資源エネルギー庁 御中

# 令和５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向上に向けた調査）

## 報告書

三菱総合研究所

先進技術・セキュリティ事業本部

2024年2月29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。こうした動きに伴い、サイバー攻撃を受ける可能性や攻撃箇所が増加するとともに、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必要があり、サイバーセキュリティ確保の重要性はこれまでになく高まっている。

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

## 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. 電力システムにおけるサイバーセキュリティ対策状況可視化ツール（以下「リスク点検ツール」と言う。）の試行利用・正式公開
3. 分散型エネルギーリソースに係るセキュリティ対策の検討
4. サプライチェーンセキュリティ対策の高度化に向けた検討
5. 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 重要インフラ分野における近年のセキュリティインシデント事例

近年発生した重要インフラ分野におけるセキュリティインシデント事例を以下に示す。

### 2.1.1 国内重要インフラ分野における近年のセキュリティインシデント事例

国内重要インフラ分野における近年のセキュリティインシデント事例を表 2-1 に示す。表中 9 件がランサムウェア攻撃被害を原因としたセキュリティインシデント事例であり、国内重要インフラ分野におけるランサムウェア脅威の高まりを確認できる。また、No.10 の事例は、委託先の不正アクセス被害を起因としたセキュリティインシデントであり、サプライチェーン・リスクが顕在化した事例の一つである。こうしたインシデントを防ぐためにも、重要インフラ事業者は委託先等のセキュリティ体制を確認する等、適切なサプライチェーン・マネジメントを行うことが求められる。加えて、脆弱性の悪用に起因する不正アクセス被害も多く発生している。不正アクセスを防止するため、保有する機器及びソフトウェアの脆弱性情報の把握し、適切な対応を講じる必要がある。

表 2-1 国内重要インフラ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 | 分野 | 発生時期 | 事例概要 |
|---|---|---|---|---|
| 1 | JAXA に対するサイバー攻撃 | 航空 | 2023 年夏頃 | ● 宇宙航空研究開発機構（JAXA）は、2023 年夏頃にサイバー攻撃を受け、組織内のネットワークを一元管理する中枢サーバ（Active Directory）が不正アクセスされたことを明らかにした。<br>● ロケット、人工衛星等に関する重要情報の漏えいの可能性はないとしている。<br>● 警察が不正アクセスを感知し、JAXA に通報していた。 |
| 2 | NHK の保有する業務用サーバへの不正アクセス | 情報通信 | 2023 年 7 月 31 日 | ● NHK の放送センターの業務用サーバが外部からの不正アクセスを受け、従業員等 23,435 名の個人情報が漏えいした可能性があると明らかにした。<br>● 個人情報が外部へ流出した明確な証拠は確認されなかったとしている。 |
| 3 | ジャックスのサーバに対するランサムウェア攻撃 | クレジット | 2023 年 7 月 25 日 | ● ジャックスは、同社サーバが外部からの不正アクセスを受け、ランサムウェア「Elbie」に感染したことを明らかにした。<br>● クレジットカードなど各種サービスの利用に影響はなく、個人情報等が外部に漏えいした痕跡はなかったとしている。 |
| 4 | ランサムウェア攻撃による名古屋港コンテナターミナルのシステム障害の発生 | 物流 | 2023 年 7 月 5 日 | ● 2023 年 7 月 4 日 6 時半頃、名古屋港コンテナターミナルの物理サーバ及び全仮想サーバがランサムウェアに感染し、情報が暗号化されたことにより、システム障害が発生した。<br>● プリンターから約 100 枚の英語脅迫文が勝手に出力され、冒頭には「LockBit Black Ransomware」が記載されていた。<br>● 2023 年 7 月 6 日 7 時半頃までに復旧が完了し、同日午後に各ターミナルで順次搬出入作業が再開した。 |
| 5 | ハッカー集団による原子力関連団体のウェブサイトへの不正アクセ | 電力 | 2023 年 7 月 1 日 | ● 国際的ハッカー集団「Anonymous」が福島第一原子力発電所の処理水海洋放出計画に抗議するためとして、日本の日本原子力研究開発機構、日本原子力発電及び日本原子力学会のウェブサイトにサイバー攻撃を仕掛けた。 |

| No. | タイトル | 分野 | 発生時期 | 事例概要 |
|---|---|---|---|---|
| | ス | | | ● Anonymous は大量のデータを送り付け、システム障害を起こす DDoS 攻撃を実行した。<br>● 日本原子力研究開発機構によると、サイトに通常の約 100 倍のアクセスがあったが、対策によって閲覧ができなくなるなどの影響は生じなかったとのことである。 |
| 6 | 不正アクセスによる三重県立総合医療センターのホームページ改ざん | 医療 | 2023 年 5 月 5 日 | ● 三重県立総合医療センターのホームページに、不正アクセスによる書き込みがあった。<br>● 内容を調査したところ、2023 年 5 月 5 日 21 時 30 分頃に更新履歴が残っていたが、この時間には、職員及び保守業務委託業者の更新作業がなかったことから、第三者による不正アクセスと判断している。<br>● 電子カルテなどの医療情報システムはインターネットから分離しているため、個人情報の漏えいはなかったとしている。 |
| 7 | 不正アクセスによる福岡徳洲会病院へのサイバー攻撃 | 医療 | 2023 年 4 月 4 日 | ● 2023 年 4 月 4 日、福岡徳洲会病院の職員が業務用 PC で外部のウェブサイトを閲覧していた際、画面に警告が表示された。記載された電話番号に連絡して指示に従って操作したところ、パソコンが遠隔操作に切り替わり、金銭を要求された。<br>● 後日、専門業者が調査した結果、マルウェアの感染は確認されなかったものの、データベースに登録されていた患者の氏名や住所などのほか、職員の氏名やメールアドレスなど、最大でおよそ 4,400 人分、5 万件程度の情報が、およそ 2 時間にわたって外部から閲覧可能な状態になっていた。 |
| 8 | 東邦化学工業のサーバへの不正アクセス攻撃 | 化学 | 2023 年 2 月 26 日 | ● 東邦化学工業のデータセンターのサーバに第三者による不正アクセスがあった。<br>● 不正アクセスの結果、株主、採用試験応募者、取引関係者、元社員などの個人情報の一部が漏えいした。 |

| No. | タイトル | 分野 | 発生時期 | 事例概要 |
|---|---|---|---|---|
| 9 | セキュリティ設定の不備による浜松ケーブルテレビの個人情報漏えい | 情報通信 | 2023 年 2 月 16 日 | ● 2023 年 2 月 16 日、浜松ケーブルテレビのインターネットサービス提供用のケーブルモデムにおける制御サーバにセキュリティ対策不備があり、顧客 ID や住所が最大 22,671 件流出した可能性があると明らかにした。<br>● 調査の結果、原因は新サーバへのセキュリティ設定の不備であり、XorDDoS と呼ばれるマルウェアが不特定のサイトに向けて DDoS 攻撃を行っていたものと判明した。<br>● 当該サーバ内に保存されていた情報が外部へ流出した可能性は低いものの、完全には否定できないと報告されている。 |
| 10 | 北海道ガス子会社の委託先がネットワーク共有している会社のサーバへの不正アクセスによる顧客情報の漏えい | ガス | 2022 年 12 月 6 日 | ● 北海道ガス株式会社の子会社である北ガスジェネックス株式会社は、同社が灯油配送業務を委託する北斗興業株式会社への不正アクセスがあったことを発表した。<br>● 調査の結果、2022 年 12 月 6 日に、北斗興業がネットワークを共有している他社サーバへの不正アクセスが確認された。さらに、北斗興業のサーバにも不正アクセスがあり、北斗興業に灯油配送業務を委託している顧客情報が漏えいした可能性があると判明した。 |
| 11 | 金沢西病院への不正アクセスによるシステム障害 | 医療 | 2022 年 12 月 3 日 | ● 金沢西病院の端末がサイバー攻撃を受け、障害が発生した電子カルテの一部が閲覧できない状況になった。<br>● 障害発生時も外来診療、人間ドック、健診等を通常どおり行っていたが、保険証のコピーや問診票の記入を求めるなど、通常より時間を要する対応を求められた。<br>● 不正アクセスによる障害は会計システムにも影響を与えていたとみられる。なお、不正アクセスを受けた原因や影響範囲の詳細については、これまで明らかにしていない。 |
| 12 | ランサムウェア攻撃による大阪急性期総合医療センターのシステム障害の発生 | 医療 | 2022 年 10 月 31 日 | ● 大阪急性期総合医療センターに対するサイバー攻撃により電子カルテを含めた総合情報システムが利用できなくなり、救急診療や外来診療、予定手術などの診療機能に大きな支障が生じた。 |

| No. | タイトル | 分野 | 発生時期 | 事例概要 |
|---|---|---|---|---|
| | | | | ● サイバー攻撃によるシステム障害を想定した BCP（事業継続計画）は策定されていなかった。<br>● バックアップデータを基にシステムの復旧作業を進め、外来診療を全面的に再開したのは 2023 年 1 月 11 日であった。 |
| 13 | ランサムウェア攻撃による沼津市の田沢医院におけるシステム障害の発生 | 医療 | 2022 年 10 月 27 日 | ● 田沢医院の職員が電子カルテシステムを起動したところ、本来の表示と異なる英文のメッセージが表示された。内容は「ファイルを暗号化した」、「金を支払え」、「問題解決の意思があるなら連絡せよ」などの攻撃者の要求であった。<br>● 同院はこれを受け、厚生労働省や静岡県警に被害を報告した。公表時点で個人情報の流出は確認されていないが、2022 年 11 月 1 日時点では、電子カルテシステムの復旧には至っておらず、紙のカルテで業務対応を行っていた。 |
| 14 | 内閣サイバーセキュリティセンター（NISC）でメールデータ漏えいの可能性 | 政府行政サービス | 2022 年 10 月上旬 | ● NISC は電子メール関連のシステムに不正通信があり、個人情報を含むメールデータの一部が外部に漏えいした可能性があると発表した。<br>● メールデータの漏えいが発覚したきっかけは、2023 年 6 月 13 日に電子メール関連システムで不正通信を示す痕跡を発見したことによる。<br>● 2023 年 6 月 14～15 日にシステムの運用を停止し、不正通信の原因と疑われる機器を交換し、他の機器に異常がないことの確認等を実施した上でシステムを再稼働した。その後、調査に当たった保守運用事業者が、機器の脆弱性により不正通信が発生したことを示す痕跡を発見した。<br>● 不正通信の痕跡発見を受け、外部の専門機関などによる調査も実施した。調査の結果、2022 年 10 月上旬～2023 年 6 月中旬の 8 カ月以上にわたり、NISC がインターネット経由で送受信した個人情報を含むメールデータの一部が、外部に漏えいした可能性があると判明した。 |

| No. | タイトル | 分野 | 発生時期 | 事例概要 |
|---|---|---|---|---|
| 15 | ランサムウェア攻撃によるみんな電力の顧客情報の流出 | 電力 | 2022 年 9 月 18 日 | ● UPDATER 社（旧みんな電力）が管理運用するファイルサーバのランサムウェア感染により、顧客や関係企業の情報が外部流出した可能性があることを発表した。 |
| 16 | 新ロシア派のハッカー集団「Killnet」による東京メトロ、大阪メトロのホームページへの DDoS 攻撃 | 鉄道 | 2022 年 9 月 6 日～2022 年 9 月 7 日 | ● 新ロシア派のハッカー集団「Killnet」が、東京メトロ、大阪メトロのホームページへの DDoS 攻撃を実施し、各社のホームページは閲覧しにくい状態となった。 |
| 17 | 三和倉庫のサーバへのランサムウェア攻撃及び不正アクセス | 物流 | 2022 年 7 月 29 日 | ● 三和倉庫のサーバに対して、第三者からのランサムウェア攻撃及び不正アクセスがあった。<br>● 攻撃によって共有フォルダ内の一部ファイルが暗号化され、その後サーバが非常停止した。また、ファイルサーバを含むエリアに侵入され、一部の個人情報が漏えいした。 |
| 18 | ランサムウェア攻撃による鳴門山上病院のシステム障害の発生 | 医療 | 2022 年 6 月 20 日 | ● ランサムウェア Lockbit 2.0 によるシステムへの侵入被害を受け、鳴門山上病院における電子カルテ、院内 LAN システムが使用不能となった。<br>● サイバー攻撃によって電子カルテや病院内の LAN が使用できなくなったが、翌日には、電子カルテシステムは復旧した。また、攻撃を受けた当日は再来患者に限定して業務を行ったが、2022 年 6 月 22 日からは、可能な範囲で新規患者も含めた診療を再開した。 |
| 19 | 不正アクセスによる岐阜市安江病院へのサイバー攻撃 | 医療 | 2022 年 5 月 27 日 | ● 岐阜市安江病院が不正アクセスを受け、同院が保有する患者の個人情報が流出した可能性があると発表した。<br>● 攻撃を受けた当日は一部の業務を制限した診療体制としていたが、翌日にはシステムを復旧し通常診療を再開した。 |
| 20 | ランサムウェア攻撃による藤井寺市青山病院のシステム障害の発生 | 医療 | 2022 年 4 月 23 日 | ● 2022 年 4 月 23 日未明、院内のサーバに保管している電子カルテが閲覧できなくなった。また、院内のプリンターが英文の書かれた紙を大量に印刷したほか、パソコンの画面に、英語で「pay」と、支払いを要求する言葉が表示された。 |

| No. | タイトル | 分野 | 発生時期 | 事例概要 |
|---|---|---|---|---|
| | | | | ● 業者に依頼して調査したところ、医療情報システムに不正アクセスされた痕跡があった。 |
| 21 | 東京都水道局及び東京都下水道局の委託業務受託者へのランサムウェア攻撃による業務関連データ流出疑惑 | 水道 | 2021 年 8 月 15 日～ 2021 年 8 月 19 日 | ● 2021 年 8 月 15 日及び 19 日の 2 回にわたり、東京都水道局の委託業務受託者（株式会社中央設計技術研究所）が属するグループ（オリエンタルコンサルタンツホールディングス）の複数のサーバに対して、ランサムウェア攻撃があった。<br>● 攻撃により、東京都水道局が提供した業務関連情報が流出した可能性があるとしている。 |
| 22 | メタップスペイメントへの不正アクセス | クレジット | 2021 年 8 月 2 日～ 2022 年 1 月 25 日 | ● 決済代行会社のメタップスペイメントに対して、2021 年 8 月 2 日から 2022 年 1 月 25 日にわたって、社内管理システムへの不正ログイン、一部アプリケーションへの SQL インジェクション攻撃、バックドアの設置が行われた。決済情報等が格納されているデータベースまで侵入され、個人情報を含む情報が外部に流出した。<br>● 漏えいの対象となったデータベースに保存されていたクレジットカード番号等は約 288 万件であったと公表した。<br>● 行政処分が行われ、2023 年 1 月 31 日、インシデント対応のため停止していた全てのサービスを順次再開していくことを発表した。 |

出所）各種公開情報に基づき三菱総合研究所作成

### 2.1.2 海外重要インフラ分野における近年のセキュリティインシデント事例

海外重要インフラ分野における近年のセキュリティインシデント事例を表 2-2 に示す。ハクティビストによるサイバー攻撃を原因としたセキュリティインシデントが多く発生していることが確認できるほか、No.9 など、サプライチェーン攻撃の高まりを確認できる。さらに、国内事例と同様にランサムウェア攻撃の被害も多く発生している。こうした攻撃を防ぐため、脆弱性情報の把握及びパッチの適用等の対策を行うほか、被害を受けた後の対応及びバックアップの整備も行う必要がある。

表 2-2 海外重要インフラ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 | 分野 | 国・地域 | 発生時期 | 事例概要 |
|---|---|---|---|---|---|
| 1 | レバノンの国際空港に対するサイバー攻撃 | 空港 | レバノン共和国・ベイルート | 2024 年 1 月 7 日 | ● レバノン共和国のベイルートにあるラフィク・ハリリ国際空港のスクリーン映像が攻撃者によって改ざんされ、レバノンのキリスト教徒グループによる政治メッセージが表示された。<br>● この攻撃により、空港の手荷物取り扱いシステムの運営にも支障をきたした。 |
| 2 | サイバー攻撃によるイラン国内のガソリンポンプの停止 | 石油 | イラン | 2023 年 12 月 18 日 | ● イラン国内の給油所に障害が発生し、給油機能が終日停止した。<br>● イラン政府はサイバー攻撃が原因と指摘し、イスラエルに関係する攻撃者集団がSNSに犯行声明を出した。 |
| 3 | 米国水道局へのハッキング | 水道 | 米国・ペンシルバニア州アリクイッパ市 | 2023 年 11 月 25 日 | ● ペンシルバニア州アリクイッパ市水道局は、遠隔管理するブースターステーションの一つがイランの支援を受けたサイバーグループによってハッキングされ、水圧を監視するコンピューター技術が突然シャットダウンし、画面にメッセージが表示された。<br>● Cyber Av3ngers として呼称されるサイバー攻撃グループが給水所の一つを攻撃したとされている。当局はただちに自動システムを停止し、手動にて業務を再開することで、サービスを中断することには至らなかった。<br>● 攻撃は Unitronics 製のプログラマブルロジックコントローラー（PLC）に対して行われた。 |
| 4 | オーストラリア港湾へのサイバー攻撃 | 物流 | オーストラリア | 2023 年 11 月 10 日 | ● 世界最大級の港湾運営企業である DP World のオーストラリアの港湾システムがハッキングされ、オーストラリア国内の 4 つの主要港での操業が停止した。<br>● DP World は身代金の要求を受けておらず、どの組織の犯行か把握していないと報じられた。また、攻撃がランサムウェアによるものかは明らかになっていない。 |

| No. | タイトル | 分野 | 国・地域 | 発生時期 | 事例概要 |
|---|---|---|---|---|---|
| 5 | チェコの銀行及び証券取引所に対する DDoS 攻撃 | 金融 | チェコ | 2023 年 8 月 30 日～2023 年 8 月 31 日 | ● チェコの複数の銀行とプラハ証券取引所が攻撃者の標的となり、銀行のウェブサイトやインターネットバンキングサービス、証券取引所のウェブサイトが攻撃された。<br>● 各銀行の顧客は一時的にバンキングサービスが停止したことで不便を被ったが、各銀行の顧客の資産に影響はなかったと、顧客や銀行の代表者は述べている。<br>● DDoS 攻撃によって、複数の銀行がウェブサイト、インターネット、モバイルバンキングの停止を発表した。プラハ証券取引所のウェブサイトに関しては、サイバー攻撃の後、2 日間サイトにアクセスしづらくなった。<br>● チェコ通信はこの攻撃はロシアのハクティビスト集団によるものと報じている。 |
| 6 | ポーランドの鉄道システムに対するサイバー攻撃 | 鉄道 | ポーランド | 2023 年 8 月 25 日～2023 年 8 月 26 日 | ● 鉄道の無線信号に対するサイバー攻撃によって、ポーランド全土で貨物と乗客を運ぶ 20 本以上の列車が停止した。<br>● ポーランド通信（PAP）は、列車を停止させるために送信された無線信号には、ロシアの国歌とプーチン大統領の演説が録音されていたと報じた。<br>● 無線停止コマンドは、無線周波数を使ったコマンドを作成するための機器（30 ドル程度）を用意するだけで、誰でも実行できるという。 |
| 7 | デンマークの重要インフラに対するサイバー攻撃 | 複数 | デンマーク | 2023 年 5 月 | ● デンマークの重要インフラのサイバーセキュリティ専門組織 SektorCERT は、デンマークの重要インフラ複数社がサイバー攻撃を受けていると発表した。<br>● 攻撃により、数日の間に 22 の企業が侵入されたことを明らかにした。一部の企業は、インターネットを切断し、その他の不要不急のネットワーク接続を遮断することを余儀なくされた。<br>● 攻撃には、Zyxel Network 社のファイアウォールの脆弱性が悪用された。 |
| 8 | DDoS 攻撃によるフランス国民議 | 政府行政サー | フランス | 2023 年 3 月 27 日 | ● フランス国民議会のウェブサイトが、親ロシア派攻撃者による DDoS 攻撃でダウンした。 |

| No. | タイトル | 分野 | 国・地域 | 発生時期 | 事例概要 |
|---|---|---|---|---|---|
| | 会の Web サイトダウン | ビス | | | |
| 9 | 3CX が提供するソフトウェア「The 3CX Client」正規版のインストーラーファイルの第三者による改ざん | 情報通信 | 世界 190 か国 | 不明（遅くとも 2023 年 3 月 29 日まで改ざんされたインストーラーファイルが配布） | ● 3CX の VoIP ソフトウェア「3CX Client」（Windows 版、MacOS 版）の正規版のインストーラーファイルが第三者に改ざんされていたことが明らかになった。改ざんには北朝鮮が関与していると分析されている。この VoIP ソフトウェアは世界 190 か国、60 万の組織で様々な分野（自動車、MSP、製造業など）で使用されており、毎日 1200 万の利用者がいると報告されている。<br>● 改ざんされたインストーラーは 2023 年 3 月 29 日まで配布されており、不正なインストーラーを使用していた場合、情報が窃取されるマルウェアに感染する可能性がある。<br>● この攻撃は、別のソフトウェア開発会社である Trading Technologies への攻撃に起因する。元々、Trading Technologies が提供するソフトウェア（インストーラー）が改ざんされ、3CX 社の従業員がこのソフトウェアをインストールしたことでマルウェアに感染し、認証情報が窃取されたことで、「3CX Client」のインストーラーが改ざんされた。 |
| 10 | バーレーン国際空港に対するサイバー攻撃 | 空港 | バーレーン | 2023 年 2 月 14 日 | ● バーレーン国際空港 Web サイトが不正アクセスによりダウンした。<br>● ハクティビスト Al-Toufan は、空港のウェブサイトをハッキングしたと主張した。 |
| 11 | 英国の郵便サービスに対するランサムウェア攻撃 | 物流 | イギリス | 2023 年 1 月 | ● 英国の郵便・宅配便会社である Royal Mail 社のシステムが 2023 年 1 月 13 日までサイバー攻撃を受け、ランサムウェアに感染し、封書や小包の海外発送ができなくなった。<br>● 英紙フィナンシャルタイムズによると、ロシアと関連があるとされる犯罪集団「LockBit」が一部データを盗み出した疑いがある。 |

| No. | タイトル | 分野 | 国・地域 | 発生時期 | 事例概要 |
|---|---|---|---|---|---|
| | | | | | ● Royal Mail 社は要求された身代金額を明らかにしていないが、100 万ドル（約 1 億 3 千万円）以上と推定されている。 |
| 12 | コスタリカの公共事業運輸省に対するランサムウェア攻撃 | 政府行政サービス | コスタリカ | 2023 年 1 月 | ● コスタリカの公共事業運輸省（MOPT）は、同省のシステムがランサムウェア攻撃を受け、12 台のサーバが暗号化されたと発表した。この被害により、MOPT の全コンピューターシステムがオフラインになった。<br>● 攻撃により、運転免許交付業務が一時中断された。 |
| 13 | ドイツの電力会社に対するサイバー攻撃による顧客 IT システムへの影響 | 電力 | ドイツ | 2022 年 10 月 26 日 | ● ドイツ最大の自治体エネルギー供給会社の一つである Enercity 社が、サイバー攻撃を受けた。<br>● エネルギー供給は継続することができたものの、顧客サービスに影響を及ぼし、IT システムの利用に制限が生じた。 |
| 14 | イタリアのエネルギー庁に対するサイバー攻撃 | 政府行政サービス | イタリア | 2022 年 9 月 2 日 | ● イタリアのエネルギー機関 Gestore dei Servizi Energetici（GSE）のシステムが、ランサムウェアグループ「BlackCat/ALPHV」による攻撃を受けた。<br>● GSE は、攻撃を検知した後、攻撃者がデータにアクセスするのを阻止するためにウェブサイトとシステムをダウンさせた。システムのダウンは 1 週間継続した。<br>● BlackCat/ALPHV は、この攻撃によりおよそ 700GB のファイルを盗んだと主張した。盗まれたファイルには、契約書、報告書、プロジェクト情報、会計文書、その他の内部文書を含む機密データが含まれているという。 |
| 15 | ギリシャの天然ガス販売会社へのサイバー攻撃 | ガス | ギリシャ | 2022 年 8 月 19 日 | ● ギリシャの天然ガス供給会社 DESFA が、IT インフラの一部にサイバー攻撃を受けたと発表した。<br>● DESFA へのサイバー攻撃は、ランサムウェア「Ragnar Locker」を使用していた。攻撃者は、国家ガスシステムオペレーターのシステムをランサムウェアに感染させ、従業員や顧客の情報を盗み、その情報をダークウェブ上に流出させた。 |

| No. | タイトル | 分野 | 国・地域 | 発生時期 | 事例概要 |
|---|---|---|---|---|---|
| | | | | | ● DESFA が攻撃者との交渉を拒否したため、ギリシャの国営天然ガスパイプライン事業者 DESFA に属する 361GB の機密データと思われるものが流出した。流出文書の中には、エンジニアリング設計や予算収益に関する文書に加え、将来の予算や過去の収益に関するスプレッドシートと思われる複数のファイル、顧客やパートナーとの秘密保持契約のコピー、ディレクトリ形式のエンジニアリング設計とそのバックアップなどが含まれていた。 |
| 16 | 米イリノイ州の病院に対するランサムウェア攻撃 | 医療 | 米国・イリノイ州 | 2021 年 2 月 | ● ランサムウェア攻撃により、イリノイ州の病院は、保険会社、メディケア、メディケイドへの請求書を数か月提出することができず、財務的な損失を被った。攻撃により、電子カルテポータル、メール、内部 IT システムがシャットダウンし、職員は 4 ヶ月間、医療ツールやコミュニケーションツールにアクセスできなくなった。<br>● 病院は手作業による記録に頼り、保険請求書の送付に最長で 1 年を費やすことになった。<br>● 2023 年 6 月 16 日、同病院はこのランサムウェア攻撃被害も一因となり、閉院した。 |

出所）各種公開情報に基づき三菱総合研究所作成

## 2.2 国内外電力分野に関するサイバーセキュリティ対策の動向

国内外の政府機関を中心とした電力分野に関するサイバーセキュリティ対策の動向等の調査結果を示す。

### （1） 日本：「重要インフラのサイバーセキュリティに係る行動計画」に関連する取組

脅威がますます高度化・巧妙化している中、重要なインフラに対する脅威は年々増加している。同時に、各重要インフラ分野ではシステムの利用形態が異なるため、組織ごとの脅威の差異も拡大している。この状況を踏まえ、政府は 2022 年 6 月にサイバーセキュリティ戦略本部において、「重要インフラのサイバーセキュリティに関する行動計画」を策定することを決定した。

重要インフラ防護の目的として、以下 2 点の両面から、強靱性を確保し、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現することとしている。

①重要インフラサービスの継続的提供を不確かなものとする自然災害、管理不良、サイバー攻撃や、重要インフラを取り巻く環境変化等をリスクとして捉え、リスクを許容範囲内に抑制すること

②重要インフラサービス障害に備えた体制を整備し、障害発生時に適切な対応を行い、迅速な復旧を図ること

本行動計画における施策群と補強・改善の方向性は表 2-3 のとおりである。本行動計画の見直しは、本行動計画の評価を踏まえ、サイバーセキュリティ戦略本部において実施し、そのために必要な調査・検討は、重要インフラ所管省庁の協力を得て重要インフラ専門調査会で行う。行動計画の見直しについては、行動計画の評価と併せて 3 年に 1 度の実施を原則としているが、社会動向の大きな変化等、本行動計画が想定し得なかった事象が発生した場合は、その限りでないとしている。

また、「重要インフラのサイバーセキュリティに係る行動計画」に基づき、安全基準等の策定・改定を支援するために、2023 年 7 月に「重要インフラのサイバーセキュリティに係る安全基準等策定指針」が策定された。安全基準等策定指針には、各重要インフラ分野に共通して求められるサイバーセキュリティの確保に向けた取組が整理・記載されている。各取組をどの安全基準等に定めるかについては、関係法令の規定及び安全基準等の構成等を踏まえ、重要インフラ分野又は重要インフラ事業者等ごとに検討されることを想定している。

表 2-3 本行動計画における施策群と補強・改善の方向性

| 本行動計画における施策群 | 第四次行動計画の施策群との対応 | 第四次行動計画からの主な補強・改善の方向性 |
|---|---|---|
| 障害対応体制の強化 | 「4.リスクマネジメント及び対処態勢の整備」の一部と「5.防護基盤の強化」の一部を統合した上で整理 | ● 重要インフラ防護を適切に行うためには、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の取組の必要性が高まってきていることを踏まえ、組織統治の一部としての障害対応体制の強化を推進<br>● サイバーセキュリティを取り巻く環境が大きく変化することを背景としたサプライチェーン・リスク等の新たな脅威への先取りした対応の推進<br>● 重要インフラ事業者等の自組織のリスクに応じた最適な防護対策の推進<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>● 事前対応のリスクマネジメントと障害発生時の危機管理の一体的な対応の推進 |
| 安全基準等の整備及び浸透 | 「1.安全基準等の整備及び浸透」を基本的に踏襲 | ● 障害対応体制の強化及びリスクマネジメントに資する安全基準等を整備することを明確化<br>● 重要インフラ事業者等の取組の継続的な改善を図ることができる調査手法の検討 |
| 情報共有体制の強化 | 「2.情報共有体制の強化」を「3.障害対応体制の強化」の一部と統合した上で整理 | ● 重要インフラ事業者等の自主的な取組の活性化を前提とした共助の推進<br>● ISAC 連携等による分野間・官民連携の枠組みの整備の検討<br>● ナショナルサートの枠組みの強化の検討との整合性保持 |

| 本行動計画における施策群 | 第四次行動計画の施策群との対応 | 第四次行動計画からの主な補強・改善の方向性 |
|---|---|---|
| リスクマネジメントの活用 | 「4.リスクマネジメント及び対処態勢の整備」の一部を整理 | ● 組織の特性を踏まえた経営層による組織のリスクの明確化<br>● 自組織に適した防護対策の実現を支援するため、既存の手引書の見直しに加え、既存の基準類をどのように自組織に活用するかを含めた新たなガイダンスの整備の方向性の明示<br>● 2020 年東京オリンピック・パラリンピック競技大会開催に向けて官民が連携して行ってきた取組の活用を検討 |
| 防護基盤の強化 | 「5.防護基盤の強化」の一部を「3.障害対応体制の強化」の一部と統合した上で整理 | ● 障害対応体制の有効性検証としての分野横断的演習の推進<br>● 警察による重要インフラ事業者等との協力等の必要な取組の支援<br>● デジタル庁と連携した地方公共団体及び重要インフラに関連する準公共部門におけるサイバーセキュリティの確保に向けた支援等の実施 |

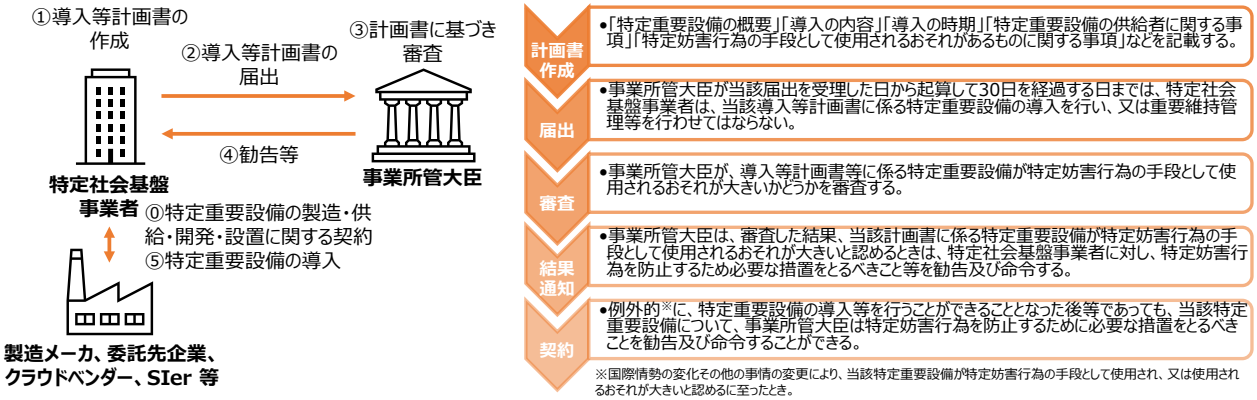
出所）NISC「重要インフラのサイバーセキュリティに関する行動計画」に基づき三菱総合研究所作成

