自家用電気工作物向け セキュリティガイドライン解説

2023/7

トレンドマイクロ株式会社

Company Profile

Our Vision

デジタルインフォメーションを安全に交換できる世界の実現

A world safe for exchanging digital information

Our Mission

お客様のデジタルライフやITインフラを脅威から守る

Defend against threats that would impact user's digital life or IT infrastructure.

日本発の世界企業へ

日本発のトレンドマイクロは、サイバーセキュリティのグローバルリーダとして50万社を超える法人組織と個人を保護しています。
35年以上サイバーセキュリティに従事し、データセンター、クラウド、ネットワーク、エンドポイントにおける多層的なセキュリティを提供します。

代表取締役社長
(CEO)
エバ・チェン

取締役副社長

大三川 彰彦

本社	東京
証券コード	4704　東証プライム 採用銘柄：TOPIX, 日経平均(日経225）他
設立	1989年10月24日
資本金	195億8,500万円 (2022年12月31日付)
事業内容	コンピュータ及びインターネット用セキュリティ関連製品・サービスの開発・販売
社員数	7,669名　(2022年12月31日付)
売上高	2,237億9,500万円 (2022年12月31日付)

トレンドマイクロ　工場セキュリティへの取組み

1988年設立以降変わらないVISION

デジタルインフォメーションを安全に交換できる世界の実現

10年以上におよぶICS/OTセキュリティへの取組

ICS/OT環境へのサイバー攻撃実証実験
産業制御システムの脆弱性調査

TREND MICRO research
ZERO DAY INITIATIVE

OT関連団体活動

EDGECROSS CONSORTIUM
セキュリティ企業での唯一の幹事会社

CLPA CC-Link PARTNER ASSOCIATION
CC-Link協会

経済産業省
産業サイバーセキュリティ研究会
工場SWG 委員

JE-ISAC Japan Electricity Information Sharing and Analysis Center

本社：東京

- Tokyo
- Taipei
- Manila

主要開発・サポート拠点
台湾・フィリピン

65ヵ国以上6,900人以上の従業員

自家用電気工作物向けのガイドライン解説を行う背景

1. 比較的新しいガイドライン

   2022年6月公布　2022年10月施行

2. あまり周知が進んでいない傾向にある

   弊社が顧客に提案した際、ご存じないケースが多い（約10件中10件）

3. 実施義務がある

   実施しない場合、**技術基準適合維持義務違反**となる可能性がある

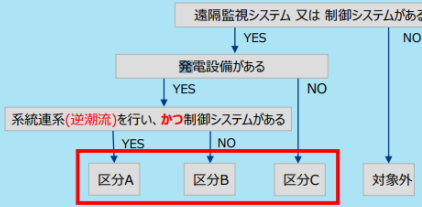
   2024年度以降、立入検査の実施項目に本ガイドラインの内容が含まれる見込み

https://www.meti.go.jp/policy/safety_security/industrial_safety/oshirase/2022/07/20220706-2.pdf

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)(通称:自家用GL)**」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)(通称:保安規程内規)**」を制定しました。
https://www.meti.go.jp/policy/safety_security/industrial_safety/oshirase/2022/06/20220610.html
※このリーフレットは設置者への周知用にご使用下さい。保安業務に従事される方は、ガイドラインやQ&A、説明資料をご覧下さい。

<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。

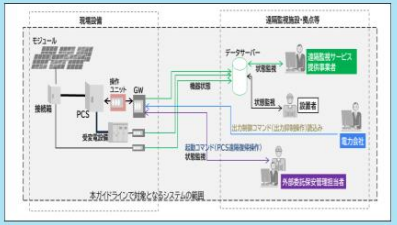
区分A~Cに応じて、CS対策の**義務(勧告的事項)**と**推奨(推奨的事項)**に分けられており、対策事項(レベル)を基本推奨的事項とし、最低限の基準として区分Aのみ一部勧告的事項がございます。

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。

裏面もご覧ください。

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、サイバー保険への加入、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。
  https://www.meti.go.jp/policy/netsecurity/mng_guide.html
  https://www.meti.go.jp/policy/netsecurity/sme-guide.html

電気事業法についての問い合わせ窓口 エリア/組織名/電話番号

北海道	北海道産業保安監督部 電力安全課	011-709-2311
東北	関東東北産業保安監督部 東北支部電力安全課	022-221-4947
関東	関東東北産業保安監督部 電力安全課	048-600-0385
中部	中部近畿産業保安監督部 電力安全課	052-951-2817
北陸	中部近畿産業保安監督部 北陸産業保安監督署	076-432-5580

