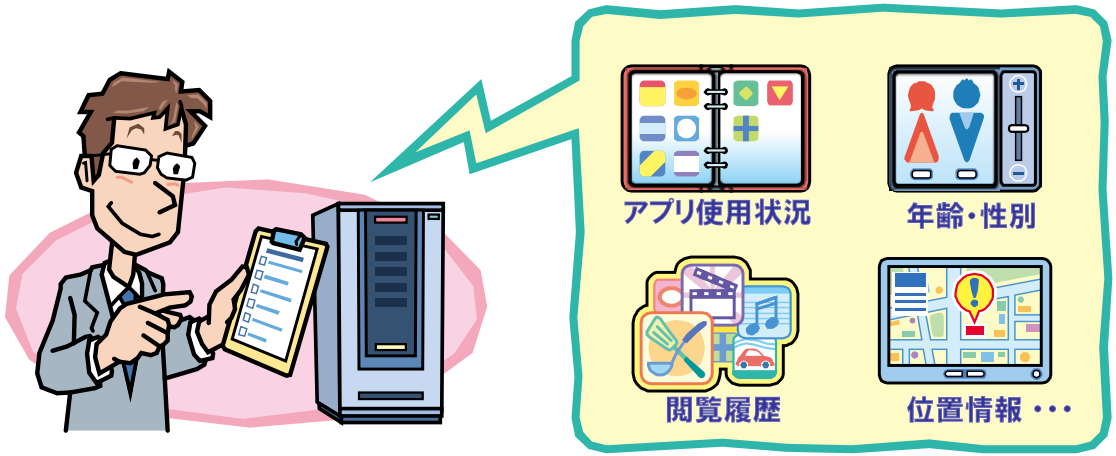
- **事例2：不正なサインインの試行**
  - 他社のサービスから漏えいした情報をもとに、サービスに不正にログインを試みた可能性がある事象

【9位】危ない！アカウントの使いまわしが被害を拡大！

- **ウェブサイト側の対策：**
  - パスワードを窃取されない為のセキュリティ対策の実施
  - 機密性の高い情報は、暗号化して保存しておく
- **利用者側の対策（PC側の対策）：**
  - ウイルス対策ソフトの導入と最新の定義ファイルの更新
  - OSやアプリケーションの脆弱性の解消

  ⇒スパイウェア等に感染しない為の対応の実施
- **利用者側の対策（運用面）：**
  - 金銭に絡むウェブサービスで利用するアカウント情報は、他のウェブサービスと同じにしない
  - 安易なパスワードの設定や紙にログインIDとパスワードを記述しない

【10位】利用者情報の不適切な取扱いによる信用失墜



☑ 必要以上に利用者情報を収集してませんか？
☐ 利用者にきちんと使用目的を伝えていますか？

- **脅威**
  - スマートフォンが保持しているプライバシー情報がウェブサイトに送出される
    - 位置情報、性別、趣向などの個人に紐づく情報
  - ウェブサイト運営者が無断、又は適切な説明無しに収集すると、プライバシー侵害の恐れがある

【10位】利用者情報の不適切な取扱いによる信用失墜

- **事例1：広告配信用プログラムのサービス終了**
  - 広告配信用プログラムは、端末にインストールしているアプリケーションの情報や使用状況を取得し、データを解析していた
  - 利用者への説明不足や許諾方法が不適切であると問題になった
  - 社会的な信用失墜に繋がり、サービスを停止するに至った

- **事例2：ゲームの利用情報をウェブサイトで無断公開**
  - 家庭用ゲーム機でプレイしたゲームなどの情報をプレイヤーの同意を得ずにウェブサイトで公開していた
  - 情報公開について利用規約に明示し、情報の開示可否を選択できる仕組みが導入された

