米国のサイバーセキュリティ態勢に関する 2024 年報告書

2024 年 5 月

国家サイバー長官事務局 大統領府

★★★★★★

本報告書について

国家サイバー部長は、合衆国法典第 6 編第 1500 条(c)(1)(C)(vi)の要請に従い、本報告書を大統領、国家安全保障問題担当大統領 補佐官、および議会に提供する。 この報告書は、米国のサイバーセキュリティ戦略、国家サイバー政策・戦略の有効性、連邦省庁による国家サイバー政策・戦略の実施状況を評価するものである。 合衆国法律集第 6 編第 1500 条(g)(1)に定義されているように、「サイバーセキュリティ態勢」とは、サイバー攻撃 または重大な結果をもたらすサイバーキャンペーンを構成しうる情報システムへの侵入を特定し、防御し、検知し、 対応し、回復する能力を意味する。

さらに、合衆国法律集第 6 編第 1500 条(c)(1)(G)に定められている通り、本書は米国が直面するサイバーセキュリティの脅威と問題について、国家安全保障、経済的繁栄、法治国家の執行に影響を及ぼす可能性のある新技術や新興技術を含め、議会に報告する。

本報告書は、過去 1 年間に起きた出来事に焦点を当て、文脈を示すために必要に応じてそれ以前の出来事も取り上げている。

★★★★★★

国家サイバー長官からの手紙

「米国のサイバーセキュリティ態勢に関する *2024* 年報告書」を発表できることを嬉しく思う。 本報告書は、米国がサイバー空間で直面する課題と機会にどのように取り組んでいるかについて、重要な最新情報を提供する初めてのものである。 われわれは、安全で豊かで公平なデジタルの未来に向けた肯定的なビジョンの実現に向けて前進してきたが、直面する脅威は依然として困難であり、われわれの防衛は難攻不落ではない。

端的に言えば、私たちは今、サイバーセキュリティにおける**根本的な変革の**真っ只中にいる。 急速に進化するサイバー脅威とダイナミックなテクノロジー環境に対応するためには、消極的な姿勢ではもはや追いつけないことは明らかであり、サイバーインシデントの最悪の影響を管理することだけを目指すのでは、もはや国家の安全保障、経済的繁栄、民主的価値を確保するのに十分ではないのである。 国家のサイバーセキュリティ改善に関する大統領令 14028 を皮切りに、バイデン-ハリス政権は、私たちを取り巻くデジタル世界を積極的かつ戦略的に形成し、私たちの経済と社会のあらゆる側面を可能にするよう位置づけることを中心に、肯定的なビジョンを進めてきた。

大統領の国家サイバーセキュリティ戦略は、デジタル世界の根底にある力学を根本的に転換し、防御可能でレジリエンシーが高く、我々の価値観に沿ったものにする必要があると主張している。 私たちが成功すれば、デジタル・エコシステムは、すべての米国人に利益をもたらす、豊かでつながった未来のための強固な基盤となりうる。 我々は、悪意あるサイバー脅威に対して強力に対応する態勢を維持しているが、敵対勢力に我々の進むべき道を左右させるようなことはしない。

この新しいビジョンを実現するには、国を挙げての協力的な取り組みが必要である。 官民を問わず、サイバー空間における最も有能で最も有利な立場にある関係者は、デジタル・エコシステムを再構築し、脆弱性を保護するために、より多くのことを行う必要がある。 私たちは、民間部門のパートナー、州、地方、部族、地域の事業体、そして世界中の志を同じくする国々と緊密に協力し、サイバー脅威に対する集団的なレジリエンスを高めていくことを約束する。

議会もまた、この実施プロセスにおける重要なパートナーであり、我々は、各省庁が必要な資源と権限を確保できるよう、議会との関与を続けていく。課題は山積しているが、政権と議会は、米国のサイバーセキュリティとレジリエンスを向上させるため、超党派で協力し続けなければならない。

戦略発表の場で大統領が述べたように、「今日我々が取る措置と選択は、今後数十年間の世界の方向性を決定する。 我々は、昨年の成功の上に築き上げ、失敗したところから教訓を学び、サイバーセ

★★★★★★

キュリティ規制の調和、セクター・リスクマネジメント機関の権限強化、有能な敵対的組織に立ち向かう小規模組織の支援といった困難な課題に取り組む必要がある。我々は共に、米国人をサイバー脅威から守り、我々の壮大な野望を可能にするデジタル世界を構築していく。

ハリー・コーカーJr.

国家サイバー長官

★★★★★★

エグゼクティブサマリー

「米国のサイバーセキュリティ態勢に関する *2024* 年報告書」は、米国のサイバーセキュリティ態勢、国家サイバー政策・戦略の有効性、連邦省庁による国家サイバー政策・戦略の実施状況を評価している。 さらに本報告書では、国家安全保障、経済繁栄、法の支配に影響を及ぼす可能性のある新技術や新興技術など、米国が直面するサイバーセキュリティ上の脅威や問題を取り上げている。本報告書はその第 1 版であり、2023 暦年を対象としている。本報告書の発行に先立ち、2024 年の動向についても追加考察を加えている。

この 1 年間、米国の国家サイバーセキュリティ態勢は改善し、2023 年国家サイバーセキュリティ戦略（NCS）のビジョンである、サイバー空間を形成する根本的な原動力の転換を通じて実現される、防御可能でレジリエンスに優れ、価値観の一致したデジタル・エコシステムの実現に向けた着実な進展に牽引された。 ガバナンスは、大統領の確固としたビジョンを現実のものとするため、連邦政府全体の各省庁の行動を調整する NCS 実施計画の実施に成功裏に着手した。 これらの初期実行行動は、デジタル・エコシステム全体の利害関係者による更なる投資と持続的なコミットメントに向けた基盤を築くものである。

戦略的環境

本報告書は、米国のサイバーセキュリティ政策と戦略にとって課題と機会の両方をもたらす戦略的環境、新興テクノロジーとサイバーリスクの状況のアセスメントから始まる。 新興技術の分析では、その内部的な技術的特性だけでなく、複雑なシステムやプロセスへの統合、人々や労働者とのつながり、機構やガバナンス構造との関係も考慮している。 本報告書はまた、サイバーリスクの状況についても検証しており、脅威行為者の能力と意図の傾向と、これらの敵対者が悪用する経路を作り出す、私たち自身の防御における進化する脆弱性の両方を考慮している。

2023 年、戦略的環境は**複雑性**、**相互接続性**、**競争を**特徴とする。 デジタル・コミュニケーション、高度なコンピューティング、量子情報科学、データの保存と処理、その他の重要な技術や新興技術の継続的な進歩は、我々の経済と社会の複雑性を急速に増大させている。 これらのテクノロジーはまた、世界中の人々をつなぎ、サイバーフィジカルシステムの普及を可能にし、あらゆる分野の重要なインフラと必要不可欠なサービスとの間に新たな依存関係を生み出している。 このような状況が進化するにつれ、悪意のある国家や非国家主体は、その継ぎ目を利用し、能力と戦略的目的を高めつつあり、サイバー空間が国際紛争や競争の他の領域と密接に連携していることを明確にしている。

★★★★★★

2023 年の戦略的環境の変化を促したのは、サイバーセキュリティに関する永続的な課題に加え、5 つのトレンドであった。

1. **重要インフラに対するリスクの進化**：国家の敵対者は、より広範な戦略的目標を推進するために、サイバー能力を使用して、本来スパイとしての価値を持たない重要インフラのシステムや資産を侵害し、リスクにさらす意思を強めていることを示した。

2. **ランサムウェア**ランサムウェアは、国家安全保障、公共の安全、経済的繁栄に対する持続的な脅威であり続け、ランサムウェアグループは、彼らの活動を挫折させるために設計された防御策や破壊策を回避したり、回避したりするための洗練された戦略を開発し続けた。

3. **サプライチェーンの悪用**：ソフトウェアやその他の情報技術、サービスの複雑で相互接続されたサプライチェーンにより、悪意のある行為者は被害者を大規模に危険にさらすことが可能になった。

4. **商業スパイウェア**：電子機器に遠隔からアクセスし、そのコンテンツを監視・抽出し、機器の使用者の認識や同意なしにそのコンポーネントを操作するために、民間業者が国家行為者に販売する高度で侵略的なサイバー監視ツールの市場が拡大していた。

5. **人工知能**人工知能(AI)は、現代において最も強力で、一般にアクセス可能なテクノロジーの一つであり、2023 年においてもその進化は続いており、大規模なサイバーリスクマネジメントの機会と課題を提示した。

現在の取り組み

戦略的環境がもたらす課題に対処し、チャンスをつかむには、連邦政府が主導し、民間部門の努力と連携した首尾一貫した行動プログラムが必要である。 国家サイバー長官室（ONCD）は、新たな行動を推進し、現在進行中の作業を向上させ、つなげることで、NCS を含む国家サイバー政策と戦略の実施を調整する。 本報告書は、連邦政府全体の省庁による国家サイバーセキュリティへの重要な貢献を反映している。

2023 年 7 月に発表された国家サイバーセキュリティ戦略実施計画（NCSIP）は、NCS のビジョンを実現するための連邦政府の取り組みの指針であり、毎年更新される。 NCSIP バージョン 1 では、連邦政府は 2024 年第 2 四半期までに 36 のイニシアチブを完了させる責任を負っていた。 本報告書に詳述されているように、これら 36 のイニシアチブのうち 33（92%）は予定通り完了し、3 つ

★★★★★★

は現在も進行中である。 さらに 33 の NCSIP バージョン 1 のイニシアティブは、今後 2 年間で完了する予定であり、順調に進んでいる。

本報告書の対象期間中に連邦政府がとった措置は以下の通りである：

1. 複数の重要インフラ部門における規制要件の策定と調和を含め、**重要インフラを保護するためのサイバー要件を確立し、活用する**。

2. サイバー防衛者をよりよく支援するために、**連邦政府の協力とパートナーシップを改善**する。これには、業務協力の強化、セクター・リスク・マネジメント・エージェンシー（SRMA）の能力向上、連邦政府のサイバー防衛能力の統合などが含まれる。

3. 脅威情報を迅速に共有し、被害者への支援を優先し、重要なインシデントやキャンペーンを検証して教訓を導き出すことで、**インシデントへの備えと対応を改善する**。

4. 国力のあらゆる手段を用いて**敵対的な活動を中断させ、弱体化させること**で、幅広い悪意あるサイバー行為者に対して、協調的でインパクトの大きい混乱キャンペーンを行う。

5. ゼロ・トラスト・アーキテクチャの原則を連邦エンタープライズ全体に統合し、レガシー・テクノロジー・システムを近代化し、共有サービスの利用を拡大することを含め、**連邦ネットワークを**迅速かつ大規模に**防御する**。

6. **国家サイバー人材**・教育戦略（NCWES）の公布や、全国の労働者、雇用主、学生、教育者との関わりを含め、**国家サイバー人材を強化する。**

7. セキュア・バイ・デザインの原則、ソフトウェア部品表（SBOM）、メモリ・セーフ・プログラミング言語などを推進する。

8. 米国のサイバートラスト・マークの認証とラベリング・プログラムを開始し、テクノロジー業界全体の競争と説明責任を促進することを含め、**消費者に力を与え、保護するデジタル経済を実現する**。

9. クリーンエネルギー経済全体にわたる**レジリエンス次世代技術への投資**、人工知能に関連する連邦政府の取り組みの指針となる大統領令の発令、インターネットの技術的基盤に存在するセキュリティ上の課題への対応などである。

★★★★★★

10. 安全でデータ・リッチな国境を越えた商取引を可能にし、プライバシー強化技術の開発を促進することで、**データ・セキュリティとプライバシーへのリスクをマネジメントする。**

11. ランサムウェアやその他のサイバー攻撃の被害者に支援を提供し、国家政策を調整し、安全でレジリエンスに優れたグローバル・サプライチェーンを促進するために、志を同じくする国々の連合を構築することで、**世界全体のレジリエンスを強化する。**

12. オープンで、自由で、グローバルで、相互運用可能で、信頼性が高く、アクセス可能で、安全なインターネットという肯定的なビジョンを推進し、商業スパイウェアのようなデジタル技術の拡散や悪用と闘い、民主的価値と人権に沿った新たな技術を形成することで、**権利を尊重するデジタル・エコシステムを推進する。**

今後の見通し

2024 年以降、連邦政府は昨年の成果を基に、NCS と NCWES の実施を継続し、進化する戦略的状況によってもたらされる新たな課題と機会に対処するためのアプローチを適応させていくことになる。 セクター・リスクマネジメント機関の能力を強化し、国家サイバー人材を強化し、2022 年重要インフラ法（CIRCIA）により指示されたインシデント報告要件を実施し、敵の妨害キャンペーンの速度と規模を強化し、分析と情報共有メカニズムを改善し、量子情報科学への投資を継続し、対外援助メカニズムにおけるサイバーセキュリティを優先する努力を維持することが必要となる。

