経済産業省

自家用電気工作物における
サイバーセキュリティ対策について

令和４年７月

産業保安グループ　電力安全課

１．スマート保安の推進

２．サイバーセキュリティ対策への措置
（自家用電気工作物）
(1)技術基準・解釈
(2)保安規程

３．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

電気事業法とは

- **電気工作物**の工事・維持・運用について、その**設置者**を規制。
- **公共の安全**を確保し、**環境の保全**を図ることも目的。

➢ 電気工作物の分類

電気事業法※1では、電気工作物を大分類、小分類。

A. 事業用電気工作物　a. 法第38条第4項各号に掲げる事業の用に供する電気工作物　・・・・一般送配電事業者が設置する**送配電設備**など

b. **自家用電気工作物**　・・・・・・・・・民間企業、行政機関等が設置するビル、工場等の**受配電設備**など

B. 一般用電気工作物　・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・一般家庭、小規模事業所等が設置する**受配電設備**など

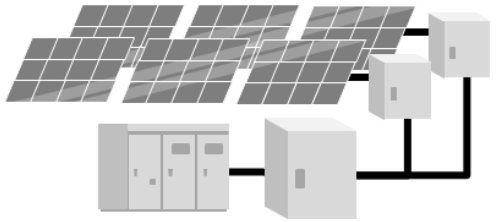
※1　電気事業法（昭和39年法律第170号）

自家用電気工作物とは

- 自家用電気工作物とは、電気事業法第３８条において、「電気事業の用に供する電気工作物及び一般用電気工作物以外の電気工作物」と定義されており、具体的には、次のようなものが該当。
- 電力会社等から**６００Ｖを超える電圧**で受電して電気を使用する設備
- 発電設備（次の**小出力発電設備を除く**。）とその発電した電気を使用する設備
- 電力会社等からの**受電のための電線路以外に構外にわたる電線路**を有する電気設備
- 火薬類（煙火を除く）を製造する事業場及び石炭坑

※**小出力発電設備**とは次のとおり。
(1)出力**５０kW未満**の太陽電池発電設備
(2)出力**２０kW未満**の風力発電設備
(3)出力**２０kW未満**及び最大使用水量１m^3/s 未満の水力発電設備(ダムを伴うものを除く。)
(4)出力**１０kW未満**の内燃力を原動力とする火力発電設備
(5)出力**１０kW未満**の燃料電池発電設備(固体高分子型のものであって、燃料・改質系統設備の最高使用圧力が０．１MPa(液体燃料を通ずる部分にあっては、１．０MPa)未満のものに限る。)

<太陽電池発電所>



<風力発電所>

<需要設備>

自家用電気工作物に対する規制とは

- 電気事業法では、自家用電気工作物の設置者に対して、自主的な保安体制の整備、確立を図るため、主任技術者、技術基準等に関する義務づけを行っている。

➢ 自家用電気工作物に関する主な規制内容

A. **保安規程の作成、届出、遵守の義務**
B. 主任技術者の選任、届出の義務
C. **技術基準の維持の義務**
D. 事故報告、公害防止等に関する届出の義務
E. その他の義務

※2　電気設備に関する技術基準を定める省令
(昭和40年６月15日通商産業省令第61号（制定）、平成９年３月27日通商産業省令第52号（全部改正））

※3　電気関係報告規則
（昭和40年通商産業省令第54号）

１．スマート保安の推進

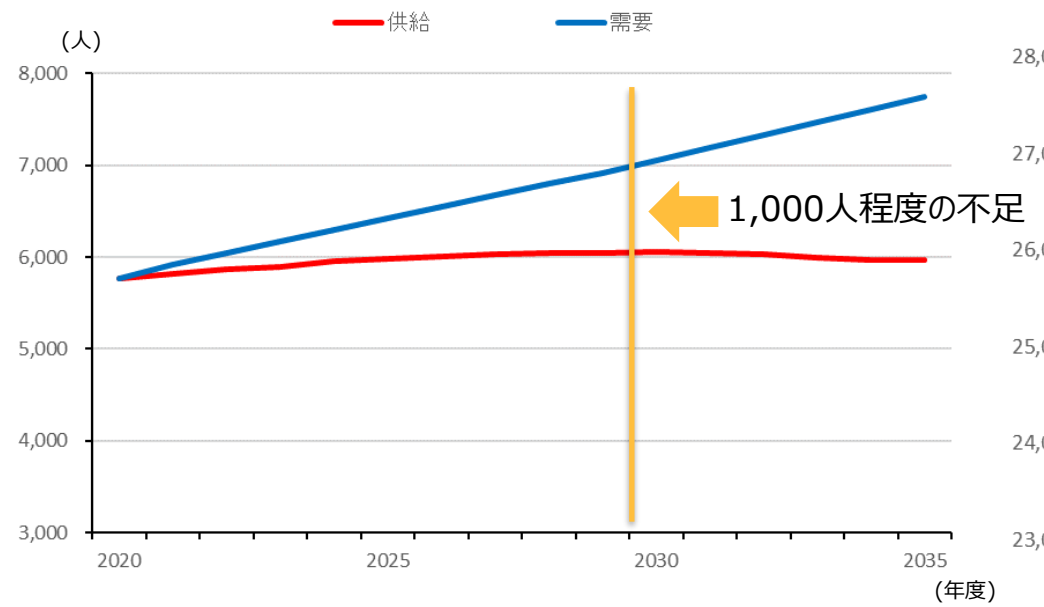
２．サイバーセキュリティ対策への措置
（自家用電気工作物）
(1)技術基準・解釈
(2)保安規程

