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

令和４年４月制定

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

目　次

1　特定卸供給事業に係るサイバーセキュリティ確保の指針の必要性等

（1）　本指針の必要性及び構成

東日本大震災以降、分散リソースや需要家側エネルギーリソース（太陽光発電、定置用蓄電池、ネガワット等）の導入拡大に伴い、新たなビジネス領域として、エネルギー・リソース・アグリゲーション・ビジネスが注目されている。

電力システム改革や IoT の発展、災害の激甚化等を踏まえ、アグリゲーションビジネスを新たなエネルギー産業として育成し、分散型・需要家側デバイスをエネルギーシステム全体の中で効果的に活用していくことは、更なる分散リソースの導入拡大や災害時・緊急時のレジリエンスを向上させる観点から重要である。

このため、自家発等の分散リソースを広く供給力として国が把握するとともに、分散リソースを束ねて供給力や調整力として活用するビジネス環境を整える観点から、強靱かつ持続可能な電気供給体制の確立を図るための電気事業法等の一部を改正する法律（令和２年法律第４９号）第２条の規定による改正後の電気事業法において、アグリゲーターを特定卸供給事業者として新たに位置付けることとされた。

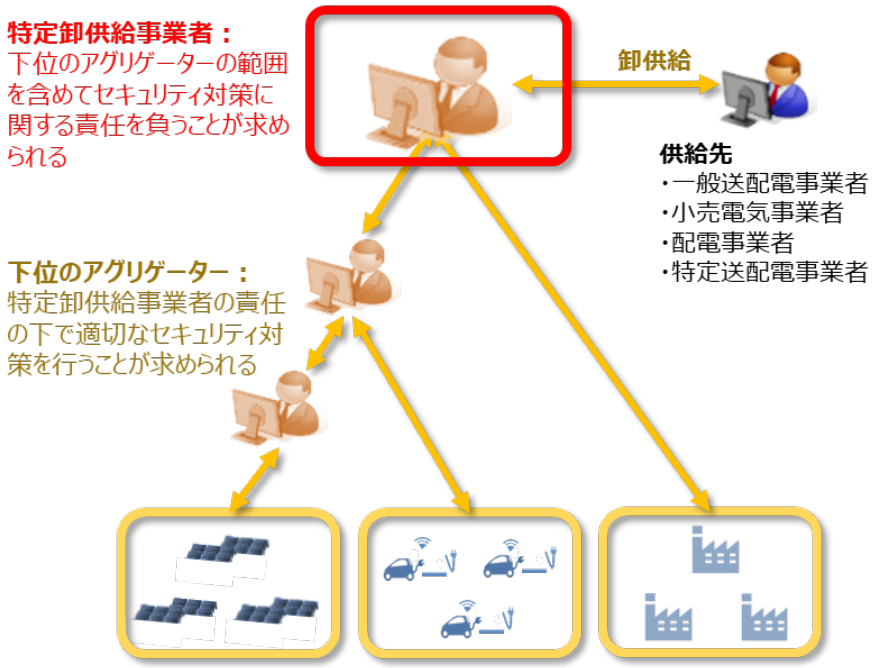
特定卸供給事業者は、多様なリソースを、システム等を用いて遠隔で制御するというその事業の性質から、サイバーセキュリティを確保する対策が必要である。

本指針は、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すことを目的としたものである。

なお、本指針に記載された事項にとどまらず、特定卸供給事業を適確に実施するために必要な対策を実施することが望ましい。

（2）　本指針を遵守すべき事業者

本指針を遵守すべき主たる関係事業者は、特定卸売供給事業者である。特定卸売供給事業者は、特定卸売供給事業者に対して電気の供給能力を有する者（下位のアグリゲーター等）の範囲を含めてセキュリティ対策に係る責任を負うことが求められる。下位のアグリゲーター等においては、特定卸供給事業者の責任の下で適切なセキュリティ対策を行うことが求められる。



（3）　本指針で用いる用語の定義

以下の各用語は、本指針において以下に定める意味を有する。

- 委託先等：特定卸供給事業の用に供するシステム等に係る委託先、再委託先及び発注先
- 下位のアグリゲーター等：特定卸供給事業者に対して電気の供給能力を有する者
- 外部記憶媒体：機器に接続してそのデータを保存するための可搬型の装置
- 外部ネットワーク：不特定多数が接続できる回線で接続するネットワーク
- 簡易指令システム：需給バランス調整等の指令を行うシステム
- 監査：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、必要な証拠を収集し、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
- 機器：システムを構成するサーバ、パソコンや可搬型の端末等及びネットワークを構成するもの
- 脅威：システム又は組織に損害を与える可能性がある、望ましくないセキュリティ事故の潜在的な原因

