IPA Better Life with IT

米国電力関係の基準の概要
（NERC CIP, ES-C2M2, NIST IR7628）

2019年8月30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

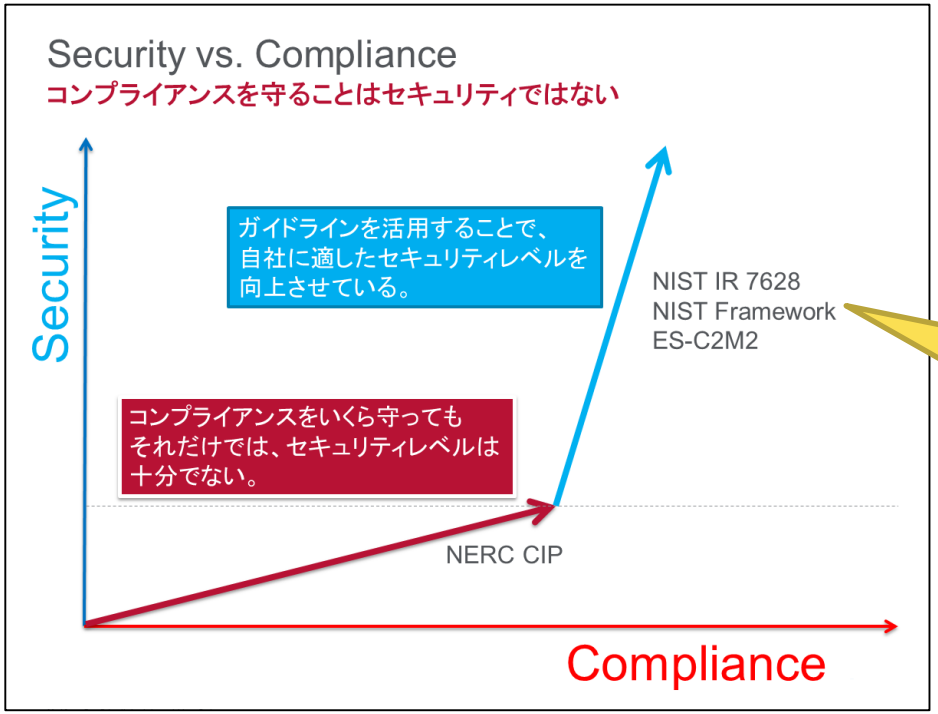
AGENDA

- 米国の電力関係基準の体系
- NERC CIP について
- ES-C2M2について
- NIST IR 7628 について

- 米国の電力関係基準の体系
- NERC CIP について
- ES-C2M2について
- NIST IR 7628 について

米国電力業界の基準概要

- コンプライアンス≠セキュリティ
- コンプライアンスの基準としてNERC CIP Standard※
- 一層のセキュリティ対策を促すためにES-C2M2、NIST IR 7628 を活用
  - 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）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」



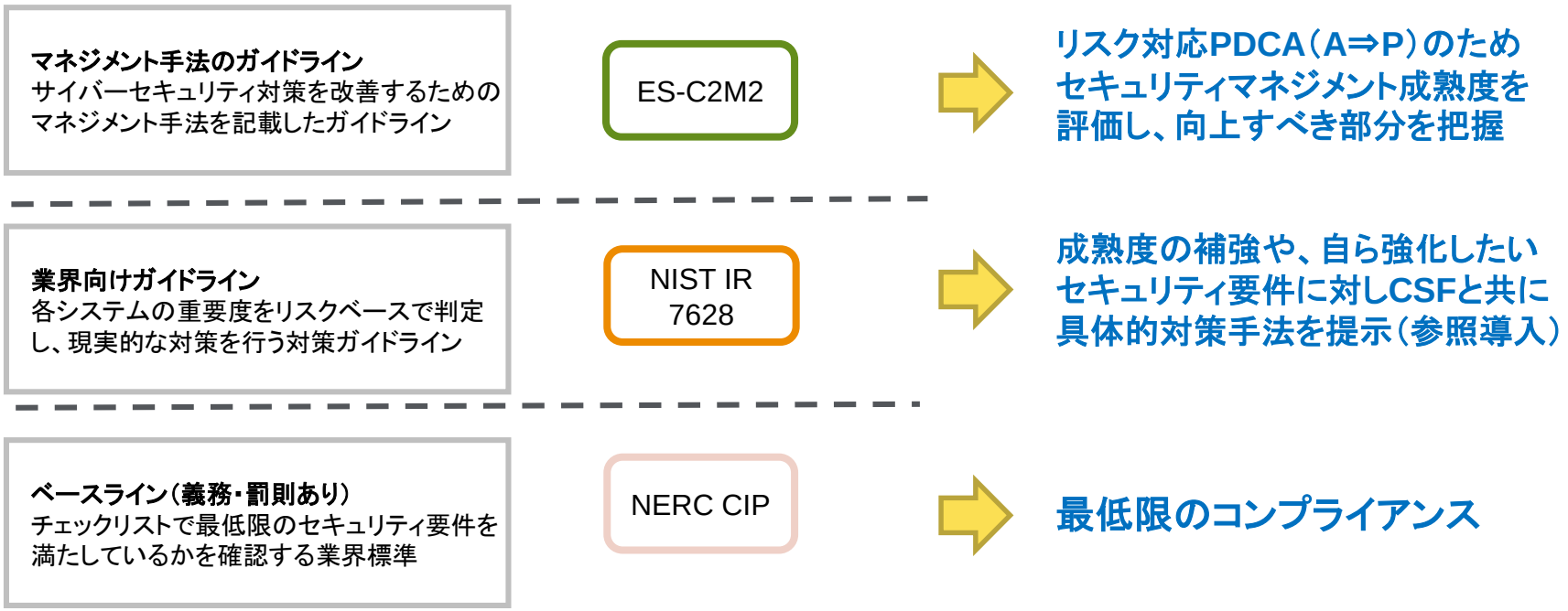
※NERC CIP Standardは、2003年の大停電を踏まえて、電力の安定供給を念頭において作成された主に大規模発電施設及び送電施設を対象としたサイバーセキュリティに関する標準
（標準であり規制でもある：違反に罰金が科される）

