intel Security

TM

米国電力システムにおける セキュリティガイドラインの アプローチ手法について

マカフィー株式会社　サイバー戦略室
佐々木　弘志，CISSP

アジェンダ

0．セキュリティガイドラインがなぜ必要なのか？

1．ガイドラインの２つのアプローチ

2．NERC CIP ver.5

3．NIST IR 7628

4．まとめ

参考．NIST Framework

0. セキュリティガイドラインがなぜ必要なのか？

制御システムのオープン化

- 制御システム間の通信インタフェースのイーサネット化
- 制御システムの汎用OS化（Windows Embedded, Linuxなどの利用）

制御システムを狙った攻撃の発生

- 2010年 Stuxnetの登場　イランの核施設を破壊。クローズ環境だったがUSBメモリ経由で感染
  SIEMENS社製のPLCプログラミングソフトStep7/Win CCがハッキングされた
- 2014年 Operation Dragonfly　欧州の電力会社数社の制御システム管理サーバー情報が漏えい

世界中でガイドラインによる対策が進行中

- 制御システムセキュリティ標準の制定（国際：IEC62443　業界：NERC CIP, NIST IR 7628）
- 国家レベルの取り組み（米国：NIST Framework　EU：ENISA, ENCS, DENSEK）

重要インフラにおいては、事業者のビジネスリスクだけではなく、国家レベルのリスクもあるので、どこまで、どうやって対策したらいいのかの基準が必要

0. 電力システム向けセキュリティガイドライン策定

（報告書概要）4. 電力システムにおけるサイバーセキュリティ対策の在り方

電力システムにおける現状と課題	米国の対策例	他産業の対策例
・これまで電力の安定供給に影響を与えたサイバーセキュリティインシデントは発生しておらず、現状の事業環境における対策としては一定の評価ができる。 ・今後は事業環境変化を踏まえた対策の検討が必要。	・事業者はセキュリティ対策に関するガイドライン（CIP※）の遵守状況をFERC（連邦エネルギー規制委員会）に提出。	・（通信）業界横断的な対策 ・（金融）内部・出口対策の強化 ・（プラント）外部からの侵入を前提とした対策の強化。マネジメントシステムの第三者認証。

提言（概要）

①マネジメントシステムの確立	②外部接続点の対策徹底	③業界横断的な情報共有	④セキュリティ人材の訓練・育成
○リスクを考慮したマネジメントシステムの確立 ・リスクアナリシス ・電力設備・機器（スマートメーター含む）の調達・廃棄における対策　等	○外部ネットワークとの接続点における対策 ・不正な通信の監視・検知 ・侵入防御の多段構成等の対策　等	○他分野（情報通信事業者等）の情報セキュリティ技術者等との情報共有の強化（共通脅威の分析等）	○経営課題としてのサイバーセキュリティ対策の重要性の啓発 ○導入、運用及びインシデント発生時、適切に対応できるセキュリティ人材の訓練・育成等

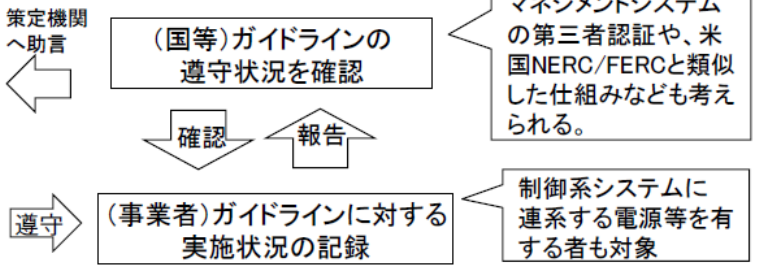
⑤電力分野のサイバーセキュリティガイドラインの策定等

○事業環境の変化も踏まえたガイドライン（日本版CIP※）の策定

■ガイドラインで規定する項目（案）（①～④を考慮して策定）

項目	概要
行動計画	セキュリティに関する行動計画を策定・実施
リスクアナリシス	リスクアナリシスを通じた重要資産の特定
対策立案	資産の重要度に応じたセキュリティ対策の立案
個別対策	電力システムの物理的保護
	電子的な接続点の保護
	サプライチェーンリスクの留意
人材育成	セキュリティ対策に資する人材育成・教育計画
危機管理	サイバーインシデントへの対応手順

○セキュリティ対策の実効性を高めるための検討



※CIP：NERC（北米電力信頼度協会）が作成するガイドライン（Cyber-security Critical Infrastructure Protection）

4

平成25年度 経済産業省　「平成25年度次世代電力システムに関する電力保安調査 」より

1. ガイドラインの２つのアプローチ
～ 仕様詳細規定型とリスクベース型 ～

仕様詳細規定型⇒守るべき項目がはっきりしている（チェックリスト、法令遵守）
リスクベース型⇒セキュリティリスクに焦点をあてて分析を行う

仕様詳細規定型アプローチ

IEC 62351： IEC 62351は、エネルギー自動化のコンテキストで、CPベースおよびシリアルプロトコルの明示的なセキュリティ対策を定義

IEC 61850-90-5：位相計測装置通信の整合性（HMACに基づく）とオプションの鍵管理の機密性（AESを使用）に関連するセキュリティに対応

NERC CIP:NERC（北米電力信頼度協議会）により発行された重要インフラストラクチャを保護するための強制的な標準

リスクベースのアプローチ

ISO/IEC 27001：「情報テクノロジーセキュリティ技法ー情報セキュリティ管理システムー要件」は、明確な管理制御のもとで情報セキュリティを導入することを目的とする管理システムについて正式に規定

ISO/IEC 27002：ISO/IEC 27002：「情報テクノロジーセキュリティ技法ー情報セキュリティ管理の実施規則」は、情報セキュリティ管理で推奨されるベストプラクティスを提供

EG2報告書：「データ処理、データ安全性および顧客保護への基本的規制要件と推奨事項」に関するTask Force Smart Grid Expert Group 2レポート

NIST Framework ：

NIST IR 7628：スマートグリッドのサイバーセキュリティに関する米国の非仕様詳細規定型勧告。

1. リスクベース型アプローチの例

機密性、完全性、可用性において、法的、財務的、人的、運用上、評判等に対してどのようなリスクがあるのかを分析

重要インフラでは可用性/完全性が重視されるケースが多い

機密性（Confidentiality）	完全性 (Integrity)	可用性 (Availability)
• 内部による情報漏えい • 外部による情報漏えい	• データ損失/エラー • 操作 • 信頼性	• 停止時間1時間未満 • 停止時間3時間未満 • 停止時間12時間未満 • 停止時間1日未満 • 停止時間1週間未満

法的な影響：警告、罰金、投獄、廃業まで多岐にわたる。2つの事項の考慮が必要：
- プライバシー法規制のコンプライアンス
- 他の法規制のコンプライアンス

財務的な影響：C-I-Aベースの経済的損失に基づく。

人的な影響：C-I-Aに起因する事故や人命の損失の可能性 。

運用上の影響： 可用性ベースのリスク：
- 地理的範囲。影響を受ける人/国の数。
- 重要インフラストラクチャの範囲。他の重要インフラストラクチャが1つのインシデントによって影響を受ける可能性がある。

