KPMG

KPMG Insight

KPMG Newsletter

Vol.19

July 2016

経営トピック⑤

重要インフラの制御システムにおける サイバーセキュリティ

kpmg.com/jp

重要インフラの制御システムにおけるサイバーセキュリティ

KPMG コンサルティング株式会社

サイバーセキュリティアドバイザリー
ディレクター　小川　真毅
シニアマネジャー　武部　達明
マネジャー　新井　保廣

近年におけるサイバー攻撃の潮流は、2000年代初頭の愉快犯や技術力誇示といった悪戯行為から、特定の組織を標的とした情報資産窃取やサービス停止を狙ったビジネス・破壊行為へと移っています。重要インフラを支える制御システムに対するセキュリティ脅威は年々増大し、プラント操業停止に至るケースも実際に発生しています。

重要インフラ事業者はサイバー攻撃の下で社会的責任をどこまで果たせるか、という大きな課題を突き付けられています。

政府は2015年にサイバーセキュリティ基本法を全面施行し、サイバーセキュリティ戦略実行の中核となる内閣サイバーセキュリティセンター（National center of Incident readiness and Strategy for Cybersecurity：NISC、以下「NISC」という）に法的権限を付与しました。今後重要インフラを防護するための政策指針が具体的に整備され、事業者自らの制御システムセキュリティ態勢強化が加速されると予想されます。

現状における政府のサイバーセキュリティ政策指針を踏まえ、国内外の業界ごとにおける制御システムセキュリティの取組みを背景に、重要インフラ事業者の取るべき対策アプローチについて解説します。

なお、本文中の意見に関する部分については筆者らの私見であることを、あらかじめお断りいたします。

小川　真毅
おがわ　まさき

武部　達明
たけべ　たつあき

新井　保廣
にいい　やすひろ

【ポイント】

- 制御システムに汎用技術が採用されて以来、サイバー攻撃による被害は年々増加の一途を辿っており、特に社会を支える重要インフラ事業者は、サイバーセキュリティ態勢についての説明責任が求められる。
- 制御システムにおけるセキュリティ統制責任は、IT部門ではなく工場の設備管理部門が有する。しかしながら同部門におけるセキュリティ意識は十分とは言えないケースも多く、IT部門との協力や、外部のサイバーセキュリティ動向を踏まえた取組みが喫緊の課題となる。
- 制御システムにおけるサイバーセキュリティ対策アプローチは、情報システムとは異なるため、情報システムセキュリティ対策はそのままでは通用しない。一例として、情報システムで利用されるアクセス制御のアクティブディレクトリは、リアルタイム応答性が遅く、操作のスピードを求められる制御システムでは受け入れられないことが多い。

I. サイバーセキュリティリスクの変遷

2010年9月、イランの核燃料施設内にある、ウラン濃縮用遠心分離機を標的としたマルウェア「Stuxnet」の攻撃により、総数約9000機のうち約1000機の遠心分離機が破損される被害が発生しました。その後、同マルウェアの亜種（派生）やさらに進んだマルウェアが作成・拡散され、制御システムを標的とするインシデントは年々増加の一途を辿っています（**図表1**参照）。

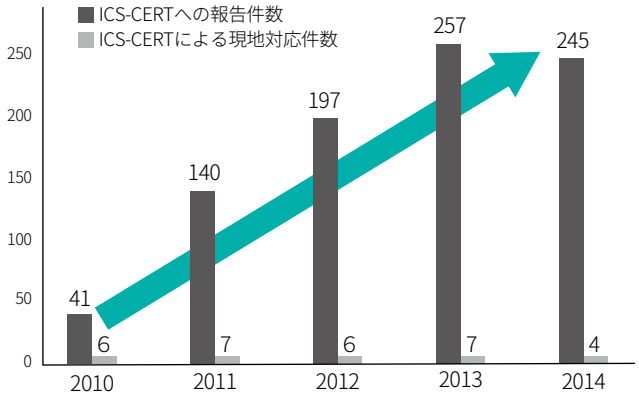
安心・安全が唱えられてきた制御システムがなぜ標的とされるようになったのか、本章ではその背景と、制御システム特有の対策課題について解説します。

1. 制御システムの変遷

従来、制御システムは独自のOSやプロトコルを採用し、情報システムから物理的に独立していました。しかしながら近年、市場からの生産性向上や利益の追求、開発コスト削減など

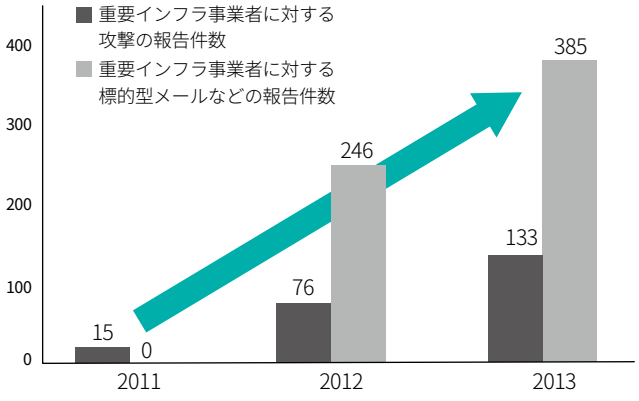
【図表1　重要インフラを対象としたサイバー攻撃の発生件数の推移】

米国における重要インフラを対象にした
サイバー攻撃の発生件数の推移



出典：ICS-CERT の公開情報より KPMG が分析

日本における重要インフラを対象にした
サイバー攻撃の発生件数の推移



出典：内閣サイバーセキュリティセンター（NISC）の公開情報より KPMG が分析

の強い要求から、制御システムベンダは制御システムに汎用的なOS、ミドルウェア、プロトコルを部品として使用し、情報システムのERP（Enterprise Resource Planning）と連携するため、汎用プロトコルを用いてネットワークと接続するようになりました。

