小出力風力発電設備に係る

サイバーセキュリティ対策ガイドライン

令和５年７月

（一社）日本小形風力発電協会

目次

1 はじめに

1.1 本実装例策定の背景・目的

あらゆる分野でデジタル化が進展する一方、多様化・巧妙化するサイバー攻撃の脅威は日々高まっており、重要インフラたる電力分野においても、サイバーセキュリティ向上に向けた不断の取組が求められている。電源の分散化やオンライン化の拡大する現状においては、電気事業者に対するサイバーリスクだけでなく、電力事業の用に供しない小規模発電設備等に対するサイバーリスクも高まりつつある。

小規模発電設備等におけるサイバーリスクの高まりをうけ、経済産業省の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（電力 SWG）や電力・ガス基本政策小委員会において、電力事業の用に供しない小規模発電設備等を系統に接続する際にすべからく求められるサイバーセキュリティ対策について議論が行われてきた。これまでの議論を通じて、以下の 3 つのセキュリティ対策の必要性が提示された。

(1) サイバーインシデントの発生を防ぐ事前防御の観点として、

対策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。

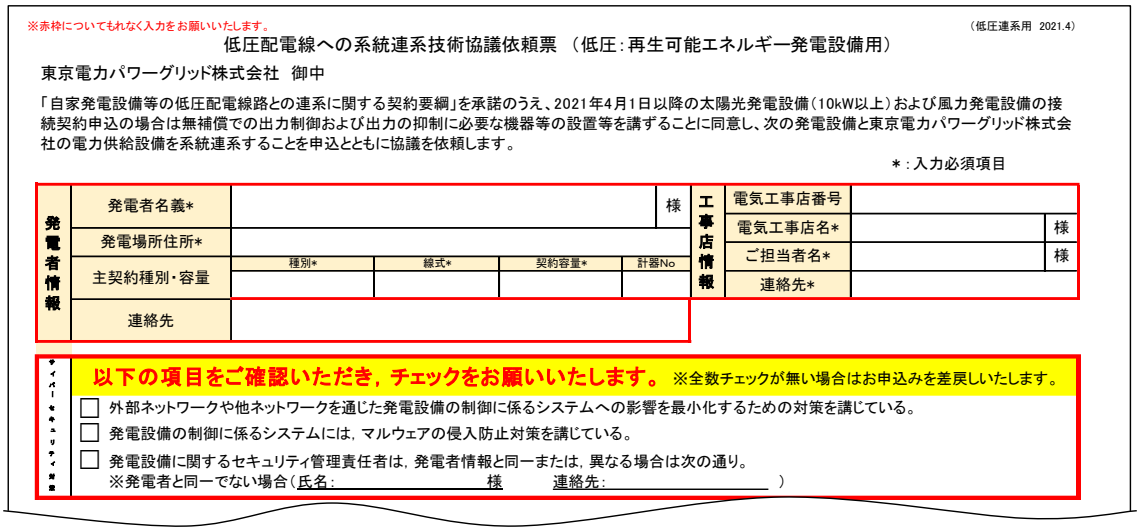
対策② データの保存・転送を行う機器・端末等のマルウェア対策：

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。

(2) インシデント発生時の影響を最小化する事後対応（早期発見、迅速な対処）の観点として、

対策③ 連系先系統運用者に対するセキュリティ管理責任者の氏名及び緊急時連絡先の通知

これらの対策の必要性を踏まえ、2020 年 10 月より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）において 3 つの要件が規定され、当該要件は 2020 年 10 月以降に契約申込みを行うもの（電源接続案件募集プロセス対象の設備にあっては、2020 年 10 月以降に入札を実施するもの）を対象に実施を求めることとされた。現在、一般送配電事業者に対する系統連系の申請に際しては、これらの対策①～対策③を実施していることを確認した上で申請することが必要となっている。（図 1-1）



※赤枠についてもれなく入力をお願いいたします。　（低圧連系用　2021.4）

低圧配電線への系統連系技術協議依頼票　（低圧：再生可能エネルギー発電設備用）

東京電力パワーグリッド株式会社　御中

「自家発電設備等の低圧配電線路との連系に関する契約要綱」を承諾のうえ、2021年4月1日以降の太陽光発電設備（10kW以上）および風力発電設備の接続契約申込の場合は無補償での出力制御および出力の抑制に必要な機器等の設置等を講ずることに同意し、次の発電設備と東京電力パワーグリッド株式会社の電力供給設備を系統連系することを申込とともに協議を依頼します。

＊：入力必須項目

発電者情報

発電者名義＊					様
発電場所住所＊					
主契約種別・容量	種別＊	線式＊	契約容量＊	計器No	
連絡先					

工事店情報

電気工事店番号		
電気工事店名＊		様
ご担当者名＊		様
連絡先＊		

サイバーセキュリティ対策

以下の項目をご確認いただき，チェックをお願いいたします。　※全数チェックが無い場合はお申込みを差戻しいたします。

☐ 外部ネットワークや他ネットワークを通じた発電設備の制御に係るシステムへの影響を最小化するための対策を講じている。

☐ 発電設備の制御に係るシステムには，マルウェアの侵入防止対策を講じている。

☐ 発電設備に関するセキュリティ管理責任者は，発電者情報と同一または，異なる場合は次の通り。
※発電者と同一でない場合（氏名：　　様　　連絡先：　　）

図 1-1 系統連系申請書におけるサイバーセキュリティ対策項目記入欄の例

（東京電力パワーグリッド株式会社、低圧再生可能エネルギー発電設備用の場合[1]）

系統連系技術要件にサイバーセキュリティ対策の要件が規定されることを受け、経済産業省は、小規模発電設備等を系統に接続する者や小規模発電設備等のメーカーに対して実態調査を行い、セキュリティ対策の実態を確認するとともに、具体的な対策の実行可能性や事業者が抱えている課題等を抽出した。調査の結果、主に以下の 3 点が確認された。

- 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る。
- 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、系統連系技術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小規模発電設備等のメーカーは懸念を持っている。
- 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。

さらに、系統連系技術要件におけるサイバーセキュリティに関する要件に関して、補足説明や設備種別ごとに対策実装例等を求める意見が多数挙げられた。

この背景に基づき、小規模発電設備等のセキュリティ対策に関する検討会を設置し、様々な設備種別における系統連系技術要件の対策実装例を議論した。この検討会では、系統連系技術要件の主な対象である小規模発電設備等のうち、一般用電気工作物に分類される小出力発電設備に対して求められるセキュリティ対策に関して議論した。我が国における導入状況やこれまでの議論を踏まえ、太陽光発電設備、風力発電設備、コージェネレーションシステム、家庭用電気設備（エネファーム、蓄電池等）の 4 つの種別を、代表的な小出力発電設備と捉え、各設備種別の典型的なシステム構成に基づ

[1] 東京電力パワーグリッド，系統連系協議依頼票 https://www.tepco.co.jp/pg/consignment/fit/workshop.html

き対策実装例を検討した。

本文書は、小出力風力発電設備に係る検討会での議論を踏まえ、小出力風力発電設備に関して系統連系技術要件のサイバーセキュリティ対策を実装するための実装例を整理したものである。系統連系技術要件では、発電設備を設置し運用する者に対してサイバーセキュリティ対策を求めており、本文書においても、設備設置者に求められるセキュリティ対策を中心に、具体的な対策実装例を示す。なお、系統連系技術要件では、2020 年 10 月以降に契約申込みを行う設備を対象に対策①～③の実施が求められるが、本文書では、この期間に連系された設備に範囲を限定せず、すべての小出力発電設備に対して実装が求められる対策実装例を記載する。また、小出力風力発電設備のセキュリティ対策においては、設備を設置し運用する者だけでなく、小出力風力発電設備の設置工事を請け負う施工業者や、関連設備を開発・製造する機器メーカーにおける実装も重要となる。そのため、本文書では設備設置者、施工業者、関連設備を開発・製造する機器メーカー等の小出力風力発電設備に関連するステークホルダーごとに、小出力風力発電設備等に実装する対策の例を整理している。なお、本文書で記載する対策実装例は、系統連系技術要件で求められる対策を実装するための例示的位置づけであり、各ステークホルダーは自組織の対策範囲についてリスクを評価した上で適切な実装例を選択することが求められる。また、本文書で記載の対策実装例以外にも、系統連系技術要件で求められる対策へ対応するための実装方法は存在することに留意する必要がある。

本文書で記載している対策実装例や、対策の不備により想定されるサイバーセキュリティリスク、及びそのリスク源等に関する記載は以下の資料を参考としている。

- 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 PCS の技術仕様について[2]
- 経済産業省：サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）[3]
- 情報処理推進機構（IPA）：IoT 開発におけるセキュリティ設計の手引き[4]

より汎用的なサイバーセキュリティ対策に関する事項や、特にこれからサイバーセキュリティ対策に取り組む者に推奨される実施事項については、以下の資料も参照されたい。

- IPA：中小企業の情報セキュリティ対策ガイドライン[5]

1.2 本実装例の対象設備

本文書の主に対象とする小出力風力発電設備は、一般用電気工作物に分類される出力 20kW 未満の系統連系する風力発電設備（小形風力設備）である（図 1-2）。

本文書の主な対象ではないものの、事業用電気工作物に関しては、電気事業法に基づく電気設備に関する技術基準を定める省令に基づきサイバーセキュリティの確保が規定されており、その技術基準の

[2] https://www.jema-net.or.jp/Japanese/res/dispersed/050.html#052
[3] https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html
[4] https://www.ipa.go.jp/security/iot/iotguide.html
[5] https://www.ipa.go.jp/security/keihatsu/sme/guideline/

解釈として、「電力制御システムセキュリティガイドライン」を参照していることに留意する必要がある。

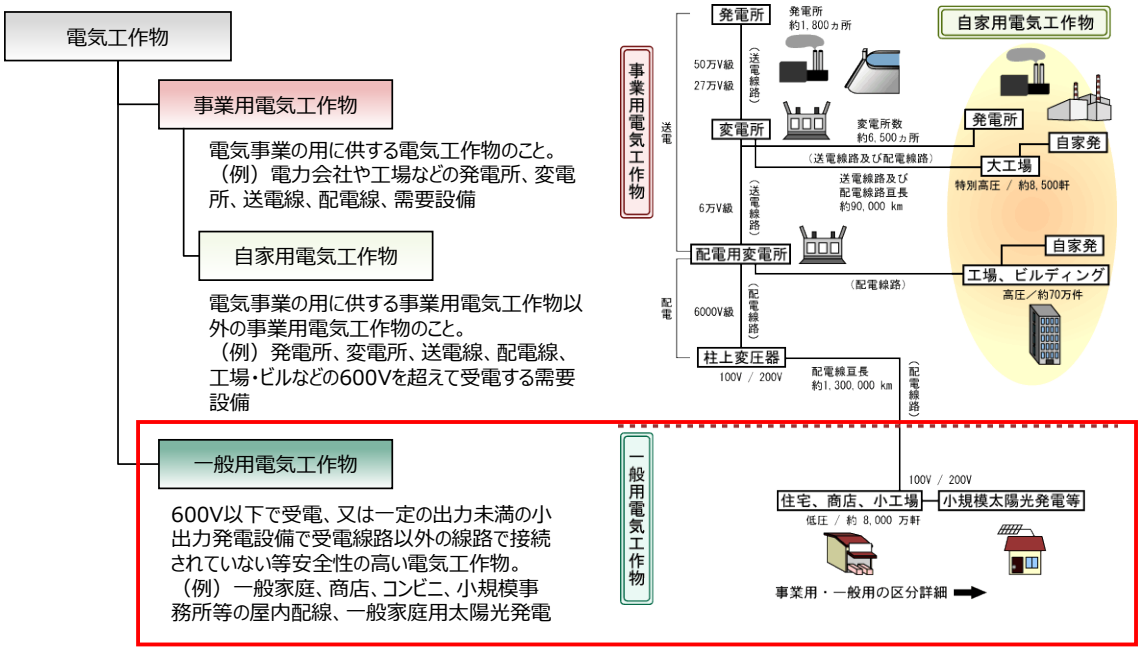


図 1-2 電気工作物の区分と本実装例の対象[6]

1.3 本実装例の対象者と活用方法

本実装例の対象者（ステークホルダー）は以下のとおりである。

- 小出力風力発電設備の設置者：
  系統連系する小出力風力発電設備を所有・設置する者。特に、組織におけるセキュリティ管理責任者を対象としている。
- 小出力風力発電設備の設置工事を請け負う施工業者：
  小出力風力発電設備の設置工事を担う事業者。
- 小出力風力発電設備等のメーカー：
  風車メーカーのほか、小出力風力発電設備に使用される PCS（パワーコンディショナー）、出力制御ユニット、通信装置等のメーカー。
- 監視サービスプロバイダー等：
  小出力風力発電設備の発電状況を監視するサービスのプロバイダー及び当該監視に必要な計測通信装装置のメーカー。

[6] 経済産業省，電気工作物の保安 に基づき作成
https://www.meti.go.jp/policy/safety_security/industrial_safety/sangyo/electric/detail/setsubi_hoan.html

系統連系にあたっては、原則的に設備設置者が系統連系申請書に記入を行い、一般送配電事業者に対して連系の申請を行う必要がある。しかしながら、電気設備の設置工事を請け負う施工業者が、申請書への記入や申請を委託されるケースも存在する。そのため、本実装例では、設備設置者だけでなく、設備工事を請け負う施工業者も対象としている。また、小出力風力発電設備等の保守・点検にあたっては、設置者が外部のオペレーション＆メンテナンス（O&M）事業者に保守・点検を依頼するケースも想定される。そのため、O&M 事業者においても、本実装例の内容を参照することが望まれる。以降ではこれらのステークホルダーごとに、小出力風力発電設備等に実装する対策の例を整理している。

