IPA Better Life with IT

情報セキュリティ10大脅威2018

～2章 情報セキュリティ10大脅威 個人編～

～引き続き行われるサイバー攻撃、あなたは守りきれますか？～

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
2018年4月

情報セキュリティ10大脅威 2018

- 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 2018
～引き続き行われるサイバー攻撃、あなたは守りきれますか？～
IPA 独立行政法人情報処理推進機構 セキュリティセンター
2018 年 3 月


2 章 情報セキュリティ 10 大脅威 2018

2017 年において社会的に影響が大きかったセキュリティ上の脅威について「10 大脅威選考会」の投票結果に基づき、「情報セキュリティ 10 大脅威 2018」では、「個人」と「組織」向けの脅威として、それぞれ表 2.1 の通り順位付けした。

本章では、「個人」と「組織」向けの脅威で 1 位～10 位となった脅威を「情報セキュリティ 10 大脅威 2018」として、「個人」向けの脅威は 2.1 節、「組織」向けの脅威は 2.2 節で解説する。

表 2.1 情報セキュリティ 10 大脅威 2018「個人」および「組織」向けの脅威の順位

「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等の不正利用	1	標的型攻撃による被害
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
ネット上の誹謗・中傷	3	ビジネスメール詐欺による被害
スマートフォンやスマートフォンアプリを狙った攻撃	4	脆弱性対策情報の公開に伴う悪用増加
ウェブサービスへの不正ログイン	5	脅威に対応するためのセキュリティ人材の不足
ウェブサービスからの個人情報の窃取	6	ウェブサービスからの個人情報の窃取
情報モラル欠如に伴う犯罪の低年齢化	7	IoT 機器の脆弱性の顕在化
ワンクリック請求等の不当請求	8	内部不正による情報漏えい
IoT 機器の不適切な管理	9	サービス妨害攻撃によるサービスの停止
偽警告によるインターネット詐欺	10	犯罪のビジネス化（アンダーグラウンドサービス）

15


組織における脅威は、経営層やシステム管理者、開発者、一般従業員等様々な立場存在します。立場が変わると注意すべき脅威も変わります。表 2.2 は、立場毎に注意すべき脅威を記載しています。立場毎の注意すべき脅威の参考にしてください。

表 2.2 10 大脅威 2018（組織）立場毎の注意すべき脅威

順位	脅威名（組織）	組織の立場	組織内の立場				
			経営層	セキュリティ管理者	システム管理者	開発部門長	一般従業員
1	標的型攻撃による被害	被害者	○	○	○	○	○
2	ランサムウェアによる被害	被害者	○	○	○	○	○
3	ビジネスメール詐欺による被害	被害者	○	○			○
4	脆弱性対策情報の公開に伴う悪用増加	ソフトウェアの提供者	○			○	
		ソフトウェアの利用者	○	○	○		○
5	脅威に対応するためのセキュリティ人材の不足	被害者	○	○	○	○	
6	ウェブサービスからの個人情報の窃取	ウェブサービスの提供者	○			○	
		ウェブサービスの利用者	○	○	○		
7	IoT 機器の脆弱性の顕在化	IoT 機器の開発者	○			○	
		IoT 機器の利用者	○	○	○		
8	内部不正による情報漏えい	被害者	○	○	○	○	○
9	サービス妨害攻撃によるサービスの停止	被害者	○	○	○		
10	犯罪のビジネス化（アンダーグラウンドサービス）	被害者	○	○	○	○	○

組織者：　代表取締役社長や理事等の組織のトップ等
セキュリティ管理者：　組織におけるセキュリティの管理者
システム管理者：　組織で運用しているシステムの管理者
開発部門長：　組織の開発者
一般従業員：　管理や組織、対策等の組織におけるIT利用者

本章で共通的に使われる用語について表 2.3 に定義を記載する。

表 2.3 情報セキュリティ 10 大脅威 2018 用語定義

用語	意味
個人	家庭等でスマートフォンや PC を利用する人
組織	企業、政府機関、公共団体等の組織およびその組織に所属している人
犯罪グループ	金銭や主義主張（ハクティビズム）を目的とした攻撃（犯罪）者集団
犯罪者	金銭や情報窃取（ストーカー行為を含む）を目的とした攻撃（犯罪）者
諜報員、産業スパイ	機密情報窃取を目的とした攻撃（犯罪）集団 国家組織の支援を受けた攻撃（犯罪）集団
IoT	モノのインターネット（Internet of Things）。ネットワークカメラや情報家電、医療機器といった様々な機器がインターネットにつながり、通信を行う仕組み。機器自体を指す場合は、IoT 機器と呼ぶ。
CSIRT	セキュリティインシデント等の問題が発生した際に原因究明や影響範囲の調査等を行う組織。自組織に関する問題に対応する場合は、自組織 CSIRT と呼ぶ。

16

情報セキュリティ10大脅威 2018

- 章構成
  - 1章.情報セキュリティ対策の基本 IoT機器(情報家電)編
    - IoT機器(情報家電)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 2018
    - 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