- 教育プログラム：第三者による、特定卸供給事業者に求められるサイバーセキュリティ対策の理解・実践に係る教育の機会
- 供給先：特定卸供給事業者により集約された電気が供給される者
- 経営層：特定卸供給事業者における経営責任を持つ者
- サイバー攻撃：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
- システム関係者：委託先等を含む特定卸供給事業の用に供するシステム等の利用、管理、開発、保守に従事する者の総称
- 詳細対策要件：特定卸供給事業者が、実運用に耐え得るべく、具体的なセキュリティ対策を自らの責任で規定したもの
- ぜい弱性：１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
- ぜい弱性情報：ぜい弱性に係る情報
- セキュリティガバナンス：経営層が主体的かつ適切にリスクを管理する仕組みを構築・運用すること
- セキュリティ事故：意図的なサイバー攻撃により、電力の安定供給、電気工作物の保安（公衆安全を含む）の確保に支障を及ぼす、又はそのおそれのあるシステムの不具合が発生した事象
- セキュリティ仕様：システム等の機能要件に応じて策定されたセキュリティ要件
- セキュリティに係る情報：セキュリティマネジメントに係る情報、セキュリティ対策の実施状況に係る情報
- 相互接続相手：相互接続する下位のアグリゲーター及び供給先
- 他ネットワーク：特定卸供給事業用ネットワーク以外のネットワークのうち、外部ネットワーク以外のもの
- 特定卸供給事業の用に供するシステム：特定卸供給事業の用に供する電子情報システム
- 特定卸供給事業用ネットワーク：特定卸供給事業の用に供するシステム同士をつなぐネットワーク
- 特定卸供給事業の用に供するシステム等：特定卸供給事業の用に供するシステム及び特定卸供給事業用ネットワークの全体
- PDCA サイクル：計画、実行、評価、改善の四段階を繰り返し、継続的に業務を改善していく手法の一つ
- 標的型攻撃：特定の組織や業界を狙ったサイバー攻撃のこと
- 文書化：情報や手順を可視化すること
- 報告：予め設定された方法及び手順に従って、文書化された情報を伝達すること
- 本指針：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
- リスク：脅威とぜい弱性の合致により損失が発生する可能性、また、その損失
- ログ：特定卸供給事業の用に供するシステム等の利用状況やデータの通信を記録したもの

2　サイバーセキュリティ確保の観点から望ましい行為

（1）　組織

ア　体制

特定卸供給事業の用に供するシステム等のセキュリティ対策及び運用を実施し、これを統制するため、次に掲げる内容を含んだ組織の体制を整備することが望ましい。

①経営層の責任の明確化

経営層は特定卸供給事業の用に供するシステム等におけるセキュリティの確保について責任を負うこと。経営層の責任の下、自社のセキュリティ対策の現状、自社が最終的に目指すべきセキュリティ対策を明確にした上で、詳細対策要件の策定及びその実現に向けたプロセスを検討すること。

②管理組織の設置

セキュリティ管理を推進し、セキュリティガバナンスの構築を行う責任主体として、セキュリティ管理責任組織を設置し、当該組織の管理下にてPDCAサイクルを回すことができる運用・管理体制を構築すること。

③目的の明確化

特定卸供給事業の用に供するシステム等のセキュリティの実施目的を明確にすること。

イ　取組

特定卸供給事業の用に供するシステム等のセキュリティ管理し、確保するための仕組みを確立するため、次に掲げる内容を含んだ取組を実施することが望ましい。

①責任者の設置

特定卸供給事業の用に供するシステム等のセキュリティ管理責任者を任命するとともに、特定卸供給事業に係る他の事業者の管理責任者間で情報共有できる体制を構築すること。

②役割の明確化

特定卸供給事業者は、システム関係者に対して、セキュリティに係る役割を明確にすること。

③委託先等及び供給先の対応

特定卸供給事業者は、一般送配電事業者との間で調整力契約を締結するにあたり、下位のアグリゲーター等のセキュリティを含むサービス品質を確保し、一般送配電事業者

に対して責任を持つこと。また、小売電気事業者のシステムと接続する場合には、小売電気事業者に対して、小売電気事業者の保有するシステムが本指針に準拠することを求めること。さらに、当該小売電気事業者に対して、本指針に基づき、別途要件を定義したセキュリティ対策を構築し、それに準拠することを求めること。