評判への影響：企業の評判への影響は、廃業につながる可能性があり、可用性に関するセキュリティ要件に副次的な影響が及ぶ。

1. リスクの影響度レベルの分析例①

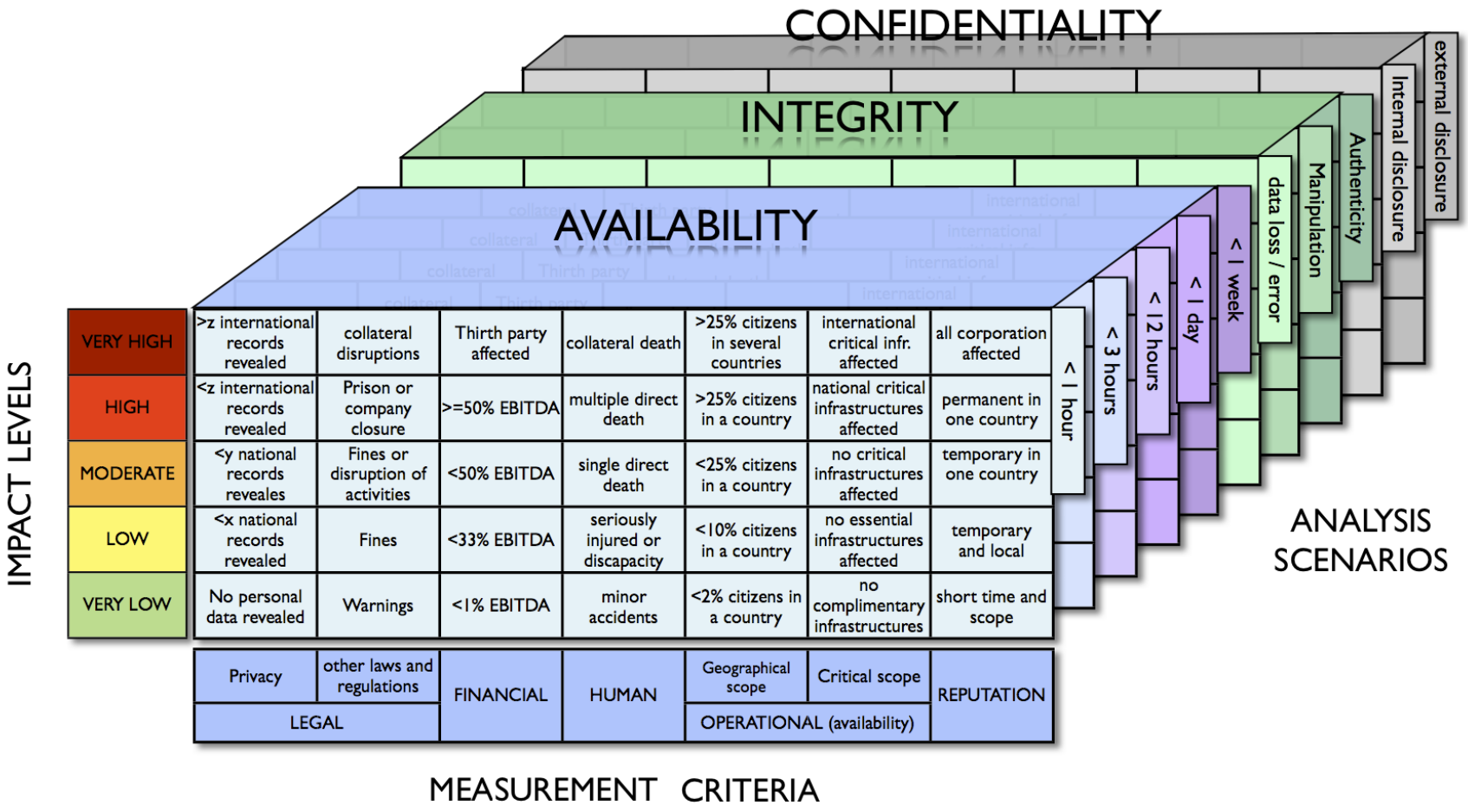
IMPACT LEVELS

	Privacy	other laws and regulations	FINANCIAL	HUMAN	Geographical scope	Critical scope	REPUTATION
	LEGAL				OPERATIONAL (availability)		
VERY HIGH	>z international records revealed	collateral disruptions	Thirth party affected	collateral death	>25% citizens in several countries	international critical infr. affected	all corporation affected
HIGH	<z international records revealed	Prison or company closure	>=50% EBITDA	multiple direct death	>25% citizens in a country	national critical infrastructures affected	permanent in one country
MODERATE	<y national records reveales	Fines or disruption of activities	<50% EBITDA	single direct death	<25% citizens in a country	no critical infrastructures affected	temporary in one country
LOW	<x national records revealed	Fines	<33% EBITDA	seriously injured or discapacity	<10% citizens in a country	no essential infrastructures affected	temporary and local
VERY LOW	No personal data revealed	Warnings	<1% EBITDA	minor accidents	<2% citizens in a country	no complimentary infrastructures	short time and scope

MEASUREMENT CRITERIA

それぞれの測定項目について発生するリスクを影響度を考慮して定義

1. リスクの影響度レベルの分析例②



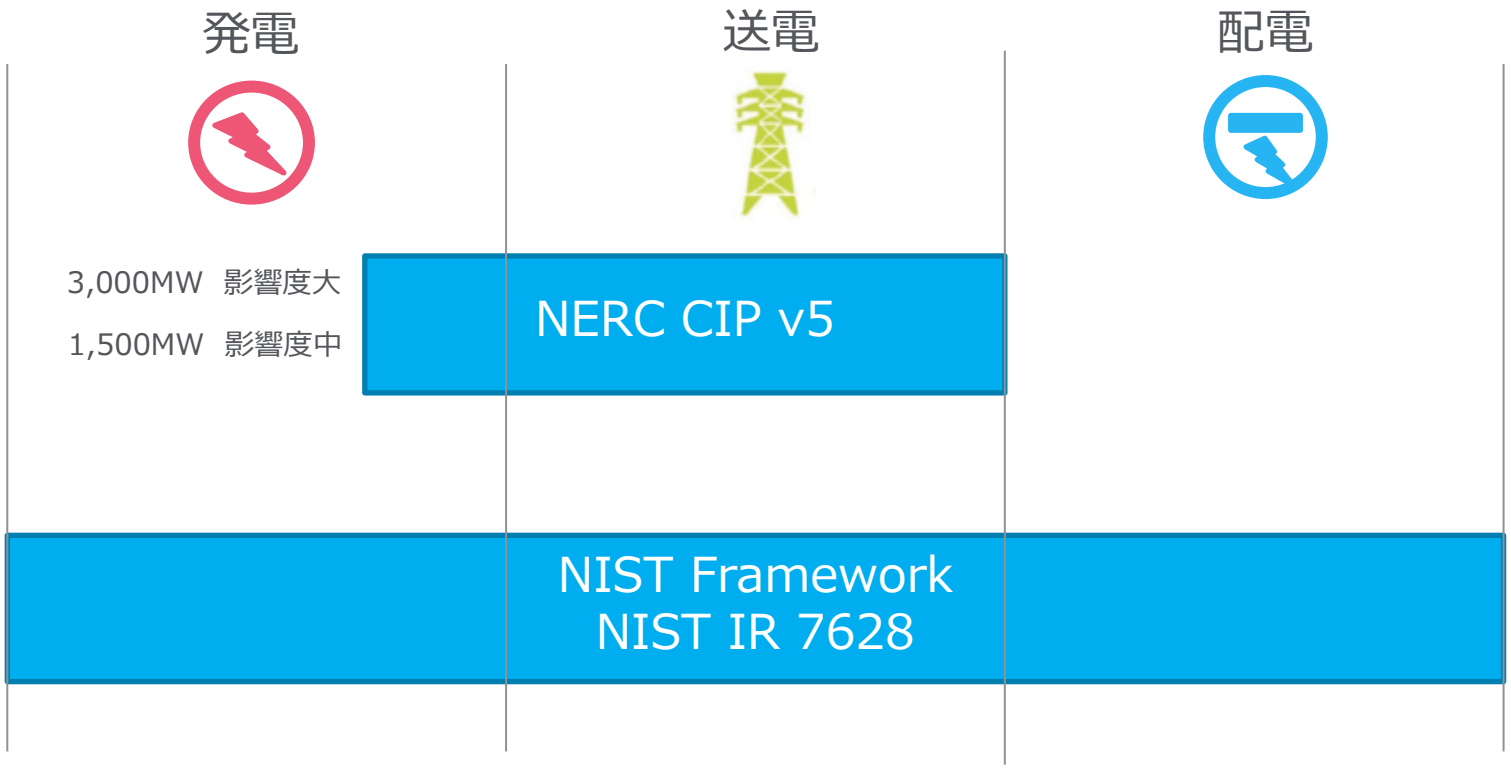
リスク分析シナリオに応じて測定項目とリスク影響度のマトリックスを生成⇒**影響度レベルに応じた対策可能**

1. 電力業界向けセキュリティ標準・ガイドライン例

標準・ガイドライン	作成機関	概要	アプローチ	強制力	有効年
NERC CIP Standard Ver. 3	NERC	発電、送電設備向けのセキュリティ標準	チェックリスト	あり (罰金)	2009
NERC CIP Standard Ver. 5	NERC	発電、送電設備向けのセキュリティ標準（対象設備の範囲がVer.3よりも拡大）	チェックリスト（資産評価にリスクベースアプローチを導入)	あり (罰金)	2016 (予定)
NIST IR 7628	NIST	スマートグリッド向けのガイドライン	**リスクベース**	なし	2010 rev1 2014
NIST Framework	NIST	重要インフラのサイバーセキュリティを向上させるためのフレームワーク	**リスクベース**	なし	2014

1. 標準・ガイドラインのマッピング

NERC CIP は電力の安定供給が主目的



NERC CIPは、**「電力の安定供給」**に主眼のある標準のため、大規模発電所と送電網に関連する電力事業者の施設のみが対象となっている。
→スマートメーター等、他の施設を守るためには、他のガイドラインの参照が必要。

