❻ 重要インフラにおける取組みと展望

応用

後藤厚宏（情報セキュリティ大学院大学）

重要インフラのセキュリティ

東京オリンピック・パラリンピック大会を迎える 2020 年，および，その将来に向けて，社会生活と産業を支える重要インフラ ☆1 において世界最高水準の総合的なサイバーセキュリティを確保することを目指す包括的な取組みとして，内閣府の戦略的イノベーション創造プログラム SIP ☆2「重要インフラ等におけるサイバーセキュリティ確保」（以降“SIP サイバー”）の研究開発が進められている [1]．

本稿では，重要インフラのサイバーセキュリティ確保に向けて，対策技術を検討する上で考慮すべき重要インフラの要件を示し，その観点から SIP サイバーでの包括的な取組みについて，背景となる問題意識，取組みの狙いや目標について概説する．最後に，今後の重要インフラのサイバーセキュリティ確保に向けて総括的に展望をまとめる．

重要インフラの制御ネットワーク

現代の重要インフラでは事業の生産性向上のために，多数のインフラ設備を運用監視センターから遠隔制御する“制御ネットワーク”を導入している．通信網，鉄道網，電力網 ☆3 等のように，設備自体が大規模である重要インフラにおいては，それを運用するための制御ネットワークが大規模化・広域化しており，制御ネットワークを構成するサーバやスイッチの機器数は数千台規模に達する（図 -1）．

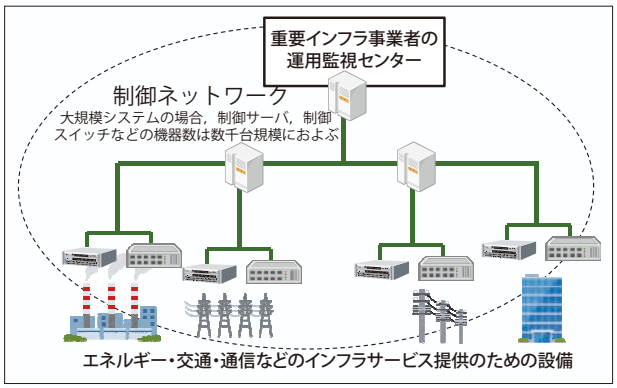

図 -1　大規模な制御ネットワーク

制御ネットワークのオープン化と IoT 活用

これまで，工場や重要インフラのプラント設備は，それぞれの事業設備（例：タービン，ポンプ，変圧器など）だけでなく，制御ネットワーク ☆4 の機器も，事業者ごとに専用の機器が使われることが多かった．

近年，監視センターの HMI ☆5 から PLC ☆6 を含む制御ネットワーク機器の機能と性能の向上や設備投資の抑制のために，標準品の利用が進みつつある．制御ネットワークのプロトコルも IP ベースに移行しつつあり，オフィスの ICT 環境と共通の技術や機器の利用が増えている．今後は，さらに事業効率の大幅な向上が期待される IoT の活用が広がる．

サイバー攻撃リスクの高まり

制御ネットワークとそのオープン化は，サイバー

☆1 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，2017 年 4 月，http://www.nisc.go.jp/active/infra/pdf/infra_rt4.pdf
☆2 Cross ministerial Strategic Innovation Promotion Program（SIP）
☆3 東京電力の次世代監視制御システム，http://www.tepco.co.jp/press/news/2016/pdf/160318a.pdf
☆4 重要工場等の制御システムでは，監視制御システム（SCADA：Supervisory Control And Data Acquisition）
☆5 HMI：Human Machine Interface
☆6 PLC：Programmable Logic Controller

攻撃リスクを高める方向にも作用する．

重要インフラの制御ネットワークが，その事業者のオフィスと接続されている場合，オフィスのPCが外部からサイバー攻撃され，それらのPC経由でIPベースの制御ネットワークに侵入されるリスクが高い．このため，制御ネットワークと外部ネットワークを物理的に隔離する“エアギャップ”を設け，常時接続しない構成が多い．

ただし，エアギャップを設けている場合でも以下の事例のようにサイバー攻撃リスクをゼロにすることはできない．

- 保守作業時の外部ネットワークとの一時的な接続やUSBメモリなどの利用（STUXNET事例[☆7]）
- 内部犯行によるもの（オーストラリアにおける下水処理場の事案[☆8]）
- 設備機器の調達時に，サプライチェーンにおいて事前に埋め込み[☆9]

