経済産業省

電力SWGの開催と電力分野における サイバーセキュリティ対策について

2018年6月12日

経済産業省

電力安全課

電力産業・市場室

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

２．電力SWGの設置について

３．電力分野におけるサイバーセキュリティに関する
　　政策動向やサイバー攻撃の現状

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

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、平成２９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を設置。

(参考)WG1における検討状況の紹介：
『サイバー・フィジカル・セキュリティ対策フレームワーク』のイメージ

- サイバー・フィジカル・セキュリティ対策フレームワークは、価値創造のための活動が営まれる産業社会を、下記の**三層構造**と**6つの構成要素**で捉え、包括的にセキュリティポイントを整理するための指針となるもの。

◆三層構造

サイバー空間におけるつながり
【第３層】

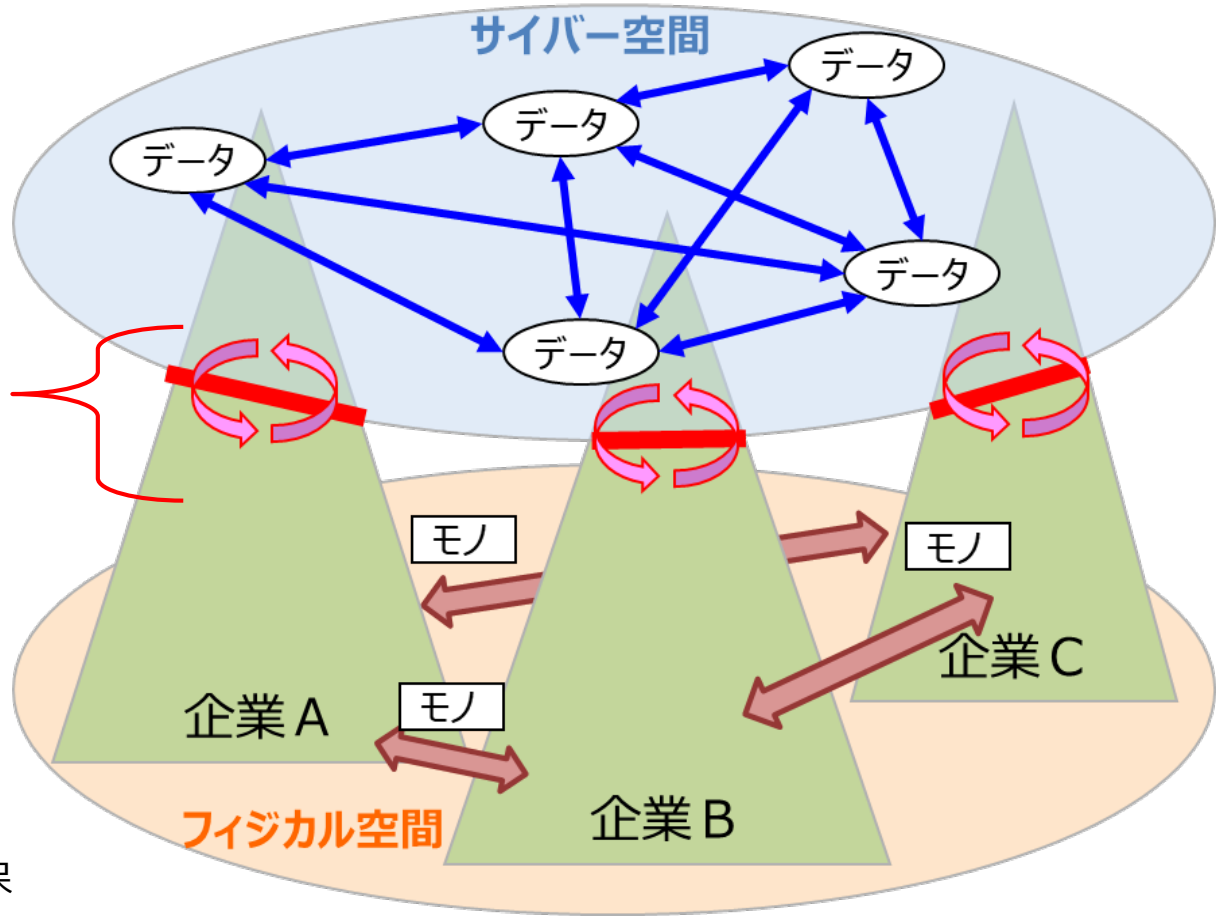
- 自由に流通し、加工・創造されるサービスを創造するためのデータの信頼を確保

フィジカル空間とサイバー空間のつながり
【第２層】

- フィジカル・サイバー間を正確に“転写“し、機能の信頼を確保
（現実をデータに転換するセンサーや電子信号を物理運動に転換するコントローラ等の信頼）

フィジカル空間における企業間のつながり（従来型サプライチェーン）
【第１層】

- 適切なマネジメントを基盤に各主体の信頼を確保



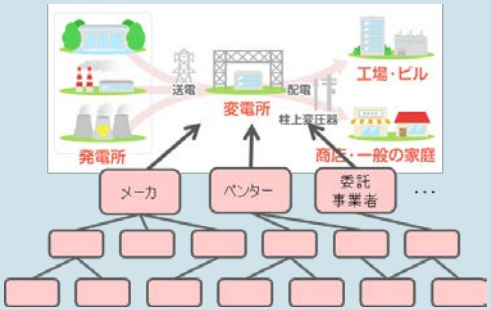
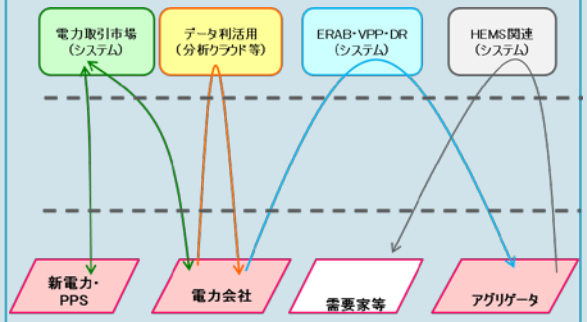
◆６つの構成要素　－組織、ヒト、モノ、データ、プロシージャ、システム

