経済産業省

資料６

電力分野におけるサイバーセキュリティについて

２０１９年8月２９日

資源エネルギー庁

サイバーセキュリティ対策について

- 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、電力の安定供給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。
- 本日は、サイバーセキュリティ対策の現状を御報告させていただくとともに、今後の検討の方向性について、御議論いただきたい。

海外のインシデント

ロンドンオリンピック会場へのサイバー攻撃（イギリス、'12）

開会式の開催中、会場の電力システムを狙った攻撃が40分間に渡って1000万回以上行われた。

製鉄所の溶鉱炉損傷（ドイツ、'14）

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。

核施設へのサイバー攻撃（イラン、'09）

マルウェアStuxnetが、制御系内システムにUSBを通じて感染

変電所へのサイバー攻撃（ウクライナ、'15）

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"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、2017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。

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）

複雑なサプライチェーンによる脅威の例：携帯端末に不正プログラムが仕掛けられた事例

フラッシュメモリに不正プログラムが仕掛けられた事例

- 2016年、**米国セキュリティ会社が携帯電話のフラッシュメモリのファームウェアに仕込まれている不正プログラムを発見**。
- 中国企業が開発・製造したもので、ユーザーの同意なしに、72時間おきに携帯電話内の情報が中国のサーバーに送信される。

日本の電気事業者によるサイバーセキュリティ対策の具体例

- 一般送配電事業者等の電気事業者は、電気事業法令に位置付けられているガイドラインも踏まえながら、サイバーセキュリティ対策を講じている。

	想定される具体的な脅威	電力各社における対策の具体例
システム・技術面	・インターネットから（事務処理系ネットワークを経由した）制御システム用ＮＷへの攻撃	・インターネットと制御システム用ＮＷとの**直接的な接続・通信の禁止** ・ログ管理による状態監視
	・事務処理系ネットワークから制御システム用ネットワークへのウイルスの侵入	
運用・管理面	・USBメモリ等**外部記憶媒体経由でのウイルス侵入**	・**不要なUSBポートの閉塞**、接続する**USBメモリの限定** ・接続前に**USBメモリのウイルスチェックを実施**
	・中央給電指令所、発電所中央制御所等の**建物へ侵入し、内部のシステムを不正操作**	・中給等への**入退出管理**（カード認証・生体認証等） ・**システムへのアクセス認証**（権限の限定化）
組織面	・セキュリティの知識を持った人材の不足 ⇒ **インシデント発生時の対応の遅れ**	・IPA産業サイバーセキュリティセンターで実施している**人材育成プログラム**やCSSCで実施している**演習への参加**
	・業界内での情報共有が充分になされないことによる対応の遅れなど	・電力ISAC設立（2017年3月）による、**電力各社間での情報共有体制の整備**。海外関連機関との連携。

（参考）電気事業法令におけるサイバーセキュリティ関連規定の整備

- 電気事業法第39条により、事業用電気工作物を設置する者に対して、省令で定める技術基準への適合維持を義務付け。
- また、省令で定める技術基準において、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電気工作物の運転を管理する電子計算機に係るサイバーセキュリティの確保を規定し、その解釈において、『電力制御システムセキュリティガイドライン』及び『スマートメータシステムセキュリティガイドライン』を位置付けている。

