経済産業省

資料５

電力分野におけるサイバーセキュリティについて

２０２０年6月１１日

資源エネルギー庁

本日御議論いただきたいこと

- 近年、サイバー攻撃の事案は増加傾向にあり、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している。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。
- こうした状況を踏まえ、第21回基本政策小委員会において、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）において、事業者のサイバーセキュリティ対策の成熟度を把握するための実態調査（対象：発電事業者、小売電気事業者、アグリゲーター）の実施について報告させていただいたところ。
- 本日は、**当該実態調査の結果について御報告**させていただくとともに、**当該実態調査のフィードバック方法**や、**設備の系統連系において求めるべきセキュリティ要件**について御議論いただきたい。

（参考）近年のサイバー攻撃について

第20回電力・ガス基本政策
小委員会資料（2019年8月）

- 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）

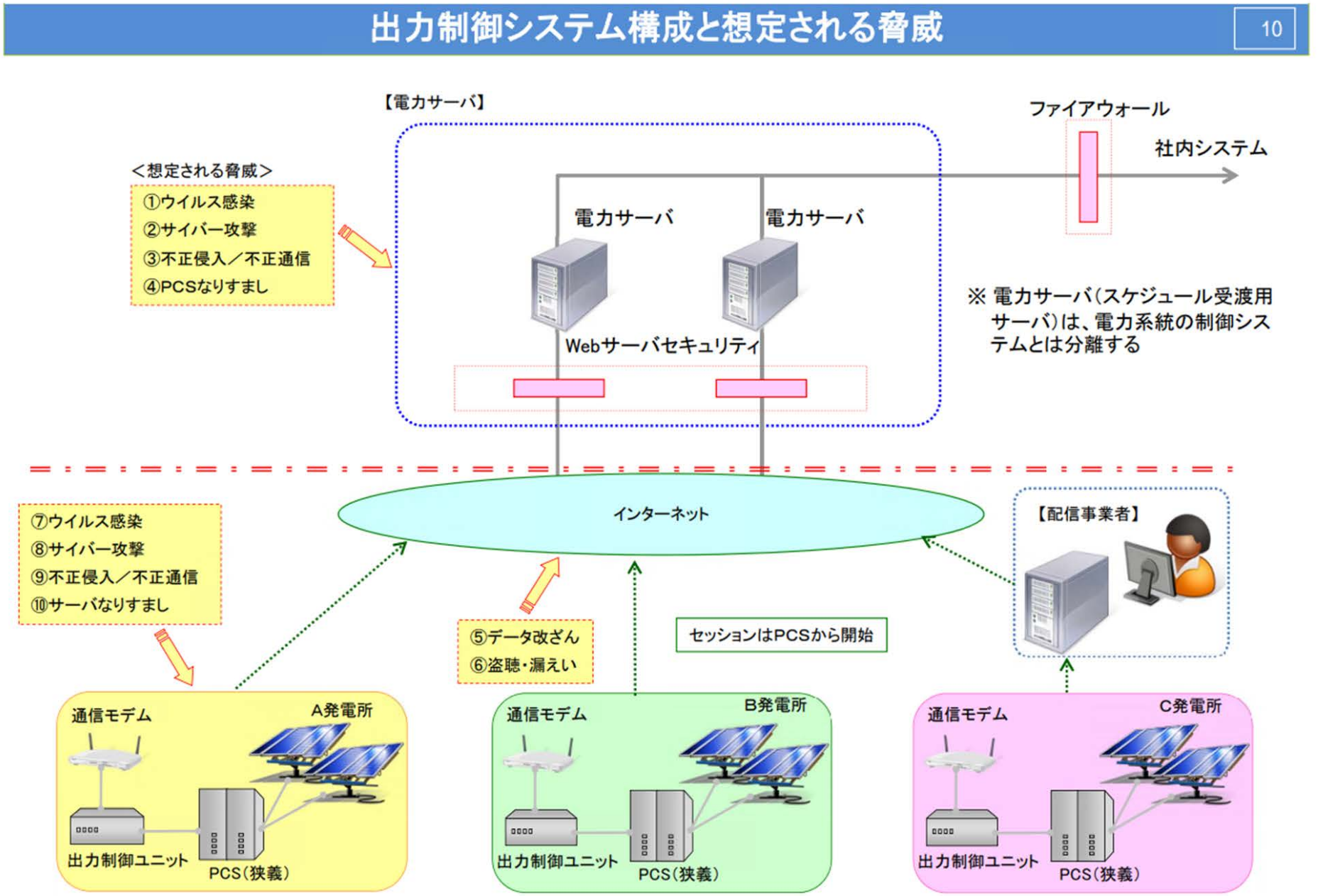
複雑なサプライチェーンによる脅威の例：携帯端末に不正プログラムが仕掛けられた事例