重要インフラの制御ネットワークは，エアギャップの有無にかかわらず，設備の構築作業，保守点検や設備機器の更新作業など，インフラ事業者の業務の中で外界と接点を持つ．このため，制御ネットワークの外部環境を含めたセキュリティ対策が必要になる．

サイバーセキュリティ確保の要件

重要インフラのサイバーセキュリティ確保においては，重要インフラ全体のリスク分析の中で，サイバーセキュリティのインシデント[☆10]によって引き起こされる重要インフラとしての事故のリスクを洗い出し，リスクを低減するセキュリティ対策とインシデント発生時の対処策を考えることになる．その際，以下に示す重要インフラとしての「要件」について考慮しなければならない．

サービスの優先事項

重要インフラにおいては，それぞれのサービス提供における優先事項があり，セキュリティ対策の考え方や，セキュリティインシデント時の対処の考え方が，通常のオフィス系のITシステムと異なる．たとえば，発電プラントのように「停めることがきわめて困難な設備」にセキュリティ脆弱性が見つかった場合やインシデントの兆候が検出された場合，それが要因となるサービスのリスクと，対処のために設備を停止することがサービスに及ぼすリスクの双方について総合的に判断する必要がある．

また，それぞれの重要インフラでは，優先事項を損なう事故（アクシデント）に備えた設備ごとの対処策として，電力網ではブレーカー，鉄道網では緊急停止装置等が備えられている．個々の設備に備えられた緊急対応装置は，機器の故障などを想定し，自律的に動作することによって事故を回避する役割を持つ．このため，制御ネットワークのセキュリティインシデントを検出した際の対処などでは，インフラ設備の緊急対応装置との連携と，相互干渉の回避が必要になる．

ライフサイクル

電力や鉄道などの大規模な重要インフラシステムでは，インフラ設備の寿命は，数十年単位であり，常時，導入年代の異なる新旧機器が混在している．また，それらの設備の投資コストが大きいため，中長期計画に基づいて設備更新が進められている．また，設備更新に合わせた計画的な人材確保と人材教育が重視されている．

このため，制御ネットワークのセキュリティ対策においても，設備機器の更改に伴う対策と，現用機器を前提とした対策の両方について進める必要がある．

サプライチェーン

重要インフラ設備は，その調達のサプライチェーンが多段かつグローバルに分散しているため，サプライチェーンにおいて悪意ある機能が組み込まれるリスクが大きい．また，ライフサイクルの長さから，

☆7 https://www.ipa.go.jp/files/000024792.pdf
☆8 http://www.nhk.or.jp/gendai/articles/3221/1.html
☆9 https://www.ipa.go.jp/files/000058299.pdf
☆10 制御システム等では，「事故などが発生するおそれのある事態」をインシデントと呼び，事故（アクシデント）と区別する

調達時に確認できなかった脆弱性が，数年後に表面化するため，設備機器の供給ベンダとインフラ事業者間の密な連携体制と，長期にわたる機器の保守体制が必須である．

今後は，インフラ設備のさらなるオープン化に加え，IoT を活用したインフラ設備の運用効率の向上や，設備のフィールド保守点検における Pad 型端末の活用[2]など，従来とは異なる機器の導入が見込まれるため，サプライチェーンのリスク管理がさらに重要になる．

組織構造

通信，電力，鉄道などに代表される大規模事業者は，長年にわたってインフラの安全な運用やサービス提供の安定性に適した組織体制を築いてきた．そこでは，設備機器の保守点検の確実な実施や機器の故障対応，台風や地震などの自然災害への適切な対応に重点が置かれてきた．

今後は，機器故障，人為的な事故，自然災害などのリスク対応に加え，サイバー攻撃のリスクが加わることになり，監視・防御技術の導入だけでなく，組織体制・運用体制としてのサイバーセキュリティ対応が必要になる．これは事業者の組織構造全体の見直しを意味している．

SIP サイバーの取組み

SIP サイバーでは，サイバーセキュリティの技術・導入・運用手順から人材までの包括的な研究開発を進めるとともに，国内外の優れた技術・ノウハウの受け皿になり得るための枠組みを重要インフラ事業者に提供することを目指している．

SIP サイバーにおける，前節の重要インフラの要件への対応を図 -2 に示す．以降，要件に対応した取組みの考え方について述べる．

総合的リスク分析と適合性，評価検証

重要インフラの要件に適合したサイバーセキュリティ確保のために，それぞれの事業者は当該インフラとして優先すべきサービス要件（安全性，安定性，一貫性など）に沿った事業全体のリスク分析を実施する．リスク分析は，その事業分野の専門家と，セキュリティの専門家の合同チームが実施し，そのリスク分析に沿って，インフラ事業（分野）ごとにサイバーセキュリティ確保のための機能を導入する．

