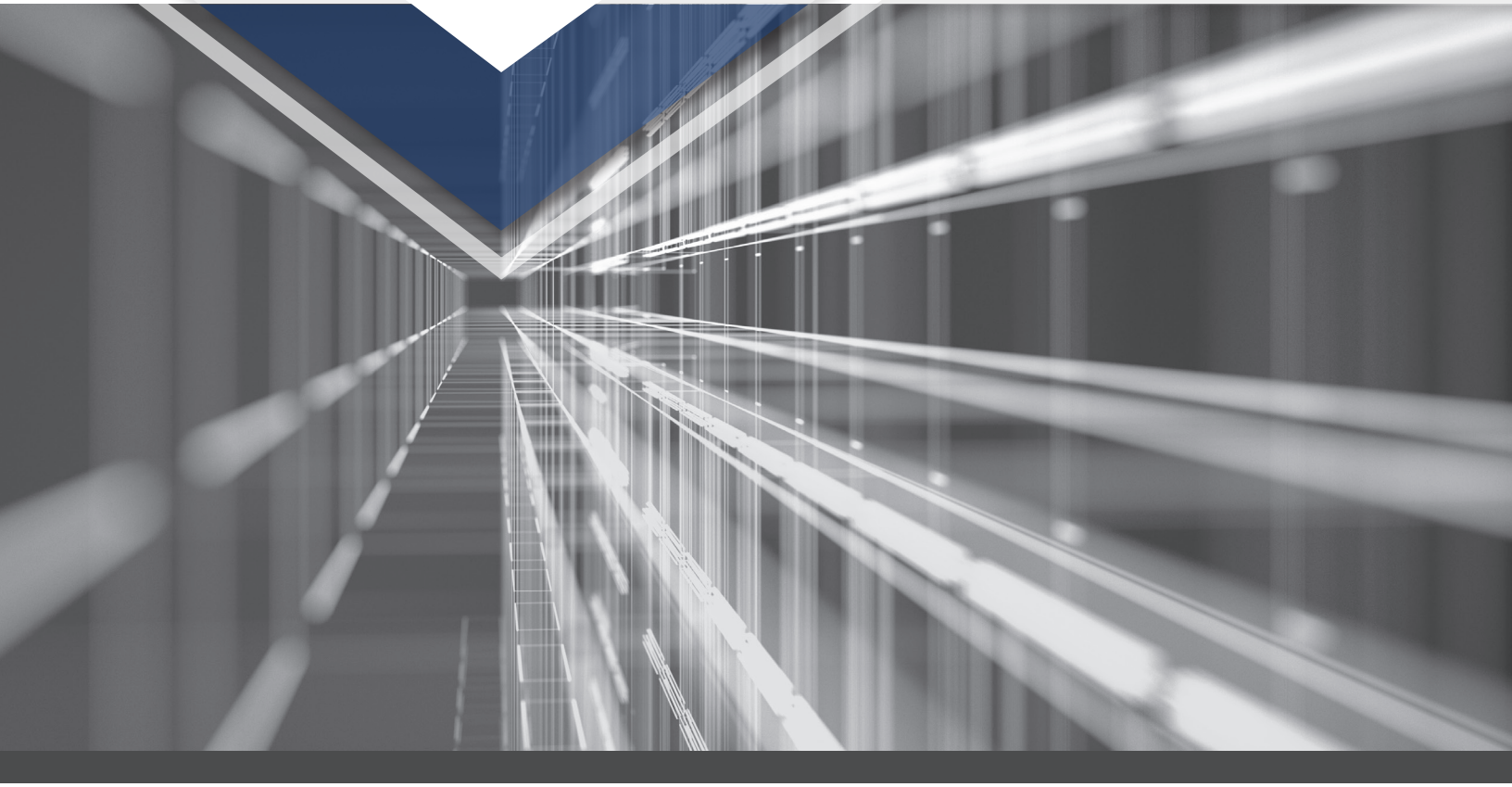
CPG

Cross-Sector Cybersecurity Performance Goals

分野横断的なサイバーセキュリティパフォーマンス目標

2023年3月更新版



PERFORMANCE GOALS

パフォーマンス目標

Version: 1.0.1

CISA長官からのメッセージ

米国のサイバー防衛機関として、CISAの最も重要な役割の一つは、米国民が毎日頼りにしている重要インフラに対するサイバーリスクを低減するという共通の目標に向けて前進するため、大小を問わず組織が直面する課題を理解することである。過去数年間にわたって、わが国がランサムウェアから国家によるスパイ活動まで、これまでになかったサイバー脅威に直面してきた中で、我々は大規模の多国籍企業から州政府や地方自治体、あらゆる規模の重要インフラ組織に至るまで、さまざまな組織が共通して繰り返す言葉を耳にしてきた。「最もインパクトが大きいセキュリティ成果に向けて投資を集中させるにはどうすればよいか?」

中小規模の病院や公共サービス提供会社からは、限られた予算、人員、専門知識で、どうやって進歩を遂げることができるのかを尋ねる声を耳にする。成熟したサイバープログラムを持つ組織からは、高度な敵からの攻撃を防ぎ、サプライチェーン内の未熟な組織のリスクを管理し、国家に対するより広範なリスクを軽減するために、さらに何ができるのかを尋ねる声を耳にする。グローバルな制御・運用技術および産業用制御システム（OT/ICS）コミュニティからは、従来のITセキュリティと同様に見られ、認識され、ますます接続が進む電力網や病院、水道施設、及びその他の重要インフラを防御するという重要な役割が支援されるよう強く求める声を耳にする。

NISTサイバーセキュリティフレームワークのような情報源からの包括的なガイダンスがあっても、多くの組織は、最も重要なサイバーセキュリティのプラクティスを特定し優先順位付けするための支援や、リスクを低減するための適切なリソースを確保するための説得力のある議論のサポートを受けることで恩恵を受けることが明らかになった。最終的には、優先順位付けされた投資は、米国民の安全・健康・生活に対する深刻なリスクに有意義に対処するのに役立つだろう。

分野横断的なサイバーセキュリティパフォーマンス目標（CPGs）は、明確に定義され、実装が容易で、最も一般的でインパクトが大きいいくつかのサイバーリスクに対処することを目的とした、取り組みやすく一般的な一連のITおよびOTサイバーセキュリティ保護策を提供することで、このニーズに対処することを目指している。CPGsは、上級ビジネス幹部を含む技術者以外の読者にわかりやすく、比較的容易に伝えることができるように書かれ、設計されている。

CPGsは、官民、国内外のさまざまな分野のエキスパートからの広範な情報を得て、サイバーセキュリティのコミュニティ全体から集められた最良の考え方のいくつかを反映している。すべてのことと同様に、常に進化し続けるテクノロジーと脅威の状況に基づいてこれらの目標を定期的に更新できるよう、CISAは継続的なフィードバックを期待している。最終的には、CPGsが我が国の重要インフラ分野全体のサイバーセキュリティを改善するための強力な基盤となるだけでなく、米国民の信頼に値するセキュリティ成果のベースラインとして機能することを期待している。

JEN
Jen Easterly
サイバーセキュリティ・インフラストラクチャセキュリティ庁（CISA）長官
2022年10月

背景と状況

今後の課題

CISAは、政府、民間企業および国際的なパートナーとともに、米国の重要インフラ（CI）全体のサイバーセキュリティの状態と脅威の状況の本質について独自の洞察を得るために、日々活動している。すべての重要インフラ分野およびそれぞれの分野リスク管理機関（SRMAs）とのパートナーシップ、米国内外の政府パートナーからの知見、および独自のサイバーアセスメント、追跡、インシデント対応活動を活用し、CISAは、基本的なサイバーセキュリティのベストプラクティスが十分に適用されていないというパターンを、重要インフラの至るところで定期的に観測している。本文書の作成過程で情報を提供した特定分野の専門家や重要インフラ事業者とも、同様の見解を共有した。

これらのギャップに対する我々の懸念は、単なる仮説ではない。米国は、病院から学区に至る重要な機能に影響するランサムウェア攻撃や、政府機関や重要インフラを標的とした高度な国家規模の攻撃キャンペーンなど、これらのギャップの実際のインパクトを目の当たりにしてきた。これらの侵入は、全体として米国の国家安全保障や経済安全保障、および米国民の健康と安全を危険にさらす。

過去1年間、CISAは何百ものパートナーと協力し、何千ものコメントを受け取り、サイバーインシデントをアセスメント・保護・対応するための取り組みから得られた長年のデータを分析した。これにより、我が国を深刻なリスクにさらす主要な課題を特定した。

1. **多くの組織は、基本的なセキュリティ保護策を導入していない。**多要素認証（MFA）、強力なパスワード管理、バックアップの維持といった基本的な保護策が欠如しているため、重要インフラは繰り返し有害なサイバー侵入にさらされている。

2. **中小企業は取り残されている。**リソースが限られている組織、またはサイバーセキュリティプログラムが成熟していない組織は、合理的なサイバーセキュリティ対策を導入するためにどこから始めればいいかを決めるという課題に直面することがよくある。NISTサイバーセキュリティフレームワークのような既存のリソースは非常に重要であるが、小規模な組織は、サイバーセキュリティ態勢に最も大きなインパクトを与えるためにどこに投資すべきかを特定する難しさ、及びサイバーセキュリティ保護策を効果的に実装する方法に関する具体的なガイダンスを特定する難しさに直面している。

