資料12

（報告）電力システムへのサイバーセキュリティ対策（概要）について

平成26年3月10日
商務流通保安グループ
電力安全課

電力システムへのサイバーセキュリティ対策は、電気設備自然災害等WGにおいて、委託事業の検討結果を報告し、必要に応じ対応策を検討することとされた。平成26年2月末に委託調査の結果報告があったため、概要を報告する。

1. 背景及び検討内容

(1)背景

○電力システムは、現状、クローズドな制御系ネットワークにて制御・運用されているものの、今後はIT技術の高度化等に伴い、外部の通信ネットワークとの相互接続機会が増加すると見込まれる。
○他方、サイバー攻撃の手法についても、複雑・巧妙化してきており、セキュリティリスクが上昇している。
○また、政府「サイバーセキュリティ戦略」(平成25年6月情報セキュリティ会議)でも、甚大化するリスクの一つとして、電力システムへのサイバー攻撃による大規模停電が挙げられており、適切な対策が求められている。

○このため、サイバー攻撃による電気設備の事故等の未然防止等に資するため、平成25年度の委託事業で、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行った。

(2)検討内容と体制

○委託事業(※)では、電力システムやサイバーセキュリティの有識者による委員会を開催。次の観点から検討。
(1)現状の電力システムにおけるサイバーセキュリティ対策
(2)将来の電力システムにおけるセキュリティリスク
(3)諸外国におけるサイバーセキュリティ対策の状況
(4)他産業におけるサイバーセキュリティ対策の状況
(5)今後の電力システムにおけるセキュリティ確保策の在り方

※委託事業について

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　誠一教授(電気通信大学)
委員	:電気事業者・メーカー・情報通信事業者・研究機関等から10名
事業期間	:平成25年10月～平成26年2月(委員会は5回開催)

2. 現状の電力システムにおけるセキュリティ対策と将来におけるリスク

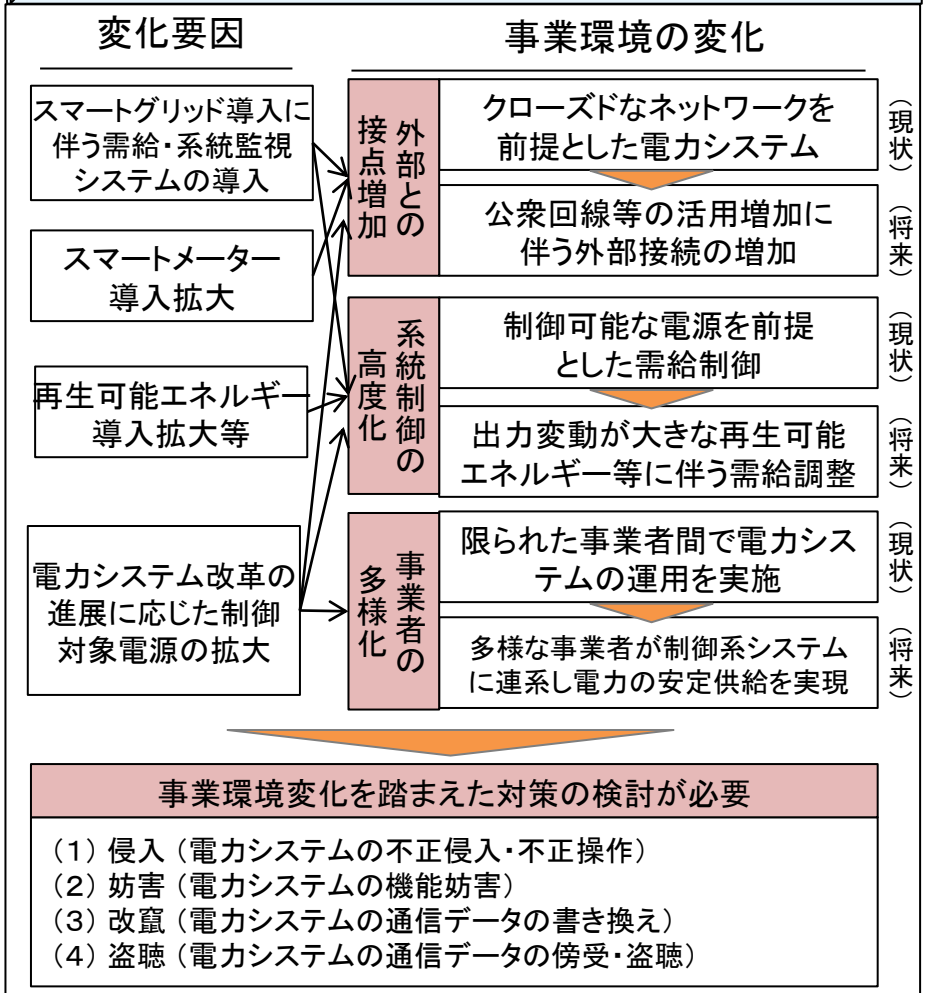
〇現状の事業環境におけるサイバーセキュリティ対策について、一般電気事業者各社へのヒアリング及びアンケートによる詳細調査を実施。調査結果の分析によると、現状の対策は一定の評価ができる。
〇ただし、今後の事業環境変化を踏まえた対策の検討が必要。

