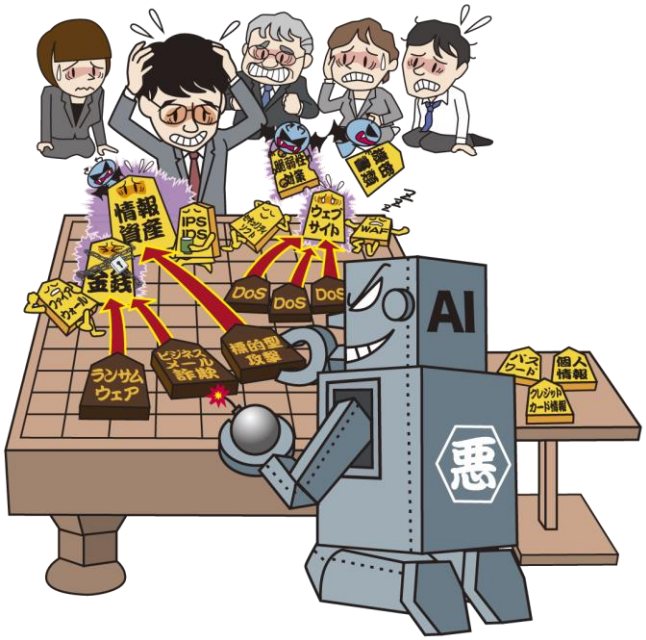
IPA Better Life with IT

# 情報セキュリティ10大脅威 2019

## ～情報セキュリティ10大脅威 個人編～

### ～局面ごとにセキュリティ対策の最善手を～




独立行政法人情報処理推進機構（IPA）
セキュリティセンター
2019年4月

# 情報セキュリティ10大脅威 2019

- 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 2019

～局面ごとにセキュリティ対策の最善手を～



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

2019 年 3 月


1 章 情報セキュリティ 10 大脅威 2019 概要

■「情報セキュリティ 10 大脅威 2019」

2018 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 2019」では、「個人」と「組織」向け脅威として、それぞれ表 1.1 の通り順位付けした。

表 1.1 情報セキュリティ 10 大脅威 2019「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 |
|---|---|---|
| クレジットカード情報の不正利用 | 1 | 標的型攻撃による被害 |
| フィッシングによる個人情報等の詐取 | 2 | ビジネスメール詐欺による被害 |
| 不正アプリによる スマートフォン利用者への被害 | 3 | ランサムウェアによる被害 |
| メール等を使った 脅迫・詐欺の手口による金銭要求 | 4 | サプライチェーンの弱点を悪用した 攻撃の高まり |
| ネット上の誹謗・中傷・デマ | 5 | 内部不正による情報漏えい |
| 偽警告によるインターネット詐欺 | 6 | サービス妨害攻撃によるサービスの停止 |
| インターネットバンキングの不正利用 | 7 | インターネットサービスからの 個人情報の窃取 |
| インターネットサービスへの不正ログイン | 8 | IoT 機器の脆弱性の顕在化 |
| ランサムウェアによる被害 | 9 | 脆弱性対策情報の公開に伴う悪用増加 |
| IoT 機器の不適切な管理 | 10 | 不注意による情報漏えい |

IPA から「10 大脅威選考会」に 2019 年版の投票を依頼するにあたり、2018 年版の脅威候補に対して見直しを行った。

本章では、「情報セキュリティ 10 大脅威 2019」の脅威候補の変更点と「情報セキュリティ 10 大脅威 2019」にランクインした脅威の特徴を記載する。なお、各脅威の詳細については 2 章にて解説する。

6

# 情報セキュリティ10大脅威 2019

- 章構成
  - 1章.情報セキュリティ10大脅威 2019 概要
    - 10大脅威の概要および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 2019
    - 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 2019 脅威ランキング

IPA

| 「個人」向け脅威 | 順位 | 「組織」向け脅威 |
|---|---|---|
| クレジットカード情報の不正利用 | 1 | 標的型攻撃による被害 |
| フィッシングによる個人情報等の詐取 | 2 | ビジネスメール詐欺による被害 |
| 不正アプリによる<br>スマートフォン利用者への被害 | 3 | ランサムウェアによる被害 |
| メール等を使った<br>脅迫・詐欺の手口による金銭要求 | 4 | サプライチェーンの弱点を悪用した<br>攻撃の高まり |
| ネット上の誹謗・中傷・デマ | 5 | 内部不正による情報漏えい |
| 偽警告によるインターネット詐欺 | 6 | サービス妨害攻撃によるサービスの停止 |
| インターネットバンキングの不正利用 | 7 | インターネットサービスからの<br>個人情報の窃取 |
| インターネットサービスへの不正ログイン | 8 | IoT機器の脆弱性の顕在化 |
| ランサムウェアによる被害 | 9 | 脆弱性対策情報の公開に伴う悪用増加 |
| IoT機器の不適切な管理 | 10 | 不注意による情報漏えい |

# 情報セキュリティ対策の基本

| 攻撃の糸口 | 情報セキュリティ対策の基本 | 目的 |
|---|---|---|
| ソフトウェアの脆弱性 | ソフトウェアの更新 | 脆弱性を解消し攻撃によるリスクを低減する |
| ウイルス感染 | セキュリティソフトの利用 | 攻撃をブロックする |
| パスワード窃取 | パスワードの管理・認証の強化 | パスワード窃取によるリスクを低減する |
| 設定不備 | 設定の見直し | 誤った設定を攻撃に利用されないようにする |
| 誘導（罠にはめる） | 脅威・手口を知る | 手口から重要視するべき対策を理解する |

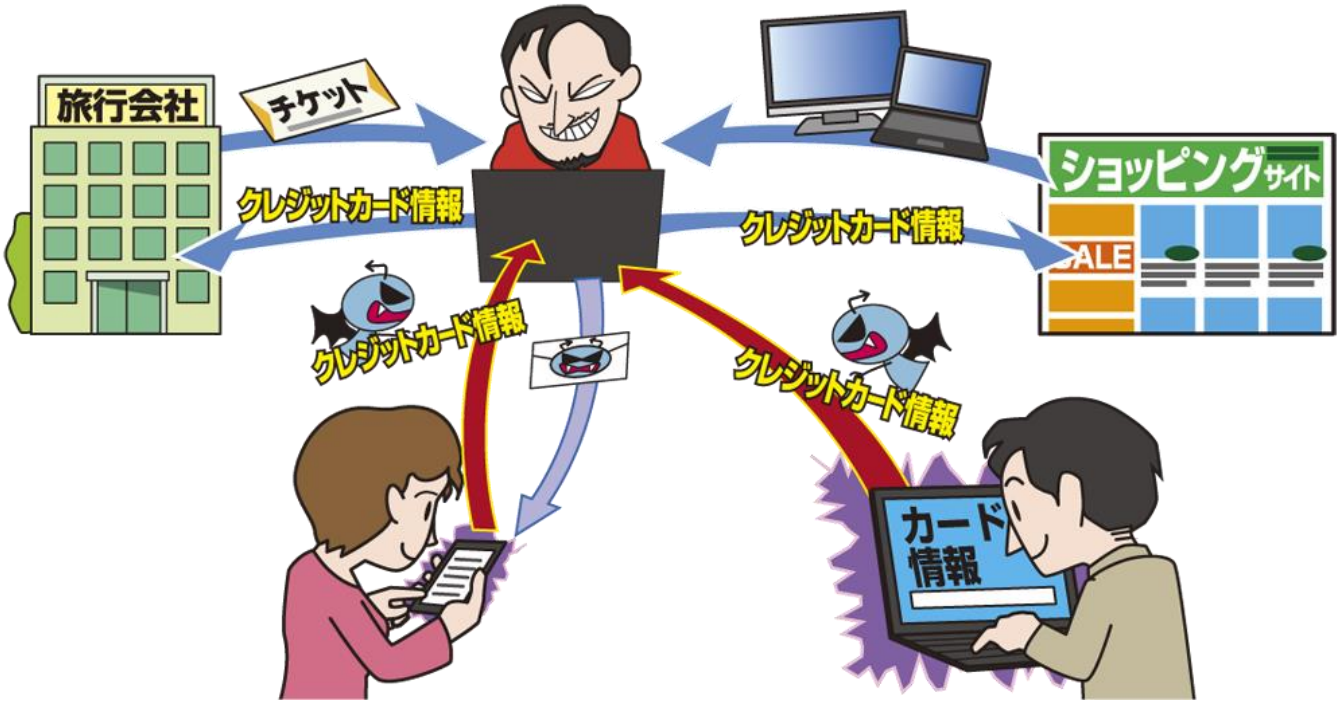
- 多数の脅威があるが「攻撃の糸口」は似通っている
- 基本的な対策の重要性は長年変わらない
- 後述する各脅威における対策のほか、上記対策は常に意識

