2019

ES-C2M2 v1.1

解説書

2019 年 7 月
独立行政法人　情報処理推進機構

Rev	発行理由	日付	作成	確認	承認
	対象ページ				
0	初版発行	2019/07/17	木下	岡下・塩田	桑名
	全ページ				

目次

1. はじめに

1-1. 本書の目的

ES-C2M2（Electricity Subsector Cybersecurity Capability Maturity Model）は、米国エネルギー省（DoE）が発行した電力業界サイバーセキュリティ能力成熟度モデル（Electricity Subsector Cybersecurity Capability Maturity Model、以下、“ES-C2M2”という。）です。

ES-C2M2は米国電力業界では電力会社の成熟度を自己評価する手順として広く用いられており、ES-C2M2とほぼ同じ内容のONG-C2M2（Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model）もあり、石油・ガス業界でも活用されています。

国内電力業界では、「電力制御システムセキュリティガイドライン」が制定され、このガイドラインにそったセキュリティ対策が行われていますが、基本的には対策のベースラインを規定するものであり、より一層高い対策を求めるための基準としては十分ではありません。本書は、国内電気事業者（以下、“電力会社”という。）および他の重要インフラ業界において、より一層のセキュリティ対策を検討する場合に、自己評価の参考資料として活用していただくことを目的としています。

また、本書には自己評価素材として、ES-C2M2 のチェックシート（日本語版）を付属しています。本書は、この ES-C2M2 チェックシートを使用するにあたって必要な情報を、ES-C2M2 v1.1[1]の内容を基に翻訳・要約したものです。

なお、ES-C2M2 の著作権、商標権についてはカーネギーメロン大学が有しており、その使用許諾については米国エネルギー省（DOE）が管理しています。ES-C2M2 v1.1 83 ページの“NOTICES”には以下の趣旨の記載がありますので、参照の上、著作権は米国 DOE に帰属することに留意をお願いします。

> NOTICES：『この資料は、テクニカルレポート「電力業界サイバーセキュリティ能力成熟度モデル（Electricity Subsector Cybersecurity Capability Maturity Model ：ES-C2M2）バージョン 1.0 (c)2012 Carnegie Mellon University」に基づいている。このバージョンの ES-C2M2 は、米国エネルギー省（DOE）によってリリースおよび維持されている。米国政府は、少なくとも、DOE が提供するこのバージョンの ES-C2M2 および対応するツールキットの、使用、変更、複製、リリース、実行、表示、または開示の無制限の権利、ならびに他者にこれらの許可を与える権利を有し、ここに他者にも同じことを行う許可を与える。ES-C2M2 は、連邦政府資金による研究開発センターであるカーネギーメロン大学ソフトウェア工学研究所の運営を目的とした

[1] ES-C2M2 参照先：
https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0-1

米国国防総省とカーネギーメロン大学との間の連邦政府契約番号 FA8721-05-C-0003 に基づく DOE の資金提供および支援を受けて作成された。』

1-2. 本書の対象読者

本書は、日本国内における電力会社のサイバーセキュリティ対策の関係者（経営者を含む）、および、対象となる業務システムの運用、保守の責任者を想定しています。

1-3. 本書の構成

本書は ES-C2M2 v1.1[2]および C2M2 Facilitator Guide[3]を基に、ES-C2M2 の概要、および ES-C2M2 チェックシート（後述）の使用方法を解説しています。
本書は以下の章立てで構成されています。

- *1 章　はじめに*
  本書の目的、対象読者、構成を解説しています。

- *2 章　ES-C2M2 の全体像*
  ES-C2M2 v1.1 のチャプター4、5、6 を要約し、ES-C2M2 の設立の背景や基準の考え方、各モデルドメインの解説を行っています。

- *3 章　ES-C2M2 チェックシートの使い方*
  ES-C2M2 チェックシート（日本語版）の使い方を解説します。

1-4. 本書の関連文書

本書の内容を補足する以下の関連文書があります。

- ES-C2M2 チェックシート（以下、“チェックシート“という。）
  ES-C2M2 v1.1 のチャプター7 に記載されている“目標とプラクティス（Objectives and Practices）”を一覧表形式でチェックシート化したものです。本書に ECXEL 形式で添付します。

[2] ES-C2M2 v1.1
https://www.energy.gov/sites/prod/files/2014/02/f7/ES-C2M2-v1-1-Feb2014.pdf

[3] C2M2 Facilitator Guide
https://www.energy.gov/sites/prod/files/2014/02/f7/C2M2-FacilitatorGuide-v1-1-Feb2014.pdf

2. ES-C2M2 の全体像

2-1. ES-C2M2 とは

2-1-1. ES-C2M2 の背景と利用用途

ES-C2M2 は米国エネルギー省が開発したサイバーセキュリティ能力成熟度モデル（Cybersecurity Capability Maturity Model、以下、“C2M2”という。）プログラムのうち、電力業界特有のサイバーセキュリティ問題に対応するために開発されたプログラムです。

本プログラムは、ホワイトハウスのイニシアチブ「電力業界サイバーセキュリティリスク管理成熟度イニシアチブ」を支援するものとして、米国エネルギー省の主導のもと、米国国土安全保障省（DHS）、官民の専門家、電力業界の電力資産所有者およびオペレーターの代表者らの協力により開発されました。イニシアチブでは、官民のパートナーシップ機構として「国家インフラ防護計画フレームワーク」が採用され、成熟度モデル（以下、モデルという。）が開発されました。

イニシアチブは既存の取り組み、モデル、およびサイバーセキュリティのベストプラクティスを活用し、ホワイトハウスの 2010 年の「Cyberspace Policy Review（サイバー空間政策レビュー）」、米国エネルギー省の「Roadmap to Achieve Energy Delivery Systems Cybersecurity（エネルギー供給システムのサイバーセキュリティ実現のためのロードマップ）」、「Energy Sector-Specific Plan（エネルギー業界分野別計画）」、「産業用制御システム合同ワーキンググループ（ICSJWG）の制御システムのサイバーセキュリティに向けたセクター横断的なロードマップ」と連携しています。

モデルのコンテンツはハイレベルな抽象度で表現されており、様々な種類・構造・規模の業界に属する組織への展開が可能です。モデルの広範な利用により、業界におけるサイバーセキュリティ能力のベンチマーキング促進が期待されます。これらの特性により、米国国立標準技術研究所（NIST）の「サイバーセキュリティフレームワーク」を電力業界に適用する際のツールとしても、ES-C2M2 を拡張することで利用可能です。

当該モデルの利用用途は以下になります。

- 電力業界におけるサイバーセキュリティ能力の強化
- 公益事業者によるベンチマークを活用した効果的かつ一貫性のあるサイバーセキュリティ能力の評価
- 知識、ベストプラクティス、および関連情報の共有によるサイバーセキュリティ能力の向上
- 公益事業者におけるサイバーセキュリティ向上のための必要なアクション、投資優先度の決定

2-1-2. ES-C2M2 v1.1（オリジナル）の文書構成

ES-C2M2 は以下の文書で構成されています。

- ES-C2M2

ES-C2M2 の主要構造・コンテンツの理解、組織による効果的な ES-C2M2 活用のサポートを目的とした文書です。

<本編>

チャプター1：ES-C2M2 の概要、対象読者、文書の説明
チャプター2：モデルに関する予備知識および開発
チャプター3：米国の電力業界の概要
チャプター4：ES-C2M2 のコンテンツと構成の理解に重要なコアとなるコンセプト
チャプター5：ES-C2M2 のアーキテクチャ
チャプター6：モデルの使用方法
チャプター7：10 ドメインにおけるモデルの目標とプラクティス

<付録>

付録 A：本文書の作成に使用した参考文献または、モデル内で特定したプラクティスの詳細情報紹介
付録 B：用語集
付録 C：この文書で使用されている頭字語定義
付録 D：ES C2M2 の文書の改訂履歴
付録 E：ES-C2M2 v1.0 の寄稿者への謝辞

C2M2 を用いてセキュリティチェックを行う際に、どのような会議を開催し、どのようなファシリテーションを行うべきかを記載した文書である「C2M2 ファシリテーターガイド」も、米国エネルギー省から発行されています。米国でどのような手順で C2M2 の評価が行われているかに興味がある人は、本書とあわせて参照頂ければと思います。

- C2M2 ファシリテーターガイド

自己評価実施のための準備、運営、評価後活動について解説している文書です。

<本編>

チャプター1：自己評価概略
チャプター2：評価の準備
チャプター3：評価の実施（評価ワークショップ）
チャプター4：フォローアップ活動
チャプター5：サマリ

<付録>

付録 A：ファシリテーターチェックリスト

付録 B：よくある論点

付録 C：参考文献

2-2. ES-C2M2 を構成するコンセプト

2-2-1. 重要インフラの目標

ES-C2M2 では、重要インフラの目標について頻繁に言及しています。

これらの目標は米国大統領政策指令第 21 号「Critical Infrastructure Security and Resilience（重要インフラのセキュリティと回復力）」[4]で定義された米国の重要インフラ 16 分野の個別のインフラ保護計画に記載されています。

言及されている目標は、ES-C2M2 の利用対象組織が提供するファンクションの多くが国家の重要インフラをサポートしていること、および、セクターのインフラ防護計画に示されたより広範なサイバーセキュリティ目標の検討の必要性を改めて問う役割を果たしています。

2-2-2. 成熟度モデル

成熟度モデルは、ある領域における能力と達成度を示す特性、属性、指標またはパターンのセットで設計されています。

成熟度モデルの内容は通常、ベストプラクティスを例示し、標準やその他の指針をまとめています。

したがって成熟度モデルは、現在取組んでいる対策や手法等の能力レベルを評価し、目標や改善のための優先順位を設定するためのベンチマークを提供します。

また、成熟度モデルが特定業界で広範に利用され、評価結果が共有されることにより、他組織の評価結果と比較することで自社の位置付けを把握することが可能になります。

業界は、構成企業の能力を分析することで、業界全体がどの程度のレベルで実施できているかを把握することができます。

進捗を評価するため、成熟度モデルには通常段階を示す「レベル」があります。ES-C2M2 では、0 から 3 の成熟度指標レベル（Maturity Indicator Level、以下“MIL”という。）が使用されます。成熟度評価モデルの詳細については 2-3-2. を参照してください。

各レベルはいくつかの属性により定義されています。それらの属性が確認できる組織で

[4] PRESIDENTIAL POLICY DIRECTIVE/PPD-21https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

あれば、示されたレベルとそのレベルが示す能力の両方を達成していると評価されます。

レベルの移行にあたっての評価可能な基準があることによって、組織は以下を測定するための尺度として利用できます。

- 現在の状態の把握
- 将来的に目指す、さらに成熟した状態の決定
- 将来の状態に達するために獲得しなければならない能力の特定

2-2-3. ファンクション

ES-C2M2 では、スコープ（評価対象範囲）を示す用語として“ファンクション”（functions）を用います。

ファンクションは ES-C2M2 モデルを使用して評価を実施する場合、対象組織のオペレーション全体のうちの一部（サブセット）を評価単位とするのが一般的です。オペレーションのサブセットと組織の境界が一致するケースが多いため、ファンクションとして部門、オペレーションのライン、個々の施設を定義するケースが多くなります。

一方、部門横断的に使用するシステムや技術に対して、モデルを適用し評価したケースもあります。たとえば、ある組織では、モデルを利用して E メール、インターネット接続、VoIP 電話などのエンタープライズ IT サービスを対象に評価を実施しています。 たとえば、脅威および脆弱性管理ドメインのプラクティス 2b に「サイバーセキュリティの脆弱性情報が収集され、ファンクションに対応して解釈されている」と記されています。この取組状況を評価するにあたり、当該組織はファンクションとして横断的な IT サービスを提供していることから、ファンクションはその IT サービスとして定義します。この例における C2M2 での取組み内容とは、エンタープライズ IT サービスに対するサイバーセキュリティ上の脆弱性情報、すなわちエンタープライズ E メールサービス、ネットワーク機器、および VoIP システムに影響を及ぼす恐れのある脆弱性の情報を収集し、ファンクションへの影響を評価することになります。

2-2-4. IT/OT の資産

ES-C2M2 ではファンクションを構成する資産を対象に目標達成評価を行います。本評価にあたっては、新旧両タイプの IT 資産や使用中の産業用制御システム（ICS）、プロセス制御システム、監視制御システム（SCADA）およびその他 OT を含めた検討を行うことが重要です。

2-3. C2M2 のモデルアーキテクチャ

2-3-1. ドメイン

ES-C2M2 では、10 のドメインが定義されています。各ドメインには複数の“目標（Objectives）”が存在し、各“目標”には複数の“プラクティス（Practices）”が存在します。10 のドメインにおいて、合計 37 の“目標”と、311 の“プラクティス”が存在します。たとえば、“リスク管理（RM）”ドメインは、組織がサイバーセキュリティリスク管理能力を身につけて強化するために実施可能なアクティビティを表すプラクティスのまとまりです。