3. **重要インフラ分野に横断的な、一貫性のある標準とサイバー成熟度が欠如している。**重要インフラの各分野内および各分野間で、サイバーセキュリティのケイパビリティ、投資およびベースラインとなるプラクティスに著しい不一致がある。この相違は、機能的なインパクトや連鎖的なインパクトを引き起こすために敵対者によって悪用される可能性のあるギャップにつながる。

4. **OTサイバーセキュリティは見落とされがちで、リソース不足のままであることが多い。**サイバーセキュリティ業界は、依然としてビジネスITシステムに重点を置いており、信頼性と可用性を最適化するよう設計され、固有のセキュリティ機能を持たないことが多いOTの重大なリスクを軽視していることが多い。これにより、より多くのOT機器がネットワークに接続されるようになると、重要インフラ事業者は深刻なリスクにさらされる。それでもなお、多くの重要インフラ事業者には、特にサイバーセキュリティがまだ主にITの問題とみなされている場合には、適切なOTサイバーセキュリティプログラムが不足している。OTサイバーセキュリティプログラムを持っている事業者でも、基本的なOTのサイバー保護策が欠如していることが多く、その環境に適したOT固有のガイダンスを見つけることができない。

目次

この課題に立ち向かう: 国家安全保障覚書 5

2021年7月、バイデン大統領は国家安全保障覚書 (NSM) -5「重要インフラ制御システムのサイバーセキュリティの向上」に署名した。この覚書では、CISAに対し、国立標準技術研究所（NIST）および省庁間コミュニティと連携して、すべての重要インフラ分野で一貫性のあるサイバーセキュリティのベースライン目標を策定することを要求した。この文書には、分野横断的なサイバーセキュリティパフォーマンス目標 (CPGs) の最新版が含まれている。さらに、2022年後半、CISAは分野リスク管理機関 （Sector Risk Management Agencies : SRMAs) と協力して、この基盤に基づいて分野固有の目標を策定する作業を開始した。

CPGsとは?

簡単に言えば、CPGsは、重要インフラ業務と米国民の両方に対するリスクを有意義に低減することを目的とした、ITおよびOTサイバーセキュリティプラクティスの優先順位付けされたサブセットである。これらの目標は、すべての重要インフラ分野に適用可能であり、CISAとその政府および産業界のパートナーによって観測された最も一般的でインパクトの大きい脅威と敵対者の戦術・技術・手順（TTPs）から情報を得ているため、大規模から小規模まですべての重要インフラ事業体が実装することが望ましい、共通の一連の保護策となっている。

CPGsの主な特徴

- サイバーセキュリティプラクティスの優先順位付けされたサブセット
- ITおよびOT向け
- リスク低減のために優先順位付けされている
- CISAとその政府および産業界のパートナーが観測した脅威から情報を得ている
- すべての重要インフラ分野に適用可能
- 重要インフラ業務と米国民の両方に対するリスクを有意義に低減することを意図している

CPGsは、包括的なサイバーセキュリティプログラムを反映したものではなく、むしろ組織が実装することが望ましい最低限のプラクティスであり、重要インフラ事業体、特に中小組織が強力なサイバーセキュリティ態勢への道を歩み始めるのを支援することを目的としている。そのため、CPGsは、サイバーリスクを低減するために組織が実装することが望ましいサイバーセキュリティ保護策について、上限ではなく下限となることを意図している。重要なことだが、CPGsは以下のようなものでは**ない**。

- **包括的である:** CPGsは、あらゆる組織を保護するために必要なすべてのサイバーセキュリティプラクティスを特定するものではなく、また、すべての潜在的なリスクから国家と経済の安全保障および公衆衛生や安全を完全に保護するものでもない。これらは、すべての分野に広く適用可能な既知のリスク低減価値を持つサイバーセキュリティプラクティスの最低限のベースラインを示すものであり、該当する場合は各分野固有の制約、脅威、成熟度をより深く掘り下げた分野固有の目標がその後に続く。
- **リスク管理または完全なサイバーセキュリティプログラム:** CPGsは、NISTサイバーセキュリティフレームワーク（NIST CSF）などの他のフレームワークで明確に示されている、リスク管理やリスクの優先順位付けといったより広範なアプローチをカバーしていない。
- **CISAによって義務付けられている:** CPGsは、NIST CSFのようなより広範なフレームワークと連携して、最も重要な成果に向けてセキュリティ投資の優先順位付けを可能にするために、組織が自主的に採用することを意図している。
- **成熟度モデル:** CPGsのプラクティスはすべての重要インフラ組織に適用され、「成熟度」のカテゴリに階層化されていない。（ただし、CPGワークシートには、「インパクト」、「コスト」、および「複雑さ」などの基準が含まれており、組織内部で投資の優先順位を決めるのに役立つ）。

CPGは定期的に更新され、少なくとも6～12カ月ごとの改訂サイクルを目標とする。CISAは新たなCPGsに対するフィードバックやアイデアを受け取るための ディスカッションページ を開設している。
同サイトへのリンクは、https://www.cisa.gov/cpgs からも利用可能である。

CPG 選定基準

前述の通り、CPGsはサイバーセキュリティプラクティスのサブセットであり、複数の基準を用いて、産業界、政府および専門家の徹底的な協議のプロセスを経て選定された。

1. 一般的に観測される分野横断的な脅威やサイバー脅威行為者のTTPsの、リスクまたはインパクトを低減する実証値
2. 明確で、実行可能で、容易に定義できる。
3. 合理的でわかりやすく、中小規模の事業者でも正常に実装するためのコストが高くない。

この基準を満たすCPGの一例としては、「組織のインターネットに接続されたシステムに、悪用された既知の脆弱性（KEVs）が存在しないことを確実にする」といったものが挙げられる。このCPGは定義可能で達成可能であり、既知の脅威、すなわち国家主体の敵対者がこれらの弱点を積極的に利用することによるリスクを直接的に低減する。逆に、「ゼロトラスト（ZT）を実装する」などのプラクティスは、曖昧で定義が不十分であり、測定も困難であるため適切なCPGとはいえず、小規模組織にとっては過度な負担となる可能性がある。

CPG モデル

本文書のCPGsは、読者が目標そのものだけでなく、意図された成果、目標が対処するリスクまたはTTPs、「良い」とはどのようなものか、およびその他の重要な情報を理解できるように、視覚モデルで表示されている。

各目標は、以下の要素で構成されている。

モデルの構成要素	構成要素の説明
成果	各CPGが実現しようと努力する最終的なセキュリティ成果。
対処されるTTP/リスク	(a) MITRE ATT&CK TTPs の主要なセット、または (b) 目標が実装された場合に、その可能性やインパクトが低下する組織的なリスクのセット。
セキュリティプラクティス	成果を達成し、TTPまたはリスクのインパクトを低減するために組織が実装することが望ましい緩和策。
範囲（スコープ）	組織がセキュリティプラクティスを適用することが望ましい資産のセットまたはサブセット。
推奨される行動	CISAのステークホルダーとの協働プロセスから得られた情報に基づき、組織がパフォーマンス目標の達成に向けて前進するのを支援するためのアプローチ例。これらの行動は、新たな脅威や防御策が特定されるたびに、定期的に更新される。
NIST CSF リファレンス	セキュリティプラクティスに最も密接に関連するCSFのサブカテゴリ。

CPGsはNIST CSF および他の標準とどう違うのか?

サイバーセキュリティに関するガイドラインやフレームワークは、特に米国政府から多くのものが存在する。例えば、NIST CSFは、最も広く採用され、よく知られているサイバーセキュリティフレームワークの1つであり続けている。CISAおよび米国政府全体は、持続可能でリスク情報サイバーセキュリティプログラムの開発と維持を可能にするために、すべての組織がNIST CSFを採用することを支持している。ステークホルダーのフィードバックに基づき、組織は、NIST CSFまたはその他のフレームワークや標準に基づく広範なサイバーセキュリティプログラムの一部としてCPGsを活用することができる。

1. **クイックスタートガイド。** CPGsは、サイバーセキュリティの経験、リソースが不足している可能性のある組織、または体制が整っていない可能性のある組織が、基本的なサイバーセキュリティ慣行を迅速に特定して実装するのに役立つ。CPGsの適用後、またはCPGsの適用と並行して、組織はNIST CSFを活用し続けて、全体的なリスク管理プログラムを構築したり、追加のNIST管理策を実装したりすることができる。

2. **優先順位付けと資金調達。** CPGsには、サイバーセキュリティプログラムが小規模または成熟度が低い組織が、どの保護策を実装するかを優先順位付けし、（技術者ではない）経営幹部に対してこれらの保護策の重要性、相対的な影響およびコストを伝えるのに役立つワークシートが含まれている（詳細は後述）。

3. **NIST CSF マッピング。** CPGsにおけるすべてのセキュリティプラクティスは、NIST CSFの対応するサブカテゴリに整合し、マッピングされる。CPGsは、NIST CSFの各サブカテゴリに完全に対応していないことに注意されたい。各セキュリティプラクティスについて、CSFサブカテゴリの特定は、CPGとNIST CSFとの関係を示している。NIST CSFをすでに採用および実装済みの組織は、関連するCPGsを実装するための追加作業を行う必要はない。

CPGsの使い方

CPG パッケージの内容

CPGsでは、3つの文書が提供されている。

1. CPG リスト（本文書）
2. CPG ワークシート（添付PDF）詳細は以下を参照。
3. CPGsの全ての生データ、他のフレームワークへのマッピングなどを含む CPG Full Data Matrix (添付 Excel 文書)

CPG ワークシート

CPGsのリストに加え、資産所有者および運用者のために、（1）どのCPGsを実装するかをレビューし優先順位を付ける、（2）現在および将来のCPG実装状況を追跡する、（3）技術系以外の幹部などの他のステークホルダーにCPGsの優先度、トレードオフ、および状況を明確に伝えるための使いやすいワークシートが用意されている。

