特集／欧米の規制動向

〈1〉米国の 2025 会計年度国防授権法におけるサイバーセキュリティ関連の重要規定とその概要

法政大学　人間環境学部　教授　**永野　秀雄**

Ⅰ　はじめに

バイデン大統領（当時）は、2025 年 12 月 23 日に、2025 会計年度国防授権法（2025 NDAA）に署名し、同法を成立させた[1]。NDAA の正式名称は年度によってしばしば異なるが、今年度は、「軍人の生活の質の向上及び 2025 会計年度国防授権法（Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025）」となっている。

2025NDAA では、約 8,952 億ドルの国防予算（連邦エネルギー省の国家安全保障プログラムを含む）が承認されている。これを昨年度の国防予算と比較すると約 90 億ドル（約１％）の増加となっている。

本稿では、2025 NDAA において規定されたサイバーセキュリティ関連規定のうち、重要性が高いものに限って概説したい。また、本年も、国防授権法を何とかして年内に成立させるという伝統にしたがって 2025NDAA が発効したことから、作成に時間のかかる正式な立法者意思を示す両院協議会報告書は存在していない。このため、本稿では立法者意思を確認するため、これに代わる簡易な文書（Joint Explanatory Statement of the Committee of Conference）を参照している[2]。

なお、バイデン前大統領は、退任する直前の 2025 年１月 15 日に、大統領令第 14114 号「国家のサイバーセキュリティにおけるイノベーションの強化と推　進（Strengthening and Promoting Innovation in the Nation's Cybersecurity）」を発出し、連邦政府によるサイバーセキュリティに関する取り組みを大幅に改善する政策を打ち出している[3]。トランプ大統領は、就任直後の 2025 年１月 20 日に、バイデン大統領が在任中に発した大統領令を大量に破棄したものの、本大統領令は、その対象とはならなかった。しかしながら、この大統領令第 14114 号には、サイバーセキュリティインフラ保全庁（CISA）の権限を拡大する条項等が含まれており、これが連邦行政機関の権

[1] Servicemember Quality of Life Improvement and National Defense Authorization Act for Fiscal Year 2025, Pub.L.No. 118-159, 138 Stat. 1773 (2024).

[2] 本稿では、該当箇所で直接引用している文献を除き、以下の英語文献を参照した。なお、本稿では、紙幅の関係から、サイテーションによりネット上で文献を特定できる場合には、URL の表示を省略している。*See* Chanda Brown, August Gweon, Stephanie Barna, Darby Rourick, Kristen Chapman & Alexandra Bruer, *President Biden signs the National Defense Authorization Act for Fiscal Year 2025*, Covington & Burling LLP. (Jan. 2, 2025); Alexander O. Canizares & Madison H. Plummer, *The FY 2025 National Defense Authorization Act: What's New for Defense Contractors*, Perkins Coie LLP. (Jan. 30, 2025); Olivia Lynch et al., *The FY 2025 National Defense Authorization Act: Key Provisions Government Contractors Should Know*, Crowell & Moring LLP. (Jan. 7, 2025); Billy Mitchell, *Senate NDAA calls for guidance to apply zero trust to 'internet of military things' devices*, DefenseScoop (July 10, 2024); Cam Sivesind, *3 Percent ($30B) of U.S. Military Funding Dedicated to Cybersecurity*, SecureWorld (Jan. 9, 2025).

[3] *See* Exec. Order No. 14114, Strengthening and Promoting Innovation in the Nation's Cybersecurity, 90 Fed. Reg. 6755 (Jan. 16, 2025).

限を縮小しようとするトランプ大統領の政策と合致していない。このため、同大統領令が、そのまま維持されるのか、あるいはこれに代わる新たな大統領令が発せられることになるのかは予測し難いと言われている[4]。

II　サイバー作戦関係

ここでは、2025NDAA 第 15 編「サイバー空間関連事項（Cyberspace-Related Matters）」第 A 章「サイバー作戦（Cyber Operations）」における重要な条文を概説していくことにする。

A　第 1503 条「国防総省ハッカソンプログラムの設立」

第 1503 条「国防総省ハッカソンプログラムの設立（Establishment of the Department of Defense Hackathon program）」は、本法の施行から 180 日が経過するまでに、国防総省最高デジタル・人工知能責任者（Chief Digital and Artificial Intelligence Officer of the Department of Defense）が、統合参謀本部議長と国防総省最高情報責任者（Chief Information Officer of the Department of Defense）との調整を経たうえで、国防総省ハッカソンプログラム（Department of Defense Hackathon Program）を策定することを義務付ける規定である。ここでいうハッカソンとは、国防総省職員が、その開催期間中に、主催者により決定されたソフトウエア又はハードウエアに関する重大な技術的課題を解決するために共同して取り組むイベントを意味している。なお、ハッカソンに参加するように招聘された職員等には、日当が支給される。

同プログラムにおいては、①国防総省最高デジタル・人工知能責任者が、ハッカソン実施のための基準を策定した上で、各年の主催者の決定、及び、技術的支援等を担い、②各戦闘軍司令官（commanders of combatant commands）及び各軍省長官（Secretaries of the military departments）が、ハッカソンを実施する主催者となり、③毎年、国防総省最高デジタル・人工知能責任者により決定された２名の戦闘軍司令官と２名の軍省長官がハッカソンを実施する義務を負うとされている。