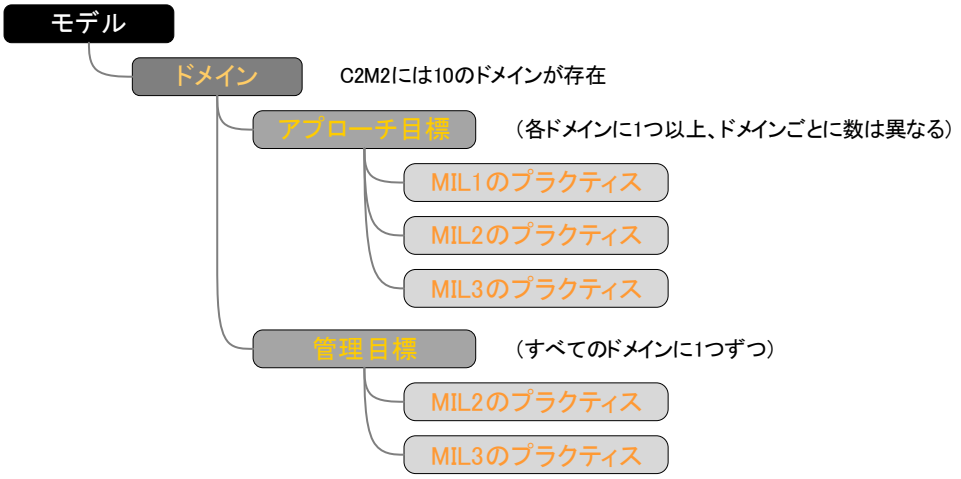
“目標”は、ドメイン毎に規定される“ドメイン固有目標”と、全ドメインでほぼ似通っている“管理目標”に分けられます。また、プラクティスは“ドメイン固有目標”に対応する“ドメイン固有プラクティス”と、“管理目標”に対応する“管理プラクティス”に分けられます。

たとえば、リスク管理ドメインは以下 3 つの目標で構成されています。

- サイバーセキュリティリスク管理戦略の策定
- サイバーセキュリティリスクの管理
- 管理アクティビティ

図 1 にモデルとドメインの要素（目標とプラクティスとの関係）をまとめました。各ドメインには 1 つ以上のドメイン固有目標と 1 つの管理目標が含まれます。ドメイン固有目標には各ドメインにおいて実施が必要なサイバーセキュリティ施策が含まれ、管理目標にはサイバーセキュリティ施策の管理化の目標が含まれます。

図 1 モデルとドメインの要素



以下に 10 のドメインの概要を解説します。

1. リスク管理（Risk Management / RM）

事業部門、子会社、関連する相互接続されたインフラおよび利害関係者を含め、組織へのサイバーセキュリティリスクを特定、分析、低減するため、エンタープライズサイバーセキュリティリスク管理プログラムを策定、運用、維持することを規定しています。

2. 資産、変更および構成管理（Asset, Change, and Configuration Management / ACM）

重要インフラに対するリスクおよび組織目標と協調し、組織のハードウェアとソフトウェア両方を含む）IT および OT 資産を管理することを規定しています。

3. アイデンティティとアクセス管理（Identity and Access Management / IAM）

電子的または物理的に組織の資産にアクセスする権限を与えられたアイデンティティを作成して管理し、重要インフラに対するリスクおよび組織目標に応じ、組織の資産へのアクセスを制限することを規定しています。

4. 脅威および脆弱性管理（Threat and Vulnerability Management / TVM）

重要インフラに対するリスクおよび組織目標と協調し、サイバーセキュリティの脅威と脆弱性を検出、特定、分析、管理および対応するための、計画、実施手順、および技術の確立と維持を規定しています。

5. 状況認識（Situational Awareness / SA）

電力システムやサイバーセキュリティについて、他のドメインからのステータスやサマリ情報などを含む情報を収集、分析、警告、表示、使用することにより共通状況認識（COP）を作成する活動と技術の確立と維持を規定しています。

6. 情報共有・コミュニケーション（Information Sharing and Communications / ISC）

重要インフラに対するリスクおよび組織目標と協調し、リスクを低減し、業務回復性を高めるため、脅威や脆弱性などのサイバーセキュリティ情報の収集および提供するにあたっての、内外エンティティとの関係の確立と維持を規定しています。

7. イベント・インシデントへの対応、業務継続（Event and Incident Response, Continuity of Operations / IR）

重要インフラに対するリスクおよび組織目標と協調し、サイバーセキュリティイベントを検出、分析、対応し、サイバーセキュリティイベント発生中の業務を持続させるための、計画、実施手順、および技術の確立と維持を規定しています。

8. サプライチェーンおよび外部依存性管理（Supply Chain and External Dependencies Management / EDM）

重要インフラに対するリスクおよび組織目標と協調し、外部エンティティに依存するサービスと資産に関連するサイバーセキュリティリスクを管理するためのコントロールの確立と維持を規定しています。

9. 要員管理（Workforce Management / WM）

重要インフラに対するリスクおよび組織目標と協調し、サイバーセキュリティの風土を生み出し、従業員の適性と能力を継続的に確保する計画、実施手順、技術、およびコントロールの確立と維持を規定しています。

10. サイバーセキュリティプログラム管理（Cybersecurity Program Management / CPM）

サイバーセキュリティの目標を、組織の戦略目標および重要インフラへのリスクと連携させつつ、組織のサイバーセキュリティ活動のためのガバナンス、戦略立案、およびスポンサーシップを提供するエンタープライズサイバーセキュリティプログラムの確立と維持を規定しています。

2-3-2. 成熟度指標レベル（MIL）

ES-C2M2 は、各ドメインで独立して評価されるレベル 0 からレベル 3 までの 4 つの成熟度指標レベル（MIL）を定義しています。

後のセクションで説明しますが、MIL は 2 つの要素（ドメイン固有プラクティスの進捗状況、管理プラクティスの進捗状況）で成熟度を定義します。

MIL の 4 つの特性を以下に示します。

1. 成熟度指標レベル（MIL）はドメイン毎に独立に評価される。

モデルを使用する組織では、ドメイン毎に独立に MIL の評価がされます。たとえば、あるドメインでは MIL1、もう 1 つのドメインでは MIL2、3 番目のドメインでは MIL3 と評価されるケースです。

2. MIL は各ドメインで累積評価される。

ドメインで、ある MIL のレベルを達成しようとする場合、そのレベルと、その前のレベルのプラクティスすべてを実行する必要があります。

たとえば、あるドメインで MIL2 を達成するには、MIL1 と MIL2 のすべてのプラクティスを実行する必要があり、また MIL3 を達成するには、MIL1、MIL2、MIL3 すべてのプラクティスを実行する必要があります。

3. サイバーセキュリティプログラム改善の効果的な戦略として、ドメインごとに MIL の目標を設定する。

MIL の目標を決定する前に、組織内でモデルが規定しているプラクティスについて熟知しておく必要があります。その上で目標レベルの到達に向けて、ギャップ分析および改善の取り組みを実施します。

4. プラクティスにより改善されるパフォーマンスと MIL の達成目標は、ビジネスの目標と組織のサイバーセキュリティ戦略に沿ったものである必要がある。

全てのドメインで一番高い MIL3 を目指すことは必ずしも最善ではなく、費用対効果と照らし合わせてドメイン別に MIL の目標設定を行うことが重要です。

なお、規模に関わらず全ての企業が全てのドメインで MIL1 を達成できるよう、MIL1 のプラクティスの実装についてはコストが課題とならないようモデルを設計しています。

2-3-3. ドメイン固有プラクティスの進捗状況

ドメイン固有プラクティスの進捗状況は各ドメインにおけるサイバーセキュリティアクティビティの実施状況を表します。進捗状況は、ドメイン内のアクティビティの網羅性、完全性、発展性によって測ることができます。組織の MIL のレベルが上がるとき、組織はより完全な、またはより進んだプラクティスを実装することになります。MIL1 で、ドメインのごく初期段階的なプラクティスのセットが求められている場合でも、組織がより高い MIL のプラクティスの実践をすることは妨げません。

表 1 で、サイバープログラム管理ドメインでのアプローチの進捗状況の例を示します。

MIL1 では、サイバーセキュリティプログラム戦略はさまざまな形で存在しますが、MIL2 では目標定義の必要性、組織戦略全体との協調、上級管理職の承認など、戦略に追加要件が加えられています。MIL3 は、MIL1 と MIL2 のプラクティスの実践に加え、ビジネスの変化、運用環境の変化、および脅威プロファイルの変化を反映するために戦略が更新されることを規定しています。

表 1 CPM ドメイン（CPM-1）におけるアプローチの進捗状況の例

MIL0	
MIL1	a. 組織にサイバーセキュリティプログラム戦略がある
MIL2	b. 組織のサイバーセキュリティアクティビティの目標は、サイバーセキュリティプログラム戦略で定義されている c. サイバーセキュリティプログラムの戦略と優先順位は文書化され、組織の戦略的目標および重要インフラに対するリスクと連携(aligned)している d. サイバーセキュリティプログラム戦略は、サイバーセキュリティアクティビティに対するプログラムの監視とガバナンスを提供する組織のアプローチを定義している e. サイバーセキュリティプログラム戦略にサイバーセキュリティプログラムの構造と組織を定義している

	f.	サイバーセキュリティプログラム戦略は、上級管理職により承認されている

MIL3	g.	ビジネスの変更、オペレーション環境の変更、脅威プロファイル（TVM-1d）の変更を反映し、サイバーセキュリティプログラム戦略が更新されている

2-3-4. 管理化の進捗（管理アクティビティの達成）状況

管理化の進捗状況は、ドメイン固有プラクティスの進捗状況とは異なり、サイバーセキュリティに関するプラクティスまたはアクティビティの実施が組織のオペレーションにどの程度浸透しているかを示します。浸透度合いに比例して、組織はプラクティスまたはアクティビティを長期間、繰り返し実施することができ、結果が一貫性を持ち、繰り返し可能で、高品質となります。

管理化の進捗状況はドメイン毎のプラクティスを管理化するために実行されるプラクティスのセットで表現されます。これらのプラクティスは全ドメインにわたってほぼ似通っており、管理プラクティスと呼ばれます。ドメイン固有目標におけるプラクティスの進捗状況は、管理プラクティスの進捗状況に相当しますが、必ずしも管理プラクティスとドメイン固有のプラクティスが対応している必要はありません。表に、リスク管理ドメインの 2 番目の目標（CPM-2：サイバーセキュリティリスク管理）のドメイン固有プラクティスと、管理プラクティスとの対応例を示します。

表 2 ドメイン固有のプラクティスと管理プラクティスの対応

	ドメイン固有プラクティス （サイバーセキュリティリスクの管理：RM-2）	管理プラクティス
MIL0		
MIL1	a. サイバーセキュリティリスクが特定されている b. 特定されたリスクが低減、承認、許容、または移転されている	① 初期のプラクティスがアドホックであっても実施されている
MIL2	c. リスク評価が実施され、リスク管理戦略に従いリスクが特定されている d. 特定されたリスクが文書化されている e. 特定されたリスクが分析され、リスク管理戦略に従い対応（レスポンス）アクティビティが優先順位付けされている f. 特定されたリスクがリスク管理戦略に従いモニターされている g. リスク分析はネットワーク （IT および（/または）OT） アーキテクチャに基づいて行っている	① プラクティスが文書化されている ② プラクティスの利害関係者が特定され、関与している ③ プロセスをサポートするための適切なリソース （人、資金、およびツール） が提供されている ④ プラクティス実装の指針となる標準および（または）ガイドラインが特定されている
MIL3	h. リスク管理プログラムが、リスク管理戦略を実践するリスク管理ポリシーおよび手順を定義、運用している i. リスク分析は、最新のサイバーセキュリティアーキテクチャに基づいて行われている j. リスク管理アクティビティをサポートするためにリスクレジスタ（リスク管理表：特定したリスクの体系的にまとめたリポジトリ）が使用されている	① アクティビティがポリシー（または他の組織的指示）とガバナンス（統制）のもと実施されている ② ポリシーは、特定された標準および（または）ガイドラインのためのコンプライアンス要件を含んでいる ③ アクティビティがポリシーに準拠しているか定期的にレビューされている ④ プラクティス実施のために必要な責任と権限が担当者に与えられている ⑤ プラクティスを実施する担当者は、適切なスキルと知識を備えている

表 2 の MIL 毎の管理プラクティスの内容を以下に示します。

・成熟度指標レベル 0（MIL0）

モデルには MIL0 のプラクティスはありません。MIL0 とは、対象となるドメインで MIL1 を達成していないことを単に意味します。

・成熟度指標レベル 1（MIL1）

各ドメインにおいて、MIL1 は初期のプラクティスを含みます。MIL1 を達成するには、これらのプラクティスをアドホックな方法であっても実施する必要があります。組織がサイバーセキュリティを管理する能力の無い状態で評価を開始する場合、当初は MIL1 のプラクティスに注力することになります。

