トランプ政権におけるサイバーセキュリティ政策の現状

中沢　潔
JETRO/IPA New York

1　サマリー

トランプ大統領は 2017 年 5 月 11 日、米国のサイバーセキュリティ強化に関する大統領令に署名した。度重なる修正の末、トランプ大統領の就任 111 日目にようやく発出された同大統領令は、同政権初の主要サイバーセキュリティ政策措置である。

3 つの最優先事項として、①連邦政府のネットワークに関するサイバーセキュリティ、②重要インフラに関するサイバーセキュリティ、③国家／国民のためのサイバーセキュリティ、に関する内容が記述されており、各連邦政府機関の長に対し、期限以内に大統領に報告書を提出するよう指示している。

同大統領令の内容は、ブッシュ政権及びオバマ政権が推進してきたサイバーセキュリティ政策の方向性を即座に変えるものではないが、改善策として以下を掲げている。

- *連邦政府機関の長に対し直接的なサイバーセキュリティリスクの管理責任を賦課*
- *NIST のサイバーセキュリティ・フレームワークの活用を連邦政府機関に義務付け*
- *連邦 IT システムの近代化計画の推進*
- *高いリスクにさらされている重要インフラの防護及びサイバーインシデント対策の強化*
- *国際連携や将来的なサイバーセキュリティ人材育成を重視*

草案段階では批判の多かったものの（例えば、国防総省の権限の強化が含まれており、安全保障上のデジタル監視活動が強化される可能性を懸念する声があった。）、その後多数の連邦政府機関の関係者及びサイバーセキュリティ政策の専門家の意見を取り入れながら修正を重ねた結果、連邦政府のサイバーセキュリティ対策の方向性を明確に示すものとして概ね評価するメディアや専門家の声は多く、トランプ大統領がこれまで発出した中で最も異論の少ない大統領令の一つといえる。

一方で、政策の実効性や有効性に懐疑的な見解を示す声もあり、専門家の間でも具体的な政策内容に関する見解は分かれている。多くの専門家は、サイバーセキュリティを強化する上で計画立案及び情報収集は重要であるが、サイバーセキュリティ大統領令が長期的に成功を収めるには、こうした戦略策定期間から早急に抜け出し、新たなランサムウェアの脅威などから重要インフラを事前に防護するための強固な国家サイバーセキュリティ措置を一刻も早く実行に移す必要があると考える。しかし、サイバーセキュリティ大統領令で提示されている主要政策が実施される具体的な時期については、少なくとも数年を要するとみられている。

ホワイトハウスは 2017 年 9 月時点で、これまで連邦政府機関から提出された報告書の数や内容について詳細を明らかにしていない[1]が、大統領技術評議会（ATC）が国家安全保障省（DHS）、行政管理予算局（OMB）、連邦調達庁（GSA）と共同で取りまとめた連邦政府の IT システム近代化に関する報告書を 8 月末に発表しており、米議会はこれらの報告書や今後提出される報告書の監督活動等に追われることになり[2]、同大統領令に基づき、拡大する新たなサイバー脅威に効果的に対応するための具体的な措置を講じるため、今後は議会が主要な役割を果たす。

[1] トランプ政権は、サイバーセキュリティ大統領令で義務付けている報告書の内容公開とその公開時期は、報告書により異なるとしている。
[2] https://insidecybersecurity.com/daily-news/trump-cyber-order-begins-producing-deliverables-congress-steps-review-

同大統領令では、連邦 IT システム近代化の取組みと並行して、電子メール、クラウド、サイバーセキュリティサービスを含む連邦政府機関の IT 調達において共有型 IT サービスを可能な限り選好することが求められており、連邦 IT 調達市場に多大な影響を与えると見込まれている。特に、クラウドサービスは、クラウドベースの政府デジタルプラットフォームの構築を目指すトランプ政権において最も注目されている。また、IT ベンダが連邦政府向けに取るべきマーケティング戦略については、多数のレガシーシステムを近代化するためにかかるコストや複雑なプロセス、時間を縮減するだけでなく、セキュリティを担保できることを前面に押し出すことが重要となると考えられる。

連邦政府機関の IT システム近代化イニシアチブは、具体的には、トランプ大統領直属の米イノベーション・オフィス及び大統領技術評議会（ATC）が Amazon 社、Apple 社、Microsoft 社、IBM 社を含む大手テクノロジー企業の CEO を含む民間セクタと連携しながら主導することになっており、企業は、同大統領令におけるサイバーセキュリティ・フレームワークの活用義務付け等により新たなセキュリティ要件が求められる可能性を含め、その動向を注視する必要がある。また、連邦政府レベルにおいては、2017 年 1 月に連邦調達庁（GSA）が契約・資金提供方法を簡素化し、政府機関におけるクラウドサービスの活用を加速化する目的で立ち上げた省庁横断組織、クラウド・センター・オブ・エクセレンス（CCoE）が 8 月末、政府機関におけるクラウドサービス調達プロセスのベストプラクティス指針として「クラウド調達責任者向けクラウド導入のサバイバル、ヒント、教訓と経験ガイド」を取りまとめ 、これまでクラウド化を実現した政府経験に基づいて政策を積極的に後押しする動きがみられ、企業はこうした動向にも注意する必要がある。

その他のサイバーセキュリティ政策の主な動きも併せて報告する。

efforts

2　サイバー防衛強化を目指すトランプ大統領のサイバーセキュリティ政策

（1）　2017 年 5 月に発出された米国のサイバーセキュリティ強化に関する大統領令の概要

トランプ大統領は 2017 年 5 月 11 日、待望されていた米国のサイバーセキュリティ強化に関する大統領令（「連邦政府のネットワーク及び重要インフラのサイバーセキュリティ強化に関する大統領令（Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure）」、以下「サイバーセキュリティ大統領令[3]」）に署名した。度重なる修正の末、トランプ大統領の就任 111 日目にようやく発出された同大統領令は、同政権初の主要サイバーセキュリティ政策措置である。

図表 1：サイバーセキュリティ大統領令に署名するトランプ大統領

※大統領署名への同席者は左から国家安全保障会議（NSC）の Josh Steinman 氏、ホワイトハウスのサイバーセキュリティ・コーディネーターの Rob Joyce 氏、国土安全保障省（DHS）補佐官の Tom Bossert 氏。
出典：CNET[4]

a.　サイバーセキュリティ大統領令発出までの経緯

トランプ大統領は、大統領選挙に介入したロシアのサイバー攻撃問題[5]を背景に、就任後 90 日以内に特別チームを編成してサイバー攻撃対策を包括的に見直し強化するための報告書をまとめる考えを大統領就任直前に明らかにするなど、サイバーセキュリティ政策を優先して取り組むべき最重要政策に据えて取り組むことを公言していた。トランプ大統領は、当初、就任後間もない 2017 年 1 月末に、各連邦省庁の長官に IT システムの刷新と官民連携でサイバーセキュリティ問題に取り組むことを義務づけるサイバーセキュリティ大統領令に署名する予定であった。当初の大統領令草案は、米国防総省（Department of Defense：DoD）に連邦政府の IT システムや重要インフラの脆弱性について見直す権限を付与し、米国家情報長官（Director of National Intelligence）に米国にサイバー脅威をもたらす敵リストを作成することなどを含む内

[3] https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal
[4] https://www.cnet.com/news/president-trump-signs-cybersecurity-executive-order/
[5] 大統領選挙期間中、民主党全国委員会（Democratic National Committee）のシステムがハッキングされ、機密情報を含むメールが流出した事件で、米政府はこれを共和党のトランプ大統領候補を勝たせるために大統領選に影響を与える目的でロシア政府が関与したと主張している。