ワークシートには、各目標の実装にかかるコスト、複雑さ、インパクトの一般的な見積もりが含まれている。これらの見積もりは、ベースラインのサイバーセキュリティのケイパビリティ（能力）における既知のギャップに対処するための投資戦略に関する情報を提供する助けとして使用されることを意図している。

CPG ワークシートの使用

1. 最初の自己評価を行う。組織は、既存のセキュリティプログラムとセキュリティ管理策をレビューして、どのCPGsがすでに実装されているかを判断することが望ましい。組織は、NIST CSFまたはISA 62443などの既存のガイダンスまたは規制へのCPGsベースの順守をすでに実装しているかもしれないが、すべてのCPGsをこれらの共通フレームワークの対応する管理策にマッピングする。

2. ギャップを特定し、優先順位をつける。組織は、CPG ワークシートに含まれているコスト、複雑さ、およびインパクトなどの要素に基づいて、CPG 実装のギャップをレビューし、投資対象の分野の優先順位付けを行う。

3. 投資し、実行する。組織は、前のステップで特定された優先順位付けされたギャップの実装を開始することができる。組織によっては、ワークシートのような資料が、サイバーセキュリティに焦点を当てたプロジェクトへの資金提供を要請するために幹部と連携する際に役立つ場合もある。

4. 定期的に12ヶ月後の進捗状況を確認する。サイバーセキュリティプラクティスの改善に向けた進捗を追跡するために、組織は12ヶ月後にワークシートを調べて、自組織のリーダーとサードパーティの両方に対して進歩状況を把握することが望ましい。

CPGsの変更点

2023年3月更新版: CPGs は初版からどう変わったか?

2022年10月に最初のCPG レポートを公開した後、CISAは複数のセクターから、NIST CSFへのマッピングをより合理的に行うよう求めるフィードバックを受け取った。これを受けてCISA は、NIST CSFの機能（識別（Identify）、防御（Protect）、検知（Detect）、対応（Respond）、復旧（Recover））に合わせてCPGs を再編成した。なお、いくつかの目標は複数の機能に対応しており、所与のCPGの実装が、参照されているNIST CSF サブカテゴリの完全な達成に必ずしもつながらないことに注意されたい。

- この2023年3月更新版 version 1.0.1では、NIST CSFの機能と密接に連携するよう、CPGsの順序と番号が変更されている。それに伴い、付属文書（チェックリストおよびマトリックス）も調整されている。初版に慣れ親しんでいるユーザーのために、元の番号からのマッピングがマトリックスに反映されている。
- さらに、MFA目標は、フィッシングに強いMFAに関する最新の CISA ガイダンス および実装の優先順位付けに関する考慮事項を反映するために更新されている。
- CISA は、組織の復旧計画を支援するために、GitHub のフィードバックに基づく目標も追加した。
- 最後に、上記のマイナーな内容変更を反映するために、用語集に若干の修正を加え、また、更新版および初版に貢献したステークホルダーに感謝するために、謝辞のセクションに修正を加えた。

識別 (IDENTIFY)

1.A 資産インベントリ

ID.AM-1, ID.AM-2, ID.AM-4, DE.CM-1, DE.CM-7

成果	推奨される行動
既知の資産、未知の資産（シャドー）、管理されていない資産をより適切に識別し、新たな脆弱性をより迅速に検出し対応する。	OTを含む、IPアドレス（IPv6を含む）を持つすべての組織資産の定期的に更新されるインベントリを維持する。このインベントリは、ITとOTの両方について、月1回以上の頻度で定期的に更新する。

対処されるTTPまたはリスク	範囲
• ハードウェアの追加 (T1200) • 外部公開されたアプリケーションへの攻撃 (T0819, ICS T0819) • インターネットに接続可能なデバイス (ICS T0883)	IT および OT 資産

1.B 組織的なサイバーセキュリティのリーダーシップ

ID.GV-1, ID.GV-2

成果	推奨される行動
一人のリーダーが、組織内のサイバーセキュリティに責任を持ち、説明責任を負う。	サイバーセキュリティ活動の計画、リソース確保、 および実行に責任を持ち、説明責任を負う役割／役職／職名を識別する。この役割は、上級レベルでのサイバーセキュリティ業務の管理、予算リソースの要求と確保、または将来の位置づけを知らせるための戦略の策定の主導、などの活動を引き受けても良い。

対処されるTTPまたはリスク	範囲
サイバーセキュリティの説明責任、投資、または有効性の欠如。	該当なし

1.C OT サイバーセキュリティのリーダーショップ

ID.GV-1, ID.GV-2

成果	推奨される行動
一人のリーダーが、OT資産を持つ組織内のOT固有のサイバーセキュリティに責任を持ち、説明責任を負う。	OT固有のサイバーセキュリティ活動の計画、リソース確保、および実行に責任を持ち、説明責任を負う役割／役職／職名を識別する。組織によっては、 1.B で識別されたのと同じ役職である場合がある。

対処されるTTPまたはリスク	範囲
OTサイバーセキュリティプログラムの説明責任、投資、または有効性の欠如。	該当なし

1.D ITとOTのサイバーセキュリティ関係の改善

ID.GV-2, PR.AT-5

成果	推奨される行動
OTサイバーセキュリティを改善し、より迅速かつ効果的にOTサイバーインシデントに対応する。	組織は、ITとOTのセキュリティ担当者間の協力関係を強化することに重点を置いた、（インシデント対応中に食事を提供するなどの）業務上のイベントではない「親睦会」を、少なくとも年に1回以上主催する。

対処されるTTPまたはリスク	範囲
ITとOTのサイバーセキュリティの不十分な協力関係や相互理解の欠如が、しばしばOTサイバーセキュリティのリスクを増大させる結果になることがある。	すべての ITおよびOTセキュリティ担当者

1.E 既知の脆弱性の緩和

ID.RA-1, PR.IP-12, DE.CM-8, RS.MI-3, ID.RA-6, RS.AN-5

成果

脅威行為者が既知の脆弱性を悪用して組織のネットワークを侵害する可能性を低減する。

対処されるTTPまたはリスク

- アクティブスキャン - 脆弱性スキャン (T1595.002)
- 外部公開されたアプリケーションへの攻撃 (T1190, ICS T0819)
- リモートサービスの悪用 (T1210, ICS T0866)
- サプライチェーンの侵害 (T1195, ICS T0862)
- 外部リモートサービス (T1133, ICS T0822)

範囲

インターネットに面した資産

推奨される行動

インターネットに面したシステムの既知の脆弱性（CISAの Known Exploited Vulnerabilities Catalog に記載されている）はすべて、リスク情報に基づいた期間内に、より重要な資産から優先してパッチを適用するか、または緩和する。

OT: パッチ適用が不可能、または可用性や安全性が実質的に侵害される可能性がある資産については、代替の管理策（例えば、セグメンテーション、監視）を適用し、記録する。十分な管理策によって、その資産は公衆インターネットからアクセスできなくなるか、脅威行為者がこれらの資産の脆弱性を悪用する能力が低下する。

1.F サイバーセキュリティ管理策の有効性の第三者検証

ID.RA-1, ID.RA-3, ID.RA-4, ID.RA-5, ID.RA-6

成果

適切な防御が不足しているTTPを識別し、組織のサイバー防御に対する 信頼を確立する。

対処されるTTPまたはリスク

サイバー防御のギャップ、または既存の防御策のセキュリティに対する誤った意識のリスクを低減する。

範囲

ITおよびOT資産とネットワーク

推奨される行動

（ITおよび／またはOT）サイバーセキュリティの確かな専門知識を持つ第三者が、組織のサイバーセキュリティ防御の有効性と適用範囲を定期的に検証する。この検証には、ペネトレーションテスト、バグ報奨金制度、インシデントのシミュレーション、又は机上演習が含まれても良く、抜き打ちテストと 事前通知ありのテストの両方を含めることが望ましい。

演習では、潜在的な敵対者が外部からネットワークに侵入する能力およびインパクト、および（例えば、侵害されることを想定して） ネットワーク内の敵対者が、制御・運用技術や産業用制御システムを含む重要なシステムにインパクトを与える可能性を示すために横方向に移動する能力の両方を考慮する。

以前のテストで発見されたインパクトの大きいものは、タイムリーに緩和されており、将来のテストで再観測されることはない。

1.G サプライチェーン・インシデントの報告

ID.SC-1, ID.SC-3

成果

組織は、ベンダやサービスプロバイダ全体の既知のインシデントまたは侵害について、より迅速に把握し、対応する。

対処されるTTPまたはリスク

サプライチェーンの侵害 (T1195, ICS T0862)

範囲

ITおよびOT資産やサービスを提供するサプライヤ

推奨される行動

サービス内容合意書（SLA）などの調達文書や契約書に、ベンダおよび／またはサービスプロバイダが、組織が決定したリスク情報に基づいた時間枠内に、セキュリティインシデントを調達顧客に通知することを規定する。

1.H サプライチェーンの脆弱性開示

ID.SC-1, ID.SC-3

成果

組織は、ベンダやサービスプロバイダが提供する資産の脆弱性について、より迅速に把握し、対応する。

対処されるTTPまたはリスク

サプライチェーンの侵害 (T1195, ICS T0862)

範囲

ITおよびOT資産やサービスを提供するサプライヤ

推奨される行動

サービス内容合意書（SLA）などの調達文書や契約書に、ベンダおよび／またはサービスプロバイダが、組織が決定したリスク情報に基づいた時間枠内に、資産の脆弱性が確認されたことを調達顧客に通知することを規定する。

