自家用電気工作物の
サイバーセキュリティ対策について

ガイドラインの概要と立入検査（セキュリティ監査）の視点から見た課題

2025年5月9日
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
情報処理安全確保支援士
第021683号

- 事業用の電気工作物（発電、蓄電、変電、送電、配電又は電気の使用のために設置する工作物）に対するセキュリティ対策は、電気事業の用に供する電気工作物については「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規格）、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。）については「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）」として定められています。

- 両ガイドラインはJISQ27001を基準とし、電力制御システムの利用環境を踏まえ、電力の保安と運用を考慮した内容となっていますが、電気工作物の設置者がITやセキュリティの専門家ではないことから、要求事項への対応に苦労している実態があります。

- 本講演では、ガイドラインの内容について監査視点から見た課題を踏まえご紹介します。

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。

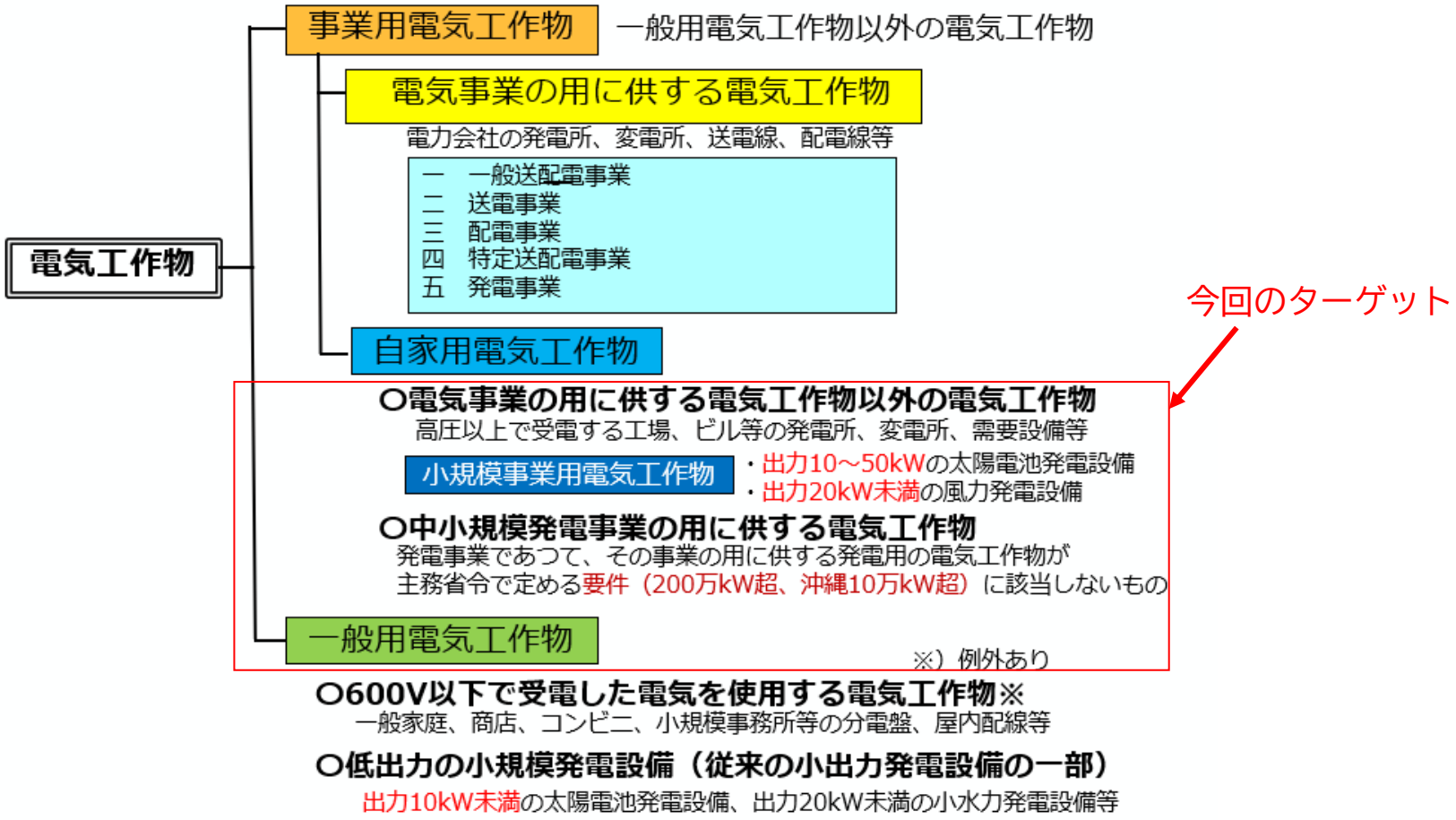
電力安全センター

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

サイバーセキュリティガイドラインの位置づけについて

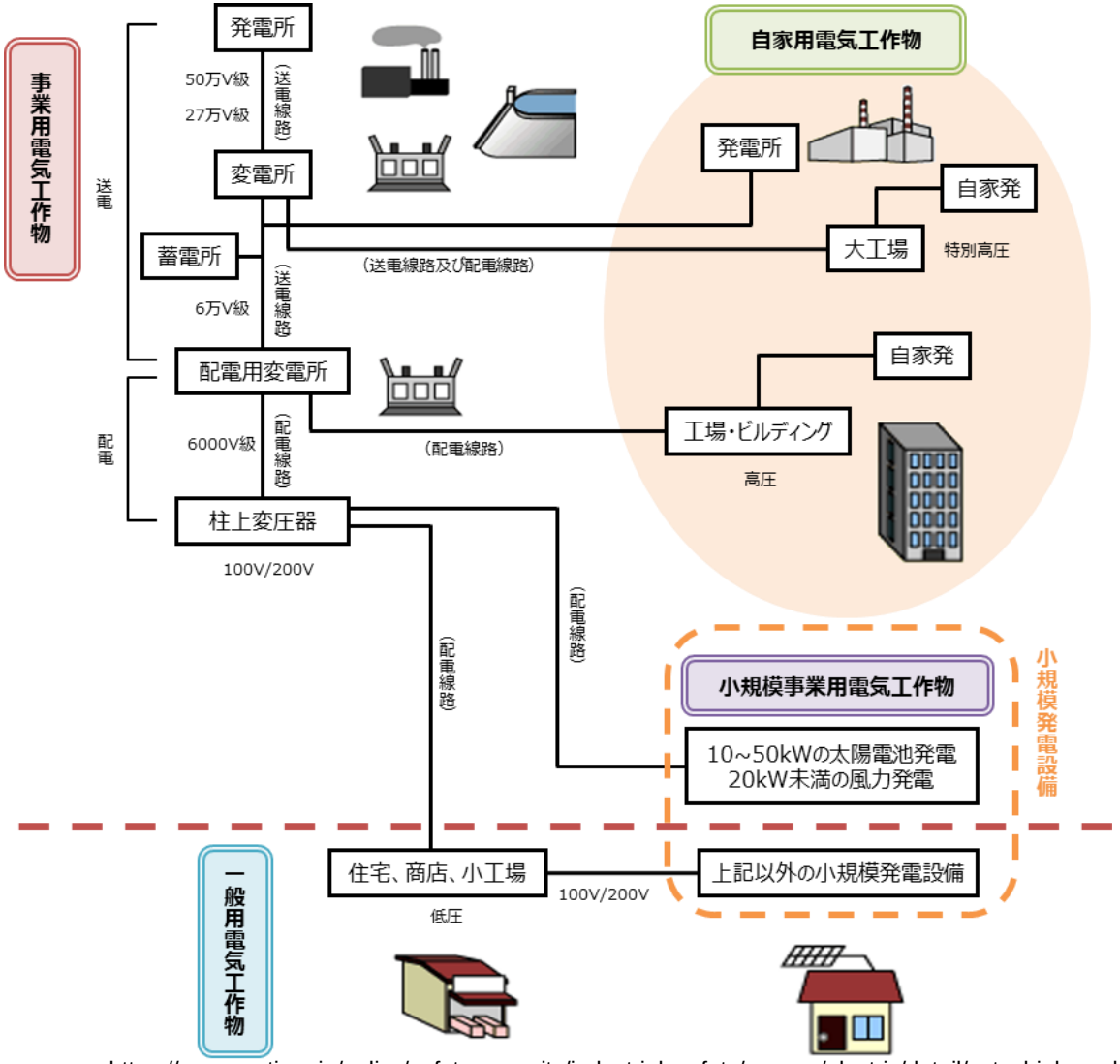
電気工作物について

発電、蓄電、変電、送電、配電又は電気の使用のために設置する工作物
（機械、器具、ダム、水路、貯水池、電線路等）



https://www.meti.go.jp/policy/safety_security/industrial_safety/sangyo/electric/detail/setsubi_hoan.html

電気工作物について



https://www.meti.go.jp/policy/safety_security/industrial_safety/sangyo/electric/detail/setsubi_hoan.html

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

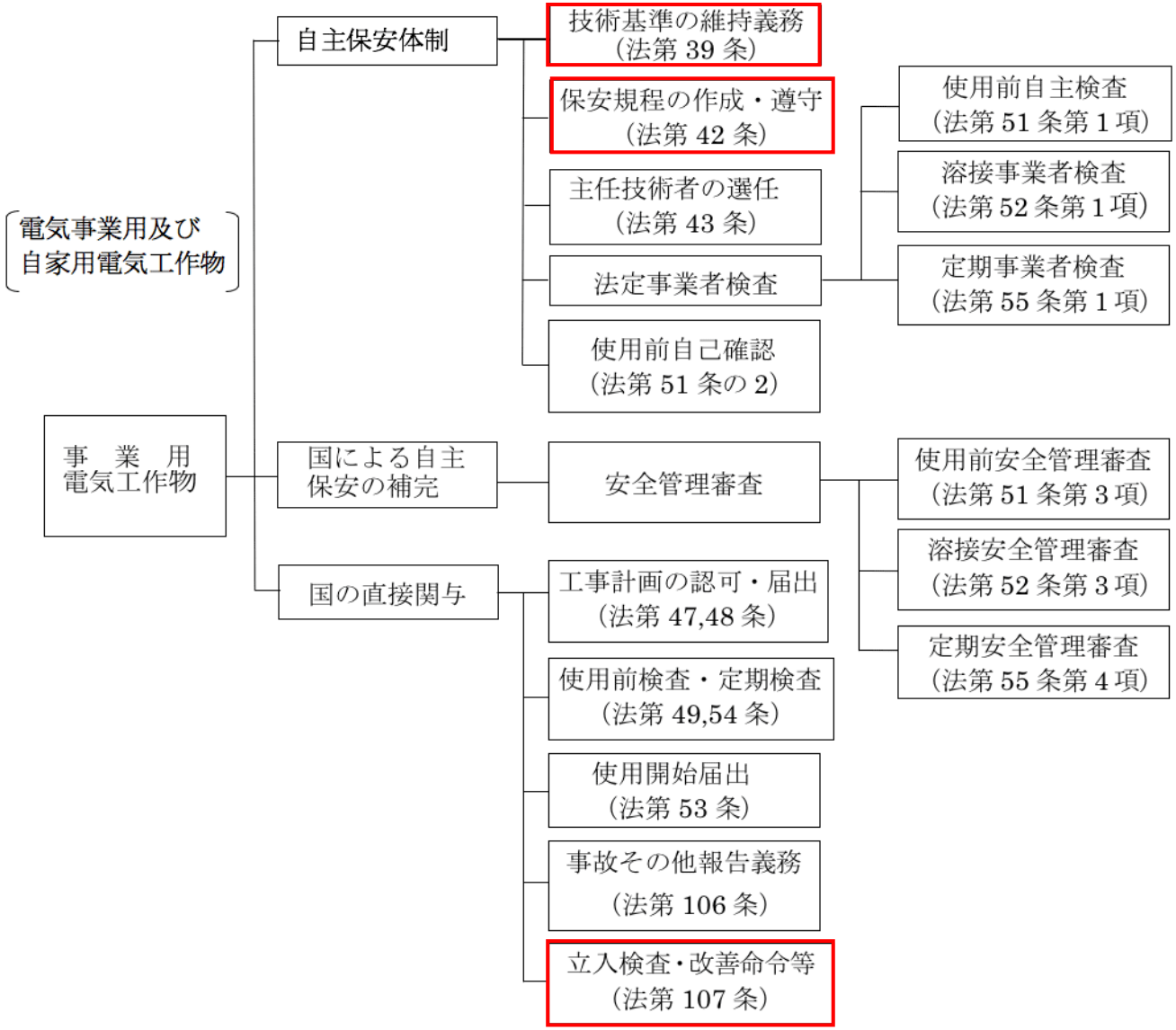
電気事業の区分		電気工作物の区分	遵守するガイドライン
一般送配電事業		電気事業法第38条第３項各号に掲げる事業の用に供する電気工作物（大手発電事業を含む）	電力制御システムセキュリティガイドライン（日本電気技術規格委員会/JESC）
送電事業			
特定送配電事業			
発電事業	200万kW以上		
