

資源エネルギー庁 御中

**令和2年度エネルギー需給構造高度化対策に関する調査等
事業（電力分野のサイバーセキュリティ対策のあり方に関
する詳細調査分析）報告書**

2021年2月26日

 **株式会社三菱総合研究所**

デジタル・イノベーション本部

目次

1. はじめに	1
1.1 調査背景・目的	1
1.2 調査実施概要	1
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	2
2.1 大手電力会社の対策の国内外比較	2
2.1.1 文献等による調査結果	2
2.1.2 海外機関へのヒアリングによる調査結果	6
2.2 新規プレーヤーの対策の国内外比較	6
2.2.1 文献等による調査結果	7
2.2.2 国内の事業者、メーカー等へのヒアリングによる実態調査の結果	12
2.2.3 海外事業者へのヒアリングによる調査結果	15
2.3 規制体系に関する諸外国の最新動向等	15
2.3.1 文献等による調査結果	15
2.3.2 海外機関へのヒアリングによる調査結果	16
3. 新規プレーヤーに関するサイバーセキュリティ対策の検討	18
3.1 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等の運営	18
3.1.1 小売電気事業者向けサイバーセキュリティ対策セミナーの運営	18
3.1.2 第1回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の運営	19
3.1.3 小売電気事業者のサイバーセキュリティ対策に係る作業会の運営	20
3.1.4 第2回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の運営	20
3.1.5 第3回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の運営	21
3.2 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項目案の作成	22
3.2.1 ガイドラインの策定スケジュール	22
3.2.2 事前質問票におけるガイドラインへの期待のまとめ	22
3.2.3 第1回小売勉強会における意見	23
3.2.4 作業会を通じた素案の作成	23
3.2.5 第2回小売勉強会、第10回電力SWGを踏まえた修正	25
3.2.6 パブリックコメント結果を踏まえた修正と第1.0版公開の承認	25
4. ワーキンググループの運営	27
4.1 第9回SWGの運営	27
4.2 第10回SWGの運営	31
4.3 第11回SWGの運営	34

図目次

図 2-1	電力供給を担う事業者の関係性と本調査における新規プレイヤーの定義.....	7
図 2-2	太陽光・風力発電設備のシステム構成イメージ.....	9
図 2-3	国内設備導入量の規模割合比較	13
図 2-4	大統領令の概要図	16
図 3-1	小売ガイドライン作成スケジュール	22

表 目 次

表 2-1	NIST Cybersecurity Framework の概要と比較の結果.....	2
表 2-2	NERC CIP の概要と比較の結果.....	3
表 2-3	Cyber Assessment Framework の概要と比較の結果	4
表 2-4	フランス首相通達 PRMD1824939A の概要と比較の結果	5
表 2-5	FERC による NIST CSF と NERC CIP ギャップ分析の概要.....	6
表 2-6	諸外国における小規模発電設備設置者に対するセキュリティ対策検討状況..	11
表 2-7	設備種別毎のヒアリング対象者区分	13
表 3-1	需要規模別の要望まとめ	23
表 3-2	第 1 回小売勉強会における主な意見	23
表 3-3	第 1 回小売勉強会での意見を踏まえた方針案の検討結果.....	24
表 3-4	小売ガイドラインの基本構成と記述内容	24
表 3-5	詳細対策事例の一覧	25
表 3-6	第 2 回小売勉強会及び第 10 回 SWG における意見.....	25

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り組みが求められている。

電力分野においては、2016年の小売全面自由化等により新規参入者が拡大するとともに、再生可能エネルギーの系統への接続やそれに伴う出力制御の実施のため、発電・送配電事業を中心として、ネットワークへの接続やデジタル技術の活用が広がりつつある。一方で、サイバー攻撃を受ける可能性や攻撃箇所の増加、また、サイバー攻撃の影響が広範囲に及ぶ可能性も高くなっている。また、分散電源が大量に導入された電力系統全体としての安定性確保のためには、機器の故障や需給バランスに留意するだけでなく、サイバー攻撃を起点とする系統不安定化を防止するためにもサイバーセキュリティ確保の重要性はこれまでになく高まっている。

こうした中、産業横断的な更なるサイバーセキュリティ対策を検討する産業サイバーセキュリティ研究会が設置され、その下のワーキンググループにおいて、制度・技術・標準化の検討が進められている。また、上述のような状況変化を踏まえ、2018年6月に電力分野のサイバーセキュリティに関する今後の取り組みについて検討を行うことを目的とし、電力サブワーキンググループが設置され、電力を取り巻くサイバーセキュリティに関する現状、事業者の取り組み、官民が取り組むべき課題と方向性の議論・検討が行われているところである。

本事業では、再生可能エネルギー主力電源化に向けて重要な課題であるサイバーセキュリティの領域にて、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、海外における取り組み状況の実態調査等必要な調査・分析を実施した。また、ワーキンググループにおける議論・検討を円滑に進めるための運営を行った。

これにより、石油や石炭、ガスの円滑な生産・流通に必要な不可欠な円滑な電力の安定供給、ひいては我が国のエネルギー安全保障の向上に資することを目的とする。

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. 新規プレーヤーに関するサイバーセキュリティ対策の検討
3. ワーキンググループの運営

2. 国内外の電力サイバーセキュリティに関する実態調査・分析

文献、インターネット、ヒアリング等により調査を行い、国内外の電力サイバーセキュリティ対策の最新動向等（大手電力会社の対策の国内外比較、新規プレーヤー（小売電気事業者、太陽光発電等の小規模な分散電源を有する者等）の対策の国内外比較、規制体系に関する諸外国の最新動向等を含む）について整理・分析を行った。

2.1 大手電力会社の対策の国内外比較

文献、インターネット、ヒアリング等により調査を行い、国内外の大手電力会社等のサイバーセキュリティに関する実態の整理・分析を行った。

2.1.1 文献等による調査結果

電力システムを対象とした国外のサイバーセキュリティ対策基準等として、次の4つの対策基準等の概要及び要求事項を文献で調査し、国内の基準である電力制御システムセキュリティガイドラインの要求事項との比較を行った。また、米国において NIST Cybersecurity Framework に関連して行われているアセスメント等の動向について調査を行った。

- (1) NIST Cybersecurity Framework
- (2) NERC CIP
- (3) Cyber Assessment Framework
- (4) フランス首相通達 PRMD1824939A

(1) NIST Cybersecurity Framework との比較

NIST Cybersecurity Framework は、米国国立標準技術研究所（NIST）によって策定された重要インフラのサイバーセキュリティ対策を策定するためのフレームワークである。NIST Cybersecurity Framework の概要と、電力制御システムセキュリティガイドラインの要求事項との比較の結果を表 2-1 に示す。

表 2-1 NIST Cybersecurity Framework の概要と比較の結果

文書名	Framework for Improving Critical Infrastructure Cybersecurity
策定機関名	National Institute of Standards and Technology (NIST)
主な適用対象	重要インフラシステム及びその管理者（電力以外を含む）
種別	ガイドライン・フレームワーク（強制力なし）
概要	重要インフラがサイバーセキュリティ脅威へ対処するため、重要インフラ事業者・運営者が自主的に利用することを目的とした対策フレームワークである。米国サイバーセキュリティ強化法に基づき、2014 年に策定された。 重要インフラに共通して期待される対策を示しており、電力分野も対象範囲に含まれる。フレームワークの5つのコア機能「ID（識別）」「PR（防御）」「DE（検知）」「RS（対応）」「RC（復旧）」に従い、それぞれに対応した対策目標のカテゴリ、サブカテゴリを提示し

	ている。組織は、手引きに従ったセルフアセスメントを実施することで、現状の把握と目標の設定を行うことができる。現状の把握は、「Tier 1: 部分的」「Tier 2: リスクが認知されている」「Tier 3: 繰り返し可能」「Tier 4: 適応的」の4層によって行われる。
比較の概要	電力制御システムセキュリティガイドラインが規制基準として運用されている一方、NIST CSF は強制力のない対策フレームワークであり位置付けが異なる。電力制御システムセキュリティガイドラインには計7条41事項の記載があるが、NIST CSF には計5機能23カテゴリ108サブカテゴリの記載があり、各対策要件の記述において抽象度が異なる。例えば、NIST CSF では、インシデントレスポンス計画に含めるべき技術的な観点の例として、フェールセーフ、ロードバランシング、ホットスワップ等について言及されているほか、インシデントレスポンス中の具体的な対応事項としてフォレンジックの実施等を示している。

(2) NERC CIP との比較

NERC CIP は、北米電力信頼度協議会（NERC）によって策定された米国内の電力設備におけるサイバーセキュリティ対策実施状況を検査するための基準である。連邦政府により、公的規制としての承認を受けている。NERC CIP の概要と、電力制御システムセキュリティガイドラインの要求事項との比較の結果を表 2-2 に示す。

表 2-2 NERC CIP の概要と比較の結果

文書名	Critical Infrastructure Protection (CIP) Standards
策定機関名	North American Electric Reliability Council (NERC)
主な適用対象	大規模電力システム及びその管理者（送配電、発電）
種別	公的規制基準（罰金規程あり）
概要	北米電力信頼度協議会（NERC）により、電力システムの信頼度向上及び電力の安定供給を目的として策定されたサイバーセキュリティ対策基準である。米国連邦エネルギー規制委員会（FERC）により、連邦政府による規制基準として採用されており、連邦電力法 215 条/215A 条として公的規制に位置付けられている。 CIP は、13 の規程から構成されており、それぞれの規程に対応して、「事業者が遵守すべき要件」、「要件遵守のエビデンスを測定する基準」を定めている。要件には、通信保護に関する要件等の技術的要件と、人員訓練等の組織的要件の両方が含まれる。
比較の概要	NERC CIP には事業者の遵守すべき要件（遵守要件）及び測定基準が記載されている。一方で、電力制御システムセキュリティガイドライン本体には事業者が実施すべき要求事項のみ記載されており、実施実態の確認は電気事業法下の保安規定に基づく取り組みの確認が検討さ

