経済産業省　御中

令和3年度新エネルギー等の保安規制高度化事業委託費

熱供給事業のサイバーセキュリティ対策に関する調査事業報告書

三菱総合研究所

デジタル・イノベーション本部
サイバーセキュリティ戦略グループ

2022年3月15日

目次

1. 調査の背景・目的

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今日の状況では、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ったサイバー攻撃が認められ、海外においては、米国のコロニアル・パイプラインにおけるランサムウェアによる攻撃事例（2021年5月）、ウクライナの電力網に対する BlackEnergy による攻撃事例（2015年12月）など重要インフラに対する攻撃が発生している、また、ウラン濃縮施設に係る事例（2010年11月）のようなインターネットに接続されない制御システムへのサイバー攻撃も現実のものとなっている。

一方、サイバーセキュリティに係る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基本法に基づく2回目の「サイバーセキュリティに関する基本的な計画」として、「サイバーセキュリティ戦略」（2018年7月閣議決定）を取りまとめ、推進しているところである。

重要インフラ、サプライチェーンを狙った攻撃等により、業務・機能・サービス障害が生じた場合、社会に大きな影響が生じる可能性が懸念される中、上記の状況、施策を踏まえて、本事業では、熱供給事業におけるプラントシステムへのサイバー攻撃のリスクに対する対応状況等の調査、分析、検討を行い、サイバー攻撃に伴う熱供給設備の事故等の未然防止に係る対応力の向上を図ることにより、熱供給事業の安定供給の確保に資することを目的とする。

2. 熱供給事業におけるプラント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

熱供給事業におけるプラントシステムの構成及び運用を調査するとともに、制御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た。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。

2.1 調査内容・手法

熱供給事業におけるプラントシステムの構成及び運用、当該システムの制御システムの基本的な構成及び運用・制御の考え方、並びに実装されているサイバーセキュリティ対策の現状及び過去のサイバー攻撃等の個別事例を把握するとともに、ヒアリング対象を選定することを目的としたアンケート調査を実施した。

表 2-1 アンケート調査概要

調査対象	一般社団法人熱供給事業協会 会員事業者
有効回答数	68 件（66 事業者※） ※1 事業者から 3 拠点の回答あり
設問数	65 項目
調査項目	基本情報について A.セキュリティ組織体制 B.ポリシー等整備状況 C. 情報資産の管理状況 D. 論理・物理的対策状況 E. システム的対策状況 F. 人的対策状況 G. 組織外コミュニケーション H. インシデント発生状況 I. その他
調査手法	メール調査
調査期間	2021 年 12 月～2022 年 1 月
発送数	75 件

また、アンケート回答結果を踏まえて、熱供給事業者が BCP の観点から想定するリスク、及びより具体的な対策状況や対策を進めるにあたっての課題等を把握するために、リスク分析の実績ある事業者、及び親会社がエネルギー系の組織ではない等、プラントシステムにおけるセキュリティ対策の知見をあまり有していないと事業者を合わせ、4 事業者を抽出してヒアリング調査を実施した。

表 2-2 ヒアリング調査概要

調査対象	一般社団法人熱供給事業協会 会員事業者のうち、アンケート回答者から抽出
有効回答数	4 事業者
調査項目	アンケート調査と同様
調査手法	ヒアリング調査（オンライン）
調査期間	2022 年 1 月～2022 年 2 月

アンケート調査及びヒアリング調査は、プラント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た。セキュリティ対策項目は、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、論理・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の 8 項目とした。

2.2 ヒアリング調査結果

ヒアリング調査の結果から、セキュリティ対策の分類ごとにセキュリティ対策状況及び現在の対策状況における脅威・脆弱性等について、そのリスクを整理した。

2.2.1 セキュリティ組織体制

（1） 現在の対策状況におけるリスク

CISO や情報セキュリティ委員会等のセキュリティ関連の体制が整備されていない場合、セキュリティ施策を推進する責任者を明確にできず、セキュリティに関する方針が定められず、セキュリティ対策が進展しない可能性がある。

さらに、インシデント対応を行う主体である CSIRT が設置されていない場合、サイバー攻撃によりプラントシステムが影響を受けた際に、原因・影響調査や暫定・恒久対策と等のインシデント対応を迅速に行えず、事業継続に影響を与えることや、社会・顧客に対して適切に対応できないリスクがある。

2.2.2 ポリシー等整備状況

（1） 現在の対策状況におけるリスク

情報セキュリティポリシーだけでなく、プラントシステムに関するセキュリティ管理規程が存在しない場合、平時のセキュリティ対策・運用方法はもちろん、インシデント発生時の対応手順が明確化されず、サイバー攻撃の発生時に迅速な対応が行えない恐れがある。

さらに、BCP の範囲にサイバー攻撃によるシステム不具合が含まれない場合、プラントシステムがサイバー攻撃を受けた際、熱供給事業の継続に影響が生じる可能性がある。

2.2.3 情報資産の管理状況

（1） 現在の対策状況におけるリスク

機器の重要度に応じたレベル分けやレベルに応じた管理が実施されていない場合、プラントシステム内の機器に対して、適切な対策が行われず、またサイバー攻撃を受けた場合の影響を迅速に判断できない恐れがある。

また、機器に対して定期的な脆弱性チェックを実施していない場合、脆弱性が放置されサイバー攻撃を引き起こすリスクが高まる点や、脆弱性が判明した際にその影響や範囲を特定することが難しくなる可能性がある。

リスクアセスメントは、組織のセキュリティリスクを見つけ出し、リスクによる事業への影響を最小限に抑えるために効果的な取組みである。リスクアセスメントが実施できていない場合は、自組織に内在するリスクを把握することができず、サイバー攻撃の発生さらには被害の拡大につながる可能性がある。

2.2.4 論理・物理的対策状況

（1） 現在の対策状況におけるリスク

プラントシステム外からアクセスされる場合、VPN やファイアウォールといったセキュリティ製品を導入した場合でも、接続元の端末が攻撃者に乗っ取られる等、プラントシステムにアクセスされる可能性はある。

プラントシステム内において入室制限対策は多くの事業者で実施されていることから、物理的なアクセス制限によりセキュリティリスクを低減できていると言える。ただし、悪意のある内部犯によるサイバー攻撃のリスクも考慮する必要はある。

セキュリティを目的としたネットワーク監視が行われていない場合、サイバー攻撃の検知・遮断が迅速に行えない懸念もある。

セキュリティ機能がない USB メモリ等の外部記憶媒体が使用されている場合、攻撃者が悪意に外部記憶媒体にマルウェアを格納し、その外部記憶媒体が接続された機器がマルウェアに感染する可能性もある。

2.2.5 システム的対策状況

（1） 現在の対策状況におけるリスク

廃止・停止したシステムに対し、データ消去や破壊といった適切な処理を行わない場合、廃止・停止したシステムに残存するデータが外部へ漏洩する等のインシデントが発生する恐れがある。

多くの事業者において業務上の特性から ID・パスワード等による認証を行わない場合も多く、サイバー攻撃のリスクは高いといえる。また何か異常が発生した場合も、誰がその事象を引き起こしたのか、確認が困難となる。

不要なネットワーク・USB ポートの閉塞を実施しないことで、管理を行っていないネットワーク・USB

ポートに不正端末等を接続される等、サイバー攻撃のリスクは高まる。

古いOSに存在する脆弱性をそのまま利用し続けることで、脆弱性を利用したサイバー攻撃が行われる可能性がある。

2.2.6 人的対策状況

(1) 現在の対策状況におけるリスク

制御セキュリティの教育や研修、訓練が十分でない場合、プラントシステムに必要なセキュリティ対策の実行やインシデント対応に支障を及ぼす可能性がある。制御システムが基本的にスタンドアローンであるとしても適切な教育が行われていない場合、マルウェアに感染する等のインシデントが発生したり、インシデント発生時に適切な対応がなされないことで、被害がより拡大したりする恐れがある。

プラントシステムにおいて管理者権限と利用者権限を区分していない場合、利用者が権限以上の行為を行えることで、サイバー攻撃が発生する可能性が高まる。

さらに、委託先の保守業者に対するセキュリティ要件が定められていない場合、適切なセキュリティ対策が実施されず、外部から持ち込まれた不正な端末経由でのマルウェア感染等、プラントシステムの運用に影響を及ぼす可能性も出てくる。

2.2.7 組織外コミュニケーション

(1) 現在の対策状況におけるリスク

セキュリティに関する情報収集が十分にできない場合、セキュリティ対策の実施やインシデント対応の際に必要な情報が収集できず、必要な脆弱性への対応や流行しているサイバー攻撃への備えが遅れたり、自社でのみ対応しなければならなくなる可能性がある。

また、取引先に要求するセキュリティ要件を事前に定義していない場合、取引先で適切な対応が行われず、事業者が取引先に提供した機密情報が漏洩する、取引先で発生したインシデントが取引元にも影響を及ぼす等のインシデントが発生する恐れがある。

2.2.8 インシデント発生状況

(1) 現在の対策状況におけるリスク

インシデントが発生した場合、対応手順が明確でないと、必要な対応が遅れたり、対応に漏れが発生したりするリスクがある。結果的に対応の不備が、プラントシステムに関わる事業の継続に影響する恐れがある。また公開ルールが定められていないと、インシデント発生時の適時かつ適切な内容での情報公開ができず、社会や顧客等のステークホルダからの信頼を失うリスクがある。

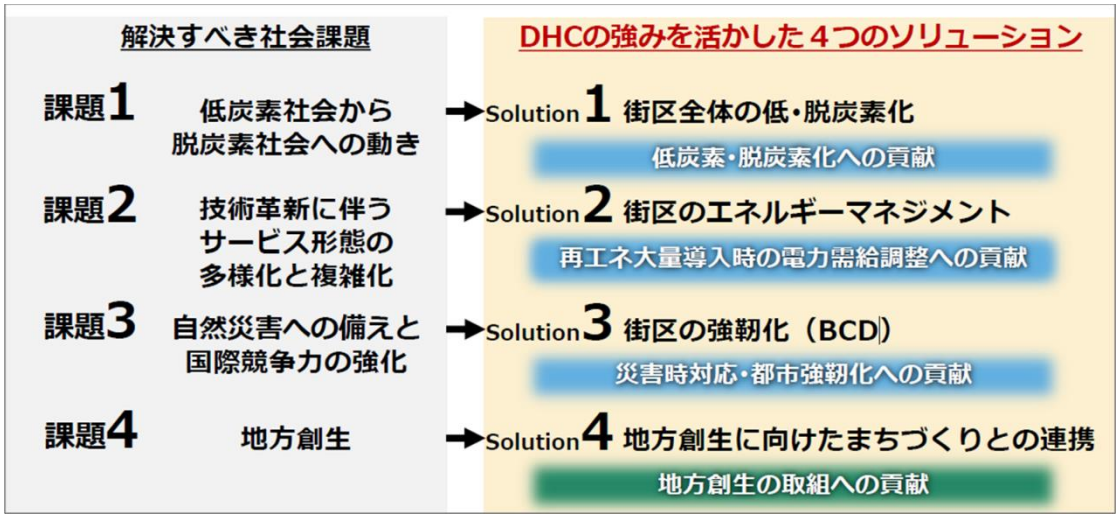
災害への対応として実施されているデータバックアップ、建物の耐震・免震設計および非常用電源といった取組みにより、インシデント発生時の被害の拡大等によるリスクは低減できていると考えられる。

