経済産業省

資料３

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３年３月２２日

産業保安グループ　電力安全課

１．検討の経緯等

- **電気事業※の用に供する電気工作物**の運転を管理する電子計算機については、**技術基準においてサイバーセキュリティの確保を義務づけ。**また、一部の事業者を除き、**保安規程においても、サイバーセキュリティの確保を規定し、その遵守を義務づけ。**

  ※一般送配電事業、送電事業、特定送配電事業及び発電事業を指す。以下同じ。

- **サイバーセキュリティ対策の具体例として、技術基準及び保安規程とともに、日本電気技術規格委員会規格（JESC）のガイドライン（スマートメーターシステムセキュリティガイドライン（GL）、電力制御システムセキュリティGL）を取りあげている。**

- 一方、**自家用電気工作物のサイバーセキュリティの確保**については、一部の事業者を除き、**技術基準や保安規程による義務づけは行われていないところ。**

- 今後、**自家用電気工作物におけるスマート化**（通信回線等を用いた遠隔での監視制御等）**の進展**により、自家用電気工作物についても**サイバー攻撃の対象となる可能性も増大する**ことから、**サイバーセキュリティの確保**は不可欠。

- これまで、**自家用電気工作物に対するサイバー攻撃の認識や、サイバー攻撃による被害想定、必要なサイバーセキュリティ対策**などについて、事業者や電気保安関連団体の**電気主任技術者等**へインタビューを実施。

- 今回のWGでは、これまでの検討状況を整理し、**今後の進め方について御議論いただきたい**。

（参考）自家用電気工作物とは

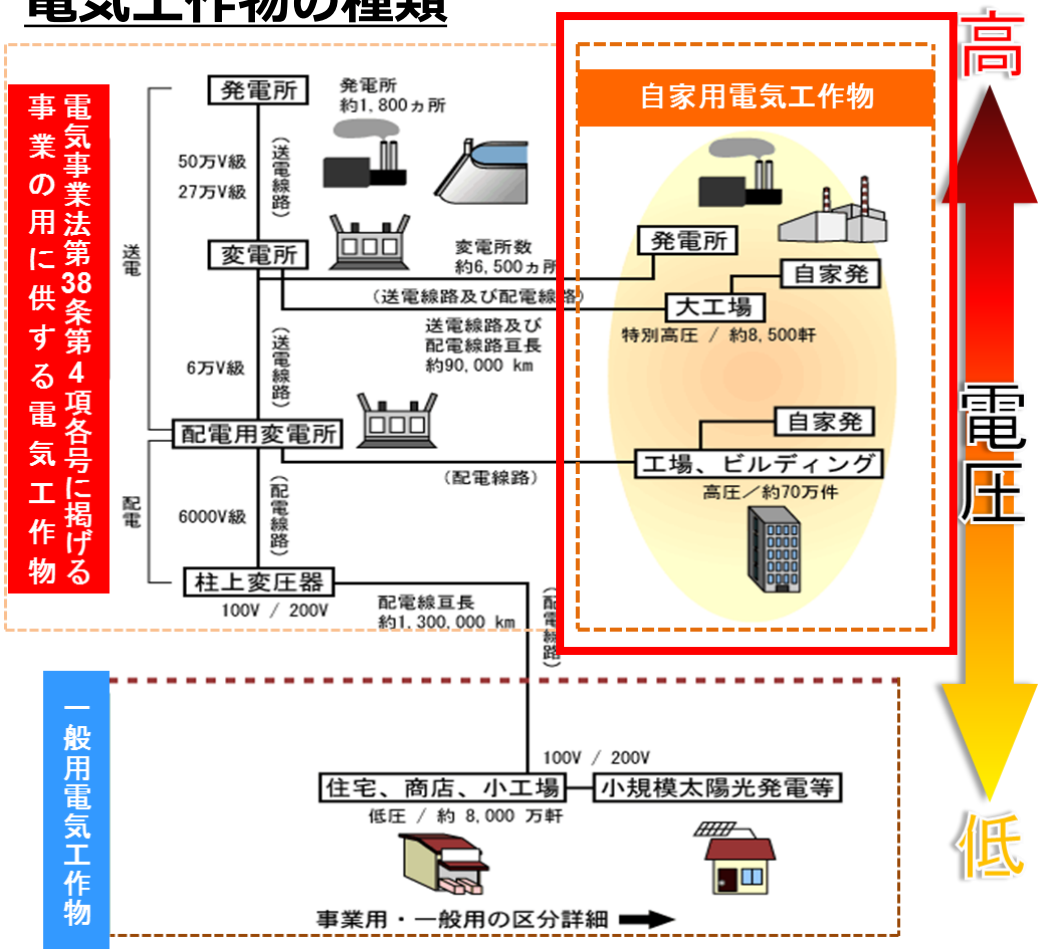
- 自家用電気工作物は、一般用電気工作物及び電気事業(一部を除く)の用に供する電気工作物以外の電気工作物。
- 具体的には、一般送配電事業者から**高圧及び特別高圧で受電するビルや工場**、小出力発電設備以外の**発電設備など**。

