IPA Better Life with IT

「情報セキュリティ10大脅威 2015」

～被害に遭わないために実施すべき対策は？～

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
2015年3月

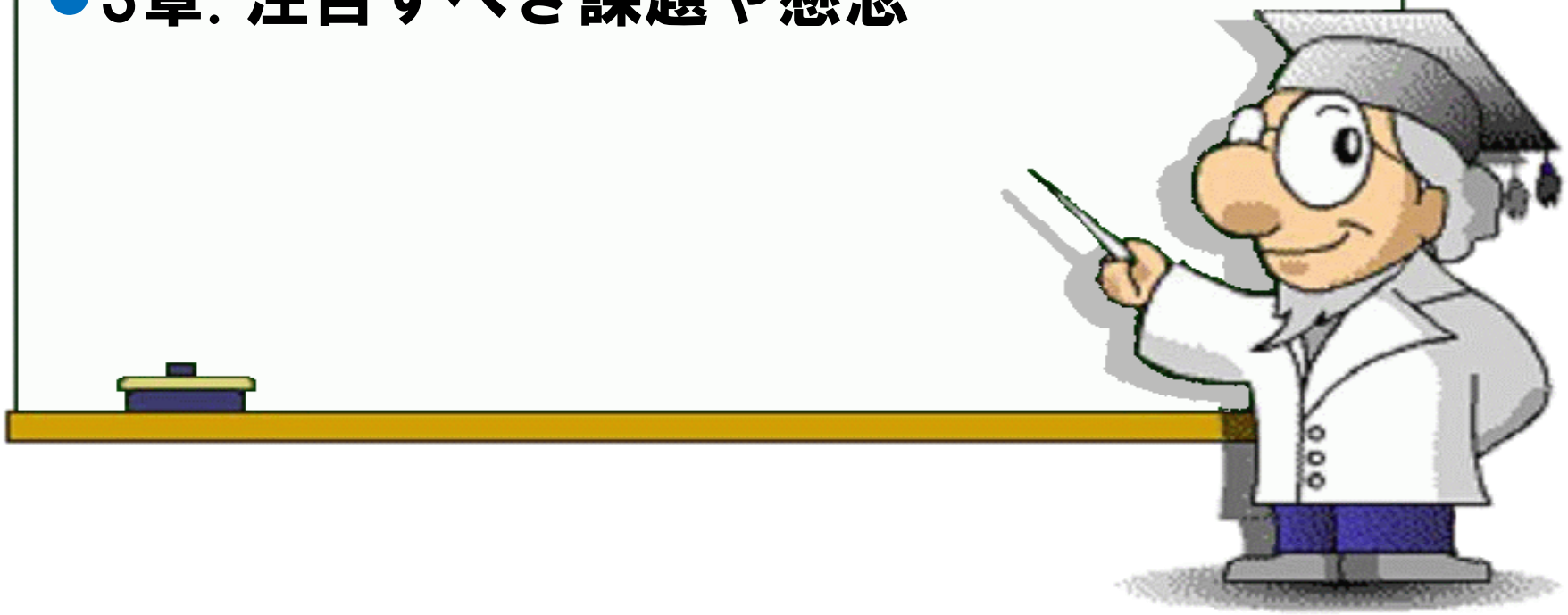
本資料に関する詳細な内容は

- 以下のページのPDF資料をご確認ください。
  本資料は要約です。

情報セキュリティ10大脅威 2015
https://www.ipa.go.jp/security/vuln/10threats2015.html

目次

- 情報セキュリティ10大脅威について
- 1章. 情報セキュリティ対策の基本
- 2章. 情報セキュリティ10大脅威 2015
- 3章. 注目すべき課題や懸念



情報セキュリティ10大脅威 2015

https://www.ipa.go.jp/security/vuln/10threats2015.html

- 10大脅威とは？
  - 2006年よりIPAが毎年発行している資料
  - 「10大脅威執筆者会」約100名の投票により、情報システムを取巻く脅威を順位付けして解説

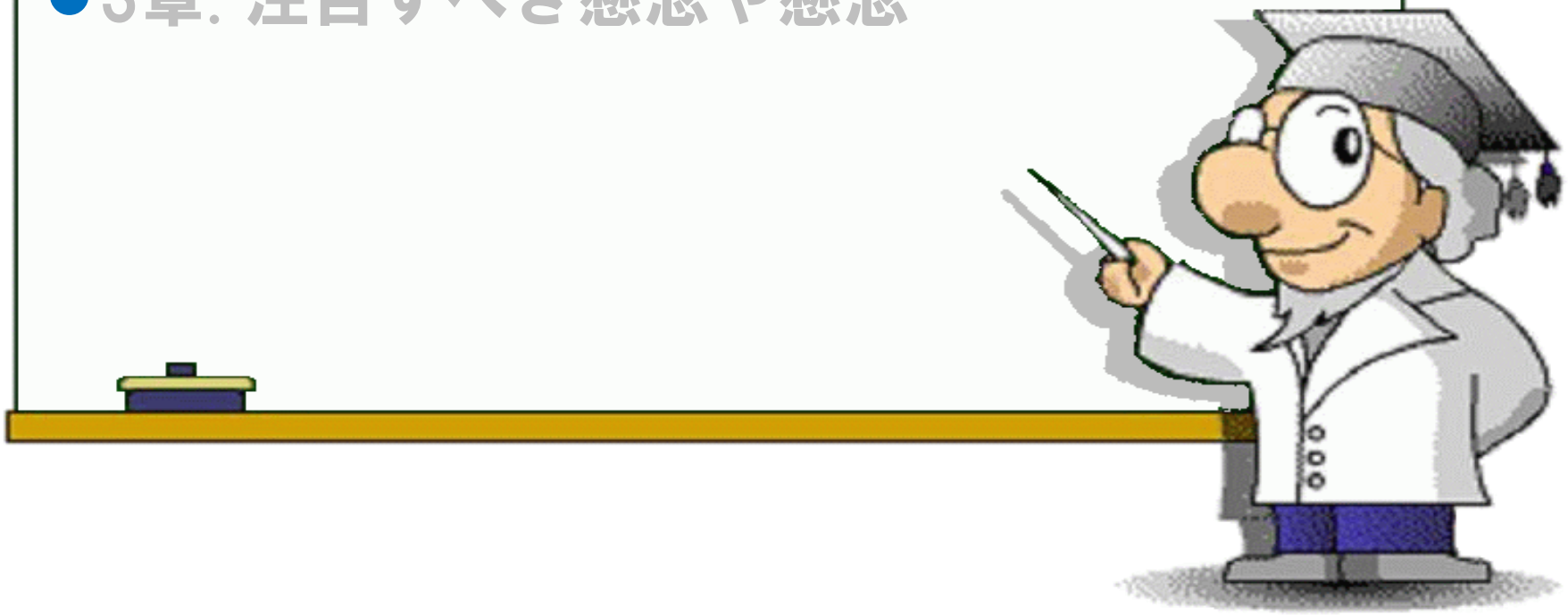
情報セキュリティ10大脅威 2015

https://www.ipa.go.jp/security/vuln/10threats2015.html

- 章構成
  - 1章.情報セキュリティ対策の基本
    - 被害を防ぐための基本的な対策を解説
  - 2章.情報セキュリティ10大脅威 2015
    - 10の脅威の概要と対策について解説
  - 3章.注目すべき課題や懸念
    - 知っておくべき課題や懸念を解説

目次

- 情報セキュリティ10大脅威について
- **1章. 情報セキュリティ対策の基本**
- 2章. 情報セキュリティ10大脅威 2015
- 3章. 注目すべき懸念や懸念