２．電力SWGの設置について

電力SWGの目的及びスケジュール

- あらゆる分野でデジタル化が進展する一方、多様化・巧妙化するサイバー攻撃の脅威は日々高まっており、重要インフラたる電力分野においても、サイバーセキュリティ向上に向けた不断の取組が求められている。
- 電力分野においては、2016年の小売の全面自由化等により新規参入者が拡大すると共に、発電・送配電事業を中心として、デジタル技術の活用が広がりつつある。加えて、2020年に東京オリンピック・パラリンピックを控え、サイバーセキュリティ確保の重要性は、これまでになく高まっている。
- こうした中で、2017年12月、産業横断的な更なるサイバーセキュリティ対策を検討する産業サイバーセキュリティ研究会が設置され、その下のワーキンググループにおいて、制度・技術・標準化の検討が進められている。
- これらの状況変化を踏まえ、電力分野のサイバーセキュリティに関する今後の取組について検討を行うため、産業サイバーセキュリティ研究会 制度・技術・標準化ワーキンググループの下に、電力サブワーキンググループ（電力SWG）を設置する。
- 電力SWGでは、電力を取り巻くサイバーセキュリティに関する現状、事業者の取り組み、官民が取り組むべき課題と方向性を議論しつつ、これらを踏まえ、官民が取り組む具体策についての検討を深める。具体的には、例えば、①電力制御系システムに関するセキュリティ向上策や、②電力制御系システムに関連した分野におけるセキュリティ向上策、③業界全体の取組向上に資する基盤整備などの具体的な対応策について、検討を深めていく。

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電力分野への適用

階層	第１層 フィジカル空間における繋がり（従来型サプライチェーン）	第２層 フィジカル空間とサイバー空間の繋がり	第３層 サイバー空間における繋がり
イメージ			・電力取引市場（システム） ・ERAB・VPP・DR（システム） ・HEMS関連（システム）　　等
関連事業者	・電力事業者 ・メーカー、ベンダー、委託先事業者	・電力事業者 ・JEPX ・アグリゲータ	・JEPX ・IoT、AI関係の事業者
対応策（例）	・調達する設備、システムのセキュリティ確保 ・取引先、委託先のセキュリティ状況の確認 ・取引先、委託先とのやり取りのセキュリティ確保	・フィジカル空間とサイバー空間の接点におけるセキュリティの確保	・データ品質の確認 ・データプラットフォームのセキュリティ確保
電力分野における特徴	・電力安定供給のコアとなる部分は電力制御システム ・電力制御システムとサイバー空間は分離されている ・近年、新規参入が相次いでいる（第２層、第３層）		
電力SWGとの関連	・第２回（案） 電力制御システムセキュリティガイドラインへの提言（短期的対応策）等	・第３回以降（案） 電力制御システムに関連した分野におけるセキュリティ向上策 業界全体の取組向上に資する基盤整備　等	

３．電力分野におけるサイバーセキュリティに関する政策動向やサイバー攻撃の現状

電力分野のサイバーセキュリティ対策の全体像（現状）

スマートメーター

ガイドライン<ベースライン>
・スマートメーター制度検討会セキュリティ検討ワーキンググループ報告書
→スマートメーターシステムセキュリティガイドライン（JESC）
→保安規制に取り込み

マネジメント<PDCAの継続促進>
・業界統一の監査制度を構築、内部監査・外部監査を実施済み
・ペネトレーションテスト（各社実施済み）

情報共有体制
<脆弱性・対策の相互参照>
・脆弱性情報共有・分析体制を電力ISACへ移行（電力10社）

制御系

ガイドライン<ベースライン>
・電力制御システムセキュリティガイドライン（JESC）
→保安規制に取り込み
・10社＋大規模発電事業者が対象

マネジメント<PDCAの継続促進>
・ガイドラインに基づく、対策の自己点検
・有識者を交えた、対策や自己評価等を含む各事業者の取組の客観的レビュー

情報共有体制
<脆弱性・対策の相互参照>
・脆弱性情報共有・分析体制（ISAC）を構築
（10社・大規模発電・広域等）
・外部有識者レビューの場として活用
→ベストプラクティスの共有

