国家サイバーセキュリティ戦略実施計画

2024 年 5 月

バージョン 2

THE WHITE HOUSE
WASHINGTON

★★★★★★

序文

バイデン大統領の国家サイバーセキュリティ戦略は、すべての米国人にとって安全でセキュアなデジタル・エコシステムの恩恵をフルに享受できるよう、サイバー空間に対する大胆で肯定的なビジョンを示している。　すなわち、サイバー空間を防衛する責任を、より能力の高い主体へと再配分すること、そして、サイバーセキュリティとレジリエンシーへの長期的な投資を促進するために、インセンティブを再編成することである。

国家サイバーセキュリティ戦略（NCS）の実施には、米国政府と米国社会全体が協調・協力して行動することが必要である。　国家サイバーセキュリティ戦略実施計画（NCSIP）はこの取り組みのロードマップであり、国家安全保障、公共の安全、経済的繁栄を守るために国家権力のツールを活用する。　国家サイバー長官室（ONCD）はこの作業を調整し、大統領と議会に実施状況を報告する。

これは NCSIP の第 2 版であり、2023 年 7 月に発表された第 1 版をベースにしている。NCSIP 第 2 版では、戦略の目標を達成するために連邦政府が進めている、行政の可視化と省庁間の調整を必要とする、インパクトの大きい 100 のイニシアティブが記述されている。　これらのイニシアチブは、最初の NCSIP に記載されたイニシアチブを引き継ぎ、追加し、構築するものであり、国家サイバーセキュリティ戦略で求められている戦略目標に向けて国家を前進させるものである。　最初のバージョンと同様に、各イニシアチブは担当機関に割り当てられ、完了までのスケジュールが設定されている。　ONCD は引き続き行政管理予算局（OMB）と協力し、大統領予算要求における資金調達案が実施計画における活動と整合していることを確認する。

民間部門、市民社会、州、地方、部族、地域政府、国際パートナー、そして政府議会との緊密な協力は、引き続き不可欠である。　各省庁は、本計画のイニシアティブを実施し、可能であれば新たなパートナーシップを構築するため、関係者と引き続き協力していく。　アセスメントは、利害関係者からのフィードバック、イニシアティブの完了、およびその有効性の評価に基づいて、実施計画のイニシアティブを模索し、実施計画の将来のバージョンに反映させていく。

本計画のいかなる内容も、新法または現行法、あるいは大統領方針の実施を損なったり、そ の他の形で影響を及ぼすものと解釈されてはならない。

★★★★★★

実施計画リーディングガイド

実施計画は、5 つの柱と 27 の戦略目標を持つ国家サイバーセキュリティ戦略に沿うように、柱と戦略目標ごとに構成されている。　各イニシアチブの分野は以下の通りである：

柱 - イニシアチブが該当する柱。

戦略目標（Strategic Objective） - イニシアチブに関連する戦略目標。

イニシアティブ番号 - <柱>.<戦略目標>.<イニシアティブ番号>の形式で、特定のイニシアティブに関連付けられた固有の番号。

イニシアチブのタイトル： - 戦略目標の全体的な成果を支援するアクションのタイトル。

イニシアチブの説明 - 行動に関連する活動の説明。

国家サイバーセキュリティ戦略(NCS)の参照 - 戦略の具体的な文言がイニシアチブと関連付けられている。

責任機関 - 他の利害関係者とのイニシアチブを主導する責任を負う連邦機関。　責任機関は、そのイニシアチブの下で貢献事業体との調整を行い、相違点を解決するために ONCD と協働する責任を負う。

貢献事業体 - 該当する場合、専門知識や資源の提供、補完的な取り組みへの関与、プログラムの要素に関する調整など、イニシアチブの開発および実施において重要な役割を持つ連邦省庁。　これは、イニシアチブの利害関係を有するすべての機関の包括的なリストとなることを意図したものではない。

完了日 - 米国政府の会計年度内の四半期ごとの完了予定日。

新しい取り組み：青枠で囲んだイニシアチブは、NCSIP バージョン 2 の新イニシアチブである**。**

キャリーオーバーの取り組み：**グレーの枠で囲んだ**イニシアチブは、NCSIP バージョン 1 から継続している。

完了したイニシアティブ：**緑色の枠で囲ま**れ、斜体で表示されているイニシアティブは、*NCSIP* バージョン *1* のイニシアティブであり、完了日が *24* 年度第 *2* 四半期以前のものである。これらは、各イニシアティブの継続的な進捗状況を反映し、*NCS* の各戦略目標を達成するための政府全体の取り組みを示すために、*NCSIP* バージョン *2* に含まれている**。**

★★★★★★

実施計画のロールアップ イニシアチブ

第一の柱：重要インフラの防衛

1.1 国家安全保障と公共の安全を支えるサイバーセキュリティ要件を確立する。

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。

1.1.2 重要インフラ部門全体でサイバーセキュリティ要件を設定する。

1.1.3 規制の整合性に情報を提供するために、フレームワークや国際標準の利用を増やす。

1.1.4 医療・公衆衛生部門全体でサイバーセキュリティのベストプラクティスの採用を推進する。

1.1.5 サイバーセキュリティ規制の相互優遇試験プログラムを検討する。

1.2 官民協働の規模

1.2.1 セキュアバイデザインとセキュアバイデフォルト技術の開発と採用を推進するために、官民パートナーシップを拡大する。

1.2.2 重要インフラセクターと *SRMA* の指定に関する勧告を提供する。

1.2.3 CISA が既存の報告メカニズムをどのように活用できるか、または SRMA のセクター固有のシステムとプロセスを統合し運用するための単一ポータルをどのように構築できるかを評価する。

1.2.4 情報共有と協力のプラットフォーム、プロセス、およびメカニズムの新規および改善の機会を調査する。

1.2.5 国家コーディネーター事務所を設置する

1.2.6 サイバーセキュリティの取り組みを調整し、教育施設サブセクター全体のベストプラクティスを推進するための協働メカニズムを確立する。

1.2.7 米国農務省（USDA）のルーラル・ユーティリティ・サービス（RUS）、ルーラル・ウォーター・サーキット・ライダー・プログラム（Rural Water Circuit Rider Program）、および EPA の技術支援プログラムを通じて、サイバーセキュリティの教育と訓練を継続する。

1.2.8 上下水道セクター全体でサイバーセキュリティのベストプラクティスの採用を引き続き推進する。

★★★★★★

1.3 連邦サイバーセキュリティセンターを統合する。

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 ンターの能力と、スピードと規模での協力に必要な 計画をアセスメントし、改善する。

1.3.2 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分類法を策定する。

1.3.3 エネルギー脅威分析センター(ETAC)の開発を通じて、エネルギー部門内の業務協力を強化する。

1.4 連邦政府のインシデント対応計画とプロセスを更新する。

1.4.1 国家サイバーインシデント対応計画（NCIRP）を更新する。

1.4.2 CIRCIA（重要インフラサイバーインシデント報告法）規則の最終版を発行する。

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開発する。

1.4.4 必要な権限を持つサイバー安全審査委員会（*CSRB*）を成文化するための法律をドラフトする。

1.4.5 サイバーインシデントや事象に関する対応リソースを分析する

1.5 連邦防衛を近代化する

1.5.1 連邦文民行政機関(FCEB)システムの機密保護

1.5.2 連邦文民行政機関(FCEB)テクノロジーの近代化

1.5.3 連邦文民行政機関（FCEB）における国家安全保障システム（NSS）の安全確保

1.5.4 連邦の未分類のシステム全体で、サイバーセキュリティシェアードサービスの利用拡大を推進し、アセスメントする。

1.5.5 サイバーサプライチェーンリスクマネジメント（C-SCRM）を推進し、サプライチェーンリスク情報の効果的なエンタープライズ全体での共有を奨励する。

★★★★★★

第二の柱：脅威行為者の破壊と解体

2.1 連邦政府の破壊活動を統合する

2.1.1 最新の国防総省サイバー戦略を公表する

2.1.2 国家サイバー捜査官合同タスクフォース（NCIJTF）の能力を強化する。

2.1.3 混乱キャンペーンに特化した組織のプラットフォームを拡大する。

2.1.4 サイバー犯罪およびサイバー犯罪を誘発する犯罪を阻止するための法律を提案する。

2.1.5 破壊活動のスピードと規模を拡大する

2.1.6 2023 年国防総省サイバー戦略を実施する

2.1.7 少年犯罪者によるサイバー犯罪およびサイバー犯罪を可能にする犯罪を防止、抑止、阻止する。

2.2 敵対勢力を攪乱するために官民の作戦協力を強化する

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。

2.2.2 悪質なサイバー活動を妨害するために、民間事業体と連邦政府機関との連携を強化する。

2.3 情報共有と被害者通知のスピードと規模を拡大する

2.3.1 各部門特有のインテリジェンスのニーズと優先事項を特定し、運用する。

2.3.2 サイバー脅威インテリジェンスとデータを重要インフラの所有者と運用者に提供する際の障壁を取り除く。

2.4 米国を拠点とするインフラの悪用を防ぐ

2.4.1 IaaS（インフラストラクチャ・アズ・ア・サービス）プロバイダと再販業者の要件、標準、 手続きに関する規則制定提案通知を公表する。

2.5 サイバー犯罪対策、ランサムウェアを撃退する

2.5.1 ランサムウェア犯罪者の隠れ家を抑制する

2.5.2 ランサムウェア犯罪を阻止する

★★★★★★

2.5.3 ランサムウェア犯罪を調査し、ランサムウェアのエコシステムを破壊する

2.5.4 ランサムウェアのリスクを低減するための民間部門および州、地方、部族、地域（SLTT）の取り組みを支援する。

2.5.5 仮想資産サービスプロバイダに対する世界的なマネーロンダリング・テロ資金供与対策（AML/CFT）標準を採用し、実施するための他国の取り組みを支援する。

