特集／サイバーセキュリティ

〈2〉2026 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

トランプ大統領は、2025 年 12 月 18 日に 2026 会計年度国防授権法（2026 NDAA）[1] に署名し、同法は成立した[2]。この 2026 NDAA における予算総額は、約 9010 億ドル（約 143 兆円）となっている。

このうち、サイバー活動関連予算は約 151 億ドル（約 2 兆 3962 億円）であり、前年度請求額より 4.1% の増加となった。同予算のうち、純粋なサイバーセキュリティ対策に約 91 億ドルが充当されている。

また、米国サイバー軍の予算は４億ドルを超え、このうちサイバー空間作戦に約 7300 万ドル、未指定活動に約 3000 万ドル、司令部の運用・維持を支援する費用として３億 1400 万ドルが割り当てられている。また、国防総省のサイバー研究費用として、約６億 1,190 万ドルが計上されている。

本稿では、2026 NDAA で規定されたサイバーセキュリティ関連規定のうち、重要性の高いものに限って、①軍人に関する人事政策についての規定、②調達に関する規定、③一般条項におけるサイバー関連の規定、④文民に関するサイバー関連の規定、及び、⑤サイバー空間関連事項における規定の順に概説する[3]。

なお、2026 NDAA については、正式な立法者意思を示した両院協議会報告書（Conference Report）は作成されていない。このため、本稿では、これに代わる簡易な両院合同付帯説明書を参照している[4]。

---

[1] National Defense Authorization Act for Fiscal Year 2026, Pub.L.No. 119-60, 139 Stat. 718 (2025).

[2] The White House, Statement by the President (Dec. 18, 2025).

[3] 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* Cynthia Brumfield, *Key cybersecurity takeaways from the 2026 NDAA*, CSO (Dec. 10, 2025); Steve Cave, Lauren J. Horneffer, Mark Villapando & Christina Wood, *FY 2026 NDAA: Domestic Sourcing, Artificial Intelligence, Cybersecurity*, King & Spalding LLP (Jan. 9, 2026); Jason Chipman, Joshua Geltzer, Hilary Hurd & Marik String, *What the NDAA Means for AI and Cybersecurity*, WilmerHale (Dec. 22, 2025); Weslan Hansen, *NDAA Drops AI Moratorium, TMF Renewal, but Packs Major Cyber Provisions*, Meritalk (Dec. 9, 2025); Natasha G. Kohne, Evan D. Wolff, Rita S. Heimes, Maida Oringher Lerner, Edward Block & Taylor Daly, *Cyber Protections Set to Advance in Must-Pass Defense Legislation*, Akin Gump Strauss Hauer & Feld LLP (Dec. 12, 2025); Ed Pagano, Hans Christopher Rickhoff, Ryan Thompson, Reggie Babin, Casey Christine Higgins, Samuel J. Olswanger, Taylor Daly & Francine Baidoo, *Congress Moves Forward with AI Measures in Key Defense Legislation*, Akin Gump Strauss Hauer & Feld LLP (Dec. 10, 2025); John Slye, *Cybersecurity Provisions in the FY 2026 National Defense Authorization Act*, Deltek (Dec. 17, 2025); *The FY 2026 National Defense Authorization Act*, Crowell & Moring LLP. (Dec. 23, 2025); *The Pentagon's $901 Billion Defense Bill Locks in Cyber Power and Exposes Its Digital Growing Pains*, Enterprise Security Tech (Dec. 29, 2025).

[4] *See* Joint Explanatory Statement to Accompany the National Defense Authorization Act for Fiscal Year 2026, *available at* https://armedservices.house.gov/uploadedfiles/fy26_ndaa_joint_explanatory_statement.pdf.

