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
（β版・差し替え版）

平成３０年１０月３１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

目次

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（β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、これまでは制御系がインターネットと切り離されていることや、ビル特有のプロトコルを使っているため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ーであり、システム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を対象としたサイバー攻撃が起きている。

- 一方で、ビルの特徴としてステークホルダーが多数存在しており、これらの関係するステークホルダーが参照できるセキュリティ対策のガイドラインが存在しておらず、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、平成３０年２月、産業サイバーセキュリティ研究会 WG1 の下に、ビルに関わる多数のステークホルダーが一堂に会し、それぞれの視点も考慮したビル向けの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、検討を進めてきた。

- 本ガイドライン（β版）は、これまで、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、各事業者等の具体的な意見を聞きながら、より具体的に実装に活用できる内容にしていくとともに、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、関連する国際規格や他の産業と比較して漏れている対策がないかなど、検討を進めていく。

１．はじめに

１．１．目的及び適用範囲

本ガイドラインの目的は、ビルシステムのセキュリティを確保するためのガイダンスを示すことであり、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る。本ガイドラインでは、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。

１．２．対象者

本ガイドラインは上述のとおり、ビルシステムを構成する全てのサブシステムにおける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ーはもちろんのこと、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なども対象としている。

具体的な対象者は以下のとおり。

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、エレベーター、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、自治体、関係省庁　等

また、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、施設等の区分を行うことが可能である。これらそれぞれの状況に応じて、適用出来るサイバーセキュリティ対策は異なっており、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。このように様々な条件の異なるビルについても、なるべく広範囲に対象とすることとしている。

１．３．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

本書執筆時点で作成段階であるサイバー・フィジカル・セキュリティ対策フレームワークについては、本ガイドラインの内容の更なる具体化等を進めていく際のリファレンスとして、３層の考え方や各対策を取り入れていくこととしている。

１．４．文書の構成

本ガイドラインのこれ以降の部分は、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:ライフサイクルやビルの条件それぞれに応じた本ガイドラインを活用の仕方について示す。

また、本ガイドには、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 のリファレンスガイドとの関係

■付録 C: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 D:参考文献

■付録 E:ビルシステムのサイバーセキュリティ対策の具体例集(リポジトリ)

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、エレベーター、防災等の個別の設備毎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非 IP（Internet Protcol）の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。

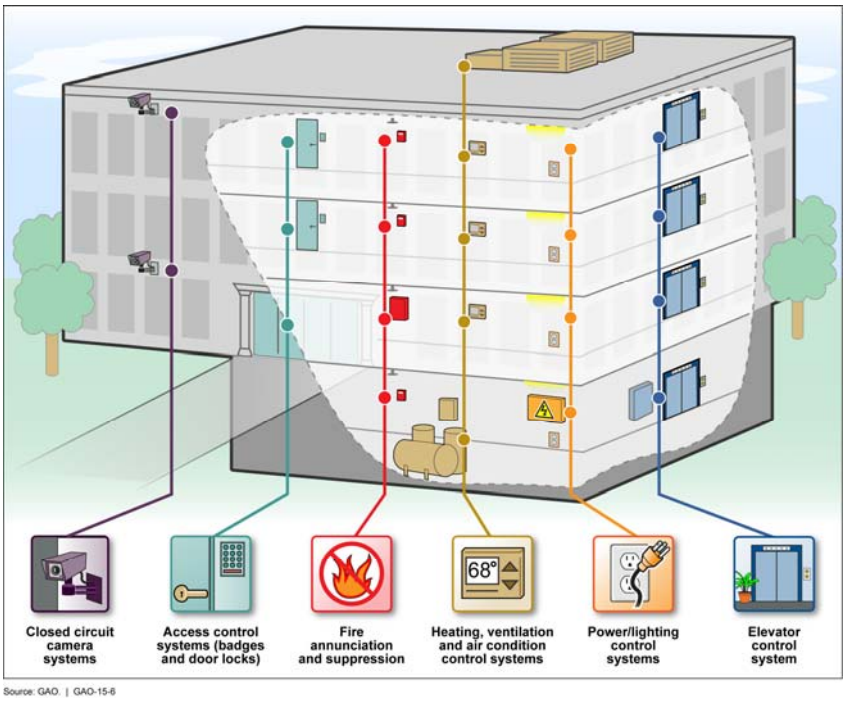


図　ビルの設備制御システムの概略例（各システムが独立専用システム）
（出典：FEDERAL FACILITY CYBERSECURITY, DHS and GSA Should Address Cyber Risk to Building and Access Control Systems (2014/12, 米国 GAO)）

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、末端のセンサー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。

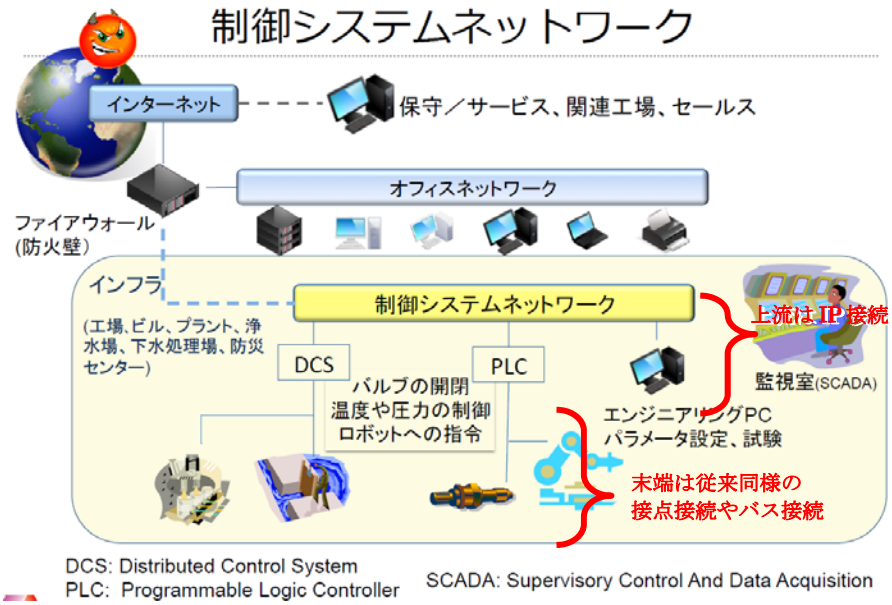


図　つながる制御システムネットワーク

（出典:制御システムセキュリティの脅威と対策の動向および 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毎のシステムを相互に接続し、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する例も増えてきている。

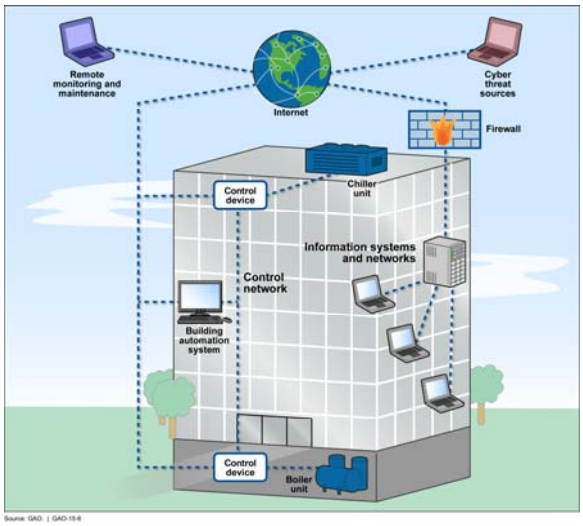


図　空調等をインターネット経由で遠隔から管理する例

（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 WindowsOS 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。

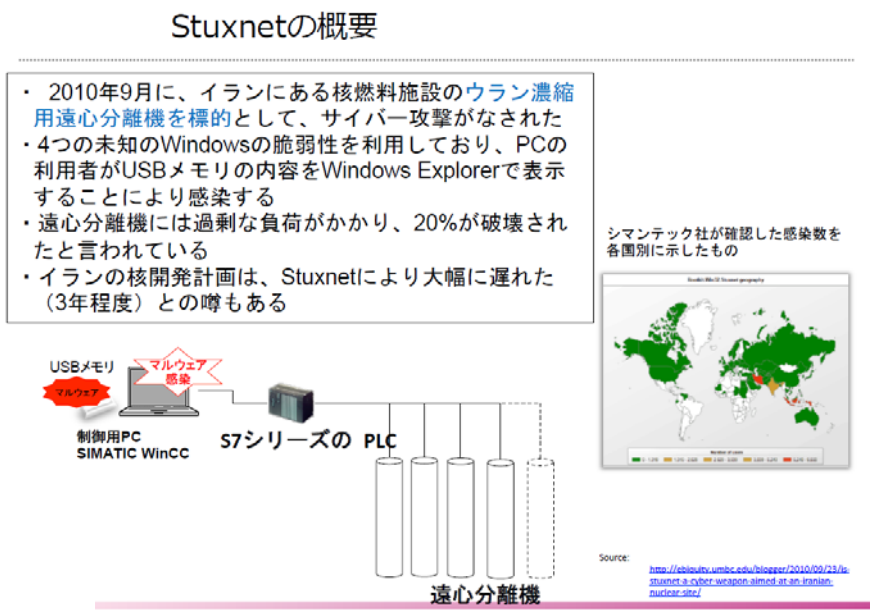


図　制御システムへの世界初の攻撃といわれる Stuxnet による攻撃
（出典：制御システムセキュリティの脅威と対策の動向および CSSC の研究概要について（2018/5/11，技術研究組合制御システムセキュリティセンター））

