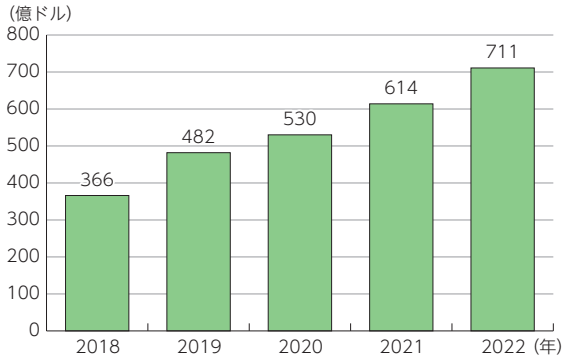
第10節 サイバーセキュリティの動向

1 市場概況

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、2022年には9兆3,495億円38.7%増）になると予測されている（図表4-10-1-1）。セキュリティ製品カテゴリー別にみると、2022年第4半期時点では、ネットワークセキュリティへの支出が最も多く、全体の27.6%を占めている。

図表4-10-1-1 世界のサイバーセキュリティ市場規模（売上高）の推移



（出典）Canalys推計*1を基に作成

関連データ

世界のサイバーセキュリティ市場規模（製品カテゴリ別）

出典：Canalys“Strong channel sales propel the cybersecurity market to US$20 billion in Q4 2022”を基に作成
URL：https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r05/html/datashu.html#f00263（データ集）

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。また、シェア最大であるPalo Alto Networksでも8.2%のシェアしか占めておらず、世界のサイバーセキュリティ市場では、シェアが分散された状態が続いている。

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/r05/html/datashu.html#f00264（データ集）

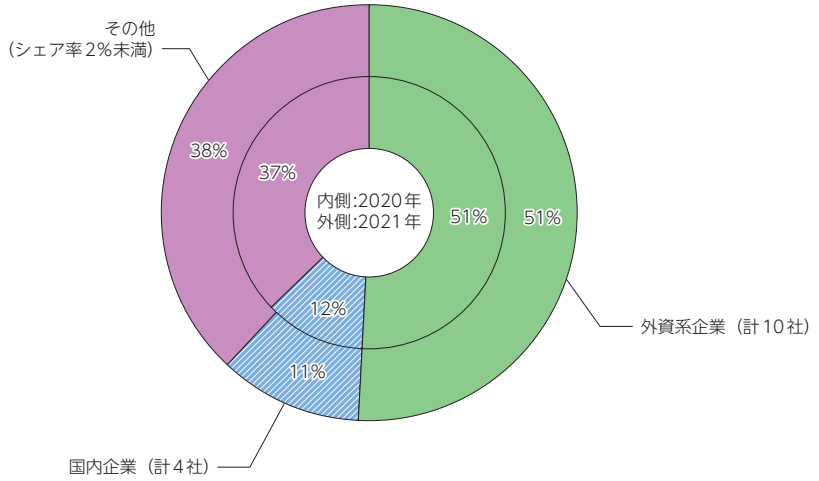
2021年の国内の情報セキュリティ製品市場（売上高）は、前年より16%増の4,360億1,500万円となった。セキュリティ製品の機能市場セグメント別では、エンドポイントセキュリティソフトウェアやネットワークセキュリティソフトウェアなどを含む、セキュリティソフトウェア市場の2021年の売上額が3,703億5,000万円で全体の84.9%を占め、コンテンツ管理、UTMやVPNなどを含むセキュリティアプライアンス市場は656億6,600万円で全体の15.1%となった。

また、2020年及び2021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、2021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2020年及び2021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

＊1 https://www.canalys.com/newsroom/cybersecurity-market-grows-9-in-2018-to-reach-us37-billion
https://canalys.com/newsroom/cybersecurity-investment-2020
https://canalys.com/newsroom/cybersecurity-market-2022

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4-10-1-2）。

図表4-10-1-2　国内情報セキュリティ製品市場シェア（売上額）　2020年～2021年



（出典）IDC Japan, 2022年7月「国内情報セキュリティ製品市場シェア、2021年：デジタルファーストで変化する市場」(JPJ47880222）を基に作成

