経済産業省

資料7-1

電力・ガス分野における
サイバーセキュリティ対策

2017年7月7日

資源エネルギー庁

背景・問題意識

- 技術の発達やデジタル化の進展により、あらゆる分野でサイバー攻撃の脅威が高まる中、電力・ガス分野においても、サイバーセキュリティ対策の重要性がこれまで以上に高まっている。
- 加えて、電力システム改革の進展により、コスト低減のための汎用技術の採用やシステムに接続する事業者の増加・多様化が進みつつある中、こうした情勢変化がサイバー攻撃のリスクが増大する可能性が高いことから、電力・ガス分野全体のサイバーセキュリティを高める取組が求められている。
- このため、昨年来、電力・ガス分野では、サイバーセキュリティ対策の法令上の義務付けや、送配電事業者や大規模発電事業者によるサイバーセキュリティ水準向上のための体制整備、サイバーセキュリティ人材の育成等に取り組んできた。
- 電力・ガス分野においても、サイバーセキュリティ対策に「完璧」はなく、不断の見直し・向上のための取組が官民ともに必要不可欠であることを踏まえつつ、本日は、最近の電力・ガス分野における取組について報告すると共に、今後目指していくべき方向性について御議論いただく。

電力分野の今後のサイバーセキュリティ対策

スマートメーター

ガイドライン<ベースライン>
・スマートメーター制度検討会セキュリティ検討ワーキンググループ報告書
→スマートメーターシステムセキュリティガイドライン（JESC）
→保安規制に取り込み

マネジメント<PDCAの継続促進>
・業界統一の監査制度を構築、内部監査・外部監査を実施済み
・ペネトレーションテスト（各社実施済み）

情報共有体制
<脆弱性・対策の相互参照>
・脆弱性情報共有・分析体制を電力ISACへ移行（電力10社）

制御系

ガイドライン<ベースライン>
・電力制御システムセキュリティガイドライン（JESC）
→保安規制に取り込み
・10社＋発電事業者が対象

マネジメント<PDCAの継続促進>
・ガイドラインに基づく、対策の自己点検
・有識者を交えた、対策や自己評価等を含む各事業者の取組の客観的レビュー

情報共有体制
<脆弱性・対策の相互参照>
・脆弱性情報共有・分析体制（ISAC）を構築
（10社・大規模発電・広域等）
・外部有識者レビューの場として活用
→ベストプラクティスの共有

広域機関システムのセキュリティ
※電力会社は広域システムを介して連係

・ペネトレーションテスト（IPA）
・セキュリティ監査・第2GSOCへの参加

情報系

会員事業者の情報セキュリティ
・新規参入者向けガイドラインの作成
・普及啓発・セキュリティ情報提供等

各社セキュリティ意識の向上・継続

経営層の関与

国際・業界間協力

G７エネルギー大臣会合サイバーセキュリティWS

各国ISACや電力会社等との国際連携

他分野ISACとの連携

【参考】昨今のサイバー攻撃①　社会インフラを狙ったサイバー攻撃の増加と政府の取組み

- 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、インフラの安定的な運用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。
- 政府は国連やOECD、APEC等で開催される国際会議や、重要インフラ防護やインシデント情報の共有等に関する専門的な多国間・二国間会合に参加し、多くの国々や民間団体と、サイバーセキュリティの確保に向けた方策の検討を行っている。

