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

Version 2.0

2025年12月

米国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）

目次

背景と状況

今後の課題

CISAは、米国の重要インフラにおけるサイバーセキュリティの状況と脅威の状況の特質に関する独自の知見を得るために、政府、民間分野、国際的なパートナーと共に日々努力している。こうしたパートナーシップ[1]およびCISA自身のサイバーアセスメント、脅威ハンティング、インシデント対応活動を通じて、重要インフラ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欠如が定期的に確認されている。本資料の策定過程で意見を提供した専門家や重要インフラ運営者も、同様の見解を示した。

各組織は、固有のサイバーセキュリティ課題に直面している。中小規模の組織では、予算、人員、専門知識が限られている場合がある。一方、成熟したサイバーセキュリティプログラムを持つ組織は、特に制御・運用技術（OT）を含む環境において、高度な敵対者の一歩先を行くために、基礎的な防御を超えた対策を講じようと努めている。

サイバーセキュリティのガイダンスは広く入手可能であるが、多くの組織から、次のような支援が必要だとの要望が頻繁に寄せられている。

1. 最大のリスク低減をもたらすプラクティスの識別。
2. 最大の効果を得るための、これらのプラクティスの優先順位付け。
3. 上級管理職や経営陣に対してプラクティスの価値を伝えること。

CISAはこうしたニーズに対応するために、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（CPG）を策定した。

CPGは、情報技術（IT）およびOT環境向けの合理化された、成果重視のサイバーセキュリティ防御策である。CPGは以下のものを提供する。

- 現実の脅威に合わせた、明確で基本的なプラクティス。
- 実装を支援するための、平易な成果重視の表現。
- 投資の指針、進捗のベンチマーク、測定可能な方法によるリスク低減のためのベースライン。

継続的な改善と米国国立標準技術研究所（NIST）サイバーセキュリティフレームワーク（CSF）2.0との整合性に対するCISAのコミットメントに基づき、CISAは、統治機能を追加することでCPGを強化した。この新たなコンポーネントは、サイバーセキュリティの監督における組織的リーダーシップの重要な役割を強調している。それは、説明責任、リスクマネジメント、および日常業務へのサイバーセキュリティの戦略的統合を強調し、効果的な統治が強靭なサイバー態勢の礎であるという原則を強化する。

CISAは、CPGを親しみやすく実用的なものとして設計した。CPGは、一般的でインパクトのあるサイバーリスクを明確かつ簡潔に対処することを目的としており、サイバーセキュリティの実務者だけでなく、経営幹部や取締役会メンバーを含む非技術的なステークホルダーにも理解しやすい内容となっている。

連邦政府、州政府、地方政府、準州政府、部族政府、民間分野の多数の組織が、2022年の初版公開以来、CPGを実装してきた。早期導入組織は、これをベースラインのサイバーセキュリティ衛生管理を評価し、サイバーセキュリティのリソース要求を通知するために使用した。しかし、大規模な公益事業体や政府機関と小規模組織との間ではCPG導入に格差が生じており、小規模組織は高レベルの目標を具体的な行動に移すことに苦労することが多い。この格差に対する我々の懸念は、単なる仮説以上のものだ。 我が国は、学校や病院を標的とするランサムウェア攻撃から、政府機関や重要インフラを狙う高度な国家主導の攻撃まで、多岐にわたる現実世界でのインパクトを目の当たりにしてきた。これらの侵入行為は総じて、国家安全保障、経済安全保障、そしてアメリカ国民の健康と安全にリスクをもたらしている。

2022年のCPG公表以来、進展は見られるものの、我が国のサイバーセキュリティリスクは依然として多い。CISAは、得られた教訓を取り入れ、最新のNIST CSF 改訂版と整合させ、以下の課題に対処するため、本CPG更新版を公表する。

[1] 具体的なパートナーには、16の重要インフラ分野にまたがる組織および各分野のリスクマネジメント政府機関が含まれる。

1. **OTサイバーセキュリティは見過ごされ、リソースが不足していることが多い。**サイバーセキュリティ業界は、主にビジネスITシステムに焦点を当て続けており、OT環境がもたらす固有かつ重大なリスクを頻繁に軽視している。製造業者は従来、これらのシステムをセキュリティではなく信頼性と可用性のために設計してきた。また、組み込みの保護機能も不足している場合が多い。ネットワークに接続できるOTデバイスが増えるにつれ、不十分なサイバーセキュリティ対策が重要インフラを深刻な脅威に晒している。 多くの組織には、まだ専用のOTサイバーセキュリティプログラムがない。これは、サイバーセキュリティをITの問題としてのみ捉えている組織では特に顕著である。現在存在するOTサイバーセキュリティプログラムは、基本的なサイバーセキュリティプラクティスや実行可能なOT固有の防御策において不十分な場合が多い。

2. **多くの組織は、基本的なセキュリティ防御策を採用していない。**多要素認証（MFA）、強固なパスワード管理、定期的なバックアップといった基本的な防御策の欠如は、重要インフラを有害なサイバー侵入に晒している。

3. **中小規模の組織は取り残されている。**リソースが限られている組織や、サイバーセキュリティプログラムの成熟度が低い組織は、合理的なサイバーセキュリティ対策の実施方法を決定する際に困難に直面することが多い。NIST CSFのような既存リソースがあるにもかかわらず、小規模組織は、サイバーセキュリティ態勢に最大の影響をもたらすためにどこに投資すべきかを特定したり、サイバーセキュリティ防御策を効果的に実装する方法を決定したりするのに困難を抱えている。[2]

4. **一貫した基準とサイバー成熟度の欠如。**重要インフラ分野では、サイバーセキュリティケイパビリティ（能力）、投資、ベースラインプラクティスに著しい不一致が存在する。この不一致は、脅威アクターが機能障害や連鎖的なインパクトを引き起こすために悪用できるギャップにつながる可能性がある。

[2] 参入障壁を下げるため、CISAは2023年に分野固有の目標（SSG）の提供を開始した。これは特定の重要インフラ分野向けにテーラリングされた、インパクトの大きいセキュリティ対策を含む追加の自主的プラクティスである。SSGはCPGを基盤としつつ、各分野固有の要件に対応するとともに、中小企業を含む組織が悪意あるサイバー活動から防御するために実行可能な対策を提供する。

課題への対応

CISAは、法定権限（合衆国法典第6編第652条）に基づき、サイバーセキュリティアセスメントという形で技術支援を提供し、米国国立標準技術研究所（NIST）およびその他の連邦機関と連携して重要インフラのベースラインのサイバーセキュリティ目標を維持している。 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（CPG）に加え、CISAは連邦セクターリスク管理機関（SRMA）および重要インフラコミュニティと連携し、追加の分野固有の目標（SSG）を策定している。

CPGとは？

端的に言えば、CPGとは、重要インフラの運用と米国国民の両方に対するリスクを実質的に低減することを目的とした、ITおよびOTの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できる。CISAおよびその政府・産業界のパートナーが観測した最も一般的かつインパクトの大きい脅威と敵対者の戦術・技術・手順（TTPs）がCPGに反映されている。これによりCPGは、大規模から小規模まで全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防御策となっている。

CPGの主な特徴

- 優先順位付けされたサイバーセキュリティプラクティスのサブセット
- ITおよびOT向け
- リスク低減を優先
- CISAおよびその政府・産業界のパートナーが観測した脅威を反映
- すべての重要インフラ分野に適用可能
- 重要インフラの運用と米国国民の両方に対するリスクを実質的に低減することが目的

CPG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、組織が実装することが望ましい最低限の一連のプラクティスである。重要インフラ事業者、特に中小規模組織が、強固なサイバーセキュリティ態勢構築への第一歩を踏み出すための支援を目的としている。したがってCISAは、CPGを組織がサイバーリスク低減のために実装することが望ましいサイバーセキュリティ防御の下限として位置付けており、上限ではない。重要な点として、CPGは**以下のようなものではない**。

- **包括的：**CPGは、あらゆる組織を防御するために必要な全てのサイバーセキュリティプラクティスを識別しているわけではない。また、あらゆる潜在的なリスクから国家安全保障、経済安全保障、および公衆衛生・安全を完全に保護するものでもない。これらは、リスク低減効果が確認され、あらゆる分野に広く適用可能な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表している。しかし、CISAは、各分野固有の制約条件、脅威、成熟度を深く掘り下げた分野固有の目標を展開している。
- **リスクマネジメントまたは完全なサイバーセキュリティプログラム：**CPGは、NIST CSFなどの他のフレームワークが明確にしているような、リスクマネジメントまたはリスクの優先順位付けに関する、より広範なアプローチを網羅していない。
- **CISAによる義務付け：**CISAは、組織がCPGを自主的に採用し、NIST CSFなどの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たセキュリティ投資の優先順位付けを可能にすることを意図している。
- **成熟度モデル：**CPGのプラクティスは全ての重要インフラ組織に適用され、「成熟度」カテゴリによる階層化は行われていない。ただし、CPGワークシートには「インパクト」「コスト」および「複雑性」などの基準が含まれており、組織が内部で投資優先順位を決定する際に役立つ。

CISAは、24ヶ月から36ヶ月の目標改訂サイクルに基づき、CPGを定期的に更新する。

CPG選定基準

CPGは、以下の基準を使用して、業界、政府、専門家による協議プロセスを経て選択されたサイバーセキュリティプラクティスのサブセットである。

1. 一般的に観察される、分野横断的な脅威およびサイバー脅威アクターのTTP（戦術・技術・手順）のリスクまたはインパクトを軽減する上での実証済みの価値があること。
2. 明確で、実行可能で、かつ容易に定義できること。
3. 中小規模の組織が、合理的に容易に、かつ法外な費用の負担なく、成功裏に実装できること。