### （2） 日本：経済安全保障推進法に関連する取組

世界情勢の不安定化や社会経済構造の変化に伴い、経済的な観点から国家安全保障に関する新たな課題が生じている。こうした状況への対応として、国家間の平和と安定、国益を確保することを目的に、「経済安全保障推進法」が 2022 年 5 月に成立した。経済安全保障推進法では、「サプライチェーン（供給網）の強化」「官民重要技術の支援」「基幹インフラの安全性確保」「特許出願の非公開化」の 4 つの柱を掲げている。

基幹インフラ役務の安定的な提供の確保に関する制度は、電気・ガス・水道等の「基幹インフラ」に対して、安全性と信頼性を確保し、国民に対して安定的なサービス提供を目指すものである。本制度では、特定社会基盤事業者が特定重要設備の導入及び重要維持管理等の委託を行う場合、事業所管大臣の審査を受けなければならないとしており、2024 年 5 月 17 日より運用が開始される。審査において、特定重要設備が特定妨害行為（我が国の外部から行われるサイバー攻撃、物理的な妨害行為等）の手段として使用されるおそれが大きいと認められたとき、事業所管大臣は、特定妨害行為を防止するため必要な措置を取るべきこと等を勧告及び命令することができる。（図 2-1 参照）

2023 年 11 月 16 日、電力分野では特定の基準を満たす 42 者が特定社会基盤事業者として指定され、特定重要設備の導入及び重要維持管理等の委託を行う場合、経済産業大臣による事前審査が必要となる。




出所）経済安全保障推進法に関する公開情報に基づき三菱総合研究所作成

図 2-1 「特定重要設備」の導入に係る事前審査のプロセス

### （3）米国 NERC：Cyber Security for Distributed Energy Resources and DER Aggregators に関連する取組

北米電力信頼度協会（NERC）は、アグリゲーター業界の関係主体に対する情報提供を目的とし、「Cyber Security for Distributed Energy Resources and DER Aggregators」を発行した。本文書では、急速な電力グリッド変革の下で電力エコシステムの安全性を向上させるための活動に焦点を当て、特に DER 及びアグリゲーターに対するサイバーセキュリティの取組に関する情報を産業界に提供している。

本文書では、アグリゲーターがサイバー攻撃にさらされると、アグリゲーターによって制御される数百又は数千の DER に影響を与える可能性があるが、現状では、アグリゲーター独自の役割を満足する標準化されたサイバーセキュリティ要件が不足している現状であるとしている。この現状に対して、アグリゲーターは、DER 単体ではなく、集約された資産全体に影響を与えるため、従来の IT セキュリティとは異なる OT 環境においてセキュリティ管理を採用すべきであること、機器レベルの UL 認証は第一歩であるが、アグリゲーターはその独自の役割に関連するリスクに対処するために OT サイバーセキュリティプログラムを採用するべきであること、IEEE 1547.3 の更新版は DER のサイバーセキュリティに関するガイドラインを盛り込んでおり、アグリゲーターが参考にすべき資料であることが述べられている。

以上を踏まえ、本文書で述べられている具体的な 4 つの推奨行動は以下のとおりである。

- DER サイバーセキュリティ認証：NERC と業界関係者は DER サイバーセキュリティ認証イニシアチブを支援し、DER 及びアグリゲーターの導入が電力システムに与える影響に関する専門知識を提供すべきである。将来の DER 機器は十分なサイバーセキュリティ措置が施され、設計、試験、商用設置されることを確認する取組が必要である。これにより、電力エコシステム全体の安全性が向上する。
- 配電相互接続要件におけるサイバーセキュリティ：AGIR（Authority Governing Interconnection Requirements）[1]が IEEE 1547 において機器の性能仕様を策定するよう

[1] 電力システムへの DER の相互接続を認証する方針及び手順を定義、明文化、伝達、管理、実施する主体。規制機関、公益事業委員会、自治体、協同組合の理事会等を指す。

に、新たに相互接続される DER が特定のサイバーセキュリティ対策を施され、運用可能に構成されるための要件を策定すべきである。IEEE 1547 を修正し、サイバーセキュリティが情報ガイドではなく規格本体に組み込まれるようにする必要がある。

- アグリゲーターの登録：NERC と業界関係者は、アグリゲーターの登録基準が不足していることを認識し、これが大量の DER を制御・運用する場合に信頼性と安全性のギャップを生む可能性があると認識すべきである。信頼性・セキュリティ技術委員会は、アグリゲーターの参加範囲や潜在的な信頼性及びセキュリティリスクを評価し、必要に応じて NERC 登録事業者としての取り扱いを検討すべきである。
- DER 及びアグリゲーターのサイバーセキュリティリスクの積極的理解：業界関係者は DER 及び DER アグリゲーターがもたらすサイバーセキュリティリスクを理解し、これに対処する方法を積極的に検討すべきである。サイバーセキュリティリスクは製品のライフサイクル全体にわたり存在するため、機器の設計から運用までを含めた総合的なアプローチが求められる。

## （4）米国 DoE: Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid に関連する取組

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・プロバイダー・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 2-4 に DER のサイバー防御のための基本行動原則を示す。

2022 年時点では、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としていた。

2023 年 9 月、DoE は、DER のサイバーセキュリティを推進するための国立研究所の新規プロジェクト 9 件に対し、3,900 万ドルの資金提供を発表した。以下の研究が例として挙げられる。

- アルゴンヌ国立研究所の研究プロジェクト：DER アグリゲーターが卸売エネルギー市場に安全に参加するための侵入診断ユニット・サイバーセキュリティ・ソフトウェア・ツールを開発する。このツールはエッジ・デバイスに配備され、クラウドサービスを利用して継続的にサポートされ、個々の DER のリアルタイム監視、脅威検出、緩和を実行する。
- ブルックヘブン国立研究所の研究プロジェクト：クラウド・サービス・プロバイダー及び電力会社と協力して、パブリック・クラウド又はハイブリッド・クラウド用の汎用セキュリティ・ソリューションを開発する。これらのクラウド・ソリューションは、特に複数の仮想発電所を通じて電力網に周波数

と電圧のサポートを提供するリアルタイムの DER アプリケーションを対象とする電力会社によって採用されている。

2024年1月、DoEは、再生可能エネルギー・蓄電サイバーセキュリティ研究(Renewable Energy and Storage Cybersecurity Research:RESCue)の開始を発表した。本取組では、関係主体との定期的な対話と協力を通じて、風力、太陽光、エネルギー貯蔵に対するベストプラクティスを調整し、ハイブリッド再生可能エネルギーシステムの発電と配電に関するサイバーセキュリティの検討を行う。

表 2-4 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[2]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。 |

[2] 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。

| カテゴリー | 基本行動原則 |
| --- | --- |
| | ● Office of Cybersecurity, Energy Security, and Emergency Response（CESER）[3]の Cyber Testing for Resilient Industrial Control Systems プログラム [4]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。 |

出所）DoE「Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid」に基づき三菱総合研究所作成

### （5）米国 NREL・UL：Cybersecurity Certification Standard for DER and Inverter-based Resources に関連する取組

2923 年 4 月、米国国立再生可能エネルギー研究所（NREL）及び UL Solutions は、DER 及びインバーターベースリソース（IBR）機器のサイバーセキュリティ認証規格 UL 2941 を発表した。

米国 DoE の Solar Futures Study によると、米国が脱炭素化目標を達成するためには、2020 年から 2030 年にかけて年平均 45GW の太陽光発電容量を導入する必要がある。最近、分散型発電の使用へ市場がシフトしているため、将来の送電網は、太陽光発電のマイルストーンを達成するために、DER の展開をサポートする必要がある。DER システムは複雑で、調整、制御、集約が可能でなければならない。これらの能力は、IT と OT の両分野で豊富なデータと高度な制御システムを必要とするコンピューター技術への依存度を高めることで可能になるが、技術革新のたびに新たな脆弱性とサイバー脅威の扉を開く可能性がある。これらの脆弱性は、米国の電力システムの攻撃対象領域を拡大し、潜在的なサイバー・フィジカル攻撃に対する感受性を高める可能性がある。

このような潜在的な攻撃の影響を緩和するために、サイバーセキュリティ認証の標準とプログラムを確立する必要があるとし、これらの基準やプログラムが、業界の利害関係者が相互接続された DER のサイバーセキュリティ態勢を評価・検証する際に役立つとしている。

NREL と UL Solutions は、機器レベルのセキュリティの基本水準を確立し、DER 関係者のための将来の UL サイバーセキュリティ自主認証基準の策定に情報を提供することを目的として、「Cybersecurity Certification Recommendations for Interconnected Grid Edge Devices and Inverter Based Resources」[5]と題されたサイバーセキュリティ認証の推奨事項を作

[3] 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。

[4] 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。

[5] NREL、Cybersecurity Certification Recommendations for Interconnected Grid Edge Devices and Inverter Based Resources https://www.nrel.gov/docs/fy22osti/80581.pdf

成した。本報告書では、2019 年に発表された NREL の報告書「Certification Procedures for Data and Communications Security of Distributed Energy Resources」で提案されたサイバーセキュリティ認証の推奨事項の検証結果を示している。

推奨事項には、トランスポート・レイヤー・セキュリティ、鍵の更新、メッセージ認証コード、証明書失効リスト、期限切れ証明書、認証管理、定期監査、サービス・バージョンのチェックについての事項が含まれる。認証勧告試験は、太陽光発電（PV）インバーターで 2 回実施され、1 回目の認証試験は、業界標準の PV で実施し、2 回目の認証試験は、DERCyST と呼ばれるバンプ・イン・ザ・ワイヤー（通信の完全性と信頼性を高めるために既存のシステムに挿入できる侵入検知通信装置）が動作する PV で実施された。

2023 年 4 月、NREL と UL Solutions は、分散型エネルギーやインバーターを利用した機器のサイバーセキュリティに関する要求事項である「UL 2941 the Outline of Investigation (OOI) for Cybersecurity of Distributed Energy and Inverter-Based Resources」を発行した。この規格は、機器メーカー、資産所有者、規制機関が DER や IBR のセキュリティ機能を強化することを支援することを目的としており、瞬間的な高電圧の風力発電、太陽光発電、ハイブリッド／蓄電発電のために一括受電システムに接続する高浸透 IBR を対象としている。UL 2941 は太陽光発電インバーター、電気自動車用充電器、風力タービン、燃料電池など、配電網で重要なリソースに関する要求事項を含んでおり、特に風力、太陽光、ハイブリッド/蓄電の発電量が増加する時間帯において、一括受電系統と連系するインバーターをベースとしたリソースのサイバーセキュリティ強化するための要求事項を規定している。

NREL と UL Solutions は、今後 UL 2941 に基づいて DER の試験を開始し、適合する製品は UL 認証を受けるとしている。これは、UL 1741 を補完するものであり、DER で使用されるインバーター、コンバーター、コントローラー、相互接続システム機器の規格に関連するオプションの追加事項となる。

## （6）欧州：Network Code on Cybersecurity に関連する取組

2022 年 7 月、ACER（The European Union Agency for the Cooperation of Energy Regulators）は、ヨーロッパ全体の電力システムのセキュリティと回復力の維持に貢献することを目的として、サイバーセキュリティに関するネットワークコードの改訂版を欧州委員会に提出した。本法案では、電力分野の事業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規則を示している。（図 2-2 参照）

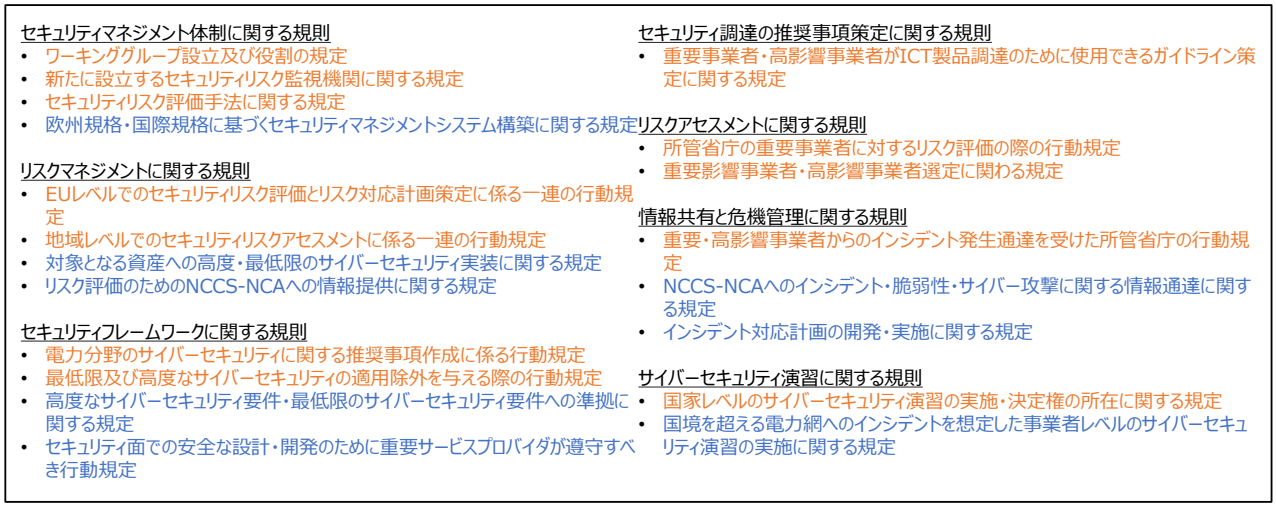
本法案では、電力分野の事業者を、電力サイバーセキュリティ影響指数（ECII）によって高影響事業者と重要影響事業者に区別するとしており、それぞれの事業者に対して課すセキュリティ要件が異なる。

本法案で示されている一部の規則は、NIS2 指令の規定を補完する形となっている。

今後、欧州委員会は本法案を審査し、委任法の採択手続きを開始する。加盟国によって採択されれば、EU 全域で法的拘束力を持つことになる。

本法案について、欧州委員会は 2023 年 10 月から 2 か月の期間でパブリックコメントを実施し、利害関係者に意見を求めた。その結果、36 件の意見が寄せられ、その 60%は EU 加盟国内に拠点を置く、エネルギー業界企業又は団体からであった。欧州委員会は、寄せられた意見を受け、法案の内容を修正し、2024 年上旬に本法案を採択する予定である

赤字：加盟国政府に対する規定事項
青字：事業者に対する規定事項




出所)「Network Code on Cybersecurity」に基づき三菱総合研究所作成

図 2-2 本法案に記載されている電力セキュリティに関する規定事項

表 2-5 対象事業者と対象規則内容

| 対象事業者名 | 対象となる規則の内容 |
|---|---|
| 重要影響事業者 | ・ リスクマネジメント：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の実装、リスク評価のための NCCS-NCA への情報の提出<br>・ セキュリティマネジメント：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<br>・ 情報共有と危機管理：インシデントに関する情報を不当な遅延なく、NCCS-NCA へ共有する など |
| 高影響事業者 | ・ リスクマネジメント：対象となる資産への最低限のサイバーセキュリティの実装、リスク評価のための NCCS-NCA への情報の提出<br>・ セキュリティマネジメント：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<br>・ 情報共有と危機管理：インシデントに関する情報の不当な遅延なく、NCCS-NCA への共有 など |
| 重要サービスプロバイダー | ・ フレームワーク：サプライチェーンとして安全な設計・開発・生産のための要件の実施 |
| MSSP | ・ 情報共有と危機管理：重要・高影響事業者の MSSP はセキュリティインシデントに関する情報の積極的な共有 |
| ENTSO, EU DSO | ・ セキュリティマネジメント体制：ワーキンググループの設立、セキュリティリスク評価手法の策定<br>・ フレームワーク：最低限及び高度なサイバーセキュリティ要件の策定、サプライチェーンセキュリティ要件の策定 など |

| 対象事業者名 | 対象となる規則の内容 |
|---|---|
| ACER | ・ セキュリティマネジメント体制：NCCS-NCA の監視業務などを遂行する機関の設立<br>・ 情報の共有と危機管理：電力部門のための EU レベルのサイバーセキュリティ危機管理計画の策定 など |
| NCCS-NCA | ・ リスクアセスメント：重要・高影響事業者への一定期間ごとのリスク評価の実施、報告書の ENTSO・DSO への提出、EU 内外の重要・高影響事業者の特定 など |
| NRA, RP-NCA, CSIRT | ・ セキュリティ演習：RP-NCA は国家レベルのセキュリティ演習の実施を決定可能、NRA・CS-NCA・CSIRT はその旨を事前に重要影響事業者に通知 |
| ENISA | ・ 情報共有と危機管理：事業者への MSSP との係り合いについて拘束力のないガイダンスの提供、電力サイバーセキュリティ早期警戒能力の促進のための情報収集・分析・定期的な報告書の作成 |

出所）「Network Code on Cybersecurity」に基づき三菱総合研究所作成

### （7）フランス：EBIOS Risk Manager に関連する取組

EBIOS RM（Expression des Besoins et Identification des Objectifs de Sécurité Risk Manager）は、情報システムリスク管理者専用のためのガイドセット（無料のオープンソースソフトウェアツール）で、フランス国立サイバーセキュリティ機関（ANSSI）が Club EBIOS[6]の支援を得て公開したサイバーセキュリティリスクの評価手法である。EBIOS RM は、フランス国内外の民間組織・公共組織において広く使用されており、主要な IT セキュリティ標準に準拠している。

EBIOS RM はサイバーセキュリティリスクを評価し、リスクに対処するためのセキュリティ対策を特定するために利用される。EBIOS RM は、主に以下を利用目的としている。

- 組織内でのサイバーセキュリティリスクの管理プロセスの構築又は強化
- IT 関連プロジェクトのリスク評価及び対処
- ユースケースや対処すべきリスクに応じた製品又はサービスが達成すべきセキュリティレベルの定義

EBIOS RM は、サイバーセキュリティリスクの管理において、ターゲットの特定から始まり、段階的にビジネス及び技術的な機能の検討に進み、リスクシナリオを検討するアプローチを採用している。この手法は、「コンプライアンス」と「シナリオ」を統合し、２つのアプローチにより最大の付加価値を得ることを目指している。このアプローチはサイバーセキュリティリスク管理のピラミッドによって表される。（図 2-3 参照）

コンプライアンスを通じたアプローチは、シナリオの基盤となるセキュリティのベースラインを決定するために使用される。特にターゲットを絞り込み、洗練されたリスクシナリオを開発するためのものである。偶発的及び環境リスクは事前にセキュリティの基盤内でコンプライアンスを通じたアプローチによって対

[6] 2006 年に設立されたフランスの非営利団体で、リスクマネジメント手法の開発を支援している。官民を問わず、フランス内外の機関及び個人の専門家、約 500 名（2024 年 2 月時点）が参加している。

処されると仮定している。したがって、EBIOS RM によって説明されるリスク評価は、主に意図的な脅威に焦点を当てている。

EBIOS RM では、リスク管理の一連のプロセスを効果的に進めるために、5 つのワークショップが用意されている。各ワークショップは特定の目的を持ち、段階的に進めることで、セキュリティリスクを適切に理解し、適切な対策を講じるための基盤を築くことが可能となる。

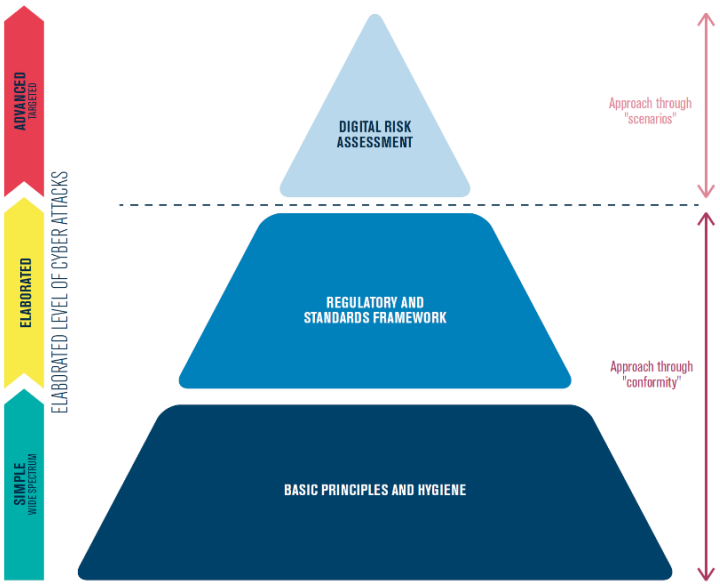
ワークショップ 1 は、対象物、ワークショップ参加者、及び時間枠を特定することを目的としている。このワークショップでは、対象物に関連するミッション、ビジネス資産、及びサポート資産をリストアップする。そして、ビジネス資産に関連する懸念事項を特定し、影響の深刻さを評価する。また、セキュリティのベースラインと差分を定義する。

ワークショップ 2 では、リスクの発生源(RO)と高レベルのターゲット(TO)を特定し、特徴づける。このワークショップの終了時には、最も関連性の高い RO/TO のペアが選択され、その結果は、リスクの発生源のマッピングとして形式化される。

ワークショップ 3 では、脅威のターゲットに対するマッピングを確立する。これにより、高レベルのシナリオである戦略的シナリオを構築可能となる。これらは、リスク発生源が目標に到達するために取る可能性のある攻撃経路を表す。これらのシナリオはエコシステム及び対象物のビジネス資産のスケールで設計されており、深刻さの観点で評価される。このワークショップの終了時点で、既にエコシステムに対するセキュリティ対策を定義できる。

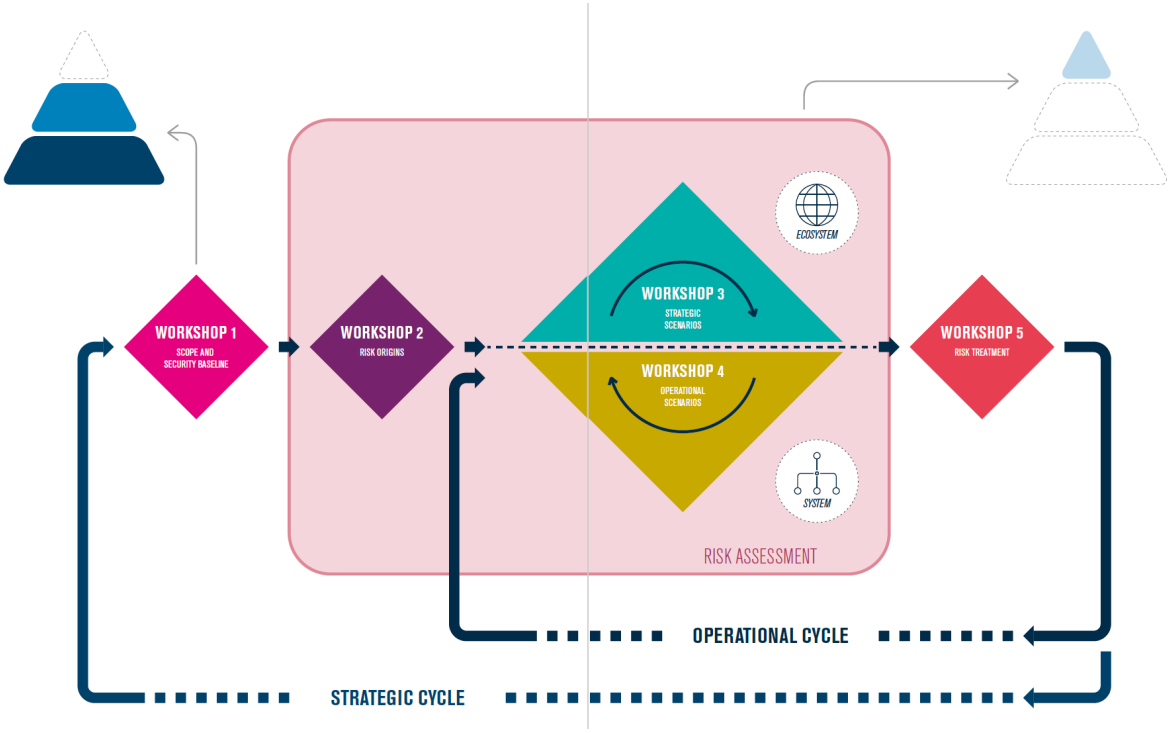
ワークショップ 4 の目的は、リスクの発生源が戦略的シナリオを実行するために使用する可能性のある攻撃手法を含む技術的シナリオを構築することである。このワークショップは、前のワークショップに似たアプローチであるが、重要なサポート資産に焦点を当てている。このワークショップでは、同時に、シナリオの発生確率を評価する。

ワークショップ 5 は、検討された全てのリスク要約を作成し、リスク対応戦略を定義することを目的としている。その後、この戦略は継続的改善計画に組み込まれるセキュリティ対策に分解される。このワークショップでは、残存リスクの要約を作成し、リスクのモニタリングフレームワークを定義する。




出所）ANSSI「EBIOS RM」[7]

図 2-3 EBIOS のコンプライアンスとシナリオの位置付け

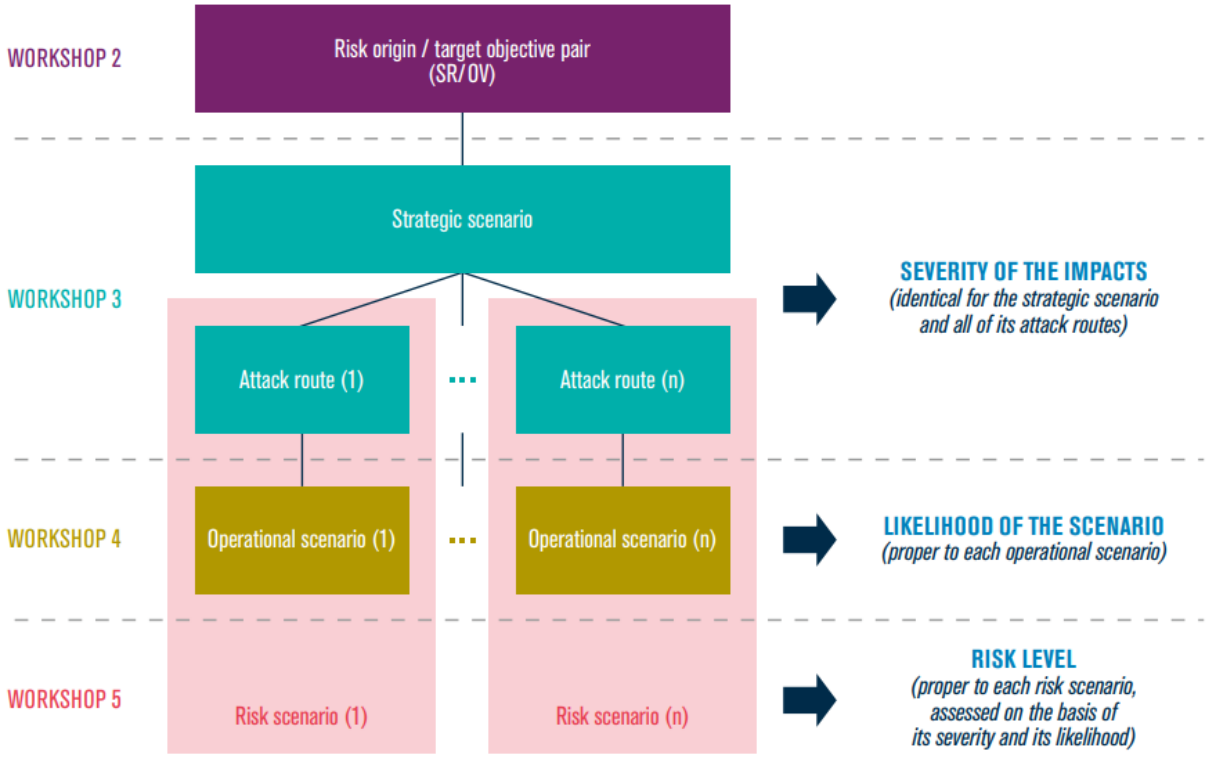



出所）ANSSI「EBIOS RM」[8]

図 2-4 EBIOS の全体像

[7] L' Agence nationale de la sécurité des systèmes d'information、EBIOS RISK MANAGER https://cyber.gouv.fr/sites/default/files/2019/11/anssi-guide-ebios_risk_manager-en-v1.0.pdf

[8] 脚注 7 参照




出所）ANSSI「EBIOS RM」[9]

図 2-5 ワークショップ間の関係

[9] 脚注 7 参照

# 3. リスク点検ツールの試行利用・正式公開

昨年度の関連事業において案を作成したリスク点検ツールについて、今年度は試行利用を実施し、課題抽出・改善を行い、リスク点検ツールを完成させた。また、リスク点検ツールの今年度中の正式公開を目標とし、ツールの位置付けや普及展開方法等について、具体的な議論・検討を行った。

## 3.1 リスク点検ツールの概要

本節では、昨年度の関連事業において案を作成したリスク点検ツールの概要を記載する。

### 3.1.1 全体構成

リスク点検ツールの全体構成は図 3-1 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。

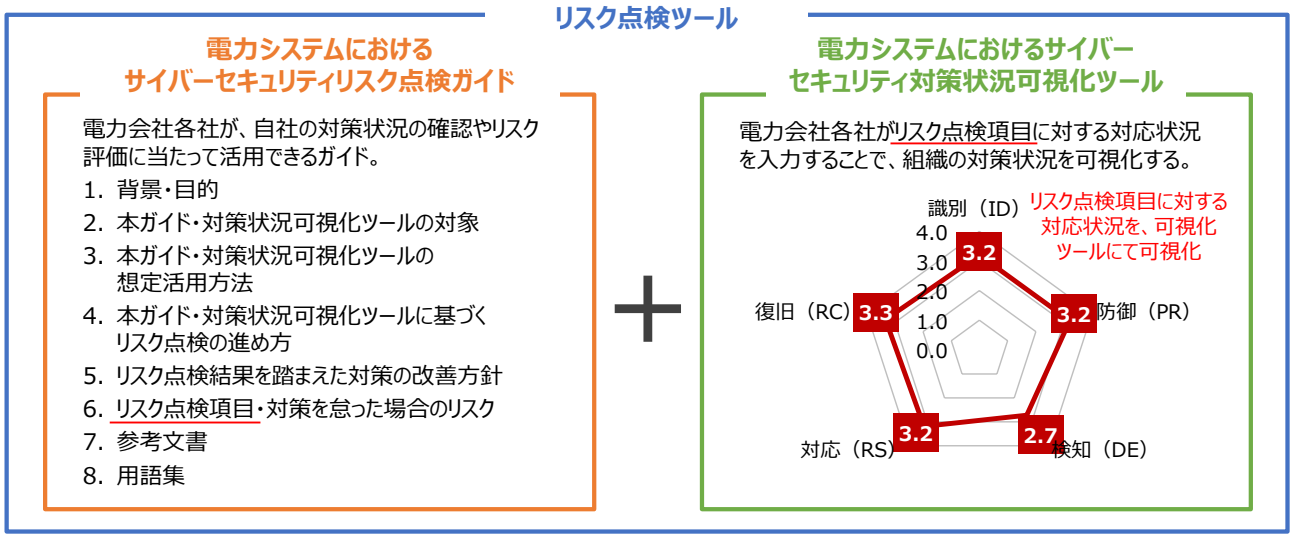



図 3-1 リスク点検ツールの全体構成

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 3.1.5 に示す。

本報告書の添付資料 2 にリスク点検ガイド、添付資料 3 に対策状況可視化ツールをそれぞれ示す。

### 3.1.2 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。また、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。