	れているところである¹。 電力制御システムセキュリティガイドラインには計 7 条 41 事項の記載がある一方、NERC CIP には計 12 エリア 42 項目 233 細則の記載がある。対策を求める領域には大きな差は見られないが、NERC CIP は細則としてより詳細な実施事項を求めている。電力制御システムセキュリティガイドラインと NERC CIP は共に、電力制御システムが電力系統に与える影響の大きさに応じて重要度のレベル分けがされているが、NERC CIP では、重要度のレベルに応じて要求が異なり、重要度のレベルが上がると遵守事項の数が多くなる。
--	---

(3) Cyber Assessment Framework との比較

Cyber Assessment Framework (CAF) は、National Cyber Security Centre (NCSC) によって策定された英国内の重要サービスにおけるサイバーセキュリティ対策のフレームワークである。CAF の概要と、電力制御システムセキュリティガイドラインの要求事項との比較の結果を表 2-3 に示す。

表 2-3 Cyber Assessment Framework の概要と比較の結果

文書名	Cyber Assessment Framework (CAF)
策定機関名	National Cyber Security Centre (NCSC)
主な適用対象	重要サービス及び重要活動（電力以外を含む）
種別	ガイドライン・フレームワーク（強制力なし）
概要	重要サービスがサイバーセキュリティ脅威へ対処するため、重要サービス事業者・運営者の自主的な利用や外部監査機関での利用を目的としたアセスメントフレームワークである。2019 年 9 月 30 日に策定された。CAF の利用に最も適している組織は以下の 3 種類としている。 • UK Critical National Infrastructure に所属している組織 • NIS 指令の対象となる組織 • 公共の安全に関わるサイバーリスクに対処している組織 CAF は、4 つの目的に基づいて 39 個の項目で構成されている。4 つの目的は、「セキュリティリスクのマネジメント」、「サイバー攻撃に対する対策」、「サイバー攻撃の検知」、「インシデント時の被害の最小化」である。各項目を「適用済み」、「一部適用済み」、「適用できていない」の 3 段階で評価される。
比較の概要	電力制御システムセキュリティガイドラインが規制基準として運用されている一方、CAF は強制力のないアセスメントフレームワークであり、その位置付けは異なる。CAF の特徴として各項目の達成基準が詳細に決定されている点がある。具体例として、サニタイジング（機器

¹ 令和元年度産業保安等技術基準策定研究開発等事業（電力分野のサイバーセキュリティ対策検討事業）報告書 https://www.meti.go.jp/medi_lib/report/2019FY/000060.pdf

	廃棄前に格納されているデータをセキュアに消去する作業）やデータバックアップと定期的な確認等が挙げられる。
--	--

(4) フランス首相通達 PRMD1824939A との比較

フランス首相通達 PRMD1824939A は、フランス政府によって策定された重要サービスにおけるサイバーセキュリティ対策の通達である。フランス首相通達 PRMD1824939A の概要と、電力制御システムセキュリティガイドラインの要求事項との比較の結果を表 2-4 に示す。

表 2-4 フランス首相通達 PRMD1824939A の概要と比較の結果

文書名	フランス首相通達 PRMD1824939A
策定機関名	フランス政府
主な適用対象	重要サービス（電力以外を含む）
種別	首相通達
概要	2016 年 7 月に EU が発出した NIS 指令を受けて、フランス政府が発出した重要サービスのサイバーセキュリティ対策に関する通達である。 2018 年 10 月 1 日に有効化された。 本通達は、ガバナンス・防護・対策・レジリエンスの 4 つに分けられており、計 23 個のルールが記載されている。各ルールに適用までの猶予期間が設定されている。
比較の概要	PRMD1824939A はフランス政府から首相通達として発せられた通達であり、電力制御システムセキュリティガイドラインと同じく公的な規制として適用されるものである。電力制御システムセキュリティガイドラインと比較して、対策を求める領域及びその具体性は概ね近いものである。一方、PRMD1824939A には一部のルールで特徴的な対策を要求している。例として、通信データのフィルタリングの詳細な条件を定めている点や、フランス国家情報システムセキュリティ庁（ANSSI）からの情報を遅滞なく受信するための窓口の設置等が挙げられる。

(5) NIST CSF のアセスメント動向

1) FERC による NIST CSF と NERC CIP ギャップ分析

米国連邦エネルギー規制委員会（FERC）は 2020 年 6 月に NERC CIP の強化に向けた情報請求告示（NOI）を発表²した。本告示では、日々進化し続けるサイバー脅威に対抗するために、NIST CSF と NERC CIP とのギャップ分析を実施し、NERC CIP で十分に考慮できていない可能性のあるカテゴリを示した。FERC による分析の概要を表 2-5 に示す。

² FERC “Potential Enhancements to the Critical Infrastructure Protection Reliability Standards”
<https://www.ferc.gov/sites/default/files/2020-06/E-5-061820.pdf>

表 2-5 FERC による NIST CSF と NERC CIP ギャップ分析の概要

カテゴリ	内容
データセキュリティに関するリスクについて	NIST CSF のサブカテゴリ PR.DS-4 (可用性を確保するための十分な通信容量の維持) は、CIP-011-2 (情報の保護) や CIP-012-1 (コントロールセンター間の通信) に含まれていない。また、サブカテゴリ PR.DS-6 (完全性チェックメカニズムの使用) は、CIP-013-1 (サプライチェーンリスク管理) の一部に含まれているものの、影響度「低」の電力設備には適用されない。
異常や事象の検知について	NIST CSF のサブカテゴリ DE.AE-2 (検知した事象の分析) 及びサブカテゴリ DE.AE-4 (検知した事象がもたらす影響の判断) は CIP-008-5 (インシデント対応計画) の一部に含まれているものの、同様に影響度「低」の電力設備に適用されない。
セキュリティ事象の緩和について	NIST CSF のサブカテゴリ RS.MI-1 (インシデントの封じ込め) やサブカテゴリ RS.MI-2 (インシデントの緩和) は、CIP-008-5 では言及されていない。また、CIP-008-5 は影響度「低」の電力設備には適用されない。また、CIP-010-2 (設定変更の管理と脆弱性の特定) では、サブカテゴリ RS.MI-3 (新たに識別された脆弱性の緩和) について、影響度「低」の電力設備には適用されない。

2.1.2 海外機関へのヒアリングによる調査結果

米国の電力セキュリティ規制機関である FERC (米国連邦エネルギー規制委員会) へのヒアリング調査結果を行った。ヒアリング対象の検討に当たっては、文献等による調査結果やワーキンググループにおける委員からの意見等を踏まえ、NIST CSF を活用した取り組みを推進している FERC を対象とした。

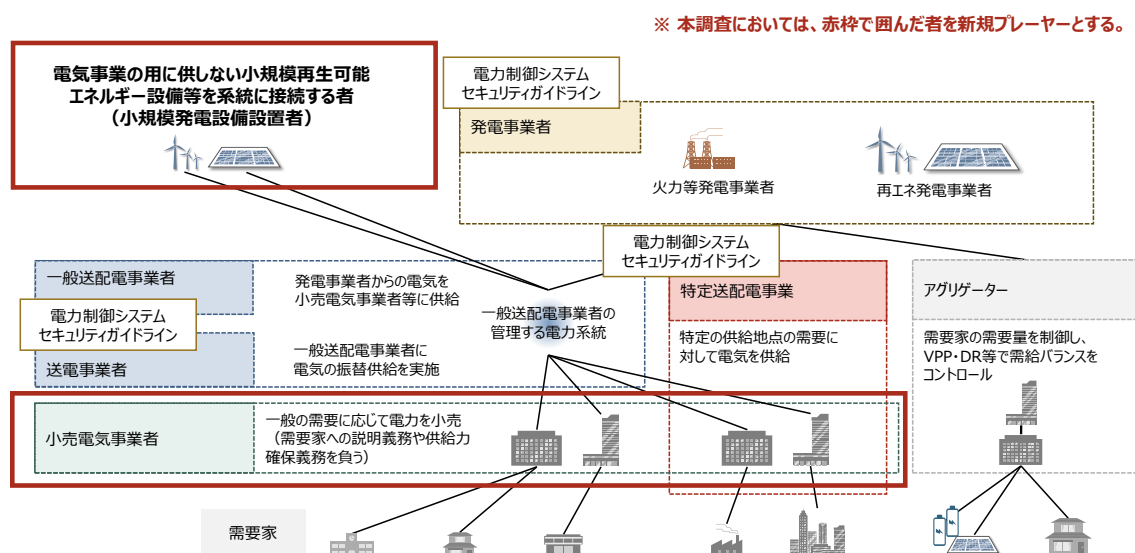
ヒアリングは、FERC が実施した CIP 基準と NIST CSF のギャップ分析の結果、今後の NIST CSF の活用方針、事業者の対策状況とフォローアップ方針等について質問をした。CIP 基準と NIST CSF のコンセプトの違いに関する分析と CIP 基準改善のための今後の方針等についての回答を得た。また、事業者の成熟度の違いに応じたフォローアップ手法の使い分け等について情報提供をうけた。

2.2 新規プレーヤーの対策の国内外比較

本調査においては、2016 年の電力小売全面自由化により電力市場に参画した小売電気事業者、電気事業の用に供さない太陽光発電等の小規模な分散電源設備等を系統連系する者を新規プレーヤーとして扱う。

サイバーセキュリティ対策に関する規制の観点では、電気事業法により、事業用電気工作物を設置する者に対しては、省令で定める技術基準への適合維持が義務付けられている。ま

た、省令で定める技術基準において、一般送配電事業、送電事業、特定送配電事業及び発電事業の用に供する電気工作物の運転を管理する電子計算機に係るサイバーセキュリティの確保を規定し、その解釈においては、日本電気技術規格委員会（JESC）の「電力制御システムセキュリティガイドライン」が位置付けられている。したがって、図 2-1 に示すとおり、電力供給を担う一部の事業者においては、ガイドラインに基づく対策が義務付けられている。



出所）経済産業省資料に基づき三菱総合研究所作成

図 2-1 電力供給を担う事業者の関係性と本調査における新規プレイヤーの定義

新規プレイヤーのうち小売電気事業者に求められるサイバーセキュリティ対策については、昨年度事業において諸外国における検討状況を整理・分析したところである。そこで、本事業では、特に小規模な分散電源設備等を系統連系する者（以下「小規模発電設備設置者」という）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、文献、インターネット、ヒアリング等により調査・分析を行った。具体的には、小規模発電設備設置者が実施しているサイバーセキュリティ対策に関する国内外の実態の調査、並びに当該者のサイバーセキュリティ対策の向上に向けて望まれる取り組みの検討を行った。