この基準を満たすCPGの例としては、「組織の、インターネットに接続されているシステムに、既知の悪用された脆弱性（KEV）が存在しないことを確実にする」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（国家レベルの脅威アクターが実際にそれらの弱点を悪用しているという脅威）からのリスクを直接的に低減する。一方、「ゼロトラストを実装する」といったプラクティスは、現時点では適切なCPGとは言えない。ゼロトラストは非常に有効なアプローチだが、CPGの対象となる多くの小規模組織は、CPGの一連の全セットをまだ実装していない場合、ゼロトラストの実装に課題を抱える可能性がある。

CPGモデル

本文書は、CPGを視覚的なモデルで表示することで、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TTP、およびその他の重要な情報を理解できるようにしている。

各目標は、以下のコンポーネントで構成されている。

これらは NIST CSF や他の標準とどのように異なるのか？

他にも、特に米国政府による既存のサイバーセキュリティガイダンス文書およびフレームワークが存在している。例えば、NIST CSFは現在最も広く採用され、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一つであり続けている。CISAおよび米国政府全体は、持続可能でリスクを認識した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、全ての組織がNIST CSFを採用することを支援している。ステークホルダーからのフィードバックに基づき、組織はNIST CSFやその他のフレームワークおよび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環として、CPGを利用できる。

1. **クイックスタートガイド。**CPGは、サイバーセキュリティの経験、リソース、または体制が整っていない組織が、基本的なサイバーセキュリティプラクティスを迅速に識別し実装するのに役立つ。CPGの適用後または並行して、組織はNIST CSFを活用し続け、包括的なリスクマネジメントプログラムを構築し、追加のNIST管理策を実装できる。

2. **優先順位付けと資金調達。**CPGには、以下で説明するワークシートが含まれている。これは、サイバーセキュリティプログラムが小規模または未成熟な組織が、実装する防御策の優先順位を判断し、それらの防御策の重要性、相対的なインパクト、コストを（技術的知識を持たない）経営陣に伝えるのに役立つ。

3. **NIST CSF マッピング。**CPGの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ている。ただし、CPGはNIST CSFの各サブカテゴリに完全に対応しているわけではない点に注意されたい。各セキュリティプラクティスにおいて、CSFサブカテゴリの識別は、CPGと NIST CSF との関連を示す。既に NIST CSF を採用・実装している組織は、関連する CPG を実装する際に追加作業を行う必要はない。

CPGの使用方法

CPG参照製品

CPGには、以下の2つの文書が提供されている。

1. CPGリスト（本文書）
2. CPGチェックリスト

CPGワークシート

CPGリストに加え、資産所有者および運用者が、以下の目的で使用できる使いやすいワークシートが用意されている。(1) 実装するCPGのレビューと優先順位付け、(2) CPG実装の現状と将来の状態の追跡、(3) 優先順位、トレードオフ、CPGの状況を非技術的な経営幹部などの他のステークホルダーに明確に伝達すること。このワークシートは、CISA.gov、およびCISAのサイバーセキュリティ評価ツール（CSET）内のCPGアセスメントモジュールから入手できる。

このワークシートには、各目標の実装にかかる費用、複雑さ、インパクトに関する一般的な見積もりが含まれている。組織はこれらの見積もりを、ベースラインのサイバーセキュ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情報を提供するための支援として活用できる。

CPGワークシートの使用方法

1. **初期の自己評価を実施する。**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、既に実装済みであるCPGを特定することが望ましい。組織はNIST CSFやISA/IEC 62443などの既存のガイダンスやフレームワークへの準拠を通じて、一部のCPGまたは多くのCPGを既に実装している可能性がある。全てのCPGは、これらの共通フレームワーク内の対応する管理策にマッピングされる。
2. **ギャップを識別し、優先順位を付ける。**組織はCPG実装におけるギャップをレビューし、コスト、複雑さ、インパクトといった要素（いずれもCPGワークシートに記載）に基づき、投資対象領域の優先順位を決定することが望ましい。
3. **投資し、実行する。**組織はステップ2で識別された優先度の高いギャップの実装を開始できる。一部の組織では、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経営陣に要請する際、ワークシートなどの資料が役立つ場合がある。
4. **12ヶ月後に進捗を定期的にレビューする。**サイバーセキュリティ対策の改善に向けた進捗状況を追跡するために、組織は12ヶ月後にワークシートを再検証し、自組織の経営陣および第三者の両方の進捗状況を把握することが望ましい。

CPGの変更点

2025年10月更新：CPG 2.0

CISAは、NISTサイバーセキュリティフレームワーク 2.0との整合を図るとともに、3年間の運用フィードバックを反映し、データ駆動型の推奨事項による新たな脅威への対応を目的として、CPGを更新した。以下に、変更点とその理由の概要を示す。

1. **構造的変更 – 新たな機能「統治」（GOVERN）**
   - 変更点：
     - 6番目のCSF機能「統治」に対応するために、既存の目標を再編成し、番号を付け直した。
     - 従来の目標はすべて、識別、防御、検知、対応、復旧の5つの機能のいずれかにマッピングされた。
   - 理由：新たな「統治」機能は、リーダーシップの説明責任、監督、リスクマネジメントを日常的なサイバーセキュリティプラクティスに統合する。これは、NIST CSF 2.0が組織統治に新たに重点を置いていることを反映している。

2. **目標の統合 – 合理化と分野横断的な整合性**
   - 変更点：
     - CPG 1.0.1のOT専用の目標（1.B/1.C/1.D; 2.I/2.J; 2.W/2.X）を汎用目標（1.A; 3.J; 3.S）に統合した。
     - 関連する目的を簡潔化のため（1.G と 1.Hを1.Dに、2.T と 2.Uを3.Qに）統合した。
   - 理由：
     - これにより、重複するガイダンスが排除され、実務者は同一の管理策について複数の目標を参照する必要がなくなる。
     - 現代のインフラではIT、モノのインターネット（IoT）、OTの境界が曖昧化していることを我々は認識している。したがって、サイロ化されたセクションではなく、1つの目標セットで全体をカバーするようになった。
     - 中小規模の事業体は、ドメイン固有の目標について混乱することなく、一つのフレームワークを全資産に適用できる。

3. **新たな目標 – 新たな脅威とギャップへの対応**
   - 変更点：
     - 4つの新たな目標を追加：
       - 1.B – 積極的なプログラム管理：1.Aを基盤とし、リーダーが戦略を適応させ、進化する脅威に対応することを促進する。
       - 1.E – マネージドサービスプロバイダーのリスク：システムへの深いアクセス権を持つ第三者プロバイダーからのリスクを捕捉する。
       - 3.H – 最小特権の徹底：水平展開を軽減するため、ゼロトラスト原則を推進する。
       - 5.A – インシデントのコミュニケーション手順：危機対応のため、内部チーム、パートナー、サプライヤーとの明確な伝達経路を確立する。
   - 理由：
     - フィードバックにより、v1.0.1では継続的なプログラムの進化、サードパーティー依存関係、又は高度なアクセス制御が明示的に扱われていなかったことが判明した。CPG 2.0の4つの新たな目標は、これらの盲点を補う。
     - マネージドサービスプロバイダーがミッションクリティカルな存在となった今、サプライチェーンの侵害を防ぐには正式なリスク管理策が不可欠である。
     - 明確に定義されたコミュニケーション手順は、インシデント発生時の透明性と調整を確実にし、混乱とダウンタイムを軽減する。

4. **削除項目と意図的な維持**
   - 変更点：
     - 以下の3つのv1.0.1の目標を削除：
       - 4.C – Security.txt の展開は、 2.D（「脆弱性開示/報告プロセスの維持」）に統合された。
       - 3.A – 関連する脅威および戦術/技術/手順の検知は、4.B（「敵対的事象の識別」）の下に統合されました。
       - 1.I – ベンダー/サプライヤーのサイバーセキュリティ要件は、1.D（「サプライチェーン・インシデント報告および脆弱性開示」）に統合された。
   - 理由：
     - これらの独立項目は採用率が低いか、より広範な目的と重複していた。すべての当初の目的は、当初の目標の成果を含め、更新された目標に引き続き存在する。
     - 実世界の使用データと実務者からのフィードバックは、これらの独立項目は混乱を招くか、十分に活用されていないということを示していた。

5. 方法論と文書化の強化

- 変更点：
  - CPGレポートおよびチェックリストに「コスト」、「インパクト」、「実装の容易性」の評価を追加した。
  - v1.0.1の「複雑性」を「実装の容易性」に置き換えた。
  - 各評価の詳細な定義とロジックを追加した。
- 理由：
  - 各スコアの根拠となるロジックを共有することで、CISAは透明性を高め、フレームワークへの信頼を構築し、推測を減らす。
  - 各評価の明確な定義を含めることで、アセッサーがCPGアセスメントを実施する際の分析の一貫性を高め、再現性を向上させることを意図している。

CPGマッピング比較

CPG v1.0.1	現在のバージョン	CPG v2.0
1.A	=	2.A
1.B	=	1.A
1.C	=	1.A
1.D	=	1.A
1.E	=	2.B
1.F	=	2.C
1.G	=	1.D
1.H	=	1.D
1.I	=	削除
2.A	=	3.A
2.B	=	3.B
2.C	=	3.C
2.D	=	3.D
2.E	=	3.G
2.F	=	3.I
2.G	=	3.E
2.H	=	3.F
2.I	=	3.J
2.J	=	3.J
2.K	=	3.K
2.L	=	3.K
2.M	=	3.L
2.N	=	3.M
2.O	=	3.N
2.P	=	2.E
2.Q	=	3.P
2.R	=	3.O
2.S	=	1.C
2.T	=	3.Q
2.U	=	3.Q
2.V	=	3.R
2.W	=	3.S
2.X	=	3.S
3.A	=	削除
4.A	=	5.B
4.B	=	2.D
4.C	=	削除
5.A	=	6.A