### 3.1.3 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。

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 3-2 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 3-2 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。

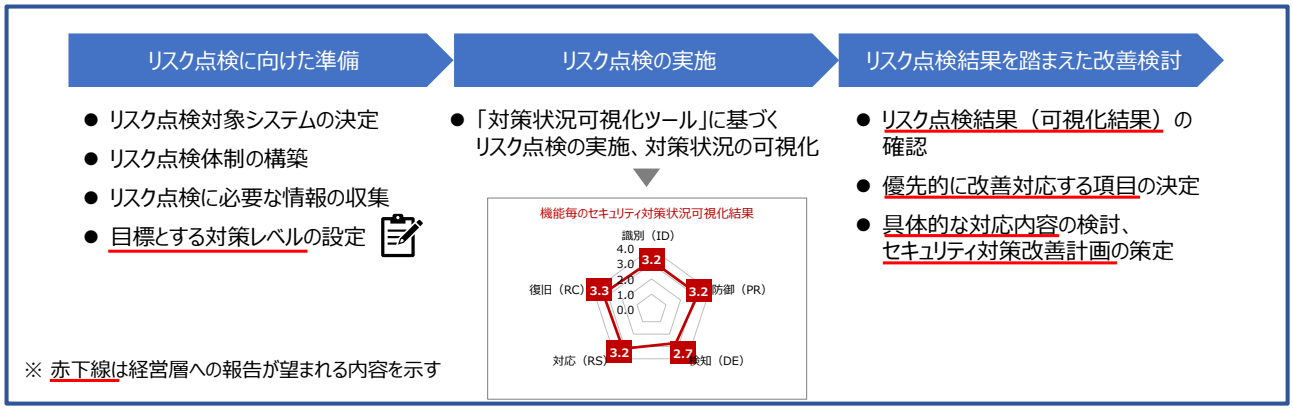



図 3-2 リスク点検の全体プロセス概要

### 3.1.4 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。具体的なリスク点検項目については、添付資料 2 のリスク点検ガイドを参照のこと。

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。

### 3.1.5 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 3-3 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 3-3 において赤枠で囲っている箇所)

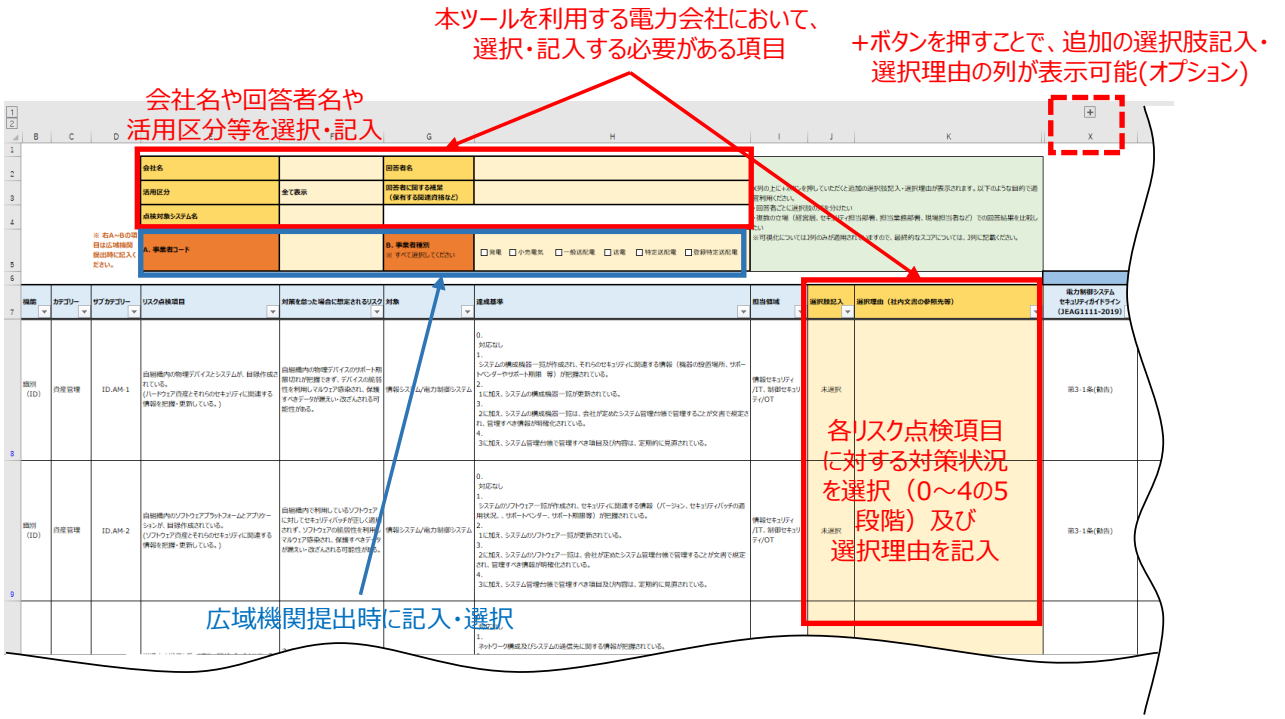



図 3-3 対策状況可視化ツールの「チェックシート」の概要

「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。また、「広域機関提出用」は基礎的なセキュリティ点検項目のみが表示されるため、事業規模やリスク点検の経験によっては「広域機関提出用」を選択し、基礎的なリスク点検を実施することも可能である。(この活用方法の場合、「広域機関用」の項目は対象外として問題ない。)

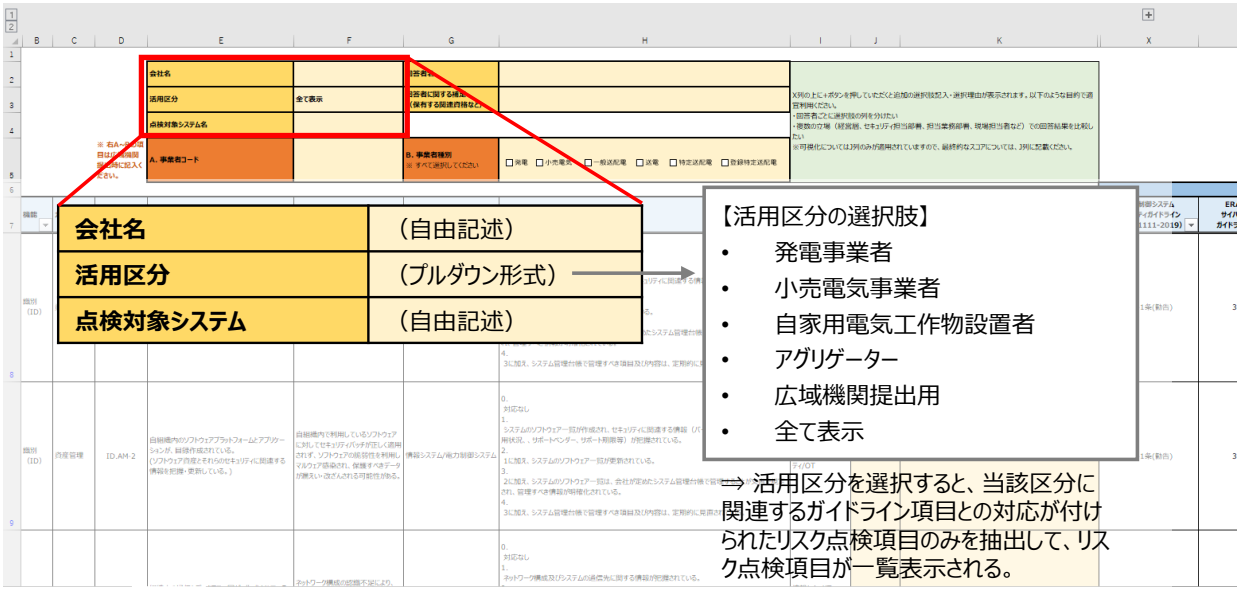



図 3-4 対策状況可視化ツールの「チェックシート」における「活用区分」の位置付け

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 3-5 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。

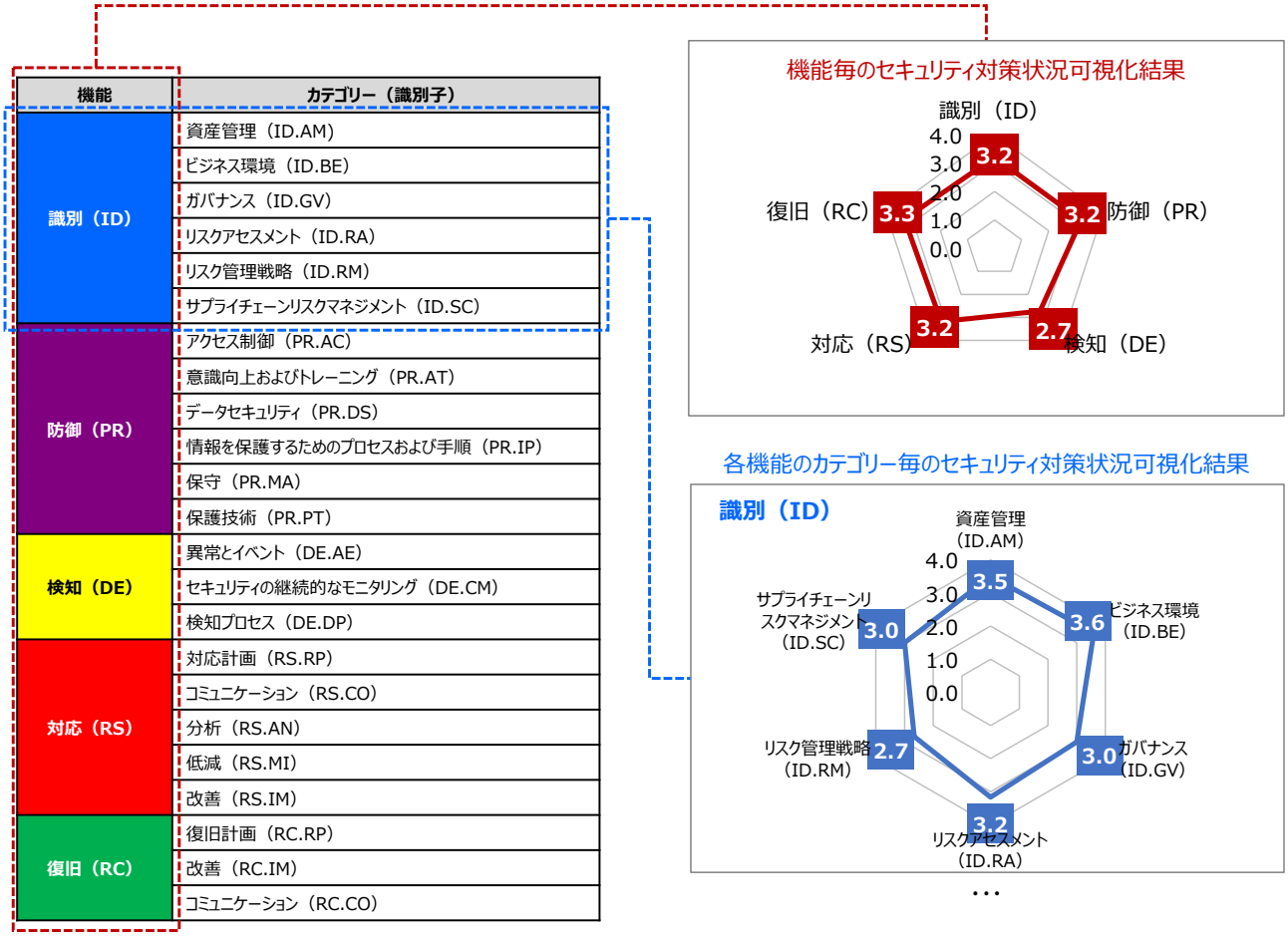



図 3-5 NIST CSF の機能･カテゴリーと対策状況可視化結果の関係

## 3.2 リスク点検ツールの試行利用結果

### 3.2.1 試行利用の概要

リスク点検ツールの正式公開に向け、ツールの課題を抽出することを目的に、リスク点検ツール案に関する試行利用を電気事業者に依頼した。試行利用では、電気事業者に対して自社の事業者区分を選択の上、リスク点検ツールを活用し、その後にアンケートへの回答を求めた。試行利用の概要は表 3-1 のとおりである。アンケートは 19 問で構成される。設問の概要を表 3-2 に示す。

表 3-1 試行利用の概要

| 項目 | 内容 |
|---|---|
| 目的 | ・ 本リスク点検ツールの正式公開に向けて、事業者がより利用しやすいツールとすることを目指し、事業者においてツールを試行利用し、課題・改善点を抽出の上でリスク点検ツールを修正する。<br>※ツールの課題・改善点の抽出が試行利用の目的であり、リスク点検結果を踏まえ何らかの対応を求めるものではない。 |
| 概要 | ・ 作成したリスク点検ツールの素案とガイドを基に、事業者の電力システムに対して、リスクに関する自己点検を実施する。<br>※基本的には事業者自身でリスク点検を進めていただくが、不明点などが出てきた際は、当社が支援した。 |
| スケジュール | ・ ～2023 年 11 月中旬：試行利用実施に向けた準備<br>・ 2023 年 11 月中旬～2023 年 12 月中旬：試行利用の実施、結果のフィードバック<br>（約 1 か月での試行利用を想定。） |
| 試行利用のアウトプット | ・ 試行利用後のアンケート<br>・ （可能であれば、）リスク点検結果の可視化シート（グラフのみ） |

表 3-2 アンケートの設問概要

| アンケートの設問概要 |
|---|
| ・ 回答者の情報 |
| ・ リスク点検ツールの対象項目を全て記入するまでに要した時間 |
| ・ リスク点検ツールの難易度について |
| ・ リスク点検ツールを回答するのに必要なスキルについて |
| ・ リスク点検ツールの項目数について |
| ・ リスク点検ツールの項目内容・リスクについて |
| ・ リスク点検ツールの達成基準について |
| ・ リスク点検ツールのガイドについて |
| ・ リスク点検ツールのメリット・改善点について |
| ・ リスク点検ツールの試行利用した結果を鑑みた今後のツール活用方針について |

### 3.2.2 試行利用の結果の概要

試行利用を 3 つの電気事業者に依頼した。各社のアンケート回答の概要は表 3-3 のとおりである。リスク点検ツールに対しておおむね好意的な意見が多く、社内のセキュリティ対策状況確認のコストダウンや外部事業者のセキュリティ対策確認の効率化等のメリットについて確認できた。アンケートの自由記述より 6 点の指摘があった。6 点の指摘とその対応について、以下の表 3-4 に示す対応方針に沿って修正した。

表 3-3 試行利用のアンケート結果概要

| | 会社 1<br>（発電事業者・アグリゲーター） | 会社 2<br>（小売電気事業者） | 会社 3<br>（小売電気事業者・アグリゲーター） |
|---|---|---|---|
| 記入時間 | 2 週間～1 カ月<br>（実質時間としては 5 時間程度） | 2 週間～1 カ月<br>（実質時間としては 15 時間程度） | 1 週間以上 2 週間未満<br>（実質時間としては 10 時間程度） |
| 難易度 | 適切 | 難しい | 難しい |
| 回答に必要なスキル | 応用情報技術者試験程度 | 情報処理安全確保支援士程度 | 情報セキュリティマネジメント試験程度 |
| 項目数 | 比較的多い | とても多い | とても多い |
| 項目内容・リスク | 分かりやすい | どちらでもない | どちらでもない |
| 達成基準 | 分かりやすい | 分かりづらい | どちらでもない |
| メリット | ・ リスク点検の外注費用を抑えられる。<br>・ 本ツールを活用することで VPP 事業でも継続的なリスク点検を実施することが可能である。 | ・ より細かな視点でセキュリティ対策をチェックすることができる。 | ・ リスク点検項目が細かく、想定されるリスクも分かりやすい。<br>・ 自社のセキュリティ対策方針作成及びシステムベンダーへのセキュリティ対策に活用可能できる。 |

表 3-4 アンケートの指摘事項と修正対応

| NO | 指摘事項 | 修正対応 |
|---|---|---|
| 1 | サブカテゴリー「DE.AE-4」における「イベント」を具体的にイメージすることが難しい。 | 「イベント」を「セキュリティ事象」という用語に変更し、意味を明確化した。 |
| 2 | サブカテゴリー「RS.RP-1」における「対応計画」が何を具体的に示しているか分からない。 | 「対応計画」を「インシデント対応計画」という用語に変更し、意味を明確化した。また、ガイドにおいても「インシデント対応計画」を用語集に追加した。 |
| 3 | サブカテゴリー「ID.AM」全体の達成基準が、運用実態と制度構築に分かれているため、分割した別の設問に分けるとより分かりやすい。 | 達成基準は NIST-CSF に基づいて策定しているため、現状の記載に留める。本リスク点検ツールの評価基準では、事実的な運用を重要視し、運用制度の構築は追加ステップとして位置付けているところ、この方針について、ガイドやツールの使い方にも記載した。 |

| NO | 指摘事項 | 修正対応 |
|---|---|---|
| 4 | 可視化結果で評価が 0 になる際に、「活用区分」の選択により該当するチェック項目がない場合と該当項目の対策が実施できていない場合の区別がつかない。 | 「活用区分」の選択により該当項目がない場合は、可視化結果シートでグレーアウトされるよう修正した。 |
| 5 | 事業区分・規模に応じて、現状より項目を絞り込んでいただきたい。 | ツールを任意活用する際は、事業者が必要だと思われる項目のみで評価することも可能である。参考としてサイバーセキュリティ経営ガイドラインのみに対応した項目のみで評価できることをガイドに記載した。 |
| 6 | 設問の達席基準に対して事業区分ごとに推奨されるレベルを示していただきたい。 | 広域機関の取組（後述）では、平均 2 点以上にすることを会員企業に推奨しており、参考値として本リスク点検ツールでも記載した。 |

## 3.3 リスク点検ツールの位置付け・普及展開方法の検討

### 3.3.1 リスク点検ツールの普及展開方法

リスク点検ツールは、任意ツールとして資源エネルギー庁の HP で公開し、周知・普及促進を図ることを予定している。3.1.2 に示したとおり、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ている。

対象事業者のうち、発電事業者、小売電気事業者、特定卸供給事業者については、登録・届出の際に、電力広域的運営推進機関（広域機関／OCCTO）への会員登録が必須である。そのため、3.3.2 に示す広域機関との取組の連携によって、これらの事業者に対して広く普及促進されることが想定される。自家用電気工作物設備設置者に対しては、必要資格である電気主任技術者の保持者を管理している全国電気管理技術者協会連合会（全技連）、電気主任技術者を主体とした日本電気技術者協会、保安協会を取りまとめている電気保安協会全国連絡会等を通じて周知を行うことが効果的である。周知・普及促進の方策と対象事業者の対応関係を図 3-6 に示す。

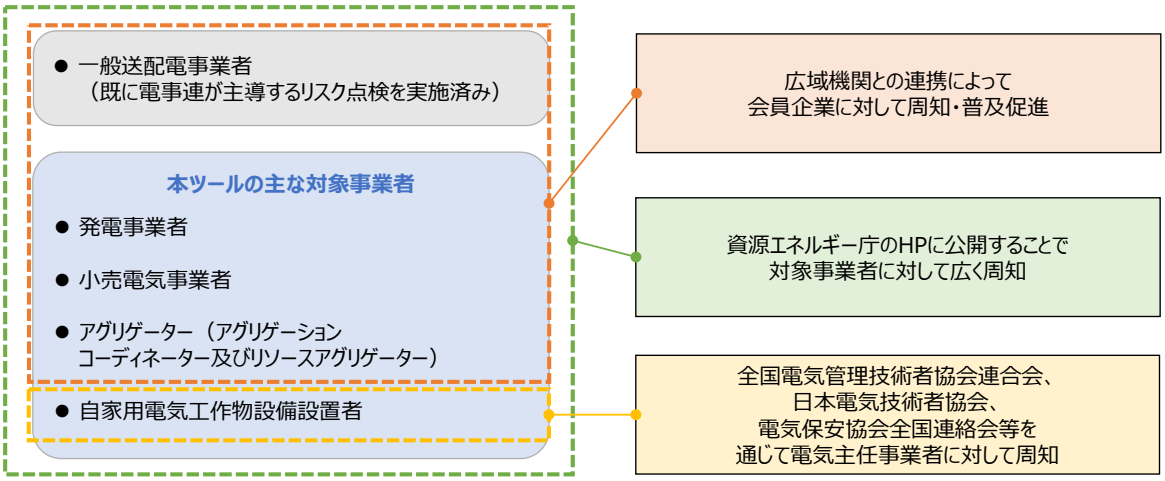



図 3-6 周知・普及促進策の対応関係

### 3.3.2 広域機関との連携

上記の普及促進策の一つである広域機関との連携について、広域機関が会員企業に対して実施しているセキュリティ自己診断に関する既存の取組との連携に向け、調整を実施した。セキュリティ自己診断に関する既存の取組とは、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、広域機関が運用している取組を指す。本取組とリスク点検ツールの連携に向けて広域機関と複数回協議を行った。

具体的な連携イメージを図 3-7 に示す。現行の広域機関の取組では、広域機関が用意した自己診断ツールに対し、会員企業が自社の対策状況を確認し、結果を広域機関に返送する形式であるが、本ツールが公開された暁には、広域機関が会員企業に対して情報セキュリティ対策レベルの把握及び報告を促す際に本リスク点検ツールに基づくリスク点検の実施及び結果の提出を依頼するスキームとなる。広域機関からリスク点検を依頼された会員企業においては、資源エネルギー庁の HP に公開されているリスク点検ツールをダウンロードし、対策状況可視化ツールの「活用区分」から「広域機関提出用」を選択した後、抽出されたリスク点検項目に対するリスク点検結果を広域機関に提出することとなる。

また、自己点検のデータについても共有を図ることを想定している。2024 年度以降の会員企業のリスク点検結果は、広域機関により個社が特定されないよう統計処理した上で、資源エネルギー庁に共有予定である。今後、電力 SWG においてはリスク点検ツールに対する取組状況や点検結果等も踏まえ、電力分野におけるセキュリティ対策のあり方を検討していく。

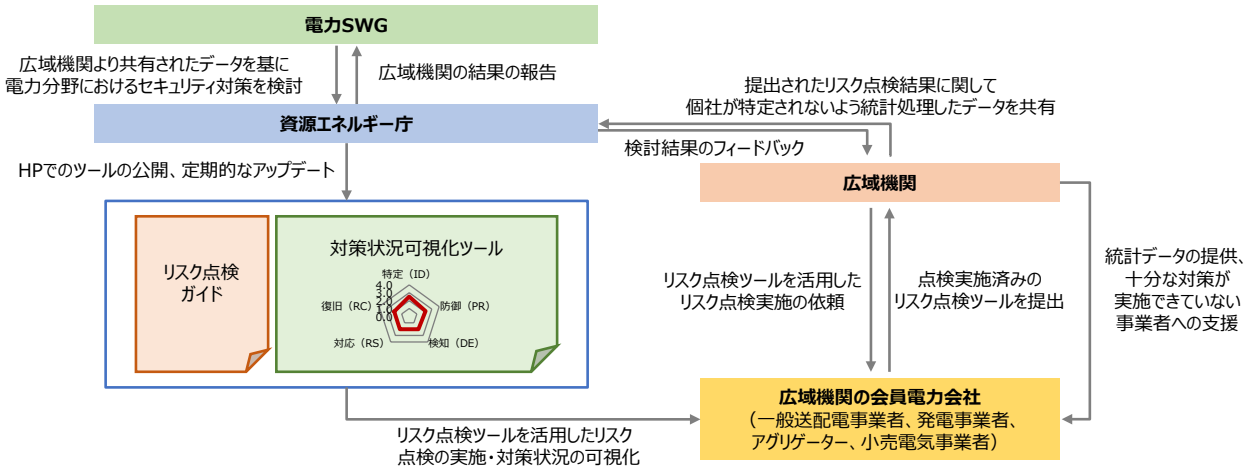



図 3-7 本リスク点検ツールと広域機関の取組との連携スキーム

### 3.3.3 リスク点検ツールのメリット

リスク点検ツールの活用が事業者に与えるメリットとして、ツールの目的としている合理的なリスク点検によるリスク可視化以外に、図 3-8 のとおり、3 点のメリットが想定される。1 点目は、規制においてセキュリティ対策が要求されている事業者において、規制要件に対する確認の効率化（①）が想定される。例えば、特定卸供給事業者は届出に当たって必要な「サイバーセキュリティ確保実施内容一覧」の記入おけるリスク点検ツールの活用が挙げられる。2 点目は、規制有無に関わらずリスク点検に対するコスト低減効果が得られる。試行利用のアンケートにおいても、リスク点検の内製化や外部委託費用の削減が想定される旨の意見があった。3 点目は、第三者に対するセキュリティ対策状況の説明が効率化される。例えば、保険会社へセキュリティ対策状況の説明が可能であり、保険料に低減につながる可能性がある。それぞれのメリットを事業者が享受できるよう、ツールの普及展開・位置付けを検討する必要がある。

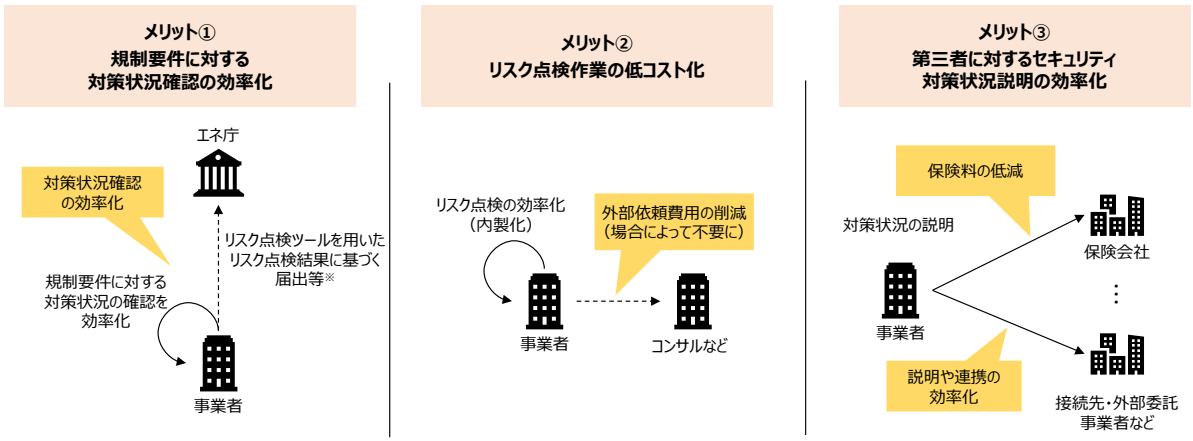



図 3-8 リスク点検ツールが事業者に与えるメリットのイメージ

### 3.3.4 今後のリスク点検ツールの位置付けの方針

今後は、広域機関との連携より得られる自己点検のデータを基にツールの浸透状況やツールに基づくリスク状況を定期的に確認し、当該状況を踏まえてリスク点検ツールの位置付けを検討していくことが

効果的だと考えられる。そのためには、広域機関のデータを解析できる環境を構築が今後求められる。

電力 SWG 委員に対する意見交換の場や電力 SWG で得られた意見より、電気事業者のセキュリティ対策向上に向けて、リスク点検ツールについては段階的に要求レベルを向上させることが重要だと考えられる。一方で、全ての事業者に求めるのではなく、事業区分や規模に応じて検討する必要がある。また、要求レベルの向上に合わせて、リスク点検ツールの利用による税制や経費面での優遇措置を含めた様々なインセンティブの検討が求められる。

# 4. 分散型エネルギーリソースに係るセキュリティ対策の検討

アグリゲーターライセンス制度の開始（令和 4 年 4 月）や蓄電池等の分散型エネルギーリソースの普及などにより、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（ERAB）が注目されている。今後、このビジネスが活発化することが期待されることを踏まえて、分散型エネルギーリソースに係るセキュリティ対策に関する実態整理を行うとともに、当該対策のあり方や実装方法について議論・検討を行った。

## 4.1 分散型エネルギーリソースに係るセキュリティ脅威事例

電力業界においては、現在まで DER に対する直接的な攻撃は報告されていないが、DER が増加する中で潜在的な攻撃リスクが増大している。（表 4-1 参照）

これらのリソースが攻撃対象となると、電力供給の中断や制御の混乱など、深刻な影響が発生する可能性がある。そのため、DER に特有の脆弱性を理解し、継続的なモニタリングと迅速なインシデントレスポンス、情報共有と業界標準の整備、意識向上トレーニング、サプライチェーンセキュリティなどの対策が不可欠である。

表 4-1 分散型エネルギーリソースに係るセキュリティ脅威

| No. | タイトル | 発生時期 | 事例概要 |
|---|---|---|---|
| 1 | コンテック社製の太陽光発電監視製品に脆弱性 | 2023 年 7 月 | ● Palo Alto Networks は 2023 年 6 月 22 日、Mirai の亜種が SolarView の脆弱性を悪用してデバイスをハッキングし、ボットネットに陥れていると報告[10]した。この脆弱性（CVE-2022-29303）は、ボットネットの標的となっている約 20 の脆弱性のうちの一つである。また、SolarView は、コンテック社が販売する太陽光発電の監視・可視化ソリューションで、3 万以上の発電所で使用されている。<br>● CVE-2022-29303 は、SolarView バージョン 6.0 に影響するコード・インジェクションの原因とされている。この脆弱性は、認証されていない攻撃者によってリモートから悪用される可能性がある。<br>● セキュリティに関する Web サイトを提供する SecurityWeek が実施した Shodan の検索によると、インターネットに公開されている SolarView システムは 600 台以上あり、そのうち 400 台以上が脆弱なバージョ |

[10] Palo Alto Networks Unit 42、沈黙の IoT:複数の IoT エクスプロイトを悪用する最新 Mirai キャンペーンの解剖 https://unit42.paloaltonetworks.jp/mirai-variant-targets-iot-exploits/

| No. | タイトル | 発生時期 | 事例概要 |
|---|---|---|---|
| | | | ンを実行している。[11] |
| 2 | 太陽光発電診断・監視ソリューションのインターネット上への公開 | 2023 年 7 月 | ● セキュリティ企業である Cyble が実施した調査[12]により、インターネットに公開されている太陽光発電（PV）診断・監視ソリューションが世界全体で 13 万件以上あることが分かった。<br>● PV の診断・監視システムに対するサイバー攻撃は、エネルギー生産の減少、システムの不安定性、物理的資産の損傷、サイバーセキュリティに関する独自の課題など、分散型エネルギー源（DER）に深刻な影響を及ぼす可能性がある。<br>● スピアフィッシング、サービス拒否（DoS）攻撃、資産への物理的損害といった脅威とは別に、攻撃者はインターネットに接続された PV プラント監視・診断システムを通じて PV インバーター制御を標的にすることができる。これらのシステムの露出度は高いため、悪意のあるハッカーの潜在的な標的になる可能性がある。<br>● PV 監視・計測ソリューションが古いファームウェアを使用している場合、これらのデバイスを悪用することは非常に容易である。これらのシステムは、脆弱性を抱えやすいウェブベースのソリューションであり、国家機関やベンダーは、PV 監視・測定ソリューションに関連するセキュリティ勧告を積極的に発表している。現在、これらのシステムには、複数の概念実証（Proof of Concepts）と脆弱性が報告されており、悪用される可能性を高めている。 |
| 3 | ソーラーパネルコンバーターの脆弱性 | 2023 年 5 月 | ● オランダ政府のデジタルインフラ検査局（RDI）が火曜日に発表した調査結果[13]によると、ソーラーパネルコンバーターはハッキングに対して脆弱であり、その多くがサイバーセキュリティ要件を満たしていないと警告している。<br>● 多くのコンバーターは干渉を引き起こし、サイバーセキュアではないため、例えば近くにある無線機器の故障や誤動作を引き起こしたり、ソーラーパネルの設置がハッキングされ |