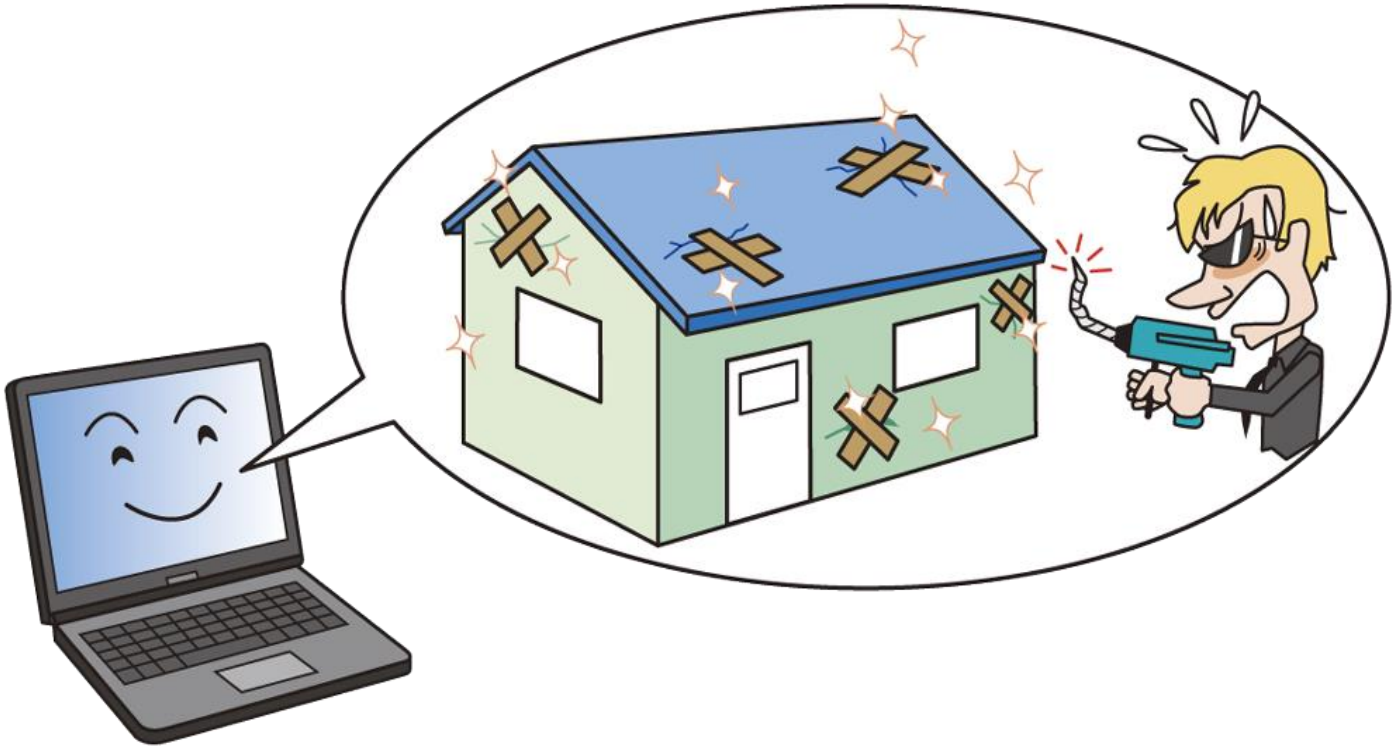


情報セキュリティ対策の基本

情報セキュリティ対策の基本
ソフトウェアの更新
ウイルス対策ソフトの導入
パスワード・認証の強化
設定の見直し
脅威・手口を知る

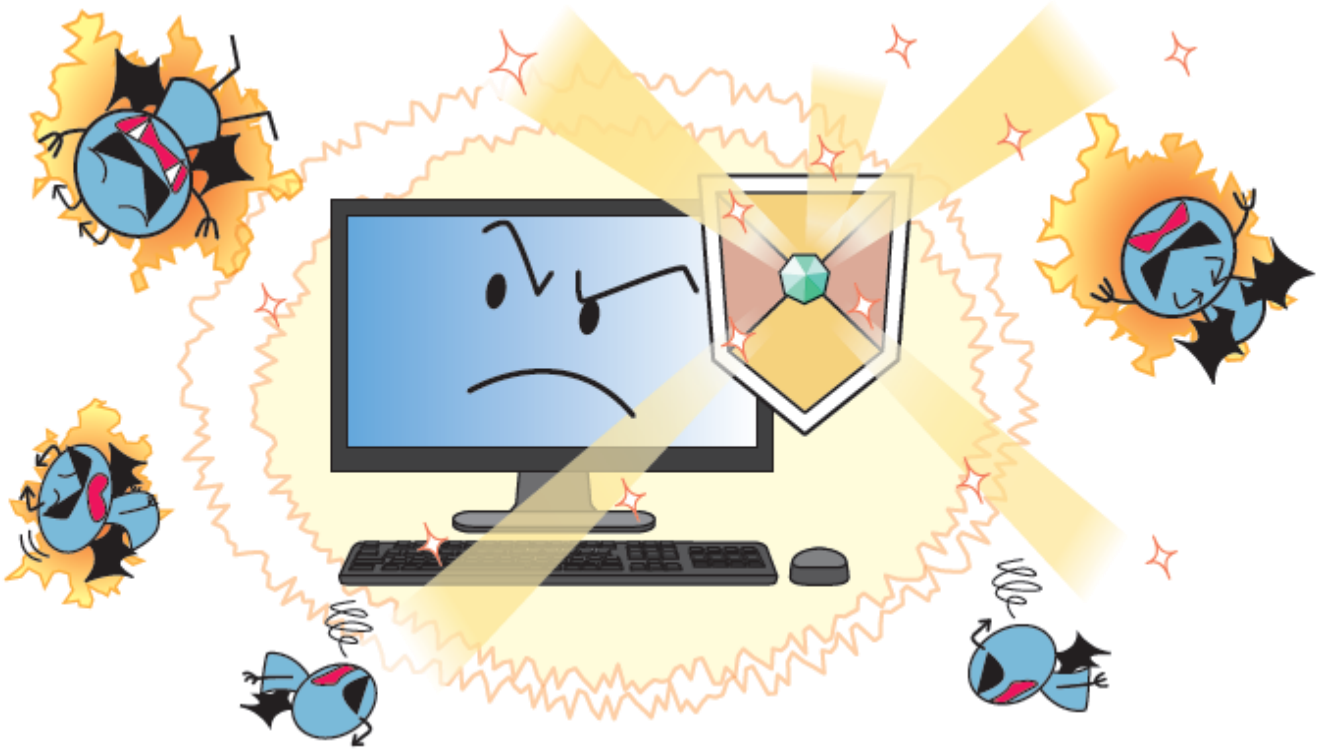
10大脅威の順位は毎年変動するが、
上記の基本的な対策の必要性は長年変わらない
IT利用者には「自発的な対策の実施」が求められている

ソフトウェアの更新



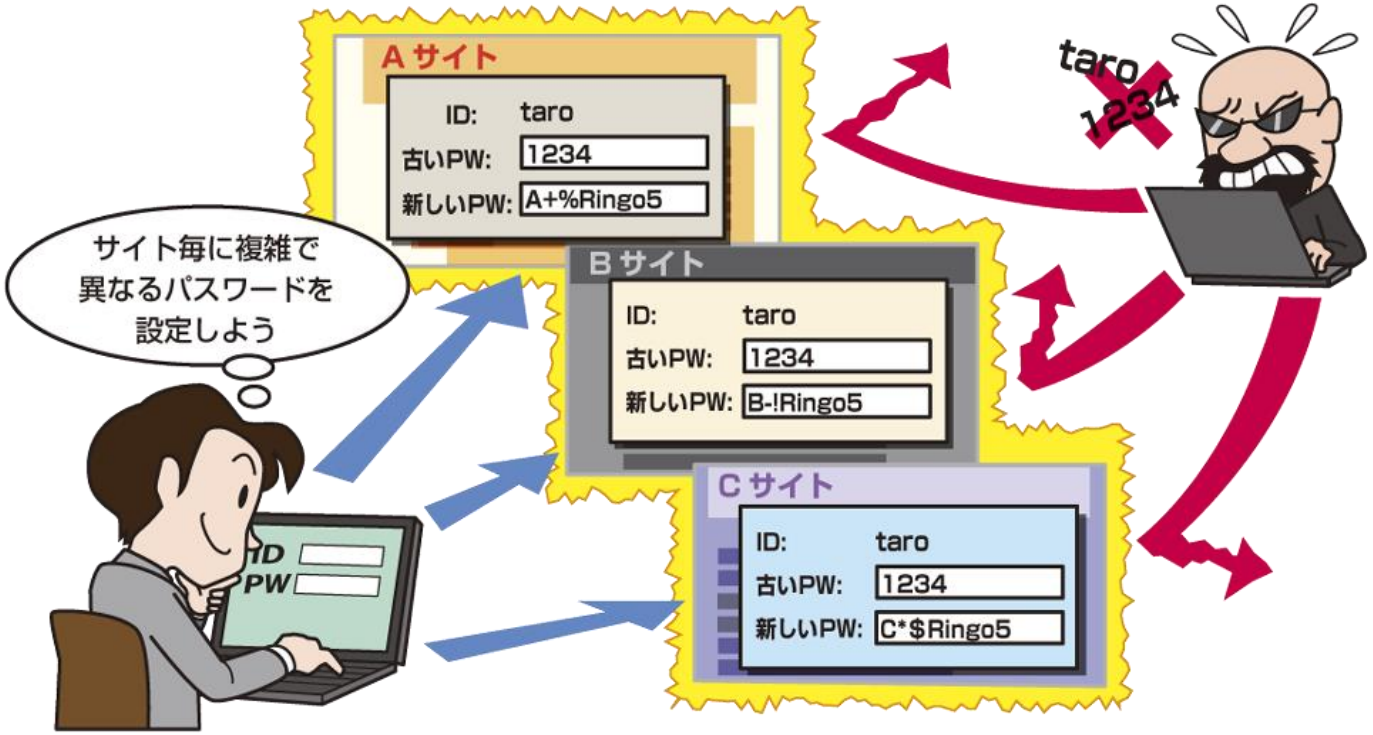
- ソフトウェアの欠陥である脆弱性は、
  ソフトウェアを更新して根本的に解消する

