資源エネルギー庁 御中

令和２年度エネルギー需給構造高度化対策に関する調査（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）報告書

2021 年 3 月 31 日

株式会社三菱総合研究所
デジタル・イノベーション本部

目 次

図 目 次

表 目 次

1. 調査の概要

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り組みが求められている。

電力分野においては、2016 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主力電源化に向けて、出力制御のオンライン化が進められるなど、発電・送配電事業を中心として、ネットワーク接続や デジタル技術の活用が広がりつつあるが、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、2021 年に東京オリンピック・パラリンピックを控え、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、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、2018 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り組みについて検討を行うことを目的とする電力サブワーキンググループが設置され、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について議論・検討が行われているところである。

また、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。

本調査事業では、国際的に議論が進められている電力分野の機器・システム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、当該検証の在り方や電力分野におけるセキュリティ規制・基準の在り方について、欧米やインド太平洋諸国とも国際的な議論を行うワークショップ（以下、WS という。）を運営し、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った。

1.2 調査実施概要

上述の調査目的を達成するために、次の項目に関連した調査・分析を実施した。

(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

電力分野における機器・システムを調達する際に考慮すべきセキュリティ検証項目とその評価方法について調査・検討を行った。令和元年度事業にて整理されたセキュリティ検

証・評価方法の検討案を踏まえながら、検証・評価項目の適切な分類方法、検証・評価のスキームとその活用方法等について分析を行い、その在り方を整理した。

調査にあたっては、諸外国において検討中の基準や取組等の動向、電力産業以外の調達時のセキュリティ検証・評価方法等についての調査結果を参考に、有識者等へのヒアリング調査や開催した勉強会における議論を通じて、詳細な検討を行った。

(2) インド太平洋地域向け日米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

インド太平洋地域向け日米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）は、経済産業省及び情報処理推進機構（IPA）産業サイバーセキュリティセンター（ICSCoE）が米国政府（国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁、国務省、エネルギー省）と連携し、2021 年 3 月 8 日から 12 日の 5 日間、完全オンラインで開催された。サイバーセキュリティウィークの実施にあたり、本調査事業では企画、運営、設備の手配などをはじめとする支援作業を行った。

1.3 略語の定義

本報告書で使用する略語の正式名称は次の通りである。

表 1-1 略語の正式名称

略語	正式名称
CC	Common Criteria
CISO	Chief Information Security Officer
CPIC	Cyber Product International Certification
CSA	Component Security Assurance
CSF	Cybersecurity Framework
CSIRT	Computer Security Incident Response Team
CSSC	Control System Security Center
DBOM	Digital Bills of Materials
ECM	Engineering Chain Management
EDSA	Embedded Device Security Assurance
HBOM	Hardware Bills of Materials
ICS	Industrial Control System
IEC	International Electrotechnical Commission
ISCI	ISA Security Compliance Institute
ISMS	Information Security Management System
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
NERC	North American Electric Reliability Corporation
PSIRT	Product Security Incident Response Team
PLC	Programmable Logic Controller
SBOM	Software Bills of Materials
SCADA	Supervisory Control and Data
SCM	Supply Chain Management

略語	正式名称
SCRM	Supply Chain Risk Management
UL	Underwriters Laboratories

2. 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

電力分野で用いられる制御機器や情報機器及びシステムについて、それらを調達する際に考慮すべきセキュリティ検証項目とその評価方法について調査・検討を行った。

令和元年度エネルギー需給構造高度化対策に関する調査（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）(以下、「令和元年度事業」という。）の調査成果であるスコアカード方式による評価方法案を踏まえながら、検証・評価項目の適切な分類方法及び改善点、スコアの検証・評価基準、検証・評価のスキームとその活用方法等についての調査・分析を行い、その在り方を整理した。

調査にあたっては、諸外国において検討中の基準や取組等の動向、電力産業以外の調達時のセキュリティ検証・評価方法等についての調査を行った上で、有識者等へのヒアリング調査や開催した勉強会の議論を通じて詳細な検討を行った。

なお、本調査を通じて実施したヒアリング調査の対象者属性と人数は次の通りであった。

- 国内外の有識者　のべ 15 者
  うち、国内の機器セキュリティの有識者のべ 10 者、国内の評価・認証機関の有識者 4 者、海外の電力関連規制機関 1 者
- 国内外の企業　のべ 20 者
  うち、国内の電力分野のユーザー企業のべ 2 者、海外のエネルギー関連事業者 1 者、国内の再生可能エネルギー事業者 6 者、国内セキュリティベンダ企業 1 者、国内セキュリティ評価企業 1 者、国内の電力関連機器メーカー9 者

2.1 調達時のセキュリティ検証・評価の大項目の整理

次に示す観点から調査を行い、電力分野における機器・システムの調達時にセキュリティ検証・評価を行うべき大項目について、整理及び改善を行った。

① 製造業における調達元組織視点のセキュリティリスクに関する調査検討
② サプライチェーンリスクマネジメントの海外動向に関する調査検討
③ 有識者等へのヒアリング調査
④ セキュリティ検証・評価の大項目の検討

2.1.1 調達時のセキュリティ検証・評価の大項目の原案について

本調査事業では、経済産業省より受領した調達時のセキュリティ検証・評価の大項目の原案に基づき、本調査事業内で実施した調査及び検討の結果を踏まえた整理と改善を行った。

調達時のセキュリティ検証・評価の大項目の原案は、令和元年度事業にて作成されたスコアカード方式による評価方法案に対して、製造業におけるユースケースの観点を踏まえた改善が行われたものである。はじめに、製造業におけるユースケースの観点を踏まえて行われた改善について、その概要を述べる。経済産業省により、ロボット革命・産業 IoT イニシ

アティブ協議会[1]の所属員等へのヒアリング調査等を通じ、製造業におけるサプライチェーンセキュリティへの対応を踏まえながら電力分野にも適用できる標準的な調達元組織とサプライヤ組織の関係の整理が行われた。

この結果において、部品の製造から製品の組み立て、利用、廃棄までの一連の SCM（サプライチェーンマネジメント）に加えて、製品の企画から設計、製造に至るまでの ECM（エンジニアリングチェーンマネジメント）を統合した全体プロセスにおいて、想定される脅威と被害を図示したものは図 2-1 の通りである。また、サプライヤから製品・サービスを調達する際のサプライヤ管理領域と、調達元組織に及ぶおそれがあるリスクの例は表 2-1 の通りである。

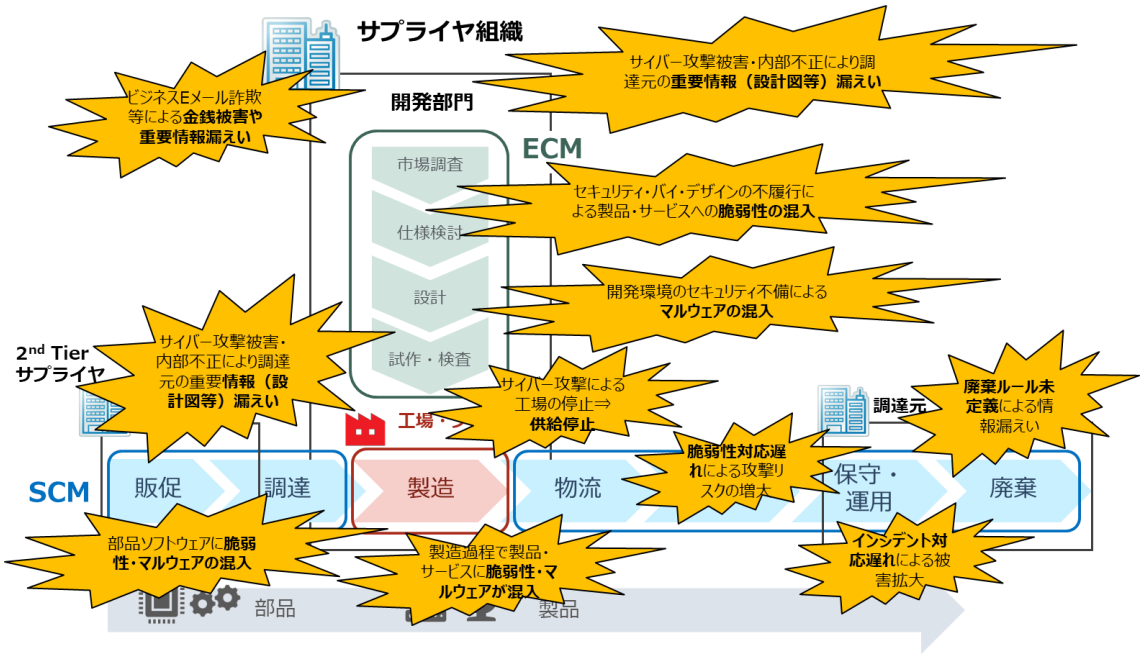


図 2-1 ECM 及び SCM 上に想定される脅威と被害

表 2-1 サプライヤ管理領域と調達元組織の関係

サプライヤ管理領域		調達元組織のリスク例
組織全般		BEC による金銭被害、共有した営業機密などの漏洩による企業競争力低下
製品・サービス	製品・サービス（本体）	欠陥仕様（パスワード固定など）、セキュリティ対策不備による情報漏洩、機能停止、人身事故などの被害
	開発プロセス	
	開発環境	マルウェア混入による情報漏洩・機能停止・人身事故などの被害、仕様書・設計図などの情報漏洩よる企業競争力低下

[1] ロボット革命・産業 IoT イニシアティブ協議会、RRI について、https://www.jmfrri.gr.jp/outline/

<table>
<tr><td colspan="3">制御システムセキュリティ</td><td>製造物へのマルウェア混入による情報漏洩・機能停止などの被害、工場・プラント停止による供給停止・不安定化</td></tr>
<tr><td rowspan="3">サプライチェーン上流</td><td rowspan="2">自組織向け</td><td>IT</td><td>共有した営業機密などの漏洩による企業競争力低下</td></tr>
<tr><td>OT</td><td>工場停止による供給停止・不安定化</td></tr>
<tr><td colspan="2">調達元向け</td><td>マルウェア・脆弱性混入による情報漏洩・機能停止・人身事故などの被害</td></tr>
<tr><td colspan="3">サプライチェーン下流
（調達元に対する保守・インシデント対応）</td><td>インシデント対応体制が不十分なことによるサイバー攻撃被害の拡大、調達リソースに脆弱性が発見された場合の対応遅れによるサイバー攻撃リスクの増大</td></tr>
</table>

2.1.2 サプライチェーンリスクマネジメントの海外動向に関する調査検討

サプライチェーンリスクマネジメントの海外動向に関して、調達時のセキュリティ検証・評価の大項目の考え方への影響を検討するため、最新の情勢について文献等による調査を行った。

(1) 米国サプライチェーンに関する大統領令（E.O. 14017）

2021 年 2 月 24 日に米国バイデン大統領は、米国のサプライチェーンをより回復力があるものとするための大統領令 14017[2]に署名した。具体的なサプライチェーンへの脅威としては、パンデミック等のバイオ脅威、サイバー脅威、気候変動及び異常気象、テロ攻撃、地政学リスク、経済競争等に言及しており、サイバー脅威は 2 番目に挙げられた。

より回復力のあるサプライチェーンは多様かつセキュアであるとされ、国内生産能力の増強、供給範囲の拡大、冗長性維持、十分な貯蓄、安全でセキュアなデジタルネットワーク、世界クラスの米国の生産拠点と生産要員を促進する要素に挙げた。加えて、これらの価値観を共有する同盟国やパートナーとの連携が重要であるとしている。

また、この大統領令はサプライチェーンの回復力を強化する戦略を策定するための体制と責任者を指定している。はじめに、先行 4 品目について、所管省庁の長官が大統領令署名から 100 日以内に、サプライチェーンリスクの特定と対応策についての報告書を大統領へ提出することを命じている。具体的な品目は、商務長官が半導体、エネルギー長官が大容量蓄電池（EV 用含む）、国防長官が重要鉱物等（レアアース含む）、保健福祉長官が医薬品及び医薬品有効成分である。

(2) 米国基幹電力システムのセキュリティ保護に関する大統領令（E.O. 13920）

米国大統領令 13920[3]は、2020 年 5 月に当時のトランプ大統領によって署名されたもので、

[2] the Executive Office of the President, Executive Order 14017 of February 24, 2021 “America's Supply Chains” https://www.federalregister.gov/documents/2021/03/01/2021-04280/americas-supply-chains

[3] the Executive Office of the President, Executive Order 14017 of February 24, 2021 “America's Supply Chains” https://www.federalregister.gov/documents/2020/05/04/2020-09695/securing-the-united-states-bulk-power-system

国防上の重要設備及び重要インフラへ電力を供給する基幹電力システムを、外国の敵対者からのサイバー攻撃等の脅威による被害を低減することを目的とした指令である。2021 年 1 月 20 日にバイデン大統領によって 90 日間の停止措置が執行されている。

大統領令 13920 の内容は、エネルギー長官に対して、基幹電力システムに関連した機器や設備の取引について、外国の敵対者の関与や、米国の重要インフラや国家安全保障への影響が認められる場合は、当該取引行為を停止する権限が与えるものであった。また、外国の敵対者に該当する国や人物の指定を行う権限、将来の取引に適用される要件を事前に設計する権限等も認められていた。

