資料６－１

日本における
ERABシステムに関するセキュリティ対策実践

2024年2月1日

梅嶋真樹

IECシステム委員会･スマートエネルギー開発計画担当コンビナ

サイバー文明研究センター(CCRC)･慶應義塾大学大学院特任准教授

Cyber Civilization Research Center（CCRC）, Keio University

- *CCRCは、米国と日本のインターネット専門家の主導のもと、サイバー空間と物理空間のセキュリティ設計に取り組む*
  - *エネルギーリソースアグリゲーションビジネスシステムのようなサイバーフィジカルシステムの信頼設計を研究テーマとし、米国、EU、ASEANの各国機関と提携して関連研究を推進*

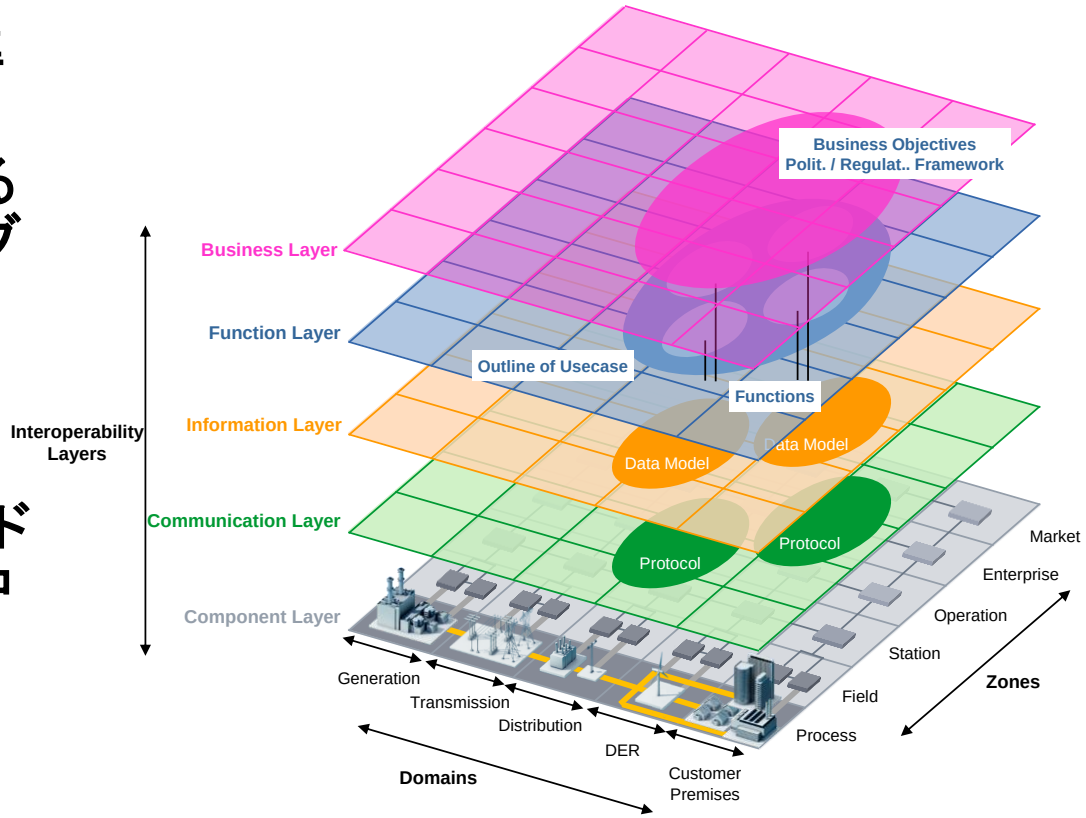
Dr. David Farber:Left
the **Internet** Hall of Fame
Fellow, the American Association for the Advancement of Science〔AAAS〕
Dr. Jun Murai:Right
the **Internet** Hall of Fame
Special Advisor to the Cabinet

Copyright © 2008 Keio University |

The IEC System Committee Smart Energy (SyC SE)

- 国際電気標準会議（IEC）は、170 か国以上から 20,000 人の専門家を集め、10,000 以上の国際標準を提供する世界的な非営利組織
- IECシステム委員会でSmart Energy分野を担当するThe IEC SyC SEは、スマートエネルギーとスマートグリッドのシステムレベルの標準化を推進。SyC SEのSmart Grid Architecture Model（SGAM）は、スマートグリッド上の新サービスの参照可能なアーキテクチャとしての役割を担う。2022 年からは本邦のERABをベースにSRD63097に関するスマートグリッド標準化ロードマップの一部となるSRD63443を開発中

Leadership	Before Nov 2023	After Nov 2023
Chair	Richard SCHOMBERG	Pascal TERRIEN
Convener of Development Plan	Hideki Hayashi	Masaki Umejima

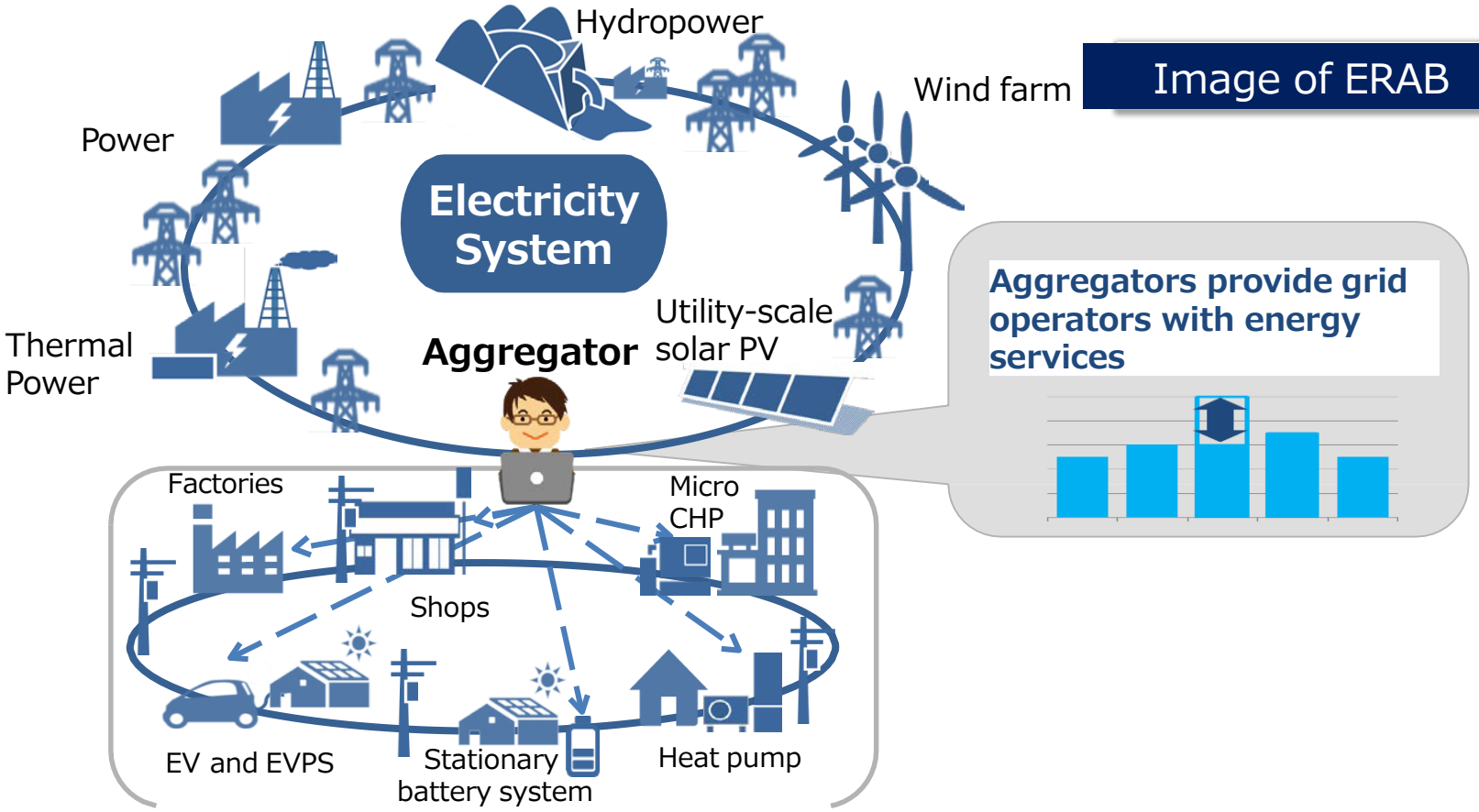


SGAM Plane by ” SMART GRID STANDARDIZATION ROADMAP” on SRD63097

3

特定卸供給事業・エネルギーリソースアグリゲーションビジネス（ERAB）

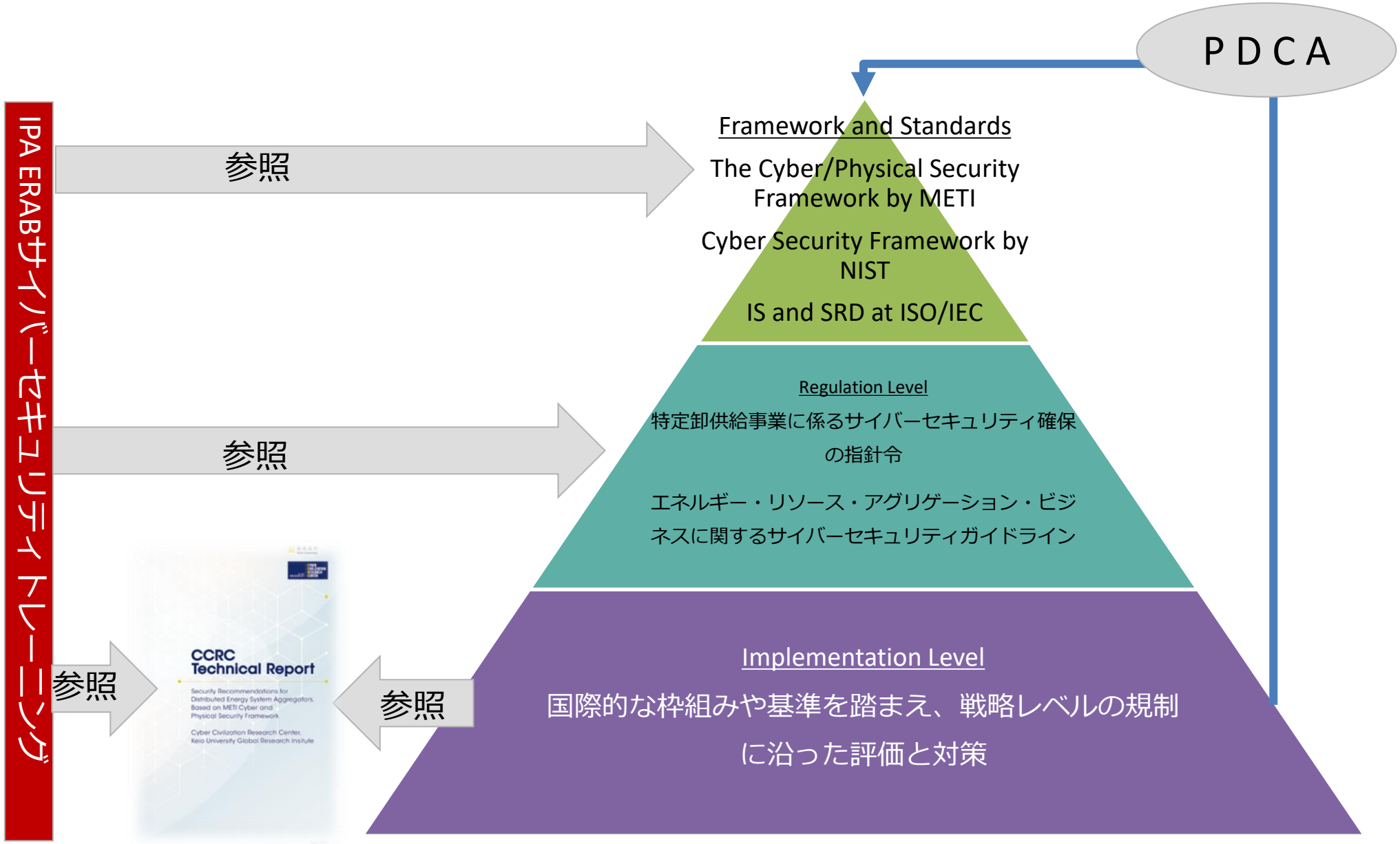
- 特定卸供給事業、エネルギーリソースアグリゲーションビジネス（ERAB）は、EV、駅用蓄電池、燃料電池、エアコンなどの需要側の分散型エネルギーリソースをコントロールする新たなビジネスの枠組み



