経済産業省

資料５－１

小規模太陽光発電設備の
サイバーセキュリティ対策の課題について

2024年10月22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対策検討の必要性

- 電力分野における近年の変化として、カーボンニュートラルに向けた動きの影響等により、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。
- 分散型電源について、一つ一つのリソースは小さく、系統への影響も限られていることもあり、従来、大規模な発電設備やその運営者と比較して、サイバーセキュリティ対策が厳格には求められてこなかった部分がある。
- しかしながら、近年、季節や天候等によっては、太陽光発電の発電量が需給全体の大きな部分を占める時間帯も発生するなど、分散型電源による需給全体や系統への影響も大きくなっている。
- そうした中で、例えば、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高まっている。
- これらの状況に鑑み、特に懸念度合いが高い小規模太陽光発電設備※を主な対象として、脅威や規制の状況を整理するとともに、想定されるリスクに対して求められる方策を検討する。

※ 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。

（参考）電気工作物の区分

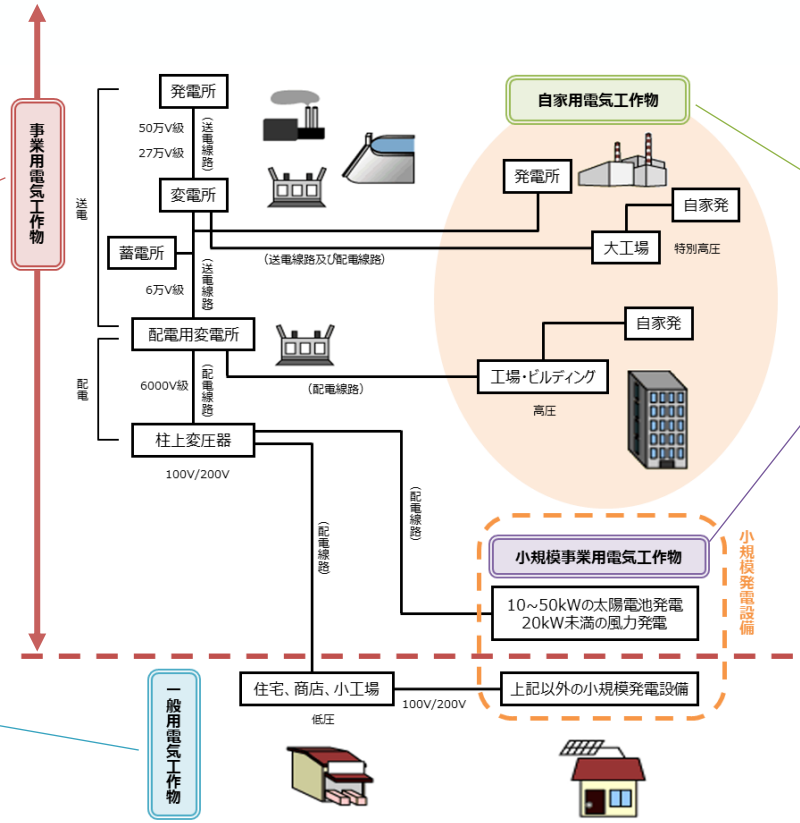
- 電気工作物は、事業用電気工作物（法第38条第２項）、自家用電気工作物（法第38条第4項）、小規模事業用電気工作物（法第38条第3項）、一般用電気工作物（法第38条第1項）に区分される。

・一般用電気工作物以外の電気工作物。

・電気事業法に基づいて事業用電気工作物を設置するためには、保安規程の届出や主任技術者の選任などの安全の確保のための措置を取らなければ設置できない。
（例）発電所、変電所、送電線路、工場・ビルなど

・一般用電気工作物とは比較的電圧が小さく安全性の高い電気工作物をいい、一般電気工作物を設置するためには保安規程の届出や主任技術者の選任などが不要であるため、一般家庭等に容易に設置することができる。