３．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

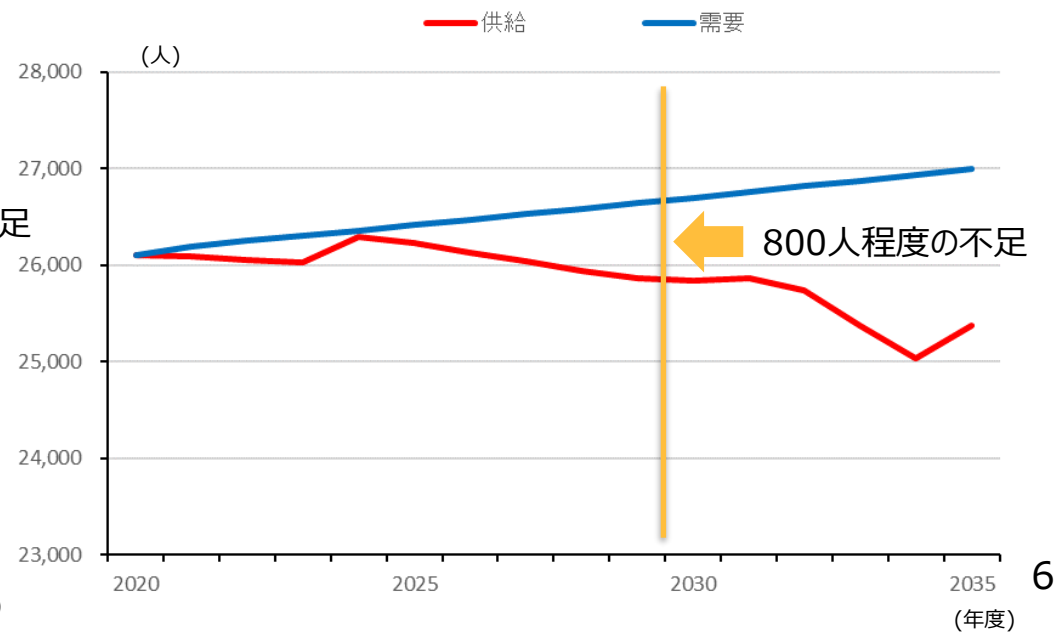
電力安全分野におけるスマート保安の必要性

- 需要設備等の高経年化や**再エネ発電設備が増加**する一方、電気保安に携わる**保安人材は減少傾向**。こうした保安人材の不足をはじめとした電力安全分野の様々な課題を克服するためには、AI、IoT、ドローン等の新たな技術を導入し、**保安力の維持・向上**と**生産性の向上を両立**する**「電気保安のスマート化」が必要**。
- スマート保安については、産業保安基本制度小委員会等において、「**保安レベルの持続的向上（保安イノベーション）を図りつつ、保安人材の枯渇の問題に早急に対処するため」、安全確保を前提に、「スマート保安の促進に向けた環境整備（政策誘導）が必要である**」とされたところ。

＜第２種電気主任技術者の需給見通し＞



＜第３種電気主任技術者（外部委託）の需給見通し＞



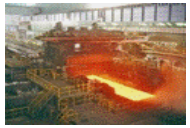
電気工作物のサイバーセキュリティの確保

- 電気保安分野における**スマート化の進展**や**再エネの導入拡大**にあわせて、**サイバーセキュリティ（以下「CS」という。）の確保も重要な課題**。
- **諸外国**においては**製鉄所、変電所等の産業施設へのサイバー攻撃**により、大規模な被害が生じており、サイバー攻撃のリスクが高まるため、CS対策の具体化を急ぐ必要がある。

諸外国における産業施設へのサイバー攻撃事例

製鉄所の溶鉱炉損傷（ドイツ、2014年）

製鉄所の制御システムに侵入し、不正操作をしたため、生産設備が損傷。



変電所へのサイバー攻撃（ウクライナ、2015年）

事務系から侵入したマルウェアCrashOverrideの感染により、変電所が遠隔制御された（数万世帯3～6時間停電）

ランサムウェア"LockerGoga"（2019年1月以降）

製造業等を標的とした新種のランサムウェア「LockerGoga」業務系システムへの攻撃が、制御系システムの運用に大きな支障をもたらす事象が発生。プラントの制御自体には支障がないものの、生産計画へのアクセスができないことによって操業を継続できないなどの被害が発生している。（ノルウェー・アルミ製造会社、アメリカ・エポキシ樹脂製造会社等）

（出展）第20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

＜産業構造審議会 産業保安基本制度小委員会 報告書（令和3年12月1日）＞

⑵サイバーセキュリティ対策

本年５月に発生した米国東部の石油パイプラインへのサイバー攻撃により、アメリカ東部の石油製品の輸送が停止した事例等も踏まえ、保安規制の見直しに際しても、サイバーセキュリティの確保が重要である。特に、各産業分野におけるスマート保安の進展や、太陽電池発電・風力発電などの再生可能エネルギー導入拡大の中で、サイバー攻撃のリスクが高まるため、サイバーセキュリティ対策の具体化を急ぐ必要がある。

