資料６－２

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報告書

2016 年 3 月

株式会社ブレインワークス

目次

1　調査背景及び目的

今日のように様々な社会インフラが情報ネットワークに常時接続されている状況では、日本年金機構の情報漏えい事案のようなシステムの脆弱性等を狙うサイバー攻撃が発生しており、また、海外においてウラン濃縮施設に係る事例（2010 年 11 月、4-1 にて後述）のように、インターネットに接続されない制御システム[1]へのサイバー攻撃も現実のものとなりつつある。これらのリスクの重要性に鑑みて政府として「サイバーセキュリティ戦略」（2015 年 9 月閣議決定）が取りまとめられた。

また、2015 年 6 月に公布された電気事業法等の一部を改正する等の法律（平成 27 年法律第 47 号）により、ガス事業法の一部改正が行われ、「ガスシステム改革」として都市ガス事業における小売全面自由化（2017 年度に施行予定）等を行うことになった。これに伴い、ガス事業における事業類型の整理が図られ、保安規制の在り方にも大きな影響を及ぼすことが予想されるため、新たな視点で保安規制の在り方について検討する必要がある。

こうした状況下、本調査事業では、都市ガスの製造・供給システムへのサイバー攻撃のリスクへの対応状況や、ガスシステム改革に伴う新たなサイバーセキュリティ対策等の調査、分析、検討を行うことで、ガス設備の事故等の未然防止等に役立たせるとともに都市ガスの安定供給の確保策の検討に参考となることを目的としたものである。

本調査事業では、都市ガス事業の業態を勘案して、都市ガス供給の大半を占める主要事業者について調査を行うこととし、「第３次重要インフラの情報セキュリティ対策に係る行動計画」により設けた GAS CEPTOAR を構成する 10 事業者を対象として実施した。

こうした前提のもと、都市ガスの製造・供給システムにおけるサイバーセキュリティ対策に関する調査、分析、検討として、次の内容を行った。

イ　都市ガスの製造・供給システムの現状及びサイバーセキュリティ対策の現状の調査

都市ガスの製造・供給システムの基本的な構成及び運用・制御の考え方についての現状を調査し、また、実装されているサイバーセキュリティ対策の現状を調査した。

ロ　都市ガスの製造・供給システムに対するサイバー攻撃等リスクに係る調査

制御システムに対するサイバー攻撃等の過去の事例を調査し、想定されるサイバー攻撃等のリスク、シナリオを分析し、課題の整理を行った。また、海外のガイドラインについても調査した。

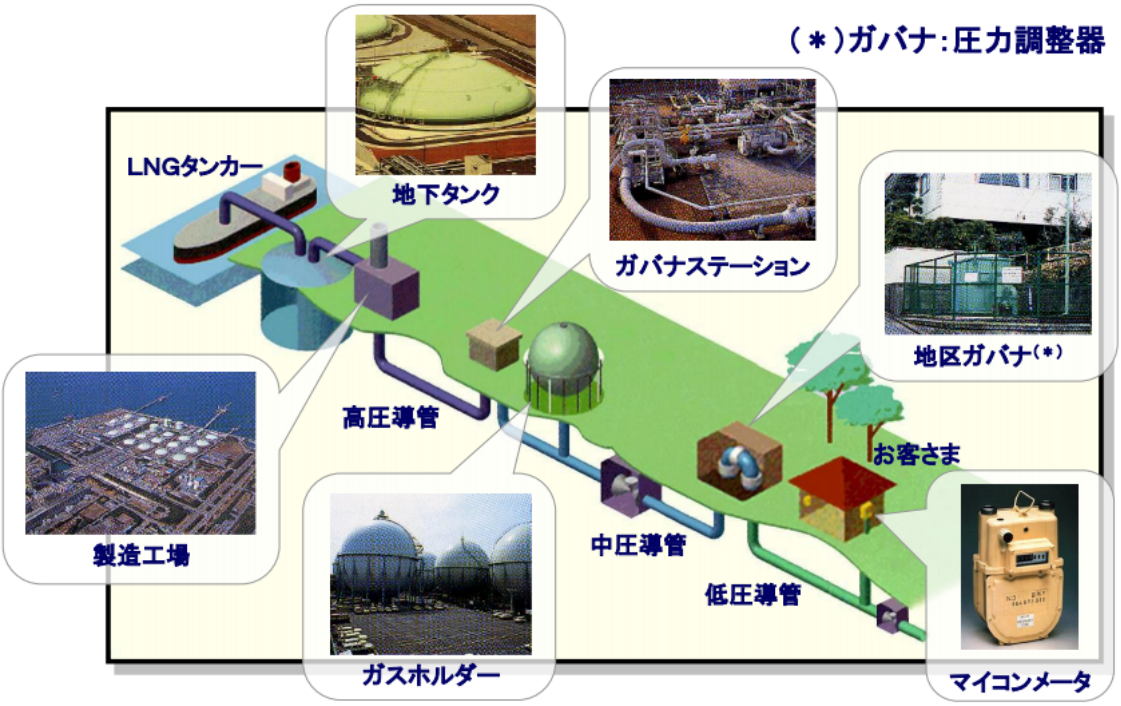
[1] 制御システムとは、機器やシステムを管理し制御するための機器、あるいは機器群のことを指す

ハ　ガスシステム改革後の想定される都市ガスの製造・供給システムの将来像の調査

電気事業法等の一部を改正する等の法律第５条による改正後のガス事業法（以下「改正ガス事業法」という。）施行後の都市ガス市場における小売全面自由化などを踏まえた都市ガスの製造・供給システムの将来像を調査、分析、検討し、将来像の想定を行った。

都市ガスの製造・供給システムに関するインフラの全体像は下図のように示される。

図表 1-1　都市ガスのインフラ概念図



（出典：一般社団法人日本ガス協会　都市ガス業界における制御系システムのセキュリティ対策強化のための活動紹介）

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。本書内では、製造システムと呼ぶ。
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。本書内では、供給システムと呼ぶ。
本書内では、両システムをあわせて、製造・供給システムと呼ぶ。

また、都市ガスの製造・供給システムに影響を与える環境変化として以下が挙げられる。

(1) 社会インフラ関連施設に対するサイバー攻撃

従来のサイバー攻撃はインターネットを介して官庁や企業を狙ったものが多かったが、ネットワークがサイバー攻撃を受けて溶鉱炉の制御システムが乗っ取られたドイツの製鉄所のケース（2014 年、4-1 にて後述）のように、最近は特に海外で公共の社会インフラ関連施設への攻撃ケースが発生している。電力・ガス・上下水道等の市民社会に密着した生活インフラ、港湾・空港・鉄道等の公共設備及び産業設備関連のインフラが攻撃されれば、その影響は大きい。

(2) ガスシステム改革

「ガスシステム改革」の目的は、新しいサービスやビジネスの創出、競争の活性化による料金抑制、ガス供給インフラの整備・拡充、競争原理導入による合理的な料金、消費者利益の保護であるが、それには保安の確保が前提となる。

2017 年内に実施予定の都市ガス事業における小売全面自由化によって、既存のエネルギー企業が様々なエネルギー供給サービスを行う「総合エネルギー企業」となり、ガス小売事業の新規参入による競争の活性化が期待されている。そこで、エネルギー供給サービスの相互参入や、新規の小売参入に伴う、製造・供給システムに与える影響を考える必要がある。

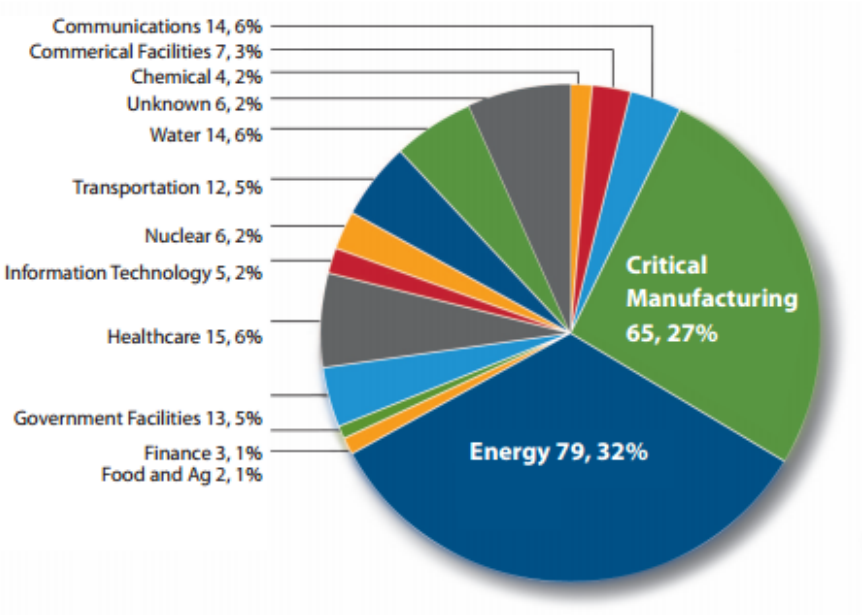
2　海外における重要インフラのサイバーセキュリティへの取り組み

本章では、都市ガスの製造・供給を担う制御システムに対するサイバー攻撃等のリスクを検討する参考情報として、海外における重要インフラへのサイバー攻撃の現状、攻撃への取り組み状況、およびガイドラインについて調査した。

2-1　重要インフラへのサイバー攻撃の現状

2015 年 3 月にアメリカ国土安全保障省（Department of Homeland Security：DHS）の産業制御システムセキュリティ機関である Industrial Control Systems Cyber Emergency Response Team（ICS-CERT）が明らかにしたところによると、アメリカ国内の重要な社会インフラへのサイバー攻撃は 2014 年の 1 年間で 245 件に達しており、攻撃対象産業の筆頭はエネルギー分野の 33%、次いで重要工業分野の 26%であった。

図表 2-1　アメリカ国内の重要な社会インフラへのサイバー攻撃



出典　ICS-CERT Monitor September 2014 - February 2015 (ICS-MM201502)

また、トレンドマイクロ社が 2013 年 3 月～6 月にわたり実施した制御システムへのサイ

バー攻撃のおとり調査では、期間中に合計 74 件のサイバー攻撃が確認されている。この調査で確認された 74 件中 10 件の攻撃は、温度出力や水ポンプ圧の改変、水ポンプシステム停止といったインフラシステムに対して深刻なダメージを引き起こすものであった。この調査では、水道局システムに見立てたハニーポット（サイバー攻撃調査用に設置したおとりシステム）をインターネット上に構築し、日本を含む 8 ヶ国 12 ヶ所に設置したが、日本に設置したハニーポットへの攻撃も確認されており、システムの脆弱性を利用して制御システム内にログインし、水圧の不正に改変した攻撃が行われたという。（出典：トレンドマイクロ株式会社『産業制御システムへのサイバー攻撃実態調査レポート 第 2 弾 産業制御システムを狙っているのは誰か？』（2013 年 9 月 20 日）Trend Micro Forward-Looking Threat Research Team: Kyle Wilhoit 氏）

近年の制御システムに対するサイバー攻撃の現状を鑑みると、先進的な制御システムが構築されているアメリカにおいては既に制御システムに対するサイバー攻撃が現実的なものになっており、将来的に日本の制御システムに対するサイバー攻撃も増加が見込まれる。アメリカで ICS-CERT が公表しているように、日本国内における制御システムへのサイバー攻撃の事例を収集・分類することは、現状を把握する上で効果的であると考えられる。

日本国内のサイバー攻撃事例は情報系システムにおいて増加傾向にあり、セキュリティインシデント[2]が起きているものの、制御システムでは深刻なインシデントが見当たらない。

警察庁によれば、2015 年上半期に産業制御システムで使用される特定のソフトウェアの脆弱性を標的としたアクセスを観測した他、産業制御システムで使用される複数のプロトコルを標的としたアクセスを継続して観測している。ただ、アクセスの多くはセキュリティ調査実施組織からのものであると推定されたが、目的の判明しないアクセスも観測しており、脆弱性を悪用する目的で探索が行われている可能性もあるとしている。（出典：警察庁 2015 年 9 月「2015 年上半期のサイバー空間をめぐる脅威の情勢について」）

4-1 で挙げる海外のインシデント例のように、制御システムの被害状況を見ていると、今後、日本の制御システムも攻撃の対象となることも十分考えられる。

アメリカの ICS-CERT モニターのサイバー攻撃事例（図表 2-1）のようにエネルギー、鉄・金属・発電・輸送部品製造等の重要工業分野、通信、交通、情報技術等と同じような分野で日本もサイバー攻撃を受ける可能性がある。

