経済産業省

産業構造審議会　保安分科会
電力安全小委員会（第１３回）資料6

サイバーセキュリティ対策の保安規制への取り込みについて

平成２８年７月１３日

商務流通保安グループ
電　力　安　全　課

１．経緯

- 近年、サイバー攻撃等の脅威が高まっていることを踏まえ、平成25年度の委託事業以降、サイバーセキュリティ対策について、産業構造審議会保安分科会電力安全小委員会（以下、電力安全小委員会）等で議論を行ってきたところ。

【 これまでのトピックス 】

平成25年度	委託事業（平成25年度次世代電力システムに関する電力保安調査）にて、サイバー攻撃のリスクの洗い出し及び必要な安全確保策の検討を実施
平成26年度	委託事業（平成26年度電気施設技術基準国際化調査（電気設備））にて、アメリカの電力システムにおけるサイバーセキュリティー対策の実態調査を実施
平成27年6月	電力安全小委員会（第10回）にて、電気事業法における保安規制に、サイバーセキュリティ対策を組み入れるべきとの結論が得られる。
平成27年度	委託事業（平成27年度電気施設保安制度等検討調査（電気設備技術基準国際化調査））にて、EU・イギリス・ドイツの電力システムにおけるサイバーセキュリティー対策の実態調査を実施
平成27年7月	資源エネルギー庁に設置されたスマートメーター制度検討会セキュリティ検討WGの報告書にて、ガイドライン策定要件等がとりまとめられる。→スマートメーターシステムセキュリティガイドラインへ反映。
平成28年3月	第85回日本電気技術規格委員会（以下、ＪＥＳＣ）本委員会にて、スマートメーターシステムセキュリティガイドライン策定。
平成28年5月	第86回ＪＥＳＣ本委員会にて、電力制御システムセキュリティガイドライン策定。

2．経済産業省の取り組み①（電力制御システムの耐性評価）

- 経済産業省は、**電力制御システム**について委託事業を活用して、**耐性調査を実施。**
- その結果、現在の事業環境における**セキュリティ対策**については、**一定の評価を確認。**

事業名：平成25年度次世代電力システムに関する電力保安調査
委託先　：　株式会社日本総合研究所
委員長　：　新　誠一(電気通信大学)
事業期間：平成25年10月～平成26年2月（委員会は5回開催）

＜H25年度委託調査＞

○アンケート（10社）及びヒアリング（3社）を通じて、現状の電力の取組を評価。
- **セキュリティポリシー**は、**電気事業連合会ガイドライン**※に則って、会社全体及び部門ごとに策定・構築。
  （※政府の「重要インフラの情報セキュリティ対策に係る行動計画」に基づき、電事連で自主ガイドラインを作成。一般電気事業者各社が、外部接続の限定等、自主的に取組を実施。）
- **対策や思想**は、外部接続点を限定した**クローズドなネットワーク構成、物理的隔離と入退所管理、記録媒体の持込制限、下請等の要員管理**などを実施。
- **接続管理**（侵入防御）は、**ファイアーウォール**等による**通信経路・方向の限定**、リモートメンテナンス回線の極小化、接続先の認証かつ必要時のみ外部接続などを実施。
- **教育**は、**サイバーセキュリティ演習**（主催：CSSC、電中研）等を通じた対処練度の向上、社員に対する**定期的な意識啓発**を実施。

○これらの取組により、これまで運転制御に影響のあるセキュリティインシデ ントは発生しておらず、**“現状のセキュリティ対策としては一定の評価ができる”**

○今後の事業環境変化を踏まえた**“提言事項”**
1. **マネジメントシステムの確立**
2. **外部接続点の対策徹底**
3. **業界横断的な情報共有**
4. **セキュリティ人材の訓練・育成**
5. **電力自由化を見据えたサイバーセキュリティガイドラインの策定等**

＜追補調査＞

○平成25年度委託調査のヒアリング項目＋αを電力11社にアンケート調査。
○有識者（IPA、JPCERT、CSSC）による評価の結果、
- **現システム**は、**出来うる可能な対策は行われており、一定以上の耐性がある**と言える。
- 巧妙化している脅威の動向や事業環境・システム環境の変化を考慮して、**PDCAサイクルの仕組みを整備・充実化**していくことが望ましい。

３．経済産業省の取り組み②（欧米の電力システム調査）

- 平成26、27年度、欧米の電力システムにおけるサイバーセキュリティーに係る制度や対策の実態を調査。
- 各国において、そのアプローチ(規制のみ（独）、電力会社の自主性の尊重（英）、それらの組み合わせ（米））に違いあり。
- 日本としては、米国型アプローチをベースに、規制により一定のセキュリティを確保した上で、事業者の自主的な更なる取り組みを促していく方向。

◘ 調査対象

【平成26年度：アメリカ】
サイバーセキュリティガイドライン作成・運用機関、政府関連機関、監督官庁、電力会社
【平成27年度：EU、イギリス、ドイツ】
EU関係機関、政府関係機関、電力会社、電気工作物のベンダー

◘ 調査結果

【アメリカ】
・セキュリティ対策は、電力の安定供給の確保が主目的。
・「遵守義務のある規制」＋「経営リスクに応じたリスクベースアプローチ」の併用。
【イギリス、ドイツ】
・セキュリティ対策は、プライバシー保護が主目的。スマートメーターシステムへの適用が先行。
・イギリスは、「リスクベースアプローチ」のみ。ドイツは、「規制」のみ（2018年適用予定）。