3. カーボンニュートラルの進展等を踏まえ想定される熱供給事業におけるプラントシステムの将来像の調査

今後のカーボンニュートラルに対する取り組みなどを踏まえた熱供給事業におけるプラントシステムの将来像を調査、分析、検討し、将来像を想定した。

3.1 将来の社会課題の解決に貢献する熱供給事業のソリューション・役割

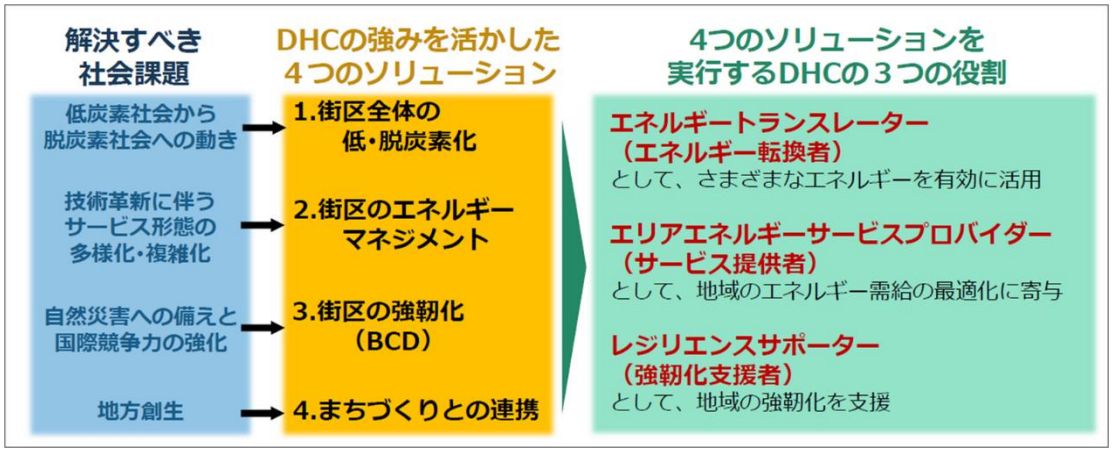
様々な環境の変化、行政の重点施策およびビル事業者の目標を踏まえると、熱供給事業における解決すべき社会課題は大きく分けて「低炭素社会から脱炭素社会への動き」、「技術革新に伴うサービス形態の多様化と複雑化」、「自然災害への備えと国際競争力の強化」および「地方創生」の 4 つに大別される。そのため、熱供給事業は持っている強みと実績を活かして、4つのソリューションである「街区全体の低・脱炭素化」、「街区のエネルギーマネジメント」、「街区の強靭化（BCD）」および「地方創生に向けたまちづくりとの連携」を提供し、2030 年に向けた社会課題の解決に貢献する。



出所） 一般社団法人日本熱供給事業協会 「社会課題の解決に貢献する熱供給事業のソリューション」（https://www.jdhc.or.jp/what/history/future/、2022 年 2 月 18 日閲覧）

図 3-1 社会課題の解決に貢献する熱供給事業のソリューション

つまり、熱供給事業はこれまでの役割に留まることなく、「エネルギートランスレーター」、「エリアエネルギーサービスプロバイダー」、「レジリエンスサポーター」としての役割を担うことで、率先して社会課題を解決する。

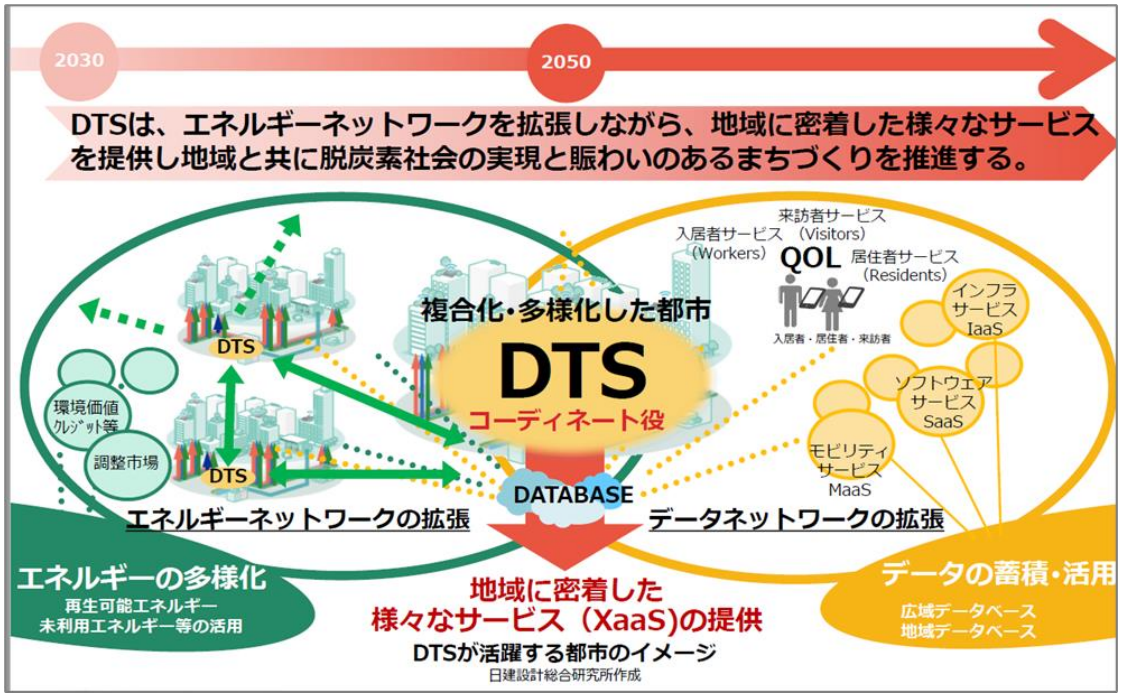


出所） 一般社団法人日本熱供給事業協会 「社会課題の解決に貢献する DHC の役割」
（https://www.jdhc.or.jp/what/history/future/、2022 年 2 月 18 日閲覧）

図 3-2 社会課題の解決に貢献する DHC の役割

2050 年においては「脱炭素化の急速な進展」、「少子高齢化と人口減少」、「都市の集約化・複合化・多様化」および「Society5.0 が描く未来社会へと進化」が想定される。

そのため、さらなる脱炭素化やエネルギーにおける需給形態の変化に対応すると共に、ビッグデータを活用した都市や街区の強靭化と活性化、そして街の魅力向上に資する新たなサービスの提供を図ることにより、熱供給事業は「DTS（District Total Service、地域総合サービス事業）」へ進化していく。

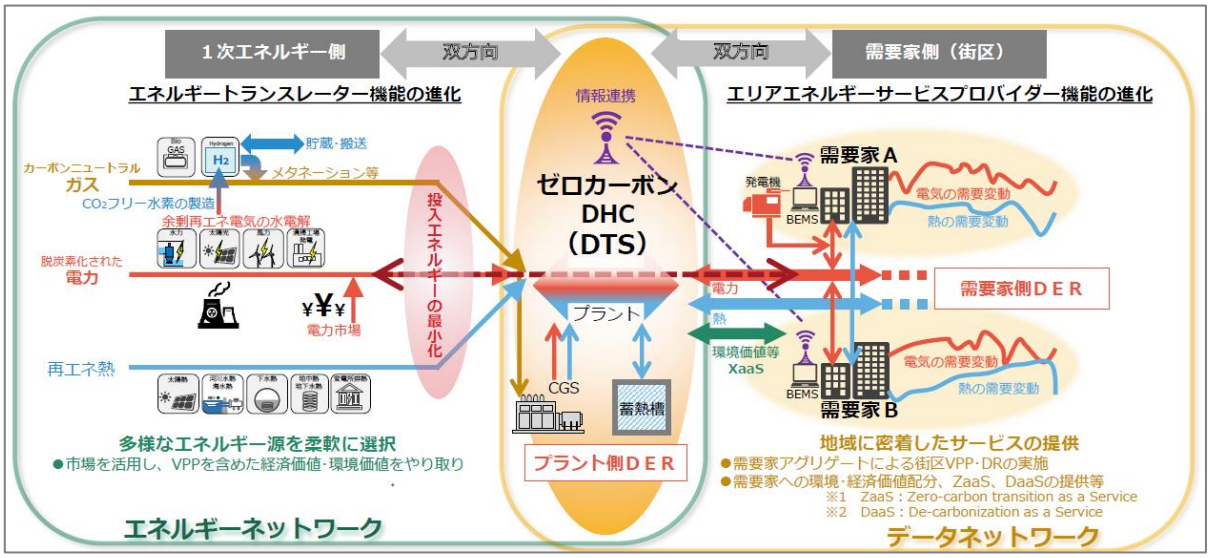


出所） 一般社団法人日本熱供給事業協会 「2050 年に DTS が活躍する都市のイメージ」
（https://www.jdhc.or.jp/what/history/future/、2022 年 2 月 18 日閲覧）

図 3-3 2050 年に DTS が活躍する都市のイメージ

DTS は、街区や地域間におけるエネルギーと情報の双方向性を更に拡大・強化。投入エネルギーの極小化を図りつつ、柔軟に再生可能エネルギー等を選択。更に、自らと需要家が保有する分散エネルギー源（DER）を活用し、大規模なエネルギー需給調整を実現。

また、地域に密着した様々なサービス（XaaS）の提供、環境価値の流通媒介等、地域とともに脱炭素社会と賑わいのあるまちづくりの実現に貢献していく。



出所） 一般社団法人日本熱供給事業協会 「2050 年における DHC（DTS）のイメージ」
（https://www.jdhc.or.jp/what/history/future/、2022 年 2 月 18 日閲覧）

図 3-4 2050 年における DHC(DTS)のイメージ

今後、熱供給事業者が DTS として様々なサービスを拡張するためには、自社内のプラントシステムだけでなく、エネルギーネットワークや、地域の需要家のビルシステム及びこれらを含むスマートシティ等、様々なシステムやネットワークに接続されていく可能性がある。このようなシステムにおいては、相互のシステムや事業の連携が深まる一方、ネットワークを通じて外部環境に接続されることで、サイバー攻撃のリスクも高まる。また、他者とのシステム接続の進展に伴い、相互に利活用を行うデータ量が膨大となり、AI 等最先端の技術の活用も進むと想定されることから、クラウドシステム等外部サービスの活用も増すことが考えられる。サイバー攻撃により自社が影響を受けるだけではなく、自社が提供するデータやサービスの影響は外部の様々な事業者に対して影響を及ぼすこととなる。

さらには、DTS という立場でより広くサービスを提供する場合、関連する様々なステークホルダとの連携が必要となる。平時からの情報共有はもちろん、インシデント発生時には相互に連携して対処する必要性が生じ、適切に情報開示を行う必要性も高まる。

このような事業の広がりにより、新たなネットワークやシステムの接続やクラウド等外部サービス利用に係るセキュリティリスクも考慮して、対策を進める必要が高まると考えられる。

4. 熱供給事業におけるプラント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、諸外国の制御システムに関するガイドラインについて文献調査を行うとともに、2～3 章の調査、分析、検討の結果を総合して、熱供給事業におけるプラントシステムに対して想定されるサイバー攻撃等のリスク、シナリオを検討して課題を整理し、取りまとめた。