近畿	中部近畿産業保安監督部 近畿支部 電力安全課	06-6966-6048
中国	中国四国産業保安監督部 電力安全課	082-224-5742
四国	中国四国産業保安監督部 四国支部 電力安全課	087-811-8587
九州	九州産業保安監督部 電力安全課	092-482-5520
沖縄	那覇産業保安監督事務所 保安監督課	098-866-6474

Agenda

1. 自家用電気工作物
2. 自家用電気工作物向けセキュリティガイドライン解説
3. ガイドライン向けセキュリティ対策概要

Appendix

- ガイドライン向け、具体的なセキュリティ対策イメージ

自家用電気工作物

参考：電気工作物の種類

電気工作物：発電、変電、送電若しくは配電又は電気の使用のために設置された工作物。

電気工作物

事業用電気工作物

一般用電気工作物以外の電気工作物
（電力会社や工場等の発電所、変電所、送電線、配電線）

一般用電気工作物

600V以下で受電または一定の出力以下の小規模発電設備でかつ受電線路以外の線路で接続されていないなど、安全性の高い電気工作物

自家用電気工作物

電気事業の用に供する事業用電気工作物以外の事業用電気工作物
（自家用発電設備、工場・ビルなどの600Vを超えて受電する需要設備等）

小規模事業用電気工作物

一部の小規模な発電設備
（10kW以上50kW未満の太陽光発電設備、20kW未満の風力発電設備）
参考：10kWの太陽光発電：パネル40枚=約50m²

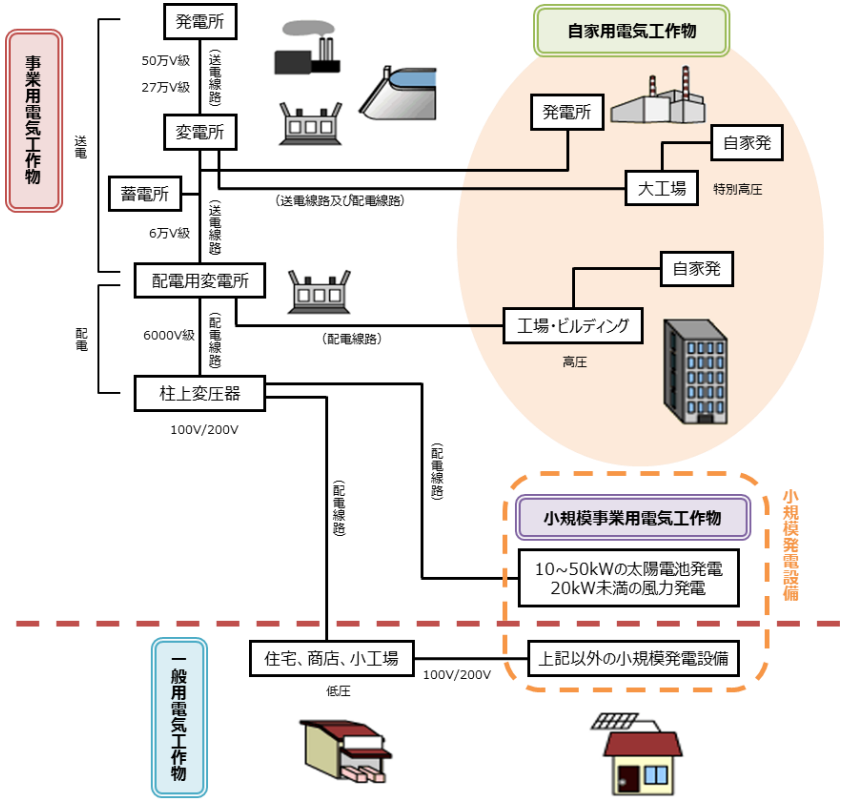
一般用電気工作物
・家庭用の電気設備

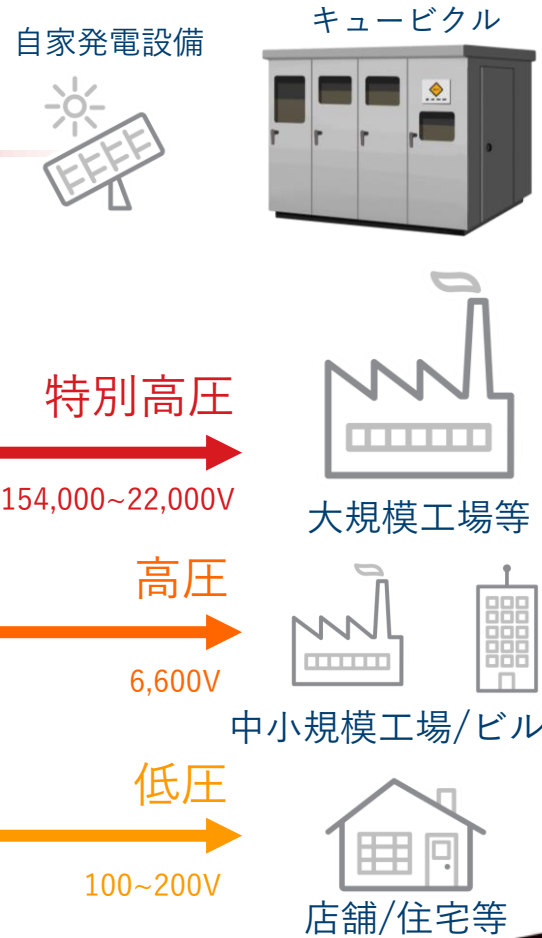
事業用電気工作物
・一般用電気工作物以外

自家用電気工作物
・事業用電気工作物の中で、電気事業に使用しないもの

ビル・工場等の電気設備

参考：電気工作物の種類





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

参考：自家用電気工作物の範囲

① 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
・6kVの高圧・20kV/60kVの特別高圧で受電する設備が該当
（**工場、事務所ビル、学校、病院、ホテル、スポーツ施設、娯楽施設など**）

② 発電設備と、その発電した電気を使用する設備
・①の受電電圧に関わらず、一定以上の出力を持った発電設備を有するもの

③ 電力会社等からの受電の為の電線路以外に構外にわたる電線路を有する電気設備
・校内以外の場所にある電気工作物に至る電線路を有するもの

④ 火薬工場および炭鉱

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/oshirase/2022/09/20220930-2.pdf

自家用電気工作物向けガイドラインが発行された背景

- 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の確保も重要な課題
- 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

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）＞

(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。

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

本ガイドラインの適用範囲

対象：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** / **制御システム** / これらのシステムに付随するネットワーク
- 上記に携わる者

対象設備
1，新設設備
2，既設設備（ハード・ソフト問わず、システムに変更があった際）

実施事項の定義
- 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**

参考）推奨的事項の考え方

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

※推奨的事項について、**検討した上で必要でないと判断された対策は講じなくても良い**
しかし、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**になる可能性がある為、
検討した際の記録は残しておく必要有り

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　Q&Aより抜粋
https://www.meti.go.jp/policy/safety_security/industrial_safety/oshirase/2023/03/20230320-22.pdf