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。

（参考）再生可能エネルギー発電設備に想定される脅威

第5回新エネルギー小委員会
系統ワーキンググループ資料
（2015年３月）



（参考）実態調査の目的

第21回電力・ガス基本政策
小委員会資料（2019年11月）

- 電力システム改革に伴い、小売電気事業に多くの新電力が参入するとともに、分散型電源を活用したアグリゲーター事業を行う事業者も出現するなど、多くの新規プレーヤーが電力分野において事業に取り組んでいる状況。
- 今後も多くの新規プレーヤーが参入すると考えられるところ、このような事業者に対しても適切にサイバーセキュリティ対策を求める必要があると考えられる。
- このため、電力システムにおける包括的なサイバーセキュリティ対策を検討する観点から、小売電気事業者及びアグリゲーターにおけるサイバーセキュリティ対策の実態について調査を実施する。
- 併せて、経営者のリスク認識を問うことによる会社全体としてのセキュリティ意識の向上や、自社のサイバーセキュリティ対策の実施状況の見直しによるサイバーセキュリティ強化を促す。

※　本調査は、11月上中旬発送、12月上旬回答締切予定。調査結果については①資源エネルギー庁にて適正に取り扱い、②各事業者の匿名性を確保の上、電力SWGや審議会における審議においてのみ使用する。

１．実態調査の結果等について

【報告】実態調査の結果

- 発電事業者、小売電気事業者及びエネルギー・リソース・アグリゲーション・ビジネス（ERAB）に参画している事業者（ERAB事業者）の計981者に対し、それぞれの事業者区分に応じて、組織的対策・技術的対策の双方の実態を確認・分析するための設問を設定し、アンケート調査を実施。
- 有効回収数（回収率）は以下のとおり。
  - 発電事業者[1]：349者（62.1%）
  - 小売電気事業者[2]：245者（56.7%）
  - アグリゲーター[3]：12者（70.6%）
  - 合計：548者（55.9%）

※ 複数事業を展開している事業者がいるため、合計数は一致しない。

1 2019年5月に発電実績のある562の発電事業者に対して、アンケート調査票を送付した。
2 2019年5月に需要実績のある432の小売電気事業者に対して、アンケート調査票を送付した。
3 平成31年度「需要家側エネルギーリソースを活用したバーチャルパワープラント構築実証事業」に参画している事業者のうち、主にリソースアグリゲーター（RA）事業を担う17者に対してアンケート調査票を送付した。

【論点１】実態調査のフィードバックについて

- 調査から確認・分析できた組織的対策・技術的対策の実態については、事業者が自らのサイバーセキュリティ対策を向上させるために利活用できると考えられることから、**事業者に対しフィードバックすることが重要**と考えられる。この点、特に、現行制度上電力に特化したサイバー対策基準等が存在しない**小売電気事業者**（※）において効果的と考えられる。

  ※発電事業者は「電力制御システムセキュリティガイドライン」を遵守。
  ※ERAB実証において、実証事業者は「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」を遵守。

- このため、**小売電気事業者**、**学識者**等が参加し、小売電気事業者が確保すべきサイバーセキュリティ対策について検討する**勉強会**を開催し、**各質問項目に関連するサイバーリスクの解説**等（次頁参照）を行うことで、各事業者において、今回の実態調査の回答状況と当該解説を照らし合わせつつ、サイバーセキュリティ対策の見直しに役立てていくこととしてはどうか。

