社会情報論
第Ⅱ部　情報通信技術の変化の社会事象への影響

第7回
情報格差と情報セキュリティ

担当　経営・社会情報学プログラム
教授　山本佳世子

第7回の講義の内容

1. 情報格差に関する問題

2. 情報セキュリティ問題

1-1. 情報弱者

■ 情報弱者

・様々な理由から，パソコンやインターネットをはじめとする情報・通信技術の利用に困難を抱える人

■ デジタルデバイド

・情報技術を活用できる層と情報弱者の間に社会的・経済的格差が生じ，あるいは格差が拡大していく現象

■ 2000年7月の九州・沖縄サミットではデジタルデバイドが議題にあげられ，情報弱者への支援とデジタルデバイドの克服が重要課題

1-2. 情報弱者への対応

■ 社会的階層によらずに情報技術を利用できる環境づくり

- (例1)公共の場所(例えば図書館)に誰でも自由に使える情報端末を整備
- (例2)安価もしくは無償で提供される教育機会(「IT講習会」など)
- アメリカではこうした問題に積極的に取り組むNPOが多く，行政も様々な施策を実施

■ 情報のバリアフリー化

- 視聴覚が不自由な人でもアクセスしやすいウェブサイト
- 障害をもった人たちにとって必要な情報を用意する

■ 情報へのアクセスには通信インフラの整備が重要

- 通信事業のユニバーサルサービス(全国均一のサービス)を維持したり，発展途上国の通信インフラ整備を援助する

1-3. 情報格差（デジタルデバイド）

■ コンピューターで扱うデジタル情報を持つ人と持たない人との間で生じている格差と，それによって生じる問題のこと

↑

■ 1990年代以降，先進国ではICTを当然の前提として社会システムの基盤を構築

■ これにともなって，情報機器を持たなかったり，持っていても使用できない人々には，このことが社会的な不利として働くように変化

■ 高度情報ネットワーク化が進展することにとって発生した新しい問題

・ICTを使えないために，手に入るはずの利益を逃したり，回避できるはずの損害を被ったりすること

1-4. 情報格差（デジタルデバイド）の概念の誕生

■ 1996年にテネシー州ノックスビルで行われた演説でのアル・ゴア（当時のアメリカ合衆国副大統領）の発言

・「情報スーパーハイウェイ構想」を2000年までにアメリカ全土の都市部から郊外・農村部に至るまで隅々に網羅させる予定

・将来の子孫達に「デジタルデバイド」によって区切られることがない世界を作りたいと演説の中に織り込む

■ これに続く形で当時の大統領であるビル・クリントンがゴアの発言で使用された「デジタルデバイド」という言葉を引用

・人々が技術を開発し知識を共有しないことは，不平等や摩擦，不安を生む切っ掛けとなるため，それらの課題に一丸となって取り組む必要

1-5. 情報格差の拡大

■ 国内デジタルデバイド

・ビジネス・デバイド（企業規模格差）とソシアル・デバイド（経済，地域，人種，教育等による格差）に分けることができる

・国内デジタル・デバイド発生の主要因

アクセス（インターネット接続料金，パソコン価格等）と知識（情報リテラシー等）と言われているが，動機も大きな要因では？

■ 国際間デバイド

・国内の問題にとどまらず，発展途上国と先進国の間の格差問題として顕在化

・情報環境が整備されていない国が，市場競争で遅れをとる「南北の格差」をさらに拡大する危惧も生じる

1-6. 情報格差の解決方法

■ インフラ面の整備

・インターネットなどのメディアの情報の流れの構造を整備することで，情報の流れを必要に応じてスムーズに流すようにする

■ コンテンツ面の整備

・情報の表現方法のことを指し，アクセシビリティやユニバーサルデザインなどを含めて，情報の伝播の障壁を取り除くようにする

■ 格差を埋めるためのサポート面の整備

・情報強者が情報弱者を救済すること
・インクルーシブデザインなどの手法で，両者にとってもメリットのある情報環境をデザイン
・アフォーダンスな手法で，全ての人に情報が自然な形で行き渡るような情報環境をデザインする

