経済産業省

資料７

電力分野におけるサイバーセキュリティについて

２０２４年4月１７日

資源エネルギー庁

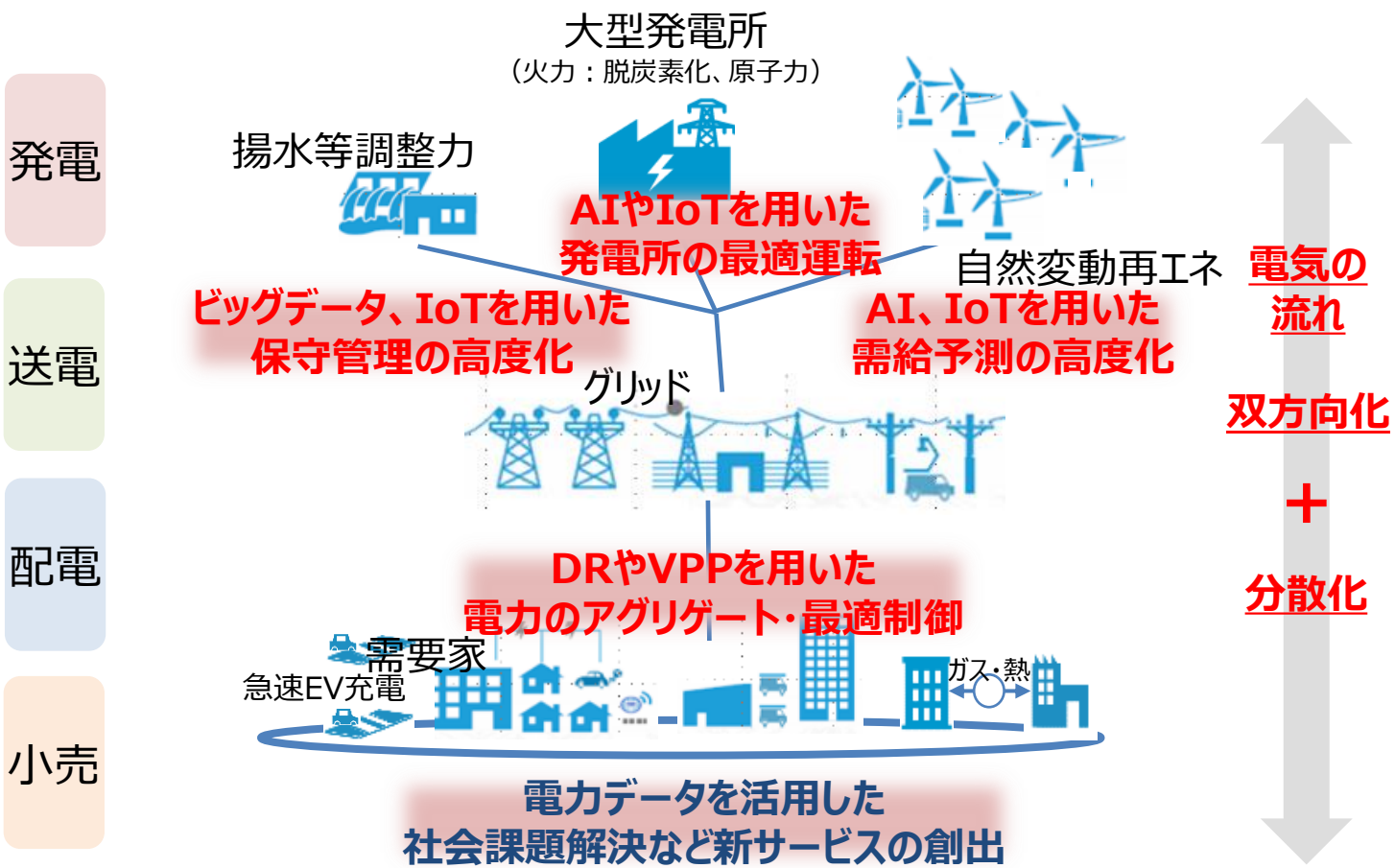
本日御議論いただきたいこと

- 電力分野において、サイバーセキュリティの重要性は高まる一方である。**再エネの導入拡大やデジタル化の進展、広域運用の拡大**は、不可逆的な流れであり、いずれも**サイバーセキュリティリスクを高める方向に働く**。
- こうした状況を踏まえ、**電力システムに対するサイバー脅威に対して、諸外国はセキュリティ対策向上に向けた取組を強化**。特に、EUは、NIS2指令、Network Code、サイバーレジリエンス法案等、強制力の高い取組を推進している。
- 国内においても、電気事業法に基づいて技術基準やガイドラインが整備されており、**電力分野に求められるセキュリティ対策事項は整理されつつある**。他方、サイバー脅威が日々進化・巧妙化している状況を踏まえると、**現状の対策で十分ということは決してなく、電力システムにおけるサイバーセキュリティ対策の継続的な改善・高度化は必要不可欠**である。
- このため、電力各社におけるサイバーセキュリティの向上に向けて、**業界大での取組を進めるためのプラットフォームとして、産業サイバーセキュリティ研究会の下に設置した電力SWGにおいて、以下の点について御議論いただいたところ、その内容について報告する**とともに、今後の取組の方向性について御議論いただきたい。
  - **電力制御システムにおけるサプライチェーン・リスクに対する対応について**
  - **アグリゲーター及び分散型エネルギー源（DER）のセキュリティ対策について**
  - **電力システムにおけるサイバーセキュリティリスク点検ツールについて**

電力産業におけるデジタル化と分散化の進展

第69回 電力・ガス基本政策小委員会
(2024年1月22日) 資料3より一部抜粋

- AI・IoT等のデジタル技術の活用が著しい中、電力分野においてもその活用が進みつつある。
- デジタル技術は、**発電・送電・配電・小売等のそれぞれの産業の効率化**に資するだけでなく、**分散化電源の活用の推進**にも活用される。さらに、**スマートメーターから得られる電力データを、防災対策や社会課題の解決に使う動き**も生まれつつある。
- こうした中で、**サイバーセキュリティ対策の強化の必要性**も高まっている。



（参考）電力ＳＷＧの位置づけ

- 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、**電力分野のサイバーセキュリティ対策**について、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

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）
- **電力**
- **防衛産業**
- **自動車産業**
- **スマートホーム**
-

［2018年6月～（１６回開催）］

＜委員名簿（敬称略・五十音順・2024年2月時点）＞

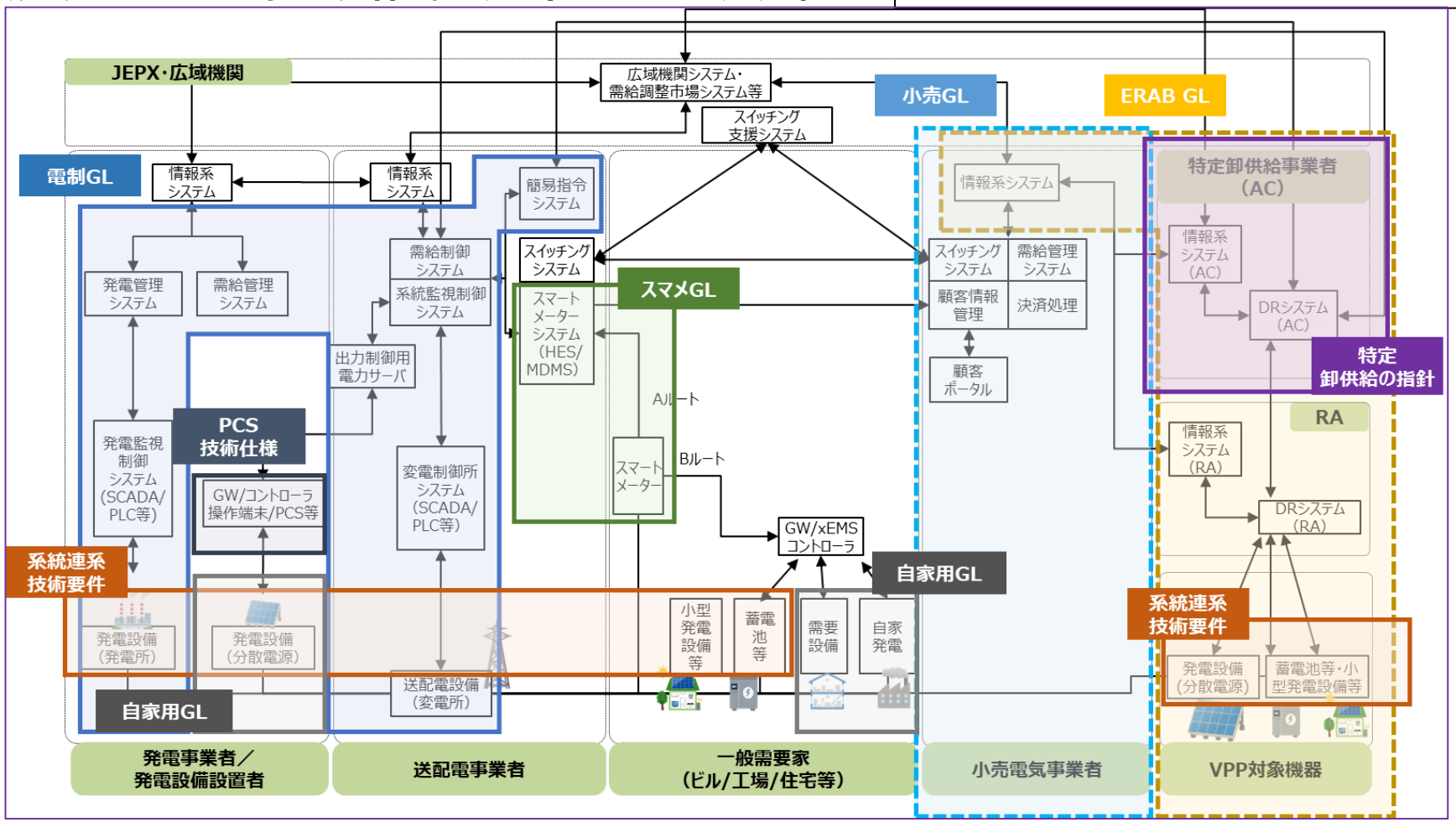
稲垣　隆一	稲垣隆一法律事務所　弁護士
内田　忠	電力ISAC　代表理事
江崎　浩	東京大学大学院　情報工学研究科教授
大崎　人士	産業技術総合研究所　サイバーフィジカルセキュリティ研究センター　インフラ防護セキュリティ研究チーム長
大浪　哲	電気事業連合会　情報通信部長
奥村　智之	日本電気協会　技術部長
小野崎　勝徳	東京電力ホールディングス㈱　セキュリティ統括室長
門林　雄基	奈良先端科学技術大学院大学　先端科学技術研究科教授
佐々木　勇人	JPCERT/CC　政策担当部長　兼　早期警戒グループマネージャ
新　誠一	電気通信大学　名誉教授
高倉　弘喜	国立情報学研究所　ストラテジックサイバーレジリンス研究開発センター長
高見　穣	情報処理推進機構　セキュリティセンター　セキュリティ対策推進部　エキスパート
手塚　悟	慶應義塾大学　環境情報学部教授
新田　哲	JFEスチール㈱　専務執行役員
渡辺　研司	名古屋工業大学大学院　社会工学専攻教授

