経済産業省

第21回　グリッドコード検討会　資料４

分散型電源のサイバーセキュリティ対策の要件化について

2026年3月31日

資源エネルギー庁

目次

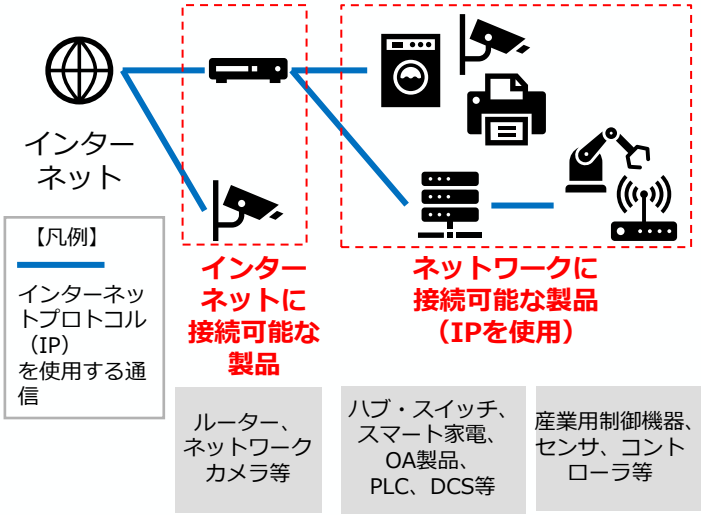
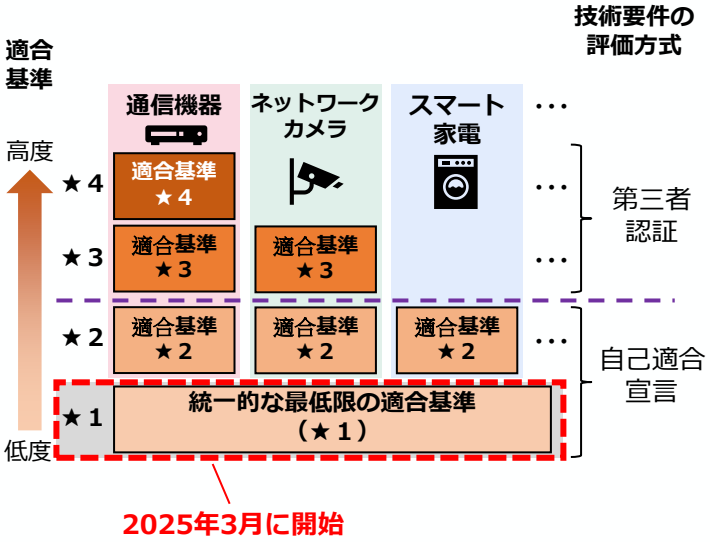
1．前回の振り返りと今回のご議論

- 諸外国では分散型電源に対するセキュリティ対策が検討されており、我が国においても、早期の対策強化が求められていることから、第20回グリッドコード検討会（2025年12月16日）において、**分散型電源を対象にJC-STAR制度の★1を取得した製品の使用の要件化についてご議論いただいた**。
- 特に、**太陽光や蓄電池について**は、今後も多数の連系が見込まれることを踏まえると、早期に対応する必要があることから、**2027年4月※から、系統連系にあたってJC-STAR★1を取得した製品の使用を必須の要件とすることとした。**

  ※低圧（50kW未満）で連系する製品については、メーカーがJC-STAR★1を取得した製品を導入した後も、一定期間、流通網に旧製品の在庫が一定数発生すると見込まれることから、2027年10月を適用開始時期とした。
- また、**風力発電や燃料電池**については、今回のグリッドコード検討会において、適用開始時期をご議論いただくことにした。
- 今回は、**風力発電および燃料電池のJC-STAR★1を取得した製品使用の要件化の適用範囲・適用開始時期**、および、**規程類の変更案**についてご議論いただきたい。

