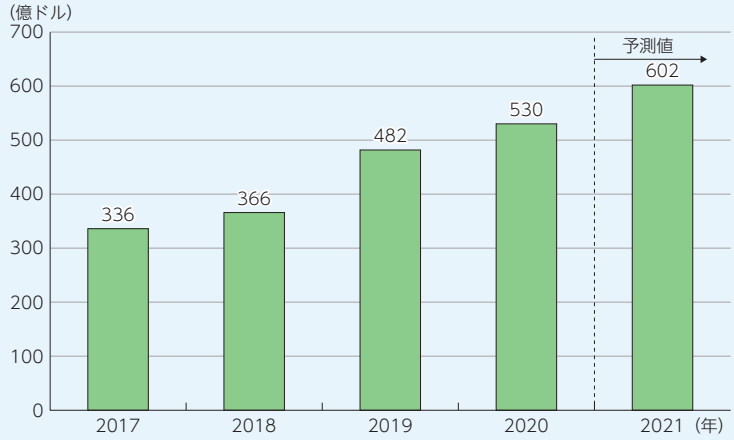
第7節　サイバーセキュリティの動向

1 世界市場の概況

世界のサイバーセキュリティの市場は、ランサムウェアなどの標的型サイバー攻撃の急増などにより、2020年には5兆6,591億円となり、2021年には6兆6,072億円（前年比16.8%増）になると予測されている（図表3-7-1-1）。

図表3-7-1-1　世界のサイバーセキュリティ市場規模の推移及び予測



（出典）Canalys推計*1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2017年から市場シェアの上位を占めている（図表3-7-1-2）。また、シェア最大であるCiscoでも10%前後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、シェアが分散されている状態である。

図表3-7-1-2　世界のサイバーセキュリティ主要事業者

事業者	世界市場シェア			
	2017年	2018年	2019年（Q1）	2020年（Q1）
Cisco	9.4%	9.9%	10%	9.1%
Palo Alto Networks	5.9%	6.9%	7%	7.8%
Check Point	6.4%	6.1%	6%	5.4%
Symantec	7.5%	6.1%	6%	4.7%
Fortinet	5.1%	5.5%	5%	5.9%

（出典）Canalys推計*2を基に作成

＊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/canalys-cybersecurity-2021-forecast

＊2　https://www.canalys.com/newsroom/cybersecurity-market-grows-9-in-2018-to-reach-us37-billion
https://www.canalys.com/newsroom/cybersecurity-market-q1-2019
https://www.canalys.com/newsroom/canalys-cybersecurity-market-q1-2020

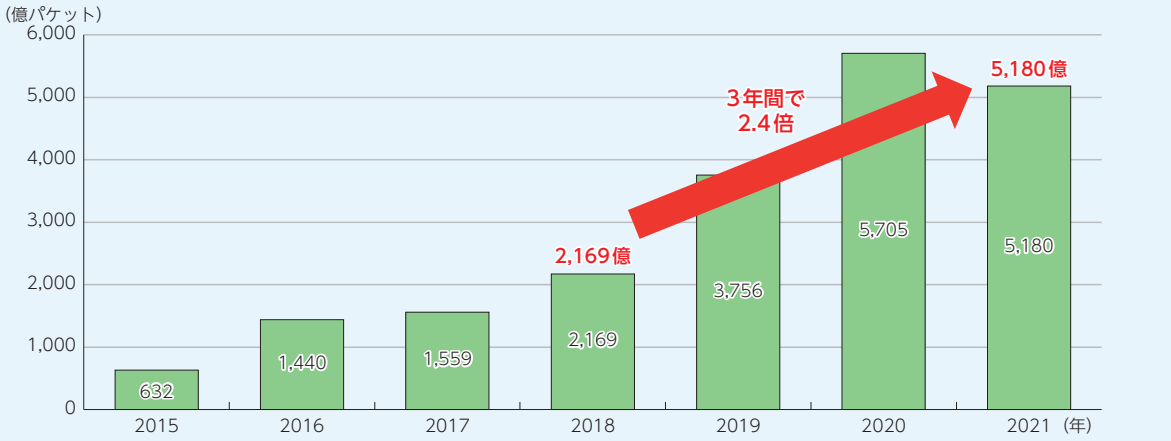
2 我が国におけるサイバーセキュリティの現状

ア　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2021年に観測したサイバー攻撃関連通信数（約5,180億パケット）は、3年前との比較では2.4倍（2018年　約2,169億パケット）、5年前との比較では3.7倍（2016年　約1,440億パケット）に増加しており、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3-7-2-1）。また、2021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18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、2021年は2020年から減少しているが、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*3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2021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。