ウイルス対策ソフトの導入



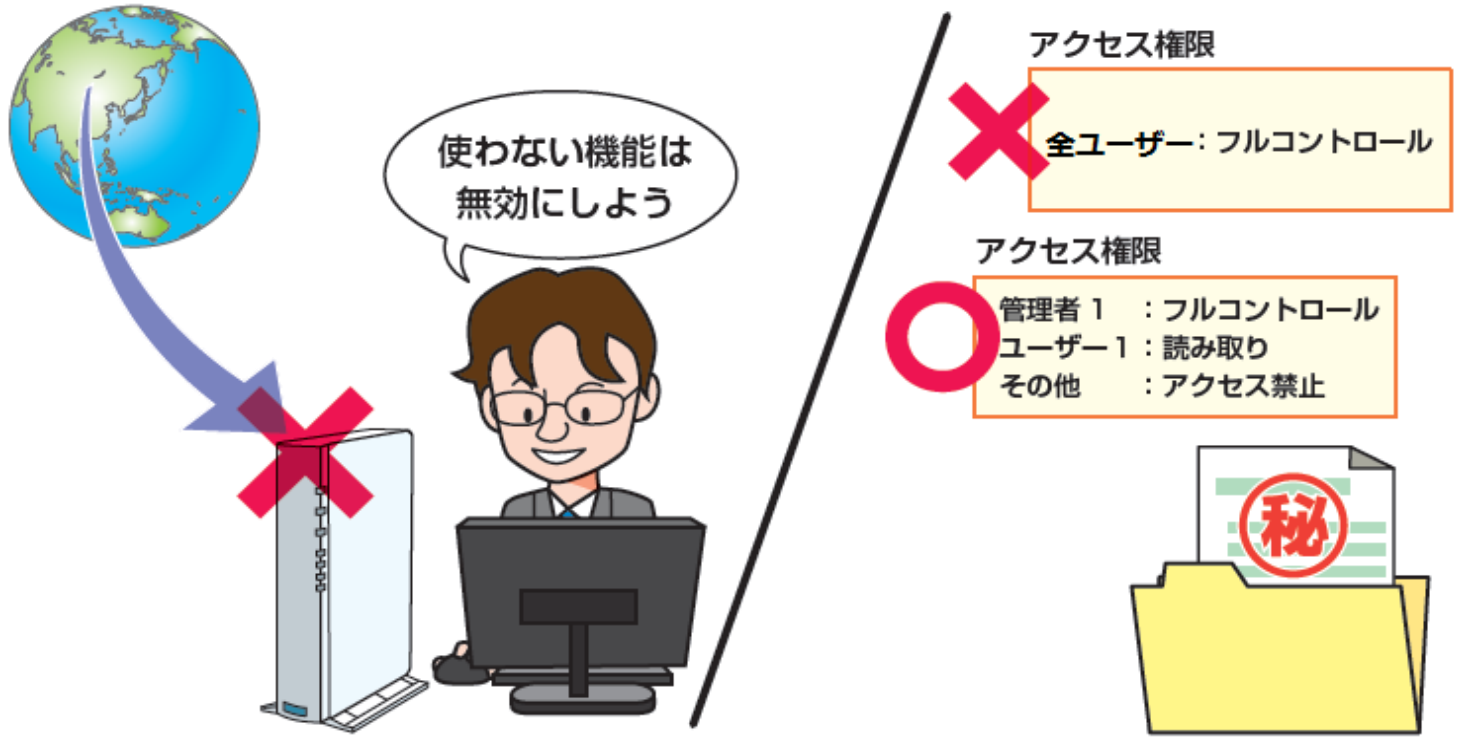
- ウイルス対策ソフトを導入し、
  流行しているウイルスの感染を未然に防ぐ

パスワードの適切な管理と認証の強化



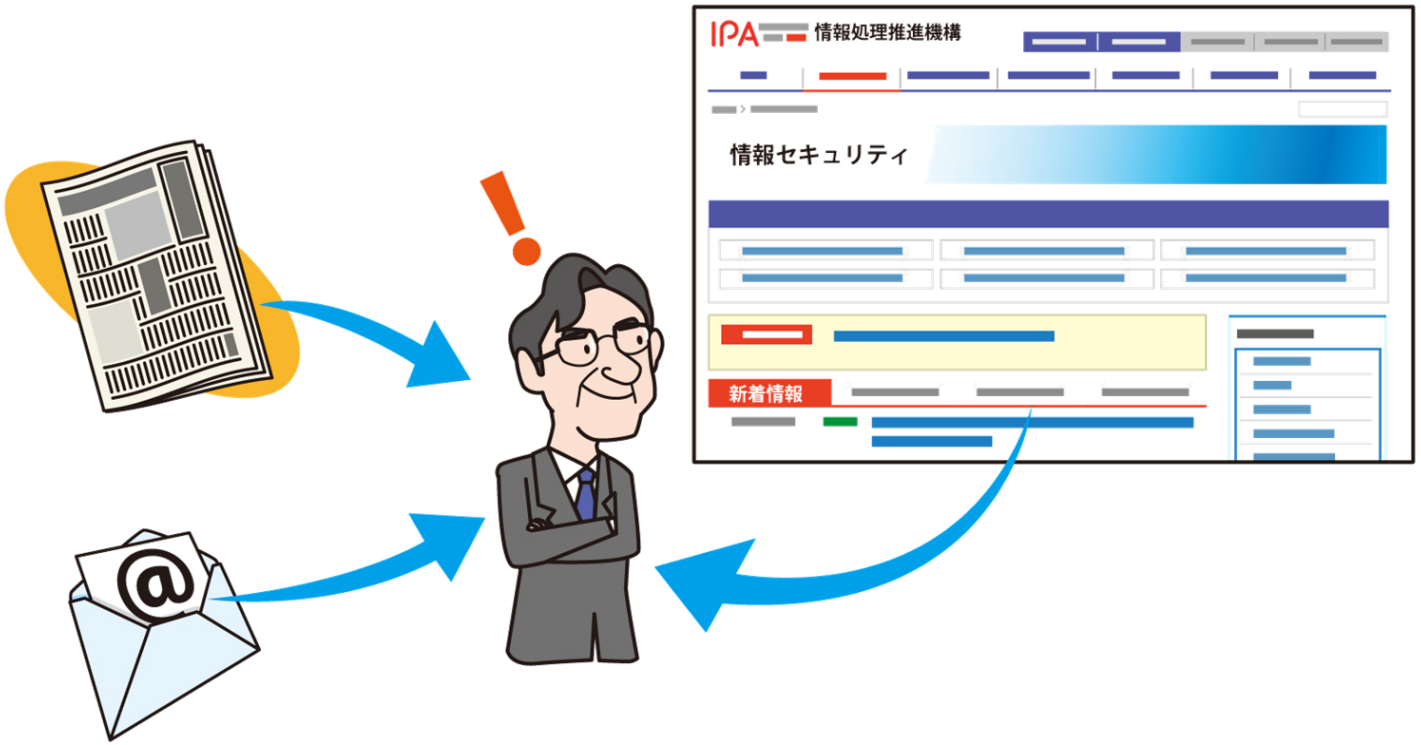
- 推測されにくい
  「記号・英数字」を含む「十分な文字数」のパスワードを設定
- 複数のウェブサービスでパスワードを使い回さない
- 二要素認証等、強い認証方式が利用できれば利用する

設定の見直し



- 不要な設定は無効にする
- フォルダや顧客管理システム等への
  アクセス制限を適切に行う

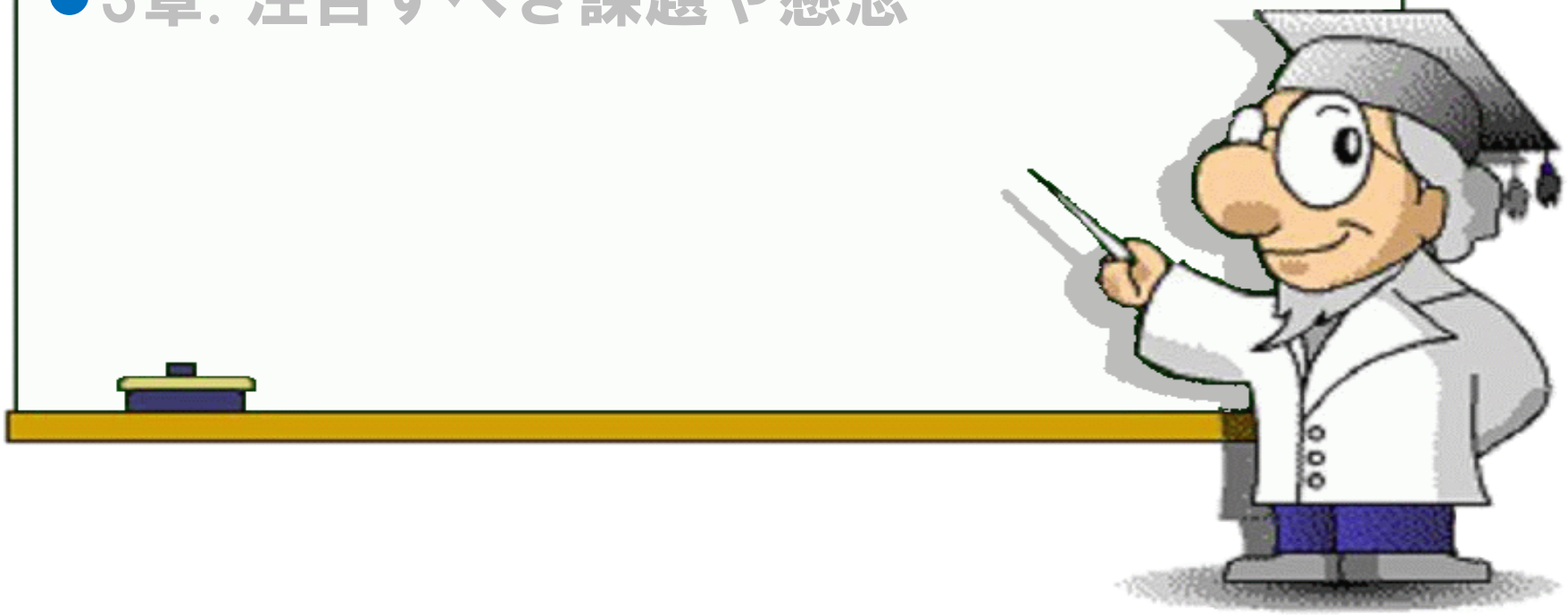
脅威や手口を知る



- 新聞やインターネット等から情報を自発的に収集し、被害に遭わないよう手口を事前に知る

目次

- 情報セキュリティ10大脅威について
- 1章. 情報セキュリティ対策の基本
- **2章. 情報セキュリティ10大脅威 2015**
- 3章. 注目すべき課題や懸念



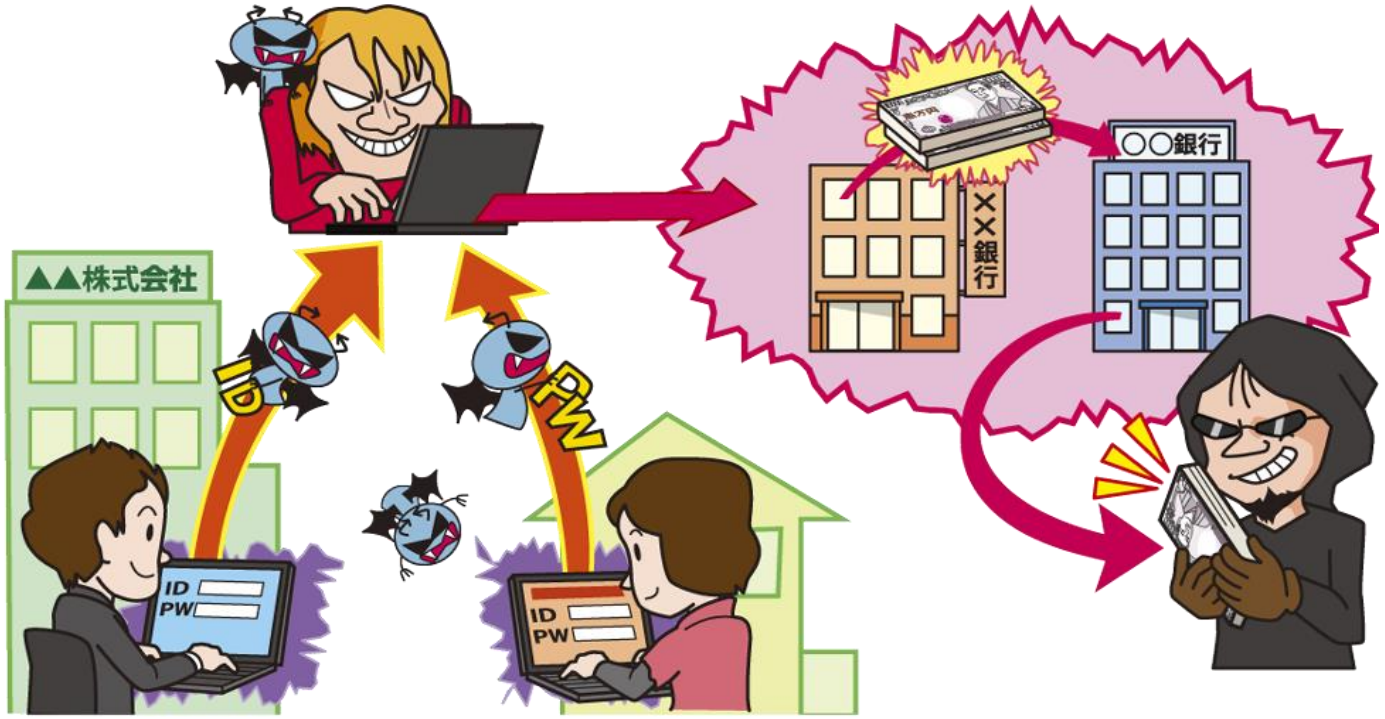
情報セキュリティ10大脅威 2015

IPA

順位	脅威
1位	インターネットバンキングや クレジットカード情報の不正利用
2位	内部不正による情報漏えい
3位	標的型攻撃による諜報活動
4位	ウェブサービスへの不正ログイン
5位	ウェブサービスからの顧客情報の窃取
6位	ハッカー集団によるサイバーテロ
7位	ウェブサイトの改ざん
8位	インターネット基盤技術を悪用した攻撃
9位	脆弱性公表に伴う攻撃
10位	悪意のあるスマートフォンアプリ

【1位】インターネットバンキングやクレジットカード情報の不正利用

～個人口座だけではなく法人口座もターゲットに～

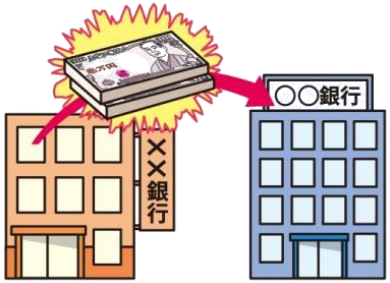


- ウイルスやフィッシング詐欺により認証情報が窃取され、不正送金される

【1位】インターネットバンキングやクレジットカード情報の不正利用

～個人口座だけではなく法人口座もターゲットに～

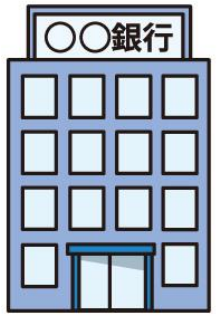
- 手口や影響
  - ウイルスに感染したパソコンが不正送金の被害に遭う
  - フィッシング詐欺により入力した認証情報が窃取される
- 2014年の事例／統計
  - 不正送金被害が急増
    - 日本のインターネットバンキング利用者を狙う
      ウイルスが横行！
    - 2014年の被害額は29億1,000万円、
      2013年の約2倍に！
      法人口座の被害が急増！