2.2.1 文献等による調査結果

(1) 小規模発電設備設置者に求められるセキュリティ対策

小規模発電設備設置者に求められるセキュリティ対策として、まず出力制御の対象となる太陽光発電システムに係る「出力制御機能付き PCS の技術仕様について」³に記載された対策が挙げられる。この文書は、太陽光発電設備の出力制御システムに求められる要件とし

³ 太陽光発電協会、日本電機工業会、電気事業連合会「出力制御機能付き PCS の技術仕様について」
https://www.meti.go.jp/shingikai/enecho/shoene_shinene/shin_energy/keito_wg/pdf/005_02_00.pdf

て、電力安定供給のために必要なセキュリティ対策を講じることを挙げており、出力制御機能を有した太陽光発電設備に想定されるセキュリティ脅威と対応する保護対策例が記載されている。具体的には、一般送配電事業者が有する出力制御システム用の電力サーバ、太陽光発電設備を系統に接続する者が有する PCS、及びそれらの間の通信経路の 3 つに想定される脅威と対策例を整理している。特に小規模発電設備者においては、以下の対策例の実装が求められる。

- 外部からのセッション開始不可
- スケジュール設定のバックアップ
- 通信先として電力サーバを指定
- SSL 通信による暗号化
- 通信に重要情報を含めない。

出力制御機能を有した風力発電設備においても、この「出力制御機能付 PCS の技術仕様について」に基づいた技術仕様⁴の策定を行っている。各一般送配電事業者はこの技術仕様に基づいて、太陽光・風力発電所出力制御機能に対する技術仕様書を公開している。

加えて、小規模発電設備設置者に求められるセキュリティ対策として、一般送配電事業者の策定する「系統連系技術要件」（託送供給等約款別冊）で定められているセキュリティ対策が挙げられる。系統連系技術要件とは、一般送配電事業者の系統に対して発電者の設備又は需要者の設備を連系する際に求められる技術要件である。系統連系技術要件は、一般送配電事業者が策定するものであるが、策定及び変更に当たっては経済産業大臣の認可を受ける必要があることから、系統連系に係る一連の規程の中で実効性及び手続の適正性を有するものと整理されている。2020 年 6 月 11 日の第 25 回電力・ガス基本政策小委員会での議論⁵に基づき、一般送配電事業者各社の系統連系技術要件に対してセキュリティ対策に関する要件が追記された。具体的には、事前防御と事後防御の観点から合計 3 つの要件が追記された。事前防御の観点では、小規模発電設備のオンライン化を踏まえ、ネットワークを通じた攻撃を防御する観点から以下の 2 つの対策が求められる。

① ネットワーク接続点の保護：

発電設備の制御を行うシステム（制御システム）とインターネットとを分離する等の措置により、外部からの不正侵入を防止し、また、他のネットワークでのインシデントが制御システムに伝播することを防止する。

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：

マルウェアの感染によりシステムに不具合が発生し、制御システムが利用できなくなることを防止する。

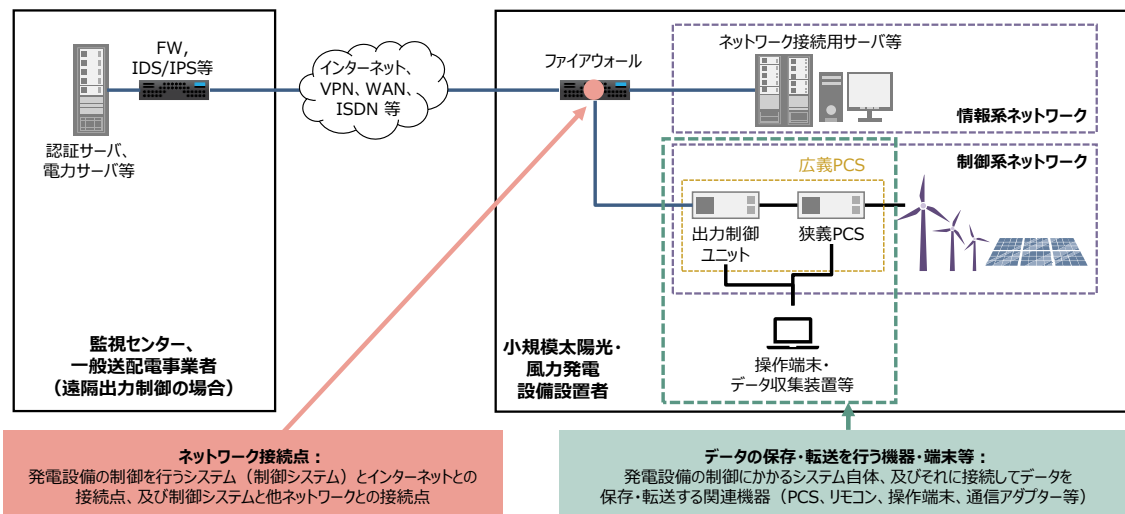
対象となるネットワーク接続点やデータの保存・転送を行う機器・端末等の範囲は設備種別や運用方法によって変わること留意が必要である。例えば、図 2-2 に示す非住宅用（商業向け）の太陽光発電や風力発電では、ファイアウォールが設置されている点が発電設備の

⁴ 日本風力発電協会、日本小型風力発電協会、電気事業連合会「風力発電遠隔出力制御に係る技術仕様について（報告）」http://jwpa.jp/keitouwg17/17th_keitouwg_shiryou5.pdf

⁵ 資源エネルギー庁 第 25 回 総合資源エネルギー調査会 電力・ガス事業分科会 電力・ガス基本政策小委員会 資料 5「電力分野におけるサイバーセキュリティについて」

https://www.meti.go.jp/shingikai/enecho/denryoku_gas/denryoku_gas/pdf/025_05_00.pdf

制御を行うシステム（制御システム）とインターネットとの接続点、及び制御システムと他ネットワークとの接続点となる。また、発電設備の制御を行う出力制御用 PCS やそれに接続してデータを保存・転送する操作端末等が、データの保存・転送を行う機器・端末等に含まれる。



出所）「出力制御機能付 PCS の技術仕様について」及び「風力発電出力制御に係る技術仕様について（報告）」を参考に三菱総合研究所作成

図 2-2 太陽光・風力発電設備のシステム構成イメージ

系統連系技術要件の事後防御の観点では、攻撃の早期発見と迅速な対処を目的として、設備設置者と系統運用者との間で迅速かつ的確な情報連絡を行うために、以下の対策が求められる。

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

系統連系技術要件に記載された 3 つの対策は、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つては、2020 年 10 月以降に入札を実施するもの）を対象に実施が求められている。なお、日本電機工業会（JEMA）は出力制御システムに関する会員企業の対策状況を調査し、全社において、項目①②の対策が既に講じられていることを確認している。また、小規模発電設備設置者が一般送配電事業者の系統連系申請書を記入する際の記入例を発表している⁶。

(2) 海外の小規模発電設備設置者に求められるセキュリティ対策

海外における小規模発電設備設置者に求められるセキュリティ対策の検討状況を文献等に基づき分析・整理した。調査の対象とした国・地域は、米国、カリフォルニア州、EU、ドイツとした。調査の結果を表 2-6 に示す。

米国全体では系統のロバスト性確保を目的とした系統連系ルールが FERC によって規定

⁶ JEMA 「出力制御システムのサイバーセキュリティについて」
https://jema-net.or.jp/Japanese/res/dispersed/data/cyber_security.pdf

されているが、具体的なサイバーセキュリティに関する要件は規定されていない。他方で、カリフォルニア州では、州法に位置付けられた系統連系ルールである **CA Rule 21** が存在し、この中でサイバーセキュリティ要件とプライバシー要件を含めることが規定されている。**CA Rule 21** の位置付けは国内の系統連系技術要件に近く、州は全体のルールのみを定めるのみで、各公益事業者が本ルールに関する管理責任を有し、それぞれの事業者（**PG&E**⁷、**SCE**⁸、**SDG&E**⁹）が具体的な規則を策定・公表している。いずれも具体的なセキュリティ要件については記載されていない。

EU 全体の取り組みとしては、2019 年 6 月に公開された **Regulation 2019/943** の中で、EU における系統連系ルールの一つであるネットワークコードの要件が示されている。そこでは、サイバーセキュリティの側面を含んだネットワークコードを採用する権限を **ENTSO-E**（欧州電力系統運用者ネットワーク）に与えること、また、**ENTSO-E** の実行要件としてサイバーセキュリティ及びデータ保護を推進することが記載されている。2020 年 5 月には、**Regulation 2019/943** を受け、ネットワークコードへの対応に向けた優先度を示した文書¹⁰を **ENTSO-E** が発表した。この文書において、今後 3 年間のネットワークコードの策定に向けた優先順位において、サイバーセキュリティに焦点を当てるべきだとしている。また、他のネットワークコードやガイドラインへの対応する影響を考慮して、コネクション・ネットワークコード（系統連系に関するネットワークコード）を改正するプロセスを開始することを提案している。

⁷ PG&E（Pacific Gas and Electric Company）“Electric Rule No.21”

https://www.pge.com/tariffs/assets/pdf/tariffbook/ELEC_RULES_21.pdf

⁸ SCE（Southern California Edison）“Rule 21” https://library.sce.com/content/dam/sce-doclib/public/regulatory/tariff/electric/rules/ELECTRIC_RULES_21.pdf

⁹ SGD&E（San Diego Gas & Electric Company）http://regarchive.sdge.com/tm2/pdf/ELEC_ELEC-RULES_ERULE21.pdf

¹⁰ ENTSO-E “Response to the European Commission’s public consultation to establish the priority list of Network Codes” <https://www.entsoe.eu/news/2020/05/26/response-to-the-european-commission-s-public-consultation-to-establish-the-priority-list-of-network-codes/>

