資源エネルギー庁 御中

令和3年度エネルギー需給構造高度化対策に関する調査等事業（電力分野のサイバーセキュリティ対策のあり方に関する詳細調査分析）

報告書

三菱総合研究所

デジタル・イノベーション本部

2022年2月28日

目次

図 目次

表 目次

1. はじめに

1.1 調査背景・目的

あらゆる分野でデジタル化が進展する一方、多様化・巧妙化するサイバー攻撃の脅威は日々高まっており、重要インフラたる電力分野においても、サイバーセキュリティ向上に向けた不断の取組が求められている。電力分野においては、平成28年の小売全面自由化等により新規参入者が拡大するとともに、再生可能エネルギーの系統への接続やそれに伴う出力制御の実施のため、発電・送配電事業を中心として、ネットワークへの接続やデジタル技術の活用が広がりつつある。一方で、サイバー攻撃を受ける可能性や攻撃箇所の増加、また、サイバー攻撃の影響が広範囲に及ぶ可能性も高くなっている。また、分散電源が大量に導入された電力系統全体としての安定性確保のためには、機器の故障や需給バランスに留意するだけでなく、サイバー攻撃を起点とする系統不安定化を防止するためにもサイバーセキュリティ確保の重要性はこれまでになく高まっている。

こうした中、平成29年12月に産業横断的な更なるサイバーセキュリティ対策を検討する産業サイバーセキュリティ研究会が設置され、その下のワーキンググループにおいて、制度・技術・標準化の検討が進められている。また、上述のような状況変化を踏まえ、平成30年6月に電力分野のサイバーセキュリティに関する今後の取組について検討を行うことを目的とし、電力サブワーキンググループを設置し、電力を取り巻くサイバーセキュリティに関する現状、事業者の取り組み、官民が取り組むべき課題と方向性を議論・検討しているところである。

再生可能エネルギー主力電源化に向け、サイバーセキュリティ対策が重要な課題となっており、本事業では、大手電力会社や新規プレーヤーにおけるサイバーセキュリティ対策等のサイバーセキュリティ上の課題に対する具体的な制度等の設計に向けて、日本国内の状況、また、海外における取組状況の実態調査等必要な調査・分析を行い、ワーキンググループ等において議論・検討を行った。

また、国際的には、米国 EIS Council による Cyber Product International Certification（CPIC）イニシアチブ等において、電力分野においてセキュリティリスクのポイントとなりうる重要な機器・システム（SCADA、PLC、保護リレー、タービン速度制御装置 等）の客観的なセキュリティ検証・評価についての議論が進められている。これらのセキュリティ検証・評価の仕組みについて、電力サブワーキンググループにおける議論や我が国の電力会社、制御システムベンダーの置かれた状況等も踏まえつつ、望ましい検証のあり方について調査・分析を行った。

また、当該検証のあり方や電力分野におけるセキュリティ規制・基準のあり方について、欧米やインド太平洋諸国とも国際的な議論をWS形式で行うことで、我が国の電力分野におけるセキュリティ政策の国際調和を促進した。

これにより、石油や石炭、ガスの円滑な生産・流通に必要不可欠な電力の安定供給、ひいては我が国のエネルギー安全保障の向上に資することが期待される。

1.2 調査実施概要

調査目的を達成するために、以下の項目に関して調査・検討・支援等を行った。

1. 電力分野のサイバーセキュリティ対策のあり方調査検討
   (1) 国内外の電力サイバーセキュリティに関する実態調査・分析
   (2) 新規プレーヤーに関するサイバーセキュリティ対策の検討
   (3) 電力システムのサイバーセキュリティリスクの分析
   (4) ワーキンググループの運営
2. 再生可能エネルギー主力電源化に向けた電力分野のサイバーセキュリティに関する海外連携のあり方等調査検討
   (1) 電力分野における機器・システムの調達時のセキュリティ検証・評価方法の調査・検討
   (2) インド太平洋地域向け日米 EU 産業制御システムサイバーセキュリティウィークの開催

2. 電力分野のサイバーセキュリティ対策のあり方調査検討

文献、インターネット、ヒアリング等により調査を行い、国内外の電力サイバーセキュリティ対策やサプライチェーンリスクへの対策の最新動向等や参考となる他分野の対策状況について整理・分析を行った。

2.1 国内外の電力サイバーセキュリティに関する実態調査・分析

2.1.1 サプライチェーンリスクへの対策に関する動向

サプライチェーンリスクへの対策に関する動向について、特に米国の動向を調査した。具体的には下記 3 つの観点に基づき調査を行った。

（1）基幹電力系統保護に関する米国の動向

（2）エネルギー分野のサプライチェーン強化に関する米国の動向

（1） 基幹電力系統保護に関する米国の動向

2020 年 5 月 1 日にトランプ前大統領が基幹電力系統の保護を目的として大統領令[1]に署名した。本大統領令は、基幹電力系統で使用される電気設備の安全性及び完全性を保護し、外国敵対者による米国電力インフラを標的とする攻撃（サイバー攻撃含む）の影響を低減させることを目的とした。エネルギー省（DoE）長官に対して、外国敵対者に該当する国の決定や対象となる設備の特定について権限が与えられるほか、特定の設備やベンダーに対する事前認定付与の権限を与えられていた。2020 年 12 月には、本大統領令に基づき中国に関連する事業体により提供された機器の調達を禁止する禁止命令[2]が発出されたが、2021 年 1 月 20 日、バイデン大統領は、本大統領令の効力を 90 日間停止する大統領令[3]に署名した。この大統領令を受け、禁止命令も同じく停止となり、最終的に禁止命令は 2021 年 4 月 20 日に失効した。

禁止命令の失効のタイミングに合わせて、DoE は基幹電力系統のサプライチェーンにおける外国の脅威に対する対応に関して意見を求めたパブリックコメント[4]を開始した。パブリックコメントは 2021 年 6 月 7 日まで実施され、パブリックコメントの結果は、国家安全保障、経済、管理可能性のバランスを考慮した後継の大統領令を推奨するかどうかの検討に用いるとしている。このパブリックコメントでは国家

[1] “Executive Order on Securing the United States Bulk-Power System” https://www.federalregister.gov/documents/2020/07/08/2020-14668/securing-the-united-states-bulk-power-system

[2] “Prohibition Order Securing Critical Defense Facilities” https://www.federalregister.gov/documents/2021/01/06/2020-28773/prohibition-order-securing-critical-defense-facilities

[3] “Executive Order on Protecting Public Health and the Environment and Restoring Science to Tackle the Climate Crisis” https://www.whitehouse.gov/briefing-room/presidential-actions/2021/01/20/executive-order-protecting-public-health-and-environment-and-restoring-science-to-tackle-climate-crisis/

[4] “Request for Information (RFI) on Ensuring the Continued Security of the United States Critical Electric Infrastructure” https://www.federalregister.gov/documents/2021/04/22/2021-08482/notice-of-request-for-information-rfi-on-ensuring-the-continued-security-of-the-united-states

安全保障と経済性、管理可能性のバランスを意識したリスク対応策の検討を目的としており、長期的な視点を意識したより戦略的な質問事項が設定された（下記参照）。結果として、電力会社、業界団体、機器ベンダー等から計 182 件のパブリックコメント回答が寄せられた。なお、パブリックコメントを求めた官報公示において、中国は米国の電力系統を弱体化させる積極的な計画を行っているとし、電力系統に不可欠な機器が中国から調達されることは大きな脅威であるとした。

【長期戦略の展開に関するパブリックコメント質問事項】

- それぞれの州や地方政府は、電力システムに関連するセキュリティの取り組みを強化するために、どのような技術的支援が必要か。
- 重要な電力インフラのセキュリティや、外国人の所有権、支配権、影響力を評価する基準をサプライチェーンのリスク管理に組み込むために、規制当局は具体的にどのような追加行動を取ることができるか、また、DoE はこれらの行動にどのようにして最善の情報を提供できるか。
- 民間企業による責任ある効果的な調達方法を促進するために、DoE はどのような行動をとることができるか。それらの行動の潜在的なコストと利益は何か。
- 外国人の所有権、支配権、影響力のリスクを軽減することを目的として、電力会社の調達方針、州の要件、FERC の信頼性基準（CIP 基準）を知らせるために、DoE が発行できる特定の基準はあるか。

【禁止の権限に関するパブリックコメント質問事項】

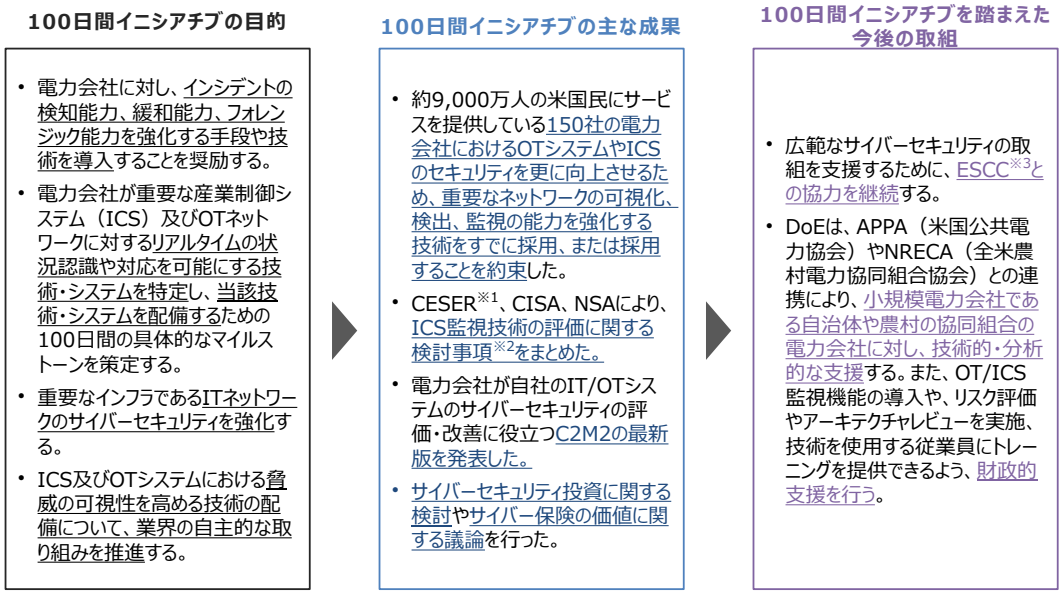
- 国家安全保障を確保するために、DoE 長官は配電システムの一部、すなわち配電機器・設備に設置された機器に適用される禁止命令などの発動を求めるべきか。
- DCEI[5]に加えて、通信、緊急サービス、医療・公衆衛生、情報技術、輸送システムなど、他の重要なインフラ分野に電力を供給する電気インフラを対象とした禁止命令の発動を求めるべきか。
- 重要インフラに加えて、国の重要な機能を実現する電力インフラを対象とした禁止命令等の発動を長官は求めるべきか。
- 電力会社は、このような要件の遵守を可能にするような、サービスエリア内の重要なインフラを十分に特定することができるか。

2021 年 4 月 20 日、DoE は、電力業界や CISA と協力して、電力会社のサイバーセキュリティを強化や、サプライチェーンセキュリティ確保を目的とした 100 日間のイニシアチブ[6]を開始した。このイニシアチブの概要を図 2-1 に示す。このイニシアチブでは、特に電力会社におけるインシデントの検知能力、緩和能力、フォレンジック能力を強化する手段や技術の導入を奨励することを目的に、官民連携での取組が進められた。このイニシアチブを通じて、米国の 150 の電力会社におけるセキュリティ強化に寄与したほか、ICS 監視技術の評価に関する検討事項の策定や C2M2（Cybersecurity Capability

[5] Defense Critical Electric Infrastructure の略で、連邦電力法第 215A 条(a)で定義される国防重要電力インフラを指し、同じく連邦電力法第 215A 条(c)で定義される重要防護施設（Critical Defense Facility: CDF）に電力を供給する。CDF は DoE 長官により指定される。

[6] “100-Day Plan to Address Cybersecurity Risks to the U.S. Electric System” https://www.energy.gov/articles/biden-administration-takes-bold-action-protect-electricity-operations-increasing-cyber-0

Maturity Model）の改定が実施された。

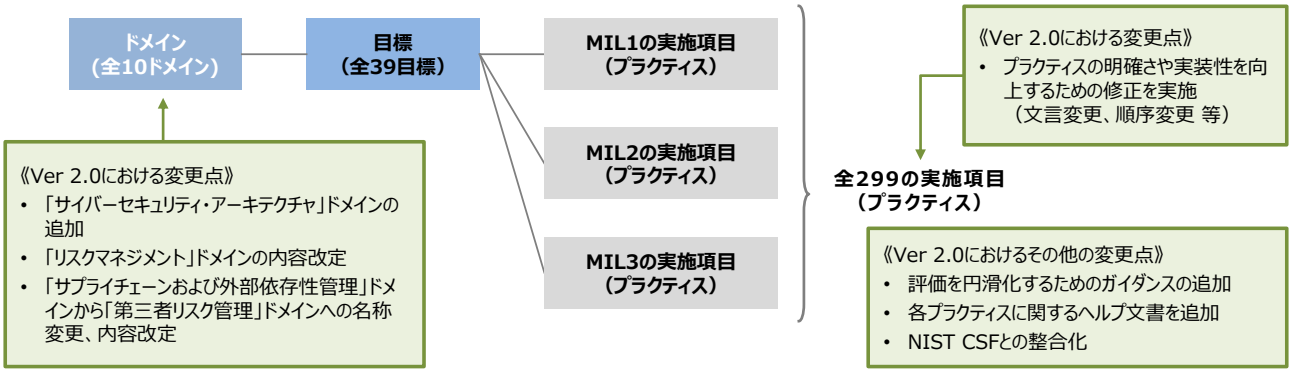


※1：Cybersecurity, Energy Security, and Emergency Responseの略で、DoE長官直属の組織。主にエネルギー分野のセキュリティを所管する。
※2：https://www.energy.gov/ceser/considerations-icsot-cybersecurity-monitoring-technologies
※3：Electricity Subsector Coordinating Councilの略で、電力会社のCEOや業界団体の代表により構成される組織。E-ISACと協力し、電力系統保護に向けた行動や戦略の策定を支援する。ホワイトハウスや政府機関とも緊密に連携している。CISAとともに、100日間イニシアチブの遂行に向けたDoEを支援した。

出所）電力分野 100 日間イニシアチブに関する公開情報に基づき三菱総合研究所作成

図 2-1 米国における電力分野 100 日間イニシアチブの概要

C2M2 は、組織におけるサイバーセキュリティの取組の評価・改善に活用できるサイバーセキュリティ能力成熟度モデルであり、10 のドメイン、39 の目標、299 の実施項目によって構成される[7]。C2M2 の概要と、100 日間イニシアチブを通じて改定された Ver 2.0 の主な変更点を図 2-2 に示す。今回の改定では、Ver. 1.1 以降に洗練化された技術や脅威に対抗することを目的とし、Ver. 2.0 では、新たなドメインが追加やいくつかのドメインの内容が改定されたほか、NIST Cybersecurity Framework（CSF）との整合性を高めるための修正が加えられた。



出所）C2M2 に関する公開情報に基づき三菱総合研究所作成

図 2-2 C2M2 (Cybersecurity Capability Maturity Model) Ver. 2.0 の概要

[7] https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

重要インフラ全体のセキュリティ向上に向けた取組として、2021 年 7 月 28 日、バイデン大統領は重要インフラ制御システムのサイバーセキュリティ向上に関する国家安全保障覚書[8]を発表した。覚書においては、重要インフラ制御システムのサイバーセキュリティ目標の策定が明文化されている。米国重要インフラのサイバーセキュリティに関する現状の課題として、以下の 3 点が覚書に明記されている。

- コロニアル・パイプラインに対するサイバー攻撃など、主に民間企業が運用している重要インフラに対するサイバー攻撃が増加している
- 米国のサイバーセキュリティ規制は重要インフラセクター毎に整備されているため、各セクターにおいて断片的な対策のみ行われている
- 重要インフラ全体での戦略的で包括的な要件が存在しない

この課題を踏まえ、覚書では、連邦政府と重要インフラコミュニティ間のイニシアチブの設立が規定された。このイニシアチブは、「産業用制御システムサイバーセキュリティイニシアチブ」と名付けられ、2021 年 4 月から電力分野で実施されていた 100 日間イニシアチブを参考としている。併せて、重要インフラ企業がセキュリティ強化に活用しうる重要インフラ制御システムのサイバーセキュリティ目標を策定することが明文化された。2021 年9月 21 日に暫定的なベースライン目標が公表[9]されており、今後 2022 年 7 月 28 日までに重要インフラセクター別の目標が策定され、公表される予定である。

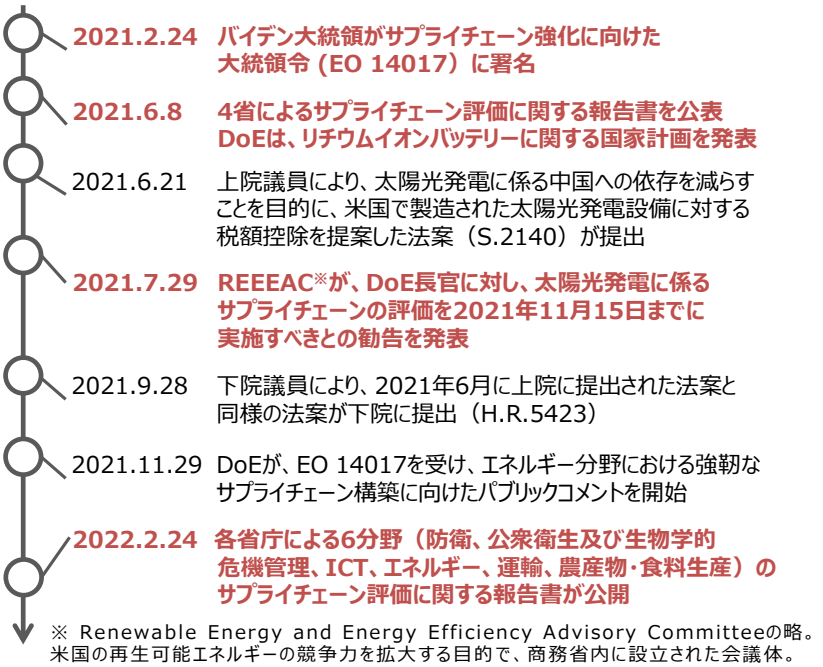
今後想定される動向として、基幹電力系統保護を目的とした大統領令を 90 日間停止した大統領令（EO 13990）では、DoE 長官及び OMB 長官に対して、「代替の大統領令を発行するかの検討」を指示しているところ、2020 年 5 月の大統領令に代わる新たな大統領令が発出される可能性がある。一方で、DoE は、期間が限定された大統領令だけでなく、広範かつ継続的なリスクに対処するための長期戦略の必要性を認識しており、この問題意識に対して、2021 年 4 月に開始されたパブリックコメントでは、電力会社におけるサプライチェーン管理のために DoE 及び関連政府機関に求められる支援や行動に関する意見を求めている。今後パブリックコメントでの意見を踏まえて、より具体的な支援策や基準が公表されると想定される。