4.1 制御システムに対するサイバー攻撃等の事例

4.1.1 2015 年 ウクライナ大規模停電

（1） インシデント概要・被害

2015 年 12 月 23 日、ウクライナで発生した電力会社へのサイバー攻撃は、様々な要因が重なった結果、大規模停電を引き起こしたとされる。発生から復旧までに最大で 6 時間を要し、22 万 5 千人の顧客に影響を与えた。

（2） 攻撃手法

対象企業のアカウント情報を入手していたと考えられ、VPN 接続やリモート管理ツールなど正規の通信経路を辿り、リモートから制御システム環境へ接続していたと想定される。

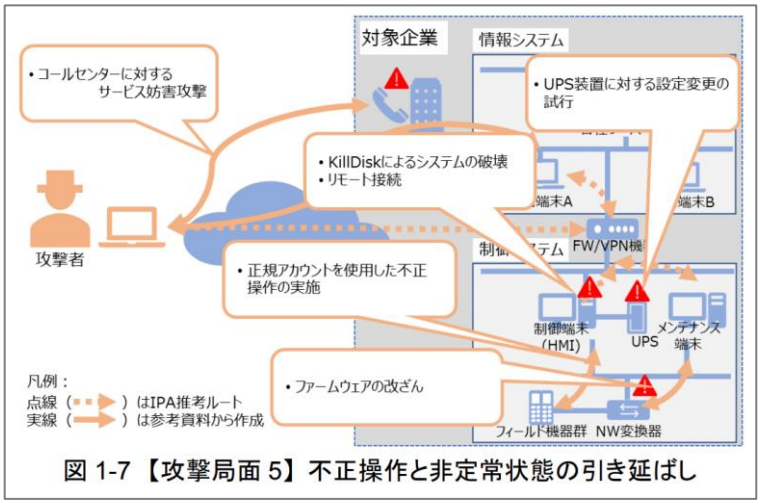


図 1-7 【攻撃局面 5】不正操作と非定常状態の引き延ばし

出所）独立行政法人情報処理推進機構「制御システムのセキュリティリスク分析ガイド補足資料：
「制御システム関連のサイバーインシデント事例」シリーズ」

図 4-1 制御システムにおけるインシデント事例（ウクライナ大規模停電）

4.1.2 2016 年 ウクライナ 電力会社におけるマルウェアによる停電

（1） インシデント概要・被害

2016 年 12 月 17 日、ウクライナの電力会社へのサイバー攻撃では、マルウェアによって意図しないコマンド（ブレーカー遮断）が送信され、当該地域で最大 1 時間 15 分の停電が発生。

（2） 攻撃手法

2015 年のウクライナへのサイバー攻撃と同様の攻撃手法によって制御システム環境まで侵入したとみられているが、最終的な攻撃はマルウェアから直接制御システムへコマンドを送信することで、停電させたとされる。

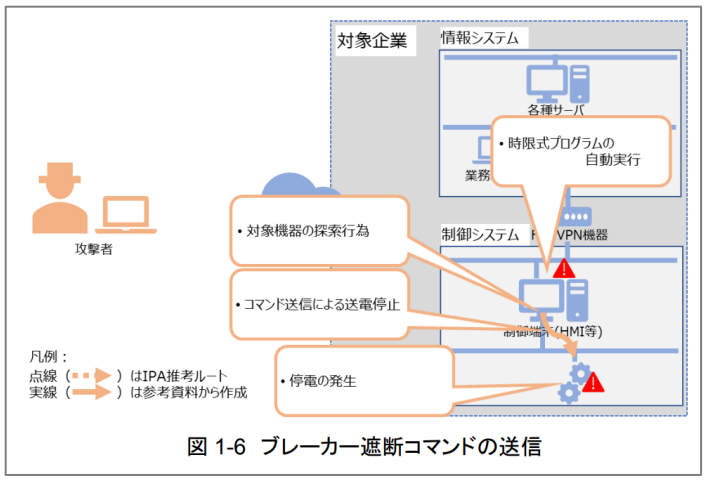


図 1-6 ブレーカー遮断コマンドの送信

出所）「制御システムのセキュリティリスク分析ガイド補足資料：
「制御システム関連のサイバーインシデント事例」シリーズ」（独立行政法人情報処理推進機構）

図 4-2 制御システムにおけるインシデント事例（電力会社におけるマルウェアによる停電）

4.1.3 2017年 安全計装システムを標的とするマルウェア

（1） インシデント概要・被害

2017 年 12 月に公表されたマルウェア「HATMAN」は、安全計装システム（以下、SIS）を標的とした初のマルウェアである。Schneider Electric 社製の SIS コントローラや関連製品に対し、サイバー攻撃を行うために開発・使用され、SIS のフェールセーフ機能が作動し、操業が一時停止した。

（2） 攻撃手法

本事例に関する公開情報では、どのように企業の SIS 環境まで侵入したのかなどの詳細な情報は公開されていない。

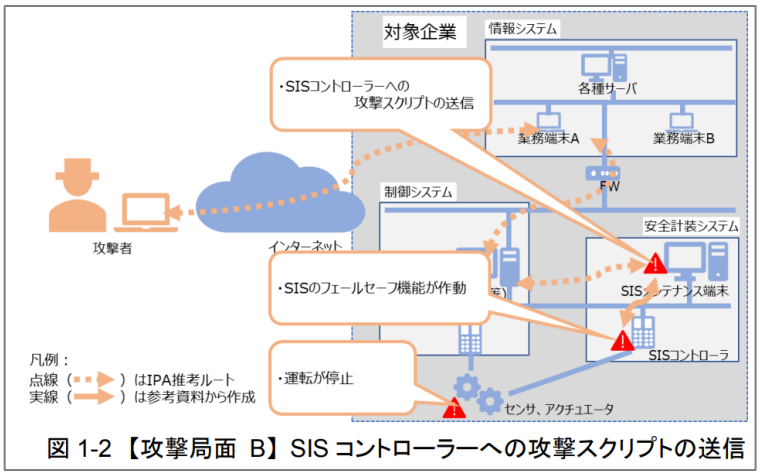


図 1-2 【攻撃局面 B】SIS コントローラーへの攻撃スクリプトの送信

出所）独立行政法人情報処理推進機構「制御システムのセキュリティリスク分析ガイド補足資料：「制御システム関連のサイバーインシデント事例」シリーズ」

図 4-3 制御システムにおけるインシデント事例（安全計装システムを標的とするマルウェア）

4.1.4 Stuxnet：制御システムを標的とする初めてのマルウェア

（1） インシデント概要・被害

Stuxnetと呼ばれるマルウェアが核燃料施設に持ち込まれ、マルウェアに感染させられたコンピュータによって、操業が一時停止する事態となった。

（2） 攻撃手法

遠心分離機を制御する PLC の設定ロジックが改ざんされ、周波数変換器が攻撃されたことにより、約 8,400 台の遠心分離機のうち約 1,000 台が稼働不能に陥った。

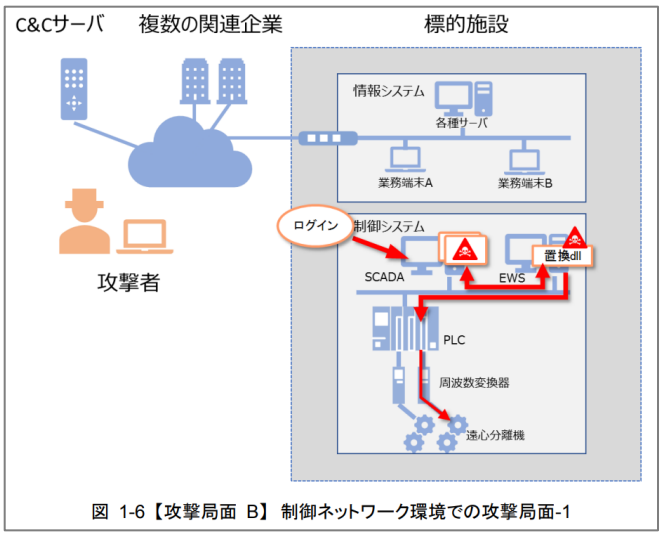


図 1-6【攻撃局面 B】制御ネットワーク環境での攻撃局面-1

出所）独立行政法人情報処理推進機構「制御システムのセキュリティリスク分析ガイド補足資料：「制御システム関連のサイバーインシデント事例」シリーズ」

図 4-4 制御システムにおけるインシデント事例（制御システムを標的とする初めてのマルウェア）

4.1.5 2019 年 アルミニウム生産企業におけるランサムウェアによる操業停止

（1） インシデント概要・被害

2019 年 3 月にノルウェーに本社を置く世界有数のアルミニウム生産企業 Norsk Hydro がランサムウェア『LockerGoga』の被害を受け数カ月の長期間にわたり生産量が低下した。

（2） 攻撃手法

被害を受けた多くはメール、発注や顧客情報管理のコンピュータ等と言われているが、製造用のコンピュータも被害を受けたと推定される。

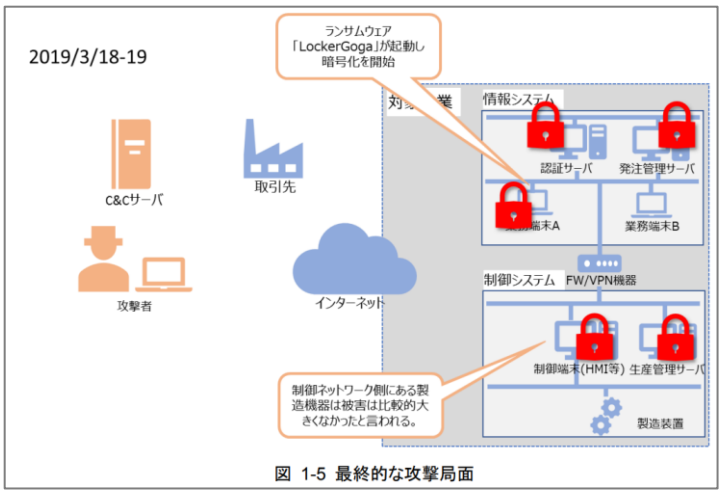


図 1-5 最終的な攻撃局面

出所）独立行政法人情報処理推進機構「制御システムのセキュリティリスク分析ガイド補足資料：
「制御システム関連のサイバーインシデント事例」シリーズ」

図 4-5 制御システムにおけるインシデント事例（アルミニウム生産企業におけるランサムウェアによる操業停止）

4.1.6 2018 年 半導体製造企業のランサムウェアによる操業停止

（1） インシデント概要

台湾の半導体製造企業 TSMC においてランサムウェア WannaCry の被害を受け多くのコンピュータと製造装置に影響を及ぼした。3 日間の生産停止による損害額は、営業利益ベースで最大 190 億円 に達する。

（2） 攻撃手法

WannaCry の亜種に感染した新規追加機器を、必要なウイルスチェックを行わず工場内のネットワークに接続で、連鎖的なネットワーク内感染が発生したと言われている。

