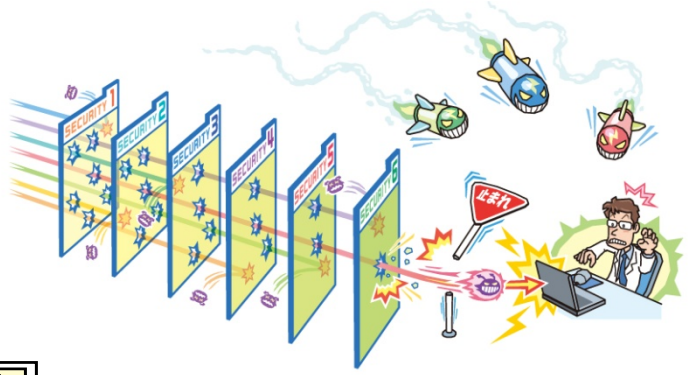
IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

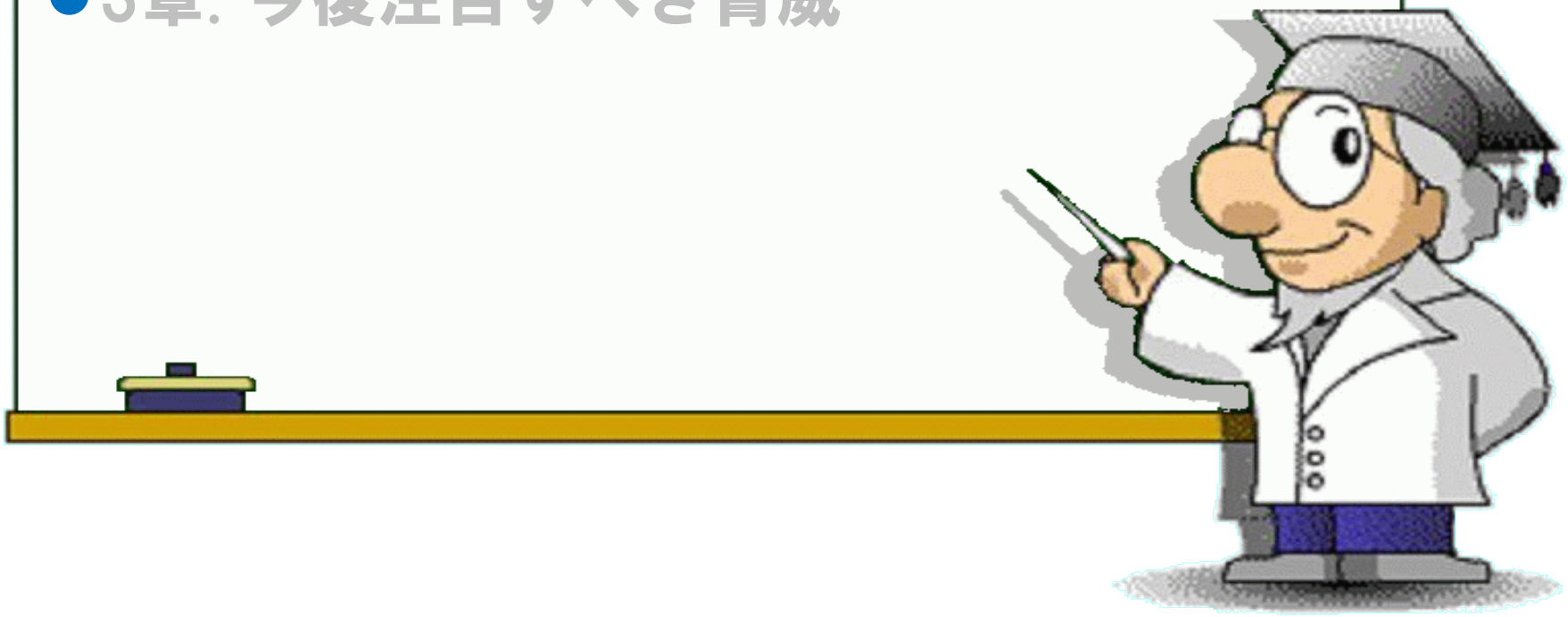
「2013年版 10大脅威」
～身近に忍び寄る脅威～



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
2013年3月

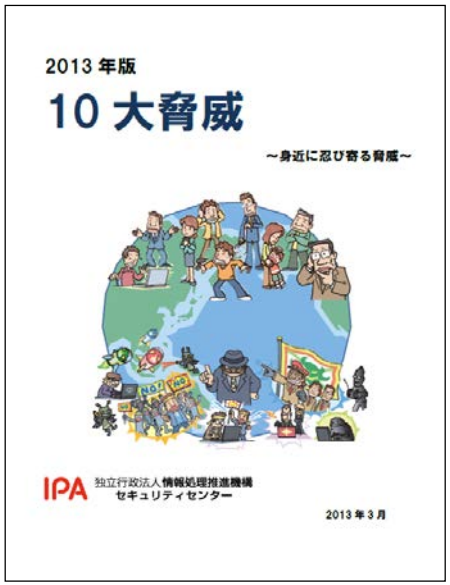
目次

- 10大脅威について
- 1章. 情報セキュリティの変遷
- 2章. 2013年版10大脅威
- 3章. 今後注目すべき脅威



2013年版 10大脅威『身近に忍び寄る脅威』

http://www.ipa.go.jp/security/vuln/documents/10threats2013.pdf

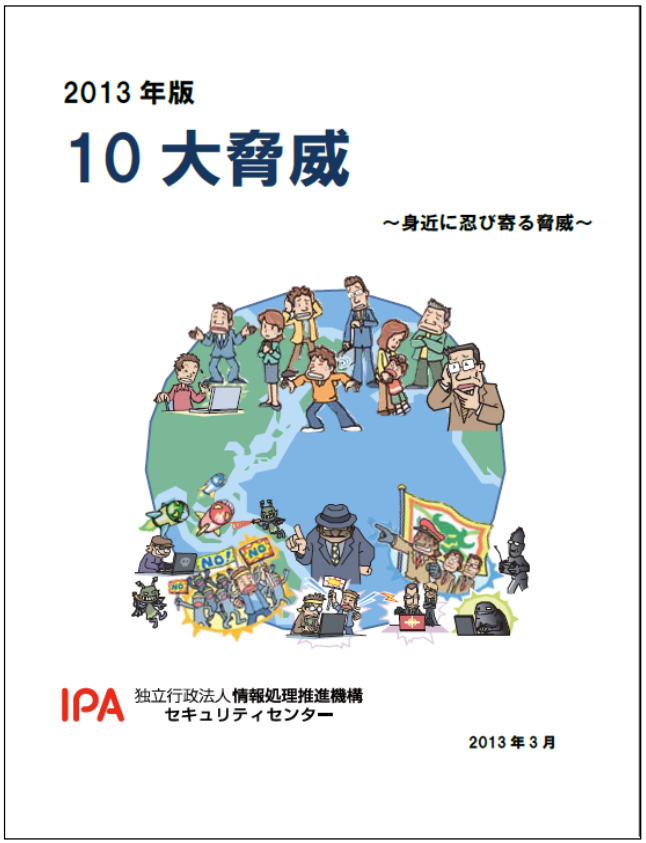


- 10大脅威とは？
  - IPAで2004年から毎年発行している資料
  - 「10大脅威執筆者会」メンバー117名の知見を集めて編集
  - 投票により、情報システムを取巻く脅威を順位付け