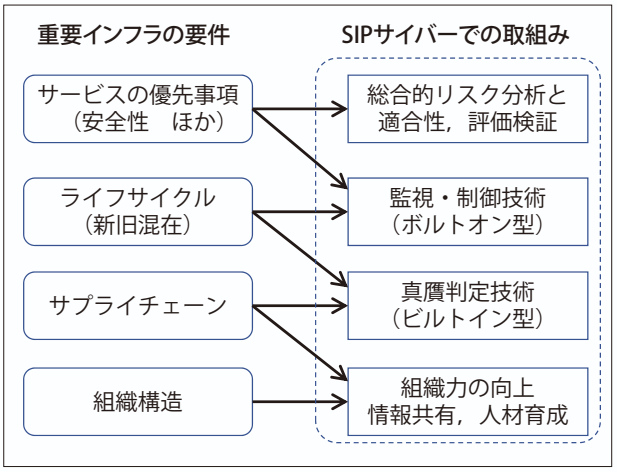

図 -2　重要インフラの要件と SIP の取組み

リスク分析結果に沿って，重要インフラの制御ネットワークに，サイバーセキュリティ確保のための機能を取り入れる際は，当該インフラ事業にとっての優先事項に悪影響を与えないことを確認・評価する必要がある．さらに，組織の運用体制（現場技術者の運用手順書などを含む）を混乱なく拡張・融合しなければならない．

以上のために，SIP サイバーでは，主要な重要インフラ事業について，マクロなリスク分析を実施し，重要インフラとしての優先事項の抽出を具体的に行い，そのインフラのセキュリティ確保のために実装すべき機能の適合性と評価を行っている．これらの取組みは，後述の組織力向上の取組みと合わせて「社会実装技術」と呼んでいる．

外部からのサイバー攻撃に向けた「砦」の強化

サイバー攻撃から制御ネットワークを守るためには，“エアギャップ”の有無にかかわらず，重要インフラ設備に関係を持つ事業者のオフィスの IT システムや，インフラ設備の保守点検のための機器等，設備の周辺環境のセキュリティ確保が必要である．

また，インフラ設備の物理環境に外部者の立ち入りを防ぐ対策や，そのための監視カメラ網やセンサ網などが重要となる．

このような「砦」のための対策技術は，通常の企業 IT システムで活用されているさまざまな対策技術や組織マネジメントの取組み，さらには海外を含め，外部の対策技術が活用できる．

制御ネットワークの「免疫力」の強化

重要インフラ設備，特に制御ネットワークでは，砦が破られた場合でもインシデントを未然に防ぐことや，インフラとしての事故（アクシデント）を引き起こす前にインシデントを検知し，対処する免疫力が必要である．

免疫力の強化は対策技術の設備内部への導入や，設備の内部情報の分析を伴う．その際，インフラ設備の構成情報や監視情報が守秘対象であることに注意が必要である．このため，外部の対策技術が活用しやすい「砦」に対し，免疫力の強化技術は外部依存せず事業者自らが主体的に取組む必要がある．

ビルトインとボルトオン

制御ネットワークのサイバーセキュリティ強化は，インフラ設備のライフサイクルが長く，新旧混在環境であることを踏まえ，2 つの観点から考える必要がある．

ビルトイン（built-in）

1 つはシステムの構築時にセキュリティ機能を当該システムに“ビルトイン”する対策である．SIP サイバーでは，制御ネットワークの免疫力強化のために，サプライチェーン上での改変や運用時のマルウェア等の混入を検知して異常動作を阻止する「真贋判定技術」の開発に取り組んでいる．本機能は脆弱性対応などの保守作業において，システム機能を正しく更新する仕組みとしても有用である．

本技術は，各機器が内蔵するセキュリティモジュールを活用して「信頼の連鎖」を構築し，真贋判定の基準とする検証情報を安全かつ効率的に伝搬・共有できる機能をシステムに作り込む．これにより，システムの運用時に，上位の機器にあらかじめ登録された検証情報を下位の各機器が自動的に入手することによって真贋判定（改ざん検知）を実現する．