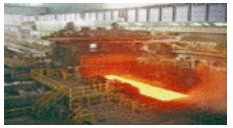
＜最近のサイバー攻撃の事例＞

電車システムへの攻撃（ポーランド、2008年）

14歳の少年がテレビのリモコンを改造して路面電車システムに侵入し、4車両を脱線させた。

製鉄所の溶鉱炉損傷（ドイツ、2014年）

何者かが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。



ロンドン五輪への攻撃（イギリス、2012年）

毎秒約１万件の不正通信。開会式会場の電力システムへの攻撃情報。手動に切り替え。

変電所へのサイバー攻撃（ウクライナ、2015年）

マルウェアの感染により、変電所が遠隔制御された結果、数万世帯で3～6時間にわたる大停電が発生。

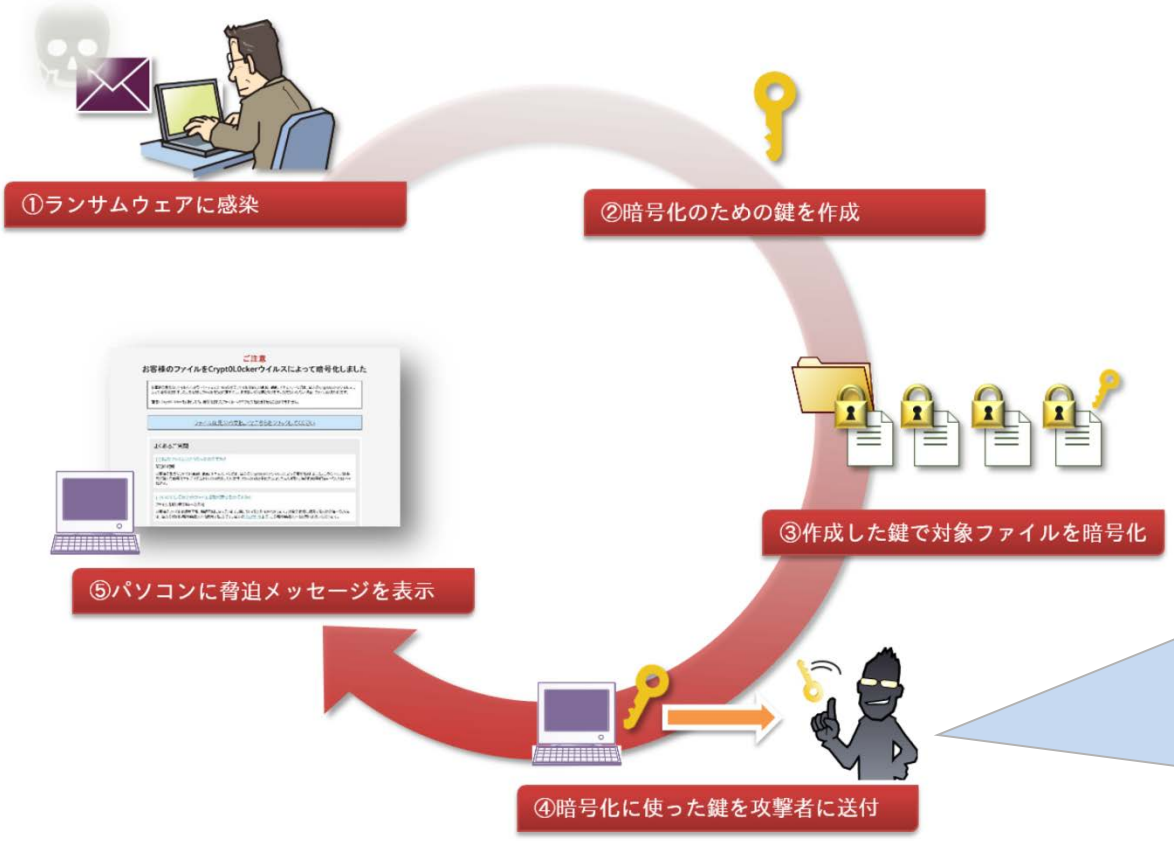
ランサムウェア”WannaCry”（世界約150ヶ国、2017年）

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、本年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。

【参考】昨今のサイバー攻撃②　ランサムウェア”WannaCry”について

- 本年5月12日頃から、世界の少なくとも約150か国において、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。
- これまでのところ、電力・ガス事業に影響を与える被害は確認されていない。



ランサムウェアのファイル暗号化の動作概要

※1　本脆弱性の修正プログラムは、本年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。

（出典）IPA　ウェブサイトより転載

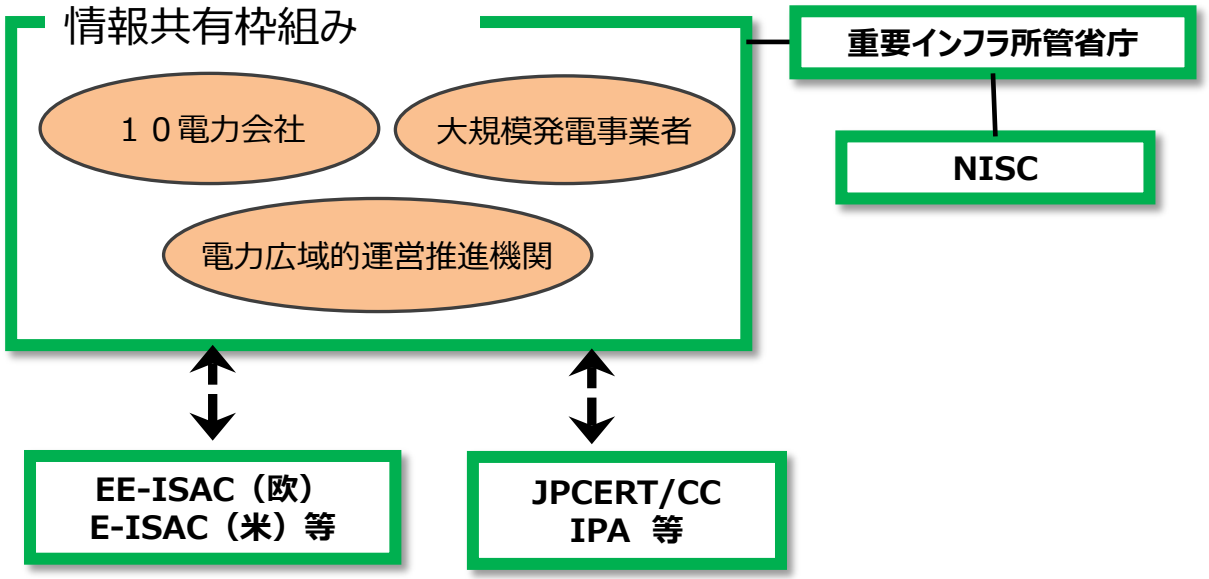
電力分野の最近の取組①　電力ISACの設立（民間事業者）

- 金融や通信等の他の重要インフラ分野の取組を踏まえ、業界大のサイバーセキュリティ対策強化を目的に、**本年３月に電力ISAC（※１）が設立**された。
- 電気の安定供給の役割を担う事業者間で、サイバーセキュリティに関する情報の収集・分析や各社のベストプラクティスに係る情報共有を行っている。
- 本年５月には電力ISACとEE-ISACの間でMOU（※２）が締結され、海外との連携体制も構築されつつある。

