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　個人編～

～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

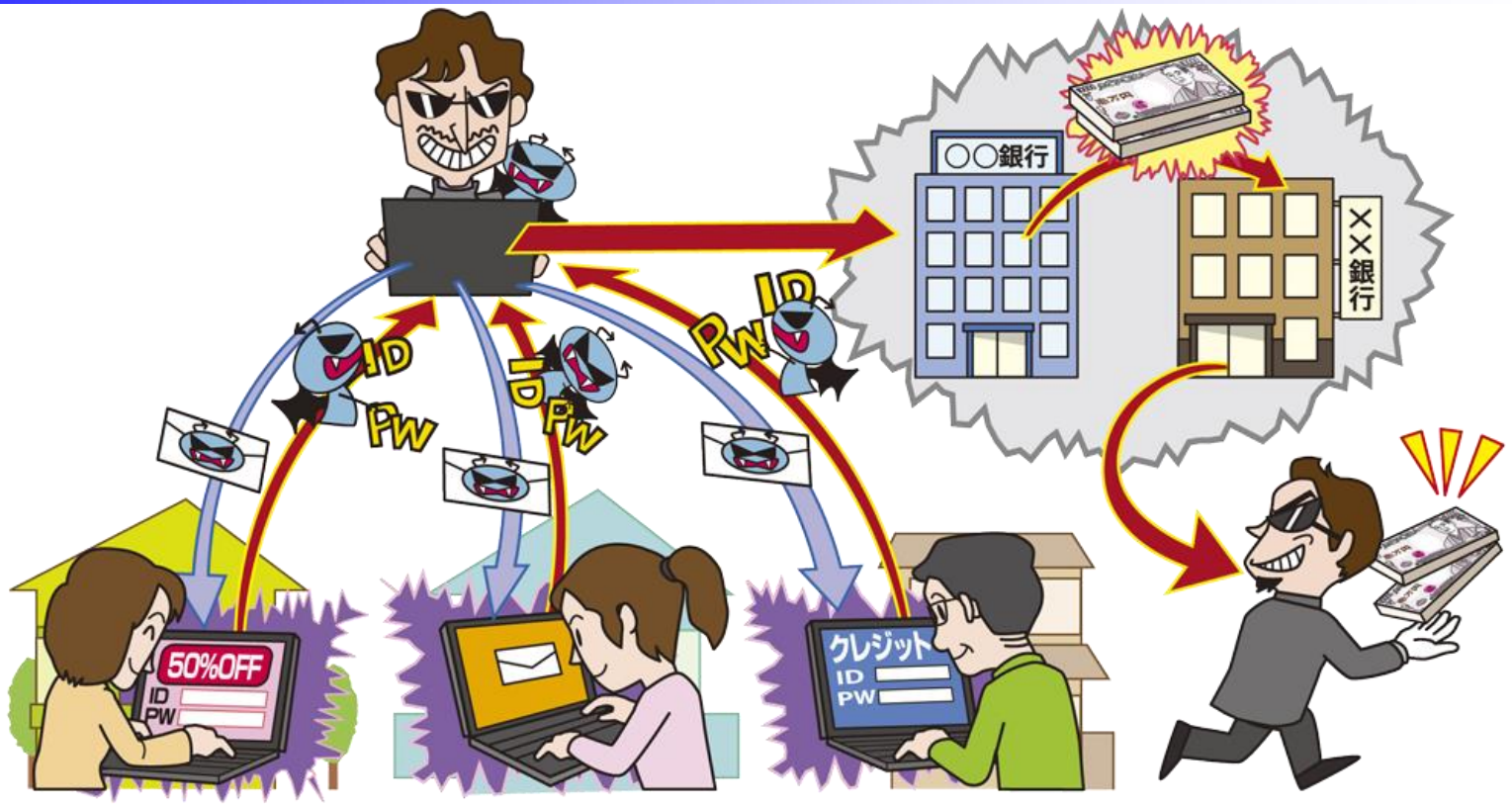
● 順位

「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
個人編

【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

～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～

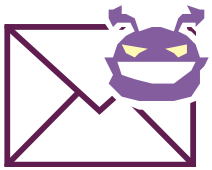


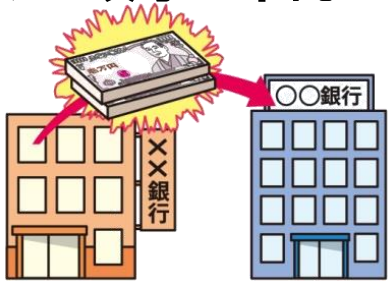
- ウイルスやフィッシング詐欺により認証情報が窃取され、不正送金される
- 被害件数・金額は減少傾向だが、引き続き警戒を

【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

～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）
    - 個人の不正送金被害額約12億5,200万円
      （前年より約3億5,500万円減少）
  - 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