2013年版 10大脅威『身近に忍び寄る脅威』

http://www.ipa.go.jp/security/vuln/documents/10threats2013.pdf

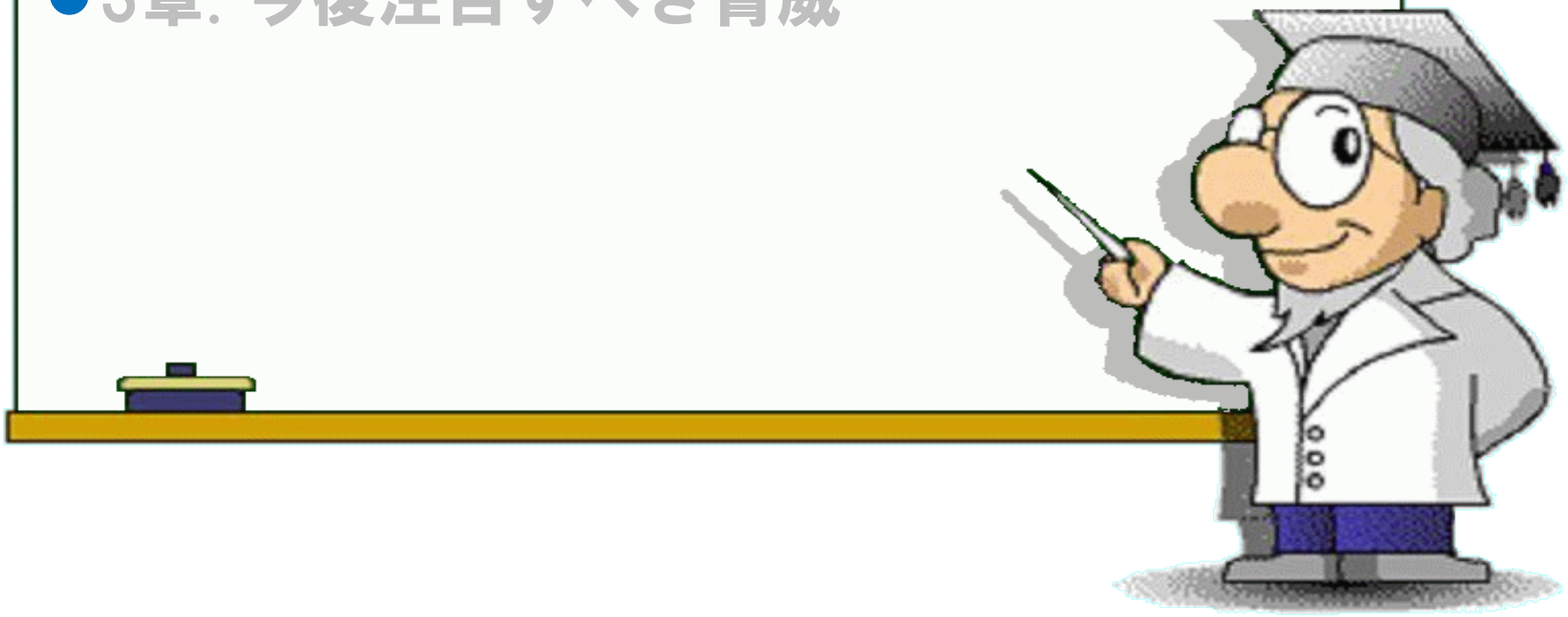
章構成



- 1章.情報セキュリティの変遷
  - '01 ～ '12年までのセキュリティの変遷
  - IT環境や攻撃意図の変化を解説
- 2章.2013年版 10大脅威
  - 2012年の事例をベースに10の脅威を選出
  - 10の脅威の概要と対策について解説
- 3章.今後注目すべき脅威
  - クラウドコンピューティングの課題
  - 重要インフラを狙った攻撃
  - 既存対策をすり抜ける攻撃の存在

目次

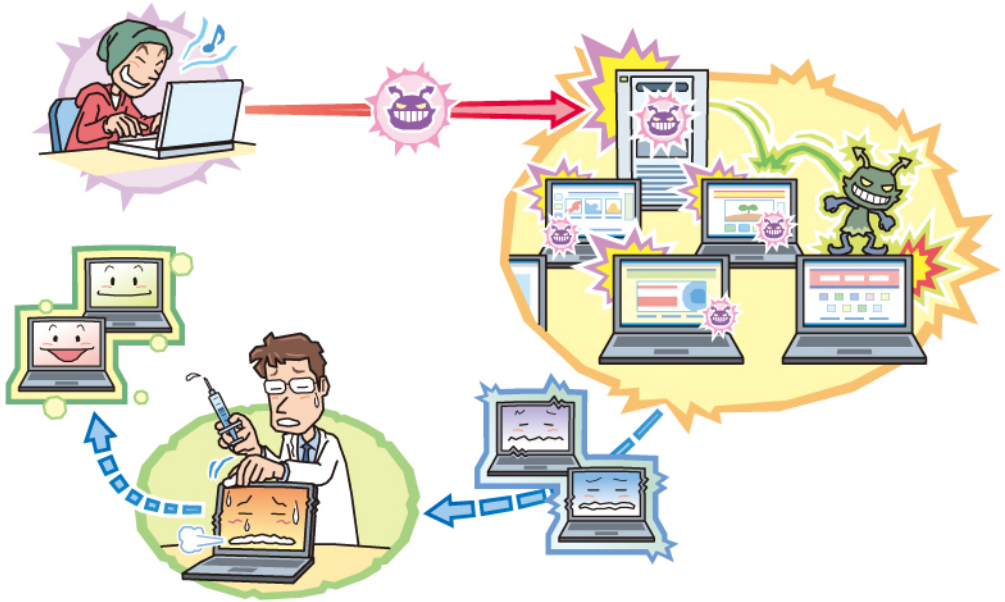
- 10大脅威について
- **1章. 情報セキュリティの変遷**
- 2章. 2013年版10大脅威
- 3章. 今後注目すべき脅威



情報セキュリティの変遷

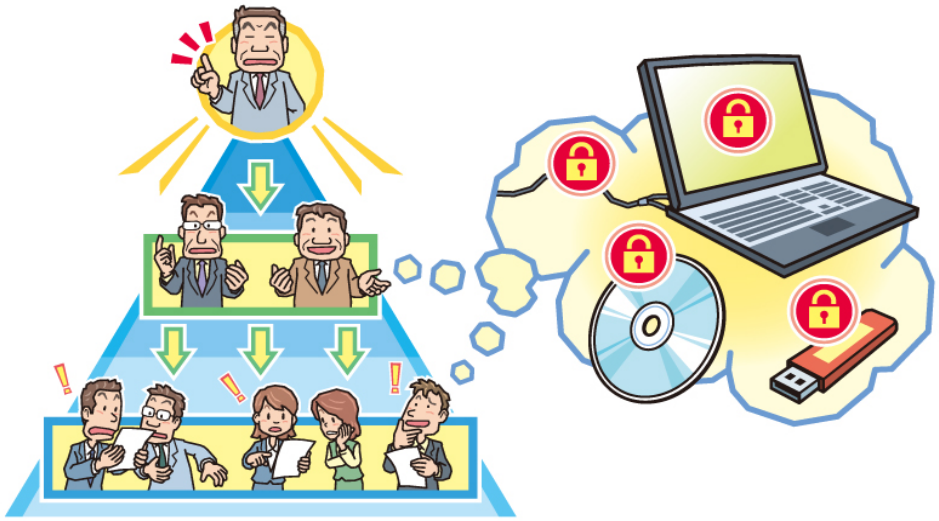
	2001～2003年	2004年～2008年	2009年～2012年
時代背景	ネットワークウイルスの全盛	内部脅威・コンプライアンス対応	脅威のグローバル化
IT環境	コミュニケーション手段の確立	e-コマースの加速	経済・生活基盤に成長
セキュリティの意味合い	サーバーやPCの保護	企業・組織の社会的責任	危機管理・国家安全保障
攻撃の意図	・いたずら目的	・いたずら目的 ・金銭目的	・いたずら目的 ・金銭目的 ・抗議目的 ・諜報目的
攻撃傾向	ネットワーク上の攻撃	人を騙す攻撃の登場	攻撃対象の拡大
攻撃対象	PC、サーバー	人、情報サービス	・スマートデバイス ・重要インフラ
対策の方向	セキュリティ製品中心	マネジメント体制の確立	・官民・国際連携の強化 ・セキュリティ人材育成強化
主なセキュリティ事件	・Nimda流行（2001） ・Code Red流行（2001） ・SQL Slammer 流行（2003）	・P2Pソフトによる情報漏えい（2005～） ・不正アクセスによる情報流出（2005～） ・スパイウェアによる不正送金（2005～）	・米韓にDDoS攻撃（2009） ・イランを狙ったStuxnet（2010） ・政府機関を狙ったサイバー攻撃（2011） ・金融機関を狙った攻撃（2012）

ネットワークウイルスの全盛期（2001～2003）
～ブロードバンド時代の到来と情報セキュリティの本格始動～



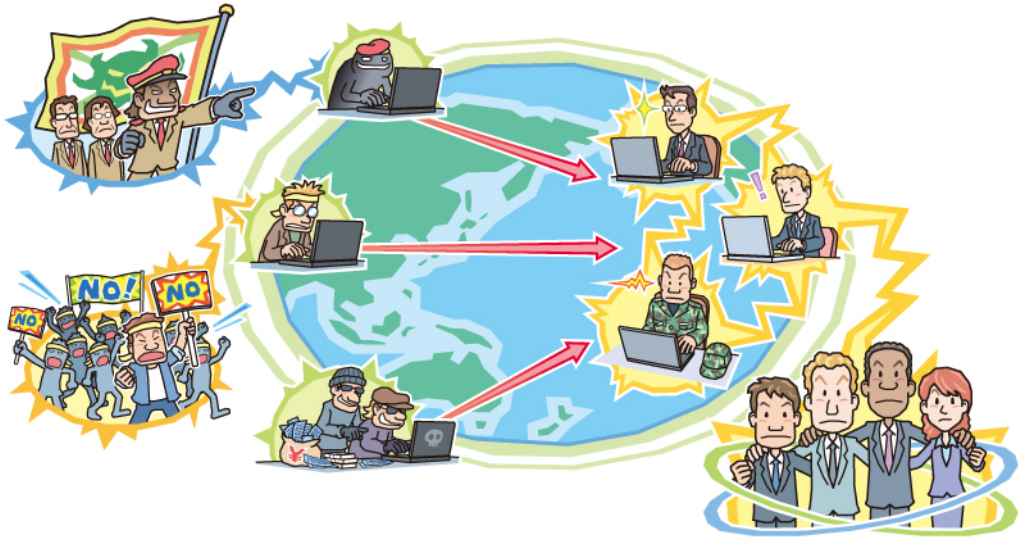
- **時代背景とセキュリティ**
  - **ブロードバンド時代の幕開け（2001）**
    - コミュニケーションツールとして、インターネットの定着
  - **インターネットを介した攻撃の広がり**
    - Nimda、CodeRed など拡散型のネットワークウイルスにより、ネットワークの帯域が圧迫
  - **セキュリティ製品中心の対策**
    - FW（ファイアウォール）、IDS（不正検知システム）などのセキュリティ製品の導入

