経済産業省 御中

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

2020 年 3 月 13 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

表目次

1. はじめに

1.1 調査背景・目的

近年、サイバー攻撃の起点は急激に拡大し、攻撃の手法も高度化しており、サイバー攻撃の脅威は、あらゆる産業活動に潜むようになっている。今や、産業界全体の取組として、サイバーセキュリティ対策の強化が求められている。

電力分野においては、2016 年の小売全面自由化等による新規参入者の増加とともに、デジタル化が進展しつつある。また、2020 年には、オリンピック・パラリンピック競技大会が我が国で開催されることとなっており、電力分野におけるサイバーセキュリティ対策の重要度は増々高まっている。

電力分野におけるサイバーセキュリティ対策の取組として、諸外国のサイバーセキュリティ対策の調査や審議会での議論に加え、2016 年に日本電気技術規格委員会が策定したスマートメーターシステムセキュリティガイドライン及び電力制御システムセキュリティガイドラインが電気事業法下の技術基準と保安規程に取り込まれ、また、電力制御システムについては取り組み確認のためのマニュアルが作成されたところである。2017 年 3 月には、民間の電気事業者間のサイバーセキュリティに関する情報共有及び分析を行う組織「電力 ISAC」が設立される等、官民で様々なサイバーセキュリティ対策が行われてきたところであるが、サイバーセキュリティ対策は継続的に対策の実施状況を確認し改善を検討していくことが重要である。

本事業では、電気事業者のサイバーセキュリティ対策の取り組みの確認をより効率的に実施するための課題の洗い出しと改善策の検討を実施した。更に、2019 年 7 月に改定された電力制御システムセキュリティガイドライン及びスマートメーターシステムセキュリティガイドラインの変更点及び関連する文献の調査結果等を踏まえながら、取り組みの確認のためのマニュアル案の作成等を行った。

1.2 調査実施概要

調査目的を達成するために、以下の項目に関して調査を行った。

1. 電気事業者の取り組み確認の効率化に向けた課題の洗い出しと改善策の検討
2. 電気事業者の取り組み状況を確認するためのマニュアル案の作成

2. 電気事業者の取り組み確認の効率化に向けた課題の洗い出しと改善策の検討

電気事業者のサイバーセキュリティ対策の取り組みの確認をより効率的に実施するため、「平成３０年度新エネルギー等の保安規制高度化事業委託調査 （電力分野のサイバーセキュリティ対策検討事業）」にて作成された「電力制御システムガイドラインに基づく立入検査マニュアル（以下、H30 マニュアル）」を用いた確認手順に係る課題の抽出と分析、改善策の検討を実施した。

課題の抽出に際しては、産業保安監督部と連携した確認作業の模擬的な実施と検証を、及び産業保安監督部による取組状況の確認実施後のヒアリング調査をそれぞれ実施した。

これらの調査検証により抽出した課題を分析することで、確認手順の改善策を検討し、取り組み確認のためのマニュアル案文に反映すべき事項を整理した。

2.1 取り組み確認作業をより効率的に実施するための検討会の開催

産業保安監督部による取組状況の確認に先立ち、マニュアル案文の内容に準じた確認手順の模擬的な実施と課題の抽出を行うために、事前の検討会を開催した。産業保安監督部と連携し、実践的な内容を重視した課題の抽出と改善策の検討を行うため、以下の点を考慮して検討会のプログラムを作成した。

- 確認作業の実施者がサイバーセキュリティの事前知識を有することを前提とせず、基礎的な内容から効率的にインプットする
- 情報セキュリティ監査等の好事例を参考に、体系的に整理した確認手順案を提示する
- 具体的な課題を抽出するため、演習やデモンストレーションの要素を盛り込む

2.1.1 検討会の開催概要

検討会の開催概要を表 2-1 に示す。第 1 回および第 2 回のプログラムは同一であり、参加者の予定に合わせて参加可能な日程への参加を促したものである。内容は、電力制御セキュリティガイドラインの各条項に関する解説及び模擬的な確認作業を行う演習を中心に構成し、各回 2 日間にわたって実施した。検討会参加者の概要を表 2-2 に示す。

表 2-1　検討会概要

名称	電力制御システムセキュリティ対策の確認に係る検討会
日程	【第 1 回】令和元年 9 月 4 日（水）～9 月 5 日（木） 【第 2 回】令和元年 9 月 12 日（木）～9 月 13 日（金）
場所	TKP 虎ノ門駅前カンファレンスセンター　カンファレンスルーム 4B
プログラム	第 1 日目 09:30-10:00　開会（本会実施の背景のご説明） 【経済産業省　電力安全課】 10:00-12:00　サイバーセキュリティ基礎 【制御システムセキュリティセンター】 12:00-13:00　昼休憩 13:00-17:00　電力制御システムセキュリティガイドライン（解説と演習） 【三菱総合研究所】 17:00-17:30　まとめと振り返り 第 2 日目 09:30-10:00　第 2 日目の要点と流れの説明 【三菱総合研究所】 10:00-12:00　電力制御システムにおけるセキュリティインシデント対策デモ【制御システムセキュリティセンター】 12:00-13:00　昼休憩 13:00-17:00　電力制御システムセキュリティガイドライン（解説と演習） 【三菱総合研究所】 17:00-17:30　閉会（まとめと今後の流れ） 【経済産業省　電力安全課】