2 小出力風力発電設備のサイバーセキュリティ対策における特徴

2.1 小出力発電設備を取り巻く環境

世界的に環境やエネルギーに対する取組が加速する中で、再生可能エネルギーの導入促進は必要不可欠である。国内においても、「第 5 次エネルギー基本計画」において、再生可能エネルギーを我が国の主力電源とすることが明記されたほか、2020 年 10 月には「2050 年カーボンニュートラル宣言」がなされ、電化の促進、電源の脱炭素化が鍵となる中で、再生可能エネルギーの最大限の導入を図っていくことが再度強調された。国内では、これまで FIT 制度による支援や系統整備等の取組を通じて、再生可能エネルギーの導入量は、電源比率で 2012 年の 9%から 2018 年の 17%にまで拡大したほか、省エネ意識の高まりや補助金による支援制度を受け、一般住宅においてもエネルギー関連設備の導入が加速している。例えば、2009 年に販売を開始した家庭用燃料電池（エネファーム）は 2021 年 6 月には累計 40 万台の導入を突破した[7]ほか、家庭用蓄電池は年間 4 万台の導入ポテンシャルを有すると推定[8]されている。また、再生可能エネルギー出力制御のオンライン化や VPP ビジネスの拡大により、小出力発電設備等のオンライン化が急速に加速している。

2.2 小出力発電設備におけるサイバーセキュリティリスク

小出力発電設備のオンライン化が進展することでより柔軟な需給の調整が可能となった一方で、ネットワークを介したサイバー攻撃の起点も拡大しており、サイバーセキュリティ上の脅威も増大している。小出力発電設備に関連するサイバーセキュリティリスクの事例として、海外製インバーターにおける脆弱性の事例や、小形風力発電設備における脆弱性の事例、蓄電池関連設備における脆弱性の事例などが挙げられる。

(1) 太陽光発電用インバーターにおける脆弱性

2017 年 8 月、セキュリティ研究者によって、ドイツ SMA 社の太陽光発電用インバーターにおける 14 個の脆弱性が公開[9]され、CVE 番号が付番された。公開された脆弱性のうち、主要な 3 つの脆弱性の概要を図 2-1 に示す。脆弱性を発見したセキュリティ研究者は、脆弱性を悪用することで複数のインバーターの制御を妨害することができ、最悪の場合電力系統全体の停電につながる脅威シナリオを示した。なお、SMA 社は、この研究に対して安全基準の継続的改善に役立つと謝意を示した上で、インバーターの構造や技術的基準を考慮していない不完全な脆弱性解析であると反論し、同社のセキュリティ対策に関して記載したガイドライン[10]を公表している。

---

[7] コージェネ財団 燃料電池室, エネファームメーカー販売台数 https://www.ace.or.jp/fc/works_0010.html

[8] 日本電機工業会, JEMA 蓄電システムビジョン Ver.6 https://www.jema-net.or.jp/jema/data/S7216(20210527).pdf

[9] "Horus Scenario"という名称で公開された。"Horus"とは古代エジプトの神であり、一つの目は太陽を表し、もう一方は月を表すとされている。今回公表された脅威シナリオは、日食の際に太陽が隠れて太陽光発電が発電できない場合と同等の影響を電力網に与えるとしており、Horus を「再現可能」であることから、この名を冠したとしている。https://horusscenario.com/

[10] SMA, 技術情報サイバーセキュリティ 公式ガイドライン https://files.sma.de/downloads/CyberSecurity-TI-ja-10.pdf

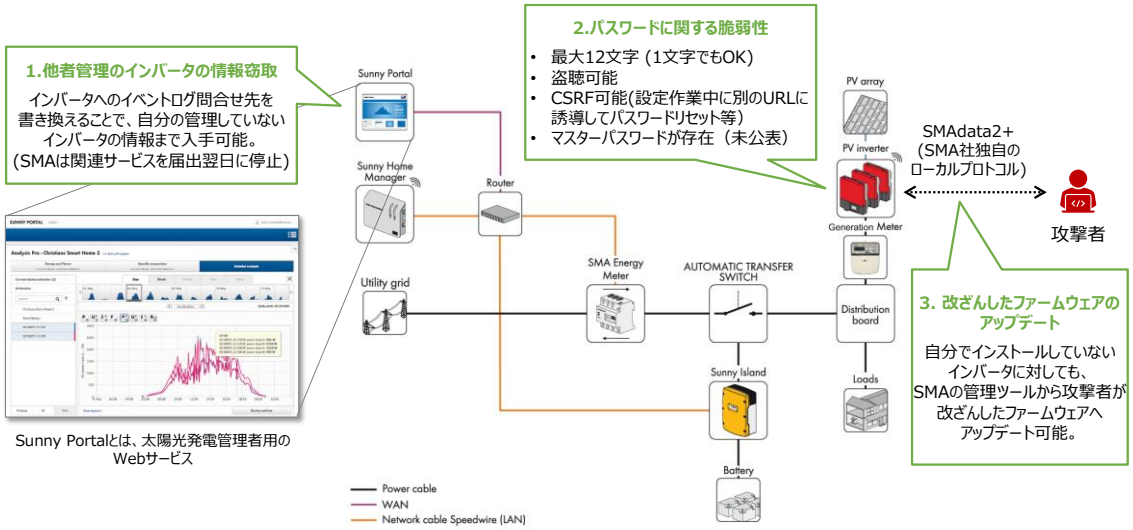


図 2-1 海外製インバーターにおける脆弱性の概要[11]

(2) 小形風力発電設備における脆弱性

2015 年から 2016 年にかけて、米国 XZERES 社の小形風力発電設備における複数の脆弱性が公開[12,13]され、CVE 番号が付番された。2015 年に公開された脆弱性はクロスサイトリクエストフォージェリ（CSRF）の脆弱性であり、この脆弱性が悪用された場合、風力発電設備の管理者機能に侵入され、パスワードの変更等が可能となることが示された。米国国土安全保障省の ICS-CERT は、脆弱性を悪用した攻撃を受けた場合、外部から風力発電設備が停止する危険性があることを指摘している[14]。XZERES 社はこの脆弱性に関してパッチを公開した。米国 ICS-CERT は、当該風力発電設備の設置者に対して、当該設備をインターネットから分離すること、制御系ネットワークと情報系ネットワークを分離すること、リモートアクセスが必要な場合には VPN 等の安全性の高い通信方法を利用すること等を推奨した。

---

[11] SMA 社インバーターに関する脆弱性情報に基づき、Wind & Sun 社資料に加筆。
http://www.windandsun.co.uk/information/solutions/on-grid-solar-pv-battery-storage-solutions/sma-flexible-storage-system-with-back-up.aspx

[12] JVN iPedia, JVNDB-2015-002017
https://jvndb.jvn.jp/ja/contents/2015/JVNDB-2015-002017.html

[13] JVN iPedia, JVNDB-2016-001814
https://jvndb.jvn.jp/ja/contents/2016/JVNDB-2016-001814.html

[14] ICS-CERT, ICS Advisory (ICSA-15-076-01) XZERES 442SR Wind Turbine Vulnerability
https://us-cert.cisa.gov/ics/advisories/ICSA-15-076-01

(3) 蓄電池関連設備における脆弱性の事例

2017 年、フランス Schneider Electric Global 社が販売する蓄電池監視装置のファームウェアにおける脆弱性が公開された[15]。米国国土安全保障省の ICS-CERT は、脆弱性を悪用した攻撃を受けた場合、本機器の再起動が実行され、サービスが停止する危険性があることを指摘している[16]。ICS-CERT は、機器のユーザーに向けて、ネットワーク接続点を最小化すること、ファイアウォールを設置すること、リモート接続の際に VPN 等の安全性の高い通信方式を利用することの 3 つの対策を実施することを推奨した。同年、Schneider Electric Global 社より脆弱性を修正したファームウェアが公開された。

2.2.1 小出力風力発電設備等におけるサイバーセキュリティリスクの例

小出力風力発電設備等に関するサイバーセキュリティリスクに関する国内での検討として、出力制御機能付 PCS の技術仕様に係る検討が挙げられる。当該技術仕様では、電力安定供給を目的として出力制御機能付 PCS 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。上記のリスク事例や国内での検討を踏まえると、小出力風力発電設備等に関するサイバーセキュリティリスクとして、例えば以下のようなリスクが想定される。

- 外部ネットワークから小出力風力発電設備等に不正アクセスがなされ、小出力風力発電設備等の動作が停止する
- 外部ネットワークから小出力風力発電設備等に不正アクセスがなされ、小出力風力発電設備等を踏み台として他のシステムに不正アクセスされる
- 小出力風力発電設備等のファームウェアが改ざんされ、マルウェア感染や悪意あるコードの実行、小出力風力発電設備等の動作停止につながる
- 小出力風力発電設備等がマルウェアに感染し、小出力風力発電設備等の動作停止や、システムへの感染拡大につながる
- 小出力風力発電設備等に接続する接続端末や監視端末がマルウェアに感染し、それが小出力風力発電設備等に接続されることで、小出力風力発電設備等もマルウェアに感染する
- セキュリティインシデントが発生した際に、連系先等の他組織に悪影響を与える

これらのサイバーセキュリティリスクが顕在化した場合、小出力風力発電設備等の動作が停止し、系統への電力供給が停止する恐れがある。複数の小出力風力発電設備等による電力供給が停止した場合、系統の安定性に影響を与え、需給のバランスに乱れが生じる可能性がある。また、小出力風力発電設備等を保護する安全装置が作用しなかった場合、小出力風力発電設備等が故障する恐れもあるほか、最悪の場合には発火や火災の発生、それによる作業員の人命に関わる致命的な影響が発生す

[15] JVN iPedia, JVNDB-2017-003054
https://jvndb.jvn.jp/ja/contents/2017/JVNDB-2017-003054.html
[16] ICS-CERT, ICS Advisory (ICSA-17-061-02) Schneider Electric Conext ComBox
https://us-cert.cisa.gov/ics/advisories/ICSA-17-061-02

る可能性もある。加えて、小出力風力発電設備等が踏み台とされた場合、他システムがサイバー攻撃を受けるおそれもある。

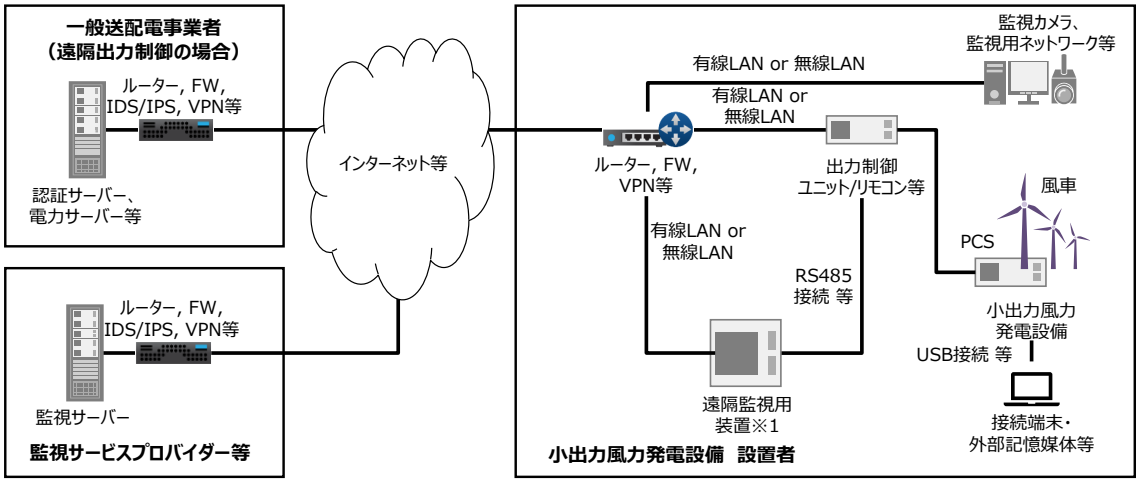
多くのサイバーセキュリティリスクは、設備種別に大きく依存せず存在するものである。しかしながら、それぞれの設備種別においてシステムやネットワークの構成及び運用状況は大きく異なるため、リスクが顕在化した場合の影響の度合いや求められる対策は異なる。本文書で対象とする小出力風力発電設備等の特徴として、再生可能エネルギーの導入促進や出力制御の状況を踏まえ、オンライン接続する発電設備が増加していることが挙げられる。仮に複数の小出力風力発電設備等が一斉にサイバー攻撃を受けた場合、系統の安定性に影響を与えかねない。小出力風力発電設備等の対策にあたっては、設備設置者による対策のほか、オンライン出力制御を司る PCS や関連通信機器におけるセキュリティ対策も重要となる。検討会では、小出力風力発電設備等の典型的なシステム構成に基づき、システム構成やセキュリティ対策の実態を踏まえ、対策実装例を検討した。

2.3 小出力風力発電設備等の代表的なシステム構成

本文書で対象とする小出力風力発電設備等の代表的なシステム構成を図 2-2 に示す。

近年の小出力風力発電設備等の多くは、出力制御の拡大に伴い、小出力風力発電設備の発電出力を制御する広義 PCS を介して、インターネットに接続される。広義 PCS は、出力制御ユニットと狭義 PCS から構成されるが、これらの機器が一体化したシステムも存在する。これらの機器の設定やソフトウェア・ファームウェアの更新にあたって、PC 等の接続端末の接続や USB 端末等の外部記憶装置の接続が必要となる場合がある。