内部脅威・コンプライアンス対応（2004～2008）
～組織・企業におけるセキュリティマネジメントの確立～



- **時代背景とセキュリティ**
  - **セキュリティ制度・法制化の流れ**
    - 個人情報保護法全面施行（2005）、日本版SOX法施行（2008）
    - 組織・企業におけるマネジメント体制、コンプライアンス強化の流れが加速
  - **相次ぐ情報漏えい事故**
    - 鞄、PCの紛失、Winny、ShareなどのP2Pソフトを介した情報漏えいが発生
    - 組織内で情報持出しのルール化に加え、情報漏えい対策ソフトが広く出回る

脅威のグローバル化（2009～2012）
～経済・生活基盤に成長したインターネット～



- インターネットへの依存度の増大
  - 経済活動・社会活動の場に成長したインターネット
  - 攻撃を受けた際のインパクト・ダメージも増大
- サイバー空間・サイバー攻撃
  - 国際公共財として「サイバー空間」の概念が一般化
  - 安全保障、経済権益確保の視点でサイバー攻撃が議論されだした

脅威のグローバル化（2009～2012）
～政府主導によるサイバー空間の統制～

- 国家を巻き込んだ大規模な攻撃
  - 米国・韓国を標的とした大規模なDDoS攻撃の発生（2009年）
  - イランの原子力施設を狙ったウイルス「Stuxnet」の発見（2010年）
    - イランの核開発を阻止しようとした特殊工作がサイバー空間を使って行われた
- 政府の関与
  - 米国防総省は「サイバー空間」を陸・海・空・宇宙空間に次ぐ「第五の戦場」であると定義
  - 政府のインターネットの閲覧を制限の動き
    - 「アラブの春」では、ソーシャルメディアを通じて、政府への抗議メッセージが拡散し、反政府運動の高まりや大規模なデモに繋がったと言われている
    - 複数の国で、政府によるインターネット閲覧を制限する動きがみられる

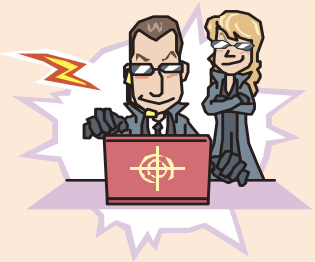
サイバー攻撃が国際情勢や安全保障に関わる問題として扱われ、関係分野が拡大している

脅威のグローバル化（2009～2012）
～攻撃意図の変化～

- 新たな攻撃意図の顕在化
  - 政治・文化的に対立する組織へ攻撃を行うハクティビスト
  - 諜報活動を目的とした攻撃の広がり

顕在化した攻撃意図

抗議・報復目的



諜報・スパイ目的

従来からの攻撃意図

金銭目的

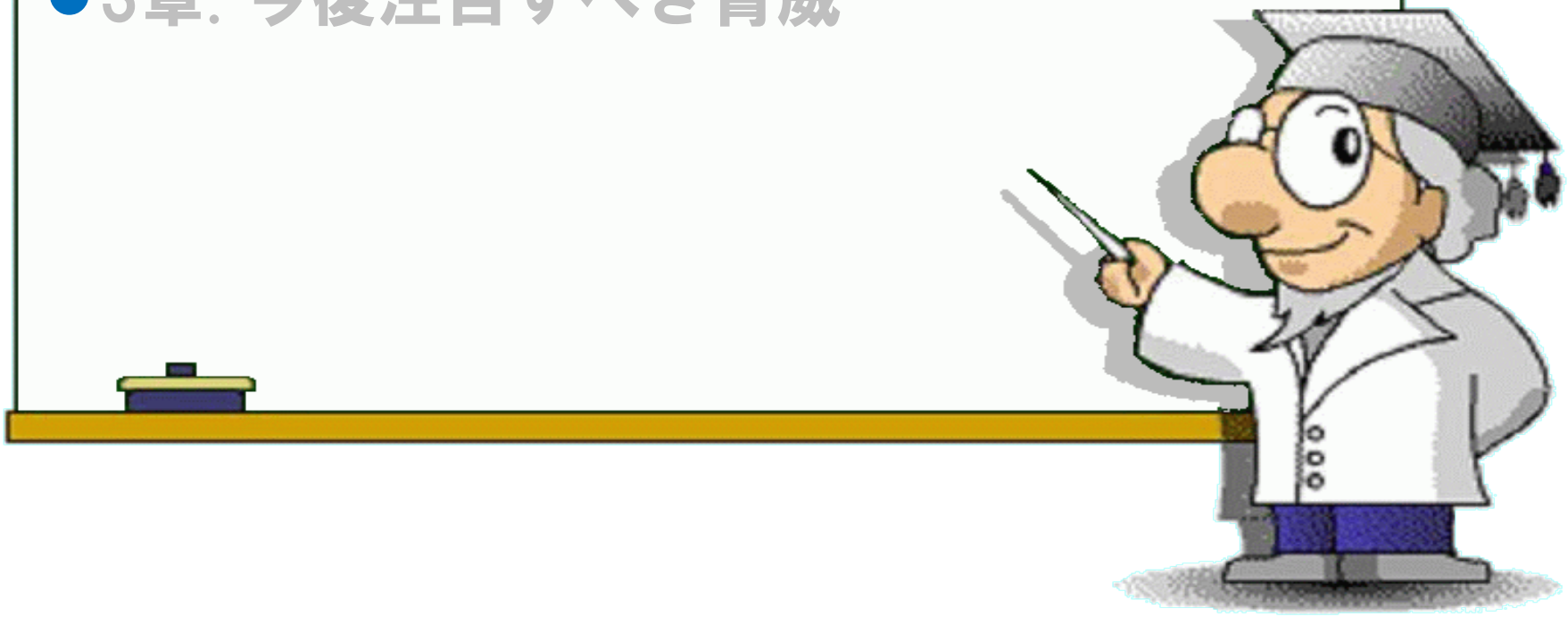
いたずら目的

脅威のグローバル化（2009～2012）
～官民連携・法制度の動き～

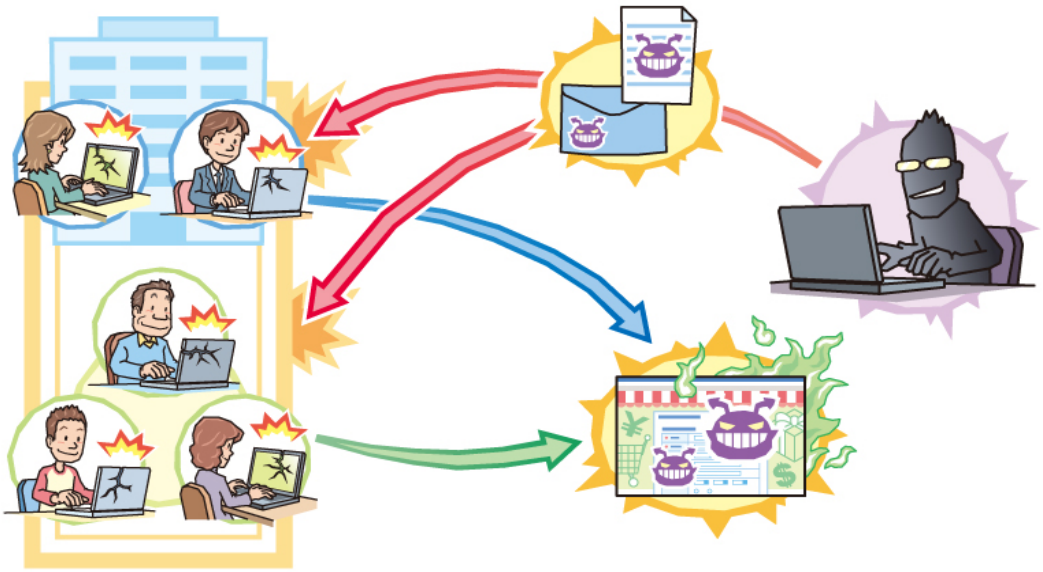
- グローバル、官民連携した対策
  - サイバー情報共有イニシアティブ（J-CSIP）の発足（2011年）
  - 高度解析協議会の発足（2012年）
- 人材育成の動き
  - 攻撃者に対抗できるスキルを持ったエンジニアの育成
  - 「CTFチャレンジジャパン大会」が政府主導で開催
- 国内の法制度の状況
  - 刑法改正（ウィルス作成罪施行）
    - 正当な理由なしで、ウイルスを「作成」「提供」する行為が犯罪として罰則化された
  - 不正競争防止法　刑事罰の強化
    - 不正に利益を得たり、保有者に損害を加えたりする目的で、企業の営業秘密を持ち出す行為が犯罪として罰則化された