[2] インシデントとは、出来事・事件のこと

2-2　アメリカにおける重要インフラに対するサイバーセキュリティへの取り組みについて

アメリカの重要インフラに対するサイバーセキュリティへの取り組みは、2013 年 2 月に経済産業省より公表された「2013 年度次世代電力システムに関する電力保安調査報告書」の中で 2011 年までの主要な内容が紹介されているが、ここでは 2012 年以降の動向を調査した。

図表 2-2　アメリカの重要インフラに対するサイバーセキュリティの取り組み(2012 年～)

2012 年 1 月 5 日	DOE（エネルギー省）が C2M2 モデル開発のキックオフミーティングを開催	ホワイトハウス主導で、DOE がリードして DHS（国土安全保障省）と協働でスタート。官民共同のパートナーシップであり、規模、業界を問わずサイバーセキュリティの能力を評価、優先順位付け、向上させるために組織に貢献する目的をもって開催された。
2012 年 5 月	DOE が Cybersecurity Risk Management Process (RMP) Guideline - Final (May 2012) を公表	DOE が NIST（国立標準技術研究所）、NERC（北米電力信頼度協議会）と協働してリスクマネジメントプロセスを作成。規模、組織構造や統治構造を問わず、組織がより効果的で効率的なサイバーセキュリティのリスクマネジメントプロセスを導入することを目的として策定された。
2012 年 5 月 31 日	DOE が C2M2 の Initiative Closeout And Model Release を公表	1 月 5 日のキックオフ、2 月 29 日の最初のモデル、3 月 22 日のパイロットモデル、5 月 4 日のパイロットの評価等を経て最初の完了モデルと公表。
2012 年 5 月 31 日	DOE が ES-C2M2 Version 1.0 を公表	組織の所有構造、規模、機能に関係なく全ての電気事業に適用されるべく策定された。
2013 年 2 月 12 日	大統領令 13636 号 Improving Critical Infrastructure Cybersecurity を発表	企業におけるサイバーセキュリティリスクの管理を支援するための、業界標準およびベストプラクティスをまとめた自主参加型の、リスクベース・アプローチに基づく「サイバーセキュリティフレームワーク（以下、本フレームワーク）」を策定することを要求。
2014 年 2 月 12 日	NIST が Framework for	重要インフラのサイバーセキュリティを向上

	Improving Critical Infrastructure Cybersecurity を公表	させるためのフレームワーク。約1年間の公開論議を経て2014年2月12日に第1版を公表。
2014年2月14日	DOEがONG-C2M2 Version 1.1を公表	ES-C2M2 Version 1.0を模範として策定されたものであり、規範的というよりは記述的なガイダンスであり、規模、所有構造などに関わらずいかなる石油およびガスの事業者に適用可能なものとして策定された。
2014年12月12日	GAO（アメリカ会計検査院）からの警鐘	GAOが連邦施設のサイバーセキュリティに関してコメント。 DHSとGSA（アメリカ連邦政府一般調達局）はビル制御システムのサイバーリスクに対処すべしと警鐘を鳴らす。
2014年12月18日	法律制定：Cybersecurity Workforce Assessment Act	DHSのサイバーセキュリティに関する評価を毎年180日以内に3年間行うことを規定。
2014年12月18日	法律制定：National Cybersecurity Protection Act of 2014	サイバーセキュリティの存在するオペレーションを成文化し体系化するものとして制定。
2014年12月18日	法律制定：Cybersecurity Enhancement Act of 2014,	サイバーセキュリティを向上させ、その研究開発、ワークフォース、教育などを強化することを官民問わずに提供することを明文化。
2015年2月10日	CTIICの設立（Cyber Threat Intelligence Integration Center）	CTIICはアメリカ連邦政府の新しい機関であり、サイバー攻撃に対して既存機関と民間のセクターをリアルタイムにつなぐフュージョンセンターとして国家情報長官オフィス内に設置。
2015年12月18日	法律制定：Cybersecurity Act of 2015,	官民間で迅速、かつ責任を持ってサイバーセキュリティに関する情報のシェア促進を明文化。

（出典　各種公開資料を基に弊社にて作成）

これらの動向を整理するため、アメリカにおける重要インフラに対するサイバーセキュリティへの対応に関わる関係組織を以下に記載する。

図表 2-3　アメリカにおける重要インフラのサイバーセキュリティにかかる関係組織

組織名	主な役割
国土安全保障省 （DHS :Department of Homeland Security）	国家サイバーセキュリティ局が管轄。その傘下には制御システムのセキュリティ運営を担当するCSSP（Control Systems Security Program）がある。
エネルギー省 （DOE：Department of Energy）	電気・石油・ガスエネルギー等の重要インフラに対するサイバーセキュリティを強化する技術やイニシアティブを担う。
国立標準技術研究所 （NIST：National Institute of Standards and Technology）	商務省傘下の組織。「2007 年エネルギー自給・安全保障法（EISA）」にて、スマートグリッドシステム及びネットワークの相互運用性などの確保を目的とした枠組み・規格 開発と定められている 。
アメリカ連邦エネルギー規制委員会 （FERC：Federal Energy Regulatory Commission ）	エネルギー省傘下の組織。サイバーセキュリティに関する規格開発等を選択・承認する役割を担う。電力向けにNERC CIP サイバーセキュリティ標準を発行（2009 年）。
北米電力信頼度協議会 （NERC：North American Electric Reliability Council）	北米（アメリカ、カナダ、メキシコ）のバルクパワーシステムの信頼性を確保することであり、連邦エネルギー規制委員会から認証を受けている。ICS セキュリティーに関する活動としては、バルク電源システムのサイバーセキュリティーに関するNER-CIP 基準を作成している。
Cyber Threat Intelligence Integration Center（CTIIC）	サイバー攻撃に対する既存機関と民間をリアルタイムにつなぐフュージョンセンターとして 2015 年 2 月 10 日に新設。CIA、FBI、司法省、軍、州政府などとの間で連邦レベルの情報共有促進のための役割を担う。
アメリカガス協会 （AGA：American Gas Association）	国内ガス販売する 200 社超で構成。国内の住宅、商業施設、産業向け等、約 7200 万の需要家のうち 94%相当（約 6800 万）に AGA 傘下のガス会社がガスを届けている。日本ガス協会とは友好関係を確立。

（出典　各種公開資料を基に弊社にて作成）

多様化し、広範にわたるサイバー攻撃への対応に向けて、アメリカでは 2015 年には組織横断的な機関として CTIIC を設立し、民間機関とリアルタイムに情報共有して対策を実行する体制を整備している。つまり、アメリカは国家全体でサイバー攻撃へ対応できる仕組みが構築されている。

2-3　重要インフラに対するサイバーセキュリティの規格、ガイドラインの整理

アメリカの重要インフラに対するサイバーセキュリティの取り組みにおいては、主にDOEやDHSがNISTやNERC、FERC等と連携して重要インフラを担う各業界に向けてガイドライン等の整備を進めている。また、IEC（International Electrotechnical Commission、国際電気技術委員会）等の国際的な組織が推進する各種規格やガイドラインと併せて、特にガス業界向けに関係する内容を中心に体系を整理する。

図表 2-4　重要インフラに対するサイバーセキュリティの規格、ガイドライン

（A．技術基準）

名称	策定組織	概要	備考
NISTIR 7628	アメリカ国立標準技術研究所 (NIST)	スマートグリッドの情報セキュリティのガイドライン。従来の電力網から情報通信、装置管理、配電等でデジタルインフラへ転換するのに必要な基準	ガス制御システムとスマートメーター等の新たな通信機器との相互接続の際に参考にできる。
EDSA	ISA Security Compliance Institute (ISCI)	組み込みデバイスのセキュリティ認証規格。セキュリティ機能実装評価(FSA)、ソフトウェア開発セキュリティアセスメント(SDSA)、通信堅牢性テスト(CRT)の３要素で構成。	組み込みデバイスのセキュリティ認証規格であり、制御システム導入時のセキュリティ技術水準を評価する上で参考となる。
IEC62443-2-4	国際電気標準会議 (IEC)	国際装置ユーザ協会(International Instrument Users' Association)にて策定されたWIBを元に、制御システムのセキュリティ製品に対する機能要件の規格。	制御システム製品を提供するメーカーへの要求規格であり、調達の際のセキュリティ技術水準を評価する際に参考になる。

NIST SP800-82	アメリカ国立標準技術研究所 (NIST)	SCADA システム、分散制御システム（DCS)、プログラマブル論理制御装置（PLC）などを含む、産業制御システムのセキュリティを確保するためのガイダンス。	産業制御システムの典型的なシステムトポロジー、脅威と脆弱性、その回避策がまとめられており、参考になる。

（B．運用基準）

名称	策定組織	概要	備考
重要インフラ保護基準 (CIP)	北米電力信頼度協議会 (NERC)	電力業界向けに大規模停電被害を踏まえて策定された重要インフラ事業を遂行する上で実施すべきセキュリティ規準を8項目の体系に分類。	重要インフラ事業全般に対するセキュリティ規準の体系として整理されており、各項目別の内容については参考にできる。
IEC62278	国際電気標準会議 (IEC)	鉄道における機能安全規格の最上位であり、構想から廃棄までのライフサイクルにおける安全規格を定義。	RAMS規格であり、ガスシステムの保安の観点でアプローチ方法は参考。
IEC 62443-2-1	国際電気標準会議 (IEC)	ISO/IEC27001（ISMS）をベースに、制御システム向けのセキュリティマネジメントシステムについて規定。	制御システムのセキュリティマネジメントシステムとしてガス製造･供給システムのオペレーションに対するサイバーセキュリティ対策の指針として参考になる。
ISO/IEC TR 27019	国際電気標準会議 (IEC)	2013年に発行されたエネルギー業界向けプロセス制御システムのための ISO/IEC 27002 に	テクニカルレポートのステータスで発行されており、言及されている情報セキュリティマネジメント

		基づくISMSの指針。	に関する指針は参考になる。
Cybersecurity Risk Management Process (RMP) Guideline	アメリカエネルギー省 (DOE)	重要インフラのサイバーセキュリティ対策にかかるリスクマネジメントプロセスの導入を目的として策定。	※本項①にて記載。
Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2)	アメリカエネルギー省 (DOE)	組織内におけるサイバーセキュリティへの対応に関する自己点検の評価指標としてツールキットも提供。	※本項②にて記載。
重要インフラのサイバーセキュリティを向上させるためのフレームワーク (Framework for Improving Critical Infrastructure Cybersecurity：NIST Cybersecurity Framework)	アメリカ国立標準技術研究所（NIST)	「サイバーセキュリティに関する大統領令（第13636号）」に基づき、サイバーセキュリティフレームワーク（枠組み）の開発の成果として公表されたフレームワーク。	※本項③にて記載。

（出典　各種公開資料を基に弊社にて作成）

ここでは、2013年2月に経済産業省より公表された「2013年度次世代電力システムに関する電力保安調査報告書」以降に発行されたガイドラインである以下の3つについて、調査した結果を記載する。

①Electricity Subsector Cybersecurity Risk Management Process (RMP Guideline)

RMP Guidelineは、2012年5月にアメリカエネルギー省（DOE）が発行した、電力業界におけるサイバーセキュリティのリスクを管理するためのアプローチ方法として政府と産業界が共同で開発したガイドラインのことである。NERC CIPやアメリカ合衆国原子力規制委員会（NRC）のガイドライン等を参考に策定されており、サイバー攻撃に対して迅速に対応できる組織を構築することに寄与することを目的にしている。リスクマネジメントモデル（経営者、運用管理者、IT担当者の３階層）、リスクマネジメントサイクル（枠組み、評価、対応、監視の４分類）、リスクマネジメントプロセス（各モデルに対する各分類での実施プロセス）で構成されたガイドラインである。

電力業界向けに策定されたものであるが、サイバーセキュリティに対するこれまでの規格や各種ガイドラインを参考にしており、サイバーセキュリティリスクを管理する上でのガイドラインとして日本のガス業界においても参考になるアプローチとなっている。

②The Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2)

ONG-C2M2は、2012年に電力業界向けに策定されたEC-C2M2を基に、2014年に石油・ガス業界向けの評価指標として公表された。C2M2は、組織の規模を問わずサイバーセキュリティへの対応能力の成熟度を評価する指標であり、例えばその指標に基づいて投資の優先順位付けや、サイバー攻撃への対応を向上させるために活用するものである。DOEは2015年までにEC-C2M2を含め、40超のC2M2 自己評価を電力、石油、天然ガスの各社に導入している。具体的には、以下の10の領域に対する評価を実施するツールとなっている。

1. リスク管理
2. 資産、変更、及び構成の管理
3. アカウント及びアクセス権の管理
4. 脅威および脆弱性の管理
5. 現状の認識
6. 情報共有とコミュニケーション
7. イベントとインシデント対応と運用の継続性
8. サプライチェーンと外部委託先の管理
9. 従業員管理
10. サイバーセキュリティプログラムの管理

