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２版

令和５年４月２０日

産業サイバーセキュリティ研究会

ワーキンググループ１(制度・技術・標準化)

ビルサブワーキンググループ

変更履歴

発行日	版	概要
2018 年 9 月 3 日	β版	β版初版発行
2018 年 10 月 31 日	β版（差し替え版）	細部修正の上、差し替え版発行
2019 年 3 月 11 日	第 1 版案（パブコメ版）	全体を通した再確認、修正の上、パブコメ版発行
2019 年 6 月 17 日	第 1 版	第 1 版発行
2023 年 2 月 15 日	第 2 版案（パブコメ版）	インシデントレスポンスの項目を追加の上、パブコメ版発行
2023 年 2 月 15 日	付属書案（パブコメ版）	インシデントレスポンスの詳細を付属書としてパブコメ版発行
2023 年 4 月 20 日	第 2 版	第 2 版発行（付属書を統合）

目次

1. はじめに 1
1.1. ガイドラインを策定する目的 1
1.1.1. ガイドラインの目的 1
1.1.2. サイバー・フィジカル・セキュリティ対策フレームワークとの関係 1
1.2. ガイドラインの適用範囲と位置づけ 2
1.2.1. ガイドラインの対象者 2
1.2.2. 対象とするビル 2
1.2.3. 対象とするビルシステム（ビルシステムの定義） 3
1.2.4. ガイドラインの位置づけ 3
1.3. 本ガイドラインの構成 7
2. ビルシステムを巡る状況の変化 8
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 8
2.2. ビルシステムにおける攻撃事例 11
2.2.1. MIT（Massachusetts Institute of Technology、マサチューセッツ工科大学）の学内ビルの照明ハッキング 11
2.2.2. ターナー・ギルフォード・ナイト収容所の警備システムハッキング 12
2.2.3. ラッペーンランタでの DDoS 攻撃による暖房停止 13
2.2.4. ホテルでの宿泊客の閉じ込め・閉め出し 14
2.2.5. インターネットカメラへの大量ハッキング 15
2.2.6. テストによるハッキング事例 16
2.2.7. ドイツにおける BAS 機器のロック事例 16
2.3. ビルシステムにおけるサイバー攻撃の影響 18
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 19
3.1. 一般的なサイバーセキュリティ対策のスキーム 19
3.2. ビルシステムの構成の整理 20
3.3. ビルシステムの特徴 25
3.3.1. 超長期の運用 25
3.3.2. 複数のフェーズに分かれた長いライフサイクルを持つこと 25
3.3.3. マルチステークホルダであること 26
3.3.4. 多種多様なビルの存在 26
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 27
3.4.1. 場所から紐解くリスクの整理とライフサイクルを考慮した対策 28
3.4.2. インシデント発生時の対応 29

3.5. ガイドラインの想定する使用例 32
3.5.1. 例１： 新築の大規模オーナービルにおける使い方 32
3.5.2. 例２： 既存の中規模テナントビルをクラウド移行する際の使い方 33
3.5.3. 例３： 既存ビルへのリスクアセスメントと対策立案での使い方 33
3.5.4. 例４： 機器等の障害対応の延長線上でインシデント対応する使い方 34
4. ビルシステムにおけるリスクと対応ポリシー 35
4.1. 全体管理 35
4.2. 機器ごとの管理策 36
5. ライフサイクルを考慮したセキュリティ対応策 44
6. インシデント発生時の対応策 45
6.1. インシデントレスポンスの概要 45
付録 A 用語集 49
付録 B JDCC の建物設備システムリファレンスガイドとの関係 53
付録 C 建物設備システム リファレンスガイド インシデント対応・セキュリティソリューション編との関係 54
付録 D サイバー・フィジカル・セキュリティ対策フレームワークの考え方と、サイバー・フィジカル・セキュリティ対策フレームワークの考え方を踏まえたビルシステムにおけるユースケース 55
付録 E 参考文献 58

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2版の策定にあたって

- ビルのサイバーセキュリティについては、2019年6月17日に「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（以下、共通編）第1版」が公開、ビルシステムに対する全般的なサイバーセキュリティ対策のガイドを示すものとして活用され、ビルのサイバーセキュリティ対策も徐々に進んできている。さらに、2022年10月24日には「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（個別編：空調システム）第1版」が公開され、ビルに係る個別のサブシステムとして空調システムを対象としたサイバーセキュリティ対策向上のために活用されるに至っている。

- 上記の共通編第1版は、ビルに導入される様々なシステムに対するサイバーセキュリティ対策のうち、主に事前に検討し、準備しておくべき対策について示したものである。しかし、導入済みのシステムの制約やコストの問題など、さまざまな問題から十分に対策ができていないといった問題、想定を超える高度なサイバー攻撃の可能性、さらにスマートビル化の進展により、ビルシステムが被害を受ける可能性がより高まっている。

- このような状況に対して、ビルシステムへのサイバー攻撃（インシデント）の発生時に、その損害を最小限に抑え、復旧にかかる時間とコストを削減するための取組（インシデントレスポンス）が重要となる。このため、ビルシステムに対するサイバーセキュリティ対策強化の一環として、インシデントレスポンスについて検討を行い、取りまとめを行った。

- この検討の成果を新たに追加する形で、本ガイドラインの改定を行い、新たに第2版として公開することとした。また、インシデントレスポンスに係る詳細の対応を「付属書　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　インシデントレスポンス・ガイドライン（案）（以下、付属書）」としてまとめることとした。

- また、本ガイドラインの活用をさらに推進するため、個別のサブシステムの状況に特化して配慮が必要なことを個別編として取りまとめており、2022年10月に「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（個別編：空調システム）第1版」を取りまとめているので参照されたい。

- 今後、本ガイドライン及びその付属書、個別編が活用されることで、ビルシステムにおける事前対策からインシデント発生時の対応まで、一貫した対策が進むことを望まれる。

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版の策定にあたって

- ビルのサイバーセキュリティについては、これまではビルシステムを構成する制御系がインターネットと切り離されていることや、ビルシステム特有のプロトコル（通信手順、通信内容を解釈するための決まり事）を使っているために攻撃の対象となりづらい、ビルシステムがマルチステークホルダ（多種多様な関係者が関与する構造であること）であり、ビルシステムのサイバーセキュリティ全体を統合管理する体制を組織しづらい等を理由にして対策が遅れている傾向があった。

- しかしながら、サイバー攻撃のレベルの向上により、特有のプロトコルであることをもって攻撃の対象から外れることはなくなってきている。また、利便性の向上の観点からインターネットに繋がるケースが増えてきており、外部からの接続を前提にした設計も増加している。

- 世界的に見てもビルシステムを対象としたサイバー攻撃が実際に発生している。

- 一方で、ビルシステムの特徴としてステークホルダ（何らかの利害関係を持つ関係者）が多数存在しており、これらのステークホルダが共通に参照できるサイバーセキュリティ対策のガイドラインが存在していないため、サイバーセキュリティ対策を進める方向性が示されていない。

- こうした問題意識から、2018 年 2 月、産業サイバーセキュリティ研究会 WG1 の下に、ビルシステムに関わる多数のステークホルダが一堂に会し、それぞれの視点も考慮して、ビルシステム向けのサイバーセキュリティ対策について議論を行うビルサブワーキンググループを設置し、検討を行ってきた。

- 本ガイドライン第 1 版は、2018 年 9 月に公開したβ版及び 2019 年 3 月から 4 月に掛けて実施したパブリックコメントに対して寄せられた多数の意見等を踏まえ、また産業サイバーセキュリティ研究会 WG1 におけるサイバー・フィジカル・セキュリティ対策フレームワークの検討も参考にしながら、ビルサブワーキンググループで検討を進めてきたビルシステムのサイバー・フィジカル・セキュリティ対策の内容を整理したものである。

- 今後、本ガイドラインが、ビルシステムに関わる多数のステークホルダに広く活用され、ビルシステムのサイバーセキュリティ対策が少しでも進むことを期待するものである。

1. はじめに

1.1. ガイドラインを策定する目的

1.1.1. ガイドラインの目的

近年のサイバー攻撃技術の高度化や様々なシステムが益々ネットワークに繋がっていくDX化が進展していく状況の中で、制御システムへのサイバー攻撃リスクも高まってきている。重要インフラ分野においては、国の政策としてサイバーセキュリティ対策を進めるとともに、各業界や個別の事業者においても取組が進んできており、ビルシステムに関しても共通編第1版の発行により、サイバーセキュリティ対策は進展しつつある。

本ガイドラインの目的は、ビルシステムのサイバーセキュリティに関して、その確保のためのガイダンスを示すことである。ここでいうビルシステムには、ビルを運営するためのシステムを構成する全てのサブシステムが含まれており、このようなビルシステムの概念について概要を整理し、それに対する脅威を示すとともに、これらの脅威に対する対策について、設計、建設、竣工検査、運用、改修／廃棄のビルシステムのライフサイクルに係わる各段階において整理して示すものである。第2版では、さらに実際に脅威に遭遇した際に取るべき対応についても整理をしている。

1.1.2. サイバー・フィジカル・セキュリティ対策フレームワークとの関係

ガイドラインを検討してきたビルサブワーキンググループは、産業サイバーセキュリティ研究会WG1（制度・技術・標準化）の下で分野別検討組織に位置づけられている。

この産業サイバーセキュリティ研究会WG1（制度・技術・標準化）では、Society5.0（仮想空間と現実空間を高度に融合させたシステムにより実現を目指す新たな人間中心の社会の姿）における新たなサプライチェーン（バリュークリエイションプロセス）の信頼性の確保に向けた『サイバー・フィジカル・セキュリティ対策フレームワーク（以下、「フレームワーク」という）』の策定を進めている。

フレームワークでは、Society5.0へ向けた産業・社会の変化に伴うサイバー攻撃の脅威の増大に対し、リスク源（サイバーリスクを生じさせる原因となりうる要素）を適切に捉え、検討すべきセキュリティ対策を漏れなく提示するために、3層構造アプローチと6つの構成要素を用いた新たなモデルを提示している。この新たなモデルを使って、3層ごとに守るべきもの、セキュリティインシデント、リスク源、対策要件を整理するとともに、セキュリティ対策要件ごとに対策例を提示している。

フレームワークは産業界全体を対象にサイバーセキュリティ対策を考えるためのモデル的枠組みを示すものであり、一方、ガイドラインは特定の産業分野を対象にその分野特有の事情を考慮したサイバーセキュリティ対策を検討する上での指針を示すも

の、という関係にある。すなわち本ガイドラインは、フレームワークに対してビル分野に特化した具体的な対応策の検討指針と位置付けられるものである。

このため、ガイドラインの検討にあたっては、フレームワークが示すセキュリティインシデントやリスク源、対策要件についての体系構造との関係整理を実施している。

なお、フレームワークの詳細については、付録 C を参照のこと。

1.2. ガイドラインの適用範囲と位置づけ

1.2.1. ガイドラインの対象者

本ガイドラインには、ビルシステムを構成する全てのサブシステムにおける共通的なセキュリティ対策が含まれており、ビルシステムに関わるステークホルダはもちろんのこと、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、セキュリティに係るベンダなども対象としている。

具体的な対象者としては以下を想定している。

- ビルオーナー
- ゼネコン、サブコン
- 設計事務所
- 個別システム事業者（ビル管理システム、空調、エレベータ、ビデオ監視、電力・熱供給　等）
- ビル管理会社
- テナント
- サービスプロバイダ
- セキュリティベンダ、ネットワークシステムベンダ
- 自治体、関係省庁　等

1.2.2. 対象とするビル

ビルにはその規模に応じて大規模ビル、中小規模ビル、利用形態に応じてオーナービル、テナントビル、建設・利用の段階に応じて新築ビル、既存ビル、用途に応じてオフィスビル、施設等、様々な視点からの区分を行うことが可能である。これらそれぞれの状況やその組み合わせに応じて、ビルシステムの構成、管理体制、運用規模等の条件が異なっているため、適用できるサイバーセキュリティ対策も異なっており、どのレベルのセキュリティを確保すべきか等の判断も異なってくる。

このように区分の仕方によって様々に条件の異なるビルであるが、本ガイドラインは、基本的に全てのビルを対象としており、条件の違いも踏まえながら適切に活用いただくことを想定している。

なお、対象とするビルの詳細については、3.3 も併せて参照のこと。

また、本ガイドラインの構成要素、各要件は、ビルに限らず同じような制御システムを用いる施設等でも参考になるものと考えられる。例えばビルではなく、一般住宅を対象とするスマートホームに関するガイドラインの検討などが産業サイバーセキュリティ研究会 WG1（制度・技術・標準化）傘下のスマートホームサブワーキンググループで進み、2021 年 4 月に「スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン」が策定された。

1.2.3. 対象とするビルシステム（ビルシステムの定義）

ビルシステムはビルの管理・運用を行うための制御システムであり、受変電制御システム、熱供給制御システム、空調制御システム、給排水制御システム、照明制御システム、昇降機制御システム、防犯・入館管理システム、防災監視システム、監視カメラシステム、またこれらを統合的に監視・管理するためのビル管理システム等の個別の設備・システムが存在する。通常はそれぞれ独立したサブシステムとなっており、全体としてビルを管理・運用するビルシステムを構成する。

このため、本ガイドラインでは、ビルシステムとしては、各サブシステム及び全体としてのビルシステムを指すこととする。なお、本ガイドラインでは、個別のサブシステムの違いではなく、共通的な要素に絞って脆弱性やリスク、セキュリティ対策等をまとめているもので、各サブシステムに何らかの関わりを持つステークホルダが、共通に検討すべきサイバーセキュリティ対策の指針を示すものである。

なおビルの管理・運用にあたっては、リソースの管理や課金管理、テナント等の顧客管理や営業管理のために IT システムも利用されているほか、制御システムと接続されているケースもあるが、IT システムのサイバーセキュリティに関しては一般的に取り組みの進んだ世界となっており、ここでは対象とはしない。但し、IT システムと接続するためのビルシステム側のインターフェースまでは対象として検討を行っている。

またビルに関連するシステムとして、最近では IoT の活用等も進みつつあり、テナントやビルの利用者向けに各種の新たなサービスを展開するシステムが、ビル内に存在するケースも増えている。ビルそのものの運用からは外れるため、ガイドラインの対象外ではあるが、将来的にはこれらのシステムについてもサイバーセキュリティの議論が必要になると思われる。

1.2.4. ガイドラインの位置づけ

ガイドラインを作成するにあたって、ビルサブワーキンググループでは、いくつかの方針を定めて検討を行ってきた。

- ガイドラインはマスト（レギュレーション）ではないものにする。ビルシステム関係者が何を優先して対策していくか決めるための情報を提供する。

- 対象者は、ビルオーナー、ゼネコン／サブコン、設計者、設備ベンダ、管理者等、ビルの企画・建設から運営管理に関わるステークホルダ全般とする。
- ガイドラインは共通編と個別編（詳細編）の 2 階建てにする。
- 共通編は初歩的な対策をまとめたものであり、厳し過ぎず、ポイントを押さえたものにする。
- 設計やテスト等の各段階のチェックプロセスについて、関係者間の共通リファレンスを作る。
- 個別編では、共通編を超える部分についての詳細な方策や、更なるセキュリティ投資に関する経営判断の材料を提供する。

本ガイドラインは上記方針の共通編にあたるものである。ビルの関係者が共通に参照し、ビルシステムについての初歩的なサイバーセキュリティ対策を考えていく上での入り口となる情報を提供することを目指している。

以下では、このガイドラインの位置づけとして、誰を対象とし、ビルシステムのサイバーセキュリティ対策について考えたり取り組んだりしていくにあたってどのように取り扱われることを想定しているのかを記す。

(1) ガイドラインはビルの全てのステークホルダを対象とする

制御システムのサイバーセキュリティに関しては、ビルシステムに限らず様々な分野で「インターネットとは接続していないからサイバー攻撃を受けることはないのでシステムは安全であり、対策も必要ない。」という声をよく聞く。しかし実際には次のような状況もみられ、必ずしも安全とは言えないのが現実である。

内部からの攻撃を受けるケース ：

- 保守作業のために持ち込まれる外部端末や保守情報等を入れた USB メモリ等が、作業員の知らないうちに別の場所で感染しており、それがビルシステムに接続されることでマルウェア等の感染がおこる場合がある。
- 悪意を持った攻撃者の場合には、金銭で作業員を買収し、内部からマルウェア等を送り込む場合もある。

繋がっていないはずの外部ネットワークから攻撃を受けるケース ：

- 現場の担当者／担当部署や保守ベンダが管理等の利便性向上のために勝手に外部回線を引き込むケースがあり、十分なセキュリティ措置が施されていないと、外部ネットワークからの侵入を受ける場合がある。

- 管理上の目的のために情報系ネットワークに接続しているが、インターネットには直接接続していないようなケースでも、情報系ネットワークを経由して、インターネットからの外部侵入を受ける場合がある。

直接狙われたわけではなくても、インターネットに広く蔓延しているマルウェア等の予期せぬ侵入を受けてしまう「もらい事故」のようなケースも考えられ、また、ありふれたビルであっても入居者が攻撃者のターゲットになり得る何かしらの条件を持っていれば狙われて攻撃されるケースも考えられる。「外部とは繋がっていないから」といった理由や、「目立つビルではないから」ということは、サイバーセキュリティについて検討しなくてもよいという理由にはならない。このため、**本ガイドラインでは、全ての種類のビル、ビルシステムに何等か関わりをもつ全てのステークホルダを対象としている。**

一方でこのガイドラインは、共通編としてなるべく幅広い状況に対応できるよう、代表的な構成を一般化したユニバーサルなものとして作られている。そのため、個別のビルに当てはめた際には、冗長な部分や異なる部分も含まれると考えられ、ガイドラインの記載された全ての項目への対策が必ず必要になるというものではない。ガイドラインの利用にあたっては、実際のビルのアセスメントに使用してみたうえで、必要な部分をピックアップして取り入れることが大事となる。

(2) ガイドラインは共通編と個別編の2階建て構成とする

3 章において、対象とするビルシステムやそのリスク、セキュリティ対策の考え方について具体的に説明をするが、**本ガイドラインでは、上述したように個別のビルシステムに特化せず、共通的な要素について整理を実施し、共通編としてまとめている。**個別のサブシステムに特化した内容については、サブシステムごとの個別編を今後検討していく予定である[1]。

(3) ガイドラインは初歩的な対策をまとめたものである

本ガイドラインはこれまでサイバーセキュリティ対策への取組が遅れていたビルシステムの世界に対して、サイバーセキュリティ対策の初歩的な情報を与えるものであり、実際の対策を考えるための、細かい情報までは提供していない。ビル業界としてサイバーセキュリティへの取組はこれからという段階であり、初歩的なものの中でも、更に可能なものから取り組むことが大事である。ガイドラインは各ステークホルダの共通の知的拠り所となるものに過ぎず、**それぞれの立場に応じて、必要な内容をピックアップし、それぞれの要求内容や要求レベルに合わせてアレンジして利用することを期待し**

[1] 個別編については、2022 年 10 月に、空調システム（熱供給制御システム、空調制御システム、給排水制御システム）を対象とした「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（個別編：空調システム）第 1 版」を策定した。

ている。但し、記述が概略的過ぎて判断に迷う点も多いと考えらえるので、具体的な対策の検討にあたっては、必要な知識を備えたコンサルティングやシステムインテグレータ、ベンダ等と相談することを勧める。サイバー攻撃は常に進歩しており、また対策についても、新しい製品が提供されることで、新しい対策が実施可能になるなどがあり、常にサイバーセキュリティの最前線の情報を備えた組織に相談することが大事である。

初歩的な対策という意味では、仮に記述内容を全て実施しても用意周到に準備された攻撃には対応できないが、最低限実施して欲しいレベルは満たしており、もらい事故やちょっとしたいたずら、ビル内部からの物理的攻撃にはある程度対応出来ると考えられる。

但し、重要度の高いビルをより強固に守りたい場合や、守る必要がある場合には、ガイドラインを入り口としつつ、それ以上の対策を実施することが望まれる。

(4) ガイドラインは検討の糸口でありマストではない

ビル及びビルシステムは様々であり、ビル1棟1棟ごとに、置かれた状況も条件も異なっている。サイバーセキュリティ対策の実施には、今までにはなかった新たなコスト負担も必要となる。このコスト負担がステークホルダの間で必要経費として認識されるまでの間は、投資効果や優先順位なども考慮して対策を行うことになると思われる。そのため、画一的な対策の適用は困難であるとともに、必ずしも適切ではないと考えられ、**本ガイドラインに記載する各セキュリティ対策もマストのものであるとは考えていない。**それぞれの状況に応じて、出来るところから始めることが大事であり、まず本ガイドラインをベースとしたリスクアセスメントを実施して、ビルシステムにどのようなサイバーセキュリティリスクがあるか知ることから始めるのが重要である。

(5) 本ガイドラインは第一歩であり、状況や立場に応じて工夫・改善をして欲しい

本ガイドラインは、これまでほとんどサイバーセキュリティ対策が行われてこなかったビル業界向けに初めてまとめられたものである。あらゆるビルにあまねく対応できるものではなく、各設備システムが個別に管理されるとともに、統合ネットワークで連携し、一部はクラウド等外部サービスを利用するようなシステム構成を想定し、そのモデルの範囲で整理している。このモデルと大幅に違う場合には、対策要件の読み替えや、絞り込み、対策内容の更なる充実化なども必要になる。それぞれの利用者の立場において必要となる情報は、利用者自身がより深く知っているものであり、是非とも本ガイドラインを唯一のものとせず、自社向け、業界向けにアレンジしたり、手引き等の副読本を作成したりすることで、利用者それぞれにとってサイバーセキュリティ対策をより進めやすくしていくことが望ましい。

1.3. 本ガイドラインの構成

ガイドラインの本節以降の部分は、以下の項目に大別される。

■第2章: ビルシステムの特徴とビルシステムに対するサイバーセキュリティの脅威の現状を示す。

■第3章: ビルシステムにおけるサイバーセキュリティ対策の基本的考え方やビルの条件に合わせたガイドラインの活用の仕方を示す。

■第4章: ビルシステムにおけるサイバーセキュリティリスクと対策ポリシーを示す。

■第5章: ライフサイクルのフェーズごとに実施すべきセキュリティ対策について示す。

■第6章: サイバー攻撃によるインシデント発生時の対応について示す。

また、本ガイドラインには、補足資料を提供する以下の付録も含まれる

■付録 A: 本書で使用する用語集

■付録 B: JDCC の建物設備システムリファレンスガイドとの関係

■付録 C: 建物設備システム リファレンスガイド インシデント対応・セキュリティソリューション編との関係

■付録 D: サイバー・フィジカル・セキュリティ対策フレームワークとの関係

■付録 E: 参考文献

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

従来のビルシステムは、電力(受変電)、熱源、空調、照明、エレベータ、防災等の個別の設備ごとにシステムが一塊のシステムとして独立しており、しかもその制御ネットワークは IP(Internet Protcol)に対応していないフィールドネットワークであることが多かった。このため、サイバーセキュリティについては、ほとんど気に掛けられることのない状態が続いていた。

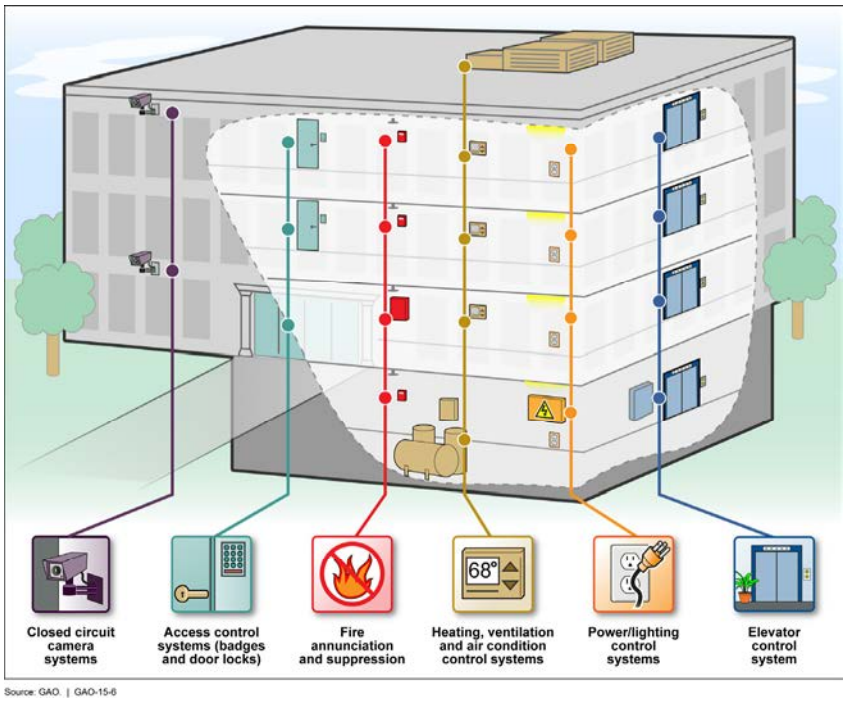


図 2-1　ビルの設備制御システムの概略例（各システムが独立専用システム）

（出典:FEDERAL FACILITY CYBERSECURITY, DHS and GSA Should Address Cyber Risk to Building and Access Control Systems (2014/12, 米国 GAO))

