経済産業省

産業構造審議会
保安・消費生活用製品安全分科会
第１９回電力安全小委員会　資料４

# 電力分野におけるサイバーセキュリティ対策と「産業サイバーセキュリティ研究会 電力SWG」での検討状況

2019年3月15日

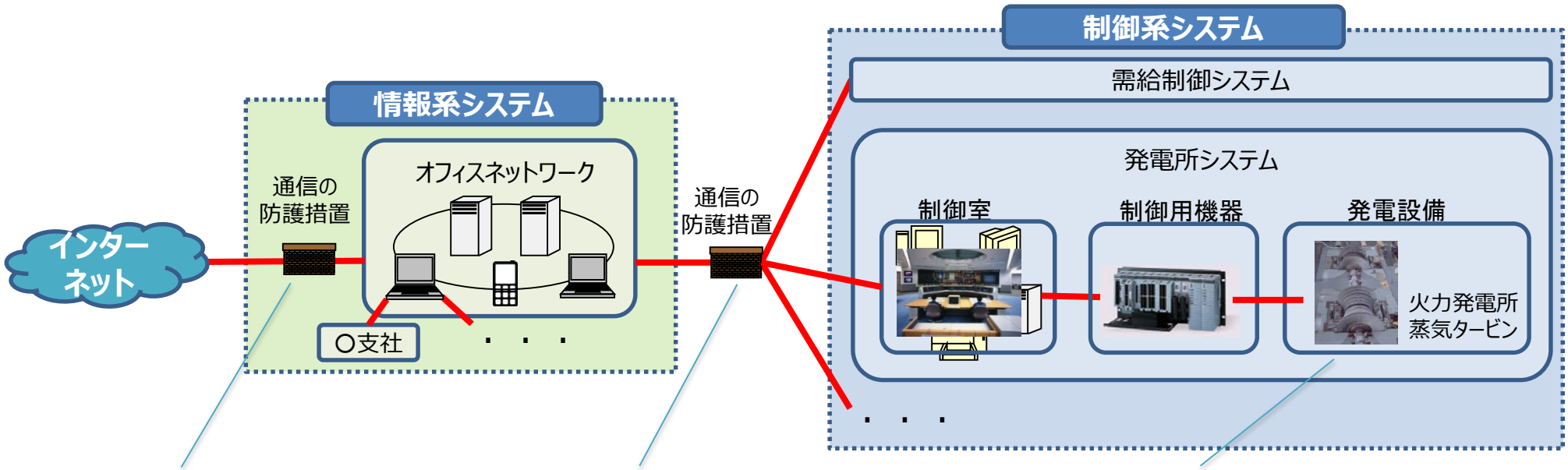
経済産業省 産業保安グループ

電力安全課

# 1．電力分野の情報ネットワークの概要

- 電力分野における情報ネットワークは、インターネットとも繋がり、顧客データ等をやりとりする「**情報系システム**」と、発電・送配電設備等をコントロールする「**制御系システム**」に大別される。
- **制御系システムはインターネットとの直接的な接続点は存在しない。**また、ファイアウォールや通信の状態監視、通信方向を限定する等により、**多層的に防御**されている。

## ＜情報系・制御系システムの模式図（電力分野）＞




・インターネットとの接続点の制限
・アクセス制御
・通信状態の監視　等

・アクセス制御
・通信方向の制限
・ログの取得　　等

・アクセス制御（通信制御、入室管理）
・マルウェア対策
・不正プログラム防止　等

# ２－１．これまでのサイバーセキュリティ対策

- サイバー攻撃の先鋭化・巧妙化や攻撃対象の増加、電力自由化に伴う多種多様な事業者の参入等の環境変化を踏まえて、経済産業省及び電気事業者においては、以下のような対策をこれまで実施してきたところ。

**＜既存の対策の例＞**

**① サイバーセキュリティ対策の法制化**

✓ 日本電気技術規格委員会（JESC）が策定した電力分野のサイバーセキュリティに関するガイドラインを電気事業法下の技術基準等に組み込み、ハード・ソフト両面の対策の実効性を担保。

**② 電力ISACの設立**

✓ 電力業界のサイバーセキュリティ対策の強化を目的に設立。電力事業者等の間で、情報の収集・分析や各社対策（対策事例のグッドプラクティスや、社内セキュリティ教育の方法等）の共有を実施。国内外の機関との連携強化。

**③ サイバーセキュリティ人材の育成（ICSCoE）**

✓ 独立行政法人 情報処理推進機構（IPA）産業サイバーセキュリティセンター（ICSCoE）が実施する実践的な演習・対策立案等のトレーニングに、電力分野からも多数参加。