The IEC SyC SE will define that the system is to **restrain or elevate the demand according to the request by retailers and a grid distributor** and to **provide the electricity traded in a supply and a demand adjustment market.**

4

日本におけるERABシステムに関するセキュリティの全体構成



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）

- サイバー空間とフィジカル空間が高度に融合したSociety 5.0（超スマート社会）では、付加価値を創造する一連の活動（サプライチェーン）の形態がより柔軟で動的なものに変化すると考えられています。新たな形のサプライチェーン（バリュークリエイションプロセス）が創出される一方で、サイバー空間とフィジカル空間の融合により、サイバー攻撃の脅威が増大する懸念が存在
- 「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）」は、Society 5.0時代のセキュリティ対策に必要となるコンセプト、ポリシー、具体的な対策方法を、体系的に整理したフレームワークであり、2019年4月に、経済産業省からVer. 1.0が公表された
  - https://www.meti.go.jp/policy/netsecurity/wg1/wg1.html

The Third Layer
(Data circulation)

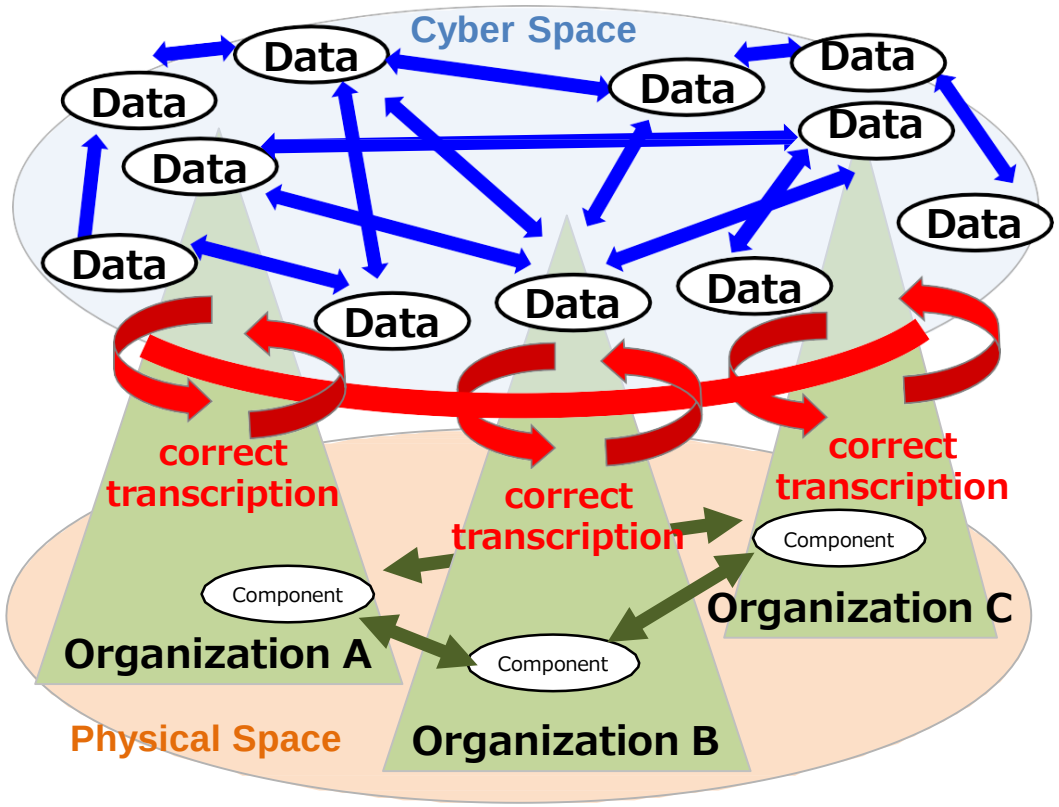
第Ⅲ部【メソッド】
第Ⅱ部で示した対策要件を対策の種類に応じて整理。

The Second Layer
(Cyber to physical/Physical to cyber)

第Ⅱ部【ポリシー】
第Ⅰ部で示したモデルを活用したリスク源の整理と、リスク源に対応する対策要件を提示。

The First Layer
(Relationship among Organizations)

第Ⅰ部【コンセプト】
サイバーセキュリティの観点から、バリュークリエイションプロセスにおけるリスク源を整理するためのモデルを整理。

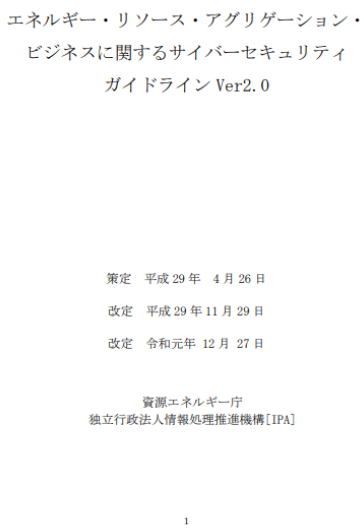


◆**Six Elements:** **Organization, people, component, data, procedure, system**

Source: The Ministry of Economy, Trade and Industry、Japan(2019)Cyber/Physical Security Framework

アグリゲーター向けのガイドライン及び指針

- 経済産業省(2022)特定卸供給事業に係るサイバーセキュリティ確保の指針令
- 資源エネルギー庁・IPA(2019)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(ERABセキュリティガイドライン)

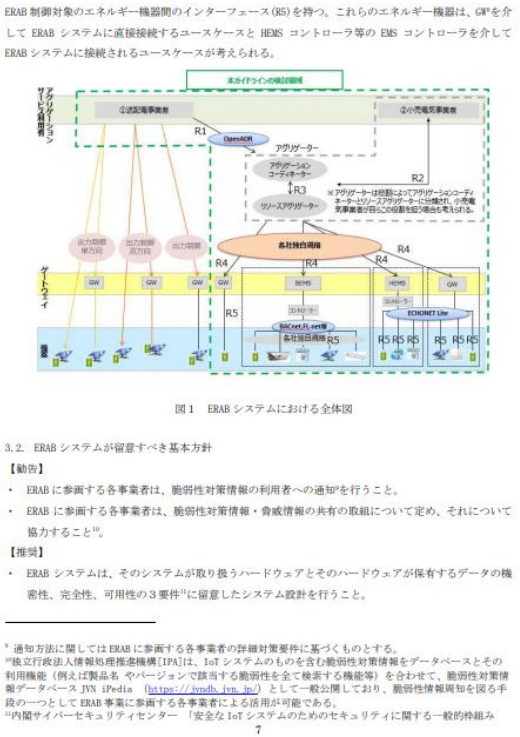


エネルギー・リソース・アグリゲーション・
ビジネスに関するサイバーセキュリティ
ガイドライン Ver2.0

策定　平成 29 年　4 月 26 日
改定　平成 29 年 11 月 29 日
改定　令和元年 12 月 27 日

資源エネルギー庁
独立行政法人情報処理推進機構[IPA]

1



ERAB 制御対象のエネルギー機器間のインターフェース(R5)を持つ。これらのエネルギー機器は、GW*を介して ERAB システムに直接接続するユースケースと HEMS コントローラ等の EMS コントローラを介して ERAB システムに接続されるユースケースが考えられる。

図 1　ERAB システムにおける全体図

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、脆弱性対策情報の利用者への通知*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[10]。

【推奨】

- ERAB システムは、そのシステムが取り扱うハードウェアとそのハードウェアが保有するデータの機密性、完全性、可用性の３要件[11]に留意したシステム設計を行うこと。

* 通知方法に関しては ERAB に参画する各事業者の詳細対策要件に基づくものとする。
[10]独立行政法人情報処理推進機構[IPA]は、IoT システムのものを含む脆弱性対策情報をデータベースとその利用機能（例えば製品名 やバージョンで該当する脆弱性を全て検索する機能等）を合わせて、脆弱性対策情報データベース JVN iPedia （https://jvndb.jvn.jp/）として一般公開しており、脆弱性情報周知を図る手段の一つとして ERAB 事業に参画する各事業者による活用が可能である。
[11]内閣サイバーセキュリティセンター 「安全な IoT システムのためのセキュリティに関する一般的枠組み

7

- ERABセキュリティガイドライン:
  - https://www.enecho.meti.go.jp/category/saving_and_new/advanced_systems/vpp_dr/download-2.html
- 特定卸供給事業に係るサイバーセキュリティ確保の指針令
  - https://www.enecho.meti.go.jp/category/electricity_and_gas/electric/summary/regulations/pdf/cyber-shishin.pdf

ERABセキュリティガイドラインに基づくセキュリティの実装

- ERABセキュリティガイドラインは、PDCAを行うこと、(それに基づく)対策をその優先順位と共に例示
- AC及びRA事業者におけるPDCAでは、構築するシステムを対象にISO/IEC12100などを参照としたリスクアセスメントを実施し、(それに基づく)対策を検討している
- ERABシステムは、「物理的な環境と仮想的な環境が高度に連携が求められる」。「全ての情報資産が自社管理ではない」、「金融資産として登録されないような小さな資産が、アグリゲーションサービス停止の原因となるDDoS攻撃の要因となる」ようなオリジナルな特色を持つ
  - 米NIST Cybersecurity Framework(CPF)、日・経産省サイバー・フィジカル・セキュリティ対策フレームワーク(CPS)がDERシステム(分散型エネルギーシステム)をターゲットとして、展開されえる

参考：ISO12100に基づくリスクアセスメント

制限の決定
リスクアセスメントの範囲および条件：●使用上の制限や条件、空間上の制限や条件、時間上の制限や条件

危険源の特定
危険源（およびそれによる危険状態）をもれなく特定

リスク見積
特定した危険源のすべてに対して、個々にリスクを見積。特定された危険源における被害における「被害の大きさ」とそれが発生する「危害の発生確率」の組合わせを用いてリスクの大小を見積り