1-7. 東日本大震災におけるデジタルデバイド

■ 様々な格差の存在

・被害格差，経済格差，復興格差などに加えて情報格差

■ 東日本大震災における情報格差

・個々人の情報入手／利用環境の状況に付随する情報環境の格差

・多様なメディアで取り上げられる／関心を持たれる情報・トピックスを巡る格差　→支援の多少にもつながる

■ 震災・原発事故を巡る情報格差

・ソーシャルメディアの利用の有無で拡大

■ 情報環境の脆弱性による情報格差

■ さらに正常性バイアスの影響で被害が拡大の可能性

1-8. 災害弱者≒情報弱者か？

■ 被災地のもともとの状況
・高齢化，貧困，様々な格差などの従来からの社会問題が内在

■ 東日本大震災による格差
・被害格差，経済格差，情報格差

■ 社会的な弱者が災害弱者になり，さらにデジタルデバイドのおかげで情報弱者にもなってしまった
←情報環境の格差のために，情報発信者，情報受信者（情報受益者）にもなることができなかった

1-9. わが国のデジタルに不慣れな高齢者への対策

■ 総務省　デジタル活用支援推進事業

・新型コロナウイルス感染症の拡大の影響
・「人と接触を避ける」非対面での行政手続きが必要であるが，「電子申請でできること自体を知らない」「電子申請の使い方が複雑」等の理由により，オンラインによる行政手続きの利用が浸透していない

■ 各自治体独自の取り組み

・東京都渋谷区では高齢者3,000人を対象にスマートフォンを貸与
・携帯電話各社等と連携し，スマートフォン教室の開催

1-9. 諸外国のデジタルに不慣れな高齢者への対策

■ 中国

・世界最大規模のネットワーク網
・貧困層の住む農村部との情報格差解消に向け，インフラ整備に加えて通信料を50%削減
・高齢者や障がい者に重点をおいた通信料金引き下げ

■ アメリカ

・2015年から低所得者層を対象とした情報格差解消の取り組み「コネクトホーム」を開始
・対象となる公共住宅に安価なブロードバンドアクセスを提供
・民間企業が「インターネット・エッセンシャルズ」という独自のプログラムを継続し，低所得家庭の子どもにインターネット環境の整備や通信機器の無償提供，デジタルリテラシー教育などのサポートを実施

2-1. 情報セキュリティの定義

- JISQ27002(ISO/IEC27002)によって，情報の機密性，完全性および可用性を維持することと定義
- さらに，真正性，責任追跡性，否認防止および信頼性のような特性を維持することを含めてもよい

■ 機密性 (confidentiality)

・情報へのアクセスを認められた者だけが，その情報にアクセスできる状態を確保すること

■ 完全性 (integrity)

・情報が破壊，改ざん又は消去されていない状態を確保すること

■ 可用性 (availability)

・情報へのアクセスを認められた者が，必要時に中断することなく，情報及び関連資産にアクセスできる状態を確保すること

2-2. 情報セキュリティ10大脅威（個人2024年）

順位	「個人」向け脅威（五十音順）	初選出年	10大脅威での取り扱い（2016年以降）
1	インターネット上のサービスからの個人情報の窃取	2016年	5年連続8回目
2	インターネット上のサービスへの不正ログイン	2016年	9年連続9回目
3	クレジットカード情報の不正利用	2016年	9年連続9回目
4	スマホ決済の不正利用	2020年	5年連続5回目
5	偽警告によるインターネット詐欺	2020年	5年連続5回目
6	ネット上の誹謗・中傷・デマ	2016年	9年連続9回目
7	フィッシングによる個人情報等の詐取	2019年	6年連続6回目
8	不正アプリによるスマートフォン利用者への被害	2016年	9年連続9回目
9	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	2019年	6年連続6回目
10	ワンクリック請求等の不当請求による金銭被害	2016年	2年連続4回目