（例）一般家庭、商店、コンビニ、小規模事務所等の屋内配線、一般家庭太陽光発電



・電気事業※の用に供する事業用電気工作物以外の事業用電気工作物。
（例）自家用発電設備、工場ビルなどの600Vを超えて受電する需要設備

※一般送配電事業、送電事業、配電事業、特定送配電事業、一部の発電事業

・小規模事業用電気工作物※については、保安規程の届出や主任技術者の選任は不要であるが、基礎情報の届出と使用前自己確認が必要。

※10kW以上50kW未満の太陽電池発電設備、20kW未満の風力発電設備

出所）経済産業省, 電気工作物の保安 https://www.meti.go.jp/policy/safety_security/industrial_safety/sangyo/electric/detail/setsubi_hoan.html

太陽光発電設備の区分

- 太陽光発電導入に関わる主な法律には「建築基準法」と「電気事業法」がある。
- システム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。

電気工作物の区分		太陽光発電の発電出力	発電事業届出	工事計画	主任技術者	保安規程
一般用電気工作物		10kW未満（※1）	不要	不要	不要	不要
事業用電気工作物	小規模事業用電気工作物	10kW以上50kW未満	不要	不要	不要	不要
				※小規模事業用電気工作物には、保安の観点から、**基礎情報の届出**、**使用前自己確認の結果の届出**等の義務を課している。		
	自家用電気工作物	50kW以上2,000kW未満	不要（※3の場合は届出）	不要	選任/外部委託（※2）	届出
		2,000kW以上	不要（※3の場合は届出）	届出	選任	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	届出	選任	届出

※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。

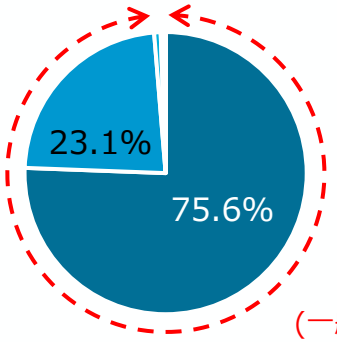
※3.①出力が1,000kW以上、②託送契約上の同時最大受電電力が5割超、③年間の逆潮流量(電力量)が5割超の3つのいずれの条件にも該当する発電等用電気工作物から、小売電気事業等の用に供する電力の合計が1万kWを超えるもの。

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/

太陽光発電設備の国内導入状況（FIT認定導入件数・容量）

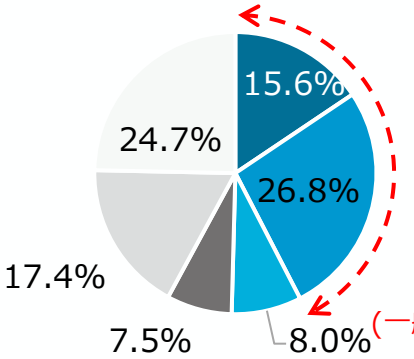
- 太陽光発電設備に関する2024年3月末のFIT認定設備導入件数は約286万件であり、うち**98.7%が50kW未満の小規模太陽光発電設備（一般用及び小規模事業用）**である。
- 容量ベースでは、**42.4%を小規模太陽光発電設備が占める**。

FIT認定設備導入件数（2024年3月末）



98.7%
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)

FIT認定設備導入容量（2024年3月末）



42.4%
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)

設備区分	件数（件）	比率
住宅10kW未満	2,160,542	75.6%
低圧10-50kW	660,127	23.1%
高圧50-500kW	21,228	0.74%
高圧500-1MW	7,316	0.26%
高圧1-2MW	7,822	0.27%
特高2MW以上	986	0.03%
合　計	2,858,021	100.0%

設備区分	容量（kW）	比率
住宅10kW未満	10,634,176	15.6%
低圧10-50kW	18,303,147	26.8%
高圧50-500kW	5,467,114	8.01%
高圧500-1MW	5,111,362	7.49%
高圧1-2MW	11,883,395	17.4%
特高2MW以上	16,828,758	24.7%
合　計	68,227,952	100.0%

