資料５－３

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（案）

令和 2 年 12 月

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(制度・技術・標準化)
電力サブワーキンググループ

目次

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策定に当たって

○　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、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ため、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。

○　電力分野におけるサイバーセキュリティ対策は、電気工作物を制御する電力制御システムを中心に行われてきた。現在、一般送配電事業や発電事業等の用に供する電気工作物を制御する電力制御システムについては、電気事業法（昭和 39 年法律第 170 号）に基づく電気設備に関する技術基準を定める省令（平成 9 年通商産業省令第 52 号）、更にはこの詳細を示した「電力制御システムセキュリティガイドライン」に基づき、サイバーセキュリティの確保が求められている。

○　一方、小売電気事業の全面自由化に伴い、電気工作物の維持・運用を行わず、電力の小売供給を行う事業類型として、小売電気事業者が出現しており、2020 年 11 月時点で小売電気事業者数は 684 事業者、全販売電力量に占める新電力の割合は 2020 年 7 月時点で約 18.4％に到達した。

○　小売電気事業においては、電気工作物の維持・運用が行われないため、既存の規定等を参考とし難い場合がある。また、産業界向けの一般的なサイバーセキュリティ対策の方向性を示すガイドラインも存在するが、これらも、小売電気事業に当てはめるに際し、工夫が必要となる場合もある。

○　サイバー攻撃が日々多様化・巧妙化する中では、小売電気事業者がサイバー攻撃を受けた結果、情報漏えいといった自らの被害だけでなく、システムを通じて、他の事業者や関係機関に被害が広がることも想定される。例えば、需要・調達計画が改ざんされる等により、電力の安定供給に影響が生じる可能性があると考えられる。したがって、小売電気事業者も電力分野におけるサイバーセキュリティ対策に主体的に取り組んでいくことが必要である。

○　こうした背景を踏まえ、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(制度・技術・標準化)電力サブワーキンググループの下に、小売電気事業者が中心となり、サイバーセキュリティに関する有識者の協力を得つつ、小売電気事業者が取り組むべきサイバーセキュリティ対策について検討を行う場として、「小売電気事業者のサイバーセキュリティ対策に係る勉強会」（以下「勉強会」という。）を設置した。

○　当該勉強会では、小売電気事業者が自身のサイバーセキュリティ対策において踏まえるべき視点を議論するとともに、小売電気事業者が実施している対策の好事例の共有を行った。

○　本ガイドラインは、当該勉強会における議論を踏まえ、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していくための指針として取りまとめた

ものであり、今後、サイバーセキュリティを取り巻く環境変化を踏まえ、随時見直しを行っていく。

○　上記のとおり、本ガイドラインは小売電気事業者による活用を想定したものであるが、記載されている対策内容は、発電事業者等の他の電気事業者においても実施することが望ましいと考えられるものが多く含まれる。これらの事業者においても、本ガイドラインが活用されることを期待する。

１．はじめに

１．１．小売電気事業へのサイバー脅威と本ガイドライン策定の背景

近年、電力システムを狙うサイバー攻撃の事案は増加傾向にある。従来の情報窃取等を目的とした攻撃だけでなく、フィジカルシステムにダメージを与える攻撃のリスクが増大しており、海外では、送配電システムへの不正アクセス攻撃による停電被害の発生事例や制御システムに対する標的マルウェアを用いた破壊工作事例等も発生している。

我が国の小売電気事業においても、電力自由化以後、数多くの小売電気事業者が事業を開始した一方、顧客サービス用のポータルサイトへの不正アクセス事案を始め、サイバー攻撃による被害も継続的に発生してきた。例えば、2019 年 12 月に、小売電気事業者の会員制 Web サービスが第三者からの大量の不正アクセスを受け、105 名が不正にログインされる事案が発生している。この事案においては、105 名中 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。また、電力分野以外のサービスにおいても、電子送金・決済サービス等でユーザーアカウントへの不正アクセス被害が発生し、数千万円規模の被害が生じた事案等、巧妙な手口のサイバー攻撃によって、従来よりも深刻な被害が発生した事例が増加している。

また、海外においても、プリペイド式電気料金支払いサービスへのランサムウェア感染被害により、料金支払いが停止し、需要家への電力供給が停止した事案[1]や、エネルギー事業者向けデータ交換サービスがサイバー攻撃によりシステムダウンした事例[2]等、電力の安定供給に影響を与えかねない事態が現実味を帯びた危機として迫っている。

小売電気事業者へのサイバー脅威が高まる一方で、小売電気事業者は自らのサイバーセキュリティ対策の実施状況を十分とは捉えていない。2019 年に実施した小売電気事業者 432 者を含む電気事業者へのサイバーセキュリティ対策実態調査では、複数のガイドライン等で小売電気事業者にも共通して求められると考えられる事項を中心に、組織的対策と技術的対策それぞれについての網羅的な設問を設定し、アンケート調査による実態把握を行った。調査結果からは、小売電気事業者としてのリスク評価に基づいた対策の優先度評価や、事業形態等に応じた適切な対策実装計画の検討等への課題意識が明らかとなった。

小売電気事業者におけるサイバーインシデントは、需要家の便益や需給バランスの安定に影響するおそれのある事態であり、社会的責任の観点から事業者の企業価値を毀損しかねない。サイバーセキュリティ対策の実施体制が構築されておらず、計画的なリスク評価やセキュリティ対策の継続的な改善が行われていないと、未対応のサイバーセキュリティリスクの顕在化やリスクの見落とし等によって、本来防げたはずの被害を生じさせ

[1] https://www.bbc.com/news/technology-49125853
[2] https://www.eenews.net/stories/1060078327

てしまう可能性がある。小売電気事業の事業責任者は、経営におけるリーダーシップを発揮し、必要な予算や人材を確保するとともに、サイバーセキュリティ対策が確実に実施されるよう指示及び統制を行うことが期待される。

上記の背景に基づき、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(制度・技術・標準化)電力サブワーキンググループの下に、小売電気事業者が、自らが取り組むべきサイバーセキュリティ対策について主体的な検討を行うための勉強会を設置した。

本ガイドラインは、当該勉強会における議論を踏まえ、小売電気事業者の抱える様々な課題に対し、包括的な視点からサイバーセキュリティ対策を整理したものである。

小売電気事業者が各々の扱う商品種別等の業務類型に適したサイバーセキュリティ対策を実践していくに当たり、対策の方針や具体的な実装方式を検討する際に参照すべき指針及び好事例集として本ガイドラインが活用されることが期待される。

１．２．本ガイドラインの構成と活用方法

本ガイドラインは、小売電気事業者が情報システムを利活用し、そのサービスの品質を高めていくに当たって、効果的なサイバーセキュリティ対策を推進するための指針である。

勉強会の中で、経営者のリーダーシップの下で企業の IT 利活用におけるサイバーセキュリティ対策を推進する「サイバーセキュリティ経営ガイドライン[3]」が多くの事業者に参照されているとの意見があったことも踏まえ、本ガイドラインは、「サイバーセキュリティ経営ガイドラインを踏襲しながら、小売電気事業者におけるより具体的な解釈及び実践のポイントを中心に記載した。

小売電気事業者のためのサイバーセキュリティ対策ガイドラインの策定に当たって
1. はじめに
2. 小売電気事業者のサイバーセキュリティ対策における特徴
3. 小売電気事業者における重要 10 項目の実践規範

小売電気事業者の経営層は、冒頭に記載された小売電気事業者を取り巻くサイバー脅威動向を認識した上で、特に小売電気事業者のサイバーセキュリティ対策における特徴を通読し、対策指示を出す際の要点を把握することが望まれる。小売電気事業を専業として営んでいない事業者においては、事業責任者（小売電気事業を統括し、事業予算の執行権限等を持つ者。セキュリティ対策を含む事業全般に説明責任を負う（例：事業部長等））と読み替えることも可能である。

小売電気事業者のセキュリティ管理責任者（小売電気事業のセキュリティ対策やインシデント対応について、実行責任を負う者（例：担当部長等））は、小売電気事業者における重要 10 項目の実践規範を参照した上で、実際に対策を設計し、実装することが求められる。このため、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」における重要 10 項目の指示事項と対応する形で、勉強会の活動を通じて整理した対策を怠った場合のシナリオと、小売電気事業者における対策実践の好例を示している。また、詳細対策事例として、小売電気事業者における取組のより具体的な内容や、有識者からの助言をもとに整理した知見についても記述した。

特に一定のセキュリティ対策に取り組んでいる事業者は、リスクシナリオを十分に認識した上で、小売電気事業者における対策例も参考にしながら、自社に必要な対策が確実に実装されるようマネジメントを行うための指針として活用されることが期待される。これからセキュリティ対策に取り組む事業者は、小売電気事業者における対策例のうち自

[3] https://www.meti.go.jp/policy/netsecurity/mng_guide.html

社で実行可能と考えられるものを参考にしつつ、対策実装までの道筋を立てるための助けとされたい。

より汎用的な対策事項の詳細な実践例や、特にこれからセキュリティ対策に取り組む事業者における実施事項については、以下の関連資料も参照されたい。

- サイバーセキュリティ経営ガイドライン Ver2.0 実践のためのプラクティス集（IPA）[4]
- 中小企業の情報セキュリティ対策ガイドライン （IPA）[5]

また、電気事業に関するシステムは、電力システムを運用する機器の物理的及び電気的特性と、その機器のサイバーによる制御を組み合わせたサイバー・フィジカル・システムである。この観点から、「サイバー・フィジカル・セキュリティ対策フレームワーク」で提案される三層構造モデル[6]に基づいたアプローチが有用であり、特に第 1 層（企業間のつながり）、第 3 層（サイバー空間におけるつながり）については小売電気事業者においても関連が深い内容になっている。本ガイドラインにおいても、これらを踏まえた内容となっているところ、リスク源の洗い出しと対策要件の特定のプロセス、参考となる対策事例集の参照については、当該フレームワークも参照されたい。

さらに、小売電気事業者が発電事業、特定送配電事業、リソース・アグリゲーション・ビジネス等を兼業することも想定される。このうち、発電事業や特定送配電事業等において電気工作物の運転を管理する情報システムを扱う事業者は、当該システムについては、「電力制御システムセキュリティガイドライン」への準拠が求められる。「電力制御システムセキュリティガイドライン」に準拠した詳細な対策実装や、リソース・アグリゲーション・ビジネスにおいて必要な対策を検討する際には、以下のようなガイドライン等も参考になる。

- 制御システムのセキュリティリスク分析ガイド 第2版（IPA）[7]
- Cybersecurity Framework Version 1.1（米国国立標準技術研究所）[8]
- 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 Ver2.0 （資源エネルギー庁/IPA）[9]

---

[4] https://www.ipa.go.jp/security/fy30/reports/ciso/index.html
[5] https://www.ipa.go.jp/security/keihatsu/sme/guideline/
[6] 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）の概要
https://www.meti.go.jp/press/2019/04/20190418002/20190418002-3.pdf
[7] https://www.ipa.go.jp/security/controlsystem/riskanalysis.html
[8] 米国国立標準技術研究所（NIST） による原文：Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 https://www.nist.gov/cyberframework
IPA による翻訳版 https://www.ipa.go.jp/security/publications/nist/index.html
[9] https://www.meti.go.jp/press/2019/12/20191227004/20191227004.html