【1位】インターネットバンキングやクレジットカード情報の不正利用

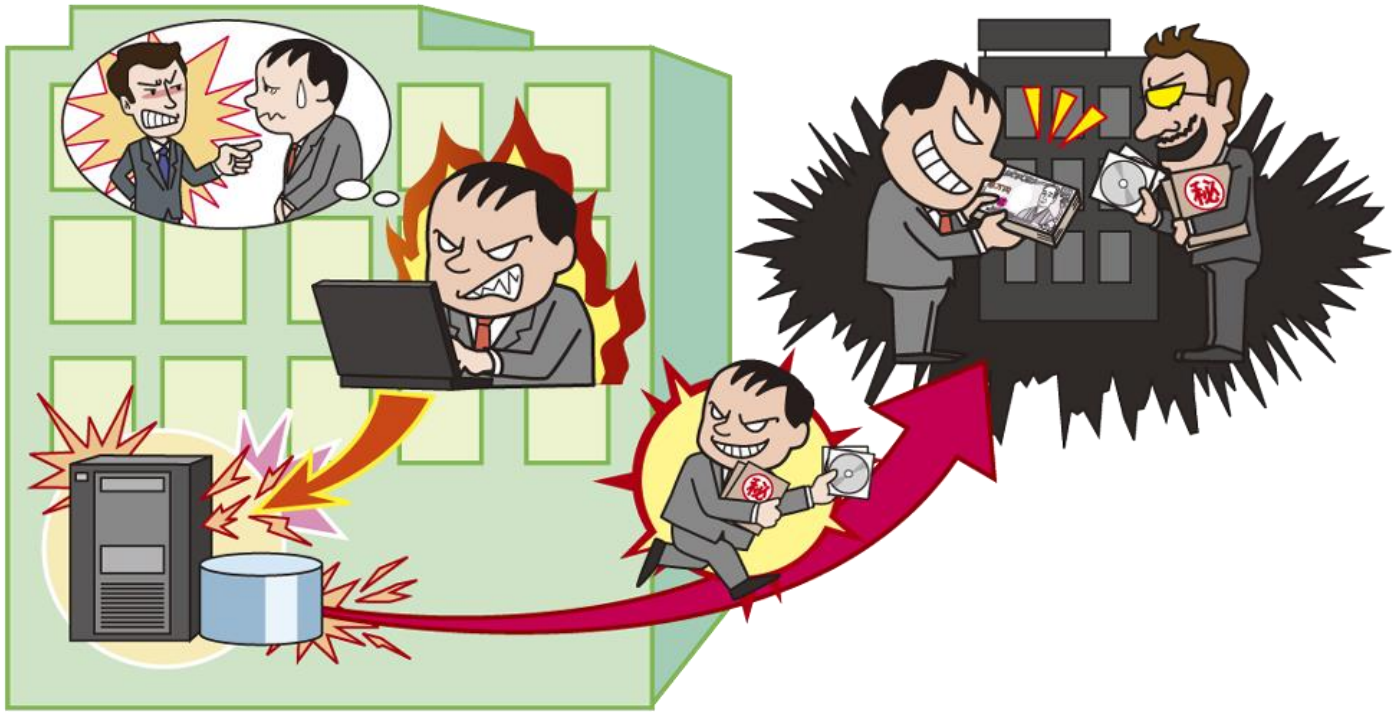
～個人口座だけではなく法人口座もターゲットに～

- **対策一覧**
  - **利用者**
    - ソフトウェアの更新
    - ウイルス対策ソフトの導入
    - 事例や手口を知る
    - 二要素認証等の強い認証方式の利用
  - **銀行/カード運営会社**
    - 利用者への事例や手口の情報提供
    - 二要素認証等の強い認証方式の提供



銀行が提供する二要素認証や
専用のウイルス対策ソフトがあれば活用！

【2位】内部不正による情報漏えい
～内部不正が事業に多大な悪影響を及ぼす～



- 従業員・職員が故意に内部情報を持ち出し私的に利用
- 企業・組織の信用が失墜し、補償・賠償が求められる

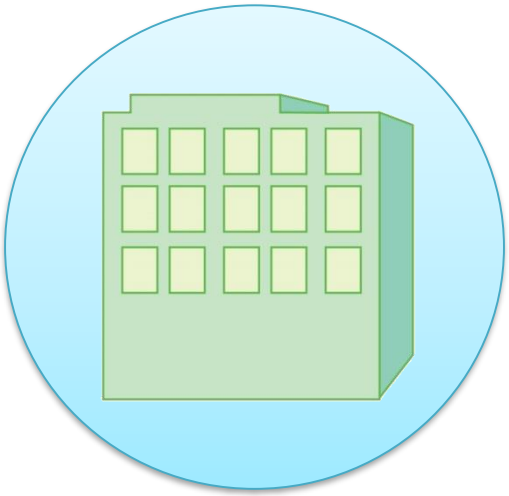
【2位】内部不正による情報漏えい
～内部不正が事業に多大な悪影響を及ぼす～

- 発生要因
  - 動機　　：処遇の不満、借金による生活苦
  - 機会　　：不正行為ができる環境
  - 正当化　：自分勝手な理由づけ

- 2014年の事例／統計
  - 通信教育大手から膨大な個人情報が漏えい
    - 委託先企業の社員が3,504万件の個人情報を持ち出し
    - 被害企業は顧客に総額200億円の補償を発表

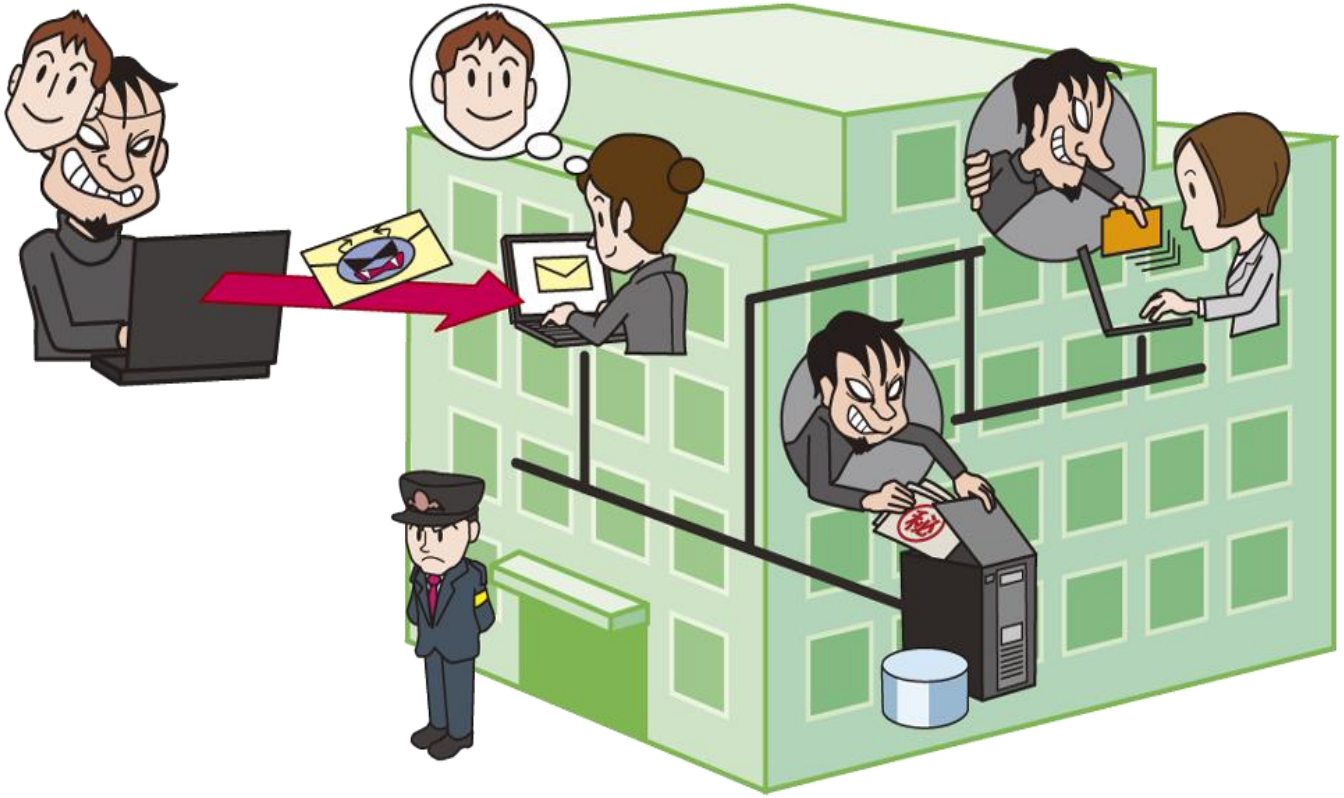
【2位】内部不正による情報漏えい
～内部不正が事業に多大な悪影響を及ぼす～

- 対策一覧
  - 経営者層
    - 就業規則およびセキュリティポリシーの整備
    - 職員や委託先との秘密保持誓約の徹底
    - 対策を推進するための体制の構築
  - システム管理者
    - 資産の把握と重要度による分類
    - アカウントや権限の管理（設定・抹消）
    - システム操作の記録と監視
    - 入退室の監視や持込み物等の確認