表 2-6 諸外国における小規模発電設備設置者に対するセキュリティ対策検討状況

項目	米国		EU	ドイツ
		カリフォルニア州		
関連規則	① FERC Order No.827 ¹¹ ② FERC Order No.842 ¹²	CA Rule 21 ¹³	Regulation (EU) 2016/631 RfG ¹⁴	① Verordnung über Allgemeine Bedingungen für den Netzanschluss und dessen Nutzung für die Elektrizitätsversorgung in Niederspannung ¹⁵ ② Technical Connection Rules for Medium-Voltage ¹⁶
位置付け	FERC による要件であり、強制力を有する	カリフォルニア州の州法で規定された系統連系技術要件の位置付けで、強制力を有する	欧州共通のネットワークコードの一つで、EU 各国は自国のグリッドコードを本規則に合致させる必要がある	① 法的に位置付けられた要件であり、強制力を有する ② 業界規格であり、法令に比べ強制力は緩い
管轄組織	FERC	California Public Utilities Commission	ENTSO-E（欧州電力系統運用者ネットワーク）	① BMWi（連邦経済エネルギー省） ② VDE（ドイツ電気技術者協会）

¹¹ FERC “FERC Order No.827” <https://www.ferc.gov/whats-new/comm-meet/2016/061616/E-1.pdf>

¹² FERC “FERC Order No.842” <https://www.ferc.gov/whats-new/comm-meet/2018/021518/E-2.pdf>

¹³ California Public Utilities Commission “Rule 21 Interconnection”

<https://www.cpuc.ca.gov/General.aspx?id=3962>

¹⁴ EC “Commission Regulation (EU) 2016/631” <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0631>

¹⁵ BMWi “Verordnung über Allgemeine Bedingungen für den Netzanschluss und dessen Nutzung für die Elektrizitätsversorgung in Niederspannung” <https://www.gesetze-im-internet.de/nav/>

¹⁶ ドイツでは電圧区分毎に異なる接続要件が規定されている。高圧に関する要件は次で示されている：
<https://www.vde.com/resource/blob/1708464/47dedcd3571bc7fdbc29fd3704dce88a/tcr-medium-voltage-data.pdf>

項目	米国		EU	ドイツ
		カリフォルニア州		
セキュリティ対策関連項目	具体的なセキュリティ関連要件はないが、②では異常な周波数状態に陥った場合には、接続を切断もしくは遮断器を作動させる必要性が規定されている。	スマートインバータベースの発電設備は、設備に対してサイバーセキュリティ要件とプライバシー要件を含めることが規定されている。	具体的なセキュリティ関連要件はないが、2019 年の Regulation (EU) 2019/943 ¹⁷ では、サイバーセキュリティ及びデータ保護を推進することが ENTSO-E の実行要件であることが記載されている。	いずれも具体的なセキュリティ関連要件はないが、②では、異常発生時に、その原因を特定する目的で系統運用者に対して必要な情報を提供する必要性が規定されている。

2.2.2 国内の事業者、メーカー等へのヒアリングによる実態調査の結果

2020 年 10 月から実施された系統連系技術要件によるサイバーセキュリティ対策の実態を詳細に確認し、具体的な対策の実行可能性及び課題を検討することを目的に、小規模発電設備に関するヒアリング調査を実施した。

(1) ヒアリング調査の実施方針

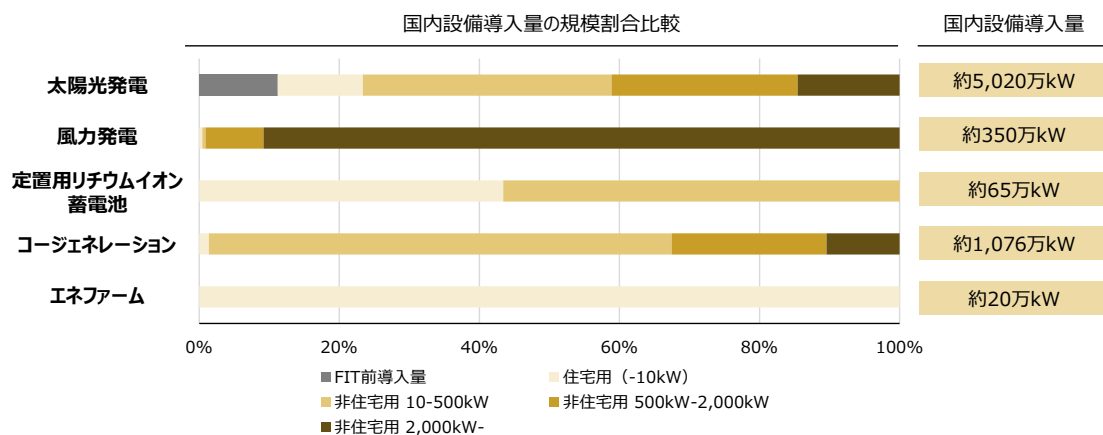
1) ヒアリング対象設備種別

ヒアリングの対象とする設備種別は、系統連系する代表的な小規模発電設備である太陽光発電設備、風力発電設備、定置用リチウムイオン蓄電池、コージェネレーションシステム及びエネファームの 5 つの設備種別とした。それぞれの設備種別における設備導入量の規模割合の比較結果を図 2-3 に示す。この図から分かるとおり、太陽光発電、風力発電、コージェネレーションの 3 種別は非住宅用（10kW 以上）の設備の割合が大きい。他方で、定置用リチウムイオン蓄電池やエネファームの導入量は他の 3 種別に比べて国内設備導入量が小さいものの、住宅用設備（10kW 未満）が多くを占めるため、導入されている設備台数が多いと考えられる。住宅用設備の割合が多い設備種別においては、設置者自身のセキュリティ対策よりも設備自体のセキュリティ対策が重要となるため、本調査では設備メーカーに対してのみヒアリングを行うこととした。

設備種別毎のヒアリング対象者区分を整理した結果を図 2-3 に示す。なお、コージェネレーションシステムのヒアリング対象区分について、業界団体との議論により、システムの設計や設置作業をシステムメーカーが担うことが多く、設置者に対するヒアリングよりも設備メーカーに対するヒアリングの方が有効と考えられるとの意見を得た。そのため、コージェネレーションシステムについては、設備メーカーに対して運用時のセキュリティ対策実態についても確認することとした。

¹⁷ EC “Regulation (EU) 2019/943”

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0943>



注) 太陽光発電設備の設備導入量及び割合は資源エネルギー庁「国内外の再生可能エネルギーの現状と今年度の調達価格等算定委員会の論点案」(2019年3月実績)に基づく。風力発電設備の設備導入量及び割合はNEDO「日本における風力発電設備・導入実績 資料集」(2018年3月実績)に基づく。定置用リチウムイオン蓄電池及びエネファームの設備導入量は、資源エネルギー庁 第10回 エネルギー・リソース・アグリゲーション・ビジネス検討会 資料7に基づく。なお、定置用リチウムイオン蓄電池の規模割合は経済産業省「定置用蓄電池の普及拡大及びアグリゲーションサービスへの活用に関する調査」に基づき作成。コージェネレーションの設備導入量及び割合は、日本ガス協会「コージェネレーションによるエネルギー高度利用と医療・福祉施設への導入について」(2018年3月)の業務用途分類毎の導入量に基づき三菱総合研究所作成。なお、国内設備導入量・台数には現状系統連系がなされていない設備も含まれていることに留意。

図 2-3 国内設備導入量の規模割合比較

表 2-7 設備種別毎のヒアリング対象者区分

設備種別	設備設置者	設備メーカー
風力発電	✓	✓ (PCS メーカー)
太陽光発電	✓	
定置用リチウムイオン蓄電池		✓
コージェネレーション		✓
エネファーム		✓

2) ヒアリング実施に向けた事前調査

小規模発電設備設置者及び設備メーカーに対して事前調整なしに具体的な対策実装等に関するヒアリングを実施した場合、本調査の背景や目的等を適切に共有できず、十分な実態把握調査に繋がらないことが懸念された。そのため、ヒアリング実施前に対策の実施状況を簡易に調査し、実際のヒアリングでは、その事前調査で得られた結果に基づき具体的な実装方法について確認することとした。なお、事前調査の対象者について各設備の関連業界団体と協議の上で決定した。

(2) 事前調査概要

1) 事前調査項目

事前調査はチェックリスト形式のアンケートで実施し、系統連系技術要件における対策①～③の対策状況を簡易的に確認するとともに、小規模発電設備等に求める対策を継続的に改善することを目的に、対策①～③以外の対策実施状況についても確認した。

設備設置者においては、対策①～③の対策状況を複数の観点から確認した。それぞれの設問について、対策を「実施している」／「実施を検討している」／「実施していない」の選択肢に対する択一式とするとともに、択一選択に対する補足事項やその他実施している事項等を記入いただく自由記述欄を設けた。

設備メーカーにおいては、対策①・②の対策の実施方法を複数の観点から確認するために、対策の実施可否と具体的な実装方法を確認した。具体的には、対策を「実施できる」／「実施できない」の択一式で対策状況を確認し、それぞれの設問に関して「実施できる」を選択した場合に、具体的な実装方法を確認する方式とした。

2) 事前調査結果

事前調査は5つの設備種別の設置者及びメーカーの計107社に配布¹⁸し、51社（回答率47.2%）から回答を得た。対策①～③の対策状況やその他の課題について、各事業者の自己評価の確認を行うとともに、設置種別ごとの傾向を把握した。

(3) ヒアリング調査概要

1) ヒアリング項目

事前調査へ回答があった太陽光発電設備、風力発電設備、定置用リチウムイオン蓄電池、コージェネレーション設備、エネファームの設置者及び関連するメーカーのうち、事前調査票への回答内容を踏まえ、複数の事業者へ対策実態についてのヒアリングを実施した。ヒアリングにおいては、技術的な対策である対策①②に係る対策を中心に確認を行った。事前質問票の回答結果に基づき、実施しているとの回答があった対策の具体的な実装方法、対策内容の妥当性の確認方法等について確認した。対策が十分ではないとの回答があった項目に対しては、対策実施に当たっての課題や障壁、対策実装への計画等を質問した。併せて、設置者とメーカー間の責任分界や、系統連系技術要件の解釈や追加情報提供等の要望について意見を伺った。

