経済産業省

資料６－１

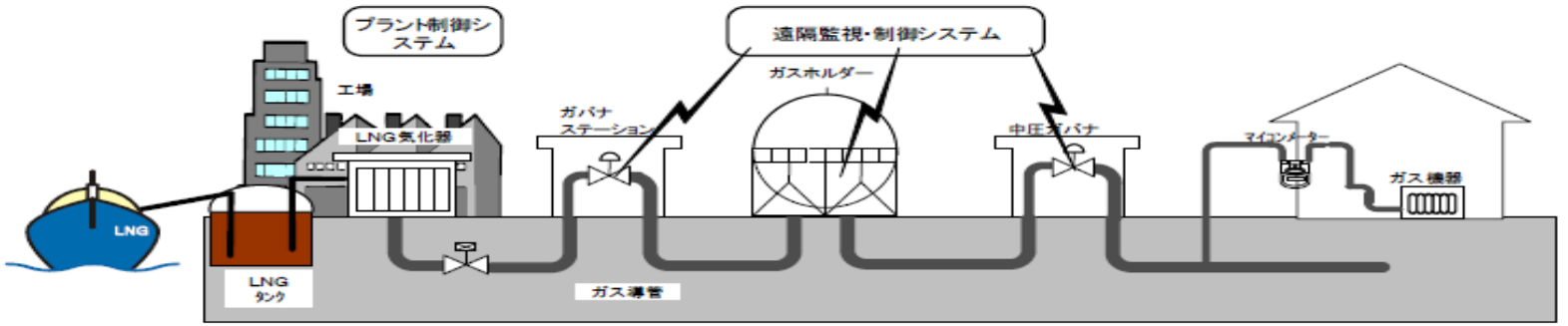
平成27年度　都市ガス製造・供給システムのサイバーセキュリティ対策に関する調査事業について

平成２８年１１月２９日

経済産業省 商務流通保安グループ
ガス安全室

1．ガス事業における制御システムの概要

（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）

《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、仮に製造が停止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。

経済産業省

2．経済産業省の取り組み（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調査）

●標的型攻撃を始めとした様々な形態のサイバー攻撃により、あらゆる分野でサイバー攻撃の脅威が高まっている中、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。
●このため、経済産業省は、「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。

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

セキュリティ対策状況に係るアンケート・ヒアリングの実施

アンケート実施期間	平成２７年12月25日～平成２８年1月25日
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	平成２８年1月22日～2月4日
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

3．都市ガス製造・供給システムの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に関する調査結果①

- セキュリティ組織体制については、製造・供給システムにおいては責任者は概ね配置されている。CISO、CSIRTの設置については、必ずしも普及していないが、既存の役員等の役職、会議体等、組織の枠組みの中で役割は明確にしている。

- 情報セキュリティポリシーについては、ガス業界の自主的な取り組みとして、一般社団法人日本ガス協会が策定した「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」を参考に全10事業者でポリシーや情報セキュリティ管理に関する規程の整備がなされている。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、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。

- 情報資産の管理状況については、情報資産の洗い出しは概ね行われており、機器・ソフトウェアの設置・更新状況の記録については適正に行われているが、情報資産の重要性に応じたレベル分けや管理については必ずしも十分ではない事業者も存在している。リスクアセスメントについて、実施していない事業者も認められ、また、リスクアセスメントは実施してはいるが、事業リスクを定義、設定していない者が一部認められた。

- 物理的対策状況については、製造・供給システムは、基本的には社内を含む他のネットワークとは、物理的、または論理的に分離された構成とし、また、製造・供給システム設置エリアへの入退室管理により外部からは容易に侵入できない状態で管理されている。ただし、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が外部記録媒体を使用する場合があることが認められており、マルウェア対策等の防護上の要注意点である。

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に関する調査結果②

- システム的対策状況については、セキュリティバイデザインを行っているとした事業者は、ほぼ全ての事業者であり、製造・供給システムに関するドキュメントについては、全事業者において揃えられていることが確認できた。廃止した製造・供給システムの廃棄についても、全事業者において、適切に措置が講じられていた。古いOSの使用が認められ、脆弱性を内包した状態で使用されている点に注意を要するが、製造・供給システムは、他のネットワークから分離され、管理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。

- 人的対策状況については、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。従業員が必要な知識を有していない場合、外部から分離している環境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措置に支障を及ぼす可能性がある。
- システムの保守に関しては外部に委託している事業者が多く、その方法として委託事業者のリモートアクセスにより行っている事業者がある。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、接続先を限定して接続するなど措置を講じて外部からの侵入を防ぐ対策を取っている事業者が大半であるが外部のネットワークと接続する以上、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ないとは言えない。

以上のとおり、都市ガスの製造・供給システムの防護は、外部のネットワークから分離したクローズドな構成とし、外部ネットワークとの分離と人的な侵入防御を基本としている。
事業者内の他の業務ネットワークと接続がある場合でも片方向ゲートウェイ等による通信経路・方向を限定し、外部記録媒体使用時には管理された外部記録媒体に限定する等により侵入防御対策を講じており、情報セキュリティに係る教育・訓練、CSSCが主催のサイバーセキュリティ演習等の参加等により人的資質の向上にも努めている
組織体制やリスクアセスメントへの取り組み等、改善が望まれる部分は一部認められるものの、上記の取り組みにより、供給に支障が及ぶようなインシデントは発生していないことが確認できた。

4．調査のまとめ

今後のサイバーセキュリティ対策の確保に向けた課題事項①

①組織体制の高度化	②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
現状の体制は、既存の組織の枠組みの中で対応がなされているが、サイバー攻撃の多様化し、巧妙かつ複雑化していることから、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	情報セキュリティポリシー等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	リスクアセスメントについて、実施していない事業者が認められた。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	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存在する
全社的なサイバーセキュリティ体制の構築等の推進が必要であり、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	情報セキュリティポリシー等は、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。	リスクアセスメントは、インシデントが発生した際の被害等を最小限化するのに有効であるが、事業者の事業リスクの定義、設定ができていないと十分なリスク評価ができていない可能性があるので、事業リスクの設定等をした上でリスクアセスメントの実施について検討することが必要。	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

4．本調査のまとめ

今後のサイバーセキュリティ対策の確保に向けた課題事項②

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	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
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あることが認められた。脆弱性を内包した状態で使用されていることが認められた。分離等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、クローズドなネットワークであっても④の事例のように侵入される可能性はある	情報セキュリティに関する教育を実施していない事業者もあった。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。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や必要な手順書が整備されていない場合、外部との分離の維持が脅かされる可能性や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可能性がある	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した事業者等が見受けられた。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マルウェア感染の可能性が皆無とは言えない
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ことが必要	情報セキュリティ教育の充実や手順書等の整備について検討することが必要	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、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

5．都市ガス事業者への展開・反映

●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、本年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の状況。

（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「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（2016年7月最終改訂）、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

ガス業界における取組

　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。

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。