1. 各標準・ガイドラインの活用方法

義務規定と任意のガイドラインを組み合わせて社内基準としている

マネジメント手法のガイドライン（任意）
改善のサイクルを回すためのセキュリティ成熟度モデル

ES-C2M2

活用

業界向けガイドライン（任意）
リスクベースの対策：ベースラインの上
現実の脅威に対抗するためのセキュリティ対策

NIST Framework

NIST IR 7628

NERC CIP v5

活用

義務規定
指示的な対策：ベースライン（フロア）
最低限のセキュリティ対策
チェックリスト方式

NERC CIP v3

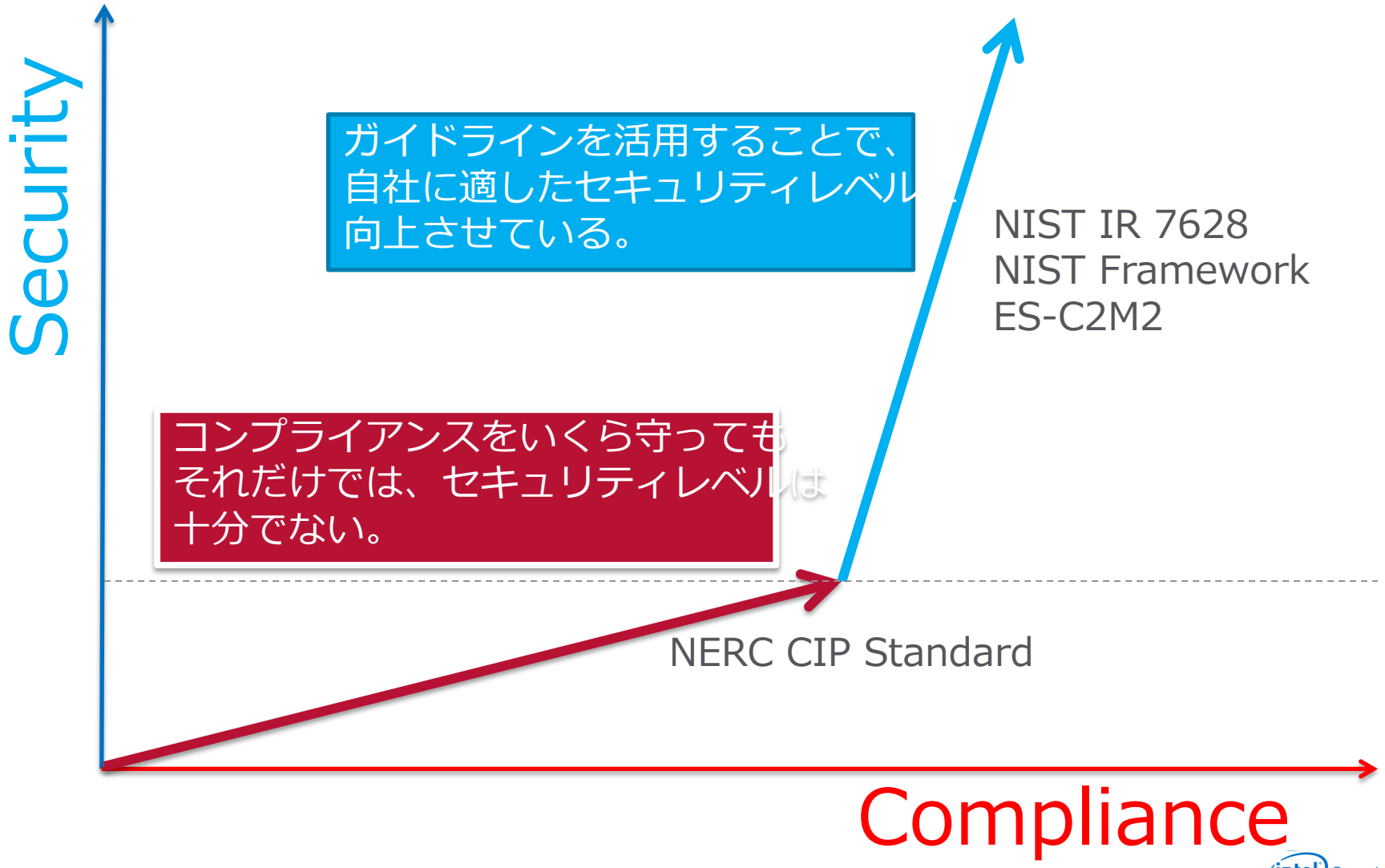
反映

電力事業者のセキュリティポリシー

様々な標準、ガイドライン、モデルを遵守
・活用しつつ、現実的な脅威に対して、独自の対策を加えた形で運用している。

1. Security vs. Compliance

コンプライアンスを守ることはセキュリティではない



2. NERC CIP とは？

・NERC　＝　北米電力信頼度評議会

(North American Electric Reliability Corporation)

北米各地への電力の安定供給を目的に、電力業界や連邦政府、州政府などによって１９６８年に創設された。電力供給システムが適正に稼働しているかどうかの評価や、大規模電力供給の計画策定等を行う。

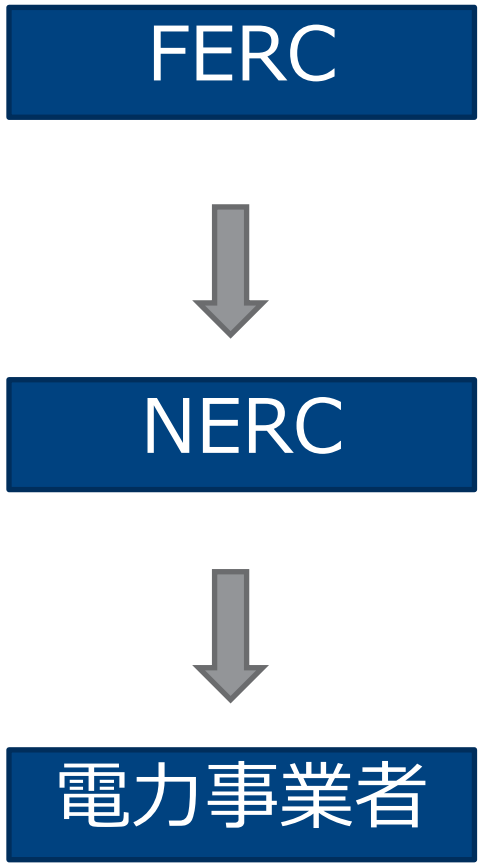
FERC（Federal Energy Regulatory Commission：米国連邦エネルギー規制委員会）の監督下にある。

・CIP　＝　重要インフラ防護

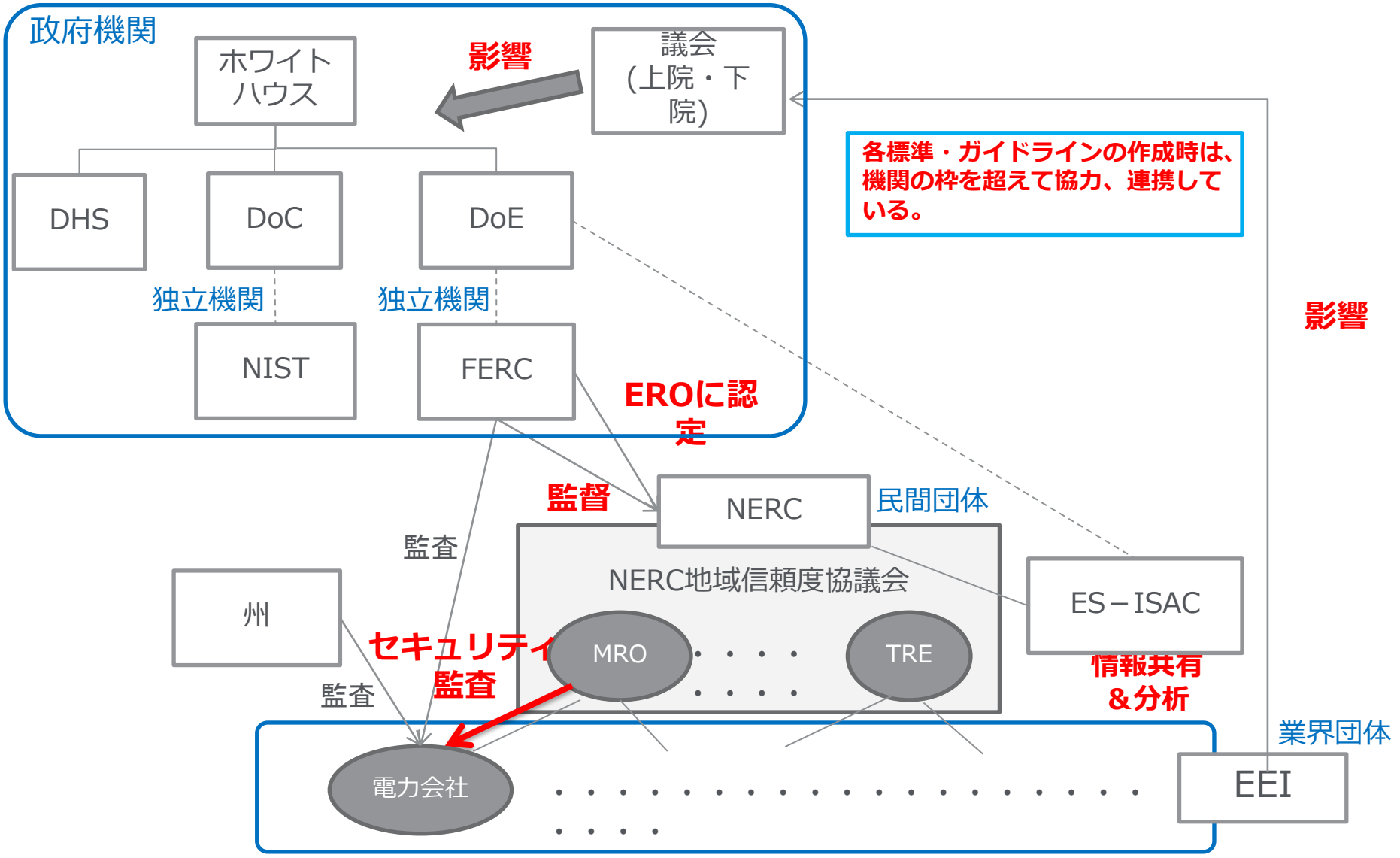
(Critical Infrastructure Protection)

・NERC CIP Standard

重要インフラ事業を遂行する上で実施すべきセキュリティ規準を分類し定義したもの。2005年にVer.1が リリースされ、現在はVer.5 にアップデートされており、2016年 7月からの発効に向けて事業者の対応が進められている。**違反すると違反の程度に応じて罰金が科せられる。**



