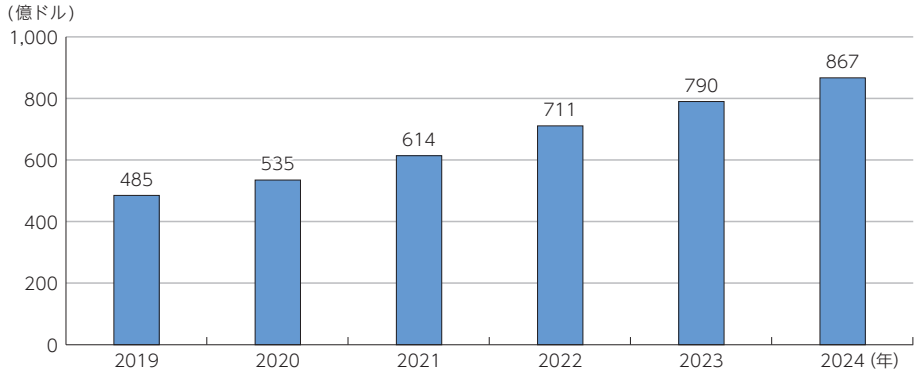
第10節　サイバーセキュリティの動向

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9.7%増加の867億ドルとなっている（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）Canalysデータを基に作成

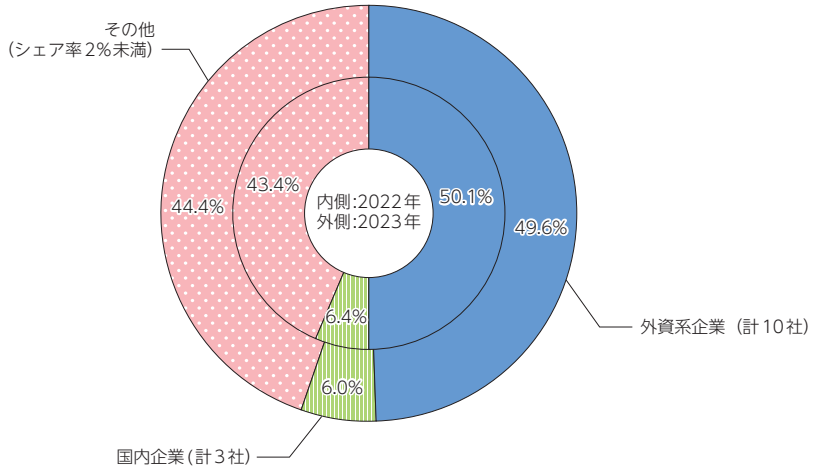
サイバーセキュリティ市場の主要事業者として、2019年からPalo Alto Networks、Cisco、Fortinetの3社が世界上位3位の市場シェアを獲得していたが、2024年第2四半期時点ではCiscoに代わりMicrosoftが上位3位に入っている。近年はトップシェアであるPalo Alto Networksの市場シェアが拡大し、10%に迫る勢いとなっている。また、Microsoftは近年急速にシェアを拡大しており、Microsoft 365 E5 Securityなど高度なセキュリティ機能をMicrosoft 365シリーズの一つとして提供しており、導入のしやすさも含めて評価されていると考えられる。

関連データ　世界のサイバーセキュリティ主要事業者
URL：https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r07/html/datashu.html#f00277（データ集）

2023年の国内の情報セキュリティ製品市場（売上高）は、前年比12.0%増の5,574億400万円となった。セキュリティ製品の機能市場セグメント別では、エンドポイントセキュリティソフトウェアやネットワークセキュリティソフトウェアなどを含む、セキュリティソフトウェア市場の2023年の売上額が4,965億1,100万円で全体の89.1%を占め、コンテンツ管理、UTMやVPNなどを含むセキュリティアプライアンス市場は608億9,300万円で全体の10.9%となった。

また、2022年及び2023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2%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2022年及び2023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5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）。

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）2022年～2023年



（出典）IDC Japan, 2025年4月「国内情報セキュリティ製品市場シェア、2024年上半期：成長するSaaS型セキュリティ市場」（JPJ50704524）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2024年の総観測パケット数（約6,862億パケット）は、2015年（約632億パケット）と比較して10.86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、2024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。

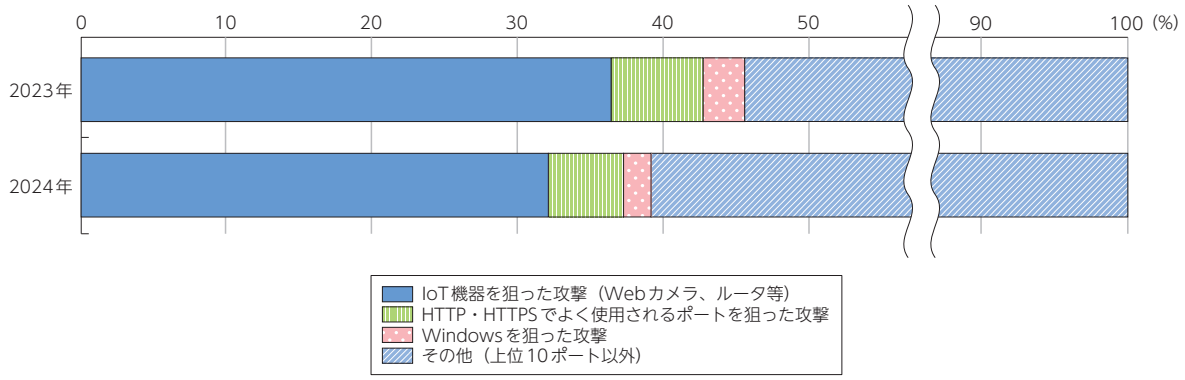
なお、2024年は過去最高の観測数を記録しており、インターネット上を飛び交う観測パケットは2023年と比較して更に活発化している状況であるといえる。

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2024」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、2023年と同様にIoT機器を狙った通信が最も多く観測され、サイバー攻撃関連通信全体の約3割を占めている。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（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2024」を基に作成

また、2024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563件であり、前年と比べ42件増加した。

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
URL：https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r07/html/datashu.html#f00283（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）。損失の範囲をどこまで捉えるかなどにより数値に幅があるが、例えば、日本では、トレンドマイクロが2024年に実施した調査によれば、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が約1億7,100万円になる。

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
トレンドマイクロ	日本	2024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	1億7,100万円 （1年前に比べて約4,600万円増）
警察庁	日本	2024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	25%が100万円未満 21%が100万～500万円未満 8%が500万～1,000万円未満 27%が1,000万～5,000万円未満 19%が5,000万以上
FBI	米国	2023年	サイバー犯罪事件による被害報告総額	125億ドル（前年比22%増）
Sophos	世界14か国（北米、中南米、欧州、アジア太平洋地域）	2024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	・平均値：約396万ドル（前年から2.6倍に増加） ・中央値：200万ドル（前年から5倍に増加）
			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）	273万ドル
IBM	世界	2024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	488万ドル
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2024年11月に実施した意識調査[*1]によると、公衆無線LANの認知度は高い（約92%）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[*2]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、2024年9月時点で、SPFは約88.4%、DMARCは約32.6%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
URL：https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r07/html/datashu.html#f00290（データ集）

＊1　https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/
＊2　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