1.I

ベンダ/サプライヤのサイバーセキュリティ要件 ID.SC-3

成果

よりセキュアなサプライヤから、よりセキュアな製品およびサービスを購入することで、リスクを低減する。

対処されるTTPまたはリスク

サプライチェーンの侵害
(T1195, ICS T0862)

範囲

ITおよびOT資産やサービスを提供するサプライヤ

推奨される行動

組織の調達文書に、サイバーセキュリティの要件および質問を含め、ベンダ選定の際には、コストや機能がほぼ同等の2つの製品がある場合、よりセキュアな製品および／またはサプライヤが優先されるよう評価する。

防御 (PROTECT)

2.A– デフォルトパスワードの変更 PR.AC-1

成果	推奨される行動
脅威行為者がデフォルトパスワードを使用して初期アクセスを達成する、またはネットワーク内を横方向に移動したりすることを防止する。	内部ネットワークまたは外部ネットワークに接続する前に、あらゆる／すべてのハードウェア、ソフトウェア、およびファームウェアのデフォルトの製造業者のパスワードを変更することを要求する、組織全体で実施されるポリシーおよび／またはプロセス。これには、OT管理のWebページなどの、OTのためのIT資産が含まれる。 デフォルトのパスワードを変更できない場合（例えば、ハードコードされたパスワードを持つ制御システム）は、適切な追加のセキュリティ管理策を実装および文書化し、それらの機器でのネットワークトラフィックおよびログイン試行のログを監視する。 OT: 組織の既存のOTのデフォルトパスワードの変更には、より多くの作業が必要となるが、新規または将来の全ての機器のデフォルトの認証情報を変更するようなポリシーを持つことを推奨する。これにより、達成が容易になるだけでなく、敵対者のTTPが変更された場合の将来の潜在的なリスクも低減される。

対処されるTTPまたはリスク	範囲
• 有効なアカウント - デフォルトのアカウント (T1078.001) • 有効なアカウント (ICS T0859)	パスワードで保護されたIT資産および新たに取得したOT資産

2.B– 最小のパスワード強度 PR.AC-1

成果	推奨される行動
組織のパスワードは、脅威行為者が推測する、または解読することが困難である。	組織は、技術的に実現可能な場合、パスワードで保護されたすべてのIT資産およびすべてのOT資産に対して、最小のパスワード長が15文字* 、またはそれ以上であることを要求するという、システムによって強制されるポリシーを持つ。** 組織は、ユーザーが十分に長いパスワードを維持しやすくするために、パスフレーズとパスワードマネージャーの活用を検討することが望ましい。最小のパスワード長が技術的に実現不可能な場合は、追加の管理策が適用されて記録され、それらの資産へのすべてのログイン試行がログに記録される。十分な強度を持つ長さのパスワードをサポートできない資産は、アップグレードまたは交換が優先される。 この目標は、MFAの広範な実装およびブルートフォース（総当たり）攻撃から保護する機能（Webアプリケーションファイアウォール、サードパーティのコンテンツ配信ネットワークなど）が欠如している組織、またはパスワードなしの認証方式を採用できない組織にとって、特に重要である。 * 最新の攻撃ツールは、8文字のパスワードを素早く解読できる。長さは、複雑さや頻繁なパスワードローテーションよりも、パスワードの強度に影響を与える重要な要素である。また、長いパスワードは、ユーザーが作成して覚えるのも容易である。 ** 中央認証メカニズム（Active Directoryなど）を使用するOT資産に対処することが最も重要である。技術的に実現できない可能性がある低リスクのOT資産には、海上掘削装置、または風力タービンなどの遠隔地にある資産が含まれる。

対処されるTTPまたはリスク	範囲
• ブルートフォース（総当たり攻撃） - パスワード推測 (T1110.001) • ブルートフォース（総当たり攻撃） - パスワード解析 (T1110.002) • ブルートフォース（総当たり攻撃） - パスワードスプレー (T1110.003) • ブルートフォース（総当たり攻撃） - クレデンシャルスタッフィング (T1110.004)	パスワードで保護されたITおよびWindowsベースのOT資産

2.C– 一意の認証情報 PR.AC-1

成果	推奨される行動
攻撃者は、侵害された認証情報を再利用して、組織全体、特にITネットワークとOTネットワークの間で横方向に移動することができない。	組織は、ITおよびOTネットワーク上の同様のサービスおよび資産へのアクセスのために、一意で個別の認証情報を設定する。ユーザーは、アカウント、アプリケーション、サービスなどのパスワードを再利用しない（またはで、再利用できない）。サービスのアカウント／マシンのアカウントは、すべてのメンバーユーザーアカウントにはない一意のパスワードを持つ。

対処されるTTPまたはリスク	範囲
• 有効なアカウント (T1078, ICS T0859) • ブルートフォース（総当たり攻撃） - パスワード推測 (T1110.001)	ITおよびOT資産

2.D– 離職する従業員の認証情報の無効化 PR.AC-1, PR.IP-11

成果	推奨される行動
元従業員による組織のアカウントまたはリソースへの不正アクセスを防止する。	離職日までに離職するすべての従業員に適用される、以下が定義された強制的な管理プロセス。 (1)すべての物理的なバッジ、キーカード、トークンなどを無効化して確実に返却する。 (2)すべてのユーザーアカウントと組織のリソースへのアクセスを無効化する。

対処されるTTPまたはリスク	範囲
有効なアカウント (T1078, ICS T0859)	離職する／離職した従業員

2.E– ユーザーアカウントと特権アカウントの分離 PR.AC-4

成果	推奨される行動
一般的なユーザーアカウントが侵害された場合でも、脅威行為者が管理者アカウントまたは特権アカウントにアクセスするのを困難にする。	常に管理者権限またはスーパーユーザー権限を持つユーザーアカウントは存在しない。管理者は、管理者の役割に関連付けられていないすべての行動と活動 (例えば、ビジネスメール、Web閲覧) に対して、個別のユーザー アカウントを保持する。与えられた権限セットの継続的な必要性を検証するために、権限を定期的に再評価する。

対処されるTTPまたはリスク	範囲
有効なアカウント (T1078, ICS T0859)	安全かつ技術的に可能な状況にあるITおよびOT資産

2.F– ネットワークセグメンテーション PR.AC-5, PR.PT-4

成果	推奨される行動
敵対者がITネットワークを侵害した後、OTネットワークにアクセスする可能性を低減する。	特定のシステム機能に対して、（例えば、IPアドレスおよびポートによって）明示的に許可されていない限り、OTネットワークへのすべての接続はデフォルトで拒否する。ITネットワークとOTネットワーク間の必要な通信経路は、適切に設定されたファイアウォール、要塞ホスト、踏み台サーバー、または非武装地帯などの、仲介となるものを通過しなければならない。これは、厳密に監視され、ネットワークログを取得し、承認された資産からの接続のみ許可する。

対処されるTTPまたはリスク	範囲
• ネットワークサービスディスカバリ (T1046) • 信頼関係 (T1199) • ネットワーク接続一覧 (ICS T0840) • ネットワークスニッフィング (T1040, ICS T0842)	安全かつ技術的に可能な状況にあるITおよびOT資産

2.G– 失敗した（自動化された）ログイン試行の検出 PR.AC-7

成果	推奨される行動
自動化された認証情報ベースの攻撃から、組織を保護する。	失敗したログインはすべてログに記録し、組織のセキュリティチームまたは関連するロギングシステムに送信する。短時間に特定の回数連続してログインに失敗（例えば、2分間で5回失敗）すると、セキュリティチームに（例えば、アラートによって）通知する。このアラートはログに記録され、過去に遡った分析のために、関連するセキュリティシステムまたはチケットシステムに保存する。 IT資産については、システムで強制されるポリシーにより、疑わしいアカウントに対して今後のログインを阻止する。例えば、これは、ある程度の時間、または特権ユーザーによってアカウントが再有効化するまでの間である。この設定は、資産で利用可能な場合に有効となる。例えば、Windows　11では、10分間に10回の不正ログインがあった後、10分間アカウントを自動的にロックアウトすることができる。

対処されるTTPまたはリスク	範囲
• ブルートフォース（総当たり攻撃） - パスワード推測 (T1110.001) • ブルートフォース（総当たり攻撃） - パスワード解析 (T1110.002) • ブルートフォース（総当たり攻撃） - パスワードスプレー (T1110.003) • ブルートフォース（総当たり攻撃） - クレデンシャルスタッフィング (T1110.004)	安全かつ技術的に可能な状況にある、パスワードで保護されたITおよびOT資産

2.H フィッシングに強い多要素認証 (MFA) PR.AC-7, PR.AC-1

成果

認証情報が侵害された資産アカウントを保護するために、重要なセキュリティレイヤを追加する。

対処されるTTPまたはリスク

- ブルートフォース（総当たり攻撃）(T1110)
- リモートサービス - リモートデスクトッププロトコル (T1021.001)
- リモートサービス - SSH (T1021.004)
- 有効なアカウント (T1078, ICS T0859)
- 外部リモートサービス (ICS T0822)

範囲

安全かつ技術的に可能な状況にある、ワークステーションやHMIなどの、リモートアクセス可能なITおよびOT資産

推奨される行動

組織は、その資産に対して利用可能な最も強力な方法を使用して、資産にアクセスするためのMFAを実装する（範囲については以下を参照）。強度の高いものから並べたMFAの選択肢は、以下の通りである。

