Deloitte.
デロイト トーマツ

電力分野のサイバーセキュリティ対策の近況について

～令和７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向上に向けた調査)～

デロイトトーマツ サイバー合同会社

2026年2月12日

MAKING AN IMPACT THAT MATTERS since 1845

電力分野のサイバーセキュリティ対策の取組

電力分野のサイバーセキュリティ対策の全体像・近況について（前提）

調査の前提

本資料の位置づけ

1. 本資料は、再生可能エネルギー主力電源化に向け、サイバーセキュリティ対策が重要な課題となっている中で、**分散型電源を運用する発電事業者や、アグリゲーターなど新規プレーヤーに求められるサイバーセキュリティ対策の課題を明確化するため、考慮すべきサイバー脅威の事例や、先行している国外の関係施策**を整理して、日本の現状と比較することによりＳＷＧでの議論に資するもの
2. 説明項目
   - ■ **国内外での電力関連サイバーインシデントの紹介**
   - ■ **国外（米・英）及び国内の施策の紹介**

※なお、本資料はデロイト トーマツ サイバー合同会社が、資源エネルギー庁様より受託している「令和７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向上に向けた調査）」の調査結果の一部をＳＷＧの資料として再構成したものである

「令和７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向上に向けた調査）」の目的

再生可能エネルギー主力電源化に向け、サイバーセキュリティ対策が重要な課題となっている中、本事業では、**電力システム全体のサイバーセキュリティの確保に向けて、大手電力会社に加え、分散型電源を運用する発電事業者や、アグリゲーターなど新規プレーヤーに求められるサイバーセキュリティ対策の課題を整理するとともに、必要な施策を検討する**
そのため、日本国内の状況、また、海外における取組状況の実態調査等、必要な調査・分析を行うとともに、具体的な制度設計等に向けて、電力分野におけるワーキンググループ等において議論・検討を進める

電力分野におけるインシデントと各国の対策

インシデント情報の公開以降も、太陽光発電設備の脆弱性対応をしていない設置者・管理者が多数存在します

既に発生した機器の脆弱性に対する対応状況調査結果

- 2024年5月、太陽光発電設備向け遠隔監視機器の約800台がサイバー攻撃を受け、インターネットバンキングの不正送金の踏み台として悪用された。
  攻撃を受けた製品の既知の脆弱性が攻撃に悪用されたことが原因である
  ※本件は第17回電力SWGでも紹介・周知されている
- 上記インシデント事例は既出事例であることから、あるべき姿として、公開済みの脆弱性が存在する機器に対するパッチ適用などの対応が必要である
  （既に発見・公開された脆弱性であり、対応しないと事例と同様に攻撃され、被害が発生する可能性が高い）
- 当該あるべき姿を検証すべく、当社にて以下深掘調査を実施した

深堀調査[*6]	調査内容	過去インシデントが発生した同様の機器への対策は実施されているか
	調査結果	■ インターネット上で観測される上記インシデント発生機器のシリーズと推定される機器について、既知の**脆弱性に対応されていない可能性がある機器が159件確認**された ■ そのうち、**深刻な脆弱性に対応されていない可能性がある機器が34件確認**された

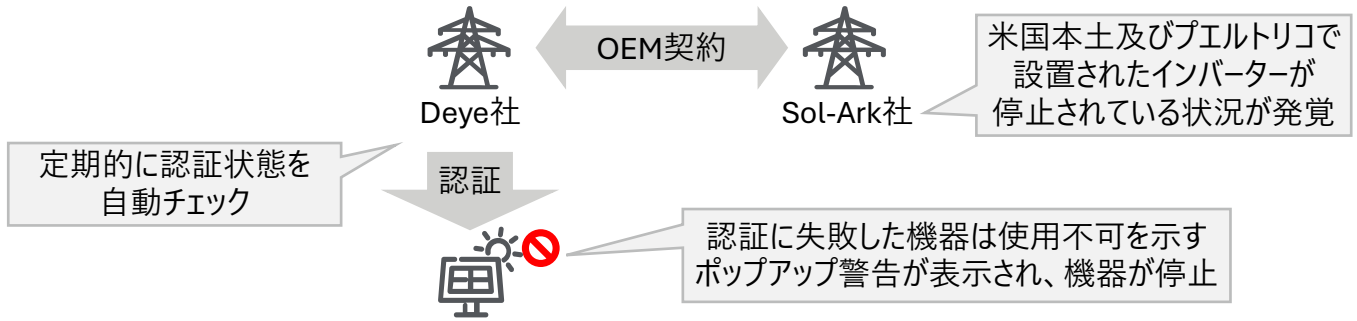
現状（問題点）	設置された機器の脆弱性対応を実施していない**設置者・セキュリティ管理者**が多数存在している

*6：“Search Engine for the Internet of Everything”, 閲覧日：2025年11月, https://www.shodan.io/

意図的に組み込まれた機能やハードウェアにより購入後に制御権を失うリスクがあります

組み込まれた機能に起因するインシデント事例

インシデント事例[*3]

発生時期	2024年11月
概要	米国Sol-Ark社ブランド又はSol-Ark社システムで使用されている中国Deye社製の**太陽光発電用インバーター**が、インターネット経由の**認証機構により一部停止**される事例が報告された
原因	当該インバーターにはDeye社による**認証チェック機構**が組み込まれており、UL認証を取得していない等米国の基準を満たさない機器が流通・設置された場合、**不正流通品と判定された機器を自動的に停止する仕組みが作動**したため、今回の停止に至ったとされている
被害	■ 停止されたインバーターが接続された太陽光発電設備が一時的に発電不能となった ■ 発電事業者や家庭が発電できなくなり、現場対応や復旧作業が必要となった
イメージ（詳細）	

現状（問題点）	製品機器購入後、設置者の意図に反した遠隔制御が可能な機能が実装されている

*3：heise online, “Photovoltaics: Deactivated Deye and Sol-Ark inverters in the USA”, 閲覧日： 2026年1月28日, https://www.heise.de/en/news/Photovoltaics-Deactivated-Deye-and-Sol-Ark-inverters-in-the-USA-10183716.html

