

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10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

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

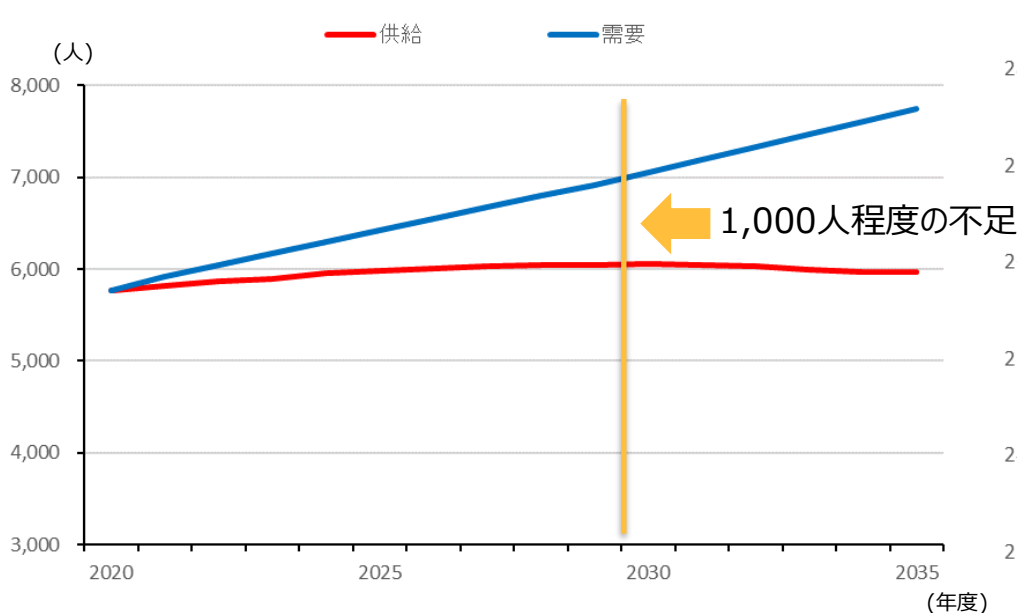
(2) 保安規程

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

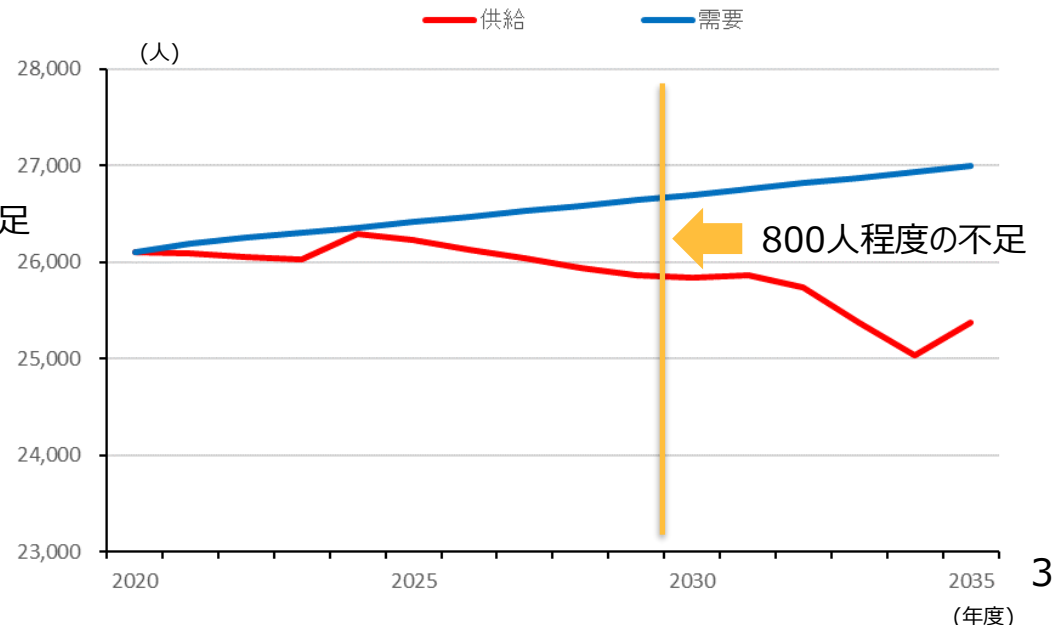
電力安全分野におけるスマート保安の必要性

- 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）

＜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）＞

(2)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。

（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

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 (<u>大手発電事業を含む</u>)	有
	送電事業		有
	配電事業		有
	特定送配電事業		有
	<u>発電事業</u> (大手)		有
	(該当なし)	自家用電気工作物 (<u>中小発電事業を含む</u>)	有
			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については、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。**