MIL1 のプラクティスは下記の特徴があります。

① 初期のプラクティスがアドホックであっても実施されている

本モデルの説明で、アドホックとは、定められた計画（口頭、文書問わず）、ポリシー、またはトレーニングのように組織的なガイダンスがない状態で、個人やチーム（およびチームのリーダーシップ）のイニシアチブや経験に大きく依存して、プラクティスを実施することを指します。

成果の質は、誰がプラクティスを実施したか、対処する問題の背景、手法、ツール、使用される技術、およびプラクティスの実施に与えられた優先度に大きく依存します。経験と能力のある人物であれば、実施がアドホックであっても高い品質の成果を出すことが可能です。しかし通常、この MIL を達成する事による教訓は組織のレベルで蓄積されないため、組織をまたぐ形での、手法と成果の、再現と改善は困難になります。

なお、目標によっては MIL1 のプラクティスが定義されていない場合がありますが、この MIL1 は評価対象外となり、全組織が自動的に MIL1 を達成していると評価されます。（チェックシートの MIL1 に「MIL1 にプラクティスなし（No practice at MIL1）」と記載されています。）

・成熟度指標レベル 2（MIL2）

下記の 4 つのプラクティスが MIL2 に存在し、各ドメインにおける作業の管理化についての初期レベルを表しています。

MIL2 のプラクティスは 4 つの管理アクティビティによって特徴づけられます。

① プラクティスが文書化されている

ドメインのプラクティスが文書化された計画に従って実施されている状態です。ここで重要なことは、プラクティスがその組織のために確実に設計（または選択）されるよう意図して計画が立案されていることです。

② プラクティスの利害関係者が特定され、関与している

プラクティスの実施に必要な利害関係者が特定され、プラクティスの実施に関与している状態です。組織がどのようにプラクティスを実施するかにより、利害関係者を組織内、組織横断的に、または組織の外から関与させることができます。

③ プロセスをサポートするための適切なリソース（人、資金、およびツール）が提供されている

人、資金、およびツールの形で十分なリソースが提供されれば、意図通りに確実にプラクティスを実施することができます。リソースの必要性は、望まれていたのにリソース不足によって実装されなかったプラクティスを特定することで評価することが可能です。組織により望ましいプラクティスが意図通りに実装されていれば、適切なリソースが提供されていることになります。

④ プラクティス実装の指針となる標準および（または）ガイドラインが特定されている

組織がドメインにおけるプラクティスの実装の情報源となる標準、もしくはガイドラインを特定している状態です。これはプラクティスの実施計画を作り込む際に、組織が参照する情報源となります。

全体的に、MIL2 のプラクティスは MIL1 に対しより完全で、イレギュラーまたはアドホックな実施はありません。結果として、組織のプラクティスの実施のパフォーマンスはより安定すると考えられます。MIL2 では、組織はドメインのプラクティスのパフォーマンスが長期にわたり継続することにさらなる確信を得ることができます。

・成熟度指標レベル 3（MIL3）

MIL3 では、ドメインのアクティビティはさらに管理化されています。
MIL3 のプラクティスは 5 つの管理プラクティスによって構成されます。

① アクティビティがポリシー（または他の組織的指示）とガバナンス（統制）のもと実施されている

ドメイン内で規定されているプラクティスが、ポリシーとガバナンスのような組織レベルの指示として実施されている状態です。ポリシーは MIL2 に定義されている計

画立案活動の拡張と言い換えることができます。

② ポリシーに特定された標準および（または）ガイドラインのためのコンプライアンス要件が含まれている

③ アクティビティがポリシーに準拠しているか定期的にレビューされている

④ プラクティス実施のために必要な責任と権限が担当者に与えられている

⑤ プラクティスを実施する担当者は、適切なスキルと知識を備えている
　作業の実施を任命された担当者が、その業務を実施するためのドメイン固有のスキルと知識を十分に有している状態です。

MIL3 では、ドメインのプラクティスは更に安定し、ポリシーなどのハイレベルな組織的な指示が与えられています。結果として組織は、プラクティスのパフォーマンスを長期かつ組織全体で維持する能力に更に確信を得ることができます。

2-3-5. プラクティスを参照する表記法

ドメイン内のプラクティスの多くはモデルの他のプラクティスと関連性があります。この場合、関連するプラクティスは、ドメインの略称で始まり、ハイフン、目標番号、およびプラクティスを表す文字による表記を使用して参照されます。

表 4 「個別のプラクティスの参照　例 RM-1c」では、RM1 リスク管理ドメインの、ドメインのプラクティス（MIL3）「c. 組織のリスク基準　（組織が業務上のリスクを、影響度、リスク許容度およびリスク対応手法に基づいて評価、カテゴリ分け、優先順位付けするための客観的基準）が定義されており、利用できる」を、モデルの他の箇所で「RM-1c」表記を用いて参照しています。

表 4 「個別のプラクティスの参照　例 RM-1c」

ドメイン	目標	MIL	プラクティス
脅威および脆弱性管理 (TVM)	1. 脅威の特定と対応	MIL3	i. 脅威の分析と優先順位付けはファンクションの（または組織の）のリスク基準を活用し実施されている (RM-1c)

RM-1. サイバーセキュリティリスク管理戦略の策定

MIL1	MIL1にプラクティスなし
MIL2	a. 文書化されたサイバーセキュリティリスク管理戦略が存在する b. サイバーセキュリティリスク管理戦略は、影響の検討を含めた、リスクの優先順位付けのためのアプローチを提供している
MIL3	**c. 組織のリスク基準　（組織がオペレーション上のリスクを、影響度、リスク許容度およびリスク対応アプローチに基づいて評価、カテゴリ分け、優先順位付けするための客観的基準）が定義されており、利用できる** d. 現在の脅威環境を反映するため、リスク管理戦略が定期的に更新されている e. 組織特有のリスク分類が文書化され、リスク管理アクティビティで使用されている

2-4. モデルドメイン

2-4-1. リスク管理（RM）

リスク管理（RM）ドメインの目的（ゴール）は、エンタープライズサイバーセキュリティリスク管理プログラムを策定、運用、維持し、事業単位、子会社、関連する相互に接続されたインフラおよび利害関係者へのサイバーセキュリティリスクを特定、分析、低減することにあります。

リスク管理（RM）ドメインは以下 3 つの目標で構成されます。

1. サイバーセキュリティリスク管理戦略の策定
2. サイバーセキュリティリスクの管理
3. 管理アクティビティ

1. サイバーセキュリティリスク管理戦略の策定

サイバーセキュリティリスク管理戦略には、リスク評価手法、リスクモニタリング戦略、およびサイバーセキュリティガバナンスプログラムが含まれます。またこれには、サイバーセキュリティプログラム管理ドメインで後ほど説明します。サイバーセキュリティプログラムの指針となるエンタープライズリスク基準（例：影響閾値、リスク対応手法）の定義も含まれます。

2. サイバーセキュリティリスクの管理

サイバーセキュリティリスクの管理には、組織のニーズと連携するかたちでリスクの定義付け、洗い出し、評価、対応（保有、許容、低減、移転）、およびモニタリング を行うことが含まれます。これらアクティビティ実施の鍵となるのは上記のサイバーセキュリティリスク管理戦略が組織全体で理解されることです。定義されたリスク基準によって、組織は特定したリスクへ一貫性を持って対応し、監視することが可能となります。リスク管理表は、特定したリスクと関連する属性の表で、この処理を円滑にします。本モデルの他のドメイン、イベント・インシデント対応と業務継続（IR）、脅威および脆弱性管理（TVM）、および状況認識（SA）等では、リスク管理表に関連付けられることで、サイバーセキュリティリスク管理プログラムと連携し、モデルのプラクティスがいかに強化されるかが明らかにします。

3. 管理アクティビティ

管理アクティビティには、ポリシーや手順の文書化およびその定期的なレビュー、担当者の能力の定義等、上記 2 つの目標を実現するために必要なアクティビティが含まれています。この目標に関しては 2-3-4. を参照してください。

2-4-2. 資産、変更および構成管理（ACM）

資産、変更および構成管理（ACM）ドメインの目的（ゴール）は、重要インフラに対するリスクおよび組織目標と協調して、組織のハードウェアとソフトウェア両方を含む IT および OT 資産を管理することにあります。

資産、変更および構成管理（ACM）ドメインは以下 4 つの目標で構成されます。

1. 資産インベントリ管理
2. 資産構成の管理
3. 資産の変更管理
4. 管理アクティビティ

1. 資産インベントリ管理

ファンクションに関係する設備等を管理するための台帳を資産インベントリと定義しています。これは、サイバーセキュリティリスクを管理する際の重要なリソースになります。ソフトウェアのバージョン、物理的位置、資産オーナー、優先順位などの重要な情報の記録により、その他多くのサイバーセキュリティ管理アクティビティが可能になります。たとえば、資産インベントリによって、パッチが必要なソフトウェアが配置されている場所を特定できます。

2. 資産構成の管理

資産構成の管理には、IT と OT の資産の構成ベースラインの定義や資産がそのベースラインに則って構成されているかの確認が含まれます。ほとんどの場合、ある種類の資産が等しく構成されているかどうかの確認においてこの取り組みが行われます。しかし、資産が特殊な場合や、個別設定が必要な場合は、運用への設置時にその資産の構成ベースラインが統制されているか、その資産構成のベースラインの準拠が維持されているかの確認も資産の管理に含まれます。

3. 資産の変更管理

資産の変更管理には、要求された変更を分析し、許容できない脆弱性が運用環境にもたらされないかの確認や、変更がすべて変更管理プロセスに則っていることの確認、および、不正な変更の特定が含まれます。要件定義、テスト、開発、保守、運用から廃棄まで、資産のライフサイクルの全期間が変更管理の対象となります。

4. 管理アクティビティ

管理アクティビティには、ポリシーや手順の文書化およびその定期的なレビュー、担当者の能力の定義等、上記 3 つの目標を実現するために必要なアクティビティが含まれています。この目標の狙いは 2-3-4. を参照してください。

2-4-3. アイデンティティおよびアクセスの管理（IAM）

アイデンティティとは、アイデンティティ管理者の責任範囲内で、エンティティを他のエンティティと十分に区別でき、エンティティを認識することができる属性値（特徴など）の集合を意味しています。アイデンティティおよびアクセスの管理（IAM）ドメインの目的（ゴール）は、電子的または物理的に組織の資産にアクセスする権限を与えられたアイデンティティを作成して管理し、重要インフラに対するリスクおよび組織目標と協調して、組織の資産へのアクセスを制限することにあります。

アイデンティティとアクセス管理（IAM）ドメインは以下 3 つの目標で構成されます。

1. アイデンティティの確立および維持
2. アクセス制御
3. 管理アクティビティ

1. アイデンティティの確立および維持

アイデンティティの確立と維持にあたり、まずアイデンティティをエンティティへプロビジョニング（アイデンティティの発行）またはデプロビジョニング（利用可能なアイデンティティが既に不要であれば削除すること）します。エンティティには資産にアクセスする必要のあるデバイス、システム、あるいはプロセスだけではなく、（内部または組織への外部からアクセスする）個人を含めることができます。また、公益事業者が共有アイデンティティを使用しなければならない場合もあります。その場合、適切なレベルのセキュリティを担保するための補完措置が必要となる可能性があります。アイデンティティの保守にはトレーサビリティ（認識されているすべてのアイデンティティが正当であると確認すること）とデプロビジョニングが含まれます。

2. アクセス制御

本節におけるアクセス制御は、ファンクション提供に関係する資産へのロジカルアクセス、フィジカル（物理）アクセス、および自動化されたアクセス制御システムに適用します。アクセス制御にはアクセス要件の決定、それらの要件に基づいた資産へのアクセス権の付与、および不要になったアクセス権の無効化が含まれます。アクセス要件は資産と紐付けられ、資産へのアクセスが許可されるエンティティの種別、許可されるアクセスの範囲、および認証パラメータを決定する際のガイドとなります。たとえば、特定の資産のアクセス要件では、ベンダーによるリモートアクセスは特定かつ事前計画された保守期間のみ許可することとし、さらに多要素認証を要求する必要があるかもしれません。上位の MIL を達成するためには、付与されるアクセス権はさらに綿密に精査される必要があります。アクセス権はファンクションへのリスクの検討の後に付与され、定期的なアクセス権のレビューが実施されます。

3. 管理アクティビティ

管理アクティビティには、ポリシーや手順の文書化およびその定期的なレビュー、担当者の能力の定義等、上記２つの目標を実現するために必要なアクティビティが含まれています。この目標の狙いは２-３-４．を参照してください。

２-４-４. 脅威および脆弱性管理（TVM）

脅威および脆弱性管理（TVM）ドメインの目的（ゴール）は、重要インフラに対するリスクおよび組織目標と協調して、サイバーセキュリティの脅威と脆弱性を検出、特定、分析、管理および対応するための、計画、実施手順、および技術を確立し維持することにあります。