開発段階からユーザーが運用・保守する段階までライフサイクル全体での考察が必要です

ライフサイクルの各段階での国内の現状や各国の対策

工程	機器開発・製造	運用・保守
現状	■ セキュリティ対策が不十分な機器が市場に流入 ■ 遠隔制御の普及により、電力設備の構成要素としてIoT機器が増加	■ 個人や小規模事業主が分散型電源の設置者となって運用・保守サービスを利用する機会が増加 ■ 電力サプライチェーンが複雑化し、機器やサービスを制御するプレイヤーが増加
脆弱性	■ セキュリティ対策を意識せず機器を購入する設置者 ■ 電力設備を構成する機器のインターネット接続	■ セキュリティの知識がない設置者や対策資金が十分でない設置者が管理する設備 ■ 組織的なセキュリティ対策を実施することが困難で、機器やサービスの選定に際して適切な判断ができない設置者
脅威	■ 脆弱性を利用した機器の乗っ取りや機器の停止	■ 誤設定や脆弱性を突いた不正アクセス・不正制御
影響	■ 適切でない機器の選択により、系統連系後のインシデント発生時に電力供給へ影響	■ 適切でない運用・保守サービス事業者の選択により、インシデント発生時に電力供給へ影響
各国の対策	■ UL 2941（米） ■ ETSI EN 303 645（英） ■ JC-STAR制度（日）	■ カリフォルニア州公益事業委員（CPUC）への登録（米） ■ Smart Secure Electricity Systems Programmeにおけるライセンス取得（英） ■ 特定卸供給事業にかかる経済産業大臣への届出（日）

サプライチェーン全体でのセキュリティ向上に向けた対策の動向を紹介します

電力関係のインシデントと各国の対策のまとめ

【主要な変化要因】

- 紹介したインシデント事例を踏まえると、分散型電源等のIoT機器に対するリスクが近年顕在化していると言える
- 具体的には、電力機器に対する不正な遠隔操作により、最悪の場合、電力の需給調整に影響する可能性がある。
  また、乗っ取られた機器が踏み台となり第三者が攻撃を受ける場合も考えられる

【検討の方向性】

- 分散型電源のセキュリティ対策を検討するには、開発・製造から保守・運用までを含めたサプライチェーン全体を考察の範囲とする必要がある
- 各国において、開発・製造と保守・運用でそれぞれ対策が行われているため、以下のスライドで紹介する

各国における対策

米国

英国

日本

開発・製造 運用

各国でDERの機器に対する認証制度の適用が進められています

各国の新規プレイヤー（機器メーカー）に対する規制：開発・製造時の認証

- 機器に対して各国で認証取得を条件とする制度の検討が進められている
- 機器メーカーの過度な負担とならないように相互認証の推進が必要とされている

	米国	英国	日本
規格	UL2941	ETSI EN 303 645	JC-STAR制度
対象機器	Distributed Energy and Inverter-Based Resources 分散型電源及びインバーターリソース	Energy Smart Appliance（ESA） 蓄電池、EV充電器、給湯器等	太陽光発電設備、蓄電設備
認証方法	第三者評価	自己評価＋OPSSによる認証	自己評価＋IPAによる認証
制度化状況	■ 米国国家規格（ANSI）認定の手続きが進行中 ■ 規格に認定されれば、州規制当局や系統運用者によって必須の連系要件として採用される見通し	■ Smart Secure Electricity Systems Programmeにおいて、2026年が準備期間となり、2027年度に必須化となる見通し	■ 太陽光発電設備、蓄電設備については、2027年4月に系統連系技術要件にて必須化 ■ その他の設備は今後適用時期を検討

各国で機器制御事業者の登録やライセンス制が導入されています

各国の新規プレイヤー（アグリゲーター等）に対する規制：機器を運用する事業者のライセンス

- 機器を制御する事業者に対して各国でライセンス取得を条件とする制度の検討が進められている
- 諸外国では電力供給や事業規模にかかわらず規制対象だが、日本では一定規模以上の電力供給を行う事業者のみが規制対象である

	米国（カリフォルニア州）	英国	日本
規制	カリフォルニア州公益事業委員（CPUC）への登録	Smart Secure Electricity Systems Programmeにおけるライセンス取得	特定卸供給事業にかかる経済産業大臣への届出
対象事業者	デマンドレスポンスや、電気料金削減、市場への卸供給などのサービスを提供する事業者	DER機器に対し、以下を行う事業者 • 機器制御信号の生成 • 機器制御信号の変更 • 機器制御信号の送信タイミングの制御	分散型エネルギーリソースの供給力を集約して小売事業者等に電気を供給する一定規模以上の事業者（特定卸供給事業者）
電力供給	**電力供給の有無にかかわらず対象**	**電力供給の有無にかかわらず対象**	**電力供給を行う事業者のみ対象**
事業規模	**規模にかかわらず対象**	**規模にかかわらず対象**	**一定規模以上のみ届け出必要**
認証方法	届け出＋宣誓	Ofgemによる認証	届け出制
セキュリティ要件	• プライバシー、データセキュリティに関する規則への準拠	• CAFプロファイル年次報告 • 第三者監査 • 重大なインシデント報告	• 「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」への準拠
備考	運用しているDERのうち、UL2941の認証を取得しているDERの割合が90パーセント以上である事業者に限定した資金調達プログラムも開始されている	2026年に申請が開始し、2027年度に必須化となる見通し 制御対象が300MWを超える事業者は、重要サービス事業者(OES)としてNIS規制の対象となる	特定卸供給事業者以のERABに参画する事業者も対象としたガイドライン（＊）が施行済みだが、認定や事業者登録等の届け出は不要

各国における対策
米国
英国
日本

米国では、DERのサイバーリスクに対してセキュリティ標準化が進められています

米国の分散型エネルギー資源の増大に伴うサイバーセキュリティ動向

背景

- 再生可能エネルギー技術の導入が加速するにつれて、電力系統には、太陽光発電（PV）システムや蓄電装置といった分散型エネルギー資源（DER※）と、これらを制御するシステムとの相互接続が増加している

※米国の分散型エネルギーリソース（DER）には燃料電池、太陽光発電、風力タービン、マイクロタービン、その他の分散型エネルギー資源、EPSに接続され、一次又は二次配電電圧レベルで相互接続された分散型エネルギー貯蔵システムが含まれる。日本の分散型エネルギー資源と同義とする。

