ERABビジネスに求められるセキュリティ：IECと日本の事例

2026年3月

IECシステム委員会コンビーナ(スマートエネルギー・ERAB担当)
慶應義塾大学グローバルリサーチインスティチュート特任教授
前橋国際大学客員教授

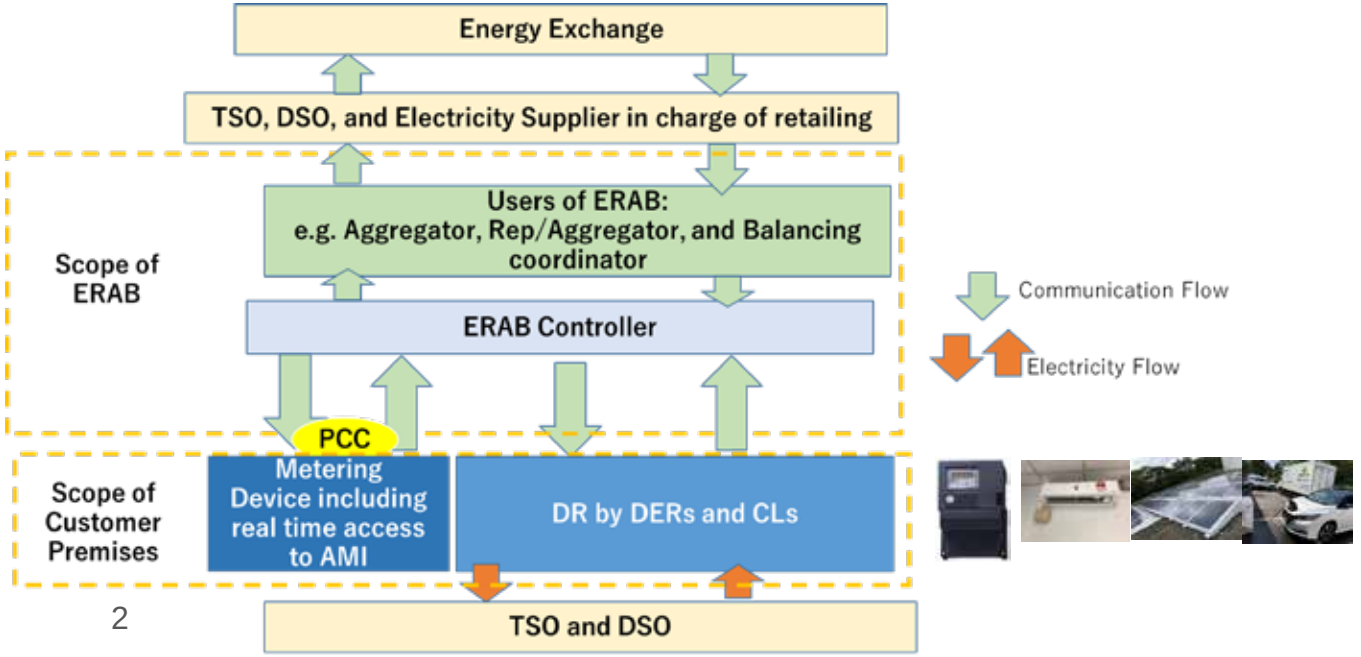
梅嶋真樹

International Electrotechnical Commission

A new international standard in 2026: Energy Resource Aggregation Business (ERAB)

IEC SRD63443 ED1: Distributed Energy Resource Aggregation Business System: Part1 Architecture and Service scenario

- **2026年2月、IECシステム委員会スマートエネルギー(SyC SE)が中心となって、日本におけるERAB(オープンな通信規格を持つ分散電源の遠隔制御とそのふるまいをスマートメーターデータを用いて監視する新たなスマートエネルギーモデル）に関する検討、それらERABのアグリゲーターによる多数の実装、資源エネルギー庁によるエネルギー･リソース･アグリゲーション･ビジネスに関するガイドライン、次世代スマートメーター制度検討会とりまとめ等の出版物を出自として、ERABのユースケースのIECにおける国際規格化(SRD)を実現。**
  - ERAB is to restrain or elevate the power generation of Distributed Energy Resources (DERs) and power demands of Controllable Loads (CLs) at customer premises in accordance with the performance measurement by the metering device at the Point of Common Coupling (PCC), allowing real time data access from customer premises and the request of the Transmission Service Operator (TSO), Distribution System Operator (DSO), Electricity Supplier, and Energy Exchange.
- Status: IEC released ERAB as the new international standard in February 2026.
  - https://webstore.iec.ch/en/publication/72787

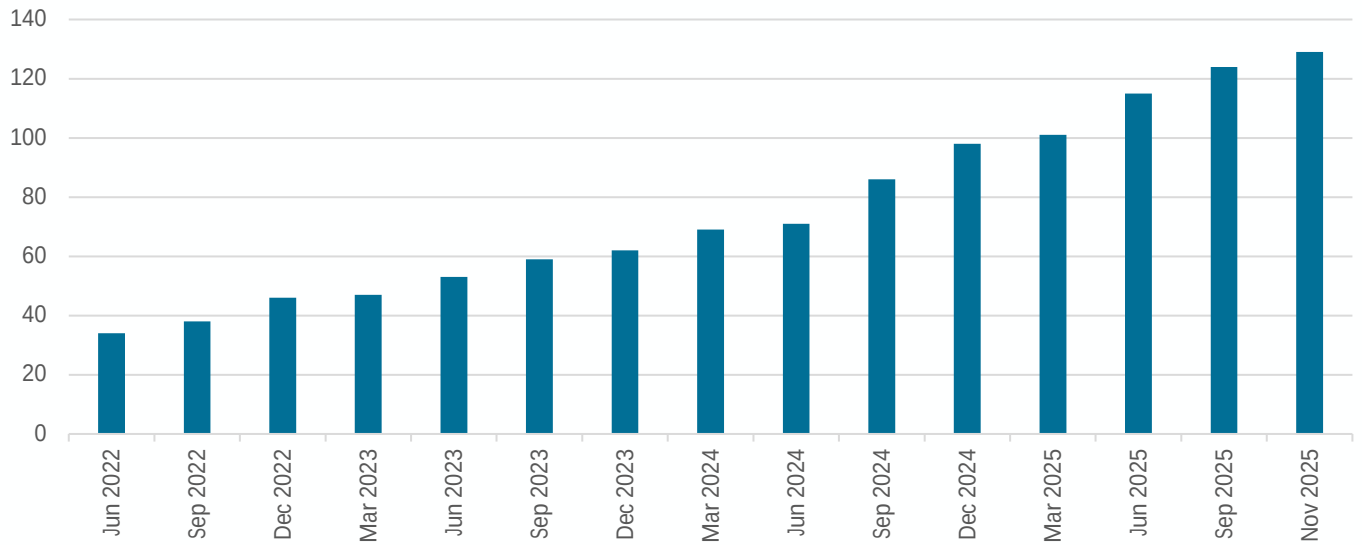


2

Status of ERAB in Japan

- As of Nov 11, 2025, there are **129 companies** have been accepted as an **Energy Resource Aggregator**, and the number continues to increase year by year.
- There are wide range of industries — such as **manufacturers, telecommunications, trading companies, oil, and gas.**
- Some companies have emerged within the electricity sector whose primary business is aggregation.

Number of energy resource aggregators (cumulative)

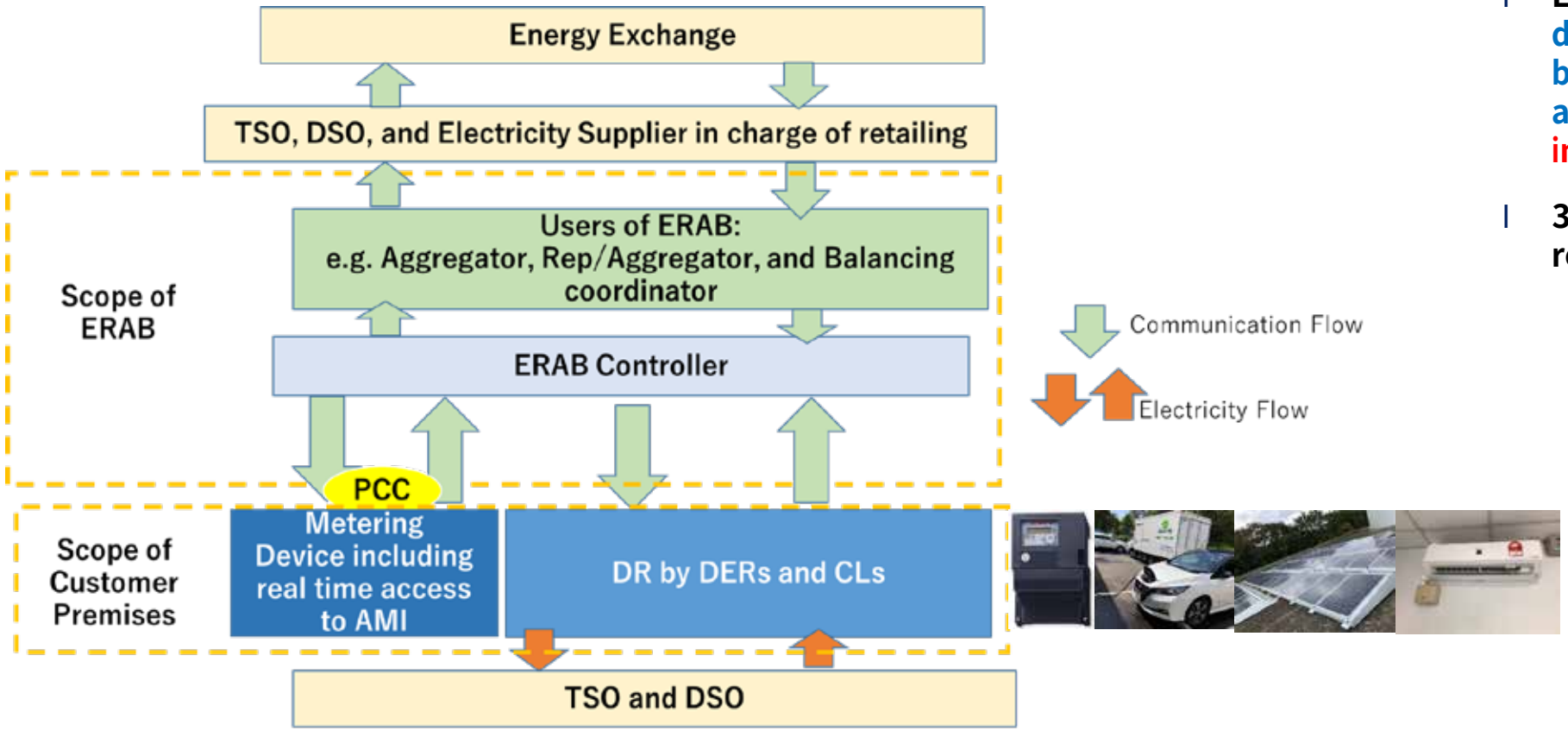


Source: Agency for Natural Resources and Energy in Japan(2026) Energy Resource Aggregation Business and Cyber Physical System Security -Recent Progress-

A new international standard in 2026: Energy Resource Aggregation Business (ERAB)

SRD63443 ED1: Distributed Energy Resource Aggregation Business System: Architecture and Service scenario

- IEC defined ERAB as: ERAB is to restrain or elevate the power generation of Distributed Energy Resources (DERs) and power demands of Controllable Loads (CLs) at customer premises in accordance with the performance measurement by the metering device at the Point of Common Coupling (PCC), allowing real time data access from customer premises and the request of the Transmission Service Operator (TSO), Distribution System Operator (DSO), Electricity Supplier, and Energy Exchange.
- Status: IEC released ERAB as the new international standard in February 2026.
- https://webstore.iec.ch/en/publication/72787



- **ERAB restrain or elevate the demand according to the request by retailers and a grid distributor and provide the electricity traded in a market.**
- **3 key necessary conditions for realizing ERAB:**
  1. **Interoperability of communication between DERs and CLs**
  2. **Transparency in a performance measurement when configuring DERs and CLs**
  3. **Security as cyber and physical system**

1. Interoperability of communication between DERs and CLs: Data interoperability in-between DERs

- Examples of ECHONET Lite: DERs and a smart meter speak the same language certified by IEC 14543-4-3(ECHONET Lite). ECHONET Lite has provided a common language for 100s of devices: home appliances, power meter, EV, and PV
  - ECHONET Lite middleware: ISO/IEC 14543-4-3
  - Detailed Requirements for ECHONET Device Objects: IEC 62394

Protocol stack for DERs and power meter with ECHONET Lite

Application layer	ECHONET Lite (application) ISO/IEC 14543-4-3
Transport layer	UDP
Network layer	IPv6
(Adaptation layer)	(6LoWPAN*1)
MAC layer	(No specific MAC layer assumed)
PHY layer	(No specific PHY layer assumed)

*1) Depends on transmission media

Other protocol examples for DERs and CLs

- Matter will enable communication across smart home devices, mobile app, and cloud services, and define a specific set of IP-based networking technologies for device certification.
- CSA in charge of Matter is the standard body for inter-connected devices created by the formerly Zigbee alliance. The membership has covered with: Amazon, Apple, COMCAST, Google, Huawei, IKEA, and so on

- **Japanese Government and Industry liaison has proposed ISO/IEC14543-4-3, to be the enabler of the demand side management, around HEMS. Internet of Things over this international standard, ECHONET Lite in Japan, has provided a common language for 100s of devices: home appliances, power meter, EV, and PV.**

- EEBUS is the euroa based protocol suite for the Internet of things that aims to standardize the interface between electrical consumers, producers, storages, and managing entities. EEBUS describes the data models necessary for the technical implementation of a use case complying with Smart Premise Interoperable Neutral Message Exchange (SPINE).