脅威および脆弱性管理（TVM）ドメインは、以下 3 つの目標で構成されます。

1. 脅威の特定と対応
2. サイバーセキュリティ脆弱性の低減策
3. 管理アクティビティ

1. 脅威の特定と対応

脅威の特定と対応は、有益な脅威の情報を信頼できるソースより収集することから始めます。その情報を組織とファンクションの状況に置き換え、ファンクションの提供に影響を及ぼす手段や動機、機会を持つ、脅威に対応します。脅威プロファイルには、考えられる意図、能力、および脅威の標的の特徴分析が含まれます。脅威プロファイルは、特定の脅威の識別、リスク管理（RM）ドメインに記載のリスク分析プロセス、および状況認識（SA）ドメインに記載の共通状況認識（COP）の構築の手引きとしても利用可能です。

2. サイバーセキュリティ脆弱性の低減策

サイバーセキュリティの脆弱性の低減策を策定するには、まず脆弱性情報の収集と分析から始めます。脆弱性は、自動スキャンツール、ネットワークペネトレーションテスト、サイバーセキュリティ演習、および監査の実施によって検出が可能です。脆弱性の分析においては、脆弱性の資産への影響、および脆弱性が存在する資産がファンクションを提供する上でどの程度重要かを検討する必要があります。脆弱性に対しては、緩和策、脅威状況のモニタリング、サイバーセキュリティパッチの適用、あるいはその他アクティビティの実装によって対応します。

3. 管理アクティビティ

管理アクティビティには、ポリシーや手順の文書化およびその定期的なレビュー、担当者の能力の定義等、上記２つの目標を実現するために必要なアクティビティが含まれてい

ます。この目標の狙いは２-３-４．を参照してください。

２-４-５. 状況認識（SA）

状況認識（SA）ドメインの目的（ゴール）は、重要インフラに対するリスクおよび組織目標と協調して、電力システムやサイバーセキュリティについて、他のモデルドメインからのステータスやサマリ情報などを含む情報を収集、分析、警告、表示、使用することにより共通状況認識（COP）を作成する活動と技術を確立し、維持することにあります。

状況認識（SA）ドメインは、以下 4 つの目標で構成されます。

1. ログの取得
2. モニタリング
3. 共通状況認識（COP）の確立と維持
4. 管理アクティビティ

1. ログの取得

ログの取得は資産のファンクションへの潜在的影響に基づいて行います。たとえば、資産が不正アクセスされた時の潜在的影響が大きいほど、組織はその資産についてより多くのデータ収集する必要があります。

2. モニタリング

モニタリングによって得られる資産の状態は運用状況の把握に役立つため、把握した運用状況を関係する意思決定者へ効果的に伝えることが必要です。これは共通状況認識（COP）の本質になります。

3. 共通状況認識（COP）の確立と維持

共通状況認識（COP）は意思決定者による運用状況の把握を支援するための仕組みです。実装には視覚化ツール（例：ダッシュボード、地図、その他グラフィカルな表示） がよく使用されますが、それらは必ずしも目標達成の要件ではありません。組織は、ファンクションのサイバーセキュリティの現状を共有するために、他の手法を使用してもかまいません。

4. 管理アクティビティ

管理アクティビティには、ポリシーや手順の文書化およびその定期的なレビュー、担当者の能力の定義等、上記２つの目標を実現するために必要なアクティビティが含まれています。この目標の狙いは２-３-４．を参照してください。

2-4-6. 情報共有・コミュニケーション（ISC）

情報共有・コミュニケーション（ISC）ドメインの目的（ゴール）は、重要インフラに対するリスクおよび組織目標と協調して、脅威や脆弱性などのサイバーセキュリティ情報を収集および提供し、リスクを低減し、業務回復性を高めるために内外のエンティティとの関係を確立し、維持することにあります。

情報共有・コミュニケーション（ISC）ドメインは、以下 2 つの目標で構成されます。

1. サイバーセキュリティ情報の共有
2. 管理アクティビティ

1．サイバーセキュリティ情報の共有

サイバーセキュリティ情報の共有は、ファンクションに関連するサイバーセキュリティ情報の収集から始めます。この情報はベンダー、行政組織、同業者などを含む多様な情報源から入手可能です。各種リスク関連情報のセキュアな共有は個々の組織と業界の健全性のために不可欠です。公益事業者は脅威に対応し、脆弱性を検出した場合は、同業者もリスクを緩和し、電力網の回復力を向上できるよう、関連データを効果的かつ適切に共有する必要があります。ES-ISAC などのフォーラムがこの共有の一助となるでしょう。

2. 管理アクティビティ

管理アクティビティには、ポリシーや手順の文書化およびその定期的なレビュー、担当者の能力の定義等、上記の目標を実現するために必要なアクティビティが含まれています。この目標の狙いは 2-3-4．を参照してください。

2-4-7．イベント・インシデント対応と業務継続（IR）

イベント・インシデント対応と業務継続（IR）ドメインの目的（ゴール）は、重要インフラに対するリスクおよび組織目標と協調して、サイバーセキュリティイベントを検出、分析、対応し、サイバーセキュリティイベント発生中の業務を持続させるための、計画、実施手順、および技術を確立し、維持することにあります。

イベント・インシデント対応と業務継続（IR）ドメインは、以下 5 つの目標で構成されます。

1. サイバーセキュリティイベントの検出
2. サイバーセキュリティイベントのエスカレーションとインシデントの宣言
3. インシデントとエスカレーションされたサイバーセキュリティイベントへの対応
4. 業務継続計画
5. 管理アクティビティ

1. サイバーセキュリティイベントの検出

サイバーセキュリティイベントの検出には、イベントを報告する社内連絡先（部門、ML等）の指定およびイベントの優先順位付けをする基準の確立が含まれます。組織は、これらの基準をリスク管理ドメインで説明されているサイバーセキュリティリスク管理戦略とを連携させ、イベントの評価の一貫性を確保し、サイバーセキュリティイベントとサイバーセキュリティインシデントを区別する仕組みを提供する必要があります。

2. サイバーセキュリティイベントのエスカレーションとインシデントの宣言

サイバーセキュリティイベントのエスカレーションには、前項「1. サイバーセキュリティイベントの検出」で説明されている基準の適用と、どのタイミングでサイバーセキュリティイベントが対応計画に従って管理されなければならないかの識別が含まれます。これらのエスカレーションされたサイバーセキュリティイベントやインシデントにより、規制機関への報告あるいは顧客への通知など組織外部への責務が発生することがあります。サイバーセキュリティのイベントやインシデントやその他記録を複数の相互関係を比較することにより、組織全体に関わる問題が明らかになることがあります。

3. インシデントとエスカレーションされたサイバーセキュリティイベントへの対応

エスカレーションされたサイバーセキュリティイベントに対応する組織には、サイバーセキュリティイベントの影響が電力業界に広がることを制限するためのプロセスが必要となります。また、そのプロセスで、組織がインシデントライフサイクルの全フェーズ（例：トリアージ（対応順位の決定）、対応、伝達、連携、およびクロージング）を管理する方法を説明する必要があります。サイバーセキュリティイベントおよびインシデント対応として学んだ経験のレビューを実施することが、インシデントにつながった脆弱性悪用を組織が排除するのに役立つでしょう。

4. 業務継続計画

業務継続計画には、重大なサイバーセキュリティインシデントまたは災害などによる中断時に、電力業界のファンクションを維持するのに必要なアクティビティが含まれます。業務影響の分析により、組織は必須資産とそれらの目標復旧時間の特定が可能になります。業務継続計画はテストされ、現実的かつ実用可能となるよう調整する必要があります。

5. 管理アクティビティ

管理アクティビティには、ポリシーや手順の文書化およびその定期的なレビュー、担当者の能力の定義等、上記の４つの目標を実現するために必要なアクティビティが含まれています。この目標の狙いは２-３-４．を参照してください。

2-4-8. サプライチェーンおよび外部依存性管理（EDM）

サプライチェーンおよび外部依存性管理（EDM）ドメインの目的（ゴール）は、重要インフラに対するリスクと組織目標と協調して、外部のエンティティに依存するサービスと資産に関連するサイバーセキュリティリスクを管理するコントロールを確立し、維持することにあります。

重要インフラ運用パートナー、サプライヤ、サービスプロバイダ、および顧客の相互依存が増加するにつれ、重要な関係の包括的理解の確立と維持、および関連するサイバーセキュリティリスクの管理は、セキュアで信頼性が高く、復元力のあるファンクションの提供には不可欠となります。

このモデルでは、外部依存関係をサプライヤと顧客に分類します。サプライヤの依存関係は、運用パートナーを含む、ファンクションの提供に依存する外部の関係者です。顧客の依存関係は、オペレーティングパートナーを含むファンクションの提供に依存する外部の関係者です。

サプライチェーンのリスクは、サプライヤの依存関係の注目すべき例です。製品やサービスのサイバーセキュリティの特性は大きく異なります。適切なリスク管理がなければ、出所が未知のソフトウェア、および偽造 (おそらく悪意のある) ハードウェアを含め、深刻な脅威をもたらします。事業者の提案要求は、しばしばハイテクシステム、デバイス、およびサービスのサプライヤに、大まかな仕様しか提示していないため、セキュリティと品質保証に関する適切な要件が欠けている可能性があります。

計画や政策によって調達活動にサイバーセキュリティの要件を含むように強いられている場合を除き、自立して行動する事業者は、しばしば個々のビジネスユニットに対しリスクをさらに増加させます。

サプライチェーンおよび外部依存性管理（EDM）ドメインは、以下 3 つの目標で構成されます。

1. 依存関係の特定
2. 依存リスクの管理
3. 管理アクティビティ

1. 依存関係の特定

依存関係の特定には、ファンクションの提供に必要となる主要な外部関係（サプライヤ、顧客）の、広範な理解の確立と維持が含まれます。

2. 依存リスクの管理

依存関係の管理には、独立（第三者）テスト、コードレビュー、脆弱性のスキャン、およびセキュアソフトウェア開発プロセスに従っているベンダーからの証明可能なエビデンスのレビュー等の手法が含まれます。サイバーセキュリティリスク低減のためのサイバーセキュリティの標準またはガイドラインを満たす、または上回ることをベンダーの責務

として定めた契約文書など、電力事業者と、プロダクトやサービスのパートナーやベンダーとの間で締結された契約は、レビューのうえ承認される必要があります。サービスレベル合意書（SLA）には、ベンダーとサービスプロバイダーがサイバーセキュリティおよびその他パフォーマンスの基準を満たしていることを確認するためのモニタリングと監査のプロセスについて明記することができます。

3. 管理アクティビティ

管理アクティビティには、ポリシーや手順の文書化およびその定期的なレビュー、担当者の能力の定義等、上記の２つの目標を実現するために必要なアクティビティが含まれています。この目標の狙いは２-３-４．を参照してください。

２-４-９. 要員管理（WM）

要員管理（WM）ドメインの目的（ゴール）は、重要インフラに対するリスクおよび組織目標と協調して、サイバーセキュリティの文化を生み出し、担当者の継続的な適合性と能力を高める計画、実施手順、技術、およびコントロールを確立し、維持することにあります。

要員管理（WM）ドメインは、以下５つの目標で構成されます。

1. サイバーセキュリティにおける責任の割り当て
2. 要員ライフサイクルの管理
3. サイバーセキュリティ要員の育成
4. サイバーセキュリティ意識の向上
5. 管理アクティビティ

1. サイバーセキュリティにおける責任の割り当て

サイバーセキュリティにおける責任の割り当てにおいて重要なことは、対象範囲が適切かつ冗長性を持って設定されていることです。たとえば、重要なサイバーセキュリティにおける責任をともなう特定の従業員の役割を定めることは簡単であることが多いですが、維持することは困難です。重要なサイバーセキュリティ上の役割（例：システム管理者）に関しては、適切なトレーニング、テスト、冗長性および、パフォーマンスの評価を実施するための計画を作成することが重要になります。もちろん、サイバーセキュリティにおける責任は従来の IT 要員に制限されるものではなく、たとえば、運用エンジニアがサイバーセキュリティにおける責任を担う可能性もあります。

2. 要員ライフサイクルの管理

要員ライフサイクルの管理には、身元調査 （例：経歴調査） や、必須サービスを提供する必要のある資産にアクセス権のある職責にリスク指定を割り当てることが含まれま

す。たとえば、重要システムのシステム管理者（一般的に設定変更、ログファイルの修正または削除、新規アカウント作成、パスワードの変更ができる者）は高いリスク指定を受けます。重要システムをこの種の担当者の偶発的または悪意のある行為から保護するためには、別個の対策を取る必要があります。

3. サイバーセキュリティ要員の育成

サイバーセキュリティ要員の育成には、判明したスキルのギャップを埋めるためのトレーニングと採用活動が含まれます。たとえば、雇用のプラクティスでは、採用担当者と面接者はサイバーセキュリティ要員のニーズを把握している必要があります。また、新たに採用した従業員（および受託業者）は、ソーシャルエンジニアリングへの脆弱性やその他脅威を緩和するためにセキュリティ意識向上トレーニングを受ける必要があります。