CPG v2.0
追加された新たな目標
1.B
1.E
3.H
4.A
4.B
5.A

コスト、インパクト、および実装の容易性に関する更新

CISAは、組織が自らの環境のあらゆる側面に適用できるようにサイバーセキュリティパフォーマンス目標（CPG）を設計した。ただし、コスト、インパクト、実装の容易性に関するガイダンス、特に明示された目標に概説されているものは、主にITインフラに適用されることに留意することが重要である。これは、これらの目標で提示されている考慮事項や推奨事項が、組織内のOTシステムまたはその他の非IT環境に必ずしも適用されるわけではないことを意味する。

<table>
<tr><th colspan="3">コスト</th></tr>
<tr><td>コスト「低」は、組織の年間セキュリティ予算の5%未満である。</td><td>コスト「中」は、組織の年間セキュリティ予算の5%から15%の間である。</td><td>コスト「高」は、組織の年間セキュリティ予算の15%を超える。</td></tr>
<tr><td colspan="3">説明：ケイパビリティ（能力）目標を実装し、維持し、廃棄するために必要な（それを支える資産の）財務的コスト。
• 実装の最初の1年間のコストと、サービスを維持するための2～3年以上の反復コストを考慮する。
• コストをセキュリティ支出に対する割合としてアセスメントする。</td></tr>
<tr><td colspan="3">費用便益分析</td></tr>
<tr><td colspan="3">実施されない可能性のあるCPGについては、費用便益分析（CBA）を実施する。これは、正当化が困難と思われる高額なコスト（$$$）がかかるCPGにとって特に重要である。定量化された便益とコストを比較するCBAは、意思決定者がより客観的に正当な情報を用いてサイバーセキュリティ投資を正当化するのに役立つ可能性がある。
コスト – CPGのライフサイクル全体におけるコスト（ハードウェア、ソフトウェア、労力のレベル（サポート時間））を考慮する。
便益 –回避された潜在的なインパクトを、財務的観点で考慮する。以下に具体的に示す。
• 生産性。ダウンタイムが業務に与える影響と、収益損失などの関連する財務上のインパクトを考慮する。
• 対応。インシデント対応チームの規模、対応に要する時間、および管理レビューの時間を考慮する。
• 交換コスト。既存のソリューションを交換するために必要な新規機器への支出を考慮する。
• その他の要因。必要に応じて、潜在的な競争優位性や有益な評判を考慮する。</td></tr>
</table>

インパクト		
インパクト「**低**」は、組織の業務、資産、または個人への限定的な悪影響を防止する。「限定的な悪影響」とは、組織がミッションを支え続けられる状態を意味する。	インパクト「**中**」は、組織の業務、資産、または個人に対する深刻な悪影響を防止する。「深刻な悪影響」とは、組織がそのミッションの一部を支えられなくなることを意味する。	インパクト「**高**」は、組織の業務、資産、または個人に対する深刻または壊滅的な悪影響を防止する。「深刻または壊滅的な悪影響」とは、組織がそのミッションを支えられなくなることを意味する。
説明：組織、個人、および環境に対する潜在的な危害に対して、ケイパビリティ（能力）目標によって提供される可能性のある防御の程度を測定する指標。 • 提供される防御を、ケイパビリティ（能力）目標によって提供されるより強固なレジリエンスと機密性、完全性、可用性（CIA）の防御による潜在的な損失の低減としてアセスメントする。 • 定性レベルでは、CPGのインパクトの定義は、CPGの影響を受ける関連するCIA要素に対するNISTリスクマネジメントフレームワークのシステム分類（低、中、高）を反映している。 この指標では、組織（例：ミッション、資産、評判）、個人（例：健康、安全）、およびエコシステムに対する従来の（直接的および間接的）損失および危害を考慮する。		
実装の容易性		
「**容易**」なプロジェクト/システムは、最小限の技術的専門知識で数ヶ月以内に実装できる。	「**中**」のプロジェクト/システムは、4～8ヶ月以内に実装可能で、中程度の技術的専門知識または管理者の関与が必要となる。	「**複雑**」なプロジェクト／システムは、一般的に実装するまでに1年近く、あるいはそれ以上の期間を要し、高度な技術的専門知識、調整、および管理層の関与が必要となる。
説明：ケイパビリティ（能力）目標の実装と管理の難易度。 評価（容易、中、複雑）は、CPG の実装と管理がどの程度明確で、実行可能で、かつ合理的に単純であるかをアセスメントする。 CPG を実装するために必要な技術的専門知識と時間の投資のレベルに焦点を当てる。		

統治（GOVERN）

1.A- サイバーセキュリティの責任を確立する

成果

組織のサイバーセキュリティプログラムに関連する役割、責任、権限は、組織内および外部パートナーとの間で確立され、伝達され、実施され、調整される。

対処されるリスク

十分な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。

範囲

経営幹部、重要部門のリーダー、物理およびサイバーセキュリティ人員、外部請負業者、ベンダー、およびサプライヤー。

推奨される行動

サイバーセキュリティに関わる全ての役割と責任は、組織のサイバーセキュリティポリシーに文書化することが望ましい。

サイバーセキュリティポリシーおよびプログラムに関連する役割と責任は、組織全体に分散されている。第三者の請負業者も、これらの活動を支援するために関与することがある。

プライバシーを含むサイバーセキュリティに関する法的および規制上の要件が実装され、管理されていることを確実にする。

OT：プロセスを合理化し、セキュリティ対策を強化し、運用有効性を高めるために、情報技術（IT）チームと制御・運用技術（OT）チームの間で継続的な連携を確立し維持する。

NIST CSF 2.0 参照	コスト	インパクト	実装の容易性
GV.RR-02	低	高	中

その他の NISTの参考文献

SP 800-53 Rev 5: PM-2, PM-13, PM-19, PM-23, PM-24, PM-29
SP 800-82 Rev 3: PS-2

サポートリソース

Cyber Storm National Cybersecurity Exercise
Executive Cybersecurity Leadership

1.B- サイバーセキュリティの監督を管理する

成果

組織のサイバーセキュリティリスクマネジメント戦略、期待、およびポリシーが確立されている。

対処されるリスク

組織の技術およびプロセスのサイバーセキュリティリスクを管理できるサイバーセキュリティポリシーおよび手順/プラクティスが不十分。

範囲

組織全体。

推奨される行動

サイバーセキュリティプログラムを管理するポリシーは、少なくとも年1回レビューし、変更が適用された際には更新する。要件、リスク、脅威、技術、組織のミッションの変化を反映するため、ポリシーを周知し、徹底する。

ポリシーは組織とそのサイバーセキュリティ戦略に基づき策定し、優先順位を周知徹底する。組織ガバナンスには、規制・法的・リスク・環境・運用上の義務を管理するために必要なポリシー、手順、プロセスを含めることが推奨される。

OT：OT固有のポリシーと手順では、既存のITサイバーセキュリティプログラムの制限を考慮して、重要な運用機能、OT固有のセキュリティ上の懸念、および代替管理策の優先順位を識別することが望ましい。

NIST CSF 2.0 参照	コスト	インパクト	実装の容易性
GV.OV-03	低	高	中

その他の NISTの参考文献

SP 800-53 Rev 5: PM-4, PM-6, RA-7, SR-6
SP 800-82 Rev 3: RA-1

サポートリソース

CISA Cybersecurity Awareness Program
Cybersecurity Best Practices

1.C- インシデント対応計画を維持する

成果

サイバーセキュリティおよびインシデント対応 (IR) 計画を実践することによって改善点を識別し、組織のサイバーセキュリティプログラムを維持し、更新する。

対処されるリスク

サイバーセキュリティインシデントについて迅速かつ効果的な隔離、封じ込め、根絶、修復、コミュニケーションができない。

範囲

組織全体。

推奨される行動

組織は、一般的かつ組織固有（分野別、地域別など）の脅威シナリオ、戦術、技術、手順（TTP）に関するIR計画を策定、維持、更新し、定期的に訓練を実施する。訓練は現実的で、関連するすべてのステークホルダーが含まれていることを確実にする。IR計画は、少なくとも年1回、見直しと訓練を実施することが望ましい。

OT：OTのIR計画は、既存のIT計画や優先事項とは異なり、固有の安全および封じ込めに関する考慮事項を考慮する。

NIST CSF 2.0 参照

ID.IM-02, ID.IM-04

その他の NISTの参考文献

SP 800-53 Rev 5: AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, CP-2, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PM-1, PS-1, PT-1, RA-1, SA-1, SC-1, SI-1, SR-1, SR-2, CA-2, CA-5, CA-7, CA-8, CP-2, CP-4, IR-3, IR-4, IR-8, PL-2, PM-4, PM-31, RA-3, RA-5, RA-7, SA-8, SA-11, SI-2, SI-4, SR-5
SP 800-82 Rev 3: CA-2, CA-5, CP-1, CP-2, CP-4, CP-10, IR-1, IR-8, SA-11, RA-3, SR-6

コスト	インパクト	実装の容易性
低	高	中

サポートリソース

CISA Tabletop Exercise Packages
Incident Response Plan (IRP) Basics
Critical Infrastructure Exercises Support
Develop an Incident Response Capability

1.D- サプライチェーン・インシデントの報告と脆弱性開示

成果

組織はベンダーやサービスプロバイダー全体にわたる既知のインシデントまたは侵害について、より迅速に学習し、対応する。

対処されるリスク

組織の技術とプロセスをセキュアにサポートできない、不十分な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（C-SCRM）のプラクティス。