このネットワーク接続は、情報システムにおけるサイバーセキュリティリスクが生産現場にまで持ち込まれるようになったことを意味し、旧来の安心安全神話は崩壊しつつあります。

さらに、IoT（Internet of Things=あらゆる“モノ”がインターネットに接続）が急速に発展する時代を迎え、生産現場の制御コントローラやフィールド装置などが、インターネットと繋がることで、直接の攻撃を受ける範囲が今後増えることが予測されます。

2. サイバー攻撃の矛先とされる制御システム

汎用部品で構成された制御システムが標的とされる現実は、特許レベルの生産技術情報の窃取や操業停止による事業機会損失、社会のライフラインの停止といったケースにまで及んでいます。攻撃が露見した企業は、経営への影響だけに留まらず、社会的信用や事業ブランドを失墜させ、ステークホルダーへの説明責任が求められます。

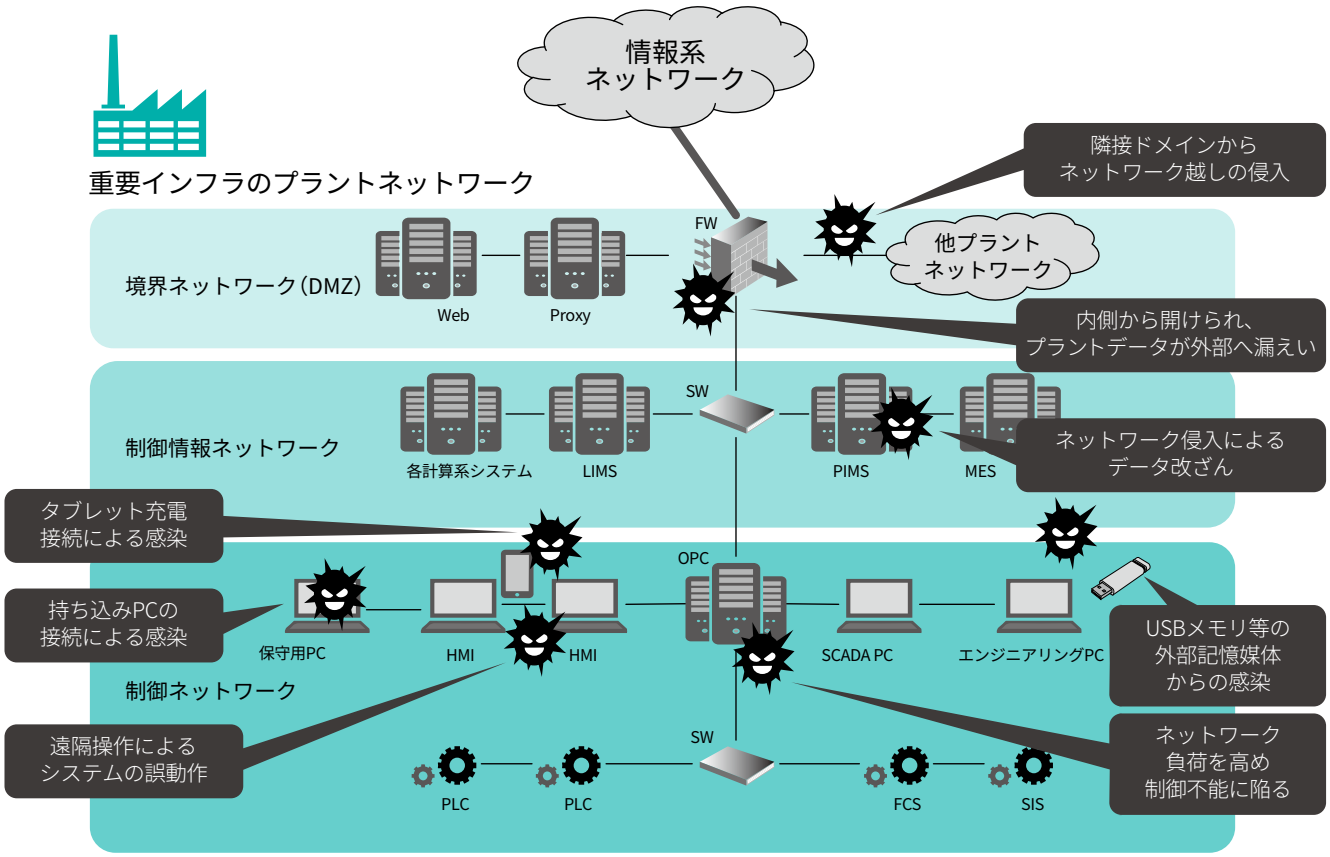
具体的な標的型攻撃の手口としては、情報システムと同様に、攻撃者は標的とする企業の社員メールアドレス等を入手し、マルウェアを添付した偽装メールを送り付け、ソーシャルエンジニアリングで対象者が開封するよう誘導して、マルウェアに感染させます。マルウェアはC&Cサーバと交信して、外部ハッカーの遠隔操作を可能にすると同時に、社内ネットワークの探索を行い、制御系ネットワークへの侵入口に到達し、内部に入り攻撃を仕掛けます。

また、制御ネットワーク内にあるマシンによく使われるUSBメモリやポータブルHDDなどの外部記憶媒体にマルウェアを忍ばせ、制御ステーション（操業監視やオペレーション専用PC）に媒体が接続された瞬間にマルウェアに感染させる事例も増えつつあります（**図表2**参照）。

