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

令和４年１０月２４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
2022 年 5 月 10 日	第 1 版案（パブコメ版）	パブコメ版発行
2022 年 10 月 24 日	第 1 版	第 1 版発行

目次

図表

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）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つながるケースが増えてきており、外部と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。

- この検討の成果は、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第 1 版」として公開され、ビルシステムに対する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。

- 上記のガイドラインは、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共通編として作成されたもので、この共通編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、今回新たに個別編としてとりまとめた。今回は、その第一弾として空調システムを取り上げて、サイバーセキュリティ対策の要件をまとめている。

- 今後、共通編ガイドラインと併せて、本ガイドライン（個別編：空調システム）が、ビルシステムや特に空調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（個別編：空調システム）を策定する目的

ビルシステムのサイバーセキュリティ確保のためのガイダンスとして、「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」が、2019 年 6 月 17 日に公開され、活用されている。

このガイドラインは、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た共通編として作成され、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うえでの入り口となる情報を提供することを目指したものである。

ガイドライン（共通編）の位置づけ：

- 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。
- 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。

これに対し、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として別途まとめていくこととしている。

その第一弾として空調システムを対象に、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要件をとりまとめた。なお、個別編は各サブシステム特有の要件を共通編との差分として抜き出したものであり、全体に共通する要件については、共通編を併せて参照して欲しい。

1.2. 対象とする空調システム（空調システムの定義）

空調システムは、室内の温湿度環境を制御するシステムであり、セントラル空調方式と個別分散空調方式の 2 種類がある。セントラル空調方式は、熱源設備、空調設備とそれらを監視制御する空調制御システムからなり、これらを制御 IP ネットワーク等で統合管理する仕組みとなっている。個別分散空調方式は、空調設備を空調専用コントローラが制御している。

空調システムの特徴として、対象とするビルの規模（大規模ビル、中小規模ビル）、利用形態（オーナービル、テナントビル）、用途（オフィスビル、病院、公共施設、データセ

ンタ等）により、設置される空調システムが異なり、サイバーセキュリティ対策として考慮する必要のある点も異なってくる。

延べ床面積が1万㎡を超える大規模ビルには、セントラル空調方式が導入される場合が多い。一方、1万㎡以下の中小規模ビルにおいては、個別分散空調方式が導入される場合が多い。近年では、1万㎡を超える大規模ビルにおいても、個別分散空調方式が採用されることも増えてきた。また、空調方式の特徴を生かすために、空調負荷が大きい大規模空間にセントラル空調方式を採用し、空調負荷変動を吸収するために、個別分散空調方式を併設するような物件も増えてきている。