NCS 実施計画の次の反復である NCSIP バージョン 2 は、昨年度の共有された成果を基礎とし、NCS を継続的に実施するための新たな取り組み方針を確立する 31 の新たな取り組みの概要を示している。 NCSIP バージョン 2 は本報告書と同時に発表され、www.whitehouse.gov/oncd からオンラインで入手できる。

★★★★★★

目次

★★★★★★

序文

根本的な変革が進行中である。 この変革の中核にあるのは、国家安全保障、経済、民主主義、そして現代的な生活様式の基礎となる新技術である。 人工知能（AI）、量子情報科学（QIS）、マイクロエレクトロニクスの分野における革新は、高度なコンピューティングの状況に革命をもたらしている。 産業用アプリケーションと消費者向け製品の両方において、私たちのデジタルと物理の世界はますますつながっている。 成長する高速インターネットへのアクセスと次世代通信ネットワークの普及は、世界中の人々とシステムをつないでいる。

このデジタル・エコシステムが進化するにつれ、敵対勢力はその脆弱性を悪用する能力と意図を繰り返し示してきた。 国家、非国家を問わず、米国の国家安全保障、治安、経済的繁栄を脅かす悪質なサイバー活動を積極的に続けている。 中華人民共和国（PRC）をはじめとする敵対勢力は、地政学的野心のために、米国の重要なサービスや公共の安全を脅かしている。 ランサムウェア・グループは、学校や病院、中小企業など、自衛能力のない多くの人々を標的としたビジネスモデルを構築している。

この決定的な瞬間に、バイデン-ハリス政権は、私たちが共有するデジタル化された未来を積極的に形成することを中心とした新たなアプローチを打ち出した。 2023 年 3 月に発表された大統領の国家サイバーセキュリティ戦略（NCS）は、防御可能でレジリエンスに優れ、我々の価値観に合致したデジタル・エコシステムという新たな肯定的ビジョンを明示している。 NCS は、悪意ある活動を有利に進めるデジタル・エコシステムで脅威行為者を管理することを前提としたこれまでのアプローチから脱却する。 その代わりに、NCS は、サイバー空間における役割、責任、リソースの配分方法について、2 つの根本的な転換を求める。(1)サイバー空間を防衛する責任を、エンドユーザーから、官民の最も能力があり、最も立場のあるアクターに振り向けること、(2)将来のレジリエンスへの長期的な投資を優先するよう、インセンティブを再調整すること。

NCS は、重要インフラのサイバーセキュリティに対する近代的で機動的な規制の枠組みの必要性を認識している。 NCS は、サイバーセキュリティの成果を低下させる経済力学に対処するため、デバイスのラベリング・ プログラムやソフトウェア責任体制などの市場介入を目標としている。 技術的な脆弱性がサイバーセキュリティを守る側に広範な課題をもたらしている場合、NCS は標準や研究開発への協調的な投資によって脆弱性を解消することを求めている。 また、NCS が明確にしているように、人材への投資はデジタルな未来への投資の重要な部分である。 2023 年国家サイバー人材・教育戦略（NCWES）は、すべての米国人がデジタル・エコシステムに参加できるようにする一

★★★★★★

方で、当面のサイバー人材ニーズと長期的なサイバー人材ニーズの両方に対処することを目的とした包括的なアプローチを概説している。

この新たな戦略的方向性が定まったことで、行政は実施という重要な仕事に着手した。 実施を成功させるためには、連邦政府、産業界、学界、市民社会、その他世界中のパートナーとの協力が不可欠である。 議会は、必要な権限と資源を各省庁に与えることで、実施プロセスに不可欠な支援を提供してきた。

NCS 実施計画（NCSIP）の第 1 版は、NCS の目標を達成するために連邦政府が実施すべき 69 の取り組みのロードマップを示している。現在までに、サイバーセキュリティ・コミュニティは NCSIP の初年度に 33 の項目を完了し、サイバー空間をより安全でセキュアなものにするために数え切れないほどの取り組みを行ってきた。 NCSIP の次のバージョンであるバージョン 2 は、実施初年度に達成された成功に基づき、新たに発生した予期せぬ課題に対応し、2023 NCS を実施するための 31 の新たな取り組みの概要を示している。 本報告書は、米国がいかに積極的かつ戦略的にデジタル・エコシステムを形成し、より防衛的でレジリエンスに富み、我々の価値観に合致したものにしているかを示すため、過去 1 年間の主な実施努力、成果、動向を紹介している。

★★★★★★

戦略的環境

戦略的環境は、人、技術、機構からなる進化するエコシステムと、このエコシステムの脆弱性を悪用して被害をもたらす悪意ある行為者からなる。 国家情報長官室が発表した「*2024* 年米国インテリジェンス・コミュニティの年次脅威アセスメント」は、国家・非国家行為者ともに、サイバー空間とそれ以外において米国の国益を脅かすサイバー能力を追求し続けていることを明らかにしている。 特に中国は、米国政府、民間企業、重要インフラ・ネットワークに対する最も活発かつ持続的なサイバー脅威であり続けている。 ロシア、イラン、朝鮮民主主義人民共和国(DPRK)の国家主体や、国境を越えた犯罪組織、その他の非国家主体は、米国や同盟国、パートナーに影響を与える悪質な活動を幅広く行っている。

しかし、サイバーリスクの状況は、このようなアクターやその悪意ある活動以上によって定義される。 脅威はリスクの一要素に過ぎず、サイバー空間における脆弱性の是正、レジリエンスの強化、あるいはサイバーインシデントが成功した場合の影響の軽減は、より直接的に私たちがコントロールできる範囲にある。 戦略的環境を分析するにあたり、本報告書は敵の能力と意図、我々のデジタル・エコシステムにおける脆弱性の分布と深刻さ、そしてこれらの課題に対処するために我々が展開するプロセスとポリシーの組み合わせを考慮する。 以下では、サイバーセキュリティに関する永続的な課題と、今年の戦略的環境の変化をもたらした新たなトレンドの両方を取り上げる。

私たちの戦略的環境は、**複雑性**、**相互接続性**、**競争の**激化によって特徴付けられている。重要かつ新たなテクノロジーが変化のペースをさらに加速させ、デジタル化された世界におけるリスクと機会を迅速に捉え直すことが求められるからである。 高度なコンピューティング技術、デジタルシステムと物理システムの融合、そして重要インフラを取り巻く新たなアクターの存在は、リスクの特定が困難な複雑な世界を作り出している。 サプライチェーンの広がり、コミュニケーション・ネットワークへのアクセスの拡大、相互依存的なグローバル・インフラによって、相互接続がますます進んだ世界となっている。 同時に、国家と非国家主体が高度なサイバー能力を駆使して利益を追求するようになり、戦略環境はますます競争が激しくなっている。 地政学的対立がサイバー空間で繰り広げられることが多くなり、米国や同盟国の重要インフラに対するリスクが増大している。

サイバーセキュリティの持続的課題

国家系、犯罪者、イデオロギー的動機に基づく行為者が米国に対してサイバー作戦を開始するケースが増加しているため、サイバー防衛者はこれまで以上に多くの敵に直面している。 これらの**敵対者は、**防衛側がパッチを開発・配備する前に攻撃者が脆弱性の悪用を開始できるという事実や、被

★★★★★★

害者を大規模に悪用することを可能にするネットワークの相互依存性など、**長年の構造的非対称性から利益を得ている**。 メモリが安全でない言語でのプログラミングなど、ソフトウェア開発コミュニティによる安全でない慣行の永続的な使用は、攻撃者をさらに有利にする。 さらに、アトリビューションに課題があるため、悪意のある行為者は結果を回避するために行動を難読化することができる。

レガシーなモバイル・ネットワークからインターネット上のデータ・ルーティングに至るまで、デジタル・エコシステム全体にわたって、セキュリティ属性の低い**レガシーなプロトコルや技術的**アーキテクチャが深く埋め込まれている。 インターネット・トラフィックを誘導するボーダー・ゲートウェイ・プロトコル（BGP）は、トラフィックのハイジャックや経路操作の影響を受けやすい。攻撃者はまた、時代遅れの暗号化プロトコルの弱点を利用して、コミュニケーションを侵害することもできる。

新しいデジタル技術は、しばしば敵対者に悪意のある悪用の新たな機会を与える。 例えば、実現可能な大規模量子コンピュータの開発は、莫大な経済的利益を約束し、全く新しい産業を創出し、我々のデジタル・エコシステムに革命をもたらす可能性がある。 しかし、量子コンピューターが、我々の情報の安全を守るために広く使われている暗号システムの多くを破る可能性があることは、数十年前から知られていた。 十分に成熟した量子コンピューターが悪の手に渡れば、デジタル・エコシステムの完全性が脅かされ、機密性の高い医療データや個人金融データが脅かされ、インターネットを利用した金融取引のセキュリティ・プロトコルが破られることになる。

重要インフラの所有者や運用者は、デジタル・オペレーションの重要な側面をマネージドサービス・プロバイダーに依存している。 例えば、クラウドサービスを採用することで、より優れた経済的なサイバーセキュリティの成果を大規模に実現することができるが、クラウドへの移行は新たなサイバーセキュリティリスクももたらす可能性がある。 組織がローカルにホストされたシステムとクラウド資産の両方を使用するハイブリッド導入では、複雑な集中型ロギングと認証レジームが導入される可能性があり、悪意のある行為者が検知を回避したり ID 管理システムを悪用したりする機会が生まれる。 2023 年の PRC による米国政府コミュニケーションの侵害は、包括的なロギ ングを維持する必要性を示している。 より広範には、組織がますます大量のデータとプロセスをクラウドに移行するにつれて、この移行は新たな部門横断的依存関係を導入し、特に複数の組織が同じプロバイダのサードパーティ・サービスに依存している場合、システミック・リスクの識別と管理を複雑にする。

★★★★★★

わが国の重要インフラは、**民間の所有と運用によって**特徴付けられ、その結果、官民間の相互依存が生じ、官民の行動、協力、パートナーシップに根ざした国家サイバーセキュリティ態勢が必要となる。 急速に拡大する宇宙産業は、技術の進歩がサイバーリスクを共有管理するための新たな課題と協力の機会をいかに生み出すかを示している。 コミュニケーション、センシング、ナビゲーション、タイミングを宇宙ベースのシステムに依存する重要なインフラ資産は増え続けている。 ロシアによる 2022 年のウクライナ侵攻までの数日間、米国の宇宙通信会社に対するサイバー攻撃は、表向きはウクライナの電気通信を妨害することを意図していたが、欧州の何千もの風力タービンで使用されているコンピューターシステムの停止にもつながった。 宇宙エコシステムが進化を続け、新たな商業参加者を統合していく中で、宇宙システムのサイバーセキュリティは共有の責任となるだろう。

米国の**サイバー労働力は**、より多くの訓練を受けたサイバーセキュリティの専門家と、より良いサイバー教育のエコシステムに対する根強いニーズと格闘し続けている。 より多くの米国人をサイバー労働力に参加させることは、国家サイバーセキュリティの成果を強化するだけでなく、高賃金の中流階級の仕事へのアクセスも提供する。 経済発展と国家安全保障の問題として、公式・非公式のサイバー教育・訓練システムを通じてサイバー人材を育成しなければならない。 米国の学校、ガバナンス、非営利団体、企業は、米国のサイバー人材の育成において前進を遂げてきたが、こうした投資は、増大する需要に対応するために必要な規模や調整に欠けていた。

2023 年のトップ・トレンド

重要インフラに対するリスクの進化

米国の重要インフラは、進化する受け入れがたいサイバーリスクに直面している。 国家の敵対者は、米国や同盟国の重要インフラを混乱させたり破壊したりする目的で、サイバー能力を開発し、アクセスを獲得している。 このような混乱は、サイバー領域以外の敵対者の戦略目標を支援したり、可能にしたりする可能性があり、重要インフラ部門内および部門間のリスクマネジメントに課題をもたらす。

敵対国がサイバー攻撃のために事前準備を行うことは長年の脅威であるが、PRC の事前準備活動は、アメリカがこれまで直面したことのない脅威である。 2023 年、ボルト・タイフーン（Volt Typhoon）として追跡された PRC のアクターは、米国とインド太平洋地域の重要インフラにアクセスした。 このキャンペーンは、スパイ活動や諜報活動の観点からはほとんど価値のない米国の事業体を標的にしたものであったが、重要インフラの運用技術システムを混乱させ、米国や同盟国の戦闘能力を妨害する可能性があった。 また 2023 年には、BlackTech として追跡された PRC の関係