これに対して、最近の社会の IT 化、ネットワーク化の流れの中にあって、ビルシステムを含む制御システム全般について、徐々に情報ネットワークとの接続がなされ、IP 化が進んできている。フィールドネットワークの物理媒体として Ethernet を採用するものも増加しており、末端のセンサや装置に対しては従来どおりの接点接続やバス接続を用いるものであっても、コントローラやゲートウェイ装置より上位の制御・監視端末側では、IP に対応した BACnet/IP 等のプロトコルを用いる物も増えている。

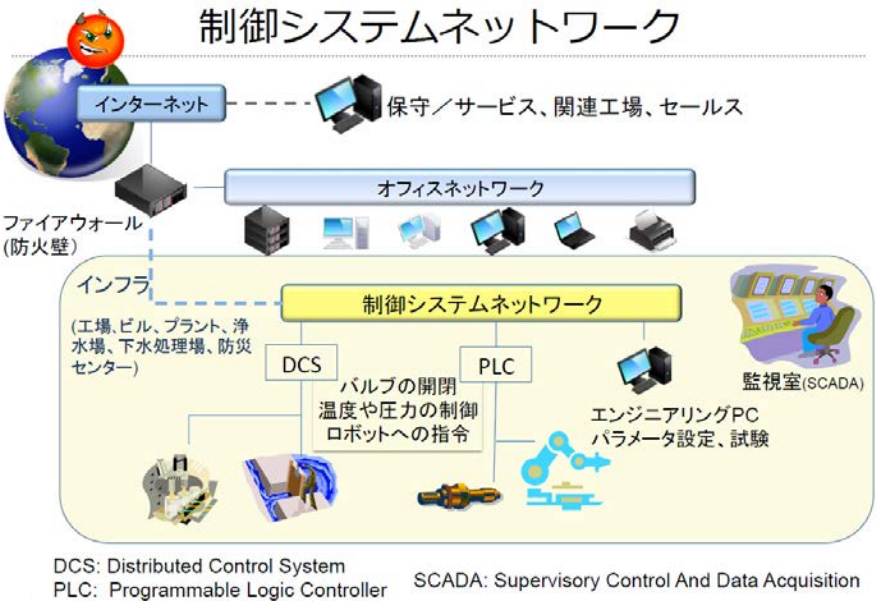


図 2-2　つながる制御システムネットワーク

（出典：制御システムセキュリティの脅威と対策の動向及び CSSC の研究概要について（2018/5/11，技術研究組合制御システムセキュリティセンター)を元に加筆）

制御システムネットワークの IP 化に伴い、従来は個別に構築していた設備ごとのシステムを相互に接続して連携させたり、外部のインターネットを経由したリモート監視やリモートメンテナンスを実施したりする例も増えてきている。

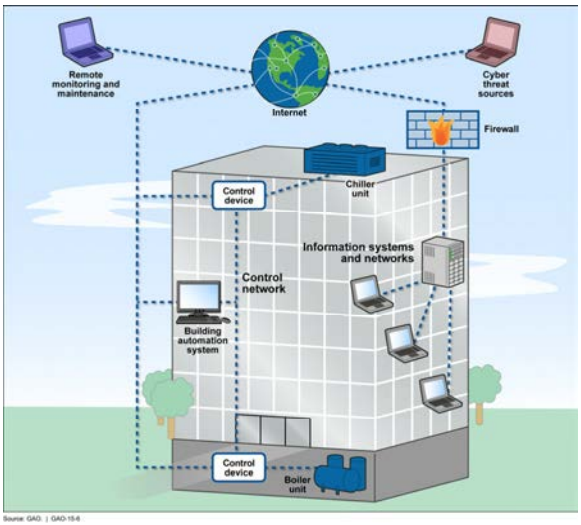


図 2-3　空調等をインターネット経由で遠隔から管理する例

（出典：FEDERAL FACILITY CYBERSECURITY, DHS and GSA Should Address Cyber Risk to Building and Access Control Systems (2014/12，米国 GAO))

このように制御システムのネットワーク化、相互接続化、インターネット対応が進むことによって、従来は想定していなかったような外部からのサイバー攻撃を受ける機会も増えてきている。例えば、監視端末（HMI/HIM）が Windows OS を採用しているようなケースでは、オフィス等における IT システムと同様にウィルスやマルウェアによる被害を受ける可能性がある。

また、特に制御システムを狙った攻撃も発生している。2010 年にイランの核燃料施設で発生したサイバー攻撃では、制御用 PC に入り込んだマルウェア Stuxnet が PLC 経由でウラン濃縮のための遠心分離機を不正に制御し、機器の破壊にまで至っている。

制御システムにおいては、システムの保護制御で想定している範囲を超えた攻撃を受けると、システムの物理的な破壊に至る可能性もあることから、システムの設計段階でサイバー攻撃を受けた場合を想定した安全設計を行うことが重要である。

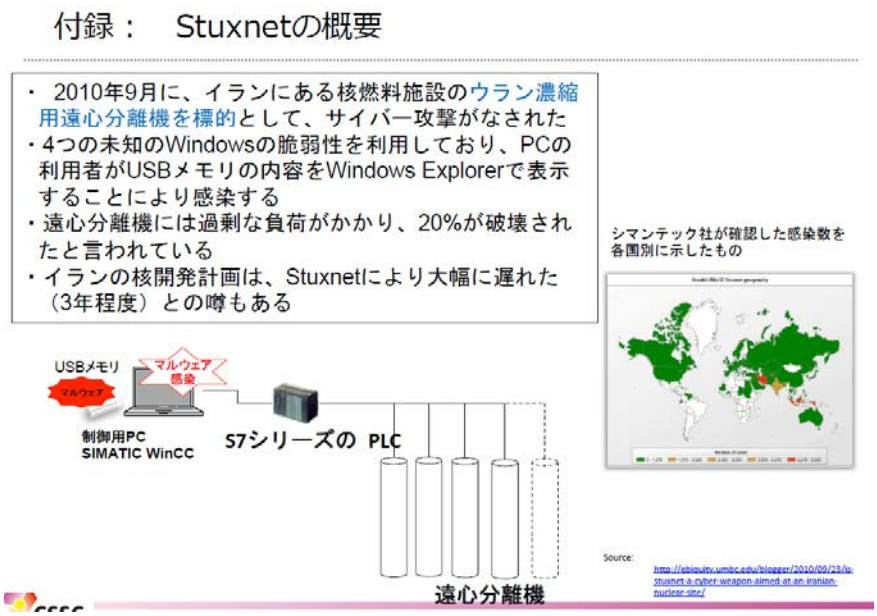


図 2-4　制御システムへの世界初の攻撃といわれる Stuxnet による攻撃

（出典：制御システムセキュリティの脅威と対策の動向及び CSSC の研究概要について（2018/5/11，技術研究組合制御システムセキュリティセンター））

この Stuxnet 以降、制御システムへの攻撃が顕在化しており、2015 年 12 月、2016 年 12 月には、ウクライナで電力会社への攻撃が発生し、制御システムが不正操作されることによって大規模な停電も発生するなど、社会的影響も生じる事態となってきている。

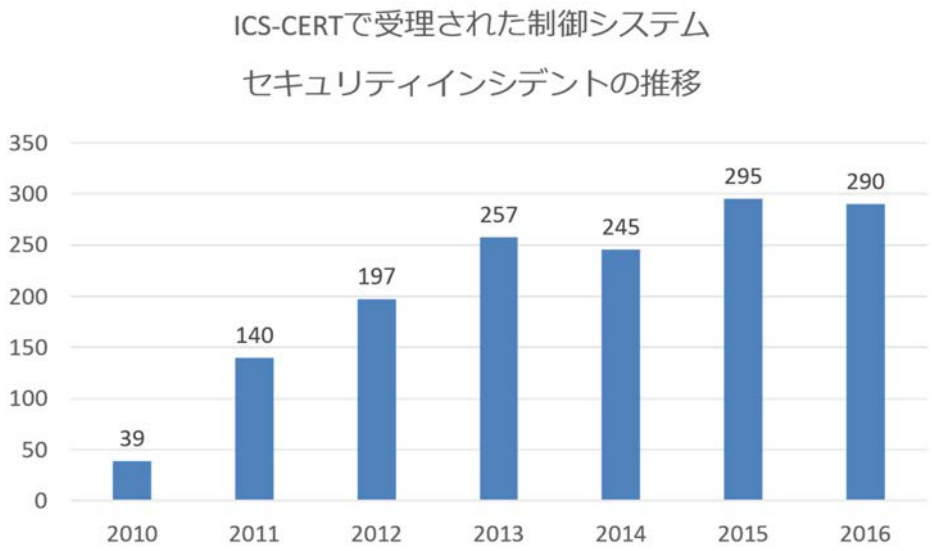


図 2-5　制御システムを狙った攻撃の増加

（出典：ICS-CERT Year in Review（米国 NCCIC）2016 年版までの複数年のレポートより作成）

このように社会の重要インフラを担う制御システムは、IT システムと同様に日常的にサイバー攻撃を受ける状況となっており、同じような制御システムを用いているビルシステムに関しても、既にサイバーセキュリティ問題と無関係ではいられない状況になっている。

実際、ビルを狙ったサイバー攻撃も海外では既に発生しており、次節ではその事例について紹介する。

2.2. ビルシステムにおける攻撃事例

実際にビルや建物、施設等の設備システムに対して行われた攻撃の例を紹介する。

2.2.1. MIT（Massachusetts Institute of Technology、マサチューセッツ工科大学）の学内ビルの照明ハッキング

2012 年 4 月、MIT の学生が学内ビルの照明をハッキングし、屋外から見える窓の照明を使って巨大なテトリスゲームにした。ハッキングは公開のもと、デモンストレーションとして行われ、実際に窓照明によって作られた巨大な画面の上から下へと、照明によって色付けされたテトリスのマスが流れ落ちる様子が、動画としても残されている。

攻撃として行われた内容自体は、いたずらのデモンストレーションであり、実害の無いものだが、実在のビルの照明のシステムを実際に乗っ取り、自由に制御できることを

示したものであり、実行する内容次第では、例えば照明を落としてその間に何らかの犯罪を行うなど、実害をもたらすような攻撃も可能であることを示している。

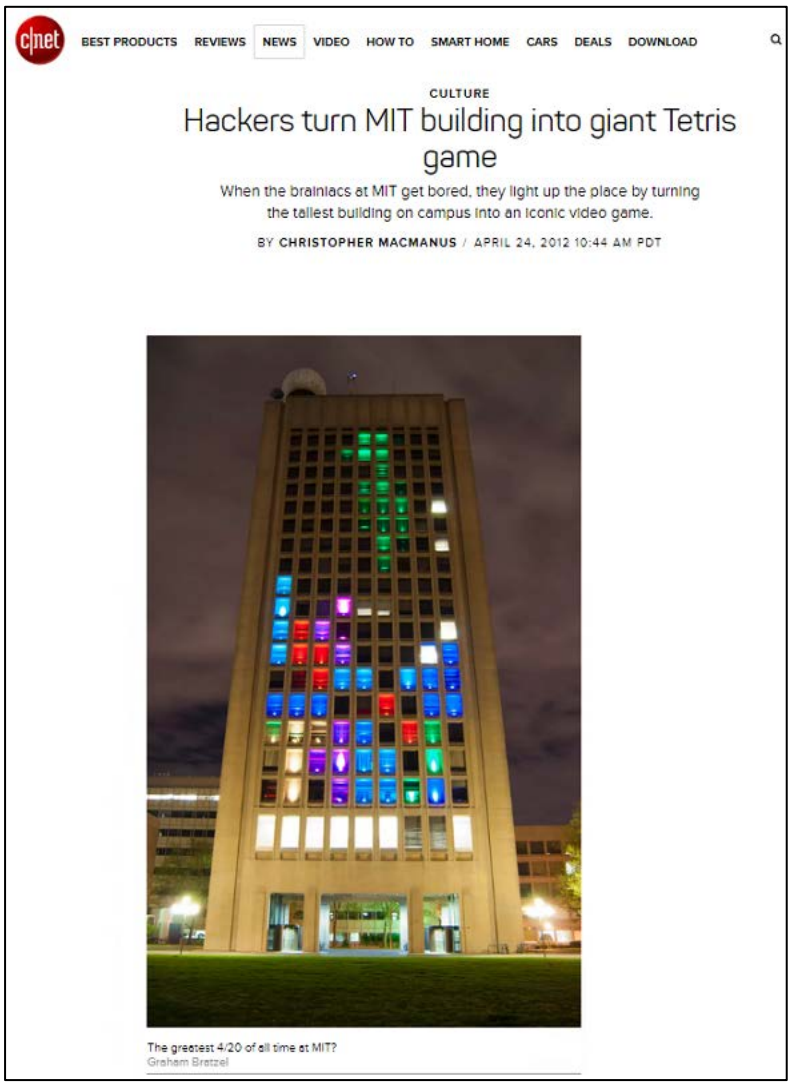


図 2-6　事件を報道する記事

（出典： https://www.cnet.com/news/hackers-turn-mit-building-into-giant-tetris-game/）

2.2.2. ターナー・ギルフォード・ナイト収容所の警備システムハッキング

2013 年 6 月、マイアミのターナー・ギルフォード・ナイト収容所の警備システムがハッキングを受けて収容房の扉がリモート解除され、収容されていた対立ギャング同士の抗争事件に発展した。実際に開放されたのは、刑務所内の収容房に限られたため、外部への影響はなかったが、収容所全体の扉が開錠されていれば、受刑者が外部へ逃走するなど、近隣社会への影響も起こり得る状況であった。

ビルにおいても多くの警備システムが稼働しており、入場者の制限や館内滞在者の安全管理等を実施している。警備システムがハッキングされることは、ビルの安全の基本を脅かすこととして、大変大きな問題だと言える。

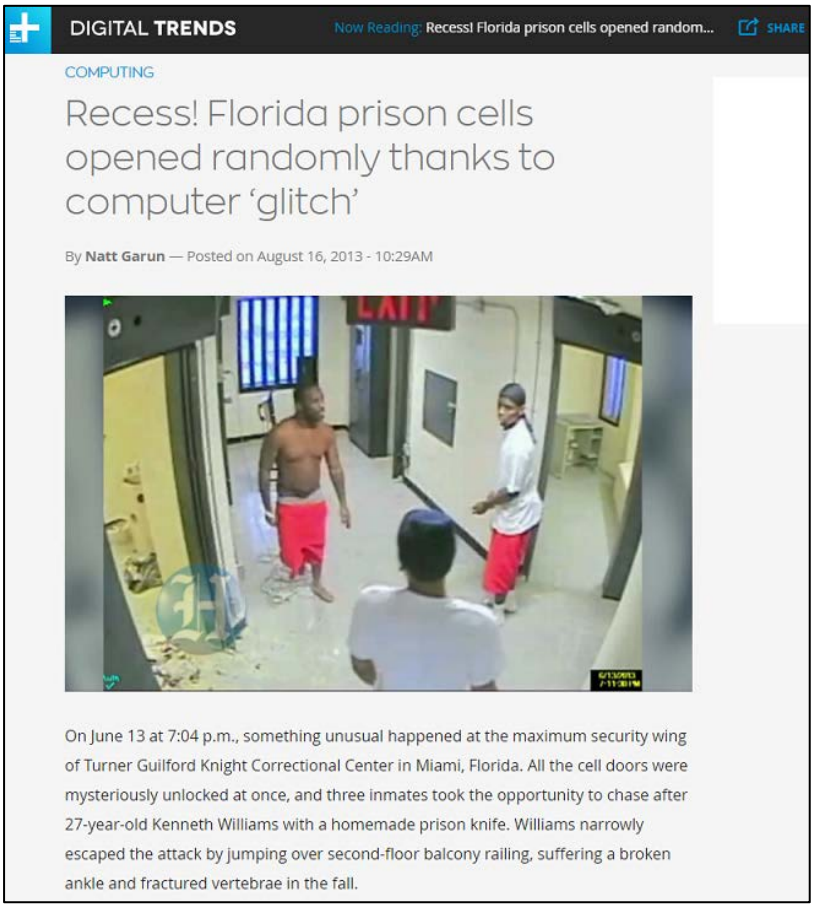


図 2-7　事件の関連情報について報道する記事

（出典： https://www.digitaltrends.com/computing/suspicious-prison-glitch-blamed-for-opening-all-cell-doors-in-max-security-wing/）

2.2.3. ラッペーンランタでの DDoS 攻撃による暖房停止

2016 年 11 月、フィンランド、ラッペーンランタのビルが DDoS 攻撃を受け、暖房が停止した。11 月のフィンランドは既に外気温マイナス 2 度の環境であり、このような中で、数時間にわたって暖房が利用できない状況が継続した。

近年、日本の夏は気温が高まる傾向にあり、2018 年の夏には全国の最高気温を更新するなど、空調が健康の維持や時には生命の維持にも欠かせないものとなってきている。例えば夏の非常に暑い気温状況の中、空調がサイバー攻撃によって停止するようなことがあれば、ビル内で働く人達の業務効率が下がるだけでなく、体調不良者を出す可能性も考えられ、またビル内に設置されたサーバ類が誤動作を起こすようなこ

とがあれば、ビジネス的損失にもつながる可能性がある。ビルのオーナーにとっても、ビルに入居するテナントやビル内で働く労働者にとっても、非常に大きな問題となる可能性がある。

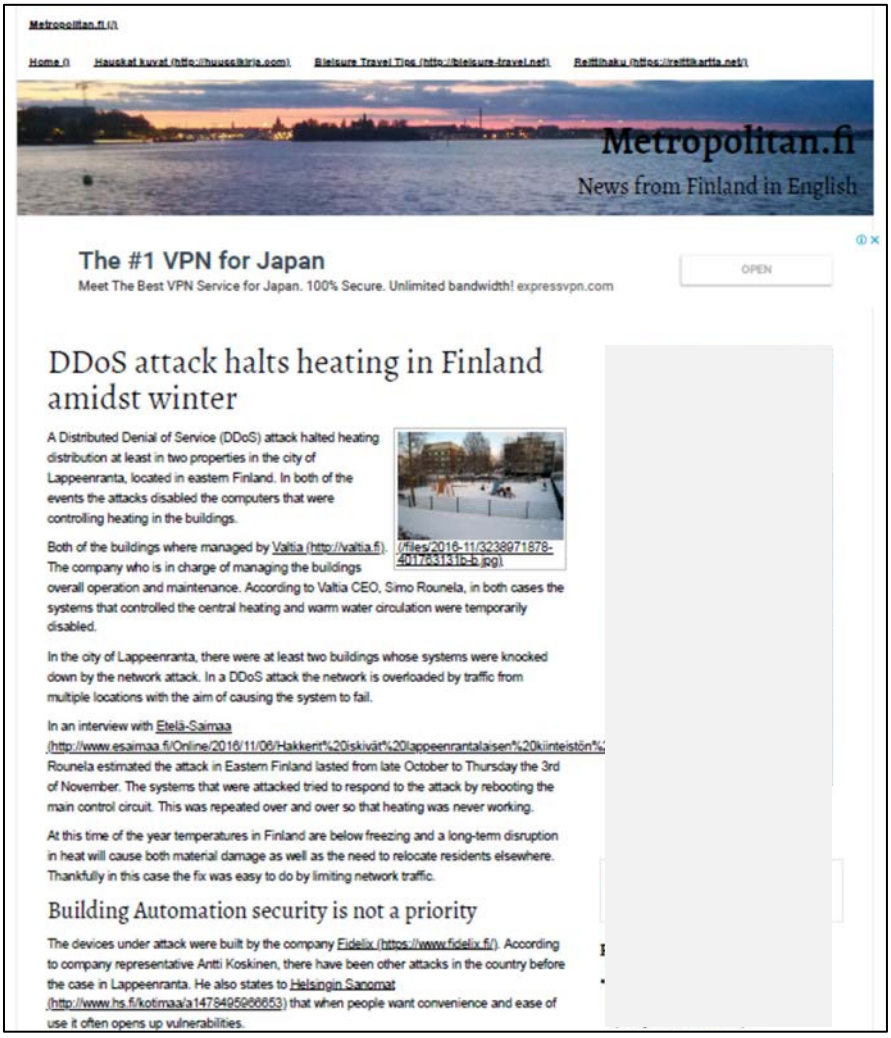


図 2-8　事件を知らせる現地報道記事

（出典： http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter）

2.2.4. ホテルでの宿泊客の閉じ込め・閉め出し

2017 年 1 月、オーストリアの 4 つ星ホテルで、客室のカードキー発行システムがランサムウェアに感染し、一切のシステム操作が不可能となったため、客室扉の施錠、開錠が不可能となり、宿泊客が閉め出される事態が発生した。制御システムの場合、狙われて攻撃される事例も多いが、ランサムウェアのように不特定多数を狙った攻撃において、もらい事故のように攻撃を受けてしまうことを示す例である。

ビルの場合でも、監視端末やコントローラに WindowsOS のような汎用の OS を使用していれば、十分に起こり得る状況であり、これは何も部屋のオートロック、セキュリティシステムに限る話ではない。一方でビルシステムの場合には、一般にパッチ当てが困難であると言われており、システムが脆弱性を抱えたまま運用することを余儀なくされることが多く、マルウェアやランサムウェアのようなシステムの脆弱性を突いた攻撃への対応が十分に取れない可能性もある。そのため、今後はこのようなもらい事故への対策も大きな課題となっていくと思われる。

なお、被害を受けたホテルでは、顧客への補償の他、しばらくの間閉館して鍵システムの刷新を余儀なくされ、結果として多額の被害を受けており、予防対策への投資の重要さを示す事例でもある。

図 2-9　事件を報道する記事

（出典： https://edition.cnn.com/2017/01/30/europe/hackers-lock-out-hotel-guests-trnd/index.html）

2.2.5. インターネットカメラへの大量ハッキング

2018 年 4 月、日本国内各地で、インターネットカメラがハッキングされ、画面が書き換えられる被害が多数発生した。典型的ないたずら事例ではあるが、監視カメラが容易にハッキングされ、情報を書き換えられてしまうことを示す事例である。ビルの監視カメラであっても、外部ネットワークから利用できる形態の監視カメラが存在する場合があ

る。もしこれが重要性の高いビルや施設の監視カメラで行われ、カメラ監視が行き届かない状態で犯罪行為が行われれば、犯罪に気がつかない、あるいは犯罪の証拠を検証できないというような事態にもなる。攻撃や障害の内容次第では、ビルとしても責任を問われるような可能性もあり、身近な問題として捕らえる必要がある。

2.2.6. テストによるハッキング事例

海外ではビルシステムのセキュリティテスト（ペネトレーションテスト）として、攻撃を実施し、実際に乗っ取りに成功してしまった事例も複数報告されている。

2013 年 8 月には、オーストラリア・シドニーのオフィスビルを対象にテスト攻撃が実施され、フロア空調やエネルギーメーター、アラームといったビル管理機能への侵入が実現してしまったという報告がある。このビルの設備管理に使われているデバイスは、世界中で数十万個が利用されているありふれたものであり、このことから世界中のビルが危険な状態にあることが分かるものである。

また、2016 年 1 月にも別のチームによって米国内の商業オフィスのビルオートメーションシステム（BAS）に対するハッキングテストが実施され、侵入を実現している。この BAS は複数のビルを遠隔で管理するものであり、全米の複数のビルにおいて自動コントローラに対する完全な指揮権を入手できることを明らかにしたものとなった。

日本においてもビルシステムを対象としたハッキングテストは行われており、やはり課題のある結果となったと報道されている。

このような事例を見る限り、今やビルシステムは普通にサイバー攻撃され得る対象であり、その影響を考慮しながら、個々に必要な対策を実施することが求められている状況にある。

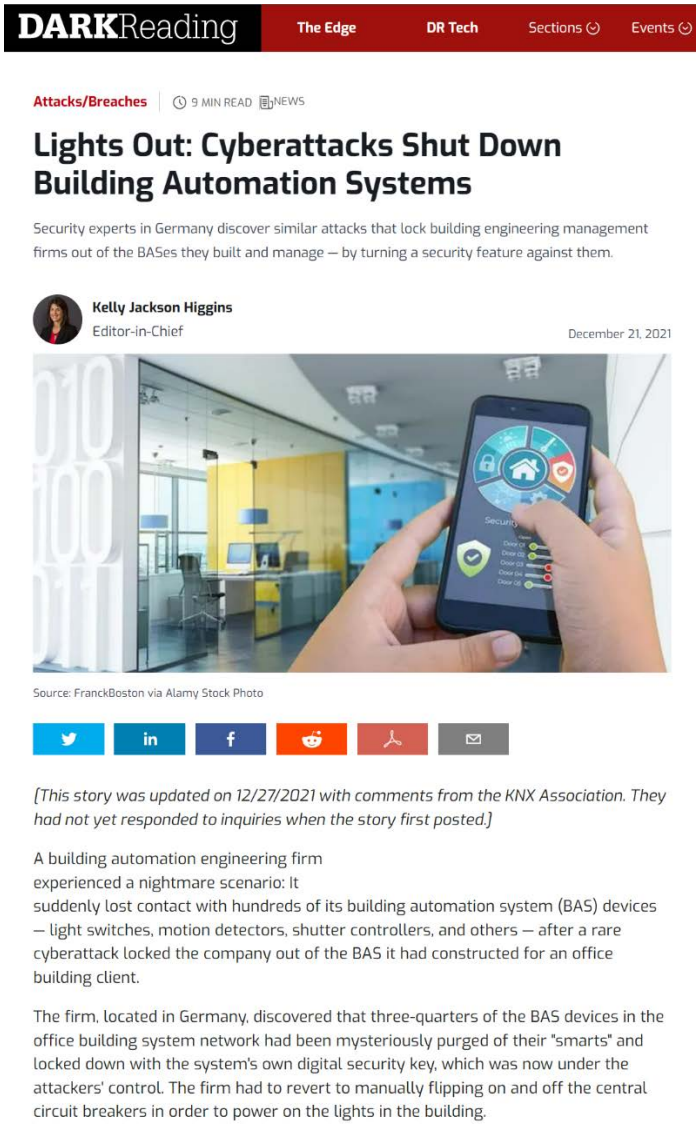
ここで紹介した事例はいずれも報道等でその事実が明らかとなっているものばかりである。海外の事例が多く、日本のビルが攻撃を受けたという記事はほとんどないが、一般に明らかになっていなくても、小さな事故は多数あるという話も聞く。これらがいつか大きな事故に発展する可能性を否定することは難しいので、リスクの程度を考えつつ、必要な対策について検討していくことは重要である。

2.2.7. ドイツにおける BAS 機器のロック事例

2021 年 10 月、ドイツのオフィスビルにおいて、ビルのシステムネットワークにある BAS 機器の 4 分の 3 が制御を失い、照明スイッチ、人感センサ、シャッターコントローラーなどの数百の BAS 機器が操作できなくなった。このビルはビル管理会社によって、遠隔で監視・制御されていたため、リモートでの操作が不可能となった結果、各装置を手動でオン／オフすることを余儀なくされた。

原因はインターネット上に公開されたままの UDP ポートから侵入され、BAS デバイスの機能をアンロードまたは消去され、独自のパスワードでロックされてしまった。そのため、ビル管理会社は BAS 機器へのリモートでのアクセスを失ってしまった。

ビルの建設段階で一時的に設置された IP ゲートウェイを経由して攻撃者が侵入したと考えられるが、この IP ゲートウェイは、ビルの引き渡し後に撤去されるはずだったものが、忘れ去られ、撤去されないままでいた。竣工検査時の確認や図面管理、ネットワーク管理の重要性を示す事例と言える。



DARKReading | The Edge | DR Tech | Sections | Events

Attacks/Breaches | 9 MIN READ | NEWS

Lights Out: Cyberattacks Shut Down Building Automation Systems

Security experts in Germany discover similar attacks that lock building engineering management firms out of the BASes they built and manage — by turning a security feature against them.