また、パブリックコメントでは、国家安全保障に関する施設に電力を供給する設備の調達禁止命令について、その必要性や実現可能性に関する意見を求めているほか、パブリックコメントを求めた官報公示では、電力系統に不可欠な機器が中国から調達されることは大きな脅威であると明記している。今後発出される可能性がある大統領令、長期戦略、禁止命令等の動向については、継続して注視していくことが望まれる。

（2）エネルギー分野のサプライチェーン強化に関する米国の動向

エネルギー分野のサプライチェーン強化に関する主な米国政策のタイムラインを図 2-3 に示す。

[8] “National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems” https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/
[9] CISA, Critical Infrastructure Control Systems Cybersecurity Performance Goals and Objectives https://www.cisa.gov/control-systems-goals-and-objectives



出所）各種公開情報に基づき三菱総合研究所作成

図 2-3 エネルギー分野のサプライチェーン強化に関する主な米国政策のタイムライン

2021 年 2 月、バイデン大統領がサプライチェーン強化に向けた大統領令[10]に署名した。この大統領令では、商務省（DoC）、DoE、国防総省（DoD）、保健福祉省（HHS）の各省長官に対して、半導体、バッテリー、重要鉱物、医薬品及び医薬品有効成分のサプライチェーンにおけるリスクを各省庁にて特定し、リスクへの対処方法を提言する報告書を 100 日以内に提出するよう指示した。また、防衛、公衆衛生及び生物学的危機管理、ICT、エネルギー、運輸、農産物・食料生産の各産業を所管する省庁に対して、大統領令から 1 年以内に各分野のサプライチェーンを評価する報告書を提出するよう指示した。

この大統領令を受け、2021 年 6 月 8 日、大統領令の指示を受けた 4 省によるサプライチェーン評価に関する報告書[11]が公表された。エネルギー分野に関連する DoE は、リチウムイオンバッテリーに関するサプライチェーン強靭化計画を発表した。具体的な計画内容として、DoE ローンプログラム室（LOP）により、車両向けバッテリーセル／パックの製造施設の建設や拡張プロジェクトに対して、DoE 先進車両製造ローンプログラム（ATVM）から約 170 億ドル規模のローン保証を付与することを含めた。また、DoE 連邦エネルギー管理プログラム（FEMP）により、連邦機関によるエネルギー貯蔵の普及に対する 2 億 6,000 億ドル以上の投資を通じて、国有地におけるエネルギー貯蔵プロジェクトの実施を促すことを含めた。

また、2021 年 11 月 29 日、DoE は上記大統領令の指示を踏まえ、エネルギー分野における強靭な

[10] “Executive Order on America’s Supply Chains” https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/

[11] “Building Resilient Supply Chains, Revitalizing American Manufacturing, and Fostering Broad-based Growth” https://www.whitehouse.gov/wp-content/uploads/2021/06/100-day-supply-chain-review-report.pdf

サプライチェーン構築に向けたパブリックコメント[12]を開始した。このパブリックコメントでは、エネルギーシステムに関する原材料、コンポーネント等を対象に、強靭なサプライチェーン構築に必要なアプローチやアクションに関する意見を求めた。具体的には、太陽光発電、風力発電、原子力発電等の特定の技術分野に焦点を当てた質問事項や半導体、ネオジム磁石等の特定の原材料に焦点を当てた質問事項のほか、横断的に検討が必要な事項として、サイバーセキュリティに関する質問事項も設定されている。サイバーセキュリティに関する主な質問事項は以下のとおりであり、特に、エネルギー分野のサプライチェーン強化に向けて政府が考慮すべき事項や、信頼できないサプライヤーへの依存度を低減するために政府に求められる措置等について意見を求めている。

【エネルギー分野のサプライチェーンにおけるサイバーセキュリティとデジタルコンポーネントに関する質問事項(抜粋)】

- 連邦政府は、物理的・仮想的な改ざんや国家安全保障上の脅威に対して、エネルギー分野の産業基盤のデジタルコンポーネントのサプライチェーンをどのように強靭化させるべきか。連邦政府は、デジタルコンポーネントのサプライチェーンの保護をどのように優先すべきか。
- ランサムウェア等のサイバー脅威に対するデジタルコンポーネントのサプライチェーン強化を支援するために、連邦政府が考慮すべきエネルギー分野特有の検討事項や優先事項はあるか。
- デジタルコンポーネントの信頼性を向上させ、信頼できないソフトウェアサプライヤー、インテグレーター、保守事業者等への依存度を低減するために、連邦政府はどのような措置を講じるべきか。
- エネルギー分野のシステムにおけるデジタルコンポーネントの出所を明らかにするために、連邦政府はどのような政策をとるべきか。サプライチェーンのリスクを管理するために政府はどのように優先順位をつけるべきか。
- 政府は、デジタルコンポーネントのサプライチェーンセキュリティ要件のギャップにどのように対処し、一貫性を確保すべきか。
- エネルギー分野の重要機能を操作するために使用されるプラットフォームやサービスのサプライチェーンセキュリティを確保するために、政府はどのような政策的措置をとるべきか。

等

2022 年 2 月 24 日、上記パブリックコメントを踏まえ、DoE よりエネルギー産業基盤の構築に向けた包括的戦略文書[13]が発表された。DoE は、エネルギー部門に直接的・間接的に関与するすべての産業、企業及び関係者、そしてそれらに関連するサプライチェーン全体を「エネルギー部門産業基盤(ESIB:Energy Sector Industrial Base)」と定義し、これには、採掘産業、製造産業、エネルギー変換・供給産業、使用済み製品や廃棄物管理産業、デジタル製品やデジタルサービスプロバイダーまで、産業とステークホルダーの複雑なネットワークが含まれる。戦略文書では、ESIB に関連するデジタルコンポーネントは脆弱であり、様々な脅威、脆弱性、影響に起因するリスクにおいてサプライチェーン攻撃

[12] "Request for Information (RFI) on Energy Sector Supply Chain Review" https://www.federalregister.gov/documents/2021/11/29/2021-25898/notice-of-request-for-information-rfi-on-energy-sector-supply-chain-review
[13] "Securing America's Clean Energy Supply Chain" https://www.energy.gov/policy/securing-americas-clean-energy-supply-chain

の対象となる可能性があるとしている。戦略文書では、特定の技術分野及び横断的なトピックに関するサプライチェーン評価結果も示している。サイバーセキュリティに関する主な評価結果として、評価の結果得られた事項と機会[14]は以下のとおりである。

- エネルギー分野におけるサプライチェーンリスクが増大

  サイバー敵対者は、エネルギー部門のデジタル資産の脆弱性に狙いを定め、これを悪用している。主な脆弱性には、信頼できない海外のサプライヤーやソフトウェア開発者に依存した脆弱性、不透明で動的なグローバルサプライチェーンに依存した脆弱性等が含まれ、主なサイバー脅威として、高度な情報収集とサイバー能力を持つ敵対国からの国家安全保障上の脅威、SolarWinds の事例のようなサプライチェーン攻撃を行う犯罪行為者からの脅威等が挙げられる。

- デジタル化、分散化、脱炭素化を考慮した将来的な脆弱性を軽減することが必要

  レガシーシステムのサイバーサプライチェーンリスクは、包括的な管理・緩和が必要な懸念事項であり続けるが、再生可能エネルギーや分散型エネルギーシステムなどの技術が導入されることに伴い、新たな資産におけるサプライチェーンリスクも考慮する必要がある。具体的には、仮想プラットフォームや AI・機械学習技術の利用が増加されており、これらのデジタル資産に対しても、サプライチェーンセキュリティを考慮した開発が求められる。

- 分散型エネルギー源管理システム及びエンドポイントデバイスの保護が必要

  送電網の近代化と脱炭素化に伴い、家庭用電気自動車の充電器等、送電網に接続されるエンドポイントデバイスの数が増加することが予想される。接続機器のファームウェアや接続・管理に使用されるソフトウェアのサプライチェーン完全性を確保するために、積極的なセキュリティ投資が必要である。

- 仮想プラットフォームのセキュア化

  産業用制御システムをより柔軟に運用する効率重視の傾向は今後も続くことが想定される。その結果、サードパーティがホストする仮想プラットフォームや仮想サービスのセキュリティが更に重要となる

- 高信頼性データのためのサイバーセキュリティ強化

  AI や機械学習は、米国の国家や経済の安全保障に欠かせない新興技術である。データは、AI や機械学習の重要なインプットであり、ソフトウェアがもたらすリスクと同様のサプライチェーンリスクをもたらす可能性がある。AI や機械学習は国家や経済の安全保障の観点でも重要であるため、データのサプライチェーンセキュリティと完全性を確保するための積極的アプローチが重要である。

これらの評価結果を踏まえ、上記戦略文書において、デジタル資産、仮想プラットフォーム及びデータのサイバーセキュリティを強化するための政策戦略が発表されている。発表された戦略の概要は以下のとおりであり、サプライチェーンに関するデータベースの開発や新たなサプライチェーン戦略の策定等が明記されている。

- データ及び分析能力の向上

  現行及び将来のサプライチェーンの脅威、リスク、脆弱性、機会を理解するためには、レジリエ

[14] “Achieving American Leadership in Cybersecurity and Digital Components” https://www.energy.gov/sites/default/files/2022-02/Cybersecurity%20Supply%20Chain%20Fact%20Sheet.pdf

ントなサプライチェーンを改善・維持するための意思決定を支援するデータと分析ツールが重要となる。現在のデータや分析ツールは断片的で一貫性がなく、不完全なものである。包括的なデータは体系的なサプライチェーンのリスクを明らかにするとともに、リスク分析や対策の進捗を確認するために重要であるため、DoE は他の連邦機関と協力して、データベース[15]と意思決定モデルを開発する。

- セキュアデジタル部品サプライチェーン戦略の策定

  サプライチェーンリスクは相互接続されたエネルギーシステム間で共有されるため、システムの強靭性とサプライチェーンセキュリティ対策を効果的に向上させるためには、より包括的なアプローチが必要である。政府及び民間セクターのステークホルダーも巻き込み、戦略的なアプローチを開発することで、重要なサプライチェーンの定義や優先順位付け、対策ベースラインや目標の設定、送電網の近代化や脱炭素化の推進に伴って予想される変化への計画等、ESIB 全体の主要機能を実現することができる。

- 管理やガイドラインの更新

  ESIB において共有されるサイバーセキュリティリスクを管理するために、より整合した方針と一貫したガイドライン、標準、プロセスを開発することが重要である。これにより、重要なデジタル部品のサプライチェーンリスクに対して、一貫性のある管理の実現につながる。既存の標準や新しいガイドラインを活用・構築し、政府や ESIB の主要関係者と連携することで、ESIB 全体で一貫性のあるセキュリティ対策を向上させることができる。

2.2 新規プレーヤーに関するサイバーセキュリティ対策の検討

電力システムに対する新規プレーヤーのうち、特に小規模発電設備等に求められるサイバーセキュリティ対策について検討を行った。具体的には、国内の小規模発電設備設置者、関連メーカー、関連業界団体等及び学識者等が参加し、小規模発電設備に求められるサイバーセキュリティ対策について検討する検討会を開催し、系統連系技術要件で求められるセキュリティ対策の実装例を記した文章の策定を行った。

2.2.1 小規模発電設備等のセキュリティ対策に関する現状

（1） 小規模発電設備等のセキュリティ対策に関するこれまでの検討

あらゆる分野でデジタル化が進展する一方、多様化・巧妙化するサイバー攻撃の脅威は日々高まっており、重要インフラたる電力分野においても、サイバーセキュリティ向上に向けた不断の取組が求められている。電源の分散化やオンライン化の拡大する現状においては、電気事業者に対するサイバーリスクだけでなく、電力事業の用に供しない小規模発電設備等に対するサイバーリスクも高まりつつある。

小規模発電設備等におけるサイバーリスクの高まりをうけ、経済産業省の産業サイバーセキュリティ

[15] 2021 年度国防権限法（NDAA）の 9413 項では、NIST に対し、サプライチェーンに関連したデータベースの構築に係るフィージビリティスタディが指示されている。このデータベースは、米国機器メーカーの能力を踏まえてサプライチェーンの混乱を最小限に抑えることが目的であり、サプライチェーンリスク、依存関係、障害点等を早期に特定し、関係者による事前対策を可能にする等、ESIB のサプライチェーンの分析を支援するものであると期待されている。

研究会ワーキンググループ 1（制度・技術・標準化）電力サブワーキンググループ（電力 SWG）や電力・ガス基本政策小委員会において、電力事業の用に供しない小規模発電設備等を系統に接続する際にすべからく求められるサイバーセキュリティ対策について議論が行われてきた。これまでの議論を通じて、以下の 3 つのセキュリティ対策の必要性が提示された。

1. サイバーインシデントの発生を防ぐ事前防御の観点として、

   対策①　ネットワーク接続点の保護：

   発電設備の制御を行うシステム（制御システム）とインターネットとを分離する等の措置により、外部からの不正侵入を防止し、また、他のネットワークでのインシデントが制御システムに伝播することを防止する。

   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：

   マルウェアの感染によりシステムに不具合が発生し、制御システムが利用できなくなることを防止する。

2. 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）の観点として、

   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

これらの対策の必要性を踏まえ、2020 年 10 月より一般送配電事業者の策定する「系統連系技術要件」（託送供給等約款別冊）において 3 つの要件が規定され、当該要件は 2020 年 10 月以降に契約申込みを行うもの（電源接続案件募集プロセス対象の設備にあっては、2020 年 10 月以降に入札を実施するもの）を対象に実施を求めることとされた。現在、一般送配電事業者に対する系統連系の申請に際しては、これらの対策①～対策③を実施していることを確認した上で申請することが必要となっている。

系統連系技術要件にサイバーセキュリティ対策の要件が規定されることを受け、昨年度事業において小規模発電設備等を系統に接続する者や小規模発電設備等のメーカーに対して実態調査を行い、系統連系技術要件におけるサイバーセキュリティに関する要件に関して、補足説明や設備種別ごとに対策実装例等を求める意見が多数挙げられた。

この背景に基づき、小規模発電設備等のセキュリティ対策に関する検討会を設置し、様々な設備種別における系統連系技術要件の対策実装例を議論した。この検討会では、系統連系技術要件の主な対象である小規模発電設備等のうち、一般用電気工作物に分類される小出力発電設備に対して求められるセキュリティ対策に関して議論した。我が国における導入状況やこれまでの議論を踏まえ、太陽光発電設備、風力発電設備、コージェネレーションシステム、家庭用電気設備（エネファーム、蓄電池 等）の 4 つの種別を代表的な小出力発電設備と捉え、各設備種別の典型的なシステム構成に基づき対策実装例を検討した。

（2）小規模発電設備に関する脆弱性事例

小出力発電設備のオンライン化が進展することでより柔軟な需給の調整が可能となった一方で、ネットワークを介したサイバー攻撃の起点も拡大しており、サイバーセキュリティ上の脅威も増大している。小出力発電設備に関連するサイバーセキュリティリスクの事例として、海外製インバーターにおける脆弱性の事例や、小形風力発電設備における脆弱性の事例、蓄電池関連設備における脆弱性の事例などが挙げられる。

2.2.2 サイバーセキュリティ対策実装例の策定

（1） 対策実装例の対象種別

今年度策定する対策実装例の対象となる小規模発電設備について、自家用電気工作物については、既に保安規制の枠組みの中でガイドライン策定が検討されていることを踏まえ、一般用電気工作物に分類される、以下の小出力発電設備を主な対象とした。

- 系統連系する 50kW 未満の太陽光発電設備（低圧太陽光発電設備）
- 系統連系する 20kW 未満の風力発電設備（小形風力発電設備）
- 系統連系する 10kW 未満のコージェネレーション設備
- 系統連系する家庭用電力設備（エネファーム、蓄電池 等）

それぞれの種別について、設備設置者、関連機器メーカー等のステークホルダーを対象とした対策実装例、すなわち計 4 つの対策実装例を作成した。各対策実装例の対象設備及び対象者を表 2-1 に示す。

表 2-1 各対策実装例の対象設備・対象者（ステークホルダー）

対策実装例の名称	小出力太陽光発電設備に係るサイバーセキュリティ対策の実装例	小出力風力発電設備に係るサイバーセキュリティ対策の実装例	小出力コージェネレーション設備に係るサイバーセキュリティ対策の実装例	家庭用電気工作物に係るサイバーセキュリティ対策の実装例
対象設備	10kW 以上 50kW 未満の太陽光発電設備（低圧事業用太陽光発電設備）	20kW 未満の風力発電設備	10kW 未満のコージェネレーション設備（ただし、エネファームを除く）	・ 10kW 未満の太陽光発電設備（低圧住宅用太陽光発電設備） ・ 家庭用蓄電池 ・ エネファーム

対策実装例の名称	小出力太陽光発電設備に係るサイバーセキュリティ対策の実装例	小出力風力発電設備に係るサイバーセキュリティ対策の実装例	小出力コージェネレーション設備に係るサイバーセキュリティ対策の実装例	家庭用電気工作物に係るサイバーセキュリティ対策の実装例
対象者	・ 小出力太陽光発電設備の設置者 ・ 小出力太陽光発電設備の設置工事を請け負う施工業者 ・ 小出力太陽光発電設備等のメーカー ・ 監視サービスプロバイダー等	・ 小出力風力発電設備の設置者 ・ 小出力風力発電設備の設置工事を請け負う施工業者 ・ 小出力風力発電設備等のメーカー ・ 監視サービスプロバイダー等	・ 小出力コージェネレーション設備の設置者 ・ 小出力コージェネレーション設備の設置工事を請け負う施工業者 ・ 小出力コージェネレーション設備等のメーカー ・ 監視･制御等のサービスプロバイダー	・ 家庭用電気工作物の設置者（設置家庭） ・ 家庭用電気工作物の設置工事を請け負う施工業者 ・ 家庭用電気工作物等のメーカー ・ 設置者向けサービスを提供する事業者等

（2） 対策実装例の項目立て･作成方針

各対策実装例の作成方針･全体像を図 2-4 に示す。各対策実装例では、系統連系技術要件で求められる 3 つの対策について、対象設備に関連する各ステークホルダーが実施すべき対策の実装例を記載することとした。また、対策の必要性を訴求するために、対象設備に想定されるサイバーセキュリティリスクや、リスクが顕在化した場合の影響も併せて記載することとした。