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**

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 （引用図）

ES-C2M2、NIST IR 7628 の位置付け

- 米国には約3000の電力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）
- 適用対象：（事業者の）部門・設備単位（例：XX発電所）
- 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



調査対象の概要

●以下3つの基準またはガイドラインを対象とし、調査を実施した。

#	規格/基準	物量	作成者	基準の概要
1	CIP※1 （Version5）	約500頁	NERC※2	米国電力事業(発電、送電、配電)が業法に基き準拠すべき基準。 12エリア42項目 233細則の規準から構成。
2	ES-C2M2※3 （Ver1.1：2014）	約100頁	DoE	米国電力企業のセキュリティマネー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 ）	約500頁	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。

※1　CIP:　Critical Infrastructure Protection Standard
（重要インフラ保護サイバーセキュリティ基準）
※2　NERC：North American Electric Reliability Corporation
（北米電力信頼性評議会）
※3　ES-C2M2：Electricity Subsector Cybersecurity Capability Maturity Model Program
（電力分野用セキュリティマネージメント成熟度モデル）

（参考）NIST CSF について

（今回の調査対象外資料）

- 米大統領令によりNISTで策定されたCyberSecurity Framework
  - EO13636:「Improving Critical Infrastructure Cybersecurity（重要インフラのサイバーセキュリティの向上）」
  - 大統領令で規定「米国の重要インフラのセキュリティとレジリエンスを高め、安全、セキュリティ、企業機密、プライバシー、および市民の自由を守ると同時に効率性、イノベーション、および経済繁栄を促進するサイバー環境を維持するための米国のポリシー」
- 政府と民間部門との連携により策定
  - 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
  - リスクベース・アプローチに基くフレームワークで、企業に新たな規制を課すことなく、ビジネスニーズに基いてコスト効率よくサイバーセキュリティリスクに対処し、リスクを管理可能
- IPAにて翻訳公開
  - https://www.ipa.go.jp/security/publications/nist/index.html

- 米国の電力関係基準の体系
- NERC CIP について
- ES-C2M2について
- NIST IR 7628 について

NERC CIP とは

- North American Electric Reliability Council（NERC：北米電力信頼度協議会）が発行した Cyber-security Critical Infrastructure Protection（CIP：「**重要インフラ防護基準**」）

  かつ

- NERCがElectric Reliability Organization（ERO：電力信頼性機関）として策定し、Federal Energy Regulatory Commission（FERC：アメリカ合衆国連邦エネルギー規制委員会）が承認した米国電力業界向け**規制標準**

NERC CIP の概要

- NERC CIPは13個の文書より構成されており、**それぞれの領域のサイバーセキュリティ**を規定
- 事業者が順守すべき**要件**（Requirement：要求事項）、要件遵守の証拠例となる**方策**（Measurement：測定基準）を記載
- コンプライアンスの監査プロセスと、コンプライアンスに違反した場合の**違反重大度レベル**（Violation Severity Level）を記載

	現行項目	項目概要	説明
CIP-002	BES Cyber System Categorization	BESサイバーシステム分類	CIPの対象となる大規模電力システム（Bulk Electric System）内の重要サイバー資産を識別することを規定
CIP-003	Security Management Controls	セキュリティ管理コントロール	セキュリティマネジメントを確立し、重要サイバー資産を保護するための計画を立案することを規定
CIP-004	Personnel & Training	人材＆トレーニング	重要サイバー資産に係る従業員の資格、トレーニングを規定
CIP-005	Electronic Security Perimeter(s)	電子的セキュリティ境界	重要サイバー資産に対する電子的セキュリティ境界の決定し保護することを規定
CIP-006	Physical Security of BES Cyber Systems	BESサイバーシステムの物理的セキュリティ	重要サイバー資産に対する物理的なアクセス制御を規定
CIP-007	System Security Management	システムのセキュリティ管理	重要サイバー資産に対するシステム的なセキュリティ対策を規定
CIP-008	Incident Reporting and Response Planning	インシデント報告と対応計画	サイバーセキュリティインシデント発生時の対応計画と報告を規定
CIP-009	Recovery Plans for BES Cyber Systems	BESサイバーシステムの復旧計画	重要サイバー資産の復旧計画を規定
CIP-010	Configuration Change Management and Vulnerability Assessments	構成変更管理と脆弱性評価	重要サイバー資産の構成管理と脆弱性対策を規定
CIP-011	Information Protection	情報保護	重要サイバー資産の情報保護を規定
CIP-012	Communications between Control Centers	コントロールセンター間の通信	送電設備と変電所を管理するコントロールセンター間の通信の保護を規定
CIP-013	Supply Chain Risk Management	サプライチェーンリスク管理	重要サイバー資産のベンダー等を対象としたサプライチェーンリスクへの対処を規定
CIP-014	Physical Security	物理的セキュリティ	大規模電力システム内の発電、送電、配電設備に対するリスク評価とその対処を規定

要求事項は計42項目（細則233項目）

要件例(CIP-005-6 R2)