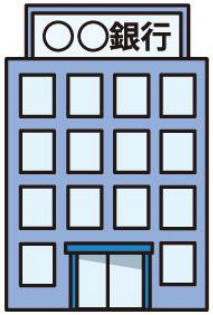




【1位】インターネットバンキングやクレジットカード情報の不正利用

～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～

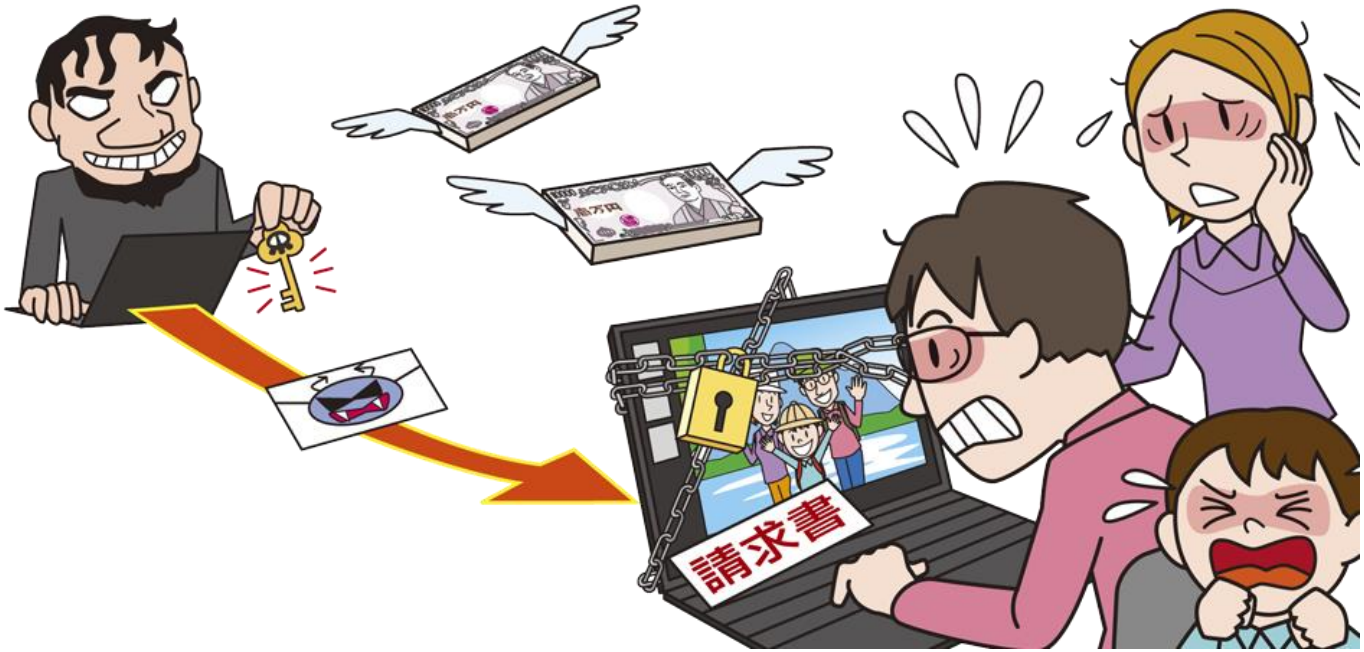
- **対策一覧**
  - **利用者**
    - 情報リテラシーの向上
      - 受信メール（添付ファイル・リンク）・ウェブサイトの十分な確認
      - ポップアップに注意
      - 事例や手口を知る
    - 被害の予防
      - OS・ソフトウェアの更新
      - セキュリティソフトの導入
      - 多要素認証等の強い認証方式の利用
    - 被害の早期検知
      - 不審なログイン履歴の確認
      - 自身の口座の利用履歴を確認する習慣をつける



