

資源エネルギー庁 再回答（再確認6項目へ） 2026-07-16

公開用の複製（株式会社I-S3 作成）。元はメール本文。行政側の担当者個人名・メールアドレス・電話番号は […]省略] に置き換えています。部署名・日付・本文はそのままです。出典: <https://www.i-s3.com/jc-star-answers/>

受信日時	2026-07-16 09:54 JST
差出人	資源エネルギー庁 電力・ガス事業部 電力基盤整備課（担当者名・アドレスは省略）
宛先	益田周防海（株式会社I-S3）
件名	RE: JC-STAR制度に関する技術的・制度設計上の確認およびご質問

本文（逐語。「>」で始まる行は引用部＝I-S3 からの照会文）

I-S3 益田さま

お世話になっております。

再度ご質問頂戴いたしました件につきまして、

以下回答申し上げますので、ご確認お願いいたします。

1. RS-485通信のみを使用するPCSの対象性

⇒通信の使用有無ではなく、IP通信機能の有無で判断しており、

IP通信機能を有さず、RS-485通信のみを使用するPCSにつきましては要件化の対象外でございます。

2. 「製品（システム）」の単位について

⇒通信機能を有する機器（PCS、BMS、EMS等の出力制御装置、遠隔監視装置）や、

ゲートウェイ等を介さずに主要な構成製品と接続している機器について要件化の対象としております。

3. 範囲決定時の脅威モデル又はリスク分析について

4. システムレベル対策との関係

⇒併せての御回答となりますが、電力の安定供給確保が重要であり、その観点においてサイバーセキュリティの確保が必要と考えております。

その上で、現状の系統連系技術要件においても、セキュリティ対策が求められているところ、

IoT製品全般に対する統一的な最低限の基準として存在するJC-STAR★1制度を活用し、実効性を高めることとしています。

具体的には、国内での電力設備におけるサイバー攻撃の事例は現時点においては限定的であるものの、

2024年5月に発生しております太陽光発電設備向け遠隔監視機器のサイバー攻撃を例としながら、

ウイルス感染・サイバー攻撃・不正侵入・なりすまし等を想定しつつ、電力の安定供給が脅かされるリスクの低減を前提として検討を進めております。

なお、過去の検討状況につきましては、第17回や18回の電力サブワーキンググループ資料を参照ください。

5. 対象範囲の技術的説明主体について

⇒「IP通信を用いる製品（システム）」の解釈につきましては、JC-STARの取得可否に関わるものかと認識いたしましたので、

そちらはIPAさまのセキュリティセンター 技術評価部 JC-STAR担当（[メールアドレス省略]）へご連絡頂ければと存じます。

その上で、他3点につきましては、ご認識のとおりいずれも資源エネルギー庁で問題ございません。

6. ご回答主体の確認について

⇒お問い合わせが多数到来しており、ご回答につきまして個人名などは差し控えさせていただいております。ご理解の程お願い申し上げます。

なお、資源エネルギー庁の中で本件の担当課室でございます電力・ガス事業部 電力基盤整備課としての回答でございます。

よろしくお願い申し上げます。

以上

-----Original Message-----

From: Suomi Masuda <s_masuda@i-s3.com>

Sent: Monday, July 13, 2026 10:57 PM

To: 電力サイバーセキュリティ <[メールアドレス省略]>

Cc: C. Lin <[メールアドレス省略]>; Mei Arai <[メールアドレス省略]>

Subject: Re: JC-STAR制度に関する技術的・制度設計上の確認およびご質問

本メールはHTMLメールをテキスト化しているため、レイアウトが乱れる、リンクが削除される場合があります。

このような場合は、送信者にテキストメールで再送していただくようご対応をお願いいたします。

経済産業省

資源エネルギー庁

ご担当者様

平素よりお世話になっております。

株式会社I-S3の益田です。

早速のご回答をいただき、ありがとうございます。

ご回答において、「グリッドコード要件化における対象範囲については弊庁にて定めております」とのご説明をいただきました。また、JC-STAR制度自体に関する質問についてはIPAへ問い合わせるべき旨、承知いたしました。

