自家用電気工作物の
サイバーセキュリティ対策

独立行政法人　製品評価技術基盤機構
国際評価技術本部電力安全センター
村上　工

NITEの紹介

NITEの事業案内

NITEは、「独立行政法人製品評価技術基盤機構法」に基づき、経済産業省のもとに設置されている行政執行法人です。

現在、製品安全分野、化学物質管理分野、バイオテクノロジー分野、適合性認定分野、国際評価技術分野の5つの分野において、経済産業省など関係省庁と密接な連携のもと、各種法令や政策における技術的な評価や審査などを実施し、わが国の産業を支えています。

また、それらの業務を通じてNITEに蓄積された知見やデータなどを広く産業界や国民の皆様に提供するとともに、諸外国との連携強化や国際的なルールづくりなどに取り組み、イノベーションの促進や世界レベルでの安全な社会の実現に貢献しています。

電力安全センター

https://www.nite.go.jp/

- ガイドライン制定の経緯
- ガイドラインの対象範囲について
- 要求事項への対応方法
- サイバーセキュリティ確保に関する自主点検の勧め

ガイドライン制定の経緯

自家用電気工作物向けのサイバーセキュリティガイドラインについて

<table>
<tr><th colspan="2">電気事業の区分</th><th>電気工作物の区分</th><th>遵守するガイドライン</th></tr>
<tr><td colspan="2">一般送配電事業</td><td rowspan="3">電気事業法第38条第３項各号に掲げる事業の用に供する電気工作物
（大手発電事業を含む）</td><td rowspan="3">電力制御システムセキュリティガイドライン
（日本電気技術規格委員会/JESC）</td></tr>
<tr><td colspan="2">送電事業</td></tr>
<tr><td colspan="2">特定送配電事業</td></tr>
<tr><td rowspan="2">発電事業</td><td>200万kW以上</td><td rowspan="3">自家用電気工作物
（中小発電事業を含む）</td><td rowspan="2">電力制御システムセキュリティガイドライン
（JESC）</td></tr>
<tr><td>200万kw未満</td></tr>
<tr><td colspan="2">（該当なし）</td><td>自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン（内規）</td></tr>
<tr><td colspan="2">【参考】</td><td>小規模事業用電気工作物
・太陽電池発電設備
（10kW以上50kW未満）
・風力発電設備（20kW未満）</td><td>対象外</td></tr>
</table>

自家用電気工作物のサイバーセキュリティ確保について

電気設備に関する技術基準
（サイバーセキュリティの確保）
第十五条の二

事業用電気工作物（小規模事業用電気工作物を除く。）の運転を管理する電子計算機は、当該電気工作物が人体に危害を及ぼし、又は物件に損傷を与えるおそれ及び一般送配電事業又は配電事業に係る電気の供給に著しい支障を及ぼすおそれがないよう、サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）を確保しなければならない。

https://elaws.e-gov.go.jp/document?lawid=409M50000400052

電気設備の技術基準の解釈
【サイバーセキュリティの確保】（省令第15条の2）

第37条の2 省令第15条の2に規定するサイバーセキュリティの確保は、次の各号によること。

一. スマートメーターシステムにおいては、日本電気技術規格委員会規格 JESC Z0003（2019）「スマートメーターシステムセキュリティガイドライン」によること。配電事業者においても同規格に準じること。

二. 電力制御システムにおいては、日本電気技術規格委員会規格 JESC Z0004（2019）「電力制御システムセキュリティガイドライン」によること。配電事業者においても同規格に準じること。

三. 自家用電気工作物（発電事業の用に供するもの及び小規模事業用電気工作物を除く。）に係る遠隔監視システム及び制御システムにおいては、「自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン（内規）」（20220530保局第1号 令和4年6月10日）によること。

https://www.meti.go.jp/policy/safety_security/industrial_safety/law/files/dengikaishaku.pdf
https://www.meti.go.jp/policy/safety_security/industrial_safety/law/denjikokuji.html

ガイドライン制定の経緯

一般送配電事業、送電事業、配電事業、特定送配電事業及び発電事業の用に供する電気工作物に係るサイバーセキュリティの確保対策は平成28年度（2016年）に制定済み
【電力制御システムセキュリティガイドライン】

- 諸外国では製鉄所等の産業施設へのサイバー攻撃が発生し大規模な被害が生じていること
- 中小企業も含む今後の電気保安分野におけるスマート化の進展

令和3年11月及び令和4年1月の電力安全小委員会電気保安制度WG（第8回及び第9回）の審議を踏まえ、R4基準及びR4解釈より、電気工作物におけるサイバーセキュリティの確保義務について、自家用電気工作物を含む事業用電気工作物へ拡大することを決定し、令和4年10月より施行。

電気設備の技術基準の解釈の解説　P.58　第37条の2【サイバーセキュリティの確保】
https://www.meti.go.jp/policy/safety_security/industrial_safety/law/files/dengikaishakukaisetsu.pdf

諸外国におけるサイバー攻撃事例

- 2010年 Stuxnet：制御システムを標的とする初めてのマルウェア
- 2015年 ウクライナ 大規模停電
  2015年12月23日、ウクライナで発生した電力会社へのサイバー攻撃。様々な要因が重なった結果、大規模停電を引き起こしたとされる。発生から復旧までに最大で6時間を要し、22万5 千人の顧客に影響を与えた。

- 2016年 ウクライナ マルウェアによる停電
  2016年12月17日、ウクライナで発生した電力会社へのサイバー攻撃。マルウェアによって意図しないコマンド（ブレーカー遮断）が送信され、当該地域で最大1時間15分の停電が発生することとなった。

- 2017年 安全計装システムを標的とするマルウェア
- 2018年 半導体製造企業のランサムウェアによる操業停止
- 2019年 アルミニウム製造企業のランサムウェアによる操業停止
- 2020年 医療関連企業のランサムウェアによる業務停止
- 2021年 水道局への不正侵入と飲料水汚染未遂
- 2021年 米国最大手のパイプラインのランサムウェア被害
- 2022年 衛星通信網へのサイバー攻撃の事例
- 2022年 電力網への攻撃の事例

制御システム関連のサイバーインシデント事例
https://www.ipa.go.jp/security/controlsystem/incident.html

電気保安分野におけるスマート化の進展

- スマート保安プロモーション委員会について
  　経済産業省は、令和２年度よりスマート保安官民協議会を設置することで、官・民連携して、スマート保安技術の的確な導入促進を行うための取組を進めています。電気保安分野では、スマート保安官民協議会電力安全部会において、スマート保安技術の妥当性確認等を行う仕組みが必要とされ、「スマート保安プロモーション委員会」を設置しています。

- スマート保安技術カタログ
  　スマート保安技術カタログ（以下「技術カタログ」という）は、電気設備の新たなスマート保安技術をカタログとしてまとめたものです。 技術カタログ上に掲載されている技術は、従来の電気設備保安技術を代替できるものとして、学識経験者等から構成されるスマート保安プロモーション委員会で評価を行ったものであり、従来の保安技術を代替できるだけではなく、設備の常時監視による保安レベルの向上や、保安点検経費の削減が見込まれます。

https://www.nite.go.jp/gcet/tso/smart_hoan.html

自家用電気工作物に対するサイバー攻撃？

太陽光発電にサイバー攻撃　機器８００台を乗っ取り　身元隠し不正送金に悪用

　各地の太陽光発電施設の遠隔監視機器、計約８００台がサイバー攻撃を受け、一部がインターネットバンキングによる預金の不正送金に悪用されていたことが１日、分かった。ハッカーはネット上の身元を隠すために機器を乗っ取ったとみられ、発電施設に障害が起きる恐れもあった。セキュリティー企業によると、中国のハッカー集団が関与した可能性がある。
　電子機器メーカーのコンテック（大阪市）によると、自社が製造した遠隔監視機器が悪用された。機器はネットにつながっており、発電施設の運営会社が発電量の把握や異常の感知に使う。コンテックは機器を約１万台販売したが、令和４年時点でこのうち約８００台について、サイバー攻撃対策の欠陥があった。
　ハッカーは欠陥を突いて遠隔監視機器に侵入し、外部からの操作を可能にするプログラム「バックドア」を仕掛けた。機器を操ってネットバンキングに不正接続し、金融機関の口座からハッカー側の口座に送金して金銭を窃取していた。

共同通信　2024年5月1日
https://nordot.app/1158206853963727018

ガイドラインに基づいたセキュリティ対策を実施していれば防ぐ事ができた！

ガイドラインの対象範囲について

第１－１条　目的

自家用電気工作物の遠隔監視システム等、制御システム等のサイバーセキュリティの確保を目的とする

サイバーセキュリティとは

電子的方式により記録され、

- 漏
- 並

必要な措置

保のために

情報について、
- 安全管理のために必要な措置
- 安全性及び信頼性の確保のために必要な措置

が講じられ、その状態が適切に維持管理されていること

（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条）

↓

自家用電気工作物の機能が適切に維持管理されていること

↓

自家用電気工作物のサイバーセキュリティ

第１－１条　目的

本ガイドラインは、自家用電気工作物（発電事業の用に供するもの及び小規模事業用電気工作物を除く。以下同じ。）の遠隔監視システム等、制御システム等のサイバーセキュリティの確保を目的として、自家用電気工作物を設置する者（以下「設置者」という。）が実施すべきセキュリティ対策の要求事項について規定したものである。