また、自家用G L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】

第〇章 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

〇条（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G L」及び「〇〇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。

※技術基準で定めている電子計算機がない電気工作物については、技術基準の適用を受けないので記載は不要。

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。**

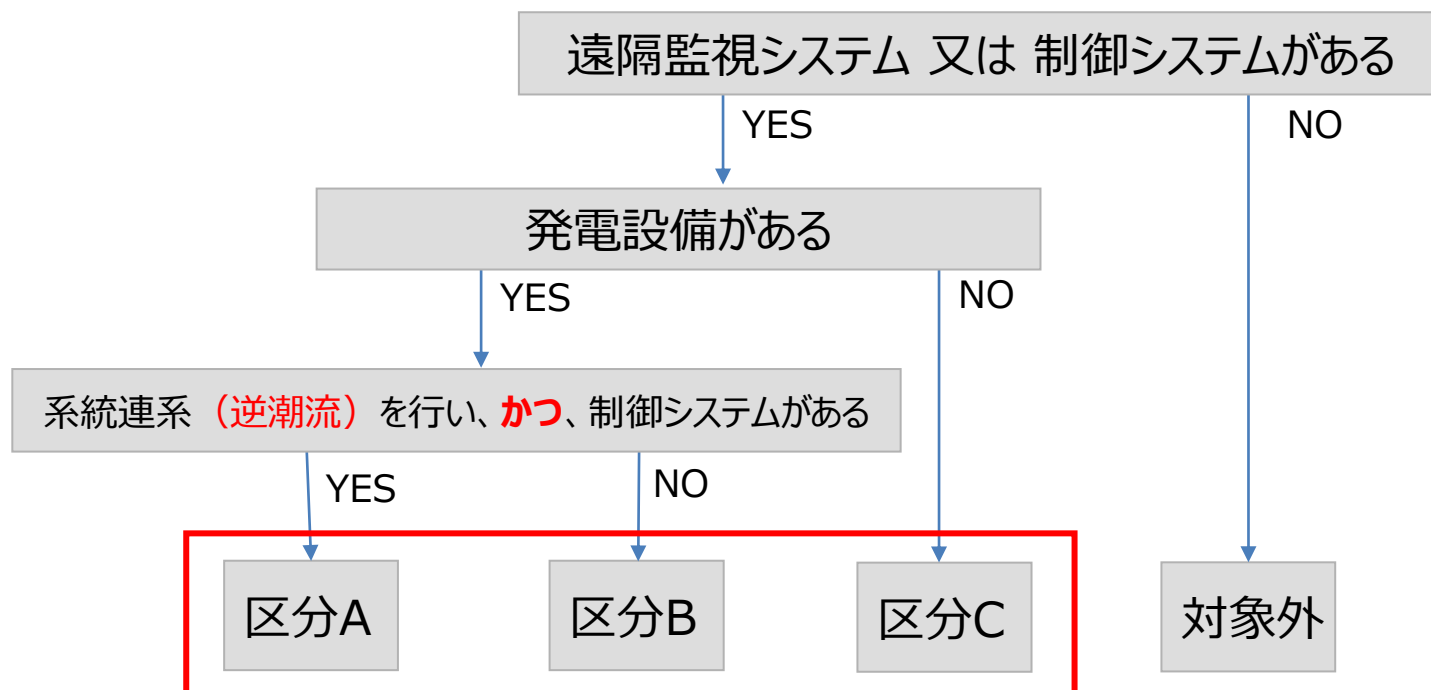
○ 自家用GLの活用者（適用先）

- 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