経産省に訪問し、確認した結果・・・

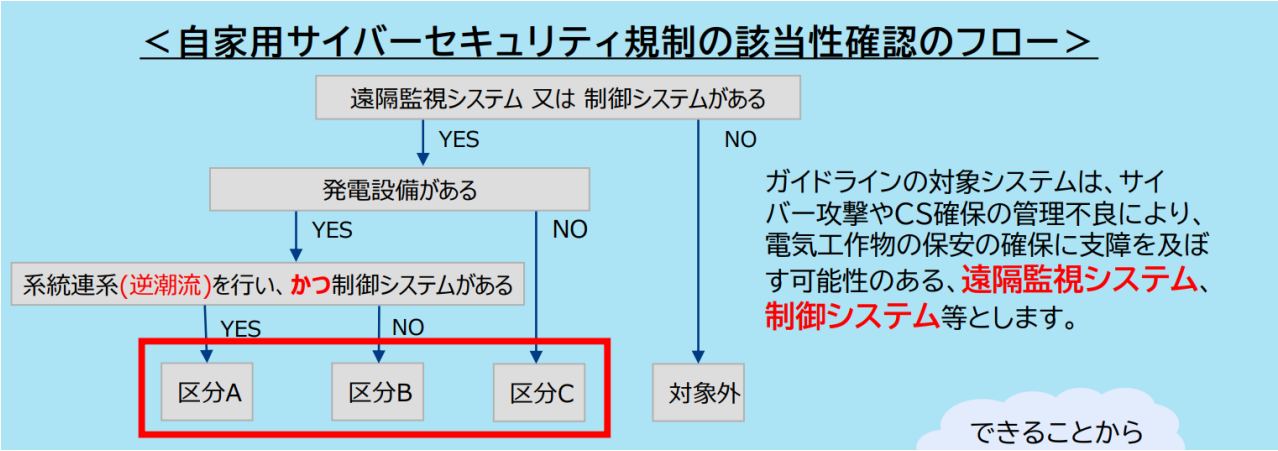
1. リスクアセスメントを実施しリスクを洗い出し、その記録を残す

2. アセスメントの結果を基に、必要なセキュリティ対策を実施する
3. セキュリティ対策を実施しない場合、その理由について記録に残す

https://www.meti.go.jp/policy/safety_security/industrial_safety/oshirase/2022/07/20220706-2.pdf

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

遠隔監視システム / 制御システムのある環境が本ガイドラインの対象
※遠隔監視システム　⇒**自社内で監視しているケースも含む**



区分A　：勧告事項あり
区分B/C　：推奨

セキュリティ事故が発生した場合の
電力系統への影響および社会的影響の大きさを考慮し、区分を設定

参考：区分の考え方

- 区分A：自家発電設備を持っており、**余剰電力を売電している**事業者
  - 再エネ事業者、余剰電力を売電しているビル・工場等
  - 電力系統に接続されている為、問題時に**送配電設備等への影響拡大が懸念**

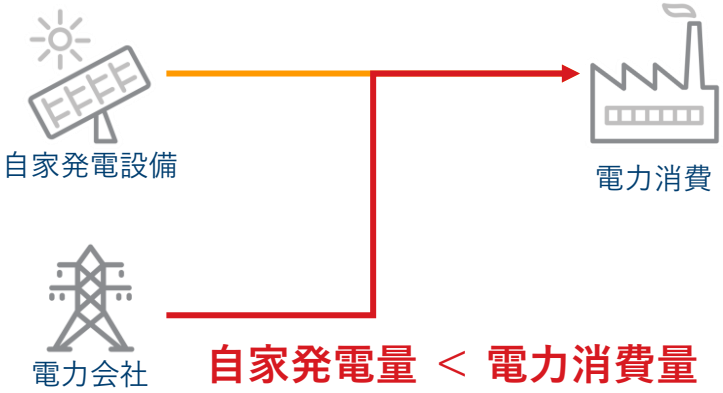
- 区分B：自家発電設備を持っており、**自家消費を行っている**事業者
  - 余剰電力が発生した場合も、売電は行わない
  - 病院・工場・ビル等の電力停止時、**社会的に大きな影響へと繋がる可能性**有り

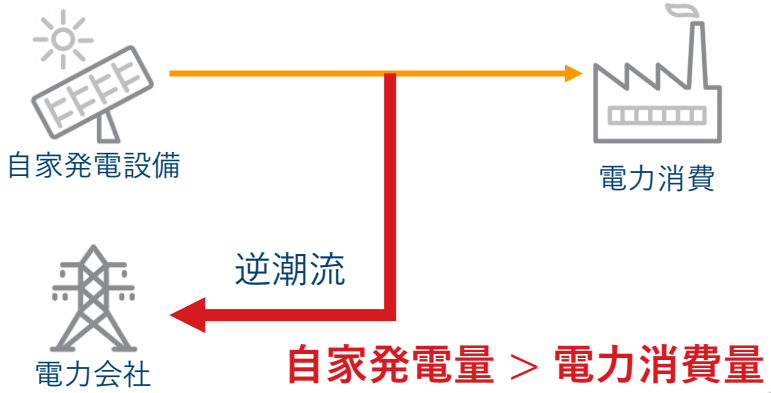
- 区分C：遠隔監視システムや制御システムを持っている事業者

参考：区分Aの環境について（系統連系 / 逆潮流）

系統連系
- 電力会社の電力系統に、発電設備を接続する事

逆潮流
- 発電電力が消費電力を上回った時、電力会社側（送電網）へ流れる事





セキュリティ対策について

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

条項		内容	区分
第1章 総則	第1-1条	目的	-
	第1-2条	適用範囲	-
	第1-3条	対象となるシステムの区分	-
	第1-4条	想定脅威	-
	第1-5条	用語の定義	-
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	推奨
第3章 文書化	第3-1条	文書管理	推奨
	第3-2条	実施状況の報告	推奨
第4章	第4-1条	セキュリティ管理	推奨
第5章 機器	第5-1条	セキュリティ仕様の確認	推奨
	第5-2条	機器の取り扱い	推奨

