IPA Better Life with IT

情報セキュリティ10大脅威2017

～2章 情報セキュリティ10大脅威　組織編～

～職場に迫る脅威！　家庭に迫る脅威！？
急がば回れの心構えでセキュリティ対策を～

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
2017年5月

情報セキュリティ10大脅威 2017

- 10大脅威とは？
  - 2006年よりIPAが毎年発行している資料
  - 「10大脅威選考会」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 2017

- 章構成
  - 1章.情報セキュリティ対策の基本 スマートフォン編
    - スマートフォンにおけるセキュリティ対策の基本を解説
  - 2章.情報セキュリティ10大脅威 2017
    - 脅威の概要と対策について解説
    - 個人と組織の2つの立場で解説
  - 3章.注目すべき脅威や懸念
    - 知っておくべき脅威や懸念を解説

情報セキュリティ10大脅威 2017

IPA

● 順位

「個人」向け脅威	順位	「組織」向け脅威
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	1	標的型攻撃による情報流出
ランサムウェアによる被害	2	ランサムウェアによる被害
スマートフォンやスマートフォンアプリを 狙った攻撃	3	ウェブサービスからの個人情報の窃取
ウェブサービスへの不正ログイン	4	サービス妨害攻撃によるサービスの停止
ワンクリック請求等の不当請求	5	内部不正による情報漏えいと それに伴う業務停止
ウェブサービスからの個人情報の窃取	6	ウェブサイトの改ざん
ネット上の誹謗・中傷	7	ウェブサービスへの不正ログイン
情報モラル欠如に伴う犯罪の低年齢化	8	IoT機器の脆弱性の顕在化
インターネット上のサービスを悪用した攻撃	9	攻撃のビジネス化 （アンダーグラウンドサービス）
IoT機器の不適切な管理	10	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章. 情報セキュリティ10大脅威2017
組織編

【1位】標的型攻撃による情報流出

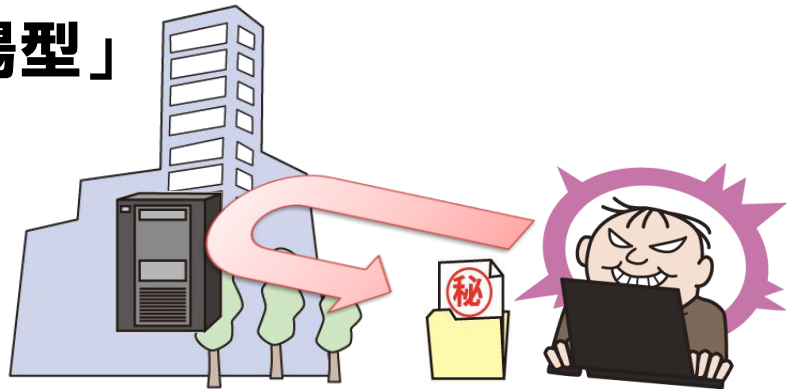
～引き続き警戒、標的型攻撃による被害が増加～

- メールによるウイルス感染等により組織内部に侵入
- 組織の機密情報が流出
- 取引先や関連会社を踏み台にして本丸を狙うことも

【1位】標的型攻撃による情報流出

～引き続き警戒、標的型攻撃による被害が増加～

- 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



- 2016年の事例/傾向
  - 旅行会社JTBから678万件の個人情報流出の可能性
    - 取引先になりすましたメールの添付ファイルを開き、ウイルスに感染
    - 遠隔操作により個人情報を保管しているサーバーへと侵害が拡大
  - 富山大学、標的型攻撃により研究成果等が外部流出の可能性
    - 感染PC内には個人情報や原発の汚染水処理に関する研究成果等を保有していた可能性
    - 非常勤の研究者のPCがウイルスに感染したことが原因

【1位】標的型攻撃による情報流出

～引き続き警戒、標的型攻撃による被害が増加～

IPA

● 対策一覧

■ 経営者層

- – 問題に迅速に対応できる体制（CSIRT）の構築
- – 対策予算の確保と継続的な対策実施

■ システム管理者

- ・被害の予防
  - – 被害を抑止するためのシステム設計
  - – アクセス制御・データの暗号化
- ・被害の早期検知・事後対策
  - – ネットワーク監視・分離

■ セキュリティ担当部署

- ・被害の予防
  - – セキュリティ教育の実施
  - – 情報の管理とルール策定
  - – 組織内CSIRTの運用
  - – サイバー攻撃に関する情報共有

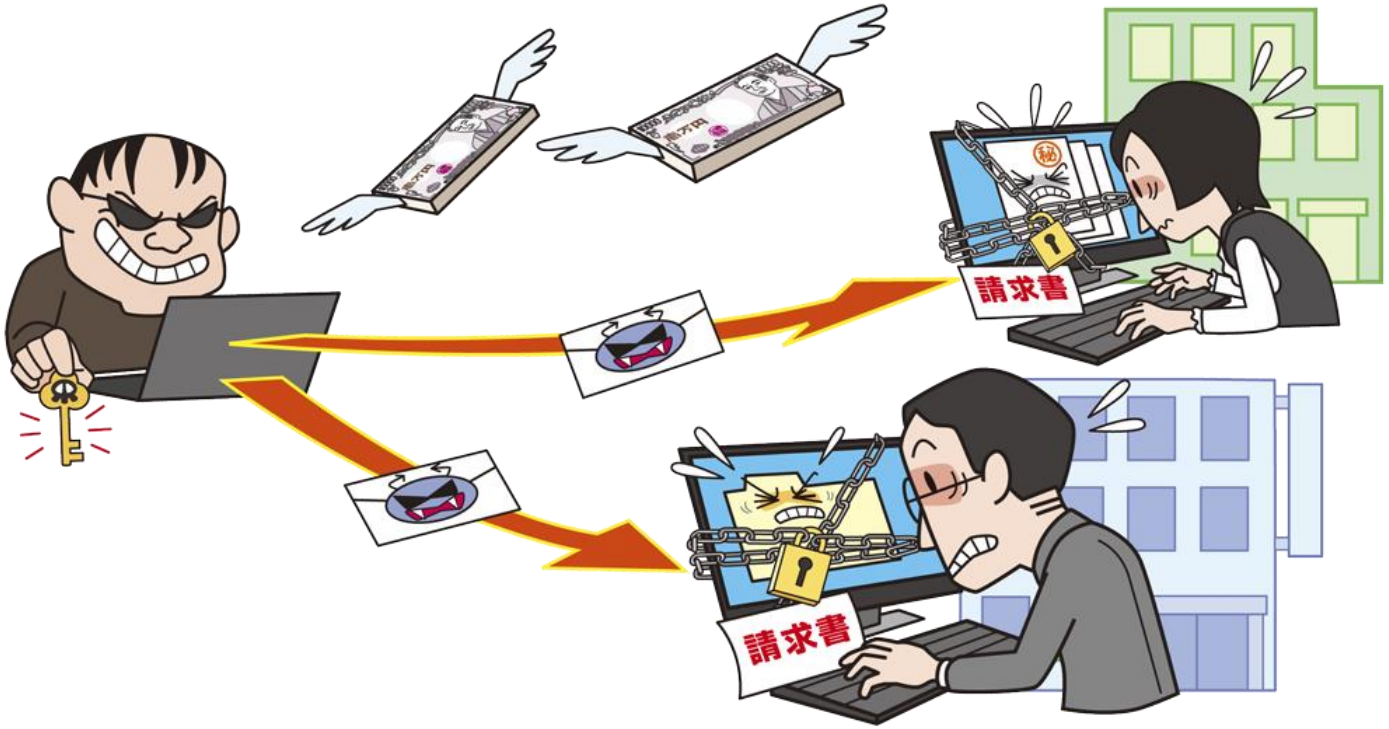
■ 従業員・職員

- ・情報リテラシーの向上
  - – セキュリティ教育の受講
- ・被害の予防
  - – OS・ソフトウェアの更新
  - – セキュリティソフトの導入・更新