組織一丸となって積極的に対策を推進する体制を

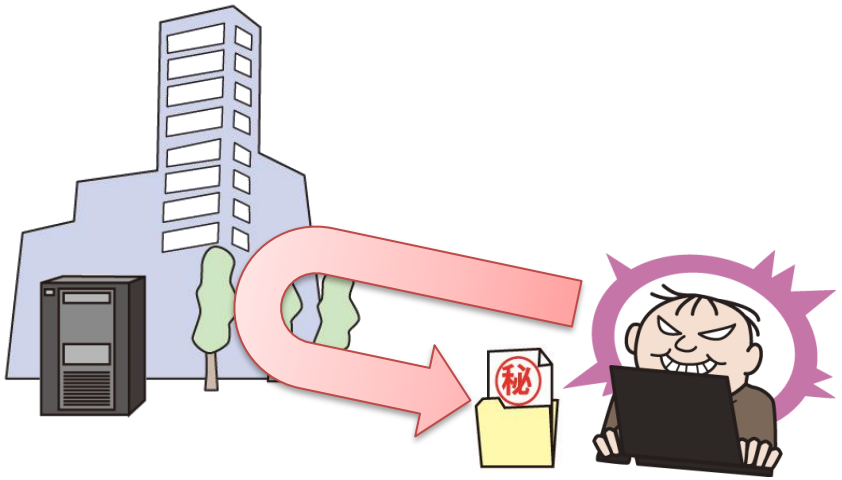
【3位】標的型攻撃による諜報活動
～標的組織への侵入手口が巧妙化～



- ネット経由のスパイ活動により企業・組織の情報が流出
- 取引先や関連会社を踏み台にして本丸を狙う傾向あり

【3位】標的型攻撃による諜報活動
～標的組織への侵入手口が巧妙化～

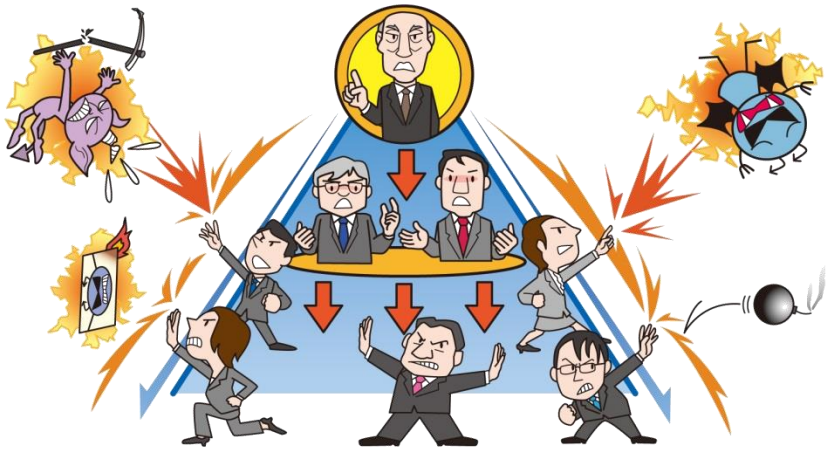
- 侵入手口
  - メールからウイルス感染「ばらまき型」「やり取り型」
  - ウェブからウイルス感染「水飲み場型」
  - 標的組織の関連会社が踏み台に



- 2014年の事例／統計
  - 「やり取り型」の顕在化
    - 問い合わせ窓口が狙われる
    - メールのやり取りの後、ウイルス入りのメールを送る手口

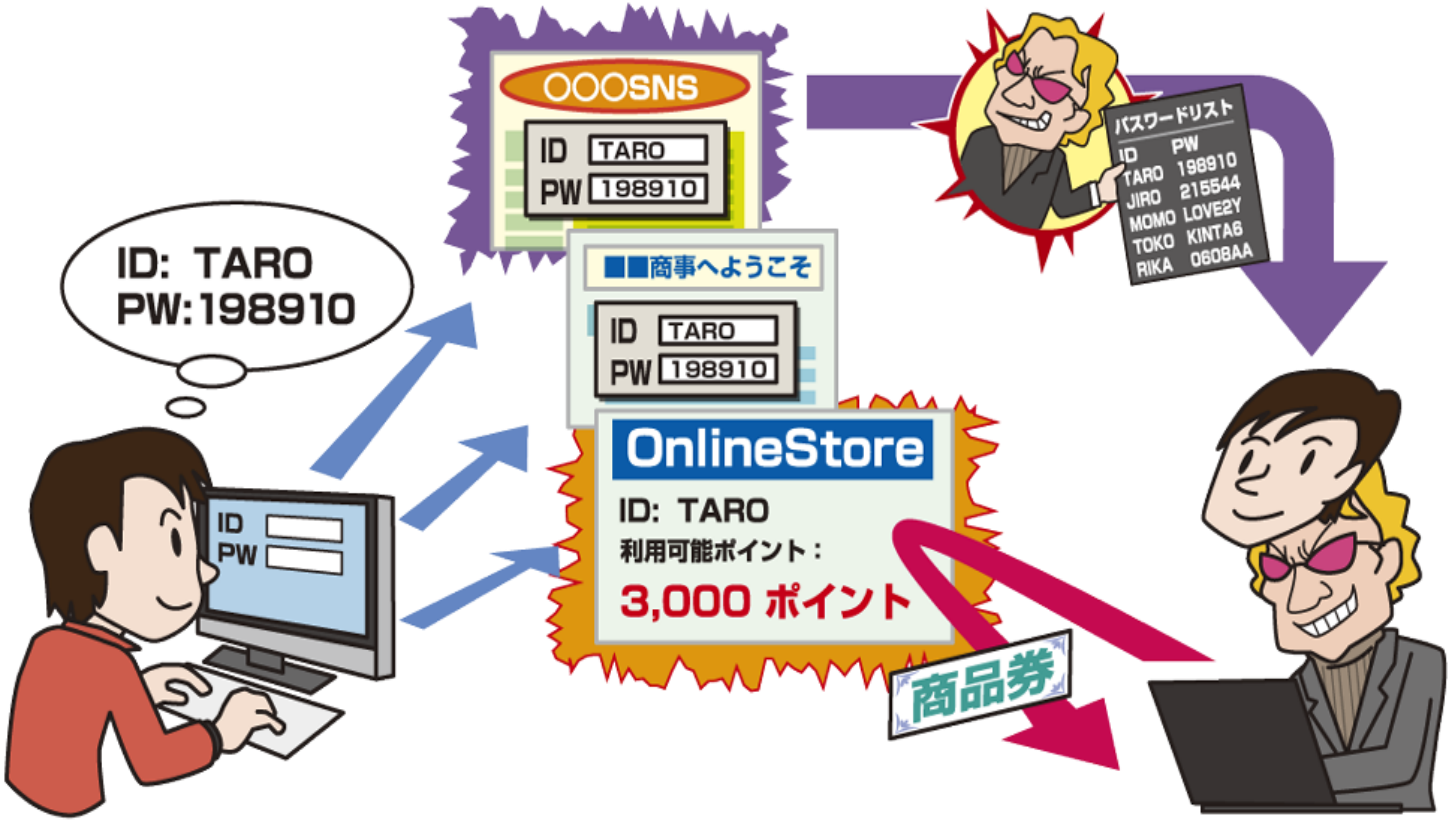
【3位】標的型攻撃による諜報活動
～標的組織への侵入手口が巧妙化～

- 対策一覧
  - 経営者層
    - 問題に迅速に対応できる体制の構築
  - セキュリティ担当部署
    - セキュリティ教育の実施
  - システム管理者
    - システム設計対策
    - アクセス制限
    - ネットワークの監視



内部へ侵入されることを想定した多層防御を

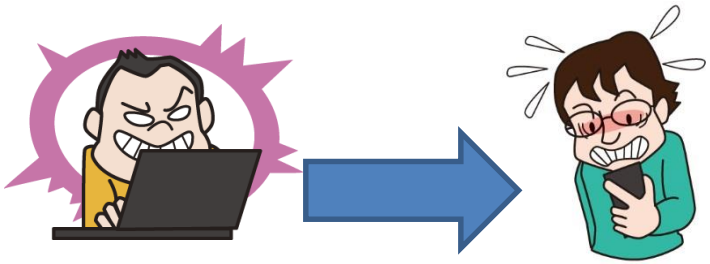
【4位】ウェブサービスへの不正ログイン
～利用者は適切なパスワード管理を～



- パスワードを窃取されウェブサービスを不正利用される
- 複数サービスでパスワードを使い回すユーザーが被害に

【4位】ウェブサービスへの不正ログイン
～利用者は適切なパスワード管理を～

- 手口と影響
  - パスワードの推測
  - パスワードの窃取（ウイルス感染、別サービスから窃取）
  - サービスに不正ログインされ、
    個人情報の窃取やポイントを不正利用される
- 2014年の事例／統計
  - SNSサービスへの不正ログイン
    - アカウントが乗っ取られる事件が多発
    - 攻撃者は友人になりすまし、プリペイドカードの購入を依頼



【4位】ウェブサービスへの不正ログイン
～利用者は適切なパスワード管理を～

- 対策一覧
  - ウェブサービス利用者
    - 推測されにくいパスワードを設定する
    - パスワードを使い回さない
    - 二要素認証等の強い認証方式の利用
  - サービス提供者
    - 安全なウェブサービスの提供
    - 複雑なパスワード設定を要求
      （少ない文字数の拒否、記号の使用の確認等）
    - 二要素認証等の強い認証方式の提供

**パスワードは推測されにくいものを設定し、
複数のサービスで使い回さない**

【5位】ウェブサービスからの顧客情報の窃取

～脆弱性や設定の不備を突かれ顧客情報が盗まれる～

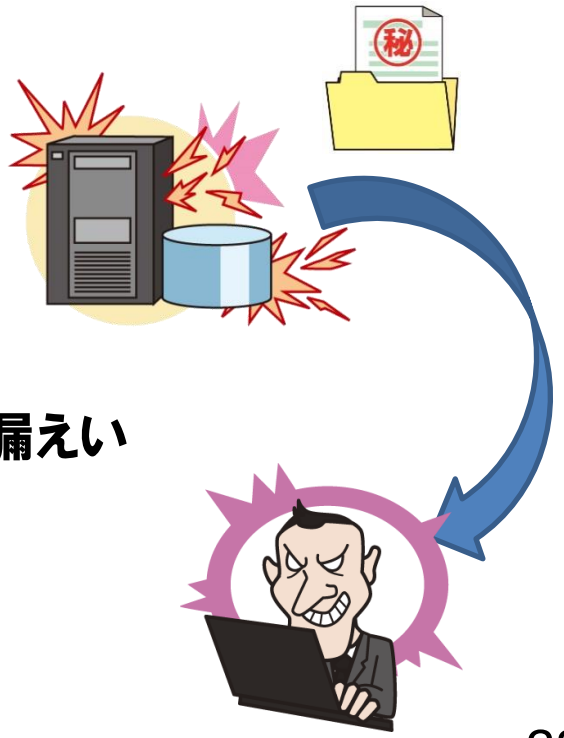
- ウェブサービスから個人情報が窃取される事件が多発
- クレジットカード情報が窃取されると金銭被害に発展

【5位】ウェブサービスからの顧客情報の窃取

～脆弱性や設定の不備を突かれ顧客情報が盗まれる～

- 手口や影響
  - ソフトウェアやウェブアプリケーションの脆弱性を悪用
  - リモート管理用のサービスからの侵入
  - 顧客情報の窃取やその情報の悪用

- 2014年の事例／統計
  - OpenSSLの脆弱性を狙った攻撃
    - カード会社が使用する
      暗号化通信ソフト（OpenSSL）の脆弱性を
      悪用し、894件のクレジットカード情報が漏えい