容であったが、その後、より幅広い連邦政府機関の関係者やサイバーセキュリティ専門家からの意見を取り入れる必要があるとの判断から、同案への署名は見送られた[6]。

2017 年 5 月 11 日のサイバーセキュリティ大統領令発出に際し記者会見した国土安全保障省（Department of Homeland Security：DHS）補佐官の Tom Bossert 氏は、発出に時間を要した理由について、トランプ政権が並行して推進する連邦政府の IT システム刷新の取組みとの関係のほか、連邦捜査局（Federal Bureau of Investigation：FBI）や米司法省（Department of Justice：DoJ）等の関連省庁のサイバーセキュリティ対策費増加を提案する大統領予算案の発表を待つ必要があったことを挙げている[7]。

サイバーセキュリティ大統領令の発出に先立つ 5 月 1 日、トランプ大統領は、連邦政府の IT システム及びデジタルサービスの近代化に向けて、政府機関全体における IT ビジョン・戦略・方向性を調整し IT 活用について勧告する新組織で大統領自らが議長を務める「大統領技術評議会（American Technology Council：ATC[8]）」を立ち上げる大統領令に署名した[9]。ATC は、ホワイトハウスの戦略的イニシアチブ担当長官を務める Chris Liddell 氏がその運営責任を担い、副大統領、国防長官、商務長官、国土安全保障長官、国家情報長官、Jared Kushner 氏をはじめとする大統領顧問のほか、ホワイトハウスのテクノロジー担当責任者などから構成され、トランプ政権は、サイバーセキュリティ政策同様、各政府機関の長が責任を持って IT システム改革を推進するよう促している[10]。また、トランプ大統領は、2017 年 3 月に発表した 2018 年度大統領予算案[11]で、500 億ドル以上に上る国防予算の大幅な引き上げに加え、主に民間セクタにおけるサイバーセキュリティ対策に責任を負う FBI や DoJ、DHS に対するサイバーセキュリティ対策資金も増額[12]させている。こうした経緯を踏まえて、Bossert 氏は、今回のサイバーセキュリティ大統領令発出は、「早過ぎも遅過ぎもしない絶好のタイミングで出された」との考えを示している。

b. サイバーセキュリティ大統領令の主な内容

サイバーセキュリティ大統領令における実質的なサイバーセキュリティ対策は、3 つの最優先事項として、①連邦政府のネットワークに関するサイバーセキュリティ、②重要インフラに関するサイバーセキュリティ、③国家／国民のためのサイバーセキュリティ、に関する内容が 3 セクションに記述されており、各連邦政府機関の長に対し、期限以内に大統領に報告書を提出するよう指示している。以下の表に、各セクションの主要内容を整理する。

[6] http://www.zdnet.com/article/trump-signs-impossible-cybersecurity-order-say-critics/
https://www.tripwire.com/state-of-security/government/100-days-office-president-trump-digital-security/
[7] http://www.defenseone.com/politics/2017/05/trump-releases-long-delayed-cyber-order/137791/
[8]ATC の運営責任者は、ホワイトハウスの戦略的イニシアチブ担当長官を務める Chris Liddell 氏で、その他のメンバーには、副大統領、国防長官、商務長官、国土安全保障長官、国家情報長官、大統領顧問などが含まれる。
[9] https://www.whitehouse.gov/the-press-office/2017/05/01/presidential-executive-order-establishment-american-technology-council
[10] http://www.nextgov.com/cio-briefing/2017/05/trump-creates-new-tech-council-tackle-federal-it-modernization/137455/
[11] https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/budget/fy2018/2018_blueprint.pdf
[12] トランプ大統領は、FBI や DoD による犯罪者やテロリストの暗号化された通信ツールの解読を支援する取組みに 6,100 万ドルの予算増のほか、DHS 予算を前年度比およそ 7%増となる約 440 億ドルを割り当てることを提案している。
http://www.nextgov.com/cybersecurity/2017/03/what-trumps-skinny-budget-says-about-cybersecurity/136217/

図表 2:サイバーセキュリティ大統領令の主要内容

	①連邦政府のネットワークに関するサイバーセキュリティ	②重要インフラに関するサイバーセキュリティ	③国家／国民のためのサイバーセキュリティ
政策方針	政府は米国民の情報／データを守る義務があり、各政府機関の長は、各々のリスク管理責任を負い、政府全体で政府の IT システムを 1 つのエンタープライズネットワークと捉え、管理する	米国政府は、その権限及び能力を活用し、米国の重要インフラの所有者と運用者によるサイバーセキュリティリスク管理の取組みを支援する	将来世代に向けてインターネットの価値を維持するため、オープンかつ相互運用可能で信頼できる安全なインターネットを推進し、プライバシーを守り、障害・詐欺・盗難を防止しながら、能率、イノベーション、コミュニケーション、経済繁栄を促進する。また、政府はサイバースペースにおける米国の目標を達成する基礎として、サイバーセキュリティと関連分野に長けた人材育成・維持を支援する
対策	・米国立標準技術研究所（NIST）の定めるサイバーセキュリティ・フレームワークの活用を各連邦政府機関に求め、各政府機関の長にリスク管理責任を負わせる ・各連邦政府機関は、IT 調達において共有型 IT サービス（shared IT services）を選好しなければならない	・公衆衛生／安全、経済の安定、又は国家安全保障に地域／全国規模で破滅的な影響を及ぼす恐れのある非常に高いサイバー攻撃リスクにさらされている重要インフラ[13]を効果的に防護し、リスク軽減につながる方策を特定する ・重要インフラのサイバーセキュリティリスク管理における市場の透明性を高め、コンピューターを乗っ取り、有益情報を盗んだり、DDoS（Distributed Denial of Service）攻撃を仕掛けるボットネットによるサイバー脅威を軽減するための戦略を策定する	・国際連携の下、国内外における敵からの攻撃を抑止し、サイバー脅威から米国民をより良く防護するための戦略を策定する ・将来に向けて必要なサイバーセキュリティ人材を育成する
報告書の提出義務	・各連邦政府機関の長は、NIST のフレームワークの実施に関する計画を含むリスク管理報告書を 90 日以内に作成し、国土安全保障長官及び行政管理予算局（OMB）局長は、その後共同で報告書を評価し、60 日以内に大統領に報告する ・大統領技術評議会（ATC）の責任者は、DHS、OMB、連邦調達庁（GSA）、商務省（DoE）の長官と共同で、府の統合ネットーワークアーキテクチャ及び共有型 IT サービスへの移行可能性に関して 90 日以内に大統領に報告する	・国土安全保障長官は、国防長官、司法長官、国家情報長官、FBI 長官、その他重要インフラ関連所管官庁の長と協力し、180 日以内に重要インフラを効果的に防護し、リスク軽減につながる方策について大統領に報告する ・国土安全保障長官とエネルギー省（DoE）長官は、国家情報長官及び州地方政府の長と連携し、90 日以内に重大なサイバーインシデントに伴う電力供給障害で予測される範囲／期間と、こうしたインシデントへの対応力、同インシデントに対応するために必要なアセット等について評価する ・国土安全保障長官と商務長官は、国防長官、司法長官、FBI 長官重要インフラ関連所管官庁の長、連邦通信委員会（FCC）委員長、連邦取引委員会（FTC）委員長と協力し、ボットネットによるサイバー脅威を軽減するための戦略策定を行い、240 日以内に仮報告書を作成、1 年以内に大統領に最終報告を行う ・国土安全保障長官、国防長官、FBI 長官、国家情報長官は米国の防衛産業のサプライチェーンや軍事プラットフォーム／システム／ネットワーク／機能などを含む防衛産業基盤が直面するサイバーセキュリティリスクと軽減策について 90 日以内に大統領に報告する	・国土安全保障長官、国防長官、国務長官、財務長官、商務長官、司法長官、国家情報庁長官、90 日以内に米通商代表部（USTR）は、国内外における敵からの攻撃を抑止し、サイバー脅威から米国民をより良く防護するための戦略に関する報告を共同で行う ・国土安全保障長官、国防長官、国務長官、財務長官、商務長官、司法長官、FBI 長官は、45 日以内に国際的なサイバーセキュリティ対策における捜査、特定、サイバー脅威情報の共有、対応、能力育成、協力等に関する優先事項について大統領に個々に報告する。また、国務長官は他の組織の長と連携し、90 日以内にサイバーセキュリティの国際連携戦略について大統領に報告する ・国土安全保障長官、国防長官、商務長官、労働長官、教育長官を含む関連組織の長は、将来の米国におけるサイバーセキュリティ人材育成の取組み範囲・十分性について共同で評価し、120 日以内に大統領に報告する。また、国家情報長官は、米国のサイバーセキュリティ上の競争力に長期的に影響すると考えられる諸外国の人材育成活動を評価し、60 日以内に大統領に報告する

