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のあり方に関する詳細調査分析）

## 報告書

三菱総合研究所

デジタル・イノベーション本部

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。

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

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

## 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. 国内外の電力サイバーセキュリティに関する実態調査・分析
2. 電力システムのサイバーセキュリティリスクの分析
3. ワーキンググループの運営

# 2. 国内外の電力サイバーセキュリティに関する実態調査・分析

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

## 2.1 電力分野における近年のセキュリティインシデント事例

近年発生した電力分野におけるセキュリティインシデント事例を表 2-1 に示す。本表のとおり、近年、電力システムを狙うサイバー攻撃は増加傾向にあり、特に、ランサムウェア攻撃やウクライナ侵攻に伴うサイバー攻撃等が数多く発生している。国内においても、小売電気事業者がランサムウェア攻撃の対象となり、個人情報や取引先情報が流出した可能性がある。

表 2-1 電力分野における近年のセキュリティインシデント事例

| No. | タイトル | 国 | 発生時期 | 事例概要 |
|---|---|---|---|---|
| a | 小規模配電事業者に対するサイバー攻撃によるシステム停止・データ破損 | 米国 | 2021 年 11 月 | コロラド州の配電事業者 Delta-Montrose Electric Association（DMEA）の企業内ネットワークシステムがサイバー攻撃を受け、約 90%のシステムが破損等の影響により停止するとともに、過去 20～25 年のデータが破損した。攻撃によりシステムが停止したことで、料金の支払い処理、請求処理、アカウント情報変更等の顧客サポートサービスも停止した。 |
| b | 発電事業者の企業内システムに対するランサムウェア攻撃 | 豪州 | 2021 年 11 月 | クイーンズランド州政府が所有する電力会社である CS Energy の企業内ネットワークシステムがランサムウェア攻撃を受けた。攻撃には標的型ランサムウェア「Conti」が関連しているとされているが、詳細は公表されていない。攻撃を受けたネットワークを攻撃発覚後すぐに他ネットワークから分離することで、ランサムウェア攻撃による影響を最小化したと発表されている。この結果、発電システムへの影響は存在せず、電力の安定供給に影響はなかったと発表している。 |

| No. | タイトル | 国 | 発生時期 | 事例概要 |
|---|---|---|---|---|
| c | 衛星通信サービスに対する攻撃による風力発電リモート制御の停止 | ドイツ・ウクライナ | 2022 年 2 月 | 衛星通信サービス大手 Viasat の通信衛星「KA-SAT」サービスの通信モデムが標的型 DoS 攻撃を受け、当該サービスを利用するウクライナや欧州の組織からの衛星ブロードバンドへの接続が一時的に不能となった。本攻撃はロシアのウクライナ侵攻に関連した攻撃であり、EU、米国、英国、カナダ等は本攻撃がロシアによるものと正式に発表し、ロシアの行動を強く非難している。ドイツでは、当該モデムを使用する風力発電所が攻撃の影響を受け、複数の事業者が管理する 7,800 基を超える風力発電のリモート制御が不能となった。 |
| d | 地方自治体が管轄する電力管理システムに対するランサムウェア攻撃 | コスタリカ | 2022 年 4 月 | コスタリカの公営電気事業者であるカルタゴ市電力サービス管理委員会がランサムウェア「Conti」の攻撃を受け、Web サイトやメールなどを管理するシステムのデータが暗号化され、顧客がアクセスできない状態となった。管理システムが暗号化されたことにより、顧客は電気料金を支払うことができなくなったほか、顧客情報などが抜き取られた可能性もある。 |
| e | 公共料金管理システムに対するランサムウェア攻撃 | 米国 | 2022 年 6 月 | ルイジアナ州アレクサンドリア市の公共料金管理システムに対してランサムウェア「BlackCat/ALPHV」による攻撃が行われ、職員が公共事業データベースと請求システムへアクセスできなくなる事態が発生した。この攻撃による個人情報の流出はないと報道されているが、検針データの入力や市民への公共料金の請求書の送付が行えなくなった。 |
| f | 発電事業者の企業内システムに対するランサムウェア攻撃・データ漏洩 | ルクセンブルク | 2022 年 7 月 | ルクセンブルクに拠点を置く発電事業者 Encevo がランサムウェア「BlackCat/ALPHV」の攻撃を受けた。電力供給への影響は確認されていないが、顧客ファイル管理システムのデータが暗号化されたことで顧客ポータルが機能しなくなったほか、パスポート・請求書・電子メールを含む 150GB の機微情報が流失した可能性がある。 |
| g | 国内小売電気事業者に対するランサムウェア攻撃 | 日本 | 2022 年 9 月 | 国内の小売電気事業者が管理・運用するファイルサーバーがランサムウェア攻撃を受けた。ランサムウェア攻撃の結果、顧客の個人情報・法人情報や取引先の情報、業務委託先の個人情報・法人情報等が流出した可能性があるが、2022 年 11 月 21 日時点で当該情報の不正利用は確認されていないと報告されている。 |

| No. | タイトル | 国 | 発生時期 | 事例概要 |
|---|---|---|---|---|
| h | 大手電力会社に対するランサムウェア攻撃・データ漏洩 | インド | 2022 年 10 月 | インドの大手電力会社である Tata Power がランサムウェアグループ「Hive」によるランサムウェア攻撃を受けた。同グループは、攻撃によって窃取した機密性の高いデータを既に外部に漏洩させており、漏洩された情報の中には、従業員の個人情報のほか、取引情報、設計図、財務情報のような社内の機微情報等も含まれている。 |

## 2.2 米国における動向

本節では、米国における電力分野のサイバーセキュリティ対策やサプライチェーンリスクへの対策に係る動向等の調査結果を示す。調査対象一覧は表 2-2 に示すとおりであり、以降では、各動向の概要について示す。

表 2-2 米国における動向等の調査対象

| No. | 取組名・文書名 | 取組開始時期・発行時期 | 取組主体・発行主体 |
|---|---|---|---|
| 1-1 | Energy Sector Software Bill of Materials (SBOM) Proof of Concept (POC)[1] | 2021 年 1 月頃 | エネルギー省（DoE） |
| 1-2 | National Cyber-Informed Engineering Strategy[2] | 2022 年 6 月 15 日 | エネルギー省（DoE） |
| 1-3 | Cybersecurity Capability Maturity Model Ver.2.1[3] | 2022 年 6 月 30 日 | エネルギー省（DoE） |
| 1-4 | Priority Open Recommendations: Department of Energy[4] | 2022 年 7 月 5 日 | 会計検査院（GAO） |
| 1-5 | Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022[5] | 2022 年 9 月 12 日 | 国土安全保障省（DHS） |
| 1-6 | Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid[6] | 2022 年 10 月 6 日 | エネルギー省（DoE） |

[1] https://sbom.inl.gov/
[2] https://www.energy.gov/ceser/articles/us-department-energys-doe-national-cyber-informed-engineering-cie-strategy-document
[3] https://www.energy.gov/ceser/articles/department-energy-releases-version-21-update-cybersecurity-capability-maturity-model
[4] https://www.gao.gov/products/gao-21-597pr
[5] https://www.federalregister.gov/documents/2022/09/12/2022-19551/request-for-information-on-the-cyber-incident-reporting-for-critical-infrastructure-act-of-2022
[6] https://www.energy.gov/eere/articles/doe-cybersecurity-report-provides-recommendations-secure-distributed-clean-energy

| No. | 取組名・文書名 | 取組開始時期・<br>発行時期 | 取組主体・<br>発行主体 |
|---|---|---|---|
| 1-7 | Cross-Sector Cybersecurity Performance Goals (CPGs)[7] | 2022 年 10 月 27 日 | 国土安全保障省(DHS) |
| 1-8 | Joint FERC-DOE Supply Chain Risk Management Technical Conference; Notice Inviting Post-Technical Conference Comments[8] | 2022 年 12 月 23 日 | 連邦エネルギー規制委員会(FERC)・エネルギー省(DoE) |

### (1) DoE: Energy Sector Software Bill of Materials (SBOM) Proof of Concept (POC)

2021 年 1 月頃より、DoE は、傘下の国立研究所であるアイダホ国立研究所(INL)及び米国商務省電気通信情報局(NTIA)と共同で、エネルギー分野における Software Bill of Materials (SBOM:ソフトウェア部品管理表)に関する実証(POC)の開始を発表した。SBOM とは、ソフトウェアコンポーネントやそれらの依存関係の情報も含めた機械処理可能な一覧リストであり、SBOM には、ソフトウェアに含まれるコンポーネントの名称やバージョン情報、コンポーネントの開発者等の情報が含まれる。SBOM をソフトウェア・サプライチェーンの上流から下流に向かって組織を越えて相互共有することで、ソフトウェア・サプライチェーンの透明性を高めることが期待されており、特に、コンポーネントの脆弱性管理の課題に対する一つの解決策として期待されている。2021 年 4 月 28 日には、POC の憲章である「Energy Sector SBOM POC Charter」を発表し、POC の目的や目標、POC における主な検討課題等が示されている。具体的な内容は表 2-3 に示すとおりである。

表 2-3 INL によるエネルギー分野の SBOM POC の概要

| | |
|---|---|
| 目的 | ● エネルギー分野での SBOM の活用について調査し、SBOM 活用を促進するとともに、ソフトウェアコンポーネントの透明性を高める。<br>● NTIA における SBOM の各 WG 活動の結果を活用しつつ、オープンな場において SBOM 導入のための技術やプロセス開発を促進する。 |

[7] https://www.cisa.gov/cpg
[8] Joint FERC-DOE Supply Chain Risk Management Technical Conference; Notice Inviting Post-Technical Conference Comments

| | |
|---|---|
| 目標 | ● エネルギー分野でのサプライヤー、アセットオーナー（事業主体）、サードパーティベンダー等を巻き込んだ多様な利害関係者を集めて、SBOM に関する知識と経験を共有する。<br>● エネルギー分野におけるベンダーとアセットオーナーの間で SBOM 情報の作成と交換を促進する。<br>● エネルギー分野において SBOM を活用するためのユースケースを調査する。<br>● SBOM 技術の実装上の課題と緩和策を特定する。 |
| 主な実施内容[9] | ● テストケースの作成やデモンストレーション等を含みながら、SBOM の作成、配布、使用について議論するワークショップを開催する。<br>● エネルギー業界へソフトウェア等を提供するサプライヤーによって作成された SBOM 及びサプライチェーンリスクの軽減のためにアセットオーナーに対して作成された SBOM を使用する。<br>● POC 活動とそこから得られた知識や課題をまとめたレポートを 1 つ以上作成する。 |
| POC における主な検討課題 | ● POC の関係者は多様であり、SBOM に関する知識レベルが様々であるため、関係者に一律の行動方針を定めることは難しいこと。<br>● 提供された情報が悪用される可能性があることに不安を感じているサプライヤーが存在すること。<br>● 容易に SBOM を作成・利用するようになるためには、具体的なユースケースや技術的な障壁を見極める必要があること。<br>● SBOM 作成のツールは既に開発されているが、脆弱性管理やライセンス管理に係る SBOM ツールは限定的であること。<br>● SBOM の作成、配布、利用のために実行可能な手順に到達するには、多様な視点と関心を調整する必要があること。 |
| 備考 | ● 今回の POC は NTIA によって開発された SBOM フォーマットや概念に基づいて実施する。<br>● 商用ツールが SBOM の活用に不可欠であるとしつつ、今回の POC では特定の商用ツールの推奨や宣伝は実施しない。 |

## （2）DoE：National Cyber-Informed Engineering Strategy

DoE は、エネルギー分野におけるレジリエントなインフラシステムの運用を目的に、エネルギー分野において Cyber-Informed Engineering（CIE）[10]を推進するためのガイダンスとして「National Cyber-Informed Engineering Strategy」を 2022 年 6 月 15 日に発表した。

本文書では、インフラシステム運用のあるべき姿として、「サイバー攻撃に直面しても、重要な機能を

[9] 新しいツールや技術の開発、特定商用ツールの使用はスコープ外とされている。
[10] システムの設計から運用に至るライフサイクルの各段階でセキュリティ対策を考慮する手法であり、2017 年にアイダホ国立研究所（INL）によって提案された。

継続的に提供可能なレジリエントな運用を行えること」「レジリエントなシステムとなるように設計段階においてもセキュリティ対策を施すことができること」を掲げている。それに対して、現状を「セキュリティ対策がシステム設計段階では考慮されず、テスト・運用開始時のみで考慮される」「設計段階でセキュリティ対策を行うためのガイドラインが存在しない」「システム設計段階で携わるエンジニアにおいて、十分なセキュリティの知識がない」と評価し、このギャップを解消すべく、表 2-4 に示す 5 つの取組を定義している。

表 2-4 CIE のあるべき姿の実現に向けた課題に対処するための 5 つの取組

| | |
|---|---|
| CIE に関する意識醸成 | ● エネルギー部門の規制機関、標準化団体、業界団体と直接連携し、CIE によるリスク低減のメリットについて認識を深める。<br>● エネルギー部門の産業基盤と直接連携し、CIE 実施による費用対効果と投資収益率に対する認識を深める。<br>● 専門規格のコミュニティを巻き込み、既存及び新規の政策、規格、ガイドラインに CIE を含めるためのサポート体制を構築する。<br>● エネルギー産業界及びそれ以外のステークホルダーを巻き込み、CIE 原則を開発・成熟させ、CIE ガイドライン及び標準開発に反映できるような技術要件に変換する。<br>● CIE の採用を促進するために、補助金の支給や費用の負担を行う。また、CIE カリキュラムの開発を促進するための教育政策の策定を行う。 |
| CIE 実践者の育成教育 | ● CIE を、EIT(Engineer in Training)[11]や PE(Professional Engineer)[12]資格などの正式な工学資格認定プログラムに取り入れる。<br>● CIE のオンライン及び対面教育の開発を支援し、大学や研修プログラムが自由に採用できるオープン教育リソースとして提供する。<br>● CIE の標準化されたカリキュラムを軍の士官学校、政府の訓練施設及び民間のサイバーセキュリティ訓練センターに導入する。<br>● CIE カリキュラムと認定資格に対する意見と検証の情報源として、エネルギー部門の産業基盤における主要な場(業界団体、製造協会など)を選定する。 |
| CIE に関する研究開発 | ● CIE をエネルギー部門産業基盤システムに適用し、成功事例、ケーススタディ、教訓を特定し、文書化することで、全体的な知識体系を構築する。<br>● CIE を適用することによって低減又は排除される結果の経済的価値を定量化する方法を開発する。<br>● 設計者・製造者が CIE を適用することを支援する CIE ツール、ケーススタディ及び教訓のオープンソースライブラリを作成し、維持する。<br>● CIE 教育指針の立案や CIE 運用から得られた課題の抽出を行う。 |

[11] NCEES(National Council of Examiners for Engineering and Surveying)が米国で使用している専門職の称号で 2 つの要件(「ABET 認定の光学プログラム又は理事会に承認されたカリキュラムを修了」「NCEES の 6 時間工学基礎試験に合格」)を満たすと認定される。

[12] 米国の各州が州ごとに設けているエンジニアの公的資格で、公共の安全・健康・福祉に奉仕するために、責任のある立場でエンジニアとして活動する者に要求される資格である。

| | |
|---|---|
| 既存インフラシステムへのCIE実装 | ● CIEを適用することで国家安全保障を支援できる既存のインフラを特定し、優先順位をつけるための結果駆動型プロセスを開発する。<br>● 防衛省の電気インフラなど、エネルギー部門の重要インフラへのCIEの適用を優先する。<br>● CIEをいつ、どのように適用するかを評価するのに役立つ実施計画や意思決定支援ツールを開発する。<br>● 調達の意思決定にCIEを組み込み、優先度の高い既存インフラの安全確保にCIEを適用して投資する資産所有者にインセンティブを与える。 |
| 将来的なインフラシステムへの実装 | ● 既存のインフラにおける脆弱な設計パターン（既存インフラシステムへの活動から抽出）を特定し、これらのパターンを排除する新しい設計を開発し、実証する。<br>● CIEを具体化するために、設計、製造に関する国際標準の作成又は改訂を推進する。<br>● エネルギーインフラシステムの連邦資金による研究開発プロジェクトに、CIEを組み込むことを義務付ける。<br>● 州の公益事業委員会、公共サービス委員会及びその他の州の規制機関に働きかけ、CIEの要件をその規制枠組みに統合させる。 |

## （3）DoE：Cybersecurity Capability Maturity Model（C2M2）Ver.2.1

DoEは、C2M2 Ver. 2.0に対する事業者のテスト結果及びフィードバックを基に改定した「C2M2 Ver. 2.1」を2022年6月30日に公開した。C2M2は、組織におけるサイバーセキュリティの取組の評価・改善に活用できるサイバーセキュリティ能力成熟度モデルであり、Ver.2.1は、10のドメイン、43の目標、356 の実施項目によって構成される。今回の改定では、高度化した技術と脅威に対応することを目的として実施項目が追加されたほか、NIST CSF との整合性を高めるための修正やユーザビリティ向上のための修正・機能の追加が施された。主な変更点を以下の表 2-5 に示す。

表 2-5 C2M2 Ver. 2.1における主な変更点

| | |
|---|---|
| NIST CSFとの整合性の向上 | ● C2M2 Ver. 2.1では、NIST CSFとの整合性を向上させるために、実施項目を追加した。 |
| 既存の実施項目の改善 | ● 明確さの向上のために以下に示す変更を主に加えた。<br>➢ 明確性と一貫性のために、一部の実施項目の文言を変更した。<br>➢ 重複を排除するために、一部の実施項目を削除した。<br>➢ モデルで扱うサイバーセキュリティ活動の包括性を向上させるために、実施項目を追加した。（Ver. 2.0では299項目であったが、Ver. 2.1では356項目となった。）<br>➢ 人材管理領域における目標の順序を変更し、明確性を向上させた |
| 目標の名称の変更 | ● 各管理目標の名称にドメイン名を追加した。また、一部の管理目標について、その意図や実施内容を明確にするため名称を変更した。 |

| | |
|---|---|
| 入門教材の充実 | ● モデルに対する理解を向上させるために、モデルのコンセプトの説明文及び各ドメインの説明文を更新した。 |
| ガイダンスとユーザビリティの追加 | ● C2M2 の自己評価の円滑化、一貫性、正確性を向上させるために、ガイダンスを追加した。<br>● 大部分の実施項目のヘルプテキストを拡充した。 |
| 自己評価ツールの更新 | ● C2M2 の自己評価ツールを明確さと一貫性向上のために更新した。また、自己評価結果の見やすさを向上させるため、可視化機能を追加した。<br>● 複数の自己評価結果を比較できる機能を追加し、旧バージョンの PDF 又は HTML ベースのツールで行った自己評価結果の読み込みを可能とした |
| C2M2 製品群の拡張 | ● C2M2 自己評価ワークショップを支援するため、自己評価ガイド、C2M2 概要プレゼンテーション、C2M2 ワークショップ・キックオフプレゼンテーション、脅威プロファイル例、自己評価ツール用ユーザガイド等のドキュメントを追加した。さらに、CMMC 認証を目指す C2M2 ユーザのためのガイダンス文書を作成した。 |

### （4）GAO：Priority Open Recommendations: Department of Energy

GAO は、DoE の業務全般の改善を促すことを目的に、「Priority Open Recommendations: Department of Energy」を 2022 年 6 月に発行した。本文書は、DoE が有する 196 件の未解決勧告のうち、優先的に注目すべきであると GAO が考える 26 件の優先勧告についての注意を促す勧告書であり、勧告内容に加えて、DoE に求める具体的なアクションが示されている。26 件の優先勧告は、サイバーセキュリティを含む 8 分野にカテゴライズ化され、サイバーセキュリティ分野では 3 つの優先勧告が記載されている。以下の表 2-6 に、DoE に対するサイバーセキュリティ分野の勧告内容と DoE に求めるアクションを記載する。

表 2-6 DoE に対するサイバーセキュリティ分野の勧告内容と求められるアクション

| 勧告事項 | 勧告内容 | DoE に求められるアクション |
|---|---|---|
| 1. サイバーセキュリティフレームワーク採用の評価 | DoE 長官は、国土安全保障省、国立標準技術研究所など、それぞれのセクターのパートナーと適宜協議し、エネルギー分野の事業者におけるサイバーセキュリティフレームワークの使用状況の評価方法を検討する必要がある。 | DoE は、使用状況を評価するための新たな手法を学んだり、国立研究所と連携して、国立標準技術研究所の指針に沿った他の派生フレームワークの利用について報告したりするなど、より多くの情報を収集するための手順を検討している。これに加え、事業者におけるフレームワークの使用状況を測定するための新たな手法を確立し、手法の効果的な導入方法を検討するべきである。 |
| 2. リスク管理プログラムの完全な確立 | DoE 長官は、GAO が特定した課題に対処するためのサイバーセキュリティリスク管理プログラムを完全に確立する必要がある。 | 2022 年 1 月、DoE は、サイバーセキュリティリスク管理及びサイバーセキュリティ要件の実施に対する同省のアプローチを組織的観点から概説する「企業サイバーセキュリティプログラム計画（E-CSPP）」を発表した。しかし、E-CSPP は、組織のリスク許容度に関する詳細な議論を含んでいない。2022 年 4 月時点で、DoE はサイバーセキュリティリスク許容度に関する追加文書を提供していない。この勧告を完全に実施するために、DoE は、組織のリスク許容度に関する詳細な議論を提供するよう計画を確立する必要がある。 |
| 3. 電力網が直面するサイバーセキュリティリスクに対処するために必要な行動 | DoE 長官は、国土安全保障省及び他の関連する関係者と連携して、電力系統が直面する重大なサイバーセキュリティリスクに対処するための戦略を策定する必要がある。 | DoE は、電力部門のサイバーセキュリティのための複数年計画を考慮した国家サイバー戦略実施計画を策定した。しかし、それらの取組は、国家戦略を実施するには不十分であり、例えば、DoE が実施したリスク評価では、重大な方法論的限界があり、電力網のサイバーセキュリティリスクを完全には分析できていなかった。DoE は、電力網に対する国家サイバー戦略を実施するための計画を策定し、その計画が国家戦略を実施するために必要な要素を完全に満たしていることを確認し、国土安全保障省等、他の関係者とその計画を調整する必要がある。 |