設備設置者が遠隔から風力発電出力を確認するために、遠隔監視サービスに加入しているケースも存在する。この場合、遠隔監視用の計測装置を導入する必要があるが、近年では遠隔監視と出力制御の両方に一台で対応した広義 PCS も販売されている。また、小出力風力発電設備等の制御にかかるシステムではないものの、設備設置場所を監視するための監視カメラを設置し、インターネットに接続するケースも存在する。



※1 本文書では、PCSに対して別途接続される遠隔監視用装置を対象とするが、遠隔監視と出力制御の両方がPCSも販売されている。

図 2-2 小出力風力発電の代表的なシステム構成

図 2-2 のうち、設置者内の小出力風力発電設備等に関して、各ステークホルダーが対策できる範囲は図 2-3 のようにマッピングされる。小出力風力発電設備等のメーカーや監視サービスプロバイダー等は、自身が開発する機器に対してセキュリティ対策を施す必要があるが、設備設置時のセキュリティ対策は、設置者及び設置者により依頼された施工業者によって実施する必要がある。さらに、小出力風力発電設備等を運用する段階では、設置者自身によって、セキュリティ対策を継続的に実施する必要がある。

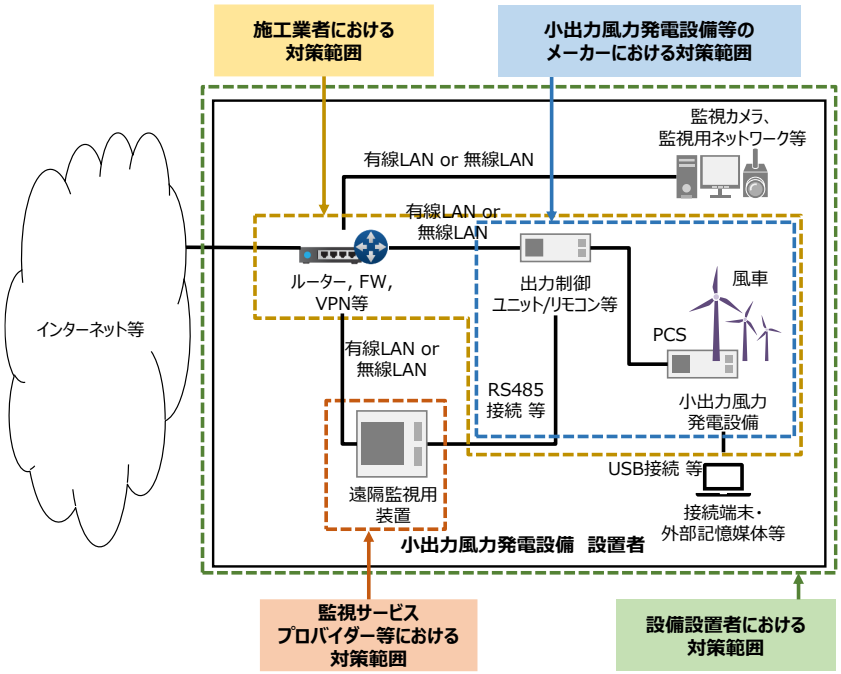


図 2-3 各ステークホルダーにおけるセキュリティ対策範囲

3 小出力風力発電設備に係るサイバーセキュリティ対策の実装例

3.1 小出力風力発電設備等に求められるサイバーセキュリティ対策

上記のとおり、系統連系する小出力風力発電設備においては、

(1) サイバーインシデントの発生を防ぐ事前防御の観点として、

対策① ネットワーク接続点の保護

対策② データの保存・転送を行う機器・端末等のマルウェア対策

(2) インシデント発生時の影響を最小化する事後対応（早期発見、迅速な対処）の観点として、

対策③ 連系先系統運用者に対するセキュリティ管理責任者の氏名及び緊急時連絡先の通知

の 3 つの対策が求められる。

対策①が実装されていないことにより想定されるサイバーセキュリティリスク、及び対応するリスク源（脅威及び脆弱性）は表 3-1 のように整理される。対策①が実装されていないことにより、外部ネットワークからの小出力風力発電設備等への不正アクセスが発生する恐れがあり、この結果、小出力風力発電設備等の動作が停止する可能性がある。このようなリスクにつながることを防ぐために、適切な防護装置を用いて、外部ネットワークとの接続点を適切に保護する必要がある。

表 3-1 対策①の不備により想定されるサイバーセキュリティリスク及びそのリスク源

対策①の不備により想定されるサイバーセキュリティリスク	リスク源	
	主な脅威	主な脆弱性
外部ネットワークから小出力風力発電設備等に不正アクセスがなされ、小出力風力発電設備等の動作が停止する	• セキュリティが実装されていない脆弱なプロトコルを悪用した不正アクセス • 不正な組織/システムによる正規エンティティへのなりすまし • 窃取した ID 等を利用した正規ホストへのなりすまし	• 利用している小出力風力発電設備等が十分なセキュリティ機能を実装していない • ネットワークの適正利用を確認していない • 通信路が適切に保護されていない • システムにおいて対処すべき脆弱性が適切に対処されていない
外部ネットワークから小出力風力発電設備等に不正アクセスがなされ、小出力風力発電設備等を踏み台として他のシステムに不正アクセスされる	• セキュリティが実装されていない脆弱なプロトコルを悪用した不正アクセス • 不正な組織/システムによる正規エンティティへのなりすまし • 窃取した ID 等を利用した正規ホストへのなりすまし • マルウェアによる制御信号の改ざん	• 利用している小出力風力発電設備等が十分なセキュリティ機能を実装していない • ネットワークの適正利用を確認していない • システムにおいて対処すべき脆弱性が適切に対処されていない

対策②が実装されていないことにより想定されるサイバーセキュリティリスク、及び対応するリスク源（脅威及び脆弱性）は表 3-2 のように整理される。対策②が実装されていないことにより、小出力風力発電設備等がマルウェアに感染する恐れがあり、その結果、小出力風力発電設備等の動作が停止する可能性がある。このようなリスクにつながることを防ぐために、小出力風力発電設備等に関するマルウェア対策を実装する必要があるほか、利用している小出力風力発電設備等においては、適切なセキュリティ機能を実装する必要がある。

表 3-2 対策②の不備により想定されるサイバーセキュリティリスク及びそのリスク源

対策②の不備により想定されるサイバーセキュリティリスク	リスク源	
	主な脅威	主な脆弱性
小出力風力発電設備等のファームウェアが改ざんされ、マルウェア感染や悪意あるコードの実行、小出力風力発電設備等の動作停止につながる	• 小出力風力発電設備等におけるセキュリティ上の脆弱性を利用したマルウェア感染 • マルウェアによる制御信号の改ざん	• 利用している小出力風力発電設備等が十分なセキュリティ機能を実装していない
小出力風力発電設備等がマルウェアに感染し、小出力風力発電設備等の動作停止や、システムへの感染拡大につながる	• 小出力風力発電設備等におけるセキュリティ上の脆弱性を利用したマルウェア感染	• 利用している小出力風力発電設備等が十分なセキュリティ機能を実装していない
小出力風力発電設備等に接続する接続端末や監視端末がマルウェアに感染し、それが小出力風力発電設備等に接続されることで、小出力風力発電設備等もマルウェアに感染する	• 小出力風力発電設備等におけるセキュリティ上の脆弱性を利用したマルウェア感染 • システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 • 小出力風力発電設備等を管理するシステムから小出力風力発電設備等への不正なコマンド送信	• 利用している小出力風力発電設備等が十分なセキュリティ機能を実装していない • ネットワークの適正利用を確認していない • システムにおいて対処すべき脆弱性が適切に対処されていない

最後に、対策③が実装されていないことにより想定されるサイバーセキュリティリスク、及び対応するリスク源（脅威及び脆弱性）は表 3-3 のように整理される。対策③が実装されていないことにより、不正アクセスやマルウェア感染等のセキュリティインシデントが発生した際に、自組織だけでなく連系先等の他組織にも悪影響を及ぼす恐れがある。このようなリスクにつながることを防ぐために、セキュリティインシデントに的確に対応するための管理責任者を明確にする必要があるほか、インシデントが発生した際の対応を明確にする必要がある。

表 3-3 対策③の不備により想定されるサイバーセキュリティリスク及びそのリスク源

対策③の不備により想定されるサイバーセキュリティリスク	リスク源	
	主な脅威	主な脆弱性
セキュリティインシデントが発生した際に、連系先等の他組織に悪影響を与える	• セキュリティが実装されていない脆弱なプロトコルを悪用した不正アクセス • システムにおけるセキュリティ上の脆弱性を利用したマルウェア感染 などのセキュリティインシデントに関するすべての脅威	• セキュリティインシデントに的確に対応するための体制が構築されていない • 風力発電設備等の停止を検知した後の対応手順が定義されていない • 他組織が自組織のセキュリティ事象発生時に適切なアクションを取ることができない

以降では、小出力風力発電設備等に関係するステークホルダーごとに、対策①～対策③を具体的に実装する方法例を示す。

3.2 小出力風力発電設備設置者におけるサイバーセキュリティ対策の実装例

3.2.1 対策①に関する対策実装例

小出力風力発電設備設置者は、「対策① ：ネットワーク接続点の保護」を実施するにあたって、以下に示す対策実装例が考えられる。

(1) 小出力風力発電設備等に係る通信のうち、インターネットを介した通信については、防護装置（ルーター、ファイアウォール、VPN 等）を必ず経由させる。
(2) 防護装置（ルーター、ファイアウォール、VPN 等）に対して、遮断する通信（小出力風力発電設備等の運転において不要な通信、事前に設定していない通信 等）に関する設定を行う。
(3) 不正アクセス等のセキュリティ事象を適切に検知できるよう、インターネットを介した通信に関してネットワーク監視や通信のモニタリングを実施する。
(4) 小出力風力発電設備等の制御に係るシステムにおいて、システムのネットワークを、情報システムのネットワークから論理的あるいは物理的にセグメントを分離する。
(5) 小出力風力発電設備等の制御に係るシステムと他ネットワークとの接続点を最小化する。
(6) 小出力風力発電設備等の運転設定に関する管理画面に対してアクセスする際の認証情報（パスワード等）を、適切に管理する。

それぞれの項目における対策箇所のイメージを図 3-1 に示す。以下に、各項目を解説する。

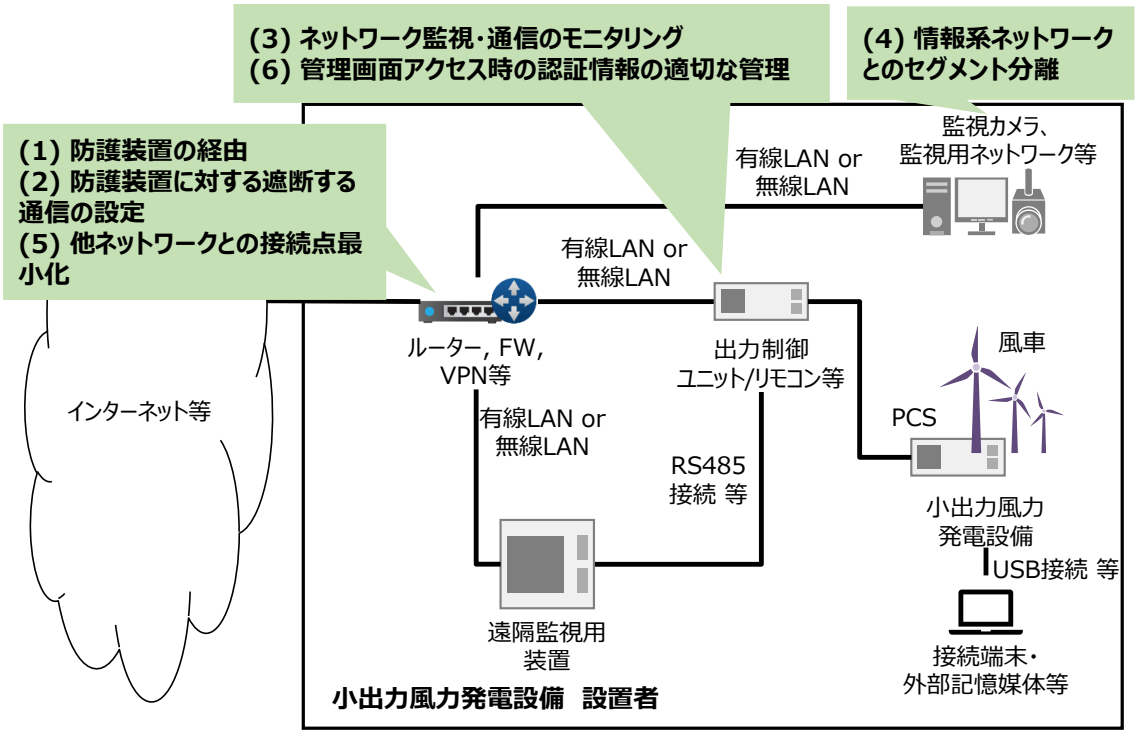


図 3-1 小出力風力発電設備 設置者における対策①に関する対策実装例

(1) 小出力風力発電設備等に係る通信のうち、インターネットを介した通信については、防護装置（ルーター、ファイアウォール、VPN 等）を必ず経由させる。

小出力風力発電設備設置者は、外部ネットワークからの不正アクセスにより小出力風力発電設備等の動作が停止するサイバーセキュリティリスクを防ぐために、ルーター、ファイアウォール、VPN等の防護装置をネットワーク接続点に設置し、必要な通信のみを通す設定とすることが求められる。必要な通信のみを通す設定とするために、次項に示す通信制御ポリシーを定める必要がある。この対策を実装していなかった場合、外部ネットワークから小出力風力発電設備等に不正アクセスがなされ、小出力風力発電設備等の動作停止につながる可能性がある。小出力風力発電設備等の動作が停止した結果、系統への電力供給が停止するほか、系統の安定性に影響を与え、需給のバランスに乱れが生じる恐れもある。加えて、小出力風力発電設備等に関する情報漏えいにつながる可能性があるほか、小出力風力発電設備等を踏み台として、接続先の電力サーバー等の他のシステムに対して不正アクセスが実行される危険性もある。