（参考）JC-STAR制度の概要

- **<u>IoT製品のセキュリティレベルを見える化するラベリング制度（JC-STAR）</u>**の最低限の基準となる★１の申請受付を2025年3月25日から開始。
- ラベル普及に向け**<u>政府調達等の要件</u>**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。
- **<u>米欧等の諸外国との制度調和</u>**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

２．風力発電へのJC-STAR★1の適用開始時期

- 風力発電及び燃料電池に係るサイバーセキュリティ対策の要件化について、関係業界及びメーカーに対するヒアリングを実施した。
- **風力発電**については、多くの設備が海外メーカー製であることに加え、**他の電源種と比較して IP 通信を用いる機器が多く**、**これらの機器全てを同時にJC-STAR★1対応させようとすると、対応に時間を要する**ことが確認された。このため、**通信機能を有する制御システムについて JC-STAR★1の取得を求めることを基本**とするものの、**優先順位を付した上で順次対応を進める**こととしてはどうか。
- 具体的には、まずは、**ウィンドファームと外部通信との結節点として重要な役割を担うゲートウェイのファイアウォール（又はこれと同等の防御機能を有する機器）について、2027年4月であればJC-STAR★1に対応した機器の導入が可能であることが確認できたため、同月から要件化することとしてはどうか**。
- なお、ゲートウェイ以外のシステムについても、**可能な限り速やかに JC-STAR制度に基づく認証の取得を進めるよう、対応を求めるものとし、その対象範囲や適用開始時期については本検討会で追ってご議論いただく**。

３．燃料電池へのJC-STAR★1の適用開始時期

- 燃料電池※1については、家庭用燃料電池の場合、燃料電池本体と給湯器との組合せに係る評価を含めた性能・安全性等についての検証、JC-STAR★1に対応するための開発、第三者認証及びJC-STARの取得を順次実施する必要があり、多くのメーカーにおいて、**JC-STAR★1を取得した機器の導入が、2028年4月までに完了する見込みであることが確認された**。このため、同月から要件化することとしてはどうか。

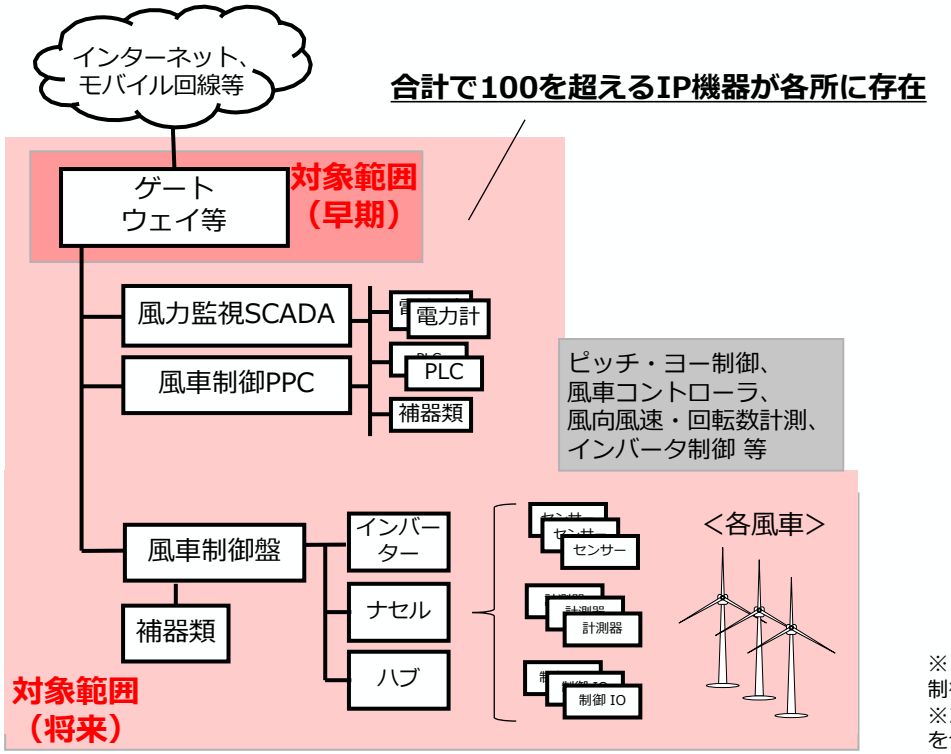
  ※1：PCSを介して連系するガスエンジンも含む

- なお、**既存在庫の流通・整理に一定の期間を要する可能性**があるが、2028年4月まで2年程度あることから、**メーカーの対応状況を確認しつつ、必要があれば経過措置期間の必要性について議論**することとしてはどうか。