# 情報セキュリティ10大脅威 2019
# 個人編　各脅威の解説

※以降の各脅威の対策では、前項の「情報セキュリティ対策の基本」は実施されている前提とし、記載には含めていません。

# 【1位】クレジットカード情報の不正利用

## ～継続する悪用の被害、被害が拡大するおそれ～




- 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を窃取される
- クレジットカード情報をショッピングサイト等で不正利用される

# 【1位】クレジットカード情報の不正利用

～継続する悪用の被害、被害が拡大するおそれ～

IPA

## ● 攻撃手口

### ・ウイルスに感染させて情報を窃取

#### ■ メールを利用したウイルス感染の手口

・悪意のある不正なファイルを添付したメールを送信し、添付ファイルを開かせるなどしてウイルスに感染させる

・ウイルスがダウンロードされるように細工した不正なウェブサイトへのリンク記載したメールを送信し、不正なウェブサイトへ誘導してウイルスに感染させる

# 【1位】クレジットカード情報の不正利用

～継続する悪用の被害、被害が拡大するおそれ～

## ● 攻撃手口

**・攻撃者が用意した偽のサイトに情報を入力させて窃取**

### ■ フィッシング詐欺による情報窃取

・実在する企業を模した偽のウェブサイト（フィッシングサイト）を攻撃者が用意する

・メールやSMSでフィッシングサイトへ誘導し、クレジットカード情報を入力させる
（入力してしまった情報は攻撃者に送信される）

# 【1位】クレジットカード情報の不正利用

## ～継続する悪用の被害、被害が拡大するおそれ～

- 2018年の事例/傾向
  - クレジットカード不正利用の被害額は増加 (※1)
    - ・2018年1月～9月の被害額は131.8億円
    - ・クレジットカードの被害の8割が番号盗用による被害
  - モバイル決済におけるクレジットカードの不正利用 (※2)
    - ・モバイル決済サービスの本人認証に不備があり、それを悪用してクレジットカードを不正利用
    - ・クレジットカード情報の流出元は不明

【出典】
※1 クレジットカード不正使用被害の集計結果
https://www.j-credit.or.jp/information/statistics/download/toukei_03_g_181228.pdf
※2 3Dセキュア(本人認証サービス)の対応と、クレジットカード不正利用への補償について
https://paypay.ne.jp/notice-static/20181227/01/

# 【1位】クレジットカード情報の不正利用

## ～継続する悪用の被害、被害が拡大するおそれ～

- 2018年の事例/傾向
  - 不正トラベルの手口が多発 (※3)
    - ・旅行代理店になりすまして旅行者からの旅行申し込みを受け付ける
    - ・別件で窃取しておいた第三者のクレジットカードを不正利用し、正規の旅行事業者が提供する旅行サービスを手配して旅行者へと中継
      （不正利用されるクレジットカードは旅行者のものではない）
    - ・被害者は旅行者ではなく使用されたクレジットカードの所有者
      （旅行者は通常通り旅行可能）

【出典】
※3 不正トラベル対策の実施
https://www.jc3.or.jp/topics/travel_fraud.html

# 【1位】クレジットカード情報の不正利用

## ～継続する悪用の被害、被害が拡大するおそれ～

- **対策**
  - **利用者**
    - ・被害の予防
      - –クレジットカード会社が提供している本人認証サービス（3Dセキュア）の利用
      - –受信メール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開かない
      - –信頼できるインターネットサービスの利用
      - –怪しい（普段は表示されない）ポップアップ等に安易に個人情報等は入力しない

# 【1位】クレジットカード情報の不正利用

## ～継続する悪用の被害、被害が拡大するおそれ～

- 対策
  - 利用者
    - ・被害の早期検知
      - –クレジットカードの利用履歴の確認
      - –利用時のメール通知機能等の利用
    - ・被害を受けた後の対応
      - –該当サービスのコールセンターへの連絡
      - –クレジットカードの再発行
      - –端末の初期化
      - –パスワードの再設定

# 【2位】フィッシングによる個人情報等の詐取

## ～有名企業を装い偽サイトへ誘導、横行するフィッシングメールに注意！～


- 金融機関や有名企業を装った偽のウェブサイト（フィッシングサイト）へ利用者を誘導
- フィッシングサイト上でIDやパスワード等の個人情報を入力させて窃取する

# 【2位】フィッシングによる個人情報等の詐取

～有名企業を装い偽サイトへ誘導、横行するフィッシングメールに注意！～

## ● 攻撃手口

**・攻撃者が用意した偽のサイトに情報を入力させて窃取**

### ■ 有名企業を装ったメールをばらまく

・実在する企業を装いフィッシングサイトへのリンクが記載されたメール（フィッシングメール）やSMS等を送信し、フィッシングサイトへアクセスさせる

・フィッシングサイトで利用者が入力した情報を窃取

### ■ システム管理者等を装ったメールを組織内に

・組織で利用するクラウドサービス等のログイン画面を模したフィッシングサイトへのリンクが記載されたメールを標的組織内にばらまく

# 【2位】フィッシングによる個人情報等の詐取

～有名企業を装い偽サイトへ誘導、横行するフィッシングメールに注意！～

- 2018年の事例/傾向
  - 有名ショッピングサイトをかたったフィッシング（※1）
    - 有名ショッピングサイトをかたり、「アカウントの有効期限が切れました」等と記載されたフィッシングメールをばらまく
    - 本物のサイトに酷似したフィッシングサイトに誘導
  - 大学を標的としたフィッシングが多発（※2）
    - 学内のメール管理者を装いフィッシングメールを学内にばらまく
    - 大学で利用しているクラウドメールサービスを模した偽の認証情報の入力画面へ誘導

【出典】
※1 Amazon をかたるフィッシング（2018/12/18）
https://www.antiphishing.jp/news/alert/_amazon_20181218.html
※2 横浜市立大学がフィッシングメール被害！個人情報5,794件が流出の可能性
https://cybersecurity-jp.com/news/25048

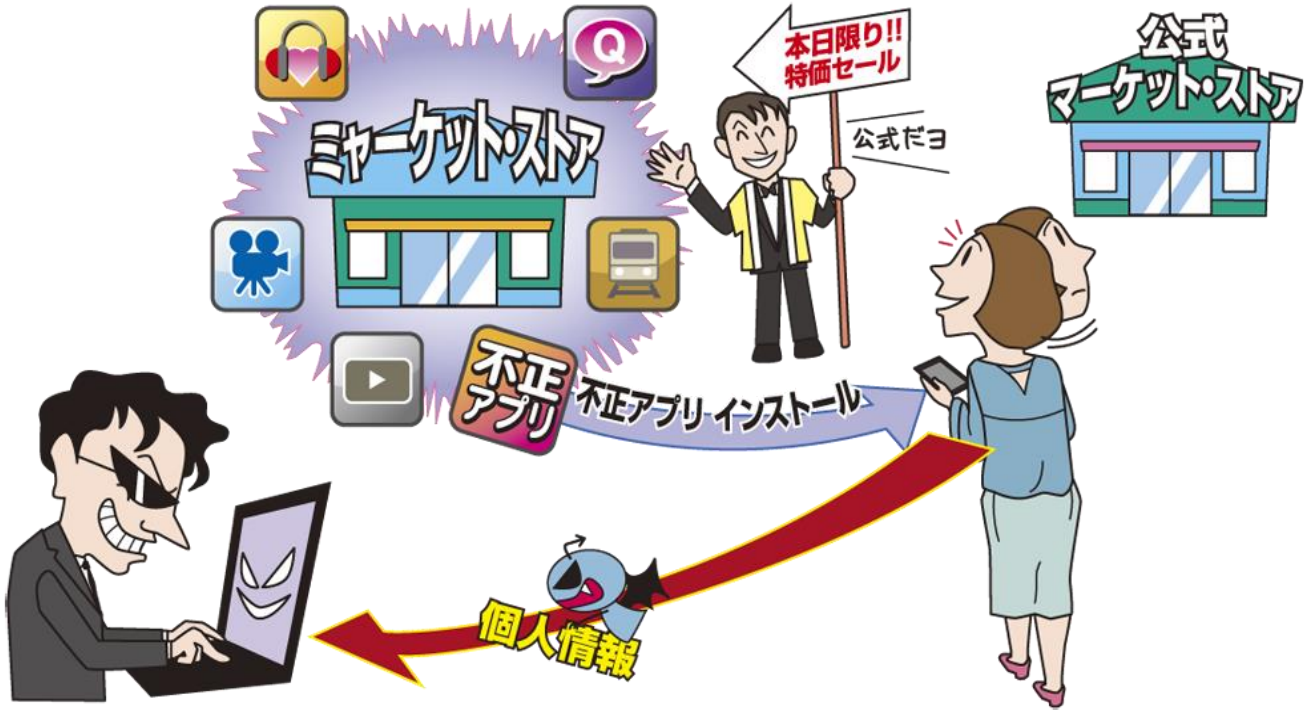
# 【2位】フィッシングによる個人情報等の詐取

## ～有名企業を装い偽サイトへ誘導、横行するフィッシングメールに注意！～

- 対策
  - インターネット利用者
    - ・被害の予防
      - －受信メールやウェブサイトの十分な確認
      - －メール内のリンクを安易にクリックしない
    - ・被害の早期検知
      - －利用するサービスのログイン履歴の確認
      - －口座、クレジットカード、キャリア決済の利用履歴の確認
    - ・被害を受けた後の対応
      - －パスワードの再設定
      - －クレジットカードの停止
      - －信頼できる機関に相談する