アメリカと日本のガス業界では市場環境が大きく異なる点はあるものの、業界に特化した評価ツールとなっており、主に前述のRMP Guidelineとリンクした評価指標となっていることから、内容としてはRMPとあわせて参考にするべきものになる。既に40社以上が導入しているとあったが、サイバーセキュリティ対策への投資の優先順位付け等に活用されているとなると、日本のガス業界でも経営者が判断する一つの指標として役立つ可能性が

あると考えられる。

③Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework)

2013年2月12日のアメリカ大統領令第13636号「Improving Critical Infrastructure Cybersecurity（重要インフラのサイバーセキュリティの向上）」に基づき、企業におけるサイバーセキュリティリスクの管理を支援するための、業界標準及びベストプラクティスをまとめた自主参加型の、リスクベース・アプローチに基づく「サイバーセキュリティフレームワーク」として、政府と民間部門との連携により策定された。

本フレームワークの特徴は、産業界で効力を発揮している標準、ガイドライン、及びベストプラクティスを集約し、サイバーセキュリティアプローチを体系化・構造化して示している点にある。本フレームワークによって、企業規模、サイバーセキュリティリスクの度合いや複雑さに関わらず、重要インフラへのサイバー攻撃に対する防護力を向上させるためのリスク管理原則及びベストプラクティスを企業が適用できるようになっている。フレームワークコア(Framework Core：サイバーセキュリティ対策のベストプラクティス、期待される成果、参考情報等のガイダンス)、フレームワークプロファイル(Framework Profile：企業におけるサイバーセキュリティ対策やビジネス要件、リスク許容度、割当可能なリソースのバランスを鑑みる方法)、およびフレームワークインプリメンテーションティア(Framework Implementation Tier：サイバーセキュリティリスクを管理する上で、自組織のアプローチの特徴を確認し、理解するための仕組み)の3つの要素で構成される。なお、2014年2月12日に発行された第1版はIPA（独立行政法人 情報処理推進機構）にて翻訳版を公表しており、詳細はそのドキュメントにて日本語で確認ができる。

当フレームワークはサイバー攻撃によるリスクを評価することを起点にしたリスクマネジメント体系として整理されたものになっており、ISMSやCSMSとは異なる視点でアプローチする内容となっている。サイバーセキュリティリスクへの対応を経営者のリーダーシップに求めるアプローチとなっているこのフレームワークは、日本のガス業界において経営者層が実施するリスクアセスメントの手法として大変に参考になると考えられる。

3　国内におけるサイバーセキュリティ対応状況

都市ガスの製造・供給システムのサイバーセキュリティを考えるにあたって、日本国内の法・制度の現状、重要インフラとしての現状、制御システムの現状、ガス業界の現状及びサイバーセキュリティ対応状況の調査結果を考察する。

3-1　サイバーセキュリティ基本法及びサイバーセキュリティ関連施策

3-1-1　サイバーセキュリティ基本法の成立

国内では、2000 年に起きた省庁ホームページ連続改ざん等以降、種々発生しているサイバー攻撃等に対応するため、2000 年に「内閣官房情報セキュリティ対策推進室」を立ち上げた後、2005 年には同室の機能を強化して「内閣官房情報セキュリティセンター（NISC: National Information Security Center）」を設置し、高度情報通信ネットワーク社会推進戦略本部（IT 戦略本部）に情報セキュリティ政策会議を置くなどサイバーセキュリティ対策を進めてきていた。近年、急速に高まっているサイバー脅威に対処し、国家の安全保障を確保するため、「サイバーセキュリティ基本法」を 2014 年に制定して国の主導的役割を明確化するとともに体制の強化等が行われた。

サイバーセキュリティ基本法は、国によるサイバーセキュリティ戦略の基盤となる法律として整備されており、サイバーセキュリティに係る定義、基本理念、サイバーセキュリティ戦略の策定、基本的施策に係る事項を明示的に定めている。その他、施策の推進主体として内閣官房長官を本部長とした「サイバーセキュリティ戦略本部」を設置して、責任、権限の付与を行って、体制強化にも力点を置いている。また、併せて内閣官房情報セキュリティセンターについては内閣サイバーセキュリティセンター（略称同じく NISC: National center of Incident readiness and Strategy for Cybersecurity）と改め、法制化するなど必要な法制整備を行った。

それ以外の基本的な施策としては、

・国の行政機関等におけるサイバーセキュリティの確保（第 13 条）
・重要インフラ事業者等におけるサイバーセキュリティの確保の促進（第 14 条）
・民間事業者及び教育研究機関等の自発的な取組の推進（第 15 条）
・犯罪の取締り及び被害の拡大の防止（第 17 条）
・我が国の安全に重大な影響を及ぼすおそれのある事象への対応（第 18 条）

・産業の振興及び国際競争力の強化（第 19 条）

・研究開発の推進等（第 20 条）

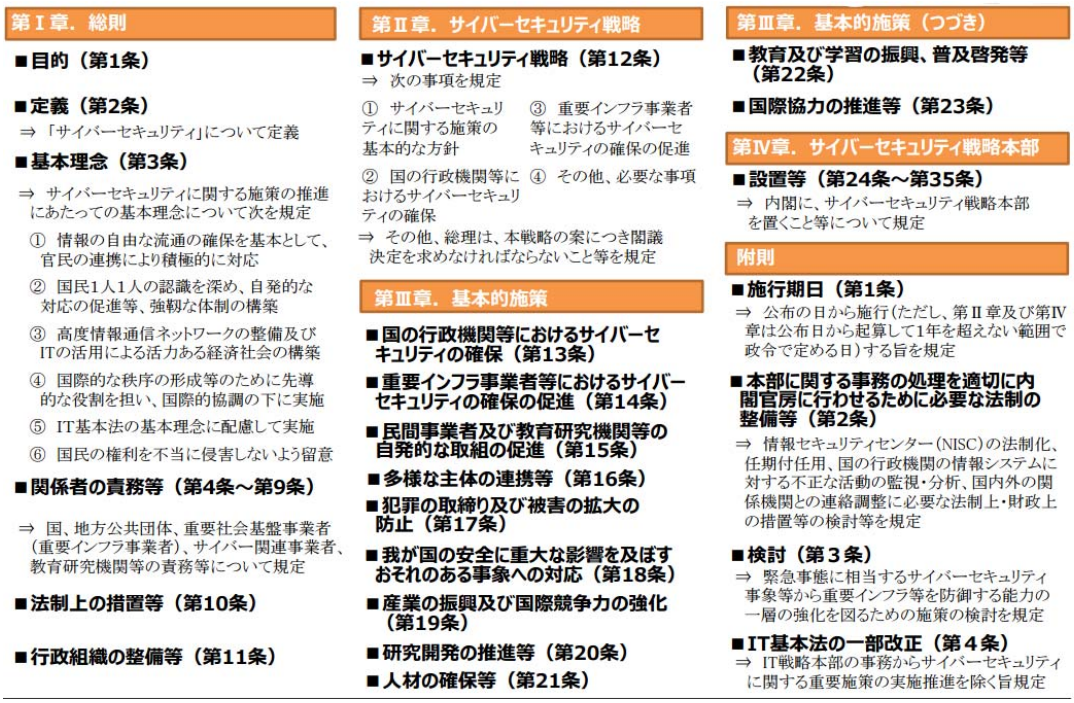
・人材の確保等（第 21 条）

・教育及び学習の振興、普及啓発等（第 22 条）

・国際協力の推進等（第 23 条）

がある。

図表 3-1　サイバーセキュリティ基本法案の概要



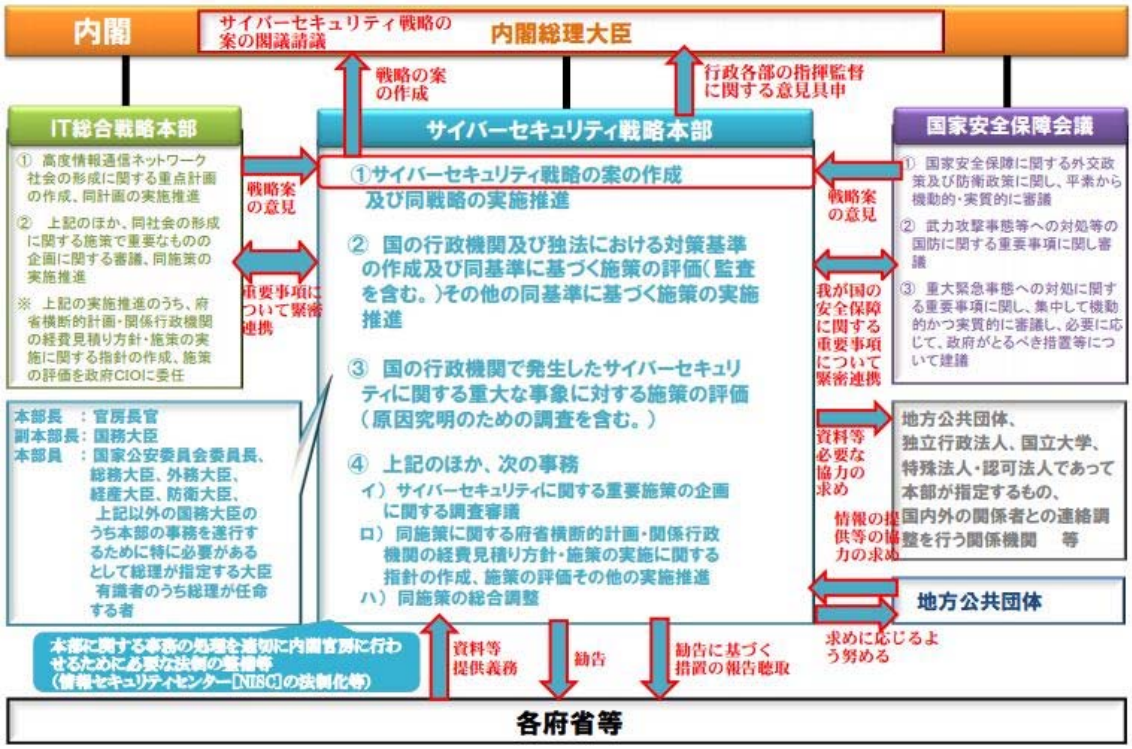
（出典：内閣サイバーセキュリティセンター（NISC））

3-1-2　サイバーセキュリティ戦略本部の設置

サイバーセキュリティ戦略本部は、サイバーセキュリティ基本法に基づき設置されており、従前、ＩＴ戦略本部に設けられた一会議体であった「情報セキュリティ政策会議」に替わり、内閣官房に置かれた機関とされている。情報セキュリティ政策会議では法的権限は有していなかったことから、その機能は企画及び調整に留まっていたが、サイバーセキュリティ戦略本部は、行政各部に対する監督に係る意見具申を行うことができ、また、各省庁に対して調査や資料提出を課し、勧告を行うことができるようになるなど、強い権限を有しており、サイバーセキュリティ対策に係る司令塔として整備がなされている。

従前の内閣情報セキュリティセンターを改組、内閣サイバーセュリティセンターとして内閣官房の組織として法制化し、サイバーセキュリティ戦略本部の事務局として活動している。NISC（内閣サイバーセキュリティセンター）は、「サイバーセキュリティ戦略」に基づき、政府のサイバーセキュリティ政策に関する総合調整を行いつつ、官民一体となって活動しており、その一環としてガス分野を含む重要インフラに係る情報セキュリティ施策を行っている。

図表3-2　サイバーセキュリティ戦略本部と政府・関係省庁の連携



（出典：内閣サイバーセキュリティセンター（NISC））

3-1-3　サイバーセキュリティ戦略

サイバーセキュリティ戦略はサイバーセキュリティ基本法第 12 条第 1 項に基づき 2015 年 9 月 4 日に閣議決定された。2020 年東京オリンピック・パラリンピックの開催、その先の 2020 年代初頭までの将来を見据えた今後 3 年程度の基本的な施策の方向性を示すものとして策定された。

「自由、公正かつ安全なサイバー空間」を創出･発展させ、「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせる社会の実現」、「国際社会の平和・安定と我が国の安全保障」に寄与することを目的とし、①情報の自由な流通の確保、②法の支配、③開放性、④自律性、⑤多様な主体の連携を基本原則としてあげている。

また、サイバーセキュリティ戦略では、重要インフラを守るための取り組みとして、次を掲げている。

・重要インフラ分野の範囲及び各分野内での「重要インフラ事業者」の範囲の継続的な見直し
・情報提供によって不利益が生じない環境の構築、より効果的、かつ、迅速な官民の情報共有（ホットライン構築、情報共有様式・手順の改良、処理の自動化等）、政府機関内での必要な連携、訓練・演習の実施の推進
・マイナンバー導入等の環境変化も見据え、地方公共団体に対し、政府として必要な支援を実施
・制御系のセキュリティについて国際標準に則した第三者認証制度の活用等推進