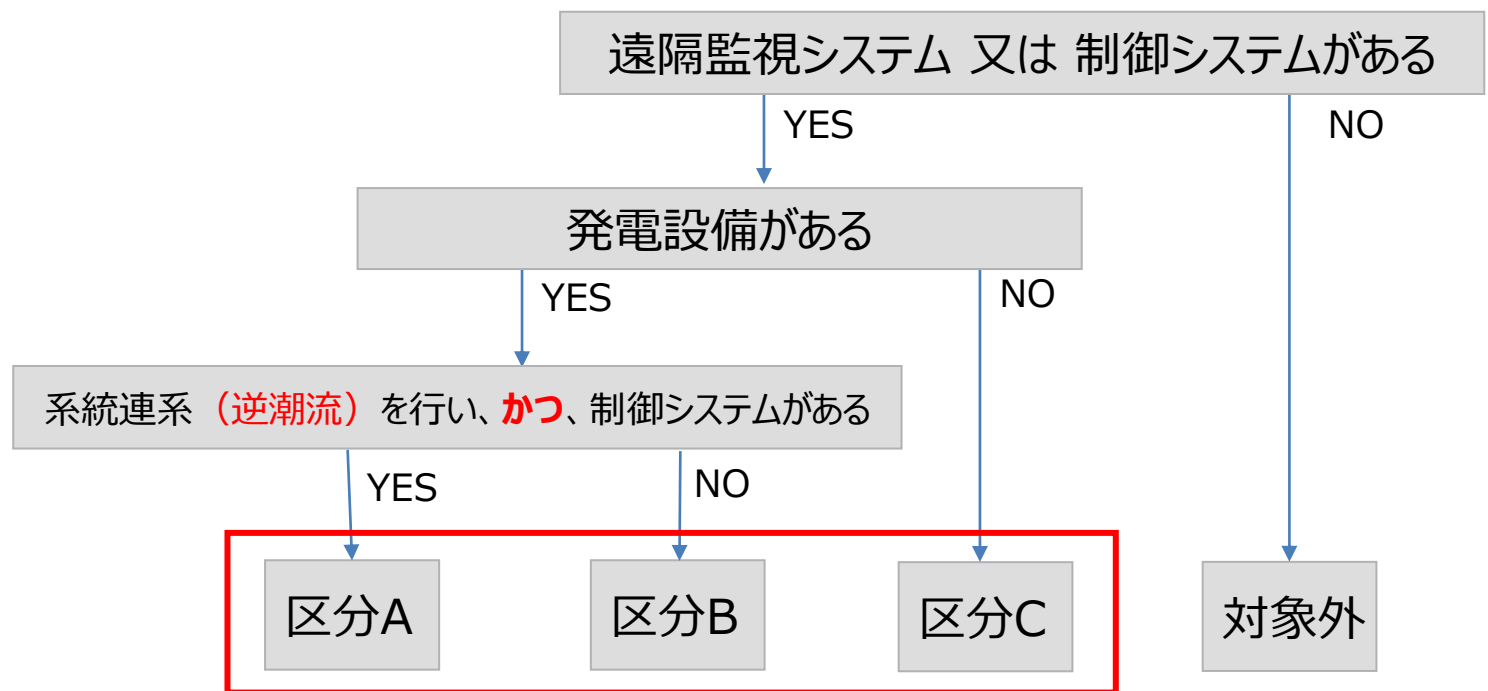
遠隔監視システム：自家用電気工作物の運転状況や構成設備の状態を、ネットワークを介して監視することができるもの（運転状況や構成設備の状態を監視するための機器を制御する機能を有する場合もあるが、発電した電気や使用するための電気の電路に施設された遮断器、開閉器の開閉操作等を行うことができないもの）

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つ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)

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。

このすべてが設置者責任で自家用GLの対象となりますが、保守点検を行う事業者、電力会社、遠隔サービス提供事業者等と設置者との間で、責任の所在を明確にすれば、設置者は設置者責任となる範囲の対策を講じることで問題ありません。