# 【3位】不正アプリによるスマートフォン利用者への被害

## ～実在の企業をかたり不正アプリのインストールへ誘導～




- 不正アプリをスマートフォンにインストールしてしまうことで、スマートフォン内の連絡先情報等が窃取される
- スマートフォンの一部機能を不正利用される
- 攻撃の踏み台にされることで意図せず加害者になるおそれも

# 【3位】不正アプリによるスマートフォン利用者への被害

～実在の企業をかたり不正アプリのインストールへ誘導～

## ● 攻撃手口

**・不正アプリをスマホ利用者にインストールさせる**

### ■ 不正アプリのダウンロードサイトへ誘導

- ・実在の企業をかたってメールやSMS等で偽サイト（不正アプリのダウンロードサイト）へ誘導
- ・正規のアプリであると誤認させて不正アプリをインストールさせる

### ■ 公式マーケットに不正アプリを紛れ込ませる

- ・不正アプリを正規のアプリと見せかけて公式マーケットに公開
- ・公式マーケットは安全だと考える利用者を狙う

# 【3位】不正アプリによるスマートフォン利用者への被害

～実在の企業をかたり不正アプリのインストールへ誘導～

## ● 攻撃手口

**・不正アプリをスマホ利用者にインストールさせる**

■ 不正アプリをインストールしてしまうと様々な被害が

- ・連絡先等の端末内の重要な情報を窃取される
- ・端末の一部機能（カメラ、通話機能など）を不正に利用される
- ・仮想通貨のマイニングに不正に利用される
- ・DDoS攻撃や悪意あるSMSの拡散等の踏み台に利用される

# 【3位】不正アプリによるスマートフォン利用者への被害

## ～実在の企業をかたり不正アプリのインストールへ誘導～

- 2018年の事例/傾向
  - 宅配便業者をかたったSMSによる誘導 (※1)
    - 偽の不在通知をスマートフォン利用者に対してSMSで送信
    - 「荷物状況の確認のため」と偽って不正アプリのダウンロードサイトへ誘導
  - ルーターの設定を改ざんして誘導 (※2)
    - ルーターの脆弱性を突いてルーターの設定を改ざん
    - そのルーター経由でインターネットへアクセスすると不正アプリのダウンロードサイトに接続される

【出典】
※1 佐川急便をかたるフィッシング (2018/08/10)
https://www.spread.or.jp/phishing/2018/08/13/5655/
※2 ルーターのDNS改竄によりダウンロードされる「facebook.apk」の内部構造を読み解く
https://blog.kaspersky.co.jp/malicious-facebook-apk/19968/

# 【3位】不正アプリによるスマートフォン利用者への被害

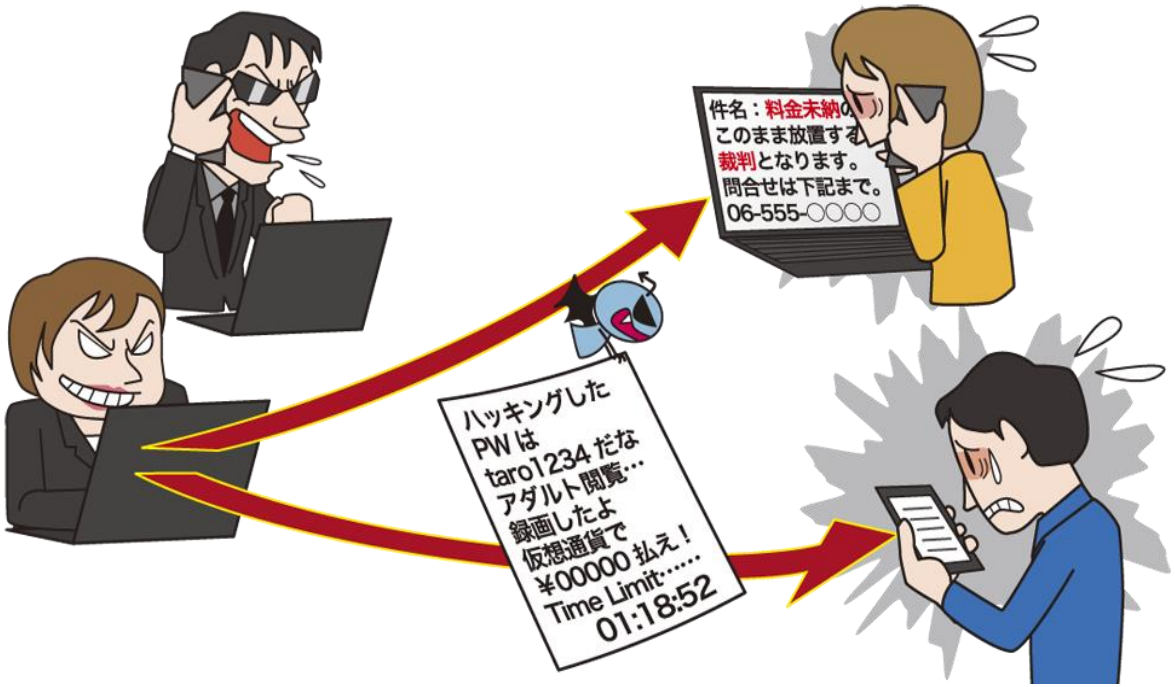
## ～実在の企業をかたり不正アプリのインストールへ誘導～

- 対策
  - スマートフォン利用者

・被害の予防
  - –アプリのインストールは公式マーケットから
    ※公式マーケットのアプリでも油断は禁物
  - –様々な情報（レビュー評価等）を確認して信頼できるアプリのみ利用
  - –アプリインストール時のアクセス権限の確認
  - –アプリインストールに関する設定に注意
    ※Androidのスマートフォンには公式マーケット以外からアプリを
    インストールできるようにする設定があり、その設定を有効にしない

・被害を受けた後の対応
  - –不正アプリのアンインストール
  - –アンインストールできない場合は端末初期化

# 【4位】メール等を使った脅迫・詐欺の手口による金銭要求
## ～仮想通貨などを要求する詐欺メールには冷静な対処を～




- 周囲に相談しにくいセクストーション（性的脅迫）のメールを送り付ける
- メール受信者は脅迫を受けて不安になり金銭を支払ってしまう
- 脅迫内容は事実に基づいていないケースが多い

# 【4位】メール等を使った脅迫・詐欺の手口による金銭要求
～仮想通貨などを要求する詐欺メールには冷静な対処を～

## ● 攻撃手口

**・脅し、騙しのメールを送り付け金銭を要求**

### ■ メール等で金銭を要求する脅迫メールを送信

- 脅しや騙しの内容を記載したメールを不特定多数にばらまく
- 金銭を要求する（仮想通貨での支払いを要求する場合も）

### ■ 周囲に相談しにくいセクストーション（性的脅迫）

- 「アダルトサイトを閲覧している姿を撮影した」、「アダルト動画を見られる有料サイトを使用した料金が未納である」等、被害者が周囲に相談しにくい内容で脅迫する

# 【4位】メール等を使った脅迫・詐欺の手口による金銭要求
## ～仮想通貨などを要求する詐欺メールには冷静な対処を～

- **攻撃手口**

**・脅し、騙しのメールを送り付け金銭を要求**

- **脅し文句の中に受信者の情報を記載する**
  - ・メール受信者のパスワード（過去に漏えいしてダークウェブ等で出回ったもの等）を記載し、本当にメール受信者のPCをハッキングしているかのように装い、脅しの内容を信じさせようとする

