IPA
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

「2014年版 10大脅威」

～複雑化する情報セキュリティ あなたが直面しているのは？～

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
2014年3月

目次

- 10大脅威について
- 1章. セキュリティ脅威の分類と傾向
- 2章. 2014年版10大脅威
- 3章. 注目すべき脅威や懸念

2014年版 10大脅威

http://www.ipa.go.jp/security/vuln/documents/10threats2014.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

2014年版 10大脅威

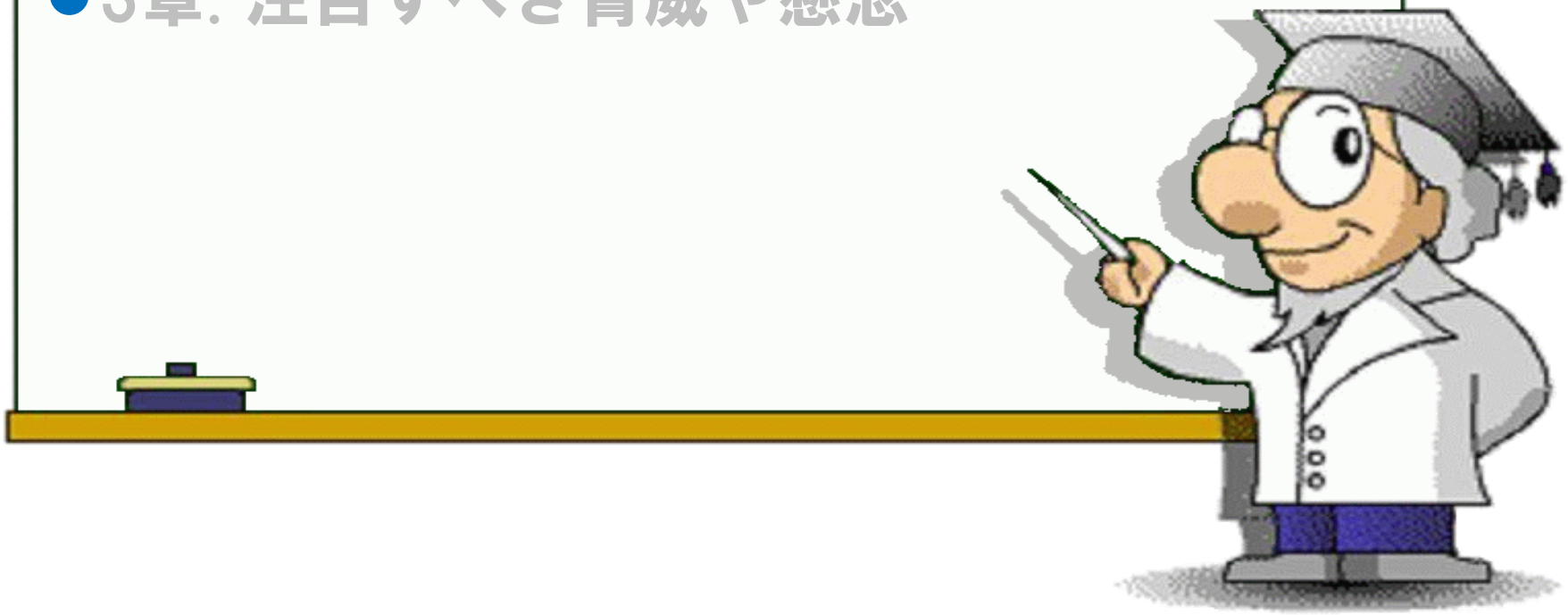
http://www.ipa.go.jp/security/vuln/documents/10threats2014.pdf

章構成

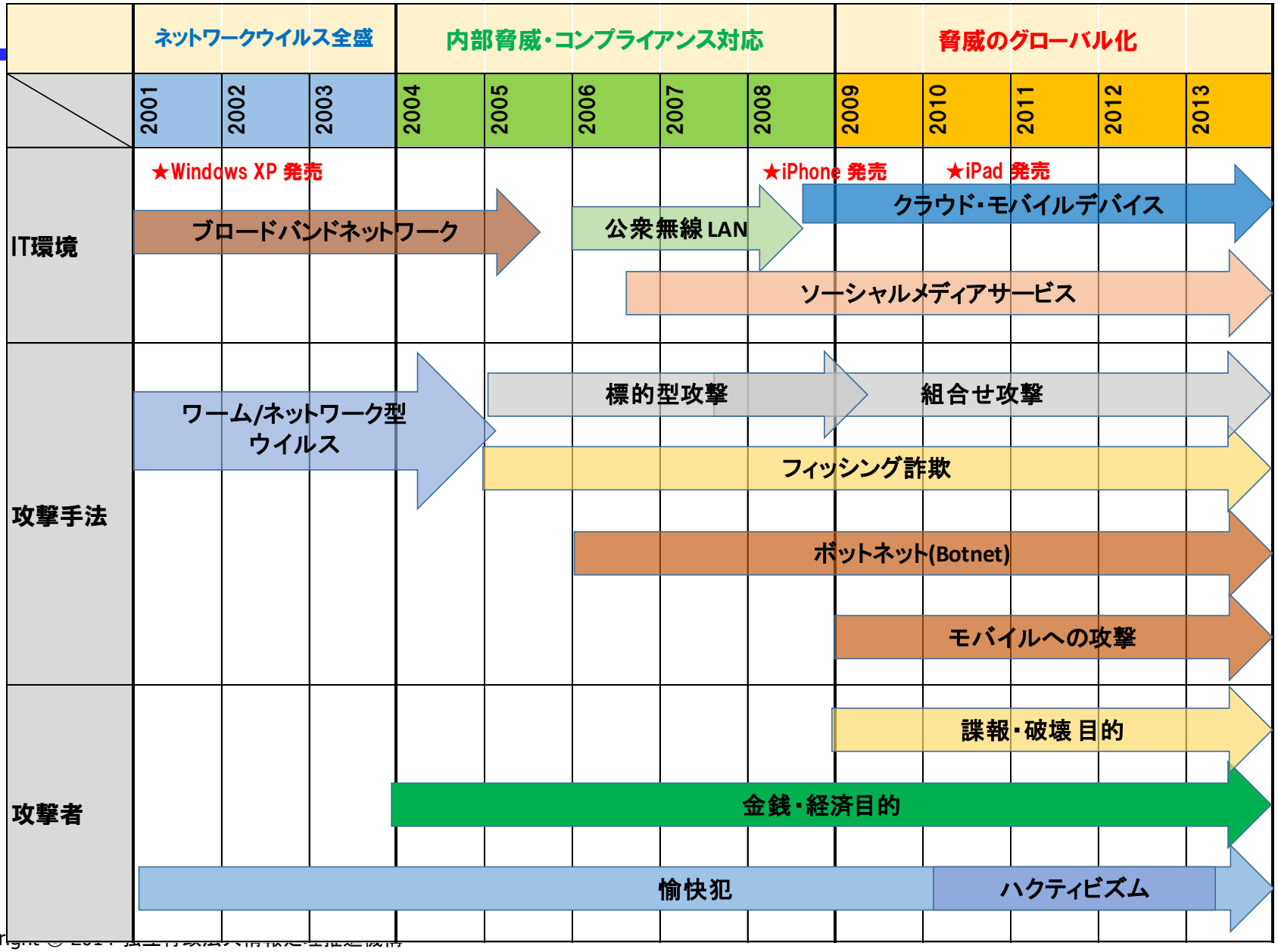
- 1章.セキュリティ脅威の分類と傾向
  - 脅威の背景、攻撃者の意図・特徴、被害者の特性等を基に分類し解説
- 2章.2014年版 10大脅威
  - 2013年の事例をベースに10の脅威を選出
  - 各脅威の概要と対策について解説
- 3章.注目すべき脅威や懸念
  - ネットワーク対応機器の増加
  - エンドポイントセキュリティの重要性
  - インターネット利用の低年齢化に伴う問題