本ガイドラインにおいては、求められるセキュリティ水準に応じて、条ごとに「勧告的事項」又は「推奨的事項」を表記しており、それぞれ次のように定義する。

勧告的事項：遠隔監視システム等、制御システム等に関する想定脅威に対して、
　　設置者等が実施すべきこと
推奨的事項：遠隔監視システム等、制御システム等に関する想定脅威に対して、
　　設置者等が実施の要否及び実施方法を判断すべきこと

●勧告的事項について
　系統連系先の一般送配電事業者等の系統連系技術要件にセキュリティ対策が定められており、未実施だと系統に接続することができない（ⅰ）。本ガイドラインでは、該当するセキュリティ対策を区分Aのみ勧告的事項（ⅱ）としている。

ⅰ.　https://www.meti.go.jp/shingikai/enecho/denryoku_gas/denryoku_gas/pdf/025_05_00.pdf
　　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（2020年6月11日開催）

ⅱ.　区分B、区分Cについては、各条の規定はいずれも推奨的事項としているが、区分Aについては、系統連系先の一般送配電事業者等が定める系統連系技術要件に基づき、本ガイドラインにおいて勧告的事項としているものがある。
　　（ガイドライン記載から抜粋）

【参考】系統連系技術要件　【託送供給等約款別冊】抜粋

■ サイバーセキュリティ対策

　　サイバー攻撃による発電設備の異常動作を防止し，または発電設備がサイバー攻撃を受けた場合に速やかな異常の除去，影響範囲の局限化などを行うために次のとおり，適切なサイバーセキュリティ対策を講じていただきます。

1. 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ること。
2. 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ること。
3. 発電者と当社との間で迅速かつ的確な情報連絡を行い，速やかに必要な措置を講じる必要があるため，発電設備に関し，セキュリティ管理責任者を設置するとともに，氏名及び一般加入電話番号，または携帯電話番号を通知すること。

- 一般送配電事業者全社の「系統連系技術要件　【託送供給等約款別冊】」に上記記載あり（系統連系申込書に対策済みである旨を記載する）
- 上記対策３項目がガイドラインの区分Ａの勧告的事項となっている。（区分Ｂ、Ｃでは推奨的事項）

※系統連系申込書抜粋

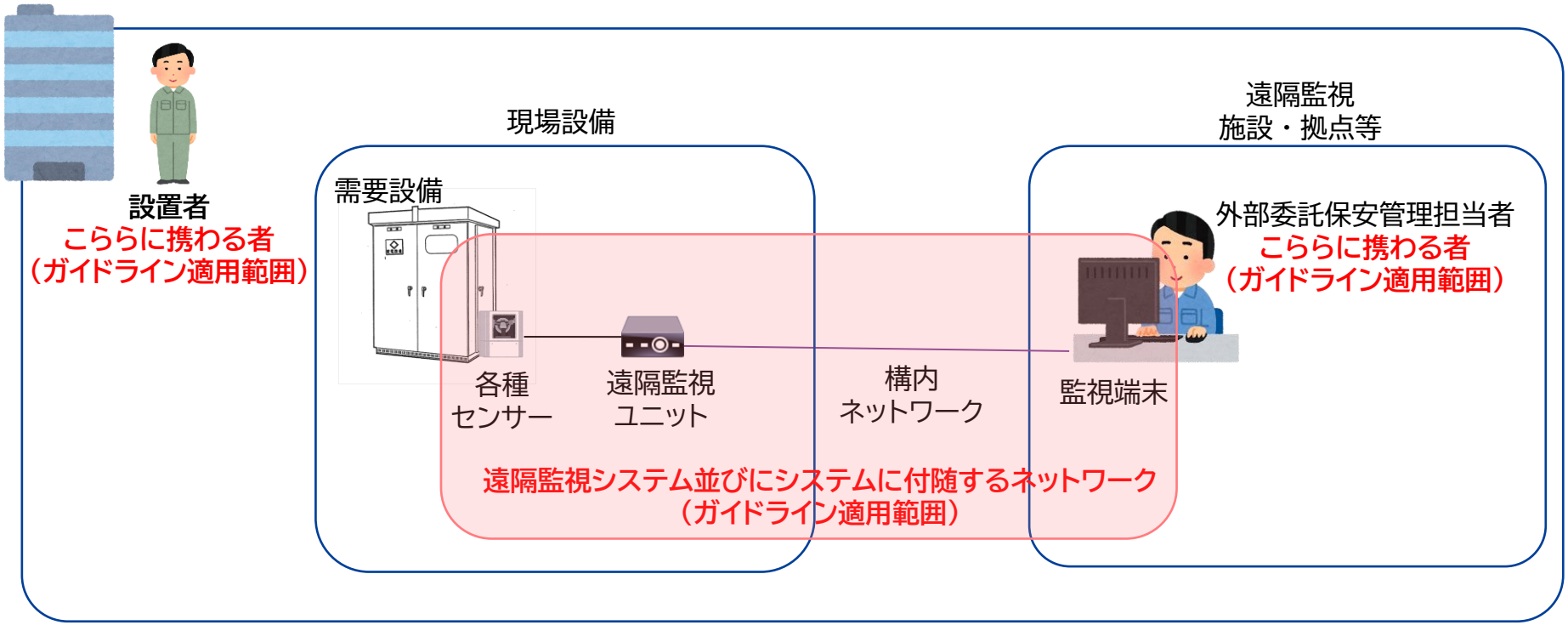
８．サイバーセキュリティ対策

【留意事項】系統連系に際して、サイバーセキュリティ対策の実施、セキュリティ管理責任者を通知いただく必要があるため、その確認をさせていただきます。

対策	☐ 系統連系技術要件に基づいた以下のサイバーセキュリティ対策を実施します。 ・発電事業の用に供する場合は、 電力制御システムセキュリティガイドラインに準拠すること。 ・発電事業の用に供さない場合は、以下の対策を講じること。 1：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 2：発電設備の制御に係るシステムへのマルウェアの侵入防止対策
セキュリティ管理責任者	☐ 様式１（６）連絡先【連絡先】の記載と同じ ☐ 様式１（６）連絡先【技術的事項に関する連絡先】の記載と同じ ☐ その他　氏名＿＿＿＿＿＿＿＿

第１－２条　適用範囲について

本ガイドラインは、設置者が施設する自家用電気工作物の遠隔監視システム及び制御システム並びにこれらのシステムに付随するネットワークを対象とし、これらに携わる者に適用する。



ガイドライン　ページ7　図3を参考に作成

第１－３条　対象となるシステムの区分

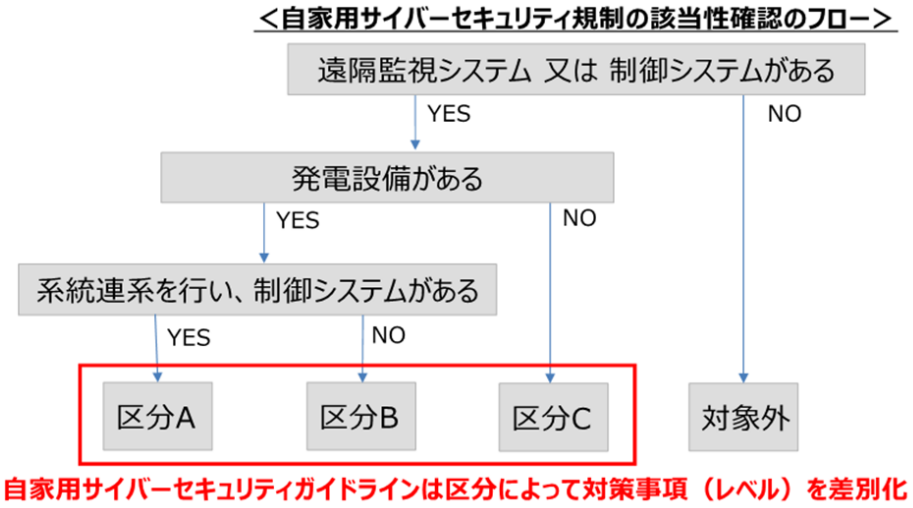
制御システム：
　自家用電気工作物の運転を制御することができるものをいう。

遠隔監視システム：
　自家用電気工作物の運転状況や構成設備の状態を、ネットワークを介して監視することができるものをいう。当該システムは、運転状況や構成設備の状態を監視するための機器を制御する機能を有する場合もあるが、発電した電気や使用するための電気の電路に施設された遮断器、開閉器の開閉操作等を行うことができないものである。

第１－３条　対象となるシステムの区分

本ガイドラインにおいて、対象となるシステムを、次のように区分する
セキュリティ事故が発生した場合の電力系統への影響及びその社会的影響の大きさから、サイバーセキュリティ対策を重視すべき度合いの指標として、発電設備が設置されているか、系統連系を行うかに基づいて判断し、区分A、区分B、区分C の順に設定

区分A	自家用電気工作物のうち系統連系する発電設備（蓄電設備を含む。）の制御システム
区分B	自家用電気工作物のうち系統連系する発電設備の遠隔監視システム並びに 自家用電気工作物のうち系統連系しない発電設備の遠隔監視システム及び制御システム
区分C	自家用電気工作物のうち発電設備以外の設備の遠隔監視システム及び制御システム