3-1-4　国内のサイバーセキュリティ対策への取り組み

国内では、独立行政法人情報処理推進機構（IPA）、一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）、技術研究組合制御システムセキュリティセンター（CSSC）といった各機関で様々なサイバーセキュリティ対策への取り組みが行われている。

図表 3-3　国内のセキュリティ推進に関する機関

機関名	組織の概要	取り組み内容
独立行政法人情報処理推進機構（IPA）	1970 年 10 月に設立された「認可法人情報処理振興事業協会」を前身とし、2004 年に独法化された。情報セキュリティ対策等に関する政府の唯一の実務実施機関。	情報セキュリティ対策施策を中心として、システムの信頼性対策及びＩＴ人材育成施策を一体的に実施。参加各業界間でのサイバー攻撃情報共有を行う J-CSIP（サイバー情報共有イニシアティブ）を実施。
一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC ）	1996 年 10 月に「コンピュータ緊急対応センター」として発足。特定の政府機関や企業からは独立した中立の組織。	コンピュータセキュリティインシデントについて、日本国内のサイトに関する報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行う。
技術研究組合制御システムセキュリティセンター（CSSC）	2012 年 3 月に発足。重要インフラの制御システムのセキュリティを確保するため、研究開発、国際標準化活動、認証、人材育成、普及啓発、各システムのセキュリティ検証にいたるまで一貫して業務を遂行する技術研究組合。	システムセキュリティ検証、高セキュア化構成・技術の確立、セキュリティ国際規格活動、国際規格準拠認証、インシデントサポート、人材育成、普及啓蒙等を実施。 ガス分野関連としては、模擬システムを使用したサイバー演習を毎年実施。
一般社団法人日本ガス協会（JGA）	1947 年 10 月に設立。一般ガス事業、一般ガス事業者の行う大口ガス事業、ガス導管事業の健全な発展を図るとともに、エネルギーの安定供給と保安の確保および環境問題等への対応を通じて、経済と国民生活の向上に寄与することを目的とする、都市ガス事業者の団体。	情報セキュリティ関連では、安全基準類の整備と周知、情報共有体制の構築、各種サイバー対応訓練を行っている。「重要インフラの情報セキュリティ対策に係る第３次行動計画」におけるガス分野のセプター事務局としても位置付けられている。

3-2　重要インフラにおける対応

3-2-1　重要インフラの情報セキュリティ対策に係る第 3 次行動計画

サイバーセキュリティ基本法の施行を踏まえ、NISC は「重要インフラの情報セキュリティ対策に係る第 3 次行動計画」（2014 年 5 月 19 日情報セキュリティ政策会議決定、以下「行動計画」という）について所要の修正を行うとともに、重要インフラの分野として化学、クレジット、石油の 3 分野の追加を行う改訂を行っている（2015 年 5 月 25 日サイバーセキュリティ戦略本部改訂）。これにより重要インフラとして、情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、化学、クレジット、石油の 13 分野を設定している。

重要インフラにおけるサービスの持続的な提供を行い、自然災害やサイバー攻撃等に起因するＩＴ障害が国民生活や社会経済活動に重大な影響を及ぼさないよう、ＩＴ障害の発生を可能な限り減らすとともに、ＩＴ障害発生時の迅速な復旧を図ることで重要インフラ防護することを目的とし、以下の 5 つの取り組みを掲げている。

1. 安全基準等の整備及び浸透
   重要インフラ各分野に横断的な対策の策定とそれに基づく各分野の安全基準等の整備・浸透の促進
2. 情報共有体制の強化
   ＩＴ障害関係の情報の共有による、官民の関係者全体で平時・大規模ＩＴ障害発生時における連携・対応体制の強化
3. 障害対応体制の強化
   官民が連携して行う演習等の実施。演習・訓練間の連携によるＩＴ障害対応体制の総合的な強化
4. リスクマネジメント
   重要インフラ事業者等におけるリスク評価を含む包括的なマネジメントの支援
5. 防護基盤の強化
   広報広聴活動、国際連携の強化、規格・標準及び参照すべき規程類の整理・活用・国際展開

3-2-2　行動計画に基づく情報共有

行動計画に基づいて重要インフラ分野での情報共有（情報連絡・情報提供）を行うため、重要インフラ 13 分野について、18 のセプターを設置している。セプターとは、重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織「Capability for Engineering of Protection, Technical Operation, Analysis and Response」の略称「CEPTOAR」のことである。

1)情報通信分野
　T-CEPTOAR
　ケーブルテレビ CEPTOAR
　放送 CEPTOAR
2)金融分野
　銀行等 CEPTOAR
　証券 CEPTOAR
　生命保険 CEPTOAR
　損害保険 CEPTOAR
3)航空分野
　航空分野における CEPTOAR
4)鉄道分野
　鉄道 CEPTOAR
5)電力分野
　電力 CEPTOAR
6)ガス分野
　GAS CEPTOAR
7)政府・行政サービス分野
　自治体 CEPTOAR
8)医療分野
　医療 CEPTOAR
9)水道分野
　水道 CEPTOAR
10)物流分野
　物流 CEPTOAR

11)化学分野

化学 CEPTOAR

12)クレジット分野

クレジット CEPTOAR

13)石油分野

石油 CEPTOAR

これらの各分野にまたがった情報共有を行うため、各セプターにより構成されるセプターカウンシルが設けられている。セプターカウンシルは、各重要インフラ分野で整備されたセプターで構成される会議体として 2009 年 2 月に設立され、①分野横断的な情報共有の推進、②重要インフラのＩＴ障害の未然防止のための情報共有体制の調整及び管理、③分野横断的な共通課題の発見及び共通認識の醸成などの活動に取り組んでいる。GAS CEPTOAR はセプターカウンシル創設時より参加している。

また、情報共有体制の能力の維持、向上のため、NISC が中心となって、情報連絡・情報提供の手順に沿ったセプター訓練、情報共有体制等の検証、課題抽出のための分野横断的演習が毎年、実施されている。分野横断的演習は、重要インフラ全体の防護能力の維持・向上を図るため、事業者等による情報セキュリティ対策の実施及び実効性確認等を通じた障害対応能力の向上を目指しており、模擬インシデントに対する初動対応等とその対応の振り返りにより、自組織の対応力の検証、課題の抽出を行って、それらを踏まえての事後の改善に繋げている。分野別横断的演習には、GAS CEPATOAR も、例年、積極的に参加している。

その他、IPA を中核として、サイバー攻撃による被害拡大防止のため、重要インフラ機器製造業者と重要インフラ業界を中心にサイバー攻撃に関する情報共有の取り組みである J-CSIP による活動を行っており、2016 年 1 月現在、7 分野、62 組織が参画している。J-CSIP は、標的型サイバー攻撃への対策の一つとして、個別企業の利害関係を越えた情報共有が社会全体の観点での最大のメリットであるということから、IPA が情報ハブ（集約点）となり、メンバー間での情報共有などを推進する役割を担い、活動が行われている。2012 年 10 月には、ガス SIG（Special Interest Group（業界ごとの情報共有グループ））の運用が開始され、現在、GAS CEPTOAR10 事業者と日本ガス協会で情報共有が図られている。

図表 3-4　セプターの概要（2015 年 3 月末時点）

（出典：2014 年度 セプターの活動状況の把握について（2015 年 3 月 NISC））

重要インフラ分野	情報通信			金融				航空	鉄道	電力	ガス	政府・行政サービス	医療	水道	物流	化学	クレジット	石油
事業の範囲	電気通信		放送	銀行等	証券	生命保険	損害保険	航空	鉄道	電力	ガス	政府公共団体	医療	水道	物流	化学	クレジット	石油
名称	T-CEPTOAR	ケーブルテレビ CEPTOAR	放送 CEPTOAR	金融CEPTOAR連絡協議会 銀行等 CEPTOAR	証券 CEPTOAR	生命保険 CEPTOAR	損害保険 CEPTOAR	航空分野における CEPTOAR	鉄道 CEPTAOR	電力 CEPTOAR	GAS CEPTOAR	自治体 CEPTOAR	医療 CEPTOAR	水道 CEPTOAR	物流 CEPTOAR	化学 CEPTOAR	クレジット CEPTOAR	石油 CEPTOAR
事務局	(一財)日本データ通信協会 テレコム・アイザック推進会議	(一社)日本ケーブルテレビ連盟	(一社)日本民間放送連盟	(一社)全国銀行協会 事務システム部	日本証券業協会 ＩＴ統括部	(一社)生命保険協会 総務部組織法務グループ	(一社)日本損害保険協会 ＩＴ推進部共同システム開発室	国土交通省 航空局 安全企画課	国土交通省 鉄道局 総務課 危機管理室	電気事業連合会 情報通信部	(一社)日本ガス協会 技術部	地方公共団体情報システム機構 情報化支援戦略部	厚生労働省 医政局 研究開発振興課 医療技術情報推進室	(公社)日本水道協会 総務部総務課	(一社)日本物流団体連合会	石油化学工業協会	(一社)日本クレジット協会	石油連盟
構成員（内訳）	２６社・団体 （固定系のﾈｯﾄﾜｰｸｲﾝﾌﾗを設置する電気通信事業者、ｱｸｾｽ系の電気通信事業者、ISP事業者、携帯電話事業者等）	310社 ((一社)日本ケーブルテレビ連盟の正会員ケーブルテレビ事業者)	１９４社・団体 （日本放送協会、地上系民間基幹放送事業者、(一社)日本民間放送連盟）	1,487社 （銀行、信用金庫、信用組合、労金、商工中金、農協等）	254社 ７機関 （証券会社、取引所等証券関係機関）	42社 ((一社)生命保険協会の定款に定める社員および特別会員)	29社 (オブザーバ３社含む) ((一社)日本損害保険協会 情報システム委員会参加会社)	２グループ ３機関 （航空運送事業者、定期航空協会、官庁［航空局、気象庁］）	２２社 １団体 １機関 （鉄道事業者22社、１団体、官庁［鉄道局］）	１２社 ２機関 （一般電気事業者、日本原電(株)、電源開発(株)、電気事業連合会、電力中央研究所）	１０社 （主要な一般ガス事業者10社）	４７ 都道府県 1,741 市区町村	１グループ ６機関 （医療機関、(公社)日本医師会、四病院団体協議会（(一社)日本医療法人協会、(公社)日本精神科病院協会、(一社)日本病院会、(公社)全日本病院協会）、保健医療福祉情報システム工業会）	８水道事業体 （会員水道事業体のうち会長都市並びに地方支部長都市） [補足]障害の内容によって、構成員を通じ、全国の日本水道協会の会員水道事業体(1,356事業体)へ情報を提供	６団体 １６社 （日本物流団体連合会、日本船主協会、日本内航海運組合総連合会、日本港運協会、日本倉庫協会、全日本トラック協会及び主要な物流事業者16社）	８社 （主要な石油化学事業者）	18社 （主要なクレジットカード会社等）	15社・グループ （主要な石油精製・元売会社）
緊急窓口	2007年4月運用開始	2012年12月運用開始	2007年4月運用開始										2008年4月運用開始			2015年1月運用開始	2014年4月運用開始	2014年12月運用開始
情報の取扱ルール	2007年1月制定	2012年11月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2007年3月制定	2006年9月制定	2007年3月制定	2007年3月制定	2008年3月制定	2008年3月制定	2008年3月制定	2014年12月制定	2014年４月制定	2014年１２月制定
情報と連絡手段	障害事例 情報等 メール、電話	障害事例 情報等 メール、電話	障害事例 情報等 メール、電話、FAX、WEB	障害事例 情報等 メール、電話、ＷＥＢ	障害事例 情報等 メール、電話、FAX、WEB	障害事例 情報等 メール、電話、携帯	障害事例 情報等 メール、電話	障害事例 情報等 メール、電話	障害事例 情報等 メール、電話	脆弱性に関する情報等 メール、電話携帯、FAX、電子会議室TV会議、会議体	障害事例 情報等 メール、電話、携帯、AX	障害事例 情報等 メール、電話、WEB	障害事例 情報等 メール、電話、携帯、衛星電話、FAX	障害事例 情報等 メール、電話、携帯、衛星電話、FAX	障害事例 情報等 メール、電話	障害事例 情報等 メール、電話、携帯電話	障害事例 情報等 メール、電話	障害事例 情報等 メール、電話