2．電力業界のセキュリティ関連組織



2. NERCと政府、電力会社との関係性

民間団体
北米信頼度協議会
1965年設立

米国政府機関
連邦エネルギー
規制委員会
1978年設立

2005年　認定

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

系統の信頼度強化のための組織　ERO（Electric Reliability Organization）としてFERCから認定される。（北米唯一）
NERCの基準・規則に関して、指示および認定を行う。

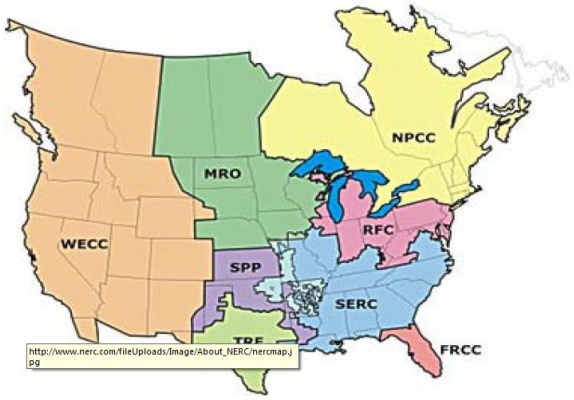
地域組織

基準
規則

基準・規則に違反している場合、違反している状況の発生時から改善が確認されるまでの不適合期間中、NERCに対して罰金を支払う。
罰金：違反毎　1日最大100万ドル

電力会社
及び関連会社

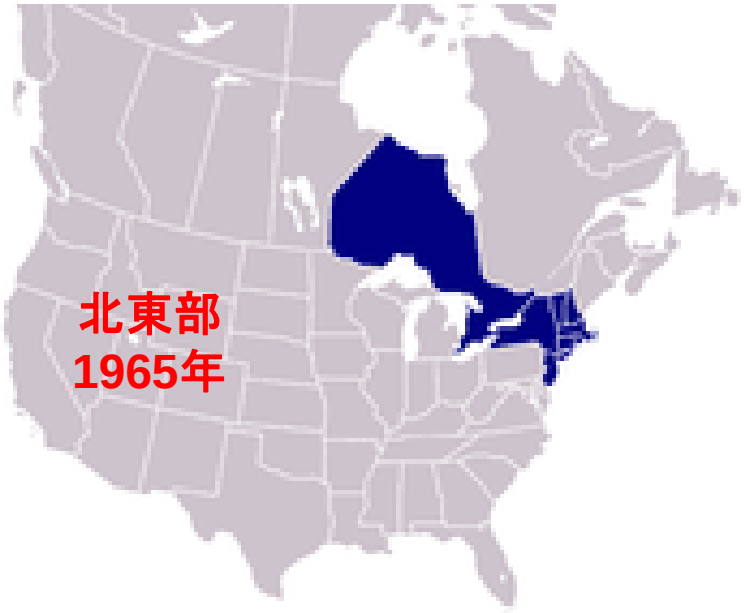
監査
コンサルティング

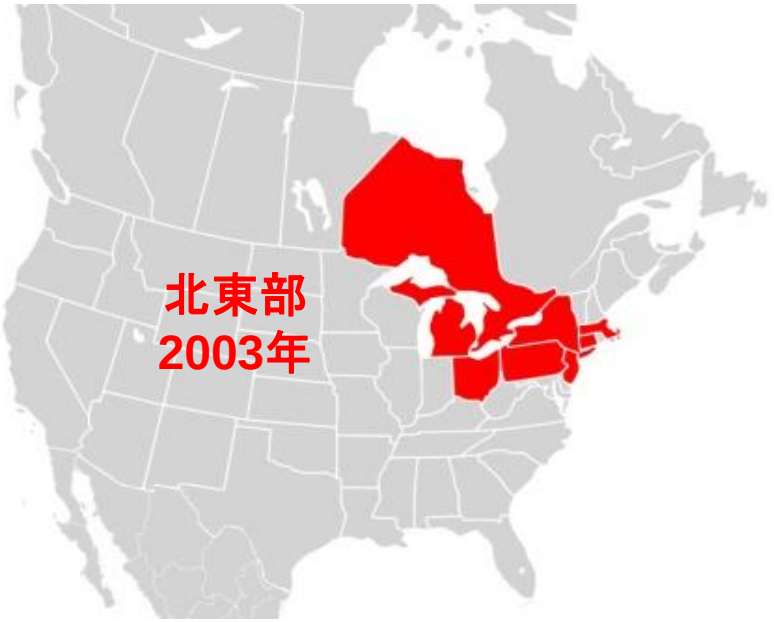


地域信頼度協議会
8組織

2. サイバーセキュリティ対策ガイドラインの背景

1965年、2003年　北米大規模停電





207,000 km²の地域で12時間停電。
2500万人に影響

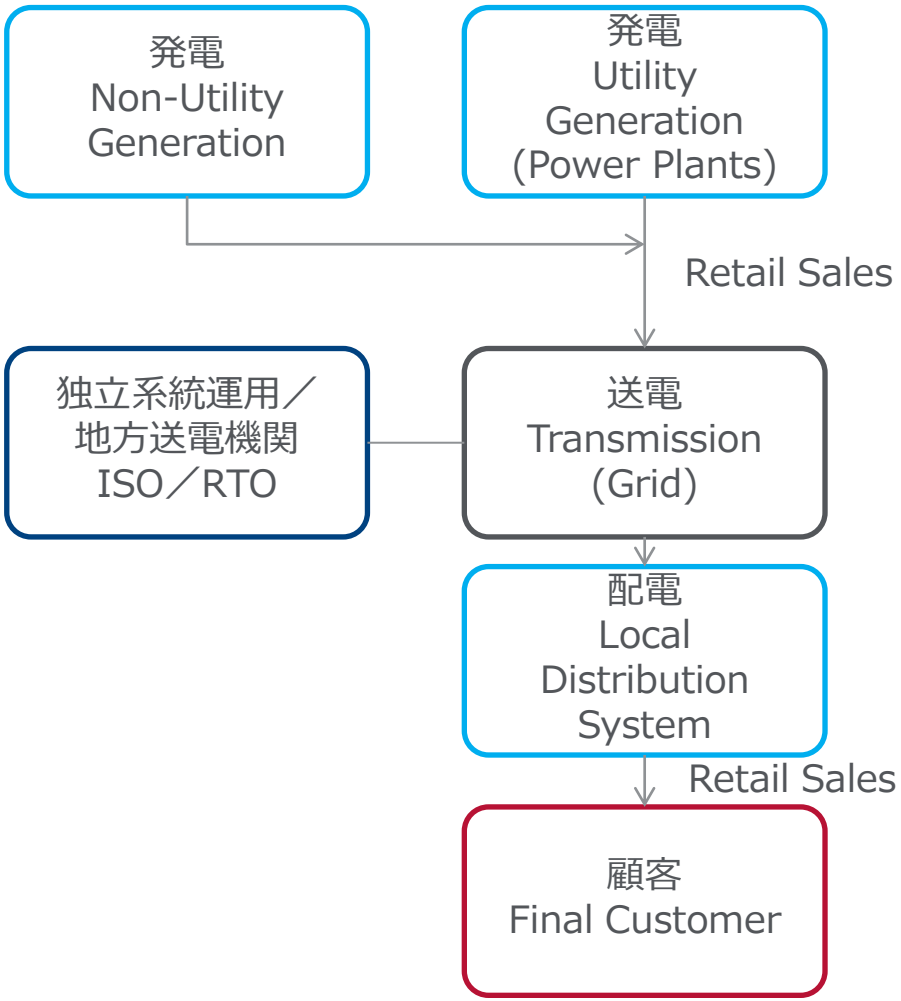
29時間の停電。5000万人に影響
送電システムの故障が原因とされる

NERCは1965年の大停電を受けて設立。2003年の大停電後には、電力の安定性確保のためにあらゆる面でのリスクヘッジの必要性が高まり、その流れで、サイバーセキュリティ対策の強化が求められた。

運用機関の任務:　明かりを灯し続けること!　Keep the light on!