2.5.6 ランサムウェア犯罪者のセーフヘイブンを阻害するための国際関与計画を実施する

2.5.7 共同作戦でランサムウェア犯罪を阻止する

★★★★★★

第三の柱安全保障とレジリエンスを推進するために市場の力を形成する

3.1 データの管理者に責任を負わせる

3.1.1 国家プライバシー研究戦略の更新

3.2 セキュアな IoT デバイスの開発を推進する

3.2.1 *2020* 年モノのインターネット（*IoT*）サイバーセキュリティ改善法に基づく連邦調達規則（*FAR*）要件を実施する。

3.2.2 米国政府の *IoT* セキュリティ・ラベリング・プログラムを開始する。

3.2.3 将来のスマートグリッドを開発するために、サイバーセキュリティのラベリング規準を研究・開発する。

3.2.4 米国政府の IoT セキュリティ・ラベリング・プログラムを策定する。

3.3 安全でないソフトウェア製品およびサービスに対する責任の転嫁

3.3.1 長期的、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求する。

3.3.2 ソフトウェア部品表(SBOM)を進め、未サポートソフトウェアのリスクを低減する

3.3.3 連携した脆弱性の開示

3.3.4 オープンソースソフトウェアのセキュリ ティリスクを把握するためのアプローチ の実現可能性をアセスメントする

3.3.5 長期的、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求する。

3.4 連邦補助金やその他のインセンティブを利用して、安全保障を構築する。

3.4.1 連邦補助金を活用して、インフラのサイバーセキュリティを改善する。

3.4.2 サイバーセキュリティ研究のための資金を優先的に調達する。

3.4.3 サイバーセキュリティの社会的、行動的、経済的研究に関す るサイバーセキュリティの研究、開発、実証を優先する。

★★★★★★

3.5 連邦調達を活用して説明責任を改善する

3.5.1 大統領令 14028 に基づく連邦調達規則（FAR）の変更を実施する。

3.5.2 ベンダーのサイバーセキュリティを改善するために、偽請求法を活用する。

3.6 連邦サイバー保険のバックアップを探る

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。

★★★★★★

第 4 の柱：レジリエンス溢れる未来への投資

4.1 インターネットの技術的基盤を確保する

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主導する

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。 プログラミング言語の採用を促進する。

4.1.3 インターネットの基盤となるインフラ機能と技術の開発、標準化、採用を加速する。

4.1.4 インターネットの基盤となるインフラ機能と技術の開発と標準化を加速し、その採用を支援する。

4.1.5 セキュアなインターネット・ルーティングを推進するために、主要な利害関係者と協力する。

4.1.6 セキュアなインターネットルーティング技術とテクノロジー導入のためのロードマップを実施する。

4.1.7 サイバー空間のビルディングブロック全体にわたって、安全で測定可能なソフトウェアソリューションを推進する。

4.1.8 より安全なオープンソースソフトウェアのエコシステムを促進する。

4.2 サイバーセキュリティのための連邦研究開発を再活性化する。

4.2.1 メモリー安全プログラミング言語の成熟、採用、安全性を加速する。

4.3 ポスト量子未来に備える

4.3.1 国家安全保障に関する覚書-10 を実施する

4.3.2 国家安全保障システム（NSS）に NSM-10 を導入する。

4.3.3 ポスト量子暗号アルゴリズムを標準化し、移行をサポートする。

4.4 クリーンなエネルギーの未来を確保する

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により、その採用を推進する。

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。

★★★★★★

4.4.3 サイバーインフォームドエンジニアリングの原則を使用した、エンジニアと技術者のためのトレーニング、ツール、サポートを構築し、改良する。

4.4.4 米国政府の脱炭素化目標を支援・実現するデジタル・エコシステムを推進する計画を実施する。

4.4.5 エネルギー部門の利害関係者と連携して、配電および分散型エネルギー資源（DER）のサイバーセキュリティ原則の策定と採用を推進する。

4.5 デジタル・アイデンティティ・エコシステムの開発を支援する

4.5.1 官民の協力を通じて、デジタル ID エコシステムの革新を支援する研究と指針を推進する。

4.6 サイバー人材強化のための国家戦略を策定する

*4.6.*1 国家サイバー人材・教育戦略を発表し、その実施を追跡する。

4.6.2 国家サイバー人材・教育戦略の実施と報告

4.6.3 技能に基づいた雇用慣行を推進する

★★★★★★

第 5 の柱共通の目標を達成するために国際的なパートナーシップを築く

5.1 デジタル・エコシステムに対する脅威に対抗するための連合を構築する

5.1.1 地域サイバー連携・調整のための省庁間チームを設置する。

5.1.2 国際サイバー空間・デジタル政策戦略を発表する。

5.1.3 同盟国やパートナーとの連邦法執行機関の協力体制を強化する。

5.1.4 地域サイバーハブ研究

5.1.5 国際サイバー空間・デジタル政策戦略を実施する。

5.2 国際パートナーの能力を強化する

5.2.1 国際パートナーのサイバー能力を強化する

5.2.2 運用法執行の協力を通じて、国際パートナーのサイバー能力を拡大する。

5.3 同盟国やパートナーを支援する米国の能力を拡大する

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、柔軟な海外支援メカニズムを確立する。

5.4 国家の責任ある行動に関するグローバルな規範を強化するための連合を構築する。

5.4.1 無責任な国家が約束を守らなかった場合、その責任を問う。

5.5 情報、コミュニケーション、運用技術製品・サービスの安全なグローバルサプライチェーン

5.5.1 安全で信頼できる情報通信技術（*ICT*）ネットワークとサービスの開発を促進する。

5.5.2 信頼できる情報通信技術（*ICT*）ベンダーの、より多様でレジリエンスに富んだサプライチェーンを促進する。

5.5.3 公共無線サプライチェーンイノベーション基金（*PWSCIF*）の運営を開始する。

5.5.4 サイバーセキュリティサプライチェーンリスクマネジメント(CSCRM)の主要なプラクティスを、重要インフラセクター全体及びセクター内で普及・浸透させる。

5.5.5 半導体の安全な開発・製造のためのガイダンスを作成する。

★★★★★★

5.5.6 オープンで相互運用可能な無線**ネットワークの**開発を支援するため、PWSCIF 補助金の交付を継続する。

★★★★★★

全社的な取り組み

6.1 有効性のアセスメント

6.1.1 国家サイバーセキュリティ戦略の実施に関する進捗と効果を報告する。

6.1.2 国家サイバーセキュリティ戦略の実施に教訓を適用する。

6.1.3 予算ガイダンスを国家サイバーセキュリティ戦略の実施と整合させる。

★★★★★★

第 1 の柱：重要インフラの防衛

戦略目標 1.1：国家安全保障と公共安全を支えるサイバーセキュリティ要件を確立する。

イニシアティブ番号：*1.1.1*

イニシアチブのタイトル：サイバー規制の調和に関するイニシアチブを確立する

イニシアティブ番号：1.1.2

イニシアチブのタイトル：重要インフラ部門全体でサイバーセキュリティ要件を設定する。

イニシアチブの内容

現在進行中の国家安全保障会議（NSC）主導の政策決定プロセスを通じて、国家安全保障局（SRMA）と規制当局は、各業界のサイバーリスクを分析し、既存の権限をどのように活用して、そのセクターのリスクを軽減するサイバー要件を確立し、セクター固有のニーズを考慮し、権限のギャップを特定し、それを埋めるための提案を策定するのかを概説する。

NCS リファレンス

連邦政府は、既存の認可を利用して、重要な部門に必要なサイバーセキュリティ要件を設定する。 連邦省庁がサイバーセキュリティの最低要件を実施するための法的権限に空白がある場合、認可は議会と協力して空白を埋める。

責任機関 NSC

事業体：SRMA、ONCD

完了時期：25 年度第 2 四半期

イニシアティブ番号：1.1.3

イニシアチブのタイトル：規制の整合性に情報を提供するために、規制当局がフレームワークや国際標準を利用する機会を増やす。

★★★★★★

イニシアチブの内容

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）は、時間の経過とともに改善、改良され、進化している。 更新は、パフォーマンス・ベースのフレームワークが技術や脅威のトレンドに対応し、学んだ教訓を統合し、ベスト・プラクティスを一般的なプラクティスに移行させるのに役立つ。 NIST は、フレームワークの大幅なアップデートを策定している：CSF 2.0 である。 NIST は最終的な CSF 2.0 を発行し、連邦政府機関から要請があれば、国際標準や NIST CSF と規制の整合に関する技術支援を提供する。

NCS リファレンス

規制はパフォーマンス・ベースであるべきであり、既存のサイバーセキュリティの枠組み、自主的なコンセンサス標準、ガイダンス（サイバーセキュリティとインフラを含む）を活用すべきである。

サイバーセキュリティ・インフラフラセキュリティ庁（CISA）の「サイバーセキュリティ・パフォーマンス目標」と国立標準技術研究所（NIST）の「重要インフラ・サイバーセキュリティ改善のためのフレームワーク」である。

責任機関 NIST

貢献した事業体 CISA、SRMA

完了時期：25 年度第 1 四半期

イニシアティブ番号：1.1.4

イニシアチブのタイトル：医療・公衆衛生部門全体でサイバーセキュリティのベストプラクティスの採用を促進する。

イニシアチブの内容

保健社会福祉省（HHS）は、国家安全保障覚書-22 に基づき義務付けられている部門別リスクマネジメント計画の一環として、医療・公衆衛生部門全体でサイバーセキュリティのベストプラクティスを採用することを引き続き強調し、部門全体で実施と説明責任の強化を支援する HHS 全体の戦略を実施する。

NCS リファレンス

連邦政府は、既存の認可を利用して、重要な部門に必要なサイバーセキュリティ要件を設定する。 連邦省庁がサイバーセキュリティの最低要件を実施するための法的権限に空白がある場合、認可は議会と協力してその空白を埋める。

責任機関 HHS

貢献事業体：CISA **完了年月：**25 年度第 1 四半期 **イニシアチブ番号：**1.1.5

★★★★★★

イニシアチブのタイトル：サイバーセキュリティ規制の相互主義パイロットプログラムを検討する。

イニシアチブの内容

国家サイバー長官室（Office of National Cyber Director：ONCD）は、（独立行政機関の規制当局のためのサイバーセキュリティフォーラムを含む）規制当局と協力し、規制の調和に関する情報提供要請から得られた知見を基に、調和と相互主義のアプローチをモデル化したサイバーセキュリティの基本要件を確立するために、1 つ以上の規制の調和と相互主義のパイロットプログラムを検討する。

NCS リファレンス

ONCD は、行政管理予算局（OMB）と協調して、以下のことを主導する。

サイバーセキュリティ規制の調和に関する行政の取り組み。サイバーインシデント報告協議会は、連邦政府のインシデント報告要件を調整し、対立を解消し、調和させる。

責任機関 ONCD

貢献した事業体 CISA、OMB

完了時期：25 年度第 2 四半期

★★★★★★

戦略目標 1.2：官民協働の拡大

イニシアティブ番号：1.2.1

イニシアティブのタイトルセキュア・バイ・デザインおよびセキュア・バイ・デフォルト・テクノロジーの開発と採用を推進するために、官民パートナーシップを拡大する。

イニシアチブの内容

サイバーセキュリティ・インフラセキュリティ庁は、技術製造者、教育者、非営利組織、学界、オープンソースソフトウェアコミュニティなどとの官民パートナーシップを主導し、セキュアバイデザインおよびセキュアバイデフォルトのソフトウェアとハードウェアの開発と採用を推進する。 CISA は、NIST、必要に応じて SRMA を含む他の連邦機関、および民間セクターと協力し、まず既存の関連する国際、産業、政府の標準および慣行を活用するセキュア・バイ・デザインおよびセキュア・バイ・デフォルトの原則と慣行を策定する。 CISA は、このような原則やベストプラクティスの採用を阻む障壁を特定し、民間セクター全体でこれらの原則を採用するための集団的行動を推進するよう努める。 セキュア・バイ・デザインおよびセキュア・バイ・デフォルトの原則と既存の標準や慣行との間のギャップが特定された場合、CISA、NIST、NSF、および必要に応じて SRMA を含む他の連邦機関は、それらのギャップを埋めるためのオープンで透明性のある官民パートナーシップを主導する。

NCS リファレンス

連邦政府はまた、より高いセキュリティとレジリエンスを実現するために、サイバーの状況を再構築する能力を持つソフトウェア、ハードウェア、マネージド・セキュリティ・サービス・プロバイダーとの業務上および戦略上の協力関係を深める。**責任機関** CISA

協力事業体：NIST、NSF、SRMA

完了時期： 24 年度第 4 四半期

イニシアチブ番号：*1.2.2*

イニシアチブのタイトル：重要インフラセクターと *SRMA* の指定に関する提言を行う。

イニシアティブ番号：1.2.3

イニシアチブのタイトル：CISA が既存の報告メカニズムをどのように活用できるか、または SRMA のセクター固有のシステムとプロセスを統合し運用するための単一ポータルをどのように構築できるかを評価する。

★★★★★★

イニシアチブの内容

サイバーセキュリティ・インフラセキュリティ庁は SRMA と協力し、情報共有にどのようなギャップが存在するかを理解し、SRMA および他の連邦パートナー間の情報交換のための相互運用可能なシステムの要件を理解する。 SRMA がすでに強固な情報共有能力を有していない場合、CISA は SRMA と協力して、その能力を成熟させるプロセスを開発する。