リスク評価
リスク見積の結果に基づいて、リスクの評価を行い、リスク低減処置が必要かどうかを決定

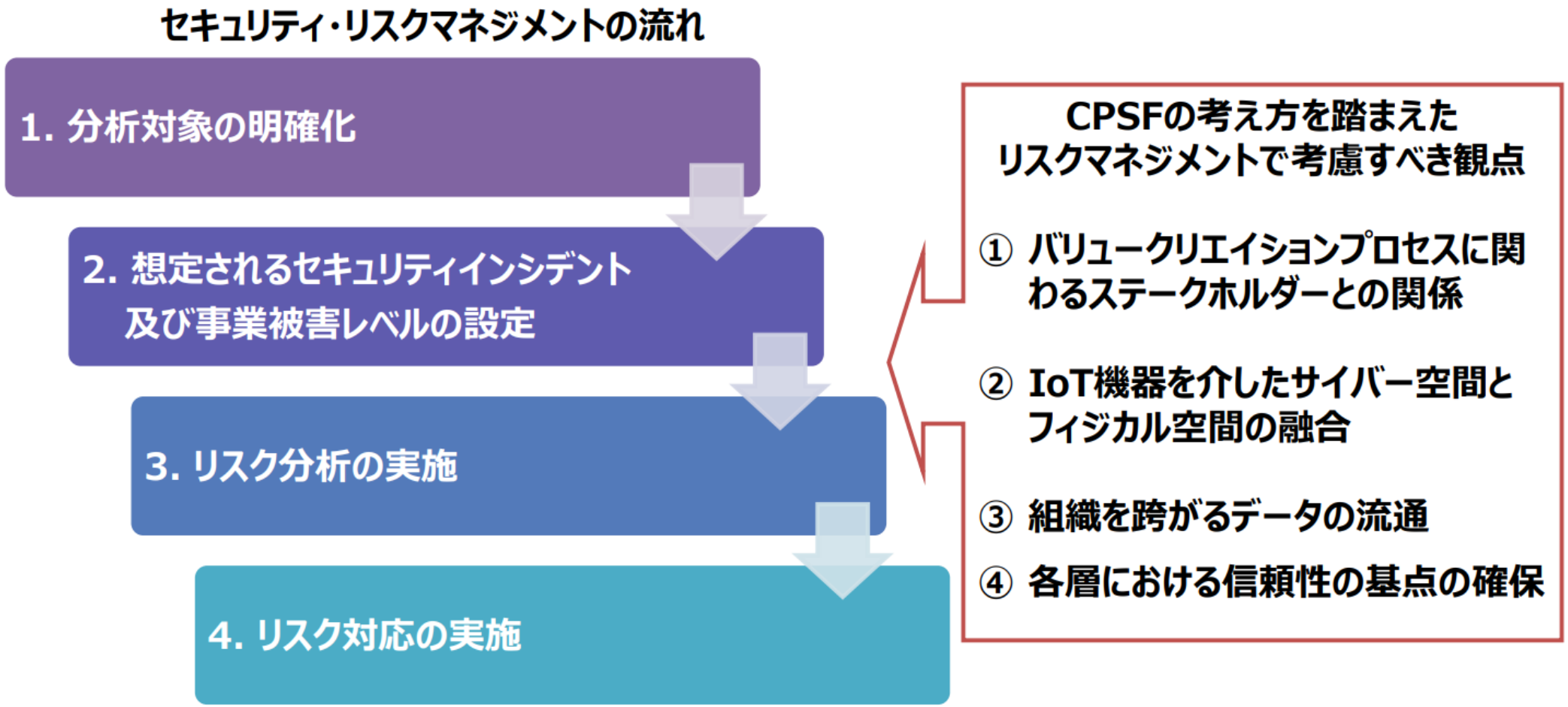
【参考】ERABサイバーセキュリティガイドライン3.6項

- ERABサイバーセキュリティガイドラインは、Step1～Step 7 のプロセスに基づく基づく各事業者の有する事業及びシステム特性を考慮したセキュリティ設計を勧告として求めている

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】ERABに参画する各事業者は、ERABシステムでは、以下の手順を踏むこと	
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	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
Step5	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
Step6	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
Step7	事故発生時の対応方法を設計・運用及び訓練すること

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）
出どころ：ERABサイバーセキュリティトレーニング

CPSFにおけるリスクマネジメント　第1ステップ：分析対象の明確化（1/2）

- リスクマネジメントの第1ステップとして、CPSFの三層構造に基づいて分析対象を明確にし、各層における構成要素を把握。

階層	特性	機能・役割	分析対象	ERABにおける分析対象例
第3層 サイバー空間のつながりにおける、データの信頼性	サイバー空間で組織を超えた多様・大量のデータの流通・処理	データの送受信、加工・分析、保管 **【信頼性の起点】**データ	• データを送受信／加工・分析／保管するモノ・システム • 組織を超えて流通するデータ 等	• クラウド環境 • ルータ • データ 等
第2層 サイバー空間とフィジカル空間のつながりにおける、要求される情報を正確に“転写”する機能の信頼性	フィジカル空間とサイバー空間のつながり拡大	フィジカル空間とサイバー空間との間のデータのやりとり **【信頼性の基点】**ルールに沿って正しくフィジカル空間とサイバー空間とを転写する機能	• データを転写するモノ • システム転写されるデータ 等	• スマートメータ • 蓄電池・エアコン等制御対象機器 • ERABコントローラ 等
第1層 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	各組織の適切なガバナンス・マネジメント	各組織のセキュリティマネジメント **【信頼性の基点】**組織・マネジメント	• 組織で管理されるモノ・システム等 • 組織内で流通するデータ 等	• 社員、従業員 • 企業のIT資産 等

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）

CPSFにおけるリスクマネジメント　第1ステップ：分析対象の明確化（2/2）

- 分析対象を明確化する際の留意点

① バリュークリエイションプロセスに関わるステークホルダーとの関係

- ✓ 直接的にプロセスに関与していない企業でもセキュリティ対策への関与（マルチステークホルダーアプローチ）が求められる
- ✓ **三層構造に基づきステークホルダーを特定、その役割や当該事業における重要度を明確にすること**

② IoT機器を介したサイバー空間とフィジカル空間の融合

- ✓ ERABシステムでは、フィジカル空間のデータとサイバー空間のデータの同期の真正性が必要
- ✓ **サイバー空間へデータとして伝送する機能を果たす機器(スマートメーター)を正確に適切に識別し、を適切に識別し、自組織のオペレーションにおける重要度等に応じて分類しておく必要がある**
- ✓ サイバー空間とフィジカル空間が融合する境界では、上述の例とは逆に、サイバー空間におけるデータの解析結果に基づき、フィジカル空間のモノが制御され得るとの認識を持つ必要がある

③ 組織を跨るデータの流通

- ✓ 組織をまたいだデータ等のやり取組織を跨いだデータ等のやり取りが活発化すると、事前に想定されていない構成要素（ソシキ、ヒト、モノ等）から適切でないデータが自組織に提供される可能性が高くなると想定される

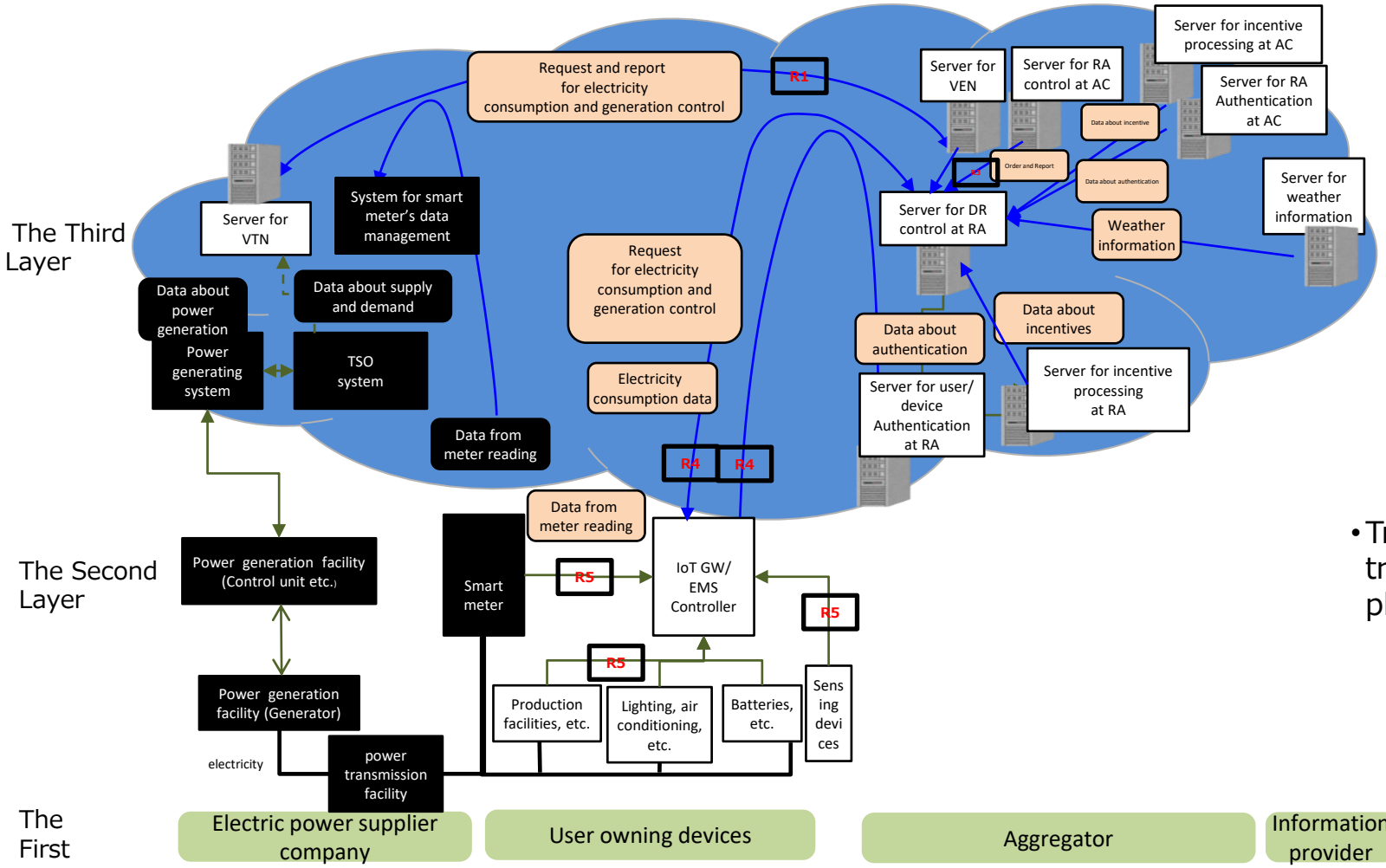
④ 各層における信頼性の基点の確保

- ✓ 従来から考慮されてきた組織のマネジメントの信頼性という観点に加え、第 2 層における IoT 機器を介した転写機能の正確性、第 3 層におけるバリュークリエイションプロセスに関わるデータそのものの信頼性という複数の観点を踏まえた対策を講ずることが、目的どおりの価値を生み出すために重要になる
- ✓ このため、**上記①～③の観点に留意し、信頼性の起点の確保を考慮した上で、起点となる要素を明確にする**ことが重要となる