【10位】利用者情報の不適切な取扱いによる信用失墜

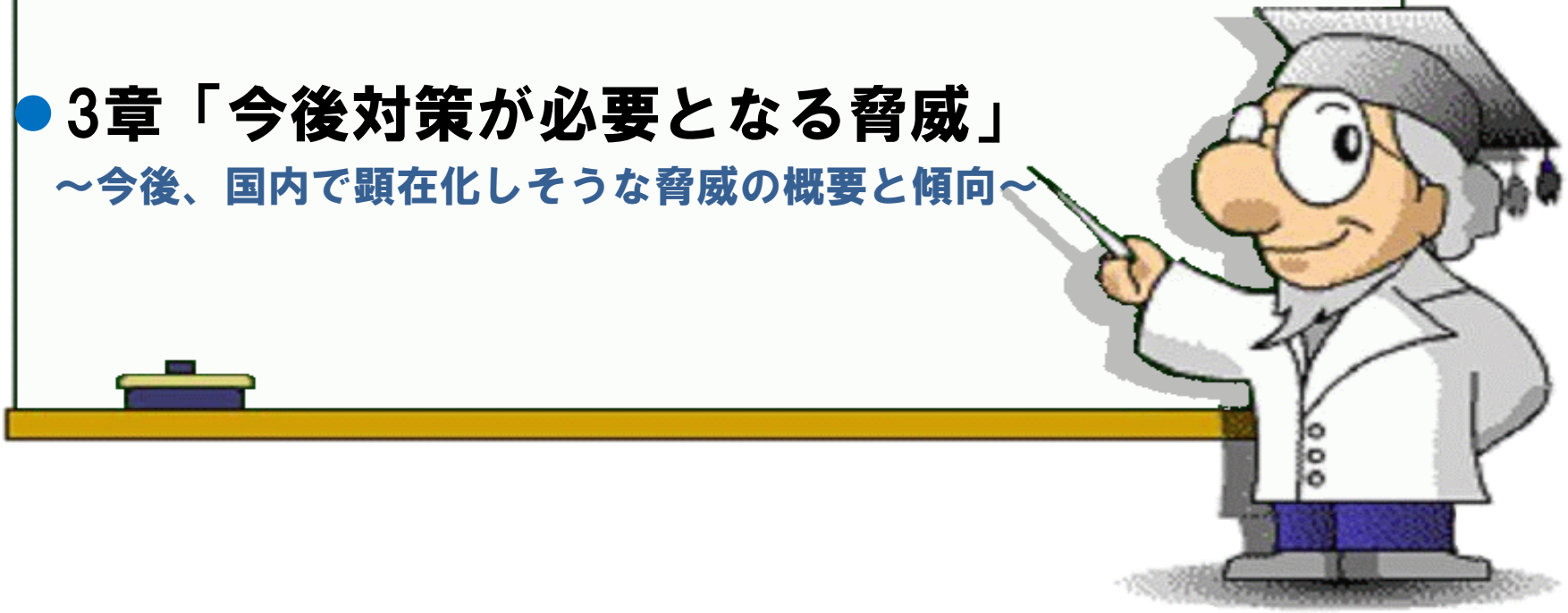
- **対策1：データ取扱い方針の検討**
  - サービス提供者は、サービス設計段階において、必要な利用者情報を洗い出し、不要な情報は取り扱わないようにする
  - サービスに必要な利用者情報について、使用目的を十分に検討して取扱うことが求められている

- **対策2：利用者への明示**
  - サービス提供に必須となる情報は、情報の取扱いについて利用者に明示して、同意を得る
  - 同意を得た利用者からのみ情報を収集するようにし、利用者の意思により、収集を停止できる手段を用意する

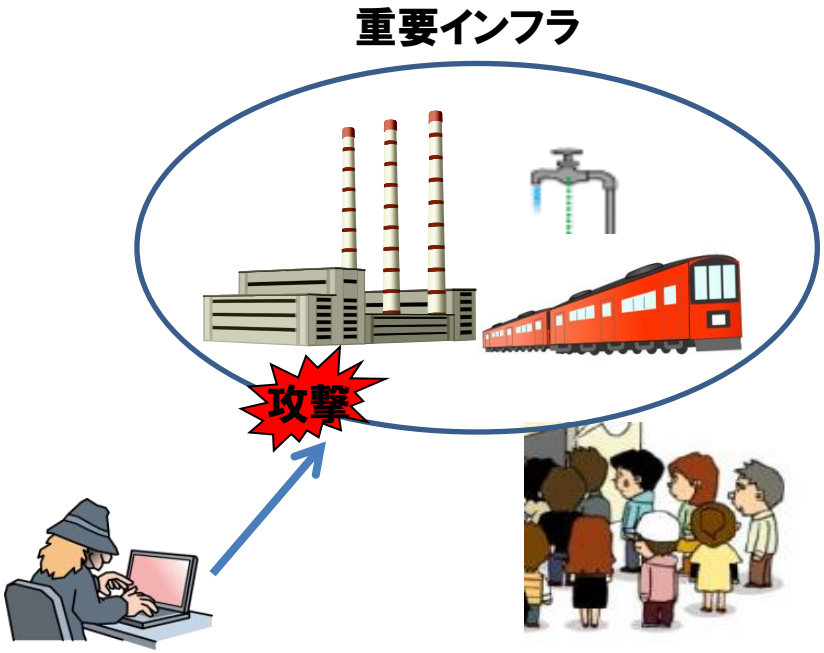
不要な情報は収集せず、必要な情報は利用者に明示した上で収集することが運営者に求められる