電力分野におけるサイバーセキュリティの確保の取組

- **電力システムの各プレイヤーは、ガイドライン等に基づいた一定の対策が求められている。**
- ガイドライン等については、定期的に見直し、改正を実施している。

＜電力システムのサイバーセキュリティ関するガイドライン等の適用範囲＞

令和４年度 エネルギー需給構造高度化対策に関する調査等事業 （電力分野のサイバーセキュリティ対策のあり方に関する詳細調査分析）報告書(2023年2月28日) より一部抜粋



※実線は義務、点線は推奨として位置づけられているガイドライン等を意味する。なお、本図は各ガイドライン等の対象を明確化するために作成したものであり、実際の電力システムを精緻に整理したものではない。

【参考】電力制御システムに対する取組（ガイドライン等）

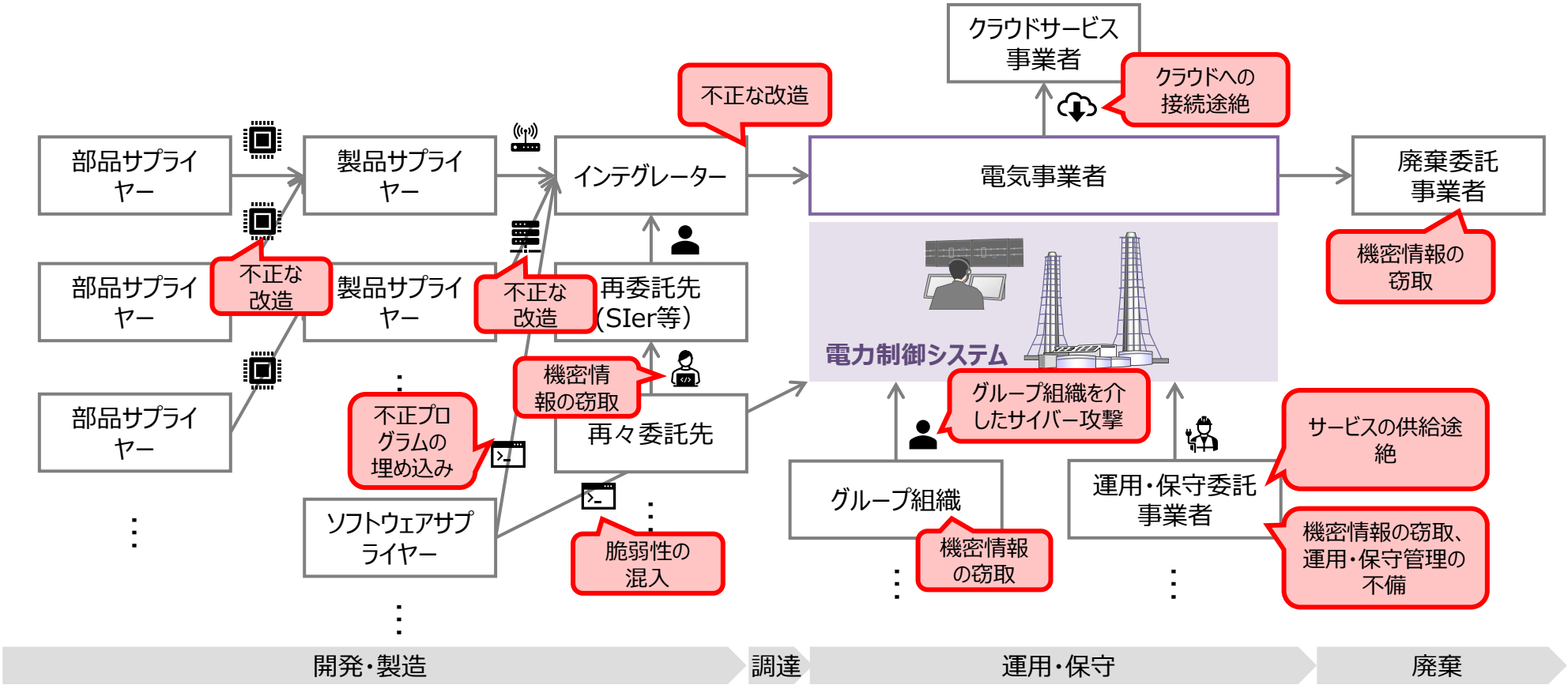
	名称	主な対象	発行主体	概要
電制GL	**電力制御システムセキュリティガイドライン**	電気事業の用に供する電気工作物	日本電気協会	電気事業法、電気設備に関する技術基準を定める省令及びその解釈に基づき、電気事業の用に供する電気工作物に対しては、本ガイドラインに基づく対策が求められる。
スマメGL	**スマートメーターシステムセキュリティガイドライン**	スマートメーターシステム	日本電気協会	電気事業法、電気設備に関する技術基準を定める省令及びその解釈に基づき、スマートメーターシステムに対しては、本ガイドラインに基づく対策が求められる。
系統連系技術要件	**系統連系技術要件**	系統連系する発電設備	各一般送配電事業者	系統連系する発電設備にすべからく求められる対策。具体的には、ネットワーク接続点の保護、マルウェア対策、系統運用者に対するセキュリティ管理責任者の通知の3点が求められる。
PCS技術仕様	**出力制御機能付PCSの技術仕様**	出力制御機能付PCS	JPEA・JEMA・電事連	出力制御機能付PCSにおいて満たすべきサイバーセキュリティ対策の要件を示した技術仕様。
自家用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（内規）**	自家用電気工作物（発電設備と需要設備の両方を含む）	経済産業省	自家用電気工作物（発電設備と需要設備の両方を含む）に求められるサイバーセキュリティ対策事項を記載したガイドライン。
小売GL	**小売電気事業者のためのサイバーセキュリティ対策ガイドライン**	小売電気事業者	資源エネルギー庁	小売電気事業者が主体的に取り組むことが求められるサイバーセキュリティ対策に関して記載したガイドライン。
ERAB GL	**ERABに関するサイバーセキュリティガイドライン Ver2.0**	ERABに関する事業者	経済産業省・IPA	ERAB のサービスレベルを維持するために ERAB に参画する各事業者が実施すべき最低限のセキュリティ対策の要求事項を示したガイドライン。
特定卸供給の指針	**特定卸供給に係るサイバーセキュリティ確保の指針**	特定卸供給事業に関するシステム	資源エネルギー庁	特定卸供給事業を実施する上で確保すべきサイバーセキュリティとその対策の内容を示すことを目的とした指針で、特定卸供給事業の届出の際に、本指針に基づく対策実施状況を記載する必要がある。

第16回電力SWGにて議論した「サプライチェーン・リスク」

第16回 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 （制度・技術・標準化）電力ＳＷＧ
（2024年2月1日）資料5-1から一部抜粋

- NISCの文書を参照し、電気事業者へ電力制御システムが納入されるまでの**開発や製造に係る一連の工程に加え**、**調達・運用・保守・廃棄を含むライフサイクル全般のサプライチェーンにおけるサイバーセキュリティ上のリスクを「サプライチェーン・リスク」と呼ぶ。**
（自然災害に起因するサプライチェーンの途絶等は、スコープ外とする。）

電力制御システムに想定されるサプライチェーン・リスクの例

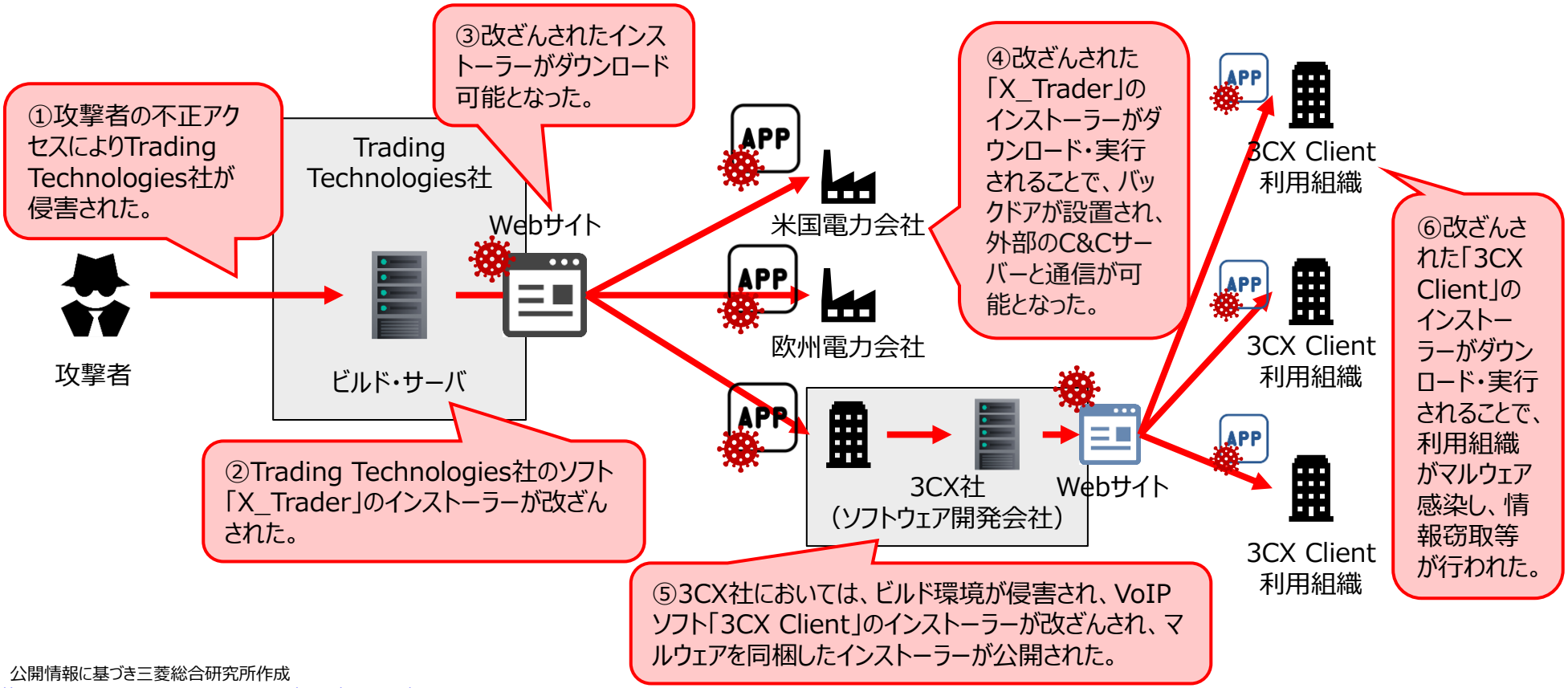


※「リスク」とは、脅威と脆弱性の合致により損失が発生する可能性、また、その損失をいう。
出所）NISC、外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書等に基づき作成 https://www.nisc.go.jp/pdf/policy/general/risktaiou28.pdf

