Expand - Collapse

- Sec01-02-3 サイバーセキュリティフレームワーク(CSF) フレームワークコア
  - ID 特定
    - 資産管理（ID.AM）
      - 組織が事業目的を達成することを可能にするデータ、職員、デバイス、システム、施設を特定し、事業目標と自組織のリスク戦略との相対的重要性に応じて管理している。
      - ID.AM-1
        - 企業内の物理デバイスとシステムの一覧を作成している。
      - ID.AM-2
        - 企業内のソフトウェアプラットフォームとアプリケーションの一覧を作成している。
      - ID.AM-3
        - 企業内の通信とデータの流れの図を用意している。
      - ID.AM-4
        - 外部情報システムの一覧を作成している。
      - ID.AM-5
        - リソース（例：ハードウェア、デバイス、データ、ソフトウェア）を、分類、重要度、ビジネス上の価値に基づいて優先順位付けしている。
      - ID.AM-6
        - すべての従業員と第三者である利害関係者（例：供給業者、顧客、パートナー）に対して、サイバーセキュリティ上の役割と責任を定めている。
    - ビジネス環境（ID.BE）
      - 自組織のミッション、目標、利害関係者、活動を理解し、優先順位付けを行っている; この情報はサイバーセキュリティ上の役割、責任、リスク管理上の意思決定を伝達するために使用される。
      - ID.BE-1
        - サプライチェーンにおける企業の役割を特定し、伝達している
      - ID.BE-2
        - 重要インフラとその産業分野における企業の位置付けを特定し、伝達している。
      - ID.BE-3
        - 企業のミッション、目標、活動に関して優先順位を定め、伝達している。
      - ID.BE-4
        - 重要サービスを提供する上での依存関係と重要な機能を把握している。

Expand - Collapse

- ID.BE-5
  - 重要サービスの提供を支援する、レジリエンスに関する要求事項を定めている。

- ガバナンス（ID.GV）
  - 自組織に対する規制、法律、リスクと、自組織の環境、運用上の要求事項を管理しモニタリングするためのポリシー、手順、プロセスを理解しており、サイバーセキュリティリスクの管理者に伝達している。
  - ID.GV-1
    - 自組織の情報セキュリティポリシーを定めている。
  - ID.GV-2
    - 情報セキュリティ上の役割と責任について、内部と外部パートナーとで調整・連携している。
  - ID.GV-3
    - プライバシーや市民の自由に関する義務を含む、サイバーセキュリティに関する法規制上の要求事項を理解し、管理している。
  - ID.GV-4
    - ガバナンスとリスク管理プロセスがサイバーセキュリティリスクに対応している。

- リスクアセスメント（ID.RA）
  - 企業は自組織の業務（ミッション、機能、イメージ、評判を含む）、自組織の資産、個人に対するサイバーセキュリティリスクを把握している。
  - ID.RA-1
    - 資産の脆弱性を特定し、文書化している。
  - ID.RA-2
    - 情報共有フォーラム／ソースより、脅威と脆弱性に関する情報を入手している。
  - ID.RA-3
    - 内外からの脅威を特定し、文書化している。
  - ID.RA-4
    - ビジネスに対する潜在的な影響と、その可能性を特定している。
  - ID.RA-5
    - リスクを判断する際に、脅威、脆弱性、可能性、影響を考慮している。
  - ID.RA-6
    - リスクに対する対応を定め、優先順位付けしている。

- リスク管理戦略（ID.RM）
  - 自組織の優先順位、制約、リスク許容度、想定を定め、運用リスクの判断に利用している。

Expand - Collapse

- ID.RM-1
  - リスク管理プロセスが自組織の利害関係者によって確立、管理され、承認されている。
- ID.RM-2
  - 自組織のリスク許容度を決定し、明確にしている。
- ID.RM-3
  - 企業によるリスク許容度の決定が、重要インフラにおける自組織の役割と、その分野に特化したリスク分析の結果に基づいて行われている。

- PR 防御
  - アクセス制御（PR.AC）
    - 資産および関連施設へのアクセスを、承認されたユーザ、プロセス、またはデバイスと、承認された活動およびトランザクションに限定している。
    - PR.AC-1
      - 承認されたデバイスとユーザの識別情報と認証情報を管理している。
    - PR.AC-2
      - 資産に対する物理アクセスを管理し、保護している。
    - PR.AC-3
      - リモートアクセスを管理している。
    - PR.AC-4
      - 最小権限および職務の分離の原則を取り入れて、アクセス権限を管理している。
    - PR.AC-5
      - 適宜、ネットワークの分離を行って、ネットワークの完全性を保護している。
  - 意識向上およびトレーニング（PR.AT）
    - 自組織の職員およびパートナーに対して、関連するポリシー、手順、契約に基づいた、情報セキュリティに関連する義務と責任を果たせるようにするために、サイバーセキュリティ意識向上教育と、十分なトレーニングを実施している。
    - PR.AT-1
      - すべてのユーザに情報を周知し、トレーニングを実施している。
    - PR.AT-2
      - 権限を持つユーザが役割と責任を理解している。
    - PR.AT-3
      - 第三者である利害関係者（例：供給業者、顧客、パートナー）が役割と責任を理解している。
    - PR.AT-4
      - 上級役員が役割と責任を理解している。