また、同大統領令に基づき、エネルギー省は、重要防衛施設に電力を供給する事業者が、その基幹電力系統制御システムに中国関連製品を調達することを禁止する行政命令[4]を 2020 年 12 月に公示していた。この根拠について、米国家安全保障局（NSA）によるサイバー脅威情勢判断と、中国の法体系等が挙げられている。調達禁止令の対象となる具体的な機器等は表 2-2 の通りである。公示内容には、2021 年 1 月 16 日からの発効予定と 3 月 17 日までの遵守証明書提出を求める計画が含まれていた。大統領令 13920 の執行停止措置を踏まえ、エネルギー省の行政命令も効力を発揮しない状態[5]となっている。

表 2-2 米エネルギー省による調達禁止令の対象機器

対象システム	重要防衛システムへの電力供給を行う基幹電力システム及び、当該システムへ直接納入される機器
対象機器種別	1. 69kV 以上の電圧に対応する負荷タップ切換器、冷却システム、衝撃圧力リレー等の制御および保護に関連するシステム 2. 高圧側定格電圧 69kV 以上の発電機昇圧（GSU）変圧器、負荷タップ切換器、冷却システム、圧力リレー等の関連する制御および保護システム 3. 69kV 以上で動作する高圧遮断器 4. 69kV 以上の無効電力設備（原子炉及びコンデンサ） 5. 上記いずれかの設備にインストールされている、または 1.から 4.にリストされている項目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

(3) ICT SCRM Task Force

米国国土保安省（DHS）は、2018 年 10 月に ICT Supply Chain Risk Management（ICT SCRM）タスクフォース[6]を設置し、続く 11 月に設置されたサイバーセキュリティー・インフラセキ

[4] Office of Electricity, Department of Energy, Prohibition Order Securing Critical Defense Facilities, https://www.federalregister.gov/documents/2021/01/06/2020-28773/prohibition-order-securing-critical-defense-facilities

[5] Office of Electricity, Department of Energy, Securing the United States Bulk-Power System Executive Order, https://www.energy.gov/oe/bulkpowersystemexecutiveorder （Updated: February 9, 2021）

[6] CISA, ICT SCRM, https://www.cisa.gov/ict-scrm-task-force

ュリティー庁の主導の下、サプライチェーン全体を対象としたリスクの特定と対応戦略の検討を進めている。この検討は官民共同の取り組みとして行われており、2021 年 3 月現在、18 の政府組織と 19 の IT 企業、17 の通信事業者が参加している。タスクフォース内には 5 つのワーキンググループが開催されており、情報共有から政策提言までが行われているが、サイバーセキュリティ脅威に限らず、サプライチェーンへの脅威がより広い観点から議論されている。

表 2-3 ICT SCRM に設置された WG と論点

No.	議題	主要論点
WG1	情報共有	・ ICT サプライチェーンリスクを軽減するために最も価値のある情報は何か ・ 情報共有の障壁となる法や課題 ・ 効果的に情報共有を行うためのフレームワーク
WG2	脅威評価	・ ICT サプライチェーンにとっての脅威は何か ・ 既存のリスク管理プラクティスとサプライチェーンリスク管理のフィットギャップ評価
WG3	適格の入札者の一覧及び適格のメーカーの一覧	・ 調達市場において、適格な入札者と製品メーカーを一覧化するための評価基準
WG4	ベンダの SCRM アシュアランステンプレート	・ 正規品、正規の販売店からの購入インセンティブを高める政策
WG5	COVID-19 影響評価	・ 新型コロナウイルスがサプライチェーンに与えた影響の分析と評価（2020 年追加）

設置から 2 年間の活動の成果としては、ICT サプライチェーンのリスクを低減するための戦略としての 6 つのステップをはじめ、主要な脅威カテゴリの分類や、入札者及びメーカーの適格性を検証するための質問票案等が示されている。それぞれの概要を表 2-4 に示す。

表 2-4 ICT SCRM の 2 年間の活動の成果

成果	主要論点
SCRM のための 6 つのステップ	組織がサプライチェーンリスクを認識し、効果的なプラクティスを成すために必要な 6 つのステップを整理したもの。 1. 人員を特定する 2. セキュリティとコンプライアンスを管理する 3. コンポーネントを評価する 4. サプライチェーンとサプライヤを知る 5. 第三者のアシュアランスを評価する 6. 結果をレビューする

成果	主要論点
ICT サプライチェーンにおける主要な脅威カテゴリ	SCRM の脅威と脅威減の分析のため、9 つの脅威カテゴリを整理したもの。NIST SP 800-161 のリスク管理プラクティスが参照されている。 1. 偽造部品 2. サイバーセキュリティ 3. 内部セキュリティの運用と管理 4. システム開発ライフサイクルプロセス・ツールに対する攻撃 5. 内部脅威 6. 経済的リスク 7. 広義のサプライヤーリスク（トレーサビリティ、出荷や輸送におけるリスク等を含む） 8. 法的リスク 9. 外的サプライチェーンリスク（自然災害リスクや地政学リスク等を含む）
ベンダ SCRM テンプレート	ICT 機器メーカーのサプライチェーンリスクマネジメントを評価するための標準質問票が作成された。質問票には次の内容を含む。 ・ セキュリティ：物理セキュリティ/サイバーセキュリティ/CUI の保護/人的セキュリティ/所有者とサプライヤの透明性 ・ インテグリティ：偽造品の防止と検出/製品の耐タンパ性 ・ レジリエンス：レジリエンス ・ クオリティ：サプライチェーンの統制と管理/ハードウェアとソフトウェアのセキュアな設計及び開発

2.1.3 有識者等へのヒアリング調査

国内の電力分野関連機器におけるセキュリティ対策の実態に基づいた意見を反映するため、メーカーの研究者や国際標準化活動に従事する技術者など、機器セキュリティの有識者 5 者、電力分野のユーザー企業 1 者、米国の電力関連規制機関 1 者にヒアリング調査を行った。

国内有識者に対しては、評価項目についての意見及び評価対象とすべき機器についての意見をヒアリングした。米国規制機関に対しては、大統領令に関連した動向を踏まえながら、電力分野関連機器のサプライチェーンリスク対策についての議論を行った。

評価項目に関しては、令和元年度事業の整理案をもとに充足性について質問した。その結果、大項目の範囲としては網羅されているが、国際標準との互換性や機器の種類、利用条件についての考慮が必要であるとの意見を得た。また、対象機器については、送配電機器が特に重要度が高いこと、送配電機器を制御するコントローラや通信機器はサイバー攻撃の経路となりえるため同様に重要であり、双方を対象とすることが妥当である旨の意見は共通していた。

有識者等へのヒアリング調査結果の概要を表 2-5 に示す。

表 2-5 有識者等へのヒアリング調査結果概要

質問項目	回答の概要
評価項目案の充足性について	・ 網羅性に不足はないが、目的に沿った重点項目の絞り込みが次の検討として重要である。 ・ 組織の情報セキュリティマネジメントやペネトレーションテストの実施をどの程度の深さで扱うかは課題である。 ・ 製品の種別による項目の適用要否の考慮が必要である。 ・ 項目への適合性を評価する際に、国際標準やデジュール標準に基づく評価が可能となる整理をすべきである。
対象機器の範囲について	・ 送配電機器は重要であり、送配電機器を制御する SCADA や PLC、遠方監視制御機器等も同等に重要になる。 ・ ネットワークへの脅威を考えればスイッチやルータのような通信機器も対象となる。重要度はシステムにより異なるが、ゲートウェイ機器の重要度は高いのではないか。 ・ 機能がシンプルで各社共通仕様が多い機器ほど評価対象に適しているだろう。 ・ 自社製品のみで構成される場合と、他社製品を組み込む場合では視点が異なり、他社製品はサプライチェーン上流の観点が求められる。 ・ グローバルな対応が求められる規制の動向は注視すべきである。
米国の電力機器のサプライチェーンセキュリティ規制について	・ エネルギー省による電力機器の調達禁止令は大統領令 13920 に基づくものであったが、大統領令が対象とした範囲の一部に対する指令の位置づけであった。 ・ 69kV という閾値は送電システムを対象とする時に用いられることがある値である。 ・ 電力設備で用いられる重要機器以外にも、機器の制御や通信を担う機器がサイバーリスクの観点から重要であるといえる。

2.1.4 セキュリティ検証・評価の大項目の検討

2.1.2～2.1.3 の調査結果を踏まえ、令和元年度事業で作成された調達時のセキュリティ検証・評価の大項目の改善について検討した結果、図 2-2 に示す 7 つの大項目（①～⑦）の体系へと改めて整理した。

開発プロセスと開発環境のリスクの観点から 7 つのカテゴリにとした大項目について、評価基準の概要と検討時の備考を表 2-6 に示す。なお、検討時の備考には、ICT SCRM 等で取り上げられている「直接的なサイバーセキュリティリスクにはあたらないサプライチェ

ーンリスク」を扱う場合の考慮点も示した。

さらに、検証・評価の対象とすべき機器について、その範囲の整理を行った。整理結果を表 2-7 に示す。

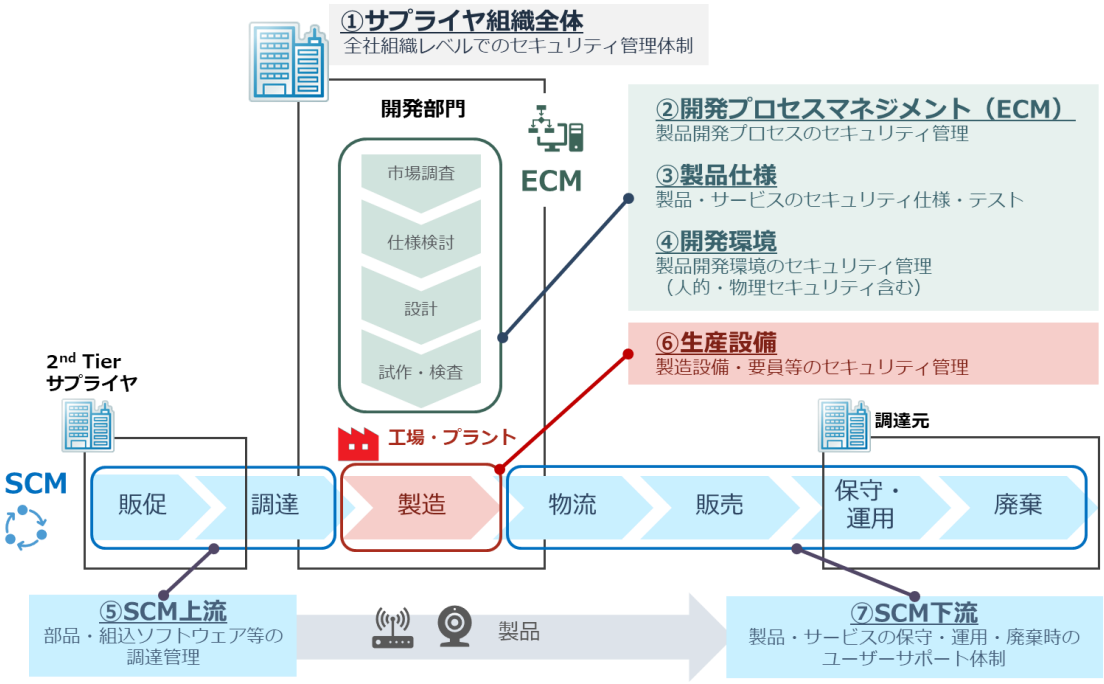


図 2-2 セキュリティ検証・評価の大項目

表 2-6 セキュリティ検証・評価の大項目 7 つのカテゴリ

検証・評価の大項目（カテゴリ名）	評価基準の概要	検討の備考
① サプライヤ組織全体（組織の管理体制）	電力関連機器ベンダが、全社組織レベルのリスク管理体制を構築し、情報セキュリティリスク等の管理・統制を行っていること	サプライヤ企業の組織単位で、情報セキュリティ管理体制を評価する。（経済的リスク、法的リスク、地政学的リスク等を評価する場合は、組織全体のカテゴリで扱う。）
② ECM（開発プロセスマネジメント）	電力関連機器ベンダが、製品開発プロセスのセキュリティ管理策を設計運用し、セキュリティに関連する設計の不備、欠陥仕様の実装、脆弱性試験の不足等が起こらないよう管理を実施していること	サプライヤ企業の組織もしくは部署単位で、ハードウェアとソフトウェアのセキュアな設計及び開発及び試験に関するプロセスについて整備状況を評価する。開発環境に関する評価は、④開発環境のカテゴリで扱う。
③ 製品仕様	電力関連機器そのものの仕様について、セキュリティ上の欠陥、既知の脆弱性の残留等がなく、脅威を防ぐ機能が有効に	機器種別ごとに仕様及びサンプル製品のセキュリティ仕様の充足性を評価する。