- この分散化とデジタル化の進展は、電力供給のレジリエンスと持続可能性を高める一方で、**サイバーセキュリティの脅威に対する系統全体の脆弱性を増大させている**と考えられている
- **制御システムに対するサイバー攻撃は系統の安定性に直接影響を及ぼす潜在的リスク**となっているため、セキュリティ強化は喫緊の課題となっている
- 既に複数の州で採用されている、電気的な安全性・製品機能を要求する規格等（**IEEE 1547-2018**, **UL 1741 SB**）では、**サイバーセキュリティに関する要求**が不足している

動向

- DERが引き起こす固有のサイバーリスクに対処するため、製品レベルからシステム運用レベルに至る**包括的なセキュリティ標準化フレームワークの確立が不可欠である**との認識のもと検討が進められている
  - ➢ このフレームワークの主要な柱として、**UL Solutionsが提供するUL 2941**と、**IEEEが策定したIEEE 1547.3**が存在し、それぞれ異なるレイヤーと役割を担っている
- UL 2941とIEEE 1547.3は、ともに米国エネルギー省（DOE）の支援を受け、国立再生可能エネルギー研究所（NREL）との協力体制のもとで開発が進められている

DERの安全性・製品機能及びサイバーセキュリティに関するガイドライン・規格があります

米国における分散型エネルギー資源に関するガイドライン・規格

■ DERに係る電気的な安全性・製品機能に関する基準はIEEE 1547-2018及びUL 1741 SB※が該当する

※IEEE1547-2018に基づく全ての機能・通信要件が追加されたより高度な機能・通信要件

■ DERに係るサイバーセキュリティ関連の基準はIEEE 1547.3-2023及びUL 2941が該当する

		目的	適用主体	適用範囲	位置づけ
電気的な安全性・製品機能	**IEEE 1547-2018** 2018年公開	DERと電力システムの相互運用性に関する統一された標準を提供する	DERの電力系統への連携・相互運用に係るステークホルダー	電力系統に接続するDER及び関連設備	ガイドライン
電気的な安全性・製品機能	**UL 1741 SB** 2021年公開 2025年改訂	**DER用インバーターの基盤規格**であり、IEEE1547-2018の要件に準拠できる能力を有している製品であることを認証する	DERメーカー	DER用インバーター	**規格（第三者認証）**
サイバーセキュリティ関連	**IEEE 1547.3-2023** 2023年公開	電力システムと相互接続されているDERに対するサイバーセキュリティの標準を提供する	DERの監視、情報交換、制御システムを扱うステークホルダー	DER及びDERと相互接続するシステム	ガイドライン
サイバーセキュリティ関連	**UL 2941** 2023年公開	**DER用インバーターのセキュリティ規格**であり、求められるセキュリティ要件に準拠できる能力を有していることを認証する	DERメーカー	DER用インバーター	**規格（第三者認証）**

開発・製造 運用

安全性・製品機能に関する規格と同様にセキュリティに関する規格も採用されつつあります

米国におけるDER機器に関する規格の採用状況

	電気的な安全性・製品機能 UL 1741 SB	サイバーセキュリティ関連 UL 2941
採用事例	■ **米国の10個の州**（オレゴン州、カリフォルニア州、ユタ州、ニューメキシコ州、ミネソタ州、ニューヨーク州、バーモント州、マサチューセッツ州、メリーランド州、デラウェア州）*9において、規制委員会又はすべての規制対象となる系統運用者が、**IEEE 1547-2018の採用プロセスを完了**している ■ 上記の10州では、**規格（UL 1741 SB）に準拠したDER機器等が必須となる日程を公表**している	■ 米国で最大規模のDER市場のカリフォルニア州では、カリフォルニア州エネルギー委員会（CEC）が主導する**仮想発電所（VPP）に関する主要な資金調達プログラム（GFO-25-302:CHOIR**がある ■ そのプログラム参加要件として、VPPを構成するDERのうち、**UL2941の認証を取得しているDERの割合が90パーセント以上であること**[*10]が求められています
傾向	他の州においても、規制委員会が、現在IEEE 1547-2018を採用するプロセスを進めている。これには、公式な採用プロセスを経たものの、規格（UL 1741 SB）に準拠したDER機器等の市場での供給が不足しているために採用を延期した州などが含まれている	現時点で、UL2941は規制当局による義務化措置には採用されていないが、ANSI（米国国家規格協会）認定に向けて手続きが進められている過渡期にある*11。認定されれば採用が進むと考えられている
	DER機器の安全性認証（UL 1741）は既に州規制当局や系統運用者によって必須の連系要件として採用されている	DER機器の安全性認証（UL 1741）と同様に、将来的に州規制当局や系統運用者によって必須の連系要件として採用されることが予想されている

*9：“IRTC, IEEE 1547-2018™ 採用トラッカー”， 閲覧日：2026年1月28日， https://irecusa.org/resources/ieee-1547-2018-adoption-tracker/
*10： “カリフォルニア州， VPPに関する主要な資金調達プログラム”， 閲覧日： 2026年1月28日，
https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.energy.ca.gov%2Fsites%2Fdefault%2Ffiles%2F2025-10%2F00_GFO-25-302_Applicaton_Manual_ada.docx&wdOrigin=BROWSELINK
*11：“ANSI, Proposed American National Standards”， 閲覧日：2026年1月28日，
https://share.ansi.org/Shared%20Documents/Standards%20Activities/American%20National%20Standards/Approved%20and%20Proposed%20ANS%20Lists/Proposed%20ANS.pdf

カリフォルニア州ではDRPやアグリゲーター等に対し、CPUCへの登録を義務付けています

カリフォルニア州におけるアグリゲーターへの規制

概要

- 米国カリフォルニア州では、デマンドレスポンスプロバイダー（以下、DRP）/アグリゲーターに対し、**カリフォルニア州公益事業委員会（以下、CPUC）**[*13]の事業者登録を義務付けている
- 事業者は登録に際し、**申請フォーム**[*14]をCPUCへ提出し、事業者の適性が審査され、承認後、事業者はCPUCの公式リストに登録され、州内での事業活動が可能となる

対象

DRP/アグリゲーター：需要家の機器を制御し、電力消費削減支援サービスを提供する事業者。複数の需要家をまとめて制御し、電力会社や市場に対して調整力を提供する事業者

