経 済 産 業 省

制定　２０２２０５３０保局第１号
令 和 ４ 年 ６ 月 １ ０ 日

改正　２０２３０３１０保局第２号
令 和 ５ 年 ３ 月 ２ ０ 日

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

経済産業省大臣官房技術総括・保安審議官

電気設備の技術基準の解釈（２０１３０２１５商局第４号）第３７条の２第３号及び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（令和４年６月１０日付け２０２２０５３０保局第１号）の規定に基づき、自家用電気工作物に係るサイバーセキュリティの確保のため、別紙のとおり定める。

（別紙）

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

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

目　　次

第1章　総　　則

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。

〔解　説〕

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、制御システム等のライフサイクルにおけるサイバーセキュリティについて規定したものである。

本ガイドラインの対象は、自家用電気工作物全般である。

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

第1-2条　適用範囲

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。

〔解　説〕

本ガイドラインは、サイバー攻撃やサイバーセキュリティ確保の管理不良を要因としたシステムの不具合により、自家用電気工作物の保安の確保に支障を及ぼす可能性のある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防護の対象とし、これらに携わる者（設置者や保守点検を行う者（保安管理業務の外部委託をする場合にあっては電気管理技術者及び電気保安法人を含む。以下同じ。）、遠隔サービス提供事業者等）に適用する。

具体的な対策は、各々の自家用電気工作物の遠隔監視システム等、制御システム等の特性を十分に踏まえ、重要性や必要性を鑑み、設置者が判断し、実施する又は設置者との協議に基づいて、保守点検を行う者、遠隔サービス提供事業者等にその一部を実施させる。

なお、対象システムは、第 1-3 条（対象となるシステムの区分）を参考に、設置者において定めることとする。

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。

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。以下同じ。）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

〔解　説〕

対象となるシステムの区分については、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 の順に設定したものである。

自家用電気工作物のうち発電設備としては、例えば、火力発電所、水力発電所、太陽電池発電所、風力発電所等に施設する発電設備のほか、需要設備の非常用予備発電装置がある。また、自家用電気工作物のうち発電設備以外の設備としては、例えば、需要設備の受配電設備等がある。

これらの設備の遠隔監視システムとは、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。また、これらの設備の制御システムとは、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。

自家用電気工作物のうち発電設備におけるシステムとして、設置者が発電設備（太陽電池発電所）の保安管理業務を外部委託する場合の例を図 1 と図 2 に示し、それぞれの図中

に本ガイドラインで対象となるシステムの範囲を表す。これらの例では、遠隔監視システムと制御システムの両方を有している。

図 1 の例では、発電設備の運転状況（出力、電力量等）や構成設備の状態（絶縁が保たれていること、設備が破損していないこと等）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している。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している。これに加えて、発電設備の出力制御コマンドが遠隔サービス提供事業者のシステムを介して発電設備側に伝達される。さらに、発電設備の起動コマンドが保安管理業務の外部委託の受託者等が接続するシステムを介して伝達される。

図 2 の例では、発電設備の運転状況（出力、電力量等）や構成設備の状態（絶縁が保たれていること、設備が破損していないこと等）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している。また、発電設備の出力制御コマンドが、系統接続先の電力会社から別のシステムを介して伝達される。

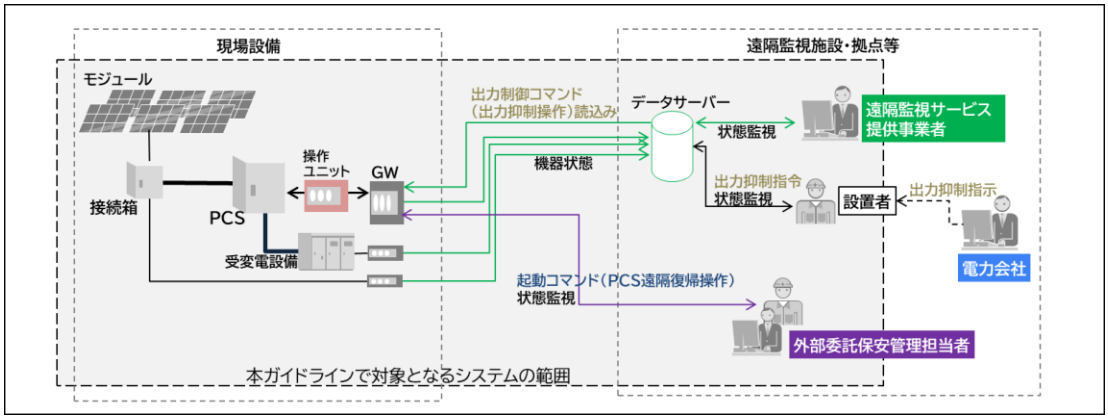

図 1：発電設備の保安管理業務を外部委託する場合の対象システムの範囲の例（発電設備の出力制御コマンドが遠隔サービス提供事業者のシステムを介して発電設備側に伝達される例）

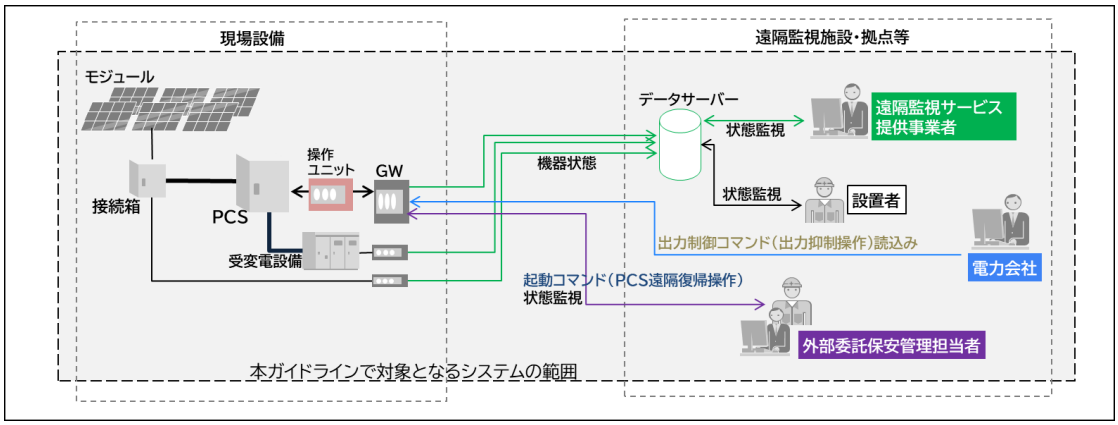

図 2：発電設備の保安管理業務を外部委託する場合の対象システムの範囲の例（発電設備の出力制御コマンドが系統接続先の電力会社から別のシステムを介して伝達される例）

自家用電気工作物のうち発電設備以外の設備におけるシステムとして、設置者が需要設備の保安管理業務を外部委託する場合の例を図 3 に示し、本ガイドラインで対象となるシステムの範囲を表す。

