資源エネルギー庁 御中

令和4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に関する国際動向調査事業）

報告書

三菱総合研究所

デジタル・イノベーション本部

2023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。

国際的には、米国 EIS Council による Cyber Product International Certification（CPIC）イニシアティブ等において、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。また、米国において、2021年にサイバーセキュリティやエネルギー分野を含む重要分野のサプライチェーンの強化に向けた大統領令が署名され、国土安全保障省やエネルギー省を中心として電力分野のサイバーセキュリティ対策が進められているほか、欧州においても電力分野でのサイバーセキュリティ対策について検討が進んでいる。

このような状況を踏まえ、本事業では、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・分析を行うとともに、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ワークショップ形式での国際的な議論を行うことで、諸外国の電力分野におけるセキュリティ政策について情報収集を行うとともに、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図る。

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. 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
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. 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

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～令和3年度の関連事業において整理した認証・評価項目案、運用スキーム案、実証結果等をベースとして、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、運用スキーム案、実証結果等をベースに、次の活動を通じて検証・評価方法の検討を進めた。

- 認証・評価項目案のうち、サプライチェーンに該当する「⑤SCM 上流（調達管理プロセス）」「⑥生産設備（製造プロセス）」「⑦SCM 下流（製品保守運用プロセス）」について、近年のサプライチェーンセキュリティに関する国内外の議論の活発化を踏まえて、「サプライチェーンに関する評価基準のあるべき姿」の検討を行った。
- サプライチェーンに関連する評価基準のあるべき姿の検討に向けて、参照すべき情報の整理を文献調査にて行った。情報や取り組みの妥当性確認のために、有識者に対するヒアリングを行った。文献調査の対象とする情報は次のものとした。
  - 米国の電力分野におけるサプライチェーン関連の取組
  - 欧州の電力分野におけるサプライチェーン関連の取組
  - 日本国内の電力分野・他分野におけるサプライチェーン関連の取組
- 文献調査等の結果に基づき、電力分野のサプライチェーンに関連する評価基準として取り入れる項目の検討を行った。具体的には、認証・評価項目案をベースに、過不足や取り組む際の課題等について、勉強会やヒアリングを通じて有識者から意見を聴取した。
- 勉強会やヒアリングを通じて確認した結果を勉強会やヒアリングを通じて有識者に提示し、次年度の取り組みについて意見を聴取したうえで課題を分析した。

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のニーズや諸外国の規制状況等の国際情勢等を勘案し、保護リレーなどに代表される、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。
- 評価項目については、認証・評価項目案のうち、サプライチェーンに該当する項目に対して、新たに取り入れるべき項目や優先度について検討を行った。
- 評価基準・方法については、特にサプライチェーンに焦点をあて、国内外の関連するガイドライン等に注目して検討を行った。
- 運用体制や運用方法については、過年度の運用スキーム案で想定した国内機関で検証・評価を行うことを前提として検討を行った。
- 制度活用主体のインセンティブについては、セキュリティ対策を実施した際のコストの多寡や負担する主体を意識し、過剰な評価工数とならないように努めた。
- CPICイニシアティブ等の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、

既存の標準規格や国外のガイドライン等との関係を整理することで、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。

- 国際機関や各国の官民における規制や基準策定状況の反映については、特に欧米の状況を文献調査等によって確認した。

文献調査は、次の文献を対象とした。

- Executive Order on America's Supply Chains
- NIS2 Directive（NIS2 指令）
- EU Cyber Resilience Act（EU サイバーレジリエンス法）
- Common Criteria based European Candidate Cybersecurity Certification Scheme（EUCC）
- Revised Network Code on Cybersecurity
- NISTIR 8259
- ETSI EN 303 645
- 重要インフラのサイバーセキュリティ対策に係る行動計画
- 電力制御システムセキュリティガイドライン
- スマートメーターシステムセキュリティガイドライン
- 自家用電気工作物に係るサイバーセキュリティ確保に関するガイドライン
- 系統連系技術要件
- 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
- ERAB に関するサイバーセキュリティガイドライン
- 特定卸供給事業に係るサイバーセキュリティ確保の指針
- 経済安全保障推進法
- IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ
- 防衛産業サイバーセキュリティ基準

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。

- ①参照すべき文献の妥当性について
  - サプライチェーンに関連する評価基準のあるべき姿の検討に向けた、文献調査の対象として参照すべき文献について、調査予定の文献リストを示しつつ、過不足や関連する情報について意見を伺った。ヒアリング対象は有識者 2 者とした。
- ②サプライチェーンセキュリティに関する論点について
  - 文献調査等の結果から抽出した、サプライチェーンセキュリティに関する論点について、その妥当性や対応する際の課題等に関する意見を伺った。ヒアリング対象はベンダ企業及び関連組織の 6 者とした。
- ③次年度以降の取り組みについて
  - 令和元年度～令和3年度の関連事業及び今年度の取り組みを踏まえて、次年度以降の取り組みに関する意見を伺った。ヒアリング対象は有識者 1 者とした。

勉強会は、下表の 2 回開催した。

表 2-1 勉強会開催の概要

	開催日・開催方式	主な検討内容
第 1 回	2022 年 11 月 30 日 （オンライン開催）	● 今年度の実施方針とスケジュールについて ● 国内外文献調査結果について ● サプライチェーンセキュリティに関する論点について
第 2 回	2023 年 2 月 8 日 （オンライン開催）	● 国内外文献調査結果（追加分）について ● サプライチェーンセキュリティに関する論点のまとめについて ● 本勉強会の活動成果と今後の課題について

2.1 国内外文献調査結果

国内の機器・システムの調達時のセキュリティ要件を検討する上で、電力分野を中心に国内外のサプライチェーンに関連する規定・文書を確認した。表 2-2、表 2-3 に調査した文献とその概要の一覧を示す。国内の文献の多くはサプライチェーンに関する要件が具体的ではなかった。海外の文献に関しては、セキュリティ要件が具体化されている文書が多いが、拘束力がある要件については、現在欧州議会等で議論中であり、案として公開されている。また、これらに加えて、国外の動向として、イスラエルの動向について調査した。

表 2-2 国外文献の概要一覧

文書名	発出主体	拘束力	対象分野・製品	ベンダへの影響	要件の具体性
Executive Order on America’s Supply Chains	米国政府	×	重要インフラ	不明	×
NIS2 Directive（NIS2 指令）	EU	○	重要インフラ	不明	×
EU Cyber Resilience Act（EU サイバーレジリエンス法）	EU	○	デジタル製品全体	製品ベンダへの直接的な要件	○
Common Criteria based European Candidate Cybersecurity Certification Scheme（EUCC）	ENISA	×	ICT 製品、サービス、プロセス	製品ベンダへの直接的な要件	×

Revised Network Code on Cybersecurity	EU/ACER	○	電力関連の事業者	電力事業者を経由してベンダに求める間接的な要件	○
NISTIR 8259	NIST	×	消費者向け IoT 製品ベンダ	製品ベンダへの直接的な要件	○
ETSI EN 303 645	ETSI	×	消費者向け IoT 製品ベンダ	製品ベンダへの直接的な要件	○

表 2-3 国内文献の一覧

文書名	発出主体	拘束力	対象分野・製品	ベンダへの影響	要件の具体性
重要インフラのサイバーセキュリティに係る行動計画	NISC	×	重要インフラ	重要インフラ事業者を経由してベンダに求める間接的な要件	×
電力制御システムセキュリティガイドライン	日本電気協会	○	発電事業者、送配電事業者	電力事業者を経由してベンダに求める間接的な要件	△
スマートメーターシステムセキュリティガイドライン	日本電気協会	○	一般送配電事業者が施設するスマートメーターシステム	電力事業者を経由してベンダに求める間接的な要件	△
自家用電気工作物に係るサイバーセキュリティ確保に関するガイドライン	経済産業省	○	自家用電気工作物を設備する者	電力事業者を経由してベンダに求める間接的な要件	△
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	資源エネルギー庁	×	小売電気事業者	電力事業者を経由してベンダに求める間接的な要件	△
ERAB に関するサイバーセキュリティガイドライン	資源エネルギー庁/IPA	×	アグリゲーター、小売電気事業者、送配電事業者	電力事業者を経由してベンダに求める間接的な要件	△
特定卸供給事業に係るサイバーセキュリティ確保の指針	資源エネルギー庁	○	特定卸供給事業者	電力事業者を経由してベンダに求める間接的な	△

				要件	
経済安全保障推進法	日本政府	○	重要インフラ	電力事業者を経由してベンダに求める間接的な要件	×
IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ	NISC	○	政府機関等	電力事業者を経由してベンダに求める間接的な要件	-
防衛産業サイバーセキュリティ基準	防衛装備庁	○	防衛装備庁との契約者	製品ベンダへの直接的な要件	○

調査の方針として、各文書の概要について確認するとともに、サプライチェーンに関連する要件を確認した。特に図 2-1 に示した機器・システムにおけるサプライチェーンの枠組みの中で、製品に直接関係する「⑤SCM 上流」、「⑥生産設備」、「⑦SCM 下流」に該当する要件を抽出して確認した。

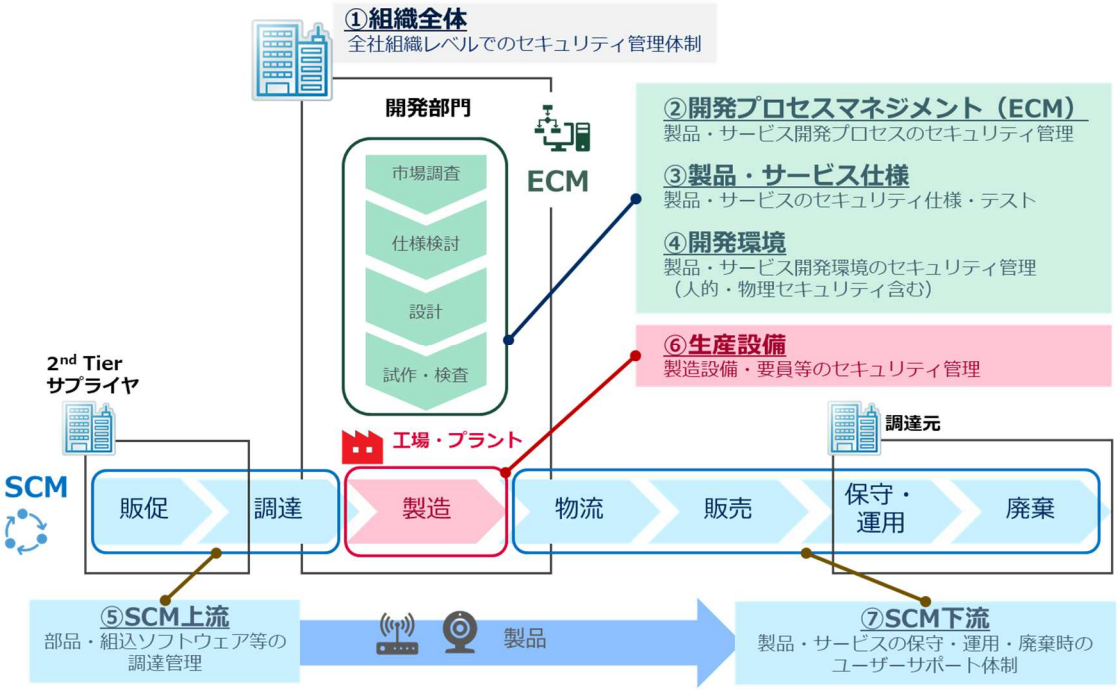

図 2-1 機器・システムのサプライチェーンの枠組み

2.1.1 国外の文献調査

(1) Executive Order on America's Supply Chains

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(EO 14017)に署名した。大統領令では、エネルギーを含めて複数の重要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。米国エネルギー省(DoE、

Department of Energy)に対しては、その他にバッテリー分野におけるサプライチェーンリスクの特定し、対処方法を提言する報告書を提出するよう指示した。これらの指示に伴い、2022 年 2 月、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が発表された。

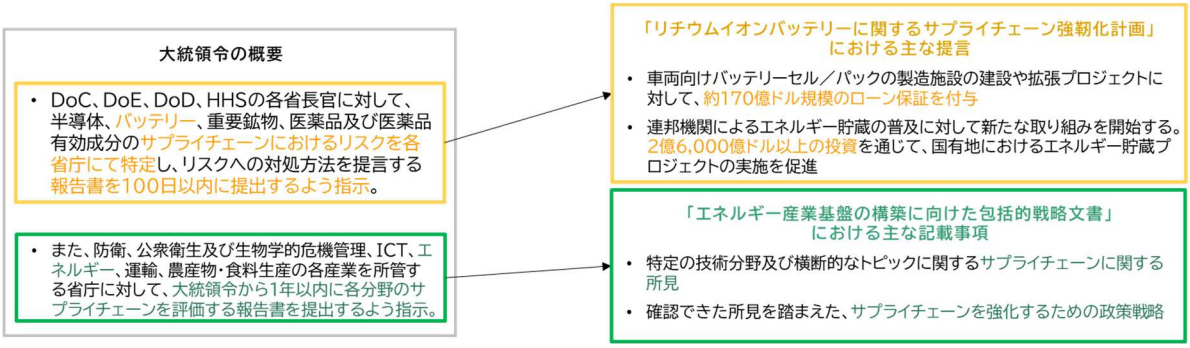

図 2-2 Executive Order on America's Supply Chains におけるエネルギー関連の概要

EO 14017 によって DoE より提言された「エネルギー産業基盤の構築に向けた包括的戦略文書」では、サイバーセキュリティを含めた 12 分野のサプライチェーンに関する報告書が作成されている。サイバーセキュリティのサプライチェーンの報告書では、5 つのサプライチェーンに関する所見と所見を基にした 3 つの戦略概要が示されている。3 つの戦略概要を推進する上で、5 つの具体的なプログラムが紹介されている。紹介された 5 つのプログラムのうち、主に SBOM/HBOM 利用、重要機器の脆弱性検証に関しては、図 2-1 における「⑤SCM 上流」、「⑦SCM 下流」に該当すると考えられる。