ECNONET Lite with IEC standards

ECHONET Consortium is an institution which promotes the IEC14543-4-3 protocol called “ECHONET Lite” for home appliances and DERs. The consortium is in charge of a protocol design and a test procedure ensuring interoperability

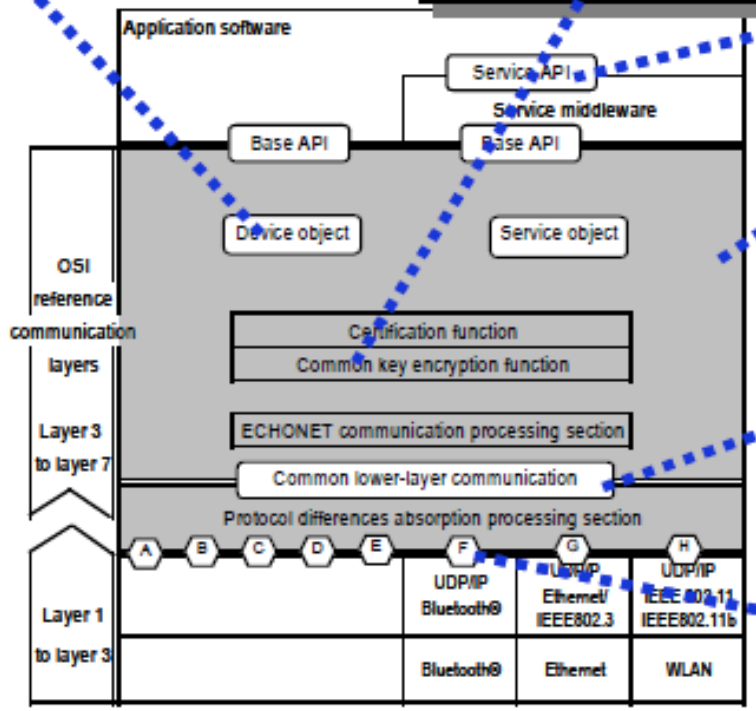
Keep Updating Device Objects

ECHONET device object
Interface for equipment maintenance
IEC TC100
Reference No. IEC62394
Published: 2006/6

Secure communication layer
Secure communication for home appliances
ISO/IEC JTC 1/SC 25/WG 1
Reference No. ISO/IEC24767-1
ISO/IEC24767-2
Published: 2008/9

Middleware adapter interface
IEC TC100
Reference No. IEC62480
Published: 2008/5

ISO/IEC14543-4-3 is for ECHONETLite



ECHONET communication middleware - upper section
ISO/IEC JTC 1/SC 25/WG 1
Reference No. ISO/IEC14543-4-1
Published: 2008/5

ECHONET communication middleware - lower section
ISO/IEC JTC 1/SC 25/WG 1
Reference No. ISO/IEC14543-4-2
Published: 2008/5

Application of TCP/IP™ to home network - cooperation with AV/PC equipment
IEC TC100
Reference No. IEC62457
Published: 2007/9

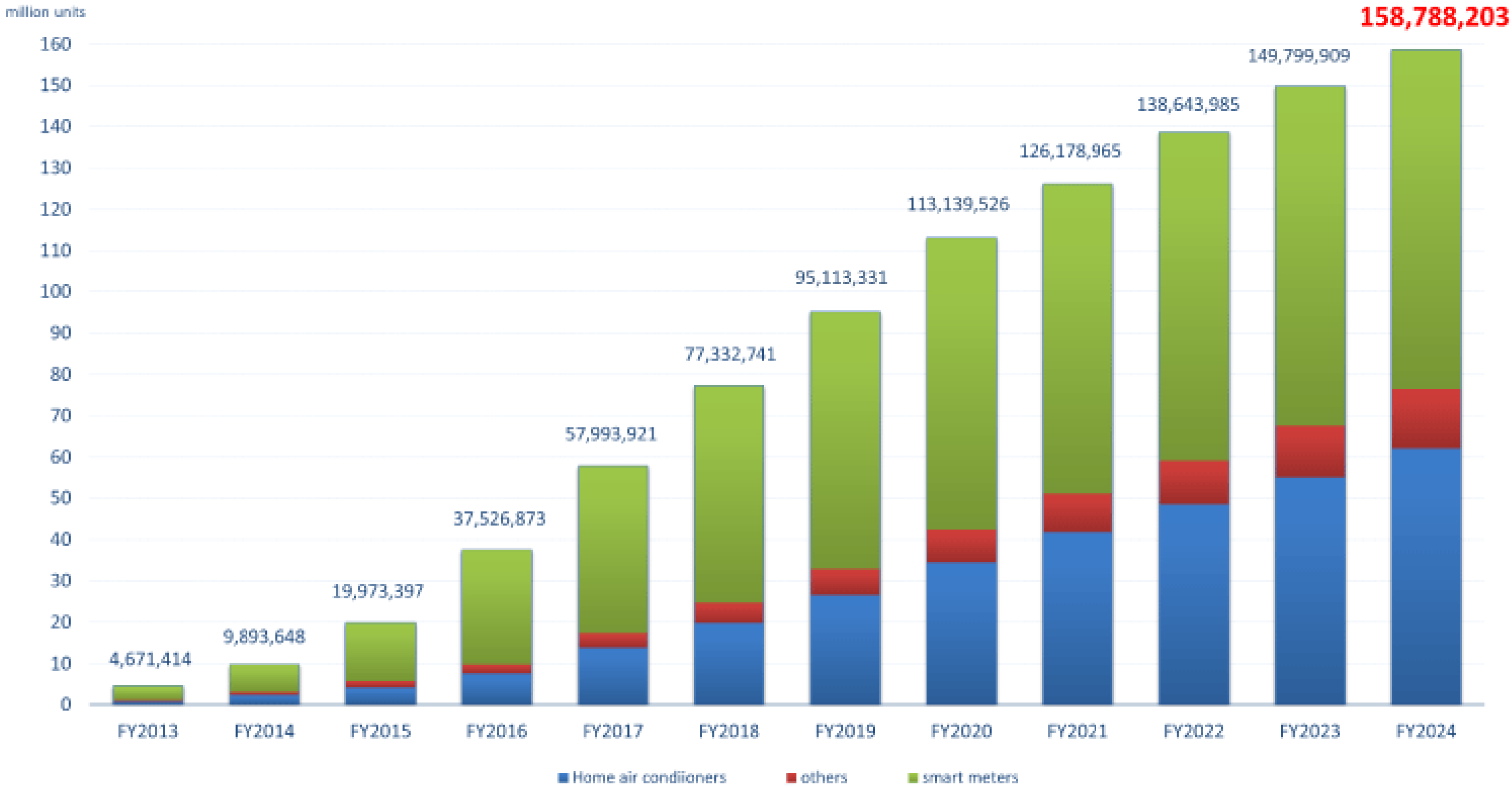
Managing Members

SHARP
TEPCO
TOSHIBA
Leading Innovation
Panasonic
MITSUBISHI ELECTRIC
Changes for the Better

Other member companies

- Tokyo GAS, OSAKA GAS
- Toyota, Denso
- Hitachi, INTEC
- Hokuriku Electric, Chubu Electric, Kansai Electric, Kyushu Electrric
- SolaX Power in China
- SUNGROW in Germany
- Tuv Rheinland in Germany

ECHONET Lite devices: Approx. 160 millions in 2024



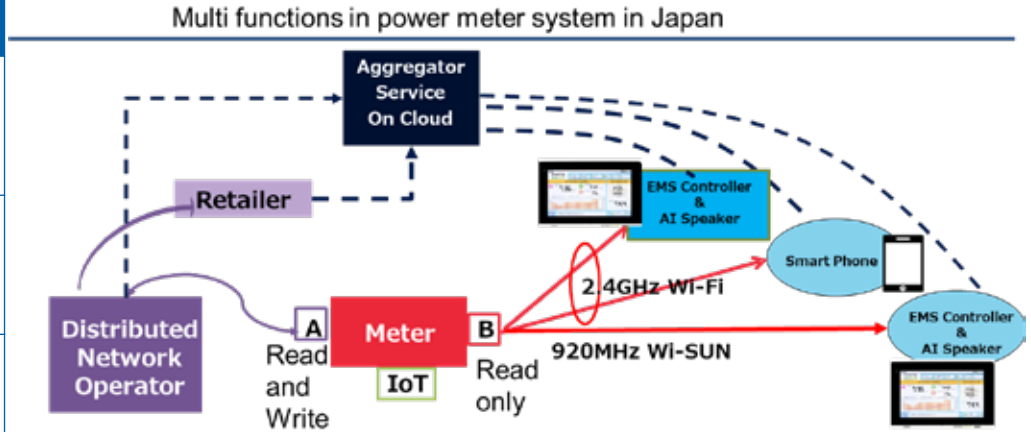
2. Transparency in measurement of performance of flexibility service.

次世代スマートメーター。全国すべての家庭と事業所に導入(2026年～)

Evaluation patterns of ERAB at PCC

Item			Abstract
Evaluation	Measurement item	Location	Measurement location to evaluate the amount of balancing power generation with DR
		Frequency	Measurement interval to evaluate the amount of balancing power generation with DR
	Criteria	Response quality shown in kW	Evaluation of capability of balancing power generation value (kW) according to the command value.
		Quantity of controlling power shown in kWh	Evaluation of capability of balancing power generation value (kW)
	Time	Timing	Time subject to response evaluation and controlled amount evaluation.
Rewards/Penalty			Reward to be paid in response to the amount of electricity provided (kWh) and a pre-shared kW target. Also, a penalty for failing to meet the DR contract requirements

