識別 (1)

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	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト:** 高 **複雑さ:** 中 **対処される戦術、技術、手順（TTP）またはリスク:** 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) **推奨される行動:** 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。 **無料のサービスおよび参考:** Cyber Hygiene Services 、"Stuff Off Search" Guide または vulnerability@cisa.DHS.gov へメール	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

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	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト:** 高 **複雑さ:** 低 **対処されるTTPまたはリスク:** 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。 **推奨される行動:** 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。	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

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	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト:** 高 **複雑さ:** 低 **対処されるTTPまたはリスク:** 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。 **推奨される行動:** 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。	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

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	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト:** 中 **複雑さ:** 低 **対処されるTTPまたはリスク:** 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。 **推奨される行動:** 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。	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

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	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト:** 高 **複雑さ:** 中 **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) **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KEV 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。 **無料のサービスおよび参考:** Known Exploited Vulnerabilities Catalog、Cyber Hygiene Services、または vulnerability@cisa.dhs.gov へメール	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

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	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト:** 高 **複雑さ:** 高 **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。 **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。 **無料のサービスおよび参考:** Critical Infrastructure Exercises	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

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	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト** 高 **複雑さ:** 低 **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) **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。	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

1.H サプライチェーンの脆弱性開示 ID.SC-1, ID.SC-3	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト** 高 **複雑さ:** 低 **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) **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。	☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

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	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト** 高 **複雑さ:** 低 **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) **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。	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

防御 (2)

2.A デフォルトパスワードの変更 PR.AC-1	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト:** 高 **複雑さ:** 中 **対処されるTTPまたはリスク:** 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) **推奨される行動:** 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。 **無料のサービスおよび参考:** CISA Bad Practices	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

2.B 最小のパスワード強度 PR.AC-1	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト:** 高 **複雑さ:** 低 **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）- 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) **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、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。 **無料のサービスおよび参考:** CISA Bad Practices、 XKCD 936	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

2.C 一意の認証情報 PR.AC-1	現状の評価	1年目の評価	メモ
コスト: $$$$ インパクト: 中 複雑さ: 中 **対処されるTTPまたはリスク:** 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) **推奨される行動:** 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。	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

2.D 離職する従業員の認証情報の無効化 PR.AC-1, PR.IP-11	現状の評価	1年目の評価	メモ
コスト: $$$$ インパクト: 中 複雑さ: 低 **対処されるTTPまたはリスク:** 有効なアカウント (T1078, ICS T0859) **推奨される行動:** 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。	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

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	現状の評価	1年目の評価	メモ
コスト: $$$$ インパクト: 高 複雑さ: 低 **対処されるTTPまたはリスク:** 有効なアカウント (T1078, ICS T0859) **推奨される行動:** 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。	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

2.F ネットワークセグメンテーション PR.AC-5, PR.PT-4	現状の評価	1年目の評価	メモ
コスト: $$$$ インパクト: 高 複雑さ: 高 **対処されるTTPまたはリスク:** 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) **推奨される行動:** 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。	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

2.G 失敗した（自動化された）ログイン試行の検出 PR.AC-7	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト:** 高 **複雑さ:** 低 **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）- 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) **推奨される行動:** 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	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

2.H フィッシングに強い多要素認証 (MFA) PR.AC-7, PR.AC-1	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト:** 高 **複雑さ:** 中 **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) **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。 **無料のサービスおよび参考:** CISA Bad Practices	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

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	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト:** 高 **複雑さ:** 低 **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) **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。 **無料のサービスおよび参考:** CISA Cyber Training	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

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	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト:** 高 **複雑さ:** 低 **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) **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。 **無料のサービスおよび参考:** CISA ICS Training	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

2.K 強力でアジャイルな暗号化 PR.DS-2	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト:** 高 **複雑さ:** 中 **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) **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。	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

2.L 機密データをセキュアにする PR.DS-1, PR.DS-5	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト:** 高 **複雑さ:** 中 **対処されるTTPまたはリスク:** 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) **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。	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

2.M 電子メールのセキュリティ PR.DS-5, PR.AC-7	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト:** 中 **複雑さ:** 低 **対処されるTTPまたはリスク:** フィッシング (T1566) ビジネスメール詐欺（BEC） **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。 **無料のサービスおよび参考:** CISA Binding Operational Directive	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