※１：ISAC：Information Sharing and Analysis Center

※２：MOU：Memorandum Of Understanding（友好関係構築を目的とした覚書）

＜情報共有体制＞



電力分野の最近の取組②　セキュリティガイドラインの電事法への組込み

- 電力分野のサイバーセキュリティ対策強化に向けて、2016年3月にスマートメーターシステムセキュリティガイドライン、2016年5月に電力制御システムセキュリティガイドラインを日本電気技術規格委員会（JESC）が策定。
- これらのガイドラインを、電気事業法下の技術基準と保安規程にそれぞれ組み込んだことにより、ハード・ソフト両面の対策の実効性を担保している。

＜スマートメータシステムセキュリティガイドライン＞

・２０１５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。
・**２０１６年３月**
　第８５回ＪＥＳＣ委員会にてガイドライン策定。

＜電力制御システムセキュリティガイドライン＞

・２０１４年９月
　日本電気技術規格委員会（ＪＥＳＣ）で検討開始。
・２０１５年６月
　同委員会情報専門部会を新たに設置。
・**２０１６年５月**
　第８６回ＪＥＳＣ委員会にてガイドライン策定。

（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

電力分野の最近の取組③：ガイドラインに基づく監査の実施（スマートメーター）

- 2015年度、2016年度において、スマートメーターシステムセキュリティガイドラインに基づき、各電力会社はスマートメーターシステムのセキュリティ対策に関する内部監査を実施。各社とも重大な指摘事項は無く、前年度の指摘事項については改善が確認されている。
- 加えて、2016年度には、新たな取組として、各電力会社において外部監査を実施。各社とも重大な指摘事項は無かった。
- 外部監査を通じて得られた要望事項等を踏まえ、より効率的・実効的な監査制度となるよう改善を図る方針。