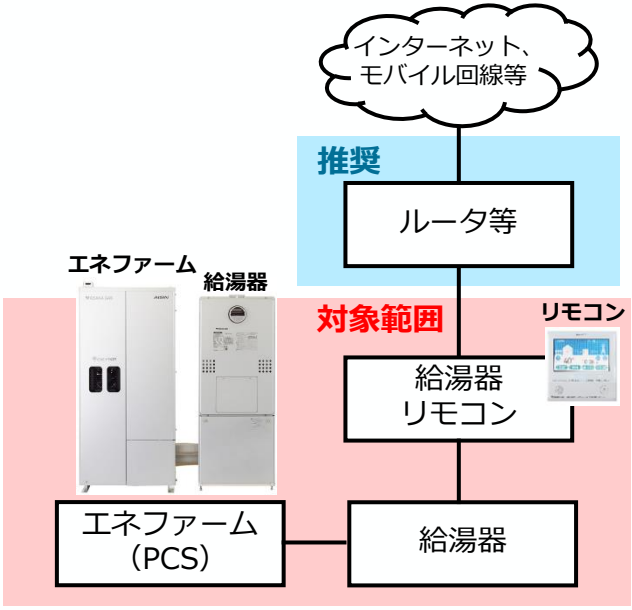
(参考)風力発電および燃料電池における サイバーセキュリティ対策要件化の対象設備

- 以上を踏まえると、下図※1の対象範囲のうち**IP通信を用いる製品（システム）がJC-STARの取得要件化の対象**となる。
- なお、サイバーセキュリティ対策の観点では、対象範囲外にあるIP通信機器※2においてもJC-STARを取得した製品を用いることが推奨される。

風力発電の主なシステム構成



燃料電池（家庭用）の主なシステム構成



※1：システム構成の一例であり、その他のケースも含め、分散型電源が採用する通信機能を有する制御システムが対象となる
※2：対象範囲外の機器においても、発電等設備に対する制御機能を有する場合や、ゲートウェイ等を介さずに主要な構成製品に連携する場合はJC-STAR取得要件化の対象となる

分散型電源のサイバーセキュリティ対策要件化(まとめ)

- これまでの議論を踏まえて、各分散型電源のサイバーセキュリティ対策要件化の適用開始時期および適用範囲は以下の通りとなる。
- なお、今後、JC-STAR制度★2以上の基準の整備や導入についても議論の動向を踏まえ要件化を進めていく。

分散型電源のサイバーセキュリティ対策要件化　まとめ

電源種	適用開始時期	適用範囲
太陽光発電	特高・高圧：2027年4月 低圧：2027年10月	通信機能を有する制御システム （PCS、EMS等）
蓄電池	特高・高圧：2027年4月 低圧：2027年10月	
燃料電池※1	2028年4月※2	
風力発電	2027年4月	ゲートウェイのファイアウォール（又は同等の防御機能を有する機器）に限定して早期適用 ただし、他の機器も速やかに対応