3. サイバーセキュリティ対策アプローチの課題

汎用IT技術の採用により情報システムと同じ進歩を辿っていながらも、制御システムのサイバーセキュリティ対策アプローチにおいてはISMS（Information Security Management System）をそのまま適用できないという大きな問題があります。

【図表2　想定される制御システムへの攻撃例】



特に製造業の工場プラントでは、24時間365日フル稼働でなければならず、制御システムを停止させることができないため、新たな脆弱性に対応するセキュリティアップデートが世にリリースされたとしても、これを即座に適用することができません。アップデート後にシステム再起動が発生し、操業の中断に影響する怖れがあるからです。

また、制御システムの寿命は15～20年と長いため、メーカーのサポートが終了したOSを使い続けるケースも実際には多く、脆弱性を抱え込んだままで制御システムが運用され続けていることも少なくありません。もともと制御システムの開発によく使われるC言語やC++言語は知らないうちに脆弱性を混入させる性質があるため、2000年以降に発展し始めたセキュアコーディング手法を教育して従事させたり、開発されたプログラムの脆弱性をツールで検査したりして対応することが理想的です。

しかしながら、予算や時間の都合からなかなか実施できていないのが実情であり、仮にツールでソースコードを検査した場合、対応しきれないほど膨大な脆弱性が指摘されることもあり得ます。つまり、制御システムには多くの脆弱性が眠っている可能性が非常に高いのです。

このような背景から、日々高まる脅威に対し、対策を打ちやすい情報システムと比較すると、制御システムは対応が遅れがちで、未熟な攻撃でも成功し、攻撃者に達成感を与えることにもなるため、相対的に標的にされやすいと考えられます。また、リアルタイムな応答性を追求して実行スピードを落とすAntiVirusの普及が進まず、仮にインストールされていたとしても、変更を避ける傾向のある制御システムではエンジンやパターンファイルのアップデートがそれほど行われないため、古いマルウェアに感染するリスクもあります（**図表3**参照）。

最近では、インターネットに接続されている制御システム機器を検索できるWebサービスも公開されているため、攻撃対象の制御システムを探索する目的でこのようなサービスが悪用されることも考慮しておく必要があります。制御システムの形名から、製品出荷時の管理者ログイン名やパスワードが判明して、インターネットからログインできてしまう可能性もあります。

また、全社レベルのセキュリティガバナンスの中核を担うIT部門が、工場設備まで統括する権限を有していない企業が大半となっており、責任部署である設備管理部門や計装部門などでは、生産性効率や安全性が優先される結果、サイバーセキュリティに対する意識レベルがIT部門に比べて低いことも大きな課題と考えられます。

【図表3　制御システムと情報システムの比較】

サイバーセキュリティ対策の前提対比		
	制御システム	情報システム
セキュリティの優先順位	継続的な安定稼働（可用性）	機密情報の漏えい防止（機密性）
セキュリティの対象	モノ（設備・製品）サービス（連続稼働）	情報
システム更新のライフサイクル	15～20年	3～5年
システム稼働時間	24時間365日（再起動は原則許容されない）	サービス提供時間内
システム運用管理	計装部門設備管理部門	情報システム部門

Ⅱ. 制御システムセキュリティへの取組み

これまで制御システムは、セキュリティを考慮せずに設計・開発されてきました。隔離されたネットワーク環境内で使われていた当時、ほとんど問題は起きませんでしたが、昨今では汎用OS上で動作するHMIとデータをやり取りするUSBからのマルウェア侵入、制御システムネットワークに保守目的で接続したベンダPCや、生産性向上のために接続された社内ネットワーク経由でのマルウェア感染などが発生しており、制御システムにおいてもセキュリティリスクが現実の課題となりました。

1. 国家の取組み

① 米国での取組み

国家として、いち早くこの課題に取り組んだのは米国です。大統領令13010、大統領指令#63、大統領令13231が発令され、国家安全保障省（Department of Homeland Security：DHS、以下「DHS」という）が設立され、重要インフラ保護のための施策を推進してきました。国家エネルギー省（Department of Energy：DOE、以下「DOE」という）、国立標準技術研究所（National Institute of Standards and Technology：NIST、以下「NIST」という）もこれに加わり、中心的役割を果たしてきました。

DHSは、組織の連携を図る枠組み（Process Control Systems Forum：PCSF、Industrial Control Systems Joint Working Group：ICSJWG）を運営して、DHS、連邦・州・民間の研究機関、重要インフラ事業者など制御システムエンドユーザ、大学、

【図表4　DOEエネルギー供給システムのサイバーセキュリティ戦略ロードマップ】

	中期	長期	ゴール
	2013〜2017	2018〜2020	2021〜
セキュリティ文化	セキュリティ保証手法普及	セキュリティエキスパート増加	ベストプラクティス
リスク評価・監視	エンドユーザのメトリックス	運用サイド向け監視ツール	あらゆる継続的監視
セキュリティ技術開発・実装	アクセス制御、セキュア通信	自己再生システム	インシデント負荷時運用可能
インシデント管理	実時間フォレンジックス解析ツール	インシデント教訓共有仕組み	インシデント時実時間復旧
継続的改善	専門家の協力体制環境	民間投資＞政府投資	産官学連携進歩

ベンダ、システムインテグレータ、セキュリティ企業、標準団体組織の情報共有・意識向上・協力が進むよう後押ししました。DOEは、エネルギー供給システムのサイバーセキュリティ戦略として、10年単位で3ステップ（短期、中期、長期）を経て、5つの戦略を達成するロードマップを示しています（**図表4**参照）。