情報系

広域機関システムのセキュリティ
※電力会社は広域システムを介して連係
・ペネトレーションテスト（IPA）
・セキュリティ監査・第2GSOCへの参加

広域機関会員事業者の情報セキュリティ
・新規参入者向けガイドラインの作成
・普及啓発・セキュリティ情報提供等

各社セキュリティ意識の向上・継続
経営層の関与

国際・業界間協力

各国ISACや電力会社等との国際連携

他分野ISAC（金融、ICT等）との情報交換

各種WGを通じた会員間の情報共有

基盤整備

人材育成
IPA産業サイバーセキュリティセンター

研究開発
電力会社　他

【参考】昨今のサイバー攻撃　社会インフラを狙ったサイバー攻撃の増加と政府の取組み

- 近年、サイバー攻撃の事案は増加傾向。従来の情報窃取等を目的とした攻撃だけではなく、社会インフラに物理的なダメージを与えるサイバー攻撃のリスクが増大。テロリストや他国家によるサイバー攻撃には、大規模停電のように生命・財産を脅かすものがある。
- このため、国民の安全に責任を持つ政府と、インフラの安定的な運用に責任を持つ事業者が連携し、対策に取り組む必要がある。
- 政府においては、国連やOECD、APEC等で開催される国際会議や、重要インフラ防護やインシデント情報の共有等に関する専門的な多国間・二国間会合に参加し、多くの国々や民間団体と、サイバーセキュリティの確保に向けた方策の検討を行っている。

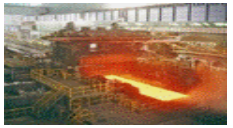
＜最近のサイバー攻撃の事例＞

電車システムへの攻撃（ポーランド、2008年）

14歳の少年がテレビのリモコンを改造して路面電車システムに侵入し、4車両を脱線させた。

製鉄所の溶鉱炉損傷（ドイツ、2014年）

何者かが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。



ロンドン五輪への攻撃（イギリス、2012年）

毎秒約１万件の不正通信。開会式会場の電力システムへの攻撃情報。手動に切り替え。

変電所へのサイバー攻撃（ウクライナ、2015年）

マルウェアの感染により、変電所が遠隔制御された結果、数万世帯で3～6時間にわたる大停電が発生。

ランサムウェア”WannaCry”（世界約150ヶ国、2017年）

5月12日頃から、マイクロソフト製品の脆弱性(※1)を悪用したランサムウェア(※2)「WannaCry」に感染する事案が発生。14日頃から国内においても被害を確認。

※1　本脆弱性の修正プログラムは、本年3月にマイクロソフトから公表済み。
※2　WannaCryに感染するとコンピュータのファイルが暗号化され、コンピュータが使用できない被害が発生。
　　攻撃者は暗号の解除に「Ransom（身代金）」を要求することから、このような不正プログラムをランサムウェアと呼ぶ。

電力分野の取組①　電力ISACの取組（民間事業者）

- 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・分析や各社のベストプラクティスに係る情報共有を行っている。
- 2017年５月には電力ISACと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。

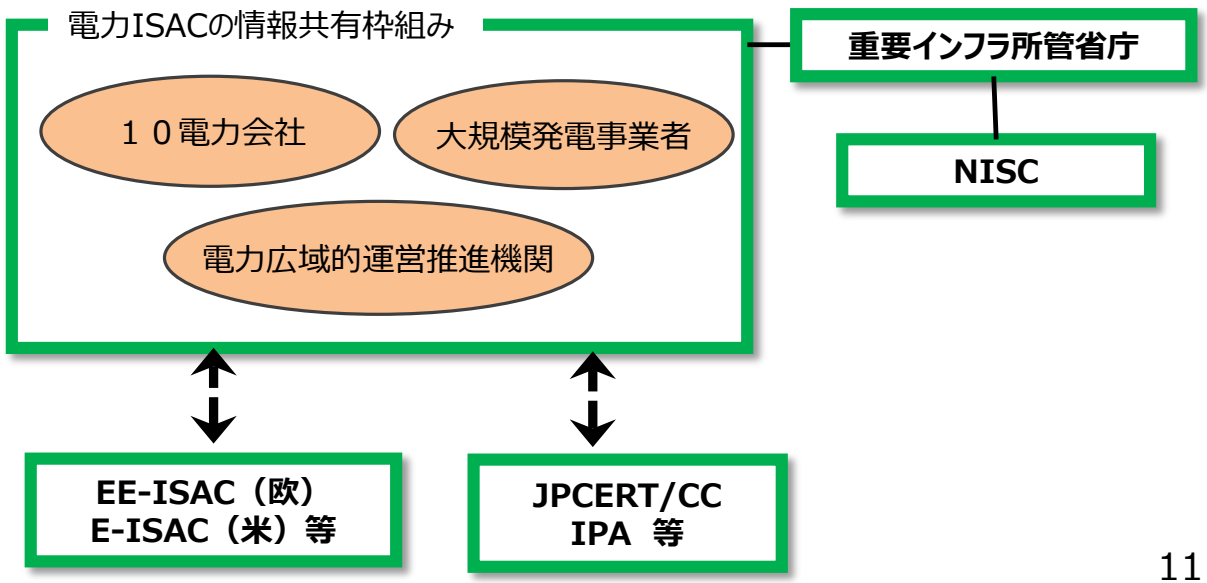
※１：ISAC：Information Sharing and Analysis Center

※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テーマ	
Ⅰ－1. 課題検討WG	電気事業の各分野（発電、送配電、ITなど）の取組みで、サイバーセキュリティに係る課題事項に関する意見交換
Ⅱ－1. ベストプラクティス共有WG	JESCガイドラインへの対応や取組みの外部有識者を交えた客観的レビューおよびベストプラクティスに関する会員間の情報交換
Ⅱ－2. セキュリティ教育WG	社内のセキュリティ教育やそのコンテンツ等に関する情報交換
Ⅱ－3. セキュリティ製品WG	ベンダーが提供するセキュリティ製品のベンチマーク、評価に関する情報共有
Ⅲ－1. セキュリティトレンドWG	定期レポートの内容に関する解説およびサイバー攻撃のトレンドや各社の対応状況に関する情報交換