ー 電子的セキュリティ境界(リモートアクセス管理) ー

CIP-005-6 R2 –リモートアクセス管理			
Part	**適用システム**	**要求事項**	**測定尺度**
R2	ー	BESサイバーシステムへの双方向リモートアクセスを許可する各責任エンティティは、技術的に可能であれば、CIP-005-6表R2ーリモートアクセス管理の該当要件パートをそれぞれ総合的に含む1件以上の文書化されたプロセスを実施するものとする。	証拠には、CIP-006 表R2–リモートアクセス管理の該当する要件パートをそれぞれ総合的に含むそれぞれの文書化したプロセスと、表の方策の欄に記載の通り、実施を実証する追加的証拠を含む必要がある。
2.1	影響度高のBESサイバーシステムとそれに関連する: • PCA 外部ルーティング接続のある影響度中のBESサイバーシステムとそれに関連する: • PCA	あらゆる双方向のリモートアクセスについて、双方向のリモートアクセスを開始するサイバー資産が、該当するサイバー資産に直接アクセスしないように、中間システムを利用する。	証拠例として、ネットワーク図またはアーキテクチャー文書を含むが、これに限定されない。
2.2	影響度高のBESサイバーシステムとそれに関連する: • PCA 外部ルーティング接続のある影響度中のBESサイバーシステムとそれに関連する: • PCA	あらゆる双方向のリモートアクセスのセッションについて、中間システムを端点とする暗号化を利用する。	証拠例として、暗号化の起点と終点を詳述するアーキテクチャー文書を含むが、これに限定されない。
2.3	影響度高のBESサイバーシステムとそれに関連する: • PCA 外部ルーティング接続のある影響度中のBESサイバーシステムとそれに関連する: • PCA	あらゆる双方向のリモートアクセスのセッションについて多要素認証が必要である。	証拠例として、使用される認証要素を詳述するアーキテクチャー文書を含むが、これに限定されない。 認証要素の例として以下を含むが、これに限定されない。 • パスワードまたはPINなど、個人が知っているもの。これにはユーザーIDは含まれない; • トークン、デジタル証明書、またはスマートカードなど、個人が持っているもの。 • 指紋、虹彩スキャン、またはその他生体情報など、個人自身の特徴。
2.4	影響度高のBESサイバーシステムとそれに関連する: • PCA 外部ルーティング接続のある影響度中のBESサイバーシステムとそれに関連する: • PCA	アクティブなベンダーリモートアクセスセッション(双方向リモートアクセスとシステム間リモートアクセスを含む)を決定する1つ以上の方法を持つ。	証拠例として、アクティブなベンダーリモートアクセスセッション(双方向リモートアクセスとシステム間リモートアクセスを含む)を決定する以下の方法の文書を含めることができるが、これに限定されない。 • アクティブなベンダーリモートアクセスセッションを決定するために、アクセスを記録するか情報を監視する方法 • アクティブなシステム間リモートアクセスセッションを決定するために、アクティビティ(たとえば、コネクションテーブルやファイアウォールのルールヒットカウンター)や開放されているポート(たとえば、現在アクティブなポートを表示するnetstatや関連コマンド)を監視する方法、あるいは • リモートアクセスを開始するためにベンダーが2つ目の要素(認証手段)を開始/要求するなどの、ベンダーが開始したリモートアクセスをコントロールする方法
2.5	影響度高のBESサイバーシステムとそれに関連する: • PCA 外部ルーティング接続のある影響度中のBESサイバーシステムとそれに関連する: • PCA	アクティブなベンダーリモートアクセスセッション(双方向リモートアクセスとシステム間リモートアクセスを含む)を無効にする1つ以上の方法を持つ。	証拠例として、アクティブなベンダーリモートアクセスセッション(双方向リモートアクセスとシステム間リモートアクセスを含む)を無効にする以下の方法の文書を含めることができるが、これに限定されない。 • システム間リモートアクセスのための該当する電子的アクセスポイントで、ベンダーリモートアクセスを無効にする方法 • 該当する中間システムで、ベンダーの双方向リモートアクセスを無効にする方法

PCA:Protected Cyber assets(保護されたサイバー資産)

違反した場合の重大度判定レベル

- 要件ごとに定義された違反レベルを測る尺度
- 低、中、高、重度と4つの違反レベルが定義されている

CIP-005-6 テーブル R2 – BESサイバーシステムの物理的セキュリティ		
Part	要求事項	測定尺度
R2	BESサイバーシステムへの双方向リモートアクセスを許可する各責任エンティティは、技術的に可能であれば、CIP-005-6表R2−リモートアクセス管理の該当要件パートをそれぞれ総合的に含む1件以上の文書化されたプロセスを実施するものとする。	証拠には、CIP-006 表R2−リモートアクセス管理の該当する要件パートをそれぞれ総合的に含むそれぞれの文書化したプロセスと、表の方策の欄に記載の通り、実施を実証する追加的証拠を含む必要がある。

#	計画対象期間	違反リスク要因	違反の重大度レベル (CIP-005-6)			
			低度	中度	高度	重度
R2	オペレーション計画と同日業務	中	責任エンティティは、要件パート2.1 から2.3における1件以上の該当項目のプロセスを文書化しなかった。	責任エンティティは、要件パート2.1から2.3の該当項目のうち1件のプロセスを実施しなかった。	責任エンティティは、要件パート2.1から2.3の該当項目のうち2件のプロセスを実施しなかった。 あるいは 責任エンティティは、アクティブなベンダーリモートアクセスセッション（双方向リモートアクセスとシステム間リモートアクセスを含む）を決定する1つ以上の方法（2.4）と、アクティブなベンダーリモートアクセスセッション（双方向リモートアクセスとシステム間リモートアクセスを含む）を無効にする1つ以上の方法（2.5）のいずれかを用意していなかった。	責任エンティティは、要件パート2.1から2.3の該当項目のうち3件のプロセスを実施しなかった。 あるいは 責任エンティティは、アクティブなベンダーリモートアクセスセッション（双方向リモートアクセスとシステム間リモートアクセスを含む）を決定する1つ以上の方法（2.4）と、アクティブなベンダーリモートアクセスセッション（双方向リモートアクセスとシステム間リモートアクセスを含む）を無効にする1つ以上の方法（2.5）のどちらも用意していなかった。

違反した場合の罰金額

- 重大度レベルに対して科される罰金額
  - 1日あたり
  - 違反ごと、または違反頻度または違反期間で決定される

	VSL（違反重大度レベル）							
違反リスク要因	低		中		高		重度	
	範囲制限		範囲制限		範囲制限		範囲制限	
	低	高	低	高	低	高	低	高
低	$1,000	$3,000	$2,000	$7,500	$3,000	$15,000	$5,000	$25,000
中	$2,000	$30,000	$4,000	$100,000	$6,000	$200,000	$10,000	$335,000
高	$4,000	$125,000	$8,000	$300,000	$12,000	$625,000	$20,000	$1,000,000