### （5）DHS：Request for Information on the Cyber Incident Reporting for Critical Infrastructure Act of 2022

2022 年 9 月、DHS のサイバーセキュリティ・インフラセキュリティ庁（CISA）は、「重要インフラ向けサイバーインシデント報告法（CIRCIA）」で要求する規制案を策定するに当たり、一般からの意見を受けるため情報提供要請を発行した。この要請では、専門家、学識経験者、産業界、公益団体及び関連す

る経済的専門知識を有する者を含むが、これらに限定されない全ての一般市民に意見を求めている。

CIRCIA では、対象事業者に対して、サイバーインシデントが発生した際に、詳細な報告書を CISA に提出することを義務付けている。これらの報告により、CISA は他の連邦政府と協力して、攻撃を受けている被害者へ迅速なリソースを配備することができるとしている。また、セクターを越えて寄せられる報告を分析して傾向を把握し、攻撃者の特性を理解することで、他の潜在的被害者に警告を発することが可能であるとしている。

本情報提供要請を通じ、CIRCIA の規制要件のうち、規制案で使用される用語の定義と解釈、CIRCIA の下で要求される報告書の形式、方法、内容、提出手順、利用された脆弱性の説明を報告する要件を含む他のインシデント報告要件に関する情報及び規制の実施に必要となる執行手順や情報保護方針に関する意見を特に要望している。(表 2-7 参照)

表 2-7 CIRCIA に関する主な情報要求項目

| | |
|---|---|
| 定義、基準及び規制の適用範囲 | ● 「対象事業者」の定義について<br>● 「対象事業者」となりそうな事業者の数について<br>● 「報告義務の対象となるサイバーインシデント」の定義について<br>● 全体又は特定の産業やセクター内で、年間ベースで発生する可能性のある対象サイバーインシデントの数について<br>● 「ランサムウェアへの支払い」及び「ランサムウェア攻撃」の定義について<br>● 対象事業者が年間ベースで払う可能性のある可能性のあるランサムウェア支払いの回数について<br>● ドメインネームシステムに関するポリシーを策定、実施、執行するマルチステークホルダー組織であるかどうかを判断する基準について |
| 報告書の内容及び提出方法 | ● 対象事業者が対象サイバーインシデントに関する報告書を提出する方法、報告書に含めるべき特定の情報、情報を提出する特定の形式について<br>● 72 時間の報告期限を開始させる、対象となるサイバーインシデントの発生を裏付ける「合理的な証拠」を構成する要素について<br>● 対象事業者がランサムウェアへの支払いに関する報告書をどのように提出すべきか、報告書に含めるべき特定の情報、情報を提出する特定の形式について<br>● 身代金の支払いに関する 24 時間以内の報告期限について<br>● 補足報告書の提出時期及び何が「実質的に新しい又は異なる情報」に該当するかについて<br>● CISA が補足報告書の期限と基準を定める場合において、「状況認識の必要性と対象事業者のサイバーインシデント対応・調査能力のバランスをとる」際に考慮すべきことについて |

| | |
|---|---|
| その他のインシデント報告要件及びセキュリティ脆弱性情報の共有化 | ● サイバーインシデントや身代金支払いの報告を要求する他の既存又は提案された連邦、州の規制、指令又は同様の政策及びそれらの規制、指令又は政策とCIRCIA の報告要件との間に実際に重複、重複又は対立する可能性がある分野について<br>● 重要インフラの所有者及び運営者からサイバーインシデント又は身代金支払いの報告を受ける連邦省庁、委員会又はその他の連邦機関の種類について<br>● 既存の報告要件又は自主的な共有の下でサイバーインシデントに関する情報を集約し報告するために、職員の給与コスト（可能であれば関連する職員の役職も）を含む通常かかる金額と時間及びサイバーインシデントの規模又は種類が報告の推定コストに与える影響について<br>● 第三者機関を利用して、対象事業者の代わりに対象となるサイバーインシデント報告書又は身代金支払い報告書を提出するためにかかる金額について<br>● サイバーインシデントに関連するデータを保持するために通常必要となる金額について |
| その他のポリシー、手順、要件 | ● 規制要件の実施に関する方針、手順について<br>● 報告を行う事業者の保護について<br>● その他、CISA が規則案で取り上げることが規制対象コミュニティの利益となる方針、手順、要件について |

### （6）DoE: Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid

2022 年 10 月、DoE は、分散型エネルギー源（DER）業界と政府間の対話の促進を目的として、DER を含む電力網のサイバーセキュリティ向上に向けて DER 業界（DER 事業者・プロバイダ・インテグレータ・開発者・ベンダー）及び政策立案者に対する推奨事項を記載した報告書「Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid」を発表した。本報告書では、対象とする DER を、電力網に接続され、系統の末端に配置された 20MW 未満のものと定義している。サイバー攻撃の高度化と DER 適用による攻撃対象領域の増加を踏まえ、DER に対するセキュリティの必要性を述べた上で、セキュリティを考慮する際に着目すべき点と推奨事項を示している。DER のセキュリティを考慮する際の推奨事項として、DER 業界のステークホルダーと協力することによる DER の利用場面に応じたサイバーセキュリティ基準規格及びベストプラクティスの開発を挙げているほか、DER のサイバー防御のための基本行動原則を挙げている。以下の表 2-8 に DER のサイバー防御のための基本行動原則を示す。

今後の動きとして、DoE は、DER 業界との関係を継続し、利用場面に応じたセキュリティ標準規格とベストプラクティスの開発を目指すとしているほか、「セキュリティ・バイ・デザイン」や「CIE 戦略」などの DER のセキュリティに関する研究へ資金を提供する予定であるとしている。

表 2-8 DER のサイバー防御のための基本行動原則

| カテゴリー | 基本行動原則 |
|---|---|
| NIST CSF 又は NERC の重要インフラ保護基準に沿ったベストプラクティスの実施 | ● DER に必要なセキュリティ要件を特定し、リスクベースかつ費用対効果の高い方法で利便性と調和させる。<br>● DER ネットワークとシステムが従来の電力網とは基本的に異なる性質を有することを理解した上で、ベストプラクティスの使用を促進する。<br>● DER がこれらの要件を満たすことを保証するために、効果的な試験と適合を確保する。 |
| 設計段階からシステムへのセキュリティの考慮 | ● DER ライフサイクルに関与する各主体の役割と責任を理解し、遵守する。<br>● コード署名、セキュアパッチ、SBOM 検証を通じて、ファームウェアのセキュリティを強化する。<br>● 悪用される可能性のあるコードの脆弱性を特定するために、ソフトウェア及びハードウェアの部品表を作成する。<br>● DER に関連する通信とイベントの監視及び異常検出の強化を実施し、DER 制御要求を検証する。<br>● 暗号的に安全な通信プロトコル及び安全な鍵の保管・配布方法を採用する。<br>● DER の電力系統相互接続の際には、通信を認証するために証明書を使用する。<br>● 個人と組織の両方に対して、効果的なアクセス制御メカニズムを実装する。 |
| DER の重要機能の安定供給を確保するためのゼロトラストモデルの採用 | ● コマンドやデータを検証する際には、Secure SCADA Protocol for the 21st Century[13]で想定されているような、暗号化された安全なメカニズムを使用する。<br>● ハードウェアとソフトウェア及びソフトウェア部品表の評価を通じて、サプライチェーンリスクを分析する。<br>● Office of Cybersecurity, Energy Security, and Emergency Response（CESER）[14]の Cyber Testing for Resilient Industrial Control Systems プログラム[15]に代表される、サイバーセキュリティ専門家が実行する敵対的テストプロセスによる準備態勢の評価を行う。<br>● サイバーセキュリティの教訓と CIE の実践を取り入れ、ゼロから安全なシステムを設計し、サイバーリスクを低減するように設計された弾力性のあるシステムを実現する。<br>● 次世代のサイバー人材を育成する。 |

[13] Secure SCADA Protocol for the 21st Century（SSP21）とは、産業用制御システム専用に設計されたセキュリティアなプロトコルである。
[14] CESER は、DoE に属する組織であり、エネルギーインフラのセキュリティの向上と DoE の国家安全保障ミッションの支援を行うことを目的とする。
[15] エネルギー分野のレジリエンスなシステム構築を目的とした、サイバーセキュリティの脆弱性テスト、フォレンジック分析、重要度の高い構成要素の優先付け等を行うプログラムである。

## （7）DHS: Cross-Sector Cybersecurity Performance Goals（CPGs）

2021 年 7 月、バイデン大統領は、重要インフラ制御システムのためのサイバーセキュリティの改善に関する国家安全保障に関する覚書に署名した。この覚書では、CISA が NIST 及び省庁間コミュニティと連携して、全ての重要インフラ部門にわたって一貫性のあるサイバーセキュリティの基本性能目標を策定することを求めている。この基本性能目標として開発された「セクター横断的なサイバーセキュリティ性能目標（CPGs）」は、基本的なサイバーセキュリティ実践のための共通セットを確立し、特に中小規模の組織のサイバーセキュリティへの取組を支援することを目的としている。

CPGs は、IT と OT のサイバーセキュリティ対策の優先順位を定めたサブセットであり、重要インフラの所有者・運用者が、リスクを低減するためのものであるとしている。この目標の策定に当たって、既存のサイバーセキュリティフレームワークとガイドライン及び CISA と政府・産業界のパートナーが検討した脅威と敵の戦術、技術、手順（TTPs）を参考にしている。これらの目標を実施することで、所有者・運用者は、重要インフラの運用だけでなく、米国民に対するリスクも減らすことができるとしている。

本文書では、8 つのカテゴリーからなる要件を明記しており、それぞれの要件に対して「推奨される対策」「対策を行う対象」「対策した結果」を示している。（表 2-9 参照）

表 2-9 CPGsで示されている要件一覧

| 分類 | 要件 | 推奨対策 | 対策実施対象 | 対策の結果 |
|---|---|---|---|---|
| アカウント保護 | 自動ログイン試行の検知 | 失敗したログインは全て記録され、組織のセキュリティチーム又は関連するログシステムに送信されるようにすること。 | パスワードで保護された IT 資産、新規に導入した OT 資産 | 自動化されたクレデンシャルベースの攻撃から組織を保護する。 |
| | 初期パスワードの変更 | 内部又は外部ネットワークに配置する前に、全てのハードウェア、ソフトウェア及びファームウェアのデフォルトの製造元パスワードを変更する | パスワードで保護された IT 資産、新規に導入した OT 資産 | デフォルトパスワードを使用したアクセスやネットワーク内の移動を防ぐ。 |
| | 多要素認証 | 利用可能な場合は多要素認証を有効にする。ほかに選択肢がない場合は、SMS 認証等を採用する。 | IT 資産及びリモートアクセス機能を持つ OT 資産 | 認証情報が漏洩した資産を保護する。 |
| | パスワード強化 | 15 文字以上のパスワードを設定するようにシステムが強制する。 | パスワードで保護された IT 資産、Windows ベースの OT 資産 | パスワードクラックが困難になる。 |
| | 権限の分離 | 管理者は、管理者の役割に関連しない全てのアクションとアクティビティ（例：ビジネスメール、Web ブラウジングなど）用に別のアカウントを設定する。 | IT 及び OT 資産 | 一般アカウントが侵害された場合でも、特権アカウントへのアクセスは困難になる。 |
| | アカウントの使いまわし廃止 | IT・OT ネットワーク上のサービスや資産へのアクセスに、一意かつ個別の認証情報を設定する。ユーザは、アカウント、アプリケーション、サービスなどのパスワードを再利用しないようにする。 | IT 及び OT 資産 | 侵害されたアカウント情報を再利用してネットワーク内を移動することが困難になる。 |
| | 退社する社員の資格取り消し | (1)全てのバッジ、キーカード、トークンなどを失効・返却させ、(2)全てのユーザアカウントと組織のリソースへのアクセスを無効にする。 | 退職する従業員 | 元従業員による組織のリソースへの不正アクセスを防ぐ。 |

| 分類 | 要件 | 推奨対策 | 対策実施対象 | 対策の結果 |
|---|---|---|---|---|
| デバイス保護 | ハードウェア・ソフトウェアの承認 | 新しいハードウェア・ファームウェア・ソフトウェアをインストールする際には、承認を必要とする管理ポリシー・自動化されたプロセスを実装する。 | IT 及び OT 資産 | 承認されていないハードウェア・ファームウェア・ソフトウェアをインストールすることを防ぐ。 |
| | マクロの無効化 | 全てのデバイスで Microsoft Office マクロ又は同様の埋め込みコードをデフォルトで無効にする。また、無効にするようシステムで強制する。 | IT 資産 | 埋め込まれたマクロや同様のコードの実行を阻止する。 |
| | 資産の棚卸 | OT を含む、IP アドレスを持つ全ての組織資産の台帳を作成する。また、更新は少なくとも毎月 1 回以上行う。 | IT 及び OT 資産 | 管理されていない資産を識別し、新しい脆弱性をより迅速に検出することが可能となる。 |
| | 不正デバイスの接続禁止 | UBS 等の外部媒体の使用を制限するほか、AutoRun を無効にして、許可されていないメディアやハードウェアが IT 及び OT 資産に接続されないようにする。OT は可能であれば、物理ポートの削除等を実施する。 | IT 及び OT 資産 | 許可されていないデバイスを介した初期アクセスやデータの窃取を阻止する。 |
| | デバイス構成の文書化 | 全ての重要な IT 及び OT 資産のベースラインと現在の構成の詳細を記述した文書を作成し、保管する。 | IT 及び OT 資産 | サイバー攻撃へより効果的にかつ効率的に対応し、サービスの継続を維持する。 |
| 情報保護 | ログ収集 | IDS/IPS、ファイアウォール等ではログを収集して、攻撃検出とインシデント対応の両方で使用する。Windows イベントログ等のログソースが無効になるとセキュリティチームに通知されるようにする。 | IT 及び OT 資産 | 可視性が向上することで、攻撃に対して効率的に対応できる。 |
| | 安全なログ保管 | ログを SIEM や中央データベースに保存し、認証されたユーザのみがアクセス可能なように設定する。 | IT 及び OT 資産 | ログが不正アクセスや改竄から保護される。 |
| | 暗号化 | TLS を使用し、技術的に可能な場合は転送中のデータを保護する。脆弱な暗号化の使用を特定し、十分に強力なアルゴリズムに更新する。 | 全ての IT トラフィックと遠隔地の OT 資産 | データの機密性の維持が可能になる。 |

| 分類 | 要件 | 推奨対策 | 対策実施対象 | 対策の結果 |
|---|---|---|---|---|
| | 機微情報の保護 | アカウント情報等の機密情報は平文のまま保存せず、認証されたユーザのみがアクセスできるように設定する。 | 全てのパスワード、認証情報、機密情報及びその他の機密又は管理された情報 | 機微情報を不正アクセスから保護することが可能になる。 |
| 管理と教育 | 組織のセキュリティ責任者の選定 | 指名された役職は、セキュリティ活動全般の責任を負う。セキュリティ運用の管理、予算リソースの確保等について主導となって活動を行う。 | N/A | 1 人のリーダーが組織内のサイバーセキュリティに責任を持つようになる。 |
| | OT 資産のセキュリティ責任者の選定 | 指名された役職は、OT 固有のセキュリティ活動全般の責任を負う。上記と同一の役職である場合がある。 | N/A | 1 人のリーダーが OT 資産のサイバーセキュリティに対して責任を持つようになる。 |
| | 基本的なサイバーセキュリティ教育 | フィッシングメール、ビジネスメール詐欺への適切な対処、適切なパスワードの設定等を含む基本的なセキュリティ教育を年 1 回実施し、セキュリティ意識を育成する。 | 全従業員 | 従業員がより安全な行動を学び実行する。 |
| | OT 資産のサイバーセキュリティ教育 | 上記の基本的な教育に加え、OT のセキュリティ責任者は少なくとも年 1 回、OT 固有のセキュリティ教育を受ける。 | OT のセキュリティに責任を持つ全担当者 | OT 資産のセキュリティ担当が、OT の専門的なセキュリティ知識を得る。 |
| | IT と OT のセキュリティ関係の改善 | IT セキュリティ担当者と OT セキュリティ担当者の協力関係を強化するために、年 1 回以上の「ピザパーティ」や同等の懇親会を後援する。 | IT・OT セキュリティ担当者全員 | OT サイバーセキュリティを改善し、OT サイバーインシデントにより迅速かつ効果的に対応する。 |
| 脆弱性管理 | 既知の脆弱性の対処 | インターネットに接続されたシステムの既知の脆弱性は全て、リスク情報に基づく期間内にパッチ適用又はその他の方法で修正を行う。また、より重要な資産から優先的に適用する。 | インターネットへ接続している資産 | 攻撃者が既知の脆弱性を悪用して侵入するリスクを減らす。 |
| | 脆弱性の開示・報告 | 研究者が組織のセキュリティチームに脆弱な資産、設定ミスのある資産を通知するための手段（メールや Web フォーム）を確保する。 | 全ての資産 | 組織が、資産の脆弱性を迅速に把握することができる。 |

| 分類 | 要件 | 推奨対策 | 対策実施対象 | 対策の結果 |
|---|---|---|---|---|
| | Security.txt ファイルの展開 | 全ての公開用ウェブドメインは、RFC9116 の勧告に準拠した security.txt ファイルを保持するようにする。 | 一般公開されている全てのウェブドメイン | 研究者が発見した脆弱性をより迅速に提出できるようになる。 |
| | インターネット上に悪用可能なサービスは置かない | 外部インターネットと接続する資産は、RDP などの悪用可能なサービスを公開しないようにする。不要な OS アプリケーションとネットワークププロトコルは全て無効にする。 | インターネットへ接続している IT・OT 資産 | 外部のユーザが、資産の脆弱性を悪用して、踏み台にすることができなくなる。 |
| | 外部インターネットへの OT 接続を制限する | OT 資産は、運用のために必要とされない限り、外部インターネットには接続しない。例外は正当化して文書化する必要がある。 | インターネットへ接続している OT 資産 | 攻撃者がインターネットに接続された OT 資産を悪用・妨害するリスクを軽減する。 |
| | サイバーセキュリティの有効性に関する第三者による検証 | サイバーセキュリティの専門知識を持つ第三者が、組織のセキュリティ対策の有効性と適用範囲を定期的に検証する。 | IT・OT 資産及びネットワーク | 適切な対策が欠如している箇所を特定し、組織のサイバーセキュリティに対する信頼を確立する。 |
| サプライチェーン | ベンダー/サプライヤーのサイバーセキュリティ要件 | 組織の調達文書では、セキュリティ要件と質問が含まれており、コストと機能が同じ場合はより安全なサプライヤーを選択する必要がある。 | IT・OT 資産及びサービスのサプライヤー | 安全なサプライヤーから製品・サービスを購入することでリスクを軽減できる。 |
| | サプライチェーンのインシデント報告 | サービスレベル契約（SLA）などの調達文書や契約では、ベンダーが、組織が決定したリスクに応じた時間枠内でセキュリティインシデントを調達先の顧客に通知することを規定する。 | IT・OT 資産及びサービスのサプライヤー | サプライヤーのインシデントについて知ることで、迅速な対応が可能になる。 |
| | サプライチェーンの脆弱性の開示 | SLA などの調達文書や契約では、ベンダーが、その資産にセキュリティ上の脆弱性が確認された場合、組織が決定するリスクに応じた時間枠内で調達先の顧客に通知することを規定する。 | IT・OT 資産及びサービスのサプライヤー | サプライヤーが提供する資産の脆弱性を知ることで迅速な対応が可能になる。 |

| 分類 | 要件 | 推奨対策 | 対策実施対象 | 対策の結果 |
|---|---|---|---|---|
| 対応と回復 | インシデント報告 | 組織はインシデント発生時に、報告する相手と手段について体系化された方針と手順を策定する。 | 組織全体 | CISA 等の組織が、支援を提供する、攻撃範囲を把握することができる。 |
| | インシデント対応計画 | IT 及び OT のインシデント対応計画を策定し、管理し、更新し、定期的な訓練を実施する。 | 組織全体 | 組織が、脅威シナリオに対するインシデント対応を維持・実施・更新する。インシデント発生時の迅速な対応が可能になる。 |
| | システムのバックアップ | 運用に必要なシステムは、少なくとも年 1 回定期的にバックアップする。 | 事業運営に必要な IT・OT 資産 | データ損失・サービス運用不可の可能性と期間を軽減する。 |
| | ネットワークトポロジーの文書化 | 組織は、全ての IT 及び OT ネットワークにおいて、更新されたネットワークトポロジーと関連情報を記述した文書を作成する。定期的なレビューと更新を実施し、定期的に調査する。 | 全ての IT・OT ネットワーク | 効率的にサイバー攻撃に対応し、サービスの継続を維持する。 |
| その他 | ネットワーク分割 | OT ネットワークへの接続は、許可されていない限り、デフォルトで拒否されるように設定する。IT・OT 間はファイアウォール、DMZ 等を通過する必要がある。 | IT・OT 資産 | IT が侵害された後、OT へ侵入される可能性を減らす。 |
| | 関連する脅威と TTP の検出 | 自組織に関連する脅威と敵対者の TTP のリストを文書化し、それらの主要な脅威のインスタンスを検出する能力（ルール、警告、検出システムなど）を保有する。 | N/A | 組織が、関連する脅威と TTP を認識し、検出することができる。 |
| | メールセキュリティ | 全ての企業メールインフラにおいて、(1)STARTTLS が有効、(2)SPF と DKIM が有効、(3)DMARC が有効で“reject”に設定する。 | メールインフラ | フィッシングなど一般的なメールベースの脅威によるリスクを軽減する。 |