目次

- 10大脅威について
- 1章. 情報セキュリティの変遷
- **2章. 2013年版10大脅威**
- 3章. 今後注目すべき脅威



【1位】クライアントソフトの脆弱性を突いた攻撃
～更新忘れのクライアントソフトが狙われている～



- **概要**
  - Adobe Reader，Adobe Flash Player，Oracle Java（JRE）を悪用した攻撃が攻撃の常套手段化している
  - 脆弱性を放置しておくことで、ウイルス感染のリスクが高まる
  - クライアントソフトを最新に保つことが、セキュリティ対策の基本

【1位】クライアントソフトの脆弱性を突いた攻撃
～ユーザの対策意識を高めることが重要～

- 攻撃に悪用される背景
  - 企業や個人で利用を控えるのは難しいソフトウェアがターゲットになる
  - ファイル・ウェブサイトや閲覧等の操作で、ウイルスに感染
  - PCを利用する上で必須操作である為、攻撃の成功率が高くなる



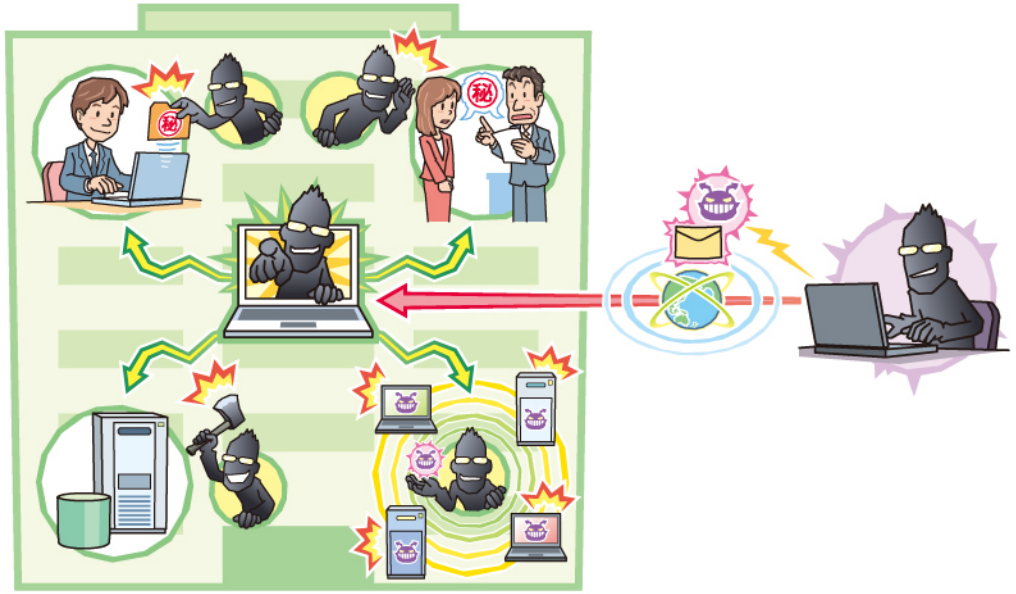
- 2012年の事例／統計
  - 99.8%が既知の脆弱性を悪用しているとのレポート（日本IBM）
  - Adobe Readerの更新は、45%のユーザーしか対応していない状況
  - MACを狙ったFlashBackにより、国内3,800台のPCがウイルス感染に

既知の脆弱性が悪用されている一方で、ユーザーの対策意識は高くない

【1位】クライアントソフトの脆弱性を突いた攻撃
～脆弱性対策に加え、被害の出にくいシステム設計を～

- **対策一覧**
  - **クライアントソフトの脆弱性対策（ユーザーの対策）**
    - タイムリーにソフトウェアの更新を行うことを心掛ける
    - 自動更新を有効にしておくことで、ユーザーが意識せずともセキュリティ対策が可能
  - **システム設計（管理者の対策）**
    - ゼロデイ攻撃、バージョンアップが出来ない場合も想定しておく必要あり
    - 被害が出にくいネットワーク構成を検討することが有効

【2位】標的型諜報攻撃の脅威
～知らない間にスパイがあなたの情報を盗んでいる～



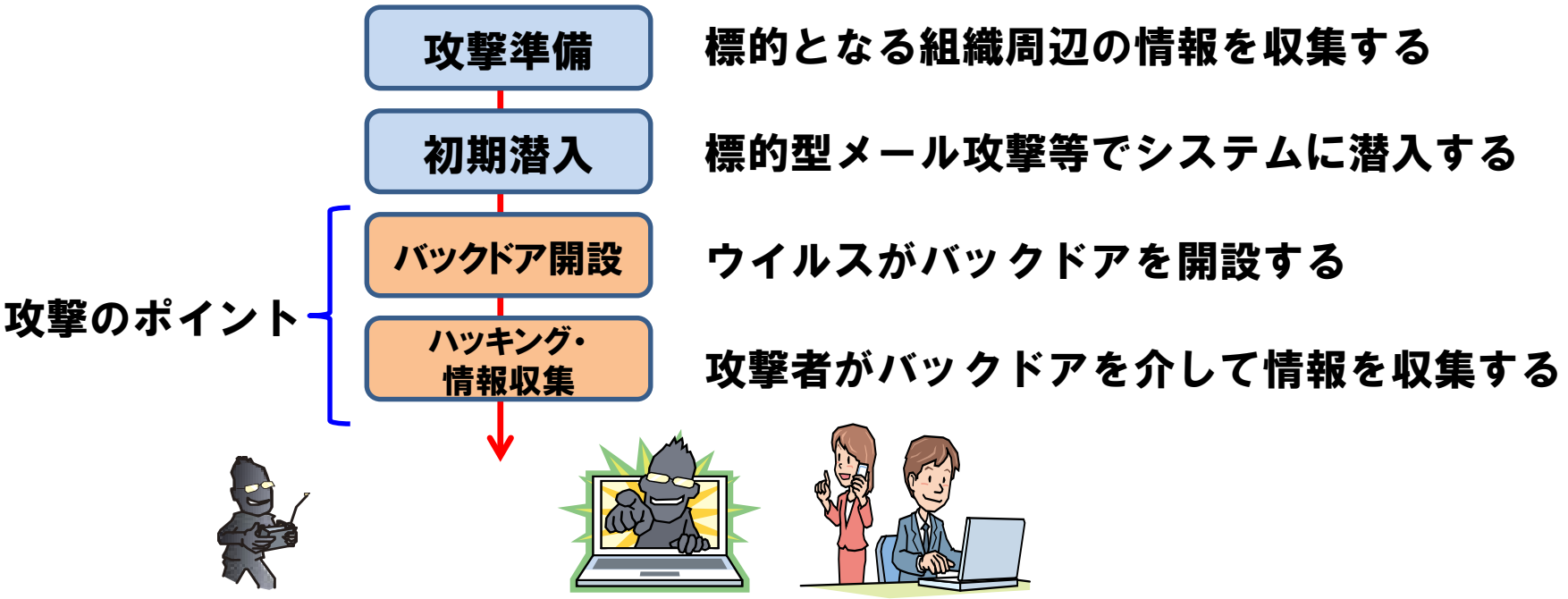
- **概要**
  - サイバー空間上で、諜報活動が行われている
  - 画面キャプチャー、職場での会話、PCの操作情報などが抜き取られる
  - 我が国の政策会議に取上げられるなど、国益にまで影響する問題

【2位】標的型諜報攻撃の脅威
～攻撃者によるウイルスを使ったリモートハッキング～

- **攻撃の手口**

他の攻撃との大きな違いは、攻撃の「**戦術性**」にある

- 攻撃の流れ



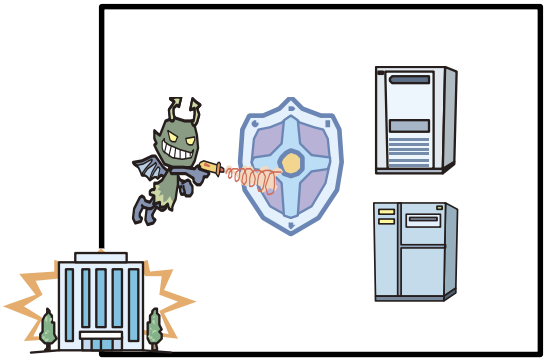
攻撃者自身が仮想的にシステム内部に潜入して、ハッキングを行っているイメージに近い

【2位】標的型諜報攻撃の脅威

～外部からだけではなく、内部からの攻撃を想定した対策を～

- **攻撃事例**
  - 農林水産省を狙った攻撃
    情報流出の可能性
  - JAXAへの攻撃
    国産ロケット「イプシロン」関する情報が盗まれた可能性