図表3-7-2-1　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2021」を基に作成

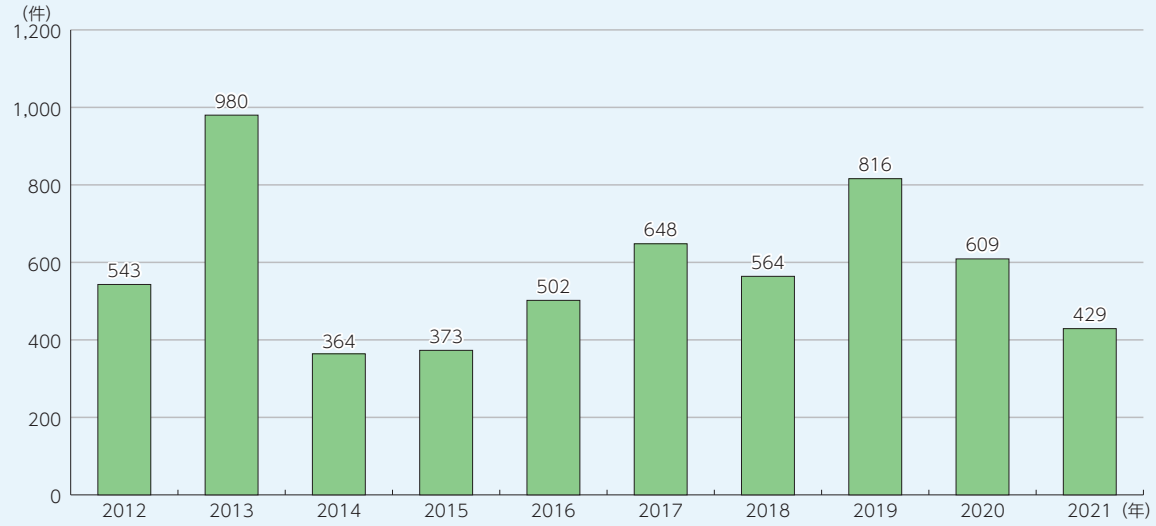
NICTERでのサイバー攻撃関連の通信内容をみると、IoT機器を狙った通信が依然として最も多い一方で、昨年は2番目に多かったWindowsを狙った通信の割合が減少し、昨年は上位には見られなかった様々なサービスで利用されるポートへの通信の割合が増加するほか、その他の占める割合が増加しており、攻撃対象多様化の傾向が継続している。

【関連データ】
NICTERにおけるサイバー攻撃関連の通信の内容
出典：NICT「NICTER観測レポート2021」を基に作成
URL：https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/html/nf307000.html（データ集）

また、2021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429件であり、前年と比べ180件減少した（図表3-7-2-2）。

＊3　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3-7-2-2　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」により作成

2021年11月より、「Emotet（エモテット）」の攻撃活動再開の兆候が確認されており、2022年2月には、感染の急拡大に伴い、独立行政法人情報処理推進機構（IPA）やJPCERT/CCより注意喚起を実施された。

また、昨今のサイバー攻撃事案のリスクの高まりを踏まえ、2022年2月23日に経済産業省より、同年3月1日に経済産業省、金融庁、総務省、厚生労働省、国土交通省、警察庁、内閣官房内閣サイバーセキュリティセンター（NISC）より、同年3月24日に経済産業省、総務省、警察庁、NISCより、サイバーセキュリティ対策の強化に関する注意喚起が実施された。同年4月25日には、経済産業省、総務省、警察庁、NISCより、長期休暇期間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。

イ　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2021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96%）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。

ウ　送信ドメイン認証技術の導入状況

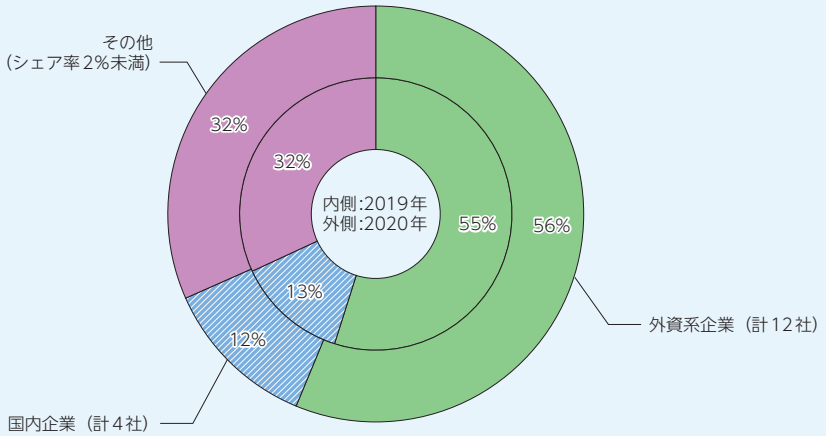
なりすましメールを防止するための「送信ドメイン認証技術」のJPドメインでの導入状況は、2021年12月時点で、SPFは約67.5%、DMARCは約2.1%となっており、いずれも微増傾向にある。

【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
出典：総務省「JPドメイン名の種別ごとにおける送信ドメイン認証技術の設定状況」
URL：https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/html/nf307000.html（データ集）

エ　サイバーセキュリティ製品の海外依存

2019年及び2020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、2020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2019年・2020年の売上額を集計した結果、2019年・2020年ともに外資系企業のシェアが高く、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言える（図表3-7-2-3）。

図表3-7-2-3　国内情報セキュリティ製品市場シェア（売上額）　2019年～2020年



（出典）IDC Japan, 2021年7月「国内情報セキュリティ製品市場シェア、2020年：外部脅威対策および内部脅威対策」(JPJ46567421）を基に作成