# 2－2．対策① サイバーセキュリティ対策の法制化

- 電力分野のサイバーセキュリティ対策強化に向けて、2016年3月に**スマートメーターシステムセキュリティガイドライン**、2016年5月に**電力制御システムセキュリティガイドラインをJESCが策定。**
- これらのガイドラインを、**電気事業法下の技術基準と保安規程にそれぞれ組み込んだ**ことにより、ハード・ソフト両面の対策の実効性を担保している。（施行日：2016年9月24日）

## 電力制御システム 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。

**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

**<u>安定供給等の観点から、システムの重要度を定義</u>**
↓
重要度に応じた追加的セキュリティ対策を提示

・ログの取得 ・入退管理

## スマートメーターシステム セキュリティガイドライン

**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

# 2－3．対策② 電力ISACの設立（情報共有体制の確立）

- 金融や通信等の他の重要インフラ分野の取組を踏まえ、業界大のサイバーセキュリティ対策強化を目的に、**2017年３月に電力ISAC（※１）が設立**された。
- 電気の安定供給の役割を担う事業者間で、**サイバーセキュリティに関する情報の収集・分析**や**各社のグッドプラクティスに係る情報共有**を行っている。
- 2018年10月には電力ISAC、E-ISAC、EE-ISACの間でMOU（※２）が締結され、海外との連携体制も構築されつつある。

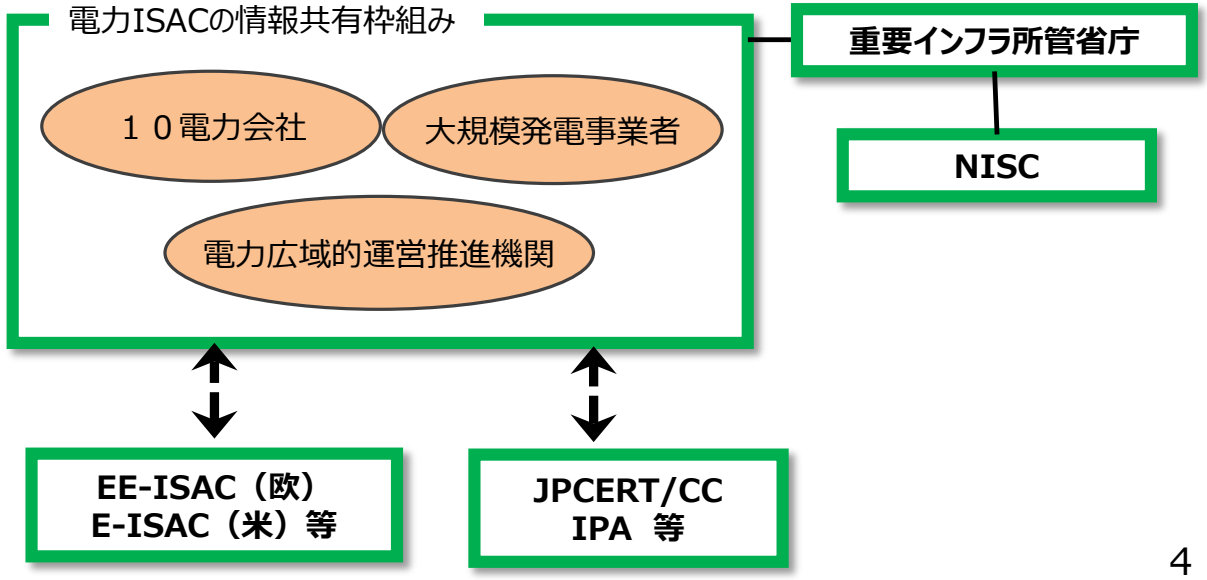
※１：ISAC：Information Sharing and Analysis Center