自家用電気工作物に該当する設備

- 600Vを越える電圧で受電する設備（ビル、工場など）
- 出力50kW以上の太陽電池発電設備
- 出力20kW以上の風力発電設備
- 出力10kW以上の内燃力発電設備
- 構外にわたる電線路を有する電気設備

など

電気工作物の種類



2．電気事業者に対する技術基準の維持（法令規程）

- 技術基準では、電気事業の用に供する電気工作物の運転を管理する電子計算機について、「サイバーセキュリティの確保」を義務づけている。

電気設備に関する技術基準を定める省令（平成９年通商産業省令第52号）

（サイバーセキュリティの確保）
第15条の２　**電気工作物（一般送配電事業、送電事業、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**。

電気設備の技術基準の解釈（20130215商局第４号）

（サイバーセキュリティの確保）
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。
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。

3．電気事業者に対する保安規程への記載（法令規程）

- 一部の事業者を除き、電気事業者が保安規程で定めるべき項目については、電気事業法施行規則第50条第2項において定められており、その解釈については、「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）」（保安規程内規）に規定されている。

電気事業法施行規則（平成７年通商産業省令77号）

（保安規程）
第50条　（略）
　一　事業用電気工作物であって、一般送配電事業、送電事業又は発電事業（法第38条第４項第４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
　二　（略）
２　前項第一号に掲げる事業用電気工作物を設置する者は、法第42条第１項の保安規程において、次の各号(その者が発電事業(その事業の用に供する発電用の電気工作物が第48条の２第１号に掲げる要件に該当するものに限る。)を営むもの以外の者である場合にあっては、第五号から第七号まで及び第十一号を除く。)に掲げる事項を定めるものとする。
　一～十四　（略）
　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

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）（20160905商局第２号）

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　**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（2016）「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。
　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。

4．電気事業者に対するGL（民間規程）

- 日本電気技術規格委員会（JESC）規格では、**「スマートメーターシステムセキュリティGL」及び「電力制御システムセキュリティGL」によって、サイバーセキュリティの確保に関する具体的な事項を定めている。**当該規格については、電気設備の技術基準の解釈及び保安規程内規において、技術基準等の省令に規定する要件を満たす具体例として取りあげられている。
- 「スマートメーターシステムセキュリティGL」は、一般送配電事業に適用。
- 「電力制御システムセキュリティGL」は、一般送配電事業、送電事業、特定送配電事業及び発電事業に適用。

スマートメーターシステム セキュリティガイドライン

（共通事項）
■ セキュリティ管理組織の設置及びマネジメントシステムの構築、教育の実施等を記載。

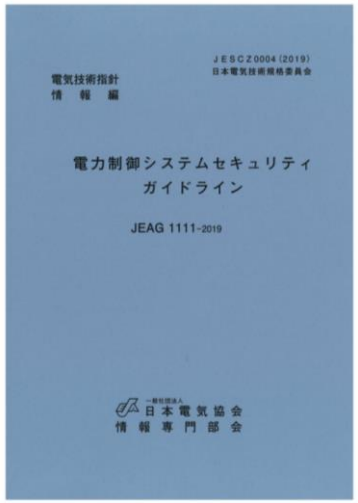
機器	・セキュリティ仕様　・ファームウェアアップデート
通信	・通信プロトコル　・暗号　・ネットワーク分離
システム	・コマンド管理　・外部記憶媒体利用制限
運用	・管理者権限管理　・ログ取得　・データ管理
物理	・セキュリティ区画保護　・アクセス管理