※1：燃料電池の内、PCSを用いる形式が対象（PCSを介して連系するガスエンジンも含む）
※2：必要に応じて経過措置を導入を検討

3．規程の変更案

- 分散型電源のサイバーセキュリティ対策の要件化に伴う規程類の変更内容は、以下のとおりである。

■電力品質確保に係る系統連系技術要件ガイドライン（資源エネルギー庁）

現行	改定案
記載なし。	第２章 連系に必要な技術要件 第１節 共通事項 ５．分散型電源のサイバーセキュリティ対策 近年、分散型電源を標的としたサイバー攻撃のリスクが高まっていることから、電力システム全体の信頼性および安全性を確保するため、連系される設備において必要なサイバーセキュリティ対策を講じるものとする。 具体的には、分散型電源が採用する通信機能を有する制御システムのうち、IP通信を用いる機器について、独立行政法人情報処理推進機構のセキュリティ要件適合評価及びラベリング制度に基づくレベル１以上の認証を取得した機器を用いることとする[注1]。 ただし、一般用電気工作物にあってはインターネット回線との接続に用いるルータ等および一般用電気工作物も含めた全ての電気工作物にあってはゲートウェイ等を介する監視カメラ等を除く。 なお、対象範囲外の機器においても、発電等設備に対する制御機能を有する場合や、ゲートウェイ等を介さずに主要な構成製品に連携する場合は対象とする。 注1：具体的には以下の分散型電源を対象とし、下記の時期以降に系統アクセスにおける契約申込みを行う案件から適用する。 特別高圧および高圧に連系する太陽光発電設備および蓄電設備：2027年4月 低圧に連系する太陽光発電設備および蓄電設備：2027年10月 風力発電：2027年4月（ゲートウェイのファイアウォール（又は同等の防御機能を有する機器）に限定。） 燃料電池：2028年4月（逆変換装置を用いた形式が対象。また、PCSを介して連系するガスエンジンも含む。必要に応じて経過措置を導入。）

３．規程の変更案

■系統連系技術要件（各一般送配電事業者：低圧）

現行	改定案
１９ サイバーセキュリティ対策 自家用電気工作物（発電事業の用に供するもの及び小規模事業用電気工作物を除く。）に係る遠隔監視システム及び制御システムは，「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」に準拠した対策を講じていただきます。 上記以外の発電設備等については，サイバー攻撃による発電設備等の異常動作を防止し，または発電設備等がサイバー攻撃を受けた場合に速やかな異常の除去，影響範囲の局限化などを行うために次のとおり，適切なサイバーセキュリティ対策を講じていただきます。 (1)　外部ネットワークや他ネットワークを通じた発電設備等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ること。 (2)　発電設備等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ること。 (3)　発電者と当社との間で迅速かつ的確な情報連絡を行い，速やかに必要な措置を講じる必要があるため，発電設備等に関し，セキュリティ管理責任者を設置するとともに，氏名及び一般加入電話番号，または携帯電話番号を通知すること。	１９ サイバーセキュリティ対策 自家用電気工作物（発電事業の用に供するもの及び小規模事業用電気工作物を除く。）に係る遠隔監視システム及び制御システムは，「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」に準拠した対策を講じていただきます。 上記以外の発電設備等については，サイバー攻撃による発電設備等の異常動作を防止し，または発電設備等がサイバー攻撃を受けた場合に速やかな異常の除去，影響範囲の局限化などを行うために次のとおり，適切なサイバーセキュリティ対策を講じていただきます。 (1)　外部ネットワークや他ネットワークを通じた発電設備等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ること。 (2)　発電設備等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ること。 (3)　発電者と当社との間で迅速かつ的確な情報連絡を行い，速やかに必要な措置を講じる必要があるため，発電設備等に関し，セキュリティ管理責任者を設置するとともに，氏名及び一般加入電話番号，または携帯電話番号を通知すること。 (4)　電力品質確保に係る系統連系技術要件ガイドラインにおいて求められている認証を取得した機器とすること。