電力制御システム セキュリティガイドライン

スマートメーターシステム セキュリティガイドライン

（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

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

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

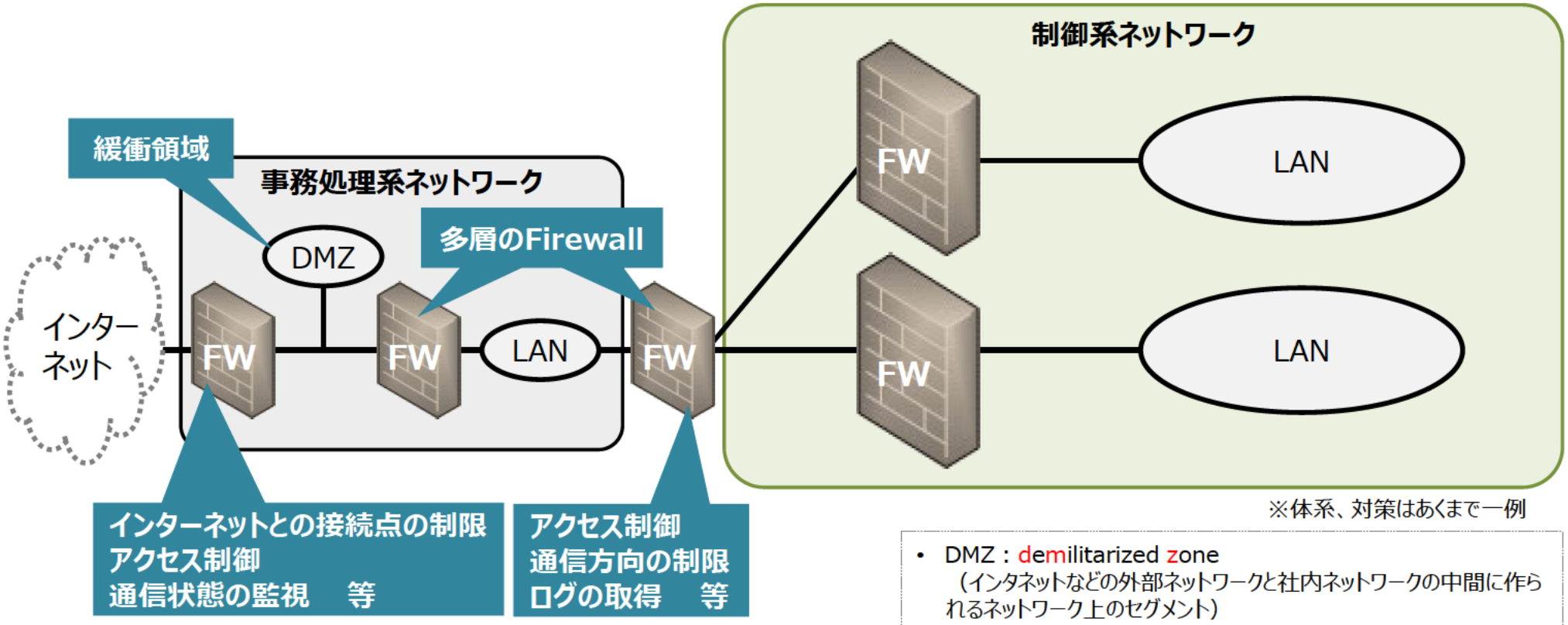
システム
・コマンド管理 ・外部記憶媒体利用制限

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

（参考）多層のFirewall等について

- 日本の電気事業者は、「電力制御システムセキュリティガイドライン」も踏まえながら、「システム・技術面」、「運用・管理面」、「組織面」でのサイバーセキュリティ対策を組み合わせて多層防御を実施。
- システム・技術面として、通信方向を限定したり、Firewall（FW）や緩衝領域（DMZ）を設ける等により多層的に防御対策を実施。こういった対策により事務系からのマルウェア感染を防御。