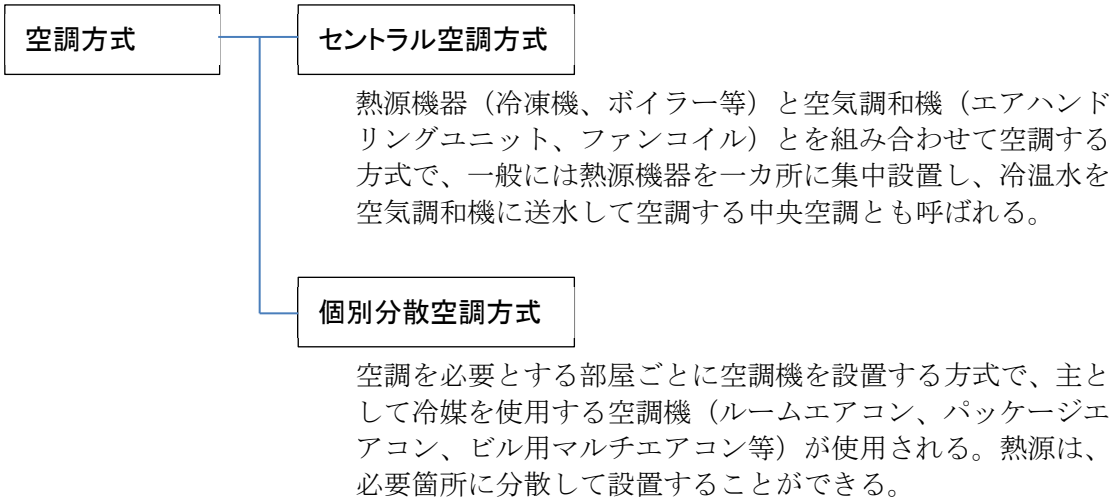
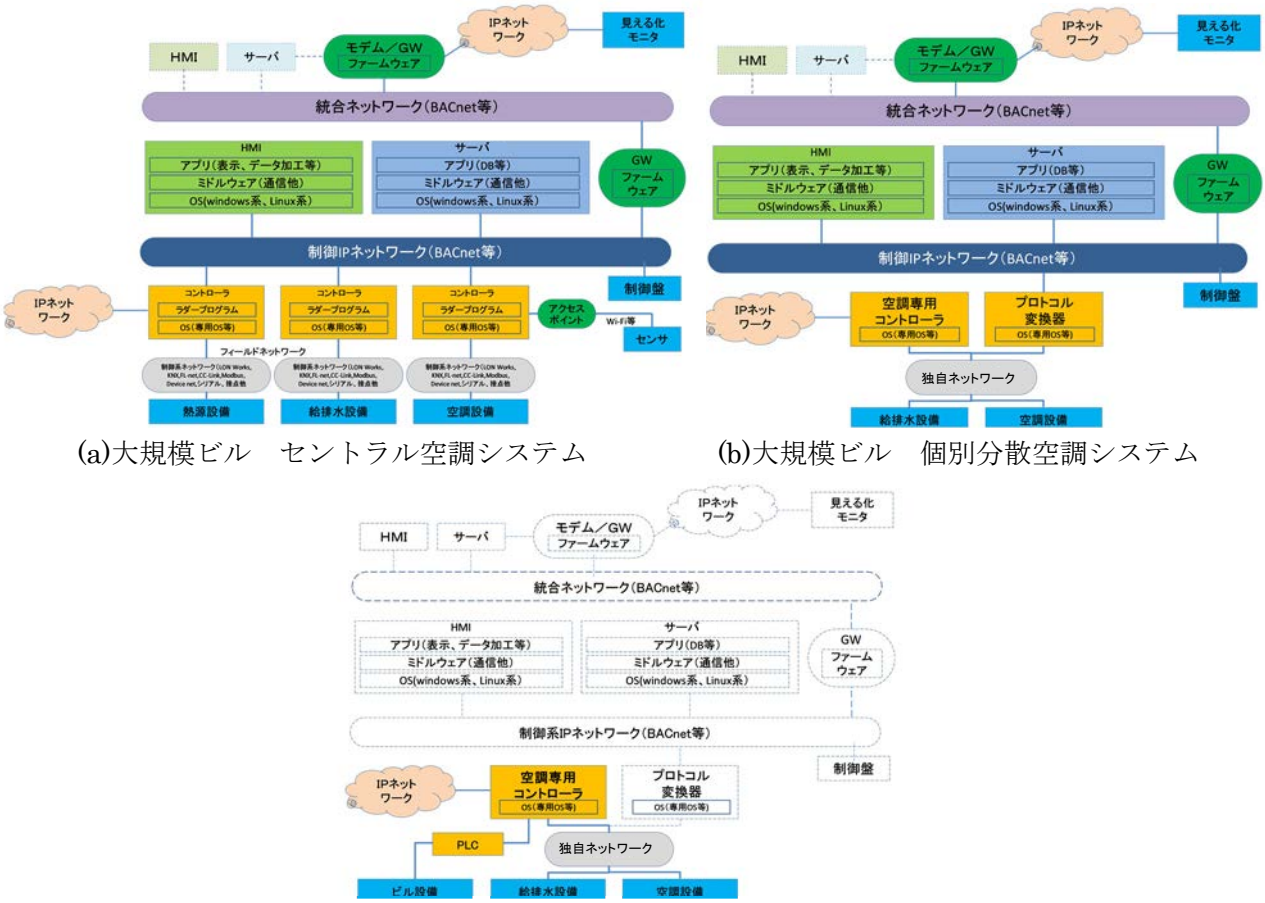


図 1-1　空調方式の違い

大規模ビルにおいては、中央監視盤（HMI とサーバからなる監視、管理（履歴・記録）、制御のシステムの総称）が設置され、空調システムを監視制御している。中央監視盤とは、セントラル空調方式（**図 1-2** (a)）では、熱源設備、給排水設備、空調設備が、それぞれ個別に制御 IP ネットワークを介して接続されている。一方、個別分散空調方式（**図 1-2** (b)）では、プロトコル変換器が制御 IP ネットワークを介してのみ接続されており、接続箇所が限定されている。

中小規模ビルでは、中央監視盤が設置されない場合が多く、空調専用コントローラが、ビル全体の空調システムを監視制御しており、空調以外のビル設備を含めて異常監視等を行う場合もある。（**図 1-2** (c)）



(a)大規模ビル　セントラル空調システム　　(b)大規模ビル　個別分散空調システム

(c)中小規模ビル　個別分散空調システム

図 1-2　ビルの規模と空調システム

1.3. ガイドライン（個別編：空調システム）の位置付け

本ガイドラインは共通編に対し個別のサブシステムに特化した内容を個別編としてまとめたものであるが、サイバーセキュリティ対策の初歩的な対策をまとめたものである点や検討の糸口でありマストではない点、ガイドラインをもとにそれぞれの状況や立場に応じて工夫・改善をして欲しいという点など、ガイドラインとしての基本的な位置付けは共通編と同じである。

共通編においても触れている通り、1つ1つのビルは規模や用途、新規・既設の別、重要度など、その置かれた状況は様々であり、サイバーセキュリティ対策として求められるレベルも対策に掛けられるコストも、また対策によって得られる効果も異なっている。

そのためガイドラインに記載された各要件の実現にあたっても、それぞれの状況に応じて、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ている。逆に、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しい。

本ガイドラインの使い方としては、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、まずはじめに、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。その上で、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。ビルの置かれた状況によって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ものとなる。本ガイドラインでは、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、運用によっては取ることのできる対策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を示しているので、ぜひともそのような視点でも検討して欲しい。