ロードマップのゴールが目指すのは、関係者にサイバーセキュリティのベストプラクティスを普及させるとともに、制御システムのセキュリティアーキテクチャおよび物理層でのセキュリティを日常的に評価・監視し、インシデント発生時に即時に問題点を特定して定常状態に戻せるようになることです。また、産官学が連携を取り、サイバーセキュリティ技術と対策を継続的に改善・進歩させることも挙げられています。

DHS管轄下のICS-CERTは、制御システム利用者・開発者・インテグレータなどの関係者に対して、セキュリティの意識向上・リスク識別・対応能力向上・セキュリティ技術レベル向上を狙ってトレーニングコース（入門、初級、中級、上級）を開発し、多くの関係者の啓蒙とレベル上げを行ってきています。

NISTは、SP 800シリーズ（Special Publication）として、「NIST SP 800-82 制御システムセキュリティガイド」や、汎用情報システムのセキュリティガイドとしての「NIST SP 800-53 連邦情報システムと組織のためのセキュリティとプライバシーコントロール」を発行して、制御システムセキュリティの基本コントロールについてのライブラリを提供すると同時に、重要インフラ経営者向けのサイバーリスク対応指針として、サイバーセキュリティフレームワークを作りあげました。

これは、「サイバーリスクの特定」、「資産の保護」、「攻撃検知」、「対応」、「復旧」という5つの基本機能（**図表5**参照）に、既存の標準、ガイドライン、ベストプラクティスをマッピングして整理しているフレームワークで、サイバーリスク対応機能をレベル（1[低]〜4[高]）に応じて網羅的に整備していくことでサイバーリスク管理ができるようにするものです。

このフレームワークでは、5つの機能ごとに対応が必要とされ

【図表5　サイバーセキュリティフレームワークコアの基本構造】

	機能	カテゴリー
ID	特定	資産管理／ビジネス環境／ガバナンス／リスク評価／リスク管理戦略
PR	防御	アクセス制御／意識向上・訓練／データセキュリティ／情報保護プロセス手順／保守／保護技術
DE	検知	異常とイベント／継続的監視／検知プロセス
RS	対応	計画作成／伝達／分析／低減／改善
RC	復旧	復旧計画作成／改善／伝達

NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 Table 1 より　KPMG 分析
（http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf 参照）

【図表6　ID（特定）を例としたセキュリティコントロール作成のヒント】

	機能	カテゴリー	サブカテゴリー	参考情報
ID	特定	資産管理	ID.AM-3:企業内の通信とデータの流れの図を用意している。	CCS CSC 1 COBIT 5 DSS05.02 ISA 62443-2-1:2009 4.2.3.4 ISO／IEC 27001:2013 A.13.2.1 NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
			ID-AM-4:外部情報システムの一覧を作成している。	COBIT 5 APO02.02 ISO／IEC 27001:2013 A.11.2.6 NIST SP 800-53 Rev. 4 AC-20, SA-9

NIST Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 Table 2 の一部を分析
（http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf 参照）

る項目について、参考にすべき各種業界ベストプラクティスやガイドラインが列挙されているため（**図表6**参照）、これらを参考にリスク管理策の実装を進めることができます。

② ヨーロッパでの取組み

英国、ドイツ、スウェーデン、オランダ、フランス各国が制御システムセキュリティについての活動をしていますが、欧州全体に渡ると、メリディアンプロセス、ENISAといった団体が活動を行い、成果物を公開しています（**図表7**参照）。

なかでも英国のCPNI（Centre for the Protection of National Infrastructure：国家インフラ防御センター）の発行した9分冊より構成される「グッド・プラクティス・ガイド、プロセス制御とSCADAセキュリティ」は、一般ガイダンス、ビジネスリスクの理解、セキュアなアーキテクチャの実装、ファイアウォールの適用、応答能力の確率、意識と熟練度の改善、サードパーティの管理、プロジェクト従事、継続統治の確立といったテーマ別に要点をまとめており、充実しています。

フランスの制御システムセキュリティスタートガイドは、既に発行された制御システムセキュリティ標準、推奨策などのドキュメントを、いくつかの属性を使って分類しているため、必

【図表7　ヨーロッパの制御システムセキュリティ業界活動状況】

国	組織*	成果物	特徴
英国	CPNI 旧NISCC	制御システムSCADAセキュリティ　安全策ガイド	カバレッジが広く、ヨーロッパのガイドラインのなかでは一番充実している。
		一般ガイダンス	
		1 ビジネスリスクの理解	
		2 セキュアなアーキテクチャの実装	
		SCADAと制御システムネットワークへのファイアウォールの適用	
		3 応答能力の確立	
		4 意識と熟練度の改善	
		5 サードパーティの管理	
		6 プロジェクト従事	
		7 継続統治の確立	
ドイツ	BSI	BSI 100-1（ISMS） BSI 100-2（IT-Grundschutz Methodology） BSI 100-3（Risk analysis on IT-Grundschutz Methodology） BSI 100-4（Business Continuity Management）	BSIが制御システムセキュリティについての主導的役割を果たすが、2大制御システムベンダ（ABB、Siemens）は国際標準団体（IEC TC65／WG 10、IEC TC 57／WG 15、ISA 99）で、多国籍企業の強みを活かして、IEC 62443、IEC 62351などに影響力を持つ。
スウェーデン	MSB	Guide to Increased Security in Industrial Control Systems	NERC CIP-002~009、NIST 800-82、CPNI GPG、などの知見をPDCAの継続的改善のフレームワークで整理している。
オランダ	TNO		重要インフラセキュリティに対する取組みに特に力をいれている。オイルメジャーの存在が大きい。
フランス	CLUSIF	Cyber Security of Industrial Control Systems: How to get started?	既存のガイドラインをいくつかの属性で分類しているので、必要なものを探すときに便利。
欧州全体	Meridian Process		各国政府機関が重要インフラを保護するために情報共有する。国レベルでの協力を行っている。
	ENISA	Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors	制御システムのセキュリティについても調査し、白書を出している。

