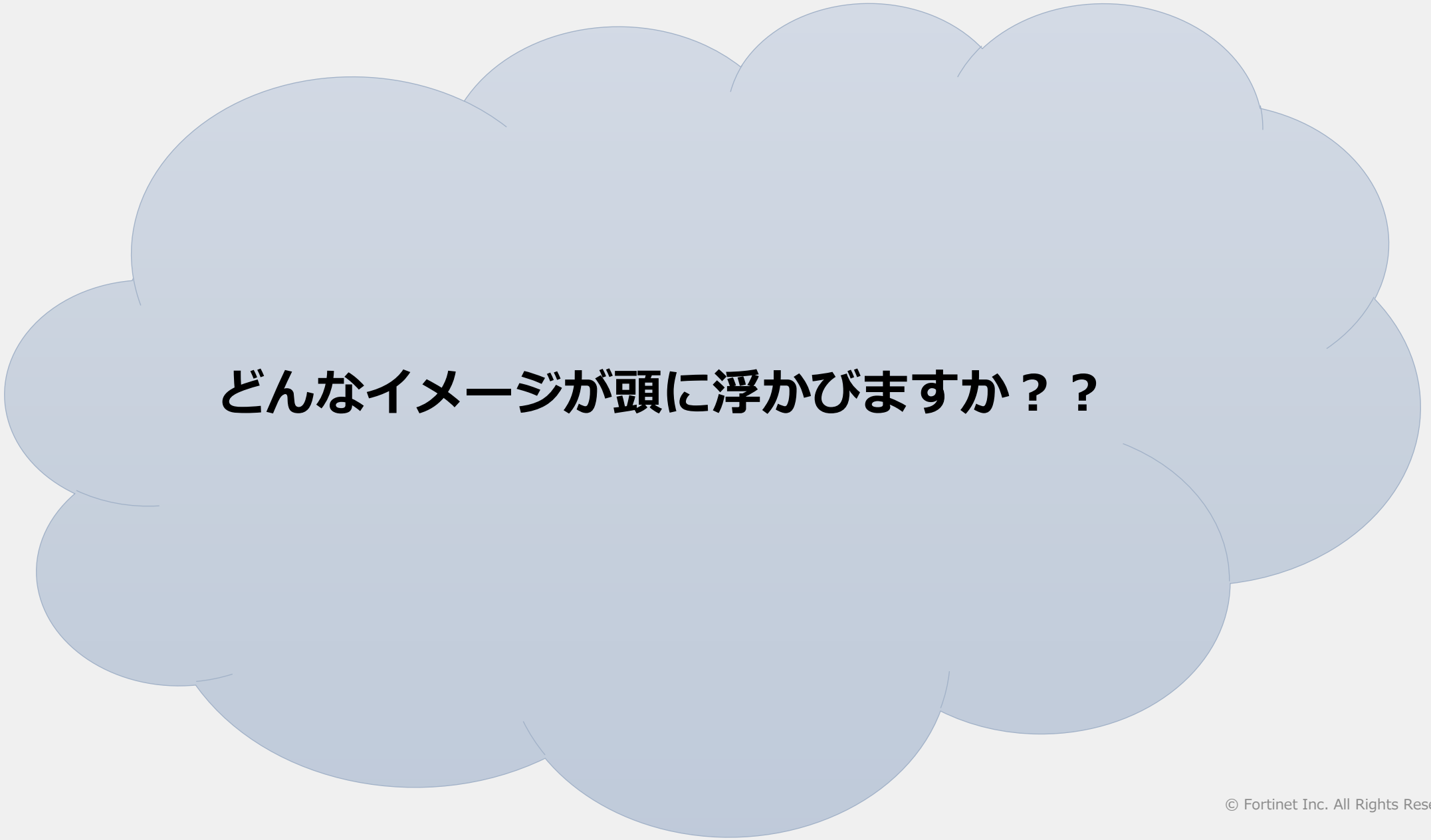
令和7年度　自家用電気主任技術者会議

# 自家用電気工作物を守るサイバーセキュリティ ～今日からできる第一歩

2025/10/23

フォーティネットジャパン合同会社
OTビジネス開発部　小泉 和也

# “サイバーセキュリティ”のイメージ



# “サイバーセキュリティ”のイメージ

- スーパーハッカーから守る？？
- 電気保安業務との関係は無いと思う
- IT部門や情報システム担当者の仕事
- 盗まれて困るような情報はないし、
  特に気にする必要はないと思う
- 用語が横文字／難解でとっつきにくい
- 大企業の話で、中小事業者は関係ない？

# 本講演の目標

- “サイバーセキュリティ“のハードルを少しでも下げる
- 電気保安におけるサイバーセキュリティ対策の重要性を学ぶ
- 今日からできそうなことを、1つでも持ち帰る

# 自己紹介

石油学会 設備維持管理士
(計装設備2016001号)

その他保有資格：
・一般計量士
・高圧ガス製造保安責任者　甲種機械
・危険物取扱者　甲種
・エネルギー管理士　熱分野
・公害防止管理者　大気１種／水質１種
・応用情報技術者

## フォーティネットジャパン合同会社　OTビジネス開発部
## 小泉 和也 (Kazuya Koizumi)

これまで石油精製プラント(重要インフラ事業者)のエンジニアとして、OT現場の最前線で従事。
フィールド機器(Level0)から制御システム(Level1/2)までの幅広い領域に知識と経験を有する。
調節弁リモート診断の企画時、OTセキュリティの大切さと自身の知識ギャップを痛感した経験から、
より広くサイバー空間の「安全安心」と「便利さ」との両立に貢献するため、セキュリティ企業へ転身。

**Mission：「“安全安心”で“便利”なOTを、サイバーセキュリティで支える！」**

**＜今現在＞**
**フォーティネットジャパン合同会社　OTビジネス開発部　マネージャー (23年12月~)**
**JNSA 調査研究部会 OTセキュリティWG SWG3リーダー (25年5月~)**
**名古屋工業大学 産学官金連携機構 ものづくりDX研究所 外部研究員 (25年8月~)**

**＜これまでの経歴＞**
**エネルギー企業：石油精製プラントにおける計測・制御設備(計装)担当エンジニア（11年）**
＋新設／改造／更新に関するエンジニアリング
＋トラブルシューティング、機器メンテナンス戦略の検討
＋新技術導入／DX案件の企画・検討・実行

# フォーティネットは、世界で最も大規模かつ信頼されているサイバーセキュリティ企業の1社です。

設立：**2000年10月**

創設者：**Ken Xie、Michael Xie**

本社：**カリフォルニア州サニーベール**

NASDAQ上場（FTNT）：**2009年11月**

構成銘柄：**NASDAQ 100、S&P 500**

企業の持続可能性指標：

**ダウ・ジョーンズ・サステナビリティ・インデックス（DJSI）のDJSI World（全世界対象）およびDJSI North America（北米地域対象）の構成銘柄に選定**

グローバルな顧客基盤

**890,000社以上**

生涯顧客

**1,401**

国際特許数
（2025年6月30日現在）

2024年度の取扱高

**65億3,000万ドル以上**

（2024年12月31日現在）

**32億ドル以上**

イノベーションに対する2017年以降の投資額
（85%はR&D）

（2024年9月30日現在）

時価総額

**809億ドル**

（2025年6月30日現在）

証券投資適格格付け：

**BBB+ Baa1**

# Agenda

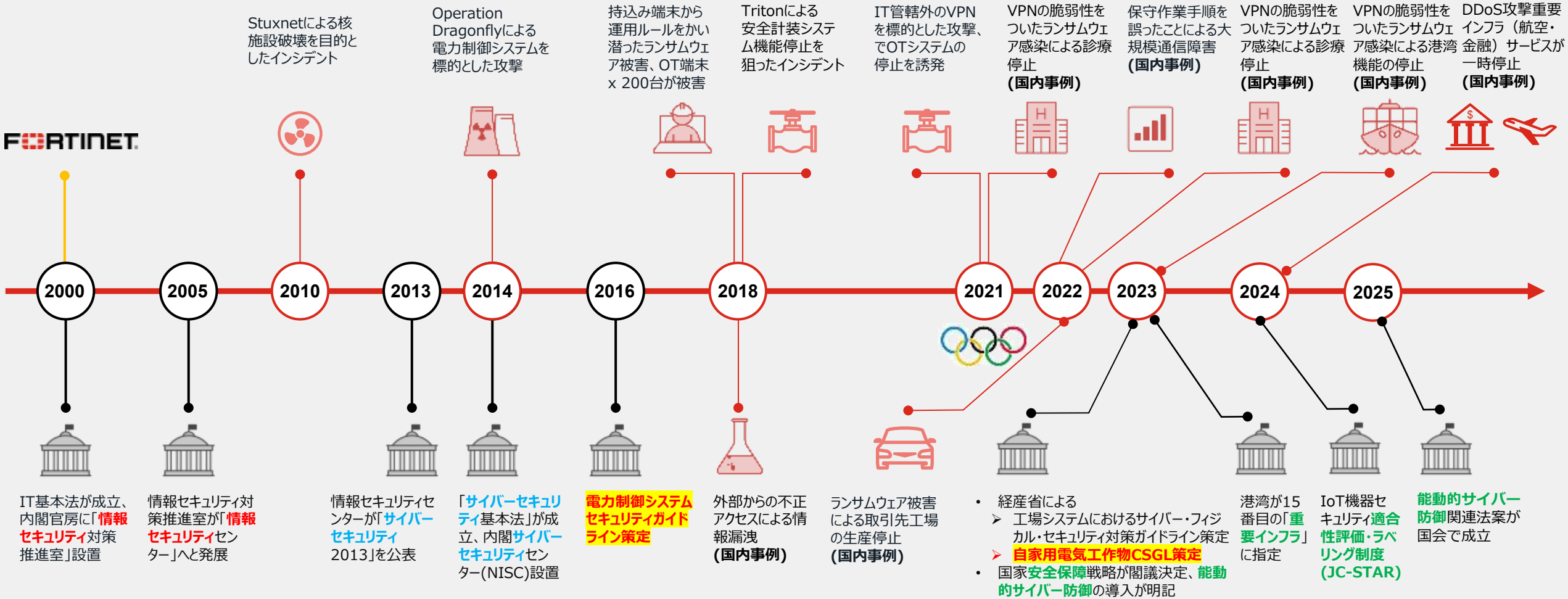
1. 電気保安とサイバーセキュリティ
2. “自家用CSガイドライン”の位置付け
3. “自家用CSガイドライン”の勘所
4. 今日からできる第一歩