内部へ侵入されることを想定した多層防御を

【2位】ランサムウェアによる被害

～ランサムウェアによる被害が急増～



- PC内のファイルの暗号化や、スマートフォンの画面のロックを行い、復元に身代金を要求
- 2016年はランサムウェアの被害が急増している

【2位】ランサムウェアによる被害

～ランサムウェアによる被害が急増～

- 手口/影響
  - メールの添付ファイルやリンクからランサムウェア感染
  - ウェブからランサムウェアに感染(脆弱性等を悪用)
  - 感染したPCだけではなく、共有サーバー等別の機器にも影響
- 2016年の事例/傾向
  - ランサムウェアの日本語化・被害拡大
    - 検出されたランサムウェアの件数が2015年の9.8倍
    - その中には日本語表記のランサムウェアを確認
  - ランサムウェアに感染したファイルを復号するツールの登場
    - 暗号化されたファイルを復号するツールが登場し、万が一暗号化されてもファイルを復元できる可能性

【2位】ランサムウェアによる被害

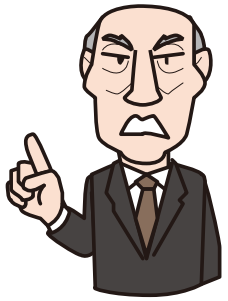
～ランサムウェアによる被害が急増～

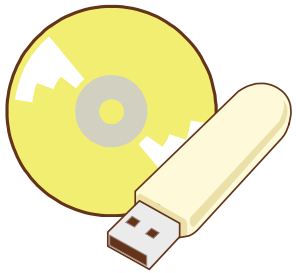
IPA

● 対策一覧

■ 経営者

- 組織としての対応体制の確立
  - 問題に対応できる体制（CSIRT等）構築
  - 予算の確保
  - セキュリティ対策の指示





■ システム管理者

■ PC・スマートフォン利用者

- 情報リテラシーの向上
  - 受信メール（添付ファイル・リンク）、ウェブサイトの十分な確認
- 被害の予防
  - OS・ソフトウェアの更新
  - セキュリティソフトの導入
  - フィルタリングツールの活用
- 被害を受けた後の対策
  - バックアップからの復旧
  - 復元できるかの事前の確認
  - 復元ツール・機能の活用

定期的なバックアップ、併せて脆弱性対策もすることで安全に

【3位】ウェブサービスからの個人情報の窃取

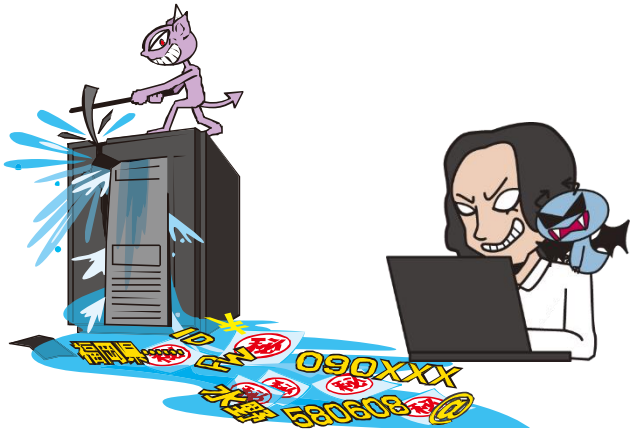
～犯罪グループの攻撃による甚大な被害～

- ウェブサービスから個人情報が窃取される事件が多発
- ウェブサービスの脆弱性を悪用

【3位】ウェブサービスからの個人情報の窃取

～犯罪グループの攻撃による甚大な被害～

- 手口/影響
  - 共通的に使われるソフトウェア(OpenSSL、Apache Struts、WordPress等)の脆弱性を悪用
  - 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

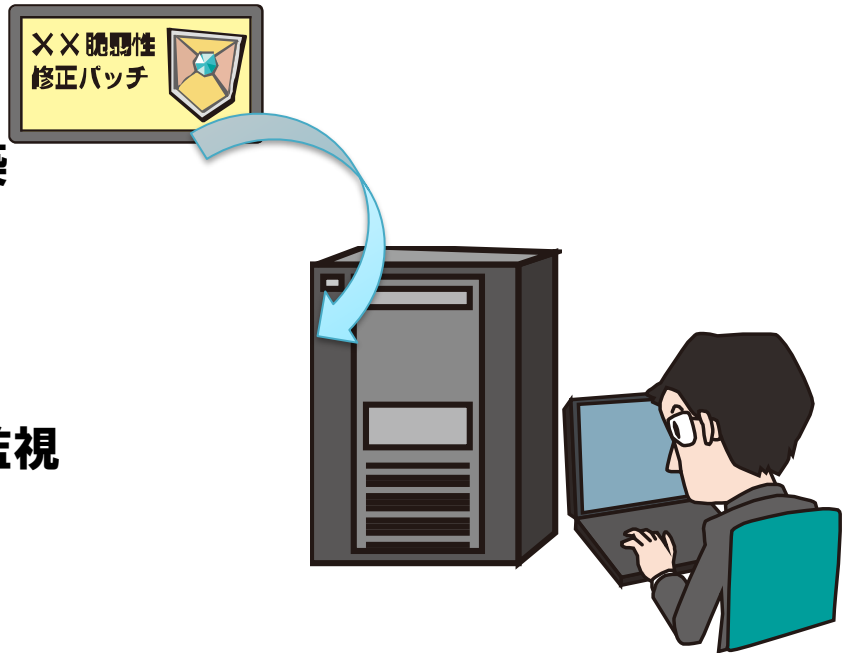


- 2016年の事例/傾向
  - 日本テレビのウェブサイトに不正アクセス
    - 最大43万件の個人情報が漏えいした可能性
    - OSコマンドインジェクションの脆弱性を悪用
  - 栄光ゼミナールのウェブサイトに不正アクセス
    - 生徒と保護者の個人情報が2,761件漏えい
    - CMSのプラグインのゼロデイの脆弱性を悪用