表 2-2　検討会参加者（合計 21 名）

第 1 回検討会参加者	北海道産業保安監督部、関東東北産業保安監督部、中部近畿産業保安監督部、中部近畿産業保安監督部・北陸産業保安監督署、中部近畿産業保安監督部・近畿支部、中国四国産業保安監督部、中国四国産業保安監督部・四国支部から計 15 名
第 2 回検討会参加者	関東東北産業保安監督部、関東東北産業保安監督部・東北支部、九州産業保安監督部、那覇産業保安監督事務所から計 6 名

「サイバーセキュリティ基礎」では、電力制御システムにおけるサイバーセキュリティ対策に関する基礎的な知識の獲得を受講目標とし、サイバー脅威の動向及び取りうる対策の基礎的な講座を実施した。具体的には、制御システムに対するサイバー攻撃事例の紹介、制御システムの定義や典型的なシステム概要についての説明、電気事業者に対する現実的脅威についてのグループディスカッション等を行った。また、「電力制御システムにおけるセキュリティインシデント対策デモ」では、電力制御システムにおけるセキュリティインシデントとその対策のデモンストレーション等を実施し、電力制御システムにおけるサイバーセキュリティに関する具体的イメージの獲得を支援した。

「電力制御システムセキュリティガイドライン（解説と演習）」では、基礎講座の内容を踏まえつつ、解説編として、電力制御システムセキュリティガイドラインの記述内容の詳細な理解と取り組み確認作業の実施手順の把握を目的に、ガイドライン及び確認マニュアルの各条項の解説を行った。また、演習編では、サンプル書面（架空の企業のセキュリティポリシー、体制図、管理規定等）を用いた模擬的な確認作業を実施し、具体的なイメージの獲得と確認作業実務を行う上で課題となり得る事項の抽出を行った。

課題となり得る事項の一覧は、当日の質疑内容の記録及び検討会後にアンケート調査を行うことにより、整理・分析を行った。

2.1.2 検討会で抽出された課題とその分析

(1) 検討会における質問及び意見の概要

検討会では、参加者からは、ガイドラインへの質問、マニュアルに対する意見の他に、技術的事項への質問や確認作業実施の段取りや進め方に関する課題の指摘があった。技術的な専門用語に対する理解・解釈に関するものから、事業者との事前調整や事後のフィードバックに関して予想される課題の共有と議論が行われた。

(2) 検討会後のアンケート結果

検討会後に実施したアンケートでは、検討会の評価、検討会の内容の理解度、マニュアルの分かりやすさ、確認作業実施にあたっての懸念点等についての設問を設けた。

検討会の内容は、基礎講座やデモ等の導入による理解度向上効果、ガイドライン及びマニュアルの解説・演習の内容理解について、多くの参加者において一定の評価が得られた。個別の条項においては、機器・設備等の対策状況の確認に関する項目など、技術的な項目の理解度が相対的に低い結果となった。また、検討会中の質疑と同様に、事業者との事前調整や事後のフィードバックに関する課題の指摘、解決案の提示等があった。

2.1.3 検討会において抽出された課題の分析と改善策の検討

(1) 検討会において抽出された課題の分析

アンケート分析の結果、検討会の構成や内容の理解度については概ね問題が見られない結果となったが、技術的事項の理解については改善の余地が残った。質問内容の詳細等を分

析すると、マニュアル内に記述を読み解く前段階として、ネットワークの概念や情報技術に関する用語と言った基礎知識面に不足がある場合に、本来の意図を理解する際の障壁となっている傾向が見られた。

事業者との事前の調整に関しては、現地の確認作業に要する時間が限られる中で、事前確認の実施イメージが具体化されていないことが懸念の要因であると考えられる。また、事後のフィードバックについて、推奨事項の取扱いを巡る課題は、指摘と助言の性質の違いを様式に反映しきれていないことがフィードバックの難しさにつながってしまったと分析できる。

(2) 検討会においてにおいて抽出された課題に対する改善策の検討

マニュアルを利用する際の技術的事項の理解度に関する課題への改善策としては、電力制御システムセキュリティガイドラインに登場する概念、用語を中心に、背景にある基礎知識を補う補助資料の作成等が考えられる。

事前の調整については、取り組み確認作業の一連の流れを示すことで全体感を把握しやすくする等の改善が考えられる。確認対象の選定から、電気事業者との調整、事後のフォローと言った手順を示すことで、一定の標準化を行う効果も期待できる。推奨事項の記述改善は、より助言事項の性質を反映した様式への修正を実施した。