[11] SecurityWeek、Exploited Solar Power Product Vulnerability Could Expose Energy Organizations to Attacks https://www.securityweek.com/exploited-solar-power-product-vulnerability-could-expose-energy-organizations-to-attacks/

[12] Cyble、Security Gaps in Green Energy Sector: Unveiling the Hidden Dangers of Public-Facing PV Measuring and Diagnostics Solutions https://cyble.com/blog/security-gaps-in-green-energy-sector/

[13] National Inspectorate for Digital Infrastructure (RDI)、Omvormers kunnen storing veroorzaken en zijn vaak makkelijk te hacken https://www.rdi.nl/actueel/nieuws/2023/05/30/omvormers-kunnen-storing-veroorzaken-en-zijn-vaak-makkelijk-te-hacken

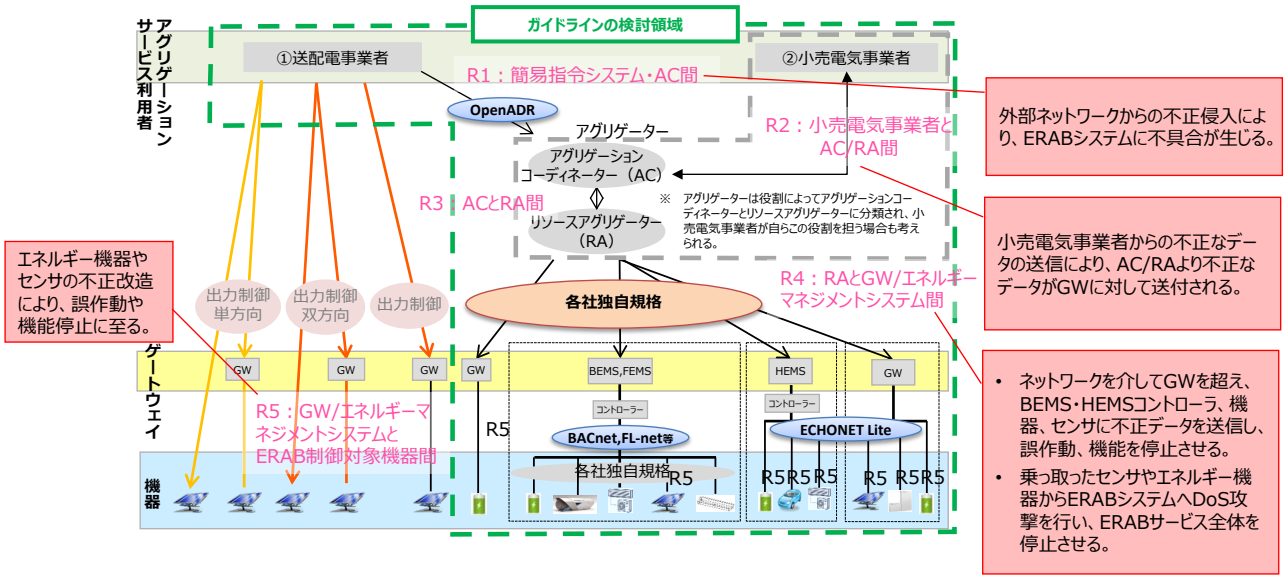
| No. | タイトル | 発生時期 | 事例概要 |
|---|---|---|---|
| | | | たりする可能性がある。<br>● ソーラーパネルコンバーターは、ソーラーパネルが受ける太陽光を確実に電気に変換する。この研究では、9 つのソーラーパネルコンバーターが分析され、5 つのコンバーターに危険な兆候が見られた。<br>● もし、攻撃者が組織的な攻撃を仕掛けて、全てのコンバーターの電源を一度に切り、再びオンにすれば、送電網にスパイクが発生し、送電網が破壊されかねない。そうなれば、オランダ全体が電力不足に陥る可能性があるとのこと。 |
| 4 | EV 充電ステーションの脆弱性 | 2020 年 11 月 | ● ニューヨーク大学の研究者らが実施した研究[14]によると、ハッカーが多数の充電ステーションに同時に侵入し、スイッチのオン・オフを繰り返すことが可能だという。これは大規模な運行の遅れや不便につながるだけでなく、送電網の変電所にある過電流リレーが作動すれば、地域的な停電につながる可能性もある。 |

出所）各種公開情報に基づき三菱総合研究所作成

## 4.2 分散型エネルギーリソースに係るセキュリティ対策の現状

ERAB システムでは、送配電事業者、アグリゲーションコーディネーター（AC）、リソースアグリゲーター（RA）、小売電気事業者など多くのステークホルダーが関与する。「ERAB に関するサイバーセキュリティガイドライン」では、ERAB システムのレイヤーを整理した上で、図 4-1 に示すとおり、ERAB システムにおいて想定されるセキュリティ脅威が示されている。

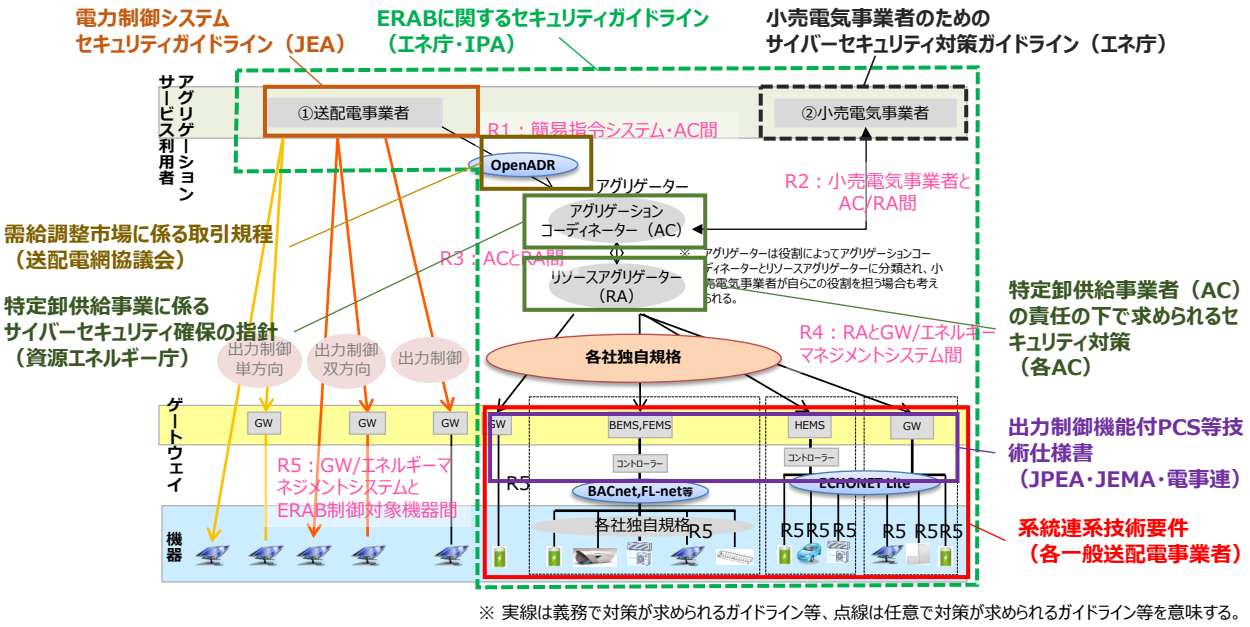
[14] IEEE、Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective
https://ieeexplore.ieee.org/document/9272723




出所）「ERAB に関するサイバーセキュリティガイドライン」に基づき三菱総合研究所作成

図 4-1 ERAB システムの概要と想定されるサイバーセキュリティ脅威

ERAB システムに求められるセキュリティガイドラインとして、図 4-2 に示すとおり、システム全体に対する「ERAB に関するセキュリティガイドライン」があるほか、個々のステークホルダーに対するガイドラインが整備されている。末端のリソースに関して、系統に接続する設備は「系統連系技術要件」に基づく対策が求められるほか、出力制御機能付 PCS について、セキュリティの要件を含んだ技術仕様書が公開されている。また、ERAB サイバーセキュリティガイドラインにおいて、対策事項の一つとして、「第三者による監査（認証を含む）や教育プログラム等によって勧告指定項目を中心にその実装を検証すること」が勧告事項として、定められているが、具体的な教育プログラムとして、IPA の産業サイバーセキュリティセンター（ICSCoE）では、ERAB 事業者に対する短期のサイバーセキュリティ教育プログラムを開催している。




出所）各種ガイドライン等に基づき三菱総合研究所作成

図 4-2 ERAB システムが準拠すべきセキュリティガイドライン等

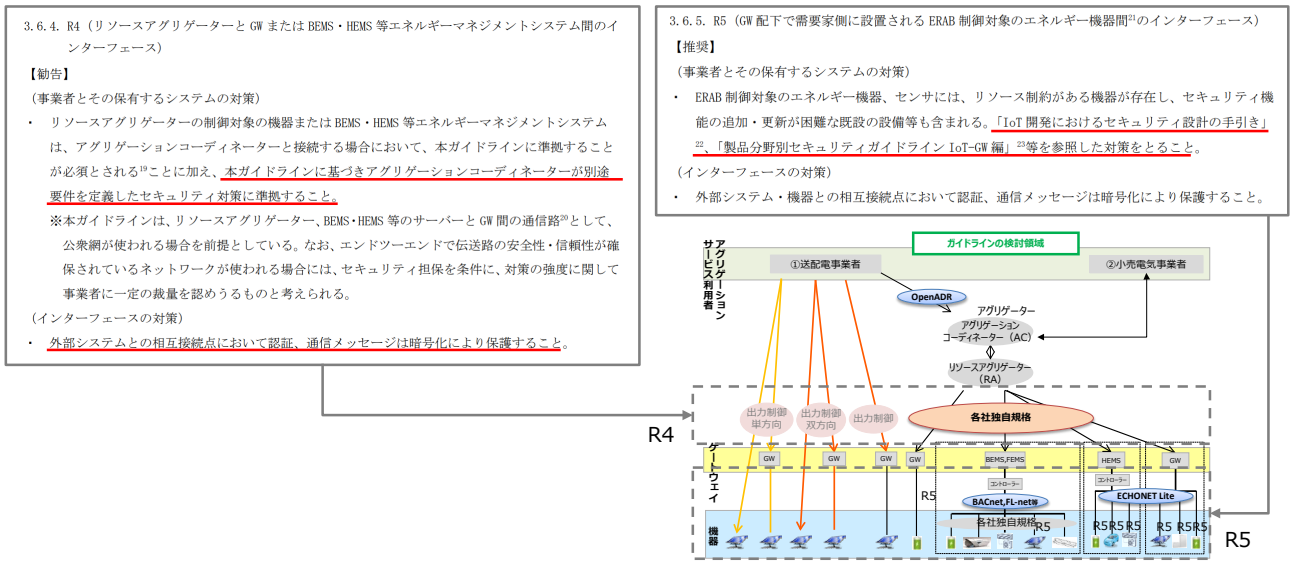
以降では、各種ガイドライン等及び取組に関する概要を示す。

## （1）「ERAB に関するサイバーセキュリティガイドライン」の概要

ERAB に関するサイバーセキュリティガイドラインは、アグリゲーターをはじめとする ERAB 事業者が取り組むべきサイバーセキュリティ対策が整理されたものであり、2017 年に初版を策定し、2019 年 12 月に改正版（Ver 2.0）が公表された。

本ガイドラインでは、ERAB に参画する各事業者が実施すべき最低限のサイバーセキュリティ対策の要求事項を示しており、各事業者はガイドラインを踏まえて、自らの責任においてセキュリティ対策を講ずることを求めている。ガイドラインの記載事項は、実装を必須として義務づけられる【勧告】と、実装を検討すべき内容である【推奨】に分類される。詳細対策要件の内容について、脅威に対する対策例を詳細に検討し規定するほか、ERAB システムに関係する特定のテーマに応じた対策について規定することが求められているが、具体的な策定方法、内容、対策のレベル感等については明記されていない。

R4 においては、インターフェースの対策として、外部システムとの相互接続点における認証や通信の暗号化が求められているほか、アグリゲーションコーディネーター（AC）が作成する詳細対策要件に対する準拠が求められている。末端の R5 においては、「IoT 開発におけるセキュリティ設計の手引き」等を参照した対策が推奨されている。




出所）「ERAB に関するサイバーセキュリティガイドライン」に基づき三菱総合研究所作成

図 4-3 ERAB セキュリティガイドラインにおける末端 DER のセキュリティ対策に関する記載

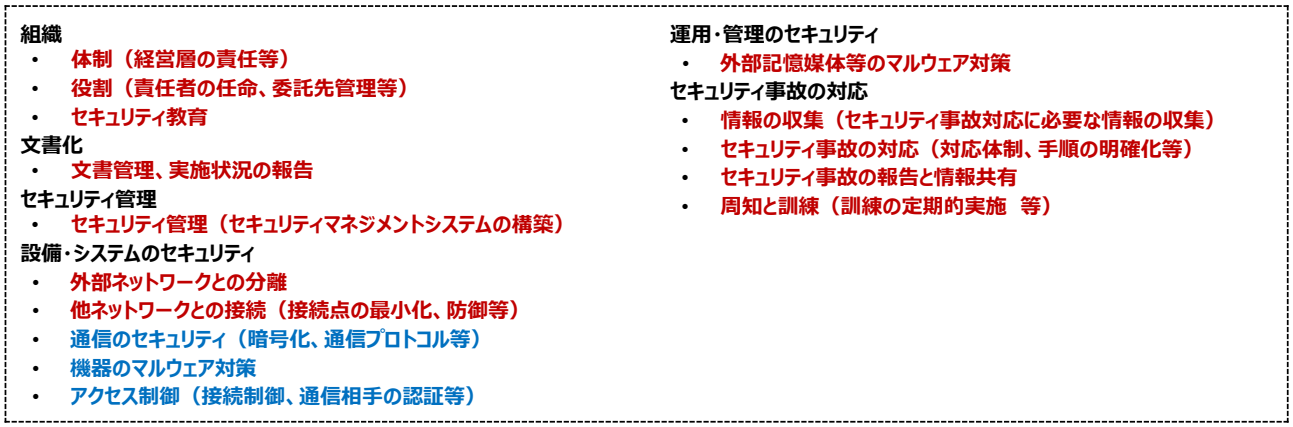
## （2）「特定卸供給事業に係るサイバーセキュリティ確保の指針」の概要

2022 年 4 月より、特定卸供給事業者（アグリゲーター）制度が開始した。現行の制度では、電力を束ねて他の電気事業者に対して卸供給を行う最上位のアグリゲーター（AC）に対してのみ規制を設け、このアグリゲーターに対しては、下位のアグリゲーター（RA）の範囲を含めて責任を課すこととしている。

アグリゲーターの事業においてはサイバーセキュリティ対策が特に重要であるところ、届出の際に対策が不十分と考えられる事業者に対しては変更命令、事業実施中に対策が不十分と考えられる事業者に対しては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。特定卸供給事業の届出時は本指針に基づき審査が行われるため、本指針の記載事項を遵守しているかを証する書類を添付する必要がある。

「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。すなわち、特定卸供給事業を実施する際、「電力制御システムセキュリティガイドライン」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」の勧告的事項についてセキュリティ対策が実施されている場合には、変更命令や業務改善命令の対象にはならない。（図 4-4 参考）




出所）「特定卸供給に係るサイバーセキュリティ確保の指針」に基づき三菱総合研究所作成

図 4-4 「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

### （3）「需給調整市場に係る取引規程」の概要

需給調整市場に係る取引規程は、需給調整市場における再生可能エネルギーの予測誤差に対応する「三次調整力②（RR－FIT）」や電源脱落に対応する「三次調整力①（RR）」など、様々な調整力に関する取引、運用、精算についての規定事項を定めている。一般送配電事業者については、全国一市場で特定の調整力を調達し、全国広域的に上げ調整及び下げ調整を行い、最経済な運用を目指すことが明記されている。

本規定では各調整力において遵守すべきセキュリティ要件についても明記されており、「電力制御システムセキュリティガイドライン」及び「エネルギー・リソース・アグリゲーション・ビジネスに関するサイバーセキュリティガイドライン」に準拠する旨が規定されている。

表 4-2 需給調整市場に係る取引規程において規定されているセキュリティ要件

| 項目 | 内容 |
|---|---|
| 第 13 条<br>リソース等が満たすべき要件 | (ｲ) 専用線オンラインで施設する場合<br>送受信機能は以下のとおりとする。<br><br>なお，当該機能については，「電力制御システムセキュリティガイドライン」に準拠する。<br>また，属地エリアの一般送配電事業者が定めるセキュリティ要件に従う。 |
| | (ﾛ) 簡易指令システムを用いたオンラインで施設する場合<br>送受信機能は以下のとおりとする。<br>なお，当該機能については，「エネルギー・リソース・アグリゲーション・ビジネスに関するサイバーセキュリティガイドライン」のセキュリティ要件に準拠するものとし，取引会員のアグリゲーションコーディネータシステムと簡易指令システム間のインターフェースの通信仕様については，OpenADR2.0b に準拠する。 |

| 項目 | 内容 |
|---|---|
| 第 14 条<br>電力制御セキュリティの確認 | 取引会員は，第 13 条（リソース等が満たすべき要件）（2）ロに定める通信設備を施設するにあたり，属地エリアの一般送配電事業者へ以下の書類等を提出し，属地エリアの一般送配電事業者は，当該書類等により当該通信設備のセキュリティの妥当性を確認する。<br>（1） 専用線オンラインの場合<br>取引会員の電力制御システムが，「電力制御システムセキュリティガイドライン」に準拠していることが確認できる書類等<br>（2） 簡易指令システムの場合<br>取引会員のシステムおよび取引会員と簡易指令システム間のインターフェースが，「エネルギー・リソース・アグリゲーション・ビジネスに関するサイバーセキュリティガイドライン」に準拠していること，簡易指令システムとの直接的な接続部においては，「電力制御システムセキュリティガイドライン」に準拠していることが確認できる書類等 |
| 第 23 条<br>性能データに関わる提出資料 | （3） 通信回線<br>「電力制御システムセキュリティガイドライン」および「エネルギー・リソース・アグリゲーション・ビジネスに関するサイバーセキュリティガイドライン」に準拠していることが確認できるもの。ただし，電源Ⅱ契約等または余力活用に関する契約を締結し三次調整力②相当の機能を有する場合はその契約書の写しをもってこれに代えることができる。 |

出所）「需給調整市場に係る取引規程」に基づき三菱総合研究所作成

### （4）「系統連系技術要件」の概要

2020 年 10 月より、一般送配電事業者が定める「託送供給等約款別冊系統連系技術要件」にサイバーセキュリティに関する要件が規定された。

本規定により、電力事業の用に供しない小規模の発電設備を含め、系統に連系する発電設備に対してはすべからくサイバーセキュリティ対策が求められる。具体的なサイバーセキュリティ対策の内容として、サイバーインシデントの発生を防ぐ事前防御の観点と、インシデント発生後の影響を最小化する事後対応の観点の両方から、3 つの対策が求められている。（表 4-3 参照）

新たな系統連系技術要件は、新たに系統に連系する場合又は既存設備のリプレース等の場合に適用される。ただし、対策③については、既に系統に連系しているものも含め、発電設備の設置者において、今般の系統連系技術要件の見直し後速やかに実施される。また、システム改修を伴うこととなる対策①及び対策②については、既存設備のリプレース等のタイミングを活用して順次新たな対応を求めていく方針が示されている。なお、追加された要件は、2020 年 10 月以降に契約申込みを行うもの（電源接続案件募集プロセス対象の設備にあっては、2020 年 10 月以降に入札を実施するもの）を対象に実施を求めることとされている。

表 4-3 系統連系技術要件で求められる 3 つの対策の概要

| 観点 | 求められる対策 |
|---|---|
| サイバーインシデントの発生を防ぐ事前防御 | 対策① ネットワーク接続点の保護 |
| | 対策② データの保存・転送を行う機器・端末等のマルウェア対策 |

| 観点 | 求められる対策 |
|---|---|
| インシデント発生時の影響を最小化する事後対応（早期発見、迅速な対処） | 対策③ 連系先系統運用者に対するセキュリティ管理責任者の氏名及び緊急時連絡先の通知 |

出所）「系統連系技術要件」に基づき三菱総合研究所作成

### （5）「出力制御機能付 PCS 等技術仕様書」の概要

出力制御機能付 PCS 等は，2015 年 2 月 17 日第 4 回系統 WG、2018 年 10 月 10 日第 17 回系統 WG 及び 2023 年 2 月 28 日第 44 回系統 WG で提案された「出力制御システム」を達成するための機能を具備することが求められる。

出力制御システム構築に当たっては、①出力制御は系統安定化のために必要最小限なものとすること②出力制御の対象となる発電事業者間の「公平性」を確保すること③出力制御システムの「運用実行性」を確保することを基本的な考え方としている。

要件は以下の表 4-4 のとおりであり、電力安定供給のため、必要なセキュリティを確保することも求められる。技術仕様書への具体的な記載例を図 4-5 に示す。

表 4-4 出力制御システムに求められる要件

| システム構築の視点 | 具体的な対応（主なもの） |
|---|---|
| コスト面，技術面等も踏まえ，確実に出力制御可能であること | 発電設備容量を考慮して通信方式を選定することが現実的であり、基本的には、出力規模の大きい特別高圧連系等は専用回線、出力規模が小さい高圧以下連系はインターネット回線を活用したシステムを構築する等 |
| 出力制御は系統安定化のために必要最小限なものとすること | ・必要最小限の出力制御を実現するため、部分制御、時間制御などきめ細かい制御が可能な仕様とする<br>・余剰買取は、自家消費分は制御しない 等 |
| 将来の情勢変化等に対して，柔軟に対応できること | ・再エネ連系量の拡大にも柔軟に対応可能な制御方式とする<br>・将来、配信事業者（アグリゲータ）などによる付加価値サービス提供などにも対応可能である 等 |
| 電力安定供給のため，必要なセキュリティを確保すること | ・インターネット回線を活用する場合、不正アクセス、サイバー攻撃などの脅威への対策を実施する<br>・制御データ改ざんや時刻改ざんなどへの対策を実施する 等 |
| 全ての一般送配電事業者に適用可能な共通の仕様とすること | ・発電事業者団体、PCS メーカー、電力会社による議論を踏まえて、技術仕様を全国共通とする |

出所）「出力制御機能付 PCS 等技術仕様書」に基づき三菱総合研究所作成

o 電力サーバとのやりとりには、個人情報等の重要情報を含めない。
・出力制御スケジュールにおいて、出力制御量（出力上限値、時間）を指定する。
・PCSは、出力制御スケジュールのダウンロードのみの機能とし、PCSから個人情報等の重要情報は送信しない。（ID設定等の識別情報など、運用に必要な情報を除く）

o 出力制御スケジュールのバックアップ（年間設定＋部分書換機能）
・ID認証により、PCSと電力サーバ間で相互に確認することで、事業者のスケジュール受信誤りを防止。
・通信故障時は、予め設定した故障前の最新スケジュール（年間設定）により制御する仕様とすることで、出力制御の実行性を担保。

o PCSの外部遠隔操作の防止
・スケジュール更新は、PCS側からセッションを開始して実施する仕様とし、電力会社を含め、外部からのスケジュール書換、遠隔操作はできない仕様とする。（最短30分毎のスケジュール更新には対応）

| 想定される脅威 | |
|---|---|
| 電力サーバ | ①ウイルス感染<br>②サイバー攻撃<br>③不正侵入／不正通信<br>④PCSなりすまし |
| 通信途中 | ⑤データ改ざん<br>⑥盗聴・漏えい |
| PCS | ⑦ウイルス感染<br>⑧サイバー攻撃<br>⑨不正侵入／不正通信<br>⑩サーバなりすまし |

| システムの対策 | |
|---|---|
| 電力サーバ | ・ファイアウォール<br>・サーバ2重化　など<br>・スケジュール設定のバックアップ<br>・ID認証（PCSとの相互確認） |
| 通信途中 | ・SSL通信による暗号化<br>・重要情報を含めない |
| PCS | ・外部からのセッション開始不可<br>・スケジュール設定のバックアップ<br>・通信先として電力サーバを指定<br>・SSL通信 |

出所）経済産業省「出力制御機能付PCSの技術仕様について」[15]

図 4-5 インターネット回線を活用する場合、必要なセキュリティを確保するための技術仕様書への記載例

### （6）「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」の概要

2021 年 2 月、経済産業省は「小売電気事業者のためのサイバーセキュリティ対策ガイドライン」を策定・公表した。本ガイドラインでは「サイバーセキュリティ経営ガイドライン」の対策内容を踏襲しつつ、小売電気事業者が各々の事業モデルに適したサイバーセキュリティ対策を実践するための重要 10 項目に対する具体的な解釈及び指針を記載している。その他、小売電気事業者に想定されるサイバーセキュリティリスクの例や、想定されるサイバー攻撃、小売電気事業者の類型等も整理されている。

表 4-5 小売電気事業者のためのサイバーセキュリティ対策ガイドラインにおける 10 項目

| 項目 | 概要 |
|---|---|
| 1 | サイバーセキュリティリスクの認識、組織全体での対応方針の策定 |
| 2 | サイバーセキュリティリスク管理体制の構築 |
| 3 | サイバーセキュリティ対策のための資源（予算、人材等）確保 |
| 4 | サイバーセキュリティリスクの把握とリスク対応に関する計画の策定 |
| 5 | サイバーセキュリティリスクに対応するための仕組みの構築 |
| 6 | サイバーセキュリティ対策における PDCA サイクルの実施 |

15 https://www.meti.go.jp/shingikai/enecho/shoene_shinene/shin_energy/keito_wg/pdf/005_02_00.pdf

| 項目 | 概要 |
|---|---|
| 7 | インシデント発生時の緊急対応体制の整備 |
| 8 | インシデントによる被害に備えた復旧体制の整備 |
| 9 | ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握 |
| 10 | 情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供 |

出所)「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」に基づき三菱総合研究所作成

### (7) 「ERAB システムに関するセキュリティ教育プログラム」の概要

ERAB 事業者に対して、ERAB サイバーセキュリティガイドラインでは、対策事項の一つとして、「第三者による監査(認証を含む)や教育プログラム等によって勧告指定項目を中心にその実装を検証すること」が勧告事項として、定められている。

具体的な教育プログラムとして、IPA の産業サイバーセキュリティセンター(ICSCoE)では、VPP の社会実装を見据え、ERAB 事業者に欠かせないサイバーセキュリティ対策スキル向上のため、ERAB に関するサイバーセキュリティガイドライン Ver2.0 に基づく、ERAB システムに関するサイバーセキュリティトレーニングを ERAB 事業者に対して提供している。本業務では、同トレーニングを受講することにより、ERAB 事業者に求められるサイバーセキュリティ対策の必要性を理解し、実践できる人材を育成することを目的としている。なお、2023 年度はプログラム更新のため休止している。

コースは大きく 4 つに分かれ、座学編のオンデマンド配信及び演習編の集合開催の形式を採用している。本プログラムを修了するためには、いずれのコースにも参加する必要がある。(表 4-6 参考)

表 4-6 ERAB システムに関するサイバーセキュリティトレーニングの内容

| 名称 | 開催形式 | 内容 |
|---|---|---|
| ガイドライン編 | オンデマンド配信 | ・ 電力分野のサイバーセキュリティ脅威に対する現況解説<br>・ 電力分野に関連するサイバーセキュリティ規制・ガイドライン類の概要解説<br>・ ERAB サイバーセキュリティガイドライン・CPSF の解説<br>・ 脅威や脆弱性を評価・検討する手法の解説 |
| リスク分析編① | オンデマンド配信 | ・ CCRC 技術参考報告書の解説<br>・ ERAB システムのリスク分析概要解説<br>・ ERAB システムにおける対策選定手法の解説<br>・ ERAB システムに想定されるリスクシナリオ(ユースケース) |
| リスク分析編② | 集合開催 | ・ ユースケースに基づくリスク分析の実演<br>・ 詳細対策要件の検討(グループワーク) |
| 模擬プラント編 | 集合開催 | ・ 模擬プラント環境を用いた実演(デモ)を中心とした演習 |

出所)IPA「実務者向けプログラム ERAB サイバーセキュリティトレーニング 2022 年度」に基づき三菱総合

研究所作成[16]

## 4.3 分散型エネルギーリソースに係るセキュリティ対策の課題

前節に示すとおり、ERAB システムを含む分散型エネルギーリソースのセキュリティ対策について、様々な取組が進められてきたところである。一方で、事業者や有識者と意見交換やヒアリングを実施したところ、対策実施に当たって様々な課題が提起された。

ヒアリングや意見交換で挙げられた主な課題は表 4-7 に示すとおりである。具体的には、ERAB セキュリティガイドラインの準拠のために、各社で詳細対策要件を作成することが求められている一方で、現状ではその作成が困難であることや、作成した詳細対策要件の妥当性を確認することが難しいことの課題が挙げられた。事実、「ERAB に関するセキュリティガイドライン」では、ERAB に参画する事業者において、具体的な対策を策定した「詳細対策要件」を自らの責任で策定することを勧告事項として求めている一方で、具体的な策定方法、内容、対策のレベル感等については明記されていない。

また、これまでのガイドラインでは具体的に想定してこなかった電力系統及びアグリゲーターシステムに接続する末端の DER 設備等のセキュリティ対策に対する懸念が示唆された。例えば、R4 におけるインターフェースの対策として、外部システムとの相互接続点における認証や通信の暗号化が求められているほか、アグリゲーションコーディネーター（AC）が作成する詳細対策要件に対する準拠が求められているが、詳細対策要件が適切に策定されていない場合、ゲートウェイ設備の対策が不十分なものになるおそれがある。特に、DER 設備は IoT 機器の側面も有するところ、今後リスクが増大することが懸念された。

加えて、業界として、アグリゲーターにおけるセキュリティ対策の実態を把握できていない課題が挙げられた。

表 4-7 ヒアリングや意見交換で挙げられたセキュリティ対策における課題

| 課題概要 | 課題内容 |
|---|---|
| 詳細対策要件の作成・確認について | ・ ERAB セキュリティガイドラインに準拠するための詳細対策要件を作成するのが難しい。<br>・ チェックシートを作成する場合は、事業の重要度によって対策要件が変わることが望まれる。<br>・ 自社で作成した詳細対策要件に抜け漏れがある可能性がある。 |
| 末端の DER 設備の脆弱性に起因する脅威について | ・ ERAB セキュリティガイドラインの R4，R5 に当たる DER 設備等のセキュリティを高めることが望まれる。<br>・ 特に太陽光のリソースは数が増えている一方、セキュリティの検討が不十分である。 |
| ガイドラインの定期アップデートについて | ・ アグリゲーションは一過性ではなく、様々な分散型エネルギー源が追加されるため、ガイドラインを定期的にメンテナンスする必要がある。 |

[16] https://www.ipa.go.jp/jinzai/ics/short-pgm/erab/2022.html

## 4.4 分散型エネルギーリソースのセキュリティ対策のあり方に関する検討

前項で示した事業者の課題等を踏まえ、分散型エネルギーリソースのセキュリティ対策のあり方に関する検討を行った。

### （1） 詳細対策要件の作成・確認に係る支援について

ERAB に参画する事業者において策定が求められる詳細対策要件について、参考となる考え方の整理や ERAB に参画する事業者が相談できる体制の整備等について、検討する必要があると考えられる。参考となる考え方の整理に当たっては、事業者が抱える課題をより詳細に把握するとともに、既に適切な詳細対策要件を作成している事業者の取組を参考として整理することが想定される。前述のとおり、ERAB システムにおいては様々なステークホルダーが関与するところ、それぞれのステークホルダーに求められる責任や役割を明確化した整理が重要となる。