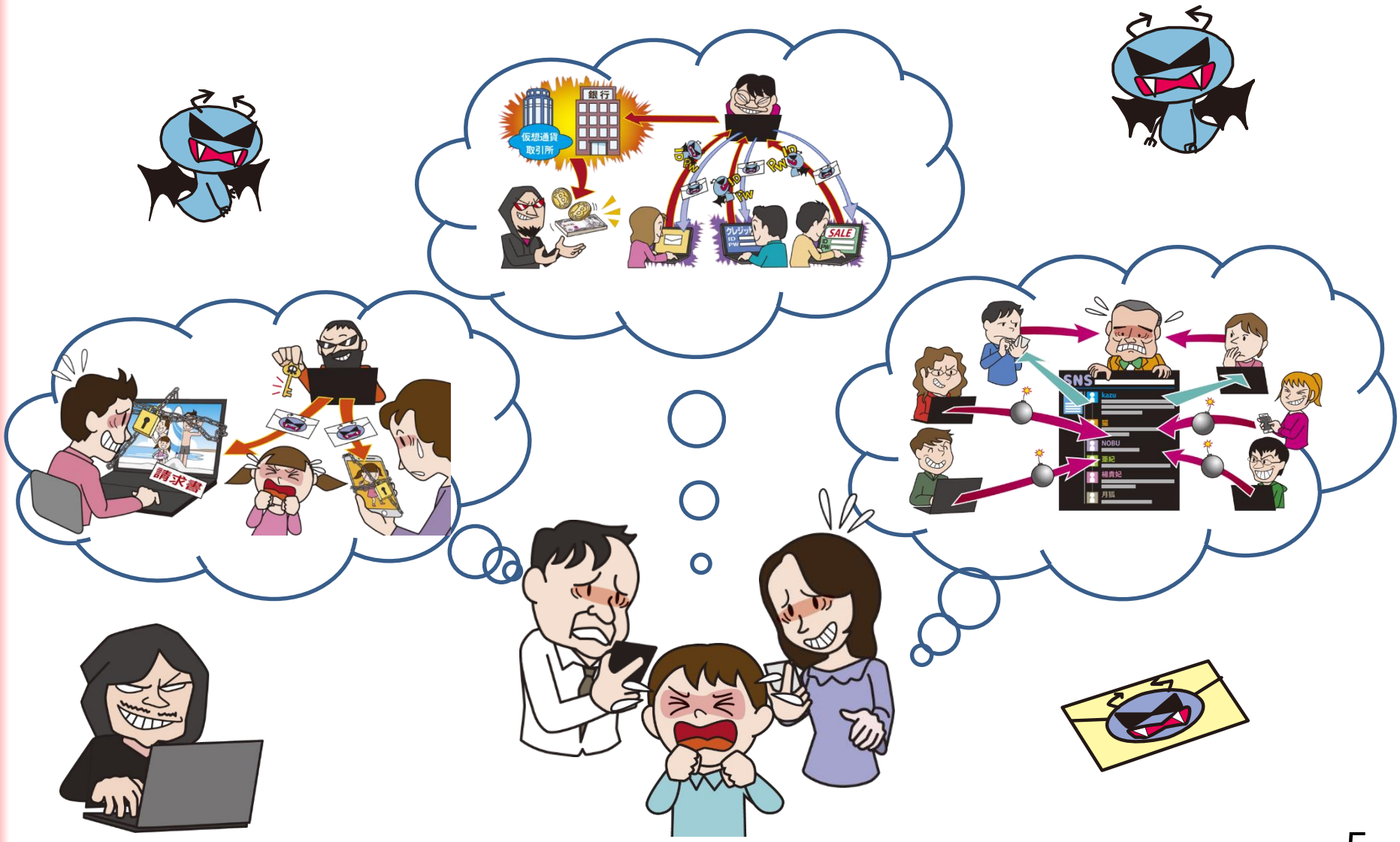
情報セキュリティ10大脅威 2018

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等の不正利用	1	標的型攻撃による被害
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
ネット上の誹謗・中傷	3	ビジネスメール詐欺による被害
スマートフォンやスマートフォンアプリを 狙った攻撃	4	脆弱性対策情報の公開に伴う 悪用増加
ウェブサービスへの不正ログイン	5	脅威に対応するための セキュリティ人材の不足
ウェブサービスからの個人情報の窃取	6	ウェブサービスからの個人情報の窃取
情報モラル欠如に伴う犯罪の低年齢化	7	IoT機器の脆弱性の顕在化
ワンクリック請求等の不当請求	8	内部不正による情報漏えい
IoT機器の不適切な管理	9	サービス妨害攻撃によるサービスの停止
偽警告による インターネット詐欺	10	犯罪のビジネス化 （アンダーグラウンドサービス）

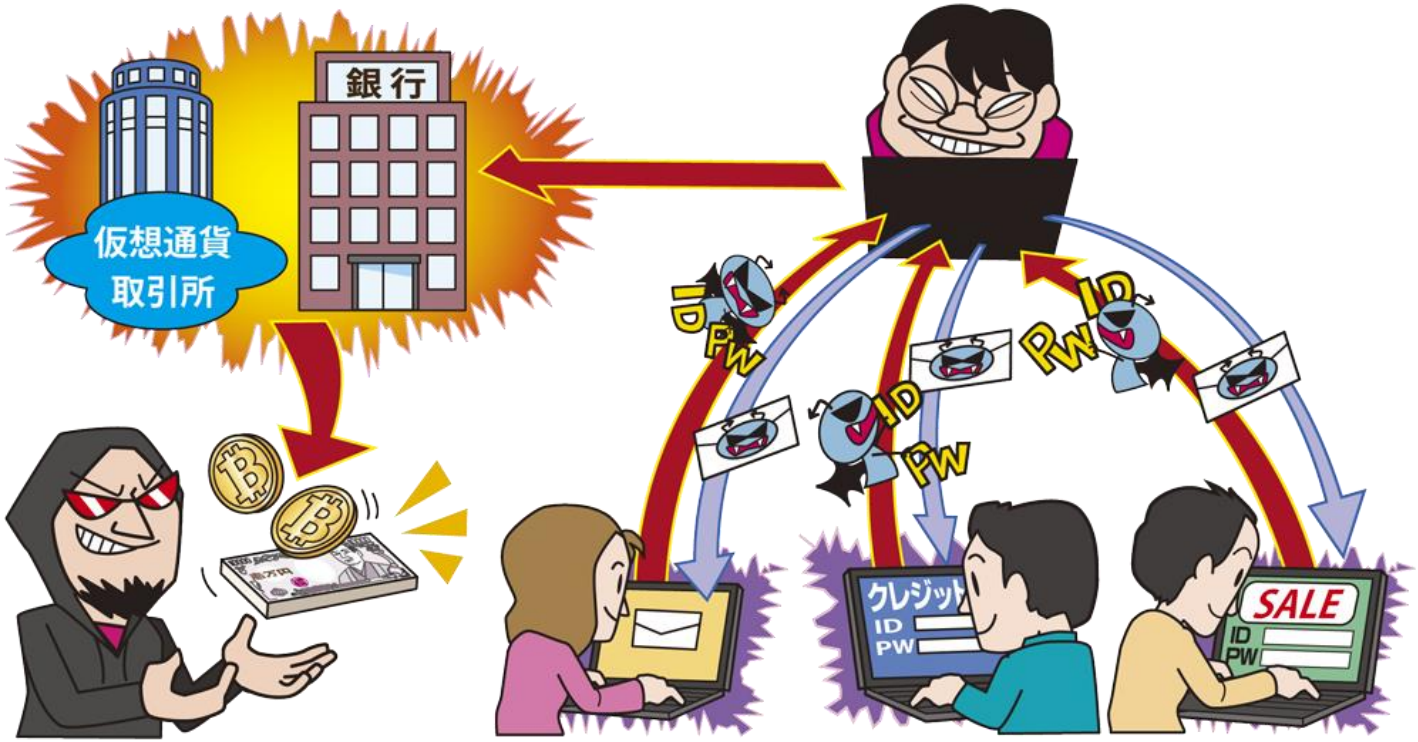
情報セキュリティ10大脅威 2018



2章. 情報セキュリティ10大脅威2018
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等の不正利用

～被害は継続して発生、仮想通貨に関する被害も～

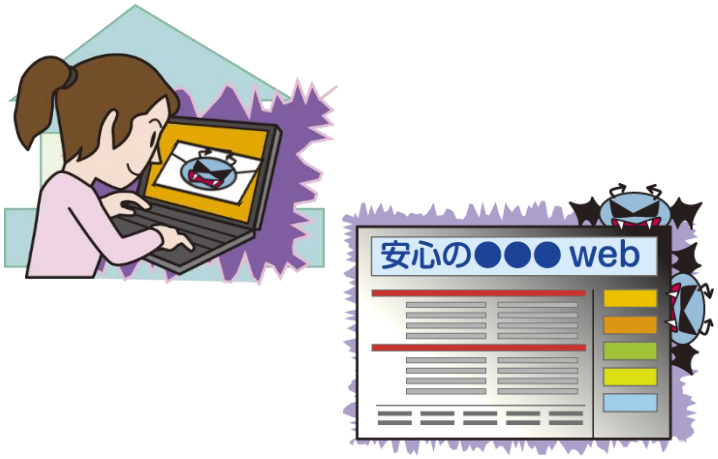


- ウイルス感染やフィッシング詐欺によりクレジットカード情報等を窃取され、不正送金等に悪用される
- ネットバンキングの他、仮想通貨利用者も標的に

【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等の不正利用

～被害は継続して発生、仮想通貨に関する被害も～

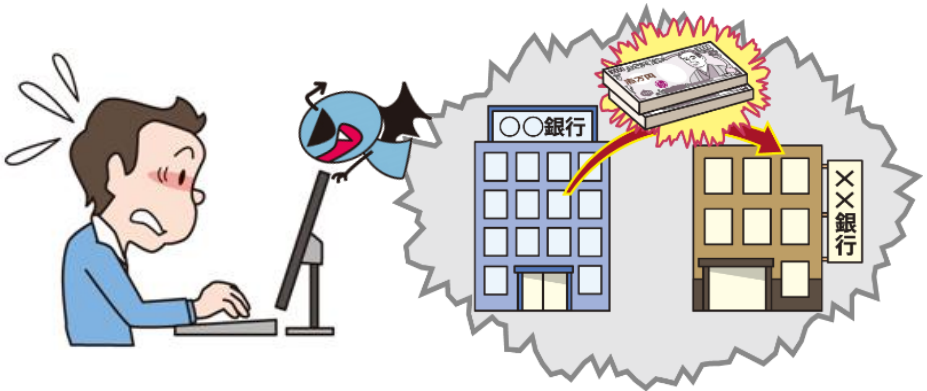
- **攻撃手口**
  - **ウイルス感染による認証情報の窃取**
    - 悪意あるファイルをメールに添付して送信し、ファイルを開かせる
    - 悪意あるウェブサイトが表示されるリンクをクリックさせる
  - **フィッシング詐欺による認証情報の窃取**
    - 実在する企業を模した偽のウェブサイトやURLを作成し、メールに記載されたリンクからアクセスさせる
    - メールの件名や本文に読まなければならないと思わせるような細工を施し、クリックを促す