そこで、前回質問のうち、JC-STAR制度そのものではなく、貴庁が定めたグリッドコード要件化の対象範囲及びその技術的根拠に限定して、以下の点を再確認させてください。個別製品の可否や、申請手の個別判断は求めておりません。

1. RS-485通信のみを使用するPCSの対象性

貴庁の公開資料（2026年2月12日開催・電力サブワーキンググループ資料5「分散型電源のサイバーセキュリティ対策について」、

および第21回グリッドコード検討会資料における同趣旨の整理）では、「対象範囲のうち、IP通信を用いる製品（システム）がJC-STAR★1取得要件化の対象」と記載されています。

この記載に基づけば、自身ではIP通信を使用せず、RS-485通信のみを使用するPCSは、JC-STAR★1取得要件化の対象外であるとの理解でよろしいでしょうか。

「対象」又は「対象外」のいずれかでご回答いただけますと幸いです。

「対象」である場合には、上記資料における「IP通信を用いる製品（システム）」との関係をご教示ください。

2. 「製品（システム）」の単位について

上記資料では「製品（システム）」との表現が用いられています。例えば、

PCS — RS-485 — Logger / Gateway — IP通信 — 外部ネットワーク

という構成の場合、「IP通信を用いる製品（システム）」とは、次のいずれを指すのでしょうか。

- a. PCS単体
- b. Logger / Gateway単体
- c. PCS及びLogger / Gatewayを含む制御システム全体

これは貴庁が定めたグリッドコード要件化の対象範囲に関する確認としてお伺いしております。

3. 対象範囲決定時の脅威モデル又はリスク分析について

関連する貴庁・グリッドコード検討会の公開資料では、JC-STAR★1について、

太陽光発電・蓄電池等に想定される脅威に対して求められるサイバーセキュリティ対策を「全て包含しているわけではない」と整理されています。

また、電力固有の高リスク設備・電子機器、想定される脅威・攻撃手法、求められるセキュリティ要件、設置者・管理者に求める対策について、

議論を深めていく必要がある旨が示されています。

一方で、JC-STAR★1取得製品の使用を系統連系要件とすることは既に決定されています。

そこで確認ですが、グリッドコード要件化の対象範囲を決定する際に用いられた脅威モデル、攻撃シナリオ又はリスク分析資料は存在しますでしょうか。

存在する場合には、公開可能な資料名又は検討会資料をご教示ください。非公開資料である場合には、資料の存在の有無のみでもご回答いただけますと幸いです。

4. システムレベル対策との関係

貴庁の公開検討では、分散型エネルギーリソースのサイバーセキュリティについて、システム側と機器側の両面からの対応が必要である旨が整理されています。

また、国産であってもシステムとしてセキュリティを高めていくことが重要である旨の指摘も、公開議論に見られます。

弊社が前回質問したBoundary Protection、Trust Boundary及びZone &

Conduitとの関係は、まさにこの「システムとしてセキュリティを高める」際の設計境界に関するものです。

貴庁がグリッドコード要件化の対象範囲を決定する際、ネットワーク境界における防御、通信経路の制限又はシステム分離によるリスク低減効果を評価されたのでしょうか。

評価された場合、その検討資料（公開可能な範囲）をご教示ください。評価していない場合には、その旨のみでも結構です。

5. 対象範囲の技術的説明主体について

今後の問い合わせ先を正確に理解するため確認いたします。

貴庁のご回答では、「グリッドコード要件化における対象範囲については弊庁にて定めております」とのことでした。

したがって、次の事項については、資源エネルギー庁が説明主体であるとの理解でよろしいでしょうか。

- ・要件化対象となる機器・システムの範囲
- ・「IP通信を用いる製品（システム）」の解釈
- ・対象範囲を当該境界とした技術的理由
- ・対象範囲決定時に想定した脅威及びリスク低減効果