目次

- 10大脅威について
- **1章. セキュリティ脅威の分類と傾向**
- 2章. 2014年版10大脅威
- 3章. 注目すべき脅威や懸念

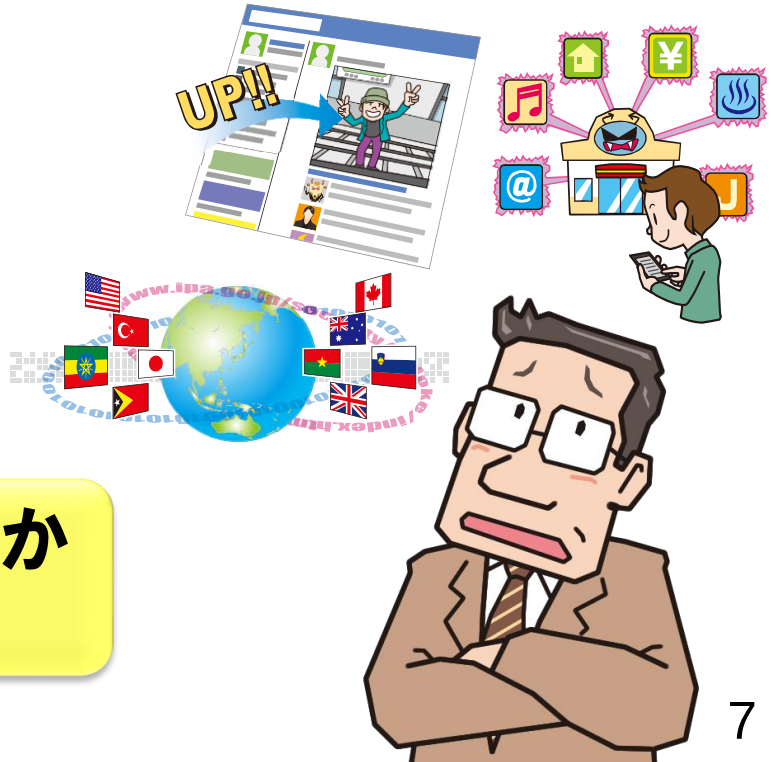


情報セキュリティの変遷



セキュリティ脅威の傾向

- ITの普及
  - SNSの普及
  - スマートフォンの普及
- 脅威の変化
  - 国際問題
  - 詐欺



どの脅威が自身に関係するか見極めが必要

セキュリティ脅威の分類

IPA

従来からの情報セキュリティ問題分野

情報・通信サービス

インターネットを使った詐欺・犯罪行為

・不正請求詐欺
・SNSの成りすまし

ウイルス・ハッキングによるサイバー犯罪

・ウェブサイト改竄
・不正ログイン
・不正送金

インターネット利用のエチケット

インターネットモラル

・誹謗中傷いじめ
・SNSによる個人情報公開

組織のセキュリティマネジメント

内部統制・セキュリティマネジメント

・情報漏洩
・内部犯行
・自然災害
・オペレーションミス

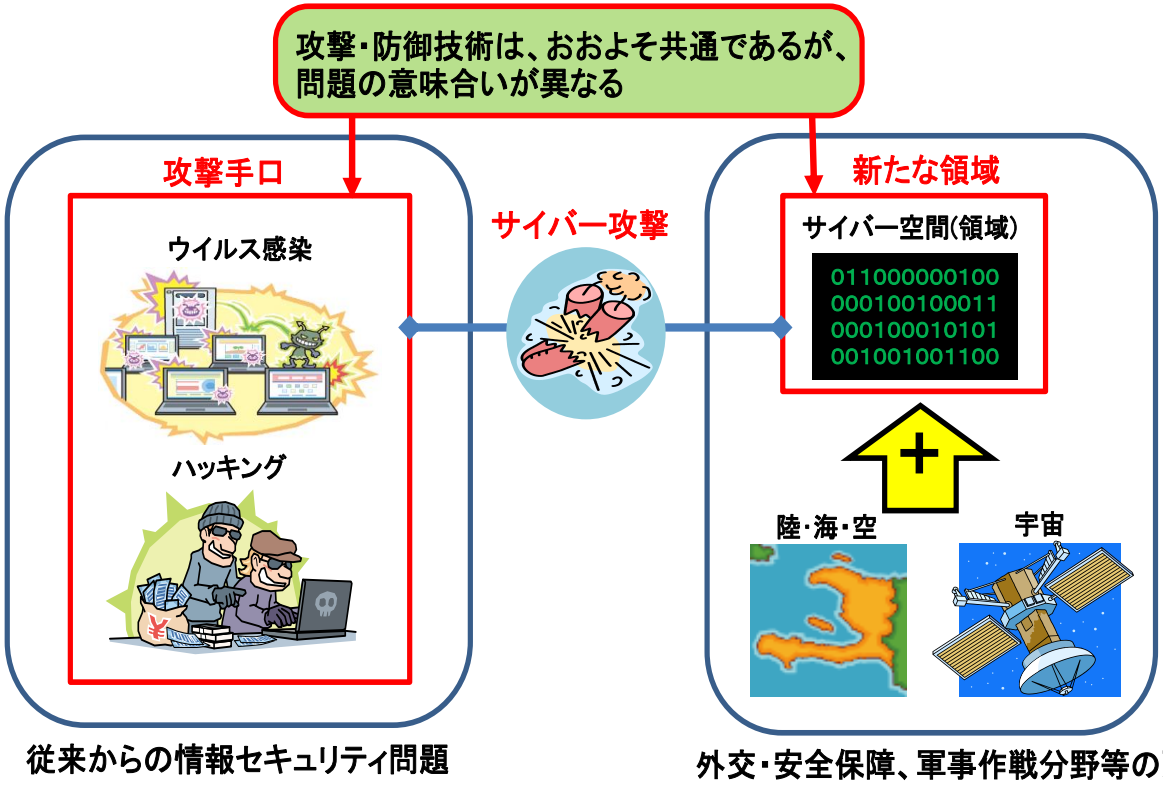
新たな問題分野

国際政治・安全保障

サイバー領域問題

・軍事的妨害活動
・国家機密の窃取
・社会インフラの破壊

サイバー領域問題



- **概要**
  - サイバー攻撃が安全保障の領域の問題として認識
  - インターネットは「国際政治」や「外交・安全保障、軍事作戦」を目的とした領域に

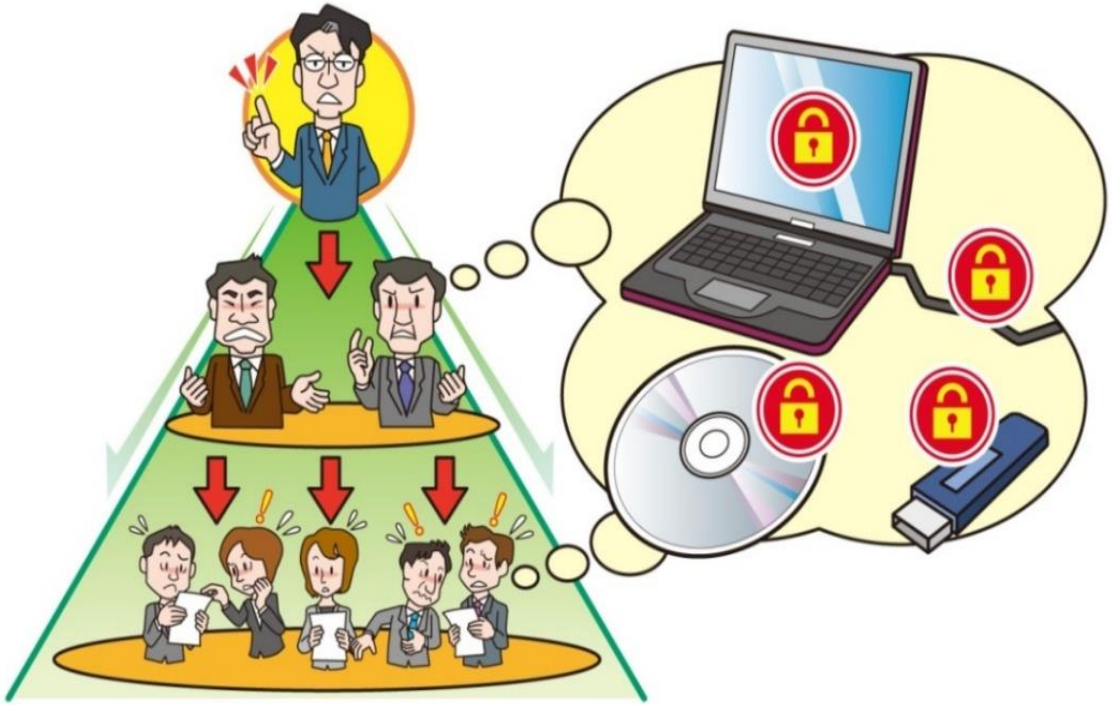
ウイルス・ハッキングを用いたサイバー犯罪

- **概要**
  - 金銭窃取を目的としたウイルス感染や不正アクセスが横行
  - 攻撃者は組織化し、年々被害規模が増大

インターネットを使った詐欺・犯罪行為

- **概要**
  - インターネット上でも、架空請求詐欺や偽物販売等の詐欺行為が繰り広げられている
  - SNSで有名人になりすました偽情報の流布も横行

内部統制・セキュリティマネジメント



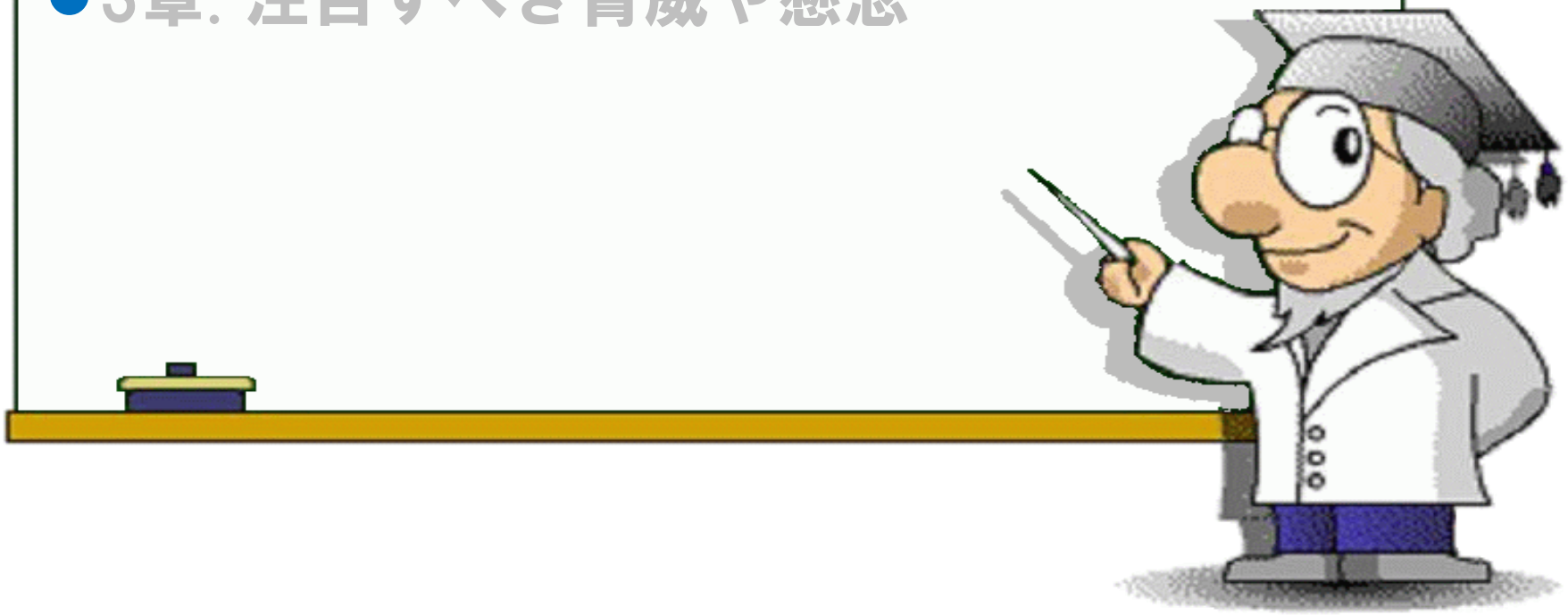
- 概要
  - 企業の情報セキュリティ体制整備が浸透
  - 情報資産の事故（漏えい、改ざん、消失、システム停止）抑止に重要な役割を果たしている

インターネットモラル