【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等の不正利用

～被害は継続して発生、仮想通貨に関する被害も～

- 2017年の事例/傾向
  - 不正送金被害は減少傾向、仮想通貨交換所が攻撃対象に
    - 不正送金発生件数425件（前年より866件減少）
    - 個人の不正送金被害額約10億8,100万円（前年より約6億円減少）
    - 2017年は、仮想通貨交換所に対して送金を行う手口を確認
  - 情報窃取ウイルス「URSNIF」亜種による感染被害の増加
    - クレジットカード情報等を窃取される他、PCを乗っ取られる可能性も
  - クレジットカードの番号盗用被害額が増加
    - 番号盗用による被害額130億3,000万円（前年より2倍近くに増加）



【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等の不正利用

～被害は継続して発生、仮想通貨に関する被害も～

- **対策一覧**
  - **利用者**
    - 被害の予防
      - メールやウェブサイトの十分な確認
      - 添付ファイルやリンクを安易にクリックしない
      - 普段表示されない画面に個人情報等を入力しない
      - 事例や手口の情報収集
      - OS・ソフトウェアの更新
      - セキュリティソフトの導入
      - ファイルの拡張子を表示させる設定
      - パスワードの適切な管理と運用
      - 銀行が推奨する認証方式の利用
      - 仮想通貨の安全な利用（ウォレットの適切な管理等）
    - 被害の早期検知
      - 不審なログイン履歴の確認
      - 口座やクレジットカードの利用履歴を確認
      - 利用時のメール連絡機能等の活用
    - 被害を受けた後の対応
      - コールセンターへ連絡
      - クレジットカードの停止
      - システムの復元・初期化
      - パスワードの再設定

【2位】ランサムウェアによる被害

～ランサムウェアの感染経路拡大～

- PCやスマートフォンを暗号化・画面ロックされ、復旧のために金銭を要求される
- OSの脆弱性を悪用し、ネットワーク経由で感染を広げるランサムウェアが登場

【2位】ランサムウェアによる被害

～ランサムウェアの感染経路拡大～

- 攻撃手口
  - メールの添付ファイルから感染
    - メールにランサムウェア付きのファイルやランサムウェアをダウンロードするファイルを添付し、添付ファイルを開かせる
  - ウェブサイトから感染
    - リンクをクリックさせ、攻撃者が用意した悪意あるウェブサイトや改ざんされたウェブサイトを閲覧させる
  - OSの脆弱性を悪用
  - 公式マーケットに不正なアプリを公開
    - 入手したアプリの実体がランサムウェアの機能を持つ不正アプリ

【2位】ランサムウェアによる被害

～ランサムウェアの感染経路拡大～

- 2017年の事例/傾向
  - 自己増殖型のランサムウェア「WannaCry」の登場（5月）
    - OSの脆弱性を悪用した、ネットワークに接続されている PC間で感染を拡大するタイプが登場
    - 国内大手企業や地方公共団体等にも被害が発生
  - 対策されていない機器が、継続して攻撃の対象に（11月）
  - セキュリティ対策が日々進化する一方、攻撃手法も進化
    - 機械学習を利用したセキュリティ対策を回避するランサムウェアの登場

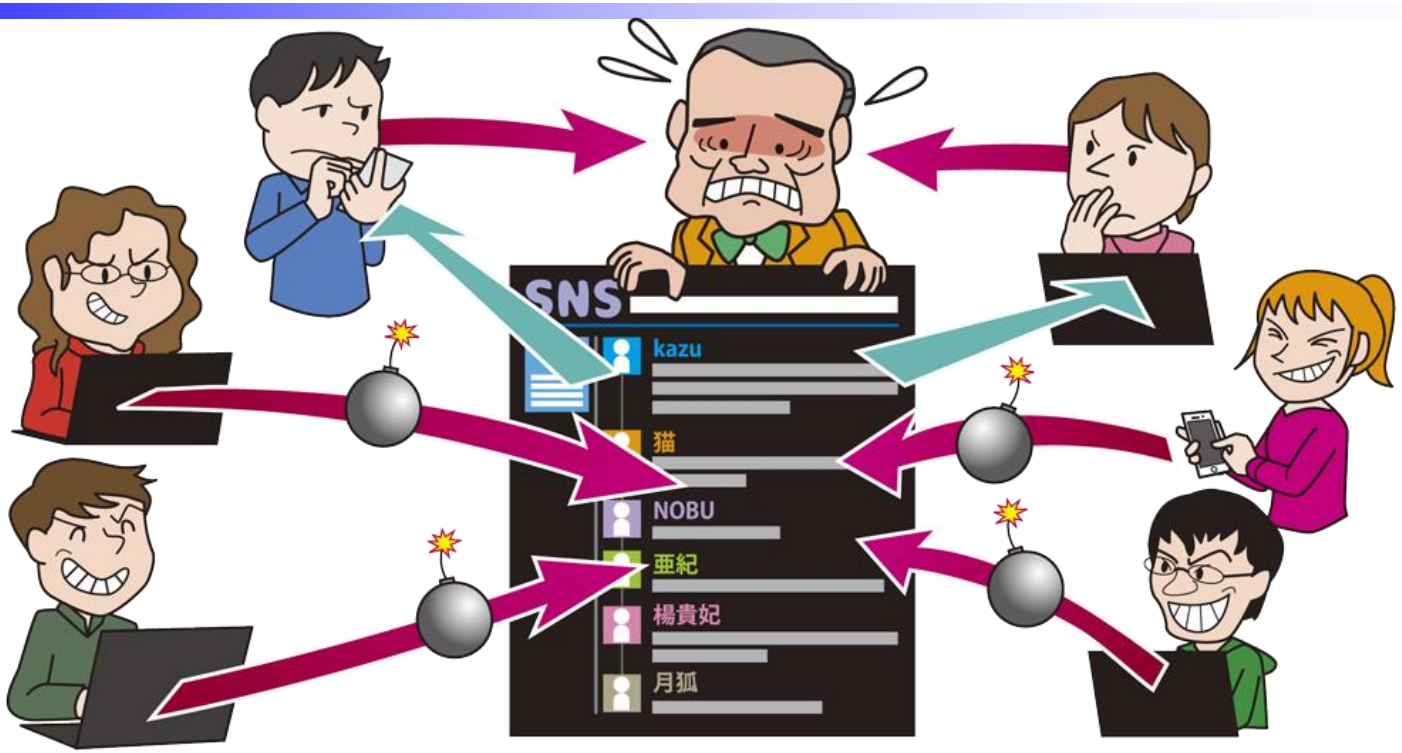
【2位】ランサムウェアによる被害

～ランサムウェアの感染経路拡大～

- 対策一覧
  - PC・スマートフォン利用者
    - 被害の予防
      - 受信メールやウェブサイトの十分な確認
      - 添付ファイルやリンクを安易にクリックしない
      - OS・ソフトウェアの更新
      - セキュリティソフトの導入、定義ファイルの更新
      - サポートの切れたOSの利用停止・移行
      - バックアップの取得
    - 被害を受けた後の対応
      - バックアップからデータを復旧
      - 復元ツールの活用
      - 復元機能の活用

【3位】ネット上の誹謗・中傷

～匿名性を悪用した心無い投稿が横行、情報モラルを身に着けよう～

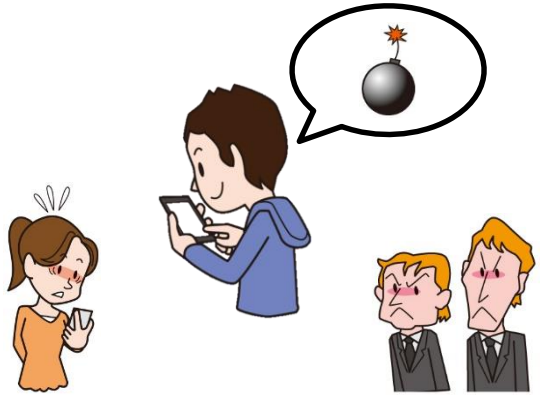


- コミュニティサイト上での誹謗・中傷や犯罪予告の書き込みが後を絶たない
- 関係のない第3者も誹謗・中傷に同調することでエスカレートすることも

【3位】ネット上の誹謗・中傷

～匿名性を悪用した心無い投稿が横行、情報モラルを身に着けよう～

- **要因/目的**
  - **情報モラルや自己抑制力の欠如**
    - 自分の発言が他人を心理的に追い詰めるおそれがあることを理解していない
    - 自身が持つ不満やストレスの捌け口として、過激な発言をしたり、個人・組織等の評判を落とすような発言を行う
  - **個人が発信できる公共の場(サービス)の増加**
    - 個人が自由に発信でき、かつ匿名であると勘違いした結果、発信者の詐称や誹謗・中傷、犯罪予告の発信に使われる