NCS リファレンス

民間部門との連携により、CISA と SRMA は、データのマシン間共有を強化し、発展させるための技術的・組織的メカニズムを探求する。**責任機関** CISA

貢献した事業体司法省、FBI、NSA、SRMA

完了時期： 24 年度第 3 四半期

イニシアティブ番号：1.2.4

イニシアチブのタイトル：情報共有とコラボレーションのプラットフォーム、プロセス、メカニズムを新規に改善する機会を調査する。

イニシアチブの内容

サイバーセキュリティ・インフラセキュリティ庁は、官民連携の仕組みを見直すセクター横断的な取り組みを主導する。 SRMA は、必要に応じて CISA と連携し、セクター連携協議会、情報共有分析センター（ISAC）、情報 共有分析組織（ISAO）、新興セクター連携イニシアティブ、その他の事業体など、各セクター の活動を代表し、官民連携の成熟度モデルを策定するために CISA に提供する。

NCS リファレンス

数十年にわたる ISAC や ISAO との協力の経験に基づき、連邦政府は、ISAC や ISAO の活動を支援した。

ガバナンスは、これらのグループや他のグループと協力して、このモデルをどのように発展させるべきかについて、共通のビジョンを策定する。

責任ある機関 CISA

事業体：SRMA の場合

完了時期： 26 年度第 1 四半期

イニシアチブ番号：1.2.5

★★★★★★

イニシアチブのタイトル：国家コーディネーター事務所の設置 [1]

イニシアチブの内容

サイバーセキュリティ・インフラセキュリティ庁は、国家安全保障覚書-22 に従い、すべての SRMA を支援するための単一の窓口となる国家調整官事務所を設置する。 同オフィスは、SRMA の能力に応じて、SRMA を支援するための CISA リソースの提供を調整する。 CISA は各 SRMA と協力して、共有サービスの選択肢と機会の評価を含め、事務所からの支援に対するニーズと優先順位を定義し、必要に応じてこの情報を使用して CISA のサービスカタログを更新する。

NCS リファレンス

連邦政府は引き続き、CISA とその他の機関との連携を強化する。

SRMA は、SRMA の能力開発への投資、その他の方法により、SRMA が各セクターの重要インフ ラ所有者および運用者のニーズに積極的に対応できるようにする。 **責任機関** CISA

事業体：SRMA、NSC

完了時期：25 年度第 4 四半期

イニシアチブ番号：1.2.6

イニシアチブのタイトル：サイバーセキュリティの取り組みを調整し、教育施設サブセクター全体のベストプラクティスを推進するための協力体制を確立する。

イニシアチブの内容

教育省（Education Department of Education）は、国家安全保障覚書（National Security Memorandum）-22 に基づき義務付けられているサブセクター固有のリスクマネジメント計画の一環として、教育施設サブセクター全体の州、地方、部族、および準州の事業体とのサイバーセキュリティのベストプラクティスを推進するための政府調整協議会（Government Coordinating Council）を含む、正式なサイバーセキュリティ調整メカニズムを確立する。

NCS リファレンス

敵対的活動やその他の脅威から重要インフラを防衛するには、インターネットの分散構造を模倣したサイバー防衛モデルが必要である。私たちは、役割と責任を構造化し、データ、情報、知識の自動化された交

[1] NCSIP バージョン 1 のこの構想は、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の役割とそれに付随する責任を概説する新しい方針を反映したものである。

★★★★★★

換によって可能になる接続性を高めることによって、防衛者間の協力を発展させ、強化することによって、この分散されたネットワーク化されたモデルを実現する。

責任機関教育

貢献した事業体 GSA、CISA

完了時期： 24 年度第 4 四半期

イニシアチブ番号：1.2.7

イニシアティブのタイトル：米国農務省（USDA）のルーラル・ユーティリティ・サービス（RUS）のルーラル・ウォーター・サーキット・ライダー・プログラムおよび EPA の技術支援プログラムを通じて、サイバーセキュリティの教育と訓練を継続する。

イニシアチブの内容

米国農務省（USDA）は、水分野の SRMA として、また国家安全保障覚書-22 に基づき要求される上下水道分野に特化したリ スクマネジメント計画の一環として、環境保護局（EPA）と協力し、USDA RUS Rural Water Circuit Rider Program を拡大し、水道システムのサイバーセキュリティ技術支援、教育、訓練を含めるようパートナーと協働する。

NCS リファレンス

敵対的活動やその他の脅威から重要インフラを防衛するには、インターネットの分散構造を模倣したサイバー防衛モデルが必要である。私たちは、役割と責任を構造化し、データ、情報、知識の自動化された交換によって可能になる接続性を高めることによって、防衛者間の協力を発展させ、強化することによって、この分散されたネットワーク化されたモデルを実現する。

責任機関米国農務省

事業体：環境保護局

完了時期： 26 年度第 1 四半期

イニシアチブ番号：1.2.8

イニシアチブのタイトル：上下水道セクター全体でサイバーセキュリティのベストプラクティスの採用を引き続き推進する。

イニシアチブの内容

環境保護局は、国家安全保障覚書-22 の下で義務付けられている部門別リスクマネジメント計画の一環として、サイバーセキュリティのベストプラクティスに関するガイダンスだけでなく、サイバーセキュリテ

★★★★★★

ィのアセスメント、専門家による協議、トレーニングという形で技術支援を提供することにより、飲料水・下水処理施設におけるサイバーセキュリティのベストプラクティスの採用を促進し、州のサイバーセキュリティプログラムを支援する。

NCS リファレンス

…SRMA は、運営するシステムや資産を保護する責任を負う、各分野のオーナーやオペレーターをサポートする。

責任機関：EPA

貢献事業体：CISA

完了時期：25 年度第 1 四半期

★★★★★★

戦略目標 1.3：連邦サイバーセキュリティセンターの統合

イニシアティブ番号：*1.3.1*

イニシアチブのタイトル：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と、スピードと規模での協力に必要な計画をアセスメントし、改善する。

イニシアティブ番号：1.3.2

イニシアチブのタイトル：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分類法を開発する。

イニシアチブの内容

国家サイバー長官室は、省庁間パートナーと協力して、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責務を明確化・分類するための分類法を開発し、統合の取り組みに反映させる。

NCS リファレンス

連邦政府は、重要インフラの防衛を支援する総責任を負う省庁の認可と能力を調整しなければならない。

責任機関 ONCD

貢献した事業体 OMB

完了時期：25 年度第 1 四半期

イニシアティブ番号：1.3.3

イニシアティブのタイトルエネルギー脅威分析センター(ETAC)の開発を通じて、エネルギー部門内の業務協力を強化する。

イニシアチブの内容

エネルギー省（DOE）は、エネルギー脅威分析センター（ETAC）プログラムを継続し、ETAC に関与する官民のエネルギー関係者の数を拡大する。

NCS リファレンス

エネルギー省（DOE）のエネルギー脅威分析センター（ETAC）の試験的な運用など、SRMA における運用協力モデルは、タイムリーで実用的かつ関連性の高い情報を、各セクターの民間セクタ ー・パートナーと直接共有する機会を提供する。**責任機関** DOE

完了時期：25 年度第 1 四半期

★★★★★★

戦略目標 1.4：連邦インシデント対応計画とプロセスの更新

イニシアティブ番号：1.4.1

イニシアチブのタイトル：国家サイバーインシデント対応計画（NCIRP）の更新

イニシアチブの内容

サイバーセキュリティ・インフラセキュリティ庁は、ONCD と連携して、大統領政策指令 41 の下位にある国家サイバーインシデント対応計画（NCIRP）の更新プロセスを主導し、"一人への呼びかけは全員への呼びかけ" という方針をより完全に実現するためのプロセス、手順、システムを強化する。 NCIRP の更新には、インシデント対応と復旧における連邦機関の役割と能力に関する外部パートナーへの明確なガイダンスも含まれる。

NCS リファレンス

...CISA は、下位の国家サイバーインシデント対応計画（NCIRP）の更新プロセスを主導する。

責任ある機関 CISA

貢献した事業体司法省、FBI、SRMA、USSS、ONCD

完了時期：25 年度第 1 四半期

イニシアチブ番号：1.4.2

イニシアチブのタイトル：重要インフラのためのサイバーインシデント報告法（CIRCIA）最終規則の発行

イニシアチブの内容

サイバーセキュリティ・インフラセキュリティ庁は、SRMA、司法省（DOJ）、その他の連邦機関と協議し、CIRCIA を実施する。 CISA は、法定要件に従って CIRCIA Notice of Proposed Rulemaking と Final Rule を公表し、インシデント・レポートの適切な機関との共有を含む、インシデント・レポートの効果的な対応を進めるためのプロセスを策定する。

NCS リファレンス

CISA は、CIRCIA の規則制定と実施の過程において、SRMA、司法省、その他の連邦機関と協議する**：** CISA

貢献した事業体司法省、FBI、SRMA、USSS

完了時期：25 年度第 4 四半期

★★★★★★

イニシアティブ番号：*1.4.3*

イニシアチブのタイトル：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の開発

イニシアチブ番号：*1.4.4*

イニシアティブのタイトル必要な権限を有するサイバー安全審査委員会（*CSRB*）を成文化するための法案を作成する。

イニシアチブ番号：1.4.5

イニシアチブのタイトル：サイバーインシデントとイベントに関する対応リソースを分析する。

イニシアチブの内容

国家サイバー局長室は、国土安全保障省（DHS）および連邦緊急事態管理庁（FEMA）と協力し、CISA や FBI を含む連邦サイバー対応機関とともに、過去のサイバーインシデントへの対応で使用された予測可能なリソースや異常なリソースを分析するケーススタディを実施する。

NCS リファレンス

連邦政府の援助が必要な場合、連邦政府は統一され、調整された政府全体の対応を示さなければならない。

責任機関 ONCD

貢献した事業体連邦緊急事態管理庁

完了時期：25 年度第 2 四半期

★★★★★★

戦略目標 1.5：連邦防衛の近代化

イニシアチブ番号：1.5.1

イニシアチブのタイトル：連邦文民行政機関（FCEB）システムの機密保護

イニシアチブの内容

行政管理予算局は、CISA と連携し、集団的運用防衛を通じて未分類の FCEB システムを保護し、集中型共有サービス、エンタープライズ・ライセンス契約、ソフトウエア・サプライチェーン・リスク軽減の利用拡大を促進するための行動計画を策定する。

NCS リファレンス

OMB は、CISA と連携して、集団的運用防御、集中型共有サービスの利用可能性の拡大、ソフトウ ェアのサプライチェーンリスク低減を通じて、FCEB システムの安全を確保するための行動計画を策定する。**担当省庁** OMB

貢献した事業体：CISA, NIST, ONCD

完了時期： 24 年度第 2 四半期

イニシアチブ番号：1.5.2

イニシアチブのタイトル：連邦文民行政機関（FCEB）テクノロジーの近代化

イニシアチブの内容

行政管理予算局は、FCEB の技術近代化を加速させるための複数年にわたるライフサイクル計画の策定を主導し、維持コストが高く、防衛が困難なレガシーシステムの排除に連邦政府の努力を優先させる。

NCS リファレンス

OMB は、FCEB 技術の近代化を加速させるための複数年ライフサイクル計画の策定を主導し、維持コストが高く、防御が困難なレガシーシステムの排除に連邦の努力を優先させる。**責任機関** OMB

貢献した事業体：GSA、CISA、ONCD

完了時期： 24 年度第 4 四半期

イニシアチブ番号：1.5.3

イニシアチブのタイトル：連邦文民行政機関（FCEB）における国家安全保障システム（NSS）の安全確保

★★★★★★

イニシアチブの内容

国家安全保障局（NSA）は、国家安全保障システム担当国家管理者の責任を果たすにあたり、FCEB 機関における NSS のセキュリティに対応する計画を策定し、実行する。