【サプライチェーンを通じたサイバー攻撃の事例（電力分野）】
先物取引ソフトを通じたサイバー攻撃

- 2023年3月、Trading Technologies社が提供する**先物取引ソフト「X_Trader」の正規インストーラーが改ざん**され、当該ソフトを利用する**電力会社やソフトウェア開発会社にサイバー攻撃が実施**された。
- 3CX社においては、同社が販売する**VoIPソフト「3CX Client」のビルド環境が攻撃の影響**を受け、**同製品のインストーラーにマルウェアが同梱**された。この結果、**3CX Clientの利用組織にも影響が波及**し、**当該利用組織におけるマルウェア感染や情報漏えい等が発生**した。

先物取引ソフトウェア（X_Trader）に関連する一連のサプライチェーンセキュリティ攻撃のイメージ

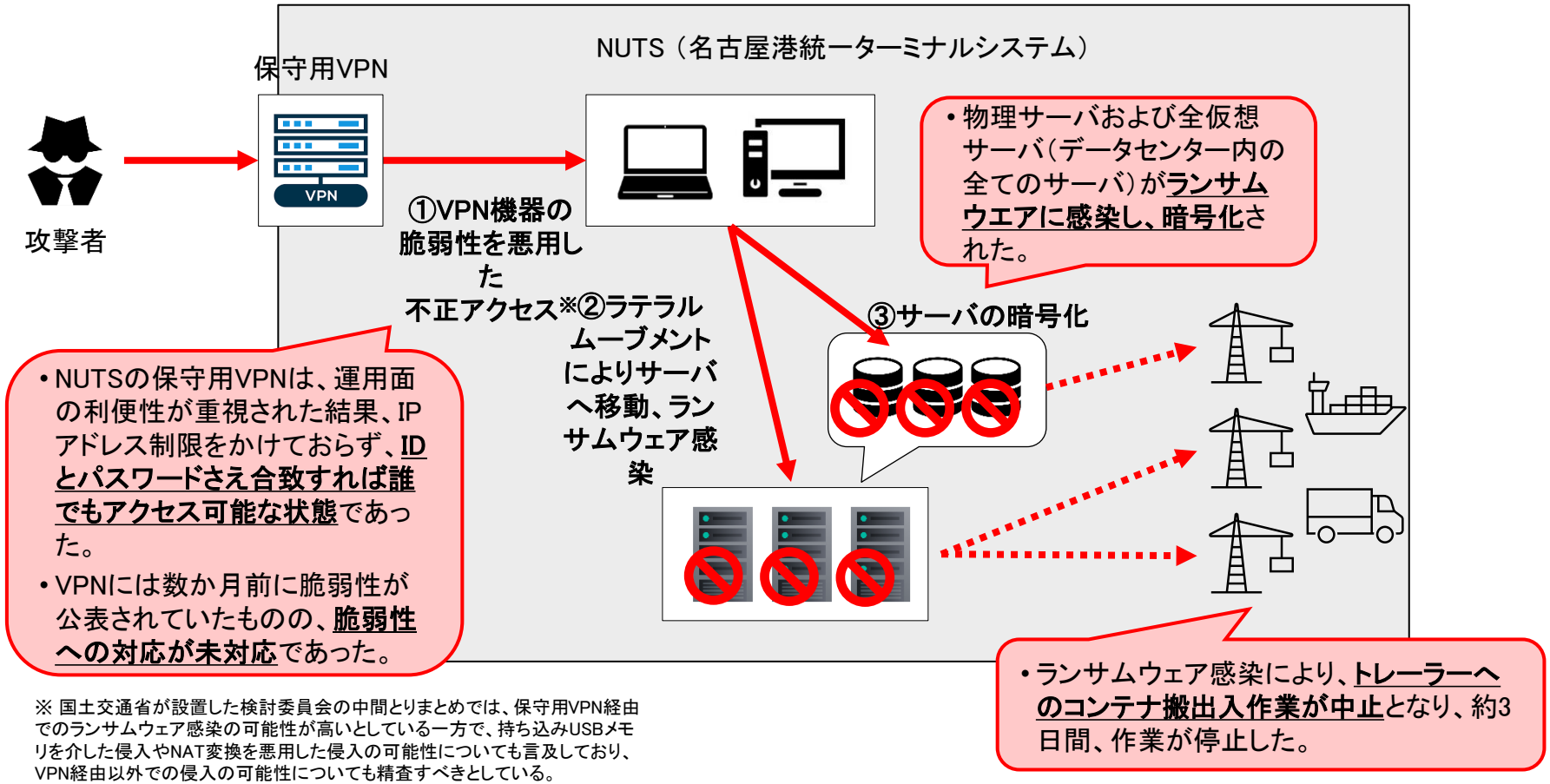


出所）公開情報に基づき三菱総合研究所作成
https://symantec-enterprise-blogs.security.com/blogs/japanese/xtradernosafuraichiengongjimiguoyayorotsuhanozhongyaoinfurazuzhiniyingxiang
https://thehackernews.com/2023/04/lazarus-xtrader-hack-impacts-critical.html

【サプライチェーンを通じたサイバー攻撃の具体的事例（港湾分野）】名古屋港コンテナターミナルに対するランサムウェア攻撃

- 2023年7月4日、**名古屋港コンテナターミナルのシステムがランサムウェア攻撃を受け、物理サーバ及びデータセンター内の全仮想サーバが暗号化**されたことで、**およそ3日間にわたりターミナルの操業が停止**した。
- 攻撃経路について、**VPN機器の脆弱性を悪用され、不正アクセスされた可能性が高い**としている。

名古屋港コンテナターミナルに対するランサムウェア攻撃のイメージ



※ 国土交通省が設置した検討委員会の中間とりまとめでは、保守用VPN経由でのランサムウェア感染の可能性が高いとしている一方で、持ち込みUSBメモリを介した侵入やNAT変換を悪用した侵入の可能性についても言及しており、VPN経由以外での侵入の可能性についても精査すべきとしている。

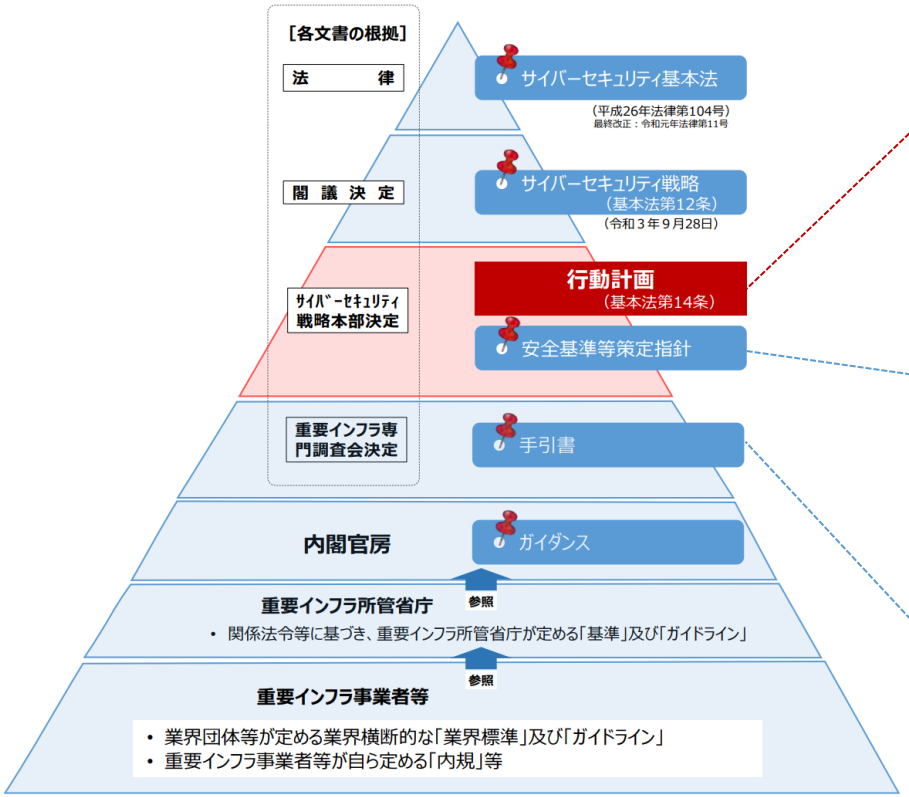
出所）公開情報に基づき三菱総合研究所作成
https://meikoukyo.com/archives/3336, https://www.mlit.go.jp/kowan/kowan_mn2_000006.html

国内電力分野に関連する取組状況

(1) NISC：重要インフラ防護に関する安全基準等の改訂

- NISCは、令和4年に策定した「重要インフラのサイバーセキュリティに係る行動計画」において、サプライチェーン・リスク対応に関して、安全基準等策定指針の記載を充実させる方針を示した。
- この方針を踏まえ、令和5年に策定した「重要インフラのサイバーセキュリティに係る安全基準等策定指針」では、**サプライチェーン・リスクに関するリスクアセスメント・対応等が、重要インフラ分野に共通して求められるサイバーセキュリティ確保に向けた取組として明記**された。

