

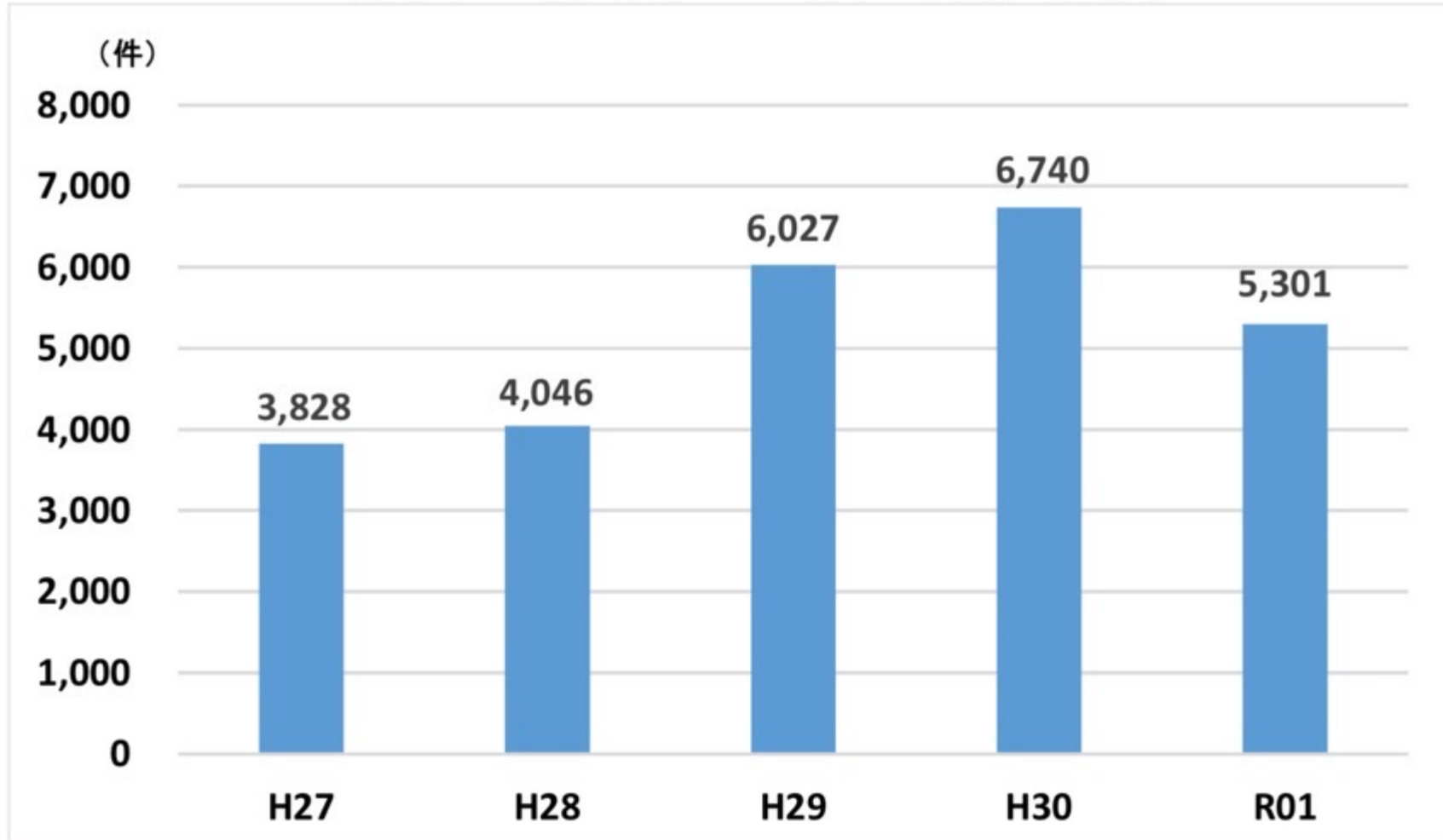
情報セキュリティ特論

第1回

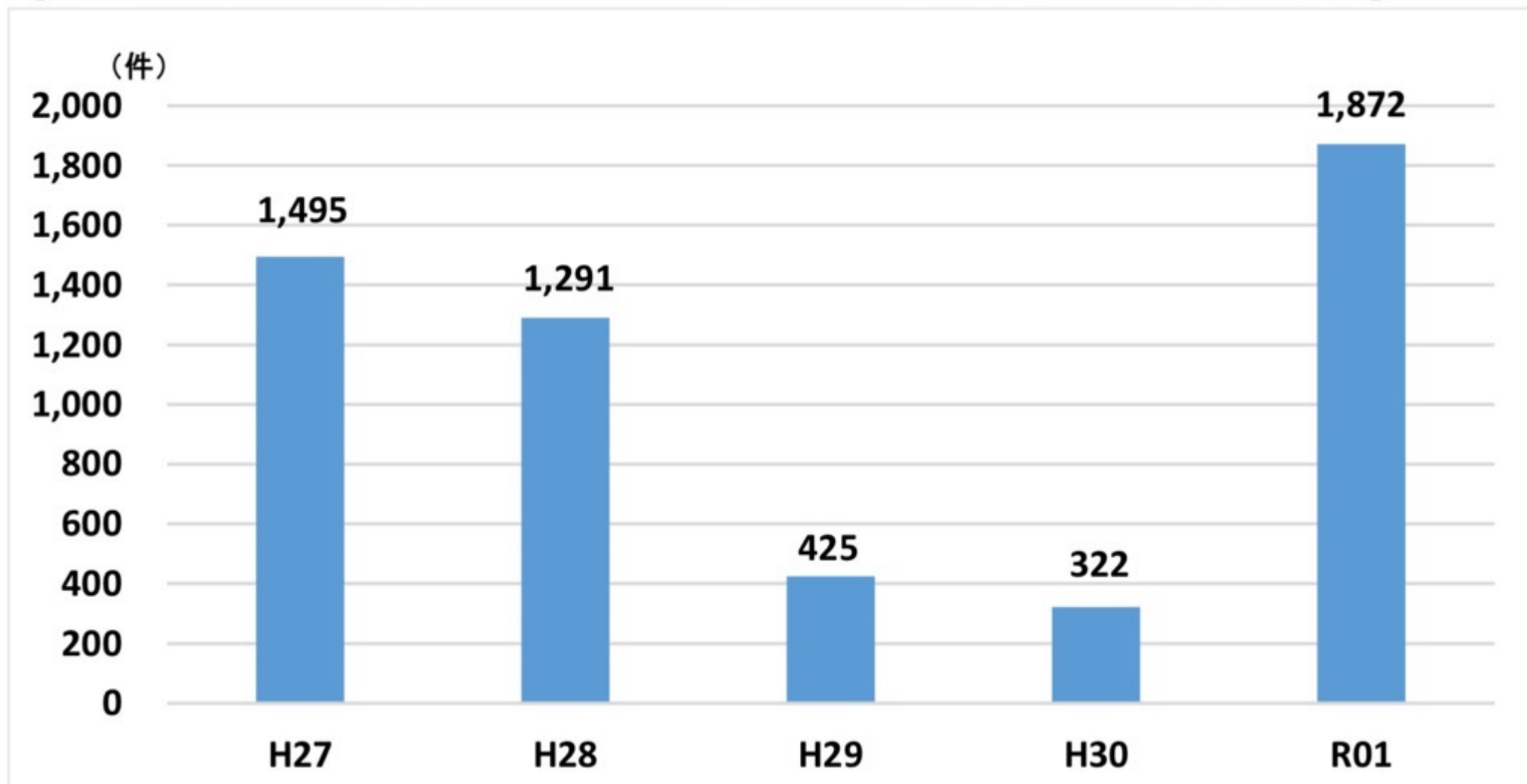
情報セキュリティの基礎

警察庁HPより

【図表 4 標的型メール攻撃の件数の推移】

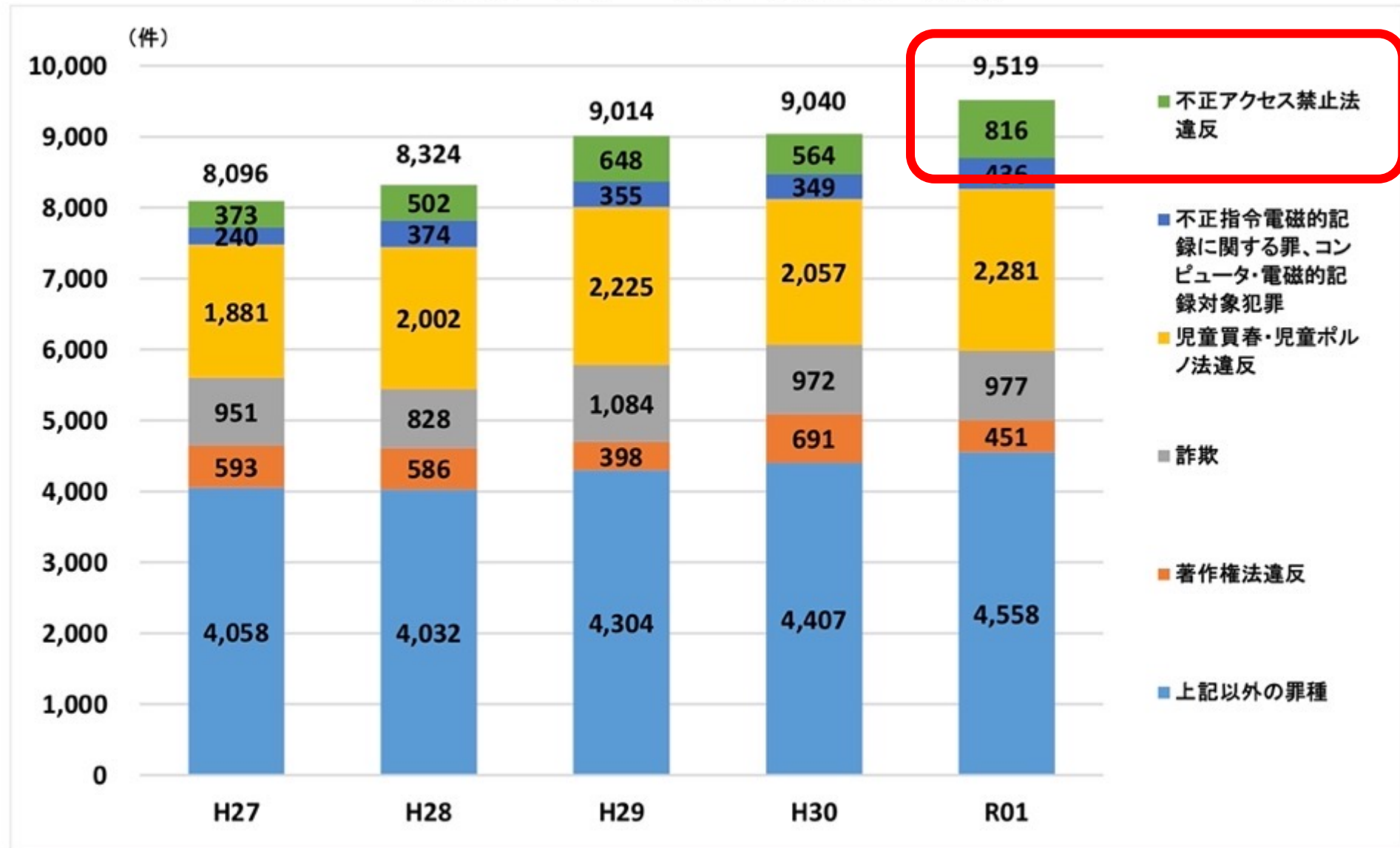


【図表11 インターネットバンキングに係る不正送金事犯の発生件数の推移】

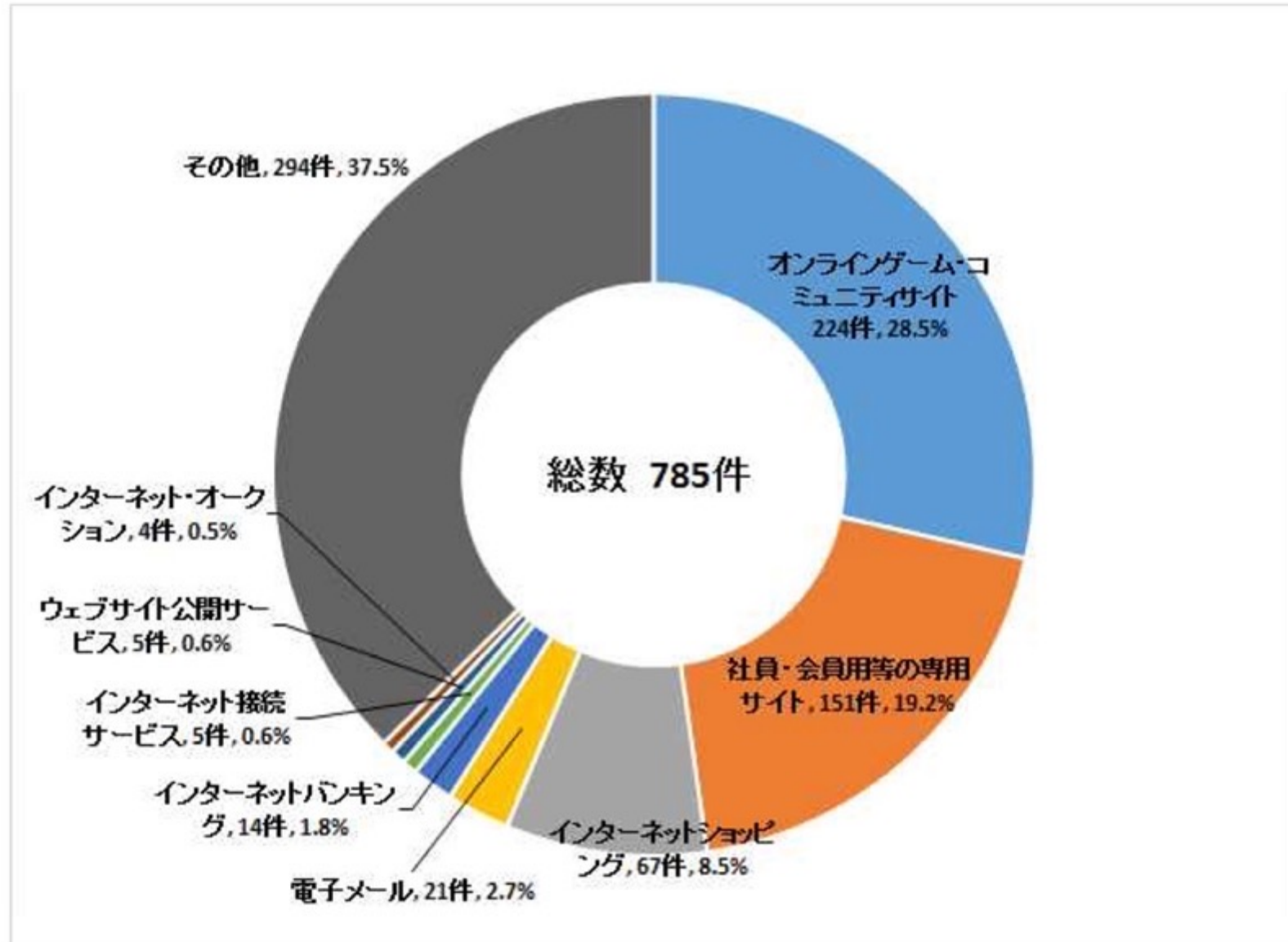


“サイバー犯罪” = “不正アクセス禁止法違反”？

【図表9 サイバー犯罪の検挙件数の推移】



(2) 不正に利用されたサービス別検挙件数（識別符号窃用型）



3つのセキュリティ

1. 物理的セキュリティ

盗難、不法侵入、破壊

2. 技術的セキュリティ

ハッキング、脆弱性攻撃、DoS攻撃

3. 人的セキュリティ