2015年度の結果（内部監査）

○初年度のため、全項目を監査する必要があり、かつ、スマートメーターシステムの運用開始と時期が重なったため、負担感が大きかった。

○事業部門（情報システム部門）が主となって監査を行った会社もあった。

2016年度の結果（内部監査／外部監査）

○内部監査については、2015年度に指摘があった事項については改善が確認された。

○外部監査の実施に当たっては、監査企業の選定等、監査前の準備に期間を要した。

○外部監査において、2016年度の内部監査の手続や実施方法等について一部助言事項があったが、重大な指摘事項はなかった。

今後の対応方針

○外部監査をとおして、内部監査に係る改善提言の妥当性の確保、及び監査品質の向上をはかる。

○外部監査では、監査標準手続の記載内容の改善（内容の明確化、わかりやすさ）、及び監査人の要件に関する現実的な運用を検討する。

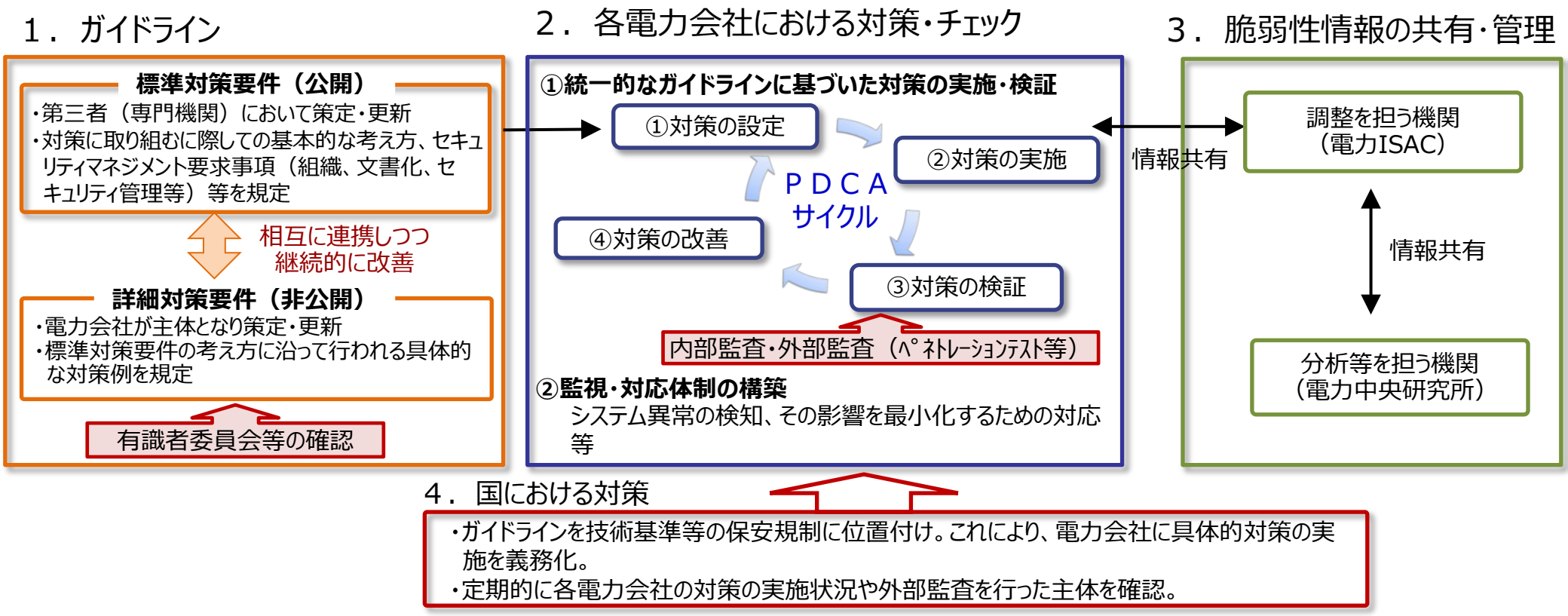
（参考）スマートメーターシステムのセキュリティ対策　（対策の枠組み）

1．**ガイドラインの策定**・継続的改善。

2．各電力会社において、ガイドラインに基づいた**対策の実施・検証**（**ペネトレーションテストを含む外部専門家による監査**等）、監視・対応体制の構築。

3．電力会社間における**脆弱性関連情報の共有・分析体制**の構築。

4．国において、ガイドラインを技術基準等の**保安規制に位置付け**、電力会社に具体的対策の実施を義務化。あわせて、定期的に各電力会社の対策の実施状況や外部監査を行った主体を確認。



（参考）スマートメーターシステムのセキュリティ確保に向けた電力会社の取組

	社内規定の整備	監査の実施			体制の構築		追加的な取組
		内部監査※	外部監査	ﾍﾟﾈﾄﾚｰｼｮﾝﾃｽﾄ（注）	セキュリティ運用・管理体制	システム監視・対応体制	
北海道	整備済（2016年3月）	実施済（2017年2月）	実施済（2017年3月）	実施済（2016年3月）	構築済（2016年3月）	構築済（2016年3月）	教育・訓練を定期的に実施
東北	整備済（2016年3月）	実施済（2016年12月）	実施済（2017年3月）	実施済（2016年3月）	構築済（2016年3月）	構築済（2016年3月）	教育を定期的に実施
東京	整備済（2015年7月）（2016年12月改定）	実施済(2017年3月)	実施済（2017年3月）	実施済（2015年1月、2016年3月）	構築済（2015年7月）	構築済（2015年7月）	・ｽﾏｰﾄﾒｰﾀｰｵﾍﾟﾚｰｼｮﾝｾﾝﾀｰ運用開始（24時間体制、2015年7月） ・有識者委員会の下、脅威分析、リスク評価を実施済（2016年7月） ・訓練を実施（1回以上／半期） ・教育を実施（1回／年）
中部	整備済（2016年3月、2014年10月に一部整備済）	実施済（2017年1月）	実施済（2017年3月）	実施済（2014年11月、2015年5月）	構築済（2014年10月。2015年11月全社大体制）	構築済（2014年10月）	ｽﾏｰﾄﾒｰﾀｰ制御管理ｾﾝﾀｰを設置（24時間監視、社外人材活用） 訓練・教育を年１回以上実施
北陸	整備済（2016年3月改定）	実施済(2016年11月)	実施済（2017年3月）	実施済(2016年3月)	構築済（2016年3月改定）	構築済（2016年2月改定）	訓練・教育を定期的に実施
関西	整備済（2016年2月改定）	実施済（2016年10月）	実施済（2017年1月）	実施済（2016年3月）	構築済（2012年6月）	構築済（2012年6月）	訓練・教育を定期的に実施
中国	整備済（2016年3月）	実施済（2016年12月）	実施済（2017年3月）	実施済（2016年3月）	構築済（2016年3月）	構築済（2016年3月）	訓練・教育を適宜実施
四国	整備済（2016年3月）	実施済（2016年12月）	実施済（2017年2月）	実施済（2016年3月）	構築済（2016年3月）	構築済（2016年3月）	訓練・教育等を定期的に実施
九州	整備済（2016年1月）	実施済（2016年11月）	実施済（2017年2月）	実施済（2016年2月）	構築済（2016年2月）	構築済（2016年2月）	訓練・教育を定期的に実施
沖縄	整備済（2016年3月）	実施済（2016年11月）	実施済（2017年3月）	実施済（2016年3月）	構築済（2016年3月）	構築済（2016年3月）	教育を適宜実施。