1. ハードウェアベースで、フィッシングに強いMFA（例えば、FIDO/WebAuthnまたは公開鍵暗号基盤（PKI）ベース-「リソース」のCISAガイダンス参照）。
2. ハードウェアベースのMFAが利用できない場合、モバイルアプリベースのソフトトークン（できれば番号照合によるプッシュ通知）またはFIDOパスキーなどの新しい技術が使用されているMFA。
3. 他の選択肢が不可能な場合のみ、ショートメッセージサービス（SMS）または音声によるMFA。

IT: すべてのITアカウントは、組織のリソースにアクセスするためにMFAを活用する。重要なITシステムの特権管理者アカウントなど、最もリスクの高いアカウントを優先する。

OT: OT環境では、ベンダ／保守アカウント、リモートアクセス可能なユーザーおよびエンジニアリングワークステーション、リモートアクセス可能なHMIなど、リモートアクセス可能なすべてのアカウントおよびシステムでMFAを有効にする。

2.I 基本的なサイバーセキュリティトレーニング PR.AT-1

成果

組織のユーザーは、よりセキュアな行動を学び、実行する。

対処されるTTPまたはリスク

ユーザーのトレーニング (M1017, ICS M0917)

範囲

すべての従業員および請負業者

推奨される行動

フィッシング、ビジネスメール詐欺（BEC）、基本的な操作のセキュリティ、パスワードのセキュリティなど、基本的なセキュリティの概念をカバーし、セキュリティとサイバー意識の社内文化を醸成するトレーニングを、すべての従業員と請負業者に対して、少なくとも年1回実施する。

新入社員は、入社後10日以内に最初のサイバーセキュリティトレーニングを受け、少なくとも年1回の定期的なトレーニングを受ける。

2.J OTサイバーセキュリティトレーニング PR.AT-2, PR.AT-3, PR.AT-5

成果

OT資産をセキュアにすることに責任を持つ社員は、OTに特化したサイバーセキュリティのトレーニングを受けている。

対処されるTTPまたはリスク

ユーザーのトレーニング (M1017, ICS M0917)

範囲

OTセキュリティに責任を持つすべての社員

推奨される行動

通常の業務の一環としてOTを維持またはセキュアにする社員は、基本的なサイバーセキュリティトレーニングに加え、少なくとも年1回、OT特有のサイバーセキュリティトレーニングを受ける。

2.K 強力でアジャイルな暗号化 PR.DS-2

成果

機密データの機密性およびEITおよびOTトラフィックの完全性を維持するために導入された効果的な暗号化。

対処されるTTPまたはリスク

- AiTM攻撃 (T1557)
- 自動収集 (T1119)
- ネットワークスニッフィング (T1040, ICS T0842)
- 無線の侵害 (ICS T0860)
- 無線のスニッフィング (ICS T0887)

範囲

（外部のエンティティと通信する）すべてのITトラフィックとリモートOT資産

推奨される行動

技術的に可能な場合、転送中のデータを保護するために、適切に設定された最新のSSL（Secure Socket Layer）/TLS（Transport Layer Security）を使用する。組織はまた、古い暗号または弱い暗号を特定し、十分に強力なアルゴリズムに更新し、ポスト量子暗号の影響を管理することを検討するよう計画することが望ましい。

OT: 遅延時間と可用性へのインパクトを最小限に抑えるため、通常、リモート／外部資産と接続しているOT通信に、可能な場合には暗号化を使用する。

2.L– 機密データをセキュアにする — PR.DS-1, PR.DS-5

成果

機密情報を不正アクセスから保護する。

対処されるTTPまたはリスク	範囲
• セキュアでない認証情報 (T1552) • Kerberos チケットの盗難または偽造 (T1558) • OS認証情報のダンプ (T1003) • 情報リポジトリからのデータ (ICS T0811) • 運用情報の盗難 (T0882)	すべてのパスワード、認証情報、秘密、およびその他の機密または管理された情報

推奨される行動

認証情報を含む機密データは、組織内のどこにも平文で保存されておらず、認証され認可されたユーザーのみがアクセスすることができる。認証情報は、認証情報／パスワードマネージャまたは金庫（vault）、またはその他の特権アカウント管理ソリューションなど、セキュアな方法で保管する。

2.M– 電子メールのセキュリティ — PR.DS-5, PR.AC-7

成果

スプーフィング、フィッシング、傍受など、一般的な電子メールベースの脅威からのリスクを低減する。

対処されるTTPまたはリスク	範囲
• フィッシング (T1566) • ビジネスメール詐欺（BEC）	すべての組織の電子メールインフラ

推奨される行動

すべての企業電子メールインフラにおいて、(1) STARTTLS が有効、(2) Sender Policy Framework (SPF) および DomainKeys Identified Mail (DKIM) が有効、および (3) Domain-based Message Authentication, Reporting, and Conformance (DMARC) が有効で「拒否」に設定されている。詳細な例および情報については、CISA's past guidance for federal agencies を参照。

2.N– マクロをデフォルトで無効にする — PR.IP-1, PR.IP-3

成果

脅威行為者のTTPとして一般的で非常に有効な、組み込みマクロや類似の実行コードによるリスクを低減する。

対処されるTTPまたはリスク	範囲
• フィッシング - 添付ファイルによるスピアフィッシング (T1566.001) • ユーザーによる実行 - 悪意のあるファイル (T1204.002)	IT資産

推奨される行動

マイクロソフトオフィスのマクロ、または同様の埋め込みコードを、すべてのデバイスでデフォルトで無効にするシステム強制のポリシー。特定の状況でマクロを有効にする必要がある場合、許可されたユーザーが特定の資産でマクロを有効にするよう要求するためのポリシーがある。

2.0– 機器の設定の文書化 — PR.IP-1

成果

組織に対するサイバー攻撃を、より効率的かつ効果的に管理、対応、回復し、サービスの継続性を維持する。

対処されるTTPまたはリスク	範囲
重要な機器およびサービス業務の機能を維持または回復する能力が、遅延、不十分、または不完全になる。	ITおよびOT資産

推奨される行動

組織は、より効果的な脆弱性管理および対応・復旧活動を促進するために、すべての重要なITおよびOT資産のベースラインおよび現在の構成の詳細を記述する正確な文書を維持する。定期的なレビューと更新を実施し、追跡する。

2.P– ネットワークトポロジーの文書化 PR.IP-1, ID.AM-3

成果

サイバー攻撃への対応をより効率的かつ効果的に行い、サービス継続性を維持する。

対処されるTTPまたはリスク	範囲
ネットワークトポロジーの不完全または不正確な理解が、効果的なインシデント対応と復旧を妨げる。	すべてのITおよびOTネットワーク

推奨される行動

組織は、すべてのITおよびOTネットワークにおいて、更新されたネットワークトポロジーおよび関連情報を詳述した正確な文書を維持する。定期的なレビューおよび更新を実施し、定期的に追跡することが望ましい。

2.Q– ハードウェアおよびソフトウェアの承認プロセス PR.IP-3

成果

展開したテクノロジー資産に対する可視性を高め、ユーザーが承認されていないハードウェア、ファームウェア、またはソフトウェアをインストールすることによ侵害の可能性を低減する。

対処されるTTPまたはリスク	範囲
• サプライチェーンの侵害 (T1195, ICS T0862) • ハードウェアの追加 (T1200) • ブラウザ拡張機能 (T1176) • 一過性のサイバー資産 (ICS T0864)	ITおよびOT資産

推奨される行動

新しいハードウェア、ファームウェア、またはソフトウェア／ソフトウェアのバージョンをインストールまたは展開する前に、承認を必要とする管理ポリシーまたは自動化プロセスを実装する。組織は、技術的に可能な場合、承認されたバージョンの仕様を含む、承認されたハードウェア、ファームウェア、およびソフトウェアのリスクの情報に基づいた許可リストを維持する。特にOT資産については、これらの行動は、定義された変更管理およびテスト活動と整合させることが望ましい。

2.R– システムのバックアップ PR.IP-4

成果

組織は、サービス提供または業務の損失時に、データ損失の可能性を低減し、期間を短縮する。

対処されるTTPまたはリスク	範囲
• データ破壊 (T1485, ICS T0809) • 影響を与えるためのデータ暗号化 (T1486) • ディスクの消去 (T1561) • システムリカバリの阻止 (T1490) • 制御不能 (ICS T0813) • 閲覧拒否/喪失 (ICS T0815, T0829) • 可用性の喪失 (T0826) • 制御の喪失/操作 (T0828, T0831)	事業運営に必要なITおよびOT資産

推奨される行動

業務に必要なすべてのシステムは、定期的な周期で（1年に1回以上）バックアップされる。

バックアップは、ソースシステムとは別に保存され、1年に1回以上、繰り返しテストされる。保存されるOT資産の情報には、少なくとも、構成、役割、PLCのロジック、エンジニアリング図面、およびツールを含める。

2.S– インシデント対応 (IR) 計画 PR.IP-9, PR.IP-10

成果

組織は、関連する脅威シナリオに対するサイバーセキュリティインシデント対応計画を維持し、実践し、更新する。

対処されるTTPまたはリスク	範囲
サイバーセキュリティインシデントを迅速かつ効果的に封じ込め、軽減し、伝達することができない。	組織全体

推奨される行動

組織は、一般的な脅威シナリオと組織固有（例えば、部門別、地域別）の脅威シナリオおよびTTPの両方について、ITおよびOTサイバーセキュリティのインシデント対応計画を持ち、維持し、更新し、定期的に訓練する。テストや訓練を実施する場合、可能な限り現実的なものとする。インシデント対応計画は、少なくとも年1回訓練し、演習や訓練で得られた教訓に基づいて、リスク情報に基づいた時間枠内に更新する。