3-2-3　電力業界の取り組み

資源エネルギー庁の「電力分野のサイバーセキュリティ対策について」（2016 年 2 月 9 日）発表資料によれば、

①サイバー攻撃の事案は増加傾向

②従来のばらまき型の攻撃ではなく、特定の政府関係機関や企業を狙った標的型サイバー攻撃により、個人情報等の情報が漏洩

③組織的あるいは国家的な攻撃が疑われる事例も存在

④近年は、制御系システムへのサイバー攻撃により、物理的な被害に及ぶ事案も発生

との現状認識がある。

特に、制御システムについては、産業構造審議会・保安分科会・電力安全小委員会で対策を検討して取りまとめ、組織的・技術的な対策要件も提示している。日本電気技術規格委員会（JESC）においてガイドラインを策定中であり、このガイドラインを電気事業法の保安規制に組み込み、実効性を担保する予定である。制御システムについては、PDCA サイクル[3]を回し続けるための仕組みの整理が必要との指摘もされている。

一方、制御システムと同じくサイバー攻撃の影響が大きいと考えられているスマートメーターシステム[4]に関しても、経済産業省のスマートメーター制度検討会セキュリティワーキンググループにおいて対策が検討され、JESC の下でのガイドラインを策定している。同システムは、情報共有体制の構築や外部監査の実施について整理が行われているところである。

電力分野においては、総合資源エネルギー調査会電力・ガス事業分科会電力基本政策小委員会において、制御システムを取り巻く状況が変化する中で課題の整理を行っている。ここでは、標準技術や汎用製品の採用が進んでいること、高度な IT 機能化や外部接続の増加という点が課題として挙げられている。また、システム改革のために新規参入者等が増加し、電力制御系システムに関わる主体の変化を見込んでいる。

電力事業者の対応について「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、電気事業連合会が自主ガイドラインを作成、電力各社が外部接続の限定等、自主的に取り組みを実施してきた。加えて、J-CSIP への参加と電気事業連合会内の情報共有体制を構築した。また NISC、CSSC 等のセキュリティ機関主催のサイバー演習への参加や一般社団法人電力中央研究所を中心とした電力業界独自のサイバー演習の実施などが進行中である。

---

[3] Plan＜計画＞→ Do＜実行＞→ Check＜評価＞→ Act＜改善＞

[4] スマートメーターを接続し、データ収集および通信制御を行うシステム

3-3　制御システムに関するサイバーセキュリティ対策

3-3-1　制御システムのセキュリティ上の特性

制御システムは、電力・ガス・水道・通信などの重要社会インフラや、プラント・工場などの産業分野において、機器や装置の制御および監視に使用されている。

制御システムは、常時ネットワークにつながっていないことから、サイバー攻撃の影響を受けづらいといわれてきた。また、制御システムの仕様は事業者ごとに固有であるため、内部仕様を熟知していなければ、有効な攻撃ができないため、一般的なＰＣが感染するウイルスや不正プログラムの影響を受けないと考えられていた。（出典：経済産業省「サイバーセキュリティと経済 研究会報告書中間とりまとめ」2011 年 8 月 5 日）

しかし、昨今は制御システムへの IT 技術の利用が進んでおり、経済産業省の調査によると、2009 年 3 月時点で制御システムの 36.8%が外部ネットワークとつながっており、88.9%で Windows 系の OS が利用されているという調査もある（出典：経済産業省委託調査 2009 年 3 月）。

制御システムのオープン化に伴い、情報システムでも見られるようなハードウェア及びソフトウェア両面での脆弱性を引き継ぐ可能性が高い。重要インフラの制御システムに存在する脆弱性が攻撃を受け、その攻撃によってシステムの動作に影響が出た場合には、その影響が社会活動の広範囲に及ぶことも考えられる。

外部ネットワークに接続されていない制御システムにおいても、USB メモリ等の外部記録媒体を介して制御システムにコンピュータウイルス等のマルウェアが持ち込まれる危険性もある。

今後、IoT（Internet of Things）が進展すると、機器のコンピュータ化に加えて、分析技術や制御技術の進化により、現場から大量のデータを収集し、業務（製造、流通、運営）モデル、経営モデル等についてバーチャルに現場を再現した上で、「多種多様かつ大量データの解析(digital)」を行い、「高度な判断サービスや自動制御」を実現する社会が実現するといわれている（出典：経済産業省「IoT 時代に対応したデータ経営 2.0 の促進」平成 26 年 12 月）。その過程ではさらに制御システムのセキュリティの強化が求められる。

3-3-2　制御システムのセキュリティ技術のための組織

図表 3-5 ガス事業者用模擬演習模擬プラント

（CSSC の HP から引用）

重要インフラの制御システムのセキュリティを確保するために、研究開発や国際標準化活動等を行っている組織として、「技術研究組合　制御システムセキュリティセンター（CSSC）」がある。個々の内容を検討する委員会として、大きく下記の４つの委員会とその役割が存在する。

１）研究開発・テストベッド委員会：

制御システムセキュリティに関連する研究開発及びテストベッド構築の方向性を定め、研究開発及びテストベッド利活用を推進する。テストベッドとは、制御システムのいくつかの重要な機能を実装し、研究開発やサイバー演習を実施するための模擬プラントのことである。

２）評価認証・標準化委員会：

制御システムセキュリティに係わる評価認証および標準化の戦略および施策について検討し、評価認証・標準化のためのテストベッドの利活用を推進する。

３）インシデント・ハンドリング委員会：

制御システムにおけるセキュリティインシデント発生に対する備え及びセキュリティインシデント発生時の対応を含めたインシデントハンドリング[5]に必要な技術開発の方向性を検討する。

４）普及啓発・人材育成委員会：

技術研究組合としての制御システムセキュリティの普及啓発・人材育成の方向を定め、テストベッドを活用した普及啓発・人材育成を推進する。

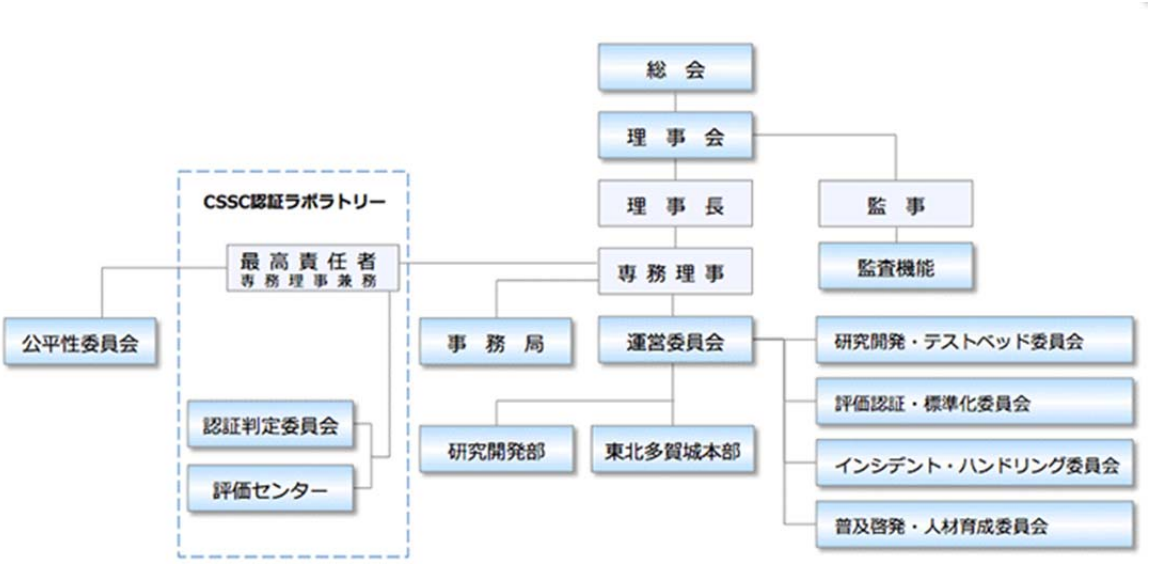
CSSC 東北多賀城本部の CSS-Base6 模擬プラントでは、現在、7 業種 9 機の模擬プラントを保有し、その一部を使って、ガス、電力、ビル、石油化学の各分野のサイバー演習を行っている。図表 3-5 がガス事業者用模擬演習模擬プラントである。

[5] インシデントハンドリングとは、インシデントの発見から対処・報告までの一連の流れのこと

このような模擬プラントでは、検証手法の確立や実システム・コンポーネントの評価の実施、普及啓発におけるセキュリティアラートとセキュリティ対策効果の体験等、幅広く活用されている。

このように CSSC は、重要インフラの制御システムのセキュリティ確保に資する研究・開発を遂行することを目的として設立されている。

図表 3-6 CSSC 組織図



（CSSC の HP からの引用）

3-3-3　CSMS（Cyber Security Management System）認証等について

これまでの情報セキュリティ対策としてはISO/IEC27001、プライバシーマークなどが日本での認証基準として維持・発展されてきた。制御システムにおいても、オープン化の進展や制御システムを狙った標的型攻撃の事件報告が増加してきている中、制御システムのサイバーセキュリティに特化した基準を用意しておく必要性に迫られてきた。安心・安定を求められる重要インフラを担う企業や組織にとって、自社におけるサイバー攻撃へ対処する体制・機能を前もって準備しておくことは重要である。

CSMS(Cyber Security Management System)とは、産業用オートメーション及び制御システム（IACS：Industrial Automation and Control System）をサイバー攻撃から守るためのセキュリティ対策を確保することを目的としたサイバーセキュリティのマネジメントシステムのことであり、国際標準 IEC 62443-2-1 をベースに、一般財団日本情報経済社会推進協会（JIPDEC）　情報マネジメント推進センターによって「CSMS 認証基準(IEC 62443-2-1:2010)」が策定された。CSMS 認証基準への適合性評価制度（CSMS 制度）は、組織が構築・運用する CSMS が CSMS 認証基準に適合しているか審査し認証登録する「認証機関」、審査員の資格を付与する「要員認証機関」、及びこれらの各機関がその業務を行う能力を備えているかを見る「認定機関」からなる総合的な運用の仕組みとなっている。

CSMS の対象者は、制御システムのライフサイクルを考慮し、制御システムのオーナーである事業者に加え、システムの構築や運用開始後のシステム改修、維持保全を分担する事業者及びシステムインテグレータが想定されており、「認定機関」である JIPDEC より認定された「認証機関」（2015 年 3 月 9 日時点で一般財団法人　日本品質保証機構　マネジメントシステム部門と、BSI グループジャパン株式会社の 2 機関）に申請し、審査を経て認証登録される。

既に 2014 年には世界に先駆けて国内で 2 社（三菱化学エンジニアリング(株)と横河ソリューションサービス(株)）が CSMS を取得した。国内でも CSMS の取得認証を支援するサービスも一部、出始めてきている。ガス事業者においても、大手事業者のガス製造プラントで CSMS 認証取得の動きがある。

今後、ISO/IEC27001、プライバシーマークが取引条件となったように、CSMS 取得そのものが取引条件となることも想定される。企業の一つの格付けとして発展していくことが考えられる。

またシステムのセキュリティを確保する為には、セキュリティが確保されているコン

ポーネントでシステムを構成することが望ましい。EDSA 認証はコンポーネント自身のセキュリティ認証であり、EDSA 認証を取得したコンポーネントを採用する事でシステムのセキュリティは大きく改善する。

EDSA 認証は 2015 年までで国内で 3 社 4 製品が取得している。

3-4　国内のガス業界のサイバーセキュリティに対する取り組み

3-4-1 都市ガス製造・供給システムの概要

都市ガスにおける制御システムは、製造システムと供給システムから構成される（図表 1-1 参照）。前者はガスの製造部分であり、海外から船で運ばれてきた LNG（液化天然ガス）を一旦 LNG タンクに入れ、工場で気化して高圧ガスにするものである。後者はその工場からガス導管を通じてガバナステーションで高圧ガスを中圧ガスに変え、中圧ガバナで低圧ガスに変えてガス需要家に送る供給部分のシステムである。製造システムで原料の気化や熱量、製造量の調整などを行い、供給システムで供給ラインにおけるガバナステーションの圧力監視や流量調整、ガスホルダーでの貯溜・送出量の調整などを行う。この一連のライン上の各所でインターネットなど外部に接続されていない制御システムが使われている。

3-4-2 都市ガス業界としての取り組み

都市ガス分野においては、国内に 206 の事業者があり、販売量では上位 4 社で 73.1%（出典：2016 年 1 月の都市ガス販売量実績について日本ガス協会）を占め、従業員 50 名未満の事業者が半数以上である。都市ガス事業者によって規模が大きく異なり、ガス設備の保有状況も異なる。それに応じて、製造・供給システムの保有状況も異なるため、都市ガス業界としては、各事業者の自主判断を尊重しつつ、業界内でＩＴ障害の判断基準となる考え方を共有できるよう取り組んでいる。日本ガス協会では①安全基準の整備と周知活動、②情報共有体制の構築、③サイバー攻撃発生時の対応訓練を主軸として都市ガス事業者のサイバーセキュリティ活動の支援を行っている。