＊組織の略語一覧
- CPNI（国家インフラ防御センター）
  Centre for the Protection of National Infrastructure
- NISCC（国立インフラセキュリティ協調センター）
  National Infrastructure Security Co-ordination Centre
- BSI（連邦情報セキュリティ局）
  Bundesamt für Sicherheit in der Informationstechnik
- MSB（スウェーデン市民緊急省）
  Myndigheten för samhällsskydd och geredskap
- TNO（オランダ応用科学研究機構）
  Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek
- CLUSIF
  CLUB DE LA SECURITE DE L’INFORMATION FRANÇAIS
- ENISA（欧州ネットワーク情報セキュリティ庁）
  European Network and Information Security Agency

要とするドキュメントを探すときに役立ちます。

③ 日本での取組み

国内では、2014年11月にサイバーセキュリティ基本法が全面施行され、内閣総理大臣直下の戦略組織としてサイバーセキュリティ戦略本部を発足しています。その司令塔は法的に然るべき権限を付与されたNISC（内閣情報セキュリティセンター）が担うこととなっており、NISCはサイバーセキュリティ戦略において重要インフラ防護をテーマとした第1次～3次行動計画を策定しています。

第3次行動計画は、重要インフラ13分野（電力、ガス、石油、化学、鉄道、航空、水道、医療、情報通信、金融など）に対して、安全基準等の整備・浸透、情報共有体制の強化、障害対応体制の強化、リスクマネジメント、防護基盤の強化を柱として、官民連携による重要インフラ防護を推進するためのものです。

一方で経済産業省は、システムセキュリティ検証や国際規格準拠の認証制度の確立、人材育成などを目的とした技術研究組合制御システムセキュリティセンター（Control System Security Center：CSSC、以下「CSSC」という）を設立しています。さらに、制御システムセキュリティの組織プロセスに係る認証プログラムCSMS（Cyber Security Management System for Industrial Automation and Control System：IEC62443-2-1基準）をスタートさせ、重要インフラ事業者は社会的信用を確保する狙いとして、今後CSMS認証取得や認証取得製品の調達などを求められることも予想されます。

2. 各業界における取組み

制御システムの消費者として、電力・石油・ガス・化学・薬品・上下水道・公共交通などの重要インフラ事業者があります。このなかには、業界単位で活動を行っているものもあります。

（1）海外における取組み

電力・石油・ガス・化学・薬品・上下水道・運輸鉄道・通信という業界ごとに、制御システムセキュリティのプロジェクトがいくつか立ち上がりました。

Instrumentation Society of Automation（ISA）は、制御システムに関する各種標準を作成しており、そのなかのISA99がセキュリティ標準、ISA62443シリーズ（旧ISA99シリーズ）を作成しています。これはIEC TC 65／WG 10にて審議され、IEC 62443シリーズとして国際標準として発行されます。

① 電力業界

電力業界では、規模の異なる多数の電力供給業者のセキュリティ信頼性を確保するため、北米電力信頼度評議会（North American Electric Reliability Corporation：NERC）がNERC CIP（Critical Infrastructure Protection）というセキュリティガイドラインを制定しており、現在のVersion 5は法的強制力を伴う監査に使用されることになっています。

NIST は、スマートグリッドに関するセキュリティガイドラインとしてNIST IR 7628 を公開しました。これには、電力市場7ドメイン（**図表8**参照）での相互運用性、各ドメイン間サービス、ユースケースの列挙とセキュリティ要件の分析などが書かれています。

【図表8　NISTスマートグリッド概念モデルの7ドメイン】

電力事業者	発電 送電 配電 運用
サービス事業者	取引所 サービスプロバイダ
需要家	顧客

スマートグリッド相互運用性パネル（Smart Grid Interoperability Panel：SGIP）のサイバーセキュリティ作業部会（Cyber Security Working Group：CSWG）は、ユースケースによるリスクチェックと、既存のスマートグリッド標準に基づく適合性評価をできるようにしています。同時に、スマートメータ（Smart Meter）用ファームウェアのセキュリティバグを安全に遠隔アップデートできるよう、高度検針インフラストラクチャー（Advanced Metering Infrastructure：AMI）のテストフレームワークも用意しています。

欧州では、スマートグリッドをベースに発展してきた国内向けのISMS規格を国際標準化組織（ISO／IEC JTC 1 SC 27／WG 1）に提案し、国際標準ISO／IEC 27019として、エネルギー供給事業者、エネルギーサービス事業者向けのISMSとして使われる可能性も出てきました。

② 石油・ガス・化学業界

石油・ガス業界では大学の研究機関主導のプロジェクトであるI3Pにおいて、制御システムセキュリティのリスク分析・相互依存・メトリックス・セキュリティツール・情報共有・技術移転の6つの分野で研究が進められています。

LOGIIC（Linking the Oil and Gas Industry to Improve Cybersecurity）は、オイルメジャー・制御システムベンダ・研究機関・セキュリティベンダ・DHS S&T（Science and

Technology）らが行っているプロジェクトで、セキュリティのテーマについて研究・対策を発表しており、現在までに以下の6つのプロジェクトを終了し、レポートを公開しています。

1. 社外・社内に流れるネットワークパケットの相関から迫り来る危機を予測する
2. 制御システムが乗っ取られたときに制御システムを監視する安全システムが正しくプラントをシャットダウンできるか
3. STUXNETの出現で脚光を浴びたアプリケーションホワイトリスティングの評価
4. 制御システム専用ワイヤレスシステムの攻撃耐性評価
5. HMI等を仮想化したときのセキュリティ評価
6. リモートアクセスセキュリティ評価