2.2 産業保安監督部による取組状況の確認実施後のヒアリング調査

事前に実施した検討会の内容も踏まえながら、2019 年 12 月より各地域の産業保安監督部によって、電気事業者へのサイバーセキュリティ対策への取組状況の確認が順次実施された。本調査では、実施を通じた課題の抽出を目的に、産業保安監督部へのヒアリング調査を実施し、改善策の検討を行った。

2.2.1 ヒアリング調査の実施概要

ヒアリング調査は、2020 年 2 月末時点で既に取組状況の確認を終えた産業保安監督部 7 者を対象に、共通の様式の調査票への回答を依頼する形で実施した。質問票には、確認対象としたシステムの属性情報、確認に先立ち実施した準備内容、当日の進捗状況、課題となった点についての設問を設けた。

質問票への各産業保安監督部の回答の概要を表 2-3 に示す。

表 2-3　産業保安監督部へのヒアリング結果の概要

ヒアリング先	ヒアリング結果の概要
産業保安監督部 A	• セキュリティ関連文書は取扱いに慎重を要するものが多い。限られた時間内に確認を完了するためには、事前ミーティングを実施することも検討しながら、念入りな認識合わせを行うことが重要である。 • 検査は概ね順調に進み計画日数との乖離もなかった。

産業保安監督部 B	• 重要度等を踏まえながら確認対象を検討している。 • 概ね計画通りの進捗であった。
産業保安監督部 C	• 社会的影響の大きい設備を優先して確認している。 • 複数社に跨る規程は、位置づけを明確に確認しておくことが重要である。
産業保安監督部 D	• 検査対象の選定には様々な要素を考慮すべきと考える。 • 検査実施日以前に条文ごとに準備すべき資料の例示を行ったことが実地確認の効率化に寄与した。 • 確認する項目の順序を工夫することで、更に効率化の余地がある。
産業保安監督部 E	• 検査実施日以前に打ち合わせによる準備を念入りに行ったことで、意思伝達に齟齬がなく、円滑に進行する事が出来た。 • 用意すべき資料のイメージを提示することで、確認対象を明確化することが出来た。
産業保安監督部 F	• 検査実施日以前に、事前提出された資料等に対する確認、質問への回答依頼等を実施した。 • 書面は取扱いに慎重を要する情報を含み、また内容の審査に高度な専門知識が求められることから、情報セキュリティマネジメントに係る研修は引き続き必要と考える。
産業保安監督部 G	• 概ね計画通りの進捗であった。 • 外部持出が禁止された資料の事前確認には限界がある。ガイドラインの条項に対応した確認対象資料のとりまとめを事業者へ依頼したことは効果的であった。

2.2.2 ヒアリング調査において抽出された課題の分析と改善策の検討

(1) ヒアリング調査において抽出された課題の分析

産業保安監督部へのヒアリングの結果からは、確認項目の説明に要する資料類の認識合わせを事前に実施することが、確認当日の円滑な進行に大きな効果を発揮することが読み取れる。資料類には、機微な情報を含み取扱いに慎重を要するものを含むため、事前の確認には、ミーティングの実施、書面の代表的名称等を具体的に示す等の様々な手段の組み合わせ、確認すべき事項の認識合わせを行うことが有効であると考えられる。

また、確認対象とすべきシステムに関しては、初年度である今回の確認においては、最も重要度の高いシステムが対象として選択されたが、次年度以降の対象選定基準についての課題が提起された。

(2) ヒアリング調査において抽出された課題に対する改善策の検討

事前の準備に関しては、検討会の段階で推奨される事項として言及を行っていたこともあり、全ての産業保安監督部において、実務上の工夫を加えながら実行計画へ反映され、確認の効率化へ寄与することが確かめられた。特に効果を発揮した事前調整の具体的事例をナレッジ化し、各産業保安監督部に展開することで、より全体の効率化を図る改善が考えられる。

また、確認対象とすべきシステムに関しては、様々な評価基準を踏まえての検討が求められることから、画一的な選定基準を提示することは適切でない。複数の評価軸を検討材料として複数提示することが改善策として考えられる。

3. 電気事業者の取り組み状況を確認するためのマニュアル案の作成

電気事業者の取り組み状況を確認するためのマニュアル案として、電力制御システムセキュリティガイドラインに基づくマニュアル案の改善、スマートメーターシステムセキュリティガイドラインに基づくマニュアル案の新規作成をそれぞれ実施した。

マニュアル案文の作成にあたっては、平成 30 年度事業での検討内容を引き継ぎつつ、令和元年の電力制御システムセキュリティガイドライン及びスマートメーターシステムセキュリティガイドラインの改定内容、電気事業者の取り組み確認の効率化に向けた課題への改善策を踏まえるとともに、電気事業者へのヒアリング調査、並びに関連する文献の調査を実施し、記載内容を検討した上でマニュアル案文を作成した。