	200万kw未満	自家用電気工作物（中小発電事業を含む）	電力制御システムセキュリティガイドライン（日本電気技術規格委員会/JESC）
（該当なし）			自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン（内規）
【参考】		小規模事業用電気工作物 ・太陽電池発電設備（10kW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

●電力制御システムセキュリティガイドライン
https://store.denki.or.jp/products/detail/702

●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/law/files/jikayouguideline.pdf

電気事業法　告示・内規等
https://www.meti.go.jp/policy/safety_security/industrial_safety/law/denjikokuji.html

事業用電気工作物の保安確保の概要について



事業用電気工作物にはサイバーセキュリティの確保義務について

- 発電事業の用に供する事業用電気工作物（発電事業者）は平成28年（2016年）9月24日より（※）
- 自家用電気工作物（発電事業の用に供する物は除く）は令和4（2022）年10月1日より（※）

※新設または、変更工事が実施された既設の事業用電気工作物が対象。
変更工事は電子計算機等（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。

○事業用電気工作物のサイバーセキュリティ確保について

電気事業法（令和６年４月１日施行）
第３章　電気工作物／第２節　事業用電気工作物／第１款　技術基準への適合
第３９条（事業用電気工作物の維持）
　事業用電気工作物を設置する者は、事業用電気工作物を主務省令で定める技術基準に適合するように維持しなければならない。

電気設備に関する技術基準を定める省令（令和５年３月２０日施行）
第１章　総則／第３節　保安原則／第２款　異常の予防及び保護対策
第１５条の２（サイバーセキュリティの確保）
　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。

電気設備の技術基準の解釈（令和５年１２月２６日改正）
第１章 総則／第５節 過電流、地絡及び異常電圧に対する保護対策
【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。

○自主的な保安におけるサイバーセキュリティ確保の対応について

電気事業法施行規則(令和６年４月１日施行)
第３章　電気工作物―第二節　事業用電気工作物―第二款　自主的な保安
（保安規程）第５０条
1.法第４２条第１項の保安規程は、次の各号に掲げる事業用電気工作物の種類ごとに定めるものとする。
①事業用電気工作物であって、一般送配電事業、送電事業、配電事業又は発電事業（法第三十八条第四項第五号に掲げる事業に限る。次項において同じ。）の用に供するもの
②事業用電気工作物であって、前号に掲げるもの以外のもの