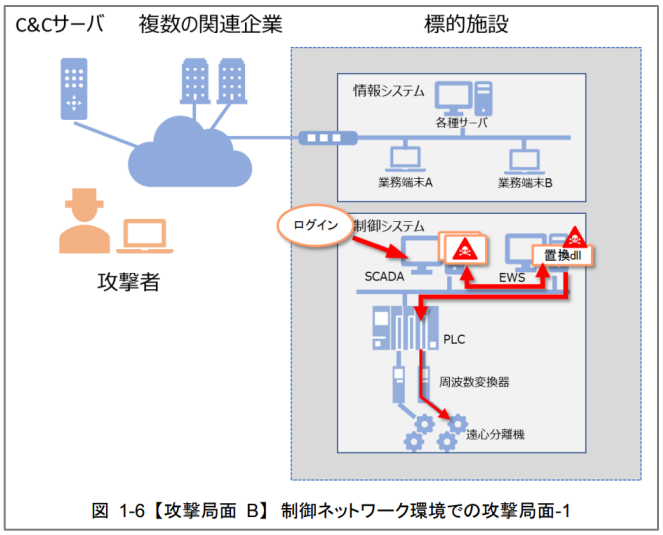


図 1-6【攻撃局面 B】制御ネットワーク環境での攻撃局面-1

出所）独立行政法人情報処理推進機構「制御システムのセキュリティリスク分析ガイド補足資料：「制御システム関連のサイバーインシデント事例」シリーズ」

図 4-6 制御システムにおけるインシデント事例（半導体製造企業のランサムウェアによる操業停止）

4.1.7 2021 年 水道局への不正侵入と飲料水汚染未遂

（1） インシデント概要・被害

米国のフロリダ州の水道局の水処理システムに何者かがインターネット経由で不正侵入し、水酸化ナトリウムの投入量を高く設定変更した。現場操作員が直ちに設定値を元に戻したため、供給される水は影響を受けず、人的被害は発生しなかった。

（2） 攻撃手法

攻撃者はインターネット上から遠隔操作ソフトウェア TeamViewer2 を用いて事務用 PC にログインした。

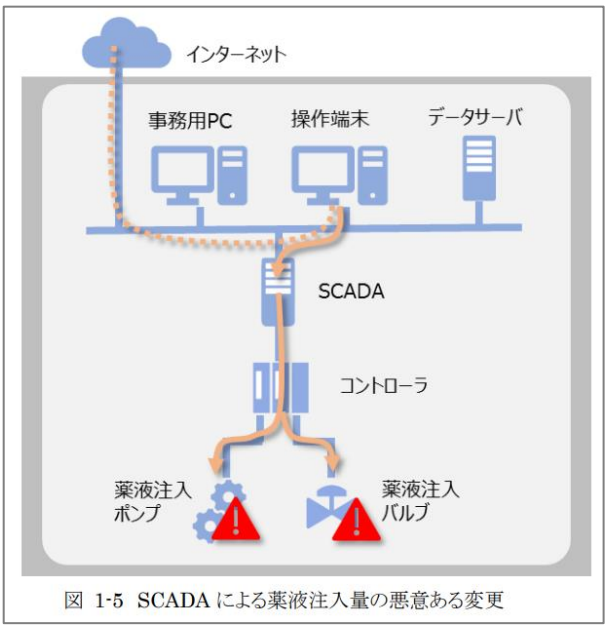


図 1-5 SCADA による薬液注入量の悪意ある変更

出所）独立行政法人情報処理推進機構「制御システムのセキュリティリスク分析ガイド補足資料：
「制御システム関連のサイバーインシデント事例」シリーズ」

図 4-7 制御システムにおけるインシデント事例（水道局への不正侵入と飲料水汚染未遂）

4.1.8 2021 年 米国最大手のパイプラインのランサムウェア被害

（1） インシデント概要・被害

2021 年 5 月 7 日米国最大手のパイプライン企業 Colonial Pipeline がランサムウェアによるサイバー攻撃を受けた。

被害は情報系であり、パイプライン制御システムそのものは直接の影響を受けていなかったが、予め決められていた全社的なインシデント対応プロセスに則って、パイプラインは予防保全的に停止された。

（2） 攻撃手法

当該インシデントについて、FBI は DarkSide ランサムウェアが関与していると声明を出している。DarkSide はランサムウェアの呼称でもあり、攻撃グループおよびランサムウェアによるサイバー攻撃のクラウドサービスの呼称でもある。

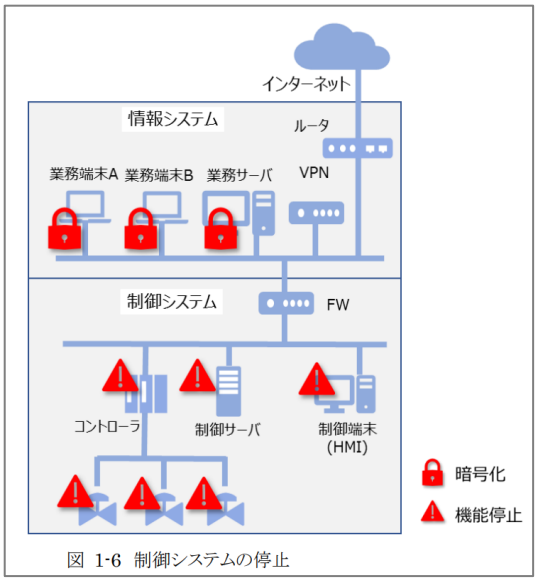


図 1-6 制御システムの停止

出所）独立行政法人情報処理推進機構「制御システムのセキュリティリスク分析ガイド補足資料：
「制御システム関連のサイバーインシデント事例」シリーズ」

図 4-8 制御システムにおけるインシデント事例（米国最大手のパイプラインのランサムウェア被害）

4.2 諸外国の制御システムに関するガイドライン

4.2.1 IEC62443

（1） 概要

IACS(Industrial Automation Control System)のセキュリティ技術仕様を提供する文書。

（2） 対象読者

製造及び制御システムの設計、実装、または管理の責任者。

ユーザ、システムインテグレータ、セキュリティ実装者、及び制御システムメーカー・ベンダーにも適用される。

（3） 記載事項

IEC62443[1]は、制御システムセキュリティの全レイヤ/プレイヤーがカバーされており、以下の構成となっている。

- IEC62443-1(General)：全般・共通事項。制御システム事業者向けに策定された規格であり、既存の ISMS(情報セキュリティマネジメントシステム)のスキームを継承することで、認証者及び受査組織双方にとって効率的な認証が実施可能となる。
- IEC62443-2(Policies & Procedures)：システム開発・運用組織のセキュリティ運用ポリシー・手順。制御システムを利用する事業者向けの要件が規定されている。
- IEC62443-3(System)：システムのセキュリティ機能。インテグレータ(構築事業者)向けの要件が規定されている。
- IEC62443-4(Component)：コンポーネントのセキュリティ(開発プロセス・機能)。装置ベンダー向けの要件が定義されている。

IEC 62443 は、制御システムセキュリティ分野で中心となる標準の一つである。グローバルで認証制度が始まっており、システム・製品、開発プロセス、組織のセキュリティマネジメント、要員が対象となっている。

[1] ISA/IEC 62443 シリーズは、ISA99 WG による「ANSI/ISA-62443」及び IEC/TC65/WG10 による「IEC 62443」があるが、大きな違いはないため、本報告書では、IEC62443 と記載する。

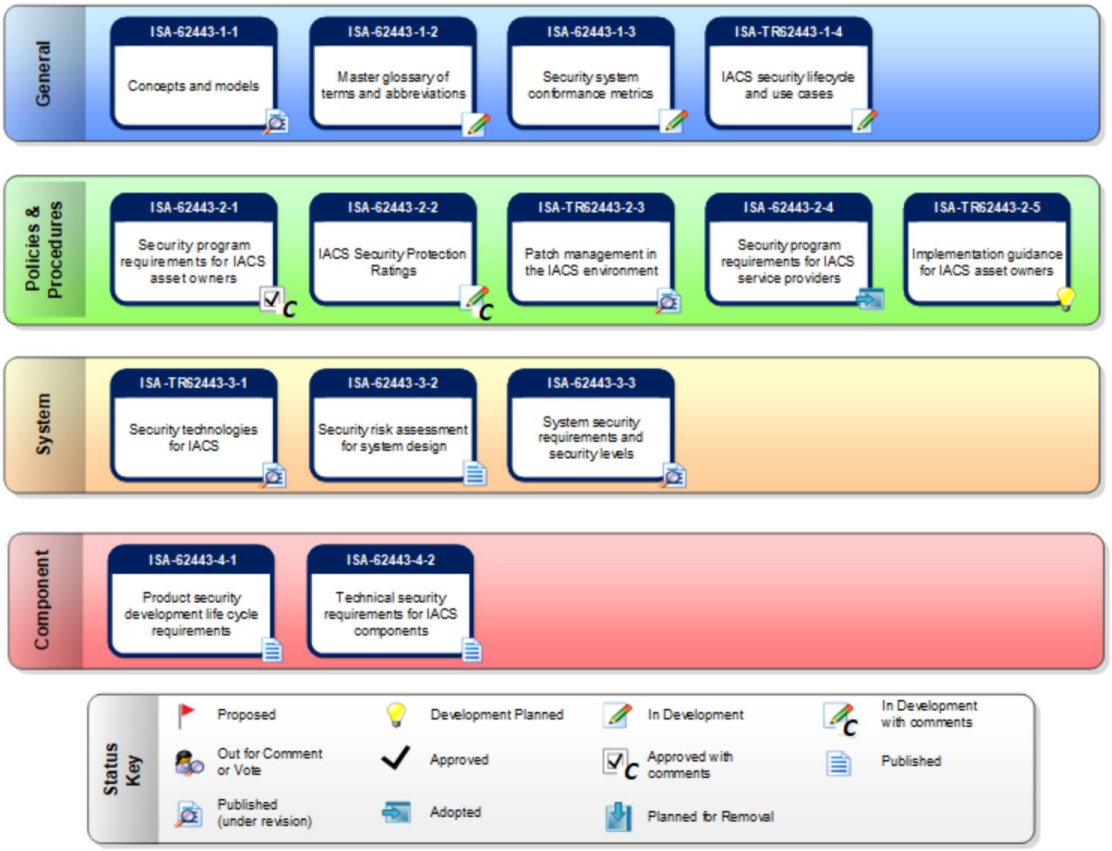


図 4-9 IEC 62443 の体系

（https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99、2022 年 2 月 27 日閲覧）

4.2.2 NIST Cybersecurity Framework

（1） 概要

重要インフラおよびその他業界におけるサイバーセキュリティリスクマネジメントの改善を目的として作成されたフレームワーク。

2014 年に v1.0 が公表、2018 年に v1.1 に更新。

（2） 対象読者

重要インフラの事業者及び運営者

（3） 記載事項

フレームワークは下記 3 つの要素から構成される。

- フレームワークコア：
  サイバーセキュリティ上の成果を達成するための対策と、成果達成のための参考情報であり、業界標準、ガイドライン、プラクティスを示したものである。
  組織のサイバーセキュリティリスクマネジメントライフサイクルを捉えるために、「識別」「防御」「検知」「対応」「復旧」の 5 つの機能で構成される。
- フレームワークインプリメンテーションティア：
  組織がサイバーセキュリティリスクをどのように捉えているか、リスクを管理するためにどのようなプロセスが存在しているかを示す。
  組織のプラクティスが「ティア 1（部分的である）」「ティア 2（リスク情報を活用している）」「ティア 3（繰り返し適用可能である）」「ティア 4（適応している）」のいずれの段階にあるかを示す。
- フレームワークプロファイル：
  自組織が選択した期待される成果を示す。

・

サイバーセキュリティの主な焦点が、情報技術（IT）であるか、産業用制御システム（ICS）であるか、サイバーフィジカルシステム（CPS）であるか、あるいはモノのインターネット（IoT）であるかに関わらず、組織に対して適用可能である。