なお、ビル全体として求めているセキュリティレベルを超えて個別システムのセキュリティレベルを特別に引き上げても、ビル全体のセキュリティレベルを上げることは難しい。したがって、空調システムを始め、個別システムのセキュリティ対策の検討にあたっても、ビル共通のセキュリティをどう確保するかという全体方針に従うことが重要であり、そういう観点においても、個別編を参照する前に、ぜひとも共通編をしっかりと理解して対策を検討して欲しい。

その上で、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。

2. 空調システムを巡る状況

2.1. 空調システムで起こりうる攻撃パターンと対応の考え方

ビル設備、あるいは空調システムがサイバー攻撃を受け、空調システムに被害が出ている場合、その被害を最小限に留める方策は重要であるが、並行していち早く空調機能の回復を図る必要がある。データセンタのサーバ室や病院、極寒地のホテル等、空調機能を消失することによって深刻なダメージを受ける場合もあり、サイバー攻撃への対策と同時に、空調機能の回復方法を設計時点から盛り込んでおくことが重要となる。

統合ネットワーク及び制御 IP ネットワークから空調システムに向かって不正に侵入された場合、それぞれの制御機器が、制御不能になり、空調システムが機能しなくなるサイバー攻撃のパターンを以下に示す。

① 上位システムの HMI が攻撃されたことで、空調システムの動作モード、温度設定値等を書き換えられ、本来の動作から逸脱してしまう。
② 統合ネットワークに接続された機器が攻撃されることで、統合ネットワークの通信トラフィックオーバーフローが発生し、上位システムから空調システムの監視制御が出来なくなる。

③ 上位ネットワークと統合ネットワークを接続する G/W がサイバー攻撃を受け、G/W が機能しなくなり、上位システムから空調システムの監視制御が出来なくなる。
④ 空調システムの制御コントローラのファームウェアが改ざんされ、空調システムが機能しなくなる。

これらのサイバー攻撃に関する一例を以下に紹介する。

2.2. 実際のサイバー攻撃事例

ビルシステムがサイバー攻撃を受けた際に、統合ネットワークや制御 IP ネットワーク等の基幹ネットワークのトラフィックが増大することで、空調システムの動作に異常をきたす例が報告されている。この場合、空調システムを基幹ネットワークから切り離した状態で、空調機能を単独で維持できることが重要となる。

個別分散空調方式では、サイバー攻撃によってプロトコル変換器が攻撃され、空調システムとして正常動作しない場合を想定し、空調機を単独で操作できるコントローラ等の別の手段を設計時に配慮しておくことが望まれる。さらに、空調機能維持が特に重要である場所については、空調システムのダウンに対応するため、空調機を二重化して設置することも考慮する必要がある。

セントラル空調方式では、複数の設備機器が連動したシステムであり、空調機のみの冗長化や復旧では空調システムを維持できない場合もある。上位ネットワークから切り離された場合の各設備機器の制御と連動や、居室等需要側での設定値変更の可否について把握し、各コントローラが自律的に行う制御や手動操作で最低限必要なレベルの空調を動作できる設計及び体制を構築しておくことが重要である。

2.2.1. ネットワークビジーで中央監視盤がシステムダウンした事例

あるビルにおいて、空調監視制御システムを新規設置する際に、試運転作業用 PC をネットワークにつないだところ、膨大なブロードキャストパケットがネットワークに流れて、それらを受信した中央監視盤がシステムダウンした。作業に使用したPCからは、マルウェア等は発見されなかった。

ビル内のネットワークケーブルの閉ループが形成されていたことが原因で、サイバー攻撃ではなく作業ミスが原因だが、このような場合には、膨大なパケットが発生する可能性があり、意図的な攻撃も成立しうる状況である。作業に使用したPCのセキュリティチェックのエビデンスが残っていなかったため、作業用 PC が原因である疑いを否定できず、原因究明に時間を要した。このような異常が発生した場合には、作業履歴のチェック、設備機器故障のチェック、設置環境のチェック等想定される要因を並行して確認す

る必要があるが、まずは現状復帰が優先され、異常と原因とを切り分けての明確な原因究明ができない場合が多い。

2.2.2. 空調機コントローラが不正アクセスによりデータを消失した事例

ある施設の空調機を遠隔監視・制御する空調専用コントローラが、インターネットから不正アクセスを受け、再起動した。この結果、空調専用コントローラが、保持していた収集データ、設定値を消失した。

空調専用コントローラは、空調機の運転状況データを収集し、定期的にサーバにアップロードするが、再起動するとアップロード待ちの保持データは消失してしまう。このため、サーバ上の収集データに一部欠損が発生した。空調専用コントローラをインターネット接続する際には、ネットワークに対するセキュリティを確保する旨を仕様書には記載していたが、現場ではそれが守られずにインターネット上から直接アクセス可能な状態になっていた。機器の使用条件として想定しているセキュリティ対策は、運用環境で順守されることが前提であり、これを怠ると、セキュリティホールが発生してしまう。