※２：MOU：Memorandum Of Understanding（友好関係構築を目的とした覚書）

＜情報共有体制＞

国内外の関係機関からの情報収集及び情報の分析のほか、会員同士の情報共有の場として、以下のWGを実施している。

| WG名 | 概要 |
|---|---|
| 火力システムWG | 火力の発電所監視制御システム等のサイバーセキュリティに関するグッドプラクティス等を共有し、課題解決に向けた意見交換を行う。 |
| 水力システムWG | 水力の発電所監視制御システム等のサイバーセキュリティに関するグッドプラクティス等を共有し、課題解決に向けた意見交換を行う。 |
| 需給・系統システムWG | 需給制御システム及び系統制御システムのサイバーセキュリティに関するグッドプラクティス等を共有し、課題解決に向けた意見交換を行う。 |
| 共通・ITシステムWG | 最新のサイバーセキュリティに関するトレンドや電力分野に係るIT/OT全般に関するグッドプラクティス等を共有し、課題解決に向けた意見交換を行う。 |
| リスクアセスメントWG | 様々なリスクアセスメント手法の概要・特徴を理解し、各社で効果的に実施していくために、課題の共有とともに解決に向けた意見交換を行う。 |
| SMシステム脆弱性情報共有WG | スマートメーターシステムに関して、重大な脆弱性・セキュリティ事故・事象が発生した際に、必要に応じて関係者間で情報交換を行う。 |



# 2－4．対策③ サイバーセキュリティ人材の育成（ICSCoE）

- 重要インフラ事業者の能力強化を目的に、2017年4月、IPAに産業サイバーセキュリティセンター(ICSCoE)を設置。各業界における人材育成やリスク評価の実施等を進めることにより、「国民が安全で安心して暮らせる社会の実現」に貢献していく。
- 人材育成の中心となる中核人材育成プログラムでは、電力、ガス、鉄鋼、石油、鉄道、放送、通信等の各業界60社以上から約80名/年の研修生を受け入れ（電力分野からは約20名/年が参加）、実践的な演習・対策立案等のトレーニングを実施している。

### ①模擬プラントを用いた対策立案（人材育成）

- 情報系システムから制御系システムまでを想定した模擬プラントを設置。専門家とともに安全性・信頼性の検証や早期復旧の演習を行う。
- 海外との連携も積極的に実施。

### ②実際の制御システムの安全性・信頼性検証等

- 社会インフラ・産業基盤に係る制御システムの安全性・信頼性に関するリスク評価を実施。
- あらゆる攻撃可能性を検証し、必要な対策立案を行う。

### ③攻撃情報の調査・分析

- 最新のサイバー攻撃情報（ex.おとりシステムの観察や民間専門機関が持つ攻撃情報）を収集。
- 新たな攻撃手法等を調査・分析し、人材育成やシステム検証に活用。

# 3－1．産業サイバーセキュリティ研究会とWG１、電力SWGの位置づけ

- 我が国の産業界が直面するサイバーセキュリティの課題を洗い出し、関連政策を推進していくため、経済産業省において2017年12月に「**産業サイバーセキュリティ研究会**」を設置。
- 制度・技術・標準化を検討するWG１では、産業分野ごとのSWG（サブワーキンググループ）を設置。**電力SWG**は2018年6月から検討を進めてきている。