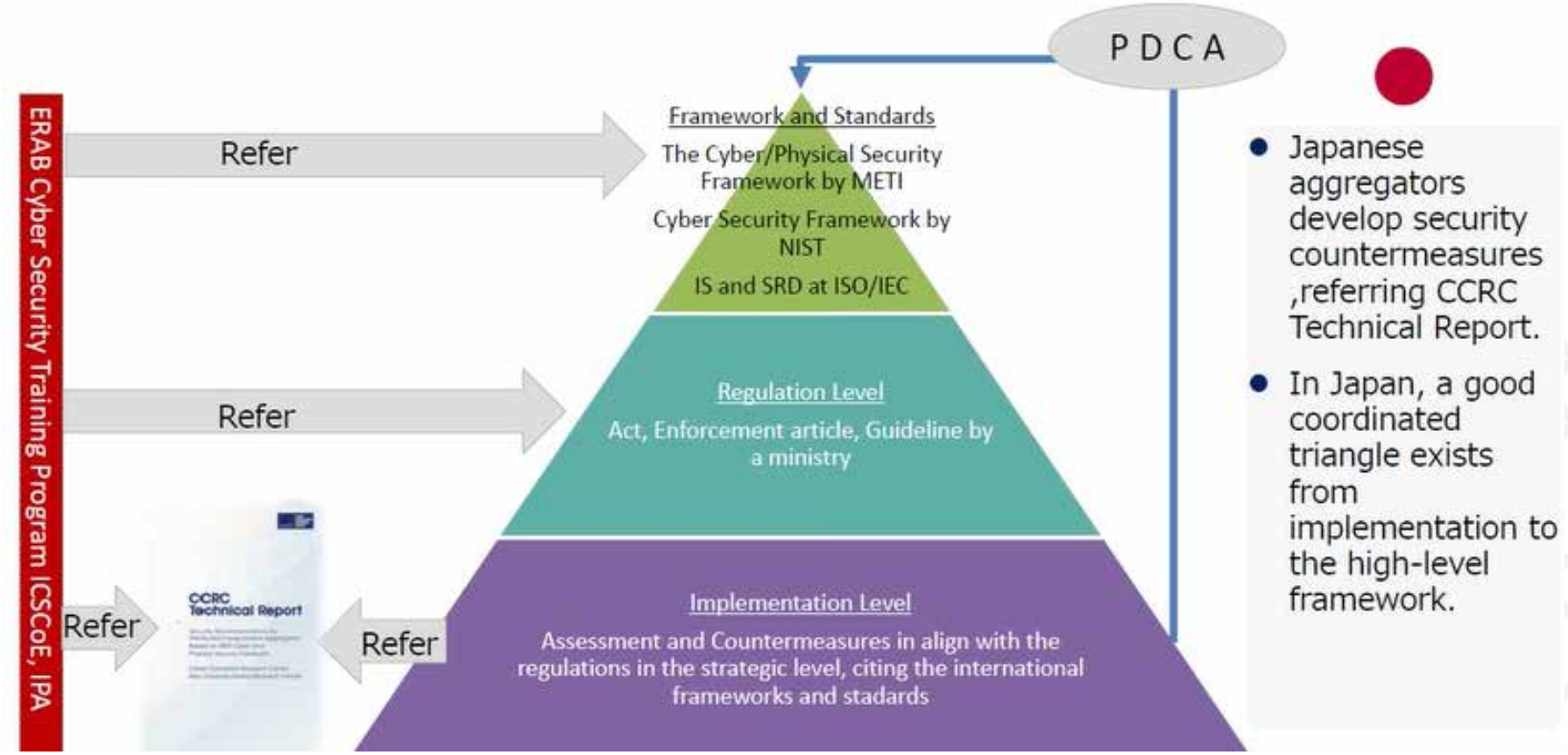
Implementation in Japan



3. Security as cyber and physical system

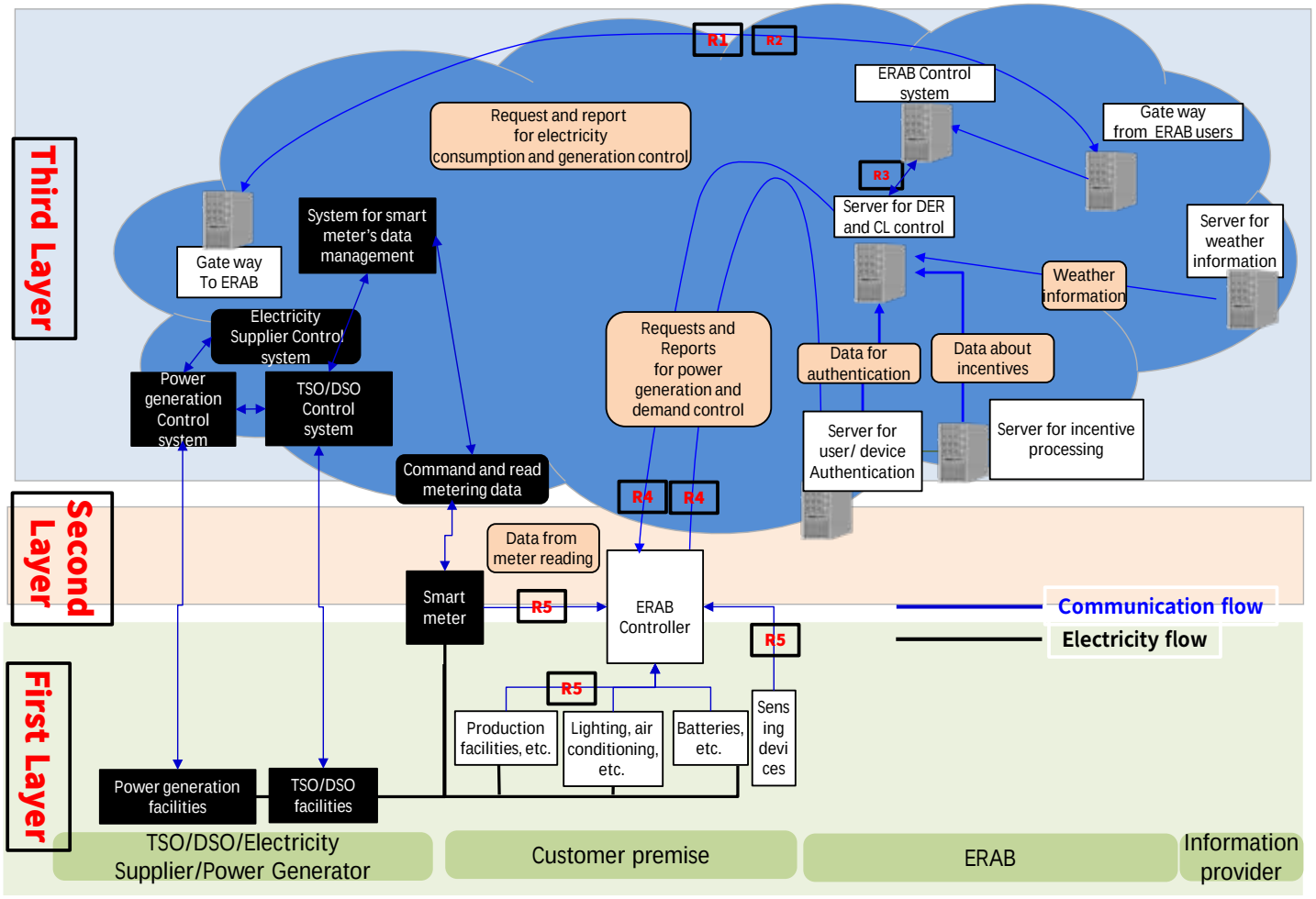
The security triangle for ERAB which is the energy IoT system

- Japan has established a highly advanced cybersecurity framework for the power sector that, while not fully prescriptive in law, functions as a leading industry benchmark and drives strong voluntary compliance. The national framework, guided by METI's Cyber-Physical Security Framework (CPSF), is aligned closely by U.S. standards such as NIST and internationally recognised ISO/IEC standards, enabling utilities and industry participants to operate under globally robust and trusted security practices following Japan's model.



3. Security as cyber and physical system

The project to create the IEC security standard on Energy Resource Aggregation Business (ERAB)
TS 63443-2 ED1: Distributed Energy Resource Aggregation Business System-PART2: Risk assessment and treatment



- The scope of this document is to show the process of risk assessment which is consisted of risk identification, risk analysis, and risk evaluation, causing the risk treatment of the example of risk assessment and treatment on Distributed Energy Resource Aggregation Business (ERAB)
- Status: ACD
- Note1: ERAB case is compatible with the BUC format shown by IEC 62559-2:2015 and SMART GRID STANDARDIZATION ROADMAP by IEC TR 63097:2017
- Note2: ERAB is defined as SRD63443-1

Map of guidelines(as of December10,2025)

🔴 Mandatory, 🟠 Voluntary (reference for national standards), 🟢 Voluntary (general best practices/guidelines)

	Region	Regulations	Standards/guidelines with enforcement	Guidelines
Power Grid	USA	🔴 **Acts:** establish legal rules for interstate electricity markets, transmission access and competition. 🔴 **FERC Orders:** convert federal laws into rules for market, transmission and interconnection.	🔴 **NERC Reliability Standards:** mandatory grid-operation rules across 14 themes. 🟠 **IEEE:** US engineering standards referenced for power-system, communication and digital technologies.	🟢 **EPRI:** provide insights and recommendations for emerging grid and DER opportunities. 🟢 **NERC Reliability Guidelines:** best-practice support for power-grid operations. 🟢 **DOE Modern Distribution Grid Report:** three-volume guidance for consistent distribution-grid modernization and investment planning.
		🔴 **EU Commission Regulations:** EU harmonized rules governing grid connection, smart grid, operations and market functions.	🔴 **EU Articles/Standards under EU Commission Regulations:** Binding technical and smart-grid requirements defined within the Regulations.	🟢 **ENISA Recommendations, Best Practices, Implementation Guidelines and System Reports:** ENISA voluntary practices supporting NIS2 and ICS/SCADA cybersecurity.
		🔴 **National Electricity Law (NEL) and National Electricity Retail Law (NERL):** NEL & NERL set market and retail legal frameworks.	🔴 **National Electricity Rules (NER):** legally enforceable and makes referenced AS/NZS standards mandatory for market participants and networks. 🔴 **AS/NZS & AS Standards:** compulsory when referenced by NER or safety laws; otherwise function as voluntary technical references adapting IEC/ISO to local conditions.	🟢 **National DER Grid Connection Guidelines (Energy Networks Australia):** framework to standardize and streamline small-scale DER connection requirements for DNSPs.
Cybersecurity		🔴 **FPA:** enables FERC to enforce cybersecurity and reliability rules via NERC standards. 🔴 **CISA Act 2018:** designates CISA as the federal lead for cybersecurity and CII coordination. 🔴 **CIRCIA 2022:** requires CII entities to report cyber incidents to CISA.	🔴 **NERC Reliability Standards:** Contains Cybersecurity Standards under "Critical Infrastructure Protection"	🔴 **NIST – Federal Information Processing Standards:** federal cryptographic and information-security standards, FIPS binding only for federal entities. 🟢 **NIST:** risk-management and interoperability guidance widely used by utilities. 🟢 **DOE C2M2 Model:** maturity model for evaluating and improving ICS/OT CS. 🟢 **CISA Best Practices**: guidance for segmentation, hardening, and incident response. 🟢 **NERC Security Guidelines:** practices that supplement CIP standards.
		🔴 **Network Code on Cybersecurity 2024:** mandates cybersecurity rules for cross-border electricity flows.	🔴 **EU Articles/Standards for Cybersecurity:** include binding cybersecurity requirements for risk, certification and monitoring.	🟢 **Council of European Energy Regulators (CEER) Guidelines:** recommendations for consistent cybersecurity practices across electricity and gas networks. 🟢 **TF TYNDP – Good Practices:** voluntary grid-planning and investment guidance for DSOs to support secure and modern distribution networks.
		🔴 **Security of Critical Infrastructure Act (SOCI, 2018):** mandates cyber-incident reporting and baseline security obligations for electricity operators. 🔴 **CIRMP Rules (2023):** require CII entities to maintain structured cyber-risk management.	🟢 **AS IEC 62443 series**: Australian adoption of IEC 62443, covers OT/ICS lifecycle security	🔴 **ASD Essential Eight + Essential Eight Maturity Model + Information Security Manual (ISM):** core ASD cybersecurity framework mandatory for Australian Government agencies but voluntary for IT/OT controls and maturity by other sectors. 🟢 **AESCSF – Australian Energy Sector Cyber Security Framework (AEMO / DCCEEW):** sector-specific maturity framework for electricity, gas and liquid fuels, used to benchmark capability and support SOCI/CIRMP obligations.
Cross Cutting			🟠 **ISO:** international management and process standards for quality and security. 🟠 **IEC:** global technical and safety standards for electrical and electronic systems.	