情報処理推進機構調査

2-3. 情報セキュリティ10大脅威（個人2024年）

順位	「個人」向け脅威（五十音順）	初選出年	10大脅威での取り扱い（2016年以降）
1	ランサムウェアによる被害	2016年	9年連続9回目
2	サプライチェーンの弱点を悪用した攻撃	2019年	6年連続6回目
3	内部不正による情報漏えい等の被害	2016年	9年連続9回目
4	標的型攻撃による機密情報の窃取	2016年	9年連続9回目
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	3年連続3回目
6	不注意による情報漏えい等の被害	2016年	6年連続7回目
7	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目
8	ビジネスメール詐欺による金銭被害	2018年	7年連続7回目
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	4年連続4回目
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017年	2年連続4回目

情報処理推進機構調査

2-4. サイバー攻撃

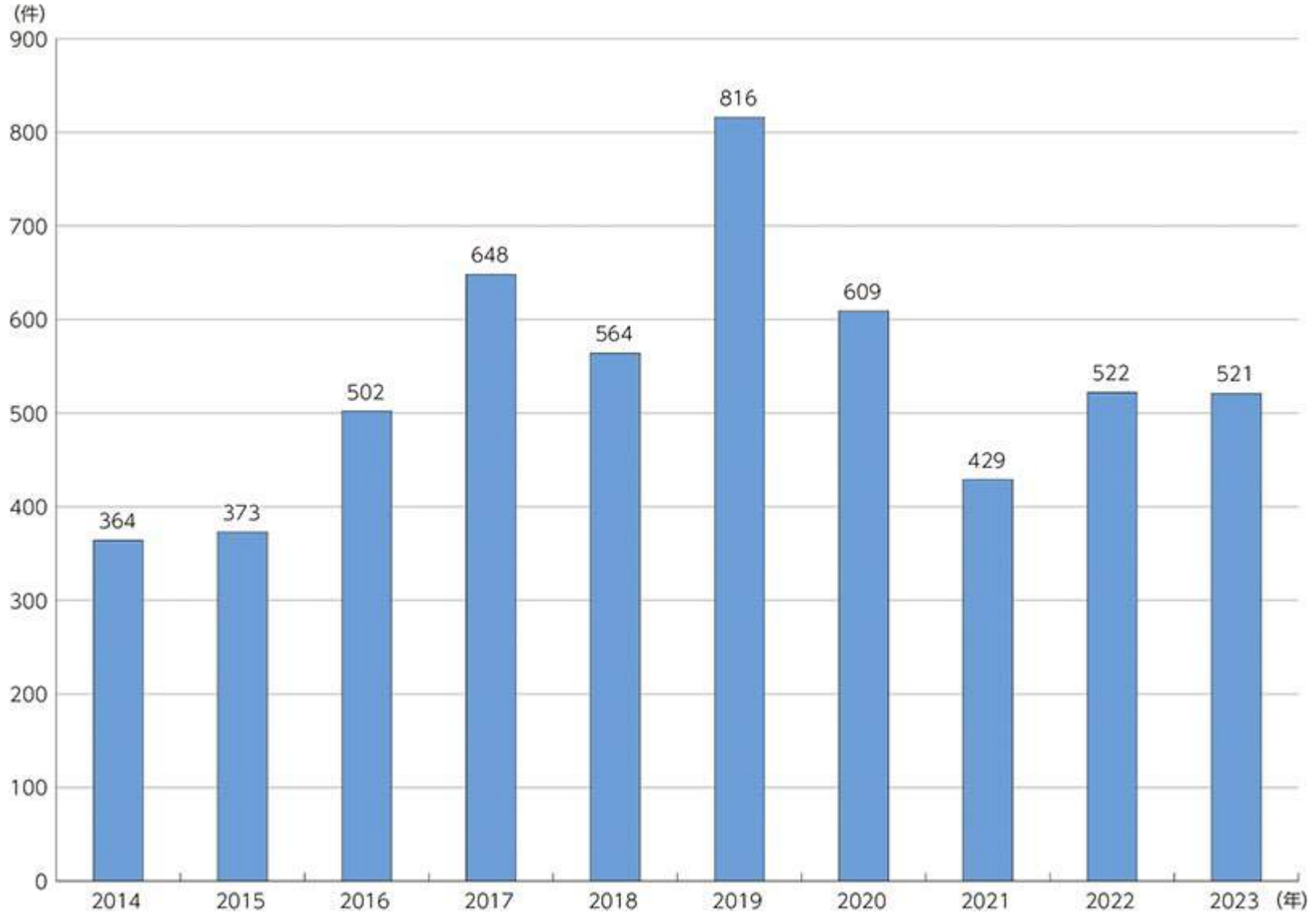
■ ネットワーク経由の情報セキュリティ事象の一つ
・国や企業の機密情報等を窃取すること，重要なデータやシステムを破壊することが目的
・2012年度中に合計1,009件の標的型メールが国内の民間事業者等に送付されたことで注目

