経済産業省

資料６－１

小規模太陽光発電設備の
サイバーセキュリティ対策について

2025年2月4日

資源エネルギー庁　電力産業・市場室

小規模太陽光発電設備のサイバーセキュリティ対策について

- カーボンニュートラルに向けた動きが進展する中で、太陽光発電設備や蓄電池等の分散型電源の活用が進みつつある。
- そうした中、太陽光発電の監視装置に内在する脆弱性が悪用され、サイバー攻撃の踏み台にされる事案が発生するなど、分散型電源に対するサイバーセキュリティ上の懸念が指摘されている。
- 前回の電力SWGでは、分散型電源の中でも普及が進みつつある一方で具体的な懸念が指摘されている点等を考慮し、小規模太陽光発電設備※を主なスコープの対象として取り上げ、脅威や対策の状況を整理するとともに、想定されるリスクに対してどのような方策が考えられるか検討することとされた。
- 今般、前回の電力SWGでの議論結果を踏まえ、小規模太陽光発電設備のサイバーセキュリティ上の脅威に関するリスク分析を行うとともに、小規模太陽光発電設備に関する制度等の状況整理を行った。
- 本日は、これらの整理結果を踏まえ、想定されるサイバーセキュリティ上の脅威に対して講じるべき方策について御議論いただきたい。特に「セキュリティ要件適合評価及びラベリング制度（JC-STAR制度）」との連携の可能性等について御議論いただきたい。

※ 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。

第17回電力SWG
（2024年10月22日）
資料より

（参考）電気事業法における太陽光発電設備の区分

- 太陽光発電設備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**（※）。
- 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		太陽光発電の発電出力	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/

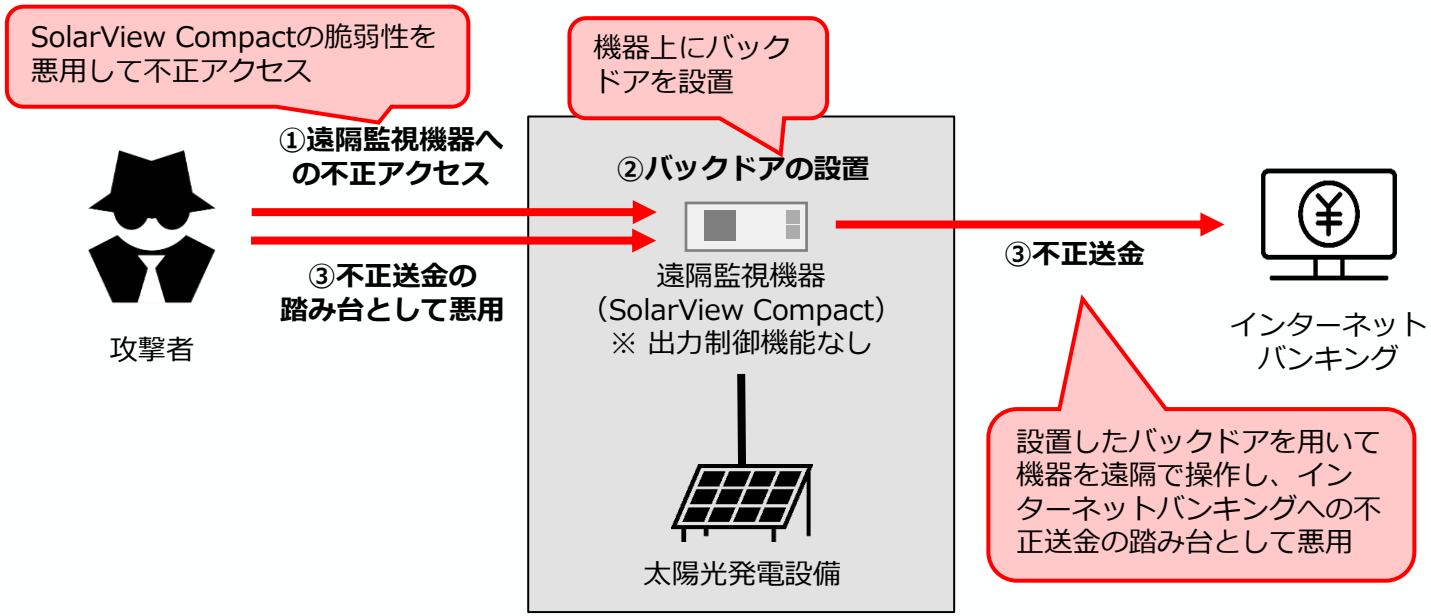
（参考）小規模太陽光発電設備に関する脅威事例

第17回電力SWG
（2024年10月22日）
資料より

(1) 太陽光発電施設の遠隔監視機器800台におけるサイバー攻撃による乗っ取り・悪用

- 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。
- 攻撃を受けたのはコンテック社のSolarView Compactであり、同製品の**脆弱性が攻撃に悪用**された。同社は、対象製品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（SolarView Compact）に関連する一連のサイバー攻撃のイメージ



