

資源エネルギー庁 初回回答（公開質問 8 項目へ） 2026-07-13

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	2026-07-13 22:15 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。

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。

よろしくお願いいたします。

以上

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

From: Suomi Masuda <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-STAR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

<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/CSWXjunl3FptEAI/review>