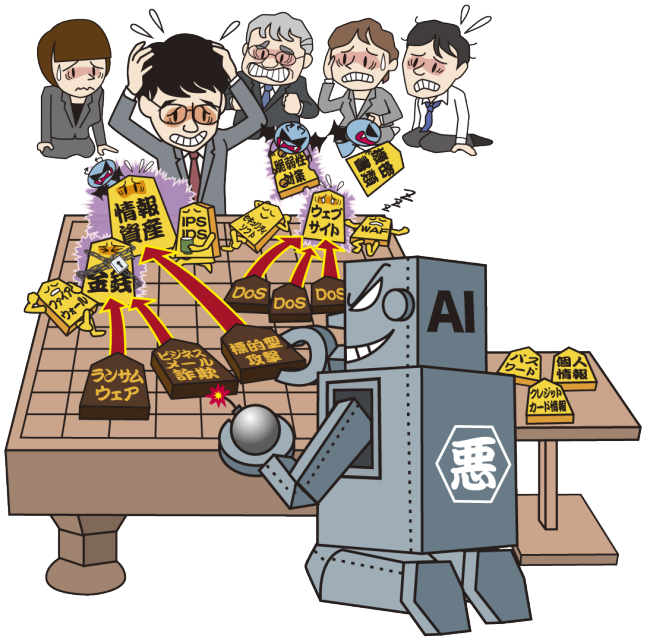
IPA Better Life with IT

# 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

# 情報セキュリティ10大脅威 2019 脅威ランキング

IPA

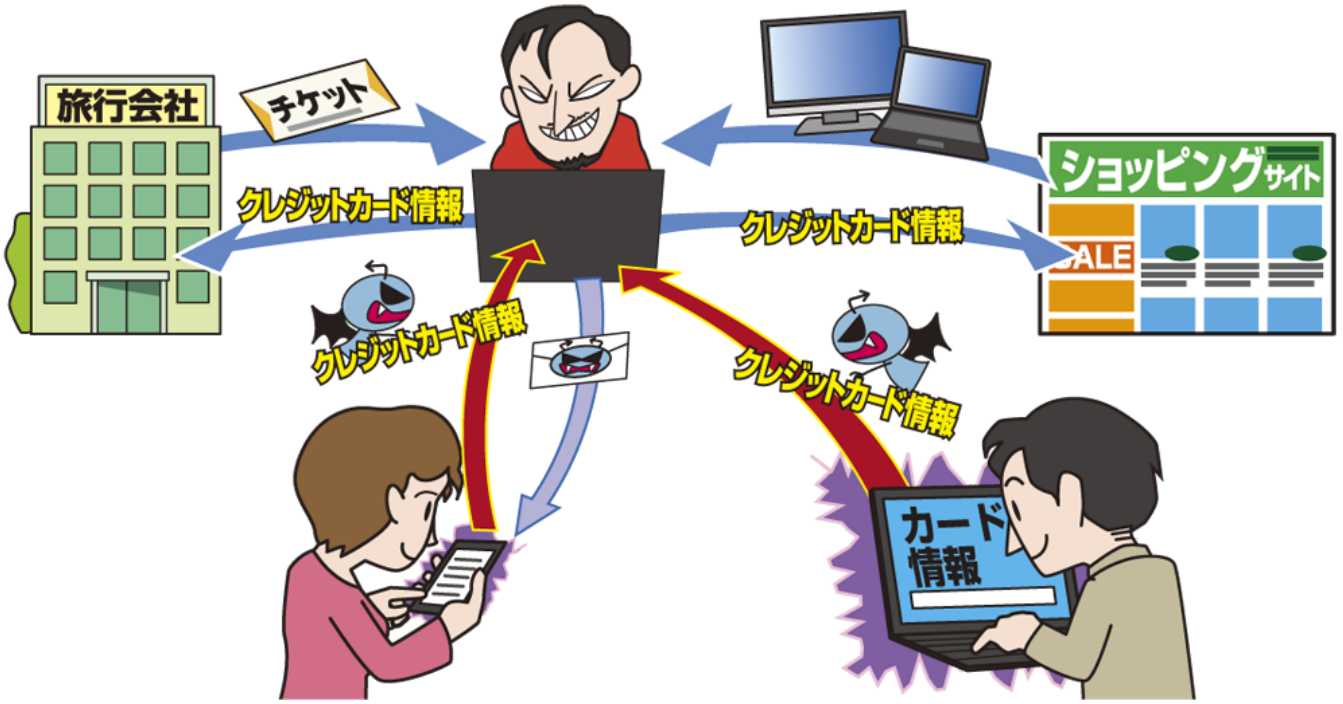
| 「個人」向け脅威 | 順位 | 「組織」向け脅威 |
|---|---|---|
| クレジットカード情報の不正利用 | 1 | 標的型攻撃による被害 |
| フィッシングによる個人情報等の詐取 | 2 | ビジネスメール詐欺による被害 |
| 不正アプリによる<br>スマートフォン利用者への被害 | 3 | ランサムウェアによる被害 |
| メール等を使った<br>脅迫・詐欺の手口による金銭要求 | 4 | サプライチェーンの弱点を悪用した<br>攻撃の高まり |
| ネット上の誹謗・中傷・デマ | 5 | 内部不正による情報漏えい |
| 偽警告によるインターネット詐欺 | 6 | サ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<br>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