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

【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

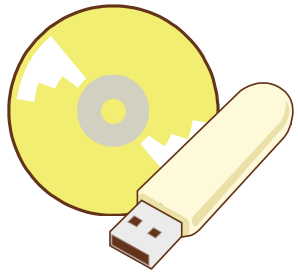
～ランサムウェアによる被害が急増～

- 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～

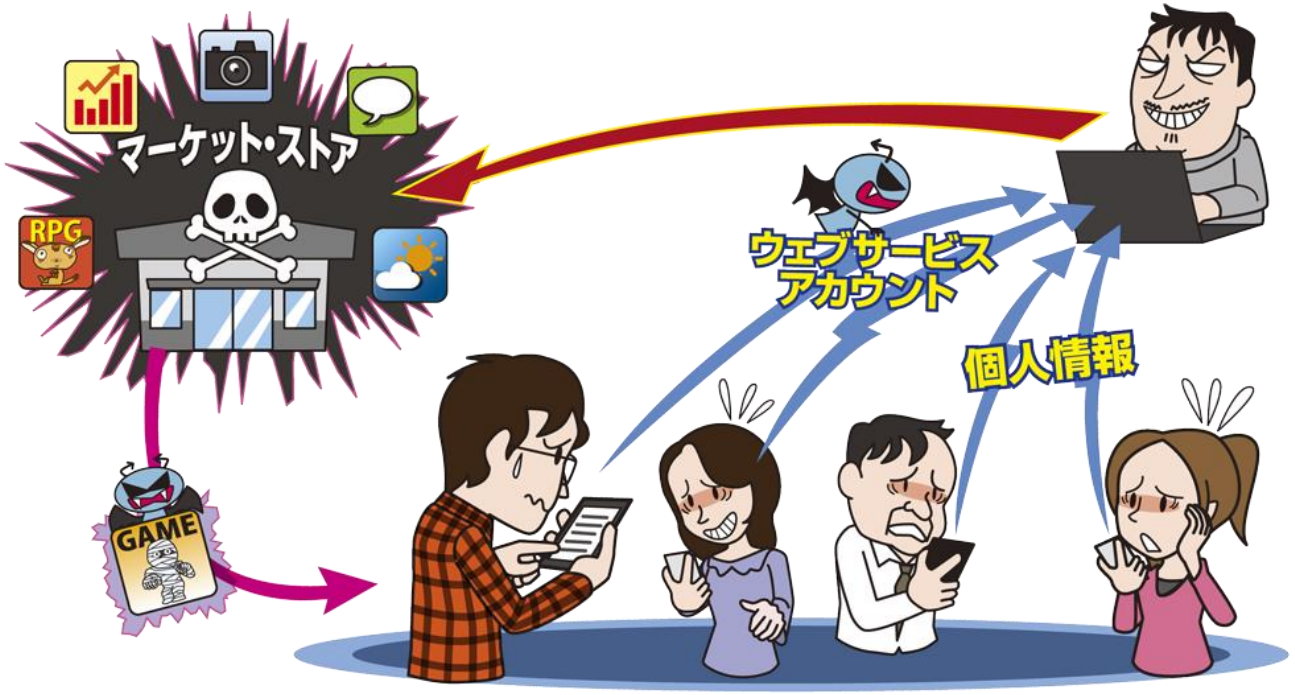
- 対策一覧
  - PC・スマートフォン利用者
    - 情報リテラシーの向上
      - メールの添付ファイル・リンクのURLを不用意に開かない
    - 被害の予防
      - OS・ソフトウェアの更新
      - ウイルス対策ソフトの導入・更新
    - 被害を受けた後の対策
      - バックアップからの復旧
      - 復元できるかの事前の確認
      - 復元ツール・機能の活用



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】スマートフォンやスマートフォンアプリを狙った攻撃

～人気アプリに酷似した不正アプリが暗躍～



- 攻撃者が人気アプリ等に偽装した不正アプリを公開
- 不正アプリをインストールすることで電話帳等の情報が攻撃者に送信される
- ランサムウェアの場合、スマートフォンをロックされる

【3位】スマートフォンやスマートフォンアプリを狙った攻撃

～人気アプリに酷似した不正アプリが暗躍～

- 手口/影響
  - 不正アプリを公式マーケット等に公開してインストールさせる
  - インストールすると情報窃取や遠隔操作がされる
  - 知人を騙して直接不正アプリをインストールするケースも

- 2016年の事例/傾向
  - 人気アプリに偽装した不正アプリ
    - 「ポケモンGO」や「スーパーマリオラン」等に偽装した不正アプリが登場
  - 日本語で恐喝するスマートフォン向けランサムウェアの登場
    - 「MINISTRY OF JUSTICE(法務省)」を語るランサムウェアが登場