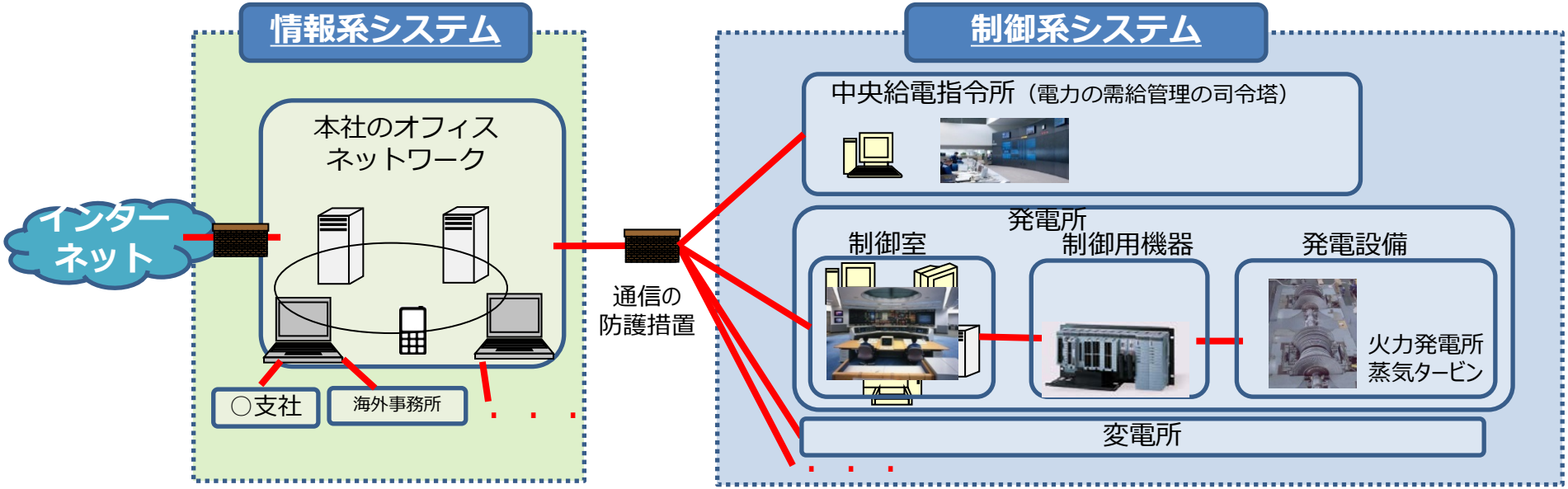
※2015年度にも実施しているが、2016年度の実施について記載

（注）システムに対する疑似的攻撃による評価、記載時期以降も各社適宜実施

電力分野の最近の取組④　制御系システムに関する取組

- 制御系システムは、情報系システムに比べ、①外部との直接の接続が少なく、②事業者毎に固有の仕様部分が多いため、従来、詳細な内部仕様等を把握できない限り、外部からの攻撃が困難だったが、標準技術・汎用製品利用の増加や外部ネットワークへの接続などにより、外部からのサイバー攻撃の可能性は増しており、攻撃の脅威が存在することを前提とした対策が必要とされている。
- 現在、各事業者は、電力制御システムセキュリティガイドラインに基づき、自社内の取組として制御系システムのセキュリティ対策を実施しているが、自らの取組を客観的に評価する機会を得ることも重要。
- このため、各事業者において、引き続き、ガイドラインに基づく対策や、当該対策について自ら評価を行うとともに、今般設立された**電力ISACにおいて、外部有識者も交えてこれらを含む各事業者の取組を客観的にレビューする場を設け、得られた有意義な知見を可能な範囲で共有**することで、業界としてのセキュリティ対策の向上を図っていく。

＜情報系・制御系システムの模式図（電力分野の例）＞



電力分野の最近の取組⑤　広域機関を中心とした電力分野全体の取組

- 電力広域的運営推進機関（広域機関）は、自らのシステムについてのセキュリティ向上の取組に加え、 電力ISAC等から収集した情報を会員事業者（小売・小規模発電事業者）へ提供すると共に、事業者のセキュリティ水準向上のための啓発活動をこれまでに実施。

①広域機関自身の取組

業務規程にて、広域機関の所有するシステムについてのサイバーセキュリティ対策を講じることとし、昨年度までに外部監査、ペネトレテスト等を実施するなどのサイバーセキュリティ対策を実施。

②情報提供

業務規程にて、会員事業者への情報提供を広域機関のミッションとするとともに、送配電等業務指針にて会員事業者の情報セキュリティ向上を義務化。

また、電力ISAC等から収集した情報を会員事業者に対して展開。

③情報セキュリティ対策ベンチマークの実施

会員事業者の対策レベルの把握により、今後のセキュリティ対策へ活用する目的と、各社への啓発の趣旨で、本年３月～６月で調査を実施（現在回答受付中）

評価項目（全４９項目）

情報セキュリティ対策（３０問）

- 組織的な取組み
- 物理的（環境的）施策
- 通信・システムの運用管理
- アクセス制御、開発・保守
- 事故対応状況
- 電力広域的運営推進機関クライアント証明書の管理状況
- 電力広域的運営推進機関に関するシステムにアクセスするユーザIDの管理状況
- 電力事業で共同利用する個人情報の管理状況

事業内容等（１９項目）

- 従業員数、売上高、拠点数
- 重要情報の保有数、IT依存度等

電力分野の最近の取組⑥ G7エネルギー大臣会合サイバーセキュリティWS

- G7エネルギー大臣会合の準備会合付属会合として、本年６月、エネルギー分野（特に電力分野）におけるサイバーセキュリティ対策の強化をテーマに、各国エネルギー事業者、セキュリティ事業者、政府関係者、国際機関等によるワークショップを開催。
- エネルギー（電力）のサイバーセキュリティに関する各地域・国際機関の取組を互いに紹介しつつ、国際的な協力のあり方について議論。