ウィルス感染、パスワード漏洩、設定ミス



「物理的セキュリティ」

- サーバ、データの物理的な盗難防止
- 電子データ媒体、紙媒体の管理・破棄
- 電源のバックアップ



1. 物理的セキュリティ

「盗難」や「不法侵入」に気をつけましょう

⇒これは、だいたいわかっているつもり、、、

以下の点に注意

- 鞆の中にPCやスマホを入れっぱなしで食堂の席取り
- クルマのエンジンをかけっぱなしでコンビニ
- アパートの鍵をかけないで外出

「技術的セキュリティ」

- サーバ、PCのセキュリティ対策
- ネットワークのセキュリティ対策
- 攻撃防御と攻撃検知



脆弱性

- 古いバージョンのOS, アプリケーション
- デフォルト設定のサーバ・ファイアウォール
- 暗号化されていない通信
- アプリケーション、スクリプトのデフォルト設定
- 簡単なパスワード、ブルートフォースアタック非対策



脆弱性

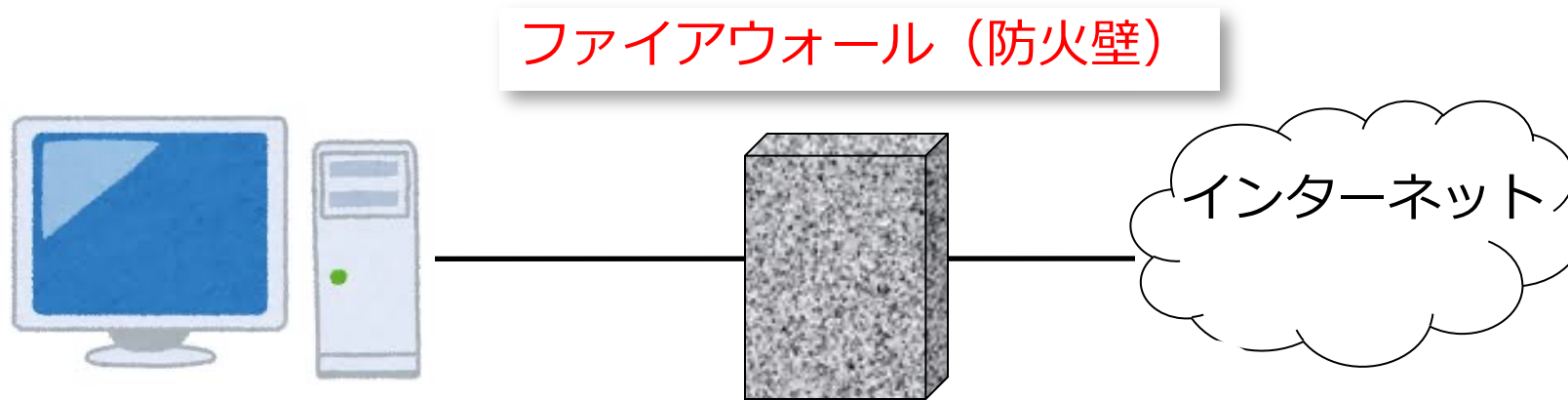
- 古いバージョンのOS, アプリケーション
- デフォルト設定のサーバ・ファイアウォール
- 暗号化されていない通信
- アプリケーション、スクリプトのデフォルト設定
- 簡単なパスワード、ブルートフォースアタック非対策



ファイアウォールとは

外部ネットワークからの侵入から内部ネットワークを安全に保つための仕組み（装置あるいはソフトウェア）

必要な通信のみを通し、それ以外は遮断する



- WWW (http)
- メール (SMTP)
- その他の通信

遮断



ファイアウォール

- WWW (http)
- メール (SMTP)
- その他公開できるもの

公開用区画

- Webサーバ
- メールサーバ

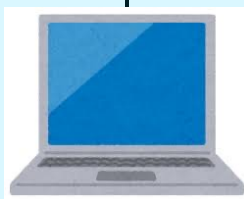
「公開用区画」との
アクセスのみ許可

- WWW (http)
- メール (SMTP)