１．スマート保安の推進

２．サイバーセキュリティ対策への措置
（自家用電気工作物）
(1)技術基準
(2)保安規程

３．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

従来の整理と自家用電気工作物のサイバー対策への措置

- 従来、**自家用電気工作物（発電事業の一部を除く）**については、技術基準や保安規程に基づく**CSの確保に関する義務づけがなかった**が、自家用電気工作物のスマート保安を推進していくにあたっては、**CSの確保も求めることが重要**。
- 一方で、**自家用電気工作物のCS対策**については、一般送配電事業者等を対象とした電制GLをそのまま適用するのではなく、**事業所の事業内容やサイバーリスクによる社会的影響度などを見極め**ながら、**実効性のある取組が必要**。
- そのため、**自家用電気工作物の実態を踏まえた適切なCS対策に関する新たなガイドライン**（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（以下「**自家用GL**」という。）**を策定**。

(2-1)従来の電気工作物におけるサイバーセキュリティ対策①（技術基準）

- 電気工作物のうち、**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**の用に供するものについては、**CSの確保を技術基準で義務づけ**。
- **CS対策の具体的内容は**、民間規格の**電力制御システムセキュリティガイドライン**（以下「**電制GL**」という。）**を引用**。
- なお、**発電事業については**、**電気事業用としての大手発電事業（事業者合計200万kW以上）と**、**自家用としての中小発電事業（事業者合計200万kW未満）に区分されるが**、**いずれの用に供するものも、CSの確保を技術基準で義務づけ**。

○ 電気設備技術基準省令

第15条の２　電気工作物（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ものに限る。）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。）を確保しなければならない。

○ 電気設備技術基準の解釈

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　（略）

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。

○ 技術基準における現行規制の整理

	電気事業の区分	電気工作物の区分	CS確保に係る技術基準維持の義務の有無
事業用電気工作物	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）	有
	送電事業		有
	配電事業		有
	特定送配電事業		有
	発電事業（大手）		有
	発電事業（中小）	自家用電気工作物（中小発電事業を含む）	有
	（該当なし）		無

(2-1)自家用サイバーセキュリティの規制措置（技術基準）

- このため、電気保安制度WGで議論を行い、**自家用サイバーセキュリティガイドラインを制定**し、①**電気設備技術基準・解釈（改正）**、②**保安規程の記載事項に係る内規（制定）**に紐付け、令和4年６月１０日付けで公示し、周知期間を設けるため、**令和４年10月1日付けで施行**。

＜ガイドラインの制定＞

○ **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（内規）（新規制定）**

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（内規）（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。

＜技術基準・解釈の改正＞

○ **電気設備に関する技術基準を定める省令（改正）**

（サイバーセキュリティの確保）

第15条の２　**事業用電気工作物**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（改正）**

【サイバーセキュリティ対策】（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・二　（略）

三　自家用電気工作物（発電事業の用に供するものを除く。）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。

（略）

附　則（２０２２０５３０保局第１号）

1　この規程は、令和４年１０月１日から施行する。

2　この規程の施行の際現に設置され、又は設置のための工事に着手している電気工作物についてのこの規程による改正後の電気設備の技術基準の解釈第37条の2第3号の適用については、この規程の施行後最初に行う変更の工事が完成するまでの間は、なお従前の例によることができる。

【省令改正】電気設備に関する技術基準を定める省令及びその解説について

- **第15条の2（サイバーセキュリティの確保）**

旧：電気工作物（一般送配電事業、送電事業、配電事業、特定送配電事業又は発電事業の用に供するものに限る。）の運転を管理する電子計算機は、……

↓

新：事業用電気工作物の運転を管理する電子計算機は、……

電気工作物のうち、一般送配電事業、送電事業、配電事業、特定送配電事業又は発電事業の用に供するものについては、電技省令第１５条の２に基づき、ＣＳの確保が義務づけられているが、自家用電気工作物にも対象を拡大し、全ての事業用電気工作物を対象にＣＳの確保を義務づけることとする。

【20220610_電技省令解説】

令和4年6月の改正では、サイバーセキュリティの確保義務の対象を自家用電気工作物を含む事業用電気工作物にも拡大した。これは、近年、諸外国において製鉄所等の産業施設へのサイバー攻撃も発生し、大規模な被害が生じており、また、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も踏まえ、より幅広い事業主体に対策を求めることが必要であると考えられることから、令和3年11月及び令和4年1月の**産業構造審議会保安・消費生活用製品安全分科会電力安全小委員会電気保安制度WG（第8回及び第9回）**において、自家用電気工作物についてもサイバーセキュリティの確保が重要とされたためである。

[R4改正点] 対象となる電気工作物を自家用電気工作物を含む事業用電気工作物に拡大した**（令和4年10月1日付けで施行）**。

※第15条の2、18条、44条、46条、48条、50条において、令和4年4月1日付けで**配電事業の追加**に伴う解説の追記あり。

【内規改正】電気設備の技術基準の解釈及びその解説について

- **第37条の2（サイバーセキュリティの確保）**

旧：（新設）

新：三　自家用電気工作物（発電事業の用に供するものを除く。）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。

【20220610_電技解釈解説】

第三号は、自家用電気工作物（発電事業の用に供されるものを除く。）に係るサイバーセキュリティの確保に関して示したものである。近年、諸外国においては製鉄所等の産業施設へのサイバー攻撃も発生し、大規模な被害が生じており、また、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も踏まえ、より幅広い事業主体に対策を求めることが必要である。

そのため、令和3年11月及び令和4年1月の**産業構造審議会保安・消費生活用製品安全分科会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とし、**令和4年10月より施行**することとした。