＜主な認識共有事項＞

○制御系システムはサイバー攻撃を受けても停止することが許されないため、情報系システムとはサイバーセキュリティ対策のアプローチが異なるものであるとともに、一定の取組の結果（product）で許容されるものではなく、継続的な取組過程（process）が重要。

○電力分野では、デジタル化やIOT技術の導入が加速化する一方でサイバー攻撃が複雑化しており、電力分野のサイバーセキュリティ対策には政策立案者・規制者・実務者による多国間の官民協力が必要。

○サイバーセキュリティ対策水準の向上には情報共有が重要だが、情報共有の活発化には、共有相手との信頼構築が必須。

＜今後に向けて＞

○各国の関係者の連携と情報共有の活性化のため、**官民の関係者を交えたビデオカンファレンスを実施**。

（参考） 産業分野のサイバーセキュリティ強化のための海外連携

- 電力・ガスを含む産業分野のサイバーセキュリティ強化に向けて、各国との間で各種の会議を設け、情報共有等を実施。各国との協力関係を構築している。

No.	会議名称	日程	開催地	内容
２０１６年				
1	日イスラエルサイバー協議	6月21日(火)-23日(木)	テルアビブ	・重要インフラのセキュリティ確保等の重要性や、各種の取組（サイバー空間のクリーンアップ等）を共有。
2	日米サイバー対話	1月20日(水)	ワシントンD.C.	・各種の取組（電力システム関連の取組、サイバー空間のクリーンアップの取組）を共有。
3	日豪サイバー協議	8月2日(火)	東京	・日ASEANによる取組（重要インフラ防護ガイドライン策定やサイバー演習等）を共有。
4	日独サイバー協議	9月9日(金)	東京	・各種の取組（日本における電力制御システムセキュリティガイドラインの策定や法令への組み込み等）を共有。
5	日英サイバー協議	10月12日(水)	東京	同上
6	第9回 日・ASEAN情報セキュリティ政策会議	10月20日(木), 21日(金)	東京	・各種の取組（HIDAとJPCERTを通じた対ASEAN人材育成協力等）を共有。
7	日韓サイバー協議	10月27日(木)OR28日(金)	ソウル	・各種の取組（日本における電力制御システムセキュリティガイドラインの策定や法令への組み込み等）を共有。
8	日露サイバー協議	11月10日(木)OR11日(金)	モスクワ	N.A.
9	日ウクライナサイバー協議	12月19日(月)（P）	ウクライナ	N.A.
２０１７年				
10	日仏サイバー協議	1月23日(月)	パリ	・各種の取組（日本における電力制御システムセキュリティガイドラインの策定や法令への組み込み等）を共有。
11	日EUサイバー協議	1月25日(水)	ブリュッセル	・日ASEANによる取組（重要インフラ護ガイドライン策定やサイバー演習等）を共有。
12	日エストニアサイバー協議	1月26日(木)	タリン	・各種の取組（IPA・産業サイバーセキュリティセンターにおけるサイバー人材育成の取組等）を共有。
13	日中韓サイバー協議	2月10日（金）	東京	・日ASEANによる取組（重要インフラ防護ガイドライン策定やサイバー演習等）を共有。

電力・ガス分野の最近の取組　サイバーセキュリティ対策を担う人材の育成

- 本年4月、独立行政法人情報処理推進機構（IPA）に産業サイバーセキュリティセンター(ICSCoE)を設置。今後、電力、ガス、鉄鋼、石油、鉄道、放送、通信等の各業界60社以上から約80名の研修生を受け入れ（電力・ガス分野からは合わせて20名程度参加）、実践的な演習・対策立案等のトレーニングを行う予定。
- 情報共有体制の強化など重要インフラ政策を実装させるには、重要インフラ事業者自身の能力強化が不可欠。センターは、各業界における中核人材の育成やリスク評価の実施等を進めることにより、「国民が安全で安心して暮らせる社会の実現」に貢献していく。

①模擬プラントを用いた対策立案（人材育成）

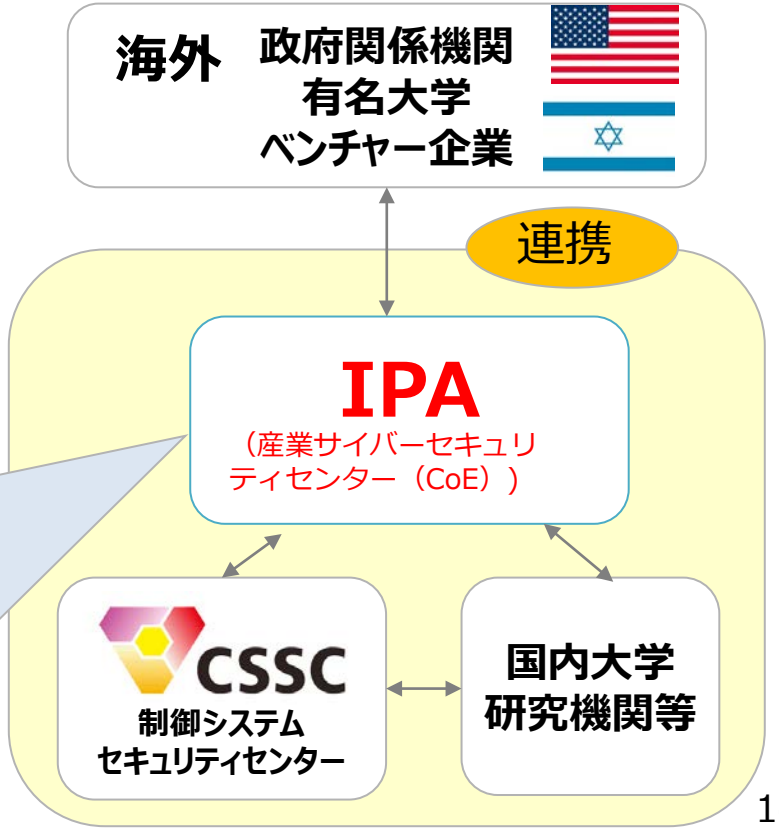
- 情報系システムから制御系システムまでを想定した模擬プラントを設置。専門家とともに安全性・信頼性の検証や早期復旧の演習を行う。
- 海外との連携も積極的に実施。