電力分野の取組②　セキュリティガイドラインの電事法への組込み

- 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日本電気技術規格委員会（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。

<スマートメータシステムセキュリティガイドライン>

・２０１５年２月
　資源エネルギー庁を中心としたスマートメーター制度検討会セキュリティ検討ＷＧにて、ガイドライン策定要件等をとりまとめ。
・**２０１６年３月**
　第８５回ＪＥＳＣ委員会にてガイドライン策定。

<電力制御システムセキュリティガイドライン>

・２０１４年９月
　日本電気技術規格委員会（ＪＥＳＣ）で検討開始。
・２０１５年６月
　同委員会情報専門部会を新たに設置。
・**２０１６年５月**
　第８６回ＪＥＳＣ委員会にてガイドライン策定。

（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

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

＋

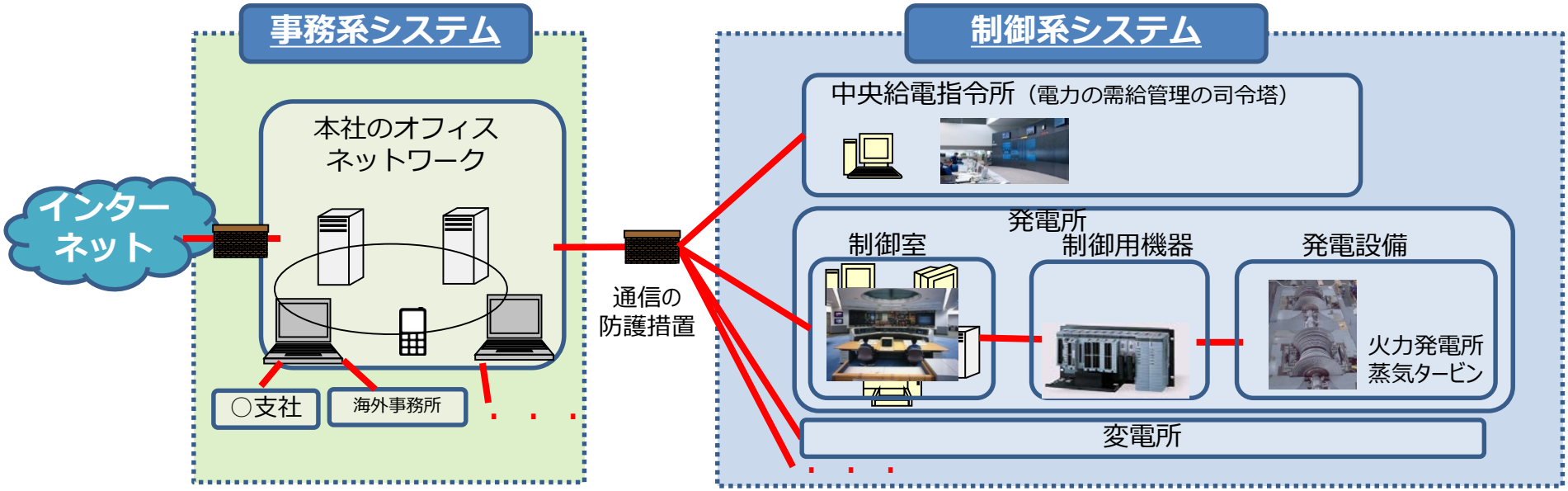
安定供給等の観点から、システムの重要度を定義
↓
重要度に応じた追加的セキュリティ対策を提示

・ログの取得　・入退管理

電力分野の取組③　制御系システムに関する取組

- 制御系システムは、事務系システムに比べ、①外部との直接の接続が少なく、②事業者毎に固有の仕様部分が多いため、従来、詳細な内部仕様等を把握できない限り、外部からの攻撃が困難だったが、標準技術・汎用製品利用の増加や外部ネットワークへの接続などにより、外部からのサイバー攻撃の可能性は増しており、攻撃の脅威が存在することを前提とした対策が必要とされている。
- 現在、各事業者は、電力制御システムセキュリティガイドラインに基づき、自社内の取組として制御系システムのセキュリティ対策を実施しているが、自らの取組を客観的に評価する機会を得ることも重要。
- このため、各事業者において、引き続き、ガイドラインに基づく対策や、当該対策について自ら評価を行うとともに、昨年設立された**電力ISACにおいて、外部有識者も交えてこれらを含む各事業者の取組を客観的にレビューする場を設け、そこで得られた有意義な知見及び各国ISAC、他分野ISACとの連携で得られた情報を共有**することで、業界としてのセキュリティ対策の向上を図っている。

＜事務系・制御系システムの模式図（電力分野の例）＞



電力分野の取組④　日米電力サイバーセキュリティワークショップの開催

- 電力分野のサイバーセキュリティにおける日米間の官民の協力関係の強化を図るべく、米国エネルギー省との共催で2018年3月に日米電力サイバーセキュリティワークショップを実施した。
- 双方の政府・電力会社・研究機関等が参加し、相互の課題や取組を共有したことで、互いの直面する課題に共通点があることが分かり、参加者間の相互の信頼関係の構築を行うことができた。

【日米電力サイバーセキュリティワークショップ】※非公開
日時： 2018年3月22日（木）10時～18時、
23日（金）10時～11時40分
場所：経済産業省本館17階　第1共用会議室～第3共用会議室
参加者：政府関係者、電力会社、電力事業団体、研究者等