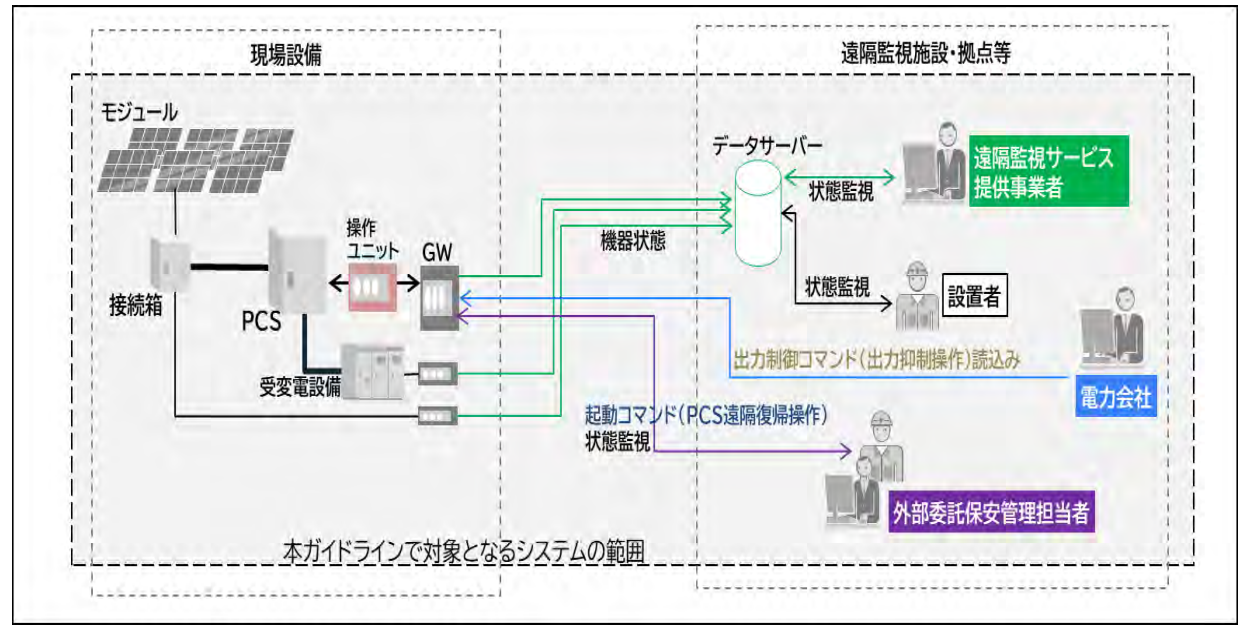


図2：発電設備の保安管理業務を外部委託する場合の対象システムの範囲の例（発電設備の出力制御コマンドが系統接続先の電力会社から別のシステムを介して伝達される例）

【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1－5条（用語の定義）

(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。**

(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。**

(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。

(1)「遠隔監視システム」、(4)「制御システム」は、自家用電気工作物の**保安の確保に資するためのシステム**をいうため、**保安の確保に資さないデマンド監視等は対象外**。
また、**ネットワークを介して**情報の通信ができるものが対象となる。（**絶縁監視装置は対象**）

(15)「サイバー攻撃」は、施設内部への**物理的な侵入による攻撃や内部不正**も含むため、インターネット等の外部と接続されていない**同一構内で完結するネットワークであっても対象**となる。

サイバーセキュリティ対策のため、まず何を行うべきか

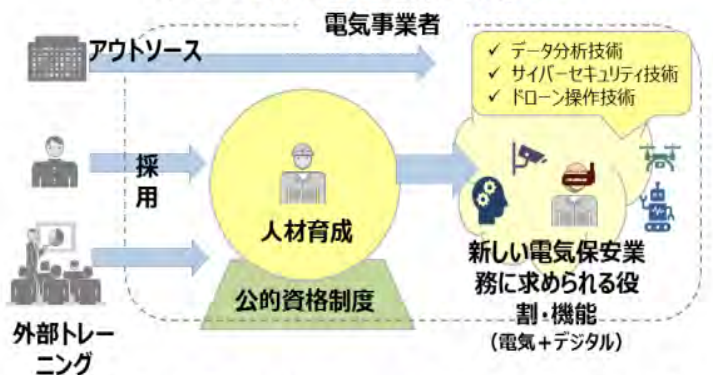
- サイバー攻撃による被害を回避し、軽減するため、具体的には、次のようなサイバーセキュリティ対策が考えられます。
 - ✓ **機器における対策:**
ウイルス対策ソフトの導入及び定期的なウイルスチェック、OS等の最新化、USBポート等の使用制限・物理的施錠など
 - ✓ **通信における対策:**
ネットワークの閉域網化、ネットワークの監視(FW、IPS/IDS、WAF等)、通信の暗号化、**他ネットワークとの接続点の最小化、接続点の防御措置**など
 - ✓ **運用面での対策:**
アカウントの制限、アクセス端末の制限、セキュリティマニュアルの整備など
 - ✓ **物理的な対策:**
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

