経済産業省

資料４

ガス分野におけるサイバーセキュリティ対応の向上に向けた取組について

平成３０年３月６日
経済産業省 産業保安グループ
ガス安全室

１．ガス事業におけるサイバーセキュリティ対応の経緯・現状

● 国民生活や社会経済活動の基盤である重要インフラにおいて、システムの汎用化が進む中でサイバー攻撃が急増したことから、サイバーセキュリティ対策の強化が重要な課題となったことから、政府は対策の一環として「重要インフラの情報セキュリティに係る行動計画」を策定し、サイバーセキュリティ対策の強化に係る取組みを進めてきた。
　重要インフラの一角を成すガス事業においても、ガスの供給に関わる制御系システムへのサイバーセキュリティ強化は重要な課題であり、「重要インフラの情報セキュリティに係る行動計画」に基づいて、セプターと呼ばれる情報共有体制等を整備するとともに、ガス業界として「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」を策定し、事業者の内規策定・改訂の支援を行っている。

● 経済産業省では、平成２７年度に「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の現状を把握し、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。
● 上記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、平成２８年7月に改定を実施し、業界内への展開を行っている。
　また、ＣＳＳＣガス分野サイバー演習、インシデントハンドリング訓練等の対応訓練の充実を図り、対応力の向上に努めてきた。

2．ガス分野におけるサイバーセキュリティ対応の向上に向けた今後の対応

●重要インフラの情報セキュリティに係る行動計画の改訂等の社会的要請

　従前の重要インフラの情報セキュリティに係る第３次行動計画による取組をさらに進展させ、オリパラ大会も見据えた施策強化を進めるため、平成２９年に「重要インフラの情報セキュリティに係る第４次行動計画」として改訂がなされ、重要インフラサービスを安全かつ持続的に提供できるよう、サイバー攻撃や自然災害等に起因する重要インフラサービス障害の発生を可能な限り減らし、その発生時には迅速な復旧が可能となるよう、情報セキュリティ対策に関する取組を推進することとされた。

　その第４次行動計画の中において、重要インフラ所管省庁において取り組む施策として、安全等を維持する観点から必要に応じて、情報セキュリティ対策を関係法令等の保安規制として位置付けること等が掲げられている。

●重要インフラの情報セキュリティに係る第４次行動計画を踏まえた対応の検討

　上記を踏まえ、また、都市ガスの安定供給を確保する観点から、ガス事業者による情報セキュリティ対策に係る取組の確実な実施を期すると、同対策をガス事業法上の保安規制の一部として位置付けることが重要である。

●ガス事業法の保安規制の一部として位置付ける方向での検討

　ガス事業法ではガス事業者に対し保安規程の作成と遵守を求めており、これに保安組織や災害その他の非常時の場合に取るべき措置等の所要の内容を盛り込むことで、保安活動の確実な実施を図ってきた。

　都市ガスの製造・供給設備の制御システムの特徴や事業者の多様性を踏まえつつ、都市ガス供給における安全を維持するため、製造・供給に係る制御システムのサイバーセキュリティ対策についても保安規程の要求事項の一として位置付け、「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」等これまでのガス業界におけるサイバーセキュリティ対策を基本とした社内規定等の整備とその確実な実施を図らせる方向で検討、具体化してはどうか。

（参考）重要インフラの情報セキュリティ対策に係る第４次行動計画

「重要インフラの情報セキュリティ対策に係る第４次行動計画」

サイバーセキュリティ基本法に基づく施策の一環としてサイバーセキュリティ戦略本部決定として、平成２９年４月に策定されてており、情報セキュリティ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。