図 3 の例では、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（電圧、電流等）や構成設備の状態（絶縁が保たれていること、設備が破損していないこと等）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している。また、需要設備の運転状況や構成設備の状態を取得するためのセンサーやカメラ、情報を伝送するための端末等に対する制御やコマンド送信が行われている。

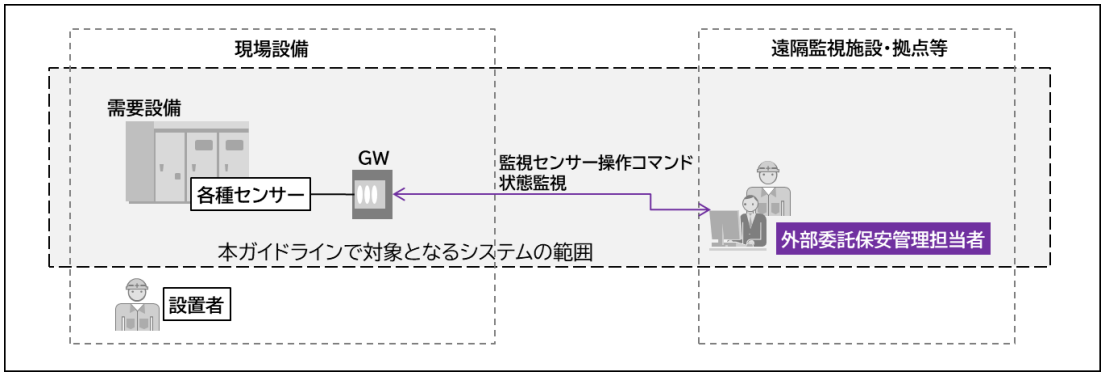

図 3：需要設備の保安管理業務を外部委託する場合の対象システムの範囲の例

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。

第1-4条　想定脅威

本ガイドラインにおいては、自家用電気工作物の保安の確保（公衆の安全及び電力系統へ波及する事故の防止を含む。以下同じ。）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。

〔解　説〕

自家用電気工作物の遠隔監視システム等、制御システム等においては、システムのぜい弱性をついたサイバー攻撃又はシステム関係者による不適正な作業といったセキュリティに関する管理の不良により、システムの不具合を意図的又は非意図的に発生させ、自家用

電気工作物の保安の確保に支障を及ぼす可能性がある。

具体的な脅威としては、例えば、遠隔監視システムにおいては、監視している情報の傍受や改ざん等が考えられ、制御システムにおいては、設定値の改ざんや不正アクセス等が考えられる。

第1-5条　用語の定義

本ガイドラインにおいて、次の各号に掲げる用語の定義は、それぞれ当該各号に定めるところによる。

(1) 「遠隔監視システム」とは、自家用電気工作物の保安の確保に資するために、電気工作物を監視する機能等を具備したシステムをいう。

(2) 「遠隔監視システム等」とは、遠隔監視システム及び遠隔監視用ネットワークの全体をいう。

(3) 「遠隔監視用ネットワーク」とは、遠隔監視システム同士を接続するネットワーク及び監視箇所と被監視箇所を接続するネットワークをいう。

(4) 「制御システム」とは、自家用電気工作物の保安の確保に資するために、自家用電気工作物を制御する機能等を具備したシステムをいう。

(5) 「制御システム等」とは、制御システム及び制御用ネットワークの全体をいう。

(6) 「制御用ネットワーク」とは、制御システム同士を接続するネットワーク及び制御箇所と被制御箇所を接続するネットワークをいう。

(7) 「ライフサイクル」とは、遠隔監視システム等、制御システム等の計画・開発・調達・運用・保守・廃止をいう。

(8) 「システムの不具合」とは、システムの障害、作業ミス及びサイバー攻撃等により、システムが設計時の期待どおりの機能を発揮せず、又は発揮できない状態をいう。

(9) 「外部委託」とは、電気事業法施行規則（平成 7 年通商産業省令第 77 号）第 52 条第 2 項の規定に基づき、自家用電気工作物の保安管理業務を委託することをいう。

(10) 「遠隔サービス提供事業者」とは、遠隔監視システム等、制御システム等の利用に関するサービスを設置者に対して提供する事業者をいう。

(11) 「セキュリティ事故」とは、意図的なサイバー攻撃により、自家用電気工作物の保安の確保に支障を及ぼし、又はそのおそれのあるシステムの不具合が発生した事象をいう。

(12) 「機器」とは、システムを構成するサーバー、パソコンや可搬型の機器等の端末及びネットワークの構成機器をいう。

(13)「コマンド」とは、システムにおける命令をいう。その中でも特に発行に慎重を要するものを「重要なコマンド」という。
(14)「ぜい弱性」とは、ソフトウェアやアプリケーション等において、システムへの不正アクセスやマルウェア等の攻撃により、その機能や性能を損なう原因となり得るセキュリティ上の問題箇所をいう。
(15)「サイバー攻撃」とは、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。
(16)「システム関係者」とは、委託先等を含む遠隔監視システム等、制御システム等の利用、管理、開発、保守に従事する者の総称をいう。
(17)「経営層」とは、設置者における経営責任を持つ者をいう。
(18)「セキュリティガバナンス」とは、経営層が主体的かつ適切に情報リスクを管理する仕組みを構築・運用することをいう。
(19)「セキュリティ面での戦略マネジメント」とは、セキュリティ戦略の検討やセキュリティ事故対応の中核を担い、経営層との橋渡しを行うこと及びセキュリティを経営・事業リスクの一つとして認識した上で、経営計画や投資計画の策定にも関わることをいう。
(20)「セキュリティ関係事業者」とは、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に関するサービスを設置者に対して提供する事業者をいう。
(21)「委託先等」とは、委託先、再委託先及び発注先をいう。
(22)「リスク」とは、脅威とぜい弱性の合致により損失が発生する可能性及びその損失をいう。
(23)「文書化」とは、情報や手順を可視化することをいう。
(24)「セキュリティに関する情報」とは、セキュリティマネジメントに関する情報及びセキュリティ対策の実施状況に関する情報をいう。
(25)「報告」とは、予め設定された報告経路及び手順に従って、文書化された情報を伝達することをいう。
(26)「セキュリティマネジメントシステム」とは、組織（企業、部、課等）におけるセキュリティを管理するための仕組みをいう。
(27)「監査」とは、セキュリティに関する取組を客観的に評価することをいう。
(28)「セキュリティ仕様」とは、遠隔監視システム等、制御システム等の機能要件に応じて策定されたセキュリティ要件をいう。
(29)「外部ネットワーク」とは、不特定多数が接続できる回線で接続するネットワークをいう。
(30)「他ネットワーク」とは、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をいう。