2.T– ログの収集 PR.PT-1

成果

サイバー攻撃を検知し、効果的に対応するために、より優れた可視性を実現する。

対処されるTTPまたはリスク	範囲
• 潜在的なサイバーインシデントを検知し対応する能力が先延ばし、不十分、または不完全である。 • 防御の棄損 (T1562)	ITおよびOT資産

推奨される行動

アクセスおよびセキュリティに重点を置いたログ（例えば、侵入検知システム／侵入防止システム、ファイアウォール、データ損失防止、仮想プライベートネットワーク（VPN））を、検知およびインシデント対応活動（例えば、フォレンジック）の両方で使用するために、収集・保存する。Windowsイベントログのような重要なログソースが無効化された場合には、セキュリティチームに通知する。

OT: ログが非標準、または利用できないOT資産については、それらの資産と他の資産との間のネットワークトラフィックおよび通信を収集する。

2.U– セキュアなログの保管 PR.PT-1

成果

組織のセキュリティログは、不正アクセスおよび改ざんから保護されている。

対処されるTTPまたはリスク	範囲
• ホスト上の痕跡の削除 - Windowsイベントログの消去 (T1070.001) • ホスト上の痕跡の削除 - LinuxやMacのシステムログの消去 (T1070.002) • ホスト上の痕跡の削除 - ファイル削除 (T1070.004) • ホスト上の痕跡の削除 (ICS T0872)	ITおよびOT資産

推奨される行動

ログは、セキュリティ情報およびイベント管理ツールまたは中央データベースなどの中央システムに保存され、認可されたユーザーまたは認証されたユーザーのみがアクセスできる。ログは、リスクまたは関連する規制ガイドラインに基づいた期間、保存される。

2.V– 不正な機器の接続禁止 PR.PT-2

成果

不正なポータブルメディアを介した、悪意のある行為者による初期アクセスまたはデータ漏出を防止する。

対処されるTTPまたはリスク	範囲
• ハードウェアの追加 (T1200) • リムーバルメディアによる複製 (T1091, ICS T0847)	ITおよびOT資産

推奨される行動

組織は、USB機器やリムーバブルメディアの使用を制限する、または自動実行（AutoRun）を無効にするなど、不正なメディアおよびハードウェアがITおよびOT資産に接続されないようにすることを確実にするためのポリシーとプロセスを維持する。

OT: 可能な場合は、不正な機器の接続を防止するために、物理ポートを削除、無効化、またはその他の方法でセキュアにする手順を確立するか、承認された例外を通じてアクセスを許可するための手順を確立する。

2.W– インターネット上で悪用可能なサービスがない PR.AC-3

成果

不正なユーザーは、公衆インターネットに面した資産の既知の弱点を悪用して、システムへの最初の足がかりを得ることはできない。

対処されるTTPまたはリスク	範囲
• アクティブスキャン - 脆弱性スキャン (T1595.002) • 外部公開されたアプリケーションへの攻撃(T1190, ICS T0819) • リモートサービスの悪用 (T1210, ICS T0866) • 外部リモートサービス (T1133, ICS T0822) • リモートサービス - リモートデスクトッププロトコル (T1021.001)	公衆インターネット上のITおよびOT資産

推奨される行動

公衆インターネット上のサービスは、リモートデスクトッププロトコルなどの悪用可能なサービスを露出していない。これらのサービスが露出される必要がある場合には、一般的な不正使用および悪用を防ぐために、適切な代替管理策を実装する。インターネットに面した資産では、不要なOSアプリケーションおよびネットワークプロトコルを、すべて無効化する。

2.X– 公衆インターネットへのOT接続の制限 PR.PT-4, PR.AC-5

成果

脅威行為者が公衆インターネットに接続されたOT資産を悪用または妨害するリスクを低減する。

対処されるTTPまたはリスク

- アクティブスキャン - 脆弱性スキャン (T1595.002)
- 外部公開されたアプリケーションへの攻撃(T1190, ICS T0819)
- リモートサービスの悪用 (T1210, ICS T0866)
- 外部リモートサービス (T1133, ICS T0822)

範囲

公衆インターネット上のOT資産

推奨される行動

運用に明示的に必要な場合を除き、公衆インターネット上に存在するOT資産は存在しない。例外は正当化され、文書化されなければならず、例外とした資産には、悪用の試みを防止および検知するための追加の保護策（ロギング、MFA、プロキシまたはその他の介在経由の強制アクセスなど）が実施されていなければならない。

検知 (DETECT)

3.A– 関連する脅威およびTTPの検知

ID.RA-2, ID.RA-3, DE.CM-1

成果	推奨される行動
組織は、関連する脅威およびTTPを認識し、検知することができる。	組織は、自組織に関連する脅威およびサイバー行為者のTTPのリストを文書化し（例えば、産業や部門に基づいて）、それらの主要な脅威の実態を（例えばール、アラート、または市販の防止・検知システムなどを介して）検知する能力を維持する。

対処されるTTPまたはリスク	範囲
関連する脅威に関する知識およびそれらを検知する能力がなければ、組織は脅威行為者が長期間にわたってネットワーク内で検知されずに存在する可能性があるリスクを負う。	該当なし

対応 (RESPOND)

4.A– インシデント報告 RS.CO-2, RS.CO-4

成果	推奨される行動
CISAおよびその他の組織が、サイバー攻撃のより広範な支援または理解を、より上手く提供することができる。	組織は、確認されたすべてのサイバーセキュリティインシデントを適切な外部エンティティ（例えば、州／連邦の規制当局、または必要に応じてSRMA、ISAC/ISAO、CISA）に、誰に、どのように報告するかについて成文化されたポリシーおよび手順を維持する。 既知のインシデントは、適用される規制ガイダンスが指示する期間内に、またはガイダンスがない場合は、安全に対応できるようになり次第、CISAおよびその他の必要な関係者に報告される。この目標は、2022年重要インフラサイバーインシデント報告法 (CIRCIA)の完全な実施後に再検討される予定である。

対処されるTTPまたはリスク	範囲
タイムリーなインシデント報告がなければ、CISAおよびその他の団体は影響を受けた組織を支援することができず、より広範な脅威の状況（特定の部門に対して広範な攻撃がはっせいしているかどうかなど）に対する重要な洞察が不足する。	組織全体

4.B– 脆弱性開示／報告 RS.AN-5

成果	推奨される行動
組織は、セキュリティ研究者によって発見された資産の脆弱性または弱点について、より迅速に学ぶ。研究者は、自らの発見を責任を持って共有する動機付けが高まる。	NIST SP 800-53 Revision 5 に準拠して、組織は、セキュリティ研究者が、脆弱な資産、誤設定された資産、またはその他の悪用可能な資産を、セキュリティ研究者が組織のセキュリティチームに（例えば、電子メールアドレス、またはウェブフォーム経由で）通知するための、公開された、容易に発見できる方法を維持する。有効な通知は、網羅性と複雑性を考慮した上で、タイムリーに承認され、対応される。検証された悪用可能な脆弱性は、その深刻度に応じて軽減される。 発見した脆弱性を善意で共有するセキュリティ研究者は、セーフ・ハーバー・ルール（Safe Harbor rules）の下で保護される。 脆弱性が検証され、開示された場合、最初に通知を提出した研究者に、公の承認が与えられる。

対処されるTTPまたはリスク	範囲
• アクティブスキャン - 脆弱性スキャン (T1595.002) • 外部公開されたアプリケーションへの攻撃 (T1190, ICS T0819) • リモートサービスの悪用 (T1210, ICS T0866) • サプライチェーンの侵害 (T1195, ICS T0862)	すべての資産

4.C– SECURITY.TXT ファイルの配置 RS.AN-5

成果	推奨される行動
セキュリティ研究者が、発見した弱点または脆弱性を、迅速に提示できるようにする。	すべての公開されたWebドメインは、RFC 9116の勧告に準拠したsecurity.txtファイルを持つ。

対処されるTTPまたはリスク	範囲
• アクティブスキャン - 脆弱性スキャン (T1595.002) • 外部公開されたアプリケーションへの攻撃(T1190, ICS T0819) • リモートサービスの悪用 (T1210, ICS T0866) • サプライチェーンの侵害 (T1195, ICS T0862)	すべての公開されたWebドメイン

復旧 (RECOVER)

5.A– インシデント計画および準備

RC.RP-1, PR.IP-9, PR.IP-10

成果	推奨される行動
組織は、サイバーセキュリティインシデントから安全かつ効果的に復旧することができる。	サイバーセキュリティインシデントによってインパクトを受ける可能性があるビジネスまたはミッションクリティカルな資産またはシステムを復旧してサービスを再開するための計画を策定、維持、および実行する。

対処されるTTPまたはリスク	範囲
資産、サービス、またはシステムの可用性の中断。	ITおよびOT資産

用語集

アクセス制御リスト（Access Control List）：リソースへのアクセスが許可されているシステムエンティティのIDを列挙することによって、システムリソースへのアクセス制御を実装するメカニズム。

管理ドメイン: 共通のポリシーによって管理されるホストおよびネットワークリソースの論理的な集合（例えば、部署、建物、会社、組織）。

資産: 価値を持つ人、構造、施設、情報、材料、またはプロセス。

自動アカウントロックアウトまたはアカウントロックアウトのしきい値: ユーザーアカウントがロックされる原因となる、サインイン失敗の回数を決定するポリシー。

ベースライン構成:情報システムまたはシステム内の構成項目に関する文書化された一連の仕様で、ある時点で正式にレビューされ、合意されたもので、変更管理手続きによってのみ変更可能なもの。

