資料７－２

電力システムにおけるサイバーセキュリティ
リスク点検ガイド（案）

令和６年●月

資源エネルギー庁 電力・ガス事業部
電力産業・市場室

目次

1. 背景と目的

あらゆる分野でデジタル化が進展する一方、多様化・巧妙化するサイバー攻撃の脅威は日々高まっている。重要インフラたる電力分野においてもサイバー攻撃の事案は増加傾向にあり、国内外問わず、電力会社を標的としたサイバー攻撃が発生している。電力系統へのサイバー攻撃が発生した場合、電気の安定供給に重大な支障を来すことが想定されるところ、サイバーセキュリティ向上に向けた不断の取組が求められる。

経済産業省・資源エネルギー庁や業界団体は、電力会社におけるサイバーセキュリティ向上の取組に向け、これまで複数のガイドライン等を発表してきた。ガイドライン等の整備により電力会社におけるサイバーセキュリティ対策の取組は進みつつある一方で、サイバーセキュリティの脅威は日々進化・巧妙化している状況を踏まえると、現状の対策で十分ということは決してなく、電力システムにおけるサイバーセキュリティ対策の継続的改善・高度化は必要不可欠である。

サイバーセキュリティ対策の継続的改善・高度化に向けては、「電力制御システムセキュリティガイドライン」にも記載のとおり、PDCA サイクルに基づくセキュリティ対策の計画・実施・点検・改善のプロセスが重要となるが、資源エネルギー庁が実施した調査によると、対策を実施している事業者の割合と比較して、定期的なセキュリティリスクの点検や継続的な対策改善を実施している事業者は限定的であった。セキュリティのリスク点検を定期的に実施しない場合、残存リスクを正しく把握することができず、適切な対策が施されない可能性がある。また、対策の継続的改善が実施されないことで、日々進化・巧妙化するサイバー脅威に対応できず、攻撃を受け、電力供給や事業継続に甚大な影響を及ぼす可能性がある。

この現状を鑑み、定期的なリスク点検を実施できていない電力会社を主な対象として、過大なコストをかけずに簡易的にリスク点検ができるよう、「電力システムにおけるサイバーセキュリティリスク点検ガイド」（本ガイド）及びガイドに付属する「電力システムにおけるサイバーセキュリティ対策状況可視化ツール」（対策状況可視化ツール）を開発した。日々進化・巧妙化するサイバー脅威に対抗するために、本ガイド及び対策状況可視化ツールを用いて自社の対策実施状況を合理的かつ効率的に点検・確認するとともに、点検結果に基づき、セキュリティ対策の見直し・改善を行うことで、対策の継続的改善を図ることが期待される。

コラム：国内における電力分野のセキュリティ対策に関するガイドライン等

2022 年現在、国内における電力分野のセキュリティ対策に関する文書として以下に示す文書が発表されているとおり、電力分野に関する様々なプレーヤーに対して、求められる対策が整備されつつあることが分かる。本ガイド及び付属する対策状況可視化ツールでは、各対策要求事項に対して、一部のガイドラインに記載された項目との対応関係も示している。各ガイドライン等で求められる対策については、それぞれの文書を参照いただきたい。

名称	主な対象	発行主体	概要
電力制御システムセキュリティガイドライン (2019年10月第2版改定)	電気事業の用に供する電気工作物	日本電気協会	電気事業法、電気設備に関する技術基準を定める省令及びその解釈に基づき、電気事業者が施設する電力制御システム等及びそれに携わる者に対しては、本ガイドラインに基づく対策が求められる。
スマートメーターシステムセキュリティガイドライン (2019年10月第2版改定)	スマートメーターシステム	日本電気協会	電気事業法、電気設備に関する技術基準を定める省令及びその解釈に基づき、スマートメーターシステムに対しては、本ガイドラインに基づく対策が求められる。
系統連系技術要件 (2020年10月より、セキュリティに関する要件追加)	系統連系する発電設備	各一般送配電事業者	系統連系する発電設備にすべからく求められる対策。具体的には、ネットワーク接続点の保護、マルウェア対策、系統運用者に対するセキュリティ管理責任者の通知の3点が求められる。
出力制御機能付PCSの技術仕様 (2015年5月公開)	出力制御機能付PCS	JPEA・JEMA・電事連	出力制御機能付PCSにおいて満たすべきサイバーセキュリティ対策の要件を示した技術仕様。
自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン（内規） (2022年6月公開)	自家用電気工作物（発電設備と需要設備の両方を含む）	経済産業省	自家用電気工作物（発電設備と需要設備の両方を含む）に求められるサイバーセキュリティ対策事項を記載したガイドライン。
小売電気事業者のためのサイバーセキュリティ対策ガイドライン (2021年2月策定)	小売電気事業者	資源エネルギー庁	小売電気事業者が主体的に取り組むことが求められるサイバーセキュリティ対策に関して記載したガイドライン。
ERABに関するサイバーセキュリティガイドライン Ver2.0 (2019年12月改定)	ERABに関する事業者	経済産業省・IPA	ERAB のサービスレベルを維持するために ERAB に参画する各事業者が実施すべき最低限のセキュリティ対策の要求事項を示したガイドライン。
特定卸供給に係るサイバーセキュリティ確保の指針 (2022年4月制定)	特定卸供給事業に関するシステム	資源エネルギー庁	特定卸供給事業を実施する上で確保すべきサイバーセキュリティとその対策の内容を示すことを目的とした指針で、特定卸供給事業の届出の際に、本指針に基づく対策実施状況を記載する必要がある。

コラム：電力分野に対する近年のサイバー脅威事例

近年、電力システムを狙うサイバー攻撃は増加傾向にあり、国内外の電力会社が悪意あるサイバー脅威の対象となっている。以下にいくつかのサイバー脅威事例を示す。特に近年ではランサムウェア攻撃が増加傾向にあり、システムの停止やデータ漏えいにつながった事例も確認できる。

事例①：ランサムウェア感染による電力供給の停止（南アフリカ・小売電気事業者）

2019 年 7 月、南アフリカの小売電気事業者の情報システムがランサムウェア攻撃を受け、データの暗号化やサービスの停止に至った。プリペイド式電力供給サービスも停止したことで、料金の支払いを行うことが必要な一部の需要家への電力供給がなされず、25 万を超える需要家において停電が発生した。

事例②：会員制 Web サービスへの不正アクセス（日本・小売電気事業者）

2019 年 12 月、国内の小売電気事業者の会員制 Web サービスに対して、第三者からの大量の不正アクセスが発生し、105 名の会員が不正にログインされた。105 名のうち 44 名が不正なポイント交換の被害を受け、その被害額は、約 14 万円相当に及んだ。

事例③：モバイルサービスに対する不正アクセスによるデータ漏えい（英国・小売電気事業者）

2021 年 2 月、イギリスの大手小売電気事業者が提供するモバイルアプリケーションサービスが不正アクセスを受け、一部の顧客の個人情報や銀行口座情報が流出した。

事例④：サイバー攻撃によるシステムの停止・データの破損（米国・発電事業者／配電事業者）

2021 年 11 月、米国コロラド州の配電事業者の企業内ネットワークシステムがサイバー攻撃を受け、約 90%のシステムが破損等の影響により停止するとともに、過去 20～25 年のデータが破損した。攻撃によりシステムが停止したことで、料金の支払い処理、請求処理、アカウント情報変更等の顧客サポートサービスも停止した。

事例⑤：ランサムウェア攻撃によるデータ漏えい（日本・小売電気事業者）

2022 年 9 月、国内の小売電気事業者が管理・運用するファイルサーバーがランサムウェア攻撃を受け、顧客の個人情報・法人情報、取引先の情報等が流出した可能性が報告された。ただし、2022 年 11 月時点で、侵害された情報に関して一般には公開されておらず不正利用につながる形跡はないことが確認された。

事例⑥：ランサムウェア攻撃によるデータ漏えい（ルクセンブルク・発電事業者）

2022 年 7 月、ルクセンブルクに拠点を置く発電事業者がランサムウェア攻撃を受けた。顧客ファイル管理システムのデータが暗号化されたことで顧客ポータルが機能しなくなったほか、パスポート・請求書・電子メールを含む 150GB の機微情報が流失した可能性がある。

事例⑦：ランサムウェア攻撃によるデータ漏えい（インド・発電事業者等）

2022 年 10 月、インドの大手電力会社がランサムウェア攻撃を受けた。攻撃グループは、攻撃によって窃取した機密性の高いデータを既に外部に漏えいさせており、漏えいされた情報の中には、従業員の個人情報のほか、取引情報、設計図、財務情報のような社内の機微情報等も含まれている。

2. 本ガイド・対策状況可視化ツールの対象

本ガイド及び対策状況可視化ツールは、主に以下の 4 つの事業区分の電力会社（電力の供給等を担う会社）及び当該企業が保有する電力制御システム・IT システムを対象としたリスク点検ツールである。

1. 発電事業者
2. 小売電気事業者
3. アグリゲーター（アグリゲーションコーディネーター及びリソースアグリゲーター）
4. 自家用電気工作物設備設置者

これらの事業区分に該当する電力会社の中でも、特に、定期的なリスク点検を現状で実施できていない企業において、本ガイド及び対策状況可視化ツールを活用したリスク点検を実施することが推奨される。定期的なリスク点検を既に実施している企業においても、リスク点検実施にあたってのコスト、知識、期間等に課題に感じている企業は、本ガイド及び対策状況可視化ツールを是非活用いただきたい。なお、対策状況可視化ツールは、電力広域的運営推進機関（OCCTO）が会員企業に対して定期的に実施を促すセキュリティ自己診断に対しても活用できる。具体的には、OCCTO からセキュリティ自己診断の依頼があった場合に、本対策状況可視化ツールを用いて実施したリスク点検の結果を OCCTO に提出することができる。

3. 本ガイド・対策状況可視化ツールの想定活用方法

本ガイド及び対策状況可視化ツールの活用方法として、以下の活用方法が想定される。

- セキュリティ対策状況の点検・改善に向けた活用：
  本ガイド及び対策状況可視化ツールを活用して自社のセキュリティ対策状況を点検することで、対策が十分に実施できていない項目を可視化することができる。また、対策状況の可視化結果を踏まえ、どのような追加対策が望まれるかを確認することができる。
- セキュリティ対策検討における活用：
  国内のセキュリティガイドラインに遵守するためにどのような対策を実施する必要があるか、その対策を怠った場合にどのようなリスクがあるか、対策の達成基準はどのようなものかといった情報を踏まえ、自社のセキュリティ対策検討を効果的に進めることができる。
- セキュリティに関する社内教育・訓練・意識啓発活動への活用：
  本ガイド及び対策状況可視化ツールを活用して自社のセキュリティ対策状況を把握・可視化することで、その結果を社内教育や訓練に組み込むとともに、対策状況を踏まえた意識啓発活動を行うことができる。
- OCCTO 等の外部関係者に対するセキュリティ対策状況報告における活用：
  自社のセキュリティ対策状況について OCCTO 等の外部関係者に報告する際、対策状況可視化ツールの可視化結果を用いて報告することができる。

4. 本ガイド・対策状況可視化ツールに基づくリスク点検の進め方

4.1. 本ガイド・対策状況可視化ツールの構成

本ガイド及び対策状況可視化ツールの構成は図 4-1 に示すとおりである。以降では、本ガイド及び対策状況可視化ツールを活用したリスク点検の進め方について説明するとともに、リスク点検を踏まえた対策の改善方針及び具体的なリスク点検項目を示す。対策状況可視化ツールでは、各リスク点検項目に対して電力会社が対策状況を入力することで、どのような対策が実施できているか／不足しているかを可視化・確認することができる。