２．小売電気事業者のサイバーセキュリティ対策における特徴

「サイバーセキュリティ経営ガイドライン」に示される経営層が認識すべき 3 原則は、以下のとおりである。小売電気事業者の経営層又は事業責任者においても、これらの原則を認識し、小売電気事業の特徴を踏まえた上で自社のサイバーセキュリティ対策を推進することが求められる。

(1) 経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要
(2) 自社は勿論のこと、ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要
(3) 平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、関係者との適切なコミュニケーションが必要

電気事業法に基づき経済産業大臣の登録を受けた小売電気事業者は、需要家への供給能力確保義務を負い、電力の安定供給における重要な役割を果たしている。

小売電気事業者が需要家から預かる個人情報等は、サイバー犯罪者にとっては非常に価値のある攻撃対象であり、常に脅威に晒されている。また、電力の安定供給を担うインフラの一部としてサイバーテロの標的となる事例も海外では見られている。小売電気事業者へのサイバー脅威は顕在化するに至っており、事業責任者はリスクを正しく認識し、適切な対策を推進することが求められるところである。

また、電力の安定供給は一般送配電事業者や発電事業者を始めとする様々な事業者により確保されているものであり、ビジネスパートナーや委託先も含めたサプライチェーンにおけるセキュリティ対策や平時及び緊急時の関係者とのコミュニケーションにおいても、電力システムの特徴を理解した対応が求められる。

２．１．小売電気事業者の事業環境とサイバーセキュリティリスク

電力システムは、様々な電気事業者が重要な役割を担いながら相互に連動することで実現されている（図 1）。一般の需要に応じて電気を供給する役割を担う小売電気事業者にとって、需要家情報の漏えいを防ぎ、需要計画の作成から利用料金請求までの一連の処理を正確かつ遅滞なく行うことはサイバーセキュリティ対策の重要な目標である。

また、小売電気事業者のシステムがサイバー攻撃を受けた場合に、他の電気事業者や関係機関へと被害が拡大すれば、電力の安定供給に支障が生じ、社会的評価を大きく毀損することとなり得る。

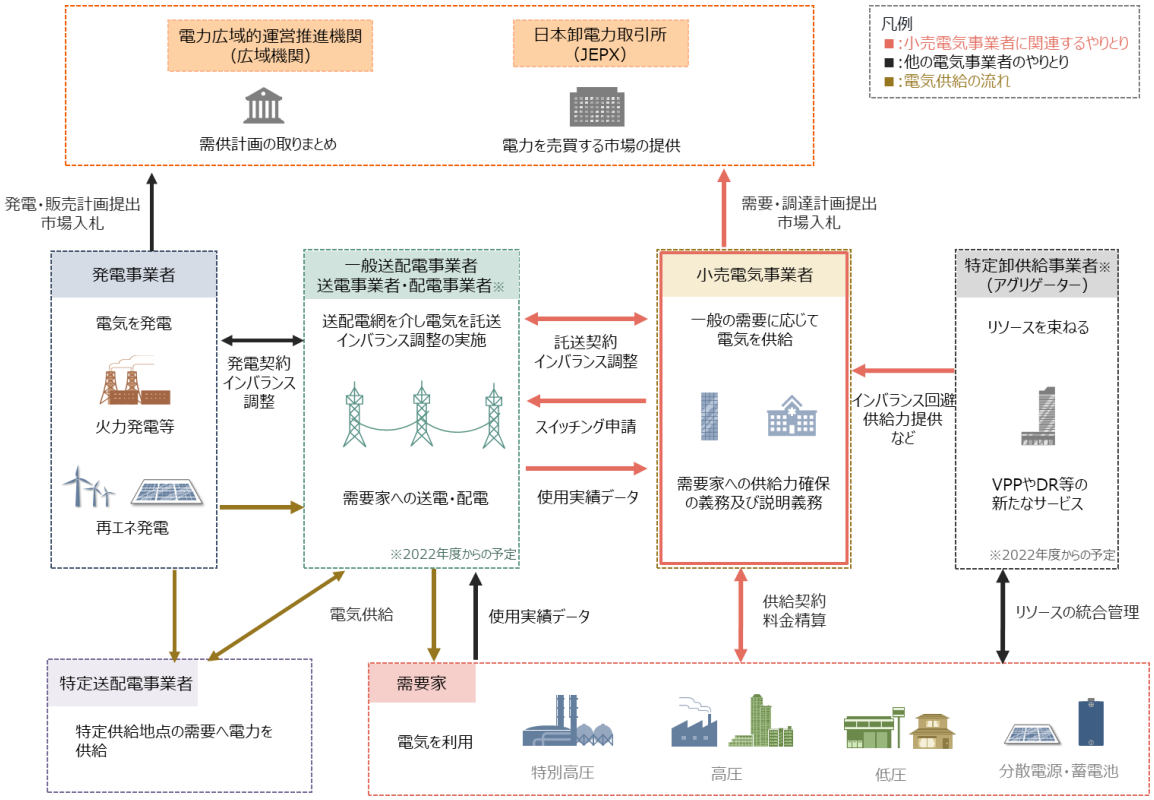

図 1　電力システムにおける小売電気事業者の役割

こうした事業環境を反映し、小売電気事業者が運用する情報システムは、需要家の個人情報や電気利用量等のデータ等を管理する顧客管理機能や、需要予測や最適な供給計画の作成を行うための需給管理機能、利用料金の計算や需要家との料金精算を管理する機能といった様々な機能を持つこととなる。

また、小売電気事業者の業務において、関係機関との需要・調達計画や電気利用実績等の情報連携は必須であり、外部機関の他システムとの通信及びデータの授受が頻繁にある。料金の決済は、金融機関により代行されることが主流であり、決済データの連

携も行われる。さらに、今後はアグリゲーター等の新しい形のサービスとのデータ連携も増加することが予想される(図 2)。

これらの実態を踏まえ、サイバーセキュリティリスクの把握とリスク対応に係る計画の策定を適切に行うことが求められる。

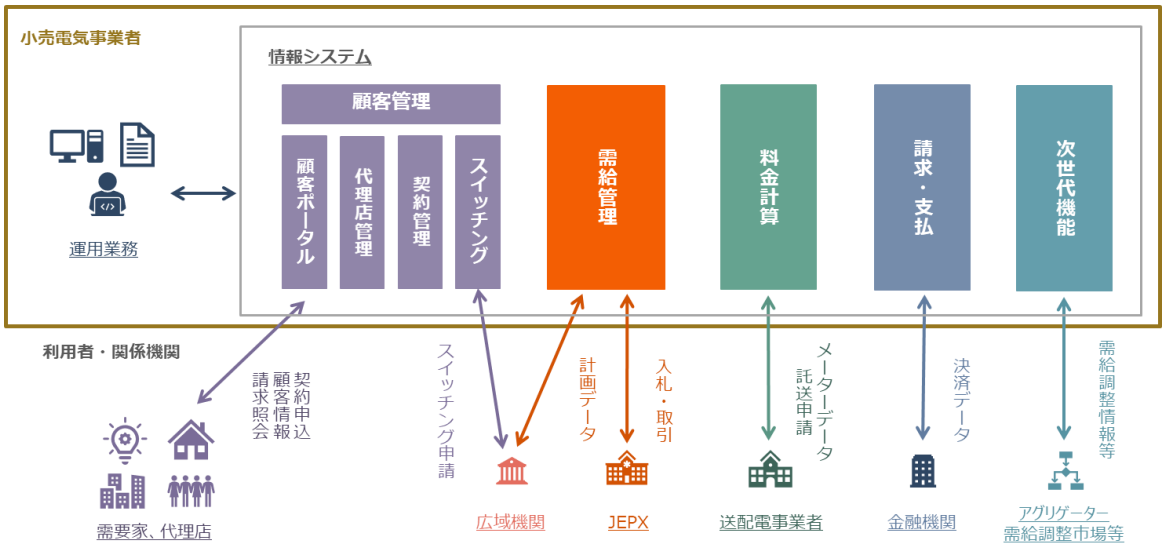

図 2　小売電気事業者のシステムと外部機関の他システムとの連携

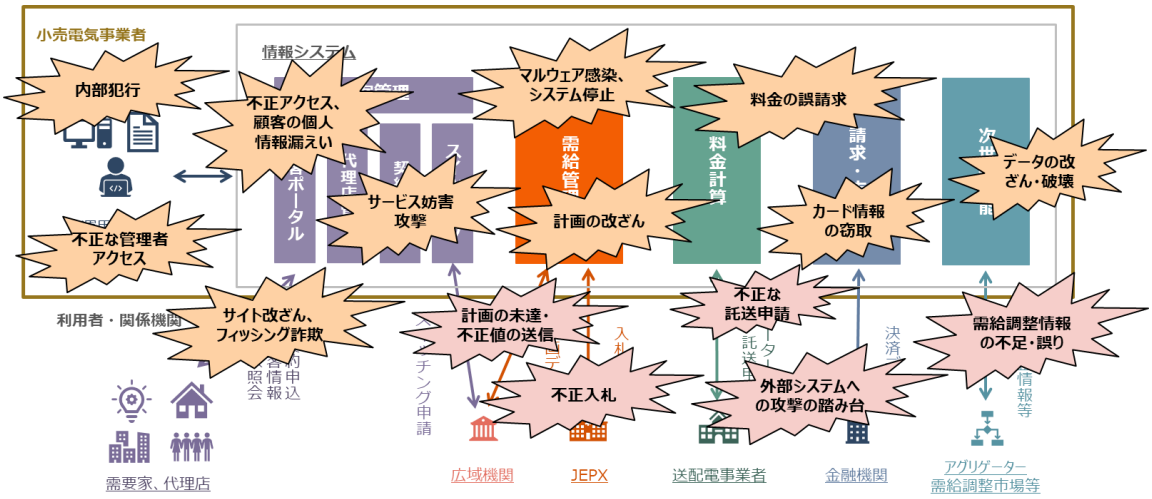

図 3　小売電気事業者に想定されるサイバーセキュリティリスクの例

小売電気事業者のシステムと外部との連携の特徴から、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としては次のような例が考えられる（図 3）。

- 顧客ポータルサイトへの不正アクセスによる顧客の個人情報の漏えいリスク
- 料金計算システムへの改ざん攻撃による需要家への料金の誤請求のリスク
- スイッチング支援システムとの通信への中間者攻撃により需要家のサービス切替えに支障を来すリスク、更に一般送配電事業者の需要家管理に影響が生じるリスク
- 需給管理システムへのランサムウェア感染による電力広域的運営推進機関（以下「広域機関」という。）へ提出すべき需要・調達計画の未達や不正値送信のリスク、それらが広域機関における系統運用業務の不具合又は遅延につながるリスク
- 運用操作端末等へのバックドア設置による一般社団法人日本卸電力取引所（以下「JEPX」という。）への不正入札のリスク　等