重要インフラ防護に関する安全基準等に係る体系、各文書におけるサプライチェーン・リスク関連の記載状況



重要インフラのサイバーセキュリティに係る行動計画（令和4年6月）

- 官民が一体となって重要インフラのサイバーセキュリティの確保に向けた取組を推進するための行動計画
- サプライチェーン・リスクへの対応について安全基準等策定指針の記載を充実させる方針を示す

重要インフラのサイバーセキュリティに係る安全基準等策定指針（令和5年7月）

- 自組織の重要システムや機能とサプライチェーンの依存関係の把握、供給者のセキュリティ対策の状況把握、**サプライチェーン・リスクに関するリスクアセスメント及びリスク対応等について、重要インフラ分野共通して求められるサイバーセキュリティ確保に向けた取組として新たに記載**

重要インフラのサイバーセキュリティ部門におけるリスクマネジメント等手引書（令和5年7月）

- サプライチェーン・リスク対応として、製品・サービスの調達・利用に当たり、サイバーセキュリティに関する要求事項を整理すること、不正機能等の埋め込みに係る脅威に対応すること等の取組を整理・記載

出所）NISC、内閣サイバーセキュリティセンター重要インフラグループ関係規程集 https://www.nisc.go.jp/pdf/policy/infra/kitei.pdf

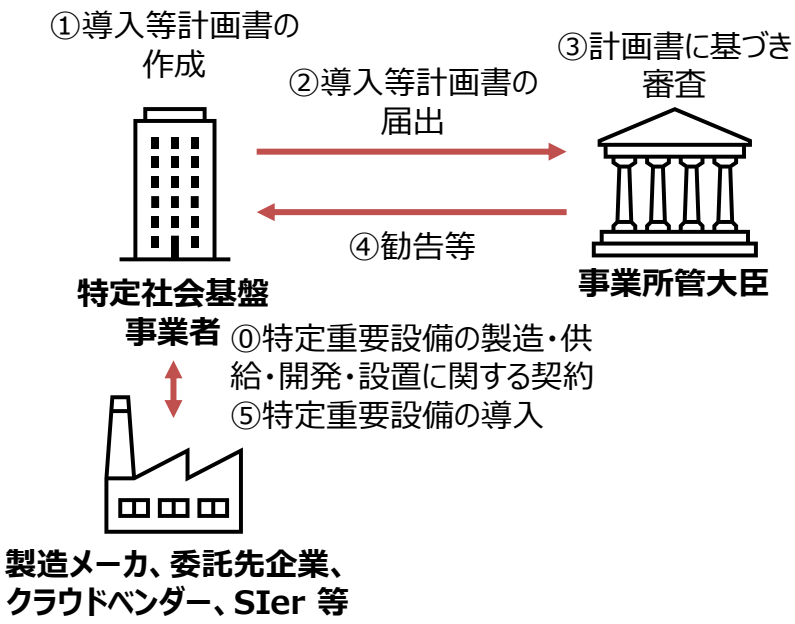
国内電力分野に関連する取組状況

第16回 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
（制度・技術・標準化）電力ＳＷＧ(2024年2月1日) 資料5-1より作成

(2) 特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する制度

- 2022年5月に成立した経済安全保障推進法では、**特定社会基盤事業者が特定重要設備（国が指定した重要設備）の導入及び重要維持管理等の委託を行う場合、事業所管大臣の審査を受けなければならない**としており、2024年5月17日より運用が開始される。
- 審査において、特定重要設備が特定妨害行為（我が国の外部から行われるサイバー攻撃、物理的な妨害行為等）の手段として使用されるおそれが大きいと認められたとき、**事業所管大臣は、特定妨害行為を防止するため必要な措置をとるべきこと等を勧告及び命令**することができる。
- 2023年11月16日、**電力分野では特定の基準を満たす42者が特定社会基盤事業者として指定**され、特定重要設備の導入及び重要維持管理等の委託を行う場合、**経済産業大臣による事前審査が必要**となる。

「特定重要設備」の導入に係るプロセス



計画書作成	•「特定重要設備の概要」「導入の内容」「導入の時期」「特定重要設備の供給者に関する事項」「特定妨害行為の手段として使用されるおそれがあるものに関する事項」などを記載する。
届出	•事業所管大臣が当該届出を受理した日から起算して30日を経過する日までは、特定社会基盤事業者は、当該導入等計画書に係る特定重要設備の導入を行わせてはならない。
審査	•事業所管大臣が、導入等計画書等に係る特定重要設備が特定妨害行為の手段として使用されるおそれが大きいかどうかを審査する。【通常のプロセスはここまで】
勧告等	•事業所管大臣は、審査した結果、当該計画書に係る特定重要設備が特定妨害行為の手段として使用されるおそれが大きいと認めるときは、特定社会基盤事業者に対し、特定妨害行為を防止するため必要な措置をとるべきこと等を勧告及び命令する。
導入後の勧告等	•例外的※に、特定重要設備の導入を行うことができることとなった後等であっても、当該特定重要設備について、事業所管大臣は特定妨害行為を防止するために必要な措置をとるべきことを勧告及び命令することができる。

※国際情勢の変化その他の事情の変更により、当該特定重要設備が特定妨害行為の手段として使用され、又は使用されるおそれが大きいと認めるに至ったとき。

出所）経済産業省、特定社会基盤事業者として指定した者（令和5年11月16日時点）https://www.meti.go.jp/policy/economy/economic_security/kokuji.pdf
特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針 https://www.cao.go.jp/keizai_anzen_hosho/doc/kihonshishin2.pdf

（参考）電気事業における規制対象

対象事業 （特定社会基盤事業）	特定社会基盤事業者の 指定基準	特定重要設備※1	重要維持 管理等※2	構成設備※3
一般送配電事業	**電気事業法第2条第1項第9号に規定する一般送配電事業者**（全者を指定）	**需給制御システム**	・維持管理 ・操作	・監視制御サーバ ・需給演算サーバ ・需給制御業務アプリケーション、OS、ソフトウェア
		系統制御システム		・監視制御サーバ ・操作サーバ ・系統制御業務アプリケーション、OS、ソフトウェア
送電事業	**電気事業法第2条第1項第11号に規定する送電事業者**（全者を指定）	**系統制御システム**		・監視制御サーバ ・操作サーバ ・系統制御業務アプリケーション、OS、ソフトウェア
配電事業	**電気事業法第2条第1項第11号の3に規定する配電事業者**（全者を指定※） ※現在営んでいる事業者が存在しないため指定事業者なし	**需給制御システム**		・監視制御サーバ ・需給演算サーバ ・需給制御業務アプリケーション、OS、ソフトウェア
		系統制御システム		・監視制御サーバ ・操作サーバ ・系統制御業務アプリケーション、OS、ソフトウェア
発電事業	所有する発電設備：**発電設備ごとの出力が50万kW以上**※ （我が国の発電容量の大半を確保できる数値として設定） ※出力は、火力・原子力等は発電機ごと、水力・風力・蓄電池等は発電所・蓄電所ごとに判断	**出力制御装置**		・監視制御サーバ ・各種制御装置（ボイラー監視制御装置、タービン監視制御装置等） ・アプリケーション、OS等のソフトウェア
特定卸供給事業	集約する電気：**50万kW以上** （発電事業と同様）	**エネルギーマネジメントシステム**		・監視制御サーバ ・アプリケーション、OS等のソフトウェア

※１　特定重要設備：「特定社会基盤事業の用に供される設備、機器、装置又はプログラムのうち、特定社会基盤役務を安定的に提供するために重要であり、かつ、我が国の外部から行われる特定社会基盤役務の安定的な提供を妨害する行為の手段として使用されるおそれがあるもの」として国が定めるもの
※２ 重要維持管理等：「特定重要設備の維持管理又は操作のうち、当該特定重要設備の機能を維持するため又は当該特定重要設備に係る特定社会基盤役務を安定的に提供するために重要であり、かつ、これらを通じて当該特定重要設備が我が国の外部から行われる特定社会基盤役務の安定的な提供を妨害する行為の手段として使用されるおそれがあるもの」として国が定めるもの
※３ 構成設備：「特定重要設備若しくは特定重要設備の一部を構成する設備、機器、装置若しくはプログラムであって特定妨害行為の手段として使用されるおそれがあるもの」として国が定めるもの

出所）特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針 https://www.cao.go.jp/keizai_anzen_hosho/doc/kihonshishin2.pdf
経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度について https://www.cao.go.jp/keizai_anzen_hosho/doc/infra_setsumeikai.pdf
電気事業における経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度の解説 https://www.meti.go.jp/policy/economy/economic_security/denki.pdf

（参考）届出事項（導入等計画書）の詳細

- 特定社会基盤事業者が作成する導入等計画書には、**「特定重要設備の概要」「導入の時期/委託の時期又は期間」「特定重要設備の供給者に関する事項/重要維持管理等の委託の相手方に関する事項」「特定重要設備の導入/重要維持管理等の委託に当たって特定社会基盤事業者が講ずる特定妨害行為を防止するための措置に係る事項（リスク管理措置）」を記載する**必要がある。
- 加えて、特定重要設備の導入時には「特定重要設備の一部を構成する設備、機器、装置又はプログラムであって特定妨害行為の手段として使用されるおそれがあるもの（構成設備）に関する事項」、重要維持管理等の委託時には「重要維持管理等の委託の相手方が他の事業者に再委託して重要維持管理等を行わせる場合にあっては、当該再委託に関する事項」（※）を記載する必要がある。