現状の一般電気事業者のセキュリティ対策（概要）

ポリシー	● 電気事業連合会のガイドラインに則って、各社が社内ポリシー又は部門ポリシーを策定・運用 ● スマートメーター等についてはNIST（米国国立技術研究所）等のガイドラインを参考に対策を実施・検討
対策/思想	● 原則、外部との接続点を限定したクローズドなネットワークを構成
物理(人)的対策	● 物理的隔離と侵入防御（守衛等による入退所管理も含む。） ● 記録媒体の持ち込み制限 ● 点検や修理に関わる事業者の要員の管理
接続管理	● ファイア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 ● 接続先を認証して必要時のみ外部接続する運用
教育/演習	● 電力中央研究所や制御システムセキュリティセンターが主催するサイバーセキュリティ演習への参加 ● サイバーセキュリティに対する定期的な意識啓発を実施

⇨ これまでのところ、電力の安定供給に影響を与えたサイバーセキュリティインシデントは発生しておらず、<u>現状の事業環境におけるサイバーセキュリティ対策として、一定の評価ができる。</u>

今後の事業環境の変化



3. 電力システムにおけるサイバーセキュリティ対策の在り方

電力システムにおける現状と課題

・これまで電力の安定供給に影響を与えたサイバーセキュリティインシデントは発生しておらず、現状の事業環境における対策としては一定の評価ができる。
・今後は事業環境変化を踏まえた対策の検討が必要。