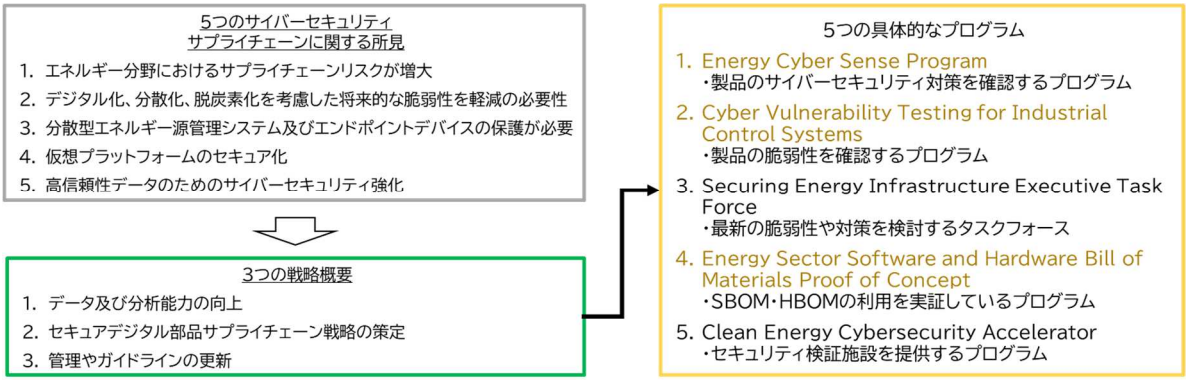

図 2-3 「エネルギー産業基盤の構築に向けた包括的戦略文書」における概要

（2）NIS2 Directive（NIS2 指令）

欧州議会と欧州理事会は、デジタル化に伴い増加したサイバー攻撃・サイバーリスクに対するセキュリティ強化を目的として、NIS2 指令を制定することに 2022 年 5 月 13 日に合意した。本指令は、対象セクターにおけるセキュリティリスク管理対策の基準と EU 加盟国間の効果的な協力のための仕組みを定めた法案であり、対象として 16 セクター（必須分野：10 セクター、重要分野：6 セクター）を指定し、3 つの目標とそれを達成するための具体案を掲げている。本指令では、現行指令と比較して対象セクターの範囲を大きく拡大したことに加え、対象セクターに求めるセキュリティリスク管理に関する項目が明記されたほか、罰則内容も具体化された。電力分野の対象事業者に関して、現行指令の対象である小売電気事業者、発電事業者、送配電事業者に加え、新たに電力市場運営者、アグリゲーターが追加された。

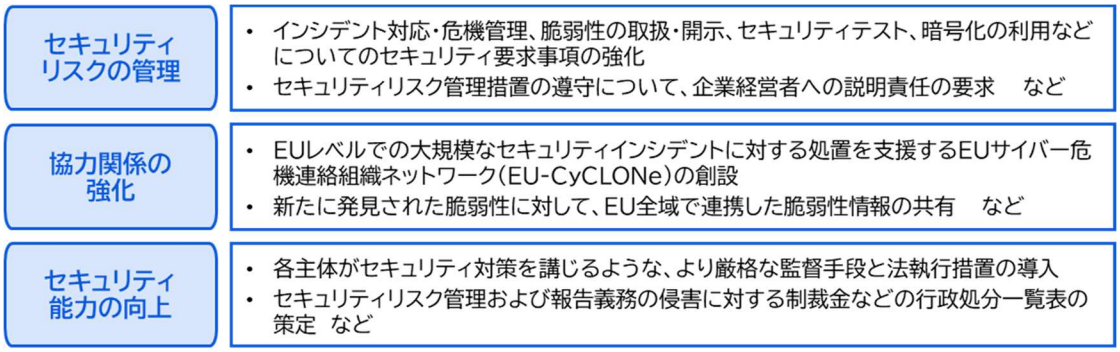

図 2-4 NIS2 指令で掲げられた 3 つの目標と具体案

本指令では、対象分野の事業者に求めるセキュリティリスク管理についての 7 項目を定義しており、その中にはサプライチェーンセキュリティも含まれている。サプライチェーンセキュリティを満たすための具体的な対策や要件については、本指令内で定義されていない。今後、NIS 協力グループは、欧州委員会と ENISA とともに、重要なシステムの特定及びそのシステムのサプライチェーン上のリスク評価を実施する。サプライチェーンのリスク評価は、技術的要因と、非技術的要因の両方を考慮するとしている。

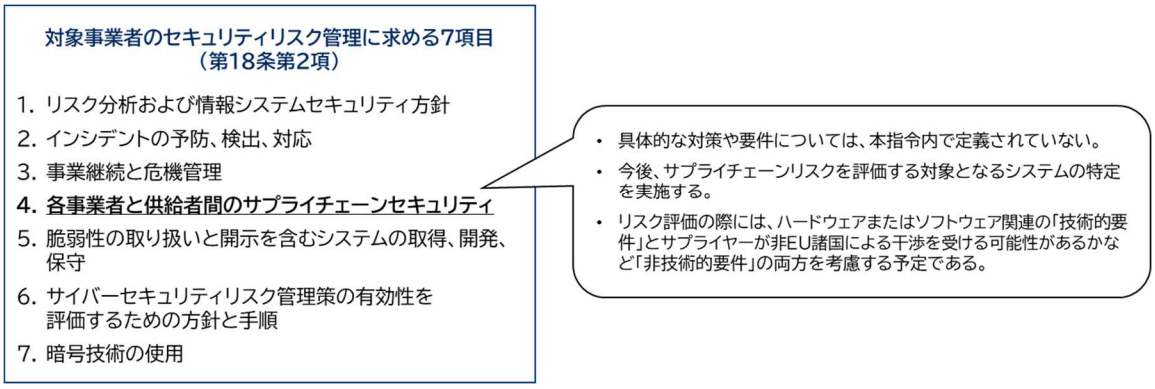

図 2-5 NIS2 指令におけるサプライチェーンセキュリティの概要

（3）EU Cyber Resilience Act（EU サイバーレジリエンス法）

欧州委員会は 2022 年 9 月、NIS2 指令を補完する目的で、EU 市場に投入されるデジタル製品のセキュリティ対応を義務付ける「EU サイバーレジリエンス法」の草案を発表した。欧州委員会は、本法案の 2025 年後半の施行を目指している。本法案では、デジタル製品を上市する際のルール、製品におけるサイバーセキュリティに関する要求事項、製造業者に課される脆弱性対応の要求事項、当該要求事項への順守を担保するための市場監督者へのルールを規定している。本法案では、対象となるデジタル製品に対する要求事項として、リスクに応じた適切なレベルのサイバーセキュリティを確保するように設計・開発・生産することや、悪用可能な既知の脆弱性がない状態で提供することを求めている。対象製品の上市に当たっては、当該製品に対するセキュリティ要件への適合性証明（自己適合宣言もしくは第三者認証）が求められる。製造業者が本法案のセキュリティに関する要件を遵守にしない場合、最大 1,500 万ユーロもしくは前会計年度の世界全体の総売上高の最大 2.5%のいずれか高い方が罰金として科される。

図 2-6 EU サイバーレジリエンス法と関連法令との関係

デジタル製品の脆弱性は、サプライチェーン全体にセキュリティ面の問題を伝播させる可能性が高いとし、本草案では「製造業者に課される脆弱性対応の要求事項」として以下に示す要件を規定している。「SBOM/HBOM の作成と公開」や「脆弱性が発見された場合のセキュリティ更新プログラムの配布」、「脆弱性を報告するための連絡先の提供」などが図 2-1 における「⑤SCM 上流」、「⑦SCM 下流」に該当すると考えられる。

- 製品に含まれる脆弱性と部品を特定し、文章化する。また、ソフトウェア部品表を作成する。
- 脆弱性に対処するためのセキュリティ更新プログラムを遅延なく提供する。
- 製造した製品のセキュリティ面の定期的なテスト・レビューを実施する。
- セキュリティ更新プログラム完成後の製品に関する脆弱性に関する情報の公開を行う。
- 脆弱性開示に関する方針の導入と実施を行う。
- アップデートを安全に配布するためのメカニズムの提供。
- 発見した脆弱性を報告するための連絡先を提供する。
- 特定されたセキュリティ問題に対処するためのセキュリティパッチやアップデートが利用可能な場合、それらが遅滞なく、かつ無料で配布されることを保証する。

図 2-7 製造業者に課される脆弱性対応の要求事項

（4）Common Criteria based European Candidate Cybersecurity Certification Scheme（EUCC）

2020年に ENISA（European Union Agency for Cybersecurity）より、EU におけるデジタル関連商品・サービス・プロセスのサイバーセキュリティ認証制度の枠組み（EUCC）が公表された。EUCC は、2019年に施行されたサイバーセキュリティ法に基づく任意の認証制度で、その枠組みも同法に定められており、既存の CC（Common Criteria）のスキームの後継として機能させることを目的としている。EU サイバーレジリエンス法・Revised Network Code on Cybersecurity においても EUCC を証明書として活用可能である旨が記載されている。EUCC 以外に、クラウドシステムを対象とした EUCS、5G ネットワークを対象とした EU5G の認証制度も検討されている。2021 年 5 月には、EUCC のスキーム候補に関する報告書（Ver 1.1.1）を公表し、ISO/IEC 15408 と ISO/IEC 18045 に基づいて、ICT 製品のサイバーセキュリティの認証を検討していることを発表した。

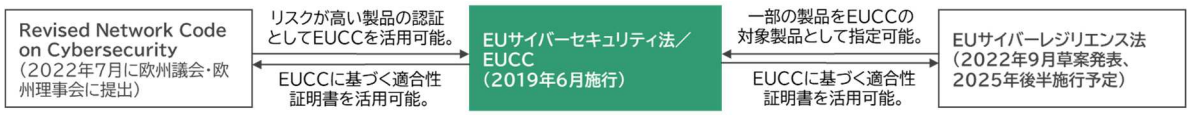

図 2-8 EUCC と他法令との関係

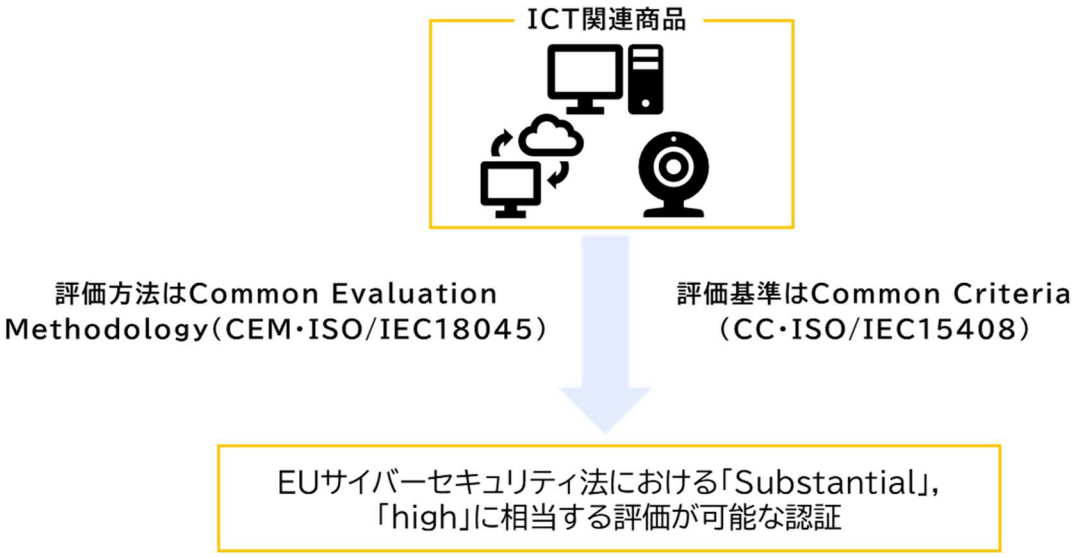

図 2-9 European cybersecurity certification（EUCC） scheme に沿った認証の概要

（5）Revised Network Code on Cybersecurity

2022 年 7 月、EU エネルギー規制協力機構（ACER、European Union Agency for the Cooperation of Energy Regulators）は、ヨーロッパ全体の電力システムのセキュリティと回復力の維持に貢献することを目的として、サイバーセキュリティに関するネットワーク・コードの改訂版を欧州委員会に提出した。本法案では、電力分野の事業体に対して「セキュリティフレームワーク」「セキュリティガバナンス」「セキュリティリスク管理」などを含む電力のサイバーセキュリティに関する規則を示している。今後、欧州委員会は本法案を審査し、委任法の採択手続きを開始する。加盟国によって採択されれば、EU 全域で法的拘束力を持つことになる。

セキュリティマネジメント体制に関する規則
- セキュリティワーキンググループの定義及び役割の規定
- セキュリティリスク評価手法及び評価サイクルの規定

セキュリティマネジメントに関する規則
- ENTSOのEU諸国レベルでのセキュリティリスク評価とリスク対応計画策定に係る一連の行動規定

セキュリティフレームワークに関する規則
- ENTSOのセキュリティマネジメントに関する推奨事項作成に係る行動規定
- 重要事業者のフレームワークへの準拠に関する行動規定