# 【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～

- 攻撃手口
  - 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、誘導してウイルスに感染させる
  - 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）

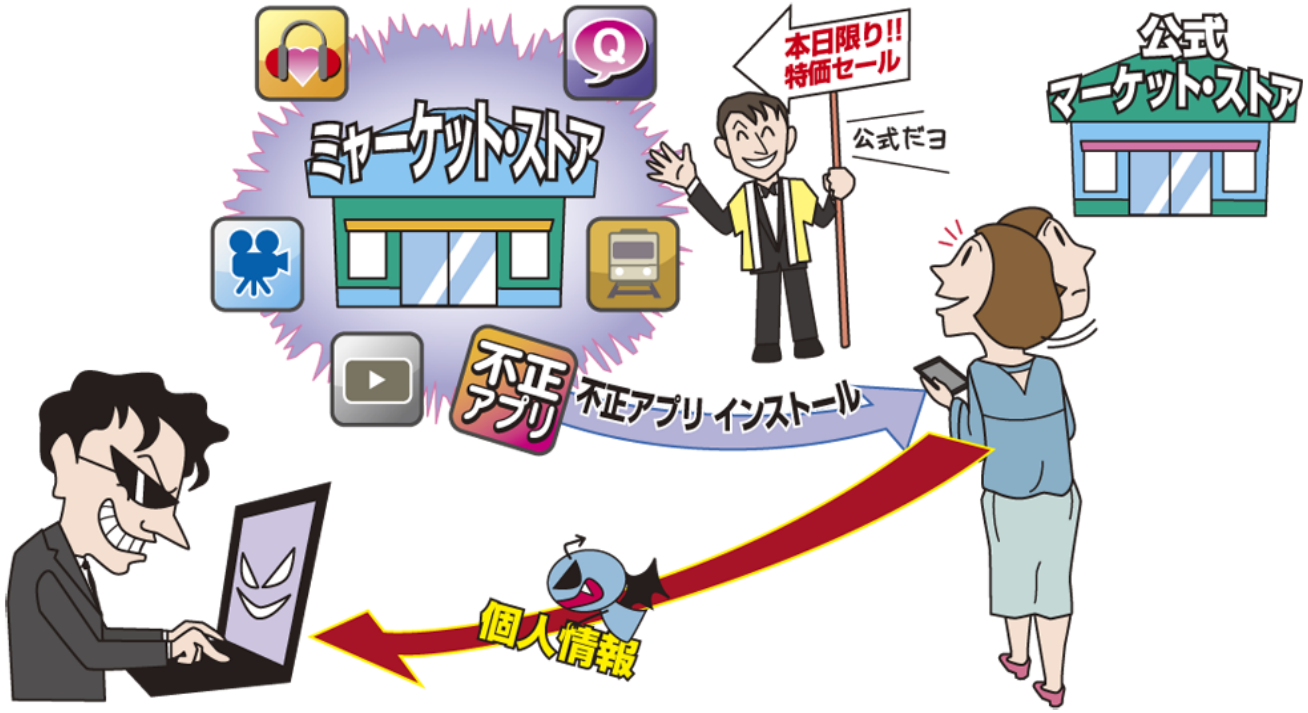
# 【1位】クレジットカード情報の不正利用
～継続する悪用の被害、被害が拡大するおそれ～