★★★★★★

者が、洗練されたツールを使用してルーターを侵害し、米国と日本のさまざまな重要インフラにアクセスした。 これらの侵入は、米国と同盟国の重要インフラをリスクにさらし、危機時における米国の意思決定を形成し、中国の地政学的目標を強化するためにサイバー能力を使用するという PRC の意図を示した。

ランサムウェア

ランサムウェアは依然として、国家安全保障、公共の安全、経済的繁栄に対する根強い脅威である。 ランサムウェアの脅威の全容に関する包括的なデータを入手することは困難であり、特にサイバーインシデントの報告要件がまだ発展途上であることや、被害者が攻撃に関する情報を共有したがらないことが影響している。 連邦捜査局（FBI）のインターネット犯罪苦情センター（IC3）は、2022 年に一時的に減少した後、米国の被害者から報告されたランサムウェアのインシデントが 22%増加した。 また、IC3 への報告によると、2023 年のランサムウェアインシデントのコストは、2022 年と比較して 74%増加した。

既存のランサムウェアグループは、アクセスを収益化し、彼らの活動を挫折させるために設計された防御策を回避または回避するための洗練された戦略を開発し続けている。 攻撃者は、被害者のデータを暗号化するだけでなく、身代金を支払わなければそのデータを売却したり公に公開したりすると脅したり、時には追加料金を支払わなければ被害者の身元を特定すると脅したりする「二重」「三重の恐喝」攻撃の利用を増やしている。 このようなランサムウェアの追加料金を支払う被害者は、流出したデータを削除し、Doxing 攻撃を控えるという攻撃者の約束に依存しているが、この約束は必ずしも守られるとは限らない。 ランサムウェアの攻撃者は互いに共謀を結び、マルウェアの開発と配備、個々の標的への攻撃の実行、暗号通貨の身代金の徴収といった作業を分担している。このような形で犯罪経済に特化することで、ランサムウェアの脅威は特に強力になっている。

サプライチェーンの搾取

ソフトウェアやその他の情報技術、サービスの複雑で相互接続されたサプライチェーンは、一般的なサードパーティ・サービス・プロバイダへの依存の高まりと相まって、巧妙な敵対者が被害者に大規模にアクセスする機会を生み出し、サイバーセキュリティ・リスクを特定・管理する防衛側の取り組みを複雑にしている。 敵対者は、組織とそのサプライヤー、顧客、ベンダー、サービスプロバイダーとの間の複雑で相互接続された関係をますます利用するようになっており、単一ノードを侵害することで、米国および世界中の被害者に密かにアクセスできるようにしている。

★★★★★★

2023 年、技術プロバイダに対するいくつかの有名な侵害事件が発生し、重要インフラの所有者や運営者を含む何千もの接続被害者が影響を受けた。 12 月には、ロシアの対外情報庁（SVR）が、コンピュータ・プログラマーがソフトウェアのコンパイルやテストに使用するサーバーを標的とした。 年明け早々には、広く利用されている ID・アクセス管理会社が侵害され、悪意のある行為者が何千もの顧客に密かにアクセスできる認証情報とセッショントークンを盗むことができた。 さらに年初には、人気の高いエンタープライズ・コミュニケーション・スイートが、まったく別のサプライチェーン攻撃で侵害された。

商用スパイウェア

電子機器に遠隔からアクセスし、そのコンテンツを監視・抽出し、機器の使用者の認識や同意なしにそのコンポーネントを操作するために、民間業者が販売する洗練された侵襲的なエンドツーエンドのサイバー監視ツールの市場が拡大している。 商用スパイウェアのプロバイダは現在、世界最高水準の能力を最高入札者に提供しており、そのプロバイダはしばしば、監視や規制の制約を受けないサイバー作戦でこれらの能力を使用している。 商業スパイウェア産業には長い歴史があるが、近年、これらのツールが拡散し悪用されることで、悪意のあるサイバー行為者は、ジャーナリスト、活動家、人権擁護者、政府高官を標的とする頻度が高まっている。

権威主義的な政権や民主的な政府が、標的を監視したり、敵対者を威嚇したり、反対意見を抑圧したり、表現、平和的集会、結社の自由を制限したり、人権を濫用したりするために、商用スパイウェアを悪用するケースが増えている。

一部の外国政府や個人は、米国政府の職員、情報、コンピュータ・システムに対して商用スパイウェアを配備しており、米国に重大な防諜およびセキュリティ・リスクをもたらしている。 これらのツールの悪用は、米国および世界中の個人のセキュリティとプライバシーをも脅かしている。

人工知能

人工知能(AI)は、現代において最も強力なテクノロジーのひとつであり、世間の注目とメディアの報道を集め続けている。 大規模言語モデル（LLM）やその他の基礎的アルゴリズムの進歩は、より手頃なコンピューティング・パワーとデータへのアクセスと相まって、新世代の AI ツールを生み出した。 これらのツールは 2023 年に人々の想像力をかき立て、アメリカ人はチャットボットや画像生成装置といった斬新なアプリケーションを体験した。 AI は、世界中の官民事業体が利益と競争上の優位性を求めてしのぎを削る中、今後も急速なペースで進化を続けることはほぼ間違いないだろう。

★★★★★★

進化する AI の状況は、サイバー防衛者に、悪意ある活動から重要インフラを守る新たな機会をもたらすだろう。 サイバーセキュリティ・コミュニティには、データ処理、電子メール・フィルタリング、マルウェア識別などの基本的なタスクに機械学習技術の力を活用してきた長い歴史がある。 AI を統合した新しいサイバー防衛ツールは、最終的にはサイバー防衛者が異常なネットワーク・トラフィックやその他の敵の活動をより効率的に検知し、複雑なシステムやネットワークの防衛を調整し、すでに手薄になっているサイバーセキュリティ人材を増強することを可能にするかもしれない。

AI ツールは、ソフトウェア開発のエコシステムをより安全でセキュアなものにするかもしれない。 LLM はプログラミング言語をある程度流暢に操るが、人間の介入なしに商業的に有用なセキュアコードを生成することはまだできない。 ソフトウェア開発ライフサイクルに AI ツールを責任を持って統合することで、開発者は新しいコードの脆弱性を特定し、修正の可能性を提案できるようになるかもしれない。 AI ツールが成熟すれば、既存のコードをメモリー安全なプログラミング言語に書き換えることで、広く使われているソフトウェア製品をより安全なものにできるかもしれない。

しかし、AI の可能性を実現することは、それがサイバーセキュリティにもたらすリスクをマネジメントすることでもある。 今日、LLM は、さまざまな言語で、説得力のあるマイクロターゲットのテキスト、画像、音声、動画を迅速かつ安価に生成することができる。 サイバー犯罪者やハクティビストなど、リソースや技術的洗練度が限られている者は、こうした能力を利用して、フィッシングキャンペーンや情報操作、その他の悪意あるサイバー活動を行う可能性がある。 AI を活用した監視・検閲技術は、権威主義政権がジャーナリストや反体制派、人権擁護者をより効果的・効率的に標的にすることを可能にする。 セーフガードなしでは、AI 技術は個人データの抽出、特定、悪用を容易にし、米国人のプライバシーをリスクにさらす可能性もある。 AI のエコシステムが進化し続ける中、その中核的要素であるデータ、コンピューティング、アルゴリズムが、悪用に対するセーフガードとともに開発されることを保証する機会がある。

★★★★★★

現在の取り組み

連邦政府は、NCS を実施し、米国の国家目標に沿ったデジタル・エコシステムを積極的に形成するため、大胆な行動プログラムを実施している。 これらの取り組みは、超党派インフラ法（BIL）、インフレ削減法（IRA）、CHIPS と科学法、CIRCIA のようなサイバーセキュリティ法、国のサイバーセキュリティの改善に関する大統領令（EO）14028、重要インフラ制御システムのサイバーセキュリティの改善に関する国家安全保障覚書（NSM）5、国家安全保障、国防省、情報システムのサイバーセキュリティの改善に関する NSM-8 などの大統領令を含む、新しいインフラへの世代的投資の上に構築されている。

2023 年 7 月に発表された NCSIP バージョン 1 は、サイバー犯罪との戦いから、熟練したサイバー人材の育成、インターネットの技術的基盤に存在するセキュリティ上の課題への対応に至るまで、影響力の大きい 69 の取り組みを通じて、NCS のビジョンを実現するための連邦政府の取り組みを指針としている。NCSIP バージョン 1 では、連邦政府は 2024 年第 2 四半期までに 36 のイニシアチブを完了させる責任を負っていた。 下表に詳述するように、これら 36 のイニシアチブのうち 33（92%）は予定通りに完了し、3 つは現在も進行中である。 さらに 33 の NCSIP バージョン 1 のイニシアティブは、今後 2 年間で完了する予定であり、順調に進んでいる。

この報告書と並行して、ONCD は NCSIP 第 2 版を発表した。この報告書は、実施初年度に達成された成功を基礎とし、進化する課題に対応し、2023 年 NCS を実施するための 31 の新たなイニシアティブを概説している。 24 の機関が NCSIP バージョン 2 のイニシアティブを主導しており、新たに 6 つの機関が NCS のビジョン達成のための実施努力に加わっている。 NCSIP バージョン 1 におけるイニシアティブの進捗状況や、NCSIP バージョン 2 における進行中および新規のイニシアティブの詳細については、www.whitehouse.gov/oncd。

NCS 実施状況

NCSIP イニシアチブ	イニシアチブのタイトル	責任機関
1.1.1	サイバー規制の調和に関するイニシアチブを確立する	ONCD
1.2.2	重要インフラ部門および部門リスクマネジメント機関の指定に関する提言を行う。	CISA
1.3.1	連邦サイバーセキュリティセンターと関連サイバーセンターの能力をアセスメントする。	ONCD

★★★★★★

NCSIP イニシアチブ	イニシアチブのタイトル	責任機関
1.4.3	サイバーインシデント対応を改善するための演習シナリオを作成する。	ONCD
1.4.4	必要な権限を持つサイバー安全審査委員会を成文化するための法律をドラフトする。	国土安全保障省
1.5.1*	連邦文民行政機関の未分類のシステムを引き続き保護するための行動計画を策定する。	OMB
2.1.1	最新の国防総省サイバー戦略を発表する。	防衛総省
2.1.4	サイバー犯罪およびサイバー犯罪を可能にする犯罪を妨害し、抑止するための法律を提案する。	司法省
2.1.5*	混乱処理のスピードと規模を拡大する	FBI
2.2.1	官民の作戦協力を通じて、敵対的破壊を増大させるメカニズムを識別する。	ONCD
2.4.1	Infrastructure-as-a-Service プロバイダと再販業者のための要件、標準、手続きに関する規則制定提案通知を公表する。	商務省
2.5.1	ランサムウェア犯罪者の隠れ家を抑制するための行動計画を策定する。	国務省
2.5.2	ランサムウェア犯罪を阻止するため、作戦のスピードと規模を拡大する。	FBI
2.5.3	ランサムウェア犯罪の調査改善	司法省
3.2.1	連邦政府規則を変更するための提案公告を発表する。 2020 年モノのインターネット・サイバーセキュリティ改善法に沿った取得規制	OMB
3.2.2	米国政府によるモノのインターネットのセキュリティ・ラベリング・プログラムを開始する。	NSC
3.3.1	長期的で柔軟かつ永続的なソフトウェア責任の枠組みを開発するためのアプローチを探る。	ONCD
3.4.1	連邦政府補助金をより効果的に活用し、インフラのサイバーセキュリティを向上させるために、連邦政府機関と被補助機関向けのガイダンスを作成する。	ONCD

★★★★★★

NCSIP イニシアチブ	イニシアチブのタイトル	責任機関
3.4.2	サイバーセキュリティを研究資金調達の優先課題に含める。	OSTP
3.5.1*	連邦政府規則を変更するための提案公告を発表する。 大統領令 14028 に概説された新たな要求事項を盛り込んだ取得規則	OMB
3.6.1	壊滅的なサイバー事象に対する連邦保険の対応の必要性をアセスメントする。	財務省
4.1.1	ネットワークセキュリティのベストプラクティスの導入をリードする	OMB
4.1.2	オープンソースソフトウェアのセキュリティとメモリー安全プログラミング言語の採用を推進する。	ONCD
4.1.3	サイバーセキュリティの国際標準に関する省庁間調整を再活性化する。	NIST
4.2.1	最新のサイバーセキュリティ研究開発戦略を発表する。	OSTP
4.4.1	連邦政府のプロジェクトにサイバー・セキュア・バイ・デザインの原則を組み込むことで、その採用を推進する。	エネルギー
4.4.2	デジタル・エコシステムが米国政府の脱炭素化目標をサポートし、実現できるようにするための計画を策定する。	ONCD
4.6.1	国家サイバー人材・教育戦略を発表し、その実施状況を追跡調査する。	ONCD
5.1.2	国際サイバー空間・デジタル政策戦略を発表する	国務省
5.2.1	国際パートナーのサイバー能力を強化するため、省庁間の調整を改善する。	国務省
5.3.1	サイバーインシデント対応支援を迅速に提供するための柔軟な海外支援メカニズムを確立する。	国務省
5.5.1	安全で信頼できる情報通信技術（ICT）ネットワークおよびサービスの開発を促進する。	国務省
5.5.2	ICT ベンダーのより多様でレジリエンシーなサプライチェーンを促進する。	国務省
5.5.3	公共無線サプライチェーン・イノベーション・ファンドの運営を開始する。	商務省