（参考）各質問項目に関連するサイバーリスクの解説のイメージ

- 実態調査では、合計145項目の調査を実施（一部の事業者のみが対象となる項目を含む）。
- 各質問項目に応じ想定されるリスク等を事業者に対し説明（下記一例）。

	質問項目の例	意図（想定されるサイバーリスク）
組織的対策	組織全体の対応方針がセキュリティポリシーとして策定され、経営責任者によって承認されている。	経営者が行うべき重要な役割の一つとして、サイバー攻撃によるリスク対処に係る方針を明確にすることがあげられる。これを行わない場合、**企業価値を高めるために IT を利活用したはずが、結果として、重大な損害を生じさせ、かえって企業の経営を揺るがす事態に発展する可能性**がある。
	自社の保有するシステム資産、サイバー脅威の最新動向等を踏まえたセキュリティリスクの評価を実施している。	リスクの大きさが、受容可能かまたは許容可能かを決定するために、リスク分析の結果を検討する。これを行わない場合、**対策にかかるコストが増大する可能性**や、**適切な対策が実施されない可能性**がある。
	インシデント発生時の緊急対応体制を構築している。	セキュリティ事故対応のための体制を作り、それぞれの責任範囲と役割を明確にし、組織内外への報告を含む手順を整理しておく。これらを行わない場合、**セキュリティ事故への対応が遅れ、損害が増大する可能性**がある。
技術的対策	ネットワークの境界では、必要最小限の通信のみを許可している。 （例：ファイアウォールの初期設定を拒否設定にし、必要な通信のみ許可設定している。）	ネットワークとの接続点に防護装置を設置し、必要な通信のみ通す設定をする。防護装置における不正な通信の監視を行う。これを行わない場合、**電力制御システム等への不正アクセスやマルウェアの侵入により、システムの不具合が生じる可能性**がある。
	外部からの不正な通信の検知・遮断のための対策を実装している。 （例：IDS/IPSを導入し、異常検知時にはアラート発報や通信遮断を行っている。）	許可された機器を管理し、許可されていない機器からの通信は遮断する。これを行わない場合、**なりすましや不正な機器を接続されることにより、他の機器や電力制御システム等の稼働に影響を与える可能性**がある。
	データの保存・転送を行うことが可能な端末にマルウェア対策を実装している。	データの授受を行う端末については、ウイルス対策ソフトを実装する等のマルウェア対策を実施することが望ましい。これを行わない場合、**マルウェア感染によりシステムの不具合が発生し、マルウェアの駆除に時間を要して電力制御システム等が長期にわたり利用できない可能性**がある。