小売電気事業の事業責任者は、これらのリスクが自社及び関係機関に与える影響を評価し、リスクの回避・低減を行うか、又はリスクを移転・許容するといった対応方針を定める判断を下す必要がある。さらに、セキュリティ管理責任者を指名し、リスク対応方針に沿った対応が適切に実装されるよう指示を出すことが求められる。

事前の対応に加えて、実際にインシデントが発生してしまった場合に被害を最小化するための準備を行うこともまた重要である。サイバー攻撃は日々新たな手法が生み出されており、完全な対策によりインシデントの発生確率をゼロにすることはできない。インシデントの発生を初期段階で検知し、被害が拡大する前に適切な緊急時対応を行うためには、情報収集を行い、あらかじめ対応計画を用意し、演習等によって習熟することが重要である。

また、インシデント対応計画を検討する際には、BCP（事業継続計画）との統合の視点からの検討を併せて行うことが望ましい。特に、広域機関への需要計画の提出等の即時性が要求される業務については、インシデント対応に時間を要する場合においても業務の継続性が求められることとなる。代替システムによる処理や人手による緊急時運用手順等をあらかじめ用意しておくことで、インシデント発生時の影響を最小化することが可能となる。

なお、自社で発生したインシデントが、関係機関へ深刻な影響を与える事態を回避するためには、連絡体制を準備しておくことが重要である。さらに、セキュリティ関連機関等への連絡手順を整理しておくことで、自社のみでは対応が難しい高度な攻撃を受けた際にも支援を要請することができる。反対に、他社で発生したインシデントによって、自

社が被害を受けることを防ぐために、平時から情報共有を行う関係性を構築しておくことが望ましい(表 1)。

表 1　インシデント発生時の連絡先と自社での対応内容の整理例

連絡先 関係機関	想定されるインシデントの例	平時対応	緊急時対応
広域機関	需要・調達計画の未達、不正値送信	緊急時の連絡先、提出手段の調整	発生している問題の説明、緊急時の提出方法への切替え連絡
JEPX	不正入札、入札不具合	緊急時の連絡先、対応手段の調整	発生している問題の説明
一般送配電事業者	メーターデータの取得不備、誤ったスイッチング	緊急時の連絡先、対応手段の調整	発生している問題の説明、代替手段への切替え連絡
金融機関	間違った料金計算と請求、決済データの不達	緊急時の連絡先、対応手段の調整	発生している問題の説明、訂正フロー等の実行
資源 エネルギー庁	需要家への被害、需給計画への影響、その他全般	緊急時の連絡先等の把握、情報共有	発生している問題の説明、原因究明、行政指導への対応
セキュリティ関連機関 (警察組織、IPA、JPCERT/CC 等)	サイバー攻撃被害	緊急時の連絡先等の把握、脅威情報等の取得	発生している問題の説明、原因究明、対応支援要請
個人情報 保護委員会	個人データの漏えい、滅失又は棄損及びそのおそれ	緊急時の連絡先等の把握	発生している問題の説明、原因究明、再発防止策と漏えいした個人への対応の説明

２．２．小売電気事業者の情報システム構成と想定されるサイバー攻撃

小売電気事業者が需要家情報管理、需給管理に用いるシステムは業務用 IT システムとして構築されることが一般的である。組織の内外と多くの連携を行う小売電気事業者のシステムは、様々な経路からのサイバー攻撃への対策を考慮することが求められる。代表的なシステム構成と想定されるサイバー攻撃として、次のような例が考えられる[10]（図 4）。

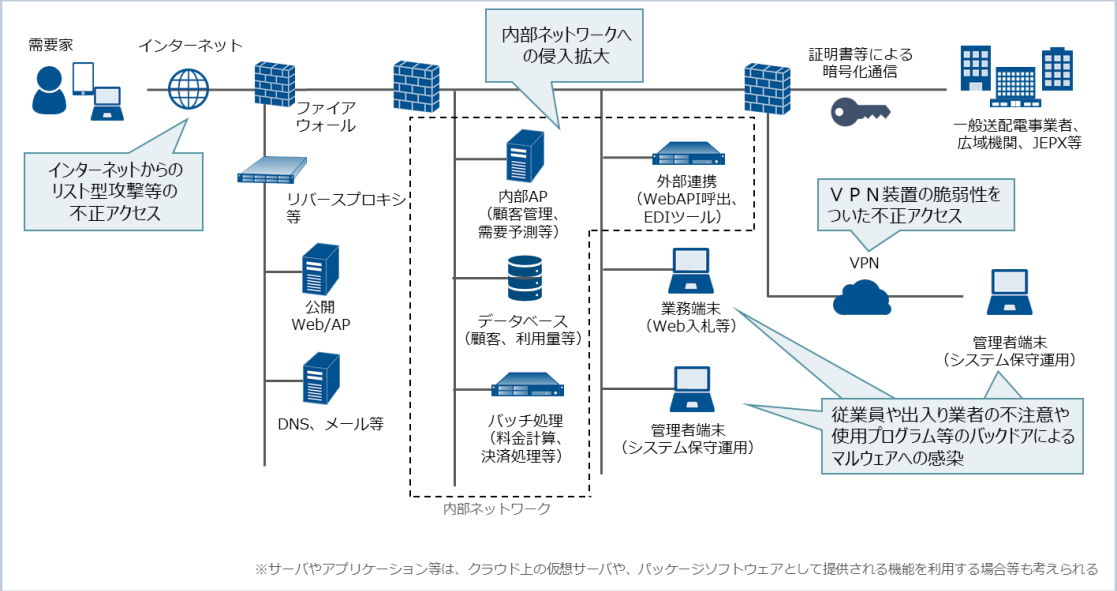

図 4　小売電気事業者の代表的なシステム構成と想定されるサイバー攻撃の例

- 需要家向けインターネットサイトへの不正アクセス（リスト型攻撃等）
- 入札等の業務に用いる端末のマルウェア感染（不正なメールの開封や悪意あるウェブサイトへのアクセス）
- システムの保守運用に用いる端末への悪性 USB メモリ等の接続
- リモートメンテナンス用の VPN 装置の脆弱性をついた不正な遠隔操作
- 侵害された端末を足掛かりにした内部ネットワークへの侵入拡大

こうした攻撃に対処するためには、リスク対応計画に基づきながら、防御・検知・分析の面からセキュリティ対策を実装する必要がある。この際、技術的対策や運用面の対策等の様々な視点を考慮し、システム全体のリスクを最小化するための対策を検討することが求められる。

[10] ここでは、小売電気事業に用いるシステムのみを指し、例えば発電事業を兼業する者が発電事業の用に別途運用するシステムは「電力制御システムセキュリティガイドライン」に準拠した対策を行う必要がある。

２．３．サイバーセキュリティ対策における小売電気事業者の類型

小売電気事業者の事業形態や使用する情報システムの構成に応じて求められる事業者の責任の範囲、求められる水準には差異があると考えられる。サイバーセキュリティにおいても、それぞれの事業形態や利用する情報システムの実態に合った対策を行うことが効果的と考えられる。

勉強会における議論を通じ、小売電気事業者のサイバーセキュリティリスクの評価及び対策において有用であると考えられる類型を検討し、結果を表 2 のとおり整理した。

表２　サイバーセキュリティ対策における小売電気事業者の類型整理

責任範囲の観点	需給管理 BG との関係性	BG 代表　／　BG 所属　／　独立 （BG 全体の需給管理）（BG 代表へ委託）（自身の需給管理）
業態の観点	電圧種別	特別高圧・高圧　／　低圧
	保有する顧客情報の種類	個人顧客　／　法人顧客等
	保有する顧客情報の管理方法	自社管理　／　外部管理等
システムの観点	システム形態	独自構築　／ パッケージ（カスタマイズ利用含む）　／ 外部サービス利用（クラウドサービス等）
	他システム接続	広域機関システム　／ 電力市場システム　／ 一般送配電事業者のシステム　／ 決済機関のシステム

責任範囲の観点では、需給管理を自ら行う事業者と外部へ委託する事業者の区別をバランシンググループ（BG）における関係性から整理した。BG 代表は自身の需給管理に加えて BG 所属企業の需給管理を行うため、データの改ざんやシステムの停止による影響も大きくなる。

業態の観点では、特別高圧・高圧では、供給力の確保においては、1 件当たりの影響が大きい一方、法人向けが中心であり個人情報の扱いは最小限である。一方で低圧は、多数の需要家から大量の個人情報を預かるため、漏えい時の影響が大きくなる。また、保有する顧客情報の管理方法によっては、必要に応じて委託先のチェック等を行う必要がある。

なお、個人情報の取扱いについては、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「個人情報保護法」という。）を参照しつつ、具体的な社内の規則等は関連するガイドラインも参照した上で定めることが望まれる[11]。「個人情報の保護に関する法律についてのガイドライン（通則編）」[12]では、個人データの漏えい、滅失又は毀損（以下「漏えい等」という。）の防止その他の個人データの安全管理のため、事業の規模及び性質等に応じた必要かつ適切な措置を講じなければならないとしている。万が一、個人データの漏えい等の事案が発生した場合は、「個人データの漏えい等の事案が発生した場合等の対応について」（平成 29 年個人情報保護委員会告示第 1 号）[13]に基づき、必要な措置を講じるとともに個人情報保護員会へ報告を行うよう努める必要がある[14]。

また、システムの観点では、システム対策の実施責任範囲の違いから、独自構築、パッケージ、外部サービス利用を類型として整理した。独自構築やパッケージでは技術的対策も含め自身で設計、実装する必要がある一方、外部サービス利用の場合は、対策の不足があったとしても自身では手を入れられないという課題がある。

他システム接続の観点は、自システムと直接接続先として対象になり得る組織のシステムを列挙し、接続の有無による分類を行うものである。

これらの類型に基づき、小売電気事業者における重要 10 項目の実践規範において、対策を怠った場合のシナリオと特に関わりの深い類型を示し、自身のサイバーリスクを把握するための参考情報を提供している。

---

[11] 個人情報保護委員 https://www.ppc.go.jp/personalinfo/legal/

[12] https://www.ppc.go.jp/personalinfo/legal/2009_guidelines_tsusoku/

[13] https://www.ppc.go.jp/personalinfo/legal/leakAction/leakAction_detail/

[14]令和 2 年 6 月に公布された改正個人情報保護法では、漏えい等が発生し、個人の権利利益を害するおそれがある場合に、個人情報保護委員会への報告及び本人への通知が義務化されるため留意が必要（施行は公布後 2 年以内）。

３．小売電気事業者における重要 10 項目の実践規範

小売電気事業の経営者又は事業責任者は、セキュリティ管理責任者に対し、達成すべきセキュリティ目標を指示し、確実に実施させることが必要である。「サイバーセキュリティ経営ガイドライン」では、サイバーセキュリティ経営の重要 10 項目として以下を示している。