2.2.3. 空調専用コントローラがマルウェア(ランサムウェア)に感染した事例

ある中小規模ビル内の空調機を監視制御するための空調専用コントローラを構成する空調監視用端末がランサムウェアに感染し、空調システム監視用プログラムが起動できなくなった。いくつかの感染原因が考えられるが、例えば中小規模ビルでは、設備監視室を設置しない場合もあり、空調専用コントローラへの物理的なアクセス管理が不十分で、オペレータの限定や動作ソフトの限定が十分でない場合がある。このような運用状態では、空調専用コントローラがサイバー攻撃にさらされる可能性がある。

3. 空調システムにおけるサイバーセキュリティ対策の考え方

空調システムにおいても、共通編で整理された、サイバーセキュリティ対策のスキームに従って、空調システムの明確化、インシデントや、被害レベルの設定、リスク特定を行うことは重要である。

ビルにおける空調システムは、他の設備と同様に、統合ネットワーク上の HMI から制御されている。HMI がハッキングされ、空調システムに異常値が設定された場合、空調システムは、設定値が動作範囲であれば室内の温湿度等を変化させてしまう。データセンタや冷凍倉庫、病院の ICU 等、温度維持が重要な施設においては、空調温度が正常範囲であることを監視し、正常範囲を逸脱した場合に、その異常を検出する HMI とは切り離された装置を別途設置し、更に空調を正常に稼働できるよう設計時に配慮しておく必要がある。

データセンタや人命に関わる医療施設等、空調システムの停止が、たとえ短時間であっても、多大な被害を発生する場合がある。このような施設においては、異常発生の検出時間、空調システムの復旧対策時間が、対策の重要なポイントになる。施設に要求される検出時間、対策時間は、システム設計時に想定し、復旧対応に必要な設備を設置当初から導入しておく必要がある。

また、空調システムは、ビルの運用が始まると、使用状況の変化に応じ、ビルの間仕切り変更への対応、用途変更に応じる居室の空調能力強化のため個別分散空調の追加等、空調システムの構成が変更される場合がある。このため、設計時点や建築段階でのセキュリティ対策は、ビル運用の変化に応じ、逐次見直す必要がある。

近年の空調システムでは、IP ネットワーク経由で、空調の運用データ、室温データを収集し、省エネや室内環境の改善などに利用している。この場合、空調システムの各種設定を変更しながら、室内環境改善、運用改善を実行している。このような運用では、空調システムが、室内状況の計測データ、変更した制御パラメータを逐次収集、保持している。

万一、サイバー攻撃を受けた際には、空調システムの保持していた計測データや設定値が、失われる可能性がある。したがって、サイバー攻撃から、スムーズに復帰するためには、復旧の優先順位を考え、機能維持の最低限のコントローラを速やかに戻せるように、必要なデータや設定値を適切な間隔でバックアップしておくことが重要である。

空調方式により、ビルネットワークへの接続形態が異なっているため、空調方式ごとに異なるサイバーセキュリティ対策が必要である。ここでは、空調方式ごとに考慮することが求められるサイバーセキュリティ対策の考え方を示す。

3.1. セントラル空調方式のセキュリティ対策

重要設備においては、サイバー攻撃で上位の HMI 経由で空調システムの温度設定を変更されることを、現場で操作ミス・認識違いによる誤操作等が起こる場合と同様に想定することが望まれる。また、HMI からの操作制御であっても、空調システムとして異常値が設定されたことを検出する手段を設け、HMI の異常の際には、その操作設定を無視できる機能（設定値上下限監視）の実装やコントローラをネットワークから分離又はネットワークを介さずに現場での手動操作で対応できる体制を構築しておく必要がある。

セントラル空調方式は、設計の自由度が高く、多数の機器メーカの製品から構成されており、一度異常が発生すると、その原因の切り分けには、膨大な時間を要することが多い。したがって、システムに異常が発生した場合には、サイバー攻撃、機器故障の両面からその原因究明を円滑に進められる作業手順を、事前に準備しておく必要がある。

セントラル空調方式で、空調・熱源を制御するコントローラは、上位と設定値やスケジュールのやり取りをする熱源機器と二次側機器を相互接続する GW を介してインターネット上のサーバと通信をするなど、IP ネットワーク対応が当たり前となっていること、専用

コントローラあるいは汎用コントローラに、Linux、Windows ベースのコントローラが増加していることから、IP ネットワークを介した攻撃の可能性を考慮したセキュリティの対策を施すことが求められる。

コントローラの中にはコントローラメーカが遠隔から監視制御できる機能を持った製品も存在しており、制御 IP ネットワークを経由することなく、直接外部クラウドに接続するコントローラも登場している。こうした遠隔からコントローラを監視制御するネットワークセキュリティに関しては、不要なユーザーがアクセスできるようになっていないか、不要なデータのやり取りをしていないか、不要な設定変更ができるようになっていないか等について十分注意を払う必要がある。