(31)「防護装置」とは、他ネットワークからの攻撃や不正アクセスから遠隔監視用ネットワーク、制御用ネットワークを防御するためのファイアウォール等の装置をいう。
(32)「外部記憶媒体」とは、機器に接続してそのデータを保存するための可搬型の装置をいう。
(33)「ログ」とは、遠隔監視システム等、制御システム等に対して行われた操作状況や動作状況を記録したものをいう。
(34)「危機管理体制」とは、自家用電気工作物の保安の確保に多大な影響や損失を及ぼすような不測の事態に備え、かつ起こった時に適切に対応する体制をいう。

〔解　説〕

用語の定義のうち、(29)「外部ネットワーク」は、例えば、VPN（Virtual Private Network）で言えば、インターネット VPN が該当し、IP-VPN（Internet Protocol -VPN）は該当しない。また、(30)「他ネットワーク」は、例えば、自社内の事務処理に用いられるネットワーク等が該当する。

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。

２．管理組織の設置

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。また、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ことが望ましい。なお、経営規模によっては、セキュリティ管理組織は個人であってもよい。これにより、設置者や保守点検を行う者、遠隔サービス提供事業者等全体のセキュリティガバナンスの構築に努める。

経営層は、セキュリティの確保に必要な資源を準備し、実施可能な体制を構築する。なお、セキュリティ管理責任組織の設置に当たっては、セキュリティ面での戦略マネジメントに関する機能の配置にも留意する。

これを行わない場合、セキュリティ管理が適切に行われない可能性や設置者の組織全体の活動と関連した活動が行われなくなる可能性がある。

３．目的の明確化

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。また、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ことも想定される。

これを行わない場合、システム関係者がそれぞれの判断において設置者の目的に反した活動をしてしまう可能性がある。

遠隔監視システム、制御システムの所管と、セキュリティの確保に携わる組織の組合せの例を図４に示す。図４の例では、セキュリティの確保に携わる設置者以外の組織においても、経営層の責任が求められる。また、保守点検を行う者や遠隔サービス提供事業者等において、セキュリティ管理組織の設置が求められる。

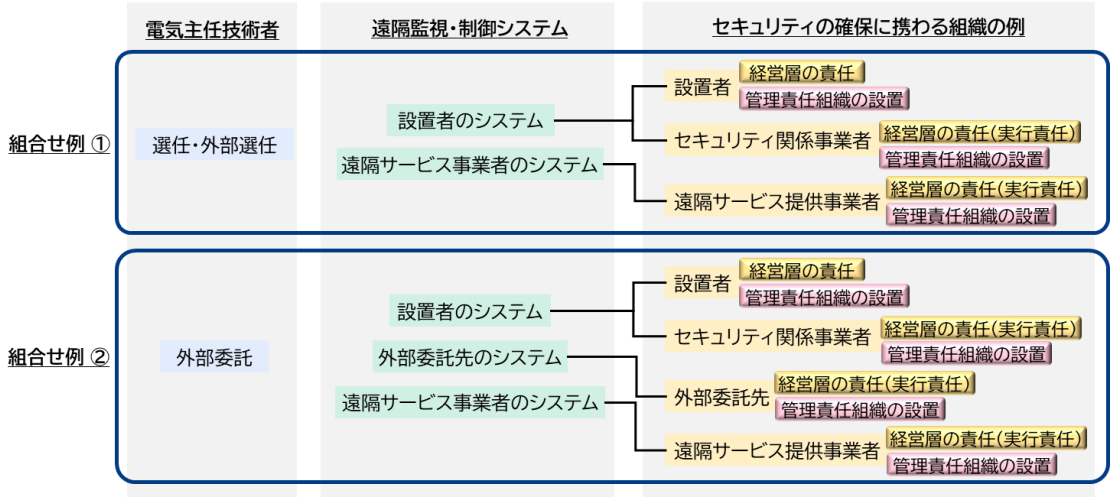

図４：遠隔監視システム、制御システムの所管と、セキュリティの確保に携わる組織の組合せ、及び経営層の責任、セキュリティ管理責任組織の設置が求められる組織の例

第2-2条　役割

１．責任者の設置**【区分 A：勧告的事項 / 区分 B、区分 C：推奨的事項】**

設置者は、区分 A の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。また、区分 B 及び区分 C の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が望ましい。

２．役割の定義**【推奨的事項】**

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が望ましい。

３．委託先等の対応**【推奨的事項】**

設置者は、自家用電気工作物の遠隔監視システム等、制御システム等に関連する委託先等の役割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に関する取組に着手し、管理するための仕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．責任者の設置

設置者は、セキュリティ管理責任者を任命する。また、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ことが望ましく、当該事業者を選択する場合は、それぞれの責任範囲を明確にする。例えば、保守点検を行う者や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、設置者は主に説明責任を負うこと等が想定される。

これを行わない場合、責任の所在の不明確さによってセキュリティ対策が適切に実施できない可能性がある。

２．役割の定義

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ことが望ましい。また、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ことが望ましい。なお、役割の定義に当たっては、システム関係者とセキュリティ管理責任組織が互いに協力しながらセキュリティに関する取組・管理を行えるよう留意する。

これを行わない場合、セキュリティ対策が適切に実施できない可能性がある。

３．委託先等の対応

設置者は、自家用電気工作物の遠隔監視システム等、制御システム等に関連する委託先等のセキュリティ確保に関する役割を明確化することが望ましい。また、委託先等に対して、セキュリティ確保の目的や対策を明確に伝達し、遵守させる取り決めを行うことが望ましい。なお、必要に応じて遵守状況の確認等を実施することが望ましい。また、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に対して、それら事業者の再委託先等に対して同様の対応を求めることが望ましい。

これを行わない場合、委託先等におけるセキュリティ対策の不備や発生した事象等を把握できず、セキュリティ事故が発生したり損害が拡大したりする可能性がある。

遠隔監視システム、制御システムの所管と、セキュリティの確保に携わる組織の組合せの例を図５に示す。図５のように、セキュリティの確保に携わる設置者以外の組織においても、必要に応じてセキュリティ管理責任者をする。