セキュリティ調達の推奨事項策定に関する規則
- ENTSOの調達時の推奨事項策定のための行動規定

セキュリティリスク評価に関する規則
- 所管省庁の重要事業体に対するリスク評価の際の行動規定
- 重要事業体選定に関わる基準

情報共有と危機管理に関する規則
- 影響度の高い事業体からのインシデント発生通達を受けた所管省庁の行動規定
- 影響度の高い事業者の行動規定

サイバーセキュリティ演習に関する規則
- 国境を超える電力網へのインシデントを想定したサイバーセキュリティ演習の実施に関する規定

図 2-10 ネットワーク・コードに記載されている電力セキュリティに関する規定事項

本法案では、共通する電力サイバーセキュリティ・フレームワークの開発から 30 か月以内にサプライチェーンのセキュリティ管理についての提案を行うとしており、サプライチェーンのセキュリティ管理に最低限含める要件を図 2-11 のように定めている。サプライチェーンセキュリティの最低管理項目には、「サプライヤーのスタッフの身元確認」や「サプライヤーの設計・開発・生産工程を監査する権利の確保」、「顧客に影響を与える可能性のあるサイバーセキュリティ・インシデントの周知」などが図 2-1 における「⑤SCM 上流」、「⑦SCM 下流」に該当すると考えられる。サプライチェーンセキュリティの発展的な項目も定義されており、「製品・サービス・プロセス認証の利用」が挙げられ、図 2-1 における「⑤SCM 上

流」に該当する。具体的な認証制度として EUCC が挙げられている。

1. ICT 製品・サービスの調達要件に、以下のセキュリティ要件を含めること
   i. ICT製品・サービスに関する技術的なサイバーセキュリティの調達要件。
   ii. 重要な資産にアクセスできるサプライヤーのスタッフの身元確認チェック。
   iii. ICT 製品・サービスにサイバーセキュリティ・バイ・デザインとゼロトラスト・アーキテクチャを採用しているか。
   iv. 供給者が企業の資産にアクセスすることを管理すること。
   v. 供給者は、第三者による企業の機密情報へのアクセスを保護・制限すること。
   vi. 供給者の下請け業者にサイバーセキュリティ調達要件を伝播すること。
   vii. ICT製品・サービスの開発から生産、納品までのサイバーセキュリティ調達要件の適用の追跡可能性。
   viii. ICT製品・サービスの全ライフサイクルを通じてのセキュリティ更新のサポート。
   ix. サプライヤーの設計、開発、生産工程を監査する権利。
2. 上記のサイバーセキュリティ調達要件を満たし、製品への十分なセキュリティレベルを有する供給者を選択し契約すること。
3. ICT製品・サービスの供給元を多様化し、ベンダーの固定化を抑制する。
4. ICT製品・サービスのライフサイクル全体を通じて、供給者のセキュリティ調達要件を定期的に監視、レビュー又は監査すること。

図 2-11 サプライチェーンのセキュリティ管理に最低限含める要件

（6）NISTIR 8259

2020 年 5 月、米国国立標準技術研究所（NIST、National Institute of Standards and Technology）は、IoT 機器のセキュリティ強化に関する推奨事項の提供を目的として、NISTIR 8259 を公表した。本文書では、IoT 機器製造企業が実施すべきセキュリティ関連活動の推奨事項が、製品の市販前・市販後で 6 つのフェーズに分けられて記載されている。市販前の活動については製品に関する要件が多く、サプライチェーンの要件としては、主に市販後の活動が対象となる。

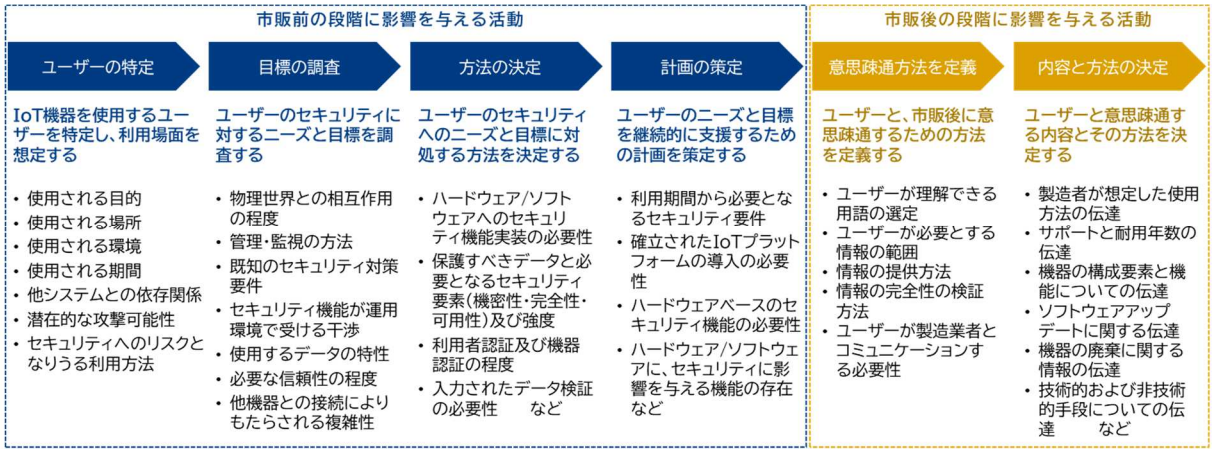

図 2-12 市販前後の段階に影響を与える活動の概要

本文書では、IoT 製品の市販後のユーザーとの意思疎通方法の定義として「ユーザーが理解できる用語の選定」「必要十分な情報の提供」「ユーザーが見つけやすい形での情報提供」「完全性を保証できる情報提供」を推奨し、図 2-1 における「⑦SCM 下流」に該当する。また、ユーザーとの意思疎通の内容と方法として「更新プログラムが提供される期間の通知」「サポート終了までのある程度の期間以内での通知」「機器の破棄に関する情報提供」などを推奨し、図 2-1 における「⑦SCM 下流」に該当する。

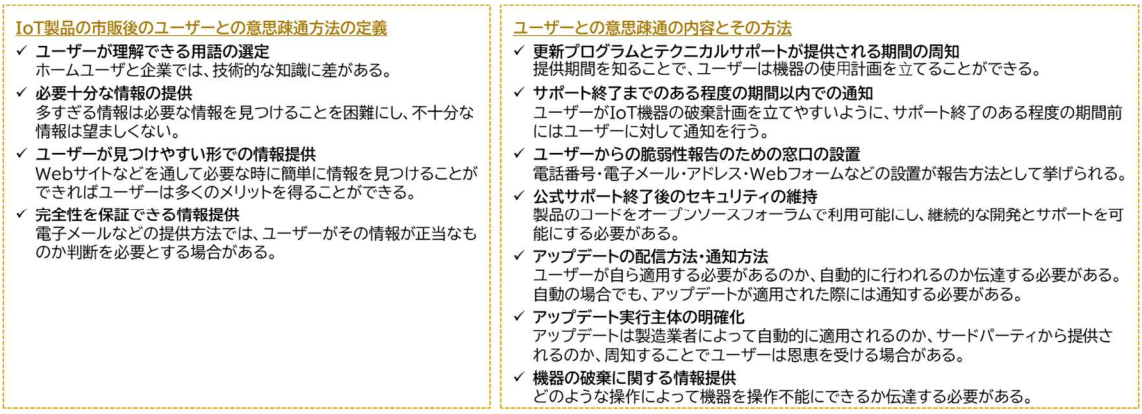

図 2-13 市販後の段階に影響を与える活動における具体的な項目

（7）ETSI EN 303 645 V2.1.1

2020 年 6 月、ETSI は、一般消費者向け IoT 機器のセキュリティ・プライバシーを奨励することを目的として、欧州規格 ETSI EN 303 645 を改訂した ETSI EN 303 645 V2.1.1 を策定した。本規格では、対象を家電や玩具などの一般消費者向け IoT 機器とし、IoT 機器に求める 13 のセキュリティ対策要件を規定している。また、IoT 機器で処理される個人データの保護に関する5つの要件も規定している。

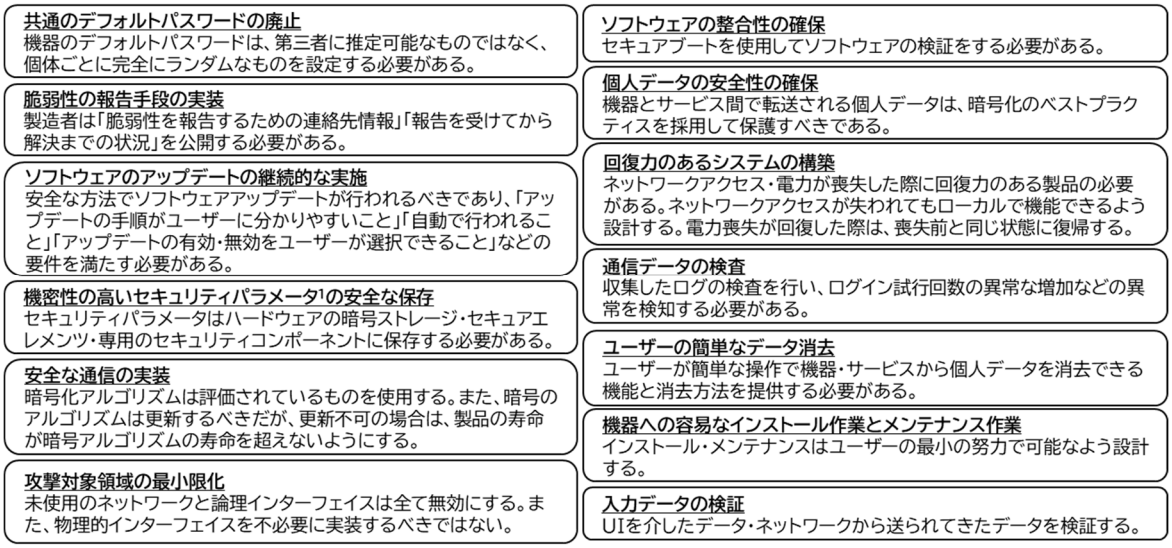

図 2-14 IoT 機器に求める 13 のセキュリティ対策要件

本文書では、保守・運用面のセキュリティ要件として、「ソフトウェア・ハードウェアコンポーネントの管理」「脆弱性報告窓口の設置」「ソフトウェアアップデートの継続的な実施」が規定され、図 2-1 における「⑦SCM 下流」に該当する。本文書で規定されている要件は、「必須」「推奨」「条件付きで必須」「条件付きで推奨」の 4 段階に分類される。現在、製造業者に対してこれらの要件への対応を求める法的な義務はないが、将来の改訂では本文書内で推奨されている規程が義務付けられる可能性があるとしている。

（8）イスラエルの動向

電力分野を含む重要インフラのサイバーセキュリティに関しては、2018 年 12 月に規制法が改正され、首相直轄のイスラエル国家サイバー総局（INCD, Israel National Cyber Directorate）が規制する権限を持つ。重要インフラを対象とした「サイバー防護法」を立法化する動きがあるが、まだ成立していない。INCD に与えられる権限の大きさに対して、国内の民間企業より多くの反発が確認されている。

INCD が公開している文書のうち、“The Corporate Defense Methodology”はサイバー防護のコンセプトが記載されている。NIST CSF ベースのため、サプライチェーンセキュリティに関連する内容も一部含まれている。

その他の動向としては、2022 年 7 月に開催された国際会議“CyberWeek”にて、INCD 局長がプロアクティブなサイバー防護の取り組みを含む“Cyber-Dome”プロジェクトを発表している。イスラエルにおける、サプライチェーンセキュリティに関連する特筆すべき動向は確認されなかった。

2.1.2 国内の文献調査

（1） 重要インフラのサイバーセキュリティに係る行動計画

内閣サイバーセキュリティセンター（NISC）は、2017 年に公表した重要インフラの情報セキュリティ対策に係る第4次行動計画の改定版の位置づけで、重要インフラのサイバーセキュリティに係る行動計画を 2022 年 6 月に公表した。具体的な取り組みとして、「障害対応体制の強化」、「安全基準等の整備及び浸透」、「情報共有体制の強化」、「リスクマネジメントの活用」、「防衛基盤の強化」の5つの方針が挙げられている。第 4 次行動計画と比較し、対象分野や取り組み方針は変わらないが、サプライチェーンなどの一部要素がより重視されている。サプライチェーンの取り組みとして、「障害対応体制の強化」においてサプライチェーン含めた全体の体制の強化を推進すること、「安全基準等の整備及び浸透」においてサプライチェーンに関する基準の整備をすることが挙げられているが、要件は具体的ではない。

障害対応体制の強化	経営層、CISO、戦略マネジメント層、システム担当等、組織全体での取組となるよう、組織統治の一部としての障害対応体制の強化を推進
安全基準等の整備及び浸透	重要インフラ防護において分野横断的に必要な対策の指針及び各分野の安全基準等の継続的改善の推進
情報共有体制の強化	官民間や分野内外間における情報共有体制の更なる強化
リスクマネジメントの活用	自組織の特性を明確化し、適した防護対策が継続的に実施されるようリスクマネジメントを活用
防護基盤の強化	分野横断的演習の推進、国際連携の推進、広報広聴活動の推進等の取組によるサイバーセキュリティ全体の底上げ

図 2-15 重要インフラのサイバーセキュリティに係る行動計画の 5 つの方針

（2）電力制御システムセキュリティガイドライン

電力制御システムセキュリティガイドラインは、2016 年に策定されたガイドラインであり、電気事業法第 39 条下の技術基準の解釈として位置付けられている。電力の安定供給や電気工作物の保安の確保の妨害等を目的としたサイバー攻撃を脅威として想定し、電気事業者が実施すべきセキュリティ対策の要求事項について規定している。求められるセキュリティ水準に応じて、要件ごとに「勧告的事項」と「推奨的事項」が示されている。勧告的事項は電気事業者が実施すべき事項、推奨的事項は電気事業者が実施の要否および実施方法を判断すべき事項と定義される。対象となるシステムの重要度が「S」「A」「B」「C」の 4 段階で定義されており、対策要件のうち「ログの取得」と「入退管理」については、この重要度に応じて勧告的事項・推奨的事項の位置付けが異なる。ガイドラインでは、多層防御による対応を求めている。すなわち、実施可能な複数の対策を重ねることで、より強固なセキュリティ対策とすることが求められている。

