情報セキュリティ

第2回：インターネット上の脅威について

授業計画

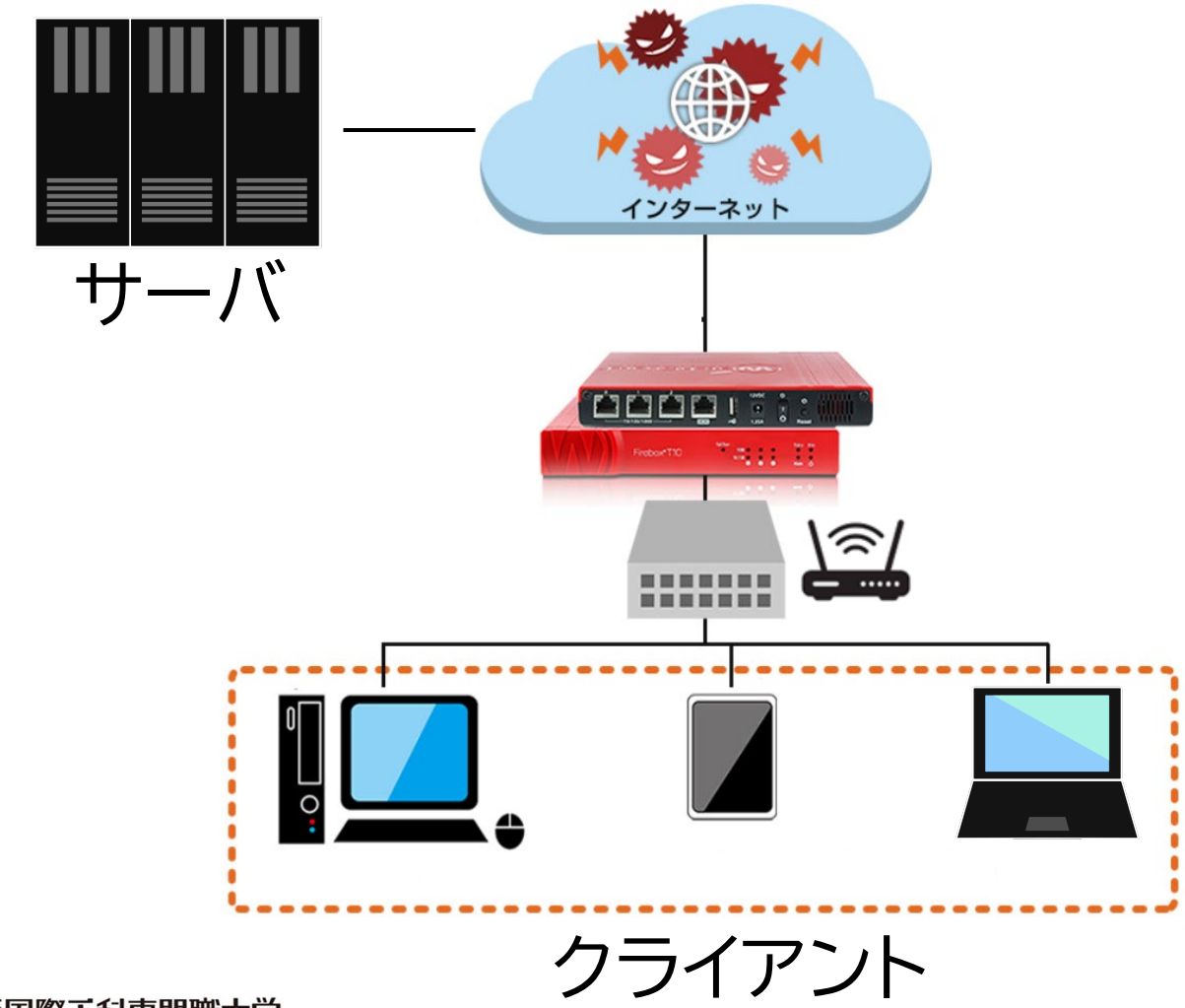
① ガイダンス
②インターネット上の脅威について
③ 攻撃について
④ コンピュータウイルス（マルウェア）について
⑤ 小テスト，ネットワーク上の各種攻撃の紹介
⑥ 攻撃の技術
⑦ 情報・ネットワーク技術の基礎
⑧ ネットワークセキュリティに関する技術と方法
⑨ 暗号の基礎
⑩ 小テスト，セキュリティ技術と方法に対する確認
⑪ 対処法１（システムリスク）
⑫ 対処法２（ソーシャルリスク：SNS）
⑬ 対処法３（ソーシャルリスク：インターネット・スマホゲーム）
⑭ 対処法に関する小テスト
⑮ 全体のまとめ