Kelly Jackson Higgins
Editor-in-Chief

December 21, 2021

Source: FranckBoston via Alamy Stock Photo

[This story was updated on 12/27/2021 with comments from the KNX Association. They had not yet responded to inquiries when the story first posted.]

A building automation engineering firm experienced a nightmare scenario: It suddenly lost contact with hundreds of its building automation system (BAS) devices — light switches, motion detectors, shutter controllers, and others — after a rare cyberattack locked the company out of the BAS it had constructed for an office building client.

The firm, located in Germany, discovered that three-quarters of the BAS devices in the office building system network had been mysteriously purged of their "smarts" and locked down with the system's own digital security key, which was now under the attackers' control. The firm had to revert to manually flipping on and off the central circuit breakers in order to power on the lights in the building.

図 2-10 事件を報道する記事

（出典： https://www.darkreading.com/attacks-breaches/lights-out-cyberattacks-shut-down-building-automation-systems）

2.3. ビルシステムにおけるサイバー攻撃の影響

ビルシステムがサイバー攻撃を受けるとどのような影響が考えられるのか。米国においてサイバーセキュリティ対策の各種基準を策定している NIST（National Institute of Standards and Technology）が SP800 というドキュメント体系を整備している。このうちの SP800-82 では、制御システムに対するサイバー攻撃を次のように分類している。

表 2-1　ICS に対するサイバー攻撃の分類

（出典： NIST SP800-82、但し表及び日本語訳は JPCERT「制御システムセキュリティの現在と展望 2017」による）

攻撃者	説明
ボットネット運用者	ボットを使って金儲け
犯罪集団	金品の詐取やゆすり
外国諜報機関	スパイ活動
ハッカー	ネットワークへの侵入
内部犯	ルール違反、雇用主への報復
フィッシャー	認証情報の詐取
スパマー	迷惑メール発信
マルウェア開発者	マルウェア作成
テロリスト	破壊工作等で社会不安を煽る

これからは、金銭目的、妨害／破壊工作、情報窃取等がサイバー攻撃の主な内容であることがわかる。

ビルシステムが攻撃を受けることで考えられる最も大きな影響は、ビルのサービスが停止し、その結果として入居者の業務が停止ないしは著しく影響をうけることである。これはビルとしての業務が妨害され、社会的信用の棄損につながるだけでなく、顧客への補償などの金銭被害や顧客離れ等の二次被害へと広がる可能性も考えらえる。

また、ランサムウェア等が仕込まれれば金銭面での直接被害も考えられ、またマルウェア侵入等で情報窃取の被害があれば、その影響がどこへ及ぶかもわからないことが多い。

このような経済的価値の棄損に対して、その影響をどのように捉え、どのように対策していくか、それぞれのビルの状況とも照らして考えていく必要がある。

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

この章ではビルシステムのサイバーセキュリティ対策の考え方について整理をしていくが、はじめに、一般的なサイバーセキュリティ対策の考え方について紹介する。

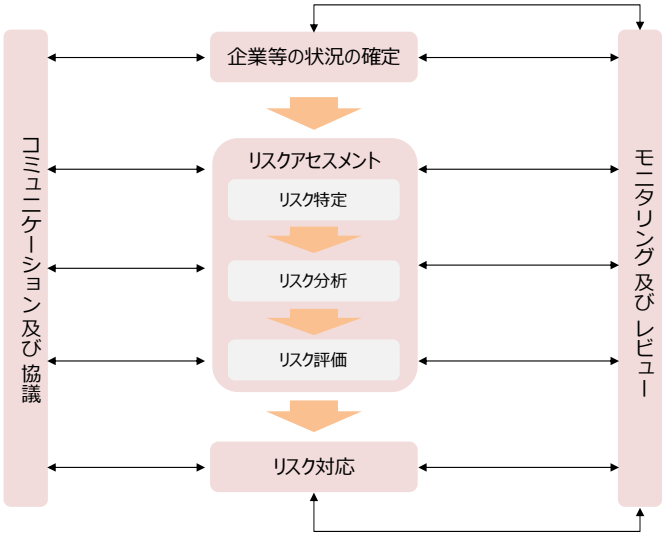


図 3-1　リスクマネジメントの一般的なプロセス（PDCA を含む全体プロセス）

（出典：　サイバー・フィジカル・セキュリティ対策フレームワーク）

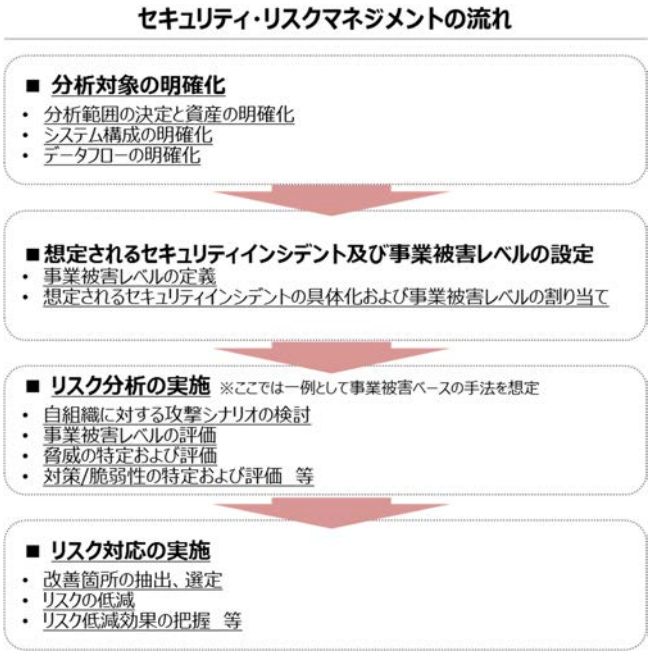


図 3-2　リスクマネジメントの流れ（上図リスクアセスメント部分の詳細）

※上図と原出典が異なるので用語等が異なるが大枠は同じことを説明

（出典：　サイバー・フィジカル・セキュリティ対策フレームワーク）

図では企業という書き方をしているが、まず対象のアセット（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。

更にこれらの過程は随時レビューし、PDCA サイクルとして回していくことが重要である。即ち、リスクアセスメントやリスク対策は 1 回実施すればよいというものではなく、随時状況をモニタし、新たな脅威の発生や対策の陳腐化に対応していかなければならない。

ビルにおいては、例えば設計や建設の段階でセキュリティ対策を実施したとしても、その後の長期にわたる運用過程において、定期的に脆弱性情報を収集し、リスクアセスメントを実施して、必要に応じた追加対策を行うことが望まれるということである。

3.2. ビルシステムの構成の整理

ビルシステムにおけるサイバーセキュリティ対策を検討する上で、前節に述べたようにまずアセット（資産）の明確化を行う。即ち対象となるシステムの構成として、どのような機器がどのように接続されているかを把握する作業を実施する。同様に、各機器がビル内のどこに置かれているのかも、物理的なセキュリティを検討する上で、重要な情報となる。

ビルがその外観デザインも、構造も、内装も、1棟1棟が異なっているように、ビルシステムもまた、1 つ 1 つそれぞれ異なっており、1つとして同じ物は存在しない。但し、ガイドラインを作成するにあたっては、なるべく多くのビルシステムを包含するような形でのモデル化が大事であり、ここでは、様々にあるパターンから現在のビルシステムの姿として代表的な概略例を示す形で、ビルシステムの構成要素についての整理を行った。

次図は様々な個別設備システムからなるビルシステムの全体像をモデル的に示したものである。各システムの構成も接続方法も、それぞれのビルの規模やビルシステムの構築ポリシーによって異なってくるが、代表的な 1 モデルという形で示している。この図においては、個別の設備システムはそれぞれ独立して運用される形となっているが、全体としては統合ネットワークにて接続されており、必要な連携（例えば火災報知器の情報をもとに、居室の鍵を全開錠とするなど）が可能となっている。設備システムごとにサーバ（BA 主装置）や制御端末（HMI）を持っているが、統合が進んだケースとして、統合ネットワークに直接接続された監視端末で、各サブシステムを統合監視するケースも増えつつあるようである。