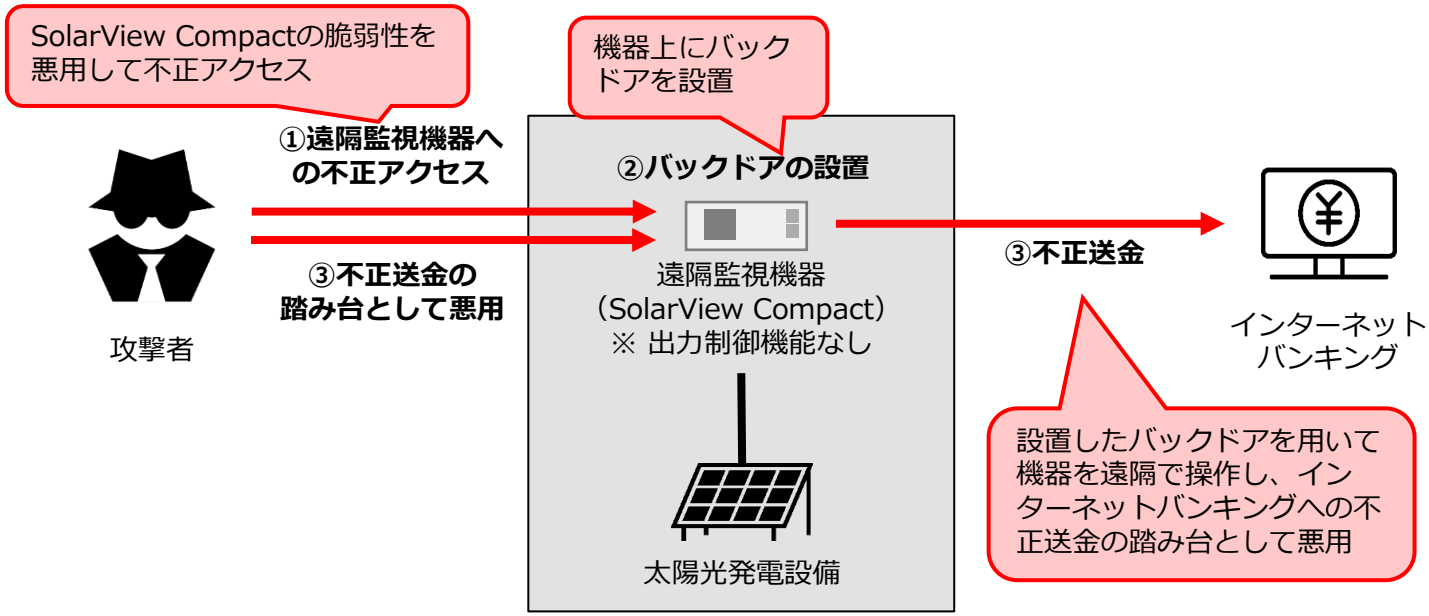
出所）資源エネルギー庁, 再生可能エネルギー電気の利用の促進に関する特別措置法　情報公表用ウェブサイトに基づき作成 https://www.fit-portal.go.jp/PublicInfoSummary