出所）日本電気協会「電力制御システムセキュリティガイドライン」及び「サイバーセキュリティ経営ガイドライン」に基づき作成

２．系統連系に際し求める要件について

系統連系に際してサイバーセキュリティ対策を求める必要性

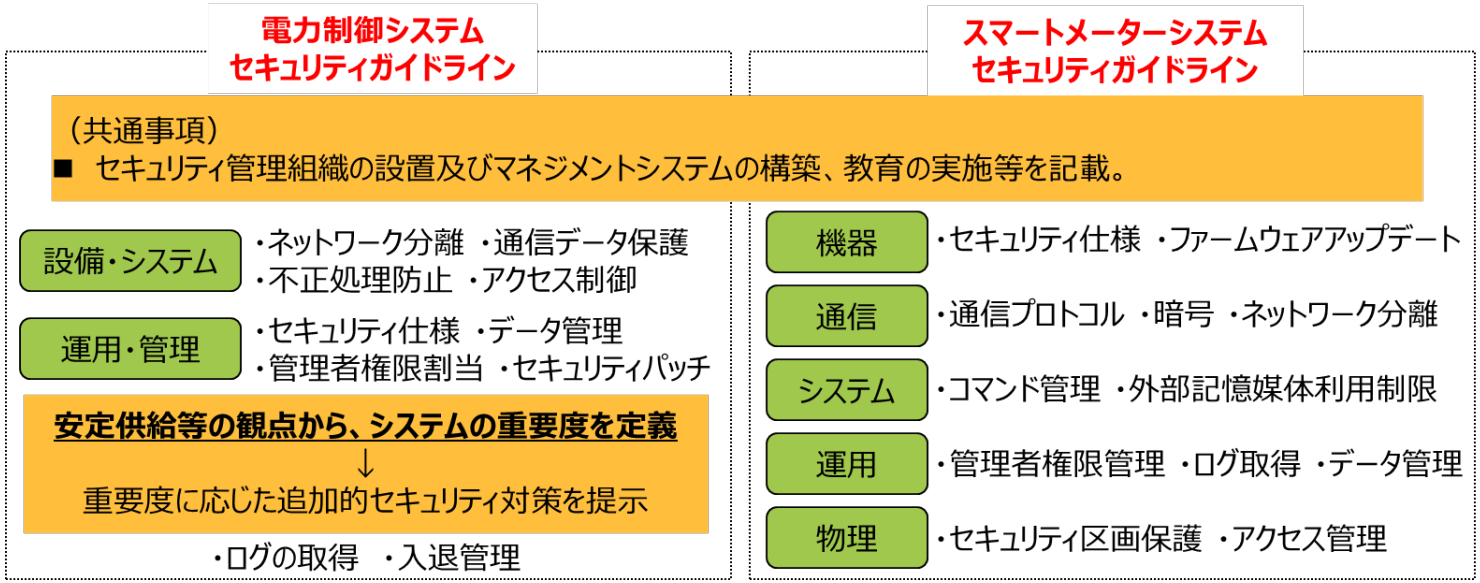
- 電気事業法に基づく電気設備に関する技術基準を定める省令第15条の2において、**一般送配電事業、送電事業、特定送配電事業及び発電事業の用に供する電気工作物の運転を管理する電子計算機**について、**サイバーセキュリティの確保**が規定されている。

  ※技術基準の解釈として、『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』を参照

- 一方で、**上記の定義に該当しない設備（小規模発電設備等）**（※）についても、サイバーセキュリティ対策は重要。今後、電源の分散化やオンライン制御の拡大を見据えれば、**サイバーリスクはより一層高まっていくと考えられる**。

  （※）接続最大電力の合計が1万kW未満の発電設備

- したがって、こうした**小規模発電設備等を含め、発電設備を系統に接続する際には、すべからく一定のセキュリティ対策を求めることが必要**と考えられる。



【論点２】系統連系に係る対策事項の基本的な考え方

- こうした観点から、**電力SWG**において、**サイバーセキュリティの専門家**や、**太陽光発電協会・日本風力発電協会等の事業者**の参画の下、発電設備を系統連系に際し求めるべき事項について御議論いただいた。
- 本小委員会においては、**電力SWGにおける専門家の検討結果を踏まえ、以下の内容について、大局的な観点からその方向性について御議論いただきたい**。
- サイバーセキュリティ対策においては、
  （１）サイバーインシデントの発生を防ぐ**事前防御**の観点
  （２）インシデント発生時の影響を最小化する**事後対応（早期発見、迅速な対処）**の観点
  の双方からの対策が必要。

（１）事前防御

- **（１）事前防御**の観点からは、再生可能エネルギー発電設備は現在はオフラインの設備が多いものの、今後、オンライン化の進展に伴い、多くが**インターネット接続型のシステム構成**になっていくことを見据えると（次頁参照）、こうした**ネットワークを通じた攻撃をいかに防ぐか**が重要となる。
- こうした観点からは、以下の対策が必要と考えられるのではないか。

  ① **ネットワーク接続点の保護**
  発電設備の制御を行うシステム（制御システム）とインターネットとを分離する等の措置により、外部からの不正侵入を防止し、また、他のネットワークでのインシデントが制御システムに伝播することを防止する。

  ② **データの保存・転送を行う機器・端末等のマルウェア対策**
  マルウェアの感染によりシステムに不具合が発生し、制御システムが利用できなくなることを防止する。