本日の講義内容

1. インターネットに潜むリスク
2. 情報セキュリティにおける被害事例
3. リスクへの一般的な対処法

1. インターネットに潜むリスク

1.1 インターネットの特徴



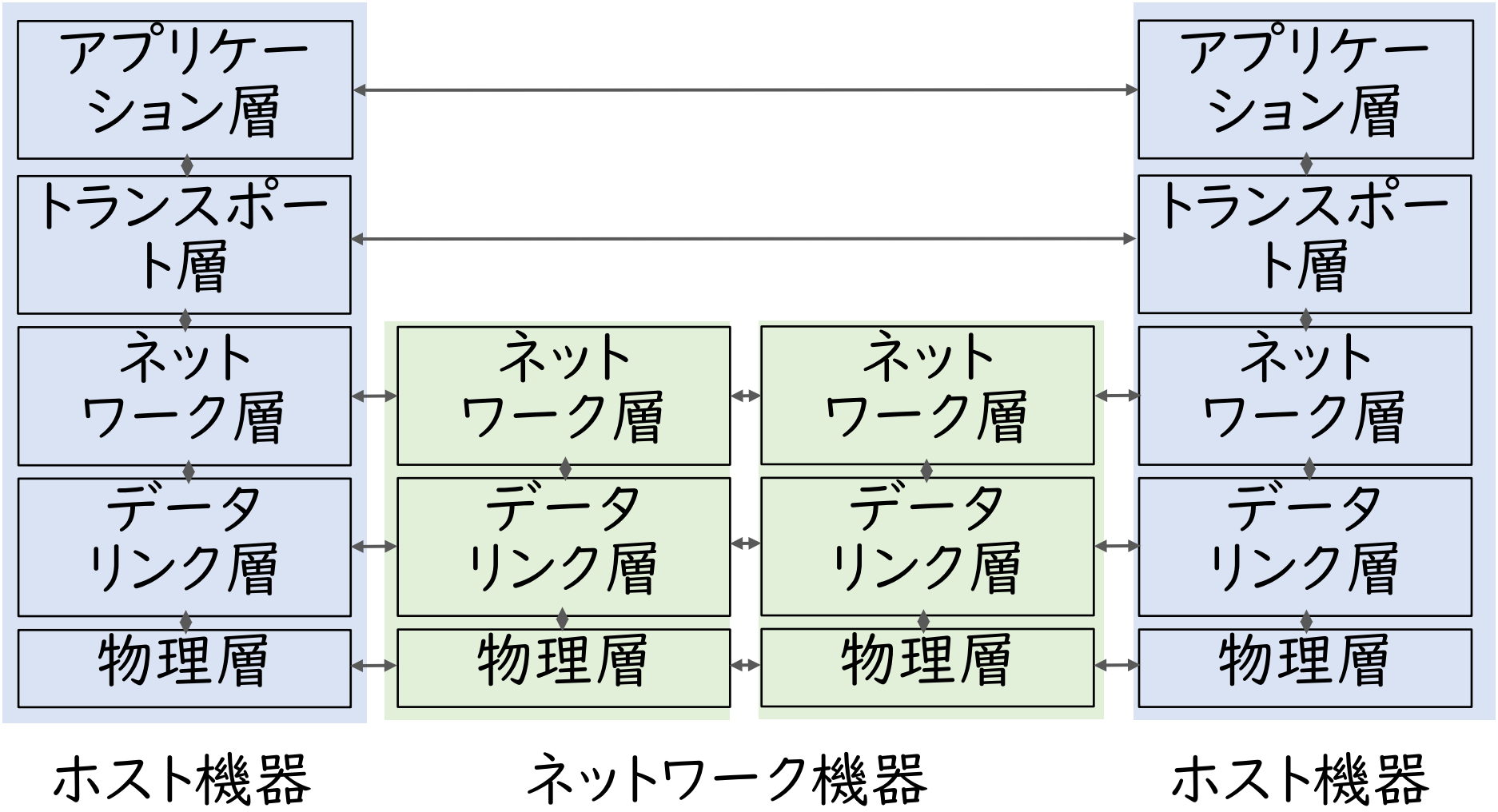
インターネットは全世界に広がっており不正アクセス等脅威がたくさん存在している

ネットワークとネットワーク機器は攻撃の対象になりやすい

端末に脆弱性など弱点がある

インターネットのTCP/IP参照モデル（5階層）

どの機器でも，どの階層でも，セキュリティ攻撃をされる可能性があります．

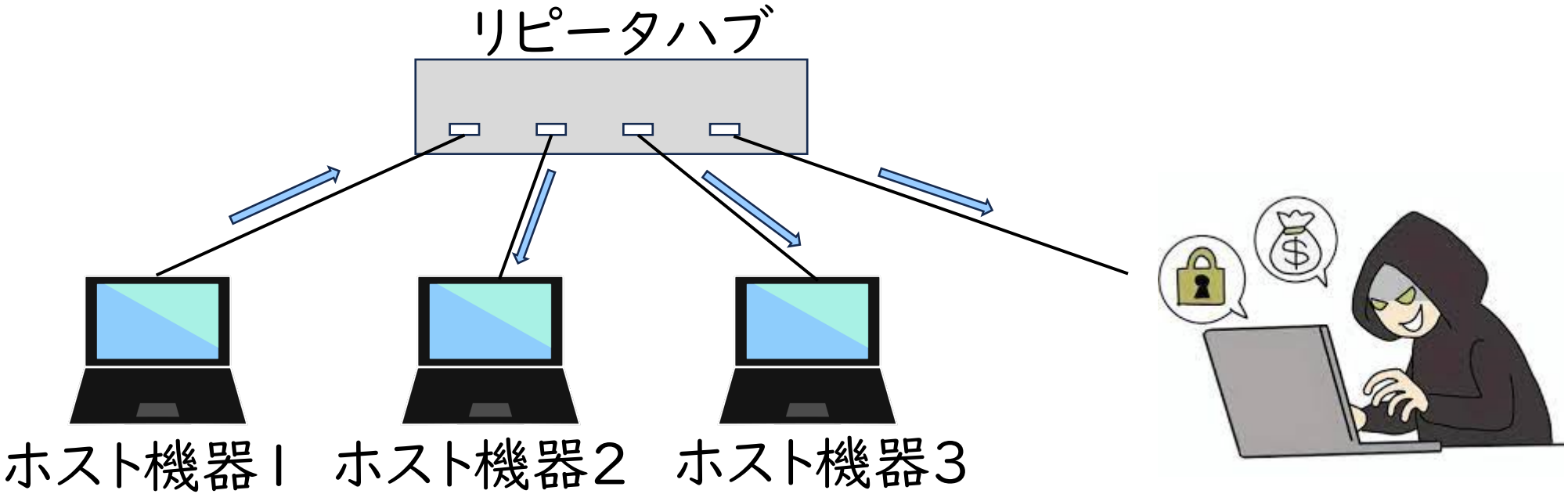


1.2 通信の盗聴や改ざん

① リピータハブによる盗聴

リピータハブは，データリンク層の中継機器です．入力されたMACフレームを，入力ポート以外のすべてのポートに送出します．

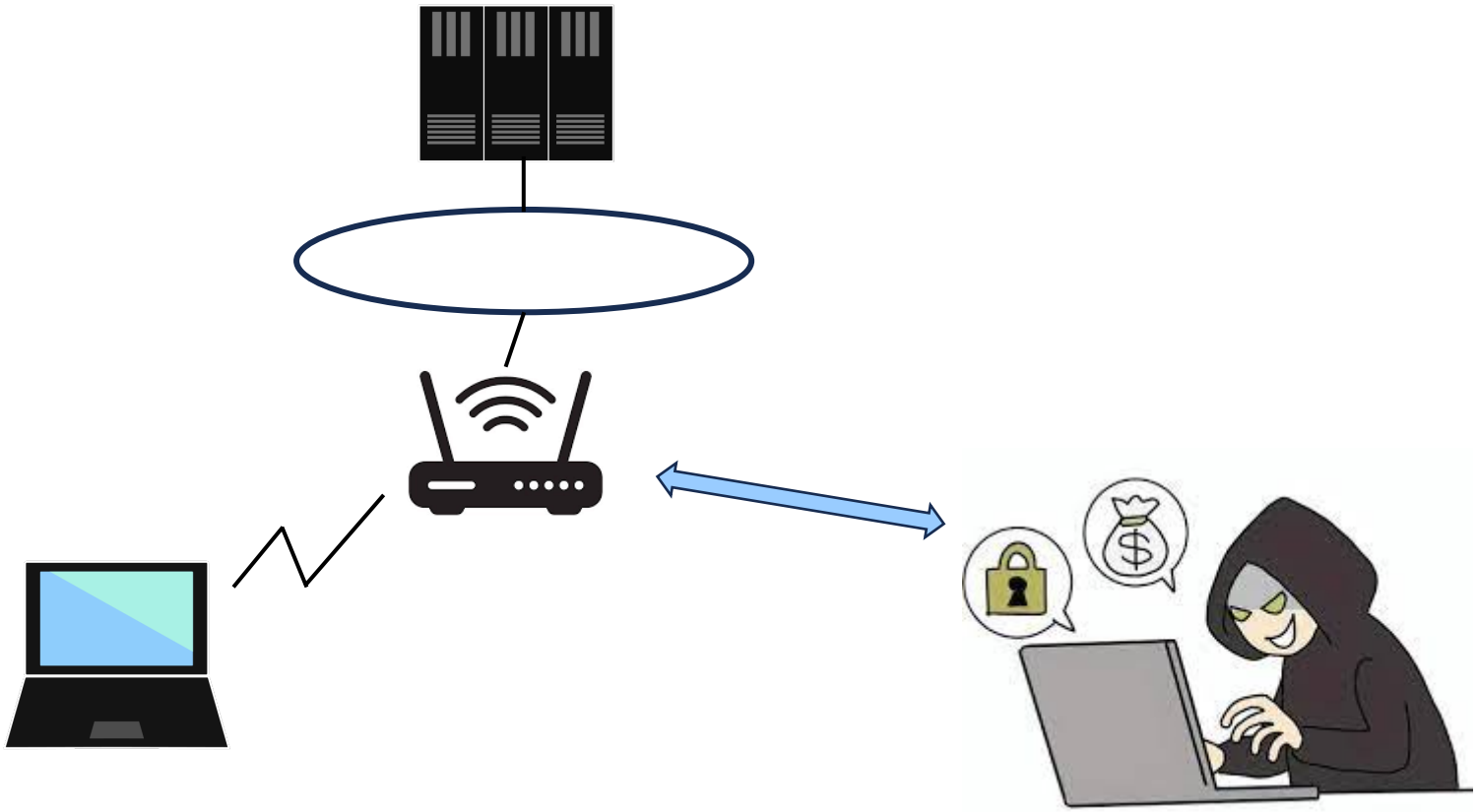
攻撃者がリピータハブをLAN回線に組み込むと，容易に盗聴が可能になります．



② 無線LAN通信の盗聴

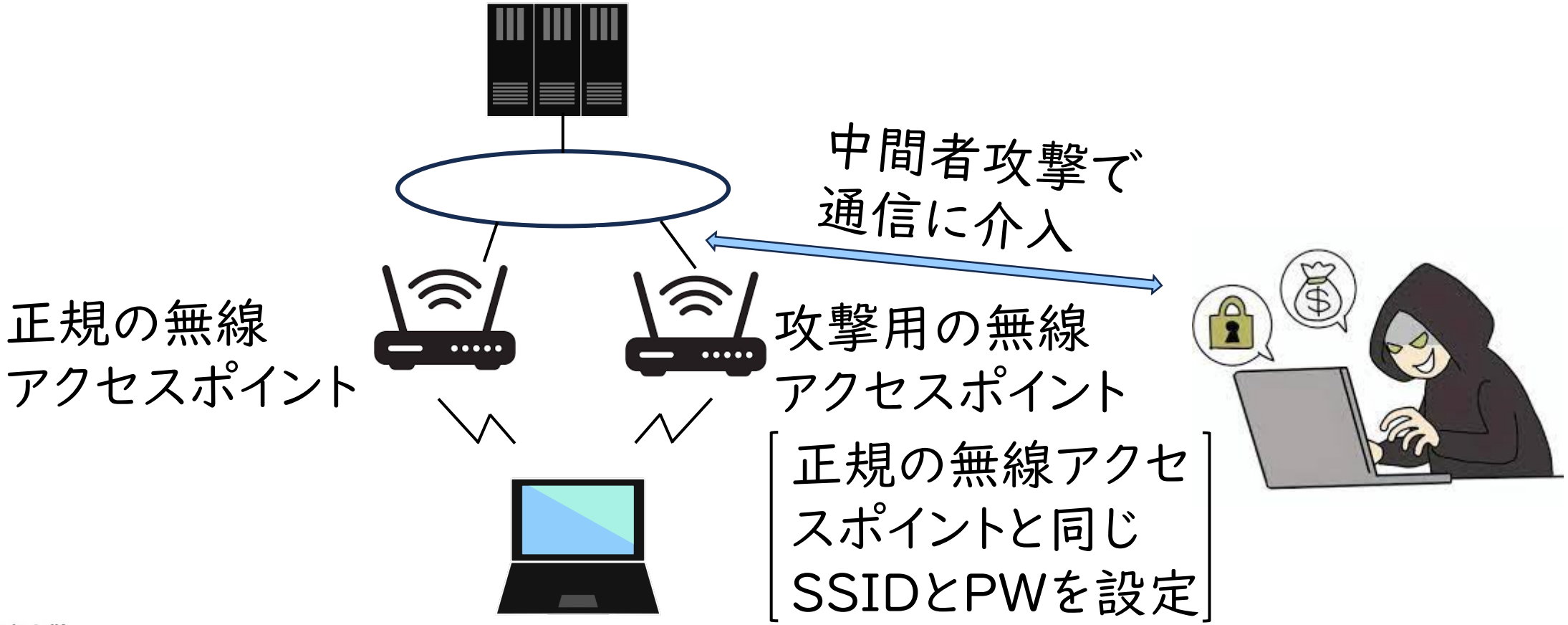
- 無線電波の傍受

  無線LANの電波の届く範囲にいる攻撃者は，無線LANのMACフレームを容易に傍受することができます．通信が暗号化されていないと，内容を盗聴されます．