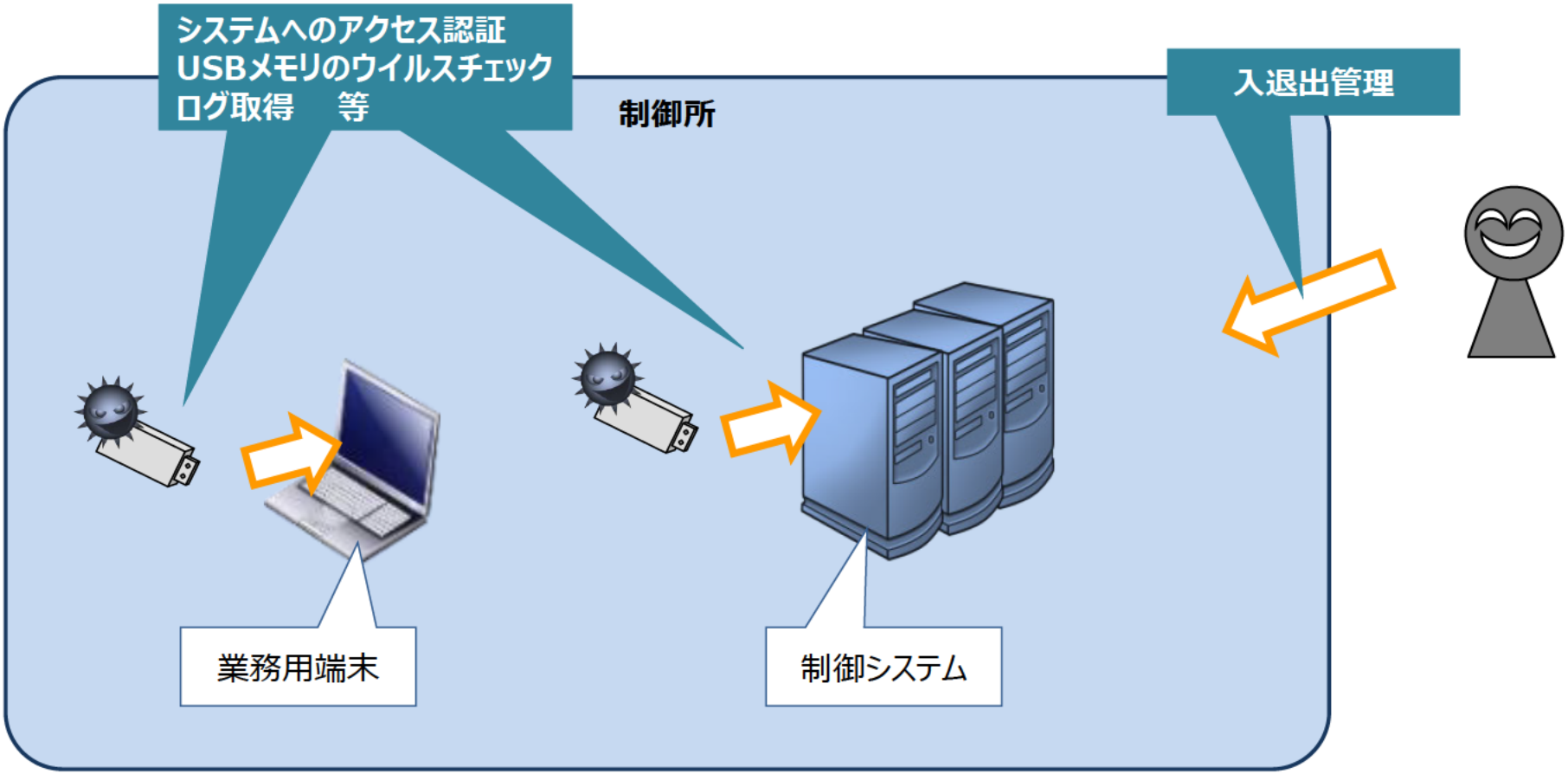


※体系、対策はあくまで一例

- DMZ：demilitarized zone
  （インタネットなどの外部ネットワークと社内ネットワークの中間に作られるネットワーク上のセグメント）
- FW：firewall
  （外部の攻撃から内部を保護するためのソフトウェアや機器、システムなど

（参考）入退出管理等について

- 運用・管理面として、ログの取得や、入退出管理等の対策を実施。こういった対策により制御所への物理的侵入やUSBからのマルウェア混入等について防御。



※対策はあくまで一例

電力ISACの取組の活動状況について

- 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。
- 電力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。

＜電力ISACの活動状況＞

【会員数の推移】

✓ 正会員（五十音順）設立当初：24社⇒27社（2019年4月1日現在）

株式会社扇島パワー、大阪ガス株式会社、沖縄電力株式会社、関西電力株式会社、九州電力株式会社、株式会社神戸製鋼所、株式会社コベルコパワー神戸、株式会社コベルコパワー神戸第二、株式会社コベルコパワー真岡、JFEエンジニアリング株式会社、JFEスチール株式会社、JFEホールディングス株式会社、株式会社JERA、四国電力株式会社、中国電力株式会社、中部電力株式会社、電源開発株式会社、東京ガス株式会社、株式会社東京ガスベイパワー、株式会社東京ガス横須賀パワー、東京電力パワーグリッド株式会社、東京電力ホールディングス株式会社、東北電力株式会社、日本原子力発電株式会社、日本原燃株式会社、北陸電力株式会社、北海道電力株式会社