(2) 防護装置（ルーター、ファイアウォール、VPN 等）に対して、遮断する通信（小出力風力発電設備等の運転において不要な通信、事前に設定していない通信 等）に関する設定を行う。

小出力風力発電設備設置者は、防護装置に対して通信制御ポリシーを定めアクセス制御を行うことで、必要な通信のみを通し、不要な通信はすべて遮断する設定とすることが求められる。

このために、出力制御用の一般送配電事業者の電力サーバーとの接続等、許可する通信の内容や通信先を洗い出し、その情報を元に通信制御ポリシーを設定することが必要である。この対策を実装していなかった場合、外部ネットワークから小出力風力発電設備等に不正アクセスがなされ、小出力風力発電設備等の動作停止につながる可能性がある。小出力風力発電設備等の動作が停止した結果、系統への電力供給が停止するほか、系統の安定性に影響を与え、需給のバランスに乱れが生じる恐れもある。加えて、小出力風力発電設備等に関する情報漏えいにつながる可能性があるほか、小出力風力発電設備等を踏み台として、接続先の電力サーバー等の他のシステムに対して不正アクセスが実行される危険性もある。

(3) 不正アクセス等のセキュリティ事象を適切に検知できるよう、インターネットを介した通信に関してネットワーク監視や通信のモニタリングを実施する。

小出力風力発電設備設置者は、不正アクセス等のセキュリティ事象を適切に検知できるように、外部ネットワークとの通信に関してネットワーク監視や通信のモニタリングを実施することが求められる。ネットワーク監視においては、外部ネットワークとの通信に必要な防護装置の動作状態を監視し、当該装置が正常に動作しているかを把握することが求められる。防護装置において動作状況を監視し異常が発生した場合に通知する機能を有している場合があるほか、ツールを活用したネットワーク監視方法も想定される。また、外部ネットワークの通信をモニタリングし、特定の送信元や多数の送信元から不正な通信や大量の通信が無いかを把握し、必要に応じて特定 IP アドレスからの通信や特定サービスの通信を遮断するなどの対応を実施することが求められる。この対策を実装していなかった場合、外部ネットワークから小出力風力発電設備等に対する不正アクセスを把握できず、セキュリティ事象に対する対応が遅延し、小出力風力発電設備等の動作停止を招く恐れがある。

(4) 小出力風力発電設備等の制御に係るシステムにおいて、システムのネットワークを、情報システムのネットワークから論理的あるいは物理的にセグメントを分離する。

小出力風力発電設備設置者は、小出力風力発電設備等の制御に係るシステムのネットワークと情報システムのネットワークを論理的あるいは物理的に分離することが求められる。想定される情報システムとして、組織の一般的な IT ネットワークや監視カメラに関するネットワークが挙げられる。物理的なネットワークの分離とは、小出力風力発電設備等の制御に係るシステムのネットワークを情報システムのネットワークと LAN で接続しない方法である。論理的なネットワークの分離とは、双方のネットワークを接続するものの、双方間で通信可能な内容を制限する方法であり、防護装置を用いたアクセス制御による方法や DMZ（Demilitarized Zone）などの緩衝地帯を設ける方法が挙げられる。アクセス制御を行うために、双方のネットワーク間で許可される通信の内容を洗い出し、それ以外の不要な通信はすべて遮断する設定とすることが求められる。この対策を実装していなかった場合、外部ネットワークから情報システムに対して不正アクセスがなされた場合に、その影響が小出力風力発電設備等の制御に係るシステムに対して伝播する可能性がある。

(5) 小出力風力発電設備等の制御に係るシステムと他ネットワークとの接続点を最小化する。

小出力風力発電設備設置者は、小出力風力発電設備等の制御に係るシステムのネットワークと他ネットワークとの接続点を最小化することが求められる。また、その接続点に対して防護装置を導入することで、適切な防護措置を講じることが求められる。この対策を実装していなかった場合、攻撃の対象となりうるポイントが増加し、攻撃によるリスクが高まる可能性があるほか、接続点の防御に関するコストが増大し、適切な対処が行われない可能性がある。

(6) 小出力風力発電設備等の運転設定に関する管理画面に対してアクセスする際の認証情報（パスワード等）を、適切に管理する。

小出力風力発電設備設置者は、小出力風力発電設備等の運転設定に関する管理画面にアクセスする際の認証情報（パスワード等）を適切に管理することが求められる。具体的な対策の方法として、小出力風力発電設備等を購入した際に、出荷段階で設定されているパスワードを推測困難なパスワードに変更することが望まれる。また、変更したパスワードは、第三者によって取得されないよう、組織内で適切に管理することが求められる。この対策を実装していなかった場合、外部ネットワークから小出力風力発電設備等の管理画面に対して不正アクセスがなされ、管理画面から運転設定が変更され、小出力風力発電設備等の動作停止につながる可能性がある。小出力風力発電設備等の動作が停止した結果、系統への電力供給が停止するほか、系統の安定性に影響を与え、需給のバランスに乱れが生じる恐れもある。加えて、小出力風力発電設備等に関する情報漏えいにつながる可能性がある。

3.2.2 対策②に関する対策実装例

小出力風力発電設備設置者は、「対策② ：データの保存・転送を行う機器・端末等のマルウェア対策」を実施するにあたって、以下に示す対策実装例が考えられる。

(1) 利用する小出力風力発電設備等や防護装置（ルーター、ファイアウォール、VPN 等）について、正規品を購入する。
(2) 小出力風力発電設備等に接続する端末（PC 等）に対して、マルウェアに対するパターンファイル型の検出・修復ソフトウェアを導入することで、攻撃コードの検知を実施する。
(3) 小出力風力発電設備等に接続する USB メモリ等の外部記憶媒体に対して、ウイルス対策ソフトによるチェック、ウイルスチェックが可能な USB メモリを用いる等の対策を行う。
(4) 屋外に設置する小出力風力発電設備等や防護装置（ルーター、ファイアウォール、VPN 等）において使用しない USB ポート、シリアルポートは栓をするなど物理的に閉塞する。
(5) 小出力風力発電設備等や防護装置（ルーター、ファイアウォール、VPN 等）に関する脆弱性、セキュリティパッチ、注意喚起等の情報を収集し、必要に応じた対応を行う。

それぞれの項目における対策箇所のイメージを図 3-2 に示す。以下に、各項目を解説する。

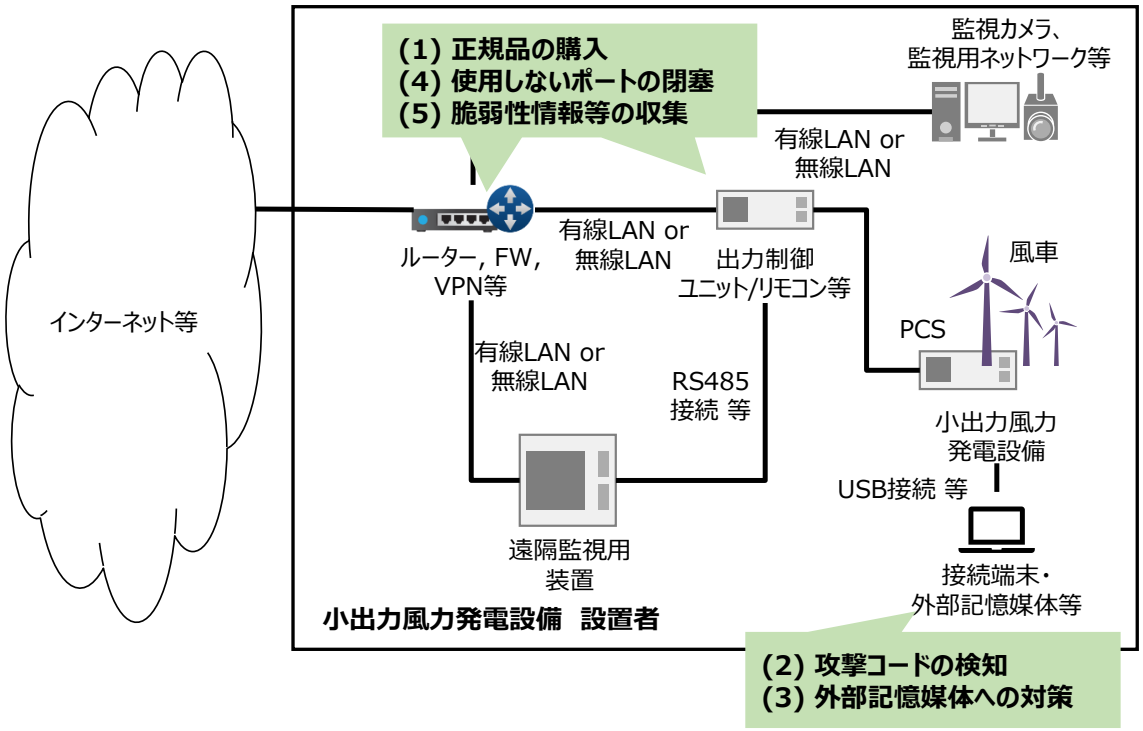


図 3-2 小出力風力発電設備設置者における対策②に関する対策実装例

(1) 利用する小出力風力発電設備等や防護装置（ルーター、ファイアウォール、VPN 等）について、正規品を購入する。

小出力風力発電設備設置者は、利用する小出力風力発電設備等や防護装置（ルーター、ファイアウォール、VPN 等）について正規品であることを確認した上で、組織内のシステムに導入することが求められる。関連事例として、ネットワークスイッチの偽造品が市場に流通した事例が存在する。この偽造スイッチは、正規品と比較してセキュリティ機能が意図的に弱体化されていたことが指摘されている。また、他産業分野においては、正規品と比較して品質が劣化した制御システム用の偽造センサが市場に流通した事例もあり、当該偽造品を用いることで制御システムの安全性に影響を及ぼしかねないことが指摘されている。正規品を購入するために、小出力風力発電設備等や防護装置のメーカーが認定している正式な販売会社から製品を調達するとともに、調達した製品が正規品であるかを製品ラベルに基づき確認することが求められる。小出力風力発電設備等に関しては、設置工事を行う施工業者とも連携し、正規品であることの確認を行うことが望ましい。この対策を実装していなかった場合、セキュリティが十分に考慮されていない偽造品がシステムに接続され、故障や悪意あるコードの実行など意図しない動作につながる可能性がある。

また、正規品の購入にあたっても、セキュリティが考慮されている小出力風力発電設備等や防護装置を選定することが望まれる。このような小出力風力発電設備等や装置の例として、業界団体に所属しているメーカーの製品、JET 認証等の第三者認証を取得している製品、ウェブサイ

ト等でセキュリティ対策の実装が確認できる製品や、製品セキュリティを維持するために製品サポート窓口や PSIRT が整備されていることがウェブサイト等で確認できるメーカーの製品が挙げられる。安全な製品の選定にあたっては、以下の文書が参考となる。

- IPA：ネット接続製品の安全な選定・利用ガイド
  https://www.ipa.go.jp/security/vuln/report/notice/guideforconsumer.html

(2) 小出力風力発電設備等に接続する端末（PC 等）に対して、マルウェアに対するパターンファイル型の検出・修復ソフトウェアを導入することで、攻撃コードの検知を実施する。

小出力風力発電設備設置者は、小出力風力発電設備等に接続する PC 等の接続端末に対して、マルウェア検出・修復ソフトウェアを導入し、攻撃コードの検知を実施することが求められる。この対策を実装していなかった場合、端末がマルウェアに感染し、それが小出力風力発電設備等に接続されることで、小出力風力発電設備等もマルウェアに感染する可能性がある。この結果、小出力風力発電設備等の動作停止につながり、系統への電力供給が停止するほか、系統の安定性に影響を与え、需給のバランスに乱れが生じる恐れもある。加えて、マルウェアに感染した小出力風力発電設備等を踏み台として、接続先サーバー等の他のシステムに対して不正アクセスが実行される危険性もある。

(3) 小出力風力発電設備等に接続する USB メモリ等の外部記憶媒体に対して、ウイルス対策ソフトによるチェック、ウイルスチェックが可能な USB メモリを用いる等の対策を行う。

小出力風力発電設備設置者は、小出力風力発電設備等に接続する USB メモリ等の外部記憶媒体に対して、適切なマルウェア対策を講じることが求められる。小出力風力発電設備等によっては、USB メモリ等を介した初期設定を行う場合が存在する。不正なプログラムやウイルスを小出力風力発電設備等に導入しないために、外部記憶媒体に対して、ウイルス対策ソフトによるチェック、ウイルスチェックが可能な USB メモリを用いる等の対策を行うことが求められる。この対策を実装していなかった場合、小出力風力発電設備等がマルウェアに感染し、小出力風力発電設備等の動作停止や、システムへの感染拡大につながる可能性がある。小出力風力発電設備等の動作停止につながった場合、系統への電力供給が停止するほか、系統の安定性に影響を与え、需給のバランスに乱れが生じる恐れもある。加えて、マルウェアに感染した小出力風力発電設備等を踏み台として、接続先サーバー等の他のシステムに対して不正アクセスが実行される危険性もある。