出所）以下の公開情報等に基づき三菱総合研究所作成
https://www.contec.com/jp/info/2024/2024050700/, https://www.trendmicro.com/ja_jp/jp-security/24/f/security-strategy-20240606-01.html

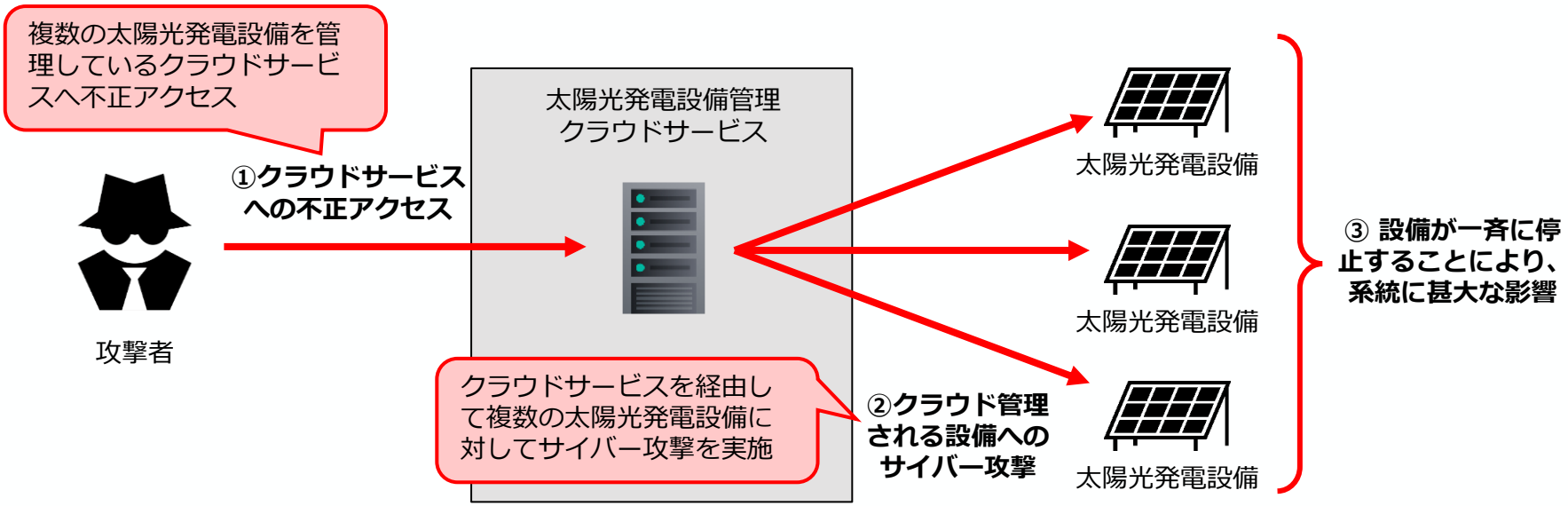
（参考）小規模太陽光発電設備に関する脅威事例

第17回電力SWG
（2024年10月22日）
資料より

(2) クラウド管理された太陽光発電設備が攻撃により一斉停止する危険性の指摘・悪用

- 2024年8月、オランダの研究者によって、**クラウドサービスにて管理されている複数の太陽光発電設備がサイバー攻撃によって一斉に停止する危険性が指摘**された。
- 同研究者は、**クラウドサービスに対して不正アクセスを実施**し、サービスを介して太陽光発電設備にサイバー攻撃を実施することで、**発電が一斉に停止**し、**系統への甚大な影響をもたらす**おそれがあると指摘している。
- 同研究者は、オランダでは15GWの発電設備が遠隔から制御されているものの、制御の実態が不透明であるため、**系統全体が脆弱になりつつある**と危険性を懸念している。