ビジネスインパクトのアセスメントまたはビジネスインパクトの分析: 重大な中断が発生した場合の、システムの緊急時要件および優先順位を明らかにするために使用される、情報システムの要件、機能、および相互依存関係の分析。

変更管理: 組織を現在の状態から将来の状態に移行させ、期待されるメリットを得るために、構造化されたアプローチを適用するプラクティス。

構成（Configuration）：情報システムまたはシステムコンポーネントを記述または配置することができる条件、パラメータおよび仕様。

継続的な監視: 組織のリスク判断をサポートするために、継続的な意識を維持すること。

共通脆弱性識別子（CVE）：セキュリティに関連するソフトウェアの欠陥の命名法および辞書。

代替管理策: NIST SP 800-53に記載されているベースラインの管理策の代わりに実装され、システムまたは組織に対して同等またはそれに相当する保護を提供するセキュリティおよびプライバシー管理策。

制御システム: 意図的な指図または操作によって、ある変数が所定の値となるようにするシステム。制御システムには、監視制御システム（SCADA）、分散制御システム（DCS）、プログラマブルロジックコントローラ（PLC）、およびそのその他の種類の産業用の計測および制御システムが含まれる。

サイバーセキュリティ意識向上トレーニングまたはITセキュリティ意識向上およびトレーニングプログラム: 政府機関の情報システムおよび情報の使用のための適切な行動ルールについて説明する。このプログラムは、従う必要がある情報技術（IT）ポリシーおよび手順を伝える。

サイバーセキュリティのライフサイクル: 連邦政府機関は、重要なミッションを成功させるために、その情報および情報システムに大きく依存している。情報システムに対する信頼性が高まり、複雑さが増すとともに、リスク環境が絶えず変化する中、情報セキュリティはミッションに不可欠な機能となっている。この機能は、政府機関に委ねられた情報、政府機関全体のミッション、および事業を行い米国民に奉仕する能力に対するリスクを低減する方法で実施されなければならない。情報セキュリティは、情報の機密性、完全性、および可用性に対するリスクを適切かつ効果的に管理することによって適用される場合、事業の成功要因となる。

サイバーセキュリティ対応計画またはインシデント対応計画: 組織の情報システムに対する悪意のあるサイバー攻撃を検知し、対応し、その結果を制限するための、あらかじめ決められた一連の指示または手順を文書化したもの。

デフォルトパスワード: 組み込みシステム、機器、アプライアンスの工場出荷時のデフォルトのソフトウェア構成には、一般に公開されているシンプルなパスワードが含まれていることが多い。これらのシステムは通常、ユーザー管理のための完全なオペレーティングシステムのインタフェースを提供しておらず、デフォルトパスワードは通常、ベンダまたは製品ライン内で同一（共通）である。デフォルトパスワードは、最初のテスト、インストール、および設定操作のためのもので、多くのベンダは、本番環境にシステムを展開する前にデフォルトパスワードを変更することを推奨している。

非武装地帯（DMZ）:内部ネットワークと外部ネットワークの間に論理的に存在する境界ネットワークセグメント。DMZの目的は、内部ネットワークの情報保証ポリシーを外部との情報交換に適用し、内部ネットワークを侵入から保護しながら、外部の信頼できないソースに、公開可能な情報への制限されたアクセスを提供することである。

暗号化する: データを暗号化して暗号文を生成する。

暗号化: 平文を暗号文に変換し、意図した受信者以外がそのデータを読むことができないようにするための暗号技術で使用される、あらゆる手順。

実行ファイルまたは実行可能ファイル: エンコードされた命令に従って、指示されたタスクを実行する。一般的には、コンピュータプログラムまたはルーチンを参照して使用される。

ファイアウォール: 接続された2つのネットワーク間のデータ通信トラフィックを制限する、ネットワーク間接続装置。ファイアウォールは、汎用コンピュータにインストールされたアプリケーションの場合もあれば、ネットワーク上でパケットを転送、または拒否／ドロップする専用のプラットフォーム（アプライアンス）の場合もある。通常、ファイアウォールはゾーン境界を定義するために使用される。ファイアウォールには一般に、どのポートを開くかを制限するルールがある。

ファームウェア: ハードウェア機器のフラッシュROMにプログラムされたソフトウェアプログラムまたは命令セット。機器が他のコンピュータハードウェアとどのように通信するかについて、必要な命令を提供する。

ハッシュ化: 一連のデータに対して、数学的アルゴリズムを適用し、データを表す数値（「ハッシュ値」）を生成するプロセス。

ヒューマンマシンインタフェース（HMI）: 人間のオペレータが制御下のプロセスの状態を監視し、制御設定を変更して制御目的を変更したり、緊急時に自動制御操作を手動でオーバーライドしたりできるソフトウェアおよびハードウェア。HMIはまた、制御エンジニアまたはオペレータが、コントローラ内のセットポイントまたは制御アルゴリズムおよびパラメータを設定することを可能にする。またHMIは、オペレータ、管理者、マネージャー、ビジネスパートナー、およびそのほかの認可されたユーザーに対して、プロセスのステータス情報、履歴情報、レポート、およびその他の情報を表示する。オペレータおよびエンジニアはHMIを使用して、セットポイントの監視と設定、アルゴリズムの制御、コマンドの送信、コントローラのパラメータの調整と設定を行う。HMIには、プロセスのステータス情報および履歴情報も表示される。

インシデント対応計画: サイバーインシデントを検知し、対応するための、あらかじめ決められ文書化された一連の手順。

情報共有分析機関（ISAO）：以下の目的のために、公的機関または民間の組織によって設立または雇用された、公式または非公式の事業体または共同体。（a）重要インフラおよび保護されたシステムに関連するセキュリティ上の問題および相互依存関係をより良く理解し、その可用性、完全性、および信頼性を確実にするために、重要インフラ情報を収集および分析すること。（b）重要インフラまたは保護されたシステムに関連する干渉、侵害、または資格はく奪の問題の影響を防止、検知、緩和、または回復するのに役立つ重要インフラ情報を伝達または開示すること。（c）重要インフラ情報を、会員、州、地方、連邦政府、または上記の目的の遂行する上で助けとなる可能性のあるその他の事業体に自発的に広めること。

情報共有分析センター（ISAC）：脆弱性、脅威、侵入、異常に関する情報を収集、分析、適切にサニタイズし、産業および政府のパートナーに広めるためのメカニズムとして機能するために、民間の重要インフラ所有者および運営者が、（要請に応じて）連邦政府と協議し、支援を受けて設立した信頼できる運営事業体。ISACは、物理的脅威・サイバー脅威および緩和策に関する情報およびベストプラクティスを共有するために、特定の重要インフラ分野内の施設や組織が協力する、分野ベースのモデルで運営される。ほとんどのISACは、その分野の状況認識を維持し、24時間週7日体制で脅威の警告およびインシデント報告を提供している。またその分野の脅威レベルを設定しているISACもある。ISACは、官民パートナーシップを成功させるためにきわめて重要であるが、個々の企業と政府との間の直接的な情報交換を妨げることを意図していない。

情報技術（IT）：データまたは情報の自動的な取得、保存、分析、評価、操作、管理、移動、制御、表示、切り替え、交換、送信、または受信に使用されるあらゆる機器、相互接続されたシステム、または機器のサブシステム。

国際電気標準会議 (IEC): IECは、世界173ヶ国が集まり、2万人の専門家の活動を調整している、世界的な非営利の会員組織である。IECの国際規格および適合性アセスメント業務は、電気・電子製品の国際貿易を支えている。IECは、電気の利用を促進し、携帯電話や冷蔵庫などの民生機器、オフィス機器、医療機器、情報技術、発電を含む電気・電子機器およびシステムの安全性、性能、相互運用性を検証している。

国際自動制御学会（ISA）：国際自動制御学会（ISA）は、自動制御を通じてより良い世界を創造するために1945年に設立された非営利の専門家団体である。ISAは、オペレーショナル・エクセレンスを達成するために自動制御コミュニティを結び付けることによって技術的能力を向上させ、標準ベースの基本的な技術リソースを提供し、 個人のキャリアと職業全体の前進を推進している。ISAは、広く使用される世界標準を策定し、 専門家を認定し、教育およびトレーニングを提供し、書籍や技術記事を出版し、会議や展示会を主催している。また、世界中の会員と顧客のために、人的ネットワーク形成およびキャリア開発プログラムを提供している。

ISA/IEC 62443: ISA99委員会によって策定され、IECによって承認されたISA/IEC 62443シリーズの標準は、産業用自動制御および制御システム（IACS）における現在および将来のセキュリティ脆弱性に対処し、緩和するための柔軟なフレームワークを提供している。

インベントリ: 組織に割り当てられた動産の正式なリストまたは動産記録。

Known Exploitable Vulnerabilities Catalog（既知の悪用された脆弱性カタログ）：CISAが悪用された、または脅威行為者によって使用されたと識別した脆弱性のリスト。「Binding Operations Directive（拘束力のある運用指令）22-01」の一環として、このカタログは連邦民間行政機関（FCEB）に対し、連邦政府のインフラを保護し、サイバー攻撃を減らすために、特定の期間内にこれらの問題を修正しなければならない、と指示している。

最小特権の原則: セキュリティアーキテクチャは、各事業体がその機能を実行するために必要な最小限のシステムリソースおよび認可を付与されるよう設計される、という原則。