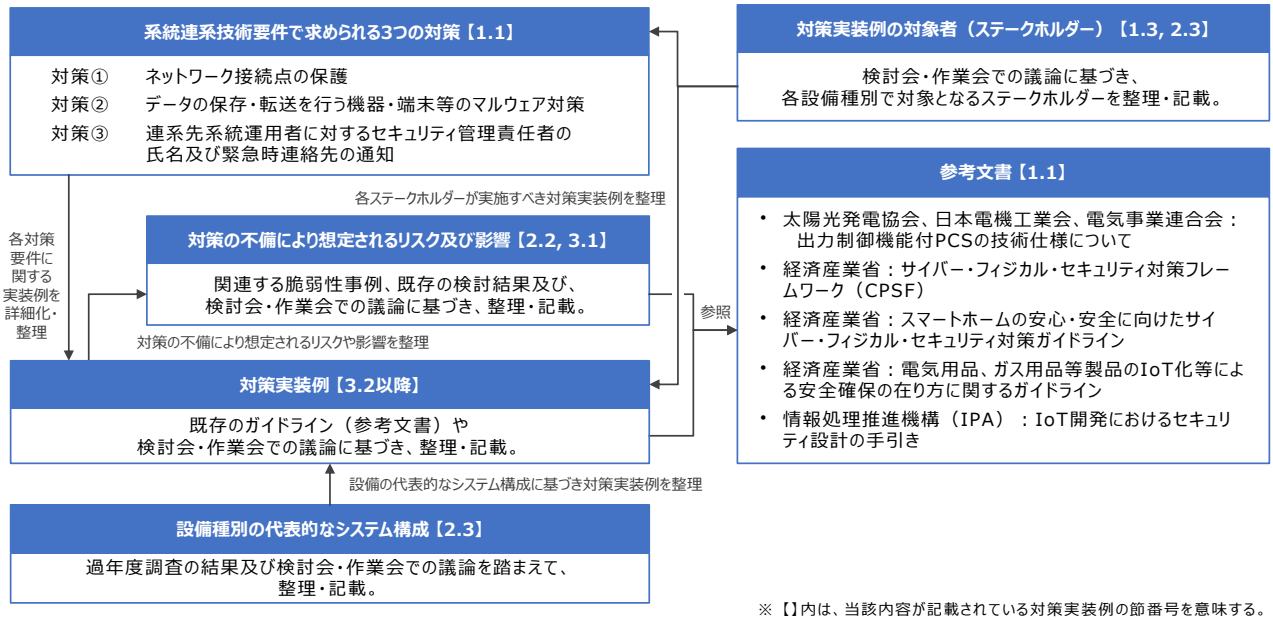


図 2-4　対策実装例の作成方針・全体像

（3）対策実装例の公開に向けた検討

策定した対策実装例の案について、2021 年 12 月 24 日開催した第12回電力 SWG において委員より確認をいただき、内容に関するコメントを頂戴した。第 12 回電力 SWG 後にいただいたコメントを踏まえ、対策実装例の内容の修正を行った。第 12 回電力 SWG では、対策実装例の公開方法に関しても報告し、その方法について確認をいただいた。第 12 回電力 SWG 以降、各対策実装例の公開に向け、関連する業界団体と調整を行った。具体的な公開方法は以下のとおりである。

- 多様なステークホルダーに必要な情報が過不足なく伝わるよう、各対策実装例は、それぞれの種別の個別検討会に参加いただいた業界団体の名義（連名）にて策定する。
- 対策の詳細が確認できる対策実装例全体（文書全体）は、業界団体の会員限り等の限定的な公開とする。
- 設備設置者・施工業者に対しても系統連系申請のための対策実装例を周知することが望まれるところ、これらのステークホルダーに向けて、対策実装例の項目リストのみを業界団体の HP で一般公開する。

2.2.3 検討会及び作業会の開催

サイバーセキュリティ対策の実装例の検討に向けて、電力サブワーキンググループの下に、「一般用電気工作物のサイバーセキュリティ対策に係る検討会」を設置した。この検討会では、各種別の対策実装例に関する計 3 回の個別検討会及び計1回の全体検討会を開催した。このほかに、サイバーセキュリティ対策の実装例作成のために計3回の作業会を開催した。各会の開催日程は以下のとおりである。

- 2021 年 11 月 8 日：小出力コージェネレーションシステムのサイバーセキュリティ対策実装に係る検討会
- 2021 年 11 月 9 日：小出力太陽光発電設備・小出力風力発電設備のサイバーセキュリティ対策実装に係る検討会

- 2021 年 11 月 12 日：家庭用設備のサイバーセキュリティ対策実装に係る検討会
- 2021 年 12 月 1 日：家庭用設備のサイバーセキュリティ対策実装に係る作業会
- 2021 年 12 月 6 日：小出力太陽光発電設備・小出力風力発電設備のサイバーセキュリティ対策実装に係る作業会
- 2021 年 12 月 8 日：小出力コージェネレーションシステムのサイバーセキュリティ対策実装に係る作業会
- 2021 年 12 月 17 日：一般用電気工作物のサイバーセキュリティ対策に係る検討会

図 2-5 に検討会及び作業会の位置づけを示す。なお、小出力太陽光発電設備と小出力風力発電設備は設備構成が類似するところ、対策実装例は別々に作成するものの、個別検討会・作業会は合同で開催した。

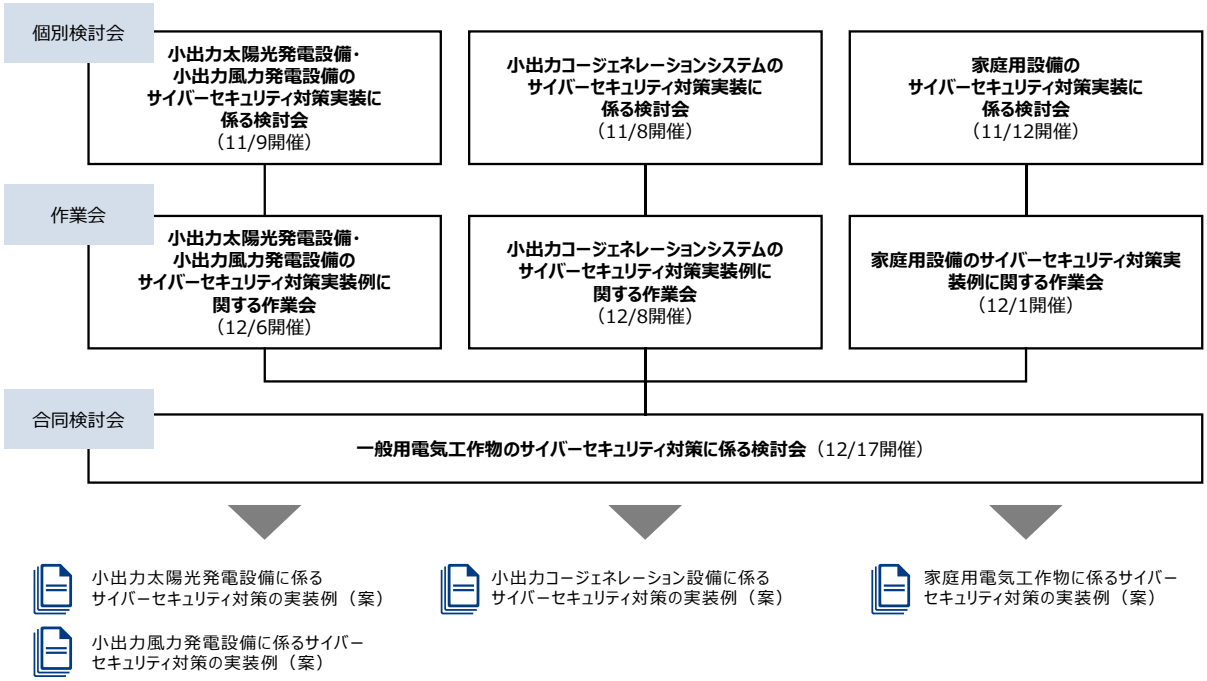


図 2-5 検討会及び作業会の位置づけの概要図

（1） 各種別におけるサイバーセキュリティ対策実装に係る検討会

各種別の検討会には、日本電機工業会、日本ガス協会、日本小形風力発電協会、太陽光発電協会、コージェネレーション・エネルギー高度利用センターの業界団体から参加いただいた。また、電力サブワーキンググループの一部の委員からも有識者としての参加いただい。

検討会では、各種別における実装例の対象者・代表的なシステム構成についての討議が行われた。また、代表的なシステム構成を踏まえ、小規模発電設備に関するサイバーセキュリティ上のリスクについて討議が行われた。そして、各リスクに対して実装すべき対策実装例の方向性が議論された。ここでは、系統連系技術要件で求められる3つの対策を基に、設備に関連するステークホルダーが実施するべき内容を整理し、対策実装例を取りまとめる方向性で進めることが合意された。また、具体的な内容は、検討会とは別に作用会を設置し、当該作業会にて検討及び編集作業を行うことについても合意された。

小出力コージェネレーションシステムのサイバーセキュリティ対策実装に係る検討会開催概要

日時　　：2021年11月8日 14時00分～16時00分
場所　　：オンライン会議
出席者　：
【セキュリティ有識者】
JPCERT/CC
情報処理推進機構
【業界団体】
一般財団法人 コージェネレーション・エネルギー高度利用センター
一般社団法人 日本ガス協会

議事次第：
1. 開会
2. 一般用電気工作物のセキュリティ対策に係る検討について
3. サイバーセキュリティ対策実装例の作成に向けた論点について
4. 自由討議
5. 閉会

小出力太陽光発電設備・小出力風力発電設備のサイバーセキュリティ対策実装に係る検討会開催概要

日時　　：2021年11月9日 15時00分～17時00分
場所　　：オンライン会議
出席者　：
【セキュリティ有識者】
JPCERT/CC
情報処理推進機構
【業界団体】
一般社団法人 日本電機工業会
一般社団法人 日本小形風力発電協会
一般社団法人 太陽光発電協会
全日本電気工事業工業組合連合会

オブザーバー ：
送配電網協議会
電気事業連合会

議事次第：
1. 開会
2. 一般用電気工作物のセキュリティ対策に係る検討について

3. サイバーセキュリティ対策実装例の作成に向けた論点について
4. 自由討議
5. 閉会

家庭用設備のサイバーセキュリティ対策実装に係る検討会開催概要

日時　　：2021年11月12日 10時00分～12時00分
場所　　：オンライン会議
出席者　：
【セキュリティ有識者】
JPCERT/CC
情報処理推進機構
【業界団体】
一般財団法人 コージェネレーション・エネルギー高度利用センター
一般社団法人 日本ガス協会
一般社団法人 日本電機工業会
一般社団法人 太陽光発電協会

議事次第：
1. 開会
2. 一般用電気工作物のセキュリティ対策に係る検討について
3. サイバーセキュリティ対策実装例の作成に向けた論点について
4. 自由討議
5. 閉会

（2）各種別におけるサイバーセキュリティ対策実装に係る作業会

各種別におけるサイバーセキュリティ対策実装に係る検討会で合意された方針を受け、「小出力太陽光発電設備に係るサイバーセキュリティ対策の実装例」・「小出力風力発電設備に係るサイバーセキュリティ対策の実装例」・「小出力コージェネレーション設備に係るサイバーセキュリティ対策の実装例」・「家庭用電気工作物に係るサイバーセキュリティ対策の実装例」の作成のための作業会が開催された。具体的には、事務局が作成した対策実装例の素案に対するレビューや修正案の検討等が行われた。

家庭用設備のサイバーセキュリティ対策実装に係る作業会開催概要

日時　　：2021年12月1日 13時00分～15時00分
場所　　：オンライン会議

出席者　：
【業界団体】
一般財団法人 コージェネレーション・エネルギー高度利用センター

一般社団法人 日本ガス協会
一般社団法人 日本電機工業会
一般社団法人 太陽光発電協会
全日本電気工事業工業組合連合会
【関連機器メーカー等】
アイシン株式会社
オムロンソーシアルソリューションズ株式会社
パナソニック株式会社
東京ガス株式会社
大阪ガスマーケティング株式会社

議事次第：
1. 開会
2. 一般用電気工作物のセキュリティ対策に係る検討について
3. サイバーセキュリティ対策実装例の作成方針について
4. 自由討議
5. 閉会

小出力太陽光発電設備・小出力風力発電設備のサイバーセキュリティ対策実装に係る作業会開催概要

日時　　：2021年12月6日 9時00分～12時00分
場所　　：オンライン会議
出席者　：
【業界団体】
一般社団法人 日本電機工業会
一般社団法人 日本小形風力発電協会
一般社団法人 太陽光発電協会
全日本電気工事業工業組合連合会
【関連機器メーカー等】
オムロンソーシアルソリューションズ株式会社
株式会社コンテック
パナソニック株式会社
リコージャパン株式会社

議事次第：
1. 開会
2. 一般用電気工作物のセキュリティ対策に係る検討について
3. サイバーセキュリティ対策実装例の作成方針について
4. 自由討議
5. 閉会

小出力コージェネレーションシステムのサイバーセキュリティ対策実装に係る作業会開催概要

日時　　：2021年12月8日 15時00分～17時00分

場所　　：オンライン会議

出席者　：

【業界団体】

一般財団法人 コージェネレーション・エネルギー高度利用センター

一般社団法人 日本ガス協会

【関連機器メーカー等】

ヤンマーエネルギーシステム株式会社

静岡ガス・エンジニアリング株式会社

大阪ガス株式会社

議事次第：

1. 開会
2. 一般用電気工作物のセキュリティ対策に係る検討について
3. サイバーセキュリティ対策実装例の作成方針について
4. 自由討議
5. 閉会

（3）一般用電気工作物のサイバーセキュリティ対策に係る検討会

各種別の検討会・作業会を通じて作成された各種別の実装例の案について、その概要と作業過程を説明したうえで、これまでの全ての参加者及び有識者によるレビューと改善のための討議を行った。実装例の各対策事項について加筆や修正を行うべき点の指摘や、実装例を今後どのように普及し、公開していくかといった方針についての議論がなされた。また、本検討会での指摘を踏まえて修正を行った実装例は、第12回電力SWGにおいて、委員に確認いただいた。

一般用電気工作物のサイバーセキュリティ対策に係る検討会開催概要

日時　　：2021年12月17日 14時00分～16時00分

場所　　：オンライン会議

出席者　：

【セキュリティ有識者】

JPCERT/CC

情報処理推進機構

【業界団体】

一般財団法人 コージェネレーション・エネルギー高度利用センター

一般社団法人 日本ガス協会

一般社団法人 日本電機工業会

一般社団法人 太陽光発電協会

一般社団法人 日本小形風力発電協会
全日本電気工事業工業組合連合会
【関連機器メーカー等】
アイシン株式会社
大阪ガス株式会社
大阪ガスマーケティング株式会社
オムロンソーシアルソリューションズ株式会社
株式会社コンテック
静岡ガス・エンジニアリング株式会社
東京ガス株式会社
パナソニック株式会社
ヤンマーエネルギーシステム株式会社
リコージャパン株式会社

オブザーバー ：
送配電網協議会
電気事業連合会

議事次第：
1. 開会
2. サイバーセキュリティ対策実装例の作成方針について
3. 自由討議
4. 閉会

2.3 電力システムのサイバーセキュリティリスクの分析

国内の電力分野における、新規事業者の参入状況、規制体系ごとに求められる対策の違い及びデジタル化の進捗状況等の環境変化を整理した上で、こうした環境変化も踏まえた電力分野におけるサイバーセキュリティ対策の状況について、効果的なリスクアセスメントの実施方法の検討、分析を行った。

2.3.1 電力システムのサイバーセキュリティ対策に関する現状分析

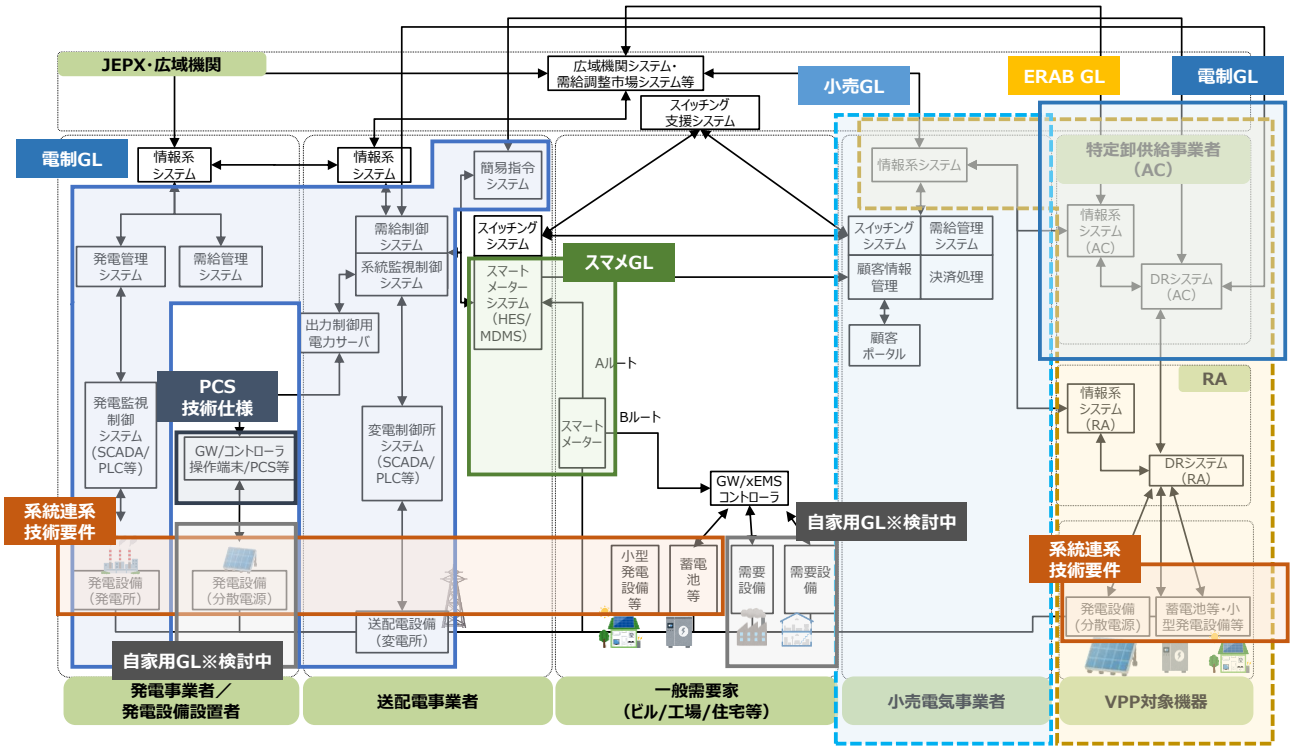
これまで、電力 SWG を中心として電力システムに求められるサイバーセキュリティ対策が議論されてきた。電力 SWG は、電力制御系システムに関するセキュリティ向上策、電力制御系システムに関連した分野におけるセキュリティ向上策、業界全体の取組向上に資する基盤整備などの具体的な対応策について検討を深める目的で設置され、これまで 12 回にわたり開催されている。第５回電力 SWG 以降は、特に以下の 3 つの観点から、電力分野のサイバーセキュリティ対策高度化に向けた議論・検討を行ってきた。