（※）重要維持管理等の委託の相手方が他の事業者に再委託して重要維持管理等を行わせる場合

導入等計画書における記載事項

事項	特定重要設備の導入を行う場合	特定重要設備の重要維持管理等を行わせる場合
特定重要設備の概要	種類、名称、機能、設置場所、使用場所	種類、名称、機能、設置場所、使用場所
導入の内容及び時期/委託の内容及び時期又は期間	導入の目的、導入に携わる者の名称等、導入の時期	委託の目的、委託の内容・場所、委託の時期又は期間
特定重要設備の供給者に関する事項/重要維持管理等の委託の相手方に関する事項	供給者の名称・住所・設立準拠法等、供給者の議決権の5%以上を保有する者、供給者の役員の氏名・生年月日・国籍等、（供給者が、外国政府等との取引が売上高の25%以上を占める場合）外国政府等の名称等、設備の製造場所の所在地	相手方の名称・住所・設立準拠法国等、相手方の議決権の5%以上を保有する者、相手方の役員の氏名・生年月日・国籍等、（相手方が、外国政府等との取引が売上高の25%以上を占める場合）外国政府等の名称等
構成設備に関する事項/重要維持管理等の再委託に関する事項	構成設備の概要（種類・名称・機能）、供給者の名称・住所・設立準拠法国、供給者の議決権の5%以上を保有する者、供給者の役員の氏名・生年月日・国籍等、（供給者の外国政府等との取引が当該供給者の売上高全体の25%以上を占める場合）取引先の外国政府等の名称等、構成設備の製造場所の所在地	再委託の内容・場所・時期又は期間、相手方の名称・住所・設立準拠法国、相手方の議決権の5%以上を保有する者、相手方の役員の氏名・生年月日・国籍等、（相手方の外国政府等との取引が当該相手方の売上高全体の25%以上を占める場合）取引先の外国政府等の名称等
リスク管理措置	導入に関するリスク管理措置	重要維持管理等の委託に関するリスク管理措置

出所）特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針 https://www.cao.go.jp/keizai_anzen_hosho/doc/kihonshishin2.pdf
経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律 https://elaws.e-gov.go.jp/document?lawid=504AC0000000043
経済安全保障推進法の特定社会基盤役務の安定的な提供の確保に関する制度について https://www.cao.go.jp/keizai_anzen_hosho/doc/infra_gaiyou.pdf

（参考）審査に当たっての考慮要素

- 特定重要設備が特定妨害行為の手段として使用されるおそれが大きいかどうかを審査するに当たっては、以下に掲げる要素等を考慮することとしている。

審査に当たっての考慮要素

① 特定社会基盤事業者が導入等を行おうとする特定重要設備の供給者等が我が国の外部にある主体から強い影響を受けているかどうか

② 特定社会基盤事業者が導入等を行おうとする特定重要設備について、特定社会基盤役務の安定的な提供が妨害されるおそれに関する評価を自ら行い、その結果に応じて、リスク管理措置を講じているかどうか

③ 特定社会基盤事業者が導入等を行おうとする特定重要設備について、その供給者等が供給する特定重要設備及び構成設備に関する製品に対して脆弱性が指摘された例、その供給者等が実施する重要維持管理等に対して不適切性が指摘された例及びその供給者等に対して我が国の法令や国際的に受け入れられた基準等の不遵守等が指摘された例

④ ①から③までのほか、特定重要設備の導入等又は特定重要設備の供給者等に関して特定重要設備が特定妨害行為の手段として使用されるおそれに関する事項

出所）特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針 https://www.cao.go.jp/keizai_anzen_hosho/doc/kihonshishin2.pdf

海外電力分野における サプライチェーン・リスクに関する規制状況

- 海外では、**罰則規定のある法規制において、電力会社におけるサプライチェーン・リスク管理を求めている**。
- ドイツでは、一部の電力会社に対して、導入する重要部品に関する政府への事前通知・審査を求めている。
- また、英国では、一部の電力会社に対して、サプライヤー契約に関する政府への通知を求めている。

海外電力分野におけるサプライチェーン・リスクに関する規制状況

国・地域				
法規制	• 連邦電力法	• ITセキュリティ法2.0 • エネルギー産業法 • BSI法	• NIS規則 • 国家安全保障・投資法（NS&I Act）	• NIS指令/NIS2指令 • EU Regulation No. 2019/943
要件文書	• NERC CIP-013: Cyber Security - Supply Chain Risk Management	• ITセキュリティカタログ（IT-Sicherheitskatalog）	• NIS Guidance • Cyber Assessment Framework (CAF)	• EU各国の国内法により規程 • Network Code on Cybersecurity
所管組織	• FERC（連邦エネルギー規制委員会） • NERC（北米電力信頼度協議会）	• BSI（連邦情報セキュリティ庁） • BMI（連邦内務省） • BNetzA（連邦ネットワーク庁）	• NCSC（国家サイバーセキュリティセンター） • Ofgem（ガス・電力市場局） • BEIS（ビジネス・エネルギー・産業戦略省）	• EU各国の所管省庁 • ENTSO-E
電力会社に求められるサプライチェーン・リスク対策	• サプライチェーン・リスク管理の実施 • サプライチェーン・リスク管理計画の定期的な見直し（少なくとも15ヶ月に一度） • サプライチェーン・リスク管理状況のNERCへの報告	• サプライチェーン・リスク管理の実施 • 導入する重要部品に関する政府への事前通知・審査 • インシデント情報等に関する政府への報告	• サプライチェーン・リスク管理の実施 • 対策状況に関する政府への定期的な報告 • サプライヤー契約に関する政府への通知 • 政府による調査・介入への協力	• サプライチェーン・リスク管理の実施 • 人的サプライチェーンへの対策（産業スパイへの対策、企業秘密の保護など） • 委託先や導入部品のサイバーセキュリティ対策の検証
罰則等	• 違反度合いに応じた罰則規程あり	• 最大2,000万ユーロ（約30億円）又は企業の全世界売上高の4%のいずれか高い方の罰金	• 最大1,700万ポンド（約30億円）の罰金	• NIS2指令では、最大1,000万ユーロ（約15億円）又は企業の全世界売上高の2%のいずれか高い方の罰金

出所）各国規制に関する公開情報に基づき作成

電力制御システムにおいて求められる サプライチェーン・リスク対策（案）

- 電力制御システムに想定されるサプライチェーン・リスクに対応するために、NISC安全基準等策定指針、経済安全保障推進法及び現行の電力制御システムセキュリティガイドラインの内容を踏まえ、**以下のような対策を事業者に求めていくべきではないか。**

項目	事業者に求めていくべきサプライチェーン・リスク対策（案）	対応するサプライチェーン・リスク
サプライチェーン・リスク管理	● 委託先等の対応に関して、電力制御システム等に関連する委託先等の役割と責任範囲を明確にする。 ● 電力制御システム等におけるサプライチェーンの依存関係及び委託先等のセキュリティ対策状況を把握する。 ● 電力制御システム等のサプライチェーン・リスクに関するセキュリティリスク管理を行う。	全リスク
セキュリティ仕様の確認	● 電力制御システム等のセキュリティ仕様に関して、電力制御システム等の調達時にセキュリティ仕様を明確にする。 ● 仕様への準拠性の確認に関して、電力制御システム等がセキュリティ仕様通りに設計、製造されていることを確認する。 ● 電力制御システム等の仕様変更に関して、セキュリティに影響を与える可能性がある変更を適切に管理する。	• 開発・製造時の不正な改造 • 開発・製造時の不正プログラムの埋め込み • 運用・保守時のソフトウェアの不正な更新
機器・外部記憶媒体の管理	● 機器・外部記憶媒体の管理に関して、機器・外部記憶媒体をライフサイクルを通じて管理し、保護する。	• 調達時の不正な改造 • 調達時の不正プログラムの埋め込み • 廃棄時の機密情報の窃取

【用語の定義（電力制御システムセキュリティガイドラインより引用）】
- 委託先等：委託先,再委託先及び発注先をいう。
- 機器：システムを構成するサーバー、パソコンや可搬型の機器等の端末及びネットワークの構成機器をいう。
- 電力制御システム：電力の安定供給、電気工作物の保安(公衆安全を含む)の確保に資するために、電気事業の用に供する電気工作物を監視・制御する機能等を具備したシステムをいう。
- 電力制御システム等：電力制御システム及び電力制御用ネットワークの全体をいう。
- 電力制御用ネットワーク：電力制御システム同士をつなぐネットワーク又は制御箇所と被制御箇所を結ぶネットワークをいう。
- セキュリティ仕様：電力制御システム等の機能要件に応じて策定されたセキュリティ要件をいう。
- ライフサイクル：電力制御システム等の計画・開発・調達・運用・保守・廃止をいう。

電力制御システムのサプライチェーン・セキュリティ向上策に関する提言

- 2024年3月22日、第16回電力SWGでの議論をとりまとめた、**電力制御システムのサプライチェーン・リスクに対するセキュリティ向上策についての提言を公表。**

2024年3月22日公表「電力制御システムのサプライチェーン・セキュリティ向上策に関する提言」から一部抜粋・編集

実際にサプライチェーン・リスクが顕在化した事例も複数存在するところ、電気事業者においては、想定されるリスクに対して適切な対策を講じることが求められる。特に、安全基準等策定指針の記載や諸外国の取組等を踏まえ、以下の取組を実施することが求められる。

■ サプライチェーン・リスク管理

電気事業者は、電力制御システム等に関連する委託先等の役割と責任範囲を明確化するほか、電力制御システム等のサプライチェーンの依存関係及び委託先等のセキュリティ対策状況を把握する。また、電力制御システム等のサプライチェーン・リスクに関するリスク分析を行い、それに基づいた対策を講じるとともに、対策の状況を定期的に把握し、把握結果に基づき対策の見直しを検討する。リスク分析の実施に当たっては、情報処理推進機構（IPA）の「制御システムのセキュリティリスク分析ガイド」等を参照し、自組織の事業環境等を踏まえて、シナリオベースや資産ベースのリスク分析等、適切な分析手法を選択又は相互補完的に組み合わせて分析することが想定される。さらに、対策状況の把握に当たっては、資源エネルギー庁「電力システムにおけるサイバーセキュリティ対策状況可視化ツール」等を活用することが想定される。

■ セキュリティ仕様の確認

電気事業者は、電力制御システム等の調達時にセキュリティ仕様を発注仕様書等において明確にするほか、電力制御システム等がセキュリティ仕様通りに設計、製造されていることを確認する。また、セキュリティに影響を与える可能性がある変更を適切に管理する。

■ 機器・外部記憶媒体の管理

電気事業者は、電力制御システム等に関わる機器・外部記憶媒体を、システムライフサイクル（運用・保守段階だけでなく、廃止段階も含む）を通じて管理し、保護する。

事業者における効果的かつ実効性のある取組の実施に向け、「電力制御システムセキュリティガイドライン」を発行する日本電気協会及び策定に携わる電気事業連合会等のその他の機関においては、ガイドラインの見直しを検討することが望まれる。