★★★★★★

NCSIP イニシアチブ	イニシアチブのタイトル	責任機関
6.1.2	国家サイバーセキュリティ戦略の実施に教訓を生かす。	ONCD
6.1.3	国家サイバーセキュリティ戦略の実施に沿った予算ガイダンスを公表する。	ONCD

* は発表日現在進行中の取り組みであることを示す。

重要インフラを防御するためのサイバー要件の確立と活用

NCS は、国家安全保障、公共の安全、経済的繁栄というわれわれの集団的目標に個人と組 織の利害を一致させるために、インセンティブと要件を活用することを求めている。 サイバーセキュリティ要件に対する連邦政府の積極的なアプローチは、すべての部門が説明されなけれ ばならないことを認識している。 サイバーセキュリティ要件が存在しない、あるいは定義が不十分な場合には、敵対勢力がその能力を高め、戦術を変化させても適応できるような俊敏性を備えた新たな要件を追求している。 規制の状況がすでに成熟している場合には、新規の規制要件と既存の規制要件を調和させ、整合させることに取り組んでいる。 また、このような取り組みがモデルとなりうる、あるいは米国の重要インフラ所有者、運営者、サードパーティ・サービス・プロバイダに影響を与える可能性のある他国の規制措置にも細心の注意を払っている。

昨年、いくつかの重要インフラ部門において、サイバーセキュリティに関する新規または更新された規則が施行された。 運輸保安局（TSA）は、石油・天然ガスパイプライン、空港・航空機運営者、鉄道事業者向けの要件を更新した。 証券取引委員会（SEC）は、上場企業に対し、サイバーセキュリティに関する重大なインシデントやリスクマネジメントの実践に関する情報開示を義務付ける新規則を採択した。 医療・公衆衛生（HPH）分野では、食品医薬品局（FDA）の認可法の一つである連邦食品・医薬品・化粧品法の改正により、特定の種類の医療機器の製造事業者に対し、ソフトウェアコンポーネントの包括的なリストの作成などを通じて、サイバーセキュリティの高い医療機器を設計・開発・維持することが義務付けられた。 FDA はまた、医療機器製造者が医療機器のサイバーセキュリティに関連する FDA の規則を遵守するための最新の勧告を確定した。 防衛産業基盤（DIB）については、国防総省（DoD）がサイバーセキュリティ成熟度モデル認証プログラムの改訂版を発表し、DIB の請負業者および下請業者に対する新たな要件を定め、自主的な DIB サイバーセキュリティ（CS）プログラムへのアクセスを拡大した。 また、海事分野では、米国沿岸警備隊が港湾と海上のサイバーセキュリティを強化するための海上セキュリティ指令と提案公告

★★★★★★

（NPRM）を発行したのに伴い、大統領は「米国の船舶、港湾、港湾、臨海施設の保護に関する規制の改正に関する EO 14116」に署名した。

すべての重要インフラ部門にわたって、CIRCIA の実施により、対象事業体は特定のサイバーセキュリティインシデントを連邦政府に報告するための新たな要件が設けられる。 2024 年 3 月、CISA は、CIRCIA 規制プログラムの他の側面と同様に、サイバーインシデントおよび身代金支払報告に関する規制案を定めた NPRM を発表した。 これらの報告書に含まれる情報は、悪質なサイバー活動に対する可視性を高め、セクター横断的なリスクの理解を改善し、集団的防衛を強化する。

連邦政府は、規制の基本要件を部門間で調和させるための対策を優先している。 連邦通信委員会（FCC）が議長を務める独立行政機関規制当局のためのサイバーセキュリティ・フォーラムは、連邦機関が規制活動の有効性と一貫性を改善するための取り組みを調整することを可能にしている。 2023 年 9 月、サイバーインシデント報告評議会は、連邦サイバーインシデント報告要件の合理化と調和に関する報告書を議会に提出した。

2023 年 7 月、ONCD は、重要インフラに対するサイバーセキュリティの基本要件と関連するアセスメントおよび監査の調和を図る機会、および調和を図る上での障害に関する情報提供の要請（Request for Information）に対する一般からの回答を募集した。 回答者は、国立標準技術研究所（NIST）のサイバーセキュリティ・フレームワーク（CSF）のような既存のフレームワークやベストプラクティスを活用して相互主義を促進することの重要性を強調し、ONCD が連邦規制機関と協力して、現在および新たなサイバーセキュリティ要件の矛盾を解消し、整合化を推進することを推奨した。

要件は、既存のサイバーセキュリティフレームワーク、自主的なコンセンサス標準、その他の技術ガイダンスと整合している場合に最も効果的であることが多い。 2023 年 3 月、CISA は利害関係者の意見に基づいてサイバーセキュリティ・パフォーマンス目標 （CPG）を更新し、SRMA に段階的アプローチによる部門別目標の策定を開始するよう働きかけた。 2024 年 2 月、NIST は CSF のバージョン 2.0 を発表した。この CSF は、進化するサイバーセキュリティリスク のマネジメント、実施、効果測定に関する最新のガイダンスを提供するものである。 エネルギー部門では、エネルギー省（DOE）が全米公益事業規制委員会協会（NARUC）と提携し、配電システムと分散型エネルギー資源のサイバーセキュリティ・ベースラインを策定した。2024 年 2 月、NARUC と DOE はベースラインを公表し、各州の規制団体や産業界とともに実施戦略と採用ガイドラインを策定する第 2 段階を開始した。

★★★★★★

連邦政府の調整とパートナーシップの強化

連邦政府は、連邦政府のサイバー能力が明確かつ協調的で効果的な方法で発揮されるよう、重要インフラ保護政策の近代化を進めている。 2024 年 4 月、ガバナンスは重要インフラのセキュリティとレジリエンスに関する NSM-22 を発表し、大統領政策指令 21（PPD-21）を重要インフラのセキュリティとレジリエンスに関する連邦政府の主要政策文書として置き換えた。 10 年以上前に発表された PPD-21 は、16 の重要セクターを定義し、サイバーやその他のオールハザードのリスクを識別しマネジメントする責任を課していた。 NSM-22 は、セクター横断的なサイバー防衛を可能にする連邦政府の能力を強化し、重要インフラのセキュリティとレジリエンスのための国家コーディネーターとしての CISA の役割を明確化し、SRMA として機能する他の連邦機関との接続性を改善し、法執行機関、情報コミュニティ、重要インフラ所有者および運用者との統合と情報共有を強化する。 NSM-22 はまた、連邦政府が協調と規制のバランスをとるためのよりよい位置づけをし、SRMA とセクター別の規制当局に最低限のセキュリティ要件を策定するよう指示している。 CISA は国家調整官として SRMA と協力し、最新のリスクアセスメントと国家インフラリスクマネジメント計画を策定する。

CISA は、重要インフラの所有者と運営者が自らを守れるようにする上で中心的な役割を果たしている。 2023 年、CISA のサイバー防衛共同体（JCDC）は、重要インフラパートナーのサイバーセキュリティとレジリエンスを強化するための 3 つの共同サイバー防衛計画を完成させた。 JCDC の遠隔モニタリング・マネジメント（RMM）計画とオープンソースソフトウェア（OSS）計画は、それぞれ RMM ソフトウェアの悪用に対処し、運用技術における OSS の安全な使用のためのベストプラクティス・ガイダンスを作成することで、分野横断的なリスクを管理する。 JCDC はまた、中小規模の公益事業者を支援するため、上下水道セクター向けのインシデント対応ガイドを発行した。
CISA は、ランサムウェア活動に関連する一般的に悪用される脆弱性を特定し、重要インフラ事業体がリスクを軽減できるよう警告するため、CIRCIA の認可を受けてランサムウェア脆弱性警告パイロット（RVMP）プログラムを設立した。2023 年、このプログラムは、1,754 の脆弱性デバイスについて、重要インフラの所有者および運営者に通知した。 さらに 2023 年 11 月、CISA は医療、上下水道、教育分野の組織にサイバーセキュリティ共有サービスを提供する自主的なパイロットプログラムを開始した。

SRMA はさらに、連邦政府が重要インフラの所有者や運営者を大規模に支援し、関与することを可能にする。 2023 年には、保健福祉省（HHS）が医療サイバーセキュリティの新戦略を発表し、医療セクター調整協議会（Health Sector Coordinating Council）と協力して医療産業サイバーセキュリティ実践ガイド（Health Industry Cybersecurity Practices Guide）を更新し、リスク識別お

★★★★★★

よびサイト臨界性ツール（Risk Identification and Site Criticality Tool）バージョン 2.0 を発表し、CISA と提携してセクター別 CPG を策定した。 環境保護庁（EPA）は、上下水道システム向けの新しいサイバーセキュリティリスク評価リソースを発表し、CISA および連邦捜査局（FBI）と協力して、このセクター向けのインシデント対応ガイドを作成した。 財務省は、クラウド導入に伴うメリットと課題に対処するため、規制当局と金融サービス機関の協力を強化するクラウド・エグゼクティブ・ステアリング・グループを設立した。 DOE は、レジリエンス産業制御システムのためのサイバーテスト（CyTRICS）プログラムを通じて、優先的なエネルギーシステムコンポーネントのソフトウェア、ハードウェア、ファームウェアのサイバーセキュリティを強化するために、主要な民間組織と新たなパートナーシップを確立した。

連邦政府は、情報共有と利害関係者の関与という SRMA の従来の強みを、計画、演習、インシデント 対応を含む民間部門との運用協力のより強固な能力で補うことに注力している。 国家安全保障局（NSA）は民間セクターのパートナーと協力して、国家安全保障システム（NSS）、米軍資産、DIB をサイバー脅威から守っている。 NSA のサイバーセキュリティ・コラボレーション・センター（CCC）は、DIB とそのサービス・プロバイダとの官民協力のための拡張可能で情報駆動型のメカニズムを提供し、2023 年には 750 を超えるパートナーシップを構築し、他の重要インフラ部門を脅かす悪意のあるサイバー活動に対する協力的な防衛をさらに可能にしている。 CCC は、保護ドメインネームシステム、アタック・サーフェイス・マネジメント、脅威インテリジェンス・コラボレーション・サービスの提供を含め、DIB へのサイバーセキュリティ支援を拡大し続けている。

米国の学校システムに影響を及ぼすサイバー攻撃を受けて、ホワイトハウスは、幼稚園から高校までの学校のサイバーセキュリティを強化するための官民の対策を調整するためのフォーラムを開催した。 教育省は、教育分野の関係者間のコミュニケーションを強化し、サイバーセキュリティのレジリエンスへの取り組みを改善するため、政府調整会議（GCC）を設立した。 FBI は、サイバー脅威への現場での対応サービスを可能にするため、56 の現場事務所を通じて全米の学区との関わりを続けている。 CISA は教育部門を支援するため、教育省との連携による部門別ガイダンスの策定や、K-12 部門の関係者に合わせたアセスメント、演習支援、トレーニングの提供など、さらなるリソースをプロバイダとして提供している。

国家宇宙会議、国家安全保障会議サイバーセキュリティ局、および ONCD はまた、宇宙システムのサイバーセキュリティに関連する固有の課題に対処するための官民の取り組みを調整している。 2023 年、ONCD はサイバーセキュリティの課題と機会について議論するため、政府と産業界の宇宙専門家を集めた一連の地域技術ワークショップを開催した。 7 月、NIST は商業衛星運用に関するサイバーリスクマネジメントの実践に関する最新報告書を発表した。 10 月には、米航空宇宙局

★★★★★★

（NASA）が、統合・相互接続が進む宇宙システムによる新たな課題に対処するためのベストプラクティスガイドを発表した。

州、地方、部族、準州（SLTT）政府は、サイバーセキュリティ態勢の強化に取り組んでいる。 超党派インフラ法は、SLTT が所有または運用する情報システムに対するサイバーセキュリティ・リスクに対処する能力を高めるため、10 億ドルの資金をプロバイダに提供している。 2023 年には、CISA と連邦緊急事態管理庁は、州・地方サイバーセキュリティ補助金プログラムを通じて 3 億 7500 万ドル、部族サイバーセキュリティ補助金プログラムを通じて 1800 万ドルを利用できるようにした。 中小企業庁（SBA）も、中小企業向けサイバーセキュリティ・パイロット・プログラム（SBA Cybersecurity for Small Business Pilot Program）を通じて助成金を提供している。 連邦政府機関は、サイバーセキュリティのベストプラクティスを共有し、サイバー対応と復旧を支援し、サイバーセキュリティの研究開発を加速させるために、SLTT 事業体や中小企業と提携を続けていく。