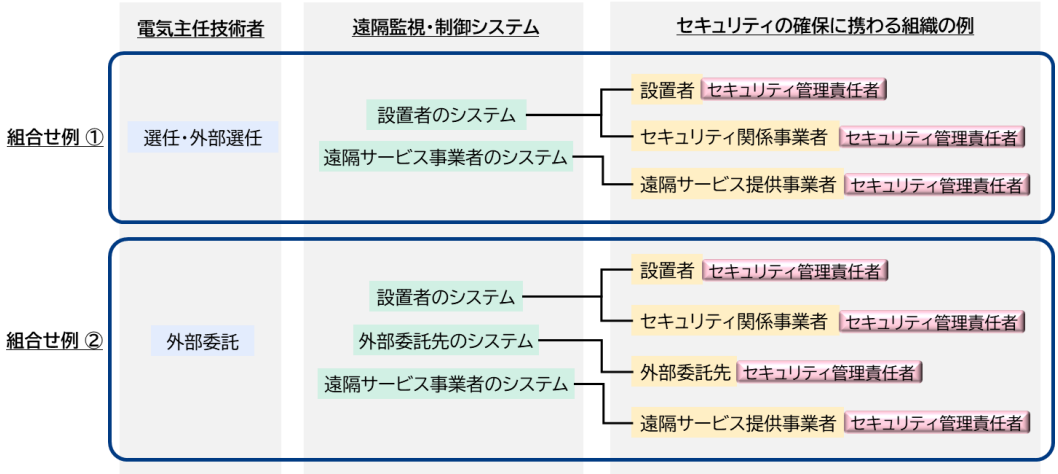

図５：遠隔監視システム、制御システムの所管と、セキュリティの確保に携わる組織の組合せ及びセキュリティ管理責任者の設置の例

第2-3条　セキュリティ教育

【推奨的事項】

１．教育の計画・実施

セキュリティ教育を計画し、実施することが望ましい。

２．教育効果の確認

セキュリティ教育の効果を確認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、制御システム等のシステム関係者がセキュリティの重要性を認識し、適切なセキュリティ対策を行えるようにするために実施することが望ましい事項である。

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．教育の計画・実施

セキュリティ管理責任者は、システム関係者が役割に応じたセキュリティ教育を受けることができるように教育を計画及び実施し、セキュリティに関する知識とスキルを持つ人材を育成することが望ましい。また、セキュリティ教育を定期的に実施することが望ましい。実施に当たっては、組織として知識とスキルを継続的に蓄積できるよう人材の配置に留意するとともに、組織外の関係機関が提供する教育の機会や資格制度等の活用も考えられる。一方、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おいてシステム関係者が役割に応じたセキュリティ教育を受けていることを確認し、又は委託契約等によって担保することが望ましい。

これを行わない場合、システム関係者のセキュリティ意識低下によるリスク増加の可能性や教育が十分でないためにセキュリティの重要性を認識できず、適切な対策の実施、セキュリティ事故発生時の適切な対応ができない可能性がある。

２．教育効果の確認

セキュリティ教育の実施者は、対象者の理解度を確認することが望ましい。その際、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、保守点検を行う者や遠隔サービス提供事業者等が同様の理解度確認を行っていることを確認し、又は委託契約等によって担保することが望ましい。

これを行わない場合、適切な対策を実施することができない可能性がある。

第3章　文書化

第3-1条　文書管理

【推奨的事項】

１．文書化

　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情報を文書化することが望ましい。

２．文書の管理

　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文書を適切に管理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に関する情報をシステム関係者に周知徹底し、最新の情報を必要な時に利用できるようにするために実施することが望ましい事項である。

実施に当たっては、次のような内容を勘案すること。

１．文書化

設置者は、自家用電気工作物の遠隔監視システム等、制御システム等のセキュリティに関する情報を適切に利用できるように文書化することが望ましい。文書化に当たっては、その目的を明確にし、文書の取扱い等について規定することが望ましい。また､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、設置者自らの文書化に加え、保守点検を行う者、遠隔サービス提供事業者等においてシステムのセキュリティに関する情報が文書化されていることを確認し、又は委託契約等によって担保することが望ましい。

これを行わない場合、必要な情報が文書化されず、情報が正しく管理されないことによって、セキュリティ事故の原因となる可能性がある。

２．文書の管理

設置者は、自家用電気工作物の遠隔監視システム等、制御システム等のセキュリティに関する文書を適切に分類し、管理することが望ましい。また、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、設置者自らの文書の管理に加え、保守点検を行う者、遠隔サービス提供事業者等においてシステムのセキュリティに関する文書を適切に分類し、管理されていることを確認し、又は委託契約等によって担保することが望ましい。

これを行わない場合、文書を不適切に取り扱うことで、セキュリティ事故の原因となる可能性がある。

第3-2条　実施状況の報告

【推奨的事項】

セキュリティ対策の実施状況に関する報告事項を定め、適切に報告を行うことができる仕組みを構築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、制御システム等に関するセキュリティ対策の実施状況を明確にするために実施することが望ましい事項である。

実施に当たっては、次のような内容を勘案すること。

１．報告の種類

設置者は、自らの組織内においてセキュリティ管理責任者、経営層に対するセキュリティ対策の実施状況に関する報告事項を予め定めることが望ましい。また、報告事項には、報告の目的に応じて判断に必要な内容を含めることが望ましい。その際、セキュリティ管理を委託する場合、委託先の事業者と連携、協議して報告事項を予め定める。一方、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おいても同様の取組を求めることが望ましい。また、それぞれの事業者から設置者に対するセキュリティ対策の報告事項についても予め定めることが望ましい。

２．定期的な報告

設置者は、自らの組織内においてセキュリティ対策の実施状況を定期的に報告させることが望ましい。その際、セキュリティ管理を委託する場合、委託先の事業者と連携してこれを実施する。一方、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おいても同様の取組を求めることが望ましい。また、それぞれの事業者から設置者に対して定期的に報告を受けることが望ましい。

これらを行わない場合、報告が管理されていないことにより、セキュリティ対策の不備が発生する可能性がある。

遠隔監視システム、制御システムの所管と、セキュリティの確保に携わる組織の組合せの例を図 6 に示す。図 6 のように、セキュリティの確保に携わる設置者以外の組織においては、組織内部での定期的な報告とともに、設置者に対する報告をする。

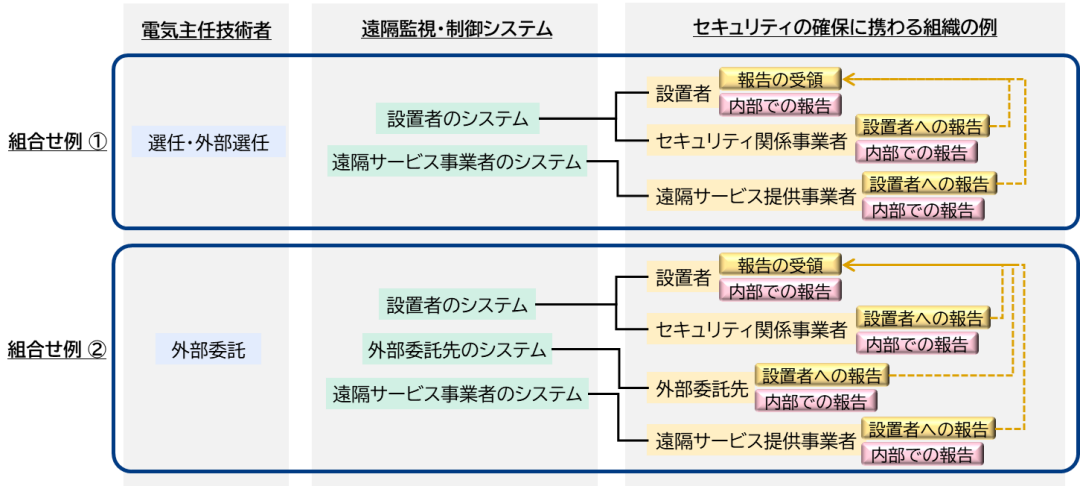

図 6：遠隔監視システム、制御システムの所管とセキュリティの確保に携わる組織の組合せ及び報告先の例

第4章　セキュリティ管理

第4-1条　セキュリティ管理

【推奨的事項】

セキュリティマネジメントシステムを構築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を継続的に改善し、対策を計画に従って適切に行えるようにするために実施することが望ましい事項である。

