ES-C2M2の活用について

（制御システムのセキュリティマネジメント成熟度自己評価の勧め）

2020年2月14日

独立行政法人 情報処理推進機構
セキュリティセンター セキュリティ対策推進部 脆弱性対策グループ
研究員（CISSP, エネルギー管理士）
木下　弦

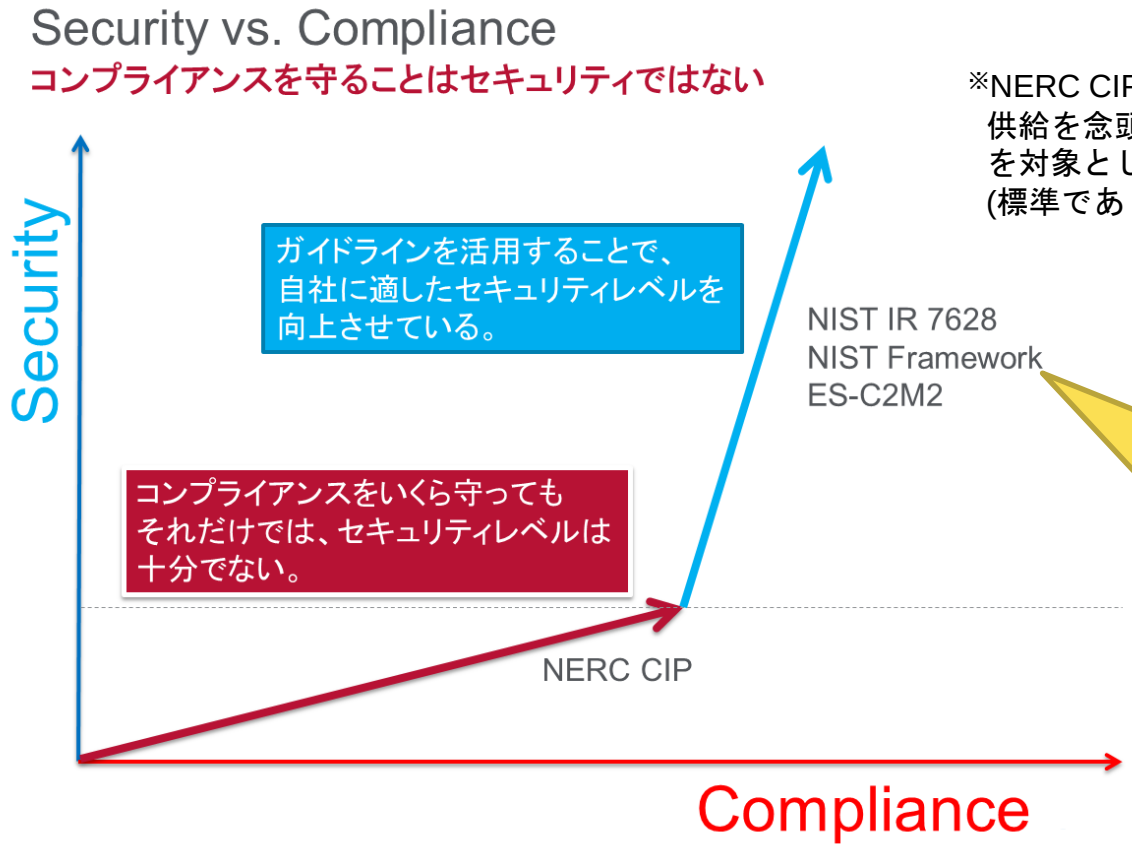
AGENDA

- 米国の標準活用状況
- 制御システムセキュリティに関するIPAの取組み
- ES-C2M2の活用について

- 米国の標準活用状況
- 制御システムセキュリティに関するIPAの取組み
- ES-C2M2の活用について

各種標準をセキュリティレベルの改善に活用
米国の事例調査より

- 経済産業省「平成26年度電気施設技術基準国際化調査(電気設備)」サイバーセキュリティ対策に関する調査報告より
  - **米国における電力会社のセキュリティ標準、ガイドライン活用方法:**
    「*コンプライアンス(NERC CIP Standard※)で最低限のセキュリティ*を確保した上で、*ガイドラインを活用*し、*必要なセキュリティレベルへの向上*を図り、社内ポリシーに反映する」

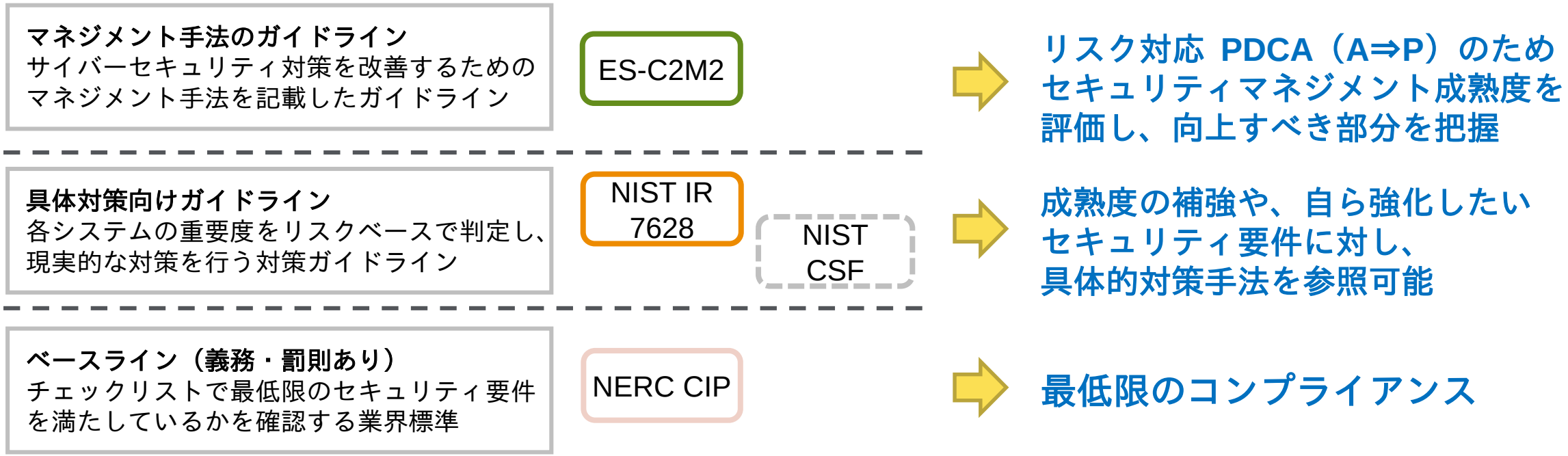


※NERC CIP Standardは、2003年の大停電を踏まえて、電力の安定供給を念頭において作成された主に大規模発電施設及び送電施設を対象としたサイバーセキュリティに関する標準
(標準であり規制でもある：違反には罰金が科される)