# 【4位】メール等を使った脅迫・詐欺の手口による金銭要求
## ～仮想通貨などを要求する詐欺メールには冷静な対処を～

- 2018年の事例/傾向
  - 性的な映像をばらまくと脅迫するメール（※1）
    - ・メール本文の日本語は不自然な文章
    - ・メール受信者のパスワードが記載されているケースがある
    - ・支払い方法として仮想通貨を要求
      （2018年10月末までに1,240万円相当の被害）
  - 有料サイトの料金未納と騙して電子マネー詐取（※2）
    - ・攻撃者が脅迫メールを送信し被害者から電話をかけさせる
    - ・電話で「裁判沙汰になる」等さらに追い込む
    - ・犯人グループによる被害総額は全国で約1億4,000万円

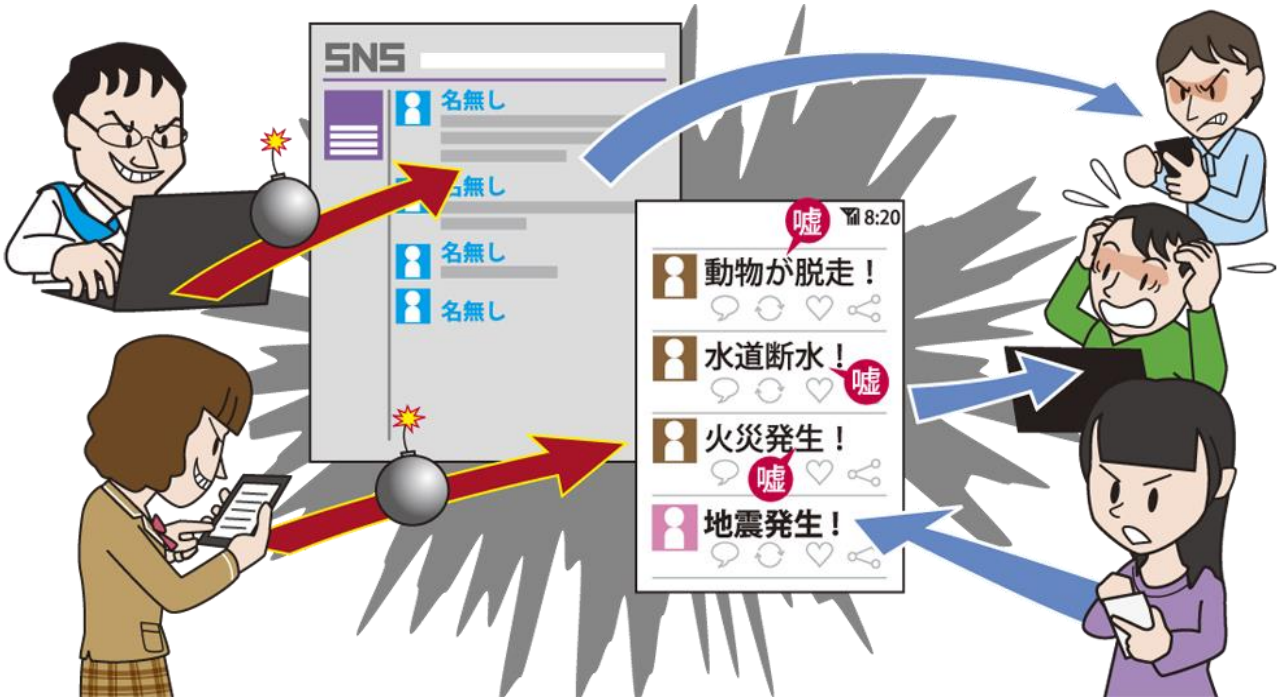
【出典】
※1 仮想通貨を要求する日本語の脅迫メールについて
https://www.jpcert.or.jp/newsflash/2018091901.html
※2 全国35都道府県で被害 1億4000万円詐取容疑で男5人を再逮捕
https://headlines.yahoo.co.jp/hl?a=20181204-03310151-saga-l41

# 【4位】メール等を使った脅迫・詐欺の手口による金銭要求
## ～仮想通貨などを要求する詐欺メールには冷静な対処を～

- 対策
  - インターネット利用者
    - ・被害の予防
      - –受信した脅迫・詐欺メールは無視する
        - ※詐欺メールに自分のパスワード等が記載されていても実際にハッキングされていることを示すものではない
    - ・被害を受けた後の対応
      - –パスワードを変更する
        - ※脅迫・詐欺メールに記載されたパスワードが自分のものと一致しているのであれば、どこかからパスワードが漏えいしたおそれがある
      - –警察に相談する

# 【5位】ネット上の誹謗・中傷・デマ

## ～投稿前に内容を再確認、軽い冗談のつもりが社会問題になることも～




- SNS等で他人を誹謗・中傷したり、脅迫・犯罪予告を書き込み、事件になる
- 嘘情報（フェイクニュース等）をいたずらに発信し、拡散されることで大きな問題になる

# 【5位】ネット上の誹謗・中傷・デマ

～投稿前に内容を再確認、軽い冗談のつもりが社会問題になることも～

## ● 要因

### ・情報モラルの欠如、匿名性の悪用

#### ■ 情報モラルや自己抑制力の欠如

・自分の発言が他人に及ぼす影響を気にすることなく、安易にネットに投稿してしまう

・不満やストレスの捌け口として、特定の個人や組織等の評判を落とすような発言等をしてしまう

#### ■ 個人が匿名で発信できる場の普及

・「匿名だから」と軽い気持ちで他人に悪影響を及ぼす情報を発信してしまう（実際には警察等の正式な調査で身元は特定できる場合が多い）

# 【5位】ネット上の誹謗・中傷・デマ

～投稿前に内容を再確認、軽い冗談のつもりが社会問題になることも～

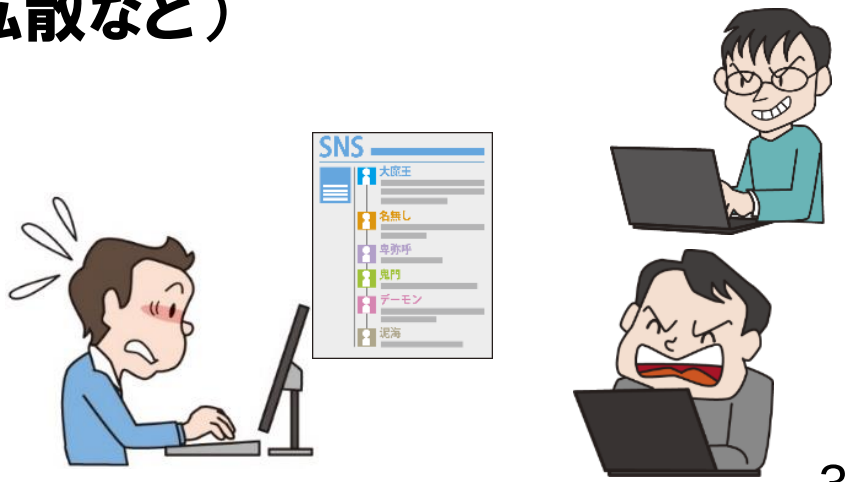
## ● 要因

**・インターネット上の情報を安易に信じてしまう**

### ■ 情報の真偽を確認せずに拡散

・インターネット上にある多くの嘘情報や真偽不明な情報を真偽を確かめることなく拡散してしまう

・有用な情報を周知してあげたいという親切心や正義感による場合も多い（災害情報の拡散など）



# 【5位】ネット上の誹謗・中傷・デマ

～投稿前に内容を再確認、軽い冗談のつもりが社会問題になることも～

- 2018年の事例/傾向
  - 学術機関に対する爆破予告の書き込み（※1）
    - ・インターネット上の掲示板に爆破予告が書き込まれ構内立ち入り禁止
  - 震災発生時における嘘情報の拡散（※2）
    - ・震災が発生した際に「大地震が数時間後に発生する」等の嘘情報が出回り、被災者が不安を募らせる事例が発生
    - ・嘘情報の発信源として自衛隊の名称が使われており、市の危機管理室に市民からの事実確認の問い合わせ多数

【出典】
※1 青学大に爆破予告 7日休校、キャンパス立ち入り禁止
https://www.asahi.com/articles/ASLB35W79LB3TIPE024.html
※2 北海道地震、SNSでデマ拡散 専門家「発信元確認を」
https://www.nikkei.com/article/DGXMZO35227790R10C18A9CC1000/

