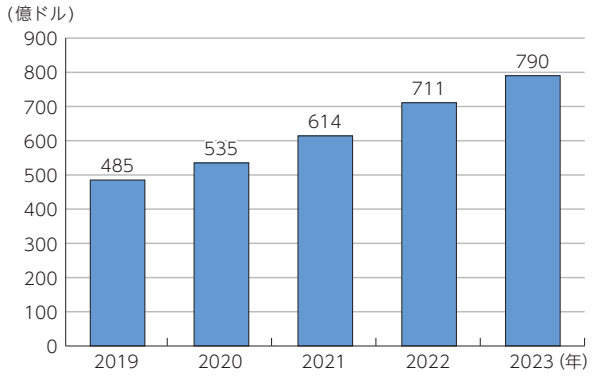
第10節 サイバーセキュリティの動向

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、2023年には790億ドル11.1%増）になると予測されている（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、Cisco、Palo Alto Networks、Check Point、Symantec、Fortinetの5社が2018年から2019年まで世界Top5の市場シェアを獲得していたが、2020年からはSymantecの代わりにTrellixが台頭し、2022年には3.1%のシェアを獲得している。しかし、2023年時点ではCheck Point、Trellixに代わりMicrosoft、Crowd StrikeがTop5に入っている。また、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。

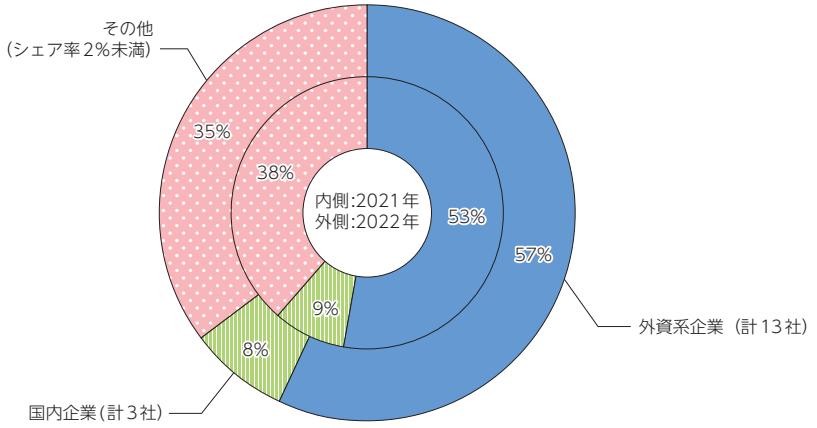
関連データ　世界のサイバーセキュリティ主要事業者

出典：Canalysデータを基に作成
URL：https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r06/html/datashu.html#f00294（データ集）

2022年の国内の情報セキュリティ製品市場（売上高）は、前年比19.8%増の5,254億5,400万円となった。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2022年の売上額が4,274億200万円で全体の81.3%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980億5,100万円で全体の18.7%となった。

また、2021年及び2022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、2022年の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2021年及び2022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割を超えており、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）　2021年～2022年



（出典）IDC Japan, 2023年8月「国内情報セキュリティ製品市場シェア、2022年：セキュリティプラットフォームの進展」（JPJ49213223）を基に作成