- 概要
  - インターネットを使う側のモラルの低さが問題を招く
  - 現実社会と同様、法律遵守やモラルを意識した利用が必要

目次

- 10大脅威について
- 1章. セキュリティ脅威の分類と傾向
- **2章. 2014年版10大脅威**
- 3章. 注目すべき脅威や懸念

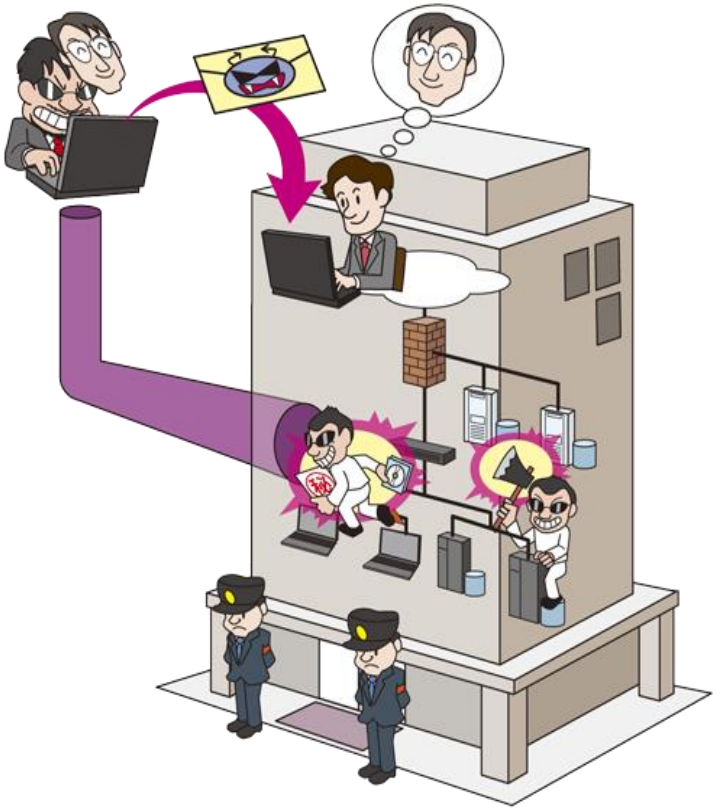


2014年版10大脅威 一覧

順位	脅威
1位	標的型メールを用いた組織へのスパイ・諜報活動
2位	不正ログイン・不正利用
3位	ウェブサイトの改ざん
4位	ウェブサービスからのユーザー情報の漏えい
5位	オンラインバンキングからの不正送金
6位	悪意あるスマートフォンアプリ
7位	SNSへの軽率な情報公開
8位	紛失や設定不備による情報漏えい
9位	ウイルスを使った詐欺・恐喝
10位	サービス妨害

【1位】標的型メールを用いた組織へのスパイ・諜報活動

～政府機関だけでない！民間企業も狙われている～



サイバー空間
（領域）問題

- **概要**
  - ネット経由で活動する「諜報・スパイ」の存在が明るみに
  - 政府機関から民間企業まで幅広く狙われている

【1位】標的型メールを用いた組織へのスパイ・諜報活動

～政府機関だけでない！民間企業も狙われている～

- **攻撃に悪用される背景**
  - 攻撃が見え難く、容易に気づけない
  - メールやウェブを介して遠隔から侵入できる
- **2013年の事例／統計**
  - **民間企業もターゲットに**
    - 「官公庁・地方自治体等」が37.7%、「金融機関」:16.4%、「マスコミ関連」:13.1%、　「IT・通信」:8.2
  - **外交問題に発展**
    - 2013年7月開催「米中戦略経済対話」、米国から中国に「サイバー攻撃による窃盗行為を止めるように」強い要請

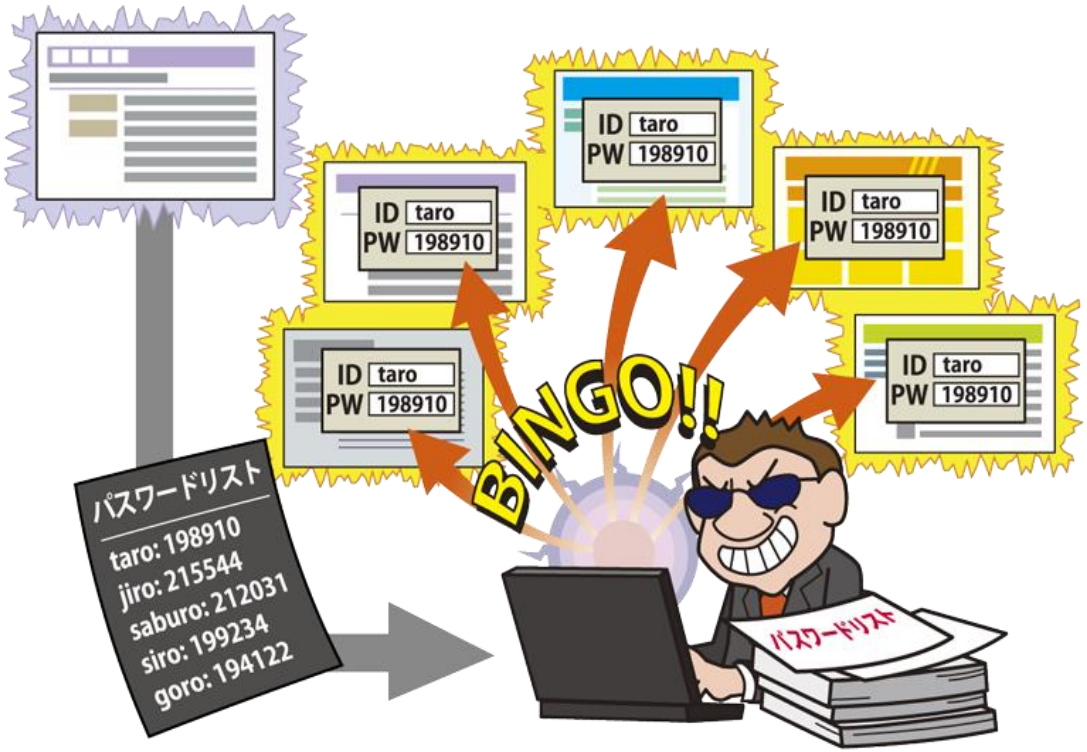
【1位】標的型メールを用いた組織へのスパイ・諜報活動

～政府機関だけでない！民間企業も狙われている～

- 対策一覧
  - システム設計
    - ネットワークのアクセス制御（部門でセグメントを分割するなど）
    - 機密情報の管理（適切なアクセス権の設定など）
  - ウイルス対策
    - ウイルス対策ソフトの導入など基本的な対策を実施する