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）

ERABシステムにおける分析対象

◆**Six Elements:** **Organization, people, component, data, procedure, system**



The Third Layer (Data circulation)

- Trustworthiness of data that freely circulate and are processed or created to produce services

The Second Layer (Cyber to physical/Physical to cyber)

- Trustworthiness of function for "correct transcription" from cyber to physical / from physical to cyber form

The First Layer (Relationship among Organizations)

- Trustworthiness of each organization based on appropriate management

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）からCCRCが導出

CPSFにおけるリスクマネジメント　第2ステップ：想定されるインシデント・被害レベルの設定（1/2）

- 第2ステップでは、明確化された分析対象に対して、重大な影響を及ぼしうるセキュリティインシデントを整理し、それによる事業への影響を整理。
- 考慮すべきセキュリティインシデントを設定するにあたり、各層の機能を脅かす事象を検討。

階層	各層の機能（守るべきもの）	機能（守るべきもの）に対する悪影響のイメージ
第3層 サイバー空間のつながりにおける、データの信頼性	• データをセキュアに加工・分析する機能 • ・データをセキュアに保管する機能 • ・データをセキュアに送受信する機能	• データ保護に係る法制度等への不準拠 • セキュアでない稼動：データ処理側でのセキュリティインシデントによる情報資産の棄損(漏洩/改ざん/破壊/利用停止) • 信頼性の低い稼動 ：データ関連サービスが意図した稼動をしないこと(誤動作、停止等
第2層 サイバー空間とフィジカル空間のつながりにおける、要求される情報を正確に“転写”する機能の信頼性	• フィジカル空間の物理事象を読み取り、一定のルールに基づいて、デジタル情報へ変換し、第3層へ送る機能 • サイバー空間から受け取ったデータに基づいて、一定のルールに基づいて、モノを制御したり、データを可視化したりするように表示したりする機能	• 機器の機能停止：IoT 機器の稼動が停止すること • 信頼性の低い稼動：IoT 機器が意図した稼動をしないこと • ・ 安全面、環境面、衛生面に問題のある稼動 • ・ 誤計測
第1層 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	• 組織として平時のリスク管理体制を構築し、適切に運用すること • 組織としてセキュリティインシデント発生時においても適切に自組織の事業を継続すること • フィジカル空間での製品・サービスが、望まれる品質を備えて入荷又は出荷されること	• 法制度等への不準拠· セキュリティインシデントの発生：情報資産の棄 • 損(漏洩/改ざん/破壊/利用停止)· セキュリティインシデントによる影響の拡大：被害拡大による事業影響(稼動停止、誤ったアウト • プット、従業員の健康や安全、環境への悪影響等

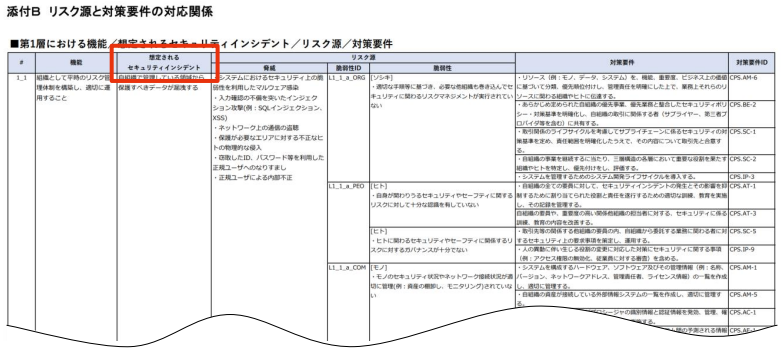
出所）経済産業省,サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）

CPSFにおけるリスクマネジメント　第2ステップ：想定されるインシデント・被害レベルの設定（2/2）

- 各層の機能、機能に対する悪影響を踏まえて、三層構造の各層で回避すべきセキュリティインシデントを整理
- 各層で回避すべきセキュリティインシデントを整理し、自社の事情を加味し、想定インシデントを具体的に検討

階層	想定されるセキュリティインシデントの例
第3層 サイバー空間のつながりにおける、データの信頼性	• … • …
第2層 サイバー空間とフィジカル空間のつながりにおける、要求される情報を正確に“転写”する機能の信頼性	• ：：： • …
第1層 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	• …

CPSFの添付Bに基づく
想定インシデントの検討


添付B　リスク源と対策要件の対応関係

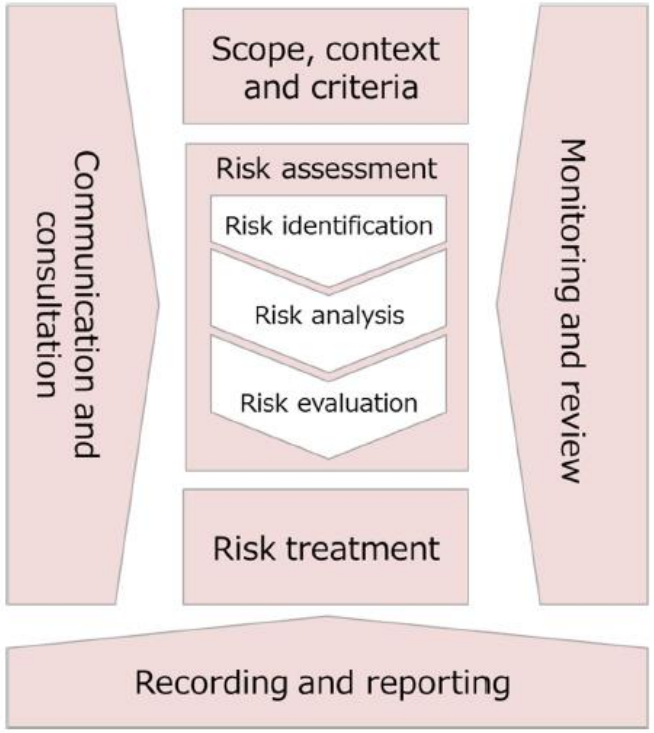
■第1層における機能／想定されるセキュリティインシデント／リスク源／対策要件

#	機能	想定されるセキュリティインシデント	脅威	リスク源 脆弱性ID	リスク源 脆弱性	対策要件	対策要件ID
1_1	組織として平時のリスクの管理体制を構築し、適切に運用すること	自組織と管理・インシデント関連のシステムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・入力確認の不備を突いたインジェクション攻撃(例：SQLインジェクション、XSS) ・ネットワーク上の通信の盗聴 ・保護が必要なエリアに対する不正なヒトの物理的な侵入 ・窃取したID、パスワード等を利用した正規ユーザへのなりすまし ・正規ユーザによる内部不正	保護すべきデータが漏洩する	L1_1_a_ORG	[ソシキ] ・適切な平時等に基づき、必要な組織も巻き込んでセキュリティに関わるリスクマネジメントが実行されていない	・リソース（例：モノ、データ、システム）を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。 ・あらかじめ定められた自組織の優先事業、優先業務と整合したセキュリティポリシー・対策基準を明確化し、自組織の取引に関係する者（サプライヤー、第三者プロバイダ等を含む）に共有する。 ・取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について取引先と合意する。 ・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。 ・システムを管理するためのシステム開発ライフサイクルを導入する。	CPS.AM-6 CPS.BE-2 CPS.SC-1 CPS.SC-2 CPS.IP-3
				L1_1_a_PEO	[ヒト] ・自身が割り当てられうるセキュリティやセーフティに関するリスクに対して十分な認識を有していない	・自組織の全ての業務に対して、セキュリティインシデントの発生とその影響を最小化するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。 自組織の要員や、重要度の高い関係自組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。 ・取引先等の関係する自組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティとの要求事項を周知し、運用する。	CPS.AT-1 CPS.AT-3 CPS.SC-5
					[ヒト] ・ヒトに関わるセキュリティやセーフティに関係するリスクに対するガバナンスが十分でない	・人の異動に伴い生じる役割の変更に対応した対策にセキュリティに関する事項（例：アクセス権限の剥奪、従業員に対する教育）を含める。	CPS.IP-9
				L1_1_a_COM	[モノ] ・モノのセキュリティ状況やネットワーク接続状況が適切に管理（例：資産の棚卸し、モニタリング）されていない	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。 ・自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する。	CPS.AM-1 CPS.AM-5

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）
出どころ：ERABサイバーセキュリティトレーニング

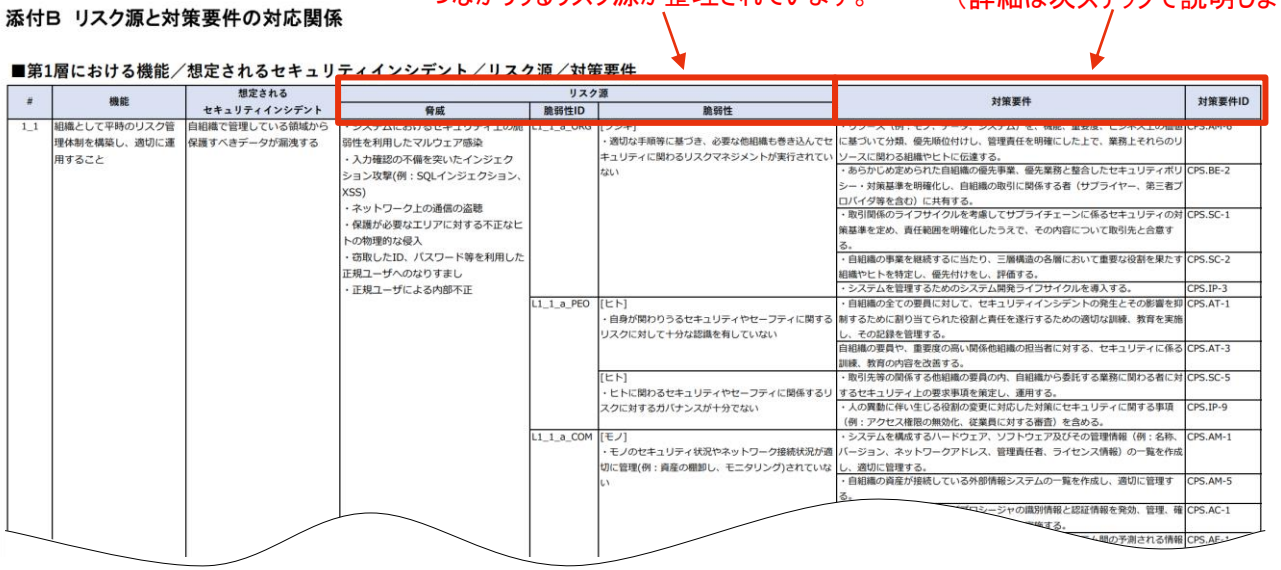
CPSFにおけるリスクマネジメント　第3ステップ：リスク分析の実施

- 第3ステップでは、抽出したセキュリティインシデントにつながるような攻撃シナリオの検討、事業被害レベル、リスク源（脅威・脆弱性）の評価等を実施
  - IEC31000や27001で定義される一般的なセキュリティアセスメント
  - CPSFの添付Bでは、セキュリティインシデントを発生、あるいは発生したインシデントの被害を拡大させる可能性がある脅威及び脆弱性を整理しており、検討すべきリスク源の抽出に活用可能