### （2） 末端の DER 設備に対する対策について

太陽光発電をはじめとして、DER の更なる追加が今後見込まれるところ、近年の IoT に関する脅威動向や取組動向を踏まえつつ、末端の IoT 機器等に求められるセキュリティ対策を整理することが必要と考えられる。その上で、どのようにそれを ERAB セキュリティガイドラインの改定に取り組んでいくかを検討すべきと考えられる。近年の IoT に関する脅威動向として、IoT に対するマルウェア攻撃は、2022 年から 2023 年にかけて 4 倍に膨れ上がったことが Zscaler 社によって報告されている [17]ほか、個別のマルウェア事例としては、Telnet（23/TCP，2323/TCP）を狙う Mirai マルウェアが依然として猛威をふるっていることが情報通信研究機構（NICT）より報告されている [18]。このような増大する脅威に対して、各国政府は対策強化に向けた取組を進めており、例えば、米国においては 2021 年 5 月の大統領令で IoT 製品に対するラベリングプログラムの検討を指示し、2023 年 6 月に連邦通信委員会（FCC）を主体としたラベリングプログラム「U.S. Cyber Trust Mark」を 2024 年に開始予定と発表したほか、英国においては、消費者向け IoT 製品に対するセキュリティ対策を義務付ける Product Security and Telecommunication Infrastructure Act（PSTI 法）が 2024 年 4 月 29 日に施行予定である。さらに EU では、EU に上市されるデジタル製品（IoT 製品以外の OS、ソフトウェア等も含む。）に対するセキュリティ対策を義務付ける Cyber Resilience Act（CRA）が 2027 年中旬頃より適用が開始される予定である。国内でも、経済産業省を中心に IoT 製品に対する適合性評価制度の検討が進められている [19]ところ、このような動向を踏まえつつ、求められるセキュリティ対策を整理すべきと考えられる。

---

[17] Zscaler，2023 年版 Zscaler ThreatLabz エンタープライズ IoT 及び OT の脅威レポート
https://www.zscaler.jp/resources/2023-threatlabz-enterprise-iot-ot-threat-report

[18] 情報通信研究機構（NICT）、NICTER 観測レポート 2022 の公開 https://www.nict.go.jp/press/2023/02/14-1.html

[19] 経済産業省、ワーキンググループ 3（IoT 製品に対するセキュリティ適合性評価制度構築に向けた検討会）
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/index.html

現状の ERAB システムではゲートウェイによる対策が前提となっているが、今後ユーザーサイドの DER のリスクが増加することを踏まえると、ゲートウェイによる対策には限界がある。Matter 等のセキュリティ対策を考慮した新たな通信規格も登場しているところ、将来的なシステムのリスクを考慮した上で、求められるセキュリティ対策を整理することが重要である。また、IoT 製品のセキュリティ対策においては、セキュリティオペレーションセンター（SOC）等による監視・検知が重要となる。SOC の重要性はアグリゲーターに認知されつつあるものの、十分に実装が浸透していない現状である。よって、監視・検知に関する課題について、事業者と協力した検討を進めることが望ましい。

DER のセキュリティ対策に関連して、表 4-1 に示したコンテック社製品における事例では CVE-2022-29303 として CVE 番号が付与されたものの、電力分野に関連する IoT 関連製品の脆弱性情報は、取扱い件数がまだ少ない。また、製品やサポート情報の供給メカニズムが一般的なソフトウェア製品と異なる点もあり、メーカーから利用者まで情報が到達しにくいケースも散見される。よって、DER の脆弱性対応の高度化に向けて、脆弱性情報の共有や管理等のあり方についても整理することが望まれる。

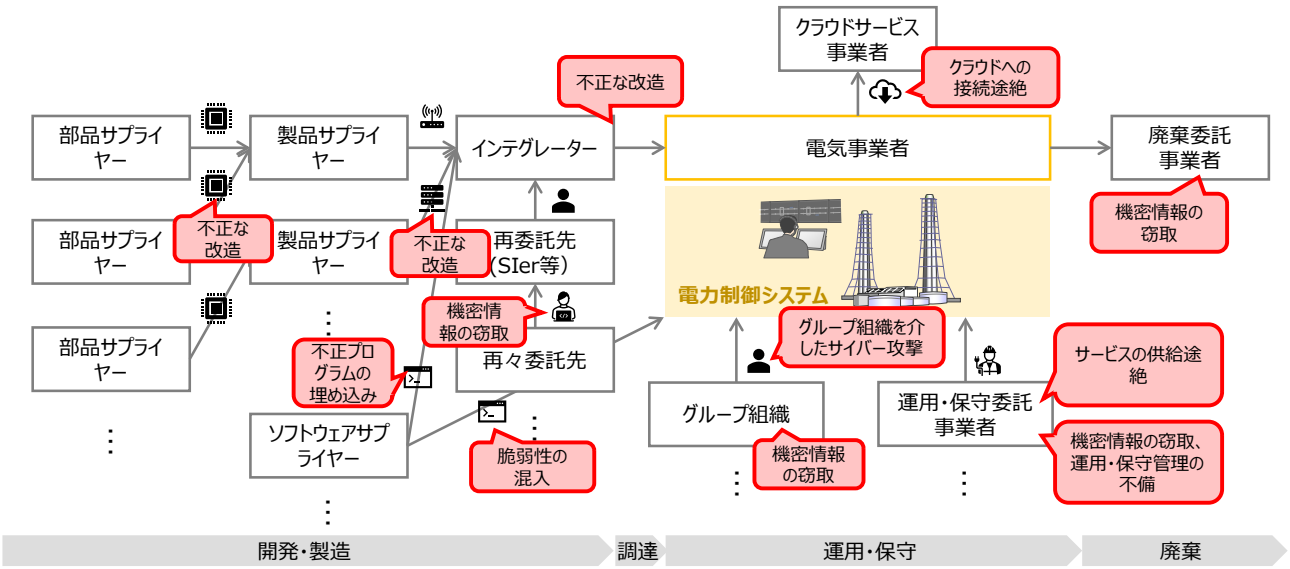
これらの検討を行った上で、既存ガイドラインへの影響や整合性等を確認しつつ、ERAB セキュリティガイドラインの改定に取り組んでいくかを検討すべきと考えられる。

### （3）アグリゲーターのセキュリティ対策の実態把握について

業界としてアグリゲーターのセキュリティ対策の実態把握をするために、前章で記載のとおり、広域機関の会員が提出するセキュリティリスク点検ツールの結果については、広域機関と資源エネルギー庁の間で連携していく予定である。点検結果の集計時期や連携される情報等について内容を確認の上、適切な施策を検討していく必要があると考えられる。

# 5. サプライチェーンセキュリティ対策の高度化に向けた検討

電力分野に限らず、産業用制御機器に関するサプライチェーン・リスクは高まりつつある中、サプライチェーンセキュリティ対策の高度化は喫緊の課題である。本事業では、国内のサプライチェーンセキュリティリスクの状況や海外の取組状況を踏まえ、昨今の電力制御システムに対する取組やガイドライン等と比較しながら、国内の電力事業者が行うべき内容についての議論・検討を行った。本事業では、NISC の定義を参照し、電気事業者へ電力制御システムが納入されるまでの開発や製造に係る一連の工程に加え、調達・運用・保守・廃棄を含むシステムライフサイクル全般のサプライチェーンにおけるサイバーセキュリティ上のリスク [20]を「サプライチェーン・リスク」と定義し、議論・検討を行った。電力制御システムに想定されるサプライチェーン・リスクの例は図 5-1 のようにマッピングされる。




出所）NISC「外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書等」[21]に基づき三菱総合研究所作成

図 5-1 電力制御システムに想定されるサプライチェーン・リスクの例

## 5.1 サプライチェーンセキュリティ脅威の動向

IPA（情報処理推進機構）が報告している 2024 年の情報セキュリティ 10 大脅威の中で、サプライチェーンへの攻撃が昨年度に引き続き 2 位に位置付けられたことは、サプライチェーンを経由したサイバー攻撃が依然として大きな懸念事項であることを示している。サプライチェーンにおけるサイバー攻撃は、特にサプライヤーが直接攻撃を受けた場合、サプライチェーン全体に深刻な影響を及ぼす可能性がある。具体的な事例として、表 2-2 の No.6 のケースでは、サプライチェーンの上流でソフトウェアが改ざんされ、その結果、下流の企業に広範な被害が発生している。

このようなサプライチェーンを通じた攻撃において注視すべき事項は、セキュリティリスクが組織外に

[20] 電力 SWG では、リスクを「サイバーセキュリティ基本法に定めるサイバーセキュリティを欠く可能性のうち、経営、人、技術又は取引によりもたらされるもの」として議論・検討した。
[21] https://www.nisc.go.jp/pdf/policy/general/risktaiou28.pdf

分散しているという点である。サプライチェーンは複数の組織やサプライヤーが連携する複雑なネットワークであり、一つの弱点が全体に影響を及ぼす可能性がある。そのため、サプライヤーとの綿密な連携やセキュリティポリシーの徹底が不可欠である。

## 5.2 電力分野のサプライチェーンセキュリティ対策の現状

電力 SWG では、第 2 回電力 SWG までの議論を取りまとめた提言である「電力制御システムのセキュリティ向上策に関する提言」[22]を平成 30 年に発表している。本提言では、電力分野で取り組むべきサイバーセキュリティ対策が示されており、その一つとして、サプライチェーン・リスクに対する対応も言及されているものの、サプライチェーン・リスクは中長期課題の一つとして位置付けられており、「関係者による引き続きの議論や検討を進めていくことが重要」という提言に留まっている。一方で、前節で示したとおり、サプライチェーン・リスクは年々高まりを見せている。電力分野におけるサプライチェーン・リスクに対し、海外の規制機関は既に取組を進めており、表 5-1 に示すとおり、罰則規定のある法規制において、事業者におけるサプライチェーン・リスク管理を明示的に求めている。

表 5-1 海外電力分野におけるサプライチェーン・リスクに関する規制状況

| 国・地域 | 米国 | ドイツ | 英国 | EU |
|---|---|---|---|---|
| 法規制 | • 連邦電力法 | • IT セキュリティ法 2.0<br>• エネルギー産業法<br>• BSI 法 | • NIS 規則<br>• 国家安全保障・投資法(NS&I Act) | • NIS 指令/NIS2 指令<br>• EU Regulation No. 2019/943 |
| 要件文書 | • NERC CIP-013: Cyber Security – Supply Chain Risk Management | • IT セキュリティカタログ(IT-Sicherheitskatalog) | • NIS Guidance<br>• Cyber Assessment Framework (CAF) | • EU 各国の国内法により規程<br>• Network Code on Cybersecurity |
| 所管組織 | • FERC(連邦エネルギー規制委員会)<br>• NERC(北米電力信頼度協議会) | • BSI(連邦情報セキュリティ庁)<br>• BMI(連邦内務省)<br>• BNetzA(連邦ネットワーク庁) | • NCSC(国家サイバーセキュリティセンター)<br>• Ofgem(ガス・電力市場局) | • EU 各国の所管省庁<br>• ENTSO-E |

[22] 電力 SWG、電力制御システムのセキュリティ向上策に関する提言
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/pdf/20181121001.pdf

| 国・地域 | 米国 | ドイツ | 英国 | EU |
|---|---|---|---|---|
| | | | • BEIS（ビジネス・エネルギー・産業戦略省） | |
| 電力会社に求められるサプライチェーン・リスク対策 | • サプライチェーン・リスク管理の実施<br>• サプライチェーン・リスク管理計画の定期的な見直し（少なくとも 15 ヶ月に一度）<br>• サプライチェーン・リスク管理状況の NERC への報告 | • サプライチェーン・リスク管理の実施<br>• 導入する重要部品に関する政府への事前通知・審査<br>• インシデント情報等に関する政府への報告 | • サプライチェーン・リスク管理の実施<br>• 対策状況に関する政府への定期的な報告<br>• サプライヤー契約に関する政府への通知<br>• 政府による調査・介入への協力 | • サプライチェーン・リスク管理の実施<br>• 人的サプライチェーンへの対策（産業スパイへの対策、企業秘密の保護など）<br>• 委託先や導入部品のサイバーセキュリティ対策の検証 |
| 罰則等 | • 違反度合いに応じた罰則規程 | • 最大 2,000 万ユーロ（約 30 億円）又は企業の全世界売上高の 4%のいずれか高い方の罰金 | • 最大 1,700 万ポンド（約 30 億円）の罰金 | • NIS2 指令では、最大 1,000 万ユーロ（約 15 億円）又は企業の全世界売上高の 2%のいずれか高い方の罰金 |

出所）各種公開情報に基づき三菱総合研究所作成

サプライチェーン・リスクに対する対応に向けては、国内でも様々な取組が進められてきた。2.2 で記載したとおり、2022 年に策定された「重要インフラのサイバーセキュリティに係る行動計画」において、サプライチェーン・リスク対応に関して、安全基準等策定指針の記載を充実させる方針が示されたほか、この方針を踏まえて 2023 年に策定した「重要インフラのサイバーセキュリティに係る安全基準等策定指針」では、サプライチェーン・リスクに関するリスクアセスメント・対応等が、重要インフラ分野に共通して求められるサイバーセキュリティ確保に向けた取組として明記された。また、2022 年 5 年に成立した経済安全保障推進法では、特定社会基盤事業者が特定重要設備の導入及び重要維持管理等の委託を行う場合、事業所管大臣の審査を受けなければならないとしており、電力分野では特定の基準を満たす 42 者が特定社会基盤事業者として指定され、特定重要設備の導入及び重要維持管理等の委託を行う場合、経済産業大臣による事前審査が必要となる。一方で、電力分野に絞ると、上記のとおり、これまでに十分な議論が行われているとは言えず、サプライチェーン・リスクに対する対応高度化に向けた取

組は必要不可欠と言える。事実、現状の「電力制御システムセキュリティガイドライン」では、委託先等の対応を求めているものの、明示的に「サプライチェーン・リスク」に関する言及は無く、サプライチェーン・リスクに対する対策を求めているわけではない。このような状況を踏まえ、電力制御システムに想定されるサプライチェーン・リスクに対応するために求められる対策を検討した。

## 5.3 電力分野におけるサプライチェーン・リスクに対する対応の検討

図 5-1で示した電力制御システムに想定されるサプライチェーン・リスクに対応するために、NISC安全基準等策定指針、経済安全保障推進法及び現行の電力制御システムセキュリティガイドラインの内容を踏まえ、以下のような対策を事業者に求めていくべきと考えられる。

表 5-2 電力制御システムにおいて求められるサプライチェーン・リスク対策(案)

| 項目 | 事業者に求めていくべきサプライチェーン・リスク対策(案) | 対応するサプライチェーン・リスク |
|---|---|---|
| サプライチェーン・リスク管理 | ・ 委託先等の対応に関して、電力制御システム等に関連する委託先等の役割と責任範囲を明確にする。<br>・ 電力制御システム等におけるサプライチェーンの依存関係及び委託先等のセキュリティ対策状況を把握する。<br>・ 電力制御システム等のサプライチェーン・リスクに関するリスク分析を行い、それに基づいた対策を講じるとともに、対策の状況を定期的に把握し、把握結果に基づき対策の見直しを検討する。 | ・ 全リスク |
| セキュリティ仕様の確認 | ・ 電力制御システム等のセキュリティ仕様に関して、電力制御システム等の調達時にセキュリティ仕様を発注仕様書等において明確にする。<br>・ 仕様への準拠性の確認に関して、電力制御システム等がセキュリティ仕様通りに設計、製造されていることを確認する。<br>・ 電力制御システム等の仕様変更に関して、セキュリティに影響を与える可能性がある変更を適切に管理する。 | ・ 開発・製造時の不正な改造<br>・ 開発・製造時の不正プログラムの埋め込み<br>・ 運用・保守時のソフトウェアの不正な更新 |
| 機器・外部記憶媒体の管理 | ・ 機器・外部記憶媒体の管理に関して、機器・外部記憶媒体を、システムライフサイクルを通じて管理し、保護する。 | ・ 調達時の不正な改造<br>・ 調達時の不正プログラムの埋め込み |

| 項目 | 事業者に求めていくべきサプライチェーン・リスク対策(案) | 対応するサプライチェーン・リスク |
|---|---|---|
| | | ・　廃棄時の機密情報の窃取 |

なお、サプライチェーン・リスクに関するリスク分析については、IPA の「制御システムのセキュリティリスク分析ガイド」[23]等を参照し、自組織の事業環境等を踏まえて適切な分析手法を選択又は相互補完的に組み合わせて分析することが想定される。また、対策状況の把握に当たっては、2023 年度に公開予定の「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」(本事業で開発したリスク点検ツールのこと。詳細は 3 章を参照。)等を活用することが想定される。

参考として、上記の「事業者に求めていくべきサプライチェーン・リスク対策(案)」について、現行の電力制御システムセキュリティガイドラインの記載内容との対比を以下に示す。

表 5-3 現行の電力制御システムセキュリティガイドラインの記載内容との対比

| 項目(案) | 事業者に求めていくべきサプライチェーン・リスク対策(案) | 現行の電力制御システムセキュリティガイドラインの記載事項 |
|---|---|---|
| サプライチェーン・リスク管理 | 委託先等の対応に関して、電力制御システム等に関連する委託先等の役割と責任範囲を明確にする。 | 【第 2-2 条 役割】<br>電力制御システム等に関連する委託先等の役割を明確にすること。 |
| | 電力制御システム等におけるサプライチェーンの依存関係及び委託先等のセキュリティ対策状況を把握すること。 | — |
| | 電力制御システム等のサプライチェーン・リスクに関するリスク分析を行い、それに基づいた対策を講じるとともに、対策の状況を定期的に把握し、把握結果に基づき対策の見直しを検討する。 | — |
| セキュリティ仕様の確認 | 電力制御システム等のセキュリティ仕様に関して、電力制御システム等の調達時にセキュリティ仕様を発注仕様書等において明確にする。 | 【第 6-1 条　セキュリティ仕様の確認】<br>1. セキュリティ仕様<br>電力制御システム等の調達時にセキュリティ仕様を明確にすることが望ましい。 |
| | 仕様への準拠性の確認に関して、電力制御システム等がセキュリティ仕様通りに設計、製造されていることを確認する。 | 【第 6-1 条　セキュリティ仕様の確認】<br>2. 準拠性の確認<br>電力制御システム等がセキュリティ仕様通りに設計、製造されていることを確認することが望ましい。 |
| | 電力制御システム等の仕様変更に関して、セキュリティに影響を与える可能性が | 【第 6-1 条　セキュリティ仕様の確認】<br>3. 仕様変更 |

[23] https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

| 項目(案) | 事業者に求めていくべきサプライチェーン・リスク対策(案) | 現行の電力制御システムセキュリティガイドラインの記載事項 |
|---|---|---|
| | ある変更を適切に管理する。 | セキュリティに影響を与える可能性がある変更を適切に管理することが望ましい。 |
| 機器・外部記憶媒体の管理 | 機器・外部記憶媒体の管理に関して、機器・外部記憶媒体を、システムライフサイクルを通じて管理し、保護する。 | 【第 6-2 条 機器・外部記憶媒体及びデータの管理】<br>1. 機器・外部記憶媒体の管理<br>機器・外部記憶媒体を管理し、保護することが望ましい。 |

日々高度化・複雑化するサプライチェーン・リスクに対応するため、「電力制御システムセキュリティガイドライン」の改訂に限らず、より中長期的な取組についても検討が望まれる。例えば、サプライチェーン・リスクの状況や事業者が抱える課題を踏まえ、サプライチェーン・リスク対応の高度化に向け、既存の取組等を活用し、事業者におけるサプライチェーン・リスク対応を支援する内容(例:委託先等を含むサプライチェーン・リスクの把握方法、リスクの管理方法等)を含んだ、より詳細な手引き文書等の策定が望まれる。

また、NISC の安全基準等策定指針において、サプライチェーン全体での対策実効性を高めることが言及されているところ、電力 ISAC、電気事業連合会等と連携し、事業者に閉じないサプライチェーン全体での教育・訓練の実施等の方策についても、検討を進めるべきと考えられる。

さらに、経済安全保障の観点を踏まえ、サイバーセキュリティ上のリスクだけでなく、物理的な妨害行為等のリスクも考慮した包括的な対策を検討することが望まれる。加えて、事業者がサプライチェーン・リスクに対応するために必要な情報を取得又は提供し、利用できるようにするための法的根拠を検討することが望まれる。これらの検討に当たっては、他分野との相互依存性を踏まえ、電力分野以外の動向も踏まえた検討が必要となる。

# 6. 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。

## 6.1 意見交換の実施

電力SWGの開催に先立ち、SWGの構成員それぞれに対して、以下の議題に関する意見交換を行った。

1. リスク点検ツール位置付け・普及促進の方針について
2. サプライチェーンセキュリティ対策の高度化に向けた検討について
3. アグリゲーターシステムや DER のセキュリティ確保に向けた検討について

リスク点検ツールの想定される位置付けについて、「①ツールに基づくリスク点検の要件化」、「②ツールに基づくリスク点検の努力義務化」、「③任意活用できるツールとして位置付け」の 3 つの位置付けを提示したところ、義務化は時期尚早であり、③→②→①の段階的な要求レベルの向上を検討すべきとの意見が多く挙げられた。また、闇雲に要求レベルの向上を目指すのではなく、各フェーズでの事業者の対応レベルやツールの浸透状況を踏まえて検討することの重要性が示唆された。リスク点検ツールの普及に当たっては、事業者におけるツール活用のインセンティブを明確化すべきとの意見が挙げられた。想定されるインセンティブとして、サイバー保険への適用や事故発生時の説明責任を果たす際に活用できうるとの意見がなされたほか、事業者の外部経済活動を支えるインセンティブを検討すべきとの意見が挙げられた。

サプライチェーンセキュリティ対策の高度化に向け、サプライチェーン・リスク管理を電気事業者に求めていく重要性が多くの委員より意見された。その上で、事業者が対応すべきリスクの明確化、サプライチェーンにおける脆弱性共有の仕組みの検討、調達基準の明確化、供給側との相互依存性の解析、インシデント発生後の影響緩和策の検討、責任分界点の明確化等に関する必要性が意見された。これらの検討に当たっては、電力制御システムのサプライヤーの意見を踏まえた検討や、中小企業の対応や課題を踏まえた検討が重要であるとの意見が挙げられた。

アグリゲーターシステムのセキュリティ確保について、ERAB セキュリティガイドラインで求められる詳細対策要件の策定が課題になりうるとの意見が挙げられた。ERAB システムは様々な接続形態が存在するところ、接続形態ごとのリスクを踏まえた検討の必要性が意見された。関連して、ERAB システムのリスク把握に当たって、本事業で開発したリスク点検ツールの活用を促すことが重要であるとの意見がなされた。DER のセキュリティ確保に関して、製品ベンダーに対してセキュリティ対策を訴求することの重要性が意見された。この訴求に関連して、ベンダーの対応状況を踏まえた検討の必要性が示唆された。また、別途検討されている IoT 適合性評価制度との連携の重要性が意見された。

## 6.2 第 16 回電力 SWG の運営

第 16 回電力 SWG では、大手電力事業者のサイバーセキュリティに係る取組、電力制御システムにおけるサプライチェーン・リスクに対する対応、アグリゲーター及び分散型エネルギー源（DER）のセキュリティ対策、電力分野におけるサイバーセキュリティリスク点検ツールについて議論が行われた。また、サイバー攻撃による被害に関する情報共有の促進に向けた検討について報告が行われた。

電力制御システムにおけるサプライチェーン・リスクに対する対応については、電力制御システムセキュリティガイドラインに対するサプライチェーンの要件に関する提言について議論された。アグリゲーター及び分散型エネルギー源（DER）のセキュリティ対策については、IoT 機器を含めたアグリゲーションシステム全体のセキュリティ対策について議論が行われた。電力分野におけるサイバーセキュリティリスク点検ツールについては、リスク点検ツールの正式公開後の普及促進策と今後の位置付けに議論が行われた。

産業サイバーセキュリティ研究会 WG1 電力 SWG（第 16 回）議事要旨

日時　：令和 6 年 2 月 1 日（木）9 時 30 分～12 時 00 分
出席者　：

| | | |
|---|---|---|
| （座長） | 渡辺 研司 | 名古屋工業大学大学院 |
| （委員） | 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 |
| | 門林 雄基 | 奈良先端科学技術大学院大学 |
| | 新 誠一 | 電気通信大学 |
| | 高見 穣 | 情報処理推進機構 |

議題

1. 大手電力事業者のサイバーセキュリティに係る取組について
2. 電力制御システムにおけるサプライチェーン・リスクに対する対応について
3. アグリゲーター及び分散型エネルギー源（DER）のセキュリティ対策について
4. 電力分野におけるサイバーセキュリティリスク点検ツールについて
5. サイバー攻撃による被害に関する情報共有の促進に向けた検討について

要旨

1. 大手電力事業者のサイバーセキュリティに係る取組について

（1）「大手電力事業者のサイバーセキュリティに係る取組について」を電気事業連合会より説明。

（2）自由討議

- サイバー環境の急激な変化を考慮し、ガイドラインの改訂周期を検討すべきである。
- ガイドラインに記載された事項の解釈の幅を狭め、遵守評価の基準を明確化するべきである。

2. 電力制御システムにおけるサプライチェーン・リスクに対する対応について

（1）「電力制御システムにおけるサプライチェーン・リスクに対する対応について」を事務局より説明。

（2）自由討論

- スピード感が重要であり、世界の動きに劣後しないことを前提に取組を進める必要がある。
- リスクの定義が現場での作業において重要であり、ガイドラインや提言においても明確な定義が求められる。また、リスク把握の手法が複数ある中で、リスク点検ツールの使用が有効であることを提言するべきである。
- サプライチェーン・リスクへの対応に当たっては、発注仕様書の記載方法と納品検査の方法が重要である。また、異なる業界間のガイドラインの整合性確保が課題であり、全ての重要インフラに共通の基本対策と電力分野における特異事項を整理されたい。
- 経済安全保障推進法の文脈では、サイバーとフィジカル両面のリスクに対する対策が必要である。
- 提言におけるセキュリティ管理に関する記載について、より詳細に、リスク分析を行うこと及びそれに基づいた対策を講じることに言及すべきである。
- 「ライフサイクル」という用語は「システムライフサイクル」と修正すべきである。
- 複数分野に跨るベースの基準を整備した上で、電力分野特有の要素を検討するべきである。この取組は、整合性の確保に留まらず、国全体のセキュリティ確保につながる。
- 国においては、サプライチェーンにおける利害関係者が、必要な情報を取得又は提供し、利用することができる法的根拠を明らかにする措置を講じるべきである。

3. アグリゲーター及び分散型エネルギー源（DER）のセキュリティ対策について

（1）「日本における ERAB システムに関するセキュリティ対策実践」を慶應義塾大学梅嶋准教授より説明。

（2）「アグリゲーター及び分散型エネルギー源（DER）のセキュリティ対策について」を事務局より説明。

（3）自由討論

- アグリゲーターや DER の進展において、ゼロトラスト・セキュリティの意識が重要であり、末端におけるリスク最小化が鍵である。
- ゲートウェイに基づくセキュリティ対策は過渡的な対策である。将来的に導入される機器に対して、ゼロトラストの観点も踏まえて適切に対策を行うこと、リスクを把握した上でシステム構築を進めることが重要である。
- IoT 製品の運用には、セキュリティオペレーションセンター（SOC）による監視が重要であり、SOC についても言及すべきである。
- ガイドライン上の文言において、対策の実施主体は明確にすべきである。
- 国外制度と本ガイドラインのアグリゲーターに対する要件の差異が懸念され、事業者視点からの検討での受容性向上が期待される。

・ DER のセキュリティ対策においては、経済産業省で別途検討されている IoT 製品に対するセキュリティ適合性評価制度と整合性が確保されることが望ましい。

4. 電力分野におけるサイバーセキュリティリスク点検ツールについて

(1)「電力分野におけるサイバーセキュリティリスク点検ツールについて」を事務局より説明。

(2)自由討論

・ 広くツールが利用されるよう、ツールの提供形式を検討すべきである。
・ リスク点検結果を踏まえ、事業者の依存関係や弱点などが自動的に解析されることが望ましい。また、専門的な内容も含まれるため、回答者の負担軽減を考慮したツールとする必要がある。
・ ツールにおいて、リスク点検実施者の氏名と保有資格を記入する欄を設けることが望まれる。その上で、公的支援を検討する場合は、適切な資格保有者に対する支援に限定することが妥当である。
・ 税制や経費に関する優遇策が重要であり、認証実施主体の能力確保、責任強化及び慎重な認定者の選定が不可欠である。第三者認証以外では、組織内人材育成と外部向け能力発信の仕組みの検討が重要である。

5. サイバー攻撃による被害に関する情報共有の促進に向けた検討について

(1)「サイバー攻撃による被害に関する情報共有の促進に向けた検討について」を経済産業省サイバーセキュリティ課より説明。

# 7. 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、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・検討を進めた。具体的には、国内外の電力サイバーセキュリティに関する実態調査・分析を行うとともに、リスク点検ツールの試行利用を行い、正式公開に向けた取組を進めた。加えて、分散型エネルギーリソースに係るセキュリティ対策やサプライチェーンセキュリティ対策の高度化に向けた検討を進めた。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。

電力分野のサイバーセキュリティに関する継続的な取組を推進するために、今後、以下に示す取組について検討することが望まれる。

## 7.1 取組①:リスク点検ツールを活用した電力システムのリスク把握

3.3 に示すとおり、今後はリスク点検ツールについて広域機関と連携して普及展開するとともに、関連団体や業界と連携して周知を行うことが望まれる。また、電力 SWG 等で確認したとおり、広域機関から共有される会員企業の自己点検のデータを分析し、その結果を基に今後の施策を検討することが望まれる。広域機関との取組については表 7-1 に示すような課題仮説を基に分析ができると良い。確認できた課題を基に、リスク点検ツールの要求レベル向上やインセンティブを検討することが望まれる。確認できた課題によっては、リスク点検ツール以外の取組の検討も求められる。

表 7-1 自己点検のデータ分析の観点例

| 課題仮説 | 検討される分析内容 |
|---|---|
| 電力システムに多大な影響を及ぼす電気事業者(重要な電気事業者)においても、セキュリティ対策が不十分な企業が多い。 | ・ 事業規模・発電容量・事業区分ごとにリスク点検のスコアを比較し、重要な電気事業者を特定し不十分なセキュリティ対策に対する支援策を検討する。 |
| 中小事業者が多い事業区分において、自己診断への回答率が低く、リスク点検ツールが普及していない。 | ・ 小売電気事業者や特定卸供給事業者などの比較的中小事業者が多い業界における自己診断の取組の回答率を確認し、リスク点検ツールの利用を促進するための支援策を検討する。 |
| 電気事業者全体においてリスクがあり、電気事業者に対して強く実施を訴求すべきセキュリティ対策がある。 | ・ 電気事業者全体でリスク点検ツールの特定のカテゴリーやサブカテゴリーのスコアに差異があるかを確認し、該当対策の促進に向けた支援策を検討する。 |
| 事業区分ごとにリスクがあり、事業区分に応じたセキュリティ対策の支援策を検討する必要がある。 | ・ 事業区分ごとに、リスク点検ツールの特定のカテゴリーやサブカテゴリーのスコアに差異があるかを確認し、事業区分に応じた効果的なセキュリティ対策の支援策を検討する。 |