(2-2)従来の電気工作物におけるサイバーセキュリティ対策（保安規程）

- 事業用電気工作物のうち、**一般送配電事業**、**送電事業**及び**大手発電事業**の用に供するものついては、**保安規程へのCSの確保に関する記載を内規で義務づけ**。
- **保安規程に記載する具体的内容は**、民間規格の**電制GLを引用**。
- なお、**発電事業については**、**電気事業用としての大手発電事業（事業者合計200万kW以上）の用に供するもののみ、社会的影響を考慮し、保安規程へのCSの確保に関する記載を内規で義務づけ**。

○ 電気事業法施行規則第50条第２項の解釈適用に当たっての考え方（内規）

（前略）発電事業（法第３８条第３項第５号に掲げる事業に限る。以下同じ。）（中略）一般送配電事業、送電事業又は発電事業の用に供する事業用電気工作物の設置者（以下「事業者」という。）の定める保安規程については、省令第50条第２項に掲げる事項について記載することが求められ、自主保安活動を行う上での基本的なルールを事業者自らの責任において適切に定めるべく、下記のように記載されることが必要である。（後略）

記１．～１１．（略）

１２．第１５号(その他保安上必要な事項)

十五 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

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。）を確保するため、次の各号により適切な措置が講じられることが必要である。

一　（略）

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（2016）「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。

また、本号は前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事業者の判断により必要となるものについて記載することを想定した規定である。

○ 保安規程における現行規制の整理

	電気事業の区分	電気工作物の区分	CS確保に係る保安規程記載の義務の有無
事業用電気工作物	一般送配電事業	電気事業法第38条第３項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）	有
	送電事業		有
	配電事業		有
	特定送配電事業		無
	発電事業（大手）		有
	発電事業（中小）	自家用電気工作物（中小発電事業を含む）	無
	（該当なし）		無

(2-2)自家用サイバーセキュリティの規制措置（保安規程）

＜保安規程内規の制定＞

○ 電気事業法施行規則第50条第３項の解釈適用に当たっての考え方（内規）（新規制定）

電気事業法（昭和３９年法律第１７０号。以下「法」という。）第４２条第１項に規定する保安規程（以下「保安規程」という。）の記載事項については、電気事業法施行規則（平成７年通商産業省令第７７号。以下「省令」という。）**第５０条第１項において、**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３８条第３項第５号に掲げる事業に限る。）の用に供するものと、**それ以外の事業用電気工作物（すなわち、特定送配電事業又は発電事業（法第３８条第３項第５号に掲げる事業以外のものに限る。以下同じ。）の用に供する事業用電気工作物及び自家用電気工作物（発電事業の用に供するものを除く。以下同じ。））に区分**し、保安を一体的に確保することが必要な組織ごとに定めることとしている。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及び自家用電気工作物の設置者の定める保安規程については、省令第５０条第３項に掲げる事項について記載することが求められ、自主保安活動を行う上での基本的なルールを設置者自らの責任において適切に定めるべく、同項第９号について下記のように記載されることが必要である。
なお、本内規に定める保安規程の記載事項は、経済産業省が、本内規の制定時において、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及び自家用電気工作物の保安確保に必要と考える標準的記載事項である。

記

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）
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（※2）
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。

○ 保安規程における現行規制

	電気事業の区分	電気工作物の区分	CS確保に係る保安規程記載の義務の有無
事業用電気工作物	一般送配電事業	電気事業法第38条第３項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）	有
	送電事業		有
	配電事業		有
	特定送配電事業		無 ※１
	発電事業（大手）		有
	発電事業（中小）	自家用電気工作物（中小発電事業を含む）	無 ※１
	（該当なし）		無 ※２

（注）保安規程に係る規制対象については、自家用電気工作物を追加することに併せ、現行規制で対象外となっていた特定送配電事業及び発電事業の一部も追加することとする。

【内規制定】電事法施行規則第50条第３項第９号の解釈適用に当たっての考え方について

- **施行規則第50条（保安規程）**

  第3項第九号（その他保安上必要な事項）

  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

参考として以下の用に保安規程の条文に記載し、詳細は社内規定やマニュアル等で定めることを推奨する。
また、自家用ＧＬ第２－２条よりセキュリティ管理責任者を設置するようにしているため、保安規程別表の体制図において、どの役職・立場の人がセキュリティ管理責任者か明記することも推奨する。

【保安規程記載例】

第○章　電気工作物の巡視、点検、検査及びサイバーセキュリティの確保

○条（サイバーセキュリティの確保）

　電気工作物の保安を確保するため、「自家用ＧＬ」及び「○○マニュアル等別で定めるもの」に基づき、サイバーセキュリティの確保のための適切な処置を講ずる。

１．スマート保安の推進

２．サイバーセキュリティ対策への措置
（自家用電気工作物）
(1)技術基準・解釈
(2)保安規程

３．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

（３）自家用電気工作物サイバーセキュリティガイドラインの考え方

- 自家用GLの内容は、**電制GLを引用**するものの、**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GLでは、各項目の要求レベルは、**実施すべき「勧告」**と、**自らが実施の要否及び実施方法を判断する「推奨」**の**２種類に区分**されているが、自家用GLでは、**「推奨」レベルを基本**とした。
- 自家用GLの解説では、**サイバーリスクによる社会的影響度などを勘案**して、それぞれの**実状に応じたCS対策が取れるように、ベースを推奨とし、最低限の勧告を書き分けた**。
- 自家用GLの活用にあたっては、**自家用電気工作物設置者や電気主任技術者等のみの対応でなく、**CS対策を専門とする**事業者への委託も可能。**