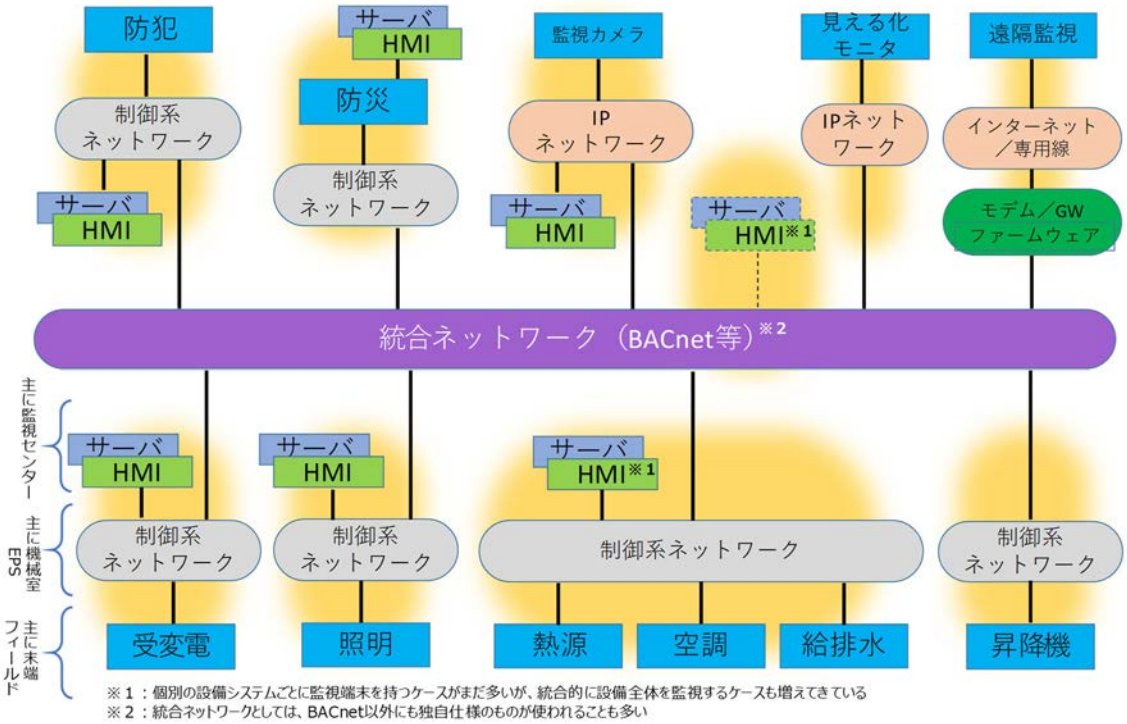


図 3-3　ビルシステムの標準的なモデル（全体像）

更に設備ごとのモデル構成図を次図以降に示す。こちらについても、それぞれビルごとに様々なものが存在するが、代表的な 1 モデルという形でそれぞれ示すものである。

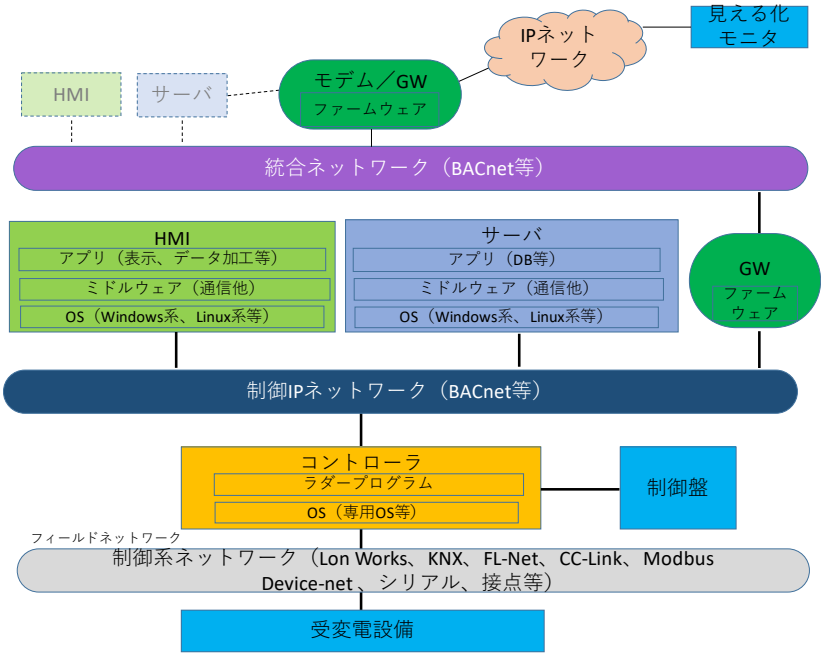


図 3-4　受変電システムの標準的なモデル

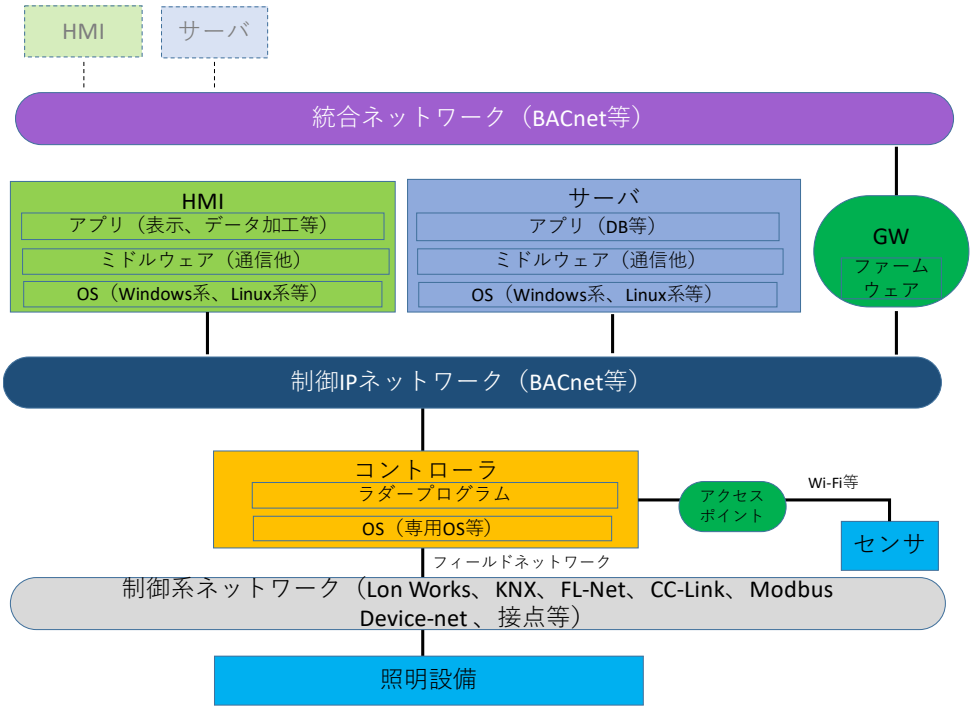


図 3-5　照明システムの標準的なモデル

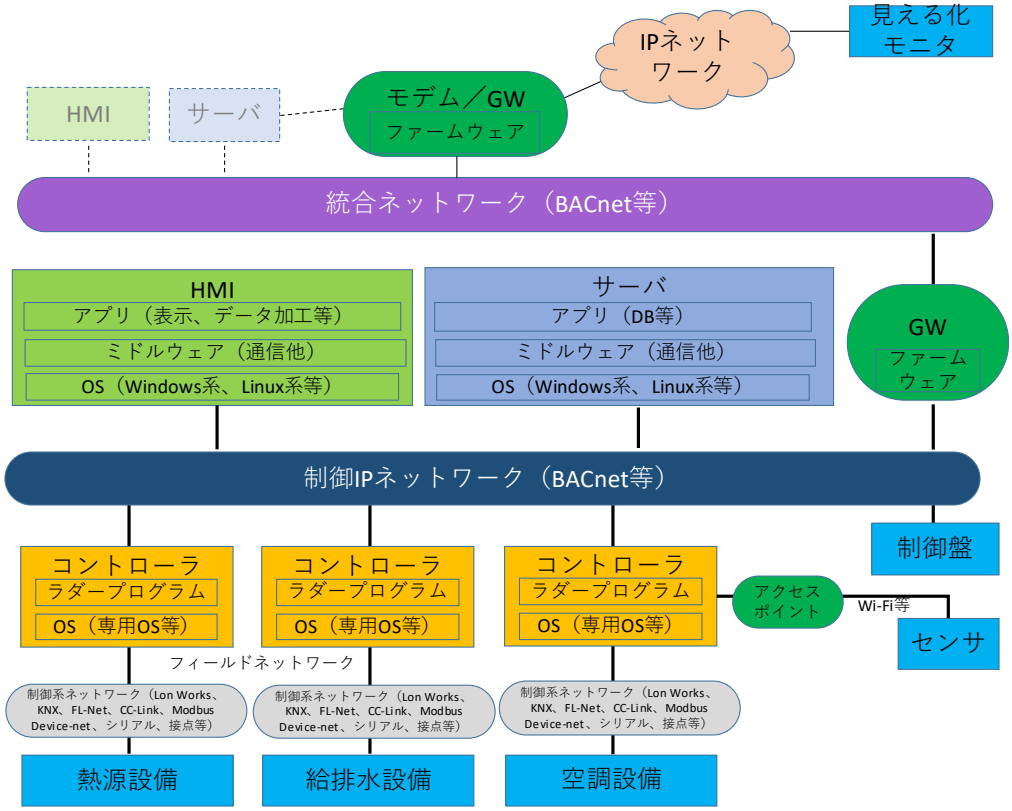


図 3-6　熱源・空調・給排水システムの標準的なモデル

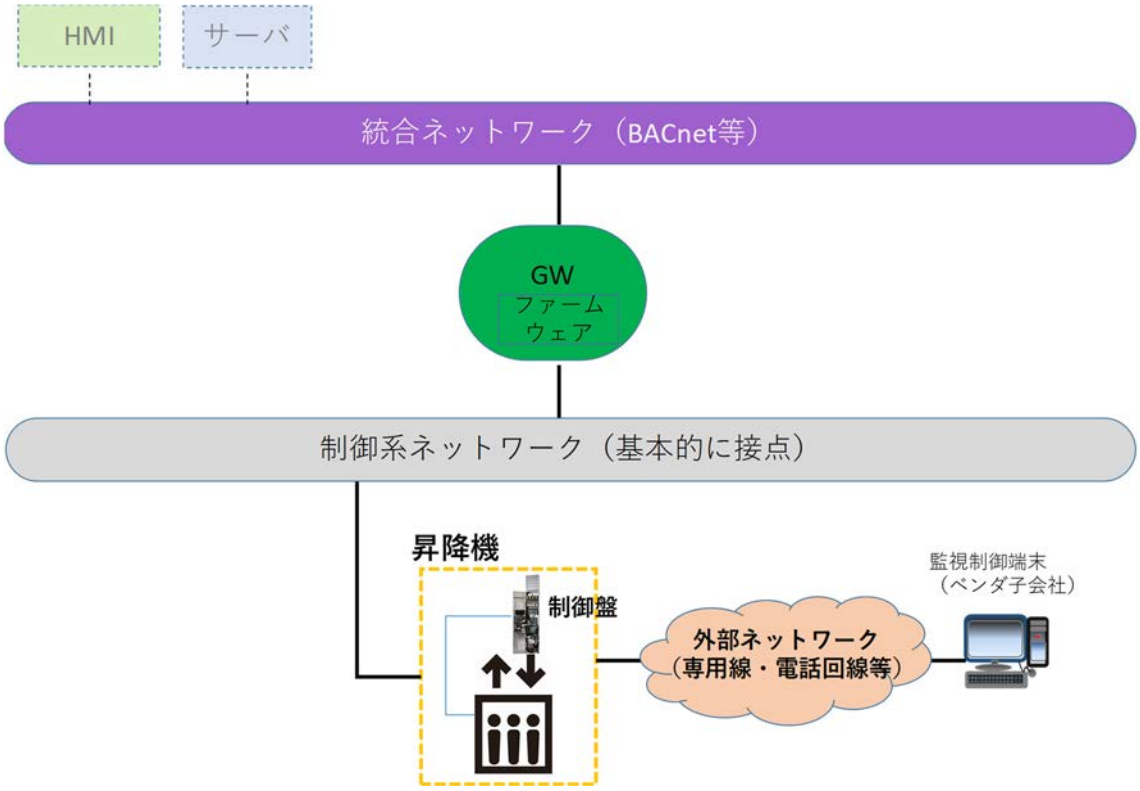


図 3-7　昇降機システムの標準的なモデル

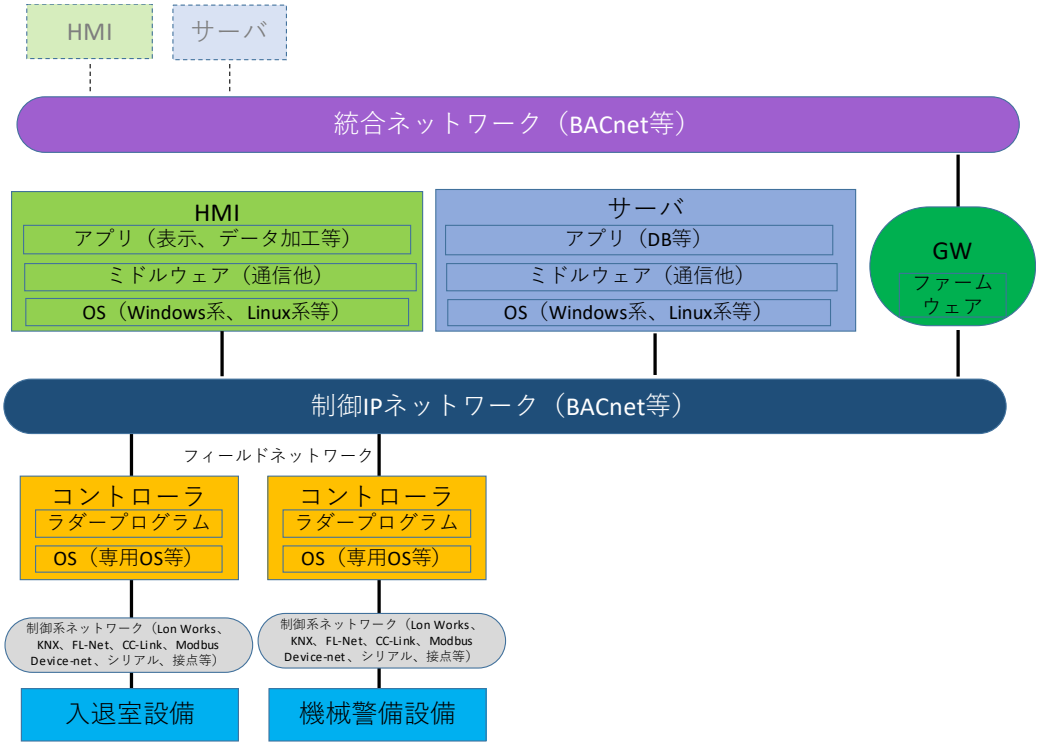


図 3-8　防犯システムの標準的なモデル

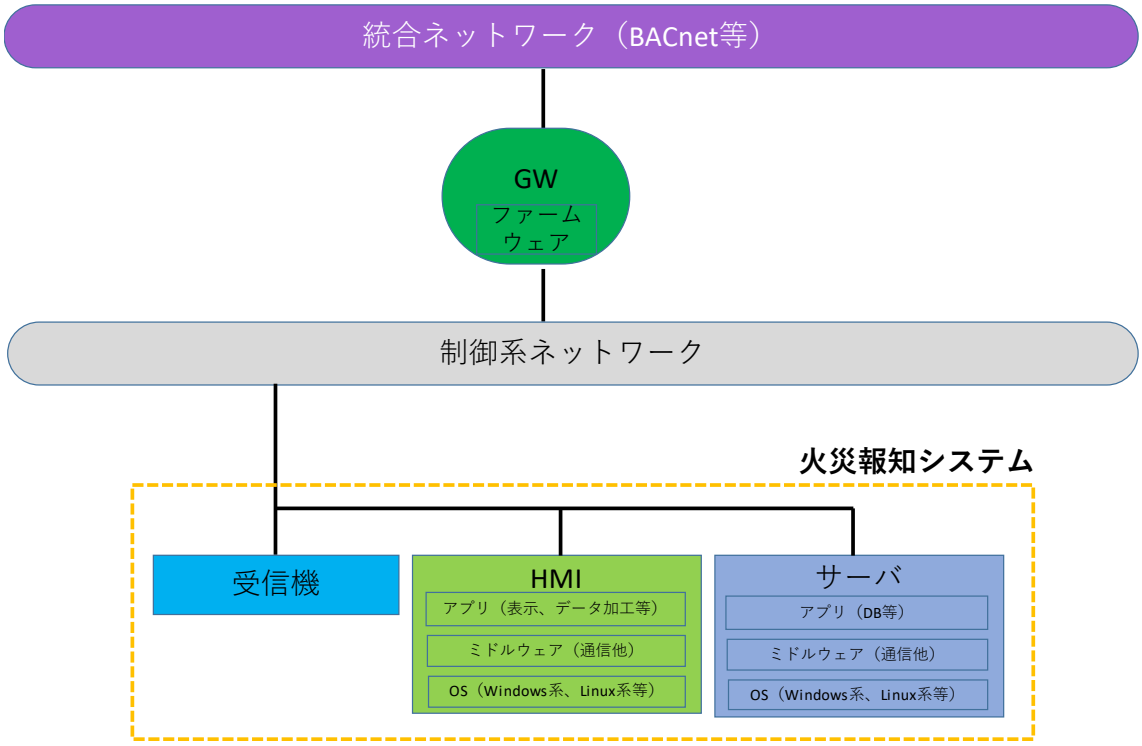


図 3-9　防災システムの標準的なモデル

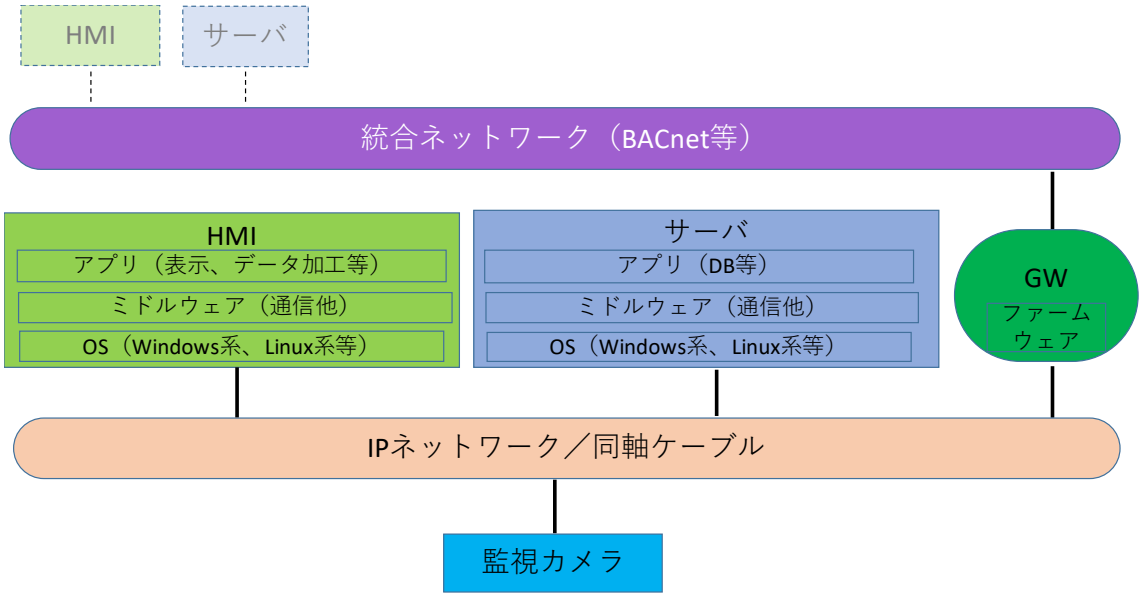


図 3-10　監視カメラシステムの標準的なモデル

いずれの図においても、場所とそこに置かれる機器の関係においては、それほど違いがないことが分かる。場所やそこに置かれる機器の脆弱性等を踏まえた時、ビルシステムに共通的に考えられるリスクポイントを整理したのが次図である。

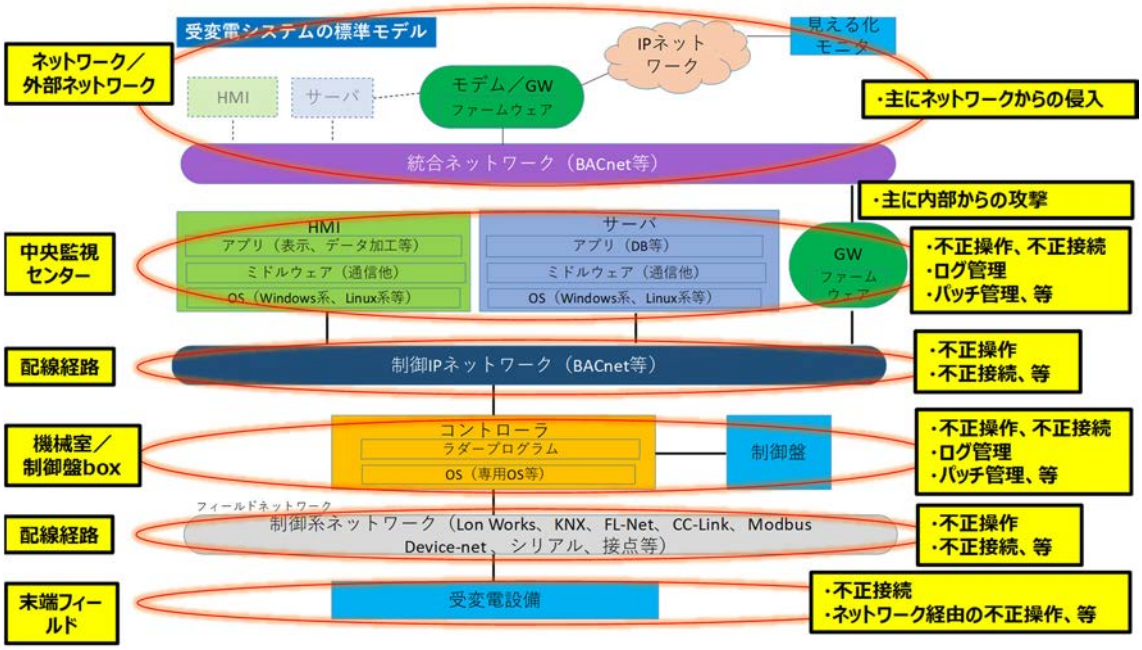


図 3-11　ビルシステムで共通的に考えられる主なリスクポイント

3.3. ビルシステムの特徴

ビルシステムに対するサイバーセキュリティ上のリスクを考える上で、IT システムや他の制御システムとは違うビルシステム特有の特徴について、事前に把握しておくことが大事である。

ビルシステムの大きな特徴としては、次のような点を挙げることができる。

3.3.1. 超長期の運用

ビルは建設後、50 年近くにわたって非常に長期の運用を行うことが一般的である。ビルシステム自体も 10 年から 20 年近くにわたって運用することが普通であり、システムの更新にあたっても、その時点の理想的なシステムを導入できるわけではなく、古い建築物が持つ制約等に影響を受ける場合も多い。このような状況のもと、長期にわたってアップデートのできないシステムを抱えているような状況が一般化している。

3.3.2. 複数のフェーズに分かれた長いライフサイクルを持つこと

ビルの企画から建設、運用、そして最終的な撤去まで、幾つかのフェーズに分かれた非常に長いライフサイクルを有している。システム的な観点でみると、設計・調達、建設・設置、竣工、運用、改修・廃棄というような各フェーズとなるが、それぞれの段階で、セキュリティを確保するための対応が異なってくることになる。例えば、設計段階では、長期の運用を意思した上でのセキュリティ対策をどのように設計仕様に盛り込むか

が課題であり、建設段階では多種・多数の業者が建設現場に入り乱れるような状況の中で如何にバックドア等を仕掛けられないようにするか人の管理の問題があり、また運用段階ではマルウェア等の侵入防止のための物理的対策およびシステム的対策の他、サイバー攻撃を受けた場合の対応についても考える必要がある。

図 3-12　ビルのライフサイクルを意識した対策が必要

3.3.3. マルチステークホルダであること

ビルやそのシステムに係わるステークホルダも多種である。ビルの持ち主としてオーナーがおり、建設に当たってはゼネコン、個別の設備に対応したサブコン、更に設計事業者、個別の設備を納入するベンダがいる。設備の種類は、一般的に、受変電、照明、熱源、空調、給排水、昇降機、防犯、防災等があり、設備ごとに異なるベンダが関わることになる。運用段階に入ると、通常は運用事業者が委託を受けてビルの管理にあたり、システムの保守では納入ベンダも関係してくる。サイバーセキュリティを確保する上では、セキュリティベンダ、ネットワークシステムベンダの支援が必要となるケースも出てくる。ビルのライフサイクルに合わせて、それぞれが自身の責任範囲についてしっかりとケアする必要がある。

3.3.4. 多種多様なビルの存在

ビルの用途や種類も様々である。新築のビルに対しては最新の対策を比較的導入しやすいが、既存のビルに対してセキュリティの向上を図るということでは、現在導入済みのシステムの制約から、採用可能な対策も限られた物となる。仮に制約を超えて

最新対策を導入しようとすると、システムの入替えなど、非常に大きなコスト負担が必要となったりするため、ビルの用途を踏まえた費用対効果を厳しく見ていく必要がある。このような場合でも運用の改善によってセキュリティ向上が可能な場合もあり、対策の選択肢を広く用意していくことが重要となる。また、ビルの規模によって求めるセキュリティ対策のレベルが違い、既存の運用状況も異なっていたりする。あるいはビルの用途、自社のオフィスビルなのか、多数のテナントを入居させるビルなのか、不特定多数の人が出入りするビルなのか等によっても、ビルオーナーが持つべき責任も異なってくるため、必要な対策レベルも異なった物となる。

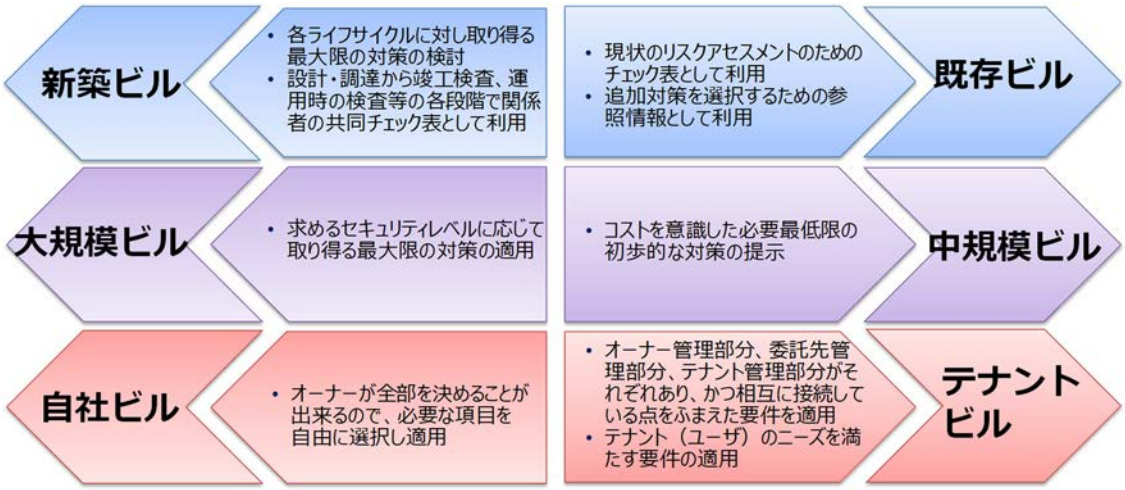


図 3-13　ビルの多様性を意識した対策が必要

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

ビルシステムの標準的な構成、ビルシステムの特徴を踏まえた上で、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を以下に示す。基本的にこのガイドラインでは、下記の方針に基づいてビルシステムに対するサイバーセキュリティ上のリスクを整理し、更にその対策をブレークダウンしている。

これはビルシステムのサイバーセキュリティ対策を考える上で、各ステークホルダがそれぞれの立場に応じて必要な対策（必要なライフサイクルにおける、必要なレベルの対策）を見つけ、検討するためのインデックスの役割も果たしており、またそのインデックスに対応した具体的な対策を参照することで、実際の対策立案の参考になることも目指している。

更に設備ごと、設備を構成する機器ごと、機器が置かれた場所ごとのリスクを確認し、現状としてどのレベルのセキュリティ対策が取られているかを確認し、セキュリティ向上のためにはどのような対策が必要かを探るための、リスクアセスメントのツールとしても利用できることを意図したものでもある。

3.4.1. 場所から紐解くリスクの整理とライフサイクルを考慮した対策

ビルシステムにおけるサイバーセキュリティ上のリスクをどのような視点から見ていくかは、いろいろな考え方がある。サブコンやベンダの立場からは、自身の担当、管理する設備のみに着目して見ることができれば効率的である。但しこの場合には、設備の数だけ対策を書き出す必要が出てくる。

一方で、どの設備についても、中央監視センターには監視端末（HMI/HIM）やサーバ類（BA 主装置）、パイプスペースには配線やスイッチ類、機械室や制御盤にはコントローラ類が置かれるというように、場所ごとに似たような機器が置かれることになるため、場所や機器ごとの共通課題として対策を整理することも可能である。また、 ビルを総体で見た場合、場所の対策、そこに置かれた機器の対策というように、場所から紐解く形で見ていく方が効率的であると考えることもできる。

そこで、本ガイドラインでは、ビル内の場所、その場所に置かれる機器や装置という単位で、どのようなサイバーリスクが存在するかを整理し、そのリスクへの対策を整理するという形をとる。また、対策に関しては、設計時に仕様として盛り込まれた対策が建設や運用にも引き継がれていくものもあり、建設時や竣工時にのみ気にすべき対策もあり、あるいはコスト等の関係から設計時にシステムの仕様としては盛り込まないようなことも運用によって対策をとる場合もあるというように、複数のライフサイクルにまたがる対策も考えられるため、ライフサイクルの各フェーズを並べて対策を示すこととする。

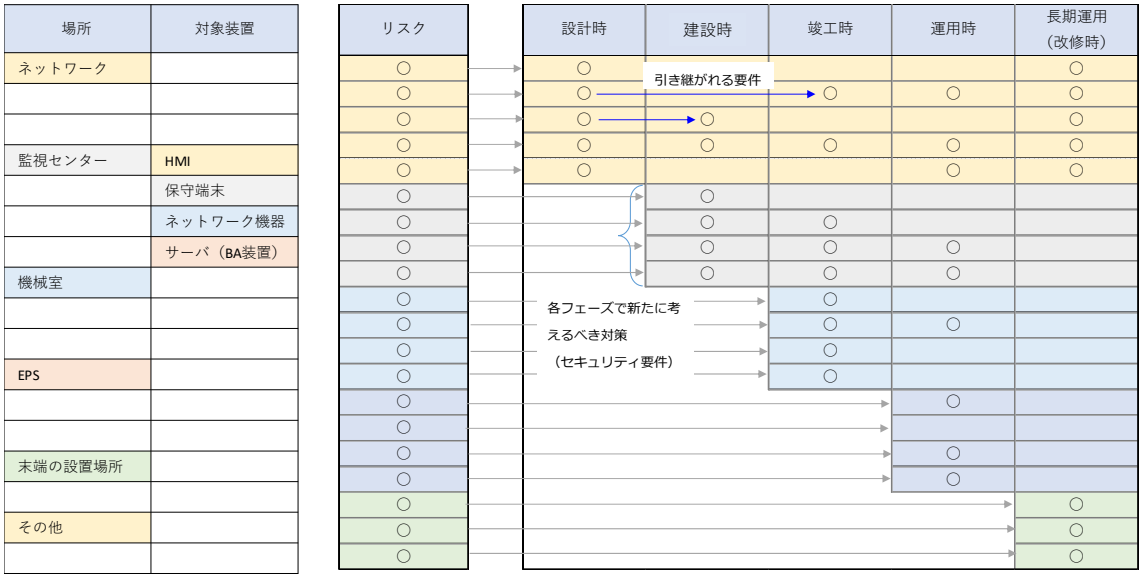


図 3-14　場所からみたサイバーセキュリティリスクとライフサイクルをまたがって適用するべき対策の概念図

次章以降では、上記の方針にもとづき、場所から紐解くサイバーセキュリティリスクとポリシーレベルの対策までを「4.ビルシステムにおけるリスクと対策ポリシー」に整理する。また、実装策レベルの対策までを一覧として整理し、リスクアセスメントやサイバーセキュリティ対策の検討のためのインデックスとしてまとめたものを「5.ライフサイクルを考慮したセキュリティ対応策」に別紙として掲載する。

3.4.2. インシデント発生時の対応

前述の方針に基づく整理及び「4.ビルシステムにおけるリスクと対策ポリシー」や「5.ライフサイクルを考慮したセキュリティ対応策」の記述は、事前にサイバーセキュリティ上のリスクを認識し、その対策を実施することで、サイバーインシデントの被害に遭う可能性を低減するための事前対策を中心としたものである。

一方で、対策を実施していたとしても、そのレベルが十分でなかったり、管理者が把握できていない脆弱なポイントが存在していたり、新たな攻撃手法が出てきたりというような様々な理由により、実際にはサイバー攻撃の被害にあう可能性は存在している。

インシデント発生時に素早くその対応を行うことで、被害やその影響を軽減し、いち早く通常の運用状態へと復旧させること、同様の被害に再び遭わないように対策を強化することが重要となってくる。このため、インシデント発生時の対応についても整理を行った。

ビルシステムのインシデントについては、設備やシステムの障害や故障として認識されることが多いと考えられ、それがサイバー攻撃によって引き起こされたのか、機器故障によって発生したのかを、障害発生時に判断することは非常に困難である。したがって、初期の対応方法は、通常の障害対応と同様になり、原因究明等をしていく中でサイバー攻撃によるインシデントであったことが判明することが多いと考えられる。本ガイドラインでは通常障害時の一般的な対応を整理し、サイバーインシデントであることが分かった段階でその対応に遷移するようなフローを考え、各段階で必要な対応を行うことを標準的な形として整理を行った。

なお、インシデント発生時の対応としては、NIST CSF で述べられているように、特定から復旧までの 5 つの機能に分けて語られることが多いが、ここではビルや建物に対するより実践的な概念として、日本データセンター協会（以下、JDCC）発行の「建物設備システムインシデント対応ガイド」の考え方を参考に、「準備段階」から「フォローアップ段階」まで、大きく5段階のフェーズに分けて整理を行った。

（出所：JDCC「建物設備システムインシデント対応ガイド」）

図 3-15　インシデントレスポンスの流れ

また、現状のビル管理のフローにおける設備やシステムの障害対応のフローと、その対応途中でサイバーインシデントであると認識したのちに取るべき対応のフローを整理している。

これらの考え方に基づくインシデント発生時の対応策の概要を「6. インシデント発生時の対応策」に整理する。そしてその対応策に基づいて具体的に検討、実施するべき内容を付属書としてまとめた。

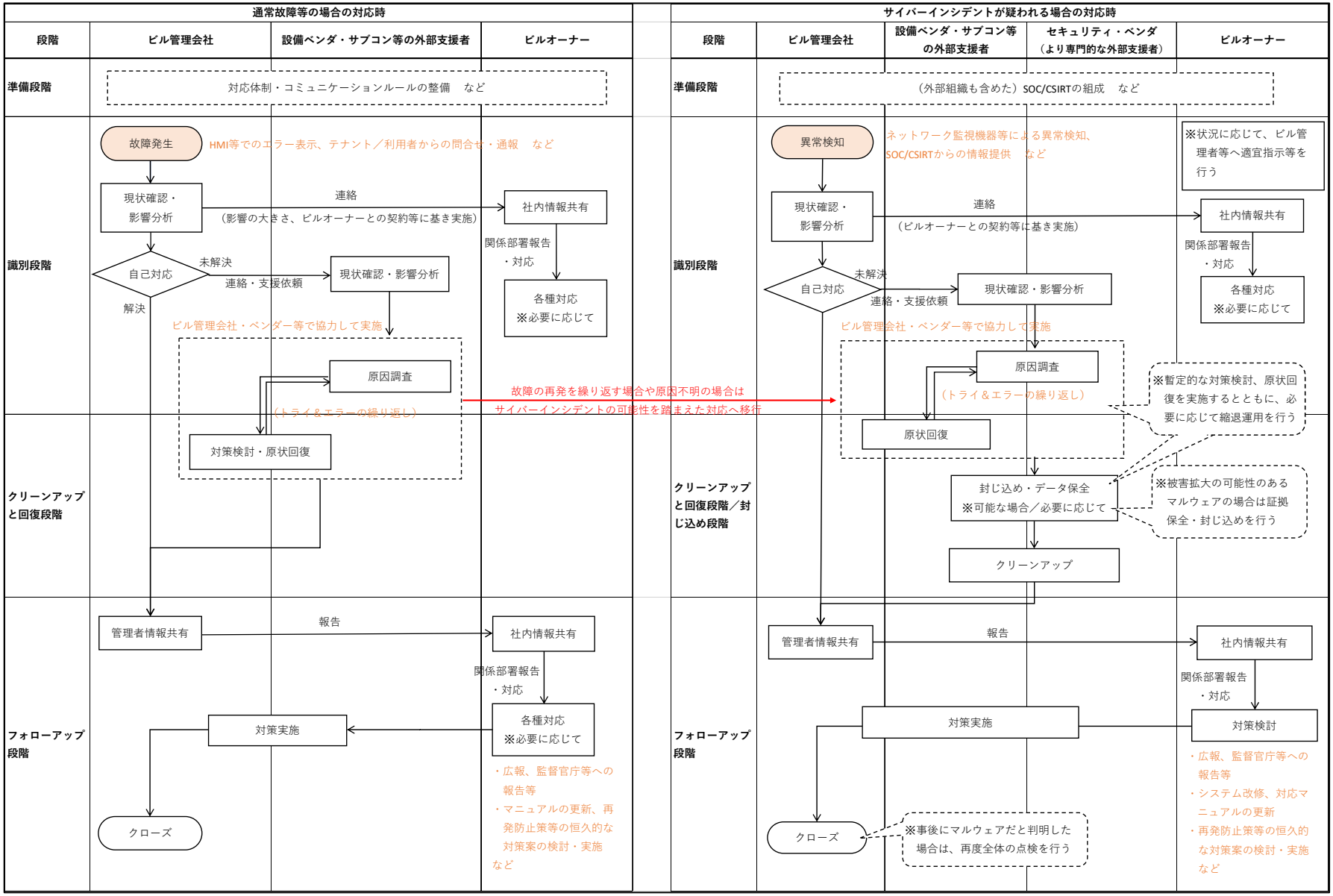


図 3-16　インシデントレスポンスのフロー（例）

3.5. ガイドラインの想定する使用例

本ガイドラインでは、ビルシステムのサイバーセキュリティ対策について、なるべく網羅的に、また、ライフサイクル別の対策については、必要に応じて複数の選択肢を示すようにしている。

ビルシステムに関するステークホルダがそれぞれの立場で、ビルの形態やライフサイクルの状況、掛けられるコスト等の状況など、ビルを取り巻く環境要因に応じて適当な対策を選んでいくことを期待しているが、選択のための参考となるよう、幾つかのケースについて、以下に例示をする。