クラウド管理された太陽光発電設備に対する一連のサイバー攻撃のイメージ



出所）Bert Hubert, The gigantic and unregulated power plants in the cloud
https://berthub.eu/articles/posts/the-gigantic-unregulated-power-plants-in-the-cloud/ に基づき三菱総合研究所作成

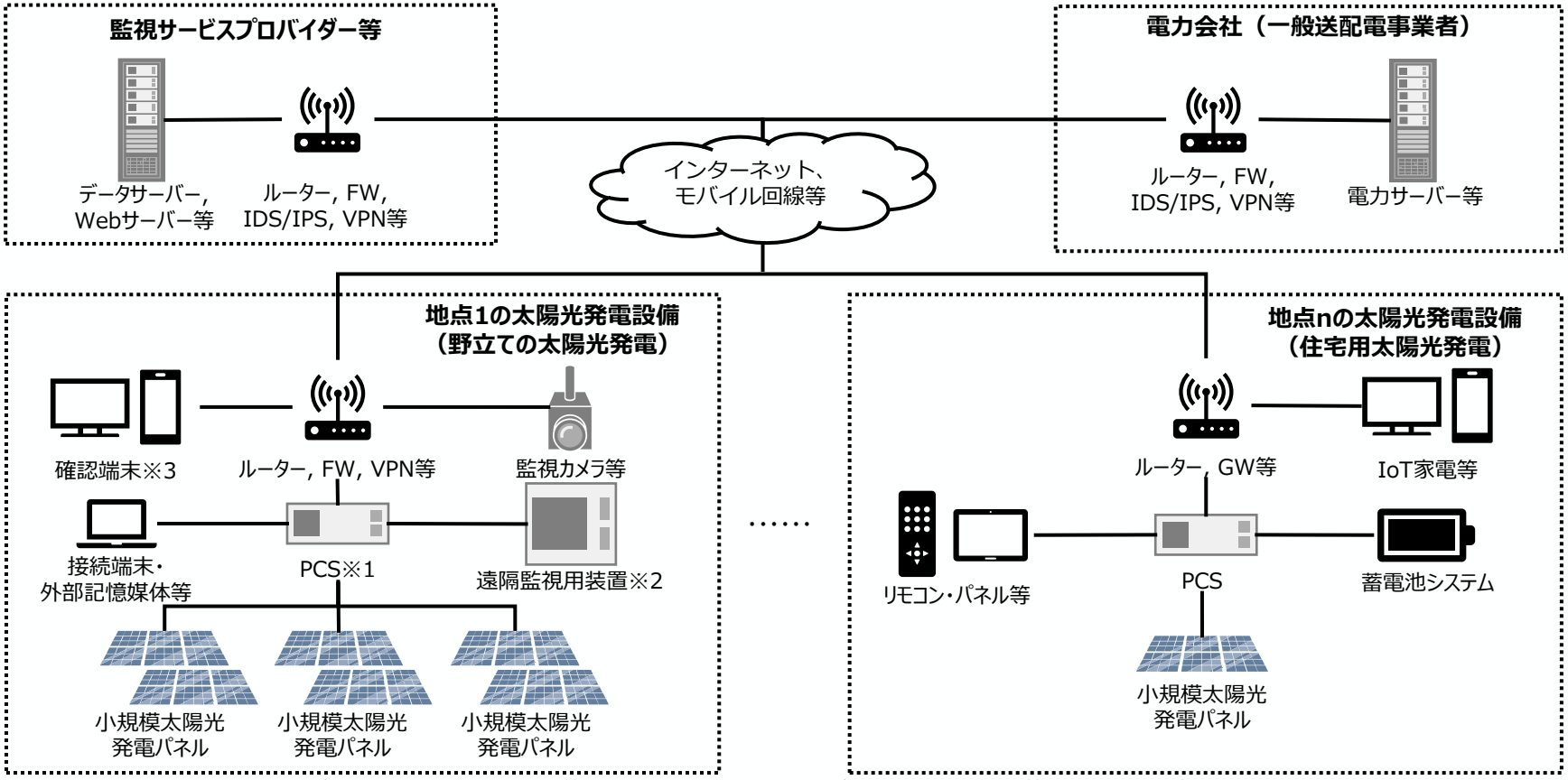
小規模太陽光発電設備に関するリスク分析結果

小規模太陽光発電設備に関する制度・文書等の整理結果

小規模太陽光発電設備に対するセキュリティ対策の方策

小規模太陽光発電設備の基本構成図（モデルシステム図）

- 小規模太陽光発電設備に対するサイバーセキュリティ上の脅威を分析するためのモデルシステム図を作成した。
- 複数台に対する同時多発的な脅威を考慮するために、複数の種別・地点の太陽光発電設備を考慮できる構成とした。