	働いていること	
④ 開発環境	電力関連機器ベンダが、当該製品を開発する環境のセキュリティ管理策を設計運用し、不正なプログラムの混入や内部不正による情報漏洩等が起こらないように管理を実施していること	サプライヤ企業の組織もしくは部署単位で、開発に用いる環境の管理計画、運用等を評価する。
⑤ SCM 上流（調達管理プロセス）	電力関連機器ベンダが、二次サプライヤから部品や組込ソフトウェアを調達する際のセキュリティ管理策を設計運用し、不正な部品やソフトウェアが完成品に含まれないよう確認を行っていること	組織単位もしくは機器種別ごとに、二次サプライヤから調達するハードウェアとソフトウェアの透明性とリスク管理状況を評価する。
⑥ 生産設備（組立・製造プロセス）	電力関連機器ベンダが、当該製品の組立・製造を行う工場等の設備、システムのセキュリティ管理体制を構築し、情報漏洩リスク等の管理・統制を行っていること	組織単位もしくは機器種別ごとに、製品の生産や組立に用いる工場等の管理計画、運用等を評価する。
⑦ SCM 下流（製品保守運用プロセス）	電力関連機器ベンダが、当該製品を調達するユーザー組織に対して、脆弱性対応に関連する情報やパッチの提供等、製品のセキュリティ機能を維持するための運用・保守・廃棄に関するサポートを行っていること	組織単位もしくは機器種別ごとに機器のユーザーへのサポート品質を評価する。 （偽造品の流通等の物流リスクを評価する場合は、SCM 下流のカテゴリで扱う。）

表 2-7 検証・評価の対象とする機器の整理

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、その他情報端末を含む
- 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
- 特に再エネ機器は、再エネ主力電源化の方針を踏まえ優先度が高いと考えられる

2.2 調達時のセキュリティ検証・評価の中分類・小分類の整理

調達時のセキュリティ検証・評価の中分類として、国内外の基準や取組についての情報を収集し、これを活用しながら大項目に対応する想定リスクや対策要件の整理を行った。また、小分類として各中分類に対応する対策実装例をまとめた。また、国際的な整合性の観点

から、諸外国の基準や取組との対応関係の整理を行った。

2.2.1 国内外の基準や取組の調査

国内外の基準や取組について、検証・評価における特徴や近年の改訂動向等について調査を行った。調査対象とした基準・取組とそれぞれの概要を表 2-8 に示す。

表 2-8 主要な基準・取組の概要

名称	概要
電力制御システムセキュリティガイドライン	日本技術規格委員会が 2016 年に策定したガイドライン。2019 年に改定された。電力制御システム等のサイバーセキュリティ確保を目的として、実施すべきセキュリティ対策が規定されたものであり、電気事業法に基づく技術基準の解釈において参照されている。システム全体の視点から要求事項が構成されており、勧告事項と推奨事項に分類される。
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）	経済産業省が 2019 年に策定したフレームワーク。Society5.0 における Connected Industries を対象に、新たなサプライチェーン全体のサイバーセキュリティ確保を目的としている。サイバー空間におけるつながり、フィジカル空間とサイバー空間のつながり、企業間のつながりの 3 つの層の視点から、ソシキ・ヒト・モノ・データ・プロシージャ・システムの 6 つの要素からサプライチェーン全体の信頼の基点と脅威及びその対策例を整理している。
IEC 62443 シリーズ	産業制御システムのセキュリティ技術仕様を記述した IEC（国際電気標準会議）規格シリーズ。大きく 4 つの規格群から構成され、コンセプト等のシリーズ共通の指針を定めた IEC 62443-1-1、ポリシーと手順を定めるマネジメント規格群 IEC 62443-2-1, 3, 4、システムのセキュリティ機能を定めた IEC 62443-3-1, 3-3、機器やコンポーネントのセキュリティ要求を定めた IEC 62443-4-1, 2 が発行されている。4-1 は開発プロセス、4-2 はコンポーネントの機能要件に対応する。 IEC 62443 シリーズに関連した認証制度として、JIPDEC による CSMS 認証（IEC 62443-2-1 準拠）、ISASecure による民間認証（IEC 62443-3-3 準拠, 4-1 準拠, 4-2 準拠）、CB スキームに基づいた IECEE 認証制度等が存在している。
Common Criteria 認証（ISO/IEC 15408）	IT 関連製品のセキュリティ機能の適切性･確実性を、ISO/IEC 15408 に基づいた評価機関の評価を、認証機関によって認証する制度。機器の種別に応じた特性を PP（Protection Profile）という検証要件に反映することが可能な制度を採用している。評価機関、認証機関はそれぞれ第三者性機関として、所定の要件を満たす必要がある。各国の評価機関によって作成された認証証は、国際的承認アレンジメント加盟国内で有効である。

名称	概要
Charter of Trust 公開文書	2018 年にミュンヘン安全保障会議で発表されたサイバーセキュリティに関するグローバルイニシアティブ。独シーメンスを中心にアリアンツ、シスコ、デル等様々な企業が参加している。日本からも三菱重工と NTT が加盟している。加盟企業は Charter of Trust の原則と基準要件に基づき、自社とサプライチェーンのサイバーセキュリティ強化を図ることで、ひいては社会全体のセキュリティ対策強化を狙う。10 の原則では、セキュリティバイデフォルトの原則やユーザー中心主義、透明性とレスポンスなど、シンプルな原則が並んでいる。
ISO/IEC 27000 シリーズ	ISO（国際標準化機構）と IEC（国際電気標準会議）のジョイント国際規格のうち、情報セキュリティに関連する規格シリーズ。ISO/IEC 27000 はシリーズ共通の概要として、ISMS（情報セキュリティマネジメントシステム）の枠組みを示しており、この ISO/IEC 27001 に ISMS 認証のための要件、ISO/IEC 27002 には実践のためのベストプラクティスが示されている。情報資産の保護に着目したセキュリティ管理がコンセプトであり、PDCA サイクルによる継続的改善のためのマネジメントを求める。サプライチェーンセキュリティに関する規格は ISO/IEC 27036 が発行されており、システムのライフサイクルを踏まえながら、取引先に求めるべき契約要件等を ISO/IEC 27002 の管理策と対応付けながら整理している。
NIST Cybersecurity Framework（NIST CSF）	米国国立標準研究所が 2014 年に発行した重要インフラ向けのサイバーセキュリティ対策のフレームワーク。サイバー攻撃への対策を主眼にしており、特定・防御・検知・対応・復旧の 5 つの機能から構成されるフレームワークコアが特徴である。攻撃の発生を前提とする考え方に基づいており、インシデントレスポンスを重視している。また、対策の成熟度は 4 段階のティアで定義される。2018 年にバージョン 1.1 に改訂され、サプライチェーンセキュリティ対策が強化された。
NIST SP 800 シリーズ	NIST（米国国立標準研究所）が発行する標準群で、SP 800-53 の政府情報システム向けのサイバーセキュリティ対策カタログから派生した対策標準が多数存在する。SP 800-82 は制御システム向け、SP 800-161 はサプライチェーンセキュリティ要件を拡張している。その他、政府調達時のサプライヤ向けの要求事項を抜粋して再構成した SP 800-171 が定められている。
NERC Critical Infrastructure Protection （NERC CIP）	NERC（北米電力信頼度協議会）が策定した北米の電力系統の信頼性保護を目的としたサイバーセキュリティ対策要件。FERC（連邦エネルギー規制委員会）の認可の下、米国の電力事業者のサイバーセキュリティ監査の基準に用いられている。対策カテゴリ毎に対策要求事項と監査基準、違反の重大度等の定義が定められている。2016 年に開発された CIP-013-1 がサプライチェーンセキュリティ対策要件を定めたもので、2020 年に正式適用として効力が認められた。

2.2.2 有識者へのヒアリング調査

セキュリティ検証・評価の運用における実効性を担保するために、機器セキュリティの有識者 5 者、電力分野のユーザー企業 1 者にヒアリング調査を行った。主に評価の基準、評価単位のあり方についてのヒアリングを実施した。

評価の基準については、プロセス管理やトレーサビリティのような透明性を重視すべき項目と機器のセキュリティ機能のような有効性を評価すべき項目を特徴毎に組み合わせること、評価基準と国際標準規格との整合性を十分考慮して広く国際的な相互認証運用を可能とすること、取得済の認証と同じ範囲の評価を再度強いることのないように配慮すること、などの意見を得た。また、評価結果の開示可能性を考慮した検討を行うべきとの指摘があった。

評価の単位については、事業者単位の評価を行う範囲と機器単位の評価を行う範囲を整理することが重要であり、機器単位の評価を行う範囲は特に必要性、有効性の高い項目に限定することで評価の実施にかかるコストを合理化することが可能という意見があった。

2.2.3 セキュリティ検証・評価の中分類・小分類の検討

2.2.1 及び 2.2.2 の調査分析結果を踏まえ、セキュリティ検証・評価の中分類・小分類の検討と整理を行った結果を示す。

(1) 中分類・小分類の整理

令和元年度事業の成果における中分類・小分類を踏まえながら、大項目の整理結果及び有識者へのヒアリング調査結果に基づいた修正を加え、再度整理した中分類の想定される脅威と期待される対策の概要を表 2-9 に示す。

また、これらの中分類に対応して、それぞれの対策例を小分類として整理し、関係する規格類との紐づけを行った結果の抜粋を図 2-3 に示す。

表 2-9 中分類の整理結果

評価項目の大枠（大項目）	具体的な評価項目（中分類）	
	想定される脅威	期待される対策の概要
① サプライヤ全体（組織の管理体制）：電力関連機器ベンダの組織全体におけるセキュリティガバナンス	• 機器に関連する情報資産の侵害（漏えい／改ざん／破壊／利用停止等） • 関連法規等への違反（業法・地域規制、プライバシー法規等）	• 経営層の責任と方針の明示 • 組織的リスクマネジメントに基づく情報保護 • 関連会社を含めた統制
		• 教育の実施によるミスの防止 • 内部不正の抑止
		• 組織端末への不正アクセスからの保護 • 組織端末へのマルウェア感染対策

評価項目の大枠（大項目）	具体的な評価項目（中分類）	
	想定される脅威	期待される対策の概要
	• インシデント発生時の被害拡大（機器関連インシデント対応の遅れ等）	• インシデントレスポンス体制の構築
	• サイバーセキュリティ以外のサプライチェーンリスク（地政学リスク、経済リスク、自然災害リスク等）	• 組織のリスクマネジメント全般
② ECM（開発プロセス）：電力関連機器ベンダの製品製造プロセスにおけるセキュリティ対策	• 不十分なセキュリティ要件	• 脅威分析に基づいたセキュリティ要件定義
	• セキュリティ要件の実装不備	• セキュリティ・バイ・デザイン • セキュア開発プロセスマネジメント（設計・開発・試験）
	• 脆弱な実装の検出漏れ	• セキュリティテスト標準（脆弱性識別試験・スキャン、ペネトレーションテスト計画）
③ 製品セキュリティ：電力関連機器に求められる一般的セキュリティ要件	• 機器、ユーザーへのなりすまし • 中間者攻撃	• 機器とユーザーの認証
	• 機器への不正アクセス	• アクセス制限とモニタリング
	• 機器への不正コマンドインジェクション	• 入力値検証
	• 機器の通信データ盗聴、改ざん	• 通信の暗号化、署名検証 • 適切な通信プロトコル選択
	• 機器データ、ソフトウェアの改ざん	• 耐タンパ性、データ保護
	• 機器へのサービス不能攻撃、災害・事故	• セーフモード • バックアップ
	• 機器固有アプリケーション、デバイスに起因する脆弱性への攻撃	• 機器固有の対策
④ 開発環境：電力関連機器ベンダの製品開発環境におけるセキュリティ対策	• 開発中モジュールへの不正機能組込み • ソースコードやデータの漏洩・改ざん	• 開発環境のセキュリティ管理 • 開発環境の整合性チェック
	• 外部コンポーネント由来の不正機能	• 外部環境との接続ルール管理 • 利用可能な外部コンポーネン

評価項目の大枠（大項目）	具体的な評価項目（中分類）	
	想定される脅威	期待される対策の概要
		トの制限
⑤ SCM 上流（調達管理プロセス）：電力関連機器のライフサイクル上流（調達）におけるセキュリティ要件	• 曖昧な責任分界のセキュリティ対策（対策漏れの発生）	• SLA の明示 • 責任者と問い合わせ窓口の明確化
	• 調達先組織における情報資産の侵害（漏えい/改ざん/破壊/利用停止等） • 調達先組織の内部不正 • 調達先組織における関連法規等違反	• 調達先企業における情報セキュリティ管理体制の確認
	• 調達先組織で発生したインシデント被害の拡大（調達部品に関連したインシデント対応の遅れ等）	• インシデント発生時の調達先企業との連携体制の確立
	• 調達部品（ハードウェア、ソフトウェア）の開発不備や設定ミスによる脆弱性の組込み	• 機器の構成及び機能に関する文書の開示（HBOM/SBOM） • 機器の設定に関するガイダンスの提供
⑥ 工場セキュリティ（製造プロセス）：電力関連機器ベンダの製品工場、製造施設、システムのセキュリティ対策	• 機器のソフトウェア改ざん、不正な部品の組込み	• 製造設備内の要員管理（外部委託先含む） • 端末の権限管理、コマンド制限 • 外部記憶媒体管理、マルウェア対策
	• 機器に関連する機密情報（ソースコード等）の持ち出し	• 重要ネットワークへのアクセス制御 • 機密データの暗号化
	• 機器供給の妨害	• バックアップ • 非常電源
⑦ 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下流（物流・保守・廃棄）におけるセキュリティ要件	• 曖昧な責任分界のセキュリティ対策	• SLA の合意 • 責任者と問い合わせ窓口の明確化
	• 配送時の不正行為 • （すり替え、不正機能の埋め込み等）	• 信頼できる配送ルートの確保
	• 偽造品の流通	• 適切な情報の流通、顧客コミュニケーション
	• 攻撃者によるゼロデイ脆	• 機器に関する不具合、脆弱性