Session 1:サイバーセキュリティ政策及び
標準・情報共有等、業界全体の課題について
Session 2:電力事業者が直面するサイバーセキュリティの課題
Session 3:サイバーセキュリティの教育・サイバー演習
Session 4:サイバーセキュリティにおける研究開発

互いの課題や取組を共有し、顔の見える信頼関係を構築

電力分野の取組⑤　新規参入事業者等への対応

- 電力広域的運営推進機関（以下「広域機関」）は、自らのシステムについてのセキュリティ向上の取組に加え、電力ISAC等から収集した情報を会員事業者（小売・小規模発電事業者）へ提供すると共に、事業者のセキュリティ水準向上のための啓発活動を実施している。
- また経済産業省は、ERAB事業者に対して、2017年4月に各事業者が取り組むべきサイバーセキュリティ対策の指針を示した「エネルギー・リソース・アグリゲーション・ビジネスに関するサイバーセキュリティガイドライン」を策定している。

広域機関の取組

〇業務規程にて、広域機関の所有するシステムについてのサイバーセキュリティ対策を講じることとし、昨年度までに外部監査、ペネトレテスト等を実施するなどのサイバーセキュリティ対策を実施。

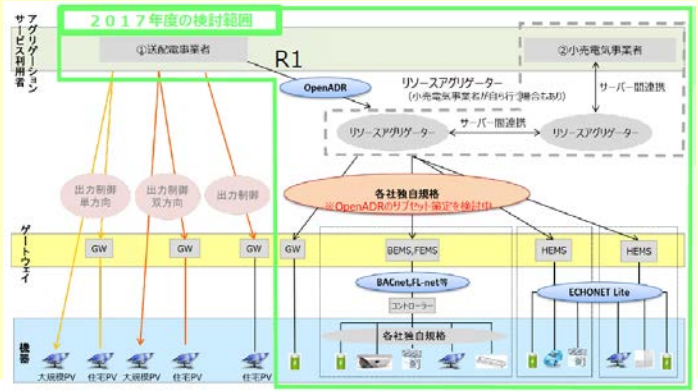
〇業務規程にて会員事業者への情報提供を広域機関のミッションとするとともに、送配電等業務指針にて会員事業者の情報セキュリティ向上を義務化。また、電力ISAC等から収集した情報を会員事業者に対して展開。

〇会員事業者の対策レベルの把握により、今後のセキュリティ対策へ活用する目的と、各社への啓発の趣旨で、年に１回調査を実施。（調査項目：全４９項目）

ERAB事業者向けの取組

〇ERAB検討会サイバーセキュリティＷＧの議論をまとめ、ERABに参画する各事業者が行うべきサイバーセキュリティ対策を整理し、ガイドラインを策定した。

〇各事業者は本ガイドライン等を踏まえ、自らの責任においてセキュリティ対策を講ずることとしている。



電力分野の取組⑥　サイバーセキュリティ対策を担う人材の育成

- 情報共有体制の強化など重要インフラ政策を実装させるには、重要インフラ事業者自身の能力強化が不可欠。本年4月、独立行政法人情報処理推進機構（IPA）に産業サイバーセキュリティセンター(ICSCoE)を設置。
- ICSCoEは、各業界における中核人材の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。今後、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名の研修生を受け入れ（電力・ガス分野からは合わせて20名程度参加）、実践的な演習・対策立案等のトレーニングを行う予定。

①模擬プラントを用いた対策立案（人材育成）

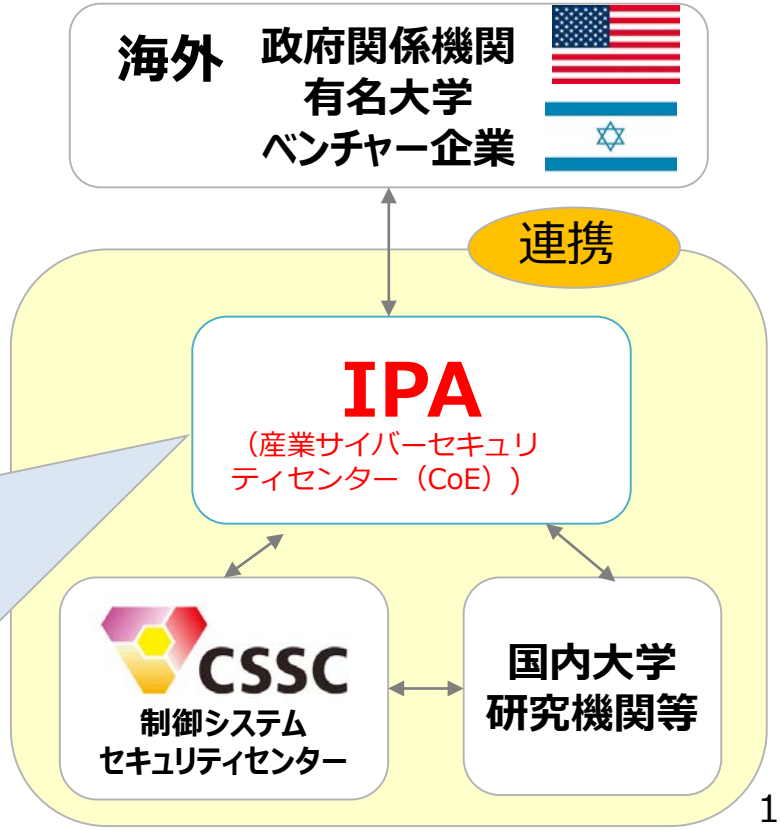
- 情報系システムから制御系システムまでを想定した模擬プラントを設置。専門家とともに安全性・信頼性の検証や早期復旧の演習を行う。
- 海外との連携も積極的に実施。