ウ　セキュリティ教育

特定卸供給事業の用に供するシステム等のシステム関係者がセキュリティの重要性を認識し、適切なセキュリティ対策を行えるようにするため、次に掲げる内容を含んだ教育に係る取組を実施することが望ましい。

①教育の計画・実施

システム関係者が適切なセキュリティ対策を行えるよう、セキュリティ教育を計画し、適時に実施すること。

②教育効果の確認

システム関係者に対してアンケートやテストを実施することにより、セキュリティ教育の効果を確認すること。

（2）　文書化

ア　文書管理

特定卸供給事業の用に供するシステム等のセキュリティに係る情報をシステム関係者に周知徹底し、最新の情報を必要な時に利用できるようにするため、次に掲げる内容を含んだ文書管理を実施することが望ましい。

①文書化

特定卸供給事業の用に供するシステム等のセキュリティに係る情報を文書化すること。

②文書の管理

特定卸供給事業の用に供するシステム等のセキュリティに係る文書を適切に管理すること。

（3）　セキュリティ管理の計画策定と実施

ア　セキュリティ管理

特定卸供給事業の用に供するシステム等のセキュリティ対策を継続的に改善し、対策を計画に従って適切に行えるようにするため、次に掲げる内容を含んだセキュリティ管理の計画策定と実施の枠組みを構築することが望ましい。

①対策の計画策定

セキュリティ対策は、事業計画に沿ってセキュリティ管理責任組織のもとで策定した方針に従って計画することとし、対象システムやネットワーク構成及び責任分界点を明らかにした上で、システムにおいて保護すべき情報・機能・資産を明確化したうえで策定すること。また、それらに対して想定される脅威に対抗する対策の候補を検討すること。特定卸供給事業者は、サイバー攻撃等の影響が系統ネットワークに拡散するリスクを管理する必要があることに留意し、具体的なセキュリティ対策を記載した詳細対策要件を自らの責任で策定すること。

②対策の実施

計画に従って、脅威レベル、被害レベル、コスト等を考慮して実施する対策を選定すること。なお、セキュリティ対策の実施には上限がないため、選定に際しては、実施に要するコストも勘案しつつ、過剰な投資を行うことなく必要十分な範囲で対策を講ずること。

③対策の点検・報告

セキュリティ対策が適切に実施されていることを第三者による監査（認証を含む。）や教育プログラム等の受講者による内部監査等によって定期的に点検・評価し、セキュリティ管理責任者に報告すること。また、セキュリティ事故発生時の対応方法について、設計・運用・訓練を実施すること。なお、詳細対策要件について、定期的にその内容の点検・更新を行うこと。

④対策の改善

対策の点検結果に基づき、セキュリティ対策の改善を行うこと。なお、詳細対策要件について、ぜい弱性が顕在化するなど早急な対策が求められる際には随時更新すること。

イ　実施状況の報告

特定卸供給事業の用に供するシステム等に係るセキュリティ対策の実施状況を明確にするため、次に掲げる内容を踏まえた報告を実施することが望ましい。

①適切な報告の仕組みの構築

セキュリティ対策の実施状況に係る報告事項を定め、システム関係者からセキュリティ管理責任者及び経営層に適切に報告を行うことができる仕組みを構築すること。

②定期的な報告

セキュリティ対策の実施状況に関して、システム関係者からセキュリティ管理責任者及び経営者へ定期的に報告を行うこと。

（4）　設備・システムのセキュリティ

ア　外部ネットワークとの分離

不特定多数がアクセスできるネットワークを介して、特定卸供給事業の用に供するシステム等が外部から不正侵入されないようにするため、簡易指令システムとの直接的な接続部は、外部ネットワークと原則分離することが望ましい。外部ネットワークとは直接接続せず、間接的に接続する場合には、外部ネットワークとの間に他ネットワークや別のシステム等の緩衝エリアを設けることが望ましい。

イ　他ネットワークとの接続

他ネットワークで発生したサイバー攻撃の影響が、特定卸供給事業の用に供するシステム等に伝播しないようにするため、次に掲げる内容を含んだ他のネットワークとの接続に係るセキュリティ対策を行うことが望ましい。

①接続点の防御・最小化

簡易指令システムとの直接的な接続部は、他ネットワークとの接続点を最小化し、接続点に防御措置を講じること。また、簡易指令システムとの直接的な接続部は、一般送配電事業者が別途定める相互接続に係るセキュリティ要求事項に準拠すること。