なお、マニュアル案文作成にあたっては、数項目について作成した段階で経済産業省と協議を行い、他の項目の案文作成後に、産業保安監督部等との調整を行った。

マニュアル案文作成に係る検討及び作業の全体概要は、以下の通りである。

表 3-1　マニュアル案文作成の概要

実施事項	電力制御システムセキュリティガイドラインに基づく確認マニュアル案文（電制マニュアル）	スマートメーターシステムセキュリティガイドラインに基づく確認マニュアル案文（スマメマニュアル）
ガイドライン改定内容の反映	H30 マニュアルへ電力制御システムセキュリティガイドライン（2019）の改定内容を反映	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）に基づき新規作成
検討会及び保安監督部へのヒアリング調査で抽出した課題への改善策の反映	検討会実施時に抽出した課題への改善策（2.1.3）及びヒアリング調査時に抽出した課題への改善策（2.2.2）をマニュアルへ反映	電制マニュアルの改善と同内容の改善を実施
電気事業者へのヒアリング調査を通じた改善	電気事業者へのヒアリング結果をマニュアルへ反映	（スマートメーターシステムを保有する一般送配電事業者へのヒアリングは本調査対象外）
スマートメーターセキュリティ関連文献の調査を通じた改善	（スマートメーターに限定した内容のため対象外）	各国のスマートメーターセキュリティ関連文献の調査結果をマニュアルへ反映

3.1 電力制御システムセキュリティガイドラインに基づく確認マニュアル案文の作成

電力制御システムガイドラインに基づく確認マニュアル案文の作成について、個々の実施事項の内容を以下に示す。

3.1.1 電力制御システムセキュリティガイドライン改定内容の反映

日本電気技術規格委員会によって 2016 年に策定された電力制御システムセキュリティガイドラインは、東京オリンピック・パラリンピック競技大会等の大規模な国際イベントの開催を間近に控え、2019 年 7 月に改定された。日常の運用・保守や、電気事業者間の情報共有を通じて寄せられた改訂要望と共に、経済産業省の設置する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 電力サブワーキンググループにおいて取り纏められた「電力制御システムのセキュリティ向上策に関する提言」の内容から速やかに織り込むべき事項が反映されている。

本事業では、H30 マニュアルを基に、電力制御システムセキュリティガイドライン（2019）の改定点の反映を行った。この改定では、いくつかの対策事項において、その解説への加筆・修正が行われている。

「電力制御システムのセキュリティ向上策に関する提言」では、（1）サイバーインシデントに対応する体制の強化、（2）人材の育成・確保、（3）事象発生時の対応強化、（4）その他 に関する対策強化が提言された。これらの提言に対し、電力制御システムセキュリティガイドラインでは、運用実態を考慮しながら、OT システム組織とセキュリティ組織の相互協力や、戦略マネジメント機能の設置と対応した人材の育成、サービス継続の観点に留意したセキュリティマネジメントを勘案することが新たに要件とされた。

これらの改定点を踏まえ、H30 マニュアルの再検証を行い、確認のポイント・確認方法等の各項目において、マニュアル案文の追記や修正の要否を検証した。

3.1.2 検討会及び保安監督部へのヒアリング調査で抽出した課題への改善策の反映

2.1.3 では、検討会実施時に抽出した課題として、技術的確認事項に対する理解度についての課題及び電気事業者との事前の調整における具体的なイメージの把握に関する課題を挙げた。

技術的確認事項への理解度の課題については、マニュアルの各項目の理解に基づく課題よりも、技術的背景知識に関する説明の不足に起因するものと分析し、基礎知識を補う補助資料の作成を改善策として検討した。これを踏まえ、マニュアル案文そのものではなく、背景知識の説明を記載した補助資料を別添として追加することとした。

具体的には、外部ネットワーク、他ネットワークといった用語の違いを理解するためのネットワークの基礎知識や、制御システムにおける機器のアクセス制御の実装方式、通信の暗号化の仕組み等の解説を行った参考資料を作成し、マニュアルの別添資料へ追加した。

電気事業者との具体的なイメージの把握に関しては、H30 マニュアルでは、電気事業者との事前調整等は作成の対象範囲外であったことから、一連の流れを整理した実施手引書を新規に作成し、マニュアルへ追加した。実施手引書へは、事前の調整、検査の実施と指摘及び助言についての実施手順例の記載を行った。

また、産業保安監督部による取組状況の確認実施後のヒアリング調査においては、事前調整における好事例のナレッジ化と、確認対象選定基準を検討する際に参考とするための評価軸の提示を改善策として挙げた。これらは、実施手引書の参考例に好事例を反映すると同時に、事前の調整時の参考情報として、システム重要度やその他の評価軸に関する解説を記載した。

3.1.3 電気事業者へのヒアリング調査を通じた改善

電気事業者の取り組み状況を確認する際に、事業種別毎の特徴を踏まえた確認を実施することを目的に、送電事業者、特定送配電事業者及び発電事業者の各 1 事業者ずつへ、電力制御システムの構成等に関するヒアリング調査を実施した。発電事業者は、2.1.3 節における課題抽出結果も踏まえ、太陽光発電システムを持つ電気事業者へのヒアリングを実施した。