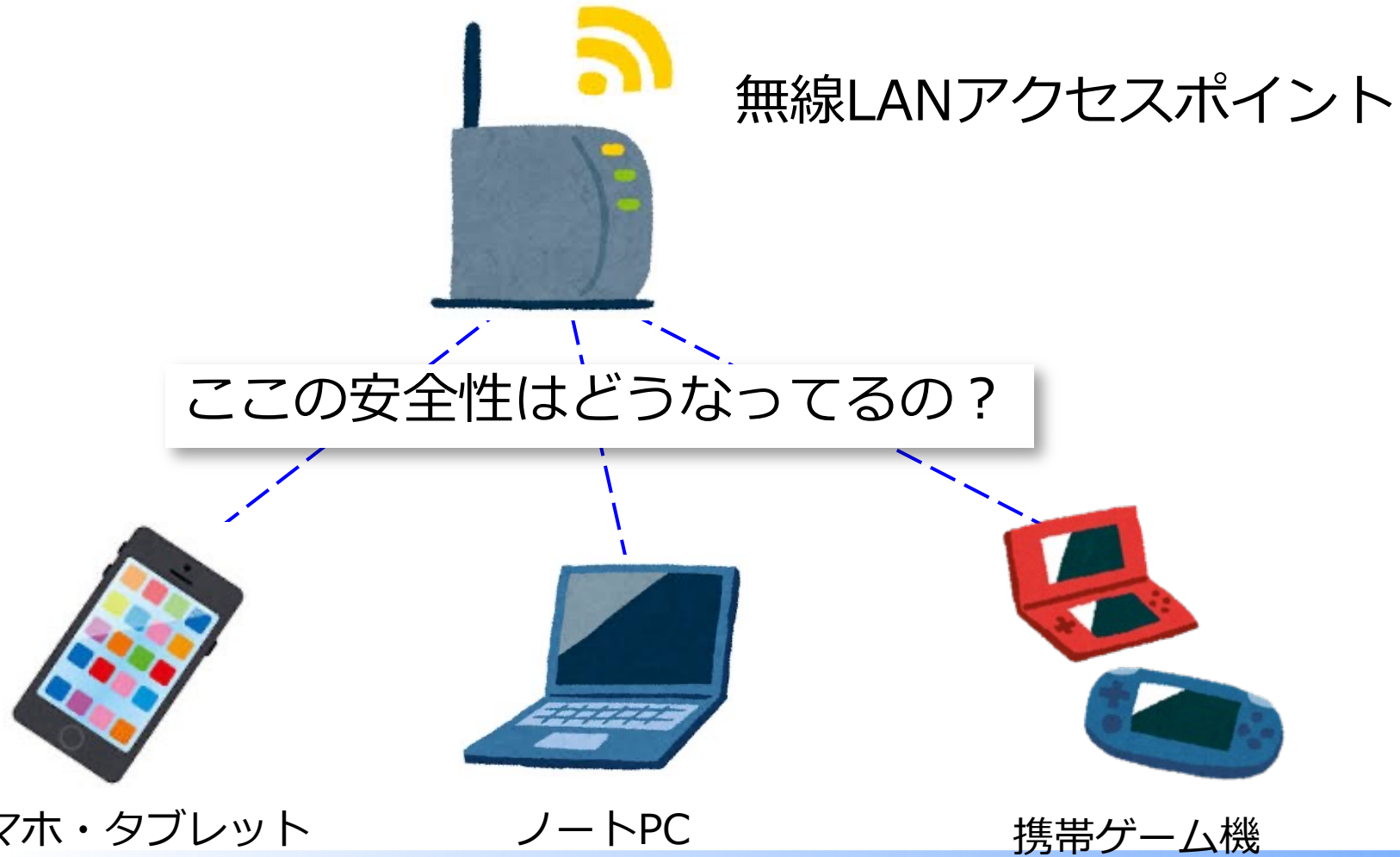
学内ネットワークが安全に保たれる

Switch

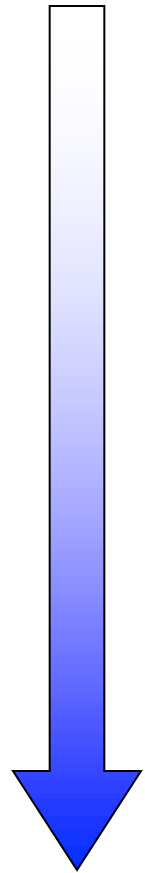
学内ネットワーク



無線LANのセキュリティ



無線LANの暗号化



WEP

- 最もポピュラーな暗号化
- 暗号鍵が固定⇒簡単に解読されてしまう

TKIP

- 鍵を定期的に変更

AES

- 鍵を定期的に変更
- 複雑な暗号化

認証: WPA, WPA2, WPA3

セキュリティが高い

「人的セキュリティ」

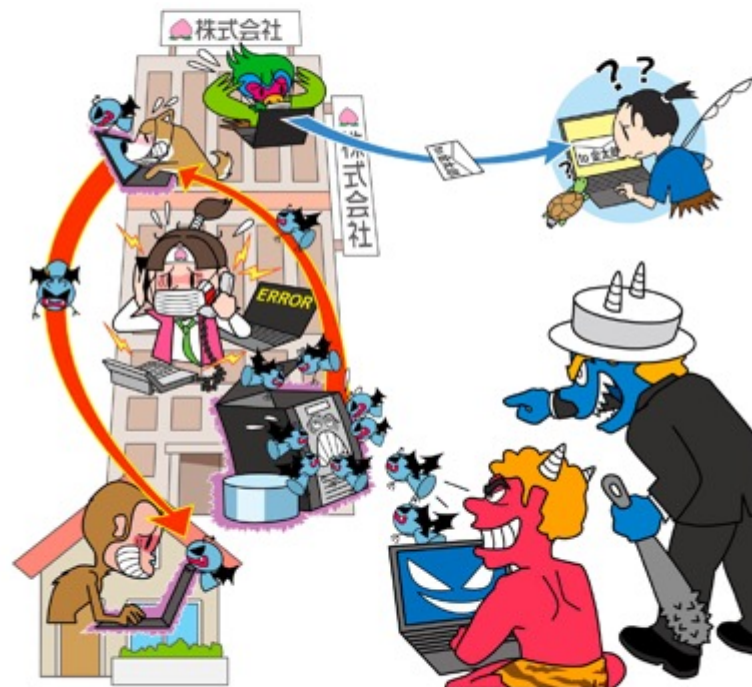
- ID/パスワード漏洩対策
- メール添付ファイル対策
- 設定ミスの解消
- 共有ユーザの管理
- ユーザのライフサイクル管理



情報セキュリティ

10大脅威 2021

～よもや自組織が被害に！呼吸を合わせて全力防御！～



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

2021 年 2 月

「今、何が起きているか」

IPA: 情報処理推進機構「情報セキュリティ10大脅威 2021」
<https://www.ipa.go.jp/security/vuln/10threats2021.html>
<https://www.ipa.go.jp/files/000088835.pdf>

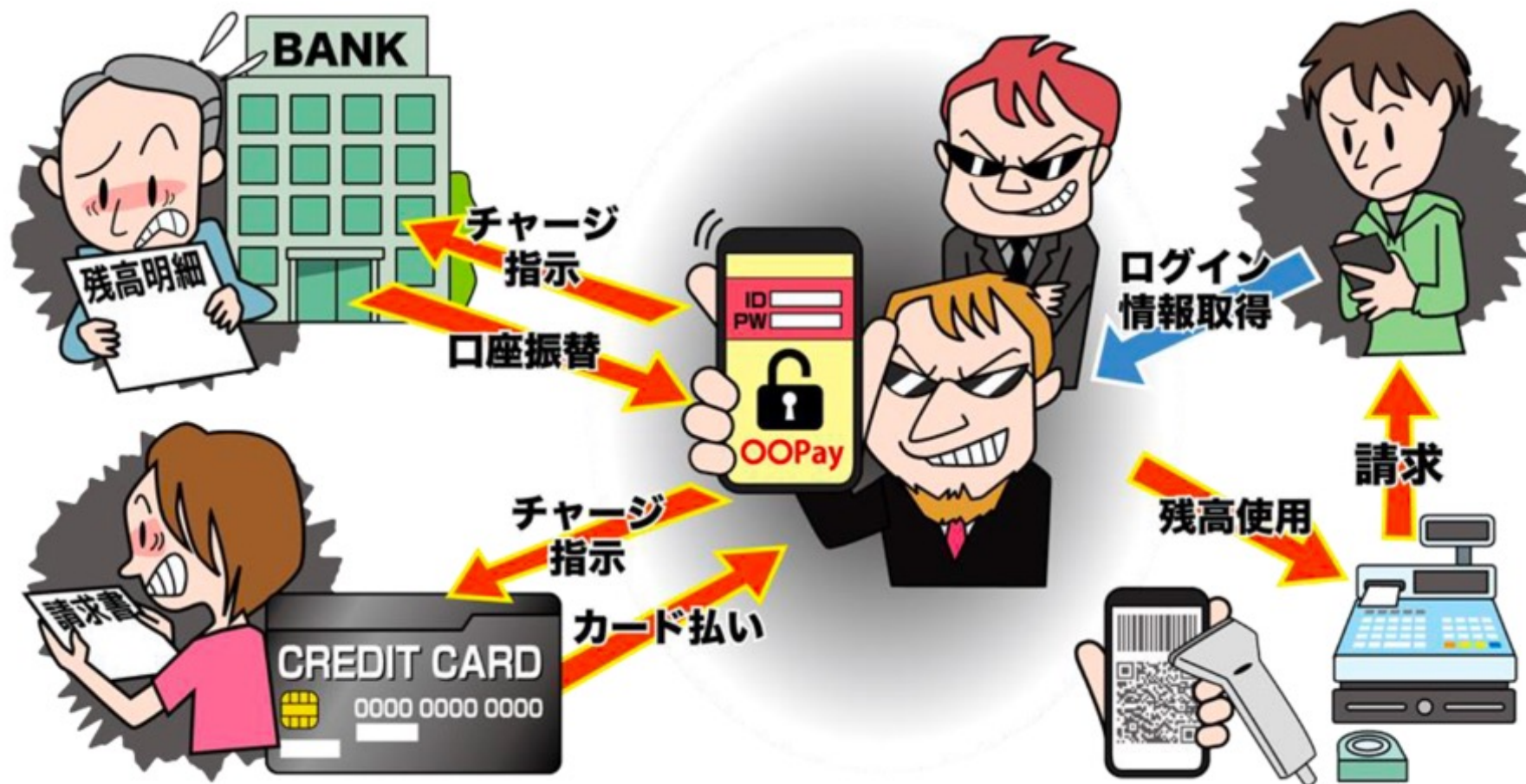
数理・データサイエンス・AI教育強化拠点コンソーシアム
サイバーセキュリティ推進校会議

