経済産業省

第19回　グリッドコード検討会　資料6

分散型電源のサイバーセキュリティ対策の要件化に係る今後の対応について

2025年6月25日

資源エネルギー庁

電力分野におけるサイバーセキュリティについて

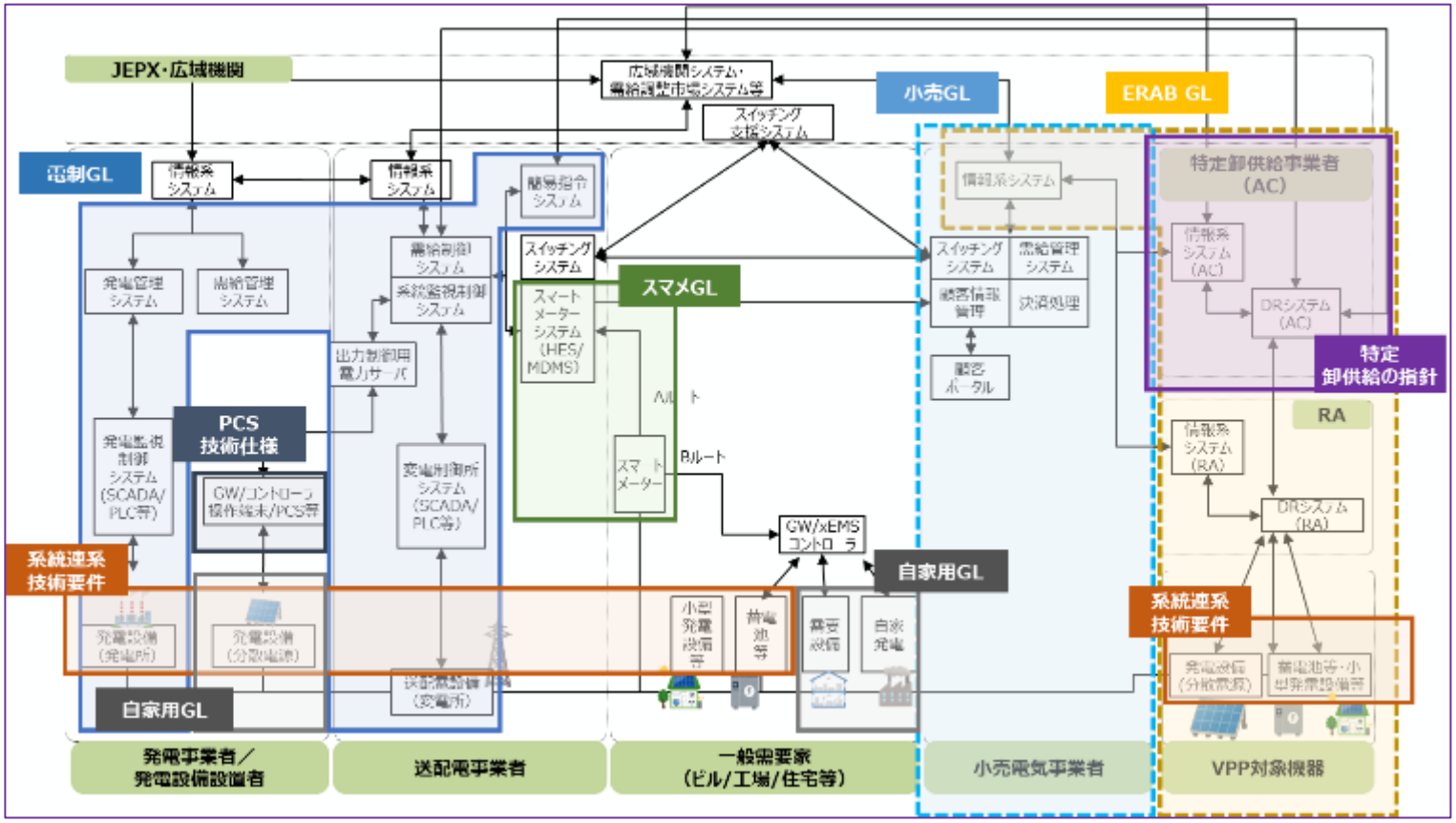
- **電力システムは、経済安全保障の確保のために重要な基盤**。電力システム改革に伴い、多種多様なプレーヤーが参入し、電力産業自体が大きな広がりを見せる中でも、電力の安定供給確保のためには**サイバーセキュリティの確保が必要不可欠**。
- **業界大での取組を進めるためのプラットフォーム**として、産業サイバーセキュリティ研究会の下に設置した**電力SWG**において、**有識者や事業者、電力ISAC等**の関係機関と、**電力分野のサイバーセキュリティを取り巻く状況について共有**し、**必要な対策について具体的な取組の整理・検討**が行われている。
- また、電力SWGでの検討結果を踏まえ、第87回電力・ガス基本政策小委員会（2025年3月31日）および第74回再生可能エネルギー大量導入・次世代電力ネットワーク小委員会（2025年6月3日）において、**分散型電源のサイバーセキュリティ対策の方向性について報告されている**。
- 国の審議会における検討状況を報告するとともに、**分散型電源のサイバーセキュリティ対策の要件化（JC-STAR★1取得のグリッドコード化）についてご議論いただきたい**。

（参考）電力分野におけるサイバーセキュリティの確保の取組

- デジタル技術の活用が進むことに伴い、電力分野におけるサイバーセキュリティリスクも拡大。
- このため、国内においても、規制やガイドラインにより、**求められるセキュリティ対策事項は整理されつつある**。他方、サイバー脅威が日々進化・巧妙化している状況を踏まえると、**現状の対策で十分ということは決してなく、電力システムにおけるサイバーセキュリティ対策の継続的な改善・高度化が必要**。