インシデントへの備えと対応の改善

連邦政府は引き続き、サイバーインシデントの被害者への支援を優先している。 司法省（DOJ）、FBI、CISA、米国シークレットサービス、およびその他の連邦事業体は、サイバー犯罪者を捜査して正義を追求し犯罪を防止すること、サイバー脅威の専門家のグローバルネットワークを採用して帰属と分析に貢献すること、サイバー脅威情報を共有して被害者対応措置に役立てること、対象となる事業体に復号機能やその他の既知の脅威緩和ツールを紹介すること、盗まれた資金や強要された資金の凍結、押収、返還を支援することなど、サイバー事件後の被害者支援に重要な資源を投入している。

FBI のインターネット犯罪苦情センター回収資産チームは、金融機構や FBI 現場事務所とのコミュニケーションを効率化し、被害者のための資金の凍結、差し押さえ、返還を支援し、2023 年には 71%の成功率を記録した。 FBI 主導の暗号通貨脅威センターは、法執行機関やインテリジェンス・コミュニティのパートナーと協力し、北朝鮮に関連する脅威行為者によって盗まれた仮想資産を含む、盗まれた暗号通貨を公に識別する米国政府の能力を高めている。FBI のサイバー・アクション・チームと、56 の FBI 支部に展開されつつあるモデル・サイバー・スクワッドは、大規模なインシデントに対応して数時間以内に捜査支援を提供できる迅速な対応能力を備えている。

CISA のハント・インシデント対応チームは、米国の重要インフラに対するサイバー脅威を特定・検知するなど、サイバーセキュリティインシデントに対応する組織を支援している。 2023 年、CISA は SRMA と定期的に連携し、重要インフラの所有者および運営者との協力と支援を強化した。 さら

★★★★★★

に、超党派インフラ法は、CISA が重大なサイバーインシデント発生時に連邦、SLTT、公共、民間事業体を支援するために使用できる 1 億ドルのサイバー対応・復旧基金を設立した。

重要なインシデントや悪質なサイバー活動に対応するため、サイバーセキュリティ・アドバイザリ（CSA）は、重要インフラの所有者や運営者、その他の事業体に、脅威を検知し対応するための指針をタイムリーに提供する。 これらの CSA の策定を連邦政府全体で、また国際的な同盟国やパートナーとの間で調整することで、 被害者への支援が向上する。 2023 年 5 月、NSA、CISA、FBI、DOE、および国際的なパートナーは、PRC が後援する Volt Typhoon Actor の戦術、技術、手順（TTPs）を詳述した CSA を発表し、その後、これらの TTPs を特定し緩和するための組織のための共同ガイダンスを提供した。

サイバーセーフティレビュー委員会（CSRB）は、重要なサイバーインシデントのレビューとアセスメントを行い、同様のインシデントが発生しないよう官民の組織に対して提言を行う。 2023 年 8 月、CSRB は脅威行為者グループ「Lapsus$」に関する分析を発表し、同グループがシステム的なエコシステムの弱点を悪用して全米の組織を被害者にしていることを明らかにした。 この報告書は、CISA と DHS による、必要なセキュリティ機能が追加コストなしに顧客にプロバイダとして提供されるようにするための、その後の継続的な取り組みにつながった。 2024 年 4 月に発表された CSRB の第 3 次報告書は、クラウド・コンピューティング環境の悪意ある標的化に 焦点を当て、クラウドにおける ID 管理と認証を強化するための提言を行っている。 CSRB が行う構造分析は、重大なサイバーインシデントから学んだ教訓を特定・共有し、実行可能な軽減策を策定する上で極めて重要な役割を果たす。

CISA は 2024 年末までに国家サイバーインシデント対応計画（NCIRP）を更新することを約束した。 NCIRP は、大統領政策指令 41「米国サイバーインシデント調整」に従い、連邦政府機関、民間事業体、SLTT 事業体の主要な役割と責任を定義することを含め、重要なサイバーインシデントをハンドリングするための国家的アプローチを概説している。 サイバー脅威の状況とサイバー防衛エコシステムは、NCIRP が 2016 年に発表されて以来、大きく進化している。 更新された NCIRP は、連邦政府、民間セクター、その他の主要パートナーにまたがる協調的な国家インシデント対応を可能にする、現代的で機敏かつ柔軟な枠組みを提供する。

敵の活動を妨害し、弱体化させる

米国は、サイバー空間における国益を守り、サイバー脅威行為者を混乱させ、解体するために、国力のあらゆる手段を用いる態勢を維持している。 ランサムウェアやその他の形態のサイバー犯罪に対抗するため、政権は外交、情報、軍事、金融、情報、法執行能力の統合的な活用を改善し、これ

★★★★★★

らの活動に連邦政府や国際機関以外のパートナーを参加させるための新たな方策を追求している。混乱させるだけでは、ランサムウェアやその他の形態の悪質なサイバー活動を打ち負かすことはできないが、この問題に意味のある影響を与えることはできる。

2023 年 9 月、国防総省は「*2023* 年国防総省サイバー戦略」を最終決定した。この戦略では、悪意あるサイバー活動が米国とその利益に影響を及ぼす前に積極的な妨害を行うため、前方防衛の方針を通じてサイバー空間作戦を活用することを強調している。 2024 年 3 月、国防総省は防衛産業基盤サイバーセキュリティ戦略を発表し、よりレジリエンスの高い統合軍と防衛エコシステムを維持するための実行可能な枠組みを提供した。 2023 年、米サイバー司令部のサイバー・ナショナル・ミッション部隊は 17 カ国に 22 回展開し、海外での悪質なサイバー活動を特定し、敵対勢力の行動の自由を制約するパートナー支援型のハント・フォワード・オペレーションを実施した。

2023 年 10 月、ホワイトハウスが主導するランサムウェア対策イニシアチブ（CRI）は、世界中のランサムウェア活動を撃退するための国際的な取り組みを調整するため、第 3 回サミットを開催した。 今年、CRI はランサムウェアの攻撃とインフラを破壊する能力の開発、情報共有の改善、ランサムウェアのエコシステムの構造的基盤に対する反撃に焦点を当てた。 これらの目標を達成するため、CRI は、情報共有と作戦協力プラットフォームの確立、CRI メンバーのサイバー能力の構築、およびメンバー政府は身代金を支払うべきではないという CRI 初の政策声明を共同で発表する新たなコミットメントを発表した。

米国が同盟国やパートナーと連携することで、テイクダウンやその他の破壊活動はより効果的なものとなり、敵対国により厳しい結果をもたらし、被害者によりインパクトのある支援を提供することができる。 これらの活動はまた、外交行動、経済制裁、悪意のあるサイバー行為者に影響を与えるよう調整されたその他のツールと組み合わせることもできる。 同盟国やパートナーはまた、悪意のあるサイバー活動を特定し、敵対者の TTP に関する重要な詳細を提供する共同 CSA の作成に大きく貢献している。 海外のパートナーとのさらなる情報共有と作戦上の協力を可能にするため、FBI はサイバーアシスタント法務担当官の海外駐在を 40%近く拡大した。

民間事業者はまた、サイバー脅威情報の共有を通じて、重要インフラ全体のサイバー脅威に対する認識を高める上で重要な役割を果たしている。 民間セクターの組織は、連邦政府にはない悪意ある活動のある側面を可視化していることが多い。 これらの組織が法執行機関と直接、あるいは NSA の CCC や CISA の JCDC を通じて情報を共有することに積極的であることは、脅威を評価・理解し、軽減策を考案し、被害者への通知を促進する連邦政府の能力を強化する。

★★★★★★

連邦政府は、悪意ある行為者が米国を拠点とするクラウド、AI、その他のサードパーティ・サービスを悪用するのを防ぐためのルール作りに取り組んでいる。 2024 年 1 月、商務省は、人工知能の安全、セキュア、かつ信頼できる開発と使用に関する EO14110、および重大な悪意のあるサイバーイネーブル活動に関する国家緊急事態に対処するための追加的な措置を講じることに関する EO13984 に基づき、米国の Infrastructure-as-a-Service プロバイダに対し、悪意のあるサイバー活動を可能にする外国人による製品およびサービスの悪用を防止することを義務付ける規則を提案した。

連邦政府は、サイバー犯罪活動に対抗し、敵対勢力が悪意ある目標を達成するためにサイバー能力を使用することを思いとどまらせるために、混乱キャンペーンの速度、規模、影響力を高めてきた。 以下のキャンペーンは、世界中の被害者に影響を及ぼしている悪質なサイバー活動を混乱させるための米国の最近の行動の範囲を示している：

- **2023 年 1 月**：司法省は、80 カ国以上で 1,500 人以上の被害者を出していた HIVE ランサムウェアグループに対する破壊キャンペーンを発表した。 FBI と国際的パートナーは HIVE のネットワークに侵入し、復号鍵を奪い、被害者がその鍵を利用できるようにした。 CISA、FBI、HHS は、共同 CSA を通じて HIVE の侵害指標（IOC）と TTP を普及させた。

- **2023 年 5 月**：司法省はコードネーム「MEDUSA」と呼ばれる作戦を発表し、「Snake」と呼ばれる巧妙なグローバルマルウェアネットワークを破壊した。 この作戦では、FBI が作成したツールを使用して、侵害されたコンピュータ上のマルウェアを無効化した。 同時に、FBI、NSA、CISA、国防総省サイバー・ナショナル・ミッション・フォース、および国際的パートナーは、マルウェアをロシア連邦保安局（FSB）に帰属させる共同 CSA を発表した。

- **2023** 年 **7 月** CISA は、年初来、400 件以上のランサムウェア作戦の未遂を阻止したと発表した。 CISA は、被害者に対し、さらなる搾取や被害を防ぐ最善の方法に関するアドバイスと技術情報を提供することで、これらの作戦を阻止した。

- **2023 年 8 月**：司法省は、Qakbot ボットネットとマルウェアを妨害し、そのインフラをダウンさせた多国籍作戦を発表した。 2023 年、サイバー犯罪者はこのインフラを利用して、世界中でランサムウェアや金融詐欺などの犯罪行為を行っていた。 このボットネットの解体には、侵害されたインフラへの包括的なアクセスを獲得し、被害者のコンピュータから悪質なコードを削除するためのカスタムスクリプトを導入する必要があった。 FBI はまた、不正

な利益として 860 万ドルの暗号通貨を押収した。 CISA と FBI は共同 CSA を通じて Qakbot のインフラ IOC を配布した。

- **2023 年 12 月**：司法省は、世界中で 1,000 人以上の被害者を出していた ALPHV/Blackcat ランサムウェアグループに対する破壊キャンペーンを発表した。 当時、ALPHV/Blackcat は世界で 2 番目に人気のあるランサムウェア・アズ・ア・サービスの亜種であり、恐喝ランサムウェア攻撃を実行するための使いやすいツールセットをサイバー犯罪者に提供していた。 FBI は復号化ツールを開発し、現場事務所や国際的なパートナーが被害を受けた被害者に支援を提供できるようにした。 CISA と FBI は、共同 CSA を通じて ALPHV/Blackcat の IOC と TTP を普及させた。

- **2023** 年 **12 月**司法省は、暗号通貨取引所である Bitzlato Ltd.の創設者であり大株主であるアナトリー・レグコディモフが、ダークマーケットでの売買の主要な仲介者であり、ランサムウェア犯罪者による不正取引の隠れ家でもあったことを認め、不正な資金を送金する送金業の罪を認めたと発表した。

- **2024 年 1 月**：司法省は、裁判所が認可したオンライン作戦により、PRC の国家支援組織が米国および同盟国の重要インフラのハッキングを隠蔽するために使用したボットネットを破壊したと発表した。 PRC の関係者は、米国の重要インフラ・ネットワークへのハッキングを隠蔽し、密かにアクセスするために、小規模家庭/小規模オフィス（SOHO）ルーターで構成されるボットネットを使用していた。 FBI、CISA、NSA は、PRC の TTP に関する詳細な技術情報を記載した複数の CSA を発行し、サイバーセキュリティの専門家がネットワークへの同様の侵入を検知・防止できるようにした。

- **2024 年 2 月：**司法省は、世界各地で 2,000 人以上の被害者を出していたランサムウェア「LockBit」グループの破壊キャンペーンを、他の国際的な法執行パートナーと連携して実施することを発表した。 英国も FBI や他のパートナーと協力し、被害に遭った被害者のために復号化機能を開発した。