LOGIICでは、制御システムセキュリティに有効な対策とその効果を、参加協力ベンダのシステムで実証しているところが特徴となっています。

ISA99の進捗を加速し、制御システムのセキュリティ認証を望んでいたオイルメジャーは、ISAセキュリティ適合機関（ISA Security Compliance Institute：ISCI、以下「ISCI」という）を制御システムベンダとともに立ち上げ、ISA99で作成しているIEC 62443シリーズをベースにしたセキュリティ評価・認証をするための、制御機器のセキュリティ評価基準、制御システムの評価基準とフレームワークを作り上げました。

これにより、一定のセキュリティレベルの確認が取れた制御機器デバイスが認証され、評価の途中で発見された制御システムにおけるセキュリティ上の問題が、少しずつ解消されていく見通しが立ってきました。

化学業界では、化学産業データ交換（Chemical Industry Data eXchange：CIDX）という非営利団体がCybersecurity Vulnerability Assessment Methodologiesでサイバーセキュリティ上の脆弱性を評価する手法をまとめ、制御システム特有のマネジメントに関する標準としてIEC62443-2-1が策定され、現在活動はChemITCという団体に引き継がれています。

③ 自動車業界

自動車に関する安全システムを規定したISO26262に対するセキュリティ規格としてSAE International J3061というものがあります。これは、自動車組込システムにかかわる生産プロセスに対するセキュリティ適用、自動車用組込システムの堅牢性を評価するツールや手法、サイバーセキュリティの取組みや基本原則、サイバーセキュリティを前提とした開発標準のあるべき姿、方向性の指針などについて記述したもので、自動車ライフサイクルのセキュリティ標準としての活用が期待されます。

また、自動車セキュリティに関する別のプロジェクトとして、ハードウェアセキュリティモジュールの規格を提唱したEVITA、セキュアかつスケーラブルなV2X（車と他の通信、Vehicle to X Communication Systems）を目指したPRESERVE（Preparing Secure Vehicle-to-X Communication Systems）といった取組みも注目を集めています。

④ 鉄道業界

鉄道業界では、アメリカ公共交通協会（American Public Transportation Association：APTA、以下「APTA」という）がガイドラインを出しています。運用制御センター・信号・駅・駐車場・案内表示ディスプレイ・チケット販売などのシステムを、サブシステム（ゾーン）として分割し、ゾーンのセキュリティを確保してゾーン間でのデータ通信を保護する方式を提示しています。

（2）国内における取組み

国内の制御システムセキュリティについての活動は、2007年～2008年頃から活発化しました。内閣官房はサイバーセキュリティ戦略で重要インフラ防護をテーマとし、経済産業省は制御システムセキュリティ検討タスクフォースを設置しました。独立行政法人情報処理推進機構（IPA）は、国内外の制御システムセキュリティについて報告書を公開しています。一般社団法人JPCERTコーディネーションセンター（JPCERT／CC）は、制御システムセキュリティ関連ドキュメントのいくつかを翻訳し、公開しています。

制御システムのセキュリティ保証をするために、CSSCが国家プロジェクトとして設立されました。CSSCは、ISAセキュリティ適合機関（ISCI）と同じ評価を行って相互認証（日本での認証が米国でも同じ認証として通用し、米国の認証も日本で同じ認証として通用すること）されるようにフレームワークを構築しています。

NISCが策定した第3次行動計画で示されるように、指定された各重要インフラ事業分野が、各分野内や分野間における情報共有・インシデントの未然防止・インシデント発生時の被害拡大防止・迅速な復旧などを目的として、これらの機能を担うセプターと呼ばれる組織を各事業分野に立ち上げており（**図表9**参照）、各セプター代表で構成されるセプターカウンシルという協議会が中核の運営組織として位置付けられています。

なお、各事業分野においてガイドライン策定や整備が進められていますが、事業者レベルでのガイドラインに沿った態勢強化施策の浸透は、これから本格化していくと見受けられます。

① 電力業界

電力業界では、「重要インフラの情報セキュリティ対策に係る行動計画」に基づき、電気事業連合会（電事連）で自主ガイドラインを作成して、電力各社が取組みを開始しました。情報共有

の仕組みを用意し、NISC、CSSCのサイバー演習に参加しています。

電力はすべてのインフラの根幹であり、古くから多様な制御システムを使用しているため、米国でのNERC-CIPの法的規制をはじめ、主要各国の動向も鑑みながらサイバーセキュリティへの対策についても先行して進んで行くことが予想されます。

② 石油業界

石油業界では、業界を先行して石油連盟がいち早く国際規格IEC62443-2-1をリファレンスとした自主ガイドラインを策定しており、同規格に準拠したCSMS認証取得に関心を示す企業も増えつつあります。特に、欧州石油メジャーが制御システムセキュリティの先進的な取組みを進めており、セキュリティ製品を調達する際の基準（例として、WIB認証取得を条件としている）を定めています。

一方で石油プラントをグローバルに統合監視するSOC（Security Operation Center、以下「SOC」という）を立ち上げた企業もあることから、これらのセキュリティ意識の高い欧州に追随する動きを示しているように見受けられます。

③ ガス業界

ガス業界では、「重要インフラの情報セキュリティ対策に係る行動計画」に基づき、主要10社で情報収集・分析の枠組みを整備しており、内閣サイバーセキュリティセンター主催分野別横断演習（平成26年12月）や都市ガス分野の訓練（平成26年10月）で得られた知見などが共有されています。

また、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ガイドライン」を策定しており、主要ガス事業者（10社）はこのガイドラインに基づいて社内規定を定める方針であると報じられています。