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．対策の計画

設置者は、セキュリティ対策について、セキュリティ管理責任組織のもとで策定した方針に従って、対象システムやネットワーク構成を把握した上で、最適なリスクアセスメント手法を用いて選択し、計画を作成することが望ましい。セキュリティ対策の実施が困難な場合は、残存リスクとして識別し、次の改善時に対応が検討できるように文書に残すことが望ましい。セキュリティ事故発生時も、影響を最小限にとどめることを基本的な考え方として対策を計画することが望ましい。その際、セキュリティ管理を委託する場合は、委託先の事業者と連携してセキュリティ対策の計画の作成を実施する。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、保守点検を行う者や遠隔サービス提供事業者等において同様の内容を実施していることを確認し、又は委託契約等によってセキュリティ対策について計画を作成していることを担保することが望ましい。

これを行わない場合、対策にかかるコストが増大する可能性や、適切な対策が実施されない可能性がある。

２．対策の実施

設置者は、セキュリティ対策を計画に従って実施することが望ましい。その際、セキュリティ管理を委託する場合は、委託先の事業者と連携してセキュリティ対策を実施する。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、保守点検を行う者や遠隔サービス提供事業者等による対策の実施を確認し、又は委託契約等によって対策の実施を担保することが望ましい。

これを行わない場合、対策が適切に実施されない可能性がある。

３．対策の点検・報告

設置者は、セキュリティ対策が適切に実施されていることを定期的に点検し、セキ

ュリティ管理責任者に報告することが望ましい。その際、セキュリティ管理を委託する場合は、委託先の事業者と連携してセキュリティ対策の点検・報告を実施する。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よる対策の定期的な点検･報告を確認し、又は委託契約等によって実施を担保することが望ましい。

これを行わない場合、残存リスクを正しく把握できず、適切な対策が実施されない可能性がある。

４．対策の改善

設置者は、セキュリティ対策の点検結果に基づき、その見直しを検討することが望ましい。また、環境の変化に応じて、セキュリティ対策の目的及び内容の変更を検討することが望ましい。その際、セキュリティ管理を委託する場合は、委託先の事業者と連携してこれを実施する。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よる対策の改善を確認し、又は委託契約等によって実施を担保することが望ましい。

これを行わない場合､適切な対策が実施されず､ぜい弱性が露呈する可能性がある。

なお、セキュリティ対策の実施状況については、自家用電気工作物の遠隔監視システム等、制御システム等の所管箇所とは別の組織又は外部の組織による監査等を実施することで、セキュリティ対策の継続的改善の効果をより一層高めることが期待できることから、重要なシステムは適切なタイミングで監査等を実施することが望ましい。また、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、保守点検を行う者や遠隔サービス提供事業者等に対しても監査等の実施を依頼し、その結果を確認することが望ましい。

第5章　機器のセキュリティ

第5-1条　セキュリティ仕様の確認

【推奨的事項】

１．セキュリティ仕様

　自家用電気工作物の遠隔監視システム等、制御システム等の調達時にセキュリティ仕様を明確にすることが望ましい。

２．準拠性の確認

　自家用電気工作物の遠隔監視システム等、制御システム等がセキュリティ仕様どおりに設計、製造されていることを確認することが望ましい。

３．仕様変更

　セキュリティに影響を与える可能性がある変更を適切に管理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、制御システム等の調達時の齟齬、仕様漏れが発生しないようにするために実施することが望ましい事項である。

実施に当たっては、次のような内容を勘案すること。

１．セキュリティ仕様

　設置者は、自家用電気工作物の遠隔監視システム等、制御システム等のセキュリティ仕様を明確にすることが望ましい。また、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仕様には、メーカーにおいて実施する事項も併せて明確化することが望ましい。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、保守点検を行う者や遠隔サービス提供事業者等のシステムのセキュリティ仕様を把握することが望ましい。

　これを行わない場合、自家用電気工作物の遠隔監視システム等、制御システム等にリスクが残る可能性や機器が有する情報が保護できない可能性がある。

２．準拠性の確認

　設置者は、自家用電気工作物の遠隔監視システム等、制御システム等の設計・製造時、出荷時等に、セキュリティ仕様どおりに設計・製造されていることを検査等により確認することが望ましい。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、保守点検を行う者や遠隔サービス提供事業者等のシステムがセキュリティ仕様どおりに設計・製造されていることを検査等により確認されていることを確認し、又は委託契約等によって担保することが望ましい。

これを行わない場合、自家用電気工作物の遠隔監視システム等、制御システム等にリスクが残る可能性や機器が有する情報が保護できない可能性がある。

3．仕様変更

設置者は、自家用電気工作物の遠隔監視システム等、制御システム等の構成や機能の変更時等に、セキュリティ対策への影響を確認し、必要に応じてセキュリティ対策の見直しを行うことが望ましい。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、保守点検を行う者や遠隔サービス提供事業者等にてセキュリティ対策の見直しが実施されていることを確認し、又は委託契約等によって担保することが望ましい。

これを行わない場合、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の不備が発生する可能性がある。

第5-2条　機器の取扱い

【推奨的事項】

1．手順の明確化

機器のライフサイクルにおいて、継続的な管理が可能な手順を明確にすることが望ましい。

2．ソフトウェアアップデート

ソフトウェアアップデートを適切かつ確実に実施することができる仕組みを構築することが望ましい。

〔解　説〕

手順の明確化は、機器を適切に保護するため、また、それぞれの機器が自家用電気工作物の遠隔監視システム、制御システム全体へ悪影響を与えないようにするために実施することが望ましい事項である。なお、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、保守点検を行う者や遠隔サービス提供事業者等が手順の明確化を実施していることを確認し、又は委託契約等によって担保することが望ましい。

実施に当たっては、次のような内容を勘案すること。

1．手順の策定

機器の管理手順を明確にするとともに、機器のライフサイクルを通じて適切な管理が行われる仕組みを構築する。

これを行わない場合、機器の管理不順により、セキュリティの不備が発生する可能

性がある。

２．知識とスキル

機器の設置、交換、撤去には、役割に応じた知識とスキルについて教育又は訓練された者を従事させる。

これを行わない場合、不適切な対応によりセキュリティの不備が発生する可能性がある。

３．機器の確認

機器が不正に置き換えられたり、変更されたりしていないかを適宜確認する。

これを行わない場合、機器の不正な置き換えや変更が把握できず、セキュリティ事故の発生や損害の増大の可能性がある。

ソフトウェアアップデートは、自家用電気工作物の遠隔監視システム、制御システムにおいて、不正なソフトウェアのアップデートによる機器の不正な動作を防止するために実施することが望ましい事項である。なお、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、保守点検を行う者や遠隔サービス提供事業者等が機器の確認を実施していることを確認し、又は委託契約等によって担保することが望ましい。