# 電気保安とサイバーセキュリティ

# サイバーセキュリティが国の経営課題に

## 情報資産に対する機密性保持から安全保障の主要テーマに

：OTセキュリティに関連するインシデント事例
：日本国内における政策、法令、政府関連組織発足に関する情報
：Fortinet, Inc. 設立




| 情報・データ | サイバー空間 | サイバー・フィジカル空間（業界別規制・ガイドライン） | サイバー安全保障 |
|---|---|---|---|

# サイバーセキュリティの定義は“CIA”

## Confidentiality (機密性)

**許可された人だけが情報にアクセスできる状態を保つこと**

**<守れなかった場合の影響>**

- 図面や製造レシピの漏洩による競争力の喪失
- 個人情報、顧客情報の漏洩による信用失墜
- セキュリティ製品の脆弱性情報漏洩による２次被害

## Integrity (完全性)

**情報やシステムの正確性・一貫性が維持され、不正に改ざんされていないこと**

**<守れなかった場合の影響>**

- 配合データの改ざんによる、異常な濃度の薬剤混入、製品不良が発生
- 設定値が偽装され、異常に気づかず装置が過負荷運転
- 品質検査記録の不正書き換えにより、規定違反・回収措置が発生

## Availability (可用性)

**必要なときに情報やサービス、製品が提供できる状態にあること**

**<守れなかった場合の影響>**

- マルウェア感染などで監視システムや制御システムのサービスが停止、結果として操業ができない
- 操業が停止することで工程全体がボトルネック化・納期遅延が発生

**乗っ取り、情報漏洩、データ改ざん、設定ミス、管理不良、ランサムウェア**

- データ侵害中、人的要素に起因する割合　・・・　74%
- サイバーセキュリティの問題中、「ヒューマンエラー」に起因する割合　・・・　95%

# OTセキュリティの定義は“CIA+S(Safety)”

## Confidentiality (機密性)

許可された人だけが情報にアクセスできる状態を保つこと

## Integrity (完全性)

情報やシステムの正確性・一貫性が維持され、不正に改ざんされていないこと

## Availability (可用性)

必要なときに情報やサービス、製品が提供できる状態にあること

## Safety (安全性)

作業員・設備・環境の安全を確保し、事故を防止すること
(5S・KY・ヒヤリハット)

**<守れなかった場合の影響>**

- PLCの異常設定、予期せぬ機械作動により従業員の重傷事故が発生
- 異常温度を検知するセンサ情報が改ざんされ、化学薬品が過熱し火災事故に発展
- 非常停止機能が無効化され、停止すべきタイミングで装置が暴走

**安心・安全の土台の上に成り立つ生産活動である以上、**
**セキュリティ対策も安心・安全を考慮する必要がある**

# 現場で起きる最悪のサイバー攻撃

## OTでセキュリティインシデントが起こると…

https://www.youtube.com/watch?v=fnbCr8mgoT8

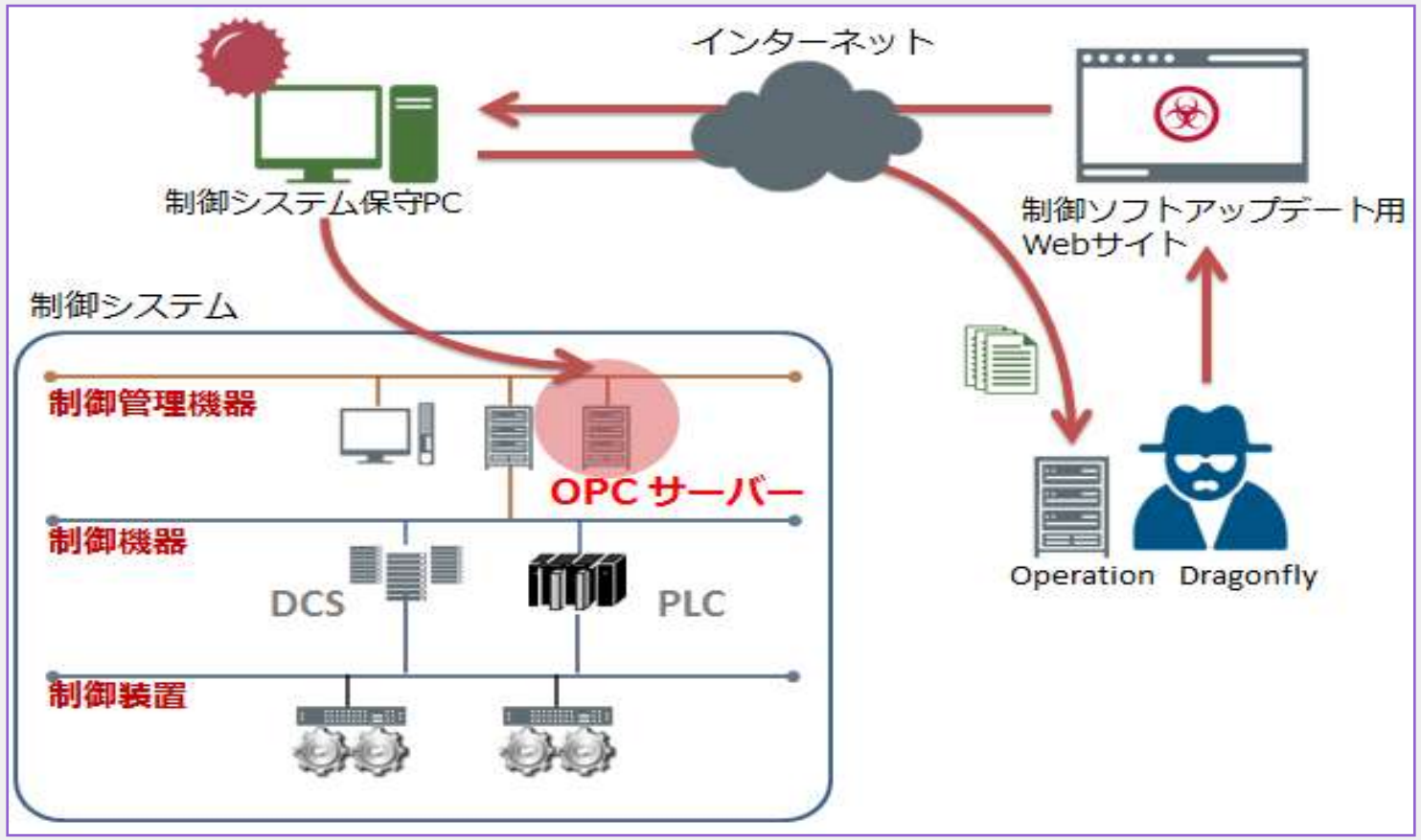

@GonjeshkeDarand

https://x.com/GonjeshkeDarand/status/1541288345183158272


**サイバー空間のインシデントにより、物理(フィジカル)空間で事故が発生**

# 電力設備に関連する
# サイバー事故（インシデント）事例

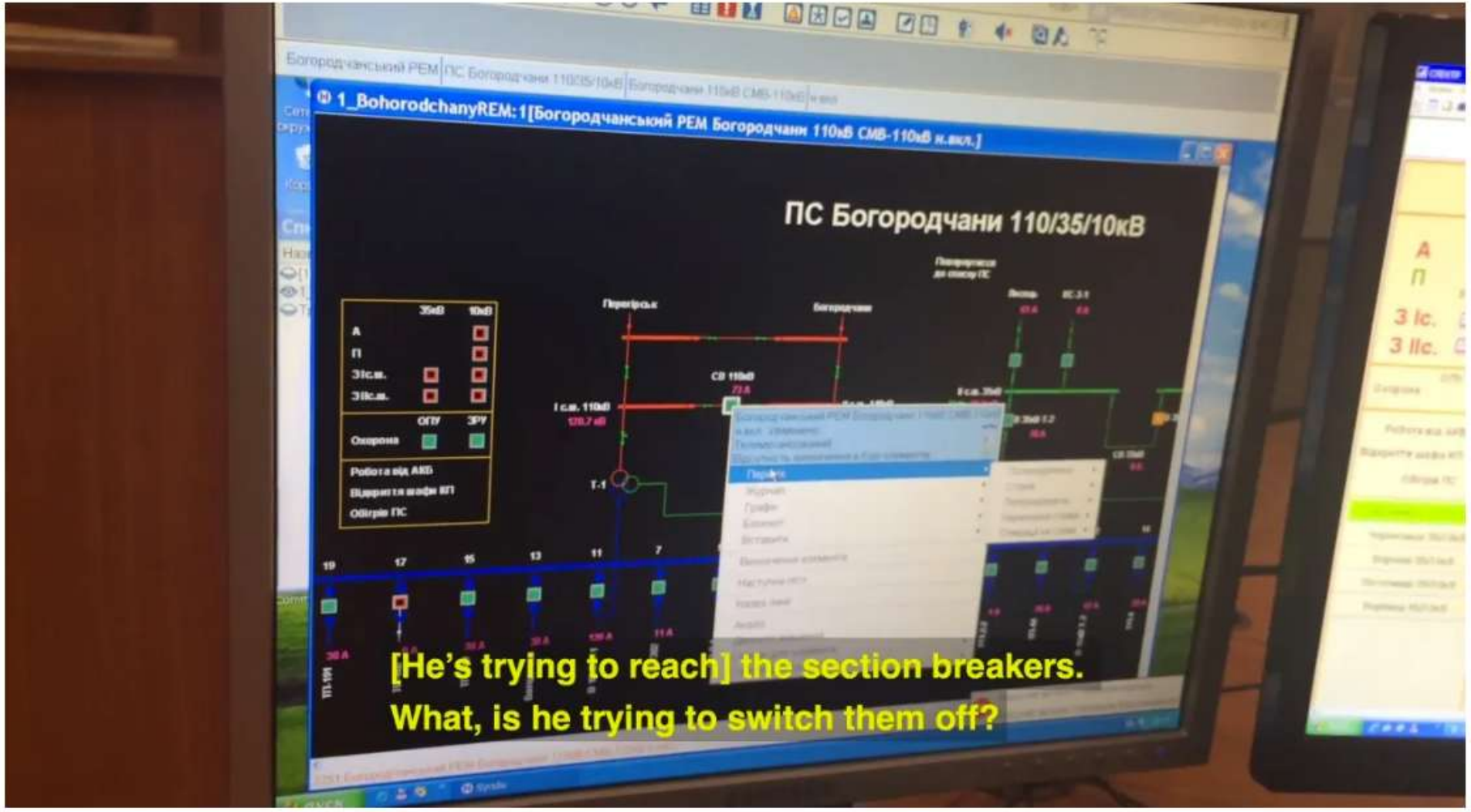
# 制御システムを狙ったサイバー攻撃(2014/06)
# ～Operation Dragonfly～