本ガイドラインに記載しているサプライチェーンセキュリティに関連する項目として、「第 6-1 条 セキュリティ仕様の確認」があり、本項目では推奨的事項として「電力制御システム等の調達時にセキュリティ仕様を明確にする」、「電力制御システム等がセキュリティ仕様通りに設計、製造されていることを確認する」などの要件が明示され、図 2-1 における「⑤SCM 上流」に該当すると考えられる。

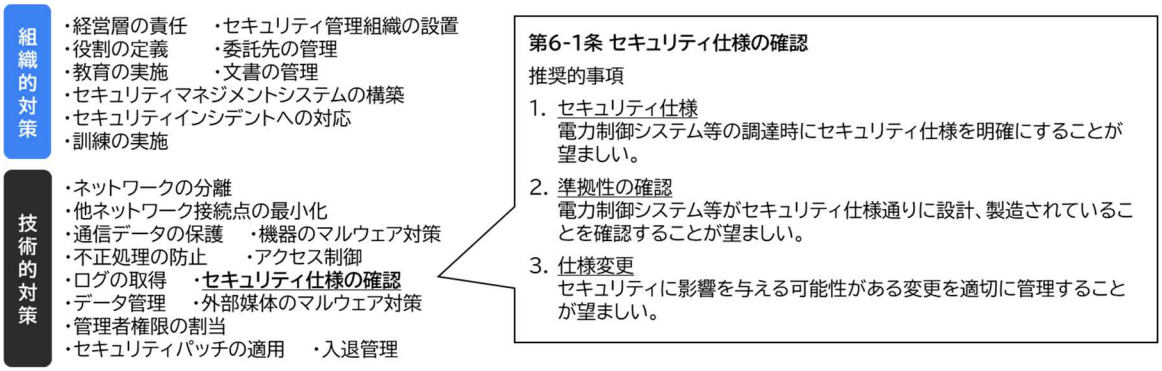

図 2-16 ガイドラインにおけるセキュリティ対策要件

（3）スマートメーターシステムセキュリティガイドライン

2016 年 3 月、日本電気協会が、スマートメーターセキュリティの確保を目的として、スマートメーターシステムセキュリティガイドラインを制定した。また、2019 年 7 月に電力制御システムのセキュリティ向上を目的に改定が行われている。本ガイドラインでは、対象を一般配送電事業者が施設するスマートメーターシステムとそれに携わる事業者としており、スマートメーターシステムの設計調達段階から保守運用段階までの一連の工程におけるセキュリティ対策の要求事項を勧告事項・推奨事項に分けて規定している。本ガイドラインに記載しているサプライチェーンセキュリティして、「第 5-1 条 セキュリティ仕様の確認」があり、本項目では推奨的事項として「機器の調達時にセキュリティ仕様を明確にする」、「機器がセキュリティ仕様通りに設計、製造されていることを確認する」などの要件が明示され、図 2-1 における「⑤SCM 上流」に該当すると考えられる。

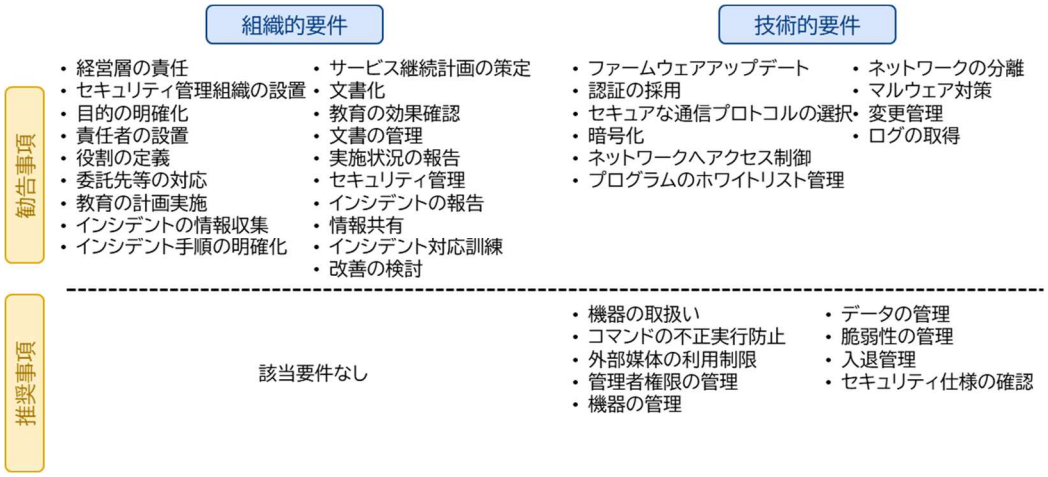

図 2-17 ガイドラインで規定されているセキュリティ対策要件

（4）自家用電気工作物に係るサイバーセキュリティ確保に関するガイドライン

「電気設備に関する技術基準を定める省令」及び「電気設備の技術基準の解釈」の改正に伴い、2022 年 10 月 1 日より、自家用電気工作物においてもサイバーセキュリティの確保が義務付けられている。対策にあたって、2022 年 6 月 10 日に公開された「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（内規）」に基づく対策が求められる。具体的な内容は「電力制御システムセキュリティガイドライン」をベースとした内容となっているが、一部の項目を除き、事業者自らが実施の要否及び実施方法を判断する「推奨」事項として設定されている。また、対象となる設備が区分 A～C に分類され、区分により「勧告」又は「推奨」となるガイドラインの条項が異なる。本ガイドラインに記載しているサプライチェーンセキュリティに関連する項目として、「第 5-1 条 セキュリティ仕様の確認」があり、区分 A～C に対する推奨的事項として「自家用電気工作物の制御システム等の調達時にセキュリティ仕様を明確にする」、「制御システム等がセキュリティ仕様通りに設計、製造されていることを確認する」などの要件が明示され、図 2-1 における「⑤SCM 上流」に該当すると考えられる。

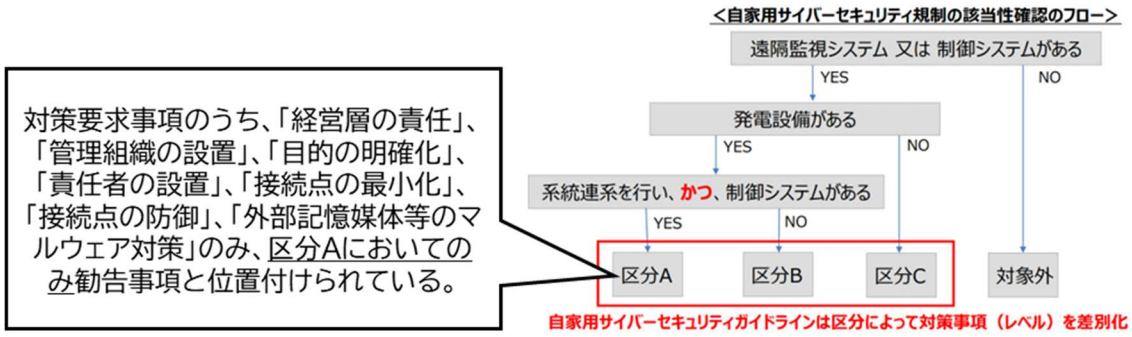

図 2-18 「自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン（内規）」の対象設備区分と対策要求の概要

（5）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

2021 年 2 月、経済産業省は、小売電気事業者がサイバーセキュリティ対策を実践する際の指針をまとめた「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・公表した。このガイドラインでは「サイバーセキュリティ経営ガイドライン」の対策内容を踏襲しつつ、小売電気事業者が各々の

事業モデルに適したサイバーセキュリティ対策を実践するための重要 10 項目に対する具体的な解釈及び指針を記載している。本ガイドライン内のサプライチェーンセキュリティ対策推進のための指針として、指示 9 では、サイバーセキュリティ対策の PDCA について、「サプライチェーンのビジネスパートナーを含めた運用をすること」、「委託の際には自組織と委託先との責任範囲の明確化を行うこと」を推奨している。対策事例として「対策状況チェックリストを利用した委託先への対策状況の申告の要求」、「委託先への監査規則の設定と監査の実施」について記載され、図 2-1 における「⑤SCM 上流」に該当すると考えられる。

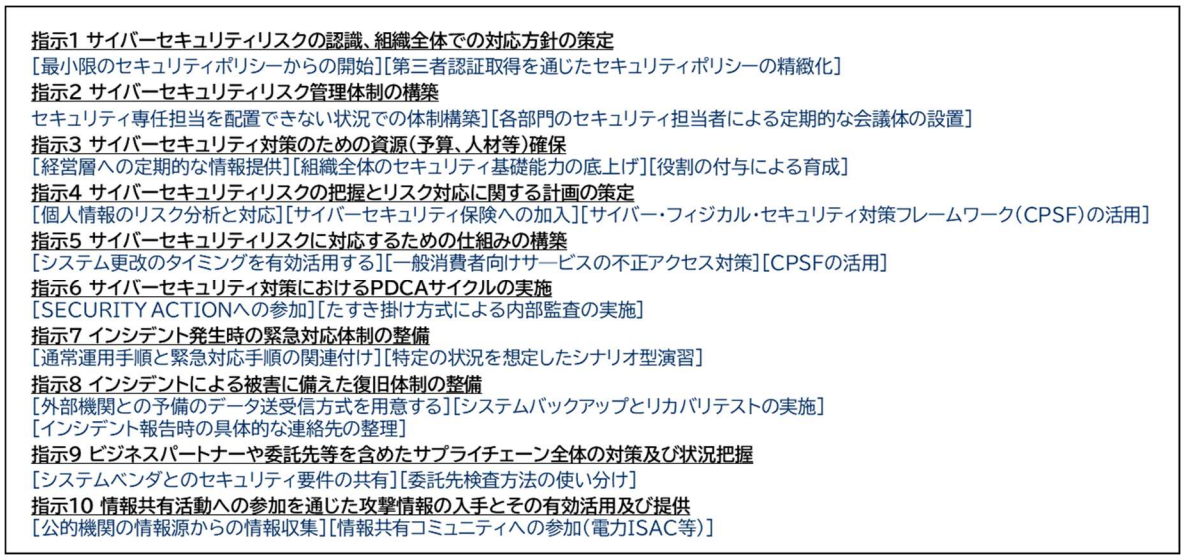

図 2-19 小売電気事業者におけるセキュリティ対策における重要 10 項目

（6）ERAB に関するサイバーセキュリティガイドライン

「ERAB に関するサイバーセキュリティガイドライン」は、VPP（Virtual Power Plant）や DR（Demand Response）を用いたビジネスであるエネルギー・リソース・アグリゲーション・ビジネス（ERAB）に参画する事業者が取り組むべきサイバーセキュリティ対策の指針を示したもので、2019 年 12 月に最新版の Ver 2.0 が公開された。ガイドラインでは、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ており、各事業者はガイドラインを踏まえて、自らの責任においてセキュリティ対策を講ずることが求められる。ガイドラインの記載事項は、実装を必須として義務づけられる【勧告】と、実装を検討すべき内容である【推奨】に分類される。ERAB に参画する各事業者は、【勧告】として、図 2-20 の手順に基づくサイバーセキュリティ対策を行うことが義務付けられる。本ガイドライン内では、各事業者における監視・対応体制等についての推奨事項として、「システム調達時にはセキュリティ仕様を明確にし、設計・製造時等にその準拠性を確認するとともに、仕様変更時にはセキュリティ対策の再構築を行うこと」と明記され、図 2-1 における「⑤SCM 上流」に該当すると考えられる。

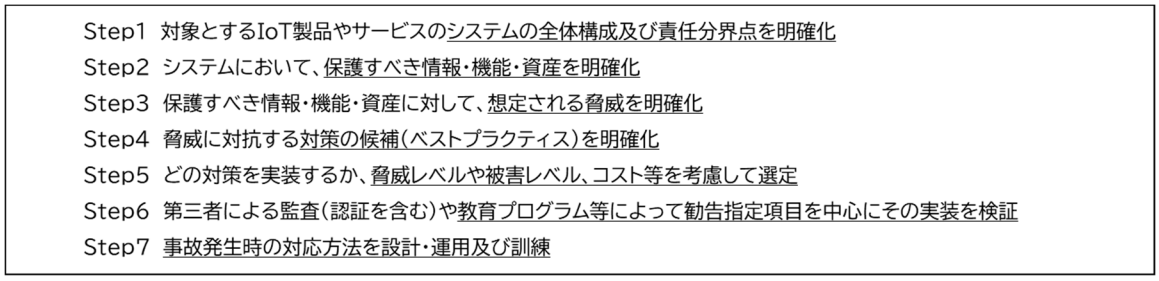

図 2-20 ERAB システムにおけるサイバーセキュリティ対策手順

(7) 特定卸供給事業に係るサイバーセキュリティ確保の指針

特定卸供給事業者(アグリゲーター)の事業においてはサイバーセキュリティ対策が特に重要であるところ、対策が不十分と考えられる事業者に対しては変更命令や業務改善命令が発動される。これらの命令の処分基準として、「特定卸供給事業に係るサイバーセキュリティ確保の指針」が 2022 年 4 月に制定された。対策事項は、「電力制御システムセキュリティガイドライン」の勧告的事項及び「ERAB に関するサイバーセキュリティガイドライン Ver2.0」の勧告的事項により構成される。サプライチェーンセキュリティ対策としては、運用・管理のセキュリティにおいて、セキュリティ仕様の明確化を推奨しており、対策内容として「システム調達時の齟齬の発生を抑制するために、セキュリティ要件を明確化すること」が記載され、図 2-1 における「⑤SCM 上流」に該当すると考えられる。