＜日本ガス協会の主な活動状況＞

① 安全基準の整備と周知活動

・「製造・供給に係る制御系システムの情報セキュリティ対策ガイドライン」の策定・改定

・「インシデントハンドリングマニュアル作成ガイド」の策定

② 情報共有体制の構築

・J-CSIP、C4TAP、JPCERT 早期警戒情報を中心とした情報共有体制の整備

・セプターカウンシルへの参加

③ サイバー攻撃発生時の対応訓練

・NISC セプター訓練への参加

・NISC 分野横断的訓練への参加

・CSSC ガス分野サイバー演習の実施

・日本ガス協会独自のインシデントハンドリング訓練の実施

日本の都市ガス業界における安全基準は「重要インフラの情報セキュリティ対策に係る行動計画」（2005 年情報セキュリティ政策会議決定）に則って整備されている。2006 年 9 月に日本ガス協会は「製造・供給に係る制御系システムの情報セキュリティ対策ガイドライン」を策定し（2012 年 1 月最終改訂）、以下の 4 項目を柱としている。

⑴組織・体制および資源の確保

⑵情報についての対策（情報の格付け、取扱い等）

⑶情報セキュリティ要件の明確化に基づく対策（アクセス制御など導入すべき機能、不正プログラムなどの脅威を防ぐために遵守すべき事項等）

⑷情報システムについての対策（入退出管理、電子計算機対策、アプリケーションソフトウェア対策、通信回線対策等）

情報共有体制の構築については、既存の連絡体制等を有効に活用するとともに、日本ガス協会内に設けられた実務者による常設のワーキンググループが未然防止策や再発防止策等の具体的な検討に取り組んでいる。また、主要事業者 10 者により「GAS CEPTOAR」を構成し、NISC の活動やセプターカウンシルの活動に参加している。

また、近年各種対応訓練も拡充させている。CSSC ガス分野サイバー演習の実施も 2015 年度で 4 回目を数え、大手事業者から中小規模の事業者まで幅広い層が参加している。また、日本ガス協会で構築したインシデントハンドリング訓練も対象を大手事業者から徐々に中規模事業者に広げているところである。

これらの多面的な取り組みから得られた知見は日本ガス協会が開催する地方説明会等を通して随時正会員に共有されている。

各ガス事業者においては、日本ガス協会が提供する製造・供給に係る制御系システムの情報セキュリティ対策ガイドライン等を参考に各社の規程・マニュアルを策定している。また、日本ガス協会からの情報提供を受け、各社独自でセキュリティ対策を推進している。大手事業者では 3-3-3 で述べたとおり CSMS 認証取得の動きがあり、日本ガス協会が提供している訓練をもとに独自の訓練を構築・実施している事業者もある。

3-4-3 アンケート及びヒアリングによるセキュリティ対策状況の調査

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実態を把握するために GAS CEPTOAR を構成する 10 事業者を対象にアンケート調査を行った。そのうち４事業者にヒアリングを行い、アンケート回答結果をより詳しく確認した。

主要ガス 10 事業者を調査対象としたのは、我が国のガス事業者は、現在、206 事業者存在するが、事業者間で事業規模、設備構成、組織体制等に大きな格差があり、実態調査にあたって一律の内容で行うことに難があること。また、供給する需要家ベースでこの１０事業者で８割超を占めている実態や、ＩＴ障害が発生した場合の影響の点からも、これらの状況を把握することで一定の有効な状況把握ができるからである。

なお、ヒアリング対象についは、主要 10 事業者での規模を考慮して、事業規模を分散して東京ガス、東邦ガス、京葉ガスの 3 事業者を選定し、また、事業形態としての特徴から公営事業者である仙台市ガス局を選定した。

アンケート及びヒアリングは、製造・供給システムに関する基本情報及びセキュリティ対策ごとに分類した設問で構成している。分類は、セキュリティ組織体制、ポリシー等整備状況、情報資産の管理状況、物理的対策状況、システム的対策状況、人的対策状況、組織外コミュニケーション、インシデント発生状況、外部環境の変化の 9 分類としている。

アンケート実施期間	2015/12/25～2016/1/25
アンケート対象事業者	北海道ガス、仙台市ガス局、東京ガス、京葉ガス、北陸ガス、静岡ガス（清水エル･エヌ･ジー）※、東邦ガス、大阪ガス、広島ガス、西部ガス

※清水エル・エヌ・ジーは GAS CEPTOAR を構成する 10 事業者ではなく、一般ガス事業者でもないが、静岡ガスの製造部門に相当する関連会社としてアンケートの回答を得たことから併せて調査対象とした。そのため、アンケート回答事業者は 11 事業者となっている。

ヒアリング実施期間	2016/01/22～2016/02/04
ヒアリング対象事業者	仙台市ガス局、東京ガス、京葉ガス、東邦ガス

4　想定されるリスクシナリオ

海外の制御システムにおけるインシデント事例調査よりインシデントの発生要因を類型化し、アンケート及びヒアリングの結果から得られた国内のガス製造・供給システムの現状を踏まえて、インシデントが発生するリスクシナリオを考える。

4-1　重要インフラにおけるサイバー攻撃及びサイバーインシデントについて

まず、インシデントの発生要因を類型化するために、重要インフラの制御システムにおけるサイバー攻撃及びサイバーインシデントを調査した。そのインシデントから発生要因を洗い出したところ、４つに類型化できることがわかった。その４つの類型化とは、①外部媒体によるマルウェア感染、②外部ネットワークからの侵入、③委託先・提携先との接点からの侵入・マルウェア感染、④内部犯である。以下に、この４つの類型をまとめている。

①外部媒体によるマルウェア感染

クローズドなネットワークを構成していたとしても、バージョンアップなどの保守、データバックアップ、別系統システムへのデータ移動などのために、外部記録媒体を利用している。これを利用した攻撃である。

②外部ネットワークからの侵入

OS やアプリケーションの脆弱性を狙い、外部ネットワークから侵入するパターン。制御システムと外部システムがどこかでつながっている可能性がある。

③委託先・提携先との接点からの侵入・マルウェア感染

委託先や提携先などとの接点において発生する。委託先の従業員によるものや、相手先のウイルス感染によるものなどがある。

④内部犯

正規の権限をもっている従業員によるシステムの不正操作や内部情報の不正利用は大きな危機を招く。制御システムは不正操作された後の社会的影響が大きい。

以上の類型化においては、それぞれのサイバー攻撃への対応策も違ってくる。類型化に即した対応策を考えることは防御だけでなく、被害の極小化につながるものと考える。

これら類型を導いた重要インフラへのサイバー攻撃事例を挙げる。

＜類型①外部媒体によるマルウェア感染の事例＞

イランの核施設を狙ったサイバー攻撃：2010 年 11 月

2010 年 11 月、Stuxnet（スタックスネット）がシーメンス社製の遠隔監視制御・情報取得（SCADA）システムで利用している独シーメンス社製 WinCC/PCS7 を攻撃し、イランの原子力開発施設（ナタンズプラント）の遠心分離機を制御する PLC（プログラマブルロジックコントローラ）を乗っ取り、周波数変換装置を攻撃し、核施設にある相当数の遠心分離機がマルウェアによって破壊された。

常時外部接続していない制御システムでもマルウェアに感染し、被害を受けることがあることを示した初めての事例として制御システムのセキュリティに大きな問題提起をした事件となった。

（出典：国内における制御システムのサイバーセキュリティ　新　誠一氏）

ブラジルの発電所が運転停止：2011 年 2 月

ブラジルの発電所で制御システムがマルウェアの「WORM_DOWNAD（ダウンアド）」に感染し、オペレーションが停止した。「WORM_DOWNAD」は複数の感染手法を用いる不正プログラム。登場当初は Windows の脆弱性を狙うタイプだったが、その後 USB メモリなどの可変媒体経由の感染、共有ネットワーク内のコンピュータへのパスワードクラック機能などを追加した亜種が登場してきたことから、発電所の制御システムに到達。その結果、システムは機能せず、現場からの運用データが表示されなくなった。復旧には数ヶ月を要したとされており、その被害は甚大なものとなった。

（出典：2012 年 6 月 12 日「IT pro」日経コンピュータ）

＜類型②外部ネットワークからの侵入の事例＞

トルコの石油パイプラインが爆発の可能性：2008 年 8 月

サイバー攻撃によりトルコ・レファヒエの石油パイプラインが爆発した可能性が指摘されている。攻撃者は、パイプラインに設置されている監視カメラの通信ソフトの脆弱性を

利用して内部ネットワークに侵入。不正に動作制御系にアクセスし、警報装置の動作を停止させ、管内の圧力を異常に高めて爆発を引き起こしたとされている。

（出典：2015 年 5 月 14 日・15 日　独立行政法人情報処理推進機構　技術本部 セキュリティセンター　主任研究員 渡辺貴仁　重大な経営課題となる『制御システム』のセキュリティリスク）

アメリカのダムで水門制御システムへの侵入：2013 年

2013 年にアメリカ・ニューヨーク州のダム管理システムがサイバー攻撃を受け、水門を制御される事態になっていたことが 2015 年 12 月になって分かった。

このサイバー攻撃はそれほど高度な手口は使われておらず、不正アクセスを試す目的で仕かけられたと当局は見ている。ハッカーはダム全体のシステムに侵入することはできなかったが、水門を制御することは可能だったという。ダムは降雨時に水流をコントロールして下流の洪水を防ぐ役割を担っている。ダムの制御に使われていたのは業界標準のソフトウェアだったという。ダムへのアクセスは携帯電話のモデムで行われたとされている。

（出典：2016 年 1 月 8 日ニューズウィーク日本版　サイバーセキュリティと国際政治　NY のダム、ウクライナの変電所…サイバー攻撃で狙われる制御システム　土屋大洋氏）

アメリカ天然ガスパイプラインが標的となったサイバー攻撃：2013 年 2 月

アメリカ DHS（国土安全保障省）の機密報告書によると、2011 年 12 月から 2012 年 6 月にかけて、アメリカ天然ガスパイプラインを運用する 23 社が、中国に関係するサイバースパイ活動の標的となっていた。対象企業は、スピア型フィッシング[6]で攻撃された。盗み出された情報は、ユーザ名、システムのマニュアル、パイプライン制御システムにアクセスする資格情報などであり、この情報を利用すると、攻撃者はコンプレッサーステーションに損害を与えることも可能になる。（出典：NRI Secure Security Information（SANS NewsBites、@RISK サマリー版）Vol.8 No.9　2013 年 3 月 5 日発行）

ドイツの製鉄所が不正アクセスにより操業停止：2014 年 12 月

ドイツの製鉄所で、サイバー攻撃によって溶鉱炉が正常にシャットダウンできず、装置および製鉄システム（操業）に大きな損害を与える事件が発生していた。攻撃は、特定の従業員らに対する標的型攻撃を通じて認証情報や機微な情報を窃取して OA ネットワークに侵入し、その後、生産システムに侵入を拡大した。

（出典：CSSC 国際的な標準・認証の動向 小林 偉昭氏）

[6]特定のターゲットに対して重要なデータや個人情報を奪おうとしてフィッシング詐欺を行う手法のこと

＜類型③委託先・提携先との接点からの侵入・マルウェア感染の事例＞

オーストラリアの上下水処理場でオペレーション妨害：2000 年 3 月

2000 年にオーストラリアの SCADA ソフトウェアを開発する企業の元従業員が、上下水処理場の運営会社の職に応募したものの不採用とされたことに恨みを抱き、2 カ月間の間 46 回にわたって同社の下水処理の制御システムに侵入し、下水排水施設のデータを書き換え、オペレーションを妨害し、結果として 264,000 ガロンもの未処理の下水を河川や公園に放出した。

（出典：総務省　自治体クラウド「情報セキュリティ対策等に関する調査研究 報告書」 2013 年 5 月）

アメリカの Davis-Besse 原子力発電所でシステム停止：2003 年 1 月

2003 年 1 月、オハイオ州 Davis Besse 原子力発電所で送電事業者と発電事業者のネットワーク相互接続中、設定の不備でファイアーウォールをバイパスして制御システムがウイルス感染した。同発電所でマイクロソフトの SQL サーバを狙った Slammer（スラマー）ワームが VPN（Virtual Private Network）接続を介して侵入・感染、SCADA システムを約 5 時間にわたって停止させた。感染した Slammer ワームに対するパッチは、その時点で公開されていたにもかかわらず、同発電所のシステムには該当パッチがあてられていなかった。プロセス・コンピュータも停止し、再運用までに約 6 時間を費やしている。また、他の電力施設を結ぶ通信トラフィックにも障害を来たし、通信の遅延や遮断が生じた。