- 違反リスク要因（低・中・高）は、要件で定義されている
- VSLの範囲制限（低・高）は監査者の裁量で判定される罰金額の下限と上限

- 米国の電力関係基準の体系
- NERC CIP について
- ES-C2M2について
- NIST IR 7628 について

ES-C2M2とは

✓ ES-C2M2：
米国DoE※が開発したCybersecurity Capability Maturity Model Program（サイバーセキュリティ能力成熟度モデル）の電力分野用モデル
※Ver1.0：2012/3、 Ver1.1：2014/2
（ Electricity Subsector - Cybersecurity Capability Maturity Model Program ）

- ✓ 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自己評価ツール
（10ドメイン×37目標×312プラクティスに対して4段階で評価）

✓ IPAで10ドメイン×37目標×312プラクティスを日本語化
- ✓ チェックシート（ドメインごとのレベルを自己評価するExcel表）
- ✓ 解説書（ドメイン毎の概要、用語定義、チェックシート使用方法等の解説ドキュメント）

※Department of Energy（エネルギー省）

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

次Page

10ドメイン

37目標

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
  (IAMの場合、目標3には「MIL1にプラクティスなし」)

(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の活用について

- 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)
- 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自己評価が可能
  - CSF(Cyber Security Framework）、METI：CPS対策フレームワークの重要インフラシステム向けマネジメント自己評価指標としても、MILの考え方は参考になる
  - 本プラクティスを理解し評価できる体制が組織内にできているかどうかが最大のポイント（OT・IT連携セキュリティ統括組織の設置等）
- ES-C2M2とほぼ同じ内容で、ONG-C2M2（Oil&Gas）、B-C2M2（Building）があり、他業種の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となる

C2M2・ONG-C2M2・ES-C2M2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

ES-C2M2
IPAで翻訳・資料作成

- ES-C2M2に関し以下を作成した

	バージョン	作成者	概要
	ES-C2M2 （Ver1.1：2014）	DoE	米国電力会社のセキュリティマネジメント成熟度を測定するモデル。

#	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

公開URL：
https://www.ipa.go.jp/**********

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		MIL3
			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		MIL2
			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		MIL1
			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」

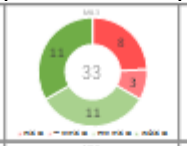
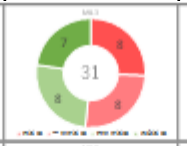
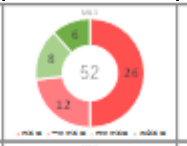
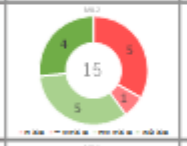
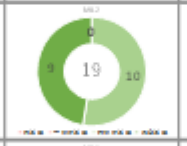
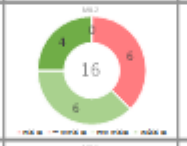
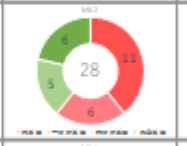
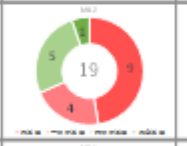
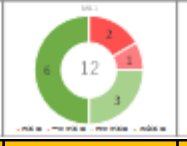
選択するとプラクティスが色付けされる
「未実装」
「一部分実装」
「大部分実装」
「完全実装」

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

IPA

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

	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
MIL3										
MIL2										
MIL1										
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）がある場合は、そのドメインの当該MILは達成していないと見なす
上記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

- 米国の電力関係基準の体系
- NERC CIP について
- ES-C2M2について
- NIST IR 7628 について

NIST IR 7628 とは

- NIST IR 7628 Guidelines for Smart Grid Cybersecurity
  NIST（アメリカ国立標準技術研究所）によって発行された
  スマートグリッドを対象にしたセキュリティガイドライン
  - スマートグリッドの普及を目指して、官民交流を目的としたスマートグリッド相互運用性パネル（Smart Grid Interoperability Panel：SGIP※）にて、NIST協力の下、米国スマートグリッドのセキュリティ標準として作成

- スマートグリッド情報システムを保有する事業者へのサイバーセキュリティガイドラインの提供を目的

- リスクベースのサイバーセキュリティ対策手法を提示
  - このガイドラインで、各事業者は現実に即したサイバーセキュリティ対策を検討することが可能

※現SEPA（Smart Electric Power Alliance）

NIST IR 7628 の構成について

「スマートグリッドサイバーセキュリティのためのガイドライン」 文書体系	
Volume 1	グリッドのセキュリティ戦略、アーキテクチャ、およびハイレベル要件
第1章	文書開発戦略（信頼性・機密性の確保とサイバーセキュリティ戦略）
第2章	グリッドの論理アーキテクチャとインタフェース（22の論理インターフェイスカテゴリ：LIC）
第3章	高レベルセキュリティ要件（LICごとのスマートグリッドの高度なセキュリティ要件）
第4章	暗号化と鍵管理
	- 付録A - サイバーセキュリティ文書のクロスウォーク - 付録B - 高度なセキュリティ要件を満たすセキュリティテクノロジとサービスの例
Volume 2	プライバシーとスマートグリッド
第5章	プライバシーとスマートグリッド
	- 付録C - 規制枠組みの変更 - 付録D - 顧客/消費者スマートグリッドのエネルギー使用量に関する推奨されるプライバシープラクティス 第三者が直接取得したデータ - 付録E - プライバシーの利用事例 - 付録F - スマートグリッドのハイレベル消費者対ユーティリティプライバシー影響評価の概要 - 付録G - プライバシー関連の定義
Volume 3	補足的な分析と参考文献
第6章	脆弱性クラス
第7章	ボトムアップ（グリッドのセキュリティ解析）
第8章	グリッドにおけるサイバーセキュリティ研究開発テーマ
第9章	標準レビューの概要
第10章	重要な電力システムのセキュリティ要件
	- 付録H - 論理インタフェースカテゴリの解析マトリクス - 付録I - 高度なセキュリティ要件へのマッピング - 付録J - 用語集および頭字語 - 付録K - SGIP-CSWGおよびSGIP 2.0 SGCC会員