- **2024 年 2 月**：司法省は、ロシアの軍事情報機関である GRU が運営する、侵害された数千台の SOHO ルーターで構成されるボットネットを破壊するためのオンライン作戦を発表した。 GRU はこのボットネットを、Moobot マルウェアで SOHO ルーターを危険にさらした犯罪ハッカーを共用して作成し、主にウクライナをターゲットとしたキャンペーンを含むスピアフィッシングや類似のクレデンシャル・ハーベスティングを支援するためのグローバル

★★★★★★

な情報収集プラットフォームにしていた。 米国は、ロシアの侵略行為やその他の悪意ある活動を促進するために使用される重要なツールをロシアの情報機関から奪った。

連邦政府のネットワークを守る

連邦政府のネットワークと重要インフラを標的にした重大なサイバーインシデントを受け、EO 14028 は、連邦システム全体で基本的なセキュリティ対策を確立することにより、サイバーセキュリティに対する連邦政府のアプローチにパラダイムシフトをもたらした。 NSM-8 は、NSS の安全確保に対する責任を明確にすることで、わが国の最も重要なシステムのサイバーセキュリティに対する説明責任をさらに変革した。 さらに同政権は、集団的防衛を支援するシステムに投資するサイバーセキュリティ近代化アジェンダを策定し、連邦民間エンタープライズ全体でゼロ・トラスト・アーキテクチャ（ZTA）を採用する最初の戦略を策定した。

2023 年、最高財務責任者（CFO）法の民間機関は、サイバーセキュリティ態勢を改善するために、インパクトの大きいサイバーセキュリティの実践を進展させた。 これらの実践には、転送中および静止中のデータの暗号化、フィッシングに強い多要素認証（MFA）の導入、エンドポイント検知・対応（EDR）サービスの導入、ロギング機能、熟練したサイバーセキュリティ・チームの雇用などの進展が含まれる。 2024 会計年度の第 1 四半期までに、CFO 法の民間機関は、四半期ごとの連邦情報システム近代化法の指標によって測定される以下の成果を実証した：

- **暗号化：**複数の CFO 法民間機関が 10%以上の増加を示している。
- **MFA:**大半の機関でフィッシングに強い MFA の導入が改善され、10 機関では少なくとも 20%以上のフィッシングに強い MFA の導入が確認された。
- **EDR：**少なくとも 1 つの EDR プラットフォームがカバーするエンドポイントの平均割合は 92%に達した。
- **ロギング：**5 つの機関が、すべての高価値資産に対して「高度な」ロギング機能を達成した。 行政管理予算局（OMB）と CISA は、インシデント対応活動を支援する、より効果的なログ収集を推進するためのワーキンググループを立ち上げた。
- **熟練サイバーセキュリティチームの採用：**各機関は引き続きサイバーセキュリティの熟練チーム採用を強化し、平均充足率 91%を達成した。

★★★★★★

連邦政府システムを迅速かつ大規模に防御するためには、政府は省庁を横断したエンタープライズ・レベルのリスク・ビューを進める必要がある。 共有サービスの採用を通じて、各省庁はその能力を強化し、攻撃対象領域を縮小し、連邦ネットワーク全体の可視性を向上させてきた。 2023 年 10 月、OMB と ONCD は省庁間ワーキンググループを招集し、連邦政府全体におけるサイバーセキュリティ共有サービ スの展開と利用について調査し、プロバイダと顧客にインタビューを行い、小規模・零細省庁に共有サービ スを導入する際のギャップと課題を特定した。

CISA は、「Known Exploited Vulnerabilities」カタログなどの政府全体の文書に沿った「Continuous Diagnostics and Mitigation（CDM）」プログラムを通じて、重要な脅威を理解し管理できるようにするとともに、サイバーセキュリティ・リスクを特定し、優先順位を付け、低減するためのより高い能力を各省庁に提供した。 2023 年、CISA は CDM プログラムを民間 CFO 法の全 23 機関と非 CFO 法の 69 機関に拡大し、97 機関を防御ドメインネームシステム・サービスに組み込むことで、共有サービスへの移行を可能にした。

CISA、OMB、および ONCD は、連邦文民行政機関に強化されたログ機能をプロバイダとして提供することの実現可能性を判断するために、産業界と協力してきた。 2024 年 2 月、これらの関与の結果、すべての機関に拡張ログが展開され、デフォルトのログ保存期間が 90 日から 180 日に延長された。 この大きな一歩は、テクノロジープロバイダーに「高品質の監査ログを追加料金なしで顧客に提供する」ことを求める CISA の Secure by Design ガイダンスに沿ったものである。

NSA 長官は、NSS のナショナル・マネージャーとして、より一元化された説明責任、政策プロセスの整合性、連邦の所有者と運営者全体にわたる NSS の標準の正式化を通じて、70 を超える連邦省庁のサイバー調整と連携を強化し続けている。

ONCD は、省庁間のパートナーと協力して、インターネット・ルーティング・セキュリティの改善を推進する計画を策定し、BGP の脆弱性への対処に焦点を当てた。 これらの脆弱性は、RPKI ROA（Resource Public Key Infrastructure Route Origin Authorizations）などのソリューションによって対処できる。 ガバナンスは、連邦政府機関用のレガシー登録サービス契約テンプレートを開発し、RPKI ROA の採用を促進するためのプレイブックを開発している。 このソリューションは、採用の大きな障壁を取り除き、RPKI ROA の政府全体への導入を促進する。

また、集団的な運用防御を改善し、侵害を迅速に隔離・修復できるようにする取り組みも進められている。 CISA の Persistent Access Capability は、大統領令 14028 から生まれた EDR イニシアチブを広く採用することで可能になったもので、リアルタイムの脅威情報共有を促進している。 連

★★★★★★

邦政府の ZTA への意図的なシフト、共有サービスの拡大、集団的運用防御の成熟は、現在のサイバー脅威の状況に対処し、将来の課題に備えるための協調的な努力を反映している。

国家サイバー人材の強化

全国で未充足のサイバー職の数は、国家安全保障上の課題であると同時に、多大な経済的機会でもあり、官民の組織は幅広い創造的な解決策を追求している。 2023 年 7 月に発表された国家サイバー人材・教育戦略（NCWES）は、サイバー人材の当面のニーズに対処するため、政府全体および社会全体のアプローチを優先している。 NCWES は 3 つの指針に焦点を当てている。(1)サイバー労働力の需要を満たすために協力的な労働力開発のエコシステムを活用する、(2)サイバー・スキルの生涯追求を可能にする、(3)多様性と包括性の拡大を通じてサイバー労働力を強化する。

連邦政府全体の高官が米国全土で戦略的なアウトリーチ活動を実施し、労働者、教育者、雇用主、地方・州・連邦政府レベルの政府指導者からサイバー人材に関する見解を集めた。 2024 年 3 月現在、90 以上の組織が NCWES の支援にコミットしており、その中には、13,000 人以上のサイバー職の雇用、2 億 8,000 万ドル以上の米国人の基礎的サイバー技能の習得、サイバー教育の変革、国家サイバー労働力の拡大、連邦サイバー労働力の強化などが含まれている。

NCWES は、サイバー教育へのアクセスが、持続可能な方法で国家サイバー労働力のニーズを満たすために必要であることを明確にしている。 NSA によって国立サイバーセキュリティ・センター・オブ・エクセレンス（NCAE-C）に指定された 440 校以上の大学が、毎年何千人もの学生に厳格なサイバーセキュリティ教育を提供している。 これらの NCAE-C 機構のうち 100 校以上が CyberCorps® に参加している：全米科学財団（NSF）が DHS および OPM と協力して主導する「SFS（Scholarship for Service)」プログラムに参加している。高校生がこれらのプログラムに参加できるよう、教育省が資金を提供するキャリア・技術教育(CTE)プログラムは、技術的スキルの開発だけでなく、キャリアのアドバイスやナビゲーションを提供し、その範囲を中学校にまで広げている。 NSA が運営し、NSA と NSF が資金を提供する GenCyber プログラムは、非公式のサマーキャンプ学習環境で、K-12 の教師と生徒のサイバー・スキルを開発している。 連邦政府の一貫した献身的な支援により、これらの取り組みは STEM 教育におけるイノベーションを拡大し、国家サイバー人材の持続的な育成の基盤を提供し続けることができる。

NIST NICE プログラムは、NICE Interagency Coordinating Council を通じて、連邦政府のサイバーセキュリティ教育と人材育成プログラムを調整している。 NICE はまた、NICE 戦略計画を実施する作業部会を含む NICE 地域調整協議会（NICE Community Coordinating Council）を通じて、連携するコミュニティを促進し、活性化させている。 NICE は、インタラクティブなジョブヒ

★★★★★★

ートマップを提供する CyberSeek.org の継続的な開発と、毎年米国サイバーチームを選出する米国サイバーゲームの協力協定を支援している。 2024 年 3 月に更新される NICE Workforce Framework for CyberSecurity は、官民のサイバーセキュリティの仕事と労働者を説明する共通の語彙を確立する。

サイバー人材育成・教育への取り組みは、小学校でのキャリア認識から始まり、中学年でのキャリアナビゲーション、高校での技術スキル準備といったスキル開発を、雇用、高等教育、起業、軍への入隊につなげることで最も効果的となる。 このようなプログラムの例としては、以下のようなものがある：

- CHIPS と科学法を通じて、NSF の地域イノベーションエンジンプログラムは、サイバーワークフォースのエコシステムを成長させるための計画助成金を提供している。 2023 年 5 月、NSF は米国の 46 の州と地域にまたがる 44 のエンジン開発賞を発表し、将来の NSF エンジンの計画を立てるために、それぞれ 2 年間で最高 100 万ドルの資金が提供された。

- 毎年開催される NICE K-12 Cybersecurity Education Conference と NICE K-12 Community of Interest は、教師の専門能力開発を支援し、学校管理者にサイバーセキュリティのキャリアの発見を促進するために必要な戦略とリソースを提供する。

- 2023 年 4 月、NIST は 15 の州における 18 のサイバーセキュリティ教育・人材育成プログラム取得者（Regional Alliances and Multistakeholder Partnerships Stimulating (RAMPS) cybersecurity education and workforce development program recipients）に協力協定を授与し、2023 年 3 月にはさらに 15 件の追加授与のための資金調達機会通知を発表した。これらの RAMPS コミュニティは、サイバーセキュリティ教育と労働力開発の統合されたエコシステムを構築し、地域経済を支援する。

- 教育省は、サイバーセキュリティ技能開発に使用できるキャリア・技術教育フォーミュラ補助金を各州に提供している。

- 一般調達局（GSA）は、政府横断的な U.S. Digital Corps（USDC）フェローシップ・プログラムを運営している。2023 年に USDC は、9 人のサイバーセキュリティ・フェローを含む 47 人の早期キャリアの技術人材を連邦政府に採用した。

- DOE には、エネルギー部門を対象とした複数のサイバー人材育成・教育プログラムがある。 CyberForce は、チーム戦と個人戦で技能を試す大学サイバー防衛競技会である。 オペレーショナル・テクノロジー（OT）ディフェンダー・フェローシップは、エネルギー部

★★★★★★

門の中・上級 OT セキュリティ・マネジャーに、エネルギー・インフラを標的にする戦略と、それに対抗するためのサイバーセキュリティ・ツールと戦術について学ぶ機会を提供する。 CyberStrike は、ICS に焦点を当てた実践的なトレーニングであり、エネルギー部門のオーナーやオペレーターのためのパイプラインや再スキルアップのための人材育成を支援する。

- 2024 年 3 月、DOE は大学を拠点とする 6 つの電力サイバーセキュリティセンターの設立に 1500 万ドルの資金を提供すると発表した。このセンターは、エネルギー・セキュリティ研究のギャップに対処し、サイバーセキュリティ教育を提供するために、エネルギー部門全体の協力を促進する。

各省庁はまた、多様で多様な経路がサイバー人材に必要なスキルを提供できることを認識し、それぞれのニーズに合った人材育成アプローチを構築している。 例えば、国防総省は「国防総省サイバー人材戦略 *2023-2027*」とそれに付随する実施計画を発表し、熟練した多様なサイバー人材を育成する方法に取り組んでいる。 OPM は、連邦政府のサイバー労働力を強化し、より良い報酬を得るための政府全体の課題と機会を取り上げた立法案を作成した。

ソフトウェア・セキュリティの向上により、より安全な製品とサービスを生み出す

ソフトウェア・セキュリティの改善は、デジタル・エコシステム全体のシステミック・リスクを低減する。 この機会を捉えるため、連邦政府は産業界、学界、市民社会と協力して、セキュア・バイ・デザインの原則と実践を推進し、リスクを軽減するために最も適した立場にあり、最も十分なリソースを有する組織にセキュリティの責任を転嫁している。 これらの行動は、ソフトウェア製品やサービスにおけるサイバーセキュリティの脆弱性に対する責任を確立するための可能な法律の土台を築くものである。