- 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/

# 【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**

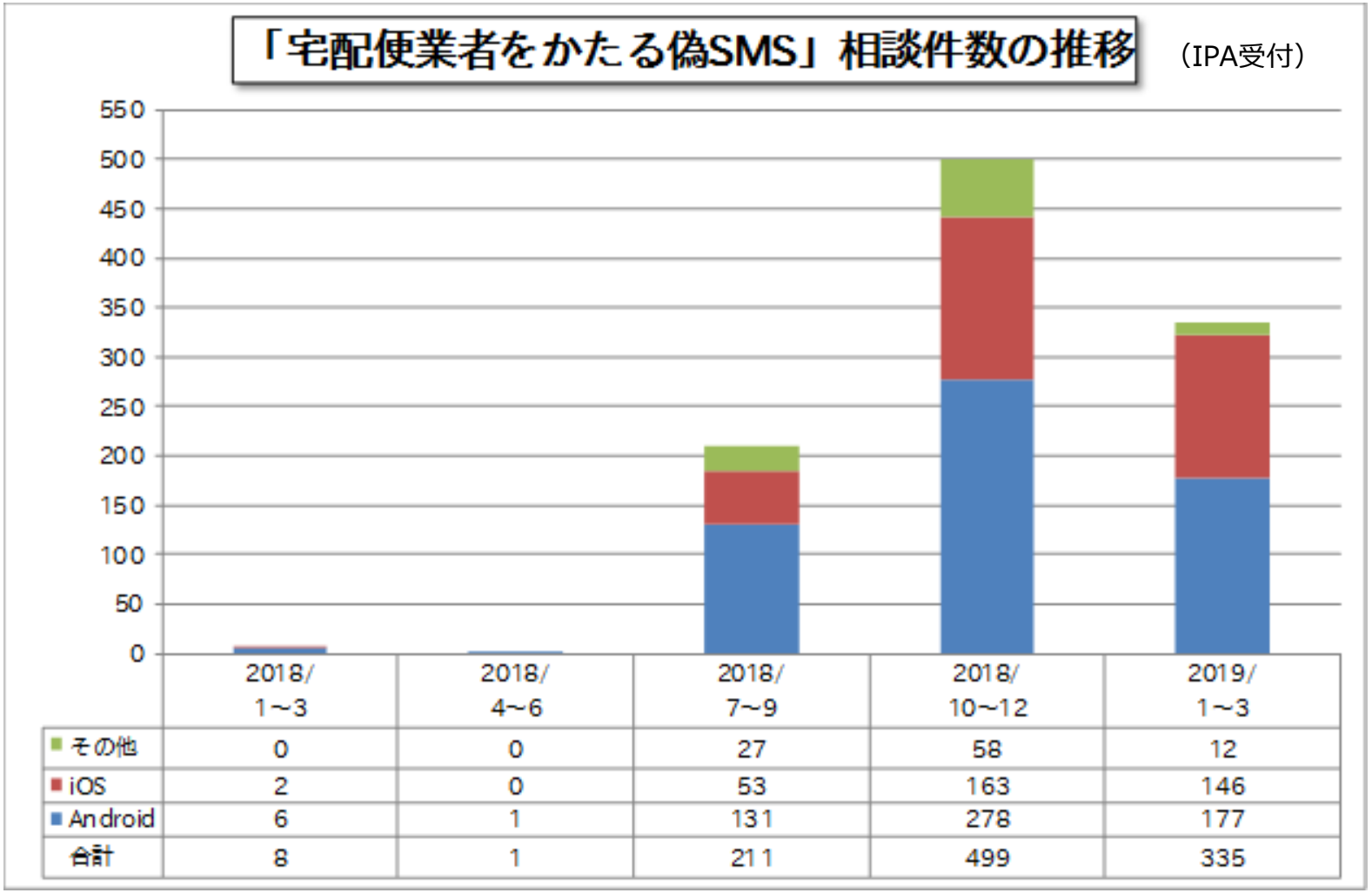
- 不正アプリのダウンロードサイトへ誘導
  - ・実在の企業をかたってメールやSMS等で偽サイト（不正アプリのダウンロードサイト）へ誘導
  - ・正規のアプリであると誤認させて不正アプリをインストールさせる
- 公式マーケットに不正アプリを紛れ込ませる
  - ・不正アプリを正規のアプリと見せかけて公式マーケットに公開
  - ・公式マーケットは安全だと考える利用者を狙う

# 【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～

- 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/

# 「宅配便業者をかたる偽SMS」事例

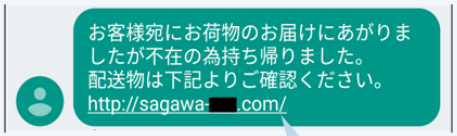



| | 2018/1～3 | 2018/4～6 | 2018/7～9 | 2018/10～12 | 2019/1～3 |
|---|---|---|---|---|---|
| その他 | 0 | 0 | 27 | 58 | 12 |
| iOS | 2 | 0 | 53 | 163 | 146 |
| Android | 6 | 1 | 131 | 278 | 177 |
| 合計 | 8 | 1 | 211 | 499 | 335 |