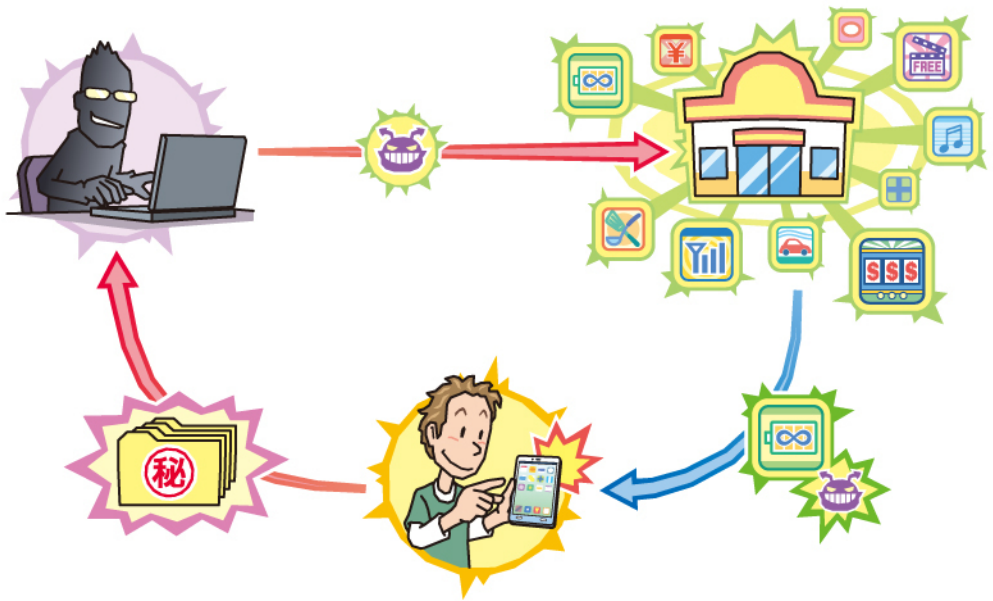
- **対策一覧**
  - 脆弱性対策
  - システム設計
  - システム監視
  - アカウント/権限管理



ウイルスがシステム内部潜入後に行われる、内部からの攻撃を想定した対策を、講じることが重要

【3位】スマートデバイスを狙った悪意あるアプリの横行

～あなたの個人情報が狙われている～



- **概要**
  - 悪意のあるアプリによりスマートデバイス内の個人情報が窃取される
  - 被害は自分だけでは留まらず、電話帳に登録された他人にも及ぶ
  - 信頼できるアプリかどうか判断した上で、利用することが重要

【3位】スマートデバイスを狙った悪意あるアプリの横行

～悪意のあるアプリが情報を根こそぎ持って行く～

- **攻撃に悪用される背景**
  - 個人や企業において、スマートデバイスが加速的に普及している
  - スマートデバイスは、高機能/多機能でありPCに近い存在
  - 個人情報が多く保存されているスマートデバイスは攻撃者にとって魅力的

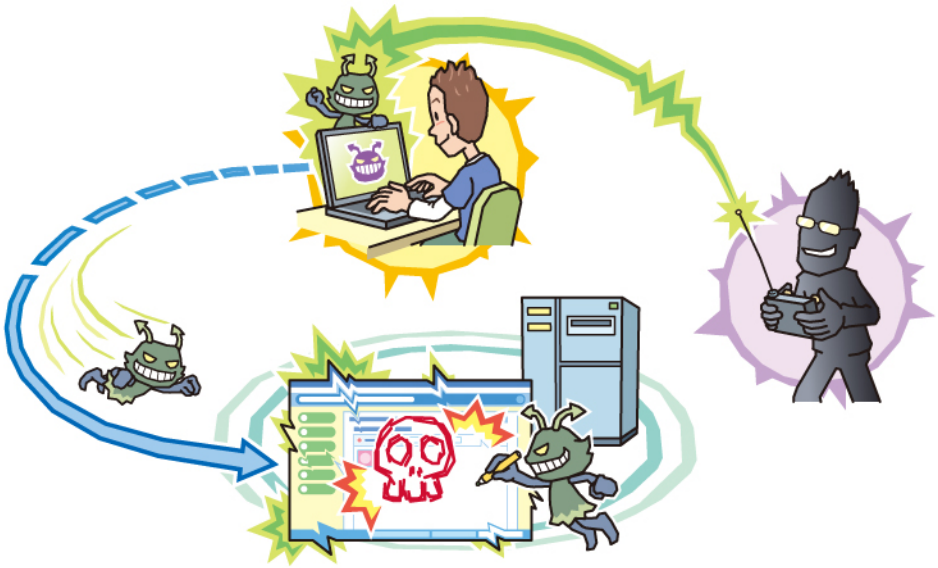
- **2012年の事例／統計**
  - 「the Movie」は、約3,300台の端末から約76万人分の個人情報を窃取
  - 「全国電話帳」など個人情報収集を明言するアプリも登場

個人情報を収集する手口は、より巧妙化しており、ユーザーは被害に気付くことが難しい

【3位】スマートデバイスを狙った悪意あるアプリの横行
～信頼できるアプリやサービスの利用を心掛ける～

- **対策一覧**
  - **教育/啓発**
    - アプリによる情報窃取の現状をユーザーが知る必要がある
    - 利用するアプリが信頼できるかどうかどのような点で判断できるか知っておく。
      （ダウンロード数/利用者数の多さ、ユーザーレビュー/ネット上の評価の良さ、
      利用規約の内容、アプリの権限/アクセス許可）
  - **ウイルス対策**
    - スマートデバイス用のウイルス対策ソフトを導入する
    - ウイルス対策ソフトによっては、個人情報へアクセスするアプリを見つける機能もある

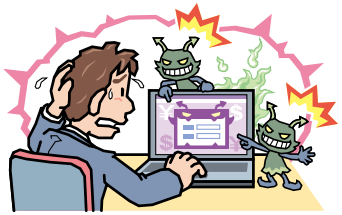
【4位】ウイルスを使った遠隔操作
～知らない間に濡れ衣を着せられることに！！～



- **概要**
  - ウイルスに感染したPCは遠隔操作されて、スパム送信やDDoS攻撃の踏み台に
  - 近年、スパイ行為など限定的な用途に利用されるようになってきた
  - 2012年の遠隔操作ウイルス事件では、より私的な目的に使われた

【4位】ウイルスを使った遠隔操作
～知らない間にウイルスによって遠隔操作される～

- 攻撃に悪用される背景
  - ウイルスに感染したPCは、攻撃者の意図通りの挙動を行う
  - 攻撃者の代わりにDDoS攻撃や、スパムメールの送信を行う
  - 標的型攻撃と呼ばれるスパイ行為では、ウイルスが内部情報を外部に送信
  - いたずらや恨みを晴らすために作成し、PCを遠隔操作する者も出てきている



- 2012年の事例／統計
  - 遠隔操作ウイルス事件が話題に。掲示板に犯行予告などを行った容疑で4人が誤認逮捕された

ウイルスは、ボットと呼ばれる大規模なものから、特別な目的を実行するものまで、多様化してきている

【4位】ウイルスを使った遠隔操作
～日頃からPCを安全な状態に～

- 対策一覧
  - 教育/啓発
    - ウイルスの手口や被害の現状を理解し、作成者が不明であるなど信頼できないソフトウエアは利用しないように心掛ける
  - 脆弱性対策
    - 脆弱性を狙うウイルスは多く存在する。利用中のソフトウェアに更新(アップデート)があれば、速やかに適用する
  - ウイルス対策
    - 広く拡散しているウイルスはウイルス対策ソフトによってブロックすることが可能であるため、PCやサーバーにはウイルス対策ソフトを導入して常に検知機能を有効にしておく

【5位】金銭窃取を目的としたウイルスの横行
～日本でもインターネットバンキングが狙われている～

- **概要**
  - 海外で猛威を振るっているインターネットバンキングをターゲットにしたウイルスが日本のユーザーを標的にし始めている
  - セキュリティの更新やウイルス対策を怠らず、インターネットバンキングで利用している銀行のウェブサイトに掲載されているお知らせを確認するなどの注意が必要

【5位】金銭窃取を目的としたウイルスの横行
～認証情報を取られると他人の口座に送金される～

- 攻撃に悪用される背景
  - インターネットバンキングは、銀行に行かなくても残高照会や送金ができ便利である反面、悪意のある第三者に認証情報を知られると金銭的被害を受ける可能性がある
  - 認証情報を狙うウイルスは、これまで海外で流行してきたが、近年は日本のユーザーをターゲットとするウイルスが登場している

- 2012年の事例／統計
  - 通常のインターネットバンキングの画面に、別の認証画面をポップアップ表示するウイルスが登場した
  - SpyEyeなどの海外で有名なウイルスも、日本の銀行の認証情報を取得できるように拡張されている

インターネットバンキングを狙うウイルスが、日本の銀行のユーザーを狙っている

【5位】金銭窃取を目的としたウイルスの横行
～PCを健全にし、自衛に努める～

- 対策一覧
  - 脆弱性対策
    - ウイルスは脆弱性を突いて感染する。利用しているソフトウェアに更新（アップデート）があるかこまめに確認し、更新があれば速やかに適用する。
  - ウイルス対策
    - 広く拡散しているウイルスはウイルス対策ソフトによってブロックすることが可能であるため、PCにはウイルス対策ソフトを導入して常に検知機能を有効にしておく
  - 教育／啓発
    - 金銭窃取を目的にインターネットバンキングの認証情報を狙うウイルスの存在を知り、利用の銀行のウェブサイトに掲載される注意喚起などを読み、自衛に役立てる