【3位】ネット上の誹謗・中傷

～匿名性を悪用した心無い投稿が横行、情報モラルを身に着けよう～

IPA

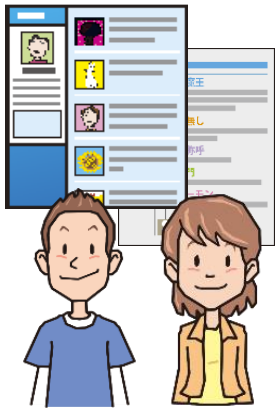
- 2017年の事例/傾向
  - 個人を中傷するブログを投稿
    - 投稿者は被害関係者から業務妨害した疑いで書類送検
    - 投稿目的は「ブログの閲覧数を伸ばし、広告収入を得るため」
  - 掲示板やウェブサイト等を使った脅迫行為
    - 家電量販店に設置されたPCを使い犯行予告を投稿
  - 容疑者の父親というデマ拡散により業務妨害
    - 嫌がらせや中傷を含む電話が容疑者と無関係な会社に殺到

【3位】ネット上の誹謗・中傷

～匿名性を悪用した心無い投稿が横行、情報モラルを身に着けよう～

IPA

- 対策一覧
  - 投稿者
    - 情報モラル・リテラシー、法令順守の意識の向上
      - 誹謗・中傷や公序良俗に反する投稿はしない
      - 投稿前に内容を再確認
  - 投稿を閲覧した側
    - 情報モラル・リテラシー、法令順守の意識の向上
      - 情報の信頼性を確認
      - 誹謗・中傷された人を支える
  - 誹謗・中傷された側
    - 被害を受けた後の対応
      - 冷静な対応と支援者への相談
      - 犯罪と思われる誹謗・中傷の投稿は警察へ被害届を提出
      - ウェブサイトの管理者やプロバイダーへ削除依頼



【4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

～依然として公式アプリストアにも不正アプリが存在、ウイルス感染に注意～

- 不正なアプリがマーケット内に公開されている
- 知らずにインストールすることで不正操作される
- ランサムウェアの機能を持つ不正アプリも確認

【4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
～依然として公式アプリストアにも不正アプリが存在、ウイルス感染に注意～

- 攻撃手口
  - 公式マーケットに不正なアプリを紛れ込ませる
  - 人気アプリに偽装
    - ダウンロード件数等が多い人気アプリに偽装して、公式マーケットに公開する
- 影響
  - 連絡先等の端末内の重要な情報を窃取
  - 録画・写真・通話録音機能を不正に利用
  - ランサムウェアへの感染
  - DDoS攻撃等の踏み台

【4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
～依然として公式アプリストアにも不正アプリが存在、ウイルス感染に注意～

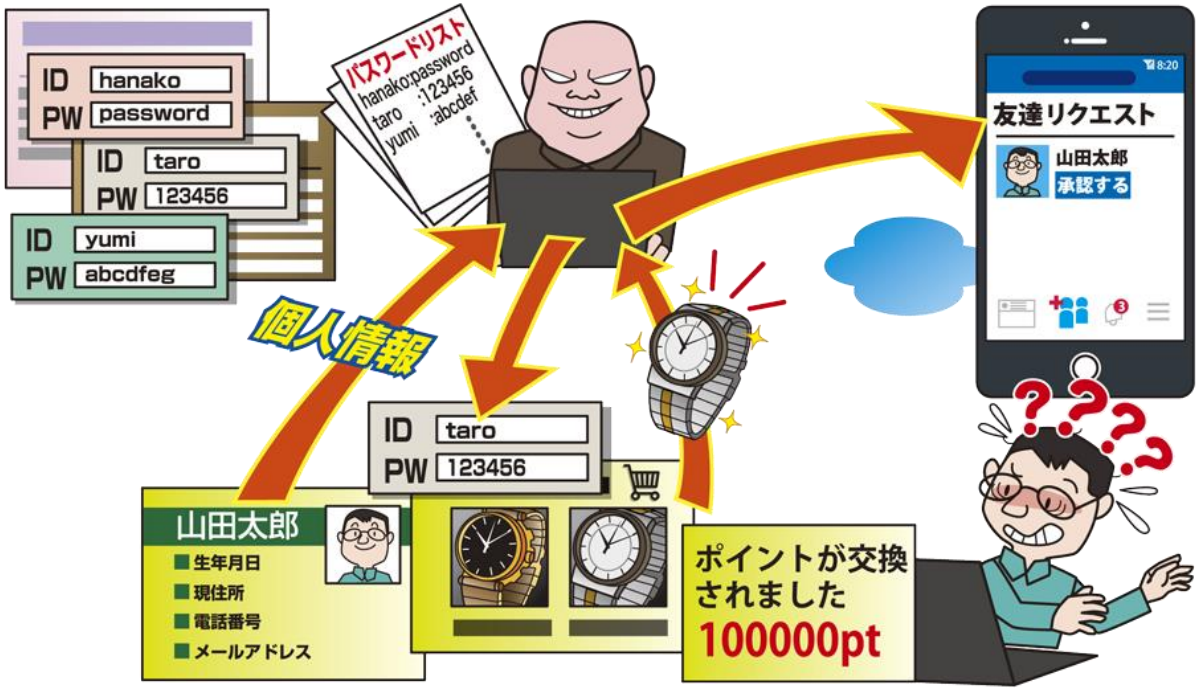
- 2017年の事例/傾向
  - 人気アプリに便乗した不正アプリが存在
  - ルートキットを組み込んだ「ZNIU」ウイルスの登場
    - Linuxの脆弱性「Dirty COW」を悪用したウイルス
    - 感染すると管理者権限を持つバックドアを仕込まれ、攻撃者にリモートでスマートフォンを乗っ取られる可能性
  - Android端末向けランサムウェア「LeakerLocker」の登場
    - 感染すると、個人情報を連絡先に登録されているすべての宛先に転送すると利用者を脅迫し、金銭を要求する
  - Android端末を攻撃の踏み台にする不正アプリの登場

【4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
～依然として公式アプリストアにも不正アプリが存在、ウイルス感染に注意～

- **対策一覧**
  - **利用者**
    - **被害の予防**
      - アプリは公式マーケットから入手
      - アクセス権限を確認
      - OS・アプリの更新
      - セキュリティソフトの導入
      - セキュリティ設定の実施
      - バックアップの取得
    - **被害を受けた後の対応**
      - 不正アプリのアンインストールや端末初期化
      - バックアップから復旧

【5位】ウェブサービスへの不正ログイン

～パスワードの使いまわしに注意～



- 不正に取得した認証情報を使い、ウェブサービスを不正利用される
- 利用者が推測されやすいパスワードの使用やパスワードの使いまわしをしている場合に被害に遭う

【5位】ウェブサービスへの不正ログイン

～パスワードの使いまわしに注意～

IPA

- 手口/影響
  - パスワードリスト攻撃
    - 他のウェブサイトから漏えいしたIDとパスワードを組み合わせて悪用
    - 複数のウェブサイトで同じIDとパスワードを利用していた場合、それらのウェブサイトも不正ログインされる
  - パスワード推測攻撃
    - 利用者が使いそうなパスワードを推測して不正ログインを試みる
    - IDとパスワードが同一、または単純な単語、連続した英数字を使用していた場合、攻撃者に推測されてしまう
  - ウイルス感染
    - 感染した端末から窃取した情報を使用して、利用者に成りすましウェブサービスを不正利用