条項		内容	区分
第6章 通信	第6-1条	暗号化・通信プロトコルの最適化	推奨
	第6-2条	ネットワークの管理	勧告
第7章	第7-1条	システムのセキュリティ	推奨
第8章 運用	第8-1条	システムの管理	勧告
	第8-2条	機器・外部記憶媒体の管理	推奨
	第8-3条	データの管理	推奨
	第8-4条	脆弱性の管理	推奨
第9章	第9-1条	物理セキュリティ	推奨
第10章 事故対応	第10-1条	情報の収集	推奨
	第10-2条	セキュリティ事故の対応体制等	推奨
	第10-3条	セキュリティ事故の報告と情報共有	推奨
	第10-4条	周知と訓練	推奨

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

TMサービスで支援可能
TM製品で支援可能

- **基本的にガイドライン掲載の項目はトレンド製品で対応可能**（暗号化・認証を除く）

条項		項目	区分
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**		
	1	暗号化・通信プロトコルの最適化	推奨
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
	2	接続点の最小化	勧告
	3	接続点の防御	勧告
	4	接続制御	推奨
	5	認証	推奨
	6	ネットワーク分割	推奨
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**		
	1	不正プログラム防止	推奨
	2	不正処理防止	推奨

条項		項目	区分
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
	2	機器のマルウェア対策	推奨
	3	外部記憶媒体等のマルウェア対策	勧告
	4	ログの取得	推奨
第8-2条	**機器・外部記憶媒体の管理**		
	1	機器・外部記憶媒体の管理	推奨
第8-3条	**データの管理**		
	1	データの管理	推奨
第8-4条	**脆弱性の管理**		
	1	脆弱性の管理	推奨

第2章	第2-3条	セキュリティ教育	推奨

OT環境の特性に合わせたセキュリティ対策製品 - TXOne シリーズ

ネットワークセグメンテーション(影響範囲局所化)

産業向け次世代FW

EdgeFire™※

侵入防止(脆弱性対策)

産業向け次世代 IPS

EdgeIPS™※

EdgeIPS™ Pro※

※集中管理用のコンソール製品(OT Defense Console)が必須です。

感染防止

産業向けエンドポイント
プロテクション

StellarProtect Standard

産業向け次世代アンチウイルス

StellarProtect Lockdown

※Trend Micro Safe Lock後継

ロックダウンソフトウェア

- 産業用PC、タッチパネルPC
- Windows

復旧(駆除)

ウイルス検索・駆除
ツール

Trend Micro
Portable Security™ 3

- スタンドアロン/クローズド環境

工場セキュリティガイドライン

目的	● 各業界・業種が自ら工場のセキュリティ対策を立案・実行することで、産業界全体、とりわけ工場システムのセキュリティレベルの底上げを図る。 ● 参照すべき考え方やステップを「手引き」として示す。
対象	● 新設・既設によらず、工場における産業制御システム（ICS/OT）を対象とする。
想定読者	● 想定読者は以下を想定とする。 • IT関係部門（情報システム部門、セキュリティ部門 等） • 生産関係部門（生産技術部門、生産管理部門、工作部門 等） • 戦略マネジメント部門（経営企画等） • 監査部門 • リスク管理部門 • 機器システム提供ベンダ、機器メーカ（サプライチェーンを含む） ● 部門間・担当間の立場や価値観の違いを認識しつつ、コミュニケーションを行っていくことが重要である。

まとめ

工場や病院、ビル等には電気設備がある(自家用電気工作物)

電力設備に関する制御システムや、発電設備を持っている事業者がいる

被害が発生した場合、社会的影響が大きくなる環境・業種がある

サイバーセキュリティの確保義務が自家用電気工作物まで拡大された

自家用電気工作物向けのガイドラインを参考にセキュリティ対策を実施する必要がある

アセスメントを実施するとともに、セキュリティ対策が必要

セキュリティ対策のご相談はトレンドマイクロまで！

お問い合わせ先

法人お問い合わせ窓口：03-5334-3601
お問い合わせフォーム：
https://www.trendmicro.com/ja_jp/contact/contact-us.html