3.5.1. 例1： 新築の大規模オーナービルにおける使い方

新築の大規模オーナービルの場合、オーナーの意向に沿って最も自由にビルのサイバーセキュリティ対策を選択していけるものとなる。これから建設するビルであれば、全ての選択肢が選択可能であり、大規模ビルの建設コストを考えれば、サイバーセキュリティに当てるコストは相対的には非常に小さいものと予想される。あとは、ビルの目的や用途の重要度を考え、最も適当な選択肢を選んでいけば良い。

なお、最低限実施すべきと考えられる対策については、基本的に全てを盛り込むことが望ましいと思われる。

(1) ビルオーナー

- ビルの目的や用途の重要度を考え、セキュリティとして確保すべきレベルを設定する。なお、最低限実施すべきと考えられる対策以上のレベルを設定することが望ましい。
- 設定したレベルに対応した対策ポリシーを参考に、設計事務所にビルの設計を依頼する。
- 設定したレベルの対策ポリシーに応じた竣工検査対策を参考に、竣工検査時にはサイバーセキュリティ対策の観点からの検査を実施する。

(2) 設計事務所、ゼネコン

- ビルオーナーより提示されたポリシーレベルの対策要求をもとに、インデックスから対応策、実装策の選択肢を抜き出し、また、これらの実装策を提供可能なベンダ等との調整を踏まえ、設計案をビルオーナーに提供する。
- 最終的に決定された設計案に基づき、個々の設備システムに関する発注仕様書を作成する。発注仕様書の作成にあたっては、ガイドラインの実装策の記述や経験リポジトリに収容された知見を参考とする。

(3) ゼネコン、サブコン

- 建設時の工程管理において、設計として採用された対応策から紐解かれる建設時の対策を参考に、サイバーセキュリティ上のチェックや対策等を実施する。

3.5.2. 例2： 既存の中規模テナントビルをクラウド移行する際の使い方

現在、既存の中規模テナントビルは、管理の効率化のため、システムの更改時等にあわせて、監視・制御等をクラウド管理へ移行するケースが増えている。これによって、システムが外部につながるようになったり、ビルには監視要員を置かなくなったりということが起こるので、外部接続に当たって確保すべきセキュリティ要件や無人運用の場合のセキュリティ要件などを参考にして、必要なセキュリティ対策の検討を行うことが望ましい。

(1) ビルオーナー

- 外部接続や無人運用に際して必要なサイバーセキュリティ対策のポリシーを参考に、サブコンやベンダに提案を依頼する。
- 設定したレベルの対策ポリシーに応じた竣工検査対策を参考に、竣工検査時にはサイバーセキュリティ対策の観点からの検査を実施する。

(2) サブコン、ベンダ

- ビルオーナーより提示されたポリシーレベルの対策要求をもとに、インデックスから対応策、実装策の選択肢を抜き出し、提供可能な製品やサービス、その際に合わせて実施すべき運用対策等をビルオーナーに提示する。

3.5.3. 例3： 既存ビルへのリスクアセスメントと対策立案での使い方

まず、現状のセキュリティ対策のレベルを確認する。そのため、ポリシーレベルの項目、そして対応策レベルの設計対策項目と突き合わせを行い、現状のビル設計時点ではどの程度の対策を盛り込んでいたのかを確認する。

確認された項目の対策レベルに合わせて、インデックスから対応する竣工対策、運用対策の項目を参照し、必要な対策レベルが竣工時、運用時にあって確保できていたのかを確認する。

十分な対策ができていたことが確認できれば、一応、セキュリティとして求めるレベルに対して必要なレベルが確保されていたということになり、そのレベルが確保されていなければ、運用対策として書かれているレベルの対策を今後取れるかどうかを検討する。新たな運用対策を取れれば、要求するレベルにおいてはセキュリティを確保できることになる。

3.5.4. 例4： 機器等の障害対応の延長線上でインシデント対応する使い方

ビルシステムがサイバー攻撃にあった場合、通常は設備等の障害として現れることとなる。この設備障害が機器等の故障によるものなのか、サイバー攻撃によるものなのかを初期の段階で判断することは非常に困難である。したがって、初期の対応方法は、通常の故障対応と同様になり、原因究明等をしていく中でサイバー攻撃によるインシデントであったことが後から判明することが多いと考えられる。

このため、通常のビル管理のフローの中で障害対応として実施し、原因がサイバー攻撃によるもの疑われる事態になった場合には、通常の障害対応に加えてセキュリティベンダ等を加えたサイバーセキュリティの観点も含めた識別やクリーンアップを実施する。対応の詳細については付属書を参照いただきたい。

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

3章において場所別に設置される機器という観点での整理を実施したが、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事前に検討するべきことを、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）のセットでまとめたものが下表である。

表 4-1 全体管理に関するビルシステムのリスクと対策ポリシー

	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
1. 構成情報／管理情報			
(1)	ビルシステムへの被害発生時に、被害確認が遅れ、復旧作業の支障となる。	ビルの構成情報が最新状態に管理できておらず、機器の最新の接続関係が把握できない。	・構築システム構成図（設計時）に対し、引渡し時のシステム構成図を竣工引渡し書類として作成するように”設計仕様”に加える。 ・システム全体構成（外部接続先を含む）の最新状態を常に把握できるようにする。
2. バックアップデータ／事業継続			
(1)	適切なバックアップデータがなく、ビルシステムへの被害発生時に復旧作業の支障となる。	バックアップが取られていない、又はバックアップの範囲や対象が適切でない。	・システムバックアップ方法を運用側と確認の上でバックアップ方法を設計時に仕様を組み込む。 ・管理ポイントや運転スケジュール等、システムを運用するにあたって必要なデータについては、バックアップを取得する機能を具備する。
(2)	システムの脆弱性をついた攻撃を受ける。	脆弱性についての認識が不十分で、脆弱性が残ったままの状態になっている。	・既知の脆弱性に対して必要な対策（パッチ等）が適用されているものを導入し管理する。 ・但し、他機器及び他システムの正常稼動については、担保しなければならない。

	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
3. 会社／要員の管理			
(1)	ビルシステムへの被害発生時に、迅速な対応ができず、被害が拡大する。	ビル管理会社においてセキュリティへの意識醸成、要員教育が十分ではなく、事前対策や対応準備ができていない。	・システム構築要件に教育訓練について明記する。
(2)	ビルシステムが内部作業員等から攻撃を受ける。	作業員等の身元確認や行動監視が不十分で、内部攻撃者が紛れることや攻撃を行うことを防ぐことができていない。	・システムの構築・施工・保守にあたって、作業員等の身元確認や行動確認についての要件を明記する。
4. 体制構築等			
(1)	攻撃等への対応が効果的にできず、被害が拡大する。	十分なリスクアセスメントができていないため、リスク対応の運用計画や体制が十分なレベルで構築できていない。	・リスクアセスメントを実施し、その結果を基に監理監査面からの「運用する管理体系」などを運用計画として定義・整備する。
(2)	ビルシステムのセキュリティ対策が不十分で、攻撃を防ぐことができない。	ビルシステムの設計・構築にあたって、十分なセキュリティ対策を盛り込むことができていない。	・ビルシステムに対して十分なセキュリティ知識を持った技術者の元で設計を実施する体制を整える。
(3)	攻撃への初動対応が遅れ、被害が拡大する。	作業員の教育、訓練が十分ではなく、十分な対応が取れない。	・入場前に適切にセキュリティ対策を実施する。
(4)	攻撃への対応が体系的に実施できず、被害が拡大する。	運用時のセキュリティ管理体制が十分なレベルで構築できていない。	・設計要件・運用要件を明記する。
(5)	攻撃に対する対応手順が分からず、被害が拡大する。	運用基準の中で、緊急時の対応手順が十分に整備されていない。	・緊急時の対応手順要件について明記する。
(6)	不正なアクセス、通信、操作があっても、気がつくのが遅れたり、見逃したりしてしまい、被害が拡大する。	システムの運用監視が十分ではなく、運用状況の監視体制が十分ではない。	・発注主側の運転管理者に対する教育について、明記する。 （教育人数・教育テキスト・教育期間・セキュリティ関連教育を含む・教育場所を明記）

4.2. 機器ごとの管理策

次に場所ごと、機器ごとの事前検討項目を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）のセットでまとめたものが下表である。

表 4-2　場所ごとのビルシステムのリスクと対策ポリシー

	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
1. ネットワーク(クラウド、情報系 NW、BACnet 等)			
10	ネットワーク		
(1)	ビルシステムの一部に起きたマルウェア感染が、ビル内のネットワーク経由で容易に拡大していく。	ビル内のネットワークに様々なビル設備機器が混在して接続され、マルウェアの感染拡大防止を意識した管理がされていない。	・ビル内のネットワークをセキュリティポリシーに基づいて物理的又は論理的に分離する。
(2)	ビルシステムの一部に起きたマルウェア感染が、ビル内のネットワーク経由で容易に拡大していく。	ビル内のネットワークでやり取りされる通信が適切に管理されておらず、リモートからの不正侵入の防止を意識した管理がされていない。	・ビル内のネットワークにおいては、セグメント間通信を必要最小限に制限する。
(3)	管理外の外部ネットワーク接続経由でマルウェア感染や不正侵入を受ける。	保守等の理由で外部接続が知らぬ間に取り付けられたり、外部との通信ポートが開けられたりするのを十分に管理・制限できていない。	・不正接続の有無を定期的に点検する。 ・外部との接続や通信はファイアウォール等により必要最小限に制限する。
(4)	管理外の外部ネットワーク接続経由で不正接続や攻撃を受ける。	ビルへの引き込み回線の管理が不十分で、勝手に不正な外部回線を引き込まれる。	・ビル内に設置する外部接続回線を管理し、不明回線の有無等を定期的に点検する。
11	クラウドサーバ・Web サーバ		
(1)	外部ネットワーク接続経由で侵入を受ける。	外部接続機器のセキュリティ対策が十分ではない。	・外部からのアクセスに制限を設ける。
(2)	テナント向けの Web 公開システム経由で不正操作をされる。	Web 公開システムの脆弱性対策が十分ではない。	・ビルシステムの制御を行うシステムをインターネットに公開する場合は、アクセス制御を行ったうえで、脆弱性対策の実施体制を構築する。
(3)	クラウドサーバを利用することで意図しない不正アクセスが発生する。	発注側がリスクを把握していない。	・リスクアセスメントを実施したうえで、発注の判断を行う。
12	情報系端末(オフィス系端末)		
(1)	外部ネットワークに接続された情報系端末経由で、ビルシステム内への攻撃を受ける。	外部ネットワークに接続された情報系端末のセキュリティ対策が十分ではない。	・外部からのアクセスに制限を設ける。

	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
13	外部接続用ネットワーク機器(ファイアウォール、ルータ)		
(1)	外部ネットワーク接続経由で攻撃を受ける。	外部接続用ネットワーク機器のセキュリティ対策が十分ではない。	・外部からのアクセスに制限を設ける。
14	ビルシステム間相互接続		
(1)	ビルシステムの一部に起きたマルウェア感染が、ビルシステム間の相互接続経由で容易に拡大していく。	ビルシステム間の相互接続環境において、感染拡大防止等のセキュリティ対策が十分ではない。	・正当な端末以外にはアクセスしない、不正な端末からのアクセスを許可しない、といった対策を施す。 ・正しい通信のみ許可するといった通信制限を施す。
2. 防災センター(中央監視室)			
20	防災センター(中央監視室)		
(1)	所定の作業員以外による画面の盗み見、不正操作が行われる。	防災センター(中央監視室)に対して、許可された入退室に限定するような管理ができておらず、許可者以外の入室を許してしまう。	・防災センター(中央監視室)の入場者を登録(事前、都度)して管理する仕組みを入れる。
			・防災センター(中央監視室)への入退室をもれなくチェックし管理する仕組みを入れる。
(2)	所定の作業員が、その権限を越えて、システムや端末／制御盤に不正操作をする。	システムの権限管理や作業監視が十分でなく、権限外の不正操作をされることを防ぐことができない。	・作業員の作業状況を常時監視する仕組みを入れる。
			・許可された作業員以外が作業できない仕組みを入れる。
21	HMI/HIM		
(1)	正規の作業員以外により不正ログイン、不正操作がされる。	端末のログイン管理やログイン情報の管理が不十分である。	・操作者を限定する機能を入れる。 ・パスワード管理を徹底させる。
(2)	所定の作業員が、その権限を越えて、システムや端末に不正操作をする。	端末やシステムの権限管理や作業監視が十分でない。	・作業員の作業状況を常時監視する仕組みを入れる。
			・許可された作業員以外が作業できない仕組みを入れる。
(3)	侵入者にシステム情報を探られ攻撃が拡大する。	ログ情報へのアクセスが容易で、侵入者にログ情報を探られ、次の攻撃のヒントを与えてしまう。	・アクセスログ、操作履歴を適切に管理する。
(4)	不正侵入に対する状況解析が困難で対策が遅れる。	適切にログが取得されておらず、侵入や感染の状況の解析が十分にできない。	・各種ログ情報の導入とログ解析の仕組みを導入する。

	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
(5)	不正なアクセス、通信、操作があっても、気がつくのが遅れたり、見逃したりしてしまい、被害が拡大する。	システムの運用監視が十分でない。	・不正なアクセスや操作を定期的に確認する仕組みを入れる。
(6)	マルウェアへの感染判明後、その感染経路が特定できず、対策が十分に取れない。	システム構築の過程や運用の節目でマルウェアの感染のチェックや管理が不十分であるため、いつの間にか感染しており、感染原因や感染経路がすぐに分からない。	・工場出荷前及び引渡し前に事前検疫を実施する。
(7)	侵入者にシステム内部を探られ、不正な操作をされる。	システムの内部構成が単純又は権限管理ができておらず、容易に全体を探られ、次の攻撃のヒントを与えてしまう。	・権限者以外、容易にシステム内部の構造が見られないようにする。
(8)	システムの脆弱性をついた攻撃を受ける。	脆弱性についての認識が不十分で、脆弱性が残ったままの状態となっている。	・既知の脆弱性に対して必要な対策（パッチ等）が適用されているものを導入し管理する。 ・但し、他機器及び他システムの正常稼動については、担保しなければならない。
(9)	外部媒体接続時に、外部媒体経由でマルウェアに侵入されてしまう。	セキュリティ確認がされていないUSB等の外部媒体が容易に接続可能となっている。	・外部媒体等を安易に利用できないようにする。
			・外部媒体等を事前検疫してから利用する。
22	保守用持ち込み端末		
(1)	外部持込端末接続時に、外部持込端末経由でマルウェアに侵入されてしまう。	セキュリティ確認がされていない外部持込端末が容易に接続可能となっている。	・保守用端末は適切に管理されたものを使う。
23	統合NWにつながるネットワーク機器（ファイアウォール、ルータ、スイッチ）		
(1)	不正端末を接続され、マルウェアを送り込まれる。	空きポートが接続可能な状態で放置されている。	・スイッチ等の空きポートが利用されないような仕組みを導入する。
24	システム管理用サーバ（ビルシステム主装置）		
(1)	所定の作業員以外による不正操作が行われる。	サーバが専用の管理区画に設置されておらず、誰でも触ることができる状態にある。	・適切に管理された専用の室、区画の中に機器を設置する。
			・区画内のラックやケースは施錠管理を行う。

	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
(2)	所定の作業員以外による不正操作が行われる。	サーバ設置区画への入退室が適切に管理されておらず、誰でも触ることができる状態にある。	・サーバ室、区画への入退室を適切に管理する。 ・関係者以外立ち入らせない。
(3)	侵入者にシステム情報を探られ攻撃が拡大する。	ログ情報へのアクセスが容易で、侵入者にログ情報を探られ、次の攻撃のヒントを与えてしまう。	・アクセスログを記録する機能を入れる。
(4)	不正侵入に対する状況解析が困難で対策が遅れる。	適切にログが取得されておらず、侵入や感染の状況の解析が十分にできない。	・各種ログ情報の導入とログ解析の仕組みを導入する。
(5)	不正なアクセス、通信、操作があっても、気がつくのが遅れたり、見逃したりしてしまい、被害が拡大する。	システムの運用監視が十分ではなかったり、運用状況の監視体制が十分でない。	・不正なアクセスや操作を確認する仕組みを入れる。
(6)	不正な命令を実行してしまい、不正な動作をさせられる。	通信相手を認証する仕組みがなく、なりすまし通信を区別することができない。	・認証されていない相手との通信を遮断する機能を入れる。
(7)	マルウェアへの感染判明後、その感染経路が特定できず、対策が十分に取れない。	システム構築の過程や運用の節目でマルウェアの感染のチェックや管理が不十分であるため、いつの間にか感染しており、感染原因や感染経路がすぐに分からない。	・工場出荷前及び引渡し前に事前検疫を実施する。 ・運用段階においても、検疫を適宜実施する。
(8)	侵入者にシステム内部を探られ、不正な操作をされる。	システムの内部構成が単純又は権限管理ができておらず、容易に全体を探られ、次の攻撃のヒントを与えてしまう。	・権限者以外、容易にシステム内部の構造が見られないようにする。
(9)	システムの脆弱性をついた攻撃を受ける。	脆弱性についての認識が不十分で、脆弱性が残ったままの状態となっている。	・既知の脆弱性に対して必要な対策（パッチ等）が適用されているものを導入し管理する。 ・但し、他機器及び他システムの正常稼動については、担保しなければならない。
(10)	外部媒体や外部持込端末接続時に、これらを経由してマルウェアに侵入されてしまう。	セキュリティ確認がされていないUSB 等の外部媒体や外部持込端末が容易に接続可能となっている。	・外部媒体等を安易に利用できないようにする。 ・外部媒体等を事前検疫してから利用する。

	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
3.機械室／制御盤ボックス			
30	機械室		
(1)	所定の作業員以外による不正操作が行われる。	許可された入退室に限定するような管理ができておらず、許可者以外の入室を許してしまう。	・機械室は施錠可能とする。
31	コントローラ(DDC、PLC 等)		
(1)	侵入者にシステム情報を探られ攻撃が拡大する。	ログ情報へのアクセスが容易で、侵入者にログ情報を探られ、次の攻撃のヒントを与えてしまう。	・ログを適切に管理可能な機器・システムを導入する。
(2)	不正侵入に対する状況解析が困難で対策が遅れる。	適切にログが取得されておらず、侵入や感染の状況の解析が十分にできない。	・各種ログ情報の導入とログ解析の仕組みを導入する。
(3)	不正なアクセス、通信、操作があっても、気がつくのが遅れたり、見逃したりしてしまい、被害が拡大する。	システムの運用監視が十分ではなく、運用状況の監視体制が十分でない。	・不正なアクセスや操作を確認する仕組みを入れる。
(4)	不正な命令を実行してしまい、不正な動作をさせられる。	通信相手を認証する仕組みがなく、なりすまし通信を区別することができない。	・許可されていない相手との通信を遮断する機能を入れる。
(5)	マルウェアへの感染判明後、その感染経路が特定できず、対策が十分に取れない。	システム構築の過程や運用の節目でマルウェアの感染のチェックや管理が不十分であるため、いつの間にか感染しており、感染原因や感染経路がすぐに分からない。	・工場出荷前及び引渡し前に事前検疫を実施する。 ・運用段階においても、検疫を適宜実施する。
(6)	侵入者に容易にアクセスされ、不正操作をされる。	ID・パスワードが適切に設定されておらず、誰でもアクセス可能な状態にある。	・ID・パスワード管理を必要とする機器においては、適切な ID・パスワードを設定する。
(7)	システムの脆弱性をついた攻撃を受ける。	脆弱性についての認識が不十分で、脆弱性が残ったままの状態となっている。	・既知の脆弱性に対して必要な対策（パッチ等）が適用されているものを導入し管理する。 ・但し、他機器及び他システムの正常稼動については、担保しなければならない。

	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
(8)	外部媒体や外部持込端末接続時に、これらを経由してマルウェアに侵入されてしまう。	セキュリティ確認がされていないUSB 等の外部媒体や外部持込端末が容易に接続可能となっている。	・外部媒体等を安易に利用できないようにする。
			・外部媒体等を事前検疫してから利用する。
			・外部持込端末は適正に管理された端末のみ接続を許可する。
32	ネットワーク機器(ファイアウォール、ルータ、スイッチ)		
(1)	不正端末を接続され、マルウェアを送り込まれる。	空きポートが接続可能な状態で放置されている。	・スイッチ等の空きポートが利用されないような仕組みを導入する。
33	ゲートウェイ機器		
(1)	不正な命令を実行してしまい、不正な動作をさせられる。	通信先を制限する仕組みがなく、なりすまし通信を区別することができない。	・ネットワーク上に、通信先を制限する仕組みを導入する。
34	各種制御盤・分電盤		
(1)	所定の作業員以外による不正操作が行われる。	業界で広く通用する鍵がついているため、容易に開錠され、機器に触れることができる状態にある。	・各種制御盤の鍵は、業界で広く使われる種類の鍵以外を使用する。 ・保守時の対応等も考慮して鍵を導入する。
4.配線経路(MDF 室、EPS、天井裏ラック)			
40	MDF 室／EPS／天井裏ラック		
(1)	不正端末を接続され、マルウェアを送り込まれる。	ネットワーク配線への人的アクセスが管理されていない。	・ビルシステム主装置以降の配線について、外的要因(人的破壊・意図した工作)に対して十分な保護対策を施す。
41	内部に置かれたネットワーク機器(スイッチ類)		
(1)	所定の作業員以外による不正操作が行われる。	機器の設置場所が安全管理されておらず、誰でも触ることができる状態にある。	・適切に管理された専用の室、区画の中に機器を設置する。
			・機器類は許可された作業員以外が容易に触れないようにする。
(2)	不正端末を接続され、マルウェアを送り込まれる。	空きポートが接続可能な状態で放置されている。	・機器類の空きポートには不正利用ができないよう、対策を実施する。

	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
5. 末端装置が置かれる場所			
50	末端装置		
(1)	不正端末を接続され、マルウェアを送り込まれる。	空きポートが接続可能な状態で放置されている。	・第三者がアクセス可能な場所には、フィールド機器や IP ネットワークに直結する機器を設置しない。 ・機器には、第三者による不正な操作ができないよう、対策を実施する。
(2)	不正な命令を実行してしまい、不正な動作をさせられる。	通信相手を認証する仕組みがなく、なりすまし通信を区別することができない。	・特定要員以外の利用を遮断するための十分な保護対策を施す。

5. ライフサイクルを考慮したセキュリティ対応策

4 章では、場所によらない構成要素及び場所ごと、機器ごとについて、考え得る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）を整理した。セキュリティポリシーは、それぞれのセキュリティリスクに対して、ポリシーレベルで記載した対策要件であり、実際の対策としては、更に 1 段、2 段のブレークダウンが必要なものである。このセキュリティポリシーを入り口として、もう 1 段具体的な対策をライフサイクルの 5 つのフェーズに展開したものが、「ライフサイクルを考慮したセキュリティ対応策」であり、一覧表の形で別紙に整理している。

対応策は、4 章の表 4-1 及び表 4-2 におけるセキュリティポリシーをそのまま引き継ぐ形で展開する形式となっているので、セキュリティポリシーをベースに、ライフサイクルの各フェーズでどのような対策を考えるべきか参照できる構造となっている。

なお、一部には、1 つのセキュリティポリシーから、複数の対応策の系列に展開しているものもあり、これは取り得る対策の代表的な選択肢を示している。但し、1.2.4 項でも説明したように、これらの選択肢のいずれかを必ず選択する必要があるというものではなく、それぞれのビルの置かれた状況に応じて、リスクを認識したうえで対策は実施しない、設計レベルでの対策は取らないが運用でカバーする、対応策に記載された対策要件を緩めて採用する、あるいは重要性の高いところについては記載よりも更に踏み込んで採用する等、あくまで 1 つの拠り所、検討の材料としてとらえ、現場の状況等に応じて調整すると良いだろう。

具体的な対応策については別紙を参照のこと。

6. インシデント発生時の対応策

4 章及び 5 章では、ビルに導入される様々なシステムに対するサイバーセキュリティ対策のうち、主に事前に検討し、準備しておくべき対策について示した。

これに対し本章では、ビルシステムに対するサイバー攻撃（インシデント）の発生時に、その損害を最小限に抑え、復旧にかかる時間とコストを削減するための取組（インシデントレスポンス）の概要について、インシデント対応の 5 段階のフェーズに分けて説明をする。

インシデントレスポンスとして検討するべき事項や対策内容の詳細については、付属書の「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　インシデントレスポンス・ガイドライン」をご参照いただきたい。

6.1. インシデントレスポンスの概要

インシデントレスポンスとして検討、実施するべきことの概要を 5 段階のフェーズに分けてまとめたものが下表である。

なお、以下はインシデント対応として検討、実施することが望まれることを網羅的に示したものであり、実際には各ビルの状況等にあわせて、可能な部分から手を付け、取り組んでいくことが大事である。