セキュリティレベルを向上させるガイドラインとして米電力業界ではこの3つが活用されている
- **NIST IR 7628**
- **NIST Framework (NIST CSF)**
- **ES-C2M2**

米電力業界における標準・ガイドライン位置付け

- 米電力業界には約3000の事業者が存在するが、規模の大小問わず、自己評価ツールとして浸透している（経済産業省平成26年度電気施設技術基準国際化調査（電気設備）サイバーセキュリティ対策に関する調査報告）
- 米国電力業界コンプライアンスは、NERC CIPがベースライン（業法に基く罰則規定を含んだ基準）として制定されている
- レベル向上のためのガイドラインとして、ES-C2M2・NIST IR 7628・NIST CSF がある



標準・ガイドラインの概要

#	規格/基準	作成者	基準の概要
1	NERC CIP ※1 （Version5）	NERC	米国電力事業(発電、送電、配電)が業法に基き準拠すべき標準。 12エリア42項目 233細則の規準から構成され、違反に対する罰金規定がある。
2	ES-C2M2 ※2 （Ver1.1：2014）	DoE ※3	米国電力企業のセキュリティマネジメントの成熟度を測定するモデル。 10分類37項目312細則の項目に対して4段階評価を実施。
3	NIST IR 7628 （R1：2014/9 ）	NIST	スマートグリッド（スマートメータ、需給制御システム等を含む）の電力制御システムのセキュリティ要件に関する NIST 内部レポート。 19エリア197項目の要件から構成。
4	NIST CSF ※4	NIST	米大統領令により NIST で策定された、リスクベース・アプローチに基く業界標準およびベストプラクティスをまとめた自主参加型のフレームワーク。 識別(ID)，防御(PR)，検知(DE)，対応(RS)，復旧(RC) の 5機能に対して 23カテゴリ/108サブカテゴリごとにプラクティスの参考情報がピックアップされている。

※1 NERC CIP： North American Electric Reliability Corporation（北米電力信頼性評議会）が発行した Critical Infrastructure Protection Standard（重要インフラ防護標準）
※2 ES-C2M2： Electricity Subsector Cybersecurity Capability Maturity Model Program（電力分野用セキュリティマネジメント成熟度モデル）
※3 DoE： Department of Energy（米国エネルギー省）
※4 NIST CSF： National Institute of Standards and Technology（米国国立標準技術研究所）によるCyberSecurity Framework

- 米国の標準活用状況
- 制御システムセキュリティに関するIPAの取組み
- ES-C2M2の活用について

制御システムのインシデント対応の指針

○ 制御システムはインシデント発生時、設備損傷や危険を伴う（安全確保の必要が生じる）ケースがあるため、
事業継続リスクとインシデント対応をBCPで考える必要がある

● NISC「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第5版）」

重要インフラサービスの安全かつ持続的な提供の実現を図る観点：
「機能保証の考え方」を踏まえ、サービスの提供に必要な情報システムのセキュリティを確保し、サイバー攻撃等による重要インフラサービス障害の発生を可能な限り減らすとともに、障害発生の早期検知や、障害の迅速な復旧を図ることが重要

- 機能保証の考え方　（「重要インフラの情報セキュリティ対策に係る第4次行動計画」からの抜粋）
  - 重要インフラサービスは、それ自体が国民生活及び社会経済活動を支える基盤となっており、その提供に支障が生じると国民の安全・安心に直接的かつ深刻な負の影響が生じる可能性がある。このため、各関係主体は、重要インフラサービスを安全かつ持続的に提供するための取組（機能保証）が求められる。
  - なお、本行動計画において、「機能保証」とは、各関係主体が重要インフラサービスの防護や機能維持を確約することではなく、各関係主体が重要インフラサービスの防護や機能維持のためのプロセスについて責任を持って請け合うことを意図している。すなわち、各関係主体が重要インフラ防護の目的を果たすために、情報セキュリティ対策に関する必要な努力を適切に払うことを求める考え方である。

● IEC62443(2010)

4.3.2.5　Business Continuity Plan (事業継続計画)

IPAは制御システムのリスク分析を支援

～セキュリティリスク分析の重要性を訴えてきた～

中国、春秋時代の軍事戦略家、孫武の兵法書『孫子』に示された名句に
「彼を知り己を知れば百戦殆うからず」がある。サイバー攻撃時代において、敵＝脅威（攻撃者を含む）、己＝自組織と置き換えてみると、セキュリティ対策において効果的な施策を実施するための教えとなる。
セキュリティリスク分析は、

己を知り、敵を知れば、百戦危うからず

を実践する、**サイバーセキュリティ時代の兵法**である。

「リスク分析」：以下を評価指標に、事業リスクを明確にするプロセス

① 評価対象（資産や事業）の価値（重要性）、想定される被害の規模・影響
② 評価対象に対して想定される脅威とその発生の可能性
③ 想定される脅威が生じた際の受容可能性（評価対象の脆弱性、対策不備）

リスク分析の重要性と有効性

- 実効的なリスクの低減の実現
- 効果的なセキュリティ投資の実現（追加対策、有効なテスト箇所の抽出）
- PDCAサイクルの確立とセキュリティの維持向上を継続するためのベース

制御システムのセキュリティリスク分析ガイド
第2版　ガイド本編と別冊、活用の手引き

- 自組織でリスクアセスメントを実施し、セキュリティ対策を向上するための実践的な分析手法の解説書
  - リスク分析の全体像の理解向上と取り組みを促進
  - リスク分析を具体的に実施するための手順や手引き
  - 2通りの詳細リスク分析の手法（資産ベース、事業被害ベース）を解説
- リスク分析のための素材を提供
- リスク分析結果の活用例の提示
  - リスク低減の対策強化策の検討方法
  - セキュリティテストの解説