(1) 電気事業者へのヒアリング実施概要

電気事業者へのヒアリング調査は、各電気事業者の保有する電力システムの種類、主要な電力制御システムの構成を中心に調査を行った。また、実施しているセキュリティ対策の概要に関しても情報提供を受けた。

表 3-2　電気事業者へのヒアリング実施概要

事業種別	送電事業者	特定送配電事業者	発電事業者
実施時期	2020 年 1 月	2020 年 1 月	2020 年 2 月
質問項目	・システムの種別と重要度 ・送電事業者と一般送配電事業者のシステムの違い ・機器とネットワーク構成 ・セキュリティ規程の体系	・全体システム構成 ・電力系統との接続方法 ・機器とネットワーク構成 ・監視/制御の拠点 ・セキュリティ対策運用	・太陽光発電システムの構成例 ・機器とネットワーク構成 ・監視/制御の拠点 ・セキュリティ対策運用

(2) 電気事業者へのヒアリング結果の分析を踏まえた改善

各電気事業へのヒアリング調査から、事業者種別毎に保有する電力制御システムには固有の特徴が複数含まれることが分かった、取り組み状況の確認を実施する際にも、それぞれの特徴を踏まえた構成を事前に想定することで、効率的な進行が可能になると考えられる。

マニュアルの改善のため、事業種別毎のヒアリング結果を踏まえ、システム構成における特徴の分析を行った。また、分析結果を整理し、事業者種別毎のサンプルシステム構成図を作成した。作成したサンプルシステム構成図は、マニュアルへ反映し、当該事業者種別の事業者への確認作業を実施する際に参照できるようにした。

3.2 スマートメーターシステムセキュリティガイドラインに基づく確認マニュアル案文の作成

スマートメーターシステムガイドラインに基づく確認マニュアル案文の作成について、個々の実施事項の内容を以下に示す。

3.2.1 改正後のスマートメーターシステムセキュリティガイドラインに基づいたマニュアルの新規作成

スマートメーターシステムセキュリティガイドラインは、電力制御システムセキュリテ

ィガイドラインと同様に、日本電気技術規格委員会によって 2016 年に策定された。スマートメーターシステムのセキュリティを確保するため、一般送配電事業者が実施すべきセキュリティ対策要求事項が定められている。

スマートメーターシステムセキュリティガイドラインに基づくマニュアルを新規作成するにあたり、改正後の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）を基準とし、一般送配電事業者のサイバーセキュリティ対策の取り組み状況を確認するためのマニュアル案文の作成を行った。電力制御システムセキュリティガイドラインに基づくマニュアルと同様に、ガイドラインの定める対策要求事項に対応する確認のポイント・確認方法等を整理した。組織的対策項目等の電力制御システムセキュリティガイドラインと共通項の多い確認項目に関しては、可能な限り確認ポイントを標準化することで、マニュアル利用者の混乱を防ぐための配慮を行った。

3.2.2 検討会及び保安監督部へのヒアリング調査で抽出した課題への改善策の反映

スマートメーターシステムセキュリティガイドラインに対して、3.1.2 で記述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くマニュアルへの改善事項と同等の内容を反映した。具体的には、背景知識の説明を記載した補助資料をスマートメーターシステムセキュリティガイドラインに基づく確認の実施時にも参照可能な内容へ調整した。

3.2.3 各国のスマートメーターシステムセキュリティ関連文献の調査を通じた改善

スマートメーターシステムセキュリティガイドラインに基づく確認マニュアル作成の参考とするため、各国のスマートメーターシステムセキュリティガイドラインに相当する文献について調査を実施した。

調査にあたっては、主要なスマートメーターセキュリティガイドラインに加えて、スマートグリッド/IoT システム向けのセキュリティガイドラインも対象に含めた。調査を行ったガイドライン、フレームワーク等は表 3-3 に示す通りである。表 3-4 から表 3-15 には、表 3-3 に挙げた 6 つの文献についての概要、評価スキーム、評価項目を整理した。

整理した内容は、特にマニュアルにおける確認のポイント及び手順の参考とし、内容へ反映した。

表 3-3　諸外国公的機関 調査文献一覧

項目	国・発行組織	文献名
1	ドイツ・BSI	BSI: Protection Profile for the Gateway of a Smart Metering System
2	英国・DECC	Smart Metering Equipment Technical Specifications – Version 2 (SMET 2)
3	フランス・ANSSI	First Level Security Certificate (CSPN)
4	米国・NIST	Guidelines for Smart Grid Cybersecurity (NISTIR 7628 Revision 1)
5	米国・NIST	Advanced Metering Infrastructure Smart Meter Upgradeability Test Framework (NISTIR 7823)
6	EU・ENISA	Baseline Security Recommendations for IoT