- **無線アクセスポイントのなりすまし**

  公衆無線LANにおいて，攻撃用の無線アクセスポイントを設置する攻撃です．利用者のPCやスマホがそれと接続してしまうと，中間者攻撃によって，通信内容を盗聴されたり改ざんされたりするリスクがあります．



1.3 なりすましと不正アクセス

① ブルートフォース攻撃（総当たり攻撃）

ブルートフォース攻撃は，パスワードや暗号鍵，暗証番号などの秘密情報に対して，考えられるすべての組合せを試行することによって秘密情報を解読，あるいは，システムに不正ログインする攻撃です．

例えば，攻撃対象の利用者IDが判明している場合で，パスワードが英字8文字の場合には，以下のように試行します．

利用者ID	パスワード
user1001	aaaaaaaa
user1001	aaaaaaab
user1001	aaaaaaac
user1001	aaaaaaad
⋮	⋮

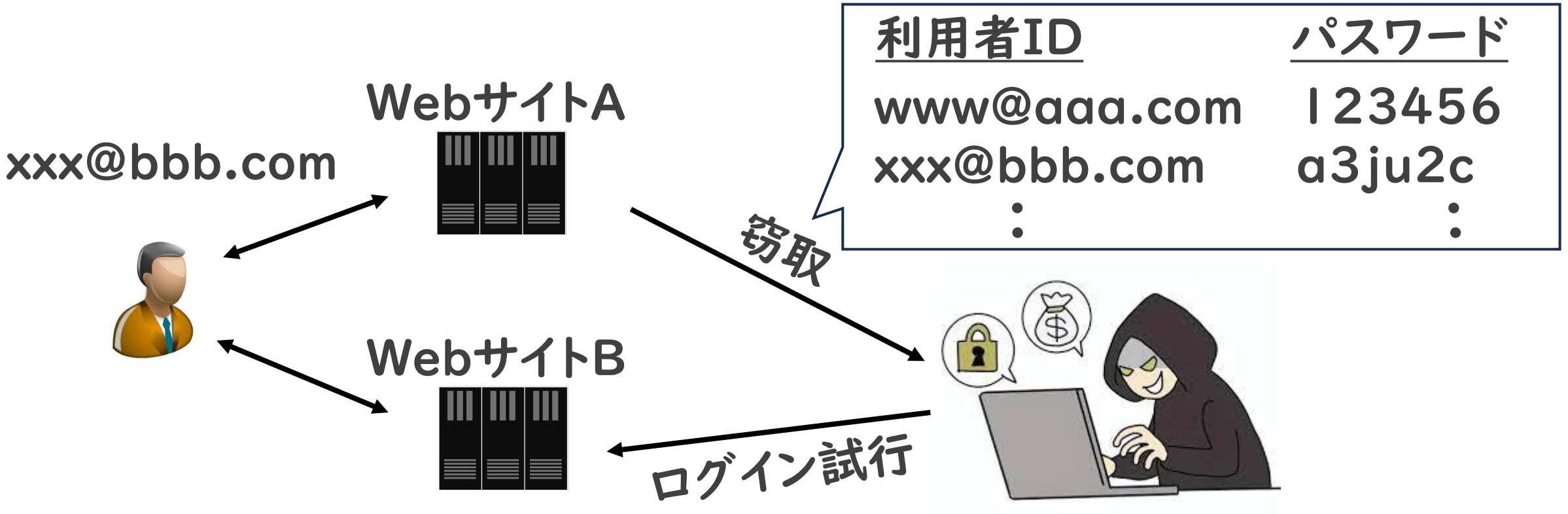
② 辞書攻撃

辞書攻撃は，利用者IDとパスワードとして使われそうな文字列を収録した辞書を使って試行する攻撃です．数万～数千万語程度を収録した辞書が流通しており，辞書に登録されているパスワードが使用されていると，少ない平均試行回数で不正ログインが成功します．辞書攻撃の例を以下に示します．