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。

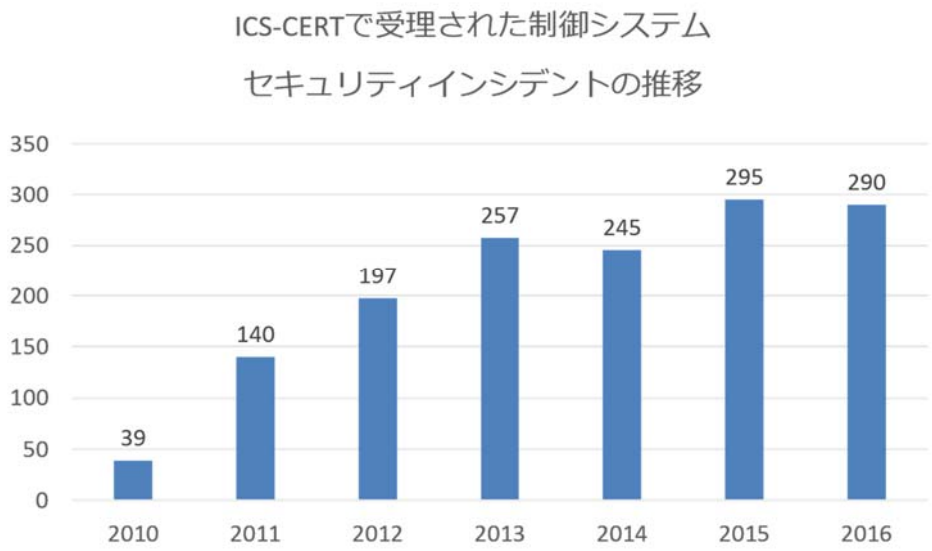


図　制御システムを狙った攻撃の増加

（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。

①　MIT[1]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

[1] Massachusetts Institute of Technology（マサチューセッツ工科大学）の略称。

撃も可能であることを示している。

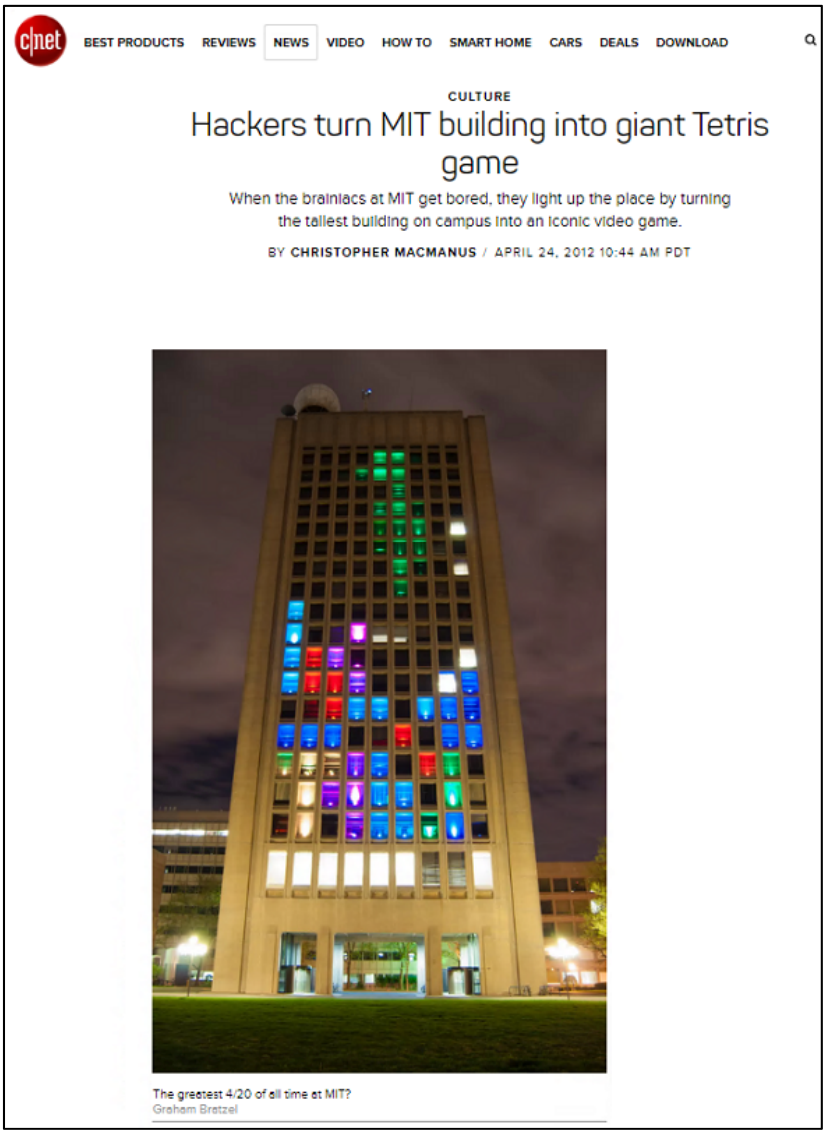


図　事件を報道する記事（https://www.cnet.com/news/hackers-turn-mit-building-into-giant-tetris-game/）

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され、収容房の扉がリモート解除されて、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、大変に大きな問題だと言える。

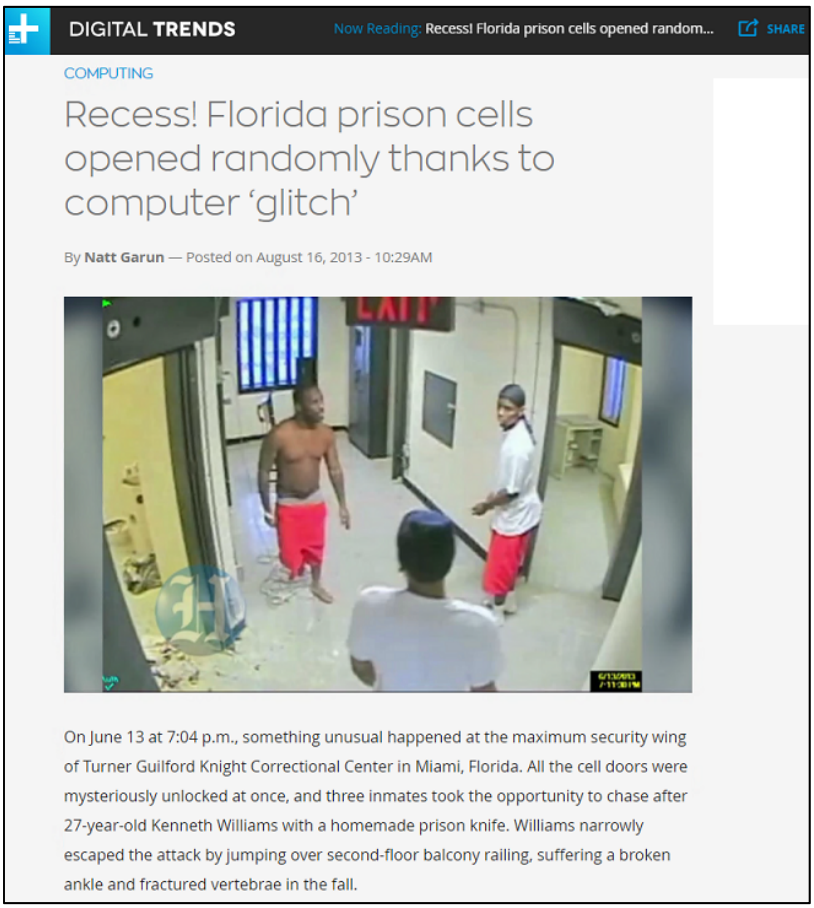


図　事件の関連情報について報道する記事

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

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、数時間に渡って暖房が利用出来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。

DDoS攻撃でビルの暖房が使えなくなり凍死寸前!?