※1　PCSは、電力会社または配信事業者が提示する出力制御スケジュール情報を取得し、そのスケジュールに応じて発電出力を制御する機能を有するPCS（いわゆる「広義PCS」）を指す。
※2　PCSに対して別途接続される遠隔監視用装置を対象とするが、遠隔監視と出力制御の両方が一体化したPCSも販売されている。
※3　監視サービスにアクセスして発電状況等を確認する端末を指す。

小規模太陽光発電設備に想定される脅威

- 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。

PCSに関して求められる対策

- IPA「制御システムセキュリティリスク分析ガイド Ver2.0」等を参照した、**リスク度合いの高い脅威に対してPCSに求められる対策**の分析結果は以下のとおり。
- 小規模発電設備設置者の規模やセキュリティレベルを考慮したとき、設置者において厳格な対策を実施することには限界があることから、**PCSやそのメーカーにおいて対策を講じることが重要**。

リスク度合いの高い脅威	脅威に対して求められる対策	
	PCSにおける対策	PCSメーカーにおける対策
不正アクセス	【通信相手の認証】 ・通信相手（クライアント）の正当性を確認する機能を機器に実装する。 【パッチ適用】 ・機器に対して容易にパッチを適用できる仕組みを実装する。 【アクセス制限】 ・機器内の情報へのアクセスを制限するための機能を機器に実装する。	【パッチ適用】 ・機器に対するパッチ提供の体制を構築する。 ・機器利用者に対し、パッチ適用方法に関する情報を提供する。
不正操作	【操作者認証】 ・操作者の正当性を確認する機能を機器に実装する。	【適切な操作】 ・機器利用者に対し、セキュアな利用方法に関する情報を提供する。
高負荷攻撃	【DDoS対策】 ・多量の通信を受信したときの対応機能を機器に実装する。 【フェールセーフ設計】 ・異常発生時に安全に再起動できる機能を機器に実装する。	ー
不正媒体・接続機器	【デバイス接続・利用制限】 ・不要・未使用のサービスへ接続・利用できないよう、物理的又は論理的に接続口を無効化する。	ー
サプライチェーン攻撃	ー	【契約時のセキュリティリスク管理】 ・機器メーカーにおいて、機器の部品調達時におけるセキュリティリスクを考慮する。