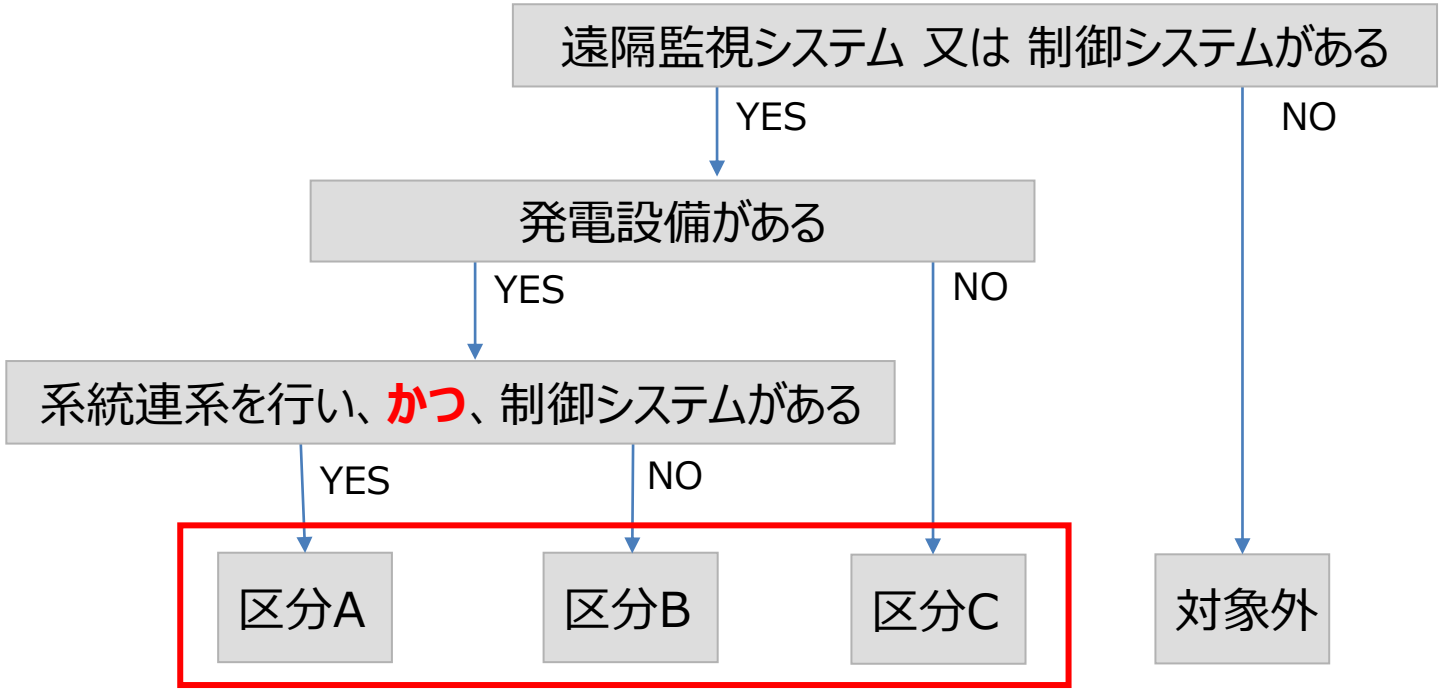
○ **自家用GLの活用者（適用先）**

- 自家用電気工作物の保安管理の責任は、原則的には設置者が担っていることを踏まえ、**本ガイドラインは基本的には設置者に対して提示**。
- 記載事項を参考とした**具体対策の実装は、電気主任技術者やベンダー、サイバーセキュリティの専門家等の監督・支援の下、設置者が実施（又は実施を委託）することを想定**。そのため、電気主任技術者等における活用のしやすさを考慮して作成。また、そのような想定を「まえがき」等にて明示。
- 対象となる自家用電気工作物は、**設置者、保安管理担当者（外部委託先）、遠隔監視サービス提供者等、複数の事業主体が関係**する。これら複数の関係者が運用する機器・システムが本ガイドラインの対象となることをガイドライン中の「まえがき」、「適用範囲」、「システム構成」等にて明示。

自家用サイバーセキュリティ規制の対象システムの考え方

- ガイドラインの対象システムは、サイバー攻撃やサイバーセキュリティ確保の管理不良により、**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、制御システム等**とする。
- また、ガイドラインの対象者は、**それらのシステム及び付随するネットワークを使用する者（設置者、保守点検を行う事業者（外部委託の保安管理業務受託者を含む）、遠隔サービス提供事業者などを想定）**とする。
- 対象となるシステムについては、系統連系における電力系統への影響に応じて、**区分A～Cに分類され、区分により勧告又は推奨となるガイドラインの条項がある。**

＜自家用サイバーセキュリティ規制の該当性確認のフロー＞



自家用サイバーセキュリティガイドラインは区分によって対策事項（レベル）を差別化

【内規制定】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について

- **第1－3条（対象となるシステムの区分）**

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**

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。

発電設備：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等

発電設備以外の設備：需要設備の受配電設備等

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（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）