✓ 特別会員（五十音順）

電力広域的運営推進機関、一般社団法人日本卸電力取引所

【具体的な活動事例】

✓ 国内外の関係機関からの情報収集及び分析

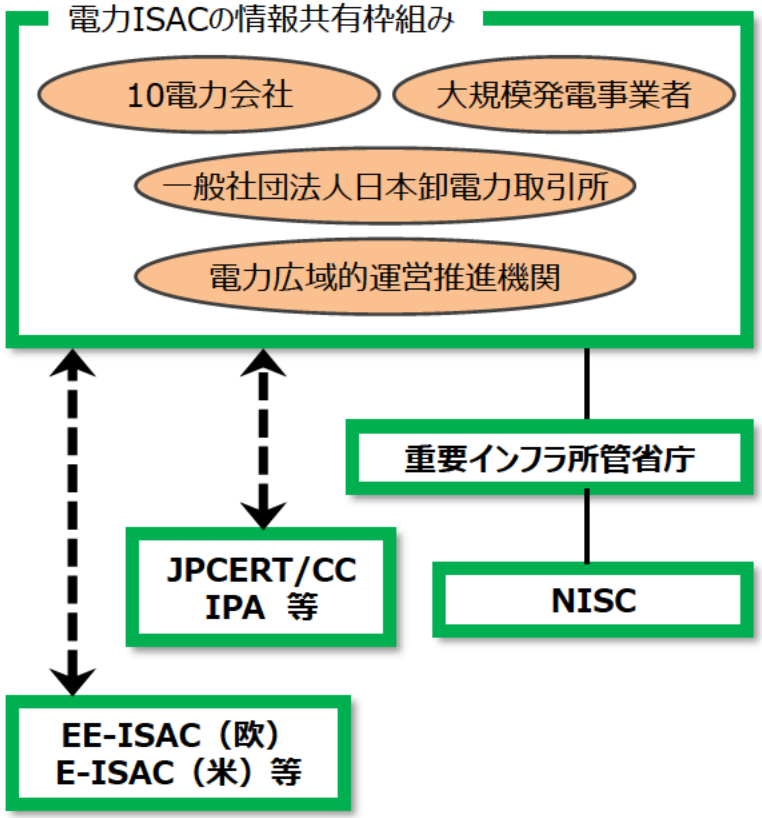
✓ グッドプラクティス等を共有する分野毎のWGを実施し、会員同士で情報共有

（例）・各会員のセキュリティに係る取組や課題を共有し、議論

・会員から提供された脆弱性情報（**未公表であるものも含む**）を会員同士で共有

✓ 電力分野でのインシデントの事例に関連する情報（他分野を含む）を収集し、対策例等をまとめた解説付きのレポートを作成

＜情報共有体制＞



（参考）諸外国との連携

- 2017年5月には電力ISAC（※1）とEE-ISAC（欧）の間でMOU（※２）が、2018年10月には日米欧三者によるMOU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）

- メンバー交流による信頼関係構築を始め、互いの組織の活動や機微情報の取り扱いに十分留意した上でサイバーセキュリティに関する各種情報交換等を含む内容となっている。

【調印式後握手を交わす日米欧の代表者】
左から
JE-ISAC（阿部克之氏）
NERC（Jim Robb氏）
EE-ISAC（Johan Rambi氏）

（出所：電力ISACホームページ）

日米電力サイバーセキュリティワークショップについて

- 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。双方の政府・電力会社・研究機関等が参加し、相互の課題や取組の共有を行い、参加者間の相互の信頼関係・協力関係の構築につながった。

【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

電力分野のサプライチェーンセキュリティ対策に関する国際的議論

- 電力分野におけるサプライチェーンセキュリティ対策について、米・英・イスラエルを中心とする新たな認証枠組みを視野に入れた**国際的な議論の場**（CPIC：Cyber Product International Certification）が立ち上がっている。
- 海外の政府機関、主要電力会社及びベンダーが準備会合に出席している中、経済産業省としても、日本の電力会社やベンダーと共に６月末@ワシントンDCの会合に出席。

CPICの方針

- グリッド運用に特に重要なハードウェア及びソフトウェア製品における、業界主導による認証基準を確立する。
- サプライチェーンリスク管理の強化のため、どの製品を対象とするか、厳格な優先順位付けを行う。
- サプライチェーンリスク管理に関する取組を一元化するため、電力事業者及びベンダー等個々の事業者の協力体制を構築する。
- 米国、英国、イスラエル、その他の国々から協力者を集め、国際的なアプローチを行う。