◘ 調査結果を踏まえ日本がとるべきアプローチ

①アメリカのアプローチを参考にして、規制によりベースラインを確保しつつ、インセンティブ等により企業のセキュリティ文化を形成。
②「自主保安」の思想の下、電力会社が、自ら第三者によるガイドライン適合に関する監査を定期的に実施。
③官民が協力し、インシデント、ベストプラクティス等の情報共有や分析機能を強化。

４．経済産業省の取り組み③（民間ガイドラインの法令への位置づけ）

● 第10回電力安全小委員会（平成27年6月26日）での審議を踏まえ、民間団体において策定されたサイバーセキュリティ対策に関する２つのガイドライン（スマートメータ、制御系）を、技術基準（ハード対策）及び保安規程（マネジメント等ソフト対策）に位置付け（電気事業法の省令に根拠規定を追加した上で、当該ガイドラインをエンドース）。

＜スマートメータシステム　セキュリティガイドライン＞

・平成27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。

・平成28年3月　第85回JESC委員会にてガイドライン策定。

＜電力システム（制御系）セキュリティガイドライン＞

・平成26年9月　日本電気技術規格委員会（JESC）で検討開始。

・平成27年6月　同委員会情報専門部会を新たに設置。

・平成28年5月　第86回JESC委員会にてガイドライン策

（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

↓

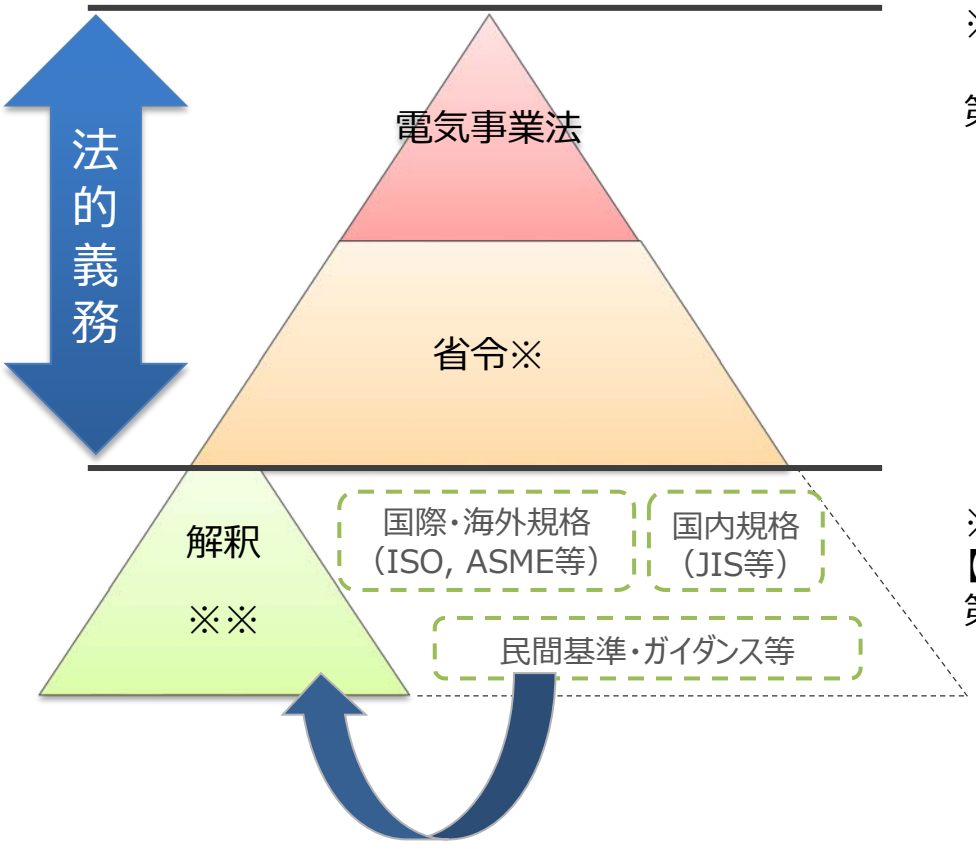
重要度に応じた追加的セキュリティ対策を提示

・ログの取得　・入退管理

【スケジュール】　現在、パブリックコメント中
平成28年8月　公布・施行

（参考）技術基準への位置づけ

- 電気事業法第３９条により、事業者に省令で定める技術基準への適合維持を義務づけ。
- 技術基準省令へサイバーセキュリティの確保を要求。
- 技術基準省令に適合する基本的な仕様規定である解釈にＪＥＳＣガイドラインを位置づけ。
  (十分な保安水準の確保が達成できる技術的根拠があれば、解釈の記載内容に限定されるものではない)



ＪＥＳＣ規格を解釈で引用。
（省令に適合するものであることの明確化）

※省令条文案
（サイバーセキュリティの確保）
第十五条の二　電気工作物（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ものに限る。）の運転を管理する電子計算機は、当該電気工作物が人体に危害を及ぼし、若しくは物件に損傷を与えるおそれがないよう、又は一般送配電事業に係る電気の供給に著しい支障を及ぼすおそれがないよう、サイバーセキュリティ（サイバーセキュリティ基本法（平成二十六年法律第百四号）第二条に規定するサイバーセキュリティをいう。）を確保しなければならない。

※※解釈条文案
【サイバーセキュリティの確保】（省令第１５条の２）
第３６条の２　省令第１５条の２に規定するサイバーセキュリティの確保は、次の各号によること。
一　スマートメーターシステムにおいては、日本電気技術規格委員会規格　ＪＥＳＣ　Ｚ０００３（２０１６）「スマートメーターシステムセキュリティガイドライン」によること。
二　電力制御システムにおいては、日本電気技術規格委員会規格　ＪＥＳＣ　Ｚ０００４（２０１６）「電力制御システムセキュリティガイドライン」によること。