(4) 屋外に設置する小出力風力発電設備等において使用しない USB ポート、シリアルポートは栓をするなど物理的に閉塞する。

小出力風力発電設備設置者は、USB メモリ等を介して小出力風力発電設備等や防護装置（ルーター、ファイアウォール、VPN 等）がマルウェア感染するリスクを低減させるために、屋外に設置する小出力風力発電設備等や防護装置（ルーター、ファイアウォール、VPN 等）においては USB ポート、シリアルポートは栓をするなど物理的に閉塞することが求められる。物理的な閉塞

にあたっては、USB ポートやシリアルポートに対してポートロック製品を用いて物理的に閉塞する方法のほか、出力制御ユニット、通信装置等や防護装置自体を施錠管理できるキャビネットに保管する方法が考えられる。USB ポートに対する対策を実装していなかった場合、不正な外部記憶媒体等が接続され、小出力風力発電設備等や防護装置がマルウェアに感染する可能性がある。また、シリアルポートに対する対策を実装していなかった場合、開放しているシリアルポートに不正端末が接続され、小出力風力発電設備等や防護装置の設定を書き換えられる可能性がある。これらの結果、小出力風力発電設備等においては動作停止につながる可能性があるほか、防護装置においては適切な防護機能が維持されない可能性があり、それらのより系統への電力供給が停止するほか、系統の安定性に影響を与え、需給のバランスに乱れが生じる恐れもある。

(5) 小出力風力発電設備等に関する脆弱性、セキュリティパッチ、注意喚起等の情報を収集し、必要に応じた対応を行う。

小出力風力発電設備設置者は、導入している小出力風力発電設備等や防護装置（ルーター、ファイアウォール、VPN 等）に関する脆弱性、セキュリティパッチ、注意喚起等の情報を収集し、必要に応じた対応を行うことが求められる。脆弱性は随時発見されることから、その脆弱性に対するセキュリティパッチは早急に適用することが求められる。公的機関からの情報収集方法として、IPA や JPCERT/CC が用意している無料でアクセス可能な情報発信サービスを活用する方法があるほか、導入している小出力風力発電設備等のメーカーのウェブサイト等を定期的に確認し、脆弱性、セキュリティパッチ、注意喚起等の情報を収集することが望まれる。

- 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/
- JPCERT/CC, IPA：JVN (Japan Vulnerability Notes)
  https://jvn.jp/index.html

この対策を実装していなかった場合、既知の脆弱性が悪用され、小出力風力発電設備等もマルウェアに感染する可能性がある。この結果、小出力風力発電設備等の動作停止につながり、系統への電力供給が停止するほか、系統の安定性に影響を与え、需給のバランスに乱れが生じる恐れもある。加えて、マルウェアに感染した小出力風力発電設備等を踏み台として、接続先サーバー等の他のシステムに対して不正アクセスが実行される危険性もある。

3.2.3 対策③に関する対策実装例

小出力風力発電設置者は、「対策③：連系先系統運用者に対するセキュリティ管理責任者の氏名及び緊急時連絡先の通知」を実施するにあたって、以下に示す対策実装例が考えられる。

(1) 組織内で、小出力風力発電設備等に関するセキュリティ管理責任者を明確化し、組織内におけるセキュリティの役割と責任を明らかにする。
(2) 明確化したセキュリティ管理責任者の氏名及び緊急連絡先を連系先系統運用者（系統連系協議を行った相手、契約先の一般送配電事業者等。）に通知し、変更があった場合には速やかに再通知を行う。

以下に、各項目を解説する。

(1) 組織内で、小出力風力発電設備等に関するセキュリティ管理責任者を明確化し、組織内におけるセキュリティの役割と責任を明らかにする。

小出力風力発電設備設置者は、組織内で小出力風力発電設備等に関するセキュリティ管理責任者を明確化することが求められる。セキュリティ管理責任者は、組織内におけるセキュリティ対策に関する責任を担い、セキュリティ事象が発生した際に速やかに必要な措置を講じる必要がある。この対策を実装していなかった場合、セキュリティインシデントが発生した際に、インシデントに対する対応が遅れ被害が拡大し、自組織の小出力風力発電設備等が停止するなどの影響を及ぼす恐れがある。この結果、連系先等の他組織に対しても悪影響を与える可能性がある。

(2) 明確化したセキュリティ管理責任者の氏名及び緊急連絡先を連系先系統運用者（系統連系協議を行った相手、契約先の一般送配電事業者等。）に通知し、変更があった場合には速やかに再通知を行う。

小出力風力発電設備設置者は、接続する連系先系統運用者（系統連系協議を行った相手、契約先の一般送配電事業者等。）と迅速かつ的確な情報連絡を行うために、セキュリティ管理責任者の氏名及び緊急連絡先を連系先系統運用者に通知することが求められる。また、迅速かつ的確な情報連絡を行うために、通知している情報に変更があった場合には、速やかに再通知を行う必要がある。この対策を実装していなかった場合、セキュリティインシデントが発生した際に、連系先系統運用者が緊急の連絡を取ることができず、被害状況の確認や対応の遅れにより、インシデントの影響が拡大する恐れがある。

3.3 施工業者におけるサイバーセキュリティ対策の実装例

小出力風力発電設備の系統連系に際しては、一般送配電事業者に対して系統連系の申請が必要となり、サイバーセキュリティ対策（対策①～対策③）についても遵守していることを確認した上で申請を行う必要がある。小出力風力発電設備の設置にあたっては、電気工事士法に基づき電気工事士（施工業者）による設置工事が必要となるが、施工業者が委託を受け、代理で系統連系申請書を記入するケースも存在する。施工業者が小出力風力発電設備等の設置工事を行い、設備設置者（施工依頼者）の代理で系統連系申請を行う場合、設置者とともに小出力風力発電設備等に対するサイバーセキュリティ対策を講じ、対策①～対策③を実施していることを確認する必要がある。具体的な対策

実装例としては、3.2 に記載した小出力風力発電設備設置者における実装例のうち、施工業者が関与しうる以下の対策実装例について、可能な限り支援することが求められる。対策の実施にあたって施工業者自身で判断に迷う場合には、適宜小出力風力発電設備等のメーカーに実施すべき内容を確認することが望まれる。なお、各項目の解説については、3.2 の記載を参照されたい。

設備設置者と施工業者の間でセキュリティ対策の責任所在が不明瞭となり、双方とも適切な対策を実施しない状況は避けなければならない。そのため、施工業者は、電気工事の依頼を受けた際、セキュリティ対策をどちらが実施するか、対策の責任所在を明確化することが望まれる。仮に設備設置者がセキュリティ対策の責任主体となる場合でも、必要となるセキュリティ対策とその実装方法に関して、可能な限り施工業者が支援することが望まれる。

3.3.1 対策①に関する対策実装例

(1) 外部通信を行う小出力風力発電設備等を設置する際、小出力風力発電設備等に係る通信のうち、インターネットを介した通信については、防護装置（ルーター、ファイアウォール、VPN 等）を必ず経由させる。

(2) 防護装置（ルーター、ファイアウォール、VPN 等）に対して、遮断する通信（小出力風力発電設備等の運転において不要な通信、事前に設定していない通信 等）に関する設定を行う。もしくは、設置者自身で設定ができるよう、設定方法に関して説明を行う。

(3) インターネットを介した通信を行う小出力風力発電設備等を設置する際、小出力風力発電設備等の制御に係るシステムにおいて、システムのネットワークを、情報システムのネットワークから論理的あるいは物理的にセグメントを分離する。もしくは、設置者自身でセグメント分離の設定を行えるよう、設定方法に関して説明を行う。

(4) インターネットを介した通信を行う小出力風力発電設備等を設置する際、小出力風力発電設備等の制御に係るシステムと他ネットワークとの接続点を最小化する。もしくは、設置者自身で接続点最小化の設定を行えるよう、設定方法に関して説明を行う。

3.3.2 対策②に関する対策実装例

(1) 施工業者が購入する小出力風力発電設備等や防護装置（ルーター、ファイアウォール、VPN 等）について、正規品を購入する。

(2) 設備設置工事において小出力風力発電設備等に対して端末（PC 等）を接続する場合、マルウェアに対するパターンファイル型の検出・修復ソフトウェアを当該端末に導入することで、攻撃コードの検知を実施する。

(3) 設備設置工事において小出力風力発電設備等に対して USB メモリ等の外部記憶媒体を接続する場合、ウイルス対策ソフトによるチェック、ウイルスチェックが可能な USB メモリを用いる等の対策を行う。

(4) 設置した小出力風力発電設備等において使用しない USB ポート、シリアルポートは栓をするなど物理的に閉塞する。もしくは、設置者自身で閉塞ができるよう、具体的な対策方法に関して説明を行う。

3.4 小出力風力発電設備等のメーカーにおけるサイバーセキュリティ対策の実装例

3.4.1 対策①に関する対策実装例

小出力風力発電設備等のメーカーは、「対策① : ネットワーク接続点の保護」を実施するにあたって、以下に示す対策実装例が考えられる。

(1) 小出力風力発電設備等において、不要なネットワークサービスやネットワークポート等をあらかじめ無効化する。
(2) 小出力風力発電設備等の運転設定に関する管理画面に対するアクセスにおいて、アカウント認証を実装する。
(3) 小出力風力発電設備等に対する信頼できるサーバー以外からのセッション開始を禁止する。
(4) 設備設置者や施工業者が防護装置（ルーター、ファイアウォール、VPN 等）に対して実施すべき設定やセキュリティ対策を、取扱説明書や施工説明書等に明記する。

それぞれの項目における対策箇所のイメージを図 3-3 に示す。以下に、各項目を解説する。

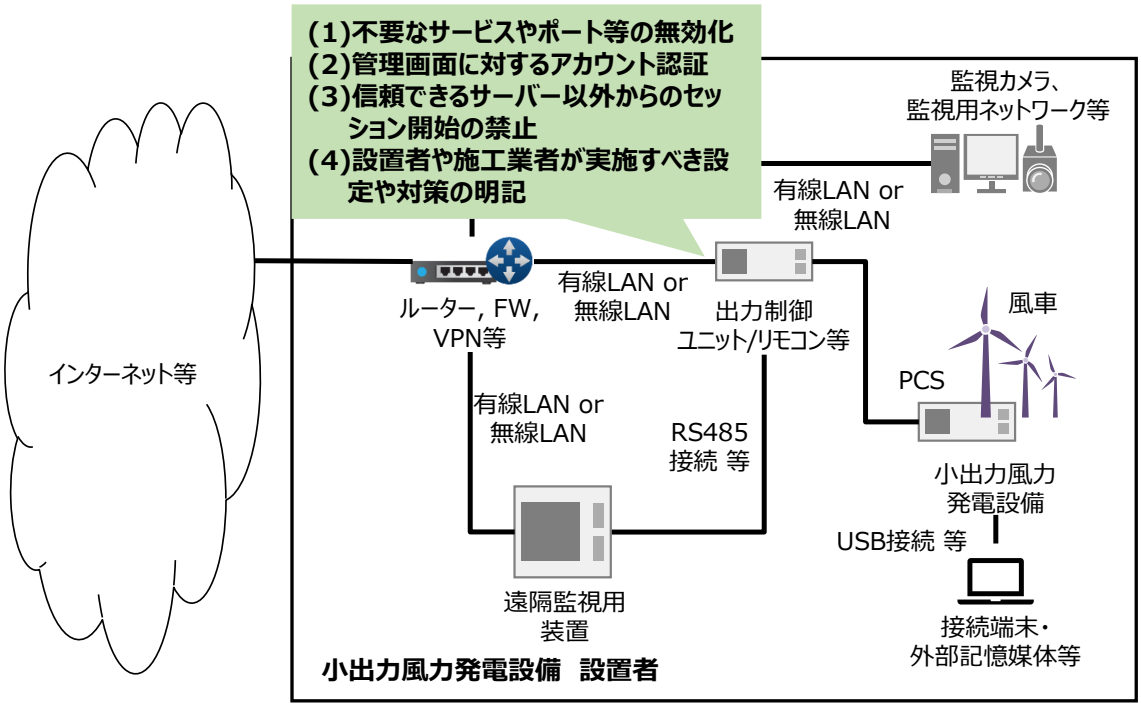


図 3-3 小出力風力発電設備等のメーカーにおける対策①に関する対策実装例

(1) 小出力風力発電設備等において、ネットワーク接続する設備において、不要なネットワークサービスやネットワークポート等をあらかじめ無効化する。

小出力風力発電設備等のメーカーは、設置者のネットワークに意図しない通信が入る可能性を踏まえ、外部からの不正侵入を防ぐ仕組みを小出力風力発電設備等で実装することが求められる。具体的には、未使用のネットワークポートやサービスに対する不正アクセスにより小出力風力発電設備等の動作が停止するサイバーセキュリティリスクを防ぐために、機器の正常動作に必要のない不要なサービスやネットワークポートを無効化することが求められる。機器の開発段階で不要なサービスやネットワークポートを無効化する処置を行うとともに、製品出荷前のテスト段階において機器に対してポートスキャン（機器上で動作しているサービスや開放しているポートを確認する診断手法）を実施し、不要なサービスやネットワークポートが存在しないかを確認することが重要である。また、実施可能である場合に、小出力風力発電設備等に対してファイアウォール機能（不要なネットワークポートを利用した通信を遮断する機能　等）を実装し、外部からの不正な通信を遮断することが望まれる。この対策を実装していなかった場合、小出力風力発電設備等に不正アクセスがなされ、小出力風力発電設備等の動作停止や小出力風力発電設備等を踏み台とした他のシステムに対する不正アクセスが実行される可能性がある。