4. サイバーセキュリティ意識の向上

従業員のサイバーセキュリティ意識の向上は、組織のサイバーセキュリティを改善する技術的対策の実施と同様に重要です。組織へのサイバー攻撃の脅威は通常、企業内の IT または OT システムに何らかの手がかりを得るところから始まります。たとえば、不用心な従業員または受託業者の信頼を得て、組織のネットワークにメディアまたは機器を設置させるような手口です。組織は、疑わしい振る舞いを特定したり、スパムやスピアフィッシングを回避したりする手法と技術に関する情報を従業員と共有し、ソーシャルエンジニアリングの攻撃を認識し、潜在的敵対者に組織の情報が漏れることを回避する必要があります。たとえば、社内ウェブサイトによって組織が属する業界の新たな脅威と脆弱性についての情報を提供することが可能です。脅威、脆弱性、およびベストプラクティスの情報を従業員と共有しなければ、従業員はセキュリティのプロセスと実施手順をおろそかにする可能性があります。

5. 管理アクティビティ

管理アクティビティには、ポリシーや手順の文書化およびその定期的なレビュー、担当者の能力の定義等、上記の 4 つの目標を実現するために必要なアクティビティが含まれています。この目標の詳細については 2-3-4. も参照してください。

2-4-10. サイバーセキュリティプログラム管理（CPM）

サイバーセキュリティプログラム管理（CPM）ドメインの目的（ゴール）は、サイバーセキュリティの目標を、組織の戦略的目標および重要インフラへのリスクと連携させつつ、組織のサイバーセキュリティ活動のためのガバナンス、戦略立案、およびスポンサーシップを提供するエンタープライズサイバーセキュリティプログラムを確立し、維持することにあります。ここで「プログラム」とはサイバーセキュリティの目標を実現するためのアクティビティの集合を示し、このドメインでは各プロジェクトの管理手法を提供すること

を目標とします。

サイバーセキュリティプログラム管理（CPM）ドメインは、は、以下 5 つの目標で構成されます。

1. サイバーセキュリティプログラム戦略の策定
2. サイバーセキュリティプログラムのスポンサーシップ
3. サイバーセキュリティアーキテクチャの策定と維持
4. セキュアなソフトウェア開発
5. 管理アクティビティ

1. サイバーセキュリティプログラム戦略の策定

サイバーセキュリティプログラム戦略はプログラムの基盤として整備されます。もっとも単純なかたちであれば、プログラムの戦略に、サイバーセキュリティの目標とそれらを達成するための計画のリストが含まれます。より成熟度の高いものになると、プログラムの戦略はより完全で、プログラムの優先度、ガバナンス手法、構成を含み、プログラムの設計に上級管理職がより多く関与しています。

2. サイバーセキュリティプログラムのスポンサーシップ

スポンサーシップは、戦略に従ったプログラムの実装に重要です。基本的なスポンサーシップの形態は、リソース（人、ツール、資金）の提供からなります。より進んだスポンサーシップの形態には、役員に代表されるシニアリーダーの関与、およびプログラムに対する責任と権限の指示が存在します。さらに、スポンサーシップには、ポリシーの確立と実装への組織的サポートや、プログラムに助言を与えるその他の組織的指示が存在します。

3. サイバーセキュリティアーキテクチャの策定と維持

サイバーセキュリティアーキテクチャは、エンタープライズアーキテクチャの不可欠な要素です。企業のセキュリティプロセス、サイバーセキュリティのシステム、従業員、および下位組織の構造と活動が記載され、組織のミッションや戦略計画と連携されます。サイバーセキュリティアーキテクチャの重要な要素の一つに、IT システムの OT システムからの効果的な分離があります。

4. セキュアなソフトウェア開発

脆弱性を誘発するソフトウェアの欠陥を減らすためには、ファンクションの提供のために、重要な資産向けの、セキュアなソフトウェア開発を実施、要求することが重要です。

5. 管理アクティビティ

管理アクティビティには、ポリシーや手順の文書化およびその定期的なレビュー、担当者の能力の定義等、上記の 4 つの目標を実現するために必要なアクティビティが含まれています。この目標の詳細については 2-3-4. を参照してください。

3. ES-C2M2 チェックシート（日本語版）の活用方法

3-1. チェックシートの説明

3-1-1. チェックシートの構造

チェックシートは以下のような構造になっています。

「ドメイン」

各要件が属するドメインが記載されています。

「目標」

C2M2 のドメイン内に定義されている目標（Objectives）が記載されています。

「MIL」

個々の要件の成熟度指標レベル（MIL）が記載されています。

「プラクティス」

C2M2 で定義されるプラクティス（Practices）が記載されています。チェックシートの記入者は、このプラクティスに適合しているかを判断する必要があります。

この欄は、評価結果が「未実装」は濃い赤、「一部分実装」は薄い赤、「大部分実装」は薄い緑、「完全実装」であった場合は、濃い緑に網掛けされます。

「評価結果」

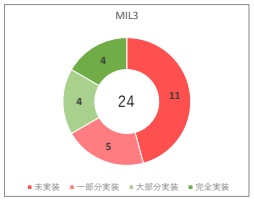
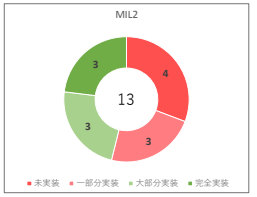
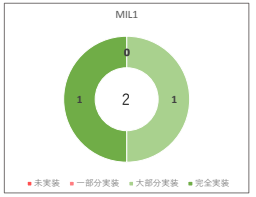
プラクティスの適合について、「完全実装」、「大部分実装」、「一部分実装」、「未実装」の中から選択します。ES-C2M2 ではこの 4 段階評価の基準は組織内で決定するよう求めていますが、以下のような目安に沿って評価基準を決定します。

- 完全実装　（プラクティスで定義されている内容がすべて実装されており、追加アクションをとる必要がない）
- 大部分実装　（プラクティスを完全実装するために必要なアクションが 1 つか、あるいは、重要度の低いアクションが残っている）
- 一部分実装　（プラクティスを完全実装するために必要なアクションが複数挙げられる）
- 未実装　（プラクティスで定義されている内容がいずれも実装されていない）

「コメント」

自由記入欄です。評価結果の根拠やメモなどの記入に利用してください。

図 2 チェックシートの例

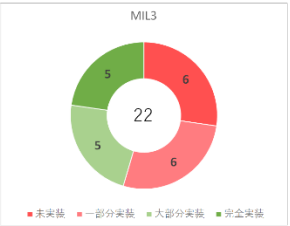
ES-C2M2					評価結果	コメント	ドーナツチャート
ドメイン	目標	MIL	プラクティス				
リスク管理 Risk Management (RM)	1. サイバーセキュリティリスク管理戦略の策定 (1. Establish Cybersecurity Risk Management Strategy)	MIL1		MIL1にプラクティスなし			
		MIL2	a. There is a documented cybersecurity risk management strategy	a. 文書化されたサイバーセキュリティリスク管理戦略が存在する	完全実装		
			a. There is a documented cybersecurity risk management strategy	b. サイバーセキュリティリスク管理戦略は、影響の検討を含めた、リスクの優先順位付けのためのアプローチを提供している	未実装		
		MIL3	c. Organizational risk criteria (objective criteria that the organization uses for evaluating, categorizing, and prioritizing operational risks based on impact, tolerance for risk, and risk response approaches) are defined and available	c. 組織のリスク基準 （組織がオペレーション上のリスクを、影響度、リスク許容度およびリスク対応アプローチに基づいて評価、カテゴリ分け、優先順位付けするための客観的基準）が定義されており、利用できる	未実装		
			d. The risk management strategy is periodically updated to reflect the current threat environment	d. 現在の脅威環境を反映するため、リスク管理戦略が定期的に更新されている	未実装		
			e. An organization-specific risk taxonomy is documented and is used in risk management activities	e. 組織特有のリスク分類が文書化され、リスク管理アクティビティで使用されている	未実装		
	2. サイバーセキュリティリスク管理 (2. Manage Cybersecurity Risk)	MIL1	a. Cybersecurity risks are identified	a. サイバーセキュリティリスクが特定されている	完全実装		
			b. Identified risks are mitigated, accepted, tolerated, or transferred	b. 特定されたリスクは低減、保有、許容または移転されている	大部分実装		
		MIL2	c. Risk assessments are performed to identify risks in accordance with the risk management strategy	c. リスク評価が実施され、リスク管理戦略に従いリスクが特定されている	大部分実装		
			d. Identified risks are documented	d. 特定されたリスクが文書化されている	一部分実装		
			e. Identified risks are analyzed to prioritize response activities in accordance with the risk management strategy	e. 特定されたリスクが分析され、リスク管理戦略に従い対応（レスポンス）アクティビティが優先順位付けされている	一部分実装		
			f. Identified risks are monitored in accordance with the risk management strategy	f. 特定されたリスクがリスク管理戦略に従いモニターされている	大部分実装		
			g. Risk analysis is informed by network (IT and/or OT) architecture	g.リスク分析は、ネットワーク （IT および（/または）OT） アーキテクチャに基いて行われている	完全実装		
		MIL3	h. The risk management program defines and operates risk management policies and procedures that implement the risk management strategy	h.リスク管理プログラムが、リスク管理戦略を実践するリスク管理ポリシーおよび手順を定義・運用している	未実装		
			i. A current cybersecurity architecture is used to inform risk analysis	i. リスク分析は、最新のサイバーセキュリティアーキテクチャに基づいて行われている	大部分実装		
			j. A risk register A risk register (a structured repository of identified risks) is used to support risk management activities	j. リスク管理アクティビティをサポートするためにリスクレジスタ（リスク管理表：特定したリスクを体系的にまとめたリポジトリ） が使用されている	完全実装		
	3. 管理アクティビティ (3. Management Activities)	MIL1	No practice at MIL1	MIL1にプラクティスなし			
		MIL2	a. Documented practices are followed for risk management activities	a. リスク管理アクティビティが文書化されたプラクティスに従い実施されている	未実装		
			b. Stakeholders for risk management activities are identified and involved	b.リスク管理アクティビティの利害関係者が特定され、関与している	未実装		
			c. Adequate resources (people, funding, and tools) are provided to support risk management activities	c. リスク管理アクティビティをサポートするための適切なリソース （人、資金、およびツール） が提供されている	一部分実装		
			d. Standards and/or guidelines have been identified to inform risk management activities	d. リスク管理アクティビティの情報源となる標準および（/または）ガイドラインが特定されている	未実装		
		MIL3	e. Risk management activities are guided by documented policies or other organizational directives	e. 文書化されたポリシーまたは他の組織的指示により、リスク管理アクティビティに指針が与えられている	一部分実装		
			f. Risk management policies include compliance requirements for specified standards and/or guidelines	f. リスク管理ポリシーには、特定された標準および（/または）ガイドラインに対するコンプライアンス要件が含まれている	未実装		
			g. Risk management activities are periodically reviewed to ensure conformance with policy	g. リスク管理アクティビティが定期的にレビューされ、ポリシーに準拠していることが保証されている	一部分実装		
			h. Responsibility and authority for the performance of risk management activities are assigned to personnel	h.リスク管理アクティビティ実施のために必要な責任と権限が担当者に与えられている	未実装		
			i. Personnel performing risk management activities have the skills and knowledge needed to perform their assigned responsibilities	i.リスク管理アクティビティを実施する担当者は、任じられた責務を遂行するために必要なスキルと知識を備えている	未実装		

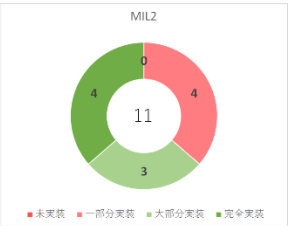
また「ドーナツチャート」欄では MIL ごとの評価数を示すドーナツチャートが自動で生成されます。