- 2013年2月より電力業界への攻撃を開始
- 制御システムベンダーのソフトのアップデートサイトをハッキング
- 制御システムベンダーのソフトのアップデータにマルウェアを同梱
- 欧州を中心に電力会社数社が感染
- 感染PCのネットワーク内にあるOPCサーバーの情報を収集し外部へ送信

**クローズドシステムの運用上の隙をついた攻撃**

# SCADA画面が乗っ取られた様子（真偽不明）



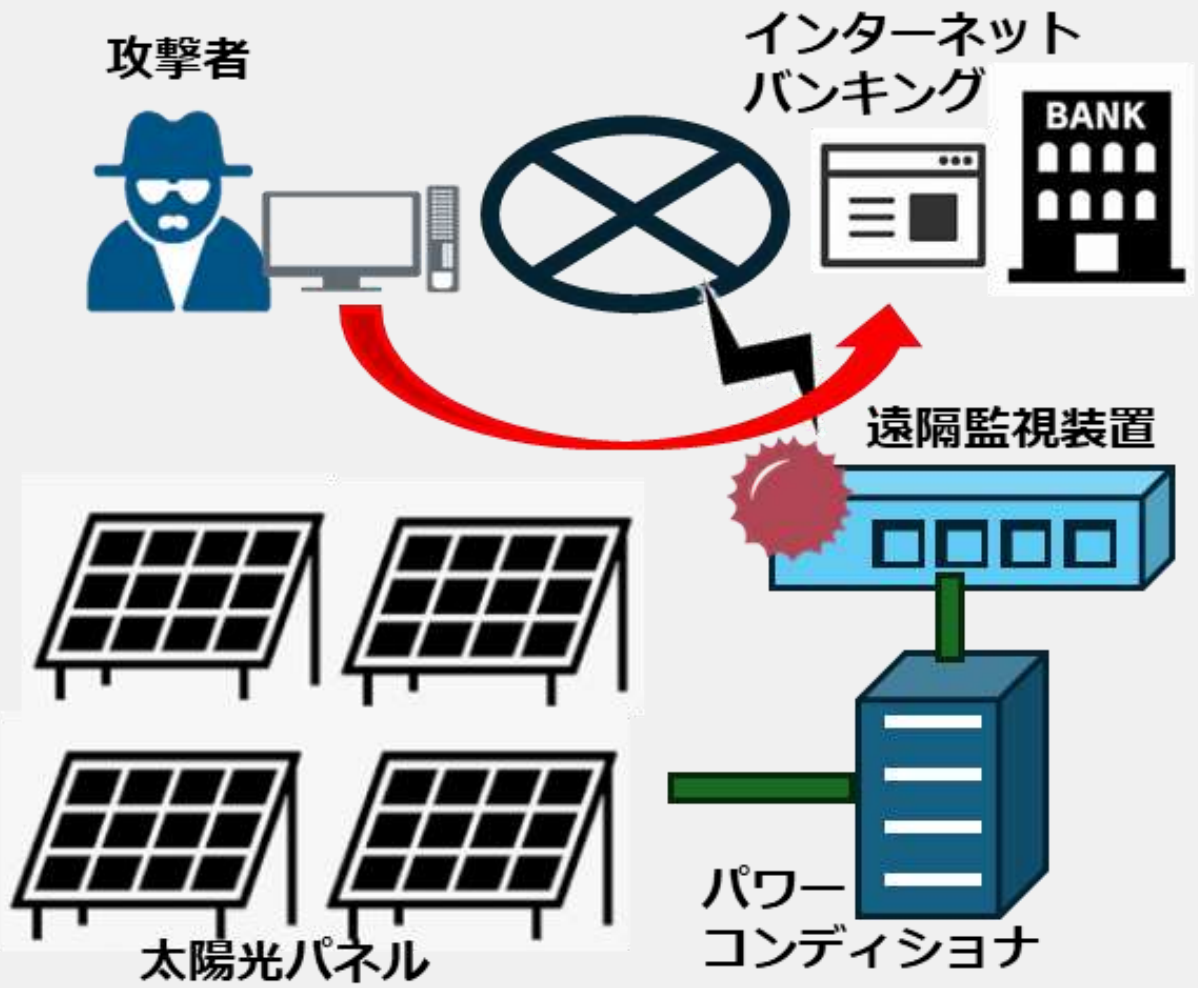

https://wired.jp/2017/07/27/video-hackers-take-over-power-grid-computer/

# 国内事例：太陽光発電施設の遠隔監視装置が不正送金の踏み台に

日本国内の太陽光発電施設の遠隔監視装置約800台がサイバー攻撃を受けて、**インターネットバンキングの不正送金に悪用**された(2024年5月に報道)。

**発生の経緯：**
中国のハッカー集団「武器庫」と推測される攻撃者が、C社製の太陽光発電の遠隔監視装置の脆弱性を利用して外部からの操作を可能にする不正プログラムを配置し、同装置を踏み台として用いて、インターネットバンキングの不正送金を行った。
C社製の同装置約800台が攻撃され、その一部が不正送金に利用された。**攻撃者が利用したとされる脆弱性は、2023年7月には公表されていたが、アップデート等の対策されない装置が多くあった**と考えられる。

**事故による被害：**
・不正送金を助長した。
・太陽光発電装置のユーザには直接的な被害はなし。
・攻撃を受けた機種は、遠隔制御機能がなかったため、乗っ取りによる発電停止などの誤作動のリスクはなかった。



# みなさんが管理する設備ではどうでしょうか？

皆さんが担当されている設備において、
“起こってほしくないこと“はなんですか？

サイバー的な要因（パソコンでの設定変更など）で
その事象／被害を起こせますか？

**フィジカル空間(物理空間)の保安確保のために
「サイバー空間の保安確保」も要考慮**

# “自家用CSガイドライン”の位置付け

# ご存知ですか？

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。

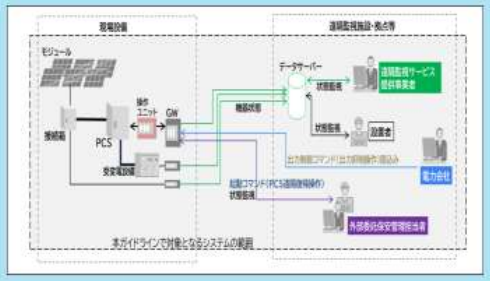
区分A～Cに応じて、CS対策の**義務（勧告的事項）**と**推奨（推奨的事項）**に分けられており、対策事項（レベル）を基本推奨的事項とし、最低限の基準として区分Aのみ一部勧告的事項がございます。

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 |

# 経産省ホームページ：
# 自家用電気工作物におけるサイバーセキュリティの確保について

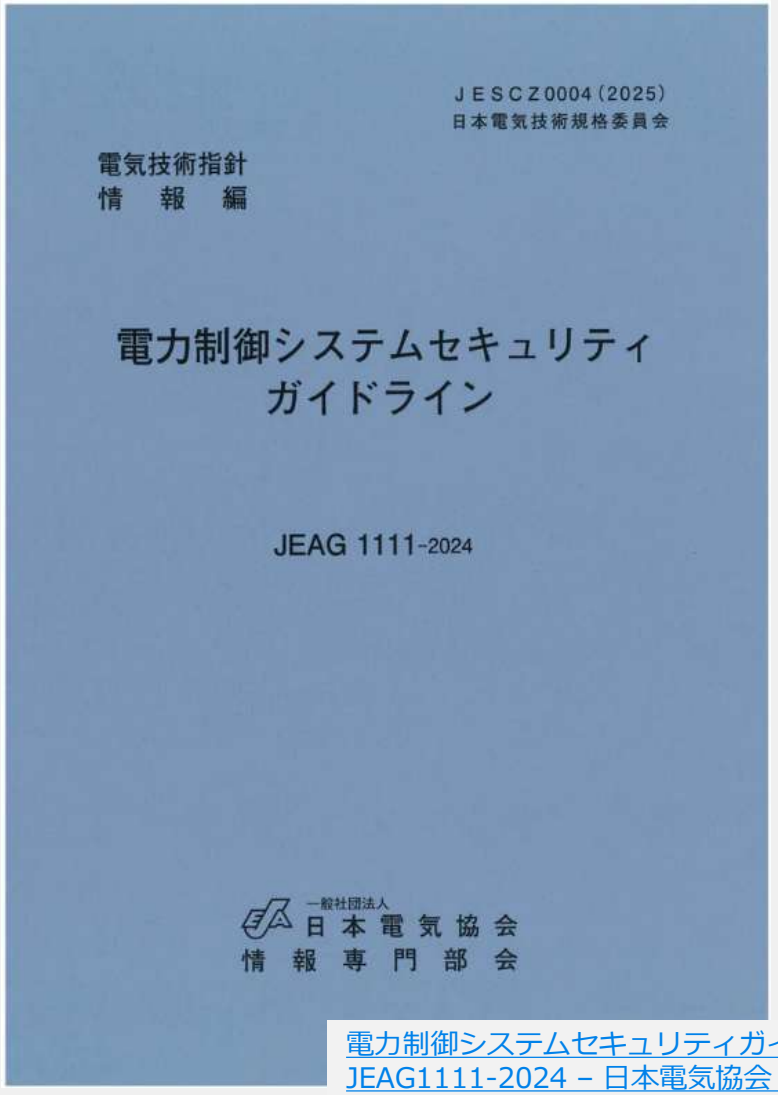

https://www.meti.go.jp/policy/safety_security/industrial_safety/sangyo/electric/detail/cybersecurity.html