NCS リファレンス

NSA 長官は NSS の国家管理者として OMB と調整し、NSM-8 の強化されたサイバーセキュリティ要件の実施を保証する FCEB 機関における NSS のための計画を策定する。 **責任機関** NSA **協力事業体** OMB、ONCD

完了時期： 24 年度第 4 四半期

イニシアチブ番号：1.5.4

イニシアチブのタイトル：連邦の未分類のシステム全体で、サイバーセキュリティ共有サービスの利用拡大を推進し、アセスメントする。

イニシアチブの内容

サイバーセキュリティ・インフラセキュリティ庁（CISA）は、OMB および ONCD と連携して、FCEB の未分類のシステム全体のリスクを低減する、高価値で費用対効果の高いサイバーセキュリティ共有サービスを目録化し、ベストプラクティスを活用し、プロセス指向の課題に対処することによって、主要な共有サービスをより効率的に理解し、実行する機会を特定する。

NCS リファレンス

OMB は、CISA と連携して、集団的運用防御、集中型共有サービスの利用可能性の拡大、ソフトウ ェアのサプライチェーンリスク低減を通じて、FCEB システムの安全を確保するための行動計画を策定する。
担当省庁 CISA

貢献した事業体：NIST、OMB、ONCD

完了時期：25 年度第 4 四半期

イニシアチブ番号: 1.5.5

イニシアチブのタイトル：サイバーサプライチェーンリスクマネジメント（C-SCRM）を推進し、サプライチェーンリスク情報の効果的なエンタープライズ全体での共有を奨励する。

イニシアチブの内容

一般調達局(GSA)は、様々なサプライチェーンリスクの特定、評価、低減、継続的監視を可能にし、敵対的脅威から保護するために、関連する専門的分析支援サービスとともに、複数コンポーネントからなるサ

★★★★★★

プライチェーンリスク照合・評価ツールへの政府全体のアクセスと利用を促進する。これらの投資は、ポスト量子暗号がサプライチェーンに与える影響の評価を含む C-SCRM を促進する。

NCS リファレンス

私たちは、連邦政府全体で集中的に行動することにより、連邦の結束力を高めていく……こうした取り組みは、これまでのプログラムを基礎とし、FCEB 情報システムを守るための政府全体のアプローチを前進させる行動を優先させる。

責任機関 GSA

貢献した事業体 OMB

完了時期：25 年度第 1 四半期

★★★★★★

第二の柱：脅威行為者の破壊と解体

戦略目標 2.1：連邦崩壊活動の統合

イニシアティブ番号：*2.1.1*

イニシアチブのタイトル：最新の国防総省サイバー戦略を発表する

イニシアティブ番号：2.1.2

イニシアチブのタイトル：国家サイバー捜査官合同タスクフォース（NCIJTF）の能力強化

イニシアチブの内容

NCIJTF は、掃討作戦と混乱キャンペーンをより迅速、大規模、高頻度で調整する能力を強化する。

NCS リファレンス

NCIJTF は、政府全体の混乱キャンペーンを調整する複数省庁の中心的存在として、より迅速かつ大規模で頻度の高い撤収・混乱キャンペーンを調整する能力を拡大する。**責任機関** FBI

貢献した事業体司法省

完了時期：25 年度第 4 四半期

イニシアティブ番号：2.1.3

イニシアチブのタイトル：混乱キャンペーンに特化した組織プラットフォームを拡大する

イニシアチブの内容

司法省は、このような脅威に特化した組織基盤を拡大し、サイバー業務に特化した有能な弁護士の数を増やすことで、サイバー犯罪者、国家敵対者、関連するイネイブラー（マネーロンダリングなど）に対する破壊キャンペーンの量と速度を増やす。

NCS リファレンス

このような統合破壊キャンペーンの量とスピードを高めるために、連邦政府は、継続的かつ協調的なオペレーションを可能にする技術的・組織的プラットフォームをさらに開発しなければならない。

責任機関司法省

★★★★★★

完了時期：25 年度第 1 四半期

イニシアティブ番号：*2.1.4*

イニシアティブ・タイトルサイバー犯罪およびサイバー犯罪を抑止するための法案を提案する。

イニシアティブ番号：2.1.5

イニシアチブのタイトル：破壊活動のスピードと規模を拡大する

イニシアチブの内容

国家サイバー捜査官合同タスクフォース、法執行機関、米サイバー軍司令部、NSA、インテリジェンス・コミュニティの他の要素は、これらの作戦のスピードと規模を拡大するために、混乱作戦を調整し実行するためのオプションメニューの開発を主導する。

NCS　リファレンス

このような統合破壊キャンペーンの量と速度を高めるために、連邦政府は、継続的で協調的な作戦を可能にする技術的・組織的プラットフォームをさらに開発しなければならない。　**責任機関** FBI

完了時期： 24 年度第 2 四半期

イニシアティブ番号：2.1.6

イニシアチブのタイトル：2023 年国防総省サイバー戦略の実施

イニシアチブの内容

国防総省（DoD）は、2023 年 DoD サイバー戦略の実施ガイダンスを完成させ、戦略で特定された 4 つの取り組み方針に沿った短期から中期のイニシアティブを通じて、ビジョンの達成に向けて前進する。イニシアティブは、米国とその利益に戦略的レベルの脅威をもたらす国家やその他の悪意ある行為者が引き起こす課題に対処する。　国防総省はまた、戦略の有効性をアセスメントし、政策、能力、資源の制約を特定する。

NCS リファレンス

…国防総省は、国家安全保障戦略、国家防衛戦略、そしてこの国家サイバーセキュリティ戦略に沿った最新のサイバー戦略を策定する。

責任機関国防総省

完了時期：25 年度第 3 四半期

★★★★★★

イニシアティブ番号：2.1.7

イニシアチブのタイトル：少年犯罪者によるサイバー犯罪およびサイバー犯罪を可能にする犯罪を防止、抑止、阻止する。

イニシアチブの内容

司法省は、連邦捜査局（FBI）および国土安全保障省（DHS）、さらに必要に応じて連邦政府、州政府、地方政府、部族政府、準州政府、国際機関、産業界のパートナーと協力し、ラプサス＄の見直しによる CSRB の勧告に沿った社会全体のアプローチを開発する。 このアプローチは、少年サイバー犯罪者の予防、抑止、方向転換を改善し、少年犯罪者による将来の悪質なサイバー活動を阻止するために、米国政府の既存のプログラムや政策を強化することを目指すものである。

NCS リファレンス

このような統合破壊キャンペーンの量と速度を高めるために、連邦政府は、継続的で協調的な作戦を可能にする技術的・組織的プラットフォームをさらに開発しなければならない。**責任機関**司法省

貢献した事業体 DHS、FBI

完了時期：25 年度第 1 四半期

★★★★★★

戦略目標 2.2：敵対勢力を攪乱するための官民作戦協力の強化

イニシアティブ番号： *2.2.1*

イニシアチブのタイトル： 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。

イニシアティブ番号： 2.2.2

イニシアチブのタイトル： 悪質なサイバー活動を阻止するため、民間事業体と連邦政府機関との連携を強化する。

イニシアチブの内容

国家サイバー長官室は、連邦機関と協力して、効果的な協力を支援する政策を特定し、民間事業体と連邦機関の間の協力のスピードと有用性を高める。

NCS リファレンス

悪意あるサイバー活動を効果的に阻止するには、独自の見識と能力を持つ民間事業体と、行動する手段と権限を持つ連邦政府機関との、より日常的な協力が必要である。

責任機関 ONCD

貢献した事業体 DoD、DOJ、CISA、FBI、NSA、**USSS**

完了時期：25 年度第 2 四半期

★★★★★★

戦略目標 2.3：情報共有と被害者通知のスピードと規模の拡大

イニシアティブ番号：2.3.1

イニシアチブのタイトル：セクター特有のインテリジェンスのニーズと優先事項を識別し、運用する。

イニシアチブの内容

2021 会計年度国防認可法 9002 条(c)(1)に規定された要件に従い、国家安全保障会議が政策決定プロセスを主導し、SRMA がセクター固有の情報ニーズと優先事項を特定するための合意されたアプローチを確立する。

NCS リファレンス

SRMA は、CISA、法執行機関、CTIIC と連携して、自部門における情報ニーズと優先事項を特定し、警告や技術的識別情報を共有するためのプロセスを開発する。

責任機関 NSC

貢献した事業体 DHS、司法省、ODNI、CIA、CISA、FBI、NSA、SRMA、USSS

完了時期：25 年度第 1 四半期

イニシアティブ番号：2.3.2

イニシアチブのタイトル：サイバー脅威インテリジェンスとデータを重要インフラの所有者と運営者に提供する際の障壁を取り除く。

イニシアチブの内容

国家情報長官室（ODNI）は、司法省（DOJ）および国土安全保障省（DHS）と連携して、重要インフラの所有者および運営者とサイバー脅威情報を共有するための方針および手順を見直し、これを可能にするためのクリアランスおよび情報アクセス拡大の必要性を評価する。

NCS リファレンス

連邦政府はまた、機密解除の方針とプロセスを見直し、実行可能なインテリジェンスを提供するために、さらなる機密アクセス権の拡大やクリアランスの拡大が必要な条件を判断する。

責任機関 ODNI

貢献した事業体 DoD、DHS、DOJ、NSA、FBI、NSC、ONCD

完了時期： 24 年度第 3 四半期

★★★★★★

戦略目標 2.4：米国を拠点とするインフラの悪用を防止する

イニシアティブ番号：*2.4.1*

イニシアチブのタイトル：インフラストラクチャ・アズ・ア・サービス（*IaaS*）プロバイダと再販業者のための要件、標準、手順に関する規則制定提案通知を公表する。

★★★★★★

戦略目標 2.5：サイバー犯罪対策、ランサムウェアの撲滅

イニシアティブ番号： *2.5.1*

イニシアチブのタイトル： ランサムウェア犯罪者の隠れ家を抑制する

イニシアチブ番号： *2.5.2*

イニシアチブのタイトル： ランサムウェア犯罪を阻止する

イニシアティブ番号： *2.5.3*

イニシアチブのタイトル： ランサムウェア犯罪を調査し、ランサムウェアのエコシステムを破壊する

イニシアティブ番号： 2.5.4

イニシアチブのタイトル： ランサムウェアのリスクを軽減するための民間部門および州、地方、部族、地域（SLTT）の取り組みを支援する。

イニシアチブの内容

サイバーセキュリティ・インフラセキュリティ庁は、JRTF（CISA と FBI が共同議長）、SRMA、その他の利害関係者と連携して、重要インフラ組織、SLTT、その他のランサムウェアの高リスク対象に対して、影響の可能性、発生時の影響の規模や期間を低減するために、トレーニング、サイバーセキュリティサービス、技術アセスメント、事前攻撃計画、インシデント対応などのリソースを提供する。

NCS リファレンス

ランサムウェアが主要な重要インフラ・サービスに与える影響を考慮し、米国は 4 つの取り組みに沿って、脅威に対抗するために国力のあらゆる要素を用いる...（3）ランサムウェア攻撃に耐える重要インフラのレジリエンスを強化する...。

合同ランサムウェア・タスクフォース（JRTF）は...ランサムウェアに対する防御を強化する民間部門と SLTT の取り組みを支援する。**担当機関** CISA

貢献した事業体 FBI、SRMA、USSS、NSC

完了時期： 25 年度第 1 四半期

イニシアチブ番号： 2.5.5

★★★★★★

イニシアチブのタイトル：仮想資産サービスプロバイダに対するグローバルなマネーロンダリング/テロ資金供与対策（AML/CFT）標準を採用し、実施するための他国の取り組みを支援する。