②実際の制御システムの安全性・信頼性検証等

- ユーザーからの依頼に基づき、実際の制御システムやIoT機器の安全性・信頼性を検証。
- 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

- 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。



検討の進め方（案）

- 電力分野のサイバーセキュリティを取り巻く現状、諸外国の状況を分析し、官民が取り組むべき課題と方向性について、短期・中長期という時間軸を加味しつつ、広く検討してはどうか。これらを踏まえつつ、官民が取り組むべき具体策として、例えば以下の項目についての検討を進めてはどうか。
- 電力制御系システムに関する更なる向上策のあり方を検討する。この際、「電力制御システムセキュリティガイドライン」への提言を具体出口の１つとして、例えばサプライチェーンのリスクマネジメントや緊急時対応の強化などといった、近年取り上げられつつある諸課題も含め、検討してはどうか。この際、2020年東京オリンピック・パラリンピックへの対応を視野に、短期的に対応すべき事項と、より中長期で見て対応すべき事項を整理して検討を進めてはどうか。
- また、電力自由化や情報化の進展、PV等の再生可能エネルギーの導入拡大に伴い、電力分野に多種多様なプレーヤーが参入してきており、基幹系の制御系システムそのもの以外にもサイバーセキュリティのリスクが広がってきている。こうした、電力制御系システムに関連した分野・事業者におけるセキュリティ向上のあり方を検討してはどうか。
- 更に、電力業界全体でのセキュリティ向上に資する基盤整備のあり方を検討してはどうか。具体的には、例えば、業界大での情報共有の更なる強化や、米国を始めとした諸外国との連携強化（情報共有等）や、人材育成基盤の強化のあり方などを検討してはどうか。

(参考)WG1における検討状況の紹介

1．産業政策と連動した政策展開

① **重要インフラの対策強化**
－情報共有体制強化　等

② **IoTの進展を踏まえたサプライチェーン毎の対策強化(Industry by industry)**
－防衛関係、自動車、電力、スマートホーム等の分野別検討と技術開発・実証の推進

③ **中小企業のサイバーセキュリティ対策強化**

2．国際ハーモナイゼーション

① **日米欧間での相互承認の仕組みの構築**

② **民間主体の産業活動をゆがめる独自ルールの広がり阻止**

3．サイバーセキュリティビジネスの創出支援

① **産業サイバーセキュリティシステムを海外に展開**

② **サービス認定創設、政府調達などの活用**

4．基盤の整備

① **経営者の意識喚起**

② **多様なサイバーセキュリティ人材の育成（ICSCoE等）**

③ **サイバーセキュリティへの過少投資解決策の検討**

(参考)WG1における検討状況の紹介

サイバー攻撃の脅威の増大についての認識

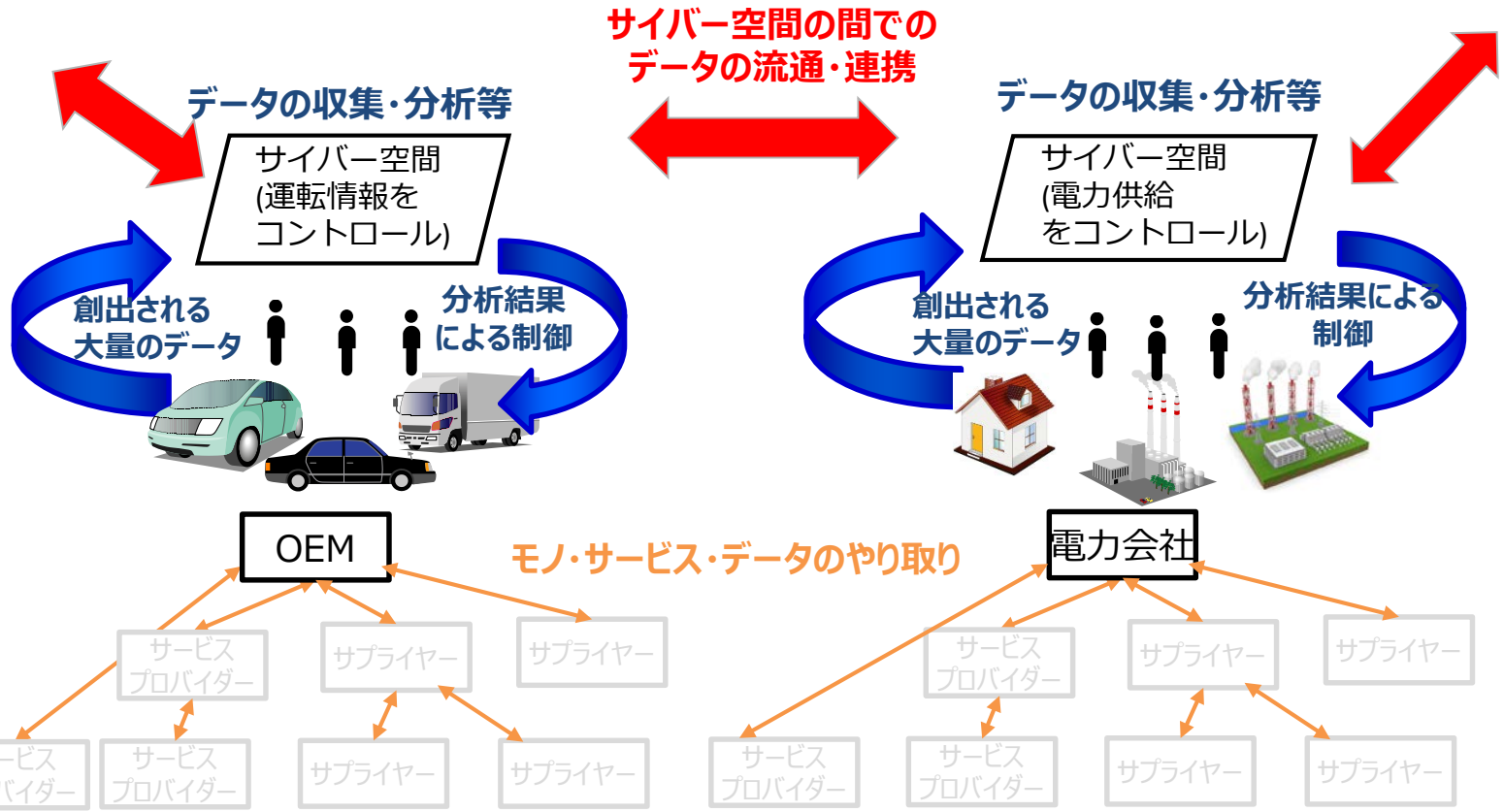
- IoTで全てのヒトとモノがつながるsociety5.0の社会では、**サイバー攻撃の起点が増大するとともに、複雑につながるサプライチェーンを通じてサイバーリスクの範囲が拡大**。
- サイバー空間とフィジカル空間が高度に融合するため、**サイバー攻撃がフィジカル空間まで到達**。
- IoTから得られる**大量のデータの流通・連携を支えるセキュリティも課題**。
- **海外においても、IoTやICS防衛のためにはサプライチェーンマネジメントでアプローチする必要が広く認識**されるようになっている。