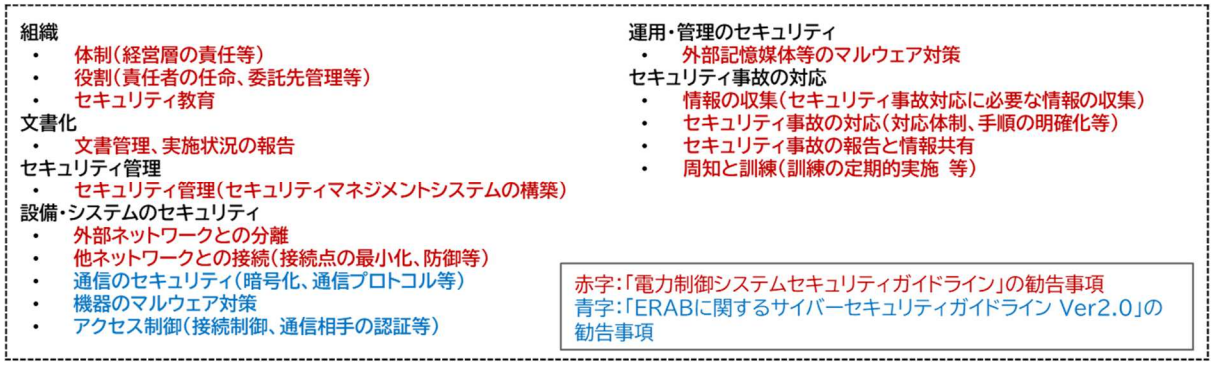

図 2-21 「特定卸供給に係るサイバーセキュリティ確保の指針」における対策要求事項

(8) 経済安全保障推進法

2022 年 5 月に、日本の経済安全保障を包括的に強化することを目的に経済安全保障推進法が成立し、2022 年 6 月～2024 年 5 月にかけて段階的に施行される予定である。経済安全保障推進法は、4 つの方針から構築されている。4 つの方針の 1 つとして、「基幹インフラ役務の安定的な提供の確保に関する制度」がセキュリティ関連の動きとして挙げられている。重要インフラとしては 14 分野が想定されている。

対象の 14 分野においては、重要設備の導入・維持管理における委託の事前審査が必要であり、事前審査の内容によっては勧告・命令もされる可能性がある。対象の 14 分野の全ての事業者が実施する必要はなく、主務省令で定める基準で選定された事業者が実施する必要がある。本制度は、委託の事前審査というサプライチェーンの対策を注視している。申請における具体的な基準等は今後公開される予定である。

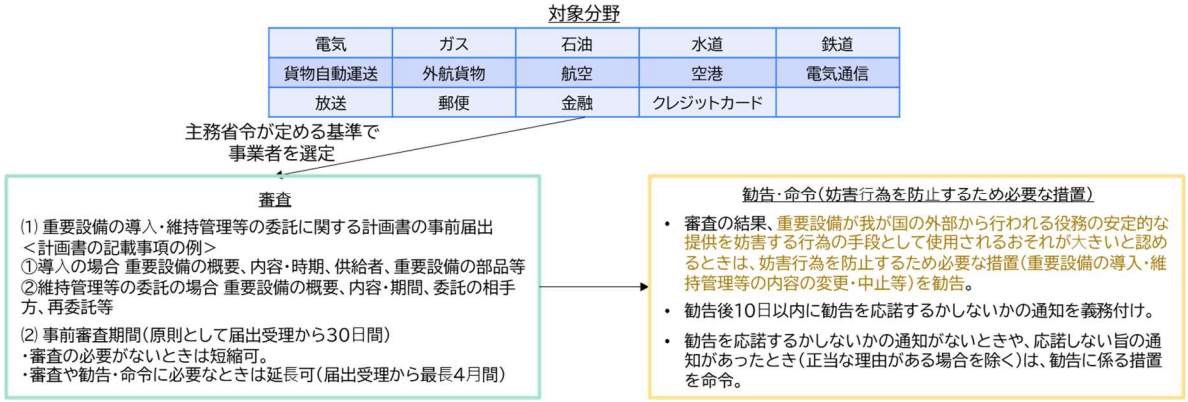

図 2-22 経済安全保障推進法の「基幹インフラ役務の安定的な提供の確保に関する制度」の概要

（9）IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ

「IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」は、省庁や独立行政法人等の政府機関等が利用する重要な IT 製品・サービス等の調達にあたって、構成機器等にサプライチェーンリスクの懸念の有無を確認し、懸念が払しょくできない場合には、NISC 及びデジタル庁が代替品への差替や低減策の実施等を助言する取組である。政府機関等は、サプライチェーンリスクの観点から必要な場合において、NISC 及びデジタル庁に対して、講ずべき必要な措置について原則助言を求める必要がある。令和 2 年度の助言実績は 3,515 件であり、そのうち 5%において「懸念あり」の助言がなされた。なお、懸念の判断基準は公開されていない。

- 通信回線装置（ハブ、スイッチ、ルータ、ファイアウォール 等）
- サーバ装置（メールサーバ、Webサーバ、DNSサーバ 等）
- 端末（デスクトップPC、ノートPC、モバイル端末 等）
- 複合機（プリンタ）
- 特定用途機器（テレビ会議システム構成機器、IP電話カメラシステム構成機器 等）
- ソフトウェア（OS、アプリケーション、ウェブコンテンツ 等）
- 周辺機器（キーボード、マウス）
- 外部電磁的記録媒体（外付けハードディスク、USBメモリ）
- 役務（システム開発、運用・保守、通信サービス 等）

図 2-23 申合せ対象の情報システム・機器・役務等

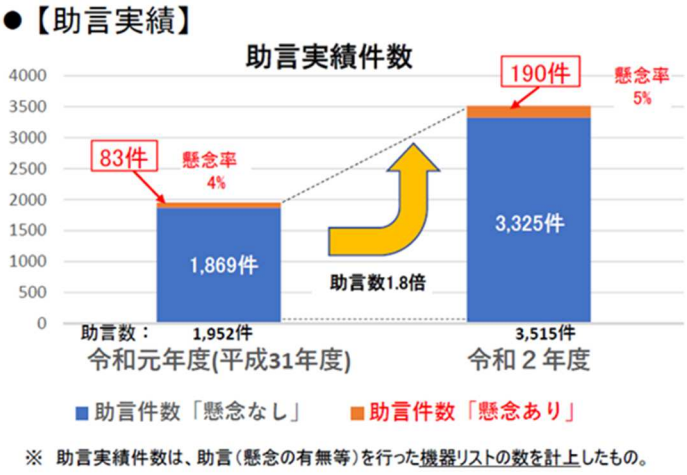

図 2-24 申合せの助言実績[1]

（10） 防衛産業サイバーセキュリティ基準

防衛産業におけるサイバーセキュリティ体制の強化を目的に、現行より厳格な管理策が盛り込まれた「防衛産業サイバーセキュリティ基準」が整備され、2023 年度以降の契約より適用される予定である。本基準は、先行する米国の取組（NIST SP800-171）を参考に、同水準の管理策を追加している。具体的な基準として「装備品等及び役務の調達における情報セキュリティ基準」を定めている。「装備品等及び役務の調達における情報セキュリティ基準」は、装備品や役務を提供する企業における保護すべき情報の適切な管理を目指し、防衛省が求める当該企業が実施すべき情報セキュリティ対策を示している。本紙では主に組織的な対策、付紙「装備品等及び役務の調達における情報セキュリティの確保に関するシステムセキュリティ実施要領」では主に技術的な対策が記載されている。当該基準は防衛省が調達時に取引先に求めることを前提に策定されているため、要件のほぼすべてがサプライチェーンの要件として適応可能であり、図 2-1 の「⑤SCM 上流」、「⑥生産設備」、「⑦SCM 下流」に該当すると考えられる。

図 2-25 防衛産業サイバーセキュリティ基準の概要[2]

[1] IT 調達に係る国等の物品等又は役務の調達方針及び調達手続に関する申合せ」の改正（案）【概要】、https://www.nisc.go.jp/pdf/council/cs/taisaku/ciso/dai18/18shiryou0201.pdf

[2] 防衛産業サイバーセキュリティ基準の整備について、https://www.mod.go.jp/atla/cybersecurity.html

2.1.3　文献調査結果のまとめ

（1） 機器・システムのサプライチェーンの枠組みとの対応

文献調査結果の図 2-1 に該当する項目を図 2-26 にまとめた。主に海外文献を参考にすることで、「⑤SCM 上流」、「⑦SCM 下流」に対応する内容は確認できた。特に SBOM/HBOM の利用は、先進的な構成管理手法であり、脆弱性の確認等に利用されることが期待されている。現時点では、SBOM/HBOM を利用した統一的な枠組みは確認できないため、今後動向を確認し、電力分野における適用方法を検討する必要がある。

一方、「⑥生産設備」における製造設備に関する要件を記載している文献は少なかった。国内では、経済産業省より「工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」が 2022 年 11 月に公表されている。当該ガイドラインは電力分野に限定されておらず、任意の取組として位置づけられている。このようなガイドラインを参考に、特に製造設備に対応する内容を加えることも検討できると考えられる。

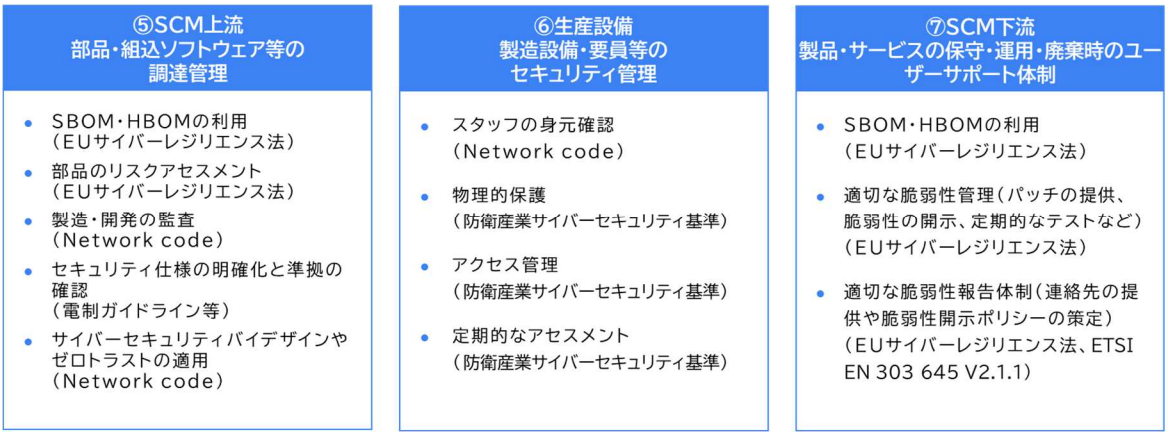

図 2-26　文献調査結果とサプライチェーンに関する評価基準の対応関係

（2） 過年度調査の評価スキーム案と IoT 製品向けスキームの比較

過年度調査では電力分野を中心としたガイドラインのベストプラクティスから、国内の電力会社やベンダ企業が対応可能な項目を中心に抽出し、既存のセキュリティ認証に対して軽量な評価方法を目指した。本評価手法における評価項目を検討する際、主に以下の標準等を参照していた。

- 電力制御システムセキュリティガイドライン（電制ガイドライン）
- 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）
- NIST CSF、NIST SP 800-53 Rev.5
- NERC CIP
- IEC 62443-2-1, 3-3, 4-1, 4-2

一方、近年では IoT 製品向けのスキームとして、本調査の対象としていた NISTIR 8259 や ETSI EN 303 645 が注目されている。

NISTIR 8259 では、IoT 製品の市販前・市販後にベンダが実施すべき推奨事項が記載されている。

市販前については、主に設計開発時の項目であり、図 2-1 の「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」に関連する。市販後については、主にユーザー運用時の支援に関する項目であり、図 2-1 の「⑦SCM 下流」に関連する。市販後の項目はアップデートの方法等に言及していて具体的であり、粒度は過年度調査で検討した評価項目の「小項目」に近い。

ETSI EN 303 645 では、IoT 機器に求める 13 のセキュリティ対策要件を規定している。13 の要件では、IoT 機器の実装や運用・保守に関連する項目が含まれている。実装については図 2-1 の「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」、運用・保守については「⑦SCM 下流」に関連する。運用・保守の項目のうち、「脆弱性の報告手段の実装」「ソフトウェアのアップデートの継続的な実施」では具体的な要件を示しており、粒度は過年度調査で検討した評価項目の「小項目」に近い。

2.2 サプライチェーンセキュリティに関する論点

文献調査等の結果に基づき、電力分野のサプライチェーンに関連する評価基準として取り入れる項目の検討を行った。具体的には、認証・評価項目案をベースに、過不足や取り組む際の課題等について、勉強会やヒアリングを通じて有識者から意見を聴取した。

2.2.1 SCM 上流（調達管理プロセス）

SCM 上流（調達管理プロセス）の各論点について、ヒアリング等で得られた主な意見を以下の表 2-4 に示す。

SBOM/HBOM の利用について、いずれ国内でも必要になるため、要求として入れるべきとの肯定的な意見が得られた。一方で、運用する際のコスト・複数の規格や流通の存在、顧客が国外に偏ることによる国内産業の空洞化、また、導入済み製品への対応の困難さ等を懸念する声が多くあがった。

部品のリスクアセスメントについて、「顧客が購入するものはシステムであるので、部品単体のリスクアセスメントではなく製品のリスクアセスメントを行うべきである」「部品の用途によってリスクアセスメントの結果が変わるので、ある程度用途が決定しないことには対応可能か不明である」との意見が得られた。部品のリスクアセスメントについては再度検討する余地がある。

セキュリティバイデザイン・ゼロトラストの適用について、セキュリティバイデザインについては対応可能であるという肯定的な意見を多く得られた。一方で、ゼロトラストについては、「まずはセキュリティアーキテクチャを決定する必要があり、調達先に求めることは時期尚早である」「機器の追加・削除が頻繁ではなく、システム的にアクセスを限定しているなど特別な運用をしている電力分野にそもそもゼロトラストが必要なのか検討すべき」という指摘が得られた。ゼロトラストの適用について改めて検討する必要がある。