【3位】スマートフォンやスマートフォンアプリを狙った攻撃

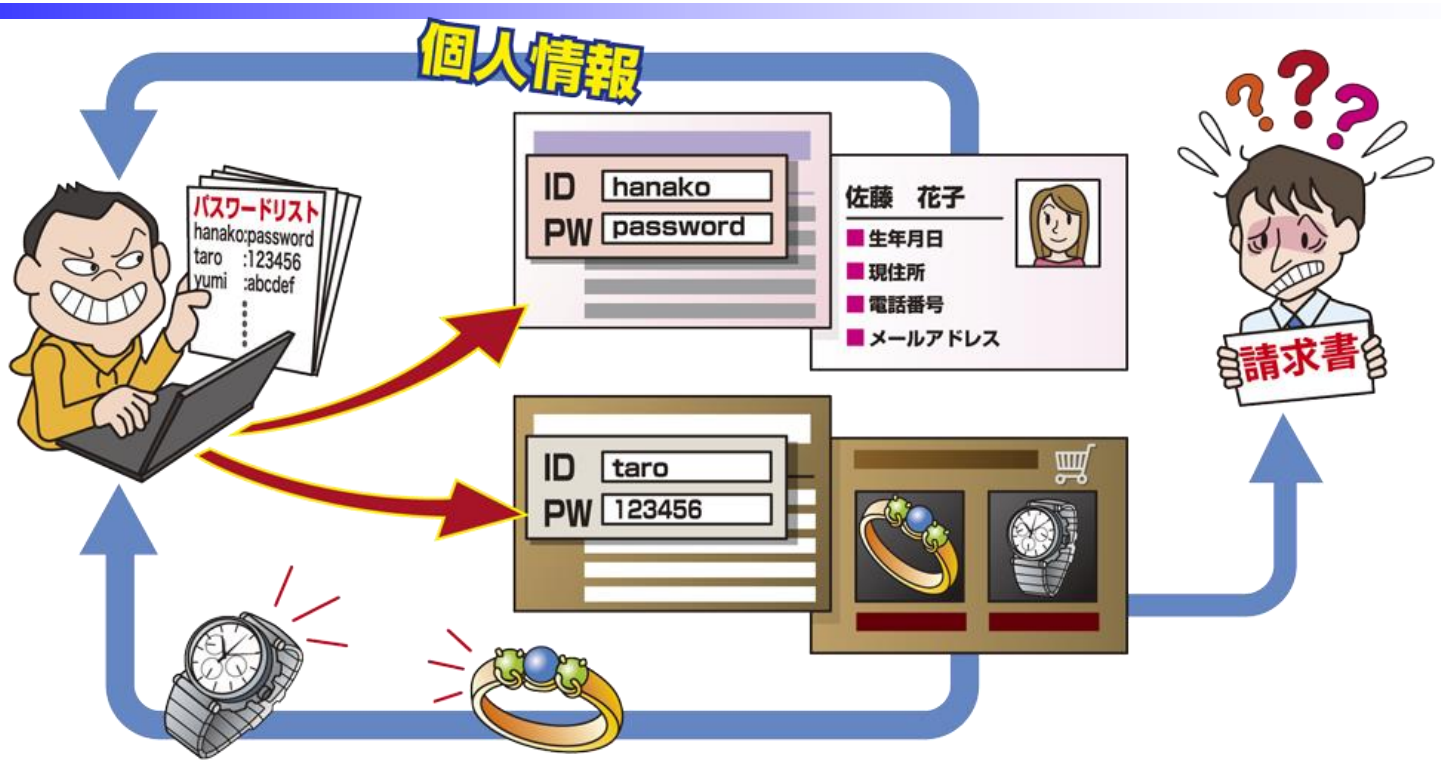
～人気アプリに酷似した不正アプリが暗躍～

- **対策一覧**
  - **スマートフォン利用者**
    - **情報リテラシーの向上**
      - アプリは公式マーケットからインストール
      - 起動時のアクセス権限の確認
    - **被害の予防**
      - OSやアプリは最新版を利用
      - セキュリティソフトの導入
      - 提供元不明のアプリを許可しない（Androidの場合）

アプリのインストールは慎重に！
公式マーケットからでも注意を

【4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～



- 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

～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

【4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
  - ウェブサービス利用者
    - 情報リテラシーの向上
      - パスワードは長く、複雑にする
      - パスワードの使い回しをしない
    - 被害の予防
      - パスワード管理ソフトの利用
      - 多要素認証等の強い認証方式の利用
      - 利用をやめたウェブサービスの退会

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】ワンクリック請求等の不当請求

～「ゼロクリック詐欺」登場！サイトを見ただけで「登録完了」～

- 有料サイトの利用料等、金銭を不正に請求するワンクリック請求の被害が引き続き発生
- クリックも必要としない、ウェブページを閲覧しただけで金銭を要求する「ゼロクリック」も登場

【5位】ワンクリック請求等の不当請求

～「ゼロクリック詐欺」登場！サイトを見ただけで「登録完了」～

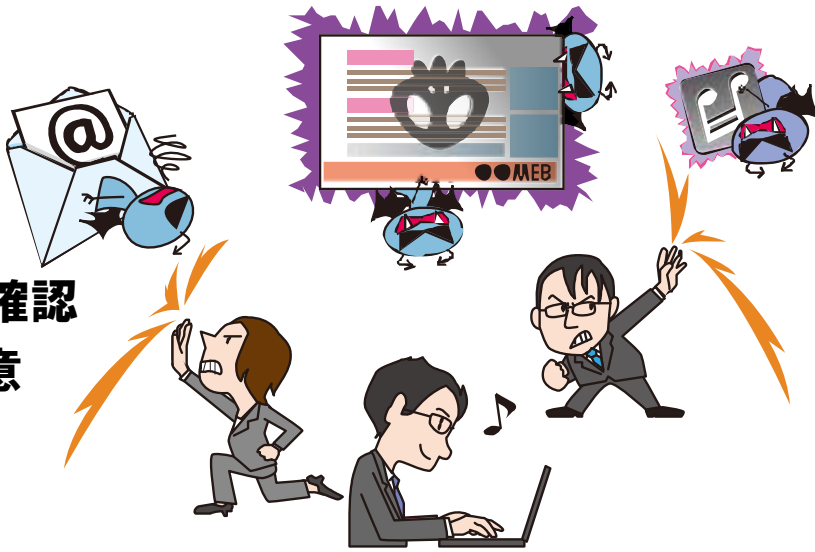
- 手口/影響
  - メールのリンク等から悪意あるサイトに誘導し、請求画面を表示
  - 請求画面の指示に従うと金銭を窃取される
  - スマートフォンの機能を悪用される
    - ・カメラのシャッター音を鳴らし、撮影されたと不安を煽る
    - ・サポートセンターへの電話を促すポップアップを表示する

- 2016年の事例/傾向
  - ゼロクリック詐欺登場
    - ・ウェブページを閲覧するだけで「登録完了」と表示し、金銭を要求
  - 熊本地震の義援金を装い、不当請求
    - ・SNSの募金というリンクをクリックすると、アダルトサイトに誘導され、「登録完了」と表示