電力制御システム セキュリティガイドライン

設備・システム	・ネットワーク分離　・通信データ保護 ・不正処理防止　・アクセス制御
運用・管理	・セキュリティ仕様　・データ管理 ・管理者権限割当　・セキュリティパッチ

安定供給の観点から、システムの重要度を定義
↓
重要度に応じた追加的なセキュリティ対策を提示

・ログの取得　・入退管理



5．自家用電気工作物のサイバーセキュリティに関するインタビュー結果

- 自家用電気工作物（太陽電池発電所や需要設備）の保安の監督を担う電気主任技術者等※に対し、サイバーセキュリティの認識等についてインタビューを実施。※スマート化実証試験中の事業者・団体等９者
- **太陽電池発電所においては、**遠隔でのPCSの制御により発電も制御が可能。仮に、サイバー攻撃を受けた場合、小型であっても**多数の太陽電池発電所が同時にサイバー攻撃を受け発電停止した場合**、需給バランスが乱れることにより、**当該地域の系統に影響を与える可能性**、との意見。よって、**太陽電池発電所や風力発電所等についても、サイバーセキュリティの確保が重要**になるのではないか。
- 需要設備においては、遠隔監視データの改ざんや通信妨害等により、異常を発見できず、長期的には設備故障や重大事故等に繋がる可能性があり、個々の設備において電力供給に支障を生じる可能性、との意見。

＜自家用電気工作物の電気主任技術者等へのインタビュー結果＞

太陽電池発電所	需要設備
✓ 発電量監視やPCS設備故障警報の監視、PCSの遠隔復帰操作を既に導入。 ✓ 通信妨害やデータ改ざんによる異常の見落とし等による事故のリスクが考えられる。 ✓ PCSの遠隔操作を導入しているため、意図せず発電停止するリスクが考えられる。	✓ 低圧電路の絶縁監視装置が既に導入されているが、サイバー攻撃の被害は、確認できず。 ✓ 将来的に、月次点検を代替するための遠隔監視装置を設置をした場合、通信妨害やデータ改ざんによる異常の見落とし等による事故発生のリスクが考えられる。

6．自家用電気工作物に対するサイバーセキュリティGL（仮称）の検討

- **自家用電気工作物のサイバーセキュリティ対策の具体的内容の検討**にあたっては、既に電気事業用のサイバーセキュリティ対策として普及している「**電力制御システムセキュリティGL」を参考**として、**スマート化技術の動向**や多くの設置者が属する**中小企業等の取組の実態・実効性の確保等を考慮しながら、検討を進めるべき**ではないか。

（参考）電力制御システムセキュリティGLの要件（目次より一部抜粋）

項目名		勧告／推奨※
第2章　組織	第2-1条　体制	勧告
	第2-2条　役割	勧告
	第2-3条　セキュリティ教育	勧告
第3章 文書化	第3-1条　文書管理	勧告
	第3-2条　実施状況の報告	勧告
第4章 セキュリティ管理	第4-1条　セキュリティ管理	勧告
第5章　設備・システムのセキュリティ	第5-1条　外部ネットワークとの分離	勧告
	第5-2条　他ネットワークとの接続	勧告
	第5-3条　通信のセキュリティ	推奨
	第5-4条　機器のマルウェア対策	推奨
	第5-5条　不正処理防止策	推奨
	第5-6条　アクセス制御	推奨
	第5-7条　ログの取得（重要度がS（※）の電力制御システム等が対象）	勧告
	第5-8条　ログの取得（重要度がA,B,C（※）の電力制御システム等が対象）	推奨

項目名		勧告／推奨※
第6章　運用・管理のセキュリティ	第6-1条　セキュリティ仕様の確認	推奨
	第6-2条　機器・外部記憶媒体及びデータの管理	推奨
	第6-3条　外部記憶媒体等のマルウェア対策	勧告
	第6-4条　管理者権限の適切な割当	推奨
	第6-5条　セキュリティパッチの適用	推奨
	第6-6条　入退管理（重要度がS,A（※※）の電力制御システム等が対象）	勧告
	第6-7条　入退管理（重要度がB,C（※※）の電力制御システム等が対象）	推奨
第7章　セキュリティ事故の対応	第7-1条　情報の収集	勧告
	第7-2条　セキュリティ事故の対応	勧告
	第7-3条　セキュリティ事故の報告と情報共有	勧告
	第7-4条　周知と訓練	勧告