# 【5位】ネット上の誹謗・中傷・デマ

～投稿前に内容を再確認、軽い冗談のつもりが社会問題になることも～

## 対策

### 投稿者

・情報モラルや情報リテラシーの向上、
法令遵守の意識の向上

－誹謗・中傷や公序良俗に反する投稿をしない

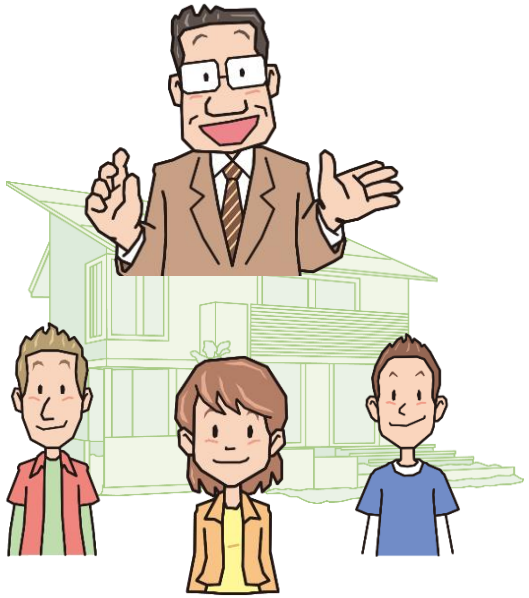
－投稿前に内容を再確認

### 家庭、教育機関

・情報モラル、情報リテラシーの教育

－自宅や学校で子供たちに情報モラルや
情報リテラシーの教育を行う

－トラブルの事例を伝え、悪質な行為は
犯罪になりうることを理解させる



# 【5位】ネット上の誹謗・中傷・デマ

～投稿前に内容を再確認、軽い冗談のつもりが社会問題になることも～

## 対策

### 閲覧者

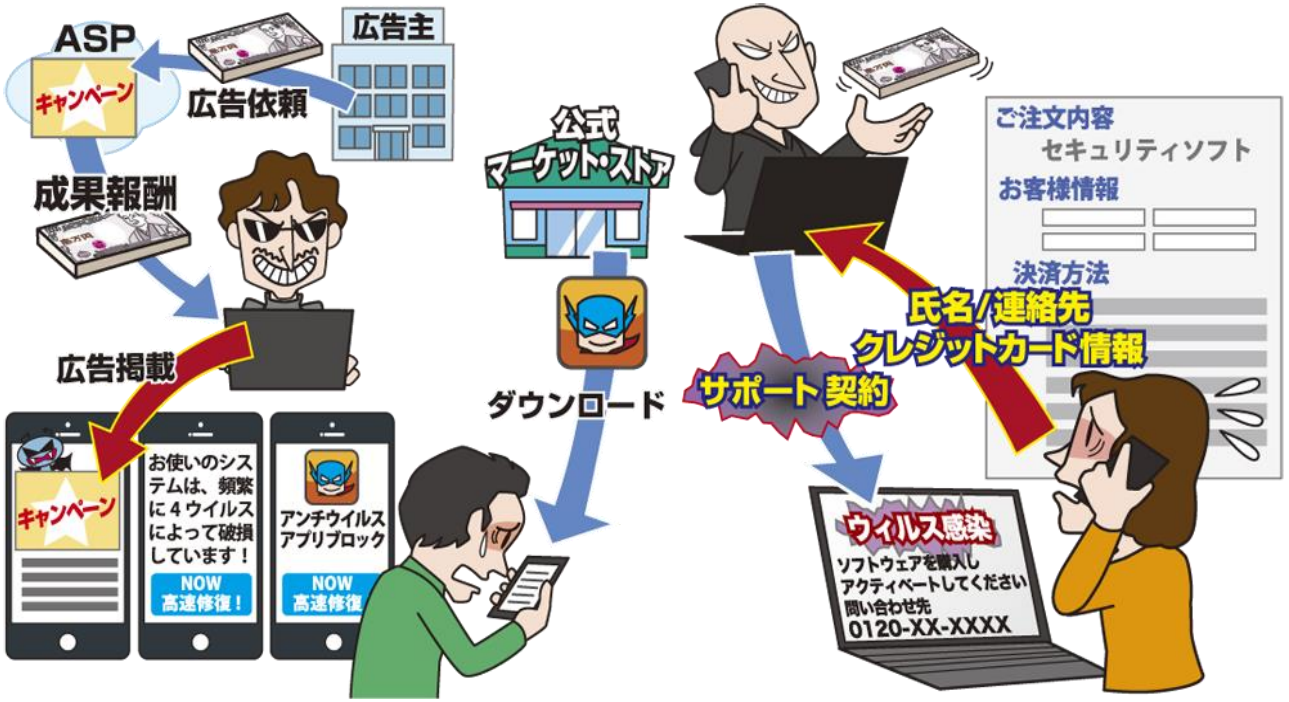
・情報モラルや情報リテラシーおよび
法令遵守の意識の向上
－情報の信頼性の確認

### 被害者

・被害を受けた後の適切な対応
－一人で抱え込まず、信頼できる周囲の
人や公的相談機関へ相談する。
・犯罪と思われる誹謗・中傷の投稿は、
警察へ被害届を提出
・管理者やプロバイダーへ情報削除依頼
※削除により炎上の火種になるおそれもあるため、
関係者等に相談して慎重に行う

# 【6位】偽警告によるインターネット詐欺

## ～落ち着いて！あの手この手の騙しの警告画面～




- インターネット閲覧中にウイルス感染やシステム破損に関する偽の警告画面（偽警告）を表示させる
- 被害者は偽警告の内容を信じてしまい、警告の内容に従って不要なソフトウェアのインストールやサポート契約を結ばされる

# 【6位】偽警告によるインターネット詐欺

～落ち着いて！あの手この手の騙しの警告画面～

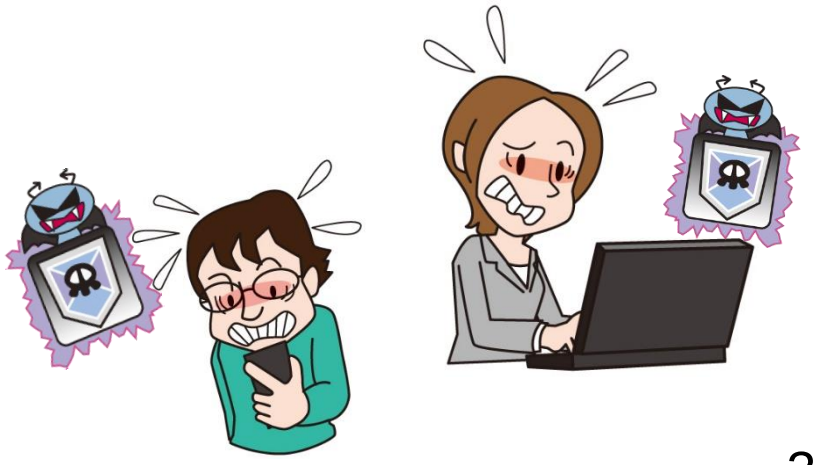
## ● 攻撃手口

**・巧妙に作成した偽警告を表示して不安を煽る**

### ■ 巧妙に細工が施された偽警告

・実在の企業ロゴを使用したり、警告音や警告メッセージを音声で流す

・警告画面を繰り返しポップアップで表示させ偽警告を閉じさせない



# 【6位】偽警告によるインターネット詐欺

～落ち着いて！あの手この手の騙しの警告画面～

## ● 攻撃手口

**・偽警告に記載した誘導に従わせる**

### ■ 偽対策ソフト（偽セキュリティソフト）

・偽のセキュリティソフトをインストールさせ、有償ソフトウェアの購入へ誘導

### ■ サポート契約詐欺

・電話窓口のオペレーターによる遠隔操作で対策したように見せかけ、有償のサポート契約へ誘導

### ■ 偽警告スマホ版

・スマホアプリのインストールへ誘導（誘導先は公式マーケット）
※アフィリエイト収益が目的か

# 【6位】偽警告によるインターネット詐欺

## ～落ち着いて！あの手この手の騙しの警告画面～

- 2018年の事例/傾向
  - 偽警告の相談件数が急増 (※1)
    - ・2018年5月、IPAの相談窓口への「偽セキュリティソフト」「サポート契約詐欺」の手口に関する相談が急増
    - ・2つを合わせた手口も(「偽セキュリティソフトをインストールさせ、機能を有効化するために電話させてサポート契約へ」)
  - 偽警告に関する注意喚起(国民生活センター) (※2)
    - ・国民生活センターへも多く相談が寄せられている
    - ・2018年9月30日までに前年度同時期の相談件数を大きく上回る

【出典】

※1 IPA 安心相談窓口だより「偽のセキュリティ警告によって有償の「ソフトウエア購入」や「サポート契約」をしてしまう相談が増加中」
https://www.ipa.go.jp/security/anshin/mgdayori20180718.html

※2 独立行政法人国民生活センター「インターネット使用中に突然表示される偽セキュリティ警告画面にご注意！」
https://www.kokusen.go.jp/news/data/n-20181107_1.html