【3位】ウェブサービスからの個人情報の窃取

～犯罪グループの攻撃による甚大な被害～

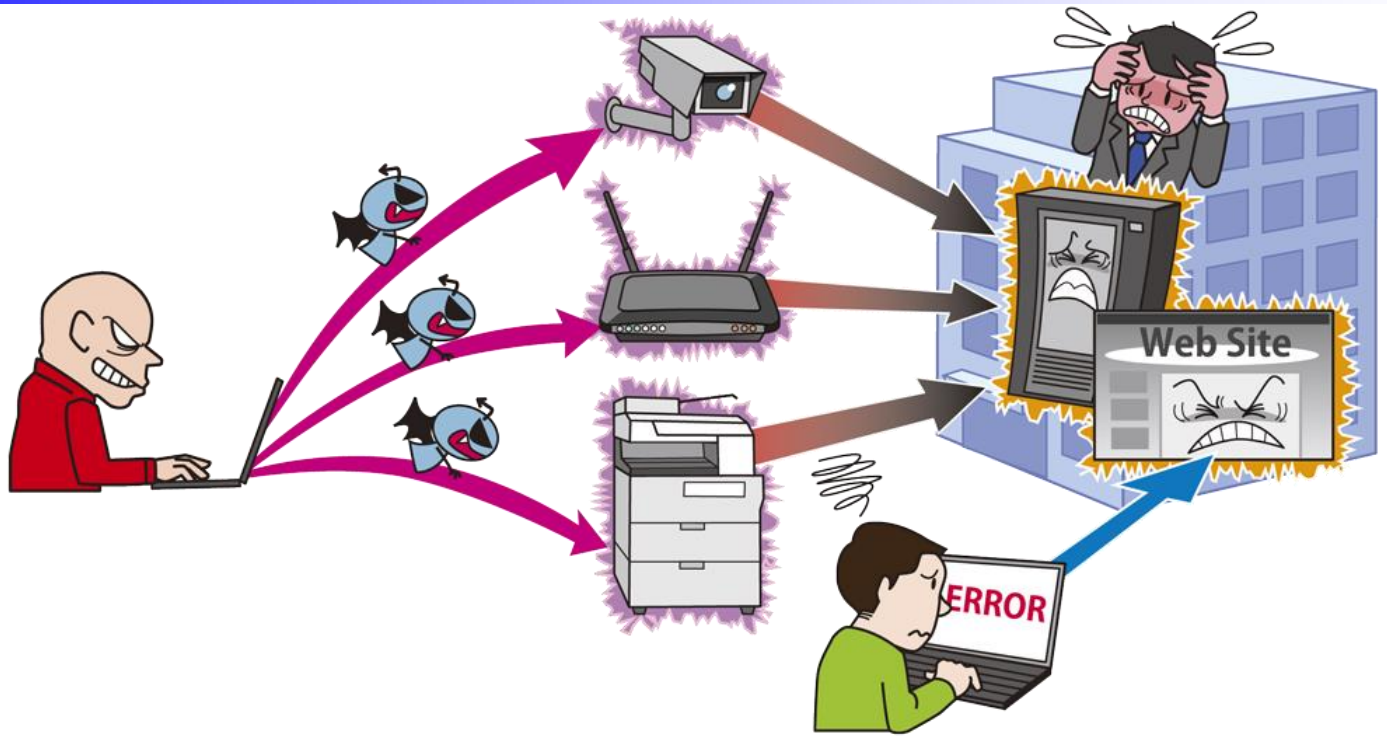
- 対策一覧
  - ウェブサービス運営者
    - 被害の予防
      - セキュアなウェブサービスの構築
      - OS・ソフトウェアの更新
      - WAF・IPSの導入
    - 被害の早期検知
      - 適切なログの取得と継続的な監視



ウェブサービスのセキュリティ対策をしっかりと
継続的なパッチの適用も

【4位】サービス妨害攻撃によるサービスの停止

～ボットネットウイルスの普及に伴う攻撃の大幅増加～



- 攻撃者に乗っ取られボット化したIT機器からDDoS攻撃
- 組織のウェブサイトや組織の利用しているDNSサーバーに大量のアクセス
- ウェブサイトの利用者がアクセスできない状態に

【4位】サービス妨害攻撃によるサービスの停止

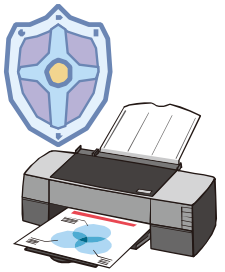
～ボットネットウイルスの普及に伴う攻撃の大幅増加～

- 手口/影響
  - ボットネットの利用
  - リフレクター攻撃（脆弱なルーター等に対して応答先を偽って通信）
  - DNS水責め攻撃（権威DNSサーバーに負荷を掛ける攻撃）
- 2016年の事例/傾向
  - 主義主張のためのDDoS攻撃
    - ICA（国際協力機構）やJCR（日本格付研究所）等のサイトにDDoS攻撃
    - 犯罪グループ（ハクティビスト）による主義主張のための日本を対象とした攻撃であった
  - ボットネットウイルスの拡散
    - 毎秒1テラビットという大規模なDDoS攻撃を確認
    - 原因は、IoT機器を踏み台にボットネットを構築するウイルス「Mirai」
    - ボットネットによる攻撃件数は昨年の6.4倍の1億2,600万件まで急増