フレームワークの具体的な使用方法としては以下の内容が挙げられる。

- サイバーセキュリティプラクティスの基本的なレビュー
- サイバーセキュリティプログラムの立ち上げまたは改善
- サイバーセキュリティ上の要求事項について利害関係者とコミュニケーションを行う
- 購入に関する決定
- プライバシーと人権を保護するための方法論　等

フレームワークを自己アセスメントに使用することで、許容可能なレベルまで、組織がリスクを低減することが可能となる。

表 4-1 機能とカテゴリの識別子

機能の識別子	機能	カテゴリーの識別子	カテゴリー
ID	識別	ID.AM	資産管理
		ID.BE	ビジネス環境
		ID.GV	ガバナンス
		ID.RA	リスクアセスメント
		ID.RM	リスクマネジメント戦略
		ID.SC	サプライチェーンリスクマネジメント
PR	防御	PR.AC	アイデンティティ管理とアクセス制御
		PR.AT	意識向上およびトレーニング
		PR.DS	データセキュリティ
		PR.IP	情報を保護するためのプロセスおよび手順
		PR.MA	保守
		PR.PT	保護技術
DE	検知	DE.AE	異常とイベント
		DE.CM	セキュリティの継続的なモニタリング
		DE.DP	検知プロセス
RS	対応	RS.RP	対応計画の作成
		RS.CO	コミュニケーション
		RS.AN	分析
		RS.MI	低減
		RS.IM	改善
RC	復旧	RC.RP	復旧計画の作成
		RC.IM	改善
		RC.CO	コミュニケーション

出所）独立行政法人情報処理推進機構「重要インフラのサイバーセキュリティを改善するためのフレームワーク」
（NIST「Framework for Improving Critical Infrastructure Cybersecurity」監修翻訳）
（https://www.ipa.go.jp/files/000071204.pdf、 2022 年 2 月 27 日閲覧）

4.2.3 経済産業省 「サイバー・フィジカル・セキュリティ対策フレームワーク」

（1） 概要

サイバー空間とフィジカル空間の融合により実現される「Society5.0」と、人・モノ・技術・組織等のつながりにより付加価値を生み出す「Connected Industries」では、サプライチェーンが柔軟で動的に変化していくことになる。

このような新たなサプライチェーンを「価値創造過程（バリュークリエイションプロセス）」と定義し、新しいサプライチェーンの概念に求められるセキュリティへの対応指針として、リスク源を適切に捉えるためのモデルを構築し、求められるセキュリティ対策の全体像を整理するとともに、産業界が自らの対策に活用できるセキュリティ対策例をまとめたガイドラインである。2019 年 4 月公表。

（2） 対象読者

バリュークリエイションプロセスに取り組むすべての主体

（3） 記載事項

サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）では、本編をコンセプト、ポリシー、メソッドの三部で構成している。

- 第 I 部【コンセプト】
  - サイバーセキュリティの観点から、バリュークリエイションプロセスにおけるリスク源を整理するためのモデル（三層構造と 6 つの構成要素）を整理。
  - 三層構造は、「Society5.0」における産業社会を3つの層に整理し、信頼性の基点を明確化したもので、第 1 層「企業（組織）のマネジメントの信頼性」、第 2 層「サイバー空間とフィジカル空間のつながりにおける“転写”機能の信頼性」、第 3 層「サイバー空間のつながりにおけるデータの信頼性」と定義している。
  - 6 つの構成要素は、対策を講じるための単位として、サプライチェーンを構成する要素を6つに整理したもので、「ソシキ・ヒト・モノ・データ・プロシージャ・システム」と定義している。
- 第 II 部【ポリシー】
  - 第 I 部で示したモデルを活用したリスク源の整理と、リスク源に対応する対策要件を提示。
  - 三層構造モデルにおける各層の特性を踏まえ、各層の機能（守るべきもの）とそれに対する悪影響のイメージを整理。
- 第 III 部【メソッド】
  - 第 II 部で示した対策要件に対応するセキュリティ対策例を提示。
  - セキュリティ対策例を実装し、リスクマネジメントプロセスを適切に実施することで、自組織のセキュリティマネジメントを改善することが可能であることを示す。

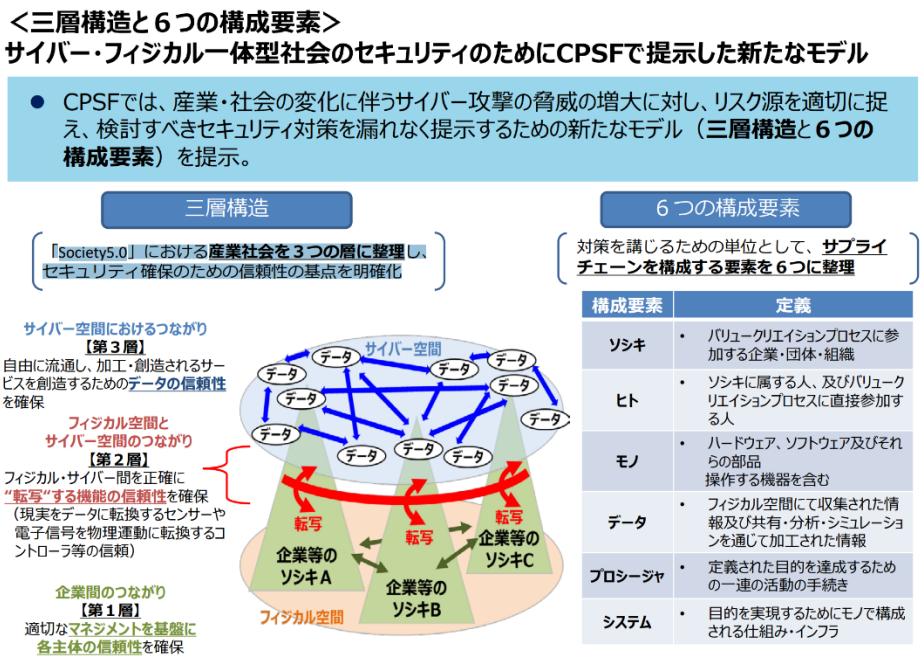


図 4-10「サイバー・フィジカル・セキュリティ対策フレームワークにおける三層構造と 6 つの構成要素」
（https://www.meti.go.jp/press/2019/04/20190418002/20190418002-1.pdf、2022 年 2 月 27 日閲覧）

表 4-2 カテゴリ名称と NIST CSF Ver1.1 の対応カテゴリ

カテゴリ名称	略称	NIST Cybersecurity Framework Ver.1.1 の対応カテゴリ
資産管理	CPS.AM	ID.AM (Asset Management)
ビジネス環境	CPS.BE	ID.BE (Business Environment)
ガバナンス	CPS.GV	ID.GV (Governance)
リスク評価	CPS.RA	ID.RA (Risk Assessment)
リスク管理戦略	CPS.RM	ID.RM (Risk Management Strategy)
サプライチェーンリスク管理	CPS.SC	ID.SC (Supply Chain Risk Management)
アイデンティティ管理、認証及びアクセス制御	CPS.AC	PR.AC (Identity Management and Access Control)
意識向上及びトレーニング	CPS.AT	PR.AT (Awareness and Training)
データセキュリティ	CPS.DS	PR.DS (Data Security)
情報を保護するためのプロセス及び手順	CPS.IP	PR.IP (Information Protection Processes and Procedures)
保守	CPS.MA	PR.MA (Maintenance)
保護技術	CPS.PT	PR.PT (Protective Technology)
異変とイベント	CPS.AE	DE.AE (Anomalies and Events)
セキュリティの継続的なモニタリング	CPS.CM	DE.CM (Security Continuous Monitoring)
検知プロセス	CPS.DP	DE.DP (Detection Processes)
対応計画	CPS.RP	RS.RP (Response Planning) RC.RP (Recovery Planning)
伝達	CPS.CO	RS.CO (Communications) RC.CO (Communications)
分析	CPS.AN	RS.AN (Analysis)
低減	CPS.MI	RS.MI (Mitigation)
改善	CPS.IM	RS.IM (Improvements) RC.IM (Improvements)

出所）経済産業省「サイバー・フィジカル・セキュリティ対策フレームワーク」
（https://www.meti.go.jp/press/2019/04/20190418002/20190418002-2.pdf、2022 年 2 月 27 日閲覧）

各産業分野において、守るべきものや許容できるリスクが異なる実態を踏まえ、CPSF を元に主要な産業分野で求められる具体的なセキュリティ対策が検討されている。

4.2.4 経済産業省 「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン」

（1） 概要

ビルシステムのサイバーセキュリティを確保するためのガイダンス。2019 年公表。

（2） 対象読者

ビルシステムに関わるステークホルダ、ビルの利用者やビルにサービスを提供するサービスプロバイダ等

（3） 記載事項

ビルシステムを巡る状況の変化」として、制御システム特徴と脅威が増大していることを示しつつ、具体的な攻撃事例を複数紹介している。

ビルシステムの構成や特徴（建設後 50 年にわたって非常に長期の運用を行う、マルチステークホルダであること、多種多様なビルが存在すること等）を整理したうえで、設計・建設・竣工・運用・長期運用（改修）といったライフサイクルの各フェーズにおけるセキュリティ対策を示す。

システム全体の構成情報や組織体制、教育など、場所によらない要素について、セキュリティインシデント・リスク源・セキュリティポリシー（対策要件）というセットで取り纏めている。

当該ガイドラインの具体的な使用方法を幾つかのケース（新築の大規模オーナービル、既存の中規模テナントビルをクラウド移行する、既存ビルへのリスクアセスメントと対策立案、等）に分けて、説明している。

表 4-3 ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン構成

1. はじめに
    1.1. ガイドラインを策定する目的
    1.2. ガイドラインの適用範囲と位置づけ
    1.3. 本ガイドラインの構成

2. ビルシステムを巡る状況の変化
    2.1. ビルシステムを含む制御システム全般の特徴と脅威の増大
    2.2. ビルシステムにおける攻撃事例
    2.3. ビルシステムにおけるサイバー攻撃の影響

3. ビルシステムにおけるサイバーセキュリティ対策の考え方
    3.1. 一般的なサイバーセキュリティ対策のスキーム
    3.2. ビルシステムの構成の整理
    3.3. ビルシステムの特徴
    3.4. ビルシステムにおけるサイバーセキュリティ対策の整理方針
    3.5. ガイドラインの想定する使い方例

4. ビルシステムにおけるリスクと対応ポリシー
    4.1. 全体管理
        1．構成情報／管理情報
        2．バックアップデータ／事業継続
        3．会社／要員の管理
        4．体制構築等

    4.2. 機器ごとの管理策
        1．ネットワーク(クラウド、情報系NW、BACnet等)
        2．防災センター（中央監視室）
        3．機械室／制御盤ボックス
        4．配線経路（MDF室、EPS、天井裏ラック）
        5．末端装置が置かれる場所

5. ライフサイクルを考慮したセキュリティ対応策
    （別紙一覧表、構成は4章と同一）
    付録 用語集、他

出所）経済産業省「ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第 1 版」
（https://www.meti.go.jp/press/2019/06/20190617005/20190617005_01.pdf、2022 年 2 月 27 日閲覧）

4.3 熱供給事業におけるプラントシステムに対して想定されるサイバー攻撃等のリスク

4.3.1 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や関連文献調査より、サイバー攻撃の主な発生要因は、(1)外部媒体や持込 PC からのマルウェア感染、(2)情報系システムやインターネットからの侵入、(3)リモート接続を用いた攻撃、(4)不正な攻撃用端末接続による中間者攻撃、(5)内部犯による攻撃が想定される。