政府においては、**電気事業者におけるこれらの取組に向けた環境整備や実施を支援していくべき**である。また、**電気事業連合会等や電気事業者は、事業者に求められる対応を詳細化した手引き文書の策定等により実効性のある対応を進めていくべき**である。さらに、サプライチェーン全体での対策実効性を高めるために、**政府又は事業者はサプライチェーン全体での教育・訓練の実施等に向けた方策について検討を進めるべき**である。加えて、電気事業者は、経済安全保障の観点を踏まえ、サイバーセキュリティ上のリスクだけでなく、物理的な妨害行為等のリスクも考慮した包括的な対策を検討することが望まれる。加えて、政府においては、事業者がサプライチェーン・リスクに対応するために必要な情報を取得、提供及び利用できるようにするための取組について、法律等において妨げるものがないか、考え方を整理することが望まれる。これらの検討に当たっては、他分野との相互依存性を踏まえ、電力分野以外の動向も踏まえた検討が必要となる。

サプライチェーン・リスクは日々高度化・複雑化していることを踏まえ、関係者による引き続きの議論や検討を進めていくことが重要である。

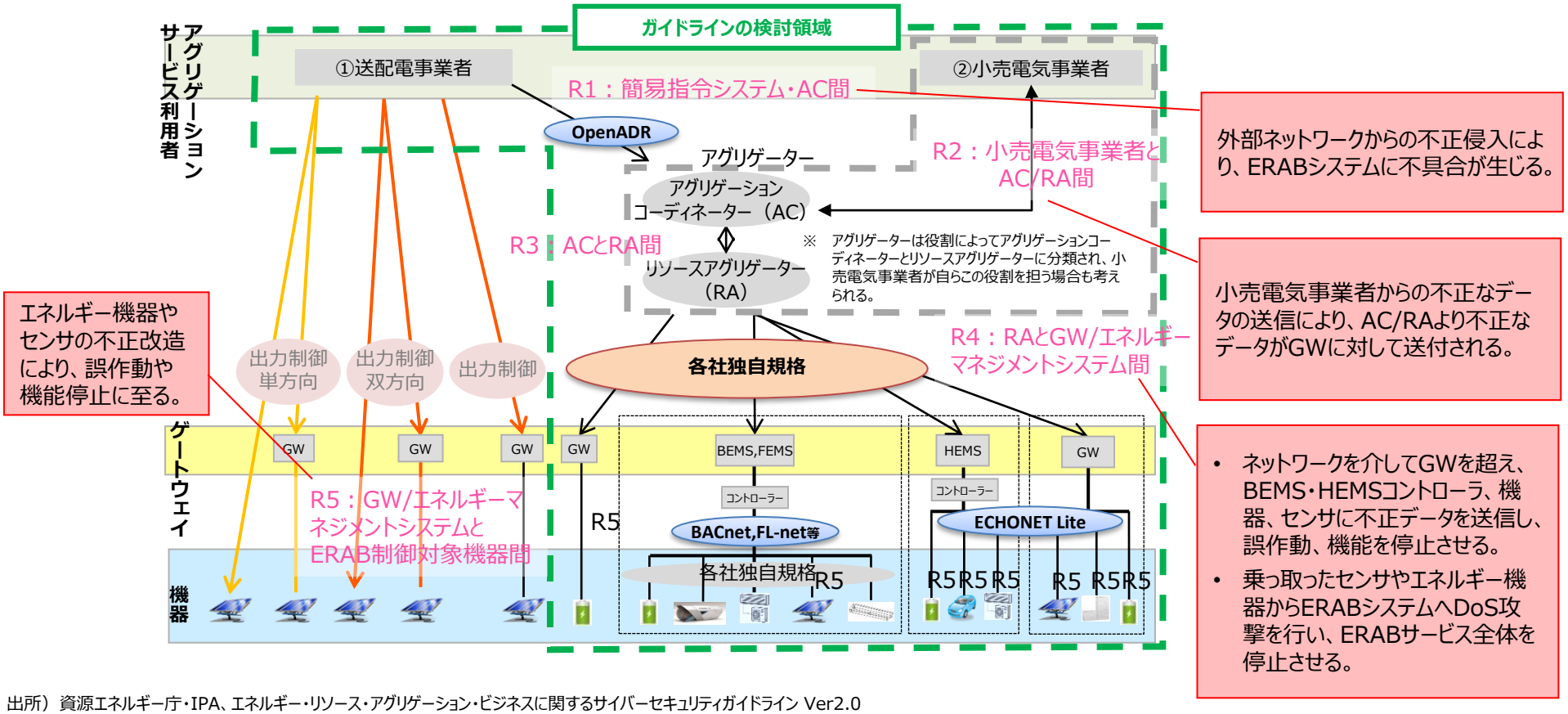
出所）電力制御システムのサプライチェーン・セキュリティ向上策に関する提言
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_denryoku/pdf/016_t01_00.pdf

ERABシステムの概要と想定されるサイバーセキュリティ脅威

第16回 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
（制度・技術・標準化）電力ＳＷＧ(2024年2月1日) 資料6-2より作成

- ERAB（エネルギー・リソース・アグリゲーション・ビジネス）システムでは、**送配電事業者、アグリゲーションコーディネーター（AC）、リソースアグリゲーター（RA）、小売電気事業者など多くのステークホルダーが関与**する。
- 「ERABに関するサイバーセキュリティガイドライン」では、ERABシステムのレイヤーを整理した上で、ERABシステムにおいて想定されるセキュリティ脅威が示されている。

ERABシステムの概要と想定されるサイバーセキュリティ脅威

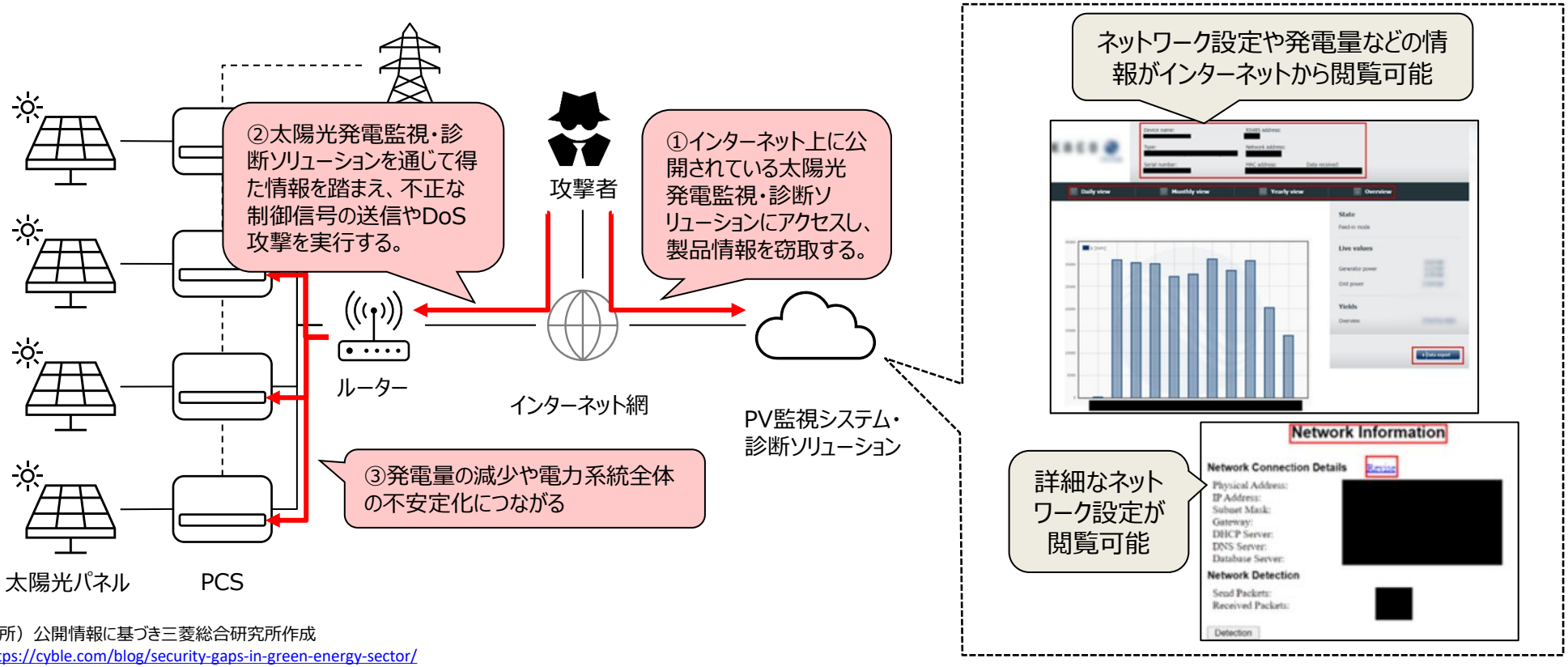


出所）資源エネルギー庁・IPA、エネルギー・リソース・アグリゲーション・ビジネスに関するサイバーセキュリティガイドライン Ver2.0
https://www.enecho.meti.go.jp/category/saving_and_new/advanced_systems/vpp_dr/files/20171129002-1.pdf

（DER設備に関する脅威事例）
インターネットからアクセス可能なPV監視・診断ソリューション

- 2023年7月、サイバーセキュリティ企業のCyble社は、**130,000件以上のPV（太陽光発電）監視・診断ソリューションがインターネット上からアクセス可能である**ことを報告した。
- 同社は、PV監視・診断ソリューションを通じて、**攻撃者が製品情報を閲覧可能な状態である**ことから、**潜在的な攻撃の対象となっていると警告**した。
- 公開されていたソリューションのベンダーには、Solar-Log社、SMA社のほか、国内ベンダーのコンテック社も含まれていた。