重要インフラにおいて、機能保障の考え方を踏まえ、サイバー攻撃や自然災害等に起因する重要インフラサービス障害の発生を可能な限り減らすとともに、その発生時には迅速な復旧を図ることにより、国民生活や社会経済活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現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
   重要インフラ防護において分野横断的に必要な対策の指針及び各分野の安全基準等の継続的改善の推進
2. 情報共有体制の強化
   連絡形態の多様化や共有情報の明確化等による官民・分野横断的な情報共有体制の強化
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重要インフラ障害対応体制の総合的な強化
4. リスクマネジメント及び対処態勢整備
   リスク評価やコンティンジェンシープラン策定等の対処態勢の整備を含む包括的なマネジメントの推進
5. 防護基盤の強化
   重要インフラに係る防護範囲の見直し、広報広聴活動、国際連携の推進、経営層への働きかけ、人材育成等の推進

（参考）ガス業界におけるサイバーセキュリティ対応状況

「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」

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」（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ガスセプター10社における内規の策定・改訂支援を目的として「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」を策定した（2016年7月最終改訂）。当該ガイドラインは以下の4項目を柱としている。

(1)セキュリティ基本方針の策定
(2)体制の構築
(3)設計・実装時のセキュリティ確保
(4)運用時のセキュリティ確保

「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」を基にした反映事項

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

ガス業界におけるサイバーセキュリティに係る訓練・演習の実施状況

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2017年度で６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・準会員に共有されている。

（参考）ガス事業における制御システムの概要

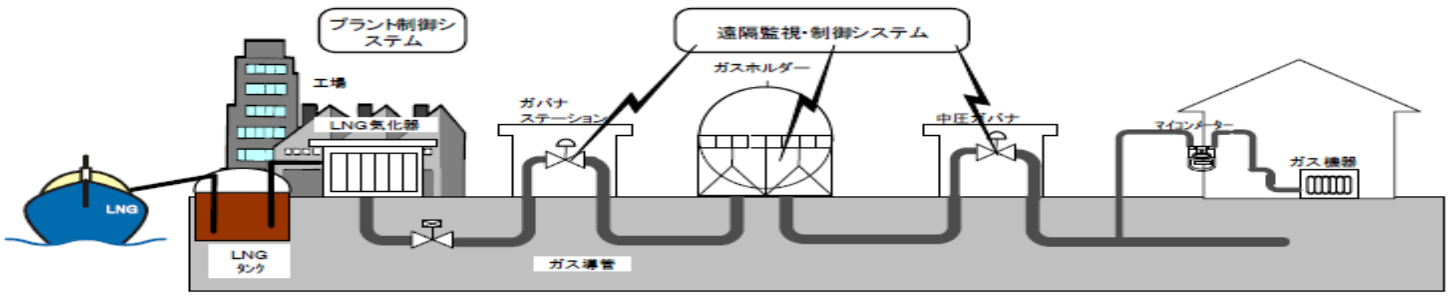
《都市ガス製造・供給システムに係る制御の特徴》

●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が困難なものとしている。

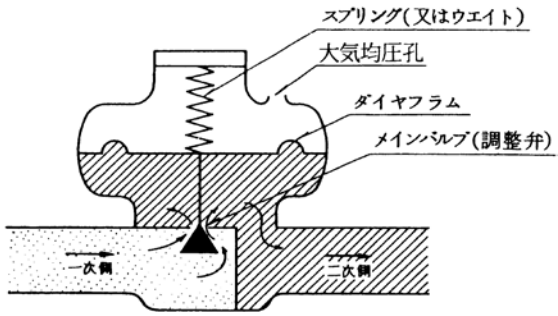
●供給系統中にガスホルダーを有している他、導管中に圧力のある気体として保有されていることから、仮に製造系統の制御システムがサイバー攻撃を受けて製造が停止しても直ちに供給支障には至らない。

●ガバナの緊急停止のための制御システムがサイバー攻撃を受けて仮に一部のガバナが閉止した場合も、冗長性を持たせた導管ネットワークでは供給支障には至らない。また、供給系統の圧力制御は制御システムによらず機械式制御のガバナで行っているため、仮に制御システムへのサイバー攻撃があっても供給支障には至らない。

（参考）都市ガス製造・供給システムの概要



【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
【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
（出典：日本ガス協会）



ガバナの基本構造