(1) 外部媒体や持込 PC からのマルウェア感染

外部とのネットワーク接続を行っていないシステムであっても、別システムへのデータ移動、データバックアップ、バージョンアップ等の保守を目的として、USB 等の外部記憶媒体を接続したり、持ち込んだ PC を接続したりする場合がある。

1)イランの核施設に対するサイバー攻撃(2010 年 9 月)

- Stuxnet と呼ばれるマルウェアが核燃料施設に持ち込まれ、マルウェアに感染させられたコンピュータによって、操業が一時停止する事態となった。
- 2007 年には、内部犯行者を通じて Stuxnet が持ち込まれたが、2009 年のコード更新時には制御システムのベンダー、サプライヤー、エンジニアリングに関する複数の請負業者が Stuxnet に感染し、エンジニアが知らずに USB フラッシュドライブを通じて核燃料施設に持ち込んだとされている。

2)半導体製造企業のランサムウェアによる操業停止(2018 年 8 月)

- ランサムウェア WannaCry の被害を受け多くのコンピュータと製造装置に影響を及ぼした。
- WannaCry の亜種に感染した新規追加機器を、必要なウイルスチェックを行わず工場内のネットワークに接続し、連鎖的なネットワーク内感染が発生したと言われている。

(2) 情報系システムやインターネットからの侵入

OS やアプリケーション等の脆弱性を突き、外部ネットワークから侵入した攻撃者が、制御システムまで侵入するケースである。

1)水道局への不正侵入と飲料水汚染未遂(2021 年 2 月)

- 米国のフロリダ州の水道局の水処理システムに何者かがインターネット経由で不正侵入し、水酸化ナトリウムの投入量を高く設定変更した。
- 攻撃者はインターネット上から遠隔操作ソフトウェア TeamViewer2 を用いて事務用 PC にログインしたとみられている。

2）ランサムウェアによる操業停止（2019 年 3 月）

- ランサムウェア『LockerGoga』の被害を受け数カ月の長期間にわたり生産量が低下した。
- 攻撃者は業務端末に設置したバックドアを通じて、攻撃ツールを投入。特権や対象企業ネットワークのアカウント情報を取得し、認証サーバの管理者権限を用いて攻撃可能範囲を広げ、最終的にランサムウェアを配布した。

（3） リモート接続を用いた攻撃

ベンダーが制御システムの運用保守を行うリモート接続を悪用し、リモート監視端末やリモートメンテナンス端末を用いてフィールド機器にサイバー攻撃を行うケースである。

1）ウクライナ大停電（2015 年 12 月）

- 攻撃者は、対象企業のアカウント情報を入手していたと考えられ、VPN 接続やリモート管理ツールなど正規の通信経路を辿り、リモートから制御システム環境へ接続していたと想定される。

（4） 不正な攻撃用端末接続による中間者攻撃

攻撃者が、制御システムの空きポートに攻撃用端末を接続することにより、中間者攻撃を実施するケースである。

具体的には、制御装置（PLC）や制御システムにおいて用いられる監視カメラが接続されたネットワーク上の通信機器等に攻撃用端末等を接続し、対象となる機器に対して攻撃を行う。あるいは、ネットワーク機器の設定ミスや機能不備を悪用してネットワークに不正に接続する。実際の公開事例はないが、制御システムへのサイバー攻撃シナリオとして想定されるものである。

（5） 内部犯による攻撃

従業員や退職した従業員等による不正操作やマルウェア等悪意を持ったプログラムの配布、情報窃取等を行うケースである。

1）米国の病院内システムを使った DDoS 攻撃未遂（2009 年 6 月）

- 病院の夜勤の契約警備員が HVAC システムや患者情報のコンピュータに侵入し、HMI 画面のスクリーンショットをオンラインで公開した。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たことで発覚し、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大規模な DDoS 攻撃を仕掛ける計画を立てていた。

4.3.2 熱供給事業において想定されるリスクシナリオ

制御系システムにおける 5 つのサイバー攻撃の発生要因により、それが現実化した場合の社会的影響について、熱供給事業者に対するアンケート及びヒアリングによる熱供給事業におけるプラント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から整理した。社会的影響としては、熱供給事業において最大のリスクと考えられる「安定的な熱供給が実現できない」状況を想定した。

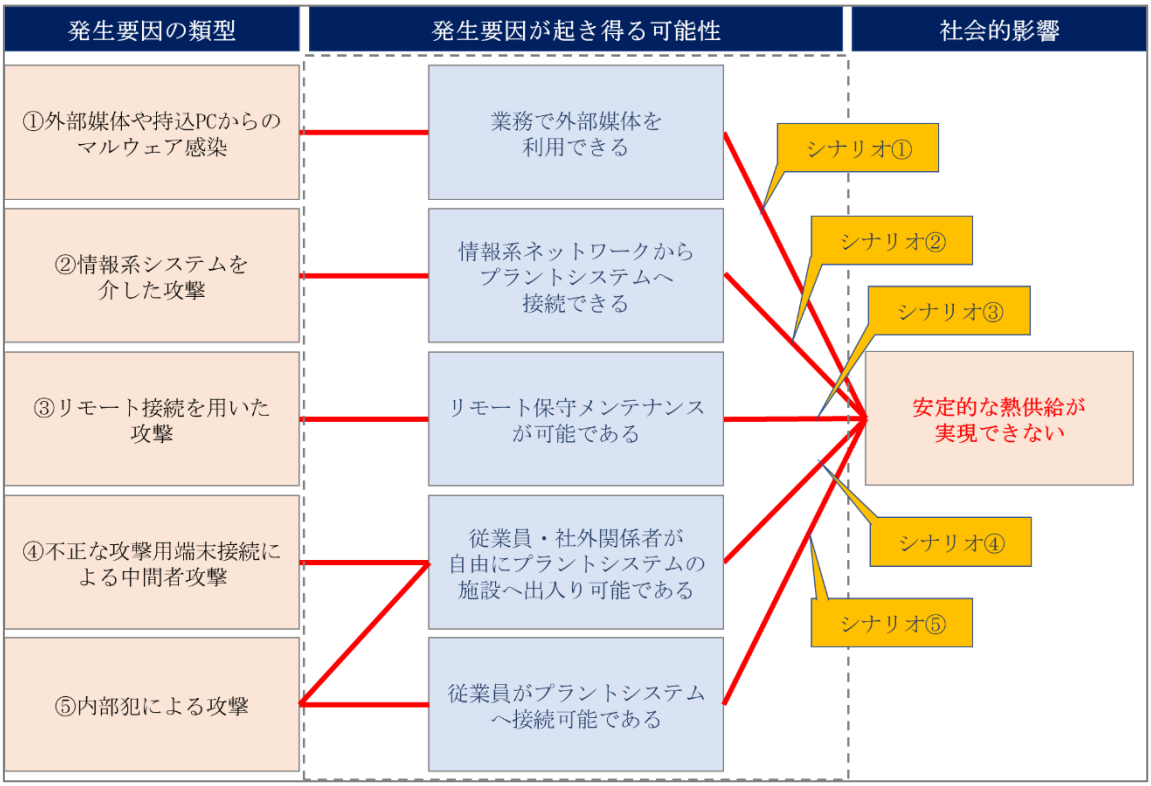


図 4-11 熱供給事業のプラントシステムに対するサイバー攻撃の発生要因と社会的影響の関係

（1） 外部媒体や持込 PC からのマルウェア感染

多くの熱供給事業者において、USB メモリ等の外部媒体が使用されていることが判明している。一部の事業者では、「セキュリティ機能付き USB メモリの使用」、「保守業者が持ち込む USB メモリに対してパターンファイルの更新エビデンスを確認」、「業務上使用しない使用しない USB ポートの閉塞」および「使用可能な USB メモリの限定」等の対策が行われているが、その他の事業者ではセキュリティ対策が行われていない可能性があり、ある端末がマルウェアに感染し、感染した端末から他端末にもマルウェアが拡散する恐れがある。

（2） 情報系システムを介した攻撃

ほとんどのプラントシステムは、情報系ネットワーク等他のネットワークとは分離されたスタンドアローンであったが、一部事業者のプラントシステムでは情報系ネットワークと接続されるケースもあった。この場合、情報系ネットワークの PC およびサーバがマルウェアに感染し、その端末経由でプラントシステムの端末もマルウェアに感染する可能性がある。

（3） リモート接続を用いた攻撃

ほとんどの事業者は保守業者によるメンテナンスをオンサイトで実施していたが、一部の事業者では製造メーカが社外からプラントシステムに外部ネットワーク経由で接続するケースが存在した。そのため、製造メーカに悪意のある攻撃者が存在する、あるいはアクセス元の製造メーカに攻撃者がなりすまし、ネットワーク機器やセキュリティ機器の設定ミスや機能不備を悪用して熱供給事業者のプラントシステムに対してサイバー攻撃が行われるというリスクシナリオが考えられる。

（4） 不正な攻撃用端末接続による中間者攻撃

多くの事業者ではプラントシステムに出入りする人員に対して、人的な監視や電子錠等の対策を実施していた。しかし、特に施錠は行っていない事業者も一部存在するため、その場合、物理セキュリティが突破され、制御システムに接続されるルータ等のネットワーク機器に中間者攻撃を実施するための不正な機器が接続される恐れがある。また、たとえ人的監視や電子錠等の対策を実施していたとしても、悪意を持った従業員や保守事業者が正規にプラントシステムの設置された区域に入り、不正な機器を接続する可能性もある。

不正な機器をプラントシステム内のネットワーク機器へ接続することで、攻撃者によりプラントシステム内の設定値を改ざんし不正な制御を行ったり、監視カメラの画像を不正に閲覧して重要な情報を入手したり、監視カメラの画像の改ざんを行うことで攻撃の発覚を遅らせる等のリスクシナリオが考えられる。

（5） 内部犯による攻撃

内部犯による攻撃では、社員や退職社員等による不正操作により、プラントシステムが影響を受けるケースが考えられる。

熱供給事業のプラントシステムでは、システムに常時ログインした状態であり、操作者に応じた利用可能な機能・データの制御は行われていない事業者が多い。組織内の監督者による人的監視は行われている場合でも、現状だと悪意を持った従業員であればプラントシステムに不正操作を行うことは可能であると考えられる。なお、不正操作とは、従業員がマルウェアを含む USB メモリ等の外部媒体をプラントシステムへ接続し、感染させるといったプラントシステムで異常動作を発生させるような振る舞いである。

また、業務上、不要なネットワークポート・USB ポートを閉塞している事業者は少数であったことから、ネットワークポート・USB ポート経由でのリスクが考えられる。

5. 熱供給事業者のプラントシステムにおいて活用するサイバーセキュリティ対策ガイドライン案の検討

2～4章の調査、分析、検討の結果を基に、熱供給事業者のプラントシステムにおいて活用するためのサイバーセキュリティ対策ガイドラインの素案を検討、作成した。以下に記載事項(案)を示す。

5.1 熱供給事業者のプラントシステムにおける状況

5.1.1 熱供給事業者のプラントシステムを含む制御システム全般の脅威の動向

従来、プラントシステムを構成する制御システムについては、クローズな環境にあり、個別プロトコル等を用いて構成されるケースが多かったが、制御システムネットワークの IP 化や汎用技術の利用の進展により、情報システムと同様のセキュリティリスクが高まっている。また、外部のインターネットを利用したリモート監視やリモートメンテナンスを実施する例も増えてきている。