【5位】ウェブサービスへの不正ログイン

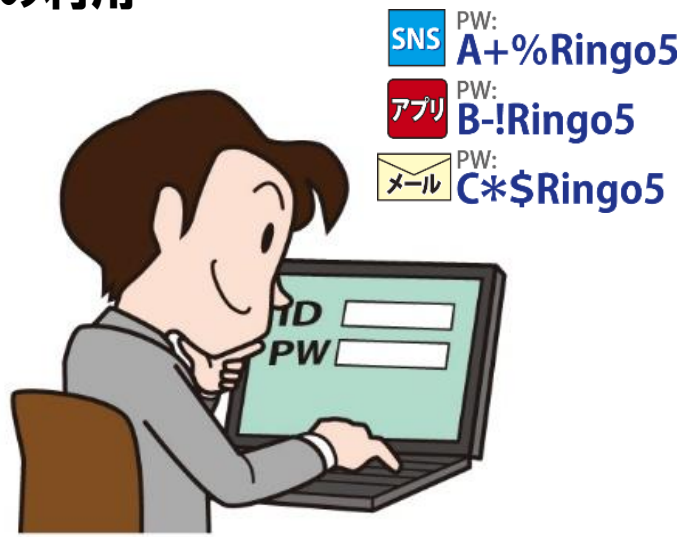
～パスワードの使いまわしに注意～

- 2017年の事例/傾向
  - 不正ログインによる個人情報流出とポイントの不正利用
    - ガス・電気料金情報のWeb照会サービスに不正ログイン
  - アカウント乗っ取りの被害を受けた経験者が全体の約4割
    - インターネットや端末のセキュリティを「意識していない」という回答をした人も全体の約3割
  - 面識のない女性のアカウントを不正利用
    - IDやパスワードはSNSに公開されている名前や誕生日から推測
    - ウェブサービスに保存されている画像を盗み見ていた

【5位】ウェブサービスへの不正ログイン

～パスワードの使いまわしに注意～

- 対策一覧
  - ウェブサービス利用者
    - 被害の予防
      - 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
      - パスワード管理ソフトの利用
      - ウェブサービスが推奨する認証方式の利用
      - 利用をやめたサービスの退会
    - 被害を受けた後の対応
      - パスワードの変更
      - クレジットカードの停止



【6位】ウェブサービスからの個人情報の窃取

～ウェブサービスの利用者は登録する個人情報を必要最小限に～

- ウェブサービスの脆弱性を悪用され、登録した個人情報やクレジットカード情報等を窃取される
- 窃取した情報を悪用され、不審メールを送信されたり、クレジットカード情報を悪用される

【6位】ウェブサービスからの個人情報の窃取

～ウェブサービスの利用者は登録する個人情報を必要最小限に～

- 手口/影響
  - ソフトウェアの脆弱性を悪用
    - 脆弱性を悪用した攻撃により、個人情報等の重要情報が窃取される
  - 広く使用されているソフトウェアの脆弱性
    - ウェブサービスで広く使用されているソフトウェアに脆弱性が発見され、かつ攻撃手法が判明すると、多くのウェブサービスで同様の攻撃や被害が発生する

【6位】ウェブサービスからの個人情報の窃取

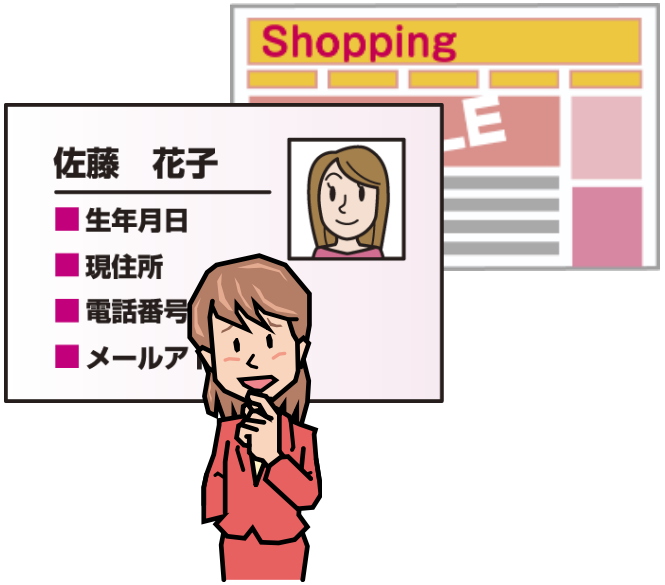
～ウェブサービスの利用者は登録する個人情報を必要最小限に～

- 2017年の事例/傾向
  - 都税クレジット支払いサイトに不正アクセス
    - 約72万件のクレジットカードに関する情報が漏えいした可能性
    - 不正アクセスは、ウェブサービスで広く利用されている「Apache Struts2」の脆弱性を悪用
  - 通販サイトのアプリケーションの脆弱性を突く不正アクセス
    - 公式通販サイトで最大189件の個人情報やクレジットカード情報が漏えいした可能性
  - テレビ局に不正アクセス
    - ウェブサイトが不正アクセスを受け、約1,270件の氏名とメールアドレスを流出した可能性
    - サーバーに存在する脆弱性を悪用され不正アクセスされた可能性

【6位】ウェブサービスからの個人情報の窃取

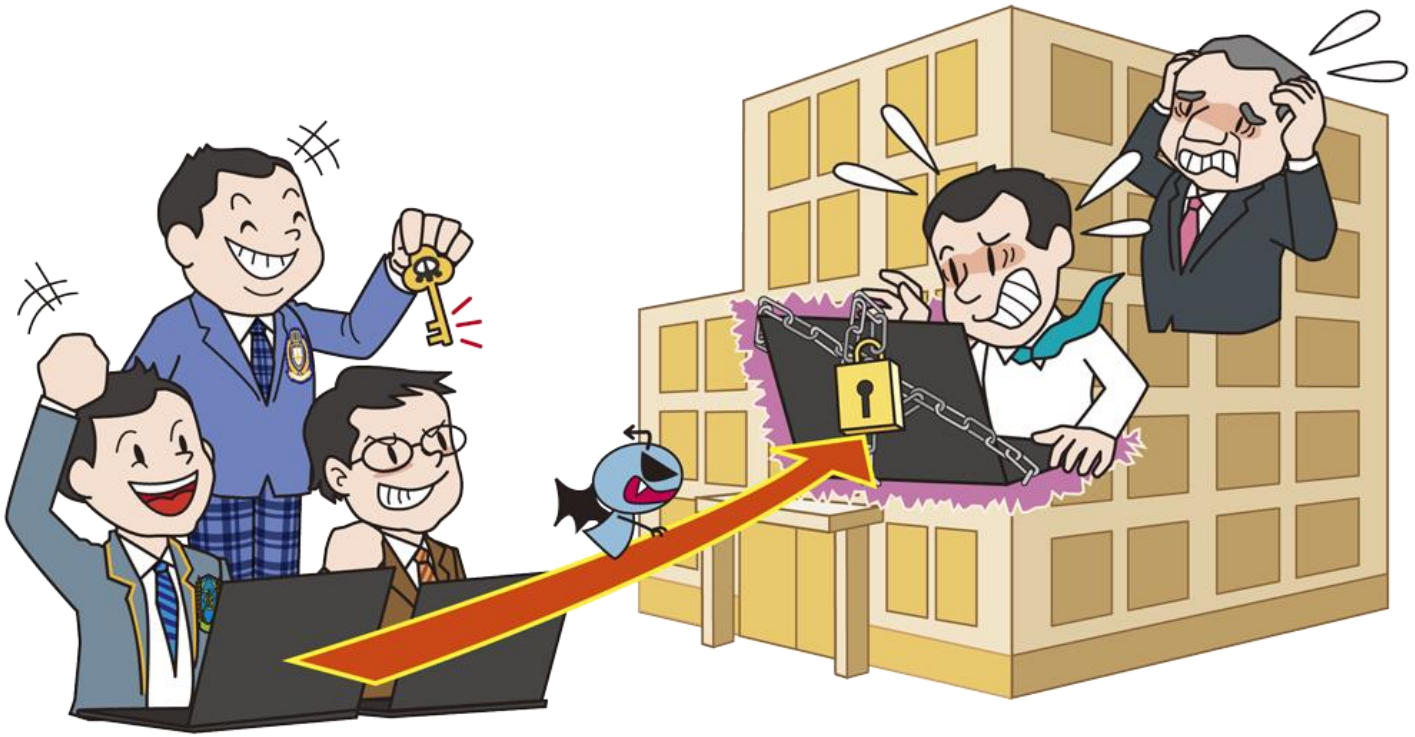
～ウェブサービスの利用者は登録する個人情報を必要最小限に～

- 対策一覧
  - ウェブサービス利用者
    - 情報リテラシーの向上
      - 不要な情報は登録しない
      - 利用しないウェブサービスの退会
    - 被害の早期発見
      - クレジットカードの利用明細を確認
    - 被害を受けた後の対応
      - カード会社へ連絡
      - クレジットカードの停止
      - パスワードの変更