＜経営者がリーダーシップをとったセキュリティ対策の推進＞

（サイバーセキュリティリスクの管理体制構築）

指示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

指示2 サイバーセキュリティリスク管理体制の構築

指示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

（サイバーセキュリティリスクの特定と対策の実装）

指示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

指示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

指示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

（インシデント発生に備えた体制構築）

指示7 インシデント発生時の緊急対応体制の整備

指示8 インシデントによる被害に備えた復旧体制の整備

＜サプライチェーンセキュリティ対策の推進＞

指示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

＜ステークホルダーを含めた関係者とのコミュニケーションの推進＞

指示 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

小売電気事業者のセキュリティ管理責任者は、以上の重要 10 項目の指示を、小売電気事業者の特徴を理解した上で解釈し、対策を実装することが求められる。以降では、小売電気事業者の視点から、各指示事項に対応して、対策を怠った場合のシナリオ及び小売電気事業者における対策実践の好事例を示した。加えて、特に対策実践のためのノウハウ等が不足している中小規模の事業者を対象に、勉強会等で共有された対策事例の詳細を記載しているため、併せて参考にされたい。

３．１．サイバーセキュリティリスクの管理体制構築

指示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

サイバーセキュリティリスクを経営リスクの一つとして認識し、組織全体での対応方針（セキュリティポリシー）を策定させる。

小売電気事業者のサイバーセキュリティリスクを、その責務や事業環境を踏まえた上で理解し、事業全体に適用するセキュリティポリシーを定める。

対策を怠った場合のシナリオ

- 小売電気事業者としてのセキュリティポリシーを策定し、周知していないと、事業全体のセキュリティ対策が一貫性を欠いてしまうおそれがある。
- 小売電気事業者としての責任や特有の事業リスクが対応方針へ反映されず、重要な対応事項の検討に漏れが生じるおそれがある。
  - 需要家の個人情報保護対策が不十分なものとなってしまうおそれがある。（**個人情報を保有**する事業者）
  - セキュリティインシデント発生時に緊急の需要計画を作成する方針等を準備できないおそれがある。（特に**電圧種別が特別高圧・高圧**の事業者）
- 電力の安定供給のためサイバーセキュリティ対策に取り組む姿勢が、関係する組織、機関等へ伝わらず、信頼性を高めることができないおそれがある。（特に**需給管理を BG 代表として**又は**独立して行う**事業者）

小売電気事業者の対策実践例

- 公開ガイドライン等の記載事項を参考にし、自らの組織の対応方針を検討した内容を反映することで、セキュリティポリシーを作成する。
  - IPA「中小企業の情報セキュリティ対策ガイドライン」に記載の内容やサンプルを参考に実施する。
  - 経済産業省「サイバーセキュリティ経営ガイドライン」や ISO/IEC 27001 等の国際規格を参考として実施する。
  - 特に重要となる個人情報の保護に関する方針は、個人情報保護法等を踏まえて、別途策定する。（**個人情報を保有**する事業者）
- 策定したセキュリティポリシーは定期的な見直しを行う。

- セキュリティポリシーを社内外に浸透させる。
  - 社内ポータルサイトへセキュリティポリシーを掲載し、周知する。
  - 社外向けウェブサイト等にセキュリティポリシーを掲載し、対外発信する。
  - 経営方針内でセキュリティポリシーを参照し、位置付けを明確化する。
  - 毎年セキュリティ啓発月間を設定し、セキュリティポリシーを浸透させる。

[詳細対策事例]

[最小限のセキュリティポリシーからの開始]

特に小売電気事業を開始して間もない場合等、セキュリティポリシーを未作成の事業者においては、最小限の基本理念を定めたセキュリティポリシーを始めに作成し、改訂を経て内容の拡充を図る方針が有効であるとの意見があった。始めに策定するセキュリティポリシーは一般公開されたサンプルを活用することも考えられる。

IPA の「中小企業の情報セキュリティ対策ガイドライン」では、これからセキュリティ対策に取り組む中小規模の事業者が、始めに取り組むべき対策事項が情報セキュリティ 5 か条としてまとめられている。また、付録 2 として、全 1 ページの「情報セキュリティ基本方針（サンプル）」を公開している。こうしたサンプルを基に自社の事情を反映した修正を加え、自社のセキュリティポリシーと位置付けることも可能である。

[第三者認証取得を通じたセキュリティポリシーの精緻化]

一定のセキュリティ対策に取り組んでいる事業者が、より高度な対策水準を目指すための方針を策定する場合等において、情報セキュリティマネジメントの国際規格である ISO/IEC 27001 の枠組みに従うことで、網羅的な視点を盛り込んだセキュリティポリシーを構成することが可能であるとの意見があった。

ISO/IEC 27001 の枠組みに従い策定した対策方針の正当性を自社で判断することが難しいと考えた事業者において、同規格に基づく ISMS 認証制度を活用することで、事前審査プロセスにおいて認証機関からの確認と助言によりセキュリティポリシーの内容の調整・改善を行ったという事例がみられた。ISMS 認証の制度では、審査対象事業者の成熟度に比して適切な水準の対策であることが重視されるため、必ずしも大規模事業者でなくとも、会社の規模や形態に応じた取組が可能であるとの意見が得られた。

指示２ サイバーセキュリティリスク管理体制の構築

サイバーセキュリティ対策を行うため、サイバーセキュリティリスクの管理体制（各関係者の責任の明確化も含む）を構築させる。その際、組織内のその他のリスク管理体制とも整合を取らせる。

小売電気事業の体制内でセキュリティ管理責任者を任命し、実施体制の構築を行う。小売電気事業以外に複数の事業を営む事業者は、組織の中の小売電気事業の位置付けや、グループ企業との関係性等を踏まえて整合を取る。

対策を怠った場合のシナリオ

- 小売電気事業のサイバーセキュリティリスク対応における責任が曖昧になり、全体を統括し、対策を推進する者がいなくなるおそれがある。
- 関係する部門との間でサイバーセキュリティ対策体制の整合性が保てないおそれがある。
  - 小売電気事業以外にも複数の事業を営む事業者では、サイバーセキュリティ対策の役割分担を明確化しないと、全社組織が責任を負う範囲と、小売電気事業を所管する部署が責任を負う範囲が不明確になってしまうおそれがある。
  - グループ企業のリスク管理体制との不整合が起き、過剰な対策の実施や小売電気事業特有のリスクへの対応漏れが発生するおそれがある。
  - 組織全体の個人情報の保護に関する方針と小売電気事業における個人情報の保護に関する方針の間で内容の一貫性が保たれないおそれがある。（**個人情報を保有**する事業者）

小売電気事業者の対策実践例

- 小売電気事業のセキュリティ管理責任者を任命し、役割を明確にする。
- セキュリティ管理責任者を経営層や事業責任者が担うことで、管理体制を公認する。
- 全社的なリスク管理体制の一環としてサイバーセキュリティリスク管理体制を決定する。
- 経営会議の議題にサイバーセキュリティ対策を含めるなどして、経営層への定期的な説明機会を設ける。
- 内部監査を定期的に実施し、体制が機能していることを確認する。
- 全社やグループのセキュリティ組織と小売電気事業を含む事業部門が連携して対策を推進する。

- 個人情報保護法等を踏まえて設置された個人情報管理責任者を、経営層が担当することで一貫性を保つ。（**個人情報を保有**する事業者）

［詳細対策事例］

［**セキュリティ専任担当を配置できない状況での体制構築**］

社員数が限られており、セキュリティ専任担当者を確保することが難しい状況において、情報システム担当者や個人情報管理担当者等の複数人が兼務体制を取ることで、セキュリティ対策推進の責任を持つ事務局を組成したという事例がみられた。また、セキュリティ管理責任者が各部署においても部署内のサイバーセキュリティを担当する者を指名し、組織全体としての意識を高める取組が行われている事例もみられた。

［**各部門のセキュリティ担当者による定期的な会議体の設置**］

大規模な組織においては、全社のセキュリティ管理責任者が全体的な方針のみを示し、個別の対策内容は部門の担当者の裁量により決定されるという役割分担が多くみられた。こうした体制では、部門間の対策方針が不整合となるおそれがあるが、各部門にセキュリティの担当者を配置し、全社のセキュリティ管理責任者と各部門の担当者全員が参加する会議を定期開催するという取組事例があった。会議の場でセキュリティポリシーの解釈の統一や情報交換を行うことで、各部門の対策の質が向上しているとの意見があった。

指示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

サイバーセキュリティリスクへの対策を実施するための予算確保とサイバーセキュリティ人材の育成を実施させる。

小売電気事業のサイバーセキュリティ対策への予算割当ての確保と、利用するシステムの開発と運用においてセキュリティ対策を実践する人材の育成等を行う。

対策を怠った場合のシナリオ

- 小売電気事業のセキュリティ対策に必要な予算が確保できず、リスクを低減するための対策の実行や、信頼できる外部ベンダへの委託が困難となるおそれがある。
  - 不正ログイン対策等の小売電気事業に必要なサイバーセキュリティリスクへの対策予算が確保されず、システムに対策を実装できなくなるおそれがある。（特に**システム形態が独自構築・パッケージ**の事業者）
  - 利用する外部サービスを検討する際に、十分なセキュリティ対策を行っているサービスを選択するための予算が確保できないおそれがある。（特に**システム形態が外部サービス利用**の事業者）
  - インシデント発生時に、対応に必要となるコストを用意できないおそれがある。
- 小売電気事業のセキュリティ対策に必要な能力を持った人材の確保、育成を行うことができなくなるおそれがある。
  - セキュリティ対策の計画を立てる人材がいないため、適切な方針の策定や体制を構築できなくなるおそれがある。
  - セキュリティ対策の妥当性を判断できる人材を確保することができず、外部ベンダの提案内容やコストの妥当性を判断できなくなるおそれがある。（特に**システム形態が独自構築・パッケージ**の事業者）
  - 外部サービスを選定する際に、サイバーセキュリティリスク対応の妥当性を評価することができず、対策が不十分なサービスを選択してしまうおそれがある。（特に**システム形態が外部サービス利用**の事業者）
  - 業務プロセスやシステムの運用において、サイバーセキュリティリスクを軽減するための設計を行えなくなるおそれがある。

小売電気事業者の対策実践例

- 小売電気事業に必要なサイバーセキュリティ対策を明確にし、具体的な予算額を要求する。

- インシデント対応を見越した予備費等をセキュリティ対策予算に組み入れる。
- リスク管理会議等において、セキュリティ投資の長期見通しを定期的に議論する。
- システムベンダ等とサイバーセキュリティ対策の面での協力体制を構築する。
- サイバーセキュリティ対策の人材育成計画を作成し、勉強会や研修等を企画する。
- 社外のセミナーや研修への参加、資格試験等を活用した能力開発を推進する。
  - IPA や JPCERT/CC 等の主催するセミナーやプログラム等への参加[15]
  - 地域のサイバーセキュリティに関連した取組やコミュニティへの参加
  - 情報セキュリティマネジメント試験[16]等の資格試験の受験を通じた学習
  - 情報処理安全確保支援士[17]等の取得を通じた専門人材育成
  - 産業サイバーセキュリティセンターにおける育成プログラム受講

[詳細対策事例]

[経営層への定期的な情報提供]