B　第 1504 条「防衛産業基盤へのサイバー脅威机上訓練プログラムの支援」

第 1504 条「防衛産業基盤へのサイバー脅威机上訓練プログラムの支援（Support for cyber threat tabletop exercise program with the defense industrial base）」では、サイバー政策担当国防次官補（Assistant Secretary of Defense for Cyber Policy）が、国防長官を代理して、本法の施行から１年が経過するまでに、サイバー脅威机上訓練プログラムを策定することが義務付けられている。本プログラムは、国防総省及び防衛産業基盤が、武力紛争の発生前又はその最中のサイバー攻撃に備えるためのものである。このことから、同プログラムは、平時の外国によるサイバーインシデントに対応する訓練を超えるレベルのものであることが分かる。

サイバー政策担当国防次官補は、①国防総省最高情報責任者、米国サイバー軍司令官、陸軍合同訓練教育センター司令官（Commander of the Army Interagency Training and Education Center）等と調整したうえで、②国防総省及び国防産業基盤内の個人又は組織で、同プログラムへの参加が適切であると判断したものへの参加の呼びかけを行うことになる。

同プログラムは、①本法の施行から１年が経過する前から 2030 年 12 月 30 日までの期間において半年に１回実施され、②サイバー政策担当国防次官補が、米国の現在及び将来の敵対者のサイバー攻撃能力及び活動をシュミレートした現実的なものにしなければならないとされている。また、同次官補は、このプログラムの実施を通じて、国防総省及び国防産業基盤のサイバーセキュリティにおける脆弱性を特定するための手続を策定する義務を負っている。

なお、同次官補は、国防長官を代理して、2025 年 10 月１日までに、またその後は 2029 年 10 月１日までの期間中は年に１回の頻度で、本プログラムに関する国防総省の前年度の活動を記した報告書を、連邦議会上下院の各軍事委員会に提出しなければなら

[4] *See* Michael Borgia & Andrew Lewis, *Analyzing President Biden's Ambitious Cybersecurity Executive Order*, Davis Wright Tremaine LLP (Feb.5, 2025).

ないとされている。

III　戦略又指針の策定

ここでは、2025NDAA 第 15 編「サイバー空間関連事項（Cyberspace-Related Matters）」第 B 章「サイバーセキュリティ」における戦略又は指針の策定にかかわる重要な条文を概説していくことにする。

A　第 1513 条「軍事作戦で使用される IoT ハードウェアへのゼロトラスト戦略の適用に関する指針」

第 1513 条「軍事作戦で使用される IoT ハードウェアへのゼロトラスト戦略の適用に関する指針（Guidance for application of zero trust strategy to Internet of Things hardware used in military operations）」では、国防総省最高情報責任者に、本法が施行されてから 180 日が経過するまでに、国防総省ゼロトラスト戦略を①米国が軍事作戦で使用する IoT（ウエアラブル端末、センサー及びその他のスマート技術を含む）、及び、②ロール ID（role identity）、認証及びアクセスに関する管理技術に適用する際の指針を作成する義務が課されている。

米軍における IoT ハードウエアは、情報収集能力等の向上に大きな役割を果たしている。その一方で、2015 年頃から、その導入により攻撃の対象となるエンドポイントが急増することが大きな課題になると指摘されていた[5]。国防総省は、2022 年 10 月 21 日付けの「国防総省ゼロトラスト戦略（DoD Zero Trust Strategy）」[6] の公表を皮切りに、2024 年 6 月にはゼロトラストの目標を達成するためのロードマップとガイドを兼ねた「ゼロトラスト・オーバーレイ」[7]（全 383 頁）を、2024 年 11 月 22 日には「ゼロトラスト実施ロードマップ」[8] を公表してきた。上記の条文は、これらに続いて、IoT にゼロトラスト戦略を適用する指針の策定を求めたものとなっている。

B　第 1514 条「マルチクラウド環境の管理及びサイバーセキュリティ」

第 1514 条「マルチクラウド環境の管理及びサイバーセキュリティ（Management and cybersecurity of multi-cloud environments）」では、本法の施行から 180 日が経過するまでに、国防総省最高情報責任者が、国防長官を代理して、国防総省におけるマルチクラウド環境の管理及びサイバーセキュリティに関する戦略を策定しなければならないと定められている。

その上で、この戦略では、以下に列挙された目標が達成されなければならないとしている。

- 同戦略において、2022 年 10 月 21 日付けの「国防総省ゼロトラスト戦略（DoD Zero Trust Strategy）」（その後の更新を含む）との整合を確保すること。
- 国防総省において、マルチクラウド環境全体にわたるネットワークの可視性と相互運用性の提供を目指すこと。
- マルチクラウド環境におけるユーザーID を、ID、認証及びアクセス管理に関する技術の実装を含めて合理化すること。
- 国防総省全体におけるエンドポイントを保護するために、同一の手法を採用すること。
- クラウド環境を導入する前又はその過程において、各クラウド環境に関するセキュリティ上の懸念事項を特定し、かつ、その解決策を向上させるための手段を提供すること。
- 国防総省におけるマルチクラウド環境に人工知能アプリケーションの導入を促進するために必要となる手段を評価すること。
- 国防総省は、当該マルチクラウド環境、及び、これに関連する物品・サービスの利用者並びにその請負者に対して、必要となるキャパシティ容量（capacity demand）、予算及び予測可能性（predictability）に関する情報を提供することで同省の計画を向上させることにより、当該マルチクラウド環境の利用に関する報告における透

[5] *See* Denise E. Zheng & William A. Carter, *Leveraging the Internet of Things for a More Efficient and Effective Military*, CSIS at 20-21 (Sept. 17, 2015).
[6] Dep't of Def., DoD Zero Trust Strategy (Oct. 21, 2022).
[7] Offi. Chief Information Officer, Dep't of Def., Zero Trust Overlays ver. 1.1 (June 2024).
[8] Chief Information Officer, Dep't of Def., Zero Trust Execution Roadmap v1.1（Nov. 22, 2024）.