イニシアチブの内容

財務省は、司法省、国務省、その他の省庁間参加者を含む政府関係者を主導し、二国間および財務省主導の金融活動作業部会（FATF）への代表団を通じて国際パートナーと協力し、ランサムウェアによる資金洗浄を可能にするプロバイダの機能停止を含め、仮想資産サービス・プロバイダに対するマネーロンダリング防止・テロ資金供与対策（AML／CFT）基準および監督の世界的な採用・実施を加速させる。 米国は、2024 年初頭から半ばにかけて出版が予定されている資料を含め、勧告 15 関連の出版物のドラフト作成と貢献を継続する。 これには、能力の低い国に対する技術支援の提供や、他の FATF 加盟国に同様の支援を提供するよう促すことも含まれる。

NCS リファレンス

…米国は、国際的な AML/CFT 標準の実施を世界的に支援し、暗号通貨の違法行為への利用を緩和する**：**財務省

貢献した事業体司法省、国務省、USSS、NSC

完了時期： 24 年度第 4 四半期

イニシアチブ番号：2.5.6

イニシアチブのタイトル：ランサムウェア犯罪者のセーフヘイブンを阻害するための国際的関与計画の実施

イニシアチブの内容

国務省は、ランサムウェア合同タスクフォース（FBI と CISA が共同議長）と連携し、ランサムウェア犯罪者のセーフヘイブンを阻害するための国際関与計画を実施するため、司法省をはじめとする米国の省庁間および国際的なパートナーや利害関係者と引き続き協力する。

NCS リファレンス

ランサムウェアが主要な重要インフラ・サービスに与える影響を考慮し、米国は以下の 4 つの方針で脅威に対抗するため、国力のあらゆる要素を駆使する：国務省

貢献した事業体 DHS、司法省、財務省、CISA、FBI、NSA、ODNI、NSC

完了時期： 24 年度第 4 四半期

イニシアチブ番号：2.5.7

イニシアチブのタイトル：共同作戦を通じてランサムウェア犯罪を阻止する

★★★★★★

イニシアチブの内容

連邦捜査局は、ランサムウェア・タスクフォース（FBI と CISA が共同議長を務める）と連携し、連邦、国際、民間セクターのパートナーと協力して、ランサムウェアのエコシステムに対する共同破壊作戦を実施し、民間セクターに脅威勧告を発信していく。

NCS リファレンス

(1)ランサムウェアのエコシステムを破壊するために国際協力を活用する、(2)ランサムウェア犯罪を捜査し、ランサムウェアのインフラと脅威行為者を破壊するために法執行機関やその他の当局を利用する、(3)身代金支払いを洗浄するための仮想通貨の悪用に対処する。

合同ランサムウェア・タスクフォース（JRTF）は、ランサムウェアの活動を混乱させるために、既存の省庁間の取り組みを調整し、対立を解消し、同期させる。**責任機関** FBI

貢献した事業体 DOJ、CISA、NSA、USSS

完了時期：25 年度第 1 四半期

第三の柱：セキュリティとレジリエンスを推進するために市場力を形成する

戦略目標 3.1：データの管理者に責任を持たせる

イニシアティブ番号：3.1.1

イニシアチブのタイトル：国家プライバシー研究戦略の更新

イニシアチブの内容

米国科学技術政策局(OSTP)は、国家科学と協力する。

プライバシーを保護する情報システムや標準の研究開発、大規模なデータ分析など、情報処理から生じるプライバシーの悪影響を防ぐための研究投資に優先順位をつける戦略を策定するために、NSF（NSF)、NIST、その他のプライバシー研究開発（R&D）省庁間ワーキンググループのパートナーが参加する。

NCS リファレンス

個人データの防御は、デジタルの未来において消費者のプライバシーを保護するための基本的な側面である。データ主導のテクノロジーは経済を変革し、消費者に利便性を提供している。**担当省庁** OSTP

協力事業体：NSF、**NIST**

完了時期：25 年度第 1 四半期

★★★★★★

戦略目標 3.2：安全な IoT デバイスの開発を推進する

イニシアティブ番号：*3.2.1*

イニシアチブのタイトル：*2020* 年モノのインターネット（*IoT*）サイバーセキュリティ改善法による連邦調達規則（*FAR*）要件の実施

イニシアティブ番号：*3.2.2*

イニシアチブのタイトル：米国政府の *IoT* セキュリティ・ラベリング・プログラムを開始する。

イニシアティブ番号：3.2.3

イニシアチブのタイトル：将来のスマートグリッドを開発するためのサイバーセキュリティのラベリング規準を研究開発する。

イニシアチブの内容

米国エネルギー省は、国立研究所および業界パートナーと協力して、将来のクリーンでスマートな送電網に不可欠なスマートメーターと電力インバーターのサイバーセキュリティラベルの規準を研究・開発する。

NCS リファレンス

…政府は引き続き、IoT セキュリティ・ラベルの開発を推進する。**責任機関** DOE

貢献した事業体 NIST、NSC

完了時期：25 年度第 1 四半期

イニシアティブ番号：3.2.4

イニシアチブのタイトル：米国政府の IoT セキュリティ・ラベリング・プログラムを策定する。

イニシアチブの内容

連邦通信委員会（FCC）は、自主的な IoT サイバーセキュリティ表示プログラムを策定するための手続きを完了する予定であり、これにより、適合する機器や製品は "U.S. Cyber Trust Mark "の表示が認可されることになる。

NCS リファレンス

…政権は、IoT セキュリティ・ラベルの開発を進めていく。

★★★★★★

責任機関 FCC

完了時期： 24 年度第 3 四半期

★★★★★★

戦略目標 3.3：安全でないソフトウェア製品とサービスに対する責任の転換

イニシアティブ番号： *3.3.1*

イニシアチブのタイトル： 長期的かつ柔軟で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

イニシアティブ番号： 3.3.2

イニシアチブのタイトル： ソフトウェア部品表（SBOM）を推進し、未サポートソフトウェアのリスクを低減する

イニシアチブの内容

重要インフラにおけるサポート対象外ソフトウェアの使用状況に関するデータを収集するため、以下のような活動を行った。

サイバーセキュリティ・インフラセキュリティ庁は、SRMA を含む主要な利害関係者と協力して、SBOM の規模および実施におけるギャップを特定し、これを削減する。 CISA はまた、使用済み／サポート終了ソフトウェアの世界的にアクセス可能なデータベースの要件を検討し、SBOM に関する国際的なスタッフレベルの作業部会を招集する。

NCS リファレンス

.....行政は、SBOM のさらなる開発を促進し、広く使用されている、または重要インフラをサポートする、サポートされていないソフトウェアが示すリスクを特定し、軽減するためのプロセスを開発する。
責任機関 CISA

完了時期：25 年度第 2 四半期

イニシアティブ番号： 3.3.3

イニシアチブのタイトル： 脆弱性情報公開の連携

イニシアチブの内容

サイバーセキュリティ・インフラセキュリティ庁は、国際的な脆弱性コーディネータの実践共同体の創設を含め、あらゆる技術タイプやセクターの官民事業体の間で協調的な脆弱性開示が期待されるよう、国内および国際的な支援の構築に取り組む。 これには、国際的なコンピュータ緊急対応チームやその他のコミュニティ主導の組織を含む国際機構を支援し、協調的な脆弱性開示に関する世界的な認識と能力を構築することも含まれる。

★★★★★★

NCS リファレンス

安全なソフトウェア開発手法の採用をさらに奨励するため、行政は、すべての技術タイプおよび部門における協調的な脆弱性開示を奨励する：CISA

拠出事業体：州

完了時期：25 年度第 4 四半期

イニシアティブ番号：3.3.4

イニシアティブのタイトルオープンソースソフトウェアのセキュリティリスクを評価するアプローチの実現可能性をアセスメントする

イニシアチブの内容

国土安全保障省は、サイバーセキュリティとインフラ安全保障省を通じ、「サイバーセキュリティとインフラ安全保障の重要性」を強調した。

アセスメントは、オープンソースコミュニティと協議し、Log4j のサイバー安全性レ ビュー委員会のレビューで推奨されたように、オープンソースソフトウェアのセキュリティリスクを評 価するための様々なアプローチ（オープンソースソフトウェアセキュリティリスクアセスメントセンターを含む）の 実現可能性を調査する。 この作業は、CISA の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基礎とし、大統領令 14028 と NIST のソフトウェアセキュリティと品質に関するガイダンス、ツール、リソースを活用する。 また、このイニシアティブでは、重要なオープンソース依存関係、当該依存関係への貢献、オープンソースソフトウェアセキュリティへの投資、重要サービスのソフトウェア保守サポート計画についても検討する。

NCS リファレンス

市場は、脆弱性のある製品やサービスをデジタルエコシステムに導入する事業体に対して、不適切なコストを課している。セキュアな開発のためのベストプラクティスを無視し、セキュアでないデフォルト設定や既知の脆弱性を持つ製品を出荷し、出所不明のサードパーティ製ソフトウェアを統合するベンダーがあまりにも多い。

責任機関国土安全保障省

貢献した事業体 CISA、NIST

完了時期：**25** 年度第 4 四半期

イニシアティブ番号：3.3.5

★★★★★★

イニシアチブのタイトル：長期的、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

イニシアチブの内容

国家サイバー長官室は、ソフトウェア責任政策に関心を持つ利害関係者の関与を継続し、ソフトウェア製品とサービスの責任体制を確立するための提案をさらに発展させる。 一連のワークショップを通じて、ONCD は市民社会、企業、および学界からの提案に対するフィードバックを求める。 ONCD はまた、終了した法律シンポジウムに従って、ソフトウェア責任に関連する法的認可を検討する。

NCS リファレンス

安全なソフトウェア開発の標準を策定し始めるため、政府は、ソフトウェア製品やサービスを安全に開発・保守する企業の責任を回避する、適応可能なセーフハーバーの枠組みの開発を推進する。

責任機関 ONCD

完了時期：25 年度第 2 四半期

★★★★★★

戦略目標 3.4：連邦補助金やその他のインセンティブを利用して、安全保障を構築する。

イニシアティブ番号： *3.4.1*

イニシアチブのタイトル： 連邦補助金を活用してインフラのサイバーセキュリティを改善する。

イニシアティブ番号： *3.4.2*

イニシアチブのタイトル： サイバーセキュリティ研究に優先的に資金を提供する。

イニシアティブ番号： 3.4.3

イニシアチブのタイトル： サイバーセキュリティにおける社会的、行動的、経済的研究の研究、開発、実証を優先する。

イニシアチブの内容

2024 年度の助成金授与を通じて、全米科学財団は、サイバー経済学、人的要因、情報完全性、および関連テーマの研究を通じて、サイバーセキュリティが個人や社会に与える影響についての理解を深めることに投資する。

NCS リファレンス

連邦政府はまた、重要インフラのサイバーセキュリティとレジリエンスを強化することを目的としたサイバーセキュリティ研究・開発・実証（RD&D）プログラムへの資金提供を優先する。

責任機関 NSF **完了日：** FY24 4Q

★★★★★★

戦略目標 3.5：連邦調達の活用による説明責任の改善

イニシアティブ番号：3.5.1

イニシアチブのタイトル：大統領令 14028 に基づく連邦調達規則（FAR）の変更を実施する。

イニシアチブの内容

行政管理予算局は、連邦調達局を通じて行動する。

政策委員会は、連邦調達規制審議会と協力して、EO 14028 に基づいて要求される FAR の変更を提案する。ドラフト規則（サイバーセキュリティインシデント報告、サイバーセキュリティ契約要件の標準化、セキュアソフトウェア）の公表を通じて、変更が最終化される前にパブリックコメントが検討される。