評価項目の大枠（大項目）	具体的な評価項目（中分類）	
	想定される脅威	期待される対策の概要
	弱性の悪用	情報の受付 • 脆弱性対策情報発信のコントロール
	• 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
	• 機器の誤った（推奨外の）取扱いを狙った攻撃	• セキュリティマニュアルの提供（機器の堅牢化、安全な初期設定、推奨手順に従った廃棄）

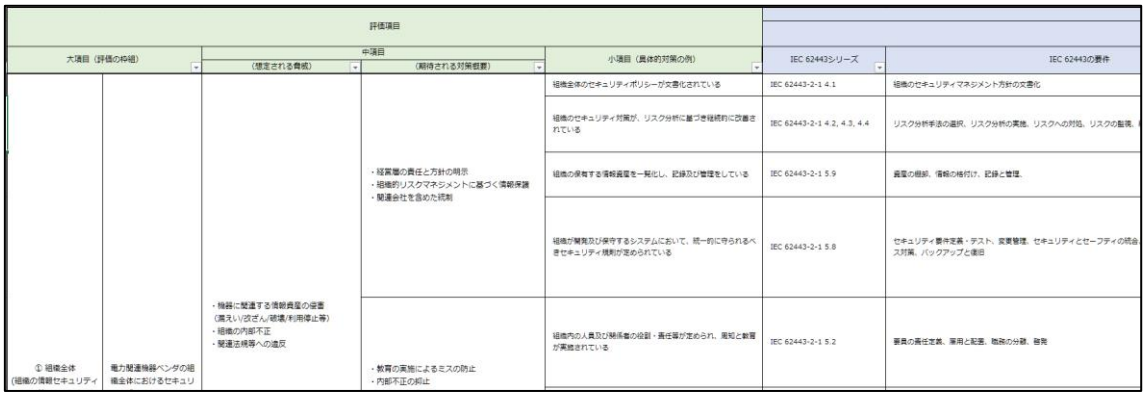


図 2-3 小分類と関連規格類のマッピング（抜粋）

(2) 国内外の基準や取組との関係性の整理

評価・検証の大項目と対応する脅威の整理結果を踏まえ、中分類の対策例と関係する認証制度・規格類の紐づけを行った。整理結果を表 2-10 に示す。表中に示した規格については、当該規格に関係する認証を取得済の場合に、評価プロセスを簡略化することが考えられる。

表 2-10 中分類と対応する規格類の整理

評価項目の大枠（大項目）	具体的な評価項目（中分類） 期待される対策の概要	関連する規格・認証制度
① サプライヤ全体（組織の管理体制）：電力関連機器ベンダの組織全体におけるセキュリティガ	• 経営層の責任と方針の明示 • 組織的リスクマネジメントに基づく情報保護 • 関連会社を含めた統制	• 国際標準規格としては、ISO/IEC 27001 に基づく ISMS 認証や IEC 62443-2-1 に基づく CSMS 認証が組織のセキュリティ管理対策の確認に該当する。 • 国別では、米国の NERC CIP に基づいた監査、SP 800-171 に基づく
	• 教育の実施によるミスの防止 • 内部不正の抑止	

評価項目の大枠（大項目）	具体的な評価項目（中分類） 期待される対策の概要	関連する規格・認証制度
バナンス	• 組織端末への不正アクセスからの保護 • 組織端末へのマルウェア感染対策	自己認証も同範囲を対象とした認証制度といえる。 • その他、多くの規格・標準等に組織の情報セキュリティ対策要件やベストプラクティスが提示されており、それらに基づいたセルフアセスメントも考えられる。
	• インシデントレスポンス体制の構築	
	• 組織のリスクマネジメント全般	• サイバーセキュリティ対策以外の様々なリスクを対象としており、それぞれに関する各組織のガバナンスレポート等を参照する形等が考えられる。
② ECM（開発プロセス）：電力関連機器ベンダの製品製造プロセスにおけるセキュリティ対策	• 脅威分析に基づいたセキュリティ要件定義	• 国際規格 IEC 62443-4-1 に基づき、制御機器・システムの開発プロセスの対策要件を評価する認証として、ISCI の SDLA 認証（組織単位）、CSA 認証（機器単位）がある。 • その他、ISMS 等の総合的な規格の一部に開発プロセスのセキュリティ要件の指針を含む。
	• セキュリティ・バイ・デザイン • セキュア開発プロセスマネジメント（設計・開発・試験）	
	• セキュリティテスト標準（脆弱性識別試験・スキャン、ペネトレーションテスト）	
③ 製品セキュリティ：電力関連機器に求められる機能的なセキュリティ要件	• 機器とユーザーの認証	• 制御機器・システムの機能的な対策要件に焦点をあてた国際規格には IEC 62443-4-2 があり、これに基づく認証としては、CSA 認証（機器単位）がある。認証試験には実機試験を含む。 • IT 機器では Common Criteria 認証にて機器の種別に応じたセキュリティ機能評価制度がある。 • その他、民間のセキュリティベンダによる機器ペネトレーション試験も行われている。
	• アクセス制限とモニタリング	
	• 入力値検証	
	• 通信の暗号化、署名検証 • 適切な通信プロトコル選択	
	• 耐タンパ性、データ保護	
	• セーフモード • バックアップ	
	• 機器固有の対策	
④ 開発環境：電力関連機器ベンダの製品開発環境におけ	• 開発環境のセキュリティ管理 • 開発環境の整合性チェック	• 制御機器・システムの開発プロセス管理の一環として IEC 62443-4-1 に含まれる。ISCI の CSA 認証（機器単位）、SDLA 認証（組織単位）

評価項目の大枠（大項目）	具体的な評価項目（中分類） 期待される対策の概要	関連する規格・認証制度
るセキュリティ対策	• 外部環境のセキュリティ管理（接続管理など） • 外部コンポーネントの検証と管理	などが関係する。 • ISO 27001 に基づく ISMS 認証や IEC 62443-2-1 に基づく CSMS 認証では開発及びサポートプロセスにおけるセキュリティ管理策を含む（組織単位）。
⑤ SCM 上流（調達管理プロセス）：電力関連機器のライフサイクル上流（調達）におけるセキュリティ要件	• SLA の明示 • 責任者と問い合わせ窓口の明確化	• 調達先企業の対策状況を認証の取得状況の開示により確認することに相当する。 • IEC 62443-2-4 では、システムベンダー等のサービス提供者としてのセキュリテイプログラム要件が規定されている。IECEE 認証制度では CB スキーム用の標準フォーマットが提供されている。 • 調達先企業の対策状況を監査やチェックリスト等を用いて確認することも考えられる。
	• 調達先企業における情報セキュリティ管理体制の確認	
	• インシデント発生時の調達先企業との連携体制の確立	
	• 機器の構成及び機能に関する文書の開示（HBOM/SBOM） • 機器の設定に関するガイダンスの提供	• IEC 62443-2-4 では、システムベンダー等のサービス提供者としてのセキュリテイプログラム要件が規定されている。IECCE 認証制度では CB スキーム用の標準フォーマットが提供されている。 • サポートサイトの URL 等により実際の公開情報を根拠とすることも考えられる。
⑥ 工場セキュリティ（製造プロセス）：電力関連機器ベンダの製品工場、製造施設、システムのセキュリティ対策	• 製造設備内の要員管理（外部委託先含む） • 端末の権限管理、コマンド制限 • 外部記憶媒体管理、マルウェア対策	• 制御システムの組織的管理策として IEC 62443-2-1 に基づく CSMS 認証が、制御システムセキュリティの観点から IEC 62443-3-3 に基づく SSA 認証がある。 • ISO/IEC 27001 の詳細管理策を工場向けに設計し、ISMS 認証で確認することも考えられる。
	• 重要ネットワークへのアクセス制御 • 機密データの暗号化	
	• バックアップ • 非常電源	

評価項目の大枠（大項目）	具体的な評価項目（中分類） 期待される対策の概要	関連する規格・認証制度
⑦ 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下流（物流・保守・廃棄）におけるセキュリティ要件	• SLA の合意 • 責任者と問い合わせ窓口の明確化	• ユーザー向けに①～⑥に示した対策や認証取得の情報を開示することに相当する。 • IEC 62443-2-4 では、システムベンダー等のサービス提供者としてのセキュリテイプログラム要件が規定されている。IECEE 認証制度では CB スキーム用の標準フォーマットが提供されている。 • SLA や責任者、問い合わせ窓口を公開している場合は、URL 等を直接参照することも考えられる。
	• 信頼できる配送ルートの確保	• 直接的な対応の見られるセキュリティの国際標準規格は見られないが、米国の ICT SCRM などでは制度的な検討も行われている。 • 組織の PSIRT 設置内容やガバナンスレポート等を参照する形等が考えられる。
	• 適切な情報の流通、顧客コミュニケーション	
	• 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	• 国際規格 IEC 62443-4-1 に基づき、機器サプライヤのセキュリティ対応ライフサイクルを評価する認証として、ISCI の SDLA 認証がある。 • 組織の PSIRT 設置内容を公開している場合は、URL 等を直接参照する形も考えられる。
	• アップデート機能の提供 • 修正プログラム、パッチの提供	
	• セキュリティマニュアルの提供（機器の堅牢化、安全な初期設定、推奨手順に従った廃棄）	

(3) 評価単位についての整理

評価項目に基づいた評価を行う単位について、有識者ヒアリング結果を踏まえながら、事業者単位で評価を行うべき項目と、製品単位で評価を行うべき項目を、中分類の単位で整理した。整理した結果を表 2-11 に示す。事業者単位の評価を行う項目については、一つの事業者内で複数の開発体制、管理体制を有する場合は、拠点単位や部署単位の評価を実施することも想定に含むものとする。

表 2-11 評価単位の分類（事業者単位／製品単位）

評価項目の大枠 （大項目）	事業者単位の評価 （中分類）	製品単位の評価 （中分類）
① サプライヤ組織全体（組織の管理体制）	・ 経営層の責任と方針の明示、組織的リスクマネジメントに基づく情報保護、関連会社を含めた統制 ・ 教育の実施によるミスの防止、内部不正の抑止 ・ 組織端末への不正アクセスからの保護、組織端末へのマルウェア感染対策 ・ インシデントレスポンス体制の構築 ・ 組織のリスクマネジメント全般	－（なし）
② ECM（開発プロセスマネジメント）	・ 脅威分析に基づいたセキュリティ要件定義 ・ セキュリティ・バイ・デザイン、開発プロセスマネジメント（設計・開発・テスト） ・ セキュリティテスト標準（脆弱性識別試験・スキャン、ペネトレーションテスト計画）	－（なし）
③ 製品仕様	－（なし）	・ 機器とユーザーの認証 ・ アクセス制限とモニタリング ・ 入力値検証 ・ 通信の暗号化、署名検証、適切な通信プロトコル選択 ・ 耐タンパ性、データ保護 ・ セーフモード、バックアップ ・ 機器固有の対策 （これらに対する実機試験を含む）
④ 開発環境	・ 開発環境のセキュリティ管理、開発環境の整合性チェック ・ 外部環境のセキュリティ管理（接続管理など）、外部コンポーネントの検証と管理	－（製品別に開発環境が異なる場合は製品単位）
⑤ SCM 上流（調達管理プロセス）	・ SLA の明示、責任者と問い合わせ窓口の明確化 ・ 調達先企業における情報セキュリティ管理体制の確認 ・ インシデント発生時の調達先企業との連携体制の確立	・ 機器の構成及び機能に関する文書の開示（HBOM/SBOM）、機器の設定に関するガイダンスの提供

評価項目の大枠 （大項目）	事業者単位の評価 （中分類）	製品単位の評価 （中分類）
⑥ 生産設備（組立・製造プロセス）	・ 製造設備内の要員管理(外部委託先含む)、端末の権限管理、コマンド制限、外部記憶媒体管理、マルウェア対策 ・ 重要ネットワークへのアクセス制御、機密データの暗号化 ・ バックアップ、非常電源	－(製品別に生産設備が異なる場合は製品単位)
⑦ SCM 下流（製品保守運用プロセス）	・ SLA の合意､責任者と問い合わせ窓口の明確化（共通） ・ 信頼できる配送ルートの確保 ・ 適切な情報の流通､顧客コミュニケーション ・ 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	・ SLA の合意、責任者と問い合わせ窓口の明確化（機器別） ・ アップデート機能の提供 ・ 修正プログラム、パッチの提供 ・ セキュリティマニュアルの提供（機器の堅牢化、安全な初期設定、推奨手順に従った廃棄）

2.3 検証・評価方法の活用方法の調査・検討

セキュリティ検証・評価方法について、その活用方法に関する調査・検討を行った。具体的には、機器・システムのセキュリティ検証・評価の主体・プロセスや、セキュリティ検証・評価の結果の共有・公表方法、セキュリティ検証・評価の結果の活用主体に関して調査・検討を行った。

2.3.1 認証・評価スキームに関する評価

情報機器・システムのセキュリティ検証・評価のスキームとして、CC（Common Criteria）認証、CSA (Component Security Assurance) 認証、CHECK に関する取り組みを調査・整理した。これら 3 つの認証スキームの概要を表 2-12 に示す。