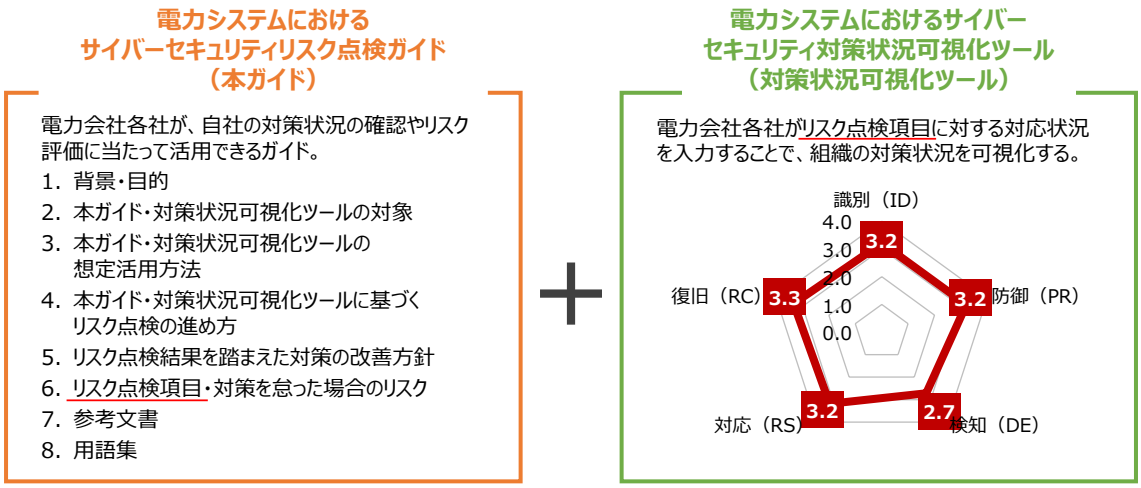


図 4-1 本ガイド及び対策状況可視化ツールの構成

本ガイド及び対策状況可視化ツールにおけるリスク点検項目は、国内外の電力会社において広く活用され、様々な事業区分に活用可能な米国 NIST の Cybersecurity Framework（NIST CSF）Version 1.1 を参考に整理している。NIST CSF はサイバーセキュリティマネジメントの枠組みを定めたフレームワークであり、業種、組織規模、リスク状況、セキュリティ対策の複雑さ等に依存せず、どのような組織においても活用可能である。事実、重要インフラ事業者に限らず官公庁や一般企業でも活用されているほか、諸外国でも認知・評価が高く、セキュリティ対策におけるグローバル・スタンダードになりつつある。NIST CSF では、5 つのセキュリティ機能（識別、防御、検知、対応、復旧）に対し、機能の詳細を定めた 23 のカテゴリー、108 のサブカテゴリーが定義されている。本ガイド及び対策状況可視化ツールでは、108 のサブカテゴリーをリスク点検項目として設定している。なお、リスク点検項目は情報処理推進機構（IPA）が公開する日本語翻訳版[1]に基づく内容であるが、それぞれのリスク点検項目に関

[1] https://www.ipa.go.jp/files/000071204.pdf

する補足説明を括弧書きで記載しているため、併せて参照いただきたい。

具体的なリスク点検項目及び各点検項目に関連する対策を怠った場合のリスクの一覧は、第 6 章に示す。

4.2. リスク点検の全体プロセス

本ガイド・対策状況可視化ツールを用いたリスク点検の全体プロセス概要を図 4-2 に示す。本図に示すとおり、リスク点検のプロセスは準備、実施、結果を踏まえた改善検討の大きく 3 つのフェーズに分かれる。以降では、各フェーズにおける実施内容について詳細に記載する。なお、図 4-2 に示しているとおり、実効性のあるリスク点検を行い、その結果を踏まえて対策を継続的に改善するために、一部の事項について経営層に報告することが望まれる。

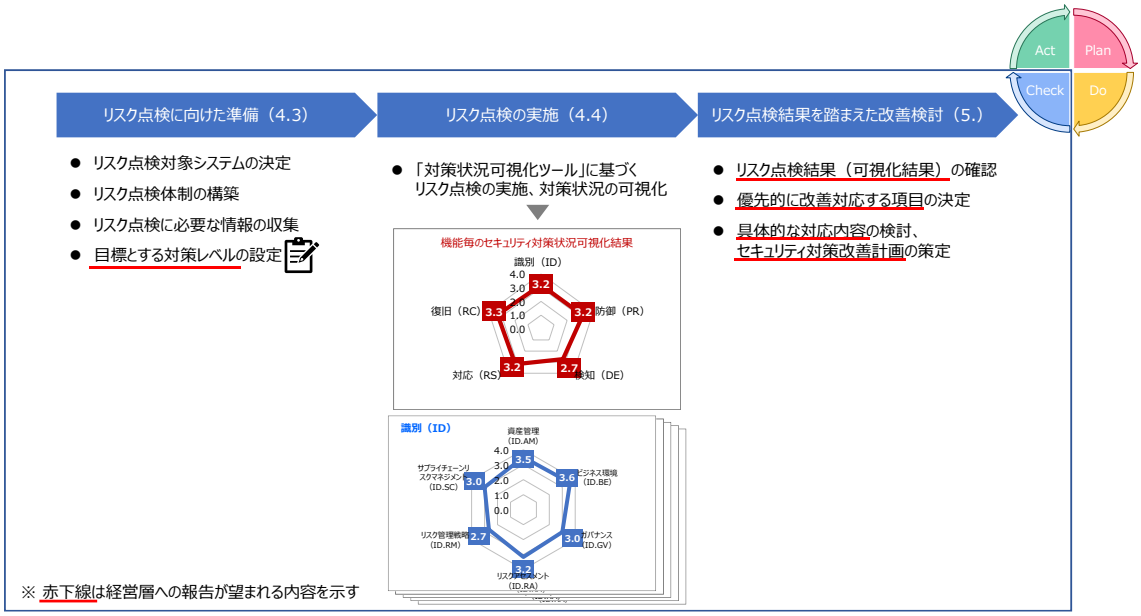


図 4-2 リスク点検の全体プロセス概要

4.3. リスク点検に向けた準備

本ガイド及び対策状況可視化ツールを用いたリスク点検に向け、体制整備、必要な情報の収集、目標レベルの設定等の準備が必要となる。初めてのリスク点検であるか、二回目以降のリスク点検であるかによって必要な準備は異なり、二回目以降のリスク点検の場合、初回のリスク点検で活用した情報に基づいた効率的なリスク点検が実施可能となる。

リスク点検にあたっては、まず、リスク点検の対象システムを決定する必要がある。社内のすべてのシステムに対してリスク点検を実施するには膨大な工数がかかるため、優先度をつけた上で、対象システムを

選定することが望まれる。対象システムの選定にあたっては、「電力制御システムセキュリティガイドライン」や「ERAB に関するサイバーセキュリティガイドライン Ver 2.0」における重要度の定義、社内のセキュリティ対策方針、対策の実施状況、対象システムに対する脅威の状況、前回のリスク点検の結果等を総合的に勘案して踏まえ、決定することが望まれる。

リスク点検の実施に向け、次に対象システムに関する知識を有した担当者（主担当）を選定することが望まれる。主担当が中心となりリスク点検を推進するが、リスクを点検する上では関係部署との連携が必要である。具体的には、経営層、社内セキュリティ関係部署、人事関係部署、リスク管理・法務関係部署、購買・調達関係部署等と連携し、リスク点検にあたって必要な情報を確認しつつ、リスク点検を進めることが必要である。また、リスク点検結果については、経営層に報告し、自社が抱えるセキュリティリスクの現状について、改善計画と合わせて伝えることが望まれる。リスク点検の実施にあたってはサイバーセキュリティに関する知識も求められるところ、IPA「情報セキュリティマネジメント試験」合格者相当の知識を有した主担当がリスク点検を主導することが推奨される。重要なシステムに対する精緻なリスク点検を行い、セキュリティ対策の見直し・改善を行う場合には、より高いスキルレベルを求める「情報処理安全確保支援士」相当の知識を有した主担当がリスク点検を主導するこが望まれる。

自社のセキュリティ対策に関する継続的改善につなげるために、リスク点検の実施に先立ち、自社が目標とする対策レベルを設定する必要がある。目標とする対策レベルは、リスク点検実施前に経営層に報告することが望ましい。本ガイド・対策状況可視化ツールでは、NIST CSF の評価基準であるティアと同様に、各リスク点検項目に対して、0～4 の 5 段階の達成基準を設定している。具体的には、0：対応できていない状態、1：部分的に対応できている状態、2：リスクが認識できる状態、3：対応に再現性がある状態、4：変化に適用可能な対応がある状態といった水準で達成基準を設けている。例えば、「ID.GV-1：組織のサイバーセキュリティポリシーが、定められ、周知されている。」というリスク点検項目について、以下の 5 段階の達成基準を設定している。

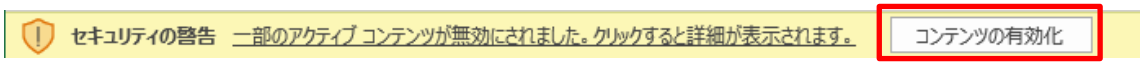
- 0: 対応なし。
- 1: 個々のシステムにおいて、独自にセキュリティ対策が検討され、適用されている。
- 2: 1 に加え、社内の各組織において、個別にセキュリティルールが策定され、遵守が求められている。
- 3.: 2 に加え、会社のセキュリティポリシーが文書で規定され、社内に周知されている。
- 4.: 3 に加え、会社のセキュリティポリシーは、社内外の最新の情報・動静を踏まえ、定期的に見直されている。

本達成基準を参考にしつつ、自社が目標とする対策レベルを設定することが望まれる。対策状況可視化ツールでは、NIST CSF の 5 つのセキュリティ機能ごと（識別、防御、検知、対応、復旧）の対策レベルの平均値と、各機能のカテゴリーごとの対策レベルの平均値とが、レーダーチャートとして可視化される。目標値の定め方や具体的な目標値は社内のセキュリティ対策方針、対策の実施状況、対象システムに対する脅威の状況、前回のリスク点検の結果等を踏まえて検討すべきであり、例えば、ガイドラインで求められる対策項目と関係するリスク点検項目はすべて 1 以上の対策レベルになること、すべてのカ

テゴリーの平均値が 2.5 以上になること、すべてのリスク点検項目について前回のリスク点検結果以上の対策レベルになること等の目標が想定される。なお、達成基準は一つの例として示しているため、社内の状況に応じて具体的な内容を修正して構わない。

4.4. リスク点検の実施

※ 対策状況可視化ツールでは、リスク点検項目のフィルタリングのためにマクロを利用しています。Excel において「セキュリティの警告」が出た場合、「コンテンツの有効化」をクリックして、マクロを有効化していただきますよう、お願いいたします。



リスク点検は、本ガイドに付随する対策状況可視化ツールを用いて行う。対策状況可視化ツールは、「使い方」、「チェックシート」、「可視化結果」、「可視化結果（広域機関用）」の 4 つのシートで構成される。「チェックシート」において、各リスク点検項目に対する対応状況を選択・入力することで、対策の状況が「可視化結果」及びのシートに表示される。「チェックシート」の概要を図 4-3 に示すとおりであり、電力会社が選択・記入する必要があるセルは黄色塗りしている。（図 4-3 において赤枠で囲っている箇所）

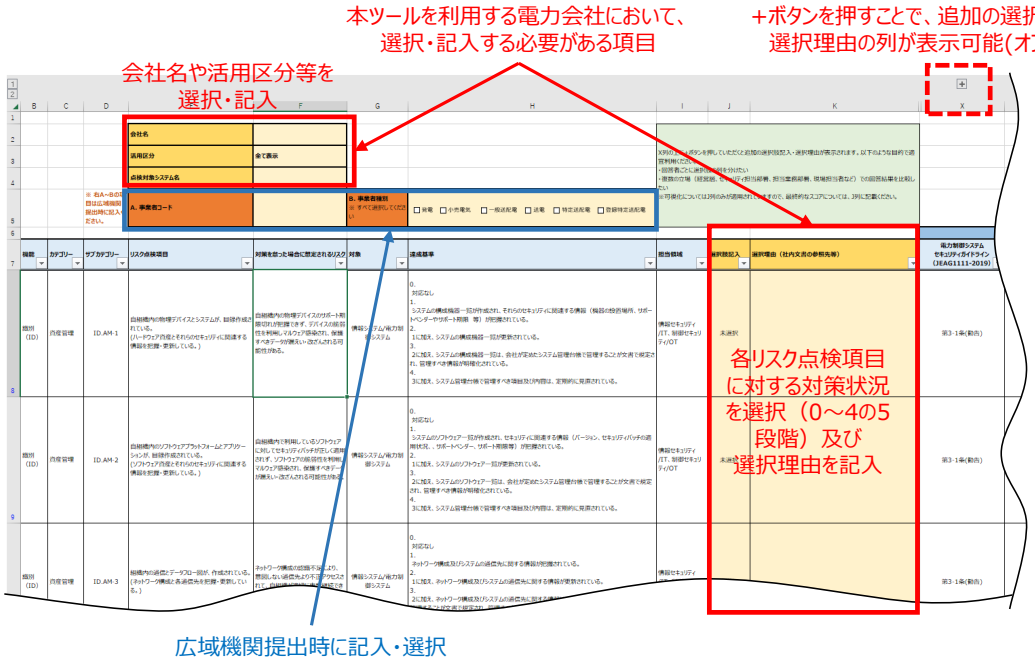


図 4-3 対策状況可視化ツールの「チェックシート」の概要

「チェックシート」では、NIST CSF ベースのリスク点検項目、当該対策を怠った場合に想定されるリス

ク、リスク点検項目に対する達成基準（0～4 の 5 段階）、リスク点検項目に関する担当領域に関する列が存在する。リスクを点検する上では関係部署との連携が必要であるところ、各点検項目の回答に適した担当領域を明記している。具体的には、経営層、情報セキュリティ/IT、制御セキュリティ/OT、人事、リスク/法務、購買/調達の 6 領域を設定しており、これらの関連する領域の部署と連携しつつ、リスク点検を進めることが望ましい。