- **Note: The European commission has Working Group Cybersecurity at Smart Energy Expert Group (SEEG) with the leadership by CNECT(DG Communications Networks, Content and Technology) and ENER(DG Energy). European Committee for Electrotechnical Standardization (CENELEC) is the member.**
- **IEEE has published the Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems(1547.3:2023)**

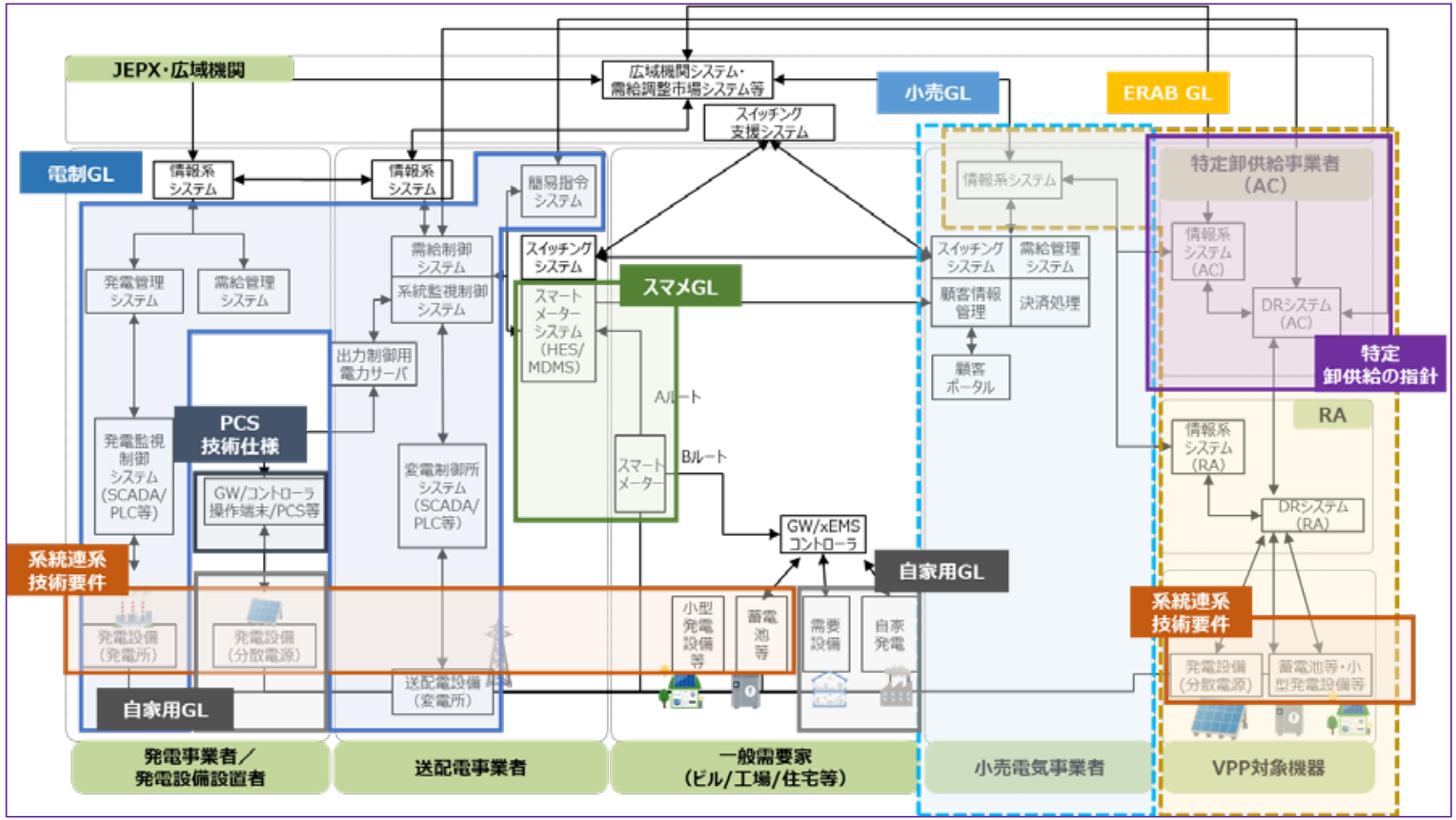
Definitions: 1) Regulations: Legally binding rules issued under statutory authority; mandatory, **2) Standards:** Technical requirements. Mandatory only when adopted by a regulator; otherwise voluntary, **3) Guidelines:** Usually non-binding best practices; advisory only.

Source: : The ERIA study group on the cyber and physical system security of DERs and NRI Singapore(2025)Government Sources, News Releases

国の電力分野におけるサイバーセキュリティ要件

- 電力システムの各事業者は、IEC規格、NIST-CSF、経産省-CPSF(サイバーフィジカルセキュリティ対策フレームワーク)、IPA制御システムのセキュリティリスク分析ガイド等を参考にし、PDCAを回すことが求められる。
- そのうえで、各国政府がガイドラインによって、標準的なセキュリティ要件を定める。強制力はガイドラインによる。

＜電力システムのサイバーセキュリティ関するガイドライン等の適用範囲＞



引用：令和４年度 エネルギー需給構造高度化対策に関する調査等事業 （電力分野のサイバーセキュリティ対策のあり方に関する詳細調査分析）報告書(2023年2月28日) より一部抜粋
※実線は義務、点線は推奨として位置づけられているガイドライン等を意味する。なお、 本図は各ガイドライン等の対象を明確化するために作成したものであり、実際の電力システムを精緻に整理したものではない。

3. Security as cyber and physical system

The security triangle of Energy Resource Aggregation Business(ERAB)

ERAB Cyber Security Training Program ICSCoE, IPA

PDCA

Refer

Refer

Refer

Refer

Framework and Standards

The Cyber/Physical Security Framework by METI

Cyber Security Framework by NIST

IS and SRD at ISO/IEC

Regulation Level

Act, Enforcement article, Guideline by a ministry

Implementation Level

Assessment and Countermeasures in align with the regulations in the strategic level, citing the international frameworks and stadards

- **Japanese aggregators develop security countermeasures ,referring CCRC Technical Report.**
- **In Japan, a good coordinated triangle exists from implementation to the high-level framework.**

サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）~ 三層構造と６つの構成要素～

- 従来のサプライチェーンでは、セキュリティ対応をしっかりと行った主体間で行われる取引であれば、そのプロセス全体のセキュリティが確保される。
- 一方、「Society5.0」では、従来のサプライチェーンのように、**組織のマネジメントの信頼性にのみ基点を置くことでバリュークリエイションプロセスの信頼性を確保することは困難。**
- こうした、従来のサプライチェーンの活動範囲から拡張された付加価値を創造する活動のセキュリティ上のリスク源を的確に洗い出し、対処方針を示すためのモデルが必要。

三層構造モデル

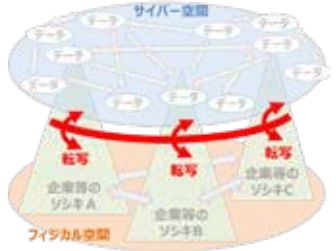
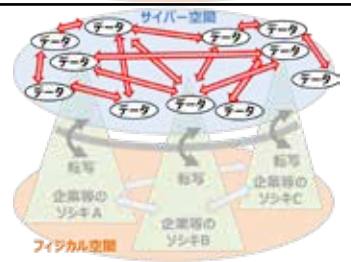
バリュークリエイションプロセスが発生する産業社会を、３つの「層」で整理。

第1層：企業間のつながり
第2層：フィジカル空間とサイバー空間のつながり
第3層：サイバー空間におけるつながり

６つの構成要素

バリュークリエイションプロセスに関与する構成要素を６つに整理。

ソシキ、ヒト、モノ、データ、プロシージャ、システム

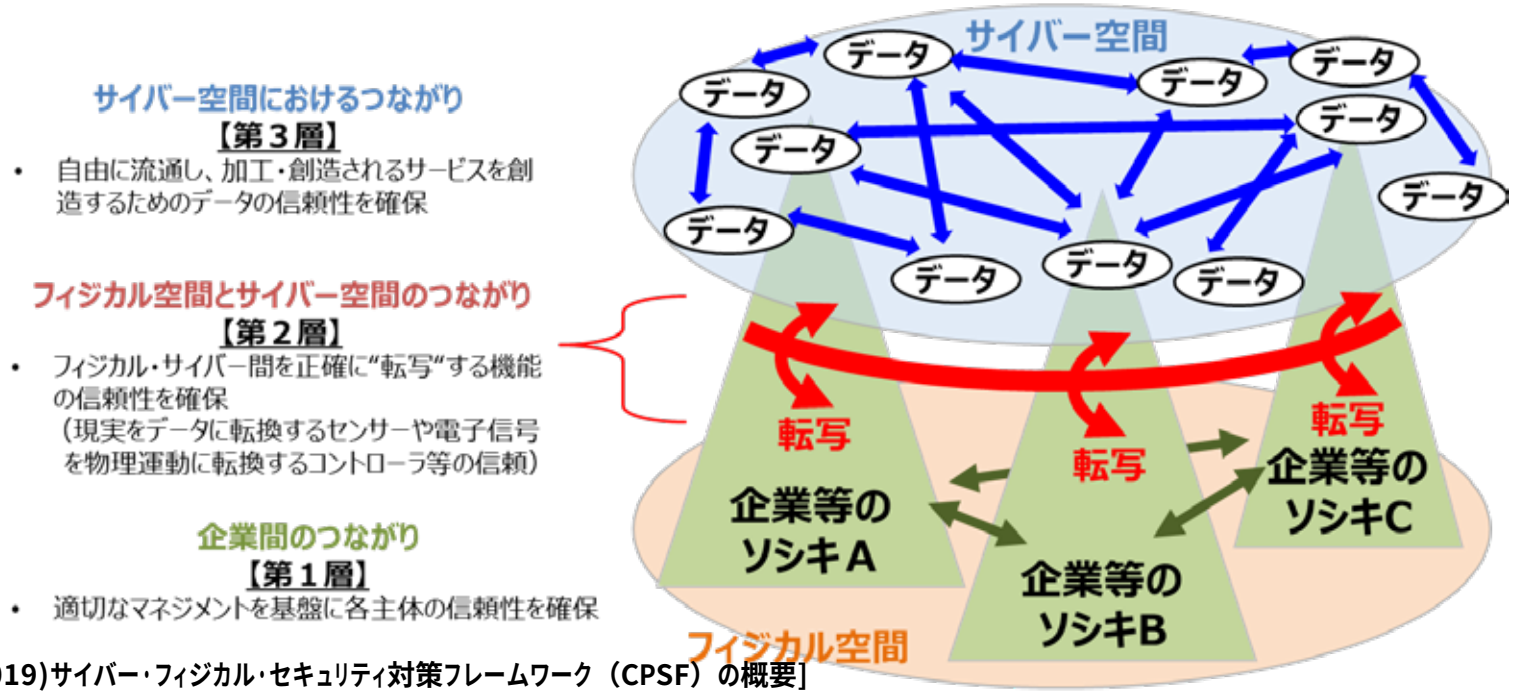
三層構造	概念図
第1層	
第2層	
第3層	

引用:経済産業省(2019)サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の概要]

三層構造アプローチの意義

~ バリュークリエイションプロセスのセキュリティを確保するための**信頼性の基点の設定**～

- **三層構造モデル**では、『Society5.0』における新たなサプライチェーン、**バリュークリエーションプロセスの信頼性の基点を的確に設定するために、産業社会を３つの「層」で整理**。
- 各層における信頼性の基点は以下のとおり。
  - **第１層**では、企業間のつながりにおける、**企業（組織）のマネジメントの信頼性**
  - **第２層**では、サイバー空間とフィジカル空間のつながりにおける、**要求される情報の正確性に応じて適切な正確さで情報が変換される“転写”機能の信頼性**
  - **第３層**では、サイバー空間のつながりにおける、**データの信頼性**



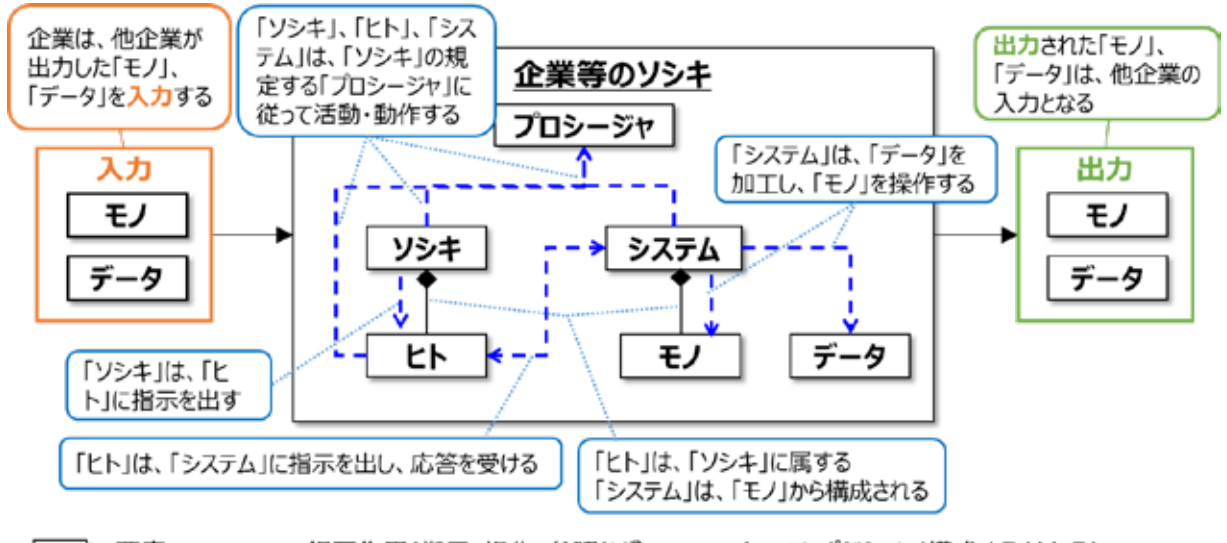
引用:経済産業省(2019)サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の概要]