(2) 小出力風力発電設備等のネットワーク接続する設備の運転設定に関する管理画面に対するアクセスにおいて、アカウント認証を実装する。

小出力風力発電設備等のメーカーは、小出力風力発電設備等の運転設定に関する管理画面に対するアクセスにおいて、アカウント認証を実装することが求められる。また、認証の際のパスワードについて、パスワード未設定の状態や出荷段階のパスワードのままとすることを許容せず、設備設置者におけるパスワード変更を必須とすることが望ましい。この対策を実装していなかった場合、小出力風力発電設備等に不正アクセスがなされ、小出力風力発電設備等の動作停止や小出力風力発電設備等を踏み台とした他のシステムに対する不正アクセスが実行される可能性がある。

(3) 小出力風力発電設備等に対する信頼できる接続先サーバー以外からのセッション開始を禁止する。

小出力風力発電設備等のメーカーは、小出力風力発電設備等に対する信頼できる接続先サーバー以外からのセッション開始を禁止することが求められる。この対策は、外部からの不正な遠隔操作を防止するために必要な対策である。出力制御機能付きの PCS の場合、「出力制御機能付 PCS 等の技術仕様」で求められているとおり、信頼できる信頼先サーバー以外に限らず、すべての外部セッション開始を禁止することが求められることに注意する。この対策を実装していなかった場合、小出力風力発電設備等に不正アクセスがなされ、小出力風力発電設備等の動作停止や小出力風力発電設備等を踏み台とした他のシステムに対する不正アクセスが実行される可能性がある。

(4) 設備設置者や施工業者が防護装置（ルーター、ファイアウォール、VPN 等）等に対して実施すべき設定やセキュリティ対策を、取扱説明書や施工説明書等に明記する。

小出力風力発電設備等のメーカーは、設備設置者や施工業者が防護装置等に対して実施すべき設定やセキュリティ対策を、取扱説明書、施工説明書等で明記することが求められる。具体的な内容として、以下の内容を明記することが望まれる。

- 小出力風力発電設備等と防護装置等との接続方法
- 接続可能な防護装置等の条件
- 系統連系技術要件の対策①を満足するために、防護装置等に対して設備設置者や施工業者が実施すべき対策
- 接続テストの実施方法
- 小出力風力発電設備等の管理画面におけるパスワードの変更方法
- 想定する利用環境やネットワーク構成
- 接続不良時に想定される原因や対処方法（トラブルシューティング）

この対策を実装していなかった場合、設備設置者により実施すべき対策が適切に実施されず、小出力風力発電設備等に不正アクセスがなされ、小出力風力発電設備等の動作停止や小出力風力発電設備等を踏み台とした他のシステムに対する不正アクセスが実行される可能性がある。

3.4.2 対策②に関する対策実装例

PCS メーカー・関連通信機器メーカーは、「対策② ：データの保存・転送を行う機器・端末等のマルウェア対策」を実施するにあたって、以下に示す対策実装例が考えられる。

(1) 小出力風力発電設備等において、実行可能なプログラムや機能をあらかじめ制限する。
(2) 小出力風力発電設備等において、ソフトウェアやファームウェアをアップデートする機能を実装し、新たな脆弱性が検出された場合等に設置者が確実にアップデートを行える仕組みを実装する。
(3) マルウェア対策やアップデートに関して設備設置者や施工業者が実施すべき設定やセキュリティ対策を、取扱説明書や施工説明書等に明記する。

それぞれの項目における対策箇所のイメージを図 3-4 に示す。以下に、各項目を解説する。

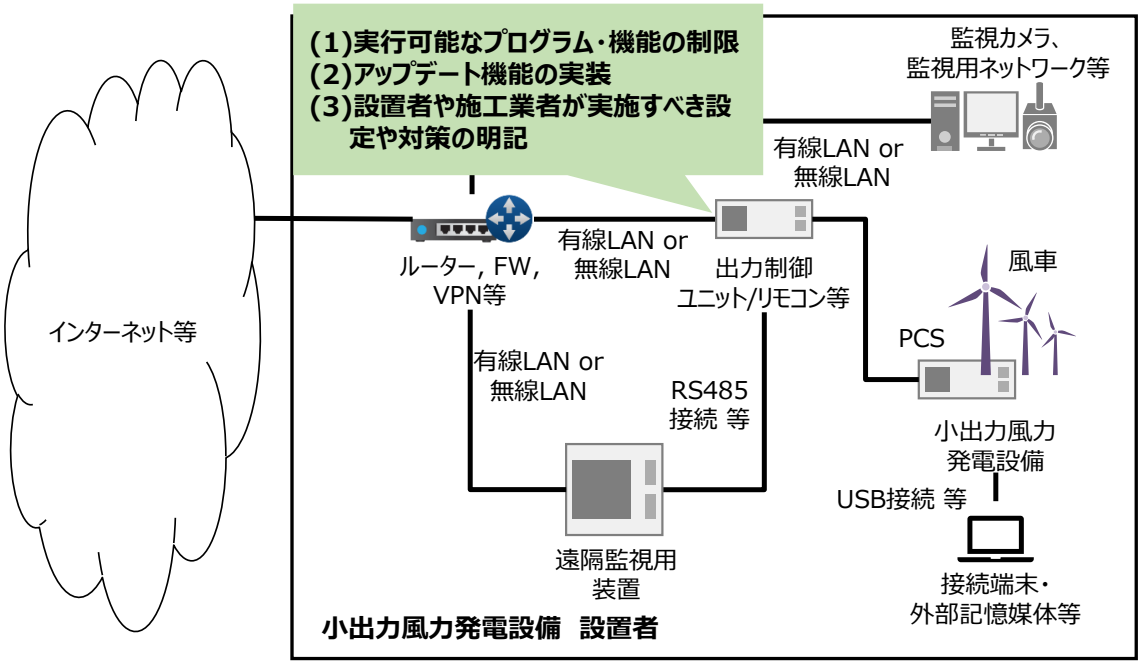


図 3-4 小出力風力発電設備等のメーカーにおける対策②に関する対策実装例

(1) 小出力風力発電設備等において、実行可能なプログラムや機能をあらかじめ制限する。

小出力風力発電設備等のメーカーは、小出力風力発電設備等において実行可能なプログラムや機能に関して、あらかじめ許可したプログラムや機能以外の動作を禁止することが求められる。この対策を実装していなかった場合、小出力風力発電設備等がマルウェアに感染し、小出力風力発電設備等の動作停止や、システムへの感染拡大につながる可能性がある。

(2) 小出力風力発電設備等において、ソフトウェアやファームウェアをアップデートする機能を実装し、新たな脆弱性が検出された場合等に設置者が確実にアップデートを行える仕組みを実装する。

小出力風力発電設備等のメーカーは、小出力風力発電設備等のセキュリティを確保・維持するために、ソフトウェアやファームウェアをアップデートする機能を実装することが求められる。そして、新たな脆弱性が検出された場合等、アップデートが必要となった場合に、設置者が速やかにアップデートを行える仕組みを実装することが求められる。可能な限り、自動アップデート機能を実装することが望まれるが、自動アップデートの実装が困難な場合においては、設備設置者がアップデート実施時期を選択できるアップデート手法を選択することが望まれる。具体的には、小出力風力発電設備等の管理画面やユーザーインタフェース上にポップアップでアップデートがあることを通知するほか、設置者や設備設置者が管理依頼している O&M 事業者等に対して電子メール等でアップデートがあることを通知するなどして、設備設置者にアップデートを促す実装を講じることが望まれる。いずれのアップデート方法であっても、次項に示すとおり、アップデートのために設備設置者が実施すべき事項を取扱説明書に明記する必要がある。この対策を実装していなかった場合、

小出力風力発電設備等に脆弱性が残存し、当該脆弱性が悪用された場合に、小出力風力発電設備等がマルウェアに感染する可能性がある。アップデートを考慮した設計にあたっての留意点やアップデート手法の違いについては、下記の IPA ガイドが参考となる。

- IPA：脆弱性対処に向けた製品開発者向けガイド
  https://www.ipa.go.jp/security/vuln/report/notice/guideforvendor.html

小出力風力発電設備等の出荷段階で脆弱性を残存させず、小出力風力発電設備等のセキュリティを高めるためには、小出力風力発電設備等に対して脆弱性検査（脆弱性診断）を実施することが望まれる。これにより、出荷後に小出力風力発電設備等において脆弱性が検出される可能性を低減できる。また、小出力風力発電設備等のメーカーに関して、出荷後に発見された脆弱性に対処するためのコストを低減できるだけでなく、脆弱性を悪用したセキュリティ事象への対処コストを削減することができる。具体的な脆弱性検査の実施手順としては、上記の IPA「脆弱性対処に向けた製品開発者向けガイド」のほか、以下の文書が参考となる。

- 経済産業省：機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き
  https://www.meti.go.jp/press/2021/04/20210419003/20210419003.html

(3) マルウェア対策やアップデートに関して設備設置者や施工業者が実施すべき設定やセキュリティ対策を、取扱説明書や施工説明書等に明記する。

小出力風力発電設備等のメーカーは、設備設置者や施工業者が防護装置等に対し、マルウェア対策やアップデートに関して実施すべき設定やセキュリティ対策を、取扱説明書、施工説明書等で明記することが求められる。具体的な内容として、以下の内容を明記することが望まれる。

- ソフトウェアやファームウェアのアップデート機能の存在
- ソフトウェアやファームウェアをアップデートするために実施すべき設定や手順
- アップデートにあたっての留意事項・免責事項
- 系統連系技術要件の対策②を満足するために、設備設置者や施工業者が接続端末や外部記憶媒体等に実施すべき対策
- 接続テストの実施方法
- アップデート不調時に想定される原因や対処方法（トラブルシューティング）

この対策を実装していなかった場合、設備設置者により実施すべき対策が適切に実施されず、小出力風力発電設備等がマルウェアに感染し、小出力風力発電設備等の動作停止や、システムへの感染拡大につながる可能性がある。

3.5 監視サービスプロバイダー等におけるサイバーセキュリティ対策の実装例

以降では、監視サービスプロバイダー等におけるサイバーセキュリティ対策の実装例として、特に設備設置者が導入する遠隔監視用装置に求められるセキュリティ対策の実装例を示す。

本文書では詳細な内容を記載しないものの、監視サービスプロバイダー自身のセキュリティ対策も極め

て重要となる。監視サービスを提供しているシステムやサーバー等の機器がサイバー攻撃の被害にあった場合、その影響は監視サービスプロバイダーのシステムに留まらず、そのサービスに接続する設備設置者に対しても影響を及ぼす恐れがある。その結果、小出力風力発電設備等に対する不正アクセスやマルウェア感染につながる可能性もある。そのため、監視サービスプロバイダーは、導入するシステムやサーバー等の機器について品質や信頼性が確保されている機器を採用し、適切な脆弱性対応を行う必要がある。加えて、サイバーセキュリティリスクの管理体制やインシデント対応の体制を構築し、サイバーセキュリティリスクの特定と対策を実装する必要がある。これらの対策の実施にあたっては、以下のような文書を参考にすることが推奨される。

- 経済産業省：サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）[17]
- 経済産業省：サイバーセキュリティ経営ガイドライン[18]
- 経済産業省：情報セキュリティ管理基準[19]

3.5.1 対策①に関する対策実装例

監視サービスプロバイダー等は、遠隔監視用装置に関して「対策①：ネットワーク接続点の保護」を実施するにあたって、以下に示す対策実装例が考えられる。

(1) 遠隔監視用装置において、不要なネットワークサービスやネットワークポート等をあらかじめ無効化する。
(2) 遠隔監視用装置の運転設定に関する管理画面に対するアクセスにおいて、アカウント認証を実装する。
(3) 遠隔監視用装置に対する信頼できる接続先サーバー以外からのセッション開始を禁止する。
(4) 設備設置者や施工業者による対策や設定が必要な場合、その内容を取扱説明書や施工説明書等に明記する。
(5) 遠隔監視用装置と監視サービスプロバイダーのサーバーとの接続は、適切なプロトコルを用いて認証・認可を行う。
(6) 遠隔監視用装置と監視サービスプロバイダーのサーバーとの通信は、適切なプロトコルを用いて暗号化する。

それぞれの項目における対策箇所のイメージを図 3-5 に示す。以下に、各項目を解説する。

[17] https://www.meti.go.jp/press/2019/04/20190418002/20190418002.html
[18] https://www.meti.go.jp/policy/netsecurity/mng_guide.html
[19] https://www.meti.go.jp/policy/netsecurity/is-kansa/