各層に想定されるセキュリティインシデントにつながりうるリスク源が整理されています。

各リスクに対する対策要件が整理されています。
（詳細は次ステップで説明します。）



添付B　リスク源と対策要件の対応関係

■第1層における機能／想定されるセキュリティインシデント／リスク源／対策要件

#	機能	想定されるセキュリティインシデント	リスク源			対策要件	対策要件ID
			脅威	脆弱性ID	脆弱性		
1_1	組織として平時のリスク管理体制を構築し、適切に運用すること	自組織で管理している領域から保護すべきデータが漏洩する	・システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・入力確認の不備を突いたインジェクション攻撃(例：SQLインジェクション、XSS) ・ネットワーク上の通信の盗聴 ・保護が必要なエリアに対する不正なヒトの物理的な侵入 ・窃取したID、パスワード等を利用した正規ユーザへのなりすまし ・正規ユーザによる内部不正	L1_1_a_ORG	[ソシキ] ・適切な手順等に基づき、必要な他組織も巻き込んでセキュリティに関わるリスクマネジメントが実行されていない	・リソース（例：モノ、データ、システム）を、機能、重要度、ビジネス上の価値に基づいて分類、優先順位付けし、管理責任を明確にした上で、業務上それらのリソースに関わる組織やヒトに伝達する。	CPS.AM-6
						・あらかじめ定められた自組織の優先事業、優先業務と整合したセキュリティポリシー・対策基準を明確化し、自組織の取引に関係する者（サプライヤー、第三者プロバイダ等を含む）に共有する。	CPS.BE-2
						・取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について取引先と合意する。	CPS.SC-1
						・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。	CPS.SC-2
						・システムを管理するためのシステム開発ライフサイクルを導入する。	CPS.IP-3
				L1_1_a_PEO	[ヒト] ・自身が関わりうるセキュリティやセーフティに関するリスクに対して十分な認識を有していない	・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。	CPS.AT-1
						自組織の要員や、重要度の高い関係他組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。	CPS.AT-3
					[ヒト] ・ヒトに関わるセキュリティやセーフティに関係するリスクに対するガバナンスが十分でない	・取引先等の関係する他組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する。	CPS.SC-5
						・人の異動に伴い生じる役割の変更に対応した対策にセキュリティに関する事項（例：アクセス権限の無効化、従業員に対する審査）を含める。	CPS.IP-9
				L1_1_a_COM	[モノ] ・モノのセキュリティ状況やネットワーク接続状況が適切に管理(例：資産の棚卸し、モニタリング)されていない	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	CPS.AM-1
						・自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する。	CPS.AM-5
						[illegible]ミッシャの識別情報と認証情報を発効、管理、確[illegible]する。	CPS.AC-1
						[illegible]の予測される情報	CPS.AE-1

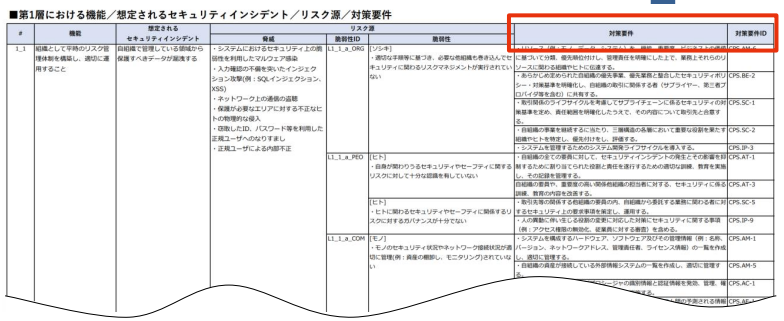
出所）経済産業省,サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）
出どころ：ERABサイバーセキュリティトレーニング

CPSFにおけるリスクマネジメント　第4ステップ：リスク対応の実施（1/2）

- 抽出されたリスクへの対応を検討
- リスクへの対応を検討する際は、リスクに対する「回避」、「低減」、「移転」、「保有」のうち、いずれの対応をとるかを発生時の被害の大きさ等に基づいて検討することが重要
  - CPSFの添付Bでは、「低減」を選択する場合の対応として、各リスク源に対して適当と考えられる対策要件を整理

1. **リスクの回避**
   リスクのある機能を削除したり全く別の方法に変更したりすることにより、リスクが発生する可能性を取り去る。
2. **リスクの低減**
   リスクに対して対策を講じることにより、発生しやすさや被害の深刻度を低減する。
3. **リスクの移転**
   保険加入や、リスクのある部分を他社製品・システムに置き換えることにより、リスクを他社などに移す。
4. **リスクの保有**
   リスクが小さい場合やリスクをとったとしても機会を追求するという場合に、特にリスクを低減するための対策を行わず、許容範囲内として受容する。

CPSFの添付Bに基づく
リスクに対する対策要件の検討


添付B　リスク源と対策要件の対応関係

■第1層における機能／想定されるセキュリティインシデント／リスク源／対策要件

#	機能	想定される セキュリティインシデント	リスク源			対策要件	対策要件ID
			脅威	脆弱性ID	脆弱性		
1_1	組織として平時のリスク管理体制を構築し、適切に運用すること	自組織で管理している領域から保護すべきデータが漏洩する	・システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 ・入力確認の不備を突いたインジェクション攻撃(例：SQLインジェクション、XSS) ・ネットワーク上の通信の盗聴 ・保護が必要なエリアに対する不正なヒトの物理的な侵入 ・窃取したID、パスワード等を利用した正規ユーザへのなりすまし ・正規ユーザによる内部不正	L1_1_a_ORG	【プロセス】 ・適切な手順等に基づき、必要な情報資産を洗い出した上で、業務上それらのリスクに対する組織やヒトに伝達する。 ・あらかじめ定められた自組織の優先事業、優先業務と整合したセキュリティポリシー・対策基準を明確化し、自組織の取引に関係する者（サプライヤー、第三者プロバイダ等を含む）に共有する。 ・取引関係のライフサイクルを考慮してサプライチェーンに係るセキュリティの対策基準を定め、責任範囲を明確化したうえで、その内容について取引先と合意する。 ・自組織の事業を継続するに当たり、三層構造の各層において重要な役割を果たす組織やヒトを特定し、優先付けをし、評価する。 ・システムを管理するためのシステム開発ライフサイクルを導入する。	CPS.BE-2 CPS.SC-1 CPS.SC-2 CPS.SP-3
				L1_1_a_PEO	【ヒト】 ・自身が関わりうるセキュリティやセーフティに関するリスクに対して十分な認識を有していない	・自組織の全ての要員に対して、セキュリティインシデントの発生とその影響を抑制するために割り当てられた役割と責任を遂行するための適切な訓練、教育を実施し、その記録を管理する。 自組織の要員や、重要度の高い関係者組織の担当者に対する、セキュリティに係る訓練、教育の内容を改善する。 ・取引先等の関係する自組織の要員の内、自組織から委託する業務に関わる者に対するセキュリティ上の要求事項を策定し、運用する。 ・人の異動に伴い生じる役割の変更に対応した対策にセキュリティに関する事項（例：アクセス権限の無効化、従業員に対する書面）を含める。	CPS.AT-1 CPS.AT-3 CPS.SC-5 CPS.SP-9
				L1_1_a_COM	【モノ】 ・モノのセキュリティ状況やネットワーク接続状況が適切に管理(例：資産の棚卸し、モニタリング)されていない	・システムを構成するハードウェア、ソフトウェアなどその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。 ・自組織の資産が接続している外部情報システムの一覧を作成し、適切に管理する。	CPS.AM-1 CPS.AM-5

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）
出どころ：ERABサイバーセキュリティトレーニング

CPSFにおけるリスクマネジメント　第4ステップ：リスク対応の実施（2/2）

- 対策要件の選定に当たって、4つの観点を踏まえた検討が重要

① バリュークリエイションプロセスに関わるステークホルダーとの関係
- ✓ 継続的に自組織を取り巻くステークホルダーの関係性の全体像を把握し、組織間でサイバーセキュリティ上の役割と責任を明確化

② IoT機器を介したサイバー空間とフィジカル空間の融合
- ✓ センサ等の機能に対する攻撃を考慮したセキュリティ対策を講ずることが必要。具体的には、データの完全性チェックメカニズムを利用できる機器の利用等を留意
- ✓ 安全性の確保を大前提として、機能安全の観点からの対策やサイバーセキュリティ対策を組合せて対応することが必要。このために、セーフティとセキュリティに係る担当者同士が、よく対話しながら検討することが必要
- ✓ また、自組織で利用するIoT機器の重要度に応じた物理的なセキュリティ対策を講ずることが必要

③ 組織を跨るデータの流通
- ✓ 組織間で交換されるデータの性質、取引先あるいは自組織が提供するサービスの内容等を勘案してリスクを分析し、セキュリティ要求事項を具体化することが重要
- ✓ 保護すべきデータに対するセキュリティインシデントを検知した場合に、適切に取引先へと状況の説明ができるよう対応手順を事前に策定し、適切に報告が必要な関係者へと周知することが必要。

④ 各層における信頼性の基点の確保
- ✓ 第1層においては、信頼関係を維持するに当たり必要なサイバーセキュリティに関係する要求事項を契約にて明確化し、定期的に遵守を確認することが重要
- ✓ 第2層においては、IoT機器による転写機能の正確性を確保するために、機器のライフサイクルを通じた対策を講じ、セキュリティ上の健全性の維持・向上することが重要
- ✓ 第3層においては、サイバー空間のデータ及び、その加工・分析・保管という諸機能の信頼性を確保

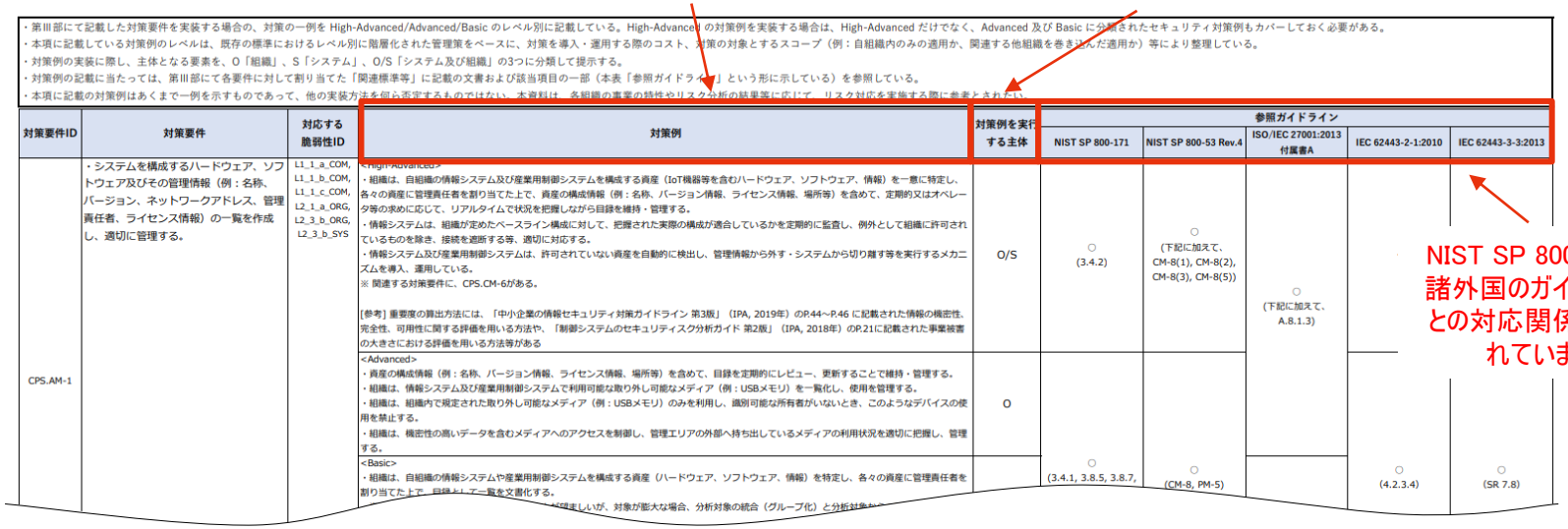
出所）経済産業省,サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）
出どころ：ERABサイバーセキュリティトレーニング