十分なサイバーセキュリティ対策予算の確保には経営層のリスク認識が不可欠であるが、重大な脅威が顕在化した際に、一から説明の準備と予算確保の調整を開始すると、多くの時間と労力を必要とするばかりか、割り当てるべきリソースが既に枯渇している可能性もある。ある事業者では、平時からサイバー脅威の動向に関する情報を定期的に経営層に提供し、経営層が一定の予算を毎年度確保する必要性への認識を高めていた。また、緊急に対応が必要な脅威が顕在化した際にも、事前知識が共有されているため、意思決定を迅速化することができているとの意見が得られた。

[15]オンラインで参照可能な映像コンテンツも提供されている。
https://www.ipa.go.jp/security/keihatsu/videos/

[16] 情報処理技術者試験の一区分で、IT の安全な利活用を推進する者を対象とする。基本的知識・技能に該当。
https://www.jitec.ipa.go.jp/1_11seido/seido_gaiyo.html

[17] サイバーセキュリティを推進する人材を対象とした国家資格。 https://www.ipa.go.jp/siensi/index.html

［役割の付与による育成］

サイバーセキュリティ対策を計画する際に、実行に必要な専門知識を有する人材が自社にいない場合がある。こうした場合に、あえて先行して予算を確保し、実行計画に着手することで社内の担当要員のスキルアップを促す事例の共有があった。情報システム担当者がセキュリティ対策の実装責任を担うことで、サイバーセキュリティ技術を学習しながら実行を主導し、徐々に専門性が高まったという。外部の専門人材を獲得する例と比べ、自社システムの現状とサイバーセキュリティ技術の双方の知見を持つことで優位な側面もあるとの意見があった。

３．２．サイバーセキュリティリスクの特定と対策の実装

指示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

経営戦略の観点から守るべき情報を特定させた上で、サイバー攻撃の脅威や影響度からサイバーセキュリティリスクを把握し、リスクに対応するための計画を策定させる。その際、サイバー保険の活用や守るべき情報について専門ベンダへの委託を含めたリスク移転策も検討した上で、残留リスクを識別させる。

小売電気事業の特性及び事業環境に基づいたサイバーセキュリティリスクの分析を行い、自社の事業形態、成長戦略を踏まえたリスク対応計画を策定する。また、残留リスクを認識し、対応方針を定める。

対策を怠った場合のシナリオ

- 小売電気事業に伴うサイバーセキュリティリスクへの対応が適正に行われず、想定外の損害を被るおそれがある。

  （想定されるリスクシナリオの例）

  - 顧客ポータルサイトへの不正アクセスによる顧客の個人情報の漏えいリスク（**個人情報を保有**する事業者）
  - 料金計算システムへの改ざん攻撃による需要家への料金の誤請求のリスク
  - スイッチング支援システムとの通信への中間者攻撃により需要家のサービス切替えに支障を来すリスク、更に一般送配電事業者の需要家管理に影響が生じるリスク
  - 需給管理システムへのランサムウェア感染による広域機関へ提出すべき需要計画の未達や不正値送信のリスク、それらが広域機関における系統運用業務の不具合又は遅延につながるリスク（特に**需給管理を BG 代表として又は独立して行う**事業者）
  - 運用操作端末等へのバックドア設置による JEPX への不正入札のリスク
- 事業環境の分析が行われず、電気事業法や個人情報保護法等の関連法規の考慮漏れが起こるおそれがある。
- 事業形態に応じた適切なリスク対応策が検討されず、リスクの大きさに対して適正な成熟度の対策が行われないおそれがある。反対に、過剰な対策により事業そのものに悪影響を及ぼしてしまうおそれもある。
- 残留リスクが識別されず、リスクへの対応が放置されてしまうおそれがある。

小売電気事業者の対策実践例

- 経営部門が中心となり、事業リスクの視点からの分析を実施する。
  - 需要家情報保護の観点から重要な情報を識別する。
  - 供給力確保の継続性の観点からリスクを分析する。
- 情報資産やシステムアプリケーション資産を棚卸してリスクを把握する。
- 内外の環境変化に関する情報やベンダの見解を考慮したリスク評価を実施する。
- 残留リスクに対して有事の際の対応を考慮に入れたリスク許容度を判断する。
- サイバーセキュリティ保険へ加入する。

[詳細対策事例]

[**個人情報のリスク分析と対応**（個人情報を保有する事業者）]

小売電気事業者は、小売供給契約を結ぶために需要家の個人情報を預かり、扱う個人情報のリスクに応じた適切な管理を行うことが求められる。特に、一般消費者向けに低圧の電気を供給する事業者は、大量の個人情報を扱うことになる。

顧客アカウントへの不正アクセスによる被害規模を見積もる際には、個人情報の量、性質を考慮し、過去の事例等を参考にしながら、補償リスクや信頼の毀損といった側面も含めた評価を行う必要があるとの意見が複数寄せられた。

アクセス管理等の手段でリスクを低減する他、始めから必要以上の個人情報を取得しない、クレジットカード情報の非保持化[18]等の対応を行うことで、リスクを回避している事例も共有された。

[18] 経済産業省「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画」
https://www.meti.go.jp/press/2018/03/20190304004/20190304004.html

［サイバーセキュリティ保険への加入］

残留リスクに対し、リスクの移転を行うためにサイバーセキュリティ保険へ加入することは有効な選択肢のひとつである。保険によりインシデント対応の費用を補填する用意を整えておくことで、支援要請等に係る費用も捻出しやすくなる。

実際にサイバーセキュリティ保険に加入している事業者からは、扱う情報の質や量により想定被害額が大きく異なるため、事業の形態や規模に応じた契約内容の調整を行うことが重要との意見があった。

また、想定される被害額の他に、被害の発生確率はリスクの試算に大きく関わるため、あらかじめ一定の水準のセキュリティ対策を実践している事業者は、保険費用を抑えることができる可能性があるとの知見が共有された。

［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）の活用］

CPSF の第Ⅱ部では、複雑なサプライチェーン構造を持つシステムへのサイバー攻撃を想定したリスク分析手法及び分析例を、三層構造モデル（「第 1 層：企業間のつながり」「第 2 層：フィジカル空間とサイバー空間のつながり」「第 3 層：サイバー空間におけるつながり」）を用いて整理している。

小売電気事業者の用いる情報システムでは、特に第 1 層における組織のセキュリティマネジメント、第 3 層におけるデータの送受信、加工・分析、保管等において想定されるセキュリティインシデントやリスク源の枠組みを、自社システムのリスク分析をする上での参考として活用することが考えられる。

指示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

サイバーセキュリティリスクに対応するための保護対策（防御・検知・分析に関する対策）を実施する体制を構築させる。

サイバーセキュリティリスクの分析結果を踏まえ、実際にリスクへ対応するための保護対策を、小売電気事業者の情報システムの特性を踏まえながら実装する。

対策を怠った場合のシナリオ

- 適切なサイバーセキュリティ対策が行われず、サイバー攻撃を受ける確率が増すとともに、実際に被害が生じた際の規模が大きくなるおそれがある。
  - 需要家向けポータルのユーザー認証機能における対策が十分でなければ、不正ログインによる情報漏えいや金銭被害等が起こるおそれがある。（**個人情報を保有**する事業者）
  - 機微なデータが暗号化されていないと、万が一個人データ等を窃取された場合に、データの中身を実際に暴露されるおそれがある。
  - 業務端末のマルウェア対策が不十分な場合、遠隔アクセスツールによる侵入を受けたり、ランサムウェアに感染し身代金を請求されたりするおそれがある。
  - リモートアクセスの安全性が確保されていない場合、攻撃者に不正アクセス経路として悪用され、情報システムの内部ネットワークへの侵入を許し、データを改ざんや破壊されるおそれがある。
- ネットワークや機器のログデータから脅威を監視し、不正を検知する仕組みを構築していない場合、サイバー攻撃を受けた事実に気付くことができず、対応が遅れ被害を拡大させてしまうおそれがある。
- 従業員にセキュリティ対策を実行させるための教育と運用を行わない場合、攻撃可能な経路を増やしてしまうおそれがある。

小売電気事業者の対策実践例

○共通して求められるシステムの防御・運用における対策

- 需要家のユーザーアカウント保護のための対策を行う。
  - 安全なパスワードの設定を強制する。
  - パスワードの使い回しに対する警告文を記載する。
  - 2 段階認証や多要素認証を実装する。

- 個人情報等の機微なデータは、機密性を保護するため、暗号化して扱う。（**個人情報を保有**する事業者）
  - 個人データは、暗号化した安全なネットワーク等を介してやり取りする。
  - 保管する個人データは暗号化し、アクセス制限をかける。
- 重要なデータはバックアップを取得し、保管する。
  - 需要家の情報や電力使用量、料金精算に関するデータ等は、定期的にバックアップを取得する。
  - バックアップデータは、通常のデータとは異なる場所や領域に保管する。
- 業務に用いる端末のセキュリティ対策を行う。
  - 不要な機能やソフトウェア、機器接続ポート等を無効化する。
  - OS やセキュリティ対策ソフト等のアップデートを遅滞なく適用する。
  - 外部記憶媒体等の管理ルールを定め、利用制限やウイルススキャン等を行う。
  - メールのフィルタリングにより不正なファイルの添付されたメールの隔離等を行う。
  - 端末の不審な挙動等を認知した際の対応を手順化し、周知・教育する。
  - EDR 等を活用し、端末の不審な挙動に対し、自動的な検知と対応を行う。
- ネットワークセキュリティ対策を行う。
  - セキュリティ要求レベルに応じたネットワーク分割を行う。
  - ファイアウォールは、必要最低限の通信要件を許可するよう設定する。
  - UTM、IDS/IPS 等の高度なネットワーク防護製品を導入する。
- ネットワークやサーバ等のログを取得し、不正通信を監視する。
  - ログデータを定期的に分析し、不正な通信の痕跡を確認する。
  - SIEM 等を活用し、不正なイベントを速やかに検知し、対応の判断を行う。
- システムや運用端末へのリモートアクセスは安全な方式で行う。
  - VPN や電子証明書等を用いた端末認証を行う。
  - アクセスログなどを定期的に分析し、不正アクセスを検知する。
  - 多要素認証を実装し、なりすまし対策を行う。

- 従業員へのセキュリティ教育を行う。
  - 基礎的なセキュリティ対策に関する研修を全従業員に対して実施する[19]。
  - システム管理者などを対象に役割に応じた個別の教育を実施する。

○特に**システム形態が独自構築・パッケージの事業者**向けのシステム防御対策

- 社内のシステム開発規程等に企画・設計段階からセキュリティ要件を策定することを含める。
- Web アプリケーションのセキュリティ対策を行う。
  - Web アプリケーション開発におけるセキュア開発のガイドライン等[20]を活用する。
  - WAF を導入し、不正なリクエストを遮断する。
- システムの脆弱性対応を行う。
  - 脆弱性対策情報を収集し、必要なセキュリティパッチの適用を行う。
  - 定期的な脆弱性検査を実施する。
  - ペネトレーションテスト等のセキュリティ診断を実施する。

[詳細対策事例]

[**システム更改のタイミングを有効活用する**（特にシステムを独自構築している、又はパッケージをカスタマイズ利用している事業者）]