2016年12月23日 09時00分更新

文● せさゅフポ

Photo by degnyg

我々の生活を便利にしてくれるはずのIoTが、犯罪の標的になってしまったことで、文字通り"震える"事態となった――。

2016年11月、フィンランド南東部の南カルヤラ県にある都市・ラッペーンランタの2棟のビルで、事件は起きた。このビルではコンピューターで空調や水道の温度を管理していたのだが、DDoS攻撃の被害に遭い、暖房が停止してしまったのだ。

さいわい、ネットワークトラフィックを制限するなどの攻撃に対応できたとのことだが、11月のフィンランド（ヘルシンキ）は、平均最低気温はマイナス2度。これでは仕事にならないどころか、ビルを利用する人にとっては健康の被害さえ考えられる。

IoTデバイスは年々リリースされ続けているが、一方で専門家や公的機関から、犯罪の被害に遭う危険性も指摘されている。消費者向けのIoTだけでなく、電気や水道など重要なインフラもインターネット経由で動作するケースが増えてきている。インフラにかかわる機器が悪意をもってハッキングされれば、地域一帯に被害が出る可能性もあるだろう。

図　事件を報道する記事（http://ascii.jp/elem/000/001/405/1405563/）

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、ランサムウエ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しではない。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　事件を報道する記事（https://edition.cnn.com/2017/01/30/europe/hackers-lock-out-hotel-guests-trnd/index.html）

⑤　インターネットカメラへの大量ハッキング

日本においてつい最近発生した事例であり、報道で見聞きしている人も多いと思われる。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出来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。

⑥　その他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際され、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出来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。

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．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、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しておくことは重要である。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 件 1 件まるで異なっているように、ビルシステムもまた、1 件 1 件それぞれ異なっており、1つとして同じ物は存在しない。ただし、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。