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】）を活用を奨励する。
- 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。



<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	ネットワークシステムズ株式会社	CSIRT能力向上研修
3	ヒートウェブ株式会社	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

参考

IT導入補助金2022

セキュリティ対策推進枠について

デジタル化の促進策（8割助成IT導入促進）について

gBizID

過去5か年のサービス等生産性向上IT導入支援事業について

IT事業者ポータル

申請マイページ

IT導入補助金について

事業概要

スケジュール

申請・手続きフロー

中小企業・小規模事業者のみなさま

ITベンダー・サービス事業者のみなさま

関連資料・動画等

目録から探す

中小企業・小規模事業者等のみなさまへ

セキュリティ対策推進枠の公募を開始しました

IT導入支援事業者を募るとい

IT導入支援事業者を募った差額な事業者にご注意ください

【交付申請_セキュリティアクションアカウントID入力画面のシステムメンテナンスのお知らせ】

これから申請をされる皆様へ：補助金の不正受給に関する注意喚起

※重要※ IT導入支援事業者を募った差額な事業者にご注意ください

gBizIDの事前取得について

IPA Better Life with IT 情報処理推進機構

HOME 情報セキュリティ 産業サイバーセキュリティセンター 社会基盤センター 未踏/セキュリティキャンプ IT人材の育成

情報セキュリティ

サイバーセキュリティお助け隊サービス制度

最終更新日：2023年6月21日
独立行政法人情報処理推進機構
セキュリティセンター 企業部
中小企業支援グループ

「サイバーセキュリティお助け隊サービス」とは？

「サイバーセキュリティお助け隊サービス」は、中小企業のサイバーセキュリティ対策に不可欠な各種サービスをワンパッケージで安価に提供するサービスです。

ぜひユーザー向けサイトもご覧ください。活用もご検討ください！

ユーザー向けサイトはこちら

IT導入補助金 で「サイバーセキュリティお助け隊サービス」のサービス利用料が支援対象となります！

脆弱性対策情報

届出・相談・情報提供

特集コンテンツ

情報セキュリティ啓発

情報セキュリティ対策

番号成程

セキュリティエコノミクス

情報セキュリティ認証関連

ISMAP

セミナー・イベント

資料・報告書・出版物

ツール

サポートデスク

セキュリティセンターについて

サイバー情報共有イニシアティブ (I-CSDP)

サイバーレスキュー隊 (I-CSDP)

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>

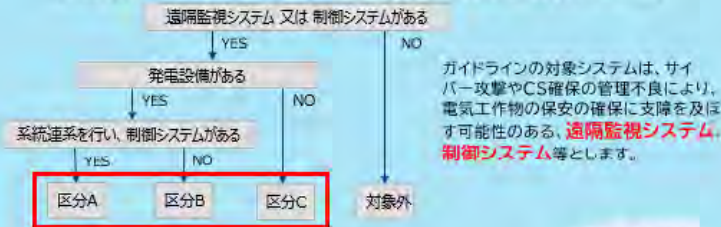
<https://www.it-hojo.jp/security/>

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>



できることから
1歩ずつ!

詳しくは裏面をご覧ください。

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。

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:**
ウイルス対策ソフトの導入及び定期的なウイルスチェック、OS等の最新化、USBポート等の使用制限・物理的施設など
 - ✓ **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、接続点の防衛措置など
 - ✓ **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。