ログ: 組織のシステムおよびネットワーク内で発生したイベントの記録。

マイクロソフト オフィス マクロ: Accessのマクロは、タスクを自動化し、フォーム、レポートおよびコントロールに機能を追加するツールである。例えば、コマンドボタンをフォームに追加すると、そのボタンのOnClickイベントにマクロが関連付けられる。

米国国立標準技術研究所 (NIST): 米国国立標準技術研究所は、経済安全保障を強化し、生活の質を向上させる方法で、計測学、標準および技術を進歩させることにより、米国のイノベーションおよび産業競争力を促進している。

ネットワークのセグメンテーションおよび分離: ネットワークのセグメンテーションは、ネットワークをより小さなネットワークに分割することであり、ネットワークの分離は、特定のホストとサービス間の通信を制御するためのルールセットを策定して適用すること。

NIST サイバーセキュリティフレームワーク (CSF): 重要インフラ分野全体に共通し、特定の成果を中心にまとめられた、一連のサイバーセキュリティ活動および参照文献。フレームワークコアは、機能、カテゴリ、サブカテゴリ、および参考情報、の4種類の要素で構成されている。

NIST リスクマネジメントフレームワーク: NIST SP 800-37で示されているリスクマネジメントフレームワーク (RMF) は、情報セキュリティおよびリスク管理の活動をシステム開発ライフサイクルに統合する、 統制のとれた構造化されたプロセスを提供している。

NIST SP 800-30: 連邦政府の情報システムおよび組織のリスクアセスメントを実施するためのガイダンスを提供し、SP 800-39のガイダンスを詳述している。リスク管理階層の3つの階層すべてで実行されるリスクアセスメントは、全体的なリスク管理プロセスの一部であり、識別されたリスクに対応する、適切な活動指針を決定するために必要な情報を、最高幹部／経営陣に提供する。

NIST SP 800-53: この出版物は、システムおよび組織の管理策を確立する。管理策は、情報を処理、保存、または送信する、あらゆる組織またはシステム内に実装することができる。これらの管理策の使用は、連邦政府の情報システムには必須である。NIST SP 800-53は、変化する脅威、脆弱性、要件、およびテクノロジーに基づいて、現在および将来の保護ニーズを満たすセキュリティおよびプライバシー管理策の包括的かつ柔軟なカタログを提供することによって、この目的を達成する。また、この出版物は、セキュリティ、プライバシー、およびリスク管理の概念の議論をサポートする共通の語彙を提供することにより、組織間のコミュニケーションを改善する。

NIST SP 800-82: 監視制御システム（SCADA）、分散制御システム（DCS）、および制御機能を実行するその他のシステムを含む産業用制御システム（ICS）をセキュアにするためのガイダンスを提供している。この文書は、ICSの概念的な概要を提供し、一般的なシステムトポロジおよびアーキテクチャをレビューし、これらのシステムに対する既知の脅威および脆弱性を識別し、関連するリスクを軽減するための推奨されるセキュリティ対策を提供している。

制御・運用技術（OT）: 物理環境と対話する（または物理環境と対話する機器を管理する）プログラム可能なシステムまたは機器。これらのシステム／機器は、機器、プロセス、およびイベントの監視や制御を通じて、直接的な変化を検知、または引き起こす。例えば、ICS、ビル管理システム、防火システム、物理的なアクセス制御メカニズム、などが含まれる。

ペネトレーションテスト（リモート）： 悪用可能な経路を識別して検証するために、実際の脅威行為者の戦術および技術をシミュレートする。このサービスは、境界の防御、外部から利用可能なアプリケーションのセキュリティ、およびオープンソース情報の悪用の可能性をテストするのに理想的である。

フィッシング: 個人をだまして機密情報を提供させるための、ソーシャルエンジニアリングのデジタルな形態。

フィッシングに強いMFA: OMB Memorandum 22-09に定義されているように、認証シークレットおよび正当なシステムになりすましたウェブサイトまたはアプリケーションへの出力の開示を検知し、防止するように設計された認証プロセス。

特権アカウント: 特権ユーザーの承認された認可を持つ情報システムのアカウント。

リモートデスクトッププロトコル（RDP）： 通常はTCPポート3389を介して、他のコンピュータへのリモート接続を可能にするマイクロソフト社独自のプロトコル。暗号化されたチャネルを介したリモートユーザーにネットワークアクセスを提供する。ネットワーク管理者は、RDPを使用して問題を診断し、サーバにログインし、その他の遠隔の活動を実行する。リモートユーザーは、RDPを使用して組織のネットワークにログインし、電子メールやファイルにアクセスする。

パスワードのソルト化またはパスワードソルト: 解読をより困難にするためにパスワードに付与されるランダムな文字列。パスワードを取得してハッシュアルゴリズムで実行し、その結果をログインデータベースに保存するのが一般的である。ユーザーがパスワードを入力すると、再びハッシュ化され、データベースと照合される。ソルトはハッシュ化の前にパスワードに追加されるランダムな文字列で、「ブルートフォース」辞書攻撃を使用してパスワードをつきとめることをより困難にする

システムアーキテクチャ: アーキテクチャとは、システムの基本的な構成であり、コンポーネント、相互の関係および環境、設計と進化に適用している原則が具体化されている。

机上演習（TTX）： 特定のIT計画で役割を持ち責任を負う社員が、教室の設定または分科会（breakout groups）で集まり、緊急時の役割と特定の緊急事態への対応について議論することで計画の内容を検証する、議論ベースの演習。進行役は、シナリオを提示し、そのシナリオに基づいて質問することによって議論を開始する。

トランスポート・レイヤー・セキュリティ(TLS): ブラウザおよびウェブサーバに広く実装されている認証および暗号化プロトコル。TLSを使用して送信されるHTTPトラフィックは、HTTPSとして知られている。

脆弱性開示プログラム: セキュリティ研究者に、脆弱性発見活動を行うための明確なガイドラインを提供し、発見された脆弱性を組織に提出するためのCISAの優先事項を伝えている。

謝辞

サイバーセキュリティのパフォーマンス目標は、官民のステークホルダーからの分野横断的なインプットなくしては、不可能であった。CISAとNISTは、これらの目標に対して貢献的なコメントを寄せてくれた以下の企業、組織、米国連邦政府機関、および国際的なパートナーに感謝の意を表する。

1898 & Co; AAC Cyber Group; ABS Group; Administration for Strategic Preparedness and Response (ASPR); Amazon Web Services; American Chemistry Council (AAC) Cybersecurity Information Sharing Group; American Fuel and Petrochemical Manufacturers (AFPM); American Gas Association; American Petroleum Institute (API); American Public Power Association (APPA); American Water Works Association; Area Maritime Security Committee Houston-Galveston; Bechtel; Boeing; Chemical Sector Coordinating Council (CSCC); City of Crystal, Minnesota; City of Phoenix Department of Aviation (Phoenix Sky Harbor International Airport); City of Pittsburgh Housing Authority; Claroty; Colorado River Energy Distributors Association; Consolidated Communications; CTIA, NCTA, USTelecom; Cyber Risk Institute; Cyber Threat Alliance; D.L.; Discover Financial Services; Eclypsium, Inc.; Dragos; Edison Electric Institute; Enbridge, Inc.; Exxon; Federal Deposit Insurance Corporation (FDIC); Federal Housing Finance Agency (FHFA); Federal Reserve (and Federal Reserve, Financial Services); FERC, Division of Dam Safety and Inspections; Financial Services Sector Coordinating Council (FSSCC); FireEye; GE; Granite Falls Consulting; Information Security Officer, Maersk Line, Limited; Honeywell; Information Technology Industry Council (ITI); Israel National Cyber Directorate (INCD); IT Sector Coordinating Council (IT-SCC); JP Morgan; Marsh; Matson Navigation Company; Microsoft; National Air Transportation Association; National Rural Electric Cooperative Association (NRECA); National Water Resources Association (CREDA/NWRA); National Cyber Security Centre (NCSC (UK)); NCTA; Netrise; Network Perception; Netwrix Corporation; Nozomi Networks; NTCA – The Rural Broadband Association; Office of the Comptroller of the Currency (OCC); Operational Technology Cybersecurity Coalition; Pacific Northwest National Laboratory (PNNL); Port Authority of New York and New Jersey; Port of Houston Authority; Schneider Electric; Securities and Exchange Commission (SEC); Securities Investor Protection Corporation (SIPC); Sera-Brynn Consulting; Siemens Government Technologies; Southern California Edison; Southern Company; State of Washington, Cybersecurity & Critical Infrastructure Protection Unit; Transportation Security Administration (TSA); U.S. Army, Materiel Command; U.S. Department of Energy (DOE); U.S. Environmental Protection Agency (EPA); U.S. Nuclear Regulatory Commission; U.S. Coast Guard; University of Miami Health System; U.S. Mint – Philadelphia; Both public and private members of CISA's Control Systems Working Group (CSWG) and Control Systems Interagency Working Group (CSIWG); Department of Health and Human Services (HHS), Food and Drug Administration (FDA), Office of the National Coordinator for Health Information Technology (ONC)); Water Environment Federation; Water Sector Coordinating Council; Waterfall Security; Woodard & Curran; Xylem.

CISAは、組織に加えて、特に貴重なフィードバックをいただいた以下の個人を評価したい。

Marco Ayala, David Batz, Bryson Bort, Mark Bristow, Lance Cleghorn, Josh Corman, Curt Dukes, Danielle Jablanksi, Chris Jager, Isaiah Jones, Robert M. Lee, Joe Marshall, Patrick Miller, Thomas Reagan, Alexander Romero, Marty Rubin, Kimberly Sanders, Gus Serino, and Nicole Thompson.