NCS リファレンス

EO 14028「国家のサイバーセキュリティの改善」は、このアプローチをさらに拡大し、サイバーセキュリティに関する契約要件を強化し、連邦政府機関全体で標準化することを保証するものである。

責任機関 OMB

完了時期： 24 年度第 1 四半期

イニシアティブ番号：3.5.2

イニシアチブのタイトル：ベンダーのサイバーセキュリティを改善するために、偽請求法を活用する。

イニシアチブの内容

司法省は、レジリエンスの構築、脆弱性の開示の増加、責任ある業者の競争上の不利の軽減、影響を受けた連邦プログラムや連邦機関の損害回復を目的として、連邦契約や助成金におけるサイバーセキュリティ要件遵守の故意の不履行を特定、追求、抑止する取り組みを拡大する。

NCS リファレンス

Civil Cyber-Fraud Initiative（CCFI）は、偽請求法に基づく司法省の権限を利用して、サイバーセキュリティの義務を果たさない政府助成金提供者や請負業者に対する民事訴訟を追行する。 CCFI は、欠陥のあるサイバーセキュリティ製品やサービスを故意にプロバイダしたり、サイバーセキュリティの実践やプロトコルを故意に虚偽表示したり、サイバーインシデントや侵害を監視・報告する義務に故意に違反したりすることによって、米国の情報やシステムをリスクにさらした事業体や個人に責任を追及する。**責任機関**司法省

完了時期：25 年度第 4 四半期

★★★★★★

戦略目標 3.6：連邦サイバー保険のバックアップを探る

イニシアティブ番号：*3.6.1*

イニシアチブのタイトル：壊滅的なサイバー事象に対する連邦保険の必要性をアセスメントする。

第 4 の柱：レジリエンスある未来への投資

戦略目標 4.1：インターネットの技術的基盤を確保する

イニシアティブ番号：*4.1.1*

イニシアチブのタイトル：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主導する

イニシアティブ番号：*4.1.2*

イニシアチブのタイトル：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促進する。

イニシアティブ番号：*4.1.3*

イニシアチブのタイトル：インターネットの基盤となるインフラ機能と技術の開発、標準化、採用を加速する。

イニシアティブ番号：4.1.4

イニシアチブのタイトル：インターネットの基盤となるインフラ機能と技術の開発と標準化を加速し、その採用を支援する。

イニシアチブの内容

国立標準技術研究所は、省庁間、産業界、学界、その他の機構と協力し、国際標準の開発、商業化、採用を推進することにより、ボーダー・ゲートウェイ・プロトコル（BGP）とインターネット・プロトコル・バージョン 6（IPv6）のセキュリティ・ギャップに対処する。

NCS リファレンス

インターネットは私たちの未来にとって重要であるが、過去の基本的な構造を保持している……私たちは、ボーダーゲートウェイのような、最も緊急で蔓延する懸念を軽減するための措置を講じなければならない。

プロトコルの脆弱性、暗号化されていないドメインネームシステムへのリクエスト、遅々として進まない

★★★★★★

IPv6... 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、セキュアなインターネットを維持し、拡張するには、標準開発プロセスに持続的に関与し、当社の価値を浸透させ、技術標準がより安全でレジリエンスに優れた技術を生み出すようにする必要がある。**担当機関** NIST

完了時期： 24 年度第 4 四半期

イニシアティブ番号：4.1.5

イニシアチブのタイトル：安全なインターネット・ルーティングを推進するため、主要な利害関係者と協力する。

イニシアチブの内容

国家サイバー長官室は、主要な利害関係者及び適切な連邦政府事業体と連携して、安全なインターネットルーティング技術及びテクノロジーの採用を拡大するためのロードマップを策定する：(1) セキュリティ上の課題を特定し、(2) インターネットルーティングおよび BGP セキュリティ上の懸念に対処するためのアプローチおよびオプションを検討し、(3) ベストプラクティスの開発を特定し、情報を提供し、(4) 必要な研究開発を特定し、(5) 採用の障壁および代替の低減アプローチを特定する。

NCS リファレンス

インターネットは我々の将来にとって重要であるが、過去の基本的な構造を保持している。オープン、フリー、グローバル、相互運用性、信頼性、安全なインターネットを維持し、拡張するには、標準開発プロセスに持続的に関与し、私たちの価値観を浸透させ、技術標準がより安全でレジリエンシーに優れた技術を生み出すようにする必要がある。

責任機関 ONCD

協力事業体：DOJ、CISA、FCC、NIST、NSA、NTIA、OSTP

完了時期： 24 年度第 3 四半期

イニシアティブ番号：4.1.6

イニシアチブのタイトル：安全なインターネット・ルーティング技術とテクノロジー導入のためのロードマップを実施する。

イニシアチブの内容

国家サイバー長官室は、主要な利害関係者及び適切な連邦事業体と連携して、NCSIP イニシアチブ 4.1.5 の下で策定されたロードマップで特定された定義された測定基準及びマイルストーンに沿って、国

★★★★★★

境ゲートウェイプロトコル資源公開鍵基盤経路起点認可（RPKI ROA）のような安全なインターネットルーティング技術及び技術の連邦政府及び民間部門の採用を促進する。

NCS リファレンス

私たちは、ボーダーゲートウェイプロトコルの脆弱性、暗号化されていないドメインネームシステムへのリクエスト、IPv6 の普及の遅れなど、蔓延する懸念のうち最も緊急性の高いものを軽減するための措置を講じなければならない。 システミック・リスクを軽減するためのこのような「クリーンアップ」の取り組みには、これらのセキュリティ課題のうち最も差し迫ったものを特定し、効果的なセキュリティ対策をさらに開発し、このインフラの上に構築されたプラットフォームやサービスを中断させることなくリスク・エクスポージャーを軽減するために、官民が緊密に協力することが必要である。 連邦政府は、インターネット・エコシステムのセキュリティを改善するソリューションを開発し採用を促進するために利害関係者と提携し、採用が遅れている理由を理解し対処するための研究を支援する。

責任機関 ONCD

協力事業体： DOJ、ODNI、CISA、NIST、NSA、NTIA、FCC、OMB

完了時期： 25 年度第 3 四半期

イニシアティブ番号： 4.1.7

イニシアチブのタイトル： サイバー空間の構成要素全体にわたって、安全で測定可能なソフトウェア・ソリューションを推進する。

イニシアチブの内容

国家サイバー長官室は、官民の専門家を招集し、プログラミング言語、ハードウェア・アーキテクチャ、形式手法を含むサイバー空間の構成要素を保護することによって、大規模に脆弱性のクラスを排除する可能性のあるサイバーセキュリティ・アプローチを特定する。

NCS リファレンス

システミック・リスクを軽減するための「クリーンアップ」の取り組みには、このようなセキュリティ上の課題のうち最も差し迫ったものを特定し、効果的なセキュリティ対策をさらに開発し、このようなインフラの上に構築されたプラットフォームやサービスを中断させることなくリスクのエクスポージャーを軽減するために、官民が緊密に協力することが必要である。

責任機関 ONCD

貢献した事業体 CISA、NSA

完了時期： 24 年度第 4 四半期

★★★★★★

イニシアティブ番号：4.1.8

イニシアチブのタイトル：より安全なオープンソースソフトウェアのエコシステムを促進する

イニシアチブの内容

国家サイバーディレクター室は、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）を通じて、引き続き連邦政府全体のオープンソースソフトウェアセキュリティを主導・推進し、OSS コミュニティと協力して OSS エコシステムを強化する。ONCD が議長を務める OS3I ワーキンググループを通じて、OS3I メンバーは OSS コミュニティを招集し、メモリー安全プログラミング言語への転換を進め、安全な OSS エコシステムへの投資を促進する。

NCS リファレンス

連邦政府は、関係者と連携して、インターネット・エコシステムのセキュリティを向上させるソリューショ ンの開発と普及を推進するとともに、普及が遅れている理由を理解し、それに対処するための研 究を支援する。**責任機関** ONCD

協力事業体：DoD、CISA、NSF、OMB

完了時期：25 年度第 1 四半期

★★★★★★

戦略目標 4.2：サイバーセキュリティのための連邦研究開発を再活性化する。

イニシアティブ番号：*4.2.1*

イニシアチブのタイトル：メモリー安全プログラミング言語の成熟度、採用、安全性を加速する

★★★★★★

戦略目標 4.3：量子化後の未来に備える

イニシアティブ番号：4.3.1

イニシアチブのタイトル：国家安全保障覚書-10 の実施

イニシアチブの内容

行政管理予算局および国家安全保障システム担当国家管理者は、ONCD と連携して、国家安全保障覚書-10 の実施と、脆弱性のある公共ネットワークとシステムの量子耐性暗号ベースの環境への移行を優先し、まず連邦情報システムと NSS に重点を置く。 OMB は NIST と協力し、将来の未知のリスクに直面した際に暗号の俊敏性を提供するための補完的な緩和戦略を開発する。

NCS リファレンス

連邦政府は、脆弱性のある公共ネットワークおよびシステムを量子耐性暗号ベースの環境へ優先的に移行し、将来の未知のリスクに直面した際に暗号の俊敏性を提供するための補完的な低減戦略を策定する。

責任機関 OMB

貢献した事業体 NSA、ONCD

完了時期：25 年度第 1 四半期

イニシアティブ番号：4.3.2

イニシアチブのタイトル：国家安全保障システム（NSS）に NSM-10 を導入する

イニシアチブの内容

NSS の耐量子暗号への移行を実施する。

NCS リファレンス

連邦政府は、脆弱性のある公共ネットワークやシステムを量子耐性暗号ベースの環境に優先的に移行させ、将来の未知のリスクに直面しても暗号の俊敏性を提供できるよう、補完的な低減戦略を開発する。

責任機関 NSA

貢献した事業体国防総省、ODNI

完了時期：25 年度第 3 四半期

イニシアティブ番号：4.3.3

イニシアチブのタイトル：ポスト量子暗号アルゴリズムの標準化と移行支援

★★★★★★

イニシアチブの内容

国立標準技術研究所は、1 つ以上の耐量子公開鍵暗号アルゴリズムを募集、評価、標準化するプロセスを最終化する。 新しい公開鍵暗号標準は、世界中で利用可能であり、量子コンピュータの出現後を含め、予見可能な将来にわたって政府の機密情報を保護することができる、1 つ以上の追加的な未分類の一般公開されたデジタル署名、公開鍵暗号化、鍵確立アルゴリズムを規定する。

NCS リファレンス

量子コンピューティングの推進と進歩と、デジタルシステムにもたらされる脅威とのバランスをとるため、NSM10「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」は、米国の暗号システムを相互運用可能な量子耐性暗号に適時に移行するためのプロセスを確立する。

責任機関 NIST

完了時期：25 年度第 1 四半期

★★★★★★

戦略目標 4.4：クリーンエネルギーの未来を確保する

イニシアティブ番号：*4.4.1*

イニシアチブのタイトル：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。

イニシアティブ番号：*4.4.2*

イニシアチブのタイトル：デジタル・エコシステムが米国政府の脱炭素化目標を確実にサポートし、実現するための計画を策定する。

イニシアティブ番号：4.4.3

イニシアチブのタイトル：サイバーインフォームド・エンジニアリングの原則を用いた、エンジニアと技術者のためのトレーニング、ツール、サポートを構築し、改良する。

イニシアチブの内容

エネルギー省は利害関係者と協力し、国家サイバー情報工学戦略に基づき、エンジニアと技術者が安全でレジリエンスに優れた運用技術と制御システムを設計、構築、運用できるようにするための訓練、ツール、支援を進める。