表 6-1　インシデント発生時のフェーズごとの対応内容

	実施事項	検討・実施内容
1. 準備段階		ビル管理の体制や対応フローの準備を行い、最終的にインシデント発生時に適切な初動対応を行うことができるよう準備を整える。
(1)	対応体制（インシデントレスポンス・チーム）の整備	・ 対応フローの実行を想定した、インシデント発生時の対応チーム（社内関係部署、サブコン・設備ベンダ、セキュリティベンダ等も含む）について検討する。IT も含む関連システムのインシデント対応主体との連携体制等についても合意形成し、各関係者に役割を果たせる職能があることを担保することが重要である ・ システムの停止や再起動、ネットワークの切断等の決定責任者、実施責任者等についてもあらかじめ決めておくと良い ・ リーダー（対応責任者）や社内外の各関係者の必要な機能や権限等を表す文書を整備することが望ましい ・ より高度な対応を行うためには、外部のセキュリティベンダ等と協力しながら、事前にインシデントの検知や対策について検討する SOC（Security Operation Center）、インシデントレスポンスの司令塔となる CSIRT（Computer Security Incident Response Team）の組成を検討することも有効である

(2)	コミュニケーションルールの整備	・ 一般的な故障発生時の対応と同様に、誰といつどうやってコミュニケーションを行うか、関係各所の連絡先一覧・ツールを整理する ・ 社内の広報、法務、営業等とのコミュニケーションルートや情報の管理ルール等も決めてことが望ましい
(3)	システムのバックアップ及び封じ込め方針等の検討	・ 復旧、封じ込め等を想定し、設備の設定等のシステムのバックアップを定期的に取得する。誰がいつ何のバックアップを取得するのか、どこに保存されるのか等を一覧にしておくとよい。なお、すべてのシステム等のバックアップを取得・管理することはコスト等の観点からも現実的でないため、重要設備や運用への影響の大きい設備を優先する等、各ビルの状況に合わせて優先順位を付けて対応することも考えられる ・ 封じ込めにあたり、インシデントの発生個所（設備・端末、システム）毎のネットワークの切断の可否等、切断した場合のテナント等への影響、これらを踏まえた対応方針等について検討する
(4)	ビル全体のシステムネットワーク一覧等の作成	・ ビルに導入されているすべてのシステムや機器（サーバ、端末、OS、アプリケーション等）を把握することのできる一覧表や、ネットワーク図、当該ビル内外の各種システムとの接続・連携構成、それぞれの担当者（担当ベンダー等）を網羅した文書を作成する ・ 設備等に変更・更新を加えた結果も反映し、現状を正しく把握できるようにする
(5)	教育・研修（訓練／演習等）	・ 事前に検討した対応フローを正しく機能させるために、訓練や演習を実施することが不可欠である
2. 識別段階		通常の故障対応では原状回復しない場合や、一旦は回復するも同様の故障が繰り返し発生する等により原因が特定できない場合は、サイバー攻撃の可能性が疑われるため、以下の手順に進む。
(1)	現状確認・影響分析	・ ビルオーナー及びビル管理者は、サブコン、設備ベンダ、セキュリティベンダ等の専門家と協力しながら、原因調査を行い、今後の対応方針を決定するとともに、原状回復を行う ・ 現状確認： いつ、どこで発生したか、現象の内容等を確認する ・ 影響分析： インシデントにより侵害された他の領域はあるか、テナント等への影響は何か等を確認する
(2)	原因調査（ベンダ等による事象確認・影響調査等）	・ 例えば以下のような段階を経て原因調査を行うことが考えられる ✓ 設備ベンダ等で対応（機器交換、再インストール等）し、事象確認・原因調査を行う ✓ 設備ベンダ等では対応できない、あるいは現象が再発する場合、複数の設備に原因・影響がある場合は、セキュリティベンダ等に支援を依頼して原因調査を行う

		・ サイバー攻撃であると確認できた場合には、速やかに社内関係部署や業界団体と情報共有し、注意喚起することが望ましい
3. 封じ込め段階		ビル管理者は、損害を最小限にとどめて、更に被害を拡大させないように、影響を受けたシステムを切り離し、その他のシステムへの被害の拡大を防ぐ。 なお、他システム等への被害拡大が想定されないインシデントの場合や、侵害されたシステムの切り離しが運用上不可能な場合は、「封じ込め段階」の対応は行わない。
(1)	システムバックアップ	・ 影響範囲や被害状況を正確に特定し、さらにはインシデントの原因を詳しく調査(データ保全・解析等)するために以下に示すような必要なデータの収集を行う ✓ 影響を受けたシステムのログデータ等 ✓ 影響を受けたシステムで発生した事象およびその他の重要なアクションを含む記録の文書化等 ・ すべての設備等のバックアップを取得するのはコスト等の観点からも非効率であるため、設備毎にバックアップの目的(どのような分析や回復に利用できるか等)、取得頻度を検討し、必要に応じて設備ベンダ等と保守契約を結ぶ
(2)	封じ込め	・ ビル管理者は、各設備を担当する設備ベンダやサブコンに確認の上、「準備段階」において予め検討した方針に基づき、ネットワークの流れを物理的に遮断(内外部のネットワークからの隔離)する。なお、電源を落とすと消えてしまう侵入痕跡もあるため、調査用データを取得完了するまでは機器の電源を切らない ・ 最終ステップとして、攻撃を受けたシステムに対策を行い、通常運用を行えるようにする
4. クリーンアップと回復段階		影響を受けたシステムをクリーンアップ(マルウェアの駆除等)し、復元する。テナント等への実被害が認められないと判断した場合は、後日の定期点検時等においてクリーンアップすることでも構わない。
(1)	クリーンアップ	・ 「識別段階」において判明した原因に対処し、影響を受けたシステムへの侵害を根絶する ・ 可能であれば、パッチやその他の対策でセキュリティの強化を行う ・ 復旧には、クリーンなバックアップがあると、復旧に要する費用が安く済むとともに時間の節約にもなる
(2)	追加調査	・ 原因不明の場合は、クリーンアップと同時に、必要に応じて更なる原因究明を行い、再発防止のための情報を収集する

5. フォローアップ段階		システムの復旧後に、同じインシデントが発生しないよう対策を行う。また、インシデントに係る対外発表や外部組織への報告等もこの段階に含まれる。
(1)	ビル管理者等における対策検討・実施内容の情報共有	・ システム全体を本来の運用状態に回復させるために実施した事項について、ビル管理者およびサブコン、設備ベンダ等で情報共有を行う ・ 情報共有に先立ち、例えば以下について検討・実施する ✓ 元のシステムや運用にどのような対策を行うかについて検討し、実施する ✓ システム復元後も、再発が無いか等について定期点検等で確認・報告してもらう
(2)	ビルオーナーにおける社内情報共有	・ ビルオーナーは、発生したインシデントに係る各種情報を社内で共有する ・ インシデントとその影響（テナントへの影響等も含む）や対策についてのすべての事象に関する文書（インシデントレスポンス・レポート）を作成する ・ 対外発表や外部組織への報告を想定し、必要に応じて想定問答集を作成する ・ 被害状況によっては、インシデントに対応した社内関係メンバー（法務、広報、営業など）を集め、検証会議を開催する

付録 A　用語集

CSIRT (Computer Security Incident Response Team)
インシデントが発生した際に対応するチームのこと。脆弱性情報などの収集と分析、インシデント発生時の対応、社内外の組織との情報共有や連携などを行う。インシデント発生時に結成されるチームの場合もある。

SOC (Security Operation Center)
サイバー攻撃の検知や分析を行い、その対策を講じることなどを専門とする組織。24 時間体制での対応が求められるため、外部委託するケースもある。

IDS(Intrusion Detection System)
サーバやネットワークの外部との通信を監視し、攻撃や侵入の試み等不正なアクセスを検知して管理者にメール等で通報するシステム。

IoT (Internet of Things)
「様々な物がインターネットにつながること」または「インターネットにつながる様々な物」を指しており、警備ロボット等がビルシステムにつながることが考えられる。

IPS(Intrusion Prevention System)
サーバやネットワークの外部との通信を監視し、侵入の試み等不正なアクセスを検知して攻撃を未然に防ぐシステム。

Society5.0
サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会（Society）のこと。狩猟社会（Society 1.0）、農耕社会（Society 2.0）、工業社会（Society 3.0）、情報社会（Society 4.0）に続く、新たな社会を指すもので、第 5 期科学技術基本計画において我が国が目指すべき未来社会の姿として提唱された。

アクチュエータ
機構又はシステムを動かし又は制御するためのデバイス。一般に電流、油圧、空気圧等のエネルギー源で作動し、そのエネルギーを運動に変える。アクチュエータは、制御システムが環境に働きかける機構である。制御システムは単純で（固定機構や電子システム）、ソフトウエアベース（プリンタドライバ、ロボット制御システム等）や人その他による。 [NIST SP 800-82 rev.2]

インシデント（サイバーインシデント／セキュリティインシデント）
望まない単独若しくは一連のセキュリティ事象、又は予期しない単独若しくは一連のセキュリティ事象であって、事業運営を危うくする確率及びセキュリティを脅かす確率が高いもの。

インシデントレスポンス（インシデント対応）
インシデント発生時に、インシデントによる損害を最小限に抑え、復旧にかかる時間とコストを削減すること等を目的とした対応を行うこと。

可用性（Availability）
認可されたエンティティが要求したときに，アクセス及び使用が可能である特性。[JIS Q 27000：2014]

完全性（Integrity）
正確さ及び完全さの特性。[JIS Q 27000：2014]

脅威
システム又は組織に損害を与える可能性がある、望ましくないインシデントの潜在的な原因。 [JIS Q 27000：2014]

機密性（Confidentiality）
認可されていない個人，エンティティ又はプロセスに対して，情報を使用させず，また，開示しない特性。[JIS Q 27000：2014]

サイバー空間
コンピュータシステムやネットワークの中に広がる仮想空間。デジタル化されたデータを活用して価値を生み出す。

サイバー攻撃(Cyber Attack)
資産の破壊、暴露、改ざん、無効化、盗用、又は認可されていないアクセス若しくは使用の試み。[JIS Q 27000：2014]

サイバーセキュリティ
電子データの漏えい・改ざん等や、期待されていたIT システムや制御システム等の機能が果たされないといった不具合が生じないようにすること。

重要インフラ

他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び社会経済活動の基盤であり、「情報通信」、「金融」、「航空」等の全部 14 分野が指定されている。

ステークホルダ

意思決定若しくは活動に影響を与え、影響されることがある又は影響されると認知している、あらゆる人又は組織。 [JIS Q 27000：2014]

制御システム

装置の動作やプロセスを制御するために使用される情報システム。制御対象資産である各装置類を管理するのに使用される監視制御データ収集システム（SCADA）、分散制御システム（DCS）、ローカルなプロセスを制御するプログラマブル論理制御装置（PLC）等を通じて制御するシステムなどがある。

脆弱性

１つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点。 [JIS Q 27000：2014]

セキュリティインシデント

望まない単独若しくは一連のセキュリティ事象、又は予期しない単独若しくは一連のセキュリティ事象であって、事業運営を危うくする確率及びセキュリティを脅かす確率が高いもの。

セキュリティ事象

セキュリティポリシーへの違反若しくは管理策の不具合の可能性、又はセキュリティに関係し得る未知の状況を示す、システム、サービス又はネットワークの状態に関連する事象。

セキュリティリスク

セキュリティリスクとは、セキュリティに関連して不具合が生じ、それによって企業の経営に何らかの影響が及ぶ可能性のこと。

センサ

計測中の物理特性（速度、温度、流量等）を表した電圧又は電流出力を発生させるデバイス。[NIST SP 800-82 rev.2]

認証（authentication）
エンティティの主張する特性が正しいという保証の提供。[JIS Q 27000：2014]

ビルシステム
ビルの管理・運用を行うための制御システムで、受変電、熱供給、空調、給排水、照明、昇降機、防犯、防災、監視カメラ等の各設備の制御システムの総称。

ファイアウォール
あるコンピュータやネットワークと外部ネットワークの境界に設置され、内外の通信を中継・監視し、外部の攻撃から内部を保護するためのソフトウェアや機器、システム等のこと。

プロトコル
複数の主体が滞りなく信号やデータ、情報を相互に伝送できるよう、あらかじめ決められた約束事や手順の集合のこと。

マルウェア(Malware)
許可されていないプロセスの実施を試みることによって、情報システムの機密性・完全性・可用性に悪影響をもたらすソフトウェア又はファームウェア。[NIST SP 800-53 rev.4]
セキュリティ上の被害を及ぼすウィルス、スパイウエア、ボット等の悪意を持ったプログラムを指す総称。

マルチステークホルダ・プロセス
3 者以上のステークホルダが、対等な立場で参加･議論できる会議を通し、単体若しくは 2 者間では解決の難しい課題解決のために、合意形成などの意思疎通を図るプロセス。[内閣府]

リスク
目的に対する不確かさの影響。[JIS Q 27000：2014]

リスク源
それ自体又はほかとの組合せによって、リスクを生じさせる力を本来潜在的にもっている要素。[JIS Q 31000：2010]

リスクマネジメント
リスクについて、組織を指揮統制するための調整された活動。[JIS Q 31000：2010]

付録 B　JDCC の建物設備システムリファレンスガイドとの関係

建物設備の情報インフラの推奨セキュリティ対策モデルとして、日本データセンター協会が『建物設備システムリファレンスガイド』を発刊している。これは、データセンターをモデルケースとし、建物設備システムのセキュリティの考え方についてまとめたガイドブックとして、21 の管理策を提示している。

この 21 の管理策では、物理的設計における管理策、建物設備システム構築時における管理策、設備システム運用における管理策に分類して、建物設備システムのセキュリティ対策の要件を分類、整理しており、ビルにおけるライフサイクルの考え方を一部取り込んだ物となっている。

ビルサブワーキンググループでは、この 21 の管理策をベースとして参照しつつ、データセンター以外のビル全般にわたるステークホルダによる議論で、より幅広い対象、状況に対応したガイドラインの策定を進めている。

図　付録 B-1　JDCC の 21 の管理策

（出典：建物設備システムリファレンスガイドとファシリティインフラ WG の紹介（2017/2、JDCC ファシリティインフラWG事務局））

付録C　建物設備システム リファレンスガイド　インシデント対応・セキュリティソリューション編との関係

日本データセンター協会は『建物設備システムリファレンスガイド』に加えて、建物設備へのインシデントは起こりえるという認識のもと、速やかなインシデント対応を可能とするように『建物設備システムリファレンス ガイド　インシデント対応・セキュリティソリューション編』を発刊している。これは、インシデント対応のモデルケースとして、準備段階、識別段階、封じ込め段階、クリーンアップと回復段階、フォローアップ段階の 5 つのフェーズに分けて、必要な対策をまとめたものである。

ビルサブワーキンググループでは、この 5 つのフェーズをベースとして参照しつつ、データセンター以外のビル全般にわたるステークホルダによる議論、特にビル管理のフローを意識する形で、インシデントレスポンスに必要な対策要件を整理し、本ガイドラインに組込んでいる。

付録Ｄ　サイバー・フィジカル・セキュリティ対策フレームワークの考え方と、サイバー・フィジカル・セキュリティ対策フレームワークの考え方を踏まえたビルシステムにおけるユースケース

１．フレームワーク策定の背景
～「Society5.0」におけるサプライチェーン構造の変化～

「Society5.0」では、データの流通・活用を含む、より柔軟で動的なサプライチェーンを構成することが可能となる。一方で、サイバーセキュリティの観点では、サイバー攻撃の起点の拡散、フィジカル空間への影響の増大という新たなリスクへの対応が必要となる。

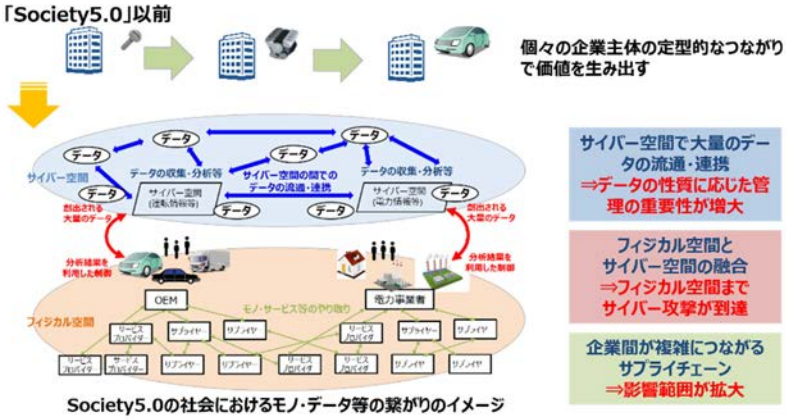


図　付録 D-1　Society5.0 社会におけるモノ・データのつながり

２．サイバー・フィジカル一体型社会のセキュリティのためにフレームワークで提示した新たなモデル
～三層構造と６つの構成要素～

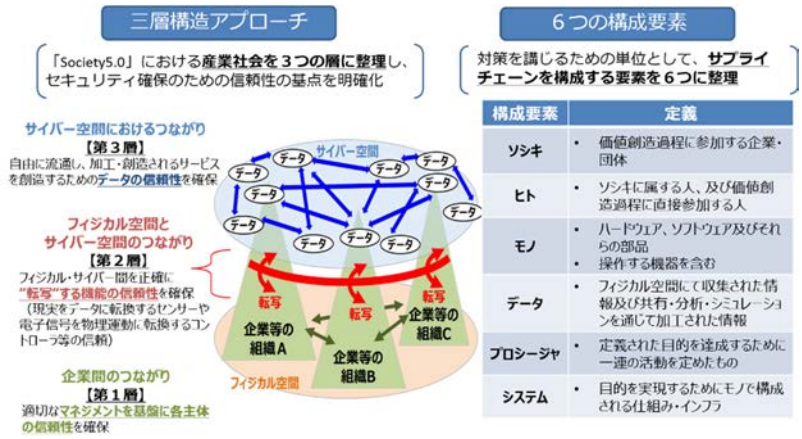


図　付録 D-2　三層構造アプローチと６つの構成要素の関係

３．フレームワークの全体概要
～リスク源と対応する方針の整理～

Society5.0 における新たなサプライチェーンの信頼性を確保する観点から、３つの層それぞれにおいて守るべきものを洗い出した上で、６つの構成要素に沿ってリスク源を抽出し、これに対する対策要件を提示。

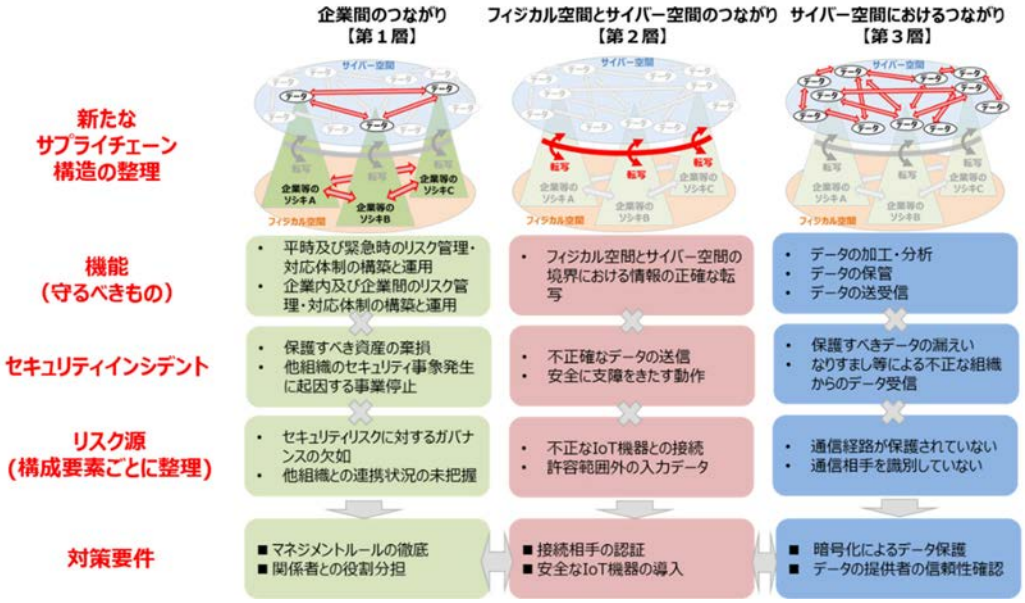


図　付録 D-3　３層構造と６つの構成要素に関連したリスク源と対策要件

４．フレームワークにおいて示されているユースケース：ビルの例

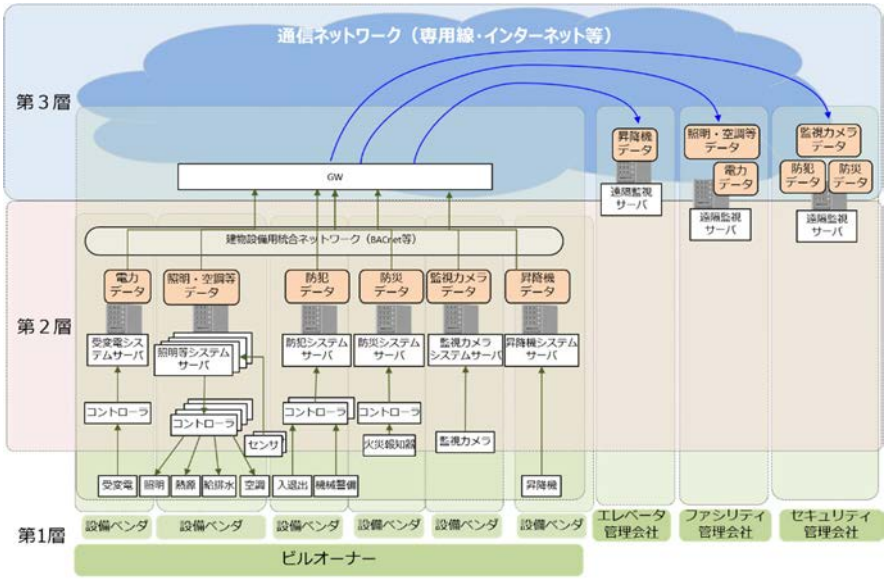


図　付録 D-4　３層構造に対応したビルのユースケース例

＜参考＞ビルの例のユースケース作成に当たっての整理について

１．本事例を作るに当たり想定したバリュークリエイションプロセス

ビルオーナーが、ファシリティ管理会社と契約等を行い、ビルから得られるデータを活用し、エネルギーマネジメントやビルの最適管理を行うプロセスや、遠隔地から監視・管理するプロセス。

２．フレームワークの留意点を踏まえた本ユースケースの特徴

ビル内の数多くの制御系システムの IP 化が進展。

ビルの遠隔地からの監視・管理を実現するためには、電力データ、昇降機データなどさまざまなデータのやり取りが必要。

エレベータ監視会社、ファシリティ管理会社など、ステークホルダが多い。

表　付録 D-1　ビルの分析対象と３層構造の関係

	分析対象の具体的イメージ
第１層	• ビル：ビルシステムにより監視・管理。 • エレベータ管理会社：ビルに導入されているエレベータの運転状況などを遠隔から監視・管理。 • ファシリティ管理会社：ビルの電力使用量などを遠隔から監視・管理。 • セキュリティ管理会社：ビルを監視カメラなどにより遠隔から監視・管理。 等
第２層	• コントローラ：照明、熱源、空調などを制御。 • 監視カメラ：異常事態の発生の有無を監視。 等
第３層	• 統合ネットワーク（BACnet等）：データのビル内外とのやりとり。 • データを取り扱うサーバ：データの保管・加工・分析等を実施。 • 取り扱うデータ －電力データ：ビルの様々な機器の電力使用量。ファシリティ管理会社が利用。 －防犯データ：入退室や機械警備などの情報を組み合わせたデータ。セキュリティ会社が利用。 等

フレームワークの議論は、産業サイバーセキュリティ研究会 WG1（制度・技術・標準化）にて随時行われている。WG の検討内容については、下記を参照のこと。

http://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/index.html

付録 E　参考文献

「建築設備設計基準　令和 3 年版」

一般社団法人公共建築協会

国土交通省大臣官房官庁営繕部設備・環境課制定（令和 3 年 3 月 16 日国土交通省国営設第 138 号）にもとづき、建築設備が備えるべき要件をまとめたもので、構内情報通信網及び中央監視制御装置についてサイバーセキュリティ確保のための要件を規定

https://www.pbaweb.jp/publication/books/kenchikusetsubi-sekkei-kijyun-r03/

「自家用電気工作物に係るサイバーセキュリティの確保に関するガイドライン」

経済産業省／電力安全課

自家用電気工作物（自家用発電設備や受配電設備等）のうち遠隔監視、制御等を行う設備に係るサイバーセキュリティの確保のためのガイドライン

https://www.meti.go.jp/policy/safety_security/industrial_safety/oshirase/2022/06/20220610.html

「制御システムのセキュリティリスク分析ガイド 第 2 版」

独立行政法人情報処理推進機構／セキュリティセンター

制御システムのセキュリティリスク分析を事業者が実施できるようにするためのガイド

https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

「サイバーセキュリティ経営ガイドライン Ver3.0」

経済産業省／サイバーセキュリティ課

大企業及び中小企業（小規模事業者を除く）を対象に、経営者のリーダーシップの下でサイバーセキュリティ対策を推進するためのガイドライン

※2023 年 3 月に ver3. 0 が公開

https://www.meti.go.jp/policy/netsecurity/mng_guide.html

「サイバーセキュリティ経営ガイドライン Ver 2.0 実践のためのプラクティス集」

独立行政法人情報処理推進機構／セキュリティセンター

「サイバーセキュリティ経営ガイドライン Ver 2.0」の「重要 10 項目」の実践に必要な事例を充実させたもの

https://www.ipa.go.jp/security/economics/csm-practice.html

「ネットワークカメラシステムにおける情報セキュリティ対策要件チェックリスト」

独立行政法人情報処理推進機構／セキュリティセンター

政府機関や自治体をはじめネットワークカメラシステムの調達者が、その機能と運用におけるセキュリティ上の対策を確認できるチェックリスト
https://www.ipa.go.jp/security/jisec/about/knowledge/nw-camera.html