＜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＞

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。

（参考）電力制御システムに対する取組（ガイドライン等）

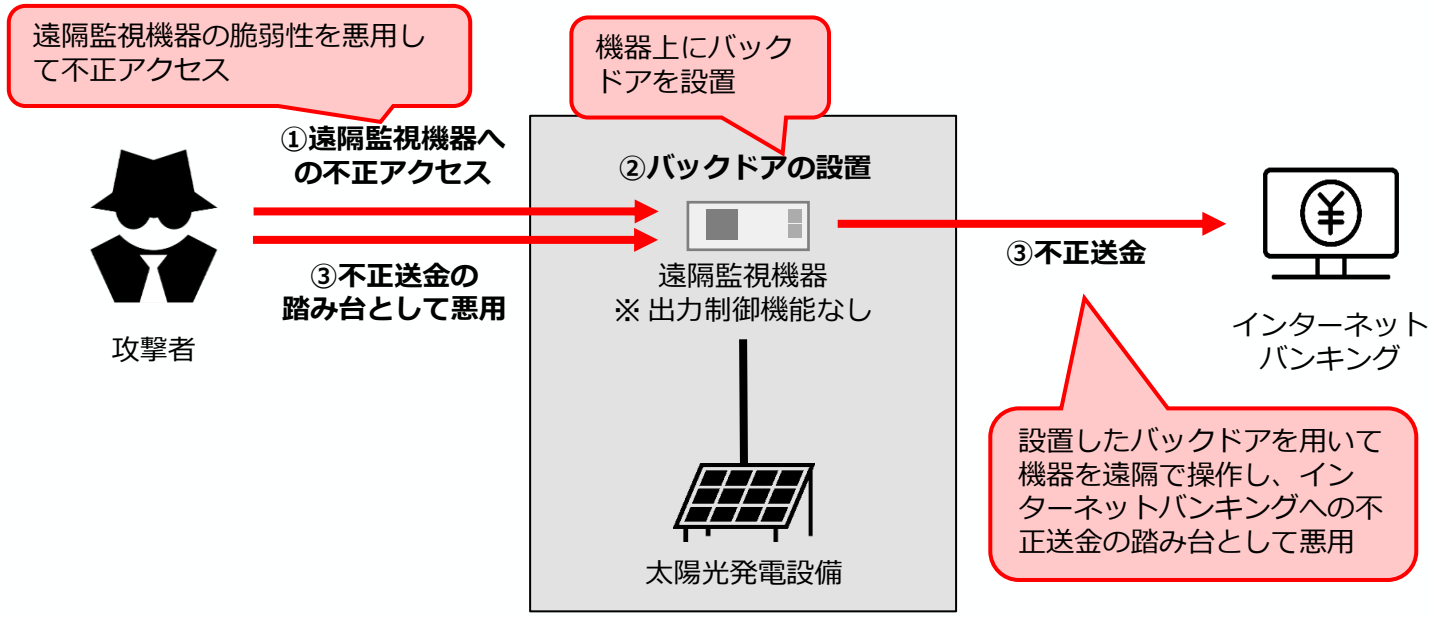
	名称	主な対象	発行主体	概要
電制GL	**電力制御システムセキュリティガイドライン**	電気事業の用に供する電気工作物	日本電気協会	電気事業法、電気設備に関する技術基準を定める省令及びその解釈に基づき、電気事業の用に供する電気工作物に対しては、本ガイドラインに基づく対策が求められる。
スマメGL	**スマートメーターシステムセキュリティガイドライン**	スマートメーターシステム	日本電気協会	電気事業法、電気設備に関する技術基準を定める省令及びその解釈に基づき、スマートメーターシステムに対しては、本ガイドラインに基づく対策が求められる。
系統連系技術要件	**系統連系技術要件**	系統連系する発電設備	各一般送配電事業者	系統連系する発電設備にすべからく求められる対策。具体的には、ネットワーク接続点の保護、マルウェア対策、系統運用者に対するセキュリティ管理責任者の通知の3点が求められる。
PCS技術仕様	**出力制御機能付PCSの技術仕様**	出力制御機能付PCS	JPEA・JEMA・電事連	出力制御機能付PCSにおいて満たすべきサイバーセキュリティ対策の要件を示した技術仕様。
自家用GL	**自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン（内規）**	自家用電気工作物（発電設備と需要設備の両方を含む）	経済産業省	自家用電気工作物（発電設備と需要設備の両方を含む）に求められるサイバーセキュリティ対策事項を記載したガイドライン。
小売GL	**小売電気事業者のためのサイバーセキュリティ対策ガイドライン**	小売電気事業者	資源エネルギー庁	小売電気事業者が主体的に取り組むことが求められるサイバーセキュリティ対策に関して記載したガイドライン。
ERAB GL	**ERABに関するサイバーセキュリティガイドライン Ver2.0**	ERABに関する事業者	経済産業省・IPA	ERAB のサービスレベルを維持するために ERAB に参画する各事業者が実施すべき最低限のセキュリティ対策の要求事項を示したガイドライン。
特定卸供給の指針	**特定卸供給に係るサイバーセキュリティ確保の指針**	特定卸供給事業に関するシステム	資源エネルギー庁	特定卸供給事業を実施する上で確保すべきサイバーセキュリティとその対策の内容を示すことを目的とした指針で、特定卸供給事業の届出の際に、本指針に基づく対策実施状況を記載する必要がある。

分散型電源に関する脅威事例

（出所）第83回電力・ガス基本政策小委員会（2024年11月20日）資料6を一部修正

- 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に悪用**された。
- 遠隔監視機器の**脆弱性が攻撃に悪用**された。攻撃された機器メーカーは、対象機器は出力制御機能を有さないため、**系統への影響はない**としている。
- 同脆弱性は以前から報告されており、**複数の攻撃実証コード（PoCコード）も公開**されていた。