小規模太陽光発電設備に関する脅威事例

(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



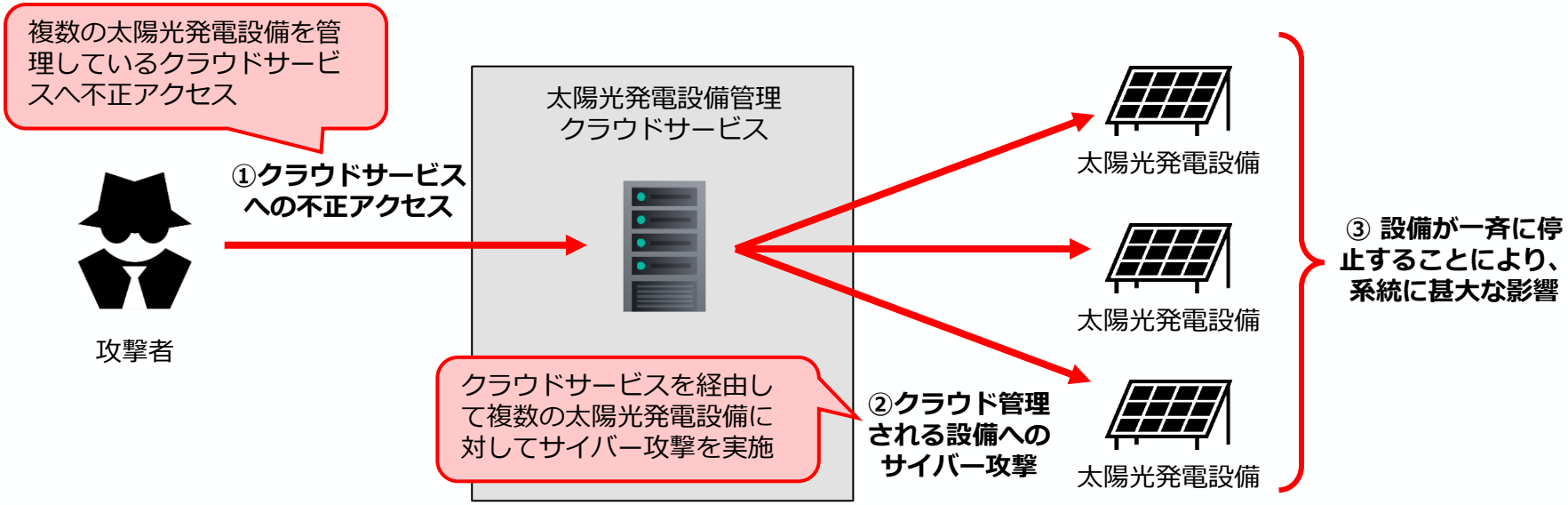
出所）以下の公開情報等に基づき三菱総合研究所作成
https://www.contec.com/jp/info/2024/2024050700/ ，https://www.trendmicro.com/ja_jp/jp-security/24/f/security-strategy-20240606-01.html

小規模太陽光発電設備に関する脅威事例

(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

太陽光発電設備に対するサイバーセキュリティ対策規制の状況

- 「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。
- ただし**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			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			無し（※）	ー	有り
事業用電気工作物	小規模事業用電気工作物		無し（※）	ー	有り
	自家用電気工作物		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
	電気事業の用に供する事業用電気工作物		有り	電力制御システムセキュリティガイドライン	有り