一貫性のあるセキュリティ対策を実装するためには、システム開発工程の初期からセキュリティ設計の検討を行うセキュリティ・バイ・デザインの実践が重要である。一方で、既に稼働中のシステムでは、抜本的な修正を速やかに行うことは難しい場合がある。こうした場合において、システムの更改のタイミングで、次期システムのセキュリティ要件に現状の課題を正確に反映することで効率的に対応している事例が得られた。この際、IPA の非機能要求グレード[21]を活用することで、網羅的な要件の検討がなされている。

また、システム更改前のリスクが残留した段階では、脅威監視機能を強化することで、不正アクセス等を検知した際には、速やかな対応を行う体制が構築されており、リスクの低減が図られている。

[19] IPA による啓発動画コンテンツ等の活用も考えられる。
https://www.ipa.go.jp/security/keihatsu/videos/

[20] 例として IPA「安全なウェブサイトの作り方」等がある。https://www.ipa.go.jp/security/vuln/websecurity.html

[21] システム構築の上流工程強化（非機能要求グレード）
https://www.ipa.go.jp/sec/softwareengineering/std/ent03-b.html

［一般消費者向けサービスの不正アクセス対策（特に低圧の電気を提供する事業者）］

決済サービスを中心に、過去に漏えいしたパスワードリストを用いて大量の不正アクセスを試行する攻撃による被害等が多発している。ユーザーがパスワードを使い回している場合、パスワード認証のみでサービス提供側で不正アクセスを防ぐことは難しく、2 段階認証や多要素認証による対応が必要となる。オープンソースソフトウェアや ID サービスプロバイダ等を活用することで導入の障壁を下げる工夫が考えられる。

小売電気事業者でも、特に個人情報を取り扱う一般消費者向けサービスは、攻撃者の標的となる可能性があり、実際に複数の被害事例も存在することから、2 段階認証等の実装に取り組んでいる事業者もいる。実装が難しい場合であっても、パスワードの使い回しを避けるよう警告する等の対応は推奨されるとの意見があった。

また、一般消費者向けサービスはオープンなインターネットアクセスを伴うことから、他のシステム機能よりも高リスクであると判断し、脆弱性診断等を実施する事業者も多かった。全てのシステムを対象にセキュリティ検証を行うことが難しい場合も、優先すべきシステムから着手することで、極力リスクを低減する工夫がみられた。

［組織全体のセキュリティ基礎能力の底上げ］

組織全体で従業員のセキュリティに関するリテラシーを高めることで、サイバー攻撃に対する人的リスクの低減や、攻撃を受けた際の認知や対処行動を適正化し被害を最小化する試みを実施する事業者が多くみられた。

具体的なアプローチとしては、E ラーニングの実施や標的型攻撃メール訓練の実施などによって、不審なファイルの添付されたメールを受信した際の行動を改善する取組が主であった。標的型攻撃メール訓練は、添付ファイルを開封した従業員を責めるのではなく、その後の対応を含めた行動の改善に注力すべきとの知見が共有された。

［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）の活用］

CPSF の第Ⅲ部では、三層構造モデル（「第 1 層：企業間のつながり」「第 2 層：フィジカル空間とサイバー空間のつながり」「第 3 層：サイバー空間におけるつながり」）に基づいた実施したリスク分析に対応する対策要件と対策例集がまとめられている。

対策例集は、3 段階のレベルに分けて記載された対策例と、対策を実装する主体が具体的にまとめられており、自社のシステムにおける対策実装方式を検討するための参考とすることができる。

指示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

計画を確実に実施し、改善していくため、サイバーセキュリティ対策を PDCA サイクルとして実施させる。その中で、定期的に経営者に対策状況を報告させた上で、問題が生じている場合は改善させる。また、ステークホルダーからの信頼性を高めるため、対策状況を開示させる。

サイバーセキュリティ対策の実施状況の評価と改善を行う。自社のセキュリティ対策への取組を開示し、需要家や関係機関からの信頼性を高める。

対策を怠った場合のシナリオ

- サイバーセキュリティ対策の実施状況の評価を行わない場合、課題の洗い出しが行われず、未対応のリスクが残留したり、非効率な対策を継続したりしてしまうおそれがある。
- 対策の見直しと改善を行わない場合、小売電気事業者としての事業環境の変化への対応や新たな脅威への対策を行えないおそれがある。
- 需要家や関係機関からサイバーセキュリティ対策への信頼が得られない場合、事業機会の損失や事業環境の悪化につながるおそれがある。

小売電気事業者の対策実践例

- 年間のセキュリティ対策計画を作成する。
- セキュリティ対策の実施状況の評価と改善の検討を定期的に行う。
  - 「SECURITY ACTION」制度[22]を活用し、自社の対策状況の把握と改善を行う。
  - 小売電気事業を対象範囲に含めて ISMS 認証を取得、運用する。
- 経営層の参加する会議体で定期的な進捗報告とレビューを実施する。
- 脅威情報等を収集し、セキュリティ対策計画の見直しに活用する。
- 定期的な脆弱性診断を実施し、検出事項に対する改善活動を行う。（特に**システム形態が独自構築・パッケージ**の事業者）
- 外部機関へ監査を依頼し、専門家からの助言への対応を行う。
- 自社のウェブサイト等でセキュリティ対策への取組状況を発信し、需要家や関係機関からの信頼性を高める。

22 IPA「SECURITY ACTION」 https://www.ipa.go.jp/security/security-action/sa/index.html

［詳細対策事例］

［SECURITY ACTION への参加］

「SECURITY ACTION」は、中小企業を対象とした情報セキュリティ対策への取組の自己宣言を行う制度である。特徴として、これからセキュリティ対策に取り組む企業のためのシンプルな目標が設定されていること、自己点検と自己宣言に基づく制度であり負荷が低いこと、ロゴマークの利用による対外発信が可能であること等が挙げられる。

取組段階には 2 段階あり、一つ星は「中小企業の情報セキュリティ対策ガイドライン」付録の「情報セキュリティ 5 か条」に取り組むことを宣言する、二つ星は同付録の「5 分でできる！情報セキュリティ自社診断」で自社の状況を把握した上で、情報セキュリティ基本方針を定め、外部に公開したことを宣言することが基準となっている。

［たすき掛け方式による内部監査の実施］

社内のサイバーセキュリティ対策の PDCA サイクルが機能しているかを詳細に確認するために、内部監査は有効な手段である。しかし、規模が大きくない事業者では情報セキュリティに関する内部監査を行うための十分な監査体制を保有していない状況にあることも考えられる。

ある事業者の事例では、複数の部署にまたがり、それぞれのセキュリティ担当者が相互の内部監査を行う「たすき掛け方式」を採用することで、客観的な検証を行っていた。セキュリティポリシー等に共通指標がある場合、外部組織による監査と比較してより具体的な確認を行うことができるメリットもある。客観性の担保のためには、指示系統の近すぎる部門同士の相互監査は行わないなどの調整や工夫が求められる。

３．３．インシデント発生に備えた体制構築

指示７ インシデント発生時の緊急対応体制の整備

影響範囲や損害の特定、被害拡大防止を図るための初動対応、再発防止策の検討を速やかに実施するための組織内の対応体制（CSIRT 等）を整備させる。被害発覚後の通知先や開示が必要な情報を把握させるとともに、情報開示の際に経営者が組織の内外へ説明ができる体制を整備させる。また、インシデント発生時の対応について、適宜実践的な演習を実施させる。

サイバーセキュリティインシデントの発生に備え、初動対応と再発防止策の検討を実施するための計画と体制を整備する。全社やグループの緊急対応組織が別個に存在する場合は、役割分担や連絡のルールなどを明確化する。

インシデントによる被害の発覚時には、影響範囲を踏まえ、需要家、広域機関、JEPX、一般送配電事業者、提携する決済機関等に対し、必要に応じた通知を行うための体制及び手続等を定める。また、関係法令等に則り、必要に応じて資源エネルギー庁等への報告を行う。

また、演習や訓練を実施し、インシデント対応体制が実際に機能するように練度を高める。

対策を怠った場合のシナリオ

- 緊急時の対応体制が整備されていないと、影響範囲等の特定や被害の拡大防止のための作業を速やかに行うことができず、需要家や自社の小売電気事業に与える損害が大きくなってしまうおそれがある。
- 関係機関への連絡が適時に行われない場合、本来防げたはずの二次被害が発生し、より広範囲に影響を及ぼす被害を招いてしまうおそれがある。

小売電気事業者の対策実践例

- 小売電気事業の特性を踏まえた被害シナリオへの対応計画を作成する。
  - 需要家の個人データの漏えい等につながるおそれのあるインシデントへの対応（**個人情報を保有**する事業者）
  - 特定顧客への供給力確保に大きな影響を与えるおそれのあるインシデントへの対応（特に**電圧種別が特別高圧・高圧**の事業者）
  - 需給計画の提出や電力市場に影響を与えるおそれのあるインシデントへの対応（特に**需給管理を BG 代表として**又は**独立して行う**事業者）

- 利用料金の計算と請求に支障を来すおそれのあるインシデントへの対応
- 利用している外部サービスが停止した場合の対応（特に**システム形態が外部サービス利用**の事業者）

- インシデントへの緊急対応体制を整備する。
  - 想定されるインシデントへの対応手順書、連絡ルールを作成する。
  - 社内の緊急連絡網の作成と維持管理を行う。
  - 委託先ベンダ等との緊急連絡体制を構築し、合意する。
  - CSIRT を組成する。
  - SIM3[23]等の成熟度モデルを活用し、CSIRT 運用を継続的に改善する。
- 社外の関係機関への連絡先一覧を作成する。
- インシデントハンドリング演習を実施する。
  - 情報連絡演習や机上シナリオ演習等を企画し、実施する。
  - 標的型攻撃メール訓練を実施し、従業員教育を行う。
  - 外部の組織が主催する演習や訓練等に参加する。

[23] Open CSIRT Foundation「SIM3 Model & References」 https://opencsirt.org/csirt-maturity/sim3-and-references/

［詳細対策事例］

［通常運用手順と緊急対応手順の関連付け］

緊急対応手順書を作成したものの、通常使用する文書ではないため、緊急時に直ちに参照することができない、内容が更新・維持されていないという問題が発生することがある。こうした問題を解消するために、通常の運用手順書内に緊急時対応手順をフローチャートとして統合し、緊急時の対応を関連付けるという工夫を行ったという事例の共有があった。これにより、緊急時にも平時と同じ枠組みの中で手順の参照を行うことが可能となる他、運用手順書の記載を見直す際にも、緊急対応手順の改訂要否の検討が漏れにくくなる効果も期待できる。

［特定の状況を想定したシナリオ型演習］

インシデントへの対応訓練を定期的に実施する際に、毎回異なる特定の状況を想定することで対応の計画と手順を多角的な視点から検証する事例が複数寄せられた。

具体的なシナリオの例としては、個人情報等の機密データへの不正アクセスが疑われる事象が発生した場合、需給管理システムが停止した場合、JEPX との通信や一般送配電事業者の託送業務システムとの通信が失敗する場合といった様々な状況を想定した演習が実施されていた。