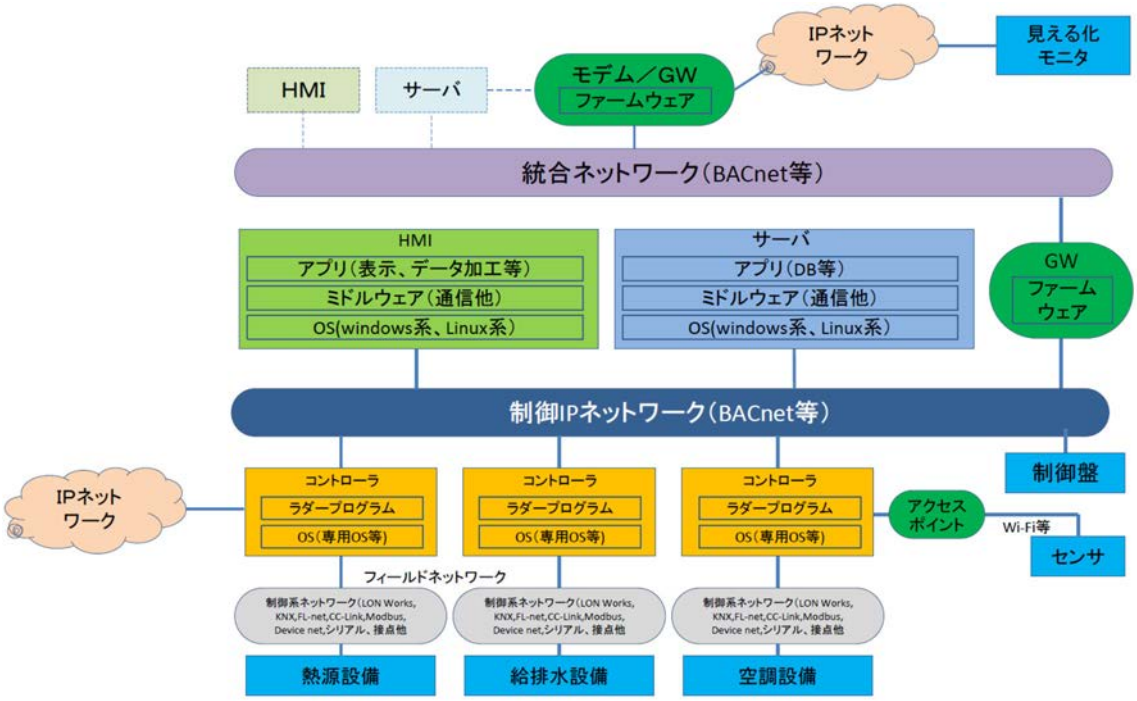


図 3-1　セントラル空調システムのネットワーク接続

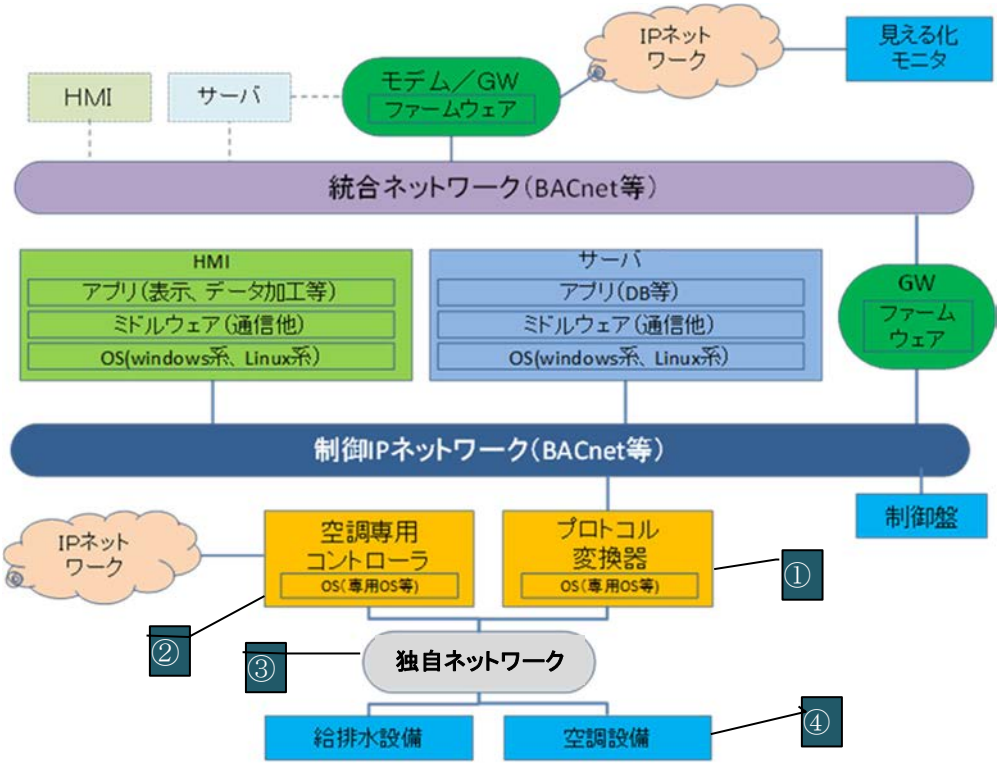
3.2. 個別分散空調方式のセキュリティ対策

重要設備においては、サイバー攻撃で上位の HMI 経由で空調システムの温度設定を変更された場合を想定し、HMI からの操作制御であっても、空調システムとして異常値を設定されたことを検出する手段を設け、HMI からの異常値設定の際には、その設定操作を無視できる機能（設定値上下限監視）を実装しておく必要がある。