2) ヒアリング結果

ヒアリングは5つの設備種別の設置者及び設備メーカー計15社に対して実施した。ヒアリングの結果、設備種別により事業や設置者の性質及び典型的なシステム構成等に異なる特性があり、セキュリティリスクの構造や標準的な対策実装の状況に違いが見られた。また、設備種別により典型的なシステム構成や広く用いられている技術の違いから、系統連系記述要件への対応実態は異なり、要件への合致性の判断についてメーカーは懸念を持っていることが明らかになった。加えて、設備種別により設置者・メーカー・システム構築ベンダー間の役割分担にも差が見られ、相互の実態把握が十分とはいえないという課題意識があることが聴取できた。

また、系統連系技術要件の求める対策に対して、補足説明や対策実装例等を示すことを求

¹⁸ 各種別の関連業界団体に所属している設置者及び設備メーカーに配布した。設備メーカーにおいて、関連設備の一部を別会社が開発・製造している場合には、当該会社へ調査票を転送頂くよう依頼した。

める意見が挙げられた。この際、設備種別により特性が異なることから、この補足説明等は設備種別毎に整理されることが望ましいとの意見も得られた。

2.2.3 海外事業者へのヒアリングによる調査結果

諸外国における小規模発電設備等に対するセキュリティ対策の実態を把握するために、海外の事業者に対してヒアリング調査を行った。ヒアリング対象国は再生可能エネルギー導入量の多いドイツを対象とした。

ヒアリングはドイツの Stadtwerke Speyer GmbH に対して実施した。Stadtwerke（シュタットベルケ）とは公共インフラを整備・運営する自治体所有の公益企業を指し、電力に限らず、ガスや水道等のインフラも含まれる。Stadtwerke Speyer GmbH は、ドイツ南西部に位置する Speyer 市のシュタットベルケであり、電力だけでなく、天然ガスや水道インフラ・廃水処理インフラ、港の運営等を担っている。Stadtwerke Speyer の電力供給は全て再生可能エネルギーによって賄われており、持続可能な電力供給を行っているとしている¹⁹。

ヒアリング調査の結果、保有する再生可能エネルギーの規模及びサイバーセキュリティリスクの評価、実施しているサイバーセキュリティ対策と将来的な対応予定等について回答を得た。

2.3 規制体系に関する諸外国の最新動向等

文献、インターネット、ヒアリング等により調査を行い、サプライチェーン等のサイバーセキュリティに関する国外の規制体系について整理・分析を行った。

2.3.1 文献等による調査結果

(1) 米国のサプライチェーンリスクマネジメントに関する大統領令

2020 年 5 月 1 日にトランプ前大統領が基幹電力系統の保護を目的として大統領令に署名した。本大統領令は、基幹電力系統で使用される電気設備の安全性及び完全性を保護し、外国敵対者による米国電力インフラを標的とする攻撃（サイバー攻撃含む）の影響を低減させることを目的としている。エネルギー省長官に対して、外国敵対者に該当する国の決定や対象となる設備の特定について権限が与えられるほか、特定の設備やベンダーに対する事前認定付与の権限を与えている。しかし、2021 年 1 月 20 日にバイデン大統領により本大統領令が 90 日間停止することが発表された。図 2-4 に本大統領令の概要図を示す。

¹⁹ Stadtwerke Speyer GmbH “Strom: Naturstrom”
<https://www.stadtwerke-speyer.de/de/Privatkunden/Strom/Naturstrom/>

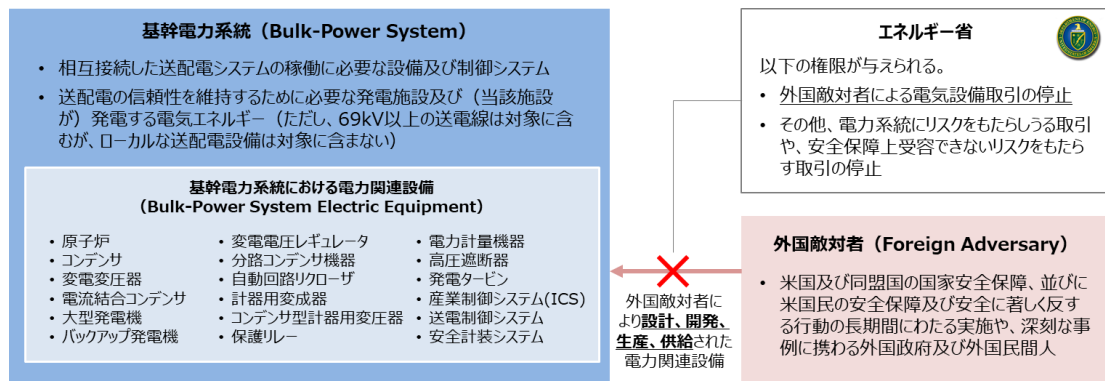


図 2-4 大統領令の概要図

2020 年 12 月 17 日に上記の大統領令を受けてエネルギー省（DoE）は、重要防衛施設に電力を供給する事業者が、基幹電力システムに関する中国製品の調達を禁止する行政命令を発表した。2021 年 1 月 16 日に発効され、1 月 16 日以降の取引にのみ適用される予定であったが、大統領令の 90 日間の停止を受け、取引停止の権限がエネルギー省に与えられていないため、本禁止令の効力も停止している状態である。

(2) EU の NIS2 指令

2020 年 12 月 16 日に EU 外務・安全保障政策上級代表から、EU における新たなサイバーセキュリティ戦略が発表された。本戦略では、「ヨーロッパのデジタル未来の形成」、「ヨーロッパのリカバリ策」、「EU の統一的なセキュリティ対策」が重要事項として挙げられている。発表されたサイバーセキュリティ戦略の一部として、サイバー脅威・フィジカル脅威への耐性を強くすることを目的に現存の NIS 指令を改訂した NIS2 指令の草案を発表した。現状、NIS2 指令は検証段階であり、各事業者は正式な適用後 18 か月以内に対応する必要がある²⁰。以下に主な変更点を示す²¹。

- 指令の対象範囲を対象業界の全ての大規模事業者と中規模事業者に拡大
- 重要サービスのオペレータとデジタルサービスプロバイダの区別を削除
- 最低限のセキュリティ事項を考慮したリスクマネジメント体制構築の要件を追加
- サプライチェーンリスクに関する事項を追加
- 各国の監査局に対してより厳格な監督措置、より厳格な執行要件を導入

2.3.2 海外機関へのヒアリングによる調査結果

米国の電力セキュリティ規制機関である、米国連邦エネルギー規制委員会（FERC）へのサプライチェーンに関するヒアリング調査結果を行った。文献等による調査結果やワーキンググループでの委員の意見を踏まえ、サプライチェーンに対して先進的な取り組みを実施している米国の規制機関をヒアリング調査対象とした。

²⁰ EC “New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient”
https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

²¹ EC “Proposal for directive on measures for high common level of cybersecurity across the Union”
<https://ec.europa.eu/digital-single-market/en/news/proposal-directive-measures-high-common-level-cybersecurity-across-union>

ヒアリングは、DoE の発した禁止の行政命令について、NERC CIP におけるサプライチェーン対策等について質問をした。DoE の発した禁止の行政命令の概要・対象・監査についての回答を得た。また、NERC CIP におけるサプライチェーンの取り組み等に関する情報提供を受けた。

3. 新規プレーヤーに関するサイバーセキュリティ対策の検討

電力分野においては、これまでの累次の改革を通じ、小売電気事業者への新規参入は着実に増加し、小売電気事業者数は 662 事業者（2020 年 7 月時点）、全販売電力量に占める新電力の割合は約 16.1%（2020 年 3 月時点）に到達した。こうした新電力を含めた小売電気事業者についても、サイバー攻撃を受けた場合には、その結果として情報漏洩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考えられる。例えば、需要・調達計画が改ざん等されると、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、電力分野におけるサイバーセキュリティ対策は、小売電気事業者も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、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、小売勉強会という）」が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 SWG の下に設置された。小売勉強会では、小売電気事業を取り巻くサイバーセキュリティに関する現状や課題を整理した上で、小売電気事業者が確保すべきサイバーセキュリティ対策の項目についての検討が行われた。

本事業では、小売勉強会及び関連する会合等の運営を行うとともに、議論の内容に基づいて「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（以下、小売ガイドラインという）」案を作成した。

3.1 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等の運営

本事業期間において、計 3 回の小売勉強会が開催された。このほかに、小売勉強会の開催に先立って行われた事前セミナー、小売ガイドライン作成のための作業会が開催された。本事業では、以下の日程でこれらの運営を行った。

- 2020 年 8 月 19 日：小売電気事業者向けサイバーセキュリティ対策セミナー
- 2020 年 11 月 6 日：第 1 回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
- 2020 年 11 月 26 日：小売電気事業者のサイバーセキュリティ対策に係る作業会
- 2020 年 12 月 9 日：第 2 回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
- 2021 年 1 月 22 日：第 3 回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

3.1.1 小売電気事業者向けサイバーセキュリティ対策セミナーの運営

小売電気事業者向けサイバーセキュリティ対策セミナーは、小売勉強会に先立って開催された。当該セミナーでは、勉強会設立の背景として、小売電気事業者に想定されるサイバー攻撃の脅威についての説明と、令和元年度に実施された全ての登録済小売電気事業者を対象としたアンケート結果の解説等を行った。加えて、有識者によるゲスト講演を通じて、直近のサイバー脅威と対策のポイントについての情報提供を行った。

小売電気事業者向けサイバーセキュリティ対策セミナー開催概要

日時：2020 年 8 月 19 日 9 時 00 分～12 時 00 分

場所：オンラインセミナー（登録制）

出席者：小売電気事業者 152 社 261 名（参加登録実績）

次第：

1. 小売電気事業者に想定されるサイバー攻撃の脅威について（資源エネルギー庁）
2. サイバーセキュリティ対策アンケート調査の結果解説（三菱総合研究所）
3. 情報セキュリティ 10 大脅威とその対策（独立行政法人情報処理推進機構）
4. 小売電気事業者をとりまくサイバーセキュリティ状況（一般社団法人 JPCERT コーディネーションセンター）
5. サイバーセキュリティ対策強化に求められる能力と、その調達方法（門林雄基 奈良先端科学技術大学院大学 先端科学技術研究科教授）
6. 勉強会のご案内