太陽光発電施設向け遠隔監視機器に関連する一連のサイバー攻撃のイメージ



（参考）電気事業法における分散型電源の区分

（出所）第18回電力SWG 資料6-1 に基づき一部修正

- 分散型電源の出力規模や電圧の種別によって、必要となる手続きが異なる。
- 「電気設備に関する技術基準を定める省令」において、事業用電気工作物においては、サイバーセキュリティの確保が義務付けられているが、**50kW未満の発電等設備（一般用及び小規模事業用）については、電気事業法上、サイバーセキュリティの確保に特化した明確な技術基準の規定までは無い**（※）。
- 一般送配電事業者が定める系統連系技術要件では、**設備規模に依らず、系統に連系する発電等設備においてはすべからくサイバーセキュリティ対策が求められる**。

電気工作物の区分		分散型電源の発電出力	発電事業届出	電気事業法上の位置づけ		系統連系技術要件に基づくセキュリティ対策の義務の有無
				サイバーセキュリティの確保に特化した明確な技術基準の規定の有無	技術基準の解釈に位置づけられているガイドライン	
一般用電気工作物		10kW未満（※1）	不要	無し（※）	ー	有り
	小規模事業用電気工作物	10kW以上50kW未満	不要	無し（※）	ー	有り
事業用電気工作物	自家用電気工作物	50kW以上2,000kW未満	不要（※3の場合は届出）	有り	自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン ※発電事業者の自家用電気工作物については、電力制御システムセキュリティガイドライン	有り
		2,000kW以上	不要（※3の場合は届出）			
	電気事業の用に供する電気工作物	発電事業の要件を満たす設備(※3)であって、合計出力200万kWを超えるもの	届出	有り	電力制御システムセキュリティガイドライン	有り

※1.低圧連系の10kW未満、もしくは独立型システムの10kW未満が該当する。
※2.外部委託は、出力5,000kW未満かつ電圧7,000V以下で連系等をする事業場のみ。
※3.①出力が1,000kW以上、②託送契約上の同時最大受電電力が5割超、③年間の逆潮流量(電力量)が5割超の3つのいずれの条件にも該当する発電等用電気工作物から、小売電気事業等の用に供する電力の合計が1万kWを超えるもの。
※4: 50kW未満の小規模太陽光発電設備（一般用及び小規模事業用）については、電気事業法上、サイバーセキュリティの確保に特化した明確な技術基準の規定までは無い。（もっとも、感電・火災のおそれがないように施設しなければならないといった技術基準への適合義務が規定されており、それにより全体として保安を確保している。）

出所）太陽光発電協会, 知っておきたい太陽光発電関連法規等を参考に作成 https://www.jpea.gr.jp/law/solarlaw/

小規模太陽光発電設備に想定される脅威

（出所）第18回電力SWG
資料6-1

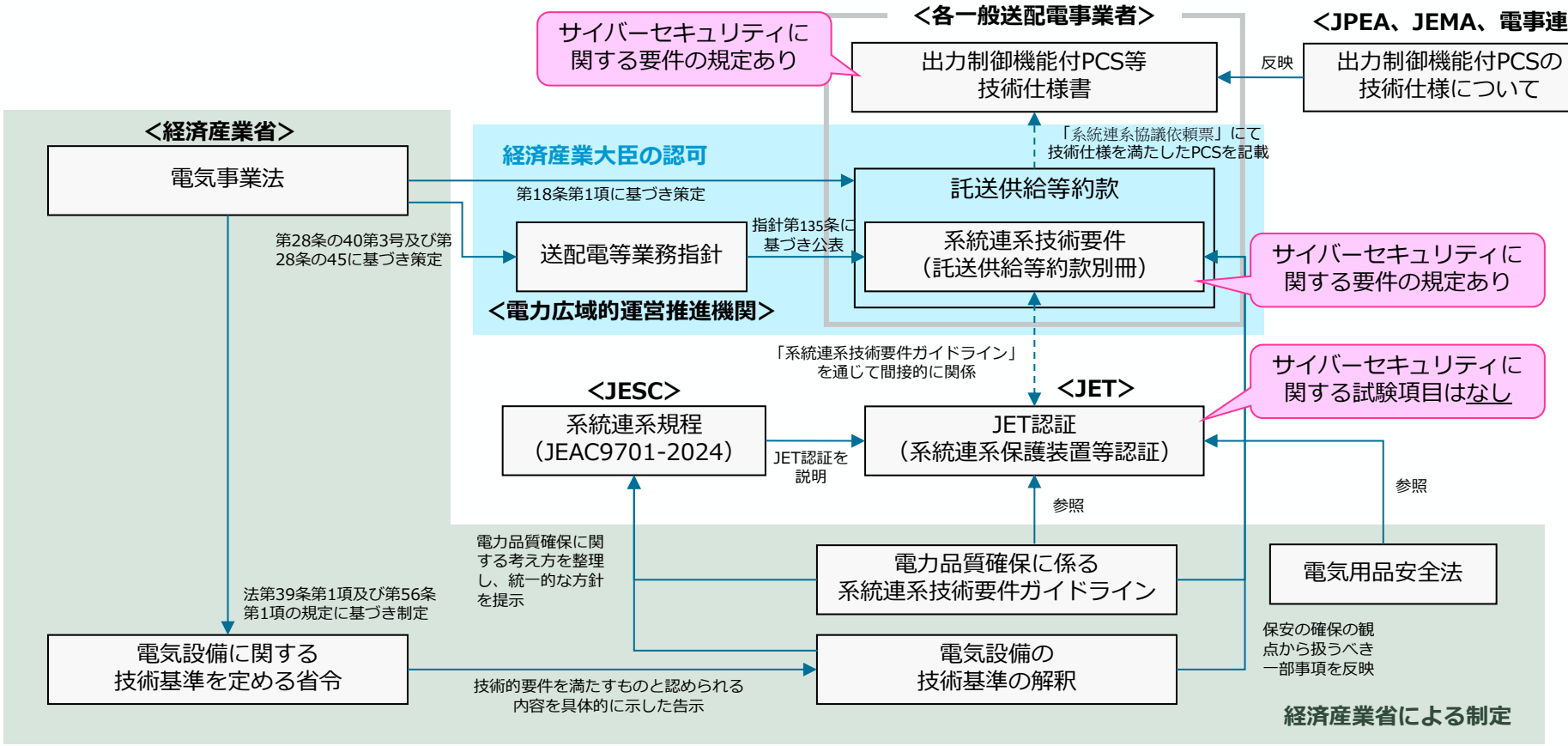
- 小規模太陽光発電設備のモデルシステム図に基づき、IPAの「制御システムセキュリティリスク分析ガイド Ver2.0」を参照して、想定される脅威の分析及びリスクの評価（資産や系統等に対する攻撃の影響度及び脅威の発生可能性の評価）を行った。
- 分析の結果、**ネットワーク機器やPCSに対する不正アクセス、不正操作、高負荷攻撃、不正媒体・機器接続、サプライチェーン攻撃**といった脅威においてリスク度合いが高く、特に対策が必要であることが明らかとなった。
- 本検討では、系統連系申請時に情報提供が必要となる**PCSを対象に、関係者の責任や対策実装にかかる負担等を考慮した上で、講じるべき対策を示す**。