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

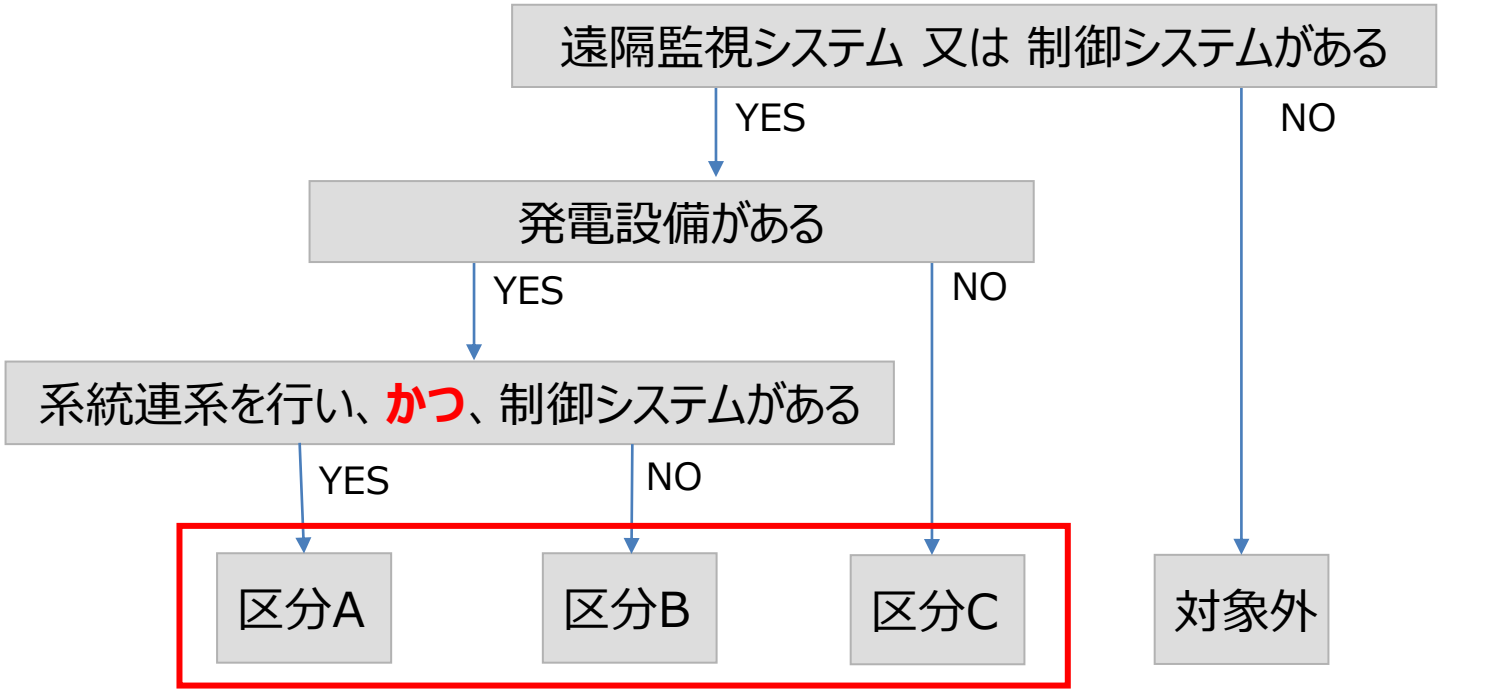
【内規制定】自家用電気工作物に係るサイバーセキュリティの確保に関するガイドラインについて

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**

＜自家用サイバーセキュリティ規制の該当性確認のフロー＞



自家用サイバーセキュリティガイドラインは区分によって対策事項（レベル）を差別化

【内規制定】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について

● 第1－1条（目的）

自家用電気工作物（発電事業の用に供するものを除く。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。

- **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）

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。

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。

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。

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。

【内規制定】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について

- **第1－3条（対象となるシステムの区分）**
- **第1－4条（想定脅威）**

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、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。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。