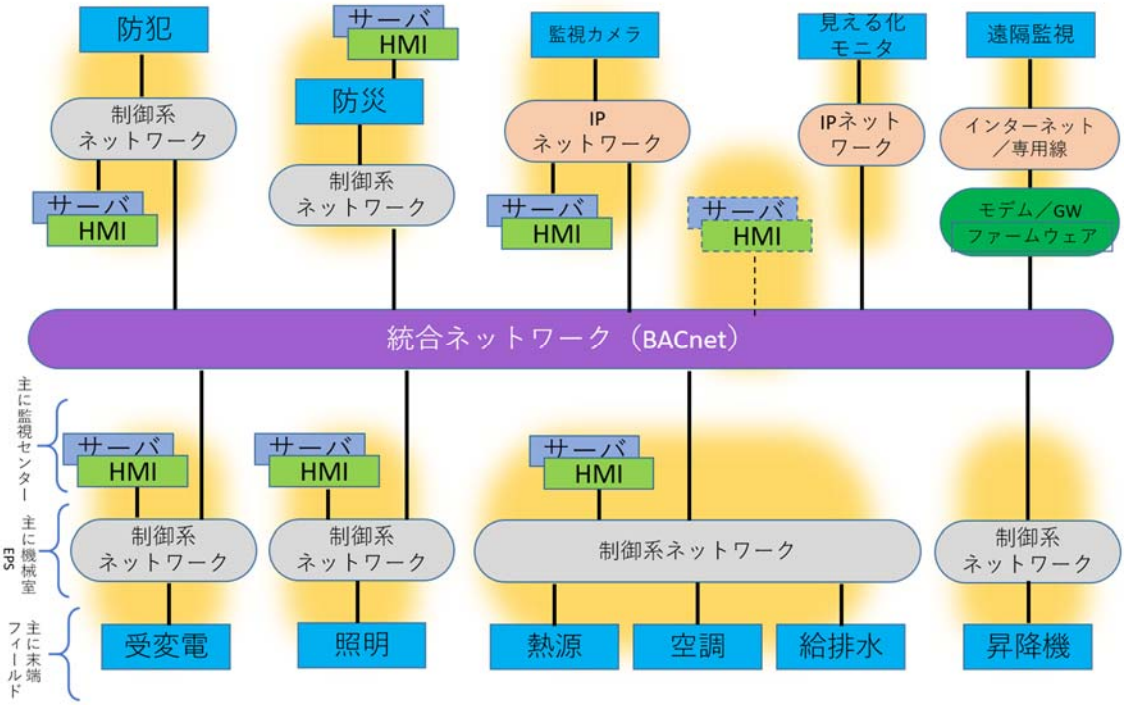


図　ビルシステムの標準的なモデル（全体像）

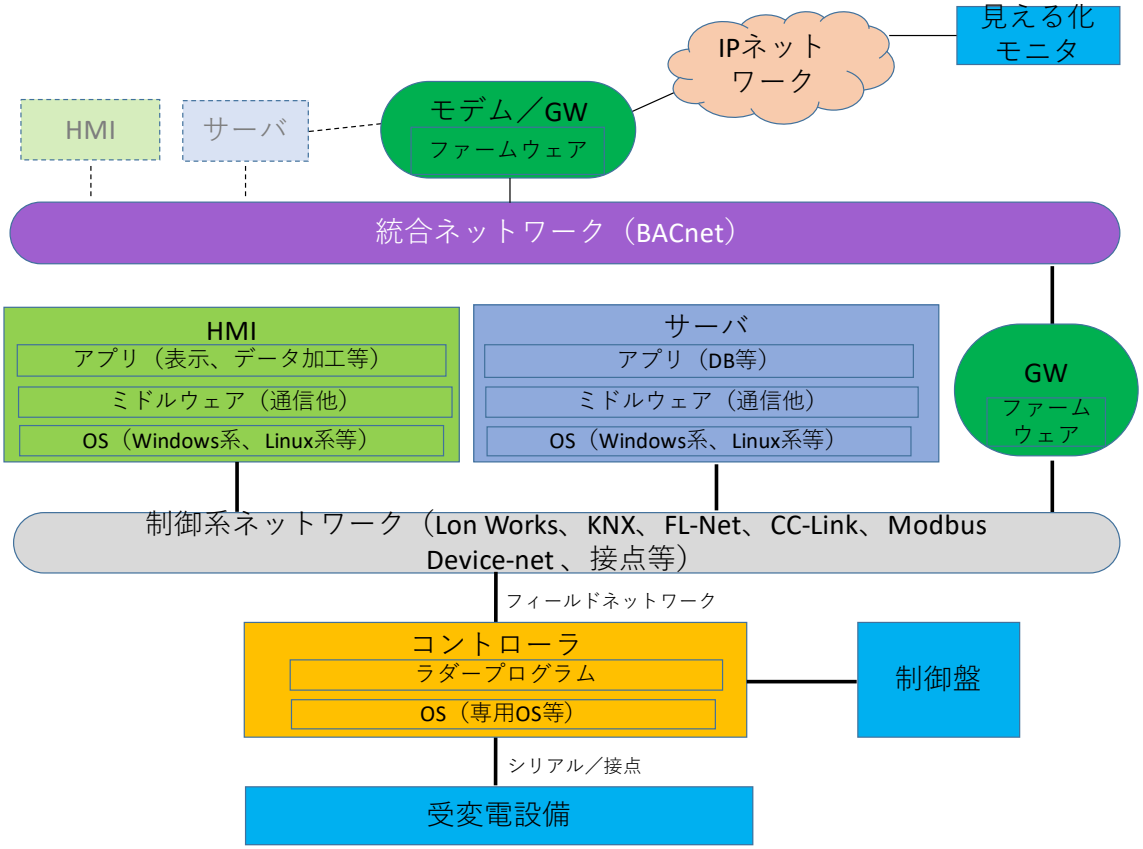


図　受変電システムの標準的なモデル

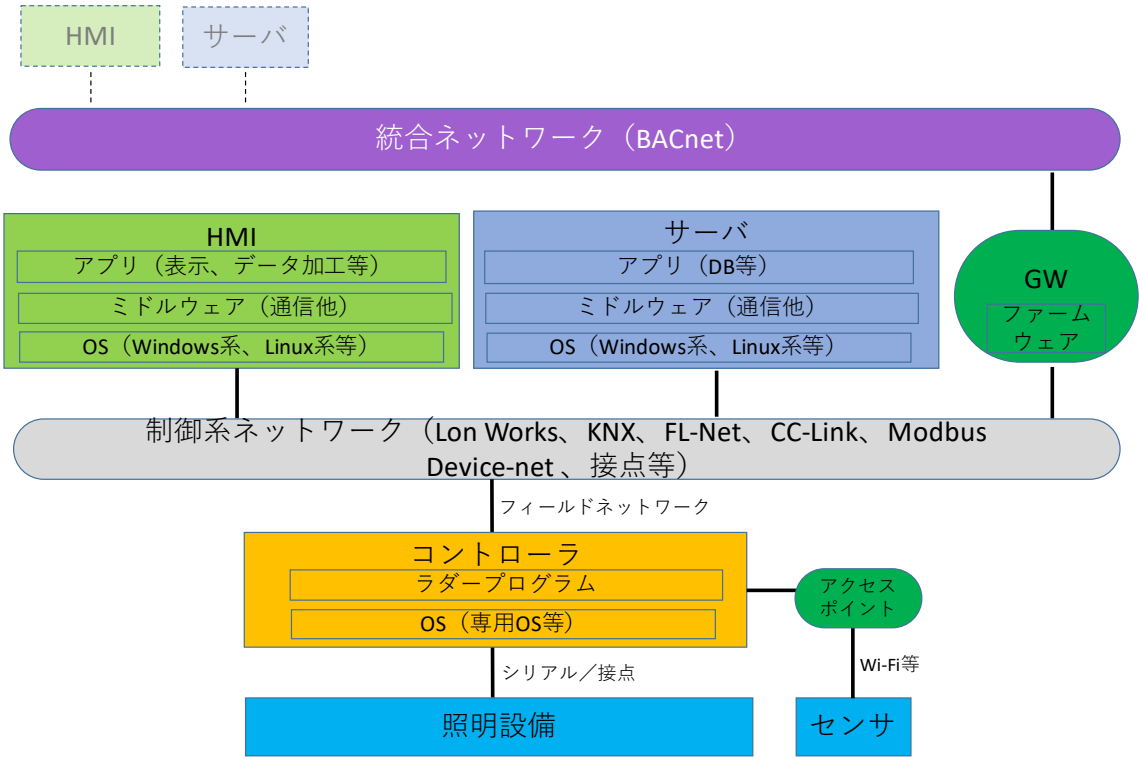


図　照明システムの標準的なモデル

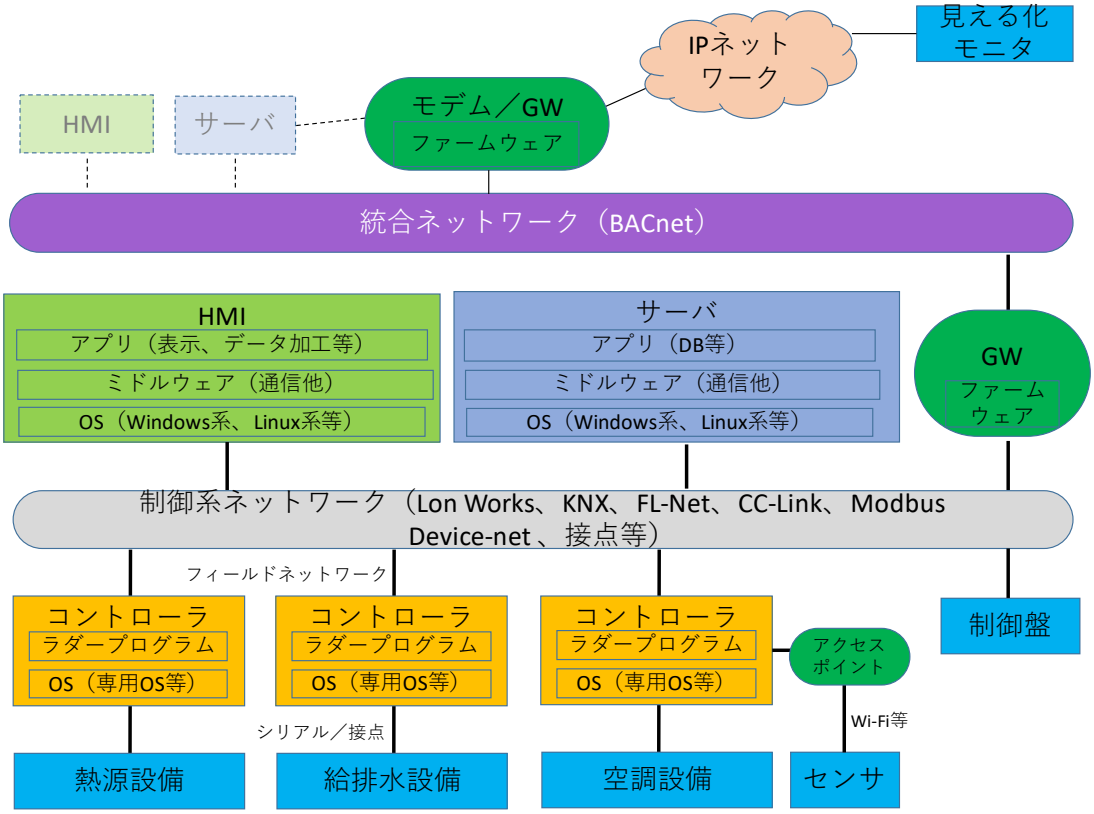


図　熱源・空調・給排水システムの標準的なモデル

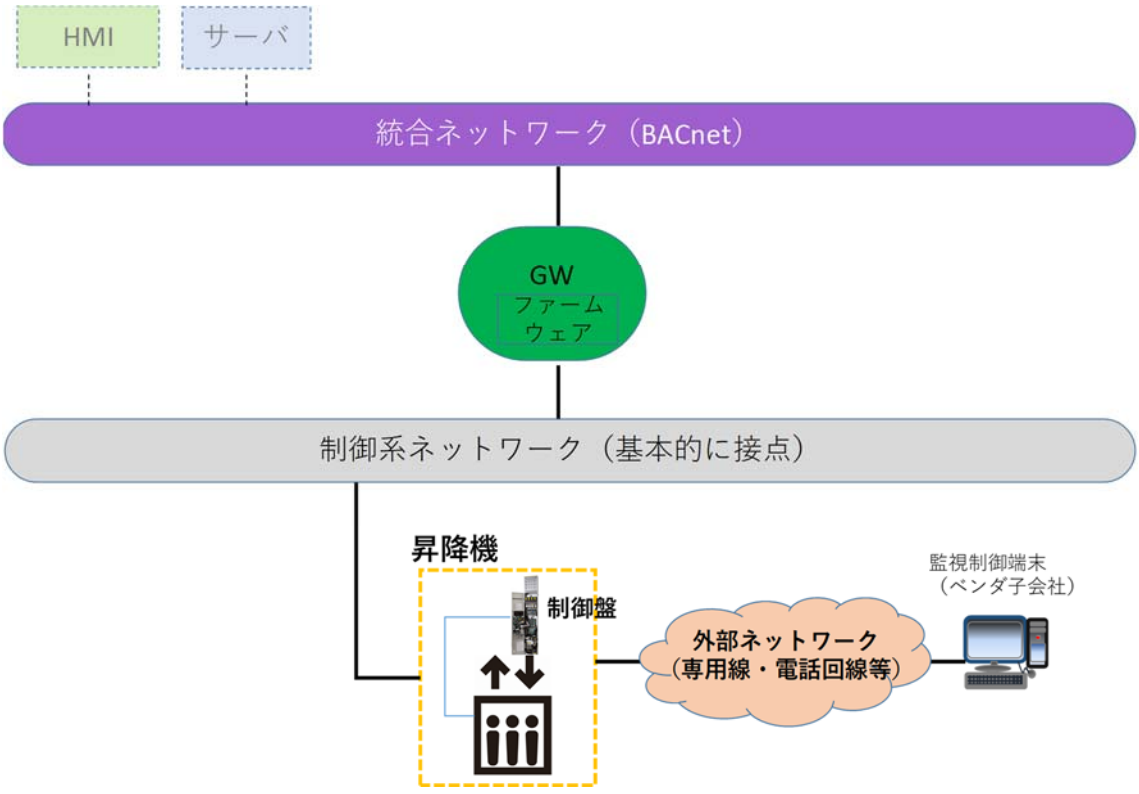


図　昇降機システムの標準的なモデル

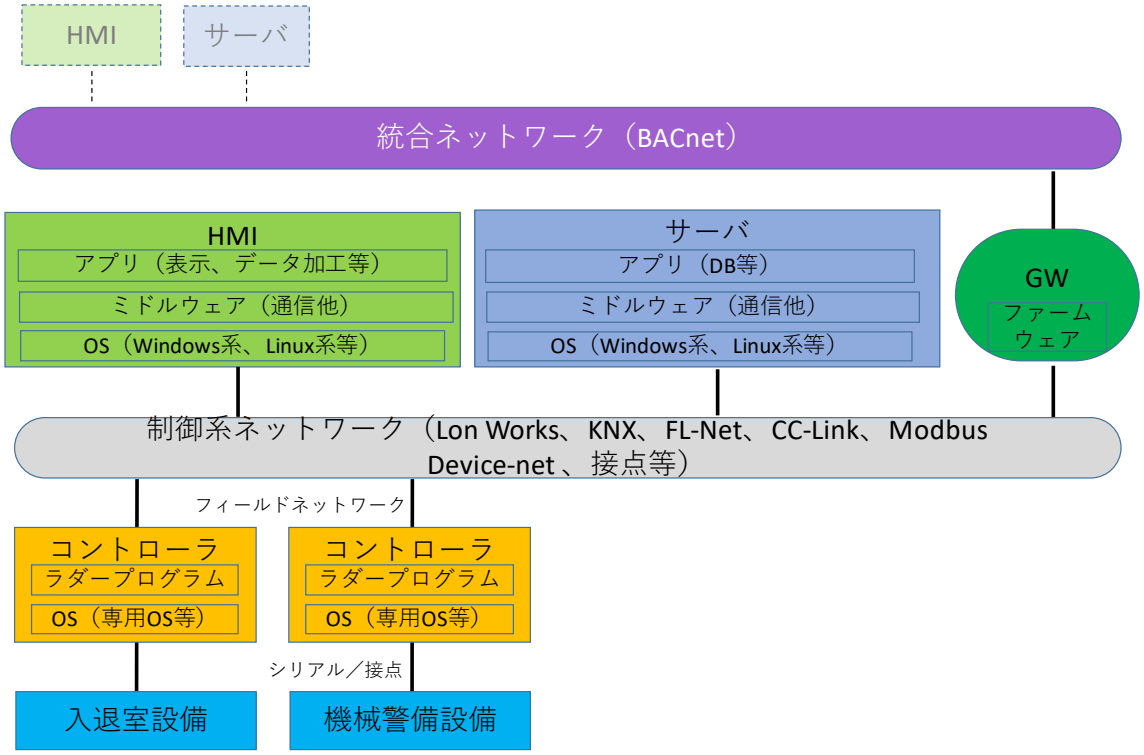


図　防犯システムの標準的なモデル

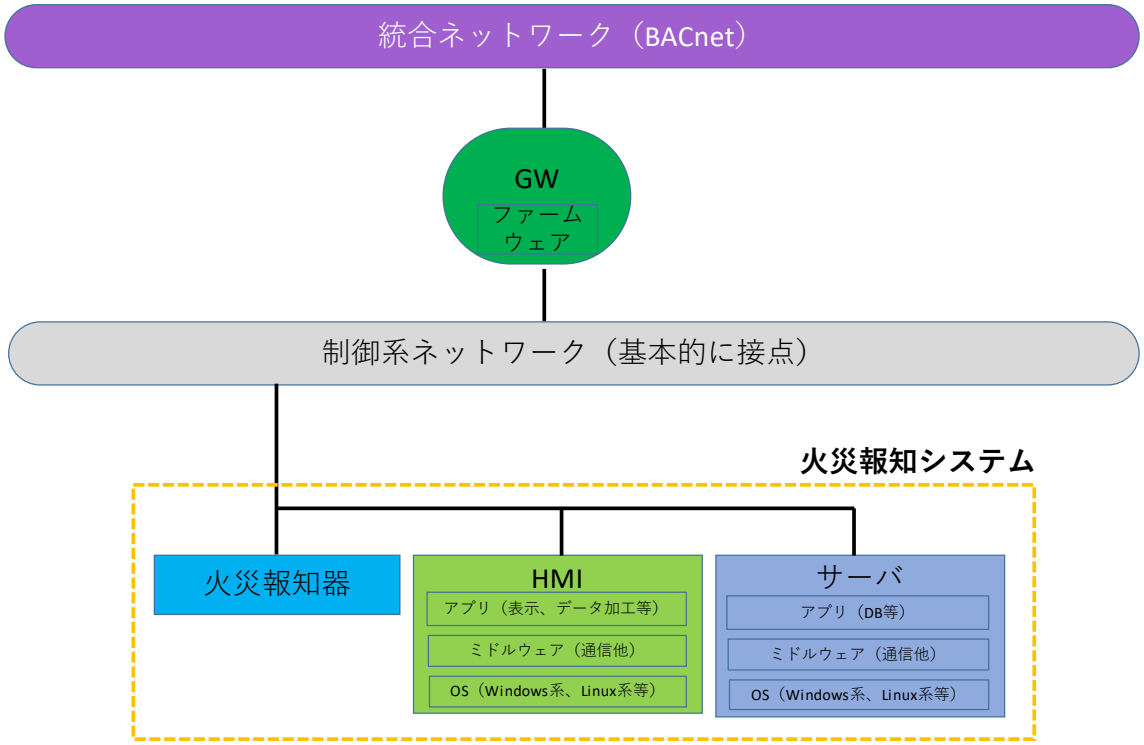


図　防災システムの標準的なモデル

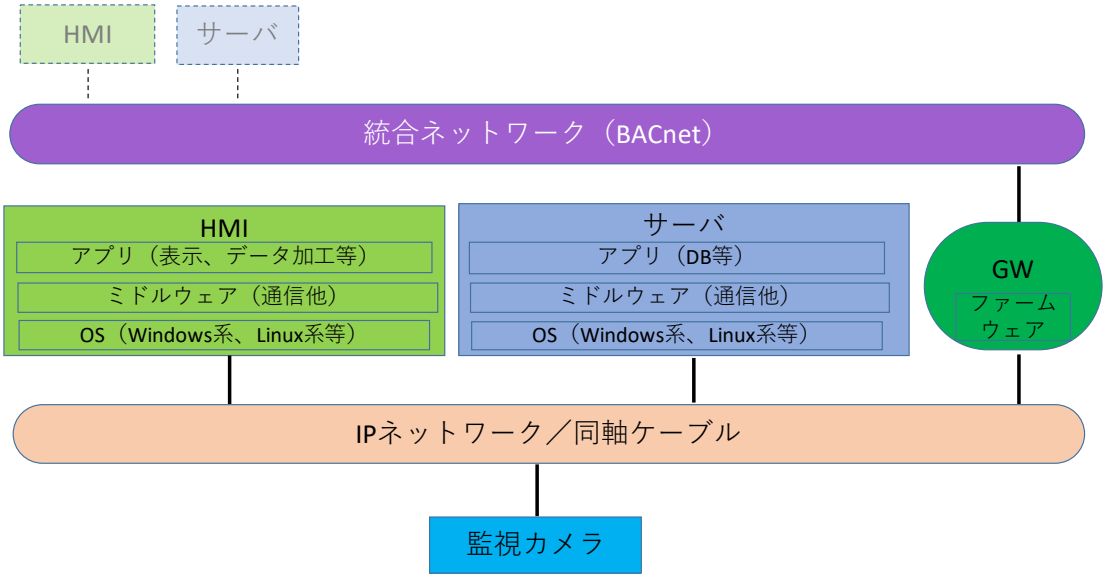


図　監視カメラシステムの標準的なモデル

３．２．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出来る。

①　超長期の運用

ビルは建設後、50 年近くに渡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 年近くに渡って運用することが普通であり、システムの更新に当たっても、その時点の理想的なシステムを導入出来るわけではなく、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、長期に渡ってアップデートの出来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。