# 【6位】偽警告によるインターネット詐欺

## ～落ち着いて！あの手この手の騙しの警告画面～


- 対策
  - インターネット利用者
    - ・被害の予防
      - －正規の警告を知る
        ※警告が本物か偽物かを判断するためOSやセキュリティソフトの仕様を把握（正規の警告に模しているケースもあるので注意）
      - －偽警告が表示されても従わない
      - －偽警告が表示されたらブラウザを終了
        ※ブラウザにより適切な対応は異なる（※1）
    - ・被害を受けた後の対応
      - －端末を初期化
      - －サポート契約の解消（近くの消費生活センターへ相談）
      - －クレジットカード会社へ連絡

【参考】
※1　被害低減のための偽警告の手口と対策を紹介する映像コンテンツを公開　※「警告画面の表示に関するよくある質問」Q2参照
https://www.ipa.go.jp/security/anshin/mgdayori20170411.html

# 【7位】インターネットバンキングの不正利用

## ～被害は継続して発生、しかし減少傾向に～


- インターネットバンキングの認証情報を悪用され不正送金される
- 認証情報はウイルス感染やフィッシング詐欺によって漏えいする

# 【7位】インターネットバンキングの不正利用

～被害は継続して発生、しかし減少傾向に～

## ● 攻撃手口

**・インターネットバンキングに関する認証情報を窃取する**

### ■ ウイルス感染による情報窃取

・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情報窃取

・実在する銀行等のウェブサイトを模した偽のウェブサイト（フィッシングサイト）を用意する

・フィッシングサイトのリンクが記載されたメールを不特定多数に送信し、フィッシングサイトへ誘導する

# 【7位】インターネットバンキングの不正利用

## ～被害は継続して発生、しかし減少傾向に～

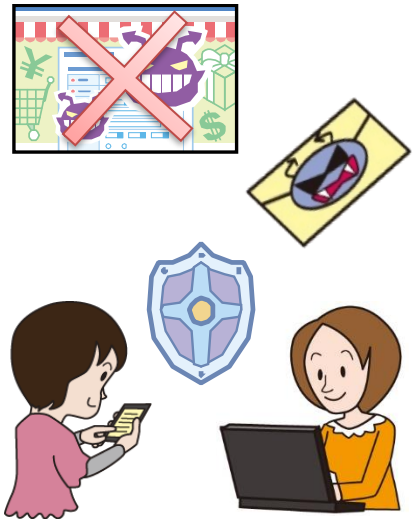
- 2018年の事例/傾向
  - インターネットバンキングの不正送金は減少傾向（※1）
    - 前年度と比較して発生件数はほぼ横ばい、被害額は減少
  - ウイルス感染を狙う新たなばらまき型メール（※2）
    - インターネットバンキング等の認証情報の窃取を目的としたウイルス「URSNIF」を感染させるばらまき型メールが多数
    - WordやExcelのマクロ機能を悪用するもののほか、VBScriptやPDFが添付された新しいばらまき型メールも

【出典】
※1 平成30年上半期におけるサイバー空間の脅威の情勢等について
https://www.npa.go.jp/publications/statistics/cybersecurity/data/H30_kami_cyber_jousei.pdf
※2 2018年7月 マルウェアレポート
https://eset-info.canon-its.jp/malware_info/malware_topics/detail/malware1807.html

# 【7位】インターネットバンキングの不正利用

## ～被害は継続して発生、しかし減少傾向に～

- **対策**
  - **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
      - –ファイルの拡張子を表示させる設定
      - –怪しい（普段は表示されない）ポップアップに個人情報等は入力しない
    - ・被害の早期検知
      - –不審なログイン履歴の確認
      - –口座の利用履歴の確認
      - –利用時のメール連絡機能等の利用



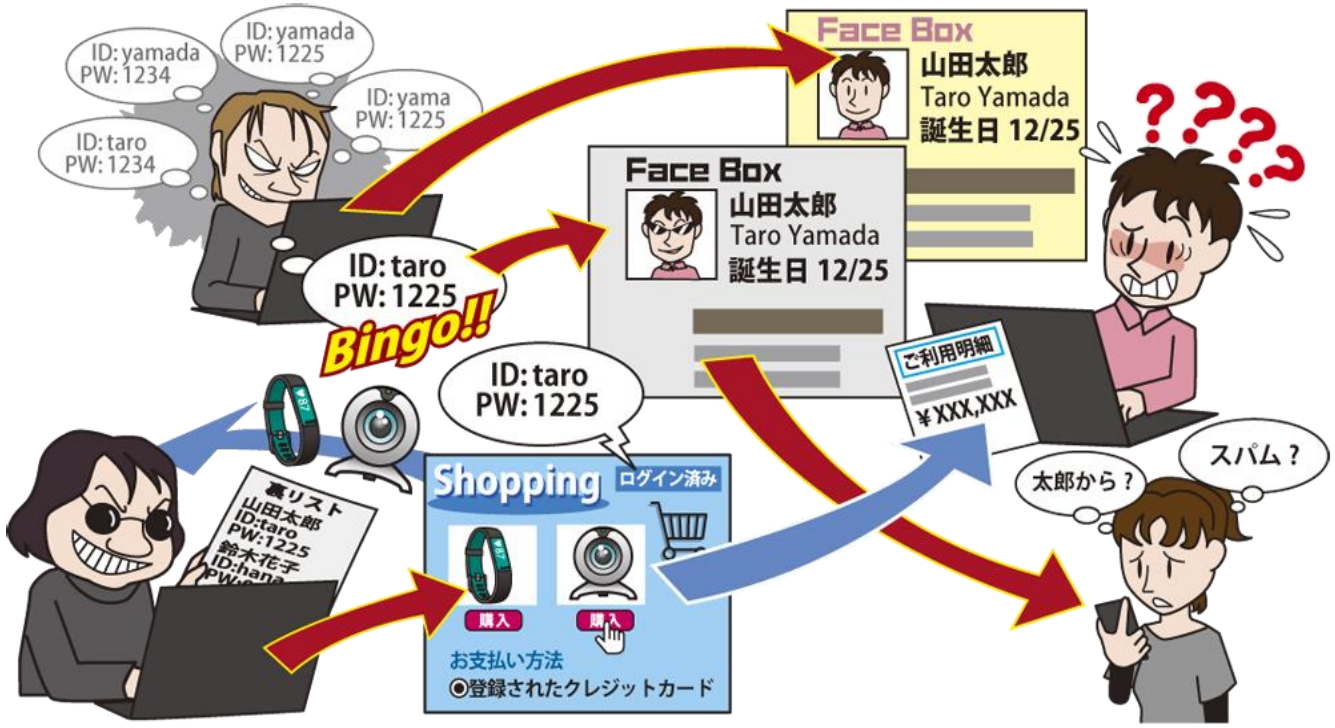
# 【7位】インターネットバンキングの不正利用

## ～被害は継続して発生、しかし減少傾向に～

- 対策
  - 利用者
    - ・被害を受けた後の対応
      - –該当サービスのコールセンターへの連絡
      - –警察への被害届の提出
      - –端末の初期化
      - –パスワードの再設定

# 【8位】インターネットサービスへの不正ログイン

## ～多要素認証や多段階認証等を利用して攻撃に備えを～




- 利用しているインターネットサービスの認証情報（ID、パスワード）が窃取または推測され、不正ログインされる
- インターネットサービスの機能に応じて、発生する被害は様々

# 【8位】インターネットサービスへの不正ログイン

～多要素認証や多段階認証等を利用して攻撃に備えを～

## ● 攻撃手口

**・不正に入手した認証情報で不正ログインする**

### ■ パスワードリスト攻撃

・何らかの方法で入手した認証情報を利用して複数のサービスにログインを試みる攻撃

・複数のサービスでパスワードを使いまわしていると1つのパスワードが漏えいすると他のサービスにも不正ログインされるおそれがある

・漏えいした認証情報はインターネット上で売買されており複数の犯罪者に取得されるおそれがある

# 【8位】インターネットサービスへの不正ログイン

～多要素認証や多段階認証等を利用して攻撃に備えを～

## ● 攻撃手口

**・不正に入手した認証情報で不正ログインする**

### ■ 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

・名前や誕生日などをパスワードに使用していると推測されやすくなる

・SNSで公開している情報などから推測される場合も

### ■ ウイルス感染による窃取

・利用者が悪意あるウェブサイトやメール等からウイルス感染することでその端末で入力したパスワード等が漏えいする

# 【8位】インターネットサービスへの不正ログイン

## ～多要素認証や多段階認証等を利用して攻撃に備えを～

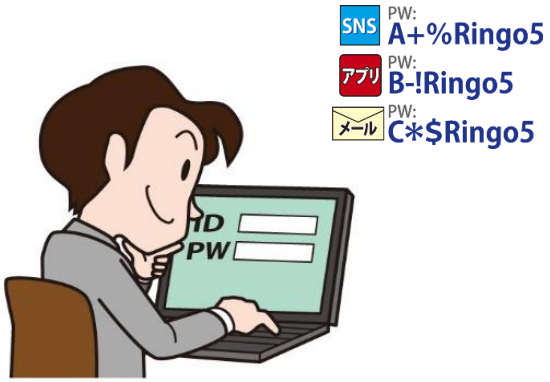
- 2018年の事例/傾向
  - オンラインストアにおけるなりすまし購入（※1）
    - パスワードリスト攻撃によって約1,800件の不正ログイン
    - そのうち約1,000件でiPhoneXを不正に購入された
    - ログインさえできれば商品を不正に購入できる仕組みを悪用された
  - 不正ログインによるポイントの窃取（※2）
    - パスワードリスト攻撃による不正ログイン
    - 52名のポイントが第三者のカードに不正に移行

