

# グリッドコードについて

2026年2月9日

資源エネルギー庁

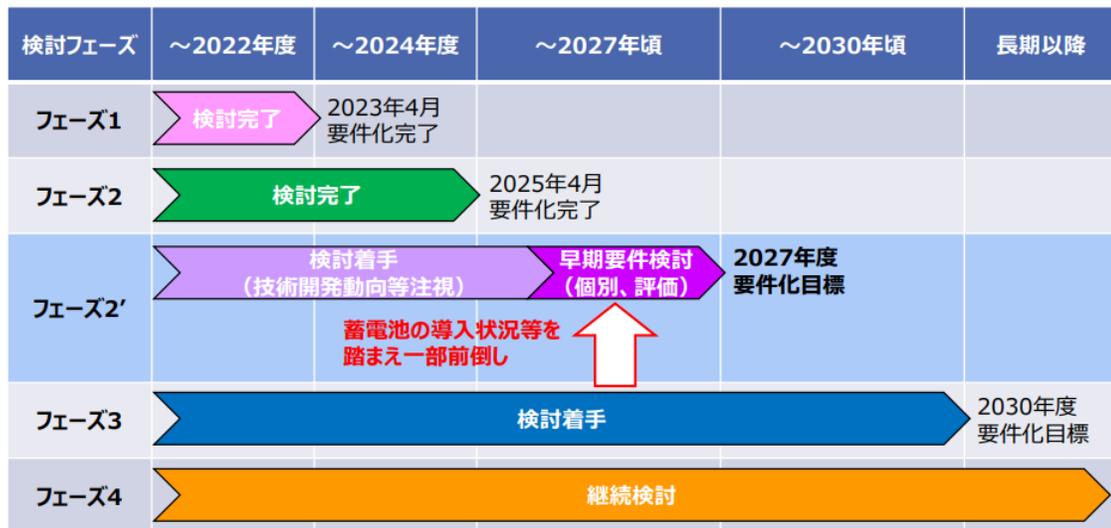
# 本日の御報告

- 新規に系統に接続される電源が遵守すべき技術要件を定めたグリッドコードの見直しについては、再エネの導入拡大を見据え、第20回系統WG（2019年3月18日）での議論を経て、電力広域的運営推進機関の検討会において検討が行われている。
- 検討にあたっては、再エネ導入比率に応じて、技術要件化の時期をフェーズ1:短期（2023年4月）、フェーズ2:中期（2025年前後）、フェーズ3:長期（2030年前後）、フェーズ4以降:継続検討と分類して検討を進めてきた。
- また、蓄電池の導入状況や最新の知見を踏まえ、フェーズ3目標期限「2030年前後」を待たずに検討が必要な技術要件を抽出し、「フェーズ2'」として分類し、足元ではフェーズ2'の2027年度要件化を目標に検討を進めている。
- 本日は、グリッドコード検討会の検討状況と、2027年にグリッドコード化が決定した分散型電源のサイバーセキュリティ対策について御報告する。