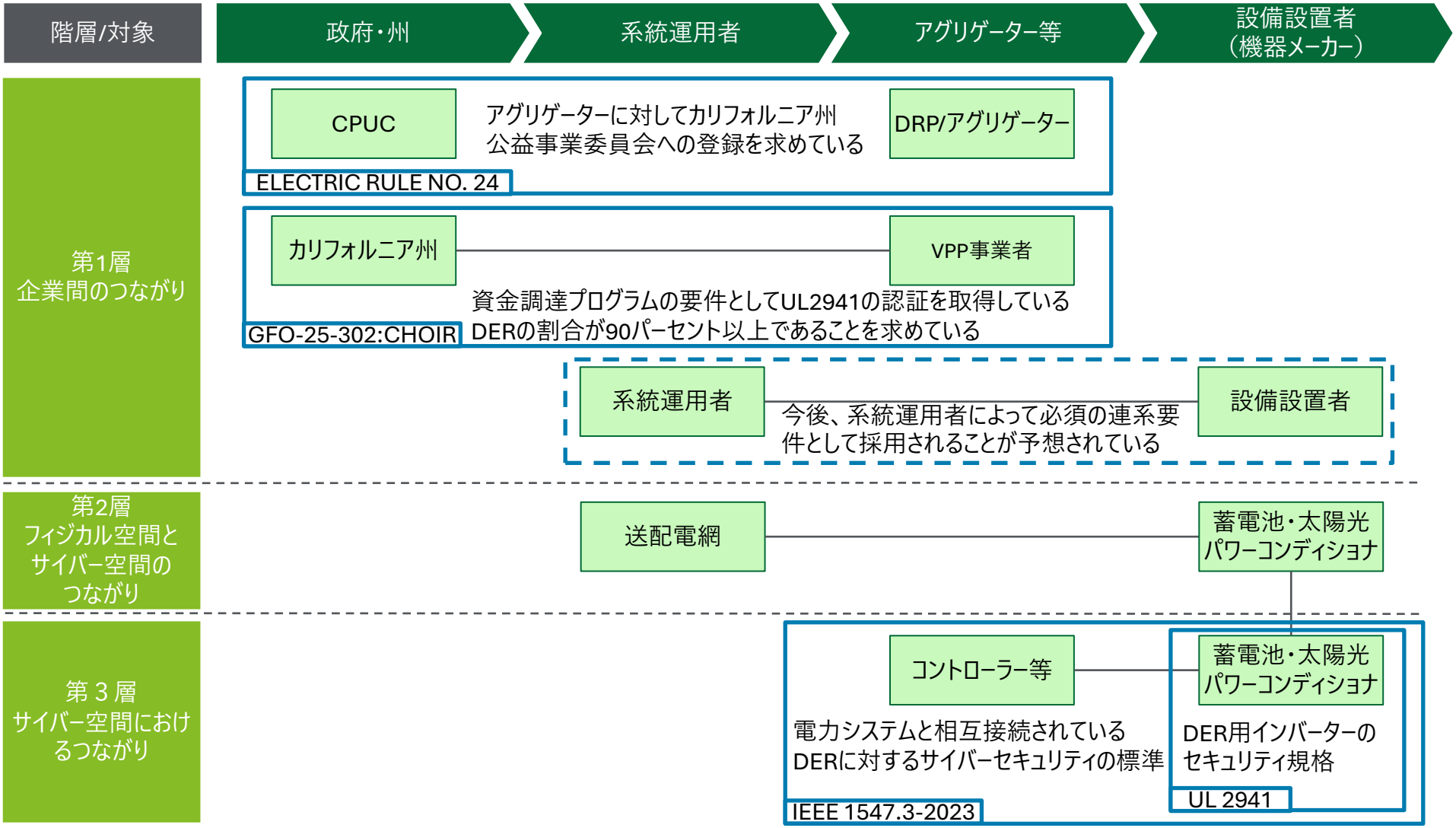
セキュリティ要件

- **米国カリフォルニア州大手電力会社（PG&E、SCE及びSDG&Es）が定める規則**[*15]の準拠（以下一部抜粋）が要求される
  - 顧客データの保護：顧客の住所や電力消費データ等を含む個人情報を適切に管理するためのセキュリティ対策及びプライバシー保護の実施
  - CPUCへの報告義務：事業者が保有する顧客情報への認可した第三者のアクセス件数や当該規則の違反件数等の年次報告

*13：“CPUC”， 閲覧日：2026年1月28日， https://www.cpuc.ca.gov/industries-and-topics/electrical-energy/electric-costs/demand-response-dr/drp-registration-information
*14：“申請フォーム”， 閲覧日：2026年1月28日， https://www.cpuc.ca.gov/-/media/cpuc-website/divisions/energy-division/documents/demand-response/drp-registration-information/drp-registration-form_revised_0208106.pdf
*15：“規則”， 閲覧日：2026年1月28日， https://www.cpuc.ca.gov/-/media/cpuc-website/divisions/energy-division/documents/demand-response/list-of-registered-demand-response-providers-drps_aggregators-and-faq/decision-d1107056.pdf

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）を参照し、対象ごとのつながりを整理しました

CPSFによる整理



各国における対策

米国

英国

日本

開発・製造 運用

英国ではDERの安全性・製品機能、サイバーセキュリティに関する枠組みが検討中です

英国の分散型エネルギー資源の増大に伴うサイバーセキュリティ動向

背景

- 再生可能エネルギー技術の導入が加速するにつれて、電力系統には、家庭用電気自動車充電ポイント（EVSCPs）や蓄電装置といった分散型エネルギー資源（DER）とこれらを制御するシステムとの相互接続が増加している
- 中でも以下への対策の必要性が高まっている[*16]
  1. サイバーセキュリティリスク
  2. 電力系統の安定性のリスク
  3. 相互運用性の欠如によるリスク
  4. 新たなビジネスモデルや技術の普及に伴う規制の遅れ