## （8）FERC/DoE: Supply Chain Risk Management Technical Conference; Notice Inviting Post-Technical Conference Comments

2022 年 12 月 7 日、FERC と DoE はサプライチェーンリスク管理に関する合同技術会議を開催し、米国電力系統のサプライチェーンリスクに関する課題や対策に関する議論を行った。また、会議で提起された課題に関するパブリックコメントを求める取組を 2022 年 12 月 23 日から開始した。技術会議での議論及びパブリックコメントを求めた質問の概要は以下のとおりである。

- 米国電力系統が直面するサプライチェーンリスクについて：
  IT 及び OT の相互接続性の向上、プロセス自動化、遠隔制御の拡大等により、サプライチェーンリスクは進化し続けている。技術会議では、サプライチェーンリスクについて、国家的・地政学的な観点から議論された。具体的には、系統に導入されるハードウェア、ソフトウェア、ネットワーク機器等のセキュリティに関するサプライチェーンや、SolarWinds のインシデントのような国家に支援された攻撃が電力分野にどのような影響を及ぼすかが議論された。この議論に関して、サプライチェーンに関連する課題やリスク、海外から供給された電力系統部品が悪意を持って操作された場合の特定可否、現在の地政学的状況がエネルギー分野のサプライチェーンに及ぼす影響等に関する質問項目に対して、パブリックコメントを求めた。
- 現在のサプライチェーンリスクマネジメント（SCRM）に関する信頼性基準、実施上の課題、ギャップ、改善の可能性について：
  FERC が SCRM に関する CIP 基準（Critical Infrastructure Protection standards）の策定を指示してから 6 年以上が経過し、最初の基準が発表されてから 2 年以上が経過したが、サプライチェーンリスクは増え続けている。技術会議では、CIP 基準について、米国電力系統を保護する上での有効性、基準の施行から得られた教訓、現状の CIP 基準におけるギャップが議論された。この議論に関して、SCRM に関する CIP 基準を実装する上での課題、CIP 基準を実施するための代替手段、諸外国で活用されている SCRM 基準等に関する質問項目に対して、パブリックコメントを求めた。
- DoE における Energy Cyber Sense Program について：
  DoE は、Energy Cyber Sense Program と呼ばれるプログラムを通じて、エネルギー分野をサイバー脅威から保護するための包括的なアプローチを提供予定である。具体的には、エネルギーシステム、ハードウェア及びソフトウェアにおけるサブコンポーネントの出所を明らかにする取組、脆弱性試験に関する環境の整備、最適な SCRM に向けた教育等を提供予定である。技術会議では、このプログラムを通じて対処すべきサプライチェーンリスクや具体的な取組について議論された。この議論に関して、ハードウェア部品表（HBOM）と SBOM の包含と連携による効果、レガシー技術に対するサプライチェーンリスク対応策、電力系統部品に対する第三者試験の位置づけ、オープンソースソフトウェア（OSS）に対するリスク管理策等に関する質問項目に対して、パブリックコメントを求めた。
- 電力系統のサプライチェーン・セキュリティ態勢の強化：
  技術会議では、サプライチェーン・セキュリティ態勢を向上させるための将来的な取組についても

議論され、具体的な取組として、ベンダー認定プログラム、製品やサービスの認証、第三者サービスの活用、官民連携などが挙げられた。この議論に関して、既存のベンダー認定プログラム、ベンダーのセキュリティ評価に関するベストプラクティスやガイダンス、効果的な製品認証の方法、サプライチェーンリスクに関する情報共有のあり方、サプライチェーンリスクに対する官民連携の可能性等に関する質問項目に対して、パブリックコメントを求めた。

## 2.3 欧州における動向

本節では、欧州における電力分野のサイバーセキュリティ対策やサプライチェーンリスクへの対策に係る動向等の調査結果を示す。調査対象一覧は表 2-10 に示すとおりであり、以降では、各動向の概要について示す。

表 2-10 欧州における動向等の調査対象

| No. | 取組名・文書名 | 取組開始時期・発行時期 | 取組主体・発行主体 |
|---|---|---|---|
| 2-1 | Network Code on sector-specific rules for cybersecurity aspects of cross border electricity flows (NCCS)[16] | 2022 年 7 月 6 日 | EU エネルギー規制協力庁（ACER） |
| 2-2 | Proposal for a Regulation on cybersecurity requirements for products with digital elements (Cyber Resilience Act)[17] | 2022 年 9 月 15 日 | 欧州委員会（EC） |
| 2-3 | Directive (EU) 2022/2555 (NIS 2 Directive)[18] | 2022 年 12 月 14 日 | 欧州委員会（EC） |

### （1） ACER: Network Code on sector-specific rules for cybersecurity aspects of cross border electricity flows

2022 年 7 月、ACER 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、電力分野の事業者及び政府機関に対して、電力分野のサイバーセキュリティに関する要求事項を示している。要求事項を以下の表 2-11 にまとめる。

16 https://www.acer.europa.eu/sites/default/files/documents/Recommendations/Revised%20Network%20Code%20on%20Cybersecurity%20%28NCCS%29_1.pdf

17 https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

18 https://www.nis-2-directive.com/

表 2-11 政府及び事業者に課す要求事項

| 区分 | 加盟国政府に対する要求事項 | 事業者に対する要求事項 |
|---|---|---|
| セキュリティマネジメント体制 | ● ワーキンググループ設立及び役割について<br>● 新設するセキュリティリスク監視機関について<br>● セキュリティリスク評価手法について | ● 欧州規格・国際規格に基づくセキュリティマネジメントシステムの構築について |
| リスクマネジメント | ● EU 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について<br>● 地域レベルでのセキュリティリスクアセスメントに係る一連の行動について | ● 対象となる資産への高度・最低限のサイバーセキュリティ実装について<br>● リスク評価のための NCCS-NCA[19] への情報提供について |
| サイバーセキュリティフレームワーク | ● 電力分野のサイバーセキュリティに関する推奨事項作成について<br>● 最低限及び高度なサイバーセキュリティの適用除外を与える際の行動について | ● 高度なサイバーセキュリティ要件・最低限のサイバーセキュリティ要件への準拠について<br>● セキュリティ面での安全な設計・開発のために重要サービスプロバイダが遵守すべき行動について |
| 調達時の推奨事項策定 | ● 重要事業者・高影響事業者が ICT 製品調達のために使用できるガイドライン策定について | 該当要求事項なし |
| リスクアセスメント | ● 所管省庁の重要事業者に対するリスク評価の際の行動について<br>● 重要影響事業者・高影響事業者選定について | 該当要求事項なし |
| 情報共有と危機管理 | ● 重要・高影響事業者からインシデント発生通達を受けた所管省庁がとるべき行動について | ● NCCS-NCA へのインシデント・脆弱性・サイバー攻撃に関する情報通達について<br>● インシデント対応計画の開発・実施について |
| サイバーセキュリティ演習 | ● 国家レベルのサイバーセキュリティ演習の実施・決定権の所在について | ● 国境を越える電力網へのインシデントを想定した事業者レベルのサイバーセキュリティ演習の実施について |

また、本法案では、電力セクターの業務プロセスに対するサイバー攻撃が起こしうる影響を推定するための指標として、「電力サイバーセキュリティ影響指数(ECII)」を定義している。対象となる電力分野の事業者を、ECII によって高影響事業者と重要影響事業者に区別するとしており、それぞれの事業者に対して課すセキュリティ要件が異なる。影響度により求められる要件を表 2-12 に示す。なお、ECII

[19] 加盟国が指定する国家政府機関又は規制当局のことである。

の評価手法にはリスク影響度マトリックスを使用し、以下の評価指標を含むとしている。

- サイバー攻撃による被害の程度
  - i. 負荷損失
  - ii. 発電量の減少
  - iii. 一次周波数準備における容量損失
  - iv. ブラックスタートのための容量損失
  - v. 顧客に影響を与える停電の予想期間と、顧客数における停電の規模
  - vi. 国境を越えた電力網に対する攻撃の影響の指標として合理的に機能しうる、その他の定量的又は定性的な基準
- サイバー攻撃発生可能性
  - i. 年間のインシデント件数

表 2-12 影響度別に求められるセキュリティ要件

| 分類 | 要求事項 |
|---|---|
| 重要影響事業者 | 最低限のサイバーセキュリティに加えて、高度なサイバーセキュリティ[20]の実装をする必要がある。サプライチェーンの管理項目については、最低限管理項目に加えて以下の管理項目が含まれる。<br>● 重要影響力資産として使用される ICT 製品、ICT サービス及び ICT プロセスがセキュリティ調達要件を満たすことを調達中に検証するための管理項目 |
| 高影響事業者 | 最低限のサイバーセキュリティ[21]を実装する必要があり、以下のサプライチェーンの最低限管理項目が含まれる。<br>● 調達要件にセキュリティ要件を含める<br>● セキュリティ要件を満たすサプライヤーを選択する<br>● サプライヤーを多様化し、ベンダーの固定化を抑制する<br>● 契約にセキュリティ要件を含める<br>● サプライヤーのセキュリティ調達要件を監査する |
| ECII が高影響の閾値を超えない事業者 | セキュリティ要件についての要求事項なし |

今後、欧州委員会は本法案を審査し、委任法の採択手続を開始する。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。

## （2）EC: Cyber Resilience Act

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（EU CRA）」の草案を発表した。欧州委員

[20] 高度なサイバーセキュリティ要件は ENTSO, EU DSO によって今後提案される予定である
[21] 最低限のサイバーセキュリティ要件は ENTSO, EU DSO によって今後提案される予定である

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、当該要求事項への遵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。

本法案の対象製品について、ソフトウェアやハードウェアを含む、他の製品やネットワークへの直接的・間接的な接続が存在するあらゆるデジタル製品（電力システムの PLC や SCADA 等の産業用制御システムを含む）が対象となるが、既存の EU 法により要求事項が課されている医療機器等は除外される。（図 2-1 参照） 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。

また、製造業者に対する要求事項として、デジタル製品の脆弱性ハンドリングに関する要求事項、製品のセキュリティ評価に関する要求事項、利用者への情報提示に関する要求事項、製品の適合性評価に関する要求事項、脆弱性の報告義務に関する要求事項が規定されている。（表 2-13 参照）

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（自己適合宣言又は第三者認証）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 万ユーロ又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。

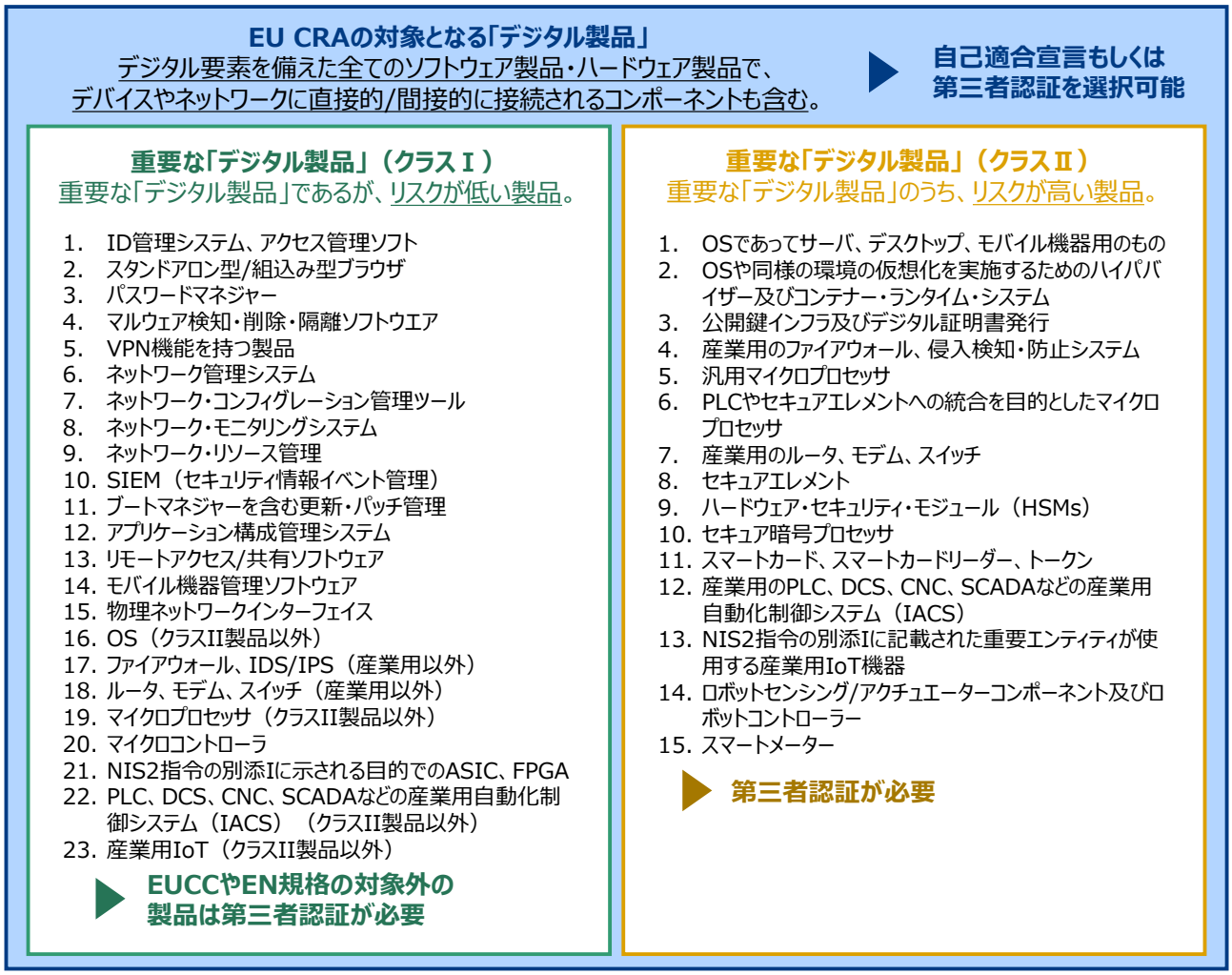



図 2-1 サイバーレジリエンス法の対象となる「デジタル製品」

表 2-13 サイバーレジリエンス法における要求事項一覧

| 要求対象 | 区分 | 具体的な要求事項 |
|---|---|---|
| デジタル製品に対する要求事項 | デジタル製品に対するセキュリティ要求事項 | (1) デジタル製品は、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。<br>(2) デジタル製品は、悪用可能な既知の脆弱性がない状態で提供すること。<br>(3) 第 10 条(2)に言及されたリスクアセスメントに基づき、デジタル製品は、以下のようにしなければならない。<br>(a) デフォルトでセキュアな設定で提供され、製品を元の状態に戻すことが可能であること。<br>(b) 認証、ID、アクセス管理システムを含むがこれに限定されない適切な管理機構により、不正アクセスから確実に保護すること。<br>(c) 保存、送信、又はその他の方法で処理された個人又はその他のデータの機密性を、最新のメカニズムによって関連データを暗号化するなどして保護すること。 |

| 要求対象 | 区分 | 具体的な要求事項 |
| --- | --- | --- |
| | | （d）保存、送信又はその他の方法で処理されたデータ、個人又はその他のデータ、コマンド、プログラム、設定の整合性を、ユーザによって許可されていない操作又は修正から保護し、また破損について報告すること。<br>（e）個人又はその他のデータを、適切かつ関連性のある、製品の使用目的に関連する必要なものに限定して処理すること（「データの最小化」）。<br>（f）サービス妨害（DoS）攻撃に対する回復力及び軽減を含む、重要な機能の可用性を保護すること。<br>（g）他の機器やネットワークが提供するサービスの可用性に及ぼす自らの悪影響を最小限に抑えること。<br>（h）外部インタフェースを含む攻撃面を制限するように設計、開発、製造すること。<br>（i）適切な悪用防止メカニズムや技術を用いて、インシデントの影響を軽減するように設計、開発、製造すること。<br>（j）データ、サービス、機能へのアクセスや変更を含む、関連する内部活動を記録や監視することにより、セキュリティ関連情報を提供すること。<br>（k）脆弱性について、セキュリティ更新（該当する場合、自動更新及び利用可能な更新のユーザへの通知を含む）を通じて対処されることを保証すること。 |
| 製造業者に対する要求事項 | 脆弱性ハンドリングに関する要求事項 | デジタル製品の製造者は、以下のことを行わなければならない。<br>（1）製品に含まれる脆弱性とコンポーネントを特定し、文書化すること。これには、少なくとも製品のトップレベルの依存関係を網羅する、一般的に使用され機械判読可能な形式のソフトウェア部品表を作成することが含まれる。<br>（2）デジタル製品にもたらされるリスクに関連して、セキュリティアップデートの提供を含め、脆弱性に遅滞なく対処し、改善すること。<br>（3）デジタル製品のセキュリティについて、効果的かつ定期的なテストとレビューを適用すること。<br>（4）セキュリティアップデートが提供された後、修正された脆弱性についての情報（脆弱性の説明、影響を受けるデジタル製品を特定できる情報、脆弱性の影響、深刻度、脆弱性を修正するための情報など）を一般に公開すること。<br>（5）脆弱性の協調的な開示に関するポリシーを導入し、実施すること。<br>（6）デジタル製品及びその製品に含まれる第三者のコンポーネントの潜在的な脆弱性に関する情報の共有を促進するための手段を講じること。（デジタル製品で発見された脆弱性を報告するための連絡先を提供することを含む） |

| 要求対象 | 区分 | 具体的な要求事項 |
| --- | --- | --- |
| | | (7) デジタル製品のアップデートを安全に配布し、悪用可能な脆弱性が適時に修正又は軽減される仕組みを提供すること。<br>(8) 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こと。 |
| 製造業者に対する要求事項 | 製品に対するセキュリティ評価に関する要求事項 | ● デジタル製品を市場に出す場合、製造業者は、その製品が附属書 I の第 1 節に定める要件(デジタル製品の特性に関するセキュリティ要求事項)に従って設計、開発及び製造されていることを確認しなければならない。<br>● 製造業者は、デジタル製品に関連するサイバーセキュリティリスクの評価を実施し、サイバーセキュリティリスクの最小化、セキュリティ事故の防止及び利用者の健康及び安全との関連性を含む当該事故の影響の最小化を目的として、デジタル製品の計画、設計、開発、生産、引渡し及び保守の段階において当該評価の結果を考慮に入れなければならない。<br>● デジタル製品を市場に出す場合、製造者は、第 23 条及び附属書 V に定める技術文書にサイバーセキュリティリスク評価を含めなければならない。特定の必須要件がデジタル製品に適用されない場合、製造者はその文書に明確な正当性を含めなければならない。<br>● 製造業者は、第三者から調達した構成部品をデジタル製品に統合する際、十分な注意を払わなければならない。製造業者は、そのようなコンポーネントがデジタル製品のセキュリティを損なわないことを保証しなければならない。<br>● 製造業者は、製品の性質及びサイバーセキュリティリスクに見合った方法で、デジタル製品に関する関連するサイバーセキュリティの側面(自らが認識する脆弱性及び第三者から提供される関連情報を含む)を体系的に文書化し、該当する場合には、製品のリスク評価を更新しなければならない。<br>● デジタル製品を市場に出す場合、予想される製品寿命又は製品を市場に出してから 5 年間のいずれか短い期間、製造業者は、当該製品の脆弱性が必須要件(脆弱性ハンドリングに関する要求事項)に従って効果的に処理されることを保証しなければならない。<br>● 製造業者は、内部又は外部の情報源から報告されたデジタル製品の潜在的な脆弱性を処理し、是正するために、附属書 I の第 2 節(5)で言及されている協調的脆弱性開示方針を含む適切な方針及び手順を有していなければならない。 |