第１－４条　想定脅威

自家用電気工作物の保安の確保の妨害等を目的としたサイバー攻撃及びセキュリティに関する管理の不良を脅威として想定する。

- サイバー攻撃
  システムに対する悪意のある電子的攻撃
  （ネットワークを介した外部からの攻撃のほか、施設内部への物理的な侵入による攻撃や内部不正）

- セキュリティに関する管理の不良
  設定の不備や関係者の操作ミス（過失）

ガイドラインの対象となるシステム

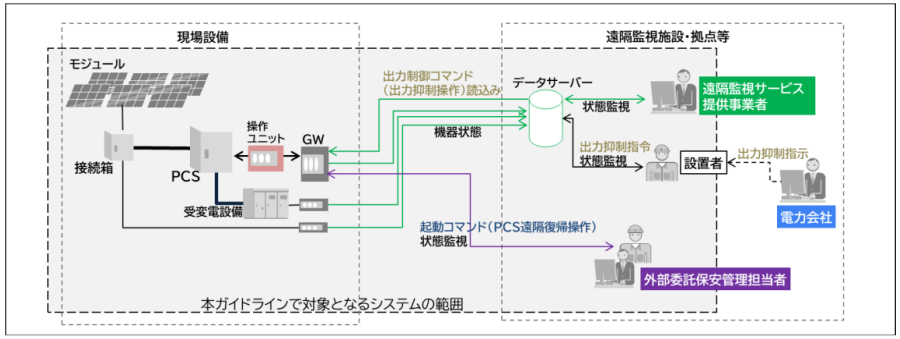
令和4年10月1日以降に新設または、変更工事が実施された既設の自家用電気工作物

- ✓ 変更の工事とは、電子計算機等（受信機、送信機、その間のネットワークなど）の変更が対象。変圧器や遮断器等の電子計算機ではない機器の取替えは対象ではない。

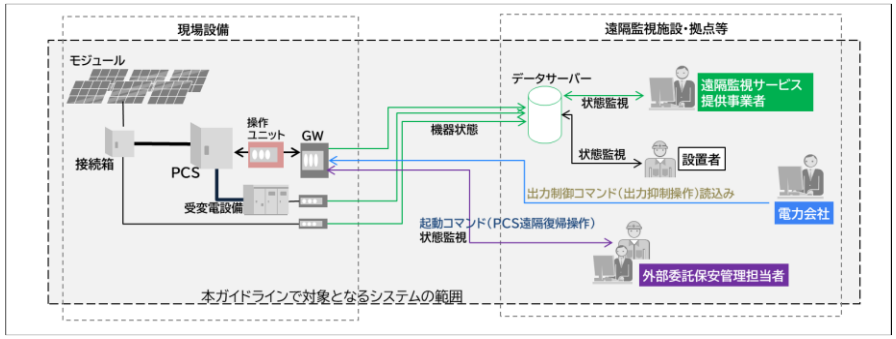
- ✓ 外部とのネットワークに接続されておらず、構内で完結しているシステムは対象となる。

  第１－５条(１５)「サイバー攻撃」において、「システムに対する悪意のある電子的攻撃（ネットワークを介した外部からの攻撃のほか、施設内部への物理的な侵入による攻撃や内部不正も含む。）をいう。」と定義されており、サイバー攻撃には、内部不正や物理的な侵入による攻撃も含まれるため

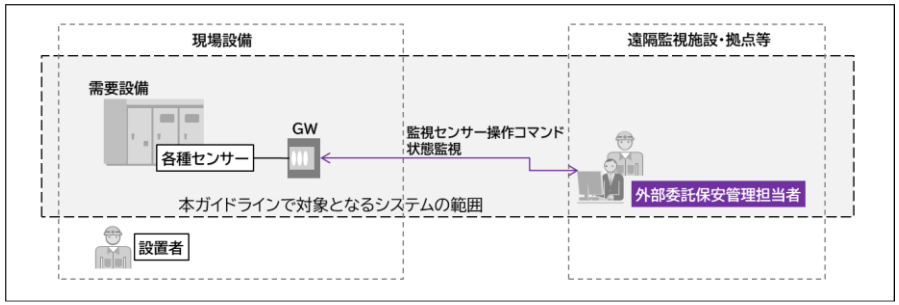
適用範囲例



発電設備の運転状況や構成設備の状態をセンサー等によって取得し、遠隔サービス提供事業者のシステムを介して設置者が遠隔の監視拠点にて監視。
また、保安管理業務の外部委託の受託者が、別のシステムを介して遠隔の監視拠点にて監視。



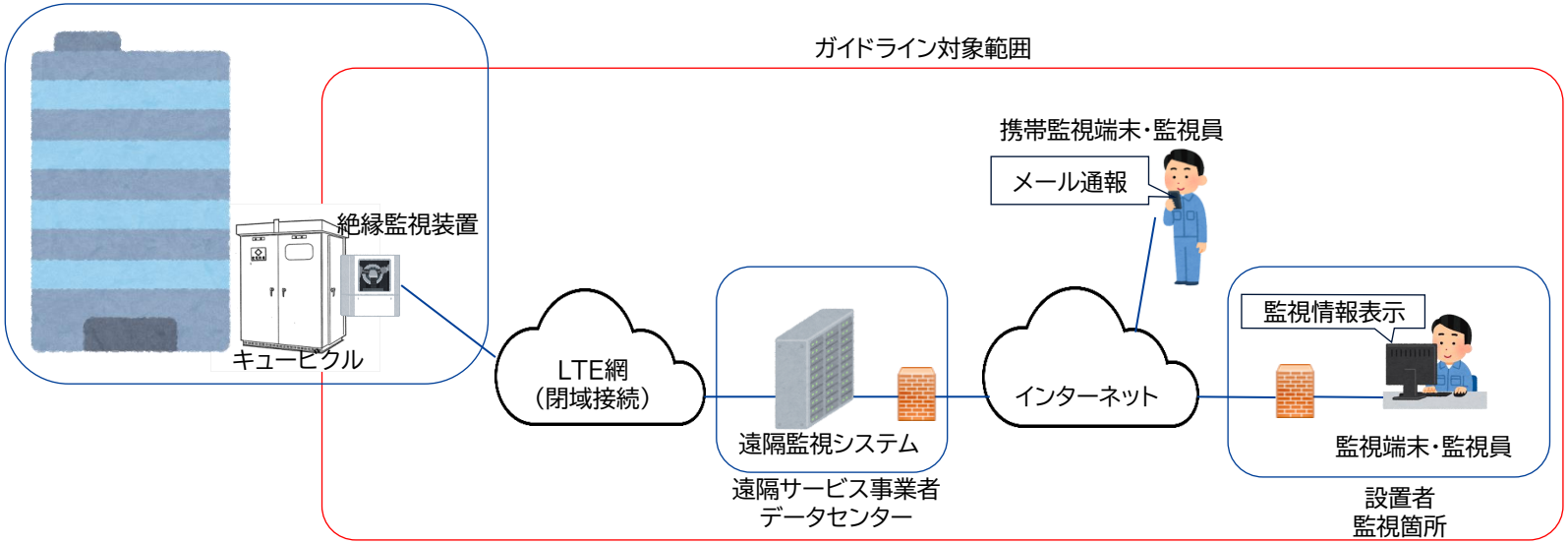
発電設備の運転状況や構成設備の状態をセンサーやカメラによって取得し、遠隔サービス提供事業者のシステムを介して設置者が遠隔の監視拠点にて監視。



遠隔監視システムのみを有している。需要設備の稼働状況や構成設備の状態をセンサーやカメラによって取得し、保安管理業務の外部委託の受託者がネットワークを介して遠隔の監視拠点にて監視。

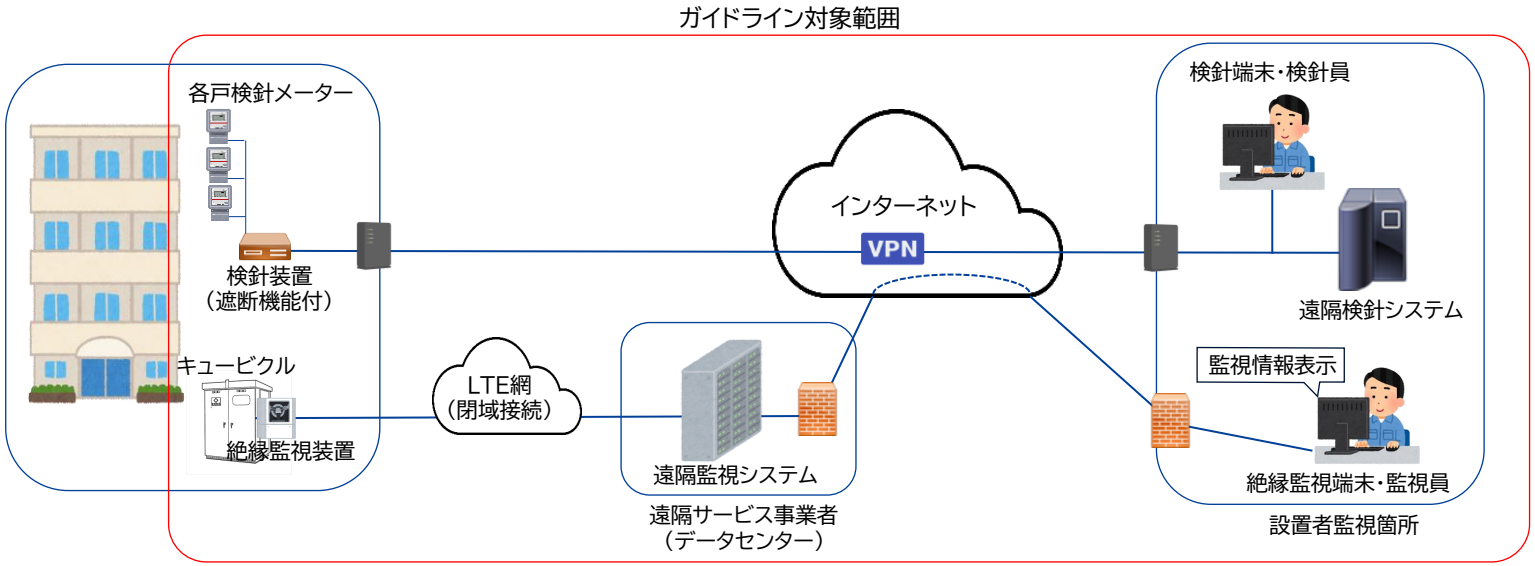
適用範囲例　需要設備（キュービクル式高圧受電設備）
発電設備以外の遠隔監視システム→区分(