目次

- 1章「情報セキュリティを取巻く環境の変化」
  ～攻撃手法、システム環境、攻撃者像、被害時のインパクトの変化について ～
- 2章「2012年版 10大脅威」
  ～セキュリティ専門家が選ぶ2011年に起こった10の脅威について～
- **3章「今後対策が必要となる脅威」**
  ～今後、国内で顕在化しそうな脅威の概要と傾向～



社会基盤である重要インフラを狙った攻撃



- 背景
  - 電力、ガス、水道、交通などの社会インフラについても、情報システム同様に複数のコンピュータで構成されている
  - インターネットに繋がっていないことや、事業者ごとに固有の仕様であるため、サイバー攻撃の影響は受けづらいと考えられていた

しかし・・・

社会基盤である重要インフラを狙った攻撃

- **取巻く状況が変化してきた**
  - 近年では利便性やコスト面のメリットから、VPN (Virtual Private Network) を利用したリモート監視や制御用端末にWindowsやUNIX系OSが採用されるようになっている
  - 情報系システム同様のシステム環境に近づきつつある

  ⇒情報系システム同様にサイバー攻撃の現実化
- **想定される脅威**
  - 重要インフラが攻撃されると・・・。
    - 交通システムの場合：電車の運行停止やダイヤの乱れなど、交通機関が麻痺
    - 水道システムの場合：水の供給が停止してしまい、我々の生命活動にまで影響を

重要インフラへの攻撃は、社会の混乱を狙ったものであるため、攻撃が発生した際に社会への影響が大きい

社会基盤である重要インフラを狙った攻撃

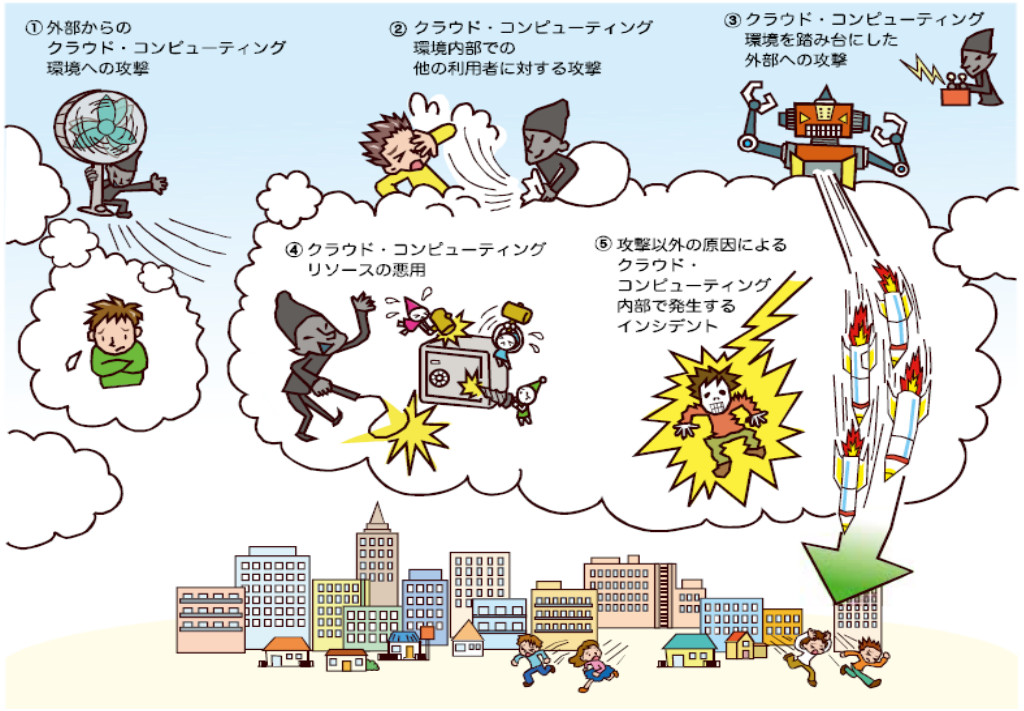
IPA

- **海外での事例**
  - 鉄道ダイヤ乱れ（2003年米国）
    - 米国東部の鉄道会社の信号管理システムがウイルスに感染
    - 周辺の3路線で列車の運行停止やダイヤ乱れが発生
  - 原子力システムへのウイルス感染（2003年米国）
    - 米国の原子力発電所でVPN接続を介して制御システムにウイルスが侵入
    - 5時間に渡ってシステムが停止してしまった

