6. CISA が初の国際戦略を発表

要約

- CISA は米国のサイバーセキュリティを担当し、重要インフラに関する国家的な調整役である。
- 近年、米国の重要インフラは外国のシステムやネットワークと密接に接続し、相互依存している。
- CISA は重要インフラのセキュリティとレジリエンス強化を目的に初の国際戦略計画を策定した。

CISA とは

CISA（Cybersecurity and Infrastructure Security Agency）とは、米国の行政機関の一つです。米国国土安全保障省の外局として米国政府のサイバーセキュリティを担当し、重要インフラ(*1)のセキュリティとレジリエンスに関する国家的な調整役を務めています。その使命は、サイバーおよび物理的インフラに対するリスクを軽減することであり、そのためにさまざまな提言を行っています。

2024 年 10 月 29 日、CISA は『2025-2026 CISA International Strategic Plan』を発表しました(*2)。これは CISA にとって初となる国際戦略計画であり、米国の重要インフラのセキュリティとレジリエンスの強化に向けてどのように国際的パートナーと積極的に関与していくかに焦点を当てています。

米国の重要インフラに関する政策と CISA の歴史

1998 年 5 月 22 日、重要インフラのセキュリティに関する初の包括的な戦略である PDD-63 が発表されました。当時の重要インフラは自動化され、相互に依存するようになっており、サイバー攻撃を始めとする外部からの影響に対して脆弱になっていました。そこで、PDD-63 ではサイバーセキュリティに対する取り組みが明確に打ち出されました。特に、インフラに対する脅威に関する情報を収集・分析し、対応する拠点として NIPC（National Infrastructure Protection Center）が設立されました。

その後、2003 年 12 月 17 日には PDD-63 を改訂した HSPD-7 が発表されました。HSPD-7 はテロ攻撃から重要インフラを守るために、各省庁が重要インフラを特定し、優先順位を設定することを目的とした国家方針です。特に、Homeland Security Act of 2002 に基づき、重要インフラの保護における中心的な役割が NIPC から米国国土安全保障省へ移されました。

2006 年 10 月 4 日には Post-Katrina Emergency Management Reform Act of 2006 が成立し、これに伴って米国国土安全保障省で組織改編が行われました。この組織改編で準備局から米国連邦緊急事態管理庁へ移管されなかった組織は、NPPD（National Protection and Programs Directorate）として再編されました。移管されなかった組織には CS&C(*3)や OIP(*4)が含まれます。

2013 年 2 月 12 日、HSPD-7 を廃止し、後継となる PPD-21 が発表されました。HSPD-7 と同様に PPD-21 は重要インフラのセキュリティに関する指令ですが、HSPD-7 と異なり、レジリエンスの重要性が明確にされています。また、官民や異なるセクター間での情報共有の重要性がより強調されています。

(*1) 物理的か仮想的かを問わないシステムおよび資産であって、その機能不全や破壊が連邦、州、地域、準州、地方の管轄区域にわたって安全保障、経済、公衆衛生、公共の安全、環境またはそれらの組み合わせに対して壊滅的な影響を及ぼす可能性があるもののこと。

(*2) CISA Releases Its First Ever International Strategic Plan

(*3) 国家のサイバーおよび通信インフラのセキュリティ、レジリエンス、信頼性を確保することを使命とした組織。

(*4) テロ行為による重要インフラおよび主要リソースへのリスクを軽減することを使命とした組織。

2018 年 11 月 16 日、Cybersecurity and Infrastructure Security Agency Act of 2018 が成立しました。これにより、NPPD は CISA に改編され、より独立性の高い組織となりました(*1)。さらに、2024 年 4 月 30 日には、PPD-21 に代わる NSM-22 が発表されました。この覚書により、CISA は「セキュリティとレジリエンスの国家的な調整役」という役割を担うこととなりました。

2025-2026 CISA International Strategic Plan

前述の通り、重要インフラが密接に結びつき、相互に依存していることは以前から認識されており、そのセキュリティやレジリエンスの方針が策定されていました。現代では、その接続先・依存先が海外の資産、システム、ネットワークとなっていることもあり、重要インフラへのリスクは国境を越えて分散しています。そのため、重要インフラを保護し、安全を確保するためには世界中の官民のパートナーとの協力が必要です。

そこで、CISA は初の国際戦略計画を策定し、その最終的な目標として以下の三つを掲げました：

目標1.　米国が依存する外国のインフラのレジリエンスを支援する。

目標2.　統合サイバー防御を強化する。

目標3.　国際活動に関する機関間の調整を一元化する。

さらに、それぞれの目標に対し、以下の小目標が設けられています：

	小目標
目標 1.	国家が依存する外国の重要インフラを特定し、優先順位をつけ、そのセキュリティとレジリエンスの強化を支援する。
	米国の重要インフラに関する優先事項と利益を海外で促進する国際的パートナーシップを強化する。
	セキュリティを向上させるための運用および技術的な国際基準、規制、政策、ガイドライン、ベストプラクティスを策定する。
目標 2.	パートナーと協力し、集団的リスクを低減するためのサイバー防御を可能にする。
	サイバーセーフティを高めるために、標準化とセキュリティの強化を大規模に推進する。
	主要なパートナーのサイバーおよび物理的なレジリエンス能力を向上させる。
目標 3.	CISA の国際活動におけるガバナンスを強化し、制度化する。
	CISA の国際的機能、能力、リソースを連携させ、同期させる。
	国際的な舞台における CISA の能力を促進するために、トレーニングと教育を通じて CISA の職員を強化する。

出典:『2025-2026 CISA International Strategic Plan』を基に大和総研作成

加えて、小目標ごとに実施措置(Enabling Measure)と効果測定指標(Measure of Effectiveness, MOE)が定められています。効果測定指標としては、リスクの対処や混乱の緩和のために取られる国内外のパートナーの活動数の増加や、グローバルパートナーと実施する共同作戦の数の増加などがあり、全体として国際的な取り組みのさらなる強化が意識されています。

示唆

今後、CISA や米国政府が各国の関連機関に対して行う働きかけは、基本的には米国の国家安全保障や経済、外交政策に沿った内容となりますが、部分的には日本にとっても重要です。そのため、日本がその働きかけに応じて作成・公表する政策や手引書は CISA が公表したさまざまなガイドラインやベストプラクティスなどに沿うものになると考えられます。したがって、CISA の公表物には目を通しておくことが望ましいでしょう。

（DIR SOC Quarterly 執筆者一同）

(*1) 廣瀬淳子『【アメリカ】サイバーセキュリティー・インフラセキュリティー庁設置』