CPSFにおけるリスクマネジメント
第4ステップ：対策要件及び対策例集を活用したリスク対応

- CPSFの添付Cでは、添付Bで示した対策要件をNISTのCybersecurity Frameworkを参考にカテゴリー分けを行う。また、各対策要件について、具体的な参考となる対策例を記載
- 事業者においては、リスクアセスメントの結果に応じて、添付Cに記載されたセキュリティ対策例を実装し、リスクマネジメントプロセスを適切に実施することで、自組織のセキュリティマネジメントを改善することが可能に

対策要件について、具体的な参考となる対策例がBasic, Advanced, High-Advancedの3段階で整理されています。

対策を実施する主体がO「組織」、S「システム」、O/S「組織及びシステム」の3つに分類され提示されています。



添付C　対策要件に応じたセキュリティ対策例

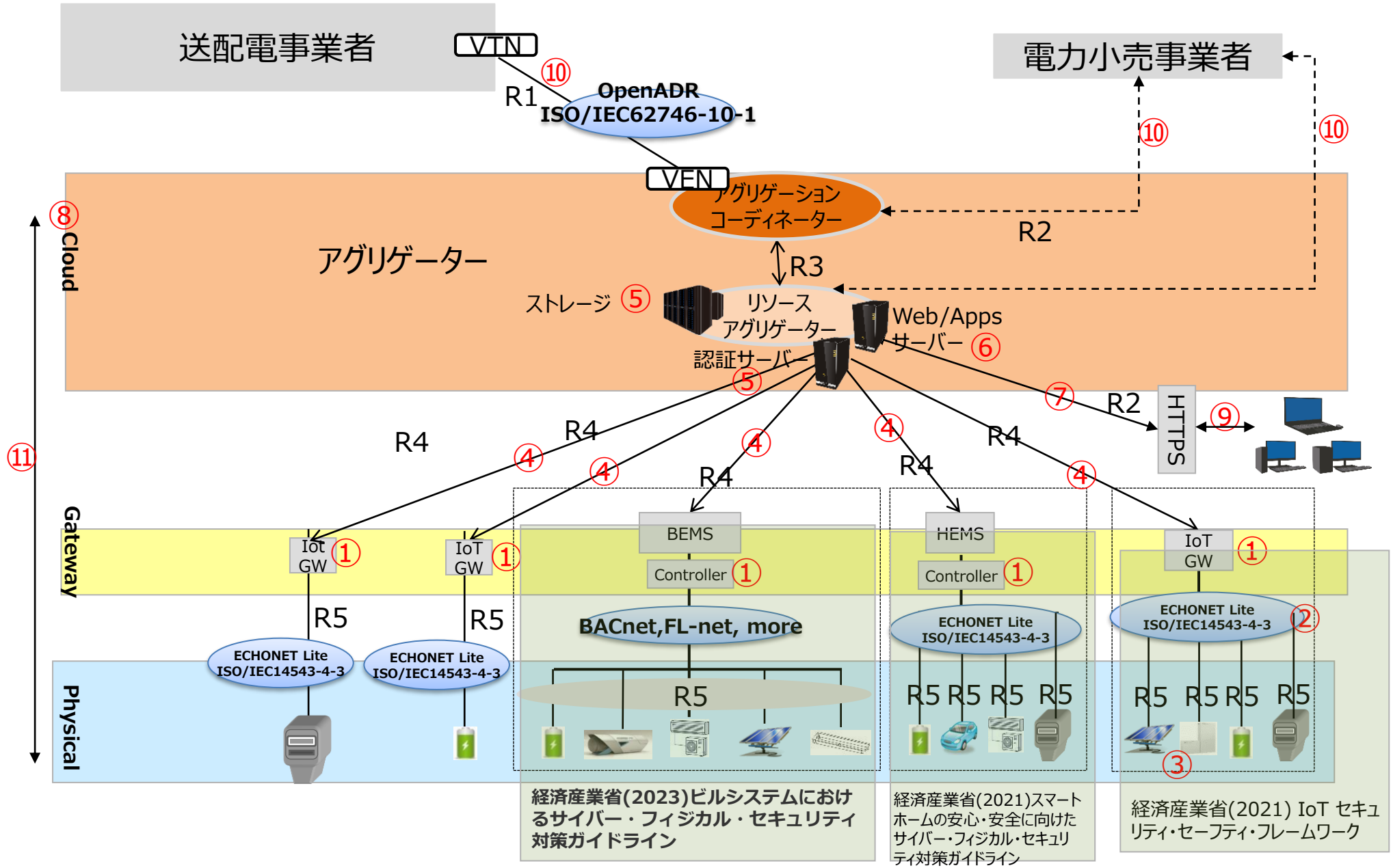
・第Ⅲ部にて記載した対策要件を実装する場合の、対策の一例を High-Advanced/Advanced/Basic のレベル別に記載している。High-Advanced の対策例を実装する場合は、High-Advanced だけでなく、Advanced 及び Basic に分類されたセキュリティ対策例もカバーしておく必要がある。
・本項に記載している対策例のレベルは、既存の標準におけるレベル別に階層化された管理策をベースに、対策を導入・運用する際のコスト、対策の対象とするスコープ（例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か）等により整理している。
・対策例の実装に際し、主体となる要素を、O「組織」、S「システム」、O/S「システム及び組織」の3つに分類して提示する。
・対策例の記載に当たっては、第Ⅲ部にて各要件に対して割り当てた「関連標準等」に記載の文書および該当項目の一部（本表「参照ガイドライン」という形に示している）を参照している。
・本項に記載の対策例はあくまで一例を示すものであって、他の実装方法を何ら否定するものではない。本資料は、各組織の事業の特性やリスク分析の結果等に応じて、リスク対応を実施する際に参考とされたい。

対策要件ID	対策要件	対応する脆弱性ID	対策例	対策例を実行する主体	参照ガイドライン				
					NIST SP 800-171	NIST SP 800-53 Rev.4	ISO/IEC 27001:2013 付属書A	IEC 62443-2-1:2010	IEC 62443-3-3:2013
CPS.AM-1	・システムを構成するハードウェア、ソフトウェア及びその管理情報（例：名称、バージョン、ネットワークアドレス、管理責任者、ライセンス情報）の一覧を作成し、適切に管理する。	L1_1_a_COM, L1_1_b_COM, L1_1_c_COM, L2_1_a_ORG, L2_3_b_ORG, L2_3_b_SYS	<High-Advanced> ・組織は、自組織の情報システム及び産業用制御システムを構成する資産（IoT機器等を含むハードウェア、ソフトウェア、情報）を一意に特定し、各々の資産に管理責任者を割り当てた上で、資産の構成情報（例：名称、バージョン情報、ライセンス情報、場所等）を含めて、定期的又はオペレータ等の求めに応じて、リアルタイムで状況を把握しながら目録を維持・管理する。 ・情報システムは、組織が定めたベースライン構成に対して、把握された実際の構成が適合しているかを定期的に監査し、例外として組織に許可されているものを除き、接続を遮断する等、適切に対応する。 ・情報システム及び産業用制御システムは、許可されていない資産を自動的に検出し、管理情報から外す・システムから切り離す等を実行するメカニズムを導入、運用している。 ※ 関連する対策要件に、CPS.CM-6がある。 [参考] 重要度の算出方法には、「中小企業の情報セキュリティ対策ガイドライン 第3版」（IPA, 2019年）のP.44～P.46 に記載された情報の機密性、完全性、可用性に関する評価を用いる方法や、「制御システムのセキュリティスク分析ガイド 第2版」（IPA, 2018年）のP.21に記載された事業被害の大きさにおける評価を用いる方法等がある	O/S	○ (3.4.2)	○ (下記に加えて、CM-8(1), CM-8(2), CM-8(3), CM-8(5))	○ (下記に加えて、A.8.1.3)		
			<Advanced> ・資産の構成情報（例：名称、バージョン情報、ライセンス情報、場所等）を含めて、目録を定期的にレビュー、更新することで維持・管理する。 ・組織は、情報システム及び産業用制御システムで利用可能な取り外し可能なメディア（例：USBメモリ）を一覧化し、使用を管理する。 ・組織は、組織内で規定された取り外し可能なメディア（例：USBメモリ）のみを利用し、識別可能な所有者がいないとき、このようなデバイスの使用を禁止する。 ・組織は、機密性の高いデータを含むメディアへのアクセスを制御し、管理エリアの外部へ持ち出しているメディアの利用状況を適切に把握し、管理する。	O					
			<Basic> ・組織は、自組織の情報システム及び産業用制御システムを構成する資産（ハードウェア、ソフトウェア、情報）を特定し、各々の資産に管理責任者を割り当てた上で、目録として一覧を文書化する。		○ (3.4.1, 3.8.5, 3.8.7,	○ (CM-8, PM-5)		○ (4.2.3.4)	○ (SR 7.8)