**産業サイバーセキュリティ研究会**　■政策の方向性を提示

**WG１　制度・技術・標準化**　■制度・技術・標準化を一体的に政策展開する戦略を議論。本年1月～２月、「サイバー・フィジカル・セキュリティ対策フレームワーク」のパブコメを実施。

- ビル（エレベーター、エネルギー管理等）
- **電　　力**
- 防衛産業
- 自動車産業
- その他コネイン関係分野（スマートホーム等）

**Industry by Industryで検討**
(分野ごとに検討するSWGを設置)

**WG２　経営・人材・国際**

**WG３　サイバーセキュリティビジネス化**

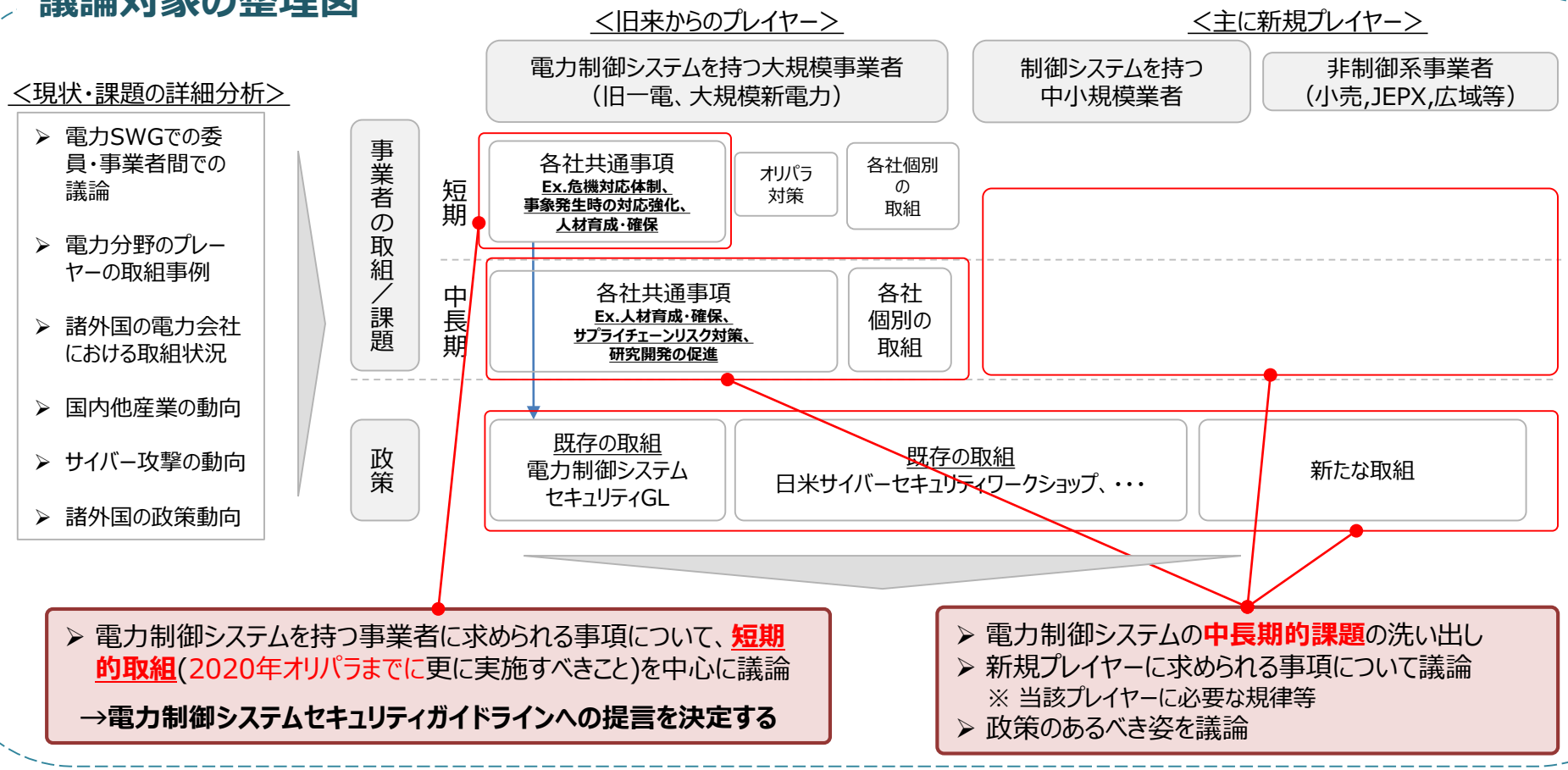
# 3－2．電力SWGにおける検討の全体像

- より効果的かつ実効的なサイバーセキュリティ対策が望まれる現状を踏まえて、以下の①だけでなく②も重要という観点から、電力SWGでは、短期的取組と中長期的取組に分けて議論を行うこととした。

  ①サイバーインシデントの発生を防ぐ（＝**事前防御の向上**）

  ②事象発生時の影響を最小化する（＝**事後対応力の強化（早期発見、迅速な対処）**）

## 議論対象の整理図



# 3－3．短期的取組

- 2020年の東京オリンピック・パラリンピックも見据え、電力分野で短期的に取り組むべきサイバーセキュリティ対策として、下記について提言として議論を取りまとめた。
- その提言を受けて、規格作成団体である**JESCにおいて電力制御システムセキュリティガイドライン**（P. 3 参照）**の改正を現在審議中**。

## （１）危機管理体制の構築

**◆危機管理体制との連携強化**

被害拡大の可能性が見込まれる場合には、危機管理体制とサイバーインシデント対応体制が連携できるよう役割や手順を予め定めておくことが期待される。

**◆情報システム（IT）部門と制御システム（OT）部門の密な連携**

ITシステムとOTシステムの間にある考え方の違いを双方の部門の関係者が認識した上で、個々の事業者における状況を踏まえた体制の構築や人材育成・交流、教育等を通じてこの差を補完していくことが重要である。

## （２）人材の育成・確保

**◆「戦略マネジメント層」の役割及び育成**

「戦略マネジメント層」を構成する人材は、セキュリティ分野のみの知見だけではなく、OTシステムや経営企画に関わる幅広い知見を有することが望ましく、組織として人材がバランスよく適材適所で配置されることが重要である。