②　複数の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をどのように防ぐか物理的対策とシステム的対策の両面で考える必要がある。

図　ビルのライフサイクルを意識した対策が必要

③　マルチステークホルダーであること

ビルやそのシステムに係わるステークホルダーも多種である。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、さらに設計事業者、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、それ毎に異なるベンダが係わることになる。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、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出てくる。

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。

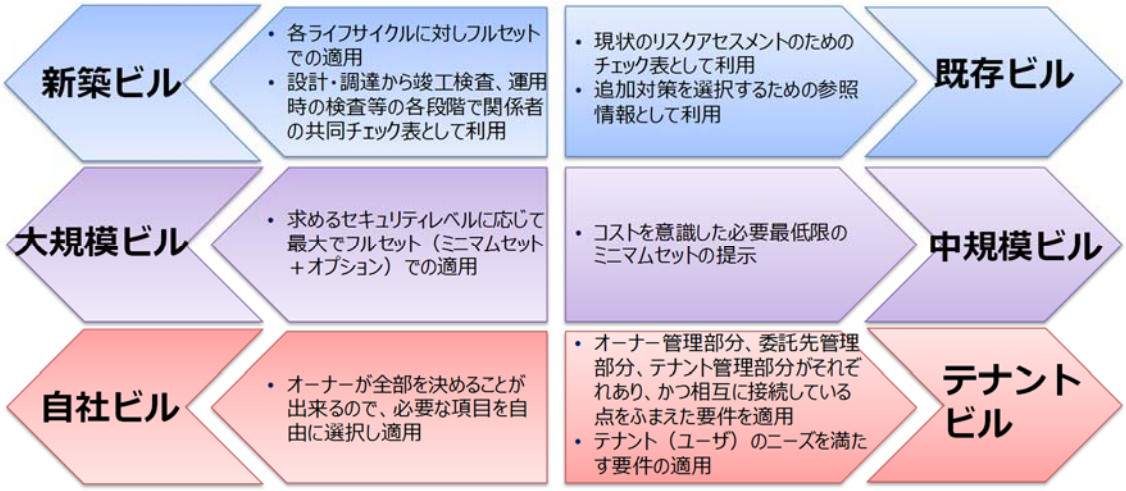


図　ビルの多様性を意識した対策が必要

３．３．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、さら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、各ステークホルダー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。