出典:各種資料[14]を基に作成

[13] これらの重要インフラは、オバマ前大統領が 2013 年 2 月に発出した重要インフラへのサイバー攻撃に対するセキュリティ強化を推進する大統領令のセクション 9 を受けて特定されているが、詳細情報は公開されていない。

[14] https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal、
https://www.apks.com/en/perspectives/publications/2017/06/president-trumps-executive-order-on-cybersecurity

c. サイバーセキュリティ大統領令の主要ポイントとオバマ政権からの変更点

連邦 IT システムの脆弱性を検知しシステム強化を図る上で、各連邦政府機関におけるサイバーセキュリティ対策と時代遅れの IT システム／ネットワークの包括的な見直しに焦点が置かれているトランプ大統領のサイバーセキュリティ大統領令の内容は、「前政権の取組みに基づくものである」と Bossert 氏が記者会見で説明したように、その内容は、ブッシュ政権及びオバマ政権が推進してきたサイバーセキュリティ政策の方向性を即座に変えるものではない。

オバマ政権時代に米国家安全保障会議（National Security Council：NSC）のサイバーセキュリティ政策長官を務めた Ben Flatgard 氏は、2015 年 6 月に米連邦人事管理局（Office of Personnel Management：OPM）がハッキングの被害に遭い、2,100 万人以上の個人情報が流出した事件を受けて 2016 年 2 月にオバマ政権が発表した米国のサイバーセキュリティ強化策である「サイバーセキュリティ国家行動計画（Cybersecurity National Action Plan：CNAP）[15]」の起草に関与した人物の一人である。同氏は、トランプ大統領のサイバーセキュリティ大統領令について、CNAP の主要項目を推進するものであり、これまで任意の適用が推奨されてきた米国立標準技術研究所（National Institute of Standards and Technology：NIST）のサイバーセキュリティ・フレームワークの活用を連邦政府のリスク管理対策として義務付けるなど、前政権で定められた政策路線を維持しながら漸進的な改善を図っていると語る[16]。

また、Bossert 氏は記者会見で、「オバマ政権下で米国のサイバーセキュリティ政策は大きく進歩したが、十分な対策とは程遠い」と述べ、トランプ政権のサイバーセキュリティ大統領令を前政権からの取組みに基づく改善策として提示[17]しているが、その主要ポイントは以下の通り[18]。

- *連邦政府機関の長に対し直接的なサイバーセキュリティリスクの管理責任を賦課*— サイバーセキュリティ大統領令は、各連邦政府機関の IT 及びサイバーセキュリティ担当者ではなく、組織の長に対しサイバーセキュリティのリスク管理における最終責任を課すことを明示しており、各機関の長が主体的にリスク軽減対策を講じるよう求めている
- *NIST のサイバーセキュリティ・フレームワークの活用を連邦政府機関に義務付け*— オバマ前大統領による 2013 年 2 月の重要インフラへのサイバー攻撃に対するセキュリティ強化を推進する大統領令発出を受けて NIST が 2014 年 2 月に策定したサイバーセキュリティ・フレームワークは、任意のセキュリティガイドラインであるが、ベストプラクティスとしてこれまで民間企業を中心に幅広く活用されている。サイバーセキュリティ大統領令は、各政府機関に同フレームワークの活用を義務付け、そのための行動計画を作成するよう求めている
- *連邦 IT システムの近代化計画の推進*— サイバーセキュリティ大統領令は、連邦政府のサイバーリスクを一元化するため、各政府機関において共有型 IT サービスの活用を求め、コスト削減へとつなげる[19]政府 IT インフラ近代化計画を同時並行で推進しており、新システムへの移行や運用に伴うあらゆるリスクを特定するよう求めている

[15] 連邦政府の IT システムの近代化のため、30 億ドルを支出することや、シリコンバレーなどから最優秀人材を集め、政府全体におけるサイバー専門家集団を結成するなど、米国の政府・民間のサイバーセキュリティ対策を強化するため、190 億ドル以上の予算を割り当てることを提案している。https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan
[16] https://arstechnica.com/tech-policy/2017/05/the-text-and-subtext-of-trumps-cyber-executive-order/
[17] https://www.theatlantic.com/news/archive/2017/05/trump-signs-cybersecurity-order-hacking-election/526407/ http://www.politico.com/story/2017/05/11/trump-cyber-executive-order-238273
[18] https://www.pwc.com/us/en/cybersecurity/assets/initial-takeaways-president-trump-cybersecurity-executive-order-may-2017.pdf
[19] 2016 年 5 月に米会計検査院（GAO）が発表した報告書によると、2015 年における連邦政府の IT 予算の 75%（およそ 610 億ドル）をシステムの運用・維持費が占めていることが明らかになっている。 http://www.gao.gov/assets/680/677436.pdf

- *高いリスクにさらされている重要インフラの防護及びサイバーインシデント対策の強化*— サイバーセキュリティ大統領令は、特に高いサイバーリスクにさらされている重要インフラのセキュリティ対策のほか、通信分野におけるボットネット脅威対策、国防総省及び防衛産業におけるリスク管理改善策、サイバーインシデントに伴う電力供給障害対策の見直しを求めている
- *国際連携や将来的なサイバーセキュリティ人材育成を重視*— サイバーセキュリティ大統領令はサイバー攻撃抑止政策として、国際連携によるサイバースペースにおけるリスク軽減のための規範策定を推進しているほか、米国における長期的な競争優位性を維持するため、サイバーセキュリティ人材の育成に向けた取組みを強化するよう求めている

こうした点に加え、トランプ政権下におけるサイバーセキュリティ政策では、国防総省（DoD）の果たす役割が今後より強化される可能性が示唆されている。イスラム教徒の入国禁止を求めるなど、大統領候補時代から過激な発言を繰り返し強硬なテロ対策を推し進める考えを示していたトランプ大統領は、2015 年 12 月にカリフォルニア州で発生した銃乱射テロ事件において、死亡した容疑者が使用していた iPhone 端末の暗号機能により捜査当局が情報を引き出すためのセキュリティ解除に時間を要した問題で、暗号化ツールがテロリスト等に対する犯罪捜査を妨げているという当局の見解を支持し、当局から下された暗号化機能の解除命令を断固拒否した Apple 社を痛烈に非難していた[20]。こうした背景から、国家安全保障問題を専門とする米シンクタンク、新アメリカセキュリティセンター（Center for a New American Security：CNAS）の上級研究員である Adam Klein 氏は、プライバシーの遵守と国家安全保障の均衡を重視したオバマ前政権とは対照的に、トランプ大統領は、2017 年 12 月末に期限切れとなる外国人の通信に対する傍受を原則的に合法化した外国情報監視法（Foreign Intelligence Surveillance Act：FISA）702 条の無条件延長に動く可能性を含め、今後政府によるデジタル監視活動を一層強化する可能性が高いとの見方を示している[21]。