６つの構成要素

~ 動的で柔軟なバリュークリエイションプロセスを捉えるための構成要素～

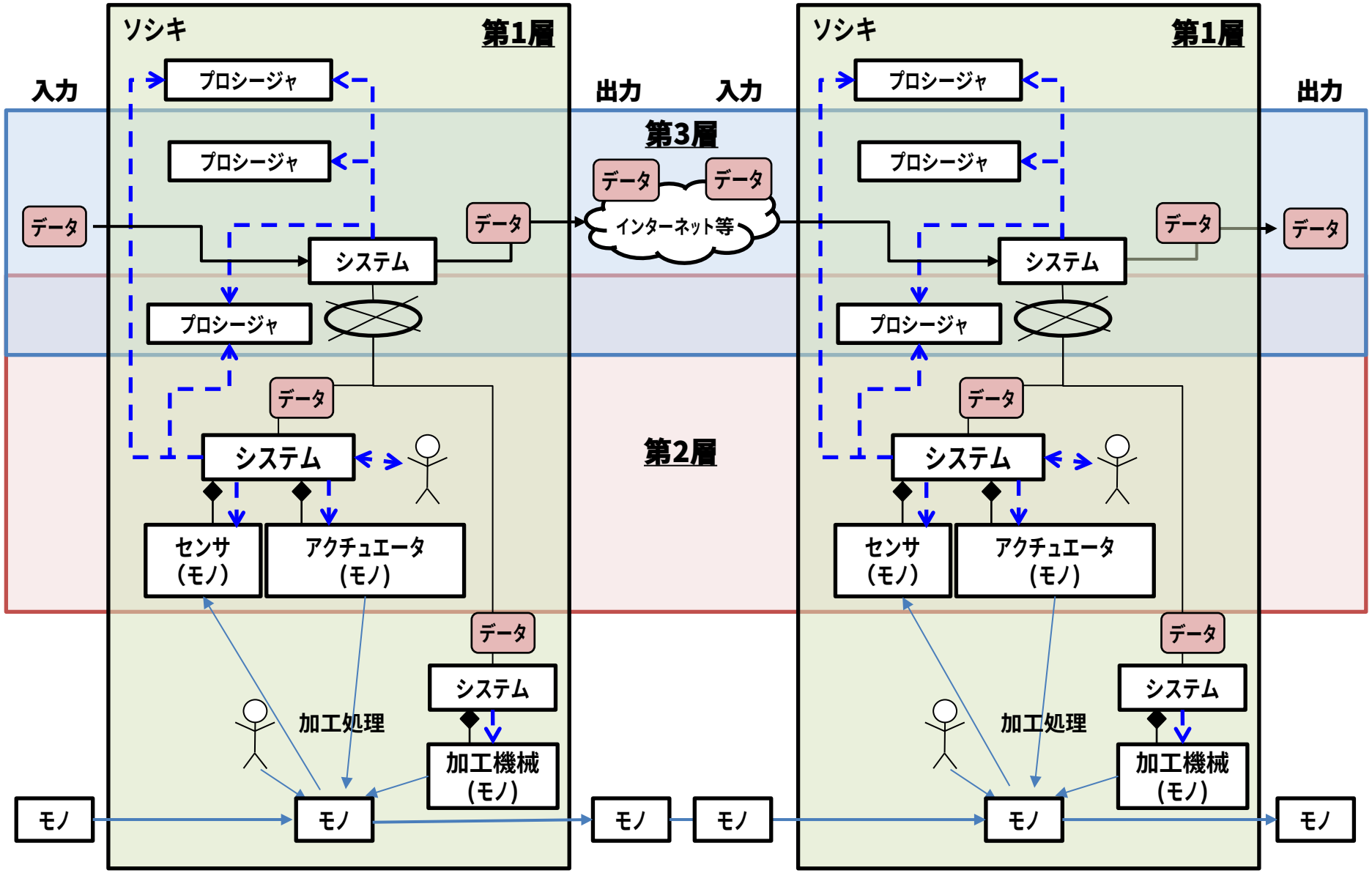
- バリュークリエイションプロセスは、**動的に柔軟に構成されることから、資産を固定的に捉えることが難しく、構成要素について一定の抽象化を行って捉えることが必要。**
- **このため、セキュリティ対策を講じる上で最適な最小単位として、６つの構成要素で整理。**

構成要素	定義	構成要素	定義
ソシキ	• バリュークリエイションプロセスに参加する企業・団体・組織	データ	• フィジカル空間にて収集された情報及び共有・分析・シミュレーションを通じて加工された情報
ヒト	• ソシキに属する人、及びバリュークリエイションプロセスに直接参加する人	プロシージャ	• 定義された目的を達成するための一連の活動の手続き
モノ	• ハードウェア、ソフトウェア及びそれらの部品操作する機器を含む	システム	• 目的を実現するためにモノで構成される仕組み・インフラ



引用:経済産業省(2019)サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の概要]

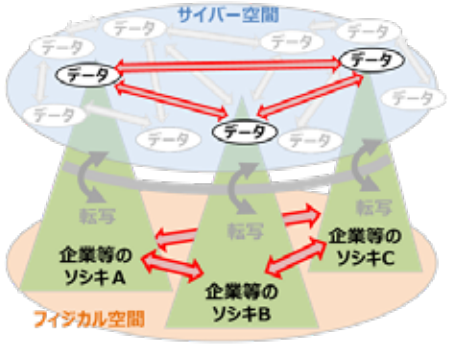
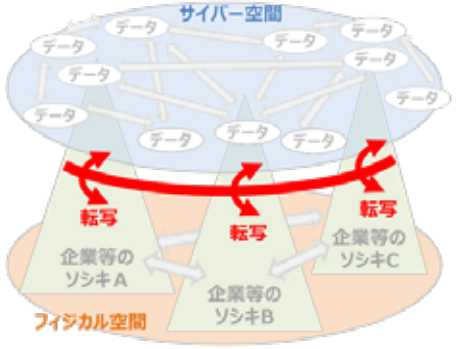
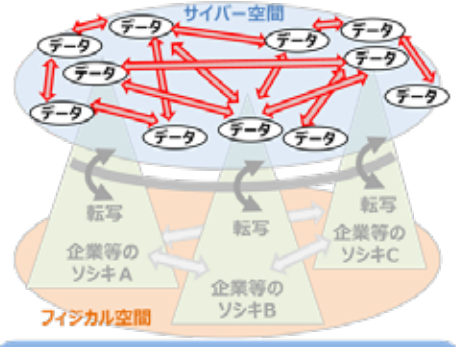
（参考）三層構造における6つの構成要素の関係



引用:経済産業省(2019)サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の概要]

CPSFの全体概要（リスク源と対応する方針の整理）

- 各層における機能、セキュリティインシデント、リスク源、対策要件を整理。

	企業間のつながり【第１層】	フィジカル空間とサイバー空間のつながり【第２層】	サイバー空間におけるつながり【第３層】
新たなサプライチェーン構造の整理			
機能（守るべきもの）	• 平時及び緊急時のリスク管理・対応体制の構築と運用 • 企業内及び企業間のリスク管理・対応体制の構築と運用	• フィジカル空間とサイバー空間の境界における情報の正確な転写及び正確な転写の証明	• データの加工・分析 • データの保管 • データの送受信
セキュリティインシデント	• 保護すべき資産の棄損 • 他組織のセキュリティ事象発生に起因する事業停止	• 不正確なデータの送信 • 安全に支障をきたす動作	• 保護すべきデータの漏えい • なりすまし等による不正な組織からのデータ受信
リスク源（構成要素ごとに整理）	• セキュリティリスクに対するガバナンスの欠如 • 他組織との連携状況の未把握	• 不正なIoT機器との接続 • 許容範囲外の入力データ	• 通信経路が保護されていない • 通信相手を識別していない
対策要件	■ マネジメントルールの徹底 ■ 関係者との役割分担	■ 接続相手の認証 ■ 安全なIoT機器の導入	■ 暗号化によるデータ保護 ■ データの提供者の信頼性確認

引用:経済産業省(2019)サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）の概要]

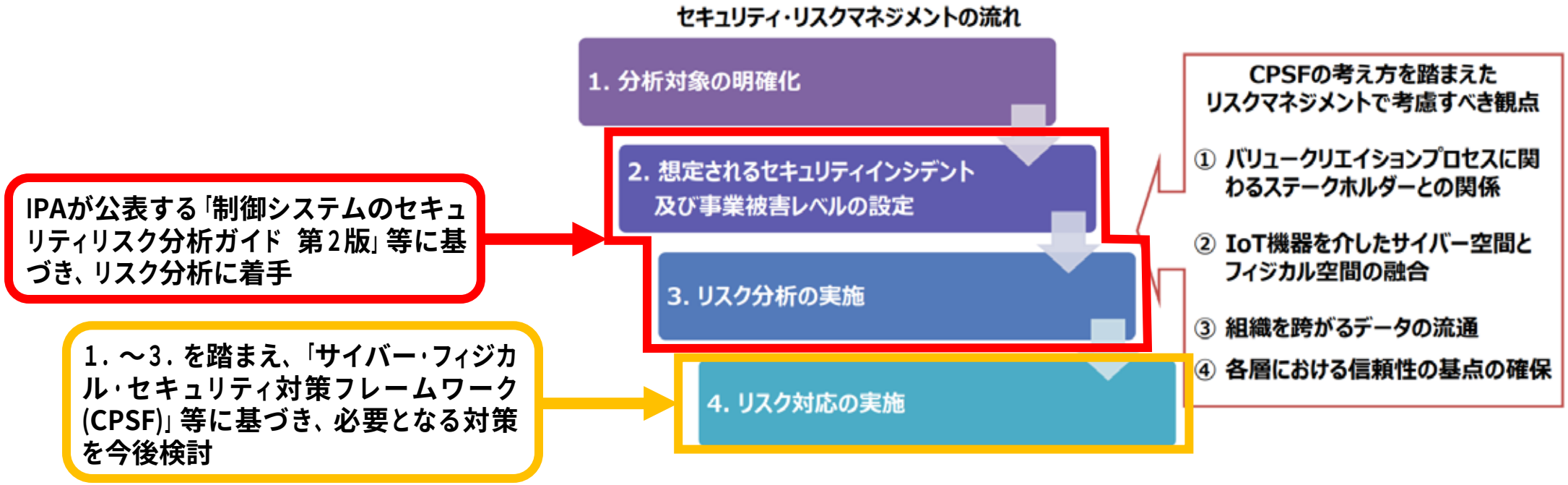
ERABサイバーセキュリティガイドラインの改定

https://www.meti.go.jp/press/2025/05/20250522001/20250522001.html

- 「制御システムのセキュリティリスク分析ガイド 第２版（2023年3月、IPA）」等に基づき、**「想定されるセキュリティインシデント及び事業被害レベルの設定」「リスク分析の実施」に着手**。