■ 不正侵入，情報の窃取や改竄，破壊，情報システムの作動停止や誤作動，不正プログラムの実行，DDos攻撃など

■ 世界規模で標的型攻撃に外国政府の関与が疑われている問題も顕在化
・グローバルなサプライチェーン等の場合には，1つの点への攻撃が他の拠点へも影響することが危惧される

■ 2017年5月　ランサム（身代金）ウェア　「ワナクライ（WannaCry）」
・マルウェアの一種
・感染したコンピュータは利用者がシステムへのアクセスを制限され，制限解除のために身代金を支払うよう要求

2-4. 不正アクセス禁止法違反事件検挙件数の推移



総務省「令和6年度版情報通信白書」

2-5. 情報セキュリティ対策

■ 情報処理推進機構による情報セキュリティ対策の提案

- 日常における情報セキュリティ対策
- 長期休暇における情報セキュリティ対策
- ウイルス対策
- 不正アクセス対策
- 脆弱性対策
- 標的型サイバー攻撃対策
- IoT対策
- 制御システム対策

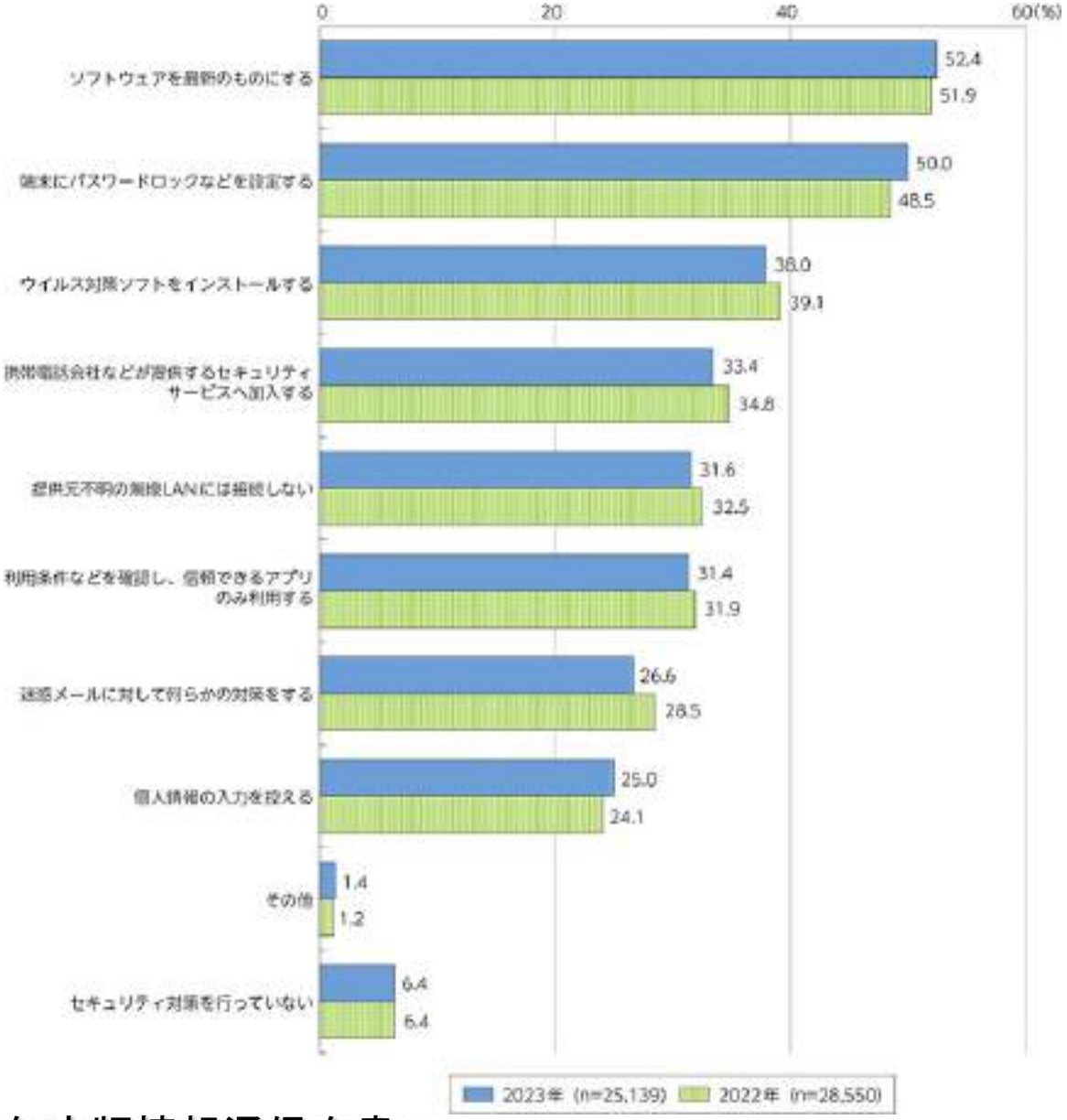
2-6. わが国のサイバーセキュリティ対策

■ 国レベル
・CYMAT（Cyber Incident Mobile Assistant）設立（2012年）

■ 情報処理推進機構
・サイバー情報共有イニシアティブ（J-CSIP（ジェイシップ））
（2012年）
・サイバーレスキュー隊J-CRAT（ジェイ・クラート）（2014年）

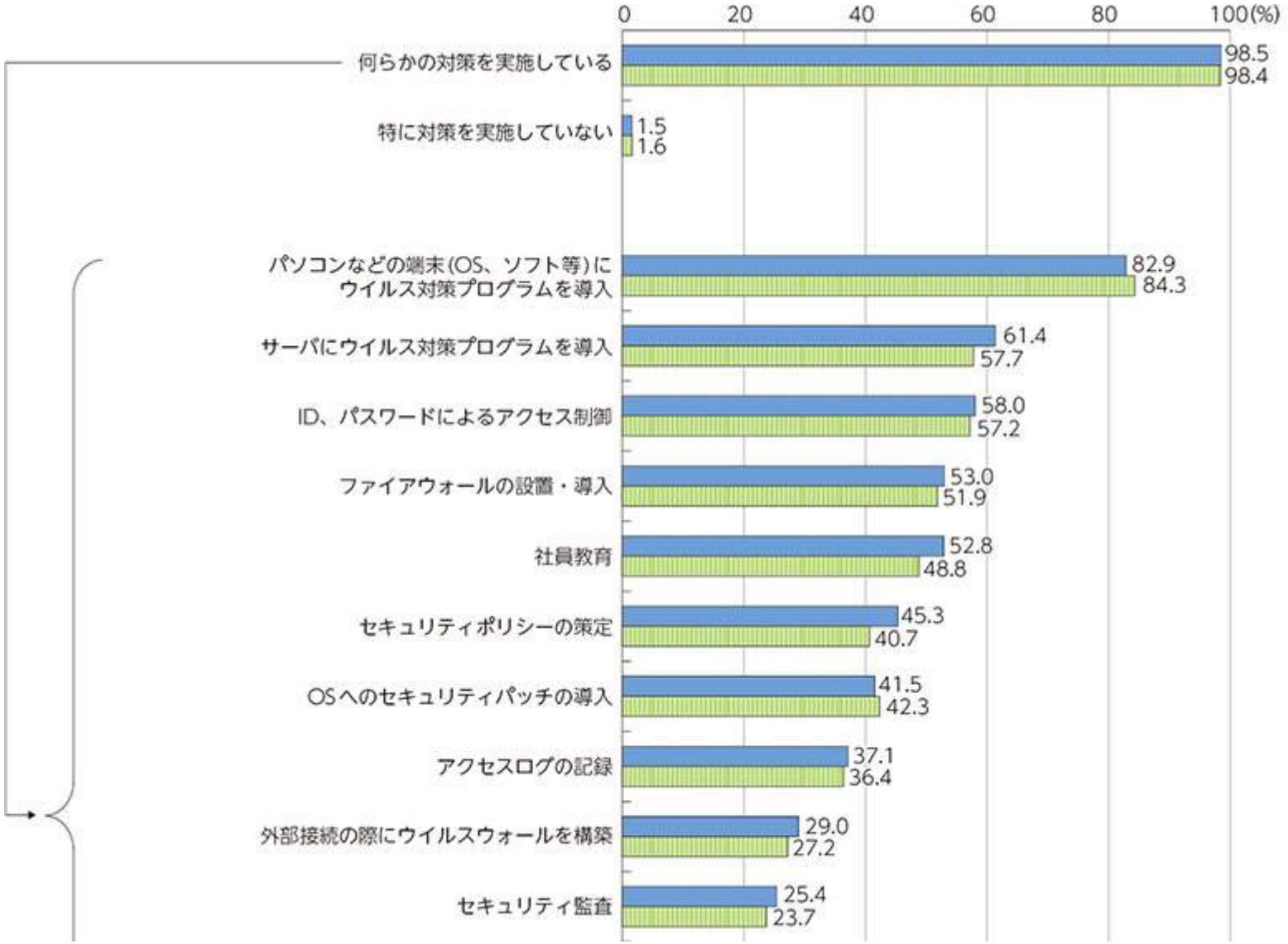
■ 中小企業や情報セキュリティの関係団体
・SECURITY ACTION（2017年）
中小企業の情報セキュリティ対策普及の加速化に向けた共同宣言に基づく