②実際の制御システムの安全性・信頼性検証等

- ユーザーからの依頼に基づき、実際の制御システムやIoT機器の安全性・信頼性を検証。
- あらゆる攻撃可能性を検証し、必要な対策立案を行う。

③攻撃情報の調査・分析

- おとりシステムの観察や民間専門機関が持つ攻撃情報を収集。新たな攻撃手法等を調査・分析。



電力分野のサイバーセキュリティ対策強化に向けた取組

- 電力・ガス分野においても、サイバーセキュリティ対策に「完璧」はなく、不断の見直し・向上のための取組が官民ともに必要不可欠。
- 電力システム改革の進展に伴い、新たに参入する事業者（小売電気事業者や小規模発電事業者等）が増加する一方、新たなエネルギーリソース（ネガワット等）の導入が拡大していくことを見据え、更なるサイバーセキュリティ対策の強化が求められている。
- 同時に、我が国の電力・ガス産業のみに留まらず、広く有益な知見を得ながら全体のセキュリティ水準を向上していくため、国内の他分野、あるいは海外との連携をより一層深めていくことが重要。

①新規参入者増大に伴う情報セキュリティ対策の検討

・自由化の先行する海外諸国では、自由化の進展に伴いサイバー攻撃の事例が増加している。
・我が国においても、全面自由化へ移行し、今後さらなる事業者の新規参入が見込まれることに加え、事業者の形態の多様化により、情報通信への依存度は更に高まることが予想される。
・こうした状況変化を踏まえ、これまでの広域機関の取組を発展させ、新規参入者向けのガイドラインの策定等により、一層の強化を図っていく。

②国内他分野、海外との連携

・サイバーセキュリティ対策には、情報の共有が必須であり、共有の枠組を広げていくことは、セキュリティ対策の水準向上において非常に重要。
・我が国では、電力に先行して、情報通信や金融分野でＩＳＡＣの枠組が構築されているほか、その他の分野でも検討が行われており、電力業界においては、これらの他分野とＩＳＡＣ間の連携を強化し、電力ＩＳＡＣを中心とした情報交換等を密にしていく。
・また、Ｇ７エネルギー大臣会合サイバーセキュリティＷＳの枠組や、電力ＩＳＡＣが推進する海外ＩＳＡＣとの連携により、海外の知見も取り入れ、我が国の電力分野のサイバーセキュリティ水準をさらに高めていく。

ガス分野のサイバーセキュリティ対策

- ガス分野のサイバーセキュリティ対策については、主に、①方針・体制の構築、 ②情報共有、③演習（訓練）、④人材育成、の観点から、（一社）日本ガス協会（JGA）が業界の窓口として中心となり、内閣サイバーセキュリティセンター（NISC）や情報処理推進機構（IPA）等と連携し、それらの枠組みへの参加等を通じて日々対策をとっている。
- 今後は、ガス事業者の各取組へのさらなる参加促進、新規のガス小売事業者や製造事業者等も含めた情報共有の拡充等を図る。

PLAN
（方針/体制構築）

- 「製造・供給に係る制御系システムのセキュリティ対策ガイドライン」の改訂（JGA策定）
- 「都市ガス製造・供給システムのサイバーセキュリティ対策に関する調査事業」の実施（経済産業省委託調査）

当該ガイドラインに基づき、主要なガス事業者は社内規程を策定・改訂し、情報セキュリティ対策を講じている。

課題の抽出・整理を行い、提言を行った。

DO
（情報収集/共有）

- ① IPA; J-CSIPへの参加
- ② NISC; C4TAPへの参加
- ③ JPCERT/CC; 早期警戒情報の共有

2016年度より参加対象を拡充し、従来の11組織（セプター10事業者＋JGA）から新たに15事業者が加わり、計25のガス事業者が参加した。

CHECK・ACT
（確認/演習）

- ① NISC; 分野横断的演習（サイバー攻撃発生時の対応訓練）
- ② NISC; セプター訓練（NISC-省庁-セプター間の連絡訓練）
- ③ NISC;リスク評価の取組への参加（2020年東京オリンピック・パラリンピック競技大会に向けた取組）
- ④ CSSC; サイバー演習（模擬製造プラントを用いた訓練）
- ⑤ JGA; インシデントハンドリング訓練の実施（ガスに特化したサイバー攻撃発生時の対応訓練）