- 電気主任技術者は外部委託
- キュービクルの監視は外部委託先が契約している遠隔サービス事業者のサービスを利用
- 監視方法は設置者の監視箇所および、監視員の携帯監視端末（スマートフォン）へのメール通報



適用範囲例　需要設備（高圧一括受電マンション）
発電設備以外の遠隔監視システム→区分(

- 電気主任技術者は外部委託
- キュービクルの監視は外部委託先が契約している遠隔サービス事業者のサービスを利用し実施
- 設置者の監視箇所から遠隔で監視を実施
- マンション各戸の検針は設置者が監視箇所から遠隔で実施



高圧一括受電マンションは住居部を含めた電気設備が自家用電気工作物であり、各戸の検針等に使用する設置者が設置しているスマートメーターはガイドラインの対象となる。
（電力会社等が設置するメーターは対象外）

要求事項への対応方法

時間の関係上、代表的な項目に絞りご紹介します。

自家用電気工作物のサイバーセキュリティガイドラインについて

区分A ～C に応じて、CS対策の義務(勧告的事項)と推奨(推奨的事項)に分けられており、対策事項(レベル)を基本推奨的事項とし、最低限の基準として区分Aのみ一部勧告的事項がございます。
ただし、同じ区分であっても、出力や電圧、設置環境等が異なるので、社会的影響度を加味した対策 が必要です。

そのため、まずは 攻撃を受ける可能性のある設備や想定される被害を洗い出し、それに対する対策の必要性を検討していただく必要があります。
それを踏まえて、過度な負担にならない範囲で可能なCS対策から取り組んでください。

【リーフレット】自家用電気工作物に係るサイバーセキュリティの確保に関するガイドラインの策定について
https://www.meti.go.jp/policy/safety_security/industrial_safety/oshirase/2022/07/20220706-2.pdf

サイバーセキュリティ対策のため、まず何を行うべきか

- サイバー攻撃による被害を回避し、軽減するため、具体的には、次のようなサイバーセキュリティ対策が考えられます。
  - ✓ 機器における対策
    ウィルス対策ソフトの導入及び定期的なウィルスチェック、OS 等の最新化、USBポート等の使用制限・物理的施錠など
  - ✓ 通信における対策
    ネットワークの閉域網化、ネットワークの監視（FW、IPS/IDS、WAF 等）、通信の暗号化、他ネットワークとの接続点の最小化、接続点の防御措置など
  - ✓ 運用面での対策
    アカウントの制限、アクセス端末の制限、セキュリティマニュアルの整備など
  - ✓ 物理的な対策
    セキュリティ区画の設定、アクセス管理の実施など

- サイバー攻撃による被害が生じた際、迅速に対応できるようにするため、次のようなサイバーセキュリティ対策も有効です 。
  - ✓ セキュリティ管理責任組織の設置、手順や報告先等の事前確認、組織内の体制・役割・責任・目的・対象システムの明確化、原因特定のためのアクセスログの記録、サイバー保険への加入、セキュリティ教育及び訓練、想定される被害の洗い出し及びその対策の要否 など

【リーフレット】自家用電気工作物に係るサイバーセキュリティの確保に関するガイドラインの策定について
https://www.meti.go.jp/policy/safety_security/industrial_safety/oshirase/2022/07/20220706-2.pdf

サイバー攻撃による被害が生じた際、迅速に対応できるようにするための サイバーセキュリティ対策

- 想定される被害の洗い出し及びその対策の要否の検討

✓　対策要否を検討した経緯や結果に関する記録は残す

【Q&A】自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン
https://www.meti.go.jp/policy/safety_security/industrial_safety/oshirase/2023/03/20230320-22.pdf

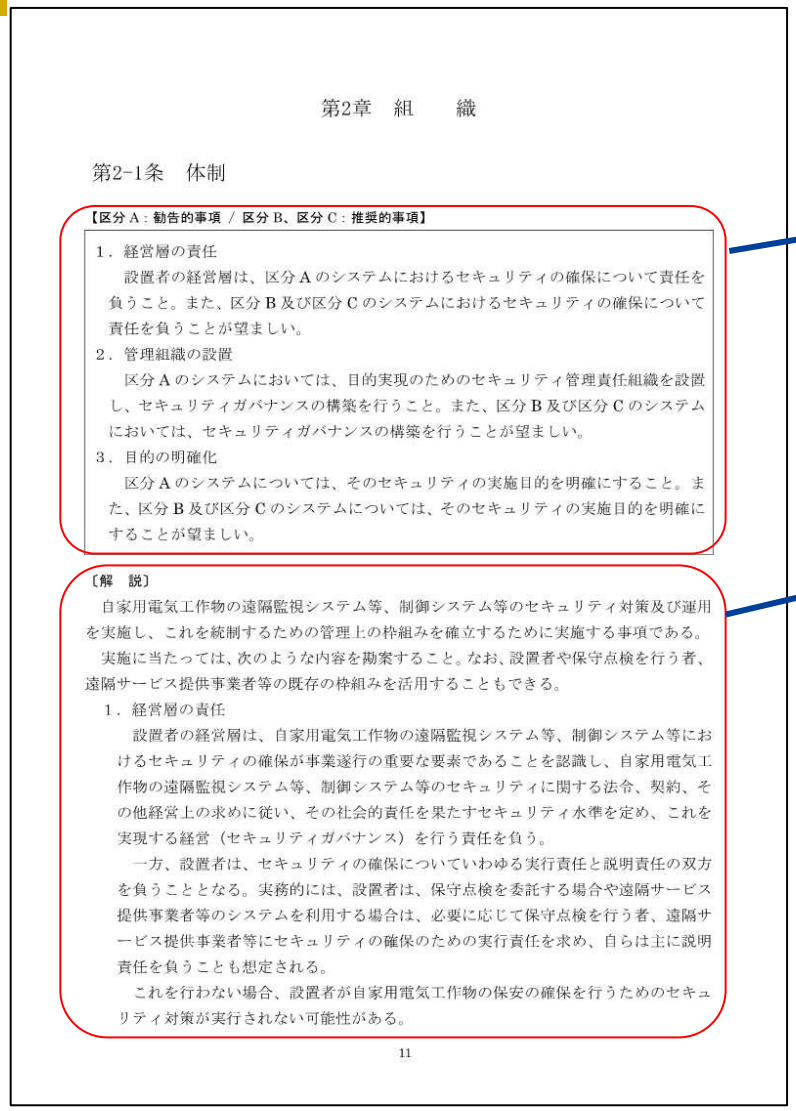
ページ10　電気設備に関する技術基準を定める省令ー技術基準違反
Q. 電技解釈等で、単に「ガイドラインによること」と規定される場合、
推奨的事項を含めて順守しなければ技術基準等の違反となり罰則の適用となるのでしょうか？

A. 自家用ＧＬの趣旨は、自家用電気工作物の遠隔監視システム等、制御システム等のサイバーセキュリティの確保を目的として、自家用電気工作物を設置する者が実施すべきセキュリティ対策の要求事項について規定したものです。そのため、サイバー攻撃を受ける可能性のある設備の洗い出しやリスクをリストアップし、社会的影響度等を考慮しながらセキュリティ対策が必要かどうかを設置者及び関係者で検討していただく必要がございます。推奨的事項については、検討した上で必要でないと判断された対策は講じていなくても技術基準違反になることはありません。

しかし、何も検討をせずに対策をしていない場合は、技術基準適合維持義務違反になる可能性がありますので、検討した際の記録は必ず残すようにしてください。

また、公衆の安全及び電力系統へ波及する事故が発生した場合若しくは、その恐れがあるにも関わらず対策を講じていない場合には、技術基準適合維持義務違反を問う可能性もございます。

自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン



第2章　組　　織

第2-1条　体制

【区分 A：勧告的事項 / 区分 B、区分 C：推奨的事項】

1．経営層の責任
　設置者の経営層は、区分 A のシステムにおけるセキュリティの確保について責任を負うこと。また、区分 B 及び区分 C のシステムにおけるセキュリティの確保について責任を負うことが望ましい。
2．管理組織の設置
　区分 A のシステムにおいては、目的実現のためのセキュリティ管理責任組織を設置し、セキュリティガバナンスの構築を行うこと。また、区分 B 及び区分 C のシステムにおいては、セキュリティガバナンスの構築を行うことが望ましい。
3．目的の明確化
　区分 A のシステムについては、そのセキュリティの実施目的を明確にすること。また、区分 B 及び区分 C のシステムについては、そのセキュリティの実施目的を明確にすることが望ましい。