3.第一項第二号に掲げる事業用電気工作物を設置する者は、法第四十二条第一項の保安規程において、次の各号に　掲げる事項を定めるものとする。
⑨その他事業用電気工作物の工事、維持及び運用に関する保安に関し必要な事項

電気事業法施行規則第５０条第３項第９号の解釈適用に当たっての考え方（内規）
（令和５年３月２０日）
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２６年法律第１０４号）第２条に規定するサイバーセキュリティをいう。）を確保するため、次に掲げる事業用電気工作物の種類ごとにそれぞれに定められたところにより適切な措置が講じられることが必要である。また、次に掲げるもののほか、事業用電気工作物の工事、維持及び運用に関する保安を行う上で設置者の判断により必要となるものについて記載することが必要である。

１．特定送配電事業又は発電事業の用に供する事業用電気工作物
①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。
②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。
２．自家用電気工作物
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）」（令和４年６月１０日付け２０２２０５３０保局第１号）によること。

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

（本資料では「自家用電気工作物ガイドライン」と表記します）

- 自家用電気工作物セキュリティガイドラインの内容は電力制御システムセキュリティガイドライン（本資料では「電制ガイドライン」と表記）の内容を引用し、自家用電気工作物の実態を踏まえたものとして策定

- 電制ガイドラインは、JIS Q 27001:2013をベースとし電力制御システムの利用環境を踏まえた内容として、電力の保安と運用を考慮し制定

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

カテゴリ	章	規定項目	カテゴリ	章	規定項目
ー	1 総則		ー	6 通信のセキュリティ	
総則	1-1	目的	技術	6-1	暗号化・通信プロトコルの最適化
総則	1-2	適用範囲	技術	6-2	ネットワークの管理
総則	1-3	対象となるシステムの区分	ー		
総則	1-4	想定脅威	技術	7-1	システムのセキュリティ
総則	1-5	用語の定義	ー	8 運用のセキュリティ	
ー	2 組織		技術	8-1	システムの管理
組織	2-1	体制	物理	8-2	機器・外部記憶媒体の管理
組織	2-2	役割	技術	8-3	データの管理
人	2-3	セキュリティ教育	技術	8-4	脆弱性の管理
ー	3 文書化		ー	9 物理セキュリティ	
組織	3-1	文書管理	物理	9-1	物理セキュリティ
組織	3-2	実施状況の報告	ー	10 セキュリティ事故の対応	
	4 セキュリティ管理		組織	10-1	情報の収集
ISMS	4-1	セキュリティ管理	組織	10-2	セキュリティ事故の対応体制等
ー	5 機器のセキュリティ		組織	10-3	セキュリティ事故の報告と情報共有
技術	5-1	セキュリティ仕様の確認	組織	10-4	周知と訓練
物理	5-2	機器の取り扱い			

JIS Q 27002:2024の管理策カテゴリ（組織的管理策、人的管理策、物理的管理策、技術的管理策）

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）

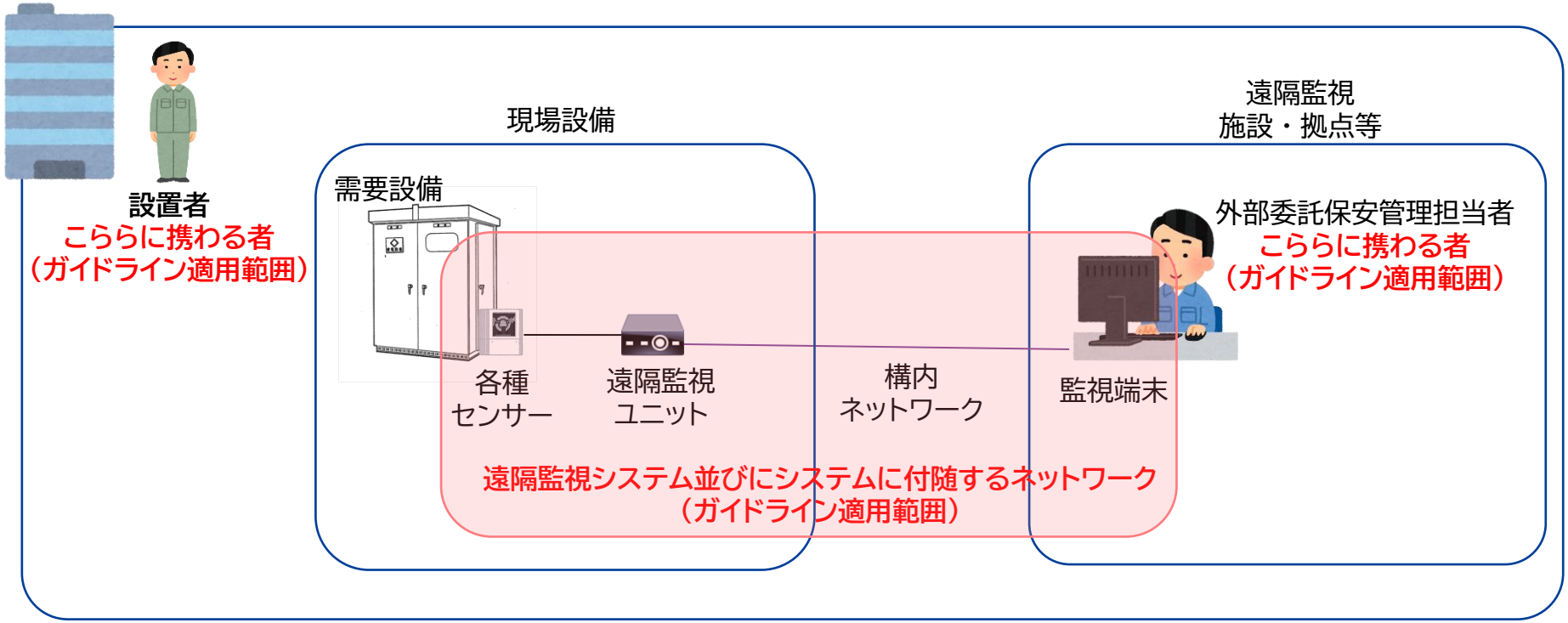
【参考】勧告的事項について（区分A）

自家用電気工作物の遠隔監視システム等、制御システム等に関する想定脅威に対して

	設置者等が実施すべき事項	設置者等が実施の要否および実施方法を判断すべき事項	
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	勧告的事項	推奨的事項	主な記載内容
第１章　総則			
第２章　組織	4	4	セキュリティ管理体制
第３章　文書化	0	3	セキュリティに関する情報の取り扱い
第４章　セキュリティ管理	0	1	セキュリティ管理体制
第５章　機器のセキュリティ	0	5	セキュリティ確保の技術的対策
第６章　通信のセキュリティ	2	5	セキュリティ確保の運用・物理的対策
第７章　システムのセキュリティ	0	2	セキュリティ確保の技術的対策
第８章　運用のセキュリティ	1	6	セキュリティ確保の運用的対策
第９章　物理セキュリティ	0	2	セキュリティ確保の物理的対策
第10章　セキュリティ事故の対応	0	4	セキュリティ事故対応の体制