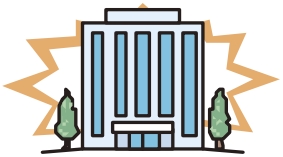
【6位】予期せぬ業務停止

～自然災害やハードウェア障害、人的ミスが思わぬ事態を引き起こす～

- **概要**
  - ハードウェア障害や人為的ミスにより、システムの不稼働が発生し、ビジネスに大きな影響を与える可能性がある
  - 大規模な自然災害も、業務停止の要因となりえる
  - 企業/組織は、業務停止への事前の準備と、日頃の堅実な運用や監視を行う必要がある

【6位】予期せぬ業務停止
～自然災害や障害は突然やってくる～

- 被害を受ける背景
  - ハードウェア障害や、2011年に発生した東日本大震災のような自然災害は、予想できないタイミングで突然発生し、業務停止を引き起こす原因となっている
  - 管理者が誤って重要データを削除してしまうなど、人為的ミスも業務停止の原因となる



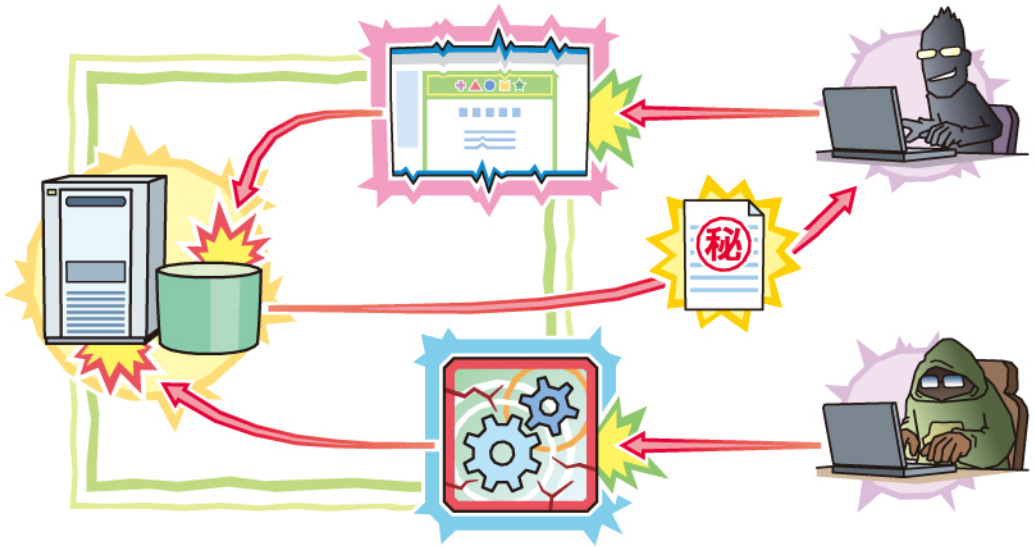
- 2012年の事例／統計
  - レンタルサーバー企業において、人為ミスによる大規模な障害が発生し、約5,700の顧客のサーバーのデータが削除された
  - 東京証券取引所において、待機系への切り替え失敗により、約300銘柄が3時間半の取引停止となった

障害や災害など、常に業務停止の原因が潜んでおり、備えておかなければ、停止が長期化する

【6位】予期せぬ業務停止
～自然災害や障害を想定したシステムと運用を～

- 対策一覧
  - システム設計
    - バックアップやシステムの二重化など、障害や災害に備えたシステム設計を行う
    - 手順書の作成や承認プロセスの確立など、人為的ミスを軽減できる運用設計を行う
  - システム監視
    - ログの監視やシステムの死活監視を行い、異常を迅速に検知する
  - アカウント/権限管理
    - 容易に削除が行えないなど、人為ミスの発生を予防するため、アカウントや権限を適切に管理する

【7位】ウェブサイトを狙った攻撃
～断続的に続くウェブサイトを狙った攻撃～



- **概要**
  - ウェブサイトはさまざまなアプリケーションで構成されているため、脆弱性や設定不備など、セキュリティのほころびが大きな被害をもたらす
  - 攻撃により、ウエブサイト内の個人情報の窃取や、主義・主張の表示や悪意のあるサイトへの改ざんが行われる

【7位】ウェブサイトを狙った攻撃
～様々な意図により狙われるウェブサイト～

- 攻撃の意図
  - ウェブサイトからの**情報の窃取**
  - **ウイルス配布**に悪用
  - ウェブサイト改ざんによる**主義・主張**

- 2012年の事例／統計
  - 国内のソフトウェアダウンロードサイトが、4回に渡り不正アクセスを受け、463件のクレジットカード情報が窃取された
  - JPCERT/CCの報告によると、2012年のウェブサイト改ざんは、前年比6倍の1,814件であった

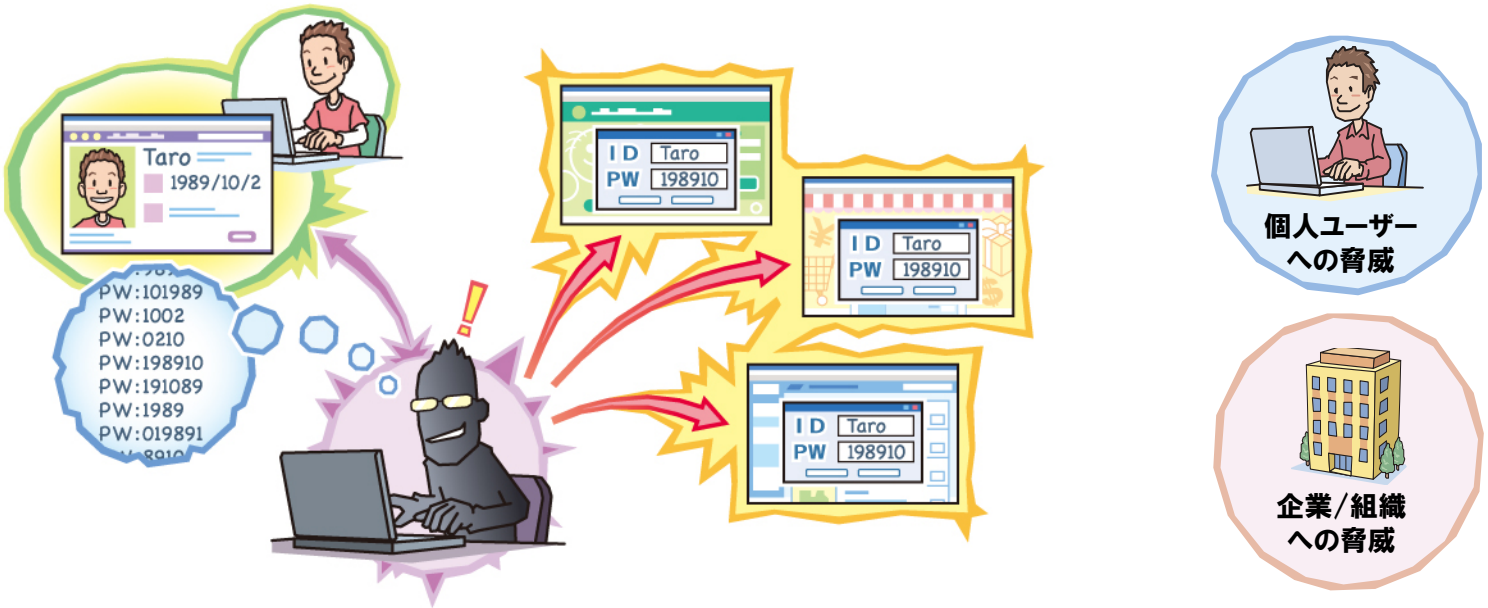
攻撃者は、ウェブサイトに存在するセキュリティ上のほころびを見つけ出し、情報窃取や改ざんを行う

【7位】ウェブサイトを狙った攻撃
～開発から運用・監視まで幅広い対策を～

- 対策一覧
  - システム設計
    - 不要なサービスやアカウントの無効など、セキュリティを考慮した設定を行う
    - 適切にログを設計する
  - システム監視
    - ログの定期的または継続的な監視を行う
  - アカウント/権限管理
    - アカウントには適切な権限を設定し、必要以上の権限を持たせない運用を行う
  - 脆弱性対策
    - ウェブシステム(アプリケーションサーバーやデータベースサーバーを含む)のOSおよびソフトウエアの脆弱性の有無を定期的に診断し、可能な限り更新を適用する
    - ウェブアプリケーションは脆弱性を作りこまず、定期的に診断し、脆弱性は修正する

【8位】パスワード流出の脅威

～知らぬ間にパスワードが盗まれていませんか？～



- **概要**
  - オンラインサービスの増加に伴い、複数のパスワードの管理が必要
  - 同一のID/パスワードを複数のウェブサイトで使い回している実態
  - 一つのウェブサイトでパスワードの漏えいが起きた際に被害が拡大