2.N マクロをデフォルトで無効にする PR.IP-1, PR.IP-3	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト:** 中 **複雑さ:** 低 **対処されるTTPまたはリスク:** 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) **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。	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

2.O 機器の設定の文書化 PR.IP-1	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト:** 高 **複雑さ:** 中 **対処されるTTPまたはリスク:** 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。 **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。	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

2.P ネットワークトポロジーの文書化 PR.IP-1, ID.AM-3	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト:** 中 **複雑さ:** 中 **対処されるTTPまたはリスク:** 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。 **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。	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

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	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト:** 高 **複雑さ:** 中 **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) 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) **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。	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

2.R システムのバックアップ PR.IP-4	現状の評価	1年目の評価	メモ
コスト: $$$$ インパクト: 高 複雑さ: 中 **対処されるTTPまたはリスク:** 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) **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。	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

2.S インシデント対応 (IR) 計画 PR.IP-9, PR.IP-10	現状の評価	1年目の評価	メモ
コスト: $$$$ インパクト: 高 複雑さ: 低 **対処されるTTPまたはリスク:** 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 **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。 **無料のサービスおよび参考:** Table Top Exercise Packages、Critical Infrastructure Exercises	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

2.T ログの収集 PR.PT-1	現状の評価	1年目の評価	メモ
コスト: $$$$ インパクト: 高 複雑さ: 中 **対処されるTTPまたはリスク:** 潜在的なサイバーインシデントを検知し対応する能力が先延ばし、不十分、または不完全である 防御の棄損 (T1562) **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。	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

2.U セキュアなログの保管 PR.PT-1	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト:** 高 **複雑さ:** 低 **対処されるTTPまたはリスク:** 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) **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。	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

2.V 不正な機器の接続禁止 PR.PT-2	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト:** 高 **複雑さ:** 高 **対処されるTTPまたはリスク:** 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) **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。	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

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	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト:** 高 **複雑さ:** 低 **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) 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) **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。 **無料のサービスおよび参考:** Cyber Hygiene Services、"Stuff Off Search" Guide または vulnerability@cisa.DHS.gov へメール	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

2.X 公衆インターネットへのOT接続の制限 PR.PT-4	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト:** 中 **複雑さ:** 中 **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) **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。 **無料のサービスおよび参考:** Cyber Hygiene Services、"Stuff Off Search" Guide または vulnerability@cisa.DHS.gov へメール	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

検知 (3)

3.A 関連する脅威およびTTPの検知 ID.RA-2, ID.RA-3, DE.CM-1	現状の評価	1年目の評価	メモ
コスト: $$$$ インパクト: 中 複雑さ: 高 **対処されるTTPまたはリスク:** 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。 **推奨される行動:** 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（例えばルール、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。	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

対応 (4)

4.A インシデント報告 RS.CO-2, RS.CO-4	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト:** 高 **複雑さ:** 低 **対処されるTTPまたはリスク:** 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。 **推奨される行動:** 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。 **無料のサービスおよび参考:** Incident Reporting および/または report@cisa.gov へメール または (888) 282-0870 へ連絡	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

4.B 脆弱性開示／報告 RS.AN-5	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト:** 低 **複雑さ:** 高 **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) **推奨される行動:** 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。 **無料のサービスおよび参考:** Vulnerability Disclosure Policy Template、Disclose.io Policy Maker、Coordinated Vulnerability Disclosure Process、脆弱性報告; vulnerability@cisa.dhs.gov へメール	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

4.C SECURITY.TXTファイルの配置 RS.AN-5	現状の評価	1年目の評価	メモ
コスト: $$$$ **インパクト:** 高 **複雑さ:** 低 **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) **推奨される行動:** 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。 **無料のサービスおよび参考:** https://securitytxt.org	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	

復旧 (5)

5.A インシデント計画および準備 RC.RP-1, R.IP-9, PR.IP-10	現状の評価	1年目の評価	メモ
コスト: $$$$ インパクト: 中 複雑さ: 低 **対処されるTTPまたはリスク:** 資産、サービス、またはシステムの可用性の中断。 **推奨される行動:** 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。	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	日付: ☐ 実装済み ☐ 進行中 ☐ 範囲指定済み ☐ 未着手	