3．規程の変更案

■系統連系技術要件（各一般送配電事業者：高圧）

現行	改定案
２３ サイバーセキュリティ対策 事業用電気工作物（発電事業の用に供するものに限る。）は，電気事業法に基づき，「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ていただきます。 自家用電気工作物（発電事業の用に供するもの及び小規模事業用電気工作物を除く。）に係る遠隔監視システム及び制御システムは，「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」に準拠した対策を講じていただきます。 上記以外の発電設備等については，サイバー攻撃による発電設備等の異常動作を防止し，または発電設備等がサイバー攻撃を受けた場合に速やかな異常の除去，影響範囲の局限化などを行うために次のとおり，適切なサイバーセキュリティ対策を講じていただきます。 (1)　外部ネットワークや他ネットワークを通じた発電設備等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ること。 (2)　発電設備等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ること。 (3)　発電設備等に関し，セキュリティ管理責任者を設置すること。	２３ サイバーセキュリティ対策 (1)　事業用電気工作物（発電事業の用に供するものに限る。）は，電気事業法に基づき，「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ていただきます。 (2)　自家用電気工作物（発電事業の用に供するもの及び小規模事業用電気工作物を除く。）に係る遠隔監視システム及び制御システムは，「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」に準拠した対策を講じていただきます。 (3)　(1)及び(2)以外の発電設備等については，サイバー攻撃による発電設備等の異常動作を防止し，または発電設備等がサイバー攻撃を受けた場合に速やかな異常の除去，影響範囲の局限化などを行うために次のとおり，適切なサイバーセキュリティ対策を講じていただきます。 a　外部ネットワークや他ネットワークを通じた発電設備等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ること。 b　発電設備等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ること。 c　発電設備等に関し，セキュリティ管理責任者を設置すること。 (4)　発電設備等を構成する機器については，電力品質確保に係る系統連系技術要件ガイドラインにおいて定められた認証を取得した機器としていただきます。

3．規程の変更案

■系統連系技術要件（各一般送配電事業者：特別高圧）

現行	改定案
２５ サイバーセキュリティ対策 事業用電気工作物（発電事業の用に供するものに限る。）は，電気事業法に基づき，「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ていただきます。 自家用電気工作物（発電事業の用に供するもの及び小規模事業用電気工作物を除く。）に係る遠隔監視システム及び制御システムは，「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」に準拠した対策を講じていただきます。 上記以外の発電設備等については，サイバー攻撃による発電設備等の異常動作を防止し，または発電設備等がサイバー攻撃を受けた場合に速やかな異常の除去，影響範囲の局限化などを行うために次のとおり，適切なサイバーセキュリティ対策を講じていただきます。 (1)　外部ネットワークや他ネットワークを通じた発電設備等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ること。 (2)　発電設備等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ること。 (3)　発電設備等に関し，セキュリティ管理責任者を設置すること。	２５ サイバーセキュリティ対策 (1)　事業用電気工作物（発電事業の用に供するものに限る。）は，電気事業法に基づき，「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ていただきます。 (2)　自家用電気工作物（発電事業の用に供するもの及び小規模事業用電気工作物を除く。）に係る遠隔監視システム及び制御システムは，「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」に準拠した対策を講じていただきます。 (3)　(1)及び(2)以外の発電設備等については，サイバー攻撃による発電設備等の異常動作を防止し，または発電設備等がサイバー攻撃を受けた場合に速やかな異常の除去，影響範囲の局限化などを行うために次のとおり，適切なサイバーセキュリティ対策を講じていただきます。 a　外部ネットワークや他ネットワークを通じた発電設備等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ること。 b　発電設備等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ること。 c　発電設備等に関し，セキュリティ管理責任者を設置すること。 (4)　発電設備等を構成する機器については，電力品質確保に係る系統連系技術要件ガイドラインにおいて定められた認証を取得した機器としていただきます。

３．他の規程の変更要否

■送配電等業務指針（電力広域的機関運営推進機関）

現行記載	変更要否
第１３５条（系統連系技術要件） 系統連系技術要件には、法令及び送配電等業務指針のほか、電力品質確保に係る系統連系技術要件ガイドラインその他の規程等を踏まえ、発電設備等及び需要設備を系統と連系する際に必要となる内容を定めなければならない。	変更なし。

■系統アクセスルール（各一般送配電事業者）

現行記載	変更要否
系統連系技術要件に準じた記載あり	系統連系技術要件と同様の記載を追加する必要がある。

■系統連系規程（日本電気協会）

現行記載	変更要否
記載なし	ガイドラインの改正を踏まえ反映予定。