【7位】情報モラル欠如に伴う犯罪の低年齢化

～未来ある若者に情報モラル教育を～

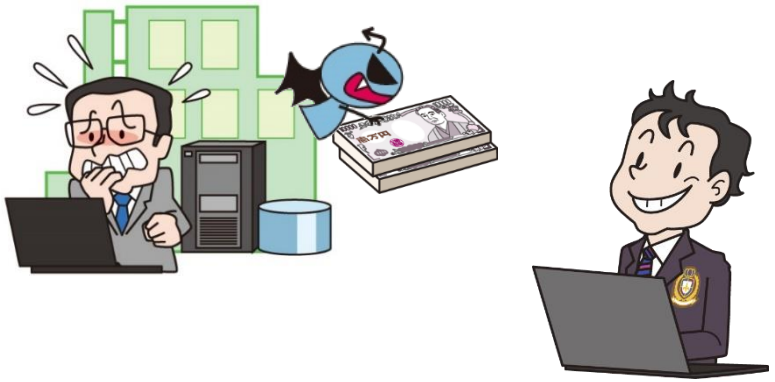


- 2017年も未成年者によるサイバー犯罪を確認
- インターネットを通じて、サイバー攻撃に悪用できるツールや知識の入手し、悪用している

【7位】情報モラル欠如に伴う犯罪の低年齢化

～未来ある若者に情報モラル教育を～

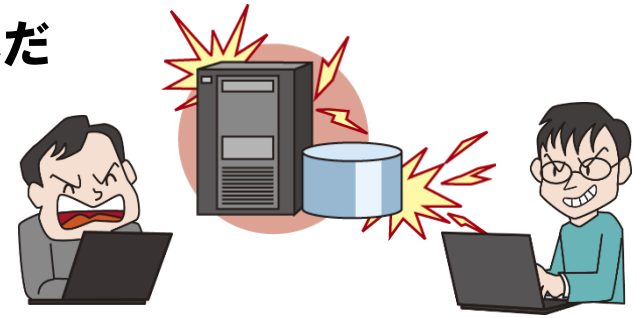
- **要因**
  - **情報モラルの欠如**
    - 自分の行為が犯罪であることを理解した上で、金銭目的などの私利私欲のためにサイバー犯罪を行う
    - 自己顕示欲や社会騒乱を目的に行う
    - 注目を集めるために、SNS等で犯行声明を出したり、標的を募集する
  - **情報リテラシーの不足**
    - 自分の行為が犯罪であることを理解せず、面白半分に行ってしまう
  - **攻撃ツールや攻撃サービスの流通**



【7位】情報モラル欠如に伴う犯罪の低年齢化

～未来ある若者に情報モラル教育を～

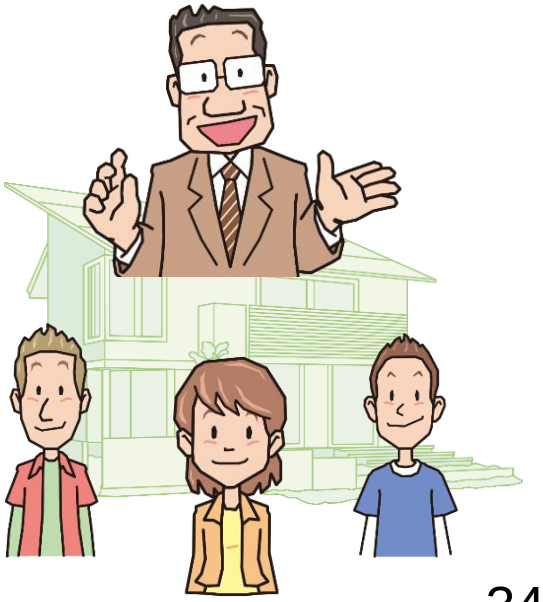
- 2017年の事例/傾向
  - 未成年者がランサムウェアを作成し逮捕される
    - 14歳の少年がインターネット上のソフトウェア等を組み合わせて作成
    - ランサムウェアを作成した動機は「自分の知名度を上げるため」
  - フリーマーケットアプリ「メルカリ」でウイルス情報を売買
    - 13歳の少年がコンピュータウイルスに関する情報を出品
    - 出品した少年は金銭目的のため、購入の意思を示した少年らはウイルスを使い、いたずらをするため
  - 高校生3人がゲームサーバーに不正アクセス
    - 被害者(中学生)のIDとパスワードを使って不正アクセスを行い、勝手に467万円分の有料契約を結んだ



【7位】情報モラル欠如に伴う犯罪の低年齢化

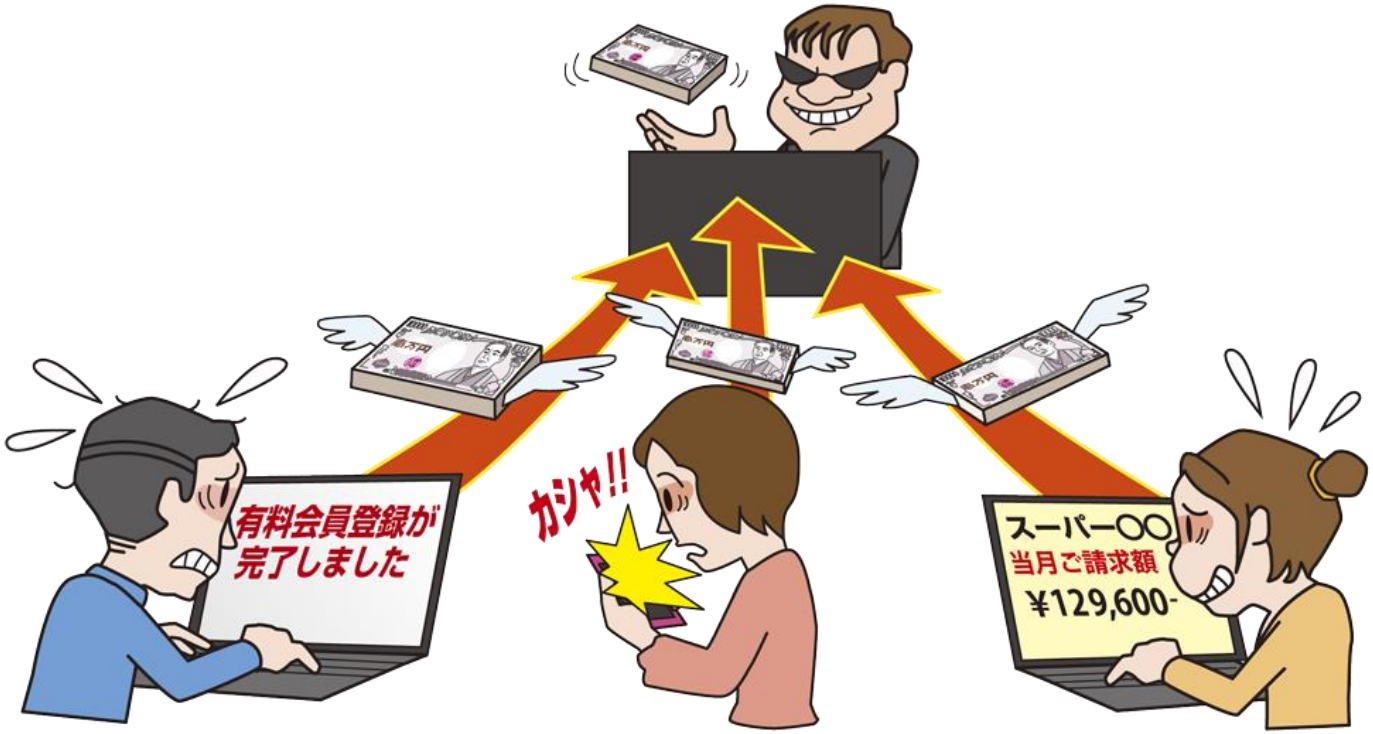
～未来ある若者に情報モラル教育を～

- 対策一覧
  - 利用者（家庭・教育機関）
    - 情報モラルや情報リテラシーの向上
      - 情報モラルや情報リテラシーの教育、法教育の徹底
    - 被害の予防
      - インターネットの利用を制限するサービスやアプリを活用
      - 未成年者に不要な機器を持たせない