2023 年 4 月、CISA は「サイバーセキュリティリスクのバランスをシフトする：セキュア・バイ・デザインの原則とアプローチ（*Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design*）」を発表した。これは、セキュア・バイ・デザインの原則を実施するための具体的な手順を組織に提供するために、米国および国際的なパートナーとともに開発したガイダンス文書である。 2023 年 10 月、CISA とそのパートナー（新たに加わった 8 つの国際機関の共同シーラーを含む）は、何百もの利害関係者からのフィードバックを反映した共同ガイダンスの更新版を発表した。 2023 年末、CISA は、セキュアなソフトウェア開発の実践と技術製品におけるセキュリティ防御に関するガイダンスを提供する初の「セキュア・バイ・デザイン（Secure by Design）」アラートも発表した。

★★★★★★

2024 年 3 月、CISA はセキュアソフトウェア開発証明書を発表した。これは、連邦政府に販売するソフトウェア製造者がセキュアな開発技術とツールセットを活用していることを確認するのに役立つ。 この書式は OMB との協議によりドラフトされ、NIST セキュア・ソフトウェア開発フレームワークで確立されたプラクティスに基づいている。

ソフトウェア部品表（SBOM）は、ソフトウェアのサプライチェーンリスクマネジメントの実践を強化することができる。 2023 年 12 月、NSA、ODNI、および CISA は、SBOM の効果的な実装と、ソフトウェア開発ライフサイクルへのオープンソースコンポーネントの安全な統合に関する業界向けガイダンスを含む技術報告書を発表した。 同月、NSA は「ソフトウェア部品表（*SBOM*）管理のための勧告」を発表した。この勧告は、ベストプラクティスに焦点を当て、NSS がサイバーセキュリティのサプライチェーン・リスクマネジメントのニーズに適した SBOM 管理機能を組み込むための勧告を提供するものである。

メモリー安全プログラミング言語を採用することで、ソフトウェア開発のエコシステムはより安全な製品やサービスを生み出すことができる。 メモリー安全プログラミング言語は、オープンソースソフトウェアとプロプライエタリソフトウェアの双方に恩恵をもたらし、デジタルエコシステム全体の脆弱性のクラス全体を排除することができる。 2023 年 12 月、CISA、NSA、FBI、および国際的なパートナーの技術専門家は、メモリー安全ロードマップのケースを発表した。 2024 年 2 月、ONCD は「*Back to the Building Blocks*」を発表した：*A Path Toward Secure and Measurable Software*）を発表し、技術コミュニティが解決に貢献できる 2 つのセキュリティ課題として、メモリ安全性とソフトウェア測定可能性を強調した。

連邦政府は、オープンソース開発者コミュニティを支援し、オープンソースコンポーネントの安全な統合を可能にすることを優先事項としている。 オープンソースソフトウェアセキュリティイニシアティブ（OS3I）は、オープンソースソフトウェアのセキュリティとレジリエンスを向上させるために、官民の利害関係者を招集している。 2023 年 8 月、ONCD はオープンソースソフトウェアのセキュリティとメモリー安全プログラミング言語に関する一般からの意見を求めた。 CISA はまた、オープンソースソフトウェア・セキュリティ・ロードマップを発表し、この分野での作業に優先順位をつけた。

消費者に力を与え、保護するデジタル経済を実現する

米国民は、安全で、公正で、アクセスしやすく、サイバー脅威に対して確実に安全なハードウェアとソフトウェアを生産するデジタル経済に参加できなければならない。 政権は、消費者に力を与

★★★★★★

え、イノベーションを促進し、サイバーセキュアな競争を奨励するため、市場形成のためのさまざまな手段を追求してきた。

2024 年 3 月、FCC は、米国人がより安全でサイバー攻撃に対する脆弱性の少ないスマートデバイスを購入できるよう支援する自主的なサイバーセキュリティ認証・表示プログラムである「米国サイバートラストマーク」を承認した。 このプログラムでは、ユニークで強力なデフォルト・パスワードの要求やソフトウェア・アップデートの安全な実装など、NIST が定める一定のサイバーセキュリティ規準を満たす IoT 機器が認証の対象となる。 すでに、大手家電メーカーや小売業者数社が、このプログラムの実施を支援することを表明している。 2023 年 7 月、DOE は、スマートメーターやソーラーインバータのような OT にラベルのアプローチを適用することの実現可能性と制限に対処するためのラベル研究努力を発表した。

連邦政府は、連邦政府の支出によって、サイバーセキュリティとレジリエンスを向上させるための措置を講じている。 国防総省、一般調達局（GSA）、NASA は、連邦調達規則（FAR）の改正を提案し、脆弱性のある IoT デバイスの購入を禁止し、SBOM の使用を義務付けるなど、非機密扱いの連邦情報システムに対するサイバーセキュリティ要件を標準化し、改善した。 連邦政府が調達するテクノロジー製品のサイバーセキュリティ標準を引き上げることは、エコシステム全体のサイバーセキュリティを促進することになる。

偽請求法（False Claims Act）に基づき、司法省の民事サイバー詐欺イニシアチブは、政府請負業者がその製品やサービスのサイバーセキュリティ属性について重大な虚偽説明を行った場合に、その責任を追及している。 2023 年、司法省は、自社製品が連邦契約と結びついたサイバーセキュリティ管理を満たしていると虚偽の説明をしていたベンダー2 社と和解に達した。

2023 年末、財務省は、壊滅的なサイバー事象に対する連邦保険対応の必要性についての初期アセスメントを完了し、そのような対応の適切な形態についてさらなる検討が必要であり、CISA および ONCD と連携して、アセスメントの次のフェーズで実施されることを明らかにした。 CISA はまた、サイバーセキュリティ保険・データ分析ワーキンググループの再結成を発表し、政府と業界の関係者が情報交換を行い、サイバーリスクの低減における保険業界の役割について議論する場を設けることを明らかにした。

レジリエンスに優れた次世代技術への投資

セキュリティとレジリエンスをデジタル・エコシステムの技術基盤に組み込むことは、後からボルトで取り付けるよりも安価で効率的なアプローチである。 2023 年、米国大統領の「米国投資アジ

★★★★★★

エンダ（Invest in America Agenda）」を原動力とする米国のイノベー ションと公共投資は、サイバーセキュリティのための重要な技術や新技術が開発・導入される際に、それらを 最適化するための官民協調の取り組みの機会を創出した。 例えば、DOE は 2023 年 11 月、電気協同組合、地方自治体、小規模な投資家所有の公益事業者のサイバーセキュリティ態勢を強化するため、「地方および自治体の公益事業に関するサイバーセキュリティ助成金および技術支援 BIL プログラム」を通じて 7,000 万ドルの資金を提供すると発表した。 このプログラムは、これらの小規模公益事業者がサイバーセキュリティの脅威から保護、検知、対応、回復するのを支援し、サイバーセキュリティ脅威情報共有プログラムへの参加を増やすものである。

現在進行中のクリーンエネルギーへの移行は、国家インフラとクリーンエネル ギーのサプライチェーンの基盤全体にわたって、安全性とレジリエンスを構築する機会を提 供するものである。 BIL および IRA に含まれる補助金プログラムの実施を通じて、DOE および他の連邦パート ナーは、補助金取得者がより安全なクリーンエネルギー技術を調達し、実施できるようにしている。 BIL はまた、同法に基づき資金提供される特定のプロジェクトに対し、そのライフサイクルにわたってプロジェクトのサイバーセキュリティを維持・改善するためのサイバーセキュリティ計画を含めることを義務付けている。

2023 年 7 月、DOE は分散型エネルギー資源（DER）のサイバーセキュリティを推進する 8 つの革新的な中小企業に資金を提供し、9 月には DER のサイバーセキュリティを推進する 9 つの新しい国立研究所プロジェクトに 3,900 万ドルの資金提供を発表した。 また 2023 年 9 月には、DOE クリーン・エネルギー・サイバーセキュリティ・アクセラレータ（DOE Clean Energy Cybersecurity Accelerator）の第 1 期生が卒業し、産業制御システム向けの認証・認可ソリューションを提供する実現技術に焦点が当てられた。 DOE はさらに、国家サイバーインフォームド・エンジニアリング戦略（National Cyber-Informed Engineering Strategy）の実施ガイドを発表し、エネルギーインフラの設計にサイバーセキュリティを組み込む組織を支援した。 2024 年 1 月、DOE は、クリーンエネルギー供給インフラをサイバー攻撃から保護する次世代ツールの研究・開発・実証（RD&D）を支援する 3,000 万ドルの資金提供機会も発表した。

連邦政府は、最先端のサイバーセキュリティとレジリエンス技術の研究開発に資金を提供している。 *2023* 年連邦サイバーセキュリティ研究開発戦略計画は、NCS と整合し、人間中心のサイ バーセキュリティ、信頼性、サイバーレジリエンス、評価指標、研究開発インフラなど、連邦政府資金 の優先順位に関する具体的な指針を連邦政府機関に提供している。 この計画はまた、サイバーセキュリティのリスクを軽減できる重要かつ新たな技術やイノベーションなど、2025 会計年度予算における複数省庁の研究開発の優先事項をまとめた 2023 年 8 月の OMB-OSTP 共同メモとも整合し

ている。 NSF は、Secure and Trustworthy Cyberspace プログラムを通じて、重要インフラのセキュリティとレジリエンスに焦点を当てた研究プロジェクトに資金を提供している。

行政は、インターネットの根本的な技術基盤に長年存在する脆弱性を保護するため、官民の行動を調整している。 BGP をよりセキュアにすることで、セキュアでないインターネット・ルーティングによる被害を大幅に減らすことができる。 2023 年 7 月、FCC と CISA は、連邦政府のパートナー、非営利団体、およびインターネット・サービス・プロバイダやクラウド・コンテンツ・プロバイダを含む業界のパートナーを招集し、最新の BGP セキュリティ改善に関する共通理解を深め、それらを加速するための取り組みを調整した。

2023 年 10 月、大統領は人工知能の安全、安心、信頼できる開発と利用に関する EO 14110 に署名し、価値観に沿った AI の開発を形成するための政府全体の取り組みを指示した。 EO 14110 は、AI がサイバーセキュリティ・コミュニティに影響を与える可能性のあるさまざまな方法を取り上げている。 第一に、より効率的なサイバー防衛活動を可能にする AI の活用方法を探るため、EO14110 は、重要なソフトウェアの脆弱性を発見・修正する AI ツールを開発する先進サイバーセキュリティ・プログラムを設立する。 第 2 に、AI が重要インフラにもたらす潜在的リスクを低減するため、EO 14110 は DHS に対し、AI 安全・セキュリティ委員会を設置し、NIST の AI リスクマネジメントフレームワークに基づき、重要インフラの所有者および運営者に安全・セキュリティガイドラインを提供するよう指示している。 第三に、サイバー脅威から AI エコシステムを保護するため、特定の AI モデルの開発者は、高度な脅威行為者に対する防御能力を商務省に報告することが義務付けられる。

連邦政府は、量子コンピューター以降の未来に備え、幅広いステークホルダーとの取り組みを続けている。 2023 年 8 月、NIST は、暗号解読に関連する量子コンピュータによる将来の攻撃に対抗するために設計された 3 つの連邦情報処理標準（FIPS）ドラフトをパブリックコメントに提出した。 連邦政府以外の暗号移行を支援するため、OMB、CISA、NIST、NSA は、各組織が独自の量子対応ロードマップを策定し、実施するためのリソースを公開した。 NIST、NSA、パートナーは、NIST が期待するポスト量子暗号標準を多様なセキュリティ標準に統合するため、複数の標準策定組織と連携している。 NIST はまた、NIST 国立サイバーセキュリティ・センター・オブ・エクセレンスにおいて、暗号の移行に関連する課題を特定し、それに対処するために、産学官のステークホルダーからなるワーキンググループとの連携を継続している。

★★★★★★

データ・セキュリティとプライバシーのリスクマネジメント

国家的なデータ・プライバシー法がない中、米国政府は、米国人のデータとプライバシーを保護し、安全でデータ・リッチな国境を越えた商取引を可能にするための的を絞った措置を追求している。

EO *14117*（*Preventing Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern*）は、司法長官に認可を与え、米国人の個人データの懸念国への大規模な移転を防止し、それらの国が米国人のセンシティブなデータにアクセスできるようにするその他の活動に対するセーフガードを提供する。 EO 14117 によって認可された防御は、ゲノムデータ、生体データ、個人健康データ、地理位置データ、金融データ、および敵対者が悪意のあるサイバー活動を含む様々な悪意のある目的のために悪用する可能性のある特定の種類の個人識別データに及ぶ。