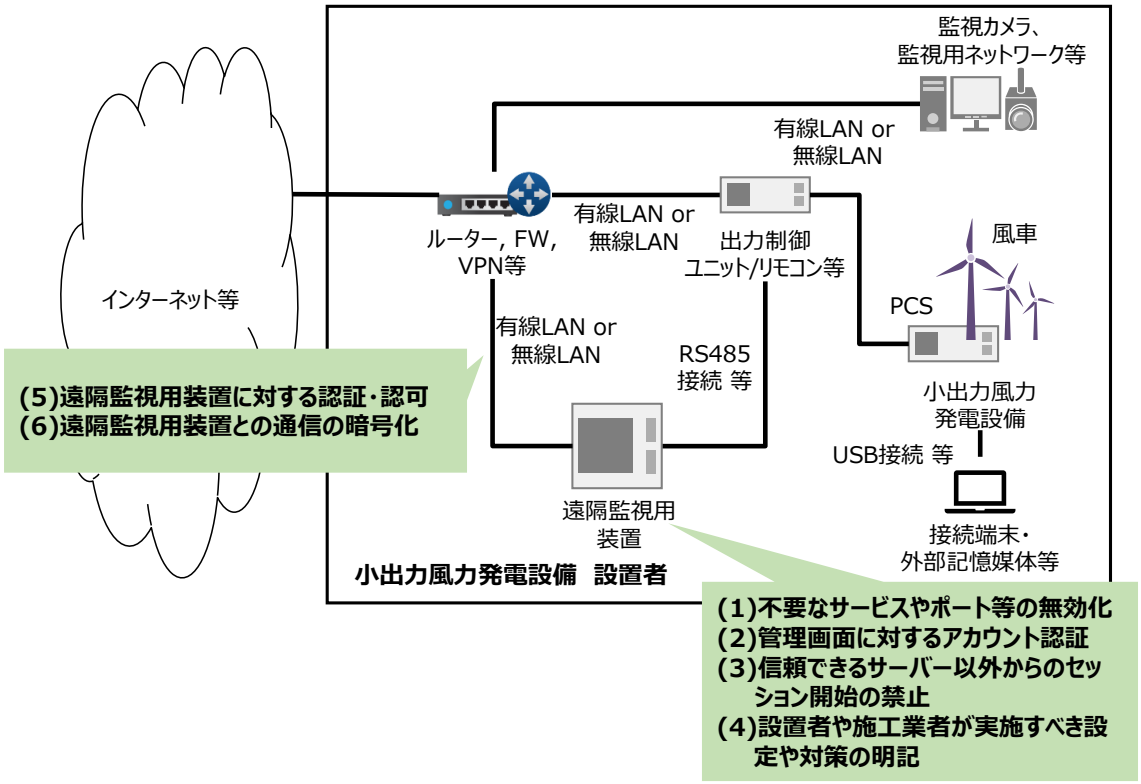


図 3-5 監視サービスプロバイダー等における対策①に関する対策実装例

(1) 遠隔監視用装置において、不要なネットワークサービスやネットワークポート等をあらかじめ無効化する。

監視サービスプロバイダー等は、遠隔監視用装置に対する未使用のネットワークポートやサービスに対する不正アクセスにより遠隔監視用装置の動作が停止するサイバーセキュリティリスクを防ぐために、装置の正常動作に必要のない不要なサービスやネットワークポートを無効化することが求められる。装置の開発段階で不要なサービスやポートを無効化する処置を行うとともに、製品出荷前のテスト段階において装置に対してポートスキャン（装置上で動作しているサービスや開放しているネットワークポートを確認する診断手法）を実施し、不要なサービスやネットワークポートが存在しないかを確認することが重要である。また、実施可能である場合に、装置に対してファイアウォール機能　（不要なネットワークポートを利用した通信を遮断する機能　等）を実装し、外部からの不正な通信を遮断することが望まれる。この対策を実装していなかった場合、遠隔監視用装置に不正アクセスがなされ、装置の動作停止や装置を踏み台とした他のシステムに対する不正アクセスが実行される可能性がある。

(2) 遠隔監視用装置の運転設定に関する の管理画面や計測画面に対するアクセスにおいて、アカウント認証を実装する。

監視サービスプロバイダー等は、遠隔監視用装置の運転設定に関する管理画面に対するアク

セスにおいて、アカウント認証を実装することが求められる。また、認証の際のパスワードについて、パスワード未設定の状態や出荷段階のパスワードのままとすることを許容せず、設備設置者におけるパスワード変更を必須とすることが望ましい。この対策を実装していなかった場合、遠隔監視用装置に不正アクセスがなされ、装置の動作停止や装置を踏み台とした他のシステムに対する不正アクセスが実行される可能性がある。

(3) 遠隔監視用装置に対する信頼できる接続先サーバー以外からのセッション開始を禁止する。

監視サービスプロバイダー等は、遠隔監視用装置に対する信頼できる接続先サーバー以外からのセッション開始を禁止することが求められる。本対策は、外部からの不正な遠隔操作を防止するために必要な対策である。この対策を実装していなかった場合、外部ネットワークから遠隔監視用装置に不正アクセスがなされ、装置の動作停止や装置を踏み台とした他のシステムに対する不正アクセスが実行される可能性がある。

(4) 設備設置者や施工業者による対策や設定が必要な場合、その内容を取扱説明書や施工説明書等に明記する。

監視サービスプロバイダー等は、遠隔監視用装置に対して設備設置者や施工業者が実施すべき設定やセキュリティ対策を、取扱説明書、施工説明書等で明記することが求められる。具体的な内容として、以下の内容を明記することが望まれる。

- 遠隔監視用装置と防護装置等との接続方法
- 接続可能な防護装置等の条件
- 系統連系技術要件の対策①を満足するために、防護装置等に対して設備設置者や施工業者が実施すべき対策
- 接続テストの実施方法
- 遠隔監視用装置の管理画面におけるパスワードの変更方法
- 想定する利用環境やネットワーク構成
- 接続不良時に想定される原因や対処方法（トラブルシューティング）

この対策を実装していなかった場合、設備設置者により実施すべき対策が適切に実施されず、遠隔監視用装置に不正アクセスがなされ、装置の動作停止や装置を踏み台とした他のシステムに対する不正アクセスが実行される可能性がある。

(5) 遠隔監視用装置と監視サービスプロバイダーのサーバーとの接続は、適切なプロトコルを用いて認証・認可を行う。

監視サービスプロバイダー等は、遠隔監視用装置と監視サービスプロバイダーのサーバーとの接続について、適切なプロトコルを用いて認証・認可を行うことが求められる。この対策を実装していなかった場合、遠隔監視用装置に不正アクセスがなされ、装置の動作停止や装置を踏み台とした他のシステムに対する不正アクセスが実行される可能性がある。

(6) 遠隔監視用装置と監視サービスプロバイダーのサーバーとの通信は、適切なプロトコルを用いて暗号化する。

監視サービスプロバイダー等は、遠隔監視用装置と監視サービスプロバイダーのサーバーとの接続について、適切なプロトコルを用いて暗号化することが求められる。暗号を用いる場合、適用範囲、暗号アルゴリズムの種別、強度及び品質を考慮した上で暗号方式を選択し、管理することが望ましい。この対策を実装していなかった場合、通信データの傍受・改ざんや不正閲覧につながる可能性がある。

3.5.2 対策②に関する対策実装例

監視サービスプロバイダー等は、遠隔監視用装置に関して「対策② ：データの保存・転送を行う機器・端末等のマルウェア対策」を実施するにあたって、以下に示す対策実装例が考えられる。

(1) 遠隔監視用装置において、実行可能なプログラムや機能をあらかじめ制限する。
(2) 遠隔監視用装置において、ソフトウェアやファームウェアをアップデートする機能を実装し、新たな脆弱性が検出された場合等に設置者が確実にアップデートを行える仕組みを実装する。
(3) マルウェア対策やアップデートに関して設備設置者が実施すべき設定やセキュリティ対策を、取扱説明書や施工説明書等に明記する。

それぞれの項目における対策箇所のイメージを図 3-4 に示す。以下に、各項目を解説する。

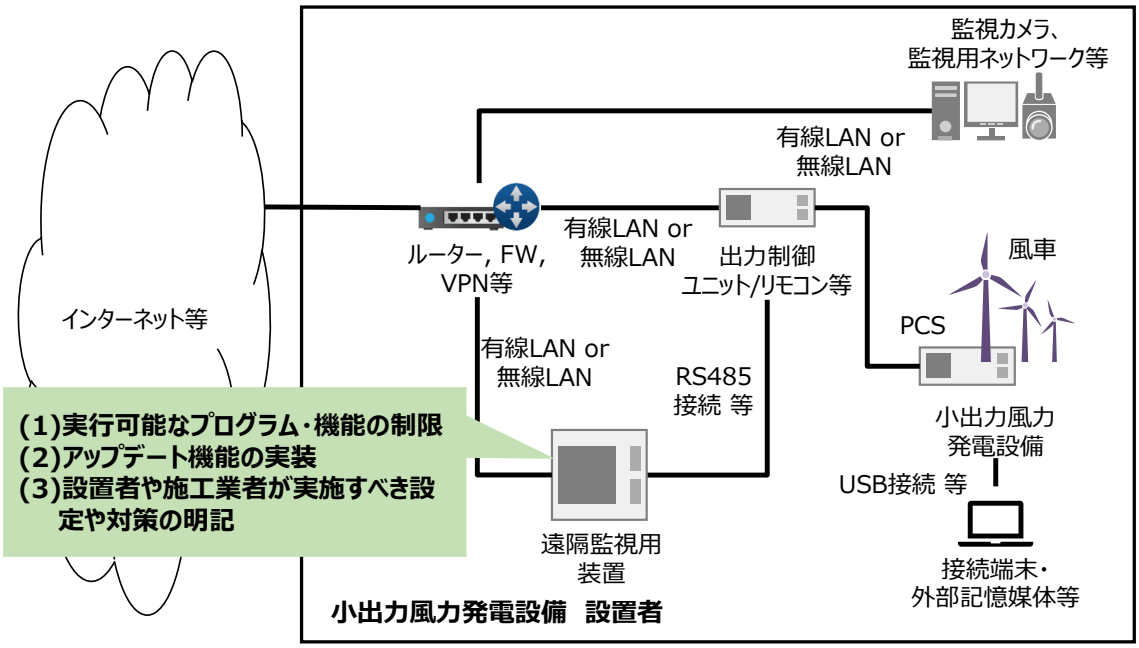


図 3-6 監視サービスプロバイダー等における対策②に関する対策実装例

(1) 遠隔監視用装置において、実行可能なプログラムや機能をあらかじめ制限する。

監視サービスプロバイダー等は、遠隔監視用装置において実行可能なプログラムや機能に関して、あらかじめ許可したプログラムや機能以外の動作を禁止することが求められる。この対策を実装していなかった場合、遠隔監視用装置がマルウェアに感染し、装置の動作停止や、システムへの感染拡大につながる可能性がある。

(2) 遠隔監視用装置において、ソフトウェアやファームウェアをアップデートする機能を実装し、新たな脆弱性が検出された場合等に設置者が確実にアップデートを行える仕組みを実装する。

監視サービスプロバイダー等は、遠隔監視用装置のセキュリティを確保・維持するために、ソフトウェアやファームウェアをアップデートする機能を実装することが求められる。そして、新たな脆弱性が検出された場合等、アップデートが必要となった場合に、設置者が速やかにアップデートを行える仕組みを実装することが求められる。可能な限り、自動アップデート機能を実装することが望まれるが、自動アップデートの実装が困難な場合においては、設備設置者がアップデート実施時期を選択できるアップデート手法を選択することが望まれる。具体的には、遠隔監視用装置の管理画面やユーザーインタフェース上にポップアップでアップデートがあることを通知するほか、設置者や設備設置者が管理依頼している O&M 事業者等に対して電子メール等でアップデートがあることを通知するなどして、設備設置者にアップデートを促す実装を講じることが望まれる。いずれのアップデート方法であっても、次項に示すとおり、アップデートのために設備設置者が実施すべき事項を取扱説明書に明記する必要がある。この対策を実装していなかった場合、遠隔監視用装置に脆弱性が残存し、当該脆弱性が悪用された場合に、遠隔監視用装置がマルウェアに感染する可能性がある。アップデートを考慮した設計にあたっての留意点やアップデート手法の違いについては、下記の IPA ガイドが参考となる。

- IPA：脆弱性対処に向けた製品開発者向けガイド
  https://www.ipa.go.jp/security/vuln/report/notice/guideforvendor.html

遠隔監視用装置の出荷段階で脆弱性を残存させず、装置のセキュリティを高めるためには、装置に対して脆弱性検査（脆弱性診断）を実施することが望まれる。これにより、出荷後に装置において脆弱性が検出される可能性を低減できる。また、監視サービスプロバイダー等に関して、出荷後に発見された脆弱性に対処するためのコストを低減できるだけでなく、脆弱性を悪用したセキュリティ事象への対処コストを削減することができる。具体的な脆弱性検査の実施手順としては、上記の IPA「脆弱性対処に向けた製品開発者向けガイド」のほか、以下の文書が参考となる。

- 経済産業省：機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き
  https://www.meti.go.jp/press/2021/04/20210419003/20210419003.html

(3) マルウェア対策やアップデートに関して設備設置者や施工業者が実施すべき設定やセキュリティ対策を、取扱説明書や施工説明書等に明記する。

監視サービスプロバイダー等は、設備設置者や施工業者が防護装置等に対し、マルウェア対策やアップデートに関して実施すべき設定やセキュリティ対策を、取扱説明書、施工説明書等で開示することが求められる。具体的な内容として、以下の内容を明記することが望まれる。

- ソフトウェアやファームウェアのアップデート機能の存在
- ソフトウェアやファームウェアをアップデートするために実施すべき設定や手順
- アップデートにあたっての留意事項・免責事項
- 系統連系技術要件の対策②を満足するために、設備設置者や施工業者が接続端末や外部記憶媒体等に実施すべき対策
- 接続テストの実施方法
- アップデート不調時に想定される原因や対処方法（トラブルシューティング）