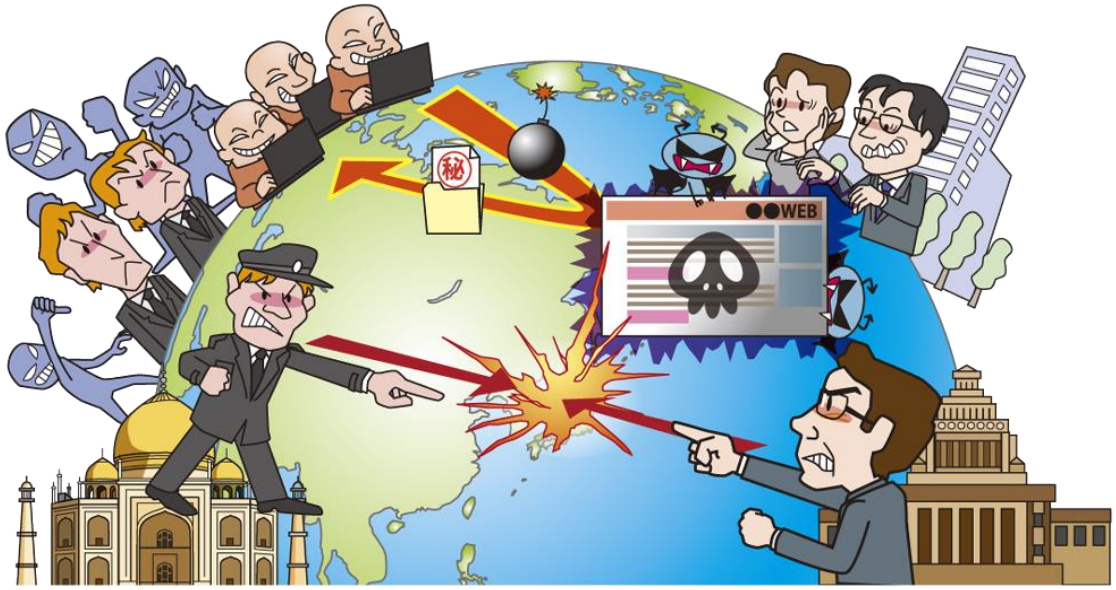


【5位】ウェブサービスからの顧客情報の窃取
～脆弱性や設定の不備を突かれ顧客情報が盗まれる～

- 対策一覧
  - ウェブサービス運営者
    - 安全なウェブサービスの構築
    - ソフトウェアの更新

安全なウェブサービスの構築は
セキュリティを担保した設計と開発が必要

【6位】ハッカー集団によるサイバーテロ
～破壊活動や内部情報の暴露を目的としたサイバー攻撃～



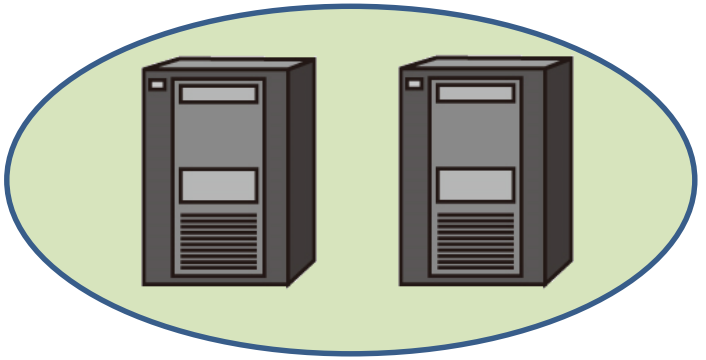
- 企業・組織にダメージを与えることを目的とした攻撃
- システムの破壊や内部情報の暴露により信用が失墜

【6位】ハッカー集団によるサイバーテロ
～破壊活動や内部情報の暴露を目的としたサイバー攻撃～

- 手口と影響
  - 脆弱性や標的型攻撃メール等により侵入され、ウェブ改ざん、システム破壊、情報窃取の被害に遭う
  - 信用の失墜やビジネス機会の損失につながる
- 2014年の事例／統計
  - 米国の映像メディア企業が標的に
    - メールや映像コンテンツ等が漏えい
    - 内部の業務システムに影響
    - 米国政府は北朝鮮によるサイバー攻撃と公表

【6位】ハッカー集団によるサイバーテロ
～破壊活動や内部情報の暴露を目的としたサイバー攻撃～

- 対策一覧
  - 経営者層
    - リスクマネジメント体制の構築
  - セキュリティ担当部署
    - セキュリティ教育の実施
  - システム管理者
    - 安全なシステム設計
    - アクセス権限の管理・アクセス制御
    - データの保護・暗号化
    - バックアップ



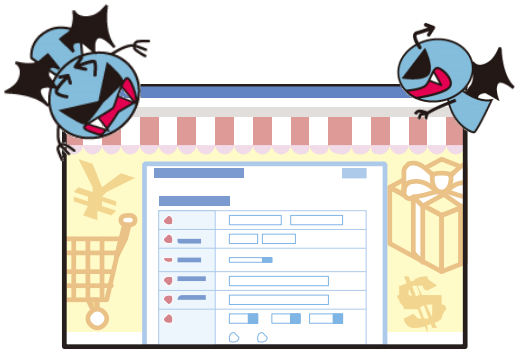
システムの復旧のためのバックアップや冗長化等、インシデント発生を想定した準備も重要

【7位】ウェブサイトの改ざん
～知らぬ間に、ウイルス感染サイトに仕立てられる～

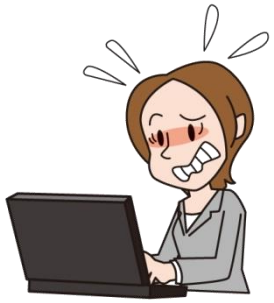
- ウェブサイトを改ざんされてウイルス感染に悪用される
- サイト運営者はウイルス感染に加担した加害者側に

【7位】ウェブサイトの改ざん
～知らぬ間に、ウイルス感染サイトに仕立てられる～

- 手口と影響
  - ソフトウェアやウェブアプリケーションの脆弱性を悪用
  - リモート管理用のサービスからの侵入
  - ウイルス感染や
    主義主張・自己顕示に悪用される

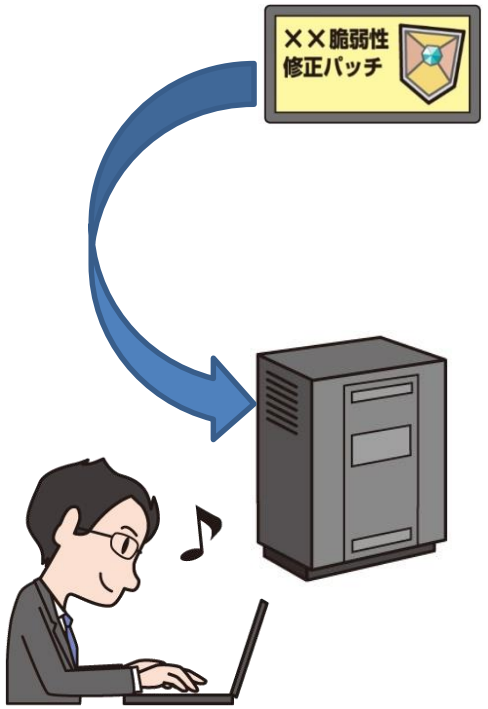


- 2014年の事例／統計
  - コンテンツ管理システム(CMS)が標的に
    - 国産CMSのWDPの脆弱性を悪用され多数のサイトが被害に
    - 管理されず放置されているウェブサイトが狙われる



【7位】ウェブサイトの改ざん
～知らぬ間に、ウイルス感染サイトに仕立てられる～

- 対策一覧
  - ウェブサイト運営者
    - サーバーソフトウェアの更新
    - サーバーソフトウェアの設定の見直し
    - ウェブアプリケーションの脆弱性対策
    - アカウント・パスワードの適切な管理
  - ウェブサイト閲覧者
    - ソフトウェアの更新
    - ウイルス対策ソフトの導入



ウェブサイト運営者は利用しているソフトウェアを適切に管理し、安全な運用を

【8位】インターネット基盤技術を悪用した攻撃

～インターネット事業者は厳重な警戒を～

- DNSや電子証明書等のインターネット基盤技術を悪用、なりすましやDDoS攻撃の被害が発生

【8位】インターネット基盤技術を悪用した攻撃
～インターネット事業者は厳重な警戒を～

- 手口と影響
  - なりすましによりドメインを乗っ取りウイルス感染サイトに誘導
  - DDoS攻撃により標的のネットワークやサーバーを麻痺させる

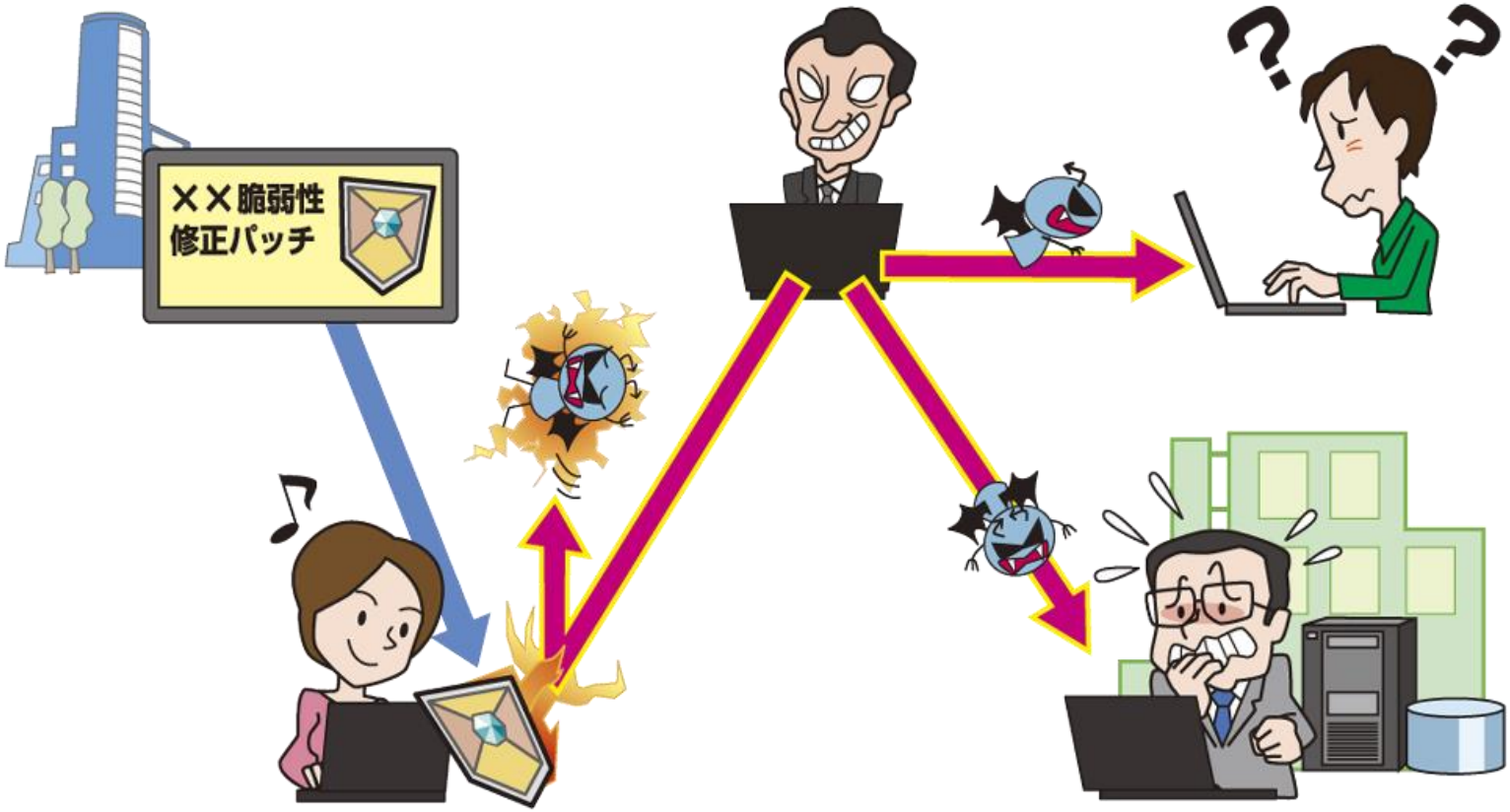
- 2014年の事例／統計
  - ドメイン名ハイジャックによる登録情報の書き換え
    - 国内の企業・組織の「.com」ドメインの登録情報が書換えられ、ウェブ閲覧者がウイルス感染サイトに誘導された