【4位】サービス妨害攻撃によるサービスの停止

～ボットネットウイルスの普及に伴う攻撃の大幅増加～

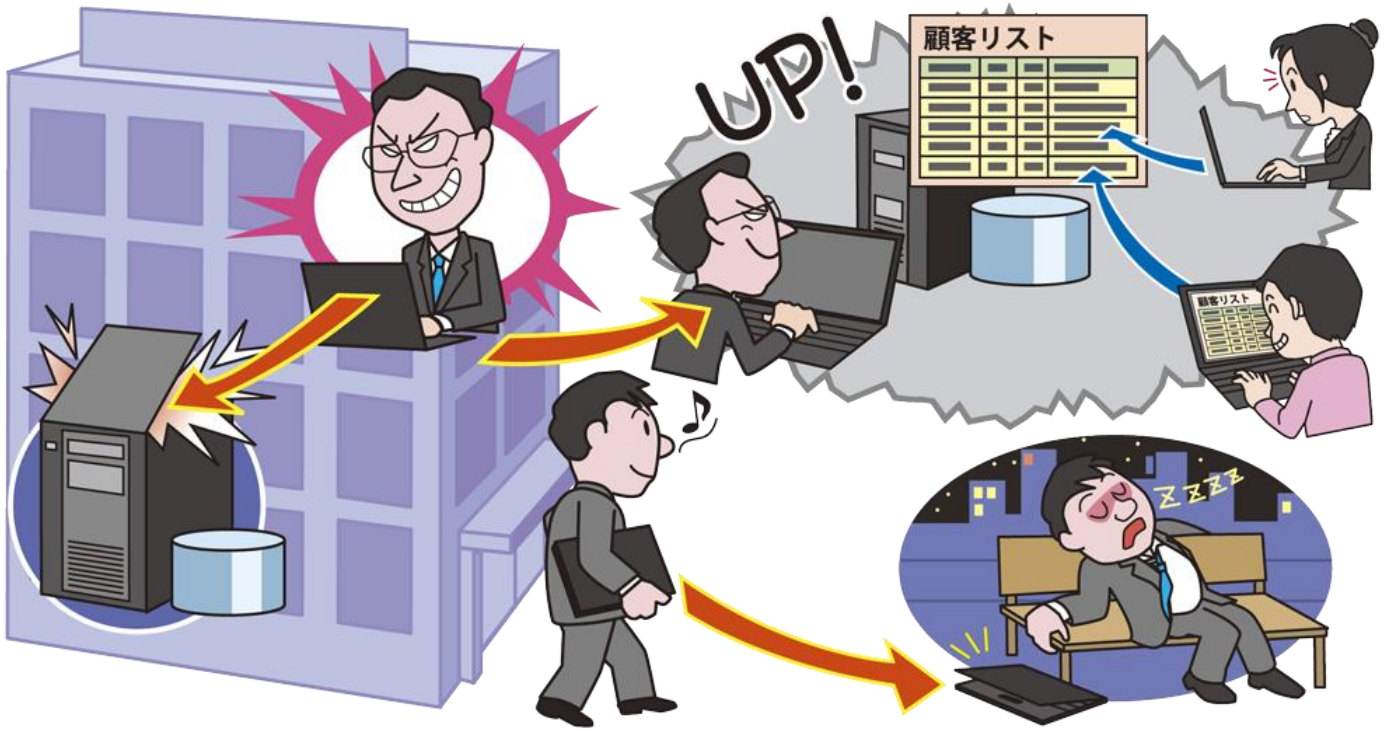
- 対策一覧
  - IoT機器ベンダー
    - 被害の予防
      - 脆弱性対策
  - ウェブサービス提供事業者
    - 被害の予防
      - DDoS攻撃の影響を緩和するISPによるサービスの利用
      - システムの冗長化等の軽減策
    - 被害を受けた後の対策
      - 通信制御（DDoS攻撃元をブロック等）
      - ウェブサイト停止時の代替サーバーの用意と告知手段の整備



DDoS被害に遭わないためにウェブサービス提供事業者だけではなく、IoT開発ベンダーも対策を

【5位】内部不正による情報漏えいとそれに伴う業務停止

～内部不正を許さない管理・監視体制を～



- 従業員・職員が故意に内部情報を持ち出し私的に利用
- 社内規則を守らず、自宅で業務を行うために持ち出し、内部情報を紛失する場合も
- 企業・組織の信用が失墜し、補償・賠償が求められる

【5位】内部不正による情報漏えいとそれに伴う業務停止

～内部不正を許さない管理・監視体制を～

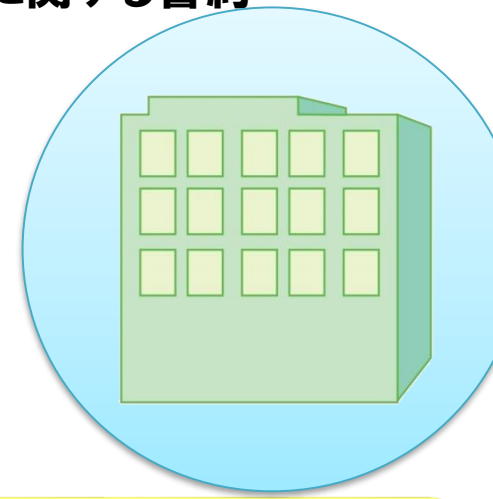
- **発生要因**
  - **職場環境や処遇の不満**
    処遇面（業務多忙、給与）の不満や復讐等の個人的な利益の享受を目的
  - **アクセス権限の不適切な付与**
    必要以上なアクセス権の付与等
  - **システム操作記録と監視の未実施**
    不正に気づきにくく、不正の発覚が遅れる

- **2016年の事例／傾向**
  - **YJFX!元従業員の持ち出しにより顧客情報18万件が流出**
    - **顧客情報がインターネット上に保存され、外部から閲覧可能**
    - **セキュリティ対策が適切ではない古い端末からアップロード**
  - **職員が個人情報を持ち出し、酒に酔って紛失**
    - **持ち出しはセキュリティポリシーで禁止されていた**

【5位】内部不正による情報漏えいとそれに伴う業務停止

～内部不正を許さない管理・監視体制を～

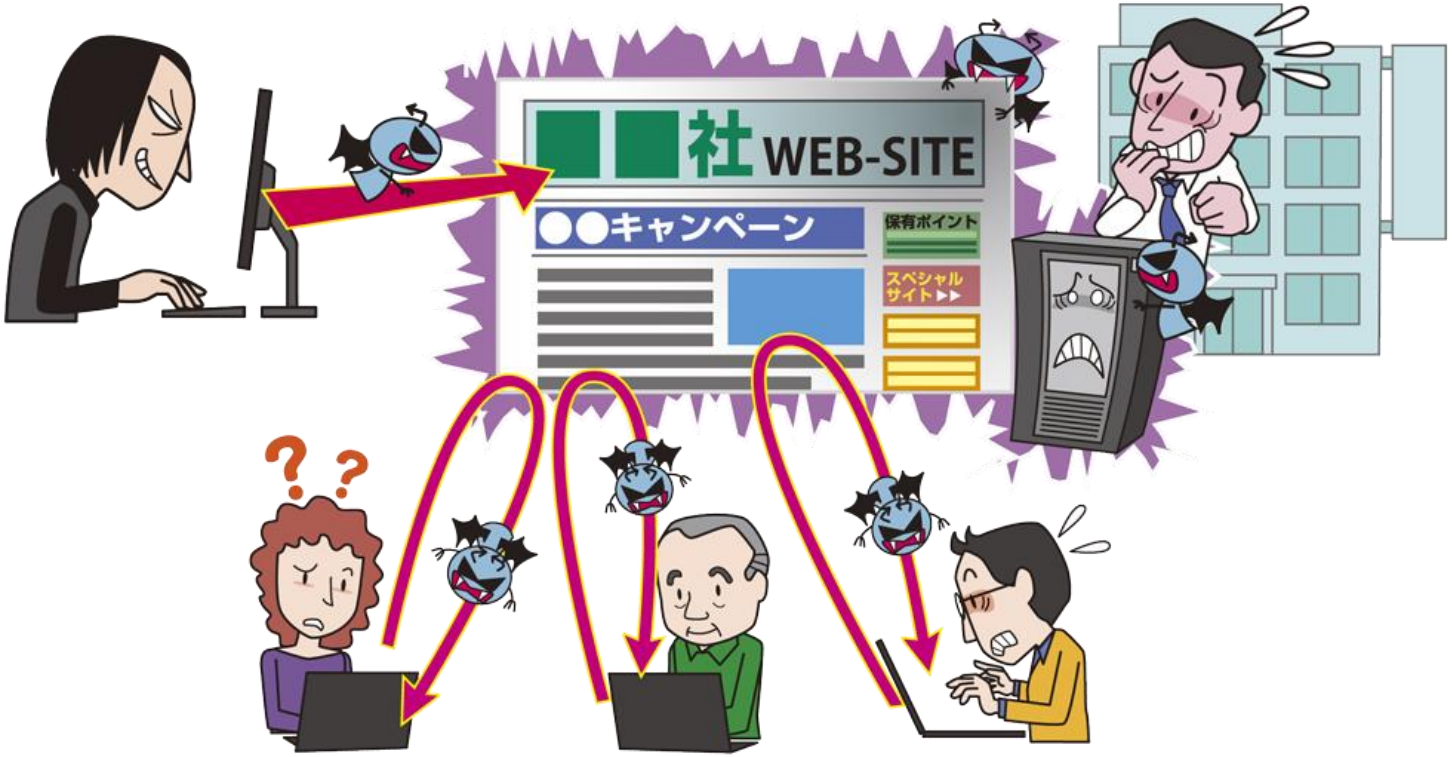
- **対策一覧**
  - **組織**
    - 被害の予防
      - 資産の把握・体制の整備
      - 情報取扱ポリシー作成および周知徹底・機密保護に関する誓約
      - 罰則の周知と相互監視の強化
      - 情報の取扱教育の実施
      - アカウント、権限の管理・定期監査
      - 重要情報の管理・保護（アクセス制御、暗号化）
    - 被害の早期検知
      - システム操作の記録・監視