3.1.2 第 1 回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の運営

小売勉強会の開催に当たっては、全ての登録小売電気事業者宛に案内を発出し、自由参加を募った。参加登録を行った事業者には事前アンケートを配布し、自社のサイバーセキュリティ対策の状況と課題についての記入を求めた。

第 1 回勉強会当日は、はじめに小売電気事業者勉強会の設置主旨が改めて告知され、小売電気事業者が必要な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場であることが確認された。また、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 SWG の下に位置付けられ、電力 SWG を構成する委員をはじめとする有識者からの支援が提供されること等が説明された。

次にこれらを踏まえ、小売電気事業者に想定される脅威とその対策状況、望ましい対策項目についての討議が行われた。望ましい対策項目は、事前アンケートにおいて多くの事業者が参照していると回答した「サイバーセキュリティ経営ガイドライン」の構成に基づく形で「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」を作成することとし、小売電気事業者向けの重要事項の整理と、小売電気事業者の対策実践例の取りまとめを行う方向性が提案され、具体的な内容については勉強会とは別に有志による作業会を設置し、当該作業会にて検討及び編集作業を行うことが合意された。

第 1 回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開催概要

日時：2020 年 11 月 6 日 10 時 00 分～12 時 00 分

場所：オンライン会議

出席者：小売電気事業者 27 社 34 名

オブザーバー：

有村 浩一 JPCERT/CC

大友 洋一 電力 ISAC

門林 雄基 奈良先端科学技術大学院大学
國松 亮一 日本卸電力取引所
桑名 利幸 情報処理推進機構
佐竹 潔泰 日本卸電力取引所 システムチームリーダー
山田 博之 電力広域的運営推進機関

議事次第：

1. 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の設置について
2. 小売電気事業者のサイバーセキュリティの確保について
 - (1) 小売電気事業者に想定される脅威
 - (2) 小売電気事業者の対策状況
 - (3) これらを踏まえた望ましい対策項目
3. 討議

3.1.3 小売電気事業者のサイバーセキュリティ対策に係る作業会の運営

第1回勉強会で合意された方針を受け、「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」の作成のための作業会を開催された。具体的には、事務局が作成した素案のレビューと小売電気事業者における対策実践の好事例集を作成するための事例についての情報提供及び執筆案の検討等が行われた。

小売電気事業者のサイバーセキュリティ対策に係る作業会開催概要

日時： 2020年11月26日 9時00分～12時00分
場所： 三菱総合研究所4階会議室及びオンライン会議の併用
出席者： 小売電気事業者6社13名
次第： 小売ガイドライン案のレビュー及び対策例集の作成

3.1.4 第2回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の運営

第2回勉強会では、作業会を通じて作成された小売ガイドライン案について、その概要と作業過程を説明した上で、勉強会参加者及び有識者によるレビューと改善のための討議を行った。小売ガイドラインの各対策事項について加筆や修正を行うべき点の指摘や、ガイドラインを今後どのように普及し、改訂していくかといった方針についての議論がなされた。また、本勉強会での指摘を踏まえて修正を行った小売ガイドラインは、第10回電力SWGにおいて審議をうけ、パブリックコメント募集の開始が承認された。これを受け、2020年12月18日から2021年1月16日までの期間にパブリックコメント募集が実施された。

第2回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開催概要

日時 : 2020年12月9日 10時00分～12時00分

場所 : オンライン会議

出席者 : 小売電気事業者 28社 46名

オブザーバー :

有村 浩一 JPCERT/CC

大友 洋一 電力 ISAC

門林 雄基 奈良先端科学技術大学院大学

國松 亮一 日本卸電力取引所

桑名 利幸 情報処理推進機構

佐竹 潔泰 日本卸電力取引所 システムチームリーダー

堀 英樹 電力広域的運営推進機関

山田 博之 電力広域的運営推進機関

議事次第 :

1. 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案の作成について
2. 討議

3.1.5 第3回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の運営

第3回勉強会は、第2回勉強会、第10回電力SWG、パブリックコメントにおける指摘の内容の共有と、これらを踏まえて修正を行った小売ガイドライン修正案を、勉強会構成員へと電子メールにて共有し、最終的な確認を行った。

小売ガイドライン最終案の内容への特段の指摘はなく、これを以て勉強会構成員による最終承認とし、第11回電力SWGにて小売ガイドライン公開へ向けた審議が行われた。

第3回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開催概要

日時 : 2021年1月22日～1月29日

場所 : 書面開催

出席者 : 小売電気事業者 36社

議事次第 :

1. 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ついて
2. 討議

3.2 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項目案の作成

本事業では、小売勉強会等の運営の活動と並行する形で、小売勉強会及び作業会における議論を取りまとめながらガイドライン案の作成と編集作業を行ってきた。作成した案は、小売勉強会及び電力 SWG への提示や、パブリックコメントに向けた草案として活用された。

3.2.1 ガイドラインの策定スケジュール

小売ガイドライン案の作成及び編集は、以下のスケジュールで行われた。

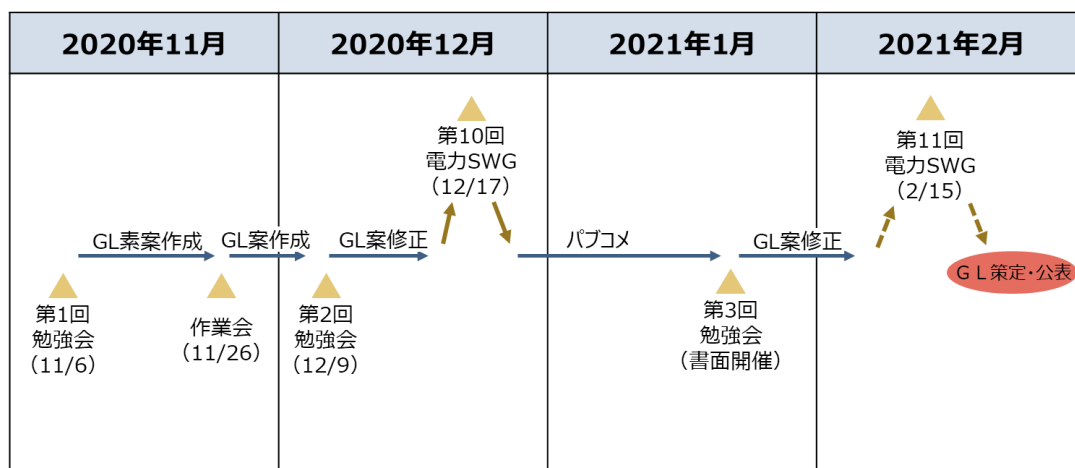


図 3-1 小売ガイドライン作成スケジュール

3.2.2 事前質問票におけるガイドラインへの期待のまとめ

小売ガイドライン案の作成に当たって、小売勉強会の事前のアンケートにおいて小売ガイドラインへの要望、期待することについて意見を求めた。この結果、ガイドラインの記述方針として、小売電気事業に特有の事項や個人情報保護の観点、最新の事例を反映することへの要望が挙げられた。また、対策内容については、事業者の規模の観点を踏まえた具体策を取りまとめることへの期待の声が多く挙げられた。さらに、現在活用しているガイドラインとしてサイバーセキュリティ経営ガイドラインが複数の事業者から挙げられた。

表 3-1 需要規模別の要望まとめ²²

	大規模	中規模	小規模
要望・期待	・ 自社のセキュリティポリシーの振り返り、見直しに役立てたい ・ 一つの基準や指針として役立つものになる ・ 組織的若しくは技術的対策の充実に期待 ・ 今後の非機能要求の参考にしたい ・ 小売電気事業における望ましい運用体制等を明示していただきたい ・ 組織的もしくは技術的対策の充実に期待する ・ ガイドラインにある程度の強制力があると、社内環境の整備を進める上での基準となるのでやすい ・ 業界特有の事項、最新の事例などを定期的に発信していただくことを期待する	・ 個人情報保護の観点を重視してほしい ・ 人材確保の観点の情報も欲しい ・ インシデント発生時における個人情報保護に役立つことへの期待 ・ 中小企業が実施できるレベルのガイドラインが欲しい ・ 中小企業でも実施可能な費用、規模の内容でのまとめを期待したい ・ 事業者規模に適した対策の案も必要と感じる ・ セキュリティ対策のロードマップについて知りたい ・ 電力事業に特化したサイバー攻撃の情報提供を期待 ・ 対策内容がチェックリストで整理できるような具体的なアウトプットになるとよい	・ 実際のセキュリティインシデントについての情報公開を希望 ・ 業界としての対応の動きを把握したい ・ 「どこまで対策すれば大丈夫なのか」という点に踏み込んだ真に活用しやすいガイドラインを目指して作成をお願いしたい ・ 個人情報の保護の観点を重視してほしい ・ 幅広い企業・業種からの意見が集約されるので、弊社がどういった対策を取るべきかより深く検討したい

3.2.3 第 1 回小売勉強会における意見

第 1 回小売勉強会では、小売電気事業者独自の視点を盛り込む必要性の認識は一致していた。個人情報等の扱う情報の特徴や、対策が未成熟な段階にある事業者も活用可能な対策例を提示することへの要望が複数挙げられた。また、小売ガイドラインを経営層の認識を高めるために活用すべきであるとの意見もあった。

表 3-2 第 1 回小売勉強会における主な意見

要望・期待	発言者
小売独自のセキュリティ対策を項目の記載が欲しい。松竹梅等の対策レベル毎に示していただけると、経営層に対して必要性や位置づけをアピールしやすい。	事業者
扱う情報によって指針があるとよい。	事業者
個人情報を扱うリスク等を踏まえて、検討のレベルを決めることが望ましいと考えている。	事業者
絞り込んだトピックでガイドラインを作成することが重要である。小売電気事業者としてのサイバーセキュリティ対策を掲げる上で、顧客情報保護の観点をよりフォーカスしてほしい。	事業者
小売電気事業者に則した外部ベンダー等のマネジメントのガイドラインがあると良いと考えている。	事業者
経営層にセキュリティの重要性を認識してもらう必要がある。セキュリティの重要性を認識しつつ実施可能なバランスを取ったセキュリティ対策を示してほしい。	オブザーバ
小売電気事業としての特異性をうまく示し、小売電気事業として何をすべきか、JEPXや広域とどのように連携すべきかが要素として組み込まれるとよい。	オブザーバ
ベストプラクティスを明文化し共有できるとよい。	オブザーバ