各リスク点検項目について、リスク点検ツールの対象事業者が確認すべきガイドライン項目との対応関係も示している。本ツールでは、以下のガイドラインとの対応関係を示している。

- 電力制御システムセキュリティガイドライン（JEAG1111-2019）
- ERAB に関するサイバーセキュリティガイドライン Ver 2.0
- 小売電気事業者のためのサイバーセキュリティ対策ガイドライン Ver 1.0
- 系統連系技術要件【託送供給等約款別冊】
- 自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン（内規）
- 特定卸供給事業に係るサイバーセキュリティ確保の指針
- サイバーセキュリティ経営ガイドライン Ver 2.0

本ツールを活用する電力会社は、リスク点検項目に対する対策状況を選択する前に、まず「活用区分」を選択いただきたい。「活用区分」はプルダウン形式となっており、本ガイド及び対策状況可視化ツールが対象とする 4 つの事業区分（「発電事業者」、「小売電気事業者」、「アグリゲーター」、「自家用電気工作物設備設置者」）、「広域機関提出用」、そして「全て表示」が選択できる。「全て表示」では NIST CSF の 108 項目に対応する全てのリスク点検項目が表示されるが、事業区分を選択した場合、当該区分に関連するガイドライン項目との対応が付けられたリスク点検項目のみが抽出されて表示される。そのため、各電力会社は、「活用区分」を選択することで、自社の事業者区分に関係するリスク点検項目のみを効率的に確認することが可能である。なお、対策状況可視化ツールを用いて実施したリスク点検の結果を OCCTO に提出する場合、「広域機関提出用」を選択し、抽出されたリスク点検項目に対して選択及び選択理由を記入する必要がある。また、「広域機関提出用」は基礎的なセキュリティ点検項目のみが表示されるため、事業規模やリスク点検の経験によっては「広域機関提出用」を選択し、基礎的なリスク点検を実施することも可能である。（この活用方法の場合、「広域機関用」の項目は対象外として問題ない。）

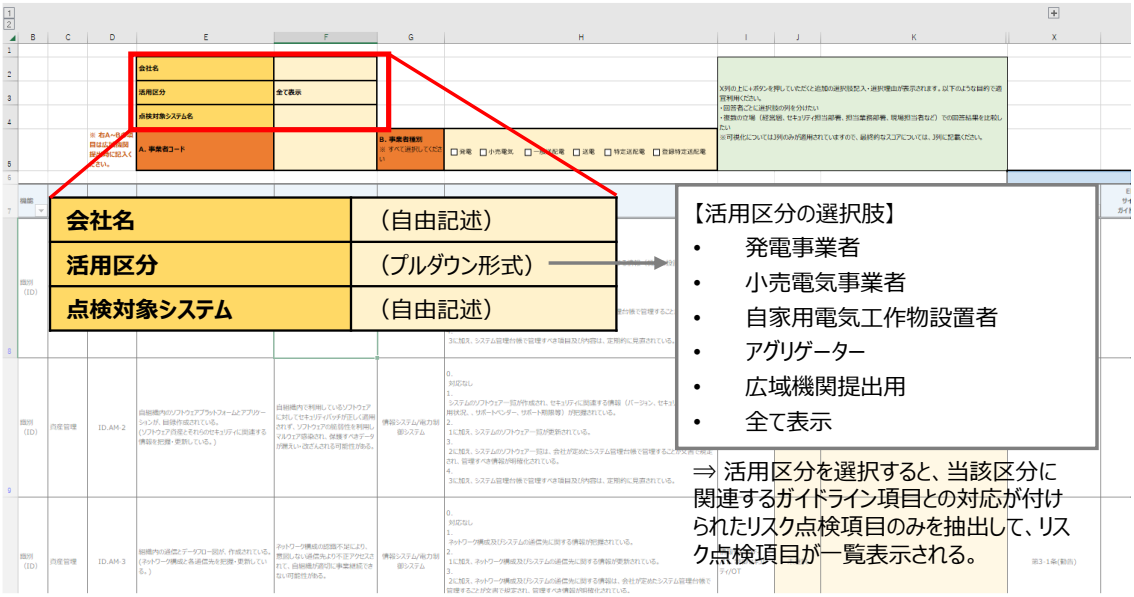


図 4-4 対策状況可視化ツールの「チェックシート」における「活用区分」の位置づけ

「活用区分」を選択後に抽出された各リスク点検項目について、図 4-3 に示すとおり、0～4 の 5 段階で、対策状況（対策レベル）の選択が必要となる。対策状況の選択にあたっては、各リスク点検項目に対する達成基準を参照し、自社の対策状況に最も近い対策状況を選択する。対策レベルについて、NIST CSF のティアの考え方と同様に各対策に関する成熟度を重要視しており、低いレベルは各対策の運用状況、高いレベルは各対策の改善に向けた制度構築状況を主に確認している。対策レベルの選択にあたっては、必要に応じて関係部署に確認することが望まれる。また、他者が選択理由を確認・レビューする可能性を踏まえ、選択理由を記載することが望まれる。記載の際には、二回目以降のリスク点検を効率的に進めるために、リスク点検にあたって活用した社内文書等の情報も合わせて明記することが望まれる。この際、記載の省力化のために、リスク点検項目に関連した社内文書の内容を転記することや、社内文書の該当項目番号を記載することも想定される。また、X 列上部の＋ボタンを押すことで、追加の選択肢記入・選択理由記入の列を表示することができる。これは、回答者ごとに選択肢の列を分けたい場合や複数の立場（経営層、セキュリティ担当部署、担当業務部署、現場担当者など）の結果を比較したい場合に活用いただきたい。

抽出されたすべてのリスク点検項目に対して対策状況を選択することで、「可視化結果」シートに対策状況が可視化される。図 4-5 に示すとおり、対策状況可視化は NIST CSF の 5 つのセキュリティ機能ごと（識別、防御、検知、対応、復旧）及び各機能のカテゴリーごとに示される。可視化されるスコアは、「活用区分」を選択後に抽出された各リスク点検項目に対する選択（0～4 の 5 段階）の平均値である。可視化された結果を踏まえ、自社の対策実施状況を確認するとともに、可視化結果に基づきセキュリティ対策の見直し・改善を行うことで、対策の継続的改善を図ることが期待される。現状の対策状況を踏まえた効果的な対策改善を行うために、可視化結果は経営層に報告することが望まれる。

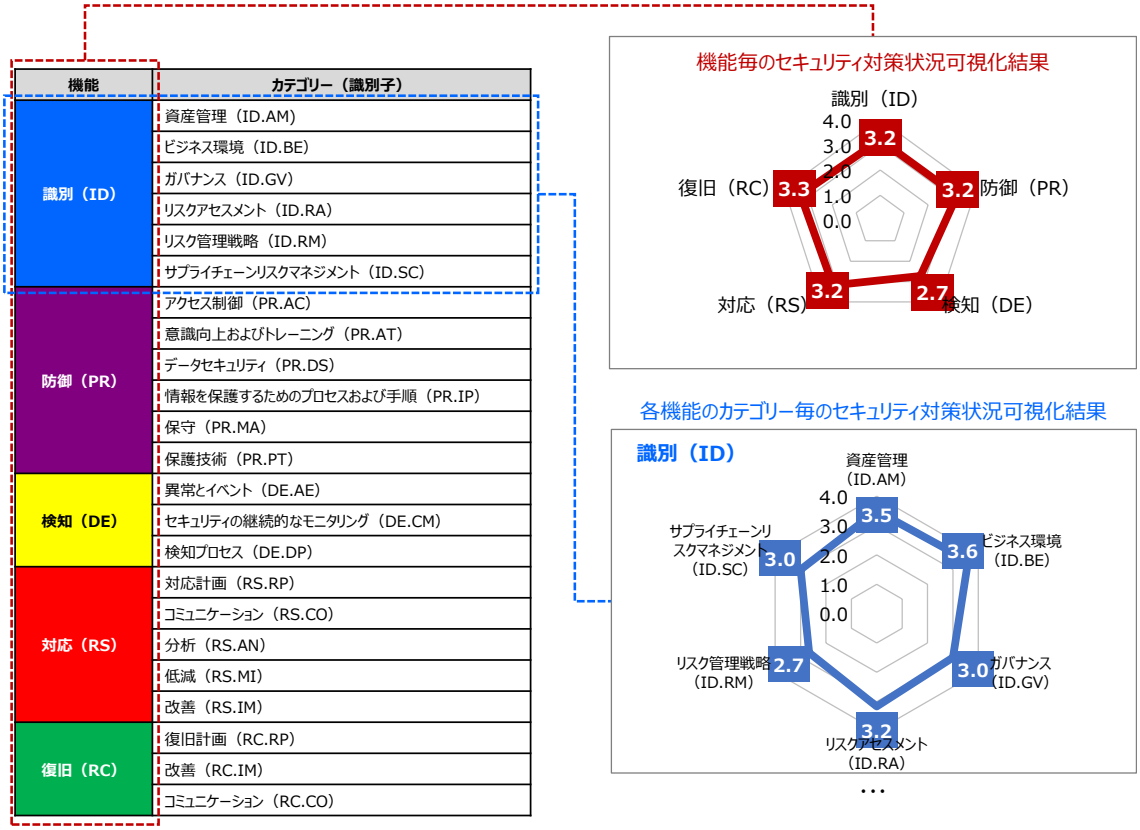


図 4-5 NIST CSF の機能・カテゴリーと対策状況可視化結果の関係

対策状況可視化ツールを用いて実施したリスク点検の結果を OCCTO に提出する場合について、OCCTO 提出用の可視化結果は「可視化結果（広域機関用）」のシートに表示される。このシートでは、OCCTO が定めた 12 のチェック項目に基づき平均スコアを算出・可視化している。可視化結果のイメージは図 4-6 に示すとおりである。