※オンライン制御に対応した再エネ発電設備については、技術仕様上、これらの要件に対応できるようになっている。

（参考）再生可能エネルギー発電設備の一般的なシステム構成

- 再エネ出力制御については、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いて、**出力制御のオンライン化**を通じた出力制御量の削減が重要との方針が示されている。
- 2020年3月末時点では、2018年秋から再エネ出力制御が実施されている九州において、事業用太陽光発電設備760万kWのうち、231万kW相当分がオンライン化。また、他エリアでも**再エネの導入状況に応じ順次オンライン化が進められている**。
- 再エネ発電設備のシステム類型は下表のとおり。オンライン方式のうち、**高圧以下はインターネット接続方式を適用**する方針。
- したがって、これらの設備に対するサイバー対策については、**今後のオンライン化の進展を見据え、ネットワークを介した攻撃を念頭に検討することが必要**。

ネットワーク接続による太陽光／風力発電システムの類型
（一般的な設備（逆潮流あり／出力制御機能あり）の場合）

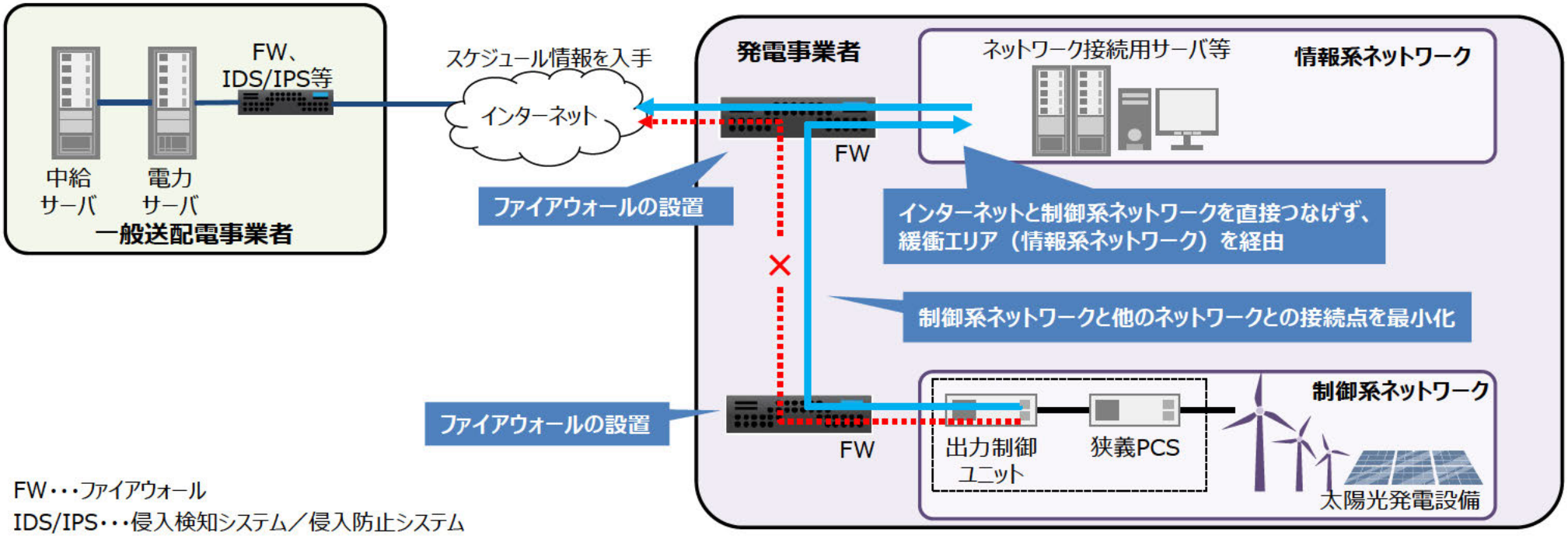
インターネット接続方式	インターネットを介して電力サーバから出力制御スケジュールを取得する方式。高圧以下の発電設備に対して適用する方針。
専用線接続方式	専用線を介して電力サーバから出力制御指令値を受信する方式。特別高圧の発電設備など系統への影響が大きい設備に対して適用する方針。
オフライン方式	固定スケジュールによって出力制御スケジュールを設定する方式、もしくは一般送配電事業者からメール等で指示されたスケジュールに基づき手動で設定する方式。ただし、遠隔監視等の出力制御以外の目的でインターネットに接続している可能性あり。