1. 大手電気事業者に求められるサイバーセキュリティ対策
2. 新規プレーヤーに求められるサイバーセキュリティ対策

3. 電力分野におけるサプライチェーンリスクへの対応

具体的には、1. 大手電気事業者に求められるサイバーセキュリティ対策の検討に関して、大手電気事業者におけるサイバーセキュリティ対策状況の実態把握を実施した。また、2. 新規プレーヤーに求められるサイバーセキュリティ対策に関して、小売電気事業者等の新規プレーヤーのセキュリティ対策状況を把握するとともに、「小売電気事業者のためのサイバーセキュリティ対策ガイドライン」を策定したほか、小規模発電事業者向けに、系統連系技術要件へのサイバーセキュリティ対策の追加を検討するとともに、2.2 節で記載したとおり、系統連系技術要件で求められる対策の補足説明や実装例を記載した対策実装例を整理・策定した。そして、3. 電力分野におけるサプライチェーンリスクへの対応に関して、米国規制の状況について把握・情報共有するとともに、国内で求められるサプライチェーンリスク管理方策について議論してきた。

電力 SWG 等の議論を通じ、現状では、電力システムのプレーヤーに対して一定の対策が講じられている。電力システムに対するサイバーセキュリティに関する現状の取組みは図 2-6 及び表 2-2 のように整理される。



出所）各種ガイドライン等の情報に基づき三菱総合研究所作成

図 2-6 電力システムにおけるサイバーセキュリティに関する現状の取組概要[16]

表 2-2 電力システムに関するプレーヤーに求められるガイドライン等

名称	主な対象	発行主体	概要
電力制御システムセキュリティガイドライ	電気事業の用に供する電	日本電気協会	電気事業法、電気設備に関する技術基準を定める省令及びその解釈に基づき、電気事業の用に供する電

[16] 各ガイドライン等の概要は表 2-2 参照。実線は義務、点線は推奨として位置づけられているガイドライン等を意味する。なお、本図は各ガイドライン等の対象を明確化するために作成したものであり、実際の電力システムを精緻に整理したものではないことに留意。

名称	主な対象	発行主体	概要
ン（電制 GL）	気工作物		気工作物に対しては、本ガイドラインに基づく対策が求められる。
スマートメーターシステムセキュリティガイドライン（スマメ GL）	スマートメーターシステム	日本電気協会	電気事業法、電気設備に関する技術基準を定める省令及びその解釈に基づき、スマートメーターシステムに対しては、本ガイドラインに基づく対策が求められる。
系統連系技術要件	系統連系する発電設備	各一般送配電事業者	系統連系する発電設備にすべからく求められる対策。具体的には、ネットワーク接続点の保護、マルウェア対策、系統運用者に対するセキュリティ管理責任者の通知の 3 点が求められる。
出力制御機能付 PCS の技術仕様（PCS 技術仕様）	出力制御機能付 PCS	JPEA・JEMA・電事連	出力制御機能付 PCS において満たすべきサイバーセキュリティ対策の要件を示した技術仕様。
自家用電気工作物サイバーセキュリティガイドライン（案）（自家用 GL）	自家用電気工作物（発電設備と需要設備の両方を含む）	経済産業省	自家用電気工作物（発電設備と需要設備の両方を含む）に求められるサイバーセキュリティ対策事項を記載したガイドライン。
小売電気事業者のためのサイバーセキュリティ対策ガイドライン（小売 GL）	小売電気事業者	経済産業省	小売電気事業者が主体的に取り組むことが求められるサイバーセキュリティ対策に関して記載したガイドライン。
ERAB に関するサイバーセキュリティガイドライン Ver2.0（ERAB GL）	ERAB に関する事業者	経済産業省・IPA	ERAB のサービスレベルを維持するために ERAB に参画する各事業者が実施すべき最低限のセキュリティ対策の要求事項を示したガイドライン。

出所）各種ガイドライン等の情報に基づき三菱総合研究所作成

図 2-6 に整理されるとおり、これまでの取組を通じて、電力システムのプレーヤーに対して一定の対策が講じられていることが分かる。しかしながら、今後さらなるデジタル化の進展や新規プレーヤーの参入が予想される一方で、サイバーセキュリティの脅威は日々進化・巧妙化している状況を踏まえると、現状の対策で十分ということは決して無く、電力システムにおけるサイバーセキュリティ対策の継続的改善・高度化は必要不可欠である。

2.3.2 有識者に対するヒアリング結果

前述のとおり、サイバーセキュリティの脅威は日々進化・巧妙化していることを踏まえると、現状の対

策で十分ということは決して無く、今後もサイバーセキュリティ対策の高度化に向けた取組を推し進める必要がある。電力分野のサイバーセキュリティ対策の高度化に向けて今後取り組むべき事項に関する検討に際して、電力分野のサイバーセキュリティに関する有識者 2 名にヒアリングを行った。

2.3.3 電力システムのサイバーセキュリティリスクの分析方針

有識者に対するヒアリングの結果、電力分野の各プレーヤーにおけるリスクを分析し、より高度な対策が求められる箇所を特定することの必要性が提示された。これを踏まえ、今後、電力分野の各プレーヤーにおけるリスクを分析するとともに、リスク分析の結果を踏まえ、より高度な対策が求められるポイントに対して適切な取組を講じることが必要と考えられる。

リスク分析に当たっては、以下の点を考慮することが望まれる。

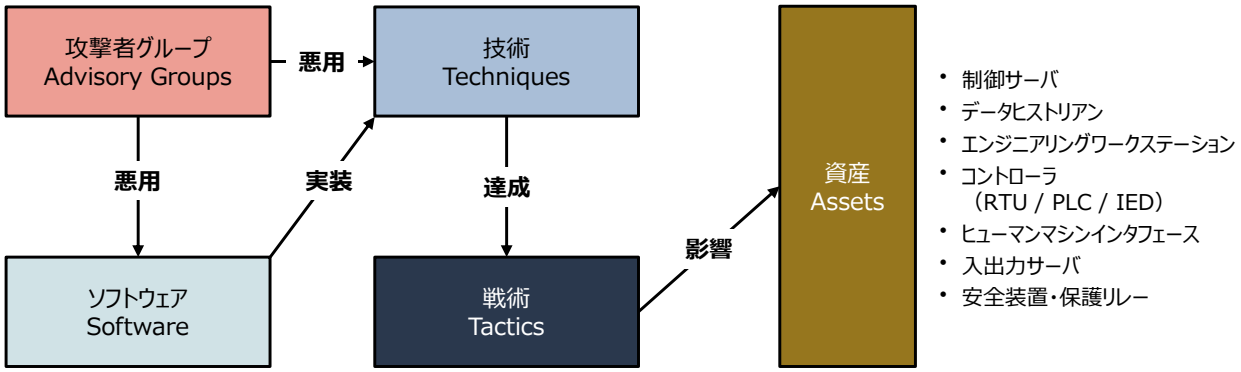
- リスク分析の目的を踏まえた対象の明確化・優先順位付け

  電力システムは非常に大規模なシステムであり、そこに関与するプレーヤーは非常に多岐にわたる。電力の安定供給の観点では、物理的に点在する制御システムに対するセキュリティ対策のみならず、サイバー空間上のデータやシステムに対するセキュリティ保護、さらには組織におけるセキュリティガバナンスや人員のセキュリティ意識も重要となる。また、電力システムは他のシステムと緊密に連携しており、デジタル化の進展により外部クラウドサービスへの依存度合いが高まっているほか、金融システム等、他の分野のシステムとも連携している。加えて、サプライチェーンリスクの観点では、電気事業者が有するシステムだけでなく、そのシステムに用いられる個々の機器に対するセキュリティ対策も重要となる。このように、多くの要素やプレーヤーの基で電力の安定供給が成り立っているが、すべての要素やプレーヤーに対して網羅的なリスク分析を行うことは現実的に困難であり、優先順位を付けた上でのリスク分析が必要となる。この際、リスク分析の目的を踏まえて優先順位を付け、リスク分析の対象を明確化することが必要であり、現状講じられている取組だけでなく、将来的な電力システムの構造も踏まえた優先順位の検討が望まれる。また、優先順位を付ける際、他の取組状況も把握することが必要である。例えば、今後経済安全保障推進法案の成立が予定されているところであるが、この法案では、電力分野を含む「基幹インフラ」の導入前に、安全保障上のリスクが無いかを確認する事前審査の制度を設けることが明記されている。他の取組状況を踏まえつつリスク分析の目的を明らかにした上で、リスク分析の対象を明確化することが必要である。

- 攻撃者視点でのリスクシナリオの検討

  リスク分析を実施するに当たって、様々なアプローチが考えられる。代表的なリスク分析のアプローチとして、保護すべき資産に基づきリスク分析を行う資産ベースのリスク分析、システムに対して攻撃が生じた際の事業被害に基づきリスク分析を行う事業被害ベースのリスク分析、既存のセキュリティ基準に基づきリスク分析を行うベースラインアプローチのリスク分析、これらのアプローチを組み合わせた組み合わせアプローチ等、様々なアプローチが想定される。それぞれのリスク分析アプローチに一長一短があるため、どのリスク分析アプローチを採用するかは対象を明確化した上で判断する必要があるが、いずれのアプローチを採用したとしても、攻撃者視点でのリスクシナリオを検討することが重要となる。すなわち、防御の視点から守るべき資産、想定される事業被害、求められる対策等を分析するだけでなく、攻撃者が採用する行動、戦術、技術、

ナレッジ、スキル等を踏まえ攻撃の可能性を分析することが重要となる。攻撃者の戦術や技術を理解する上では、MITRE が発表する ATT&CK（Adversarial Tactics, Techniques, and Common Knowledge）フレームワークや、当該フレームワークの産業制御システム向けである ATT&CK for ICS が活用できる。ATT&CK for ICS では「攻撃者グループ」、「ソフトウェア」、「技術」、「戦術」、「資産」及び「レベル」という複数の構成要素が規定され、それぞれが相互に関連することで、事業者の持つ資産（産業制御システム）に対して攻撃の影響を与えるものとしている（図 2-7）。攻撃者グループが選択する戦術とそれを達成するための技術は関係付けられており、攻撃の影響に結びつく戦術と対応する技術を選定・分析することが可能であるため、リスク分析に当たっては、電力分野に関わるプレーヤーが有する資産に対し、攻撃者の戦術・技術がどれだけ適用され、結果としてどのような影響が生じうるかを整理することが可能となる。



出所）MITRE ATT&CK for ICS ホームページに基づき三菱総合研究所作成

図 2-7 ATT&CK for ICS における構成要素の関係性

- 各プレーヤーにおけるセキュリティ対策状況の適切な把握

  いずれのリスク分析アプローチにおいても、電力分野に関係するプレーヤーにおける現状のセキュリティ対策状況の評価が必要となる。セキュリティ対策状況の評価にあたっては、その評価の項目や基準を決定する必要がある。評価項目や基準の決定にあたっては、リスク分析の対象を踏まえ、既存のガイドラインやフレームワーク等を活用することが効果的である。ただし、電力系統に関わる IT システム・OT システムの両方を対象とした網羅的なガイドライン・フレームワークはこれまで発表されていないところ、既存のガイドライン等をベースに、一部の項目や基準を今回のリスク分析向けに修正した形で活用することが望ましい。また、具体的な評価の方法について、チェックリスト等に基づく自己評価、アンケート調査に基づく評価、ヒアリング調査に基づく評価等、様々な方法が想定される。いずれの評価の方法においても、対象となるプレーヤーの協力が必要となるほか、チェックリスト等に基づく自己評価の場合は透明性担保のために、セキュリティ専門家による客観的な評価も加えることが望まれる。

リスク分析を実施した後、リスク分析を通じて得られた課題に対して、サイバーセキュリティ対策の高度化に向けた取組を検討することが必要である。具体的な取組の方向性はリスク分析を通じて明らかになるものであるが、以降では、現状で想定される今後の取組について、取組を進める上で参考となる関連する国内外の取組を概説する。

（1） ICSCoE における人材育成の取組

IPA の産業サイバーセキュリティセンター（ICSCoE）では、制御システムと情報システムのサイバーセキュリティ対策の必要性を把握し、経営層と現場担当者を繋ぐ中核人材を対象とした一年間の長期教育プログラムである「中核人材育成プログラム」を開講しており、令和 3 年度は第 5 期にあたる。このプログラムでは初歩的なレベル合わせからハイレベルな卒業プロジェクトまで実施されるとともに、受講者の出身組織に近い環境での演習を体験できるよう、各業界のシステムを想定した模擬システムを使用可能である。令和 2 年度（第 4 期）の受講者の出身業界としては電力分野が最も多い一方で、受講費用は 500 万円／年であり、企業としては一年間人材を派遣することになることから、中小企業をはじめとする新規プレーヤー等から人材においては受講のハードルが高いと想定される。

ICSCoE では、ERAB 事業者（主にアグリゲーター）のセキュリティ対策スキルを向上させるため、ERAB 事業者向けのサイバーセキュリティトレーニングを提供する予定であり、初回は 2022 年 2 月～3 月のうち 3 日間で開催される。このトレーニングでは、電力分野のサイバーセキュリティの概要や ERAB 事業者に関するガイドラインの解説がなされるほか、ERAB システムに対するリスク分析手法の解説・実演が実施される予定である。加えて、実機を用いたデモを中心とした演習も実施される予定である。受講料は 20 万円で、トレーニング期間が 3 日間と短期間であるため、上述の中核人材育成プログラムと比較すると、中小規模の事業者であっても参加しやすいと想定される。したがって、本事業で検討しうる新規プレーヤーを対象とした教育プログラムについても、ERAB 事業者向けのサイバーセキュリティトレーニングと同等の規模の教育プログラムとすることが望ましい。

（2） 米国 DoE における ES-C2M2 に関する取組

ES-C2M2（Electricity Subsector Cybersecurity Capability Maturity Model）とは、米国 DoE や DHS が開発した電力会社のサイバーセキュリティマネジメントに関する成熟度を測定するためのセルフアセスメントツールである。本ツールを活用することで、サイバーセキュリティ能力の評価が可能となるほか、評価を通じて、サイバーセキュリティ向上のために必要な行動や優先的な投資先が把握できるとしている。米国では、リスク分析を実施する際に NIST CSF を活用することが困難な電力会社において ES-C2M2 が活用されることもあり、本事業においてセルフアセスメント用のチェックリストの開発する際、その記載内容や粒度について参考になると考えられる。なお、IPA より ES-C2M2 の解説書及びチェックシート（日本語版）が公開[17]されている。

（3） 金融 ISAC における取組

より高度な情報共有機会の提供や情報共有基盤の構築にあたって、金融分野における ISAC である金融 ISAC の取組が参考となる。金融 ISAC は、日本の金融機関の間でサイバーセキュリティに関する情報の共有・分析、及び安全性の向上のための協働活動を行い、金融サービス利用者の安心・安全を継続的に確保することを目的とした組織であり、日々発生するインシデントや脆弱性を会員間で共有する「コレクティブインテリジェンス」と、共通の課題に対しリソースを共有し、協働しながら対策の検討を進めていく「リソース・シェアリング」の 2 つを活動の柱としている。専用のポータルサイトを通じて、日々

[17] IPA，米国発のセキュリティマネジメント成熟度の評価モデル「ES-C2M2」の解説書およびチェックシートの公開
https://www.ipa.go.jp/security/controlsystem/usenergy.html

のインシデントや脆弱性情報等をリアルタイムに共有しているほか、特定の重要課題についてワーキンググループを設け、会員共同で対策検討等を行いながら知見と対応力を高めている。

金融 ISAC においても中小金融機関の加盟拡大が課題であった。これに対し、全国各地のワークショップに金融 ISAC が参加し、情報共有・地域連携の必要性をアピールしたほか、一年度分無償で金融 ISAC に所属できる「トライアル会員」[18]を新たに設立し、中小金融機関に対してはまずトライアル会員の加盟を推進することで、中小金融機関の会員数を着実に増加させた実績がある。本事業において中小企業も含めた情報共有機会・情報共有基盤の構築する際、これらの取組が参考になると考えられる。なお、2022 年 2 月現在、正会員 423 会員、賛助会員 1 会員、アフィリエイト会員 30 会員が金融 ISAC に加盟している。

2.4 ワーキンググループの運営

有識者（学識経験者やサイバーセキュリティ関連団体等を含む）や電気事業者等の委員によって構成され、我が国の電力分野における更なるサイバーセキュリティ向上策についての検討を行う、産業サイバーセキュリティ研究会ワーキンググループ 1 傘下の電力サブワーキンググループ（SWG）が、経済産業省によって開催されており、本事業ではその運営を行った。SWG では、電気事業者によるサイバーセキュリティ対策の実態把握や海外・他業種の動向調査を踏まえ、強化していくべき中長期的課題に対する取り組みを主に議論した。検討した主な中長期的課題は以下の 4 点である。

1. 小規模発電設備等におけるサイバーセキュリティ対策について
2. 大手電気事業者のサイバーセキュリティ対策について
3. サプライチェーンリスクへの対応について
4. 電力システムの高度化に向けたリスク分析について

なお、本 SWG は平成 30 年度から継続的に開催されているものであり、本事業では第 12 回から第 13 回の運営を行った。

2.4.1 第 12 回電力 SWG の運営

第 12 回 SWG では、東京オリンピック・パラリンピックの電力分野のサイバーセキュリティ対策について、サイバーセキュリティ体制及び大会に向けて実施した対策と今後の対応について議論が行われた。

大手電気事業者のサイバーセキュリティ対策について、2020 年度の取組の総括、2021 年度の取組における改善・スケジュールについて報告が行われた。また、小規模発電設備等におけるサイバーセキュリティ対策について、実装例を作成する上で設置された検討会・作業会の体制、各種別の実装例の内容・普及展開方法について報告が行われた。また、サプライチェーンセキュリティ規制の海外動向に関する報告が行われ、国内の対応について議論された。

産業サイバーセキュリティ研究会 WG1 電力 SWG（第12回）議事要旨

日時　　：令和3年12月24日（金）10時00分～12時00分

[18] トライアル中は一部サービスに制限があることに注意。なお、通常の正会員の年会費は 80 万円である。

出席者　：

（座長）渡辺　研司　　名古屋工業大学大学院

（委員）

有村　浩一	JPCERT/CC
稲垣　隆一	稲垣隆一法律事務所
内田　忠	電力 ISAC
江崎　浩	東京大学大学院
大崎　人士	産業技術総合研究所
大友　洋一	電気事業連合会
門林　雄基	奈良先端科学技術大学院大学
桑名　利幸	情報処理推進機構
新　　誠一	電気通信大学
高倉　弘喜	国立情報学研究所
谷口　浩	東京電力ホールディングス株式会社
都筑　秀明	日本電気協会　（代理：金子　貴之）
手塚　悟	慶應義塾大学