資産	リスク度合いの高い脅威	太陽光の出力停止に至る攻撃シナリオの一例
PCS	• 不正アクセス • 不正操作 • 高負荷攻撃 • 不正媒体・機器接続 • サプライチェーン攻撃	• PCSの脆弱性が悪用され、外部ネットワークから複数のPCSに対する不正アクセスが実施される。外部ネットワークを介して不正な出力制御指令が送信されることで、複数の太陽光発電設備における発電が停止する。 • PCSに対する高負荷攻撃が実施され、正規の出力制御指令が受信できなくなる。その結果、本来抑制すべき発電が行われることとなり、系統に影響を及ぼす。
ネットワーク機器（ルーター、GWなど）	• 不正アクセス • 不正操作 • 高負荷攻撃 • 窃盗 • サプライチェーン攻撃	• ネットワーク機器において電力会社からの出力制御指令が改ざんされることで、複数の太陽光発電設備における発電が停止する。
小規模太陽光発電パネル	• サプライチェーン攻撃	• 開発段階で、小規模太陽光パネルに不適切な停止機能が意図的に追加される。同時に停止機能が作動することで、複数の太陽光発電設備における発電が停止する。

（出所）第18回電力SWG
資料6-1に基づき一部修正

（参考）分散型電源の系統連系に関する制度・文書等

- 分散型電源の系統連系に関する制度・文書等は複数存在する。
- **サイバーセキュリティに関する要件は「出力制御機能付PCS等技術仕様書」及び「系統連系技術要件（託送供給等約款別冊）」において規定**されている。



出所）内閣府, 第28回 再生可能エネルギー等に関する規制等の総点検タスクフォース 会議資料
https://www8.cao.go.jp/kisei-kaikaku/kisei/conference/energy/20231110/agenda.html を基に作成

系統連系に関する制度・文書等におけるセキュリティ要件

（出所）第18回電力SWG 資料6-1

- 「出力制御機能付PCS等技術仕様書」では、**通信のセキュリティ対策や通信仕様等に関する技術仕様**が規定されている。
- 「系統連系技術要件」では、**外部ネットワークを介した脅威への対策**に加え、**マルウェア侵入防止対策やセキュリティ管理責任者に関する対策**も規定されている（下表においては低圧設備を対象としたものの例を記載）。

要件	JET認証※1	出力制御機能付PCS等技術仕様書	系統連系技術要件※2
通信のセキュリティ	×	電力サーバとのやりとりに個人情報等の重要情報を含めないこと	外部ネットワークや他ネットワークを通じた、システムへの影響を最小化するための対策を講じること
	×	出力制御スケジュールをバックアップ（ID認証により出力制御機能付PCS等と電力サーバ間で相互に確認）すること	
	×	出力制御機能付PCS等の外部遠隔操作を防止（外部からのセッション開始禁止）すること	
	×	通信を暗号化すること（SSL通信）	
マルウェア侵入防止対策	×	×	マルウェアの侵入防止対策を講じること
セキュリティ管理責任者の設置	×	×	セキュリティ管理責任者の設置をすること

※1 通信に関する試験項目は存在するが、セキュリティに関する内容を含んだ試験項目ではない。
※2 自家用電気工作物、事業用電気工作物にあたる設備（高圧設備）は別途、「自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン」、「電力制御システムセキュリティガイドライン」に準拠した対策を講じる必要がある。

出所）JET, 系統連系保護装置等認証 https://www.jet.or.jp/products/protection/index.html,
東京電力PG, 系統連系技術要件 【託送供給等約款別冊】, https://www.tepco.co.jp/pg/consignment/notification/pdf/keitou_renkei20230401.pdf,
JPEA, JEMA, 電事連, 出力制御機能付PCS等技術仕様書 https://www.meti.go.jp/shingikai/enecho/shoene_shinene/shin_energy/keito_wg/pdf/005_02_00.pdf に基づき作成