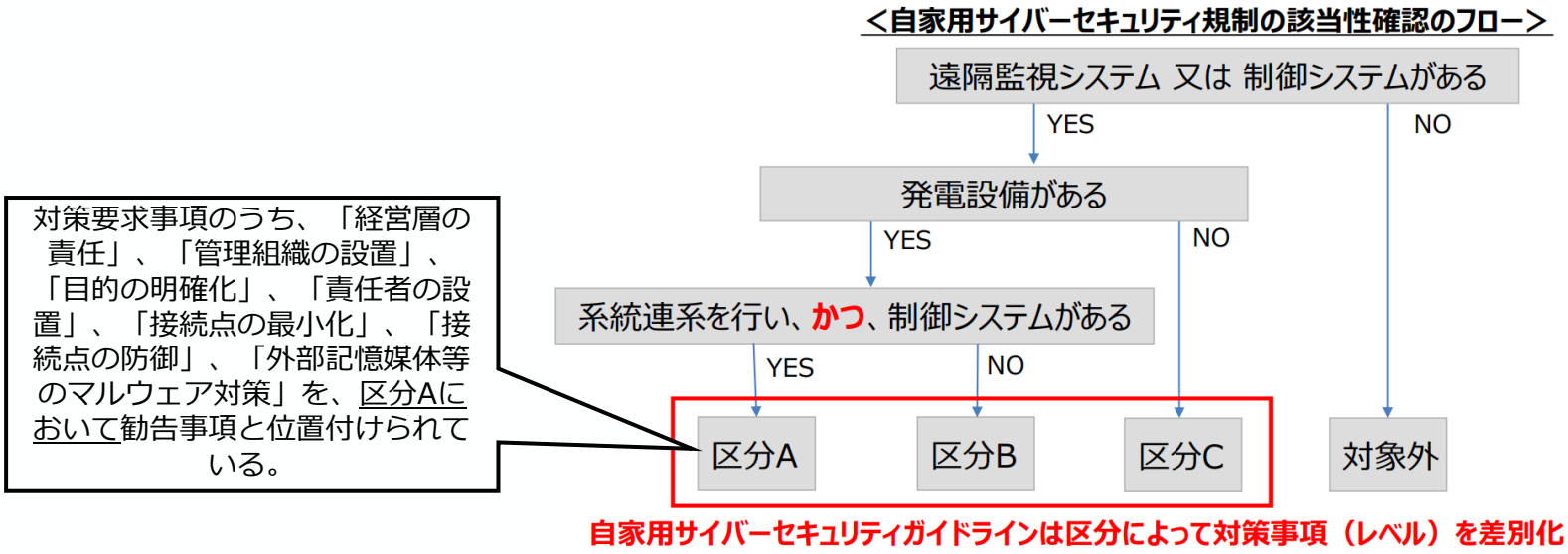
（※）50kW未満の小規模太陽光発電設備（一般用及び小規模事業用）については、電気事業法上、サイバーセキュリティの確保に特化した明確な技術基準の規定までは無い。

（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。）

（参考）自家用電気工作物サイバーセキュリティガイドラインの概要

- 「電気設備に関する技術基準を定める省令」及び「電気設備の技術基準の解釈」の改正に伴い、2022年10月1日より、自家用電気工作物においてもサイバーセキュリティの確保を義務付け。
- 対策にあたって、「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」（2022年10月1日施行、2023年3月20日最終改正）に基づく対策が求められる。
- 本ガイドラインは「電力制御システムセキュリティガイドライン」をベースとした内容となっているが、一部の項目を除き、事業者自らが実施の要否及び実施方法を判断する「推奨」事項として設定されている。
- また、対象設備は区分A～区分Cに分類され、区分により「勧告」又は「推奨」となる条項が異なる。

「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 」の対象設備区分と対策要求の概要



出所）経済産業省、「自家用電気工作物におけるサイバーセキュリティ対策について」の制定について
https://www.meti.go.jp/policy/safety_security/industrial_safety/oshirase/2022/07/20220706-1.pdf