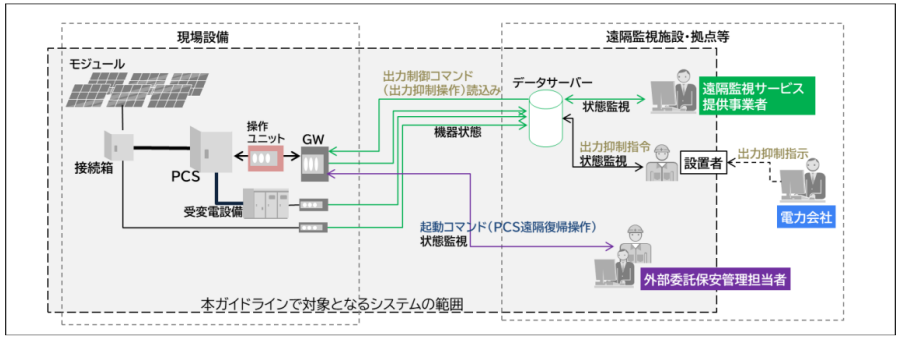
第１－２条　適用範囲について

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。

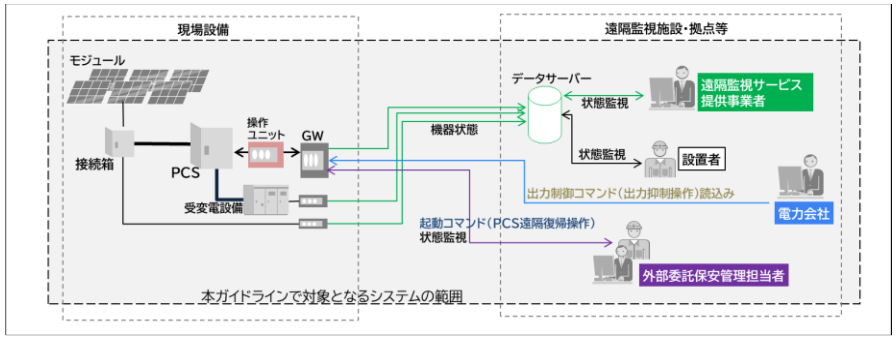


ガイドライン　ページ7　図3を参考に作成

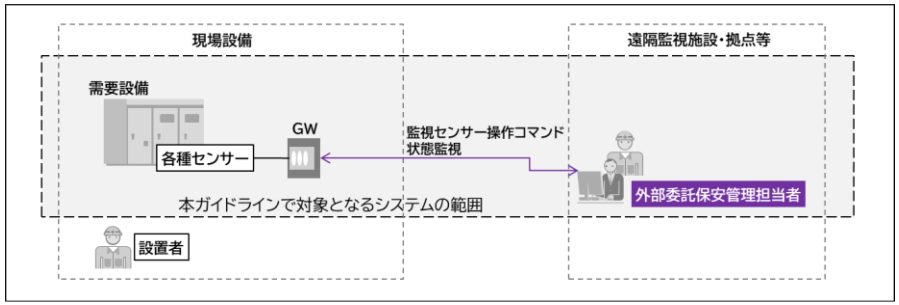
適用範囲例



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。

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。

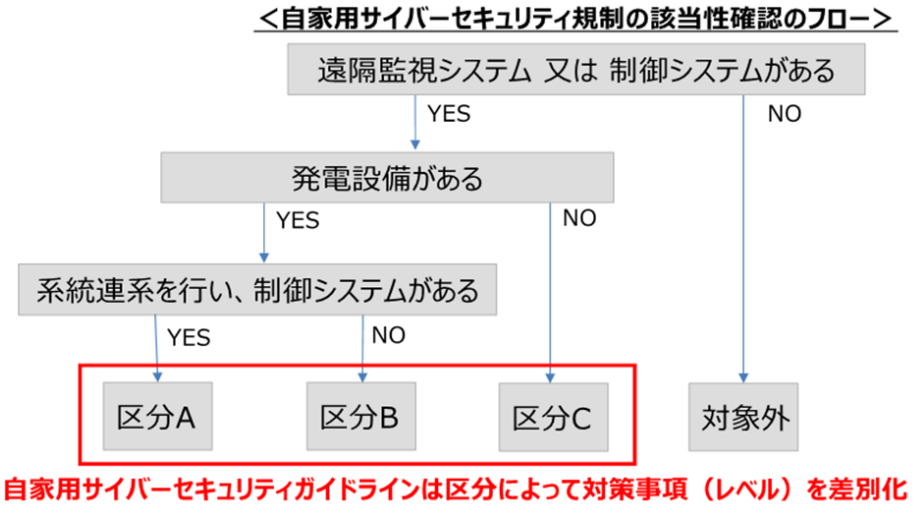
遠隔監視システム：

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



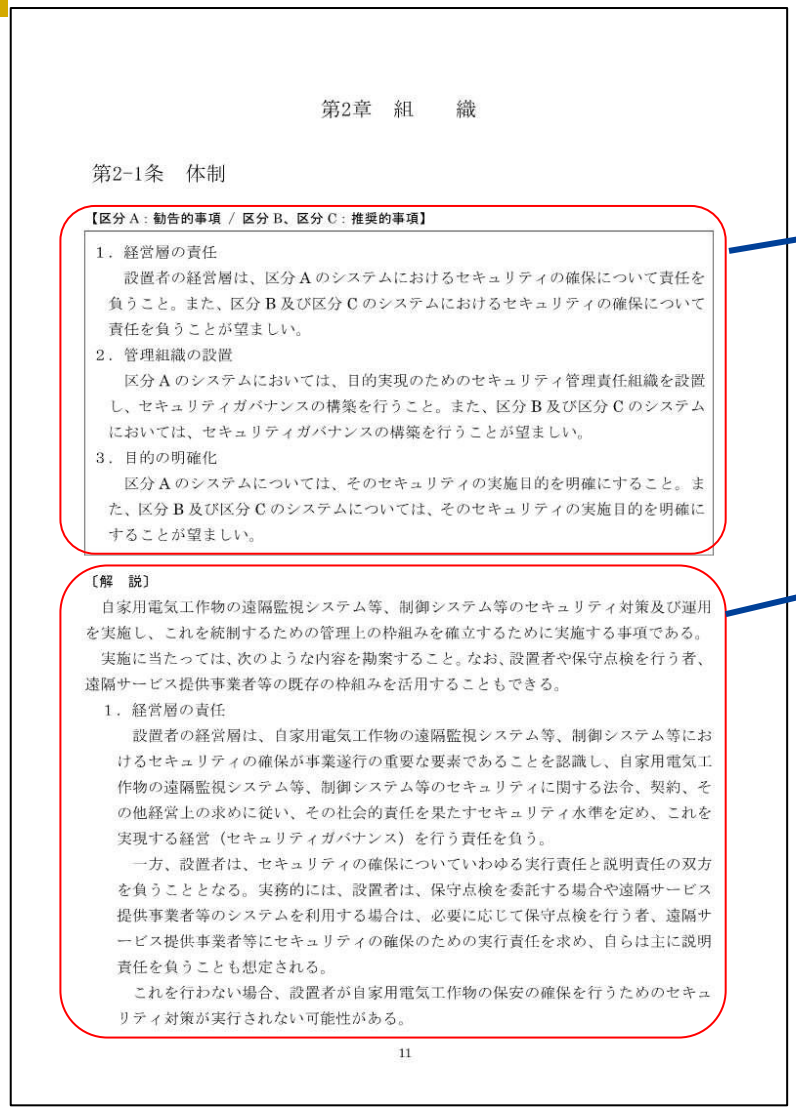
第１－４条　想定脅威

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）

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
●要求事項について



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。

↑

立入検査で確認する内容（監査基準）

- ISMS（セキュリティマネジメントシステムの構築）としての課題
- 組織的対策の課題
- 人的対策の課題
- 物理的対策の課題
- 技術的対策の課題

- ISMS（セキュリティマネジメントシステムの構築）としての課題
- 組織的対策の課題
- 人的対策の課題
- 物理的対策の課題
- 技術的対策の課題

カテゴリ	章	規定項目	カテゴリ	章	規定項目
―	1 総則		―	6 通信のセキュリティ	
総則	1-1	目的	技術	6-1	暗号化・通信プロトコルの最適化
総則	1-2	適用範囲	技術	6-2	ネットワークの管理
総則	1-3	対象となるシステムの区分	―		
総則	1-4	想定脅威	技術	7-1	システムのセキュリティ
総則	1-5	用語の定義	―	8 運用のセキュリティ	
―	2 組織		技術	8-1	システムの管理
組織	2-1	体制	物理	8-2	機器・外部記憶媒体の管理
組織	2-2	役割	技術	8-3	データの管理
人	2-3	セキュリティ教育	技術	8-4	脆弱性の管理
―	3 文書化		―	9 物理セキュリティ	
組織	3-1	文書管理	物理	9-1	物理セキュリティ
組織	3-2	実施状況の報告	―	10 セキュリティ事故の対応	
	4 セキュリティ管理		組織	10-1	情報の収集
ISMS	4-1	セキュリティ管理	組織	10-2	セキュリティ事故の対応体制等
	5 機器のセキュリティ		組織	10-3	セキュリティ事故の報告と情報共有
技術	5-1	セキュリティ仕様の確認	組織	10-4	周知と訓練