議題

1. 東京オリンピック・パラリンピックの電力分野のサイバーセキュリティ対策について
2. 「大手電気事業者のサイバーセキュリティ対策状況の実態把握」に関する取組について
3. 小規模発電設備等におけるサイバーセキュリティ対策について
4. 米国サプライチェーン規制等の状況について

要旨

1. 東京オリンピック・パラリンピックの電力分野のサイバーセキュリティ対策について
   （1）「東京オリンピック・パラリンピックの電力分野のサイバーセキュリティ対策について」を事務局より説明。
   （2）「東京オリパラ大会におけるサイバーセキュリティ対策の実施結果」を電気事業連合会より説明。
   （3）自由討議
   - 東京オリンピック・パラリンピックについて、電力供給停止に繋がるインシデントの発生は生じなかった。今回の経験を蓄積・共有していくことが重要。
   - 自然災害とインシデントの同時発生を考慮した訓練を実施すべき。

2. 「大手電気事業者のサイバーセキュリティ対策状況の実態把握」に関する取組について
   （1）「2021 年度「大手電気事業者のサイバーセキュリティ対策状況」の実態把握について」を電気事業連合会より説明。
   （2）自由討議
   - サイバーセキュリティ対策状況の実態把握を通じて、経営層を巻き込んだ対応策の検討を

実施することが重要である。
- 業界全体のセキュリティ対策の底上げに向けて、大手電気事業者で実施した内容を小規模電気事業者へ共有できるとよい。
- 電力分野を取り巻く環境の変化に対応して、評価項目を随時更新することが重要である。

3. 小規模発電設備等におけるサイバーセキュリティ対策について
(1)「小規模発電設備等のサイバーセキュリティ対策に係る検討について」を事務局より説明。
(2) 自由討議
- ネットワーク接続点の保護は重要であるため、その責任の所在について明記できるとよい。
- 対策実装例の実効性を上げる施策を引き続き検討する必要がある。特に、対策実装に当たってのコストの問題を検討する必要がある。
- 電力分野以外にガス・水道・ビル等の他分野を複合したサイバーフィジカル空間に求められる対策を今後検討できるとよい。

4. 米国サプライチェーン規制等の状況について
(1)「米国サプライチェーン規制等の状況について」を事務局より説明。
(2) 自由討議
- サプライチェーンは製品・部品以外に情報や人材まで範囲として含まれる。注目すべき範囲を適宜広げた上で、情報や人材のサプライチェーンへの考慮が望まれる。

2.4.2 第 13 回電力 SWG の運営

第 13 回 SWG では、大手電気事業者のサイバーセキュリティ対策について、2021 年度の評価結果のまとめや有識者の事前意見について報告が行われた。また、評価結果と今後の取り組みの進め方について議論が行われた。

電力分野のセキュリティ対策の高度化に向けた取組の方向性について、今後の電力分野におけるセキュリティ対策について議論が行われた、また、小規模発電設備等におけるサイバーセキュリティ対策について、第 12 回 SWG より実装例集に加えた変更点と実装例集の公開方法について報告が行われた。また、CPIC の取組について、国内での CPIC の検討状況と今後の展望について議論された。

産業サイバーセキュリティ研究会 WG1 電力 SWG(第13回)議事要旨

日時　　:令和4年2月21日(月)10時00分～12時00分
出席者　:
(座長) 渡辺 研司　　名古屋工業大学大学院
(委員)
有村 浩一　　JPCERT/CC
稲垣 隆一　　稲垣隆一法律事務所
内田 忠 電力 ISAC (代理:澤井 志彦)
大崎 人士　　産業技術総合研究所

大友 洋一	電気事業連合会
門林 雄基	奈良先端科学技術大学院大学
桑名 利幸	情報処理推進機構
新　 誠一	電気通信大学
高倉 弘喜	国立情報学研究所
都筑 秀明	日本電気協会
手塚 悟	慶應義塾大学
新田 哲	JFE スチール

議題

1. 「大手電気事業者のサイバーセキュリティ対策状況の実態把握」に関する取組について
2. 電力分野のセキュリティ対策の高度化に向けた取組の方向性について
3. 小規模発電設備等におけるサイバーセキュリティ対策について
4. CPIC に関する取組状況について

要旨

1. 「大手電気事業者のサイバーセキュリティ対策状況の実態把握」に関する取組について
   （1）「2021 年度「大手電気事業者のサイバーセキュリティ対策状況の実態把握」に関する評価結果ついて」を電気事業連合会より説明。
   （2）自由討議
   - 総じて良い方向に進んでいると考えているが、取組が陳腐化することを懸念している。ノウハウを蓄積・伝承しつつ、取組を継続することを期待する。
   - 管理的アプローチは、セキュリティ改善の一手法であり、最悪の事態を想定したアプローチも重要である。
   - サイバーセキュリティに関する観点だけでなく、サイバーフィジカルセキュリティに関する観点も含めた形で取組が進められると良い。
   - 自己評価によるベンチマークには限界がある。各社の事情を踏まえた評価や透明性の確保についても検討できると良い。

2. 電力分野のセキュリティ対策の高度化に向けた取組の方向性について
   （1）「電力分野のセキュリティ対策の高度化に向けた取組の方向性について」を事務局より説明。
   （2）自由討議
   - 電力安定供給のためには、IT と OT の両方についてセキュリティ対策の高度化を目指していくことが重要である。
   - 対策実施の主体や検討するテーマを拡大しつつ、事業者のセキュリティ対策意識の強靭化が重要である。具体的な取組においては、事業者が実際に対応できるよう、実効性のある対策を検討する必要がある。
   - 電力分野とガス分野は強く関連し、ガス分野においても自由化が進展しているところ、セキュリティ対策の検討にあたっても、電力分野とガス分野とが連携して検討を進められると

良い。

- 電力産業の性質を踏まえ、すべてのプレーヤーを取りこぼすことなく、優先度を付けた上で対策を検討することが重要となる。
- 対策が実施できている事業者の意見を抽出するだけでなく、対策ができていない要因についても検討することが必要である。
- リスク分析にあたっては、攻撃者の意図・作戦・戦略を検討した上で、その作戦を実行する際にどのような手口を使って侵入するのか、その結果どのような影響が生じうる可能性があるかを考えることが望まれる。
- IT システムの運用においてはアウトソースの比率が高いことを踏まえ、個社での対策だけでなく、業界全体としてのルールの検討が重要である。
- DX が進展する中で、新電力などではクラウド活用が進んでいる。火力発電等では運用の集中化も進んでおり、これらを突いた攻撃は影響が広範囲に及ぶので、そのような点にも留意して欲しい。

3. 小規模発電設備等におけるサイバーセキュリティ対策について

(1)「小規模発電設備等のサイバーセキュリティ対策実装例の公開について」を事務局より説明。

4. CPIC に関する取組状況について

(1)「CPIC に関する取組状況について」を経済産業省サイバーセキュリティ課より説明。

(2) 自由討議

- 国内電気事業者の事業形態は他国と大きく異なる。国内の事業者にとってメリットとなるような取組を検討できると良い。

3. 電力分野における機器・システムの調達時のセキュリティ検証・評価方法の調査・検討

電力分野における機器・システムの調達時のセキュリティ検証・評価方法に関して、令和元年度及び令和2年度の「再生可能エネルギー主力電源化に向けた電力分野のサイバーセキュリティに関する海外連携のあり方等調査事業」において整理した認証・評価項目案及び運用スキーム案をベースとして、実用可能な検証・評価方法を提案した。

具体的には、認証・評価項目案及び運用スキーム案をベースに、次の活動を通じて検証・評価方法を検討することとした。

- 過年度に検討したスコアカード方式による詳細評価項目に基づき、評価基準及び評価手順を具体化する。
- 策定した評価基準及び評価手順を検証するために、実機を用いた模擬評価を実施する。
- 2021 年度内に実施可能な作業量を考慮して、詳細評価項目の 7 つの大分類のうち、設計・開発・品質保証に該当する「②開発プロセスマネジメント(ECM)」「③製品・サービス仕様」「④開発環境」の 3 つを優先して実施する。
- 実機を用いた模擬評価では、「保護リレー」を候補とする。
- 実機を用いた模擬評価は、書面(設計・開発・品質保証に関する文書)による評価を中心とする。

検討にあたっては、次の内容を考慮した。

- 対象製品・システムの範囲については、ユーザー及びベンダーのニーズや諸外国の規制状況等の国際情勢等を勘案し、電力分野の制御システムにおける主要な構成要素とした。
  特に保護リレーについて、実機を用いた模擬評価の対象機器に選定することで、当該製品の検証・評価方法の知見を蓄積することに努めた。
- 評価基準・方法については、特に製品の設計・開発・品質保証のフェーズに焦点をあて、当該フェーズに対応する既存規格である IEC 62443-4-1 及び IEC 62443-4-2 に注目して検討を行った。
- 運用体制については、過年度の運用スキーム案で想定した国内認証機関と連携し、当該機関で検証・評価を行うことを視野に入れて、具体的な検証・評価手順の検討を行った。
- 運用方法については、実機を用いた模擬評価においても、関係者間での NDA 締結や、検証・評価結果のフィードバック方法などの検討を行った。
- 制度活用主体のインセンティブについては、評価手順を検討する際に、評価工数を削減するための評価方法の工夫や、効率的な検証が可能な評価項目の選定などに努めた。
- 国際的なセキュリティ検証・認証に関するスキームとの連携については、評価基準書及び評価手順書の案を策定する際に、既存の標準規格との関係を整理するとともに、国際的なスキームに直接提示できる内容となるように努めた。

実用的な検証・評価方法の提案にあたり、文献調査及びヒアリング調査を実施し、また勉強会を開催

した。また、実際の製品として保護リレーを 1 機種選定し、評価方法の実証を行った。

文献調査は、次の文献を対象とした。

- IEC 62443-4-1 及び IEC 62443-4-2
- NREL DERCF

ヒアリング調査は、次の内容について、各組織に対して実施した。

- ①実機を用いた模擬評価の対象機器について
  - 実機を用いた模擬評価の対象機器について、機器提供依頼を兼ねてベンダー各社に今年度の実機を用いた模擬評価の概要を説明し、進め方や実施内容に関する意見を伺った。ヒアリング対象はベンダー企業 5 者とした。
- ②認証・評価項目の評価基準について
  - 認証・評価項目の評価基準について、「評価基準書」及び「評価手順書」の案に関する意見を伺った。ヒアリング対象はベンダー企業及び関連組織、有識者の 9 者とした。
- ③実機を用いた模擬評価の実施結果を踏まえた検証・評価方法について
  - 実機を用いた模擬評価の実施結果を踏まえた検証・評価方法について、「評価基準書」及び「評価手順書」の改善に関する意見を伺った。ヒアリング対象はベンダー企業及び関連組織 6 者とした。

勉強会は、下表の 3 回開催した。

表 3-1 勉強会開催の概要

	開催日・開催方式	主な検討内容
第 1 回	2021 年 11 月 5 日 （オンライン開催）	● 評価基準書・評価手順書の策定方針について ● 評価基準書の記載内容について
第 2 回	2022 年 1 月 12 日 （書面開催）	● 評価手順書の記載内容について
第 3 回	2022 年 2 月 15 日 （オンライン開催）	● 評価基準書・評価手順書の記載内容について ● 関連する動向について

3.1 評価基準書の策定

過年度に検討したスコアカード方式による詳細評価項目に基づき、評価基準を記載した「評価基準書」の案を策定した。評価基準書の策定にあたっては、次の方針で検討を進めた。

- 過年度検討したスコアカード方式の詳細評価項目の 7 つの大分類のうち、設計・開発・品質保証に該当する「②開発プロセスマネジメント（ECM）」「③製品・サービス仕様」「④開発環境」の 3 つについて、評価基準の具体化を実施する。
- 上記②③④の詳細評価項目は、「サイバー・フィジカル・セキュリティ対策フレームワーク」（CPSF）では、いずれも対策要件「CPS.IP － 情報を保護するためのプロセス及び手順」のう

ち、CPS.IP-3「システムを管理するためのシステム開発ライフサイクルを導入する。」と対応する。このため、個々の詳細評価項目に対応する評価基準の具体化においては、他の既存の標準などを参照する必要がある。

- そこで、大枠としては CPSF の CPS.IP-3 に対応しているとしつつ、個別の評価項目（小項目）に対応する評価基準は、IEC 62443 ベースで検討する。
- ②③④に対応付けられた IEC 62443 の項目は、IEC 62443-4-1 及び IEC 62443-4-2 に集中している。このため、評価基準も IEC 62443-4-1 及び IEC 62443-4-2 の記述を参考にして検討する。
- ただし、IEC 62443-4-2 はベンダー側に求める取り組みとなっているため、ユーザー側で検証可能な評価基準となるように工夫する。
  （例：「○○機能を備えている」→「ユースケースを想定して、○○機能の要否を判断している。」）
- 評価結果のスコアリングについて、詳細評価項目毎のスコアに加えて、総合スコア等の考え方も検討範囲に含める。
  成熟度モデルを取り入れた電力分野のスコアリングの例として、ES-C2M2 をベースにした NREL の DERCF（Distributed Energy Resources Cybersecurity Framework）を参考とする。

上記の方針に基づき、評価基準書の素案を作成し、勉強会及びヒアリングを通じて改善点などの意見の収集を行った。提示された主な意見は次表の通りであった。また、主な意見のうち、現時点で評価基準書に反映可能な内容は、評価基準書の案に反映した。

表 3-2 評価基準書の案に対する主な意見や改善点

全般に関する意見	● 評価基準については、ユーザーとベンダー間で合意が取れたものがあるとよい。 ● 機種ごとに認証するのか、ソフトウェアなどの部品変更による再認証が必要なのか、という観点の検討が必要だろう。 ● 組織やプロセスに関する確認であれば、調達時の仕様確認の代替として本評価スキームの認証を活用できると思われるが、認証制度で評価する内容が組織やプロセスに偏ってしまうと、あいまいな評価制度となってしまうのではないか。 ● 最終的にどのような認証制度・スキーム（第三者認証・セルフチェック等）になるかを懸念している。 ● 自己診断＋外部診断を組み合わせながら診断方法によって結果をラベル分けなどできるとよいのではないか。

3.1.1 IEC 62443 に基づく評価基準の検討

評価基準の検討にあたっては、既存のガイドラインや標準を参考とした。特に、今回検討対象とした「②開発プロセスマネジメント（ECM）」「③製品・サービス仕様」「④開発環境」では、IEC 62443-4-1

及び IEC 62443-4-2 の内容を参考とした。

策定した評価基準書では、過年度に検討したスコアカード方式による詳細評価項目で検討済みであった「想定する脅威」「期待される対策概要」に加えて、「参考としたガイドライン等」に IEC 62443-4-1 及び IEC 62443-4-2 の項目を付記した。

「②開発プロセスマネジメント(ECM)」「③製品・サービス仕様」「④開発環境」の大項目ごとに、参考とした標準の項目の一覧を下表に示す。

表 3-3 参考としたガイドライン等一覧

大項目	参考としたガイドライン等
②開発プロセスマネジメント(ECM)	【IEC 62443-4-1】 ● SM-1: Development process ● SM-3: Identification of applicability ● SM-11: Assessing and addressing security-related issues ● SM-13: Continuous improvement ● SR-1: Product security context ● SR-2: Threat model ● SR-3: Product security requirements ● SR-5: Security requirements review ● SD-1: Secure design principles ● SD-2: Defense in depth design ● SD-3: Security design review ● SI-2: Secure coding standards ● SVV-1: Security requirements testing ● SVV-3: Vulnerability testing ● SVV-4: Penetration testing ● SVV-5: Independence of testers
③製品・サービス仕様	【IEC 62443-4-2】 ● CR1.1: Human user identification and authentication ● CR1.2: Software process and device identification and authentication ● CR1.3: Account management ● CR1.4: Identifier management ● CR1.13/NDR1.13: Access via untrusted networks ● CR1.6/NDR1.6: Wireless access management ● CR2.2: Wireless use control ● CR2.8: Auditable events ● CR2.9: Audit storage capacity ● CR2.10: Response to audit processing failures ● CR2.11: Timestamps

大項目	参考としたガイドライン等
	● CR2.13/EDR2.13/HDR2.13/NDR2.13: Use of physical diagnostic and test interfaces ● CR3.1: Communication integrity ● CR3.5: Input validation ● CR3.9: Protection of audit information ● CR3.11: Physical tamper resistance and detection ● CR3.14/EDR3.14/HDR3.14/NDR3.14: Integrity of the boot process ● CR4.1: Information confidentiality ● CR4.3: Use of cryptography ● CR5.1: Network segmentation ● CR5.2/NDR5.2: Zone boundary protection ● CR6.1: Audit log accessibility ● CR7.1: Denial of service protection ● CR7.2: Resource management ● CR7.3: Control system backup ● CR7.4: Control system recovery and reconstitution ● CR7.6: Network and security configuration settings
④開発環境	【IEC 62443-4-1】 ● SM-6: File integrity ● SM-7: Development environment security ● SM-9: Security requirements for externally provided components

3.1.2 NREL DERCF を参考としたスコアリングの検討

評価結果のスコアリングの方法については、次の方針で検討を進めた。検討にあたっては、後述する NREL DERCF の考え方を参考とした。

- 7 つの大項目に対して、大項目単位に評価した「項目別評価点」、及びそれらを統合した「総合評価点」を示す。
- 総合評価点及び項目別評価点は、「得点／満点」とする。
- 総合評価点は、項目別評価点の足し合わせ（Σ（項目別得点）／Σ（項目別満点））とする。
  ただし、満点の違い（例：大項目①が 100 点満点・大項目②が 50 点満点、など）で大項目間の優劣が出ないように、後述する「重みづけ」で調整する。
- 項目別評価点は、評価基準別得点（評価結果）の足し合わせ（Σ（評価基準別得点）／Σ（評価基準別満点））とする。
  ただし、項目別評価点の違い（例：評価基準 A の配点が 0 点～1 点、評価基準 B の配点が 0 点