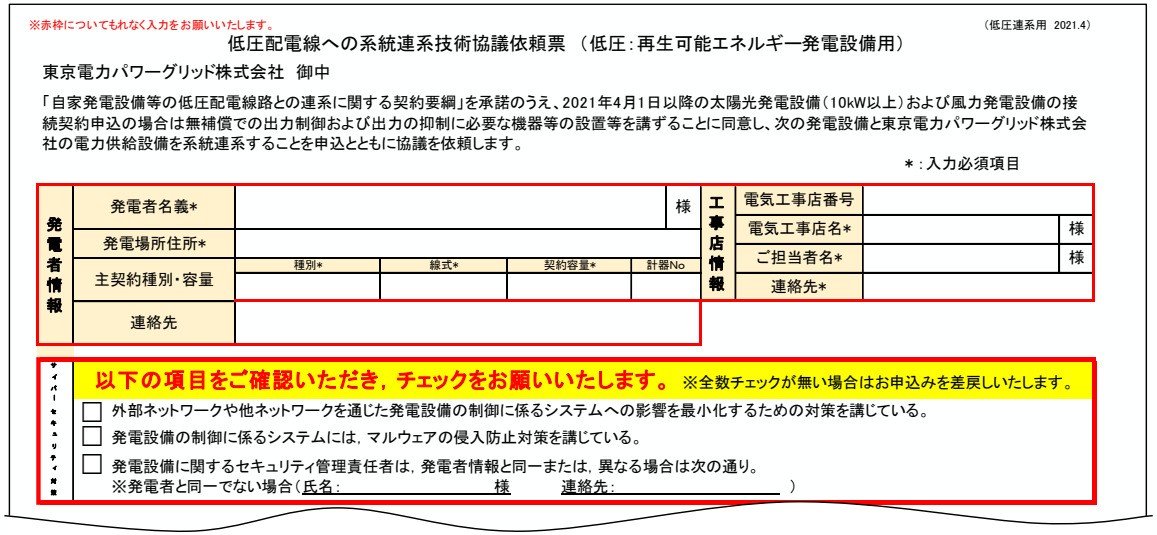
（参考）系統連系技術要件の概要

- 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。

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

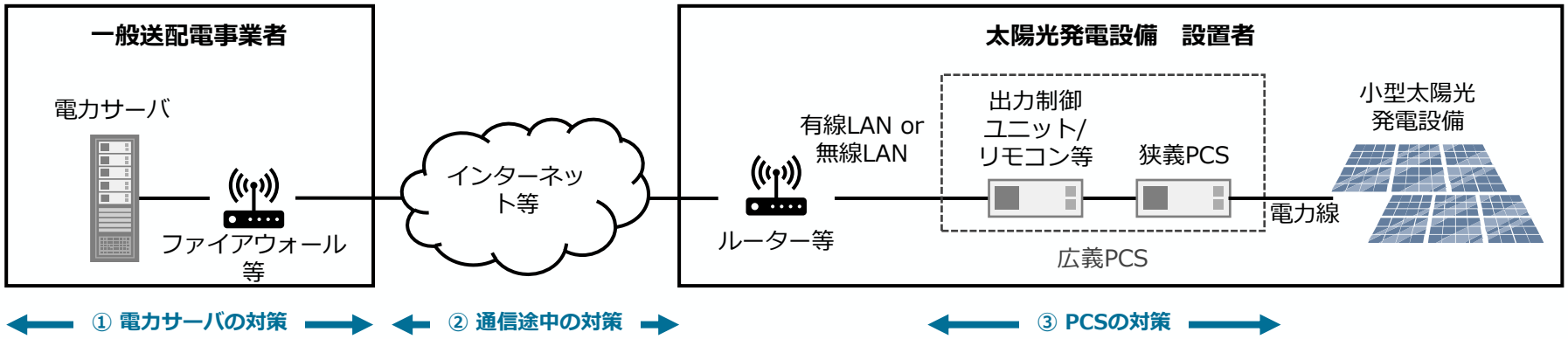
以下の項目をご確認いただき，チェックをお願いいたします。 ※全数チェックが無い場合はお申込みを差戻しいたします。

- ☐ 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

出力制御機能付きPCSに対するセキュリティ対策の状況

- 「出力制御機能付PCSの技術仕様」では、出力制御システムに対して想定される脅威が整理され、脅威に対して求められる各構成要素の対策が整理されている。
- **外部からのセッション開始不可、スケジュール設定のバックアップ、通信先の指定、SSL通信（暗号化）**が技術仕様上のセキュリティ対策として求められている。



想定される脅威		システムの対策	
電力サーバ	①ウイルス感染 ②サイバー攻撃 ③不正侵入／不正通信 ④PCSなりすまし	電力サーバ ①	・ファイアウォール ・サーバ2重化　など ・スケジュール設定のバックアップ ・ID認証（PCSとの相互確認）
通信途中	⑤データ改ざん ⑥盗聴・漏えい	通信途中 ②	・SSL通信による暗号化 ・重要情報を含めない
PCS	⑦ウイルス感染 ⑧サイバー攻撃 ⑨不正侵入／不正通信 ⑩サーバなりすまし	PCS ③	・外部からのセッション開始不可 ・スケジュール設定のバックアップ ・通信先として電力サーバを指定 ・SSL通信