【8位】パスワード流出の脅威
～オンラインサービス増加に伴うパスワード使い回しの現状～

- 攻撃に悪用される背景
  - オンラインサービスの増加に伴ったパスワードの管理の煩雑さにより、同一ID/パスワードを使い回す利用者が増加
  - 攻撃者は、入手したパスワードで本人の権限を利用し不正な操作が可能

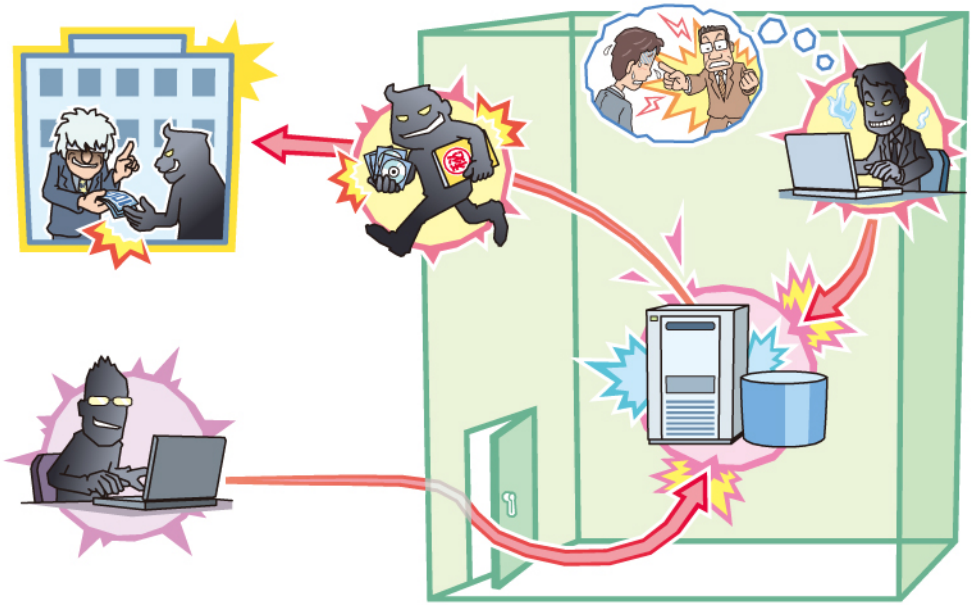
- 2012年の事例／統計
  - 7割の利用者が3種類以下のパスワードを使い回している状況
  - オンラインゲームサービスでは、ID/パスワードのリストを悪用した不正ログイン被害が多発

不正アクセス制限等を実施していても、パスワードが漏えいしてしまうと、攻撃を防ぐことができない

【8位】パスワード流出の脅威
～安全なパスワードの運用・管理が重要～

- 対策一覧
  - アカウント/権限管理(ユーザー/管理者の対策)
    - 十分な長さと強度を持ち容易に推測されないパスワードを使用する
    - サービスごとに別のパスワードを設定する
  - 教育/啓発(管理者の対策)
    - 利用者へのパスワード設定、管理の強化を図るための教育を実施する
  - システム設計(管理者の対策)
    - パスワードをソルト付きでハッシュ化する
    - パスワード推測攻撃に備えて、アカウントロックを設定しておく
    - ワンタイムパスワードなどの認証ソリューションの導入

【9位】内部犯行
～あなたの職場は大丈夫？内部に潜む犯行者～



- **概要**
  - 従業員や元従業員による故意の情報漏えいや不正操作による被害
  - 正当な権限を利用した犯行のため、被害が大きくなる傾向
  - 技術的対策だけでは防止が困難

【9位】内部犯行
～金銭目的での内部犯行が多発～

- 犯行の背景
  - 従業員は自らの権限で業務妨害、情報持ち出しなどを行うことが可能
  - 退職者、委託社員などはバックドア等を利用し内部情報を窃取
  - 情報の転売、流用、業務妨害など内部犯行の目的や手口は様々



- 2012年の事例／統計
  - 内部犯行の動機の32%が金銭目的で、組織への不満、転職目的が26%
  - 委託社員による三百数十口座分の顧客データ抜き取りによって、キャッシュカードの偽造、現金の不正引き出しの被害が発生

内部犯行は人為的なものであるため、技術的な対策だけでは犯行を防ぎにくい

【9位】内部犯行
～不正を起こしづらい状況を創出～

- 対策一覧
  - アカウント/権限管理
    - 各ユーザーには必要以上の権限を与えず、適切な権限を付与する
  - ポリシー/ルール
    - 内部情報の持ち出し禁止を企業/組織内で明示する
  - システム設計
    - 重要情報へのアクセス制限と監視を適切に行えるシステムの導入する
    - 作業実施者と承認者を分離するなど厳格な運用手順を確立する
  - システム監視
    - ログを監視するなど不正に対し目を光らせておくことで、犯行の起こりにくい状況を作る

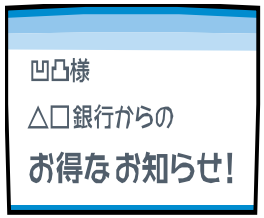
【10位】フィッシング詐欺

～あなたの口座から預金が無くなっていませんか？～

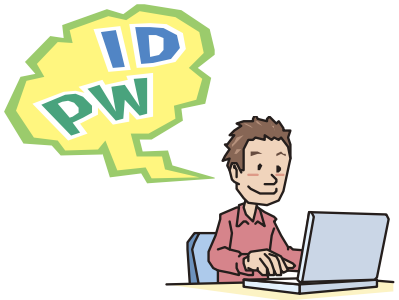
- **概要**
  - インターネットユーザーをターゲットにしたフィッシング詐欺が横行
  - ユーザーが騙されることで、ID・パスワードが盗み取られる
  - 盗まれたID・パスワードが悪用され、不正送金などの被害が発生

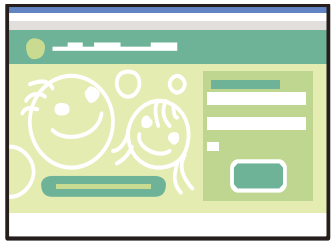
【10位】フィッシング詐欺
～メールとウェブサイトを使った詐欺行為～

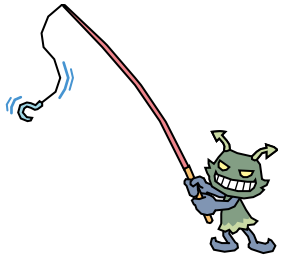
- 攻撃の手口
  - (1) 銀行などの実在する組織を装ったメールがユーザーに送りつけられる
  - (2) メールには、フィッシングサイトに誘導するためのリンクが貼られている



  - (3) リンクをクリックすると、本物そっくりのフィッシングサイトに誘導され、ユーザーがID/パスワードなどを入力することで、攻撃者に盗まれてしまう







【10位】フィッシング詐欺
～あなたの口座から預金が無くなっていませんか？～

- 2012年の事例／統計
  - フィッシング詐欺被害状況

    報告件数：52件／月、フィッシングサイト数：207件（共に2012年12月時点）
  - 大手銀行を装ったフィッシング詐欺

    2012年は、大手銀行を装ったフィッシング詐欺が広く行われ、当該銀行からユーザーに対して、注意喚起が行われた

- 対策一覧
  - 教育／啓発
  - アカウント／権限管理

    （ワンタイムパスワード・二要素認証の採用）

ユーザーが騙されないための教育・啓発
二要素認証等の強い認証方式を利用するのが良い

目次

- 10大脅威について
- 1章. 情報セキュリティの変遷
- 2章. 2013年版10大脅威
- **3章. 今後注目すべき脅威**

1．クラウド利用における課題

～クラウドサービスの拡大と新たな懸念～

- **概要**
  - クラウドサービスは、企業向けに留まらず、個人向けストレージや動画サービスなど、一般ユーザーにとって身近な存在になっている
  - システム管理者による管理操作の制限や、個人向けサービスの業務利用など、システム管理者にとり新たな課題が見えてきている

1．クラウド利用における課題
～クラウド導入の利点と主なセキュリティ事故～

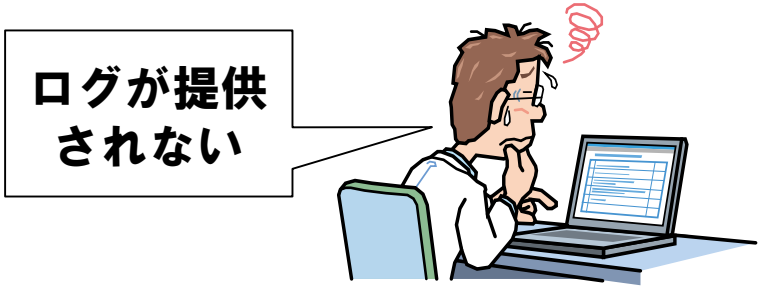
- クラウドを利用することの利点
  - システム導入・運用コストの低減
    - システムの調達・構築の手間が省け、運用に係る諸費用も抑えることができる
  - 使いたい時にどこからでも利用可能（業務効率の向上）
    - 職場だけでなく自宅や出先での操作を可能とし業務効率の向上が期待できる
  - 災害時の代替として最適（信頼性の向上）
    - 災害等でシステムに障害が起きた場合でも、短期間での代替が可能となる