Expand - Collapse

- PR.AT-5
  - 物理セキュリティおよび情報セキュリティの担当者が役割と責任を理解している。

- データセキュリティ（PR.DS）
  - 情報と記録（データ）を情報の機密性、完全性、可用性を保護するために定められた自組織のリスク戦略に従って管理している。
  - PR.DS-1
    - 保存されているデータを保護している。
  - PR.DS-2
    - 伝送中のデータを保護している。
  - PR.DS-3
    - 資産について撤去、譲渡、廃棄プロセスを正式に管理している。
  - PR.DS-4
    - 可用性を確保するのに十分な容量を保持している。
  - PR.DS-5
    - データ漏えいに対する保護対策を実施している。
  - PR.DS-6
    - ソフトウェア、ファームウェア、および情報の完全性の検証に、完全性チェックメカニズムを使用している。
  - PR.DS-7
    - 開発・テスト環境を実稼働環境から分離している。

- 情報を保護するためのプロセスおよび手順（PR.IP）
  - （目的、範囲、役割、責任、経営コミットメント、組織間の調整を扱う）セキュリティポリシー、プロセス、手順を維持し、情報システムと資産の保護の管理に使用している。
  - PR.IP-1
    - 情報技術／産業用制御システムのベースラインとなる設定を定め、維持している。
  - PR.IP-2
    - システムを管理するためのシステム開発ライフサイクルを導入している。
  - PR.IP-3
    - 設定変更管理プロセスを導入している。
  - PR.IP-4
    - 情報のバックアップを定期的に実施、保持し、テストしている。
  - PR.IP-5
    - 自組織の資産の物理的な運用環境に関するポリシーと規制を満たしている。

Expand - Collapse

- PR.IP-6
  - ポリシーに従ってデータを破壊している。
- PR.IP-7
  - 保護プロセスを継続的に改善している。
- PR.IP-8
  - 保護技術の有効性について、適切なパートナーとの間で情報を共有している。
- PR.IP-9
  - 対応計画（インシデント対応および事業継続）と復旧計画（インシデントからの復旧および災害復旧）を実施し、管理している。
- PR.IP-10
  - 対応計画と復旧計画をテストしている。
- PR.IP-11
  - 人事に関わる対策にサイバーセキュリティ（例：アクセス権限の無効化、従業員に対する審査）を含めている。
- PR.IP-12
  - 脆弱性管理計画を作成し、実施している。

- 保守（PR.MA）
  - 産業用制御システムと情報システムのコンポーネントの保守と修理をポリシーと手順に従って実施している。
  - PR.MA-1
    - 自組織の資産の保守と修理は、承認・管理されたツールを用いて、タイムリーに実施し、ログを記録している。
  - PR.MA-2
    - 自組織の資産に対する遠隔保守は、承認を得て、ログを記録し、不正アクセスを防げる形で実施している。

- 保護技術（PR.PT）
  - 関連するポリシー、手順、契約に基づいて、システムと資産のセキュリティと耐性・復旧力を確保するための、技術的なセキュリティソリューションを管理している。
  - PR.PT-1
    - ポリシーに従って監査記録／ログ記録の対象を決定、文書化し、そうした記録を実施して、レビューしている。
  - PR.PT-2
    - ポリシーに従って取り外し可能な外部記録媒体を保護し、そうした媒体の使用を制限している。
  - PR.PT-3

Expand - Collapse

- 最小機能の原則を取り入れて、システムと資産に対するアク
  る。
- PR.PT-4
  - 通信ネットワークと制御ネットワークを保護している。

- DE 検知
  - 異常とイベント（DE.AE）
    - 異常な活動をタイムリーに検知し、イベントがもたらす可能性のある影響を把握している。
    - DE.AE-1
      - ネットワーク運用のベースラインと、ユーザとシステム間の予測されるデータの流れを特定し、管理している。
    - DE.AE-2
      - 攻撃の標的と手法を理解するために、検知したイベントを分析している。
    - DE.AE-3
      - イベントデータを複数の情報源やセンサーから収集し、相互に関連付けている。
    - DE.AE-4
      - イベントがもたらす影響を特定している。
    - DE.AE-5
      - インシデント警告の閾値を定めている。
  - セキュリティの継続的なモニタリング (DE.CM)
    - サイバーセキュリティイベントを検知し、保護対策の有効性を検証するために、情報システムと資産を離散間隔でモニタリングしている。
    - DE.CM-1
      - 発生する可能性のあるサイバーセキュリティイベントを検知できるよう、ネットワークをモニタリングしている。
    - DE.CM-2
      - 発生する可能性のあるサイバーセキュリティイベントを検知できるよう、物理環境をモニタリングしている。
    - DE.CM-3
      - 発生する可能性のあるサイバーセキュリティイベントを検知できるよう、個人の活動をモニタリングしている。
    - DE.CM-4
      - 悪質なコードを検出できる。
    - DE.CM-5
      - 悪質なモバイルコードを検出できる。