2. サイバーセキュリティ対策ガイドラインの背景

米国の電力システムの構成



米国の電力システムは、発電、送電、配電、リテールの各部門が分離している。

送電施設の多くは民間の所有であるが、送電系統の運用や卸売市場はISO／RTOと呼ばれる独立した機関で運営されている。

電力事業者間の情報のやり取りは100%すべてISOを経由して行われる。

いわゆる「電力事業者」は民間、公営、組合などの形態に分かれているが、総数としては、約3,000社以上存在する。

割合としては公営事業者（2,000社以上）が多い。

事業者の規模としては、大手電力事業者から配電のみを行うような小規模事業者まで幅広い。

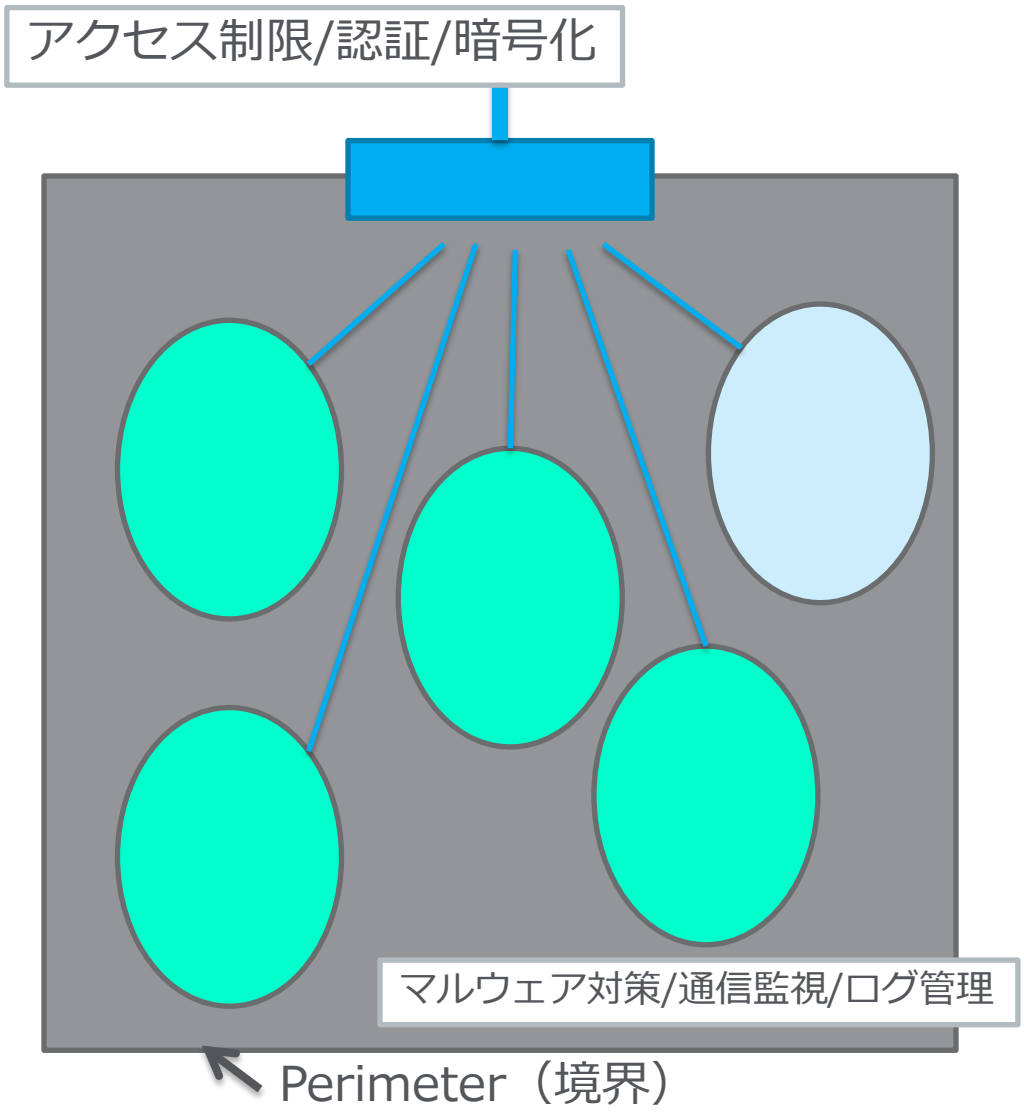
各電力会社にはCISOが必ずいる。また、CEOもサイバーセキュリティの重要性について認識

セキュリティ対策に関して事業者間で格差が
生じるが、全体のレベルを底上げするため、小規模事業者にもベースライン以上の対策を求めている。

2. NERC CIP ver.5 の項目

項目	項目概要	説明
CIP-002-05	サイバー上の重要資産の特定	リスクベースアプローチ（Ver.5より導入）に基づき重要サイバー資産を特定する。
CIP-003-05	セキュリティ管理	セキュリティ管理の確立。重要サイバー資産を保護するための行動計画の策定・実施。
CIP-004-05	人的管理とトレーニング	重要サイバー資産に電子的・物理的にアクセスする人に対するトレーニング、啓発活動
CIP-005-05	電子セキュリティ境界	重要サイバー資産を含むシステムに対する電子的なアクセス境界（ESP: Electronic Security Perimeter）の決定とセキュリティ対策
CIP-006-05	物理セキュリティ	重要サイバー資産を物理的に保護するための行動計画
CIP-007-05	システムセキュリティ管理	重要サイバー資産のセキュリティ対策
CIP-008-05	インシデント報告と対応計画	重要サイバー資産のインシデント報告と対応計画策定
CIP-009-05	復旧計画	重要サイバー資産の復旧計画の策定
CIP-010-01	設定変更管理と脆弱性検査	重要サイバー資産を保護するための設定変更管理と脆弱性検査の要件の策定
CIP-011-01	情報保護	重要サイバー資産の誤作動、不安定性につながる侵害から保護するための情報保護ポリシーの策定

2. NERC CIP の基本思想



サイバー上の重要資産の特定

電子的境界（Perimeter）の管理

電子的境界内の管理

定期的な脆弱性診断・ログのレビューによる改善
ドキュメント管理

2. NERC CIP ver.5 項目例

CIP-007-5表R1-ポートとサービス			
パート	該当するシステム	要件	方策
1.1	影響度高のBESサイバーシステムと、それに付随する： 1. EACMS； 2. PACS；および 3. PCA 外部ルーティング接続付き影響度中のBESサイバーシステムと、それに付随する： 1. EACMS； 2. PACS；および 3. PCA	技術的に可能な範囲で、ダイナミックポートの使用に必要なポート範囲またはサービスを含め、責任主体により必要と判断された論理ネットワークにアクセス可能なポートだけを有効にすること。デバイスが、デバイス上に論理ポートを無効または制限する設定が無い場合、オープンなポートは、必要であるとみなされる。	証拠例として以下を含むが、これに限定されない： - 個別、グループ別に拘わらず、該当するサイバー資産および電子アクセスポイント全てで有効なあらゆるポートの必要性を示す文書。 - 個別、グループ別に拘わらず、デバイスの設定ファイル、またはコマンド出力（netstat等によるもの）、オープンポートのネットワークスキャン結果等から得られる、サイバー資産におけるリスニングポートのリスト；あるいは -ホストベースのファイアウォールまたは必要なポートのみを許可し他一切を遮断するその他のデバイスレベルのメカニズムの設定ファイル。

チェックリスト型

⇒**何をすべきか**が書かれているため遵守しやすい

但し、**何を使うか**まででは書かれていないので事業者による選択の余地はある

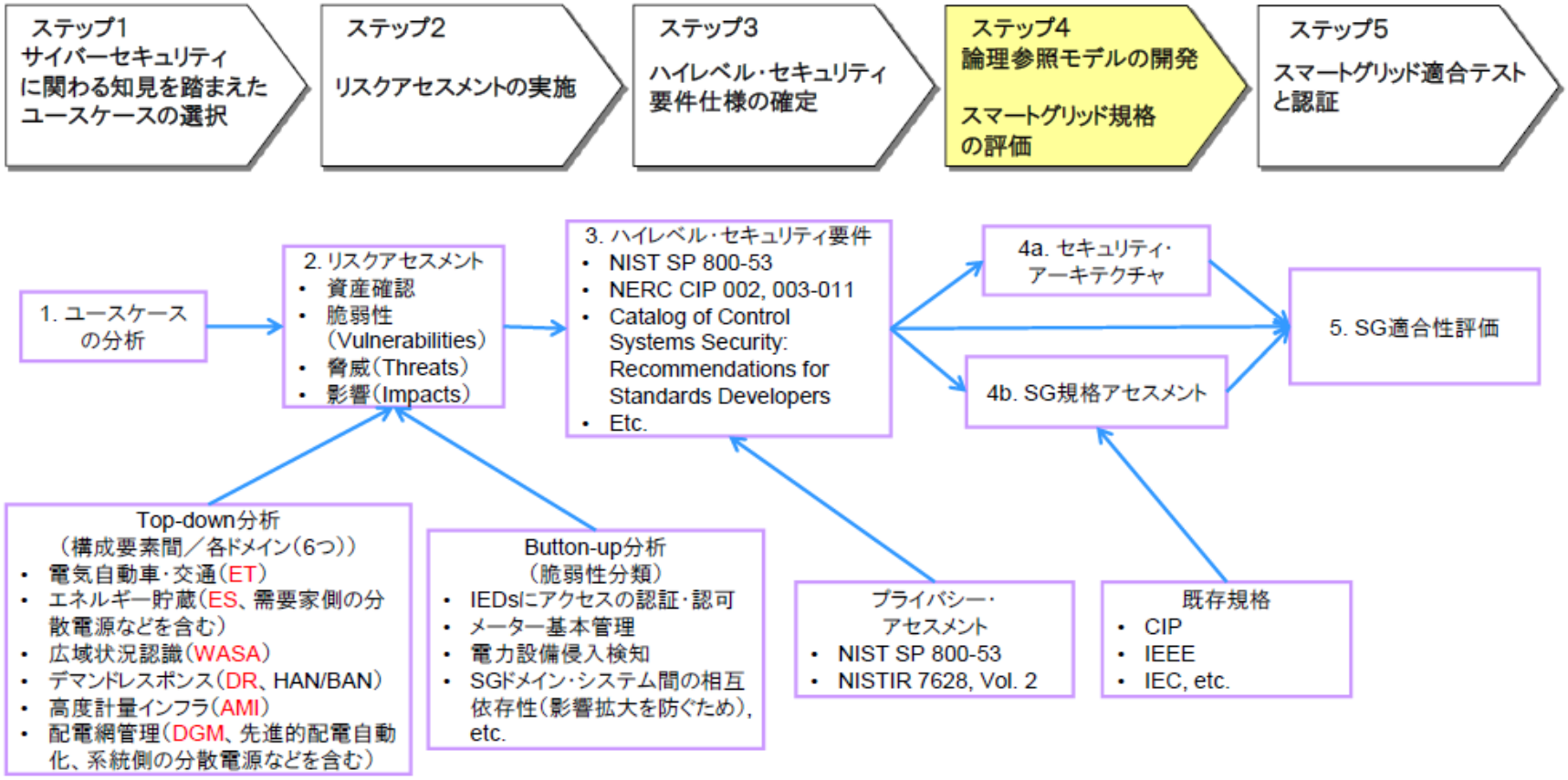
3. NIST IR 7628とは？

NIST (National Institute of Standards and Technology) 米国国立標準技術研究所が、2010年に発表したスマートグリッドセキュリティに関するガイドラインである。