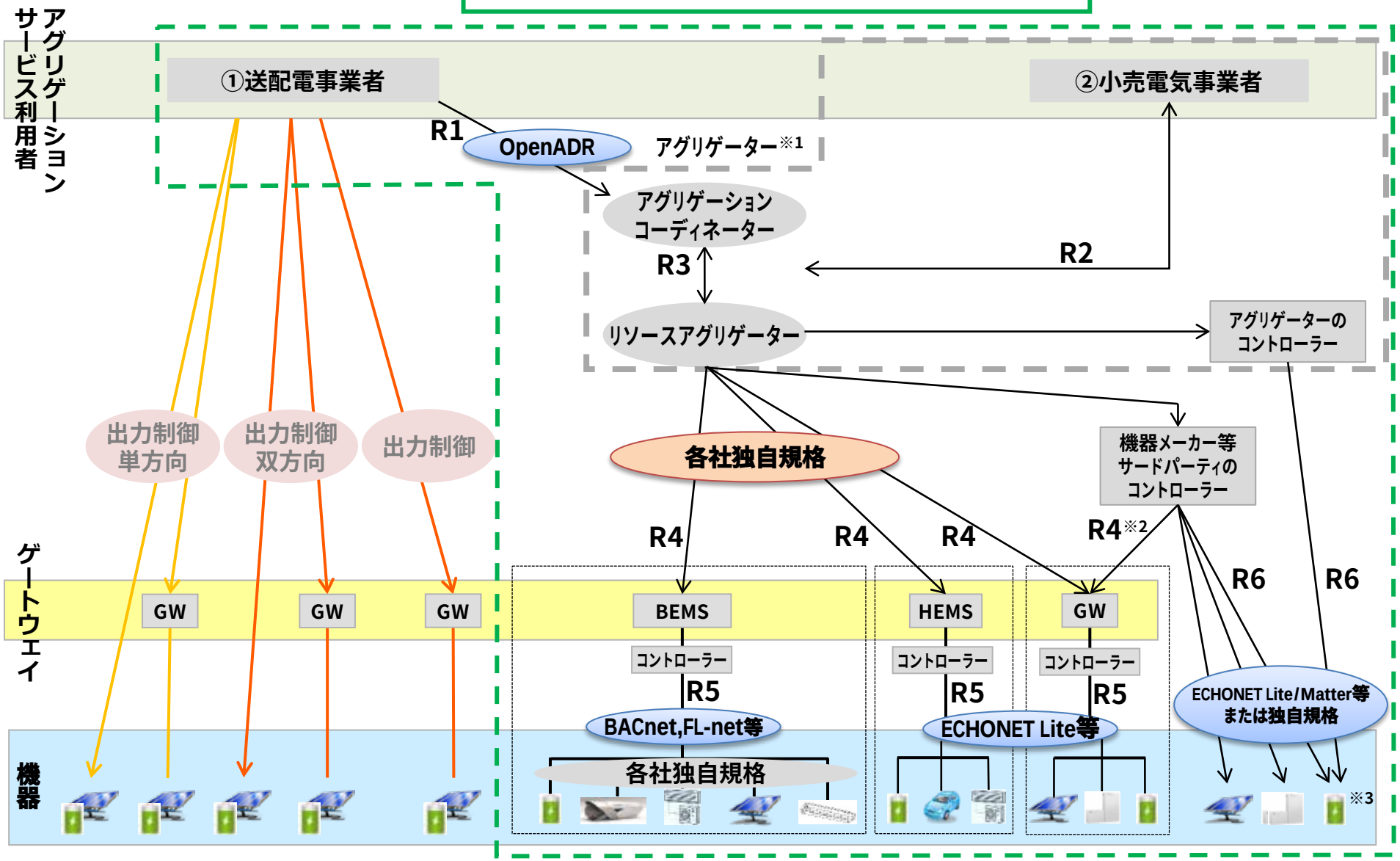
三層構造モデルを活用したリスクマネジメントの流れ

- CPSFでは、三層構造モデルに基づいてリスク源の整理と対策要件の特定を行う。CPSFは、以下のステップでのセキュリティ・リスクマネジメントを提唱。



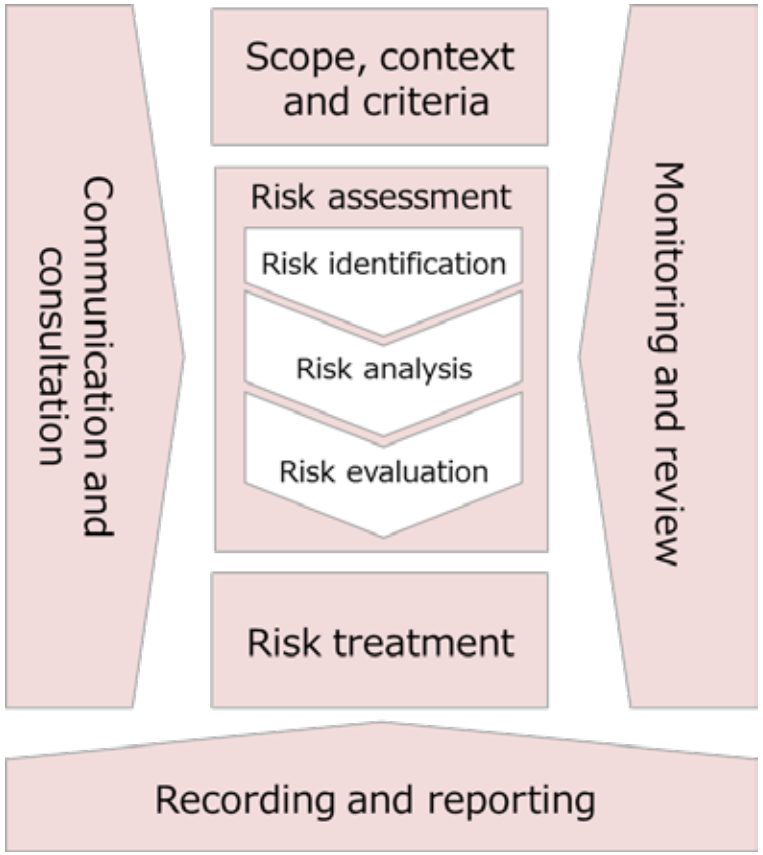
出所）経済産業省,サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）10
出どころ：ERABサイバーセキュリティトレーニング

ERABサイバーセキュリティガイドラインの検討領域

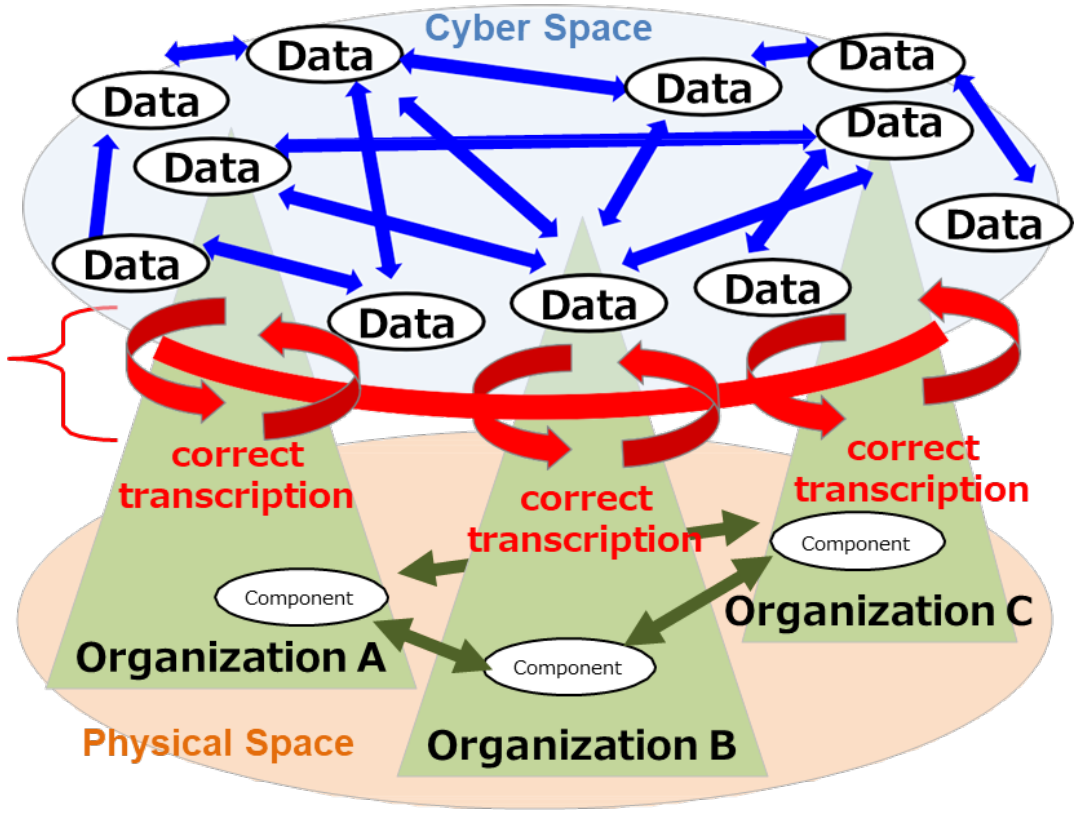


※1　アグリゲーターは役割によってアグリゲーションコーディネーターとリソースアグリゲーターに分類され、小売電気事業者が自らこの役割を担う場合も考えられる。
※2　HEMSやBEMSと連携する場合もある。
※3　単一の機器に、複数の異なる仕様のプロトコルスタックが共存する場合がある。

Security assessment of ERAB by Cyber/Physical Security Framework (CPSF) and the ISO31000 approach



Security assessment certified with ISO 31000:2018



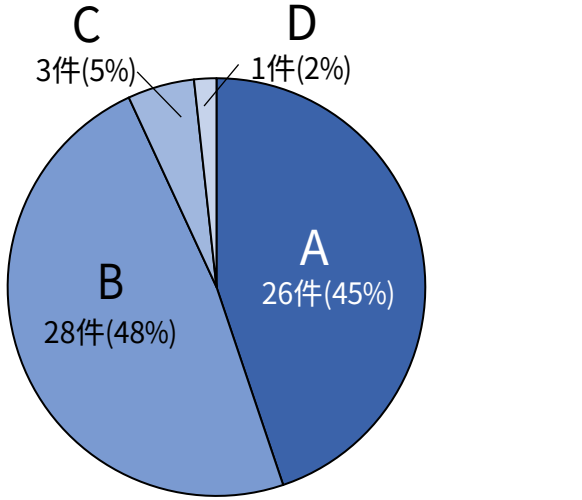
Cyber/Physical Security Framework (CPSF)

CCRCが実施した、国のERABサイバーセキュリティガイドラインの改定案作成時のアセスメント
Identification of possible threats in the ERAB system and risk assessment in 2025

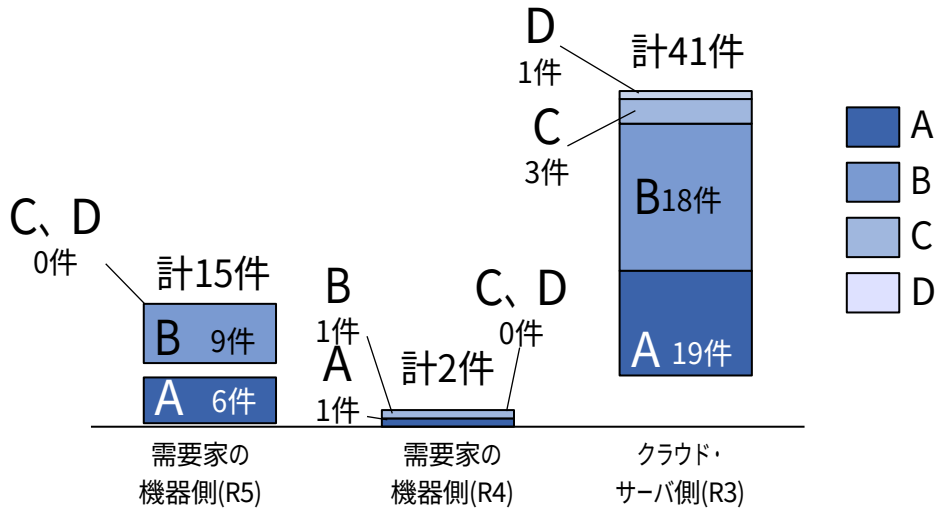
追加されたリスクシナリオ（58件）における脅威･攻撃シナリオの内訳

脅威･攻撃シナリオ	該当シナリオ数
不正アクセス	15
マルウェア感染	7
設定ミス	6
機器のなりすまし	4
DoS/DDoS攻撃	4
中間者攻撃	4
ランサムウェア感染	3
災害･障害等	3
パスワード総当たり攻撃	2
フィッシング攻撃	2
Webサイトの改ざん	2
内部者攻撃	2
セキュリティ機能の設定の不備	2
誤操作	1
機器製造時のマルウェア混入	1

追加されたリスクシナリオ（58件）におけるリスクレベル



各インターフェースにおけるリスクレベルの内訳



※A（リスクが非常に高い）～ D（リスクが低い）

引用：資源エネルギー庁 **エネルギー･リソース･アグリゲーション･ビジネスに関するサイバーセキュリティガイドラインVer3.0パブリックコメント説明資料**

ERABサイバーセキュリティガイドライン3.0改定(2025年5月)