【8位】ワンクリック請求等の不当請求

～複数回のクリックにより不当請求されるケースも～



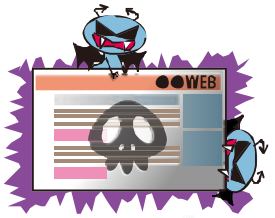
- PCやスマートフォンに請求画面が表示され、金銭を不当に請求される被害が依然として発生
- 複数回クリックさせることで、請求の正当性を主張するケースも

【8位】ワンクリック請求等の不当請求

～複数回のクリックにより不当請求されるケースも～

IPA

- 手口/影響
  - 悪意あるウェブサイトの閲覧
    - 表示されている画像をクリックすることで、会員登録完了画面に遷移し、不当に金銭を要求される
  - メールに記載されたリンクのクリック
    - 入会完了画面が表示され、高額な入会金を請求される
  - 不正プログラム・アプリをインストールさせる
    - 無料動画ダウンロード等と偽り、インストールを促す
  - 電話をかけるように誘導
    - 電話をかけさせ、金銭の支払いを迫る
    - 退会や支払いを免除するためと称して個人情報を聞き出す
  - スマートフォンの機能の悪用
    - 偽のシャッター音を鳴らすことで利用者の不安を煽り、金銭を要求する



【8位】ワンクリック請求等の不当請求

～複数回のクリックにより不当請求されるケースも～

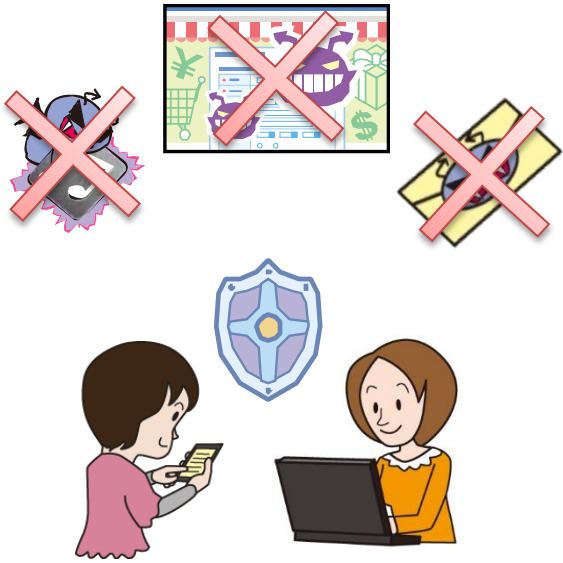
- 2017年の事例/傾向
  - 依然として多いワンクリック請求サイト
    - 2017年10月には160万件以上の詐欺サイトを確認
    - PCだけでなくスマートフォンを対象にした詐欺サイトも
  - 複数回クリックさせる詐欺の登場
    - 「再生」や「同意」等の項目を複数回クリックしたことを入会の意思とし、不当な請求を行う
  - ワンクリック請求の被害者を狙った詐欺
    - 被害者が「消費生活センター」と検索し、検索結果の上位に表示された公的機関以外に相談した結果、依頼料が請求される
  - ワンクリック請求によりギフト券を騙し取る
    - 退会料という名目でギフト券を購入させ、利用番号を聞き出す

【8位】ワンクリック請求等の不当請求

～複数回のクリックにより不当請求されるケースも～

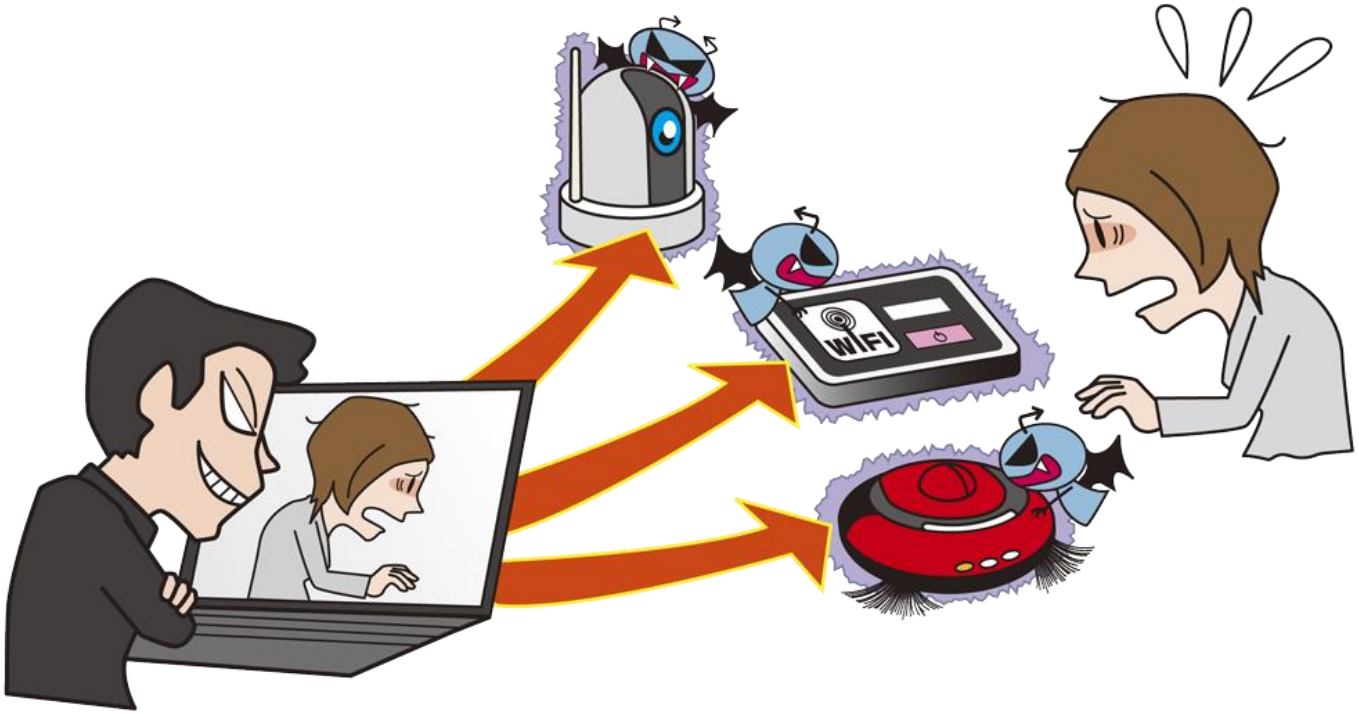
IPA

- 対策一覧
  - ウェブサービスの利用者
    - 被害の予防
      - 不当請求に応じない
      - 受信したメールの内容を確認
      - アクセスするウェブサイトの確認
      - SNS（Twitter、Facebook 等）のメッセージのリンクを不用意にクリックしない
      - アプリのアクセス権限の確認
      - 事件・手口の情報収集と学習
    - 被害を受けた後の対応
      - 相談する際には信頼できる機関を利用（国民生活センター・消費生活センター・警察）
      - システムの復元・初期化



【9位】IoT機器の不適切な管理

～普及するIoT 製品、利用の前にセキュリティ対策を～



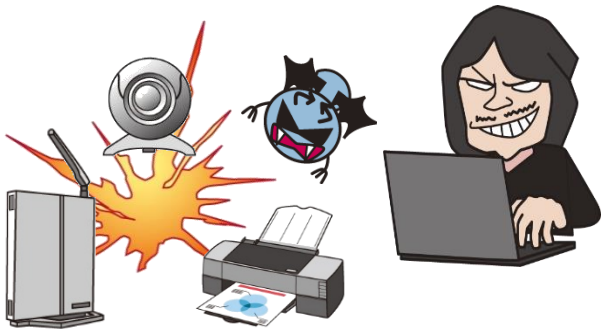
- 管理を怠っているIoT機器が乗っ取られる
- 遠隔からIoTカメラを通じて室内の覗き見や盗撮をされる
- 「悪意の無い加害者」としてDDoS攻撃に加担してしまう