組織一丸となって積極的に対策を推進する体制を

【6位】ウェブサイトの改ざん

～気づかぬうちにウイルスをばら撒くウェブサイトに～

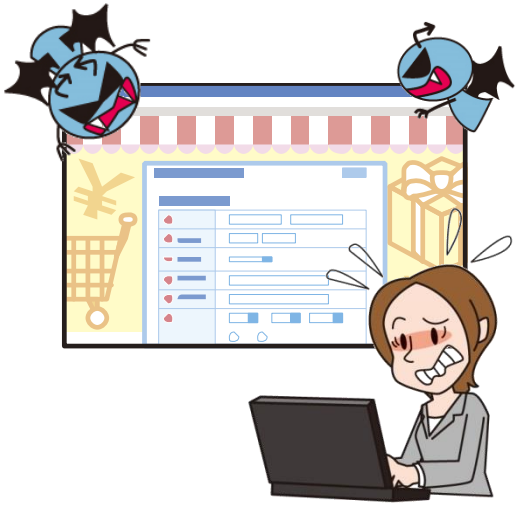


- ウェブサイトを改ざんされてウイルス感染に悪用される
- サイト運営者はウイルス感染に加担した加害者側に

【6位】ウェブサイトの改ざん

～気づかぬうちにウイルスをばら撒くウェブサイトに～

- 手口/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



- 2016年の事例/傾向
  - 動物園のHPが改ざん
    - 「動物を自由にしろ」等のメッセージを表示、主義主張を目的と見られる
    - ウェブアプリケーションの脆弱性を悪用された可能性があった
  - CMSの脆弱性を悪用した攻撃の観測
    - CMS Joomla!の脆弱性修正版公開後、24時間内に攻撃が活性化
    - 3日間の内に、27,000件以上の攻撃を観測

【6位】ウェブサイトの改ざん

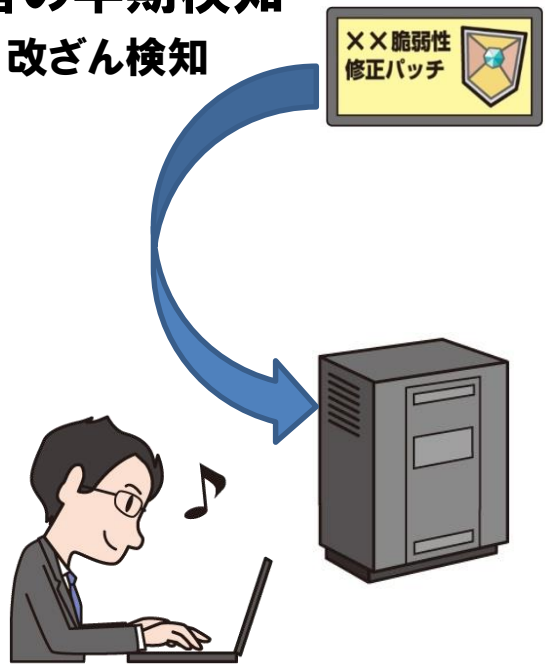
～気づかぬうちにウイルスをばら撒くウェブサイトに～

IPA

対策一覧

ウェブサイト運営者

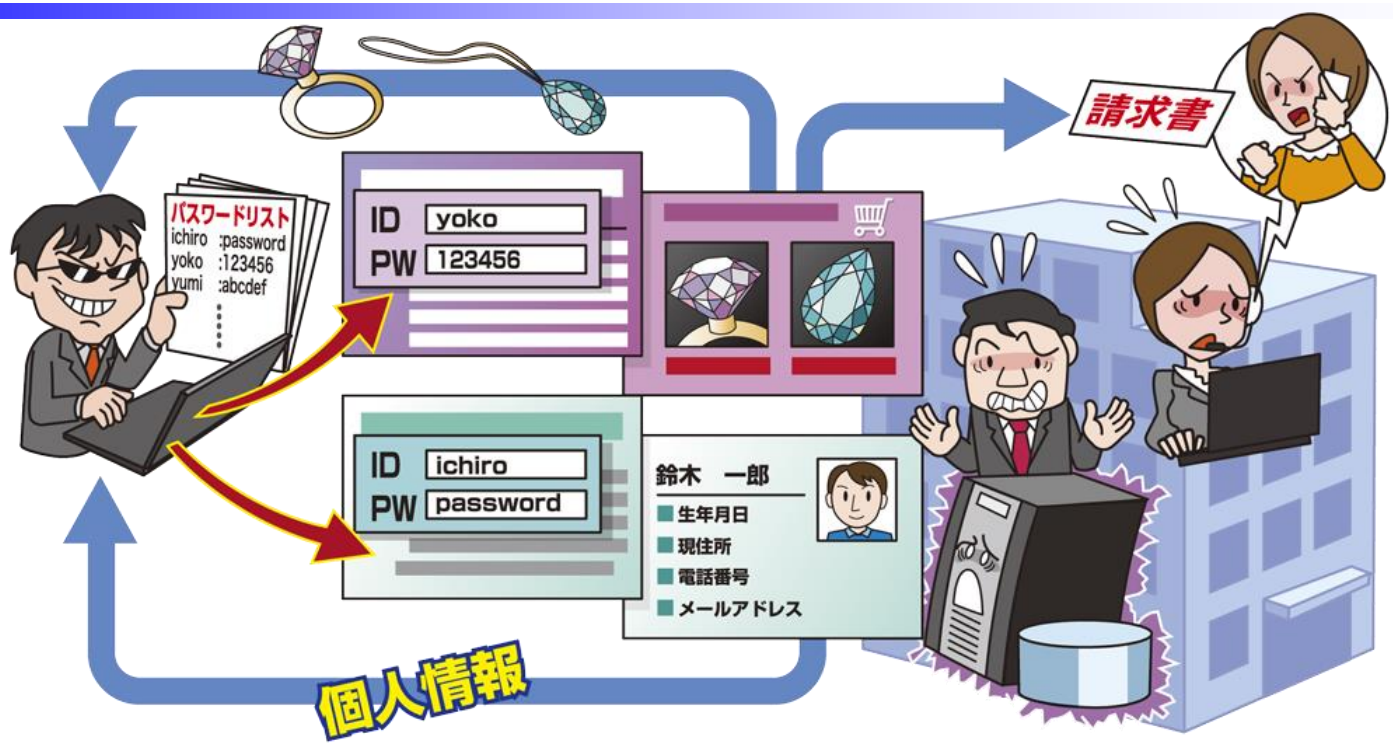
- 情報リテラシーの向上
  - アカウント・パスワードの適切な管理
- 被害の予防
  - OS・サーバーソフトウェアの更新
  - ウェブアプリケーションの脆弱性対策
  - 管理用端末のOS・ソフトウェアの更新
  - 管理用サービスの多要素認証を利用
  - 管理用サービスへのアクセス制限
  - 利用者に多要素認証の仕組みを提供
  - セキュリティを考慮したインフラ基盤
- 被害の早期検知
  - 改ざん検知