2-7. 個人の情報セキュリティ対策の実施状況



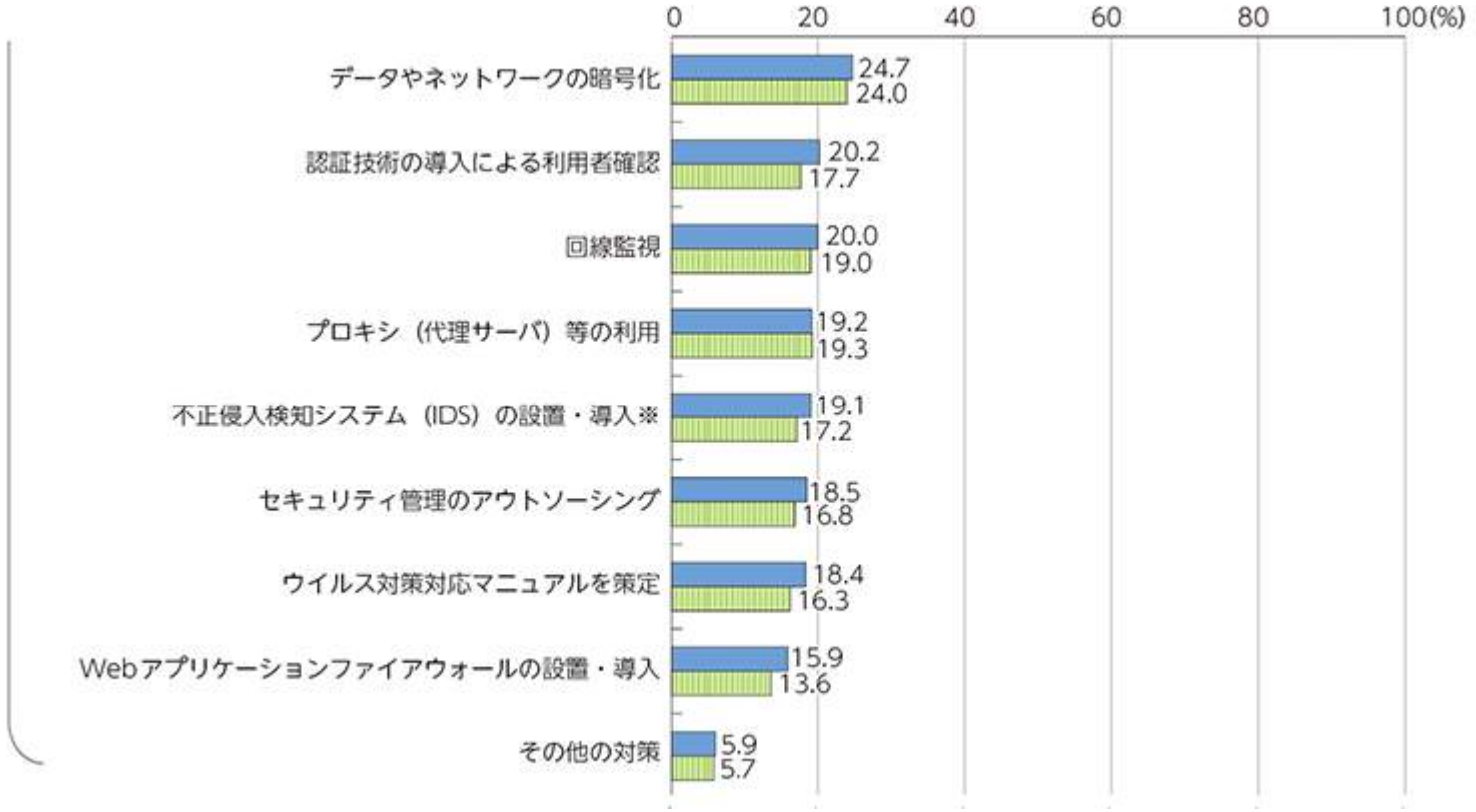
総務省「令和6年度版情報通信白書」

2-8. 企業の情報セキュリティ対策の実施状況(1)