【出典】
※1 「iPhone X」不正購入被害1000件 「ドコモオンラインショップ」に不正ログイン、リスト型攻撃で
https://www.itmedia.co.jp/news/articles/1808/13/news084.html
※2 WAONのポイント不正移行、被害者数を上方修正 - 個人情報流出の可能性も
https://www.security-next.com/098231

# 【8位】インターネットサービスへの不正ログイン

## ～多要素認証や多段階認証等を利用して攻撃に備えを～

- **対策**
  - **利用者**

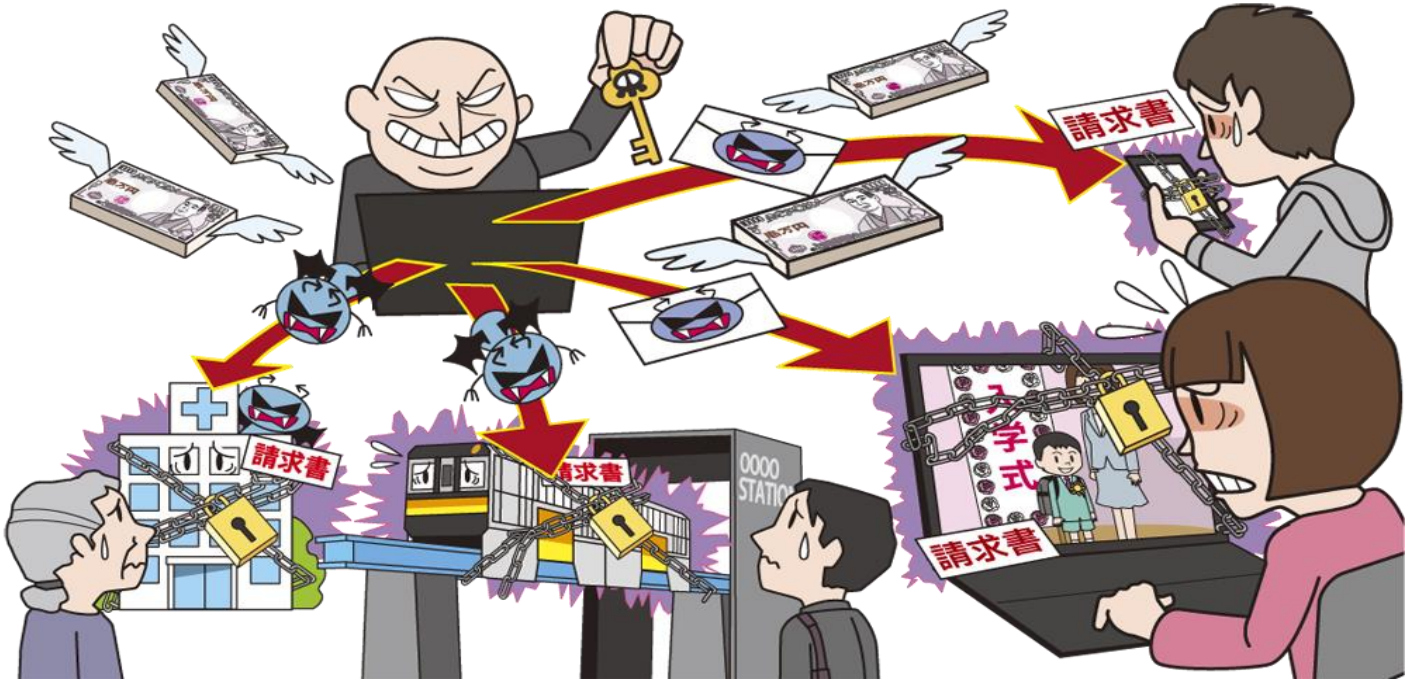



・被害の予防
  - –パスワードは長く、複雑にする
  - –パスワードの使いまわしをしない
  - –パスワード管理ソフトの利用
  - –サービスが推奨する認証方式の利用
  - –不審なウェブサイトで安易に認証情報を入力しない
  - –利用頻度が低いサービスや不要なサービスの
    アカウント削除

・被害を受けた後の対応
  - –パスワードを変更する
  - –クレジットカードの停止
  - –インターネットサービス運営者への連絡

# 【9位】ランサムウェアによる被害

## ～ランサムウェアに感染し、思い出の写真や知人の連絡先情報等が閲覧不可に～




- PCやスマートフォンのファイル暗号化や画面ロックを行い制限をかけ、解除と引き換えに金銭要求
- 家族や友人との思い出や知人の連絡先情報が閲覧できなくなるおそれ

# 【9位】ランサムウェアによる被害

～ランサムウェアに感染し、思い出の写真や知人の連絡先情報等が閲覧不可に～

## ● 攻撃手口

**・メールやウェブサイトからランサムウェアに感染させる**

### ■ メールからの感染

・メールの添付ファイルやメール本文中のリンクを開かせることでランサムウェアに感染させる

### ■ ウェブサイトからの感染

・攻撃者が用意したウェブサイトを閲覧させることでランサムウェアに感染させる

（被害者のPCで利用しているソフトウェアの脆弱性を悪用）

# 【9位】ランサムウェアによる被害

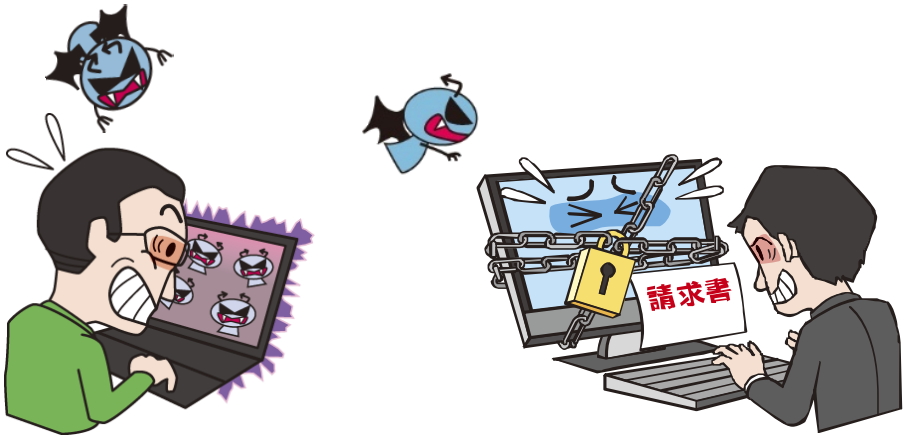
～ランサムウェアに感染し、思い出の写真や知人の連絡先情報等が閲覧不可に～

## ● 攻撃手口

**・OSの脆弱性を悪用してランサムウェアを感染させる**

### ■ 脆弱性を悪用したネットワーク越しの感染

・PCのOSの脆弱性を悪用し、脆弱性を解消せずにインターネットへ接続しているPCをランサムウェアに感染させる



# 【9位】ランサムウェアによる被害

～ランサムウェアに感染し、思い出の写真や知人の連絡先情報等が閲覧不可に～

- 2018年の事例/傾向
  - 病院の電子カルテシステムがランサムウェア感染 (※1)
    - ・電子カルテシステムがランサムウェアに感染し、約2日間使用不可
    - ・身代金支払い要求には応じず、システム復旧まで紙カルテおよび伝票運用による治療を行った
  - 脅迫してランサムウェアに感染させる攻撃も (※2)
    - ・盗撮した画像や動画を公開すると嘘による脅しを行い金銭を騙し取ったり、ランサムウェアに感染させたりする事例を確認

【出典】
※1 電子カルテシステムの障害発生について
https://www.city.uda.nara.jp/udacity-hp/oshirase/change-info/documents/press-release.pdf
※2 恥ずかし画像詐欺とランサム攻撃が融合 -「証拠動画」のリンクにワナ
https://http://www.security-next.com/100906