実施に当たっては、次のような内容を勘案すること。

４．手順の策定

ソフトウェアアップデートは、予め定められた手順に従って実行する。

５．データの確認

ソフトウェアアップデートに利用するデータは、正しいものであることを確認できる仕組みを構築し、不正なソフトウェアのアップデートが行われないようにする。

６．不正アップデートへの対応

不正なソフトウェアのアップデートを確認した場合は、当該機器を無効化するか、当該機器からのデータを無効化する仕組みを構築する。

これらを行わない場合、機器のなりすましやアップデート時の不正なプログラム、マルウェア等の混入により、機器の無効化、他の機器やネットワークの機能に対する影響が発生する可能性がある。

第6章　通信のセキュリティ

第6-1条　暗号化・通信プロトコルの最適化

【推奨的事項】

機器間の通信における傍受や、機器が保有する重要データの漏えい、改ざんの危険が高い区画においては、暗号化・通信プロトコルの最適化を行い、通信データの保護を行うことが望ましい。

〔解　説〕

自家用電気工作物の遠隔監視システム等、制御システム等において、機密性を確保する必要があるデータを不特定多数の人がアクセス可能な区画で取り扱う場合は、機器間の通信における傍受、不正なデータの挿入、機器が保有する重要なデータの漏えい、改ざんが発生しないよう、通信データを保護するために実施することが望ましい事項である。なお、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、保守点検を行う者や遠隔サービス提供事業者等が通信データの保護を実施していることを確認し、又は委託契約等によって担保することが望ましい。

実施に当たっては、次のような内容を勘案すること。

１．暗号化

データが傍受、改ざんされた場合のリスクを考慮し、必要に応じてデータを暗号化することが望ましい。

暗号を用いる場合は、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て、暗号方式を選択し、暗号鍵を適切に配付し、管理することが望ましい。

２．通信プロトコルの最適化

通信路上のセキュリティ確保が必要な区間を予め定め、その内容に従って通信プロトコルを選択することが望ましい。

採用した通信プロトコルについては、ぜい弱性情報を定期的に収集することが望ましい。また、通信プロトコルをカスタマイズする場合は、当初のセキュリティ機能を損なうことがないように実装することが望ましい。

これらを行わない場合、通信データや保管データの傍受・改ざん、不正な閲覧の可能性がある。

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**【推奨的事項】**

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、分離することが望ましい。

２．接続点の最小化**【区分 A：勧告的事項 / 区分 B、区分 C：推奨的事項】**

区分 A のシステムにおいて、他ネットワークとの接続点は、最小化すること。

区分 B 及び区分 C のシステムにおいて、他ネットワークとの接続点は、最小化することが望ましい。

３．接続点の防御**【区分 A：勧告的事項 / 区分 B、区分 C：推奨的事項】**

区分 A のシステムにおいて、他ネットワークとの接続点に防御措置を講じること。

区分 B 及び区分 C のシステムにおいて、他ネットワークとの接続点に防御措置を講じることが望ましい。

４．接続制御**【推奨的事項】**

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ることが望ましい。

５．認証**【推奨的事項】**

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ることが望ましい。

６．ネットワーク分割**【推奨的事項】**

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することが望ましい。

〔解　説〕

外部ネットワークとの分離は、不特定多数がアクセスできるネットワークを介して、自家用電気工作物の遠隔監視システム等、制御システム等が外部から不正侵入されないようにするために実施することが望ましい事項である。なお、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、保守点検を行う者や遠隔サービス提供事業者等が外部ネットワークとの分離を実施していることを確認し、又は委託契約等によって担保することが望ましい。

実施に当たっては、次のような内容を勘案すること。

１．外部ネットワークとの分離

制御システム等は、外部ネットワークと分離することが望ましい。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ことが望ましい。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こと

が望ましい。

これを行わない場合、不特定多数の攻撃者からサイバー攻撃を受け、自家用電気工作物の遠隔監視システム等、制御システム等に不正侵入される可能性がある。

接続点の最小化、接続点の防御は、他ネットワーク内で発生したサイバー攻撃の影響が、自家用電気工作物の遠隔監視システム等、制御システム等に伝播しないようにするために実施することが望ましい事項である。なお、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、保守点検を行う者や遠隔サービス提供事業者等が接続点の最小化、接続点の防御を実施していることを確認し、又は委託契約等によって担保することが望ましい。

実施に当たっては、次のような内容を勘案すること。

２．接続点の最小化

他ネットワークからの脅威を防ぐためには、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することが望ましい。具体的には、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ことが望ましい。

これを行わない場合、他ネットワークとの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。

３．接続点の防御

不正アクセスを制限する防御の措置は、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ことや、防護装置における不正な通信の監視を行うことといった事例があげられる。なお、他の措置で目的を満たす場合はこの限りではない。

これらを行わない場合、自家用電気工作物の遠隔監視システム等、制御システム等への不正アクセスやマルウェアの侵入により、システムの不具合が生じる可能性や情報が保護できない可能性がある。

接続制御、認証、ネットワークの分割は、不正接続された機器やサイバー攻撃を受けた機器により、他の機器や遠隔監視システム等、制御システム等の不正な動作を防止するために実施することが望ましい事項である。なお、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、保守点検を行う者や遠隔サービス提供事業者等が接続制御、認証、ネットワークの分割を実施していることを確認し、又は委託契約等によって担保することが望ましい。

実施に当たっては、次のような内容を勘案すること。

４，接続制御

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することが望ましい。

５．認証

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、認証することが望ましい。

６．ネットワーク分割

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することが望ましい。

これらを行わない場合、なりすましや不正な機器を接続されることにより、他の機器や自家用電気工作物の遠隔監視システム等、制御システム等の稼働に広範囲に影響を与える可能性がある。

第7章　システムのセキュリティ

第7-1条　システムのセキュリティ

【推奨的事項】

１．不正プログラム防止 不正なプログラムの実行を阻止する仕組みを講じることが望ましい。 ２．不正処理防止 本来の操作によらない処理が発行されないよう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、制御システムにおける不正な処理を防止するために実施することが望ましい事項である。なお、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、保守点検を行う者や遠隔サービス提供事業者等が実施していることを確認し、又は委託契約等によって担保することが望ましい。