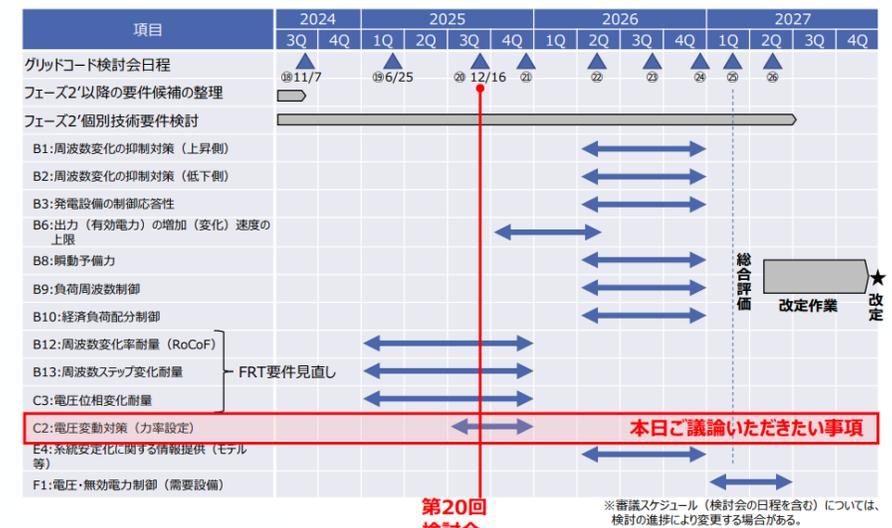
# グリッドコードの検討状況

- フェーズ2'として蓄電池の導入状況や最新の知見を踏まえ、2030年を待たずに要件化が必要と考えられるものについて検討している。
- 現時点では、**高低圧の蓄電池を対象にした電圧変動対策（充電側力率設定）を要件化**することが決定し、FRT※要件見直しに向けた検討等を進めている。
- 今後、早期に要件化が必要となる項目の精査を継続しつつ、**電力品質に必要な蓄電池・需要設備等に対する技術要件について検討を進める予定**。

## 要件化ロードマップ



## フェーズ2'の検討スケジュール



(出所) 第19回グリッドコード検討会（2025年6月25日）資料3

(出所) 第20回グリッドコード検討会（2025年12月16日）資料3

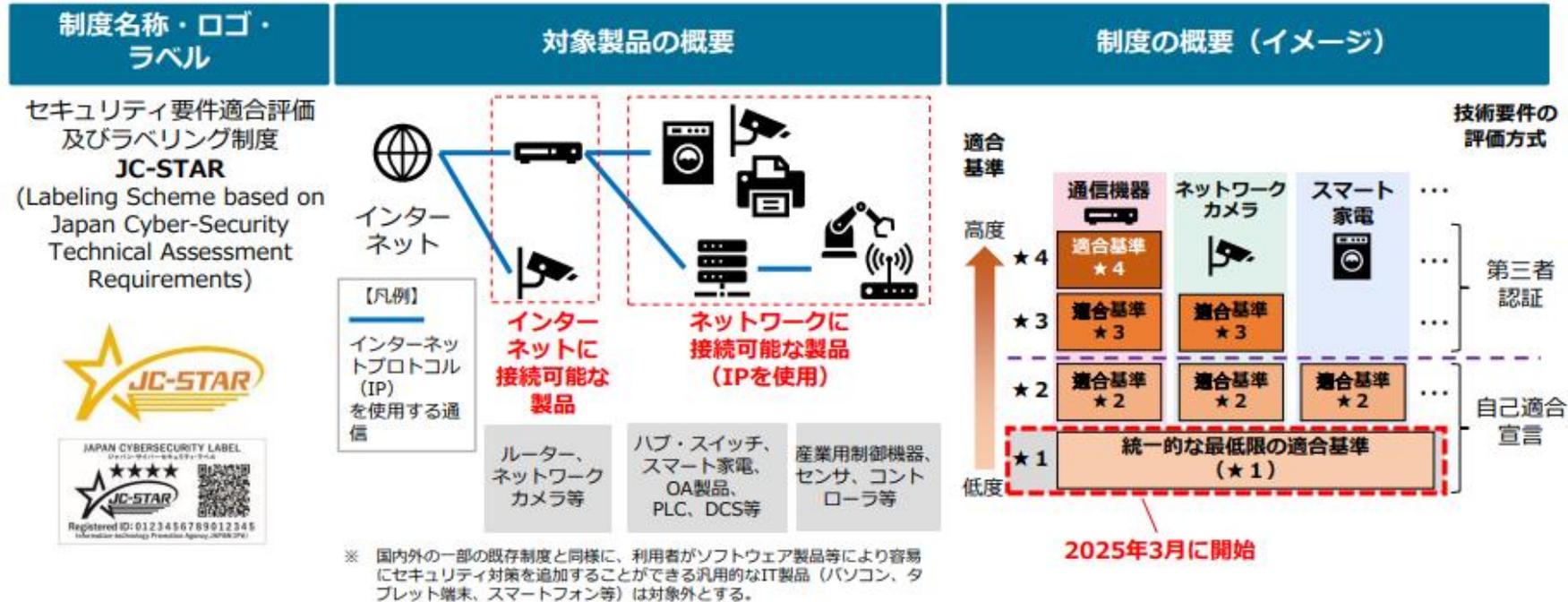
※Fault Ride Through：事故時運転継続

# 分散型電源のサイバーセキュリティ対策の要件化

- 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を取得した製品を用いることを要件化することとした。**
- 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こととした。**
- なお、太陽光および蓄電池のうち、**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、**経過措置期間を半年程度置くこととし、適用開始時期を2027年10月とすることとした。**
- 今後、風力や燃料電池等についてもJC-STAR★1を取得した製品使用の要件化の適用範囲・適用開始時期について官民で調整していく。
- さらに、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JC-STAR★2以上の適合基準の整備や導入に関しては、国の審議会等で議論を進める。