(1) BSI: BSI-CC-PP-0077

BSI の策定した Protection Profile for the Gateway of a Smart Metering System は、スマートメーターのセキュリティ及びプライバシー対策を対象とした評価保証基準である。ドイツ国内のスマートメーターは、本基準に基づいたセキュリティ認証を取得することが義務付けられている。

表 3-4　BSI: BSI-CC-PP-0077 調査・整理結果

名称	**Protection Profile for the Gateway of a Smart Metering System (BSI-CC-PP-0077, BSI-CC-PP-0077-V2)**
発行機関	BSI (Federal Office for Information Security)
概要	Protection Profile for the Gateway of a Smart Metering System は、ドイツ連邦電子情報保安局（BSI）によって 2014 年に策定された、スマートメーターのセキュリティ及びプライバシー対策を対象とした評価保証基準である。スマートメーターのうち、ゲートウェイ機器もしくは機能を評価対象とする点に特徴がある。ゲートウェイの定義は、メーターデータの収集、送信機能に加えデータの管理、統合を行う機能とされる。 国際標準規格であるコモンクライテリア（CC）認証の基準に従った評価を行う。エネルギー産業法に準拠した規制によって、ドイツ国内のスマートメーターは、本基準に基づいたセキュリティ認証を取得することが義務付けられている。
評価スキーム	コモンクライテリア認証仕様に則った手順によって認証が行われる。 BSI もしくは BSI の認定する認証機関が、認証を求めるスマートメーターを対象に、BSI が作成したプロテクションプロファイルの要求事項への準拠性の評価を実施する。 要求される評価保証レベルは EAL4+である。EAL4 で求められる方式設計、テスト、レビューの実施証跡の確認に加え、脆弱性分析を踏まえたテスト、レビューが要求される。また、認証プロセスに関する技術的ガイドラインとして、BSI TR-03109 が存在する。
評価項目	スマートメーターゲートウェイのセキュリティ及びプライバシーを評価するための項目が整理されている。 主要な評価項目は、メーターデータの暗号化、スマートメーターとサーバの機器間認証といった等、データの機密性と完全性を保証するための対策事項である。 PTB による詳細要件では、ゲートウェイモジュールに加え、スマートメーターシステムのサーバ、メーター設置点の通信アダプタ等に対する技術要件についても記述されている。非常に詳細な確認を行う仕様であり、多大な対策項目の評価を行うこととなるためドイツのスマートメーターのコスト高の原因となっているという批判もある。

表 3-5　BSI: BSI-CC-PP-0077 評価項目の概要

No.	セキュリティ対策項目
1	暗号サポート
2	利用者データ保護
3	ID と認証
4	セキュリティ管理
5	セキュリティ機能の保護
6	高信頼パス/チャネル

(2) DECC: SMET2

DECC の策定した Smart Metering Equipment Technical Specifications – Version 2 は、Data Communications Company (DCC)へ送信できる通信ユニットに関する仕様を含めたスマートメーターの技術仕様である。

表 3-6　DECC: SMET2 調査・整理結果

名称	**Smart Metering Equipment Technical Specifications – Version 2 (SMET 2)**
発行機関	DECC (Department of Energy and Climate Change)
概要	SMETS 2 は、英国エネルギー・気候変動省(DECC)によって策定されたスマートメーターの技術仕様であり、2012 年に策定された SMETS 1 の後継にあたる。SMETS 2 では、最新のスマートメーターについて取り扱うため、Data Communications Company (DCC)へ送信できる通信ユニットに関する仕様が含まれる。 2019 年 9 月時点では、新しく導入されるスマートメーターの約 73%が SMETS 2 に準拠している。既存の SMETS 1 メーターについては、2020 年末までに更新を行い、DCC システムを利用可能にする予定である。 ADM 等の SMETS 以前のメーターについては、最小限の機能は相互運用性があるが、通信機能等が利用できない場合もある。
評価スキーム	国の機関である通信電気セキュリティグループ(CESG)が、Commercial Product Assurance (CPA)の認証仕様を参照して Smart Metering Security Requirements と呼ばれるスマートメーターのセキュリティ要求事項を定めている。CPA 以外の国際標準規格を評価基準として参照することも可能である。CSEG による認定を受けた機関が評価を実施する。
評価項目	スマートメーターに関する物理的・機能的要件に加えて、インターフェース及びデータに関する要件を細かく定義している。ガスメーターに 33 件、電気メーターに 39 件の要求事項が存在する。機能要件の中にセキュリティに関する要求を含めている。

表 3-7　DECC: SMET2 評価項目の概要

No.	セキュリティ対策項目
1	セキュリティ証明書
2	暗号化アルゴリズム
3	ファームウェア
4	通信
5	セキュリティログ

(3) ANSSI: CSPN

ANSSI の策定した First Level Security Certificate は、様々な製品を対象として高水準のセキュリティレベルを認めるものであり、スマートメーターとデータセンターのセキュリティ認証で用いられている。