大規模ビルに設置される個別分散空調システムは、セントラル空調システム同様、中央監視盤によって監視制御が行われる。個別分散空調システムも、ビルに設置された制御 IP ネットワークの通信プロトコルに合わせたプロトコル変換器を経由して、ビルの統合ネットワークに接続される。このプロトコル変換器は、専用プログラムによる組み込み型の機器や、Linux、Windows ベースの機器で構成されている。これらのコントローラを空調メーカが遠隔から監視制御するものも増加しており、制御 IP ネットワークを経由

することなく、直接外部クラウドに接続するコントローラも多い。コントローラと空調メーカの外部クラウドをつなぐネットワークに関しては、十分なセキュリティ対策を行う必要がある。

　これらの機器は、サイバー攻撃の標的になりえるため、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、万一の攻撃の際にも、空調機能を消失しない安全設計を行う必要がある。



① プロトコル変換器 ： 空調システムを上位の制御ネットワークの通信プロトコル（BACnet 等）で監視制御できるように、プロトコル変換する装置

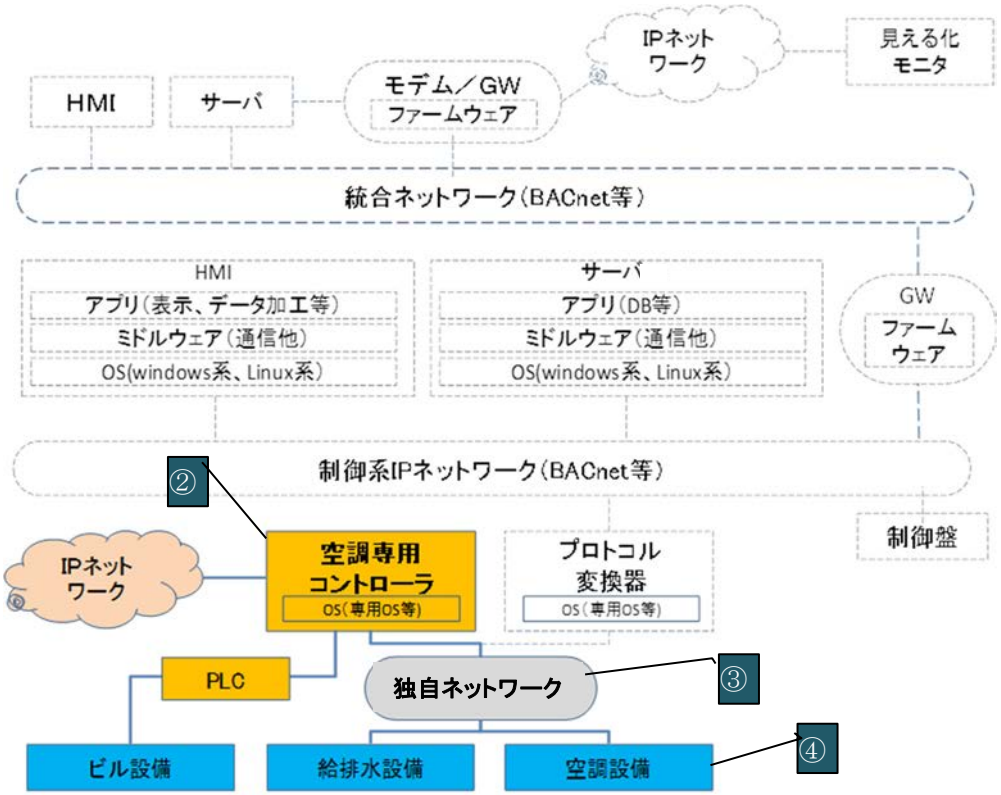
② 空調専用コントローラ ： 中央監視盤（HMI とサーバ）から空調システムの制御監視ができない場合、プロトコル変換器をネットから取り外した際に、空調システムを監視制御する装置。

③ 独自ネットワーク ： 空調機の室外機と室内機を繋ぐネットワークで、メーカ毎に異なる独自の通信プロトコル、電気信号を使う。

④ 空調設備 ： 複数の室内機、室外機、制御コントローラから構成され、空調システムとしては、これで完結した空調動作、制御ができる。

図 3-2 個別分散空調システム（大規模ビル）のネットワーク接続

また、中小規模ビルにおいては、上位の中央監視盤を設置しない場合が多く、空調専用コントローラが、他のビル設備の異常信号を監視するようなシステムを構築する場合がある。また、空調専用コントローラが、ビルの統合ネットワーク経由でクラウドサービスに接続される場合もある。したがって、空調専用コントローラの運用に関して、セキュリティ対策の観点から、一層厳格な運用が求められる