- クラウドのセキュリティ事故
  - ハードウェア障害
  - オペレーションミス
  - アクセス権の奪取

クラウド事業者の約款を十分に理解したうえで、自社の運用に即した事業者を選ぶことが重要

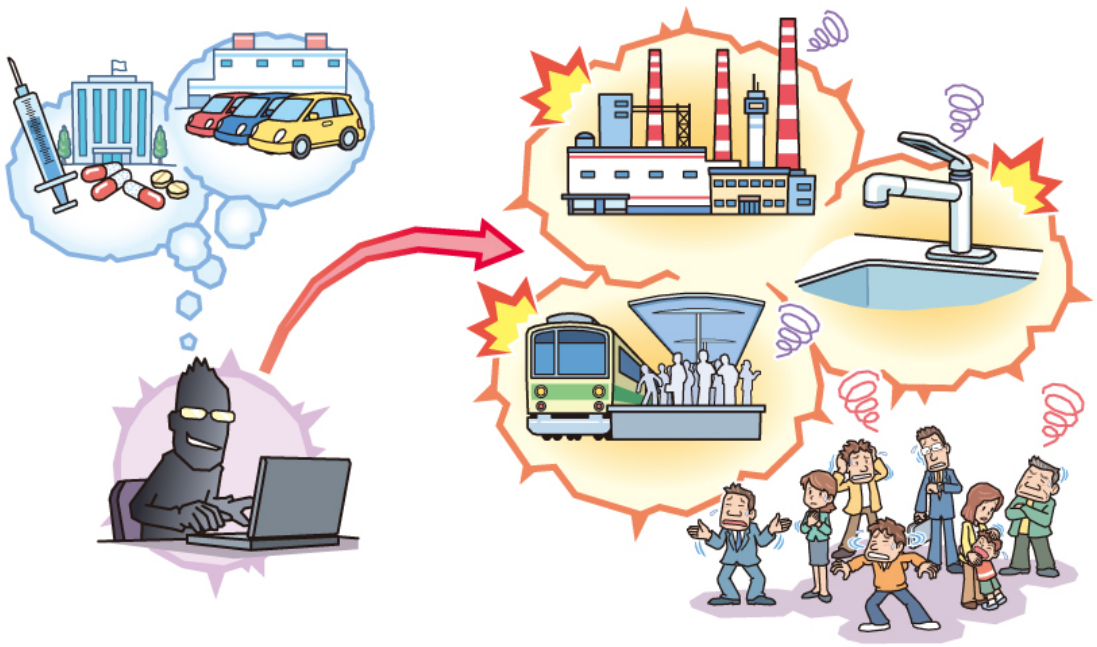
1．クラウド利用における課題
～システム管理者上の課題～

- インシデント対応に影響
  - 管理操作が制限されていることが想定される
  - 被害状況が確認できない可能性が考えられる
  - セキュリティ事故発生を想定し、事前に確認しておくことが重要



- 個人向けサービスの利用問題
  - 個人所有のデバイスの持ち込みや、個人契約サービスを業務利用の増加
  - 業務データが個人契約サービスに保管されるなど、データ管理が複雑に
  - 個人契約サービスの利用におけるルール化やシステム制限の検討が必要

2. 重要インフラを狙った攻撃
～様々な技術分野へ広がる脅威～



- **概要**
  - サイバー攻撃とは縁の薄かった、制御システムへの攻撃の懸念
  - 近年、制御システムの脆弱性の公表件数が増加している
  - 自動車やメディカルデバイスなどの機器にも、新たな脅威の懸念

2. 重要インフラを狙った攻撃
～重要インフラを狙った攻撃状況と影響～

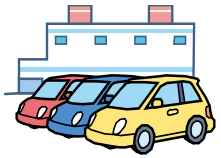
- 重要インフラを狙った攻撃
  - 近年、重要インフラ（エネルギー、生産ライン、化学プラント、輸送、通信など）に対する攻撃が懸念
  - 米国内の重要インフラに対するインシデントの報告件数は
    - 2009年：9件、2010年：41件、2011年：198件
  - 国家の安全保障、危機管理上の重要な課題となりつつある

- 重要インフラが狙われることの影響
  - 機器が故障、誤動作するなどの「物理的な被害」に発展
  - 電気・ガス・水道・交通システムが攻撃を受けた場合、社会生活に影響
  - 国内では表立った被害は無いが、海外では被害事例あり

2. 重要インフラを狙った攻撃
～セキュリティ対策状況と新たな脅威～

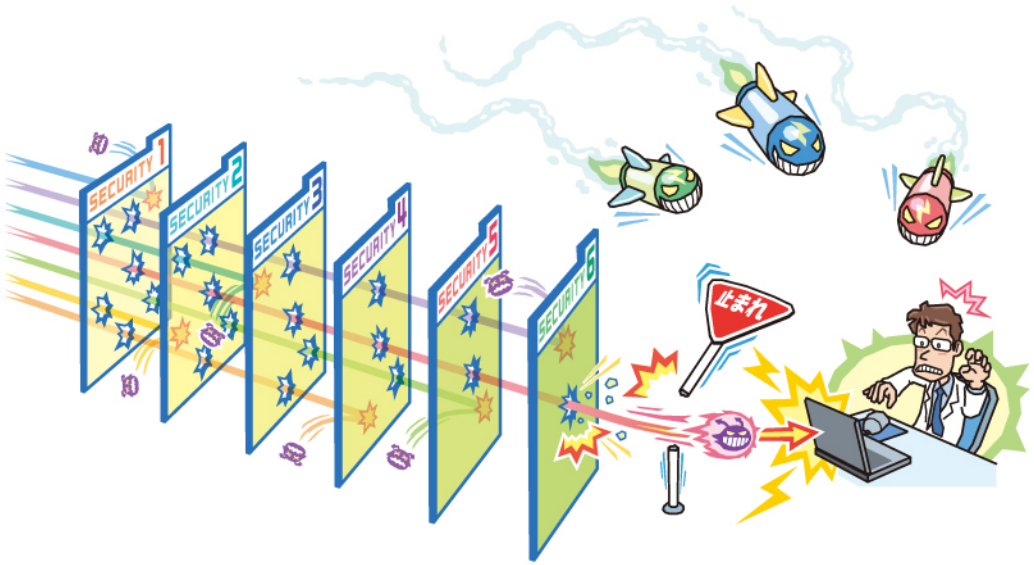
- 重要インフラへのセキュリティ対策に関する取組み
  - 制御システムセキュリティセンター（CSSC）設立（2012）
    - 重要インフラを含む制御システムのセキュリティを確保するため、研究開発等を推進
  - 認証制度
    - 制御システムセキュリティに関する国際規格の整備が推進。

- その他のシステムへの攻撃拡大の懸念（攻撃実績なし）
  - 自動車のセキュリティ
    - 自動車の装備にカーナビゲーションや車載カメラなど情報通信技術が導入されている
    - 特定の自動車の制御等に影響を与える可能性
  - メディカルデバイス
    - 米国の研究者がインスリンを投与するメディカルデバイスを遠隔操作できることを実証
    - 米国会計検査院のレポートで、メディカルデバイスの遠隔操作が脅威になると警告



3. 既存対策をすり抜ける攻撃の広がり

～攻撃の全体像を把握したセキュリティ対策を～



- **概要**
  - 2010年頃より特定のミッションに特化した高度な作りのウイルスが発見
  - 近年、既存対策で検知できないウイルスや攻撃が主流になりつつある
  - 検知・遮断に頼る対策から、攻撃の全体像を把握した対策が重要となる

3．既存対策をすり抜ける攻撃の広がり

～特定のミッションを遂行する為にウイルスが利用される～

- **高度なウイルスの登場**
  - 2010年、イランの原子力施設を狙ったとされる「Stuxnet」が発見
  - その後、「Flame」「Gauss」といった第二、第三の「Stuxnet」が登場
  - プログラムサイズの大きさや高度な作り、攻撃範囲が限定的などの特徴

- **攻撃の背景**
  - 情報破壊、諜報・スパイ目的に使われたと言われている
  - 国家などの大きな組織の関与が噂されている

3. 既存対策をすり抜ける攻撃の広がり

～攻撃の全体像を把握したセキュリティ対策を～

- **攻撃検知の限界**
  - ウイルス対策ソフトによる検知をすり抜ける攻撃が主流になりつつある
  - 個別に作り込まれたウイルスについては、検知するのは極めて困難
  - 攻撃ツールと管理ツールの区別が困難
    - 管理ツールが攻撃に悪用されるケースも散見されだしている

- **セキュリティ対策**
  - 全体像を把握したセキュリティ対策
    - ネットワーク設計、ログ監視などの対策を実施
  - セキュリティパッチの適用
    - 攻撃の基になる脆弱性対策を実施し、攻撃者に隙を与えない対策

おわりに

IPAでは、本資料が近年の情報システムを取り巻く脅威の理解や対策の実施に活用されることを期待しています。

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