表 3-8　ANSSI: CSPN 調査・整理結果

名称	**First Level Security Certificate (CSPN)**
発行機関	ANSSI (National Cybersecurity Agency of France)
概要	CSPN は、2008 年に ANSSI によって制定された国際標準規格であるコモンクライテリア（CC）に基づく認証スキームである。様々な製品を対象として高水準のセキュリティレベルを認めるものであり、スマートメーターとデータセンターのセキュリティ認証で用いられている。 ANSSI によって認定された認証機関による審査が可能であり、時間及び人的リソースの削減、製品のセキュリティ仕様との整合性の分析、セキュリティ機能の有効性の測定等が主な特徴として挙げられる。
評価スキーム	ANSSI によって認定された認証機関によって、セキュリティ要件が十分に満たされているかを確認する。評価基準や手順等のフレームワークが ANSSI によって提供されており、異なる審査機関においても統一的な評価プロセスが可能である。 評価プロセスには、公開されている脆弱性をベースとした実製品のテストが含まれており、その結果をテクニカルレポートに纏め認証機関に提出し審査される。審査プロセスは通常 8 週間以内に完了されなければならない。
評価項目	製品のセキュリティ機能についてのチェックリストが与えられており、セキュリティ監査、コミュニケーション、暗号化サポート、ユーザーデータ保護、識別と認証、プライバシー保護等を確認する。 製品の適合性、脆弱性等に関する分析も評価項目に含まれる。

表 3-9　ANSSI: CSPN 評価項目の概要

No.	セキュリティ対策項目
1	セキュリティ監査

No.	セキュリティ対策項目
2	通信
3	暗号サポート
4	利用者データ保護
5	ID と認証
6	セキュリティ管理
7	プライバシー
8	セキュリティ機能の保護
9	資源利用
10	評価スコープへのアクセス

(4) NIST: NISTIR 7628

NIST の策定した NISTIR 7628 は、組織がスマートグリッドのセキュリティ対策を実装するための指針を提供するためのセキュリティガイドラインである。

表 3-10　NIST: NISTIR 7628 調査・整理結果

名称	**Guidelines for Smart Grid Cybersecurity (NISTIR 7628 Revision 1)**
発行機関	NIST (National Institute of Standards and Technology)
概要	NISTIR 7628 は、組織がスマートグリッドのセキュリティ対策を実装するための指針を提供するため、NIST が発行したセキュリティガイドラインである。アグリゲーターや市場運用者を含む、スマートグリッドに関連する事業者を対象とし、リスクの評価や適切な対策実施のためのフレームワークを提供している。リスクベースアプローチによって、スマートグリッドにおける脅威のシナリオをもとに、ハイレベルな安全性要件、リスク評価の枠組み、プライバシー問題の評価等が定められている。SGIP（Smart Grid Interoperability Panel）の下部組織 である CSWG（Cyber Security Working Group）が 2010 年に初版を策定、2014 年に改訂。
評価スキーム	サイバーセキュリティ戦略の策定ステップを 5 段階（①ユースケースの分析、②リスクアセスメント、③セキュリティ要件の評価・選択、④論理関係の確認とセキュリティ以外の推奨事項の確認、⑤適合性評価の実施）で提示している。②のリスクアセスメントでは、スマートグリッドの構成要素の特徴からのトップダウンの分析と、スマートグリッドの脆弱性となり得る要素からのボトムアップ分析が行われる。⑤の適合性評価については、The SGIP Smart Grid Testing and Certification Committee (SGTCC)が、Interoperability Process Reference Manual (IPRM) Version 2.0 に推奨手順を纏めている。
評価項目	22 種類の論理インターフェース分類（LIC）ごとに、機密性・完全性・可用性への影響レベルが 3 段階（高・中・低）で評価されており、推奨されるセキュリティ要件がリスト化されている（19 ファミリー197 要

	件）。各セキュリティ要件については、NIST SP800-53 や NERC CIP 等の複数のガイドラインと対応付けがなされている。

表 3-11　NIST: NISTIR 7628 評価項目の概要

No.	セキュリティ対策項目
1	アクセス制御
2	セキュリティ意識向上トレーニング
3	監査及びその説明
4	セキュリティアセスメント及び認可
5	構成管理
6	緊急時対応計画
7	識別及び認証
8	情報・文書管理
9	インシデント対応
10	メンテナンス
11	メディアの保護
12	物理的保護及び環境保護
13	計画作成
14	セキュリティプログラム管理
15	職員によるセキュリティ
16	リスクアセスメント
17	システム及びサービスの調達
18	システム及び通信の保護
19	システムの完全性及び情報の整合性

(5) NIST: NISTIR 7823

NIST の策定した NISTIR 7823 は、スマートメーターのアップグレード機能に関する要件である NEMA SG-AMI 1-2009 への適合性を確認するためのフレームワークである。