NCS リファレンス

..... 行政は、この戦略的機会を捉え、これらの接続機器が広く配備された後にセキュリティ管理の継ぎ接ぎを開発するのではなく、議会が指示した国家サイバーインフォームド・エンジニアリング（CIE）戦略の実施を通じて、サイバーセキュリティを積極的に構築する。**責任機関** DOE

貢献した事業体 NIST

完了時期：25 年度第 4 四半期

イニシアティブ番号：4.4.4

イニシアチブのタイトル：米国政府の脱炭素化目標を支援・実現するデジタル・エコシステムを推進する計画を実施する。

イニシアチブの内容

国家サイバー長官室は、国内気候政策室（CPO）、エネルギー省、省庁間パートナーと協力し、クリーンエネルギー移行を支援するために必要な斬新な技術や力学をデジタルエコシステムに取り入れる準備を確

★★★★★★

実にするための計画に関連した 1 年目の活動を実施する。 この計画は、サイバーセキュリティのベストプラクティスを、バッテリー、インバーター、電気自動車などのクリーンエネルギー移行を推進する基盤技術に統合するための政府全体の活動を調整するものである。

NCS リファレンス

米国が新たなエネルギー・インフラに生成的な投資を行うにあたり、政権はこの戦略的機会を捉え、これらの接続機器が広く普及した後にセキュリティ管理のパッチワークを開発するのではなく、議会が指示した国家サイバーインフォームド・エンジニアリング戦略の実施を通じて、サイバーセキュリティを積極的に構築する。 ガバナンスは、電気自動車充電器、ゼロ・エミッション給油インフラ、ゼロ・エミッション輸送バス・スクールバスの安全で相互運用可能なネットワークを展開するため、連邦政府、産業界、SLTT の利害関係者の作業を調整している。

責任機関 ONCD

貢献した事業体：DOE、CPO、NEC、OSTP

完了時期：25 年度第 2 四半期

イニシアティブ番号：4.4.5

イニシアチブのタイトル：エネルギー部門の利害関係者と連携し、配電および分散型エネルギー資源（DER）のサイバーセキュリティ原則の策定と採用を推進する。

イニシアチブの内容

エネルギー省は、配電および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するため、適宜、産業界、州、連邦規制当局、その他の機関と協力する。

NCS リファレンス

DOE はまた、産業界、州、連邦規制当局、議会、および他の機関と連携して、配電および 分散型エネルギー資源のサイバーセキュリティを引き続き推進する。

担当省庁 DOE

完了時期：25 年度第 1 四半期

★★★★★★

戦略目標 4.5：デジタル・アイデンティティ・ｴｺシステムの開発を支援する

イニシアティブ番号：4.5.1

イニシアチブのタイトル：官民協働により、デジタル ID エコシステムにおける革新を支援する研究と指針を推進する。

イニシアチブの内容

国立標準技術研究所は、官民の協力を通じてデジタル ID エコシステムの革新を継続的に支 援するための研究と指針を進める。 このイニシアチブには、デジタル ID ガイドラインの発行、顔認識および分析技 術の評価、属性妥当性確認サービスに関する検討事項の発行などが含まれる。

NCS リファレンス

連邦政府は、セキュリティ、アクセシビリティおよび相互運用性、金融および社会的包摂、 消費者のプライバシー、および経済成長を促進する、強力で検証可能なデジタル ID ソリューションへの投資を奨励し、可能にする。CHIPS および科学法（CHIPS and Science Act）で認可された NIST 主導のデジタル ID 研究プログラムに基づいて、これらの取り組みには、デジタ ル・クレデンシャルのセキュリティ強化、属性およびクレデンシャルの妥当性確認サービスの提供、基礎研究の 実施、一貫した使用と相互運用性をサポートする標準、ガイドライン、および統治プロセスの更新、 透明性と測定を促進するデジタル ID プラットフォームの開発などが含まれる。 **責任機関** NIST

貢献した事業体 DHS、GSA

完了時期：25 年度第 2 四半期

★★★★★★

戦略目標 4.6：サイバー人材強化のための国家戦略を策定する。

イニシアティブ番号：*4.6.1*

イニシアチブのタイトル：国家サイバー人材・教育戦略を発表し、その実施を追跡する。

イニシアティブ番号：4.6.2

イニシアチブのタイトル：国家サイバー人材・教育戦略の実施と報告

イニシアチブの内容

国家サイバー長官室は、引き続き国家サイバー人材・教育戦略を実施し、実施に向けた進捗状況を報告する。 ONCD は、連邦政府のパートナー、州、地方、部族、および準州政府、教育機関、学界、図書館、コミュニティベースの組織、および企業と協力して、サイバー労働力と教育のエコシステムを拡大するためのプレイブックを開発し、サイバー職業へのオンランプを広げ、サイバー労働者に対する増大する需要に対応する国の能力を高める。

NCS リファレンス

この課題に対処するため、ONCD は国家サイバー人材・教育戦略の策定を主導し、実施を監督する。

責任機関 ONCD

完了時期：25 年度第 4 四半期

イニシアティブ番号：4.6.3

イニシアチブのタイトル：スキルベースの雇用慣行を促進する

イニシアチブの内容

国家サイバー局長室は、人事管理局（OPM）および OMB と協力し、連邦取得契約、職務記述書、および学歴要件がない職種の求人公告から、大卒などの最低学歴要件を削除するために連邦機関と協力する。

OPM は、連邦省庁が使用するスキルベースの採用アセスメントを開発する。ONCD は、サイバー職のスキルベースの雇用慣行を推進するよう民間部門に働きかける。

NCS リファレンス

この課題に対処するため、ONCD は国家サイバー人材・教育戦略の策定を主導し、実施を監督する。

責任機関 ONCD

貢献した事業体 OPM、OMB

★★★★★★

完了時期：25 年度第 1 四半期

第 5 の柱共通の目標を追求するための国際的パートナーシップの構築

戦略目標 5.1：デジタル・エコシステムに対する脅威に対抗するための連携を構築する

イニシアティブ番号：5.1.1

イニシアチブのタイトル：地域サイバー協力・調整のための省庁間チームを創設する。

イニシアチブの内容

国務省は、サイバー空間とデジタル政策に関連する職員の知識と技能を向上させ、国や地域の省庁間サイバー・チームを設立・強化し、相手国との調整を促進するために活用できるようにする。

NCS リファレンス

…米国と国際的なカウンターパートは、サイバー脅威情報の共有、サイバーセキュリティの模範事例の交換、セクター固有の専門知識の比較、セキュアバイデザインの原則の推進、政策とインシデント対応活動の調整によって、サイバーセキュリティの共通の利益を促進することができる。

責任機関国

貢献した事業体商務省、DHS、司法省、CISA、FBI、USAID

完了時期：25 年度第 1 四半期

イニシアティブ番号：*5.1.2*

イニシアチブのタイトル：国際サイバー空間・デジタル政策戦略の発表

イニシアティブ番号：5.1.3

イニシアチブのタイトル：同盟国やパートナーとの連邦法執行機関の協力体制を強化する。

イニシアチブの内容

FBI は、サイバー犯罪者や国家的敵対者、それに関連する資金洗浄者（マネーロンダリングなど）に対する国際的な法執行妨害キャンペーンの量と速度を高める取り組みにおいて、同盟国やパートナーとの連携を確保するためのメカニズムを開発または拡大する。

★★★★★★

NCS リファレンス

(1)米国と国際的なカウンターパートは、サイバー脅威情報を共有し...政策とインシデント対応活動を調整することにより、共通のサイバーセキュリティ上の利益を促進することができる。(2)米国は...国際的な犯罪者やその他の悪意のあるサイバー行為者を共同で破壊し、国際的な同盟国やパートナーの能力を構築し、...破壊的、破壊的、不安定化する悪意のあるサイバー活動に従事する者を処罰する。**担当機関** FBI

貢献した事業体 DHS、DoD、司法省、国務省、財務省

完了時期： 25 年度第 4 四半期

イニシアティブ番号： 5.1.4

イニシアチブのタイトル： 地域サイバーハブ研究

イニシアチブの内容

国家サイバー局長室は、欧州サイバー犯罪センターに関する調査を委託し、将来のサイバーハブの開発に役立てる。

NCS リファレンス

このモデルを拡大するため、他の地域のパートナーとともに効果的なハブを構築する努力を支援する。

責任機関 ONCD

貢献した事業体司法省、国務省、FBI

完了時期： 24 年度第 4 四半期

イニシアティブ番号： 5.1.5

イニシアチブのタイトル： 国際サイバー空間・デジタル政策戦略の実施

イニシアチブの内容

国務省は、国際サイバー空間・デジタル政策戦略を実施し、その進捗状況を報告する。 短期から中期的なイニシアティブを通じて、有意義な接続性を促進し、サイバー空間における責任ある国家の行動を形成し、権利を尊重する国際協力を強化する。 パートナーとの積極的な関与を通じて、サイバー空間と重要インフラに対する脅威に対抗し、安全なデジタル・エコシステムを構築・維持し、国際パートナーのデジタルおよびサイバー能力を強化し、デジタルおよびサイバー支援を迅速かつ効率的に提供するためのツールを開発する。

★★★★★★

NCS リファレンス

米国は、国際社会と協力するために、各国のサイバーセキュリティ関係者による新たな協力モデルの拡大に取り組む。　我々は、連合を拡大し、多国籍犯罪者やその他の悪意あるサイバー行為者を協力して崩壊させ、国際的な同盟国やパートナーの能力を構築し、サイバー空間における国家の行動に対する既存の国際法の適用法を強化し、平時における国家の責任ある行動に関する世界的に認められた自主的な規範を支持し、破壊的、破壊的、不安定化させる悪意あるサイバー活動に従事する者を処罰する。

責任機関州の**完了時期：**25 年度第 2 四半期

★★★★★★

戦略目標 5.2：国際パートナーの能力強化

イニシアティブ番号：*5.2.1*

イニシアチブのタイトル：国際パートナーのサイバー能力を強化する

イニシアティブ番号：5.2.2

イニシアチブのタイトル：法執行機関の業務協力を通じて国際パートナーのサイバー能力を拡大する

イニシアチブの内容

連邦法執行機関は、国際的な同業者やそれに近い法執行機関のパートナーとの作戦上の協力を強化し、それによって、米国の法執行機関の目標と一致するスピードと規模で、最も重要なサイバー脅威を破壊するパートナーの能力を向上させる。

NCS リファレンス

我々は、同盟国やパートナーが、作戦上の協力を通じて法執行能力と有効性を構築できるようにしなければならない。

責任機関司法省

貢献した事業体州、FBI、HSI、USSS

完了時期： 26 年度第 4 四半期

★★★★★★

戦略目標 5.3：同盟国やパートナーを支援する米国の能力を拡大する。

イニシアティブ番号：*5.3.1*

イニシアチブのタイトル：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。

★★★★★★

戦略目標 5.4：責任ある国家行動の世界的規範を強化するための連合を構築する

イニシアティブ番号：5.4.1

イニシアティブ・タイトル：無責任な国家が約束を守らなかった場合、その責任を問う

イニシアチブの内容

国務省は、オープンエンド・ワーキング・グループを通じて、サイバー空間における国家の責任ある行動の枠組みを前進させ、悪意ある行為者に責任を負わせる意思のある国家連合を強化する。

NCS リファレンス

米国は、新たな積極的外交の中核として、無責任な国家が約束を守らなかった場合には、その責任を追及する。　敵対国を効果的に拘束し、武力紛争の閾値以下の悪意ある活動に対抗するため、われわれは同盟国やパートナーと協力し、非難の声明と意味のある結果を課すことをセットにしていく。