範囲

サードパーティーベンダーおよびサービスプロバイダー。

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、ベンダーおよび／またはサービスプロバイダーが、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。

OT：OT資産を保有する組織は、シリアル番号、チェックサム、デジタル証明書／署名、またはベンダーが提供するOTハードウェア、ソフトウェア、およびファームウェアの真正性を検証できるその他の識別機能を文書化し追跡する必要がある。

NIST CSF 2.0 参照

GV.SC-01, GV.SC-05

その他の NISTの参考文献

SP 800-53 Rev 5: SA-4, SA-9, PM-30, SR-2, SR-3, SR-5, SR-6, SR-10
P 800-82 Rev 3: PL-1

コスト	インパクト	実装の容易性
中	中	複雑

サポートリソース

Information and Communications Technology Supply Chain Security
Supply Chain Risk Management (SCRM) in a Connected World

マネージドサービスプロバイダーからのリスクを管理する

成果

マネージドサービスプロバイダー（MSP）によってもたらされるリスクは、関係が継続する過程において、識別され、記録され、評価され、優先順位付けされ、監視され、更新される。

対処されるリスク

敵対者は、信頼されたサードパーティーとの関係を悪用することで、脆弱性を悪用することができる。

範囲

組織のITおよび/またはOTインフラ、サイバーセキュリティプロセス、および/またはその他の関連業務を遠隔で管理するサービスプロバイダー。

推奨される行動

MSPが提供するセキュリティ製品を含むサービスについての理解を深め、維持する。契約上の合意を理解し、契約の範囲外にあるセキュリティ上のギャップに積極的に対処する。例えば、契約において、MSPが顧客の環境に影響を与えるインシデントをいつどのように顧客に通知するかを詳述することが望ましい。

NIST CSF 2.0 参照

GV.SC-07

コスト	インパクト	実装の容易性
中	中	複雑

その他の NISTの参考文献

SP 800-53 Rev 5: RA-9, SA-4, SA-9, SR-3, SR-6
SP 800-82 Rev 3: RA-9, SA-4, SR-1, SR-2, SR-3, SR-6

サポートリソース

Information and Communications Technology Supply Chain Security
Supply Chain Risk Management (SCRM) in a Connected World

識別（IDENTIFY）

2.A- 組織の資産を管理する

成果	推奨される行動
ダウンタイムの削減、復旧の支援、防御の強化、および準備の改善によってサイバーセキュリティのレジリエンスを向上させるために維持された資産インベントリ。	組織のすべての資産（データ、ハードウェア、ソフトウェア、システム、施設、人員など）の定期的に更新されたインベントリを維持する。 ビジネスまたは運用機能にとって重要であると判断されたITおよびOT資産は、より頻繁に更新することが望ましい。

対処されるリスク	範囲
敵対者は、コンピュータ周辺機器、ネットワークハードウェア、またはその他のデバイスを、システムまたはネットワークに侵入するためのエントリポイントとして使用する可能性がある。	データ、ハードウェア、ソフトウェア、システム、施設、人員。

NIST CSF 2.0 参照	コスト	インパクト	実装の容易性
ID.AM-01	低	高	中

その他の NISTの参考文献	サポートリソース
SP 800-53 Rev 5: CM-8, PM-5 **SP 800-82 Rev 3**: CM-8	Asset Inventory for OT Asset Management CISA Insights: Secure High Value Assets (HVAs)

2.B- 既知の脆弱性を緩和する

成果	推奨される行動
脅威アクター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が低減する。	脆弱性管理プログラムを実装し、設定ミスのあるソフトウェアにタイムリーにパッチを適用し、軽減する。 行動計画およびマイルストーン（POA&M）、リスク登録簿、およびリスク詳細レポートなどのツールを通じて、リスク対応の進捗状況を監視する。 提案された変更の潜在的なリスクを文書化し、ロールバックのガイダンスを提供する。様々なステークホルダーからのサイバーセキュリティ脅威、脆弱性、またはインシデント開示の処理および対応するための責任を割り当て、手順が順守されていることを確実にする。可能であれば、レガシーシステムに対応するために、補完的なセキュリティ管理策（多層防御など）を組み込む。 OT：パッチ適用が不可能、あるいは可用性または安全性を著しく侵害する可能性がある資産については、代替管理策（セグメンテーション、監視など）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、脅威アクターがこれらの資産の脆弱性を悪用する能力が低下する。

対処されるリスク	範囲
敵対者は、パッチが適用されていないシステムや設定ミスがあるシステム、特にインターネットに公開されているシステムを標的にすることが多い。敵対者は、ソフトウェアの脆弱性、一時的な誤動作、設定エラーを悪用してネットワークへの最初のアクセスを得ることがよくある。	インターネットに面しているものも含む、組織のすべての資産。

NIST CSF 2.0 参照	コスト	インパクト	実装の容易性
ID.RA-01, ID.RA-06, ID.RA-08	高	高	複雑

その他の NISTの参考文献	サポートリソース
SP 800-53 Rev 5: CA-2, CA-7, CA-8, PM-9, PM-18, PM-30, RA-3, RA-5, RA-7, SA-11(02), SA-15(07), SA-15(08), SI-4, SI-5 **SP 800-82 Rev 3**: CA-1, CA-2, CA-5, RA-3, RA-7, SA-11, SI-2, SI-3, SI-5	Known Exploited Vulnerabilities Catalog CISA Cyber Hygiene Services Think Twice Before Putting Off Updates! Understanding Patches and Software Updates ICS Recommended Practices

2.C- サイバーセキュリティ管理策の独立した妥当性確認を得る

成果

実装されたセキュリティ管理策が適切に構成され、意図した通りに機能していることの妥当性を確認する。

対処されるリスク

サイバー防御のギャップ、または既存の防御策に対する過信によるリスクを削減する。

範囲

組織の資産およびネットワーク。

推奨される行動

組織は定期的にサードパーティーのサイバーセキュリティ専門家を起用して、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、および机上演習などの様々な演習を通じて、防御の妥当性を確認する。これらのテストは、告知のあり・なし共に、重要なシステムを標的として、ネットワーク内に侵入して横方向に移動する敵対者の能力をアセスメントする。これらのテストの結果に確実に対処する。

NIST CSF 2.0 参照	コスト	インパクト	実装の容易性
ID.RA-01, ID.RA-03	高	高	複雑

その他の NISTの参考文献

SP 800-53 Rev 5: CA-2, CA-7, CA-8, PM-12, PM-16, RA-3, RA-5, SA-11(02), SA-15(07), SA-15(08), SI-4, SI-5
SP 800-82 Rev 3: AT-2(2), CA-1, CA-2, CA-5, RA-3, SA-11, SI-2, SI-3, SI-5

サポートリソース

CISA Cyber Hygiene Services
Cybersecurity Performance Goals (CPG) Assessment Training
Risk and Vulnerability Assessments

2.D- 脆弱性開示／報告のプロセスを維持する

成果

組織は、脆弱性または弱点についてより迅速に学ぶ。

対処されるリスク

企業のソフトウェア、ネットワーク、デバイス、およびシステムの既知のセキュリティ脆弱性を、組織に直接報告することで、敵対者が悪用する前に、組織はこれらの脆弱性に対処し軽減することができる。

範囲

すべての公開された資産およびWebドメイン

推奨される行動

組織は、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、個々人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個人は、セーフ・ハーバー・ルール（safe harbor rules）の下で保護される。セーフ・ハーバー・ルールは、特定の条件下で個人またはエンティティを罰則から保護する法律の規定である。

RFC 9116の推奨事項に準拠するSecurity.txtファイルは、脆弱性通知を効率化するために一般的に使用される標準の1つである。これは、すべての公開されたウェブドメインに適用されることが望ましい。

NIST CSF 2.0 参照	コスト	インパクト	実装の容易性
ID.RA-08	低	低	中

その他の NISTの参考文献

SP 800-53 Rev 5: RA-5
SP 800-82 Rev 3: RA-5, SI-2, SI-3, SI-5

サポートリソース

CISA Coordinated Vulnerability Disclosure Program
Vulnerability Disclosure Policy Template
security.txt: A Simple File with Big Value

2.E- ネットワークトポロジーを文書化する

成果

インシデントに対応し、サービスの継続性をより効率的かつ効果的に維持する。

対処されるリスク

ネットワークトポロジーの理解が不完全または不正確であると、効果的なインシデント対応と復旧が妨げられる。

範囲

組織のネットワーク。

推奨される行動

組織は、すべてのITおよびOTネットワークにわたって、現在のネットワークトポロジーと関連情報を記述した正確な文書を維持する。ネットワークのレビューは年次ベースで実施および追跡し、ネットワークトポロジーに変更があった際には文書を更新することが望ましい。

NIST CSF 2.0 参照	コスト	インパクト	実装の容易性
PR.PS-01, ID.AM-03	低	高	中

その他の NISTの参考文献

SP 800-53 Rev 5: CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-8, CM-9, CM-10, CM-11
SP 800-82 Rev 3: CM-1, CM-9

サポートリソース

Introduction to Network Diagramming
Cybersecurity Best Practices for Smart Cities

3.A- デフォルトのパスワードを変更する

成果

脅威アクターがデフォルトのパスワードを使用してネットワークへの初期アクセスを達成し、横方向に移動することを防止する。

推奨される行動

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を内部または外部のネットワークに接続する前に、デフォルトのメーカーのパスワードを変更することを義務づける組織全体のポリシーを実装する。これには、OT管理用Webページなど、OTで使用されるIT資産も含まれる。