表 2-12 CC 認証、CSA 認証及び CHECK の概要

	CC（Common Criteria） 認証	CSA (Component Security Assurance) 認証	CHECK (IT Health Check Service)
概要	IT 関連製品のセキュリティ機能の適切性･確実性を、ISO/IEC 15408 に基づき第三者（評価機関）が評価し、その評価結果を認証機関が認証する制度。	制御システム製品のサイバー攻撃に対する基本的な耐性を、IEC 62443-4-1 や IEC 62443-4-2 に基づき、第三者（評価機関）が評価し、その評価結果を認証機関が認証する制度。従来の EDSA 認証を拡張した位置づけである。	英国政府機関や重要インフラ事業者の保有する IT システムを対象としたペネトレーションテストに基づいた評価サービス。

	CC（Common Criteria）認証	CSA (Component Security Assurance) 認証	CHECK (IT Health Check Service)
検証・評価の実施主体	評価機関（テストラボ等）[7]	評価機関（テストラボ等）[8]	検証実施機関（Check Company）
スキームオーナー	各国セキュリティ機関（日本では IPA）	ISCI（ISA Security Compliance Institute）	英国 NCSC（National Cyber Security Centre）
評価・検証の対象	主に政府調達される IT 関連製品（ソフトウェア、ハードウェア、ファームウェア）及びシステム	制御システム製品（組込み機器を含むコンポーネント製品）	政府機関や重要インフラの IT システム
特徴	国際標準に基づく国際的な枠組み[9]が存在し、国内で認証を受けた製品は、協定に参加している各国においても認証された製品とみなされる。	製品自体のセキュリティ耐性だけでなく、ソフトウェア開発プロセスの妥当性も評価される。また、認証された製品は国際的に相互認証される。	Check Company の人材は、NCSC の審査により認定され、セキュリティクリアランス等が求められる。（ただし、民間資格との互換性も認められている。）
検証・評価にかかる費用	1,000 万円以上	1,000 万円以上	100 万円以上

(1) CC 認証の概要

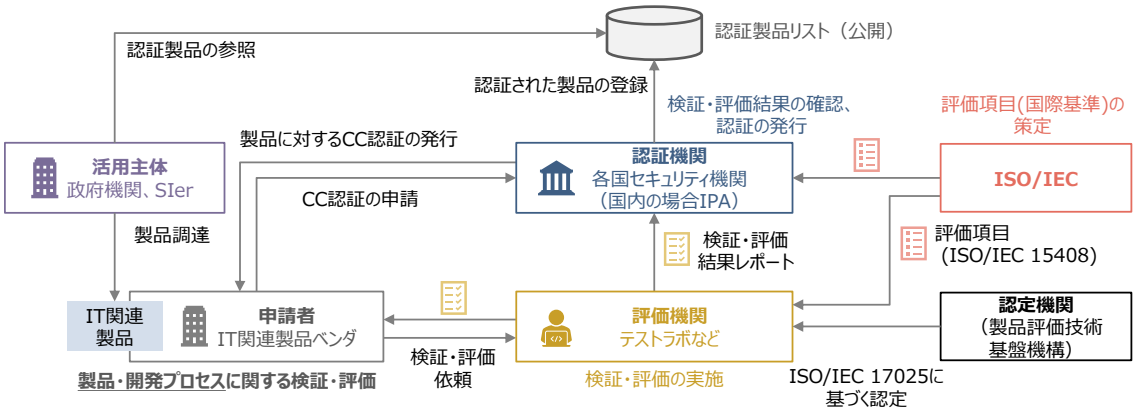
CC 認証は IT 関連製品のセキュリティ機能の適切性･確実性を、ISO/IEC 15408 に基づき第三者（評価機関）が評価し、その評価結果を認証機関が認証する制度である。IT 関連製品[10]の CC 認証取得のためには、認定機関によって認定された評価機関によって検証・評価が実施される必要がある。CC 認証の検証・評価スキームを図 2-4 に示す。評価機関によって作成された検証・評価結果レポートは認証機関（各国のセキュリティ機関）に報告され、検証・評価の結果に基づき、製品が認証を受ける。認証機関は、評価結果を確認した後、その製品に対する認証書を発行する。なお、認証は国際的承認アレンジメント加盟国でも通用する。

[7] 国内では、一般社団法人 IT セキュリティセンターや株式会社 ECSEC Laboratory が評価機関である。

[8] 国内では、CSSC 認証ラボラトリーが評価機関である。

[9] 日本を含む 33 か国（認証国 17 か国、受入国 14 か国）が加盟している。

[10] CC 認証の対象となる製品としては、ファイアウォールのように直接セキュリティに関係する機能を提供する製品に限らず、OS、データベース、あるいはグループウェアなど、保護すべき資源を保有する製品はすべて評価対象となる。



（出所）各種資料をもとに三菱総合研究所作成

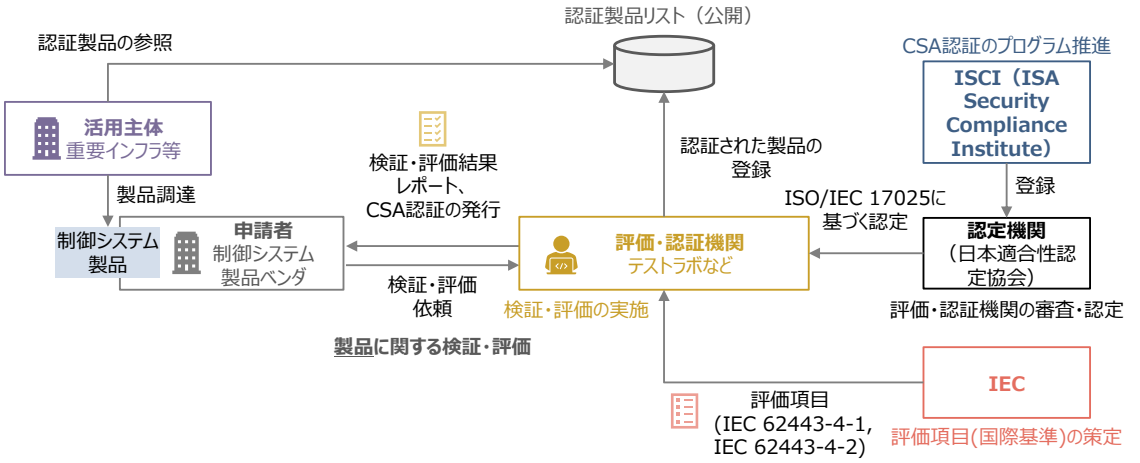
図 2-4 CC 認証の検証・評価スキーム

CC 認証は主に政府調達において活用される。そのため、活用主体は政府機関や SIer となる。認証された製品リストは公開[11]されており、調達時に CC 認証を受けた製品を確認することができる。

(2) CSA 認証の概要

CSA 認証は、制御システム製品のサイバー攻撃に対する基本的な耐性を、IEC 62443-4-1,4-2 に基づき、第三者（評価機関）が評価し、その評価結果を認証機関が認証する制度である。この認証制度は 2019 年 8 月から開始され、従来の EDSA 認証制度を拡張して組み込み機器も含めたコンポーネント製品も対象としている。IEC 62443-4-2:2019 の発行に合わせて一新されたが、特定製品の開発プロセス・セキュリティ機能・脆弱性評価を実施する点は EDSA 認証から大きく変化はない。CSA 認証はソフトウェア開発プロセスのセキュリティ評価、機能的セキュリティ評価、脆弱性テストの 3 つの観点から実施される。CSA 認証取得のためには、認定機関によって認定された評価・認証機関によって検証・評価が実施される必要がある。CSA 認証の検証・評価スキームを図 2-5 に示す。

[11] https://www.ipa.go.jp/security/jisec/certified_products/cert_listv31.html



（出所）各種資料をもとに三菱総合研究所作成

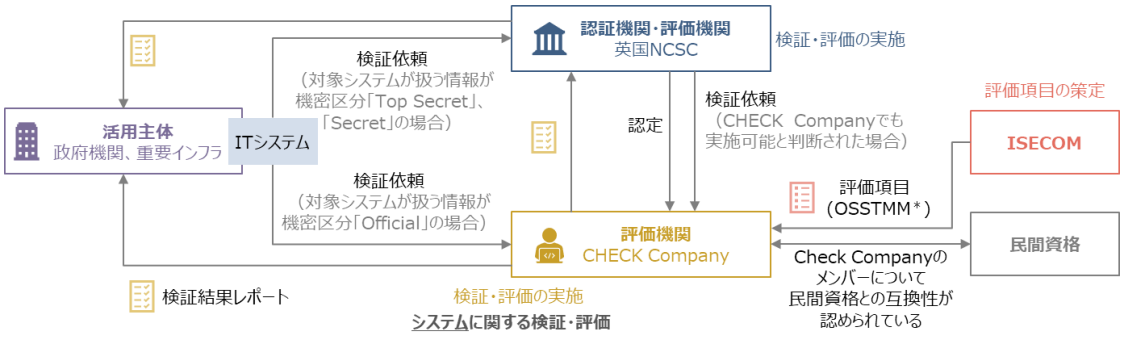
図 2-5 CSA 認証の検証・評価スキーム

CSA 認証は主に重要インフラにおける制御システムの調達において活用される。そのため、活用主体は主に重要インフラ事業者となる。従来の EDSA 認証に限れば、認証された製品のリストは、国内では CSSC 認証ラボラトリーによって公開[12]されているほか、国際的な各認証機関から認証された製品のリストは ISASecure によっても公開[13]されている。

(3) CHECK の概要

CHECK サービスでは、英 NCSC によって認定された評価機関（CHECK Company[14]）によって、政府機関や重要インフラの IT システムのペネトレーションテストが実施される。対象とする IT システムが扱う情報が機密区分「Official」の場合、NCSC に認定された民間の評価機関である CHECK Company によって検証の実施が可能である。機密区分が「Top Secret」、「Secret」の場合、NCSC に申請した上で、申請した内容に基づき NCSC が直接実施するか、適切な CHECK Company により実施されるかが判断される。Check Company の人材は、NCSC の審査により認定される。ただし、民間資格[15]との互換性も認められている。CHECK の検証・評価スキームを図 2-6 に示す。

[12] http://www.cssc-cl.org/jp/certified_devices/index.html
[13] https://www.isasecure.org/en-US/End-Users/IEC-62443-4-2-Certified-Components
[14] CHECK Company の一覧は NCSC の公式ウエブサイトで公開されている。
https://www.ncsc.gov.uk/section/products-services/all-products-services-categories
[15] 互換性のある民間資格として、CREST, Tiger Scheme, Cyber Scheme が認められている。



（出所）各種資料をもとに三菱総合研究所作成

図 2-6 CHECK の検証・評価スキーム

検証結果は依頼した機関に報告されるとともに、CHECK Company で実施された場合でも NCSC にコピーが提出される。一般には検証結果は公開されない。

2.3.2 認証・評価機関等へのヒアリング調査

現存する認証の実態を把握するために、認証・評価機関の有識者 4 者及びセキュリティ評価企業 1 者にヒアリング調査を実施した。「認証制度の主要スキーム種類とその違い」、「認証制度普及における典型的課題、関係者のインセンティブを高める仕組み」、「本調査で検討中のセキュリティ検証・評価に特徴的であると言える点、注意工夫すべきポイント」の 3 点についてヒアリングした。

認証制度のスキームには、認証機関が独自に発行するプライベート認証、認定機関による管理が行われる認証、国際標準スキームに則った国際相互認証の 3 つがあった。また、認証の種類としては、マネジメント品質認証と機器認証があった。さらに、例えば、製品認証スキームの国際標準を規定した ISO/IEC 17067（JIS Q 17067）では、タイプ 1～タイプ 6 までの区分があり、標準的な製品認証はタイプ 5 であるとのことであった。

認証制度への関係者のインセンティブを高めるための仕組みについては、機器等を調達する際の要件として認証の取得を要求する事例や、サイバーセキュリティ保険の仕組みにおいて、被保険者のリスク把握や料金の割引計算等に活用される事例の例示があった。特に、石油化学分野や船舶製造業などでは、こうした調達制度やサイバーセキュリティ保険活用への取組みが進んでいるとの意見があった。

製品軸でサプライチェーンリスクを検証する点やスコアカードによる製品セキュリティ評価である点が、ヒアリング対象組織が実施している検証・評価と比較して、本調査で検討中のセキュリティ検証・評価の特徴的な点として挙がった。また、コスト最小化に対する工夫や国際的に運営する際の注意点についての意見が多く得られた。