製造・開発の監査について、肯定的な意見として「定期的な顧客からの監査がすでに実施されているのでその延長上で対応可能」「大企業で IEC62443-4-1 を取得しているので同様の要件であれば対応可能」であるといった意見が得られた。一方で、「Network Code で要求されているような要件を必要とすると対応できるベンダが限られる」「中小企業はコスト面の問題もあり対応が難しいのではないか」という懸念が挙げられた。

セキュリティ仕様の明確化と準拠の確認の有効な取り組みについては、「仕様だけではなく規格適合を評価する手順・基準の明確化も行うとよい」との意見をいただいた。一方で、「厳格な要件を要求すると調達先が見つからなくなる」という懸念事項も挙がった。

表 2-4 「SCM 上流(調達管理プロセス)」の各論点についてヒアリング等で得られた主な意見

論点	ヒアリング等で得られた意見
SBOM/HBOM の利用について EU サイバーレジリエンス法で製品の製造者に求められる「製品に含まれる脆弱性とコンポーネントを特定し、文書化する」等の取り組みは、国内の電力分野においても対応可能か。	● 米国で SBOM/HBOM の利用を求める動きが出てきている。いずれ国内においても SBOM/HBOM への対応が必要になることが考えられるので、要求として入れていくべきであると感じる。 ● HBOM は、経験上、それぞれの業界の規格(例えば MIL 規格(Military Specification and Standards))に準拠しているか確認すればよいので、証跡を残す制度さえ整備されれば対応可能であると感じる。 ● 自社製造品に関しては対応可能であるが、購入品の対応が困難であると感じる。 ● 導入済み製品について、対応を求めることは困難であると感じる。新規製品については検討の余地があるのではないか。 ● 各社で使用する SBOM のフォーマットが統一されていない。データの連携を行い、脆弱性の発見に至るためには、使用する SBOM のフォーマットを国際的に統一する必要がある。 ● 業界内でのルール及びツールが整備されない限り、実現は厳しいのではないか。 ● Linux の exe ファイルが 2 万程存在することもあり、コンポーネントを特定し、文書化する」ことには時間と費用がかかる。 ● 端末 OS ベンダ等が対応に応じるか疑問であるが、特に SBOM/HBOM に取り組む上では端末 OS ベンダ等の協力が必須である。 ● SBOM/HBOM への対応義務が国内では課せられ、一方で国外では課せられないなどの場合があると、国外プラントの方が運用コストを抑えられるため、利益を求めると顧客が国外に偏ることになり、国内の産業の空洞化が進むことが考えられる。 ● SBOM の利用を、特定の機器に限定して実施することも選択肢の1つである。その際に、SCADA 周りはソースコードが多いので、一旦置いておくということも考えられ

論点	ヒアリング等で得られた意見
	る。遮断機や保護リレーから手を付ける選択もあるが、SCADA の方が脆弱性の観点では重要なため、段階的に考慮していく必要がある。
部品のリスクアセスメント EU サイバーレジリエンス法でデジタル要素を持つ製品に求められるリスクアセスメントに基づくセキュリティ要求事項は、国内の電力分野においても対応可能か。	● システム全体に対するリスクアセスメントを実施するべきなので、部品ではなく製品のリスクアセスメントを行うべきである。 ● リスクアセスメント結果は部品の用途によって変わるので、対応可能かは疑問が残る。ある程度の使い方を決定しないことには何とも言えない。 ● 現在のリスクアセスメントは、様々な形式が存在し、国や顧客によって要求する観点が異なる（IT 寄りの内容のものもあれば、経営に関する内容も含んでいるものもある）。 国際標準となるように IPA のリスクアセスメントの手法を海外にも広めると国内企業の対応も円滑に加速できると感じる。
サイバーセキュリティバイデザインやゼロトラストの適用 Network Code on Cybersecurity で求められるサイバーセキュリティバイデザインやゼロトラストの取り組みを調達先に求めることは、国内の電力分野においても対応可能か。	● 既存の IEC 62443 のセキュリティ要求事項を考慮すると、セキュリティバイデザインを多少なりとも取り入れることになるので、程度次第ではあるが、対応可能であると感じる。その場合、段階的に要求されることが望ましい。 ● ゼロトラストについては、時期尚早であると感じる。調達先にゼロトラストを求める以前に、自社製品においても対応できていない。ゼロトラストは、アーキテクチャやコンセプトレベルの話であり、取り組むとなると、電力会社のシステム全体のセキュリティアーキテクチャについて考慮する必要があり、そこについて決定しないと物事を考えられない。 ● 機器の追加・削除が頻繁ではなく、システム的にアクセスを限定している等の特別な運用がなされている電力分野に、ゼロトラストがそもそも必要かについても議論が必要である。ゼロトラストが、多要素認証などの要件だけで完結するのならば対応可能だと感じる。 ● プラントシステムでは、境界防御を多重化することでセキュリティを構築していたが、これはプラントの安全（Safety）で執られてきた多重防御とも通じる思想だからと考えている。ゼロトラスト導入を議論する際は Safety との整合も論点になると考える。
製造・開発の監査 Network Code on Cybersecurity で求められる供給者の製造・開発プロセ	● 定期的に顧客からの監査があるので、その延長線上で対応可能であると感じるが、製造設備・工場設備の手直しが必要となると、すぐには対応できず、数年の期間が必要で

論点	ヒアリング等で得られた意見
スの監査や、高度な取り組みである製品・サービス・プロセス認証は、国内の電力分野においても対応可能か。	ある。 ● 開発プロセスについては、IEC 62443-4-1 の取得が主要な流れであり、大企業が取得した例をよく見る。IEC 62443-4-1 に含まれている要件と同様の要件への対応ならば可能ではないか。一方で、中小企業については、コスト面の問題もあり対応が難しいと感じる。 ● 自社で既に取り組んでいるものに関しては顧客に費用の請求はしないが、追加で取り組むこととなると顧客に追加の費用を請求することになる。国の方針が決まることで、各社自発的に取り組むようになるのではないか。 ● Network Code では細かなものが要求されているということもあり、同じような要件を求めるとベンダが絞られるという懸念がある。 ● 開発プロセスに対する監査は実施しているが、ISO/IEC においても、製造に対する監査は実施していない。ISO/IEC でも実施していない工場監査を求めるべきなのか疑問である。
セキュリティ仕様の明確化と準拠の確認 電制ガイドラインの「第 6-1 条セキュリティ仕様の確認」の推奨的事項を調達先に求める場合、具体的にはどのような取組が有効と考えられるか。	● 事前にリスクアセスメントを実施し、セキュリティ仕様を明確化することが有効であると感じる。 ● 仕様だけではなく、規格適合を評価する手順・基準を明確にすると良い。 ● 顧客に要求されたセキュリティ要件は、ベンダに伝えて実装してもらうようにしているが、厳格な要件を要求すると、調達先が逃げていく可能性がある。

2.2.2 生産設備(製造プロセス)

生産設備(製造プロセス)の各論点について、ヒアリング等で得られた主な意見を以下の表 2-5 に示す。

スタッフの身元確認については、「国内では個人情報保護の観点があり、法律が作成され枠組みが整備されない限り、自主的に対応することは難しい」との意見が多数挙げられ、再度検討する必要があると思われる。

物理的保護に関しては、「電制ガイドラインでも重要度が高いシステムについては対策を求めており、その範囲内で対応可能である」という意見が得られた。一方で、「より厳しい要件への対応が必要となるとコストがかかることになる」とコスト面を懸念する声も挙がった。

アクセス管理・定期的なアセスメントについても、「電制ガイドラインに記載があり、その範囲内であれ

ば対応可能である」との意見をいただいた。

表 2-5 「生産設備(製造プロセス)」の各論点についてヒアリング等で得られた主な意見

論点	ヒアリング等で得られた意見
スタッフの身元確認 Network Code on Cybersecurity で求められる供給者のスタッフの身元確認チェックは、国内の電力分野においても対応可能か。	● 個人情報保護の観点があるため対応は厳しいのではないか。法律を作成し、枠組みを整備してもらわない限り、対応することは厳しい。 ● 国外での要求が緩く、利益が上がりやすいとなると、顧客が国外へ偏るということも考えられる。
物理的保護 防衛産業サイバーセキュリティ基準の「第 8 物理的及び環境的セキュリティ」や、NIST SP800-171 の「3.10 物理的保護」で求められるセキュリティ要件は、国内の電力分野においても対応可能か。	● 電制ガイドラインに物理的保護についての記載があり、重要度が高いものについては対応を求めている。その範囲内では、対応可能であろうと考えている。 ● 防衛分野で実施しているので、技術的には対応可能である。 ● 原子力分野では既に行っているので、同様の要件であれば対応可能だと考えるが、さらに厳しい要件となると対応は難しいのではないか。また、原子力分野でもコストはかかっているので、コスト面の懸念がある。 ● 経済産業省にて策定している「工場セキュリティガイドライン」を基準に考えると良い。
アクセス管理 防衛産業サイバーセキュリティ基準や、NIST SP800-171 で求められるセキュリティ要件は、国内の電力分野においても対応可能か。	● 電制ガイドラインに記載があるため、その範囲で対応可能ではないか。 ● 防衛分野で実施しているので、技術的には対応可能である。 ● 経済産業省にて策定している「工場セキュリティガイドライン」を基準に考えると良い。
定期的なアセスメント 防衛産業サイバーセキュリティ基準や、NIST SP800-171 で求められるセキュリティ要件は、国内の電力分野においても対応可能か。	● 電制ガイドラインに記載があるため、その範囲で対応可能ではないか。 ● 経済産業省にて策定している「工場セキュリティガイドライン」を基準に考えると良い。

2.2.3 SCM 下流(製品保守運用プロセス)

SCM 下流(製品保守運用プロセス)の各論点について、ヒアリング等で得られた主な意見を以下の表 2-6 に示す。

SBOM/HBOM の利用について、「SCM 上流(調達管理プロセス)と同様な懸念事項が生じ、管理コスト・流通面の整備を懸念する」「利用者と提供者の関係性も考慮する必要があり、管理コストを持つ

主体が誰になるのかという懸念が生じる」との意見を得た。SCM 上流（調達管理プロセス）と同様に慎重に検討する必要がある。

脆弱性管理について、「パッチの適用や脆弱性開示などのアクションは必要であり、現在も実施している不具合対応の延長線上で対応可能である」、「電力のように顧客が特定され、管理されている条件下であれば、脆弱性を公に開示する必要はない」との意見を得た。また、「脆弱性通報から 24 時間以内の対処要求は厳しいので避けたい」と、要求事項によっては対応が厳しいとの意見をいただいた。

表 2-6 「SCM 下流（製品保守運用プロセス）」の各論点についてヒアリング等で得られた主な意見

論点	ヒアリング等で得られた意見
<u>SBOM/HBOM の利用</u> EU サイバーレジリエンス法で製品の製造者に求められる「製品に含まれる脆弱性とコンポーネントを特定し、文書化する」等の取り組みは、SCM 下流ではどのように有効活用できるか。	● SCM 上流の話と立場が逆になるだけなので、流通面での整備の話に収束する。 ● 保守・管理を実施するとなると、管理コストがかかる点について懸念している。 ● 利用者と提供者の関係性も考慮する必要があり、管理コストを持つ主体が誰になるのかという懸念が生じる。
<u>適切な脆弱性管理</u> EU サイバーレジリエンス法で製品の製造者に求められる脆弱性ハンドリング要件は、国内の電力分野においても対応可能か。	● パッチの適用や脆弱性開示などのアクションは、具体的な行動に移す必要がある。 ● メーカーでは、不具合対応のための体制を構築し実施しているので、その一環として、セキュリティ対応も必要であると認識できれば、体制づくりは可能だと考える。 ● 電力のように顧客が特定されている場合、CRM（Customer Relationship Management）の対応がしっかりできている条件の下で、脆弱性ハンドリングは対応可能である。実施する際は、脆弱性を公開しない方法で行うと良い。 ● 脆弱性の通報から 24 時間以内の対処を要求されるとなると、負担が重く、避けたいという本音がある。 ● ソフトウェア開発時に OSS を使用する場面が多々あるが、OSS の管理が完璧になされている事業者は少ないのではないか。自社においても対応が追い付いていない状態であると感じる。 ● 課題は、人と費用である。また、脆弱性を発見するためには、ハッキングと同等のことを行う必要があるので、そのための能力開発・教育も必要である。

2.3 活動成果と今後の課題

2.3.1 活動成果

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、本年度を含めて 4 年間にわたって検討を行った。主な活動成果を表 2-7 に示す。

表 2-7 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・評価方法に関する主な活動成果

年度	主な活動成果
平成 31 年度 ／令和元年度（2019 年度）	● 電力分野の製品・機器に関するスコアカード方式による評価項目を策定した。 ● 評価項目を 7 つのカテゴリ（大項目）に分類し（図 2-27 参照）、想定脅威と期待される対策概要（中項目）、具体的評価項目例（小項目）を定めた（図 2-28 参照）。
令和 2 年度（2020 年度）	● スコアカード方式による製品・機器の検証・評価スキームを検討し、EIS Council をスキームオーナーとした場合の国内の体制案を策定した（図 2-29 参照）。 ● 評価対象とすべき電力分野の製品・機器の種別について検討を行った（図 2-30 参照）。
令和 3 年度（2021 年度）	● 7 つのカテゴリのうち、設計・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、評価基準及び評価手順の具体化を実施し、評価基準書及び評価手順書として取りまとめた（図 2-31、図 2-32 参照）。 ● 評価基準書、評価手順書の実効性を確認するために、実機（保護リレー1 機種）に対して一部の評価項目に対する模擬評価を実施した。
令和 4 年度（2022 年度）	● 7 つのカテゴリのうち、サプライチェーンセキュリティに該当する「⑤SCM 上流（調達管理プロセス）」「⑥生産設備（製造プロセス）」「⑦SCM 下流（製品保守運用プロセス）」について、近年のサプライチェーンセキュリティに関する国内外の議論の活発化を踏まえて、「サプライチェーンセキュリティに関する評価基準のあるべき姿」の検討を行った（図 2-33 参照）。