表 3-12　NIST: NISTIR 7823 調査・整理結果

名称	**Advanced Metering Infrastructure Smart Meter Upgradeability Test Framework (NISTIR 7823)**
発行機関	NIST (National Institute of Standards and Technology)
概要	NISTIR 7823 は、スマートメーターのアップグレード機能に関する要件である NEMA SG-AMI 1-2009 への適合性を確認するためのフレームワークである。米国では、マッチングファンド制度により 2009 年から 2010 年の間に大量のスマートメーターが設置されたが、現在は異なる会社の異なる技術レベルのスマートメーターが混在している。新しいスマートメーターの設置が進められる中、適宜適切なアップグレードが求められている。

評価スキーム	認証機関またはその役割を持つ組織が、A&A（評価および承認）や認証スキームに従って本のフレームワークを使用する場合には、その責任において検証手続きの採用・更新・調整を行い、どのようなテストを実行するかを決定する。
評価項目	スマートメーターの機能に対する要求事項（Functional Requirements）とそれらを検証する手法に対する要求事項（Assurance Requirements）が記述されている。機能に対する要求事項は 25 項目あり、必須項目、条件付きで必須の項目、推奨項目の 3 つに分類されている。検証手法に対する要求事項には、ベンダーへの要求事項と手順に対する要求事項がある。

表 3-13　NIST: NISTIR 7823 評価項目の概要

No.	セキュリティ対策項目
1	ファームウェアバージョンの特定
2	ファームウェアのリカバリー
3	ファームウェアの完全性の検証
4	ファームウェアの整合性の検証
5	アップグレード時のログ出力
6	計量再校正の不必要性
7	構成の継続
8	計測の継続
9	ファームウェアアップグレードの起動
10	ファームウェアアップグレードの権限
11	ファームウェアの認証
12	暗号化アルゴリズム
13	暗号化強度
14	AMI システムのレジリエンス
15	コマンドメッセージの認証と整合性
16	ファームウェアのアップグレードおよび通信切断時のセキュリティ保護
17	運用・プライバシー要件サポート
18	偽造防止
19	ホームエリアネットワークからの多層防御
20	侵入検知
21	認証・暗号化通信失敗時のログ出力
22	アップグレードマネジメントシステムによるファームウェアアップグレードの起動
23	アップグレードマネジメントシステムによるファームウェアのリカバリー
24	アップグレードマネジメントシステムのセキュリティ要件
25	アップグレードマネジメントシステムによるプグレード時のログ出力

(6) ENISA: Baseline Security Recommendations for IoT

ENISA の策定した Baseline Security Recommendations for IoT は、主に重要インフラ向け IoT システムに必要とされるベースラインセキュリティを提言している。

表 3-14　ENISA: Baseline Security Recommendations for IoT
調査・整理結果

名称	**Baseline Security Recommendations for IoT**
発行機関	ENISA (European Union Agency for Cybersecurity)
概要	Baseline Security Recommendations for IoT は、2017 年に ENISA によって作成されたガイドであり、主に重要インフラ向け IoT システムに必要とされるベースラインセキュリティを提言することを目的としている。机上調査や、IoT システムに関わる者及び専門家へのヒアリング結果を反映し、IoT に対する脅威や攻撃シナリオ、推奨セキュリティ対策／グッドプラクティス、現状とあるべき状態のギャップ分析手法、セキュリティ改善のための提言等が纏められている。 本ガイドラインを元に 2018 年に作成された「Good Practices for Security of Internet of Things in the context of Smart Manufacturing」では、IIoT（Industrial IoT）とスマートマニュファクチャリングに関するグッドプラクティスが紹介されている。
評価スキーム	推奨対策基準等を記述したガイドであり、評価スキームに関しては言及されていない。
評価項目	既存の IoT に関するセキュリティガイドラインや基準を参考に、IoT のセキュリティ対策／グッドプラクティスを、3 分類、24 項目、83 要件に纏めている（ポリシー：4 項目 12 要件、技術的対策：15 項目 57 件、組織的・人的・運用的対策：5 項目 14 要件）。

表 3-15　ENISA: Baseline Security Recommendations for IoT
評価項目の概要

No.	セキュリティ対策項目
1	セキュリティ・バイ・デザイン
2	プライバシー・バイ・デザイン
3	情報資産管理
4	リスクと脅威の特定・評価
5	ハードウェアのセキュリティ
6	トラストと完全性の管理
7	初期設定のセキュリティ・プライバシー強化
8	データの保護とコンプライアンス
9	システムの安全性と信頼性
10	ソフトウェア・ファームウェアのセキュリティアップデート
11	認証

No.	セキュリティ対策項目
12	認可
13	アクセス制御（物理・環境）
14	暗号化
15	コミュニケーションのセキュリティ・トラスト
16	インターフェース・ネットワークのセキュリティ
17	入出力の制御
18	ログの出力
19	監視と監査
20	サポートの終了
21	実績のあるソリューション
22	脆弱性とインシデントの管理
23	人的セキュリティと教育・訓練
24	サードパーティとの関係性

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

2020 年 3 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