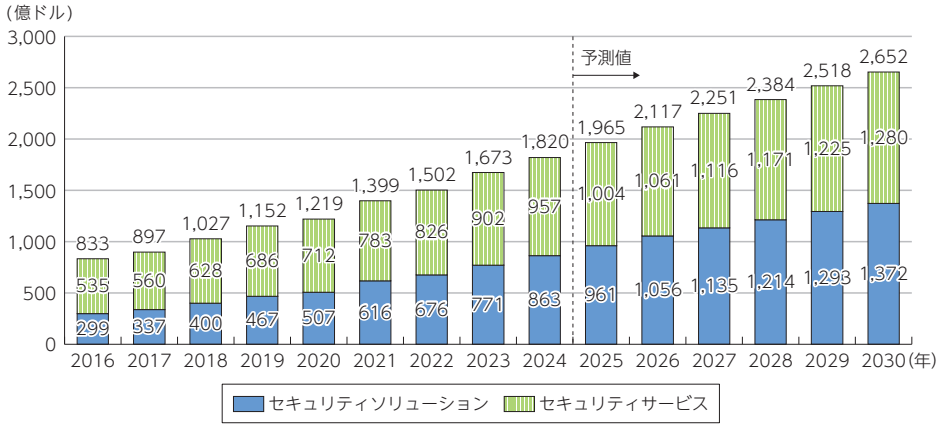
第10節　サイバーセキュリティの動向

1　市場の概況

世界のサイバーセキュリティの市場（売上高）は引き続き堅調で、2024年には前年同期比8.8%増加の1,820億ドルとなっている（図表Ⅱ-1-10-1）。

図表Ⅱ-1-10-1　世界のサイバーセキュリティ市場規模の推移



（出典）Statista（2026年2月10日取得データ）を基に作成*1

サイバーセキュリティ主要事業者の市場シェアについて、セキュリティアプライアンス市場におけるベンダー別シェアの推移を見ると、Palo Alto Networksは、2022年第4四半期の16.6%から2024年第2四半期には22.4%へとシェアを拡大し、首位となっている。同社は、次世代ファイアウォールを中心としたプラットフォーム戦略や、クラウドセキュリティ分野への積極的な事業展開が奏功したものと見られる。Fortinetも20%前後のシェアを占めており、上位2社がセキュリティアプライアンス市場を牽引する構図となっている。

関連データ　世界のサイバーセキュリティ主要事業者のシェア

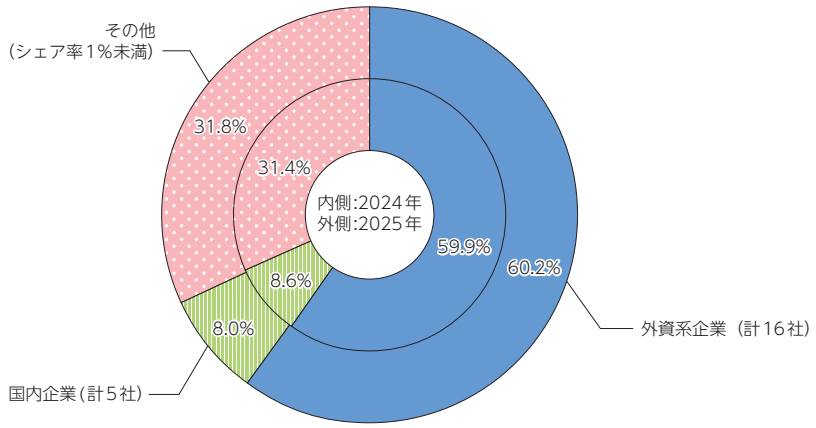
出典：Statista（IDC）（2026年2月10日取得データ）を基に作成
URL：https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r08/html/datashu.html#f00265（データ集）

2025年の国内の情報セキュリティ製品市場の市場規模（売上額ベース）は、前年比13.8%増の7,434億3,900万円となった。

また、2024年及び2025年の国内情報セキュリティ製品のベンダー別シェア（売上額）について、市場全体のシェア率が1%以上の企業を「外資系企業」と「国内企業」に分類し、それら企業における2024年及び2025年の売上額を集計した結果、ともに外資系企業のシェアが6割程度を占めており、国内のサイバーセキュリティ製品はその多くを海外に依存している状況が引き続いているといえる（図表Ⅱ-1-10-2）。