【5位】ワンクリック請求等の不当請求

～「ゼロクリック詐欺」登場！サイトを見ただけで「登録完了」～

- **対策一覧**
  - **ウェブサービスの利用者**
    - 情報リテラシーの向上
      - 受信メール、ウェブサイトの十分な確認
      - TwitterやSNS等のメッセージに注意
      - 怪しいアプリは利用しない
      - 事例・手口の情報収集

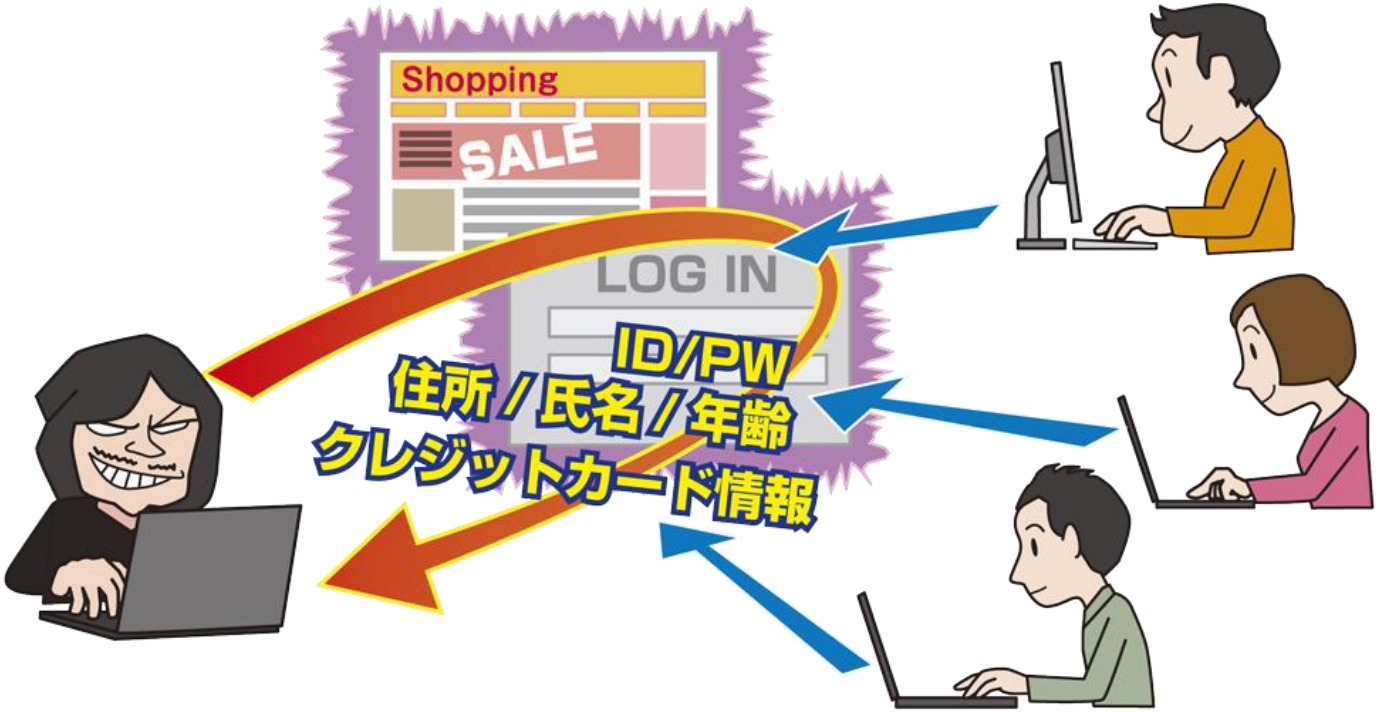


※購入の意思がないのであれば
金銭を要求されても慌てず、請求に応じない

怪しいソフトウェアの利用や怪しいサイトへの
アクセスは控え、万が一要求されても冷静に

【6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～

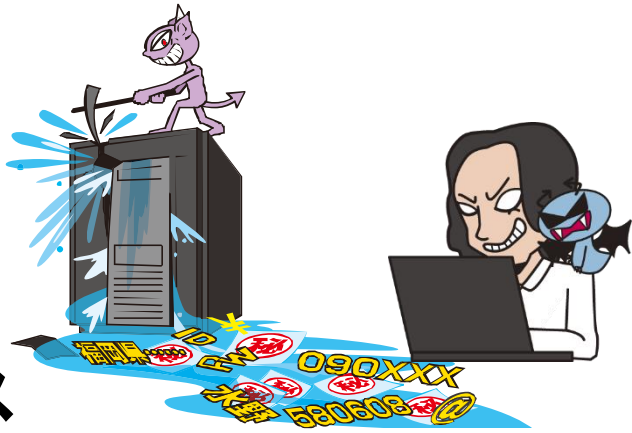


- ウェブサービスから個人情報が窃取される事件が多発
- ウェブサービスの脆弱性を悪用

【6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
  - 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



- 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(修正プログラムが開発ベンダーより提供される前の脆弱性)を悪用

【6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
  - ウェブサービス利用者
    - 情報リテラシーの向上
      - 必須項目以外の情報登録しない
      - 利用をやめたウェブサービスの退会