（参考）系統連系技術要件の概要

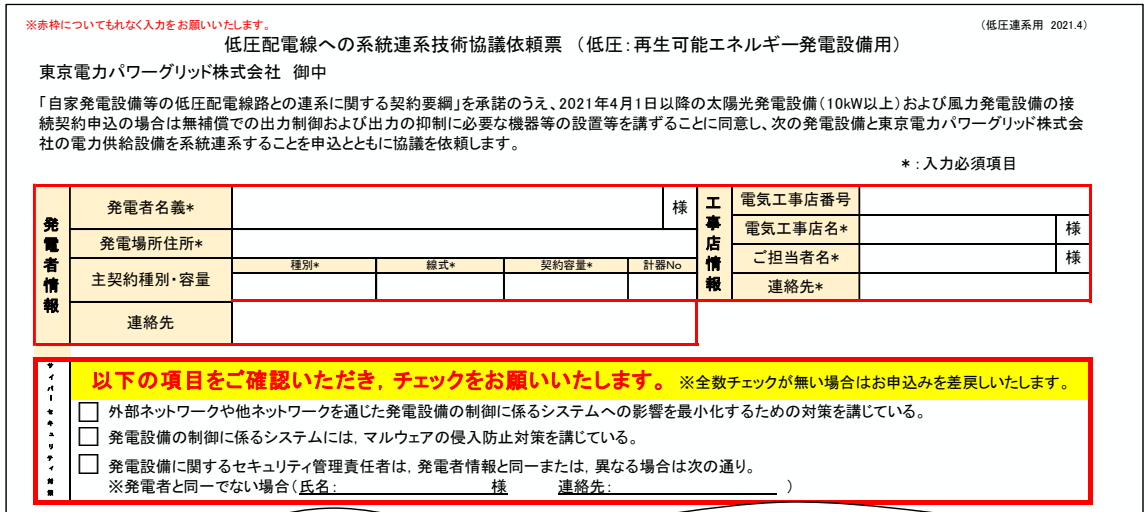
（出所）第18回電力SWG 資料6-1

- 2020年10月より、一般送配電事業者が定める「託送供給等約款別冊（系統連系技術要件）」にサイバーセキュリティに関する要件が規定された。
- 本規定により、電気事業の用に供しない小規模の発電設備を含め、系統に連系する発電設備に対しては、一般送配電事業者に対する系統連系申請の際に、すべからくサイバーセキュリティ対策が求められている。
- 具体的な対策の内容として、サイバーインシデントの発生を防ぐ事前防御の観点と、インシデント発生後の影響を最小化する事後対応の観点の両方から、3つの対策が求められている。各一般送配電事業者に対する系統連系申請に当たり、これら3つの対策が実施できていることを確認する必要がある。

系統連系技術要件で求められる3つの対策

観点	求められる対策
サイバーインシデントの発生を防ぐ事前防御	対策①　ネットワーク接続点の保護
	対策②　データの保存・転送を行う機器・端末等のマルウェア対策
インシデント発生時の影響を最小化する事後対応（早期発見、迅速な対処）	対策③　連系先系統運用者に対するセキュリティ管理責任者の氏名及び緊急時連絡先の通知

系統連系申請書におけるサイバーセキュリティ対策に関する確認項目例
（東京電力パワーグリッドの場合）



※赤枠についてもれなく入力をお願いいたします。　（低圧連系用　2021.4）

低圧配電線への系統連系技術協議依頼票　（低圧：再生可能エネルギー発電設備用）

東京電力パワーグリッド株式会社　御中

「自家発電設備等の低圧配電線路との連系に関する契約要綱」を承諾のうえ、2021年4月1日以降の太陽光発電設備（10kW以上）および風力発電設備の接続契約申込の場合は無補償での出力制御および出力の抑制に必要な機器等の設置等を講ずることに同意し、次の発電設備と東京電力パワーグリッド株式会社の電力供給設備を系統連系することを申込とともに協議を依頼します。

＊：入力必須項目

発電者情報
- 発電者名義＊　様
- 発電場所住所＊
- 主契約種別・容量　種別＊　線式＊　契約容量＊　計器No
- 連絡先

工事店情報
- 電気工事店番号
- 電気工事店名＊　様
- ご担当者名＊　様
- 連絡先＊

サイバーセキュリティ対策

以下の項目をご確認いただき，チェックをお願いいたします。 ※全数チェックが無い場合はお申込みを差戻しいたします。

- ☐ 外部ネットワークや他ネットワークを通じた発電設備の制御に係るシステムへの影響を最小化するための対策を講じている。
- ☐ 発電設備の制御に係るシステムには，マルウェアの侵入防止対策を講じている。
- ☐ 発電設備に関するセキュリティ管理責任者は，発電者情報と同一または，異なる場合は次の通り。
  ※発電者と同一でない場合（氏名：　様　連絡先：　）

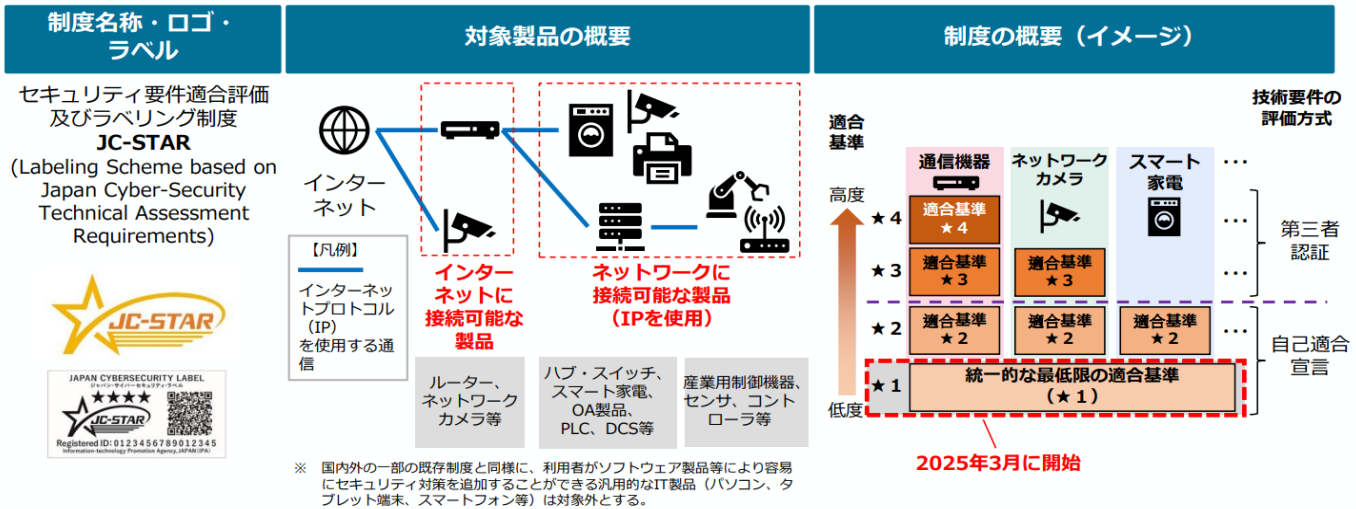
出所）東京電力パワーグリッド，系統連系協議依頼票 https://www.tepco.co.jp/pg/consignment/fit/workshop.html