物理	5-2	機器の取り扱い			

セキュリティマネジメントシステムの構築について

- 現場の実態
  - 要求あるいは実施事項の記載内容が理解できず、セキュリティマネジメントシステムを構築できない
  - ＩＴ部門がある設置事業者なら構築することもできるが、ほとんどの設置事業者は対応が（ほぼ）不可能

- 監査の視点
  - ＩＳＭＳの作業な困難な設置者にどのように実施してもうらうか？
  - 教科書的なリスクアセスメントを実施してもうらことが理想だが、現実的には実施が困難な事から代替的な手段を案内する

推奨的事項の実施有無を検討し、検討結果の記録を残す

- ✓ 経済産業省は記録を残すことを推奨
  - 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
  - チェックリストを公開している

https://www.meti.go.jp/policy/safety_security/industrial_safety/sangyo/electric/detail/cybersecurity.html

- ISMS（セキュリティマネジメントシステムの構築）としての課題
- **組織的対策の課題**
- 人的対策の課題
- 物理的対策の課題
- 技術的対策の課題

カテゴリ	章	規定項目	カテゴリ	章	規定項目
ー	1 総則		ー	6 通信のセキュリティ	
総則	1-1	目的	技術	6-1	暗号化・通信プロトコルの最適化
総則	1-2	適用範囲	技術	6-2	ネットワークの管理
総則	1-3	対象となるシステムの区分	ー		
総則	1-4	想定脅威	技術	7-1	システムのセキュリティ
総則	1-5	用語の定義	ー	8 運用のセキュリティ	
ー	2 組織		技術	8-1	システムの管理
組織	2-1	体制	物理	8-2	機器・外部記憶媒体の管理
組織	2-2	役割	技術	8-3	データの管理
人	2-3	セキュリティ教育	技術	8-4	脆弱性の管理
ー	3 文書化		ー	9 物理セキュリティ	
組織	3-1	文書管理	物理	9-1	物理セキュリティ
組織	3-2	実施状況の報告	ー	10 セキュリティ事故の対応	
	4 セキュリティ管理		組織	10-1	情報の収集
ISMS	4-1	セキュリティ管理	組織	10-2	セキュリティ事故の対応体制等
ー	5 機器のセキュリティ		組織	10-3	セキュリティ事故の報告と情報共有
技術	5-1	セキュリティ仕様の確認	組織	10-4	周知と訓練
物理	5-2	機器の取り扱い			

組織的な対策について（管理体制）

- 現場の実態
  - セキュリティの管理体制について役割分担がわからないので未対応
  - 電気工作物の保安は業務を委託しているので、よくわからない

- 監査の視点
  - 電力保安は電気工作物の工事、維持、運用について管理する者を定める必要がある。
    サイバーセキュリティの確保は電力保安の１項目のため、電力保安の管理体制の
    一環として整備してもらう
    （従来の体制図等にセキュリティ管理者を追加する）