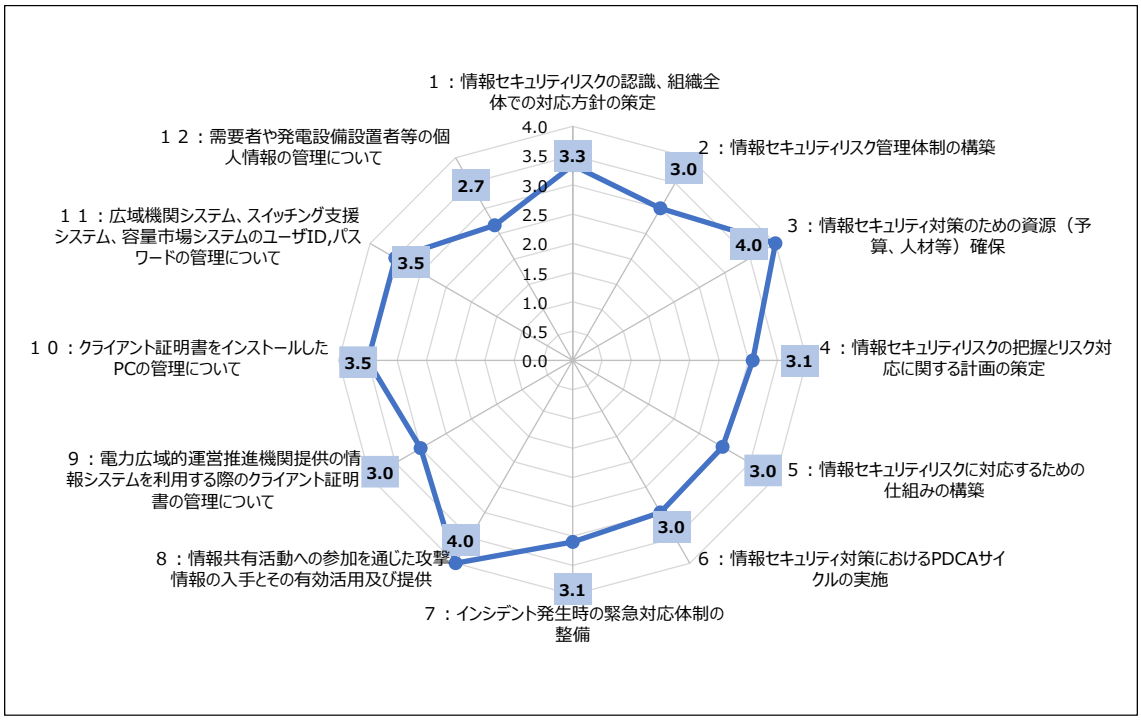


図 4-6「可視化結果（広域機関用）」シートにおける対策状況可視化結果例

5. リスク点検結果を踏まえた対策の改善方針

リスク点検結果を踏まえ、システムに対するセキュリティ対策の改善計画を講じ、当該計画に基づいて対策の改善を実施することで、PDCA サイクルに基づくセキュリティ対策の計画・実施・点検・改善のプロセスを実行することが求められる。リスク点検結果を踏まえた対策改善の基本的な考え方として、選択した対策状況の数値が低いリスク点検項目の方が十分なセキュリティ対策が講じられておらず、当該リスクに対する改善対応を優先的に検討する必要がある。ただし、本ガイド・対策状況可視化ツールのリスク点検項目は広範であり、一つの項目における対策状況の数値が低い場合でも、関連する他の項目で十分な対策ができている場合、想定されるリスクが顕在化しない場合もある。そのため、個々のリスク点検項目による評価ではなく、NIST CSF の 5 つのセキュリティ機能ごと（識別、防御、検知、対応、復旧）及び各機能のカテゴリーごとの可視化結果を踏まえ、改善検討を行う方針も想定される。いずれの方針であっても、対応する人員や予算は限られているため、現実的な工数で改善を実施するために、優先的に改善する項目をまず選定する必要がある。

優先的に改善する項目の選択について、一つの考え方として、リスク点検実施前に設定した目標値とリスク点検結果とが大きく乖離している項目について優先的に改善する方針がある。ほかにも、関連ガイドラインの「勧告的事項」と関連するリスク点検項目のうち、対策状況の数値が低いリスク点検項目について優先的に改善する方針が想定される。加えて、ガイドラインの要求事項等に依らず、対応が実施されていない「0」の対策状況である項目について、優先的に改善を行う方針も考えられる。対策の改善は事業者全体の損失に影響する問題であるため、経営層を含めた協議によって、優先的に改善する項目を決定することが望ましい。なお、改善対応にかかるコストや期間も重要となるところ、後述するリスク低減方針を検討した上で経営層と協議することが望まれる。

優先的に改善対応する項目が決まった後、具体的な対応を検討する必要がある。一般的に、リスク対応の手法は、リスク回避、リスク低減、リスク移転、リスク保有の大きく 4 つに区別されるが、本ガイドではリスク低減の方針について記載する。対応検討にあたっては、改善対応する項目について、現状の対策レベルの次の達成基準でどのような対策が求められているかを確認するとともに、当該項目に関連するガイドラインの要求事項を確認した上で、具体的な対応策を検討する必要がある。具体的な対策の検討にあたっては、当該項目に関連するガイドラインの要求事項のほか、経済産業省の「サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）」[2]が参考となる。CPSF では、産業社会を 3 つの層で捉え、各層における対策要件等を整理しているほか、添付 C では、各対策要件に対する具体的な対策例が記載されている。

優先的に改善対応するリスク点検項目に対し、CPSF を用いた対策例の検討イメージを図 5-1 に示す。CPSF の添付 D では、CPSF の対策要件と NIST CSF との対策要件の関係性が示されているため、まず改善対応する項目のサブカテゴリー（対策要件 ID）に対応する CPSF の対策要件を逆引きすることが効率的である。その後、CPSF の添付 C を用いて、具体的な対策例を検討する。CPSF の

[2] https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html

添付 C で記載されている対策例は、対策を導入・運用する際のコストや対策の対象範囲を踏まえ、Basic、Advanced、High-Advanced の 3 レベルに分かれている。改善対応にかかるコストや期間も重要となるところ、現状の対策レベル及び費用対効果を踏まえて、適切な対策を選定することが望まれる。

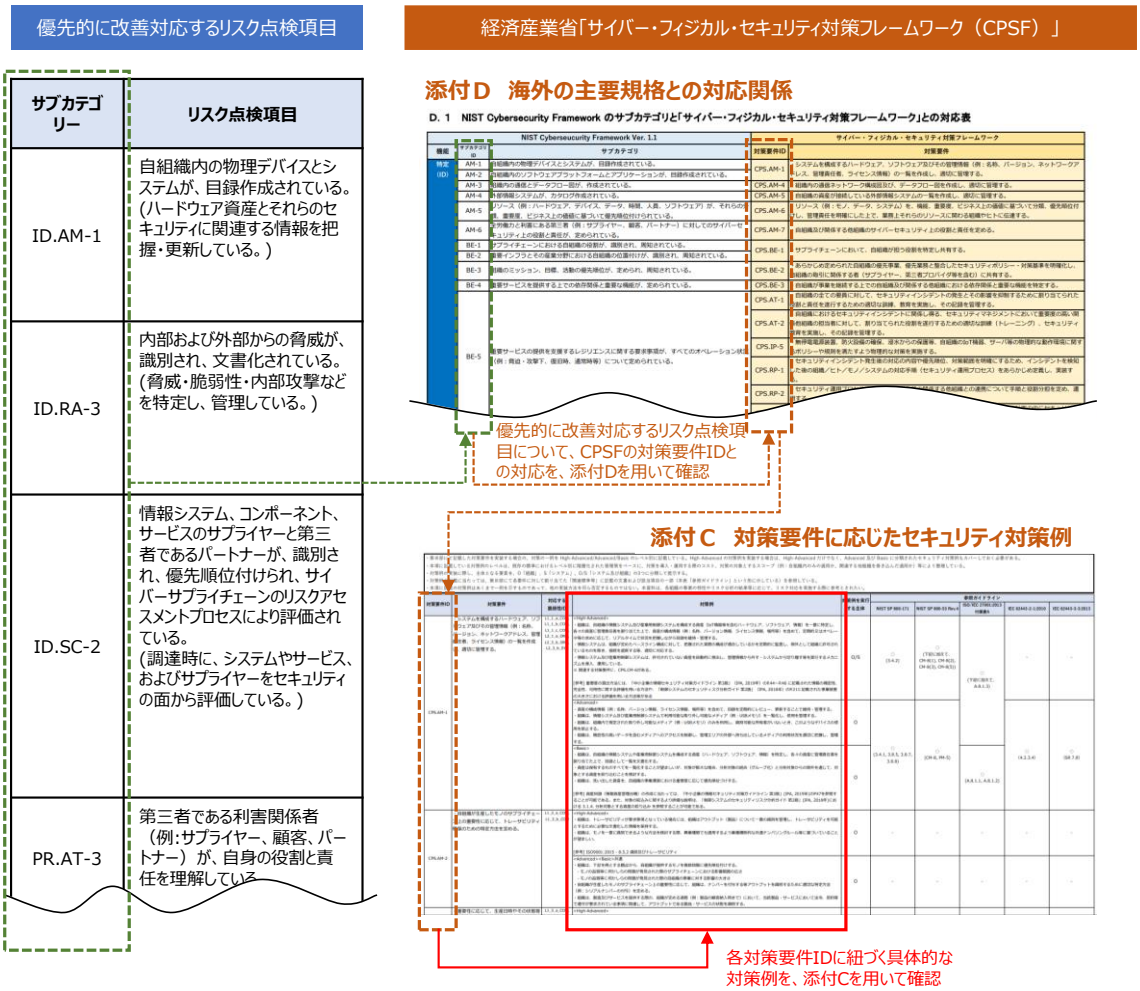


図 5-1　優先的に改善対応するリスク点検項目に対する CPSF を用いた対策例の検討方針

優先的に改善対応する項目に対する対応内容が決定した後、その内容をセキュリティ対策改善計画書としてまとめ、経営層に報告することが望まれる。なお、リスク点検は、一度のみの実施では効果は薄く、定期的に実施することで着実な改善が期待される。前述のとおり、本ガイド及び対策状況可視化ツールを用いた二回目以降のリスク点検の場合、初回のリスク点検で活用した情報に基づいて効率的なリスク点検が実施可能となる。前回に実施したリスク点検の結果も参照しつつ、最低限一年に一度、リスク点検を定期的に実施することが望まれる。

6.リスク点検項目・対策を怠った場合に想定されるリスク

NIST CSF の各機能・カテゴリー・サブカテゴリーに基づく 108 のリスク点検項目及び当該対策を怠った場合に想定されるリスクは以下に示すとおりである。

機能	カテゴリー	サブカテゴリー	リスク点検項目	対策を怠った場合に想定されるリスク
識別（ID）	資産管理	ID.AM-1	自組織内の物理デバイスとシステムが、目録作成されている。(ハードウェア資産とそれらのセキュリティに関連する情報を把握・更新している。)	自組織内の物理デバイスのサポート期限切れが把握できず、デバイスの脆弱性を利用しマルウェア感染され、保護すべきデータが漏えい・改ざんされる可能性がある。
識別（ID）	資産管理	ID.AM-2	自組織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が、目録作成されている。(ソフトウェア資産とそれらのセキュリティに関連する情報を把握・更新している。)	自組織内で利用しているソフトウェアに対してセキュリティパッチが正しく適用されず、ソフトウェアの脆弱性を利用しマルウェア感染され、保護すべきデータが漏えい・改ざんされる可能性がある。
識別（ID）	資産管理	ID.AM-3	組織内の通信とデータフロー図が、作成されている。(ネットワーク構成と各通信先を把握・更新している。)	ネットワーク構成の認識不足により、意図しない通信先より不正アクセスされて、自組織が適切に事業継続できない可能性がある。
識別（ID）	資産管理	ID.AM-4	外部情報システムが、カタログ作成されている。(外部連携先システムを把握・更新している。)	意図しない外部情報システムからの接続により、通信経路上でデータを改ざんする中間者攻撃を受けて、保護すべきデータが漏えい・改ざんされる可能性がある。

機能	カテゴリー	サブ カテゴリー	リスク点検項目	対策を怠った場合に 想定されるリスク
識別 （ID）	資産管理	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）が、それらの分類、重要度、ビジネス上の価値に基づいて優先順位付けられている。 (システム資産・情報資産に対する重要度分類基準があり、資産はこれに基づいて分類されている。また、これらの基準が更新されている。)	システムの管理不足により、認識していないシステムが高負荷攻撃を受けて、自組織のシステムが停止する可能性がある。
識別 （ID）	資産管理	ID.AM-6	全従業員及び利害関係にある第三者（例:サプライヤー、顧客、パートナー）に対してのサイバーセキュリティ上の役割と責任が、定められている。 (システムの関係者に対し、セキュリティ上の役割と責任を定めている。)	他組織で発生したセキュリティインシデントにより、自組織が適切に事業継続できない可能性がある。
識別 （ID）	ビジネス 環境	ID.BE-1	サプライチェーンにおける自組織の役割が、識別され、周知されている。 (自社のサプライチェーン全体における組織の役割を特定し、社内の関係者やサプライヤーとの間で共有されている。)	自組織のセキュリティインシデントにより、取引関係者が適切に事業継続できない可能性がある。