内部侵入を想定した対策で
攻撃者の動きをブロック！

【2位】不正ログイン・不正利用
～ユーザーの安全なパスワード管理が重要！～

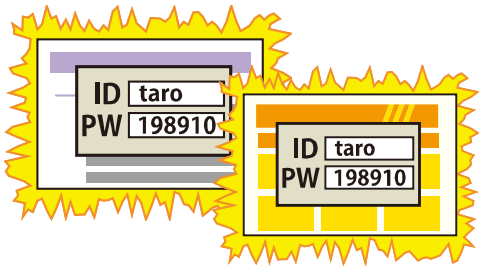


ウイルス・ハッキング
サイバー攻撃

- **概要**
  - ID/パスワードが窃取や推測されて、サービスやシステムが不正利用
  - パスワードリストを使った手口が拡大、ID/パスワードを使いまわすユーザーが被害に遭っている

【2位】不正ログイン・不正利用
～ユーザーの安全なパスワード管理が重要！～

- 攻撃に悪用される背景
  - ID/パスワードによるユーザー認証は、標準的な認証手段
  - ID/パスワードが分かればサービスを不正利用可能
  - 複数のサービスで同じID/パスワードを使い回してしまう



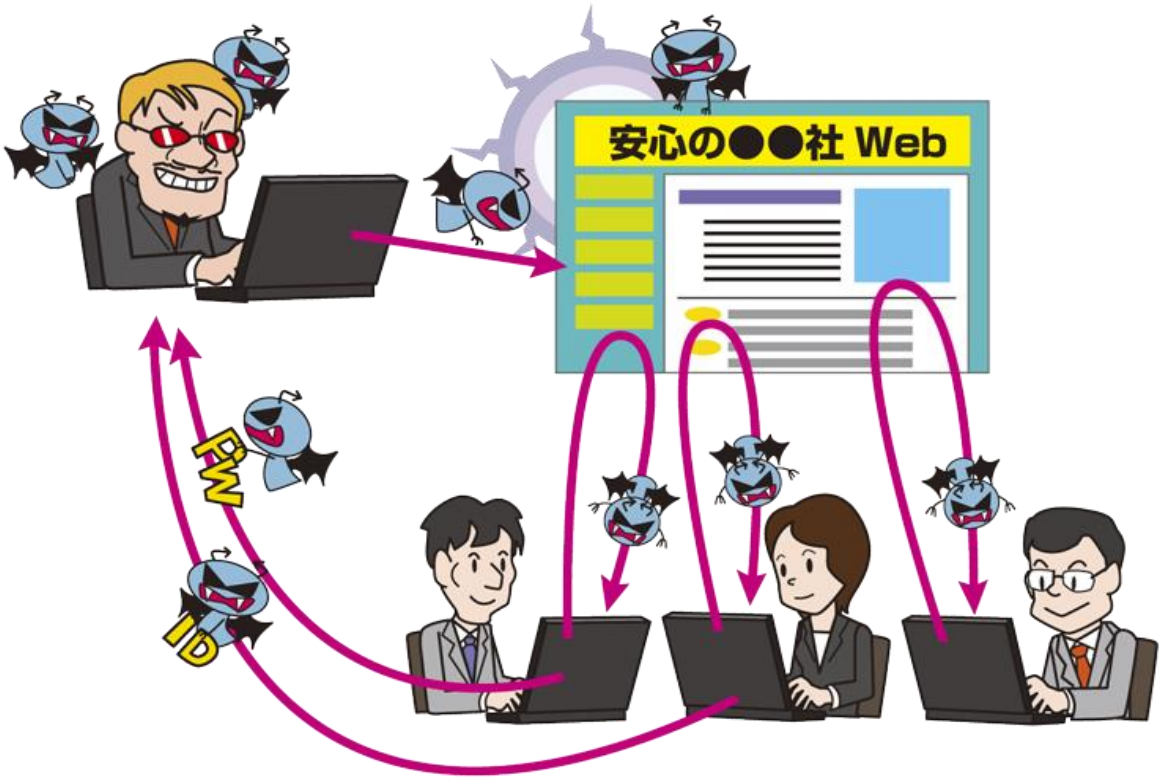
- 2013年の事例／統計
  - パスワードリスト攻撃の急増
    - 不正に入手したID/パスワードリストを使用する攻撃
    - クレジットカード会社、ショッピングサイトなど幅広く狙われた
    - 多くの不正ログイン成立率は0%台と低いものの、成功件数は十分な数（例、試行件数の0.15%にあたる23,926件が不正ログイン成立）

【2位】不正ログイン・不正利用
～ユーザーの安全なパスワード管理が重要！～

- **対策一覧**
  - **長く複雑なパスワードを設定する**
    - 長い文字列、英数字・大文字・小文字・記号を使用する
  - **パスワードを使い回さない**
    - サービス・システムごとに違うパスワードを設定する
  - **パスワード以外の認証方式の利用**
    - ワンタイムパスワード・認証トークンが提供されていれば利用する

パスワードは使い回さず、適切に管理！

【3位】ウェブサイトの改ざん
～気づかぬうちにウイルス感染～

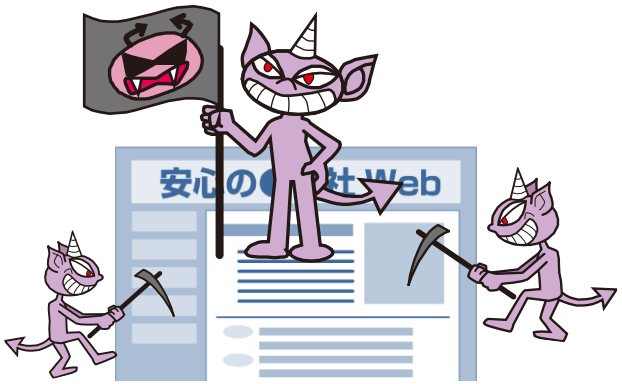


ウイルス・ハッキング
サイバー攻撃

- **概要**
  - ウェブサイト改ざんがウイルス感染の常套手段となっている
  - 改ざんされたサイトは攻撃に加担することになる

【3位】ウェブサイトの改ざん
～気づかぬうちにウイルス感染～

- 攻撃に悪用される背景
  - 管理者端末をウイルスが狙っている
  - FTPやSSH等、管理用サービスから侵入
  - コンテンツ管理システム（CMS）など汎用的なソフトウェアが狙われる
  - ウェブアプリケーションの脆弱性も狙われる



- 2013年の事例／統計
  - ウェブサイト改ざん被害急増
    - 2013年6月は4,000件超、4月と比較して2倍以上に急増
  - レンタルサーバーにおける改ざん被害
    - 国内レンタルサーバー企業が管理する8,438サイトが大量改ざん

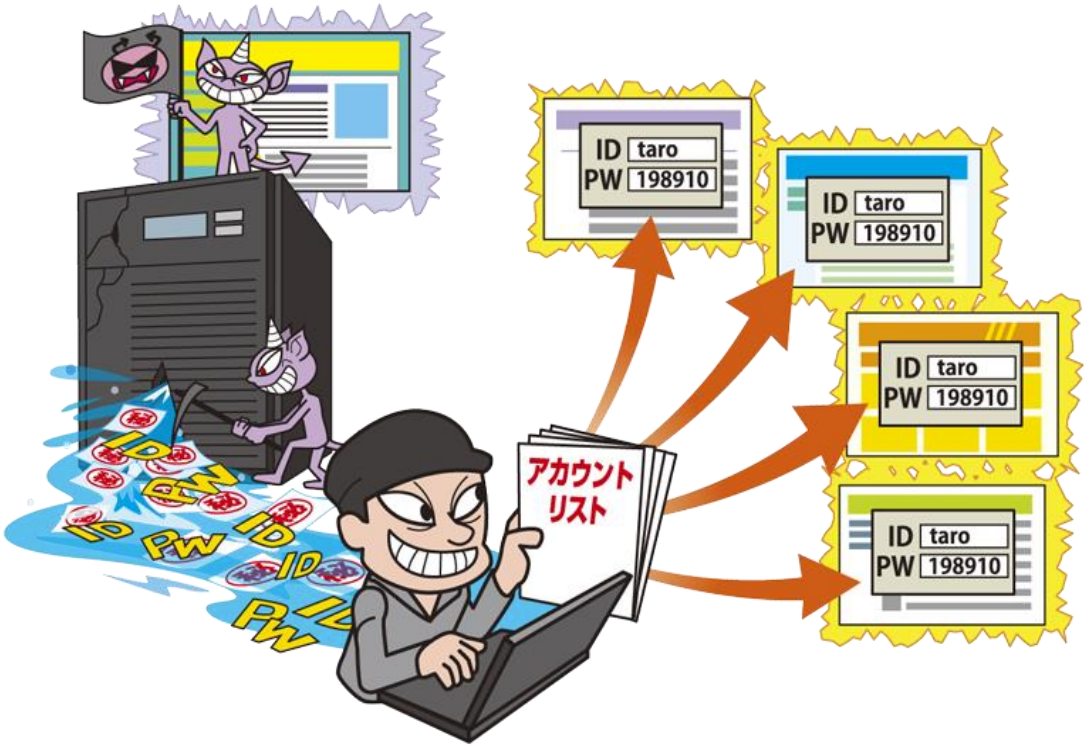
【3位】ウェブサイトの改ざん
～気づかぬうちにウイルス感染～

- 対策一覧
  - セキュアなサーバーの設定
    - 不要なサービスの無効などの設定、アクセス権設定、ログ設定など
  - アカウント・パスワードの管理
    - 複数人でアカウントを共有せず、複雑なパスワードの利用する
  - OS・ソフトウェアの定期的な更新
    - OS、ミドルウェア、フレームワークなどを定期更新
  - ウェブアプリケーションの脆弱性対策
    - セキュア開発、公開前や定期的な脆弱性検査・診断の実施