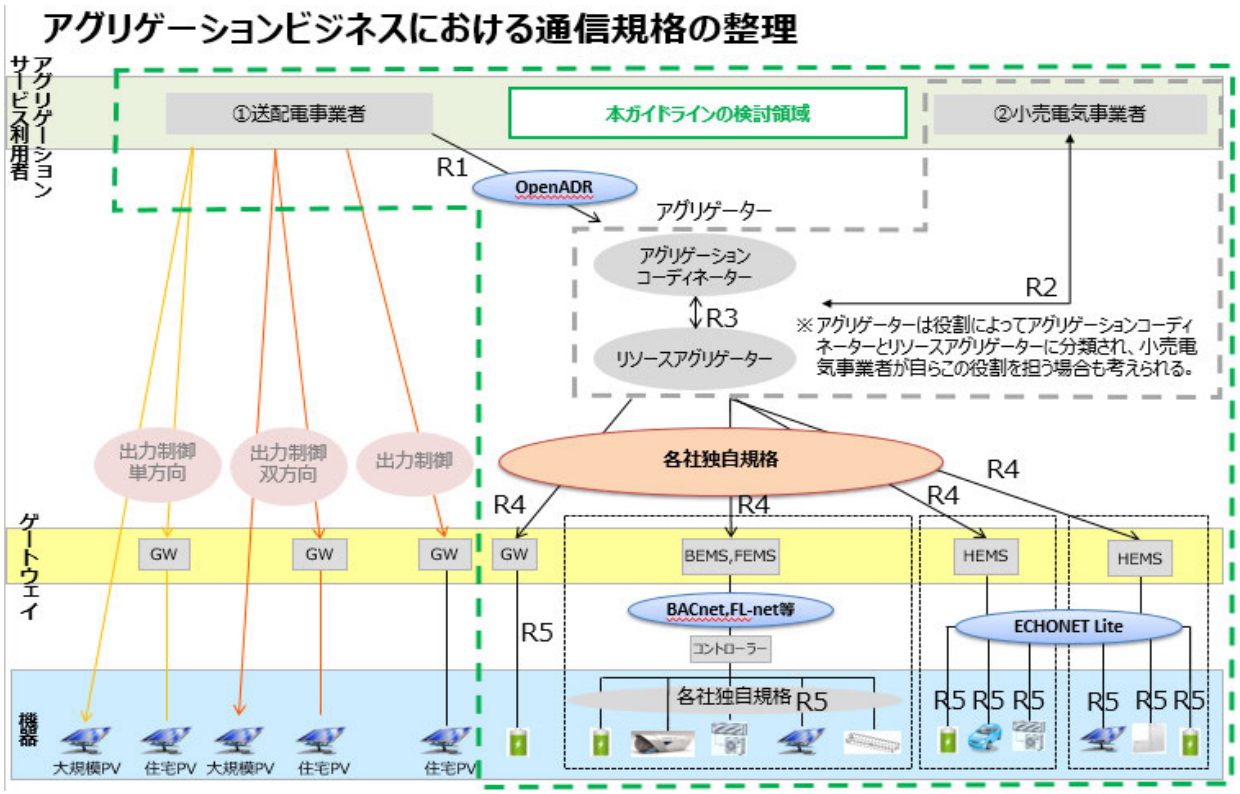
準備会合への海外の出席者

1．政府機関等　米国：DoE、DoD、DHS 、FERC 、NERC
　　イスラエル：INCD
2．電力会社等　米国：E-ISAC、EEI、PJM 、サザンカンパニー
　　イスラエル：IEC
　　欧州：National Grid、ENEL
3．ベンダー　　米国：GE
　　欧州：ABB、シュナイダー

Inaugural CPIC meeting in London, June 2018

エネルギー・リソース・アグリゲーション・ビジネス（ERAB）における取組

- 分散型エネルギーリソースを統合制御することで、需要抑制量（ネガワット）のアグリゲーション、逆潮流分（ポジワット）のアグリゲーションの実用化に向けた実証事業が進められている。
- 当該事業者（アグリゲーター）が取り組むべきサイバーセキュリティ対策を整理するため、2016年度、ERAB検討会サイバーセキュリティWGにおいて、「ERABに関するサイバーセキュリティガイドライン ver.1.0」を制定。その後、2017年度に改定を実施。
- 2019年度、一般送配電事業者のシステムとアグリゲーターのシステムが接続すること想定した際に必要となると考えられるサイバーセキュリティ対策を検討しているところ。2019年度内の当該ガイドラインの改定を予定。