〔解　説〕

自家用電気工作物の遠隔監視システム等、制御システム等のセキュリティ対策及び運用を実施し、これを統制するための管理上の枠組みを確立するために実施する事項である。

実施に当たっては、次のような内容を勘案すること。なお、設置者や保守点検を行う者、遠隔サービス提供事業者等の既存の枠組みを活用することもできる。

1．経営層の責任
　設置者の経営層は、自家用電気工作物の遠隔監視システム等、制御システム等におけるセキュリティの確保が事業遂行の重要な要素であることを認識し、自家用電気工作物の遠隔監視システム等、制御システム等のセキュリティに関する法令、契約、その他経営上の求めに従い、その社会的責任を果たすセキュリティ水準を定め、これを実現する経営（セキュリティガバナンス）を行う責任を負う。
　一方、設置者は、セキュリティの確保についていわゆる実行責任と説明責任の双方を負うこととなる。実務的には、設置者は、保守点検を委託する場合や遠隔サービス提供事業者等のシステムを利用する場合は、必要に応じて保守点検を行う者、遠隔サービス提供事業者等にセキュリティの確保のための実行責任を求め、自らは主に説明責任を負うことも想定される。
　これを行わない場合、設置者が自家用電気工作物の保安の確保を行うためのセキュリティ対策が実行されない可能性がある。

11

要求事項が記載されている。

要求事項を満たすための、具体的な実施事項が記載されている。

サイバー攻撃による被害が生じた際、迅速に対応できるようにするための サイバーセキュリティ対策

- セキュリティ管理責任組織の設置、手順や報告先等の事前確認、組織内の体制・役割・責任・目的・対象システムの明確化、原因特定のためのアクセスログの記録、サイバー保険への加入、セキュリティ教育及び訓練、想定される被害の洗い出し及びその対策の要否 など

第2-1条 体制
２．管理組織の設置
【要求事項】
目的実現のためのセキュリティ管理責任組織を設置し、セキュリティガバナンスの構築を行うこと。

【実施事項】
- 設置者は、セキュリティ管理を推進する責任主体として、セキュリティ管理責任組織を設置する。
- 保守点検を委託する場合や遠隔サービス提供事業者等のシステムを利用する場合は、自らの組織内にセキュリティ管理責任組織を設置している事業者を選択する。

サイバー攻撃による被害が生じた際、迅速に対応できるようにするための サイバーセキュリティ対策

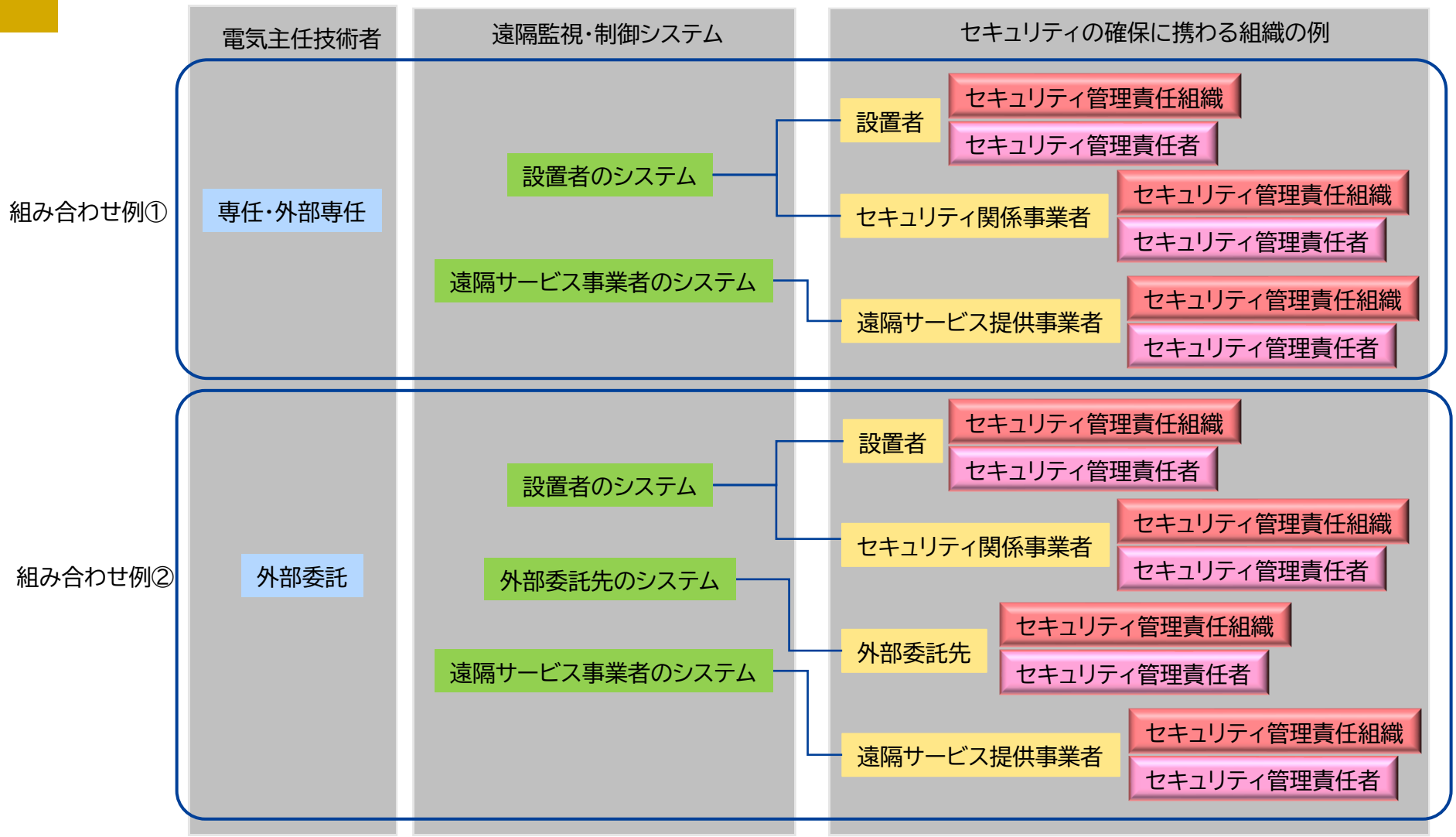
- セキュリティ管理責任組織の設置、手順や報告先等の事前確認、組織内の体制・役割・責任・目的・対象システムの明確化、原因特定のためのアクセスログの記録、サイバー保険への加入、セキュリティ教育及び訓練、想定される被害の洗い出し及びその対策の要否 など

第2-2条 役割
１．責任者の設置
【要求事項】
設置者は、システムに係るセキュリティ管理責任者を任命すること。

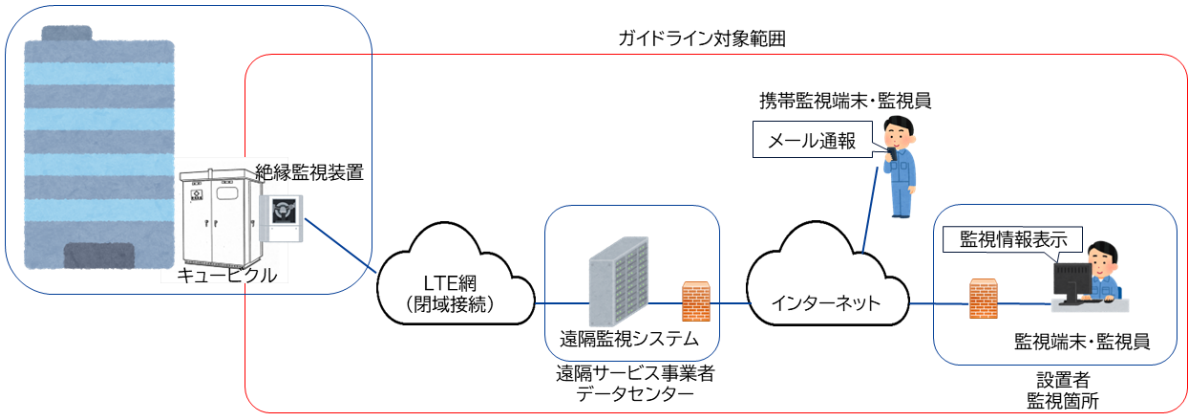
【実施事項】
- 設置者は、セキュリティ管理責任者を任命する。
- 保守点検を委託する場合や遠隔サービス提供事業者等のシステムを利用する場合、自らの組織内にセキュリティ管理責任者を任命している事業者を選択する。