このなかで、国内の大手都市ガス会社は、IEC62443-2-1をベースにしたCSMS認証を取得したことが明らかになりました。今後、他のガス会社も同認証を取得していくことが予想されます。

また、セキュリティリスクを自主的に研究して、制御システムの脆弱性検査の調査を開始している事業者もあります。

Ⅲ. 重要インフラ事業者が採るべきアプローチ

1. 要諦となる経営陣の意識改革

重要インフラ事業にとって、経営上、サイバーセキュリティ活動は経済的利益にならないと捉えられ、多くの経営陣にとって技術的に難解であることから、対応が後手に回りがちです。しかしながら、なおざりにしたときにインシデントが発生した場合のインパクトは、経営を大きく揺るがすことになります。インシデントの発生や被害の拡大を防ぐためには、従業員全員が一丸となってセキュリティに取り組むことが不可欠であり、経

【図表9　主な重要インフラ事業分野における取組み】

重要インフラ分野	セプター名称	事務局	取組み内容
電力	電力 CEPTOAR	電気事業連合会	NERC（北米電力信頼度協議会）が作成したガイドライン、CIP（Cyber-Security Critical Infrastructure Protection）をリファレンスとして、日本版 CIP のサイバーセキュリティガイドラインの策定を進めている。ガイドラインの主な項目として、行動計画・リスクアナリシス・対策立案・個別対策・人材育成・危機管理 などが挙げられている。
石油	石油 CEPTOAR	石油連盟	「石油分野における情報セキュリティ確保に係る安全ガイドライン」を発行。 また、JPCERT／CC が提供する制御系システムのセルフアセスメントツールである J-CLICS を使った一斉調査を実施。
ガス	ガス CEPTOAR	日本ガス協会	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発行。 CSSCガス分野サイバー演習への参加や、事業者横断的なインシデントハンドリング演習を定期的に開催。
化学	化学 CEPTOAR	石油化学工業協会	NISCが策定した安全基準等の指針に基づく浸透状況の調査やJPCERT／CC提供のJ-CLICSを使った一斉調査の実施。 CSSC化学分野サイバー演習への参加。
鉄道	鉄道 CEPTOAR	国土交通省	NISCが策定した安全基準等の指針に基づく「鉄道分野における情報セキュリティ確保に係る安全ガイドライン」を発行。

営陣が主体的にリーダーシップを発揮することが強く求められます。

ゴーイングコンサーンとしての事業継続責任を全うするためには、サイバーセキュリティ態勢強化に取り組むことが必要であり、そのためにはまず経営者自身による理解が必要です。そのうえで然るべき経営資源を投入し、経営にかかわるリスクを評価して、リスクに対応できるようセキュリティ組織（発生したセキュリティ問題に対処するCSIRT：Computer Security Incident Response Team、セキュリティ監視を行うSOC）を構築する必要があります。

さらに、サプライチェーンとなるパートナー企業を含めて事業継続計画・管理を行うことができるように組織改革することが肝要であり、そのためには、専門家の知見を活用し、人材教育・訓練・育成や、セキュリティリスクに対する経営体力を醸成することも求められます。

重要インフラ制御システムのセキュリティリスクを考慮すると、制御システムのリスクレベル別の分割（ゾーン）、ゾーン間通信の保護、マルウェア対策、バックアップと復元、定期保守点検などを利用したパッチ適用計画、ディザスタリカバリ、リモートアクセスの制限と監視、制御システム導入時の侵入試験などのコントロールを制御システムセキュリティ標準から選択して、ベンダ、システムインテグレータ、保守サービス事業者等の支援と協力の基に適用することがセキュリティ改善のヒントとなります。

経済産業省がスタートしたCSMSでは、経営陣の承認に基づく「事業上の根拠の策定」から開始するようにガイドされています。

すなわち、経営陣は社会責任や経営責任を鑑みて、セキュリティ対策強化に取り組む指針を明確に宣言する必要があります。経営陣はこの指針にしたがって、効率的に組織を再構築する支援を遂行しなければなりません。また事業に関与するステークホルダーすべてがこの指針を理解し、対策方針や対策標準・対策基準といったセキュリティポリシー策定から、ポリシーに準じた態勢作りに取り組むことが必要です。