# 電力制御システムに関連する２つのガイドライン

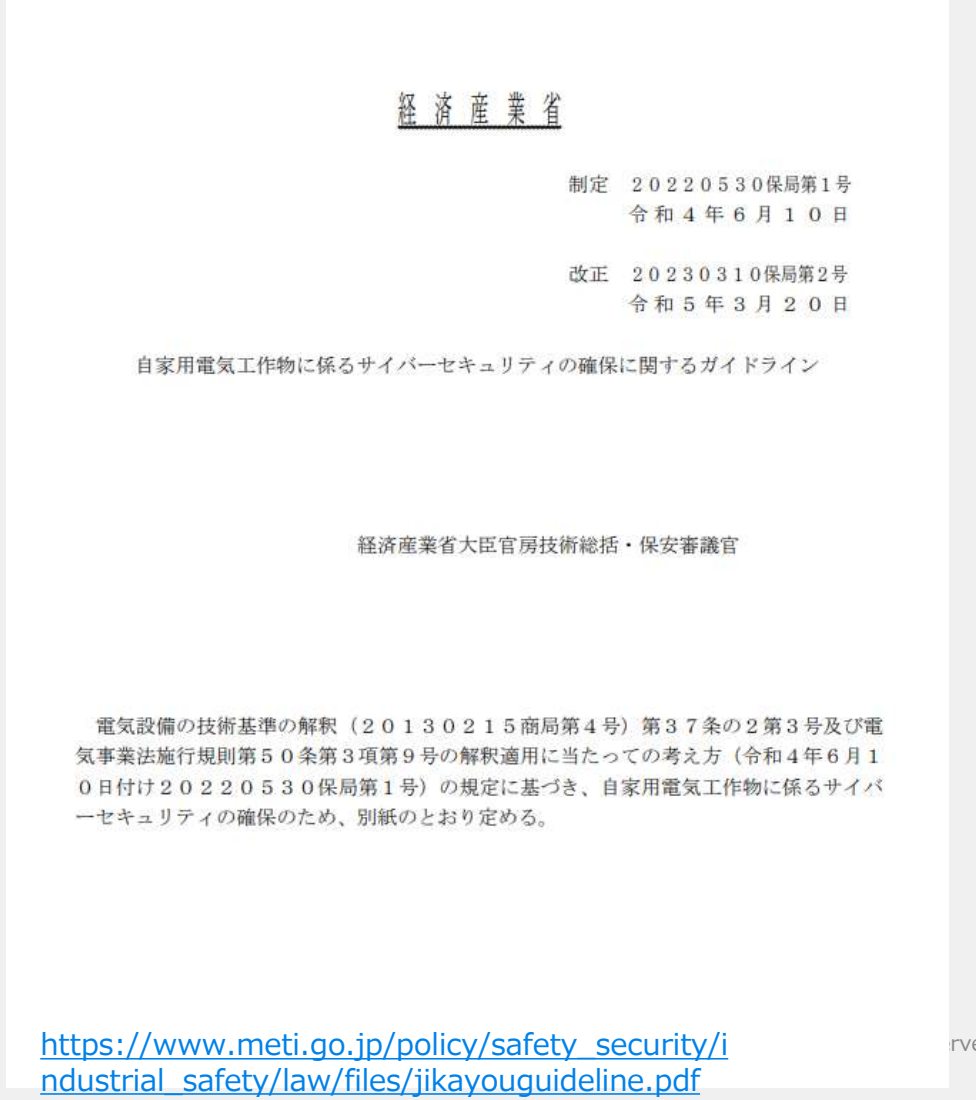
**電力制御システムセキュリティガイドライン（電制GL）**

≒

**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GL）**




電力制御システムセキュリティガイドライン
JEAG1111-2024 – 日本電気協会　Webストア



経済産業省

制定　２０２２０５３０保局第１号
令和４年６月１０日

改正　２０２３０３１０保局第２号
令和５年３月２０日

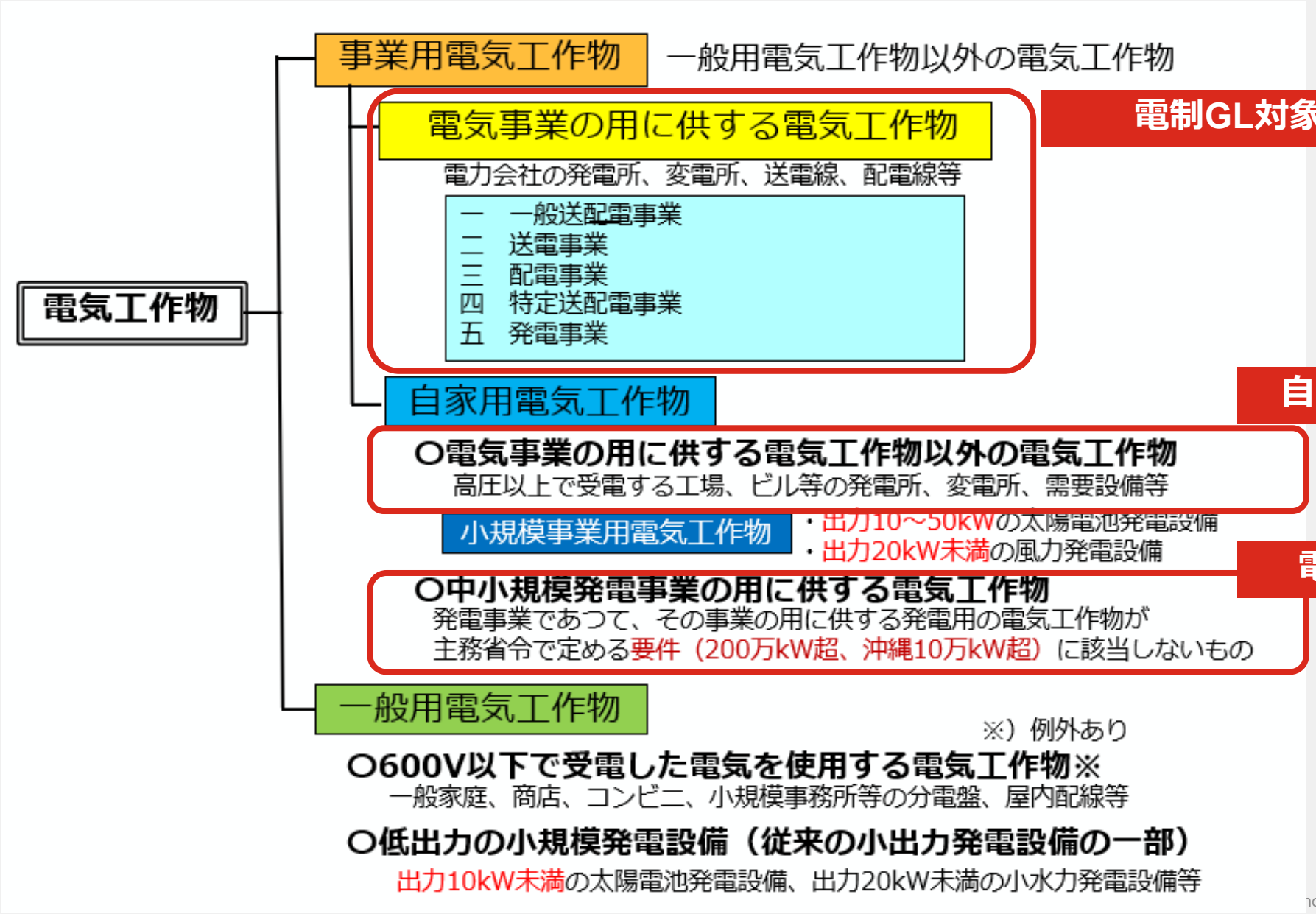
自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン

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。

https://www.meti.go.jp/policy/safety_security/industrial_safety/law/files/jikayouguideline.pdf

# 「電気工作物」の分類



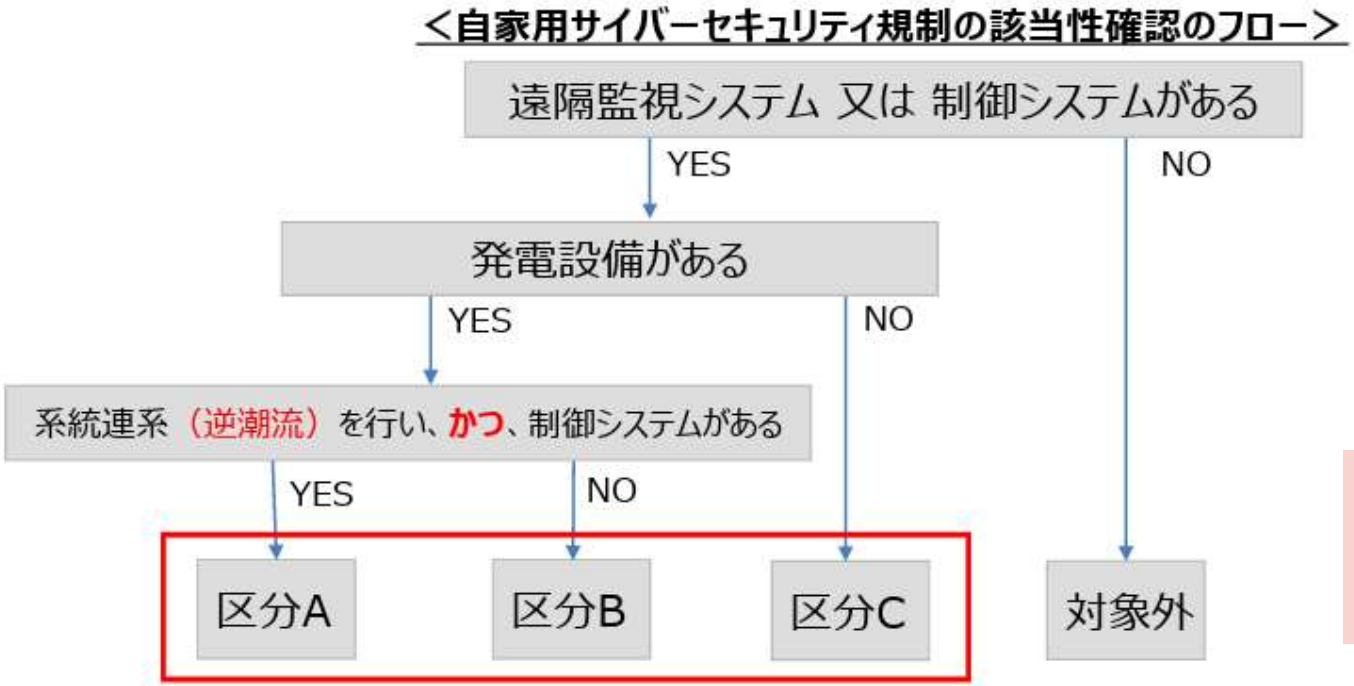




https://www.meti.go.jp/policy/safety_security/industrial_safety/sangyo/electric/detail/setsubi_hoan.html