機能	カテゴリー	サブ カテゴリー	リスク点検項目	対策を怠った場合に 想定されるリスク
識別 （ID）	ビジネス 環境	ID.BE-2	重要インフラとその産業分野における自組織の位置づけが、識別され、周知されている。 (経営戦略・事業ニーズ等を基に策定されたシステム戦略やシステムアーキテクチャが社内に周知されている。)	自組織のセキュリティインシデントにより、関係する他組織が適切に事業継続できない可能性がある。
識別 （ID）	ビジネス 環境	ID.BE-3	組織のミッション、目標、活動の優先順位が、定められ、周知されている。 (自組織におけるミッション、事業目標、リスク管理活動の優先順位がリスク管理基準によって定めており、その周知に努めている。)	優先順位が高いセキュリティインシデントの対応が遅れたことにより、自組織が適切に事業継続できない可能性がある。
識別 （ID）	ビジネス 環境	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が、定められている。 (重要サービスの提供に必要な重要資産と関連サプライヤーを把握・更新している。)	重要なサプライヤーで発生したセキュリティインシデントにより、自組織が適切に事業継続できない可能性がある。
識別 （ID）	ビジネス 環境	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が、すべてのオペレーション状況（例：脅迫・攻撃下、復旧時、通常時等）について定められている。 （重要サービスに求められるサービスレベルと要求事項が整理・更新されている。）	本来達成すべきサービスレベルに達していない重要サービスが攻撃されることで、適切に事業継続できない可能性がある。

機能	カテゴリー	サブ カテゴリー	リスク点検項目	対策を怠った場合に 想定されるリスク
識別 （ID）	ガバナンス	ID.GV-1	組織のサイバーセキュリティポリシーが、定められ、周知されている。 （組織のサイバーセキュリティポリシーが規定され、社内に周知されている。）	ID・パスワードなどの窃取による正規のユーザへのなりすましによって、保護すべきデータが漏えい・改ざんされる可能性がある。
識別 （ID）	ガバナンス	ID.GV-2	サイバーセキュリティ上の役割と責任が、内部の担当者と外部パートナーとで調整・連携されている。 (セキュリティ対策は、社外の委託先やパートナーを含めて連携して実施している。)	管理されてないリソースに対して高負荷攻撃を受けて、自組織のシステムが停止する可能性がある。
識別 （ID）	ガバナンス	ID.GV-3	プライバシーや人権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が、理解され、管理されている。 (セキュリティ・プライバシーに関する法制度を把握・対応している。)	法制度等で規定されている水準のセキュリティ対策を実装できず、自組織のシステムの停止される可能性がある。
識別 （ID）	ガバナンス	ID.GV-4	ガバナンスとリスクマネジメントプロセスが、サイバーセキュリティリスクに対処している。 (サイバーリスクを特定し、リスク管理手法の検討に利用している。)	特定されていないサイバーセキュリティリスクを悪用した攻撃により、保護すべきデータが漏えい・改ざんされる可能性がある。
識別 （ID）	リスクアセスメント	ID.RA-1	資産の脆弱性が、識別され、文書化されている。 (システムの脆弱性を特定し管理している。)	システムにおけるセキュリティ上の脆弱性を利用しマルウェア感染され、保護すべきデータが漏えい・改ざんされる可能性がある。

機能	カテゴリー	サブカテゴリー	リスク点検項目	対策を怠った場合に想定されるリスク
識別（ID）	リスクアセスメント	ID.RA-2	サイバー脅威に関する情報が、複数の情報共有フォーラム及び複数のソースから入手されている。（サイバー脅威に関する情報を複数のソースから入手している。）	未知の脅威によってシステムがマルウェア感染し、保護すべきデータが漏えい・改ざんされる可能性がある。
識別（ID）	リスクアセスメント	ID.RA-3	内部及び外部からの脅威が、識別され、文書化されている。(脅威・脆弱性・内部攻撃などを特定し、管理している。)	未知の脅威によってシステムがマルウェア感染し、保護すべきデータが漏えい・改ざんされる可能性がある。
識別（ID）	リスクアセスメント	ID.RA-4	ビジネスに対する潜在的な影響とその発生可能性が、識別されている。(セキュリティリスクが顕在化する可能性と、顕在化した場合の影響を把握・分類している。)	セキュリティリスクが顕在化した際の影響が適切に評価されないことで、セキュリティ対策が過少となり、攻撃を受けた場合に適切に事業継続できない可能性がある。
識別（ID）	リスクアセスメント	ID.RA-5	脅威、脆弱性、発生可能性、影響が、リスクを判断する際に使用されている。(脅威情報、脆弱性情報、発生可能性、影響度から、リスクを管理している。)	セキュリティリスクが顕在化した際の影響が適切に評価されないことで、セキュリティ対策が過少となり、攻撃を受けた場合に適切に事業継続できない可能性がある。
識別（ID）	リスクアセスメント	ID.RA-6	リスク対応が、識別され、優先順位付けされている。（リスク対応計画が作成され、優先度付けされている。）	セキュリティリスクが顕在化した際の対応が優先度付けされないことで、本来対策すべき箇所にセキュリティ対策が実施できず、攻撃を受けた場合に適切に事業継続できない可能性がある。

機能	カテゴリー	サブカテゴリー	リスク点検項目	対策を怠った場合に想定されるリスク
識別（ID）	リスク管理戦略	ID.RM-1	リスクマネジメントプロセスが、組織の利害関係者によって定められ、管理され、承認されている。 (セキュリティリスク管理プロセスが策定され、運用・管理されている。)	セキュリティリスクが顕在化した際の影響が適切に管理されないことで、セキュリティ対策が過少となり、攻撃を受けた場合に適切に事業継続できない可能性がある。
識別（ID）	リスク管理戦略	ID.RM-2	組織のリスク許容度が、決定され、明確に表現されている。 (セキュリティリスク対策の実施基準が策定されている。)	セキュリティリスク許容度が適切に評価されないことで、セキュリティ対策が過少となり、攻撃を受けた場合に適切に事業継続できない可能性がある。
識別（ID）	リスク管理戦略	ID.RM-3	自組織によるリスク許容度の決定が、重要インフラにおける組織の役割と、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。 (リスク対策の実施基準が社会への影響や重要システム・サービスを考慮して定められている。)	セキュリティリスク許容度が適切に評価されないことで、セキュリティ対策が過少となり、攻撃を受けた場合に適切に事業継続できない可能性がある。
識別（ID）	サプライチェーンリスクマネジメント	ID.SC-1	サイバーサプライチェーンのリスクマネジメントプロセスが、組織の利害関係者によって、識別され、定められ、評価され、管理され、承認されている。 (サプライチェーンにおけるセキュリティリスク管理手法が、社内で確立されている。)	サプライチェーンに関するセキュリティリスク許容度が適切に評価されないことで、サプライチェーンに関するセキュリティ対策が過少となり、攻撃を受けた場合に自組織が適切に事業継続できない可能性があるほか、第三者の事業継続に影響を及ぼす可能性がある。

機能	カテゴリー	サブカテゴリー	リスク点検項目	対策を怠った場合に想定されるリスク
識別（ID）	サプライチェーンリスクマネジメント	ID.SC-2	情報システム、コンポーネント、サービスのサプライヤーと第三者であるパートナーが、識別され、優先順位付けられ、サイバーサプライチェーンのリスクアセスメントプロセスにより評価されている。 (調達時に、システムやサービス、及びサプライヤーをセキュリティの面から評価している。)	他組織の管理するシステムにおけるセキュリティ上の脆弱性を利用しマルウェア感染され、関係する他組織で管理している領域から自組織の保護すべきデータが漏えい・改ざんされる可能性がある。
識別（ID）	サプライチェーンリスクマネジメント	ID.SC-3	サプライヤー及び第三者であるパートナーとの契約が、組織のサイバーセキュリティプログラムやサイバーサプライチェーンのリスクマネジメント計画の目的を達成するための適切な対策の実施に活用されている。 (調達時の契約は、サプライチェーンにおけるセキュリティリスクへの対応が考慮されている。)	自組織のデータを格納している他組織のシステムがマルウェア感染することで、自組織の保護すべきデータが漏えい・改ざんされる可能性がある。
識別（ID）	サプライチェーンリスクマネジメント	ID.SC-4	サプライヤー及び第三者であるパートナーが、監査、テストの結果、又はその他の評価に基づき、契約上の義務を満たしているか、定期的に評価されている。 (サプライチェーンにおけるセキュリティリスクをサプライヤーやパートナーに対して定期的に評価している。)	自組織のデータを格納している他組織のシステムがマルウェア感染することで、自組織の保護すべきデータが漏えい・改ざんされる可能性がある。

機能	カテゴリー	サブカテゴリー	リスク点検項目	対策を怠った場合に想定されるリスク
識別（ID）	サプライチェーンリスクマネジメント	ID.SC-5	対応・復旧計画の策定とテストが、サプライヤー及び第三者プロバイダーと共に行なわれている。 (会社のインシデント対応計画・復旧計画は、サプライヤー等を含めて考慮されている。)	他組織を考慮した対応・復旧計画が策定されず、自組織のセキュリティインシデントが発生した際に、関係する他組織が適切に事業継続できない可能性がある。
防御（PR）	アクセス制御	PR.AC-1	認可されたデバイス、ユーザ、プロセスのアイデンティティと証明書が、発行、管理、検証、取り消し、監査されている。 (ユーザの識別情報と認証情報の管理されている。)	不適切な認証情報の管理により、正規ユーザによる内部不正が行われ、保護すべきデータが漏えい・改ざんされる可能性がある。
防御（PR）	アクセス制御	PR.AC-2	資産に対する物理アクセスが、管理され、保護されている。 （システムの構成機器が物理的に保護され、物理アクセスに対する対策が施されている。）	適切な物理的な対策が実施されず、悪意を持った自組織内外の関係者が不正に侵入し、故障や正確でないデータの送信等が発生する可能性がある。
防御（PR）	アクセス制御	PR.AC-3	リモートアクセスが、管理されている。 （リモートアクセスのセキュリティ対策や管理基準が規定・運用されている。）	リモートアクセスの管理不足により、悪意のある第三者が正規ユーザへなりすまし、保護すべきデータが漏えい・改ざんされる可能性がある。

機能	カテゴリー	サブカテゴリー	リスク点検項目	対策を怠った場合に想定されるリスク
防御（PR）	アクセス制御	PR.AC-4	アクセスの許可及び認可が、最小権限の原則及び役割の分離の原則を組み入れて、管理されている。(システムに対する ID の発行、アクセス権限の付与が必要最小限となるよう、また利用者に対し個別の ID が発行されるよう管理している。)	共通 ID を発行し、その共通 ID が外部に漏えいした場合に、正規のユーザへのなりすましによって遠隔からシステムに不正アクセスされ、システムが不正操作される可能性がある。
防御（PR）	アクセス制御	PR.AC-5	ネットワークの完全性が、保護されている（例:ネットワークの分離、ネットワークのセグメント化）。(セキュリティレベルに応じたネットワーク分離を行っている。)	重要システムのネットワークに適切な防護措置がされず、通信経路上でデータを改ざんする中間者攻撃を受けて、保護すべきデータが漏えい・改ざんされる可能性がある。
防御（PR）	アクセス制御	PR.AC-6	ID は、ID 利用者の本人確認がなされ、証明書に紐付けられ、インタラクションで使用されている。(システムが利用者の本人確認と利用資格の確認を行っている。)	利用者の本人確認がされず、悪意のある組織内外の関係者が正規ホストへなりすまし、システム内部に不正アクセスされ、システムが不正操作される可能性がある。
防御（PR）	アクセス制御	PR.AC-7	ユーザ、デバイス、その他の資産は、トランザクションのリスク（例:個人のセキュリティ及びプライバシー上のリスク、その他組織にとってのリスク）の度合いに応じた認証（例:多要素認証など）が行われている。(リスクに応じた認証方式を採用している)	重要システムに適切な認証方法が設定されず、第三者が正規のホストになりすまし、自組織で利用しているシステムに不正アクセスされ、システムが不正操作される可能性がある。