※ リスク度合いの高い脅威を踏まえ、ネットワーク機器（ルーター、GWなど）においても同様の対策が求められることに留意。

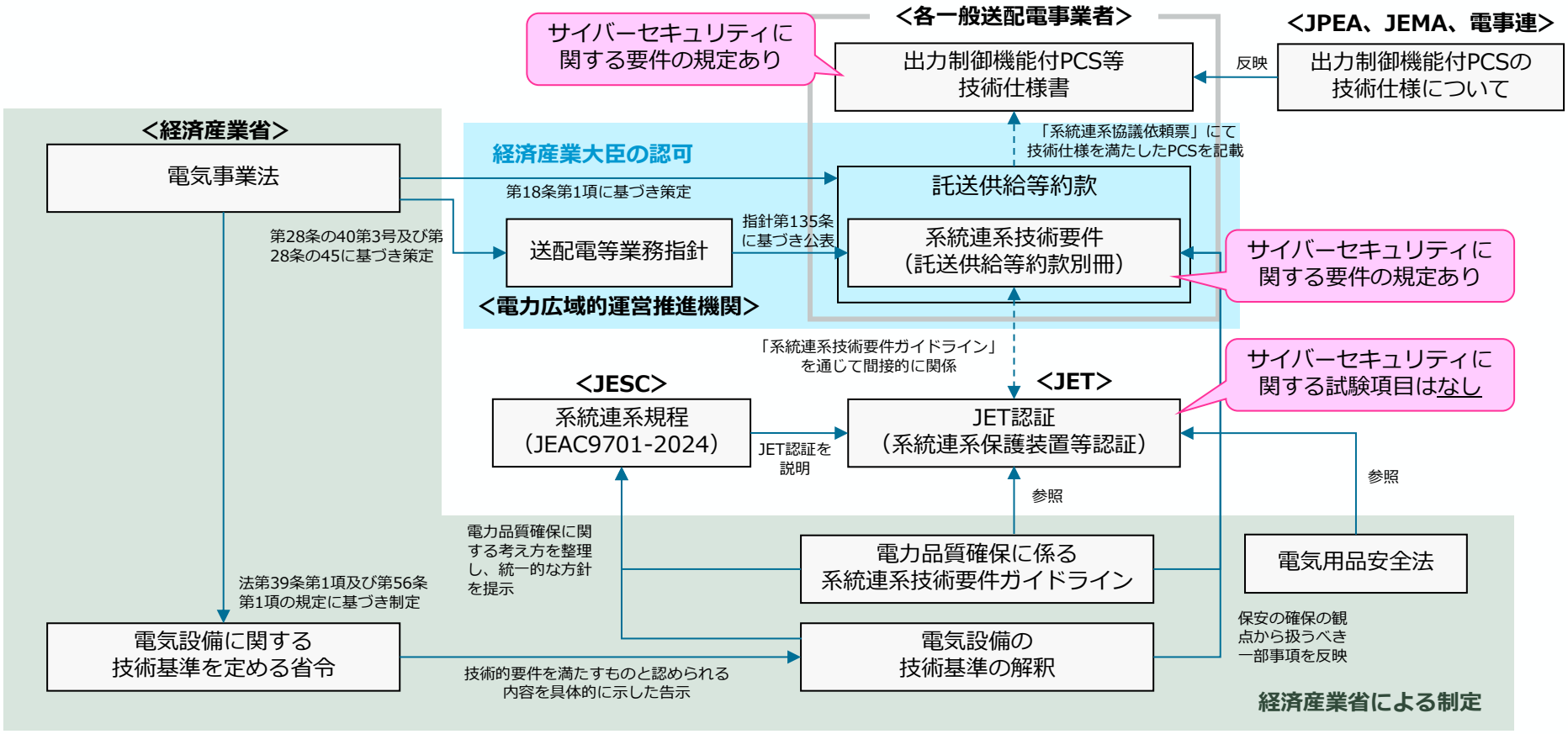
小規模太陽光発電設備に関するリスク分析結果

小規模太陽光発電設備に関する制度・文書等の整理結果

小規模太陽光発電設備に対するセキュリティ対策の方策

小規模太陽光発電設備の系統連系に関する制度・文書等

- 小規模太陽光発電設備の系統連系に関する制度・文書等は複数存在する。
- **<u>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</u>**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

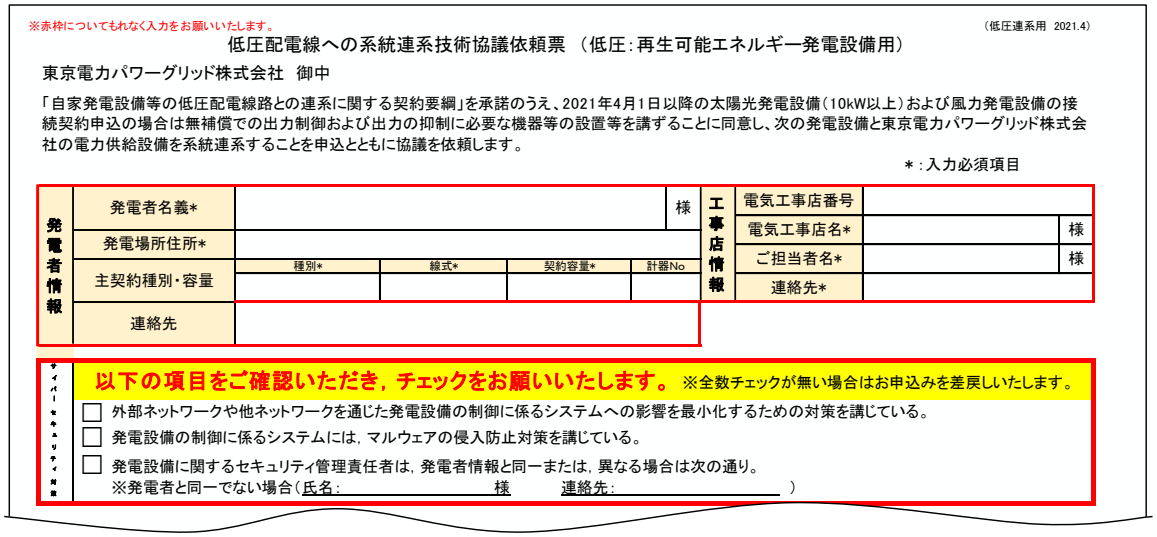
第17回電力SWG
（2024年10月22日）
資料を一部修正

- 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請ずることに同意し、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