# 自家用GL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ガイドラインは区分によって対策事項（レベル）を差別化**

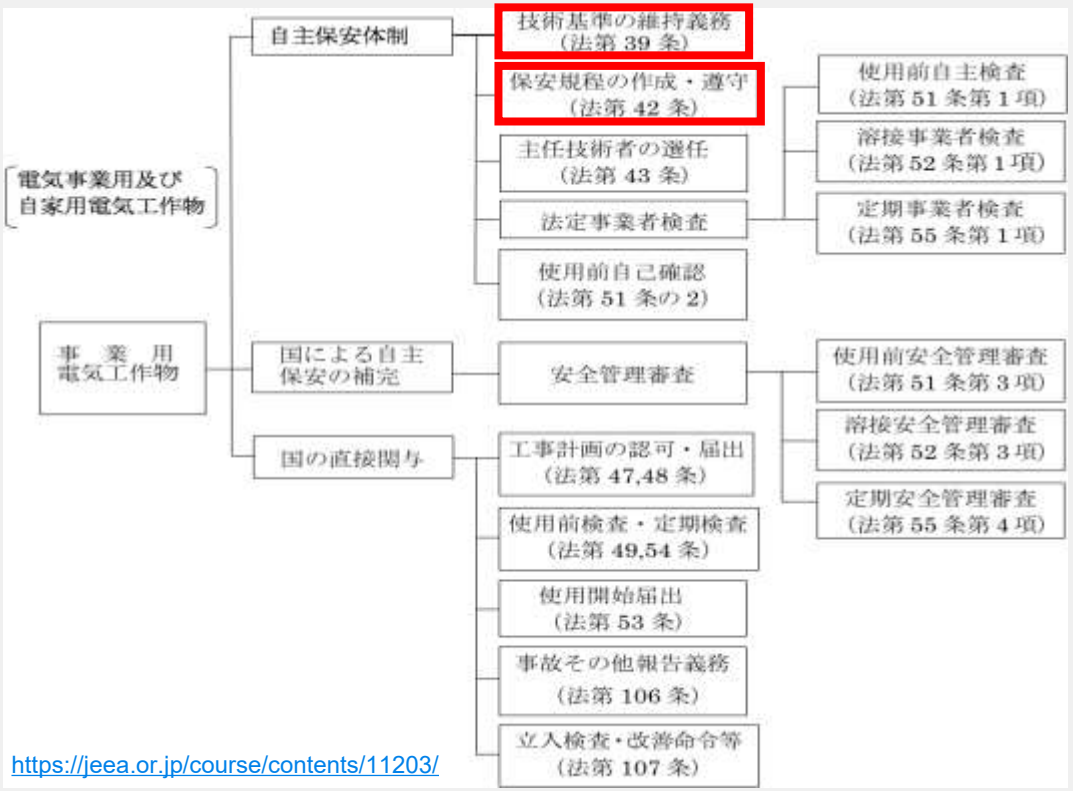
**対策事項は、基本的に“推奨的事項”**
**（区分Aのみ、一部勧告的事項がある）**
**→事業者側で、対策要否含めた検討が必要**

16

https://www.meti.go.jp/policy/safety_security/industrial_safety/oshirase/2022/09/20220930-2.pdf

# 電制GL／自家用GLの位置付け

## 電気事業法における保安規制




https://jeea.or.jp/course/contents/11203/

**技術基準の維持、保安規程の作成・遵守が、事業者には法的に求められている。**
**＝GL対応についての“説明責任“がある**

## 技術基準と各GLとの紐づけ

**経済産業省：電気設備の技術基準の解釈**

【サイバーセキュリティの確保】（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　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。配電事業者においても同規格に準じること。
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。配電事業者においても同規格に準じること。
三　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。）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。

https://www.meti.go.jp/policy/safety_security/industrial_safety/law/files/dengikaishaku.pdf

## 保安規程と各GLとの紐づけ

「保安規程」に事業者が定めるべき内容を規定する、**電気事業法施行規則第５０条第２項**(電気事業)／**第３項第９号**(その他事業)**の解約適用に当たっての考え方（経産省内規）**において、電制GL／自家用GLが引用。

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　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。

https://www.meti.go.jp/policy/safety_security/industrial_safety/law/files/hoankiteikaisyaku.pdf

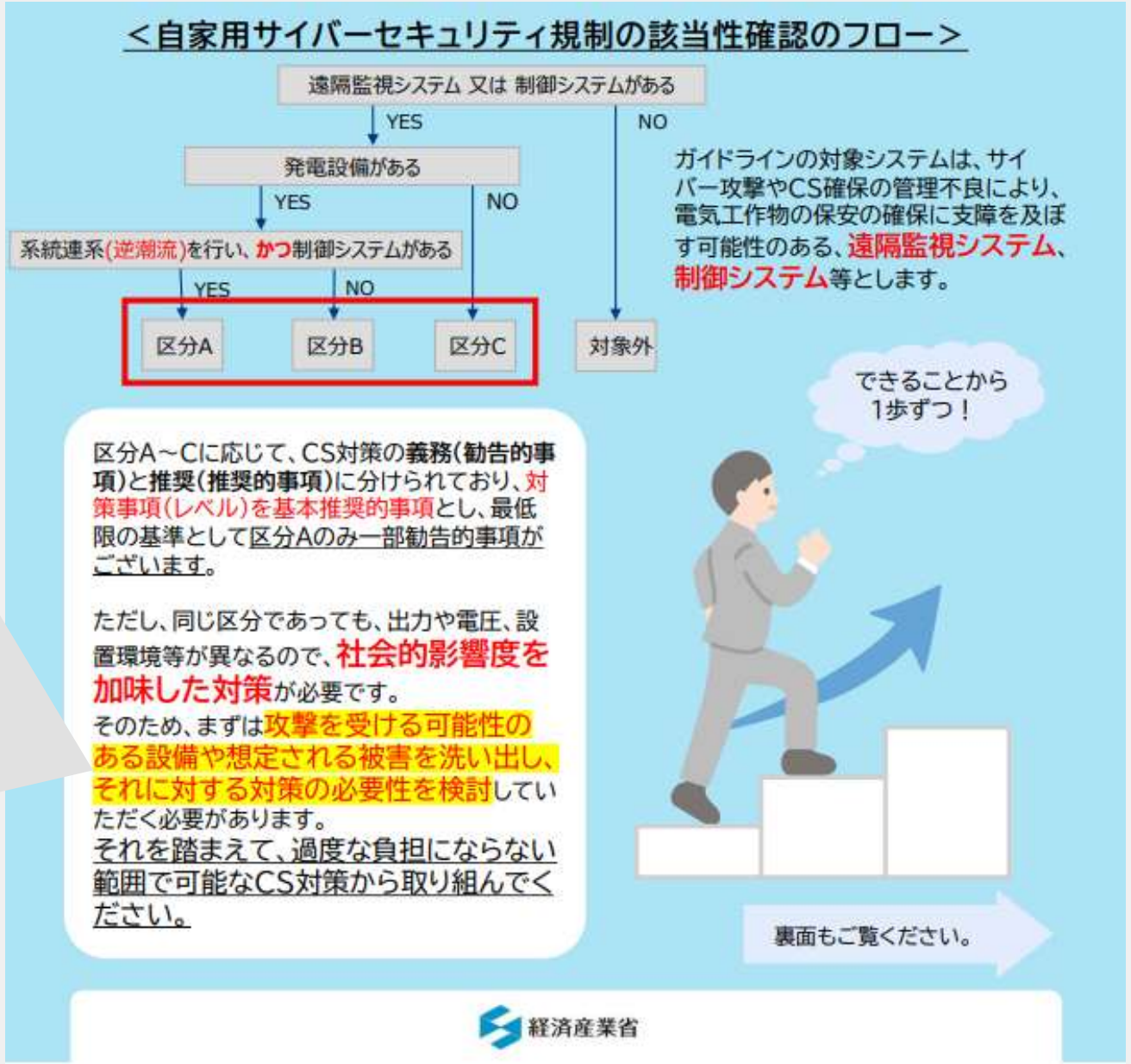
２．自家用電気工作物
遠隔監視システム及び制御システムにおいては、「自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン（内規）」（令和４年６月１０日付け２０２２０５３０保局第１号）によること。

# “自家用CSガイドライン”の勘所

# チェックリストの確認前に、最初に考えること・・・

**皆さんが担当されている設備において、“起こってほしくないこと“はなんですか？**
**(安全、環境、地域社会、品質、コスト等々)**

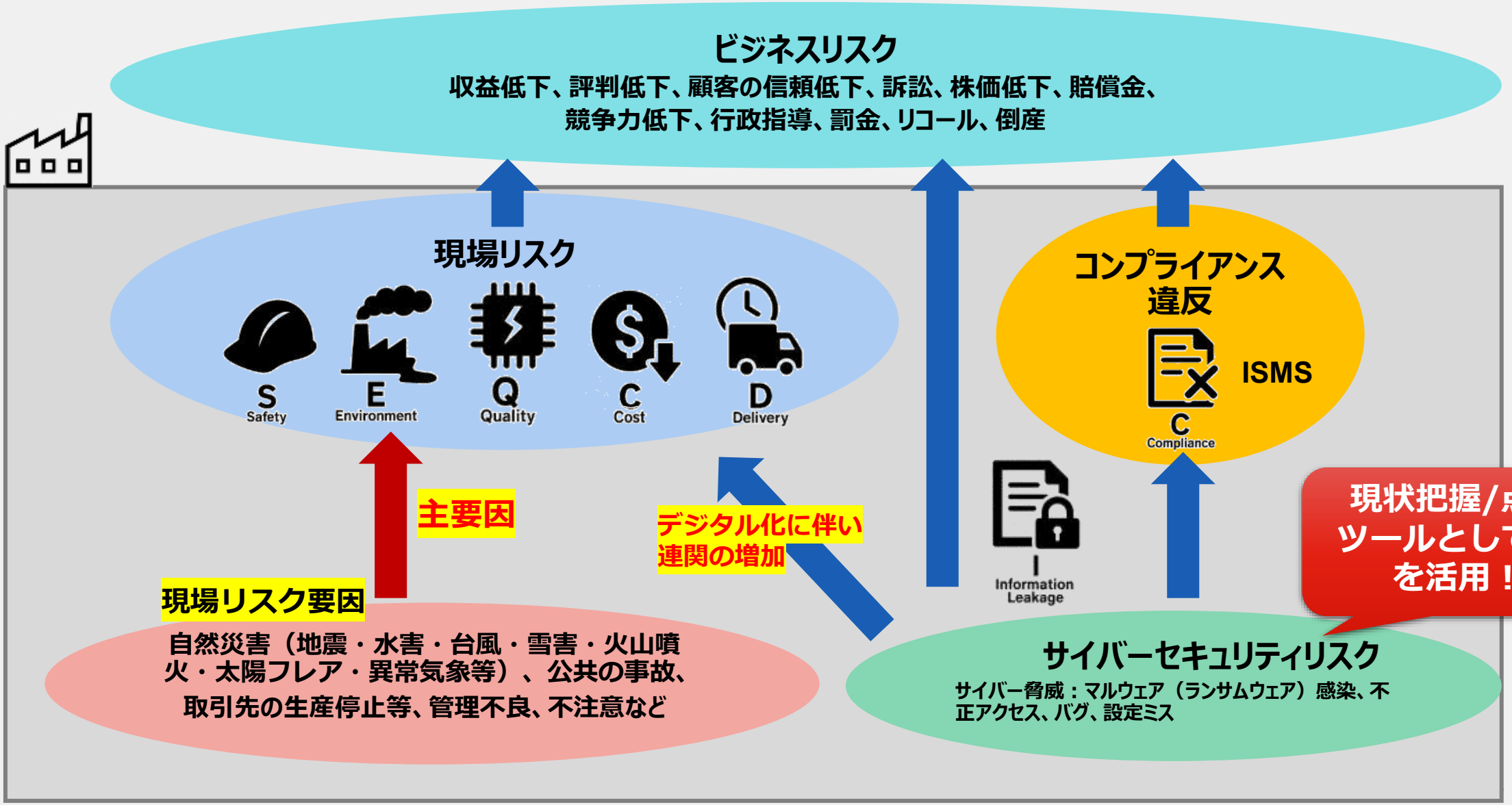
**サイバー的な要因（パソコンでの設定変更など）で、その事象／被害を起こせますか？**