動向

- 上記のようなリスクを鑑み、英国政府は機器とシステムの安全性、また機器の相互運用性を確保するための標準化や規制整備の必要性を認識している
- 政策検討・準備が2022年から開始され、**Smart Secure Electricity Systems (SSES) Programme （以下、「SSESプログラム」）**が立ち上がった
  - SSESプログラムの開発段階にあり、現段階ではプログラムにおけるガバナンス体制や計画を設計・準備している
  - 2026年から2029年半ばには移行フェーズになり、DERのうち、蓄電池やEV充電機器等を含む**エナジースマートアプライアンス（以下、「ESA」）**に対する認証制度や、ESAを制御する事業者（**以下、「LC」**）と呼ばれる事業者に対するライセンス取得が実施される
  - 2029年以降には運用フェーズに入り、ESAの相互運用性に応じたセキュリティ要件の追加や実装が予定されている[*17]

*16：“Smart Secure Electricity Systems (SSES) Programme”， 閲覧日：2026年1月28日， https://assets.publishing.service.gov.uk/media/6808a2630324470d6a394eb2/SSES-consultation-response.pdf

*17：“Consultation outcome Smart Secure Electricity Systems (SSES) Programme: Enduring Governance (accessible webpage)”， 閲覧日：2026年1月28日，https://www.gov.uk/government/consultations/smart-secure-electricity-systems-programme-sses-enduring-governance/smart-secure-electricity-systems-sses-programme-enduring-governance-accessible-webpage

開発・製造 運用

SSESプログラムではLC及びESAメーカーが規制対象となります

SSESプログラムの概要・対象・検討状況

概要

- エネルギーシステムのスマート化と分散化を推進しつつ、サイバーセキュリティや設置者保護の強化を目指す取り組み
- 設置者がより安価な電力へアクセスできるようにするための技術・規制的枠組みを構築する取り組み

対象

① **LC**

② **ESAメーカー**

検討状況

- 機器に対する規制として、DERのうち、蓄電池やEV充電機器等を含むESAに対する認証制度の適用を検討中
- 組織に対する規制として、LCに対するライセンス制度（以下、「LCライセンス」）の適用を検討中

開発・製造 運用

SSESプログラムは段階的に規制を導入する計画になっています

SSESプログラムのスケジュール

SSESプログラムの実施スケジュール*18

対象/時期※1	2026年	2027年	2028年	2029年	2030年

※1: 移行期間と各規制開始時期は現時点で一部定まっていないため、以下はあくまでスケジュールの一部を抜粋して参考として記載

LC

LCライセンス導入に向けた移行期間
LCライセンス申請受付開始

LCライセンスの施行開始

■ 以下の要件に適合することを義務付け

- Cyber Assessment Framework基準への準拠状況の年次報告
- 第三者監査の実施
- 重大なインシデント報告
- 違反が特定された場合は、是正措置計画を実施し、遵守達成のために取られている措置の証拠の提出

ESAメーカー

ESA認証取得に向けた移行期間
約20か月のESA認証導入準備期間

ESAデバイス規則の施行開始

■ 以下の要件に適合することを義務付け

- ETSI EN 303 645（民生用IoTサイバー機器のサイバーセキュリティに関する欧州規格）への準拠※2
- ランダム遅延の導入の義務付け

※2: ETSI EN 303 645は、民生用IoT機器のサイバーセキュリティセキュリティパッチに関する欧州規格であり、ソフトウェアの自動アップデート機能の適用が推奨されている

*18：“Smart Secure Electricity Systems (SSES) Programme”， 閲覧日：2026年1月28日， https://assets.publishing.service.gov.uk/media/6808a2630324470d6a394eb2/SSES-consultation-response.pdf