分散型電源のサイバーセキュリティ対策について

（出所）第74回大量導入小委　資料1

- 第87回電力・ガス基本政策小委員会（2025年3月31日）では、**小規模太陽光発電設備（※1）のPCS**について、**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、**IoT製品のセキュリティ機能を評価・可視化するJC-STAR★１制度（※2）が活用できないか、同制度の普及状況を踏まえつつ、官民で連携して検討**していくこととされた。併せて、小規模太陽光発電設備に限らない**分散型電源においてJC-STAR★1制度を活用できないか検討**していくこととされている。
- さらに、分散型電源固有の脅威や特性、PCSに必要な機能を考慮した**PCS独自の★2以上の適合基準の整備についても併せて検討**していくこととされた。
- なお、関連する取組として、**分散型電源を管理するアグリゲーターが行うセキュリティ対策の強化**として、今年５月に、**ERABサイバーセキュリティガイドラインの改定**が行われている。

JC-STAR制度の概要（※3）



(※1) 電気事業法上、サイバーセキュリティ確保に特化した明確な技術基準適合義務が規定されていない50kW未満の太陽電池発電設備（一般用電気工作物及び小規模事業用電気工作物に該当する太陽光発電設備）を指す。
(※2) IPA「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」 https://www.ipa.go.jp/security/jc-star/index.html
(※3) 出典：第87回電力・ガス基本政策小委員会（2025年3月31日）資料７

（参考）小規模太陽光発電設備における サイバーセキュリティ対策向上の方策について

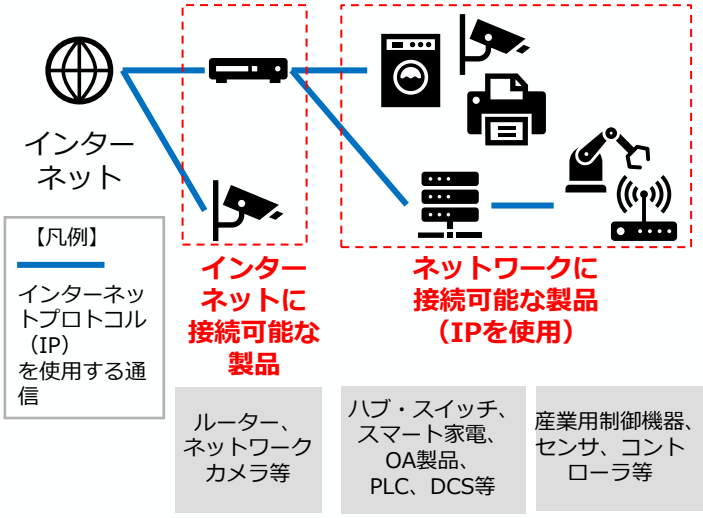
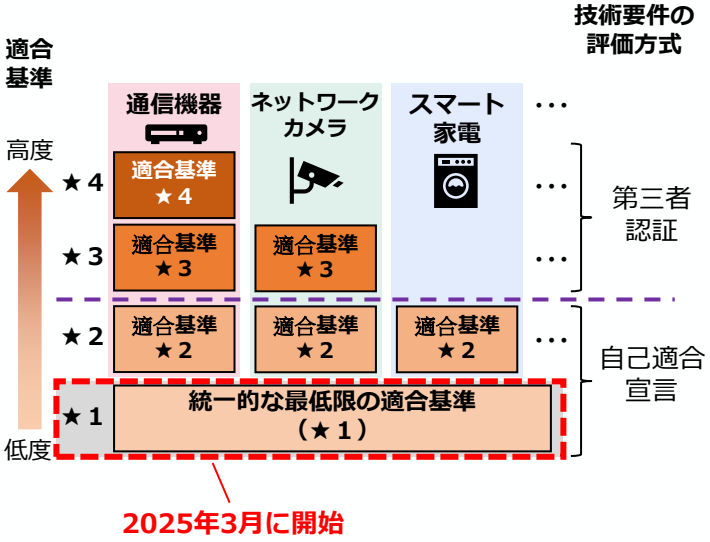
（出所）第18回電力SWG 資料6-1

- **小規模太陽光発電設備の設備設置者に対してのみに厳格なセキュリティ対策を求めることは、設置者の過度な負担につながることが懸念される**。これを避けるため、**設置者自身に高度なセキュリティ対策を求める代わり**に、**少なくともJC-STAR制度のラベル取得がされているPCSを使用した小規模太陽光発電設備の利用を求める**ことで、小規模太陽光発電設備のサイバーセキュリティの向上を進めることが考えられる。
- 具体的には、現在の小規模太陽光発電設備にかかる制度等を踏まえれば、**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、**JC-STARのラベル取得がされている製品を利用していることを確認することが考えられる**。JC-STAR★１は、2025年3月下旬から制度開始される予定であり、そ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を進めてはどうか**。
- 一方で、JC-STAR★1適合基準は、IoT製品全般に対する統一的な最低限の基準であり、太陽光発電設備に想定される脅威に対して求められる対策を全て包含しているわけではなく、また、一部のPCSではそもそも★１基準の一部項目に関する機能を有していない製品があることも確認されていることから、今後、**分散型電源固有の脅威や特性、PCSに必要な機能を考慮したPCS独自の★2以上の適合基準の整備についても検討を進めていくこととしてはどうか**。
- また、サイバーセキュリティ対策としては、**JC-STAR制度によらない対策によりサイバーセキュリティを確保することは否定されるものではなく**、むしろ、**JC-STARのラベル取得に加えて、例えば、小規模太陽光発電の制御に利用する通信等にセキュリティが確保されたサービス※を利用するなどの対策を行うことは推奨されるべき**である。
- 小規模太陽光発電設備のセキュリティ確保に向けた考え方の整理に当たっては、こうした点やJC-STARのラベル取得に関するメーカーに生じる負担、JC-STAR制度の普及の状況についても考慮しつつ検討を進める必要がある。