実施に当たっては、次のような内容を勘案すること。

１．不正プログラム防止

自家用電気工作物の遠隔監視システム、制御システムにおいて、予め定められたプログラムのみが実行されるように設定することが望ましい。

これを行わない場合、不正なプログラムにより遠隔監視システム、制御システムの稼働に影響を与える可能性がある。

２．不正処理防止

自家用電気工作物の遠隔監視システム、制御システムにおいて、コマンドが不正に発行されないような仕組みを構築し、特に重要なコマンドについては、誤ってコマンドが発行されない仕組みを構築することが望ましい。また、コマンド発行者の権限は最小限にすることが望ましい。

これを行わない場合、不正なコマンド発行により自家用電気工作物の遠隔監視システム、制御システムの稼働に影響を与える可能性がある。

第8章　運用のセキュリティ

第8-1条　システムの管理

１．管理者権限の適切な割当**【推奨的事項】**

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が望ましい。

２．機器のマルウェア対策**【推奨的事項】**

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が望ましい。

３．外部記憶媒体等のマルウェア対策**【区分 A：勧告的事項 / 区分 B、区分 C：推奨的事項】**

区分 A のシステムにおいて、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。

区分 B 及び区分 C のシステムにおいて、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は、ウイルスチェックを行うことが望ましい。

４．ログの取得**【推奨的事項】**

遠隔監視システム等、制御システム等のログを取得し、保管することが望ましい。

〔解　説〕

管理者権限の適切な割当は、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いて、セキュリティを保った運用環境を構築するために実施することが望ましい事項である。なお、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、保守点検を行う者、サービス提供事業者等が管理者権限の適切な割当を実施していることを確認し、又は委託契約等によって担保することが望ましい。

実施に当たっては、次のような内容を勘案すること。

１．管理者権限の適切な割当

管理者権限の割当については、以下のとおり実施することが望ましい。

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。

これを行わない場合、管理者権限の不適切な利用による不正アクセスや情報漏えい等の可能性がある。

機器及び外部記憶媒体等のマルウェア対策は、自家用電気工作物の遠隔監視システム等、制御システム等の機器へのマルウェアの侵入を防ぐために実施する事項である。なお、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、保守点検を行う者、遠隔サービス提供事業者等が機器及び外部記憶媒体等のマルウェア対策を実施していることを確認し、又は委託契約等によって担保すること。

実施に当たっては、次のような内容を勘案すること。

２．機器のマルウェア対策

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ことが望ましい。

３．外部記憶媒体等のマルウェア対策

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。

これらを行わない場合、マルウェア感染によりシステムの不具合が発生し、マルウェアの駆除に時間を要して、自家用電気工作物の遠隔監視システム等、制御システム等が長期にわたり利用できない可能性がある。

なお、マルウェア対策は、自家用電気工作物の遠隔監視システム等、制御システム等の可用性に影響を与えない範囲で実施する。

ログの取得は、自家用電気工作物の遠隔監視システム等、制御システム等の管理者権限による不正侵入や、内部不正を確認するために実施することが望ましい事項である。なお、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、保守点検を行う者、遠隔サービス提供事業者等がログの取得を実施していることを確認し、又は委託契約等によって担保することが望ましい。

実施に当たっては、次のような内容を勘案すること。

４．ログの取得

自家用電気工作物の遠隔監視システム等、制御システム等のログについては、取得する対象、保存期間、件数、定期的に確認すべき項目等を当該システムの構成等を考慮して予め設定することが望ましい。ログについては、改ざん行為等を防ぐために許可されていないアクセスから保護することが望ましい。

これを行わない場合、セキュリティ事故の把握が遅れ、自家用電気工作物の遠隔監視システム等、制御システム等の稼働に影響を与えたり、再発防止等の改善が適切に行われなかったりする可能性がある。

第8-2条　機器・外部記憶媒体の管理

【推奨的事項】

機器・外部記憶媒体を管理し、保護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、制御システム等の機器・外部記憶媒体及びデータに関するセキュリティ事故の発生を予防し、又はセキュリティ事故を迅速に把握し対応できるようにするために実施することが望ましい事項である。なお、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、保守点検を行う者、遠隔サービス提供事業者等が機器・外部記憶媒体の管理を実施していることを確認し、又は委託契約等によって担保することが望ましい。

実施に当たっては、次のような内容を勘案すること。

１．機器・外部記憶媒体の管理

機器・外部記憶媒体の管理については、以下のとおり実施することが望ましい。

a) 機器は、その構成情報（管理番号、設置箇所、ソフトウェアのバージョン等機器に関する情報をいう。）も含めて把握し、存在について確認する。

b) 可搬型の機器・外部記憶媒体は、利用状況を把握し、適切に管理する。

これらを行わない場合、管理不備により、セキュリティの不備が発生する可能性がある。また、なりすましや機器の不正な動作、紛失・漏えいに気づかない可能性がある。

第8-3条　データの管理

【推奨的事項】

遠隔監視システム等、制御システム等に関連するデータを管理し、保護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、制御システム等の機器・外部記憶媒体及びデータに関するセキュリティ事故を迅速に把握し対応できるようにするために実施することが望ましい事項である。なお、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、

保守点検を行う者、遠隔サービス提供事業者等がデータの管理を実施していることを確認し、又は委託契約等によって担保することが望ましい。

実施に当たっては、次のような内容を勘案すること。

１．データの管理

遠隔監視システム等、制御システム等に関連するデータを把握し、適切に管理及び保護することが望ましい。また、プライバシー情報が含まれる場合は、プライバシーに関する規定に基づいて保護する。

これを行わない場合、管理不備により、セキュリティの不備が発生する可能性がある。また、なりすましや機器の不正な動作、紛失・漏えいに気づかない可能性がある。

第8-4条　ぜい弱性の管理

【推奨的事項】

ぜい弱性に関する情報を継続的に管理することが望ましい。

また、重大なぜい弱性に対応するセキュリティパッチがリリースされ、自家用電気工作物の遠隔監視システム等、制御システム等へのリスクがあると判断された場合は、影響度を踏まえて可能な範囲でセキュリティパッチを適用するか、代替策を適用することが望ましい。

〔解　説〕

ぜい弱性に関する情報の継続的な管理については、自家用電気工作物の遠隔監視システム、制御システムのぜい弱性に起因するセキュリティ事故の発生を予防するために実施することが望ましい事項である。なお、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、保守点検を行う者、遠隔サービス提供事業者等がぜい弱性に関する情報の継続的な管理を実施していることを確認し、又は委託契約等によって担保することが望ましい。

実施に当たっては、次のような内容を勘案すること。

１．情報の収集

自家用電気工作物の遠隔監視システム、制御システムで利用する機器やソフトウェア、通信プロトコル等におけるぜい弱性に関する情報を定期的に収集することが望ましい。

２．対応手順の策定

収集したぜい弱性に対する対応手順を策定することが望ましい。対応手順には、ぜい弱性が修正された機器やソフトウェア、通信プロトコル等を適用した場合の影響評価や、それらを適用できない場合の対応を含めておくことが望ましい。