利用者ID	パスワード
user1001	123456
user1001	admin
user1001	password
user1001	qwerty
：	：

③ パスワードリスト攻撃（リスト型攻撃）

パスワードリスト攻撃は，Webサイトで使用されている実在する利用者IDとパスワードの組みのリストを用いて，他のWebサイトへ不正ログインする攻撃です．二つのWebサイトの利用者が，同じ利用者IDと同じパスワードを使い回している場合に不正ログインが成功します．



④ リプレイ攻撃（再使用攻撃）

リプレイ攻撃は，通信を盗聴して入手した情報を，そのまま再使用して不正アクセスを試行する攻撃です．例えば，最初のログインをリプレイ攻撃して，セッションIDを窃取し，それを再使用して他人のセッションを乗っ取ります．

1.4 Web利用による被害の可能性

① Webページを閲覧しただけで不正なプログラムに感染してしまう

Webサーバ自体がウイルスに感染していたり，悪意のある者によってWebページにウイルスやスパイウェアなどの不正なプログラムが仕込まれているケースです．ブラウザの設定が勝手に変更されてしまうこともあります．

② リンクをクリックしただけで不正な請求をされる，個人情報が盗まれる

ワンクリック請求の典型的な例です．また，悪意のある者がクロスサイトスクリプティング攻撃を仕掛けていると，クリックしたユーザのCookieが盗まれることにより，なりすましなどの被害に遭います．

③ 不正なプログラムを誤ってダウンロードしてしまう

Webサイトに置かれている一見役に立ちそうなプログラムが，実は不正なプログラム（ウイルス，スパイウェアなど）だったというケースがあります．

1.5 電子メール利用による被害の可能性

① スパムメール

宣伝や勧誘目的で大量に送られてくる迷惑なメールです．現状では根本的な対策はありませんが，スパムフィルタを利用する，スパムメールは開かずにすぐに削除する，などの方法で対処します．また，掲示板やブログなどの不特定多数の人に公開される場所には，メールアドレスを書き込まないようにします．

② マルウェアによる感染

ウイルス，スパイウェア，ボットなどの悪意のあるプログラムをマルウェアといいます．マルウェアは，多くの場合，メールの添付ファイルを利用して感染を拡大します．そのため，添付ファイルの取り扱いには特に注意が必要です．

③ フィッシングメール

メールを使ったフィッシングサイトへの誘導が増えています．不審なメールの本文中にあるリンクを絶対にクリックしない，個人情報の入力は必要最小限にとどめる，という心がけが大切です．

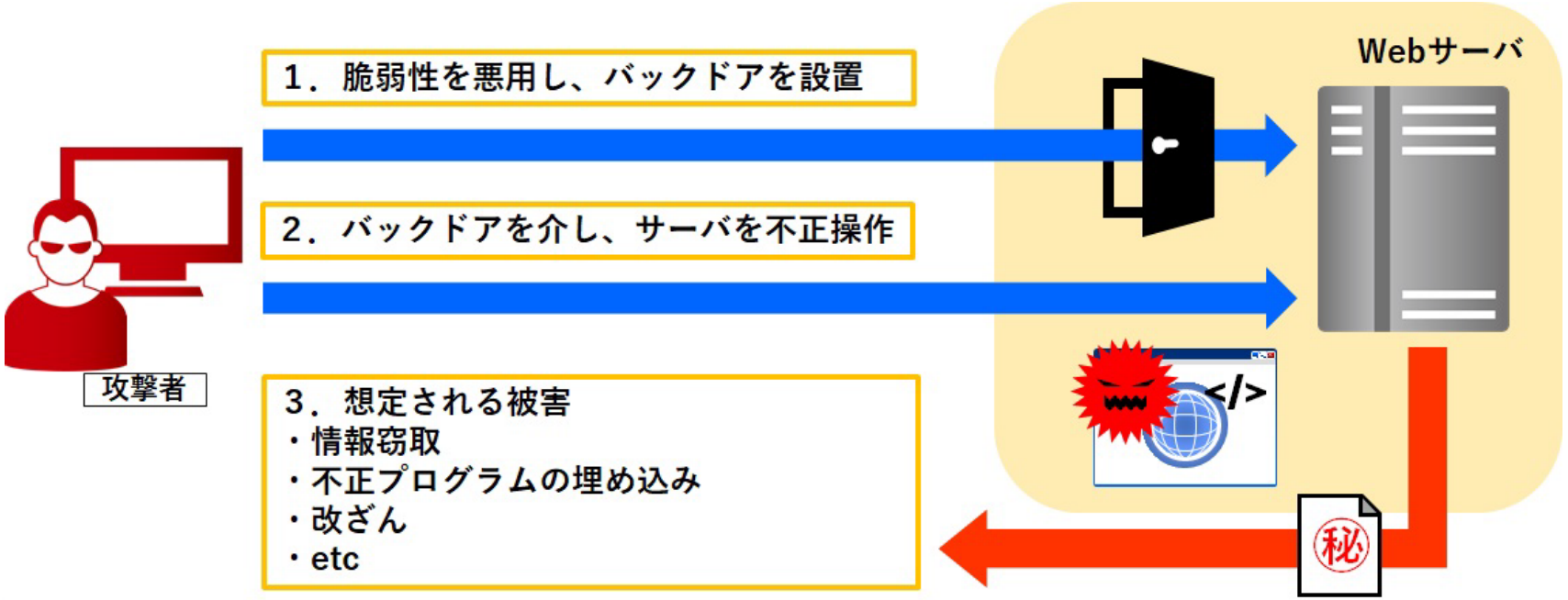
総務省　国民のためのサイバーセキュリティサイト

https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/enduser/enduser_case.html