| 要求対象 | 区分 | 具体的な要求事項 |
| --- | --- | --- |
| | 利用者への情報提示に関する要求事項 | ● 製造業者は、デジタル製品に、附属書Ⅱに規定する情報及び指示を電子的又は物理的形態で添付することを確実にしなければならない。当該情報及び指示は、利用者が容易に理解できる言語でなければならない。それらは、明確で、理解しやすく、分かりやすく、読みやすいものでなければならない。また、デジタル技術を用いた製品の安全な設置、操作、使用を可能にしなければならない。<br>● 製造業者は、EU 適合性宣言をデジタル製品に添付するか、EU 適合性宣言にアクセスできるインターネットアドレスを付属書 II に定める指示と情報に含めなければならない。 |
| | セキュリティ要件の適合性の維持に関する要求事項 | ● デジタル製品の上市から予想される製品寿命又は上市後 5 年間のいずれか短い期間、デジタル製品又は製造者が実施したプロセスが付属書 I（サイバーセキュリティの必須要件）に定める必須要件に適合していないことを知っているか、適合していないと理由できる製造業者は、デジタル技術を用いた製品又は製造者のプロセスを適合させるために必要な修正措置を直ちに講じ、必要に応じて製品を撤回するか回収しなければならない。<br>● 製造業者は、市場監視当局からの理由ある要請があれば、同当局が容易に理解できる言語で、デジタル製品及び製造事業者が実施するプロセスが附属書 I に定める必須要件に適合していることを示すために必要な全ての情報及び文書を紙又は電子形式で提供しなければならず、その要請に応じて、市場に投入したデジタル製品がもたらすサイバーセキュリティ上のリスクを排除するために講じた措置について同局と協力しなければならない。<br>● 事業を停止し、その結果、本規則に定める義務を遵守することができなくなった製造業者は、事業の停止が効力を発する前に、関連する市場監視当局に状況を通知するとともに、利用できるあらゆる手段で、可能な限り、市場に出されたデジタル製品の使用者にもこの状況を通知しなければならない。 |
| 製造業者に対する要求事項 | 脆弱性の報告義務 | ● 製造業者は、過度の遅滞なく、いかなる場合においても、認識してから 24 時間以内に、デジタル製品に含まれる積極的に悪用される脆弱性を ENISA に通知しなければならない。通知には、当該脆弱性に関する詳細、及び、該当する場合には講じられた是正又は軽減措置が含まれるものとする。<br>● 製造業者は、デジタル要素を有する製品のセキュリティに影響を及ぼす事象について、過度の遅滞なく、いかなる場合であってもその認識から 24 時間以内に ENISA に通知しなければならない。 |

| 要求対象 | 区分 | 具体的な要求事項 |
| --- | --- | --- |
| | | ● 製造業者は、過度の遅滞なく、かつ、認識した後に、デジタル製品の利用者に対して、事故について、また必要に応じてユーザが事故の影響を軽減するために展開できる是正措置について通知しなければならない。<br>● 製造業者は、オープンソースコンポーネントを含む、デジタル製品に組み込まれたコンポーネントの脆弱性を特定した場合、そのコンポーネントを保守する個人又は団体に報告しなければならない。 |
| | 罰則 | ● 附属書Ⅰに規定されたサイバーセキュリティの必須要件及び第 10 条と第 11 条に規定された義務(セキュリティ要件の対応やセキュリティに関する報告等)を遵守しない場合、最高 1,500 万ユーロ又は違反者が事業者の場合、前会計年度の全世界の年間総売上高の 2.5%のいずれか高い方の行政罰の対象となる。<br>● 本規則に基づくその他の義務に違反した場合、最高 1,000 万ユーロ又は違反者が事業者の場合は、前会計年度の全世界の年間総売上高の 2%のいずれか高い方の行政罰が課される。<br>● 要求に対する回答として、不正確、不完全又は誤解を招く情報を通知機関及び市場監視当局に提供した場合、5 百万ユーロ又は違反者が事業者の場合、前会計年度の全世界の年間総売上高の 1%以下のいずれか高い方の行政罰の対象となる。 |
| EU 加盟国関係機関に対する要求事項 | EU 加盟国に対する要求事項 | ● 加盟国は、この規則に従って適合性評価を実施する権限を有する適合性評価機関を欧州委員会及び他の加盟国に通知しなければならない。<br>● 加盟国は、適合性評価機関の評価及び届出並びに届出機関の監視(第 31 条の遵守を含む)のために必要な手続を設定し実施する責任を負う届出機関を指定しなければならない。<br>● 加盟国は、適合性評価機関の審査及び届出、届出機関の監視に関する自国の手続並びにその変更について欧州委員会に報告しなければならない。 |
| | 欧州委員会に対する要求事項 | ● 欧州委員会は、附属書Ⅰの第 2 節(1)に定めるソフトウェア部品表の様式及び要素を実装法令によって規定することができる。これらの実装法令は、第 51 条(2)にいう審査手続に従って採択されなければならない。<br>● 欧州委員会は、実装法令によって、11 条 1 及び 2 に従って提出される届出の情報の種類、様式及び手続をさらに定めることができる。これらの実装法令は、第 51 条(2)にいう審査手続に従って採択されるものとする。 |

| 要求対象 | 区分 | 具体的な要求事項 |
|---|---|---|
| | ENISA に対する要求事項 | ● ENISA は、サイバーセキュリティリスクに関連する正当な理由がない限り、過度の遅延なく、製造メーカから脆弱性通知を受領次第、当該加盟国の指令（NIS2 指令）に従い、協調的脆弱性開示を目的として指定された CSIRT に転送し、市場監視当局に通知した脆弱性について通知するものとする。<br>● ENISA は、サイバーセキュリティリスクに関連する正当な理由がない限り、製造メーカからデジタル要素を有する製品のセキュリティに影響を及ぼす事象を受領次第、過度の遅滞なく、NIS2 指令に従って指定された単一の連絡先に通知を転送するものとする。<br>● ENISA は、通知されたインシデントについて市場監視当局に通知する。インシデントの通知にはインシデントの重大性と影響に関する情報を含め、該当する場合、製造者がインシデントを不法行為又は悪意ある行為によるものと疑っているか又は国境を越えた影響があるとみなしているかを示すものとする。<br>● ENISA は、NIS2 指令によって設立された欧州サイバー危機連絡組織ネットワーク（EU-CyCLONe）に、11 条 1 及び 2 に従って通知された情報が、大規模サイバーセキュリティ事件及び危機の運用レベルでの協調管理に関連している場合、提出しなければならない。<br>● ENISA は、11 条 1 及び 2 に従って受領した通知に基づいて、デジタル要素を有する製品におけるサイバーセキュリティリスクに関する新たな傾向について 2 年ごとの技術報告書を作成し、NIS2 指令で言及されている協力グループに提出するものとする。最初の当該報告書は、11 条 1 及び 2 に規定する義務の適用開始後 24 か月以内に提出するものとする。 |

## （3）EC: NIS 2 Directive

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、現行の NIS 指令を改定した 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、採択され 2023 年 1 月 16 日に発効された。加盟国は、2024 年 10 月 17 日までに、指令を遵守するための措置を公表し、2024 年 10 月 18 日から措置を適用する。

本指令では、現行指令と比較して、対象分野の範囲が大きく拡大された（表 2-14 参照）ことに加え、対象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。これまでの NIS 指令においても電力分野を含む「エネルギー分野」が対象となっていたが、NIS2 指令では、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。

表 2-14 NIS2 指令の対象となる事業種

| 必須分野 | 重要分野 |
|---|---|
| 1. エネルギー<br>2. 運輸<br>3. 銀行<br>4. 金融市場インフラ<br>5. 保健医療<br>6. 上水道<br>7. デジタルインフラ<br>8. 下水道<br>9. 行政機関<br>10. 宇宙 | 1. デジタルサービス提供者<br>2. 郵便・配送サービス<br>3. 廃棄物管理<br>4. 化学薬品<br>5. 食品<br>6. 製造業<br><br>※赤字は NIS2 指令で新たに追加されたもの |

本指令は、対象分野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る法案であり、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。(表 2-15 参照)

表 2-15 NIS2 指令で掲げている目標と達成のための具体案

| 目標 | 達成のための具体案 |
|---|---|
| セキュリティリスクの管理 | ● 対象に求める以下の 7 項目を定義しているが、具体的な対策方法や要件については明記されていない。<br>➢ リスク分析及び情報システムセキュリティ方針<br>➢ インシデントの予防、検出、対応<br>➢ 事業継続と危機管理<br>➢ サプライチェーン・セキュリティ<br>➢ 脆弱性の取扱いと開示を含むシステムの取得、開発、保守<br>➢ サイバーセキュリティリスク管理策の有効性を評価するための方針と手順(テストと監査)<br>➢ 暗号技術の使用 |
| 協力関係の強化 | ● 各加盟国へ 1 つ以上の CSIRT を設置<br>● 各国の CSIRT 及び CERT-EU 間で CSIRT ネットワークを形成し、インシデント、脅威及び脆弱性についての情報共有を行う。なお、欧州委員会は CSIRT ネットワークの監視者として機能し、ENISA は事務局の提供を行うことで CSIRT ネットワークを支援する。<br>● 各加盟国へ危機管理当局を 1 つ以上設置<br>● 危機管理当局、欧州委員会及び ENISA で EU-CyCLONe を設立し、大規模なインシデントに対応する支援を行う。ENISA は、本ネットワーク |

| 目標 | 達成のための具体案 |
|---|---|
| | の事務局を提供し、情報交換を支援する。 |
| セキュリティ能力の向上 | ● 各主体がセキュリティ対策を講じるような、より厳格な監督手段と法執行措置の導入。<br>● セキュリティリスク管理及び報告義務の侵害に対する制裁金などの行政処分一覧表の策定。<br>● 制裁金について、セキュリティリスク管理（第 18 条）及び報告義務（第 20 条）を侵害した場合は、1,000 万ユーロ又は事業者の前年度世界総売上高の 2%のいずれか高い方を課す。 |

また、本指令は、対象分野として 2 つのカテゴリー（必須分野・重要分野）からなる 16 分野を指定している。本指令は、必須分野・重要分野に属する対象事業者に適用されるが、所轄官庁が、対象事業者に対して有する権限について必須分野・重要分野で異なる。本指令第 29 条及び第 30 条には以下の表のように明記されており、所轄官庁は、必須分野に属する対象事業者に対して、より厳格な監査・執行を行う権限を有する。（表 2-16 参照）

表 2-16 必須分野・重要分野に対して所轄官庁が有する権限の違い

| 必須分野の事業者 | 重要分野の事業者 |
|---|---|
| 抜き打ち検査を含む立入検査及びオフサイト監査 | 立入検査及び事後のオフサイト監督 |
| 定期的な監査 | - |
| リスク評価又はリスク関連の利用可能な情報に基づく標的型セキュリティ監査 | リスク評価又はリスク関連の利用可能な情報に基づく標的型セキュリティ監査 |
| 客観的、無作為的、公正かつ透明なリスク評価基準に基づくセキュリティ検査 | 客観的、公正かつ透明なリスク評価基準に基づくセキュリティ検査 |
| 文書化されたサイバーセキュリティポリシーを含む、事業者が採用したサイバーセキュリティ対策を評価するために必要な情報、ENISA への通知義務の遵守要請 | 文書化されたサイバーセキュリティポリシーを含むサイバーセキュリティ対策を事後に評価するために必要なあらゆる情報、ENISA への通知義務の遵守要請 |
| 監督業務の遂行に必要なデータ、文書又はあらゆる情報へのアクセス要求 | 監督業務の遂行に必要なデータ、文書又は情報へのアクセス要求 |
| 有資格監査人により実施されたセキュリティ監査の結果及びその根拠となる証拠など、サイバーセキュリティ対策の実施に関する証拠の要求 | - |

## 2.4 国内の電力分野における動向

本節では、国内における電力分野のサイバーセキュリティ対策やサプライチェーンリスクへの対策に係る動向等の調査結果を示す。調査対象一覧は表 2-17 に示すとおりであり、以降では、各動向の概要

について示す。

表 2-17 国内電力分野における動向等の調査対象

| No. | 取組名・文書名 | 取組開始時期・発行時期 | 取組主体・発行主体 |
|---|---|---|---|
| 3-1 | 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[22] | 2022 年 4 月 1 日 | 資源エネルギー庁 |
| 3-2 | 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）[23] | 2022 年 6 月 10 日 | 経済産業省 |
| 3-3 | 重要インフラのサイバーセキュリティに係る行動計画[24] | 2022 年 6 月 17 日 | NISC |

### （1） 資源エネルギー庁：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

近年、新たなビジネス領域として、エネルギー・リソース・アグリゲーション・ビジネスが注目されている。分散リソースを束ねて供給力や調整力として活用するビジネス環境を整える観点から、電気事業法等の一部を改正する法律第二条の規定による改正後の電気事業法において、アグリゲーターを特定卸供給事業者として新たに位置づけることとされた。特定卸供給事業者においては、サイバーセキュリティ対策が不十分と考えられる事業者に対して、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。本指針における対策事項は、「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。（図 2-2 参照）

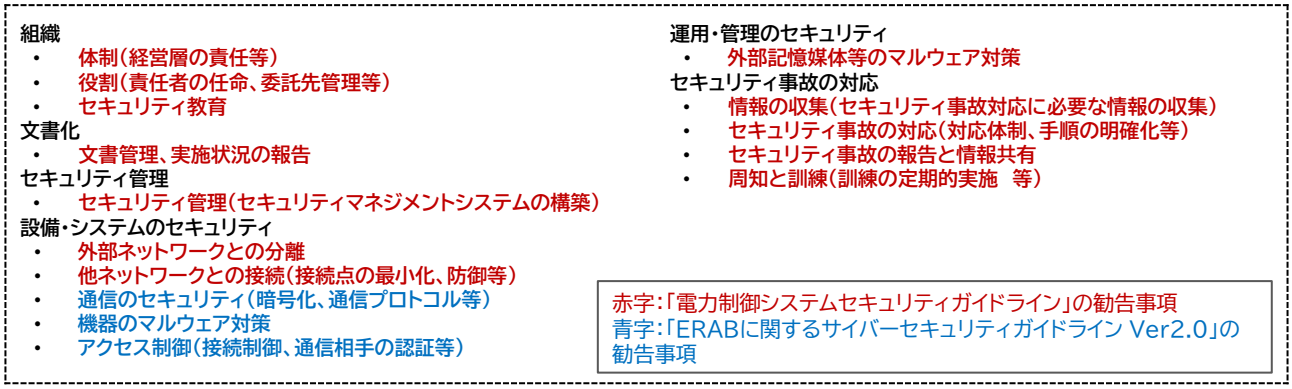



図 2-2 「特定卸供給に係るサイバーセキュリティ確保の指針」における対策要求事項

22 https://www.enecho.meti.go.jp/category/electricity_and_gas/electric/summary/regulations/pdf/cyber-shishin.pdf

23 https://www.meti.go.jp/policy/safety_security/industrial_safety/oshirase/2022/07/20220706.html

24 https://www.nisc.go.jp/policy/group/infra/siryou/index.html

### （2）経済産業省：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）

「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た。対策に当たって、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。本ガイドラインは、サイバー攻撃やサイバーセキュリティ確保の管理不良を要因としたシステムの不具合により、自家用電気工作物の保安の確保に支障を及ぼす可能性のある遠隔監視システム及び制御システム並びにこれらのシステムに付随するネットワークを対象とし、設置者や保守点検を行う者、遠隔サービス提供事業者等に適用される。（図 2-3、図 2-4、図 2-5 参照）

対象となる設備は「区分 A：自家用電気工作物のうち系統連系する発電設備（蓄電設備を含む）の制御システム」「区分 B：自家用電気工作物のうち系統連系する発電設備の遠隔監視システム並びに自家用電気工作物のうち系統連系しない発電設備の遠隔監視システム及び制御システム」「区分 C：自家用電気工作物のうち発電設備以外の設備の遠隔監視システム及び制御システム」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。

対策要求事項のうち、「経営層の責任」、「管理組織の設置」、「目的の明確化」、「責任者の設置」、「接続点の最小化」、「接続点の防御」、「外部記憶媒体等のマルウェア対策」のみ、区分 A に対しての勧告事項と位置づけられている。

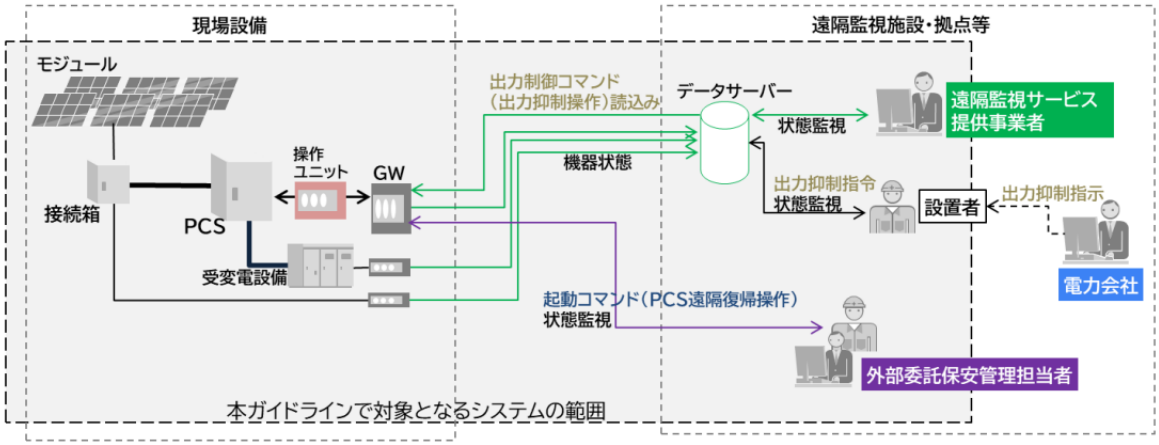



図 2-3 発電設備の保安管理業務を外部委託する場合の対象システムの範囲の例（発電設備の出力制御コマンドが遠隔サービス提供事業者のシステムを介して発電設備側に伝達される例）[25]

[25] 経済産業省、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
https://www.meti.go.jp/policy/safety_security/industrial_safety/law/files/jikayouguideline.pdf

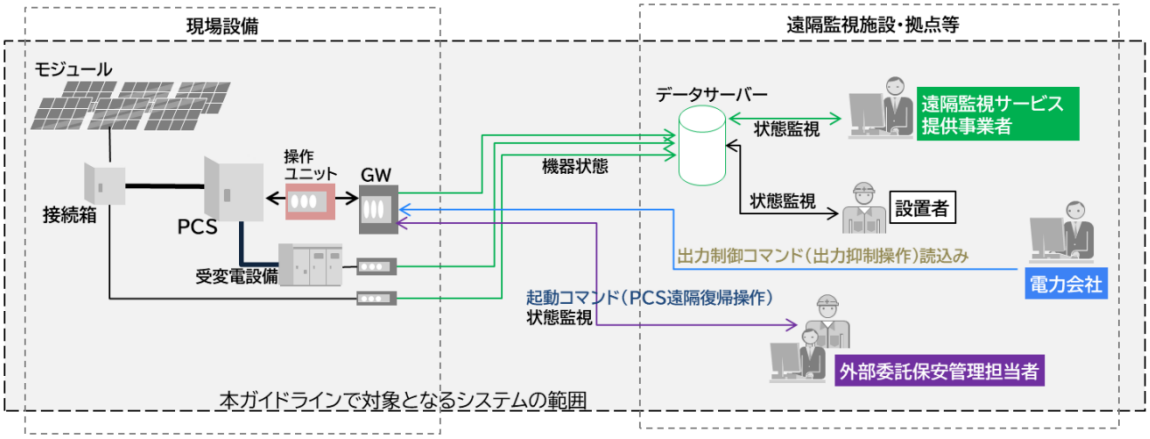



図 2-4 発電設備の保安管理業務を外部委託する場合の対象システムの範囲の例(発電設備の出力制御コマンドが系統接続先の電力会社から別のシステムを介して伝達される例)[26]

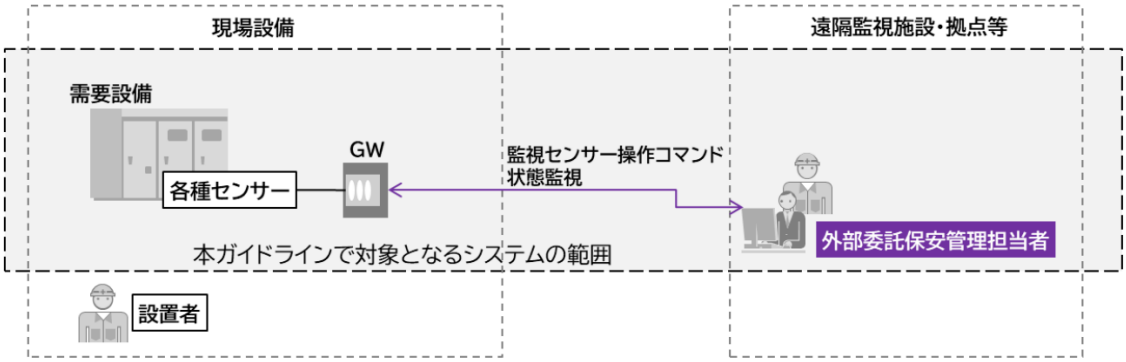



図 2-5 需要設備の保安管理業務を外部委託する場合の対象システムの範囲の例[27]