もしこれらについてIPAが回答主体となる場合には、どの質問をどの機関へ照会すべきか、質問項目ごとにご教示いただけますと幸いです。

弊社としても、所管外の事項を繰り返し照会することは本意ではなく、各機関の役割分担を正確に理解した上で質問を行いたいと考えております。

6. ご回答主体の確認について

今回いただいたご回答は、「電力サイバーセキュリティ」の共有メールアドレスから送信されておりますが、ご担当者名、所属課室名及び役職等の記載が確認できませんでした。

本件については、弊社において制度検証の対象として継続的に調査しており、今回のご回答についても、今後、回答内容を正確に引用・公開し、技術的及び制度的観点から検証する予定です。

そのため、今回のご回答が、次のいずれに該当するのか、ご教示ください。

- ・資源エネルギー庁としての公式な回答
- ・特定の課室としての回答
- ・担当者個人による一次的な案内

また、差し支えなければ、ご回答を担当された部署名、課室名及びご担当者名をご教示いただけますでしょうか。

個人名の開示が困難である場合には、少なくとも本回答の内容について行政組織上の責任主体となる課室名及び役職レベルをご教示ください。

特に今回のご回答には、「グリッドコード要件化における対象範囲については弊庁にて定めております」とのご説明が含まれております。

弊社としては、この記載を資源エネルギー庁の公式な制度説明として引用して差し支えないのか、それとも担当窓口による非公式な案内として理解すべきなのかを正確に確認する必要があります。

本回答の行政組織上の帰属主体及び公式性について、明確にご回答いただけますと幸いです。

参照（公開資料）：

- ・電力SWG第19回（2026-02-12）開催ページ

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/019.html

- ・第21回グリッドコード検討会資料

https://www.occto.or.jp/assets/iinkai/gridcode/21/gridcode_21_04.pdf

- ・第19回グリッドコード検討会資料

https://www.occto.or.jp/assets/iinkai/gridcode/2025/files/gridcode_19_06.pdf

- ・当社の公開質問記録

<https://www.i-s3.com/jc-star-meti-inquiry-2026.html>

何卒よろしくお願い申し上げます。

益田 周防海 (Suomi Masuda Ph. D)

株式会社I-S3 (I-S3.CO <<http://i-s3.co/>>., Ltd)

本社: 群馬県安中市嶺638番地3 (HQ: 638-3 Mine, Annaka, Gunma, Japan)

高崎Office: 群馬県高崎市飯塚町1311-1

(Takasaki Office: 1311-1 Iizuka-Machi, Takasaki, Gunma, Japan)

Tel: [電話番号省略]

Fax: [電話番号省略]

E-mail: s_masuda@i-s3.com<mailto:s_masuda@i-s3.com>

<https://www.i-s3.com>

レビューコメント等はこちらへ / Share your experience with us! Leave a review.

<https://g.page/r/CSWXjunl3FptEAl/review>

On Mon, Jul 13, 2026 at 10:15 PM 電力サイバーセキュリティ <[メールアドレス省略]> wrote:

> I-S3 益田さま

>

> お世話になっております。

>

> グリッドコード要件化における対象範囲については弊庁にて定めておりますが、

> JC-STARの制度自体に関するご質問が太宗を占めるかと存じますので、その場合につきましては、

> 恐れ入りますが、IPAさまへお問い合わせ頂ければ幸いです。

>

> よろしく願いいたします。

>

> 以上

>

> -----Original Message-----

> From: Suomi Masuda <s_masuda@i-s3.com<mailto:s_masuda@i-s3.com>>

> Sent: Friday, July 10, 2026 10:45 AM

> To: 電力サイバーセキュリティ < [メールアドレス省略] >

> Cc: C. Lin < [メールアドレス省略] >; Mei Arai < [メールアドレス省略] >

> Subject: JC-STAR制度に関する技術的・制度設計上の確認およびご質問

>

> *****

> 本メールはHTMLメールをテキスト化しているため、レイアウトが乱れる、リンクが削除される場合などがあります。

> このような場合は、送信者にテキストメールで再送していただくようご対応をお願いいたします。

> *****

>

> 経済産業省

> ご担当者様

>

> 平素より大変お世話になっております。

>

> 弊社では、産業用制御システムおよび再生可能エネルギー設備におけるサイバーセキュリティについて、

> IEC62443等の国際標準を踏まえた技術調査・分析を行っております。

>

> 現在、JC-STAR制度について公開資料をもとに制度分析を進めておりますが、技術的および制度設計上、公開情報のみでは理解できない点がございました。

>

>

> 本制度は、日本のサイバーセキュリティ水準向上を目的とした重要な制度であると認識しております。本問い合わせは制度そのものを否定するものではなく、制度の技術的合理性や設計思想を正しく理解し、より信頼性・透明性の高い制度となることを期待する立場からお伺いするものです。