IR は Internal Report（内部報告書）の略

NIST IR 7628では、リスクベースアプローチによって、スマートグリッドにおけるハイレベルな安全性要件、リスク評価の枠組み、プライバシー問題の評価等が定められており、スマートグリッドに関わる電力事業者全てが参照可能な内容となっている。

3. NIST IR 7628 のアプローチ



ユースケース⇒リスクアセスメント⇒ハイレベルなセキュリティ要件を確定

平成25年度 経済産業省　「平成25年度次世代電力システムに関する電力保安調査 」より

3. NIST IR 7628 のユースケース分析例

Category: Transmission Operations	Privacy Use Case #36

Scenario: Real-Time Normal Transmission Operations Using Energy Management System (EMS) Applications and SCADA Data

Category Description

Transmission operations involve monitoring and controlling the transmission system using the SCADA system to monitor and control equipment in transmission substations. The EMS assesses the state of the transmission system using applications typically based on transmission power flow models. The SCADA/EMS is located in the utility's control center, while the key equipment is located in the transmission substations. Protective relaying equipment monitors the health of the transmission system and takes corrective action within a few milliseconds, such as tripping circuit breakers if power system anomalies are detected.

Scenario Description

Transmission normal real-time operations involve monitoring and controlling the transmission system using the SCADA and EMS. The types of information exchanged include—

Monitored equipment states (open/close), alarms (overheat, overload, battery level, capacity), and measurements (current, voltage, frequency, energy).

Operator command and control actions, such as supervisory control of switching operations, setup/options of EMS functions, and preparation for storm conditions.

Closed-loop actions, such as protective relaying tripping circuit breakers upon power system anomalies.

Automation system controls voltage, VAR, and power flow based on algorithms, real-time data, and network linked capacitive and reactive components.

スマートグリッドの特徴	サイバーセキュリティ要件	潜在的な利害関係者問題
-電力の品質を提供 -資産活用の最適化 -システム妨害を予測、対応	-完全性は送電システムの安全と信頼性において致命的 -可用性は保護リレー（例：4ms未満）、オペレータのコマンド（例：1秒）にとって重要 機密性は重要でない	-顧客の安全 -顧客のデバイス標準 -顧客によるデマンドレスポンスの受け入れ

Data Privacy Recommendations

No personal data, or information that could point to an individual or specific account, is involved within this use case.