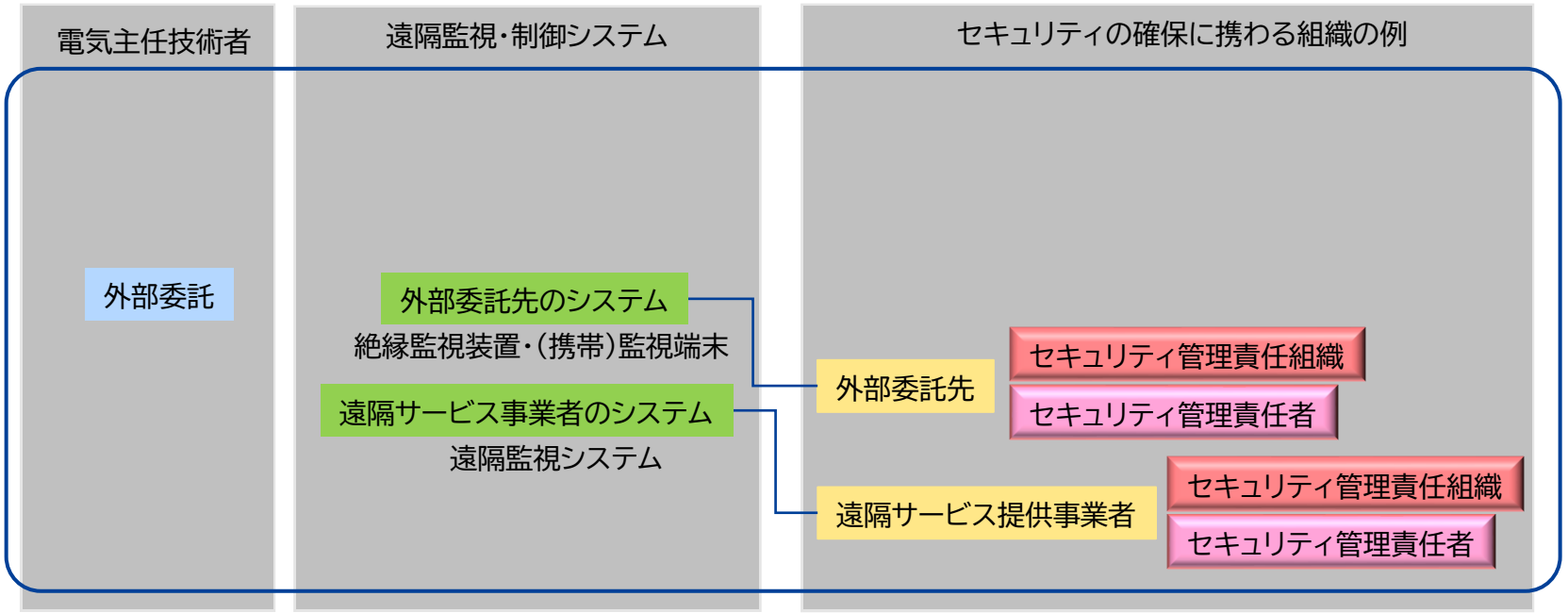
✓ セキュリティ管理責任組織／セキュリティ管理責任者は対象システムのセキュリティ管理を行う目的に設置するため、システムの所管組織に設置。
✓ システムの所管箇所が複数に分かれている場合は、それぞれの所管箇所毎に設置。

セキュリティ管理責任組織/セキュリティ管理責任者の設置イメージ



セキュリティ管理責任組織/セキュリティ管理責任者の設置イメージ





サイバー攻撃による被害が生じた際、迅速に対応できるようにするための サイバーセキュリティ対策

- セキュリティ管理責任組織の設置、手順や報告先等の事前確認、組織内の体制・役割・責任・目的・対象システムの明確化、原因特定のためのアクセスログの記録、サイバー保険への加入、セキュリティ教育及び訓練、想定される被害の洗い出し及びその対策の要否 など

第2-1条 体制
３．目的の明確化
【要求事項】
セキュリティの実施目的を明確にすること。

【実施事項】
- 設置者は、セキュリティに関する意識を明確にし、共有できるようにセキュリティの実施目的、自家用電気工作物の保安における重要性を明確にする。
- 保守点検を委託する場合や遠隔サービス提供事業者等のシステムを利用する場合、保守点検を行う者、遠隔サービス提供事業者等に対しても同様の取組の実施を求める。

サイバー攻撃による被害が生じた際、迅速に対応できるようにするための サイバーセキュリティ対策

- セキュリティ管理責任組織の設置、手順や報告先等の事前確認、組織内の体制・役割・責任・目的・対象システムの明確化、原因特定のためのアクセスログの記録、サイバー保険への加入、セキュリティ教育及び訓練、想定される被害の洗い出し及びその対策の要否 など

第2-2条 役割

２．役割の定義

【要求事項】

設置者は、自家用電気工作物の遠隔監視システム等、制御システム等に係るシステム関係者の役割を明確にすること。

【実施事項】

- 設置者は、システム関係者に対して、セキュリティに関する役割を明確にし、それぞれの役割を理解させる。
- 保守点検を委託する場合や遠隔サービス提供事業者等のシステムを利用する場合、保守点検を行う者や遠隔サービス提供事業者等のセキュリティ管理責任組織、セキュリティ管理責任者と連携、協議して、セキュリティに関するそれぞれの事業者の役割を明確にする。

サイバー攻撃による被害が生じた際、迅速に対応できるようにするためのサイバーセキュリティ対策

- セキュリティ管理責任組織の設置、手順や報告先等の事前確認、組織内の体制・役割・責任・目的・対象システムの明確化、原因特定のためのアクセスログの記録、サイバー保険への加入、セキュリティ教育及び訓練、想定される被害の洗い出し及びその対策の要否 など

第10-3条 セキュリティ事故の報告と情報共有

１．セキュリティ事故の報告

【要求事項】

セキュリティ事故が発生した場合は、対応手順に従い報告を行うことが望ましい。

【実施事項】

- セキュリティ事故を検知した場合は、対応手順に従って組織内外への報告を迅速に行う。
- 検知したセキュリティ事故を記録し、後の対応に活用できるようにする。
- 同様のセキュリティ事故が他の自家用電気工作物の遠隔監視システム等、制御システム等で発生していないかを確認し、発生状況に応じて対応する。
- セキュリティ事故の原因や対応等に関する情報は、再発防止策の検討及びセキュリティ事故対応の見直しを含めて報告する。

セキュリティ事故発生時の報告先の考え方

- セキュリティ事故全てが電気事故ではない。
- 電気事故でも、サイバー攻撃が事故原因と特定することに時間を要する場合がある。

- ✓ 一義的には第10－2条で定めた組織内のセキュリティ事故報告先（委託事業者等が対応している場合は、自組織に加え設置者）に報告を行う
- ✓ セキュリティ事故が電気事故の場合は電気関係報告規則第3条に基づく報告を行う。
- ✓ 必要に応じてIPA（独立行政法人　情報処理推進機構）に報告・相談を行う。
  ※コンピュータウイルス・不正アクセスによる被害の場合
  https://www.ipa.go.jp/security/todokede/crack-virus/about.html

サイバー攻撃による被害を回避し、軽減するためのサイバーセキュリティ対策
✓ 機器における対策

- ウィルス対策ソフトの導入及び定期的なウィルスチェック、OS 等の最新化、USBポート等の使用制限・物理的施錠など

第8-1条 システムの管理
２．機器のマルウェア対策
【要求事項】
遠隔監視システム等、制御システム等の機器について、マルウェア対策を実施すること。

【実施事項】
自家用電気工作物の遠隔監視システム等、制御システム等の機器のうち、データの授受を行う端末については、マルウェア対策を実施する。

サイバー攻撃による被害を回避し、軽減するためのサイバーセキュリティ対策
✓ 機器における対策

- ウィルス対策ソフトの導入及び定期的なウィルスチェック、OS 等の最新化、USBポート等の使用制限・物理的施錠など

第8-1条 システムの管理
３．外部記憶媒体等のマルウェア対策
【要求事項】
遠隔監視システム等、制御システム等に接続する外部記憶媒体及び可搬型の機器について、ウイルスチェックを行うこと。

【実施事項】
自家用電気工作物の遠隔監視システム等、制御システム等に接続する外部記憶媒体や可搬型の機器については、自家用電気工作物の遠隔監視システム等、制御システム等とは切り離された端末を使ってウイルスチェック等を行い、又はデータ搬送を行うシステム関係者に対して事前にウイルスチェック等を行った証跡を提出させる等の方法で異常のないことを確認する。

サイバー攻撃による被害を回避し、軽減するためのサイバーセキュリティ対策
✓ 通信における対策

- ネットワークの閉域網化、ネットワークの監視（FW、IPS/IDS、WAF 等）、通信の暗号化、他ネットワークとの接続点の最小化、接続点の防御措置など

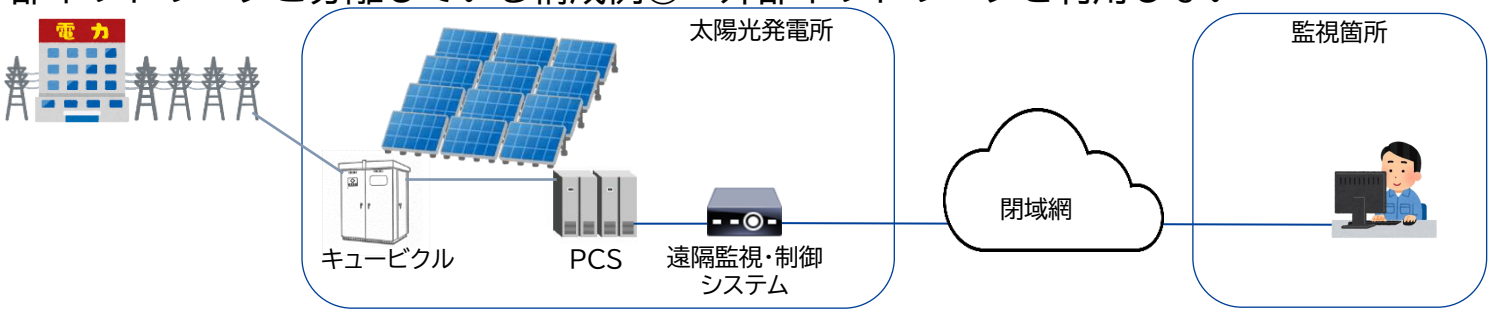
第6-2条 ネットワークの管理
1．外部ネットワークとの分離
※不特定多数が接続できる回線で接続するネットワーク