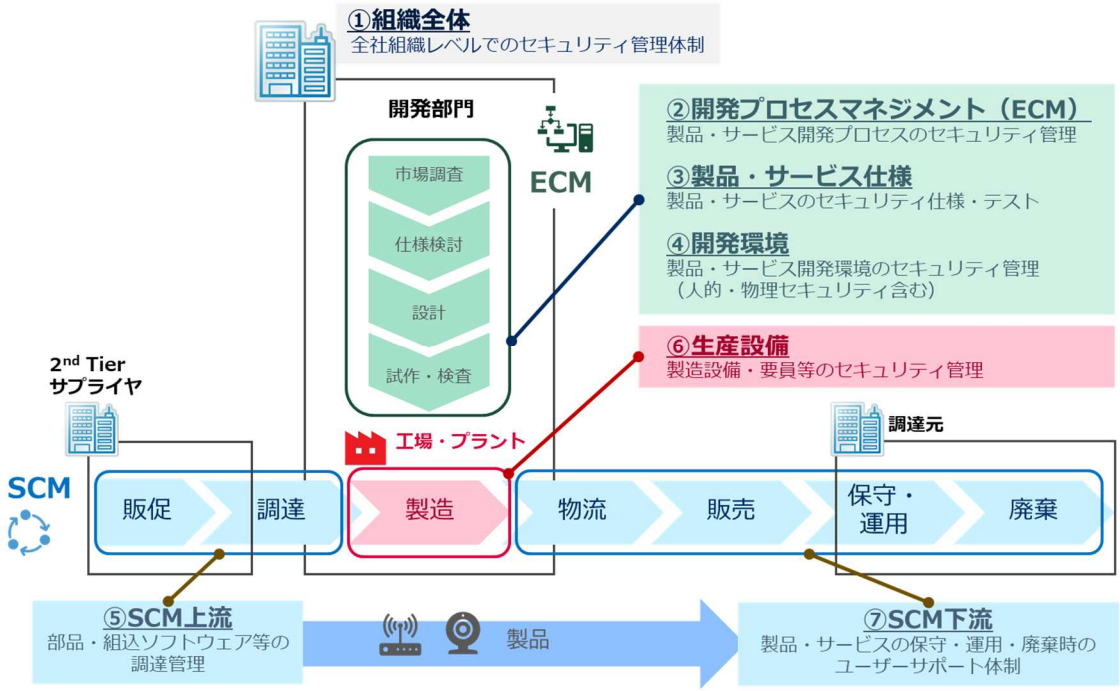

図 2-27 機器･システムのサプライチェーンの枠組み(再掲)

大項目
(CPIC評価カテゴリ)

中項目
(評価カテゴリ内の想定脅威と期待される対策概要)

小項目
(具体的評価項目例)

評価項目				評価対象
大項目（評価の枠組）		中項目		
		（想定される脅威）	（期待される対策概要）	小項目（具体的対策の例）	該当／対象外
⑤ SCM下流（製品保守運用プロセス）	電力関連機器のライフサイクル上流（物流・保守・廃棄）におけるセキュリティ要件	・攻撃者によるゼロデイ脆弱性の悪用	・機器に関する不具合、脆弱性情報の受付 ・脆弱性対策情報発信のコントロール	製品のユーザー及び外部機関等から、機器の脆弱性等セキュリティに関する問題の報告・情報提供を受け付けている	
				報告されたセキュリティに関する問題は、分析・対応策を整理した後、情報の発信を実施している	
		・攻撃者による未対応の脆弱性の悪用	・アップデート機能の提供 ・修正プログラム、パッチの提供	セキュリティアップデートの正当性検証・アップデート実施方式等に関する文書等の提示が可能である	
				利用OSや依存コンポーネントのアップデートに関する対応方針が定まっている	
				修正プログラム、修正パッチが適時提供される	
		・機器の誤った（推奨外の）取扱いを狙った攻撃	・機器の堅牢化、安全な初期設定 ・推奨される手順に従った廃棄	機器を安全に設定し堅牢化するためのマニュアルが提供される	
				機器の安全な利用、廃棄を行うためのマニュアルが提供される	
				ユーザーアカウントの安全な設定、利用を行うためのマニュアルが提供される	

※⑤SCM下流の例

ユーザーもしくはベンダの指定による評価対象外項目の個別設定を想定

図 2-28 各評価カテゴリで想定される脅威と期待される対策(中･小項目)

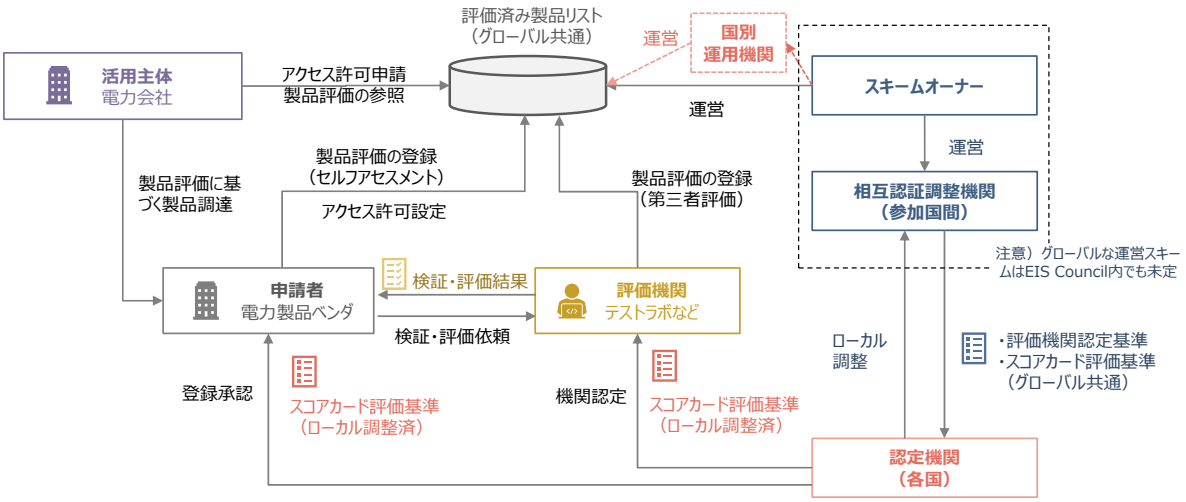

図 2-29 スコアカード方式による製品・機器の検証・評価スキームの国内の運用体制案

1．主に送配電設備に納入される電力制御機器及び付帯設備を対象とする

- 送配電設備に納入される保護リレー、変圧器、遮断機等の送配電の制御に係る機器
- 上記機器の装置にインストールされている、又は機器の操作に使用される関連ソフトウェアおよびファームウェア
  ※SCADA、PLC等のコントローラ、通信ルータ、GW機器等を含む
- これらの機器もしくはソフトウェア・ファームウェアを製造しているメーカー

2．将来的に同様の定義を用いて送配電以外の電力設備への拡張も検討する

- 大容量の再エネ設備や関連機器の取扱いのための拡張性も考慮する

図 2-30 評価対象とすべき電力分野の製品・機器の種別

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

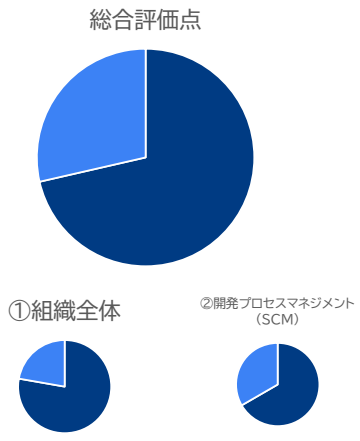

図 2-31 評価結果（スコアリング）のイメージ

図 2-32 評価基準書及び評価手順書のイメージ

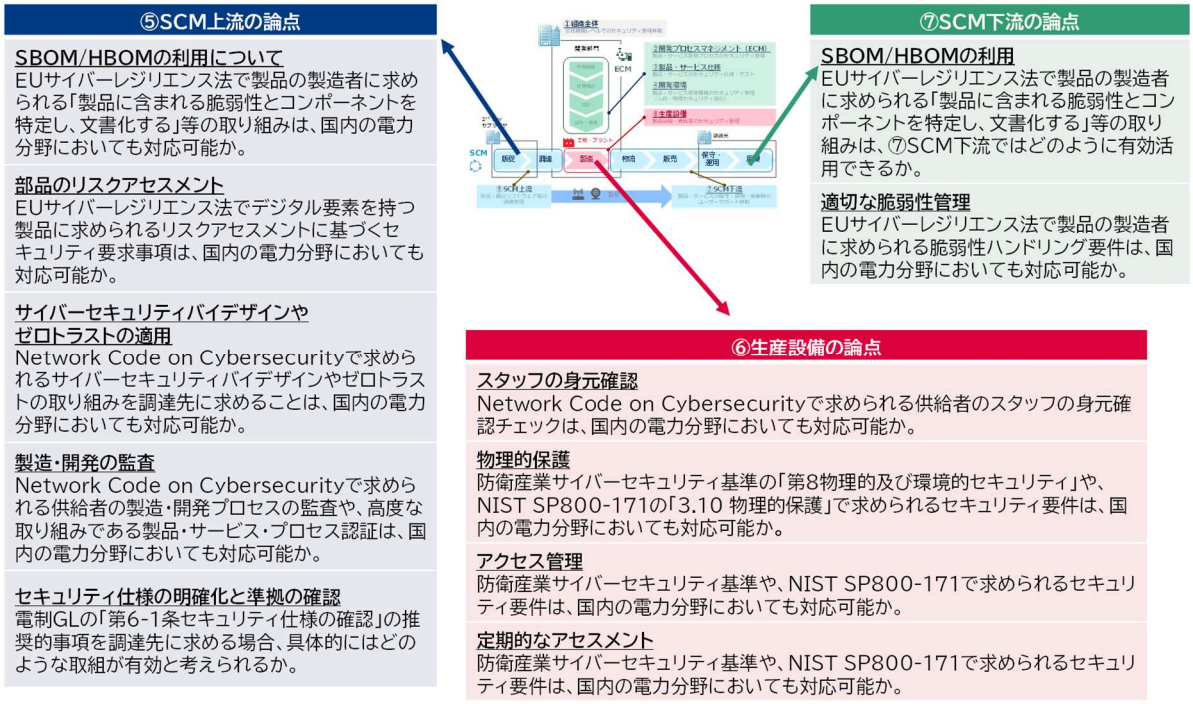

図 2-33 「サプライチェーンセキュリティに関する評価基準のあるべき姿」の検討の論点

2.3.2 今後の課題

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、前項で示した活動成果や国内外の動向を勘案して、次年度以降に検討すべき活動や課題を次に示す。

(1) EIS Council の動向に応じた活動

本取組を開始する発端となった CPIC(Cyber Product International Certification)は、サプライチェーンリスク管理(SCRM)の強化を目的として、米・英・イスラエルの官民を中心に EIS Council で立ち上がったプロジェクトであった。

今後は、CPIC 検討の母体である EIS Council の動向を引き続き注視し、状況を国内にフィードバックすることが求められる。

また、EIS Council の動向を踏まえて、これまでの活動成果を EIS Council へ提案する時期を模索する必要がある。

（2）サプライチェーンセキュリティに関する国内外動向の継続的な分析

サプライチェーンセキュリティに関する取り組みは、国内外で引き続き活発に行われている。

今後は、欧米の電力分野の動向に加えて、国内外の電力分野以外での取り組みについても継続的に確認・分析し、情勢に即したセキュリティ対策を確認してゆく必要がある。

（3）SBOM/HBOM の利用についての再検討

SBOM/HBOM の利用に関しては、初期導入のコストが大きいことに加え、運用・維持面においてもコストがかかることが予想される。また、国外で SBOM/HBOM への対応義務がない場合、国内と比べて国外の方が運用コストを抑えられるようになる。そうした状況になると、ベンダ企業が利益を追及すると顧客が国外に偏ることになり、国内の産業の空洞化が進む事態も想定される。

今後は、国内で先行して実証が進んでいる分野（医療、自動車など）を参考に、電力分野における SBOM/HBOM の利用について検討を進める必要がある。

（4）脆弱性の開示範囲についての再検討

電力分野に代表される国内の重要インフラ分野では、制御機器を利用する顧客が特定されており、ベンダ側でシステムの詳細を把握しているケースが多い。このような状況下であれば、すべての脆弱性を公開する必要は必ずしもない。一方、サプライチェーンセキュリティ強化の観点からは、IoT 製品の脆弱性情報を積極的に公開するなど、適切な取り扱いに向けた取組が各分野で進められている。

今後は、最新の動向を踏まえて、電力分野における脆弱性情報の取扱いについて、改めて検討する必要がある。

3. 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ワークショップ形式での国際的な議論を行うことで、諸外国の電力分野におけるセキュリティ政策について情報収集を行うとともに、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 2022 年 10 月 26 日から 28 日の3日間にわたりオンライン形式(一部講師は会場入りするハイブリッド形式)で開催した。なお、2022 年 10 月 24 日から 25日及び 27 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 2022(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。

3.1 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 DHS(Department of Homeland Security)、CISA(Cybersecurity and Infrastructure Security Agency)、DOS(Department of State)、DOE(Department of Energy)、INL(Idaho National Laboratory)、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)の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5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 EU 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 3-1 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
- 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
  - J202 (ICS セキュリティ遠隔ハンズオン&ディスカッション)
  - J402(プロセスオートメーションセキュリティ遠隔ハンズオン)
- INL による CCE(Consequence-driven Cyber-informed Engineering)ワークショップ

- サイバー妨害工作と重要機能保証
- 経済産業省による人材育成ワークショップ
  - 人材育成の取り組みについて紹介

(3) 日米 EU ICS サイバーセキュリティセミナー

- 政策＆ガイドライン
- ランサム＆インシデント
- 従来型電力
- 新電力
- 標準化
- サプライチェーンリスクマネジメント

3.1.1 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(受講生)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)の招聘機関から責任者の推薦をうけた 37 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 130 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。