［机上演習等の活用］

自社のシステムへ疑似的なサイバー攻撃を加える形の演習は、システムの一時的な停止を行うか、同構成のシステムを用意する等の必要が生じるという理由から、常時需給管理と入札に対応する小売電気事業者にとっては障壁が高いという意見があった。

ある事業者では、緊急時の対応計画の検証を主要目的とした机上演習や、連絡体制が機能することを確認するための情報連絡演習等を積極的に活用しており、必ずしもシステムを停止させなくとも大きな効果を得られているとのことであった。

また、技術的なインシデント対応能力を向上させる目的では、外部の組織が主催するハンズオン研修等を受講することで、基本技術を習得するという方法も考えられる。

［インシデント報告時の具体的な連絡先の整理］

インシデント報告を行う際に、連絡先の情報が適切に維持管理されていないと、速報性が損なわれ、防げたはずの被害の拡大や信用の失墜につながってしまうおそれがある。連絡先の担当者情報を正しく保つとともに、代表連絡先等を併せて控えておくことで不測の事態に備えることが望ましいとの意見があった。

（主な連絡先の例）

- 資源エネルギー庁（全般）

https://www.enecho.meti.go.jp/category/electricity_and_gas/electric/summary/entry/

- IPA（脆弱性関連情報の届出）

https://www.ipa.go.jp/security/vuln/report/index.html

- JPCERT/CC（インシデント対応支援）

https://www.jpcert.or.jp/form/

- 警察組織（サイバー犯罪）

https://www.npa.go.jp/cyber/soudan.htm

- 個人情報保護委員会（個人データの漏えい等の対応）

https://www.ppc.go.jp/personalinfo/legal/leakAction/

等

指示８ インシデントによる被害に備えた復旧体制の整備

インシデントにより業務停止等に至った場合、企業経営への影響を考慮していつまでに復旧すべきかを特定し、復旧に向けた手順書策定や、復旧対応体制の整備をさせる。BCP との連携等、組織全体として整合のとれた復旧目標計画を定めさせる。

また、業務停止等からの復旧対応について、適宜実践的な演習を実施させる。

インシデントの影響で実際に小売電気事業を停止せざるをえない状況に至った場合を想定し、復旧目標や復旧に向けた手順書、体制等の整備を行う。内容は BCP との整合性を考慮する。

また、演習や訓練を実施し、復旧手順が実際に機能するように練度を高める。

対策を怠った場合のシナリオ

- インシデントによる被害からの回復や通常業務への復旧を適切な時間内に行うことができず、事業経営に致命的な影響を与えるおそれがある。
  - 需要家の個人データの漏えい等への補償対応等を行うことができず、企業価値の毀損や訴訟リスクを抱えるおそれがある。（**個人情報を保有**する事業者）
  - 需要計画提出を中断せざるを得なくなった場合に、再開の見通しを立てられないことで、関係機関への二次的な影響が長期にわたり継続してしまうおそれがある。（特に**需給管理を BG 代表として又は独立して行う**事業者）
  - 適切な支援要請先をあらかじめ把握できていないために、本来得られるはずであったサポートを受けられなくなるおそれがある。
- 演習や訓練を実施していないと、計画したとおりに復旧手順に基づいた対応を行うことができず、必要以上に時間を要したり、復旧に失敗したりするおそれがある。
  - 記載された手順や連絡先に誤りがあり、復旧計画が機能しないおそれがある。
  - バックアップデータ取得の失敗等のミスが見過ごされてしまい、復旧のために必要な材料が揃わなくなってしまうおそれがある。

小売電気事業者の対策実践例

- インシデントにより小売電気事業に被害が生じた状況からの復旧計画を作成する。
- BCP とインシデントからの復旧計画を統合する。
- システムのバックアップを取得し、復旧作業や再構築の実施手順を確立する。（特に**システム形態が独自構築・パッケージ**の事業者）

- システムの停止等を想定した代替策による事業継続手段を確立する。
- 危機管理広報の一環として、一般向けの報道対応体制を準備する。
- サイバーインシデントに伴う想定被害事象と対応する連絡先の一覧を整理する。

（連絡先の一例）

  - 個人データの漏えい等：需要家、個人情報保護委員会、資源エネルギー庁 等
  - 需給計画への影響：広域機関、JEPX、資源エネルギー庁　等
  - 利用料金計算への影響：需要家、一般送配電事業者、資源エネルギー庁、電力・ガス取引監視等委員会　等
  - 不正アクセス、サイバー犯罪が疑われる事象：セキュリティ関連機関（IPA、JPCERT/CC）、警察組織、資源エネルギー庁　等

- サイバー攻撃被害が発生した後の対応を想定した演習や訓練を行う。
  - 代替運用への切替えと切戻しの手順をテストする。
  - 事業継続訓練のシナリオにサイバーセキュリティ対策の継続の観点を含める。
- CSIRT が復旧プロセスの計画と実施を統制する。

［詳細対策事例］

［**外部機関との予備のデータ送受信方式を用意する**（他システム接続を行う事業者）］

セキュリティインシデントが発生した際に、被害箇所によっては外部機関とのデータ送受信を平時の方式で行うことができなくなってしまう場合がある。小売電気事業者が関係機関とやりとりをする需要計画や入札データ、電力使用量データ等は一定の即時性が求められる側面があり、被害からの回復に時間がかかる場合にも代替手段により運用されることが望ましいとの意見があった。

ある事業者では、広域機関や JEPX 等の外部機関のシステムと平時は自社の需給管理用システムを介したシステム間通信を行っているが、非常時を想定して Web 画面からのアップロード手順をあらかじめ代替手段として整備している。この例では、Web アップロード方式を行う場合にも証明書の設定等が必要であるため、緊急時の一刻を争う状況下で速やかな対応を行うためには、事前に手順化とテストを済ませておくことが重要であるという知見が共有された。

［システムバックアップとリカバリテストの実施］

ランサムウェア等のマルウェア被害では、データの暗号化や破壊等によって、システムの復旧や業務の再開に必要なデータが失われてしまう場合がある。こうした場合には、バックアップデータからの復元を行うことが事業継続のために必須の要件となる。

ある事業者では、システムからのバックアップ機能のテストに加えて、バックアップデータのリストアを通じたシステム復旧までのテストを適宜実施する運用を行っている。大規模なバックアップとリストアのテストは、実施機会を確保することが簡単ではないが、システム更改の機会に全体を通したテストを実施する、システムのメンテナンス時に可能な範囲のバックアップとリストアのテストを同時に行うといった工夫が共有された。

［外部サービスの停止を想定した BCP（システム形態が外部サービス利用の事業者）］

クラウドサービスの普及等に伴い、自社でシステム基盤を保有せずに外部のサービスを活用し、効率的なサービス提供を行う事業者も多い。一方、外部のクラウドサービス内で発生したインシデントやシステム障害が、自社システムの停止や不具合に直結してしまう事例も発生しており、事業継続リスクへの備えが求められるところである。

紹介された事例には、異なるクラウドサービス基盤間で冗長構成を採用するものがあった。さらにリスクを低減した事例としては、別個のクラウドサービス事業者の基盤上に同一のシステムを構築し、一方の基盤上でサービス停止等が発生した際は、他方の基盤上でリソースの割り当てを増強した上でアクセスを集中させる形でフェイルオーバー構成を実現するといったものがある。

コスト等の制約により複数のクラウドサービスを利用することが難しい場合には、複数の地域システム基盤（例：東京拠点と大阪拠点）を選択可能なクラウドサービスを利用し、地域冗長性を有するフェイルオーバー構成を実現する例もある。

３．４．サプライチェーンセキュリティ対策の推進

指示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

監査の実施や対策状況の把握を含むサイバーセキュリティ対策の PDCA について、系列企業、サプライチェーンのビジネスパートナーやシステム管理の運用委託先等を含めた運用をさせる。システム管理等の委託について、自組織で対応する部分と外部に委託する部分で適切な切り分けをさせる。

システムの開発や運用の委託先企業や BG を通じた関係を持つ事業者とのサイバーセキュリティ対策における役割分担を明確化し、委託先や取引先においてもサイバーセキュリティ対策の継続的改善に取り組まれていることを確かめる。

対策を怠った場合のシナリオ

- 委託先や取引先のセキュリティ対策が不十分であった場合、それらの事業者を踏み台としたサイバー攻撃の被害を自社が受けるおそれがある。さらに、自社を踏み台としたサイバー攻撃によって他社が二次被害を受けるおそれもある。
- インシデント発生時の原因究明などの際に、委託先や取引先からの協力が得られないおそれがある。
- 自社が責任を負う範囲と外部委託先の責任範囲が適切に識別されていないと、どちらも自身の責任範囲と認識していないリスクへの対応が漏れるおそれがある。

小売電気事業者の対策実践例

- 取引先、委託先との契約書へサイバーセキュリティ上の責任を明記する。
- グループ企業や BG 所属企業間で適用するセキュリティガイドラインを作成し、各社の対応を標準化する。（**BG 代表又は BG に所属する事業者**）
- サービス利用約款におけるサイバーセキュリティ上の規定を確認する。（特に**システム形態がパッケージ、外部サービス利用**の事業者）
- 対策状況チェックリストを利用し、委託先へ対策状況の申告を求める。
- 委託先への監査規則を設定し、必要に応じて監査を実施する。
- 個人情報保護に関する責任を契約内容に具体的に定める。（**個人情報を保有**する事業者、**顧客情報を外部管理**している事業者）

［詳細対策事例］

［**システムベンダとのセキュリティ要件の共有**（特にシステム形態が外部サービス利用、パッケージのカスタマイズの事業者）］

一般にクラウドサービスの利用時や、システムベンダにパッケージ等をカスタマイズしたシステムの構築・運用を委託している場合には、システムの管理が委託先に任せきりになってしまうことも多い。しかし、こうした場合にはベンダの把握していない脅威情報や規制対応要件への対応漏れが生じ、リスクを抱えてしまう可能性がある。

ある事業者では、システム管理の大部分をベンダに委託しながらも、利用者でも設定が可能な項目や制限等の情報開示を積極的に依頼し、共に管理する姿勢を保っている。責任を共有することで、脅威への対応方針等も共通の認識を持つことができている。

また、パッケージをカスタマイズしている事業者において、SLA を明文化することで、自社の定めるセキュリティポリシーとの乖離がないことを確認するという取組がみられた。

［**委託先検査方法の使い分け**］

多くの委託先や取引先を抱える大規模事業者で、効率的に各社の検査を行うため、複数の検査方法を使い分けているという事例があった。扱う情報量の差に着目し、検査の程度を調節している。大量のデータを扱うシステムベンダ等に対しては直接現地監査を行う一方、少数の機密性の低い情報のみを扱う委託先に対しては、簡易なチェックリストによる確認のみを行うなどの濃淡がつけられている。この方法は、委託先や取引先へ一律に自己申告型のチェックリストを配布して確認する方式等と比較して、チェック観点の認識齟齬等によるリスクの把握漏れが起こりにくいと思われる。