【8位】インターネット基盤技術を悪用した攻撃
～インターネット事業者は厳重な警戒を～

- 対策一覧
  - インターネット事業者、ドメインや電子証明書等を使用する企業・組織等
    - 登録変更申請内容の真偽の確認強化
    - 定期的な登録情報の確認
    - 利用機器やソフトウェアの適切な設定

偽者による
ドメイン登録変更や証明書発行依頼に注意！

【9位】脆弱性公表に伴う攻撃
～求められる迅速な脆弱性対策～



- 公表された広く利用されているソフトウェアの脆弱性が相次いで攻撃に悪用される

【9位】脆弱性公表に伴う攻撃
～求められる迅速な脆弱性対策～

- 手口と影響
  - 脆弱性の情報から攻撃コードを作成
  - 公表に気付かない、対応・判断が遅れた利用者が被害に

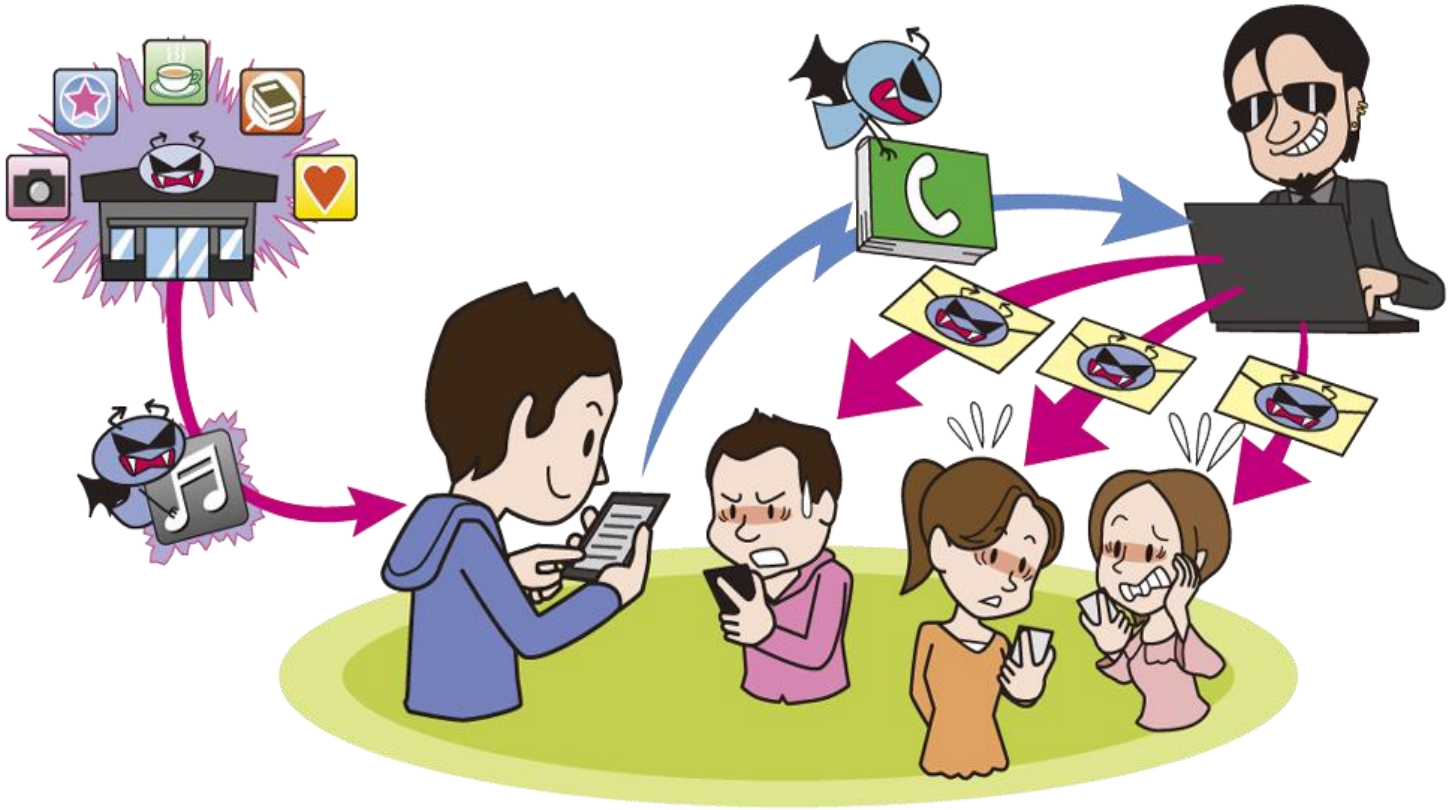
- 2014年の事例／統計
  - サーバーソフトウェアの脆弱性の公表
    - OpenSSLの“Heartbleed”やbashの“ShellShock“の脆弱性を悪用する攻撃の観測
    - Apache Struts2の脆弱性の修正が不十分で再度パッチを公開

【9位】脆弱性公表に伴う攻撃
～求められる迅速な脆弱性対策～

- 対策一覧
  - 経営者層
    - 迅速な対応に向けた体制の整備
  - ソフトウェア利用者
    - 管理しているシステムの把握
    - 定期的な脆弱性情報の収集
    - ソフトウェアの更新

脆弱性公表をキャッチして迅速に対応できる体制や習慣を作る

【10位】悪意のあるスマートフォンアプリ
～アプリのインストールで友人に被害が及ぶことも～



- スマホ内の電話帳等の情報が第三者に送信される
- 個人情報を悪用され、友人や知人に被害が及ぶ場合も

【10位】悪意のあるスマートフォンアプリ
～アプリのインストールで友人に被害が及ぶことも～

- 手口と影響
  - 偽物のアプリを公開して誘導
  - アップデートで悪意のあるアプリに豹変
  - 別のアプリを勝手にインストール
  - 端末内の情報窃取や盗聴・盗撮

- 2014年の事例／統計
  - 人気のAndroidアプリの偽物アプリ
    - 多くの偽物アプリを非公式のダウンロードサイトで確認

【10位】悪意のあるスマートフォンアプリ
～アプリのインストールで友人に被害が及ぶことも～

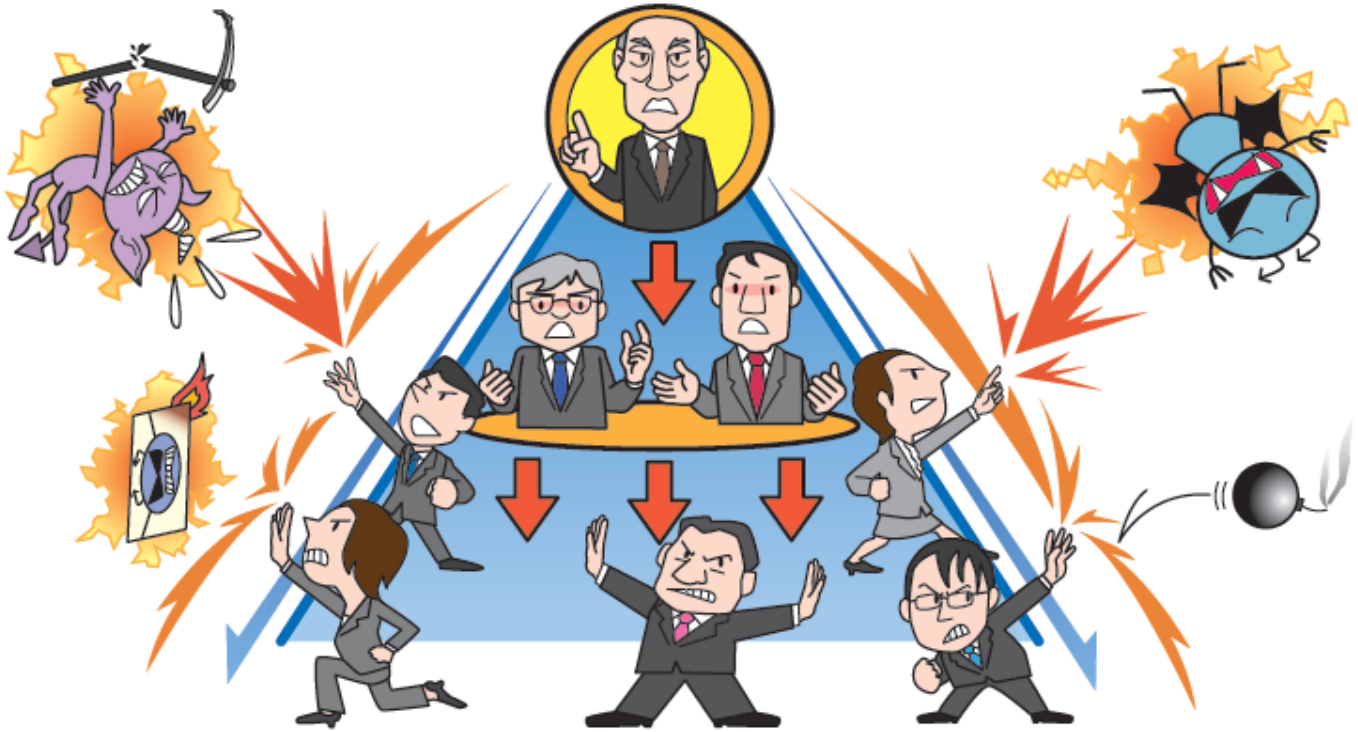
- 対策一覧
  - スマートフォン利用者
    - 信頼できるアプリかどうかを確認
    - アクセス権限の確認
    - OSやアプリは最新版を利用
    - ウイルス対策ソフトの導入

アプリのインストールは慎重に！

目次

- 情報セキュリティ10大脅威について
- 1章. 情報セキュリティ対策の基本
- 2章. 2014年版10大脅威
- **3章. 注目すべき課題や懸念**
  1. **迅速に対応できる体制の構築**
  2. **ネットワーク対応機器の増加**
  3. **拡大するネット犯罪の被害**