NIST IR 7628 のセキュリティ要件

■セキュリティ要件

✓ 19 ファミリ
✓ 197 要件（19ファミリの要件総合計）

■セキュリティ要件の各種考察

以下のように様々な側面からの考察がなされている

① 文書の横断比較
- NIST SP800-53
- DHSカタログ
- NERC CIP

② 論理インターフェースカテゴリ（LIC）と影響レベル

③ 脆弱性クラスと対抗策
（要件を満たすことが対抗策となる）

④ LICごとに推奨されるセキュリティ要件

セキュリティ要件ファミリ		要件数
SG.AC	アクセス制御 Access Control	21
SG.AT	啓発と人材育成 Awareness and Training	7
SG.AU	監査と説明責任 Audit and Accountability	16
SG.CA	セキュリティ評価と認可 Security Assessment and Authorization	6
SG.CM	構成設定管理 Configuration Management	11
SG.CP	運用の継続 Continuity of Operations	11
SG.IA	識別と認証 Identification and Authentication	6
SG.ID	情報及び文書管理 Information and Document Management	5
SG.IR	インシデント・レスポンス Incident Response	11
SG.MA	スマート・グリッド情報システムの開発と保守 Smart Grid Information System Development and Maintenance	7
SG.MP	メディア防護 Media Protection	6
SG.PE	物理および環境セキュリティ Physical and Environmental Security	12
SG.PL	セキュリティ計画 Planning	5
SG.PM	セキュリティプログラム管理 Security Program Management	8
SG.PS	人的セキュリティ Personnel Security	9
SG.RA	リスク管理と評価 Risk Management and Assessment	6
SG.SA	スマート・グリッド情報システムとサービスの取得 Smart Grid Information System and Services Acquisition	11
SG.SC	スマート・グリッド情報システムと通信の保護 Smart Grid Information System and Communication Protection	30
SG.SI	スマート・グリッド情報システムと情報の保全 Smart Grid Information System and Information Integrity	9
	合計要件数	197

NIST IR 7628 の文書の横断比較

①NIST SP800-53、DHSカタログ、NERC CIP との比較対応表（SG.AC抜粋）

該当項目なし：－　　Category ： White = Common Governance, Risk and Compliance (GRC)　Light Gray = Common Technical Requirement(CTR)　Dark Gray = Unique Technical Requirement(UTR)

Smart Grid Cyber Security Requirement Category	NISTIR 7628 Number	Smart Grid Cyber Security Requirement Name	Category	NIST SP 800-53 Revision 4		DHS Catalog of Control Systems Security: Recommendations for Standards Developers		NERC CIPS (1-9) Version 3 October 2010
アクセス制御（SG.AC） Access Control (SG.AC)	SG.AC-1	アクセス制御の方針と手順 Access Control Policy and Procedures	GRC	AC-1	Access Control Policy and Procedures	2.15.1	Access Control Policies and Procedures	CIP 003-3 (R1, R5, R5.2, R5.3) CIP 005-3a (R1, R1.1, R1.6) CIP 006-3c (R2)
	SG.AC-2	リモートアクセスの方針と手順 Remote Access Policy and Procedures	GRC	AC-17	Remote Access	2.15.23	Remote Access Policy and Procedures	CIP 005-3a (R1, R1.1, R1.2, R1.6, R2, R2.3, R2.4) CIP 007-3a (R5)
	SG.AC-3	アカウント管理 Account Management	GRC	AC-2	Account Management	2.15.3	Account Management	CIP 003-3 (R5, R5.1, R5.2, R5.3) CIP 004-3a (R4, R4.1, R4.2) CIP 005-3a (R2.5.1, R2.5.3) CIP 007-3a (R5, R5.1, R5.1.3, R5.2, R5.2.3)
	SG.AC-4	アクセスの実施 Access Enforcement	GRC	AC-3	Access Enforcement	2.15.7	Access Enforcement	CIP 004-3a (R4) CIP 005-3a (R1.6, R2, R2.1-R2.4) CIP 007-3a (R5)
	SG.AC-5	情報フローの実施 Information Flow Enforcement	UTR	AC-4	Information Flow Enforcement	2.15.15	Information Flow Enforcement	－
	SG.AC-6	職務の分離 Separation of Duties	GRC	AC-5	Separation of Duties	2.15.8	Separation of Duties	CIP 005-3a (R2, R2.1) CIP 007-3a (R5.1, R5.2)
	SG.AC-7	最小限の特権 Least Privilege	GRC	AC-6	Least Privilege	2.15.9	Least Privilege	CIP 007-3a (R5.1, R5.2)
	SG.AC-8	ログイン試行の失敗 Unsuccessful Login Attempts	CTR	AC-7	Unsuccessful Login Attempts	2.15.20	Unsuccessful Logon Notification	CIP 007-3a (R5)
	SG.AC-9	スマート・グリッド情報システム利用通知 Smart Grid Information System Use Notification	CTR	AC-8	System Use Notification	2.15.17	System Use Notification	CIP 005-3a (R2.6)
	SG.AC-10	前回ログオンの通知 Previous Logon Notification	UTR	AC-9	Previous Logon (Access) Notification	2.15.19	Previous Logon Notification	－
	SG.AC-11	同時セッションのコントロール Concurrent Session Control	UTR, Availability	AC-10	Concurrent Session Control	2.15.18	Concurrent Session Control	－
	SG.AC-12	セッションロック Session Lock	UTR	AC-11	Session Lock	2.15.21	Session Lock	－
	SG.AC-13	リモートセッションの終了 Remote Session Termination	UTR	－	－	2.15.22	Remote Session Termination	CIP 007-3a (R6)
	SG.AC-14	識別または認証なしで許可されるアクション Permitted Actions without Identification or Authentication	UTR	AC-14	Permitted Actions without Identification or Authentication	2.15.11	Permitted Actions without Identification and Authentication	－
	SG.AC-15	リモートアクセス Remote Access	UTR	AC-17	Remote Access	2.15.24	Remote Access	CIP 005-3a (R2, R2.1-R2.5, R3, R3.1, R3.2) CIP 007-3a (R2.1, R5)
	SG.AC-16	無線アクセスの制限 Wireless Access Restrictions	GRC	－	－	2.15.26	Wireless Access Restrictions	CIP 005-3a (R1.1, R2, R2.4, R3, R3.2)
	SG.AC-17	ポータブルおよびモバイルデバイスのアクセス制御 Access Control for Portable and Mobile Devices	GRC	AC-19	Access Control for Mobile Devices	2.15.25	Access Control for Portable and Mobile Devices	CIP 005-3a (R2, R2.1, R2.2, R2.4, R3, R3.2)
	SG.AC-18	外部情報管理システムの利用 Use of External Information Control Systems	GRC	SC-7	Boundary Protection	2.15.29	Use of External Information Control Systems	CIP 005-3a (R2.4)
	SG.AC-19	制御システムのアクセス制限 Control System Access Restrictions	CTR	－	－	2.15.28	External Access Protections	CIP 005-3a (R1.6) CIP 007-3a (R5)
	SG.AC-20	パブリックにアクセス可能なコンテンツ Publicly Accessible Content	GRC	AC-22	Publicly Accessible Content	－	－	－
	SG.AC-21	パスワード Passwords	GRC	－	－	2.15.16	Passwords	CIP 007-3a (R5.3, R5.3.3)