表 1.1 情報セキュリティ 10 大脅威 2021 「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
スマホ決済の不正利用	1	ランサムウェアによる被害
フィッシングによる個人情報等の詐取	2	標的型攻撃による機密情報の窃取
ネット上の誹謗・中傷・デマ	3	テレワーク等の ニューノーマルな働き方を狙った攻撃
メールや SMS 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
クレジットカード情報の不正利用	5	ビジネスメール詐欺による金銭被害
インターネットバンキングの不正利用	6	内部不正による情報漏えい
インターネット上のサービスからの 個人情報の窃取	7	予期せぬ IT 基盤の障害に伴う業務停止
偽警告によるインターネット詐欺	8	インターネット上のサービスへの 不正ログイン
不正アプリによる スマートフォン利用者への被害	9	不注意による情報漏えい等の被害
インターネット上のサービスへの 不正ログイン	10	脆弱性対策情報の公開に伴う悪用増加

1位 スマホ決済の不正利用

～スマホ決済の不正利用被害に備え利用状況の確認を～



2位 フィッシングによる個人情報等の詐取

～コロナ禍の生活の変化に乗じてオンラインショッピングに関連するフィッシングが急増～



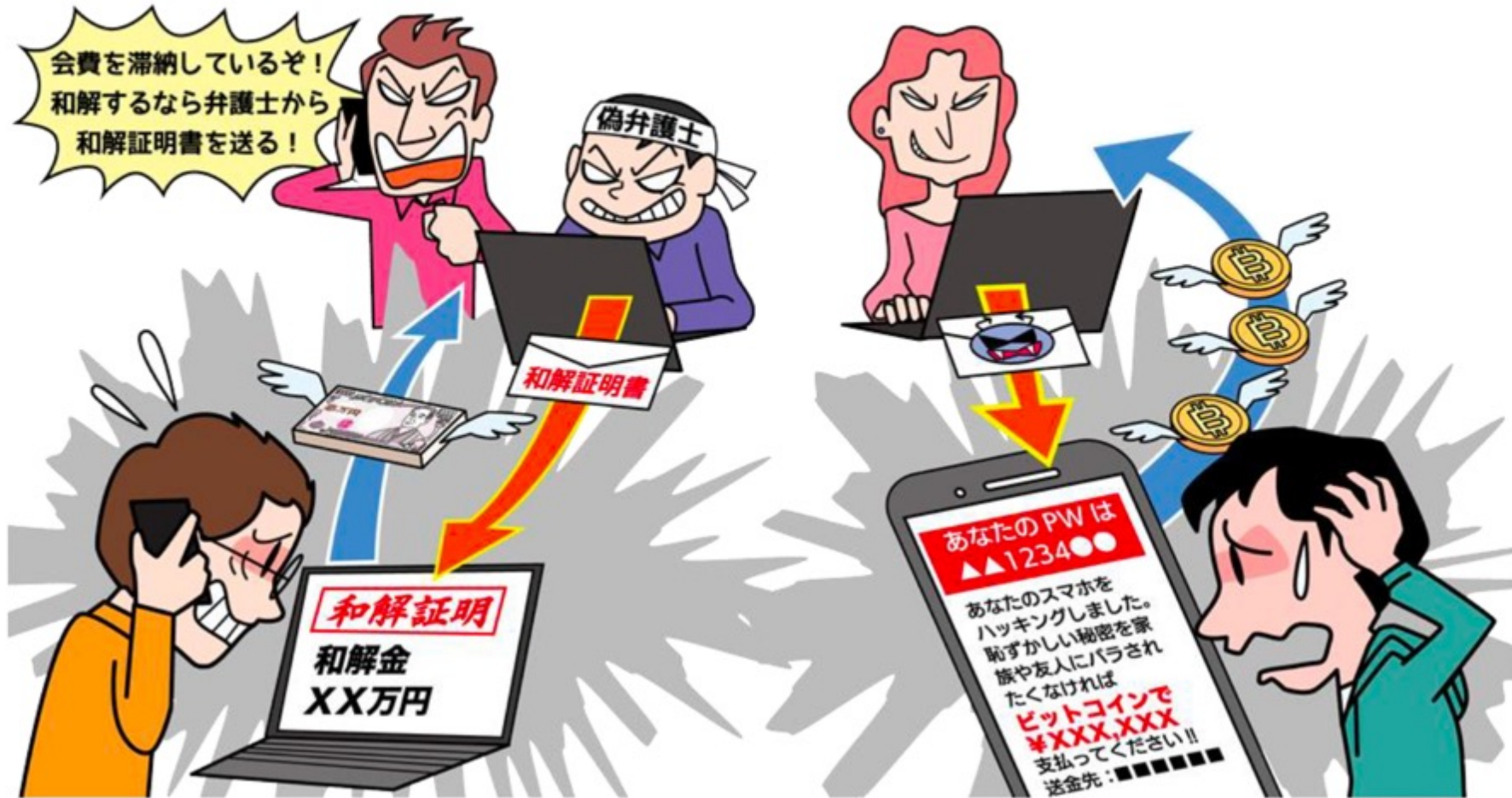
3位 ネット上の誹謗・中傷・デマ

～安易な書き込みが、他者と自分の人生を脅かす～



4位 メールや SMS 等を使った脅迫・詐欺の手口による金銭要求

～脅迫・詐欺メールの指示に従うと相手のおもうつぼ～



「架空請求メール」の例

宛先：darekasan@daredare.co.jp

差出人：プロバイダ管理人"mailmaster@daredare.co.jp"