2018年10月15日　第2版公開

ガイド本編

380頁

別冊

94頁

活用の手引き

36頁

https://www.ipa.go.jp/security/controlsystem/riskanalysis.html　からダウンロード可能

リスクアセスメント　（ISMSの定義から引用）

リスク特定	リスク分析	リスク評価
リスク発見・認識のプロセス	リスク特質理解とリスクレベル決定	リスクが対応・受容可能かを決定

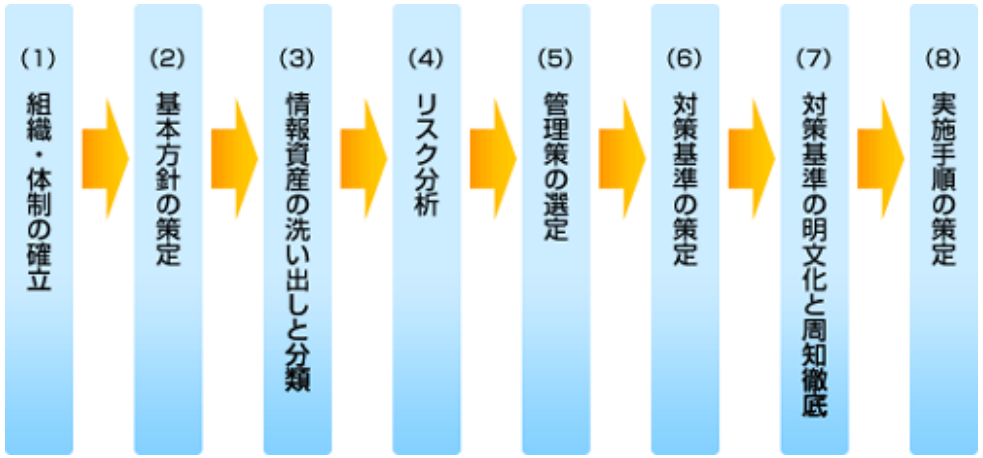
→ リスクマネジメント

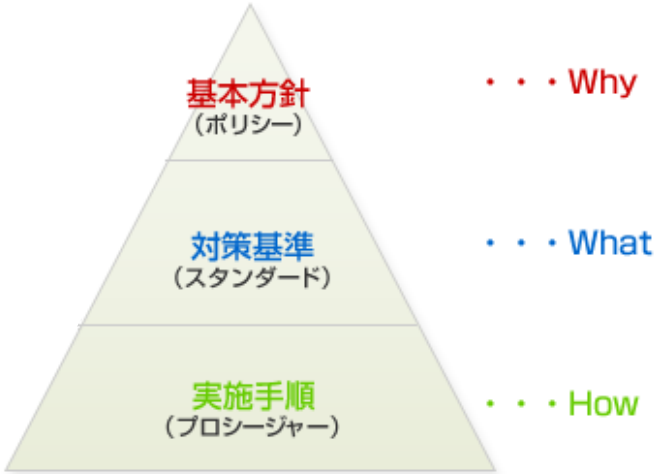
リスクマネジメント支援の補強

「情報セキュリティマネジメントとPDCAサイクル」

○ 制御システムにおけるセキュリティマネジメントに関してのガイドライン補強

① PLAN：　セキュリティポリシーの策定／マネジメントシステムの確立

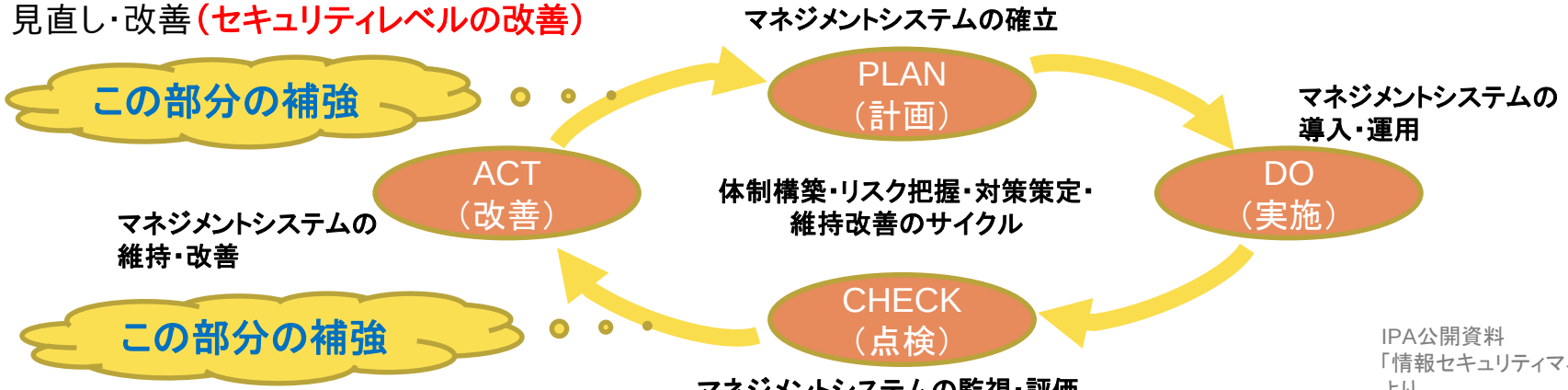




② DO：　リスクアセスメントの実施／リスクへの対応／管理策の導入と運用

③ CHECK：　セキュリティの評価（セキュリティレベルの評価）

④ ACT：　見直し･改善（セキュリティレベルの改善）



IPA公開資料
「情報セキュリティマネジメントとPDCAサイクル」
より

- 制御システムセキュリティに関するIPAの取組み
- 米国の標準活用状況
- ES-C2M2の活用について

ES-C2M2
IPAで翻訳・資料作成

	作成物	概要
1	チェックシート	10ドメイン37目標312プラクティスの項目を日本語化 4段階評価を実施して評価結果をドーナツチャートで表示
2	解説書	チェックシートの使用方法、基準の概要、用語の定義等の解説ドキュメント