# 不在通知SMSのリンクを開いてしまうと・・・

Android

**1. 偽の不在通知のSMSを受信**




**2. 記載のURLをタップ**

**3. 偽サイトが表示されると同時にダウンロードが始まる**

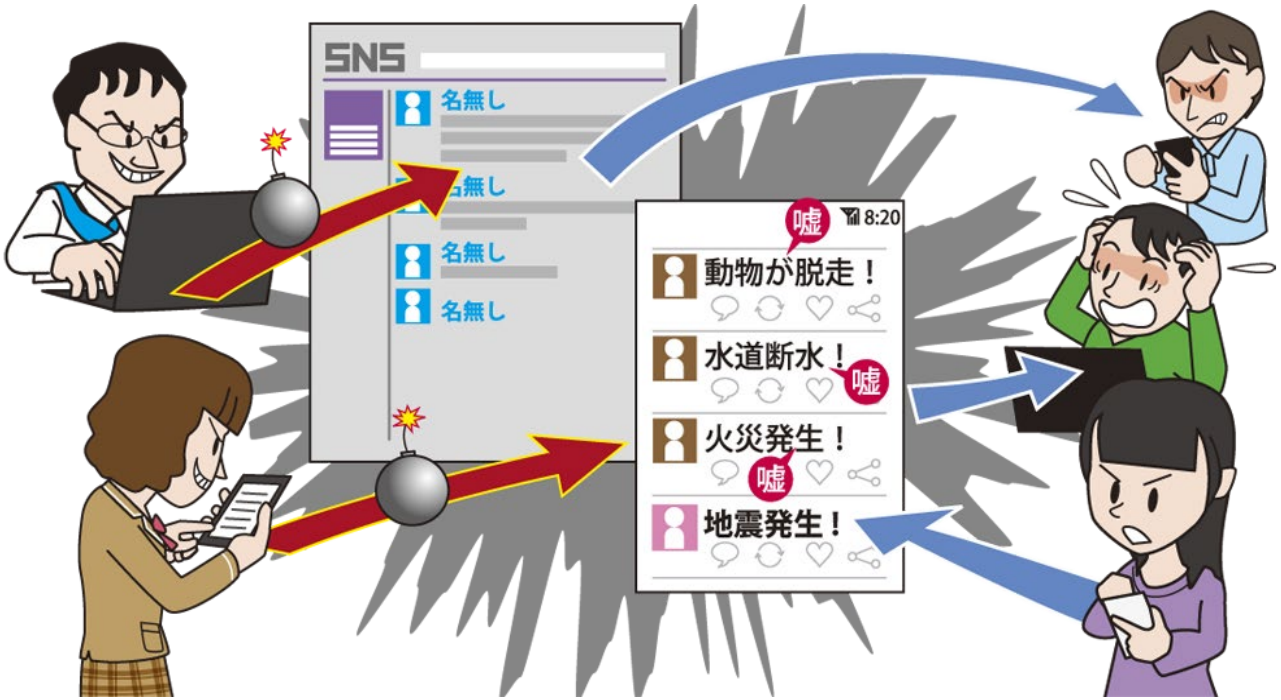

ダウンロードが開始される直前で、警告メッセージが表示されている例

**4. 偽サイトに記載の手順に従ってインストールする**


インストールしてしまうと被害につながる

# 【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～

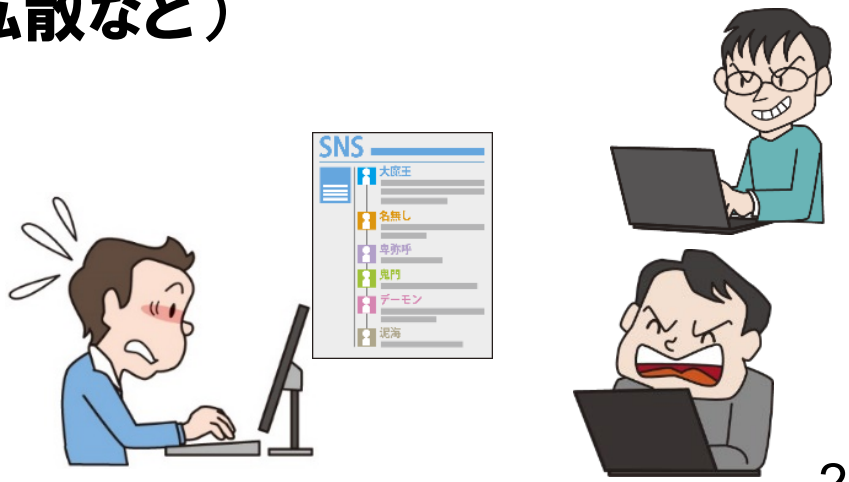