3.2.4 作業会を通じた素案の作成

作業会では、事前質問票への回答及び第 1 回小売勉強会での意見を踏まえ、複数事業者で活用中であるサイバーセキュリティ経営ガイドラインの構成を踏襲しながら、小売電気事

²² 勉強会では、需要の観点では、大（年間 20 億 kWh 以上）、中（年間 2 千万 kWh 以上）、小（年間 2 千万 kWh 未満）、売上規模の観点では、大（年間 50 億円以上）、中（年間 5 千万円以上）、小（5 千万円未満）を目安に議論した。

業者として特に重視すべき事項や、小売勉強会参加者の実践している対策の好事例を網羅的な視点から整理し、小売ガイドライン素案の作成を行った。また、作業会参加者の対策事例をより詳細に聴取し、詳細対策事例として整理し、対策事例集に追記した。

表 3-3 第 1 回小売勉強会での意見を踏まえた方針案の検討結果

御意見のまとめ	ガイドライン作成方針案
1 - 自社のセキュリティーポリシーの検討に活用したい - 組織的対策と技術的対策の視点が含まれるべき	複数事業者でポリシー検討に活用中であるサイバーセキュリティ経営ガイドラインの構成を踏襲し、網羅的な視点から整理
2 - 経営層への訴求や社内調整に本ガイドラインを使いたい - 電力分野におけるサイバー攻撃事例の情報がほしい	1章にガイドラインの位置づけ及び具体的な国内外のサイバー攻撃事例を記載することで、対策の必要性を強調
3 - 小売電気事業者独自の観点を盛り込んでほしい - 扱う情報や関係組織にも着目した分類を行ってほしい	2章に小売電気事業者の特徴と事業の種類の解説を記載。3章の対策には特に関わりの深い類型を紐づけ
4 対策リストとして活用したい	3章に事業者の対策事例をリスト化して記載
5 - 中小規模の事業者でも対応可能な水準のまとめがほしい - 幅広い事例の中で自社にあてはまる水準を検討したい	これから対策に取り組む事業者にとっても活用しやすいような詳細事例解説を追記
6 個人情報保護の観点を重視して記載してほしい	特に低圧で重要な個人情報保護の観点からの対策は、ガイドライン3章においてもポイントを明示

ガイドライン素案の基本構成と記載内容は以下のとおりである。

表 3-4 小売ガイドラインの基本構成と記述内容

目次構成	記載内容
1. はじめに	○小売電気事業者へのサイバー脅威と本ガイドライン策定の背景 経営層向けに対策の必要性を喚起するために、脅威動向の情報、ガイドライン策定の背景を記載 ○本ガイドラインの構成と活用方法 ガイドラインの構成と想定読者、サイバーセキュリティ経営ガイドラインとの関係を記載。
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	○小売電気事業者の企業環境とサイバーリスク ○小売電気事業者の情報システム構成の例 ○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特性やシステム構成を加味したサイバーリスクの特徴と小売電気事業者の事業形態を踏まえた類型について記載。
3. 小売電気事業者における重要10項目の実践規範	○指示1～指示10 サイバーセキュリティ経営ガイドラインと同様に、重要10項目の指示事項のそれぞれについて、「対策を怠った場合のシナリオ」と「小売電気事業者の対策実践例」を記載した。 また、本ガイドライン独自の取り組みとして、「詳細対策事例」として、より具体的な取組に至った背景やノウハウに関する記述を含む事例集を追記した。

表 3-5 詳細対策事例の一覧

指示事項別の詳細対策事例
- 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 [最小限のセキュリティポリシーからの開始] [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] - 指示 2 サイバーセキュリティリスク管理体制の構築 [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] [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] - 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 [経営層への定期的な情報提供] [組織全体のセキュリティ基礎能力の底上げ] [役割の付与による育成] - 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 [個人情報リスクの分析と対応] [サイバーセキュリティ保険への加入] [CPSFの活用] - 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 [システム更改のタイミングを有効活用する] [一般消費者向けサービスの不正アクセス対策] [CPSFの活用] - 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 [SECURITY ACTIONへの参加] [たすき掛け方式による内部監査の実施] - 指示 7 インシデント発生時の緊急対応体制の整備 [通常運用手順と緊急対応手順の関連付け] [特定の状況を想定したシナリオ型演習] - 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 [外部機関との予備のデータ送受信方式を用意する] [システムバックアップとリカバリテストの実施] [インシデント報告時の具体的な連絡先の整理] - 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 [システムベンダーとのセキュリティ要件の共有] [委託先検査方法の使い分け] - 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 [公的機関の情報源からの情報収集] [情報共有コミュニティへの参加（電力ISACの紹介）]

3.2.5 第 2 回小売勉強会、第 10 回電力 SWG を踏まえた修正

小売ガイドライン素案に対し、第 2 回小売勉強会及び第 10 回電力 SWG において、勉強会参加者間の議論、有識者からの指摘等を踏まえた修正作業を行った。修正した小売ガイドライン案は、パブリックコメント募集時の原案とされた。

表 3-6 第 2 回小売勉強会及び第 10 回 SWG における意見

御意見のまとめ	ガイドライン修正方針
1 • 典型的なシステム構成図の表現へのご意見	• より解釈が明確となる形の表記へ修正
2 • 活用可能な参考情報等についてのご意見	• 注釈欄への記載を充実
3 • パッケージベンダー等にヒアリングをして意見聴取すべきである	• パッケージベンダー 2 社にヒアリングし、内部犯行の脅威への考え方を補記
4 • 事業継続性の重要性を強調すべきである	• 2章に事業継続の観点からの対策の必要性を追記
5 • プログラムの完全性確保をより強調すべきである	• 2章に処理や値の正確性が失われた場合の脅威等を追記

3.2.6 パブリックコメント結果を踏まえた修正と第 1.0 版公開の承認

パブリックコメントでの指摘を踏まえた修正を加えた小売ガイドラインを「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 Ver1.0」の最終案とした。最終案に対する審議が第3回勉強会、第11回電力SWGにおいて行われ、公開版として承認された。公開版は、経済産業省のウェブサイトへの掲載が行われた。²³

²³ 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 Ver1.0」
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/20210222_report.html

4. ワーキンググループの運営

有識者（学識経験者やサイバーセキュリティ関連団体等を含む）や電気事業者等の委員によって構成され、我が国の電力分野における更なるサイバーセキュリティ向上策についての検討を行う、産業サイバーセキュリティ研究会ワーキンググループ 1 傘下の電力サブワーキンググループ（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。SWG では、電気事業者によるサイバーセキュリティ対策の実態把握や海外・他業種の動向調査を踏まえ、強化していくべき中長期的課題に対する取り組みを主に議論した。検討した主な中長期的課題は以下の 3 点である。

1. 新規プレーヤーのサイバーセキュリティ対策について
2. 大手電気事業者のサイバーセキュリティ対策について
3. サプライチェーンリスクへの対応について

なお、本 SWG は平成 30 年度から継続的に開催されているものであり、本事業では第 9 回から第 11 回の運営を行った。

4.1 第 9 回 SWG の運営

第 9 回 SWG では、大手電力会社のサイバーセキュリティ対策について、電気事業連合会の取りまとめの下で実施中の実態把握調査の進捗状況及び直近のサイバーセキュリティインシデントの情報に基づいた議論が行われた。

また、新規プレーヤーのサイバーセキュリティ対策について、小規模発電設備等におけるセキュリティ対策ヒアリングの実施方針案、小売電気事業者のサイバーセキュリティ対策の確保のための勉強会設置案について討議され、了承された。また、サプライチェーンセキュリティ規制の海外動向に関する報告が行われ、国内の対応について議論された。

第 9 回 SWG の出席者、議題及び議事要旨を以下に示す。

産業サイバーセキュリティ研究会 WG1 電力 SWG（第9回）議事要旨

日時：2020年9月29日 10時00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）	有村 浩一	JPCERT/CC
	稲垣 隆一	稲垣隆一法律事務所
	岩見 章示	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
	大友 洋一	電気事業連合会
	桑名 利幸	情報処理推進機構
	新 誠一	電気通信大学
	高倉 弘喜	国立情報学研究所
	谷口 浩	東京電力ホールディングス株式会社
	手塚 悟	慶應義塾大学
	新田 哲	JFE ホールディングス株式会社

議題

1. 大手電気事業者のサイバーセキュリティ対策について
2. 新規プレーヤーのサイバーセキュリティ対策について
3. サプライチェーンリスクへの対応について

要旨

1. 大手電気事業者のサイバーセキュリティ対策について

- （1） 「大手電気事業者の実態把握について」を事務局より説明。
- （2） 「大手電気事業者のサイバーセキュリティ対策状況の把握の進捗状況について」を電気事業連合会より説明。
- （3） 自由討議

- NIST Cybersecurity Framework を基準とした対策状況把握を実施するに当たって、ISMS 等の他の基準とは目的や背景が異なることに留意し、評価を行う必要がある。
- サイバーセキュリティの脅威は日々高度化しており、脅威として想定する範囲も動的に検討しなければならない。電力広域的運営推進機関や電力市場への影響等も範囲に含めた検討を深めていくべきではないか。
- 国際比較は、日本と海外の間でシステム的前提等が異なることを踏まえ、比較の目的と利益を明確にした上で実施すべきである。
 - 国際的に標準的な水準と見なされている対策を、我が国として見落としがな
いことを確認することが第一の目的である。