② 空調専用コントローラ　：　中小規模ビルでは、空調システム以外の設備からも異常の移報を受けビル全体を監視制御する装置

③ 独自ネットワーク　：　空調機の室外機と室内機を繋ぐネットワークで、メーカ毎に異なる独自の通信プロトコル、電気信号を使う

④ 空調設備　：　複数の室内機、室外機、制御コントローラから構成され、空調システムとしては、これで完結した空調動作、制御ができる

※数字番号は**図 3-2** に合わせている

図 3-3　個別分散空調システム（中小規模ビル）のネットワーク接続

3.2.1. 個別分散空調システムのセキュリティ対策事例

ビルに設置された空調設備が、サイバー攻撃の標的になった場合、室内温度等の異常状態を認識した場合に初めて、サイバー攻撃を受けた可能性が生まれる。したがって、異常状態が発生していないかを常時監視し、万一異常状態の発生を認識した場合に、サイバー攻撃の有無を確認し、対応を行う。

3.2.1.1. 空調システムの管理

① 空調システムの設置状態の管理

ビルの運用変更に応じ、部屋の間仕切り変更、空調能力増強のため空調機の増設を行うことがある。このような変更に対応し、各室の空調機の設置状態、監視制御

系統のネットワークへの接続状況を常に把握し図面や設備機器リスト等で管理しておく。

② 空調状態や空調システムの運用状態の管理

- 空調維持が重要な場所では、空調状態をオフラインで温度計測し、許容された温度範囲に維持されていることを監視し、異常がないかを確認する。
- 中央監視盤から空調機を監視制御している場合、運転状態、運転モード、設定温度など空調に関わる設定値に異常がないかを確認する。
- 空調機のデータを収集している場合、収集したデータに抜け等の異常がないかを確認する。

万一の異常発生に備え、必要に応じたシステムのバックアップ保存、定期的な設定・計測データの自動保存化、重要機器(サーバ、コントローラ)の A 系・B 系の二重化等、異常時の対応体制を構築しておく。

③ 異常発生時の対応

③-1 中央監視盤のサイバー攻撃を想定する(**図 3-4** (a))

A) 中央監視盤から空調設定値を空調機に再設定し、正常に設定されることを確認する。

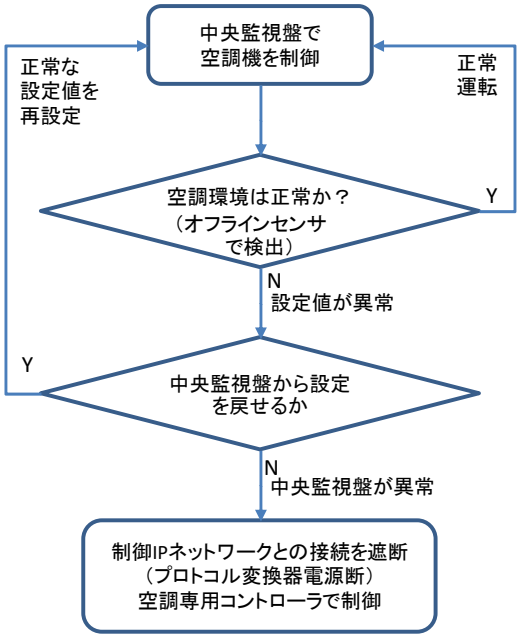
B) 空調監視盤から空調設定温度を再設定できない場合には、制御 IP ネットワークに接続しているプロトコル変換器を遮断(電源を off にするか、ネットワーク接続線を抜く)し、空調専用コントローラによる制御に切り替える。

③-2 空調専用コントローラのサイバー攻撃を想定する。(**図 3-4** (b))

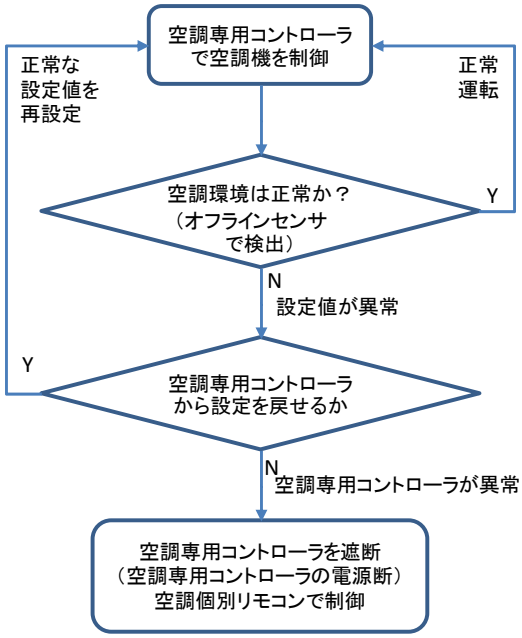
A) 空調設定値を空調機に再設定し、正常に設定されることを確認する。

B) 空調専用コントローラから空調設定温度を再設定できない場合には、空調機の独自ネットワークに接続している空調専用コントローラを遮断(電源を off にするか、ネットワーク接続線を抜く)し、空調個別リモコンによる制御に切り替える。