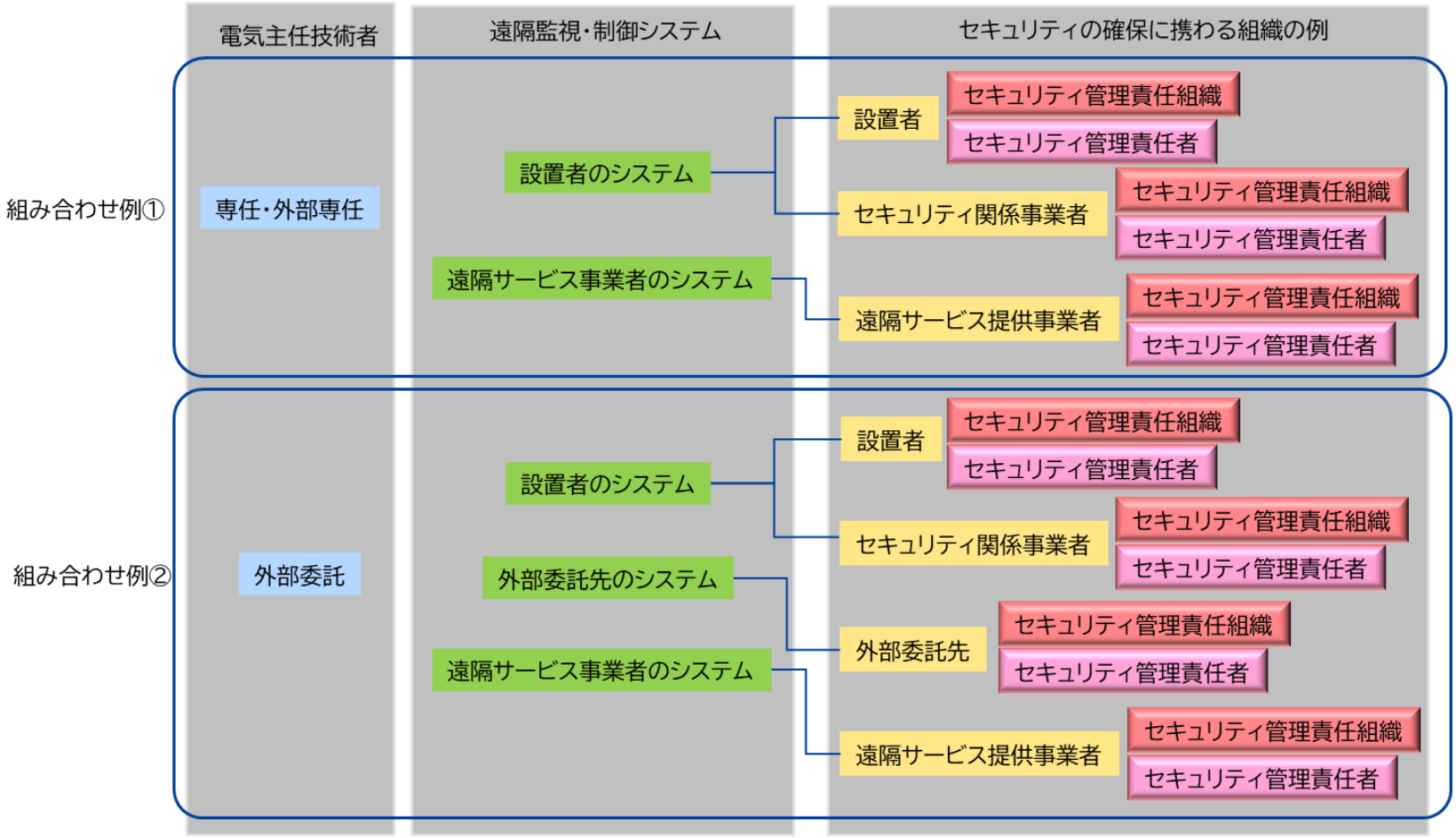
組織的な対策について（役割）

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。

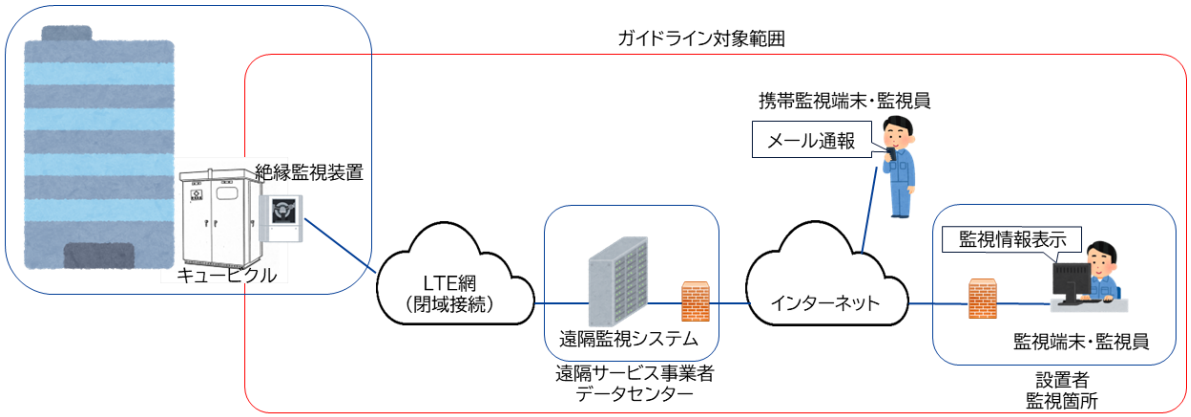
【実施事項】
- 設置者は、セキュリティ管理責任者を任命する。
- 保守点検を委託する場合や遠隔サービス提供事業者等のシステムを利用する場合、自らの組織内にセキュリティ管理責任者を任命している事業者を選択する。

✓ 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



電気主任技術者	遠隔監視・制御システム	セキュリティの確保に携わる組織の例
外部委託	外部委託先のシステム 絶縁監視装置・(携帯)監視端末	外部委託先 セキュリティ管理責任組織 セキュリティ管理責任者
	遠隔サービス事業者のシステム 遠隔監視システム	遠隔サービス提供事業者 セキュリティ管理責任組織 セキュリティ管理責任者

組織的対策（セキュリティ事故の対応）

- 現場の実態
  - セキュリティ事故の対応体制は整備していない
    - ✓ 整備体制イメージがわからない
    - ✓ サイバー攻撃が発生していないので体制整備は不要

- 監査の視点
  - セキュリティ事故（サイバー攻撃）は設備障害の原因の一つであることを認識してもらう
  - セキュリティ事故対応は保安の一環となるため、従来の事故対応の一項目として整備する

- ISMS（セキュリティマネジメントシステムの構築）としての課題
- 組織的対策の課題
- **人的対策の課題**
- 物理的対策の課題
- 技術的対策の課題

カテゴリ	章	規定項目	カテゴリ	章	規定項目
ー	1 総則		ー	6 通信のセキュリティ	
総則	1-1	目的	技術	6-1	暗号化・通信プロトコルの最適化
総則	1-2	適用範囲	技術	6-2	ネットワークの管理
総則	1-3	対象となるシステムの区分	ー		
総則	1-4	想定脅威	技術	7-1	システムのセキュリティ
総則	1-5	用語の定義	ー	8 運用のセキュリティ	
ー	2 組織		技術	8-1	システムの管理
組織	2-1	体制	物理	8-2	機器・外部記憶媒体の管理
組織	2-2	役割	技術	8-3	データの管理
人	2-3	セキュリティ教育	技術	8-4	脆弱性の管理
ー	3 文書化		ー	9 物理セキュリティ	
組織	3-1	文書管理	物理	9-1	物理セキュリティ
組織	3-2	実施状況の報告	ー	10 セキュリティ事故の対応	
	4 セキュリティ管理		組織	10-1	情報の収集
ISMS	4-1	セキュリティ管理	組織	10-2	セキュリティ事故の対応体制等
ー	5 機器のセキュリティ		組織	10-3	セキュリティ事故の報告と情報共有
技術	5-1	セキュリティ仕様の確認	組織	10-4	周知と訓練
物理	5-2	機器の取り扱い			

人的対策について

- 現場の実態
  - 設置事業者の情報セキュリティ管理体制で実施しているセキュリティ教育を活用して実施している場合もあるが、大多数の設置者は実施していない（できない）
    - ✓ セキュリティ教育の実施内容がわからない
    - ✓ サイバー攻撃が発生していないので実施していない

- 監査の視点
  - サイバー攻撃は通常障害の原因の一つであることを認識してもらう
  - 電力保安の中では保安教育を義務づけている
  - サイバーセキュリティの確保は技術基準で定められているので保安教育の一環として実施する

- ISMS（セキュリティマネジメントシステムの構築）としての課題
- 組織的対策の課題
- 人的対策の課題
- **物理的対策の課題**
- 技術的対策の課題

カテゴリ	章	規定項目	カテゴリ	章	規定項目
ー	1 総則		ー	6 通信のセキュリティ	
総則	1-1	目的	技術	6-1	暗号化・通信プロトコルの最適化
総則	1-2	適用範囲	技術	6-2	ネットワークの管理
総則	1-3	対象となるシステムの区分	ー		
総則	1-4	想定脅威	技術	7-1	システムのセキュリティ
総則	1-5	用語の定義	ー	8 運用のセキュリティ	
ー	2 組織		技術	8-1	システムの管理
組織	2-1	体制	物理	8-2	機器・外部記憶媒体の管理
組織	2-2	役割	技術	8-3	データの管理
人	2-3	セキュリティ教育	技術	8-4	脆弱性の管理
ー	3 文書化		ー	9 物理セキュリティ	
組織	3-1	文書管理	物理	9-1	物理セキュリティ
組織	3-2	実施状況の報告	ー	10 セキュリティ事故の対応	
	4 セキュリティ管理		組織	10-1	情報の収集
ISMS	4-1	セキュリティ管理	組織	10-2	セキュリティ事故の対応体制等
ー	5 機器のセキュリティ		組織	10-3	セキュリティ事故の報告と情報共有
技術	5-1	セキュリティ仕様の確認	組織	10-4	周知と訓練
物理	5-2	機器の取り扱い			