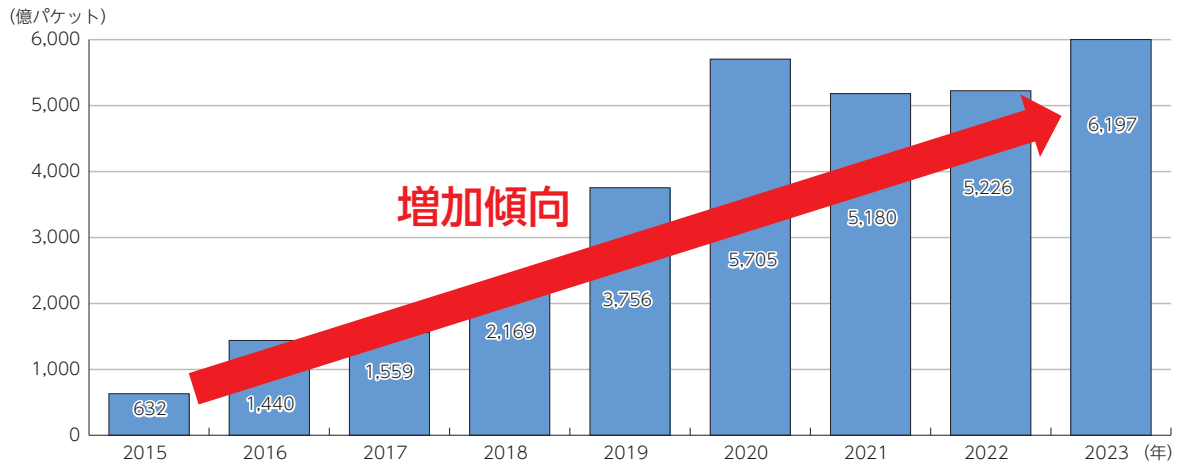
② サイバーセキュリティの現状

① サイバーセキュリティ上の脅威の増大

国立研究開発法人情報通信研究機構（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2023年の総観測パケット数（約6,197億パケット）は、2015年（約632億パケット）と比較して9.8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、2023年の総観測パケット数は各IPアドレスに対して14秒に1回観測されたことに相当する。

なお、2023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2022年と比較して更に活発化している状況であると言える。

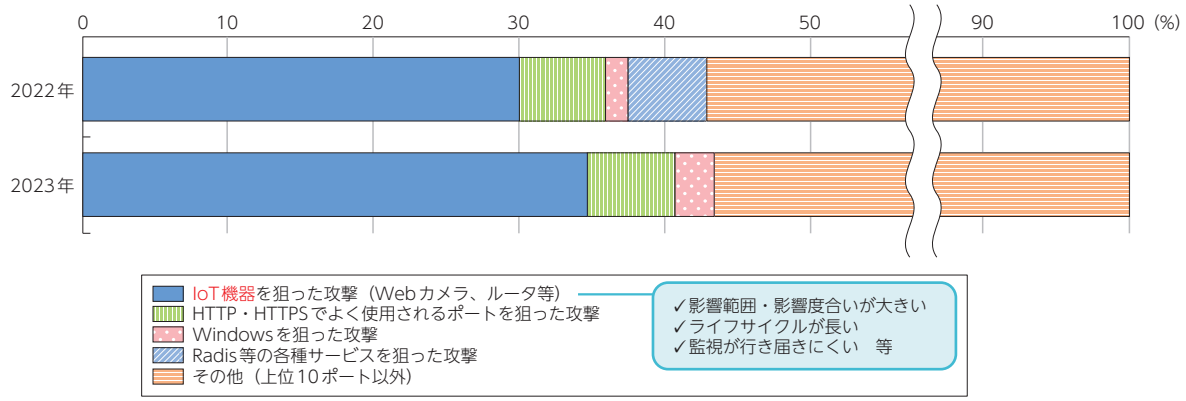
図表Ⅱ-1-10-3　NICTERにおけるサイバー攻撃関連の通信数の推移



（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2023」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、2022年と同様にIoT機器を狙った通信が多く観測され、サイバー攻撃関連通信全体の約3割を占めている。また、HTTP・HTTPSで使用されるポートへの攻撃についても同程度の割合で観測されている（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



※NICTERで2022年・2023年に観測されたもの（調査目的の大規模スキャン通信を除く。）について、上位10ポートを分析。
（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2023」を基に作成

また、2023年中の不正アクセス行為の禁止等に関する法律（平成11年法律第128号。以下「不正アクセス禁止法」という。）違反事件の検挙件数は521件であり、前年と比べ1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/r06/html/datashu.html#f00300（データ集）

近年ではランサムウェアによるサイバー攻撃被害が国内外の様々な企業や医療機関等で続き、国民生活や社会経済に影響が出る事例も発生している。また、2023年3月には「Emotet（エモテット）」の活動再開が確認され、同月、独立行政法人情報処理推進機構（IPA）やJPCERT/CCより注意喚起が実施された。最近では日本の政府機関・地方自治体や企業のホームページ等を標的としたDDoS攻撃により、業務継続に影響のある事案も発生し、国民の誰もがサイバー攻撃の懸念に直面している。

こうした依然として厳しい情勢の下、直近では、大型連休がサイバーセキュリティに与えるリスクを考慮し、2023年4月に経済産業省、総務省、警察庁、NISCより春の大型連休に向けて実施が望まれる対策について注意喚起が実施された。

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2023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1億2,528万円になる。

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	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
Fastly	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%

（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3月に実施した意識調査によると、公衆無線LANの認知度は高い（約94%）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、7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割程度の利用者がセキュリティ上の不安を感じているものの、そのうちの4割程度が「漠然とした不安」として挙げている。

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、2023年12月時点で、SPFは約82.9%、DMARCは約10.2%となっており、いずれも微増傾向にある。

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

URL：https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r06/html/datashu.html#f00307（データ集）