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

# 現場リスクとサイバーセキュリティリスクの関係性

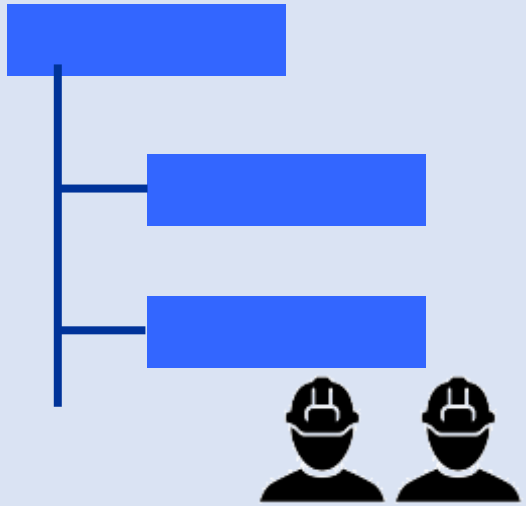
サイバーセキュリティ対策を、多様なビジネスリスクの“原因事象の一つ”に対するリスク対応として考える



# OTセキュリティ４本柱 – 組織/運用/技術/SCM

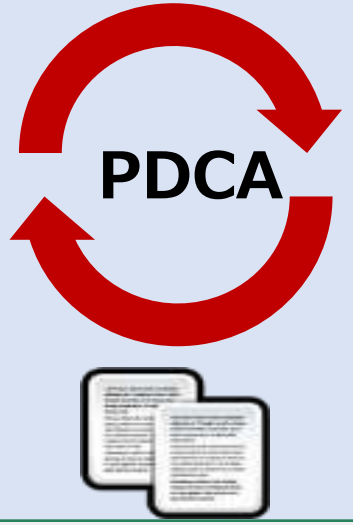
『自家用GL』には、個々の対策における標準的手法が記載されている。
これらの対策がリスク低減にどのように寄与するのか、各要求事項の理由や背景を理解することが重要。

## 組織



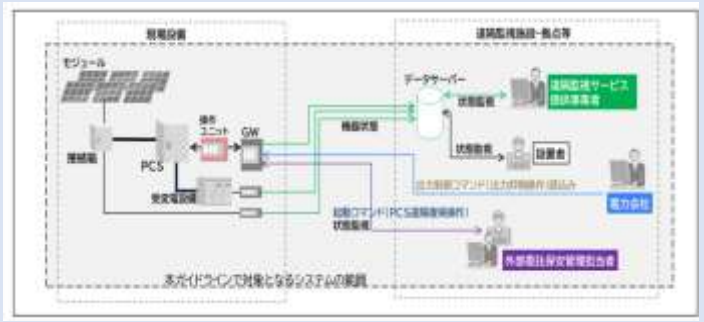
- ガバナンス体制
- 現場教育

## 運用



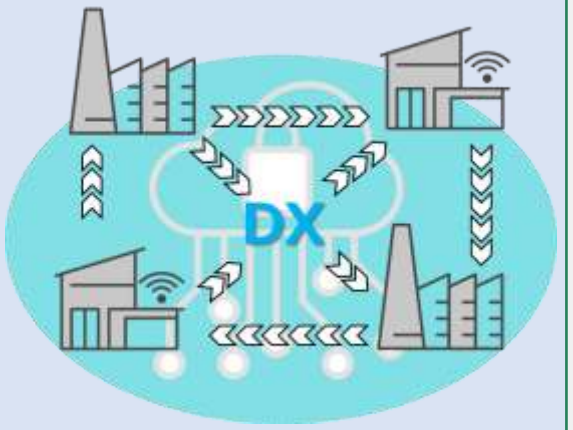

- 定期評価
- ルール策定・管理
- 資産管理
- インシデント対応

## 技術



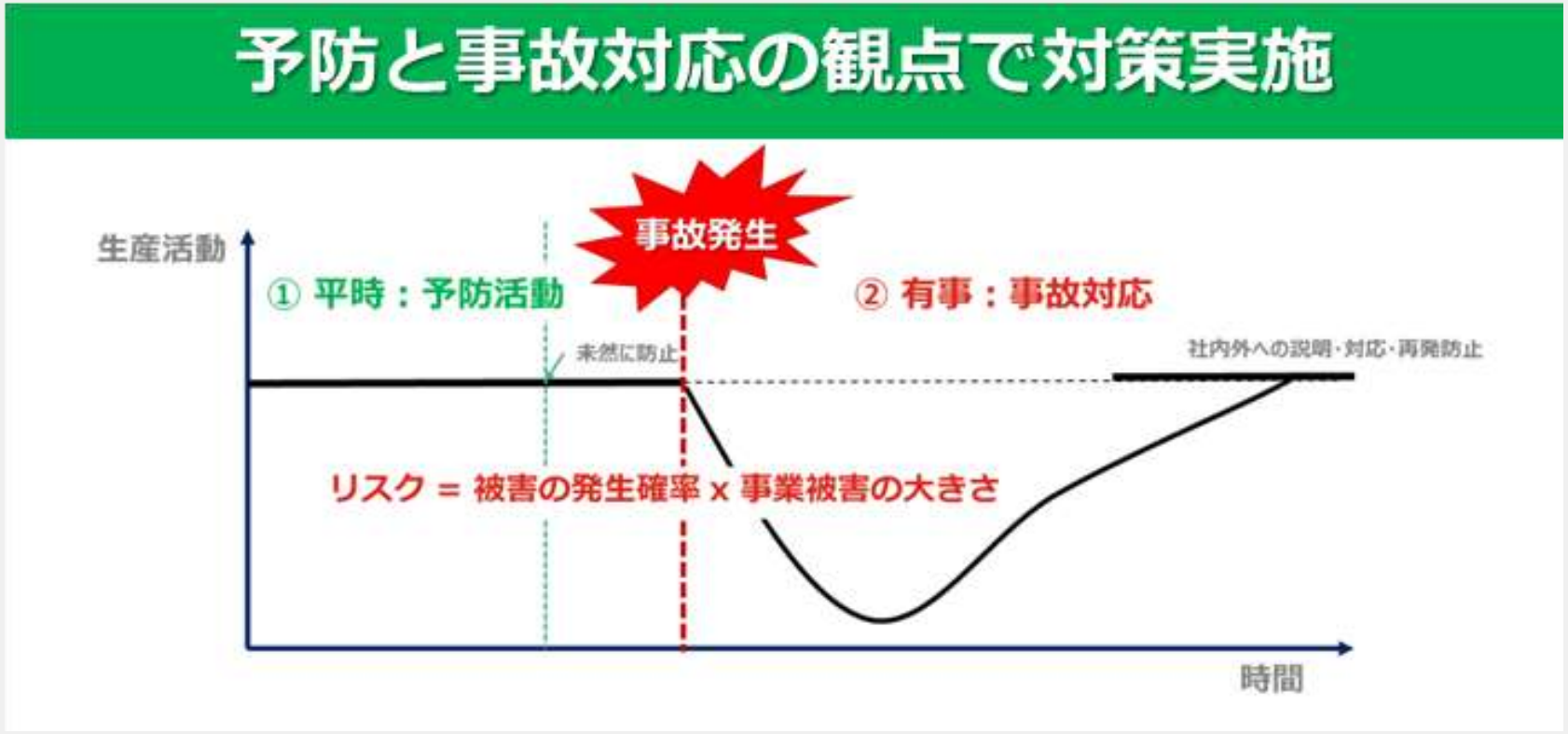
- 端末保護
- ネットワーク
- ログ
- 物理セキュリティ

## SCM




- 外部管理
- 内部管理

# OTセキュリティのやることは２つ、①平時の予防活動と②有事の事故対応




技術導入で予防的観点で
効果を発揮
技術

組織・運用の建て付け、
対応訓練が不可欠
組織
運用

サイバー空間を安心・安全に保つことで「現場も安全・安心に、そして生産活動の維持」に貢献

# 自家用GL要求事項：組織・運用・技術・SCM観点の関連付け

| カテゴリ | サブ項目 | 章 | 規定項目 |
|---|---|---|---|
| - | - | 2 組織 | 予防 事故対応 |
| 組織 | ガバナンス体制 | 2-1 | 体制 |
| 組織 | ガバナンス体制 | 2-2 | 役割 |
| 組織 | 現場教育 | 2-3 | セキュリティ教育 |
| - | - | 3 文書化 | 予防 事故対応 |
| 運用 | ルール策定・管理 | 3-1 | 文書管理 |
| 運用 | 定期評価 | 3-2 | 実施状況の報告 |
| - | - | 4 セキュリティ管理 | 予防 事故対応 |
| 運用 | ルール策定・管理 | 4-1 | セキュリティ管理 |
| - | - | 5 機器のセキュリティ | 予防 |
| SCM | 内部管理 | 5-1 | セキュリティ仕様の確認 |
| SCM | 外部管理 | | |
| 運用 | 資産管理 | 5-2 | 機器の取り扱い |
| 運用 | 定期評価 | | |
| - | - | 10 セキュリティ事故の対応 | 事故対応 |
| 運用 | インシデント対応 | 10-1 | 情報の収集 |
| 運用 | インシデント対応 | 10-2 | セキュリティ事故の対応体制等 |
| 運用 | インシデント対応 | 10-3 | セキュリティ事故の報告と情報共有 |
| 運用 | インシデント対応 | 10-4 | 周知と訓練 |

| カテゴリ | サブ項目 | 章 | 規定項目 |
|---|---|---|---|
| - | - | 6 通信のセキュリティ | 予防 |
| 技術 | ネットワーク | 6-1 | 暗号化・通信プロトコルの最適化 |
| 技術 | ネットワーク | 6-2 | ネットワークの管理 |
| - | - | 7 システムのセキュリティ | 予防 |
| 技術 | 端末保護 | 7-1 | システムのセキュリティ |
| - | - | 8 運用のセキュリティ | 予防 |
| 技術 | 端末保護 | 8-1 | システムの管理 |
| 技術 | ログ | 事故対応 | |
| 運用 | ルール策定・管理 | 8-2 | 機器・外部記憶媒体の管理 |
| 技術 | 端末保護 | 8-3 | データの管理 |
| 技術 | 端末保護 | 8-4 | ぜい弱性の管理 |
| | | 9 物理セキュリティ | 予防 |
| 技術 | 物理 | 9-1 | 物理セキュリティ |