機能	カテゴリー	サブカテゴリー	リスク点検項目	対策を怠った場合に想定されるリスク
防御（PR）	意識向上及びトレーニング	PR.AT-1	すべてのユーザは、情報が周知され、トレーニングが実施されている。(セキュリティに関する社員の意識啓発や教育を実施している。)	悪意を持った自組織内の関係者が保護すべきデータを持ち出したことによって、保護すべきデータが漏えい・改ざんされる可能性がある。
防御（PR）	意識向上及びトレーニング	PR.AT-2	権限を持つユーザが、自身の役割と責任を理解している。(システム利用者が、自身が実施すべきセキュリティ対策とその責任を理解している。)	セキュリティ責任を理解していない自組織内の関係者が不正にデータを改ざんすることで、システムの異常動作等の意図しない動作が生じる可能性がある。
防御（PR）	意識向上及びトレーニング	PR.AT-3	第三者である利害関係者（例:サプライヤー、顧客、パートナー）が、自身の役割と責任を理解している。（サプライヤーやパートナーが、セキュリティ管理における役割と責任を理解している。）	セキュリティ責任を理解していない利害関係者が不正にデータを改ざんすることで、機器の破損等の意図しない品質劣化が生じる可能性がある。
防御（PR）	意識向上及びトレーニング	PR.AT-4	上級役員（セキュリティ担当役員）が、自身の役割と責任を理解している。（任命されたセキュリティ責任者が、セキュリティに関する責任を担い、役割を発揮している。）	上級役員の判断の遅れにより、自組織のセキュリティインシデントに対して適切な対応がなされず、自組織が事業継続できない可能性がある。
防御（PR）	意識向上及びトレーニング	PR.AT-5	物理セキュリティ及びサイバーセキュリティの担当者が、自身の役割と責任を理解している。（物理的なサイバーセキュリティ確保の担当者が、対策を実施・管理している。）	重要区画に対して物理的対策がされず、社内関係者が重要区画に不正に侵入し、保護すべきデータが漏えい・改ざんされる可能性がある。

機能	カテゴリー	サブカテゴリー	リスク点検項目	対策を怠った場合に想定されるリスク
防御（PR）	データセキュリティ	PR.DS-1	保存されているデータが、保護されている。(システムや電子記憶媒体に保存した重要なデータに対して、セキュリティ対策を行っている。)	重要なデータに対する対策が不十分であり、データが漏えい・改ざんされる可能性がある。
防御（PR）	データセキュリティ	PR.DS-2	伝送中のデータが、保護されている。(伝送中の重要なデータに対し、セキュリティ対策を行っている。)	重要データの伝送において正しい対策がされず、中間者攻撃を受けて、保護すべきデータが漏えい・改ざんされる可能性がある。
防御（PR）	データセキュリティ	PR.DS-3	資産は、撤去、譲渡、廃棄に至るまで、正式に管理されている。（システムの撤去、譲渡、廃棄方法が定義・運用されている。）	不正な機器がシステムに接続され、故障や正確でないデータの送信などが発生する可能性がある。
防御（PR）	データセキュリティ	PR.DS-4	可用性を確保するのに十分な容量が、維持されている。（システムの安定稼働を行うためのリソースが想定・確保されている。）	システム障害に対する対策が不足し、システムを構成する IT 機器、通信機器等が高負荷攻撃を受けて、IT 機器や通信機器の機能が停止する可能性がある。
防御（PR）	データセキュリティ	PR.DS-5	データ漏えいに対する防御対策が、実装されている。（重要なデータの特定とそのデータに対する情報漏えい対策を管理・実施している。）	重要なデータが暗号化されず、保護すべきデータが漏えい・改ざんされる可能性がある。
防御（PR）	データセキュリティ	PR.DS-6	完全性チェックメカニズムが、ソフトウェア、ファームウェア、及び情報の完全性を検証するために使用されている。(システムの改ざんを管理・検証している。)	システムのファイル更新の検証不足のため、不正のアップデートが実施され、保護すべきデータが改ざんされる可能性がある。

機能	カテゴリー	サブ カテゴリー	リスク点検項目	対策を怠った場合に 想定されるリスク
防御 （PR）	データセキュリティ	PR.DS-7	開発・テスト環境が、実稼働環境から分離されている。 （システムの本番環境と開発・テスト環境のネットワークが分離されている。）	開発中の脆弱性があるパッチが間違って IT 機器に適用されたことによって、脆弱性を悪用した不正アクセスが行われ、事前に想定されていない動作をする可能性がある。
防御 （PR）	データセキュリティ	PR.DS-8	完全性チェックメカニズムが、ハードウェアの完全性を検証するために使用されている。 (システムの構成機器の完全性（不正な変更など）を確認している。)	正規の機器を模した偽造品の挿入によって、システムの異常動作等の意図しない動作が生じる可能性がある。
防御 （PR）	情報を保護するためのプロセス及び手順	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構成は、セキュリティ原則 （例:最低限の機能性の概念）を組み入れて、定められ、維持されている。 (セキュリティを考慮したシステムの設計標準を作成・利用している。)	セキュリティ設計が不十分のため、システムに残存したセキュリティ上の脆弱性が悪用され、自組織のシステムが停止する可能性がある。
防御 （PR）	情報を保護するためのプロセス及び手順	PR.IP-2	システムを管理するためのシステム（開発）ライフサイクルが、実装されている。 (システムのライフサイクルを定義・運用している。)	システムの運用・保守段階で実施すべき事項の検討不足により、システムにおけるセキュリティ上の脆弱性を利用しマルウェア感染され、保護すべきデータが漏えい・改ざんされる可能性がある。
防御 （PR）	情報を保護するためのプロセス及び手順	PR.IP-3	構成変更管理プロセスは、策定されている。 （システムの構成変更管理プロセスが策定・運用されている。）	構成管理変更が正しく管理されず、システムに残存した脆弱性を悪用して不正アクセスされ、保護すべきデータが漏えい・改ざんされる可能性がある。

機能	カテゴリー	サブカテゴリー	リスク点検項目	対策を怠った場合に想定されるリスク
防御（PR）	情報を保護するためのプロセス及び手順	PR.IP-4	情報のバックアップが、実施され、維持され、テストされている。（システム復旧に必要なデータがバックアップされ、復旧テストが行われている。）	情報のバックアップがないため、自組織のセキュリティインシデントから復旧できず、自組織が適切に事業継続できない可能性がある。
防御（PR）	情報を保護するためのプロセス及び手順	PR.IP-5	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が、満たされている。（システム環境の運用対策（例：災害対策、入退室管理など）が規定・運用されている。）	入退室管理が正しく実施されず、悪意を持った自組織内外の関係者による計測機能に対する不正行為が行われ、システムが停止する可能性がある。
防御（PR）	情報を保護するためのプロセス及び手順	PR.IP-6	データは、ポリシーに従って破壊されている。(データ消去又は読み取りできない状態にする場合は、不正利用を防ぐよう対策している。)	データが残存する廃棄済みの記録媒体が、悪意を持った自組織内外の関係者に持ち出されたことによって、保護すべきデータが漏えい・改ざんされる可能性がある。
防御（PR）	情報を保護するためのプロセス及び手順	PR.IP-7	防御プロセスは、改善されている。(セキュリティ関連情報を収集して、セキュリティ対策の改善を図っている。)	最新の脆弱性情報が把握できず、システムにおけるセキュリティ上の脆弱性を利用しマルウェア感染され、保護すべきデータが漏えい・改ざんされる可能性がある。
防御（PR）	情報を保護するためのプロセス及び手順	PR.IP-8	防御技術の有効性に関する情報が、共有されている。(最新のセキュリティ対策技術の収集と共有が行われている。)	最新の脆弱性情報が把握できず、システムにおけるセキュリティ上の脆弱性を利用しマルウェア感染され、保護すべきデータが漏えい・改ざんされる可能性がある。

機能	カテゴリー	サブカテゴリー	リスク点検項目	対策を怠った場合に想定されるリスク
防御（PR）	情報を保護するためのプロセス及び手順	PR.IP-9	対応計画と復旧計画が、策定され、管理されている。(セキュリティインシデントが発生した場合のインシデント対応計画、業務継続計画、システム復旧計画を策定している。)	システム復旧計画の検討不足のため、セキュリティインシデントが発生した際に、適切に事業継続できない可能性がある。
防御（PR）	情報を保護するためのプロセス及び手順	PR.IP-10	対応計画と復旧計画が、テストされている。(セキュリティインシデントが発生した場合のインシデント対応計画、業務継続計画、システム復旧計画について、訓練や演習を行っている。)	システム復旧テストを実施できておらず、セキュリティインシデントが発生した際に、関係する他組織が適切に事業継続できない可能性がある。
防御（PR）	情報を保護するためのプロセス及び手順	PR.IP-11	サイバーセキュリティには、人事に関わるプラクティス（例:アクセス権限の無効化、人員のスクリーニング）が含まれている。（人員の採用時・退職時・異動時にサイバーセキュリティを考慮した対策が実施されている。)	退職する社員が把握していたセキュリティに関する重要データが漏えいする可能性がある。
防御（PR）	情報を保護するためのプロセス及び手順	PR.IP-12	脆弱性管理計画が、作成され、実装されている。（脆弱性情報を収集・特定し、対応手順が管理されている。)	最新の脆弱性情報が把握できず、システムにおけるセキュリティ上の脆弱性を利用しマルウェア感染され、保護すべきデータが漏えい・改ざんされる可能性がある。

機能	カテゴリー	サブ カテゴリー	リスク点検項目	対策を怠った場合に 想定されるリスク
防御 （PR）	保守	PR.MA-1	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実施され、ログが記録されている。 (システム上の作業は、承認を受け、手順に則って行われ、記録されている。)	システム上の作業が記録されないことで、インシデント発生時の原因が特定できず、自組織が適切に事業継続できない可能性がある。
防御 （PR）	保守	PR.MA-2	組織の資産に対する遠隔保守は、承認を得て、ログが記録され、不正アクセスを防止した形式で実施されている。 (遠隔保守用の回線を保護し、アクセスを制限・管理している。)	遠隔保守用の回線が不正アクセスされ、保護すべきデータが漏えい・改ざんされる可能性がある。
防御 （PR）	保護技術	PR.PT-1	監査記録/ログ記録の対象が、ポリシーに従って決定され、文書化され、実装され、その記録をレビューされている。 (システムの重要度によってログの取得・保護を実施している。)	システムのログが取得されないことで、インシデント発生時の原因が特定できず、自組織が適切に事業継続できない可能性がある。
防御 （PR）	保護技術	PR.PT-2	リムーバブルメディアは、保護され、その使用がポリシーに従って制限されている。 (外部記憶媒体のルールが策定され、運用されている。)	外部記録媒体が管理されず、悪意ある関係者が保護すべきデータを不正に持出すことによって、保護すべきデータが漏えい・改ざんする可能性がある。

機能	カテゴリー	サブ カテゴリー	リスク点検項目	対策を怠った場合に 想定されるリスク
防御 （PR）	保護技術	PR.PT-3	最低限の機能性の原則が、必須の機能のみ提供するようにシステムを構成することによって組み入れられている。 (システムはユーザやクライアントに応じて、必要最低限の機能を提供している。)	重要システムに適切な認証方法が設定されず、第三者が正規のホストになりすまし、自組織で利用しているシステムに不正アクセスされ、システムが不正操作される可能性がある。
防御 （PR）	保護技術	PR.PT-4	情報通信ネットワークと制御ネットワークが、分離して保護されている。 （外部ネットワーク、社内ネットワーク、重要なネットワークが区別され、それぞれで適した防御策を実施・管理している。）	情報通信ネットワークで発生したインシデントの影響が制御ネットワークに及ぶことで、制御システムが停止する可能性がある。
防御 （PR）	保護技術	PR.PT-5	メカニズム（例:フェールセーフ、ロードバランシング、ホットスワップ）が、平時及び緊急時においてレジリエンスに関する要求事項を達成するために実装されている。 (システムの可用性を高めるための機能を設計・実装している。)	不正な機器に対する高負荷攻撃によって、安全に支障をきたす動作をする可能性がある。
検知 （DE）	異常とイベント	DE.AE-1	ネットワーク運用のベースラインと、ユーザとシステムで期待されるデータフローが、定められ、管理されている。 (正常時のネットワークのベースラインを作成し、異常を検知している。)	通常時のネットワーク通信が把握できず、システムに対する不正アクセスを特定できない可能性がある。