（出典：2012 年 11 月 15 日独立行政法人情報処理推進機構の「サイバー攻撃と組込みセキュリティ」より）

＜類型④内部犯の事例＞

ロシアでパイプラインのガス供給量コントロール狙われる：1999 年

1999 年、ロシアのガス会社ガスプロム（Gazprom）がハッカーによって侵入された。その攻撃にはガスプロムの内部者が協力していた。世界最大の天然ガス生産業者ガスプロムは西ヨーロッパへの最大のガス供給者でもあるが，ハッカーたちはパイプラインのガス供給量をコントロールするセントラル・スイッチボードのコントロールを得るために「トロイの木馬」を使用したといわれている。（出典：クリストファー・ベッグス「オーストラリアにおけるサイバーテロ」　岡田好史氏翻訳）

アメリカで病院内システムを使った DDos 攻撃の実行前に逮捕：2009 年 6 月

アメリカのダラス（テキサス州）にある W.B. CarrellMemorial Clinic の夜勤の契約警備員が同病院の HVAC システムや患者情報のコンピュータに侵入し、HVAC システムの HMI 画面のスクリーンショットをオンラインで公開。この公開画面では病院の様々な機能のメニューが確認できる。アラーム設定の停止で HVAC システムのアラームがプログラムどおりに機能しないことで、SCADA セキュリティの専門家が調査し、FBI 及びテキサス州検察局に報告したことで発覚、警備員は逮捕された。同警備員はこの病院のシステムを使って独立記念日（7 月 4 日）に大規模な DDoS 攻撃を仕掛ける計画を立てていたが、実行前に逮捕された。

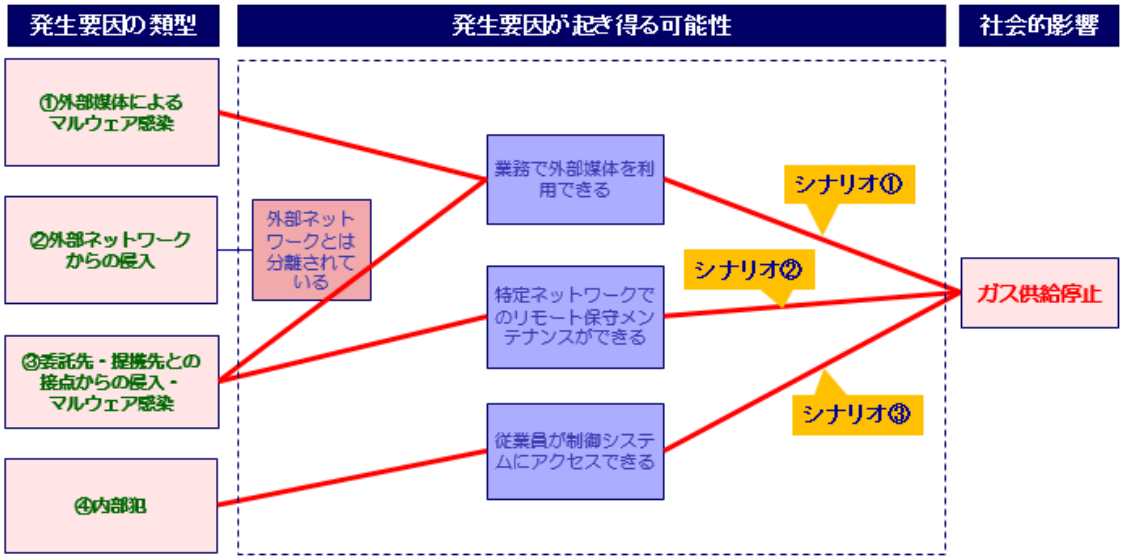
（出典：技術研究組合制御システムセキュリティセンター「制御システムセキュリティの脅威と対策の動向および CSSC の研究概要について」2015 年 2 月 9 日）

4-2　都市ガスの製造・供給システムの制御システムにおけるリスクシナリオ

都市ガス製造・供給システム自体のセキュリティが確保できなくなる主要なリスクシナリオについて考える。海外における事例を参考に発生要因を分析した。発生要因は、①外部媒体によるマルウェア感染、②外部ネットワークからの侵入、③委託先・提携先との接点からの侵入・マルウェア感染、④内部犯の 4 つに類型化でき、リスクシナリオの検討材料とした。

類型化した 4 つの発生要因により、どのように社会的影響をもたらすのかを、アンケート及びヒアリングによる製造・供給システムのサイバーセキュリティ対策に関する実態調査結果から検討を行った。社会的影響については、都市ガスにおいて発生すると影響が大きいと考えられるガス供給停止について考察した。リスクシナリオ導出における検討内容を図表 4-1 に示す。

図表 4-1　発生要因と社会的影響への関連性



まず 4 つの発生要因のうち、「②外部ネットワークからの侵入」については、製造・供給システムがいずれの事業者も外部ネットワークから分離されている現状から社会的影響に至るものではないと判断した。残り 3 つの発生要因は、社会的影響に及ぶ可能性があると判断できる。まず製造・供給システムにおいて外部記録媒体が使用される場合があることから、「①外部媒体によるマルウェア感染」「③委託先・提携先との接点からの侵入・マルウェア感染」については発生する可能性がある。「③委託先・提携先との接点からの侵入・マルウェア感染」については特定のネットワークを使用してリモート保守メンテナ

ンスが行われている場合もあることから、このケースも発生の可能性がある。「④内部犯」については、製造・供給システムに限らず、情報セキュリティ対策を行う上で、考慮すべき共通の脅威であり可能性はある。

社会的影響については、製造段階においては、製造所の制御システムが乗っ取られ適切な制御を喪失したとしても、製造所の各所に設けられた機械式の安全弁により、異常圧力でパイプラインにガスが流れない仕組みとなっている。供給段階においてはガバナの 2 次圧が遠隔制御可能なものもあるが、遠隔制御を行えない安全装置（所定の圧力以上に設定できない機械的制約や圧力上限検知によるガス遮断弁閉止機能等）により、2 次圧の異常上昇を防止する機構を備えている。またガスホルダーについても、圧力上昇時のガス受入弁自動閉止機能やホルダー上部に機械式安全弁を備え、これらは遠隔制御と切り離されている。これらの状況を加味して分析した結果、社会的影響をガス供給停止に絞り、以下の 3 つのリスクシナリオを導出した。

シナリオ① 委託先・提携先含む外部媒体利用

リスクシナリオとしては、インターネットに接続可能な情報系システム端末がマルウェアに感染していた場合、データ移行に使っている USB メモリも感染し、そこから製造・供給システムもマルウェアに感染するという可能性がある。製造・供給システムの OS 等に脆弱性が内在した状態ではその可能性は高くなると考えられる。また、Stuxnet の様な新種のマルウェアに USB が感染している場合、ウイルスチェックをしても発見されないというリスクもある。

シナリオ② リモート保守業務

リスクシナリオとしては、委託先従業員が保守以外の目的で、製造・供給システムにリモートでアクセスし不正操作をするということが考えられる。

また、リモート保守を行っている委託先のパソコン端末がマルウェア感染し、そのままリモート保守することで、製造・供給システムがマルウェア感染するというリスクシナリオも想定される。

シナリオ③ 内部犯

内部不正によるリスクシナリオは、社員や退職社員等による不正操作が考えられる。

製造・供給システムは、24 時間 365 日稼働しており、常時ログインした状態であることが多い。外部からは容易に侵入できないよう入退室管理を行っているが、内部犯行による意図的な不正操作については留意が必要である。

5　ガスシステム改革を踏まえた都市ガスの製造・供給システムの将来像

本章では、ガスシステム改革が制御システムに与える影響について検討し、都市ガスの製造・供給システムの将来像について検討した。

5-1　ガスシステム改革の内容

ガスシステム改革を踏まえた保安規制については、産業構造審議会保安分科会ガス安全小委員会において、2014 年 6 月からガスの保安水準の維持・向上を前提とし、今後の望ましい在り方について検討を進めてきた。そして、2015 年 2 月に審議内容の報告書として「ガスシステム改革等を踏まえた保安規制の在り方について」がとりまとめられた。

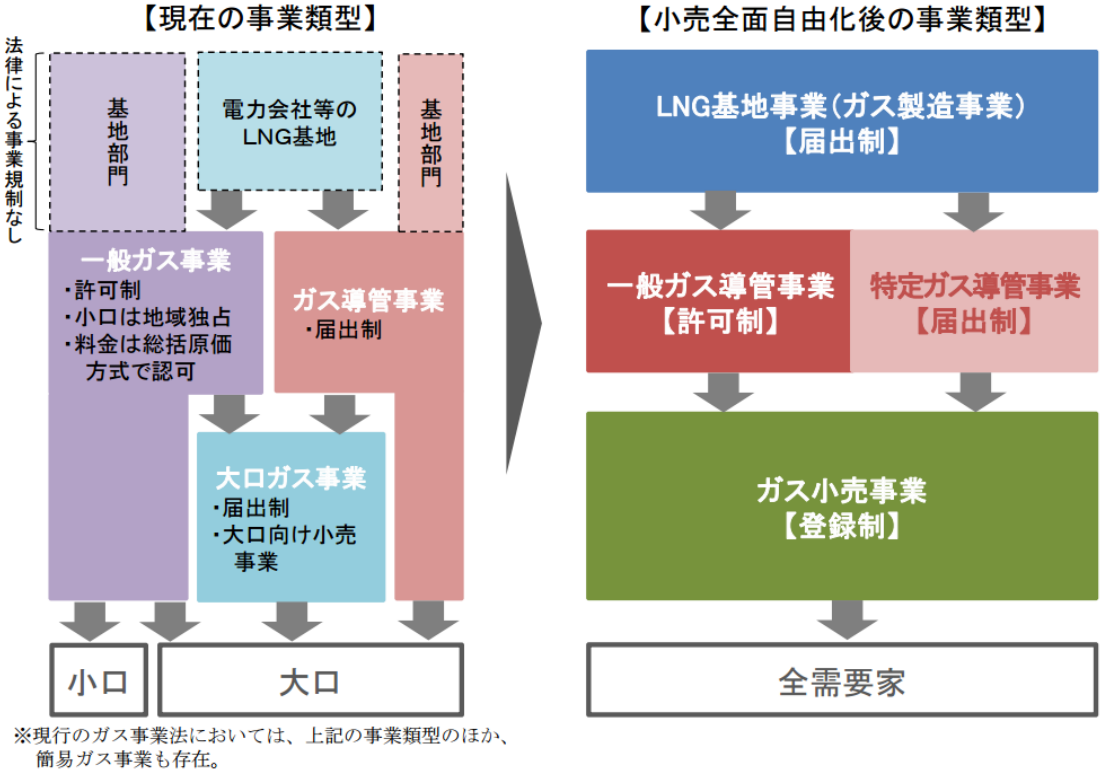
これを受け、2015 年 6 月に成立した電気事業法等の一部を改正する等の法律第 5 条におけるガス事業法改正では、ガスの小売全面自由化後の保安規制として、当該報告書の内容に即した改正が行われてきたところである。

改正ガス事業法は①小売参入の全面自由化、②ライセンス制の導入、③LNG 基地の第三者利用、④ガス導管網の整備促進に加えて、⑤保安の確保を大きな柱にしている。

具体的には、（ⅰ）これまでの小売の地域独占を撤廃し、登録を受けた事業者による小売事業への新規参入が可能になること、（ⅱ）「一般ガス事業者」や「簡易ガス事業者」といった区別がなくなり、一般ガス導管事業（許可制）、ガス小売事業（登録制）、ガス製造事業（届出制）といったライセンス制度に移行といった内容である。現行制度と小売全面自由化後の事業類型の変更点は図表 5-1 のとおりである。

また、改正ガス事業法では、保安水準の維持・向上の観点から保安規制についても所要の見直しを行っており、（ⅰ）導管網の保安及び内管保安、緊急時対応に関する義務を、従来の都市ガス事業者などのガス導管事業者に課す、（ⅱ）災害発生時も含めた「公共の安全の維持又は災害の発生の防止」に関する連携・協力について、全てのガス事業者に義務を課す、（ⅲ）新規参入者を含むガス小売事業者に対して、適正な消費機器の調査・周知の実施を担保するために、調査・周知等の保安業務に関して「保安業務規程」を作成する制度を創設等の措置している。