ウェブサイトには十分なセキュリティ対策を！
運用・監視も怠らない

【4位】ウェブサービスからのユーザー情報の漏えい

～ハッキングによりユーザー情報がごっそり盗まれる～



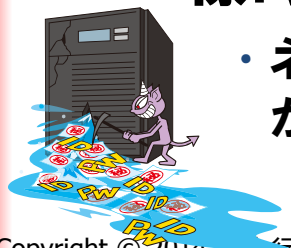
ウイルス・ハッキング
サイバー攻撃

- **概要**
  - ウェブサービスから大量のユーザー情報が流出する「メガリーク」が横行
  - 個人情報やクレジットカード情報の漏えいは影響が広範囲に及ぶ

【4位】ウェブサービスからのユーザー情報の漏えい
～ハッキングによりユーザー情報がごっそり盗まれる～

- **攻撃に悪用される背景**
  - インターネット上のウェブサービスは、生活に必要不可欠な存在に
  - 会員制サービスは、クレジットカード情報等の大量の個人情報を保持

- **2013年の事例／統計**
  - クレジットカード情報漏えい事故多発
    - 眼鏡販売サイトのミドルウェアApache Struts 2の脆弱性を悪用、2,059件のクレジットカード情報が漏えい
    - ネットスーパーのサイトで、最大15万165件のクレジットカード情報が不正に閲覧された可能性
  - 標的型攻撃による情報漏えい
    - ネット検索大手企業が、最大148.6万の情報漏えいを発表。内部のパソコンが標的型攻撃を受けたことが原因

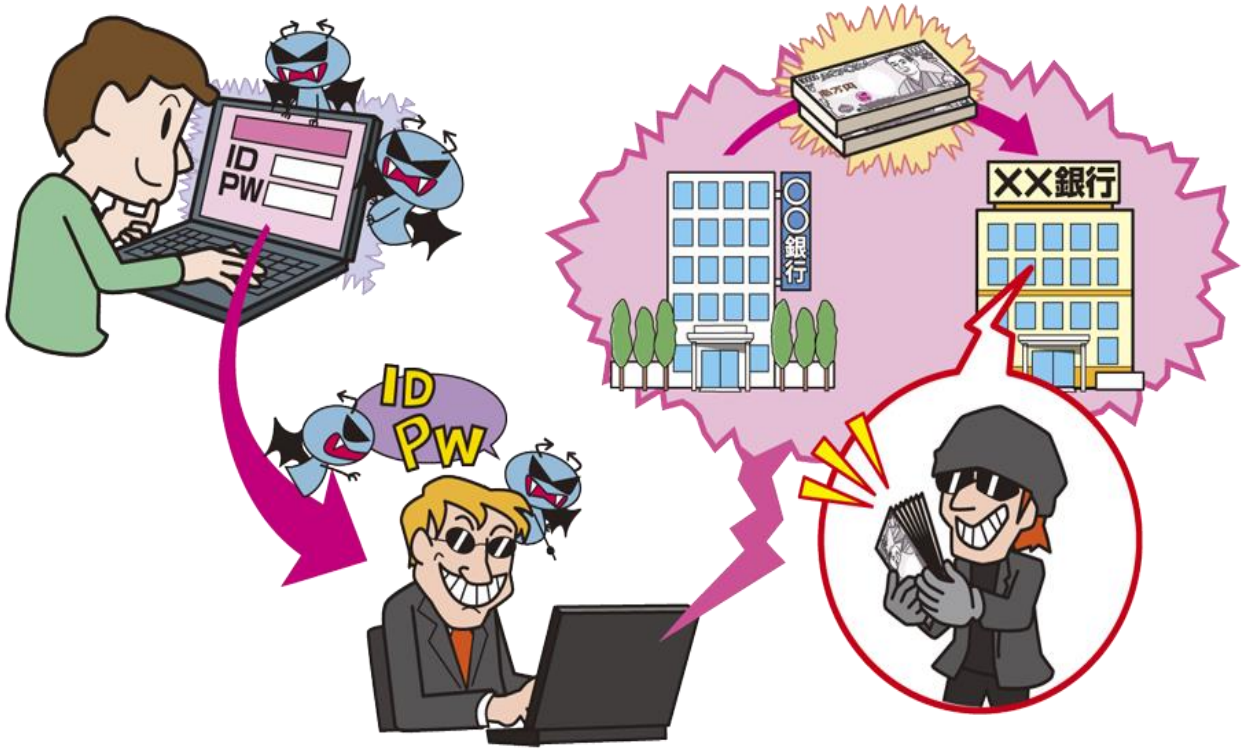


【4位】ウェブサービスからのユーザー情報の漏えい
～ハッキングによりユーザー情報がごっそり盗まれる～

- **対策一覧**
  - **ネットワークアクセス制御**
    - 外部からも内部からも不正アクセスを防ぐ
  - **セキュアなサーバーの設定**
    - 不要なサービスの無効などの設定、アクセス権設定、ログ設定など
  - **OS・ソフトウェアの更新**
    - OS、ミドルウェア、フレームワークなどを定期更新
  - **ウェブアプリケーションの脆弱性対策**
    - セキュア開発、公開前や定期的な脆弱性検査・診断の実施

外部からはもちろん
内部からも侵入されない対策を！

【5位】オンラインバンキングからの不正送金
～攻撃者が銀行の認証情報を狙っている～

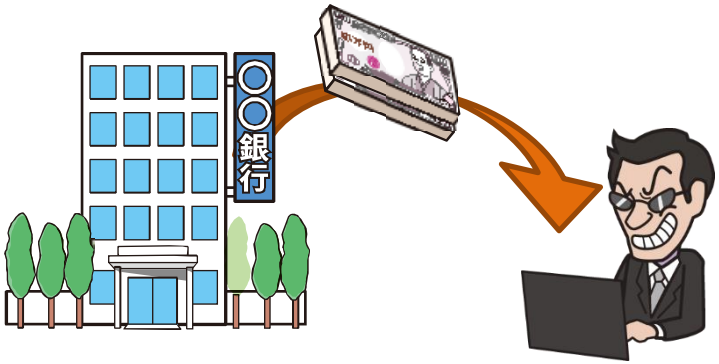


ウイルス・ハッキング
サイバー攻撃

- **概要**
  - 窃取した認証情報を使って、本人に成りすまして不正送金
  - 2013年、オンラインバンキングの不正送金の被害額が過去最大に

【5位】オンラインバンキングからの不正送金
～攻撃者が銀行の認証情報を狙っている～

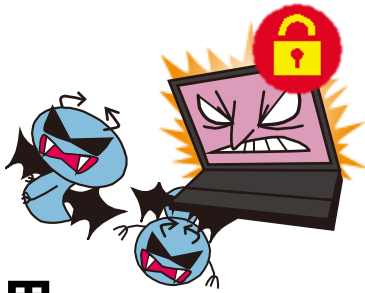
- 攻撃に悪用される背景
  - 認証情報を窃取できれば、成りすまして不正送金可能
  - 大手銀行から地方銀行やネット銀行まで幅広くターゲットに
  - フィッシング詐欺の手口も継続して横行

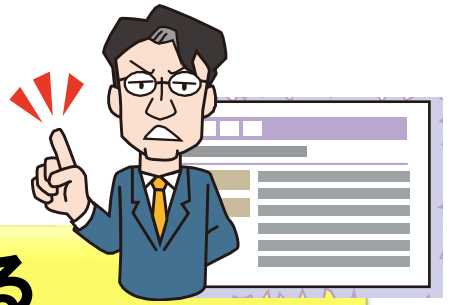


- 2013年の事例／統計
  - ウイルスによる不正送金被害の急増
    - 2013年の被害額は約11億8,400万円と警察庁公表、2011年の約4倍に
  - ワンタイムパスワードの窃取
    - ワンタイムパスワードをメールで受け取る仕組みを悪用し、攻撃者による被害者のメールボックスのハッキング

【5位】オンラインバンキングからの不正送金
～攻撃者が銀行の認証情報を狙っている～

- 対策一覧
  - OS・ソフトウェアの更新
    - Windows Updateの実施と、Adobe製品やJREを定期的に更新
  - ウイルス対策ソフトの導入
    - ウイルス対策ソフトでウイルスの感染を防止
  - ワンタイムパスワードの利用
    - 銀行が用意するオンラインバンキング向け認証方式を活用
  - 事例や手口を知る
    - 銀行のウェブサイトのお知らせなどを確認する