デフォルトのパスワードの変更が不可能な場合（例えば、制御システムにハードコードされたパスワード）、適切な補完的なセキュリティ管理策を文書化して実装し、これらのデバイスにおける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：既存のOTシステムのデフォルトのパスワードを変更し、すべての新規または将来のデバイスのデフォルトの認証情報を変更するためのポリシーを確立する。これにより、脆弱性が変化した場合の潜在的リスクが低減される。

対処されるリスク

敵対者が、初期アクセス獲得、永続性の維持、特権の昇格、または防御の回避のために、デフォルトアカウントの認証情報を取得し、悪用する可能性がある。

範囲

パスワードで保護された新たに取得した、およびレガシーのIT・OT資産

NIST CSF 2.0 参照	コスト	インパクト	実装の容易性
PR.AA-01	低	高	容易

その他の NISTの参考文献

SP 800-53 Rev 5: AC-1, AC-2, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
SP 800-82 Rev 3: IA-2, IA-3, IA-8

サポートリソース

How Manufacturers Can Protect Customers by Eliminating Default Passwords
Risks of Default Passwords on the Internet

3.B- 最低限のパスワード強度を定める

成果

組織のパスワードは、脅威アクターが推測する、または解読することが困難である。

推奨される行動

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、16文字以上のパスワード長を含む最低限のパスワード強度を定める、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、代替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。

対処されるリスク

敵対者は、パスワードが不明な場合、またはハッシュ値を取得した場合、ブルートフォース（総当たり）手法を使用してパスワードを解読する。敵対者は、サービスとやり取りして認証情報の妥当性を確認するか、取得したデータを使ってオフラインで作業することで、反復的な手法を使用して体系的にパスワードを推測する。

範囲

ユーザーアカウントのパスワード。

NIST CSF 2.0 参照	コスト	インパクト	実装の容易性
PR.AA-01	低	高	容易

その他の NISTの参考文献

SP 800-53 Rev 5: AC-1, AC-2, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
SP 800-82 Rev 3: IA-2, IA-3, IA-8

サポートリソース

Use Strong Passwords
Require Strong Passwords

3.C- 一意の認証情報を生成する

成果

敵対者は、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

対処されるリスク

敵対者は、アカウントの認証情報を取得して悪用することで、アクセス権の取得、永続性の維持、特権の昇格、または防御の回避が可能となる、これらの認証情報は、ネットワークアクセス制御を回避し、リモートシステムおよび外部サービスへの継続的なアクセスを可能にする。

範囲

ユーザーアカウント。

推奨される行動

組織は、ITおよびOTネットワークとOTネットワークにまたがる類似のサービスおよび資産へのアクセスに対して、それぞれ異なる認証情報を作成する。ユーザーは、アカウント、アプリケーション、およびサービスでパスワードを再利用しない。さらに、システム管理者/マシンアカウントは、通常のユーザーアカウントとは異なる一意のパスワード認証情報を持つ。汎用的な非人間エンティティ（NPE）アカウントのパスワードは配布しないことが望ましい。NPEデバイスを使用する場合は、それぞれに異なるパスワードを利用する。可能な限り、ITシステムおよびOTシステムには、役割ベースのアカウントを利用する。

NIST CSF 2.0 参照	コスト	インパクト	実装の容易性
PR.AA-01	低	高	容易

その他の NISTの参考文献

SP 800-53 Rev 5: AC-1, AC-2, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
SP 800-82 Rev 3: IA-2, IA-3, IA-8

サポートリソース

Cyb3R_Sm@rT!: Use a Password Manager
Using Rigorous Credential Control

3.D- 離職する従業員の認証情報を無効化する

成果

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。

対処されるリスク

敵対者は、検知を回避するために、元従業員の非アクティブなアカウントを悪用できる。

範囲

離職する従業員（請負業者、ベンダーなどを含む場合がある）

推奨される行動

組織は、従業員（例えば、社員、請負業者、ベンダー）を離職させるための明確な管理プロセスを定め、実施することが望ましい。このプロセスには、すべての物理的なトークンおよび/またはバッジの返却、ならびにシステムおよび施設へのすべてのアクセスの取り消しが含まれることが望ましい。

ユーザーアクセスをレビューし、一定期間（例えば、30日間）非アクティブなアカウントを無効化する。理想的には、このレビューは自動化されたプロセス、およびスクリプトまたはプラットフォームの機能を通じて実装された事前に設定されたポリシーを用いて実施する。

NIST CSF 2.0 参照	コスト	インパクト	実装の容易性
PR.AA-01	低	高	中

その他の NISTの参考文献

SP 800-53 Rev 5: AC-1, AC-2, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
SP 800-82 Rev 3: IA-2, IA-3, IA-8

サポートリソース

Managing Risk of Adverse/Involuntary Employee Separations

3.E- 失敗した（自動化された）ログイン試行を監視する

成果

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。

対処されるリスク

敵対者は、デフォルトのアカウント認証情報を取得し悪用して、アクセス権を獲得したり、永続性を維持したり、特権を昇格したり、防御を回避したりする可能性がある。

範囲

パスワードで保護された、新たに取得した、およびレガシーのITおよびOT資産。

推奨される行動

組織のセキュリティポリシーに従い、すべての失敗したログインを補足しログに記録する。短時間に特定の回数連続してログイン試行に失敗した場合、および通常のユーザー行動から逸脱した場合、セキュリティ担当者に（例えば、アラートによって）通知される。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される。

NIST CSF 2.0 参照	コスト	インパクト	実装の容易性
PR.AA-01	中	高	中

その他の NISTの参考文献

SP 800-53 Rev 5: AC-1, AC-2, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
SP 800-82 Rev 3: IA-2, IA-3, IA-8

サポートリソース

Stop Ransomware Guide
Brute Force Attacks Conducted by Cyber Actors

3.F- 多要素認証（MFA）を実装する

成果

資産アカウントを保護するために、重要な追加のセキュリティレイヤを追加する。

対処されるリスク

正当な認証情報を事前に知らない敵対者は、様々なアカウントでよく使われるパスワードを試して、アクセスしようとする可能性がある。また、反復的な手法を用いて体系的にパスワードを推測する可能性もある。

範囲

ワークステーションおよびヒューマンマシンインターフェース（HMI）など、安全かつ技術的に実行可能なリモートアクセスを備えた組織資産。

推奨される行動

組織は、その資産にMFAを利用可能な場合、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に、MFAを要件とする。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. フィッシング耐性のあるMFA（例えば、FIDO/WebAuthnまたは公開鍵暗号基盤（PKI）ベース- 「サポートリソース」のCISAガイダンス参照）。
2. フィッシング耐性のある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）。
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システムの特権的な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：ベンダー／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（利用可能な場合）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を有効化する。MFAが利用できない場合は、リモートアクセスを削除し、追加のセグメント化手順を導入し、認証情報管理を優先する。

NIST CSF 2.0 参照	コスト	インパクト	実装の容易性
PR.AA-03	中	高	中

その他の NISTの参考文献

SP 800-53 Rev 5: AC-7, AC-12, IA-2, IA-3, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11
SP 800-82 Rev 3: IA-2, IA-3, IA-8

サポートリソース

Implementing Phishing-Resistant MFA
Protect Our World with MFA

3.G- 管理者がユーザーアカウントと特権アカウントの分離を維持する

成果

一般的なユーザーアカウントが侵害された場合でも、脅威アクター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。

対処されるリスク

敵対者は、初期アクセス、永続化、特権の昇格、または防御回避のために、既存のアカウントの認証情報を得て悪用する可能性がある。これらの侵害された認証情報は、ネットワークアクセス制御を回避し、リモートシステムおよび外部サービスへの継続的なアクセスを提供することができる。

範囲

安全かつ技術的に実行可能な組織資産。

推奨される行動

ユーザーアカウントには、管理者権限がない。管理者は、ビジネスメールおよびウェブ閲覧など、管理者の役割とは関係のない活動のために、別のユーザーアカウントを保持している。権限は、定期的に再評価し、与えられた権限の継続的な必要性の妥当性を確認する。

職務の分離は、複数の個人または役割に責任を分散することで維持され、不正な行動、エラー、または詐欺のリスクを低減する。

NIST CSF 2.0 参照

PR.AA-05

コスト	インパクト	実装の容易性
低	高	容易

その他の NISTの参考文献

SP 800-53 Rev 5: AC-1, AC-2, AC-3, AC-5, AC-6, AC-10, AC-16, AC-17, AC-18, AC-19, AC-24, IA-13
SP 800-82 Rev 3: AC-1, AC-5, AC-6, IA-1, IA-2, IA-3, IA-8, PS-2

サポートリソース

Top Ten Cybersecurity Misconfigurations
Enhancing Cyber Resilience: Insights from CISA Red Team
NIST - Separation of Duty

3.H- 最小特権の原則を実装する

成果

システム、データ、およびプロセスへの不正アクセスを最小限に抑え、人的エラーを減らし、悪意のある行為を防ぐ。これにより、組織の機密情報および重要な資産を確実に防御する。

対処されるリスク

ネットワークリソースへの不正アクセスおよび敵対者が検知されずにシステム間を移動し、機密データおよび重要なシステムを侵害する可能性。

範囲

すべての組織アカウント。

推奨される行動

すべてのユーザーアカウント、システムの役割、およびプロセスは、そのタスクを実行するために必要な最小限の権限で動作する。

アクセス権限および役割の割り当てを四半期ごとにレビューし、確立されたポリシーへの準拠を確認する。

コスト	インパクト	実装の容易性
低	高	容易

NIST CSF 2.0 参照

PR.AA-05

その他の NISTの参考文献

SP 800-53 Rev 5: AC-5, AC-6, SA-8(14), SA-17(7), SC-3
SP 800-82 Rev 3: AC-5, AC-6

サポートリソース

Weak Security Controls and Practices Routinely Exploited
Enhanced Visibility and Hardening Guidance
Principle of Least Privilege