これは、当初のサイバーセキュリティ大統領令草案は、民間部門におけるサイバーセキュリティ政策監督機関である国土安全保障省（DHS）と同等の権限を DoD に付与し、その役割を強化する内容であったことからも明らかであり、同案に対しては、顧客のプライバシー問題よりも安全保障上のデジタル監視活動が重視されるようになる可能性を懸念する民間企業や関連政府機関の関係者などから懸念の声が上がっていた[22]。こうした声を受け、最終的なサイバーセキュリティ大統領令では、関連する条項は削除され、重要インフラのサイバーセキュリティ政策における DHS の主導的役割を尊重する内容に修正された。しかし、重要インフラのサイバーセキュリティ対策の見直しには、他の関連所管官庁に加え国防長官も協力するよう求めているほか、サイバー攻撃抑止に向けた国際連携の取組みでは、国土安全保障長官、国防長官、国務長官、財務長官、商務長官、司法長官、FBI 長官が共同でサイバーセキュリティの国際連携戦略を策定するよう求めるなど、DoD が米国のサイバーセキュリティ政策において果たす役割はこれまでより拡大しており[23]、今後の動向を注視する必要がある。

d. サイバーセキュリティ大統領令に対する有識者の評価

草案段階では批判の多かったものの、その後多数の連邦政府機関の関係者及びサイバーセキュリティ政策の専門家の意見を取り入れながら修正を重ねて発出されたサイバーセキュリティ大統領令は、連邦政府のサイバーセキュリティ対策の方向性を明確に示すものとして概ね評価するメディアや専門家の声は多く、トランプ大統領がこれまで発出した中で最も異論の少ない大統領令の一つといえる。一方で、政策の実効性や有効性に懐疑的な見解を示す声もあり、専門家の間でも具体的な政策内容に関する見解は分かれている。

図表 3：サイバーセキュリティ大統領令に対する主な有識者の意見

[20] https://www.eff.org/deeplinks/2016/12/trump-and-his-advisors-surveillance-encryption-cybersecurity
[21] https://www.csoonline.com/article/3172933/security/what-to-expect-from-the-trump-administration-on-cybersecurity.html
[22] https://www.theguardian.com/us-news/2017/jan/31/trump-cybersecurity-order-pentagon-surveillance
[23] http://www.mcclatchydc.com/news/nation-world/national/national-security/article150066642.html

評価する意見	• 現在、すべての連邦政府機関はそれぞれ固有のサイバーセキュリティプロセスに従って独自システムのセキュリティを管理しているが、サイバーセキュリティ大統領令は政府全体を 1 つのエンタープライズと捉え、そのセキュリティを包括的に管理するよう義務付け、個別のシステムごとにセキュリティプロトコルを構築するのではなく、各政府機関における全ての人、プロセス、ポリシーを分析・報告する必要性を認識しており、これはサイバーセキュリティに対する連邦政府の見方が大きく文化的にシフトしたことを意味する（Mike Shultz 氏、テキサス州に拠点を置くサイバーリスク管理サービス企業 Cybernance 社 CEO） • サイバーセキュリティ監査とリスク軽減に向けた計画は、あらゆる企業にとって肝心なものとなっており、連邦政府機関もその精査を受けなければならない。ビジネスの世界では、こうした計画はビジネスリスク評価活動の一部であり、ただ単に計画を有しているだけではいけない（Jess Richter 氏、カリフォルニア州に拠点を置くサイバーセキュリティ分析企業 DarkLight Cyber 社最高販売責任者） • サイバーセキュリティ大統領令は、各連邦政府機関の長に対し、各組織の現在のサイバーセキュリティ体制の総責任を負わせるだけでなく、サイバーセキュリティリスクをどの程度戦略的に捉え、どのような要因に基づいて優先順位に関する決定を行ったかを示すよう求めており、こうした報告書作成を行うことは各機関にとって非常に貴重な訓練の機会を提供するものである（Kevin Magee 氏、カリフォルニア州に拠点を置くネットワークトラフィックの可視化ソリューションを提供する企業 Gigamon 社グローバルセキュリティ・ストラテジスト）
批判的（課題・懸念を示す）意見	• サイバーセキュリティ大統領令の内容は、官民連携のアプローチというより、主に政府が政策の思案や施行を行うものであり、米国が火急の対応を必要とするサイバー脅威に民間主導で実行すべき課題について言及されていないのは残念であり、政府機関よりも民間の対応力を概して高く評価しているトランプ政権の政策としてはいくぶん驚きである（Daniel Castro 氏、米シンクタンクの情報技術とイノベーション財団（Information Technology and Innovation Foundation：ITIF）バイスプレジデント） • サイバーセキュリティ大統領令は NIST のサイバーセキュリティ・フレームワークの活用を義務付けているが、同フレームワークを用いてリスク評価を行うことと、リスク評価で特定した問題を修正するために行動を起こすことは全く別物であり、政府機関にフレームワークツールの活用法についての研修を義務付けておらず、政府機関内におけるツールの最善の活用法や問題に対する修正策、ツールでは対応できない問題や問題に対応しなかった場合の結果について一致した意見はない。サイバーセキュリティ大統領令の内容を期限内に実行するのは非常に難しいだろう（John Kronick 氏、カナダに拠点を置くクラウドサービス企業 Stratiform 社 ATG サイバーセキュリティソリューション担当ディレクタ） • 共有型サービスにより連邦政府の IT システムを一元化することは、単一の政府機関が最も聡明で有能な人材・システムを採用すれば、全ての政府機関もその利益を受けられる一方で、セキュリティ上の穴が一箇所でも見つかり、共有型 IT インフラにアクセスできれば、あらゆる連邦機関のシステムへの侵入を許すことになる（John Bambenek 氏、メリーランド州に拠点を置く高度なサイバー脅威・情報漏洩防止ソリューションを提供する企業 Fidelis Cybersecurity 社脅威リサーチマネージャー） • 議会がタイムリーに予算を成立させられなければ、多くの政府機関はセキュリティ対策の改善に必要な投資をすぐに実施できない。例え利用できる資金があっても、連邦調達規則（Federal Acquisition Regulations）によりテクノロジーの調達プロセスに長期間を要する可能性があり、資金や法令の整備が必要である（John Chirhart 氏、メリーランド州に拠点を置くネットワークセキュリティソリューションを提供する企業 Tenable Network 社連邦技術ディレクタ） • サイバーセキュリティ大統領令は連邦政府内の監督権限の集約を目指していると思われ、サイバーセキュリティの管理責任を一元化するために連邦最高情報セキュリティ責任者（Federal Chief Information Security Officer（連邦 CISO））を据え、投資の優先順位や計画実行の監督を任せるのは理にかなっている。しかし、連邦 CISO のポストは空席のままであり[24]、大統領令に従って様々な報告書から必要な改善が特定されたとしても、政府のサイバーセキュリティニーズへの対応はサイロ化されたバラバラのアプローチで行われる可能性がある（Kevin Magee 氏）

出典：各種資料[25]を基に作成

[24] 連邦 CISO は、他の連邦政府機関の CISO 及びセキュリティ予算・プログラムを統合管理する目的で 2016 年 9 月に新設され、退役准将の Gregory Touhill 氏が初代連邦 CISO に任命されたが、同氏はトランプ大統領就任直後に辞任しており、以後、連邦 CISO のポストは空席のままとなっている。

[25] http://searchsecurity.techtarget.com/news/450418734/Trump-cyber-executive-order-focuses-on-cyber-risk-

（2） 今後の展望

a. サイバーセキュリティ大統領令の施行における今後の見通し

オバマ政権時代にホワイトハウスのサイバーセキュリティ・コーディネーターを務めた Michael Daniel 氏は、トランプ大統領のサイバーセキュリティ政策の方向性を高く評価する一方、各政府機関による報告書の提出とその評価プロセスを経てさらなる具体的なサイバーセキュリティ対策を講じる必要があるとし、サイバーセキュリティ大統領令は「新たな計画を立てるための計画（a plan for a plan）」にすぎないとの考えを示している[26]。サイバーセキュリティを強化する上で計画立案及び情報収集は重要であるが、サイバーセキュリティ大統領令が長期的に成功を収めるには、こうした戦略策定期間から早急に抜け出し、「WannaCry[27]」を含む新たなランサムウェアの脅威などから重要インフラを事前に防護するための強固な国家サイバーセキュリティ措置を一刻も早く実行に移す必要があると考える専門家は多い。