**◆セキュリティ人材の確保**

優秀な人材を育成し、社内に定着させるためには、社内のセキュリティ人材に求められる役割・機能を明確にし、キャリアパスや育成プランを用意することが望ましい。

## （３）事象発生時の対応強化

**◆社外連携の強化**

地域や電力業界に設置されているセキュリティ連絡会等での活動機会を活用し、社外との連携を強化することで自組織のみならず利害関係者全体のサイバーレジリエンスをより強化することが望まれる。

**◆危機管理体制の実効性向上**

サイバーインシデントの発生と連鎖障害の拡大等を想定したシナリオを設定し、既存のマニュアルやルール、プロセスや体制に関する課題、改善策を抽出する「演習」を行うことが有効である。

# ３－４．中長期的課題

- 今後、電気事業者によるサイバーセキュリティ対策の実態把握や海外や他業種の動向調査を進めつつ、強化していくべき取組の内容を具体化していく予定。
- 下記の中長期的課題について、**次年度以降も電力SWGにて継続して検討を行う。**

【検討事項】

① サプライチェーンリスク対策について、政府や他分野等の取組も進められているところ、電力分野において、どのような対策が考えられるか。

② 大手電気事業者のサイバーセキュリティの実態をどのように把握し、今後の対策の検討を行うことが適切か。

③ 新規参入者へのサイバーセキュリティに関する意識の醸成をどのように図っていくべきか。

# 【参考】電力分野におけるサイバーセキュリティを取り巻く状況と目指す方向

**＜脅威の高まり＞**

**＜攻撃事例＞**

①攻撃の先鋭化・巧妙化
- 特定の制御系にまで攻撃が浸透→攻撃力の向上
- 攻撃回数の指数的増加
- システム、機器製造時に不正プログラムを仕込む

ウクライナ大停電('15,'16)
・情報系システムから制御系まで不正侵入

携帯メモリの不正プログラム発見('16)
・中国のサーバーへの情報漏洩が発覚(米)

ロンドン('12),リオ五輪('16)
・毎秒1万回以上の不正通信

②攻撃対象の拡大
- IoT機器拡大、ネット接続機器は300億個へ（2020年には現在の1.7倍）
- 電力自由化により多様なプレイヤーが参入

小規模PVや風力の脆弱性指摘('18)
・セキュリテ会社が新たな脅威として警鐘

③攻撃への備えが不十分
- 危機や必要な対策への認識と取組が不十分
- 下請け企業ほど対策が遅れがち（サプライチェーンのリスク拡大）

WannaCryの猛威 ('17)
・150か国23万台のPCが感染。Windows脆弱性の指摘に関わらず、対策を怠るPCを中心に感染拡大

**①サイバーインシデントを防ぐ（＝事前防御の向上）**
**②インシデント発生時の影響を最小化する（＝事後対応力の強化（早期発見、迅速な対応））**

**＜旧来からのプレイヤー＞**

**＜主に新規プレイヤー＞**

| | 電力制御システムを持つ大規模事業者（旧一電、大規模新電力） | 制御システムを持つ中小規模業者 | 非制御系事業者（小売,JEPX,広域等） |
|---|---|---|---|
| **事業者の主な取組** 事前対策 | ➢ 組織；専門組織・管理責任者の設置<br>➢ 人材；セキュリティ教育、外部教育機関への人材派遣<br>➢ 技術；マルウェア防止対策、通信ログ管理、不正処理検知<br>➢ 物理；制御システムの原則分離、外部媒体管理、入退管理・制限 | 電力制御システムGLに記載された事項の取組<br>※電力制御GLは発電事業者までが対象 | 各社はセキュリティポリシーを策定、取組 |
| 事後対策 | ➢ 組織；事故時対応の具体化<br>➢ 人材；事故時に対応する訓練の実施 | | |

電力制御システム／スマートメーター／その他各社個別取組

中小事業者向けGLに記載された事項の取組

**主な政策**

電力制御システムセキュリティGL制定('16~)
・制御系システムを持つ事業者に各対策を推奨・勧告（電技解釈に引用）

スマートメーターシステムセキュリティGL制定('16~)
・スマメセキュリティ対策を推奨・勧告（電技解釈に引用）

電力ISAC設立('17~)
・サイバー情報の共有・分析組織

IPA人材育成研修('17~)
・制御系のセキュリティ専門人材養成(ICS-COE)

日米電力サイバーセキュリティWS('18~)
・日米の政府、電力、業界団体、研究機関、有識者が知見を共有

ERABセキュリティGL('17~)
・ERAB事業者が取り組むべき推奨事項（法的義務なし）

セキュリティチェックツール('16~)
・電力広域機関が会員企業向けにサービス提供