2016年度より参加対象を拡充し、ガスセプター10事業者の演習参加に加え、14事業者が見学参加した。

人材育成

- IPA; 産業サイバーセキュリティセンターの人材育成プログラムへの参加

長期・短期プログラム共にガス事業者からも参加した。

（参考）都市ガス製造・供給システムのサイバーセキュリティ対策に関する調査事業の概要

事業名：平成２７年度都市ガス製造・供給システムのサイバーセキュリティ対策に関する調査事業
委託先：ブレインワークス（株）
委員長：新　誠一（電気通信大学教授）
事業期間：　平成２７年１１月～平成２８年３月

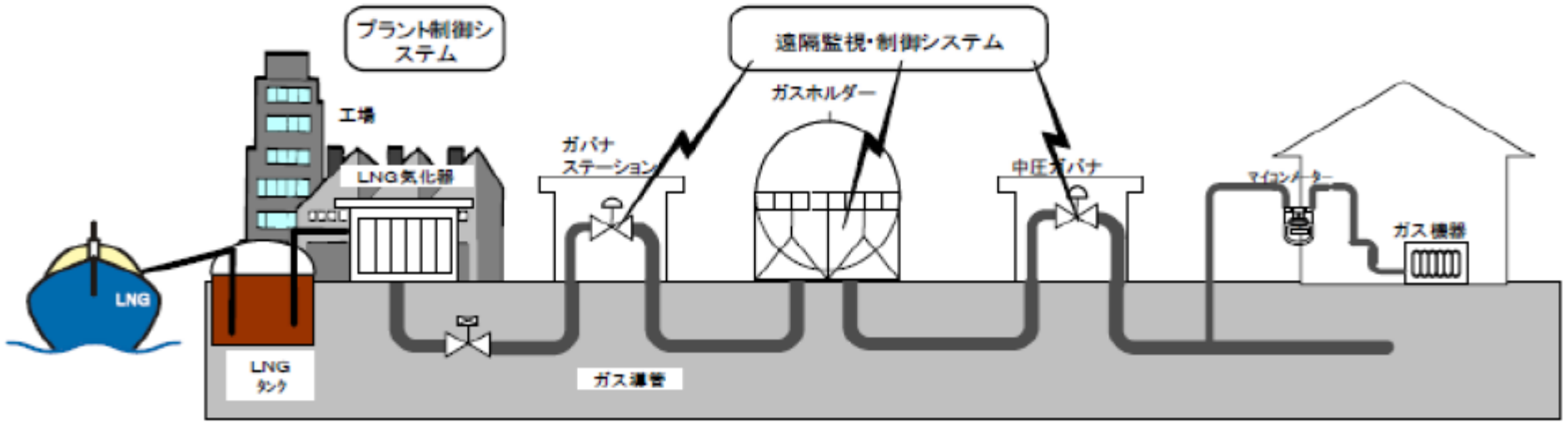
●「都市ガス製造・供給システムのサイバーセキュリティ対策に関する調査事業」を委託事業として実施し、都市ガス製造・供給システムにおけるサイバーセキュリティ対策現状を把握し、改良すべき課題の抽出・整理を行い、所要の提言事項を示した。

●本調査により得られた課題事項
①組織体制の高度化
②情報セキュリティポリシー等の整備・管理
③事業リスクを設定したリスクアセスメントの実施
④外部記録媒体の使用の極小化・管理の徹底
⑤制御システムにおけるホワイトリスト等の導入、多層防御化等
⑥サイバーセキュリティに係る教育の充実等
⑦外部接続の極小化、対策徹底等
を踏まえた対応の充実を期待

●本調査の内容を踏まえ、日本ガス協会では、「製造・供給に係る制御系システムのセキュリティ対策ガイドライン」の内容を見直し行い、2016年7月に改定を実施。
●正会員に通知するとともに地方説明会を開催し、新ガイドラインの業界内への展開は実施済み。
●「製造・供給に係る制御系システムのセキュリティ対策ガイドライン」に基づき、主要ガス事業者（１０社）は社内規程を定め、情報セキュリティ対策を講じている。また、その他のガス事業者も、それぞれの事業形態や情報システムの形態に応じた情報セキュリティ対策を実施。

（参考）都市ガス製造・供給システムの概要

- 都市ガスの製造、供給に係る制御システムは、インターネットとは分離した構成とすることを基本としており、インターネット経由の攻撃を困難なものとしている。
- 供給系統のガスホルダーや導管の内部にガスが保有されていることから、仮に、サイバー攻撃などにより製造が停止する事態に陥ったとしても、直ちに供給支障には至らない。
- 供給系統の圧力調整機能は機械式構造であり、仮に遠隔制御ができなくなっても、一定の圧力調整機能は保持される。



①プラント制御システム（製造系）
ガスの製造（原料の気化、熱量調整、付臭等）のために圧力・流量の制御及び監視を行う

②遠隔監視・制御システム（供給系）
供給ライン圧力・流量の監視や遠隔遮断弁・ガバナ（圧力調整器）等の制御を行う