2. 情報セキュリティにおける被害事例

2.1 事例1：狙われるWebサイト ー 正規のWebサイトでも要注意

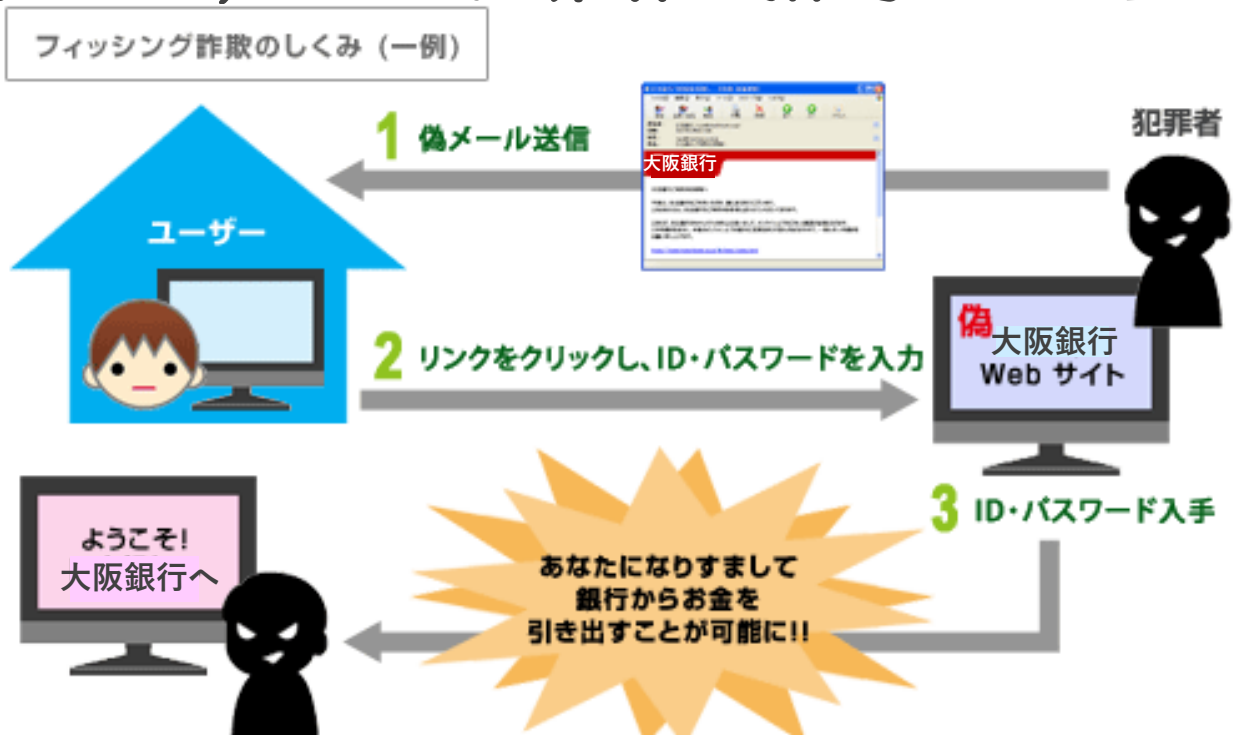
- 情報窃取
- 改ざん
- 不正プログラムの埋め込み（ダウンロードさせられる）
- 不正なWebサイトへの誘導する仕掛け など



大手，中小企業を問わなく，各種企業や組織に運営されている脆弱性のあるWebサイト

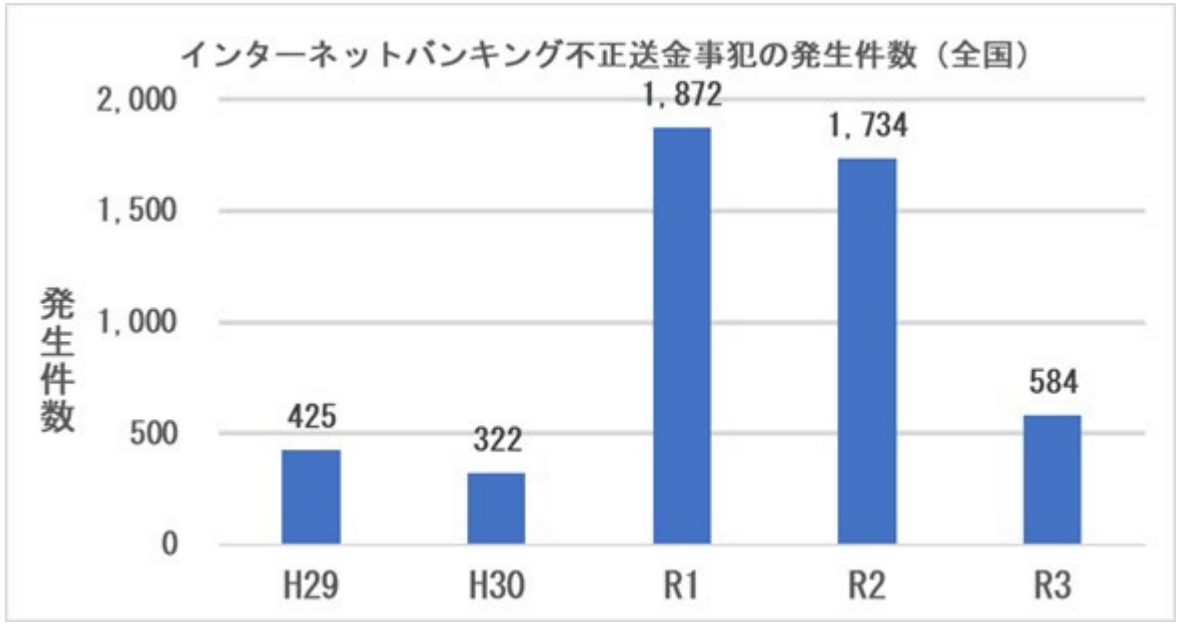
2.2 事例2：巧妙化するフィッシング詐欺 ー うっかりしているとだまされる

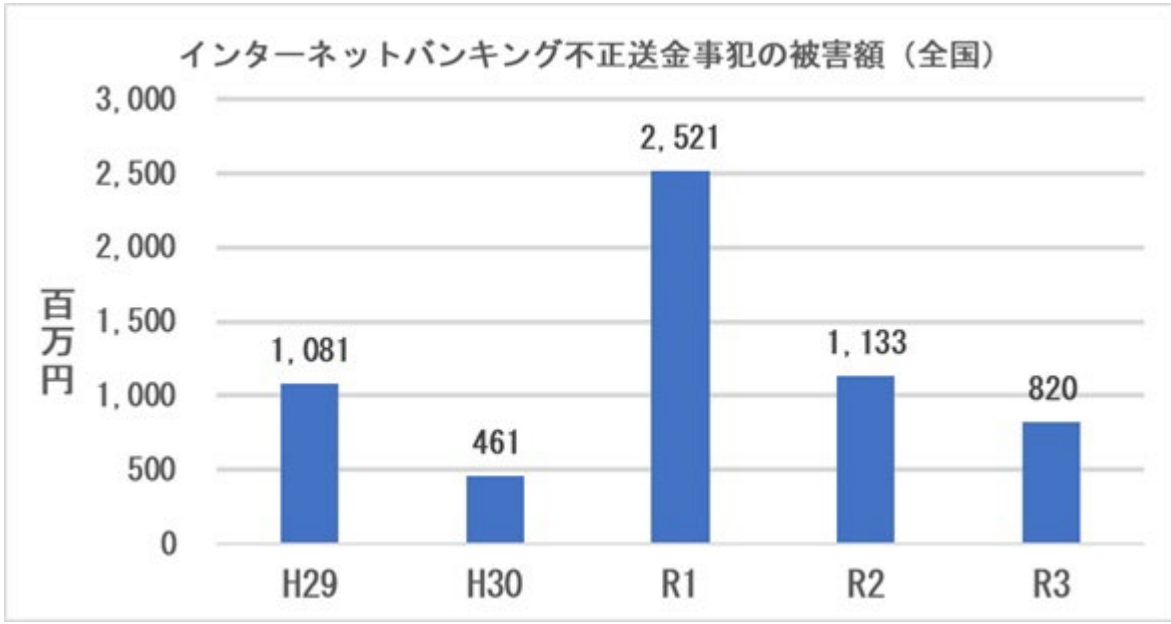
- 正規の金融機関などを装った偽メールやショートメッセージをユーザに送信.
- その中に含まれた偽のWebサイトに誘導し, 個人ID, 口座番号, クレジットカード番号, 暗証番号などの機密情報を入力させます.
- このように不正に入手した機密情報を使って正規の金融機関などでお金を引き出し, または犯罪者の指定する口座へ送金してしまいます.