さらに設備毎、設備を構成する機器毎、機器が置かれた場所毎のリスクを確認し、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出来ることを意図したものでもある。

(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出来れば効率的である。ただしこの場合には、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、場所毎に似たような機器が置かれることになるため、場所や機器毎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出来る。

そこで、本ガイドでは、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。

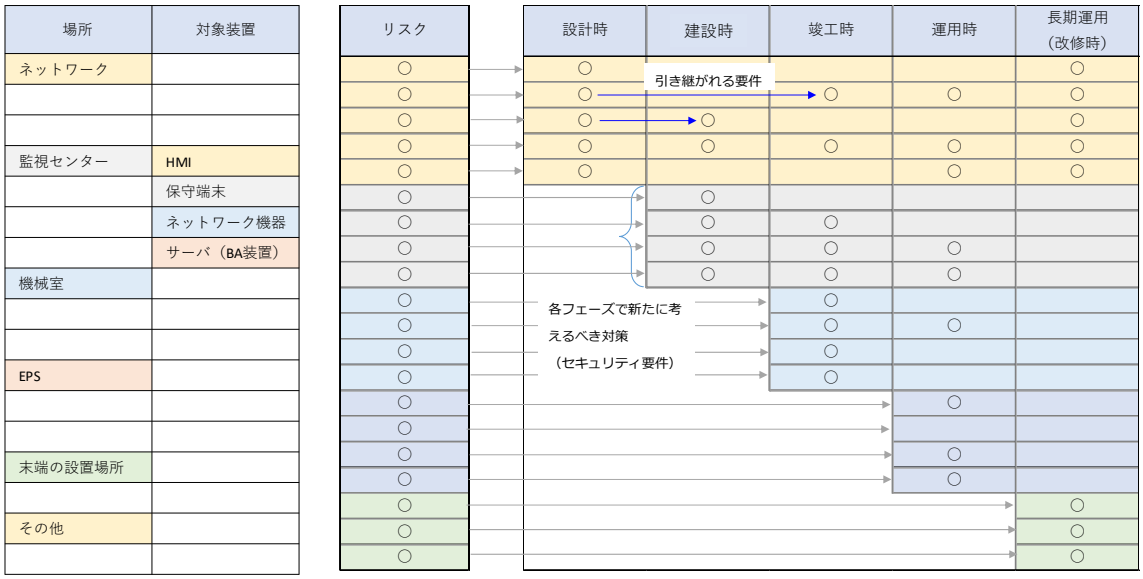


図　場所からみたサイバーセキュリティリスクとライフサイクルをまたがって適用するべき対策

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次章に整理する。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次々章別紙として掲載する。また、個々の対策については、その次の章で詳細に解説を行う。

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

	脅威	リスク要因	セキュリティポリシー
1. 構成情報／管理情報			
(1)	システムの構成情報が最新になっておらず、機器の接続関係等が把握できないため、被害の確認や復旧のための作業の支障となる。	最新の構成情報の管理が出来ていない。	・構築システム構成図（設計時）に対し、引き渡し時のシステム構成図を竣工引き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)	システムのバックアップ等が適切に取得・管理されておらず、被害時の復旧のための作業の支障となる。	定期的なバックアップが取られていない。	・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、定期的にバックアップを取得する機能を具備する。
(2)	脆弱性情報等を定期的にチェックしていない。必要な対応措置を事前にとっていないために、脆弱性を突いた攻撃にあう可能性がある。	適切なアップデート／パッチ適用がなされていない。またはそれに代わる対策が取られていない。	・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。 ・ただし他機器および他システムとの接続性については、担保しなければならない。
3. 会社／要員の管理			
(1)	ビル管理会社においてセキュリティ意識が醸成されておらず、事前のセキュリティ対策が十分に取られず、攻撃を受けた際の対応も遅れる可能性がある。	ビル管理会社のセキュリティ意識が低い。	・システム構築要件に教育訓練について明記する。
(2)	作業員に内部攻撃者が紛れることを防げず、内部からの攻撃を受ける可能性がある。	作業員の身元管理や行動確認が出来ていない。	・システムの構築・施工に関する要件を明記する。
4. 体制構築等			
(1)	リスク対応体制が十分なレベルで構築されておらず、攻撃等への対応が効果的に実施出	リスク対策の運用計画や体制が十分なアセスメントに基づいていな	・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

	来ない可能性がある。	い。	管理体系」などを事業計画として定義・整備する。
(2)	設計・構築において、技術者のセキュリティへの知識が不足しており、十分にセキュアなシステムを構築出来ない。	十分なセキュリティ知識と技術をもった設計者が設計をしていない。	・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)	作業員のセキュリティ教育が十分でなく、初期対応等に遅れが生じる。	作業員１人１人のセキュリティ意識が低い。	・入場前に適切にセキュリティ対策を実施する。
(4)	十分なセキュリティ管理体制を構築できておらず、セキュリティを十分に担保した運用が出来ていない。	セキュリティ意識の高い運用体制を組織出来ていない。	・設計要件・運用要件を明記する。
(5)	インシデント対応手順が運用基準の中で整備されておらず、初期対応等に遅れが生じる。	緊急時の対応手順が整備されていない。	・緊急時の対応手順要件について明記する。
(6)	システム運用状況の確認、管理が行われておらず、不正なアクセスや通信の発生、操作等を見逃す可能性がある。	システムの運用監視が十分でない。	・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・セキュリティー関連教育を含む・教育場所を明記）

４．２．機器ごとの管理策

	脅威	リスク要因	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)			
10	ネットワーク		
(1)	ビル内のネットワークがセキュリティポリシーに基づいて分離されておらず、マルウェア感染拡大の可能性がある。	ネットワークを介して伝搬するマルウェアへの感染を想定した感染拡大防止対策が出来ていない。	・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または論理的に分離する。
(2)	ビル内のネットワークにおいて、不要な通信が許容されることにより、広範囲なマルウェア拡散や活動の可能性がある。	ネットワークを介して伝搬するマルウェアへの感染や RAT(Remote Access Tool)等による不正侵入を想定した防止対策ができていない。	・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)	ビル内のネットワークにおいて、不必要もしくは管理されていない外部ネットワーク接続を介してマルウェア感染や不正侵入を受ける可能性がある。	外部からのネットワークを介したビル内システムへの不正侵入やマルウェア感染を想定した防止対策が十分でない。	・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 FW 等により必要最小限に制限する。

	(4)	ビル内に外部接続回線が不正に引き込まれ、ビル内ネットワークへの不正接続や盗聴・盗撮等の攻撃に用いられる可能性がある。	ビルに引き込まれる外部接続回線の管理が十分でない。	・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)	外部ネットワークとの接続があり、情報を遣り取りする通信があるため、その通信を偽装して外部からの侵入を受ける可能性がある。	外部との接続を持つシステムにおいて、システムの脆弱性チェックや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)	ビルシステムの制御を行うためのインターネット公開システム(Web サーバ)に脆弱性が存在した場合、外部から不正操作等の攻撃を受ける可能性がある。	インターネット公開システムが用いるソフトウェアに重大な脆弱性が発覚した場合の緊急対応に時間を要する。	・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。
12	情報系端末			
	(1)	BA システムと外部システムの接続に当たって十分なセキュリティ確保が行われず、攻撃を受けたり、侵入、乗っ取りを受ける可能性がある。	外部との接続を持つシステムにおいて、システムの脆弱性チェックや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。
13	外部接続用ネットワーク機器(FW、ルータ)			
	(1)	外部接続を前提としたシステムとしての十分な脆弱性の確認が行われず、脆弱性が放置されたままの状態のため、攻撃を受けたり、侵入、乗っ取りを受ける可能性がある。	外部との接続を持つシステムにおいて、システムの脆弱性チェックや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	BA システム間相互接続(BACnet 等)			
	(1)	他の設備システムとBACnet を介した相互接続があり、ある設備への侵入が発生すると別の設備に拡大する恐れがある	BACnet による設備システム間の相互接続において、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出口対策を施す。
2. 監視センター(中央制御室)				
20	監視センター			
	(1)	重要情報や BA システムの設置・保管場所に、許可を受けた者以外の入室を許してしまい、システム画面の盗み見、	監視センター(中央制御室)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いない。	・監視センター(中央制御室)の入場者を登録(事前、都度)して管理する仕組みを入れる。