機能	カテゴリー	サブカテゴリー	リスク点検項目	対策を怠った場合に想定されるリスク
検知（DE）	異常とイベント	DE.AE-2	検知したイベントは、攻撃の標的と手法を理解するために分析されている。（セキュリティ事象の分析手法を管理・運用している。）	インシデントの原因が分析できず、再度セキュリティインシデントが発生し、自組織が適切に事業継続できない可能性がある。
検知（DE）	異常とイベント	DE.AE-3	イベントデータは、複数の情報源やセンサーから収集され、相互分析されている。（セキュリティ事象に関連するデータが、複数の情報源から収集・分析されている。）	セキュリティ事象に関連するデータが取得されないことで、インシデント発生時の原因が特定できず、自組織が適切に事業継続できない可能性がある。
検知（DE）	異常とイベント	DE.AE-4	セキュリティ事象がもたらす影響が、判断されている。（セキュリティ事象の影響度を特定し、適宜共有・分析している。）	セキュリティ事象に関連するデータが分析されないことで、インシデントの兆候や発生を特定できず、自組織が適切に事業継続できない可能性がある。
検知（DE）	異常とイベント	DE.AE-5	インシデント警告の閾値が、定められている。(インシデント発生を宣言する基準が明確になっている。)	インシデント警告の閾値が定められないことで、インシデントの兆候や発生を特定できず、自組織が適切に事業継続できない可能性がある。
検知（DE）	セキュリティの継続的なモニタリング	DE.CM-1	ネットワークは、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。（ネットワークのログが取得され、原因調査・異常検知に利用されている。）	ネットワークのログが取得されないことで、インシデント発生時の原因が特定できず、自組織が適切に事業継続できない可能性がある。
検知（DE）	セキュリティの継続的なモニタリング	DE.CM-2	物理環境は、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。（物理的な侵入検知対策が実施・運用されている。）	保護が必要なエリアに対する物理的な不正侵入が検知できず、保護すべきデータが漏えい・改ざんされる可能性がある。

機能	カテゴリー	サブカテゴリー	リスク点検項目	対策を怠った場合に想定されるリスク
検知（DE）	セキュリティの継続的なモニタリング	DE.CM-3	人員の活動は、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。（システムの利用者の活動のログ取得し、活用している。）	システム利用者の活用ログが取得されないことで、自組織における悪意ある関係者の保護すべきデータの適切でない持出行為を検知できず、保護すべきデータが漏えい・改ざんする可能性がある。
検知（DE）	セキュリティの継続的なモニタリング	DE.CM-4	悪質なコードは、検知されている。(マルウェア等の悪意あるプログラムを検知できる対策を実施・管理している。)	マルウェア等の悪意あるプログラムが検知できず、端末に対するマルウェア攻撃によって、保護すべきデータが漏えい・改ざんされる可能性がある。
検知（DE）	セキュリティの継続的なモニタリング	DE.CM-5	不正なモバイルコード（Web サイトなどを通してダウンロードされる不正なスクリプトコードなど）は、検知されている。（不正なコードを検知できる仕組みが構築されている。）	端末に対する不正コードによる攻撃が検知できず、保護すべきデータが漏えい・改ざんされる可能性がある。
検知（DE）	セキュリティの継続的なモニタリング	DE.CM-6	（業務委託先など）外部サービスプロバイダーの活動は、潜在的なサイバーセキュリティ事象を検知できるようにモニタリングされている。(委託先企業や協力会社の活動を、セキュリティの観点で監視している。)	他組織の管理するシステムがマルウェア感染することによって、他組織で管理している領域から自組織の保護すべきデータが漏えい・改ざんされる可能性がある。
検知（DE）	セキュリティの継続的なモニタリング	DE.CM-7	権限のない人員、接続、デバイス、ソフトウェアのモニタリングが、実施されている。（ユーザの認証・PC・ソフトウェアのログが取得され、不正利用の検知などに利用している。）	悪意のある関係者がソフトウェアを不正にインストールすることで、保護すべきデータが漏えい・改ざんされる可能性がある。

機能	カテゴリー	サブカテゴリー	リスク点検項目	対策を怠った場合に想定されるリスク
検知（DE）	セキュリティの継続的なモニタリング	DE.CM-8	脆弱性スキャンが、実施されている。 (システムに対し脆弱性診断を実施している。)	システムに残存した脆弱性を特定できず、その脆弱性を悪用したマルウェア攻撃によって保護すべきデータが漏えい・改ざんされる可能性がある。
検知（DE）	検知プロセス	DE.DP-1	検知に関する役割と責任は、説明責任を果たせるように明確に定義されている。 （異常検知され場合の対応方針・体制が策定・運用されている。）	システムの異常が正しく検知されないことで、インシデントの発生の特定できず、自組織が適切に事業継続できない可能性がある。
検知（DE）	検知プロセス	DE.DP-2	検知活動は、該当するすべての要求事項を準拠している。 （異常検知するための項目を定め、検知活動を実施している。）	システムの異常が正しく検知されないことで、インシデントの発生の特定できず、自組織が適切に事業継続できない可能性がある。
検知（DE）	検知プロセス	DE.DP-3	検知プロセスが、テストされている。 （異常検知プロセスが構築・テストされている。）	システムの異常が正しく検知されないことで、インシデントの発生の特定できず、自組織が適切に事業継続できない可能性がある。
検知（DE）	検知プロセス	DE.DP-4	イベント検知情報が、周知されている。 （異常が検知された際の、情報共有体制・手順が運用されている。）	システムの異常が関係者に適切に共有されず、インシデント対応に遅れが生じ、自組織が適切に事業継続できない可能性がある。
検知（DE）	検知プロセス	DE.DP-5	検知プロセスが、継続的に改善されている。 （セキュリティ事象に関する異常を検知する仕組みが、定期的にテストされ、改善されている。）	セキュリティ事象の検知プロセスが認識されず、自組織のセキュリティインシデントに正しく対応できず、自組織が適切に事業継続できない可能性がある。

機能	カテゴリー	サブカテゴリー	リスク点検項目	対策を怠った場合に想定されるリスク
対応（RS）	対応計画	RS.RP-1	インシデント対応計画が、インシデントの発生中又は発生後に実行されている。（インシデント発生時の対応計画が作成・運用している。）	インシデントの対応体制・計画が認識されず、自組織のセキュリティインシデントに正しく対応できないことで、自組織が適切に事業継続できない可能性がある。
対応（RS）	コミュニケーション	RS.CO-1	人員は、対応が必要になった時の自身の役割と行動の順序を認識している。（インシデント時の対応体制が整備・運用している。）	インシデントの対応体制・計画が認識されず、自組織のセキュリティインシデントに正しく対応できないことで、自組織が適切に事業継続できない可能性がある。
対応（RS）	コミュニケーション	RS.CO-2	インシデントが、定められた基準に沿って報告されている。（インシデントの報告手順が作成・運用している。）	インシデントの報告手順が作成されず、自組織のセキュリティインシデントに正しく対応できないことで、自組織が適切に事業継続できない可能性がある。
対応（RS）	コミュニケーション	RS.CO-3	インシデント対応計画に従って、情報が共有されている。（インシデント対応計画にしたがって、各関係者間での情報共有が速やかに実施されている。）	インシデントの情報共有手順が作成されず、自組織のセキュリティインシデントに正しく対応できないことで、自組織が適切に事業継続できない可能性がある。
対応（RS）	コミュニケーション	RS.CO-4	利害関係者との間で調整が、インシデント対応計画に従って行なわれている。（インシデント対応時には、対応計画に従って社内外の利害関係者と調整されている。）	自組織のセキュリティインシデントの他組織への影響が把握されず、自組織でインシデントが発生した場合に、関係する他組織が適切に事業継続できない可能性がある。

機能	カテゴリー	サブカテゴリー	リスク点検項目	対策を怠った場合に想定されるリスク
対応（RS）	コミュニケーション	RS.CO-5	サイバーセキュリティに関する状況認識を広げるために、外部利害関係者との間で自発的な情報共有が行なわれている。（自社から社外組織等に対してサイバーセキュリティに関する情報が共有されている。）	自組織のセキュリティインシデントが法律等に沿って外部組織に適切に報告されず、自組織のレピュテーションが低下する可能性がある。
対応（RS）	分析	RS.AN-1	検知システムからの通知は、調査されている。（セキュリティ事象の検知・調査方法が策定・運用している。）	システムの異常が正しく検知されないことで、インシデントの発生の特定できず、自組織が適切に事業継続できない可能性がある。
対応（RS）	分析	RS.AN-2	インシデントがもたらす影響は、把握されている。（検知されたインシデントが分析され、その結果で対応している。）	セキュリティインシデントに対して正しい優先度で対応できず、自組織が適切に事業継続できない可能性がある。
対応（RS）	分析	RS.AN-3	フォレンジックが、実施されている。（インシデント対応計画に沿って、フォレンジック（インシデントの被害・原因分析）が実施されている。）	インシデント発生時の原因究明や責任の所在を明確化できない可能性がある。
対応（RS）	分析	RS.AN-4	インシデントは、対応計画に従って分類されている。（インシデント対応計画に沿って、発生したインシデントが分類されている。）	自組織のセキュリティインシデントに対して正しく対応できず、自組織が適切に事業継続できない可能性がある。

機能	カテゴリー	サブ カテゴリー	リスク点検項目	対策を怠った場合に 想定されるリスク
対応 （RS）	分析	RS.AN-5	プロセスは、内外のソース（例:内部テスト、セキュリティ情報、セキュリティ研究者）から報告された脆弱性情報を、自組織が受け取り、分析し、対応するために定められている。 (脆弱性情報を受け取り、分析し、対応するための手順が定めている。)	最新の脆弱性情報が把握できず、システムにおけるセキュリティ上の脆弱性を利用しマルウェア感染され、保護すべきデータが漏えい・改ざんされる可能性がある。
対応 （RS）	低減	RS.MI-1	インシデントは、封じ込められている。 （インシデントの重大度によって、封じ込めの計画・手法が策定している。）	自組織のセキュリティインシデントに対して被害を最小化できず、自組織が適切に事業継続できない可能性がある。
対応 （RS）	低減	RS.MI-2	インシデントは、緩和されている。 (インシデントの根絶対象と方法が策定されている。)	自組織のセキュリティインシデントに対して被害を最小化できず、自組織が適切に事業継続できない可能性がある。
対応 （RS）	低減	RS.MI-3	新たに識別された脆弱性は、許容できるリスクである場合にはその旨を文書化され、そうでない場合にはリスクが緩和されている。 (脆弱性対策を実施している。もしくはリスクとして許容している。)	最新の脆弱性情報が把握できず、システムにおけるセキュリティ上の脆弱性を利用しマルウェア感染され、保護すべきデータが漏えい・改ざんされる可能性がある。
対応 （RS）	改善	RS.IM-1	（インシデント）対応計画は、学んだ教訓を取り入れられている。 (社内で起きたインシデントの教訓から、インシデント対応計画を見直している。)	インシデント発生に至った根本原因が修正されず、再度セキュリティインシデントを受けることで、適切に事業継続できない可能性がある。

機能	カテゴリー	サブカテゴリー	リスク点検項目	対策を怠った場合に想定されるリスク
対応（RS）	改善	RS.IM-2	対応戦略は、更新されている。（収集したインシデント事例を基に、対応計画が更している。）	他組織の受けたインシデントと同様のインシデントを受けることで、自組織が適切に事業継続できない可能性がある。
復旧（RC）	復旧計画	RC.RP-1	復旧計画が、サイバーセキュリティインシデントの発生中又は発生後に実施されている。（システムの復旧計画に従って、システムの復旧が実施されている。）	自組織のセキュリティインシデントから復旧できず、自組織が適切に事業継続できない可能性がある。
復旧（RC）	改善	RC.IM-1	復旧計画は、学んだ教訓を取り入れている。（システムを復旧した際の情報が収集され、システム復旧計画の改善に活用されている。）	セキュリティインシデント後に正しく復旧されなかった不具合により、自組織が適切に事業継続できない可能性がある。
復旧（RC）	改善	RC.IM-2	復旧戦略は、更新されている。（収集したインシデント事例を基に、復旧計画が更している。）	他組織の受けたインシデントと同様のインシデントを受けることで、自組織が適切に事業継続できない可能性がある。
復旧（RC）	コミュニケーション	RC.CO-1	広報活動が、管理されている。（セキュリティインシデントの外部発信体制を構築している。）	セキュリティインシデントに対する対応が正しく広報されず、自組織のレピュテーションが低下する可能性がある。
復旧（RC）	コミュニケーション	RC.CO-2	評判は、インシデント発生後に回復されている。（インシデント発生後の会社のレビューテーションが調査・回復されている。）	セキュリティインシデントにより低下したレピュテーションを回復できず、自組織の事業が継続できない可能性がある。