NIST SP 800-171等、諸外国のガイドライン等との対応関係も整理されています。

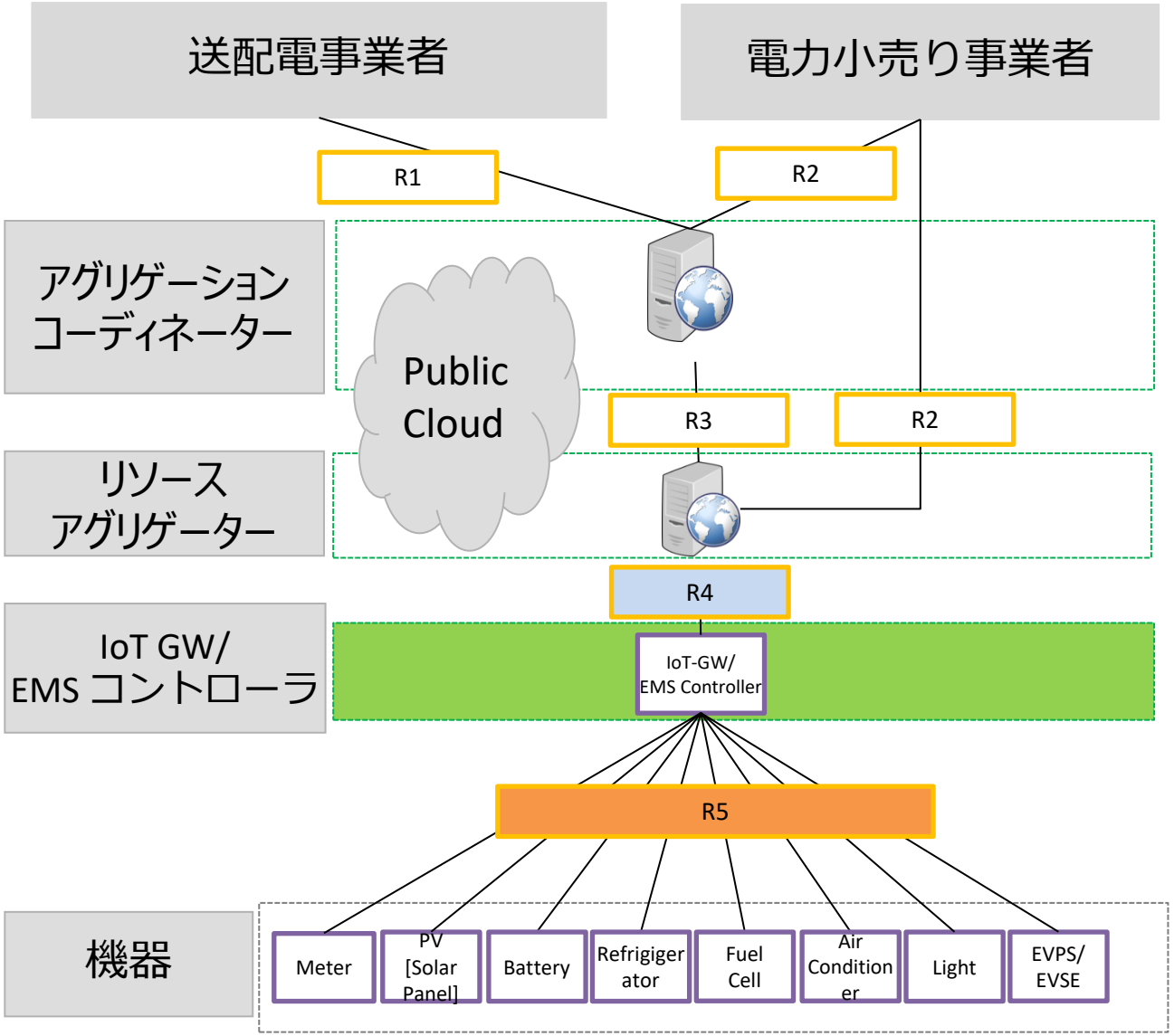
出所）経済産業省,サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）
出どころ：ERABサイバーセキュリティトレーニング

ERABシステムとCPSFの同期



ERABシステムに関するセキュリティアセスメント事例

資源エネルギー庁・IPA(2019)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における規定



R4	【勧告】（事業者とその保有するシステムの対策） ・リソースアグリゲーターの制御対象の機器またはBEMS・HEMS等エネルギーマネジメントシステムは、アグリゲーションコーディネーターと接続する場合において、本ガイドラインに準拠することが必須とされる ことに加え、本ガイドラインに基づきアグリゲーションコーディネーターが別途要件を定義したセキュリティ対策に準拠すること。 ※本ガイドラインは、リソースアグリゲーター、BEMS・HEMS等のサーバーとGW間の通信路 として、公衆網が使われる場合を前提としている。なお、エンドツーエンドで伝送路の安全性・信頼性が確保されているネットワークが使われる場合には、セキュリティ担保を条件に、対策の強度に関して事業者に一定の裁量を認めうるものと考えられる。 （インターフェースの対策） ・外部システムとの相互接続点において認証、通信メッセージは暗号化により保護すること。
R5	【推奨】（事業者とその保有するシステムの対策） ・ERAB制御対象のエネルギー機器、センサには、リソース制約がある機器が存在し、セキュリティ機能の追加・更新が困難な既設の設備等も含まれる。「IoT開発におけるセキュリティ設計の手引き」、「製品分野別セキュリティガイドラインIoT-GW編」等を参照した対策をとること。 （インターフェースの対策） ・外部システム・機器との相互接続点において認証、通信メッセージは暗号化により保護すること。

攻撃ツリー(事例)

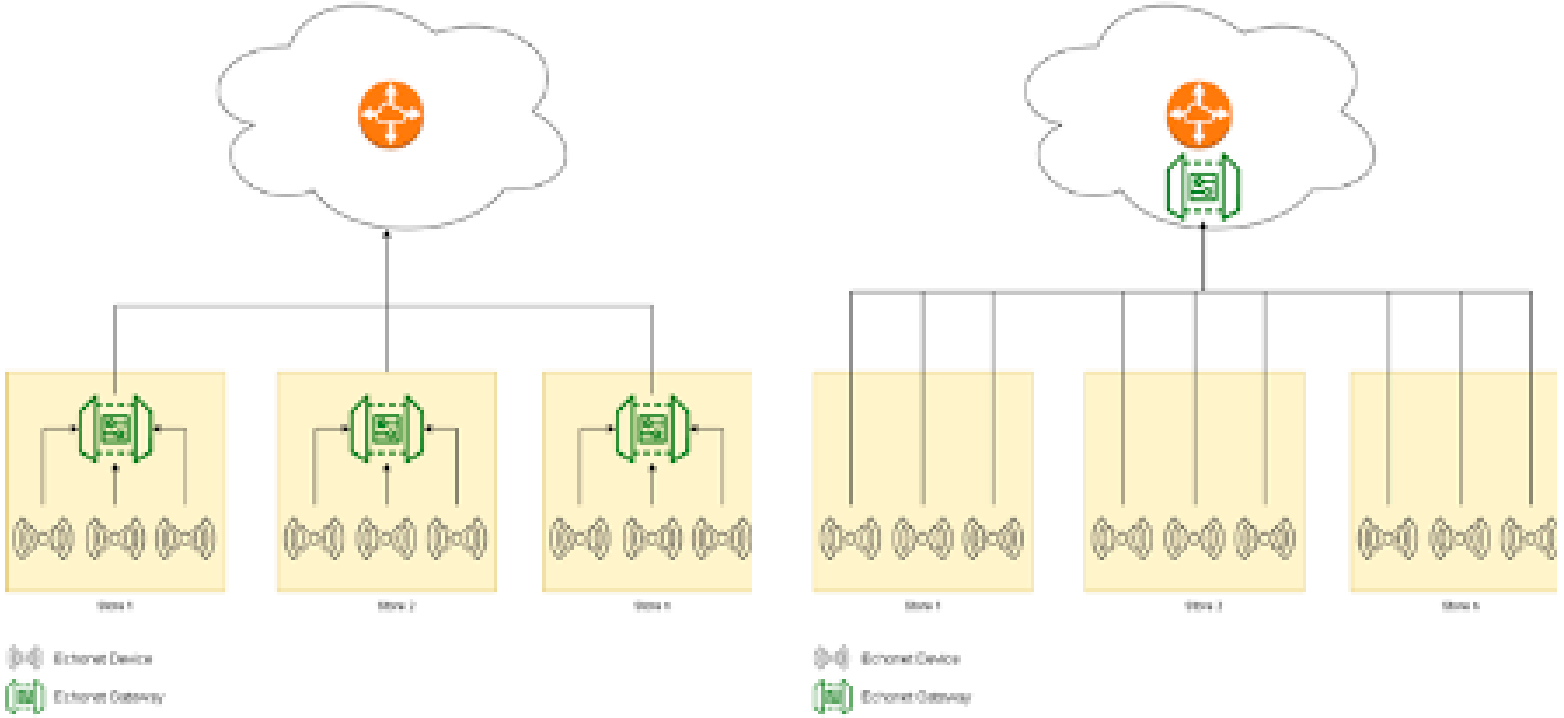
【リスクシナリオ】
悪意ある第三者が、需要家構内の有線/無線LANポートより侵入。DRを無効化する

誰が	どこから	どうやって				どこで		何をする
攻撃者	侵入口	経由1	経由2	経由3	経由4	攻撃拠点	攻撃対象	最終攻撃
悪意のある第三者	有線/無線LANルータ	構内LAN	構内NW接続機器			需要家構内NW接続機器	蓄電池PCS	DRの不成立

需要家構内有線LANポートより侵入		攻撃ステップ
	従業員やシステム管理者へのなりすましによる不正アクセス	攻撃ステップ
	全機器探索でアクセス可能な機器の制御可能なコマンドを入手(蓄電池とスマートメーターの通信情報を入手)	攻撃ステップ
	中間者攻撃で機器へのインプラント攻撃によるデータ改ざんや機器の不正制御	攻撃ステップ
	制御指示が届かずDRサービスが実施不可	最終攻撃ステップ

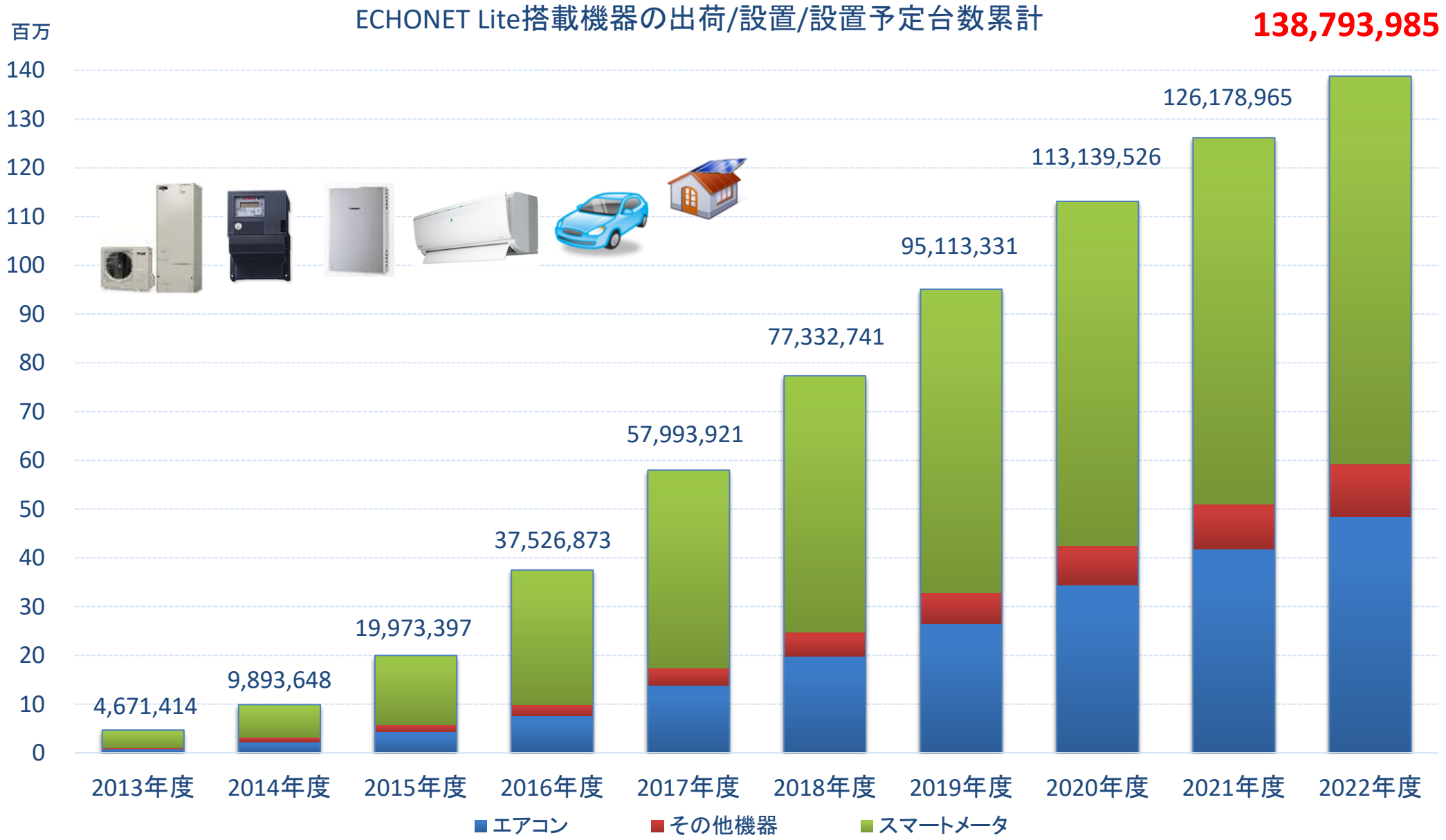
ERABにおける新しいリソースコントロールモデルの普及

- DER-GWは、さまざまな分散電源(DER)からデータを収集・集約
  - DER、IoT デバイス、センサー、その他の機器とクラウド間の通信の橋渡しを担う
  - 物理空間とクラウドを体系的に接続することにより、DER-GWはローカル処理およびストレージ機能に加えて、AIやセンサー入力データに基づいてDERを自律的制御する機能を提供



a Physical GW (left), b Virtual GW (right)