件名：【大切なお知らせ】超過利用と支払いについて

登録名 "darekasan@daredare.co.jp" 殿

2025年4月1日から5月31日の本プロバイダの利用状況が調査の結果、契約された範囲を超過いたしておりました。

つきましては約款第10条8項に基づき、超過分の利用料を以下の手順に従ってお納めいただくようお願いいたします。

「高額請求」が来てしまったら

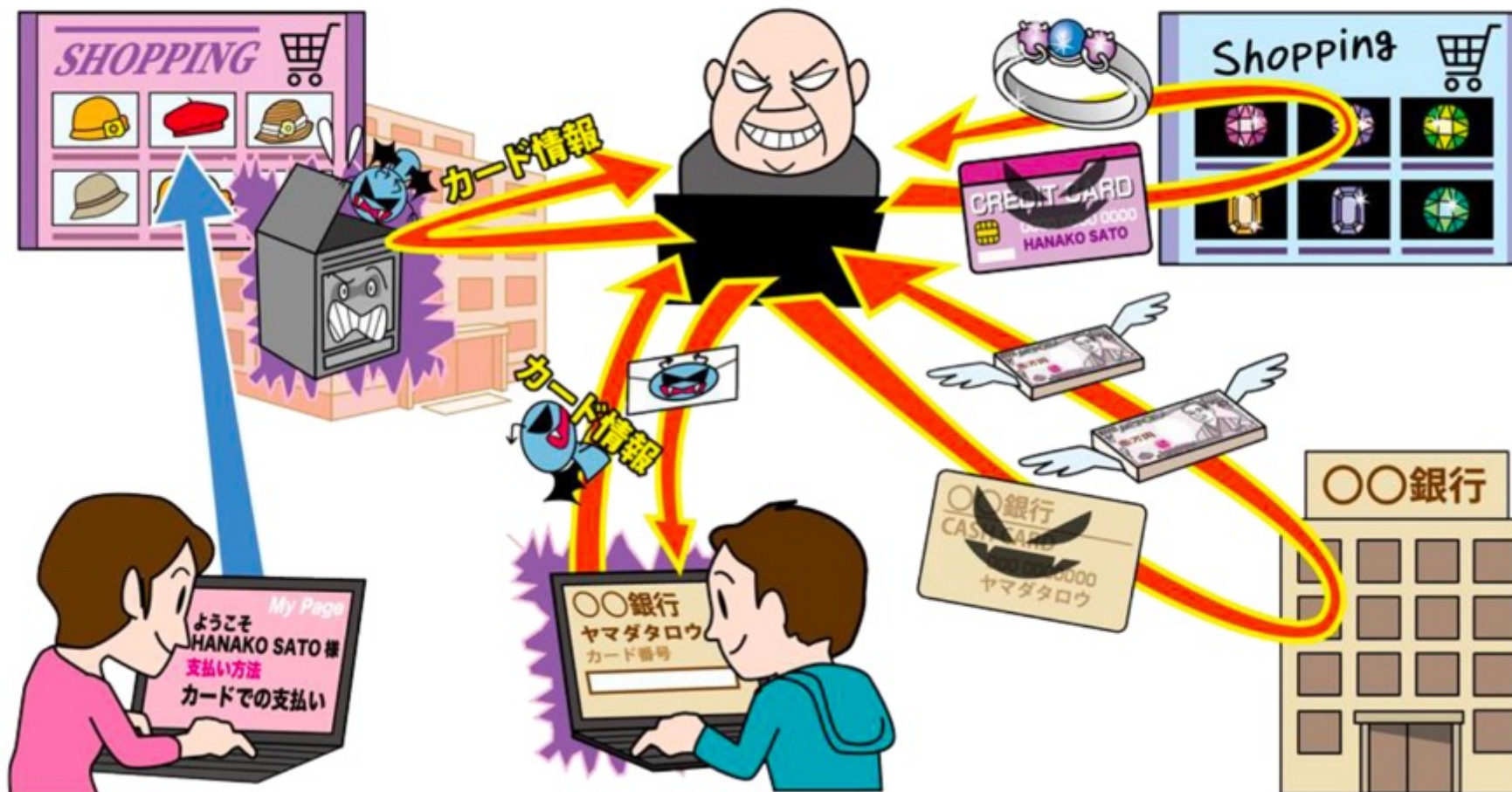
自分の身に覚えが無いのなら、ほぼ間違いなく「架空」な請求です。

以下のことをチェックして、心配な場合は[消費生活センター](#)へ
事件性がありそうな場合（盗品販売等）は警察へ行くのも手です。

- 有料サイトを登録して使用した**（「無い」なら無視してOK）
- 請求元がサイトやプロバイダではなく債権回収業者になっている**
（この場合は無視してOK）
- 法定外の金利や延滞料、手数料を要求してくる**
（この場合は無視してOK）