開発・製造 運用

ETSI EN 303 645は欧州において全ての民生用IoT機器に適用される基本的な規格です

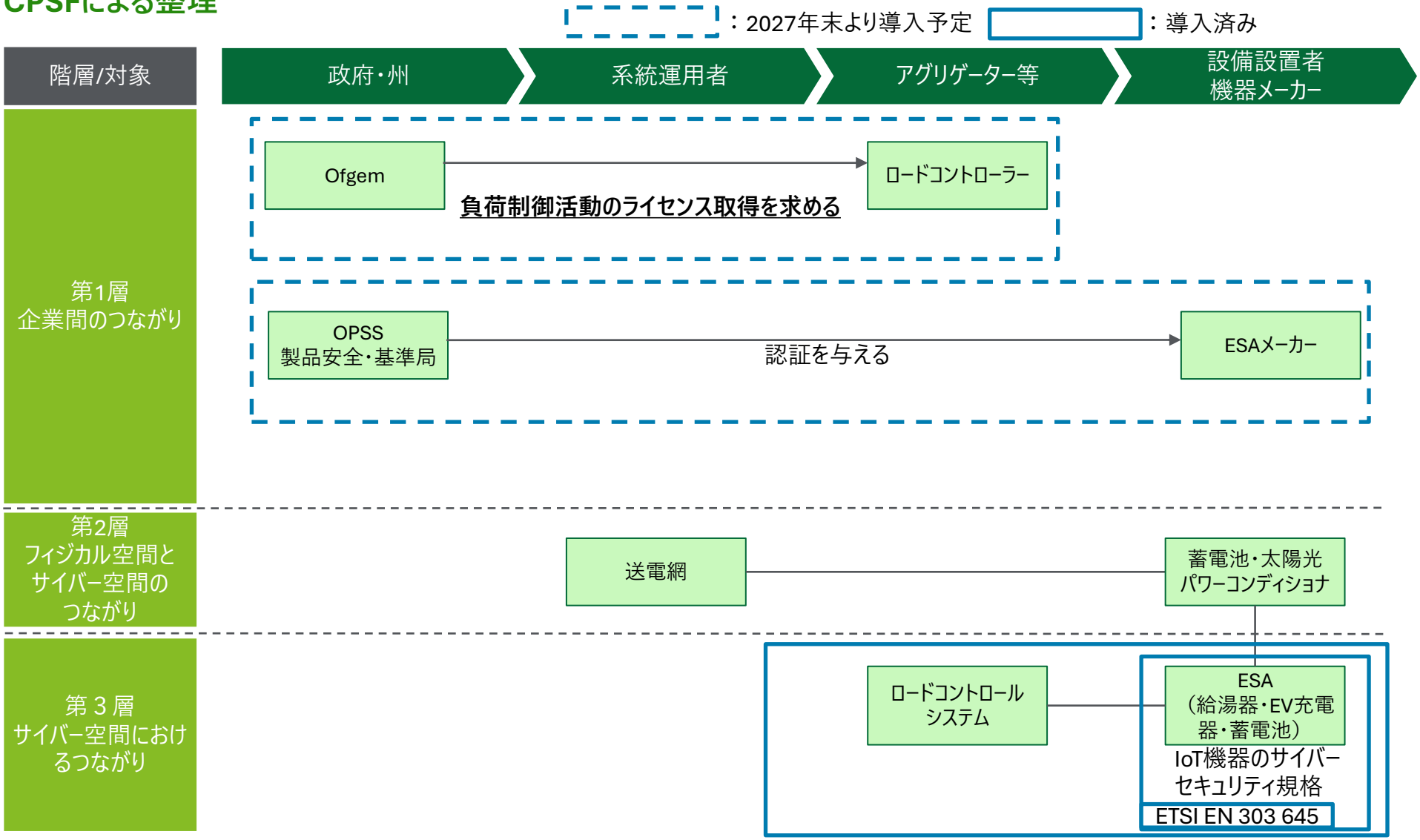
ETSI EN 303 645の概要

概要	■ 2022年6月に欧州電気通信機構（ETSI）が発表した、ネットワークインフラ（インターネットやホームネットワークなど）に接続される民生用IoT機器と、その関連サービスとのやりとりに関する高レベルのセキュリティ及びデータ保護に関する規格 ■ 消費者向けのIoT機器としては初めてグローバルに適用される規格
目的	■ 民生用 IoT 機器の開発・製造に 関わるすべての関係者に、製品をセキュアにするガイダンスを提供すること ■ 消費者に対して、ETSI EN 303 645[*19]に適合した製品を選択することで、消費者が直面する可能性のあるIoTサイバーセキュリティリスクを軽減すること ■ 製造者に対して、ETSI EN 303 645はフレームワークを提供し、自社の製品が要求事項を満たすように設計されていることを保証すること
対象	■ 家庭や個人向けのインターネット接続機器[*20]（スマートホーム製品・ウェアラブルデバイス・カメラ・ルーター等）
補足	■ 欧州のみならず、世界のIoTセキュリティ標準化にも影響を与えており、多くの国や企業が参考にしている ■ 日本では、IoT製品に対する適合基準への適合性を確認・可視化するために作られた、JC-STAR制度の参考にもされている[*21]

*19：“ETSI EN 303 645 V2.1.1”， 閲覧日：2026年1月28日， https://www.ipa.go.jp/security/controlsystem/hjuojm000000418j-att/000108215.pdf
*20：DEKRA 100， ” ETSI EN 303 645準拠セキュリティアセスメント”， 閲覧日：2026年1月28日， https://www.dekra.co.jp/ja/etsi-en-303645-for-iot-security/
*21：IPA， “セキュリティ要件適合評価及びラベリング制度（JC-STAR）”， 閲覧日：2026年1月28日， https://www.ipa.go.jp/security/jc-star/index.html

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）を参照し、対象ごとのつながりを整理しました

CPSFによる整理



各国における対策

米国

英国

日本

開発・製造 運用

日本では、DERのサイバーリスクに対してセキュリティ標準化が進められています

日本の分散型エネルギー資源の増大に伴うサイバーセキュリティ動向

背景

- 再生可能エネルギー技術の導入が加速するにつれて、太陽光発電（PV）システムや蓄電装置などの**分散型エネルギー資源とシステムを相互に接続するエネルギーアグリゲーションビジネスが増加**している
- この分散化とデジタル化の進展は、電力供給のレジリエンスと持続可能性を高める一方で、実際に**太陽光発電設備の遠隔監視装置が複数乗っ取られるサイバーインシデントが発生**するなど、**系統全体の脆弱性を増大させる要因**となりうると考えられている
- 一方、設置された機器の**脆弱性対応を実施していない設置者やセキュリティ管理者が多数存在**するなど、**設置者のリテラシーに依存したセキュリティ対策のみでは不十分**な状況である

動向

- **設置者のリテラシーのみに依存しないセキュリティ対策**の一つとして、基本的なセキュリティ対策が実施された機器を使用することを目的とし、**設置する機器に対するJC-STAR制度の適用**が検討されている
- 設置される機器だけでなく、分散型エネルギーリソースの供給力を集約して小売事業者などに電気を供給する一定規模以上の事業者（**特定卸供給事業者**）について、**届出制とするとともに、「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」への準拠**が求められている
- また、一定規模に達しない事業者や電気の供給を伴わない制御を行う事業者に対しても「**ERABに関するサイバーセキュリティガイドラインVer3.0**」が公開された