# サイバーセキュリティ・脅威の入口

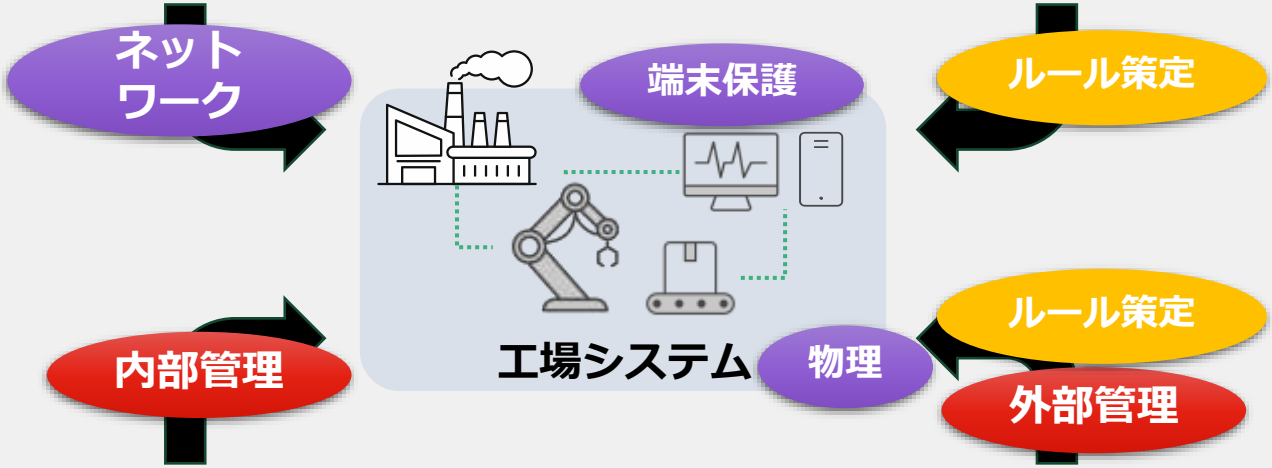
制御システムに対する脅威の入口（侵入経路）は大まかに４種類！

## 工場に被害をもたらす４つの脅威の入口

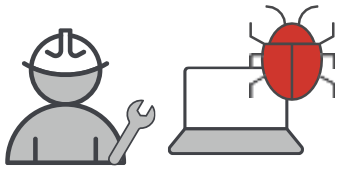
| | |
|---|---|
|  | ① 外部ネットワーク経由のサイバー攻撃 |
|  | ② USBメモリ経由のサイバー攻撃 |
|  | ③ 外部からの持ち込みデバイス |
|  | ④ 不正な動作をするコードを調達時に埋込み |

①外部NW

②USBメモリ (外部記憶媒体)




④調達品経由



③持込デバイス

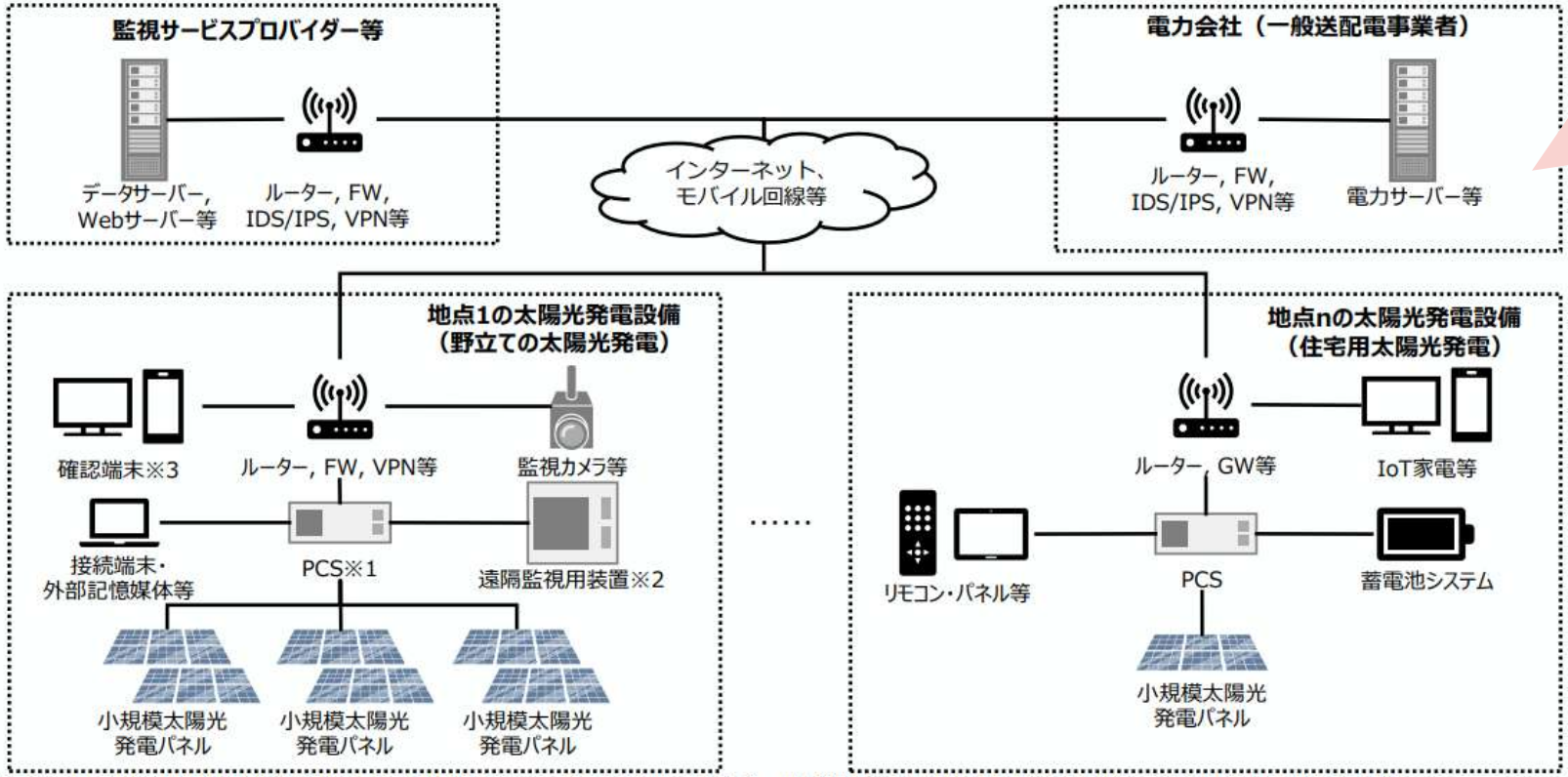
**外部ネットワーク経由のサイバー攻撃が全体の90%**

**工場のセキュリティは「確率だけでなく、被害の大きさ」で判断しないと最悪の事態は回避できない**

# 小規模太陽光発電設備のリスク分析例

# 基本構成図（モデルシステム例）

- 小規模太陽光発電設備に対するサイバーセキュリティ上の脅威を分析するためのモデルシステム図を作成した。
- 複数台に対する同時多発的な脅威を考慮するために、複数の種別・地点の太陽光発電設備を考慮できる構成とした。




※1 PCSは、電力会社または配信事業者が提示する出力制御スケジュール情報を取得し、そのスケジュールに応じて発電出力を制御する機能を有するPCS（いわゆる「広義PCS」）を指す。
※2 PCSに対して別途接続される遠隔監視用装置を対象とするが、遠隔監視と出力制御の両方が一体化したPCSも販売されている。
※3 監視サービスにアクセスして発電状況等を確認する端末を指す。

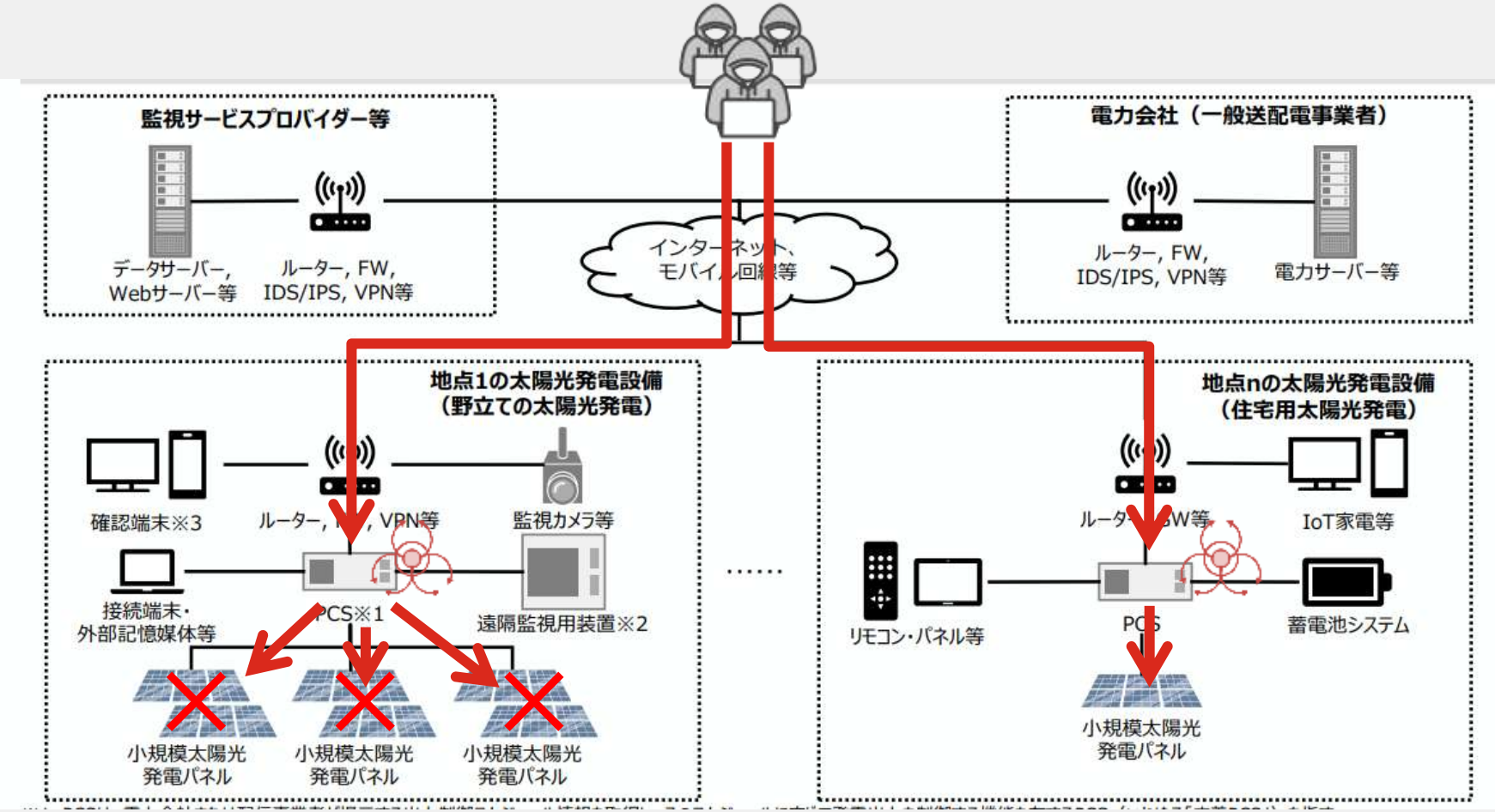
**“起こってほしくないこと“はなんですか？**
**(安全、環境、地域社会、品質、コスト等々)**