3.I- 論理的／物理的ネットワークセグメンテーションを実装する

成果

潜在的な侵害のインパクトを制限し、敵対者が機密データ、空間、および/または重要インフラへのアクセスを防止する。

対処されるリスク

ネットワークが不正なユーザーによって侵害された場合、セキュアに分離されたネットワークは悪意のある出来事を封じ込めることができる。

範囲

安全かつ技術的に実行可能な組織資産。

推奨される行動

ルーターはネットワーク間に設置され、境界を作成し、ブロードキャスティングドメインの数を増やし、ユーザーのブロードキャスティングトラフィックを効果的にフィルタリングする。
これらの境界は、トラフィックを別々のセグメントに制限することによってセキュリティ侵害を封じ込めるために使用でき、敵対者が侵入中にネットワークのセグメントをシャットダウンして、敵対者のアクセスを制限することもできる。
OT：適用可能な場合、OTエンクレーブを物理的にセグメント化する（例えば、データダイオード）。

NIST CSF 2.0 参照

PR.IR-01, DE.CM-01

コスト	インパクト	実装の容易性
高	高	複雑

その他の NISTの参考文献

SP 800-53 Rev 5: AC-2, AC-3, AC-4, AU-12, CA-7, CM-3, SC-4, SC-5, SC-7, SI-4
SP 800-82 Rev 3: AU-1, AU-2, SA-8, SC-1, SC-7(18), SI-1, SI-4, PL-8

サポートリソース

Layering Network Security Through Segmentation

3.J- サイバーセキュリティトレーニングを実施する

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。

対処されるリスク

スピアフィッシング、ソーシャルエンジニアリング、およびユーザーとのやり取りを伴うその他の手法が成功してしまうリスクを軽減するために、敵対者によるアクセスまたは操作の試みを認識するようユーザーをトレーニングする。

範囲

組織の非公開リソースの、すべての従業員、請負業者、パートナー、サプライヤー、プロバイダー、およびその他のユーザー。

推奨される行動

新入社員はコンピュータシステムにアクセスする前に、最初のサイバーセキュリティトレーニングを受ける。

すべての組織ユーザーに対して、少なくとも年1回のサイバーセキュリティトレーニングを提供し、ソーシャルエンジニアリングの試み、およびその他の一般的な攻撃の認識、攻撃および疑わしい行動の報告、利用規定の順守、および基本的なサイバー衛生タスク（例えば、パスワードの選択、認証情報の保護）の実施についてトレーニングする。

物理的セキュリティ担当者とサイバーセキュリティ担当者、システム管理者、財務担当者、上級管理職、および業務上重要なデータにアクセスする者など、組織内の専門的な役割を識別する。請負業者、パートナー、サプライヤー、およびその他のサードパーティーを含む、専門的な役割を持つすべての人に、役割ベースのサイバーセキュリティトレーニングを提供する。

OT：担当者は、OT環境向けのセキュリティ意識向上およびトレーニングを受けることが望ましい。さらに、組織は重要なOTの役割と責任を担うすべての人員を識別し、文書化し、トレーニングすることが望ましい。

NIST CSF 2.0 参照

PR.AT-01, PR.AT-02

コスト	インパクト	実装の容易性
低	高	中

その他の NISTの参考文献

SP 800-53 Rev 5: AT-2, AT-3
SP 800-82 Rev 3: AT-2, AT-3

サポートリソース

CISA Training
Cybersecurity Training & Exercises

3.K- 強力な暗号化を活用する

成果

暗号化が、組織のネットワーク全体で機密データの機密性と完全性を維持し、不正アクセスから防御するために導入されている。

対処されるリスク

敵対者は、ネットワークに接続されたデバイスの間に自らを配置して、ネットワークのスニッフィングおよびデータ操作を実行したり、個人的な利益または将来の作戦のために環境から運用データを窃取したりすることができる。

範囲

パスワード、認証情報、秘密、およびその他の機密情報、または管理された情報。

推奨される行動

暗号化、デジタル署名、および暗号学的ハッシュを使用して、ネットワーク通信の機密性と完全性を防御する。

転送中および保存中に保護する重要な電子ファイルの種類およびデータを識別する。これには、個人情報および機密情報、専有情報または企業秘密情報（例えば、PLCプログラムコード、ロボットプログラム、CAD（コンピュータ支援設計）またはCAM（コンピュータ支援製造）ファイル、操作マニュアルおよび文書、電気回路図、ネットワーク図、生産履歴データ）が含まれる場合がある。

パスワードを含む機密データは、組織内のいかなる場所にも平文で電子保存されず、認可されたユーザーおよび認証されたユーザーのみがアクセスできる。認証情報は、認証情報／パスワードマネージャーなどのセキュアな方法で保存される。

OT：外部接続および遅延の問題が運用にインパクトを与えない場合は、暗号化を使用する。

NIST CSF 2.0 参照	コスト	インパクト	実装の容易性
PR.DS-01, PR.DS-02, PR.DS-10	中	高	複雑

その他の NISTの参考文献

SP 800-53 Rev 5: AC-2, AC-3, AC-4, AU-9, AU-13, AU-16, CA-3, CP-9, MP-8, SA-8, SC-4, SC-7, SC-8, SC-11, SC-12, SC-13, SC-16, SC-24, SC-28, SC-32, SC-39, SC-40, SC-43, SI-3, SI-4, SI-7, SI-10, SI-16
SP 800-82 Rev 3: AC-6, CM-2, CM-6, MP-1, PL-10, SA-8, SC-8, SC-13, SC-28

サポートリソース

How to Protect the Data that is Stored on Your Devices

3.L- 電子メールのセキュリティを有効化する

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によるリスクを軽減する。

対処されるリスク

敵対者は、被害者のシステムで有害なコードを実行することを目的として、悪意のある添付ファイルまたはリンクを含む電子メールを被害者に送る可能性がある。また、ソーシャルメディアプラットフォームなどのサードパーティーサービスを介して、フィッシングを実行することもできる。

範囲

組織のすべて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で、(1) STARTTLSが有効化されている、（2）送信者ポリシーフレームワーク（SPF）およびDKIM送信ドメイン認証が有効化されている、（3）ドメインに基づくメッセージ認証、レポート、および適合性（DMARC）が有効化され、「拒否」に設定されている。

NIST CSF 2.0 参照	コスト	インパクト	実装の容易性
PR.DS-01, PR.DS-02, PR.DS-10	低	高	中

その他の NISTの参考文献

SP 800-53 Rev 5: AC-2, AC-3, AC-4, AU-9, AU-13, AU-16, CA-3, CP-9, MP-8, SA-8, SC-4, SC-7, SC-8, SC-11, SC-12, SC-13, SC-16, SC-24, SC-28, SC-32, SC-39, SC-40, SC-43, SI-3, SI-4, SI-7, SI-10, SI-16
SP 800-82 Rev 3: AC-6, CM-2, CM-6, MP-1, PL-10, SA-8, SC-8, SC-13, SC-28

サポートリソース

BOD 18-01: Enhance Email and Web Security
CISA Insights - Enhance Email & Web Security

3.M- 自動実行＆マクロをデフォルトで無効にする

成果

埋め込みマクロや同様の実行可能コードからのリスクを減らす。

対処されるリスク

敵対者は、ユーザーが悪意のあるファイルを開いてコードを実行することに依存している。ユーザーにそのようなファイルを開かせるよう仕向けるために、ソーシャルエンジニアリングの手法が使われる可能性がある。

範囲

すべての組織資産。

推奨される行動

コードまたはアプリケーションの自動実行を防止するために、すべてのデバイスでマクロ、または同様の埋め込みコードをデフォルトで無効にするシステム強制ポリシー。

特定の状況でマクロを有効にする必要がある場合、認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に要求するためのポリシーを確立する。

USBまたは光学ドライブなどのソースからの意図しないコード実行を防ぐため、自動実行またはオートプレイもデフォルトで無効化することが望ましい。

NIST CSF 2.0 参照	コスト	インパクト	実装の容易性
PR.PS-01, ID.RA-07	低	中	容易

その他の NISTの参考文献

SP 800-53 Rev 5: CA-7, CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-8, CM-9, CM-10, CM-11
SP 800-82 Rev 3: CM-1, CM-3, CM-4, CM-5, CM-9

サポートリソース

Using Caution with USB Drives
Disable AutoRun Properly

3.N- 変更管理プロセスを確立する

成果

システム変更と構成を管理するためのポリシーおよび手順が存在する。

対処されるリスク

重要なデバイスおよびサービス運用の機能を維持または復旧する能力の遅延、不十分または不完全。

範囲

組織の資産。

推奨される行動

技術プラットフォーム向けのセキュアな変更管理を策定、文書化、維持するためのポリシー及びプロセスを実装し、不正な変更を防止するための構成制限を適用する。

技術的な構成変更管理プロセスが実施され、承認されない限り、不正な変更を禁止する。提案された変更を非本番環境でテストおよび文書化し、実装前に潜在的インパクトを分析する。

OT：OT運用に必要な特定の機能、プロトコル、およびサービスのみを許可することで、機能制限を実施する。

NIST CSF 2.0 参照	コスト	インパクト	実装の容易性
PR.PS-01, PR.PS-02, PR.PS-03	中	高	複雑

その他の NISTの参考文献

SP 800-53 Rev 5: CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-8, CM-9, CM-10, CM-11, MA-3(06), SA-10(01), SA-10(03), SI-2, SI-7, SC-03(01), SC-39(01), SC-49, SC-51
SP 800-82 Rev 3: CM-1, CM-9, MA-1, MA-2, MA-6, SA-3, SA-22, SI-2, SI-3