＊1　https://www.statista.com/outlook/tmo/cybersecurity/worldwide

図表Ⅱ-1-10-2　国内情報セキュリティ製品市場シェア（売上額）　2024～2025年



（出典）IDC Japan, 2026年5月「国内情報セキュリティ製品市場シェア、2025年：アイデンティティ／アクセス管理が鍵となるセキュリティ製品市場」（JPJ53501926）を基に作成

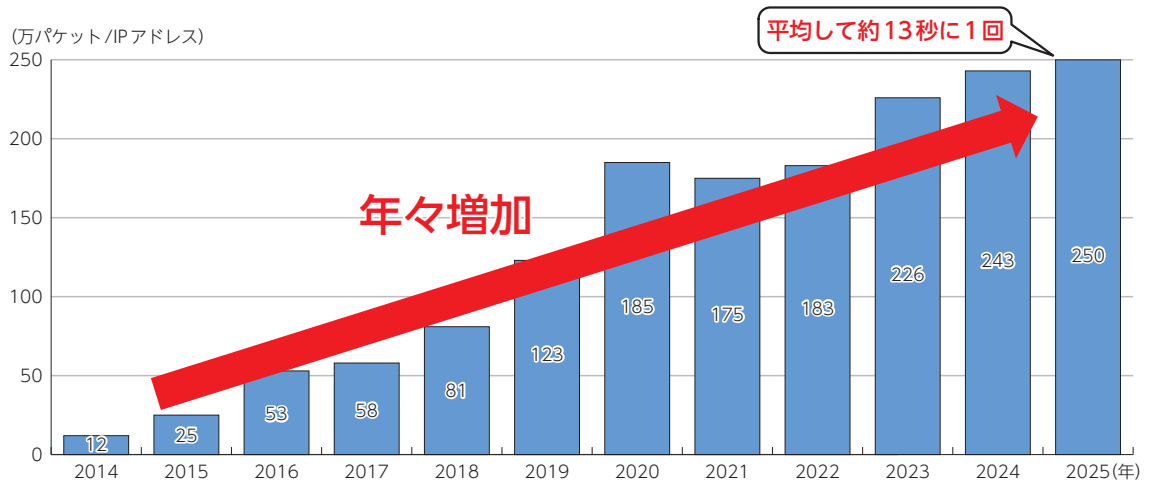
2　サイバーセキュリティの現状

1　サイバーセキュリティ上の脅威の増大

NICTが運用している大規模サイバー攻撃観測網（NICTER）のダークネット観測で確認された2025年の1IPアドレス当たりの観測パケット数（約250万パケット）は、2015年（約25万パケット）と比較して10倍となっているなど、依然多くの観測パケットが届いている状態である（図表Ⅱ-1-10-3）。また、2025年の総観測パケット数は各IPアドレスに対して約13秒に1回観測されたことに相当する。

なお、2025年は過去最高の観測数を記録しており、インターネット上を飛び交う観測パケットは2024年と比較して更に活発化している状況であるといえる。

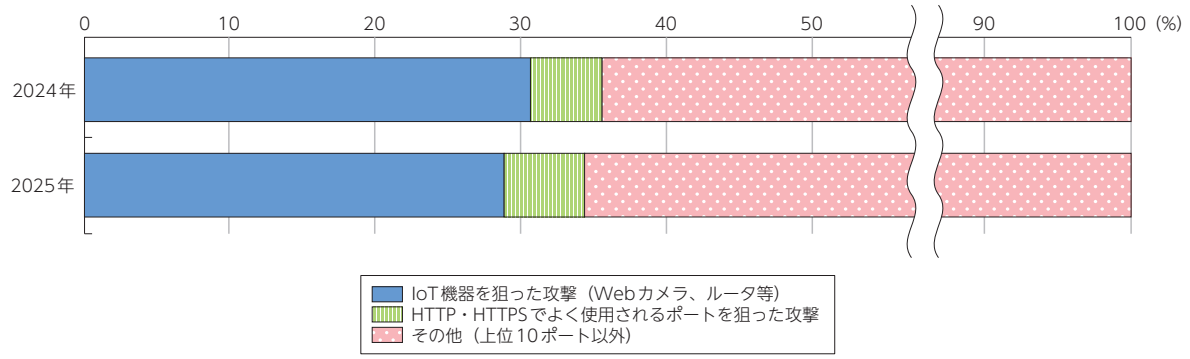
図表Ⅱ-1-10-3　NICTERにおけるサイバー攻撃関連の通信数の推移



（出典）国立研究開発法人情報通信研究機構「NICTER観測レポート2025」を基に作成

NICTERでのサイバー攻撃関連の通信内容をみると、2024年と同様にIoT機器を狙った通信が最も多く観測されている。次いで、HTTP・HTTPSで使用されるポートへの攻撃が多く観測されている。また、多数の宛先ポートにスキャンを行うIoTマルウェアによる攻撃が増加し、上位10ポート以外の「その他」宛ての攻撃割合が増加している（図表Ⅱ-1-10-4）。