物理的対策の課題

- 課題は無く、適切な運用が実施されている

- ISMS（セキュリティマネジメントシステムの構築）としての課題
- 組織的対策の課題
- 人的対策の課題
- 物理的対策の課題
- 技術的対策の課題

カテゴリ	章	規定項目	カテゴリ	章	規定項目
ー	1 総則		ー	6 通信のセキュリティ	
総則	1-1	目的	技術	6-1	暗号化・通信プロトコルの最適化
総則	1-2	適用範囲	技術	6-2	ネットワークの管理
総則	1-3	対象となるシステムの区分	ー		
総則	1-4	想定脅威	技術	7-1	システムのセキュリティ
総則	1-5	用語の定義	ー	8 運用のセキュリティ	
ー	2 組織		技術	8-1	システムの管理
組織	2-1	体制	物理	8-2	機器・外部記憶媒体の管理
組織	2-2	役割	技術	8-3	データの管理
人	2-3	セキュリティ教育	技術	8-4	脆弱性の管理
ー	3 文書化		ー	9 物理セキュリティ	
組織	3-1	文書管理	物理	9-1	物理セキュリティ
組織	3-2	実施状況の報告	ー	10 セキュリティ事故の対応	
	4 セキュリティ管理		組織	10-1	情報の収集
ISMS	4-1	セキュリティ管理	組織	10-2	セキュリティ事故の対応体制等
ー	5 機器のセキュリティ		組織	10-3	セキュリティ事故の報告と情報共有
技術	5-1	セキュリティ仕様の確認	組織	10-4	周知と訓練
物理	5-2	機器の取り扱い			

技術的対策について（ネットワークの管理）

- 技術的対策（ネットワークの管理）の特徴
  - 一般的ではない用語の定義を用いており、要求（実施）事項が理解しにくい
  - 要求（実施）事項が大規模システムの構成を想定している

- 現場の実態
  - 要求（実施）事項を満たしていないネットワーク構成が多い
    - ✓ ガイドラインを認識しておらず、要求事項を満たしていないネットワーク構成
    - ✓ ガイドラインは認識しているが、要求事項を正確に理解していない
    - ✓ ガイドライン施行前からネットワークを構築している

- 監査の視点
  - ✓ ネットワークの用語や構成の考え方について理解を深めてもらう

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

第6-2条 ネットワークの管理

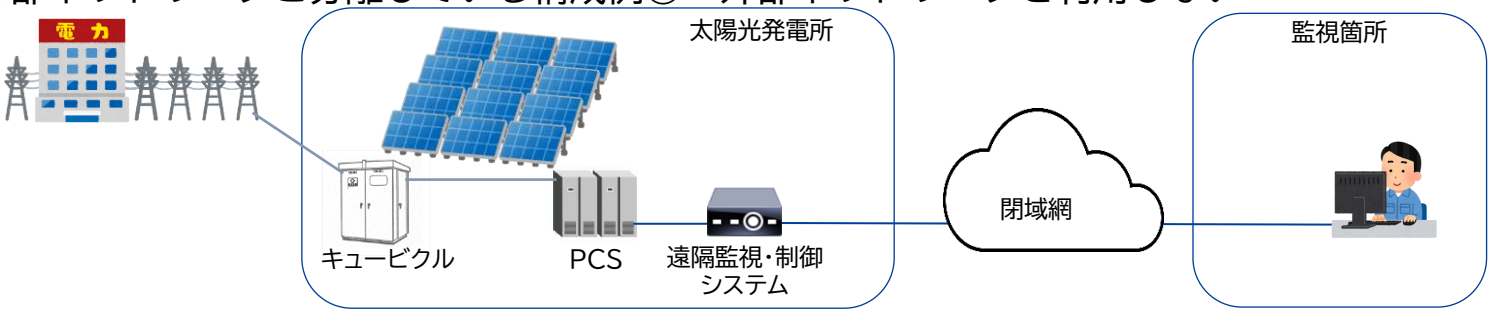
１．外部ネットワークとの分離
※不特定多数が接続できる回線で接続するネットワーク

【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

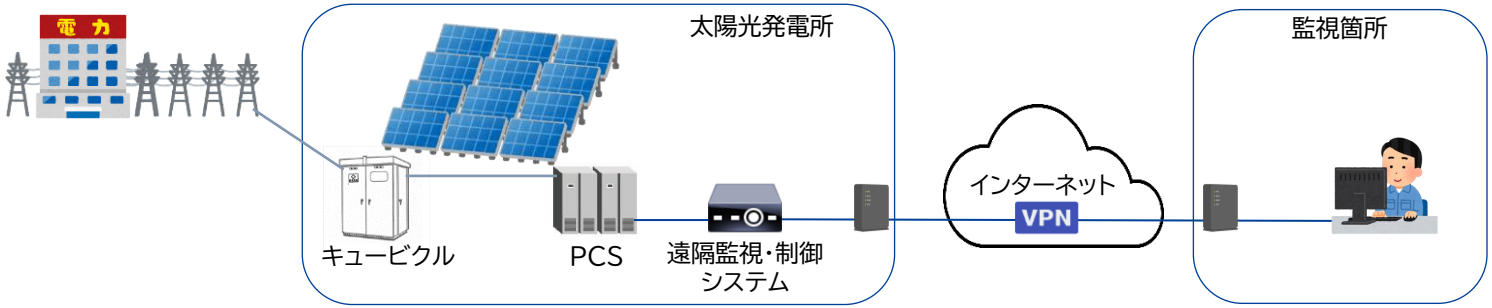
【実施事項】
- 制御システム等は、外部ネットワークと分離する
- 遠隔監視システム等も、可能な範囲で外部ネットワークと直接接続しない
- いずれのシステムも、外部ネットワークと接続する際には、その間に他ネットワークや別のシステム等の緩衝エリアを設けて、間接的にデータ連携を行う仕組み等を構築する