【9位】IoT機器の不適切な管理

～普及するIoT 製品、利用の前にセキュリティ対策を～

IPA

- 手口/影響
  - 初期設定のままのIoT機器にウイルスを感染させる
  - 脆弱性を悪用した攻撃
    - 公開された脆弱性を悪用し、IoT機器を乗っ取る
  - IoT機器からIoT機器へと感染を拡大させる
  - 覗き見や盗撮
    - カメラ機能を持つIoT機器を乗っ取り、遠隔からカメラを操作する
  - DDoS攻撃等の踏み台



【9位】IoT機器の不適切な管理

～普及するIoT 製品、利用の前にセキュリティ対策を～

- 2017年の事例/傾向
  - IoT機器に感染するウイルス「Mirai」亜種が活発化
    - 国内メーカーのWiFiルーター11機種が被害を受ける
  - IoT機器を破壊するウイルス「BrickerBot」
    - 感染すると、IoT機器を完全に使用不能にする
    - 目的は「Mirai」などのウイルス感染したIoT機器に対抗するため
  - ロボット掃除機を不正に操作される脆弱性
    - 脆弱性を悪用されることで、掃除機を乗っ取られる

【9位】IoT機器の不適切な管理

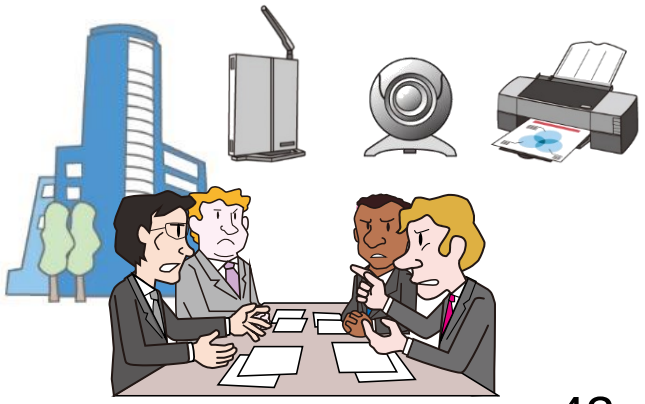
～普及するIoT 製品、利用の前にセキュリティ対策を～

IPA

● 対策一覧

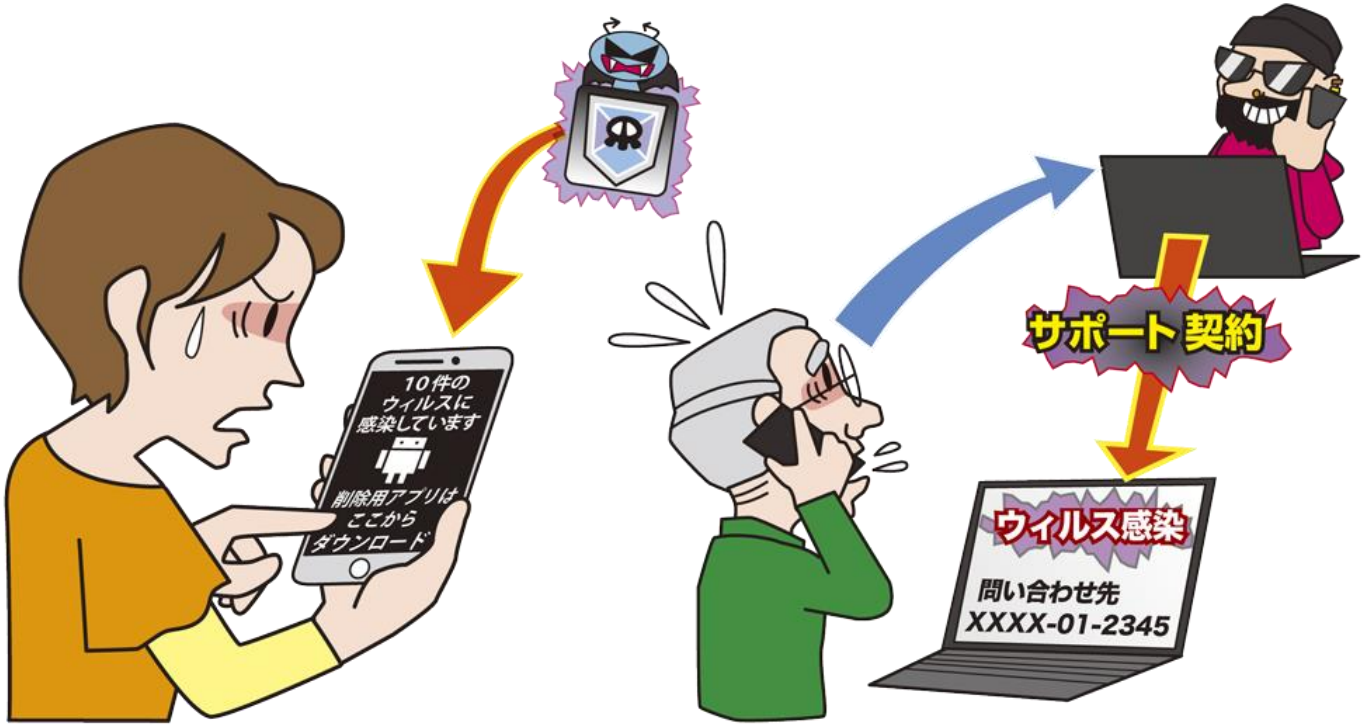
■ IoT機器の利用者

- 情報リテラシーの向上
  - 使用前に取り扱い説明書を確認
- 被害の予防
  - 初期設定のパスワードから長く複雑なものへ変更
  - 不要な機能やポートは無効化
  - パッチが更新されたら迅速に更新（自動更新を有効にする）
  - 使用していないときはIoT機器の電源を切る
  - 廃棄前や下取りに出す前に必ず初期化
- 被害を受けた後の対応
  - IoT機器の電源を切る
  - IoT機器の初期化後、「被害の予防」を実施
  - メーカーのサポート窓口に相談する



【10位】偽警告によるインターネット詐欺

～その警告メッセージ、信じて大丈夫？～



- 偽警告に記載された操作を行うことで、金銭的な被害や個人情報などを窃取される
- 巧妙な細工が施され、偽警告の閲覧者を信じ込ませる

【10位】偽警告によるインターネット詐欺

～その警告メッセージ、信じて大丈夫？～

- 手口/影響
  - 「ウイルスに感染している」等の偽警告を表示し、従わせる
  - 警告音や警告アナウンスを流して不安を煽る
    - スマートフォンの場合、バイブレーション機能を使用するケースも
  - サポート窓口を装い、電話をかけさせる
    - 電話越しに「遠隔操作で確認する」という旨を説明し、不正な遠隔操作ソフトをインストールさせる

【10位】偽警告によるインターネット詐欺

～その警告メッセージ、信じて大丈夫？～

- 2017年の事例/傾向
  - アニメーション等を利用した巧妙な騙しの手口
    - マウスのポインターが勝手に動いているようなアニメーションを表示
    - マイクロソフト社のURLにアクセスしているような画像を表示
    - 「5分以内」等の時間制限を表示して利用者を焦らせる
  - Google社を騙る偽警告
    - スマートフォン上に「ウイルスに感染している」という偽警告が表示
    - Google社を偽装した画面が表示され、アプリの入手と実行を促される

【10位】偽警告によるインターネット詐欺

～その警告メッセージ、信じて大丈夫？～

- 対策一覧
  - インターネット利用者
    - 被害の予防
      - 事例や手口の情報収集
      - 偽警告が表示されても安易に従わない
      - 偽警告が表示されたらブラウザを終了する
    - 被害を受けた後の対応
      - 遠隔操作ソフトをアンインストール
      - サポート契約の解消

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 2018
https://www.ipa.go.jp/security/vuln/10threats2018.html