## 7.2 取組②：分散型エネルギーリソースに係るセキュリティ対策の高度化に向けた検討

4.4 に記載のとおり、分散型エネルギーリソースのセキュリティ対策の高度化に向けては、詳細対策要件の作成・確認に係る支援を講じるほか、末端の DER 設備に対する対策を検討することが望まれる。前者については、詳細対策要件の作成に当たって参考となる考え方の整理や ERAB に参画する事業者が相談できる体制の整備等が想定される。後者については、国内外の既存の動向を踏まえ、DER 設備に求められるセキュリティ対策を整理するとともに、末端 DER 設備における脆弱性情報の管理方法について、そのあり方を整理することが望まれる。これらの整理に当たっては、現状の ERAB システムの構成ではなく、将来的なシステム構成を見据えた整理が必要となる。そして、以上の検討を行った上で、ERAB セキュリティガイドラインの改定に取り組んでいくかを検討すべきと考えられる。ガイドラインの改定に当たっては、次世代の分散型電力システムに関する検討会等、既存の座組等を活用し、有識者や事業者の議論を踏まえた改定が重要となる。また、事業者の課題を聴取し、具体的な高度化策を検討する上では、エネルギーリソースアグリゲーション事業協会（ERA）等の事業者団体と連携した取組を進めることが重要となる。

## 7.3 取組③：サプライチェーンセキュリティ対策の高度化に向けた検討

日々高度化・複雑化するサプライチェーン・リスクに対応するため、5.3 に記載のとおり、事業者におけるサプライチェーン・リスク対応を支援する内容を含んだ、より詳細な手引き文書等の策定が望まれる。関連する取組として、米国では、セキュアな電力システムの調達に係るガイドライン [24]や太陽光発電のサプライチェーン対策に関する推奨事項をまとめた文書 [25]等が政府関係機関より発表されている。国内で策定する文書については、国内電気事業者の課題や商慣習等を踏まえ、委託先等を含むサプライチェーン・リスクの把握方法、リスクの管理方法等のより詳細な内容を含む文書とすることが望まれる。当該文書の策定に当たっては、既存の取組を踏まえつつ、電力 ISAC、電気事業連合会等と連携した検討が必要となる。このために、電力 SWG 配下に別途作業部会を設置し、実務者による具体的な議論を行うことが望まれる。

[24] NERC, Security Guideline -Product Security Sourcing Guide-
https://www.nerc.com/comm/RSTC Reliability Guidelines/Product%20Security%20Sourcing%20Guide.pdf
[25] NREL, Supply Chain Cybersecurity Recommendations for Solar Photovoltaics,
https://www.nrel.gov/docs/fy23osti/87135.pdf

令和 5 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向上に向けた調査）

2024 年 2 月

株式会社三菱総合研究所
先進技術・セキュリティ事業本部
TEL (03)6858-3578

（様式２）

# 二次利用未承諾リスト

令和５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向上に向けた調査）報告書

令和５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向上に向けた調査）

株式会社三菱総合研究所

| 頁 | 図表番号 | タイトル |
|---|---|---|
| 26 | 図2-3 | EBIOSのコンプライアンスとシナリオの位置付け |
| 26 | 図2-4 | EBIOSの全体像 |
| 27 | 図2-5 | ワークショップ間の関係 |
| 49 | 図4-5 | インターネット回線を活用する場合、必要なセキュリティを確保するための技術仕様書への記載例 |

# 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

令和６年●月

資源エネルギー庁　電力・ガス事業部
電力産業・市場室

目次

## 1. 背景と目的

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いる。重要インフラたる電力分野においてもサイバー攻撃の事案は増加傾向にあり、国内外問わず、電力会社を標的としたサイバー攻撃が発生している。電力系統へのサイバー攻撃が発生した場合、電気の安定供給に重大な支障を来すことが想定されるところ、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る。

経済産業省・資源エネルギー庁や業界団体は、電力会社におけるサイバーセキュリティ向上の取組に向け、これまで複数のガイドライン等を発表してきた。ガイドライン等の整備により電力会社におけるサイバーセキュリティ対策の取組は進みつつある一方で、サイバーセキュリティの脅威は日々進化・巧妙化している状況を踏まえると、現状の対策で十分ということは決してなく、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、資源エネルギー庁が実施した調査によると、対策を実施している事業者の割合と比較して、定期的なセキュリティリスクの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。セキュリティのリスク点検を定期的に実施しない場合、残存リスクを正しく把握することができず、適切な対策が施されない可能性がある。また、対策の継続的改善が実施されないことで、日々進化・巧妙化するサイバー脅威に対応できず、攻撃を受け、電力供給や事業継続に甚大な影響を及ぼす可能性がある。

この現状を鑑み、定期的なリスク点検を実施できていない電力会社を主な対象として、過大なコストをかけずに簡易的にリスク点検ができるよう、「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」（本ガイド）及びガイドに付属する「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）を開発した。日々進化・巧妙化するサイバー脅威に対抗するために、本ガイド及び対策状況可視化ツールを用いて自社の対策実施状況を合理的かつ効率的に点検・確認するとともに、点検結果に基づき、セキュリティ対策の見直し・改善を行うことで、対策の継続的改善を図ることが期待される。

**コラム：国内における電力分野のセキュリティ対策に関するガイドライン等**

2022 年現在、国内における電力分野のセキュリティ対策に関する文書として以下に示す文書が発表されているとおり、電力分野に関する様々なプレーヤーに対して、求められる対策が整備されつつあることが分かる。本ガイド及び付属する対策状況可視化ツールでは、各対策要求事項に対して、一部のガイドラインに記載された項目との対応関係も示している。各ガイドライン等で求められる対策については、それぞれの文書を参照いただきたい。

| 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。 |
| **特定卸供給に係るサイバーセキュリティ確保の指針** (2022年4月制定) | 特定卸供給事業に関するシステム | 資源エネルギー庁 | 特定卸供給事業を実施する上で確保すべきサイバーセキュリティとその対策の内容を示すことを目的とした指針で、特定卸供給事業の届出の際に、本指針に基づく対策実施状況を記載する必要がある。 |

**コラム：電力分野に対する近年のサイバー脅威事例**

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、国内外の電力会社が悪意あるサイバー脅威の対象となっている。以下にいくつかのサイバー脅威事例を示す。特に近年ではランサムウェア攻撃が増加傾向にあり、システムの停止やデータ漏えいにつながった事例も確認できる。

事例①：ランサムウェア感染による電力供給の停止（南アフリカ・小売電気事業者）

2019 年 7 月、南アフリカの小売電気事業者の情報システムがランサムウェア攻撃を受け、データの暗号化やサービスの停止に至った。プリペイド式電力供給サービスも停止したことで、料金の支払いを行うことが必要な一部の需要家への電力供給がなされず、25 万を超える需要家において停電が発生した。

事例②：会員制 Web サービスへの不正アクセス（日本・小売電気事業者）

2019 年 12 月、国内の小売電気事業者の会員制 Web サービスに対して、第三者からの大量の不正アクセスが発生し、105 名の会員が不正にログインされた。105 名のうち 44 名が不正なポイント交換の被害を受け、その被害額は、約 14 万円相当に及んだ。

事例③：モバイルサービスに対する不正アクセスによるデータ漏えい（英国・小売電気事業者）

2021 年 2 月、イギリスの大手小売電気事業者が提供するモバイルアプリケーションサービスが不正アクセスを受け、一部の顧客の個人情報や銀行口座情報が流出した。

事例④：サイバー攻撃によるシステムの停止・データの破損（米国・発電事業者／配電事業者）

2021 年 11 月、米国コロラド州の配電事業者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。

事例⑤：ランサムウェア攻撃によるデータ漏えい（日本・小売電気事業者）

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、顧客の個人情報・法人情報、取引先の情報等が流出した可能性が報告された。ただし、2022 年 11 月時点で、侵害された情報に関して一般には公開されておらず不正利用につながる形跡はないことが確認された。

事例⑥：ランサムウェア攻撃によるデータ漏えい（ルクセンブルク・発電事業者）

2022 年 7 月、ルクセンブルクに拠点を置く発電事業者がランサムウェア攻撃を受けた。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。

事例⑦：ランサムウェア攻撃によるデータ漏えい（インド・発電事業者等）

2022 年 10 月、インドの大手電力会社がランサムウェア攻撃を受けた。攻撃グループは、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えいさせており、漏えい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. 本ガイド・対策状況可視化ツールの対象

本ガイド及び対策状況可視化ツールは、主に以下の 4 つの事業区分の電力会社（電力の供給等を担う会社）及び当該企業が保有する電力制御システム・IT システムを対象としたリスク点検ツールである。

1. 発電事業者
2. 小売電気事業者
3. 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）
4. 自家用電気工作物設備設置者

これらの事業区分に該当する電力会社の中でも、特に、定期的なリスク点検を現状で実施できていない企業において、本ガイド及び対策状況可視化ツールを活用したリスク点検を実施することが推奨される。定期的なリスク点検を既に実施している企業においても、リスク点検実施にあたってのコスト、知識、期間等に課題に感じている企業は、本ガイド及び対策状況可視化ツールを是非活用いただきたい。なお、対策状況可視化ツールは、電力広域的運営推進機関（OCCTO）が会員企業に対して定期的に実施を促すセキュリティ自己診断に対しても活用できる。具体的には、OCCTO からセキュリティ自己診断の依頼があった場合に、本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 OCCTO に提出することができる。

## 3. 本ガイド・対策状況可視化ツールの想定活用方法

本ガイド及び対策状況可視化ツールの活用方法として、以下の活用方法が想定される。

- セキュリティ対策状況の点検・改善に向けた活用：
  本ガイド及び対策状況可視化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、対策状況の可視化結果を踏まえ、どのような追加対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：
  本ガイド及び対策状況可視化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。
- OCCTO 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 OCCTO 等の外部関係者に報告する際、対策状況可視化ツールの可視化結果を用いて報告することができる。

# 4. 本ガイド・対策状況可視化ツールに基づくリスク点検の進め方

## 4.1. 本ガイド・対策状況可視化ツールの構成

本ガイド及び対策状況可視化ツールの構成は図 4-1 に示すとおりである。以降では、本ガイド及び対策状況可視化ツールを活用したリスク点検の進め方について説明するとともに、リスク点検を踏まえた対策の改善方針及び具体的なリスク点検項目を示す。対策状況可視化ツールでは、各リスク点検項目に対して電力会社が対策状況を入力することで、どのような対策が実施できているか／不足しているかを可視化・確認することができる。

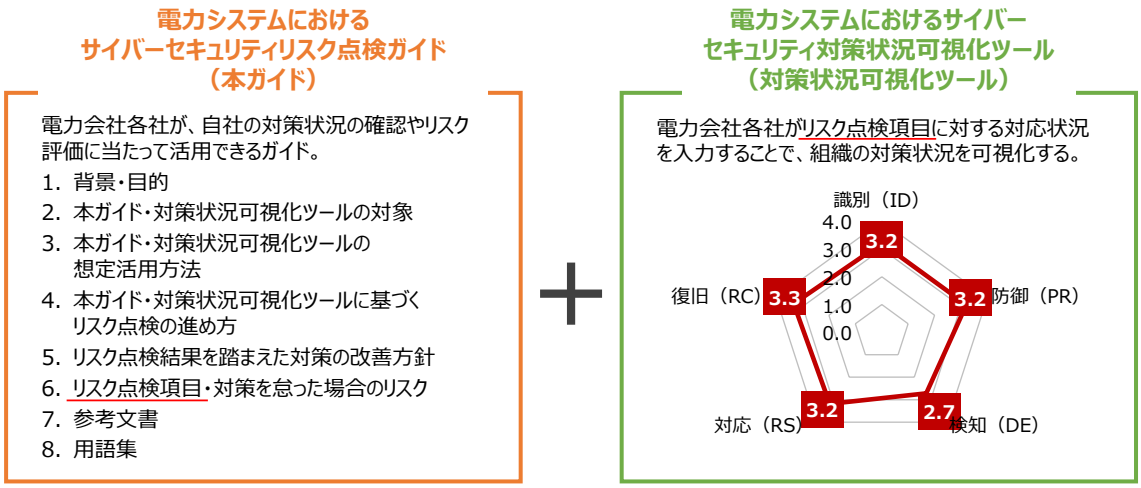



**図 4-1 本ガイド及び対策状況可視化ツールの構成**

本ガイド及び対策状況可視化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 を参考に整理している。NIST CSF はサイバーセキュリティマネジメントの枠組みを定めたフレームワークであり、業種、組織規模、リスク状況、セキュリティ対策の複雑さ等に依存せず、どのような組織においても活用可能である。事実、重要インフラ事業者に限らず官公庁や一般企業でも活用されているほか、諸外国でも認知・評価が高く、セキュリティ対策におけるグローバル・スタンダードになりつつある。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。本ガイド及び対策状況可視化ツールでは、108 のサブカテゴリーをリスク点検項目として設定している。なお、リスク点検項目は情報処理推進機構（IPA）が公開する日本語翻訳版 [1]に基づく内容であるが、それぞれのリスク点検項目に関

[1] https://www.ipa.go.jp/files/000071204.pdf

する補足説明を括弧書きで記載しているため、併せて参照いただきたい。

具体的なリスク点検項目及び各点検項目に関連する対策を怠った場合のリスクの一覧は、第 6 章に示す。

## 4.2. リスク点検の全体プロセス

本ガイド・対策状況可視化ツールを用いたリスク点検の全体プロセス概要を図 4-2 に示す。本図に示すとおり、リスク点検のプロセスは準備、実施、結果を踏まえた改善検討の大きく 3 つのフェーズに分かれる。以降では、各フェーズにおける実施内容について詳細に記載する。なお、図 4-2 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、一部の事項について経営層に報告することが望まれる。

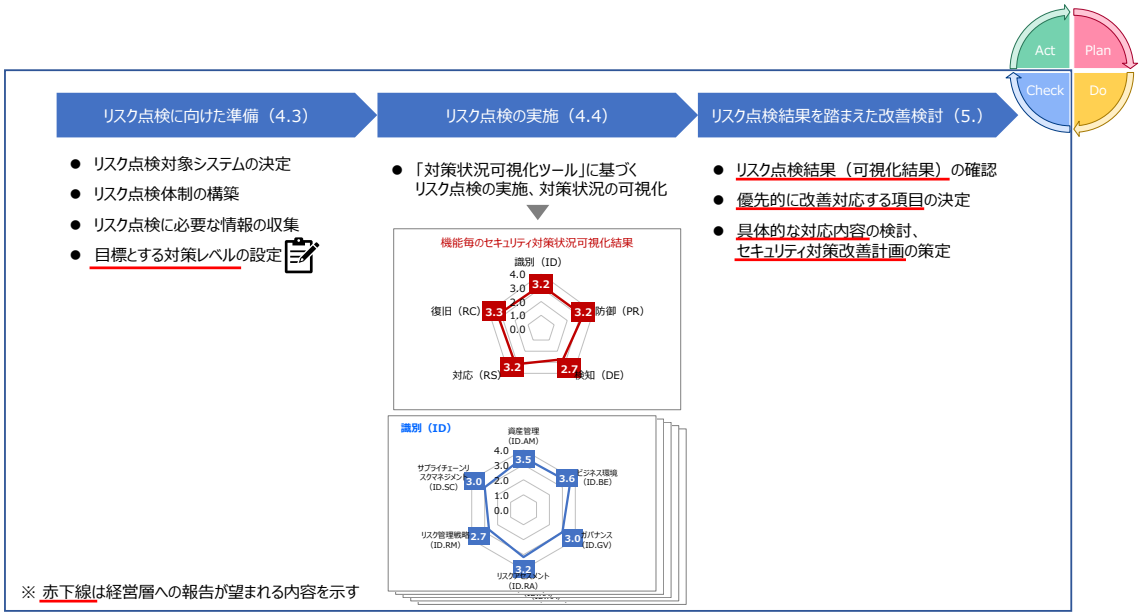



**図 4-2 リスク点検の全体プロセス概要**

## 4.3. リスク点検に向けた準備

本ガイド及び対策状況可視化ツールを用いたリスク点検に向け、体制整備、必要な情報の収集、目標レベルの設定等の準備が必要となる。初めてのリスク点検であるか、二回目以降のリスク点検であるかによって必要な準備は異なり、二回目以降のリスク点検の場合、初回のリスク点検で活用した情報に基づいた効率的なリスク点検が実施可能となる。

リスク点検にあたっては、まず、リスク点検の対象システムを決定する必要がある。社内のすべてのシステムに対してリスク点検を実施するには膨大な工数がかかるため、優先度をつけた上で、対象システムを選定することが望まれる。対象システムの選定にあたっては、「電力制御システムセキュリティガイドライン」や「ERAB に関するサイバーセキュリティガイドライン Ver 2.0」における重要度の定義、社内のセキュリティ対策方針、対策の実施状況、対象システムに対する脅威の状況、前回のリスク点検の結果等を総合的に勘案して踏まえ、決定することが望まれる。

リスク点検の実施に向け、次に対象システムに関する知識を有した担当者（主担当）を選定することが望まれる。主担当が中心となりリスク点検を推進するが、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。具体的には、経営層、社内セキュリティ関係部署、人事関係部署、リスク管理・法務関係部署、購買・調達関係部署等と連携し、リスク点検にあたって必要な情報を確認しつつ、リスク点検を進めることが必要である。また、リスク点検結果については、経営層に報告し、自社が抱えるセキュリティリスクの現状について、改善計画と合わせて伝えることが望まれる。リスク点検の実施にあたってはサイバーセキュリティに関する知識も求められるところ、IPA「情報セキュリティマネジメント試験」合格者相当の知識を有した主担当がリスク点検を主導することが推奨される。重要なシステムに対する精緻なリスク点検を行い、セキュリティ対策の見直し・改善を行う場合には、より高いスキルレベルを求める「情報処理安全確保支援士」相当の知識を有した主担当がリスク点検を主導するこが望まれる。

自社のセキュリティ対策に関する継続的改善につなげるために、リスク点検の実施に先立ち、自社が目標とする対策レベルを設定する必要がある。目標とする対策レベルは、リスク点検実施前に経営層に報告することが望ましい。本ガイド・対策状況可視化ツールでは、NIST CSF の評価基準であるティアと同様に、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ている。具体的には、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ている。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ている。

- 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。

本達成基準を参考にしつつ、自社が目標とする対策レベルを設定することが望まれる。対策状況可視化ツールでは、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）の対策レベルの平均値と、各機能のカテゴリーごとの対策レベルの平均値とが、レーダーチャートとして可視化される。目標値の定め方や具体的な目標値は社内のセキュリティ対策方針、対策の実施状況、対象システムに対する脅威の状況、前回のリスク点検の結果等を踏まえて検討すべきであり、例えば、ガイドラインで求められる対策項目と関係するリスク点検項目はすべて 1 以上の対策レベルになること、すべてのカテゴリーの平均値が 2.5 以上になること、すべてのリスク点検項目について前回のリスク点検結果以上の対策レベルになること等の目標が想定される。なお、達成基準は一つの例として示しているため、社内の状況に応じて具体的な内容を修正して構わない。

## 4.4. リスク点検の実施

リスク点検は、本ガイドに付随する対策状況可視化ツールを用いて行う。対策状況可視化ツールは、主に「使い方」、「チェックシート」、「可視化結果」、「可視化結果（広域機関用）」の 4 つのシートで構成される。対策状況可視化ツールは、リスク点検項目のフィルタリングのためにマクロを利用しているため、図 4-3 を参考に、マクロを有効化したうえで活用することが必要である。


**図 4-3 マクロ実行の方法**

「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」及びのシートに表示される。「チェックシート」の概要を図 4-4 に示すとおりであり、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 4-4 において赤枠で囲っている箇所）

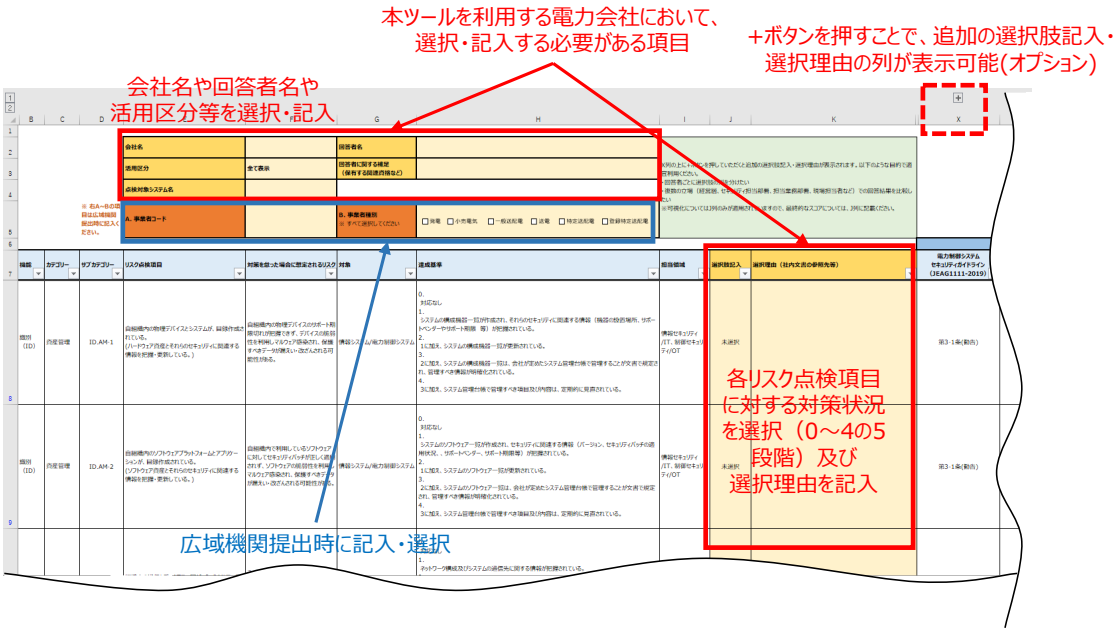



**図 4-4 対策状況可視化ツールの「チェックシート」の概要**

「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に関する列が存在する。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ている。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 領域を設定しており、これらの関連する領域の部署と連携しつつ、リスク点検を進めることが望ましい。

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ている。本ツールでは、以下のガイドラインとの対応関係を示している。

- 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

本ツールを活用する電力会社は、リスク点検項目に対する対策状況を選択する前に、まず「活用区分」を選択いただきたい。「活用区分」はプルダウン形式となっており、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。「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されて表示される。そのため、各電力会社は、「活用区分」を選択することで、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 OCCTO 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。また、「広域機関提出用」は基礎的なセキュリティ点検項目のみが表示されるため、事業規模やリスク点検の経験によっては「広域機関提出用」を選択し、基礎的なリスク点検を実施することも可能である。（この活用方法の場合、「広域機関用」の項目は対象外として問題ない。）

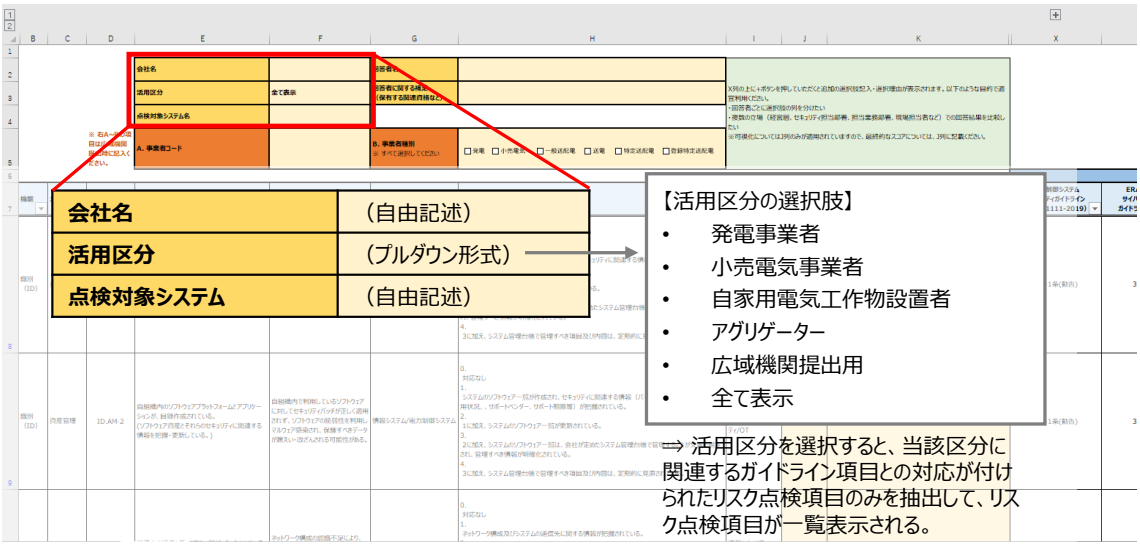



**図 4-5 対策状況可視化ツールの「チェックシート」における「活用区分」の位置づけ**

「活用区分」を選択後に抽出された各リスク点検項目について、図 4-4 に示すとおり、0～4 の 5 段階で、対策状況（対策レベル）の選択が必要となる。対策状況の選択にあたっては、各リスク点検項目に対する達成基準を参照し、自社の対策状況に最も近い対策状況を選択する。対策レベルについて、NIST CSF のティアの考え方と同様に各対策に関する成熟度を重要視しており、低いレベルは各対策の運用状況、高いレベルは各対策の改善に向けた制度構築状況を主に確認している。対策レベル

の選択にあたっては、必要に応じて関係部署に確認することが望まれる。また、他者が選択理由を確認・レビューする可能性を踏まえ、選択理由を記載することが望まれる。記載の際には、二回目以降のリスク点検を効率的に進めるために、リスク点検にあたって活用した社内文書等の情報も合わせて明記することが望まれる。この際、記載の省力化のために、リスク点検項目に関連した社内文書の内容を転記することや、社内文書の該当項目番号を記載することも想定される。また、X 列上部の＋ボタンを押すことで、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。これは、回答者ごとに選択肢の列を分けたい場合や複数の立場（経営層、セキュリティ担当部署、担当業務部署、現場担当者など）の結果を比較したい場合に活用いただきたい。

抽出されたすべ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。図 4-6 に示すとおり、対策状況可視化は 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示される。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選択（0～4 の 5 段階）の平均値である。可視化された結果を踏まえ、自社の対策実施状況を確認するとともに、可視化結果に基づきセキュリティ対策の見直し・改善を行うことで、対策の継続的改善を図ることが期待される。現状の対策状況を踏まえた効果的な対策改善を行うために、可視化結果は経営層に報告することが望まれる。

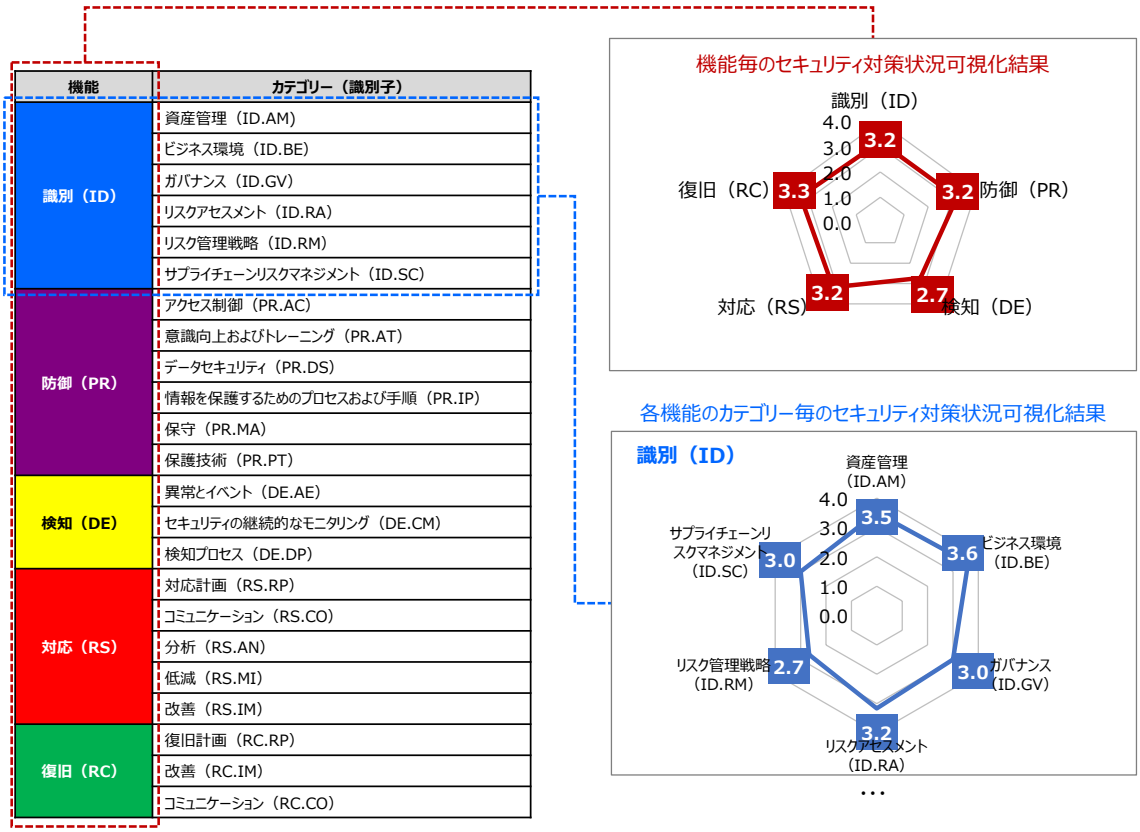



**図 4-6 NIST CSF の機能・カテゴリーと対策状況可視化結果の関係**

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 OCCTO に提出する場合について、OCCTO 提出用の可視化結果は「可視化結果（広域機関用）」のシートに表示される。このシートでは、OCCTO が定めた 12 のチェック項目に基づき平均スコアを算出・可視化している。可視化結果のイメージは図 4-7 に示すとおりである。

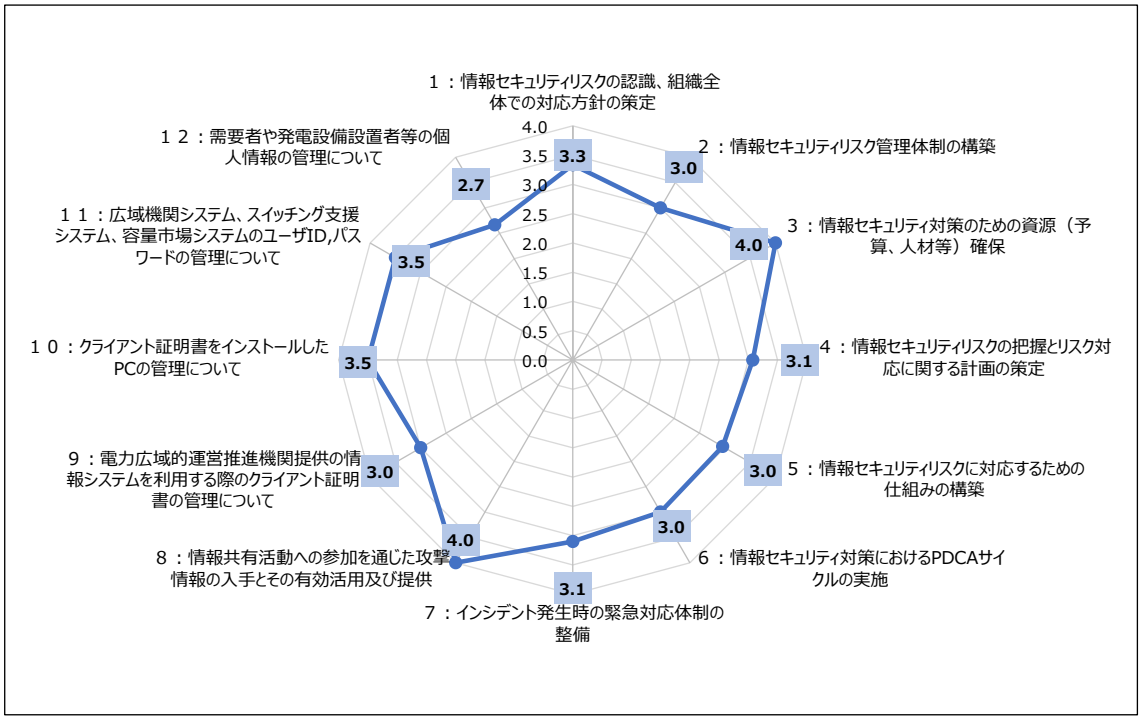



**図 4-7「可視化結果（広域機関用）」シートにおける対策状況可視化結果例**

## 5.リスク点検結果を踏まえた対策の改善方針

リスク点検結果を踏まえ、システムに対するセキュリティ対策の改善計画を講じ、当該計画に基づいて対策の改善を実施することで、PDCA サイクルに基づくセキュリティ対策の計画・実施・点検・改善のプロセスを実行することが求められる。リスク点検結果を踏まえた対策改善の基本的な考え方として、選択した対策状況の数値が低いリスク点検項目の方が十分なセキュリティ対策が講じられておらず、当該リスクに対する改善対応を優先的に検討する必要がある。ただし、本ガイド・対策状況可視化ツールのリスク点検項目は広範であり、一つの項目における対策状況の数値が低い場合でも、関連する他の項目で十分な対策ができている場合、想定されるリスクが顕在化しない場合もある。そのため、個々のリスク点検項目による評価ではなく、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の可視化結果を踏まえ、改善検討を行う方針も想定される。いずれの方針であっても、対応する人員や予算は限られているため、現実的な工数で改善を実施するために、優先的に改善する項目をまず選定する必要がある。