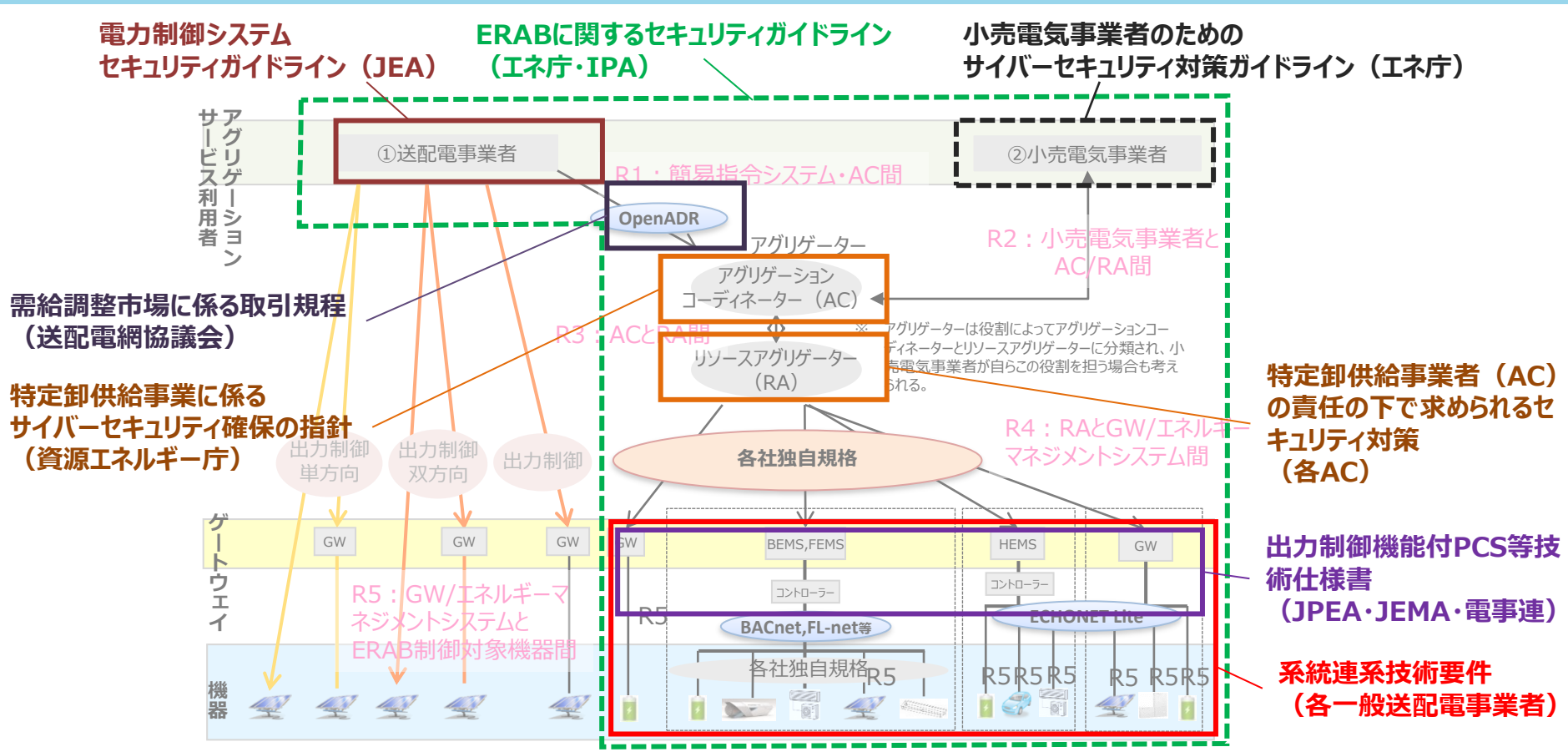
実際にインターネットからアクセス可能であったページと情報を悪用した攻撃のイメージ



出所）公開情報に基づき三菱総合研究所作成
https://cyble.com/blog/security-gaps-in-green-energy-sector/

ERABシステムが準拠すべきセキュリティガイドライン等

- ERABシステムに求められるセキュリティガイドラインとして、**システム全体に対する「ERABに関するサイバーセキュリティガイドライン（以下、ERABセキュリティガイドライン）」があるほか、個々のステークホルダーに対するガイドラインが整備**されている。
- 末端のリソースに関して、系統に接続する設備は「系統連系技術要件」に基づく対策が求められるほか、出力制御機能付PCSについて、セキュリティの要件を含んだ技術仕様書が公開されている。



出所）各種ガイドラインに基づき三菱総合研究所作成

※ 実線は義務で対策が求められるガイドライン等、点線は任意で対策が求められるガイドライン等を意味する。

アグリゲーターが抱えるセキュリティにおける課題

- これまで、アグリゲーターのセキュリティ対策に関する様々な取組が進められてきたところであるが、事業者や有識者と意見交換やヒアリングを実施したところ、以下の課題が確認された。
- 具体的には、ERABセキュリティガイドラインの準拠のために、**各社で詳細対策要件を作成することが求められている一方で、現状ではその作成が困難であることや、作成した詳細対策要件の妥当性を確認することが難しいことの課題**が挙げられた。
- 加えて、これまでのガイドラインでは具体的に想定してこなかった電力系統及びアグリゲーターシステムに接続する**末端のIoT機器等のセキュリティ対策に対するリスク**が示唆された。
- また、業界として、アグリゲーターにおけるセキュリティ対策の実態を把握出来ていない課題が挙げられた。

課題概要	課題内容
詳細対策要件の作成・確認について	• **ERABセキュリティガイドラインに準拠するための詳細対策要件を作成するのが難しい。** • チェックシートを作成する場合は、事業の重要度によって対策要件が変わることが望まれる。 • **自社で作成した詳細対策要件に抜け漏れがある可能性**がある。
末端のIoT機器等の脆弱性に起因する脅威について	• **ERABセキュリティガイドラインのR4,R5にあたるIoT機器等のセキュリティを高めることが望まれる。** • **特に太陽光のリソースは数が増えている一方、セキュリティの検討が不十分である。**
ガイドラインの定期アップデートについて	• アグリゲーションは一過性ではなく、様々な分散型エネルギー源が追加されるため、ガイドラインを定期的にメンテナンスする必要がある。

アグリゲーター及びDERのセキュリティ対策推進の方向性について

- 今後、太陽光発電をはじめとして、DERの更なる追加が見込まれるところ、まずは、**近年のIoTに関する脅威動向や取組動向を踏まえつつ、末端のIoT機器等に求められるセキュリティ対策を整理することが必要ではないか。**また、末端のIoT機器等における脆弱性対応の高度化に向け、**脆弱性情報の共有や管理等のあり方についても整理することが必要ではないか。**
- その上で、**既存ガイドラインへの影響や整合性等を確認した上で、どのようにこれらをERABセキュリティガイドラインの改定に取り組んでいくか、検討すべきではないか**。
- また、**詳細対策要件の策定が進められるよう、参考となる考え方の整理や、ERABに参画する事業者が相談できる体制の整備等について、事業者のビジネス環境を考慮したうえで検討する必要があるのではないか。**
- 業界としてアグリゲーターの**セキュリティ対策の実態把握**をするために、広域機関の会員が提出する**サイバーセキュリティリスク点検ツールの**結果については、広域機関と資源エネルギー庁の間で連携していく。**点検結果の集計時期や連携される情報等について、検討する必要があるのではないか。**

リスク点検ツールの必要性・作成

- サイバーセキュリティ対策の継続的改善・高度化に向けては、「電力制御システムセキュリティガイドライン」にも記載のとおり、**PDCAサイクルに基づくセキュリティ対策の計画・実施・点検・改善のプロセスが重要**となるが、過年度事業における調査によると、対策を実施している事業者の割合と比較して、**定期的な対策状況の評価（リスク点検）や継続的な対策改善を実施している事業者は限定的**であった。
- 併せて、過年度調査では、電力システムに関連する様々なプレイヤーが**過大なコストをかけることなく簡易的にリスク点検ができるようなツール（チェックリスト等）の必要性が提示された**。
- このような議論を踏まえ、昨年度の事業において、コストを抑えて簡易的にリスク点検ができる**「電力システムにおけるサイバーセキュリティ対策状況可視化ツール」の案を作成**した。
- 今年度、**電気事業者による試行利用を通じてリスク点検ツールの課題等を抽出**するとともに、**試行利用結果を踏まえてツールの改善を行い、リスク点検ツールの正式公開を行った**。また、**リスク点検ツールの正式公開にあたり、リスク点検ツールの位置づけや普及促進策についても検討を行った**。

リスク点検ツールの構成

- リスク点検ツールは、**「電力システムにおけるサイバーセキュリティリスク点検に関するガイド（参考資料2）」と「電力システムにおけるサイバーセキュリティ対策状況可視化ツール （参考資料3）」によって構成**する。
- ガイドは、国内電気事業者において自社の対策状況の確認やリスク評価に当たって活用できる文書とし、**リスク点検項目を示しつつ、リスク点検結果を踏まえた対策の改善方針も示す。**
- 対策状況可視化ツールは、各事業者が**リスク点検項目に対する対応状況を入力することで簡易に組織の成熟度や対策状況を可視化できるツール**とし、Excel形式にて作成する。

リスク点検ツールの構成案

リスク点検ツール

電力システムにおけるサイバーセキュリティリスク点検に関するガイド

事業者が、自社の対策状況の確認やリスク評価に当たって活用できるガイド。具体的には以下の目次構成を設定する。

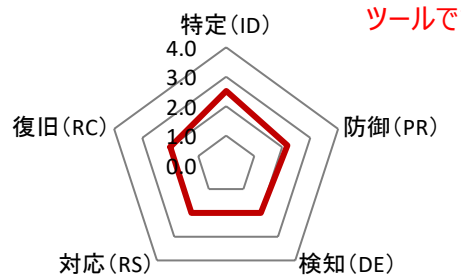
1. 背景・目的
2. 本ガイド・対策状況可視化ツールの構成
3. 本ガイド・対策状況可視化ツールの対象
4. 本ガイド・対策状況可視化ツールの想定活用方法
5. リスク点検項目・対策を怠った場合のリスク
6. リスク点検結果を踏まえた対策の改善方針
7. 参考文書
8. 用語集

＋

電力システムにおけるサイバーセキュリティ対策状況可視化ツール

各事業者がリスク点検項目に対する対応状況を入力することで、組織の対策状況を可視化する。ヒアリング結果を踏まえ、Excel形式にて作成する。

リスク点検項目に対する対応状況を、可視化ツールで記載



リスク点検ツールの対象事業者

- リスク点検ツールの対象事業者について、一般送配電事業者については電事連によるリスクアセスメントが推進されているところ、その他の**①発電事業者、②小売電気事業者、③アグリゲーター（アグリゲーションコーディネーター及びリソースアグリゲーター）、④自家用電気工作物設備設置者の4区分を主な対象**とする。
- 4区分のうち、大手事業者の多くはリスク点検を既に定期的に実施しているところ、本事業で開発する**リスク点検ツールでは、中小事業者をはじめとするこれまでリスク点検を実施してこなかった事業者をメインスコープ**とし、当該事業者における簡易的かつ効率的なリスク点検を支援する内容とする。