## (3) NISC:重要インフラのサイバーセキュリティに係る行動計画

2017 年に公表された「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、重要インフラ事業者のサイバーセキュリティ対策に係る行動計画を 2022 年 6 月に公表した。具体的な取組として、「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。5 つの方針とその取組内容を表 2-18 に示す。

第 4 次行動計画と比較し、対象分野や取組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要視されている。サプライチェーンの取組として、「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。

[26] 経済産業省、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
https://www.meti.go.jp/policy/safety_security/industrial_safety/law/files/jikayouguideline.pdf
[27] 経済産業省、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
https://www.meti.go.jp/policy/safety_security/industrial_safety/law/files/jikayouguideline.pdf

表 2-18 5 つの方針と取組内容

| 方針 | 取組内容 |
| --- | --- |
| 障害対応体制の強化<br>重要インフラ事業者等は組織全体としてサイバーセキュリティの確保に取り組んだ上で、官民の相互連携を密にした障害対応体制の強化を推進する。 | 1. 組織統治の一部としての障害対応体制<br>● 経営層、CISO、戦略マネジメント層、システム担当等組織全体及びサプライチェーン等に関わる事業者を含めた障害対応体制の強化を推進<br>2. 障害対応体制の強化に向けた取組<br>● 障害対応体制を強化するため、BCP/IT-BCP、CSIRT、監査体制等の効果的な取組を推進<br>3. 官民一体となった障害対応体制の強化<br>● 政府と重要インフラ事業者等の相互連携を密にした官民一体としての対応を検討<br>4. 重要インフラに係る防護範囲の見直し<br>● 環境変化に対応するため、サプライチェーンを含めた「面としての防護」の確保及び国の安全等の確保の観点からの取組 |
| 安全基準等の整備及び浸透<br>自組織に最適な防護対策を実施するため、重要インフラ事業者等の関係主体における「安全基準等」の整備及び浸透の取組を推進する。 | 1. 指針の継続的改善<br>● 組織統治の一部としてサイバーセキュリティを取り入れる方策の強化や、サプライチェーンに関する基準の整備<br>● 自組織に適した継続的改善のための基準の整備<br>2. 安全基準等の継続的改善<br>● 内部・外部監査や演習への参加等によるリスク評価を経た、安全基準等の継続的な改善<br>● 重要インフラ所管省庁による安全基準等の改善状況を調査<br>3. 安全基準等の浸透<br>● 重要インフラ事業者等におけるサイバーセキュリティ確保に向けた取組について、実態把握のための調査<br>4. 安全基準等の文書の明確化<br>● 安全基準等策定指針、安全基準等の理解促進のため、文書の一覧化や文書間の関係性を明確化 |
| 情報共有体制の強化<br>個々の重要インフラ事業者等が日々変化するサイバーセキュリティ動向に対応できるよう、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に取り組む。 | 1. 情報共有の更なる促進<br>● 共有された情報のリスクマネジメント等への積極的な活用<br>● 重要インフラサービス障害に係る情報及び脅威や脆弱 性情報の集約、分析、共有<br>● 共有すべき情報の明確化（情報系だけでなく制御 |

| 方針 | 取組内容 |
| --- | --- |
| | 系や IoT システムも対象となること等を明示）<br>● 環境変化等が生じた場合における適時適切な見直し<br>2. 重要インフラ事業者等の活動の更なる活性化<br>● 経営層のリーダーシップの下、障害対応体制の構築・強化<br>● セプター内、セプター間の情報共有の更なる充実<br>● ISAC への参画及び ISAC 間の情報共有の促進<br>● より実態に即した形でのセプター訓練の実施 |
| <u>リスクマネジメントの活用</u><br>重要インフラサービスの継続的提供の強靭性確保のため、自組織に適した防護対策の計画・実施、評価・改善の繰り返しによる継続的な取組を推進する。 | 1. リスクマネジメントの推進<br>● 自組織のプロファイルを明確化し、自組織に適した防護対策の実現に向けた取組の推進<br>● 有効な対策や既存の基準類の活用方法について検討し、手引書の見直し、新たなガイダンス等を整備する<br>2. リスクに関する調査・分析<br>● デジタル化を伴うDXの進展によるサイバー空間の変容等によるリスクに対応するため、環境変化調査を実施する<br>● 重要インフラサービス障害等が生じた場合に、ほかのどの重要インフラ分野に影響が波及するかという相互依存性に関する調査を実施する。 |
| <u>防衛基盤の強化</u><br>重要インフラの防護基盤の強化のため、障害対応体制の有効性検証、人材育成、関係機関との連携、国際連携、広報広聴活動等、行動計画の全体を支える共通基盤的な取組を推進する。 | 1. 障害対応体制の有効性検証<br>● 分野横断的演習による障害対応体制の検証<br>● 演習で得た課題を活用した障害対応体制の改善<br>2. 人材育成の推進<br>● 経営層と緊密な連携を行えるよう、戦略マネジメント層の育成<br>● IT 部門に限らない、組織全体の意識向上<br>3. 国際連携の推進<br>● 政府間や事業者間の様々な枠組みを活用した多面的・多角的な国際連携の推進<br>4. 警察・デジタル庁との連携強化<br>● サイバー犯罪や、DX に伴う新たな技術に対する意識向上による全体としてのセキュリティ確保の推進<br>5. 広報広聴活動の推進<br>● 行動計画の枠組みや取組の国民への積極的な発 |

| 方針 | 取組内容 |
| --- | --- |
| | 信<br>● 関連文書及び関連規格の整備 |

## 2.5 国内の他分野における動向

国内における電力分野以外の動向について、工場・宇宙・ビル・防衛産業分野のサイバーセキュリティ動向について調査した。

### 2.5.1 工場分野におけるサイバーセキュリティ対策に関する動向

「Society5.0」や「Industry4.0」の登場から工場におけるデータ利活用が促進され、従来ネットワークに接続されてない工場が外部ネットワークに接続されるようになり、新たなセキュリティリスク源が増加した。これらの状況を踏まえて工場分野のサイバーセキュリティ対策について議論することを目的に、「産業サイバーセキュリティ研究会」の「ワーキンググループ 1(制度・技術・標準化)」の「工場サブワーキンググループ(工場 SWG)」が 2022 年 1 月に設置された。

工場 SWG では、2022 年 1 月より工場のサイバーセキュリティ対策の推進に向けたガイドラインを取りまとめることを目標に活動し、2022 年 11 月に「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(以降、「工場セキュリティガイドライン」という。)」を公表した。

工場セキュリティガイドラインは、企業の IT システム部門、生産関係部門、監査部門などを想定読者とし、自らの工場のセキュリティ対策を立案・実行することを目的に、参照すべき考え方やステップを示した手引きである。具体的に示されているステップは図 2-6 のとおりである。

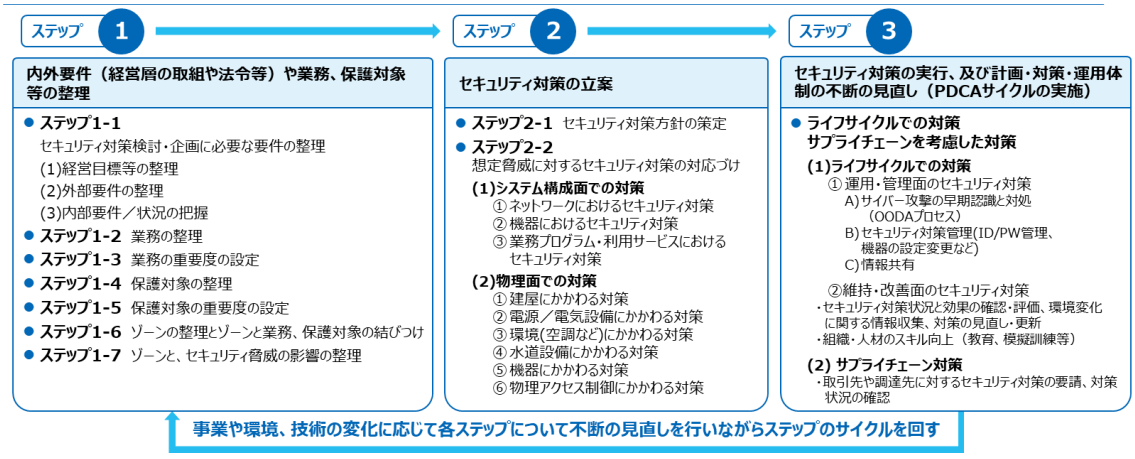



図 2-6 工場におけるセキュリティ対策企画・導入の進め方[28]

具体的なステップとして、ステップ 1 で工場セキュリティの要件を設定したのちに、保護対象の整理・優先度付けを行い、ゾーンとの対応付けを行うことが推奨されている。ゾーンは、工場セキュリティガイド

[28] 経済産業省、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 概要資料
https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline_gaiyou.pdf

ラインにおける特徴的な要素であり、同等のセキュリティ対策が求められている領域と定義づけしている。ゾーンごとに対策を管理することで、複雑な工場システムの管理を効率化することを目指している。ステップ２では、整理されたゾーンごとに想定した脅威に対する、システム構成面・物理面でのセキュリティ対策を検討する。工場セキュリティガイドラインには、事業者が検討すべき対策の粒度を示すことを目的に、システム構成面・物理面でのセキュリティ対策における主要対策が記載されている。ステップ 3 では、ライフサイクルでの対策、サプライチェーン対策が検討され、ステップ 2 と同様に対策の例が記載されている。

工場セキュリティガイドラインでは、特に実施いただきたい対策について記載しているチェックリストが作成されている。チェックリストの概要を図 2-7 に示す。準備・組織的対策・運用的対策（システム関連等）・技術的対策・工場システムサプライチェーン対策の 5 つのカテゴリーに分けられている。また、達成度は 5 段階で設定されている。本チェックリストは、参考的なチェックリストとして位置づけられ、自社の状況に応じて項目の追加・削除や内容の修正を行うことが想定されている。

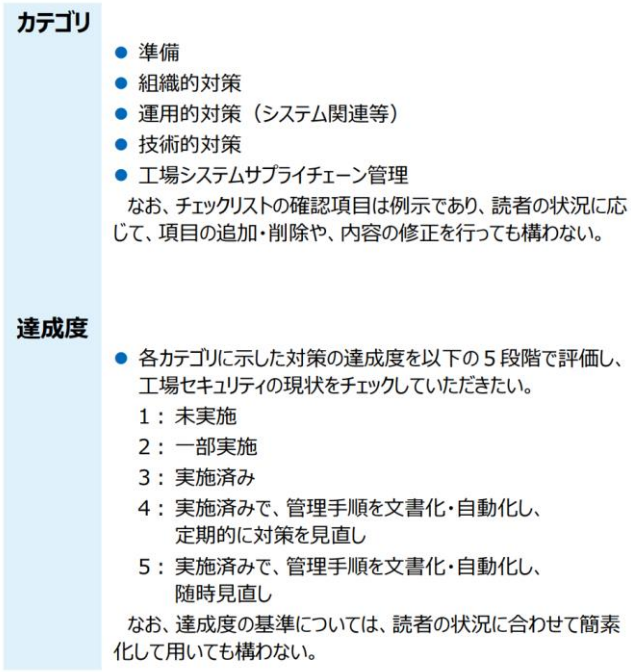



図 2-7 工場セキュリティガイドラインにおけるチェックリストの概要[29]

## 2.5.2 宇宙分野におけるサイバーセキュリティ対策に関する動向

我が国の安全保障や経済社会における宇宙システムの役割の増大、宇宙システムの省人化・自動化・クラウド利用の増加、宇宙システムに関するステークホルダーの多様化、サプライチェーンの複雑化等に伴い、宇宙システムのサイバーセキュリティ確保が重要かつ困難になりつつある。これらの状況を踏まえて宇宙分野のサイバーセキュリティ対策について議論することを目的に、「産業サイバーセキュリティ研究会」の「ワーキンググループ 1（制度・技術・標準化）」の「宇宙産業サブワーキンググループ（宇宙産業 SWG）」が 2021 年 1 月に設置された。そして、宇宙産業 SWG やその参加の作業部会及びコアメ

[29] 経済産業省、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 概要資料
https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline_gaiyou.pdf

ンバー会議での議論を通じて、「民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.0（以降、「宇宙セキュリティガイドライン」という。）」が 2022 年 7 月 21 日に公開された。

宇宙セキュリティガイドラインは、民間宇宙事業者のビジネスを振興する観点から、宇宙システムに係るセキュリティ上のリスク、宇宙システムに関わる各ステークホルダーが検討すべき基本的セキュリティ対策、対策の検討に当たり参考になる参考文献、活用可能な既存施策等について分かりやすく整理して示し、民間事業者における自主的な対策を促すことを目的とし、特に、民間企業が主体となる衛星システム及び地上システム（衛星運用設備、衛星データ利用設備、開発・製造設備）を対象に、標準的なシステムモデル、リスクシナリオ、対策を整理している。宇宙セキュリティガイドラインで示されている民間宇宙システムの標準モデルを図 2-8 に示す。宇宙セキュリティガイドラインでは、この標準的モデルを踏まえ、民間宇宙システムに重大な事業被害を及ぼしうるシナリオ例を 7 つ整理している。そして、このリスクシナリオの検討を踏まえ、全組織に関わる共通的な対策と、宇宙システム特有の対策をそれぞれ示している。共通的な対策には、組織的なセキュリティリスクマネジメント、クラウドセキュリティ対策、テレワークセキュリティ対策、内部犯行対策及び外部へのインシデント報告が含まれる。そして、宇宙システムの特有の対策としては、法令上求められる対策と、各サブシステム（衛星本体、衛星運用設備、衛星データ利用設備及び開発・製造設備）に求められる対策が整理されている。

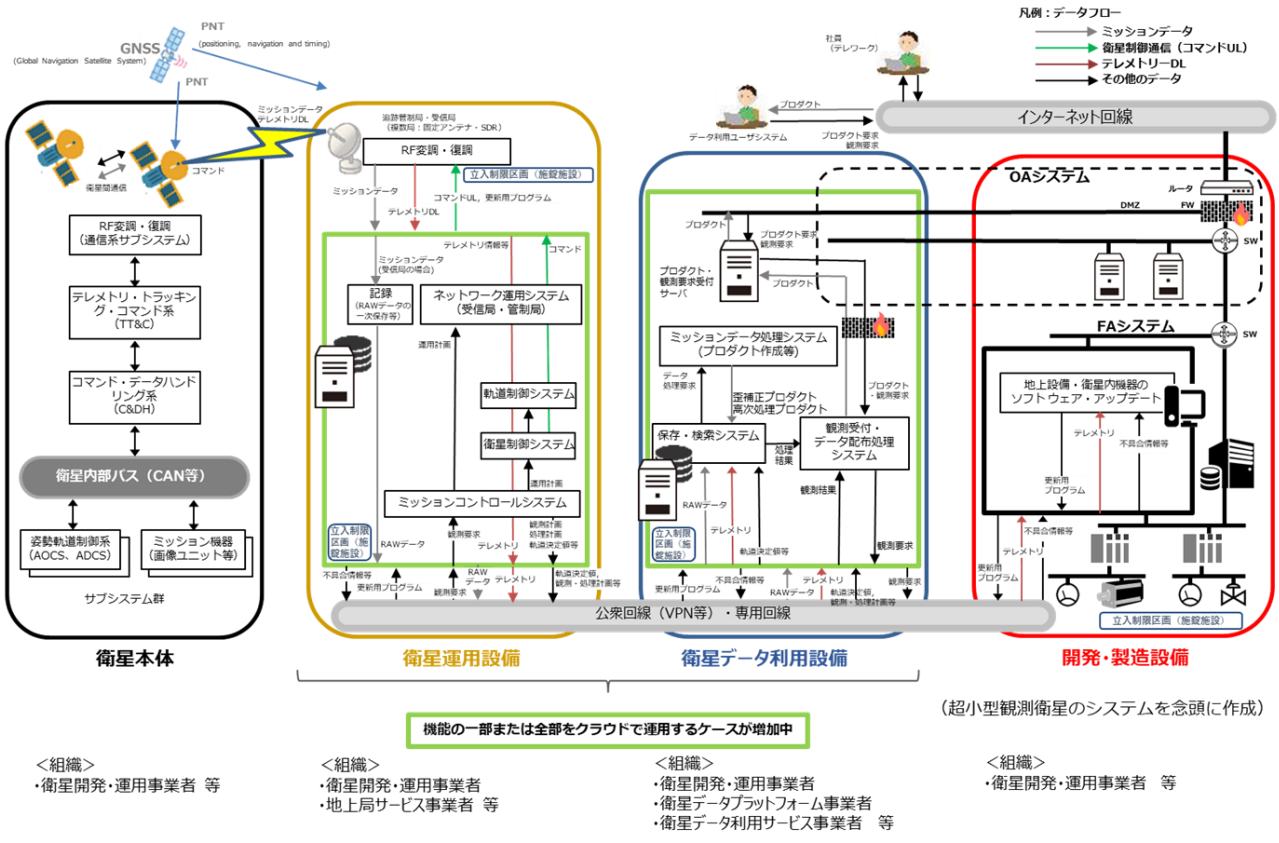



図 2-8 民間宇宙システムの標準的なモデル[30]

[30] 経済産業省、民間宇宙システムにおけるサイバーセキュリティ対策ガイドライン Ver 1.0 概要資料
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_uchu_sangyo/pdf/20220721_2.pdf

### 2.5.3 ビル分野におけるサイバーセキュリティ対策に関する動向

ビル分野のサイバーセキュリティは、従来ビルシステム特有のプロトコルを利用していることやビルの制御システムがインターネットと切り離されていたため、攻撃の対象になりにくいと考えられていた。しかし、サイバー攻撃のレベルの向上や利便性によるインターネット接続が増えてきたことによりセキュリティリスクが増加したことにより、サイバー攻撃を受ける事例が増えてきている。このような状況を踏まえて、複数のステークホルダーが関係しているビルにおいて、共通的に参照できるサイバーセキュリティ対策のガイドラインを作成することを目的に、「産業サイバーセキュリティ研究会」の「ワーキンググループ 1（制度・技術・標準化）」の「ビルサブワーキンググループ（ビル SWG）」が 2018 年 2 月に設置された。

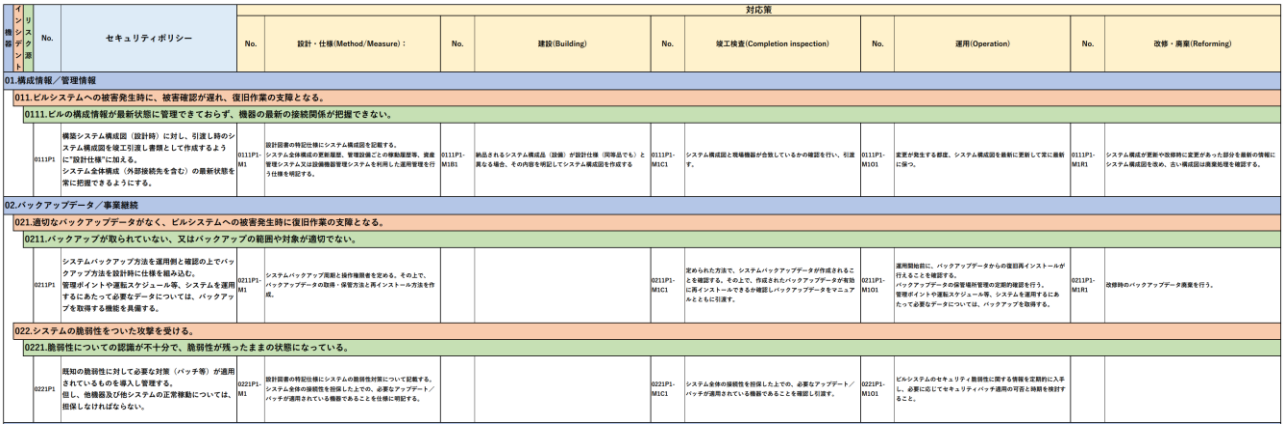
ビル SWG にはビルシステムに関わる多数のステークホルダーが参加し、ガイドラインの策定に向けて議論が行われた結果、パブリックコメントを経て 2019 年 6 月に「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（以降、「ビルセキュリティガイドライン」という。）」が公表された。