責任機関国

貢献した事業体国防総省、司法省、FBI

完了時期：25 年度第 4 四半期

★★★★★★

戦略目標 5.5：情報・コミュニケーション・運用技術製品およびサービスのグローバル・サプライチェーンの確保

イニシアティブ番号：*5.5.1*

イニシアチブのタイトル：安全で信頼できる情報通信技術（*ICT*）ネットワークとサービスの開発を促進する。

イニシアティブ番号：*5.5.2*

イニシアチブのタイトル：信頼できる情報通信（*ICT*）ベンダーの、より多様でレジリエンスに富んだサプライチェーンを促進する。

イニシアティブ番号：*5.5.3*

イニシアチブのタイトル：公共無線サプライチェーンイノベーション基金（*PWSCIF*）の運営を開始する。

イニシアティブ番号：5.5.4

イニシアチブのタイトル：サイバーセキュリティ・サプライチェーンリスクマネジメント(CSCRM)の重要なプラクティスを、重要インフラ部門全体および部門内で普及・浸透させる。

イニシアチブの内容

ソフトウェア・サプライチェーン・セキュリティ・ナショナル・サイバーセキュリティ・センター・オブ・エクセレンス・プロジェクトを通じて、国内外における C-SCRM のベスト・プラクティスを普及・増幅させ、海外サプライヤーの信頼を高める。

NCS リファレンス

信頼できないサプライヤーからの重要な外国製品やサービスへの依存は、私たちのデジタル・エコシステムに複数のシステミック・リスクをもたらす。 このリスクを低減するには、グローバル・サプライチェーンのバランスを見直し、透明性、安全性、レジリエンシー、信頼性を高めるために、国内外の官民が長期的かつ戦略的に協力する必要がある。**責任機関** NIST

完了時期：25 年度第 2 四半期

イニシアティブ番号：5.5.5

★★★★★★

イニシアチブのタイトル：半導体の安全な開発・製造のためのガイダンスを策定する。

イニシアチブの内容

国立標準技術研究所は、省庁間および半導体業界と協力して、半導体の開発・製造の安全確保に関するガイダンスを作成する。 このガイダンスには、半導体の安全確保に関する勧告と、半導体の安全性を確保するための技術的な指針が含まれる。

サイバーセキュリティ・フレームワーク・プロファイルは、半導体製造業界向けにカスタマイズされている。

NCS リファレンス

...このモデルを他の重要技術にも拡大するには、グローバル・サプライ・チェーンのバランスを調整し、より安全でレジリエンスに富み、信頼できるものにするために、国内外の官民が長期的かつ戦略的に協力する必要がある。**責任機関** NIST

貢献した事業体 DoD、NSA、ONCD

完了時期：25 年度第 3 四半期

★★★★★★

イニシアティブ番号：5.5.6

イニシアチブのタイトル：オープンで相互運用可能な無線ネットワークの開発を支援するため、PWSCIF補助金の授与を継続する。

イニシアチブの内容

国家電気通信情報局(NTIA)は、10 年間で 150 万ドルの PWSCIF の管理を通じて、オープンで相互運用可能な標準ベースのネットワークの開発と普及を引き続き促進する。 これらの重要な投資を通じて、NTIA はサプライチェーンのレジリエンスを強化し、技術革新を促進し、競争を促進する。

NCS リファレンス

…と国家電気通信情報局（NTIA）は、公共無線サプライチェーンイノベーション基金を通じて、オープンで相互運用可能な標準ベースのネットワークの開発と採用を促進するための活動を行っている。

責任機関 NTIA

貢献した事業体 DHS、DoD、ODNI、NIST、FCC

完了時期： 24 年度第 3 四半期

実施全体の取り組み

実施 6.1：効果のアセスメント

イニシアティブ番号：6.1.1

イニシアチブのタイトル：国家サイバーセキュリティ戦略の実施に関する進捗と効果を報告する。

イニシアチブの内容

国家サイバー局長室は、この戦略、関連政策、フォローアップ行動の有効性を評価し、大統領、国家安全保障問題担当大統領補佐官、議会に最初の年次報告書を提出する。

NCS リファレンス

ONCD は、NSC スタッフ、OMB、各省庁と連携し、本戦略の有効性を評価し、本戦略、関連政策、および目標達成のための事後措置の有効性について、大統領、国家安全保障問題担当大統領補佐官、および議会に毎年報告する。

責任機関 ONCD

貢献した事業体 OMB

完了時期： 24 年度第 3 四半期

イニシアティブ番号：*6.1.2*

イニシアチブのタイトル：国家サイバーセキュリティ戦略の実施に教訓を生かす。

イニシアティブ番号：*6.1.3*

イニシアチブのタイトル：予算ガイダンスを国家サイバーセキュリティ戦略の実施と整合させる。

★★★★★★

使用される略語

1Q	First Quarter	第 1 四半期
2Q	Second Quarter	第 2 四半期
3Q	Third Quarter	第 3 四半期
4Q	Fourth Quarter	第 4 四半期
AML	Anti-Money Laundering	反マネーロンダリング
BGP	Border Gateway Protocol	ボーダーゲートウェイプロトコル
CCFI	Civil Cyber-Fraud Initiative	サイバー詐欺民事イニシアチブ
CFT	Countering the Financing of Terrorism	テロ資金対策
CHIPS	Creating Helpful Incentives to Produce Semiconductors	半導体製造に役立つインセンティブを生み出す
CIA	Central Intelligence Agency	アメリカ中央情報局
CIE	Cyber-Informed Engineering	サイバー・インフォームド・エンジニアリング
CIRCIA	Cyber Incident Reporting for Critical Infrastructure Act	重要インフラのためのサイバーインシデント報告法
CISA	Cybersecurity and Infrastructure Security Agency	サイバーセキュリティ・インフラセキュリティ庁
CPO	White House Climate Policy Office	ホワイトハウス気候政策室
C-SCRM	Cybersecurity Supply Chain Risk Management	サイバーセキュリティ サプライチェーンリスクマネジメント
CSF	Cybersecurity Framework	サイバーセキュリティ・フレームワーク
CSRB	Cyber Safety Review Board	サイバーセーフティ審査会
CTIIC	Cyber Threat Intelligence Integration Center	サイバー脅威インテリジェンス統合センター
DER	Distributed Energy Resources	分散型エネルギー資源
DHS	Department of Homeland Security	国土安全保障省
DoD	Department of Defense	国防総省
DOE	Department of Energy	エネルギー省
DOJ	Department of Justice	司法省
Education	Department of Education	教育省
EO	Executive Order	大統領令
EPA	Environmental Protection Agency	環境保護庁
ETAC	Energy Threat and Analysis Center	エネルギー脅威分析センター
FAR	Federal Acquisition Regulation	連邦調達規則
FATF	Financial Action Task Force	金融活動作業部会
FEMA	Federal Emergency Management Agency	連邦緊急事態管理庁

★★★★★★

FBI	Federal Bureau of Investigation	連邦捜査局
FCC	Federal Communications Commission	連邦通信委員会
FCEB	Federal Civilian Executive Branch	連邦文民行政機関
FY	Fiscal Year	会計年度
GSA	General Services Administration	一般調達局
HHS	Department of Health and Human Services HSI	保健福祉省 HSI
HIS	Homeland Security Investigations	国土安全保障省
IaaS	Infrastructure-as-a-Service	インフラストラクチャー・アズ・ア・サービス
ICT	Information and Communication Technology	情報コミュニケーション・テクノロジー
IoT	Internet of Things	モノのインターネット
IPv6	Internet Protocol version 6	インターネット・プロトコル・バージョン 6
ISAC	Information Sharing and Analysis Center	情報共有分析センター
ISAO	Information Sharing and Analysis Organization	情報共有・分析組織
JRTF	Joint Ransomware Task Force (Co-chaired by CISA and FBI; membership includes DHS, DoD, DOJ, ODNI, State, Treasury, CIA, NSA and USSS)	合同ランサムウェア・タスクフォース（CISA と FBI が共同議長を務め、DHS、DoD、DOJ、ODNI、State、Treasury、CIA、NSA、USSS がメンバーに含まれる）
NCIJTF	National Cyber Investigative Joint Task Force (Led by the FBI; membership includes CIA, CISA, NSA, USSS)	国家サイバー捜査官合同タスクフォース（FBI が主導、メンバーには CIA、CISA、NSA、USSS が含まれる）
NCIRP	National Cyber Incident Response Plan	国家サイバーインシデント対応計画
NCS	National Cybersecurity Strategy	国家サイバーセキュリティ戦略
NCSIP	National Cybersecurity Strategy Implementation Plan	国家サイバーセキュリティ戦略実施計画
NEC	National Economic Council	国家経済会議
NIST	National Institute of Standards and Technology	国立標準技術研究所
NPRM	Notice of Proposed Rulemaking	規則制定提案公告
NSA	National Security Agency	国家安全保障局
NSC	National Security Council	国家安全保障会議
NSF	National Science Foundation	全米科学財団
NSM	National Security Memorandum	国家安全保障に関する覚書
NSS	National Security Systems	ナショナル・セキュリティ・システムズ
NTIA	National Telecommunications and Information Administration	国家電気通信情報局
ODNI	Office of the Director for National Intelligence	国家情報長官室

★★★★★★

OMB	Office of Management and Budget	行政管理予算局
ONCD	Office of the National Cyber Director	国家サイバー局長室
OPM	Office of Personnel Management	人事管理局
OS3I	Open-Source Software Security Initiative	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
OSTP	Office of Science and Technology Policy	米国科学技術政策局
PPD	Presidential Policy Directive	大統領政策指令
PWSCIF	Public Wireless Supply Chain Innovation Fund	パブリック・ワイヤレス・サプライチェーン・イノベーション・ファンド
R&D	Research and Development	研究開発
RD&D	Research, development, and demonstration	研究、開発、実証
RPKI ROA	Remote Private Key Identification Route Origin Authentication	リモート秘密鍵識別 ルート・オリジン認証
RUS	Rural Utilities Service	ルーラル・ユーティリティー・サービス
SBOM	Software Bill of Materials	ソフトウェア部品表
SLTT	State, local, Tribal, and territorial	州、地方、部族、準州
SRMA	Sector Risk Management Agency*	セクター・リスクマネジメント・エージェンシー*（リスクマネジメント機関
State	Department of State	国務省
TMF	Technology Modernization Fund	技術近代化基金
Treasury	Department of the Treasury	財務省
USAID	United States Agency for International Development	米国国際開発庁
USDA	U.S. Department of Agriculture	米国農務省
USSS	United States Secret Service	米国シークレットサービス

*各重要インフラ部門には、重要インフラのセキュリティとレジリエンスに関する国家安全保障覚書（NSM-22）で特定された SRMA が指定されており、以下にリストアップされている：

化学部門 - 国土安全保障省

商業施設部門 - 国土安全保障省

コミュニケーション部門 - 国土安全保障省

重要製造部門 - 国土安全保障省

★★★★★★

ダム部門 - 国土安全保障省

防衛産業基盤セクター - 国防総省

緊急サービス部門 - 国土安全保障省

エネルギー部門 - エネルギー省

金融サービス部門 - 財務省

食品・農業セクター - 農務省および保健福祉省

政府サービス・施設部門 - 国土安全保障省および一般調達局

医療・公衆衛生部門 - 保健福祉省

情報技術部門 - 国土安全保障省

原子炉・材料・廃棄物部門 - 国土安全保障省

運輸システム部門 - 国土安全保障省・運輸省

上下水道部門 - 環境保護庁