NIST IR 7628 の論理インターフェースカテゴリ

②論理インターフェースカテゴリ（LIC）と影響レベル

論理参照モデルの開発－論理インターフェス分類（ 22 種類）			分類別の影響レベル		
No.	論理インターフェース分類（LIC）	例	C：機密性	I：完全性	A：可用性
1	高可用性で、計算能力と帯域幅の両方、またはいずれか一方で制限がある、制御システムと設備の間のインターフェース	・送電 SCADA と変電設備の間 ・配電 SCADA と高優先変電所とポールトップ機器の間 ・発電所内の SCADA と DCS の間	低	高	高
2	非高可用性だが、計算能力と帯域幅の両方、またはいずれか一方上制限がある、制御システムと設備の間のインターフェース	・配電 SCADA と優先度の低いポールトップ機器の間 ・ポールトップ IEDs（インテリジェント電子デバイス）と他のポールトップ IEDs の	低	高	中
3	高可用性で、計算能力や帯域幅上制限がない、制御システムと設備の間のインターフェース	・送電 SCADA と変電所自動システムの間	低	高	高
4	非高可用性で、また計算能力や帯域幅上制限もない、制御システムと設備の間のインターフェース	・配電 SCADA とポールトップ IED分配用にバックボーンネットワークに接続されたコレクタノードの間	低	高	中
5	同じ組織内部の制御システムの間のインターフェース	・同じユーティリティ内の複数の DMS （配電管理システム）システム間 ・DCS 内のサブシステムと、発電所内の補助制御システムの間	低	高	高
6	別の組織の制御システムの間のインターフェース	・地域送電事業者/独立系統運用者のエネルギー管理システムとユーティリティエネルギー管理システムの間	低	高	中
7	共通管理機関下の事務系システムの間のインターフェース	・顧客情報システムとメーターデータ管理システムの間	高	高	低
8	違う管理機関下の事務系システムの間のインターフェース	・サードパーティの課金システムとユーティリティメータデータ管理システムの間	高	高	低
9	B2B関係の金融やマーケットのシステムの間のインターフェース	・小売集計システムとエネルギー中央集配センターの間	高	高	中
10	制御システムと非制御／事務系システムの間のインターフェース	・作業管理システムと地理情報システムの間	低	高	中
11	環境パラメータを測定するためのセンサーとセンサーネットワーク（普通はおそらくアナログ測定の簡単なセンサーデバイス）の間のインターフェース	・変圧器の温度センサとレシーバの間	低	中	中
12	センサーネットワークと制御システムの間のインターフェース	・センサレシーバと変電所マスタの間	低	中	中
13	高度計量インフラネットワークを利用するシステムの間のインターフェース	・メーターデータ管理システム（MDMS）とメーターの間 ・負荷管理システム（LMS）/分散電源管理システム（DRMS）と顧客エネルギー管理システムの間	高	高	低
14	可用性の高い高度計量インフラネットワークを利用するシステムの間のインターフェース	・メーターデータ管理システムとメーターの間 ・負荷管理システム/分散電源管理システムと顧客エネルギー管理システムの間 ・配電管理システムアプリケーションと顧客の分散電源の間。 ・配電管理システムアプリケーションと配電オートメーションフィールド機器の間	高	高	高
15	HAN(Home Area Network)、BAN (Building Area Network)などの顧客（住宅、商業、および産業）サイトネットワークを使用するシステム間のインターフェイス	• 顧客エネルギー管理システムと顧客のアプライアンス機器との間 • 顧客エネルギー管理システムと顧客の分散電源との間 • エネルギーサービスインターフェース (ESI) と PEVs (プラグイン電気媒体) との間	低	中	中
16	外部システムと顧客サイトとの間のインターフェース	• サードパーティとホームエリアネットワークゲートウェイとの間 • エネルギーサービスプロバイダと分散電源との間 • 顧客と顧客情報システムWebサイト	高	中	低
17	システムと現地スタッフのモバイルパソコン／機器の間のインターフェース	• フィールドクルーと地理情報システムとの間 • フィールドクルーと変電所設備との間	低	高	中
18	測定装置の間のインターフェース	• メーターからサブメーターの間 • プラグイン電気媒体メーターとエネルギーサービスプロバイダの間	中	高	低
19	運営決定サポートシステムの間のインターフェース	• 広域計測システムと独立系統運用者/地域送電事業者の間	低	高	中
20	エンジニアリング／保守システムと制御装置の間のインターフェース	• エンジニアリングと変電所のリレー設定用中継機器の間 • メンテナンスのためのエンジニアリングとポールトップ機器間 • 発電プラント内	低	高	中
21	保守およびサービスのための、制御システムとシステム構築ベンダとの間のインターフェース	• SCADAシステムと構築ベンダー間	低	高	中
22	セキュリティ／ネットワーク／システム管理操作端末と、全てのネットワーク及びシステムの間のインターフェース	• セキュリティコンソールとネットワークルーター、ファイアウォール、コンピュータシステム、およびネットワークノードの間	高	高	高