2023 年 7 月に最終決定された EU と米国のデータ・プライバシー枠組みは、安全で信頼できる国境を越えたデータの流れに必要な国際的パートナーシップの代表例である。 同枠組みの最終決定と同時に、商務省は国境を越えたデータ移転に参加する企業のためのデータ・プライバシー枠組みプログラムのウェブサイトを公開した。

人工知能の安全、安心、信頼できる開発と使用に関する EO14110 は、新興技術におけるプライバシーリスクの低減の重要性を強化している。 EO 14110 は、各省庁に対し、AI の開発と展開において米国人のプライバシーを保護するための措置を講じるよう指示している。 2023 年 12 月、NIST は各省庁向けに差分プライバシー保証保護の評価に関するガイダンス草案を発表した。 2024 年 2 月、DOE と NSF は、プライバシー強化技術（PETs）の研究、開発、実装を進めるための Research Coordination Network を設立した。

PET は、安全で信頼でき、権利を尊重するデジタル・エコシステムを目指す政権の肯定的ビジョンの重要な一部である。 PETs を活用する連邦政府の取り組みを調整するため、同政権は 2023 年 3 月、「プライバシー保護データ共有・分析を推進する国家戦略」を発表した。 同戦略は、医療、気候変動、金融犯罪、人身売買、パンデミック対応といった共通の課題に取り組む上で役立つ形で、PETs の研究、開発、採用のためのロードマップを提供している。 米国はまた、2023 年 3 月の民主主義のためのサミットで受賞者を発表した PETs Prize Challenge を通じて、国際的なパートナーや学界の関係者と協力してきた。

★★★★★★

世界中でセキュリティとレジリエンスを強化する

サイバー空間はグローバルな領域であり、米国は同盟国やパートナーと手を携えて、共通のサイバー脅威から防衛し、共通のレジリエンスを構築している。 このような集団防衛のアプローチは、統合化が進む作戦能力と、戦略的な連携の深化の両方に根ざしている。 昨年、連邦政府各省庁は、フィンランド、韓国、ヨルダンを含む広範な海外パートナーとの二国間協力を強化するための新たな取り決めに調印した。

2023 年を通じて、米国は危機の際にパートナーや同盟国に対応し、コスタリカやアルバニアなどの国々を資金、リソース、技術的専門知識で支援し、サイバー攻撃からの復旧を支援した。 最近のインシデントから、より安全でレジリエンスに優れたサイバーエコシステムを構築するためには、即時のインシデント対応リソースと長期的な技術支援の両方が必要であることが示された。

政権は引き続き、パートナーのサイバー能力構築のための柔軟で革新的な道筋を拡大していく。 議会の支援を受けて設立された新しい「サイバー空間・デジタル接続・関連技術基金」は、紛争の内外を問わず、パートナーのニーズに合わせて規模を拡大できる持続的な資金調達メカニズムの必要性を認識している。 この基金が全額拠出されれば、国務省は柔軟かつ強固で、迅速な対応が可能なサイバー、デジタル、新興技術プログラムを通じて対外援助を提供することができる。

同政権はまた、同盟国、パートナー、民間セクターと協力し、サイバー能力を構築している。 例えば、2023 年 12 月、米国、ウクライナ、その他 9 つのパートナーの間で、ウクライナを支援するための民間サイバー能力構築を調整・促進する手段として、タリン・メカニズムが正式に発足した。 タリン・メカニズムは、ウクライナの長期的なサイバー・レジリエンスと備えを強化するため、政府と民間部門の双方からの支援と貢献を体系化したものである。

米国は、米州機構（OAS）、西アフリカ諸国経済共同体（ECOWAS）、東南アジア諸国連合（ASEAN）などの地域連合を活用し、サイバーセキュリティ支援の需要が範囲と規模の両面で拡大する中、サイバーセキュリティ能力を構築してきた。 2023 年 9 月、DHS は第 1 回西半球サイバー会議を開催し、21 カ国の政府からサイバーセキュリティのリーダーを招集してサイバーセキュリティの課題を議論し、協力分野を特定した。 持続可能なサイバー・キャパシティ・ビルディングに関するマルチステークホルダーによるグローバルな取り組みを支援するため、米国は「サイバー・レジリエンス開発のためのアクラ・コール」を承認した：行動フレームワーク」を承認した。

2024 年 5 月、国務省は「国際サイバー空間・デジタル政策戦略」を発表し、デジタル連帯、多国間関与、連合構築、国際サイバー能力の強化に関する政権の積極的なビジョンを打ち出した。 この

★★★★★★

戦略の重要な要素は、同盟国やパートナーと協力し、デジタル・エコシステムの安全性を確保することである。

同政権は、5G や 6G、クラウドインフラやデータセンター、半導体、海底ケーブル、衛星コミュニケーションといった技術の研究開発、標準開発、サプライチェーンのセキュリティと多様化を優先している。国務省の国際技術セキュリティ・イノベーション（ITSI）基金は、世界の半導体サプライチェーンの多様化、安全な ICT 接続の促進、機敏な対応プログラムの提供、外国の敵対勢力から米国人の機密データを保護するために、5 年間で年間 1 億ドルを提供する。 国務省はまた、研修プログラムの拡充により、国内外における独自の専門知識と能力を強化しており、2024 年末までに、これらの問題に関与するすべてのミッションに、訓練を受けたサイバー・デジタル政策担当官を配置する予定である。

権利尊重のデジタル・エコシステムを推進する

米国は、志を同じくする同盟国やパートナーとともに、デジタル世界がわれわれの共有する民主主義的価値を反映し、強化するよう取り組んでいる。 世界各国は、テクノロジーの恩恵について、人権を尊重した肯定的なビジョンを推進すると同時に、テクノロジーの悪用やデジタル権威主義の台頭への対策に取り組んでいる。

この課題に対応するため、2023 年と 2024 年の民主主義首脳会議では、米国と 70 カ国以上が、オープンで自由、グローバル、相互運用可能、信頼性が高く、アクセス可能で安全なインターネットという肯定的なビジョンを推進し、商業スパイウェアのようなデジタル技術の拡散や悪用と闘い、民主主義の価値と人権に沿った新たな技術を形成するというコミットメントを強調した。 これらの国々の多くは、フリーダム・オンライン連合を通じて、インターネットの自由を支援し、世界中の人権を守るために米国とともに活動している。 2023 年、米国はフリーダム・オンライン連合の議長国に就任し、インターネットの自由を支える標準と規範を形成する同連合の活動を強化した。

CISA は、高度な持続的脅威の標的にされるリスクが高まっており、自ら防御する能力が限られているコミュニティと提携するため、「高リスク・コミュニティ防御イニシアティブ」を立ち上げた。CISA は市民社会組織やテクノロジー企業と提携し、市民社会のサイバーセキュリティを向上させるリソースを開発してきた。 国境を越えた弾圧の脅威にさらされる市民社会のサイバーセキュリティに関する戦略的対話」を通して、CISA は英国、オーストラリア、カナダ、デンマーク、エストニア、フランス、日本、ニュージーランド、ノルウェーの関係者と協力し、市民社会のサイバーセキュリティを強化し、国境を越えた弾圧に対するレジリエンスを向上させるための世界的な取り組みを進めてきた。

★★★★★★

ガバナンスは、デジタル抑圧の最も侵入的な形態の 1 つである商用スパイウェアの拡散と悪用に対抗するため、政府を挙げて取り組んでいる。 2023 年 3 月に発行された「国家安全保障にリスクをもたらす商用スパイウェアの米国政府による使用禁止に関する EO 14093」は、国家安全保障にリスクをもたらす、または外国政府もしくは外国人による不正使用の重大なリスクをもたらす商用スパイウェアの米国政府による運用上の使用を制限するものである。 EO14093 は、商用スパイウェアの拡散と悪用がもたらす脅威に対抗するための広範なキャンペーンの第一歩である。(2)特定の商用スパイウェアベンダーに対する商務省の輸出規制の継続、(3)商用スパイウェアを悪用したり、その悪用から利益を得たりする者を対象とした国務省の新しいビザ発給禁止政策、(4)商用スパイウェアベンダーとその指導者に対する財務省の制裁。

当政権は、我々のデジタル・エコシステムにおける既存の脆弱性の被害を低減するだけでなく、国際的なサイバー規範を通じて我々の価値を促進することを目指している。 米国は、サイバー空間における国家の責任ある行動に関する国連（UN）の枠組みを推進し、信頼醸成措置を進展させ、国連オープンエンド・ワーキング・グループを通じて規範を堅持することにコミットしている。 米国はまた、国連の枠組みを推進するため、常設の国連サイバー行動計画（POA）の設立を引き続き推進しており、総会では 161 の政府がこのようなメカニズムの設立を支持する票を投じた。

米国は、同盟国やパートナー、米・EU 貿易技術評議会や国際電気通信連合などの組織と協力し、米国の価値観に沿った技術標準を策定していく。 2023 年 5 月、同政権は史上初となる「クリティカルで新たな技術のための国家標準化戦略」を発表した。この戦略では、透明性、開放性、公平性とコンセンサス、有効性と妥当性、一貫性、幅広い参加を包含する標準の肯定的ビジョンを提唱している。

★★★★★★

今後の見通し

米国のサイバーセキュリティ態勢に関する *2024* 年報告書」は、防御可能でレジリエンスに優れ、我々の価値観に沿ったデジタル・エコシステムという NCS のビジョンを実現するために、連邦政府全体で行われているサイバーセキュリティ・イニシアチブの幅広さと深さを強調している。 戦略的環境は今後も進化し続け、新たな技術的・ガバナンス的課題だけでなく、チャンスももたらされるだろうが、現在のプログラムの多くは今後数年間にわたって存続し続けるだろう。 政権の確固としたビジョンに向けた一歩一歩の積み重ねが、サイバーセキュリティの態勢を強化し、全国の地域社会の経済的繁栄を築くことになる。

連邦政府が現在行っている取り組みの継続的な実施と並行して、来年度に特に焦点を当てる必要のある取り組みがいくつかある。 2025 会計年度の大統領予算概算要求では、それぞれに資源が割り当てられている。

- SRMA として指定された責務を持つ連邦機関は、米国の重要インフラのセキュリティとレジリエンス政策および国土安全保障法に沿って、それぞれの部門内での業務協力を可能にし、重要インフラの所有者および運営者に専門的な知識を提供するための努力を引き続き強化しなければならない。

- 各省庁は、国家サイバー人材を強化し、サイバー教育を改善し、連邦サイバー人材が直面する固有の課題に対処するため、多様なプログラムや権限を通じて NCWES を大規模に実施していく。

- CIRCIA の実施により、すべての重要インフラ部門の対象事業体に対して、特定のサイバーセキュリティインシデントを連邦政府に報告する新たな要件が設けられる。 これらの報告に含まれる情報は、悪意のあるサイバー活動やランサムウェアに対する新たな可視性を提供し、部門横断的なリスクに対する理解を深め、集団的防衛を強化する。 CISA および CIRCIA の責任を持つ他の省庁は、これらの新しいインシデント報告を受け取り、処理し、共有し、対応する準備を進めている。

- 2023 年、司法省は悪質なサイバー活動を阻止し対応する能力を高めるため、国家安全保障サイバー課を新設した。 このセクションは、国家的敵対勢力とその代理人による、ますます巧妙で攻撃的になるサイバー脅威に取り組むため、司法省全体、政府内、海外、民間部門の連携を促進する。

★★★★★★

- サイバーセキュリティの共通運用環境を構築するため、CISA は新しいサイバー分析・データシステムを開発している。 このインフラは、サイバーセキュリティのデータセットを統合し、データの取り込みと統合を促進する内部ツールと機能を提供し、悪質なサイバー活動の迅速な特定、検知、低減、防止を支援するためのデータ分析を組織化し、自動化するために使用される。

- 連邦政府は、NSM-10「脆弱な暗号システムに対するリスクを低減しつつ、量子コンピューティングにおける米国のリーダーシップを促進する」に基づき、脆弱な公共ネットワークおよびシステムの量子耐性暗号への移行計画を継続している。 2023 年、連邦省庁は脆弱性のある暗号アルゴリズムを含む可能性のある連邦暗号システムの最初のインベントリを作成し、量子耐性暗号移行にかかるコスト見積もりを作成した。これらのインベントリとコスト見積もりは、今後の移行活動の計画に反映される。

NCSIP バージョン 2 は、2023 年の成功に基づき、リソース調整のための青写真を作成する。
ONCD は、実施プロセスの透明性を維持し、連邦の一貫性を確保することを約束し、NCSIP は、完了した作業を反映し、ダイナミックなサイバー脅威の状況の新たな要求を満たすために必要な措置を特定するために、毎年更新され続ける。