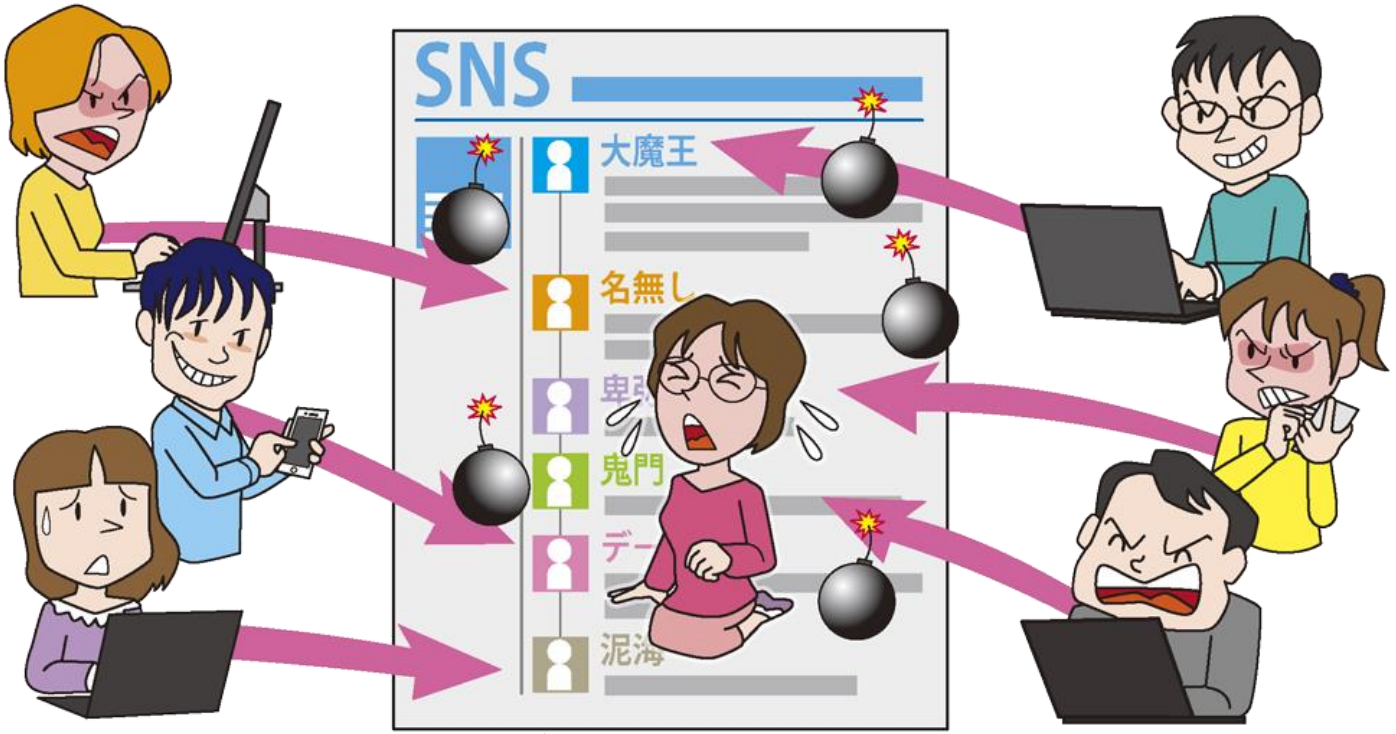
【参考】

  - ウェブサービス運営事業者
    - 被害の予防
      - システム構築時の脆弱性対策を含めたセキュリティ対策
      - ウェブサービス運営時のウェブサイトシステムを構成しているソフトウェアの継続的な脆弱性対応

ウェブサービス運営事業者側の対策が必要だが
利用者側でも漏えいを想定した対応を

【7位】ネット上の誹謗・中傷

～不満やストレス発散を目的とした過激な投稿の増加～

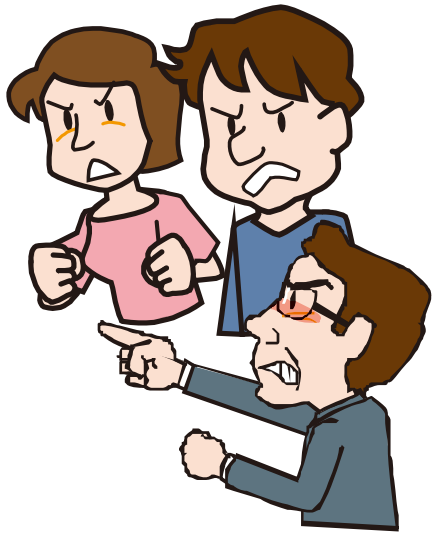


- コミュニティサイト（ブログ、SNS、掲示板等）で誹謗中傷や犯罪予告の書き込みが行われている
- 被害者への心理的脅迫や社会混乱等を招いている
- 投稿者は名誉棄損や営業妨害に問われることもある