# (参考) JC-STAR制度の概要

- 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) 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。



(※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](https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/index.html)

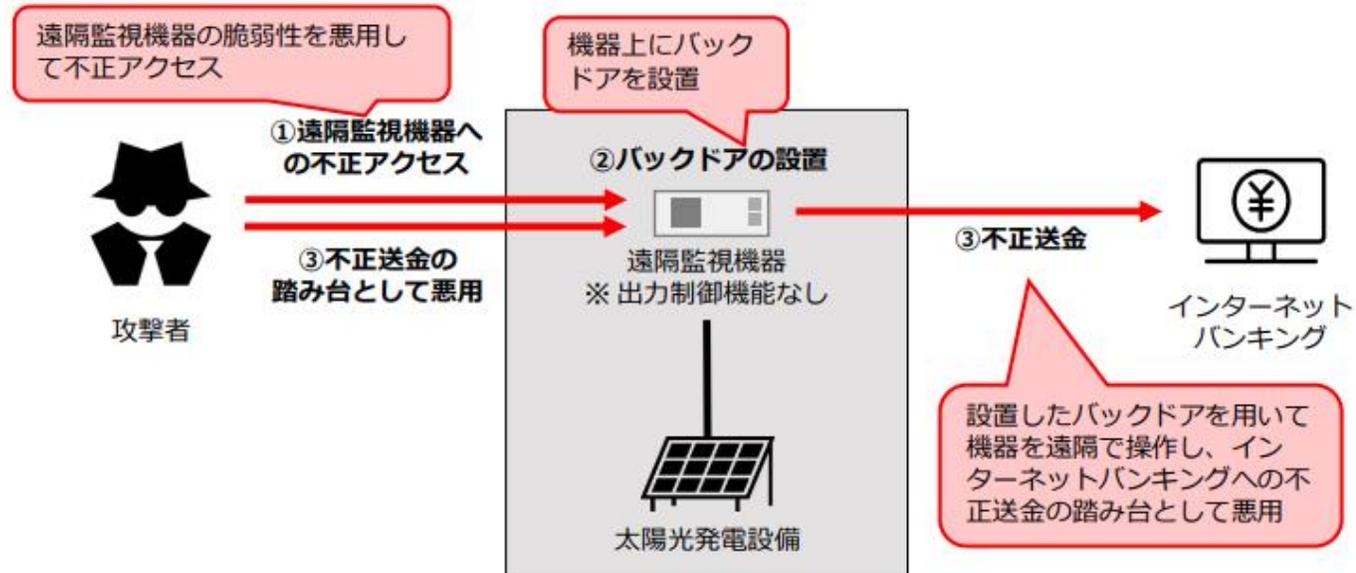
(※2)IPA「セキュリティ要件適合評価及びラベリング制度 (JC-STAR)」 <https://www.ipa.go.jp/security/jc-star/index.html>

## (参考) 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、システム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



# グリッドコードの変更内容に関する周知について

- 2027年10月において、低圧電源を対象とした系統連系技術要件の改定が予定されている。  
**系統連系技術要件の改定以降に連系の契約申込みを行う案件については、要件に適合しない発電等設備を系統に接続することは基本的に不可能**になる。
- 低圧電源においては流通在庫が存在することを考慮して経過措置期間を設定しているものの、発電等設備の設置から申込みまでに一定のリードタイムが存在するケースもあることから、最新の連系要件に適合した製品を早期に利用することが望まれる。
- また、円滑な系統接続を実現していく観点から、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）の改定等を通じて、**2027年10月におけるグリッドコードの変更について、関係団体などの協力を得ながら周知を図っていく**。