3.6. ERABシステムにおけるサイバーセキュリティ対策【勧告】

- **Step1**：対象とする**IoT製品やサービスのシステムの全体構成及び責任分界点を明確化すること。**
- **Step2**：システムにおいて、保護すべき情報・機能・資産を明確化すること。
- **Step3**：保護すべき情報・機能・資産に対して、想定される脅威を明確化すること。
- **Step4**：システムが扱う資産ベース及び攻撃シナリオベースによるリスク分析を行うこと。
- **Step5**：脅威に対抗する対策の候補（ベストプラクティス） **を明確化すること。**
- **Step6**：どの対策を実装するか、脅威レベルや被害レベル、コスト等を考慮して選定すること。
- **Step7**：第三者による監査（認証を含む）や教育プログラム等によって**勧告指定項目を中心にその実装を検証すること。**
- **Step8**：事故発生時の対応方法を設計・運用及び訓練すること。
- **Step9**：自組織の資産の脆弱性を特定、文書化し、それをリソースアグリゲーターとの間で共有すること。

3.8. 標準対策要件に基づく詳細対策要件の設計

- **【勧告】：ERABに参画する各事業者は、実運用に耐え得るべく、標準対策要件の考え方に基づき、具体的なサイバーセキュリティ対策を自らの責任で策定すること。**

表１　標準対策要件と詳細対策要件

標準対策要件 ※本ガイドラインに相当	• 事故が起こり得ることを前提として継続的に対策を改善する必要があることを踏まえつつ、ERAB システムのセキュリティ対策に取り組むに際しての基本的な考え方、各セキュリティマネジメント要求事項を実施する目的・考え方等を規定したもの。 • ERAB システムのサービスレベルを維持するために事業者が実施すべき最低限のセキュリティ対策を規定したもの。
詳細対策要件	• ERAB に参加する各事業者が、実運用に耐え得るべく、標準対策要件の考え方に沿って行われる具体的な対策を自らの責任で規定したもの。 • 具体的には、ERAB システムの構成要素ごとに想定される脅威、当該脅威と事業リスクとの相関関係を踏まえつつ、（ｉ）抑止、（ii）内部防御・情報保護、（iii）侵入・攻撃検知、（iv）被害把握・事業継続の各フェーズにおける当該脅威に対する対策、標的型攻撃等への対策、サイバー攻撃と物理攻撃の組合せによる攻撃への対策を規定したもの。

詳細な改定内容（【追加】3.2. ERABシステムが留意すべき基本方針）

対策要件の追加が必要と考えられる理由とその対策

●追加要件が必要な理由となる脅威･リスク：【脅威･リスクIV】

Ø ERABシステムにおいて、以下の課題が見られる中、1つのシステムとしてセキュリティ確保の全体的な管理が行なわれていないため、特定のERAB制御対象のエネルギー機器等で発生したインシデントの影響が、ERABシステム全体に波及する可能性がある。

- ERABシステムを構成する各システムコンポーネントの管理主体が多岐にわたる。
- 新たに機器メーカー等のサードパーティの資産についても、ERABシステムに接続されるようになっている。
- 各システムコンポーネント間で使用されるプロトコルについて、特定の規格のプロトコルのみが採用される状況になっていない。

●全般的な対策

Ø このような状況下で、需要家を含む利用者が、アグリゲーションの制御対象リソースの管理主体となる場合も見られる中、利用者が、同リソースの脆弱性対策情報･脅威情報について何も把握していないという状況を発生させないように、情報共有体制を構築することが重要。

新しく盛り込むべき事項の方向性

3.2. ERABシステムが留意すべき基本方針

【勧告】

- ERABに参画する各事業者は、自組織の管理するERABシステムの利用者（ERAB制御対象のエネルギー機器の設置場所の需要家を含む。）へ脆弱性対策情報･脅威情報の通知を行うこと。
- ERABに参画する各事業者は、脆弱性対策情報･脅威情報の共有の取組について定め、それについて協力すること。

（以下、略）

詳細な改定内容（【追加】3.3. ERABシステムが想定すべき脅威）

対策要件の追加が必要と考えられる理由とその対策

●追加要件が必要な理由となる脅威･リスク：【脅威･リスクⅠ、Ⅱ及びⅢ】

Ø リスク評価を行った結果、不正アクセス、不正操作、機能停止、情報の窃取、情報の改ざん、プロセスの不正な実行、高負荷攻撃（バッファーオーバーフロー攻撃、DoS/DDoS攻撃）、不正送信、バックドアを悪用する攻撃、マルウェア感染、ランサムウェア感染、盗聴、異常動作（誤動作）等の危険度の高いリスクが多数存在することを確認できた。

●全般的な対策

Ø このようなさまざまなリスクを想定し、必要な対策を講じることが重要。

新しく盛り込むべき事項の方向性

3.3. ERABシステムが想定すべき脅威

【推奨】

ERABシステムは、以下の観点を前提として対策の検討を進めること。

- 標的型攻撃、不正アクセス、不正操作、機能停止、情報の窃取、情報の改ざん、プロセスの不正な実行、高負荷攻撃（バッファーオーバーフロー攻撃、DoS/DDoS攻撃）、不正送信、バックドアを悪用する攻撃、マルウェア感染、ランサムウェア感染、盗聴、異常動作（誤動作）等の多様なリスクを想定すること。
- インシデント検知のためにシステムのログを取得すること。
- 閉域網だから安全であるという考えに立脚しないこと。
- セキュリティ対策については、安全な状態が完全に達成されることはなく、継続的に対策を改善すること。

（以下、略）

ERABサイバーセキュリティガイドライン

詳細な改定内容（【追加】3.4. ERABシステムが維持すべきサービスレベル）

対策要件の追加が必要と考えられる理由とその対策

●追加要件が必要な理由となる脅威･リスク：【脅威･リスクⅠ、Ⅱ】

Ø GW配下ではなくなるため、ERAB制御対象のエネルギー機器や制御用通信が直接、攻撃者の標的となり、不正アクセスや通信路上での盗聴･改ざん、なりすましなどのインターネット上の脅威にさらされる可能性がある。

Ø インターネットとの通信を行えるコントローラーやERAB制御対象のエネルギー機器が、インターネット上のさまざまな脅威の標的となっている。

●全般的な対策

Ø インターネットとの通信が行える幅広いIoT製品を対象として、共通的な物差しで製品に具備されているセキュリティ機能を評価･可視化することを目的とした「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」が、2025年3月から運用開始されることに伴い、IoT機能を有するコントローラーやERAB制御対象のエネルギー機器においても、同制度との効果的な連携を図ることにより、セキュリティを強化することが重要。

新しく盛り込むべき事項の方向性

3.4. ERABシステムが維持すべきサービスレベル

【勧告】

各事業者及びその保有するシステムは以下の定義でのサービスレベルの確保が求められる。

- 容量市場、需給調整市場等における要求事項に準拠したサービスレベル
- 簡易指令システムを有する事業者とそのシステム：「電力制御システムセキュリティガイドライン」に準拠したサービスレベル
- アグリゲーションコーディネーターとその保有するシステム：本ガイドラインに準拠したサービスレベル、加えて簡易指令システムとの直接的な接続部においては「電力制御システムセキュリティガイドライン」に準拠したサービスレベル、簡易指令システムを運用する送配電事業者が「電力制御システムセキュリティガイドライン」と「本ガイドライン」に基づき別途要件を定義したセキュリティ対策に準拠したサービスレベル
- リソースアグリゲーターとその保有するシステム：アグリゲーションコーディネーターと接続する場合は、本ガイドラインに準拠したサービスレベル、加えて、アグリゲーションコーディネーターが「本ガイドライン」に基づき別途要件を定義したセキュリティ対策に準拠したサービスレベル
- ERAB制御対象のエネルギー機器やGW等：「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」が定めるIoT製品に対するセキュリティ要件に準拠したサービスレベル（現時点においては、★１（レベル１）以上を満たすこと。なお、今後、製品類型ごとの特徴を考慮した★２（レベル２）以上の詳細要件が決定した場合においては、★２（レベル２）以上を満たすことが望ましい。）

Creation of risk scenarios and calculation of risk values in the ERAB system

Identification of possible threats in the ERAB system and risk assessment in 2026

Breakdown of the 80 threat/attack scenarios in 2026 (+22 to Y2025)

Threat/attack scenario	Number of cases
Unauthorised access	24(+9)
Malware infection	7
Setup error	6
Equipment spoofing	4
DoS/DDoS attack	4
Man-in-the-middle attack	4
Ransomware infection	5(+2)
Disaster, disability etc.	3
Brute-force password attack	2
Phishing attack	2
Website tampering	2
Insider attack	2
Failure to configure security features	2
Mis-operation	1
Malware contamination during equipment manufacture	1
Caused by R6 (interface between energy device and aggregator subject to ERAB control without installing the GW20 on the consumer side)	9(+9)
Others	2(+2)

Analysis is ongoing

CCRC IN JAPAN CONTRIBUTES TO DESIGN ERAB SYSTEM SECURITY

TOKYO, JAPAN
KEIO UNIVERSITY

CYBER CIVILIZATION RESEARCH CENTER

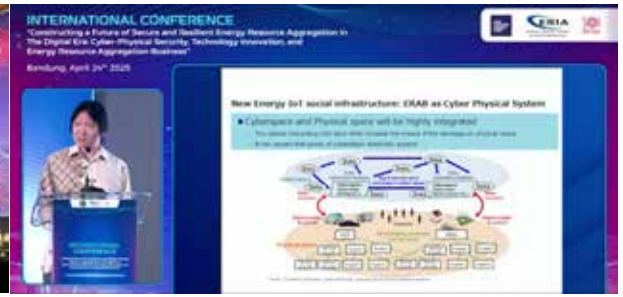
- **In 2021, CCRC published the technical report on "Security Recommendations for Distributed Energy System Aggregators, Based on METI Cyber and Physical Security Framework", showing 51 recommendations to be countermeasures to the major vulnerabilities of ERAB system.**
  - The report is backed by 5 years experience of running a prototype system
  - The full report is available at
    - https://www.ccrc.keio.ac.jp/ccrc-technical-report-202109/

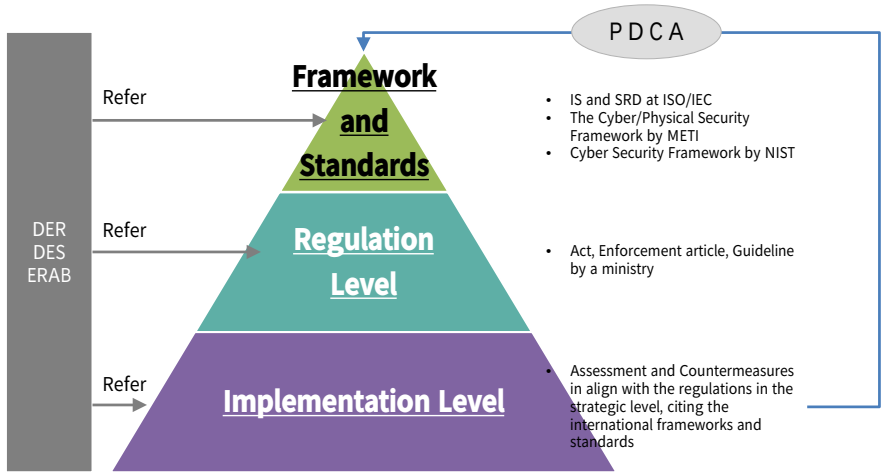
ERIA ERAB/分散電源・電力グリッドのサイバーセキュリティ高度化の取り組み