【7位】ネット上の誹謗・中傷

～不満やストレス発散を目的とした過激な投稿の増加～

- 要因/目的
  - 情報モラルの欠如
  - 不満やストレスの発散
  - 知名度を上げるため
- 2016年の事例/傾向
  - 犯行予告の書き込み
    - 大学や自治体等を爆破する旨の犯行予告を投稿する事例が複数あった
    - 対象の組織は安全のため立ち入りを禁止する等の対応を行った
    - 投稿目的は「いたずらのつもりだった」や「目立ちたかった」であった
  - 某教授が軽率な発言で炎上
    - 過労自殺の事件に対して「過労死するのは情けない」と発言
    - 発言がネット上で拡散、批判が殺到した
    - 後に教授はコメントを削除し、謝罪のコメントを投稿

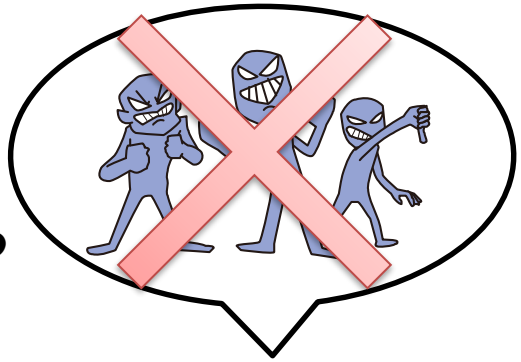


【7位】ネット上の誹謗・中傷

～不満やストレス発散を目的とした過激な投稿の増加～

IPA

- 対策一覧
  - 投稿者
    - 情報モラル・リテラシーの向上
      - 誹謗中傷や公序良俗に反する投稿を控える
      - 投稿前に内容を再確認
      - 情報モラル・リテラシーの教育
  - 誹謗中傷された側
    - 被害を受けた後の対策
      - 冷静な対応と支援者への相談
      - SNS運営会社に投稿の削除を依頼
      - 犯罪と思われる誹謗中傷の投稿は、警察へ被害届を提出



コメントを投稿するときは受け手に配慮を
誹謗中傷を受けた場合は、周囲の人に相談を

【8位】情報モラル欠如に伴う犯罪の低年齢化

～情報モラルを教育できる体制を構築しよう～

- 未成年者によるIT犯罪が引き続き発生
- 組織を狙った攻撃だけでなく、個人を狙った攻撃も

【8位】情報モラル欠如に伴う犯罪の低年齢化

～情報モラルを教育できる体制を構築しよう～

- 要因
  - 情報モラルの欠如
  - 情報リテラシー不足
  - 攻撃ツールの普及により誰でも攻撃を行える環境
- 2016年の事例/傾向
  - オンラインゲーム会社に対するDDoS攻撃
    - 大阪府高槻市の男子高校生が書類送検
    - 攻撃対象の会社の反応等を見るのが面白かった、自己顕示欲を満たしたかった、と供述している
  - 遠隔操作ウイルス感染
    - 16歳の男子高校生が逮捕
    - チートプログラムと騙して不特定多数にダウンロードさせていた

【8位】情報モラル欠如に伴う犯罪の低年齢化

～情報モラルを教育できる体制を構築しよう～

- 対策一覧
  - PC・スマートフォン利用者
    - 情報モラル・リテラシーの向上
      - 情報モラル・情報リテラシーの教育

家庭や学校でしっかりとした
情報モラル・情報リテラシーの教育を

【9位】インターネット上のサービスを悪用した攻撃

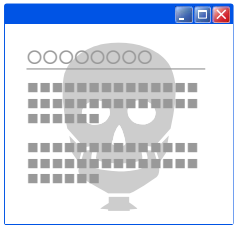
～怪しいサイトは見ないは通用しない。基本的な対策を確実に～

- ウェブサイトの不正広告によるウイルス感染被害が発生
- 正規サービス内のファイルをC&Cサーバーとして悪用し、不正な通信を正常な通信と誤認させる事例も

【9位】インターネット上のサービスを悪用した攻撃

～怪しいサイトは見ないは通用しない。基本的な対策を確実に～

- 手口/影響
  - 正規のウェブサイトに不正広告を表示し、クリックまたは閲覧した人をウイルスに感染させる
  - 正規サービスの通信に見せかけてC&Cサーバーと通信
- 2016年の事例/傾向
  - 音楽配信サービス「Spotify」の無料版に不正広告
    - ブラウザ上に不審なポップアップが表示され、トロイの木馬がダウンロードされる等の被害
  - 無料オンライン画像共有サービス「Imgur」を悪用してC&C通信
    - ウイルス感染によりPC内のデータをPNG形式の画像ファイルに加工し画像共有サービスにアップロード
    - ウイルスを検出されにくくする手法として利用したと考えられる