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

【7位】ウェブサービスへの不正ログイン

～多要素認証の活用を～



- 漏えいしたパスワードや推測したパスワードで不正アクセス
- 利用者は個人情報を窃取されたり、不正利用されたりする
- 運用事業者は企業の信用が失墜し、クレーム対応等に追われる

【7位】ウェブサービスへの不正ログイン

～多要素認証の活用を～

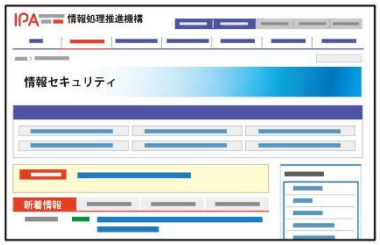
- 手口/影響
  - パスワードの推測攻撃
  - パスワードリスト攻撃（別サービスから窃取したIDやパスワード）
  - サービスに不正ログインされ、
    個人情報の窃取やポイントを不正利用される

- 2016年の事例/傾向
  - ブログへの不正ログイン
    - 5月と11月に「Ameba」への不正ログインの被害
    - 11月の攻撃では約59万の不正ログインを確認
  - オンラインショッピングへの不正ログイン
    - 「ビックカメラドットコム」にて不正ログインされ、ポイントを不正利用
    - 他のサイトで漏えいしたパスワードが使われた可能性があった

【7位】ウェブサービスへの不正ログイン

～多要素認証の活用を～

- **対策一覧**
  - **ウェブサービス運営者**
    - 被害の予防
      - 簡単なパスワードを許可しない
      - 多要素認証の導入

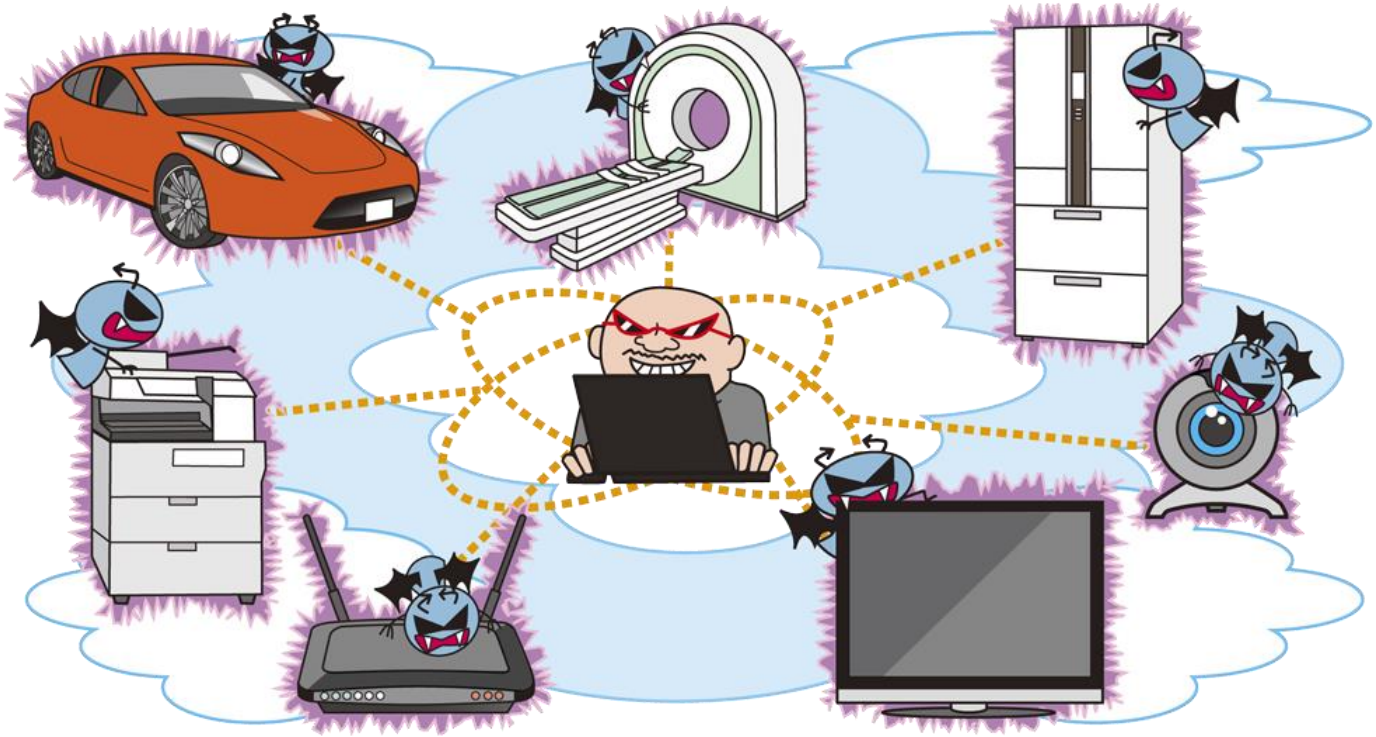


ID PW

利用者が被害に遭わないために
多要素認証等の適切なセキュリティ対策の提供

【8位】IoT機器の脆弱性の顕在化

～IoT機器のボットネットを悪用した大規模なDDoS攻撃を観測～



- IoT機器の脆弱性が悪用され、ウイルス感染や不正利用される
- 不正利用されたIoT機器がボット化し、DDoS攻撃等に悪用されるケースも

【8位】IoT機器の脆弱性の顕在化

～IoT機器のボットネットを悪用した大規模なDDoS攻撃を観測～

- 手口/影響
  - IoT機器の脆弱性を悪用してウイルスに感染させる
  - ウイルスに感染後、DDoS攻撃を行い組織のサービスを妨害する
  - 不正利用や情報窃取される場合も