３．５．ステークホルダーを含めた関係者とのコミュニケーションの推進

指示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

社会全体において最新のサイバー攻撃に対応した対策が可能となるよう、サイバー攻撃に関する情報共有活動へ参加し、積極的な情報提供及び情報入手を行わせる。また、入手した情報を有効活用するための環境整備をさせる。

セキュリティ専門機関からの情報発信の利用や電気事業者間の情報共有の取組等に参加する等して、サイバー攻撃に関する情報の入手及び提供を行う。

対策を怠った場合のシナリオ

- 最新のサイバー脅威情報を収集しない場合、新たな手口による深刻な被害の発生を防ぐことができないおそれがある。
- 社内で発生したセキュリティインシデント情報の報告と共有を行わない場合、同様の手口による他組織や関係機関への被害を未然に防止することができず、コミュニティに協調の姿勢が生まれにくくなってしまうおそれがある。

小売電気事業者の対策実践例

- IPA、JPCERT/CC 等の提供する注意喚起情報、脅威情報を収集する。
- システムベンダやグループ CSIRT 等からの情報提供を受ける。
- セキュリティベンダ等に脅威情報の分析支援を依頼する。
- 業界や地域の情報共有コミュニティへの参加・交流を通じた情報共有を行う。
- 資源エネルギー庁や IPA、JPCERT/CC 等への自社インシデント報告及び相談を行う。
- 個人データの漏えい等のインシデントは、個人情報保護法等を踏まえて個人情報保護委員会への報告を行う。（**個人情報を保有**する事業者）

［詳細対策事例］

［公的機関の情報源からの情報収集］

IPA や JPCERT/CC 等の公的機関は、無料でアクセス可能なサイバーセキュリティ関連の情報発信を積極的に行っている。ここでは、その一例を示す。

（重大な脅威等をまとめた定期レポート）

- IPA「情報セキュリティ 10 大脅威」
  https://www.ipa.go.jp/security/vuln/
- JPCERT/CC「Weekly Report」
  https://www.jpcert.or.jp/wr/

（脆弱性や対策等に関連する速報性の高い情報）

- IPA「重要なセキュリティ情報一覧」
  https://www.ipa.go.jp/security/announce/alert.html
- JPCERT/CC「注意喚起情報」
  https://www.jpcert.or.jp/at/
- JPCERT/CC「早期警戒情報」
  https://www.jpcert.or.jp/wwinfo/

（主にセキュリティ技術者等が確認する脆弱性情報の詳細）

- JVN (Japan Vulnerability Notes)
  https://jvn.jp/index.html

［情報共有コミュニティへの参加］

業界や地域の情報共有コミュニティ等に参加することで、他社からの情報収集及び自社の取組や課題、インシデント事例等の共有を通じて、コミュニティ全体としてのセキュリティ対策レベルを向上させることができる。自社の課題を共有し対策を議論することは、同様の課題を抱える他社にとっても参考となることに加え、他社にも自社へより具体的な情報を提供するモチベーションを与えることができる。

電力分野における代表的な情報共有コミュニティとしては、電力 ISAC が挙げられる。電力 ISAC は 2017 年に発足し、サイバーセキュリティに関する情報の収集・分析及び会員間での共有を活動内容として、2020 年 8 月時点で小売電気事業者を含む 51 企業・団体が加入している[24]。

[24] 電力 ISAC https://www.je-isac.jp/

（付録）用語集

(1) **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。

(2) **オープンソースソフトウェア**

利用者の目的を問わずソースコードを使用、調査、再利用、修正、拡張、再配布が可能なソフトウェアの総称。

(3) **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。

(4) **個人情報の保護に関する法律（平成 15 年法律第 58 号、個人情報保護法）**

個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とした個人情報の取扱いに関する法律。

(5) **サイバー攻撃**

コンピュータシステムやネットワークに、悪意を持った攻撃者が不正に侵入し、データの窃取・破壊や不正プログラムの実行等を行うこと。

(6) **サイバーセキュリティ**

サイバーセキュリティとは、電子データの漏えい・改ざん等や、期待されていた IT システムや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。

(7) **サイバーセキュリティリスク**

サイバーセキュリティリスクとは、サイバーセキュリティに関連して不具合が生じ、それによって企業の経営に何らかの影響が及ぶ可能性のこと。

(8) **残留リスク**

リスク対応（回避、低減、移転）後に残るリスク。保有リスクともいう。

(9) **情報処理推進機構（IPA）**

日本の IT 国家戦略を技術面・人材面を支えるために設立された独立行政法人。

(10) **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。具体的には、株主、債権者、顧客、取引先等である。

(11) **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。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。

(12) **セキュリティ・バイ・デザイン**

企画・設計の段階で情報セキュリティを確保する方法。発生する問題と対応方法を設計段階から想定することで手戻りのコスト等が削減される。

(13) **中間者攻撃**

二者間の通信へ不正な方法によって割り込み、通信の傍受・盗聴を行い、入手した情報をもとに更なる攻撃を仕掛けるサイバー攻撃。

(14) **電力 ISAC**

日本の電気の安定供給を守るためサイバーセキュリティの観点で関係する事業者間で情報共有・分析等を行う組織。

(15) **バックドア**

コンピュータへ不正に侵入するための入り口のこと。バックドア設置とは、入り口を内部に設置するサイバー攻撃。

(16) **ビジネスパートナー**

業務の委託先や受託元、物品・サービスの調達先等の取引関係のある企業のこと。

(17) **標的型攻撃**

特定の組織内の情報や人物を狙って行われる高度なサイバー攻撃。

(18) **ファイアウォール**

内部ネットワークに侵入する不正アクセスを阻止するシステム。

(19) **フェイルオーバー構成**

稼働中のシステムに問題が発生した際に、自動的に別途用意されている待機システムに切り替える仕組み。

(20) **ペネトレーションテスト**

明確な意図を持った攻撃者にその目的が達成されてしまうかを検証するためのセキュリティテストの一種。

(21) **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、ボットなどの悪意のあるプログラムを指す総称。これらのプログラムは、使用者や管理者の意図に反して（あるいは気付かぬうちに）コンピュータに入り込み悪意ある行為を行う。

(22)ランサムウェア

マルウェアの一種であり、感染したコンピュータ等では、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る。制限解除と引き換えに、身代金の支払い等が要求される。

(23)リスク

国際規格(ISO/IEC 27000)では、「諸目的に対する不確かさの影響」と定義されている。

(24)リスク対応(回避、低減、移転、保有)

対処の方法には、大きく分けて「リスク回避」、「リスク低減」、「リスク移転」、「リスク保有」の 4 つがある。なお、さらに詳細化した分類として、JIS Q 0073 リスクマネジメント―用語では、リスク回避、機会を追及するためのリスクを取る又は増加させる、リスク源の除去、起こりやすさを変更すること、結果を変えること、リスク移転、リスク保有の 7 分類が定義されている。

① リスク回避

「リスク回避」とは、脅威発生の要因を停止あるいは全く別の方法に変更することにより、リスクが発生する可能性を取り去ることである。例えば、「インターネットからの不正侵入」という脅威に対し、外部との接続を断ち、Web 上での公開を停止してしまうような場合などが該当する。

② リスク低減

「リスク低減」とは、脆弱性に対してセキュリティ対策を講じることにより、脅威発生の可能性を下げることである。ノートパソコンの紛失、盗難、情報漏えいなどに備えて保存する情報を暗号化しておく、サーバ室に不正侵入できないようにバイオメトリック認証技術を利用した入退室管理を行う、従業員に対するセキュリティ教育を実施することなどが該当する。

③ リスク移転

「リスク移転」とは、リスクを他社などに移すことである。例えば、リスクが顕在化したときに備え、保険で損失をカバーすることや、組織内の IT システムの運用を他社に委託し、契約などにより不正侵入やマルウェア感染の被害に対して損害賠償などの形で移転すること等が該当する。

④ リスク保有

「リスク保有」とは、ある特定のリスクにより、起こり得る損失の負担を受容することである。

(25)リスク評価

リスクの大きさが、受容可能か又は許容可能かを決定するために、リスク分析の結果をリスク基準(リスクの重大性を評価するために目安とする条件であり、組織の目的並びに外部環境及び内部環境に基づいたもの)と比較するプロセスのこと。

(26)リスク分析

リスクの特質を理解し、リスクレベル(ある事象の結果とその起こりやすさとの組合せとして表現される、リスクの大きさ)を決定するプロセスのこと。

(27) ログ

コンピュータの利用状況やデータの通信記録。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。

(28) BCP(Business Continuity Plan)

企業が自然災害、テロ攻撃、サイバー攻撃などによる被害が発生した場合において、中核となる事業の継続、早期復旧を実現するために、平時及び緊急時における事業継続のため手段等を取り決めておく計画のこと。

(29) CSIRT(Computer Security Incident Response Team)

インシデントの発生に対応するための体制のこと。

(30) EDR(Endpoint Detection and Response)

パソコンや携帯電話等のエンドポイントに対するサイバー攻撃を検出して対応するシステム。

(31) IDS(Intrusion Detection System)

ネットワークを監視し不正アクセスの検知を実施するシステム。

(32) IPS(Intrusion Prevention System)

ネットワークへの不正アクセスを検知し通信を遮断するシステム。

(33) ISO/IEC 27001

情報セキュリティマネジメントシステム(ISMS)に関する国際規格。情報の機密性・完全性・可用性の 3 つのバランスをマネジメントし、情報を活用するための組織の枠組みを示している。

(34) JPCERT/CC

一般社団法人 JPCERTコーディネーションセンターの略称。サイバーセキュリティの情報を収集し、インシデント対応の支援、サイバーセキュリティ関連情報の発信などを実施している。

(35) OS (Operating System)

システム全体を管理し、オペレーション(操作・運用・運転)を司るシステムソフトウェア。Windows や Linux 等を指す。

(36) PDCA

Plan-Do-Check-Act の略。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。

1. Plan:問題を整理し、目標を立て、その目標を達成するための計画を立てる。
2. Do:目標と計画をもとに、実際の業務を行う。
3. Check:実施した業務が計画取り行われて、当初の目標を達成しているかを確認し、評価する。
4. Act:評価結果をもとに、業務の改善を行う。

(37) SIEM(Security Information and Event Management)

セキュリティ/ネットワーク機器のログを収集し分析することでサイバー攻撃を検知するシステム。

(38) SLA(Service Level Agreement/サービス水準合意)

サービスを提供する事業者が契約者に対して、サービスの水準を保証する契約。

(39) UTM(Unified Threat Management)

複数の異なるセキュリティ機能を一元管理し、サイバー攻撃等の脅威からネットワークを保護する管理手法。

(40) VPN(Virtual Private Network)

インターネット上に仮想の専用線を設け、プライベートなネットワークを拡張する技術及びそのネットワーク。

(41) WAF(Web Application Firewall)

Web アプリケーションのネットワークに配置し、通信の内容を機械的に検査するサイバー攻撃への対策の一種。

(42) 2 段階認証/多要素認証

アクセス権限を取得するための本人確認に用いられる認証の方式。同一の認証要素を 2 つ組み合わせた場合が 2 段階認証であり、異なる要素を 2 つ組み合わせた場合は、2 要素認証となる。