経済産業省

資料３

第１回の議論内容と第２回の論点等について

2018年９月４日

電力SWG事務局

１．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

２．電力SWGでの検討全体像（案）

３．第１回電力SWGにおける議論と第２回の論点

1．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

①攻撃先鋭化・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

②攻撃箇所の拡大
- IoT機器拡大、ネット接続機器は300億個へ（20年、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

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）

具体的攻撃事例

ウクライナ大停電(‘16)
・情報系システムから制御系まで不正侵入

ロンドン(‘12),リオ五輪(‘16)
・毎秒1万回以上の不正通信

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)

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

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

最悪の事態では、大規模電源や重要施設の電源脱落、広域・長期的なブラックアウト、といった可能性

目指す方向

①如何にサイバーインシデントを防ぎ（＝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か？（＝事後対応力の強化（早期発見、迅速な対処））

事業者の現在の主な取組

	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）
事前対策	➢ 組織；専門組織・管理責任者の設置、各対策の外部監査 ➢ 人材；セキュリティ教育、外部教育機関への人材派遣 ➢ 技術；マルウェア防止対策、通信ログ管理、不正処理検知 ➢ 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 ※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 ➢ 人材；事故時に対応する訓練の実施		

スマートメーター／オリパラ対策（東電）／G20対策（関電）／その他各社個別取組／ERAB事業者向けGLに記載された事項の取組

現在の主な政策

電力制御システムセキュリティGL(‘16~)
・制御系システムを持つ事業者に各対策を推奨・勧告(電技省令で義務化)

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)

スマートメーターシステムセキュリティGL(‘16~)
・スマメセキュリティ対策を推奨・勧告

オリパラ組織委、内閣官房オリパラ幹事会
・東電によるIOC基準を満たすオリパラ・電力供給対策の実装状況を確認

電力ISAC設立 (‘17~)
・サイバー情報の共有・分析組織

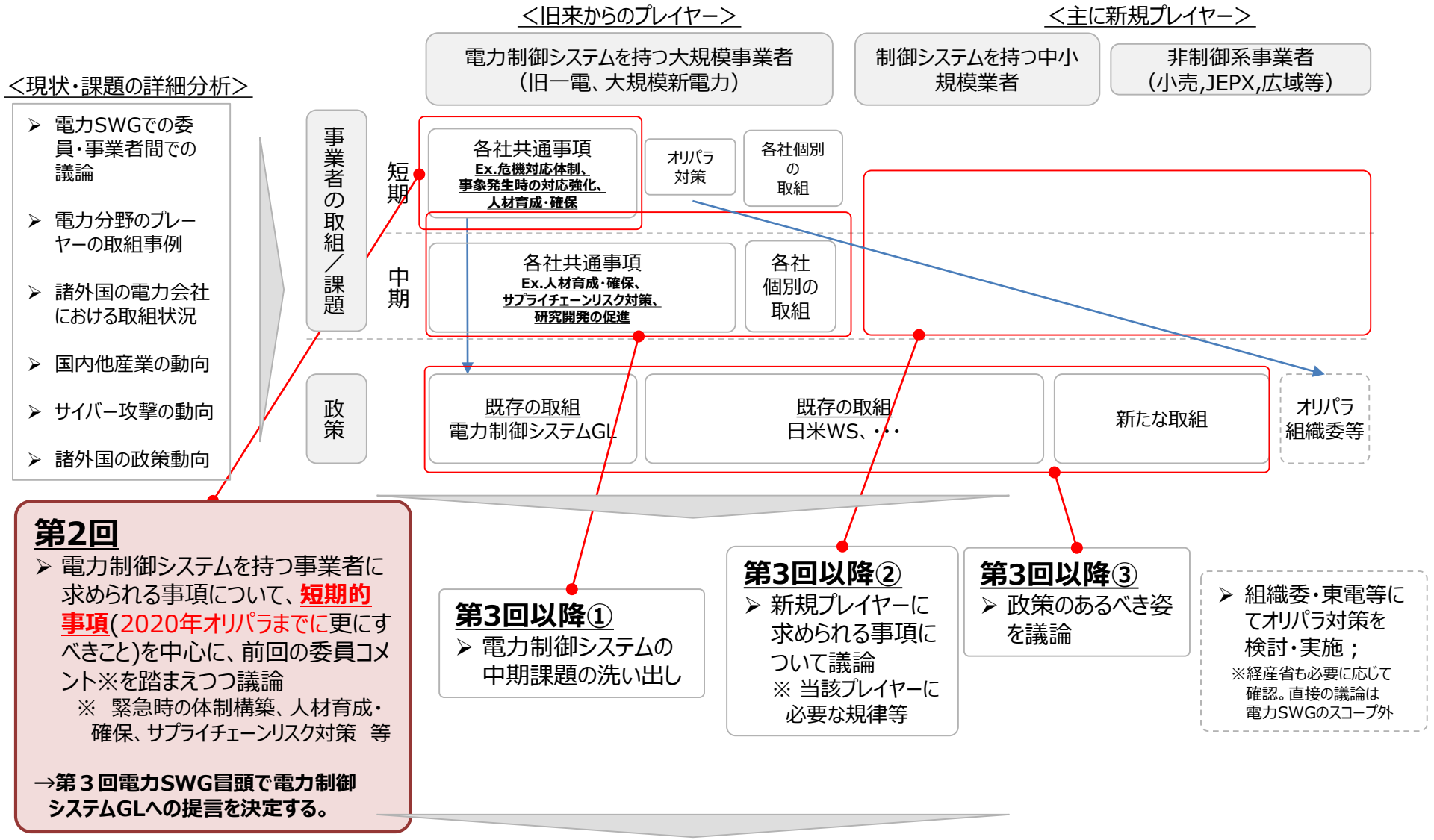
日米電力サイバーセキュリティWS(‘18~)
・日米の政府、電力、業界団体、研究機関、有識者が知見を共有