	対象バージョン	作成者	補足
	Ver1.1：2014	DoE	Ver1.1 ベース （Ver2.0への対応は現時点では未定）

ES-C2M2　ドメインと目標の概要

略号	Domain	Objective	ドメイン	目標
RM	1 Risk Management	1. Establish Cybersecurity Risk Management Strategy	1. リスク管理	1. サイバーセキュリティリスク管理戦略の策定
		2. Manage Cybersecurity Risk		2. サイバーセキュリティリスク管理
		3. Management Activities		3. 管理アクティビティ
ACM	2 Asset, Change, and Configuration Management	1. Manage Asset Inventory	2. 資産、変更および構成管理	1. 資産インベントリ管理
		2. Manage Asset Configuration		2. 資産構成の管理
		3. Manage Changes to Assets		3. 資産の変更管理
		4. Management Activities		4.管理アクティビティ
IAM	3 Identity and Access Management	1. Establish and Maintain Identities	3. アイデンティティおよびアクセスの管理	1.アイデンティティの確立および維持
		2. Control Access		2. アクセス制御
		3. Management Activities		3. 管理アクティビティ
TVM	4 Threat and Vulnerability Management	1. Identify and Respond to Threats	4. 脅威および脆弱性管理	1. 脅威の特定と対応
		2. Reduce Cybersecurity Vulnerabilities		2. サイバーセキュリティ脆弱性の低減策
		3. Management Activities		3. 管理アクティビティ
SA	5 Situational Awareness	1. Perform Logging	5. 状況認識	1.　ログの取得
		2. Perform Monitoring		2. モニタリング
		3. Establish and Maintain a Common Operating Picture (COP)		3. 共通状況認識（COP）の策定と維持
		4. Management Activities		4. 管理アクティビティ
ISC	6 Information Sharing and Communications	1. Share Cybersecurity Information	6. 情報共有・コミュニケーション	1. サイバーセキュリティ情報の共有
		2. Management Activities		2. 管理アクティビティ
IR	7 Event and Incident Response, Continuity of Operations	1. Detect Cybersecurity Events	7. イベント・インシデント対応と業務継続	1. サイバーセキュリティイベントの検出
		2. Escalate Cybersecurity Events and Declare Incidents		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. Respond to Incidents and Escalated Cybersecurity Events		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. Plan for Continuity		4. 業務継続計画
		5. Management Activities		5. 管理アクティビティ
EDM	8 Supply Chain and External Dependencies Management	1. Identify Dependencies	8. サプライチェーンおよび外部依存性管理	1. 依存関係の特定
		2. Manage Dependency Risk		2. 依存リスクの管理
		3. Management Activities		3. 管理アクティビティ
WM	9 Workforce Management	1. Assign Cybersecurity Responsibilities	9. 要員管理	1. サイバーセキュリティにおける責任の割り当て
		2. Control the Workforce Life Cycle		2. 要員ライフサイクルの管理
		3. Develop Cybersecurity Workforce		3. サイバーセキュリティ要員の育成
		4. Increase Cybersecurity Awareness		4. サイバーセキュリティ意識の向上
		5. Management Activities		5. 管理アクティビティ
CPM	10 Cybersecurity Program Management	1. Establish Cybersecurity Program Strategy	10. サイバーセキュリティプログラム管理	1. サイバーセキュリティプログラム戦略の策定
		2. Sponsor Cybersecurity Program		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. Establish and Maintain Cybersecurity Architecture		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. Perform Secure Software Development		4. セキュアなソフトウェア開発
		5. Management Activities		5. 管理アクティビティ

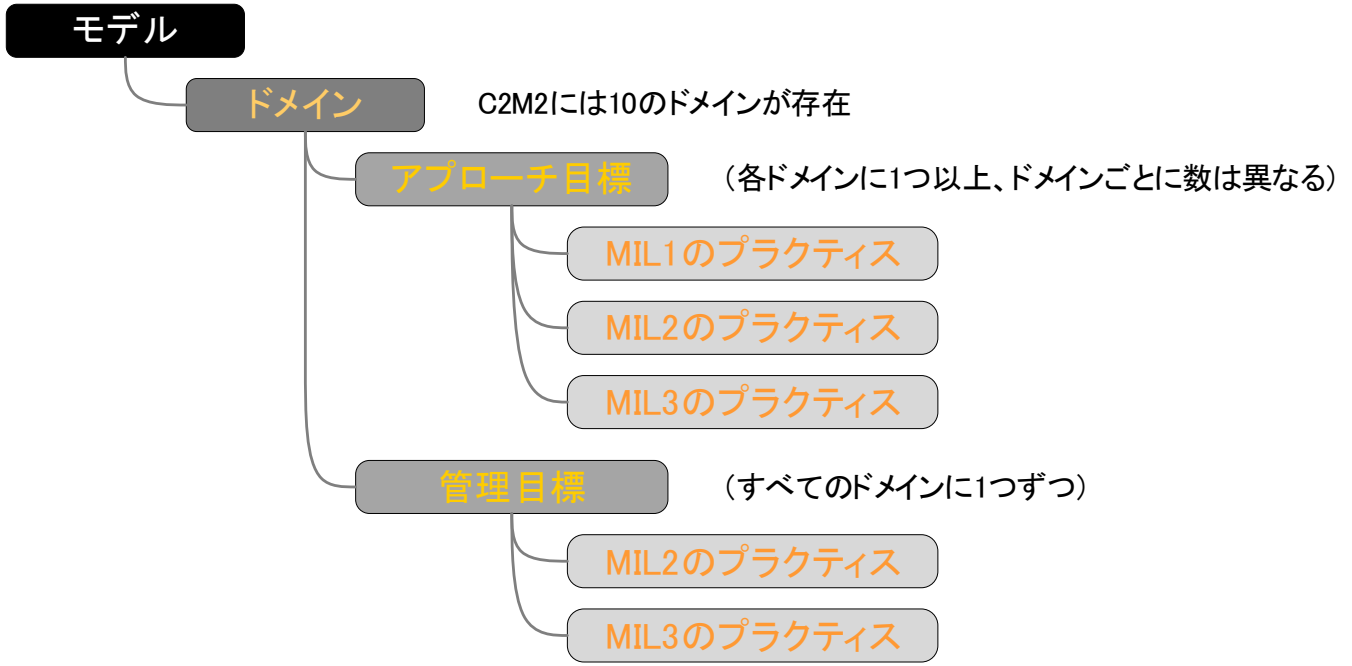
10 ドメイン

37 目標（ 312 プラクティス ）

ES-C2M2　ドメインの構成

○ C2M2モデルの10ドメインに共通する構成

- 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）”が存在する



“目標”は、ドメイン毎に規定されるドメイン固有の“アプローチ目標”と、
全ドメインでほぼ共通の“管理目標”（管理アクティビティ）で構成される

ES-C2M2
プラクティスと評価レベルMIL(Maturity Indicator Level)