優先的に改善する項目の選択について、一つの考え方として、リスク点検実施前に設定した目標値とリスク点検結果とが大きく乖離している項目について優先的に改善する方針がある。ほかにも、関連ガイドラインの「勧告的事項」と関連するリスク点検項目のうち、対策状況の数値が低いリスク点検項目について優先的に改善する方針が想定される。加えて、ガイドラインの要求事項等に依らず、対応が実施されていない「0」の対策状況である項目について、優先的に改善を行う方針も考えられる。対策の改善は事業者全体の損失に影響する問題であるため、経営層を含めた協議によって、優先的に改善する項目を決定することが望ましい。なお、改善対応にかかるコストや期間も重要となるところ、後述するリスク低減方針を検討した上で経営層と協議することが望まれる。

優先的に改善対応する項目が決まった後、具体的な対応を検討する必要がある。一般的に、リスク対応の手法は、リスク回避、リスク低減、リスク移転、リスク保有の大きく 4 つに区別されるが、本ガイドではリスク低減の方針について記載する。対応検討にあたっては、改善対応する項目について、現状の対策レベルの次の達成基準でどのような対策が求められているかを確認するとともに、当該項目に関連するガイドラインの要求事項を確認した上で、具体的な対応策を検討する必要がある。具体的な対策の検討にあたっては、当該項目に関連するガイドラインの要求事項のほか、経済産業省の「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）」[2]が参考となる。CPSF では、産業社会を 3 つの層で捉え、各層における対策要件等を整理しているほか、添付 C では、各対策要件に対する具体的な対策例が記載されている。

優先的に改善対応するリスク点検項目に対し、CPSF を用いた対策例の検討イメージを図 5-1 に示す。CPSF の添付 D では、CPSF の対策要件と NIST CSF との対策要件の関係性が示されているため、まず改善対応する項目のサブカテゴリー（対策要件 ID）に対応する CPSF の対策要件を逆引きすることが効率的である。その後、CPSF の添付 C を用いて、具体的な対策例を検討する。CPSF の

[2] https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html

添付 C で記載されている対策例は、対策を導入・運用する際のコストや対策の対象範囲を踏まえ、Basic、Advanced、High-Advanced の 3 レベルに分かれている。改善対応にかかるコストや期間も重要となるところ、現状の対策レベル及び費用対効果を踏まえて、適切な対策を選定することが望まれる。

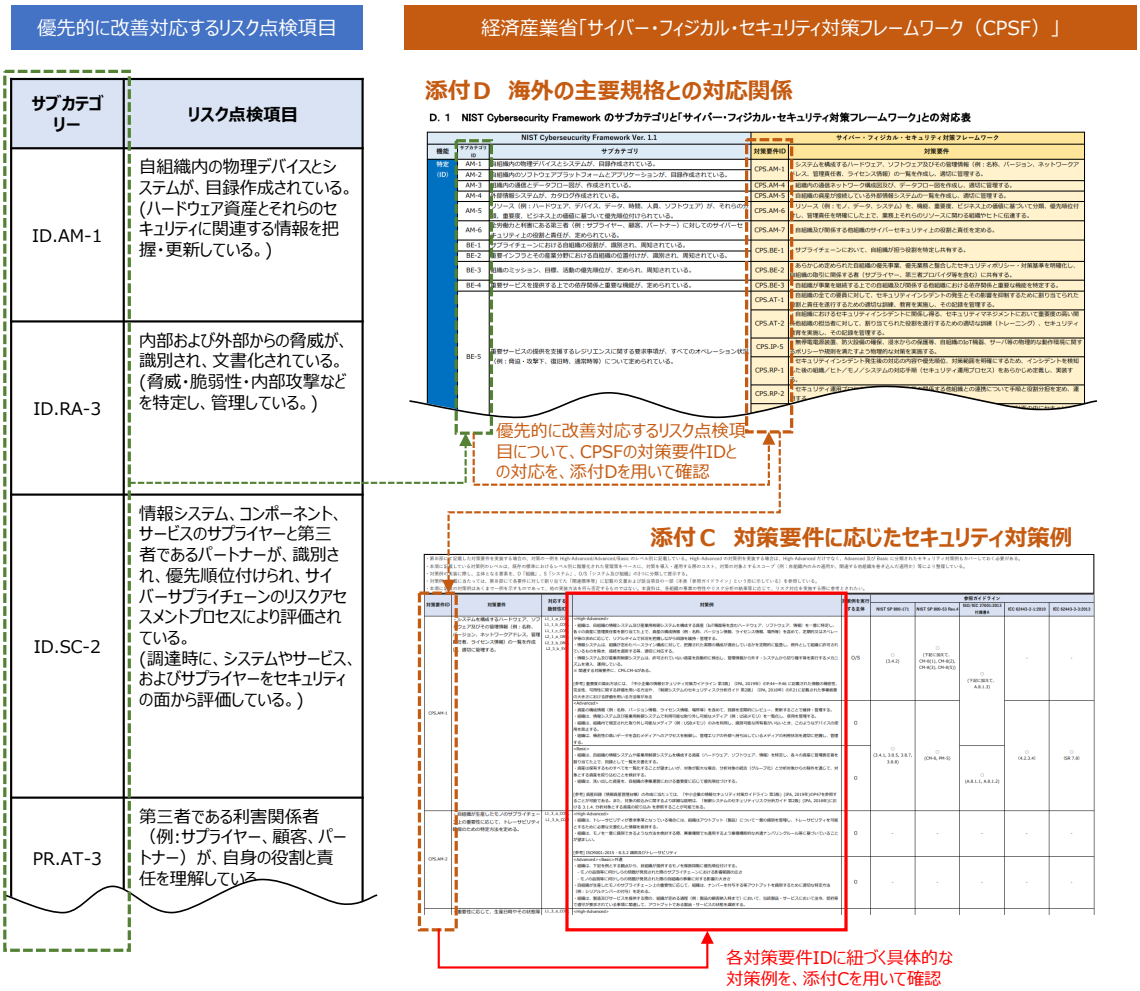



**図 5-1　優先的に改善対応するリスク点検項目に対する CPSF を用いた対策例の検討方針**

優先的に改善対応する項目に対する対応内容が決定した後、その内容をセキュリティ対策改善計画書としてまとめ、経営層に報告することが望まれる。なお、リスク点検は、一度のみの実施では効果は薄く、定期的に実施することで着実な改善が期待される。前述のとおり、本ガイド及び対策状況可視化ツールを用いた二回目以降のリスク点検の場合、初回のリスク点検で活用した情報に基づいて効率的なリスク点検が実施可能となる。前回に実施したリスク点検の結果も参照しつつ、最低限一年に一度、リスク点検を定期的に実施することが望まれる。

## 6.リスク点検項目・対策を怠った場合に想定されるリスク

NIST CSF の各機能・カテゴリー・サブカテゴリーに基づく 108 のリスク点検項目及び当該対策を怠った場合に想定されるリスクは以下に示すとおりである。

| 機能 | カテゴリー | サブカテゴリー | リスク点検項目 | 対策を怠った場合に想定されるリスク |
|---|---|---|---|---|
| 識別（ID） | 資産管理 | ID.AM-1 | 自組織内の物理デバイスとシステムが、目録作成されている。(ハードウェア資産とそれらのセキュリティに関連する情報を把握・更新している。) | 自組織内の物理デバイスのサポート期限切れが把握できず、デバイスの脆弱性を利用しマルウェア感染され、保護すべきデータが漏えい・改ざんされる可能性がある。 |
| 識別（ID） | 資産管理 | ID.AM-2 | 自組織内のソフトウェアプラットフォームとアプリケーションが、目録作成されている。(ソフトウェア資産とそれらのセキュリティに関連する情報を把握・更新している。) | 自組織内で利用しているソフトウェアに対してセキュリティパッチが正しく適用されず、ソフトウェアの脆弱性を利用しマルウェア感染され、保護すべきデータが漏えい・改ざんされる可能性がある。 |
| 識別（ID） | 資産管理 | ID.AM-3 | 組織内の通信とデータフロー図が、作成されている。(ネットワーク構成と各通信先を把握・更新している。) | ネットワーク構成の認識不足により、意図しない通信先より不正アクセスされて、自組織が適切に事業継続できない可能性がある。 |
| 識別（ID） | 資産管理 | ID.AM-4 | 外部情報システムが、カタログ作成されている。(外部連携先システムを把握・更新している。) | 意図しない外部情報システムからの接続により、通信経路上でデータを改ざんする中間者攻撃を受けて、保護すべきデータが漏えい・改ざんされる可能性がある。 |

| 機能 | カテゴリー | サブ<br>カテゴリー | リスク点検項目 | 対策を怠った場合に<br>想定されるリスク |
|---|---|---|---|---|
| 識別<br>（ID） | 資産管理 | ID.AM-5 | リソース（例:ハードウェア、デバイス、データ、ソフトウェア）が、それらの分類、重要度、ビジネス上の価値に基づいて優先順位付けられている。<br>(システム資産・情報資産に対する重要度分類基準があり、資産はこれに基づいて分類されている。また、これらの基準が更新されている。) | システムの管理不足により、認識していないシステムが高負荷攻撃を受けて、自組織のシステムが停止する可能性がある。 |
| 識別<br>（ID） | 資産管理 | ID.AM-6 | 全従業員及び利害関係にある第三者（例:サプライヤー、顧客、パートナー）に対してのサイバーセキュリティ上の役割と責任が、定められている。<br>(システムの関係者に対し、セキュリティ上の役割と責任を定めている。) | 他組織で発生したセキュリティインシデントにより、自組織が適切に事業継続できない可能性がある。 |
| 識別<br>（ID） | ビジネス<br>環境 | ID.BE-1 | サプライチェーンにおける自組織の役割が、識別され、周知されている。<br>(自社のサプライチェーン全体における組織の役割を特定し、社内の関係者やサプライヤーとの間で共有されている。) | 自組織のセキュリティインシデントにより、取引関係者が適切に事業継続できない可能性がある。 |

| 機能 | カテゴリー | サブ<br>カテゴリー | リスク点検項目 | 対策を怠った場合に<br>想定されるリスク |
|---|---|---|---|---|
| 識別<br>（ID） | ビジネス<br>環境 | ID.BE-2 | 重要インフラとその産業分野における自組織の位置づけが、識別され、周知されている。<br>(経営戦略・事業ニーズ等を基に策定されたシステム戦略やシステムアーキテクチャが社内に周知されている。) | 自組織のセキュリティインシデントにより、関係する他組織が適切に事業継続できない可能性がある。 |
| 識別<br>（ID） | ビジネス<br>環境 | ID.BE-3 | 組織のミッション、目標、活動の優先順位が、定められ、周知されている。<br>(自組織におけるミッション、事業目標、リスク管理活動の優先順位がリスク管理基準によって定めており、その周知に努めている。) | 優先順位が高いセキュリティインシデントの対応が遅れたことにより、自組織が適切に事業継続できない可能性がある。 |
| 識別<br>（ID） | ビジネス<br>環境 | ID.BE-4 | 重要サービスを提供する上での依存関係と重要な機能が、定められている。<br>(重要サービスの提供に必要な重要資産と関連サプライヤーを把握・更新している。) | 重要なサプライヤーで発生したセキュリティインシデントにより、自組織が適切に事業継続できない可能性がある。 |
| 識別<br>（ID） | ビジネス<br>環境 | ID.BE-5 | 重要サービスの提供を支援するレジリエンスに関する要求事項が、すべてのオペレーション状況（例：脅迫・攻撃下、復旧時、通常時等）について定められている。<br>（重要サービスに求められるサービスレベルと要求事項が整理・更新されている。） | 本来達成すべきサービスレベルに達していない重要サービスが攻撃されることで、適切に事業継続できない可能性がある。 |

| 機能 | カテゴリー | サブ<br>カテゴリー | リスク点検項目 | 対策を怠った場合に<br>想定されるリスク |
|---|---|---|---|---|
| 識別<br>（ID） | ガバナンス | 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。<br>（組織のサイバーセキュリティポリシーが規定され、社内に周知されている。） | ID・パスワードなどの窃取による正規のユーザへのなりすましによって、保護すべきデータが漏えい・改ざんされる可能性がある。 |
| 識別<br>（ID） | ガバナンス | ID.GV-2 | サイバーセキュリティ上の役割と責任が、内部の担当者と外部パートナーとで調整・連携されている。<br>(セキュリティ対策は、社外の委託先やパートナーを含めて連携して実施している。) | 管理されてないリソースに対して高負荷攻撃を受けて、自組織のシステムが停止する可能性がある。 |
| 識別<br>（ID） | ガバナンス | ID.GV-3 | プライバシーや人権に関する義務を含む、サイバーセキュリティに関する法規制上の要求事項が、理解され、管理されている。<br>(セキュリティ・プライバシーに関する法制度を把握・対応している。) | 法制度等で規定されている水準のセキュリティ対策を実装できず、自組織のシステムの停止される可能性がある。 |
| 識別<br>（ID） | ガバナンス | ID.GV-4 | ガバナンスとリスクマネジメントプロセスが、サイバーセキュリティリスクに対処している。<br>(サイバーリスクを特定し、リスク管理手法の検討に利用している。) | 特定されていないサイバーセキュリティリスクを悪用した攻撃により、保護すべきデータが漏えい・改ざんされる可能性がある。 |
| 識別<br>（ID） | リスクアセスメント | ID.RA-1 | 資産の脆弱性が、識別され、文書化されている。<br>(システムの脆弱性を特定し管理している。) | システムにおけるセキュリティ上の脆弱性を利用しマルウェア感染され、保護すべきデータが漏えい・改ざんされる可能性がある。 |

| 機能 | カテゴリー | サブ<br>カテゴリー | リスク点検項目 | 対策を怠った場合に<br>想定されるリスク |
|---|---|---|---|---|
| 識別<br>（ID） | リスクアセスメント | ID.RA-2 | サイバー脅威に関する情報が、複数の情報共有フォーラム及び複数のソースから入手されている。<br>（サイバー脅威に関する情報を複数のソースから入手している。） | 未知の脅威によってシステムがマルウェア感染し、保護すべきデータが漏えい・改ざんされる可能性がある。 |
| 識別<br>（ID） | リスクアセスメント | ID.RA-3 | 内部及び外部からの脅威が、識別され、文書化されている。<br>(脅威・脆弱性・内部攻撃などを特定し、管理している。) | 未知の脅威によってシステムがマルウェア感染し、保護すべきデータが漏えい・改ざんされる可能性がある。 |
| 識別<br>（ID） | リスクアセスメント | ID.RA-4 | ビジネスに対する潜在的な影響とその発生可能性が、識別されている。<br>(セキュリティリスクが顕在化する可能性と、顕在化した場合の影響を把握・分類している。) | セキュリティリスクが顕在化した際の影響が適切に評価されないことで、セキュリティ対策が過少となり、攻撃を受けた場合に適切に事業継続できない可能性がある。 |
| 識別<br>（ID） | リスクアセスメント | ID.RA-5 | 脅威、脆弱性、発生可能性、影響が、リスクを判断する際に使用されている。<br>(脅威情報、脆弱性情報、発生可能性、影響度から、リスクを管理している。) | セキュリティリスクが顕在化した際の影響が適切に評価されないことで、セキュリティ対策が過少となり、攻撃を受けた場合に適切に事業継続できない可能性がある。 |
| 識別<br>（ID） | リスクアセスメント | ID.RA-6 | リスク対応が、識別され、優先順位付けされている。<br>（リスク対応計画が作成され、優先度付けされている。） | セキュリティリスクが顕在化した際の対応が優先度付けされないことで、本来対策すべき箇所にセキュリティ対策が実施できず、攻撃を受けた場合に適切に事業継続できない可能性がある。 |

| 機能 | カテゴリー | サブカテゴリー | リスク点検項目 | 対策を怠った場合に想定されるリスク |
|---|---|---|---|---|
| 識別（ID） | リスク管理戦略 | ID.RM-1 | リスクマネジメントプロセスが、組織の利害関係者によって定められ、管理され、承認されている。<br>(セキュリティリスク管理プロセスが策定され、運用・管理されている。) | セキュリティリスクが顕在化した際の影響が適切に管理されないことで、セキュリティ対策が過少となり、攻撃を受けた場合に適切に事業継続できない可能性がある。 |
| 識別（ID） | リスク管理戦略 | ID.RM-2 | 組織のリスク許容度が、決定され、明確に表現されている。<br>(セキュリティリスク対策の実施基準が策定されている。) | セキュリティリスク許容度が適切に評価されないことで、セキュリティ対策が過少となり、攻撃を受けた場合に適切に事業継続できない可能性がある。 |
| 識別（ID） | リスク管理戦略 | ID.RM-3 | 自組織によるリスク許容度の決定が、重要インフラにおける組織の役割と、その分野に特化したリスク分析の結果に基づいて行われている。<br>(リスク対策の実施基準が社会への影響や重要システム・サービスを考慮して定められている。) | セキュリティリスク許容度が適切に評価されないことで、セキュリティ対策が過少となり、攻撃を受けた場合に適切に事業継続できない可能性がある。 |
| 識別（ID） | サプライチェーンリスクマネジメント | ID.SC-1 | サイバーサプライチェーンのリスクマネジメントプロセスが、組織の利害関係者によって、識別され、定められ、評価され、管理され、承認されている。<br>(サプライチェーンにおけるセキュリティリスク管理手法が、社内で確立されている。) | サプライチェーンに関するセキュリティリスク許容度が適切に評価されないことで、サプライチェーンに関するセキュリティ対策が過少となり、攻撃を受けた場合に自組織が適切に事業継続できない可能性があるほか、第三者の事業継続に影響を及ぼす可能性がある。 |

| 機能 | カテゴリー | サブカテゴリー | リスク点検項目 | 対策を怠った場合に想定されるリスク |
|---|---|---|---|---|
| 識別（ID） | サプライチェーンリスクマネジメント | ID.SC-2 | 情報システム、コンポーネント、サービスのサプライヤーと第三者であるパートナーが、識別され、優先順位付けられ、サイバーサプライチェーンのリスクアセスメントプロセスにより評価されている。<br>(調達時に、システムやサービス、及びサプライヤーをセキュリティの面から評価している。) | 他組織の管理するシステムにおけるセキュリティ上の脆弱性を利用しマルウェア感染され、関係する他組織で管理している領域から自組織の保護すべきデータが漏えい・改ざんされる可能性がある。 |
| 識別（ID） | サプライチェーンリスクマネジメント | ID.SC-3 | サプライヤー及び第三者であるパートナーとの契約が、組織のサイバーセキュリティプログラムやサイバーサプライチェーンのリスクマネジメント計画の目的を達成するための適切な対策の実施に活用されている。<br>(調達時の契約は、サプライチェーンにおけるセキュリティリスクへの対応が考慮されている。) | 自組織のデータを格納している他組織のシステムがマルウェア感染することで、自組織の保護すべきデータが漏えい・改ざんされる可能性がある。 |
| 識別（ID） | サプライチェーンリスクマネジメント | ID.SC-4 | サプライヤー及び第三者であるパートナーが、監査、テストの結果、又はその他の評価に基づき、契約上の義務を満たしているか、定期的に評価されている。<br>(サプライチェーンにおけるセキュリティリスクをサプライヤーやパートナーに対して定期的に評価している。) | 自組織のデータを格納している他組織のシステムがマルウェア感染することで、自組織の保護すべきデータが漏えい・改ざんされる可能性がある。 |

| 機能 | カテゴリー | サブカテゴリー | リスク点検項目 | 対策を怠った場合に想定されるリスク |
|---|---|---|---|---|
| 識別（ID） | サプライチェーンリスクマネジメント | ID.SC-5 | 対応・復旧計画の策定とテストが、サプライヤー及び第三者プロバイダーと共に行なわれている。<br>(会社のインシデント対応計画・復旧計画は、サプライヤー等を含めて考慮されている。) | 他組織を考慮した対応・復旧計画が策定されず、自組織のセキュリティインシデントが発生した際に、関係する他組織が適切に事業継続できない可能性がある。 |
| 防御（PR） | アクセス制御 | PR.AC-1 | 認可されたデバイス、ユーザ、プロセスのアイデンティティと証明書が、発行、管理、検証、取り消し、監査されている。<br>(ユーザの識別情報と認証情報の管理されている。) | 不適切な認証情報の管理により、正規ユーザによる内部不正が行われ、保護すべきデータが漏えい・改ざんされる可能性がある。 |
| 防御（PR） | アクセス制御 | PR.AC-2 | 資産に対する物理アクセスが、管理され、保護されている。<br>（システムの構成機器が物理的に保護され、物理アクセスに対する対策が施されている。） | 適切な物理的な対策が実施されず、悪意を持った自組織内外の関係者が不正に侵入し、故障や正確でないデータの送信等が発生する可能性がある。 |
| 防御（PR） | アクセス制御 | PR.AC-3 | リモートアクセスが、管理されている。<br>（リモートアクセスのセキュリティ対策や管理基準が規定・運用されている。） | リモートアクセスの管理不足により、悪意のある第三者が正規ユーザへなりすまし、保護すべきデータが漏えい・改ざんされる可能性がある。 |

| 機能 | カテゴリー | サブカテゴリー | リスク点検項目 | 対策を怠った場合に想定されるリスク |
|---|---|---|---|---|
| 防御（PR） | アクセス制御 | PR.AC-4 | アクセスの許可及び認可が、最小権限の原則及び役割の分離の原則を組み入れて、管理されている。(システムに対する ID の発行、アクセス権限の付与が必要最小限となるよう、また利用者に対し個別の ID が発行されるよう管理している。) | 共通 ID を発行し、その共通 ID が外部に漏えいした場合に、正規のユーザへのなりすましによって遠隔からシステムに不正アクセスされ、システムが不正操作される可能性がある。 |
| 防御（PR） | アクセス制御 | PR.AC-5 | ネットワークの完全性が、保護されている（例:ネットワークの分離、ネットワークのセグメント化）。(セキュリティレベルに応じたネットワーク分離を行っている。) | 重要システムのネットワークに適切な防護措置がされず、通信経路上でデータを改ざんする中間者攻撃を受けて、保護すべきデータが漏えい・改ざんされる可能性がある。 |
| 防御（PR） | アクセス制御 | PR.AC-6 | ID は、ID 利用者の本人確認がなされ、証明書に紐付けられ、インタラクションで使用されている。(システムが利用者の本人確認と利用資格の確認を行っている。) | 利用者の本人確認がされず、悪意のある組織内外の関係者が正規ホストへなりすまし、システム内部に不正アクセスされ、システムが不正操作される可能性がある。 |
| 防御（PR） | アクセス制御 | PR.AC-7 | ユーザ、デバイス、その他の資産は、トランザクションのリスク（例:個人のセキュリティ及びプライバシー上のリスク、その他組織にとってのリスク）の度合いに応じた認証（例:多要素認証など）が行われている。(リスクに応じた認証方式を採用している) | 重要システムに適切な認証方法が設定されず、第三者が正規のホストになりすまし、自組織で利用しているシステムに不正アクセスされ、システムが不正操作される可能性がある。 |

| 機能 | カテゴリー | サブカテゴリー | リスク点検項目 | 対策を怠った場合に想定されるリスク |
|---|---|---|---|---|
| 防御（PR） | 意識向上及びトレーニング | PR.AT-1 | すべてのユーザは、情報が周知され、トレーニングが実施されている。<br>(セキュリティに関する社員の意識啓発や教育を実施している。) | 悪意を持った自組織内の関係者が保護すべきデータを持ち出したことによって、保護すべきデータが漏えい・改ざんされる可能性がある。 |
| 防御（PR） | 意識向上及びトレーニング | PR.AT-2 | 権限を持つユーザが、自身の役割と責任を理解している。<br>(システム利用者が、自身が実施すべきセキュリティ対策とその責任を理解している。) | セキュリティ責任を理解していない自組織内の関係者が不正にデータを改ざんすることで、システムの異常動作等の意図しない動作が生じる可能性がある。 |
| 防御（PR） | 意識向上及びトレーニング | PR.AT-3 | 第三者である利害関係者（例:サプライヤー、顧客、パートナー）が、自身の役割と責任を理解している。<br>（サプライヤーやパートナーが、セキュリティ管理における役割と責任を理解している。） | セキュリティ責任を理解していない利害関係者が不正にデータを改ざんすることで、機器の破損等の意図しない品質劣化が生じる可能性がある。 |
| 防御（PR） | 意識向上及びトレーニング | PR.AT-4 | 上級役員（セキュリティ担当役員）が、自身の役割と責任を理解している。<br>（任命されたセキュリティ責任者が、セキュリティに関する責任を担い、役割を発揮している。） | 上級役員の判断の遅れにより、自組織のセキュリティインシデントに対して適切な対応がなされず、自組織が事業継続できない可能性がある。 |
| 防御（PR） | 意識向上及びトレーニング | PR.AT-5 | 物理セキュリティ及びサイバーセキュリティの担当者が、自身の役割と責任を理解している。<br>（物理的なサイバーセキュリティ確保の担当者が、対策を実施・管理している。） | 重要区画に対して物理的対策がされず、社内関係者が重要区画に不正に侵入し、保護すべきデータが漏えい・改ざんされる可能性がある。 |

| 機能 | カテゴリー | サブカテゴリー | リスク点検項目 | 対策を怠った場合に想定されるリスク |
|---|---|---|---|---|
| 防御（PR） | データセキュリティ | PR.DS-1 | 保存されているデータが、保護されている。(システムや電子記憶媒体に保存した重要なデータに対して、セキュリティ対策を行っている。) | 重要なデータに対する対策が不十分であり、データが漏えい・改ざんされる可能性がある。 |
| 防御（PR） | データセキュリティ | PR.DS-2 | 伝送中のデータが、保護されている。(伝送中の重要なデータに対し、セキュリティ対策を行っている。) | 重要データの伝送において正しい対策がされず、中間者攻撃を受けて、保護すべきデータが漏えい・改ざんされる可能性がある。 |
| 防御（PR） | データセキュリティ | PR.DS-3 | 資産は、撤去、譲渡、廃棄に至るまで、正式に管理されている。（システムの撤去、譲渡、廃棄方法が定義・運用されている。） | 不正な機器がシステムに接続され、故障や正確でないデータの送信などが発生する可能性がある。 |
| 防御（PR） | データセキュリティ | PR.DS-4 | 可用性を確保するのに十分な容量が、維持されている。（システムの安定稼働を行うためのリソースが想定・確保されている。） | システム障害に対する対策が不足し、システムを構成する IT 機器、通信機器等が高負荷攻撃を受けて、IT 機器や通信機器の機能が停止する可能性がある。 |
| 防御（PR） | データセキュリティ | PR.DS-5 | データ漏えいに対する防御対策が、実装されている。（重要なデータの特定とそのデータに対する情報漏えい対策を管理・実施している。） | 重要なデータが暗号化されず、保護すべきデータが漏えい・改ざんされる可能性がある。 |
| 防御（PR） | データセキュリティ | PR.DS-6 | 完全性チェックメカニズムが、ソフトウェア、ファームウェア、及び情報の完全性を検証するために使用されている。(システムの改ざんを管理・検証している。) | システムのファイル更新の検証不足のため、不正のアップデートが実施され、保護すべきデータが改ざんされる可能性がある。 |

| 機能 | カテゴリー | サブ<br>カテゴリー | リスク点検項目 | 対策を怠った場合に<br>想定されるリスク |
|---|---|---|---|---|
| 防御<br>（PR） | データセキュリティ | PR.DS-7 | 開発・テスト環境が、実稼働環境から分離されている。（システムの本番環境と開発・テスト環境のネットワークが分離されている。） | 開発中の脆弱性があるパッチが間違って IT 機器に適用されたことによって、脆弱性を悪用した不正アクセスが行われ、事前に想定されていない動作をする可能性がある。 |
| 防御<br>（PR） | データセキュリティ | PR.DS-8 | 完全性チェックメカニズムが、ハードウェアの完全性を検証するために使用されている。(システムの構成機器の完全性（不正な変更など）を確認している。) | 正規の機器を模した偽造品の挿入によって、システムの異常動作等の意図しない動作が生じる可能性がある。 |
| 防御<br>（PR） | 情報を保護するためのプロセス及び手順 | PR.IP-1 | 情報技術/産業用制御システムのベースラインとなる構成は、セキュリティ原則（例:最低限の機能性の概念）を組み入れて、定められ、維持されている。(セキュリティを考慮したシステムの設計標準を作成・利用している。) | セキュリティ設計が不十分のため、システムに残存したセキュリティ上の脆弱性が悪用され、自組織のシステムが停止する可能性がある。 |
| 防御<br>（PR） | 情報を保護するためのプロセス及び手順 | PR.IP-2 | システムを管理するためのシステム（開発）ライフサイクルが、実装されている。(システムのライフサイクルを定義・運用している。) | システムの運用・保守段階で実施すべき事項の検討不足により、システムにおけるセキュリティ上の脆弱性を利用しマルウェア感染され、保護すべきデータが漏えい・改ざんされる可能性がある。 |
| 防御<br>（PR） | 情報を保護するためのプロセス及び手順 | PR.IP-3 | 構成変更管理プロセスは、策定されている。（システムの構成変更管理プロセスが策定・運用されている。） | 構成管理変更が正しく管理されず、システムに残存した脆弱性を悪用して不正アクセスされ、保護すべきデータが漏えい・改ざんされる可能性がある。 |

| 機能 | カテゴリー | サブカテゴリー | リスク点検項目 | 対策を怠った場合に想定されるリスク |
|---|---|---|---|---|
| 防御（PR） | 情報を保護するためのプロセス及び手順 | PR.IP-4 | 情報のバックアップが、実施され、維持され、テストされている。（システム復旧に必要なデータがバックアップされ、復旧テストが行われている。） | 情報のバックアップがないため、自組織のセキュリティインシデントから復旧できず、自組織が適切に事業継続できない可能性がある。 |
| 防御（PR） | 情報を保護するためのプロセス及び手順 | PR.IP-5 | 組織の資産の物理的な運用環境に関するポリシーと規制が、満たされている。（システム環境の運用対策（例：災害対策、入退室管理など）が規定・運用されている。） | 入退室管理が正しく実施されず、悪意を持った自組織内外の関係者による計測機能に対する不正行為が行われ、システムが停止する可能性がある。 |
| 防御（PR） | 情報を保護するためのプロセス及び手順 | PR.IP-6 | データは、ポリシーに従って破壊されている。(データ消去又は読み取りできない状態にする場合は、不正利用を防ぐよう対策している。) | データが残存する廃棄済みの記録媒体が、悪意を持った自組織内外の関係者に持ち出されたことによって、保護すべきデータが漏えい・改ざんされる可能性がある。 |
| 防御（PR） | 情報を保護するためのプロセス及び手順 | PR.IP-7 | 防御プロセスは、改善されている。(セキュリティ関連情報を収集して、セキュリティ対策の改善を図っている。) | 最新の脆弱性情報が把握できず、システムにおけるセキュリティ上の脆弱性を利用しマルウェア感染され、保護すべきデータが漏えい・改ざんされる可能性がある。 |
| 防御（PR） | 情報を保護するためのプロセス及び手順 | PR.IP-8 | 防御技術の有効性に関する情報が、共有されている。(最新のセキュリティ対策技術の収集と共有が行われている。) | 最新の脆弱性情報が把握できず、システムにおけるセキュリティ上の脆弱性を利用しマルウェア感染され、保護すべきデータが漏えい・改ざんされる可能性がある。 |