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

２．電力SWGでの検討全体像（案）

2．電力SWGでの検討全体像（案）



①如何にサイバーインシデントを防ぎ（＝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か？（＝事後対応力の強化（早期発見、迅速な対処））に向けて、幅広く議論し、政策への知見を得る

３．第１回電力SWGにおける議論と第２回の論点

３．第１回電力SWGにおける議論と第２回の論点

（１）危機管理体制の構築、人材の育成・確保

現状・課題

・サイバーインシデントの一般的な特徴として、事象レベルの見極めを誤り、初動が遅れると被害が拡大する点が挙げられる。
サイバー攻撃を受けた際には定められたセキュリティ管理体制の下、情報共有を密接に行い、必要に応じて、危機管理体制を迅速に構築することが重要である。
担当部署のみで対応しているうちに事態が深刻化し、対策本部を立ち上げたときには手遅れになっているという状況は避けなければならない。

・一般的に、停電の原因がサイバー攻撃かどうかの判断は難しく、制御システムを使用する社員が機器故障と判断してしまう可能性がある。サイバーインシデントの可能性を疑い、迅速に危機管理体制を構築するためには、電力制御システムを使用する社員の感覚や判断力の強化が必要である。
また、インシデントに係る担当部署からの情報を適切に収集・評価かつ対応し、経営層に的確に報告し判断を求める戦略マネジメント層（サイバー事案の翻訳者）の役割が重要になる。