>

> つきましては、以下の点につきましてご教示いただけますと幸いです。

> -----

> 1. RS-485通信のみを有するPCSについて

>

> 太陽光発電用パワーコンディショナの中には、自身ではIP通信機能を持たず、RS-485通信のみを有する構成の製品があります。

>

> このような構成では、インターネットとの通信境界はSmartLoggerやGateway等の外部機器に存在すると理解しております。

>

> この場合においてもPCS単体をJC-STAR認証対象とする技術的理由をご教示ください。

> -----

> 2. IEC 62443との整合性について

>

> IEC 62443では、Zone & ConduitおよびBoundary

> Protectionによってシステム全体のサイバーセキュリティを確保する考え方が採用されています。

>

> JC-STARでは、Boundary Protectionのみでは十分ではないとの考え方を採用しているのでしょうか。

>

> もしそうであれば、その技術的根拠をご教示ください。

> -----

> 3. 想定される脅威モデルについて

>

> RS-485通信のみを有し、自身ではIP通信を行わないPCSについて、JC-STARではどのようなサイバー攻撃シナリオを想定されているのでしょうか。

>

> また、そのリスクはBoundary Protectionによって十分に低減できないと考えられている理由についてもご教示いただけますでしょうか。

> -----

> 4. PCによる制御との関係について

>

> RS-485は一般的なシリアル通信規格であり、USB-RS485インターフェースを備えた汎用PCから通信を行うことは技術的に可能です。

>

> また、PC上にロガー相当の機能を実装することも技術的には可能です。

>

> このような構成において、PCS単体へJC-STAR認証を要求することで、どのようなセキュリティ向上効果を期待されているのでしょうか。

> -----

> 5. 制度が対象としているセキュリティ範囲について

>

> JC-STARは、

>

> - PCS単体のサイバーセキュリティ

>

> を評価する制度でしょうか。

>

> あるいは、

>

> - システム全体のサイバーセキュリティ

>

> を評価する制度でしょうか。

>

> Boundary Protectionによって十分保護可能なシステム構成についてもPCS認証を要求する制度設計とした技術的理由をご教示ください。

> -----

> 6. 外国法的環境等の評価について

>

> 公開資料では、「外国法的環境等」も評価対象となることが示されています。

>

> この評価項目は、

>

> - 純粋な技術的リスク評価

> - 経済安全保障上のリスク評価

>

> のいずれとして位置付けられているのでしょうか。

>

> また、これらはどのような考え方で技術認証制度の中へ位置付けられているのか、ご教示いただけますと幸いです。

> -----

> 7. 制度の透明性および説明責任について

>

> JC-STARIは制度上は任意認証制度と理解しております。

>

>

> しかしながら、現在では系統連系要件として採用されることにより、日本市場へ製品を投入するための実質的な前提条件となっており、市場参入に極めて大きな影響を及ぼす制度となっています。

>

> そのような制度であるにもかかわらず、

>

> - 不認証理由を原則として開示しないこと

> - 審査過程および判断理由が公開されないこと

> - 「政府が把握している情報」を総合的に判断するとされる一方、その内容について申請者が確認・反論する仕組みが制度上明確ではないこと

>

> について、制度の透明性および説明責任の観点からどのように整理されているのでしょうか。

>

> また、実質的に市場参入へ大きな影響を与える制度について、このような審査方法で十分な予見可能性および説明可能性が確保できるとお考えでしょうか。

> -----

> 8. 制度の長期的な運営について

>

> JC-STARは今後、国際的な相互認証や海外企業による利用も視野に入れた制度であると理解しております。

>

> 一方で、本制度はサイバーセキュリティに関する*技術認証制度*として設計されています。

>

>

> 一般に、技術認証制度は一度技術基準として制度化されると、将来の国際情勢や外交・安全保障環境が変化した場合においても、その運用変更については技術的合理性をもって説明できることが重要であると考えます。