		端末／制御盤への不用意な操作をされる恐れがある。		・監視センター（中央制御室）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)	重要情報や BA システムの設置・保管場所において、作業員（運用員、保守要員）の権限を越えて、システムや端末／制御盤に対して不審な操作をされる恐れがある。	監視センター（中央制御室）に対して、作業員が許可された以外の作業をすることを防げない。またその作業によって、実際にシステムや端末が操作できてしまうことを防げない。	・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)	いつ、どのような経路で感染したのか分からない。竣工前に感染した可能性を排除できない。	いつの間にか感染しており、感染原因等がすぐに分からない。	・ウィルスチェック済みの機器を納入する。 ・（ネットワークや端末の動作など）各種ログ情報の導入とログ解析の仕組みを導入する。
21	HMI/HIM			
	(1)	正規の作業員以外が容易にシステムにログインでき、不正な操作をされる可能性が高い。	ID/PW が容易に入手／類推でき、許可された作業員以外による作業を防げない。	・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)	操作権限のレベル設定がなく、どの作業員でもあらゆる操作が可能で、不正な設定や操作をされる可能性がある。	作業員が許可された以外の作業をすることを防げない。またその作業によって、実際にシステムや端末が操作できてしまうことを防げない。	・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)	アクセスログが適切に管理されておらず、侵入者にシステムの情報を与えてしまったり、逆に侵入状況の解析を困難にする可能性がある。	ログ管理が不適切で、侵入者に次の攻撃のヒントを容易にあたえてしまう。	・アクセスログ、操作履歴を適切に管理する。
			ログ管理が不適切で、感染原因、感染経路等がすぐに分からない。	・各種ログ情報の導入とログ解析の仕組みを導入する。
	(4)	システム運用状況の確認、管理が行われておらず、不正なアクセスや通信の発生、操作等を見逃す可能性がある。	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。
	(5)	いつ、どのような経路で感染したのか分からない。竣工前に感染した可能性を排除できない。	いつの間にか感染しており、感染原因等がすぐに分からない。	・工場出荷前および引渡し前に事前検疫を実施する。
	(6)	システム内部のプログラム等が容易に探られ、操作される可能性がある。	システムの内部構成が単純または権限管理できておらず、容易に全体を探られてしまう。	・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。

	(7)	システムとしての脆弱性の確認が行われず、脆弱性が放置されたままの状態のため、攻撃を受けたり、侵入、乗っ取りを受ける可能性がある。	適切なアップデート／パッチ適用がなされていない。	・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。
	(8)	USB 等の外部媒体を接続することで、外部媒体経由でマルウェア等の侵入を許してしまう可能性がある。	セキュリティ確認がされていない USB 等の外部媒体や持込端末が容易に接続可能となっている。	・外部媒体等を簡単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)	メンテナンス用の持込端末をネットワークに接続することで、マルウェア等の侵入を許してしまう可能性がある。	保守用端末や外部媒体がパッチ管理やウィルス検疫されていない。	・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（FW、ルータ、SW）			
	(1)	ネットワークにつながるネットワーク機器（スイッチ等）の空きポートに不正端末を接続され、マルウェア等を送り込まれる可能性がある。	スイッチ等の空きポートに不正端末が容易に接続可能となっている（物理的、電気的）。	・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（BA 主装置）			
	(1)	システム管理用サーバ（BA 主装置）が専用区画に設置されておらず、作業員以外が容易に触れられる可能性がある。	許可された作業員以外が装置に容易に接触可能で、不正な作業をすることを防げない。	・適切に管理された専用の室、区画の中に機器を設置する。 ・サーバ類は容易に許可された作業員以外が触れないようにする。
	(2)	サーバの設置区画への入退室が適切に管理されておらず、作業員以外が容易に区画に侵入し、サーバに触れられる可能性がある。	許可された作業員以外が装置に容易に接触可能で、不正な作業をすることを防げない。	・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)	アクセスログが適切に管理されておらず、侵入者にシステムの情報を与えてしまったり、逆に侵入状況の解析を困難にする可能性がある。	ログ管理が不適切で、侵入者に次の攻撃のヒントを容易にあたえてしまう。	・アクセスログを記録する機能を入れる。
			ログ管理が不適切で、感染原因、感染経路等がすぐに分からない。	・各種ログ情報の導入とログ解析の仕組みを導入する。
	(4)	システム運用状況の確認、管理が行われておらず、不正なアクセスや通信の発生、操作等を見逃す可能性がある。	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。

	(5)	通信プロトコル等に相手先認証機能がないため、不正な命令信号を送られても実行してしまう可能性がある。	相手認証無く命令を実行する仕組みとなっている。	・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。
	(6)	いつ、どのような経路で感染したのか分からない。竣工前に感染した可能性を排除できない。	いつの間にか感染しており、感染原因等がすぐに分からない。	・工場出荷前および引渡し前に事前検疫を実施する。
	(7)	システム内部のプログラム等が容易に探られ、操作される可能性がある。	システムの内部構成が単純または権限管理できておらず、容易に全体を探られてしまう。	・工場出荷前および引渡し前に事前検疫を実施する。
	(8)	システムとしての脆弱性の確認が行われず、脆弱性が放置されたままの状態のため、攻撃を受けたり、侵入、乗っ取りを受ける可能性がある。	適切なアップデート／パッチ適用がなされていない。	・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。
	(9)	メンテナンスのために USB 等の外部媒体を接続することで、外部媒体経由でマルウェア等の侵入を許してしまう可能性がある。	セキュリティ確認がされていない USB 等の外部媒体や持込端末が容易に接続可能となっている。	・外部媒体等を簡単安易に利用できないようにする。
3.機械室／制御盤ボックス				
30	機械室			
	(1)	重要情報や BA システムの設置・保管場所に、許可を受けた者以外の入室を許してしまい、端末／制御盤への不用意な操作をされる恐れがある。	許可された入退室に限定するような管理ができていない。	・機械室は施錠可能とする。
31	コントローラ（DCM、PLC 等）			
	(1)	操作ログが適切に管理されておらず、侵入者にシステムの情報を与えてしまったり、逆に侵入状況の解析を困難にする可能性がある。	ログ管理が不適切で、侵入者に次の攻撃のヒントを容易にあたえてしまう。	・ログを適切に管理可能な機器・システムを導入する。
			ログ管理が不適切で、感染原因、感染経路等がすぐに分からない。	・各種ログ情報の導入とログ解析の仕組みを導入する。
	(2)	システム運用状況の確認、管理が行われておらず、不正なアクセスや通信の発生、操作等を見逃す可能性がある。	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。

	(3)	通信プロトコル等に相手先認証機能がないため、不正な命令信号を送られても実行してしまう可能性がある。	相手認証無く命令を実行する仕組みとなっている。	・不正な機器が繋がれないように物理的セキュリティの対策を強化する。
	(4)	いつ、どのような経路で感染したのか分からない。竣工前に感染した可能性を排除できない。	いつの間にか感染しており、感染原因等がすぐに分からない。	・ウィルスチェック済みの機器を納入する。
	(5)	ID・パスワードが適切に設定されておらず、システム内への侵入者に容易にアクセスされ、不正操作をおこなわれる可能性がある。	設備設置時に適切な ID・パスワードの設定作業が行われていない。	・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。
	(6)	システムとしての脆弱性の確認が行われず、脆弱性が放置されたままの状態のため、攻撃を受けたり、侵入、乗っ取りを受ける可能性がある。	適切なアップデート／パッチ適用がなされていない。	・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。
	(7)	メンテナンスのために USB 等の外部媒体を接続することで、外部媒体経由でマルウェア等の侵入を許してしまう可能性がある。	セキュリティ確認がされていない USB 等の外部媒体や持込端末を容易に接続可能となっている。	・不要な USB ポート・イーサネットポートは使用できないようにする。
32	ネットワーク機器（FW、ルータ、SW）			
	(1)	ネットワークにつながるネットワーク機器（スイッチ等）の空きポートに不正端末を接続され、マルウェア等を送り込まれる可能性がある。	スイッチ等の空きポートに不正端末が容易に接続可能となっている（物理的、電気的）。	・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)	通信プロトコル等に相手先認証機能がないため、不正な命令信号を送られても実行してしまう可能性がある。	相手認証無く命令を実行する仕組みとなっている。	・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)	係員以外の立入が制限された区画内に部外者の侵入を許してしまい、制御盤内のシステムに対しての不用意な操作をおこなわれたり、悪意のある機器を取り付けられる可能性がある。	制御盤・分電盤が業界で広く通用する鍵のみで開いてしまう。	・各種制御盤の鍵は、他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)	配線等がむき出しの状態で置かれ、ま	スイッチ等の空きポートに不正端末	・BA 主装置以降の配線については、