出所）第5回系統WG資料「出力制御機能付PCSの技術仕様について」及び
第17回系統WG資料「風力発電遠隔出力制御に係る技術仕様について（報告）」に基づき作成

（参考）ネットワーク接続点の保護

- 出力制御スケジュールの取得に際しては、一般送配電事業者がスケジュールをアップロードし、再エネ設備側がインターネットを介してこの情報を取得することとなっている。
- この際のウイルス感染等を回避するための対策として、**インターネットと制御系システムを直接接続しない（緩衝エリアを経由する）こと**が必要。
- また、ネットワーク接続点の保護のためには、①**他のネットワークとの接続点の最小化**、②**ファイアウォールの設置**等の対策も有効と考えられる。

※これらに加え、前頁②マルウェア対策として、セキュリティパッチの適用、外部記憶媒体のウイルスチェック等が必要。



FW･･･ファイアウォール
IDS/IPS･･･侵入検知システム／侵入防止システム

図の出所）第8回電力SWG資料を一部改変
※第5回系統WG資料「出力制御機能付PCSの技術仕様について」及び第17回系統WG資料「風力発電遠隔出力制御に係る技術仕様について（報告）」を参考に三菱総合研究所作成

（２）事後対応（早期発見、迅速な対処）

- **（２）事後対応（早期発見、迅速な対処）**の観点からは、設備設置者と系統運用者との間で迅速かつ的確な情報連絡を行い、速やかに必要な措置を講ずる必要がある。
- このため、設備設置者の負担を考慮した上で、系統運用者が適切な情報に基づいたインシデント対応を行えるようにするために最低限必要な事項として、**③「連系先系統運用者に対する、セキュリティ管理責任者の氏名及び緊急時連絡先の通知」**を求めるべきではないか。

【論点３】系統連系に係る対策事項の規定方法・施行時期

- 現在、系統に接続する全ての者が従うことになっている規定として、**一般送配電事業者の策定する「系統連系技術要件」（託送供給等約款別冊）**が存在。この系統連系技術要件は、策定及び変更にあたって**経済産業大臣の認可**を受ける必要があることから、系統連系に係る一連の規程の中で、**実効性及び手続の適正性を有するもの**と整理されている。
- したがって、論点２（１）、（２）で整理したサイバーセキュリティ対策について、**「系統連系技術要件」に追記することを一般送配電事業者に求めることとしてはどうか**。
- これらの対策は**速やかに対応を求めることが必要**。他方、系統接続の検討期間が原則3か月であることから、この周知期間にも配慮した上で、**2020年10月から実施を求めてはどうか**。（※）

（※）新たな系統連系技術要件は、新たに系統に連系する場合又は既存設備のリプレース等の場合に適用されることとなるが、少なくとも、③「連系先系統運用者に対する、セキュリティ管理責任者の氏名及び緊急時連絡先の通知」については、既に系統に連系しているものも含め、発電設備の設置者において、今般の系統連系技術要件の見直し後速やかに実施されることが望ましい。

また、システム改修を伴うこととなる①「ネットワーク接続点の保護」及び②「データの保存・転送を行う機器・端末等のマルウェア対策」については、既存設備のリプレース等のタイミングを活用して順次新たな対応を求めていくことが望ましい。

なお、新たな要件は、2020年10月以降に契約申込みを行うもの（電源接続案件募集プロセス対象の設備にあっては、2020年10月以降に入札を実施するもの）を対象に実施を求める。

＜参考＞電気事業法（抜粋）

（託送供給等約款）

第十八条　一般送配電事業者は、その供給区域における託送供給及び電力量調整供給（以下この条において「託送供給等」という。）に係る料金その他の供給条件について、経済産業省令で定めるところにより、託送供給等約款を定め、経済産業大臣の認可を受けなければならない。これを変更しようとするときも、同様とする。

２～１２　（略）