サポートリソース

Configuration and Change Management
Importance of Configuration and Change Management to Security

3.O- システムのバックアップと復元能力を維持する

成果

組織はデータ損失およびサービス中断のリスクを低減しつつ、継続的なサービス提供を維持するために、インシデントを効率的に管理、対応、復旧する。

対処されるリスク

敵対者は、重要なシステムを妨害し、製品またはサービスの提供を停止することができる。敵対者はデータを削除し、復旧サービスを無効化することで、システムの復旧を妨げることができる。敵対者は、破損したシステムの復旧を支援するために設計されたサービスを停止させるかもしれない。

範囲

事業運営に必要な組織資産。

NIST CSF 2.0 参照

PR.IR-01, DE.CM-01

その他の NISTの参考文献

SP 800-53 Rev 5: AC-2, AC-3, AC-4, AU-12, CA-7, CM-3, SC-4, SC-5, SC-7, SI-4
SP 800-82 Rev 3: AU-1, AU-2, SA-8, SC-1, SC-7(18), SI-1, SI-4, PL-8

推奨される行動

インストールメディア、ライセンスキー、構成情報、および情報のバックアップ保存期間を含む、維持されているすべてのバックアップのリストを策定する。

重要な業務システムはほぼリアルタイムでバックアップし、組織のニーズに合致した定期的なスケジュールで、業務に必要な全システムを頻繁にバックアップする。

バックアップは、オフサイトかつオフラインで、セキュアに保管する。バックアップと復旧は、定期的にテストする。少なくとも年1回は実施する。

復元を開始する前に、復元対象のバックアップおよびその他の資産の完全性を検証する。この検証プロセスでは、データが完全かつ正確で信頼性があることを確実にし、復元プロセス中データ破損のリスクを最小限に抑える。

復元資産を使用する前に、侵害の痕跡、ファイル破損、およびその他の完全性の問題がないか確認する。バックアップ情報を定期的にテストし、メディアの信頼性及び情報の完全性を検証する。

OT：OT資産の保存情報には、少なくともデバイス構成、役割、設計図面、およびツールが含まれる、

コスト	インパクト	実装の容易性
高	高	中

サポートリソース

CISA Stop Ransomware Guide
Cyber Guidance for Small Businesses

3.P- ハードウェアとソフトウェアの承認プロセスを維持する

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る侵害の可能性を低減する、

対処されるリスク

敵対者は、製品または配信メカニズムを、最終ユーザーに届く前に操作し、データまたはシステムの侵害を試みることができる。敵対者は、産業用制御システムおよび生産ネットワークを横断するデバイスを標的にすることができる。

範囲

組織資産。

NIST CSF 2.0 参照

PR.PS-02, PR.PS-03, ID.RA-07

その他の NISTの参考文献

SP 800-53 Rev 5: CA-7, CM-3, CM-4, CM-7(09), CM-11, MA-3(06), SA-10(01), SC-3(01), SC-39(01), SC-49, SC-51, SI-2, SI-7
SP 800-82 Rev 3: CM-3, CM-4, CM-5, MA-1, MA-2, MA-6, SA-3, SA-22, SI-2, SI-3

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をインストールまたは展開する前に、レビュー、テスト、および承認を義務付ける管理ポリシーおよび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、およびそふぃとウェアのリストを維持する。

OT：パッチおよび更新を展開する際には、OT環境を持つ組織の追加要件を考慮する。これには、運用能力または安全性に影響を与えないことを確実にするためのテストおよび妥当性確認が含まれる。

コスト	インパクト	実装の容易性
中	高	中

サポートリソース

Securing the Software Supply Chain

3.Q- ログ収集および保管を維持する

成果

セキュリティログを不正アクセスおよび改ざんから防御されていることを確実にしながら、サイバーインシデントを検知し、対応するために強化された可視性。

対処されるリスク

潜在的なサイバーインシデントを検知し対応する能力の遅れ、不足、または不完全さ。

範囲

安全かつ技術的に実現可能な場合、すべての資産における組織資産。

推奨される行動

管理およびセキュリティ関連のログ（例えば、オペレーティングシステム、アプリケーション、およびサービス；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）は、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および保存する。

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および認証されたユーザーのみがアクセスまたは変更できる。ログは、リスクまたは関連する規制ガイドラインによって通知された期間保存される。

重要なログ期のが無効化されると、セキュリティチームに通知される。

OT：ログが非標準または使用できないOT資産については、当該資産と他の資産間のネットワークトラフィックおよび通信が収集される。

NIST CSF 2.0 参照	コスト	インパクト	実装の容易性
PR.PS-04	中	高	中

その他の NISTの参考文献

SP 800-53 Rev 5: AU-2, AU-3, AU-6, AU-7, AU-11, AU-12
SP 800-82 Rev 3: AU-1, AU-3, SI-4

サポートリソース

Best Practices for Event Logging and Threat Detection
Guide to Computer Security Log Management
Improving Investigative and Remediation Capabilities

3.R- 不正な機器の接続を禁止する

成果

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

対処されるリスク

敵対者は、USBドライブなどのリムーバブルメディアにマルウェアをコピーすることで、切断されたネットワークまたはエアギャップネットワークを含むシステムに侵入する可能性がある。

範囲

組織資産。

推奨される行動

組織は、USBデバイスおよびリムーバブルメディアの私用を制限するなど、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。

NIST CSF 2.0 参照	コスト	インパクト	実装の容易性
PR.DS-01	中	高	複雑

その他の NISTの参考文献

SP 800-53 Rev 5: CA-3, CP-9, MP-8, SC-4, SC-7, SC-12, SC-13, SC-28, SC-32, SC-39, SC-43, SI-3, SI-4, SI-7
SP 800-82 Rev 3: MP-1, SC-8(1), SC-13, SC-28

サポートリソース

Using Caution with USB Drives
Proposed Security Requirements for Restricted Transactions

3.S-

インターネットに面したデバイスをセキュアにする

成果

不正なユーザーは、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。

推奨される行動

可能な限り、インターネットに面した資産を最小限に抑える。ソフトウェアを最新の状態に保つことを優先し、タイムリーなパッチ適用と更新を実施する。更新を適用できない場合は、その資産の削除を検討するか、一般的な形式の悪用を防ぐための代替管理策を実装する。これらの管理策には、ネットワークセグメンテーションまたはファイアウォールが含まれる場合がある。

ミッションクリティカルなアプリケーションに必要でない、すべてのオペレーティングシステムアプリケーション、ソフトウェアおよびネットワークプロトコルは、インターネットに面した資産上で無効化する。

ネットワーク管理インターフェース（NMI）は、公衆インターネットに公開しないようにし、事業体ネットワーク内からのみアクセス可能とすることが望ましい。

信頼境界とプラットフォームの種類（例えば、IT、IoT、OT、モバイル、ゲスト）に基づき、クラウドベースのプラットフォームを含む事業体ネットワークと生産ネットワークを論理的にセグメント化し、セグメント間の通信は必要なもののみ許可する。

対処されるリスク

敵対者は、ソフトウェアのバグ、一時的な不具合、又は設定ミスを標的にして、インターネットに面したホストまたはシステムの弱点を悪用し、最初のネットワークアクセスを得る可能性がある。

範囲

公衆インターネット上の組織資産。

NIST CSF 2.0 参照

PR.IR-01

コスト	インパクト	実装の容易性
中	高	複雑

その他の NISTの参考文献

SP 800-53 Rev 5: AC-3, AC-4, SC-4, SC-5, SC-7
SP 800-82 Rev3: PL-8, SA-8, SC-1, SC-7(18), SI-1

サポートリソース

Remediate Vulnerabilities for Internet-Accessible Systems
Internet Exposure Reduction Guidance
Mitigating the Risk from Internet-Exposed Management Interfaces

検知（DETECT）

4.A- 悪意のあるコードの検知を確立する

成果

脅威の早期識別を可能にし、システムの完全性を強化し、迅速な修復のための知見を提供し、ダウンタイムを最小限に抑える。

対処されるリスク

悪意のあるソフトウェアには、ペイロード、ドロッパー、バックドアなどが含まれる。敵対者はマルウェアを使用して、リモートマシンを制御し、防御を回避し、侵害後の行動を実行する。

範囲

組織全体。

推奨される行動

システムのエンドポイントで悪意のあるコードを検知および根絶するために、シグネチャベースのメカニズム（脅威を識別しブロックするためにアンチウィルスソフトウェアで使用される既知のパターンまたは悪意のあるコードのシグネチャに依存しているもの）および非シグネチャベースのメカニズム（動作、ヒューリスティック、または異常に着目するもの）を実装する。アンチウィルスソフトウェアが更新され、稼働状態にあり、メールおよびリムーバブルメディア（例えば、フラッシュドライブ）をランサムウェアおよびその他のマルウェアに対して自動的にスキャンするよう設定されていることを確実にする。

OT：OTデバイスでアンチウィルスソフトウェアを使用するには、互換性チェック、変更管理、およびパフォーマンスインパクト指標を含む特別なプラクティスが必要となる場合がある。これらのプラクティスは、新しいシグネチャおよび悪意のあるコードの防御ソリューションの新バージョンをテストするために採用することが望ましい。

NIST CSF 2.0 参照	コスト	インパクト	実装の容易性
DE.CM-09	中	高	中

その他の NISTの参考文献

SP 800-53 Rev 5: AC-4, AC-9, AU-12, CA-7, CM-3, CM-6, CM-10, CM-11, SC-34, SC-35, SI-4, SI-7
SP 800-82 Rev 3: AU-1, MP-2, SI-3, SI-4, SI-7