II　軍人に関する人事政策についての規定

ここでは、2026 NDAA 第５編「軍人に関する人事政策（Military Personnel Policy）」第 E 章「構成員の訓練（Member Training）」における第 547 条「パフォーマンス訓練とその習熟度評価のための生成型人工知能及び空間コンピューティングに関するパイロットプログラム（Pilot program for generative artificial intelligence and spatial computing for performance training and proficiency assessment）」を概説する。

この第 547 条「パフォーマンス訓練とその習熟度評価のための生成型人工知能及び空間コンピューティングに関するパイロットプログラム」において、海軍長官は、本法が施行されてから 90 日が経過するまでに、没入型訓練（immersive training）及びその評価を行うために活用する生成型人工知能及び空間コンピューティングを最適化するためのパイロットプログラムを開発し、これを実施する義務を負っている。

このパイロットプログラムにおいては、①少なくとも５つの職業分野に対応する開発を行うとともに、②生成型人工知能及び空間コンピューティングを用いた訓練に関する実現可能性と有効性とを、他の訓練手法と比較して評価すること（特に、訓練目標を達成するために要する費用と時間に関する評価方法）が求められている。

なお、このパイロットプログラムは、①その開始から１年後に終了するとともに、②海軍長官は、本パイロットプログラムに関する報告書を、同プログラムの終了から 90 日以内に、連邦議会上下院の軍事委員会に提出しなければならないと規定されている。

III　調達に関する規定

ここでは、2026 NDAA 第８編「調達方針、調達管理及び関連事項（Acquisition Policy, Acquisition Management, and Related Matters）」第 F 章「産業基盤事項（Industrial Base Matters）」における第 866 条「サイバーセキュリティ規制の調和（Cybersecurity Regulatory Harmonization）」について概説する。

この第 866 条「サイバーセキュリティ規制の調和」の下で、国防長官は、2026 年６月１日までに、国防総省最高情報責任者、各軍省の最高情報責任者、及び、各軍省の調達責任者（service acquisition executive）と連携して、①国防総省全体の防衛産業基盤に適用されるサイバーセキュリティ要件を調和させ、②国防総省における特定の契約又はその他の合意に特有なサイバーセキュリティ要件の数を減らし、かつ、③上記２つの要件を実施するために講じた措置に関する報告書を連邦議会上下院の軍事委員会に提出する義務を負っている。

また、上記①のサイバーセキュリティ要件の調和を実現するために、重複している、あるいは、矛盾しているサイバーセキュリティ要件や、単一の契約においてのみ求められているサイバーセキュリティ要件を特定し、これらを排除するための手続及びガバナンス構造を設け、かつ、この手続・ガバナンス構造を十分に機能させることが求められている。なお、この手続・ガバナンス構造においては、組織の内部及び外部の利害関係者への可視性を確保するとともに、その意見を反映させるためのメカニズムが含まれていなければならないとされている。

なお、国防総省最高情報責任者は、2026 年 12 月 31 日までに、その後は３年にわたり年１回の頻度で、記載されるべき事項を記した報告書を連邦議会上下院の軍事委員会に提出しなければならないと定められている。

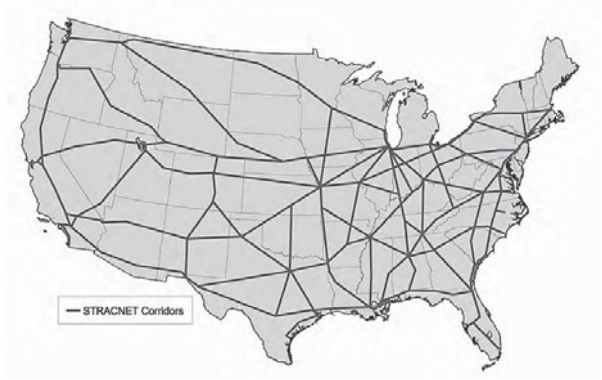
IV　一般条項におけるサイバー関連の規定

ここでは、2026 NDAA 第 10 編「一般条項（General Provisions）」第 F 章「研究及び報告書（Studies and Reports）」における第 1067 条「戦略的鉄道回廊ネットワークの評価におけるサイバーセキュリティ及びレジリアンスに関する付属評価書の追加」、同編第 G 章「その他の事項（Other Matters）」における第 1086 条「技術移転及び外国への開示政策を改革するためのフレームワーク」、及び、同編第 G 章における第 1093 条「重要インフラの互換性に関する机上演習」について概説する。