【要求事項】
遠隔監視システム等、制御システム等と外部ネットワークとは、分離すること。

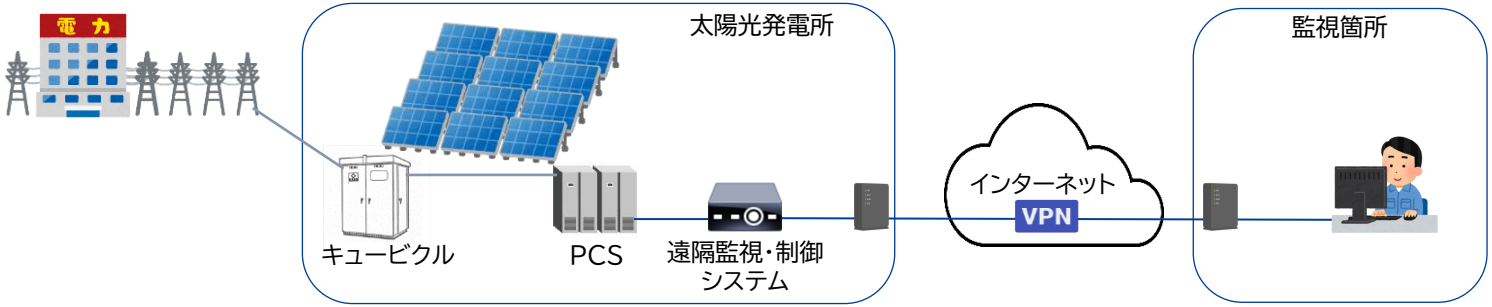
【実施事項】
- 制御システム等は、外部ネットワークと分離する。
- 遠隔監視システム等も、可能な範囲で外部ネットワークと直接接続しない。
- いずれのシステムも、外部ネットワークと接続する際には、その間に他ネットワークや別のシステム等の緩衝エリアを設けて、間接的にデータ連携を行う仕組み等を構築する。

外部ネットワークとの分離

●外部ネットワークと分離している構成例①　外部ネットワークを利用しない

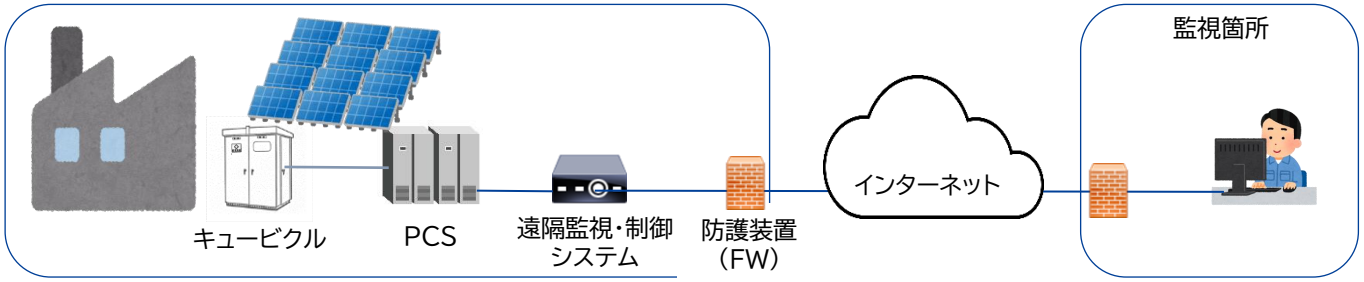


●外部ネットワークと分離している構成例②　外部ネットワーク上に仮想的な閉域網（VPN）を構築する



※VPNは『Virtual Private Network』の略。インターネット上でセキュリティを強化した通信経路（仮想専用回線）を構築する。

●外部ネットワークと直接接続しない構成例　防護装置（ファイアウォール等）を設置する



サイバー攻撃による被害を回避し、軽減するためのサイバーセキュリティ対策
✓ 通信における対策

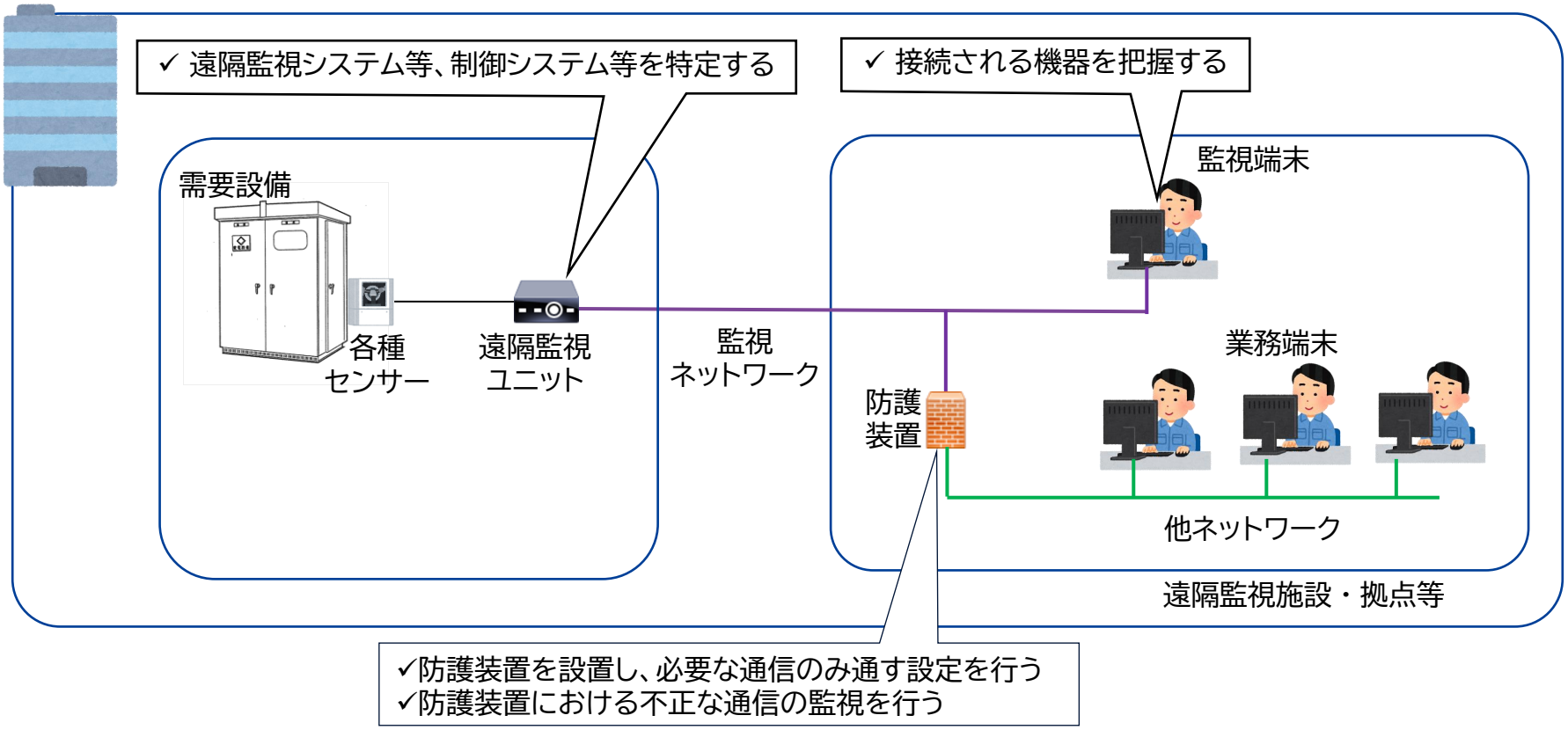
● ネットワークの閉域網化、ネットワークの監視（FW、IPS/IDS、WAF 等）、通信の暗号化、他ネットワークとの接続点の最小化、接続点の防御措置など

第6-2条 ネットワークの管理
【要求事項】
２．接続点の最小化
他ネットワークとの接続点は、最小化すること。
※遠隔監視用ネットワーク、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もの

3. 接続点の防御
他ネットワークとの接続点に防御措置を講じること。

【実施事項】
２．接続点の最小化
他ネットワークとの接続は必要最小限とした上で、他ネットワークとの接続点を有する自家用電気工作物の遠隔監視システム等、制御システム等を特定するとともに、遠隔監視用ネットワーク、制御用ネットワークに接続される機器を把握する。
３．接続点の防御
- ネットワークとの接続点に防護装置を設置し、必要な通信のみ通す設定を行う。
- 防護装置における不正な通信の監視を行う。
- なお、他の措置で目的を満たす場合はこの限りではない。