3.2 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 3-2 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 24 日(月)	
11:00-11:30	受付
11:30-12:00	プレオープニングセッション
12:00-14:30	J202R (1)

14:30-15:30	ロングブレイク
15:30-18:00	J202R (2)
18:00-18:30	ネットワーキングセッション

2 日目 ： 10 月 25 日(火)	
11:00-11:30	受付
11:30-14:30	J202R(3)
14:30-15:30	ロングブレイク
15:30-18:00	J202R(4)
18:00-18:30	ネットワーキングセッション

3 日目 ： 10 月 26 日(水)	
11:00-11:30	受付
11:30-12:10	開会の辞・基調講演
12:10-13:10	政策＆ガイドラインセミナー
13:10-13:30	ショートブレイク
13:30-14:30	ランサム＆インシデントセミナー
14:30-15:30	ロングブレイク
15:30-16:50	従来型電力セクターセミナー
16:50-17:10	ショートブレイク
17:10-18:30	新電力セクターセミナー

第 4 日目 ： 10 月 27 日(木)	
11:00-11:30	受付
11:30-14:00	J402
14:00-14:30	ネットワーキングセッション
14:30-15:30	ロングブレイク
15:30-16:50	標準化セミナー
16:50-17:10	ショートブレイク
17:10-18:30	サプライチェーンリスクマネジメントセミナー

第 5 日目 ： 10 月 28 日(金)	
11:00-11:30	受付
11:30-14:30	INL ワークショップ(1)
14:30-15:30	ロングブレイク
15:30-16:30	INL ワークショップ(2)
16:30-16:50	ショートブレイク
16:50-17:40	人材育成ワークショップ
17:40-17:50	ショートブレイク

17:50-18:30	クロージングセレモニー

3.3 各セッションの概要

3.3.1 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。
- 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。

3.3.2 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。

- ICS テストベッドを用いて、基本的な ICS サイバーセキュリティの知識と技術を習得する。
- 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、教訓について参加者とグループディスカッションを行う。
- ICS 環境におけるセキュリティ対策に関する課題を共有する。

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、以下の 6 スロットで構成されている。

3.3.3 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、グループ内で参加者相互の交流の機会を持った。10 月 24 日、25 日の J202 演習後及び 10 月 27 日の J402 演習後の合計 3 回実施した。

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

主催者を代表して、日米 EU の各関係組織より開会挨拶があった。また、基調講演が行われた。

（1） 講演者一覧

表 3-3 開会の辞・基調講演の講演者一覧

開会挨拶	● 上村昌博、経済産業省 サイバーセキュリティ・情報化審議官 ● Mr. Eric GOLDSTEIN, Executive Assistant Director for Cybersecurity, U.S. Department of Homeland Security, Cybersecurity, and Infrastructure Security Agency (DHS/CISA) ● 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	● "The Growing Danger of Criminal Ransomware in Critical Industries," Mr. Marty EDWARDS, Vice President, Tenable

3.3.5 政策&ガイドラインセミナー／Policy & Guidelines Seminar

日本、米国、EU のスピーカーがサイバーセキュリティ政策と戦略についてアップデートするセミナーである。政府はどのようにサイバーセキュリティの意識を高めることができるのか、。サイバーセキュリティのレベルを向上させるためには、どのようなインセンティブや規制が有効なのか。等について、3 人のスピーカーがこれらの課題に対するヒントを提供した。

(1) 講演者一覧

表 3-4 政策&ガイドラインセミナーの講演者一覧

モデレーター	Ms. Karolina Kozłowska, Policy Officer, European Commission, EC, DG CNECT.
講演者及びタイトル	1. "Cybersecurity Policy for Industry Sector in Japan," 星代介 経済産業省 商務情報政策局 サイバーセキュリティ課 企画官 2. "CYBERSECURITY POLICY: A SNAPSHOT OF US TRENDS," Mr. Ian Wallace, Digital Industries, Strategy & Technology, Cybersecurity, Siemens AG 3. "Cyber Resilience Act proposal", Ms. Raluca Stefanuc, team leader European Commission, DG CONNECT

3.3.6 ランサム&インシデントセミナー／Ransom & Incident Seminar

ランサム＆インシデントセミナーでは、日本、米国、EU の専門家が、最新のサイバー脅威とその対応策を解説した。また、この地域の状況を共有するために統計を示し、産官学の連携スキームを紹介した。

(1) 講演者一覧

表 3-6 ランサム&インシデントセミナーの講演者一覧

モデレーター	Mr. Chris Butera, Senior Technical Director for Cyber, Cybersecurity Division, CISA
講演者及びタイトル	1. "Ransomware cases in Japan","小宮山功一朗 一般社団法人 JPCERT コーディネーションセンター(JPCERT/CC) 国際部部長

	2. ” Operational Collaboration During Critical Incidents and to Counter Ransomware: a US Perspective,” Mr. Clayton Romans, Associate Director, Cybersecurity Division, Associate Director, Cybersecurity Division 3. ”Possibilities and Limitations of Cyber Threat Intelligence in Energy Systems,” Dr. Csaba Krasznay, PhD, HEAD OF INSTITUTE OF CYBERSECURITY of the Hungarian National University of Public Service

3.3.7 従来型電力セクターセミナー／Conventional Electricity Seminar

従来電力セクターは最重要インフラの一つであるため、悪意ある攻撃者はこのセクターを攻撃の良いターゲットと見なしている。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促進されているが、サイバー攻撃には脆弱なままである。各国政府はそれぞれ、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おり、安全で信頼性の高い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。これらの取組・動向について紹介を行った。

（1） 講演者一覧

表 3-7 従来電力セミナーの講演者一覧

モデレーター	長谷川弘幸 中部電力パワーグリッド株式会社システム部総括グループ副長
講演者及びタイトル	1. ”The Approach to Cyber Security Measures of Chubu Electric Power Grid” 長谷川弘幸 中部電力パワーグリッド株式会社システム部総括グループ 副長 2. Mr. Matthew Duncan, Director of Intelligence, E-ISAC, North American Electric Reliability Corporation 3. ”Cybersecurity TRANSMISSION SYSTEM OPERATOR VIEW” Mr. Radek Hartman, Chair of ENTSO-E’s Information and Communication Technologies Committee (ICTC), ENTSO-E

3.3.8 新電力セクターセミナー／New Electricity Seminar

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資源集約事業（ERAB）の拡大により、送電網が不安定になり、相互接続性からサイバーセキュリティリスクが高まっている。この新電力セクターでは、サイバーセキュリティの政策的な取り組みは、従来電力セクターほど成熟していない。このセミナーでは、依然として新

たな課題である ERAB のさまざまな関係者すべてが適切に対処する必要性について議論を行った。

（1） 講演者一覧

表 3-8 新電力セミナーの講演者一覧

モデレーター	Mr. Tom Wilson, Senior Vice President, CISO, Southern Company, Inc.
講演者及びタイトル	1. ”(Managing Risk Related to New Renewable and Distributed Energy Resources (DER)),” Mr. Tom Wilson, Senior Vice President, CISO, Southern Company 2. ”(CCRC technical report on Security Recommendations for Distributed Energy System Aggregators, Based on METI Cyber and Physical Security Framework),” 梅嶋真樹 慶應義塾大学大学院政策・メディア研究科、サイバー文明研究セン ター准教授、IEC システム委員会(スマートエネルギー)専門委員 3. ”CYBERSECURITY PROGRESS UPDATE on ENTSO-E contribution to improve grid cyber resilience,” Mr. Grzegorz Bojar, CIO, Member of ENTSO-E’s Information and Communication Technologies Committee (ICTC), ENTSO-E

3.3.9 日米 ICS サイバーセキュリティトレーニング(J402，ハンズオン)／JP-US ICS Cybersecurity Training for the Indo-Pacific Region - J402 (Remote Hands-on)

本トレーニングは以下を目的として開催された。

- プロセスオートメーションに関連する ICS サイバーセキュリティの知識と技術を習得する。
- リモートハンズオン形式で、OT システムを保護するための人工知能(AI)の活用方法について学習する。

演習は 10 月 27 日の午前に、プロセスオートメーション、ファクトリーオートメーションに特化した ICS サイバーセキュリティ演習を実施した。工場で AI、クラウド、IoT が使用される環境におけるサイバー脅威と対応について知識を身に着けた。演習内容としては、ICSCoE 中核プログラム第5期生のプロジェクト「セキュアな ICS クラウド導入指南書」を元に作成された座学演習を実施した。

3.3.10 標準化セミナー／Standardization Seminar

サイバーセキュリティの標準については、米国では NIST が CSF を発表し、日本では経済産業省が CPSF を制定している。また、ISO、IEC、ETSI などの国際標準化機構を通じた国際的な議論も進んでいる。 最近 EU は、新たな適合性評価手続きを構築するために、EU サイバーレジリエンス法のドラフトを公表した。本セミナーでは、日米 EU の講演者が、今後のサイバーセキュリティ標準と適

合性評価手続きについて、それぞれの立場から意見を述べた。

（1） 講演者一覧

表 3-9 標準化セミナーの講演者一覧

モデレーター	Mr. Tonnie De Koster, Adviser for International Aspects of Digital Transformation, European Commission
講演者及びタイトル	1. ”Framework, standard and Conformity Assessment on Cybersecurity,” 西村美香 経済産業省サイバーセキュリティ課 課長補佐 2. ”Coordinated Vulnerability Disclosure (CVD) for Industrial Control Systems (ICS)” Ms. Lindsey Cerkovnik, ICS Vulnerability Disclosure Lead, Cybersecurity Division, CISA 3. ”Consumer Device Security,” Sonia COMPANS, Technical Officer, ETSI (European Telecom. Standards Institute)

3.3.11 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 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最も大きな課題の一つとなっている。COVID-19 によるデジタル化の進展に伴い、日本、米国、EU において、サプライチェーンにおけるサイバーセキュリティリスクが高まっている。日米 EU の政府、民間企業はそれぞれサイバーセキュリティガイドラインの策定や製品・ソリューションの認証取得に取り組み、リスクの軽減に努めている。

（1） 講演者一覧

表 3-10 サプライチェーンリスクマネジメントセミナーの講演者一覧

モデレーター	佐々木弘志 ICSCoE 専門委員／フォーティネットジャパン株式会社
講演者及びタイトル	1. ”Supply Chain Risk Management overview and initiatives in Japan,” 佐々木弘志 ICSCoE 専門委員／フォーティネットジャパン株式会社 2. “Software Bill of Materials: Transparency in the Supply Chain,”Dr. Allan Friedman, Senior Advisor and Strategis, CISA 3. “GOOD PRACTICES FOR ICT/OT SUPPLY CHAIN CYBERSECURITY IN EU,” Dr. Konstantinos Moulinos, Senior Cybersecurity Expert, Policy Development and Implementation, ENISA

3.3.12 INL ワークショップ／Cyber-enabled Sabotage and Critical Function Assurance by INL

アイダホ国立研究所で開発された CCE（Consequence-driven Cyber-informed Engineering）を紹介するセミナーである。現在のサイバー攻撃の脅威環境を把握することの重要性及び所属機関が有する重要機能とそれらがどのように機能を失うかについて理解することの重要性について触れた。後半では、安全で信頼できる運用のためにサイバーセキュリティの原則を工学と統合することの重要性について紹介した。

3.3.13 人材育成ワークショップ／Human Resources Workshop

本セミナーでは、ICS 人材開発のための日本と米国のフレームワーク・アプローチ及び課題や教訓、ベストプラクティスについて紹介した。また、組織内で能力を測定管理する方法について触れたほか、人材開発に関連するガイドラインと手順について改善の余地がある領域を特定した。

（1） 講演者一覧

表 3-12 人材ワークショップセミナーの講演者一覧

モデレーター	星代介 経済産業省 サイバーセキュリティ課 企画官
講演者及びタイトル	1. “Risk Assessment Training Seminar for Industrial Control Systems by IPA” 高見穣 独立行政法人情報処理推進機構（IPA）セキュリティセンター 脆弱性対策グループ エキスパート 2. “Core Human Resources Development Program for cyber security” 杉浦良祐 株式会社豊田自動車織機 IT ソリューションズ チーフエンジニア 3. “Introduction if International Cooperation Initiatives” 佐々木圭一郎 外務省 総合外交政策局 経済安全保障政策室 主査

3.3.14 クロージングセレモニー／Closing Ceremony

主催者を代表して、日米 EU の関係組織より閉会挨拶があった。

（1） 講演者一覧

表 3-13 閉会の辞の講演者一覧

開会挨拶	● 遠藤信博 独立行政法人情報処理推進機構（IPA） 産業サイバーセキュリティ

	センター（ICSCoE） センター長 ● Mr. Evangelos Ouzounis, Head of Unit for Policy Development and Implementation, European Union Agency for Cybersecurity（ENISA）

3.4 プログラムの総括

プログラム全体を通じ、日米 EU の産官学産官学の専門家から、電力系統をサイバー攻撃から守るための仕組みづくりや取組、再生可能エネルギー等の活用のための電力集約や電力融通の仕組みをサイバー攻撃から守るための政策や取組、サイバーセキュリティ確保に向けた政策や規格・フレームワーク・ガイドライン等の標準化プロセス、サプライチェーンの安全確保のための政策的取組、インシデントに対応するための情報共有の取組などについて、様々な政策の紹介や解説が行われた。また、ICSCoE や INL による実践的なワークショップも行われ、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、それらの具体的手法を体験的に習得する機会となり、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4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に関する国際動向調査事業） 報告書

2023 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４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に関する国際動向調査事業）報告書

令和４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に関する国際動向調査事業

株式会社三菱総合研究所

頁	図表番号	タイトル
19	図2-24	申合せの助言実績
19	図2-25	防衛産業サイバーセキュリティ基準の概要