| 機能 | カテゴリー | サブ<br>カテゴリー | リスク点検項目 | 対策を怠った場合に<br>想定されるリスク |
|---|---|---|---|---|
| 防御<br>（PR） | 情報を保護するためのプロセス及び手順 | PR.IP-9 | 対応計画と復旧計画が、策定され、管理されている。<br>(セキュリティインシデントが発生した場合のインシデント対応計画、業務継続計画、システム復旧計画を策定している。) | システム復旧計画の検討不足のため、セキュリティインシデントが発生した際に、適切に事業継続できない可能性がある。 |
| 防御<br>（PR） | 情報を保護するためのプロセス及び手順 | PR.IP-10 | 対応計画と復旧計画が、テストされている。<br>(セキュリティインシデントが発生した場合のインシデント対応計画、業務継続計画、システム復旧計画について、訓練や演習を行っている。) | システム復旧テストを実施できておらず、セキュリティインシデントが発生した際に、関係する他組織が適切に事業継続できない可能性がある。 |
| 防御<br>（PR） | 情報を保護するためのプロセス及び手順 | PR.IP-11 | サイバーセキュリティには、人事に関わるプラクティス（例:アクセス権限の無効化、人員のスクリーニング）が含まれている。<br>（人員の採用時・退職時・異動時にサイバーセキュリティを考慮した対策が実施されている。） | 退職する社員が把握していたセキュリティに関する重要データが漏えいする可能性がある。 |
| 防御<br>（PR） | 情報を保護するためのプロセス及び手順 | PR.IP-12 | 脆弱性管理計画が、作成され、実装されている。<br>（脆弱性情報を収集・特定し、対応手順が管理されている。） | 最新の脆弱性情報が把握できず、システムにおけるセキュリティ上の脆弱性を利用しマルウェア感染され、保護すべきデータが漏えい・改ざんされる可能性がある。 |

| 機能 | カテゴリー | サブ<br>カテゴリー | リスク点検項目 | 対策を怠った場合に<br>想定されるリスク |
|---|---|---|---|---|
| 防御<br>（PR） | 保守 | PR.MA-1 | 組織の資産の保守と修理は、承認・管理されたツールを用いて実施され、ログが記録されている。<br>(システム上の作業は、承認を受け、手順に則って行われ、記録されている。) | システム上の作業が記録されないことで、インシデント発生時の原因が特定できず、自組織が適切に事業継続できない可能性がある。 |
| 防御<br>（PR） | 保守 | PR.MA-2 | 組織の資産に対する遠隔保守は、承認を得て、ログが記録され、不正アクセスを防止した形式で実施されている。<br>(遠隔保守用の回線を保護し、アクセスを制限・管理している。) | 遠隔保守用の回線が不正アクセスされ、保護すべきデータが漏えい・改ざんされる可能性がある。 |
| 防御<br>（PR） | 保護技術 | PR.PT-1 | 監査記録/ログ記録の対象が、ポリシーに従って決定され、文書化され、実装され、その記録をレビューされている。<br>(システムの重要度によってログの取得・保護を実施している。) | システムのログが取得されないことで、インシデント発生時の原因が特定できず、自組織が適切に事業継続できない可能性がある。 |
| 防御<br>（PR） | 保護技術 | PR.PT-2 | リムーバブルメディアは、保護され、その使用がポリシーに従って制限されている。<br>(外部記憶媒体のルールが策定され、運用されている。) | 外部記録媒体が管理されず、悪意ある関係者が保護すべきデータを不正に持出すことによって、保護すべきデータが漏えい・改ざんする可能性がある。 |

| 機能 | カテゴリー | サブカテゴリー | リスク点検項目 | 対策を怠った場合に想定されるリスク |
|---|---|---|---|---|
| 防御（PR） | 保護技術 | PR.PT-3 | 最低限の機能性の原則が、必須の機能のみ提供するようにシステムを構成することによって組み入れられている。(システムはユーザやクライアントに応じて、必要最低限の機能を提供している。) | 重要システムに適切な認証方法が設定されず、第三者が正規のホストになりすまし、自組織で利用しているシステムに不正アクセスされ、システムが不正操作される可能性がある。 |
| 防御（PR） | 保護技術 | PR.PT-4 | 情報通信ネットワークと制御ネットワークが、分離して保護されている。（外部ネットワーク、社内ネットワーク、重要なネットワークが区別され、それぞれで適した防御策を実施・管理している。) | 情報通信ネットワークで発生したインシデントの影響が制御ネットワークに及ぶことで、制御システムが停止する可能性がある。 |
| 防御（PR） | 保護技術 | PR.PT-5 | メカニズム（例:フェールセーフ、ロードバランシング、ホットスワップ）が、平時及び緊急時においてレジリエンスに関する要求事項を達成するために実装されている。(システムの可用性を高めるための機能を設計・実装している。) | 不正な機器に対する高負荷攻撃によって、安全に支障をきたす動作をする可能性がある。 |
| 検知（DE） | 異常とイベント | DE.AE-1 | ネットワーク運用のベースラインと、ユーザとシステムで期待されるデータフローが、定められ、管理されている。(正常時のネットワークのベースラインを作成し、異常を検知している。) | 通常時のネットワーク通信が把握できず、システムに対する不正アクセスを特定できない可能性がある。 |

| 機能 | カテゴリー | サブカテゴリー | リスク点検項目 | 対策を怠った場合に想定されるリスク |
|---|---|---|---|---|
| 検知（DE） | 異常とイベント | DE.AE-2 | 検知したイベントは、攻撃の標的と手法を理解するために分析されている。（セキュリティ事象の分析手法を管理・運用している。） | インシデントの原因が分析できず、再度セキュリティインシデントが発生し、自組織が適切に事業継続できない可能性がある。 |
| 検知（DE） | 異常とイベント | DE.AE-3 | イベントデータは、複数の情報源やセンサーから収集され、相互分析されている。（セキュリティ事象に関連するデータが、複数の情報源から収集・分析されている。） | セキュリティ事象に関連するデータが取得されないことで、インシデント発生時の原因が特定できず、自組織が適切に事業継続できない可能性がある。 |
| 検知（DE） | 異常とイベント | DE.AE-4 | セキュリティ事象がもたらす影響が、判断されている。（セキュリティ事象の影響度を特定し、適宜共有・分析している。） | セキュリティ事象に関連するデータが分析されないことで、インシデントの兆候や発生を特定できず、自組織が適切に事業継続できない可能性がある。 |
| 検知（DE） | 異常とイベント | DE.AE-5 | インシデント警告の閾値が、定められている。(インシデント発生を宣言する基準が明確になっている。) | インシデント警告の閾値が定められないことで、インシデントの兆候や発生を特定できず、自組織が適切に事業継続できない可能性がある。 |
| 検知（DE） | セキュリティの継続的なモニタリング | DE.CM-1 | ネットワークは、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。（ネットワークのログが取得され、原因調査・異常検知に利用されている。） | ネットワークのログが取得されないことで、インシデント発生時の原因が特定できず、自組織が適切に事業継続できない可能性がある。 |
| 検知（DE） | セキュリティの継続的なモニタリング | DE.CM-2 | 物理環境は、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。（物理的な侵入検知対策が実施・運用されている。） | 保護が必要なエリアに対する物理的な不正侵入が検知できず、保護すべきデータが漏えい・改ざんされる可能性がある。 |

| 機能 | カテゴリー | サブ<br>カテゴリー | リスク点検項目 | 対策を怠った場合に<br>想定されるリスク |
|---|---|---|---|---|
| 検知<br>（DE） | セキュリティの継続的なモニタリング | DE.CM-3 | 人員の活動は、サイバーセキュリティの潜在的なイベントを検知できるようにモニタリングされている。<br>（システムの利用者の活動のログ取得し、活用している。） | システム利用者の活用ログが取得されないことで、自組織における悪意ある関係者の保護すべきデータの適切でない持出行為を検知できず、保護すべきデータが漏えい・改ざんする可能性がある。 |
| 検知<br>（DE） | セキュリティの継続的なモニタリング | DE.CM-4 | 悪質なコードは、検知されている。<br>(マルウェア等の悪意あるプログラムを検知できる対策を実施・管理している。) | マルウェア等の悪意あるプログラムが検知できず、端末に対するマルウェア攻撃によって、保護すべきデータが漏えい・改ざんされる可能性がある。 |
| 検知<br>（DE） | セキュリティの継続的なモニタリング | DE.CM-5 | 不正なモバイルコード<br>（Web サイトなどを通してダウンロードされる不正なスクリプトコードなど）は、検知されている。<br>（不正なコードを検知できる仕組みが構築されている。） | 端末に対する不正コードによる攻撃が検知できず、保護すべきデータが漏えい・改ざんされる可能性がある。 |
| 検知<br>（DE） | セキュリティの継続的なモニタリング | DE.CM-6 | （業務委託先など）外部サービスプロバイダーの活動は、潜在的なサイバーセキュリティ事象を検知できるようにモニタリングされている。<br>(委託先企業や協力会社の活動を、セキュリティの観点で監視している。) | 他組織の管理するシステムがマルウェア感染することによって、他組織で管理している領域から自組織の保護すべきデータが漏えい・改ざんされる可能性がある。 |
| 検知<br>（DE） | セキュリティの継続的なモニタリング | DE.CM-7 | 権限のない人員、接続、デバイス、ソフトウェアのモニタリングが、実施されている。<br>（ユーザの認証・PC・ソフトウェアのログが取得され、不正利用の検知などに利用している。） | 悪意のある関係者がソフトウェアを不正にインストールすることで、保護すべきデータが漏えい・改ざんされる可能性がある。 |

| 機能 | カテゴリー | サブカテゴリー | リスク点検項目 | 対策を怠った場合に想定されるリスク |
|---|---|---|---|---|
| 検知（DE） | セキュリティの継続的なモニタリング | DE.CM-8 | 脆弱性スキャンが、実施されている。<br>(システムに対し脆弱性診断を実施している。) | システムに残存した脆弱性を特定できず、その脆弱性を悪用したマルウェア攻撃によって保護すべきデータが漏えい・改ざんされる可能性がある。 |
| 検知（DE） | 検知プロセス | DE.DP-1 | 検知に関する役割と責任は、説明責任を果たせるように明確に定義されている。<br>（異常検知され場合の対応方針・体制が策定・運用されている。） | システムの異常が正しく検知されないことで、インシデントの発生の特定できず、自組織が適切に事業継続できない可能性がある。 |
| 検知（DE） | 検知プロセス | DE.DP-2 | 検知活動は、該当するすべての要求事項を準拠している。<br>（異常検知するための項目を定め、検知活動を実施している。） | システムの異常が正しく検知されないことで、インシデントの発生の特定できず、自組織が適切に事業継続できない可能性がある。 |
| 検知（DE） | 検知プロセス | DE.DP-3 | 検知プロセスが、テストされている。<br>（異常検知プロセスが構築・テストされている。） | システムの異常が正しく検知されないことで、インシデントの発生の特定できず、自組織が適切に事業継続できない可能性がある。 |
| 検知（DE） | 検知プロセス | DE.DP-4 | イベント検知情報が、周知されている。<br>（異常が検知された際の、情報共有体制・手順が運用されている。） | システムの異常が関係者に適切に共有されず、インシデント対応に遅れが生じ、自組織が適切に事業継続できない可能性がある。 |
| 検知（DE） | 検知プロセス | DE.DP-5 | 検知プロセスが、継続的に改善されている。<br>（セキュリティ事象に関する異常を検知する仕組みが、定期的にテストされ、改善されている。） | セキュリティ事象の検知プロセスが認識されず、自組織のセキュリティインシデントに正しく対応できず、自組織が適切に事業継続できない可能性がある。 |

| 機能 | カテゴリー | サブカテゴリー | リスク点検項目 | 対策を怠った場合に想定されるリスク |
|---|---|---|---|---|
| 対応（RS） | 対応計画 | RS.RP-1 | インシデント対応計画が、インシデントの発生中又は発生後に実行されている。（インシデント発生時の対応計画が作成・運用している。） | インシデントの対応体制・計画が認識されず、自組織のセキュリティインシデントに正しく対応できないことで、自組織が適切に事業継続できない可能性がある。 |
| 対応（RS） | コミュニケーション | RS.CO-1 | 人員は、対応が必要になった時の自身の役割と行動の順序を認識している。（インシデント時の対応体制が整備・運用している。） | インシデントの対応体制・計画が認識されず、自組織のセキュリティインシデントに正しく対応できないことで、自組織が適切に事業継続できない可能性がある。 |
| 対応（RS） | コミュニケーション | RS.CO-2 | インシデントが、定められた基準に沿って報告されている。（インシデントの報告手順が作成・運用している。） | インシデントの報告手順が作成されず、自組織のセキュリティインシデントに正しく対応できないことで、自組織が適切に事業継続できない可能性がある。 |
| 対応（RS） | コミュニケーション | RS.CO-3 | インシデント対応計画に従って、情報が共有されている。（インシデント対応計画にしたがって、各関係者間での情報共有が速やかに実施されている。） | インシデントの情報共有手順が作成されず、自組織のセキュリティインシデントに正しく対応できないことで、自組織が適切に事業継続できない可能性がある。 |
| 対応（RS） | コミュニケーション | RS.CO-4 | 利害関係者との間で調整が、インシデント対応計画に従って行なわれている。（インシデント対応時には、対応計画に従って社内外の利害関係者と調整されている。） | 自組織のセキュリティインシデントの他組織への影響が把握されず、自組織でインシデントが発生した場合に、関係する他組織が適切に事業継続できない可能性がある。 |

| 機能 | カテゴリー | サブカテゴリー | リスク点検項目 | 対策を怠った場合に想定されるリスク |
|---|---|---|---|---|
| 対応（RS） | コミュニケーション | RS.CO-5 | サイバーセキュリティに関する状況認識を広げるために、外部利害関係者との間で自発的な情報共有が行なわれている。（自社から社外組織等に対してサイバーセキュリティに関する情報が共有されている。） | 自組織のセキュリティインシデントが法律等に沿って外部組織に適切に報告されず、自組織のレピュテーションが低下する可能性がある。 |
| 対応（RS） | 分析 | RS.AN-1 | 検知システムからの通知は、調査されている。（セキュリティ事象の検知・調査方法が策定・運用している。） | システムの異常が正しく検知されないことで、インシデントの発生の特定できず、自組織が適切に事業継続できない可能性がある。 |
| 対応（RS） | 分析 | RS.AN-2 | インシデントがもたらす影響は、把握されている。（検知されたインシデントが分析され、その結果で対応している。） | セキュリティインシデントに対して正しい優先度で対応できず、自組織が適切に事業継続できない可能性がある。 |
| 対応（RS） | 分析 | RS.AN-3 | フォレンジックが、実施されている。（インシデント対応計画に沿って、フォレンジック（インシデントの被害・原因分析）が実施されている。） | インシデント発生時の原因究明や責任の所在を明確化できない可能性がある。 |
| 対応（RS） | 分析 | RS.AN-4 | インシデントは、対応計画に従って分類されている。（インシデント対応計画に沿って、発生したインシデントが分類されている。） | 自組織のセキュリティインシデントに対して正しく対応できず、自組織が適切に事業継続できない可能性がある。 |

| 機能 | カテゴリー | サブ<br>カテゴリー | リスク点検項目 | 対策を怠った場合に<br>想定されるリスク |
|---|---|---|---|---|
| 対応<br>（RS） | 分析 | RS.AN-5 | プロセスは、内外のソース（例:内部テスト、セキュリティ情報、セキュリティ研究者）から報告された脆弱性情報を、自組織が受け取り、分析し、対応するために定められている。<br>(脆弱性情報を受け取り、分析し、対応するための手順が定めている。) | 最新の脆弱性情報が把握できず、システムにおけるセキュリティ上の脆弱性を利用しマルウェア感染され、保護すべきデータが漏えい・改ざんされる可能性がある。 |
| 対応<br>（RS） | 低減 | RS.MI-1 | インシデントは、封じ込められている。<br>（インシデントの重大度によって、封じ込めの計画・手法が策定している。） | 自組織のセキュリティインシデントに対して被害を最小化できず、自組織が適切に事業継続できない可能性がある。 |
| 対応<br>（RS） | 低減 | RS.MI-2 | インシデントは、緩和されている。<br>(インシデントの根絶対象と方法が策定されている。) | 自組織のセキュリティインシデントに対して被害を最小化できず、自組織が適切に事業継続できない可能性がある。 |
| 対応<br>（RS） | 低減 | RS.MI-3 | 新たに識別された脆弱性は、許容できるリスクである場合にはその旨を文書化され、そうでない場合にはリスクが緩和されている。<br>(脆弱性対策を実施している。もしくはリスクとして許容している。) | 最新の脆弱性情報が把握できず、システムにおけるセキュリティ上の脆弱性を利用しマルウェア感染され、保護すべきデータが漏えい・改ざんされる可能性がある。 |
| 対応<br>（RS） | 改善 | RS.IM-1 | （インシデント）対応計画は、学んだ教訓を取り入れられている。<br>(社内で起きたインシデントの教訓から、インシデント対応計画を見直している。) | インシデント発生に至った根本原因が修正されず、再度セキュリティインシデントを受けることで、適切に事業継続できない可能性がある。 |

| 機能 | カテゴリー | サブカテゴリー | リスク点検項目 | 対策を怠った場合に想定されるリスク |
|---|---|---|---|---|
| 対応（RS） | 改善 | RS.IM-2 | 対応戦略は、更新されている。（収集したインシデント事例を基に、対応計画が更している。） | 他組織の受けたインシデントと同様のインシデントを受けることで、自組織が適切に事業継続できない可能性がある。 |
| 復旧（RC） | 復旧計画 | RC.RP-1 | 復旧計画が、サイバーセキュリティインシデントの発生中又は発生後に実施されている。（システムの復旧計画に従って、システムの復旧が実施されている。） | 自組織のセキュリティインシデントから復旧できず、自組織が適切に事業継続できない可能性がある。 |
| 復旧（RC） | 改善 | RC.IM-1 | 復旧計画は、学んだ教訓を取り入れている。（システムを復旧した際の情報が収集され、システム復旧計画の改善に活用されている。） | セキュリティインシデント後に正しく復旧されなかった不具合により、自組織が適切に事業継続できない可能性がある。 |
| 復旧（RC） | 改善 | RC.IM-2 | 復旧戦略は、更新されている。（収集したインシデント事例を基に、復旧計画が更している。） | 他組織の受けたインシデントと同様のインシデントを受けることで、自組織が適切に事業継続できない可能性がある。 |
| 復旧（RC） | コミュニケーション | RC.CO-1 | 広報活動が、管理されている。（セキュリティインシデントの外部発信体制を構築している。） | セキュリティインシデントに対する対応が正しく広報されず、自組織のレピュテーションが低下する可能性がある。 |
| 復旧（RC） | コミュニケーション | RC.CO-2 | 評判は、インシデント発生後に回復されている。（インシデント発生後の会社のレビューテーションが調査・回復されている。） | セキュリティインシデントにより低下したレピュテーションを回復できず、自組織の事業が継続できない可能性がある。 |

| 機能 | カテゴリー | サブ<br>カテゴリー | リスク点検項目 | 対策を怠った場合に<br>想定されるリスク |
|---|---|---|---|---|
| 復旧<br>（RC） | コミュニケーション | RC.CO-3 | 復旧活動は役員と経営陣だけでなく、内外の利害関係者にも周知されている。(内部の関係者、外部の関係者に対し、情報共有を行い、必要に応じて支援を求める。) | セキュリティインシデントによりサプライヤーからの信頼が落ち、自組織が適切に事業継続できない可能性がある。 |

## 7. 参考文書

- **日本電気協会：電力制御システムセキュリティガイドライン**
  電力の安定供給や電気工作物の保安の確保の妨害等を目的としたサイバー攻撃を脅威として想定し、電気事業者が実施すべきセキュリティ対策の要求事項について規定したガイドライン。電気事業法第 39 条下の技術基準の解釈として位置付けられている。

- **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）**
  発電事業の用に供するものを除く自家用電気工作物の遠隔監視システム等、制御システム等のサイバーセキュリティの確保を目的として、自家用電気工作物を設置する者が実施すべきセキュリティ対策の要求事項について規定したガイドライン。電気事業法第 39 条下の技術基準の解釈として位置付けられている。

- **経済産業省：小売電気事業者のためのサイバーセキュリティ対策ガイドライン**
  小売電気事業者が各々の事業モデルに適したサイバーセキュリティ対策を実践するための重要 10 項目に対する具体的な解釈及び指針を記載したガイドライン。

- **経済産業省：特定卸供給事業に係るサイバーセキュリティ確保の指針**
  特定卸供給事業者が、特定卸供給事業を実施する上で確保すべきサイバーセキュリティとその対策の内容を示した指針。

- **資源エネルギー庁・IPA：エネルギー・リソース・アグリゲーション・ビジネスに関するサイバーセキュリティガイドライン**
  エネルギー・リソース・アグリゲーション・ビジネス（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。

- **各一般送配電事業者：託送供給等約款別冊　系統連系技術要件**
  電気設備を各一般送配電事業者の電力系統に連系するにあたり遵守する必要がある技術要件を定めたもの。2020 年 10 月よりサイバーセキュリティに関する要件が新たに規定され、新たに発電設備を系統に連系する場合又は既存発電設備のリプレース等の場合にサイバーセキュリティ対策が求められる。

- **経済産業省：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）**
  新たなサプライチェーン（バリュークリエイションプロセス）全体のサイバーセキュリティ確保を目的として、産業に求められるセキュリティ対策の全体像を整理したフレームワーク。

- **経済産業省：サイバーセキュリティ経営ガイドライン**
  大企業及び中小企業（小規模事業者を除く）の経営者を対象として、サイバー攻撃から企業を守る観点で、経営者が認識する必要がある「3 原則」、及び経営者がサイバーセキュリティ対策を実施する上での責任者となる担当幹部（CISO 等）に指示すべき「重要 10 項目」をまとめたガイドライン。

- **米国国立標準研究所（NIST）：Framework for Improving Critical Infrastructure Cybersecurity（NIST CSF）**
  組織におけるサイバーセキュリティリスクの低減とより適切な管理を実現することを目的とし、企業・組織の業種に依存しない体系的な対策基準を整理したフレームワーク。

- **米国国立再生可能エネルギー研究所（NREL）：Distributed Energy Resource Cybersecurity Framework (DERCF)**
  Web ベースのアプリケーションとして提供されている分散型エネルギー源のサイバーセキュリティ対策に関するセキュリティ評価サービスである。評価は 3 つの大項目（ガバナンス、技術的管理策、物理的セキュリティ）ごとにまとめられており、計 414 項目の質問に対して 5 段階の成熟度（例：Unimplemented, Partial, Risk Informed, Repeatable, Adaptive）を答えることで、対策状況のスコアリングが行われる。

- **米国エネルギー省：Electricity Subsector Cybersecurity Capability Maturity Model（ES-C2M2）**
  米国の電力業界で活用されているセキュリティレベル向上のためのガイドラインであり、電力会社が現在取り組んでいる対策や手法等の能力レベルの評価と、それによる対策の目標や改善のための優先順位の設定が可能となる。IPA により V1.1 の日本語版解説書・チェックシートが公開されている。

- **ISO/IEC 27019: Information security controls for the energy utility industry**
  エネルギーの安定供給及び信頼性確保を目的としたエネルギーシステム向けの国際標準で、情報セキュリティマネジメントの国際標準規格である ISO/IEC 27002 に対し、エネルギー関連の対策要件を追加して策定された。特に、設備内のプロセス制御機器を対象としたセキュリティ要件が拡充されている。

## 8. 用語集

- CIO（Chief Information Officer）
  企業や組織内において IT 戦略を立案したり実行したりするために設置される責任者のこと。
- CISO（Chief Information Security Officer）
  企業や組織内において実効力のあるセキュリティ施策を行うために設置される責任者のこと。サイバー攻撃やセキュリティ事件・事故の際の判断や対応を行う。
- CSIRT（Computer Security Incident Response Team）
  コンピューターセキュリティに関連するインシデントへの対応を支援する目的で確立される機能のこと。CIRT（Computer Incident Response Team）や、CIRC（Computer Incident Response Center, Computer Incident Response Capability）とも呼称されることがある。[NIST SP 800-61 Rev.2]
- DMZ（DeMilitarized Zone）
  外部ネットワークからの攻撃より、組織内部のネットワークを保護する緩衝地帯のこと。
- IDS（Intrusion Detection System）
  サーバやネットワークの外部との通信を監視し、攻撃や侵入の試み等不正なアクセスを検知して管理者にメール等で通報するシステムのこと。
- IPS（Intrusion Prevention System）
  サーバやネットワークの外部との通信を監視し、侵入の試み等不正なアクセスを検知して攻撃を未然に防ぐシステムのこと。
- ISMS（Information Security Management System）
  組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源を配分して、システムを運用するための仕組みのこと。国際規格 ISO/IEC 27001 に要求事項が定められている。
- PDCA サイクル
  Plan-Do-Check-Act の略で、品質改善や環境マネジメントでよく知られた手法であり、次のステップを繰り返しながら、継続的に業務を改善していく手法の一つのこと。
- VPN（Virtual Private Network）
  インターネットや通信事業者の独自ネットワーク上に構築する仮想の専用線のこと。
- VPP（Virtual Power Plant）
  需要家側のエネルギーリソース、電力系統に直接接続されている発電設備、蓄電設備の保有者もしくは第三者が、そのエネルギーリソースを制御（需要家側エネルギーリソースからの逆潮流も含む）することで、発電所と同等の機能を提供すること。
- インシデント

サイバーセキュリティ分野において、サイバーセキュリティリスクが発現・現実化した事象のこと。

- インシデント対応計画
  障害発生時に、重大な影響を受けるシステムとデータをできるだけ素早く復旧するための手順をまとめた事業継続性計画。

- 可用性
  認可されたエンティティが要求したときに、アクセス及び使用が可能である特性のこと。[JIS Q 27000:2014]

- 監査
  組織内においてサイバーセキュリティ対策が適切に実施されているかどうかを判定するために、監査証拠を収集し、それを客観的に評価するための、体系的で、独立し、文書化したプロセスのこと。監査は、内部監査（第一者）又は外部監査（第二者・第三者）のいずれでも、又は複合監査（複数の分野の組合せ）でもあり得る。[JIS Q 27000:2014]

- 完全性
  正確さ及び完全さの特性のこと。[JIS Q 27000:2014]

- 機密性
  認可されていない個人、エンティティ又はプロセスに対して、情報を使用させず、また、開示しない特性のこと。[JIS Q 27000:2014]

- 脅威
  システム又は組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因のこと。[JIS Q 27000:2019]

- 高負荷攻撃
  システムの可用性を侵害する攻撃手法のひとつで、サーバやネットワークなどのリソースに対して意図的に過剰な負荷をかけたり、脆弱性をついたりすることでサービスを妨害する攻撃のこと。

- サイバー攻撃
  資産の破壊、暴露、改ざん、無効化、盗用、又は認可されていないアクセスもしくは使用の試みのこと。[JIS Q 27000:2019]

- サイバーセキュリティ
  電子データの漏えい・改ざん等や、期待されていた機器、IT システム、制御システム等の機能が果たされないといった不具合が生じないようにすること。

- サプライチェーン
  複数の開発者間でリンクされたリソース・プロセスで、製品とサービスについて、調達にはじまり設計・開発・製造・加工・販売及び購入者への配送に至る一連の流れのこと。[ISO 28001:2007, NIST SP 800-53 Rev.5]

- 残存リスク

リスク対応（回避、低減、移転）後に残るリスクのこと。保有リスクともいう。

- ステークホルダー
  意思決定又は活動に影響を与え、影響されることがある又は影響されると認知している、あらゆる人又は組織のこと。具体的には、株主、債権者、顧客、取引先等である。
- 脆弱性
  一つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点のこと。[JIS Q 27000:2019]
- 脆弱性診断
  システム、ネットワーク、Web アプリケーション等において脆弱性が存在しないかを診断すること。
- セキュリティ事象
  セキュリティ方針への違反若しくは管理策の不具合の可能性又はセキュリティに関係し得る未知の状況を示すシステム、サービス又はネットワークの状態に関連する事象のこと。[JIS Q 27000:2019]
- セキュリティパッチ
  OS やアプリケーションの脆弱性を解消するための追加プログラムのこと。
- セキュリティポリシー
  企業・組織におけるセキュリティに関する理念である意図と方針を経営者が正式に表明したもののこと。セキュリティポリシーに沿って、組織内セキュリティ対策が規定される。
- データ消去
  すべてのユーザアドレス指定可能なストレージ領域のデータに対して、データ抹消処理を行うための論理的な技術を適用し、単純な非侵襲のデータ回復技術から保護すること。[NIST SP 800-88 Rev.1]
- 認証
  エンティティの主張する特性が正しいという保証の提供のこと。[JIS Q 27000:2014]
- ファイアウォール
  ネットワークの結節点となる場所に設置し、ネットワークの通信をさせるかどうかを判断し、許可又は拒否するシステム・装置のこと。
- フェールセーフ
  機器やシステムの設計などについての考え方の一つのことで、部品の故障や破損、操作ミス、誤作動などが発生した際に、なるべく安全な状態に移行するような仕組みにしておくこと。
- 不正アクセス
  本来アクセス権限を持たない者が、システムの内部へ侵入を行う行為のこと。
- ホットスワップ

機器の電源を入れ稼働状態を保ったまま、部品やケーブルなどを交換、装着、抜去すること。また、そのような仕組みやコネクタなどの構造のこと。

- フォレンジック
  インシデント対応や法的紛争・訴訟に際し、電磁的記録の証拠保全及び調査・分析を行うとともに、電磁的記録の改ざん・毀損等についての分析・情報収集等を行う一連の科学的調査手法・技術のこと。

- マルウェア
  セキュリティ上の被害を及ぼすウイルス、スパイウエア、ボットなどの悪意を持ったプログラムを指す総称のこと。これらのプログラムは、使用者や管理者の意図に反して（あるいは気づかぬうちに）コンピューターに入り込み悪意ある行為を行う。

- ランサムウェア
  感染したコンピューター等においてデータが強制的に暗号化される等して、本来の利用が制限され、制限解除と引き換えに、身代金の支払い等が要求されるマルウェアの一種のこと。

- リスク
  目的に対する不確かさの影響のこと。[JIS Q 27000:2019]

- レジリエンス
  システムが以下の状態を維持できること：①悪条件下にあっても、あるいは負荷が掛かった状態であっても、（顕著に低下した状態又は無力化したような状態に陥ったとしても）稼働して、基礎的な運用能力を維持すること②ミッションニーズと平仄が合う時間内に、有効的に運用されている状態に復旧すること。[NIST SP 800-53 Rev.4]

- ログ
  コンピューターの利用状況やデータの通信記録のこと。操作を行った者の ID や操作日付、操作内容などが記録される。セキュリティ上、インシデントの原因追究などに利用する。