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

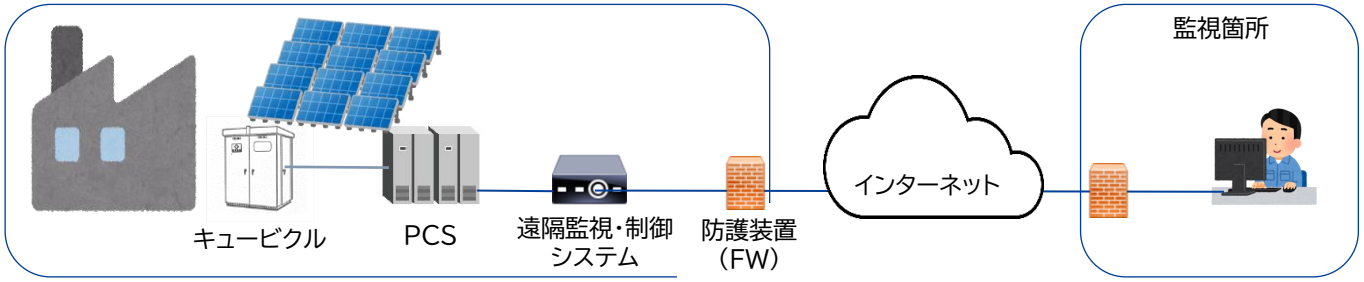


●外部ネットワークと分離している構成例②　外部ネットワーク上に仮想的な閉域網（VPN）を構築する



※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

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】

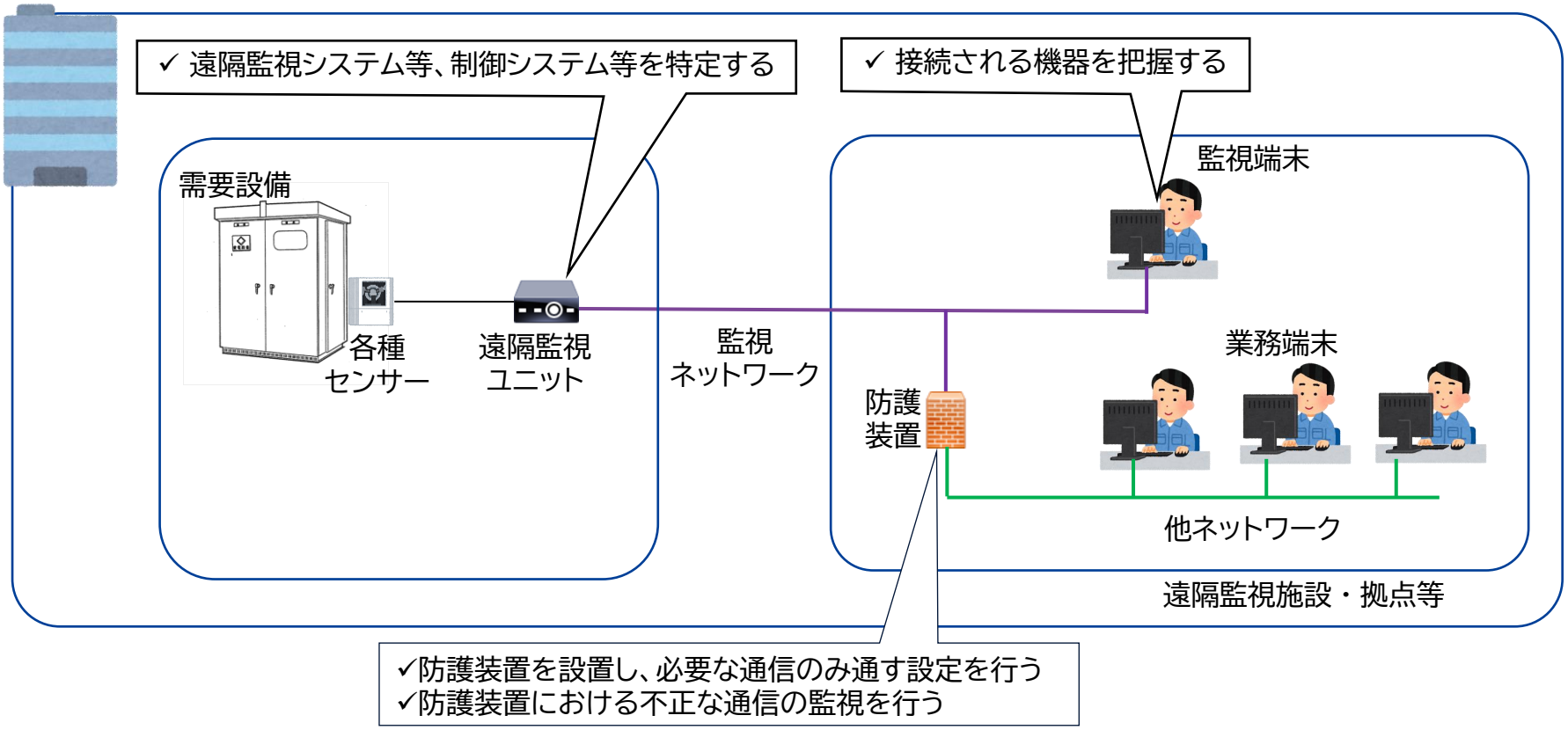
２．接続点の最小化

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

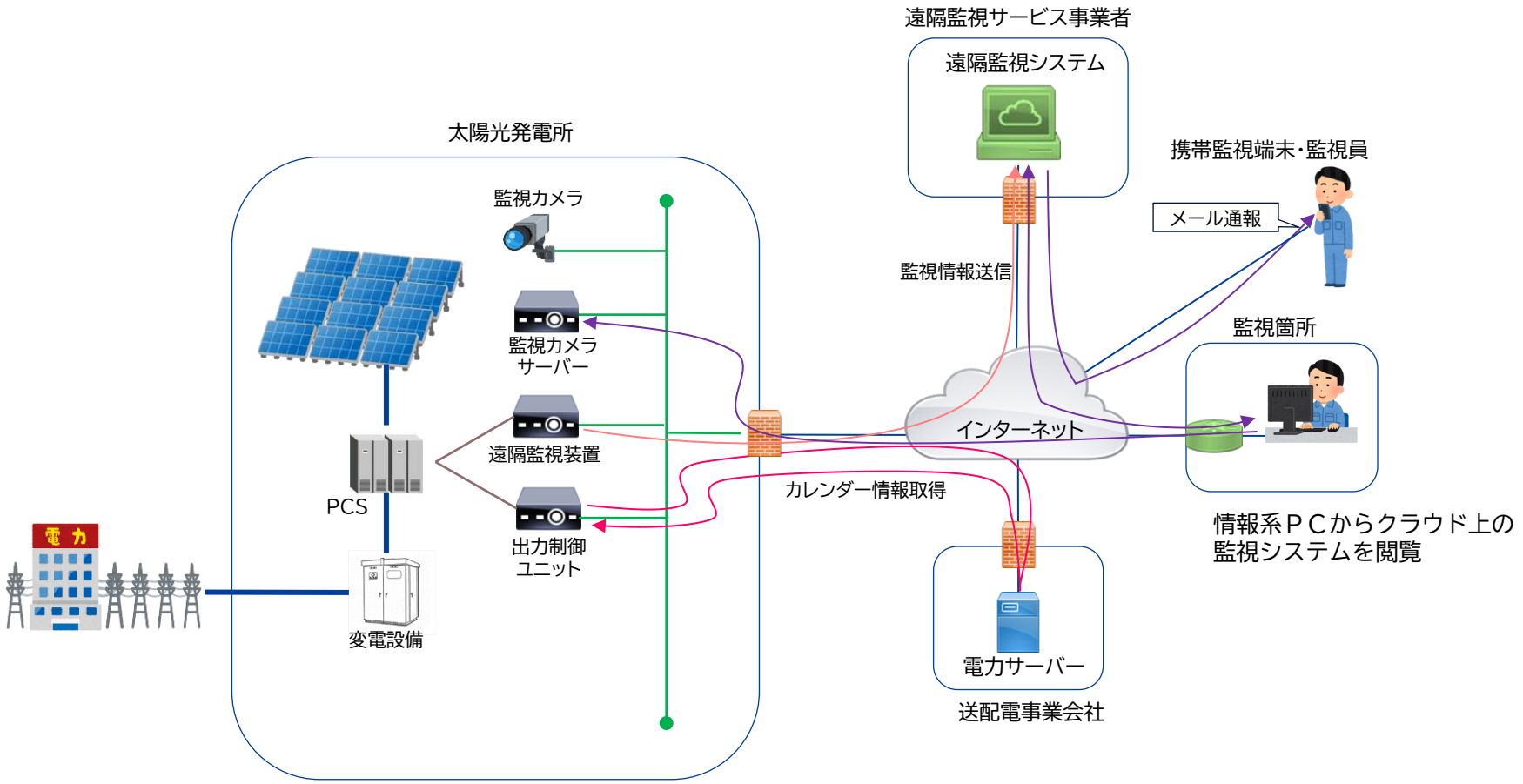
３．接続点の防御

- 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



太陽光発電所のネットワーク構成の実態イメージ



サイバーセキュリティ確保の原則/サイバーセキュリティ立入検査の原則

- サイバーセキュリティの確保は、対策を実施すべき要求事項を全て実施することが原則だが、様々な理由で全てを実施することが難しい場合もある
- セキュリティ対策が実施できていない事は問題ではなく、実施できていない要求事項を放置しておくような状況がでてくる場合、そのような状況が問題となる
- 実施できない事によるリスクを把握し、リスクが顕在化した際の対応を設置者が整備しておくことが重要

実施できない事も含め、全てを把握しておくことがサイバーセキュリティ確保の原則

サイバー立入検査は要求事項の実施状況を確認することが原則だが、それに固執せず
設置者がサイバーセキュリティ確保の原則の理解し対応していることを確認する

ご静聴頂きありがとうございます。