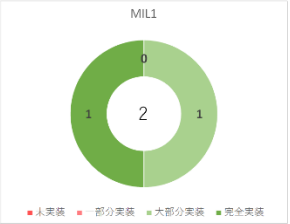
以下はすべての項目を記入したチェックシートの記入例です。

図 3 チェックシートの記入例

ES-C2M2					評価結果	コメント	ドーナツチャート
ドメイン	目標	MIL		プラクティス			
情報共有・コミュニケーション Information Sharing and Communications (ISC)	1. サイバーセキュリティ情報の共有 (1. Share Cybersecurity Information)	MIL1	a. Information is collected from and provided to selected individuals and/or organizations	a. 情報が選ばれた個人および（/または）組織から収集され、提供されている	大部分実装		
			b. Responsibility for cybersecurity reporting obligations are assigned to personnel (e.g., internal reporting, DOE Form OE-417, ES-ISAC, ICS-CERT, law enforcement)	b. サイバーセキュリティの報告義務の責任が職員に割り当てられている （内部報告、DOE Form OE-417、 E-ISAC、ICS-CERT、法令など）	完全実装		
		MIL2	c. Information-sharing stakeholders are identified based on their relevance to the continued operation of the function (e.g., connected utilities, vendors, sector organizations, regulators, internal entities)	c. 情報共有の利害関係者がファンクションの継続した運用との関連性に基づいて特定されている （例：接続されている公益事業者、ベンダー、セクター組織、規制当局、内部エンティティ）	大部分実装		
			d. Information is collected from and provided to identified information-sharing stakeholders	d. 情報が特定された情報共有の利害関係者から収集され、提供されている	一部分実装		
			e. Technical sources are identified that can be consulted on cybersecurity issues	e. サイバーセキュリティの課題を相談可能な技術的リソース（人、ベンダ等）が特定されている	部分実装		
			f. Provisions are established and maintained to enable secure sharing of sensitive or classified information	f. 機微情報や機密情報の安全な共有を可能にするため、規定が策定され、維持されている	一部分実装		
			g. Information-sharing practices address both standard operations and emergency operations	g. 情報共有のプラクティスは、標準オペレーションと緊急オペレーションの両方に対応している	完全実装		
		MIL3	h. Information-sharing stakeholders are identified based on shared interest in and risk to critical infrastructure	h. 情報共有の利害関係者は、重要インフラへの共通の関心およびリスクに基づき特定されている	大部分実装		
			i. The function or the organization participates with information sharing and analysis centers	i. ファンクションまたは組織は、情報共有・分析センター（ISAC)に参加している	完全実装		
			j. Information-sharing requirements have been defined for the function and address timely dissemination of cybersecurity information	j. 情報共有の要件がファンクションのために定義され、サイバーセキュリティ情報のタイムリーな配信に対応している	未実装		
			k. Procedures are in place to analyze and de-conflict received information	k. 受信した情報の分析とコンフリクト（不整合、矛盾点等）を取り除く実施手順が定められている	未実装		
			l. A network of internal and external trust relationships (formal and/or informal) has been established to vet and validate information about cyber events	l. サイバーイベントについての情報を精査、検証するための信頼関係のネットワークが公式であれ非公式であれ組織内外に確定されている	未実装		
	2. 管理アクティビティ (2. Management Activities)	MIL1	No practice at MIL1	MIL1にプラクティスなし			
		MIL2	a. Documented practices are followed for information-sharing activities	a. 情報共有のアクティビティが文書化されたプラクティスに従い実施されている	完全実装		
			b. Stakeholders for information-sharing activities are identified and involved	b. 情報共有のアクティビティの利害関係者が特定され、関与している	一部分実装		
			c. Adequate resources (people, funding, and tools) are provided to support information-sharing activities	c. 情報共有のアクティビティをサポートするための適切なリソース （人、資金、およびツール） が提供されている	大部分実装		
			d. Standards and/or guidelines have been identified to inform information-sharing activities	d. 情報共有のアクティビティの情報源となる標準および（/または）ガイドラインが特定されている	完全実装		
		MIL3	e. Information-sharing activities are guided by documented policies or other organizational directives	e. 文書化されたポリシーまたは他の組織的指示により、情報共有のアクティビティに指針が与えられている	部分実装		
			f. Information-sharing policies include compliance requirements for specified standards and/or guidelines	f. 情報共有のポリシーには、特定の標準および（/または）ガイドライン準拠のためのコンプライアンス要件が含まれている	未実装		
			g. Information-sharing activities are periodically reviewed to ensure conformance with policy	g. 情報共有のアクティビティが定期的にレビューされ、ポリシーに準拠していることが確保されている	未実装		
			h. Responsibility and authority for the performance of information-sharing activities are assigned to personnel	h. 情報共有のアクティビティ実施のための責任と権限が担当者に与えられている	大部分実装		
			i. Personnel performing information-sharing activities have the skills and knowledge needed to perform their assigned responsibilities	i. 情報共有の管理アクティビティを実施する担当者に、任じられた責務を遂行するために必要なスキルと知識が備わっている	未実装		
			j. Information-sharing policies address protected information and ethical use and sharing of information, including sensitive and classified information as appropriate	j. 情報共有ポリシーは、保護された情報、センシティブな情報や機密情報を含めた情報の、倫理的な使用、および共有について規定している	一部分実装		







3 - 1 - 2 . ドーナツチャートの見方

図 2 の MIL3 のドーナツチャートを図 4 に抜き出し、説明します。

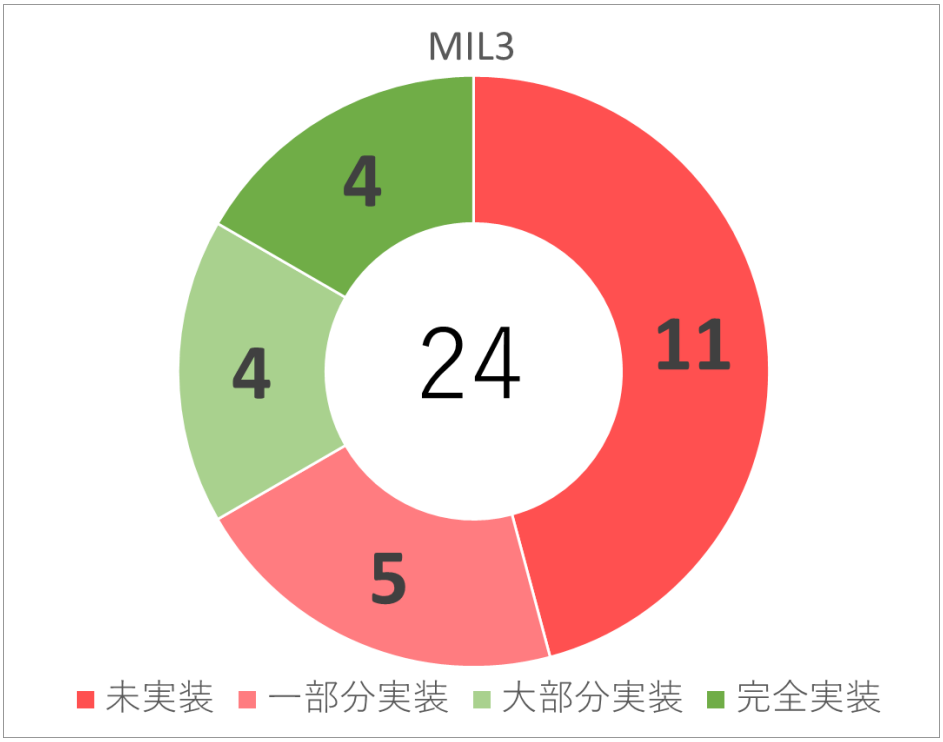


図 4 ドーナツチャートによる MIL の表現

ドーナツチャートは、そのドメインの各 MIL（MIL1～MIL3）の達成状況を示しています。ドーナツチャート中心の数字（24）はリスク管理ドメイン（RM）の MIL1～MIL3 のプラクティスの総数を示しています。また、プラクティスを評価した結果、「完全実装」「大部分実装」「一部実装」「未実装」と評価されたプラクティス数の小計がドーナツチャートに記載されています。

・完全実装（緑：4 つのプラクティスが完全に実装されている）
・大部分実装（薄い緑：4 つのプラクティスが大部分実装されている）
・一部分実装（薄い赤：5 つのプラクティスが一部分実装しかしていない）
・未実装（赤：11 のプラクティスが未実装である）

図 2 の MIL3 のドーナツチャートは MIL1 と MIL2 と MIL3 のプラクティスが表示され、MIL2 のドーナツチャートは MIL1 と MIL2 のプラクティスが、MIL1 のドーナツチャートは MIL1 のプラクティスのみ表示されます。（ドーナツチャートの中心の数字は、MIL1 から、MIL 2 、MIL 3 と達成数が加算されていく表記となります）。図 2 の RM ドメインの例だと、MIL 1 のプラクティス数は 2、MIL 2 のプラクティス数は 11 のため、ドーナツチャートの中央には、MIL2 では 13（2 + 11）が表示され、MIL1 では 2 が表示されます。

3-2. 結果サマリの見方

図 5　ES-C2M2 評価のドメインのグラフィカルな結果サマリ

	RM	ACM	IAM	TVM	SA	ISC	IR	EDM	WM	CPM
	リスク管理	資産・変更および構成管理	アイデンティティおよびアクセスの管理	脅威および脆弱性管理	状況認識	情報共有・コミュニケーション	イベント・インシデント対応と業務継続	サプライチェーンおよび外部依存性管理	要員管理	サイバーセキュリティプログラム管理
MIL評価	1	1	0	2	1	1	0	0	3	0

結果サマリ（図 5）は、シンプルでグラフィカルな成熟度評価のサマリで、各ドメインの MIL の状態が 3×10 のドーナツチャートとして描かれ、経営層が ES-C2M2 の達成状況を一望にできます。ES-C2M2 チェックシートの ECXEL(添付)では、本結果サマリも、自動算出されるようになっています。

図 5 において、薄い赤（一部分実装）と赤（未実装）がある場合は、そのドメインの当該 MIL は達成していないと見なされ、その結果、MIL 評価値としては図 5 の下段に示す通り、たとえば RM ドメインおよび ACM ドメインでは MIL 評価値＝ 1 、IAM ドメインでは MIL 評価値＝ 0 、TVM ドメインでは MIL 評価値＝ 2 となります。

従って、図 5 から、各ドメインは以下の状態である事が読み取れます。

- MIL 3 のドメイン：WM のみ
- MIL 2 のドメイン：TVM のみ
- MIL 1 のドメイン：RM, ACM, SA, ISC の 4 つ
- MIL 0 のドメイン：IAM、IR、EDM、CPM の 4 つ

ES-C2M2 では、サイバーセキュリティの 10 ドメインにわたる成熟度を評価し、下の図 6 に示す一般的なプロセス改善プロジェクトの PDCA サイクルを実行させることにより、改善活動を定量的に測定する手順を提供しています。

図 6 のプロセス改善活動の手順は、Perform Evaluation（評価の実行）、Analyze Identified Gaps（識別されたギャップの分析）、Prioritize and Plan（優先順位付けと計画の策定）、Implement Plans（計画の実施）から構成されます。

ES-C2M2 では達成すべき特定の MIL を規定していませんが、全ての組織が、少なくとも ES-C2M2 ドメインすべてにおいて MIL 1 を満たすことを推奨しています。

また、MIL の達成レベルを一律にあげるのではなく、たとえば社内検討によって、情報共有・コミュニケーション（ISC）ドメインの目標を MIL 2 に設定する一方、資産、変更および構成管理（ACM）およびイベント・インシデント対応と業務継続（IR）ドメインの目標を MIL 3 に設定する等、各事業者の状況（費用対効果）に合わせて改善計画を策定することが重要です。

図 6　プロセス改善プロジェクト

	インプット	アクティビティ	アウトプット
評価の実行	1. C2M2 自己評価 2. ポリシーと手順 3. サイバーセキュリティプログラムの理解	1. 適切な関係者の出席のもと、C2M2 自己評価ワークショップを実施する	C2M2 自己評価報告書
識別されたギャップの分析	1. C2M2 自己評価報告書 2. 組織の目標 3. 重要インフラへの影響	1. 組織の状況におけるギャップを分析する 2. ギャップから生じる可能性のある事態を評価する 3. 対処が必要なギャップを特定する	ギャップと生じ得る事態のリスト
優先順位付けと計画策定	1. ギャップと生じ得る事態のリスト 2. 組織上の制約	1. ギャップに対処するためのアクションを特定する 2. アクションの CBA（Cost-benefit analysis：費用便益分析)を実施する 3. （CBA と生じ得る事態に基づき）アクションに優先順位を付ける 4. 優先順位に基づきアクションの実装を計画する	優先順位に基づく実装計画
計画を実施する	1. 優先順位に基づく実施計画	1. 計画の進捗状況を追跡する 2. 定期的に、または大きな変更化に応じて再評価する	プロジェクト追跡データ

用語説明

以下、本解説書で使われている ES-C2M2 の固有用語を含む用語を説明します。

用語	説明	出典
情報技術 (IT)	情報の収集、処理、保守、利用、共有、発信、配置のために整備された電子情報リソースの個々のセット。ES-C2M2 の中では、相互接続している、または従属したビジネス・システムと、それらを運用する環境が定義に含まれる	DOE RMP
アイデンティティ (identity)	アイデンティティ管理者の責任範囲内で、エンティティを他のエンティティと十分に区別でき、エンティティを認識することができる属性値（特徴など）のセット	CNSSI 4009
アイデンティティとアクセス管理 (IAM)	組織の資産に論理的または物理的にアクセスする権限の与えられたエンティティの ID の作成と管理を目的とする ES-C2M2 のドメイン。重要インフラに対するリスクおよび組織目標と協調して、組織の資産へのアクセスを制限する	ES-C2M2
アクセス (access)	施設に入る、システムと通信または操作応答させる、システムのリソースを使用して情報を処理する、システムが保持する情報を得る、システムコンポーネントやファンクション（functions）を制御するといった能力や手段	CNSSI 4009
アクセス制御 (access control)	組織の資産へのアクセスを権限の与えられたエンティティ（例：ユーザー、プログラム、プロセス、またはその他システム）のみに制限する	CNSSI 4009
アクセス管理 (access management)	組織の資産に対し付与されたアクセスが、重要インフラおよび組織目標に対するリスクに見合ったものであることを確保するための管理プロセス	CERT RMM