カテゴリ

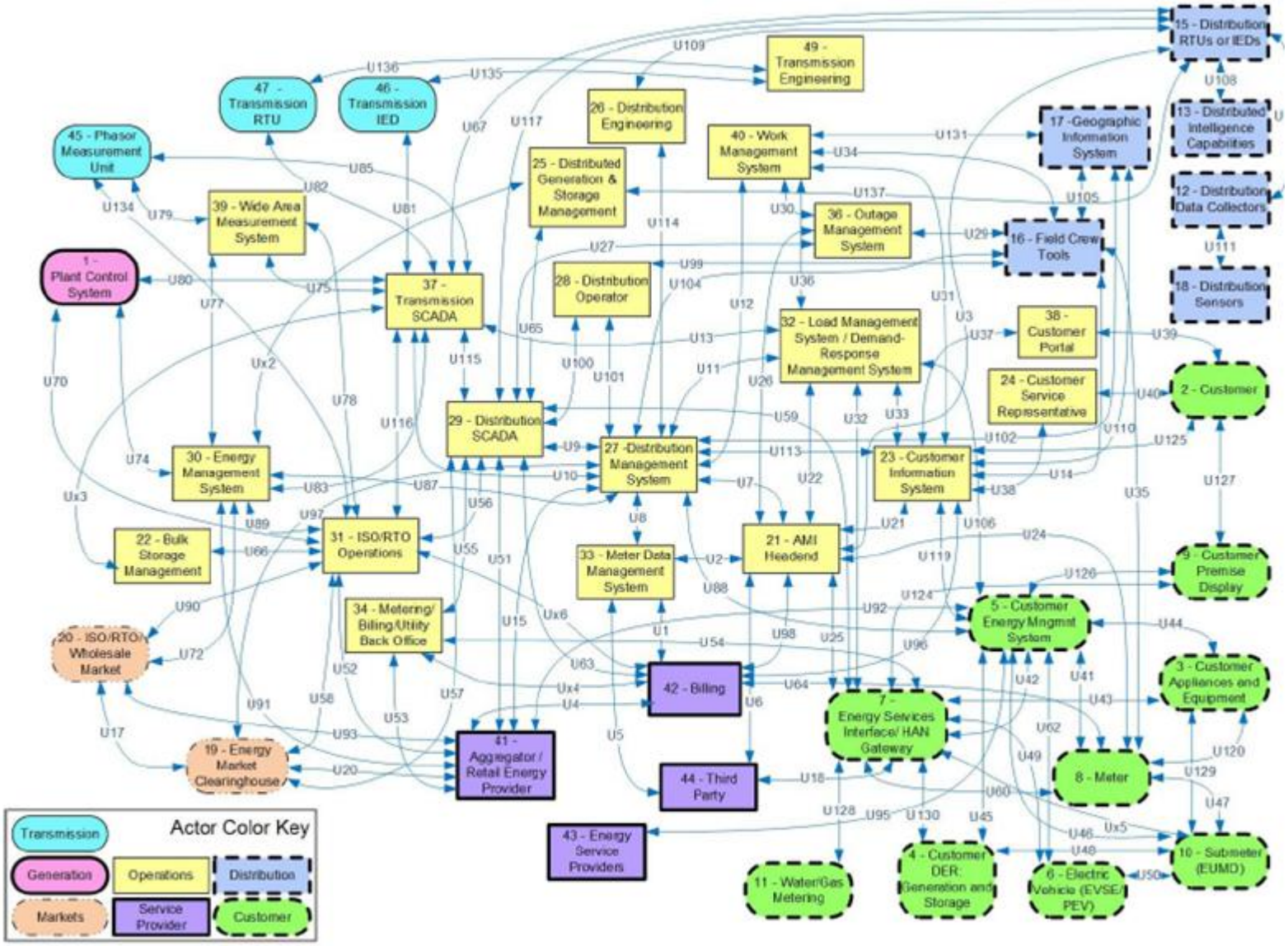
シナリオ

カテゴリ説明

シナリオ説明

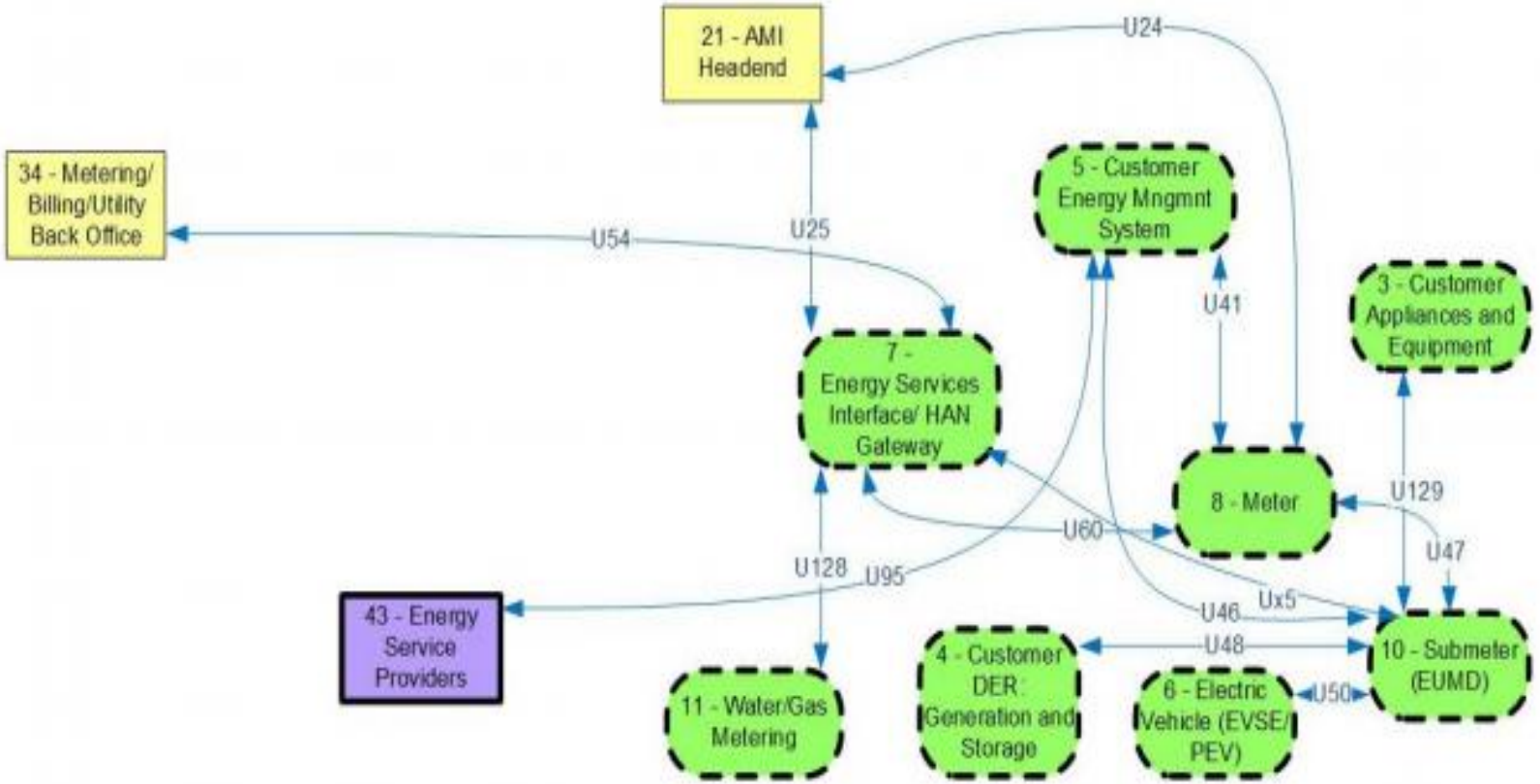
データプライバシー

3. NIST IR 7628 のリスクアセスメント①



3. NIST IR 7628 リスクアセスメント例②

例）メータリング装置間のインターフェース (22個あるうちのNo.18)



関係するインタフェース間の全てのリスク分析

No.18ではメーターに関する内容のため、機密性、完全性、可用性の影響度がそれぞれ「中」、「高」、「低」となっている。

3. NIST IR 7628 ハイレベルセキュリティ要件

セキュリティ要件と22個のインタフェースにおける適用性のマトリックス

セキュリティ要件グループ	Serial No.	SG サイバーセキュリティ要件名	論理インターフェース分類における適用性																					
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Access Control (SG.AC)	SG.AC-5	InformationFlow Enforcement																						
	SG.AC-6	Separation of Duties	Applies at moderate and high impact levels																					
	SG.AC-8	Unsuccessful Login Attempts	Applies at all impact levels																					
	SG.AC-10	Previous Logon Notification																						
	SG.AC-11	Concurrent Session Control																						
	SG.AC-12	Session Lock							H	H									L				L	H
	SG.AC-13	Remote Session Termination																	M		M			
	SG.AC-14	Permitted Actions without Identification or Authentication	H	H	H	H	H	H	M	M	M	H			H	H	M	M	H	H		H	H	H
	SG.AC-16	Wireless Access Restrictions	Applies at all impact levels																					
	SG.AC-18	Use of External Information Control Systems	Applies at all impact levels with additional requirement enhancements at moderate and high impact levels																					
	SG.AC-19	Control System Access Restrictions	Applies at all impact levels																					
	SG.AC-20	Publicly Accessible Content	Applies at all impact levels																					
	SG.AC-21	Passwords	Applies at all impact levels																					
Awareness and	SG.AT-5	Contact with Security Groups and																						

セキュリティ要件の適用性のレベルにリスク分析が反映
⇒メリハリのある対策が可能

4. まとめ

セキュリティガイドラインには、仕様詳細規定型とリスクベース型アプローチがあり、それぞれ事業者のセキュリティポリシー・対策に反映されている。

米国では、ガイドラインをベースとしたマーケットが存在する。
ガイドラインのような共通基盤の存在があると以下のようなメリットがある。

エンドユーザーのメリット：仕様書策定が楽、説明責任が果たせる
ベンダーのメリット：エンドユーザー個社へのカスタマイズが不要、
ガイドライン対応がビジネスになる

今後、電力をはじめとして、ガス、石油、化学等の重要インフラ業界でセキュリティガイドラインの策定が検討されていくものと考えられる

エンドユーザー：
制御システムも含めたセキュリティ管理ができる体制の構築（人材交流など）
ベンダー：
ガイドライン対応がビジネスになることを考慮して今から準備しておく

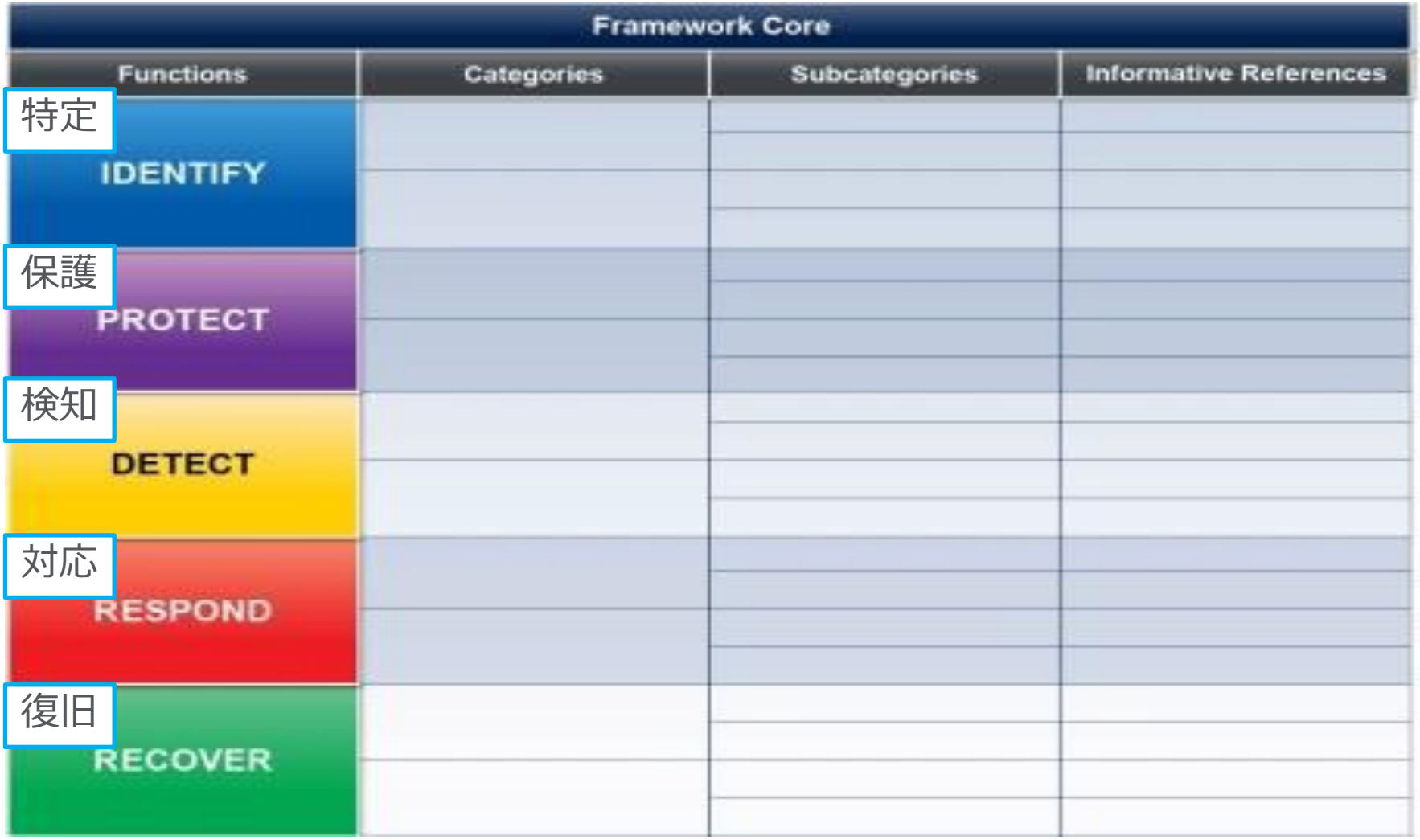
参考. NIST Framework とは？

NIST (National Institute of Standards and Technology) 米国国立標準技術研究所が、重要インフラ事業者向けのセキュリティフレームワークとして、Cybersecurity Framework Version 1.0を2014年2月に公開

組織のリスク管理に関する意思決定を強化するリスクベース型アプローチを採用したツール

- 技術スタッフとビジネス上の意思決定者の間のコミュニケーションを改善する
- 組織的なサイバーセキュリティの問題を検討するときに共通の言語を使用する
- 組織のセキュリティの現状を評価する
- 組織のセキュリティプロファイルの目標を展開する
- 詳細情報に基づいて、サイバーセキュリティの状況を改善するロードマップを作成できるようにする
- 組織内のサイバーセキュリティリスク管理に関する意思決定を強化する