2.3 事例3：増加する金融取引被害 ー 便利と危険は隣あわせ

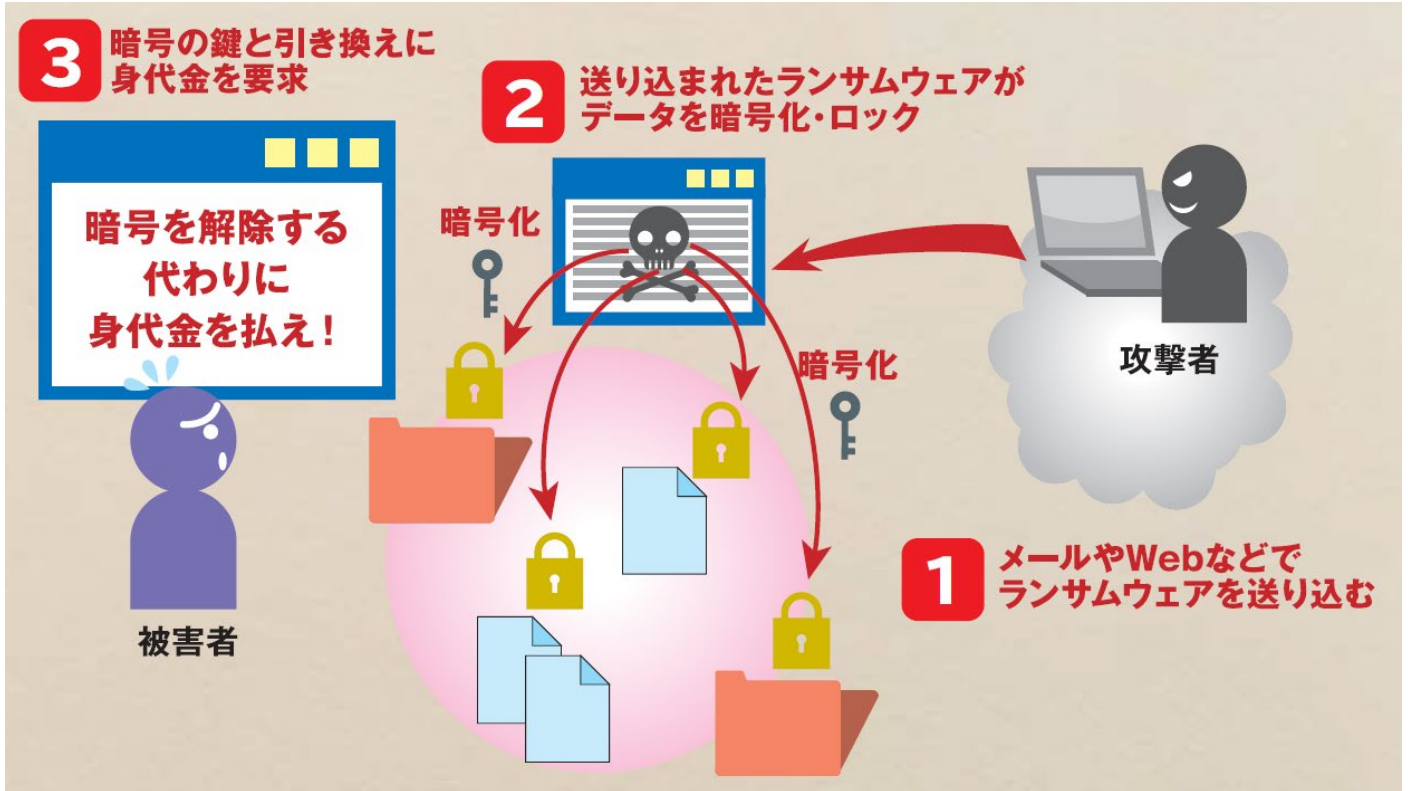
- インターネットバンキング利用者のIDとパスワードが，犯罪者や犯罪組織に取得され，銀行口座にあった預金が別口座に移されて現金が引き出されます．
- 一度被害に遭うと金銭的ダメージも大きい．





2.4 事例4：ファイルを人質に金銭要求 ー ランサムウェアによる被害

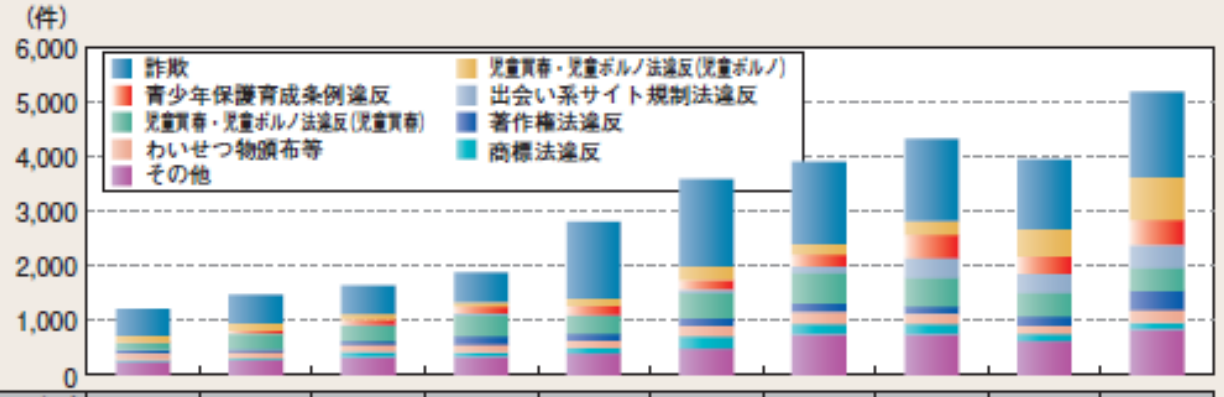
- パソコン内のファイルを勝手に暗号化し，元に戻すための情報と引き換えに金銭を要求するウイルスのことがランサムウェアと呼ばれます．
- メール送信できないなどの障害を起こすようなランサムウェアもあります．例：WannaCryおよびその亜種．



2.5 事例5：犯罪に使われるインターネット ー 共犯者募集

- 携帯サイトやインターネットの掲示板が，フィッシング詐欺，殺人の依頼，強盗や窃盗の共犯募集など悪用されました．
- 出会い系サイトやSNSで，相手の素性がわかりにくいこともあり，女性や未成年者が犯罪に巻き込まれて被害に遭ってしまいます．