認証・評価機関等へのヒアリング調査の概要を表 2-13 に示す。

表 2-13 認証・評価機関等へのヒアリング調査結果概要

質問項目	回答結果概要
認証制度の主要スキームの種類とその違いについて	・ 認証の種類としては、マネジメント品質認証と機器認証がある。 ・ 製品認証スキームの国際標準を規定した ISO/IEC 17067（JIS Q 17067）では、製品認証スキームのタイプがタイプ 1～タイプ 6 まで区分されている。通常、製品認証という場合はタイプ 5 を指す場合が多い。 ・ 製品認証（タイプ 5）では、代表サンプルと同じ品質の製品の出荷まで認証機関が検査するが、適合性評価（タイプ 1）は代表サンプルと同じ品質であることは自己宣言する。 ・ 認証スキームには、認証機関が独自に発行するプライベート認証、認定機関による管理が行われる認証、国際標準スキームに則った国際相互認証の 3 つがある。 ・ 適合性評価では認証の更新は不要だが、3 年以上が経過した後は相手国で受け入れを拒否することができる。製品認証（タイプ 5）では年 1 回の工場検査が行われる。 ・ プロセス認証は一定期間ごとにプロセスの差分を確認することで更新が可能である。 ・ 機器認証では、小規模の変更に関しては影響度分析を自ら実施し、影響が小さいと認められる場合は再審査を省略することが可能である。
認証制度普及における典型的課題、関係者のインセンティブ高める仕組みについて	・ アセットオーナーのセキュリティ認証に対する意識が肝心である。認証の取得が調達要件に含まれた石油や船舶分野等では普及が早い。 ・ 文書化されたエビデンスの確認を求める要件は、被認証組織の作業負荷が大きいため制度の普及を阻害する要因にもなりやすい。確認する文書の範囲を絞りやすいプロセス認証が先に普及することで、セキュリティ性能の認証も後から普及しやすくなるものと考えられる。 ・ サイバー保険の仕組みと認証を関連付けることでユーザーにコスト面のインセンティブを創出することもできる。セキュリティ要件が調達先ごとに違うため、保険会社にとっても統一的な認証制度の存在は効果的である。
本調査で検討中のセキュリティ検証・評価に特徴的であると言える点、注意工夫すべきポイントについて	・ 製品軸でサプライチェーンリスクを検証する点、スコアカードによる製品セキュリティ評価である点は特徴的である。 ・ 被認証組織のリスクの特定からはじめる必要がある場合は、リスクの特定までと、リスクの特定後にフェーズを分割し、それぞれの料金を設定する必要があるだろう。

	・ 第三者機関はセルフアセスメントの妥当性を確認することや国際標準を採用することで認証申請者のコスト負担を最小化できる。 ・ 要求の主旨は同じまま異なる評価基準を許容する形式等で国別の差を許容する必要がある。 ・ 複数の評価機関のスキルを平準化するためには、認定機関の役割が重要になる。 ・ 評価方法と判定基準の策定を審議・承認するステークホルダーを委員とした認証制度委員会を構築する必要がある。 ・ 製品の種別と評価基準を対応付ける場合、評価は明確になるが、対象製品の拡大コストは大きくなる。 ・ チェックリストに対してエビデンスを申請者が紐づけを行った上で審査を依頼できるとよい。 ・ 調達の観点では、成熟度モデルのような明示的なランク付けがあるとよい。 ・ 審査のインターバルを検討する必要がある。

2.3.3 ユーザーニーズ把握のための企業向けヒアリング調査

ユーザー側のサプライチェーンの実態を把握するために、国内の再生可能エネルギー事業者 6 者、国内の電力関連機器メーカー9 者、海外の再生可能エネルギー関連事業者 1 者、計 16 事業者にヒアリング調査を実施した。「サプライチェーンリスクへの認識」、「望ましい製品調達プロセス」の 2 点についてヒアリングを実施した。

再生可能エネルギー事業者は、信頼している取引先と新規の取引先で対応を変えてサプライチェーンリスクに対応している場合があった。また、親会社の影響でグループ共通のルールが策定される場合もあった。製品調達プロセスとして、第三者が確認可能な仕組みやハイリスク製品をリスト化するブラックリスト型の仕組みを望む意見があった。

電力関連機器メーカーは、実績のある企業の製品を選択することでサプライチェーンリスクに対応している場合があった。サプライチェーンリスクとして、責任分界とサイバーリスクの管理を懸念しているという意見があった。また、製品調達プロセスとして、調達先の与信情報も含めて確認できる仕組みを望む意見があった。

今回ヒアリングをした海外の再生可能エネルギー関連事業者は、特にスマートメーター・ゲートウェイのサプライチェーンリスクを重視していた。ドイツでは、情報セキュリティ庁の定めるスマートメーターセキュリティ評価保証基準への対応が義務付けられており、今回ヒアリングした事業者も利用しているスマートメーターの適合性に注意を払っていた。スマートメーター・ゲートウェイへの具体的なサプライチェーンセキュリティ対策要件として開発及び物流プロセスの透明性・安全性の確保への取り組みが規定されており、事業者は必然的に基準を満たした製品を調達することとなるとの説明があった。

ヒアリング調査結果の概要を表 2-14 に示す。

表 2-14 ユーザーニーズ把握のための企業向けヒアリング調査結果の概要

ユーザー種別	サプライチェーンリスクへの認識について	望ましい製品調達プロセスについて
再生可能エネルギー事業者（太陽光、風力等）	・ 調達製品の納入時に製品データを取得し、管理している。 ・ 信頼している取引先の製品はサプライチェーンリスクの対策も行われていると認識している。新規の取引先は、提供された情報を読み込み、リスクが認められる場合には取引をしない。 ・ 中古で取得した施設には海外製品が多く用いられている場合があり、調達経路を辿ることが難しい。 ・ 親会社がサプライチェーンリスクに厳しい分野の事業を実施しているため、グループとして共通のルールが適用されている。 ・ 取引に規制がかかる可能性のある国の状況を注視している。	・ ベンチマークテストのようにセキュリティレベルを第三者が確認可能な仕組みがあるとよい。 ・ 継続可能な運用にする工夫が必要である。 ・ 調達する立場としては、ハイリスクの製品が個別に識別されているブラックリスト型であるとよい。 ・ 確認プロセスが機器メーカーにとって不合理な参入障壁にならないように配慮が必要である。
電力関連機器メーカー（出力制御ユニット、蓄電池、コージェネレーション機器等）	・ 自社製品には、実績のあるメーカーの製品を組み込んでいる。 ・ 自社製品の責任範囲外にあるサイバーリスクを懸念している。 ・ ガス会社からサプライチェーンリスク対策のための確認要望を受けるケースがあった。 ・ リスクマネジメントの一環として、新型コロナによる納期遅延等のサプライチェーンリスクやサイバーセキ	・ 調達先の企業経営における信頼性も考慮する必要がある ・ 取引先企業の情報セキュリティ管理を ISMS 認証の取得状況等を参考に確認する必要がある。 ・ 規制が適用される前に既にリスクのある製品は市場に出回ってしまう状況を解決できるとよい。

	ュリティリスクを管理している。	
海外の再生可能エネルギー関連事業者	・ 特にスマートメーター・ゲートウェイに関してはサプライチェーンリスク対応が実践されている。政府組織の主導によりサプライチェーン要件も含めたセキュリティ標準が開発されており、機器メーカーに適合が義務付けられている。	・ スマートメーター・ゲートウェイは、輸送時に特殊な鍵を有した輸送ボックスが必要である。 ・ サプライチェーンの具体的な要件として、開発と物流プロセスの透明性・安全性が求められ、試験に合格した機器を政府組織が承認している。従って利用者も承認済製品を調達することになる。

2.3.4 電力分野における機器・システムの調達時のスキーム案の検討

認証・評価スキームに関する文献調査及びヒアリング調査結果を踏まえ、電力分野における機器・システムの調達時のスキーム案の検討を行った。スキーム図の案を図 2-7 に示す。

組織の対策状況の評価等は主にセルフアセスメントでの実施を想定し、取得済の認証を合理的に活用する。

評価基準は国際標準等に基づく運用を想定し、最低限の各国固有のローカル調整を加えることを認めるものとする。ローカル調整済の評価基準は、相互認証調整機関の承認を受けることで評価結果を国際的に相互承認することを想定する。

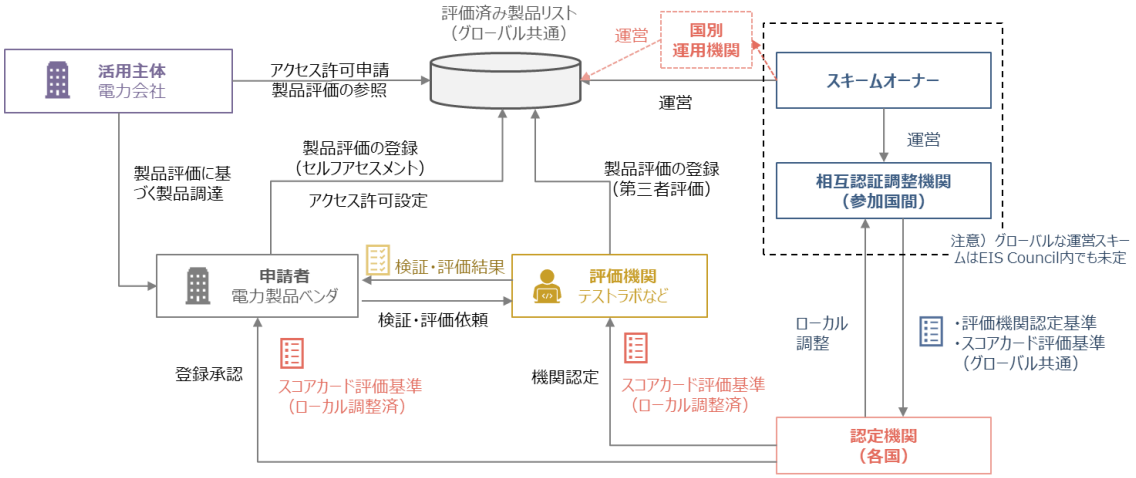


図 2-7 検証・評価スキーム図（案）

スキームの詳細設計を行うにあたり、更に検討が必要と考えられる課題として、次が挙げられる。これらの具体的な検討を行うにあたっては、ユーザー、メーカー、認証機関によって試行的な検証を行うなど、実務視点にたった丁寧な議論が行われることが望まれる。

- 評価基準及び評価手順の詳細（必要なエビデンスレベル、機器のセキュリティ試験の詳細項目・評価手順等）
- 項目別の望ましい保証水準（セルフアセスメント、サンプル品の適合性検査、機器認証試験の水準）
- 評価結果の開示内容・範囲、評価の更新タイミング
- ユーザーの SCRM コスト合理化によるビジネス効果の検証
- ユーザーへのインセンティブを向上するその他の施策（サイバー保険制度との関連付け支援等）
- スキームに必要な体制作り（認定機関・評価機関を担う組織、その他必要な役割）

2.4 電力以外の分野における機器・システムの調達時のセキュリティ検証・評価方法等

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・検討を行うに当たり、他の分野における同様の取組の状況を調査し、その特徴を整理した。調査対象とする分野は、電力同様に高いセキュリティ水準が求められ、機器セキュリティへの積極的な取組がみられる自動車、情報通信、医療分野とした。

2.4.1 自動車分野における機器・システムの調達時のセキュリティ検証・評価方法等

(1) TISAX（Trusted Information Security Assessment Exchange）

TISAX は、VDA（ドイツ自動車工業会）による自動車メーカーとサプライヤ間のサプライチェーンにおける情報セキュリティの評価・審査の標準化と結果の共有を制度化した取組である。サプライチェーンの信頼性を高めるために情報を透明化し、多重監査を避けることで効率化することを目的としている。2017 年から制度が運用開始され、頻繁な改版が行われており、2020 年 8 月からバージョン 5 に移行した。

自動車分野では、自動車メーカーや部品サプライヤへのサイバー攻撃によって、数多くの顧客情報の流出事案やソースコードの不正改変事案などが発生している。

TISAX の評価項目は、サプライチェーンの情報セキュリティへの脅威を中心に、各サプライヤの組織的な情報セキュリティマネジメントシステムを検証する構成をとっている。情報セキュリティマネジメントシステムの検証項目は、ISO/IEC 27001/27002 に対応付けられている。加えて、独自の項目としてドイツ連邦データ保護法への準拠、試作品の保護に関する管理策への対応を要求している。

評価の保証水準には、3 段階のレベルがあり、自己評価のみの AL1 から証拠文書、インタビュー、オンサイト検査等を要求する AL3 がある。評価結果は成熟度に基づき 0-5 の 6 段階で表される。評価結果は VDA から運営を委託された ENX（European Network Exchange）協会のポータルサイトに登録され、アクセス許可された範囲で共有される。

(2) ISO/SAE 21434

ISO/SAE 21434 は、ISO（国際標準化機構）と SAE（米国自動車技術者協会）の協力協定に基づいて開発された国際標準規格である。前身となった規格 SAE J.3061 は、自動車産業向けのサイバーセキュリティ・ガイドブックで自動車が他者に悪用される可能性を最小限に抑えつつ、新たな機能・サービスを実装する統合的システム設計のためのベストプラクティスを提供する目的で作成された。ISO/SAE 21434 の規格構成は SAE J.3061 の基本構成を踏襲しており、自動車の機能安全規格である ISO 26262 と整合する形で整理されている。

ISO/SAE 21434 はマネジメント規格であり、自動車のライフサイクル全体に渡ったサイバーセキュリティ対策フレームワークを規定している。フレームワークは 7 つの要素から構成されており、それぞれ「サイバーセキュリティマネジメント」「継続的サイバーセキュリティ活動」「リスクマネジメント」「コンセプト段階」「製品開発」「サポートプロセス」の活動段階を規定している。コンセプト段階からのセキュリティを組み込むマネジメントを重視している。