サポートリソース

Ensure Your OS Antivirus and Anti-Malware Protections are Active
Control System Defense: Know the Opponent

4.B- 敵対的な事象を識別する

成果

組織は敵対的なセキュリティ事象を識別できる。

対処されるリスク

初期アクセス、権限昇格、および横方向への移動。

範囲

組織全体。

推奨される行動

組織が敵対的な事象に関する明確な基準およびプロセスを定義していることを確実にする。敵対的な事象が疑われる場合、インシデント対応計画に概説されている手順に従って、状況をエスカレーションする。

疑わしい敵対的な事象の調査期間を短縮するために、可能な限り事象の情報分析を自動化する。これにより、アナリストはこれらの事象を有効に軽減するための時間および能力を確保できる。

サイバーインシデントが疑われる場合に従うべき適切な手順および手続きについて、アナリストの役割に特化したトレーニングを実施する。

OT：組織は、プロセスと環境におけるOT固有の事象や異常を考慮に入れることが望ましい。侵入を示す可能性のある動作または事象に対する特定のツールやアラートは、OT環境内では実際には正常である場合があることを認識することが重要である。

NIST CSF 2.0 参照	コスト	インパクト	実装の容易性
DE.AE-08	中	高	複雑

その他の NISTの参考文献

SP 800-53 Rev 5: IR-4, IR-8
SP 800-82 Rev 3: IR-4

サポートリソース

Planning Considerations for Cyber Incidents
Cybersecurity Incident & Vulnerability Response Playbooks
Continuously Hunt for Network Intrusions

対応（RESPOND）

5.A- インシデントのコミュニケーション手順を確立する

成果	推奨される行動
内部および外部の組織パートナーおよび重要サプライヤー間の危機コミュニケーション方法を調整する。	インシデント発生中のステークホルダー及び調整およびコミュニケーションメカニズムを識別するコミュニケーション計画を策定する。 ステークホルダーと連携し、対応計画および情報共有の合意と整合性のある情報を、セキュアに共有する。情報共有の優先事項には、他のシステムおよびネットワークへの感染拡大防止が含まれる。 重大なインシデントの状況について、上級管理職に定期的に報告する。 悪意のあるインサイダーによる活動が発生した場合は、人事部門に通知する。 メディアとのやりとりおよび情報開示に関する組織のポリシーに準拠した、インシデント対応のためのメディアコミュニケーション手順を確立し、それに従う。

対処されるリスク	範囲
確立されたコミュニケーション手順がない場合、インシデントは対応チーム間の調整を妨げ、インシデントの解決を遅らせ、ダウンタイムを増やし、全体的な損害の拡大を招く。	組織全体。

NIST CSF 2.0 参照	コスト	インパクト	実装の容易性
RS.CO-03	低	高	中

その他の NISTの参考文献	サポートリソース
SP 800-53 Rev 5: IR-4, IR-6, IR-7, SR-3, SR-8 SP 800-82 Rev 3: IR-4, IR-6	Guidance on effective communications in a cyber incident Incident Management

5.B- インシデントの報告手順を確立する

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、必要に応じて州／連邦の規制当局またはセクターリスクマネジメント機関（SRMA）、情報共有分析センター（ISAC）、情報共有分析機関（ISAO）、およびCISA）に、誰に、どのように報告するかに関する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によって指示された期間内に、またはガイダンスがない場合は、安全に実行可能な限り速やかに、CISAおよびその他の必要な関係者に報告される。

対処されるリスク	範囲
タイムリーなインシデント報告がなければ、CISAおよびその他のグループは影響を受けた組織を支援することが難しくなり、特定の分野に対する広範な攻撃が発生しているかどうかといった、脅威の状況に関する重要な知見が不足する。	組織全体。

NIST CSF 2.0 参照	コスト	インパクト	実装の容易性
RS.CO-02, RS.MA-01	中	高	中

その他の NISTの参考文献	サポートリソース
SP 800-53 Rev 5: IR-4, IR-6, IR-7, IR-8, SR-3, SR-8 SP 800-82 Rev 3: IR-4, IR-6, IR-8	Cybersecurity Incident Response Critical Infrastructure Threat Information Sharing Framework Cyber Incident Reporting

復旧（RECOVER）

6.A- インシデント復旧計画を実行する

成果

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。

推奨される行動

サイバーセキュリティインシデントの影響を受ける可能性のある、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のサービスを復旧および復元するための計画を実行する。これには、重要な資産またはインターネットへのアクセスさえもできない状態で、ミッション上重要な機能を実行する能力が含まれる場合がある（例えば、紙ベースの業務への移行、無線通信）。

インシデント後の分析を実施して改善点を識別し、インシデント対応計画を改善する。得られた教訓の反映、検知および対応能力の強化、トレーニングを含むポリシーおよび手順の更新、およびすべてのステークホルダーへの変更の確実な周知に重点を置く。

対処されるリスク

資産、サービス、またはシステムの可用性の中断。

範囲

組織資産。

NIST CSF 2.0 参照	コスト	インパクト	実装の容易性
RC.RP-01, ID.IM-02, ID.IM-04	中	高	複雑

その他の NISTの参考文献

SP 800-53 Rev 5: AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, CP-2, CP-10, IA-1, IR-1, IR-4, IR-8, MA-1, MP-1, PE-1, PL-1, PM-1, PS-1, PT-1, RA-1, SA-1, SC-1, SI-1, SR-1, CA-2, CA-5, CA-7, CA-8, CP-2, CP-4, IR-3, IR-4, IR-8, PL-2, PM-4, PM-31, RA-3, RA-5, RA-7, SA-8, SA-11, SI-2, SI-4, SR-2, SR-5
SP 800-82 Rev 3: CA-2, CA-5, CP-4, CP-1, CP-2, CP-10, IR-1,IR-8, RA-3, SA-11, SR-6

サポートリソース

Incident Response Training
Cybersecurity Incident & Vulnerability Response Playbook
Incident Response Plan (IRP) Basics

用語集

アクセス制御リスト（Access Cotrol 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。出典：NIST SP 800-82 Rev. 3

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）。出典：NISTIR 4735

資産：価値を持つ人、構造、施設、情報、資材、またはプロセス。出典：DHS Risk Lexicon

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、サインイン試行の失敗の回数を決定するポリシー。出典：Account lockout threshold

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。出典：CNSSI 4009-2015

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。出典：NIST SP 800-34 Rev. 1

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。出典：NIST SP 800-128

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。出典：NIST SP 800-137

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。出典：NIST SP 800-126 Rev.3

代替管理策：NIST SP800-53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。出典：NIST SP 800-37 Rev. 2

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。出典：NIST SP 800-82 Rev. 3

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行動を検知し、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。出典：NIST SP 800-34 Rev. 1

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、ベンダー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、多くのベンダーは、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。出典：CISA Alert TA13-175A

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。出典：NIST SP 1800-12

暗号化する：データを暗号化して暗号文を生成する。出典：IETF RFC 4949 Ver2

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。出典：NIST SP 800-101 Rev. 1

実行可能ファイルまたは実行可能プログラム：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。出典：NIST SP 800-82 Rev. 3

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。出典：NISTIR 8183

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。出典：NIST SP 800-72

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。出典：NIST SP 800-82 Rev. 2

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。出典：NIST SP 800-34 Rev. 1

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。 出典：Homeland Security Act of 2002, 6 U.S.C. § 650(13)

情報共有分析センター（ISAC）：物理的脅威・サイバー脅威および緩和策に関する情報共有およびベストプラクティスを促進するために、重要インフラ所有者および運営者によって設立された信頼できる事業体。出典：“National Council of ISACs: About Isacs.” 2025年8月20日閲覧。出典：https://www.nationalisacs.org/about-isacs

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。出典：NIST SP 800-12 Rev. 1

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。出典: https://www.iec.ch/homepage

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。出典：“International Society of Automation” https://www.isa.org/

国際自動制御学会／国際電気標準会議（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。出典：上記のISA/IEC項目を参照。

資産台帳：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。

既知の悪用された脆弱性カタログ（Known Exploitable Vulnerabilities Catalog）：CISAが悪用された、または脅威アクター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、インシデントを減らすために、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。差出人：CISA KEV

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。出典：NIST SP 800-53 Rev. 5

ログ：組織のシステムおよびネットワーク内で発生した事象の記録。出典：NIST SP 800-92

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。出典：“Introduction to Access Programming” https://support.microsoft.com/en-us/office/introduction-to-access-programming-92eb616b-3204-4121-9277-70649e33be4f

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。出典：NIST

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。出典：“Introduction to Access Programming” https://support.microsoft.com/en-us/office/introduction-to-access-programming-92eb616b-3204-4121-9277-70649e33be4f

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。出典：NIST CSF

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。出典：NIST SP 800-37 Rev. 2: RMF

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。出典：NIST SP 800-30

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。出典：NIST SP 800-53 Rev. 5

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。出典：NIST SP 800-82 Rev. 3

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。出典：NIST SP 800-37 Rev. 2

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多要素認証（Phishing-Resistant MFA）：行政管理予算局（OMB）覚書 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。出典：OMB M-22-09

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。出典：CNSSI 4009-2015

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。出典：”MS-ISAC Security Primer - Remote Desktop Protocol” https://www.cisecurity.org/insights/white-papers/security-primer-remote-desktop-protocol

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。出典：”MS-ISAC Security Primer - Remote Desktop Protocol” https://www.cisecurity.org/insights/white-papers/security-primer-remote-desktop-protocol

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。出典：”ISO/IEC/IEEE 42010:2022” https://www.iso.org/standard/74393.html

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。出典：NIST SP 800-84

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。出典：NISTIR 7711

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。出典： CISA　Vulnerability Disclosure Policy

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; 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.