②相互接続の中止

特定卸供給事業者は、相互接続相手に本指針の実装が確認できない場合には、システム全体のセキュリティ被害を最小化することを目的として、該当するシステム間での相互接続を速やかに中止すること。

ウ　通信のセキュリティ

特定卸供給事業の用に供するシステム等において、機器間の通信における傍受、不正なデータの挿入並びに機器が保有する重要なデータの漏えい及び改ざんを防ぐため、次に掲げる内容を含んだ通信に係るセキュリティの対策を行うことが望ましい。

①認証・暗号化

外部ネットワークとの相互接続点において認証を行い、通信メッセージは暗号化により保護すること。

②データ等の改ざん対策

通信機器や通信路に対して、データ等の改ざんに対する対策を講じること。

エ　マルウェア対策

特定卸供給事業の用に供するシステム等の機器へのマルウェア侵入を防ぐため、特定卸供給事業の用に供するシステム等にはぜい弱性に対処するセキュリティパッチを適用するとともに、システムを構成する機器や外部記憶媒体等へのマルウェア対策を行うことが望ましい。

また、システムにおける管理者権限の割当を適切に行うとともに、不正な行為やプログラムの実行を阻止し、本来の操作によらない処理が発行されないよう対策を講じることが望ましい。加えて、システムを構成する機器や外部記憶媒体、取り扱うデータを把握し、適切に管理及び保護することが望ましい。

オ　なりすまし対策

不正接続された機器やサイバー攻撃を受けた機器により、他の機器や特定卸供給事業の用に供するシステム等の不正な動作を防止するため、許可されていない機器からの通信遮断やネットワーク分割等により、なりすまし対策を講じることが望ましい。

（5）　運用・管理のセキュリティ

ア　セキュリティ仕様の明確化

特定卸供給事業の用に供するシステム等調達時の齟齬、仕様漏れが発生しないようにするため、特定卸供給事業の用に供するシステム等は、そのシステムが取り扱う機器とその機器が保有する情報の機密性、完全性及び可用性の確保並びに機器の動作に係る利用者等に対する安全確保に必要な要件を明確化することが望ましい。

イ　データの管理

特定卸供給事業の用に供するシステム等のデータに係るセキュリティ事故の発生を予防し、又はセキュリティ事故を迅速に把握し対応できるようにするため、特定卸供給事業の用に供するシステム等が保有するデータを把握し、適切に管理及び保護するとともに、システムが個人情報を扱う場合には、個人情報保護法に準拠した対策を取ることが望ましい。

（6）　セキュリティ事故の対応

ア　情報の収集

特定卸供給事業の用に供するシステム等のセキュリティ事故に対して、適切に対応できるようにするため、セキュリティ事故の対応に必要なログ（必要と判断した場合）や文書等の情報を収集することが望ましい。

イ　事故時の対応の明確化

特定卸供給事業の用に供するシステム等のセキュリティ事故における損害を最小限にするため、次に掲げる内容を含んだ対応を実施することが望ましい。

①責任と手順

PDCAサイクルを回すことができる運用・管理体制を構築することを前提とするとともに、システムの状況の監視やインシデントへの対応が可能な体制を構築し、それぞれの責任範囲と役割を明確にすること。また、セキュリティ事故が実際に生じ得ることを前提に、実際に対応を行えるよう有事の際の役割や手順を策定すること。

②損害の最小化

作成した手順に従い、インシデント発生時の損害を考慮し、そのインシデントがより大規模な事故に発展しないよう、その異常を最小限にとどめるための対応を実施すること。

ウ　報告と情報共有

特定卸供給事業の用に供するシステム等のぜい弱性に起因するセキュリティ事故の予防及び再発防止のため、次に掲げる内容を含んだ対応を実施することが望ましい。

①報告

セキュリティ事故が発生した場合には、対応手順に従い資源エネルギー庁等の関係機関に報告を行うこと。なお、特定卸供給事業者は、ぜい弱性関連情報の利用者への通知を行うこと。

②情報の共有

セキュリティ事故から得られた知見を、セキュリティ事故の予防及び再発防止に活用する仕組みを構築すること。特定卸供給事業者は、システム関係者、事業者間の調整を担う機関、ぜい弱性関連情報の分析等を担う機関の間において、ぜい弱性対策情報・脅威情報を共有・管理すること。

エ　周知と訓練

特定卸供給事業の用に供するシステム等のセキュリティ事故発生時に、迅速かつ適切に対応するため、セキュリティ事故発生時の対応の周知や、対応計画に基づいた訓練を継続的に実施することが望ましい。また、訓練の効果についても確認することが望ましい。