リスク点検ツールの対象事業者

以下の4区分の事業者のうち、中小事業者をはじめとする
これまでリスク点検を実施してこなかった事業者を主な対象とする。

① 発電事業者

② 小売電気事業者

③ アグリゲーター
（アグリゲーションコーディネーター及びリソースアグリゲーター）

④ 自家用電気工作物設備設置者

【参考】リスク点検項目の概要

- **具体的なリスク点検項目について**、国内外の事業者において広く活用され、電事連が電力10社を対象に実施したリスク評価でも活用された**NISTのCybersecurity Framework（NIST CSF）を参考に整理**。
- NIST CSFでは、5つのセキュリティ機能（特定、防御、検知、対応、復旧）に対し、機能の詳細を定めた23のカテゴリー、108のサブカテゴリーが定義されているため、**本リスク点検ツールでは108のサブカテゴリーをリスク点検項目として設定**する。

機能	カテゴリー		サブカテゴリー数
特定(ID)	ID.AM	資産管理	6
	ID.BE	ビジネス環境	5
	ID.GV	ガバナンス	4
	ID.RA	リスクアセスメント	6
	ID.RM	リスク管理戦略	3
	ID.SC	サプライチェーンリスクマネジメント	5
防御(PR)	PR.AC	アクセス制御	7
	PR.AT	意識向上及びトレーニング	5
	PR.DS	データセキュリティ	8
	PR.IP	情報を保護するためのプロセス及び手順	12
	PR.MA	保守	2
	PR.PT	保護技術	5

機能	カテゴリー		サブカテゴリー数
検知(DE)	DE.AE	異常とイベント	5
	DE.CM	セキュリティの継続的なモニタリング	8
	DE.CP	検知プロセス	5
対応(RS)	RS.RP	対応計画	1
	RS.CO	伝達	5
	RS.AN	分析	5
	RS.MI	低減	3
	RS.IM	改善	2
復旧(RC)	RC.RP	復旧計画	1
	RC.IM	改善	2
	RC.CO	伝達	3

NIST CSFの各サブカテゴリーを、リスク点検ツールにおけるリスク点検項目として設定

【サブカテゴリーに基づくリスク点検項目の例】

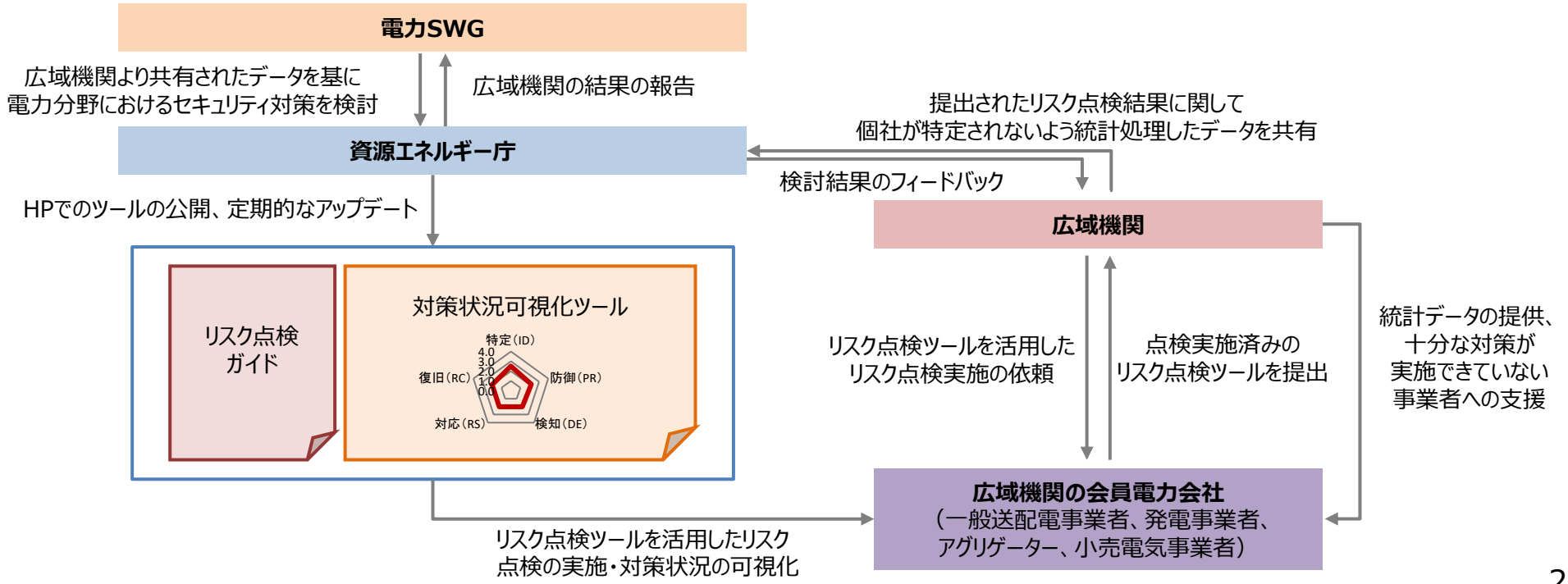
PR.PT-1：監査記録/ログ記録の対象が、ポリシーに従って決定され、文書化され、実装され、その記録をレビューされている。(ログの取得を実施している。)

PR.PT-2：リムーバブルメディアは、保護され、その使用がポリ シーに従って制限されている。(外部記憶媒体をルールに則って管理している。)　等

広域機関の自己診断票との連携

- これまで使用されていた**広域機関の自己診断票を今回のリスク点検ツールと統合する**。
- 資源エネルギー庁HPにてリスク点検ツールを公開後、広域機関では、**公開されたホームページを参照する形式でリスク点検の実施を会員企業に依頼**する。**会員企業は、エネ庁HPから公開されたツールに基づきリスク点検を実施し、実施結果を広域機関に提出**する。
- 会員企業のリスク点検結果は、**広域機関により個社が特定されないよう統計処理した上で、資源エネルギー庁に共有いただく**。今後、**電力SWGにおいてはリスク点検ツールに対する取組状況や点検結果等も踏まえ、電力分野におけるセキュリティ対策のあり方を検討していく**。

リスク点検ツールの広域機関との連携スキーム



【参考】リスク点検ツールのニュースリリース（2024年3月22日）

「電力システムにおけるサイバーセキュリティリスク点検ガイド」と「電力システムにおけるサイバーセキュリティ対策状況可視化ツール」を電気事業者向けに公表しました

2024年3月22日

▶ エネルギー・環境

サイバーセキュリティ対策の継続的改善・高度化に向けては、PDCAサイクルに基づくセキュリティ対策の計画・実施・点検・改善のプロセスが重要です。そのため、今般、電気事業者を主な対象として、過大なコストをかけずに簡易的にリスク点検ができるよう、「電力システムにおけるサイバーセキュリティリスク点検ガイド」及び「電力システムにおけるサイバーセキュリティ対策状況可視化ツール」を開発し、公表しました。

1. 対象

電力システムにおけるサイバーセキュリティリスク点検ガイド（以下、「本ガイド」という。）及び電力システムにおけるサイバーセキュリティ対策状況可視化ツール（以下、「対策状況可視化ツール」という）は、主に以下の4つの事業区分の電気事業者等及び当該事業者等が保有する電力制御システム・ITシステムを対象としています。

① 発電事業者
② 小売電気事業者
③ アグリゲーター
（アグリゲーションコーディネーター及びリソースアグリゲーター）
④ 自家用電気工作物設備設置者

2. 本ガイド・対策状況可視化ツールの概要

本ガイドは、自社の対策状況の確認やリスク評価に当たって活用できる文書であり、リスク点検項目を示しつつ、リスク点検結果を踏まえた対策の改善方針も示します。
対策状況可視化ツールは、各事業者がリスク点検項目に対する対応状況を入力することで簡易に組織の成熟度や対策状況を可視化できるツール（Excel形式）です。

出所）「電力システムにおけるサイバーセキュリティリスク点検ガイド」と「電力システムにおけるサイバーセキュリティ対策状況可視化ツール」を電気事業者向けに公表しました
https://www.meti.go.jp/press/2023/03/20240322003/20240322003.html

今後の取組の方向性

１．電力制御システムにおけるサプライチェーン・リスクに対する対応について

- 「電力制御システムのサプライチェーン・セキュリティ向上策に関する提言」を踏まえた形で、今年度、日本電気協会において、電力制御システムセキュリティガイドラインの改定の作業が進められる予定であり、電力SWGにおいて、提言を踏まえた形で進められているか、その状況をフォローしていく。
- また、電気事業者がこの改訂された内容を実装していくことを促進するために必要となる対応を電力SWGにおいて検討していく。

２．アグリゲーター及び分散型エネルギー源（DER）のセキュリティ対策について

- 第16回電力SWGの議論も踏まえた形で、DERにおけるサイバーセキュリティ・リスクへの対応等について強化するため、今年度、「ERABに関するサイバーセキュリティガイドライン」の改定に着手する。また、ガイドラインに基づき、アグリゲーター等が詳細対策要件の策定が進められるよう、参考となる考え方の整理や、ERABに参画する事業者が相談できる体制の整備等について、ビジネス環境を考慮しつつ、業界団体等と検討を開始する。
- DERの活用とセキュリティ対策について、IECにおいて進められているERABの基本システムの標準化の取組を踏まえつつ、東アジア・アセアン経済研究センター（ERIA）と連携して日ASEAN大での普及策等の検討に取り組んでいく。

3．電力システムにおけるサイバーセキュリティリスク点検ツールについて

- 第16回電力SWG において整理したとおり、2024年度から主に広域機関の会員企業に任意で活用されることになる。広域機関の会員企業における活用を促進するため、業界団体等とも連携して、電気事業者による活用を促すための周知を行う。
- 点検結果等について、広域機関とも連携して、今年度の電力SWGへ報告するとともに、事業者・アグリゲーターのヒアリングも行いながらインセンティブや支援の検討を行う。