- MIL (Maturity Indicator Level):
  - ✓成熟度指標レベル(MIL0～3の4段階)
  - ✓目標に対して実施すべきプラクティスがMIL毎(MIL1:51, MIL2:126, MIL3:135)に合計312個リストアップされている
    ※MIL1のプラクティスはコストをかけずに実装できるよう設計されている
- ✓プラクティスの個別評価(4段階):
  青字は達成、赤字は未達の評価となる
  「完全実装(Fully Implemented)」
  「大部分実装(Largely Implemented)」
  「一部分実装(Partially Implemented)」
  「未実装(Not-Implemented)」
- ✓MILの評価:
  MILはドメイン毎に集計して評価。
  ドメインのあるMILのプラクティスを全て実施したら該当MILは「達成」評価となる
  右図例だと:
  IAMの目標1のMIL1プラクティスa～c(IAM-1a～c)
  および目標2のMIL1プラクティスa～c(IAM-2a～c)の
  全て達成でMIL1、どれか一つでも未達成だとMIL0の評価となる
  (目標3は「MIL1にプラクティスなし」なので影響しない)

(例)ドメイン「IAM」

ES-C2M2 プラクティス一覧			
ドメイン	目標	MIL	プラクティス
アイデンティティおよびアクセスの管理 Identity and Access Management (IAM)	1.アイデンティティの確立および維持 (1. Establish and Maintain Identities)	MIL1	a. アイデンティティが、資産へアクセスを必要とする担当者およびその他エンティティ(例:サービス、デバイス)にプロビジョニングされている(なお、本要件は共有アイデンティティを除外するものではない)
			b. クレデンシャル(credential)が資産へのアクセス権を必要とする担当者およびエンティティに発行されている(例:パスワード、スマートカード、証明書、キー)
			c. 不要になったアイデンティティは抹消されている
		MIL2	d. アイデンティティのレポジトリが定期的にレビューされ、更新され、正当であることが保証されている(例:アイデンティティがまだアクセス権を必要としていることを保証)
			e. クレデンシャル(credential)が定期的にレビューされることで、資格情報が正しい個人またはエンティティに紐付いていることが保証されている
			f. 不要になったアイデンティティは組織で定義した制限期間内に抹消されている
		MIL3	g. クレデンシャル(credential)の要件は組織のリスク基準を基にしている(例:リスクの高いアクセスに対しては多要素認証のクレデンシャル要)(RM-1c)
	2. アクセス制御 (2. Control Access)	MIL1	a. リモートアクセスも含めてアクセス要件が定められている(アクセス要件は資産と紐付けられ、資産にアクセス権を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について指針(guide)が与えられている)
			b. 要件に基づきアインデンティティにアクセス権が付与されている
			c. 不要になったアクセス権が無効化されている
		MIL2	d. アクセス要件が最小権限と職務分掌の原則に基いている
			e. アクセス制御に対する要求が資産オーナーによりレビューされ承認されている
			f. root権限、管理者アクセス、緊急アクセス、および共有アカウントには、追加の精査とモニタリングが行われている
		MIL3	g. アクセス権限が組織で定義した頻度でレビューされ、正当であることが保証されている
			h. 資産へのアクセス権は、ファンクションに対するリスクに基づき資産オーナーにより付与されている
			i. サイバーセキュリティイベントの兆候を示す指標として異常なアクセスの試みがモニターされている
	3. 管理アクティビティ (3. Management Activities)	MIL1	MIL1にプラクティスなし
		MIL2	a. 文書化したプラクティスに従いアイデンティティが確立、維持され、アクセス制御が行われている
			b. アクセス権およびアイデンティティ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
			c. アクセス権とアイデンティティの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
			d. アクセス権とアイデンティティの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
		MIL3	e. 文書化されたポリシーまたは他の組織的指示により、アクセス権とアイデンティティの管理アクティビティに指針が与えられている
			f. アクセス権とアイデンティティの管理ポリシーには、特定された標準および(/または)ガイドライン準拠のためのコンプライアンス要件が含まれている
			g. アクセス権とアイデンティティの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
			h. アクセス権とアイデンティティの管理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
			i. アクセス権とアイデンティティの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

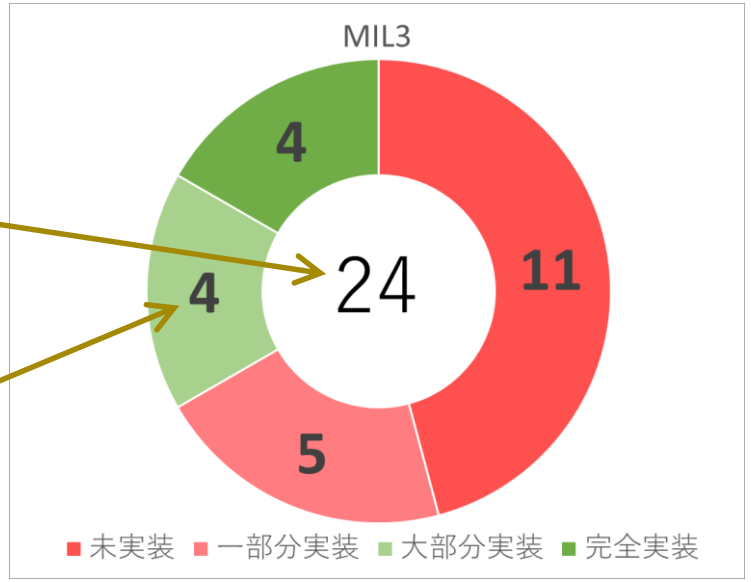
ES-C2M2でマネジメント成熟度を把握

- MIL（Maturity Indicator Level）に関して
  - ✓ （DoE提唱）MIL2,MIL3 の達成等を強制するものではなく、個々の事業者が対策の必要性(脅威）と効果を考え、各社の判断基準※1を定めて改善を行うためのモデル
  - ✓ ※1(例)　クレデンシャルの要件は組織のリスク基準を基にしている(IAM-1g)、現在および将来のオペレーションのニーズをサポートするサイバーセキュリティ要員管理目標が策定され、維持されている（WM-3e）　＜引用はいずれもMIL3プラクティス＞
- ES-C2M2の活用で、サイバーセキュリティのリスクマネジメントにおける観点に漏れがないかの視点でも自己評価が可能
- MIL評価を視覚的に把握可
  - ドーナツチャート（ドメイン各MIL達成状況を表示）