想定され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。

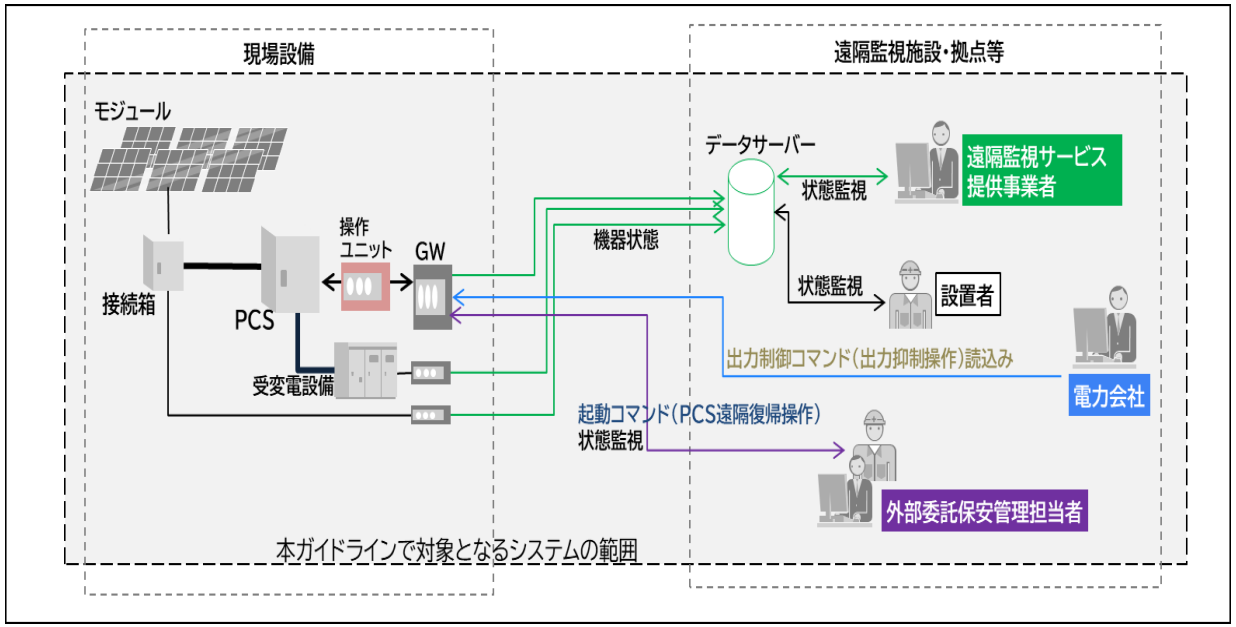


図2：発電設備の保安管理業務を外部委託する場合の対象システムの範囲の例（発電設備の出力制御コマンドが系統接続先の電力会社から別のシステムを介して伝達される例）

【内規制定】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について

- **第2－1条（体制）【区分Ａ：すべて勧告的事項】**

1．経営層の責任：設置者の経営層は、セキュリティの確保について責任を負うこと。

2．管理組織の設置：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。

3．目的の明確化：そのセキュリティの実施目的を明確にすること。

1．**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。

2．**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。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。

3．**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。

【内規制定】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について

● 第2－2条（役割）【区分Ａ：1.のみ勧告的事項】

1．経営層の責任：設置者は、セキュリティ管理責任者を任命すること。

2．役割の定義：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。**

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。

● 第2－3条（セキュリティ教育）

1．教育の計画・実施

2．教育効果の確認

1．**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。

2．**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。

【内規制定】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について

- **第6－2条（ネットワークの管理）【区分Ａ：2.3.のみ勧告的事項】**

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。**

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。**

２．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

３．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。

- **第8－1条（システムの管理）【区分Ａ：3.のみ勧告的事項】**

３．外部記憶媒体等のマルウェア対策：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。**

３．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。

【内規制定】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について

● 第10－1条（情報の収集）

セキュリティ事故の**対応に必要な情報**を収集すること。

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。

● 第10－2条（セキュリティ事故の対応体制等）

セキュリティ事故の**対応体制**と**手順**を明確にすること。

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。

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。

【内規制定】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について

● 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：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。**

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。

1．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。

● 第10－4条（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**定期的に行うこと。**

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。

サイバーセキュリティ対策のため、まず何を行うべきか

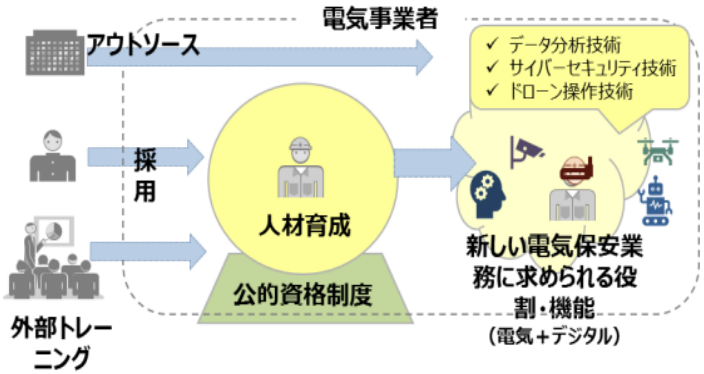
- サイバー攻撃による被害を回避し、軽減するため、具体的には、次のようなサイバーセキュリティ対策が考えられます。
  - ✓ 機器における対策：
    ウィルス対策ソフトの導入及び定期的なウィルスチェック、OS等の最新化、USBポート等の使用制限・物理的施錠など
  - ✓ 通信における対策：
    ネットワークの閉域網化、ネットワークの監視（FW、IPS/IDS、WAF等）、通信の暗号化、他ネットワークとの接続点の最小化、接続点の防御措置など
  - ✓ 運用面での対策：
    アカウントの制限、アクセス端末の制限、セキュリティマニュアルの整備など
  - ✓ 物理的な対策：
    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
- サイバーセキュリティ対策について不明な点があれば、システム構築事業者（SI）や、サイバーセキュリティ専門事業者へ相談することを推奨します。 また、「IT導入補助金」の制度を活用してサイバーセキュリティお助け隊サービス制度等も積極的にご活用ください。

サイバーセキュリティ対策は設置者責任となります。上記はあくまで一例であり、設備や事業者によって様々なリスクが存在するため、想定される被害を洗い出し、責任の所在を明確にし、セキュリティ管理責任組織と連携をとりながらそれぞれにあった対策を講じていただくようお願いいたします。また、赤字の対策例は特に重要であるため、積極的にご検討いただくようお願いします。

自家用サイバーセキュリティ規制に向けた周知及び人材育成の取組

- 自家用電気工作物におけるサイバーセキュリティ規制を適正に執行するためには、設置者や電気主任技術者等への制度の周知が必要。
- また、各設置者に対して、民間が実施する**サイバーセキュリティに関する研修**（例：第四次産業革命スキル習得講座【経産省経済産業局産業人材課】）を活用を慫慂する。
- なお、**サイバーセキュリティ対策の実施**については、設置者、外部委託先の事業者等が自ら実施することが困難な場合は**委託**も可能である。