～4 点、など)で評価項目間の優劣が出ないように、正規化(0 点～1 点)を行うか、後述する「重みづけ」で調整する。

- 評価基準別の得点(評価結果)は、評価基準の内容に応じて、次の NREL DERCF の方式を参考とし、実際のスコアリングで用いる得点の付け方については、評価手順書にて定める。
  - Yes/No 方式。Yes(評価基準を満たしている)は満点。No(評価基準を満たしていない)は零点。
  - 成熟度方式。5 段階の成熟度(例:Unimplemented, Partial, Risk Informed, Repeatable, Adaptive)に応じて 0 点～4 点。満点は 4 点。
  - 選択方式:評価基準に対して取りうる対応項目を選択肢として示し、選択された対応項目数に応じて配点。満点は選択肢数、あるいはそれ以下で定めた数(例:選択肢を 5 つ提示し、そのうち 3 つ以上選択できれば満点、など)。
- 評価対象とする機器や、その機器を使用するシステムの種類(重要度等)によって、重要視する評価項目が異なることが想定される。このため、評価項目に対して「重みづけ」を行える仕組みを導入する。標準的な重みづけに加えて、活用主体(エンドユーザ、インテグレータなど)が独自に検討した重みづけで対象機器の評価点を計算する仕組みも検討する。
  例:「大項目③製品・サービス仕様」を重要視するために、当該項目の重みづけを他の項目の倍にする、など。
- 可視化の方法は、総合評価点及び項目別評価点を円グラフで表示する。可視化のイメージを下図に示す。

評価項目	評価結果 (得点／満点)
総合評価点	△△／〇〇
①組織全体	△△／〇〇
②開発プロセスマネジメント(ECM)	△△／〇〇
③製品・サービス仕様	△△／〇〇
④開発環境	△△／〇〇
⑤SCM上流	△△／〇〇
⑥生産設備	△△／〇〇
⑦SCM下流	△△／〇〇

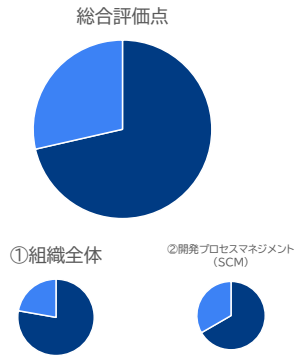


図 3-1 スコアリング結果の可視化イメージ

(1) NREL DERCF

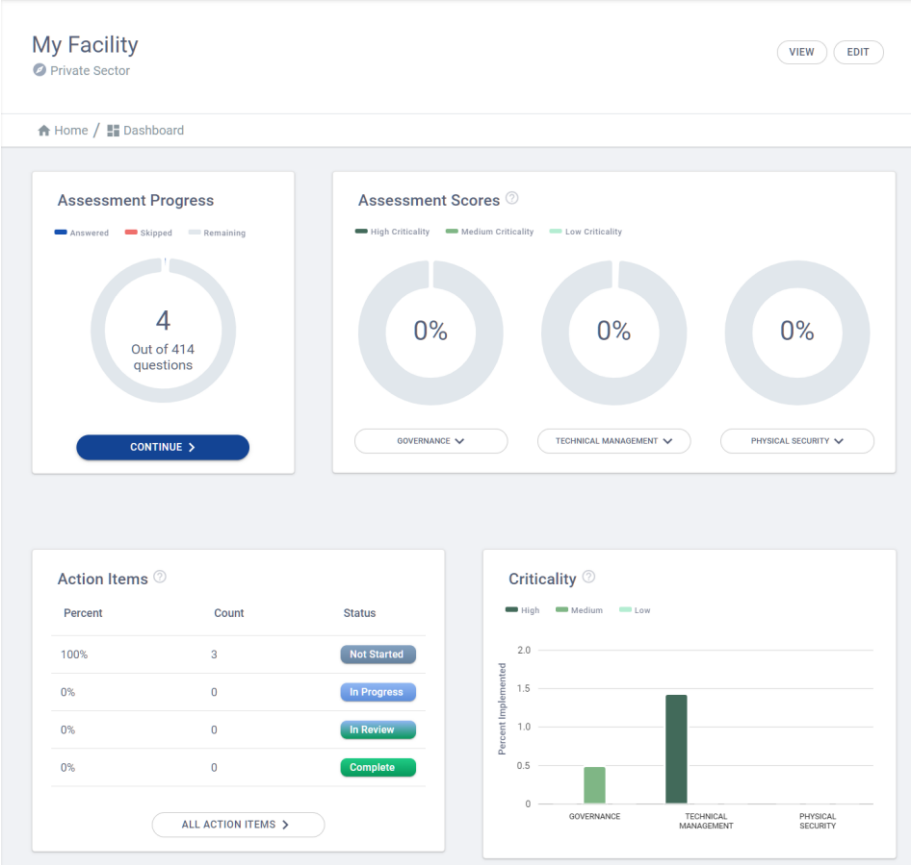
米国立再生可能エネルギー研究所(NREL, National Renewable Energy Laboratory)が開発した DERCF(Distributed Energy Resources Cybersecurity Framework)は、2019 年 12 月に発行された。2018 年 5 月に DOE が発行した Cybersecurity Strategy(DOE 2018)に対応して策定された。

NREL DERCF は、Web ベースのアプリケーション(Tool)として提供される[19]。また、ES-C2M2 の

[19] https://www.nrel.gov/docs/fy20osti/75044.pdf

成熟度モデルをベースとして、一部拡張している。

評価は 3 つの大項目(ガバナンス、技術的管理策、物理的セキュリティ)毎にまとめられており、414 項目の質問(2021 年 10 月時点)に対して 5 段階の成熟度(例:Unimplemented, Partial, Risk Informed, Repeatable, Adaptive)を答えることでスコアリングが行われる(一部の技術的管理策については Yes/No や選択式)。



出所)https://dercf.nrel.gov/app#/dashboard

図 3-2 NREL DERCF のスコアリングと可視化のイメージ

3.2 評価手順書の策定

前項で検討した評価基準書の案に基づき、評価の具体的な手順を記載した「評価手順書」の案を策定した。評価手順書の策定にあたっては、次の方針で検討を進めた。

- 評価基準書の策定時に参考とした、IEC 62443-4-1 及び IEC 62443-4-2 の記述を参考にする。
- 評価基準書の策定時に参考とした成熟度モデルの一部では、アセスメントガイド等でレベル分け(評価)手法(監査・評価時の方法)を示しているため、評価手順書策定の参考とする。
- スコアリングについて、検討時に「評価基準別得点(評価結果)」としていたものを「スコア1」(詳細項目ごとに付与するスコア)、7 つの大項目単位に評価した「項目別評価点」としていたものを「スコア2」(スコア 1 に基づき評価大項目ごとに付与するスコア)と定義した。

- 重みづけについては、「スコア 1」及び「スコア 2」を用いて活用主体が付与できるものとし、評価手順書では定義しないこととした。そのため、7 つの大項目の評価を統合した「総合評価点」については、評価手順書では定義せず、「スコア 2」の単純な足し合わせとした。
- なお、IEC では現在、評価手法を定めた以下の標準を策定中である。IEC TS 62443-6-2 は、IEC 62443-4-2 に対応した評価手法となるため参考としたいが、2021 年 10 月時点で CD（委員会原案）の段階で参照できない。国際規格としての発行は 2023 年 7 月予定なので、今回策定する評価手順書は、IEC TS 62443-6-2 発行後にその内容を確認することが望まれる。
  - IEC TS 62443-6-1
    Security evaluation methodology for IEC 62443 – Part 2-4: Security program requirements for IACS service providers
  - IEC TS 62443-6-2
    Security evaluation methodology for IEC 62443 – Part 4-2: Technical security requirements for IACS components

上記の方針に基づき、評価手順書の案を作成し、勉強会及びヒアリングを通じて改善点などの意見の収集を行った。また、後述する「実機を用いた模擬評価」の実施を踏まえた改善点の検討も行った。提示された主な意見や改善点は次表の通りであった。また、主な意見や改善点のうち、現時点で評価手順書に反映可能な内容は、評価手順書の案に反映した。

表 3-4 評価手順書の案に対する主な意見や改善点

全般に関する意見	● 文書内に書くべき項目（確認すべきドキュメントやエビデンス等）について、一定のレベルでの記載としていただきたい。レベルが過度に詳細であると縛りが生まれるため、バランスを考慮していただきたい。 ● セルフチェックを想定した場合は、ベンダー側が評価できるように各資料の記載を修正する必要がある。 ● ペネトレーションテストについては、実施した項目や結果等、文書や記録の有無以外の評価も含められるとよい。 ● ペネトレーションテストの結果については、ユーザーの意向を考慮した上で、含められるとよい。 ● 内部にペネトレーションテストの優秀な技術者が在籍しているケースもあるため、第三者が実施した方がペネトレーションテストの内容が優れているとは限らない。内部の技術者による検証に加えて第三者による検証を実施することで、結果の信頼性が増す。 ● 製品仕様などの詳細項目確認は、オプションとして追加してもよいのではないか。
スコアリングに関する意見	● 詳細項目の点数であるスコア1と大項目の点数であるスコア 2 以外に、全体をまとめたスコア 3 があるとよい。 ● スコア 1 だけでなく、スコア 2 の重みづけも考えるべきである。例えば、7 つの大項目のうち、特に「②開発プロセスマネジメント（ECM）」を重視する、などのポリ

	シーがある場合にスコア 2 のレベルで重みづけができる。また、重みづけの考え方はユーザーによって異なる。 ● セキュリティ管理要件と脅威分析については重視できるとよい。 ● セキュリティ体制より機器自体の評価にもフォーカスを当てられるとよい。 ● スコア 1 のスコアリング方式が 0,1,2 の線形的なスコアになっている。非線形的なスコア(10, 30, 80 等)の方がより実態に近いのではないか。 ● スコアの改善状況についても評価できるとよいのではないか。例えば、初回の評価がやや低かった場合でも、2 回目の評価で改善されている点が見えるようになるとよい。
記載内容の修正に関する意見	● 「脆弱性情報」についてバランスを考慮したうえで、定義をいただきたい。 ● 「評価手順書」と「評価方法と妥当性判定基準」の関係性をわかりやすくするために、項番等を整理いただきたい。

3.2.1 評価方法と評価のスコアリング

評価手順書では、認証機関などの第三者が機器の検証・評価を行うことを想定し、下図の評価手順を含んだ構成とした。本調査の検討においては、このうち主に評価方法及び評価のスコアリングについて詳細に検討を行った。

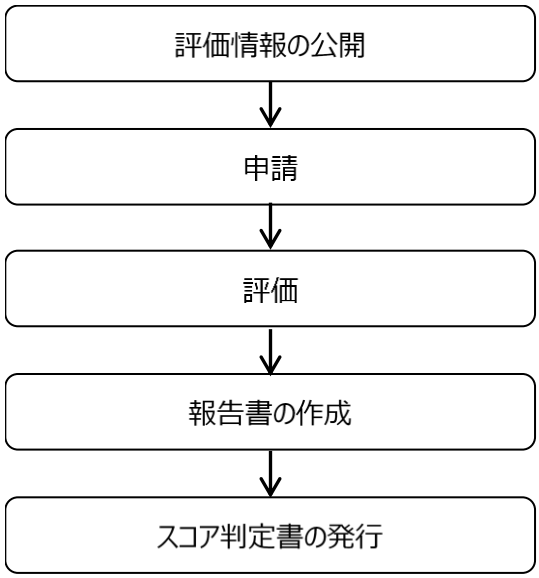


図 3-3 評価手順書で想定する評価手順のフロー

(1) 評価方法

評価方法では、既存の検証・評価等で用いられる、次の 3 つの手法を用いることとした。

① 受審者資料を参照する評価:
受審者の資料と記録により、プロセスの存在とプロセスの実施の確認を行う。

② 受審者へのインタビューによる評価：
受審者へのインタビューを実施して、プロセスの存在やプロセスの実施の確認を行う。

③ 実機確認による評価：
評価対象の実機を用いて、評価項目が実機に適切に反映されていることを評価する。

（2）評価のスコアリング

評価のスコアリングについては、次の 2 種類のスコアを付与することとした。

① 詳細項目ごとに付与するスコア（スコア1）

- 評価基準の詳細項目ごとに、各プロセス文書や定義文書、実施記録等によるエビデンスの有無による判定を基本とする。ただし、エビデンスが不十分な場合には、インタビュー等により情報を補足し、評価に活用する。
- 採点は次の基準に従い、評価項目ごとに 2,1,0 のスコアを付与する。検討の過程では NREL DERCF と同様に 5 段階等の多段階なスコアを検討したが、スコアの段階が増えることで評価者による評価点のブレが生じる可能性があったため、判断基準の明確化のために 3 段階とした。
  - スコア：2
    各評価項目に記載の各プロセス文書や定義文書があり、かつ実施記録がある
  - スコア：1
    プロセス文書があり、一部のプロセス実行のエビデンスはあるが、プロセスがすべて実施されたことを示すエビデンスが無い
  - スコア：0
    プロセス文書が無い 又は プロセス文書はあるが、実行されたエビデンスが無い

② 詳細項目に付与したスコア（スコア 1）に基づき、評価大項目ごとに付与するスコア（スコア2）

- 詳細項目ごとに付与するスコア（スコア 1）の獲得可能最大値を 100 とし、実際に獲得したスコア 1 の合算値の比率（「獲得度」と呼ぶ）から、以下の基準に従いスコアを付与する。
  - スコア：5
    獲得度が 80 を超える場合（最大は 100）
  - スコア：4
    獲得度が 60 を超え 80 以下である場合
  - スコア：3
    獲得度が 40 を超え 60 以下である場合
  - スコア：2
    獲得度が 20 を超え 40 以下である場合
  - スコア：1
    獲得度が 20 以下である場合

3.2.2 IEC 62443 に基づく評価手順の検討

評価手順の検討にあたっては、既存のガイドラインや標準を参考とした。特に、今回検討対象とした「②開発プロセスマネジメント(ECM)」「③製品・サービス仕様」「④開発環境」では、IEC 62443-4-1 及び IEC 62443-4-2 の内容を参考とした。

策定した評価手順書では、前段で策定した評価手順書の案における詳細評価項目のそれぞれに対して、「評価方法」「確認資料」「妥当性」の 3 つを具体的に記載した。

① 評価方法
評価基準を評価する具体的な手段

② 確認資料
評価するときに参照すべき資料の例

③ 妥当性
評価のスコアを定めるための指標

なお、評価方法や確認資料を検討する際に参考とした IEC 62443 関連のドキュメントを次に示す。

- IEC 62443-4-1 Ed. 1.0:2018
- IEC 62443-4-2 Ed. 1.0:2019
- IEC 62443-3-3 Ed. 1.0:2013
- SDLA-312-Sec-Dev-Lifecycle-Assess(v5_5)
- CSA-311-Functional-security-assessment-for-components-(v1_11)
- SSA-311-Functional-security-assessment-for-systems(v2_1)

3.3 実機を用いた模擬評価

策定した評価基準書及び評価手順書の案について、その妥当性を検証するために、実機を用いた模擬評価を実施した。評価対象には、国内で利用されている汎用の保護リレー1 機種(以下、「評価対象機器」という)を選定した。また、実機を用いた模擬評価にあたっては、評価対象機器の設計情報や脆弱性情報に触れる可能性があるため、模擬評価に関わる対象者を限定し、NDA を締結して実施した。

実機を用いた模擬評価は次のステップで実施した。以降ではその詳細を示す。

① 評価者による実機確認
② 被評価者によるセルフチェックシート作成
③ 評価者によるセルフチェックシート評価
④ 評価者による被評価者へのインタビュー
⑤ 評価者による評価報告書作成
⑥ 評価者及び被評価者による評価基準書・評価手順書への改善提案

3.3.1 評価者による実機確認

実機を用いた模擬評価を行うにあたり、評価者による実機確認を行った。

具体的には、被評価者から評価者に対して評価対象機器を貸し出し、評価者で実際に稼働させることで、評価対象機器がもつ機能等を事前に確認した。

3.3.2 被評価者によるセルフチェックシート作成

続いて、被評価者にて、評価手順書に基づいた評価のセルフチェックを行った。

具体的には、評価者側で用意したセルフチェックシートを被評価者に提供し、被評価者がセルフチェックシートに記入し、記入済みのセルフチェックシートを評価者に提出した。

セルフチェックシートには、評価手順書の評価項目ごとに、「確認結果」と「確認に用いた文書の名称等」を記載することとした。

3.3.3 評価者によるセルフチェックシート評価

続いて、被評価者から提出されたセルフチェックシートを用いて、評価者による評価を実施した。

具体的には、セルフチェックシートに記載された「確認結果」と「確認に用いた文書の名称等」を確認し、当該内容で十分評価できるか、不足している文書等がないかを確認した。

3.3.4 評価者による被評価者へのインタビュー

続いて、評価者による被評価者へのインタビューを実施した。

具体的には、セルフチェックシートの評価結果を用いて、確認結果に関する質疑や、不足している文書等の所在確認、文書等が不在の場合のプロセス実施の有無などを、評価手順書の評価項目ごとにインタビュー形式で確認した。

3.3.5 評価者による評価報告書作成

続いて、セルフチェックシートの評価及びインタビュー結果を踏まえて、評価基準書の各項目に対するスコア（スコア 1）及び、大項目毎のスコア（スコア 2）を判定し、それらを記載した「評価報告書」を作成した。

評価報告書は、評価機関による第三者評価の結果として利用可能な形式とし、被評価者にフィードバックを行った。

3.3.6 評価者及び被評価者による評価基準書・評価手順書への改善提案

最後に、実機を用いた模擬評価を通じて、評価者及び被評価者が感じた評価基準書・評価手順書に対する改善点について、取りまとめを行った。評価者及び被評価者から提示された主な改善提案を次表に示す。

表 3-5 実機を用いた模擬評価を通じた評価者及び被評価者から提示された主な改善提案

評価者	● 評価基準に ID と略称が欲しい。評価結果を「評価報告書」に記載する際、ID 又は ID+略称を利用すると見やすくなる。 ● 評価項目・方法に記載された用語(セキュリティモジュールなど)について，具体例などがあると分かりやすい。 ● 評価基準に「○○が文書化されている」という項目があるが、「文書化」をうたう評価基準は不要ではないか。 評価時にプロセスの存在やプロセスの実施記録を確認する際に、文書の存在は確認するため、文書化の有無を評価基準の項目にする必要はない。 ● 詳細評価項目のスコア(スコア 1)は、0,1,2 のほかに「n/a (non-applicable)」を追加した方が良い。 ● スコアを「0」とするか「評価対象外」とするかは、判定基準を可能な範囲で明確化した方が良い。 評価対象外とする基準を明確化すると、実施する評価項目数が事前に分かり、評価にかかる工数や費用を算出しやすくなる。 ● 詳細評価項目のスコアは 0,1,2 を付けるが、評価基準書に書かれる評価方法には、評価内容(プロセスが存在する、文書化されている、実施記録がある、など)ごとに「○△×」などで評価した方が分かりやすい。 ● 評価基準のうち、「外部環境との接続、外部コンポーネント利用ルールを定めている 」について、今回はサプライチェーンの視点での評価手法を考えたが、「④開発環境」の外部接続を考える場合、ISO/IEC 27000 との関係を含めて考える必要があるのではないか。 ● IEC 62443-4-1 における「サードパーティでカスタム開発させるときのセキュリティルール(SM-10)」も、評価基準書の評価基準に含むべきではないか。 ● 評価項目毎に、過去の評価例(理由付き)があると、新たな機器を評価するときの手間の削減や、評価のばらつきの抑制に繋がる。 ● 評価機関などが第三者評価を行う場合、事前に評価項目に関して被評価者に説明し問い合わせ対応を行う。本評価スキームでも実際の評価の前段でそのような説明を行う機会を検討した方がよい。
被評価者	● 評価手順書に基づく実機評価(インタビュー)において、開発プロセス関連の質問と、仕様に関する質問が散逸していたため分かりにくかった。質問の適切なグルーピングが必要と感じた。 ● 実機評価時に事前に準備するものが不明瞭だった。慣れていないため、事前準