開発・製造 運用

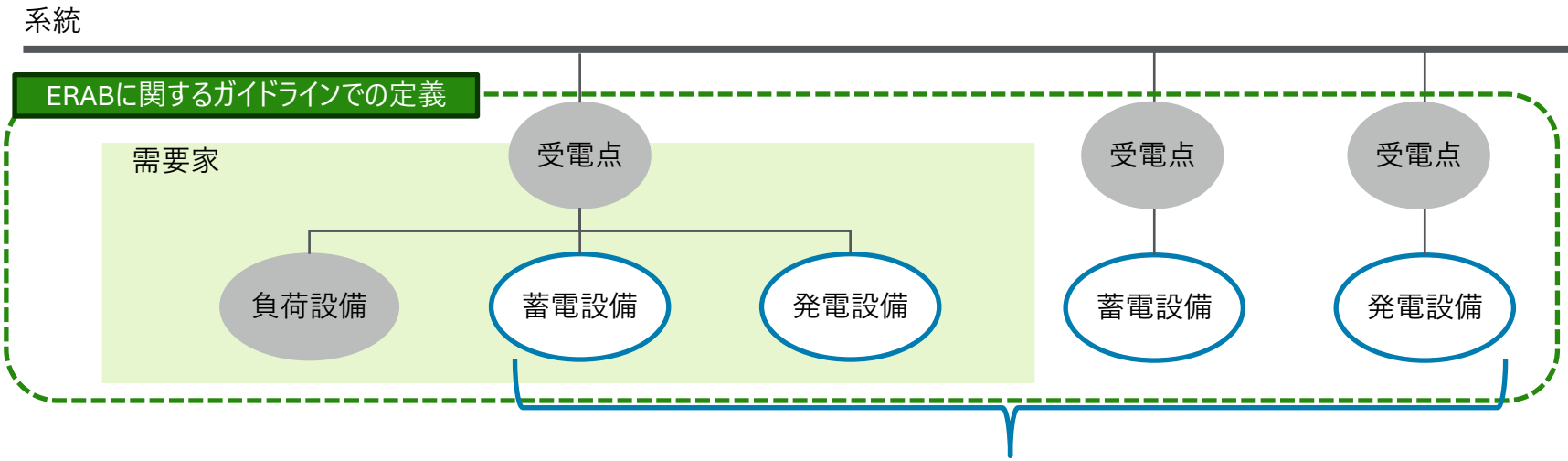
設置者に対してJC-STAR制度適合製品の設置を求める制度の検討が進んでいます

日本における設置者（機器）への規制

小規模太陽光発電設備について、JC-STAR制度の普及状況を踏まえつつ、系統連系手続きにおけるサイバーセキュリティ対策の確認としての活用について、官民で連携して検討が進められている。まずはIoT製品全般に対する最低限度のサイバーセキュリティ対策としてのJC-STAR★1の活用を進めるとともに、今後はJC-STAR★2以上の基準の整備や導入についても検討していくことになっている。

ERABに関するガイドラインでの「分散型エネルギーリソース」の定義

需要家の受電点以下に接続されているエネルギーリソース(発電設備、蓄電設備、負荷設備)に加えて、**系統に直接接続される発電設備、蓄電設備**を総称するもの。



太陽光発電設備や蓄電池設備について、**2027年4月の系統連系技術要件の改定においてJC-STAR★1を取得した製品を用いることを必須の要件とする**。ただし、低圧（50kW未満）で連携する製品については、経過措置期間を半年程度設定し、2027年10月とする。
分散型電源固有の脅威や特性、PCS等に必要な機能を考慮した分散型電源独自のJCSTAR★2以上の適合基準の整備や導入の検討も進んでいる。

現時点でJC-STAR制度認証製品は限定的であるため活用促進が必要です

JC-STAR★1取得製品（電力関連製品）について

2025年12月時点でのJC-STAR★1取得製品[*22]は、限定的であり、製品分類によっては、１社しか取得していない製品分類もある。

製品分類	ラベル取得事業者数	ラベル取得製品数
発電所施設等の遠隔監視及び制御	1社	4製品
電気事業関連機器 （スマートメーター、発電設備など）	1社	3製品
蓄電池システム	1社	1製品
エネルギー関連機器 （エネファーム、PCS、ガス給湯器など）	20社	36製品
合計	23社	44製品

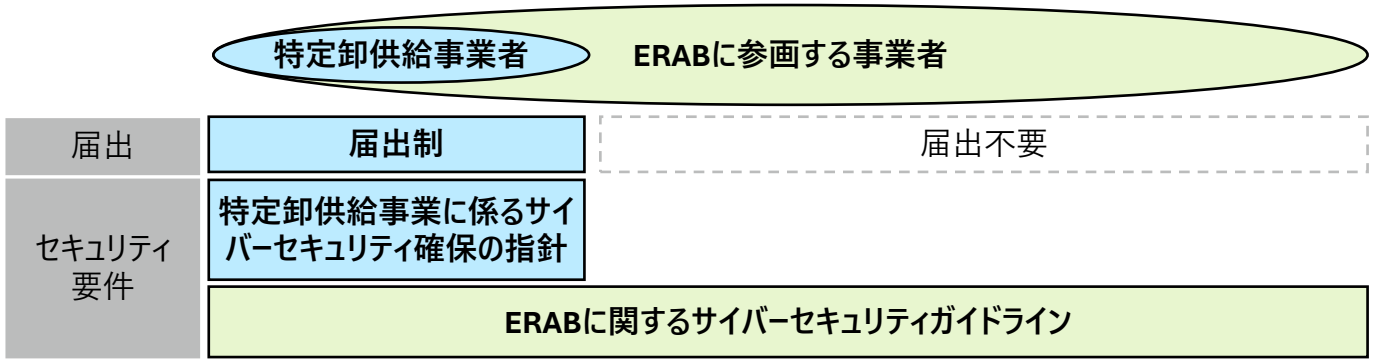
*22：“IPA, 適合ラベル取得製品リスト”， 閲覧日：2026年1月29日， https://www.ipa.go.jp/security/jc-star/list/jc-star-product-list/index.html

