第4節　サイバーセキュリティ

デジタル活用が社会のあらゆる面で拡大する一方、世界情勢の不安定化・緊迫化等も背景にしたサイバー攻撃の複雑化・巧妙化や、デジタル活用拡大に伴うシステムの複雑化やインターネットに面したアタックサーフェス（攻撃可能面）の拡大等により、ランサムウェアやゼロデイ攻撃等による機密情報の漏えい、重要インフラのサービス停止等のセキュリティリスクが拡大傾向にある。

デジタルインフラへの社会の依存度が増す中、ひとたびサイバーインシデントにより被害を受けた際の規模・範囲もますます拡大すると想定され、安全保障上も懸念が大きい。

デジタル空間におけるサイバーセキュリティ確保のためには、各ステークホルダーの水準の向上と連携が求められる。政府の対応、官民連携、国際連携、技術的対応、国民リテラシー向上等、すべての関係者による総合的な対応が重要となっている。

1　主な課題の概要

サイバー攻撃のリスクは、年々拡大傾向にある。例えば、国立研究開発法人情報通信研究機構（NICT）によれば、NICTERのダークネット観測網における2024年の1 IPアドレス当たりの年間総観測パケット数は、前年の2023年から更に増加しており、インターネット上を飛び交う探索活動が更に活発化していることがうかがわれる[*1]。

また、社会経済活動における重要インフラが、サイバー攻撃により被害・サービス停止した場合、大きな社会的な混乱が引き起こされるおそれがある。2024年度中にも、重要インフラ等を狙った様々なサイバー攻撃事案等が発生した。

関連データ　国内で2024年度に発生した重要インフラ関連のサイバー攻撃被害事例
URL：https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r07/html/datashu.html#f00075（データ集）

2　対応の方向性

デジタル空間におけるサイバーセキュリティ確保のためには、各ステークホルダーの水準の向上と連携が求められるが、ここでは最近の動きとして、政府の対応としての能動的サイバー防御に関する法整備について取り上げる。

近年、サイバー攻撃による政府や企業の内部システムからの情報窃取等が大きな問題となっているほか、重要インフラ等の機能を停止させることを目的とした高度な侵入・潜伏能力を備えたサイバー攻撃に対する懸念が急速に高まっている。特に重要インフラの機能停止や破壊等を目的とした重大なサイバー攻撃は、国家を背景とした形でも日常的に行われるなど、安全保障上の大きな懸念となっている。

こうした情勢に対処するため、「国家安全保障戦略」（2022年12月16日閣議決定）に基づき、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるべく、2025年の第217回国会（常会）に「重要電子計算機に対する不正な行為による被害の防止に関する法律」及び「重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律」の両法案が提出され、原案修正の上、2025年5月に可決・成立した。

＊1　第Ⅱ部第1章第10節2「サイバーセキュリティの現状」参照