2018 年に公開した国連欧州経済委員会の自動車基準調和世界フォーラム（WP29）では、自動運転の分科会 GRVA において、サイバーセキュリティ法規基準を策定しており、ISO/SAE 21434 はこの基準に参照されている。国土交通省が発表した自動運転車の安全運転技術ガイドラインでも GRVA のガイドラインを参照することが求められている。自動運転車に関連した産業では対応が求められる可能性がある。

(3) UL VCSP

UL VCSP は、電気製品、産業機器、自動車部品等の広範な製品の検査試験を実施している UL の開発した認証プログラムである。UL は日本を含む 100 か国以上に事業展開しており、日本にも事業所を有している。

ネットワーク接続製品のソフトウェア脆弱性の検証を行う UL2900-1 規格に基づき自動車のサイバーセキュリティを検証するサービスを提供している。UL2900-1 は、ANSI（米国国家規格協会）及び SCC（カナダ規格審議会）の承認も受けている。

検証項目はサイバー脅威分析、リスク評価、脆弱性検査、ペネトレーションテスト等の試験を含み、ツールも活用した技術的な検証を多く含む点に特徴がある。特にコード解析を含むソフトウェアセキュリティの検証項目が豊富である。

民間認証であり準拠の義務は存在しないが、検査試験に合格することで UL マークの利用が許可される。UL マークの掲示によって顧客に向けて安心をアピールすることが可能であり、ビジネスインセンティブによる需要を生んでいる。

2.4.2 情報通信分野における機器・システムの調達時のセキュリティ検証・評価方法等

(1) EUCC Candidate Scheme

EUCC Candidate Scheme は、情報通信機器のサイバーセキュリティ認証を行う Common Criteria 認証を基に設計された EU 域内共通の EUCC 制度として運用を予定する制度設計案である。このスキームは、ENISA（欧州ネットワーク・情報セキュリティ機関）が策定した

EU 域内共通のセキュリティ認証制度に求められる要件を定めた EU Cybersecurity Certification Framework に準拠した候補スキームであり、2020 年 7 月に発表された。

評価基準は Common Criteria（ISO/IEC 15408）及び、IT セキュリティ評価共通手法（ISO/IEC 18405）に基づく。一方、保証レベルは 2 段階（substantial：相応、high：高度）であり、7 段階の EAL（評価保証レベル）を設定する Common Criteria とは異なる。運用は、欧州の Common Criteria 運用を担っている SOG-IS が担うことが予定されている。

スキームは EU 域内への適用を前提としたものだが、記述は第三国との相互認証についての条項が含まれており、EU 圏外の国家との取引にも影響を及ぼす可能性がある。

(2) Security Visa

Security Visa は、フランス ANSSI（国家情報システムセキュリティ庁）がサイバーセキュリティに関連する製品、サービスの堅牢性、セキュリティ品質を検証・評価し、フランス政府としての認証を行う制度である。

検証・評価基準はフランス国内で最高レベルのセキュリティ検証基準である CSPN 等に基づく。また、検証・評価は、ANSSI によって認定された評価機関によって実施され、ペネトレーションテストなどの技術的試験を含む。検証・評価レポートは ANNSI に報告され、認定済製品リストに掲載される。

評価には、サービスのセキュリティ品質を示す「Certification」と規制等への準拠性を保証する「Qualification」の 2 種類がある。Qualification は、主に政府機関や重要インフラ機関に納入される機器へ適用される。

2.4.3 医療分野における機器・システムの調達時のセキュリティ検証・評価方法等

(1) IMDRF ガイダンス（Principles and Practices for Medical Device Cybersecurity）

IMDRF ガイダンスは、IMRDF（国際医療機器規制当局フォーラム）によって 2020 年 3 月に取りまとめられた医療機器のサイバーセキュリティ対策の国際的な一般原則及びベストプラクティスを共有するガイダンスである。医療機器の使用に伴って起こり得るサイバーセキュリティリスクを最小化し、患者への危害を防ぐことを目的とし、ペースメーカーや輸液ポンプなどのソフトウェアを有する医療機器、もしくは医療用ソフトウェア製品を対象とする。

医療機器ベンダには透明性をもって情報を開示することを求め、医療機関には購入から利用、維持管理、廃棄に至るまでの一連のライフサイクルにおいて継続的なサイバーセキュリティ対策を行うために、役割分担と協調を実践することを求めている。

一般原則には、国際整合、製品ライフサイクルの全体、共同責任、情報共有が位置づけられている。ベストプラクティスは、機器の市販前後に分けて整理されている。市販前は、主にベンダ視点で、セキュリティリスクマネジメントプロセスに基づいたセキュアな設計開発の指針などが示されている。市販後の対策は、医療機関とベンダほかの役割と責任を分類しながら、意図する使用環境における機器の運用、関係者間の情報共有の実践、脆弱性情報の開示調整、インシデントレスポンスなどについて記載されている。

現時点で IMDRF ガイダンス自体に拘束力は存在しないが、日本国内では厚生労働省が、

令和 2 年 5 月に「国際医療機器規制当局フォーラム（IMDRF）による医療機器サイバーセキュリティの原則及び実践に関するガイダンスの公表について（周知依頼）」を公表している。この中で、現在の「医療機器のサイバーセキュリティの確保に関するガイダンスについて（平成 30 年）」に基づいた対策の推進に加えて、今後 3 年程度を目途に IMDRF ガイダンスを導入する方針について言及している。

2.5 勉強会の開催

国内のベンダ事業者等を集め、「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に係る勉強会」を 3 回開催した。本勉強会においては、本調査内容の報告・審議を行うとともに、評価項目のみならず、グローバル展開を念頭に置いた上で、国内の電力業界における評価スキームの構築に関わる議論を行い、今後の評価制度構築・実証を視野に入れた検討を行った。

2.5.1 勉強会の実施概要

第 1 回勉強会では、本年度の勉強会の活動方針や海外の評価スキーム等の関連動向について紹介した上で、スコアカード方式を用いた電力関連機器の評価における評価項目・対象機や検証・評価方法について意見交換を行った。

第 2 回勉強会では、各認証機関やベンダ企業の有識者へ実施したヒアリング結果を紹介した上で、CPIC の評価方法と運用スキーム案について意見交換を行った。第 2 回については、評価方法や運用スキーム案について詳細な意見をいただくため、書面開催とした。

第 3 回勉強会では、インド太平洋地域向け日米産業制御システムサイバーセキュリティウィークで発表された事例を紹介した。また、今年度の取りまとめと次年度以降に向けた検討を示し意見交換を行った。

【第 1 回】

日程	令和 3 年 1 月 7 日（木） 10:30～12:00
場所	オンライン開催
参加者	有識者 11 名（5 社）、オブザーバ 13 名、事務局 4 名
議題	1. 勉強会の活動方針について 2. 関連する動向について 3. 評価項目案の充足性、対象機器の範囲について 4. 検証・評価方法の活用方法について

【第 2 回】

日程	令和 3 年 3 月 17 日 （水）
場所	書面開催
参加者数	有識者 12 名（5 社）、オブザーバ 4 名、事務局 5 名
議題	1. CPIC 評価方法について 2. CPIC 運用スキーム案について

【第 3 回】

日程	令和 3 年 3 月 24 日（水）

場所	オンライン開催
参加者数	有識者 12 名（5 社）、オブザーバ 14 名、事務局 5 名
議題	1. インド太平洋地域向け日米産業制御システムサイバーセキュリティウィークについて 2. 本年度の取りまとめと次年度以降に向けた検討について

2.5.2 第 1 回勉強会の運営

第 1 回勉強会では、本年度の勉強会の活動方針として、ユーザーサイド（電力会社側）の意見も反映し、運用スキームの検討する方針を示した。また、電力関連機器等の国際的認証体制構築に関する海外と日本の動きを紹介した。

上記の内容を踏まえて、評価項目案の充足性と対象機器の範囲について、昨年度の議論内容や現状の素案を基に議論した。また、海外における検証・評価方法のスキームの調査内容を基に日本における運用スキームについて議論された。

2.5.3 第 2 回勉強会の運営

第 2 回勉強会では、事務局にて検討した評価方法・対象機器・運用スキームの案を紹介した。また、検討材料とした勉強会メンバーと各認証機関のヒアリング結果を参考情報と紹介した。上記の内容を踏まえて、評価方法と運用スキーム案について書面で意見を得た。

2.5.4 第 3 回勉強会の運営

第 3 回勉強会では、インド太平洋地域向け日米産業制御システムサイバーセキュリティウィークで発表された検証等の事例について紹介した。また、事務局にて検討した今年度の取りまとめと次年度以降に向けた検討について紹介した。上記の内容を踏まえて、次年度以降の方針・課題について議論された。

3. インド太平洋地域向け日米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

3.1 サイバーセキュリティウィークの開催概要

インド太平洋地域向け日米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）は、経済産業省及び情報処理推進機構（IPA）産業サイバーセキュリティセンター（ICSCoE）が米国政府（国土安全保障省サイバーセキュリティ・インフラストラクチャセキュリティ庁、国務省、エネルギー省）と連携し、2021 年 3 月 8 日から 12 日の 5 日間、完全オンラインで開催された。サイバーセキュリティウィークの実施にあたり、本調査事業では企画、運営、設備の手配などをはじめとする支援作業を行った。

本調査事業の検討当初では対面による開催も予定されていたが、新型コロナウイルス感染症のため、緊急事態宣言下での感染拡大防止や、主な参加者であるインド太平洋地域から日本への入国が困難であることなどから、完全オンラインでの開催することとなった。

サイバーセキュリティウィークは、表 3-1 に示す 3 つのプログラムにより構成された。①および②は、インド太平洋地域とサプライチェーンを共有する日本が、地域全体でのサイバーセキュリティ能力の向上と各国との連携強化を図ることを目的とした。③は、日本、米国、EU のポスト・コロナにおけるサイバーセキュリティに関するセミナーとして開催された。

表 3-1 サイバーセキュリティウィークにおけるプログラムの構成

①日米産業制御システムサイバーセキュリティ演習	
	プレトレーニングセッション（リモート・ハンズオン） リスクアセスメントワークショップ サプライチェーン・リスクマネジメントワークショップ 人材開発ワークショップ
②日米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	
	電力セクターワークショップ 1 電力セクターワークショップ 2 プロセスオートメーションセクターワークショップ スマートホーム・ビルセクターワークショップ
③日米欧サイバーセキュリティセミナー	
	政策・標準化ワークショップ ヘルスケアセクターワークショップ

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、参加申請者の中から 40 名が選定された。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（Operation 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、サイバーセキュリティウィークには、インド太平洋地域からの受講者に加え、ICSCoE の中核人事育成プログラムの研修生が参加した。加えて、日本、米国、欧州、インド太平洋地域の有識者等がオブザーバとして参加し、総計 100 名程度がオンラインで参加した。

3.2 ワークショップ等の概要

3 月 10 日～12 日の 3 日間に開催されたサイバーセキュリティウィークでのワークショップ等のタイムテーブルは表 3-2 の通りであった。ワークショップの各セッションの概要を以降に示す。

表 3-2 ワークショップ等のタイムテーブル

Day 1 (March 10, Wednesday)	
11:30-12:00	当日の登録
12:00-13:00	オープニングリマークとキーノート・スピーチ
13:00-13:30	ショート・ブレイク
13:30-15:00	サプライチェーン・リスクマネジメントワークショップ
15:00-16:00	ロング・ブレイク
16:00-17:30	スマートホーム・ビルセクターワークショップ
17:30-18:00	ショート・ブレイク
18:00-19:30	人材開発ワークショップ準備作業
Day 2 (March 11, Thursday)	
11:30-12:00	当日の登録
12:00-13:30	電力セクターワークショップ 1
13:30-14:00	ショート・ブレイク
14:00-15:30	リスクアセスメントワークショップ
15:30-16:30	ロング・ブレイク
16:30-18:00	電力セクターワークショップ 2
18:00-18:30	ショート・ブレイク
18:30-20:00	政策・標準化ワークショップ
Day 3 (March 12, Friday)	
11:30-12:00	当日の登録
12:00-13:30	プロセスオートメーションセクターワークショップ
13:30-14:00	ショート・ブレイク
14:00-15:30	人材開発ワークショップ
15:30-16:30	ロング・ブレイク

16:30-18:00	ヘルスケアセクターワークショップ
18:00-18:30	ショート・ブレイク
18:30-19:15	クロ―ジング・セレモニー

3.2.1 オープニングリマークとキーノート・スピーチ

司会者によるセッションの目的を説明する短い開会の挨拶から始まり、日本、米国、EU からの開会の挨拶が続けられた。日本、米国、EU の各政府からのビデオメッセージが事前に準備され、参加者に向けて映像が配信された。ビデオメッセージでの登壇者は次の通りであった。

- 長坂 康正
  経済産業副大臣
- Brandon WALES
  Acting Director, U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (DHS/CISA)
- Joseph YOUNG
  Chargé d'Affaires ad interim, U.S. Embassy Tokyo
- Khalil ROUHANA
  Deputy Director General, Directorate-General for Communications Networks, Content and Technology (DG Connect), European Commission

続いて、次の演題でキーノート・スピーチが行われた。

スピーカー	講演タイトル
Robert M. LEE CEO and Founder, Dragos	Threat Landscape of Industrial Cybersecurity