PCSにおいて求められる対策に関するGap分析

- リスク分析を通じて導出された対策と現行制度における対策との比較は以下のとおり。
- **現行制度**においても、**小規模太陽光発電設備も含めてセキュリティ対策が求められている**が、その**実効性向上のため**、**具体的な対策を明示する**ことで、**事業者の取組を促進することが有効ではないか**。

← リスク分析を通じて導出された対策 → ← 現行制度で求められる対策 →

リスク度合いの高い脅威	脅威に対してPCS／PCSメーカーに求められる対策	対応する出力制御機能付PCS等技術仕様書の対策	対応する系統連系技術要件の対策
不正アクセス	【通信相手の認証】	• 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	• 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 • マルウェアの侵入防止対策を講じること
	【パッチ適用】	ー	
	【アクセス制限】	• 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	
不正操作	【操作者認証】	ー	ー
高負荷攻撃	【DDoS対策】	• 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	• 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
	【フェールセーフ設計】	ー	ー
不正媒体・接続機器	【デバイス接続・利用制限】	ー	ー
	【適切な操作】	ー	ー
サプライチェーン攻撃	【契約時のセキュリティリスク管理】	ー	ー

小規模太陽光発電設備に関するリスク分析結果

小規模太陽光発電設備に関する制度・文書等の整理結果

小規模太陽光発電設備に対するセキュリティ対策の方策

小規模太陽光発電設備に対するセキュリティ対策の方策

- 分散型電源の活用が進められる中で、**小規模太陽光発電設備についても、サイバー攻撃の被害が発生**したり、**セキュリティ上のリスクが指摘**されたりしている。こうした状況の中で、電力の安定供給を維持するためには、**小規模太陽光発電設備においても、適切なセキュリティ対策を講じていくことは重要**。
- 現行の**系統連系技術要件においても対策が求められている**が、具体的な対策は明らかにされておらず、適切な対策が取られていない事業者もいると考えられる。一方で、**小規模太陽光発電設備設置者の規模やそのセキュリティ対策能力を考慮したとき、設置者に対してのみに厳格な対策を求めることは困難と考えられる。**
- こうした中で、具体的な対策として以下が考えられるのではないか。

  ①PCSやそのメーカーにおいて、小規模太陽光発電の制御設備（PCS）において適切な対策を講じ、適切な対策が講じられている設備の利用を進める。
  ②小規模太陽光発電の制御に利用する通信等のサービスについて、セキュリティが確保されたサービスを利用する。
  ③小規模太陽光発電の制御装置も含む分散型電源について、それを管理するアグリゲーターが行うセキュリティ対策を強化する。
- このうち、①について、PCSメーカーにおけるセキュリティ対策の取組を進めるために、共通的な物差しでIoT製品の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制度）」と連携する**ことについて整理を行った。
- ②、③の方策については資料６－２、資料６－３において議論させていただく。

（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月に制度構築方針を公表。**9月30日にIPAから「JC-STAR」という制度名にて制度開始の案内**(※2)を実施。
- **★１については2024年度中の制度開始**を予定。**政府調達等の要件**等とすべく関係省庁と議論中。**米欧等の諸外国との制度調和**を図るため議論中。

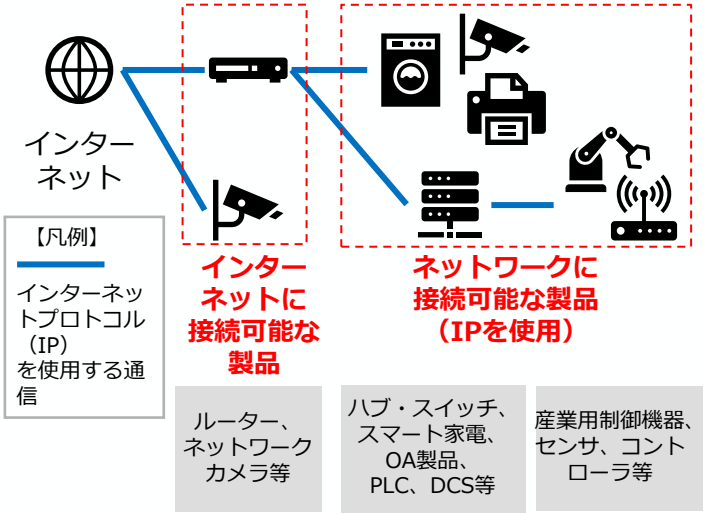
制度名称・ロゴ・ラベル

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)