※例えば、閉域網を活用し、不正アクセスや高付加攻撃への対策を講じたソリューションの導入等が想定される。

（参考）JC-STAR制度の概要

- 2022年11月より検討会(※1)を開催し、2024年3～4月のパブコメを経て、8月に制度構築方針、9月30日にIPAから**「JC-STAR」という制度**(※2)を発表。**2025年3月下旬に最低限の基準となる★1の申請受付を開始**した。
- ラベル普及に向け**政府調達等の要件**等とすべく関係省庁と協議中。 ★2以上の適合基準は、通信機器とネットワークカメラを対象に検討中。他の製品類型も順次整備していく。
- **米欧等の諸外国との制度調和**を図るため議論中。

制度名称・ロゴ・ラベル	対象製品の概要	制度の概要（イメージ）
セキュリティ要件適合評価及びラベリング制度 **JC-STAR** (Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements)		

※ 国内外の一部の既存制度と同様に、利用者がソフトウェア製品等により容易にセキュリティ対策を追加することができる汎用的なIT製品（パソコン、タブレット端末、スマートフォン等）は対象外とする。

(※1)経済産業省「ワーキンググループ3（IoT製品に対するセキュリティ適合性評価制度構築に向けた検討会）」 https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/index.html
(※2)IPA「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」 https://www.ipa.go.jp/security/jc-star/index.html

（参考）求められるサイバーセキュリティ対策と、JC-STAR制度★1適合基準(※1)

（出所）第18回電力SWG資料6-1

- JC-STAR★1適合基準は、現行制度で求められるサイバーセキュリティ対策要件、脅威に対して求められる対策を概ね内包しているところ、**JC-STAR★1のラベルを取得したPCSは、小規模太陽光発電設備に対して想定される脅威に対し、一定の対策が実施されていると見なすことができるのではないか**。

★1で考慮する主な脅威			脅威に対抗するために★1で求める適合基準			
			IoT製品に対する適合基準		IoT製品ベンダーに対する適合基準	
			カテゴリ	適合基準の概要	カテゴリ	適合基準の概要
1.	①弱い認証機能により、	外部からの不正アクセスの対象となり、マルウェア感染や踏み台となる攻撃等を受けることで、情報漏えい、改ざん、機能異常の発生につながる脅威	識別・認証、アクセス制御	(1)適切な認証に基づく**アクセス制御** (2)**容易に推測可能なデフォルトパスワードの禁止** (3)パスワード等の認証値の変更機能 (4)ネットワーク経由のユーザ認証に対する**総当たり攻撃からの保護**	情報提供	(16)ユーザへの**セキュアな利用・廃棄方法に関する情報提供**(初期設定手順、セキュリティ更新、サポート期限、安全な廃棄手順等)
	②脆弱性の放置により、		脆弱性対策、ソフトウェア更新	(6)ソフトウェアコンポーネントのアップデート機能 (7)**容易かつ分かりやすいアップデート手順** (8)アップデート前のソフトウェアの完全性の確認機能 (10)ユーザが型式番号を認識可能とする記載・機能	情報・問い合わせの受付、情報提供	(5)連絡先・手続き等の**脆弱性開示ポリシーの公開** (9)セキュリティアップデートの優先度決定方針の文書化
	③未使用インタフェースの有効化により、		インターフェイスへの論理アクセス	(13)**不要かつリスクの高いインタフェースの無効化**(物理的・論理的な通信ポート等)	―	―
	①～③共通		データ保護	(11)製品に保存される守るべき情報の保護(**保存データの暗号化、匿名化**等)	―	―
2. 機器の通信が盗聴され、守るべき情報が漏えいする脅威			データ保護	(12)ネットワーク経由で伝送される守るべき情報の保護(**通信の暗号化、保護された通信環境の利用**等)	―	―
3. 廃棄・転売等された機器から、守るべき情報が漏えいする脅威			データ保護	(15)**製品内に保存される守るべき情報の削除機能**	情報提供	※(16)に含む
4. ネットワーク切断や停電等の事象が発生した際に、セキュリティ機能に異常が発生する脅威			レジリエンス向上	(14) 停電・ネットワーク停止等からの復旧時の**認証情報やソフトウェア設定の維持**(初期状態に戻らないこと)	―	―

(※1) IPA「セキュリティ要件適合評価及びラベリング制度（JC-STAR） ＞ ★1（レベル1）適合基準・評価ガイド」 https://www.ipa.go.jp/security/jc-star/tekigou-kizyun-guide/label1/index.html

（参考）JC-STAR制度★1適合基準に関するヒアリング調査結果

- PCSメーカー等に対するヒアリングを通じ、PCSメーカーにおけるJC-STAR制度★1適合基準の準拠状況や課題に関して、以下の点が明らかとなった。
  - ✓ 現行製品に関して、**JC-STAR制度★1の適合基準への準拠が可能なメーカーと、準拠困難なメーカーの双方が存在**
  - ✓ **デフォルトパスワードや保存データ保護に関する適合基準への準拠が特に困難**
  - ✓ 準拠困難なメーカーにおいて**今後★1の適合基準へ準拠するためには、相当の対応コスト・対応期間が必要**