ドーナツチャート中心の数字（24）は当該ドメインにおける MIL1 から MIL3 までのプラクティス評価総数（MIL1＋MIL2＋MIL3）

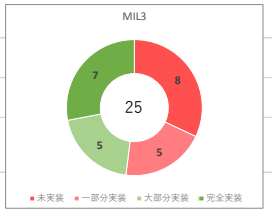
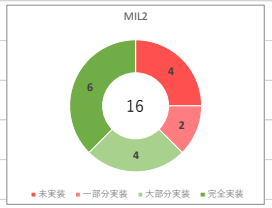
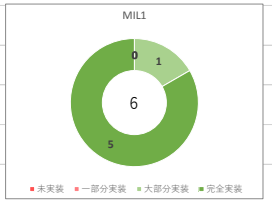
「完全実装」「大部分実装」「一部実装」「未実装」各評価数の小計を個別記載　ただし、この表示も MIL1から MIL3 までの累計数字

薄い緑（大部分実装：4つのプラクティスが大部分実装されている）



ES-C2M2　チェックシートの概要

（ ○ 例:ドメイン「IAM」）

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			
アイデンティティおよびアクセスの管理 Identity and Access Management (IAM)	1.アイデンティティの確立および維持 (1. Establish and Maintain Identities)	MIL1	a. Identities are provisioned for personnel and other entities (e.g., services, devices) who require access to assets (note that this does not preclude shared identities)	a. アイデンティティが、資産へアクセスを必要とする担当者およびその他エンティティ （例：サービス、デバイス） にプロビジョニングされている （なお、本要件は共有アイデンティティを除外するものではない）	完全実装		
			b. Credentials are issued for personnel and other entities that require access to assets (e.g., passwords, smart cards, certificates, keys)	b. クレデンシャル(credential)が資産へのアクセス権を必要とする担当者およびエンティティに発行されている （例：パスワード、スマートカード、証明書、キー）	完全実装		
			c. Identities are deprovisioned when no longer required	c. 不要になったアイデンティティは抹消されている	完全実装		
		MIL2	d. Identity repositories are periodically reviewed and updated to ensure validity (i.e., to ensure that the identities still need access)	d. アイデンティティのレポジトリが定期的にレビューされ、更新され、正当であることが保証されている （例：アイデンティティがまだアクセス権を必要としていることを保証）	未実装		
			e. Credentials are periodically reviewed to ensure that they are associated with the correct person or entity	e. クレデンシャル(credential)が定期的にレビューされることで、資格情報が正しい個人またはエンティティに紐付いていることが保証されている	未実装		
			f. Identities are deprovisioned within organizationally defined time thresholds when no longer required	f. 不要になったアイデンティティは組織で定義した制限期間内に抹消されている	完全実装		
		MIL3	g. Requirements for credentials are informed by the organization's risk criteria (e.g., multifactor credentials for higher risk access) (RM-1c)	g. クレデンシャル(credential)の要件は組織のリスク基準を基にしている （例：リスクの高いアクセスに対しては多要素認証のクレデンシャル要） （RM-1c）	未実装		
	2. アクセス制御 (2. Control Access)	MIL1	a. Access requirements, including those for remote access, are determined (access requirements are associated with assets and provide guidance for which types of entities are allowed to access the asset, the limits of allowed access, and authentication parameters)	a. リモートアクセスも含めてアクセス要件が定められている （アクセス要件は資産と紐付けられ、資産にアクセス権を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について指針(guide)が与えられている）	完全実装		
			b. Access is granted to identities based on requirements	b. 要件に基づきアインデンティティにアクセス権が付与されている	完全実装		
			c. Access is revoked when no longer required	c. 不要になったアクセス権が無効化されている	大部分実装		
		MIL2	d. Access requirements incorporate least privilege and separation of duties principles	d. アクセス要件が最小権限と職務分掌の原則に基いている	大部分実装		
			e. Access requests are reviewed and approved by the asset owner	e. アクセス制御に対する要求が資産オーナーによりレビューされ承認されている	未実装		
			f. Root privileges, administrative access, emergency access, and shared accounts receive additional scrutiny and monitoring	f. root権限、管理者アクセス、緊急アクセス、および共有アカウントには、追加の精査とモニタリングが行われている	一部分実装		
		MIL3	g. Access privileges are reviewed and updated to ensure validity, at an organizationally defined frequency	g. アクセス権限が組織で定義した頻度でレビューされ、正当であることが保証されている	大部分実装		
			h. Access to assets is granted by the asset owner based on risk to the function	h. 資産へのアクセス権は、ファンクションに対するリスクに基づき資産オーナーにより付与されている	未実装		
			i. Anomalous access attempts are monitored as indicators of cybersecurity events	i. サイバーセキュリティイベントの兆候を示す指標として異常なアクセスの試みがモニターされている	未実装		
	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 to establish and maintain identities and control access	a. 文書化したプラクティスに従いアイデンティティが確立、維持され、アクセス制御が行われている	一部分実装		
			b. Stakeholders for access and identity management activities are identified and involved	b. アクセス権およびアイデンティティ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	大部分実装		
			c. Adequate resources (people, funding, and tools) are provided to support access and identity management activities	c. アクセス権とアイデンティティの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	大部分実装		
			d. Standards and/or guidelines have been identified to inform access and identity management activities	d. アクセス権とアイデンティティの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. Access and identity 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、アクセス権とアイデンティティの管理アクティビティに指針が与えられている	完全実装		
			f. Access and identity management policies include compliance requirements for specified standards and/or guidelines	f. アクセス権とアイデンティティの管理ポリシーには、特定された標準および（/または）ガイドライン準拠のためのコンプライアンス要件が含まれている	一部分実装		
			g. Access and identity management activities are periodically reviewed to ensure conformance with policy	g. アクセス権とアイデンティティの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 access and identity management activities are assigned to personnel	h. アクセス権とアイデンティティの管理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	一部分実装		
			i. Personnel performing access and identity management activities have the skills and knowledge needed to perform their assigned responsibilities	i. アクセス権とアイデンティティの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		