(4) 「会員制 Web サービスでの不正アクセスインシデントについて」を電気事業連合会より説明。

(5) 自由討議

- Web サービスを対象としたサイバー攻撃が増加している。事業者間で情報共有を行
いつつ、引き続き警戒する必要がある。

2. 新規プレーヤーのサイバーセキュリティ対策について

(1) 「小規模発電設備等におけるセキュリティ対策実態ヒアリングの方針について」
を事務局より説明。

(2) 自由討議

- 必ずしも設置者自身によってサイバーセキュリティ対策が行われる場合ばかりで
はない。対策実態を確認する際には、想定する脅威や簡易的な対策実施チェックリ
スト等による事前確認を行った上で、詳細内容をヒアリング等で確認することが
有効ではないか。
- 期間が限られているため、ヒアリング対象者に優先度を付け、リスクが高いと考え
られる領域からヒアリングを実施する必要がある。
- ヒアリング項目が重要となる。委員からの意見を反映するための事前照会を実施
していただきたい。

(3) 「小売電気事業者のサイバーセキュリティの確保について」並びに「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について（案）」を事務局より説明。

(4) 自由討議

- 重要な取組であると考え。知見や方法論を蓄積し、他の新規プレーヤーに対しても
も応用できると良い。

- 自主的な取組である一方、内容が不十分なものにならないように配慮する必要がある。
- 勉強会は、本サブワーキンググループの配下に位置付け、ガイドラインの内容に関する審議も行うことを予定している。
- 小売電気事業者は電気事業法上の技術基準適合義務の対象ではないものの、登録制であることは留意すべきである。

3. サプライチェーンリスクへの対応について

- (1) 「米国サプライチェーン規制等の状況について」を事務局より説明。
- (2) 「CPIC 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。
- (3) 自由討議
 - サプライチェーンリスク管理のためには、個社ではなく複数社によるコレクティブな対応が必要である。リスクがセキュリティの許容対策レベルを超えた際に、どのような緩和策を取っていくかも考えていくべきである。
 - サプライチェーンの議論も含め、事業者には様々なチャネルからセキュリティに関連する情報が入ってきている。電力広域的運営推進機関のような、多数の事業者との連絡経路を持つ組織とも連携しながら議論を進められると良い。

(以上)

4.2 第 10 回 SWG の運営

第 10 回 SWG では、電力システムに想定される脅威の広がりを踏まえ、日本卸電力取引所及び電力広域的運営推進機関を迎え、それぞれのサイバーセキュリティ対策への取り組みについて説明を受けるとともに、これに基づいた議論や委員からの助言などが行われた。

また、新規プレーヤーのサイバーセキュリティ対策について、小規模発電設備等における実態ヒアリングの中間報告及び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作成方針についての説明が行われ、これについて議論と了承がなされた。

第 10 回 SWG の出席者、議題及び議事要旨を以下に示す。

産業サイバーセキュリティ研究会 WG1 電力 SWG（第 10 回）議事要旨

日時 : 2020 年 12 月 17 日 10 時 00 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)	有村 浩一	JPCERT/CC
	稲垣 隆一	稲垣隆一法律事務所
	岩見 章示	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
	大友 洋一	電気事業連合会
	門林 雄基	奈良先端科学技術大学院大学
	桑名 利幸	情報処理推進機構
	新 誠一	電気通信大学
	高倉 弘喜	国立情報学研究所
	谷口 浩	東京電力ホールディングス株式会社
	手塚 悟	慶應義塾大学
	新田 哲	JFE ホールディングス株式会社

議題

1. 日本卸電力取引所及び電力広域的運営推進機関におけるサイバーセキュリティ対策について
2. 新規プレーヤーのサイバーセキュリティ対策について

要旨

1. 日本卸電力取引所及び電力広域的運営推進機関におけるサイバーセキュリティ対策について

- (1) 「日本卸電力取引所と電力広域的運営推進機関におけるサイバーセキュリティ対策について」を事務局より説明。
- (2) 「日本卸電力取引所におけるサイバーセキュリティ対策」を日本卸電力取引所よ

り説明。

- (3) 「電力広域的運営推進機関におけるサイバーセキュリティ対策」を電力広域的運営推進機関より説明。
- (4) 自由討議
- 日本卸電力取引所、電力広域的運営推進機関のそれぞれが実施するセキュリティ対策の詳細の確認及び委員からの助言が行われた。
 - 日本卸電力取引所及び電力広域的運営推進機関が、それぞれのセキュリティへの期待やレベルを認識し、対策を講じていくことが重要である。

2. 新規プレーヤーのサイバーセキュリティ対策について

- (1) 「小規模発電設備等における実態ヒアリングに関する現状報告」を事務局より説明。
- (2) 自由討議
- 機能保証の観点で、業務の継続性や復旧の基準・手法についてヒアリングで確認する必要がある。
 - 新規設置に関する観点だけでなく、設置後の運用やメンテナンスに係る観点も確認できるとよい。
 - 想定外の事象が起きた場合の対応方針や訓練の実施状況についてヒアリングで確認する必要がある。
- (3) 「小売電気事業者のサイバーセキュリティの確保について」を事務局より説明。
- (4) 自由討議
- システム開発時の完全性の確保について追記する必要がある。
 - 利用方法を適切に誘導できるようなガイドラインの構成にしていきたい。
 - ガイドラインを本電力 SWG の名義で公表することには同意する。一方、継続して改訂することが重要であり、業界団体を中心に活用を推進できるとよい。

(以上)

4.3 第 11 回 SWG の運営

第 11 回 SWG では、大手電気事業者の実態把握に関連して、電気事業連合会からの国内大手電気事業者のサイバーセキュリティ対策に関する実態把握調査についての評価結果の報告、米国規制機関へのヒアリングを通じた海外動向に関する情報等に基づき、今後望まれる対応の方向性などについて議論が行われた。

また、新規プレーヤーのサイバーセキュリティ対策に関連して、小規模発電設備等におけるサイバーセキュリティ対策に関する実態把握ヒアリング調査結果を踏まえた施策の検討が行われた。

このほか、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パブリックコメント募集の結果が共有され、対応内容及びガイドラインの発行が承認された。さらに、アグリゲーターのサイバーセキュリティ対策制度についての報告が行われた。

第 11 回 SWG の出席者、議題及び議事要旨を以下に示す。

産業サイバーセキュリティ研究会 WG1 電力 SWG（第 11 回）議事要旨

日時 : 令和 3 年 2 月 15 日（月）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）	有村 浩一	JPCERT/CC
	稲垣 隆一	稲垣隆一法律事務所
	江崎 浩	東京大学大学院
	大崎 人士	産業技術総合研究所
	大友 洋一	電気事業連合会
	門林 雄基	奈良先端科学技術大学院大学
	桑名 利幸	情報処理推進機構
	新 誠一	電気通信大学
	高倉 弘喜	国立情報学研究所
	谷口 浩	東京電力ホールディングス株式会社
	都筑 秀明	日本電気協会
	手塚 悟	慶應義塾大学
	新田 哲	JFE ホールディングス株式会社

議題

1. 大手電気事業者のサイバーセキュリティ対策について
2. 新規プレーヤーのサイバーセキュリティ対策について

要旨

1. 大手電気事業者のサイバーセキュリティ対策について

- （1） 「大手電気事業者の実態把握について」を事務局より説明。
- （2） 「「大手電気事業者のサイバーセキュリティ対策状況の実態把握」に関する評価結果」を電気事業連合会より説明。
- （3） 「米国電気事業者のセキュリティ対策状況調査について」を事務局より説明。

(4) 自由討議

- 大手電気事業者のサイバーセキュリティ対策状況の実態把握は良い取組であり、継続的な改善のためには今後も実施し続けることが重要である。
- 継続的にアセスメントを実施する上で、実施担当者の交代等によって評価の基準や結果が変わってしまう可能性がある。評価のノウハウを共有できる場があるとよい。
- こうしたアセスメントを実施する意義や継続の必要性を経営層に理解してもらうことが重要。
- 電力分野を取り巻く環境の変化に対応して、アセスメントの対象範囲を拡大できると良い。

2. 新規プレーヤーのサイバーセキュリティ対策について

(1) 「小規模発電設備等におけるサイバーセキュリティ対策について」を事務局より説明。

(2) 自由討議

- 系統連系技術要件の対策実装例のような指針を示す方針に同意する。ただし、実装例を示すという取組以外にも、セキュリティ対策の重要性を啓発する取組や、経営層の理解を深めるための取組も必要である。
 - 業界団体と協力し、発電種別毎のガイドライン等を作成するようなやり方も考えられるのではないか。系統への影響が大きい設備から優先して作成することが望ましいだろう。
 - 小規模発電事業者には多くの事業形態が存在するため、役割や能力、事業者間の関係性等の整理軸を考慮した検討が必要である。
- 小規模発電は FIP 制度への移行における重要な論点である。特に蓄電池のような分散電源を含むシステムでは機器認証も論点とすべきではないか。
- より一般化した視点からは、サイバー空間上でのデータの授受に関する議論に基づき、安全安心にデータのやり取りができるサイバー空間を構築できるとよいと言えるだろう。

(3) 「新規プレーヤーのサイバーセキュリティ対策確保の方策について」を事務局より説明。

(4) 自由討議

- 最上位のアグリゲーターに責任を集中させるという整理について、それぞれが別

個のシステムを用いる際にどこまで実効性があるか懸念している。

- 今回は法体系の面からの報告であるが、ERAB セキュリティガイドライン上に記載のある教育プログラム等も考慮した上で、実効性を高めるための取組については引き続き議論させていただきたい。
- システムのクラウドへの依存度が上がってきていると認識している。ネットワークトラブル発生時に連絡手段を喪失するような事態を懸念しており、クラウドに障害等が発生した際の電力系統への影響も評価されたい。
 - ERAB セキュリティガイドラインにおいても、重要な観点として考慮された点である。具体的な基準策定の際にも再度確認をしたい。
- 「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」の公表について了承をする。
- ガイドライン等を作成する際には、具体的な基準や対策の選択肢を提示することが重要である。情報過多とならないよう記載の粒度にも留意する必要がある。

(以上)

令和２年度エネルギー需給構造高度化対策に関する調査（電力分野のサイバーセキュリティ対策のあり方に関する詳細分析）

報告書

2021 年 2 月

株式会社三菱総合研究所
デジタル・イノベーション本部
TEL (03) 6858 - 3578