この対策を実装していなかった場合、設備設置者により実施すべき対策が適切に実施されず、遠隔監視用装置がマルウェアに感染し、設備等の動作停止や、システムへの感染拡大につながる可能性がある。

付録A　小出力風力発電設備設置者における対策実装例リスト

小出力風力発電設備（一般用電気工作物に分類される出力 20kW 未満の小形風力発電設備）の設置者は、以下の実装例を参考に、系統連系技術要件が求める３つのサイバーセキュリティ対策を実施する必要がある。サイバーセキュリティ対策の実施にあたっては、関連する小出風力発電設備等（小出力風力発電設備及びそれに付随する PCS（パワーコンディショナー）、出力制御ユニット、通信装置等）のメーカーが説明書等に記載している実施すべき事項や注意事項を確認し、施工業者と連携しつつ対策を実施することが望まれる。

本リストで示す対策実装例は系統連系技術要件で求められる対策を実装するための例示的位置づけであり、小出力風力発電設備設置者は自組織の対策範囲についてリスクを評価した上で適切な実装例を選択することが求められる。また、記載の対策実装例以外にも、系統連系技術要件で求められる対策へ対応するための実装方法は存在することに留意する必要がある。

対策実装例	
対策①　ネットワーク接続点の保護	
	(1) 小出力風力発電設備等に係る通信のうち、インターネットを介した通信については、防護装置（ルーター、ファイアウォール、VPN 等）を必ず経由させる。
	(2) 防護装置（ルーター、ファイアウォール、VPN 等）に対して、遮断する通信（小出力風力発電設備等の運転において不要な通信、事前に設定していない通信 等）に関する設定を行う。
	(3) 不正アクセス等のセキュリティ事象を適切に検知できるよう、インターネットを介した通信に関してネットワーク監視や通信のモニタリングを実施する。
	(4) 小出力風力発電設備等の制御に係るシステムにおいて、システムのネットワークを、情報システムのネットワークから論理的あるいは物理的にセグメントを分離する。
	(5) 小出力風力発電設備等の制御に係るシステムと他ネットワークとの接続点を最小化する。
	(6) 小出力風力発電設備等の運転設定に関する管理画面に対してアクセスする際の認証情報（パスワード等）を、適切に管理する。
対策②　データの保存・転送を行う機器・端末等のマルウェア対策	
	(1) 利用する小出力風力発電設備等や防護装置（ルーター、ファイアウォール、VPN 等）について、正規品を購入する。
	(2) 小出力風力発電設備等に接続する端末（PC 等）に対して、マルウェアに対するパターンファイル型の検出・修復ソフトウェアを導入することで、攻撃コードの検知を実施する。
	(3) 小出力風力発電設備等に接続する USB メモリ等の外部記憶媒体に対して、ウイルス対策ソフトによるチェック、ウイルスチェックが可能な USB メモリを用いる等の対策を行う。
	(4) 屋外に設置する小出力風力発電設備等や防護装置（ルーター、ファイアウォール、VPN 等）において使用しない USB ポート、シリアルポートは栓をするなど物理的に閉塞する。

対策実装例	
	(5) 小出力風力発電設備等や防護装置（ルーター、ファイアウォール、VPN 等）に関する脆弱性、セキュリティパッチ、注意喚起等の情報を収集し、必要に応じた対応を行う。
対策③ 連系先系統運用者に対するセキュリティ管理責任者の氏名及び緊急時連絡先の通知	
	(1) 組織内で、小出力風力発電設備等に関するセキュリティ管理責任者を明確化し、組織内におけるセキュリティの役割と責任を明らかにする。
	(2) 明確化したセキュリティ管理責任者の氏名及び緊急連絡先を連系先系統運用者（系統連系協議を行った相手、契約先の一般送配電事業者等。）に通知し、変更があった場合には速やかに再通知を行う。

付録B　施工業者における対策実装例リスト

小出力風力発電設備（一般用電気工作物に分類される出力 20kW 未満の小形風力発電設備）の設置に係る施工業者は、設備設置者が系統連系技術要件で求められるサイバーセキュリティ対策を実施できるよう、以下の実装例を参考に設備設置者の対策を支援することが望まれる。

本リストで示す対策実装例は系統連系技術要件で求められる対策を実装するための例示的位置づけであり、小出力風力発電設備の設置者が対策範囲についてリスクを評価した上で適切な実装例を選択できるよう、対策を支援することが望まれる。また、記載の対策実装例以外にも、系統連系技術要件で求められる対策へ対応するための実装方法は存在することに留意する必要がある。

対策実装例	
対策①　ネットワーク接続点の保護	
	(1) 外部通信を行う小出力風力発電設備等を設置する際、小出力風力発電設備等に係る通信のうち、インターネットを介した通信については、防護装置（ルーター、ファイアウォール、VPN 等）を必ず経由させる。
	(2) 防護装置（ルーター、ファイアウォール、VPN 等）に対して、遮断する通信（小出力風力発電設備等の運転において不要な通信、事前に設定していない通信 等）に関する設定を行う。もしくは、設置者自身で設定ができるよう、設定方法に関して説明を行う。
	(3) インターネットを介した通信を行う小出力風力発電設備等を設置する際、小出力風力発電設備等の制御に係るシステムにおいて、システムのネットワークを、情報システムのネットワークから論理的あるいは物理的にセグメントを分離する。もしくは、設置者自身でセグメント分離の設定を行えるよう、設定方法に関して説明を行う。
	(4) インターネットを介した通信を行う小出力風力発電設備等を設置する際、小出力風力発電設備等の制御に係るシステムと他ネットワークとの接続点を最小化する。もしくは、設置者自身で接続点最小化の設定を行えるよう、設定方法に関して説明を行う。
対策②　データの保存・転送を行う機器・端末等のマルウェア対策	
	(1) 施工業者が購入する小出力風力発電設備等や防護装置（ルーター、ファイアウォール、VPN 等）について、正規品を購入する。
	(2) 設備設置工事において小出力風力発電設備等に対して端末（PC 等）を接続する場合、マルウェアに対するパターンファイル型の検出・修復ソフトウェアを当該端末に導入することで、攻撃コードの検知を実施する。
	(3) 設備設置工事において小出力風力発電設備等に対して USB メモリ等の外部記憶媒体を接続する場合、ウイルス対策ソフトによるチェック、ウイルスチェックが可能な USB メモリを用いる等の対策を行う。

対策実装例	
	(4) 設置した小出力風力発電設備等において使用しない USB ポート、シリアルポートは栓をするなど物理的に閉塞する。もしくは、設置者自身で閉塞ができるよう、具体的な対策方法に関して説明を行う。

付録C　小出力風力発電設備等のメーカーにおける対策実装例リスト

小出力風力発電設備等（一般用電気工作物に分類される出力 20kW 未満の小形風力発電設備及びそれに付随する PCS（パワーコンディショナー）、出力制御ユニット、通信装置等）のメーカーは、設備設置者が系統連系技術要件で求められるサイバーセキュリティ対策を実施できるよう、以下の実装例を参考に、小出力風力発電設備等に対して適切な対策を講じることが望まれる。

本リストで示す対策実装例は系統連系技術要件で求められる対策を実装するための例示的位置づけであり、小出力風力発電設備等のメーカーは、小出力風力発電設備等についてリスクを評価した上で適切な実装例を選択することが求められる。また、記載の対策実装例以外にも、系統連系技術要件で求められる対策へ対応するための実装方法は存在することに留意する必要がある。

対策実装例	
対策①　ネットワーク接続点の保護	
	(1) 小出力風力発電設備等において、不要なネットワークサービスやネットワークポート等をあらかじめ無効化する。
	(2) 小出力風力発電設備等の運転設定に関する管理画面に対するアクセスにおいて、アカウント認証を実装する。
	(3) 小出力風力発電設備等に対する信頼できるサーバー以外からのセッション開始を禁止する。
	(4) 設備設置者や施工業者が防護装置（ルーター、ファイアウォール、VPN 等）に対して実施すべき設定やセキュリティ対策を、取扱説明書や施工説明書等に明記する。
対策②　データの保存・転送を行う機器・端末等のマルウェア対策	
	(1) 小出力風力発電設備等において、実行可能なプログラムや機能をあらかじめ制限する。
	(2) 小出力風力発電設備等において、ソフトウェアやファームウェアをアップデートする機能を実装し、新たな脆弱性が検出された場合等に設置者が確実にアップデートを行える仕組みを実装する。
	(3) マルウェア対策やアップデートに関して設備設置者や施工業者が実施すべき設定やセキュリティ対策を、取扱説明書や施工説明書等に明記する。

付録D　監視サービスプロバイダー等における対策実装例リスト

小出力風力発電設備（一般用電気工作物に分類される出力 20kW 未満の小形風力発電設備）の発電状況を監視するサービスのプロバイダー及び当該監視に必要な計測通信装置のメーカーは、設備設置者が系統連系技術要件で求められるサイバーセキュリティ対策を実施できるよう、以下の実装例を参考に、遠隔監視用装置に対して適切な対策を講じることが望まれる。

本リストで示す対策実装例は系統連系技術要件で求められる対策を実装するための例示的位置づけであり、小出力風力発電設備の発電状況を監視するサービスのプロバイダー及び当該監視に必要な計測通信装置のメーカーは、当該装置についてリスクを評価した上で適切な実装例を選択することが求められる。また、記載の対策実装例以外にも、系統連系技術要件で求められる対策へ対応するための実装方法は存在することに留意する必要がある。

対策実装例	
対策①　ネットワーク接続点の保護	
	(1) 遠隔監視用装置において、不要なネットワークサービスやネットワークポート等をあらかじめ無効化する。
	(2) 遠隔監視用装置の運転設定に関する管理画面に対するアクセスにおいて、アカウント認証を実装する。
	(3) 遠隔監視用装置に対する信頼できる接続先サーバー以外からのセッション開始を禁止する。
	(4) 設備設置者や施工業者による対策や設定が必要な場合、その内容を取扱説明書や施工説明書等に明記する。
	(5) 遠隔監視用装置と監視サービスプロバイダーのサーバーとの接続は、適切なプロトコルを用いて認証・認可を行う。
	(6) 遠隔監視用装置と監視サービスプロバイダーのサーバーとの通信は、適切なプロトコルを用いて暗号化する。
対策②　データの保存・転送を行う機器・端末等のマルウェア対策	
	(1) 遠隔監視用装置において、実行可能なプログラムや機能をあらかじめ制限する。
	(2) 遠隔監視用装置において、ソフトウェアやファームウェアをアップデートする機能を実装し、新たな脆弱性が検出された場合等に設置者が確実にアップデートを行える仕組みを実装する。
	(3) マルウェア対策やアップデートに関して設備設置者が実施すべき設定やセキュリティ対策を、取扱説明書や施工説明書等に明記する。

付録E　用語集

1. 一般用電気工作物

600V 以下で受電する需要設備又は小出力発電設備で、構外にわたる配電線路を有さない設備のこと。

2. 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のこと。

3. 脅威

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

4. サイバー攻撃

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

5. サイバーセキュリティ

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

6. サプライチェーン

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

7. 自家用電気工作物

事業用電気工作物のうち、電気事業の用に供する電気工作物以外のもの。

8. CVE

Common Vulnerabilities and Exposures の略で、個別製品中の脆弱性に付与される識別子のこと。

9. 出力制御

電力会社が発電事業者に対して発電設備からの出力停止又は抑制を要請し、設備の発電量を管理する仕組みのこと。

10. 小出力風力発電設備

一般用電気工作物に分類される出力 20kW 未満の風力発電設備のこと。小形風力発電設備とも呼ばれる。

11. 小出力風力発電設備等

小出力風力発電設備及び設備に付随する PCS、出力制御ユニット、通信装置等のこと。

12. 小出力発電設備

出力 50kW 未満の太陽電発電設備、出力 20kW 未満の風力発電設備、出力 20kW 未満の水力発電設備（ダムを伴うものを除く）、出力 10kW 未満の内燃力を原動力とする火力発電設備、出力 10kW 未満の燃料電池発電設備のこと。

13. 脆弱性

一つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点のこと。[JIS Q 27000:2019]

14. 他ネットワーク

電力制御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こと。具体的には，組織内の事務処理に用いられるネットワーク等を指す。

15. DMZ

Demilitarized Zone の略で、外部ネットワークからの攻撃より、組織内部のネットワークを保護する緩衝地帯のこと。

16. ファイアウォール

ネットワークの結節点となる場所に設置し、ネットワークの通信をさせるかどうかを判断し、許可又は拒否するシステム・装置のこと。

17. PSIRT

Product Security Incident Response Team の略で、自社で製造・開発する製品やサービスを対象に、セキュリティレベルの向上やインシデント発生時の対応を行う組織のこと。

18. VPN

Virtual Private Network の略で、インターネットや通信事業者の独自ネットワーク上に構築する仮想の専用線のこと。

19. VPP

Virtual Power Plant の略で、需要家側のエネルギーリソース、電力系統に直接接続されている発電設備、蓄電設備の保有者もしくは第三者が、そのエネルギーリソースを制御（需要家側エネルギーリソースからの逆潮流も含む）することで、発電所と同等の機能を提供すること。

20. 不正アクセス

本来アクセス権限を持たない者が、システムの内部へ侵入を行う行為のこと。

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、ボットなどの悪意を持ったプログラムを指す総称のこと。これらのプログラムは、使用者や管理者の意図に反して（あるいは気づかぬうちに）コンピュータに入り込み悪意ある行為を行う。

22. リスク

目的に対する不確かさの影響のこと。[JIS Q 27000:2019]