A　第 1067 条「戦略的鉄道回廊ネットワークの評価におけるサイバーセキュリティ及びレジリアンスに関する付属評価書の追加」

第 1067 条「戦略的鉄道回廊ネットワークの評価におけるサイバーセキュリティ及びレジリアンスに関する付属評価書の追加（Cybersecurity and resilience annex in Strategic Rail Corridor Network assessments）」は、国防長官が、運輸長官及び国土安全保障長官と連携して、本法施行後に実施される戦略的鉄道回廊ネットワークの定期評価において、サイバーセキュリティと物理的インフラの回復力に関する評価を添付文書として作成する義務を負うことを規定した条文である。

この戦略的鉄道回廊ネットワークとは、米国の国防上重要な民間鉄道網のことを意味しており、国防総省が部隊や戦車等の重装備を迅速かつ安全に移動できるように支援するものであり、国防総省及び連邦鉄道局（Federal Railroad Administration）により指定されている。参考までに、以下に同ネットワークの地図を示しておく[5]。



本条で作成が義務付けられている添付文書では、①本ネットワークの運用に影響をもたらす恐れのあるサイバー関連の脅威や脆弱性に関する記述、②米国の敵対者によるサイバー攻撃やその他の妨害行為に対する本ネットワークの回復力に関する評価、③本ネットワークにおけるサイバーセキュリティ上の防御及び物理的インフラを向上させるために、連邦議会及び連邦行政機関が採用するべき推奨事項、④上記③における推奨事項を実施するためのスケジュール及び予算等が記されていなければならないとされている。

B　第 1086 条「技術移転及び外国への開示政策を改革するためのフレームワーク」

第 1086 条「技術移転及び外国への開示政策を改革するためのフレームワーク（Framework for Reforming Technology Transfer and Foreign Disclosure Policies）」は、サイバーセキュリティのみならず、CISTEC Journal の読者の方々が専門とされている領域に直結する内容が規定されている。このため、以下では、その内容を多少詳しく説明しておきたい。

本条では、まず、国防長官に対して、本法が施行されてから 180 日が経過するまでに、各軍の省（military departments）及び外国への技術移転及び対外情報開示にかかわる諸委員会（technology transfer and foreign disclosure committees）における外国への技術移転と対外情報開示に関する指針及び手続を改訂するためのフレームワークを策定することが命じられている（本条第 (a) 項）。

次に、本条において国防長官に策定が命じられているフレームワークには、以下の要素が含まれていなければならないとされている（本条第 (b) 項）。

① 技術及び機密指定された情報の保護と、技術及び機密指定された防衛情報（classified defense information）を共有する際の要件とのバランスをとるための指針。
② 本条第 (d) 項に従い、国防総省における技術移転と対外情報開示に関する指針及び手続の改訂に活用する目的で、連邦行政機関及び産業界の利害関係者から意見を募集し、検討し、適切な場合にはこれらを採用するための手続。
③ 国防機密情報に関する開示指針（National Disclosure Policy）の改訂にあたり、新興・先端防衛技術の利用に対処するための勧告。なお、この新興・先端防衛技術には、人工知能、指向性エネルギー、マイクロ波システム、対無人航空システム、ミサイル防衛、サイバーセキュリティ、量子技術、極超音速技術、自律システム、

[5] *See* Military Surface Deployment and Distribution Command, Transportation Engineering Agency, Strategic Rail Corridor Network (STRACNET) & Defense Connector Lines (2023 ed.) at 6.