評価結果を選択：
（プルダウンメニュー）
「未実装」
「一部分実装」
「大部分実装」
「完全実装」

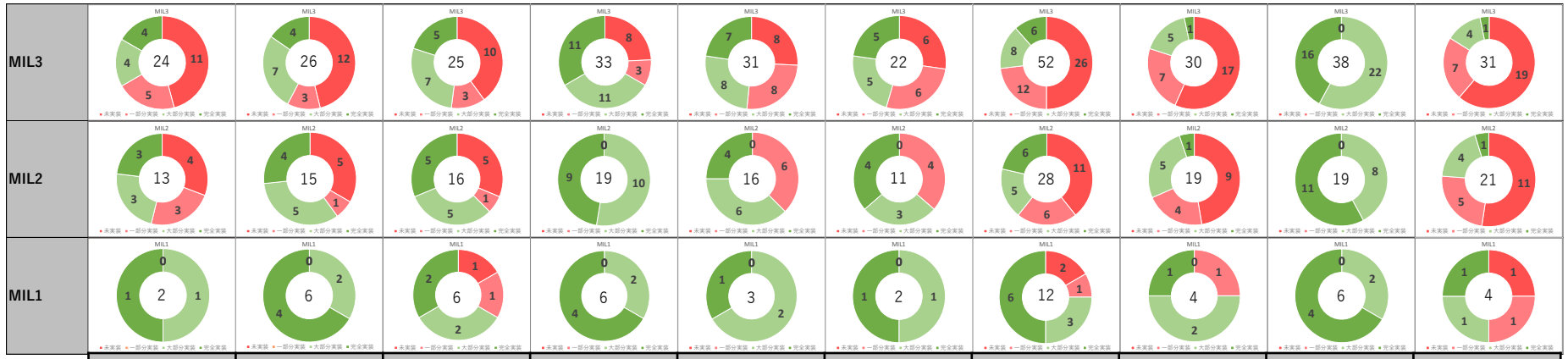
選択するとプラクティスが色付けされる
- 「未実装」
- 「一部分実装」
- 「大部分実装」
- 「完全実装」

ドーナツチャート：
そのドメインの各MIL（MIL1～MIL3）達成状況を示す

- チャートはMIL1～MIL3累計表示
（MIL3はMIL1,MIL2, MIL3の合計結果を表す）
- チャート中心の数字
（25）はIAMドメインのMIL1～MIL3 プラクティスの総数

ES-C2M2　チェックシートのグラフィカルサマリー

10ドメインの評価結果一覧で、ドメインごとの評価バランスが一目でわかる（オリジナル同様）



	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

（凡例）

緑：完全実装

薄緑：大部分実装

ピンク：一部分実装

濃赤：未実装

濃赤（未実装）とピンク（一部分実装）がある場合、そのドメインの当該MILについては達成していないとみなす
上記の例では、各ドメインは以下の評価になる

□MIL 3 のドメイン：　WM　　□MIL 2 のドメイン：　TVM　　□MIL 1 のドメイン：　RM, ACM, SA, ISC　　□MIL 0 のドメイン：　IAM、IR、EDM、CPM

ES-C2M2は自己評価ツール（汎用的に活用可能）

－　PDCA改善活動のファーストステップに　－

- リスクマネジメントのPDCAサイクル点検改善フェーズ活動支援
  - 自組織のリスクマネジメントの成熟度を分析・把握
- 成熟度評価から補強が必要な分野を特定し改善につなげる
  - 客観的に未成熟レベルのドメイン(分野)を把握
  - ドメインごとの改善活動を導入し、再評価をして効果測定ができる
- C2M2なら補強すべき具体的な方向性も把握できる
  - 未成熟レベル判定のプラクティス ⇒ 満たせば成熟度レベルアップ
- ES-C2M2とほぼ同じ内容で、ONG-C2M2（Oil&Gas）、B-C2M2（Building）があるが、ES-C2M2を他業種重要インフラ事業者や制御システム所有者が参照しても有用
  - 汎用的なツールとして活用が可能

C2M2 / ONG-C2M2 / ES-C2M2 との差異比較

○ プラクティスにおける差異は「情報源」「報告先」等の記載のみ（ONG-C2M2はC2M2と全く同じ）

ドメイン	目標	MIL	C2M2	ONG-C2M2	ES-C2M2	ES-C2M2プラクティス訳
TVM	1. 脅威の特定と対応（1. Identify and Respond to Threats）	MIL1	a. Information sources to support threat management activities are identified (e.g., US-CERT, various critical infrastructure sector ISACs, ICS-CERT, industry associations, vendors, federal briefings)	a. Information sources to support threat management activities are identified (e.g., US-CERT, various critical infrastructure sector ISACs, ICS-CERT, industry associations, vendors, federal briefings)	a. Information sources to support threat management activities are identified (e.g., ES-ISAC, ICS-CERT, US-CERT, industry associates, vendors, federal briefings)	a. 脅威管理のアクティビティをサポートするための情報源が洗い出されている（例：E-ISAC、ICS- CERT、US-CERT、業界団体、ベンダー、連邦による情報提供の場）
	2. サイバーセキュリティ脆弱性の低減策（2. Reduce Cybersecurity Vulnerabilities）	MIL1	a. Information sources to support cybersecurity vulnerability discovery are identified (e.g., US-CERT, various critical infrastructure sector ISACs, ICS-CERT, industry associations, vendors, federal briefings, internal assessments)	a. Information sources to support cybersecurity vulnerability discovery are identified (e.g., US-CERT, various critical infrastructure sector ISACs, ICS-CERT, industry associations, vendors, federal briefings, internal assessments)	a. Information sources to support cybersecurity vulnerability discovery are identified (e.g., ES-ISAC, ICS-CERT, US-CERT, industry associations, vendors, federal briefings, internal assessments)	a. サイバーセキュリティの脆弱性の発見をサポートするための情報源が洗い出されている（例：E-ISAC、ICS- CERT、US-CERT、業界団体、ベンダー、連邦による情報提供の場、内部評価）
ISC	1. サイバーセキュリティ情報の共有（1. Share Cybersecurity Information）	MIL1	b. Responsibility for cybersecurity reporting obligations are assigned to personnel (e.g., internal reporting, ICS-CERT, law enforcement)	b. Responsibility for cybersecurity reporting obligations are assigned to personnel (e.g., internal reporting, ICS-CERT, law enforcement)	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）
IR	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（3. Respond to Incidents and Escalated Cybersecurity Events）	MIL1	c. Reporting of escalated cybersecurity events and incidents is performed (e.g., internal reporting, ICS-CERT, relevant ISACs)	c. Reporting of escalated cybersecurity events and incidents is performed (e.g., internal reporting, ICS-CERT, relevant ISACs)	c. Reporting of escalated cybersecurity events and incidents is performed (e.g., internal reporting, DOE Form OE-417, ES-ISAC, ICS-CERT)	c. 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とインシデントの報告が実施されている（内部報告、DOE Form OE-417、E-ISAC、ICS-CERTなど）