Expand - Collapse

- DE.CM-6
  - 発生する可能性のあるサイバーセキュリティイベントを検知できるよう、外部サービスプロバイダの活動をモニタリングしている。
- DE.CM-7
  - 権限のない従業員、接続、デバイス、ソフトウェアのモニタリングを実施している。
  - 参考情報
    - • NIST SP 800-53 Rev. 4 AU-12, CA-7, CM-3,　CM-8, PE-3, PE-6, PE-20, SI-4
- DE.CM-8
  - 脆弱性スキャンを実施している。

検知プロセス（DE.DP）

- 異常なイベントをタイムリーに、かつ正確に検知するための検知プロセスおよび手順を維持し、テストしている。
- DE.DP-1
  - 説明責任を果たせるよう、検知に関する役割と責任を明確に定義している。
- DE.DP-2
  - 検知活動は必要なすべての要求事項を満たしている。
- DE.DP-3
  - 検知プロセスをテストしている。
- DE.DP-4
  - イベント検知情報を適切な関係者に伝達している。
- DE.DP-5
  - 検知プロセスを継続的に改善している。

RS 対応

対応計画（RS.RP）

- 検知したサイバーセキュリティイベントにタイムリーに対応できるよう、対応プロセスおよび手順を実施し、維持している。
- RS.RP-1
  - イベントの発生中または発生後に対応計画を実施している。

伝達（RS.CO）

- 法執行機関からの支援を必要に応じて得られるよう、内外の利害関係者との間で対応活動を調整している。
- RS.CO-1
  - 対応が必要になった時の自身の役割と行動の順番を従業員は認識している。
- RS.CO-2

Expand - Collapse

- 定められた基準に沿って、イベントを報告している。
- RS.CO-3
  - 対応計画に従って情報を共有している。
- RS.CO-4
  - 対応計画に従って、利害関係者との間で調整を行っている。
- RS.CO-5
  - サイバーセキュリティに関する状況認識を深めるために、外部利害関係者との間で任意の情報共有を行っている。

- 分析 (RS.AN)
  - 適切な対応を確実にし、復旧活動を支援するために、分析を実施している。
- RS.AN-1
  - 検知システムからの通知を調査している。
- RS.AN-2
  - インシデントがもたらす影響を把握している。
- RS.AN-3
  - フォレンジクスを実施している。
- RS.AN-4
  - 対応計画に従ってインシデントを分類している。

- 低減（RS.MI）
  - イベントの拡大を防ぎ、その影響を緩和し、インシデントを根絶するための活動を実施している。
- RS.MI-1
  - インシデントを封じ込めている。
- RS.MI-2
  - インシデントを低減している。
- RS.MI-3
  - 新たに特定された脆弱性に関して、許容できるリスクである場合にはその旨を文書化し、そうでない場合には低減している。

- 改善（RS.IM）
  - 現在と過去の意思決定／対応活動から学んだ教訓を取り入れることで、自組織の対応活動を改善している。
- RS.IM-1
  - 学んだ教訓を対応計画に取り入れている。
- RS.IM-2
  - 対応戦略を更新している。

Expand - Collapse

- RC 復旧
  - 復旧計画（RC.RP）
    - サイバーセキュリティイベントによる影響を受けたシステムや資産をタイムリーに復旧できるよう、復旧プロセスおよび手順を実施し、維持している。
    - RC.RP-1
      - イベントの発生中または発生後に復旧計画を実施している。
  - 改善（RC.IM）
    - 学んだ教訓を将来的な活動に取り入れることで、復旧計画およびプロセスを改善している。
    - RC.IM-1
      - 学んだ教訓を復旧計画に取り入れている。
    - RC.IM-2
      - 復旧戦略を更新している。
  - 伝達（RC.CO）
    - コーディネーティングセンター、インターネットサービスプロバイダ、攻撃システムのオーナー、被害者、その他のCSIRT、ベンダなどの、内外の関係者との間で復旧活動を調整している。
    - RC.CO-1
      - 広報活動を管理している。
    - RC.CO-2
      - イベント発生後に評判を回復している。
    - RC.CO-3
      - 復旧活動について内部利害関係者と役員、そして経営陣に伝達している。