しかし、サイバーセキュリティ大統領令で提示されている主要政策が実施される具体的な時期については、少なくとも数年を要するとみられている。例えば、同大統領令は、連邦政府のネットワークに関するサイバーセキュリティでは各連邦政府機関によるセキュリティ問題の評価を 90 日以内に実施した後、これらの問題に対応するため、DHS と共同で、OMB に必要な政策予算について 60 日以内に提示・評価するよう求めているが、Flatgard 氏は、OMB が例え期日（2017 年 10 月はじめ）通りに予算を提示できたとしても、その政策措置が実際に講じられるのは最も早くて 2019 年又は 2020 年の予算になるとの見通しを示している[28]。

ホワイトハウスは 2017 年 9 月時点で、これまで連邦政府機関から提出された報告書の数や内容について詳細を明らかにしていない[29]が、サイバー攻撃に対する国際連携に関する報告書のほか、重要インフラの市場透明化、電力インフラのインシデント対応能力、防衛産業基盤に対するサイバーリスク、サイバー抑止における戦略的選択肢に関する報告書の提出期限は既に過ぎている。また、ホワイトハウスは、大統領技術評議会（ATC）が DHS、OMB、GSA と共同で取りまとめた連邦政府の IT システム近代化に関する報告書を 8 月末に発表しており、米議会はこれらの報告書や今後提出される報告書の監督活動に追われることになる[30]。議会では、秋以降、サイバーセキュリティの抑止、コネクテッドカーのセキュリティ、連邦政府の IT 近代化、強健なサイバーセキュリティ人材の育成など多数のサイバーセキュリティ関連法について議論される見込みであり、サイバーセキュリティ大統領令に基づき、拡大する新たなサイバー脅威に効果的に対応するための具体的な措置を講じるために、今後は議会が主要な役割を果たす。

サイバーセキュリティ大統領令の施行に関連したこれまでの動きでは、上院国土安全保障・政府問題委員会（Senate Homeland Security and Governmental Affairs Committee）が連邦政府機関全体でサイバーセキュリティに関する規制措置を調整・簡素化するための中央組織を DHS 内に新設するための法案作成作業を主導している[31]。また NIST は、サイバーセキュリティ大統領令で新たに義務付けられた連邦政府機

---

management
https://www.bankinfosecurity.com/blogs/trumps-cybersecurity-executive-order-will-be-judged-by-action-inspires-p-2523
https://www.cyberscoop.com/trump-signs-long-awaited-cybersecurity-executive-order/

[26] https://www.theatlantic.com/news/archive/2017/05/trump-signs-cybersecurity-order-hacking-election/526407/

[27] 古いバージョンの Microsoft Windows コンピューターを標的にしたワーム型ランサムウェアで、サイバーセキュリティ大統領令が発出された翌日の 2017 年 5 月 12 日から全世界の政府機関、企業、個人のコンピューターシステムで感染が拡大した。

[28] https://arstechnica.com/tech-policy/2017/05/the-text-and-subtext-of-trumps-cyber-executive-order/

[29] トランプ政権は、サイバーセキュリティ大統領令で義務付けている報告書の内容公開とその公開時期は、報告書により異なるとしている。

[30] https://insidecybersecurity.com/daily-news/trump-cyber-order-begins-producing-deliverables-congress-steps-review-efforts

[31] https://insidecybersecurity.com/daily-news/johnson-calls-central-authority-perhaps-dhs-coordinate-cyber-regulation

関におけるサイバーセキュリティ・フレームワークの導入を支援するため、大統領令発出直後、同フレームワークを活用して各連邦政府機関がリスク管理計画を策定、実施、改善するための方法をベストプラクティスとしてまとめた組織内文書（Interagency Report：IR）「連邦政府機関に対するサイバーセキュリティ・フレームワークの施行ガイダンス（The Cybersecurity Framework: Implementation Guidance for Federal Agencies）」の草案を発表[32]しているほか、2017 年 8 月末、SP 800-37「連邦政府情報システムに対するリスク管理フレームワーク適用ガイド（Guide for Applying the Risk Management Framework to Federal Information Systems）」の改訂版[33]を間もなく発出する計画を明らかにしている[34]。さらに NIST は、フレームワーク標準及びサプライチェーンのリスク管理に対する評価指標に関する新条項を含むサイバーセキュリティ・フレームワークの改訂作業（第 1.1 版改訂案）も進めており、その第 2 草案を今秋発表予定である[35]。こうした進展がある一方で、2017 年 8 月末、米国家インフラ諮問委員会（National Infrastructure Advisory Council：NIAC[36]）の 28 名の委員のうち 8 名が辞任を表明[37]したことを受け、業界では大統領令の施行に遅れをきたす可能性が懸念されており[38]、今後の行方が注目される。

b. 連邦 IT 調達市場への影響

サイバーセキュリティ大統領令では、連邦 IT システム近代化の取組みと並行して、電子メール、クラウド、サイバーセキュリティサービスを含む連邦政府機関の IT 調達において共有型 IT サービスを可能な限り選好することが求められており、連邦 IT ベンダ市場に多大な影響を与えると見込まれている。特に、クラウドサービスは、クラウドベースの政府デジタルプラットフォームの構築を目指すトランプ政権において最も注目されている。

米国では、前オバマ政権が 2010 年に掲げた「クラウド・ファースト（Cloud First）」政策において、連邦政府の IT インフラの近代化ソリューションとしてクラウド化が推進されてきた。同政策により、内務省（Department of Interior）が 2012 年に組織全体におけるクラウド電子メールサービス契約を Google 社と、中央情報局（Central Intelligence Agency：CIA）が 2013 年に Amazon 社と Amazon Web Services（AWS）を採用したクラウドコンピューティングプラットフォーム導入契約をそれぞれ締結するなどして話題を集めたが、連邦政府全体におけるクラウドサービスの利用は遅々として進んでいない。この理由の一つとして、オバマ政権下では 2011 年 12 月、各政府機関におけるクラウドサービスの活用を加速化するため、連邦政府におけるクラウドサービス調達のための共通セキュリティ基準を定めた「連邦政府のリスク・認証管理プログラム（Federal Risk and Authorization Management Program：FedRAMP[39]）」が制定されたが、同プログラムに対しては、各省庁で求められるセキュリティ上のリスク許容度がかなり異なるため、運用認

[32] NIST は 2017 年 6 月 30 日まで同案に対する意見募集を行っていた。https://www.assured.enterprises/nist-issues-guidance-on-federal-government-cybersecurity-best-practices/
[33] 同改訂版は、NIST のサイバーセキュリティ・フレームワーク標準を連邦情報セキュリティ管理法（Federal Information Security Management Act：FISMA）で定められているセキュリティ評価指標を基に評価することを主な目的としている。
[34] https://insidecybersecurity.com/daily-news/nist-eyeing-trump-order-incorporates-cyber-framework-risk-management-guide
[35] https://insidecybersecurity.com/daily-news/nist-issue-second-draft-framework-update-seeking-more-comment-metrics
[36] 2001 年の米同時多発テロ事件を受けて設立された組織で、大統領に米国の重要インフラに関する問題及びサイバーセキュリティについて勧告する役割を担っている。
[37] 辞任を表明した委員は、その理由として、2017 年 8 月中旬にバージニア州シャーロッツビル（Charlottesville）で起きた白人至上主義団体と反対派が衝突し死傷者が出た事件で、トランプ大統領が「双方に責任がある」と発言したことのほか、大統領選挙プロセスに影響するシステムを含む米国民にとって重要なシステムのサイバーセキュリティに対して増大する脅威に十分な注意を払っていないことなどを挙げている。https://www.rollcall.com/news/policy/members-trumps-infrastructure-panel-resign-protest
[38] https://www.wired.com/story/trump-cybersecurity-executive-order/
[39]連邦情報セキュリティ管理法（FISMA）の下で制定された FedRAMP は、連邦政府全体におけるクラウド コンピューティング製品・サービスの評価、監視及び認定方法に一定のセキュリティ基準を策定しており、そのセキュリティ標準は、NIST の策定する SP 800-53（連邦政府情報システムおよび連邦組織のためのセキュリティ管理策とプライバシー管理策）基準に基づいている。https://www.fedramp.gov/