事業者の届出制度は中小規模の新規プレイヤーの対象となっていません

日本におけるアグリゲーターへの規制

機器を制御する事業者のうち一定規模（合計が1,000kW超）かつ電気の供給を行う事業者のみが届出の対象[*23][*24]となる。

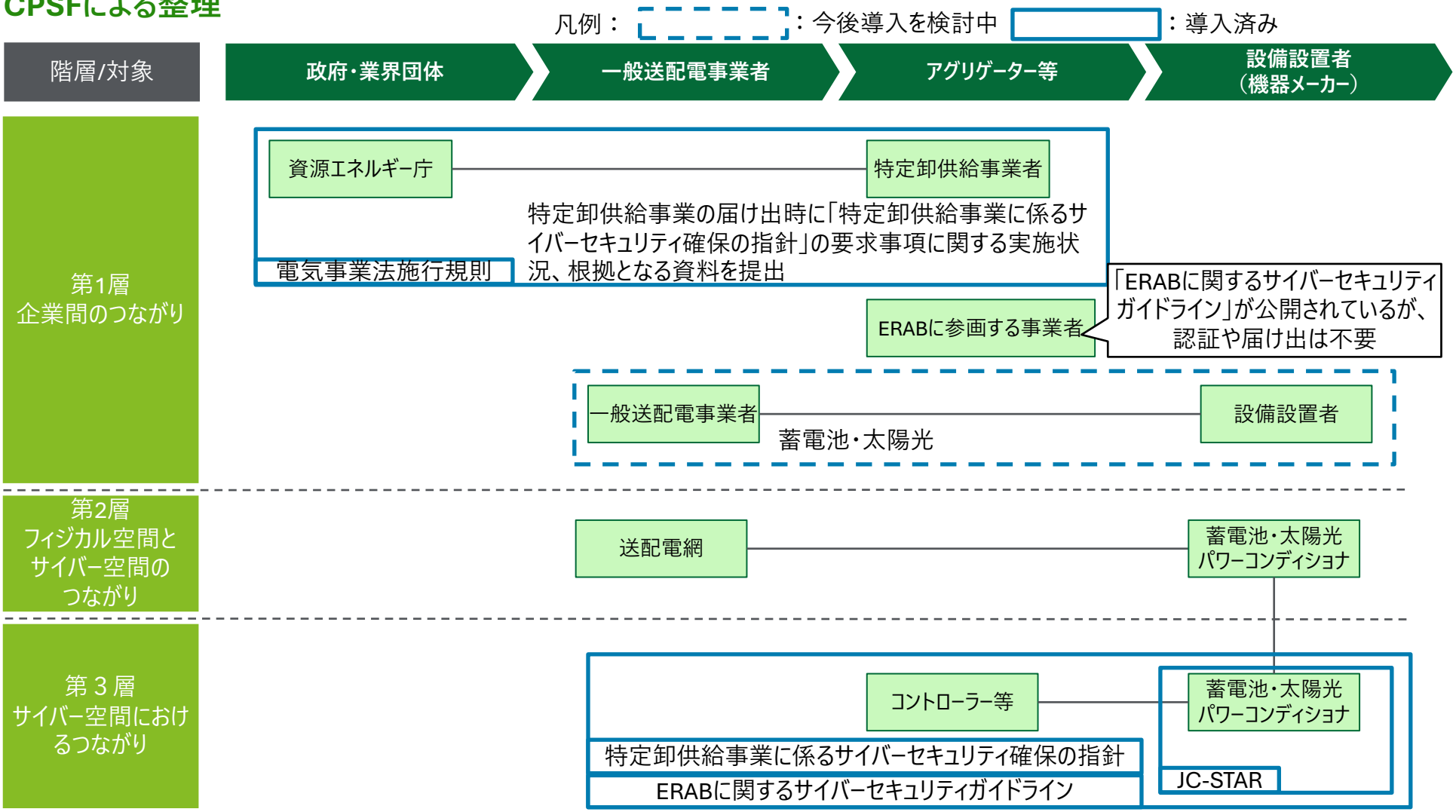
	制御対象	取引先	規模	提供するもの
ERABに参画する事業者	**需要家側エネルギーリソース** 発電設備 蓄電設備	一般送配電事業者、小売電気事業者、**需要家**、**再生可能エネルギー発電事業者**といった取引先	制約なし	調整力、インバランス回避、**電力料金削減**、**出力抑制回避**等の**各種サービス**
特定卸供給事業者	発電用の電気工作物 蓄用の電気工作物	小売電気事業、一般送配電事業、配電事業又は特定送配電事業	指示等の対象となる供給能力の合計が**1,000kWを超える事業者**	事業の用に供するための**電気として供給**



*23：“電気事業法”， 閲覧日：2026年1月29日， https://laws.e-gov.go.jp/law/339AC0000000170/
*24：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・ビジネスハンドブック”， 閲覧日：2026年1月29日, https://www.enecho.meti.go.jp/category/saving_and_new/advanced_systems/vpp_dr/files/erab_handbook.pdf

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）を参照し、対象ごとのつながりを整理しました

CPSFによる整理



ここまでのインシデント等を踏まえて、サプライチェーン全体でのセキュリティ向上に向けた対策案を紹介します

電力関係の直近の動向のまとめ

【まとめ】

■ インシデント及び各国の動向を踏まえると、電力需給に影響を及ぼす機器に対する製造から運用保守までのサプライチェーンを通じた網羅的なセキュリティ対策を講じる必要がある

【気づきの点】

■ 米国・英国・日本の政策を比較してみても、分散型電源のセキュリティ・リスクに対して、ガイドラインや規格を通じて対策していくという点で大きな方向性は同じ

■ 一方で、米国では機器の第三者評価による認証制度を導入、また米英両国では制御を行う事業者に対して、電力供給の有無や事業規模に関わらない広範なライセンス制度を導入している点で日本とは違いがある

		米国	英国	日本
機器の認証方法		第三者評価	自己評価＋OPSSによる認証	自己評価＋IPAによる認証
ライセンス	電力供給	**電力供給の有無にかかわらず対象**	**電力供給の有無にかかわらず対象**	**電力供給を行う事業者のみ対象**
	事業規模	**規模にかかわらず対象**	**規模にかかわらず対象**	**一定規模以上のみ届け出必要**

Deloitte.
デロイト トーマツ

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーである合同会社デロイト トーマツ グループならびにそのグループ法人（有限責任監査法人トーマツ、合同会社デロイト トーマツ、デロイト トーマツ税理士法人およびDT弁護士法人を含む）の総称です。デロイト トーマツ グループは、日本で最大級のプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従いプロフェッショナルサービスを提供しています。また、国内30都市以上に2万人超の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト、www.deloitte.com/jpをご覧ください。

Deloitte（デロイト）とは、Deloitte Touche Tohmatsu Limited（“Deloitte Global”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して“デロイトネットワーク”）のひとつまたは複数を指します。Deloitte Globalならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。Deloitte Globalおよびその各メンバーファームならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。Deloitte Globalはクライアントへのサービス提供を行いません。詳細はwww.deloitte.com/jp/aboutをご覧ください。
デロイト アジア パシフィック リミテッドは保証有限責任会社であり、Deloitte Globalのメンバーファームです。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける100を超える都市（オークランド、バンコク、北京、ベンガルール、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、ムンバイ、ニューデリー、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、最先端のプロフェッショナルサービスを、Fortune Global 500®の約9割の企業や多数のプライベート（非公開）企業を含むクライアントに提供しています。デロイトは、資本市場に対する社会的な信頼を高め、クライアントの変革と繁栄を促進することで、計測可能で継続性のある成果をもたらすプロフェッショナルの集団です。デロイトは、創設以来180年の歴史を有し、150を超える国・地域にわたって活動を展開しています。“Making an impact that matters”をパーパス（存在理由）として標榜するデロイトの約46万人の人材の活動の詳細については、www.deloitte.comをご覧ください。

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301

IS/BCMSそれぞれの認証範囲はこちらをご覧ください
http://www.bsigroup.com/clientDirectory

Member of
Deloitte Touche Tohmatsu Limited