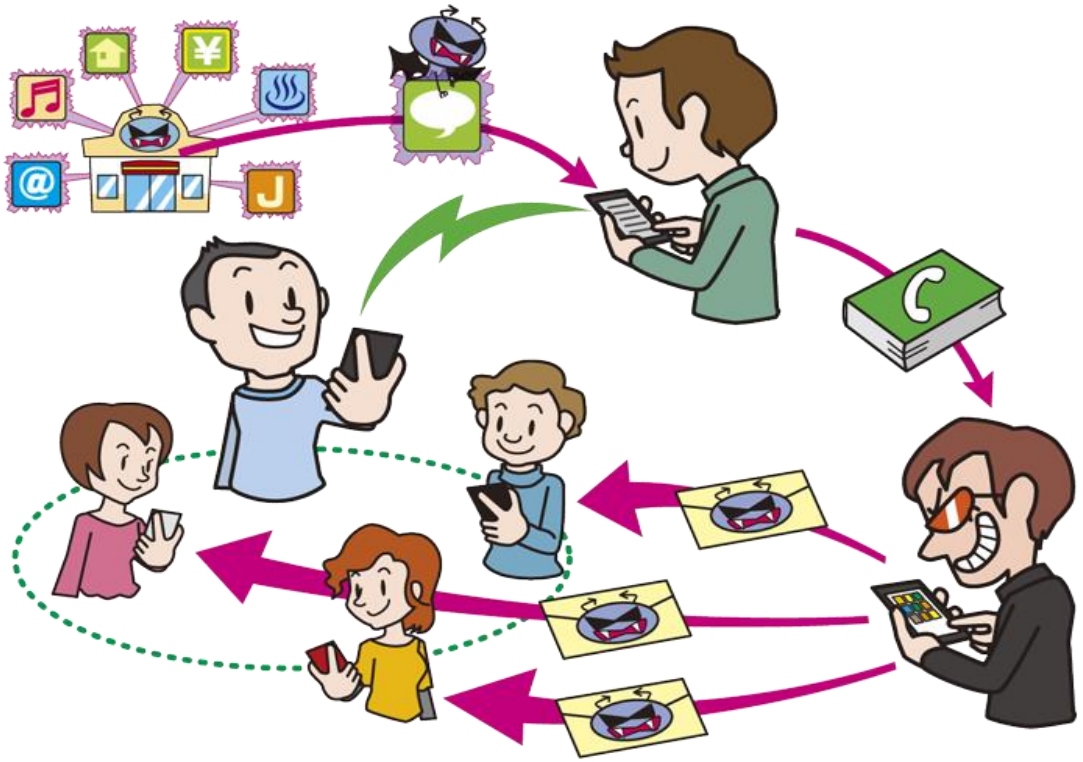




オンラインバンキングが用意する
ワンタイムパスワードなどの認証を活用

【6位】悪意あるスマートフォンアプリ

～スマートフォンに保存されているデータが盗み取られています～

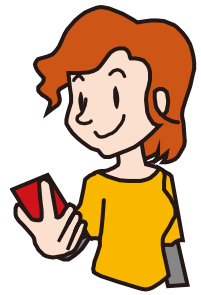


ウイルス・ハッキング
サイバー攻撃

- **概要**
  - 悪意あるスマートフォンアプリを使った電話帳情報の窃取が横行
  - 窃取情報はスパム送信や不正請求詐欺などに悪用され、二次被害が発生する

【6位】悪意あるスマートフォンアプリ
～スマートフォンに保存されているデータが盗み取られています～

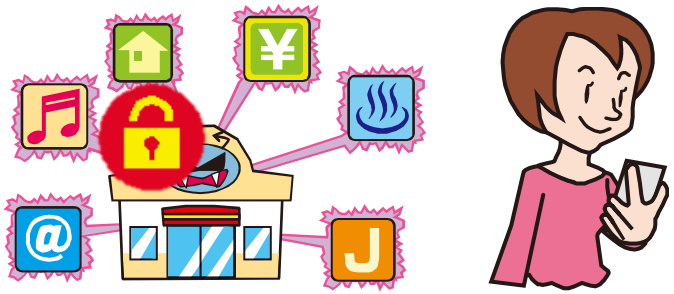
- 攻撃に悪用される背景
  - スマートフォンが急速に普及
  - 好きなアプリをスマートフォンに自由にインストール
  - 電話帳の情報を盗み取る悪意のあるアプリ
  - スマートフォンもPCと同様にマルウェアのターゲットに



- 2013年の事例／統計
  - モバイルマルウェアの爆発的な増加
    - スマートフォンをターゲットにしたマルウェアが1年で614％増加
  - 81万人のデータ抜き取り
    - 偽「ウイルス対策」アプリで電話帳データが約3,700万人分の抜き取った犯人逮捕。メールで自身が運営するサイトを宣伝、約3億8,900万円を売上

【6位】悪意あるスマートフォンアプリ
～スマートフォンに保存されているデータが盗み取られています～

- **対策一覧**
  - スマートフォンのOSとアプリは常に最新の状態に更新
  - アプリは信頼できる場所から、ユーザーレビュー／評価を確認してインストール
  - Android端末では、「提供元不明のアプリ」はインストールしない設定に
  - Android端末では、アプリをインストールする際にアクセス許可を確認
  - セキュリティ対策ソフトを利用



アプリをインストールする前にアクセス許可を確認！

【7位】SNSへの軽率な情報公開
～悪乗りや失言が社会問題に～

インターネットモラル

- **概要**
  - ブログやSNS（ソーシャルネットワーキングサービス）は、自己表現やコミュニケーションのツールとして普及
  - 一方で、従業員の投稿によって企業・組織が損害を受ける事例が問題に

【7位】SNSへの軽率な情報公開
～悪乗りや失言が社会問題に～

- 攻撃に悪用される背景
  - SNSユーザーの自己顕示欲の増長
  - 投稿内容の予想外の情報拡散
  - 公開範囲の誤認識

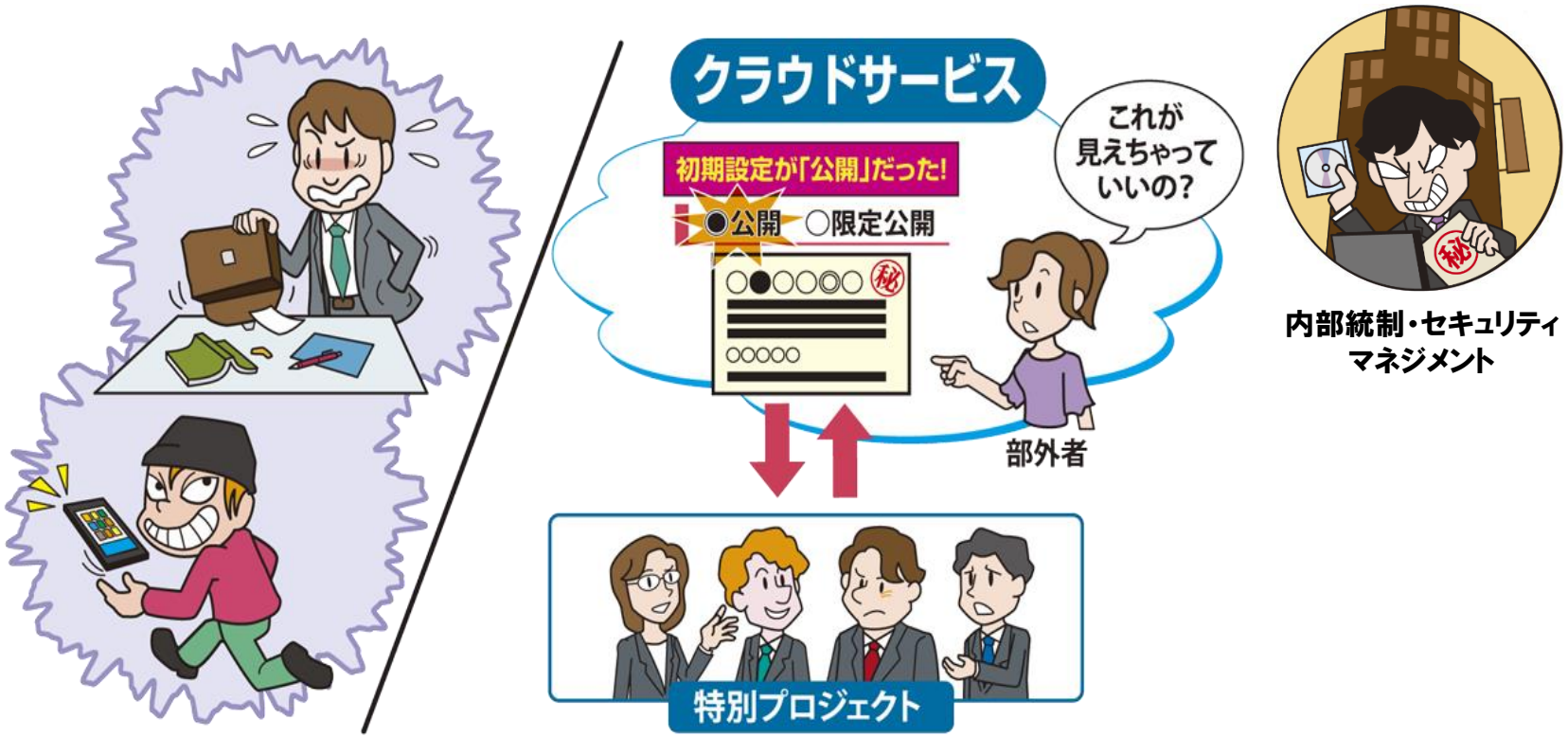
- 2013年の事例／統計
  - Twitterで馬鹿げた写真を公開「バカッター」が社会問題に
    - コンビニの冷凍ケースに入っている写真をTwitterに投稿した事例を皮切りに、多くの事例が注目され問題に
  - 官僚による不適切な発言
    - 不適切な発言をTwitterに投稿した官僚に30日間の停職処分
    - ブログで不適切な暴言や批判をしていた官僚に2ヶ月の停職処分