・セキュリティ人材はどの業界でも必要とされ不足していることもあり、人材の流動が激しい。
優秀な人材を育成し、社内に定着させる必要がある。

論点①　電力制御システムを使用する社員の感覚や判断力を強化するにはどうすれば良いか。

→　電力制御システムの利用者への社内外の教育・演習の機会を通じて、サイバーインシデントのパターンや発生時の対応を体得するのはどうか。

　現場で制御システムの日常運用に携わる社員が、サイバーインシデントの知識を得られる教育・演習をするのはどうか。

論点②　経営方針に基づくセキュリティ戦略の検討やインシデント対応における中核を担い、経営層との橋渡し役にもなる、「戦略マネジメント層」をどのように育成するか。

→　戦略マネジメント層の候補として、経験が豊富なベテラン社員やセキュリティ対応要員として育成される社員が期待される。

　育成にあたっては、社内でのセキュリティ教育・訓練に加えて、ICS-CoEのような社外の育成プログラムや情報処理安全確保支援士等の資格制度も有用であり、活用してはどうか。

論点③　上記人材を活かし、早期に態勢を確立するためにどのような社内管理体制とするべきか。

→　サイバー攻撃による電力制御システムの不具合が疑われる事象について、当初は被害が小さくても、今後被害の拡大が予想される場合に備え、危機管理体制とリンクさせられるような役割や手順を予め定めておくのはどうか。その際、戦略マネジメント層には、経営層への報告にあたり、情報収集・分析や対策検討、技術面での解説時の中核を担うといった役割が期待される。

論点④　育成された戦略マネジメント層が社内に定着し、活躍するためにはどうするか。

→　個々の事業者における状況を踏まえ、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のはどうか。キャリアパスが存在することで、セキュリティ人材のモチベーション向上や、効率的かつ効果的な人材育成が可能になるものと期待される。

3．第１回電力SWGにおける議論と第２回電力SWGの論点

（２）事象発生時の対応強化

現状・課題

サイバー攻撃によりセキュリティ事象が発生する可能性があることを予め想定し、事象の検知から対応までを迅速かつ適切に行うことで、攻撃を無効化したり、被害を極小化する取り組みが重要である。

論点⑤　危機管理広報の充実や危機管理体制の実効性向上にはどのような取り組みが有効か。

→　サイバーインシデント発生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。また、社内での演習だけでなく、例えば地域に設置されているセキュリティ連絡会等の組織での活動機会を活用し、自治体や警察、消防、地域内の重要インフラ事業者と合同での演習が実施できると、さらに大きな効果が期待できる。
これは、利用者への広報のみならず、地域の企業・自治体等との間での情報共有が重要となるためである。

また、これらの演習は、使用するリスクシナリオの作成過程が人材育成の場になるとともに、最終的な判断を行う経営層への意識付け、理解促進にもつながるものと期待される。

論点⑥　サイバーセキュリティに関して地域の重要インフラ企業や自治体等との連携を強化するにはどうすればよいか。

→　地域の重要インフラ企業や自治体等のセキュリティ担当者間でface-to-faceの関係を構築したり、ICS-CoE修了生のネットワークを活用するのはどうか。地域の重要インフラ企業や自治体等の間のネットワーク強化、サイバーレジリエンス強化につながるものと期待される。

３．第１回電力SWGにおける議論と第２回電力SWGの論点

（３）サプライチェーンリスク対策

現状・課題

・サプライチェーンリスクへの対応状況は業界ごとに状況が異なるので、電力業界はどこまで対策するかという線引きが必要。電力会社は様々な取引先から電力制御システムに関する機器やサービスを調達しており、サプライチェーンといっても幅広い。適切に優先順位を付けないと混乱をきたす恐れがある。産業分野全体での検討状況を踏まえつつ、コストの観点や日本の電力分野のサプライチェーンの特徴を考慮し、バランスのとれた対応を行うことが必要である。

・納品物に対してトレーサビリティがとれておらず問題が発生した際に解明まで長期間を要する場合がある。直接取引しているサプライヤーについては程度把握できるが、間接的な取引については困難な場合もある。

論点⑦　電力事業者におけるサプライチェーンマネジメントをどのように行うか

→　公益事業者としての責務である電力の安定供給を確保するため、電力制御システムにおけるメーカーや委託先等との役割を明確にし、機器等のセキュリティ仕様を把握しておくとともに、事案が発生した場合は速やかに対処できるよう連絡体制を構築するのはどうか。