JC-STAR制度との連携に関するヒアリング結果概要

区分	ヒアリング対象	JC-STAR★1適合基準への準拠	JC-STAR制度との連携に関する課題
PCS	PCSメーカーA	概ね満たしていると考えているが、詳細確認中。	ー
	PCSメーカーB	現行販売している一部の製品において、一部基準の準拠は困難。	• 現状の製品ではデフォルトパスワードを使用しているほか、保存データの保護策は講じていない。 • 義務化された場合、準拠した製品の設計・開発・販売には3.5年～4年程度を要する可能性がある。また、従業員数の少ないメーカーにおいては、特に影響が大きいおそれがある。
	PCSメーカーC	概ね満たしている。	• データの削除機能のみ一部実装できていないが、難しい実装ではないため、特段のコストをかけず対応（★1取得）が可能。
	PCSメーカーD	現行販売している製品において、一部基準の準拠は困難。	• 現状の製品ではデフォルトパスワードを使用しているほか、保存データの保護策は講じていない。また、脆弱性スキャンも実施していない。 • ★1に対応する対策を製品に実装する場合、相当の対応コストが必要となる。 • 義務化された場合、準拠した製品の設計・開発・販売には2年以上を要する。
遠隔監視装置	遠隔監視装置メーカーA	問題なく準拠可能。	• ファームウェア更新によりセキュリティに影響を及ぼす場合、ラベルの再申請が必要となるため、追加コストがかかる可能性がある。
業界団体	業界団体A	現行販売している製品において、一部基準の準拠は困難。	• ユーザ認証に関する対策が実施できていないほか、データの削除機能を実装していない製品が多い。 • データ削除機能を追加実装するためには、1,000万円オーダのコストが必要となる。

本資料にてご議論いただきたい事項および今後の進め方

- 第87回電力・ガス基本政策小委員会（2025年3月31日）および第74回再生可能エネルギー大量導入・次世代電力ネットワーク小委員会（2025年6月3日）において、**分散型電源のサイバーセキュリティ対策向上の方策として、JC-STAR★１制度の活用について、同制度の普及状況を踏まえつつ、官民で連携して検討することとした**。
- この点、**電力分野におけるJC-STAR★1制度の活用が始まりつつある**ことから、これらの方針に基づき、**グリッドコード（系統連系技術要件）においてJC-STAR★1を要件化する方針で検討を進めることについて**、ご意見を伺いたい。
- なお、JC-STAR★1のグリッドコード化を進める場合、**国と電力広域的運営推進機関の協力のもと、このグリッドコード検討会において、適用開始時期等について調整を進めることとしたい**。

（参考）ERABセキュリティガイドライン改定の今後の進め方について

（出所）第12回 次世代の分散型電力システムに関する検討会資料を一部修正

- **パブリックコメントの提出意見を踏まえた変更点を加えた「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（案）（パブリックコメント後）」を改定版とし、公表することとする。**
- なお、本ガイドラインの要件に関連するセキュリティ要件適合評価及びラベリング制度（JC-STAR）が、申請受付を開始していない状況であることから、**当該制度の開始時期を勘案し、「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」を公表することとする**。
- また、セキュリティ要件適合評価及びラベリング制度（JC-STAR）については、2025年3月下旬より★１（レベル１）の申請受付が開始される予定であり、まだ、適合ラベルを取得したIoT製品は、存在しない状況。
- 今後、JC-STAR制度が開始され、**ERABシステムに関連する機器について、JC-STAR制度の適合ラベルを取得した機器がある場合において、本ガイドラインの3.6.4.R4、3.6.5.R5、3.6.6.R6の下記要求事項に準拠するためには、リソースアグリゲーターの制御対象にIoT製品を新たに導入する場合、「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」が定める適合基準である★１（レベル１）以上※を満たす製品を選択することが求められる**。

  【要求事項】（3.6.4.R4、3.6.6.R6においては勧告、3.6.5.R5においては推奨）

  リソースアグリゲーターの制御対象にIoT製品を新たに導入する場合においては、「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」が定める適合基準である★１（レベル１）以上※を満たす製品を選択すること。

  ※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）以上を満たす製品を選択することが望ましい。

（参考）長期脱炭素電源オークションにおける検討状況

（出所）第103回制度検討作業部会
（2025年5月28日）資料3-3

＜蓄電池＞ 論点②　事業規律の強化

（サイバーセキュリティの強化）

- 本制度を通じて蓄電池の導入が急速に進みつつある中で、サイバーセキュリティの観点での懸念が高まりつつある。このため、一層のサイバーセキュリティの確保を図るため、情報処理推進機構（IPA）の運用する**JC-STARラベリング制度（次頁参照）の★１の取得を新たな要件**とすることとしてはどうか。
  ※太陽光・風力発電設備を構成するPCSに対しても同じ要件を課す。

（セルの供給源の多角化）

- リチウムイオン蓄電池の安定供給確保のため、サプライチェーンの途絶リスクの高いセル（日本国外で製造されたセル）を搭載したリチウムイオン蓄電池に対して、**セル製造国の１国当たりの募集上限（kWベースで30%未満※）を設ける**こととしてはどうか。
  ※30%を跨ぐ案件は不落札とする。落札後に、審査に合格した場合は導入する蓄電池を変更することは可能だが、セルの製造国を変更することは不可。

（実現可能性の確保）

- 本制度の第1回・第2回において、多くのリチウムイオン蓄電池の案件が落札したが、蓄電池の価格が数年後に下がることに期待して、現時点では実現困難なレベルの金額で応札し、将来、蓄電池の価格が下がらなければ、ペナルティを支払って市場退出するつもりの案件が横行しているのではないか、との指摘がある。
- このため、蓄電池の応札規律に関しては、応札後の計画断念が頻繁に起きていないか、今後も引き続き確認し、**市場退出ペナルティの引き上げや保証金の設定等について、必要に応じて検討していく**こととしてはどうか。

25