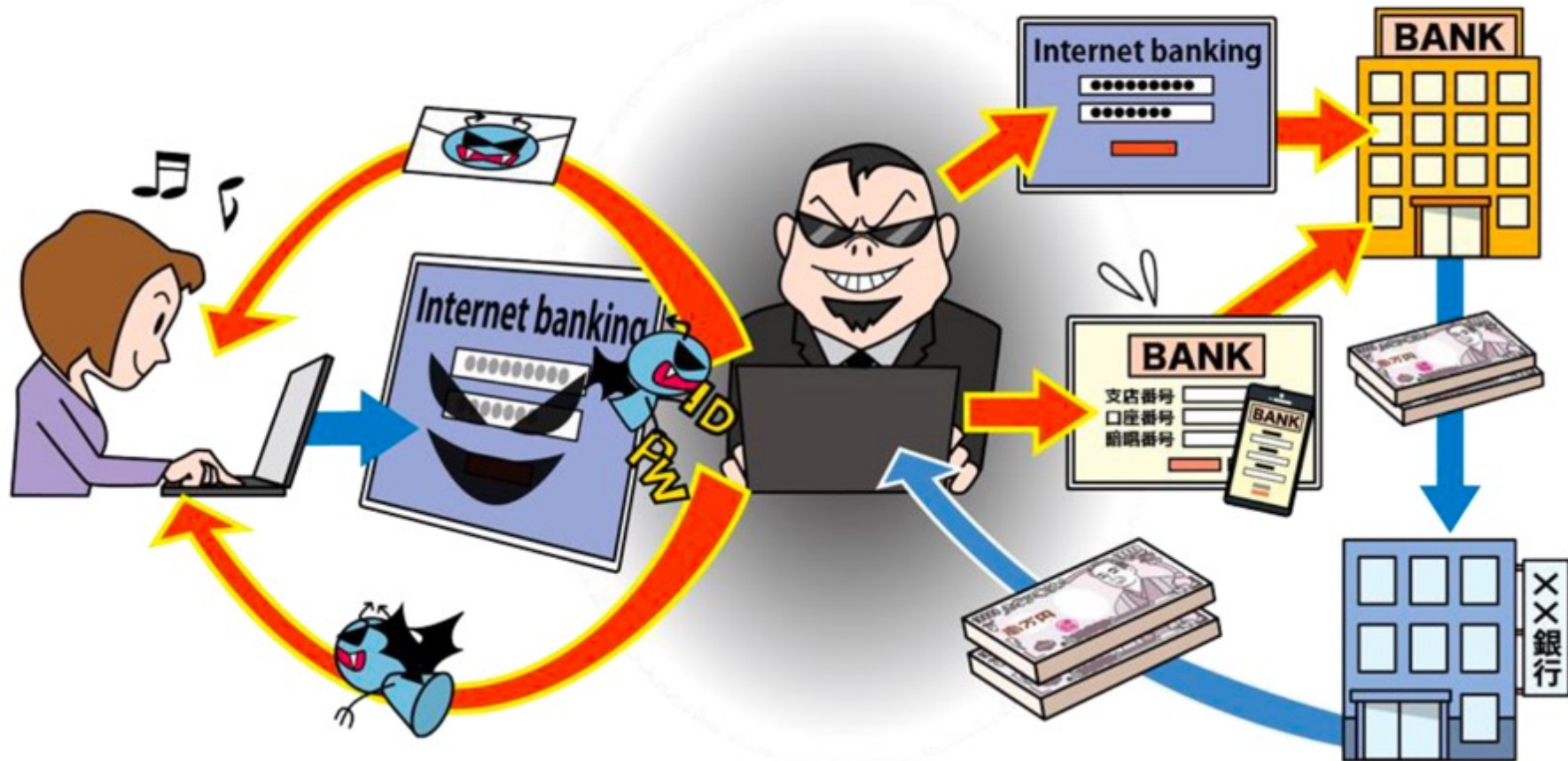
5位 クレジットカード情報の不正利用

～知らない間に流出し不正利用されているかも～



6位 インターネットバンキングの不正利用

～こまめな口座の利用履歴の確認および不審なログイン履歴がないかの確認を～



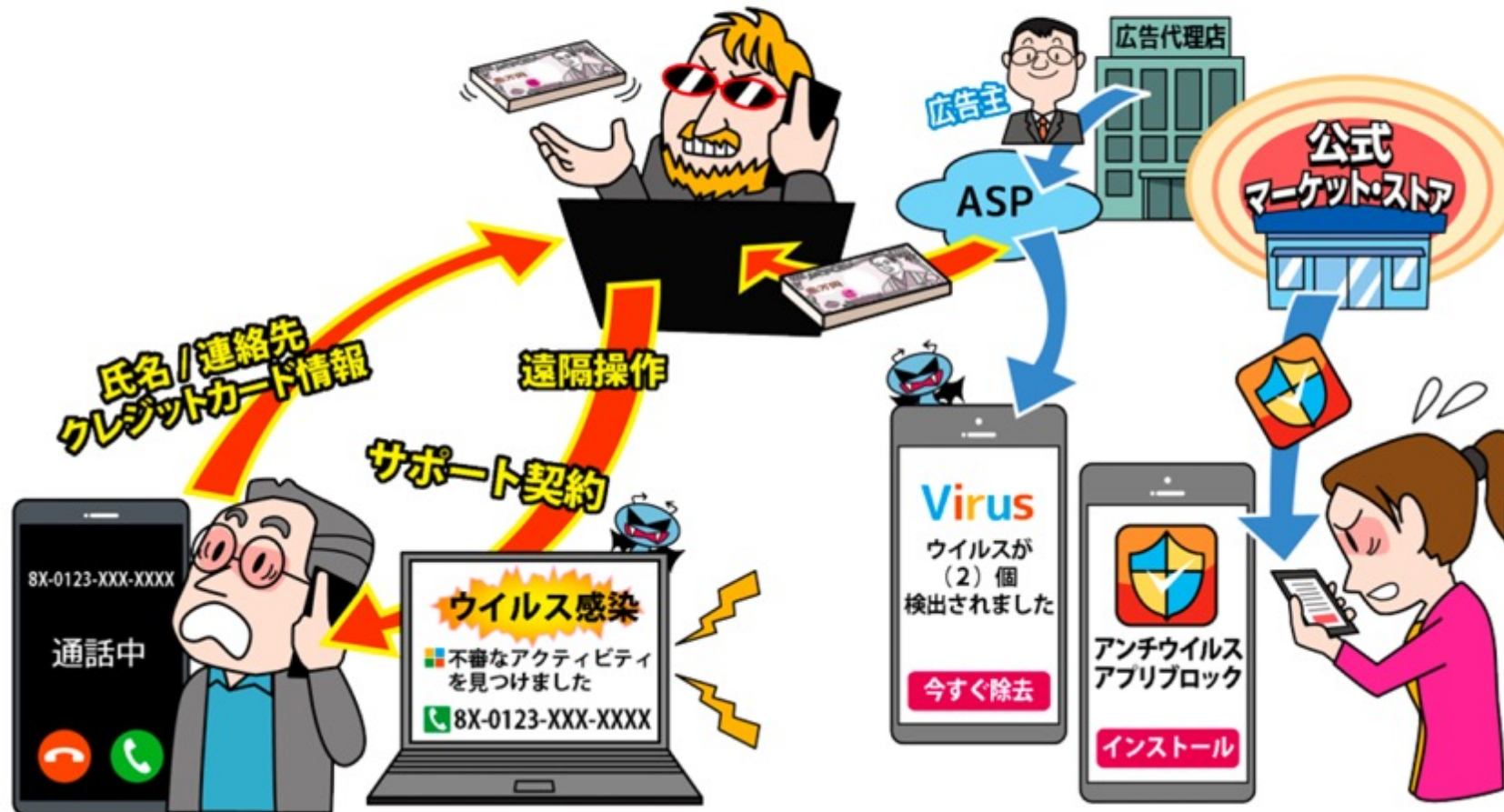
7位 インターネット上のサービスからの個人情報の窃取

～利用者でできる対策を忘れずに、ID やパスワードの使いまわしに注意～



8位 偽警告によるインターネット詐欺

～突然の警告は本物？慌てず、焦らず、落ち着いて～



9位 不正アプリによるスマートフォン利用者への被害

～宅配業者を装った SMS にご用心！油断に付け入る不正アプリ～



スマートフォンのセキュリティ

スマートフォンは個人情報の塊

- 持ち主と相手の個人情報

名前、電話番号、メールアドレス

- 使用者の情報

電話やインターネットの使用状況

GPSでの位置情報



「アンドロイド」スマートフォンによる情報漏洩の例

2012年4月発生

- ゲームを装ったアプリで個人情報情報が漏洩
- 使用者や通話先の個人情報情報が特定のサーバへ送信
- 100万人の情報が漏洩した可能性



「簡単にインストール」の罠

本ソフトウェアは一見、ものすごく良さそうなソフトウェアに見えます。実際、使ってみると驚く程快適で、これまでの生活が一変するくらい便利なソフトウェアです。ただし、インストール後、あなたの個人情報を特定のサーバに送信します。本当にあなたの個人情報を送信します。確実にあなたの個人情報を送信します。すっかりそのままあなたの個人情報を送信します。一つ残らずあなたの個人情報を特定のサーバに送信します。最後にもう一度言います。インストール後、あなたの個人情報を特定のサーバに送信します。使用している間は気がつきません。ネットで騒いで話題になってからではもう手遅れでしょう。取得した情報は有効に利用させていただきます。あしからず。