米国の対策例

・事業者はセキュリティ対策に関するガイドライン（CIP※）の遵守状況をFERC（連邦エネルギー規制委員会）に提出。

他産業の対策例

・（通信）業界横断的な対策
・（金融）内部・出口対策の強化
・（プラント）外部からの侵入を前提とした対策の強化。マネジメントシステムの第三者認証。

提言（概要）

①マネジメントシステムの確立

〇リスクを考慮したマネジメントシステムの確立
・リスクアナリシス
・電力設備・機器（スマートメーター含む）の調達・廃棄における対策　等

②外部接続点の対策徹底

〇外部ネットワークとの接続点における対策
・不正な通信の監視・検知
・侵入防御の多段構成等の対策　等

③業界横断的な情報共有

〇他分野（情報通信事業者等）の情報セキュリティ関係者との情報共有の強化（共通脅威の分析等）

④セキュリティ人材の訓練・育成

〇経営課題としてのサイバーセキュリティ対策の重要性の啓発
〇導入、運用及びインシデント発生時、適切に対応できるセキュリティ人材の訓練・育成等

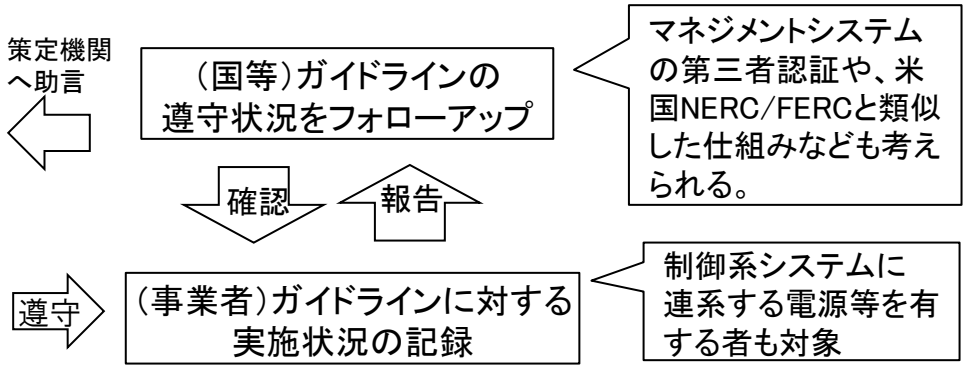
⑤電力分野のサイバーセキュリティガイドラインの策定等

〇事業環境の変化も踏まえたガイドライン（日本版CIP※）の策定

■ガイドラインで規定する項目（案）（①～④を考慮して策定）

項目	概要
行動計画	セキュリティに関する行動計画を策定・実施
リスクアナリシス	リスクアナリシスを通じた重要資産の特定
対策立案	資産の重要度に応じたセキュリティ対策の立案
個別対策	電力システムの物理的保護
	電子的な接続点の保護
	サプライチェーンリスクの留意
人材育成	セキュリティ対策に資する人材育成・教育計画
危機管理	サイバーインシデントへの対応手順

〇セキュリティ対策の実効性を高めるための検討



※CIP：NERC（北米電力信頼度協会）が作成するガイドライン（Cyber-security Critical Infrastructure Protection）

（参考）諸外国・他産業のサイバーセキュリティ対策の現状

1．米国の例

〇米国では、NERC（北米電力信頼度協会）がサイバーセキュリティ対策に関するガイドライン（CIP）を策定。
　CIPでは、システムの重要度別にセキュリティ要件とその確認方法が具体的かつ定量的に規定。
〇事業者はCIPの遵守状況についてFERC（連邦エネルギー規制委員会）に提出し、FERCが評価。

諸外国でのサイバーインシデントの事例

施設	国	時期	被害内容	原因
ウラン濃縮施設	イラン	2010年	ウラン濃縮施設の遠心分離機が全て停止	マルウェア（Stuxnet）のコンピューター感染
スマートメーター	米国	2009年	電力消費量記録の改竄	インターネットで入手可能なソフトによる改竄
制御システム	米国	2007年	制御システムにアクセス可能なPCのアクセス権限が不正取得	Windows脆弱性

※米国で報告されたサイバーインシデントのうちエネルギー関連事業は41.4%（米国DHS－CERT(2011年10月1日～2012年9月30日）

CIPにおける標準例と概要

（CIPver.5は2014改定予定で10の標準が存在）

標準	概要
CIP002-5	リスクベースのアプローチによって重要資産を特定し、これに基づき重要サイバー資産を定める。
CIP003-5	最小限のセキュリティ管理を確立して重要サイバー資産を保護するためのセキュリティに関する行動計画を策定・実施する。
CIP004-5	重要サイバー資産へのアクセスを電子的・物理的に許可された人員に対して、必要なトレーニングを施し、セキュリティ意識を啓発する。

2．他産業における取り組み例

〇情報通信：電力システムにおける公衆回線活用機会の増加を見据え、送信元ブラックリスト等の情報共有、
　　電力と情報通信が参加する演習の共同開催など、業界横断的な取り組みの充実化の検討
〇金融　　：内部への侵入を前提とした内部対策、及び出口対策の強化
　　（マルウェア対策ソフトの高度化、データベースアクセス監視、不審な通信の検知等）
〇プラント産業：外部からの侵入・感染を前提とした対策の強化（侵入後に重要なシステムまでは到達を許さない多段構成、侵入検知システム、ホワイトリスト方式（※）の導入等）
　　制御システムのセキュリティマネジメントシステムに関し第三者認証の試験的事業を開始

示唆

※事前に認証されたプログラムのみ動作する方式

〇外部接続点を極小化するクローズドなネットワーク構成を前提としつつも、
　外部からの侵入はあり得るという想定に立った、二重三重の多層的な対策を実施することが重要。