	備に手間取った。ドキュメントリストや開発計画書、規定類など準備物のヒントを、手順書の注に入れておくとよい。 ● 被評価者は、IEC 62443 や ISCI 等の認証に慣れていないことが想定されるため、事前に関連規格や審査概要などのレクチャーが必要だと感じた。 ● スコアカードの使い方について、購買者が重視したい点をはっきりさせる工夫（例：レーダーチャートで示す、など）が必要。 ● 評価対象機器（保護リレー、等）に限定すると、例えば悪意による操作をされにくくするのであれば、当該機器自体には高性能なセキュリティ対策は不要（機器の外部で対策を実施する、など）と考えられる。そのような業界でのコンセンサス作りが重要。

3.4 今後の課題

本事業では、過年度に策定した詳細評価項目を具体化し、7 つの評価大項目のうち「②開発プロセスマネジメント（ECM）」「③製品・サービス仕様」「④開発環境」の 3 項目について、評価基準書及び評価手順書の案を策定した。また、策定した評価基準書・評価手順書の案の一部の評価項目について、実機（保護リレー）を対象とした模擬評価を実施し、評価の基準や手順の妥当性などを確認した。

今後取り組むべき残された課題として、以下が考えられる。

- 「①組織全体」「⑤SCM 上流」「⑥生産設備」「⑦SCM 下流」の評価基準書、評価手順書を策定する。
  特に、サプライチェーンに対するサイバーセキュリティ対策要件となる⑤⑥⑦については、米国を中心とした海外での取り組みが急速に進んでいるため、それらの取り組みにおける知見を活用して、評価基準書、評価手順書の具体化を行うことが考えられる。
- 実機を用いた模擬評価について、評価基準書、評価手順書の妥当性を検証し、汎用性を高めるためには、複数の実機を対象とした模擬評価を行う必要がある。

なお、実証終了後の勉強会や、勉強会メンバーや有識者へのヒアリングで出された意見等を踏まえ、今後の取り組み時に検討すべき論点を以下に示す。

3.4.1 スコアリングについて

（1） スコアの重みづけについて

評価手順書案では、詳細評価項目毎のスコア（スコア 1）と、それを集計した 7 つの大項目毎のスコア（スコア 2）の付け方を示しており、重みづけについては評価結果の利用者（電力会社など）が別途実施することを想定した。具体的には、評価結果をデータベース等で保管し、重みづけを利用者が設定できるツール等の提供を想定した。

一方、本評価スキームにおける標準的な重みづけの考え方（例えば、セキュリティ管理要件や脅威分

析を重視する、「③製品・サービス仕様」を重視する、サプライチェーンを重視する、など）を示すことも有用だと考えられる。そうした標準的な重みづけは、国内のユーザーとベンダーが合意できるものを示すことが望ましい。

（2） 非線形的なスコアについて

評価手順書案では、詳細評価項目ごとのスコア（スコア 1）は線形（0,1,2）としたが、評価項目ごとに異なる非線形なスコア（0～100で等間隔でない配点）を設定することも考えられる。例えば、特定の詳細評価項目において（10, 30, 80）の 3 段階とすることで、非適合の場合にスコアを大きく落とすことも可能となる。

（3） スコアの改善状況の見える化について

スコアカード方式では動的にスコアが変わるが、例えば初回の評価時にスコアが低かった場合でも、2 回目以降でスコアが改善している状況がわかるようにする運用も検討すべきである。スコアの改善状況を確認できるようにするために、評価結果をデータベース等で保管し、過去からのスコアの変遷や改善点が確認できるツールを提供することが想定される。

ただし、そうしたスコアの見える化を図る場合は、スコア開示の可否（誰が閲覧できるか）について、ベンダー側で管理できるようにする必要がある。

また、改善状況の見える化は、評価制度の運用によって要件が変わることが想定される。スコア開示の可否や運営について、公的機関が実施するのか、あるいはセルフチェックにするのか等の検討を行ったうえで、改善状況の見える化に関して検討を進めるべきである。

3.4.2 評価方法について

（1） セルフチェックを想定した記載内容について

評価手順書案は、評価機関などの第三者が評価することを意識して記載した。一方、評価の専門家ではないベンダー自身によるセルフチェックを意識すると、手順などをより具体的に記載する必要がある。

なお、本評価スキームは、合否で判断しないスコアリング制度を目指しており、被評価者の成熟度が求められている。そのため、評価項目を過度に概要化すると、特にセルフチェックでは評価が困難となるおそれがある。

（2） ペネトレーションテストの実施項目や評価について

評価手順書案では、ペネトレーションテストについても、ベンダー側で実施しているプロセスの有無（文書化）と、実施エビデンスの有無で評価を行うことを想定した。一方、特にペネトレーションテストに関

しては、実施している試験項目やその結果（脆弱性の有無等）が重要とも考えられる。

ペネトレーションテストの項目については、ユーザーとベンダーの間で合意が取れた項目を示すことが望ましい。ただし、製品単体に対するペネトレーションテストでは、製品の細かな設計を理解していないユーザー側で試験項目を設定することは難しい。また、ペネトレーションテストを実施しているプロセスの有無よりも、その結果として脆弱性が管理できていることをユーザー側では重要視することが想定される。製品の細かな設計を理解しているベンダー側で設定したペネトレーションテストの評価項目に対して、大枠の項目だけでもユーザー側と合意が取れることが望まれる。

また、ユーザー側では、製品単体ではなくシステムに対するペネトレーションテストの項目であれば設定可能だろう。システムに対するペネトレーションテストの項目はユーザーとベンダーの間で合意が取りやすいが、製品に対する評価制度を目指す本評価スキームのスコープ外となる点に注意が必要である。

（3） ペネトレーションテストの評価者の力量について

評価手順書案では、第三者によるペネトレーションテストを重視している。一方、ベンダーが社内で実施している場合でも、一定レベルの評価は十分に可能との考え方もある。ベンダー側でセルフテストを実施した場合に、テスト実施者のレベルを評価する方法（例：テスターの資格や経験、評価結果内容の確認、など）を検討する必要がある。

第三者認証を実施する際にも、評価者の力量によって評価にかかる工数やコストが変わってくることも想定される。少ない工数やコストでの第三者認証を目指す場合、審査する組織における評価者の力量について考慮し、必要に応じて本評価スキームの中で教育を実施するなども検討すべきである。

加えて、第三者の意義も明確にすべきだろう。品質の良し悪し以外に、ベンダーでは第三者認証をマーケティングの観点で取得しているケースが多い。こうした観点を含めて整理しないと、第三者認証の要否の議論に、マーケティングとセキュリティの話題が混ざってしまうおそれがある。

評価結果に関しては、セルフチェックによる評価結果、認証団体による評価結果、認証団体が認めた機関による評価結果、などを区別して示す必要がある。また、いずれの評価結果も、ユーザーとベンダーの間でのリスクコミュニケーションで利用することも想定して検討することが望ましい。

3.4.3 実機を用いた模擬評価について

（1） 被評価者に対する事前説明について

既存のセキュリティ認証制度において評価機関などが第三者評価を行う場合、事前に評価項目に関して被評価者に説明し、問い合わせ対応を行う場合が多い。被評価者がセキュリティ認証制度に慣れていないケースでは、関連する標準規格や、評価プロセスなどの説明を実施することが望ましい。

本評価スキームにおける実機を用いた評価においても、実際の評価の前段でそのような説明を行う機会を検討した方がよい。

（2）インタビュー実施時の留意点について

今年度の実機を用いた模擬評価では、セルフチェックシートを用いた評価ののち、評価者による被評価者へのインタビューを行った。この際、評価基準書案の項目に沿って質疑を行ったが、開発プロセス関連の質問と、製品仕様に関する質問が混在しており、被評価者からわかりにくかったとの指摘が出た。

今後インタビューを行う際には、セフルチェックシートを分析し、被評価者が回答しやすい質問構成（順序など）をインタビュー前に検討し、評価者がテストプランとして作成することが望まれる。質問する順序については、例えばインタビューに対応する被評価者部署やメンバーでグルーピングしたり、組織内のプロセスの確認と製品に対する実施記録の確認を分ける、などが考えられる。

（3）実機評価にかかる工数やコストについて

本評価スキームでは、既存のセキュリティ評価よりも少ない工数やコストで、製品に対する評価が効率的・効果的に実施できることを目標としている。そこで、模擬評価を通じて、工数やコストがどの程度かかるのかを確認し、評価基準や評価手順の妥当性や項目数の削減を検討する必要がある。

また、工数やコストの削減について、既存の認証制度による代替を検討し、そのような認証を取得している際に、本評価スキームの工数やコストが削減できるようにすることが望まれる。

3.4.4 その他の検討すべき点について

（1） 認証の対象や再認証の要否について

本評価スキームでは機器を対象とした評価・認証を目指しているが、認証を実施する対象について、今後改めて検討する必要がある。例えば、評価を機種ごとに実施するのか、あるいは同一ベンダーで設計・製造やサプライチェーンが同様の機種をまとめて取り扱うことができるようにすべきか、などが検討のポイントである。

また、ソフトウェア更新などがあった場合に、機種ごとに都度再認証が必要とするか否かについても検討が必要である。ソフトウェア更新毎に再認証を実施すると、評価コストが高くなることに加えて、脆弱性対策などのソフトウェア更新頻度を下げるような悪影響も想定される。

例えば、マネジメントの観点でソフトウェア更新の管理について評価することで、ソフトウェア更新ごとの再認証を代替できる可能性がある。また、評価項目の中には、製品ごとに変わる項目と、組織ごとに変わる項目があるため、それらを区別したうえで検討できるとよいだろう。

（2）組織やプロセスに偏らない評価について

評価手順書案では、文書化や実施記録などの組織やプロセスに重点を置いた評価とした。一方、ペネトレーションテストについては、プロセスのみならず、実施内容やテスト結果も評価すべきである。組織やプロセスに偏らない評価として、例えば「③製品・サービス仕様」の評価基準として、オプション（加点要

素）として実施内容やテスト結果などを評価することも考えられる。

製品の機能やプロセスの内容に踏み込んだ評価を考慮した場合、評価者による評価のブレや、評価にかかる工数やコストの増大を抑える対策についても、合わせて検討すべきである。

（3） 認証制度・スキームについて

本認証スキームでは、セルフチェックと第三者認証を組み合わせることを想定して検討を進めてきた。また、すでに既存の認証制度があるものはそれらを活用する（例えば「①組織全体」についてはCSMC/ISMS 等を活用）ことを想定している。今年度の評価基準・評価手順の検討にあたっては、セルフチェックと第三者認証の双方が実施可能となるよう、より厳格な対応が求められる第三者認証が可能な形式で整理を進めた。

今後、さらに検討を深めるためには、具体的な認証制度やスキームの検討を進めて、認証・評価の結果の活用方法等の明確化が求められる。特に、ユーザー（アセットオーナー）による調達を想定し、調達要件で重要視される項目を重点的に評価するような仕組みが必要だろう。

サプライチェーンの管理の 1 つとして、SBOM に関する議論が国内外で活発化している。SBOM で収集された情報の管理についても議論が行われているなか、本評価スキームでソフトウェアに関する評価を行うのであれば、SBOM を含めて情報を共通管理することも検討する必要がある。

また、本評価スキームの中で脆弱性管理を行いながら、各事業者に脆弱性情報を通知することも想定できる。製品の評価に加えて、社会設計や事故対応につなげる活動についても検討する必要がある。

（4） セキュリティ評価機関の拡充について

本認証スキームでは、中立的な評価機関を含めたエコシステムを構築する必要がある。セキュリティ認証が普及するエコシステムを構築するために、安定した母体をもつ評価機関に対応可能な人材がいることが望ましい。また、評価機関に対して認証制度の評価方法に関する教育を実施できるとよい。

（5） 暗号鍵管理、バックアップデータの暗号化について

評価手順書案では、「③製品・サービス仕様」において、暗号化に関する要件に対する評価方法の案を示した。一方、暗号化に関するセキュリティ要件を検討する際は、暗号鍵管理などの運用フェーズにおける考慮も重要である。また、バックアップデータに関する要件に対する評価方法の案も示したが、運用フェーズにおけるバックアップデータの暗号化についても考慮する必要がある。

これら、運用フェーズでの取り組みと合わせてセキュリティ対策が可能となる項目については、「⑦SCM 下流」にて運用・保守に対する要件を検討する際に、「③製品・サービス仕様」で示した評価方法との整合性に留意することが望まれる。

（6） 経済安全保障との連携について

経済安全保障についての法案が検討されている中、サプライチェーンの要素も法案に含まれている。今後、検討範囲をサプライチェーンに広げる際は、国内で検討中の経済安全保障の法案等の動向を注視しながら、様々なステークホルダーと連携して取り組みを進めることが望まれる。

4. インド太平洋地域向け日米 EU 産業制御システムサイバーセキュリティウィークの開催

電力分野におけるセキュリティ検証のあり方やセキュリティ規制・基準のあり方について、欧米やインド太平洋諸国との国際的な議論をワークショップ形式で行うことで、電力分野におけるセキュリティ政策について米 EU 等の動向を把握するとともに、我が国の政策との国際調和を図ることを目的に、エネルギーセクター・サイバーセキュリティワークショップを 2021 年 10 月 27 日から 29 日の3日間にわたりオンライン形式で開催した。なお、2021 年 10 月 25 日から 26 日に開催された産業サイバーセキュリティセンター(ICSCoE)主催のハンズオントレーニングとあわせ、全体としては「インド太平洋地域向け日米 EU 産業制御システムサイバーセキュリティウィーク(以下、サイバーセキュリティウィーク)」として、全5日間のプログラムとして実施している。

4.1 開催概要

サイバーセキュリティウィークは、経済産業省、ICSCoE、米国の CISA(Cybersecurity and Infrastructure Security Agency)、欧州委員会の DG CONNECT(Directorate-General for Communications Networks, Content and Technology)が協力し、インド太平洋地域における産業制御システム(ICS)サイバーセキュリティに焦点を当てた 1 週間のオンライントレーニングプログラムである。

この演習は、インド太平洋地域からの参加者の ICS サイバーセキュリティ能力を向上させることを目的としており、今回で 4 回目を迎える。重要インフラ事業者の OT/IT サイバーセキュリティ専門家、各国 CSIRT のサイバーセキュリティ専門家、関係省庁の政策専門家が参加しており、インド太平洋地域からの参加者は、日米欧の専門家からエネルギー分野を含むサイバーセキュリティに関する様々なトピックを学び、参加者がそれぞれの経験や見解を共有するユニークで貴重な機会を得ることができるものとなっている。

全体プログラムの構成を下表に示す。

表 4-1 全体プログラムの構成

(1) セレモニアルセッション
- オープニングセレモニー(開会の辞・基調講演)
- クロージングセレモニー
(2) 日米 ICS サイバーセキュリティトレーニング
- ICSCoE によるハンズオントレーニング
- INL と ICSCoE によるリスクアセスメントワークショップ
- INL と ICSCoE による人材育成ワークショップ
(3) ICS サイバーセキュリティセミナー
- プロセスオートメーションセクターセミナー
- 電力セクターセミナー
- 政策・標準化セミナー

- サプライチェーンリスクマネジメントセミナー

4.1.1 サイバーセキュリティウィークの参加者

サイバーセキュリティウィークの主な招聘参加者（受講者）は、インド太平洋地域（ASEAN 加盟国、インド、バングラデシュ、スリランカ、モンゴル、台湾）の招聘機関から適任者の推薦をうけた 40 名である。参加者はそれぞれインド太平洋地域の重要インフラ事業者や、国の CSIRT における OT（Operational Technology：制御技術）・IT（Information Technology：情報技術）のサイバーセキュリティ担当者、関連する政府機関における政策担当者などであった。

また、セミナーセッションに関しては、ICSCoE の中核人事育成プログラムの研修生の他、日本、米国、欧州、インド太平洋地域の有識者等、約200名がオーディエンスとして受講のみの枠で参加している。

4.2 プログラムの概要

プログラムのタイムテーブルを以下に示す。なおタイムテーブルは日本時間で示しているため、時差の関係でインド太平洋地域の各地では毎日の開始時間から次のような読み替えが必要である。

午前 11 時（UTC+9）	日本
午前 10 時（UTC+8）	ブルネイ、マレーシア、モンゴル、フィリピン、シンガポール、台湾
午前 9 時（UTC+7）	カンボジア、インドネシア（ジャカルタ）、ラオス、タイ、ベトナム
午前 8 時（UTC+6）	バングラデシュ
午前 7 時 30 分（UTC+5:30）	インド、スリランカ

表 4-2 プログラムのタイムテーブル（＊表示は日本時間）

1 日目 ： 10 月 25 日（月）	
11:00-11:30	受付
11:30-12:30	プレオープニングセッション
12:30-13:00	ショートブレイク
13:00-15:00	J202R (1)
15:00-16:00	ロングブレイク
16:00-17:30	J202R (2)
17:30-18:00	ショートブレイク
18:00-19:30	ネットワーキング・セッション

2 日目 ： 10 月 26 日（火）	
11:00-11:30	受付
11:30-13:00	J202R(3)
13:00-13:30	ショートブレイク

13:30-15:00	J202R(4)
15:00-16:00	ロングブレイク
16:00-17:30	J202R(5)
17:30-18:00	ショートブレイク
18:00-19:30	J202R(6)

3 日目 ： 10 月 27 日(水)	
11:00-11:30	受付
11:30-12:30	開会の辞・基調講演
12:30-13:00	ショートブレイク
13:00-15:00	プロセスオートメーションセクターセミナー
15:00-16:00	ロングブレイク
16:00-17:30	電力セクターセミナー(1)
17:30-18:00	ショートブレイク
18:00-19:30	電力セクターセミナー(2)