ビルセキュリティガイドラインは、サイバー・フィジカル・セキュリティ対策フレームワークを参考に、ビルのサイバー・フィジカル・セキュリティ対策の内容を整理している。ガイドラインは、必須の対策ではなく、ビルシステムの関係者がガイドラインを参考に優先付けしてセキュリティ対策を実施できる文書としている。また、ビルセキュリティガイドラインは、共通編と個別編の 2 本立てであり、2019 年 6 月に公表されたガイドラインが共通編である。共通編は初歩的な対策をまとめた文書であるが、個別編では、個別のサブシステムに関する対策やセキュリティ投資が記載されている。個別編については、第 1 弾として、2022 年 10 月に「ビル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（個別編：空調システム）」が公表された。ビルセキュリティガイドラインの構成は表 2-19 のとおりである。ビルシステムの特徴や攻撃事例を示すとともに、ビルセキュリティにおけるセキュリティ対策の基本的な考え方、リスク、セキュリティ対策を示している。

表 2-19 ビルセキュリティガイドラインの構成

| 章番号 | 内容 |
|---|---|
| 第 1 章 | はじめに（背景・想定読者等） |
| 第 2 章 | ビルシステムの特徴とビルシステムに対するサイバーセキュリティの脅威の現状を示す。 |
| 第 3 章 | ビルシステムにおけるサイバーセキュリティ対策の基本的考え方やビルの条件に合わせたガイドラインの活用の仕方を示す。 |
| 第 4 章 | ビルシステムにおけるサイバーセキュリティリスクと対策ポリシーを示す。 |
| 第 5 章 | ライフサイクルの各フェーズで実施すべきセキュリティ対策について示す。 |

ビルセキュリティガイドラインの特徴としては、ガイドラインの想定する使い方例が具体的に記載されている点である。使い方例では、大きく 3 つの例が記載され、ステークホルダーごとに必要な対策が記載されている。また、第 4 章において示されているサイバーセキュリティリスクと対策ポリシーを参考にライフサイクルごとに実施すべき具体的な対策を記載した別紙が作成されている。ライフサイクルは、設計・使用、建設、竣工検査、運用、改修・廃棄の 5 段階であり、各段階の対応策が示されている。



| 機器 | インシデント | リスク源 | No. | セキュリティポリシー | 対応策 No. | 設計・仕様(Method/Measure)： | No. | 建設(Building) | No. | 竣工検査(Completion inspection) | No. | 運用(Operation) | No. | 改修・廃棄(Reforming) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 01.構成情報／管理情報 | | | | | | | | | | | | | | |
| 011.ビルシステムへの被害発生時に、被害確認が遅れ、復旧作業の支障となる。 | | | | | | | | | | | | | | |
| 0111.ビルの構成情報が最新状態に管理できておらず、機器の最新の接続関係が把握できない。 | | | | | | | | | | | | | | |
| | | 0111P1 | 0111P1 | 構築システム構成図（設計時）に対し、引渡し時のシステム構成図を竣工引渡し書類として作成するように"設計仕様"に加える。<br>システム全体構成（外部接続先を含む）の最新状態を常に把握できるようにする。 | 0111P1-M1 | 設計図書の特記仕様にシステム構成図を記載する。<br>システム全体構成の更新履歴、管理設備ごとの稼動履歴等、資産管理システム又は設備機器管理システムを利用した運用管理を行う仕様を明記する。 | 0111P1-M1B1 | 納品されるシステム構成品（設備）が設計仕様（同等品でも）と異なる場合、その内容を明記してシステム構成図を作成する | 0111P1-M1C1 | システム構成図と現場機器が合致しているかの確認を行い、引渡す。 | 0111P1-M1O1 | 変更が発生する都度、システム構成図を最新に更新して常に最新に保つ。 | 0111P1-M1R1 | システム構成が更新や改修時に変更があった部分を最新の情報にシステム構成図を改め、古い構成図は廃棄処理を確認する。 |
| 02.バックアップデータ／事業継続 | | | | | | | | | | | | | | |
| 021.適切なバックアップデータがなく、ビルシステムへの被害発生時に復旧作業の支障となる。 | | | | | | | | | | | | | | |
| 0211.バックアップが取られていない、又はバックアップの範囲や対象が適切でない。 | | | | | | | | | | | | | | |
| | | 0211P1 | 0211P1 | システムバックアップ方法を運用例と確認の上でバックアップ方法を設計時に仕様を組み込む。<br>管理ポイントや運転スケジュール等、システムを運用するにあたって必要なデータについては、バックアップを取得する機能を具備する。 | 0211P1-M1 | システムバックアップ周期と操作権限者を定める。その上で、バックアップデータの取得・保管方法と再インストール方法を作成。 | | | 0211P1-M1C1 | 定められた方法で、システムバックアップデータが作成されることを確認する。その上で、作成されたバックアップデータが支障なく再インストールできるか確認しバックアップデータをマニュアルとともに引渡す。 | 0211P1-M1O1 | 運用開始前に、バックアップデータからの復旧再インストールが行えることを確認する。<br>バックアップデータの保管場所管理の定期的確認を行う。<br>管理ポイントや運転スケジュール等、システムを運用するにあたって必要なデータについては、バックアップを取得する。 | 0211P1-M1R1 | 改修時のバックアップデータ廃棄を行う。 |
| 022.システムの脆弱性をついた攻撃を受ける。 | | | | | | | | | | | | | | |
| 0221.脆弱性についての認識が不十分で、脆弱性が残ったままの状態になっている。 | | | | | | | | | | | | | | |
| | | 0221P1 | 0221P1 | 既知の脆弱性に対して必要な対策（パッチ等）が適用されているものを導入し管理する。<br>但し、他機器及び他システムの正常稼動については、担保しなければならない。 | 0221P1-M1 | 設計図書の特記仕様にシステムの脆弱性対策について記載する。<br>システム全体の機能性を担保した上での、必要なアップデート／パッチが適用されている機器であることを仕様に明記する。 | | | 0221P1-M1C1 | システム全体の脆弱性を担保した上での、必要なアップデート／パッチが適用されている機器であることを確認し引渡す。 | 0221P1-M1O1 | ビルシステムのセキュリティ脆弱性に関する情報を定期的に入手し、必要に応じてセキュリティパッチ適用の可否と時期を検討すること。 | | |

図 2-9 ライフサイクルを考慮したセキュリティ対応策のイメージ図[31]

空調システムの個別編の構成は共通編と同様であり、ライフサイクルを考慮したセキュリティ対応策についても作成されている。空調システムは、個別編の第 1 弾として公表されているため、今後ほかの個別システムに関しても公表されると考えられる。

## 2.5.4 防衛産業分野におけるサイバーセキュリティ対策に関する動向

我が国の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、2022 年 4 月に防衛装備庁より、「防衛産業サイバーセキュリティ基準」が新たに整備された。現行の防衛サイバーセキュリティ基準より厳格な管理策が新たに追加されている。本サイバーセキュリティ基準は 2023 年度の契約から適用される。

現行の防衛産業サイバーセキュリティ基準は、ISO/IEC 27001 を基に構築されたサイバーセキュリティ基準であったが、新たに公表された防衛産業サイバーセキュリティ基準は、NIST SP 800-171 を参考に構築されたサイバーセキュリティ基準である。NIST SP 800-171 は米国の NIST が構築した基準であり、米国の国防調達において義務化されている基準である。現行の防衛産業サイバーセキュリティ基準では、NIST Cybersecurity Framework（NIST CSF）における特定・防御までを対象範囲としていたが、新たな防衛産業サイバーセキュリティ基準では、検知・対応・復旧を含めて対象範囲としている。

[31] 経済産業省、ビル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第 1 版別紙
https://www.meti.go.jp/press/2019/06/20190617005/20190617005.html

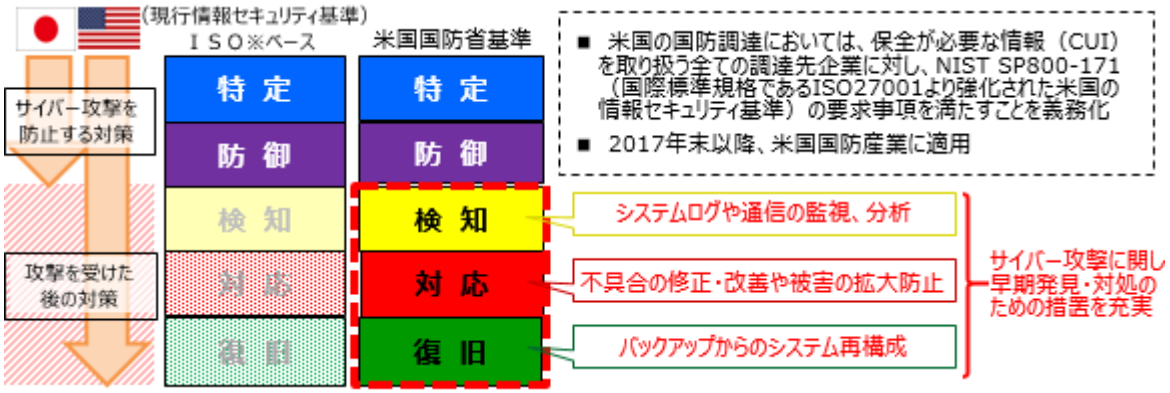



図 2-10 防衛産業サイバーセキュリティ基準の概要[32]

新たに公表された防衛産業サイバーセキュリティ基準の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。本基準は、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。



図 2-11 本紙「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」の目次構成



図 2-12 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」の目次構成

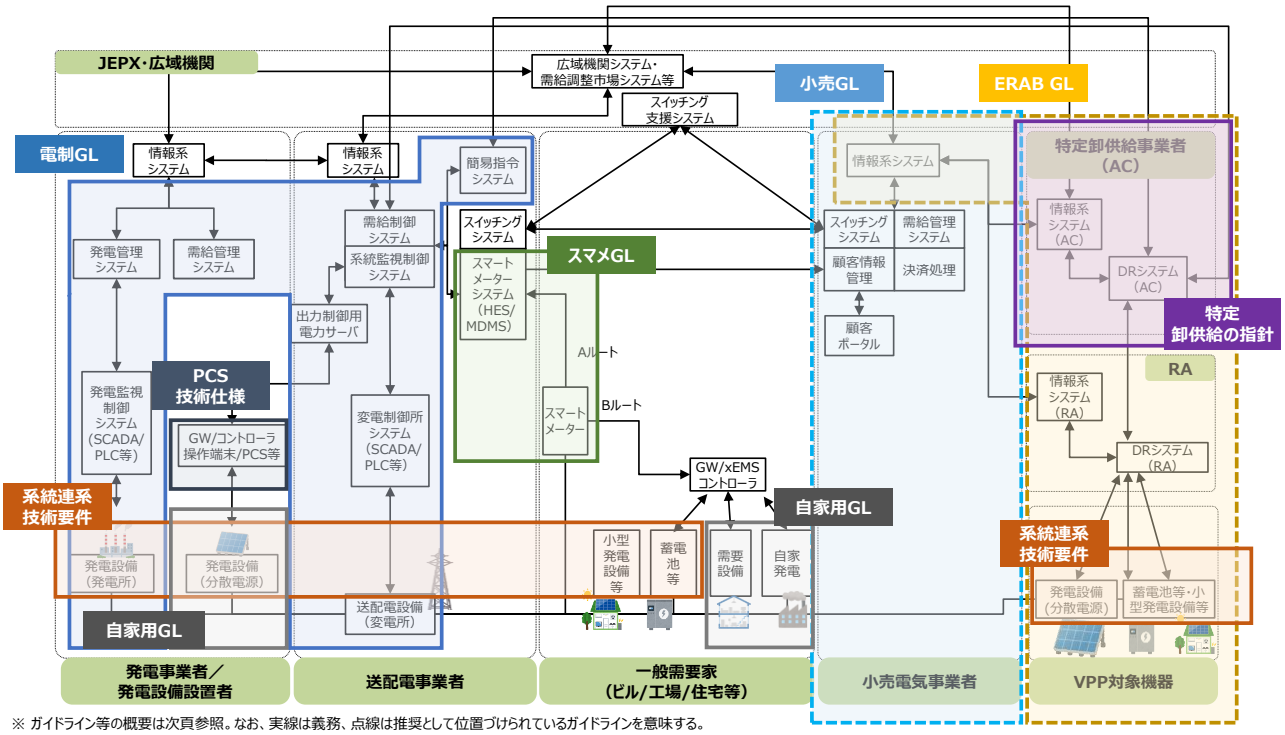
[32] 防衛省、防衛産業サイバーセキュリティ基準の整備について https://www.mod.go.jp/atla/cybersecurity.html

# 3. 電力システムのサイバーセキュリティリスクの分析

国内の電力分野における新規事業者の参入状況やデジタル化の進捗状況等の環境変化を踏まえ、各プレーヤーのリスクを点検するツールの案を作成した。また、作成するツールを関係事業者に普及させるための効果的な方策についても検討した。

## 3.1 電力システムにおけるサイバーセキュリティ対策の取組の現状

これまで、電力 SWG を中心として電力システムに求められるサイバーセキュリティ対策が議論されてきた。電力 SWG 等の議論を通じ、現状では、電力システムのプレーヤーに対して一定の対策が講じられている。電力システムに対するサイバーセキュリティに関する現状の取組は図 3-1 及び表 3-1 のように整理される。




※ ガイドライン等の概要は次頁参照。なお、実線は義務、点線は推奨として位置づけられているガイドラインを意味する。

図 3-1 電力システムにおけるサイバーセキュリティに関する現状の取組概要[33]

[33] 各ガイドライン等の概要は表 3-1 参照。実線は義務、点線は推奨として位置づけられているガイドライン等を意味する。なお、本図は各ガイドライン等の対象を明確化するために作成したものであり、実際の電力システムを精緻に整理したものではないことに留意。

表 3-1 電力システムに関するプレーヤーに求められるガイドライン等

| 名称 | 主な対象 | 発行主体 | 概要 |
|---|---|---|---|
| 電力制御システムセキュリティガイドライン（2019年10月第2版改定） | 電気事業の用に供する電気工作物 | 日本電気協会 | 電気事業法、電気設備に関する技術基準を定める省令及びその解釈に基づき、電気事業者が施設する電力制御システム等及びそれに携わる者に対しては、本ガイドラインに基づく対策が求められる。 |
| スマートメーターシステムセキュリティガイドライン（2019年10月第2版改定） | スマートメーターシステム | 日本電気協会 | 電気事業法、電気設備に関する技術基準を定める省令及びその解釈に基づき、スマートメーターシステムに対しては、本ガイドラインに基づく対策が求められる。 |
| 系統連系技術要件（2020年10月より、セキュリティに関する要件追加） | 系統連系する発電設備 | 各一般送配電事業者 | 系統連系する発電設備にすべからく求められる対策。具体的には、ネットワーク接続点の保護、マルウェア対策、系統運用者に対するセキュリティ管理責任者の通知の3点が求められる。 |
| 出力制御機能付 PCSの技術仕様（2015年5月公開） | 出力制御機能付PCS | JPEA・JEMA・電事連 | 出力制御機能付PCSにおいて満たすべきサイバーセキュリティ対策の要件を示した技術仕様。 |
| 自家用電気工作物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）（2022年6月公開） | 自家用電気工作物（発電設備と需要設備の両方を含む） | 経済産業省 | 自家用電気工作物（発電設備と需要設備の両方を含む）に求められるサイバーセキュリティ対策事項を記載したガイドライン。 |
| 小売電気事業者のためのサイバーセキュリティ対策ガイドライン（2021年2月策定） | 小売電気事業者 | 資源エネルギー庁 | 小売電気事業者が主体的に取り組むことが求められるサイバーセキュリティ対策に関して記載したガイドライン。 |
| ERAB に関するサイバーセキュリティガイドライン Ver2.0（2019年12月改定） | ERAB に関する事業者 | 経済産業省・IPA | ERAB のサービスレベルを維持するためにERAB に参画する各事業者が実施すべき最低限のセキュリティ対策の要求事項を示したガイドライン。 |

図 3-1 に整理されるとおり、これまでの取組を通じて、電力システムのプレーヤーに対して一定の対策が講じられていることが分かる。しかしながら、今後さらなるデジタル化の進展や新規プレーヤーの参入が予想される一方で、2.1 に示すとおりサイバーセキュリティの脅威は日々進化・巧妙化している状況を踏まえると、現状の対策で十分ということは決してなく、電力システムにおけるサイバーセキュリティ対

策の継続的改善・高度化は必要不可欠である。

サイバーセキュリティ対策の継続的改善・高度化に向けては、「電力制御システムセキュリティガイドライン」にも記載のとおり、PDCA サイクルに基づくセキュリティ対策の計画・実施・点検・改善のプロセスが重要となるが、過年度事業の調査によると、対策を実施している事業者の割合と比較して、定期的な対策状況の評価（リスク点検）や継続的な対策改善を実施している事業者は限定的であった。また、過年度及び今年度の調査の結果、定期的なリスク点検実施に当たっての課題として、コスト面、人員面、知識・技術面での課題を事業者が多く抱えていることが明らかになった。

以上を踏まえると、国内の状況について、規制及びガイドラインにより一定の対策が求められているものの、対策の継続的改善に向けた定期的な対策状況の評価（リスク点検）に課題を抱えている事業者が多く存在する状況と言える。この状況を踏まえ、本事業では、国内電力会社が活用できるサイバーセキュリティ対策に係るリスク点検ツールの作成を行った。

## 3.2 ヒアリング調査結果

リスク点検ツールの作成に向けて、各事業者がリスク点検について抱える課題や、その課題を解決するために望まれるツールの位置づけ・内容を把握する目的でヒアリングを実施した。また、ヒアリング結果を踏まえてリスク点検ツールの素案を作成後、作成した素案に対する改善・修正意見を確認する目的で、追加のヒアリングを実施した。表 3-2 に各ヒアリングの目的・実施時期等の概要を示す。

表 3-2 ヒアリングの目的・実施時期・事業者数

| | ヒアリングの目的 | 実施時期 | 事業者数 |
|---|---|---|---|
| ヒアリング 1 | リスク点検ツールの作成に向けて、各事業者がリスク点検について抱える課題やその課題を解決するために望まれるツールの位置づけ・内容を把握すること。 | 2022 年 9 月～ 11 月 | 7 |
| ヒアリング 2 | 作成したリスク点検ツールの素案に対する改善・修正意見を聴取すること。 | 2022 年 12 月～ 2023 年 1 月 | 7 |

### 3.2.1 リスク点検に関するヒアリング（ヒアリング 1）

#### （1） ヒアリング対象者

リスク点検ツールの対象事業者について、一般送配電事業者については電事連によるリスクアセスメントが推進されているところ、発電事業者、小売電気事業者、アグリゲーター（アグリゲーションコーディネーター及びリソースアグリゲーター）及び自家用電気工作物設備設置者の 4 区分を候補とした。ヒアリングに先立ち、各区分について、セキュリティ規制状況、過年度調査から確認できたセキュリティ対策に関する状況、リスク点検に関する課題を整理した。過年度調査より、各事業者によってリスク点検の課題に相違はあるが、コストが高いリスク点検に人員・予算が避けないことやリスク点検の重要性を事業者が理解できていないことが具体的な課題として挙げられた。これらのリスク点検の課題を仮説として、計 7 の事業者に対してヒアリングを実施した。具体的なヒアリング項目及びヒアリング結果は次項以降に示す。

## （2）ヒアリング項目

リスク点検ツールの作成に向けて、サイバーセキュリティリスク点検に関する実施状況、サイバーセキュリティリスク点検に関する課題、作成するサイバーセキュリティリスク点検ツールに対する要望の 3 点について確認した。具体的なヒアリング項目は表 3-3 に示す。

表 3-3 ヒアリング項目

| カテゴリー | ヒアリング項目 |
|---|---|
| サイバーセキュリティリスク点検に関する実施状況 | ● サイバーセキュリティリスク点検を実施している場合、どのようなシステムに対して、どの程度の頻度で実施しているか。<br>● また、リスク点検の実施に当たって活用している既存のガイドラインやツール等はあるか。 |
| サイバーセキュリティリスク点検に関する課題 | 【サイバーセキュリティリスク点検を実施している場合】<br>● リスク点検の実施に当たって抱えている課題はあるか。<br>【サイバーセキュリティリスク点検が現状十分に実施できていない場合】<br>● 現状リスク点検が十分にできていない要因として、どのような要因があるか。 |
| サイバーセキュリティリスク点検ツールに対する要望 | ● 本事業で作成するリスク点検ツールを活用するために、ツールに関する要望などはあるか。 |

## （3）ヒアリング結果

ヒアリング結果を表 3-4 にまとめる。リスク点検の実施状況として、定期的に実施できている企業から全く実施できていない企業がいることを確認できた。また、リスク点検の実施に関する課題として、コスト面、人員面（リソース面）、知識・技術面での課題が挙げられた。リスク点検ツールに対する要望として、可能な限りコストをかけずに実施できることや、既存の電力広域的運営推進機関（広域機関）のチェックリストと対応付けられるツールであることが意見された。