※勧告的事項　：　電気事業者が実施すべき事項。
推奨的事項　：　電気事業者が実施の要否及び実施方法を判断する事項。

７．今後の進め方

- 自家用電気工作物の保安を監督する電気主任技術者等へのインタビュー等を踏まえ、スマート化の進展を見据えて、自家用電気工作物のサイバーセキュリティ対策の基礎的な検討を行ってきたところ。
- 今後、**自家用電気工作物のサイバーセキュリティ対策の具体的な内容の検討**にあたっては、太陽電池発電所等が遠隔で発電制御が可能である実態を踏まえつつ、これからの**スマート化技術の動向**や**多くの設置者が属する中小企業等の取組の実態・実効性の確保等**を考慮しながら、**専門家による集中的な議論を令和3年度中に行うべき**ではないか。
- また、電気事業の用に供する電気工作物と同様に、（スマート化技術を電気保安に用いる場合には、）**技術基準等による規制**に加え、**自家用電気工作物の設置者に対しても、サイバーセキュリティの確保を保安規程への記載事項**とするべきではないか。
- あわせて、**自家用電気工作物の設置者において**は、必ずしも**サイバーセキュリティに関する知見を有した人材を確保できるとは限らない**ことから、**サイバーセキュリティを担う人材の育成についても、民間の取組と連携し、強力に推進していくべきではないか。**

（参考）サイバーセキュリティ人材育成に関する民間の取組

スマート保安官民協議会
第３回電力安全部会
資料１－１　P.64
（令和３年３月１６日）

4-2. 民の取組④サイバーセキュリティ

- スマート化に伴い、**監視装置等が通信回線へ接続**されることとなり、悪意のある者からの攻撃の機会ともなっていく恐れが高まるため、**サイバーセキュリティ対策が必要**。
- 電力制御システム等については、**「電力制御システムセキュリティガイドライン」**等を技術基準（ハード対策）の解釈及び保安規程（マネジメント等ソフト対策）にて定める事項に関する内規にエンドースし、事業者に対応を求めているところ。
- これに加えて、サイバーセキュリティ対策を実施するための人材育成が必要であり、企業の対策状況に合わせた外部の人材育成プログラムの活用が有効。例えば、（独）情報処理推進機構 産業サイバーセキュリティセンター（ICSCoE）が開講する、サイバーセキュリティを経営課題として認知するための「戦略マネジメントセミナー」や、重要インフラのセキュリティの中核を担う人材を育成するための「中核人材育成プログラム」等がある。

（独）情報処理推進機構 産業サイバーセキュリティセンター　開講プログラム

「戦略マネジメント系セミナー」

サイバーセキュリティは経営課題であること及び経営層をはじめ関係者が認知すべきセキュリティ機能の重要性の理解を目指す。
2020年度はオンラインで開講。先進事例・課題や解決策・ノウハウなどを体系的に学ぶプログラムを提供。

「業界別サイバーレジリエンス強化演習（CyberREX）」

業界別に、シナリオによる実践的演習の形式を中心としたトレーニングを行う。ビジネスパートナーが直面するサイバーセキュリティ規制やガイドライン等の解説に関する集中講義と演習を実施。
※電力業界を対象としたコースを定期的に開講。

- 対象業界（今年度実績）：
情報通信・自動車（スマートモビリティ・製造）、ガス、金属、石油、化学、電力、鉄道、ファクトリーオートメーションなどの業界
- 電力業界からの参加実績：
H29：6名、H30：12名、R1：17名、R2：19名

「中核人材育成プログラム」

重要インフラ企業を中心にセキュリティの中核を担う人材育成を目標としたプログラム。
電力、石油、ガス、化学、自動車、鉄道分野等の企業からセキュリティ担当予定者を1年間派遣させ、制御系セキュリティに精通する講師により、実機を使った模擬プラントを実際に攻撃して脆弱性を洗い出す等の実践的なプログラムを行う。