# 【9位】ランサムウェアによる被害

## ～ランサムウェアに感染し、思い出の写真や知人の連絡先情報等が閲覧不可に～

- 対策
  - 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
      - –スマホアプリはアクセス権限の確認
      - –バックアップの取得

      ※バックアップに使用する記録媒体は、ランサムウェアによって暗号化されないように、バックアップするときのみPCに接続する。

# 【9位】ランサムウェアによる被害

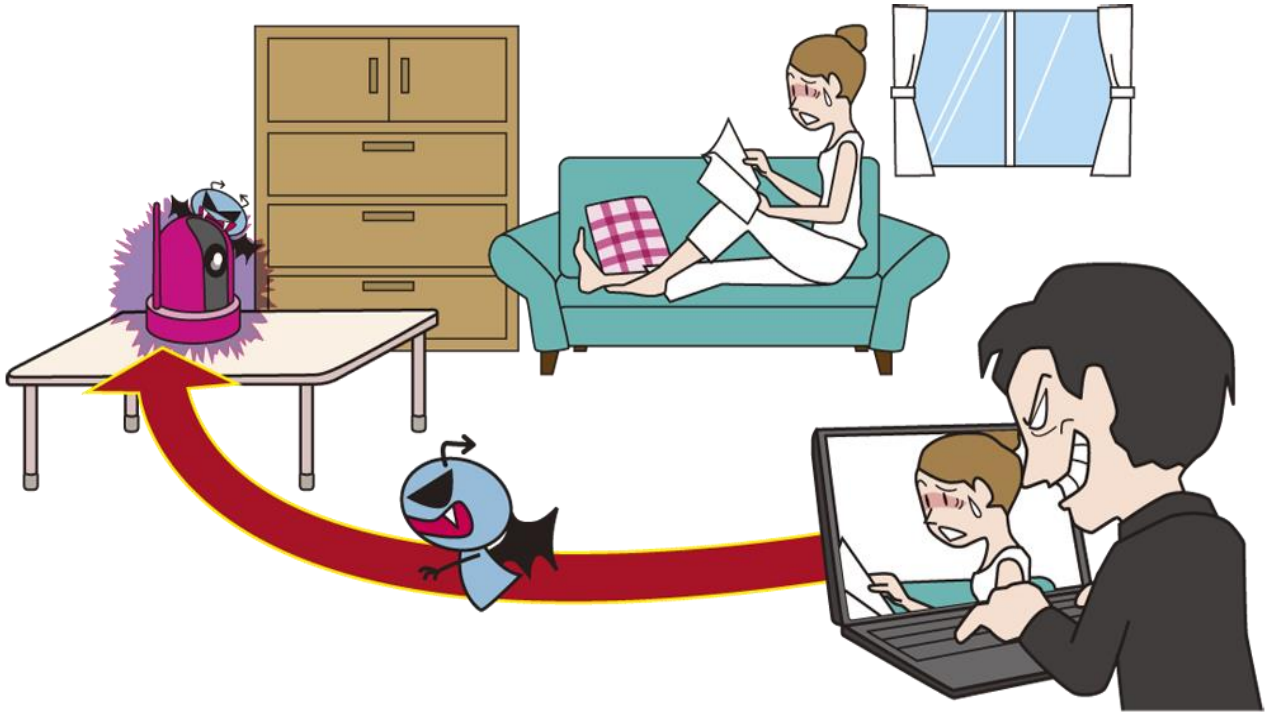
～ランサムウェアに感染し、思い出の写真や知人の連絡先情報等が閲覧不可に～

- 対策
  - 利用者
    - ・被害を受けた後の対応
      - –バックアップから復旧
      - –復号ツールの活用
      - –復元機能の活用

      ※DropBoxやGoogleドライブ、Microsoft OneDrive等のクラウドサービスの中には復元機能を持っているものもあるのでその機能を活用する。

# 【10位】IoT機器の不適切な管理

## ～増え続けるIoT機器を悪用する攻撃～



- 企業だけでなく一般家庭でもインターネット経由で操作できるIoT機器の利用が増えている
- パスワードの設定や管理が不十分なIoT機器に不正アクセスされ、情報の盗み見などの被害

# 【10位】IoT機器の不適切な管理

～増え続けるIoT機器を悪用する攻撃～

IPA

## ● 攻撃手口

**・IoT機器の設定不備や脆弱性を悪用**

### ■ 初期パスワードのままのIoT機器へログイン

・工場出荷時に製品共通の初期パスワードが設定されたIoT製品に対し、当該初期パスワードによるログインを試みる

### ■ 脆弱性を悪用

・IoT機器が持つすでに公開された脆弱性を悪用し、パッチ適用が行われていないIoT機器を乗っ取る

### ■ ウイルスを用いた攻撃

・ネットワーク上の脆弱性を持ったIoT機器がないかを探索し、次々とウイルス感染させる

# 【10位】IoT機器の不適切な管理

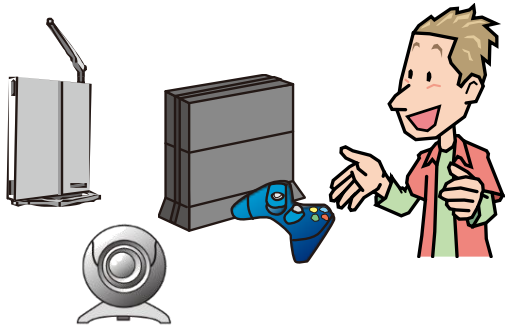
## ～増え続けるIoT機器を悪用する攻撃～

- 2018年の事例/傾向
  - 監視カメラ(ウェブカメラ)へ不正にログイン
    - 被害に遭ったウェブカメラはいずれも初期パスワードのまま
    - ウェブカメラの映像に攻撃者が設定したメッセージが表示されるように不正に操作された
  - IoTウイルス「サトリ」の攻撃が増加
    - このウイルスに感染したIoT機器からのDDoS攻撃が発生
    - 「サトリ」が形成するボットネットを通じて特定のルーターの脆弱性を悪用する新たなウイルスに感染させようとする攻撃が世界各地で確認された

# 【10位】IoT機器の不適切な管理

## ～増え続けるIoT機器を悪用する攻撃～

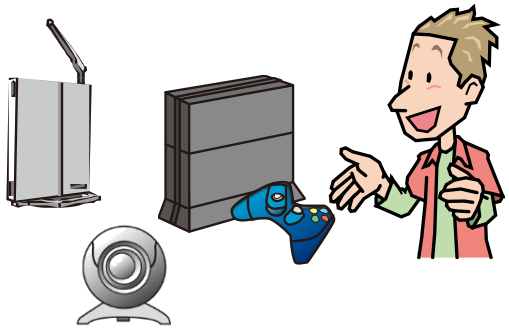
- 対策
  - 利用者
    - ・情報リテラシーの向上
      - –信頼できるメーカーの製品を使用
      - –使用前に取扱説明書で適切な使用方法を確認
    - ・被害の予防
      - –初期パスワードから長く複雑なパスワードへ変更
      - –外部からの不要なアクセス制限
      - –不要な機能やポートは無効化
      - –パッチが公開されたら迅速に更新
        （自動更新機能も活用する）
      - –廃棄前や下取りに出す前に初期化



# 【10位】IoT機器の不適切な管理

## ～増え続けるIoT機器を悪用する攻撃～

- 対策
  - 利用者
    - ・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、前項の「被害の予防」を実施
      - –パッチが公開されない場合は機器の使用中止を検討



# まとめ

## 情報セキュリティ対策の基本を実践

- 「10大脅威」の順位は毎回変動するが、基本的な対策の重要性は長年変わらない

## 各脅威の手口の把握および対策を実践

- 新たな機器やサービスの普及に伴いインターネット利用における脅威なども変化する
- 公的機関の注意喚起やニュースなどから脅威の手口に関する情報を収集し、変化する手口を理解して適切な対策を実践することが重要

# 詳細な資料のダウンロード

## ■情報セキュリティ10大脅威　2019

本資料に関する詳細な内容は以下のウェブサイトをご覧ください

※以下のURLへアクセス、またはQRコードをスマートフォンの
　QRコードリーダーアプリで読み込み、ウェブサイトをご覧ください


https://www.ipa.go.jp/security/vuln/10threats2019.html

## ■アンケートご協力のお願いについて

IPAが公開しているツールや資料の品質向上のため、アンケートへのご協力をお願い致します

https://touroku.ipa.go.jp/?url=http%3A%2F%2Fspd-evsan-ap01.ipa.go.jp%2Fentry%2FMemberLogin%3Fevent_id%3DEA0000000074