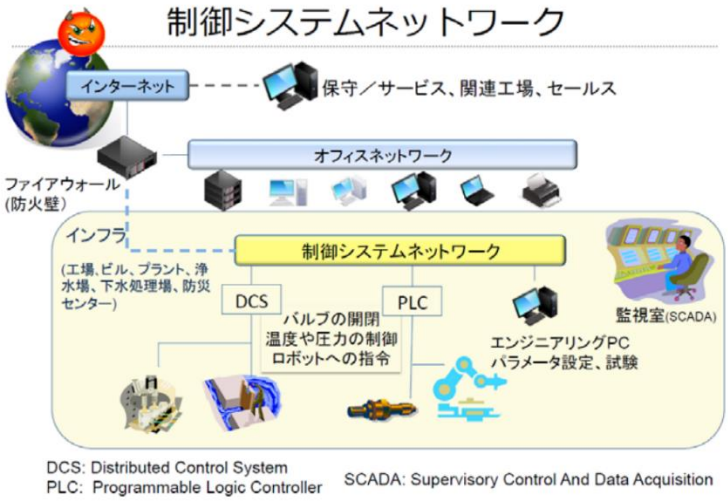


図 5-1 つながる制御システムネットワーク(CSSC)

制御システムを対象としたインシデントも高度化・巧妙化が増しており、制御システムは情報システムと同様、日常的にサイバー攻撃を受けるリスクが高まっている。

5.1.2 制御システムにおける攻撃事例

熱供給事業のプラントシステムを狙った深刻なサイバー攻撃は国内では発生していないが、制御システムにおいては、深刻なダメージを与えるサイバー攻撃の事例が発生している。

5.1.3 熱供給事業者のプラントシステムにおけるサイバー攻撃の影響

熱供給システムは下記の項目を考慮し地域に導入される。

- 熱媒及びエネルギーソースに応じた 熱製造システム決定（ボイラー、冷凍機、ヒートポンプ 等）
- 熱媒、熱需要及び地理的条件に応じた 熱配給システムの決定（配管本数、埋設方法、配管経路等）
- 供給区域内の需要の種類及び地理的条件を考慮した最適熱媒の決定（蒸気、高温水、低温水、冷水 等）

主なシステム構成としては、以下のようなものが考えられる。

- コジェネレーションシステム導入ケース
- 蓄熱システム
- シンプルシステム（ターボ冷凍機＋ボイラ）
- シンプルシステム（吸収式冷温水機＋ボイラ）
- 再生可能エネルギー・未利用エネルギー活用システム

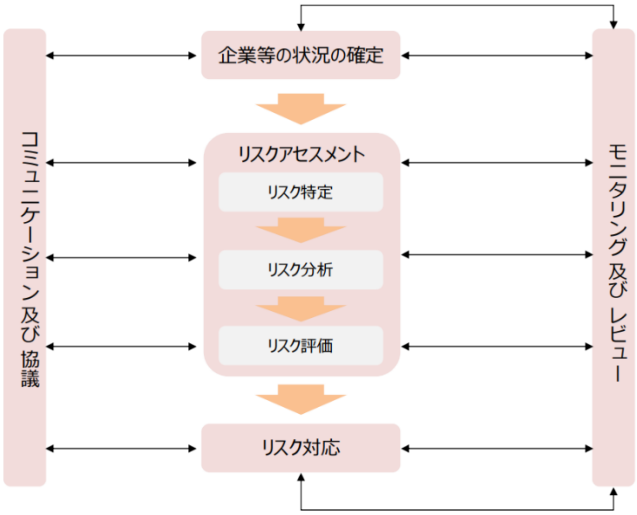
熱供給事業者のプラントシステムに対するサイバー攻撃が発生した場合、安定した熱供給ができなくなることで、需要家に影響することが考えられる。

なお、今後、熱供給事業者が DTS として様々なサービスを拡張する際には、自社内のプラントシステムだけでなく、エネルギーネットワークや、地域の需要家のビルシステム及びこれらを含むスマートシティ等、様々なシステムやネットワークに接続されていく可能性がある。このようなシステムにおいては、サイバー攻撃よる影響はより後半に及ぶことが想定される。

5.2 熱供給事業者のプラントシステムにおけるセキュリティ対策の考え方

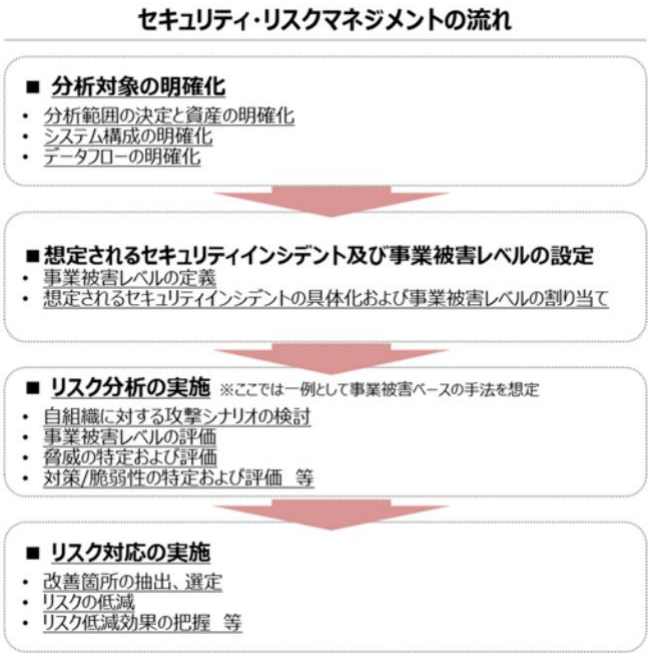
5.2.1 一般的なサイバーセキュリティ対策の考え方

一般的なサイバーセキュリティ対策の考え方としては、対象のアセット（資産）を明確化し、それに対して想定されるインシデントや被害レベルを設定し、リスクの特定を行う。次に、事業被害や脅威について分析と評価を行う。この評価結果をもとに、改善の必要な箇所を抽出しリスクの低減対策を実施する。



出所）経済産業省「サイバー・フィジカル・セキュリティ対策フレームワーク）」

図 5-2 リスクマネジメントの一般的なプロセス（PDCA を含む全体プロセス）



出所）経済産業省「サイバー・フィジカル・セキュリティ対策フレームワーク）」

図 5-3 リスクマネジメントの流れ（上図リスクアセスメント部分の詳細）

5.2.2 熱供給事業者のプラントシステムの構成、特徴

熱供給事業者のプラントシステムの構成は以下の通り。

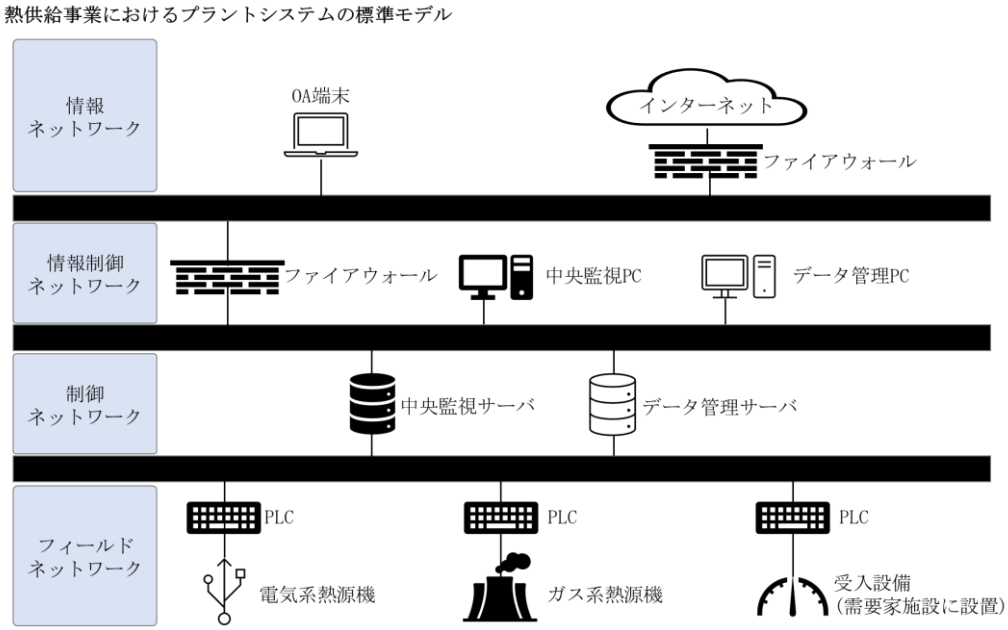


図 5-4 熱供給事業者のプラントシステムの構成

現状、外部ネットワークやシステムと接続されるケースはそれほど多くないが、外部記録媒体を通じたデータのやりとりやプラントシステムの運用がある。

また、今後、外部ネットワークやシステムとの接続が進展する可能性がある。

5.3 熱供給事業者のプラントシステムにおけるリスクとセキュリティ対策

5.3.1 熱供給事業者のプラントシステムにおいて特に留意すべきセキュリティ対策

(1) 外部媒体や持込 PC からのマルウェア感染への対策

社内で USB メモリ等の外部媒体を使用する場合、使用する外部媒体の一覧を作成・管理し、一覧に記載されている機器以外は使用不可とすることで、把握していない機器からマルウェア感染するリスクは低減することが可能である。外部媒体の使用時のルールについても定義する必要がある。例えば、使用許可された外部媒体については、予め保管場所を決めて置き、使用後は決められた保管場所に戻す運用を徹底することで、社外の悪意ある攻撃者に外部媒体を不正利用されるリスクを低減することができる。

また、外部媒体および持込 PC を使用するのが社内の人員か社外の人員かに関わらず、外部媒体に対し、事前にウイルス対策ソフトによるチェックを実施することや、ウイルスチェックが可能な USB メモリ

を使用することも有効である。

さらに、業務上使用しない USB ポートやシリアルポートは物理的に閉塞するといった対策も持ち込まれた外部媒体および PC からのマルウェア感染リスク低減に効果的である。

（2）情報系システムを介した攻撃への対策

サイバー攻撃の起点となる可能性がある OA 端末に対し、アンチウイルスソフト等のマルウェア対策を実施することで、当該ケースのリスクを低減することができる。

また、OA 端末が感染した場合でも、VLAN によるネットワーク分割やファイアウォールによるアクセス制御を行うことで、OA 端末を起点としたマルウェアの横感染を最小限とすることが期待される。

さらに、ファイアウォールや各種セキュリティ機器を SOC のようなサイバー攻撃の検知を目的とした組織で監視することで、迅速にサイバー攻撃を検出し、インシデント対応につなげることが可能である。

（3）リモート接続を介した攻撃への対策

製造メーカが社外からプラントシステムにリモートアクセスする場合、リモート接続時に ID・パスワード認証や多要素認証等の認証方式を採用することで、本来アクセスするべきでない悪意のある攻撃者が故意にアクセスするリスクを低減することができる。

また、定期的にプラントシステムへリモートアクセスを行う関係者に対し、リモートアクセスの運用状況を監査することも適切に業務を行っているか確認する上で効果的である。

さらに、リモートアクセス元の端末とアクセス先の端末間にファイアウォールや IPS といったアクセス制限・振る舞い制限の機能を持つ機器を導入することで、本来アクセスすべきでない攻撃者の侵入や意図しない通信データを防止・検知することができる。