※図は、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Ver 1.2（原案）2019年3月19日ERAB検討会時点のもの

再生可能エネルギー大量導入・次世代電力ネットワーク小委員会における議論

- 2019年8月、再生可能エネルギー大量導入・次世代電力ネットワーク小委員会の中間整理が行われ、再生可能エネルギーのオンライン制御に当たり、オンライン制御の促進とともに、オンライン化を進めるに当たっては、引き続きサイバーセキュリティ対策にも取り組んでいくことが重要であるとされた。

総合資源エネルギー調査会　省エネルギー・新エネルギー分科会／電力・ガス事業分科会　再生可能エネルギー大量導入・次世代電力ネットワーク小委員会　中間整理（第３次）

Ⅳ．再生可能エネルギーの大量導入を支える次世代電力ネットワーク

２．再生可能エネルギー導入拡大に向けた適切な出力制御の在り方

②オンライン制御の拡大

オンライン制御の拡大は、上述のメリットが大きい一方で、現状では、発電事業者が自主的にオンライン化に対応するためのインセンティブが弱いことから、一般送配電事業者は必要な再エネ運用システムの整備を進めつつ、国や発電事業者の業界団体とともに、まずは特別高圧のオフライン事業者のオンライン化から順次促していくべきである。加えて、出力制御量の低減とオンライン化のメリットが両立するような出力制御の運用の見直しを含めた環境整備を進めていくべきである。なお、<u>オンライン化を進めるに当たっては、引き続きサイバーセキュリティ対策にしっかりと取り組むことが重要</u>である。

産業サイバーセキュリティ研究会ワーキンググループ１における検討体制

- 産業サイバーセキュリティ研究会のワーキンググループ１（制度・技術・標準化）の下、電力SWG（サブワーキンググループ）にて検討・議論を行っている。

産業サイバーセキュリティ研究会

ＷＧ１　制度・技術・標準化

［2018年2月～（５回開催）］
2019年４月　フレームワークの策定・公表

標準モデル

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

- **ビル**（エレベーター、エネルギー管理等）
  ［2018年２月～（９回開催）］
  2019年6月　ガイドライン第1版を公開
- **電力**
  ［2018年6月～（５回開催）］
- **防衛産業**
  ［2018年３月～（３回開催※）］
  （防衛装備庁 情報セキュリティ官民検討会）
  ※防衛産業SWGとして開催した回数のみ
- **自動車産業**
  ［2019年4月～（２回開催）］
- **スマートホーム**
  ［2018年３月～（９回開催）］
  2019年度までにガイドライン取りまとめを目指す（予定）
  (JEITA スマートホーム部会 スマートホームサイバーセキュリティWG)
- **その他コネイン関係分野**

電力SWG（サブワーキンググループ）における議論

- 電力SWGでは、サプライチェーンリスクへの対応、大手電気事業者への対応、新規プレーヤーへの対応にわけて、それぞれの対策について検討が進められている。
- 電力システムのデジタル化、オンライン化の進展に伴い、更に包括的な対策を進めていくことが重要。

＜構成員＞座長：渡辺　研司　名古屋工業大学大学院教授

有識者（大学教授、弁護士等）、電気事業者、業界団体

＜方向性＞

- 電力制御系システムに関するセキュリティ向上策
  → **「電力制御システムセキュリティガイドライン」への提言**（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）
  →2020年**東京オリパラへの対応を視野に、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

- 電力自由化等に伴う多種多様なプレイヤー参入による、制御系システム周辺に拡がりつつあるサイバーセキュリティリスクへの対応策
  →**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

- 業界全体の取組向上に資する基盤整備
  → **情報共有の更なる強化、諸外国との連携強化、人材育成基盤の強化**　等

＜中長期的に検討していく課題＞

- **サプライチェーンリスクへの対応**について
  ・海外の事業者や国内他分野の動向を踏まえると、日本の電力分野においてはどのようなリスクが存在するか。
  ・日本の電力分野の関係者が継続的に取り組むべき事項は何か。
- **大手電気事業者**のサイバーセキュリティ対策について
  ・大手電気事業者のサイバーセキュリティ対策の取組の現状分析と、今後取り組むべき事項は何か。
- **新規プレーヤー**のサイバーセキュリティ対策について
  ・新規プレーヤー等のサイバーセキュリティ対策の取組の現状分析と、今後取り組むべき事項は何か。