The ERIA CPSF ERAB Initiative

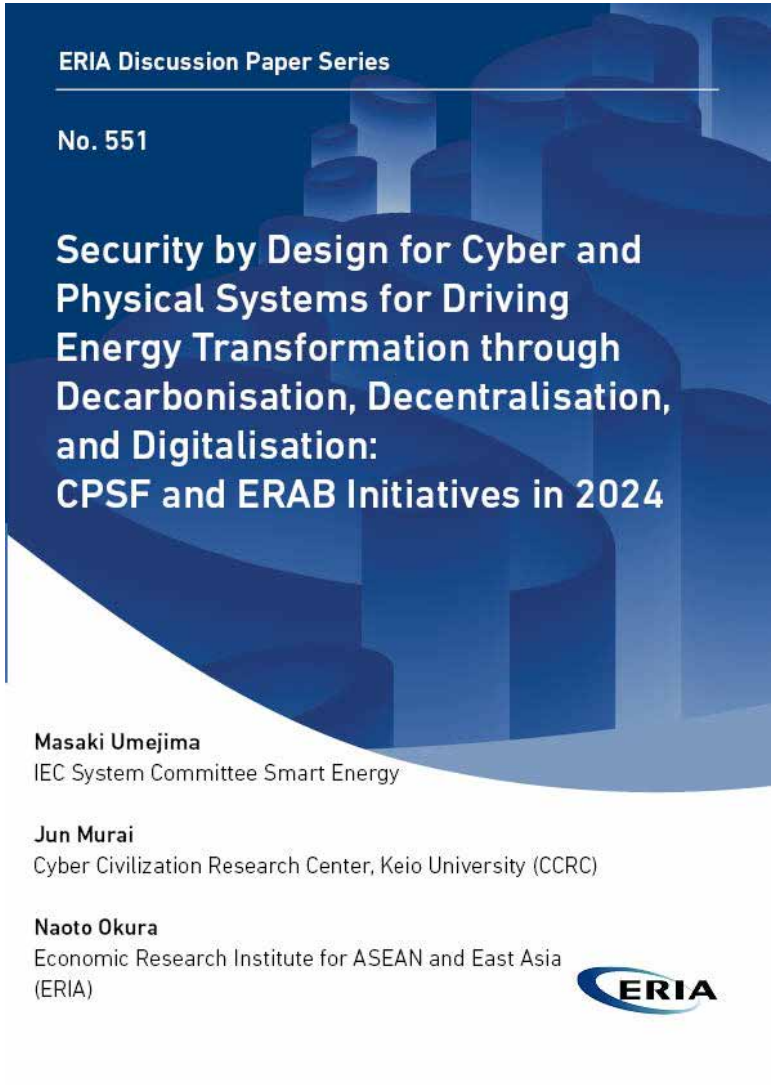
Study Group 5 – 24 April 2025, Bandung Indonesia

- More than 50 delegates from Indonesia, Thailand, Malaysia, Singapore, and Japan participated.
- It concluded emphasizing CPSF contextualisation and a shared cyber-physical security concept.
- Participants reviewed the ERAB security triangle, three-layer cyberspace/physical model, and six CPSF elements.
- A common ASEAN understanding of cyber-physical systems for the energy sector was urged.



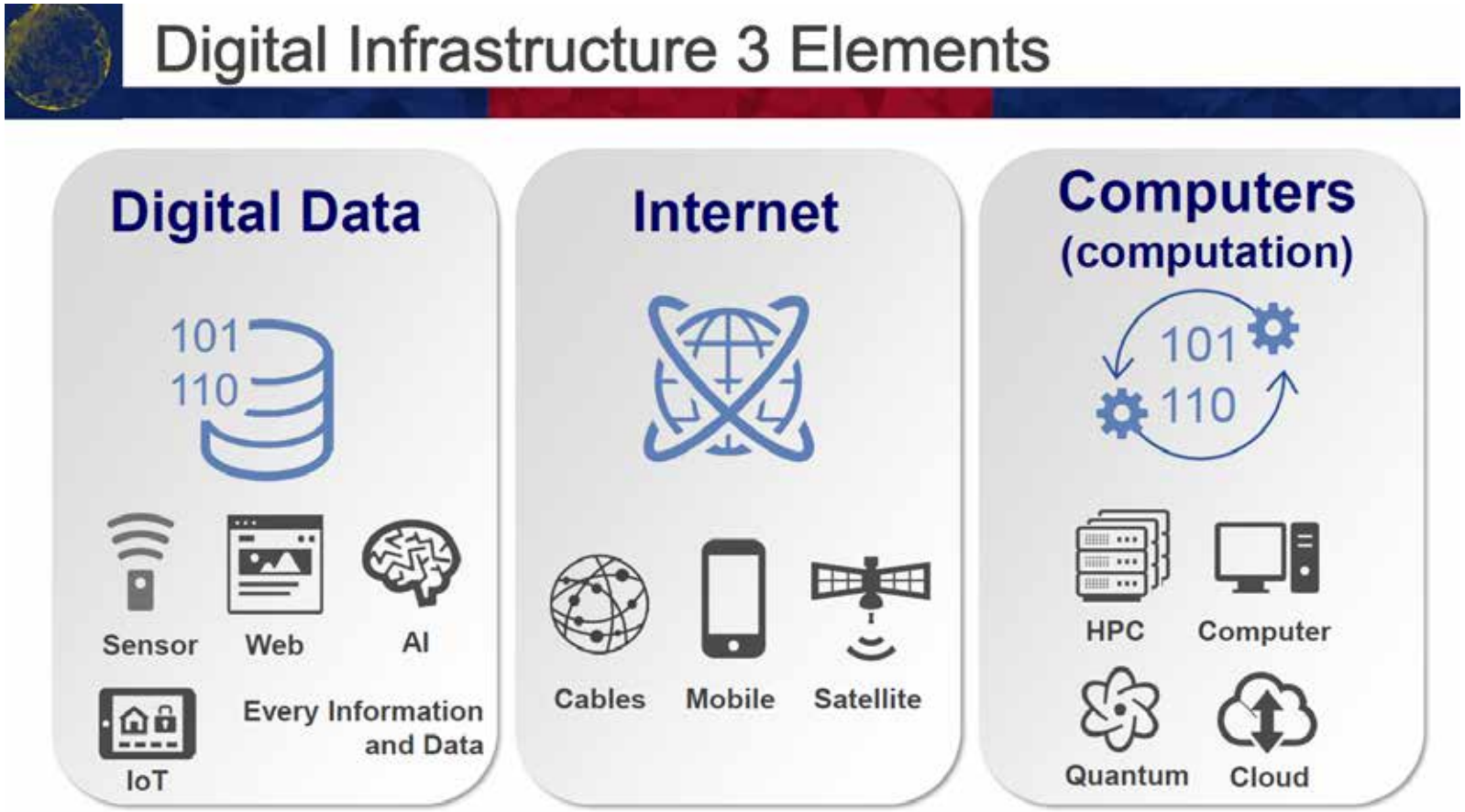


Discussion Paper (Published on 28 July 2025)



Philosophy in the ERIA CPSF ERAB Initiative

Maintain the philosophy supporting the success of the Internet: open-standard, autonomous, and distributed architecture design, and global governance to manage multiple stakeholders, allowing redundancy into the system.



Source :Jun Murai(2026)" ENERGY, DATA, COMPUTER AND THE INTERNET5thFebruary" the ERIA Conference on Cyber Resilience by Design: Securing Distributed Energy Systems

The ERIA study group on the cybersecurity of DERs in ASEAN and Japan
The community facilitates experts from government, academia, and industry in ASEAN

METI
Ministry of Economy, Trade and Industry

IEC

CYBER CIVILIZATION RESEARCH CENTER

The ERIA study group on the cyber and physical system security of DERs

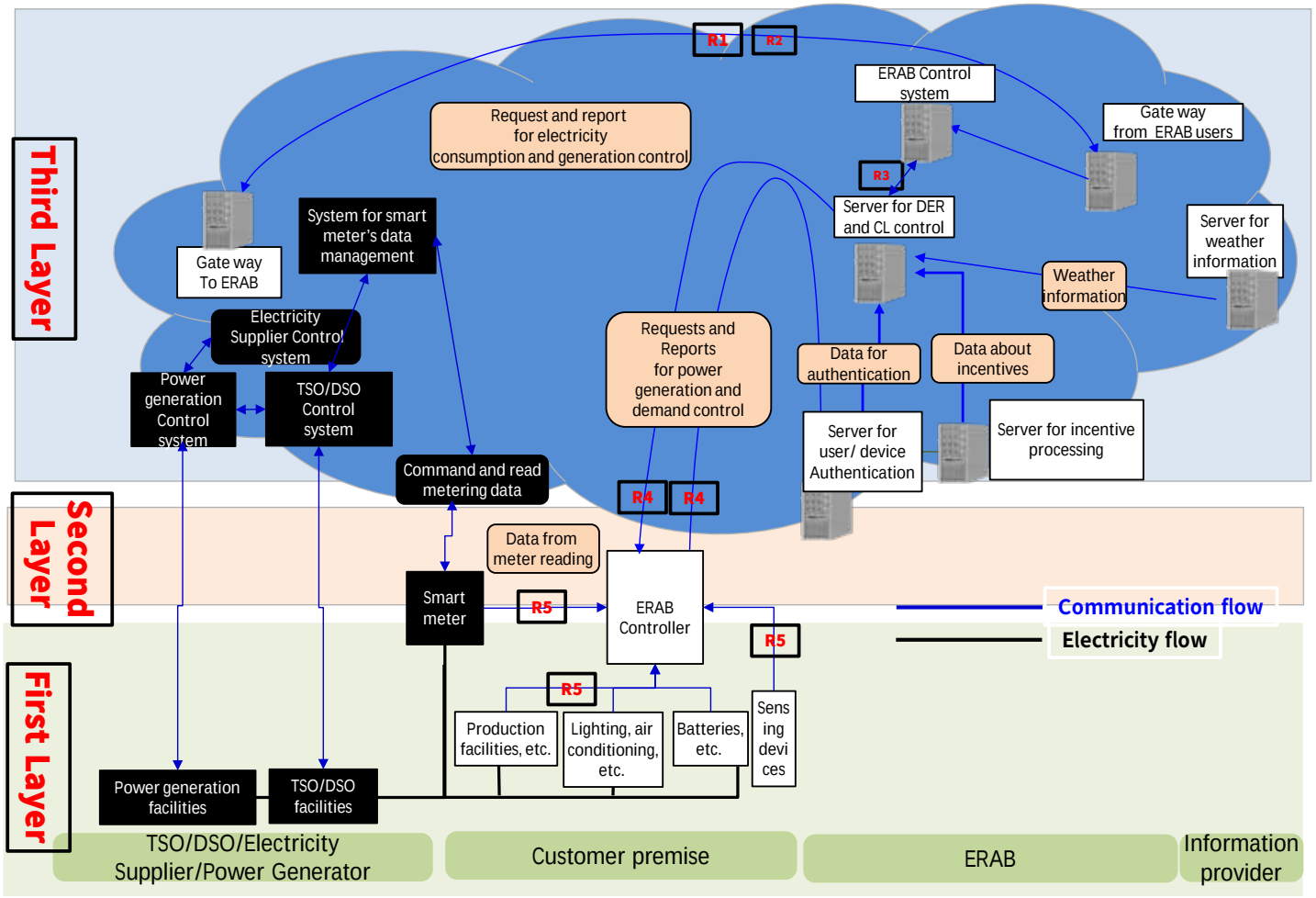
- Cybersecurity Malaysia(Ministry of Digital)
- Malaysian Communications and Multimedia Commission (MCMC)
- IPv6 Forum Malaysia
- Universiti Tenaga Nasional (UNITEN)
- Cybersecurity Research Centre (CYRES) at Universiti Sains Malaysia
- Multimedia University, Malaysia
- TNBX, Tenaga Nasional Berhad

- Special Advisor to the Indonesian President for Energy
- National Cyber and Crypto Agency (BSSN)
- Planning Bureau, Ministry of Energy and Mineral Resource(ESDM)
- National Research and Innovation Agency (BRIN)
- Indonesia Internet of Things Association (ASIOTI)
- Center for Excellence for Defense and Security Science and Technology, Bandung Institute of Technology, Indonesia
- Communication and Information Technology Insfrastucture, elkom University(CITI)
- Digital and Information Technology, PT Perusahaan Listrik Negara (Persero)

- National Cyber Security Agency (NCSA)
- Digital Technology Operation Division, Electricity Generating Authority of Thailand (EGAT)
- National Electronics and Computer Technology Center(NECTEC)
- Faculty of Engineering, Chulalongkorn University
- Kasetsart University
- Mahidol University
- Thai IoT Association

asean

The project to create security standards on Energy Resource Aggregation Business (ERAB)
SRD 63443-2 ED1: Distributed Energy Resource Aggregation Business System-PART2: Risk assessment and treatment



- The scope of this document is to show the process of risk assessment which is consisted of risk identification, risk analysis, and risk evaluation, causing the risk treatment of the example of risk assessment and treatment on Distributed Energy Resource Aggregation Business (ERAB)
- Note1: ERAB case is compatible with the BUC format shown by IEC 62559-2:2015 and SMART GRID STANDARDIZATION ROADMAP by IEC TR 63097:2017
- Note2: ERAB is defined as SRD63443-1

ありがとうございました。

Contact to umejima@collaboyou.com