3.2.2 サプライチェーン・リスクマネジメントワークショップ

本セッションの目的は次の通りであった。

- 現在の脅威の状況と ICS SCRM のための政策に関する日本と米国の視点を提示する。
- 政府や産業界が適用しているサイバーセキュリティの課題と対策について議論する。
- SCRM 関連活動の改善と調和の可能性を見出す。

プログラムのモデレータは、佐々木 弘志氏（ICSCoE 専門委員、マカフィー株式会社）が務めた。パネルディスカッションは、「Industrial efforts for mitigating Supply Chain Risk」をテーマに行われた。参加したパネリストとプレゼンテーションのタイトルは次の通りであった。

パネリスト	プレゼンテーションのタイトル
Hiroshi SASAKI	What is SCRM? - Challenges and Classification -",

Advisor, Industrial Cyber Security Center of Excellence (ICSCoE)	
Takeshi YONEDA Member of Industrial Security Action Group, Robot Revolution & Industrial IoT Initiative (RRI), Mitsubishi Electric	Trustworthiness Profile Exchange across supply chain
Cheri CADDY Senior Advisor for Cybersecurity, U.S. Department of Energy (DOE)	ICS Supply Chain Vulnerability Testing
Dan DAGHER Program Manager for 5G, ICT SCRM, and Supply Chain Risk Analysis, DHS/CISA	CISA and Industry Activities to Mitigate Supply Chain Risk

3.2.3 スマートホーム・ビルセクターワークショップ

本セッションの目的は次の通りであった。

- ICS のサイバーセキュリティを成功させるための、日本と米国のスマートホームやビルの取り組みを伝える。
- インド太平洋地域の参加者が業界レベルで直面している課題と教訓をレビューする。
- スマートホームやビルのサイバーセキュリティの取り組みを前進させるために、調和と協力のための可能な機会を特定する。

プログラムのモデレータは、井上 裕司氏（エヌ・ティ・ティコミュニケーションズ株式会社 プロジェクト・ジェネラル・マネージャー）が務めた。パネルディスカッションは、「Guidelines and Measures for Smart Home and Building」をテーマに行われた。パネリスト間の対話に続いて、インド太平洋地域の参加者との質疑応答が行われた。

参加したパネリストとプレゼンテーションのタイトルは次の通りであった。

パネリスト	プレゼンテーションのタイトル
Michael FAGAN Computer Scientist, National Institute of Standards and Technology (NIST)	The Threat landscape of IoT devices
Yuji “UG” INOUE Project General Manager, NTT Communications Co, Ltd	Smart Building Security Guidelines and Good Practices
Yu INOSE Deputy Director of Cybersecurity Division, METI	Guidelines for Cyber/Physical Security Measures for Safe and Secure Smart Home
Jason CHRISTMAN Vice President and Chief Product Security Officer, Johnson Controls	Smart Building Cybersecurity

3.2.4 電力セクターワークショップ 1

本セッションの目的は次の通りであった。

- ICS のサイバーセキュリティを成功させるために、バルク発電や送配電などの伝統的な電力セクターにおける日本と米国の取り組みを共有する。
- 政策レベル、セクターレベル、個々の企業レベルでの課題、学んだ教訓、ベスト・プラクティスを議論する。
- グループ討議で得られたフィードバックに基づき、提言の改善と調和の可能性を見出す。

プログラムのモデレータは Tom WILSON 氏（Senior Vice President and Chief Information Security Officer Southern Company）が務めた。パネルディスカッションは、「Industrial efforts for keeping the light on」をテーマに行われた。パネリスト間の対話に続いて、インド太平洋地域の参加者との質疑応答が行われた。参加したパネリストとプレゼンテーションのタイトルは次の通りであった。

パネリスト	プレゼンテーションのタイトル
Takashi OISHI Deputy Director, International Business Development & Promotion Division, Tokyo Electric Power Services Co., Ltd. (TEPSCO)	Power Sector’s O&M under/after COVID-19
Tom WILSON Senior Vice President and Chief Information Security Officer, Southern Company	OT Security Focus Across Operations
Tim ROXEY President, Eclectic Technology	Effective Cyber Security And Supply Chain Controls
Hiroyuki HASEGAWA Assistant Manager, Chubu Electric Power Grid Co., Inc.	The Approach to Cyber Security Measures of Chubu Electric Power Grid

3.2.5 リスクアセスメントワークショップ

本セッションの目的は次の通りであった。

- リスクアセスメントワークショップの第二部として、ICS に関する日米のリスクアセスメント・ガイドラインを、インド太平洋地域の参加者に伝える。
- 典型的な ICS ネットワークへのガイドラインやベスト・プラクティスの適用について、参加者とのグループディスカッションを行う。
- グループディスカッションからのフィードバックに基づき、推奨ガイドラインの改善と調和の可能性を見出す。

プログラムのファシリテータは、Andrew BOCHMAN 氏（Senior Grid Strategist Idaho National Laboratory (INL)）が務めた。参加したスピーカーとプレゼンテーションのタイトルは次の通りであった。

スピーカー	プレゼンテーションのタイトル
Andrew BOCHMAN Idaho National Laboratory (INL)	Application of Consequence-driven, Cyber-informed Engineering (CCE)
Toshiyuki KUWANA Deputy General Manager, IT Security Countermeasures Dept., IT Security Center, Information Promotion Agency (IPA)	Risk Assessment Guide for Industrial Control System

ワークショップでは、インド太平洋地域の受講者によって、次のようにグループディスカッションを行い、最後にグループディスカッションの成果を発表した。

- サンプル産業用制御システムのリスク評価を CCE 手法に沿って机上で議論する。
- 各グループ A～H（1 グループ 5～6 名）は、ICSCoE および JPCERT/CC のグループディスカッションコーディネータがサポートした。

3.2.6 電力セクターワークショップ 2

本セッション電力セクター2 のワークショップの目的は、次の通りであった。

- ICS のサイバーセキュリティに関連した再生可能エネルギーマネジメントについて、日本と米国の電力セクターの取り組みをレビューする。
- 政策レベルでの課題とベスト・プラクティスを明らかにする。
- この分野における今後の推奨経路の改善と調和の可能性を特定する。

プログラムのモデレータは、梅嶋真樹氏（慶應義塾大学グローバルリサーチインスティテュート准教授）が務めた。パネルディスカッションは、「Mitigating the risk of Distributed Energy Resource as Cyber-Physical Systems」をテーマに行われた。パネリスト間の対話に続いて、インド太平洋地域の参加者との質疑応答が行われた。参加したパネリストとプレゼンテーションのタイトルは次の通りであった。

パネリスト	プレゼンテーションのタイトル
Masaki UMEJIMA Associate Professor, Global Research Institute, Keio University	Cybersecurity Guidelines for Energy Resource Aggregation Business (ERAB) in align with CSF and CPSF
Jonathan WHITE Director of Cybersecurity Program Office, National Renewable Energy Laboratory (NREL)	Emerging Challenges for Securing High Penetration DER Systems
Selvakumar Manickam Associate Professor, National Advanced IPv6 Centre (NAv6), University of Science-Malaysia	Malaysian perspective to DER system security in align with CPSF
Jason HOLLERN Program Manager: Cyber Security for Generation Assets, Electric Power Research Institute (EPRI)	Cyber Security Challenges and Trends in Renewable Generation”,

3.2.7 政策・標準化ワークショップ

本セッションの目的は次の通りであった。

- 日本、米国、EU から、成功するサイバーセキュリティ・アプローチ（ICS に焦点を当てて）のための政策・規制オプションを提示する。
- 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を明らかにする。

プログラムのモデレータは、Tonnie De KOSTER 氏（Adviser for the International Aspects of the Digital Transition, European Commission, DG CONNECT）が務めた。パネルディスカッションは、「Implementing a successful cybersecurity policy: the role of regulation, awareness building, standardization & certification, and international cooperation」をテーマに、日米欧から次の 3 者のプレゼンテーションが行われた。

- 欧州
  - Jakub BORATYŃSKI
    Deputy Director of Directorate CNECT H, Digital Society, Trust and Cybersecurity, DG Connect, European Commission
- 日本
  - Toshikazu OKUYA
    Director of Cybersecurity Division, METI
- 米国
  - Matthew KELLEY
    Associate Director, Strategy, Performance and Resources (SPR) - Cybersecurity Division (CSD), DHS/CISA

参加したパネリストは次の通りであった。また、インド太平洋地域の参加者からの質問を中心に、パネリスト間のディスカッションが行われた。

- 政府代表
  - Toshikazu OKUYA
    METI
  - Matthew KELLEY
    DHS/CISA
  - Aristotelis TZAFALIAS
    DG Connect - Cybersecurity Unit
- 産業界代表
  - Toshinori KAJIURA
    Chair of Cybersecurity Enhancement Working Group, KEIDANREN（Japan Business Federation）
  - Alberto DI FELICE
    Director for Infrastructure, Privacy and Security, DigitalEurope
- 標準化団体および標準化に関連する政府機関代表：
  - Xavier PIEDNOIR
    Head of External Relations, ETSIs

- Adam SEDGEWICK
  Senior Information Technology Policy Advisor, NIST

3.2.8 プロセスオートメーションセクターワークショップ

本セッションの目的は次の通りであった。

- ICS のサイバーセキュリティを成功させるための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）に対する日本と米国の取り組みを伝える。
- 課題、ユースケース、ソリューションを相互に共有し、政策レベル、産業レベル、個別企業レベルの活動から得られた教訓を共有する。
- 調和と協力の可能性を確認する。

プログラムのモデレータは、Marty EDWARDS 氏（Vice President, Operational Technology, Tenable）が務めた。参加したパネリストとプレゼンテーションのタイトルは次の通りであった。パネリストの講演に続いて、インド太平洋地域の参加者との質疑応答が行われた。

パネリスト	プレゼンテーションのタイトル
Eric KNAPP Director of Cybersecurity Research, Honeywell	A Close Look at the Top Threat Vectors into OT
Bryan OWEN Security Architect, OSIsoft LLC	Advancing the Fight Against Ransomware
Akiomi MONDEN Head of System Integration Technology Centre, Yokogawa Electric International Pte Ltd	The Only Viable Thing to Do: Security Program - ISA/IEC62443

3.2.9 人材開発ワークショップ

本セッションの目的は次の通りであった。

- ICS 人材育成のための日本と米国のフレームワークとアプローチを共有する。
- ICS 人材育成の課題、教訓、ベスト・プラクティスについて議論する。
- 組織内のコンピテンシーを測定・管理する方法を理解する。
- 人材育成に関連するガイドラインや手順の改善及び調和のための分野を特定する。

プログラムのファシリテータは、Shane D. STAILEY 氏（Senior Industrial Control Systems Cybersecurity Professional Training Opportunities and Strategy Lead,INL）が務めた。ワークショップは、「Managing Organizational Competency」をテーマに行われた。

参加者は小グループに分かれて、割り当てられたトピックについてディスカッションが行われた。各グループのコーディネーターは、JPCERT/CC（日本）、ICSCoE（日本）、DHS/CISA（米国）、NIST（米国）がそれぞれ務めた。グループディスカッションの後、選ばれた参加者のグループが議論の成果について発表した。

3.2.10 ヘルスケアセクターワークショップ

本セッションの目的は次の通りであった。

- ヘルスケア分野におけるサイバー脅威の状況について共通の理解を深める。
- ヘルスケア分野におけるサイバーセキュリティの課題と対策について、日本、米国、EU の視点を提供する。
- COVID-19 パンデミックの際にヘルスケア分野で得られたサイバーセキュリティの教訓を共有する。

プログラムのモデレータは、Evangelos OUZOUNIS 氏（Head of Unit Policy Development and Implementation Unit European Union Agency for Cybersecurity（ENISA））が務めた。参加したスピーカーとプレゼンテーションのタイトルは次の通りであった。各スピーカーからプレゼンテーションが行われた後、各 5 分間の質疑応答が行われた。

スピーカー	プレゼンテーションのタイトル
Lorena Boix ALONSO, Director, Digital Society, Trust and Cybersecurity DG Connect, European Commission	Developing a policy and regulatory framework for cybersecurity in healthcare: the EU example
Keiichiro OZAWA Regulatory Specialist, FUJIFILM Corporation, Japan	Cybersecurity of medical device manufacturer in Japan
Beau WOODS Senior Advisor and Strategist, COVID Task Force, DHS/CISA	Preparing for and responding to cyber threats in healthcare

3.2.11 クロ―ジング・セレモニー

クロージング・セレモニーでは次の日米欧の各機関の代表者から閉会の挨拶が行われた。

- Nobuhiro ENDO
  Director General, ICSCoE, IPA
- Zachary TUDOR
  Director of National & Homeland Security Directorate, INL
- Juhan LEPASSAAR
  Executive Director, European Union Agency for Cybersecurity (ENISA)

続いて修了者を代表して、3 者から挨拶が行われた。また、今回の演習を修了した参加者に、別途、修了証が贈られることとなった。

最後に、近年、サイバーセキュリティ対策は一企業や一国の取組では不十分であり、サプライチェーン全体で連携した対策が求められること、本演習プログラムを通じて、インド太平洋地域と日米欧の関係が強化され、増大するサイバー脅威への対処に向けたさらなる国際協力の基盤となることが期待されることが説明され、閉会した。

令和２年度エネルギー需給構造高度化対策に関する調査
（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）報告書

2021 年 3 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