表 3-4 ヒアリング結果の概要

| カテゴリー | ヒアリング項目 |
|---|---|
| サイバーセキュリティリスク点検に関する実施状況 | ● 発電所に対して、東京オリンピックを背景に 3 年前に電制 GL を用いて全社的な点検を実施した。現状は、リスク点検の実施を各発電所に委ねている。VPP については、ERAB・電制 GL に基づき要件定義を実施した。<br>● セキュリティ点検の必要性は感じているが、会社の承認が得られず、実施できていない。<br>● 小売システム・DR システムに対して年に一度点検を実施している。リスク点検は電制・ERAB ガイドラインを基に実施している。<br>● ISMS 活動の一環としてリスク計画を策定してリスク評価を行ってい |

| カテゴリー | ヒアリング項目 |
| --- | --- |
| | るほか、広域機関のチェックリストに基づくリスク点検を行っている。<br>● 年 1 回のペースで親会社主導のリスク点検を実施してきたほか、広域機関のチェックリストに基づくリスク点検も毎年実施している。 |
| サイバーセキュリティリスク点検に関する課題 | ● コンサルを使用せず自社のみでリスク点検を行うというのは、ノウハウがないので困難である。リスク点検の必要性は感じているが、コスト・人・技術全てのリソースが不足している状況である。<br>● コストの観点から、経営層に対して必要性を訴求できていない。<br>● リスク点検を行う現場においてセキュリティの専門家が存在せず、回答に時間を要することがある。<br>● コスト面・人材面の課題があり、ノウハウ・知識の継承が難しい。また、脆弱性が発見された場合の対策の実施判断が難しい。<br>● 従業員のセキュリティリテラシーが低いという課題がある。 |
| サイバーセキュリティリスク点検ツールに対する要望 | ● コストをかけず、リスクが可視化されると良い。また、点検の結果、具体的に求められるアクションが分かると良い。<br>● セキュリティの知識がない現場の人でも、コストをかけずにリスク点検ができるものになると良い。<br>● 他設問の回答によって回答項目を減らすことができる階層的な構造であると良い。また、各項目の意義や想定されるリスクが明記されていると良い。解説があることでセキュリティ意識も高まる。<br>● リスクがあった際、具体に望まれるアクションについても記載いただきたい。また、広域機関のチェックリストも対応するとなるとコストがかかるため、統合されると良い。加えて、新たなリスクや最新情報を踏まえ、ツールは定期的に更新されることが望ましい。<br>● チェック項目が簡素化されると良い。また、リスク点検後の具体的な対策案を解説として掲載していただきたい。 |

### 3.2.2 作成したリスク点検ツールに関するヒアリング（ヒアリング 2）

#### （1） ヒアリング対象者

作成したリスク点検ツールに関する意見を確認することを目的にヒアリングを実施した。ヒアリング企業の対象者は前回のヒアリングと同様にリスク点検ツールの対象事業者に対して、計 7 事業者に対して実施した。

#### （2） ヒアリング項目

リスク点検ツールに対する意見を確認することを目的に、サイバーセキュリティリスク点検ツールの対策状況可視化ツールの「チェックシート」の改善点、サイバーセキュリティリスク点検の対策状況可視化ツールの「可視化結果」の改善点、サイバーセキュリティリスク点検ツールの活用に対する意見の 3 点に

ついて確認した。具体的なヒアリング項目は表 3-5 に示す。

表 3-5 ヒアリング項目

| カテゴリー | ヒアリング項目 |
|---|---|
| サイバーセキュリティリスク点検ツールの対策状況可視化ツールの「チェックシート」の改善点 | ● リスク点検項目の達成基準の具体性は適切か。<br>● リスク点検項目と対応付けしてほしいガイドラインはほかにあるか。また、現状の対応付けに関して意見はあるか。<br>● 現状のリスク点検項目に基づくリスク点検を実施した場合、どの程度の追加の負荷（追加コスト）を要すると想定するか。<br>● その他、対策状況可視化ツールの「チェックシート」について意見はあるか。 |
| サイバーセキュリティリスク点検の対策状況可視化ツールの「可視化結果」の改善点 | ● 可視化しているスコア以外に、「可視化結果」シートに含めるべき情報はあるか。<br>● その他、対策状況可視化ツールの「可視化結果」について意見はあるか。 |
| サイバーセキュリティリスク点検ツールの活用に対する意見 | ● 紹介した活用方法以外に、社内で検討されうる活用方法はあるか。特に外部関係者へ報告する際にチェックシートを利用できる場合は、その用途は何か。<br>● リスク評価結果の活用に当たって、ガイドラインに追記すべき内容はあるか。<br>● その他、サイバーセキュリティリスク点検ツールに対する意見はあるか。 |

## （3）ヒアリング結果

ヒアリング結果を表 3-6 にまとめる。ヒアリングでは、リスク点検ツールに対して項目の内容や達成基準の具体性等に関する肯定的な意見が多く、ツールの位置づけや構成については問題ないことを確認できた。「チェックシート」・「可視化結果」やリスク点検ガイドに関して修正すべき意見に関しては、リスク点検ツールの修正を行った。また、その他の意見に関しては、リスク点検ツールの普及促進策や運用方法に関連する内容であり、次年度に向けた取組として検討した。

表 3-6 ヒアリング結果の概要

| カテゴリー | ヒアリング項目 |
|---|---|
| サイバーセキュリティリスク点検ツールの対策状況可視化ツールの「チェックシート」の改善点 | ● 「対策を怠った場合のリスク」において、リスクが起きる原因について明記できると良い。<br>● 達成基準のレベル感を合わせ、より選択しやすくできると良い。<br>● 点検の実施時期を確認できる欄を設けられると良い。 |

| カテゴリー | ヒアリング項目 |
| --- | --- |
| | ● 最初のチェックには時間がかかることが予想できる。リスク点検項目と文書を照らし合わせる管理台帳を用意すれば、2 回目以降は初回より少ない時間で実施できると思う。 |
| サイバーセキュリティリスク点検の対策状況可視化ツールの「可視化結果」の改善点 | ● 経営層への訴求においても、自身の対策スコアを比較できる基準値があると良い。基準値を記載する際には、最低限の目標としつつ、定期的に改善することが必要な旨を明記することが望まれる。<br>● 自社に該当しない項目を可視化から除外できるようカスタマイズできると良い。 |
| サイバーセキュリティリスク点検ツールの活用に対する意見 | ● リスク点検結果に対する改善策については、事業者として予算上の関係で対応できない可能性もあるため、参考・推奨であることを明記できると良い。一方で、経営層への予算確保にも利用したいため、バランスをとった記載であるとなお良い。<br>● スコアの収集などを目的にする場合はツールのオンライン化も検討できると良い。<br>● アグリゲーションコーディネーターのライセンス取得時にセキュリティへの対応が求められるので、その申請の際に活用できると良いと感じる。<br>● 点検結果をホームページ上で対外向けに公開し、自社のセキュリティ対策の実情を示すことに使用することも考えられる。<br>● 本リスク点検ツールが業界標準として使用されるようになり、事業者へ提示することができるようになれば理想である。 |

## 3.3 リスク点検ツールに関する概要

### 3.3.1 全体構成

ヒアリング及び電力 SWG で挙げられた意見を踏まえ、リスク点検ツールの案を作成した。リスク点検ツールの全体構成は図 3-2 に示すとおりであり、「電力システムにおけるサイバーセキュリティリスク点検ガイド（リスク点検ガイド）」と「電力システムにおけるサイバーセキュリティ対策状況可視化ツール（対策状況可視化ツール）」によって構成した。

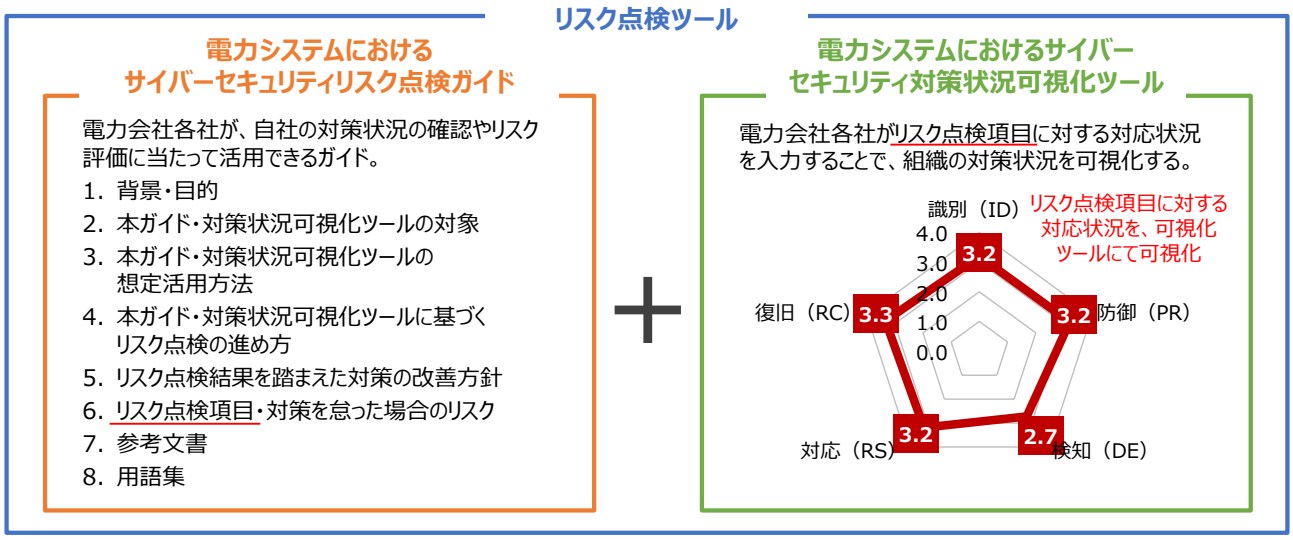



図 3-2 リスク点検ツールの全体構成

リスク点検ガイドは、国内電気事業者において自社の対策状況の確認やリスク評価に当たって活用できる文書であり、本リスク点検ツールの対象や想定活用方法、リスク点検ツールを活用したリスク点検の進め方を詳細に示した。また、具体的なリスク点検項目を示しつつ、リスク点検結果を踏まえた対策の改善方針も含めた。加えて、リスク点検は主に対策状況可視化ツールを用いて行うところ、対策状況可視化ツールの具体的な使い方についても記載した。

対策状況可視化ツールは、各事業者がリスク点検項目に対する対応状況を入力することで簡易に組織の成熟度や対策状況を可視化できるツールとし、Excel 形式にて作成した。対策状況可視化ツールの概要は 3.3.5 に示す。

## 3.3.2 対象事業者

リスク点検ツールの対象事業者について、一般送配電事業者については電事連によるリスクアセスメントが推進されているところ、本リスク点検ツールでは、発電事業者、小売電気事業者、アグリゲーター（アグリゲーションコーディネーター及びリソースアグリゲーター）及び自家用電気工作物設備設置者の 4 区分を主な対象とした。ヒアリングで意見されたとおり、大手事業者の多くはリスク点検を既に定期的に実施しているところ、本事業で開発するリスク点検ツールでは、中小事業者をはじめとするこれまでリスク点検を実施してこなかった事業者をメインスコープとし、当該事業者における簡易的かつ効率的なリスク点検を支援する内容とした。

## 3.3.3 想定活用方法

本ガイド及び対策状況可視化ツールの活用方法として、以下の 4 つの活用方法を設定した。

- セキュリティ対策状況の点検・改善に向けた活用：
  リスク点検ツールを活用して自社のセキュリティ対策状況を点検することで、対策が十分に実施できていない項目を可視化することができる。また、可視化の結果を踏まえ、対策の改善のためにどのような方策が望まれるかを確認することができる。

- セキュリティ対策検討における活用：
  国内のセキュリティガイドラインに遵守するためにどのような対策を実施する必要があるか、その対策を怠った場合にどのようなリスクがあるか、対策の達成基準はどのようなものかといった情報を踏まえ、自社のセキュリティ対策検討を効果的に進めることができる。
- セキュリティに関する社内教育・訓練・意識啓発活動への活用：
  リスク点検ツールを活用して自社のセキュリティ対策状況を把握・可視化することで、その結果を社内教育や訓練に組み込むとともに、対策状況を踏まえた意識啓発活動を行うことができる。
- 電力広域的運営推進機関等の外部関係者に対するセキュリティ対策状況報告における活用：
  自社のセキュリティ対策状況について広域機関等の外部関係者に報告する際、リスク点検ツールを活用して可視化した結果を報告することができる。

最後の項目について、広域機関では、会員企業のサイバーセキュリティ対策向上の一環として、各会員自らの情報セキュリティ対策レベルを把握し、対策を促すための自己診断ツールを任意の取組として運用している。今回のリスク点検ツール作成に合わせて、広域機関の自己診断ツールを今回のリスク点検ツールと連携する予定であり、連携に向け広域機関と複数回協議を行った。

本リスク点検ツールを用いたリスク点検の全体プロセス概要を図 3-3 に示す。本図に示すとおり、リスク点検のプロセスを準備、実施、結果を踏まえた改善検討の大きく 3 つのフェーズに分け、各フェーズにおける実施内容をリスク点検ガイドで記載した。また、図 3-3 に示しているとおり、実効性のあるリスク点検を行い、その結果を踏まえて対策を継続的に改善するために、経営層への報告が望まれる内容を明記した。

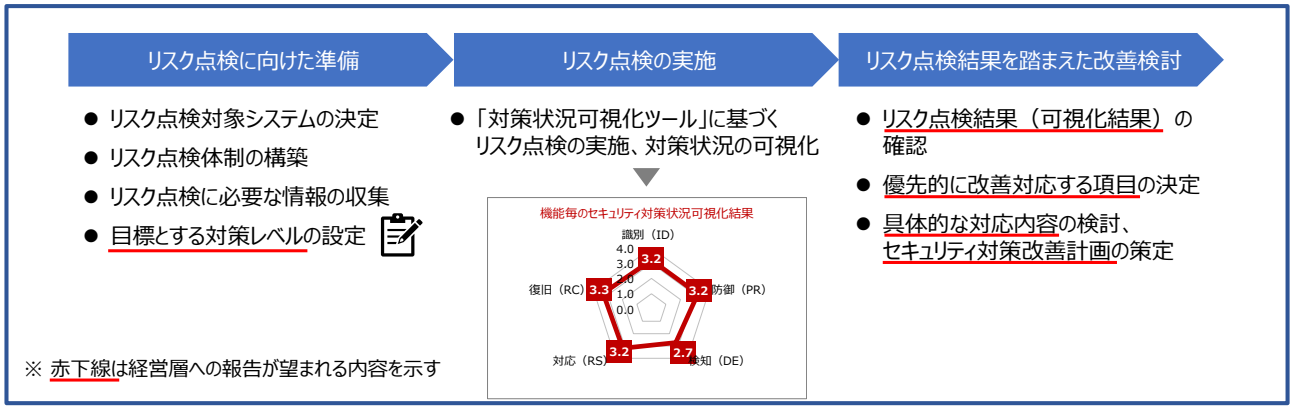



図 3-3 リスク点検の全体プロセス概要

## 3.3.4 リスク点検項目

本リスク点検ツールにおけるリスク点検項目は、国内外の電力会社において広く活用され、様々な事業区分に活用可能な米国 NIST の Cybersecurity Framework（NIST CSF） Version 1.1 を参考に整理した。NIST CSF では、5 つのセキュリティ機能（識別、防御、検知、対応、復旧）に対し、機能の詳細を定めた 23 のカテゴリー、108 のサブカテゴリーが定義されているが、本リスク点検ツールでは、108 のサブカテゴリーをリスク点検項目として設定した。

リスク点検を実施する電力会社の対策レベルを可視化するために、各リスク点検項目に対して、0～4の 5 段階の達成基準を設定した。具体的には、NIST CSF のティアの概念を参考に、0：対応できていない状態、1：部分的に対応できている状態、2：リスクが認識できる状態、3：対応に再現性がある状態、4：変化に適用可能な対応がある状態といった水準で達成基準を設けた。例えば、「ID.GV-1：組織のサイバーセキュリティポリシーが、定められ、周知されている。」というリスク点検項目について、以下の 5 段階の達成基準を設定した。

- 0: 対応なし。
- 1: 個々のシステムにおいて、独自にセキュリティ対策が検討され、適用されている。
- 2: 1 に加え、社内の各組織において、個別にセキュリティルールが策定され、遵守が求められている。
- 3: 2 に加え、会社のセキュリティポリシーが文書で規定され、社内に周知されている。
- 4: 3 に加え、会社のセキュリティポリシーは、社内外の最新の情報・動静を踏まえ、定期的に見直されている。

### 3.3.5 対策状況可視化ツールの概要

前述のとおり、リスク点検は主に対策状況可視化ツールを用いて行うことが想定される。本事業で作成した対策状況可視化ツールは、「チェックシート」「可視化結果」、「可視化結果（広域機関用）」の 3 つのシートで構成され、電力会社各社が「チェックシート」において各リスク点検項目に対する対応状況を選択・入力することで、対策の状況が「可視化結果」のシートに表示される形式とした。「チェックシート」の概要を図 3-4 に示す。リスク点検のために電力会社が選択・記入する必要があるセルは黄色塗りしている。（図 3-4 において赤枠で囲っている箇所）

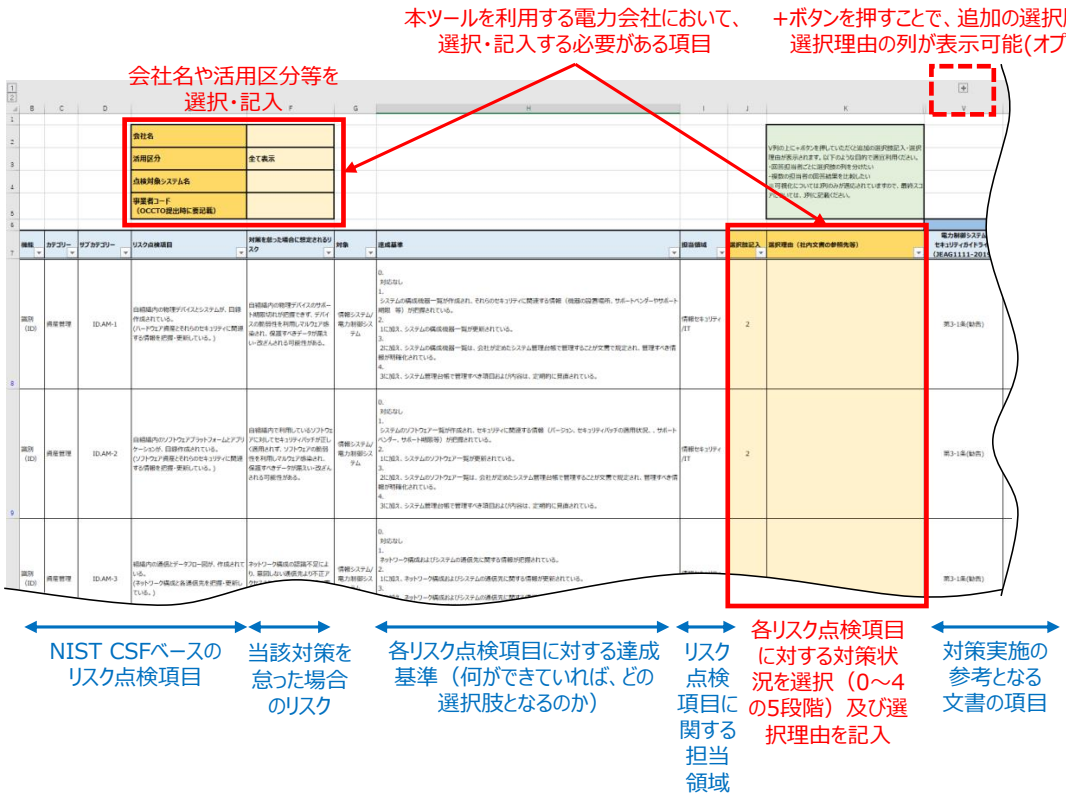



図 3-4 対策状況可視化ツールの「チェックシート」の概要

「チェックシート」では NIST CSF ベースのリスク点検項目、当該対策を怠った場合に想定されるリスク、リスク点検項目に対する達成基準（0～4 の 5 段階）、リスク点検項目に関する担当領域を明記した。ツールを活用する電力会社においては、各リスク点検項目に対する達成基準を踏まえ、対策状況の選択（0～4 の 5 段階）及び選択理由の記入が求められる。リスクを点検する上では関係部署との連携が必要であるところ、各点検項目の回答に適した担当領域を明記した。具体的には、経営層、情報セキュリティ/IT、制御セキュリティ/OT、人事、リスク/法務、購買/調達の 6 領域を設定した。また、回答担当者ごとに選択肢の列を分けたい場合や複数の回答者の結果を比較したい場合を想定し、Excel 上で追加の選択肢記入・選択理由記入の列を表示することができる形式とした。

各リスク点検項目について、リスク点検ツールの対象事業者が確認すべきガイドライン項目との対応関係も示した。特に、以下のガイドラインとの対応関係を示した。

- 電力制御システムセキュリティガイドライン（JEAG1111-2019）
- ERAB に関するサイバーセキュリティガイドライン Ver 2.0
- 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 Ver 1.0
- 系統連系技術要件【託送供給等約款別冊】
- 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）
- 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
- サイバーセキュリティ経営ガイドライン Ver 2.0