出所）太陽光発電協会, 日本電機工業会, 電気事業連合会, 出力制御機能付ＰＣＳの技術仕様について
https://www.meti.go.jp/shingikai/enecho/shoene_shinene/shin_energy/keito_wg/pdf/005_02_00.pdf

国内外の取組の比較分析

- 小規模太陽光発電設備は、**諸外国の規制においても規制範囲の対象外**に位置づけられる。
- 一方で、**一部の国・地域では、PCS等のインターネットに接続する設備に対して、法的な対策義務を課している**。

国・地域				
法規制上の対策義務	電気事業法上、技術基準の適合義務における明確な規定はなし※1	連邦電力法の規制基準（NERC CIP基準）の対象外	NIS2指令による規制の対象外	NIS Regulationによる規制の対象外
系統接続時の対策義務	「系統連系技術要件」に基づく対策義務あり	系統接続ルールを定めたFERC Order（No.827, 842）では対策義務に関する規定なし	Network Code on Cybersecurityにより、系統接続される設備のリスクマネジメントが義務化	Grid Codeにおいて対策義務が規定されているが、小規模太陽光発電は対象外（NIS Regulationの対象に限定）
設備（PCS等）に対する対策義務	「出力制御機能付PCSの技術仕様」において出力抑制用PCSに対する対策を整理	国全体での対策義務はなし ただし、カリフォルニア州及びオレゴン州のみ対策義務あり※2	現状は対策義務なし ただし、サイバーレジリエンス法（EU-CRA）施行後は対策義務あり	PSTI法に基づく対策義務あり※3

※1 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。）。

※2.カリフォルニア州は「California Civil Code Division 3 Part. 4 Title 1.81.26. Security of Connected Devices」、オレゴン州は「Oregon Revised Statutes Vol. 16 Title 50 Chapter 646A. 813: Security requirements for Internet-connected devices」に基づく。いずれも太陽光発電設備のみを対象とした法律ではなく、IoT製品全般を対象としたものである。求められる要件として、適切な認証方法の実装とデータ保護が求められる。いずれの法律も違反時のペナルティに関する規定はない。

※3.太陽光発電設備のみを対象とした法律ではなく、IoT製品全般を対象としたものである。求められる要件として、出荷時に共通パスワードを設定しないこと、脆弱性情報の報告方法を提供すること、製品のセキュリティサポート期間を明示することが挙げられる。違反した場合、最大1,000万ポンド又は事業者世界売上高の4%の罰金が科される。

小規模太陽光発電設備の対策に関して求められる取組について

- カーボンニュートラルへの取組の推進等に伴い、分散型電源が普及し、小規模太陽光発電による需給全体への影響が高まる一方で、サイバー攻撃の事案が発生するなど、サイバーセキュリティ上の懸念が高まっている。今後、小規模太陽光発電に対して大規模なサイバー攻撃が発生すれば、系統に一定程度の影響を及ぼす可能性も否定できない。
- 国内では、一般送配電事業者が定める系統連系技術要件において最低限のセキュリティ対策が義務付けられている一方で、電気事業法上の明確な対策義務は存在しない。またPCSについては、「出力制御機能付PCSの技術仕様」において求められるセキュリティ対策が整理されている一方で、一部の国・地域では法的な対策義務が検討されている。
- こうした現状を踏まえれば、分散型電源の中でも、まずは、**小規模太陽光発電について**、**想定されるリスクを整理**したうえで、**小規模太陽光発電に関わる関係者に期待される役割や責任**を明らかにし、セキュリティ対策の実装にかかる負担や実効性なども考慮しつつ、**求められる方策を検討**することが必要ではないか。
- その際の対応の方向性として、**経済産業省・IPAの「セキュリティ要件適合評価及びラベリング制度（JC-STAR）」の活用やERAB事業者によるセキュリティ確保も考えられるのではないか**。