警察庁　ネットワーク利用犯罪の検挙件数の推移（平成13～22年）

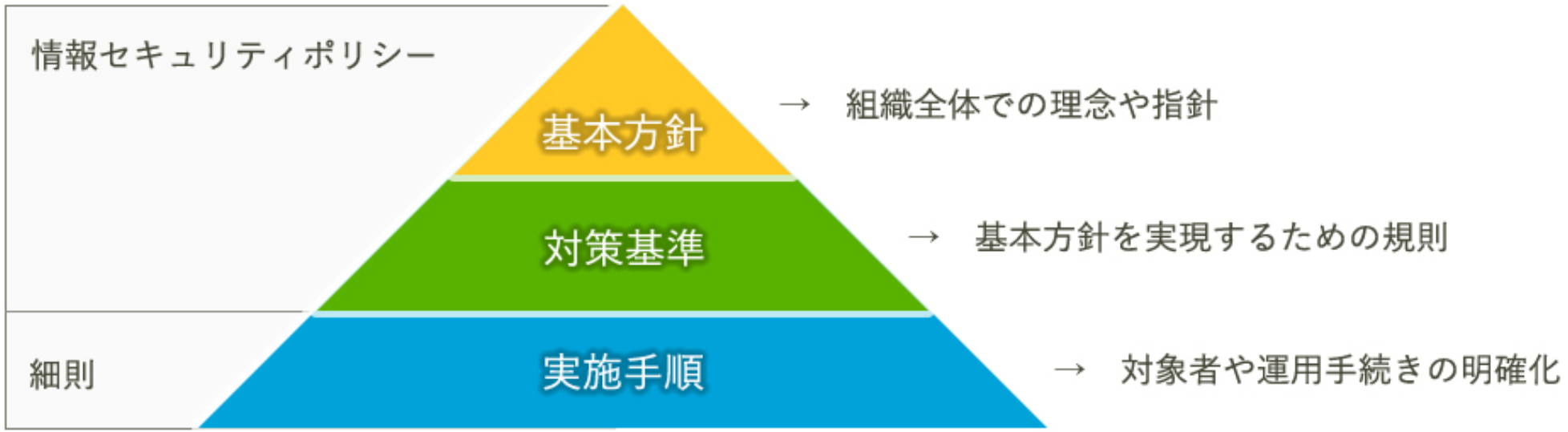


区分＼年次	13	14	15	16	17	18	19	20	21	22
合計（件）	1,209	1,471	1,649	1,884	2,811	3,593	3,918	4,334	3,961	5,199
詐欺	485	514	521	542	1,408	1,597	1,512	1,508	1,280	1,566
児童買春・児童ポルノ法違反（児童ポルノ）	128	140	102	85	136	251	192	254	507	783
青少年保護育成条例違反	10	70	120	136	174	196	230	437	326	481
出会い系サイト規制法違反	ー	ー	8	31	18	47	122	367	349	412
児童買春・児童ポルノ法違反（児童買春）	117	268	269	370	320	463	551	507	416	410
著作権法違反	86	66	87	174	128	138	165	144	188	368
わいせつ物頒布等	103	109	113	121	125	192	203	177	140	218
商標法違反	31	37	95	82	109	218	191	192	126	119
その他	249	267	334	343	393	491	752	748	629	842

3. リスクへの一般的な対処法

3. 1　情報セキュリティの基本を知ろう

- どのようなセキュリティリスクがあるのかを知ります.
- 適切な対策を行われば安心して利用できることを理解します.
- 意識+行動　が重要　（個人と組織）.

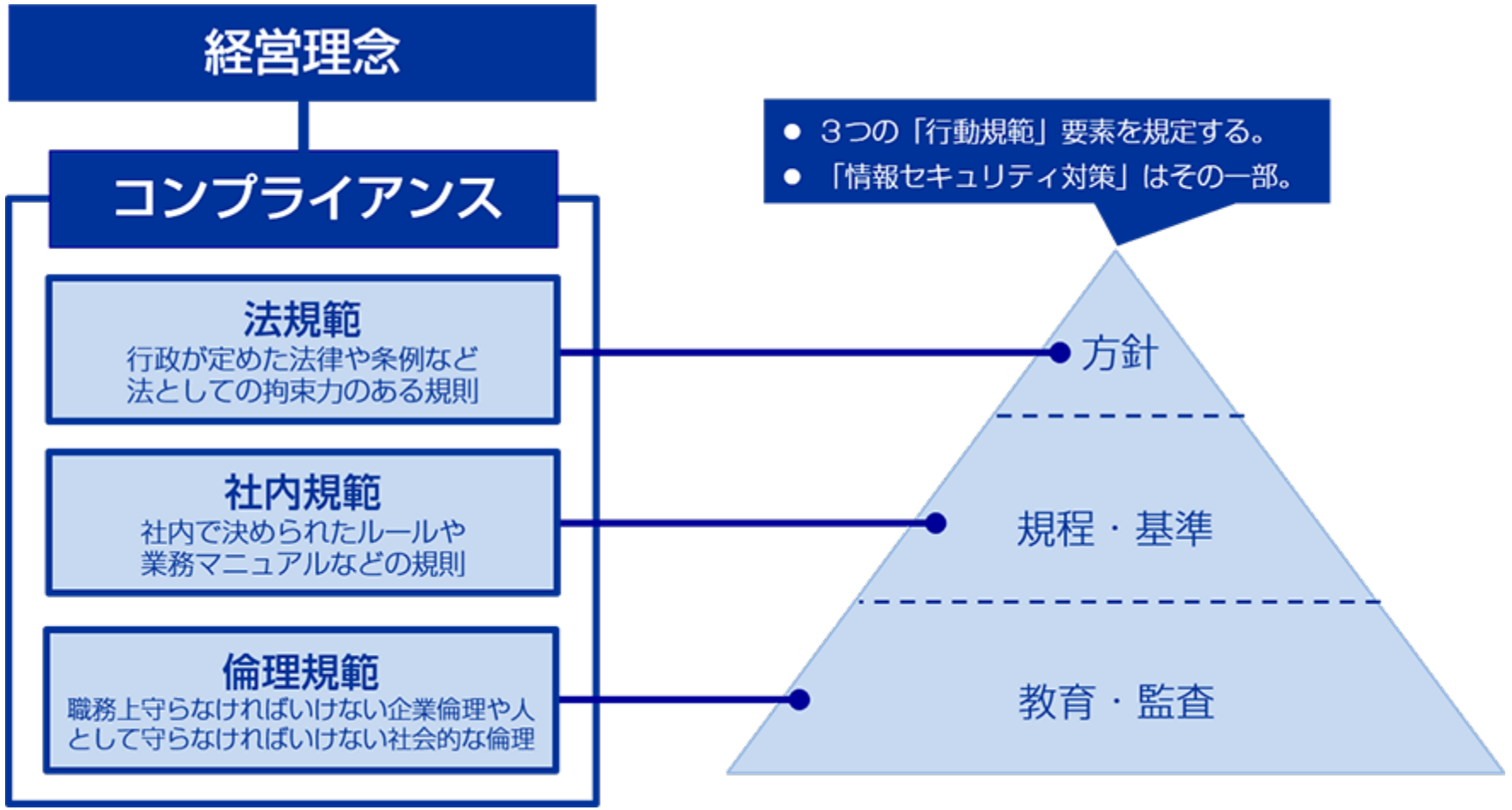


3.2 ウイルスなどの不正プログラム（マルウェア）について理解しよう

- ウイルスは猛威を振るっています（インターネット経由で増殖・拡散しやすい）.
- マルウェアは急増したり，派生したりします.