定（authority to operate：ATO）を受けたサービスでも、各組織レベルでセキュリティ要件について再度確認する必要があり、認定プロセスの短縮とサービスの活用迅速化に必ずしもつながっていないことが挙げられる[40]。

OPM のハッキング被害による大規模な情報漏洩事件などを受け、政府の老朽化した IT システムに対するセキュリティリスクが高まる中、トランプ政権は、連邦政府機関全体で標準化されたサイバーセキュリティ上の防護機能とクラウド上のデータ暗号化機能を担保し、オープンなインターネットへのアクセスポイントを最小限にとどめた単一のネットワークインフラを官民連携で構築することを目指しており、各連邦政府機関がクラウドを中心とする共有型サービスを提供する IT ベンダのサービスをより容易に調達できるようにし、政府の IT システムの刷新及びセキュリティ強化を早急に進めたい考えである[41]。しかし、現時点で、サイバーセキュリティ大統領令における連邦政府のネットワークに関するサイバーセキュリティに関して、各政府機関のサイバーセキュリティリスク管理に関する報告書を統合政府戦略としていかに調整・合理化するかについて不明な点が多いことから、将来的な連邦 IT 調達市場への具体的な影響を予測できる段階にはない。

一方、IT ベンダが連邦政府向けに取るべきマーケティング戦略について、企業及び政府向けにソフトウェア及び情報ソリューションサービスを提供する米 Deltek 社のリサーチアナリストである John Slye 氏は、政府向けクラウドサービスでは、既に Amazon 社や Microsoft 社といった大手 IT 企業が積極的にサービスを提供しているが、今後クラウドサービスを提供する IT ベンダがクラウドサービスを売り込む上で、「多数のレガシーシステムを近代化するためにかかるコストや複雑なプロセス、時間を縮減するだけでなく、セキュリティを担保できることを前面に押し出すことが重要なセールスポイントとなる」と述べる。また、米 IT 市場調査会社 Gartner 社のリサーチ・バイスプレジデントを務める Katell Thielemann 氏は、連邦政府機関向けにこれまでサービスを提供してきた企業は、政府の求めるテクノロジー要件に対応するため継続的に投資を行ってきたが、今後のマーケティング戦略として、政府機関が共有型サービスを活用して中央デジタルプラットフォームへと移行することを考慮した上で必要なセキュリティ要件を満たすことのできるサービス提供に向け、主体的に投資する必要性を指摘している[42]。

連邦政府機関の IT システム近代化イニシアチブは、具体的には、トランプ大統領直属の米イノベーション・オフィス（Office of American Innovation：OAI[43]）及び大統領技術評議会（ATC）が Amazon 社、Apple 社、Microsoft 社、IBM 社を含む大手テクノロジー企業の CEO を含む民間セクタと連携しながら主導することになっており、企業は、サイバーセキュリティ大統領令におけるサイバーセキュリティ・フレームワークの活用義務付け等により新たなセキュリティ要件が求められる可能性を含め、その動向を注視する必要がある。連邦政府レベルにおいては、2017 年 1 月に連邦調達庁（General Services Administration：GSA）が契約・資金提供方法を簡素化し、政府機関におけるクラウドサービスの活用を加速化する目的で立ち上げた省庁横断組織、クラウド・センター・オブ・エクセレンス（Cloud Center of Excellence：CCoE[44]）が 8 月末、政府機関におけるクラウドサービス調達プロセスのベストプラクティス指針として「クラウド調達責任者向けクラウド導入のサバイバル、ヒント、教訓と経験ガイド（Cloud Acquisition Professionals Cloud Adoption Survival Tips, Lessons, and Experiences：CASTLE Guide）」を取りまとめ[45]、これまでクラウド化を実現し

[40] https://www.apks.com/en/perspectives/publications/2017/06/president-trumps-executive-order-on-cybersecurity
https://federalnewsradio.com/reporters-notebook-jason-miller/2017/05/new-cloud-buying-guide-underpins-it-modernization-bill-cyber-eo/
[41] https://www.govtechworks.com/how-cyber-executive-order-could-change-federal-it/#gs.EPUH1ls
https://about.bgov.com/blog/trumps-cyber-order-excites-government-contractors/
[42] http://www.ecommercetimes.com/story/84693.html
[43] 2017 年 3 月に発出された大統領令により、民間組織からの構想を基に連邦官僚制を改革することを目的に新設された組織で、トランプ大統領の娘婿で大統領上級顧問である Jared Kushner 氏が同組織の責任者を務めている。
[44] CCoE は、GSA、農務省（USDA）、DHS、FCC、米退役軍人省（VA）を含む 48 の省庁、140 名以上の政府関係者などから構成されており、FCC の CIO を務める David Bray 氏がその取組みを主導していたが、民間企業に移籍するため、2017 年 9 月末より USDA リスク管理局（Risk Management Agency）の CIO を務める Chad Sheridan 氏がその後継となる。
[45] CCoE は、今後数週間以内にクラウドサービスベンダや業界関係者から同ガイドに対する意見募集を行う計画である。

た政府経験に基づいて政策を積極的に後押しする動きがみられ、企業はこうした動向にも注意する必要がある。

3　他のサイバーセキュリティ政策の主な動き

（1）　NIST に対する連邦政府機関のサイバーセキュリティ対策に関する監査権限付与を巡る問題

下院 科学・宇宙・技術委員会（House Science, Space and Technology Committee）は 2017 年 3 月、同委員会委員長を務める Lamar Smith 下院議員（テキサス州選出）を含む共和党議員が中心となり、連邦政府機関のサイバーセキュリティ対策状況を NIST に監査させる法案（「NIST サイバーセキュリティ・フレームワーク評価及び監査法（NIST Cybersecurity Framework Assessment and Auditing Act[46]）」）を可決した。具体的に同法案は、NIST に対し各連邦政府機関におけるサイバーセキュリティ対策への初期評価を 6 カ月以内に実施し、最もセキュリティリスクの高い機関を優先して 2 年以内にその全面審査を完了するよう命じているほか、官民機関における NIST のサイバーセキュリティ・フレームワークの採用状況に関する年次報告書をホワイトハウス科学技術政策局（Office of Science and Technology Policy）が策定し、同フレームワークの普及に向けたより幅広い対策を講じるよう NIST に求めている。

NIST の権限拡大を提案する同案は、サイバーセキュリティ大統領草案段階から NIST のサイバーセキュリティ・フレームワークを連邦政府機関に義務付ける考えを示していたトランプ政権の政策方針と合致するものであり、同方針に従って各政府機関におけるセキュリティ対策についてより厳格な監査任務を担える組織は NIST 以外にないとして共和党議員の全面的な支持を得ている。一方で、同下院委員会ランキング・メンバーの Eddie Bernice Johnson 議員（民主党、テキサス州選出）をはじめとする民主党議員は、同案は文民政府機関におけるサイバーセキュリティ対策の主要責任を負う OMB 及び DHS の権限を NIST に委譲するものであり、サイバーセキュリティ標準の策定とあくまでその活用の勧告のみを行う機関として機能してきた NIST が他の政府機関のサイバーセキュリティ対策を監査することはできないと反対する姿勢を示し[47]、議論を呼んでいる。

同下院委員会での法案可決を受けて、NIST の情報セキュリティ及びプライバシーに関する諮問委員会（Information Security and Privacy Advisory Board：ISPAB）は 6 月末、同法案の内容に反対の意を示す書簡を NIST、商務省（Department of Commerce：DoC）、DHS、OMB の長に送付する計画を明らかにした。書簡では、監査機関となれば各組織における問題を検知し指摘する必要があることから、中立の勧告機関として先入観なく政府機関や業界との関係を維持することが困難になる可能性があること、また、NIST に対する関連予算が削減傾向にありリソースが不足状態にある[48]中で監査業務が新たに追加されることになれば、NIST がこれまで主要任務としてきたサイバーセキュリティの標準策定や教育活動に支障を来す恐れがあると警告している。同法案は関連予算の割り当てに関する言及を一切行っていないが、米議会予算

http://www.nextgov.com/cloud-computing/2017/08/heres-cloud-guide-written-feds-feds-will-white-house-listen/140478/