図表Ⅱ-1-10-4　NICTERにおけるサイバー攻撃関連の通信の内容



（出典）国立研究開発法人情報通信研究機構「NICTER観測レポート2025」を基に作成

また、2025年中の不正アクセス行為の禁止等に関する法律（以下「不正アクセス禁止法」という。）違反事件の検挙件数は431件であり、前年と比べ132件減少した。

関連データ　不正アクセス禁止法違反事件検挙件数の推移

出典：警察庁・総務省・経済産業省「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」を基に作成
URL：https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r08/html/datashu.html#f00271（データ集）

2 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

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について、様々な組織が調査・分析を公表している（図表Ⅱ-1-10-5）。例えば、日本では、日本ネットワークセキュリティ協会が2017年1月～2024年6月に実施した調査によれば、ランサムウェア感染被害組織の平均被害金額が約4,959万円になるとされている。また、米国では、FBIが実施した調査によれば、2024年に発生したサイバー犯罪事件による被害報告総額が166億ドルとなるとされている。

図表Ⅱ-1-10-5　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
日本ネットワークセキュリティ協会	日本	2017年1月～2024年6月	ランサムウエア感染被害組織の平均被害金額	4,959万円 （直近2年（2022年7月～2024年6月）は6,019万円）
警察庁	日本	2025年	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	18%が100万円未満 20%が100万～500万円未満 10%が500万～1,000万円未満 36%が1,000万～5,000万円未満 10%が5,000万～1億円未満 6%が1億円以上
FBI	米国	2024年	サイバー犯罪事件による被害報告総額	166億ドル（前年比33%増）
Sophos	世界17か国	2025年	ランサムウェア攻撃の修復に支払った1組織あたりの身代金	中央値：100万ドル
			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（身代金の支払いは除く）	153万ドル
IBM	世界	2024年3月～2025年2月	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	444万ドル
Statista	世界	2018～2029年	世界におけるサイバー犯罪の推定コスト	2024年は9.22兆ドル 2029年は15.63兆ドル

（出典）各種公開資料を基に作成

3 無線LANセキュリティに関する動向

無線LANの利用者のセキュリティ意識などを把握するために総務省が2026年2月に実施した意識調査[*2]によると、公衆無線LANの認知度は高い（約91%）が実際に利用している人はその半数程度にとどまっている。また、公衆無線LANを利用していない最多の理由として、6割程度が「セキュリティ上の不安がある」と回答している。また、公衆無線LAN利用者のうち、9割弱がセキュリティ上の不安を感じており、特に情報窃取、外部からの不正侵入を不安材料に挙げる利用者が多い。

OpenRoaming[*3]に対応した公衆Wi-Fiでは、通信の暗号化や偽の公衆Wi-Fiへの接続を防止する技術が使われており、ユーザーは安全に公衆Wi-Fiを利用することができるほか、一度OpenRoamingの利用登録をすることで、全世界のOpenRoaming対応の公衆Wi-Fiを追加設定なしで利用することができる。国内では東京や大阪をはじめとした都市圏で導入が進んでおり、対応する公衆Wi-Fiも順次拡大される予定である。

4 送信ドメイン認証技術の導入状況

なりすましメールを防止するための「送信ドメイン認証技術」のJPドメインでの導入状況は、2025年12月時点で、SPFは約89.6%、DMARCは約37.2%となっており、いずれも増加傾向にある。

関連データ　送信ドメイン認証技術のJPドメイン導入状況等

出典：電気通信事業者4社の協力により、総務省がとりまとめ
URL：https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r08/html/datashu.html#f00278（データ集）

＊2　https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/
＊3　最新のWi-Fi技術やサービスの導入・推進を実施するグローバル組織であるWireless Broadband Allianceが支援している国際的なWi-Fi Roaming基盤