1．迅速に対応できる体制の構築
～脆弱性の公表や事件発生に対応できる体制作り～



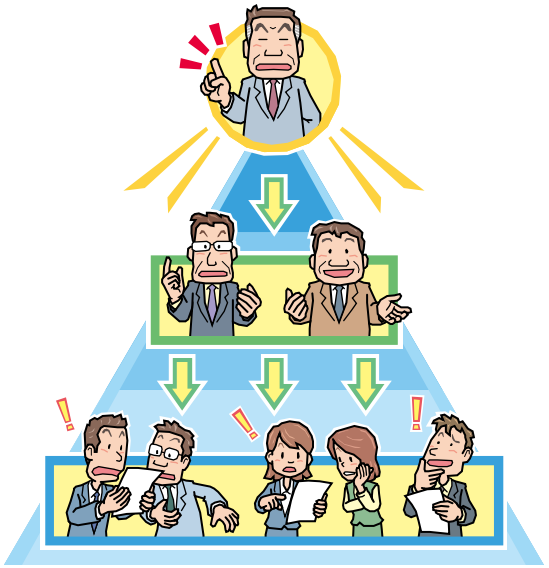
- 様々なセキュリティの問題に迅速に対応するため、
  組織としての体制強化が求められる

1．迅速に対応できる体制の構築
～脆弱性の公表や事件発生に対応できる体制作り～

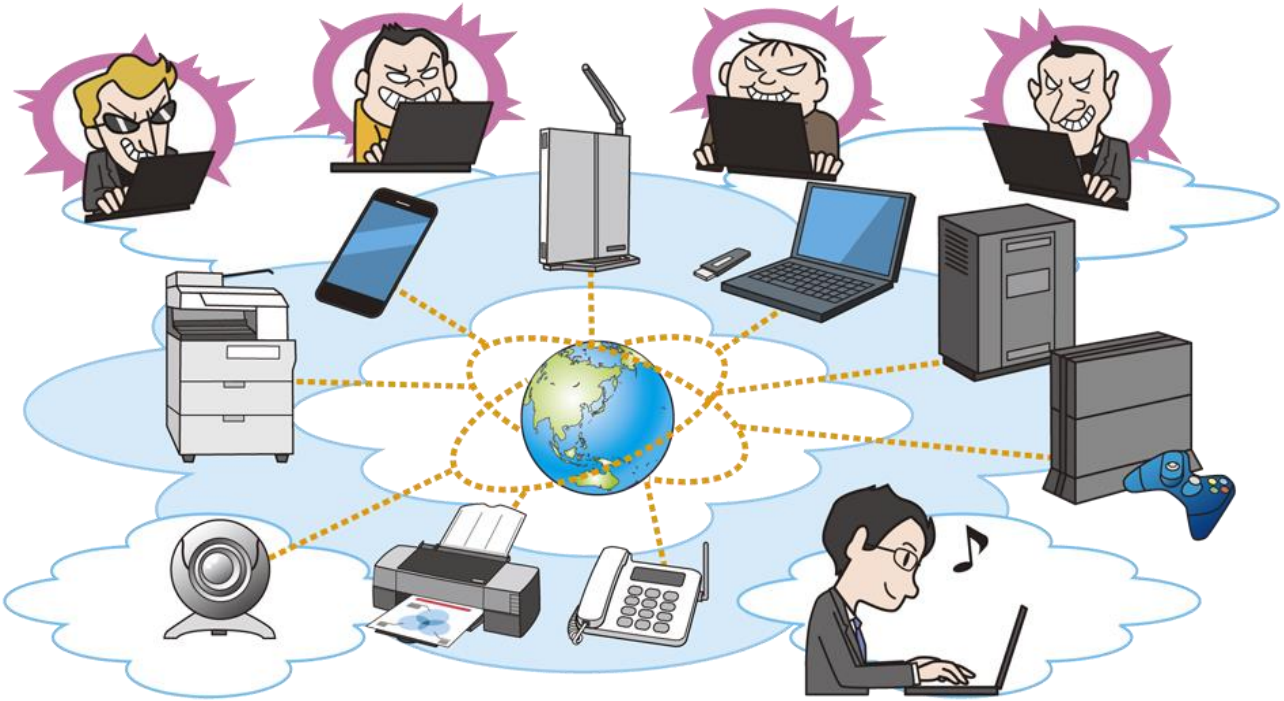
- 2014年に発生した迅速な対応が求められた例
  - 広く利用されている製品の脆弱性の公表
    - サーバーソフトウェアのApache Struts、OpenSSL、bash 等
    - クライアントソフトウェアのInternet Explorer、Adobe Flash Player 等
  - 内部不正による情報漏えい事件
    - ベネッセ、3,504万件の顧客情報が漏えい

1．迅速に対応できる体制の構築
～脆弱性の公表や事件発生に対応できる体制作り～

- 体制を構築するには
  - 経営層が対策の内容と実施について責任を持つ
  - 体制構築と継続的な対策の実施のために予算を確保
  - 企業・組織内に「CSIRT」を設置



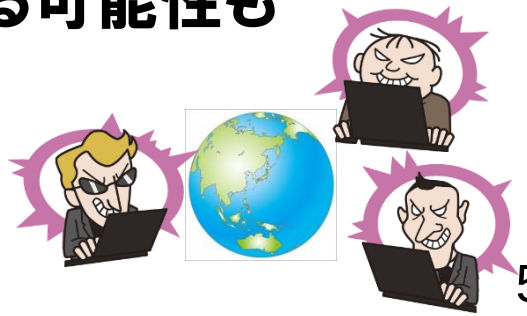
2. ネットワーク対応機器の増加
～モノのインターネット（IoT）にもセキュリティ対策を～



- 家電、オフィス機器、制御機器等のネットワーク対応機器が増加
- ネットワークを介して機器が攻撃された場合、
  乗っ取りや情報漏えいの被害を受ける可能性あり

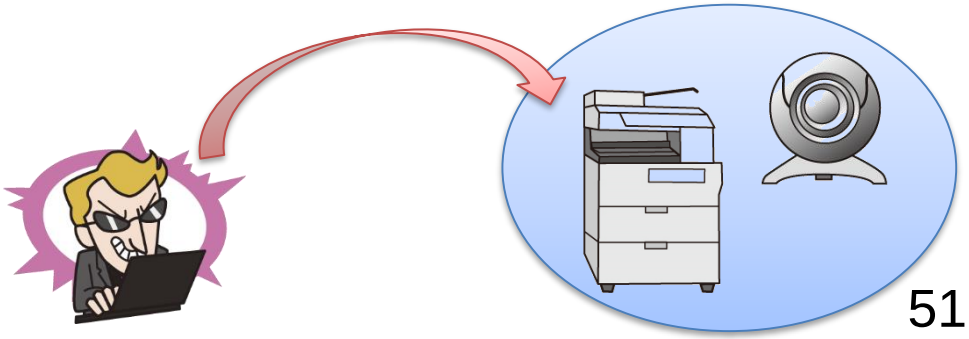
2. ネットワーク対応機器の増加
～モノのインターネット(IoT)にもセキュリティ対策を～

- モノのインターネット(IoT)
  - ネットワーク対応機器は、IoT(Internet of Things)と称される
  - 将来、爆発的な増加が見込まれている
    - ガートナーは2009年の9億台から、2020年に260億台と試算
- ネットワーク対応機器の危険性と攻撃
  - インターネット接続で世界中から攻撃される
  - 無線LANルーターへのウイルスの感染も確認されている
  - 制御システム、車載システムや医療機器等への侵害は人命にかかわる可能性も



2. ネットワーク対応機器の増加
～モノのインターネット(IoT)にもセキュリティ対策を～

- ネットワーク対応機器の問題点
  - セキュリティを充分考慮せず設計されている
  - 意図せずにインターネットからアクセス可能な状態
  - 更新プログラムが自動で配信されない
- 機器への留意点・対策
  - 製品開発者：初期状態からセキュリティの高い設定で提供する
  - システム管理者：インターネットからのアクセスを制限する
  - 利用者：セキュリティが保たれるよう適切に設定して利用する

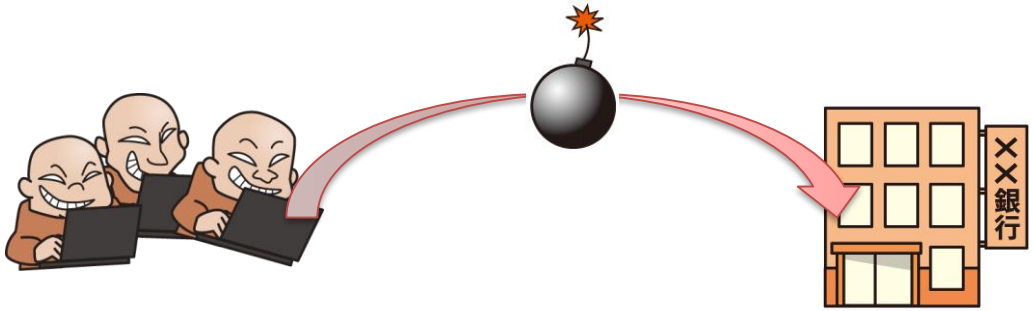


3. 拡大するネット犯罪の被害
～巧妙化するウイルスやネット詐欺による金銭被害～

- ITを悪用して金銭を窃取する事件が増加
- ウイルスによる不正送金や不当な会費の請求詐欺が横行

3. 拡大するネット犯罪の被害
～巧妙化するウイルスやネット詐欺による金銭被害～

- 犯罪者もITを利用
  - 犯罪者はメールやウェブサイトを悪用する
  - SNS（FacebookやLine等）を利用する攻撃も



- 金銭被害の増加
  - インターネットバンキングに関わる不正送金被害の急増
    - 不正送金被害は2014年が29億1,000万円で2013年の約2倍

3. 拡大するネット犯罪の被害
～巧妙化するウイルスやネット詐欺による金銭被害～

- 不正請求の手口
  - ワンクリック請求
  - 偽ウイルス対策ソフト
  - ランサムウェア

- ITにも防犯が必要
  - ウェブサイトから攻撃の手口や事例を知ることも防犯対策
    - 警察庁のサイト
    - 利用している銀行のサイト
    - IPAのサイト　等
  - 修正プログラムの適用やウイルス対策ソフトの導入等、基本的な対策も必要不可欠

本資料に関する詳細な内容は

- 以下のページのPDF資料をご覧ください。

情報セキュリティ10大脅威 2015
https://www.ipa.go.jp/security/vuln/10threats2015.html

情報セキュリティ船中八策

一、ソフトウェアの更新
～ 善は急げ ～

二、ウイルス対策ソフトの導入
～ 予防は治療に勝る ～

三、パスワードの適切な管理
～ 敵に塩を送ることのなきように ～

四、認証の強化
～ 念には念を入れよ ～

五、設定の見直し
～ 転ばぬ先の杖 ～

六、脅威・手口を知る
～ 彼を知り己を知れば百戦殆からず ～

七、クリック前に確認
～ 石橋を叩いて渡る ～

八、バックアップ
～ 備えあれば憂いなし ～


IPA
Better Life
with IT