参考. NIST Framework 「コア」



リスク管理すべきセキュリティ機能を５つに分類

参考. フレームワークコア - 特定（ID）

処理	カテゴリー	サブカテゴリー	参考資料
特定（ID）	**資産管理（ID.AM）:**組織がビジネス目標を達成できるようにするデータ、スタッフ、デバイス、システムおよび設備を特定し、ビジネス目標の重要度や組織のリスク方針に合わせて管理する	**ID.AM-1**:組織内の物理デバイスおよびシステムをインベントリ処理する	· **CCS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: 組織内のソフトウェアプラットフォームおよびアプリケーションをインベントリ処理する	· **CCS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3:組織のコミュニケーションおよびデータフローをマッピングする	· **CCS CSC** 1 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: 外部情報システムをカタログ化する	· **COBIT 5** APO02.02 · **ISO/IEC 27001:2013** A.11.2.6 · **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: 分類、重要度およびビジネス価値に基づいて、リソース（たとえば、ハードウェア、デバイス、データおよびソフトウェア）に優先順位を設定する	· **COBIT 5** APO03.03, APO03.04, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.6 · **ISO/IEC 27001:2013** A.8.2.1 · **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
		ID.AM-6:すべての従業員および利害関係のある第三者（たとえば、サプライヤ、顧客、パートナー）のサイバーセキュリティに関する役割（ロール）および責務を確立する	· **COBIT 5** APO01.02, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1 · **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11

参考. リスク管理と成熟度「ティア」

コア

Framework Core			
Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

リスクは、カテゴリー/サブカテゴリーのリストに基づいて、リスクの詳細を確認する機能により評価される

プロファイルの例:エネルギー分野

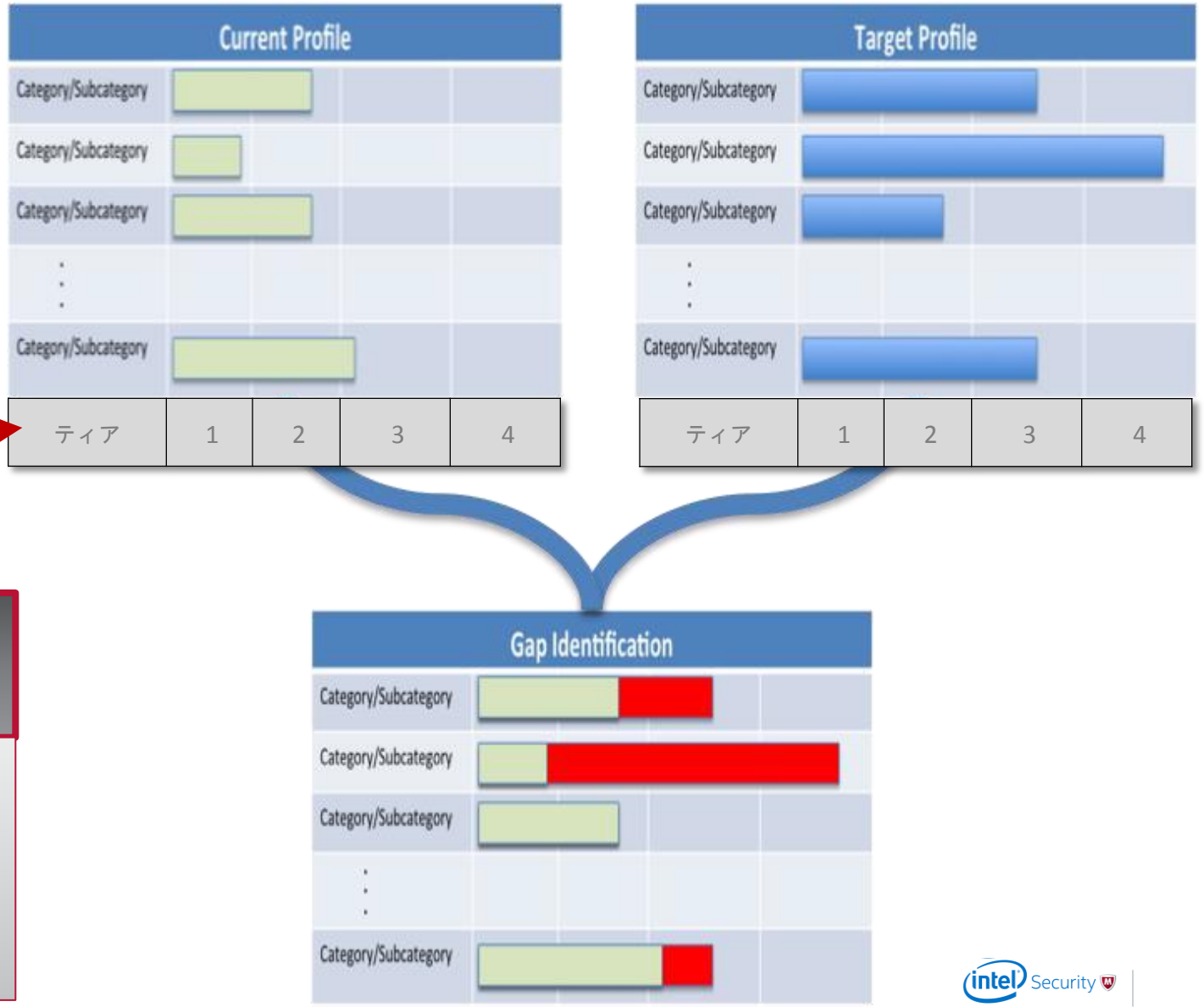
ティア

ティア3:アダプティブ
ティア2:反復可能
ティア1:十分なリスク情報
ティア0:部分的

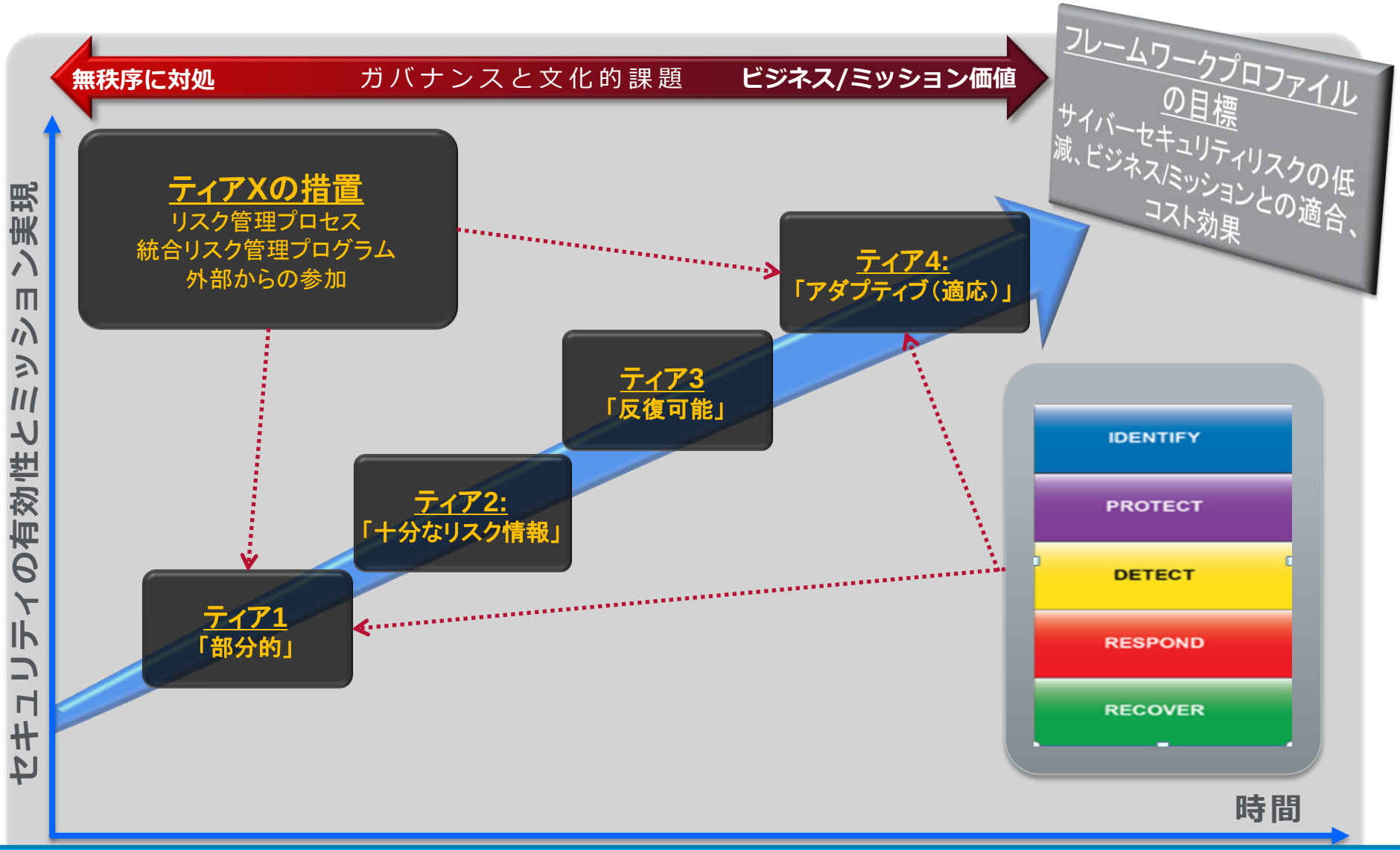
ティアと成熟度レベル

1. 組織は、必要なリスク耐性に合わせた目標成熟度レベルを設定する
2. 組織は、目標に対して管理度を確認し、ギャップ(差異)を評価する

参考. NIST Framework プロファイルの比較



参考. NIST Framework の自発的改善モデル



セキュリティリスクを管理しつつ、
自発的に改善プログラムを実行するフレームワーク