<デジタル人材育成の取組>



<第四次産業革命スキル習得講座認定制度>

IT・データを中心とした将来の成長が強く見込まれ、雇用創出に貢献する分野において、社会人が高度な専門性を身に付けキャリアアップを図る、**専門的・実践的な教育訓練講座を経済産業大臣が認定**する制度。
「専門実践教育訓練給付制度」と連携し、**訓練経費及び訓練中の賃金の一部を助成**。

Reスキル

出所）**電気保安分野 スマート保安アクションプラン / 電気保安分野 スマート保安アクションプランの概要**
https://www.meti.go.jp/shingikai/safety_security/smart_hoan/denryoku_anzen/20210430_action_plan.html

<外部研修の例（第四次産業革命スキル習得講座認定制度）>

No.	申請者（法人名）	講座名
1	シーティーシー・テクノロジー株式会社	セキュリティエンジニア養成講座
2	ネットワンシステムズ株式会社	CSIRT能力向上研修
3	ヒートウェーブ株式会社	サイバーセキュリティ技術者育成コース
4	大日本印刷株式会社	サイバー・インシデントレスポンス・マネジメントコース 基礎演習
5	大日本印刷株式会社	サイバー・インシデントレスポンス・マネジメントコース 実践演習
6	大日本印刷株式会社	サイバー・インシデントレスポンス・マネジメントコース 実践演習II
7	大日本印刷株式会社	サーティファイド・サイバー・オフェンス・プロフェッショナルコース
8	大日本印刷株式会社	サイバー・インシデントレスポンス・マネジメントコース 産業制御系・基礎
9	一般社団法人高度ITアーキテクト育成協議会	AITAC集中セミナー
10	株式会社バルクホールディングス	CYBERGYM's Zero to Hero
11	ヒートウェーブ株式会社	ホワイトハッカー育成コース
12	株式会社デジタルハーツ	DH・CyberBootCamp
13	一般社団法人JAIST支援機構	IoTセキュリティ実践講座（RESION2）
14	一般社団法人JAIST支援機構	サイバーセキュリティ実践（RECS）
※	株式会社グローバルテクノ	ISMS審査員研修コース

出所）https://www.meti.go.jp/policy/economy/jinzai/reskillprograms/pdf/kouzaichiran.pdf

参考

経産省商務情報政策局サイバーセキュリティ課では、サイバーセキュリティに関する取り組みを行っており、インシデント発生時の整理しておくべき事項や体制構築・人材確保の手引きについてガイドラインを定めております。

また、中小企業を対象とした「ＩＴ導入補助金」という制度もあり、情報処理推進機構ＩＰＡの**「サイバーセキュリティお助け隊サービス制度」**という事業も補助金対象となっておりますので、対象となる企業はぜひご活用ください。

https://www.meti.go.jp/policy/netsecurity/mng_guide.html

https://www.meti.go.jp/policy/netsecurity/sme-guide.html

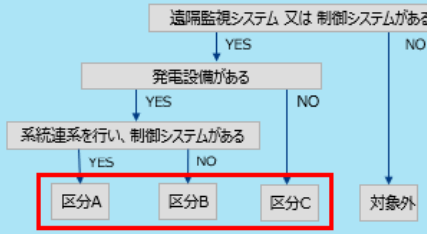
https://www.it-hojo.jp/security/

周知用のリーフレット

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制定について

電気保安分野におけるスマート化の推進や再エネの導入拡大に合わせて、**自家用電気工作物（発電事業の一部を除く）に対し、令和4年10月1日より、サイバーセキュリティ（CS）の確保と保安規程への記載を求める**こととしました。
それに伴い、技術基準省令・解釈の改正及び「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）」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（内規）」を制定しました。
https://www.meti.go.jp/policy/safety_security/industrial_safety/oshirase/2022/06/20220610.html

＜自家用サイバーセキュリティ規制の該当性確認のフロー＞



ガイドラインの対象システムは、サイバー攻撃やCS確保の管理不良により、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、制御システム**等とします。

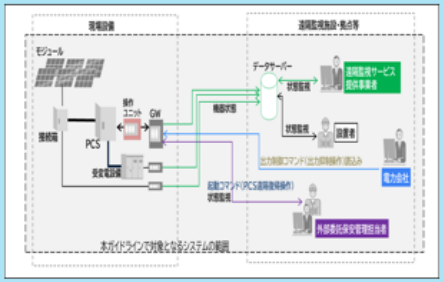
区分A～Cに応じて、CS対策の義務（勧告的事項）と推奨（推奨的事項）に分けられており、対策事項（レベル）を基本推奨的事項とし、最低限の基準として区分Aのみ一部勧告的事項がございます。

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。

詳しくは裏面をご覧ください。

経済産業省

本ガイドラインの適用範囲は、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**に適用します。



＜これらに携わる者の具体例＞

- 設置者
- 保安管理業務の外部委託の受託者
- 系統接続先の電力会社
- 遠隔監視サービス提供事業者など

セキュリティ管理責任組織を構築

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、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
- サイバーセキュリティ対策について不明な点があれば、（独）情報処理推進機構（IPA）や、サイバーセキュリティ専門事業者へ相談することを推奨します。

○○	○○産業保安監督部 電力安全課	00-0000-0000