【7位】SNSへの軽率な情報公開
～悪乗りや失言が社会問題に～

- 対策一覧
  - 個人ユーザーのモラル向上
    - 社会通念やモラルを意識してSNSを利用する
  - 企業・組織での教育
    - 不適切な投稿が損害を招く可能性を周知
  - SNS利用ポリシーの規定
    - 業務に関係する情報を投稿しないなどのポリシーを定める

教育やポリシーで問題発生前から対策を

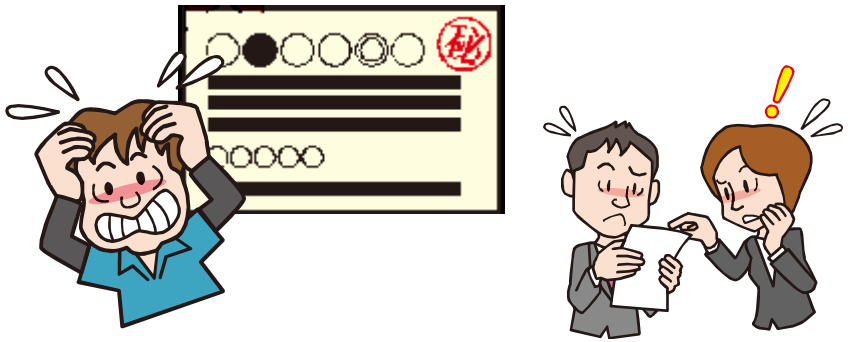
【8位】紛失や設定不備による情報漏えい
～管理者によるコントロールが年々困難に～



- **概要**
  - ノートパソコンやUSBメモリなどの紛失による事故は後を絶たない
  - スマートフォンやクラウドサービスなど、新たな情報漏えいの媒介が登場している

【8位】紛失や設定不備による情報漏えい
～管理者によるコントロールが年々困難に～

- 攻撃に悪用される背景
  - 情報を蓄積したパソコンやデバイス等の紛失による情報漏えい
  - 個人所有のスマートフォンやタブレットが急速に普及
  - オフィス機器やクラウドサービスの設定不備が原因の情報漏えいも拡大



- 2013年の事例／統計
  - Googleグループを一般公開
    - 2013年7月、クラウドサービスGoogleグループで情報共有していた情報が、誰でも閲覧できる状態に
  - インターネットから閲覧可能な複合機
    - 2013年11月、インターネットからアクセス可能な複合機の存在を報道機関が指摘

【8位】紛失や設定不備による情報漏えい
～管理者によるコントロールが年々困難に～

- 対策一覧
  - 持ち出しルールや暗号化対策
    - 外部への情報持ち出しにルールと暗号化などのシステム的な対策を
  - BYODの組織ポリシーの徹底
    - 個人が組織に持ち込む機器に対してポリシーを
  - ユーザー教育
    - セキュリティ事故発生の可能性を認識させる
  - 利用するサービスの仕様の理解
    - 仕様の理解が適切な対策に導く
  - アカウント・アクセス権限の管理
    - 適切に利用ユーザーを制限する

オフィス機器にもセキュリティ対策を！
クラウドサービスの利用も注意

【9位】ウイルスを使った詐欺・恐喝

～偽ウイルス対策ソフトや恐喝ソフトによる金銭要求～

ウイルス・ハッキング
サイバー攻撃

- **概要**
  - パソコンをロックして身代金を要求するランサムウェアの被害が増加
  - 感染すると書類や写真など重要なデータにアクセスできなくなる

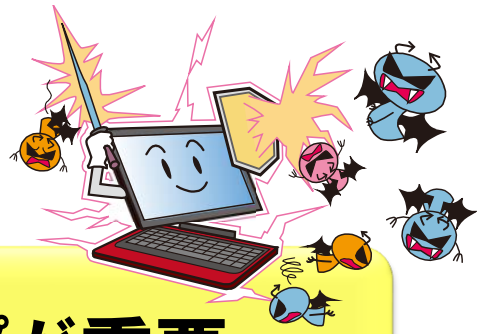
【9位】ウイルスを使った詐欺・恐喝
～偽ウイルス対策ソフトや恐喝ソフトによる金銭要求～

- 攻撃に悪用される背景
  - クレジットカードでの支払いを要求するウイルスが巧妙化
  - 画面のロックやファイルの暗号化など手口がより悪質に

- 2013年の事例／統計
  - ランサムウェアCryptoLockerが登場
    - ファイルを暗号化するランサムウェアCryptoLockerの感染拡大。2013年10月には前月比の3倍を記録
    - ファイル復号鍵とツールを高額（日本円で約300万円）で売りつける

【9位】ウイルスを使った詐欺・恐喝
～偽ウイルス対策ソフトや恐喝ソフトによる金銭要求～

- 対策一覧
  - ウイルス対策ソフトの導入
    - ウイルス対策ソフトでウイルスの感染を防止
  - OS・ソフトウェアの更新
    - Windows Updateの実施と、Adobe製品やJREを定期的に更新
  - データのバックアップ
    - 重要なデータはバックアップを取得、職場で共有しているネットワークドライブも



ウイルス対策とデータのバックアップが重要

【10位】サービス妨害

～妨害手口はさまざま、気づかず加担することもある～

ウイルス・ハッキング
サイバー攻撃

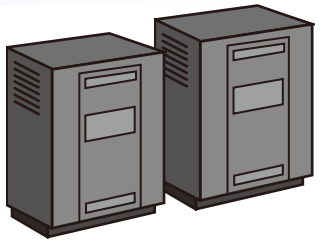
- **概要**
  - システム破壊やネットワーク逼迫によってサービスや業務が停止
  - ウイルス感染などにより分散型サービス妨害（DDoS）攻撃に加担してしまう場合もある

【10位】サービス妨害
～妨害手口はさまざま、気づかず加担することもある～

- 攻撃に悪用される背景
  - ITの普及と依存度が日増しに拡大
  - システム破壊やネットワーク帯域の逼迫で業務遂行不能な状態に

- 2013年の事例／統計
  - 韓国で発生したサイバー攻撃
    - 2013年3月20日、韓国の複数の企業の数万台のパソコンが、マルウェアの攻撃により突如停止、起動できない事態が発生し業務に影響
  - DNSオープンリゾルバを悪用した攻撃
    - オープンリゾルバ状態のDNSサーバーを悪用して、大量の応答パケットを送りつける
    - 米国で100Gbpsのトラフィックが絶え間なく9時間継続観測、史上最大のDDoS攻撃

【10位】サービス妨害
～妨害手口はさまざま、気づかず加担することもある～



- 対策一覧
  - セキュアなサーバーの設定
    - システムの重要度によってはシステムを冗長化構成に
  - 通信制御
    - DDoS攻撃の特徴がある特定の通信をネットワーク機器などでブロック
  - ウイルス対策ソフトの導入
    - ウイルス対策ソフトでウイルスの感染を防止
  - OS・ソフトウェアの更新
    - Windows Updateの実施と、Adobe製品やJREを定期的に更新

ウイルス対策は、被害だけでなく
攻撃に加担しないための重要な対策

目次

- 10大脅威について
- 1章. セキュリティ脅威の分類と傾向
- 2章. 2014年版10大脅威
- **3章. 注目すべき脅威や懸念**

1．ネットワーク対応機器の増加

～サーバーやパソコン以外の機器も攻撃対象に～

- **概要**
  - インターネットに接続できる便利な機器が増加
  - 一方で、セキュリティの甘い機器が狙われ、情報漏えいや乗っ取りなどの被害が発生

1．ネットワーク対応機器の増加

～サーバーやパソコン以外の機器も攻撃対象に～

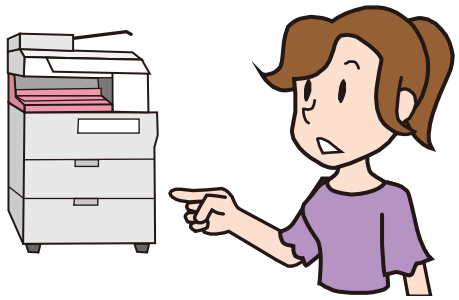
- **インターネット接続機器の増加**
  - ウェブインタフェースにより設定・管理できる、オフィス機器や家電機器が増加（複合機、ウェブカメラ、ネットワーク対応ハードディスク、テレビなど）
  - 機器をインターネットに接続することで、世界中の誰でもアクセスできる状態となり、不正アクセスの危険性