用語	説明	出典
アドホック (adhoc)	定められた計画（文書・口頭を含む）、方針、またはトレーニングのようなかたちで組織的なガイダンスをほとんど行うことなく、個人やチーム（およびチームのリーダーシップ）のイニシアチブや経験に大きく依存する方法でプラクティスを実施すること。 成果の質は、誰がプラクティスを実施したか、対処する問題の背景、手法、ツール、使用される技術、およびプラクティスの実施に与えられた優先度に大きく依存する。経験と能力のある人物であればアドホックなプラクティスであっても高い品質の成果を出すことは可能だが、そこで得られた教訓は概して組織レベルでは蓄積されないため、アプローチや成果を組織全体で再現・改善することは困難である	ES-C2M2
アーキテクチャ (architecture)	*サイバーセキュリティアーキテクチャ*の項を参照	
依存リスク (dependency risk)	依存リスクは、ファンクションが依存するサプライヤーや外部関係者によって引き起こされる IT、OT システムの損害の発生可能性と重大度によって評価される。依存リスクの評価には、侵害されうるシステムの重要度の評価や、組織のオペレーション、資産、個人、その他組織、および国家が侵害されることによる影響の評価が含まれる	NIST 7622
イベント・インシデント対応と業務継続 (IR)	重要インフラに対するリスクおよび組織目標と協調して、サイバーセキュリティ事象を検出、分析、対応し、サイバーセキュリティ事象発生中の業務を持続させるための、計画、実施手順、および技術の確立と維持を目的とする ES-C2M2 のドメイン	ES-C2M2

用語	説明	出典
インシデント (incident)	重要インフラ、かつ/または、組織の資産およびサービスに重大な影響を与え（または重大な影響を与えるおそれがあり）、組織（およびおそらくその他利害関係者）が何らかの方法で悪影響を防止するか制限する必要のある単一の事象（または連続する事象）である	CERT RMM
インシデントライフサイクル (incident lifecycle)	インシデントの検出からクローズまでの段階のセット。集合的に、インシデントライフサイクルには、プロセスの検出、報告、ロギング、トリアージ（行動順位決定）、宣言、トラッキング、文書化、処理、調整、エスカレーションと通知、証拠の収集と保全、およびインシデントのクローズが含まれる。エスカレーションされたイベントは、正式にインシデントと宣言されない場合でも、インシデントライフサイクルに従う	CERT RMM
影響 (impact)	(電力)業界のファンクションへのネガティブな結果	ES-C2M2
SME	オペレーション・システムを理解し知見を有する分野専門家（Subject Matter Expert）の略	
エンタープライズ (enterprise)	ES-C2M2 の評価に関与する組織が属する最大の（または最高次の）組織的エンティティ。関与する側にとって、調査が実施される組織がエンタープライズそれ自体となる場合がある	SGMM v1.1 用語集
エンタープライズアーキテクチャ (enterprise architecture)	エンタープライズの IT と OT の全体の設計と記述。IT と OT の構成方法、統合方法、エンタープライズ境界での外部環境との接続方法、エンタープライズのミッションをサポートするための運用方法、エンタープライズの全体的なセキュリティ体制への対応方法などが含まれる	DOE RMP（但し、ICS から OT に変更）
エンティティ (entity)	独立している、あるいは他と区別できる何らかの存在	Merriam-Webster.com

用語	説明	出典
確立と維持（establish and maintain）	プラクティスの目標の設定と維持（プログラムなど）を意味する。たとえば、「アイデンティティの確立と維持」は、アイデンティティが支給されるだけではなく、文書化され、所有権が割り当てられ、修正措置、要件の変更、改善等の際に関連して維持されることを意味する	CERT RMM
可用性（availability）	情報に対し、迅速で信頼できるアクセスと使用を確保すること。資産においては、必要なときにいつでも認証済みユーザー（人、プロセス、機器）がアクセスできる品質を指す	DOE RMP / CERT RMM
完全性（integrity）	不適切な情報の修正や破壊からの保護。完全性には、否認不可性と真正性の保証が含まれる。資産にとっての完全性とは、所有者が意図した状態にあり、意図した目的で継続利用できる品質のことである	DOE RMP / CERT RMM
管理目標（management objectives）	管理目標はドメインの管理化を目指す目標を示す。管理化は、サイバーセキュリティに関するプラクティスまたはアクティビティの実施が組織のオペレーションにどの程度浸透しているかを示している	ES-C2M2
管理プラクティス（management practices）	各ドメインにおける固有のプラクティスが管理化されているかを測定するためのプラクティス	ES-C2M2
管理アクティビティ（management activities）	C2M2 において、各ドメインにおける管理プラクティスのセットを管理アクティビティと呼ぶ	ES-C2M2
ガイドライン（guideline）	SME およびコミュニティのコンセンサスを代表する広く認められた権威体または自組織内で作成された推奨されるプラクティスのセット	ES-C2M2

用語	説明	出典
ガバナンス (governance)	責務を満たし、適切にリスクを管理し、効率的に財政的、人的リソースを利用するために、戦略的な指示を与える組織的なプロセス。またガバナンスには、スポンサーシップ（経営目線での確認）、コンプライアンス（組織がコンプライアンスの責務を遵守しているか確認）、および連携（サイバーセキュリティプログラム管理のプロセスが戦略目標に連携していることを確認）等のコンセプトが含まれる	CERT RMM
脅威 (threat)	不正アクセスによる、IT、OTまたは通信インフラを経由した、情報への破壊、暴露、改竄および/またはサービス妨害が、組織の運営（ミッション、ファンクション、イメージ、評判も含まれる）、リソース、その他の組織に悪影響を与える可能性のある状況またはイベント	DOE RMP
脅威および 脆弱性管理 (TVM)	重要インフラ に対するリスクおよび組織目標と協調して、サイバーセキュリティの脅威と脆弱性を検出、特定、分析、管理および対応するための、計画、実施手順、および技術の確立と維持を目的とする ES-C2M2 のドメイン	ES-C2M2
脅威分析 (threat assessment)	IT および ICS または組織に対する脅威の重大度を評価し、脅威の性質を説明するプロセス	ES-C2M2
共通状況認識(COP)	他のモデルドメインのステータスやサマリ情報等を含むサイバーセキュリティ情報を収集、分析、警告、表示、および使用するアクティビティとテクノロジー	ES-C2M2

用語	説明	出典
業務回復性 (operational resilience)	組織の中核的オペレーションに影響するリスクへの適応力。業務回復性は効果的な業務上のリスク管理における新出の特性であり、セキュリティおよびビジネス継続性のようなアクティビティによりサポートされ有効となる。 エンタープライズの回復性がビジネスリスクおよび信用リスクのようなリスク分野を含む一方で、エンタープライズ回復性のサブセットである業務回復性は組織の業務上のリスクを管理する能力にフォーカスしている	CERT RMM
業務上のリスク (operational risk)	不適切あるいは失敗した内部処理、システムまたは技術的失敗、故意または不注意な人的行為、あるいは外部の事象に起因する資産と関連サービスへの潜在的影響。ES-C2M2 ではサイバーセキュリティ脅威からの業務上のリスクにフォーカスしている	CERT RMM
機密性 (confidentiality)	個人のプライバシーや専有情報の保護の手段など、情報のアクセスと公開に関する承認された制限を維持すること。情報資産において機密性は、認証された人、プロセスおよび機器のみ、その資産にアクセス可能であるという性質を意味する	DOE RMP / CERT RMM
検証 (validate)	たとえば、情報、モデル、製品、システムあるいはコンポーネントなどの何等かの対象が特定の目的に即しているかの品質を確認および確証するために行う証拠集めと評価	ES-C2M2
構成ベースライン (configuration baseline)	IT/OT システム、資産、またはシステム内の構成アイテムのための仕様を文書化したもので、任意の時点で正式にレビューされ承認を得ているもの。構成ベースラインは変更管理手順を経由してのみ変更が可能である。構成ベースラインは将来のビルド、リリース、かつ/または変更の基礎として使用される	NIST800-53 用語集

用語	説明	出典
構成管理 (configuration management)	資産の完全性を確立、維持することにフォーカスしたアクティビティのセット。これには資産のライフサイクルを通じた構成の初期化、変更、およびモニタリング等が含まれる	NIST SP 800-128
コントロール (controls)	機密性、完全性およびシステムとその情報の可用性を保護するため、IT および ICS のために記述された、管理、オペレーション、技術的手法、方針、および実施手順。手動、自動を問わない （例：セーフガードまたは対抗手段）	DOE RMP
サービスレベル合意書 (SLA)	関連するサイバーセキュリティ要求事項の達成や提供されるサービスの品質に対する顧客の期待の設定など、サービスプロバイダーにおける特定の責務を定義した文書	CNSSI 4009
サイバー攻撃 (cyber attack)	サイバースペース経由で、コンピューティング環境/インフラの停止、無効化、破壊または悪意をもってコントロールする、あるいは、データの完全性を破壊または秘匿された情報を盗むために、企業のサイバースペースの使用を標的にした攻撃	DOE RMP
サイバーセキュリティ (cybersecurity)	サイバースペースの使用をサイバー攻撃から保護するあるいは防御する能力。コンピュータまたはコンピュータ化したシステムを不正なアクセスまたは攻撃から保護するために取られる手段	DOE RMP / Merriam-Webster.com
サイバーセキュリティアーキテクチャ (cybersecurity architecture)	組織のミッションや戦略計画と協調し、企業のセキュリティプロセス、サイバーセキュリティのシステム、担当者、および下位組織の構造と活動を定義するエンタープライズアーキテクチャにとって不可欠な部分	DOE RMP
サイバーセキュリティインシデント (cybersecurity incident)	*インシデント*の項を参照	

用語	説明	出典
サイバーセキュリティプログラム (cybersecurity program)	サイバーセキュリティプログラムは、組織かつ/またはファンクションのサイバーセキュリティの目標を達成するためにデザインされ、管理される各アクティビティを統合したものである。サイバーセキュリティプログラムは、組織またはファンクションいずれのレベルでも実装可能だが、全社的なアクティビティの統合や、特定のリソースへの投資の集中といった、よりハイレベルな実装と全企業的視点は、組織に利益をもたらす可能性がある	ES-C2M2
サイバーセキュリティプログラム管理 (CPM)	サイバーセキュリティの目標を、組織の戦略的目標および重要インフラへのリスクと協調し、組織のサイバーセキュリティ活動のためのガバナンス、戦略立案、およびスポンサーシップを提供するエンタープライズサイバーセキュリティプログラムの確立と維持を目的とする ES-C2M2 のドメイン	ES-C2M2
サイバーセキュリティプログラム戦略 (cybersecurity program strategy)	組織がミッション、ビジョン、サイバーセキュリティプログラムの目的を達成するために設定したパフォーマンス目標を達成するために設計された行動計画	CERT RMM
サイバーセキュリティにおける責任 (cybersecurity responsibilities)	組織のサイバーセキュリティ要求事項を満たすための責務	ES-C2M2
サイバーセキュリティリスク (cybersecurity risk)	情報、IT および OT に対する不正アクセス、不正使用、暴露、妨害、改竄、または破壊によって引き起こされる、組織の運営（ミッション、ファンクション、イメージ、評判等も含まれる）、リソース、および他の組織へのリスク	DOE RMP

用語	説明	出典
サプライチェーン (supply chain)	製品やサービス（部分要素を含む）を作ってサプライヤーから組織の顧客へ移動させるための組織、人、アクティビティ、情報、リソースのセット。 サプライチェーンは、設計、開発、およびカスタムまたは商用オフザシェルフ（COTS）製品の取得、システム統合、その環境内でのシステム運用、廃棄を含む、製品の全ライフサイクルを包含する。人、プロセス、サービス、プロダクト、およびプロダクトを構成する要素がサプライチェーンに影響を与える	NISTIR 7622 [NDIA ESA] の原文のパラグラフ 1 から引用
サプライチェーンおよび外部依存性管理 (EDM)	重要インフラに対するリスクと組織目標と協調して、外部のエンティティに依存するサービスと資産に関連するサイバーセキュリティリスクを管理するコントロールの確立と維持を目的とする ES-C2M2 のドメイン	ES-C2M2
重要インフラ (critical infrastructure)	社会を下支えする必須サービスを提供する資産。国家は数多くの重要リソースを所有しており、テロリストが悪用または破壊すれば、大量破壊兵器の使用に匹敵する壊滅的な健康への影響または大量の死傷者を生むおそれや、国家の名声、士気に深刻な影響を与えるおそれがある。加えて、不可欠である重要インフラが無力化、悪用、または破壊されれば、セキュリティおよび経済的健全性を衰退させるような影響が及ぶ可能性がある	HSPD-7
状況認識 (SA)	重要インフラに対するリスクおよび組織目標と協調して、電力システムやサイバーセキュリティについて、他のモデルドメインからのステータスやサマリ情報などを含む情報を収集、分析、警告、表示、使用することにより共通状況認識（COP）を作成する活動と技術を確立し、維持することを目的とする ES-C2M2 のドメイン	ES-C2M2