		ったく保護されれておらず、誰でもが触れたり、不正機器を取り付けたりすることが可能である。	が容易に接続可能となっている(物理的、電気的)。	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(SW 類)			
	(1)	機器類が安全な場所に設置・管理されておらず、作業員以外が容易に機器類に触れられる可能性がある。	許可された作業員以外が装置に容易に接触可能で、不正な作業をすることを防げない。	・適切に管理された専用の室、区画の中に機器を設置する。 ・機器類は容易に許可された作業員以外が触れないようにする。
	(2)	機器の通信・接続ポートが空いたままで置かれ、まったく保護されれておらず、誰でもが触れたり、不正機器を取り付けたりすることが可能である。	スイッチ等の空きポートに不正端末が容易に接続可能となっている(物理的、電気的)。	・スイッチ等の空きポートには不正利用ができないよう、ハードウェアもしくはソフトウェアにて対策を実施する。
	(3)	ネットワークにつながるネットワーク機器(スイッチ等)の空きポートに不正端末を接続され、マルウェア等を送り込まれる可能性がある。	スイッチ等の空きポートに不正端末が容易に接続可能となっている(物理的、電気的)。	・不要な USB ポート・イーサネットポートは使用できないようにする。
5. 末端装置が置かれる場所				
50	フィールド機器類(センサー、アクチュエータ等)			
	(1)	機器の通信・接続ポートが空いたままで置かれ、まったく保護されれておらず、誰でもが触れたり、不正機器を取り付けたりすることが可能である。	スイッチ等の空きポートに不正端末が容易に接続可能となっている(物理的、電気的)。	・第三者がアクセス可能な場所には、ネットワークフィールド機器を設置しない。
	(2)	通信プロトコル等に相手先認証機能がないため、不正な命令信号を送られても実行してしまう可能性がある。	相手認証無く命令を実行する仕組みとなっている。	・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。
51	IP ネットワークに直結する機器類(IP カメラ、サイネージ)			
	(1)	機器の通信・接続ポートが空いたままで置かれ、まったく保護されれておらず、誰でもが触れたり、不正機器を取り付けたりすることが可能である。	スイッチ等の空きポートに不正端末が容易に接続可能となっている(物理的、電気的)。	・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。
	(2)	通信プロトコル等に相手先認証機能がないため、不正な命令信号を送られても実行してしまう可能性がある。	相手認証無く命令を実行する仕組みとなっている。	・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．本ガイドラインの使い方

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、具体的対策については、優先順位や対策のレベルを記した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ー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。

５．１．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。

５．２．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。

５．３．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。

十分な対策が出来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出来ることになる。

付録 A　用語集

今後作成予定

付録 B　JDCC のリファレンスガイド

・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にして、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。

・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 SWG 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渡るステークホルダーによる議論で、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。

JDCC 日本データセンター協会 Japan Data Center Council

21の管理策

■ **建物設備システムにおけるセキュリティ管理策として21項目を抽出。より具体的なセキュリティ対策の例示を行う。**

物理的設計における管理策	
1	建物設備システムの重要な構成機器(端末・コントローラー・ネットワークを含む)を設置した室・空間は専用のものとすること
2	建物設備システムの構成機器(端末・コントローラー・ネットワークを含む)を設置された室・空間においてはアクセス制御と入退室記録の管理を行うこと
3	建物設備システム端末においては、建物設備システム以外のネットワーク・メディアが不用意に接続されることが無いよう保護措置を取ること
建物設備システム構築時における管理策	
4	建物設備システムを構成する機器リストならびに構成図を作成すること
5	建物設備システムネットワークと他ネットワークの分離を行うこと
6	建物設備システム端末上でのウイルス対策を実施すること
7	サポートされないソフトウェアは利用しないこと
8	不要なサービスを無効にすること
9	パスワードのルールを定め、徹底すること
10	出荷時（デフォルト）のパスワードを変更すること
設備システム運用時における管理策	
11	建物設備システムのネットワークに接続する機器（PC、可搬媒体等）のウイルス検疫は事前に実施されていること
12	建物設備システムのセキュリティ監視手順，インシデント対応手順を整備し、その教育と訓練を定期的に実施し、継続的に対応能力の向上に努めること
13	リモート接続のルールを策定すること
14	適切にマネジメントシステムが運用され、機能していることを評価すること
15	建物設備システムの最新構成情報の管理すること
16	建物設備システムに対する脆弱性と脅威を把握しておくこと
17	建物設備システムのバックアップデータを取得すること
18	要員のアカウント管理を厳密に行うこと
19	建物設備システムのセキュリティ脆弱性に関する情報を定期的に入手し、必要に応じてセキュリティパッチを適用すること
20	建物設備システムの稼動状況やログを定期的に確認すること
21	建物設備システムの重要な構成機器(端末・コントローラー・ネットワークを含む)を設置した室・空間への訪問者のアクセスには関係者が付き添うこと

図　JDCC の 21 の管理策

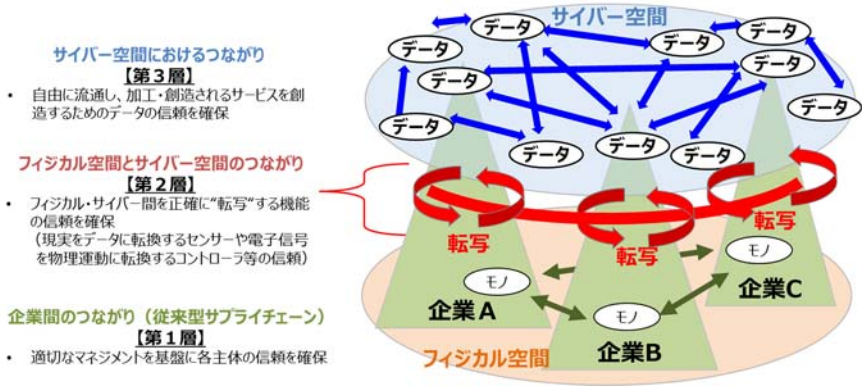
（出典：建物設備システムリファレンスガイドとファシリティインフラ WG の紹介（2017/2、JDCC ファシリティインフラＷＧ事務局））

付録 C　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ビルシステムにおける対策との関係

・2018 年 4 月、産業サイバーセキュリティ研究会 WG1（制度・技術・標準化）において、Society5.0、Connected Industries の進展によって複雑化していくサプライチェーンのサイバーリスクに対応する新たな対策フレームワークの原案を作成しパブリックコメントを実施した。

・同フレームワークでは、IoT やビッグデータの活用などに伴う新たなリスクに対応するため、産業社会を三層（企業間、フィジカル-サイバー、サイバー空間）に分類した新たなアプローチを提示している。（下図のとおり）

・今回示したビルシステムにおける対策は、従来はそれぞれ独立に構築されていたビルの設備システムを中心にリスク分析を行っており、第 2 層における対策中心の傾向がある。一方で、各設備を相互に接続した統合管理も増える傾向にあり、このような状況を踏まえたセキュリティ向上へ向けて、同フレームワークをレファレンスとして、3 層のバランスの良い対策の確立を目指していく。



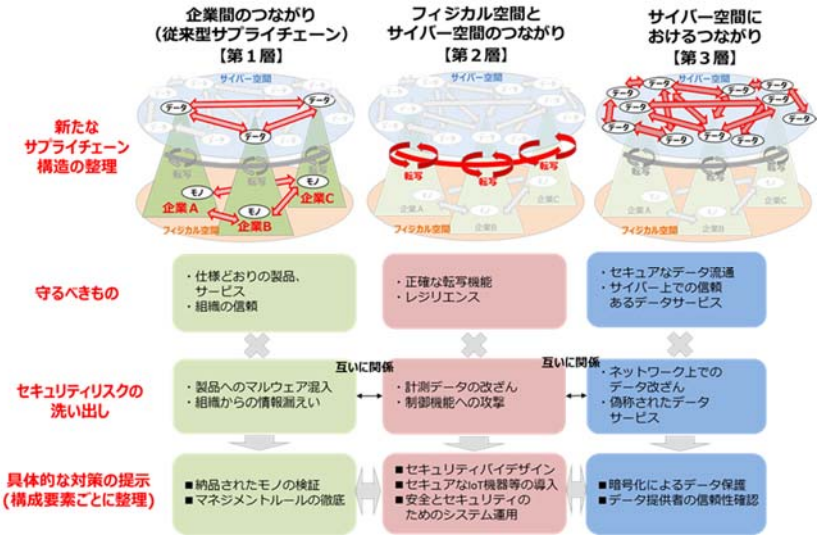


図　サイバー・フィジカル・セキュリティ対策フレームワークにおける3層の考え方

付録 D　参考文献

今後作成予定

付録 E　経験のレポジトリ

今後作成予定