- **実際に起こった事例**
  - 複合機の情報が閲覧可能な状態に
    - 2013年11月、複合機がインターネットからアクセス可能な状態で設置されていると報道機関が指摘、複合機メーカーや業界団体がユーザーへの注意喚起
  - ベビーモニターのハッキング
    - 攻撃者がインターネットから乳児見守り用機器を介して、赤ん坊に罵声を浴びせる事件発生

1．ネットワーク対応機器の増加

～サーバーやパソコン以外の機器も攻撃対象に～

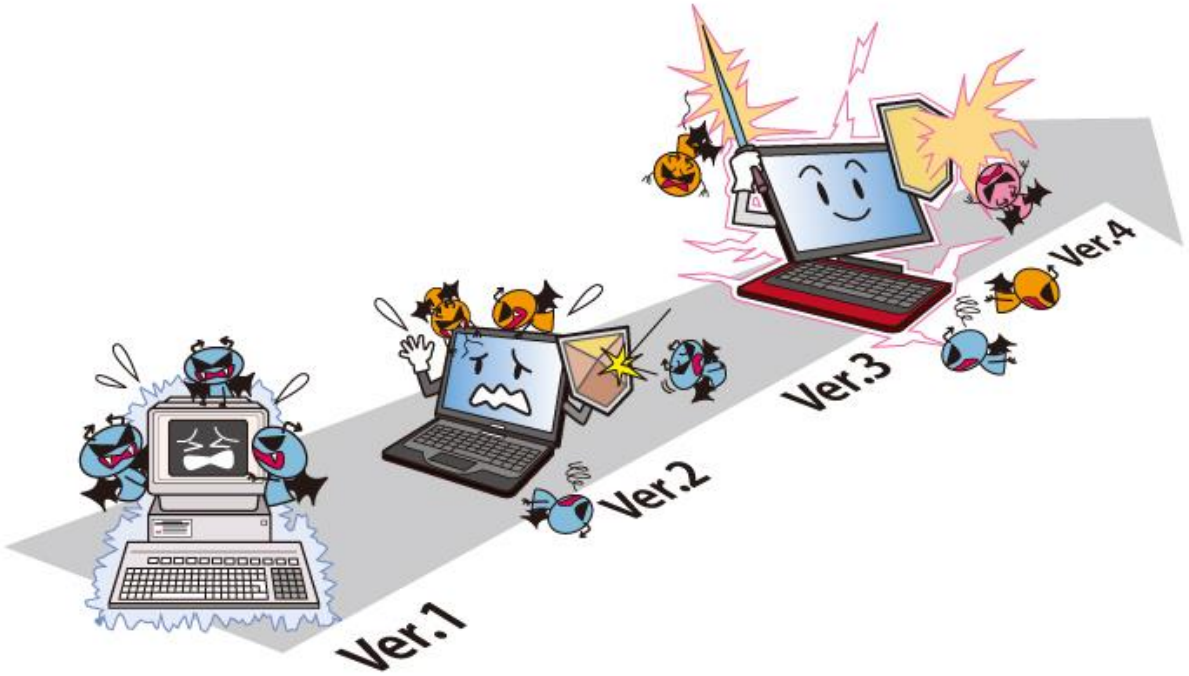
- **ユーザー側の認識不足が要因**
  - ユーザー側で仕様を十分に理解できていない
  - 機器がインターネットに公開されることに気づいていない
  - システム管理部門ではなく総務系の部門などの管理となっている



- **安全に機器を利用する為の注意点**
  - 機器の管理者は、
    - 機器に付属している説明書をよく読み、適切な設定を施す
    - 必要が無い限り機器をインターネットに接続しない
  - ネットワーク管理者は、
    - ファイアウォールやブロードバンドルーターでインターネットから機器への通信を制限する

2. エンドポイントセキュリティの重要性

～最新のソフトウェアを使用することがセキュリティ対策の近道～

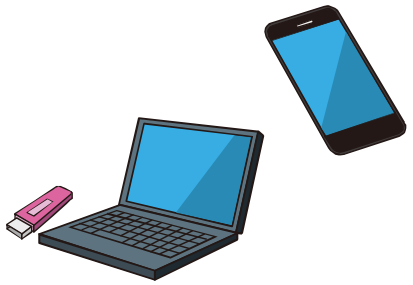


- **概要**
  - ネットとの境界だけでなく、端末自身で防御する必要性拡大
  - 最新バージョンのOSやソフトウェアの使用がエンドポイントセキュリティ強化への近道

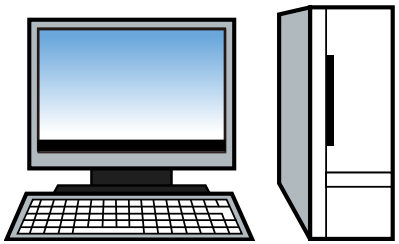
2. エンドポイントセキュリティの重要性

～最新のソフトウェアを使用することがセキュリティ対策の近道～

- **境界防御の限界**
  - 標的型メール攻撃が顕在化、インターネットとの境界での防御に限界があることは明らか
  - PCやスマートフォン等エンドポイントの対策が重要



- **狙われるソフトウェア**
  - Oracle Java(JRE)、Adobe Acrobat/Adobe Reader、Adobe Flash Player、Microsoft Officeなど
  - パソコンを利用する上で欠かせない製品の脆弱性が悪用される



2. エンドポイントセキュリティの重要性

～最新のソフトウェアを使用することがセキュリティ対策の近道～

- **新しいソフトウェアほどセキュリティ機能が強固**
  - OSやアプリケーションベンダーは、継続的にセキュリティ機能を強化
  - Windows XPは11.3%の感染率、Windows 7(32bit)は4.8%に減少
  - その他の製品(Adobe Flash、Adobe Reader、JRE)にも悪用阻止技術あり

- **Windows XPのサポート終了**
  - Windows XPが2014年4月9日(日本時間)をもってサポートを終了
  - サポート終了に伴う影響
    - XP上で稼動するアプリケーションも順次サポート終了
    - 保守サービスの終了
  - 購入コストだけでなくランニングコストも考えて、早期移行が望ましい

3. インターネット利用の低年齢化に伴う問題

～未成年者がネット犯罪の加害者・被害者になってしまう～

- **概要**
  - 掲示板やSNSを利用したいじめが問題に
  - 未成年者がインターネットで犯罪に巻き込まれたり、IT犯罪で補導・書類送検されるケースも続発

3. インターネット利用の低年齢化に伴う問題

～未成年者がネット犯罪の加害者・被害者になってしまう～

- **ITユーザーの低年齢化**
  - 携帯電話・スマートフォンを使用する小学生・中学生が増加
  - オンラインゲームや学習教材、コミュニケーションツール等のコンテンツが充実し、年々利用開始年齢が低下

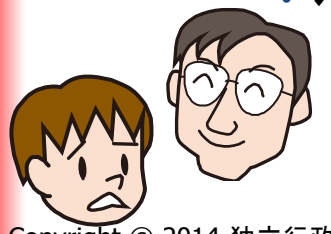
- **インターネットのトラブルや犯罪**
  - 利便性が高い反面、偽名でも利用可能、悪用や誹謗中傷が問題
  - 出会い系サイトでの被害者は、2013年上半期だけで74名
  - 無料通話アプリ「LINE」で、個人情報を教えてしまい、犯罪に巻き込まれる事例も増加
  - 「個人情報を教えない」「安易に見知らぬ人と会わない」等、若年層からの教育が必要

3. インターネット利用の低年齢化に伴う問題

～未成年者がネット犯罪の加害者・被害者になってしまう～

- **保護者への高額請求**
  - 子供がゲームのアイテムを購入し、保護者に高額請求される事例が増加
  - 国民生活センターへの相談件数が、2013年3,000件超
    - 「高校2年生の息子が、約60万円分のアイテムを購入」
    - 「孫がクレジットカードを勝手に使い、オンラインゲーム会社から20万円弱の高額請求」

- **IT犯罪の低年齢化**
  - **被害者ではなく加害者になる事件も増加**
    - 同級生のID/パスワードを使って不正アクセスした12歳の児童が補導
    - ウイルス作成などのITの専門知識を有した行為も確認
  - **幼少期や中高生にも教育や対策を**
    - 保護者が適切なインターネット利用について理解し、子供と会話を
    - ペアレンタルコントロール機能を活用することも有効



おわりに

- ITの普及により、
  脅威はより身近なものに
- 脅威を理解することが、
  情報セキュリティの強化に繋がる

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