JC-STAR

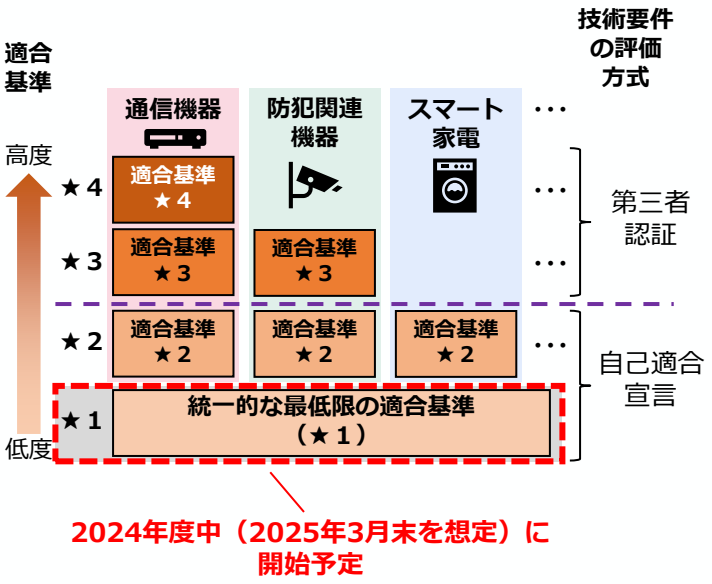
JAPAN CYBERSECURITY LABEL
JC-STAR
Registered ID:0123456789012345

対象製品の概要



※　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。

制度の概要（イメージ）



(※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「IoT製品に対するセキュリティ要件適合評価・ラベリング制度を開始します」 https://www.ipa.go.jp/pressrelease/2024/press20240930.html

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)

- 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

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。

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

- **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月末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）東アジア・ASEAN経済研究センター（ERIA）と連携した取組
～日ASEANにおける分散型エネルギーシステムの普及とサイバーセキュリティの確保

- 2024年度から、**ERIA**において、**アジア・ゼロエミッション共同体（AZEC）のイニシアティブに基づくプロジェクトの一つ**として、電力の脱炭素化に向けた**分散型エネルギーシステム（DES）の普及とサイバーセキュリティの確保推進に向けたプロジェクト**を実施中。
- 我が国からは、分散型電源の活用に向けた取組として、**エネルギーリソースアグリゲーションビジネス（ERAB）推進**に係る取組とともに、その**セキュリティ確保に向けたガイドライン（サイバー・フィジカル・セキュリティフレームワークやERABセキュリティガイドライン）**や**IoTセキュリティの取組（JC-STAR制度）**、慶應義塾大学サイバー文明研究センター(CCRC)からは学術的取組、またIEC（国際電気標準会議）からは関連国際規格の最新状況、ASEAN各国からは最新研究状況が、ワークショップで紹介された。
- 2025年春に、インドネシアにおいて日ASEANの産官学が参加するカンファレンスを開催する予定であり、現在整理を進めている**日ASEANの分散型電源の活用に関するサイバーセキュリティ確保のコンセプトをまとめた文書等の公表を行う予定。**

＜2025年1月22日のワークショップの様子＞

＜今年度の取組＞

- 2024年10月15日、**ERIA事務所（インドネシア・ジャカルタ）にて初回ワークショップを開催。**
- 2025年1月20日、22日、**ASEAN議長国であるマレーシアにおいて、テストベッドの見学を含む専門家議論と、ワークショップが開催された。**
- 2025年4月頃にプロジェクトのまとめとして、インドネシアにて大規模カンファレンスを開催する予定であり、**日ASEANの分散型電源の活用に関するサイバーセキュリティ確保の考え方**について公表し、ASEAN各国における分散型電源のセキュリティ確保の取組につなげる。

（出所）https://www.eria.org/news-and-views/eria-and-ipv6-forum-malaysia-host-workshop-on-cybersecurity-for-energy---iot