【9位】インターネット上のサービスを悪用した攻撃

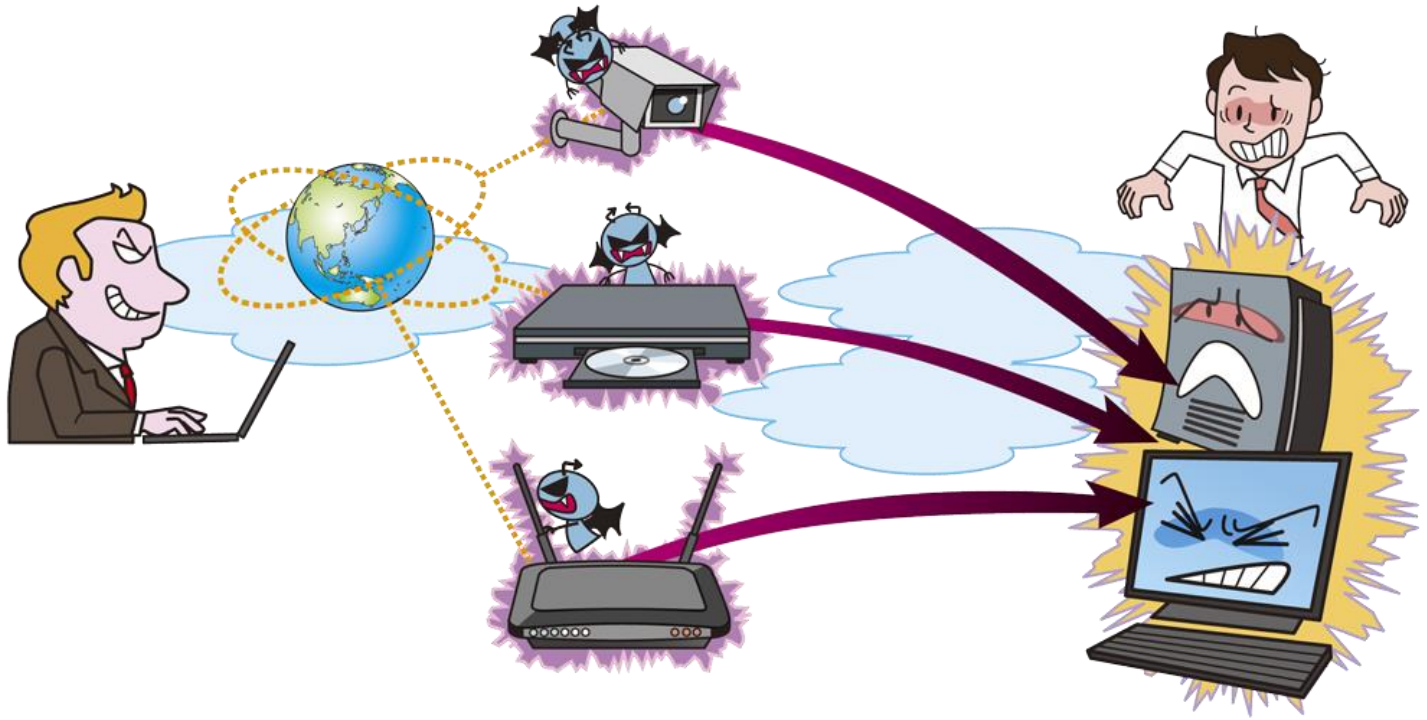
～怪しいサイトは見ないは通用しない。基本的な対策を確実に～

- **対策一覧**
  - **サービス提供ベンダー**
    - 情報リテラシーの向上
      - 登録情報の確認強化
      - 悪用防止に向けたサービスの見直し
    - 被害の早期検知
      - 運用やサービスの監視強化
  - **サービス利用者**
    - 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
      - 広告ブロックソフトウェアの利用

サービス提供ベンダーおよび利用者ともに
セキュリティ対策の実施を

【10位】IoT機器の不適切な管理

～ウイルス「Mirai」によるDDoS攻撃の被害が深刻化～



- 初期設定のまま利用しているIoT機器がウイルス感染し、DDoS攻撃等に悪用されている
- IoT機器の利用者は知らないうちに攻撃者となっている

【10位】IoT機器の不適切な管理

～ウイルス「Mirai」によるDDoS攻撃の被害が深刻化～

- 手口/影響
  - 初期設定に使用され易いユーザー名やパスワードを使ってIoT機器をウイルス「Mirai」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
  - 初期設定のままのIoT機器を乗っ取る

- 2016年の事例/傾向
  - TwitterやAmazon等、5時間にわたる接続困難になる被害
    - 該当組織のDNSサービスを提供している会社にDDoS攻撃
    - Miraiに感染したIoT機器で構成されたボットネットからの攻撃であった
  - 日本国内のネットワークカメラを覗き見
    - パスワードが未設定のままのネットワークカメラを利用されていた
    - 約4,300台分の映像が公開されていた

【10位】IoT機器の不適切な管理

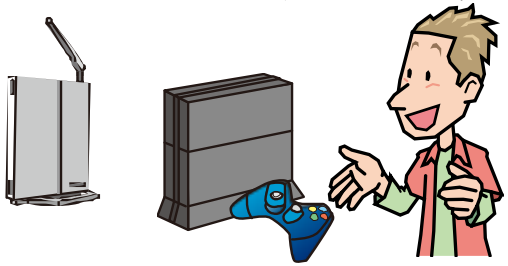
～ウイルス「Mirai」によるDDoS攻撃の被害が深刻化～

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
  - 初期設定されたパスワードを十分な長さを持つパスワードへ変更
  - 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
  - 初期パスワード変更の強制化
  - 脆弱性対策
  - 安全なデフォルト設定
  - わかり易い取扱説明書の作成

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

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