3.3 実際のセキュリティ対策を施そう

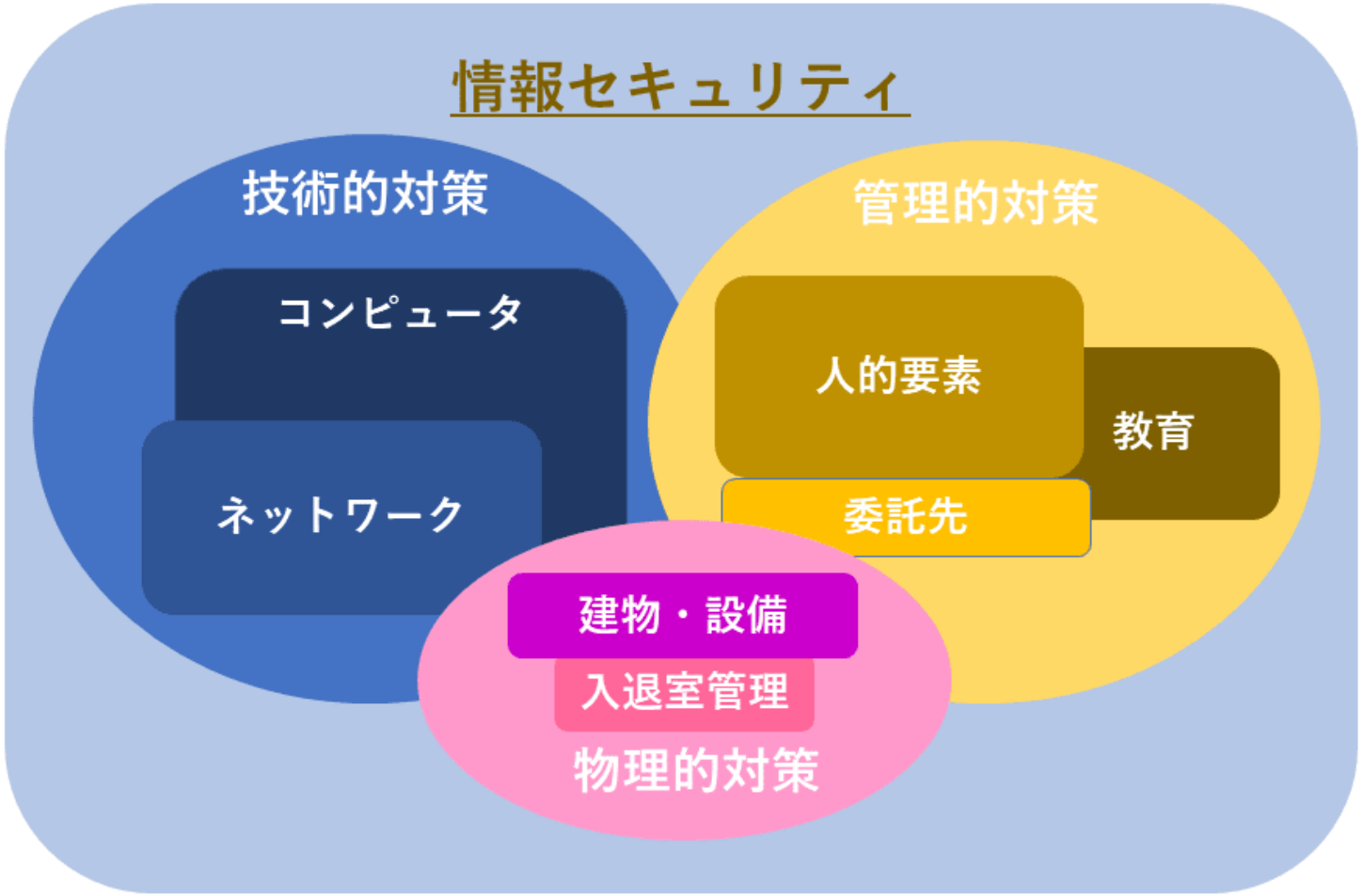
- ユーザ個人として守るべき規範があります.
- 組織内の一員として守るべき規範もあります.



3.4 情報セキュリティに使われている技術を理解しよう

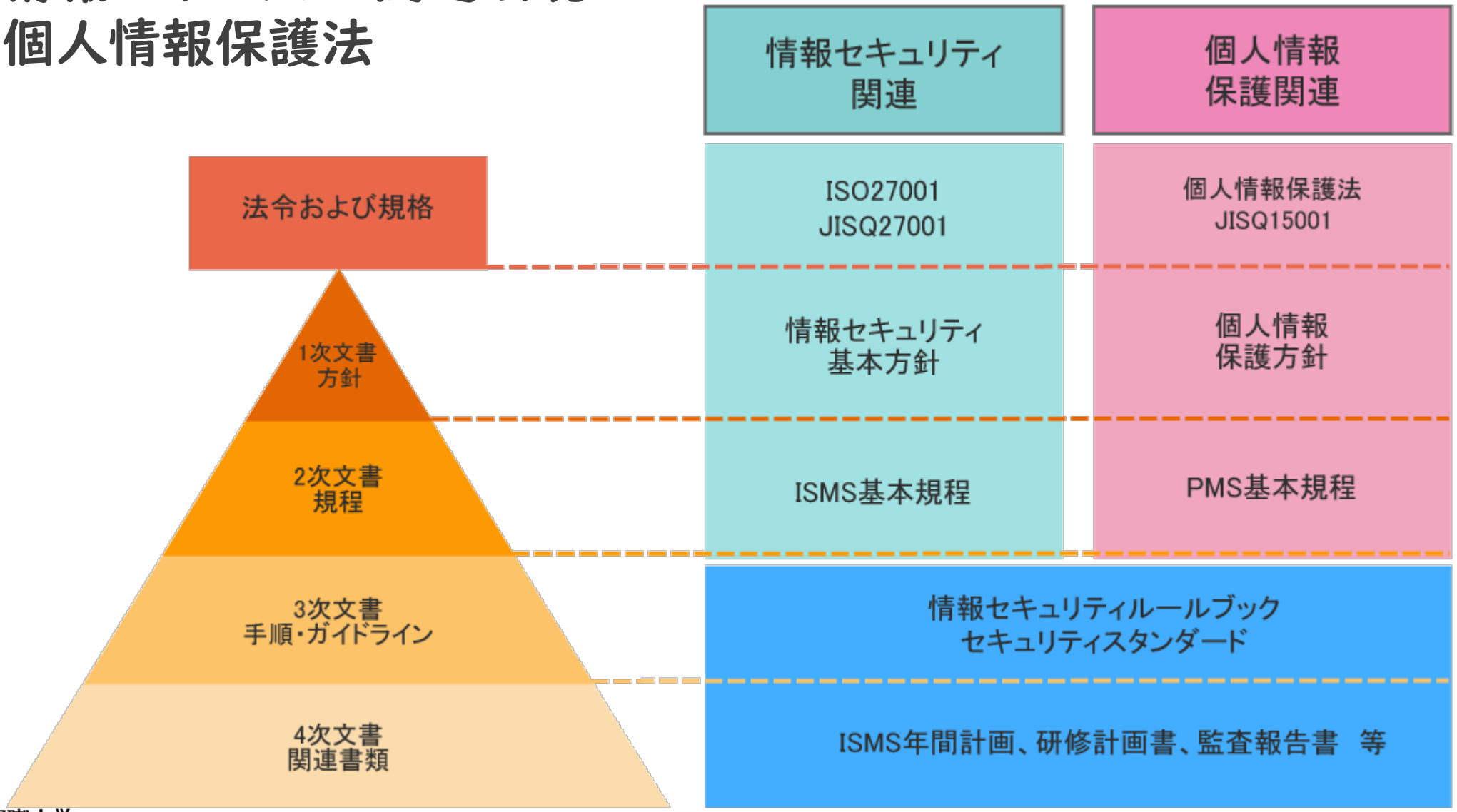
- セキュリティ対策には技術が使われます.
- 技術的対策と他の対策を合わせて実施することで良い効果が得られます.

情報セキュリティの全体イメージ



3.5 法律について認識しよう

- 情報セキュリティ関連法規
- 個人情報保護法



練習問題

授業（資料）で紹介した各種の情報セキュリティ被害に関して，リストを作り，それぞれの脅威およびその防止方法を書きなさい．