接続点の最小化・防御の構成例



サイバー攻撃による被害を回避し、軽減するためのサイバーセキュリティ対策
✓ 運用面での対策

- アカウントの制限、アクセス端末の制限、セキュリティマニュアルの整備など

第8-1条 システムの管理
１．管理者権限の適切な割当
【要求事項】
遠隔監視システム等、制御システム等における管理者権限の割当を適切に行い、不正な行為が行われない仕組みを構築すること。

【実施事項】
管理者権限の割当については、以下のとおり実施する。
a. 誰がその管理者権限を利用して業務を遂行したかを確認し、及び記録する仕組みを構築する。
b. 自家用電気工作物の遠隔監視システム等、制御システム等において管理者権限を悪用した不正行為がないことを確認する仕組みを構築する。
c. 管理者権限の割り当て状況を、定期的に確認する。

サイバー攻撃による被害を回避し、軽減するためのサイバーセキュリティ対策
✓ 物理的な対策

● セキュリティ区画の設定、アクセス管理の実施など

第9-1条 物理セキュリティ
【要求事項】
1．セキュリティ区画
セキュリティ区画を明確にし、保護対象となる施設及び区画について適切に保護すること。
2．アクセス管理
セキュリティ区画には、許可された者だけがアクセスできるようにすること。

【実施事項】
1．セキュリティ区画
- 重要な施設や機器が含まれる場所を、物理的なセキュリティ区画として設定する。
- セキュリティ区画については、システム関係者が適切に判断することができるよう、区画に応じたセキュリティの指針を策定し、適用する。

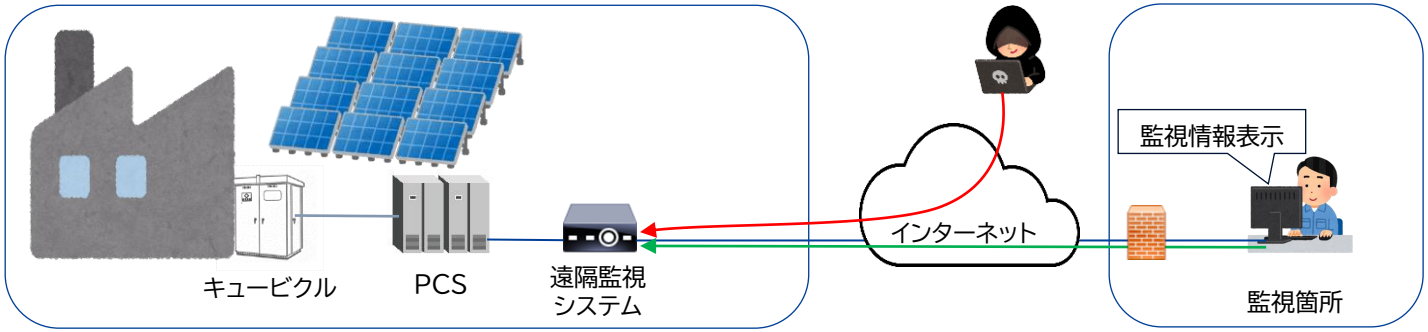
2．アクセス管理
- セキュリティ区画には、許可された者だけがアクセスできるようにする。

太陽光発電施設向け当社遠隔監視機器へのサイバー攻撃報道について

一部報道機関より当社の太陽光発電施設向け遠隔監視機器がサイバー攻撃を受け、一部の機器が悪用されたとの報道があり、お客様ならびに関係者の皆様には大変ご心配をおかけしましたことを深くお詫び申し上げます。

1. サイバー攻撃の概要
   悪意あるハッカーが当社の太陽光発電施設向け遠隔監視機器（SolarView Compact）の脆弱性を突き、当社が推奨する対策を行っていない一部の機器に不正中継を実施できるバックドア※を設置、機器が悪用されうる状況にありました。
   ※バックドアとは、コンピューターへ不正に侵入するための入り口のこと

2024/05/07　コンテック社プレスリリースより
https://www.contec.com/jp/info/2024/2024050700/



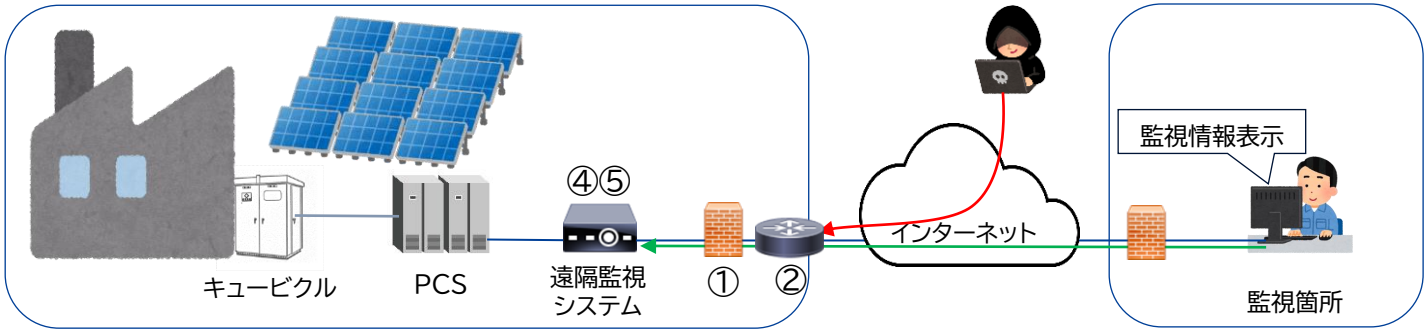
メーカー推奨恒久対策とガイドラインの要求事項の関連について

公開日 2023年07月18日　株式会社コンテック
インターネットからのSolarView Compactへの不正アクセスの影響について

■恒久的な対策
インターネットから閲覧可能な機器は常に不正アクセスされるリスクがあります。
このリスクに対応する為に下記の実施を強く推奨します。

①本製品のネットワークの上流側にファイアウォールを設置する	→第6-2条　1. 外部ネットワークの分離
②本製品のネットワークの上流側のルータにて接続可能なIPアドレスを制限する	→第6-2条　4. 接続制御
③本製品のネットワークアクセスを信頼できる閉域網で構成する	→第6-2条　1. 外部ネットワークの分離
④本製品のソフトウェアを常に最新のものにする	→第8-4条　ぜい弱性の管理
⑤本製品のパスワードを定期的に更新する	→要求事項ではないが、一般的に推奨

https://www.contec.com/jp/api/downloadlogger?download=/-/media/Contec/jp/support/security-info/contec_security_solarview_230718_jp.pdf



サイバーセキュリティ確保に関する自主点検の勧め

自主点検の勧め

			要求事項	実施事項	実施状況	○、×、対象外を選択した根拠を記載
第6章 通信のセキュリティ						
第6－2条	ネットワークの管理	①外部ネットワークとの分離	遠隔監視システム等、制御システム等と外部ネットワークとは、分離している	制御システム等は、外部ネットワークと分離している	対象外	制御装置がないため。
				遠隔監視システム等も、可能な範囲で外部ネットワークと直接接続していない	○	遠隔監視装置への操作はクラウドサービスを用いて行っているが、遠隔監視装置とクラウドサービス間は携帯電話事業者の閉域網サービスにて接続している。
				いずれのシステムも、外部ネットワークと接続する際には、その間に他ネットワークや別のシステム等の緩衝エリアを設けて、間接的にデータ連携を行う仕組み等を構築している	対象外	閉域網接続のため。
		②接続点の最小化	他ネットワークとの接続点は、最小化している 【区分A:勧告的事項】	他ネットワークからの脅威を防ぐために、組織全体のネットワーク構成を把握し、接続の有無や想定される攻撃ルートを把握している	対象外	他ネットワークと接続を行っていないため。
				他ネットワークとの接続は必要最小限とした上で、他ネットワークとの接続点を有する自家用電気工作物の遠隔監視システム等、制御システム等を特定するとともに、遠隔監視用ネットワーク、制御用ネットワークに接続される機器を把握している	対象外	他ネットワークと接続を行っていないため。
		③接続点の防御	他ネットワークとの接続点に防御措置を講じている 【区分A:勧告的事項】	ネットワークとの接続点に防護装置を設置し、必要な通信のみ通す設定を行っている	対象外	他ネットワークと接続を行っていないため。
				防護装置における不正な通信の監視を行っている	対象外	他ネットワークと接続を行っていないため。
		④接続制御	予め許可された機器以外の接続を許可しない仕組みを講じている	許可された機器を管理し、許可されていない機器からの通信は遮断している	対象外	遠隔監視装置以外の機器が接続できない構成のため。
		⑤認証	通信相手が予め許可された機器であることを確認する仕組みを講じている	必要に応じて、認証を必要とする機器と範囲を予め定め、その内容に従って機器を識別し、認証している	×	システム仕様で機能が存在しないため。 クラウドサービスで利用者認証を実施している。
		⑥ネットワーク分割	遠隔監視システム等、制御システム等内において、利用目的等に応じてネットワークを分割している	損害の拡大防止の観点から、利用目的に応じてシステム単位等により遠隔監視用ネットワーク及び制御用ネットワークを分割している	対象外	遠隔監視装置のみのため。
			【保守点検を委託し、委託先が所有する遠隔監視システム、制御システムを利用している場合や遠隔サービス提供事業者等のシステムを利用している場合】 保守点検を行う者や遠隔サービス提供事業者等が、要求事項１～６を実施していることを確認している、又は委託契約等によって担保している		○	遠隔監視装置は外部委託事業者所管だが、実施状況は上記に記載。

ご静聴頂きありがとうございます。