**サイバー的な要因（パソコンでの設定変更など）で、その事象／被害を起こせますか？**

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/pdf/018_06_01.pdf

# リスク分析の例

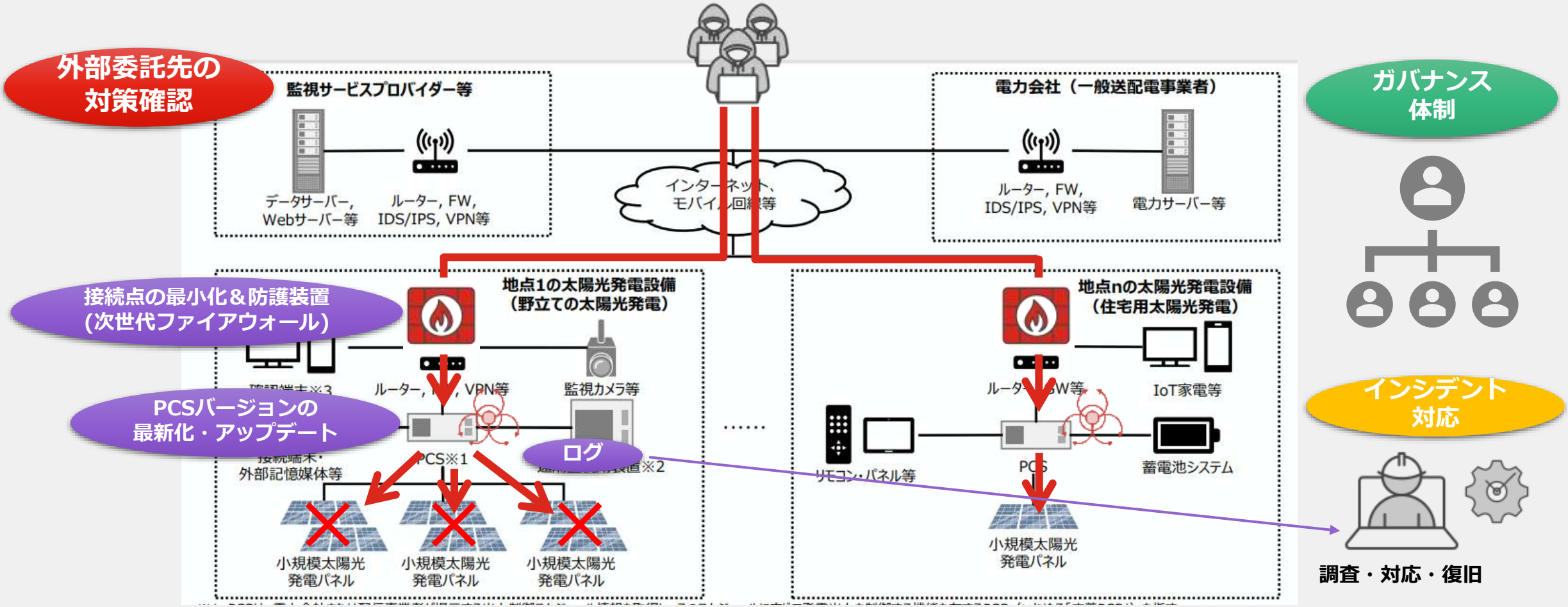
**攻撃シナリオ例：**
PCSの脆弱性が悪用され、**外部ネットワークから複数のPCSに対する不正アクセス**が実施される。外部ネットワークを介して不正な出力制御指令が送信されることで、**複数の太陽光発電設備における発電が停止**する。




https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/pdf/018_06_01.pdf　より、一部改変

# リスク分析を踏まえた予防／事故対応対策の例

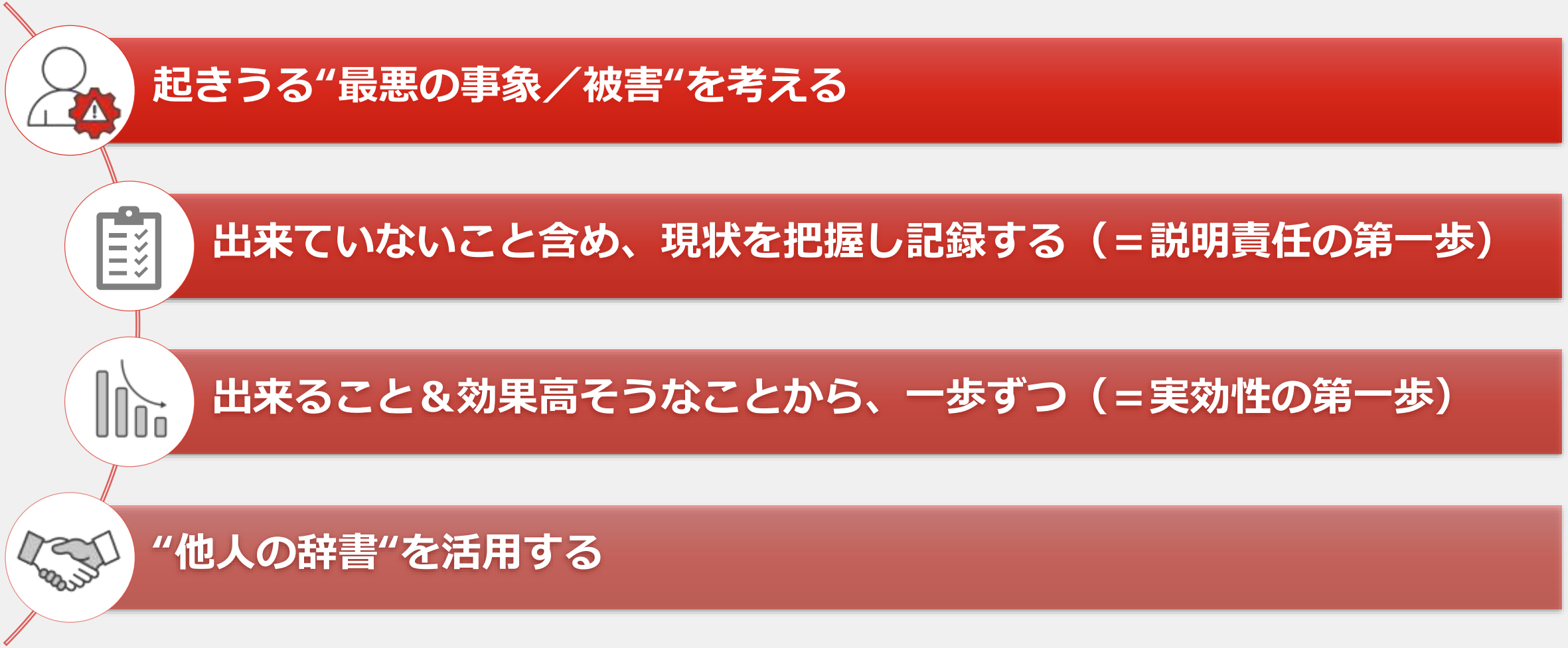
**攻撃シナリオ例：**
PCSの脆弱性が悪用され、**外部ネットワークから複数のPCSに対する不正アクセス**が実施される。外部ネットワークを介して不正な出力制御指令が送信されることで、**複数の太陽光発電設備における発電が停止**する。




https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/pdf/018_06_01.pdf　より、一部改変

# 今日からできる第一歩

# 今日からできる第一歩



# “説明責任“も重視される時代ですが・・・”実効性”を忘れずに！

そもそも論ですが、「サイバーセキュリティ対策」の目的は何ですか？

説明責任

実効性

- 規制/ガイドラインへの適合
- ルールの制定、文書化

▼

**形骸化に注意**

“経済産業省のガイドラインに
適合しています！”

- ルールの順守状況
- 運用コスト含む効率性
- リスク評価に応じた濃淡

▼

**「組織」「運用」「技術」のバランス**

“経済産業省のガイドラインを参考に
自社のリスク応じた対策に
落とし込んでいます！”

**現場のビジネスリスクの低減が目的。ガイドライン適合はその手段。**

# 安全安心で便利な電気保安の明日のために／できることから一歩ずつ！

## 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。

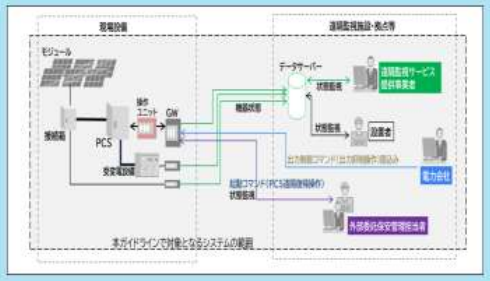
区分A～Cに応じて、CS対策の**義務（勧告的事項）**と**推奨（推奨的事項）**に分けられており、対策事項（レベル）を基本推奨的事項とし、最低限の基準として区分Aのみ一部勧告的事項がございます。

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

| | | |
|---|---|---|
| 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 |

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

FORTINET

# OTセキュリティといえばフォーティネット