用語	説明	出典
情報共有・伝達 (ISC)	重要インフラに対するリスクおよび組織目標と協調して、脅威や脆弱性などのサイバーセキュリティ情報を収集および提供し、リスクを低減し、業務回復性を高めるために内外のエンティティとの関係を確立、維持することを目的とする ES-C2M2 のドメイン	ES-C2M2
資産オーナー (asset owner)	組織の内部または外部の、組織の資産の能力、生産性、回復力に最も大きな責任を負っている人物または組織の部門	CERT RMM
スポンサーシップ (sponsorship)	上級管理職がサイバーセキュリティの正式な方針を示す、または経営層がリソースを提供するとともにサイバーセキュリティプログラムに対するコミットメントを宣言する、などの全社規模のサポート。上級管理職は、サイバーセキュリティプログラムのパフォーマンスと実行を監視し、積極的に進行中のサイバーセキュリティプログラムのあらゆる側面の継続的な改善活動に積極的に参加する	ES-C2M2
脆弱性 (vulnerability)	サイバーセキュリティの脆弱性とは、脅威元によってエクスプロイトされる可能性のある IT、OT、通信システム、機器、システムの実施手順、または、内部統制や実装の弱点や欠陥のこと。*脆弱性*クラスは、共通的な脆弱性のグループである	NIST IR7628 Vol. 1, pp. 8
成熟度 (maturity)	組織がモデルのサイバーセキュリティのプラクティスを実装または管理化しているかの度合い	ES-C2M2
成熟度モデル (maturity model)	組織のサイバーセキュリティ能力がどの程度成熟しているかを示すモデルであり、C2M2 の中核となるコンセプト	ES-C2M2
制御・運用技術 (OT)	物理環境と相互作用する（あるいは物理環境と相互作用する機器の管理をする）プログラム可能なシステムや機器。例としては、産業用制御システム、ビル管理システム、火器管制システム、および、物理アクセス制御機構などがある	ES-C2M2

用語	説明	出典
管理化 (institutionalization)	あるプラクティスまたはアクティビティが組織のオペレーションに浸透している度合い。アクティビティが組織の運用の一部になるほど、そのアクティビティは長期間にわたり、高品質な一貫性をともなって実施される傾向がある（「企業がルーティン的に従う企業文化の一部として浸透した業務の方法に組み込まれること」 - CERT RMM）	ES-C2M2
セキュアソフトウェア開発 (Secure software development)	ソフトウェア開発のライフサイクルを通じ、認められたプロセス、安全なコーディング標準、ベストプラクティス、およびソフトウェアシステム内でセキュリティの脆弱性を最小にすることが証明されているツールを使用してソフトウェアを開発すること。重要な点の 1 つに、セキュアソフトウェア開発の訓練がされているプログラマーやソフトウェアアーキテクトに従事させることがあげられる	ES-C2M2
資産 (asset)	組織にとって何らかの価値を持つもの。資産には、技術、情報、従業員が遂行する役割、設備など多くのものが含まれる。 本モデルの目的において考慮すべき資産は､IT と OT のハードウェアおよびソフトウェア資産やファンクションの運用にとって必須となる情報である	ES-C2M2
資産、変更および構成管理 (ACM)	重要インフラに対するリスクおよび組織目標と協調して、組織のハードウェアとソフトウェア両方を含む IT および OT 資産を管理することを目的とする ES-C2M2 のドメイン	ES-C2M2
戦略目標 (strategic objectives)	組織がミッション、ビジョン、価値、目的を達成するために設定したパフォーマンス目標	CERT RMM
戦略計画 (strategic planning)	戦略目標とこれらの目標を達成するための計画を開発するプロセス。	CERT RMM

用語	説明	出典
組織の目標 (organizational objectives)	*戦略目標*の項を参照	CERT RMM
多要素認証 (multifactor authentication)	本人認証されるために 2 つ以上の要素を使用する認証。要素には、(i) その人物が知っていること（例：パスワード/PIN）、(ii) その人物が持っているもの（例：暗号 ID 機器, トークン）、(iii) その人物にあるもの（例：biometric）、または (iv) その人物が居ると言っている場所（例：GPS トークン）などがある	NIST800-53
デプロビジョニング (deprovisioning) - アクセス無効化	組織の資産へのアイデンティティのアクセスを無効または削除するプロセス	CERT RMM
電力業界 (electricity subsector)	発電、送電、配電が含まれるエネルギーセクターの一部門	ES-SPP
ドメイン (domain)	本モデル構造において、サイバーセキュリティのプラクティスを論理的にグループ分けした単位をドメインという	ES-C2M2
トレーサビリティ (traceability)	元々の属性がどのように作られ、時間とともにどのように変化したかを示す履歴に保存されている証拠に基づき、与えられた属性の現状（たとえば、システムの現在の構成あるいは、ユーザーのものとされるアイデンティティなど）が正当か否かを判断する能力	ES-C2M2
認証 (Authentication)	ユーザー、プロセス、または機器のアイデンティティを、IT または ICS のリソースへのアクセス許可の前提条件として検証すること	DOE RMP
標準 (standard)	標準は、同意により定められ、ルール、ガイドライン、またはアクティビティの特徴やその結果を提供する文書	ISO/IEC Guide2:2004

用語	説明	出典
変更管理 (change control/change management)	最小限の中断（disruption）で、承認された変更を実現可能にする、インフラ関連またはサービスの各側面の情報や技術資産への変更を管理する継続的プロセス	CERT RMM
ファンクション (function)	ハイレベルな電力システムのアクティビティ、あるいは、モデルが適用される公益事業者により実行されるアクティビティのセット。一般的にファンクションは、発電、送電、配電、および/またはマーケットである。ES-C2M2 の評価サーベイを使用する際、ファンクションは、モデルを完了して評価される組織の業務ライン（発電、送電、配電、またはマーケット）のこと	ES-C2M2
プラクティス (practice)	C2M2 で定義されているサイバーセキュリティ能力を強化するために実践すべき要件であり、MIL1～MIL3 それぞれのレベルに応じた難易度のプラクティスが定義されている	ES-C2M2
プロビジョニング (provisioning)	アイデンティティのプロファイルおよびそれに関連付けられた役割とアクセス特権を割り当てる、もしくはアクティベートするプロセス	CERT RMM
POC (point of contact)	ワークショップへのメンバー参加管理等を担い、ファシリテーターを支援する役割をもつ組織の窓口	本書にて作成
MIL (成熟度指標レベル)	C2M2 において成熟度を示すレベルであり、MIL1～MIL3 までが定義されている。上位のレベルを達成するほど、組織のサイバーセキュリティ能力が成熟していることを示す	ES-C2M2
目的 (ゴール)	C2M2 の各ドメインで定義されている、サイバーセキュリティ能力として実現したい要件	ES-C2M2
目標 (Objective)	C2M2 の各ドメインで定義されている、サイバーセキュリティ能力を向上するための目標であり、各ドメインで 2 から 5 つの目標が定義されている	ES-C2M2

用語	説明	出典
目標復旧時間 (RTO)	組織が重要なインフラおよび組織の目標を達成するために、中断したファンクションの復旧について組織が設定し、文書化したゴールとパフォーマンス目標	ES-C2M2
モニタリング (monitoring)	システムおよび人の振舞いとアクティビティの情報を収集、記録、配布して、運用とサービスの提供に悪影響を与えるおそれのある組織の資産と重要インフラへのリスクを特定、分析する継続的なプロセスをサポートすること	CERT RMM
要員管理 (WM)	重要インフラに対するリスクおよび組織目標と協調して、サイバーセキュリティの風土を生み出し、担当者の継続的な適合性と能力を高める計画、実施手順、技術、およびコントロールを確立・維持することを目的とする ES-C2M2 のドメイン	ES-C2M2
利害関係者 (stakeholder)	その組織またはこのモデルを使用し評価されるファンクションとそのプラクティスに既得権がある、組織または内外の人物またはグループ。任意のプラクティスの実施に関与する利害関係者には、ファンクション内、組織全体から、あるいは、組織の外部の者を含めてよい	出典：CERT RMM
リスク (risk)	組織が潜在的な状況または事象により脅威にさらされる範囲の尺度。通常は、（1）状況または事象により発生する悪影響、（2）発生の可能性の相関関係	DOE RMP
リスク分析 (risk analysis)	リスクの状況と潜在的影響の理解にフォーカスし、リスクの優先順位付け、リスク対応の手順の決定を行うリスク管理アクティビティ。洗い出された各リスクの重要度を決定し、組織がリスクへ対応しやすいようにする。	CERT RMM
リスク評価 (risk assessment)	IT と ICS の運用の結果生じる、組織のオペレーション（ミッション、ファンクション、イメージ、評判などを含む）、リソース、その他組織、国家に対するリスクを洗い出すプロセス。	DOE RMP

用語	説明	出典
リスク基準 (risk criteria)	業務上のリスクを、影響度、リスク許容度およびリスク対応手法に基づき、評価、カテゴリ分け、優先順位付けするために組織が使用する目標基準	ES-C2M2
リスク管理 プログラム (risk management program)	組織のオペレーション（ミッション、ファンクション、イメージ、評判などを含む）、リソース、その他組織、国家に対するサイバーセキュリティリスクを管理するプログラムと支援プロセス。これには、（1） リスク関連アクティビティのためのコンテキストの確立、（2） リスク評価、（3） 確定したリスクへの対応、（4） 継続的なリスクのモニタリングを含む	DOE RMP
リスク管理 (RM)	事業単位、子会社、関連する相互接続インフラおよび利害関係者へのサイバーセキュリティリスクを特定、分析、低減するためのエンタープライズサイバーセキュリティリスク管理プログラムを策定、運用、維持することを目的とした ES-C2M2 のドメイン	ES-C2M2
リスク管理戦略 (risk management strategy)	上級管理職が組織のオペレーション、リソースその他組織に関するリスクをどのように管理するかを決める戦略レベルの意思決定	DOE RMP
リスク低減 (risk mitigation)	適切なリスク削減コントロールの優先順位付け、評価、実装	DOE RMP
リスク管理表 (risk register)	組織に対して発生しうるリスクをスプレッドシートやデータベースで登録し、一元的に管理できるようにしたもの	ES-C2M2
リスク対応 (risk response)	組織のオペレーション、リソース、およびその他組織へのリスクの保有、回避、低減、共有、または移転	DOE RMP

用語	説明	出典
リスク分類 (risk taxonomy)	組織が被害を受ける可能性があり、管理する必要がある共通リスクの種類と一覧。リスク分類は、組織の資産やサービスがリスクの影響を受けていれば、これらのリスクを理解し、その組織の部門または業務ラインに固有の低減措置を策定する際に用いるコミュニケーションのための手段	CERT RMM
ロギング (logging)	ロギングは通常、自動化されたシステム、ネットワーク、またはユーザーアクティビディの（IT または OT システムの要素による）記録管理をいう。保護された資産や制限されたエリアに従業員による物理的アクセスの手書きによる記録（たとえば、入館記録）を付けることもロギングに含まれるが、物理アクセス活動は自動ロギングするのが一般的である。（手動または自動ツールによる）ログの定期的なレビューと監査は（例：サイバーセキュリティ事象または弱点の検出による）状況認識に不可欠な重要なモニタリング活動である	ES-C2M2

頭字語

頭字語	定義
C2M2	Cybersecurity Capability Maturity Model
CBA	Cost Benefit Analysis
CERT®-RMM	CERT® Resilience Management Model
CIP	Critical Infrastructure Protection
COP	Common Operating Picture
COTS	Commercial Off-The-Shelf
CRPA	Cyber Risk Preparedness Assessment
CVSS	Common Vulnerability Scoring System
DHS	Department of Homeland Security
DOE	Department of Energy
ES-C2M2	Electricity Subsector Cybersecurity Capability Maturity Model
ES-ISAC	Electricity Sector Information Sharing and Analysis Center
FIRST	Forum of Incident Response and Security Teams
FERC	Federal Energy Regulatory Commission
GWAC	GridWise Architecture Council
HR	Human Resources
IAM	Identity and Access Management
ICS	Industrial Control System
ICS-CERT	Industrial Control Systems Cyber Emergency Response Team
ICSJWG	Industrial Control Systems Joint Working Group
IEC	International Electrotechnical Commission
ISAC	Information Sharing and Analysis Center
IT	Information Technology
MIL	Maturity Indicator Level
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
OT	Operations Technology
RAWG	[European Union M/490] Reference Architecture Working Group
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RMP	Electricity Subsector Cybersecurity Risk Management Process Guideline

頭字語	定義
SCADA	Supervisory Control And Data Acquisition
SEI	Software Engineering Institute
SGIP	Smart Grid Interoperability Panel
SLA	Service Level Agreement
SME	Subject Matter Expert
US-CERT	United States Computer Emergency Readiness Team
VoIP	Voice over Internet Protocol