第 4 日目 ： 10 月 28 日(木)	
11:00-11:30	受付
11:30-13:00	リスクアセスメントワークショップ(1)
13:00-13:30	ショートブレイク
13:30-15:00	リスクアセスメントワークショップ(2)
15:00-16:00	ロングブレイク
16:00-17:30	政策・標準化セミナー(1)
17:30-18:00	ショートブレイク
18:00-19:30	政策・標準化セミナー(2)

第 5 日目 ： 10 月 29 日(金)	
11:00-11:30	受付
11:30-13:00	人材育成ワークショップ(1)
13:00-13:30	ショートブレイク
13:30-15:00	人材育成ワークショップ(2)
15:00-16:00	ロングブレイク
16:00-18:00	サプライチェーンリスクマネジメントセミナー
18:00-18:30	ショートブレイク
18:30-19:30	クロージングセレモニー

4.3 各セッションの概要

4.3.1 プレオープニングセッション／Pre-Opening Session

サイバーセキュリティウィークの開始にあたって、イベント全体についての説明等が行われた。

- 司会者挨拶、サイバーセキュリティウィークに関係するプロジェクトチーム紹介。
- インド太平洋地域からの各参加者による簡単な自己紹介。
- 5 日間のプログラム概要の説明。
- ICSCoE とその訓練施設についての紹介、バーチャルツアー。

4.3.2 ネットワーキング・セッション／Networking Session

インド太平洋地域からの参加者同士のコミュニケーションを高めるため、参加者をいくつかのグループに分け、グループ内で各自簡単な自己紹介を実施した。

4.3.3 日米 ICS サイバーセキュリティトレーニング（J202R, ハンズオン）／JP-US ICS Cybersecurity Training for the Indo-Pacific Region, （J202R Remote Hands-on）

本トレーニングは以下を目的として開催された。

- 簡易な ICS テストベッドを用いた ICS サイバーセキュリティの基礎知識・技術の習得。
- ICS サイバーセキュリティに関するベストプラクティス、ガイドライン、教訓についてのグループディスカッション。
- ICS 環境におけるセキュリティ対策に関する課題を共有。

プログラムはリモートハンズオントレーニングにより実施され、6 つのスロットで構成されている。インド太平洋地域からの参加者は、10 個の小グループ（1 グループあたり参加者 4 名＋日本人ファシリテーター1 名）に分けられ、小グループ単位での演習を中心に実施された。

4.3.4 開会の辞・基調講演／Opening Remarks and Keynote Speech

主催者を代表して、日米欧の各関係組織より開会挨拶（ビデオメッセージ）があった。また、基調講演が行われた。

（1） 講演者一覧

表 4-3 開会の辞・基調講演の講演者一覧

開会挨拶	● 細田 健一、経済産業副大臣 ● Mr. Eric GOLDSTEIN, Executive Assistant Director for Cybersecurity, U.S. Department of Homeland Security,

	Cybersecurity and Infrastructure Security Agency (DHS/CISA) ● Mr. Raymond F. GREENE, Chargé d'Affaires ad interim, U.S. Embassy Tokyo ● Ms. Lorena BOIX ALONSO, Director in the European Commission's Directorate-General for Communications Networks, Content and Technology, Directorate H: Digital Society, Trust and Cybersecurity, Directorate - General for Communications Networks, Content and Technology (DG Connect), European Commission
基調講演	● "Threat Landscape of Industrial Cybersecurity," Mr. Robert M. LEE, CEO and Founder, Dragos

4.3.5 プロセスオートメーションセクターセミナー／Process Automation Sector Seminar

プロセスオートメーション分野は、ICS サイバーセキュリティの先進的な産業の一つである。国際オートメーション学会(ISA)が設立され、ICS サイバーセキュリティ規格(ISA99)を策定し、これが一般的な ICS の国際規格(IEC62443)となっている。急速なデジタル化や新たな ICS の脅威(Triton など)に伴い、政府の取り組みではなく、エネルギー業界全体の取り組みが推進されてきたことは特筆すべきことである。

これらの状況を踏まえ、本セミナーは以下を目的に開催された。

- プロセスオートメーション分野(石油、ガス、化学プラントなど)の ICS サイバーセキュリティを確保するための日米欧の取り組みの現状の確認。
- 政策レベル、産業レベルにおける課題とベストプラクティスの紹介。
- 将来のサイバーセキュリティの取り組みのために、プロセスオートメーション部門における調和と協力の可能性を紹介。

(1) 講演者一覧

表 4-4 プロセスオートメーションセクターセミナーの講演者一覧

モデレーター	Mr. Marty EDWARDS, Vice President, Operational Technology Security, Tenable
講演者及びタイトル	1. "The Only Viable Thing to Do: Security Program- ISA/IEC 62443," Mr. Akiomi MONDEN, Head of System Integration Technology Centre, Yokogawa Electric International Pte Ltd 2. "The Carrot or the Stick? Ways between Best Practices and Regulation Towards Better OT Security," Mr. Jens WIESNER, Team Lead for Industrial Control and Automation Systems, Federal Office for Information Security, BSI, Germany

	3. “IEC 62443,” Dr. Kai WOLLENWEBER, Digital Industries, Strategy & Technology, Cybersecurity, Siemens AG 4. “Industrial Control Systems (ICS) Security”, Mr. Alex RENIERS, Section Chief, Industrial Control System Section, Cybersecurity Division/Threat Hunt, CISA

4.3.6 電力セクターセミナー(1)／Electricity Sector Seminar 1

従来の電力部門は最も重要な重要インフラの一つであり、そのため、悪意ある行為者は電力部門を混乱させる良いターゲットとして認識している。また、送電網のデジタル化により、再生可能エネルギーの導入が進んでいるが、サイバー攻撃には脆弱なままである。政府はそれぞれ、この分野を保護するためのサイバーセキュリティ政策と規制の枠組み／ガイダンスの策定に取り組んでいる。これらの取り組みには産業界の積極的な参加が必要であり、安全で信頼できる機器を調達することで、新たな ICS の脅威に対するサイバーセキュリティ能力を強化することができる。

これらの状況を踏まえ、本セミナーは以下を目的に開催された。

- バルク発電や送電・配電などの伝統的な電力セクターにおける、ICS サイバーセキュリティを確保するための日本、米国、EU の現在の取り組みについてのレビュー。
- 政策レベル、セクターレベル、個々の企業レベルでの課題、教訓、ベストプラクティスの紹介。
- 将来のサイバーセキュリティの取り組みのために、伝統的な電力セクターにおける調和と協力の可能性の提示。

(1) 講演者一覧

表 4-5 電力セクターセミナー(1)の講演者一覧

モデレーター	Mr. Tom WILSON, Senior Vice President and CISO, Southern Company
講演者及びタイトル	1. “OT Security Focus Across Operations,” Mr. Tom WILSON, Senior Vice President and CISO, Southern Company 2. “Effective Cybersecurity and Supply Chain Controls,” Mr. Tim ROXEY, President, Eclectic Technology 3. “The Approach to Cyber Security Measures of Chubu Electric Power Grid,” Mr. Hiroyuki HASEGAWA, Assistant Manager, PG-CSIRT Cybersecurity Evangelist/Specialist, Chubu Electric Power Grid Co., Inc. 4. “Network Code as ENTSO-E Contribution to Improve Grid Cyber Resilience,” Mr. Grzegorz BOJAR, Vice Chair of the Digital committee, ENTSO-E

4.3.7 電力セクターセミナー(2)／Electricity Sector Seminar 2

二酸化炭素排出量削減のため、世界中で再生可能エネルギーが推進されている。再生可能エネルギーの急激な増加やエネルギー・リソース・アグリゲーション・ビジネス(ERAB)の拡大により、相互接続の増加等によるサイバーセキュリティリスクが高まっている。この分野では、サイバーセキュリティの政策的な取り組みは、従来の電力セクターほど成熟していない。

これらの状況を踏まえ、本セミナーは以下を目的に開催された。

- 再生可能エネルギー管理に関する日本、米国、EU の電力セクターの取り組みを、ICS サイバーセキュリティと関連づけながらレビュー。
- 政策レベル、セクターレベル、個々の企業レベルでの課題とベストプラクティスの紹介。
- この分野での改善と調和の可能性を確認し、今後の推奨経路を紹介。

(1) 講演者一覧

表 4-6 電力セクターセミナー(2)の講演者一覧

モデレーター	Mr. Daisuke HOSHI, Director for International Affairs, Cybersecurity Division, METI
講演者及びタイトル	1. “Security Recommendations for Distributed Energy System Aggregators, Based on METI Cyber and Physical Security Framework,” Dr. Masaki UMEJIMA, Associate professor in Cyber Civilization Research Center, Keio University 2. “Securing Grid Decarbonization by Design,” Dr. Jonathan WHITE, Director of Cybersecurity Program Office, National Renewable Energy Laboratory (NREL) 3. “Cyber Security Challenges and Trends in Renewable Generation,” Mr. Jason HOLLERN, Program Manager: Cyber Security for Generation Assets, Electric Power Research Institute (EPRI) 4. ”Cyber Security Risk Management in Enel,” Mr. Yuri RASSEGA, CISO, Enel Group

4.3.8 リスクアセスメントワークショップ／Risk Assessment Workshop

以下を目的とするワークショップを実施した。プログラムは講演とグループワークで構成され、講演内容は表に示す通りである。

- 重要システムのサイバーリスク評価における結果主導のアプローチの理解。
- 事例をもとに、重要な機能、ビジネス上の影響を特定。
- ICS リスク評価に関する米国のフレームワークと日本のガイドラインの理解。

（1） 講演者一覧

表 4-7 リスクアセスメントワークショップの講演者一覧

モデレーター	Mr. Andrew BOCHMAN, Senior Grid Strategist, INL Dr. Tomomi AOYAMA, ICSCoE Advisor
講演者及びタイトル	1. “Engineering out the Cyber Risk, Scaling Consequence-driven Cyber-informed Engineering (CCE),” Mr. Andrew BOCHMAN, Senior Grid Strategist, INL 2. “Risk Assessment Guide for Industrial Control System,” Mr. Yutaka TAKAMI, Chief Researcher, Vulnerability Countermeasures Group, IT Security Countermeasures Dept., IT Security Center, Information-technology Promotion Agency

4.3.9 政策・標準化セミナー／Policy and Standardization Seminar

デジタル技術とネットワークは、経済の繁栄と社会の幸福に不可欠である。また、新しいデジタルソリューション（特に 5G と IIoT）は、重要なインフラにおけるデジタル変革に有益である。Covid-19 の大流行により、このことはさらに明白になった。同時に、サイバーセキュリティの脅威が急速に増加している。したがって、重要インフラのサイバーセキュリティは、経済、国民、社会、そして我々の価値を守るために、これまで以上に重要かつ戦略的になっている。サイバーセキュリティ（ICS サイバーセキュリティを含む）に関する包括的な政策の策定は、日本、米国、EU の公的機関の継続的な優先事項であり、現在も継続している。また、国際標準の策定は、サイバーセキュリティ（ICS サイバーセキュリティを含む）に関する堅実かつ効率的な政策の不可欠な部分である。最後に、国際協力と経験とベストプラクティスの交換は、これらのサイバーセキュリティの枠組みを強化するための鍵である。

これらの状況を踏まえ、本セミナーは以下を目的に開催された。なお、本セミナーは前半をセミナー講演、後半をパネルディスカッションとする 2 部制で実施された。

- 日本、米国、EU のサイバーセキュリティアプローチを成功させるための政策と規制の選択肢を提示（ICS に若干の焦点を当てる）。
- サイバーセキュリティを成功させるためのグローバルな標準化の必要性の提示。

（1） 講演者一覧

表 4-8 政策・標準化セミナーの講演者一覧

モデレーター	Ms. Karolina Angela KOZLOWSKA, DG CONNECT
講演者及びタイトル	1. “Building the Joint Cyber Unit”, Mr. Jakub BORATYŃSKI, Deputy Director of Directorate CNECT H, Digital Society, Trust and Cybersecurity, DG CONNECT 2. “Creating a rulebook for cybersecurity in international electricity exchanges”, Mr. Felipe Castro BARRIGON, Policy Officer- Energy Security and Safety, Directorate-General for

	Energy (DG ENER) 3. “Control Systems Cybersecurity Performance Goals”, Mr. Peter COLOMBO, Senior Advisor, Cybersecurity Division, CISA 4. “ METI’s Industrial Cybersecurity Initiatives”, Mr. Daisuke HOSHI, Director for International Affairs, Cybersecurity Division, METI
パネリスト	1. Mr. Xavier PIEDNOIR, InDiCo Program Manager, European Telecommunication Standards Institute (ETSI) 2. Mr. Koji NAKAO, Distinguished Researcher, Cybersecurity Research Institute, National Institute of Information and Communications Technology (NICT) 3. Ms. Amy MAHN, International Policy Specialist; Program Coordinator for the Cybersecurity Framework, National Institute of Standards and Technology (NIST)

4.3.10 人材育成ワークショップ／Workforce Development Workshop

以下を目的とするワークショップを実施した。プログラムは講演とグループディスカッションで構成され、講演内容は表に示す通りである。

- ICS 人材育成のための日米のフレームワーク/アプローチの共有。
- ICS 人材育成の課題、教訓、ベストプラクティスについての議論。
- 組織内のコンピテンシーをどのように測定し、管理するかの理解。
- 人材育成に関連するガイドラインや手順の改善と調和を図るための領域の特定。

(1) 講演者一覧

表 4-9 人材育成ワークショップの講演者一覧

モデレーター	Dr. Shane D. STAILEY, Senior Industrial Control Systems Cybersecurity Professional, Training Development and Strategy Lead, INL Dr. Tomomi AOYAMA, ICSCoE Advisor
講演者及びタイトル	1. “Workforce Frameworks & Organizational Competency” Dr. Shane D. STAILEY, Senior Industrial Control Systems Cybersecurity Professional, Training Development and Strategy Lead, INL 2. “Guidebook for Establishing Cybersecurity Systems and Securing Necessary Human Resources,” Ms. Yu INOSE, Deputy Director, Cybersecurity Division, METI

4.3.11サプライチェーンリスクマネジメントセミナー／Supply Chain Risk Management Seminar

ICS のサプライチェーンリスクマネジメント（SCRM）は、近年、国際的なパートナーの間で大きな問題の一つとなっている。COVID-19 時代におけるデジタル化の推進は、SCRM のサイバーセキュリティリスクを高めるため、日米欧の政府や業界団体はそれぞれ、リスクを軽減するためのサイバーセキュリティガイドラインや製品・ソリューション認証を策定しようとしている。

これらの状況を踏まえ、本セミナーは以下を目的に開催された。

- 日本、米国、EU における、現在の脅威の状況や ICS SCRM についての政策面の考え方のレビュー。
- 政府や産業界によるサイバーセキュリティへの取組や対策についての確認。
- SCRM 関連活動の改善と調和の可能性についての確認。

（1） 講演者一覧

表 4-10 サプライチェーンリスクマネージメントセミナーの講演者一覧

モデレーター	Mr. Daisuke HOSHI, Director for International Affairs, Cybersecurity Division, METI
講演者及びタイトル	1. “What Is Supply Chain Risk Management?”, Mr. Hiroshi SASAKI, ICSCoE Advisor (Fortinet) 2. “The RRI’s Industrial Supply Chain Security Questionnaire for Trustworthiness Evaluation,” Ms. Ayaji FURUKAWA, Member of Industrial Security Action Group, Robot Revolution & Industrial IoT Initiative (RRI) (Toshiba Corporation) 3. “Supply Chain Integrity – An Old Problem with Great Future – The EU Approach,” Dr. Evangelos OUZOUNIS, Head of Policy Development and Implementation Unit, European Union Agency for Cyber Security (ENISA) 4. “Control Systems Supply Chain Risk Management,” Ms. Jennifer W. PEDERSEN, Senior Technical Advisor to the National Risk Management Center (NRMC), DHS/CISA 5. “A Red Team Approach in SCRM, Under Recognized Risks and Real-World Examples”, Mr. Terry MCCORKLE, prior DoD Red Team Member and ICS Vulnerability Researcher, and Founder and CEO of PhishCloud, Inc.

4.3.12 クロージングセレモニー／Closing Ceremony

まず、インド太平洋地域から本イベントに参加し、全課程を修了した者に対して、修了証の授与式が行

われた（全員オンライン参加のため、後日別途送付）。次に主催者を代表して、日米 EU の各関係組織より閉会挨拶（ビデオメッセージ）があった。続いてインド太平洋地域からの参加者の代表による挨拶が行われ、イベントを閉会した。

（1） 講演者一覧

表 4-11 クロージングセレモニーの講演者一覧

閉会挨拶	● 遠藤信博、産業サイバーセキュリティセンター センター長、IPA ● Mr. Zachary TUDOR, Director of National & Homeland Security Directorate, INL ● Mr. Juhan LEPASSAAR, Executive Director, European Union Agency for Cybersecurity (ENISA)
参加者代表挨拶	● the representatives from Critical Infrastructure Operator ● the representatives from National CERT ● the representatives from Government Agency

4.4 プログラムの総括

プログラム全体を通じ、日米 EU の官民の専門家から、プロセスオートメーションに関する国際標準（IEC62443 規格等）についての内容や関連した取組、電力系統に関する規則体系の策定を含めた政策や民間における取組、再生可能エネルギー分野に関する政策やベストプラクティス、産業制御システムに対するリスク評価の方法、サイバーセキュリティ確保に向けた政策や標準化プロセス、サプライチェーンの安全確保のための政策的取組や国際連携などについて、様々な情報共有や解説が行われた。いずれについても、日米 EU の最新の取組についての情報が得られたとともに、インド太平洋地域からの参加者にとっては産業制御システムに関する世界の最先端の取組に触れる機会となり、非常に高い満足度を得る結果となった。さらに個別の知識習得だけでなく、国際間での人脈づくりにも役立つ結果となり、今後の継続的な連携にも多くの期待が寄せられた。

本プログラムはインド太平洋地域における産業制御システムサイバーセキュリティの確保に向けた主導的人材の育成に貢献するものであり、参加者が今回の経験をそれぞれの国に持ち帰り今後の対策を主導していくことで、インド太平洋地域全体のレベルアップに貢献していくものと期待される。

令和3年度エネルギー需給構造高度化対策に関する調査等事業
（電力分野のサイバーセキュリティ対策のあり方に関する詳細調査分析） 報告書

2022 年 2 月

株式会社三菱総合研究所
デジタル・イノベーション本部
TEL (03)6858-3578

（様式２）

二次利用未承諾リスト

令和３年度エネルギー需給構造高度化対策に関する調査等事業（電力分野のサイバーセキュリティ対策のあり方に関する詳細調査分析）報告書

令和３年度エネルギー需給構造高度化対策に関する調査等事業（電力分野のサイバーセキュリティ対策のあり方に関する詳細調査分析）

株式会社三菱総合研究所

頁	図表番号	タイトル
41	図3-2	NREL DERCFのスコアリングと可視化のイメージ