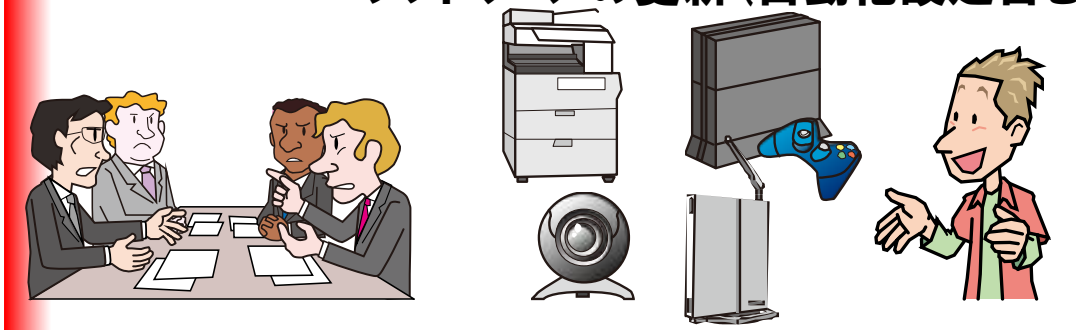
- 2016年の事例/傾向
  - 海外ルーターの脆弱性を悪用とした攻撃
    - 脆弱性を悪用されたIoT機器はボット化し、DDoS攻撃に悪用される
  - 電気自動車の専用アプリに遠隔操作可能となる脆弱性
    - 専用アプリのAPIに認証の仕組みが実装されておらず、遠隔操作される可能性
  - 医療機器インスリンポンプに遠隔操作可能となる脆弱性
    - 患者の治療情報や機器のデータの取得や機器を操作される脆弱性
    - 修正版のファームウェアをリリースする予定はない

【8位】IoT機器の脆弱性の顕在化

～IoT機器のボットネットを悪用した大規模なDDoS攻撃を観測～

IPA

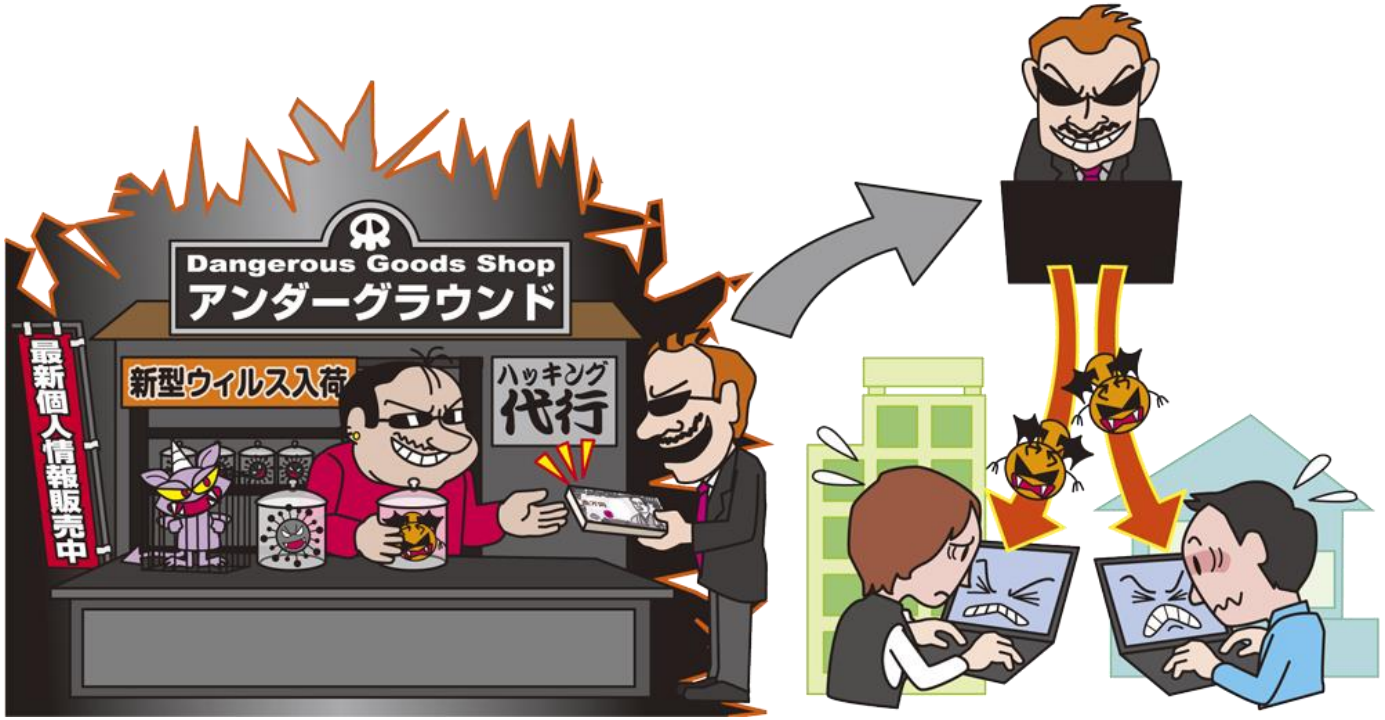
- **対策一覧**
  - **IoT機器の利用者**
    - 情報リテラシーの向上
      - 機器使用前に説明書を確認
    - 被害の予防
      - 不要な機能の無効化（telnet等）
      - 外部からの不要なアクセスを制限
      - ソフトウェアの更新（自動化設定含む）
  - **IoT機器の開発者**
    - 被害の予防
      - セキュアプログラミングの適用
      - 脆弱性の解消
      - ソフトウェア更新手段の自動化
      - 分り易い取扱説明書の作成
      - 迅速なセキュリティパッチの提供
      - 不要な機能の無効化（telnet等）
      - 安全なデフォルト設定
      - 利用者への適切な管理の呼びかけ



利用者は利用しているIoT機器の適切な管理を
開発者は適切な利用者を意識した対策を

【9位】攻撃のビジネス化（アンダーグラウンドサービス）

～サイバー犯罪を目的としたサービスやツールの売買～



- アンダーグラウンド市場に攻撃サービス、攻撃ツールが存在
- サービスやツールを利用して、容易に攻撃が行われる
- ランサムウェアへの感染被害や、DDoS攻撃の被害も

【9位】攻撃のビジネス化(アンダーグラウンドサービス)

～サイバー犯罪を目的としたサービスやツールの売買～

- 手口/影響
  - アンダーグラウンドで売買されているツール・サービスを購入・レンタル
  - ツールの機能により様々な被害

- 2016年の事例/傾向
  - エクスプロイトキットを使ったランサムウェアの拡散
    - ランサムウェアの感染のためにツールを使った攻撃を行っている
  - インターネットバンキング詐欺ツール
    - 金融関連情報を窃取する等の機能があるウイルス
    - ウイルス感染した端末でインターネットバンキングを利用すると、IDやパスワード等が窃取され、銀行口座から不正送金が行われる
  - 海外DDoS代行サービス利用者逮捕
    - 欧州サイバー犯罪センターと13カ国の警察当局が国際的に連携