「入退管理システムにおける情報セキュリティ対策要件チェックリスト」
独立行政法人情報処理推進機構／セキュリティセンター
政府機関や自治体をはじめ入退管理システムの調達者が情報セキュリティ上の要件や対策を確認するためのチェックリスト
https://www.ipa.go.jp/security/jisec/about/knowledge/nyutaikanri.html

「スマートホームの安心・安全に向けたサイバー・フィジカル・セキュリティ対策ガイドライン」
スマートホームにおけるサイバー・フィジカル・セキュリティ対策の考え方や各ステークホルダが考慮すべき最低限の対策について整理したガイドライン
https://www.meti.go.jp/press/2021/04/20210401005/20210401005.html
https://home.jeita.or.jp/smarthome/security/

「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（個別編：空調システム）第１版」
ビルのサブシステムの内、空調システムに特化して必要なサイバーセキュリティ対策の要件をまとめたガイドライン
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_building/20221024_report.html

「ISO8102-20:2022」
ISO（国際標準化機構、The International Organization for Standardization）
エレベータ, エスカレーター及び動く歩道に対する電気的要求事項として、サイバーセキュリティ対策要件をまとめたもの
https://www.iso.org/standard/78576.html

「IEC62443」
IEC（国際電気標準会議、The International Electrotechnical Commission）
制御システムに関するセキュリティ標準の体系。複数のサブ標準からでき上がっており、現在も検討、標準策定が続いている。制御システムのセキュリティ標準として、ビルシステムのセキュリティをこの標準で考えようというアイデアもある。
IEC TS 62443-1-1:2009　https://webstore.iec.ch/publication/7029

IEC 62443-2-1:2010	https://webstore.iec.ch/publication/7030
IEC TR 62443-2-3:2015	https://webstore.iec.ch/publication/22811
IEC 62443-2-4:2015	https://webstore.iec.ch/publication/61335
IEC TR 62443-3-1:2009	https://webstore.iec.ch/publication/7031
IEC 62443-3-3:2013	https://webstore.iec.ch/publication/7033
IEC 62443-4-1:2018	https://webstore.iec.ch/publication/33615
IEC 62443-4-2:2019	https://webstore.iec.ch/publication/34421

「Facility Cybersecurity Framework (FCF)」

Pacific Northwest National Labratory（米国エネルギー省）

住宅、商業施設、連邦ビルなど様々なタイプの建物を対象にサイバーセキュリティのベストプラクティス、ポリシー、プロセスにおける改善策を提供するフレームワーク

https://facilitycyber.labworks.org/assessments/coreAssessment

「Facility Cybersecurity Capability Maturity Model (F-C2M2)」

Pacific Northwest National Labratory（米国エネルギー省）

ビルのサイバーセキュリティに関する組織の成熟度をレビューするためのオンラインツール

https://facilitycyber.labworks.org/assessments/fc2m2

「UL 2900-2-3」

UL LLC （Underwriters Laboratories Limited Liability Company）

ビル等で利用する IoT 機器のセキュリティ認証のためのスキーム文書

https://news.ul.com/news/ul-2900-2-3-helps-mitigate-iot-cybersecurity-risk

※本ガイドライン（第 2 版）の検討体制

産業サイバーセキュリティ研究会　ワーキンググループ 1(制度・技術・標準化)
ビルサブワーキンググループ　構成員一覧

※敬称略、五十音順

座長	江崎浩　東京大学教授
	松浦知史　東京工業大学准教授
	アズビル株式会社
	イーヒルズ株式会社
	NTT コミュニケーションズ株式会社／株式会社 NTT ファシリティーズ／日本電信電話株式会社
	鹿島建設株式会社
	株式会社九電工
	株式会社きんでん
	技術研究組合制御システムセキュリティセンター
	産業サイバーセキュリティセンター（ICSCoE）施設管理（ビル）業界関係有志
	セコム株式会社
	ダイキン工業株式会社
	株式会社竹中工務店
	株式会社日建設計
	日本生命保険相互会社
	一般社団法人日本ビルヂング協会連合会
	株式会社日立製作所／株式会社日立ビルシステム
	一般社団法人ビルディング・オートメーション協会
	一般社団法人不動産協会
	三井不動産株式会社
	三菱地所株式会社／メック情報開発株式会社
	三菱電機株式会社／三菱電機インフメーションシステムズ株式会社
	横浜市

（オブザーバー）
国土交通省（大臣官房官庁営繕部設備・環境課、土地・建設産業局建設業課、土地・建設産業局不動産業課、住宅局住宅生産課、総合政策局情報政策課）

内閣サイバーセキュリティセンター東京 2020 グループ
中部国際空港株式会社／中部国際空港施設サービス株式会社

（事務局）
経済産業省（商務情報政策局サイバーセキュリティ課、製造産業局産業機械課）
株式会社三菱総合研究所

産業サイバーセキュリティ研究会　ワーキンググループ 1(制度・技術・標準化)
ビルサブワーキンググループ　インシデント・レスポンス作業グループ　構成員一覧

※敬称略、五十音順

イーヒルズ株式会社
株式会社九電工
株式会社きんでん
技術研究組合制御システムセキュリティセンター
株式会社竹中工務店
ICSCoE２期ビルチーム有志

（事務局）
経済産業省（商務情報政策局サイバーセキュリティ課）
株式会社三菱総合研究所

付属書

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
インシデントレスポンス・ガイドライン

産業サイバーセキュリティ研究会

ワーキンググループ1(制度・技術・標準化)

ビルサブワーキンググループ

目次

1. はじめに 1
1.1. 付属書の目的 1
1.1.1. 本付属書の目的 1
1.1.2. 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との関係 1
1.2. ガイドラインの適用範囲と位置づけ 2
1.2.1. 想定する読者 2
1.2.2. 対象とするビル 2
1.2.3. 対象とするビルシステム 2
1.2.3.1. ビルシステムの定義 2
1.2.3.2. ビルシステムの構成 3
1.3. 本ガイドラインの構成 5
2. サイバーインシデントへの対応 6
2.1. サイバーインシデントへの対応の流れ 6
2.1.1. 準備段階 8
2.1.2. 識別段階 11
2.1.3. 封じ込め段階 12
2.1.4. クリーンアップと回復段階 15
2.1.5. フォローアップ段階 16
3. ビルシステムに係るセキュリティ関連サービス 18
3.1. ネットワーク設計サービス 19
3.2. 既存システムのセキュリティ診断サービス 19
3.3. 運用・監視サービス 19
3.4. 教育・研修サービス 20
3.5. 各種コンサルティングサービス 20
付録 A 用語集 21
付録 B 参考文献 23

1. はじめに

1.1. 付属書の目的

1.1.1. 本付属書の目的

「付属書　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　インシデントレスポンス・ガイドライン（案）（以下、付属書）」では、「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（以下、共通編）第 2 版」において記述したインシデントレスポンスの詳細を記述するものとする。

付属書では、インシデントレスポンスに係る事前準備からフォローアップについて、順を追って説明していく。

1.1.2. 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との関係

ビルシステムにおけるサイバー・フィジカル・セキュリティ対策に関しては、ビルシステムに共通して対策すべき事項を共通編、各サブシステムに特化して対策すべき事項を個別編という、2 階建て構造を取っているところ、本付属書は、共通編のインシデントレスポンスの詳細を記述する文書として、共通編に紐づくものである。

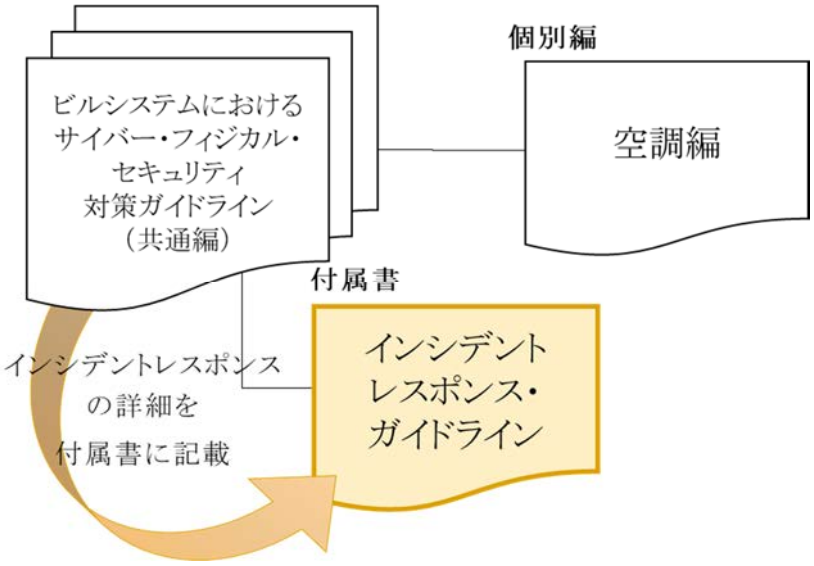


図 1-1　付属書の位置づけ

1.2. ガイドラインの適用範囲と位置づけ

1.2.1. 想定する読者

本ガイドラインでは、ビルシステムに対するサイバー攻撃によるインシデントへの対応において検討すべき事項について解説しており、主にビルシステムに関わるステークホルダを主な読者の対象としている。

特に、ビルオーナーが体制整備やビル管理に係るマニュアル等の作成の参考にすることを想定しており、具体的な対象者としては以下を想定している。

【主な読者】

- ビルオーナー

【参考にして欲しい読者】

- ゼネコン、サブコン
- 個別システム事業者（ビル管理システム、空調、エレベータ、ビデオ監視、電力・熱供給　等）
- ビル管理会社　など

1.2.2. 対象とするビル

サイバーインシデントは、運用段階における端末やネットワーク経由による攻撃だけでなく、ビルに導入する情報システムの構築段階におけるアプリケーション等の脆弱性、セキュリティホール等のリスクもある。

そのため、本ガイドラインが対象とするビルは、統合ネットワークに接続しているビルシステムを有するビルを対象として記載した。

1.2.3. 対象とするビルシステム

対象とするビルシステムは、原則として「共通編」と同等とする。以下、関連する内容について、「共通編」から転載した。

1.2.3.1. ビルシステムの定義

ビルシステムはビルの管理・運用を行うための制御システムであり、受変電制御システム、熱供給制御システム、空調制御システム、給排水制御システム、照明制御システム、昇降機制御システム、防犯・入館管理システム、防災監視システム、監視カメラシステム、またこれらを統合的に監視・管理するためのビル管理システム等の個別の設備・システムが存在する。通常はそれぞれ独立したサブシステムとなっており、全体としてビルを管理・運用するビルシステムを構成する。

このため、本ガイドラインでは、ビルシステムとしては、各サブシステム及び全体としてのビルシステムを指すこととする。なお、本ガイドラインでは、個別のサブシステムの違いではなく、共通的な要素に絞って脆弱性やリスク、セキュリティ対策等をまとめて

いるもので、各サブシステムに何らかの関わりを持つステークホルダが、共通に検討すべきサイバーセキュリティ対策の指針を示すものである。

なおビルの管理・運用にあたっては、リソースの管理や課金管理、テナント等の顧客管理や営業管理のために IT システムも利用されていたり、制御システムと接続されていたりするケースもあるが、IT システムのサイバーセキュリティに関しては一般的に取り組みの進んだ世界となっており、ここでは対象とはしない。但し、IT システムと接続するためのビルシステム側のインターフェースまでは対象として検討を行っている。

またビルに関連するシステムとして、最近では IoT の活用等も進みつつあり、テナントやビルの利用者向けに各種の新たなサービスを展開するシステムが、ビル内に存在するケースも増えている。ビルそのものの運用からは外れるため、ガイドラインの対象外ではあるが、将来的にはこれらのシステムについてもサイバーセキュリティの議論が必要になると思われる。

1.2.3.2. ビルシステムの構成

ビルシステムにおけるサイバーセキュリティ対策を検討する上で、まず資産（アセット）の明確化を行う。即ち対象となるシステムの構成として、どのような機器がどのように接続されているかを把握する作業を実施する。同様に、各機器がビル内のどこに置かれているのかも、物理的なセキュリティを検討する上で、重要な情報となる。

ビルがその外観デザインも、構造も、内装も、1棟1棟が異なっているように、ビルシステムもまた、1 つ 1 つそれぞれ異なっており、1つとして同じ物は存在しない。但し、ガイドラインを作成するにあたっては、なるべく多くのビルシステムを包含するような形でのモデル化が大事であり、ここでは、様々にあるパターンから現在のビルシステムの姿として代表的な概略例を示す形で、ビルシステムの構成要素についての整理を行った。

図 1-2 は様々な個別設備システムからなるビルシステムの全体像をモデル的に示したものである。各システムの構成も接続方法も、それぞれのビルの規模やビルシステムの構築ポリシーによって異なってくるが、代表的な 1 モデルという形で示している。この図においては、個別の設備システムはそれぞれ独立して運用される形となっているが、全体としては統合ネットワークにて接続されており、必要な連携（例えば火災報知器の情報をもとに、居室の鍵を全開錠とするなど）が可能となっている。設備システムごとにサーバ（BA 主装置）や制御端末（HMI）を持っているが、統合が進んだケースとして、統合ネットワークに直接接続された監視端末で、各サブシステムを統合監視するケースも増えつつあるようである。

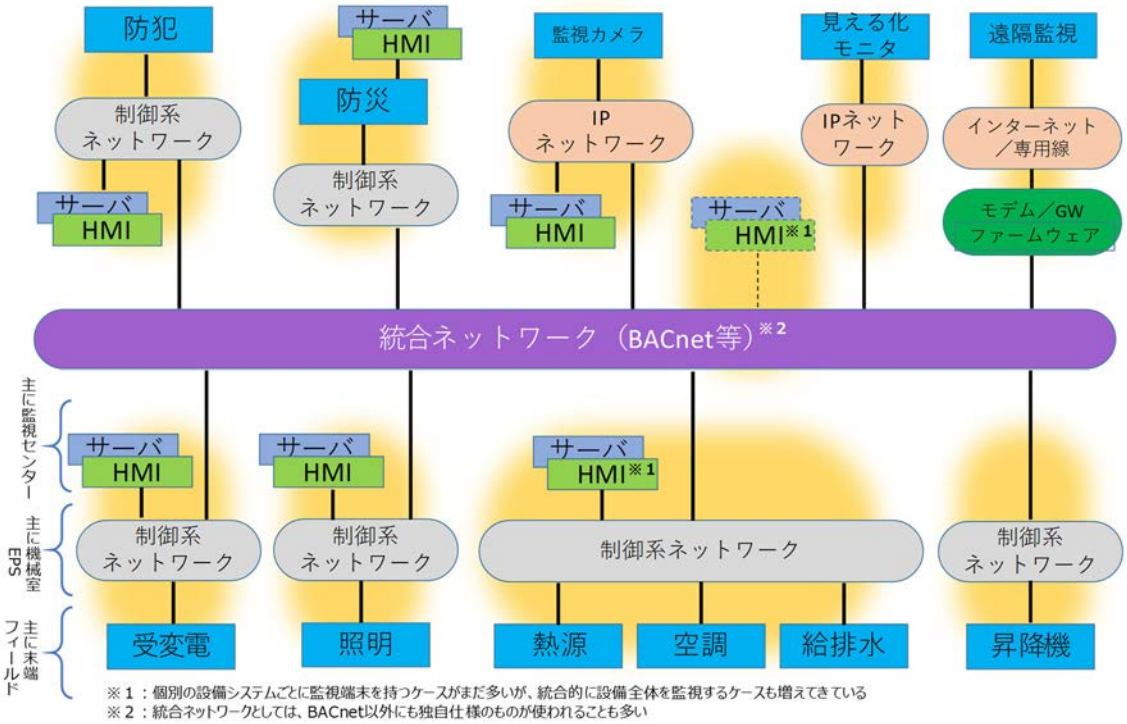


図 1-2　ビルシステムの標準的なモデル（全体像）

1.3. 本ガイドラインの構成

ガイドラインの本節以降の部分は、以下の項目に大別される。

■第2章： インシデントへの対応について、各フェーズにおけるステークホルダ別に実施すべき事項等を示す。

■第3章： セキュリティベンダ等によるセキュリティ関連サービスの概要を紹介する。

また、本ガイドラインには、補足資料を提供する以下の付録も含まれる

■付録 A： 本書で使用する用語集

■付録 B： 参考文献

2. サイバーインシデントへの対応

2.1. サイバーインシデントへの対応の流れ

ビルシステムのインシデントについては、それがサイバー攻撃によって引き起こされたのか、あるいは、何らかのファシリティの故障によって発生したのかを、故障等の発生時に判断することは非常に困難である。したがって、初期の対応方法は、通常の故障対応と同様になり、原因究明等をしていく中でサイバー攻撃によるインシデントであったことが判明するものと考えられる。

ここでは、日本データセンター協会（以下、JDCC）発行の「建物設備システムインシデント対応ガイド」の考え方を参考に、インシデントレスポンスを「準備段階」から「フォローアップ段階」まで、大きく5段階のフェーズに分割して考える（図 2-1）。以下、それぞれの段階について説明する。

（出所：JDCC「建物設備システムインシデント対応ガイド」）

図 2-1　インシデントレスポンスの流れ

また図 2-2 は、上記を踏まえた、ビル管理におけるインシデントレスポンスの一般的なフローの例である。

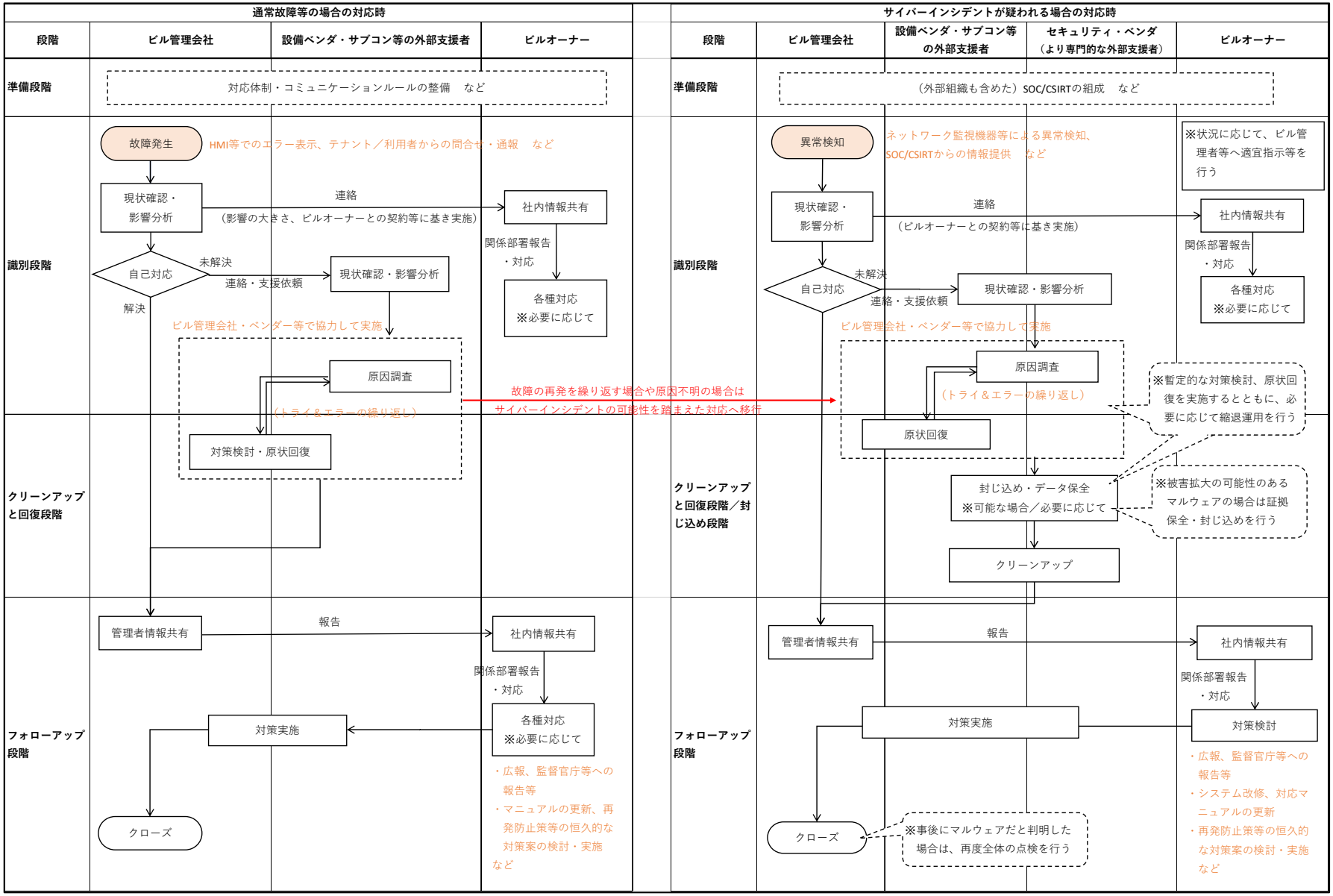


図 2-2　インシデントレスポンスのフロー（例）

人も予算もリソースには限度があるため、全てのインシデントに対応する事は出来ない。そこで、組織のビジネスの影響度に応じて対応の優先度をどのようにするのか等、インシデント時に迅速な判断をできるよう、計画を予め作成することが必要である。例えば、USB などの外部メディアからの攻撃によってインシデントが発生した場合や、DDoS 攻撃、内部犯による攻撃などインシデントの種類によって優先度を考える。その際に検討する関連要因としては、以下のようなものが考えられる。

1)　ビジネス機能へのインパクト

インシデントがビジネスを行うために必要なシステムの機能にどれくらい影響があるか(テナントや来訪者への影響など)

2)　情報へのインパクト

情報やデータ(顧客情報等)に対してインシデントが影響する場合には、その情報の機密性(Confidentiality)、完全性(Integrity)、可用性(Availability)にどれくらい影響するか

3)　インシデントからの回復性

インシデントから回復するのに必要とする時間とリソースはどれくらいか

4) 対応結果の評価の仕組み

インシデントへの対応結果を評価する仕組みを決め、将来のインシデントレスポンスにおける計画／戦略の見直しを行う。

また、インシデントレスポンスに用いるツールも整備する必要がある。例えば以下のようなツールを整備しておくことが考えられる。

- 関係者との連絡ツール(連絡網(連絡先一覧)、電話/メールなど)
- 報告フォーム、コンタクトフォーム
  ※通常時からのビル管理者への意識づけとして、現場のビル管理者からビルオーナーへの故障対応の報告書様式に、明示的に「サイバー攻撃への対応」に関する記載項目を設けること等も考えられる。
- 対応方針に係るポリシーや対応手順を確認するマニュアルやワークフロー(やりとりする内容)
- 教育・研修に係るマニュアル・資料　など

2.1.1. 準備段階

(1) 目的及びゴール

インシデントの対応は、主に2つの行動に分けることができる。

- 事態を収拾するために「今すぐ」行う必要がある行動
- 何が起こったか診断し、混乱を片付けるための行動

ビルオーナーは、上記2つの行動を円滑に実施できるよう、ビルのテナントとの関係も含む優先事項等の運用方針を踏まえたビル管理の体制や対応フローの準備を行い、最終的にインシデント発生時に適切な初動対応を行うことができるよう準備を整えることを目指す。具体的には、各ビル管理の現状等を踏まえて、図 2-2 に示したインシデントレスポンスのフロー（例）等を具体化し、実現するための準備を行う。

(2)　活動内容と役割

ビルオーナーは、準備として以下の項目について検討し、文書化しておく。インシデント発生前に行っておくべきものを揃え、各関係者との調整を行うと共に、それらが実際に機能するかをできる限り確認する。ただし、ビル管理に係る既存の運用ポリシーや計画等がある場合は、サイバー攻撃への対応を想定した観点から必要に応じて記述の修正・追加を行うことでもよい。

①　対応体制（インシデントレスポンス・チーム）の整備

前述の「インシデントレスポンスのフロー（例）」（図 2-2）に示したフローの実施を想定した、インシデント発生時の対応チームについて検討する。対応チームは、各関係者に役割を果たせる職能があることを担保することが重要である。

対応チームは、社内関係部署、サブコン・設備ベンダ、セキュリティベンダ等から構成されるが、恒常的な組織ではなく、インシデント発生時に必要に応じて組織される場合や、既存組織が対応する場合もある。そのため、リーダー（対応責任者）や社内外の各関係者の必要な機能や権限について検討し、相互の協力関係を構築する。権限とは、情報リソースにアクセスできる権限であり、情報漏洩や間違った情報流出を防ぐため、適切に管理される必要がある。また、システムの停止や再起動、ネットワークの切断等の決定責任者、実施責任者等についてもあらかじめ決めておくと良い。さらに、接続の切断、疑いのある活動の監視、インシデントについての報告義務も含める。