NIST IR 7628 の論理参照カテゴリの属性と定義

②LICの属性は、機密性、完全性、および可用性の影響レベルを決定したガイド

論理インターフェースカテゴリ ＼ 属性	ATR-1a: 機密性の要件	ATR-1b: プライバシーに関する懸念	ATR-2: 完全性要件	ATR-3: 可用性要件	ATR-4: 通信チャネルの低帯域幅	ATR-5: メモリ及び演算能力へのマイクロプロセッサの制約	ATR-6: ワイヤレスメディア	ATR-7: 未熟または独自のプロトコル	ATR-8: 組織間相互作用	ATR-9: レイテンシ問題の低トレランスに備えたリアルタイム運用要件	ATR-10: レガシーなエンドデバイスとシステム	ATR-11: レガシーなコミュニケーションプロトコル	ATR-12: セキュアでない、信頼できないロケーション	ATR-13: 多数のデバイスのキー管理	ATR-14: スケーラビリティと通信を含むデバイスのパッチおよび更新管理の制約	ATR-15: 相互作用の予測できない、ばらつきまたは多様性	ATR-16: 環境および物理的なアクセス制約	ATR-17: 一次電力のための限られた動力源	ATR-18: 自律制御
1	高可用性で、計算能力と帯域幅の両方、またはいずれか一方で制限がある、制御システムと設備の間のインターフェース			•	•	•	•	•	•		•	•	•	•	•	•		•		•
2	非高可用性だが、計算能力と帯域幅の両方、またはいずれか一方上制限がある、制御システムと設備の間のインターフェース			•		•	•	•	•		•	•	•	•	•	•		•	•	•
3	高可用性で、計算能力や帯域幅上制限がない、制御システムと設備の間のインターフェース			•	•			•	•		•	•	•	•	•	•		•		•
4	非高可用性で、また計算能力や帯域幅上制限もない、制御システムと設備の間の			•				•	•		•	•	•	•	•	•	•	•		•
5	同じ組織内部の制御システムの間のインターフェース			•	•						•		•			•				•
6	別の組織の制御システムの間のインターフェース			•	•					•	•		•			•				
7	共通管理機関下の事務系システムの間のインターフェース	•	•	•												•				
8	違う管理機関下の事務系システムの間のインターフェース	•	•	•						•						•				
9	B2B関係で繋がっている金融やマーケットのシステムの間のインターフェース	•	•	•	•					•	•						•			
10	制御システムと非制御／事務系システムの間のインターフェース	•	•	•	•				•	•						•	•			
11	環境パラメータを測定するためのセンサーとセンサーネットワーク（普通はおそらくアナログ測定の簡単なセンサーデバイス）の間のインターフェース					•	•	•	•		•	•	•	•				•	•	
12	センサーネットワークと制御システムの間のインターフェース			•	•	•	•	•	•		•	•	•		•			•	•	•
13	高度計量インフラネットワークを利用するシステムの間のインターフェース	•	•	•		•	•	•	•	•				•	•	•	•	•		
14	可用性の高い高度計量インフラネットワークを利用するシステムの間のインターフェース	•	•	•	•	•	•	•	•	•				•	•	•	•	•		
15	HAN(Home Area Network)、BAN (Building Area Network)などの顧客（住宅、商業、および産業）サイトネットワークを使用するシステム間のインターフェイス	•	•	•	•		•	•	•	•	•			•	•		•	•		•
16	外部システムと顧客サイトとの間のインターフェース	•	•	•			•		•	•				•	•		•			
17	システムと現地スタッフのモバイルパソコン／機器の間のインターフェース			•	•	•		•	•					•	•	•		•		
18	測定装置の間のインターフェース	•	•	•		•	•	•	•	•		•	•	•	•	•		•		
19	運営決定サポートシステムの間のインターフェース			•	•					•	•									
20	エンジニアリング／保守システムと制御装置の間のインターフェース			•	•	•	•					•	•	•	•	•		•		
21	保守およびサービスのための、制御システムとシステム構築ベンダとの間のインターフェース			•	•					•				•	•	•		•		
22	セキュリティ／ネットワーク／システム管理操作端末と全てのネットワーク及びシステムの間のインターフェース	•	•	•	•						•	•	•		•	•	•	•		