対策状況可視化ツールの「チェックシート」のうち、「活用区分」に関する項目はプルダウン形式とし、本ガイド及び対策状況可視化ツールが対象とする 4 つの事業区分（「発電事業者」、「小売電気事業者」、

「アグリゲーター」、「自家用電気工作物設備設置者」)、「広域機関提出用」、そして「全て表示」が選択できる形とした。「全て表示」では、NIST CSF の 108 項目に対応する全てのリスク点検項目が表示されるが、事業区分を選択した場合、当該区分に関連するガイドライン項目との対応が付けられたリスク点検項目のみが抽出して一覧表示される。これにより、リスク点検を行う電力会社が自社の事業者区分に関係するリスク点検項目のみを効率的に確認することが可能である。なお、対策状況可視化ツールを用いて実施したリスク点検の結果を広域機関に提出する場合、「広域機関提出用」を選択し、抽出されたリスク点検項目に対して選択及び選択理由を記入する必要がある形式とした。

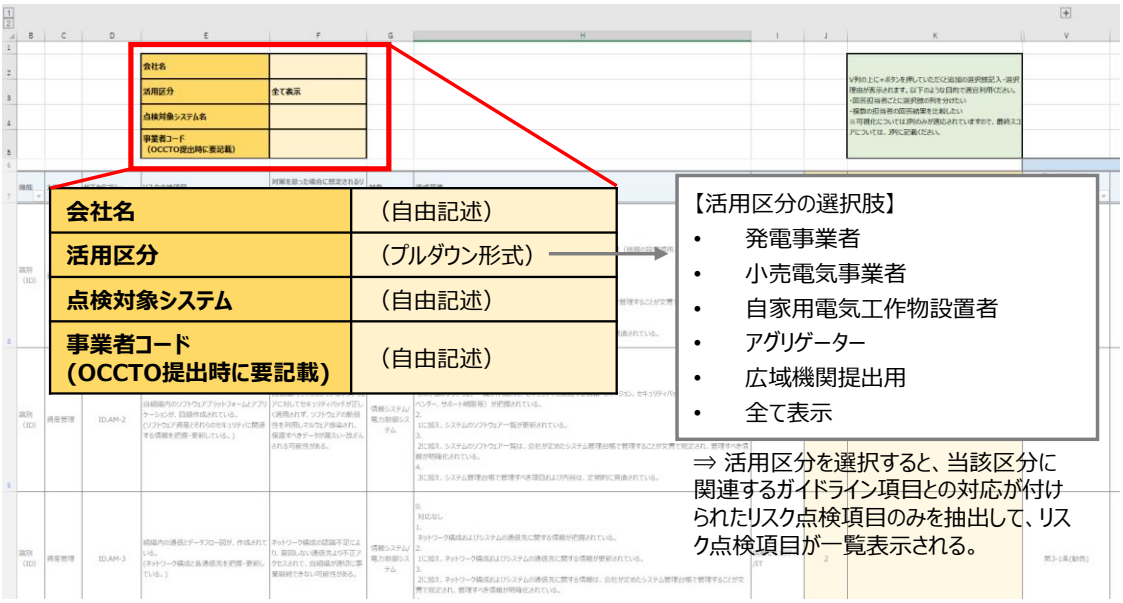



図 3-5 対策状況可視化ツールの「チェックシート」における「活用区分」の位置づけ

抽出された全てのリスク点検項目に対して対策状況を選択することで、「可視化結果」シートに対策状況が可視化される形とした。図 3-6 に示すとおり、対策状況の可視化結果は NIST CSF の 5 つのセキュリティ機能ごと(識別、防御、検知、対応、復旧)及び各機能のカテゴリーごとに表示される形式とした。なお、可視化されるスコアは、「活用区分」を選択後に抽出された各リスク点検項目に対する電力会社の選択(0～4 の 5 段階)の平均値である。

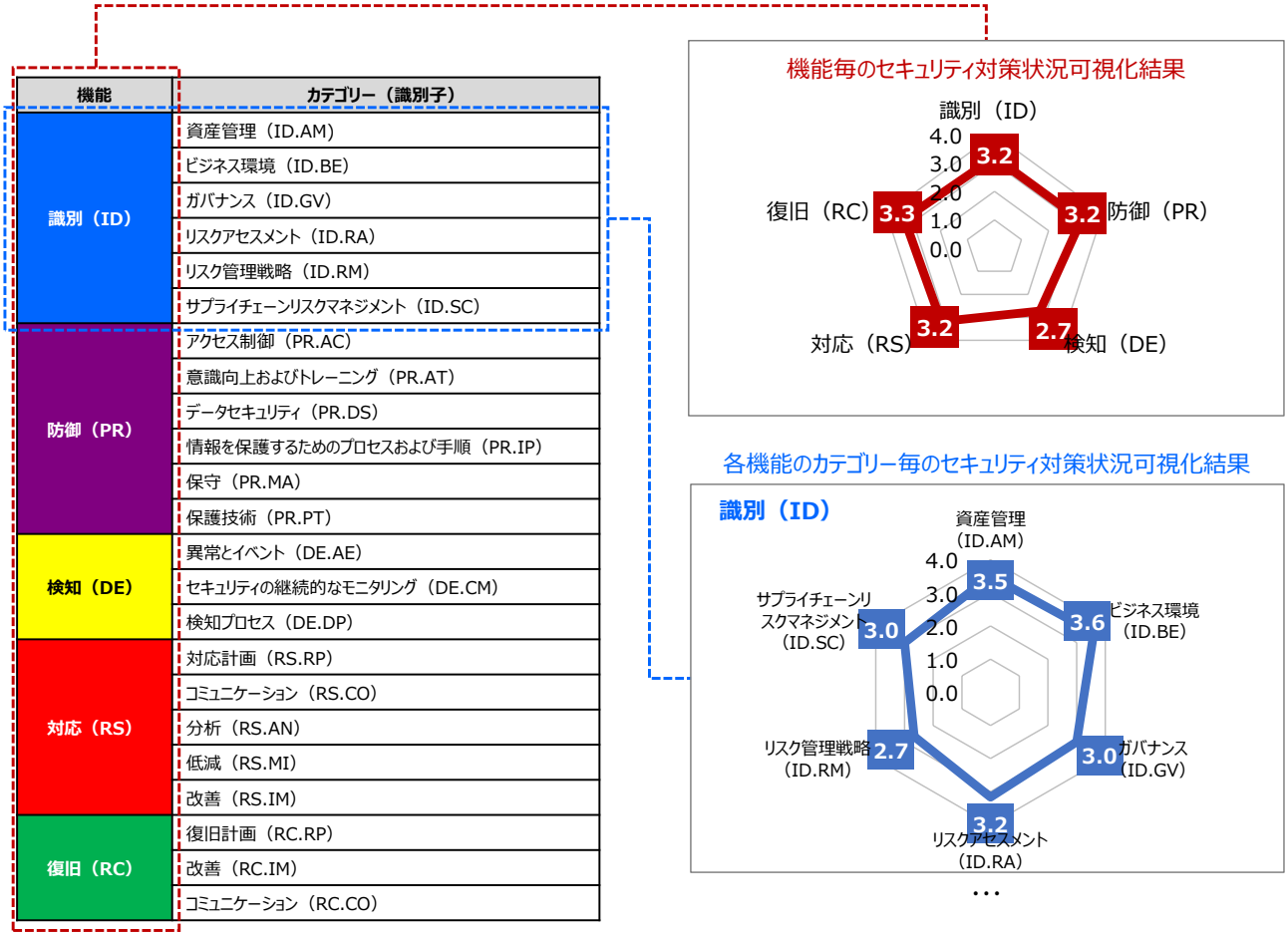



図 3-6 NIST CSF の機能･カテゴリーと対策状況可視化結果の関係

## 3.4 次年度以降の取組

今年度事業を通じてリスク点検ツールの案を作成した。次年度の正式公開に向け、次年度議論すべき内容として、大きく 2 点挙げられる。1 点目として、ヒアリング等では得られなかったリスク点検ツールの細かい修正点や、ツールに基づくリスク点検に要するコスト･スキル等を確認することを目的に、ツールの試行利用を検討する必要がある。2 点目として、リスク点検ツールの公開に向け、リスク点検ツールの普及促進策や運用方法について、検討する必要がある。

試行利用は、次年度の公開に向けてツールの最終確認を行い、改善することを主な目的とする。試行利用を検討する上で、試行利用の対象事業者と試行利用における確認事項の洗い出しを行う必要がある。本リスク点検ツールは、発電事業者、小売電気事業者、アグリゲーター（アグリゲーションコーディネーター及びリソースアグリゲーター）及び自家用電気工作物設備設置者の 4 区分を主な対象とし、特に中小事業者をはじめとするこれまでリスク点検を実施してこなかった事業者をメインスコープとしている。そのため、リスク点検を実施してこなかった事業者を高い優先度としつつ、様々な事業者のリスク点検状況に応じた確認項目を設定して、試行利用を行うことが効果的だと考えられる。試行利用の具体的な対象事業者は、リスク点検状況を詳細に把握できているヒアリング対象事業者を第一候補にすることが望まれる。

普及促進策・運用方法について、現時点では、リスク点検ツールを任意で活用可能なツールとして資源エネルギー庁のホームページ等で提供することが現実的である。その上で、さらに普及を行う取組が想定される。具体的には、以下のような普及促進策が効果的と考えられる。

- 太陽光発電協会・風力発電協会等の事業者が所属している業界団体を通じた周知・展開
- 各事業者に対してエネ庁から個別に周知・展開
- 自家用電気工作物におけるセキュリティ対策の実装を行う電気主任技術者が所属する日本電気技術者協会などとの業界団体と連携し、本ツールを周知・展開
- 本ツールが電力業界における業界水準となるよう、電力事業のサプライチェーン上のリスク管理における推奨ツールとして広く展開

上記の取組以外に、ツール利用の支援を委託する事業者を可視化し、その事業者によってツール利用が継続的に利用・改善される体制の構築も重要であると考えられる。自社のみでツールを利用することが難しい電力事業者に対して、ツール利用の支援を委託できる事業者を紹介することで、ツールの継続利用・高度化につながると考えられる。このような体制を構築する上で、事業者への委託・支援をサポートする補助金制度等、資金の流れを検討することが望まれる。同様に、ツールの利用を支援する目的で、リスク点検ツールの状況に応じて相談できる窓口やフォローアップの機会を設けることが望まれる。例えば、業界団体における相談窓口の設置などが検討されうる。

中長期的なリスク点検ツールの運用に関して、一社での運用に限らず、電力サプライチェーンに関係する企業間で相互運用するほか、その他の重要インフラ分野への横展開も検討される。水道・電力・ガス・医療等の重要インフラには相互に依存関係があるため、電力分野だけではなく、関連する重要インフラ分野と連携した取組も想定される。

# 4. ワーキンググループの運営

有識者（学識経験者やサイバーセキュリティ関連団体等を含む）や電気事業者等の委員によって構成され、我が国の電力分野における更なるサイバーセキュリティ向上策についての検討を行う、産業サイバーセキュリティ研究会ワーキンググループ 1 傘下の電力 SWG が、経済産業省によって開催されており、本事業ではその運営を行った。

## 4.1 第 14 回電力 SWG の運営

第 14 回 SWG では、電力分野におけるサイバーセキュリティの取組の現状について、電力分野におけるセキュリティリスク点検ツールの作成について議論が行われた。また、経済安全保障推進法の状況について報告が行われた。

電力分野におけるサイバーセキュリティの取組の現状について、電力分野におけるインシデント状況と国内外の電力に関する動向について議論が行われた、また、電力分野におけるセキュリティリスク点検ツールの作成について、作成したセキュリティリスク点検ツールの素案の方向性や内容について議論が行われた。経済安全保障推進法の状況について、報告された。

産業サイバーセキュリティ研究会 WG1 電力 SWG（第 14 回）議事要旨

日時　　：令和 4 年 12 月 22 日（木）13 時 00 分～15 時 00 分
出席者　：
（座長）
渡辺 研司　　名古屋工業大学大学院
（委員）
有村 浩一　　JPCERT/CC
稲垣 隆一　　稲垣隆一法律事務所
内田 忠　　電力 ISAC
江崎 浩　　東京大学大学院
大崎 人士　　産業技術総合研究所
大浪 哲　　電気事業連合会
奥村 智之　　日本電気協会
小野崎 勝徳　　東京電力ホールディングス株式会社
桑名 利幸　　情報処理推進機構
高倉 弘喜　　国立情報学研究所
手塚 悟　　慶應義塾大学
新田 哲　　JFE スチール

議題

1. 電力分野におけるサイバーセキュリティの取組の現状
2. 電力分野におけるセキュリティリスク点検ツールの作成について
3. 経済安全保障推進法の状況について

要旨

1. 電力分野におけるサイバーセキュリティの取組の現状
   (1)「電力分野におけるサイバーセキュリティの取組の現状」を事務局より説明。
   (2) 自由討議
      - 出力制御機能付 PCS の技術仕様について、サイバー脅威の現状を踏まえ、サイバーセキュリティに関する内容の改訂を検討すべきではないか。
      - 力分野におけるサイバーセキュリティ対策の検討に当たっては、電力安定供給のみを目的にするのではなく、データの安全性に対する対策の検討も必要である。
      - 製品におけるセキュリティ対策に当たっては、適合性証明の透明性やアカウンタビリティの確保に向けた取組も検討する必要がある。
      - 対策の責任主体が多様化しているところ、個々のガイドラインだけではなく、電力制御システム全体に求められる対策について俯瞰できると良い。
      - ディマンド・リスポンスの推進に併せて、需要家に対するセキュリティ対策の取組が必要である。
      - 電気工作物に対するセキュリティ対策だけではなく、スコープを拡大する必要がある。

2. 電力分野のセキュリティ対策の高度化に向けた取組の方向性について
   (1)「電力分野におけるセキュリティリスク点検ツールの作成について」を事務局より説明。
   (2) 自由討議
      - リスク点検の実施者に求められるスキルレベルを明確にすると良い。
      - 本リスク点検ツールを参考に、事業者の状況に合わせて事業者自身が適宜加工しつつ、本格的なセルフアセスメントにも活用できる形式とすることが良い。
      - セキュリティ対策の課題を企業統治の観点で可視化するために、複数の担当者が回答できるリスク点検ツールにすると良い。
      - 過度に回答欄を増やすと事業者の負担になりかねない。バランスを踏まえた設計が必要である。
      - リスク点検ツールを普及させるためには、事業者の取組と足並みを揃える必要がある。事業者の現行の取組を阻害しない形で改善の取組を支援できると良い。
      - 将来的には、リスク点検項目に対する対策状況を自動で評価できる仕組みが開発できると良い。
      - 中小規模の事業者に対して支援を行うことが、リスク点検ツールを普及する上で重要である。
      - リスク点検ツールの試行利用先については、事業区分だけでなく、事業規模や事業形態を踏まえた検討が必要である。
      - リスク点検結果を踏まえ残存リスクを把握しつつ、セキュリティ対策の継続的改善に向

けたさらなる計画を立てることが重要である。
- リスク点検結果は機微情報に当たるため、取扱いには留意する必要がある。
- リスク点検の結果、対策が不十分と明らかになった事業者に対して、最優先で取り組むべき事項を明確化できると良い。
- 事業者において、リスク点検結果を踏まえた対策改善の必要性を適切に認識いただく必要がある。
- リスク点検ツールの普及に向けて、ツールの位置づけを今後検討することが重要である。

3. 経済安全保障推進法の状況について

(1)「経済安全保障推進法の状況について」を事務局より説明。

## 4.2 第 15 回電力 SWG の運営

第 15 回 SWG では、電力分野におけるセキュリティリスク点検ツールの作成について議論が行われた。また、サイバーセキュリティ施策の取組状況について報告が行われた。

電力分野におけるセキュリティリスク点検ツールの作成について、セキュリティリスク点検ツールの修正内容や試行利用・普及促進策について議論が行われた。修正した素案の方向性や内容について議論が行われた。経済安全保障推進法の状況について、報告された。

産業サイバーセキュリティ研究会 WG1 電力 SWG(第15回)議事要旨

日時　　:令和5年2月20日(月)10時00分～11時30分
出席者　:
(座長)
渡辺 研司　　名古屋工業大学大学院
(委員)
有村 浩一　　JPCERT/CC
稲垣 隆一　　稲垣隆一法律事務所
内田 忠　　電力 ISAC
大崎 人士　　産業技術総合研究所
大浪 哲　　電気事業連合会
奥村 智之　　日本電気協会
小野崎 勝徳　　東京電力ホールディングス株式会社
門林 雄基　　奈良先端科学技術大学院大学
桑名 利幸　　情報処理推進機構
新　誠一　　電気通信大学
高倉 弘喜　　国立情報学研究所

議題

1. 電力分野におけるセキュリティリスク点検ツールの作成について
2. サイバーセキュリティ施策の取組状況について

要旨

1. 電力分野におけるセキュリティリスク点検ツールの作成について

（1）「電力分野におけるセキュリティリスク点検ツールの作成について」を事務局より説明。

（2）自由討議

- リスク点検項目とその補足内容との整合が取れている必要がある。
- リスク点検ツールに用いられる用語の定義は明確にする必要がある。
- リスク点検ツールは早い段階で試行いただき、継続的に改善することが重要である。
- 試行利用で得られた結果を踏まえ、リスク点検ツールの精査・修正を行うことで、実効性のある取組になると考えられる。
- リスク点検の実施者に求められるスキルレベルについて、既存の資格で求められる内容と対象企業の実態を踏まえて整理すると良い。
- リスク点検結果を保存し、次回のリスク点検時や事故発生時に活用することの必要性を明記する必要がある。
- リスク点検ツールは、一社に限定した取組ではなく、電力業界のサプライチェーンや他の重要インフラ分野と連携した取組として活用できると良い。
- 自社のリスク点検結果と比較できる基準値を検討することが重要である。基準値の検討にあたっては、業界団体と連携しつつ、業界毎の基準値も検討できると良い。
- 十分な取組が難しい事業者に対する相談窓口や支援の検討が必要である。
- リスク点検ツールを広く普及する上で、ツールを活用することのメリットを訴求することが必要である。各事業者が自発的に活用した結果、ツールを使うことが業界標準となるようなエコシステムが構築できると良い。
- 事業者が既に実施している取組と整合が図れる形でツールの運用方法が検討されると良い。
- 将来的には、リスク点検結果を踏まえた対策の改善を継続的に行うために、リスク点検項目に対する改善計画をツール内に記載できるとよい。
- リスク点検ツールの普及促進策について、ツール利用にあたって支援を受けることができる事業者を可視化する取組が必要ではないか。さらに、当該事業者によるツールの継続的改善のほか、当該事業者を支援する資金の流れを検討することが望まれる。ツールの継続的改善にあたっては、人材育成の観点も考慮することが望まれる。
- リスク点検ツールが対象とする電力会社が扱う情報資産の特性が異なることを踏まえ、強制的に使わせるのではなく、自発的に活用いただく環境づくりが重要である。

2. サイバーセキュリティ施策の取組状況について

（1）「サイバーセキュリティ施策の取組状況について」を経済産業省サイバーセキュリティ課より説明。

# 5. まとめ

本事業では、大手電力会社や新規プレーヤーにおけるサイバーセキュリティ対策等のサイバーセキュリティ上の課題に対する具体的な制度等の設計に向けて、国内外の電力サイバーセキュリティ対策やサプライチェーンリスクへの対策の動向等や参考となる他分野の対策状況について整理・分析した。また、各プレーヤーのリスクを点検するツールの案を作成するとともに、当該ツールを関係事業者に普及させるための効果的な方策についても検討した。加えて、我が国の電力分野における更なるサイバーセキュリティ向上策についての検討を行う電力 SWG の運営を行った。

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のあり方に関する詳細調査分析） 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のあり方に関する詳細調査分析）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のあり方に関する詳細調査分析）

株式会社三菱総合研究所

| 頁 | 図表番号 | タイトル |
|---|---|---|
| 34 | 図2-3 | 発電設備の保安管理業務を外部委託する場合の対象システムの範囲の例（発電設備の出力制御コマンドが遠隔サービス提供事業者のシステムを介して発電設備側に伝達される例） |
| 35 | 図2-4 | 発電設備の保安管理業務を外部委託する場合の対象システムの範囲の例（発電設備の出力制御コマンドが系統接続先の電力会社から別のシステムを介して伝達される例） |
| 35 | 図2-5 | 需要設備の保安管理業務を外部委託する場合の対象システムの範囲の例 |
| 38 | 図2-6 | 工場におけるセキュリティ対策企画・導入の進め方 |
| 39 | 図2-7 | 工場セキュリティガイドラインにおけるチェックリストの概要 |
| 40 | 図2-8 | 民間宇宙システムの標準的なモデル |
| 42 | 図2-9 | ライフサイクルを考慮したセキュリティ対応策のイメージ図 |
| 43 | 図2-10 | 防衛産業サイバーセキュリティ基準の概要 |