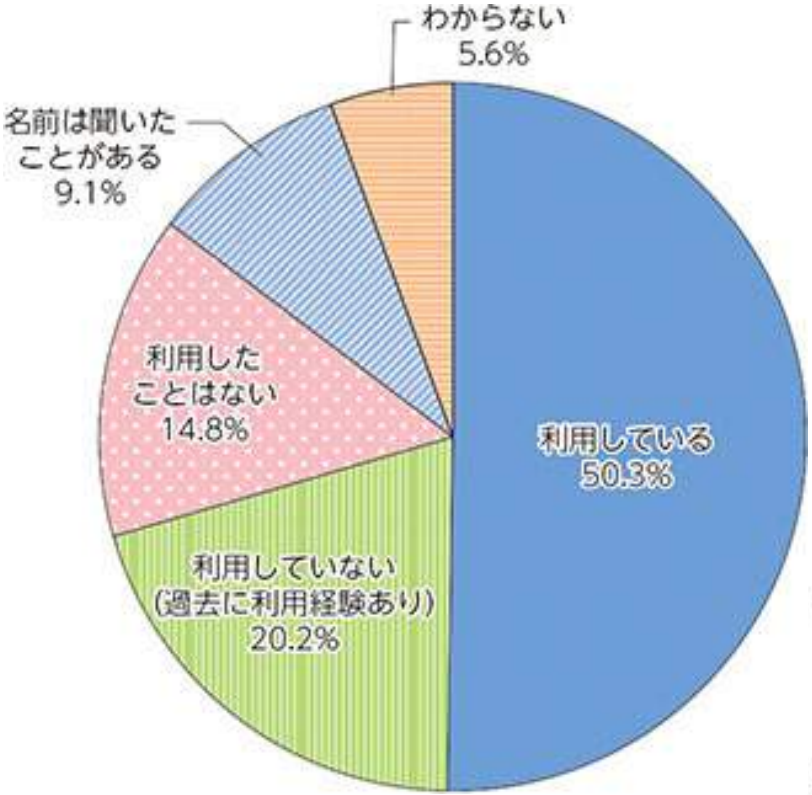
総務省「令和6年度版情報通信白書」

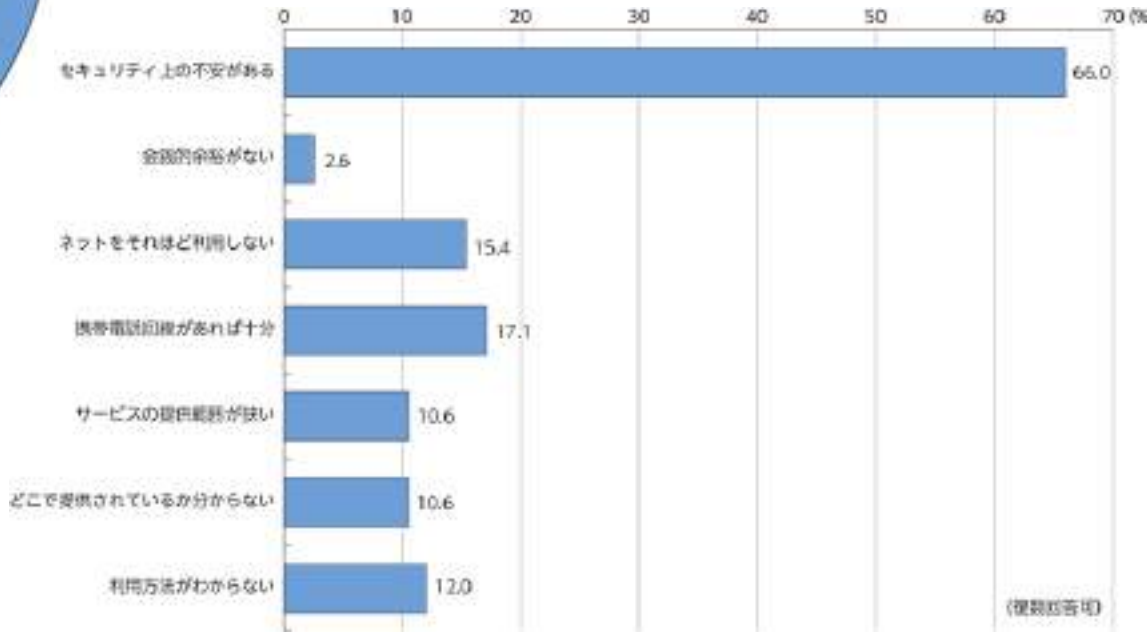
2-9. 企業の情報セキュリティ対策の実施状況(2)



総務省「令和6年度版情報通信白書」

2-10. 公衆無線LANの利用の有無と利用していない理由





総務省「令和6年度版情報通信白書」

2-11. サイバーセキュリティに関する問題が引き起こす経済的損失

調査・分析の実施主体	対象地域	対象期間	経済的損失の概要	損失額
トレンドマイクロ	日本	2023年【調査時期】	過去3年間でのサイバー攻撃の被害を経験した法人組織の累計被害額の平均	1億2,528万円
警察庁	日本	2023年上半期	ランサムウェア被害に関連して要した調査・復旧費用の総額	26%が100万円未満 19%が100万~500万円未満 25%が500万~1,000万円未満 23%が1,000万~5,000万円未満 8%が5,000万円以上
FBI	米国	2022年	サイバー犯罪事件による被害報告総額	102億ドル
NFIB	英国	2023年	サイバー犯罪による被害報告総額	560万ポンド
Sophos	世界14か国	2023年	直近のランサムウェア攻撃の修復に要した1組織あたりの年間平均コスト	182万ドル
IBM	世界16か国	2023年	組織における1回のデータ侵害にかかる世界平均コスト	445万ドル
Cybersecurity Ventures	世界	2025年【予測】	サイバー犯罪によるコスト	10兆5,000億ドル
Fastl	北米、欧州、アジア、太平洋地域	2023年	サイバー攻撃を受けた企業の損失	過去12ヶ月間収益の9%

総務省「令和6年度版情報通信白書」