【9位】攻撃のビジネス化（アンダーグラウンドサービス）

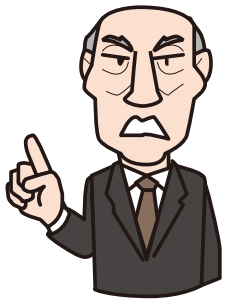
～サイバー犯罪を目的としたサービスやツールの売買～

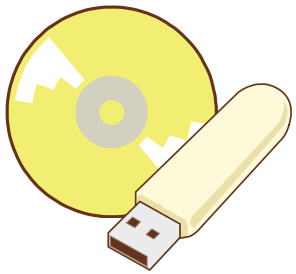
IPA

● 対策一覧（一例）

■ 経営者

- 組織としての対応体制の確立
  - 問題に対応できる体制（CSIRT等）構築
  - 予算の確保
  - セキュリティ対策の指示





■ システム管理者

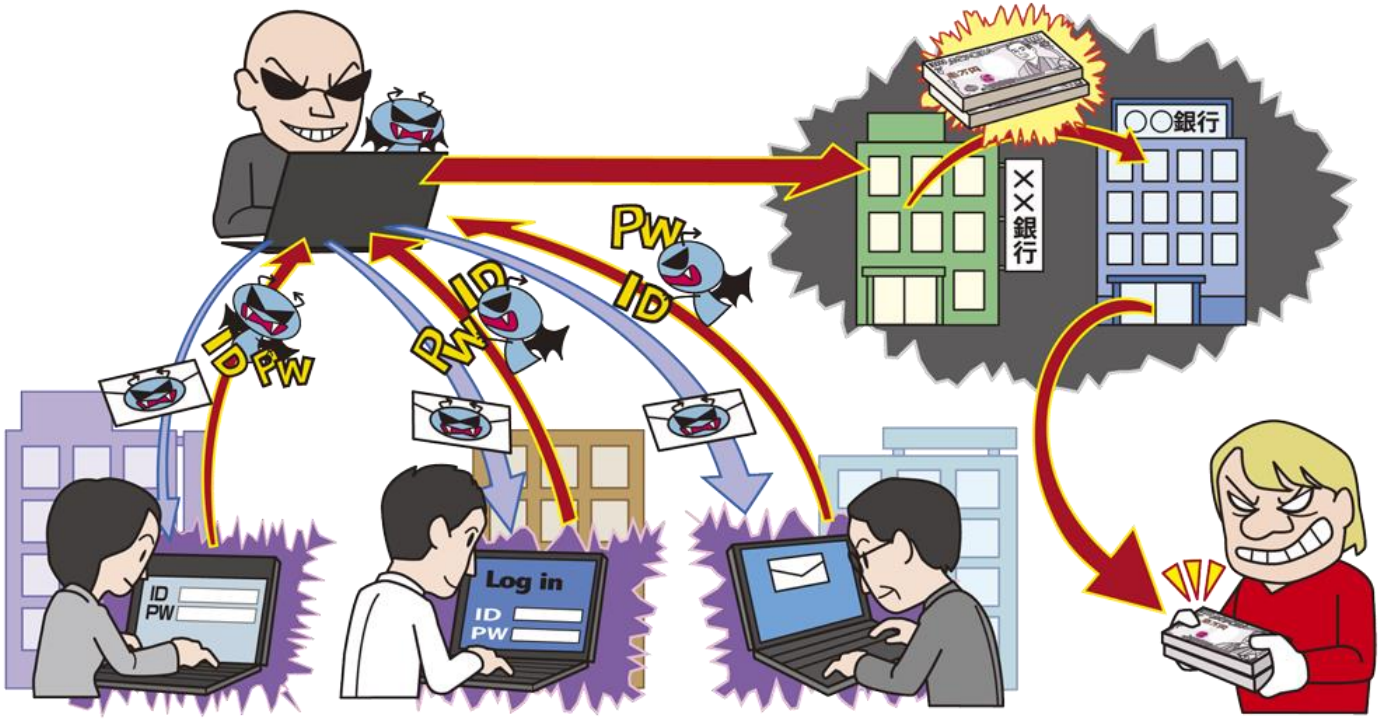
■ PC・スマートフォン利用者

- 情報リテラシーの向上
  - 受信メール（添付ファイル・リンク）、ウェブサイトの十分な確認
- 被害の予防
  - OS・ソフトウェアの更新
  - セキュリティソフトの導入
  - フィルタリングツールの活用
- 被害を受けた後の対策
  - バックアップからの復旧
  - 復元できるかの事前の確認
  - 復元ツール・機能の活用

ツールやサービスの機能により対策は様々
他の脅威の対策を参考に

【10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

～攻撃件数および被害額は減少しているが、引き続き警戒が必要～

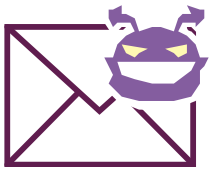


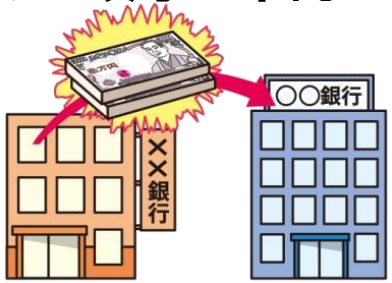
- ウイルスやフィッシング詐欺により認証情報が窃取され、不正送金される
- 被害件数・金額は減少傾向だが、引き続き警戒を

【10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

～攻撃件数および被害額は減少しているが、引き続き警戒が必要～

- 手口/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
- 2016年の事例/傾向
  - 不正送金被害は減少傾向
    - 不正送金事件件数1,291件（前年より204件減少）
    - 組織の不正送金被害額約4億3,500万円
      （前年より約10億3,100万円減少）
  - 日本語で書かれたメールによるウイルス拡散
    - 1回の攻撃で400通以上のウイルスメールを配信する攻撃を確認

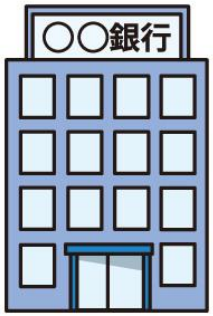




【10位】インターネットバンキングやクレジットカード情報の不正利用

～攻撃件数および被害額は減少しているが、引き続き警戒が必要～

- **対策一覧**
  - **利用者**
    - 情報リテラシーの向上
      - 受信メール（添付ファイル・リンク）・ウェブサイトの十分な確認
      - ポップアップに注意
      - 事例や手口を知る
    - 被害の予防
      - OS・ソフトウェアの更新
      - セキュリティソフトの導入
      - 多要素認証等の強い認証方式の利用
    - 被害の早期検知
      - 不審なログイン履歴の確認
      - 自身の口座やクレジットカードの利用履歴の確認



不審なメールは要注意
銀行が提供する多要素認証等の活用を

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 2017
https://www.ipa.go.jp/security/vuln/10threats2017.html