Society5.0の社会におけるモノ・データ等の繋がりのイメージ

大量のデータの流通・連携 ⇒データプロテクションの重要性が増大

フィジカルとサイバーの融合 ⇒フィジカル空間までサイバー攻撃が到達

複雑につながるサプライチェーン ⇒影響範囲が拡大



(参考)WG1における検討状況の紹介

フレームワークの構造～Society5.0型サプライチェーン“価値創造過程”への対応

- あらゆるものがつながるIoT、データがインテリジェンスを生み出すAIなどによって実現される**Society5.0（人間中心の社会）、Connected Industriesでは、製品/サービスを生み出す工程（サプライチェーン） も従来とは異なる形態をとる**ことになる。
- 本フレームワークでは、**Society5.0型サプライチェーンを**これまでのサプライチェーンと区別するため、**価値創造過程（バリュークリエイションプロセス）と定義**し、そのセキュリティへの対応指針を示す。

- 本フレームワークは、価値創造のための活動が営まれる産業社会を、下記の**三層構造**と**6つの構成要素**で捉え、包括的にセキュリティポイントを整理し、それらに対応するための指針となるもの。

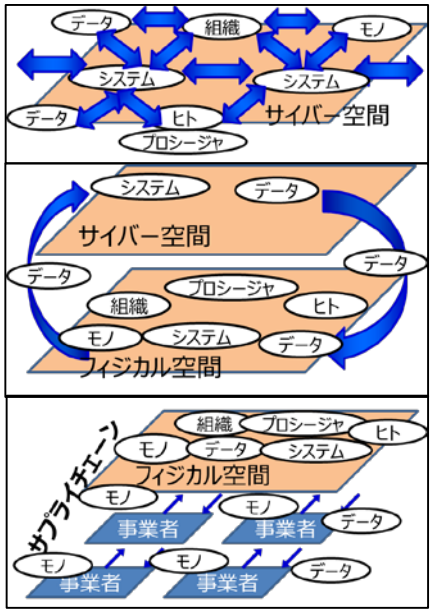
  ⇒ **詳細は次頁以降参照**

◆三層構造

－サイバー空間におけるつながり

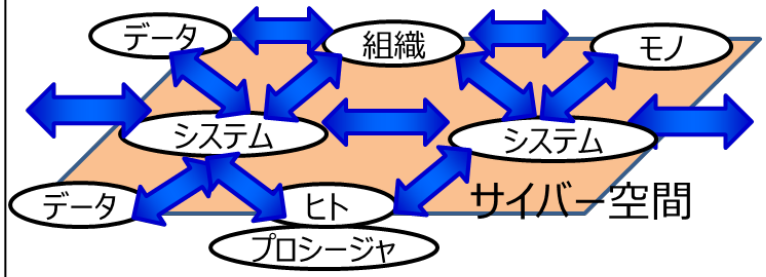
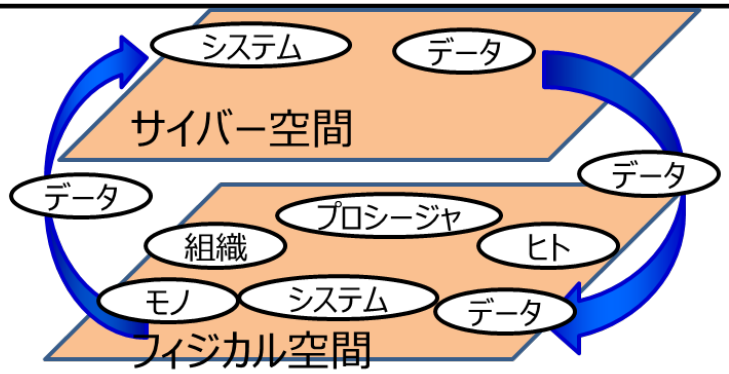
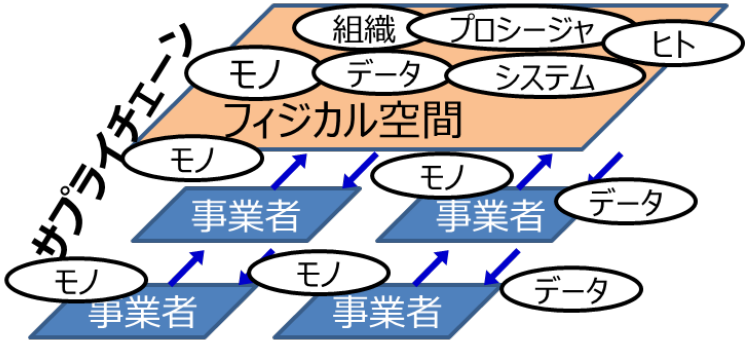
－フィジカル空間とサイバー空間のつながり

－企業間のつながり（従来型サプライチェーン）



◆６つの構成要素　－組織、ヒト、モノ、データ、プロシージャ、システム

(参考)WG1における検討状況の紹介
フレームワークの構造～Society5.0型サプライチェーン“価値創造過程”への対応
（１）価値創造過程が展開する産業社会の三層構造

	概念図	想定される脅威
サイバー空間におけるつながり【第３層】		データプラットフォームへの攻撃 － データ改ざん － 大規模な情報漏えい　等
フィジカル空間とサイバー空間のつながり【第２層】（フィジカル－サイバー層）		サイバー空間を通じたフィジカルへの攻撃 － センサの計測データ改ざん － IoT機器等で得られて加工されたデータの改ざん　等
企業間のつながり（従来型サプライチェーン）【第１層】		サプライチェーンを介した攻撃 － マルウェア混入 － 機器へのバックドア － 情報漏えい(設計図面等) － 不正機器混入・接続　等

(参考)WG1における検討状況の紹介
フレームワークの構造～Society5.0型サプライチェーン“価値創造過程”への対応
（２)価値創造過程に関わる６つの要素

構成要素	ポイント