このようなインシデントレスポンス・チームの役割、責任、権限レベルを表す文書を整備することが望ましい。

さらに、IT を含む関連システムのインシデント対応主体との情報共有や連携体制について予め合意形成しておくことが重要である。可能であれば、双方のインシデントレスポンス・マニュアルにも合意内容を記載する。

なお、これらの体制整備については、比較的リスクの高いビルから検討を開始する等、各社の状況に合わせて優先順位を付けて対応することも考えられる。

より高度な対応を行うためには、外部のセキュリティベンダ等と協力しながら、事前にインシデントの検知や対策について検討する SOC（Security Operation Center）、インシデントレスポンスの司令塔となる CSIRT（Computer Security Incident Response Team）の組成を検討することも有効である。

表 2-1　インシデントレスポンス・チームの役割等の例

関係主体	主な役割	責任
ビルオーナー	• インシデントレスポンスに係る各種判断・決定	最終的なすべての責任主体となる
ビル管理会社	• 現場における事象確認・影響調査 • 一次対応 • サブコン等への対応指示 • ビルオーナーへの各種報告 • テナント対応　など	ビルオーナーの指示に基づく現場の管理
サブコン・設備ベンダ	• ビル管理会社及びセキュリティベンダとの協力によるシステム又は設備の復旧及び原因究明 • ビル管理会社への各種報告	ビルオーナー又はビル管理会社の指示（例えば契約等）に基づくシステム又は設備の復旧・原因究明
セキュリティベンダ	• ビル管理会社及びサブコン・設備ベンダとの協力によるインシデントの解消及び原因究明 • ビル管理会社への各種報告	ビルオーナー又はビル管理会社の指示（例えば契約等）に基づくインシデントに係る復旧・原因究明

②　コミュニケーションルールの整備

一般的な故障発生時の対応と同様に、サイバーインシデント発生時のコミュニケーション手法についても定める。関係各所の連絡先一覧等も作成する。

インシデントの内容や影響範囲、現状のコミュニケーション方針等を勘案して、誰と、どうやって、いつコミュニケーションを行うか、予め検討する。正しい相手に対して、適切な情報だけを伝え、相互にやりとりできるように予め検討してガイドラインを決めておくことが大切である。

上記を踏まえ、社内の広報、法務、営業等とのコミュニケーションルートやツール（メール等）についても詳細に決めておく必要がある。他にも、不確定情報や承認済み情報の管理などの取り扱いのルールを細かく決めておくとよい。

③　システムのバックアップ及び封じ込め方針等の検討

インシデントが発生した場合の復旧、封じ込め等を想定し、設備の設定等のシステムのバックアップを定期的に取得する。より速やかな復旧のためには、バックアップの対象は何か、誰が取得するのか、いつ取得するのか、どこに保存されるのか等を一覧にしておくとよい。バックアップを取得することができない場合は、バックアップが無い前提での対応方針等を検討する。なお、ビル内のすべてのシステムや設備のバックアップを取得・管理することはコスト等の観点からも現実的でないため、例

えば中央監視設備等の重要設備や運用への影響の大きい設備を優先する等、各ビルの状況に合わせて優先順位を付けて対応することも考えられる。

また、インシデント発生時の封じ込めを想定し、インシデントの発生個所（設備・端末、システム）毎のネットワークの切断の可否及び切断ポイント、切断した場合のテナントやビジネス等への影響、これらを踏まえた対応方針等についても検討する。

④　ビル全体のシステムネットワーク一覧等の作成

インシデントに対して適切に対応し復旧するためには、設備等に加えた変更・更新結果も反映された、ビル全体のシステム及びネットワークの最新の状況を正確に把握することが重要である。

そのため、ビルオーナーは、ビルに導入されているすべてのシステムや機器（サーバ、端末、OS、アプリケーション等）を把握することのできる一覧表や、ネットワーク図、当該ビル内外の各種システムとの接続・連携構成、それぞれの運用・管理担当者（担当設備ベンダ等）を網羅した文書を作成する必要がある。

⑤　教育・研修（訓練／演習等）

インシデントが発生した際に、事前に検討した対応フローを正しく機能させるためには、訓練や演習が不可欠である。例えば、サイバー攻撃に係る基本知識、対応フローの内容の確認、インシデントを想定した机上シミュレーション等が考えられる。また、参加対象者も、社内のみ、またはサブコン等も含むなど、いくつかの形態が考えられる。

2.1.2.　識別段階

(3)　　目的及びゴール

ビルオーナー及びビル管理者は、外部のサブコン、設備ベンダ、セキュリティベンダ等の専門家と協力しながら、原因調査によるインシデントの切り分けを行い、今後の対応方針を決定するとともに、原状回復を行う。多くの場合において、原因調査と原状回復はトライ＆エラーを繰り返して実施することになる。

(4)　活動内容と役割

ビルオーナー及びビル管理者は、セキュリティベンダ等の外部の専門家にも加わってもらい、さらに原因の特定及び原状回復に取り組む。

なお、事前の自己対応として、ビル管理者は、日常の実施事項（メンテ、空調の変更等）の記録の確認、通常の故障対応と同様の決められた対応（設備の交換、端末の再起動など）、確認・対処したことの記録を行う。例えば、以下のような場合にサイバー攻撃の可能性が疑われる。

- メンテナンスの後のタイミングで故障した場合

- 不審なパケットが確認された場合
- 空調等の設備がスケジュールとは異なる動作をしている場合
- 監視画面などのシステムが暗号化され脅迫文が表示された場合　など

通常の故障対応により原状回復した場合は、サイバー攻撃によるインシデントではないと考えられるため、通常の故障対応として、インシデントレスポンスは終了する。通常の故障対応では原状回復しない場合や、一旦は回復するも同様の故障が繰り返し発生する等により原因が特定できない場合は、以下の手順に進む。

①　現状確認・影響分析

ビル管理者は、インシデント発生を発見した場合に以下に示す事項について明らかにする。なお、一般的な故障対応と概ね同様であるが、ここでは特にサイバー攻撃によるインシデントを想定して記述した。

【現状確認】

- インシデントがいつ、どこで発生したか？
- 誰がインシデントを発見、報告したか？
- どのように発見したか？
- インシデントのソース（原因、発生源）は特定されているか？どこで、いつ、何か？
- 現象の内容（スケジュール外の動作、データの暗号化、不審なパケット　など）

【影響分析】

- インシデントによって侵害された他の領域はあるか？もしあるならば、それらはどこで、いつ発見されたか？
- インシデントのソース（原因、発生源）及び特性を踏まえて、影響の範囲はどこか？
- ビジネス・テナント等へはどのような影響があるか？

②　原因調査（設備ベンダ等による事象確認・影響調査等）

例えば以下のような段階を経て原因調査を行うことが考えられる。また、サイバー攻撃であると確認できた場合には、速やかに社内関係部署（広報、営業、他ビル管理部署等）や業界団体と情報共有し、注意喚起することが望ましい。

1）設備ベンダ等で対応（機器交換、再インストール等）し、事象確認・原因調査を行う
2）設備ベンダ等では対応できない又は現象が再発する場合、複数の設備に原因・影響がある場合は、セキュリティベンダ等に支援を依頼して原因調査を行う

2.1.3.　封じ込め段階

(5)　目的及びゴール

設備ベンダや外部の専門家等と協力しながら被害を最小限に留めて、更なる被害の拡大を防ぐ。この作業には、自社が他社やユーザに対して加害者とならないようにすることも含まれる。

(6)　活動内容と役割

ビル管理者は、損害を最小限に留めて、更に被害を拡大しないように、影響を受けたシステムを切り離し、その他のシステムへの被害の拡大を防ぐ。さらに、後の対策段階で必要になる検証材料(証拠)を破壊しないようにする。必要に応じて、「識別段階」あるいは「クリーンアップと回復段階」と同時に実施する。

なお、他システム等への被害拡大が想定されないインシデントの場合や、侵害されたシステムの切り離しが運用上不可能な場合は、「封じ込め段階」の対応は行わない。

表 2-2　インシデントと対応の例

インシデントの例	対応の例
システムの脆弱性を突いた攻撃を受けた	• 攻撃を受けたシステムから他システムへ侵入される可能性があるため、テナントへの影響等を考慮した上で、可能な範囲でシステムを切り離す「封じ込め」を行う（LAN ケーブルの抜線など）
一部のシステム・端末がマルウェアに感染した	• マルウェアの種類やシステム・端末への影響を調査し、他システムへの感染拡大等が無いと判断された場合は、当該システム・端末のマルウェアの駆除を行う（「封じ込め」は行わない）。 • 影響が通常運用の許容範囲内の場合は、例えば定期点検時に駆除することも考えられる

ここでの対策は、以下の 2 つに分類できる。ただし、切り離しの難しいシステム(中央監視システムなど)もあるため、運用に問題のないよう、できる限り事業継続の可能な施策を検討する必要がある。

③ システムバックアップ

影響範囲や被害状況を正確に特定し、更にはインシデントの原因を詳しく調査(データ保全・解析等)するために必要なデータの収集を行う。以下のようなことが出来ているか確認する必要がある。

1) 更なる分析に必要な、影響を受けたシステムのログデータ等のコピーが作成されているか？

2) インシデントが発生してから、影響を受けたシステムで発生した事象およびその他の重要なアクションを含む記録が全て文書化されているか？

- 文書化出来ていない場合は、裁判あるいは後日のフォローアップのために、すべての証拠を確実に残すためにできるだけ早くに文書化を行う。

3) 解析を行うためのデータは安全な場所に保管されているか？

- 保管されている場合は、③長期封じ込めの作業に進む。
- 保管されていない場合は、データを安全な場所に配置して、偶発的な損傷や改ざんを防止する。

ログデータのバックアップおよび分析は、サイバー攻撃の侵入経路やどのような攻撃を受けたか等の分析にあたって重要な情報となる。また、各種設備等の設定値データのバックアップは、早期に原状回復するために有効である。一方で、これらのバックアップをすべて取得するのはコスト等の観点からも非効率である。そのため、各システムや設備毎に、ログ等のバックアップの目的（どのような分析や回復に利用できるか等）、取得頻度を検討し、必要に応じて設備ベンダ等とバックアップの取得に係る保守契約を結ぶ。

④ 封じ込め

システムの侵害を制限し被害拡大を防ぐために、「準備段階」において予め検討した方針で、ネットワークの切断等を実施する。あわせて、設備等の設定、データ、ログのバックアップが残っているかを確認する。なお、影響を受けたシステムは、電源を落とすと消えてしまう侵入痕跡もあるため、切り離した後も詳細調査用データを取得完了するまでは機器の電源を切らずに置いておく。

具体的には、以下のようなことを検討、実行する。

1) 侵害を受けているシステムなどの問題箇所を特定することが出来ているか？

- 出来ていない場合は、システムの所有者やマネージャーと協力して、問題を封じ込めるために必要な追加の対策を決定する。

2) 影響を受けたすべてのシステムは、影響を受けていないシステムから分離されているか？

- 分離されていない場合は、インシデントがこれ以上拡大しないように、短期的な封じ込めが完了するまで、影響を受けるシステムの隔離を継続する。

建物管理の設備（電源、空調・熱交換、照明など）は、原則、外部ネットワーク（インターネット）またはビル内ネットワークから隔離しても、安全性や可用性を担保した上で設備単体での安定動作が可能な設計・竣工がなされている。そのため、ビル管理者は、各設備を担当する設備ベンダに確認の上、ネットワークの流れを物理的に遮断（内外部のネットワークから隔離）する。ただし、近年はオープン化、クラウド化、

設備ネットワークの IP 化が進んでいるため、必ずサブコン及び各設備を担当するベンターに確認することが必要である。

ネットワークの流れの物理的な遮断を行うことで、建物の安全性や可用性に悪影響がある場合、または原因追及を優先する場合は、可能であれば、代替手段として、不審な通信（収集したシステムのログから分析を元に特定した通信）を F/W（ファイアウォール）やルータ、L2SW や L3SW、セキュティ機器などで、論理的に遮断する措置のみに留める。

さらに、最終ステップとして、攻撃を受けたシステムに対策を行い、通常運用を行えるようにする。例えばソフトウェアの脆弱性に起因するインシデントの場合は、セキュリティパッチをあてる等の対策を実施する。

1) システムをオフラインにできる場合は、次の「クリーンアップと回復段階」に進む。
2) システムを運用状態のままにする必要がある場合は、影響を受けるシステムからすべてのマルウェアやその他の侵害による影響を削除して、長期的な封じ込めを進め、影響を受けるシステムのイメージを再作成できる理想的な状況になるまで、影響を受けるシステムをさらなる攻撃から防ぐように強化する。

2.1.4. クリーンアップと回復段階

(7) 目的及びゴール

影響を受けたシステムをクリーンアップ（マルウェアの駆除等）し、全く汚染されていないシステムとして復元する。なお、テナント等への実被害が認められないと判断した場合は、後日の定期点検時などにおいてクリーンアップすることでも構わない。

(8) 活動内容と役割

影響を受けたシステムをクリーンアップし、全く汚染されていないシステムとして復元する。

⑤ クリーンアップ

「識別段階」において判明した原因に対処を行い、影響を受けたシステムへの侵害を根絶する。

なお、「封じ込め」段階で実施している「システムバックアップ」（インシデントの原因を詳しく調査するフォレンジックを行うために必要なデータ）に関連して、法的措置のために一定期間は「クリーンアップと回復」が実施できないこともある。

1) 可能であれば、システムのイメージを再作成し、パッチやその他の対策でセキュリティの強化を行う。また、その他の対策により攻撃のリスクを防止または軽減できるかどうかを検討する。もし、そのような対策が難しい場合には、その理由をビル管理者等に報告させる。

2) 攻撃者によって残されたすべてのマルウェアやその他の侵害の痕跡が削除され、影響を受けるシステムがさらなる攻撃に対して強化されているかどうかを確認する。そうでない場合、その理由をビル管理者等に報告させる。

復旧にはクリーンなバックアップがあると、復旧に要する費用が安く済むとともに、時間の節約にもなる。設備ベンダに「竣工当時の制御システムの各種設定・データなどのバックアップ」が保存されていることが多いため、このバックアップを利用して復旧にかかる時間の短縮や費用の削減に有効活用できないか確認する。

⑥ 追加調査

原因不明の場合は、クリーンアップと同時に、必要に応じて更なる原因究明を行い、再発防止のための情報を収集する。

2.1.5. フォローアップ段階

(9) 目的及びゴール

システムの復旧後に、同じインシデントが発生しないよう対策を行う。また、インシデントに係る対外発表や外部組織への報告等もこの段階に含まれる。

(10) 活動内容と役割

⑦ ビル管理者等における対策検討・実施内容の情報共有

システム全体を本来の運用状態に回復させるために実施した事項について、ビル管理者およびサブコン、設備ベンダ等で情報共有を行う。情報共有に先立ち、例えば以下について検討・実施することが考えられる。

1) 元のシステムや運用にどのような対策を行うかについて検討し、実施する。
2) 元のシステムや運用に対応策が適用され、将来の同様の攻撃に対しても強化されていることを、複数の関係者で確認し、情報共有する。
3) システム復元後も、再発が無いか等について定期点検等で確認・報告してもらう。

⑧ ビルオーナーにおける社内情報共有

ビルオーナーは、発生したインシデントに係る各種情報を社内で共有する。情報共有にあたっては、以下のような検討、対応を行う。

1) ビルオーナーのインシデントレスポンス・チームは、インシデントとその影響（テナントへの影響等も含む）や対策についてのすべての事象に関する文書（インシデントレスポンス・レポート）を作成する。作成できていない場合は、できるだけ早

く文書化し、インシデントレスポンスにあたっての重要事項をレポートに記載する。

2) インシデントの影響範囲に応じて、法務、広報、営業などのステークホルダに適切に情報提供することが重要である。そのため、対外発表や外部組織への報告を想定し、必要に応じて想定問答集を作成する

3) 被害状況によっては、インシデント解決から一定期間内に、インシデントに対応した社内関係メンバー（法務、広報、営業など）を集め、例えば以下のようなテーマで検証会議を開催する。

- インシデントレスポンスにあたったメンバーによる、発生したインシデントの対応プロセスの確認
- 対応プロセスがより適切に処理できた可能性のある点や、間違いについての振り返り

3. ビルシステムに係るセキュリティ関連サービス

サイバーセキュリティの脅威の顕在化を受けて、各社からさまざまなソリューションが提供されている。インシデントレスポンスを実現するため、例えば、ネットワーク設計支援やアプライアンス機器等の導入にサイバー演習支援、既存システムに対する脆弱性の診断、遠隔における健全性のモニタリングのための NOC、SOC ソリューション、更には AI を用いた高度な脅威検知なども提案されている。

表 3-1　ビルシステムに係るセキュリティ関連サービスの例

サービス分類	概要
ネットワーク設計サービス	• 各設備ネットワークに各種セキュリティ製品と連携したネットワーク設計を行う。これにより、未承認デバイスの設備ネットワークへのアクセス排除、攻撃被疑端末の位置特定、設備通信内容の解析等のサイバーセキュリティ対策を実現
既往システムのセキュリティ診断サービス	• BA システム全般の脆弱性診断を行う。Web アプリケーションやクラウドシステム、IoT 機器を含むネットワーク全般等を対象に、リスク評価、潜在的な問題点の洗い出し等を行う • さらに、新規採用予定の機器等について、セキュリティ標準規格への準拠性や設定ミス、潜在的な脆弱性の診断を行う
運用・監視サービス	• 顧客の国内監視拠点や海外監視拠点それぞれに NOC/SOC を設置し、24 時間 365 日でシステムの運用・監視サービスを提供
教育・研修サービス	• 「従業員のセキュリティ意識の向上」を図るため、座学やゲーム形式の体験型演習等の研修サービスを提供 • 実際に起きているサイバー攻撃手法シナリオに基づいた対応プロセスを、身をもって体験することにより、初動対応のスキルを習得する
各種コンサルティングサービス	• 既設建物への対策立案や第三者評価等を実施 ➢ 情報資産台帳策定支援サービス ➢ 情報セキュリティ対策サービス ➢ 第三者評価支援サービス ➢ 情報セキュリティ教育支援サービス　など

3.1. ネットワーク設計サービス

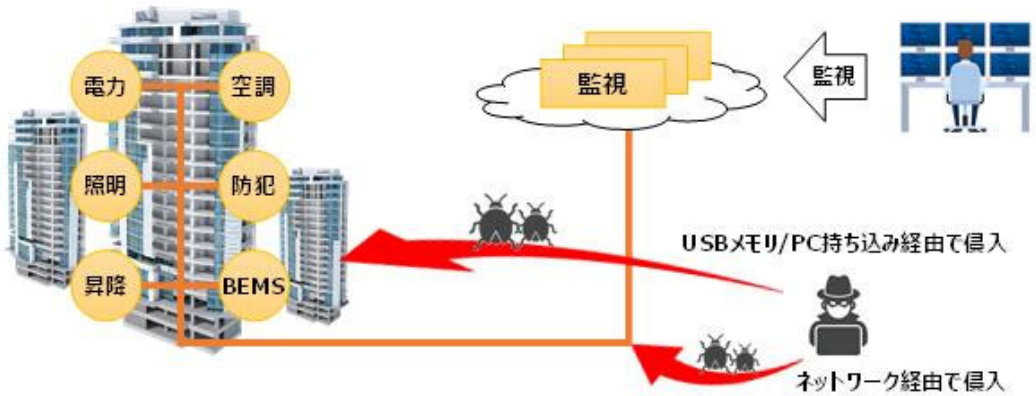
近年のビル設備ネットワークおよびマネジメントシステムはオープン化（IP・Web 化）により中央監視室での集中管理を行う場合が多い。そのため、外部（インターネット）、内部からのサイバー攻撃を意識したシステム構成を導入し、アラームを監視し、インシデント対応を準備する必要がある。

このような背景から、各設備ネットワークに各種セキュリティ製品と連携したネットワーク設計を行うサービスが提供されている。これにより、例えば、未承認デバイスの設備ネットワークへのアクセス排除、攻撃被疑端末の位置特定、設備通信内容の解析等のサイバーセキュリティ対策を実現することができる。

3.2. 既存システムのセキュリティ診断サービス

既に運用されているシステムや設備等のインフラは、導入時もセキュリティに留意した設計・構築を行っていても、進化するサイバー攻撃手法に対応しきれていない場合もある。

そのため、BA システム全般の脆弱性診断を行うサービスが提供されている。Web アプリケーションやクラウドシステム、IoT 機器を含むネットワーク全般等を対象に、リスク評価、潜在的な問題点の洗い出し等を行う。さらに、新規採用予定の機器等について、セキュリティ標準規格への準拠性や設定ミス、潜在的な脆弱性の診断を行う。



（出所：https://news.panasonic.com/jp/press/jn200114-1）

図 3-1　サイバー攻撃のリスク評価

3.3. 運用・監視サービス

ビルシステムにおいては、「サイバー攻撃を止める、不審なアクセスを遮断する」といったシステム保護を目的とした対策は、可用性の観点から非常に困難である。そのため、特に既存ビルの運用においては、セキュリティ製品の導入等によるシステムの監

視を行いつつ、SOC 等と連携することが考えられる。これをサポートするものとして、顧客の国内監視拠点や海外監視拠点それぞれに SOC を設置し、24 時間 365 日でシステムの運用・監視サービスが提供されている。

（出所：https://www.softbanktech.co.jp/special/blog/sbt_sbt/2022/0013/）

図 3-2　運用・監視サービスのイメージ

3.4. 教育・研修サービス

サイバー攻撃から守るためのセキュリティ製品やサービスの使用、防御を突破されてしまった場合の対応は原則として従業員が行うことから、さまざまな教育・研修サービスが提供されている。

（出所：https://jpn.nec.com/cybersecurity/theme/hr-dev.html）

図 3-3　クイズ・ゲーム形式によるスキルアップ

3.5. 各種コンサルティングサービス

上記のほか、各社からさまざまなコンサルティングサービスが提供されている。

- 既設建物への対策立案や第三者評価等を実施
- 情報資産台帳策定支援サービス
- 情報セキュリティ対策サービス
- 第三者評価支援サービス
- 情報セキュリティ教育支援サービス　など

付録 A　用語集

CSIRT (Computer Security Incident Response Team)
インシデントが発生した際に対応するチームのこと。脆弱性情報などの収集と分析、インシデント発生時の対応、社内外の組織との情報共有や連携などを行う。インシデント発生時に結成されるチームの場合もある。

IoT (Internet of Things)
「様々な物がインターネットにつながること」または「インターネットにつながる様々な物」を指しており、警備ロボット等がビルシステムにつながることが考えられる。

SOC (Security Operation Center)
サイバー攻撃の検知や分析を行い、その対策を講じることなどを専門とする組織。24 時間体制での対応が求められるため、外部委託するケースもある。

インシデント（サイバーインシデント／セキュリティインシデント）
望まない単独若しくは一連のセキュリティ事象、又は予期しない単独若しくは一連のセキュリティ事象であって、事業運営を危うくする確率及びセキュリティを脅かす確率が高いもの。

インシデントレスポンス（インシデント対応）
インシデント発生時に、インシデントによる損害を最小限に抑え、復旧にかかる時間とコストを削減すること等を目的とした対応を行うこと。

サイバー攻撃(Cyber Attack)
資産の破壊、暴露、改ざん、無効化、盗用、又は認可されていないアクセス若しくは使用の試み。[JIS Q 27000：2014]

機密性（Confidentiality）
認可されていない個人，エンティティ又はプロセスに対して，情報を使用させず，また，開示しない特性。[JIS Q 27000：2014]

完全性（Integrity）
正確さ及び完全さの特性。[JIS Q 27000：2014]

可用性（Availability）

認可されたエンティティが要求したときに，アクセス及び使用が可能である特性。[JIS Q 27000：2014]

ステークホルダ

意思決定若しくは活動に影響を与え、影響されることがある又は影響されると認知している、あらゆる人又は組織。 [JIS Q 27000：2014]

脆弱性

１つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点。 [JIS Q 27000：2014]

ビルシステム

ビルの管理・運用を行うための制御システムで、受変電、熱供給、空調、給排水、照明、昇降機、防犯、防災、監視カメラ等の各設備の制御システムの総称。

マルウェア(Malware)

許可されていないプロセスの実施を試みることによって、情報システムの機密性・完全性・可用性に悪影響をもたらすソフトウェア又はファームウェア。[NIST SP 800-53 rev.4]
セキュリティ上の被害を及ぼすウィルス、スパイウエア、ボット等の悪意を持ったプログラムを指す総称。

付録 B　参考文献

「建物設備システム リファレンスガイド　インシデント対応・セキュリティソリューション編」
特定非営利活動法人日本データセンター協会
データセンターにおけるインシデントレスポンスに係るガイドブック
（一般には非公開）

「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」
産業サイバーセキュリティ研究会　ワーキンググループ 1(制度・技術・標準化)　ビルサブワーキンググループ
ビルシステムにおけるサイバーセキュリティの確保のためのガイドブック
https://www.meti.go.jp/policy/netsecurity/wg1/20190617005_01.pdf