ERABが制御可能な機器の拡大:ECHONET Lite機器も類型1.3億台超

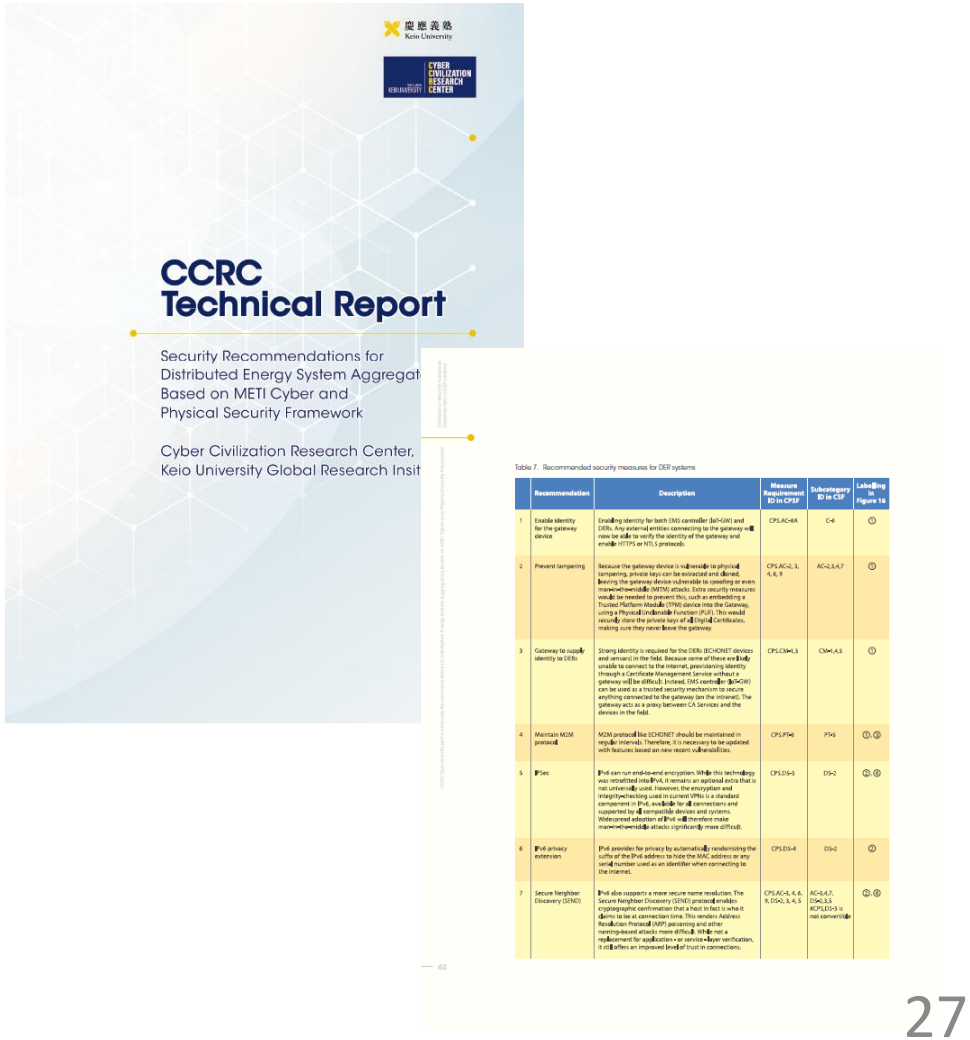


CCRC CONTRIBUTES TO DESIGN ERAB SYSTEM SECURITY

TOKYO, JAPAN
KEIO UNIVERSITY

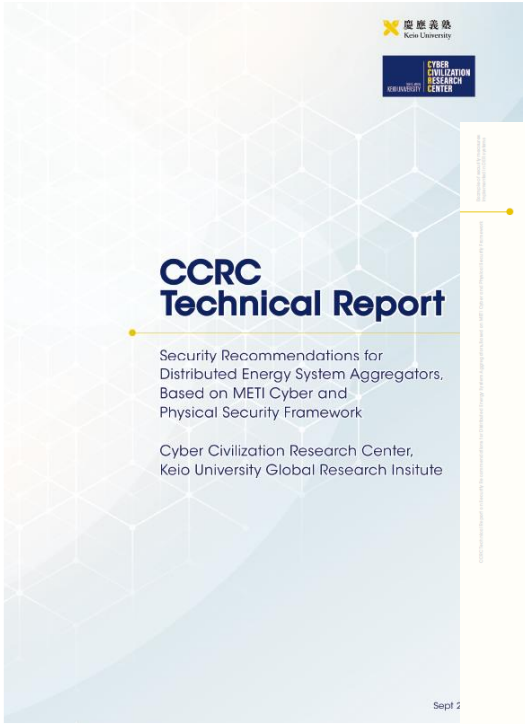
CYBER CIVILIZATION RESEARCH CENTER

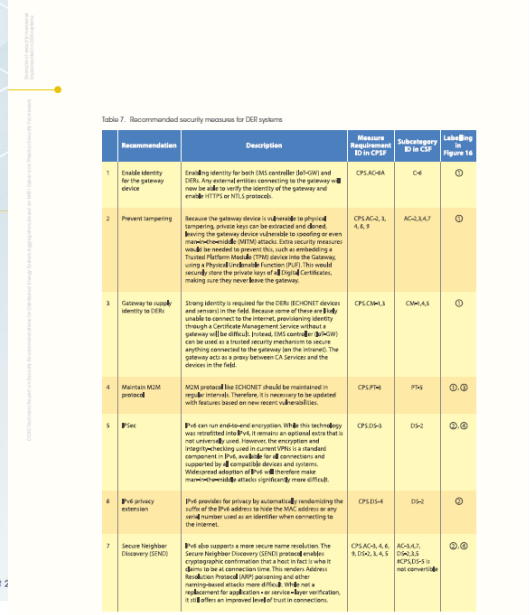
- **CCRCは2021年に「経済産業省のサイバー・フィジカルセキュリティフレームワークに基づく分散型エネルギーシステムアグリゲータに対するセキュリティ推奨に関する技術報告書を発行し、ERABシステムの主要な脆弱性への対策となる51の推奨事項を示した。**
  - The report is backed by 5 years experience of running a prototype of ERAB system
  - The full report is available at
    - https://www.ccrc.keio.ac.jp/ccrc-technical-report-202109/

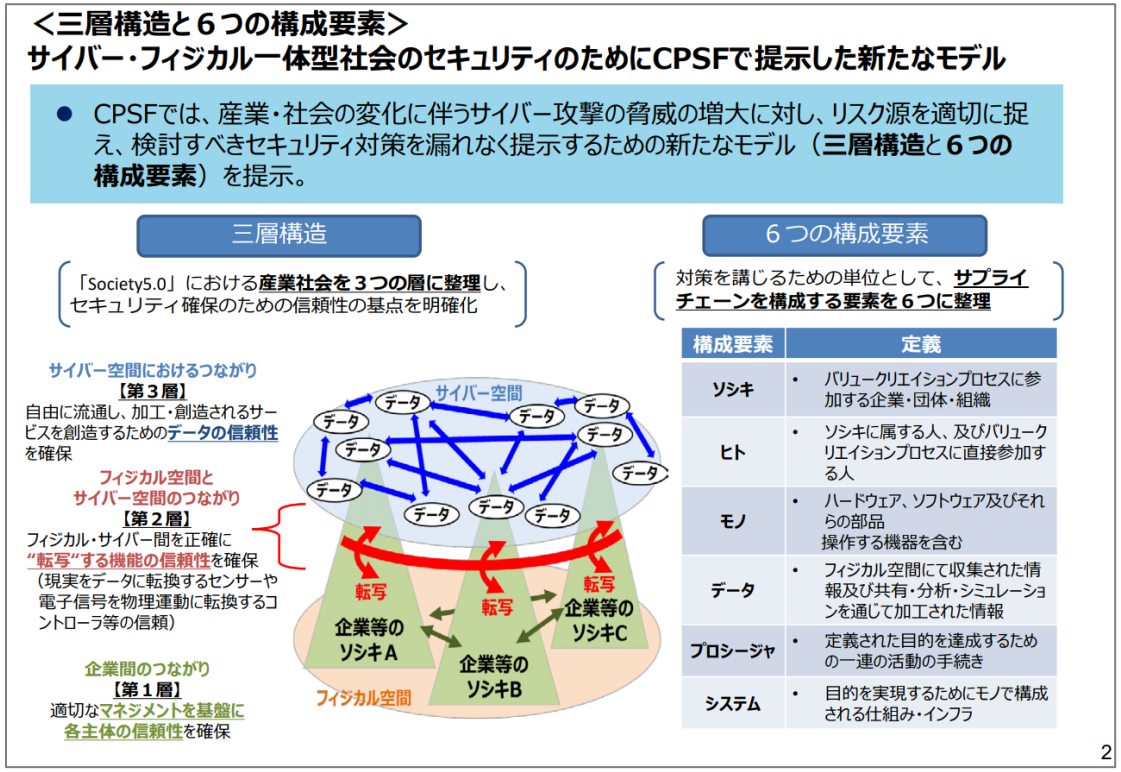


CPSFに基づくリスク分析からの対策事例

- リスクアセスメントの実施は重要インフラに求められている。CCRC Technical Report(2021)は、経済産業省の「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）」に基づき、ERABシステムを三層構造に分解の上、**事業被害と発生頻度の両面から影響が大きいリスクを抽出**
  - https://www.ccrc.keio.ac.jp/wp-content/uploads/2021/09/Appendix-DERs.pdf
  - 本文は、https://drive.google.com/file/d/1Q5pKsbNZ4HDvvybGDhovOjUPzvw7DD5F/view
  - 注)前提となるシステムが2021年当時







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）のポイント」より