組織	[対象]・サプライチェーンを構成する法人(製品やサービスを提供、または利用する) [要件]・ユニークな識別子（ID）で識別できること ・セキュリティポリシーに従い策定したセキュリティマネジメントシステムを運用していること
ヒト	[対象]・組織に属する人（組織から役割、権限を与えられ、何らかの責任を負う） [要件]・組織のセキュリティマネジメントシステムに従って行動すること ・ユニークな識別子（ID）で識別できること ・人の正当性、真正性が担保されていること
モノ	[対象]・機器、ソフトウェア、およびそれらを構成する部品 [要件]・ユニークな識別子（ID）で識別できること ・モノの正当性、真正性が担保されていること
データ	[対象]・フィジカル空間にて収集される(符号化された)情報、およびその情報をシェアし分析・シミュレーションすることで得られる付加価値を含む情報 [要件]・データの完全性が担保されていること
プロシージャ	[対象]・定義された目的を達成するための一連の手続き [要件]・プロシージャの信頼性、安全性、可用性が担保されていること
システム	[対象]・複数のヒト、モノ、データ、プロシージャで構成され、機能やサービスを実現する仕組み・インフラ [要件]・ユニークな識別子（ID）で識別できること ・システムの信頼性、安全性、可用性が担保されていること

(参考)WG1における検討状況の紹介

『サイバー・フィジカル・セキュリティ対策フレームワーク』のイメージ

WG1において検討を進め、年度内に大枠を整理することを目指す

3つの切り口	脅威が守るべきものへ与える影響(リスク分析) 守るべきもの	脅威	具体的な対応策 (構成要素ごとに整理)
企業と企業の繋がり	・仕様通りの製品、サービス ・情報の秘密保持 ・安全な取引	■マルウェアの混入 ■不正な機器の混入(調達段階)	**セキュアなサプライチェーン構築のために取引先に確認すべき項目** ■納入されるモノのセキュリティ確保 ■取引先のセキュリティ状況の確認 ■取引先とのやり取りのセキュリティ確保
フィジカル空間とサイバー空間の繋がり	・実現したい機能 ・レジリエンス ・セキュリティ ・セーフティー　等	■不正な機器の混入(設置段階) ■計測データの改ざん ■制御機能への攻撃	**セキュアなCPS構築に向けて必要な対策の項目** ■安全なIoTシステムの導入 ■CPS/IoTの構築と運用 ■組織文化の醸成　等
サイバー空間とサイバー空間の繋がり	・セキュアなデータ流通 ・サイバー上でのサービス利用	■データベースに格納されるデータの信ぴょう性 ■データプラットフォームへの攻撃 ■ネットワーク上での攻撃	**セキュアなデータ連携・活用に必要な対策の項目** ■データプラットフォームのセキュリティ ■データ品質の確認 ■データプラットフォームに参加する企業のセキュリティの確認　等

互いに関係

互いに関係

各分野のライフサイクルや求められる機能を踏まえたセキュリティ対策ガイドライン