図表 5-1　ガスの小売全面自由化後における事業類型の変化



（出典：2015 年 8 月 20 日、第 22 回ガスシステム改革小委員会事務局提出資料　改正ガス事業法及び改正熱供給事業法について）

改正ガス事業法の５つの柱

①小売参入の全面自由化

○現在、一般ガス事業者にしか認められていない家庭等へのガスの供給について、小売の地域独占を撤廃し、登録を受けた事業者であればガスの小売事業への参入を可能とする。

○小売料金規制を原則撤廃。ただし、需要家保護の観点から、競争が不十分な地域には規制料金メニューの提供を経過措置として義務付ける。

○また、都市ガスの小売全面自由化に併せ、簡易ガス事業について許可制の下での地点独占、料金規制を廃止し、ガス小売事業者として都市ガスの供給区域に参入することを可能にする。

②ライセンス制の導入

○小売参入全面自由化により、「一般ガス事業」や「大口ガス事業」といった区別がなくなることから、ＬＮＧ基地事業（ガス製造事業）、ガス導管事業、ガス小売事業ごとに、それぞれ必要な規制を課す。（ＬＮＧ基地事業は届出制、一般ガス導管事業は許可制、特定ガス導管事業は届出制、ガス小売事業は登録制とする。）

③LNG 基地の第三者利用

○ＬＮＧ基地を保有する事業者を対象に、第三者による利用を正当な理由なく拒否することを法律により禁止。

○料金の算定方法など利用条件を約款として届出・公表することを義務付け、条件が不適当な場合は国が変更を命令。

④ガス導管網の整備促進

○一般ガス導管事業者については、地域独占や料金規制を維持し、安定供給を確保。

○全てのガス導管事業者に、導管の相互接続に係る努力義務を課す。

○導管接続を促すため、国が事業者間の協議を命令・裁定できる制度を創設。

⑤保安の確保

○導管網の保安及び小口需要家が保有する内管の点検・緊急保安に関する法律上の義務を、従来の都市ガス事業者をはじめとしたガス導管事業者等に課す。保安に係る費用については、託送供給約款等において制度的に担保し、確実に回収。

○消費機器の調査・危険発生防止の周知に関する義務を、消費者と接点の多いガス小売事業者に課す。

○災害発生時も含めた、「公共の安全の維持又は災害の発生の防止」に関するガス事業者間の連携・協力について、全てのガス事業者に義務を課す。自由化や分社後もこれまでと同様の災害対応ができるよう、ガス導管事業者と新規参入者を含めたガス小売事業者の連携ルール等を整備する予定。定期的な訓練や情報共有を実施することで、円滑な緊急時対応に備える。

5-2　ガスシステム改革による都市ガスの製造・供給システムへの影響と将来像

ガスシステム改革が都市ガスの製造・供給システムにどういう影響を及ぼすかについて、前項（5-1）で触れた「小売参入の全面自由化」を踏まえて課題を整理する必要がある。しかしながら、改正ガス事業法施行後の制度設計に関しては、大枠は整っているものの、現時点で詳細設計はまだ整備途上であることから、都市ガスの製造・供給システムについて、その将来像を踏まえたサイバーセキュリティ対策の具体的な内容を整理するには制度の詳細の確定を待つ必要がある。

一方で、2016 年 4 月より電気の小売が自由化されるが、これによりガス事業者が電気事業に参入していくことが予定されている。また、2017 年の都市ガスの小売参入の自由化に際しては、天然ガス輸入の一方の雄である電気事業者がガス小売に参入することが見込まれるなど、相互に乗り入れることとなる。このような中で、電気事業においては、電力設備のサイバーセキュリティについて、保安規制に組み込んで制度的措置を講じる方向で検討が進んでおり、日本電気規格協会（JESC）の策定する電力システムのセキュリティガイドラインを 2016 年度早期にも技術基準等に位置付けることが見込まれている。そのため、今後は都市ガス事業においても、当該基準の内容を考慮に入れて対応していくことが必要になるものと思われる。

今回の調査により、調査対象である主要 10 事業者の現状の都市ガスの製造・供給システムに係る状況については、概ね把握することができ、製造系、供給系とも他のネットワークからの分離を基本とした対応が講じられていることが確認できた。しかし、その一方で将来的に考慮することが望ましい懸念点も確認できたことから、今後は、「小売の全面自由化」を踏まえた課題の整理と併せつつ、よりセキュアなシステムとする取り組みを継続していくことが必要だと考えられる。

6. 都市ガスの製造・供給システムに求められるサイバーセキュリティの在り方

調査の結果及び評価における懸念点を踏まえ都市ガスの製造・供給システムのサイバーセキュリティ対策の更なる高度化に向けて実施を検討すべき事項として以下の提言を行う。

①組織体制の高度化

現状の組織体制は、既存の組織の役職者が情報セキュリティに係る責任者を担い、また、IT 関連の会議体にて所要の審議、検討等を行っている等、既存の組織の枠組みの中で対応がなされているが、事業環境は日々変化し、また、サイバー攻撃の手段、方法も多様化し、巧妙かつ複雑化している。これにより、情報セキュリティに係る懸念の範囲は広くなり、既存の組織の枠組みを跨いでの課題やインシデントが発生することも想定されるが、そのような場合に迅速、適切な対応ができない可能性がある。

このため、既存の組織の枠組みに縛られることなく、全社的なサイバーセキュリティ体制の構築の推進やインシデント発生時に適切な対応が行えるようにすることが必要であると考えられることから、セキュリティ担当役員（CISO）の設置や、情報セキュリティ委員会の運営、CSIRT の構築・運用等について検討を行うことも必要である。

②ポリシー等の整備・管理

情報セキュリティポリシーや情報セキュリティ管理に関する規定の整備や製造・供給システム関連規程の整備は行われているが、適宜に行うべき改訂が必ずしも十分には行われていない。他方、BCP を策定している事業者は多く、BCP へのサイバー攻撃等の取り込みも進んでいる状況が認められた。

情報セキュリティポリシーや情報セキュリティ管理に関する規定に反映するべき事項等は、社内の要求の変化、社会環境の変化、技術の進展、新たな脅威の出現等に応じて、見直しを適宜に行い、実践されなければ、必要な効果が得られないと考えられることから適切な管理・見直し、確実な実践を行うことが必要である。

③事業リスクを設定した上でのリスクアセスメントの実施

リスクアセスメントについて、実施していない事業者が一部認められた。また、リスクアセスメントを実施している事業者であっても、そのリスクについて事業リスクを定義、設定していない者が一部認められた。

リスクアセスメントは、インシデントが発生した場合に被害や影響を最小限化するのに有効な手法であると考えられるが、前提として、事業者の事業リスクの定義、設定などができていない場合には、十分な妥当性のあるリスク評価が実施できていないものと考えられる。そのため、システムの重要度に応じたレベル分けや事業リスクを設定した上でリスクアセスメントの実施について検討する必要がある。

④外部記録媒体の使用の極小化・管理の徹底

製造・供給システムの運用・保守上の理由から、USB メモリ等の外部記録媒体を使用する場合があることが認められた。ウイルス対策を講じた上で管理された状態で使用されているなど一定の侵入防御対策は講じられているが、Stuxnet のように、クローズドなネットワーク環境下においても外部記録媒体を通じてマルウェアの侵入を許した事例もあり、また、マルウェア自体の高度化も進み、新たなウイルス、マルウェアが出現していること等を考慮すると外部記録媒体の使用の極小化や管理の徹底を図っていくことが必要である。

⑤制御システムにおけるホワイトリスト等の導入、多層防護化等

供用中においては、OS の製品寿命よりも製造・供給システム全体の供用期間が長いこと等の理由から使用している OS の一部に古いものが残されている場合が見受けられた。都市ガスの製造・供給システムの防護は外部からの分離を基本としており、事実、一定の管理がなされていることから、その脆弱性が外部に晒される可能性は低い環境下にはあるが、④でも記したとおり、クローズドなネットワークであっても侵入される可能性はあるというということを常に意識しておくことが必要であり、今後の制御システムのセキュリティ対策では、あらかじめ登録されたアプリケーションやコマンドしか実行できないホワイトリストや接続点での侵入検知・防御、外部への通信に対する防御などについて検討する必要がある。

⑥サイバーセキュリティに係る教育の充実等

情報セキュリティに関する教育について、実施している事業者が多いものの、実施していない事業者もあった。製造・供給システムに係る従業者が制御システムに必要な知識を有していない場合、外部との分離の維持が脅かされる可能性がある他、インシデント発生時の早期認識や応急処置に支障を及ぼすことも考えられることから、情報セキュリティ教育の充実についても取り組むことが重要である。

また、セキュリティインシデント対応に関する手順書を策定していない事業者もあった。上記と同様に、インシデント対応に関する手順書等が策定されていないとインシデント発

生時の早期認識や応急処置に支障を及ぼすことも考えられるので手順書等の整備についても検討すべきである。

⑦外部接続の極小化、対策徹底等

保守に関して、オンサイトで実施するとしている事業者が多いものの、リモートアクセスで行うとしている事業者もあった。また、保守用の機器については、委託事業者管理のものを使用しているといった事業者等が見受けられた。メンテナンス時以外は物理的に遮断するなどの対策が取られているが、外部のネットワークと接続することができ、その機会がある以上、不正アクセスを許す可能性や委託事業者のマルウェア感染の影響が及ぶ可能性が皆無とは言えない。このため、外部接続の極小化について検討することが必要である。また、⑤で述べたとおり、接続点での侵入検知・防御、外部への通信の検知・遮断などの対策、ホワイトリストなどの導入について検討することも必要である。

おわりに

本調査では、都市ガスの製造・供給システムのサイバーセキュリティ対策について、現状把握を行い、その結果から考えられる課題の抽出を行った。調査対象は、GAS CEPTOARを構成する主要10事業者に限定したものではあるものの改めて実態の把握を行ったことは一定の意義があったものと思われる。

我が国の都市ガス事業においては、一般社団法人日本ガス協会の「製造・供給に係る制御系システムの情報セキュリティ対策 ガイドライン」を参考にして、各事業者で情報セキュリティポリシー等を整備し、それぞれの事業者に応じた対策を講じてきており、それらが奏功して、これまでのところ、ガスの供給に支障を及ぼすような事故は発生していないところである。

しかしながら、改めて検討してみると次の事項について、改善の努力を要する課題が存在することが確認できた。

① 組織体制の高度化
② ポリシー等整備管理
③ 事業リスクを設定してのリスクマネジメントの実施
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の等の導入、多層防護化等
⑥ サイバーセキュリティに係る教育の充実
⑦ 外部接続の極小化、対策徹底

これらは、組織に係るものから技術的な内容のものまで多岐に亘っているものであり、具体的な検討、その対応には、個々の事業者が、それぞれの事業規模、実態に応じた取り組みを行うことが求められる。

サイバーセキュリティ対策で重要なのは、その取り組みに当たっては、事業者として、その経営層から個々の従業員までが、それぞれ意識を持って臨むことが必要であるという点である。経営層として取り組むべきものから、現場の従業員の日々の活動におけるものまで幅広いものであり、特定の担当者が取り組めば足りるというものではないということに留意が必要である。組織のどの階層の対応が欠けていても、それが蟻の一穴となる可能性がある。事業者自身を護り、需要家の生活や事業活動を護るためにも弛まぬ改善が望まれる。

付録 1 有識者委員名簿

本事業では下記の委員からなる「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に係る有識者委員」を設立し、全２回の委員会を開催して検討を進めた。

（委員長）

新 誠一	国立大学法人　電気通信大学　情報理工学研究科　教授

（委　員）

新井 貴之	横河電機株式会社 IAPF グローバル開発センタープロジェクト管理部技術開発課
金野 千里	独立行政法人 情報処理推進機構 技術本部　セキュリティセンター 情報セキュリティ技術ラボラトリー ラボラトリー長
谷 吉智	一般社団法人日本ガス協会 技術部保安技術グループ 副部長
宮地 利雄	一般社団法人 JPCERT コーディネーションセンター 経営企画室 主席研究員／技術顧問
吉松 健三	技術研究組合 制御システムセキュリティセンター 研究開発部 研究員

※敬称略、委員は五十音順、所属等は委員会開催時

付録 2 有識者委員会概要

第１回

日時：平成 27 年 12 月 14 日（月） 15:00 ~ 17:00

場所：経済産業省　本館 1 階　西共用会議室

議事：本調査事業の概要、スケジュールについて

都市ガスの製造・供給システムの概要について

我が国のサイバーセキュリティに対する取り組み、対応等について

諸外国のサイバーセキュリティに対する取り組み、対応等について

調査アンケート、ヒアリングの設問項目・内容について

制御システムにおけるリスクについて

ガスシステム改革を踏まえた都市ガスの製造・供給システムの将来像について

都市ガスの製造・供給システムに求められるサイバーセキュリティの在り方について

第２回

日時：平成 28 年　3 月　3 日（木）　9:30 ~ 12:30

場所：経済産業省　別館 10 階　 1031 各省庁共用会議室

議事：アンケート、ヒアリングの結果について

調査報告書案について