2　サイバーセキュリティの現状

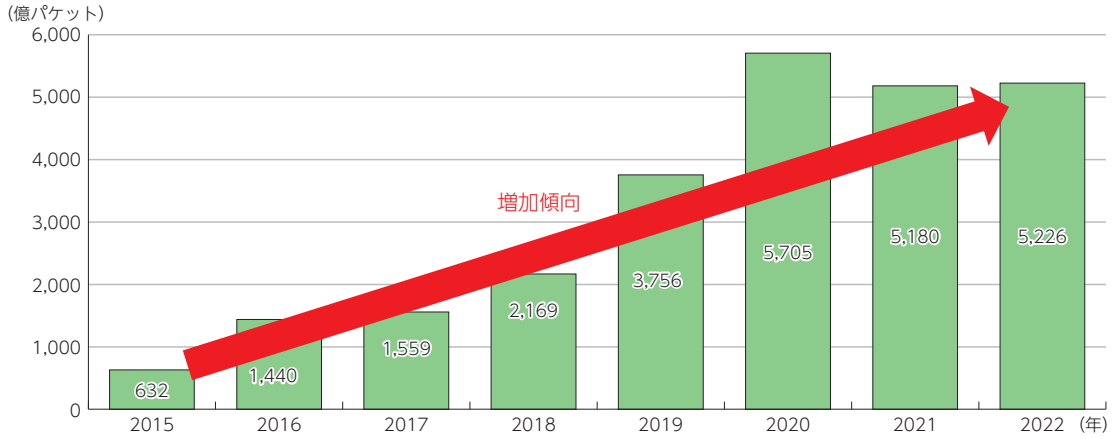
1　サイバーセキュリティ上の脅威の増大

NICTが運用している大規模サイバー攻撃観測網（NICTER）が2022年に観測したサイバー攻撃関連通信数（約5,226億パケット）は、2015年（約632億パケット）と比較して8.3倍となっているなど、依然多くの攻撃関連通信が観測されている状態である（図表4-10-2-1）。また、2022年に観測されたサイバー攻撃関連通信数は各IPアドレスに対して17秒に1回攻撃関連通信が行われていることに相当する。

なお、2020年から観測数が減少しているが、これは、2020年に観測された特異的な事象（大規模なバックスキャッタ*2や、特定の送信元からの集中的な大量の調査目的と思われる通信）が2022年には観測されなかったことなどが要因として挙げられる。

*2　送信元IPアドレスが詐称されたDoS攻撃（SYN-flood攻撃）を受けているサーバーからの応答（SYN-ACK）パケットのこと。IPアドレスがランダムに詐称されている場合には、DoS攻撃を受けているサーバーから多くの応答パケットがダークネットにも到来するため、DoS攻撃の発生を検知できる。

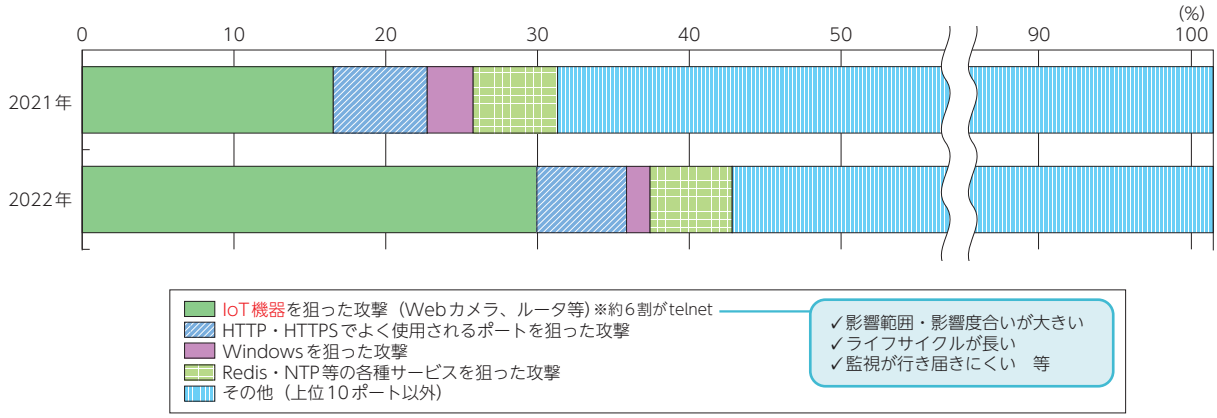
図表4-10-2-1　NICTERにおけるサイバー攻撃関連の通信数の推移



（出典）NICT「NICTER観測レポート2022」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、2021年に比べIoT機器を狙った通信が大幅に増加し、サイバー攻撃関連通信全体の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は昨年と同程度の割合で観測されている（図表4-10-2-2）。

図表4-10-2-2　NICTERにおけるサイバー攻撃関連の通信の内容



※NICTERで2021年・2022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2022」を基に作成

また、2022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522件であり、前年と比べ93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/r05/html/datashu.html#f00270（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いただきたい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4-10-2-3）。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、トレンドマイクロが実施した調査によれば、日本では2021年度1年間で発生したセキュリティインシデントに起因した1組織あたり年間平均被害額は約3億2,850万円になると算出されている。

図表4-10-2-3　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	2021年	セキュリティインシデントに起因した1組織あたり年間平均被害額	3億2,850万円
警察庁	日本	2022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	20%が100万円未満 14%が100万～500万円未満 10%が500万～1,000万円未満 37%が1,000万～5,000万円未満 18%が5,000万以上
FBI	米国	2021年	サイバー犯罪事件による被害報告総額	69億ドル
NFIB	英国	2022年	サイバー犯罪による被害報告総額	630万ポンド
Sophos	世界31か国	2021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	140万ドル
IBM	世界	2022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	435万ドル
Cybersecurity Ventures	世界	2023年【予測】	サイバー犯罪によるコスト	8兆ドル
McAfee、CSIS	世界	2020年	サイバー犯罪によるコスト	9,450億ドル

（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2022年11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を利用していない理由としては、「セキュリティ上の不安がある」が他の理由を引き離しトップとなっている。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、そのうちの半数は「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、2022年12月時点で、SPFは約77.2%、DMARCは約2.7%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/r05/html/datashu.html#f00277（データ集）