Appendix

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

TMサービスで支援可能
TM製品で支援可能

- **基本的にガイドライン掲載の項目はトレンド製品で対応可能**（暗号化・認証を除く）

条項	項目		区分
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**		
	1	暗号化・通信プロトコルの最適化	推奨
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
	2	接続点の最小化	勧告
	3	接続点の防御	勧告
	4	接続制御	推奨
	5	認証	推奨
	6	ネットワーク分割	推奨
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**		
	1	不正プログラム防止	推奨
	2	不正処理防止	推奨

条項	項目		区分
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
	2	機器のマルウェア対策	推奨
	3	外部記憶媒体等のマルウェア対策	勧告
	4	ログの取得	推奨
第8-2条	**機器・外部記憶媒体の管理**		
	1	機器・外部記憶媒体の管理	推奨
第8-3条	**データの管理**		
	1	データの管理	推奨
第8-4条	**脆弱性の管理**		
	1	脆弱性の管理	推奨

第2章	第2-3条	セキュリティ教育	推奨

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

条項	項目	区分	内容	提案
第6-1条	**暗号化・通信プロトコルの最適化**			
	1 暗号化	推奨	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	
	2 通信プロトコルの最適化	推奨	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 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 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	

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

条項		項目	区分	内容	提案
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	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	DMZの構築 ・EdgeFire
	2	接続点の最小化	勧告	他ネットワークとの接続点は、最小化すること	遠隔監視システム、制御システムの特定 / 遠隔監視・制御システムネットワークに接続される機器の特定
	3	接続点の防御	勧告	他ネットワークとの接続点に防御措置を講じること	2項で特定したネットワーク接続点の防御 ・Edgeシリーズ
	4	接続制御	推奨	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	許可されていない通信の遮断 ・Edgeシリーズ
	5	認証	推奨	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	必要時応じて、認証を必要とする機器と範囲を定め、識別と認証を行う
	6	ネットワーク分割	推奨	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	損害の拡大防止の観点で、利用目的に応じて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 ・EdgeFire

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

条項	項目	区分	内容	提案
第7-1条	**システムのセキュリティ**			
	1	不正プログラム防止	推奨	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すること	ホワイトリスト型セキュリティソフトの導入 ・StellarProtect
	2	不正処理防止	推奨	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	不正操作・不正なコマンドの監視・防止 ・Deep Discovery Inspector ・Edgeシリーズ ・StellarProtect

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

条項		項目	区分	内容	提案
第8-1条	**システムの管理**				
	1	管理者権限の適切な割り当て	推奨	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 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 管理者権限の割り当て状況を、定期的に確認する	
	2	機器のマルウェア対策	推奨	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	セキュリティソフトの導入 ・StellarProtect ・ApexOne、DeepSecurity等 ・TMPS
	3	外部記憶媒体等のマルウェア対策	勧告	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、異常のないことを確認する ・接続前にウイルスチェック等を行う ・事前にウイルスチェック等を行った証跡を提出させる	持ち込みPC向けの事前スキャン ・TMPS 持ち込みUSBのセキュリティ対策 ・TMPS Pro(セキュアストレージ)
	4	ログの取得	推奨	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	トレンド製品のセキュリティログはSyslog等で提供可能

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

条項	項目	区分	内容	提案
第8-2条	**機器・外部記憶媒体の管理**			
	1 機器・外部記憶媒体の管理	推奨	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）も含めて把握し、存在について確認する 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	資産管理 ・TMPS ・Edgeシリーズ 外部記憶媒体の管理 ・TMPS Pro
第8-3条	**データの管理**			
	1 データの管理	推奨	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。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	

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

条項		項目	区分	内容	提案
第8-4条	**脆弱性の管理**				
	1	情報の収集	推奨	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	定期的な情報収集および、脆弱性対策製品の導入による情報収集を行う ・TMPS
	2	対応手順の策定	推奨	収集したぜい弱性に対する対応手順を策定すること 対応手順には、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	パッチ適用手順を整備する
	3	セキュリティパッチの適用	推奨	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、適用することによる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 適用を見送る場合は、残存リスクを管理すること	可能であれば、該当システムのセキュリティパッチを適用する 代替策として、脆弱性対策製品でのパッチ適用を行う ・Edgeシリーズ