[46] https://www.congress.gov/bill/115th-congress/house-bill/1224/text?q=%7B%22search%22%3A%5B%22NIST+Cybersecurity+Framework%2C+Assessment%2C+and+Auditing+Act+of+2017%22%5D%7D&r=1

[47] http://www.nextgov.com/cybersecurity/2017/03/nist-enforcer-house-committee-passes-bill-expand-agencys-responsibilities/135805/?oref=ng-relatedstories
http://www.nextgov.com/cybersecurity/2017/03/nist-must-audit-federal-cybersecurity-because-dhs-isnt-hill-staffer-says/136638/

[48] トランプ大統領は、2018 年度大統領予算案において NIST に対する IT リサーチ関連の予算を 13%、サイバーセキュリティリサーチ関連の予算を 9%削減することを提案している。

局（Congressional Budget Office：CBO ）は同法案の実施にかかる費用は今後 4 年間で 4,800 万ドルに上ると推定している[49]。

NIST のサイバーセキュリティ・フレームワークが連邦政府機関における効果的なリスク管理策として義務付けられる中、新たなサイバー脅威に対する各機関のサイバーセキュリティ対策が十分であるかについて継続的にその進展・改善状況を監査する必要がある[50]。同法案はこうしたニーズを背景に策定されたが、民主党議員を中心に NIST の権限拡大に懸念を示す声は多い。しかし、現時点で法案内容が今後修正される可能性や下院本会議に法案が提出される時期、上院で関連法案が審議される計画などの詳細は明らかになっていない。

（2） NIST による SP800-53 改訂案の発出

NIST は 2017 年 8 月、NIST SP 800-53 の第 5 版改訂案「情報システムおよび組織のためのセキュリティ／プライバシー管理策（Security and Privacy Controls for Information Systems and Organizations）」を発表した[51]。SP 800-53 は元々、連邦政府機関が 2002 年に制定された連邦情報セキュリティ管理法（Federal Information Security Management Act：FISMA）に基づく連邦情報システムのセキュリティ標準及びガイドラインを提供するために策定されたもので、前回（第 4 版）の改訂は 2014 年に行われている。第 5 版改訂案は民間・防衛・情報機関の代表で構成されるタスクフォースにより策定された。

NIST は、今回の改訂案策定には、汎用コンピューターシステムやサイバーフィジカルシステム（CPS）、クラウド／モバイルシステム、産業／プロセス制御システム、IoT（Internet of Things）デバイスを含むあらゆる種類のプラットフォームを防護するために、幅広い官民組織が主体的かつ体系的に利用できる包括的なセキュリティ措置を講じる必要性が認識されたことが背景にあると説明している[52]。特に同案は、カメラ、センサー、音声コントロールツールをはじめとする IoT デバイスの普及に伴うプライバシー保護問題に新たに対応しており、改訂案策定のタスクフォースを主導する NIST フェローの Ron Ross 氏は、同案の発出に伴い、「これらのデバイスにおいて個人の特定が可能な情報をハッキング被害から保護するために、各セキュリティ／プライバシー担当者が協力して必要なプライバシー保護対策を講じることが重要である」と述べている[53]。
これまでの SP 800-53 改訂版は連邦政府機関（連邦情報システム）のみを対象としており、産業界を含めその他の機関が適応するか否かは自主的判断に任されていた。しかし第 5 版改訂案では、このようにセキュリティやプライバシーを保護しなければならない「システム」の対象が大幅に拡大したことで、企業のセキュリティ／プライバシー責任者やシステムエンジニアなどのニーズにも対応する内容となっている[54]。SP 800-53 の第 5 版改訂案における主要ポイントは以下の通り[55]。

[49] http://www.nextgov.com/cybersecurity/2017/06/cyber-advisory-board-gives-thumbs-down-nist-oversight-role/139135/
[50] https://www.csoonline.com/article/3219787/data-protection/achieving-long-term-resilience-with-nist-s-cybersecurity-framework.html
[51] http://csrc.nist.gov/publications/drafts/800-53/sp800-53r5-draft.pdf
[52] https://csrc.nist.gov/News/2017/NIST-Release-First-Draft-SP-800-53-Rev-5
[53] https://fedtechmagazine.com/article/2017/09/feds-get-new-guidance-nist-protect-data-iot-devices
[54] https://www.nist.gov/news-events/news/2017/08/nist-crafts-next-generation-safeguards-information-systems-and-internet
[55] https://www.lexology.com/library/detail.aspx?g=353b798e-e355-4f48-becb-c506fc3efc3e
https://insidecybersecurity.com/daily-news/nist-releases-proposed-update-federal-guidance-data-privacy-security-requirements

- 文書の表題から「連邦」の記載が削除され、ガイドラインの対象範囲の拡大に伴い「情報システム」の代わりに「システム」の用語が用いられており、連邦政府機関のみならず、州政府や地方自治体、民間企業がガイドラインとして活用するよう推奨している
- システムが扱う情報の重要性に応じて定められた最低限のセキュリティ要件に加え、プライバシー要件も提示している
- 連邦政府機関以外の組織の利便性を考慮し、セキュリティ／プライバシー管理策について、情報セキュリティ管理システムの国際規格である ISO/IEC27001 やセキュリティ管理策の NIST のサイバーセキュリティ・フレームワーク及び他のガイダンスとの整合性を図っており、システムエンジニアやソフトウェア開発者など、様々な立場にある関係者がニーズに応じてセキュリティ対策を選択できるようにしている
- 改訂案は、OPM のハッキング被害による大規模な情報漏洩事件を受け、前オバマ政権が 2016 年 7 月に発行した連邦政府機関の情報資産管理に関する「OMB 通達 A-130（OMB Circular A-130）」の改訂版で全ての連邦政府機関に義務付けられたリスクベースの情報・ネットワーク管理手法の採用と、トランプ政権が推進する連邦政府のデータ及びネットワークの保護に向けた取組みにも対応するガイダンスを提供している

同改訂案に対する意見募集を 2017 年 9 月 12 日まで実施していた NIST は、今後 10 月に最終改訂案を発出後、年末までに文書を最終化し発行する見込みである。

（3） IoT デバイスのセキュリティ対策に関する超党派法案

上院サイバーセキュリティコーカス（Senate Cybersecurity Caucus[56]）の共同議長を務める Mark Warner 上院議員（民主党、バージニア州選出）と Cory Gardner 上院議員（共和党、コロラド州選出）は 2017 年 8 月はじめ、他の上院議員 2 名と共同で、連邦政府機関向けに販売される IoT デバイスに一定のセキュリティ基準を求める内容の法案「IoT サイバーセキュリティ向上法（Internet of Things （IoT） Cybersecurity Improvement Act of 2017）[57]」を提出した。Gartner 社によると、世界における IoT デバイスの利用台数は 2017 年の 84 億台から 2020 年には 204 億台に達する見込みである[58]。しかし、IoT デバイスのセキュリティ対策は急激な市場成長の速度に追いついておらず、2016 年 10 月、DVR やウェブカメラなどのセキュリティが脆弱な IoT デバイスを利用した大規模な DDoS 攻撃により Netflix、Google、Twitter などの米大手ウェブサイトがダウンした事件[59]などを受け、IoT デバイスに対するセキュリティ懸念は高まっている。

こうした事態を背景に提出された同法案は、連邦政府機関に IoT デバイスを販売する企業に対し、販売時に既知のセキュリティ上の脆弱性問題への対策がとられていることや、セキュリティ上の脆弱性問題が発見された場合に適切なアップデートやセキュリティパッチを適用できるようにすること、変更できないハードコードのパスワード使用の禁止[60]を義務付けている。また同案は、全ての連邦政府機関に対し各機関で使用中の IoT デバイスとメーカー名のリストを作成・公開することや、善意で IoT デバイスの潜在的なセキュリティ問題を特定・報告したハッカーを刑事訴追から法的に保護することなどを提示している。Warner 上院議員は、同法案について、「IoT デバイス市場における明白な問題を修正し、関連デバイスメーカーによる製品のセキュリティ向上に向けた競争を促すことを期待するもの」とし、IoT デバイスの技術イノベーションを阻害せずにセキュリティを強化することが主な狙いであると説明する[61]。