## ● 要因

**・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～

## 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

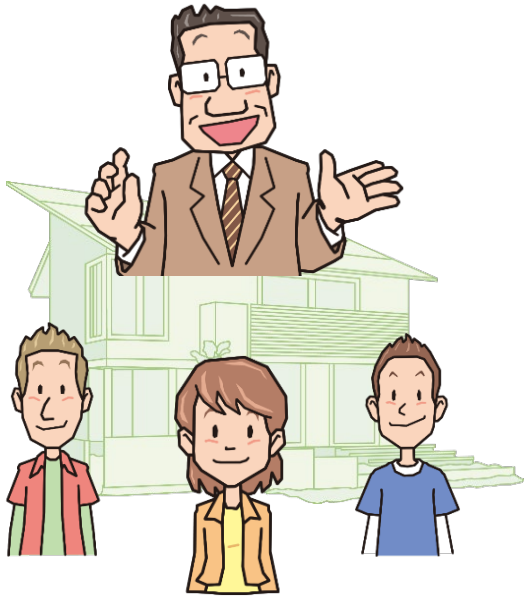
－投稿前に内容を再確認

### 家庭、教育機関

・情報モラル、情報リテラシーの教育

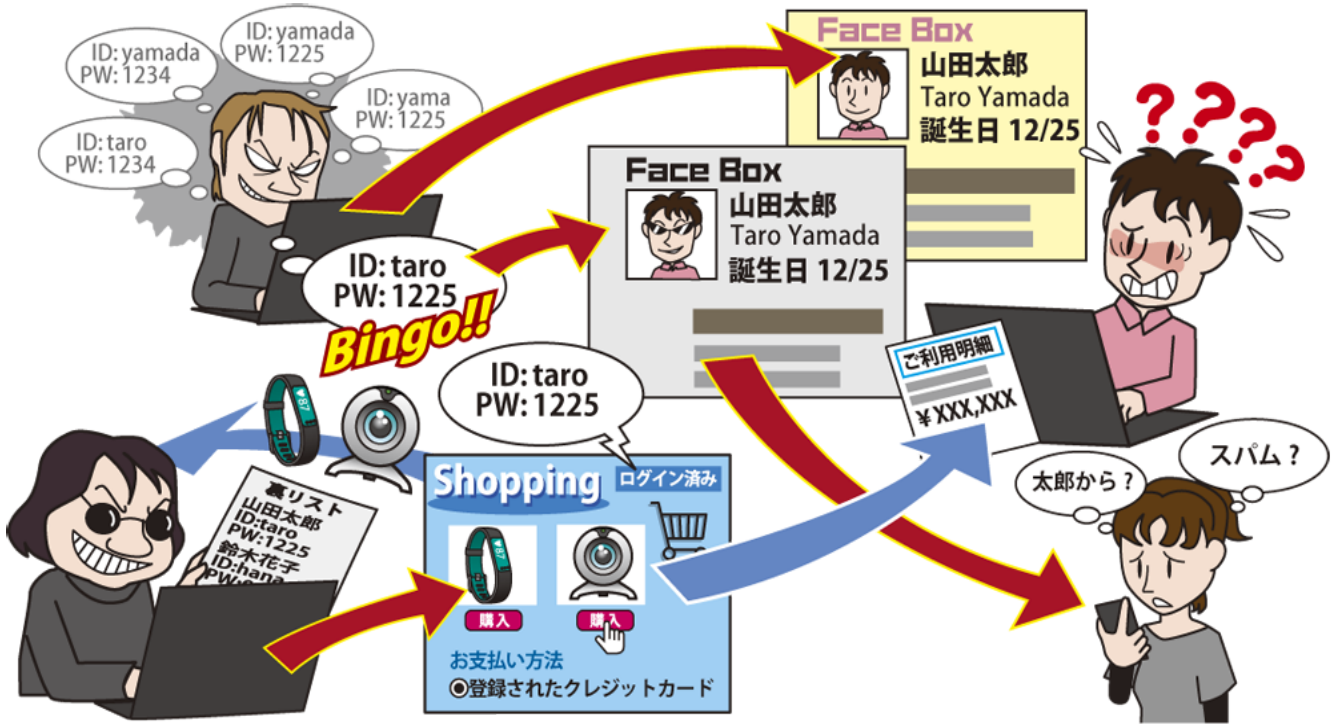
－自宅や学校で子供たちに情報モラルや
情報リテラシーの教育を行う

－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



# 【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～

- 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