インストールに同意

キャンセル

よく読まないで「同意」を押してませんか？

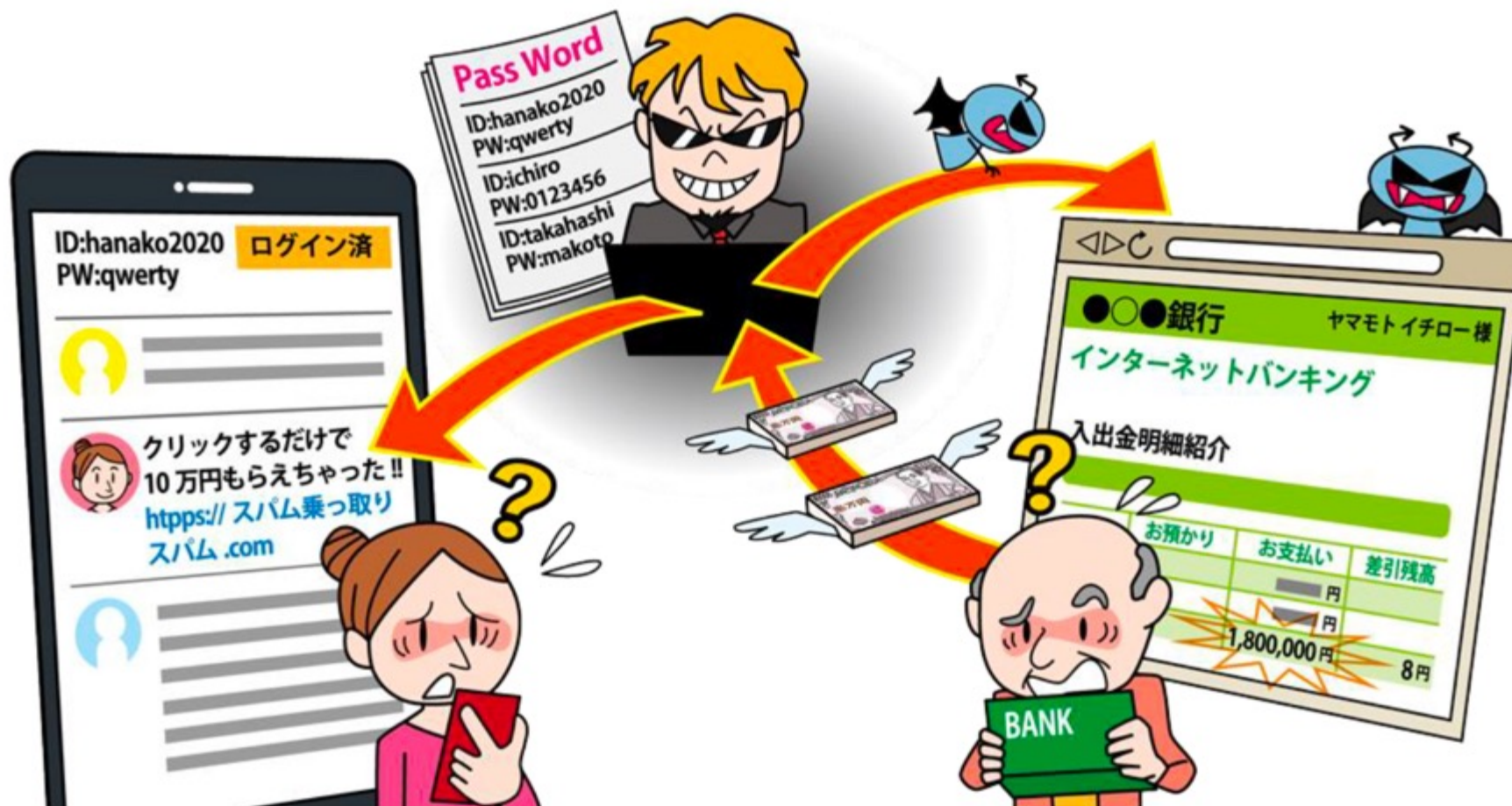
これに対処するには

- まずはネットで評判を確かめる
- インストールの前に同意文書をちゃんと読む
- 携帯電話会社が提供しているアプリ配布サービスを利用する

いちおう、このくらいはやっておいてもいいかも知れません。
(でも完璧ではありませんが)

10位 インターネット上のサービスへの不正ログイン

～不正ログインによる大きな金銭的被害や個人情報漏えいのおそれ～



(1) 不正アクセス行為（識別符号窃用型）に係る手口別検挙件数

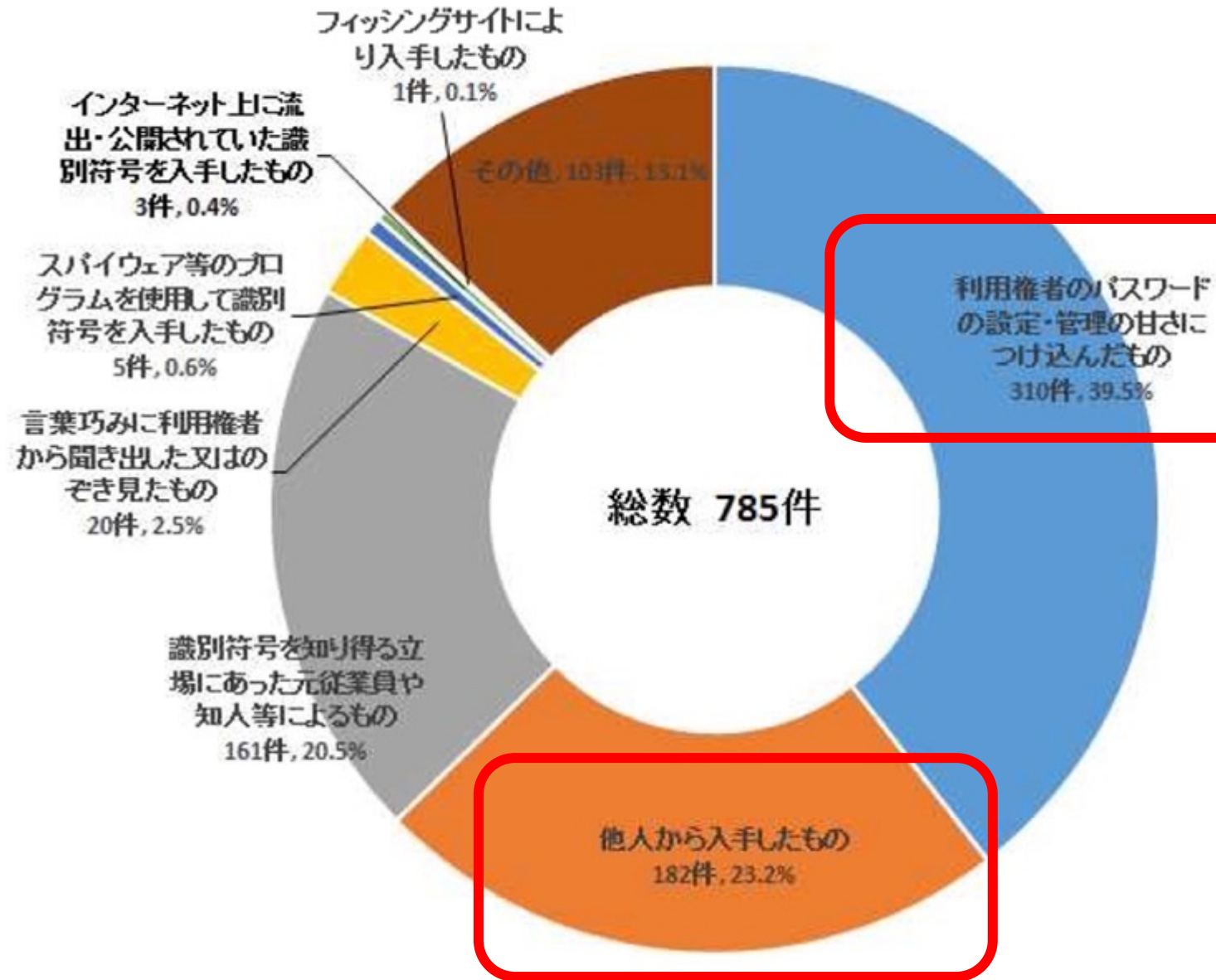


表 1.3 情報セキュリティ対策の基本

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	手口から重要視すべき対策を理解する

「パスワード漏洩」や「設定ミス」に気をつけましょう

⇒ 最近、これを利用したハッキングが増えています

簡単に他人を信用してはいけない

- 「あのパスワードなんだっけ？」には答えない
- パスワードを紙に書いて置いておくのはダメ
- なるべく、個人情報を入れることを避ける

最近IT業界では “ID・パスワードは限界” と言われています。

なぜか？

ID・パスワード (ID/PW)が氾濫しすぎているから

全部「違うID・パスワードの組」は無理！

せめて、これだけはやっておこう

ユーザIDが“メールアドレス”の場合

ユーザID: hogehoge@universal-mail.jp

パスワード: * * * * * * * * * * * (何文字か足す)

(メールを使うときと同じパスワード) ➡ 別のパスワードになる

メールを使うときのパスワードと**同じにしない**