>

> 仮に将来、国際情勢や外交関係が変化した場合においても、

>

> - 技術認証制度としての整合性

> - 技術的合理性

> - 説明可能性

>

> を維持したまま制度運営を継続できるよう設計されているのでしょうか。

>

> また、そのような長期的な制度運営も考慮した制度設計となっているのでしょうか。

> -----

> 参考資料

>

> 弊社では、JC-STAR制度について技術的・制度的観点から整理した記事を公開しております。

>

> 参考までにご覧いただけますと幸いです。

>

> 【参考URL】

>

> JC-STAR制度に関する弊社公開記事（参考資料）】

> 1. JC-STAR徹底調査レポート — 公開情報で検証する制度の透明性・公平性・実効性

> <https://www.i-s3.com/jc-star-research-report.html>

> 2. Trust Boundaryを無視したJC-STARは本当にサイバーセキュリティなのか — 国際標準との決定的矛盾を問う

> <https://www.i-s3.com/jc-star-iec62443-contradiction.html>

> 3. 認証対象ではなく「認証境界」を議論しませんか？ — 太陽光発電システムと信頼境界

> <https://www.i-s3.com/jc-star-trust-boundary-solar-pv.html>

> 4. JC-STARは技術認証か、経済安全保障政策か — 「後で説明に困る制度」を作っていないか

> <https://www.i-s3.com/jc-star-certification-or-security-policy.html>

> 5. JC-STAR要件化時代に問う「Dynamic Resilience by Architecture」

>

> <https://www.i-s3.com/energy-iot-cybersecurity-jc-star-resilience.html>

> 6. 認証済みなら本当に安全なのか？太陽光発電システムとサイバーセキュリティの根本問題

>

> <https://www.i-s3.com/certified-secure-resilient-by-architecture.html>

> 7. JC-STARを議論する — 認証境界・動的レジリエンス・公開質問（議論ハブ）

> <https://www.i-s3.com/jc-star-debate.html>

> -----

> おわりに

>

> 本制度は、日本のサイバーセキュリティ水準向上に資する重要な制度であると理解しております。

>

> 一方で、その重要性が高まるほど、制度の*技術的合理性、透明性、説明可能性および長期的な持続可能性*も一層重要になるものと考えております。

>

>

> また、現在では実質的に市場参入へ大きな影響を及ぼす制度となっていることから、制度への信頼は、技術的な正当性だけでなく、申請者や市場参加者が納得できる説明可能性によって支えられるものと考えております。

>

>

> 本問い合わせは制度への批判を目的としたものではなく、日本発のサイバーセキュリティ認証制度が、国際的にも信頼され、長期にわたり持続可能な制度として発展することを期待し、その技術的・制度的背景について理解を深めるためにお伺いするものです。

>

> ご多忙のところ誠に恐縮ではございますが、ご回答いただけますと幸いです。

>

> 何卒よろしくお願い申し上げます。

>

> 益田 周防海 (Suomi Masuda Ph. D)

> 株式会社I-S3 (I-S3.CO <<http://i-s3.co/>>, Ltd)

> 本社: 群馬県安中市嶺638番地3 (HQ: 638-3 Mine, Annaka, Gunma, Japan)

> 高崎Office：群馬県高崎市飯塚町1311-1

> (Takasaki Office: 1311-1 Iizuka-Machi, Takasaki, Gunma, Japan)

> Tel: [電話番号省略]

> Fax: [電話番号省略]

> E-mail: s_masuda@i-s3.com<mailto:s_masuda@i-s3.com>

>

> <https://www.i-s3.com>

>

> レビューコメント等はこちらへ / Share your experience with us! Leave a review.

> <https://g.page/r/CSWXjunl3FptEAl/review>

>