機能	カテゴリー	サブ カテゴリー	リスク点検項目	対策を怠った場合に 想定されるリスク
復旧 （RC）	コミュニケーション	RC.CO-3	復旧活動は役員と経営陣だけでなく、内外の利害関係者にも周知されている。(内部の関係者、外部の関係者に対し、情報共有を行い、必要に応じて支援を求める。)	セキュリティインシデントによりサプライヤーからの信頼が落ち、自組織が適切に事業継続できない可能性がある。

7. 参考文書

- **日本電気協会：電力制御システムセキュリティガイドライン**
  電力の安定供給や電気工作物の保安の確保の妨害等を目的としたサイバー攻撃を脅威として想定し、電気事業者が実施すべきセキュリティ対策の要求事項について規定したガイドライン。電気事業法第 39 条下の技術基準の解釈として位置付けられている。

- **経済産業省：自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン（内規）**
  発電事業の用に供するものを除く自家用電気工作物の遠隔監視システム等、制御システム等のサイバーセキュリティの確保を目的として、自家用電気工作物を設置する者が実施すべきセキュリティ対策の要求事項について規定したガイドライン。電気事業法第 39 条下の技術基準の解釈として位置付けられている。

- **経済産業省：小売電気事業者のためのサイバーセキュリティ対策ガイドライン**
  小売電気事業者が各々の事業モデルに適したサイバーセキュリティ対策を実践するための重要 10 項目に対する具体的な解釈及び指針を記載したガイドライン。

- **経済産業省：特定卸供給事業に係るサイバーセキュリティ確保の指針**
  特定卸供給事業者が、特定卸供給事業を実施する上で確保すべきサイバーセキュリティとその対策の内容を示した指針。

- **資源エネルギー庁・IPA：エネルギー・リソース・アグリゲーション・ビジネスに関するサイバーセキュリティガイドライン**
  エネルギー・リソース・アグリゲーション・ビジネス（ERAB）のサービスレベルを維持するために ERAB に参画する各事業者が実施すべき最低限のセキュリティ対策の要求事項を示したガイドライン。

- **各一般送配電事業者：託送供給等約款別冊　系統連系技術要件**
  電気設備を各一般送配電事業者の電力系統に連系するにあたり遵守する必要がある技術要件を定めたもの。2020 年 10 月よりサイバーセキュリティに関する要件が新たに規定され、新たに発電設備を系統に連系する場合又は既存発電設備のリプレース等の場合にサイバーセキュリティ対策が求められる。

- **経済産業省：サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）**
  新たなサプライチェーン（バリュークリエイションプロセス）全体のサイバーセキュリティ確保を目的として、産業に求められるセキュリティ対策の全体像を整理したフレームワーク。

- **経済産業省：サイバーセキュリティ経営ガイドライン**
  大企業及び中小企業（小規模事業者を除く）の経営者を対象として、サイバー攻撃から企業を守る観点で、経営者が認識する必要がある「3 原則」、及び経営者がサイバーセキュリティ対策を実施する上での責任者となる担当幹部（CISO 等）に指示すべき「重要 10 項目」をまとめたガイドライン。

- **米国国立標準研究所（NIST）：Framework for Improving Critical Infrastructure Cybersecurity（NIST CSF）**
  組織におけるサイバーセキュリティリスクの低減とより適切な管理を実現することを目的とし、企業・組織の業種に依存しない体系的な対策基準を整理したフレームワーク。

- **米国国立再生可能エネルギー研究所（NREL）：Distributed Energy Resource Cybersecurity Framework (DERCF)**
  Web ベースのアプリケーションとして提供されている分散型エネルギー源のサイバーセキュリティ対策に関するセキュリティ評価サービスである。評価は 3 つの大項目（ガバナンス、技術的管理策、物理的セキュリティ）ごとにまとめられており、計 414 項目の質問に対して 5 段階の成熟度（例：Unimplemented, Partial, Risk Informed, Repeatable, Adaptive）を答えることで、対策状況のスコアリングが行われる。

- **米国エネルギー省：Electricity Subsector Cybersecurity Capability Maturity Model（ES-C2M2）**
  米国の電力業界で活用されているセキュリティレベル向上のためのガイドラインであり、電力会社が現在取り組んでいる対策や手法等の能力レベルの評価と、それによる対策の目標や改善のための優先順位の設定が可能となる。IPA により V1.1 の日本語版解説書・チェックシートが公開されている。

- **ISO/IEC 27019: Information security controls for the energy utility industry**
  エネルギーの安定供給及び信頼性確保を目的としたエネルギーシステム向けの国際標準で、情報セキュリティマネジメントの国際標準規格である ISO/IEC 27002 に対し、エネルギー関連の対策要件を追加して策定された。特に、設備内のプロセス制御機器を対象としたセキュリティ要件が拡充されている。

8. 用語集

- CIO（Chief Information Officer）
  企業や組織内において IT 戦略を立案したり実行したりするために設置される責任者のこと。
- CISO（Chief Information Security Officer）
  企業や組織内において実効力のあるセキュリティ施策を行うために設置される責任者のこと。サイバー攻撃やセキュリティ事件・事故の際の判断や対応を行う。
- CSIRT（Computer Security Incident Response Team）
  コンピューターセキュリティに関連するインシデントへの対応を支援する目的で確立される機能のこと。CIRT（Computer Incident Response Team）や、CIRC（Computer Incident Response Center, Computer Incident Response Capability）とも呼称されることがある。[NIST SP 800-61 Rev.2]
- DMZ（DeMilitarized Zone）
  外部ネットワークからの攻撃より、組織内部のネットワークを保護する緩衝地帯のこと。
- IDS（Intrusion Detection System）
  サーバやネットワークの外部との通信を監視し、攻撃や侵入の試み等不正なアクセスを検知して管理者にメール等で通報するシステムのこと。
- IPS（Intrusion Prevention System）
  サーバやネットワークの外部との通信を監視し、侵入の試み等不正なアクセスを検知して攻撃を未然に防ぐシステムのこと。
- ISMS（Information Security Management System）
  組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源を配分して、システムを運用するための仕組みのこと。国際規格 ISO/IEC 27001 に要求事項が定められている。
- PDCA サイクル
  Plan-Do-Check-Act の略で、品質改善や環境マネジメントでよく知られた手法であり、次のステップを繰り返しながら、継続的に業務を改善していく手法の一つのこと。
- VPN（Virtual Private Network）
  インターネットや通信事業者の独自ネットワーク上に構築する仮想の専用線のこと。
- VPP（Virtual Power Plant）
  需要家側のエネルギーリソース、電力系統に直接接続されている発電設備、蓄電設備の保有者もしくは第三者が、そのエネルギーリソースを制御（需要家側エネルギーリソースからの逆潮流も含む）することで、発電所と同等の機能を提供すること。
- インシデント

サイバーセキュリティ分野において、サイバーセキュリティリスクが発現・現実化した事象のこと。

- インシデント対応計画
  障害発生時に、重大な影響を受けるシステムとデータをできるだけ素早く復旧するための手順をまとめた事業継続性計画。

- 可用性
  認可されたエンティティが要求したときに、アクセス及び使用が可能である特性のこと。[JIS Q 27000:2014]

- 監査
  組織内においてサイバーセキュリティ対策が適切に実施されているかどうかを判定するために、監査証拠を収集し、それを客観的に評価するための、体系的で、独立し、文書化したプロセスのこと。監査は、内部監査（第一者）又は外部監査（第二者・第三者）のいずれでも、又は複合監査（複数の分野の組合せ）でもあり得る。[JIS Q 27000:2014]

- 完全性
  正確さ及び完全さの特性のこと。[JIS Q 27000:2014]

- 機密性
  認可されていない個人、エンティティ又はプロセスに対して、情報を使用させず、また、開示しない特性のこと。[JIS Q 27000:2014]

- 脅威
  システム又は組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因のこと。[JIS Q 27000:2019]

- 高負荷攻撃
  システムの可用性を侵害する攻撃手法のひとつで、サーバやネットワークなどのリソースに対して意図的に過剰な負荷をかけたり、脆弱性をついたりすることでサービスを妨害する攻撃のこと。

- サイバー攻撃
  資産の破壊、暴露、改ざん、無効化、盗用、又は認可されていないアクセスもしくは使用の試みのこと。[JIS Q 27000:2019]

- サイバーセキュリティ
  電子データの漏えい・改ざん等や、期待されていた機器、IT システム、制御システム等の機能が果たされないといった不具合が生じないようにすること。

- サプライチェーン
  複数の開発者間でリンクされたリソース・プロセスで、製品とサービスについて、調達にはじまり設計・開発・製造・加工・販売及び購入者への配送に至る一連の流れのこと。[ISO 28001:2007, NIST SP 800-53 Rev.5]

- 残存リスク

リスク対応（回避、低減、移転）後に残るリスクのこと。保有リスクともいう。

- ステークホルダー
  意思決定又は活動に影響を与え、影響されることがある又は影響されると認知している、あらゆる人又は組織のこと。具体的には、株主、債権者、顧客、取引先等である。
- 脆弱性
  一つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点のこと。[JIS Q 27000:2019]
- 脆弱性診断
  システム、ネットワーク、Web アプリケーション等において脆弱性が存在しないかを診断すること。
- セキュリティ事象
  セキュリティ方針への違反若しくは管理策の不具合の可能性又はセキュリティに関係し得る未知の状況を示すシステム、サービス又はネットワークの状態に関連する事象のこと。[JIS Q 27000:2019]
- セキュリティパッチ
  OS やアプリケーションの脆弱性を解消するための追加プログラムのこと。
- セキュリティポリシー
  企業・組織におけるセキュリティに関する理念である意図と方針を経営者が正式に表明したもののこと。セキュリティポリシーに沿って、組織内セキュリティ対策が規定される。
- データ消去
  すべてのユーザアドレス指定可能なストレージ領域のデータに対して、データ抹消処理を行うための論理的な技術を適用し、単純な非侵襲のデータ回復技術から保護すること。[NIST SP 800-88 Rev.1]
- 認証
  エンティティの主張する特性が正しいという保証の提供のこと。[JIS Q 27000:2014]
- ファイアウォール
  ネットワークの結節点となる場所に設置し、ネットワークの通信をさせるかどうかを判断し、許可又は拒否するシステム・装置のこと。
- フェールセーフ
  機器やシステムの設計などについての考え方の一つのことで、部品の故障や破損、操作ミス、誤作動などが発生した際に、なるべく安全な状態に移行するような仕組みにしておくこと。
- 不正アクセス
  本来アクセス権限を持たない者が、システムの内部へ侵入を行う行為のこと。
- ホットスワップ

機器の電源を入れ稼働状態を保ったまま、部品やケーブルなどを交換、装着、抜去すること。また、そのような仕組みやコネクタなどの構造のこと。

- フォレンジック
  インシデント対応や法的紛争・訴訟に際し、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術のこと。

- マルウェア
  セキュリティ上の被害を及ぼすウイルス、スパイウエア、ボットなどの悪意を持ったプログラムを指す総称のこと。これらのプログラムは、使用者や管理者の意図に反して（あるいは気づかぬうちに）コンピューターに入り込み悪意ある行為を行う。

- ランサムウェア
  感染したコンピューター等においてデータが強制的に暗号化される等して、本来の利用が制限され、制限解除と引き換えに、身代金の支払い等が要求されるマルウェアの一種のこと。

- リスク
  目的に対する不確かさの影響のこと。[JIS Q 27000:2019]

- レジリエンス
  システムが以下の状態を維持できること：①悪条件下にあっても、あるいは負荷が掛かった状態であっても、（顕著に低下した状態又は無力化したような状態に陥ったとしても）稼働して、基礎的な運用能力を維持すること②ミッションニーズと平仄が合う時間内に、有効的に運用されている状態に復旧すること。[NIST SP 800-53 Rev.4]

- ログ
  コンピューターの利用状況やデータの通信記録のこと。操作を行った者の ID や操作日付、操作内容などが記録される。セキュリティ上、インシデントの原因追究などに利用する。