- **重要システムにおけるセキュリティ対策の難しさ**
  - 情報系システムとは異なり、「システムを止めない事」が重要視される傾向
  - 我々の生活に密接に絡んでいるため、24時間365日稼働することが求められる
  - 情報システムと異なり、パッチ適用のためにシステムを停止することが難しい。如何にシステムを止めずにセキュリティを確保するかが課題

クラウド利用における脅威

-



- **背景**
  - 2011年の国内クラウド・コンピューティング（以降クラウド）の市場規模は、662億円規模となる見込み
  - 2015年には、2010年比5.6倍の2,550億円になると予測

⇒新しいサービスの登場に伴い新たな脅威が発生

クラウド利用における脅威

- 想定される脅威
  - 外部からクラウド環境への攻撃
    - クラウド環境が外部からの攻撃に晒される脅威
  - クラウド環境内部から他のクラウド利用者へ攻撃
    - クラウド環境内に攻撃者が潜んでおり、他のクラウド利用者が攻撃される脅威
    - 仮想化技術の脆弱性等を悪用し、クラウド環境を通して攻撃されることが想定される
  - クラウドを踏み台とした攻撃
    - クラウドを踏み台にして、第三者にDoS等の攻撃が仕掛けられる脅威
  - コンピューティングパワーの悪用（パスワード解析や暗号解析等）
    - クラウド環境が攻撃のためのリソースとして悪用される脅威
  - 攻撃以外の原因（停電、システム不具合等）
    - 停電、システム不具合等のクラウド事業者側のトラブルにより、クラウドの利用者がサービスを利用できなくなる懸念がある
    - 国内のクラウド事例の大半を占める事象

企業におけるスマートデバイスの管理

- 背景
  - スマートデバイスを導入している国内企業は、全体の16%程度
  - 全体の約1/4の企業がスマートデバイスを「導入している」「導入を予定している」と回答
  - 1年前の調査に比べて、スマートフォン導入企業は約1.6倍、タブレットPC導入企業は約2.5倍の拡大している

企業におけるスマートデバイスの管理

- スマートデバイスが企業に導入されることで、
  - スマートデバイスに企業の業務関連の情報が蓄積される
  - スマートデバイスは携帯性に優れているため、外出先での紛失や盗難のリスクが高まる

  ⇒情報漏洩による企業への影響が懸念

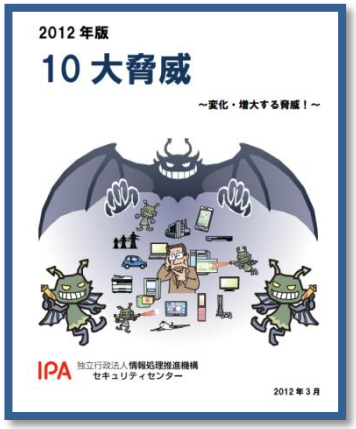
- BYOD (Bring Your Own Device) への関心の高まり
  - 米国を中心に個人のスマートデバイスを持ち込ませる気運の高まり
  - 企業で個人所有のデバイスをどこまで監視・制限すべきなのか課題あり

企業におけるスマートデバイスの管理

- 対策
  - スマートデバイス利用ルールの制定
  - スマートデバイスからアクセス可能な情報の範囲の決定
  - スマートデバイスに保存可能な情報の範囲、紛失・盗難時の対応ポリシーの制定
  - （MDM：Mobile Device Management）によって、スマートデバイスに搭載されているOSのアップデートの徹底やインストールできるアプリの制限などを企業側で強制的に管理する

おわりに

情報セキュリティを取り巻く状況の理解やセキュリティ対策の参考に、本書をご活用ください。



http://www.ipa.go.jp/security/vuln/10threats2012.html
http://www.ipa.go.jp/security/vuln/documents/10threats2012.pdf

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