（4）不正な攻撃用端末接続による中間者攻撃への対策

外部の悪意のある攻撃者が事業者のプラントシステムへ物理的に侵入し、不正な攻撃用端末を接続するような事態を避けるため、重要エリアの施錠、入退室管理、生体認証の導入、監視カメラの設置および持ち物検査といった物理セキュリティ対策が有効である。

また、攻撃者にプラントシステムへの物理的な侵入を許した場合でも、ARP テーブルを管理可能なスイッチやホワイトリスト機能を保有するスイッチを導入することで、ARP スプーフィングといった中間者攻撃のリスクを低減することが可能である。

さらに、制御用 IDS・IPS の導入は攻撃による異常を迅速に検知・遮断するために有効であり、通信経路・データそのものの暗号化も攻撃者による盗聴を困難にするために効果的である。

（5）内部犯による攻撃への対策

悪意のある従業員等の内部犯による攻撃を防止するために、ID・パスワードといったユーザアカウントの使用や、「最小権限の原則」に基づく各ユーザへの権限制御が効果的である。このような対策を導入することで、本来許可されていない操作の実施を未然に防ぐことが可能となる。また、プラントシステムでも特に重要と位置付けられるシステムについては、ユーザアカウントによるアクセス管理だけでなく、「SMSおよびメール認証」等も加えた多要素認証の仕組みを導入することで、不正アクセス・操作のリスクを低減することができる。なお、ユーザアカウントや権限制御を導入する際には、既存業務との兼ね合いも考慮することで、各事業者にとって最適な対策を導入することが推奨される。

内部犯による攻撃時に開放された USB ポート・ネットワークポートが悪用されることも考えられる。そのため、業務上使用しない USB ポート・ネットワークポートは閉塞する等の対策を講じることが望ましい。

5.3.2 熱供給事業者のプラントシステムにおいて必要となるセキュリティ対策

（1） 組織体制の整備

現状、熱供給事業者において、CISO や情報セキュリティ委員会、あるいはインシデント対応を行う CSIRT を設置している事業者は少ない。外部からのサイバー攻撃に対応する必要性は強く意識されている状況ではないと考えられるが、サイバー攻撃の手法も高度化する中、事業者の状況や想定されるセキュリティリスクに応じて適切なセキュリティ方針を定め、対策を進めていくためには、セキュリティに関する責任者を定め、組織として統一的な方針の下に対策を進める必要があるとともに、インシデントが発生した場合に迅速に対応するための体制を整備する必要がある。

多くのプラントシステムがスタンドアローンである現状や、既存の組織規模を考慮すると、必ずしも部署として立ち上げることをしなくても、プラントシステムにおけるセキュリティの責任者や担当者の役割と権限を明確化する等、実効的な対策を進めるための体制を整えていくことが有効であると考えられる。

（2） プラントシステムにおけるセキュリティポリシーの策定

事業所内で適用す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程を定めている事業者は多いが、プラントシステムを対象としたセキュリティ管理規程を定めている事業者はほとんど存在しておらず、またほとんどの事業者において BCP の範囲にサイバー攻撃が含められていない。

昨今のサイバー攻撃は制御システムを狙ったものも高度化しているという点や、情報系でもランサムウェア等の悪質なマルウェアが制御系システムへも影響を与えるケースもある。プラントシステムにおけるサイバー攻撃は、熱供給事業そのものに影響を与えることから、プラントシステムにおけるセキュリティポリシーの策定を進めることが必要と考えられる。

もちろん、セキュリティポリシーについては、攻撃の高度化や社会からの要請、あるいは自組織の事業やシステムの状況を踏まえて、定期的に見直し、反映を行いながら、プラントシステムにおけるセキュリティ対策を進めることが重要である。

（3） 制御システムセキュリティに関する教育の実施

情報セキュリティに関する教育については多くの事業者が実施していたが、制御システムセキュリティに関する教育は実施していない事業者が多かった。

熱供給事業者の従業員においては、制御システムセキュリティに関して必ずしも専門的な知識が求められる訳ではないが、プラントシステムにおけるセキュリティリスクの認識や、インシデント発生時の対応に関する手順書の整備（操作、報告等）及び訓練等、基礎的な事項や対応については、理解を深めることが、プラントシステムにおけるセキュリティ対策を実効的に進めるために必要である。

特に、プラントシステムに何らかの異常が発生した場合、それがサイバー攻撃による可能性があるという意識を持つことで、早期に適切な対応ができるようになる。また、セキュリティインシデント対応に関する手順書を整備し、訓練を行うことで、インシデントに関しての早期検知と迅速な対応が可能となり、被害防止・最小化に繋げることが可能となる。

（4） 外部記憶媒体の管理徹底

熱供給事業においては、プラントシステムの保守運用のために USB メモリを利用したり、事業者によってはプラントデータを活用するために USB メモリを利用したりする場合が多い。スタンドアローンのプラントシステムにおいては外部からの攻撃が困難であるため、攻撃者も悪意を持って外部記憶媒体にマルウェアを格納し、制御システムへのマルウェア感染を狙う場合もある。利用者の実態をみると、組織で管理している USB メモリを利用しているという事業者もいたが、セキュリティ機能がない USB メモリを利用している場合もあった。

現状、熱供給事業のプラントシステムにおいては、外部記録媒体のリスクが大きいと考えられるため、USB メモリ等の利用を可能な限り減らしていくことや、組織としてウイルスチェックを行った USB メモリ等を利用する、USB ポートを閉塞するなど、不必要に様々な制御システムに USB メモリを刺すことのないようにする等、管理の徹底を図っていくことが必要である。

（5） 外部接続の極小化、セキュリティ対策の徹底

多くの事業者のプラントシステムはスタンドアローンであったため、外部接続があるケースに関してはファイアウォールや VPN 等のセキュリティ対策が取られていた。

今後、外部のネットワークと接続するケースは増えていくと考えられるが、セキュリティリスクを軽減するためには、外部接続については極小化していくとともに、外部接続を行う際には、ネットワークの監視、侵入検知・防御、外部への不正な通信の検知・遮断、セキュリティの確保された通信路の利用、相手先の認証など、必要なセキュリティを徹底する必要がある。

（6） ランサムウェア対策

昨今はランサムウェアを利用したサイバー攻撃が頻発しており、熱供給事業者においても様々な経路

からランサムウェアがプラントシステムへ侵入する可能性がある。

ランサムウェアへの感染を防ぐためには、プラントシステムに対する外部からのアクセスを限定し、強固な認証を行うことに加え、OS やソフトウェアのバージョンを常に最新に保つことが必要である。セキュリティソフトが導入された端末の場合は、定義ファイルを最新の状態に保つことも有効である。

さらに、万が一感染した場合に備え、バックアップを実施することが有効である。ランサムウェアはシステム全体に影響を及ぼす可能性があるため、データだけではなく、OS やアプリケーション等のシステム全体をバックアップ対象とすることも有効である。また、バックアップからの復旧を迅速に行うために、バックアップからの復旧手順の整備、定期的な訓練を行うことで、インシデント発生時の迅速な対応に役立てることが可能である。

（7）外部委託先管理

運転業務の委託先や、プラントシステムの設置業者及びメンテンナンス業者等、プラントシステムを設置・運用するためには、外部事業者に対する委託を行うことが多い。外部委託先のセキュリティに関する不備が自組織に影響を及ぼす可能性も十分考えられることから、外部委託先に要求するセキュリティ要件を定義することが推奨される。また、合意したセキュリティ要件が委託先で遵守されているか定期的に確認することも有効である。

さらに、契約終了時においても、機密情報の破棄や委託先に付与した入館証・アカウントの処分等、セキュリティに関する手続を定め・運用することで、セキュリティリスクを低減することができる。

6. 今後の熱供給事業のサイバーセキュリティ対策の在り方

本調査では、熱供給事業のサイバーセキュリティ対策について、アンケート調査及びヒアリング調査による現状把握を行い、カーボンニュートラルの進展等を踏まえ想定される熱供給事業におけるプラントシステムの将来像を踏まえ、熱供給事業におけるプラントシステムに対するサイバー攻撃等リスクの検討、及び熱供給事業者のプラントシステムにおいて活用するサイバーセキュリティ対策ガイドライン素案の検討を行った。

熱供給事業は、現在、国が定める重要インフラ分野ではないが、熱供給事業は社会にとって必要なサービスとなりつつあり、制御システムであるプラントシステムがひとたびサイバー攻撃を受けると、安定的な熱供給に影響を与える可能性もある。

現状の熱供給事業におけるプラントシステムは、その多くが外部のネットワークから切り離されており、外部ネットワークを通じたサイバー攻撃のリスクは低いと考えられる。しかし、現状調査を踏まえると、以下の事項について、セキュリティ対策に関する取組みを進めていくことが望ましいと考えられる。

(1)組織体制の整備 (責任者の設置、インシデント対応体制の整備)
(2)プラントシステムにおけるセキュリティポリシーの策定
(3)制御システムセキュリティに関する教育の実施
(制御系システムのセキュリティリスクの認識、
インシデント発生時の対応・訓練、手順書の整備(操作、報告)等)
(4)外部記憶媒体の管理徹底
(5)外部接続の極小化、セキュリティ対策の徹底
(6)ランサムウェア対策
(7)外部委託先管理

熱供給事業者は必ずしも大規模な事業者ではなく、またプラントシステムについてもまだクローズなものが多いことから、セキュリティ対策についても、個々の事業者の事業規模やシステム状況、体制を踏まえて、実態に応じた取組を進めることが求められる。

今後、熱供給事業においては事業の拡大や社会において果たすべき役割が重要となるにつれて、求められるセキュリティがより高度なものとなっていく可能性もある。熱供給システムの変化やエネルギー等他のシステムとの連携、それから社会からの要請を踏まえ、セキュリティ対策については、今後も見直し、改善を進めていくことが望ましい。

付録１ 有識者委員名簿

本事業では下記の委員からなる「熱供給事業におけるプラントシステムのサイバーセキュリティ対策に関する検討委員会」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　　電気通信大学 名誉教授

（委員）

有村 浩一　　一般社団法人 JPCERT コーディネーションセンター

小澤 浩　　アズビル株式会社 ビルシステムカンパニー

桑名 利幸　　独立行政法人 情報処理推進機構

永田 善信　　一般社団法人 日本熱供給事業協会

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

（敬称略、五十音順、所属は検討会開催時点のもの）

付録２ 有識者検討会概要

第１回

日時 ： 2021 年 12 月 21 日(火) 10:00 - 12:00

場所 ： オンライン開催 (Teams)

議事 ：

今年度の事業について

熱供給事業におけるプラントシステムに対するサイバー攻撃等のリスク等について

アンケート調査について

今後のスケジュールについて

第２回

日時 ： 2022 年 3 月 11 日(金) 13:00 - 15:00

場所 ： オンライン開催 (Teams)

議事 ：

アンケート・ヒアリング調査結果について

調査報告書(案)について

熱供給事業におけるプラントシステムのセキュリティガイドライン(素案)について

熱供給事業のサイバーセキュリティ対策に関する調査事業報告書

2022 年 3 月

株式会社三菱総合研究所
デジタル・イノベーション本部
サイバーセキュリティ戦略グループ
TEL 03-6858-3578