これらを行わない場合、放置されたぜい弱性を把握できていないことにより、自家用電気工作物の遠隔監視システム、制御システムの稼働に影響を与える可能性やセキュリティ事故の未然防止ができない可能性がある。

セキュリティパッチの適用については、自家用電気工作物の遠隔監視システム等、制御システム等に関する重大なぜい弱性が内包した状態で、当該ぜい弱性を悪用したサイバー攻撃を阻止するために実施することが望ましい事項である。なお、保守点検を委託し、委託先が所有する遠隔監視システム等、制御システムを利用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、保守点検を行う者、遠隔サービス提供事業者等がセキュリティパッチの適用を実施していることを確認し、又は委託契約等によって担保することが望ましい。

実施に当たっては、次のような内容を勘案すること。

３．セキュリティパッチの適用

セキュリティパッチを適用しないことによるセキュリティリスクと、セキュリティパッチを適用することによる自家用電気工作物の遠隔監視システム等、制御システム等の可用性及び性能への影響を踏まえ、可能であれば、セキュリティパッチを適用するか、代替策を適用することが望ましい。また、適用を見送る場合は、残存リスクを管理することが望ましい。

これを行わない場合、放置されたぜい弱性を悪用したサイバー攻撃が行われ、自家用電気工作物の遠隔監視システム等、制御システム等の不具合が発生する可能性がある。

第9章　物理セキュリティ

第9-1条　物理セキュリティ

【推奨的事項】

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が望ましい。 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、制御システム等に関連する施設又は施設に設置される自家用電気工作物の遠隔監視システム等、制御システム等を適切に保護するために実施することが望ましい事項である。なお、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、保守点検を行う者、遠隔サービス提供事業者等がこれらを実施していることを確認し、又は委託契約等によって担保することが望ましい。

実施に当たっては、次のような内容を勘案すること。

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ことが望ましい。

　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、適用することが望ましい。

　これを行わない場合、その区画や内部に設置された機器の保護ができない可能性がある。

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ことが望ましい。

　これを行わない場合、施設内の機器やそれを利用した業務が侵害される可能性がある。

なお、重要な箇所に監視対策を講じることで、不正行為の抑止効果が期待できる。

第10章　セキュリティ事故の対応

第10-1条　情報の収集

【推奨的事項】

セキュリティ事故の対応に必要な情報を収集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事故に対して、適切に対応できるようにするために実施することが望ましい事項である。なお、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、保守点検を行う者、遠隔サービス提供事業者等が情報の収集を実施していることを確認し、又は委託契約等によって担保することが望ましい。

実施に当たっては、次のような内容を勘案すること。

１．情報の収集

セキュリティ事故対応手順の策定対象となるセキュリティ事故の種類を予め明確にすることが望ましい。セキュリティ事故の対応に必要なログや文書等の情報を定義し、これを収集できるような仕組みを構築することが望ましい。

これを行わない場合、セキュリティ事故の対応に必要な情報が不足し、適切な対応ができない可能性がある。また、再発防止策の検討ができない可能性がある。

第10-2条　セキュリティ事故の対応体制等

【推奨的事項】

セキュリティ事故の対応体制と手順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事故における損害を最小限にするために実施することが望ましい事項である。なお、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、保守点検を行う者、遠隔サービス提供事業者等が実施していることを確認し、又は委託契約等によって担保することが望ましい。

実施に当たっては、次のような内容を勘案すること。

１．責任と手順

設置者は、セキュリティ事故対応のための体制を作り、それぞれの責任範囲と役割を明確にすることが望ましい。また、経営層をはじめとする組織内の関係個所及び組織外の関係機関へのセキュリティ事故の報告を含むセキュリティ事故対応についての手順を策定し、定期的に見直しを実施することが望ましい。手順には、セキュリティ事故対応及び再発防止策の検討のための活動を含む。なお、役割や手順の策定に当たっては、セキュリティ事故対応のための体制や必要に応じた危機管理体制の迅速な立ち上げ及び体制間での密接な情報共有等の連携にも留意する。

なお、政府機関が大規模サイバー攻撃事態と判断した時には、政府機関の要請があれば、これに協力するよう努める。

２．セキュリティ事故の対応

作成した手順に従い、セキュリティ事故の対応を行うことが望ましい。

これらを行わない場合、セキュリティ事故への対応が遅れ、損害が増大する可能性がある。

第10-3条　セキュリティ事故の報告と情報共有

【推奨的事項】

１．セキュリティ事故の報告

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。

２．情報の共有

セキュリティ事故から得られた知見を、セキュリティ事故の予防及び再発防止に活用する仕組みを構築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、制御システム等のぜい弱性に起因するセキュリティ事故の予防及び再発防止のために実施することが望ましい事項である。なお、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、保守点検を行う者、遠隔サービス提供事業者等がセキュリティ事故の報告と情報の共有を実施していることを確認し、又は委託契約等によって担保することが望ましい。なお、本条の規定は、国その他の機関に対しセキュリティ事故の発生の報告を求める他の法令の規定の適用を妨げるものではない。

実施に当たっては、次のような内容を勘案すること。

１．セキュリティ事故の報告

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ことが望ましい。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

うにすることが望ましい。また、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ことが望ましい。

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ことが望ましい。

これを行わない場合、セキュリティ事故対応を迅速に行えず、損害の拡大を未然に防ぐことができない可能性がある。

２．情報の共有

自らの組織で見つかった自家用電気工作物の遠隔監視システム等、制御システム等のぜい弱性や脅威について、他の組織でも同様の問題が発生し得ると判断した場合は、情報共有に努めることが望ましい。また、他の組織が報告したぜい弱性や脅威についても情報を収集し、対応を行うことが望ましい。

これを行わない場合、自らの組織の損害が他の組織に影響を与える可能性がある。また、セキュリティ事故の未然防止や再発防止策の検討ができない可能性がある。

第10-4条　周知と訓練

【推奨的事項】

セキュリティ事故発生時の対応に関する周知や訓練を定期的に行うことが望ましい。

〔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事故発生時に、迅速かつ適切に対応するために実施することが望ましい事項である。なお、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、保守点検を行う者、遠隔サービス提供事業者等が周知と訓練を実施していることを確認し、又は委託契約等によって担保することが望ましい。

実施に当たっては、次のような内容を勘案すること。

１．周知と訓練

セキュリティ事故発生時の対応に関する周知や訓練を定期的に実施することが望ましい。訓練の手法としては、手順の確認、連絡訓練、机上演習等が考えられる。なお，訓練のシナリオ作成においては，セキュリティ事故対応の理解を深めるためにシステム関係者が協力して行うことが有効である。また、電気事業者や重要インフラ事業者、組織外の関係機関等との合同の訓練・演習の機会を活用し、これに参画することも考えられる。

これを行わない場合、セキュリティ事故対応を迅速かつ適切に行えず、損害の拡大

を防ぐことができない可能性がある。