本技術を重要インフラ事業の中に実装する場合，設備の更改は十数年単位で行われるため，事業者が計画的に進めることが必要である．また，技術導入の促進には，業界としてのセキュリティガイドラインの整備，認証制度や適合性確認制度を通した側面支援が求められる．

ボルトオン（bolt-on）

設備のライフサイクルが長い重要インフラにおいては，ビルトイン型のセキュリティ対策の導入と並行して，非更改システムの免疫力を強化するボルトオン（bolt-on）型の対策が必要である．

SIP サイバーでは，制御ネットワークの挙動を監視して，セキュリティインシデントを早期に検知できる技術に取り組んでいる．本技術開発においては，検知性能に加え，重要インフラ向けの機能として満たさなければならない 2 つの要件への対応に重点を置いている．

1 つは検知のためのプローブ機器等が現用システムに与える影響を皆無にすることである．本技術は，ちょうど聴診器のようにシステム状態を収集し，取得できる情報が限られる中，異常（インシデントの兆候）を検出できることを目指している．

2 つ目は現用システムに当初から組み込まれている監視機能等（故障検知など，サイバーセキュリティ監視を主目的としないもの）との技術面での協調とオペレーション手順としての協調である．

組織力の向上

SIP サイバーでは，サイバーセキュリティの環境変化（攻撃の増加，攻撃内容の変化，オリンピック・パラリンピック等の新たなターゲットの出現など）

に適応的に対応するため，組織力向上を目的とした社会実装技術に取り組んでいる．具体的には，導入する技術の事前評価のプラットフォームと導入ガイドライン，情報共有基盤と人材育成である．

技術の導入と運用の体制作り

重要インフラの運用現場において最も重要な取組みは，これまでの運用手順にサイバーセキュリティインシデントの検知時の対応手順を追加することである．通常，初期の異常検知時点で，サイバーセキュリティのインシデントと機器故障などを切り分けることは容易ではない．このため，現場技術者が適切な対応が可能な初動マニュアル整備が重要である．

情報共有体制の構築

サイバーセキュリティにかかわるインシデント情報を事業者内で迅速に情報共有できることが組織全体としての対応力の向上につながる．さらに，それぞれの事業者内だけでなく，セキュリティインシデントにかかわる情報を事業者間や関連組織と共有することは，セキュリティインシデントの未然防止，発生時の被害の局所化にとって重要である．

このような情報共有体制の構築には，組織内と組織間での運用ガイドラインと，それを支援する情報共有プラットフォームが重要になる．SIP サイバーでは，国際標準化が進められている STIX/TAXII ☆11 フォーマットをプラットフォームに採用し，国内外の組織間での情報共有支援を目指している．

☆11 STIX：脅威情報構造化記述形式（Structured Threat Information eXpression），TAXII：検知指標情報自動交換手順（Trusted Automated eXchange of Indicator Information）

人材育成の取組み

重要インフラの安定運用は現場の人の力で支えられている．これからはサイバー攻撃への対処も担える人材が必要になる．

サイバーセキュリティ人材育成は産官学が協働で取組むべき我が国の重要課題の 1 つである．SIP サイバーでは，組織力，特に現場の技術者のサイバーセキュリティ対応力の向上を目指す講義教材・演習教材の開発を進めている．

IoT 時代に向けた展望

今後，重要インフラのサイバーセキュリティ確保に向けてさらに強化すべき取組みは，IoT 普及に備えて，IoT セキュリティの技術開発と認証制度作りへの先行的取組みである．また，大規模な重要インフラ分野におけるサイバーセキュリティ対策投資と被害リスクを経済価値として定量化する手法の開発も不可欠な取組みである．

参考文献

1) 内閣府 政策統括官（科学技術・イノベーション担当）：戦略的イノベーション創造プログラム（SIP）重要インフラ等におけるサイバーセキュリティの確保 研究開発計画，2017 年 4 月，http://www8.cao.go.jp/cstp/gaiyo/sip/keikaku/11_cyber.pdf
2) 長橋和哉，後藤厚宏：インフラ維持管理業務におけるスマートデバイスの利用に関する考察，研究報告マルチメディア通信と分散処理（DPS），情報処理学会（2015 年 12 月）．

（2017 年 8 月 6 日受付）

後藤厚宏（正会員）■ goto@iisec.ac.jp

並列・分散処理，インターネットセキュリティ技術の研究開発等に従事．2011 年 7 月より情報セキュリティ大学院大学教授．本会フェロー．現在，本会理事．2017 年 4 月より同大学院学長．