NIST IR 7628 の脆弱性クラスと対抗策

③脆弱性クラスごとに対応する対策要件（ただし、SG.RA「リスク管理と評価」が欠落）

脆弱性クラス			スマート・グリッドのセキュリティ要件ファミリ （脆弱性に対して適用可能なセキュリティ要件）																	
			SG.AC	SG.AT	SG.AU	SG.CA	SG.CM	SG.CP	SG.IA	SG.ID	SG.IR	SG.MA	SG.MP	SG.PE	SG.PL	SG.PM	SG.PS	SG.RA	SG.SA	SG.SC	SG.SI
要員、方針および手順	トレーニング	訓練の不十分な要員		●				●			●					●					
		不十分なセキュリティトレーニングと啓発プログラム		●				●			●					●					
	方針および手順	不十分なID 検証、バックグラウンドチェック	●						●			●		●		●	●				
		不十分なセキュリティ方針	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●			●	●
		不十分なプライバシー方針				●										●					
		不十分なパッチ管理プロセス	●				●	●	●		●					●			●		●
		不適切な変更と構成の管理					●									●			●		
		不要なシステム接続	●				●		●				●	●		●	●				
	リスクマネジメント	不十分な定期セキュリティ監査			●											●					
		不十分な管理者によるセキュリティ監視		●	●	●								●		●	●				
		不十分な運用または災害復旧計画の継続性				●		●							●	●					
		不十分なリスク評価プロセス														●					
		不適切なインシデント対応プロセス					●				●			●	●	●					
プラットフォームソフトウェア/ファームウェアの脆弱性	ソフトウェア開発	コード品質における脆弱性		●								●				●	●		●	●	●
		認証の脆弱性		●	●				●			●				●			●		●
		認可の脆弱性		●	●				●			●				●			●		●
		暗号化の脆弱性		●								●				●			●		
		環境の脆弱性	●	●					●			●				●	●		●	●	
		エラー処理の脆弱性		●								●				●			●		●
		一般的な論理エラー		●								●				●			●		
		ビジネス論理エラー		●								●				●			●		
		入力と出力の検証		●								●				●			●		●
		ログと監査の脆弱性		●					●			●				●			●		
		パスワード管理の脆弱性	●	●					●			●				●			●		
		パスの脆弱性		●								●				●			●		
		プロトコルエラー		●								●				●			●		
		範囲と種類のエラーの脆弱性		●								●				●			●		
		機密性データ保護の脆弱性		●						●		●				●			●		
		セッション管理の脆弱性		●								●				●			●		
		同時処理、同期、タイミングの脆弱性		●								●				●			●		
		不十分なモバイルコード保護		●								●				●			●		
		バッファオーバーフロー		●								●				●			●		
		未定義/不適切に定義された、または「不正な」条件の誤った取り扱い		●								●				●			●		
		セキュアでないプロトコルの使用		●								●				●			●	●	
		ファイルやディレクトリに影響を与える弱点		●								●				●			●		
	API の使用と実装	API の乱用		●								●				●			●		
		危険な API の使用		●								●				●			●		
プラットフォームの脆弱性	デザイン	不十分なセキュリティアーキテクチャと設計の使用	●	●	●			●	●		●	●			●	●	●		●	●	●
		セキュリティ設計のための外部または内部レビューの欠如	●	●	●			●	●		●	●			●	●	●		●	●	●
	実装	ホワイトリスト（ベストプラクティス）			●		●					●									
		ファイル完全性の監視（ベストプラクティス）								●		●	●						●		●
		不十分なマルウェア対策		●	●			●			●				●				●	●	●
		インストール済みのセキュリティ機能がデフォルトで有効になっていない	●	●	●		●		●						●				●	●	●
		装置実装ガイドラインの不在または不足	●	●	●		●		●						●	●			●	●	
	運用	ソフトウェアベンダからの迅速なセキュリティ修正プログラム提供の欠如			●			●			●								●	●	●
		不要なサービスの実行		●	●		●								●				●	●	●
		不十分なログ管理	●	●	●		●	●	●		●		●		●				●	●	●
	設定の貧弱な装置	不十分なアノマリ追跡	●	●	●			●	●		●			●	●		●		●	●	●
ネットワーク	ネットワーク	不十分な完全性チェック				●	●					●				●			●		●
		不十分なネットワーク分離				●	●					●							●	●	●
		不適切なプロトコルの選択				●	●					●				●			●	●	●
		認証プロセスまたは認証キーの弱点					●					●							●		
		不十分な冗長性	●			●	●		●			●		●		●	●				
		デバイスへの物理的なアクセス	●			●	●		●			●		●		●	●		●		

LICへのセキュリティ要件割り当て

④LICごとに推奨されるセキュリティ要件（SG.AC抜粋）

White = Common Governance, Risk and Compliance　Light Gray = Common Technical Requirement　Dark Gray = Unique Technical Requirement

スマートグリッドのセキュリティ要件		論理インターフェースカテゴリ（LIC）																				
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
SG.AC-1	アクセス制御の方針と手順	全ての影響レベルに適用																				
SG.AC-2	リモートアクセスの方針と手順	全ての影響レベルに適用																				
SG.AC-3	アカウント管理	全ての影響レベルに適用																				
SG.AC-4	アクセスの実施	全ての影響レベルに適用																				
SG.AC-6	職務の分離	中と高の影響レベルに適用																				
SG.AC-7	最小限の特権	中と高の影響レベルに適用																				
SG.AC-8	ログイン試行の失敗	全ての影響レベルに適用																				
SG.AC-9	スマート･グリッド情報システム利用通知	全ての影響レベルに適用																				
SG.AC-11	同時セッションのコントロール									高								高				
SG.AC-12	セッションロック							高	高	中						中		中				中	高
SG.AC-13	リモートセッションの終了									中						中		中		中			
SG.AC-14	識別または認証なしで許可されるアクション	高	高	高	高	高	高	中	中	中	高			高	高	中	中	高	高		高	高	高
SG.AC-15	リモートアクセス									高						中					高	高	高
SC.AC-16	無線アクセスの制限	全ての影響レベルに適用																				
SG.AC-17	ポータブル/モバイルデバイスのアクセス制御	中と高の影響レベルでの追加向上要件とともに全ての影響レベルに適用																				
SG.AC-18	外部情報管理システムの利用	中と高の影響レベルでの追加向上要件とともに全ての影響レベルに適用																				
SG.AC-19	制御システムのアクセス制限	全ての影響レベルに適用																				
SG.AC-20	パブリックにアクセス可能なコンテンツ	全ての影響レベルに適用																				
SG.AC-21	パスワード	全ての影響レベルに適用																				

ただし、SG.AC-5,SG.AC-10にはセキュリティ要件割当がない

～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