[56] サイバーセキュリティに関する主要政策問題について議論するために両議院 2016 年に立ち上げた超党派の議員連盟。
[57] https://www.scribd.com/document/355269230/Internet-of-Things-Cybersecurity-Improvement-Act-of-2017
[58] http://www.zdnet.com/article/iot-devices-will-outnumber-the-worlds-population-this-year-for-the-first-time/
[59] https://www.cnet.com/how-to/ddos-iot-connected-devices-easily-hacked-internet-outage-webcam-dvr/
[60] これは、2016 年 10 月に起きた DDoS 攻撃で、ハッキングされた IoT デバイスのログインに用いられる認証パスワードに「admin」等のハッカーが容易に予想できるハードコードパスワードが用いられていたことが背景にある。
[61] https://www.warner.senate.gov/public/index.cfm/pressreleases?id=06A5E941-FBC3-4A63-B9B4-523E18DADB36

図表 4：IoT サイバーセキュリティ向上法案を共同提案した Mark Warner 上院議員

出典：Lima Charlie News

IoT デバイスの規制策定には慎重な姿勢を示す米政府であるが、インターネットセキュリティの第一人者でハーバード大学の講師を務める Bruce Schneier 氏を含む業界有識者は、「政府が介入しなければ手遅れになるまで市場は動かない」との見解を示し、今回の法案提出の動きを概ね歓迎している[62]。また、米データセキュリティ企業 Signal Sciences 社の戦略バイスプレジデントを務める Tyler Shields 氏は、同法案は IoT デバイスの最低限のセキュリティ標準を満たすことを企業に求めるもので、エネルギー使用に関するデータを収集するために GSA の建物に設置されているセンサーや、米海洋大気庁（National Oceanic and Atmospheric Administration：NOAA）が鯨の移動及び海底火山の調査に用いているセンサーなど、コスト削減や研究を目的として連邦政府機関が導入しているあらゆる IoT デバイスのセキュリティ問題を解決できるものでは到底ないとしている。一方で同氏は、「同法案が一般消費者向け IoT デバイスのセキュリティ強化に向けた基準策定のきっかけとなることを期待する」と述べており[63]、今後の法案審議の行方と同時に、これまで IoT デバイスのセキュリティ問題に目をそらしてきた業界への影響が注目される。

（4） 米サイバー軍の統合軍への昇格と NSA からの分離

トランプ大統領は 2017 年 8 月、米軍のサイバー戦争における米国の実行・防衛力を高めるため、米サイバー軍（US Cyber Command）を米太平洋軍（Pacific Command）や米中央軍（Central Command）を含む計 9 つの主要独立戦略部隊と同格の統合軍（Unified Command）に昇格するよう命じた[64]。DoD で過去数年間にわたり議論されてきたサイバー軍の統合軍への昇格は、2016 年 12 月に成立した 2017 年度国防権限法（National Defense Authorization Act for Fiscal Year 2017）の中に盛り込まれており、今回のトランプ大統領の発表はこの決定を公式に承認したことになる[65]。

米サイバー軍は、サイバースパイ等の脅威に対抗するため前オバマ政権下で 2009 年に創設されて以来、米国の核戦力部隊の統括とミサイル防衛を担う戦略軍（Strategic Command）の下に置かれており、米軍におけるサイバー戦の実行及び戦場の戦闘部隊が用いるネットワーク防衛戦略と調整しながら任務を遂行してきた。また、サイバー軍の指揮権は、これまで米国家安全保障局（National Security Agency：NSA）長

[62] https://limacharlienews.com/tech/internet-of-things-legislation/
[63] https://www.cnet.com/news/congress-senate-iot-device-makers-your-security-sucks/
[64] https://www.whitehouse.gov/the-press-office/2017/08/18/statement-donald-j-trump-elevation-cyber-command
[65] https://federalnewsradio.com/on-dod/2017/08/elevation-of-us-cyber-command-recognizes-its-coming-of-age/

官が兼任しており、サイバー軍の本部もメリーランド州フォート・ミード（Fort Meade）にある NSA 本部に置かれている[66]。

図表 5：現在 NSA のキャンパス内に設置されている米サイバー軍本部（左）とサイバー軍の統括責任を担う NSA の Mike Rogers 長官（右）

出典：The Washington Times[67]、FCW[68]

これは、サイバー軍が米国の主要諜報機関である NSA と様々なリソースを共有することで、サイバー軍に従事するハッカー及び組織の迅速な育成につなげたいとする政府の意図であったが、サイバー軍創設から 8 年が経過した現在、機密情報の収集を任務とする NSA とサイバースペースでの軍事目的達成を任務とするサイバー軍は相反する目的のために衝突することもあり、2 つの組織の間の緊張は近年高まりつつある。例えば、オバマ大統領が 2016 年、サイバー軍に対し、サイバースペースにおけるイスラム国への攻撃を強化するよう命じた際、イスラム国の通信インフラをシャットダウンすることを提案する軍と、サーバーは別の場所で簡単に再構築できることから、サーバーを停止させるよりもイスラム国がそのシステムに保有する情報を探ることが重要と考える NSA との間で摩擦が生じている[69]。

トランプ大統領は、サイバー軍を統合軍に昇格させる命令発令に伴い、国防長官に対し、NSA 長官が兼任していたサイバー軍の指揮権を分離させる可能性を検討するよう命じたことも明らかにしている。DoD の国土防衛・グローバルセキュリティ部（Homeland Defense and Global Security）次官補を務める Kenneth Rapuano 氏によると、サイバー軍が独立した統合軍となるには、新たな指揮官の指名と確定を待たなければならず、現時点で NSA の Rogers 長官に代わり新たなサイバー軍指揮官が就任する具体的な時期については決まっていないという。2017 年度国防権限法は、国防長官及び米統合参謀本部（Joint Chiefs of Staff）に対し、サイバー軍を NSA から分離させることでサイバースペースにおける米国の能力が損なわれないことを認証するよう義務付けており、同氏はこうしたプロセスにかかる時間を考慮すると、少なくともあと 1 年間は NSA 長官がサイバー軍の指揮官を兼任する体制が継続すると予測している[70]。

[66] サイバー軍に従事する人員数は軍民合計 700 名以上である。また、サイバー軍が統括する米軍所有の各サイバー部隊は拡充され、最終的には 133 チーム、約 6,200 人編成となる見込みである。http://www.pbs.org/newshour/rundown/u-s-create-independent-u-s-cyber-command-split-off-nsa/
[67] http://www.washingtontimes.com/news/2017/jul/17/us-to-create-independent-military-cyber-command/
[68] https://fcw.com/articles/2017/09/19/cybercom-spinoff-williams.aspx
[69] http://foreignpolicy.com/2017/08/18/trump-elevates-cyber-command/
[70] https://www.washingtonpost.com/news/checkpoint/wp/2017/08/18/president-trump-announces-move-to-elevate-cyber-command/?utm_term=.5472af915c3d

また、サイバー軍が創設された 2009 年時、海軍の艦隊サイバーコマンド（Fleet Cyber Command）の副司令官を務めていた退役海軍少将の Bill Leighter 氏は、サイバー軍と NSA の共同指揮体制が公式に継続するかに関係なく、米国政府のサイバースペースにおける諜報活動と軍事活動の衝突を回避するため、両組織間の人事異動を含め、サイバー軍は今後も NSA と密接な関係を維持せざるを得ないとの考えを示している[71]。

[71] https://federalnewsradio.com/on-dod/2017/08/elevation-of-us-cyber-command-recognizes-its-coming-of-age/