※「ES-ISAC」は「E-ISAC」に名称変更した

各資料公開情報

- ES-C2M2　（NERC CIP、NIST IR 7628の簡単な説明資料もある）
  https://www.ipa.go.jp/security/controlsystem/usenergy.html

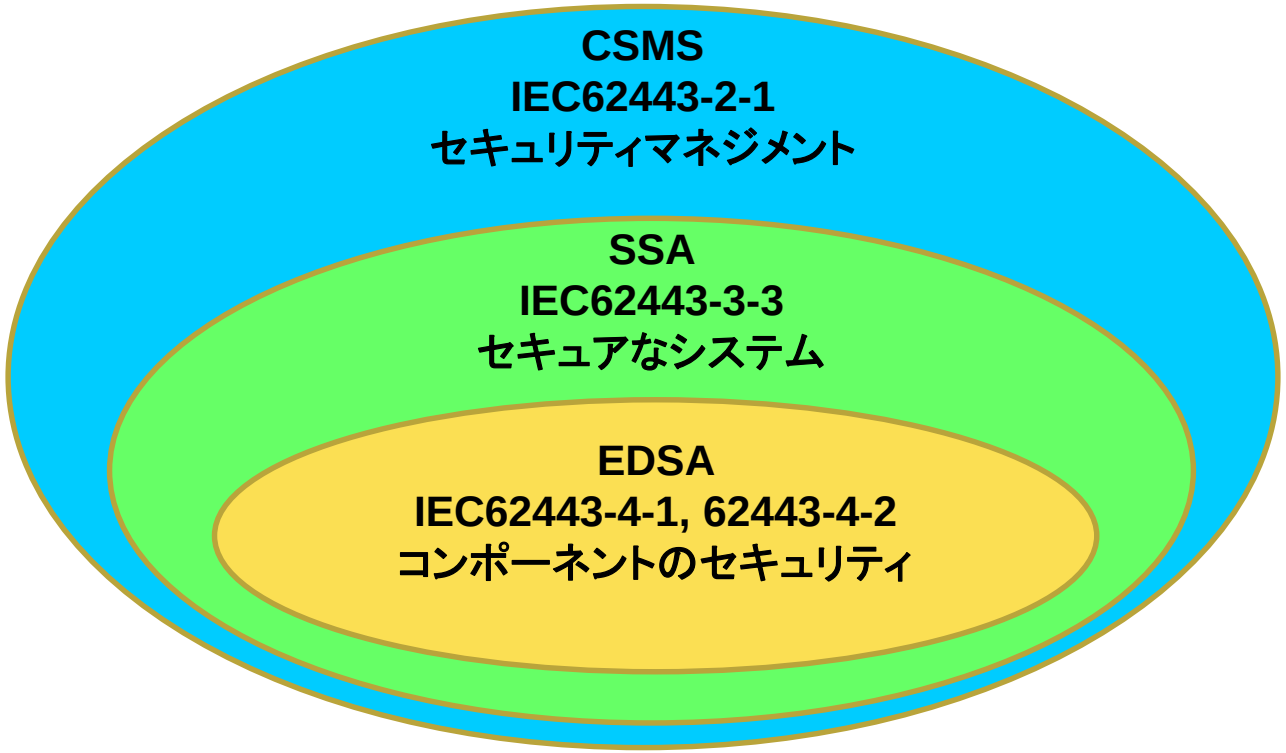
- NIST CyberSecurity Framework（NIST CSF）
  および
  NIST SP800-53
  https://www.ipa.go.jp/security/publications/nist/index.html

- NIST SP800-82
  https://www.jpcert.or.jp/ics/information02.html

（2020年1月時点）

（参考）リスクマネジメントの方法論

IEC62443制御セキュリティの考え方



- CSMS
  Cyber Security Management System
  国際標準IEC 62443-2-1で規定される
  産業用制御システムのセキュリティマネジメントに対する
  組織認証

  SSA
  System Security Assurance
  国際標準IEC 62443-3-3で規定される
  産業用制御システムに対するセキュリティ要件に沿った
  システム認証

  EDSA
  Embedded Device Security Assurance
  国際標準IEC 62443-4-1および4-2で規定される産業用
  制御システムのセキュリティに対するコンポーネント認証

- ベンダーの思想や体制などによってもセキュアなシステムを構築する手段や方法論に差が生じたり、対策機能の導入や、設定が難しかったりする制御システムは、セキュリティマネジメントを前提としたデプロイメントとオペレーションを必要とする

IEC62443参照アーキテクチャと分割アーキテクチャ
（〇DMZ構築と侵入されにくい構成の参考）

防御対策が難しい制御システムのセキュリティは
①「**リスクマネジメント**」　（分析したリスクへの対応をどのように行うか）
②「**インシデント対応体制整備**」（誰の権限／責任でリスク対応を行うか）
③「**セキュアなシステム構築**」　（できるだけ侵入に時間を要し、脅威を検知し易く、運用がし易い）
が重要

①の1st step に：
- **「制御システムのセキュリティリスク分析ガイド」を活用**

②の参考に：
- **IEC62443-2-1 (CSMS)**
  （①のマネジメント方法も含めて）

③の参考に：
- **標題のアーキテクチャ（以前は“Zone”“Conduit”と呼ばれた）**
- **詳細はIEC62443-2-1 Figure A.8 などにも記載がある**
  （将来的にはIEC62443-3-2が発行される予定）

※IEC62443の内容は著作権の関係で引用不可のため、各自で購入が必要

～最後に～

- 本件に関するお問い合わせ・・・

セキュリティセンター セキュリティ対策推進部
脆弱性対策グループ
isec-ics@ipa.go.jp