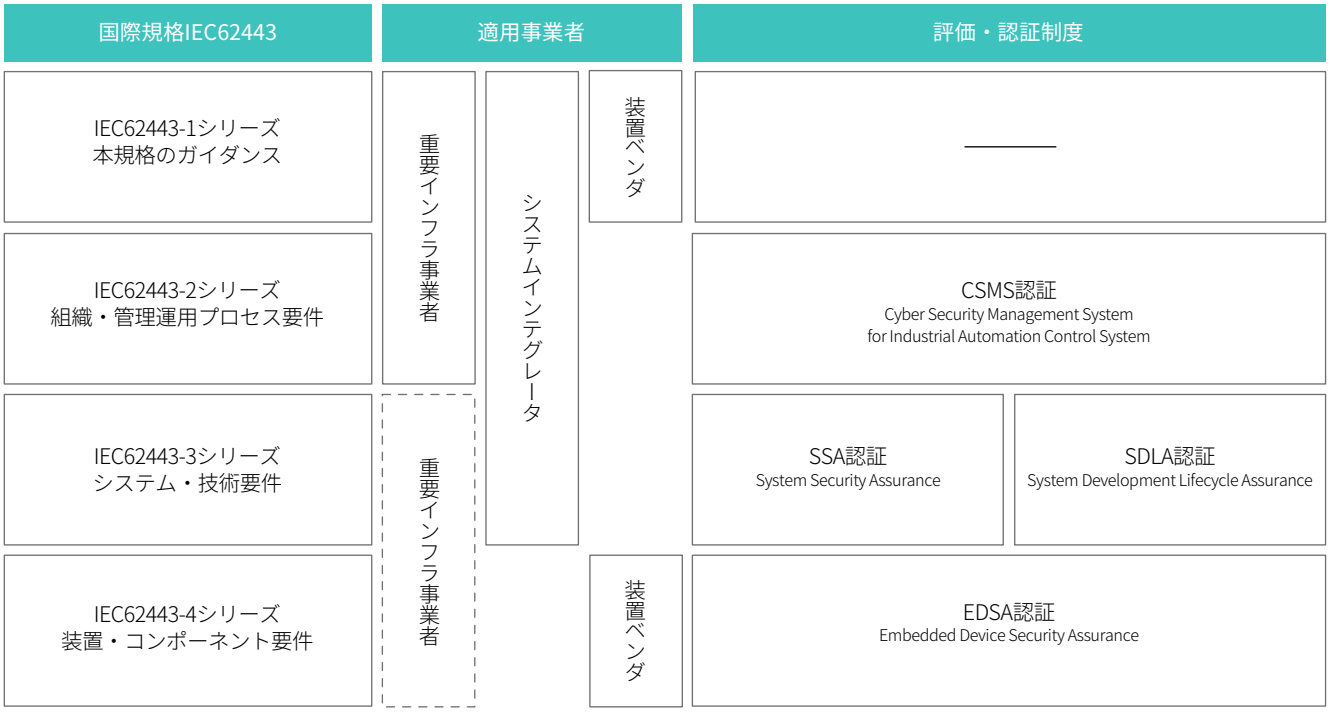
2. ガイドライン活用による態勢強化

制御システムでは情報システムセキュリティの対策アプローチをそのままでは適用できないことから、Ⅱ章で紹介したような各ガイドラインを参照した取組みが、成功への近道と言えます。ここでは、各ガイドライン活用のポイントについて解説します。

（1）セキュリティフレームワーク確立

サイバーセキュリティ全般のフレームワーク、つまりPlan（計画）・Do（実施）・Check（点検・監査）・Action（改善）のPDCAサイクルの管理策については、特に業界ごとに異なるフレームワークが存在するものではなく、ISO／IEC27001、27002をベースにした汎用制御システム向けセキュリティマネジメントの国際規格IEC62443-2-1を利用することが基本となります。さらに、

【図表10　IEC62443とその評価・認証制度の全体像】



自社のサイバーセキュリティ態勢について社会的な信用を得るためには、IEC62443-2-1をベースとしたCSMS認証基準に沿った取組みも推奨されます。

セキュリティフレームワークを確立するにあたっては、日々高まる脅威に対抗した継続的な態勢改善プロセスを備えることが最大のポイントと言えます。

(2) ガイドラインの活用

IEC62443-2-1ではひととおりの管理項目が網羅されていますが、具体的な管理手法のレベルまでは触れられていません。そのため、識別認証やアクセス制御、操作制御などの技術対策要件については、IEC62443-3-3や、ISCIのEDSA・SDLA・SSAなどを参照することが求められます。特にISCIの管理基準に基づく認証制度も国内において確立しつつあり、調達・外部委託の観点から、システム製品やシステムインテグレータの選定基準として、これらの認証取得を条件に含めることも有効であると考えられます(**図表10**参照)。

業界固有のリファレンスとしては、LOGIIC(石油業界)やAGA12(ガス業界)、APTA(鉄道業界)などがあります。たとえばLOGIICでは、特に制御システムのセキュリティ対策に効果のある対策を選定して評価しています。各企業は、これらの対策を適用する際に、自社の制御システムのリスク評価、リスクレベルごとによるシステムの分割(ゾーニング)、システム間通信のセキュリティ(コンジット)対策を実施し、制御システムへの高度なセキュリティ管理策を順次導入していくこと、つまり、自社における現状のサイバーセキュリティリスクを把握したうえで、適用すべき対策を吟味することが制御システムにおける最適なサイバーセキュリティ環境実現に向けた重要な一歩となります。

サイバーセキュリティサーベイ2016

2015年6月刊

目次

サイバー攻撃は企業にとって、事業継続上、深刻なダメージを引き起こすものであり、その対応は社会的に喫緊の課題となっています。本報告書は、「KPMGグローバルCEO調査2015」から得た、グローバル企業におけるサイバーセキュリティに関する対応調査(有効回答:1276名)、ならびに国内大手企業の情報システム部門責任者を対象に実施したサイバーセキュリティに関する対応調査(有効回答:363名)から構成されています。

資料請求はこちらのウェブサイトからお願いいたします。

http://www.kpmg.com/jp/cybersecurity-survey-2016

【バックナンバー】

サイバーリスク最新トレンドと対応戦略
(KPMG Insight Vol.15/Nov.2015)

サイバーインテリジェンス活用戦略
(KPMG Insight Vol.16/Jan.2016)

サイバーインシデント対応戦略
(KPMG Insight Vol.17/Mar.2016)

サイバー イン ザ ボールドルーム
(KPMG Insight Vol.18/May.2016)

本稿に関するご質問等は、以下の担当者までお願いいたします。

KPMG コンサルティング株式会社
ディレクター 小川　真毅
masaki.ogawa@jp.kpmg.com

シニアマネジャー　武部　達明
tatsuaki.takebe@jp.kpmg.com

マネジャー　新井　保廣
yasuhiro.niii@jp.kpmg.com

サイバーセキュリティアドバイザリー
cybersecurity@jp.kpmg.com

KPMGジャパン

marketing@jp.kpmg.com
www.kpmg.com/jp