③-3 空調個別リモコンで制御できない場合は、空調機器の故障として処理する。(**図 3-5**)



a） 中央監視盤での監視



b） 空調専用コントローラでの監視

図 3-4　サイバー攻撃対応フロー

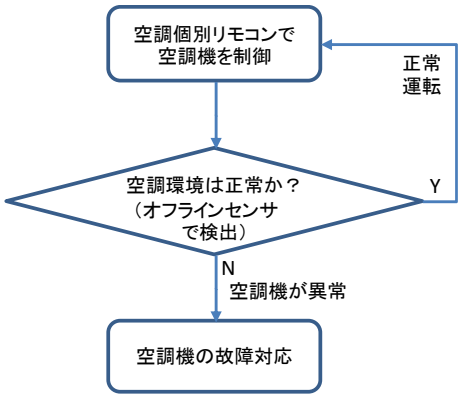


図 3-5　空調機の故障フロー

4. ビルシステムにおけるリスクと対応ポリシー

4.1. 空調システムの管理策

空調システムに関連する設備の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）を前述のサイバー攻撃対応フローで示した中央監視盤及び空調専用コントローラの2つに分け、さらに保守用持ち込み端末を加えた 3 つのパターンで整理したものを表 4-1　空調システムに関するビルシステムのリスクと対策ポリシーとして、表にまとめた。

表 **4-1**　空調システム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
6.空調システム			
60	空調システム		
(1)	設置した空調機への電源や通信線が外され、空調機自体が運転できない状態になる。	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。	・重要な場所を空調する機器（セントラル空調方式の場合は各設備機器）は、適切に管理された専用の室、区画内に設置する。 ・重要な場所を空調する機器（セントラル空調方式の場合は各設備機器）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)	中央監視盤がサイバー攻撃を受け、空調システムが制御不能となり、室内の温湿度等を維持できなくなる。	空調制御システムへのサイバー攻撃により、空調用制御機器がダウンしてしまう。	個別空調で、分オーダーで空調を復旧させたい場合（例：データセンタ、ICU 等） ・空調システムを二重化し正常動作可能な機器で空調を維持する。 ・空調専用コントローラを併設する。 ・居室単位に個別リモコンを設置する。

	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
			個別空調で、数時間オーダーで空調を復旧させたい場合（例：冷凍倉庫等） ・空調専用コントローラを併設する。 ・居室単位に個別リモコンを設置する。
			セントラル空調の場合 ・空調制御システムを動かすために必要な設備機器や制御を事前に把握し、空調用制御システムのダウンにつながる要因について、共通編を参考にリスク及びポリシーを決定する。 （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。）
			セントラル空調の場合 ・各コントローラが自律的に行う制御や手動操作で最低限必要なレベルの空調を動作できる設計及び体制を構築する。 （緊急時の対応手順要件について明記する。）
(3)	中央監視盤がサイバー攻撃を受け、空調システムからのデータ収集ができなくなる。	制御 IP ネットワークへのサイバー攻撃で、大量のデータが流れるなどにより、空調制御のデータ送受信に支障をきたす状態が発生する。	・万一のネットワーク停止時間を想定し、停止時間以上の時間、データ収集をできるように、空調専用コントローラにデータ収集機能を用意する。 ・システムバックアップ方法を運用側と確認のうえでバックアップ方法を設計時に仕様を組み込む。

	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
61	空調専用コントローラ		
(1)	メーカクラウドへのアクセスの際に、サイバー攻撃を受ける。	メーカクラウドへのアクセスの際にネットワークセキュリティの確保ができていない。	・メーカクラウド、空調専用コントローラ間のネットワークでは、通信対象の正当性を適切な方法で確認する。
			・メーカクラウド、空調専用コントローラ間のネットワークでは、通信データに適切な秘匿性を確保する。
(2)	USB 経由や、外部アクセスにより不正接続や攻撃を受ける。	一般ユーザーが、空調システム用監視盤を意識せず、USB を使った内部データの取り出し、ネット検索等の操作を行ってしまう。	・ウイルス感染やネットワークからの不正アクセスを防ぐために、不必要なインタフェースを制限する。（ネットワーク上に、通信先を制限する仕組みを導入する）
			・ウイルス感染やネットワークからの不正アクセスを防ぐために、不必要なインタフェースを制限する。（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。）
(3)	空調専用コントローラがサイバー攻撃を受け、空調システムからのデータ収集ができなくなる。	制御 IP ネットワークへのサイバー攻撃で、大量のデータが流れるなどにより、空調データの送受信に支障をきたす状態が発生する。	・万一のネットワーク停止時間を想定し、停止時間以上の時間、データ収集できるよう空調専用コントローラにデータ収集する機能を用意する。 ・システムバックアップ方法を運用側と確認のうえでバックアップ方法を設計時に仕様を組み込む。
(4)	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。	大規模ビルでは、空調専用コントローラが設置されている防災センター（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。

	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
		中小規模ビルでは、空調専用コントローラが、一般居室に設置されるなどにより、操作許可する作業員が限定できていない。	・重要施設用と一般オフィス用を分離し、重要施設用空調専用コントローラは、管理者だけが操作できるように設置する。 （適切に管理された専用の室、区画の中に機器を設置する）
			・重要施設用空調専用コントローラは、施設管理者が許可した操作者のみが操作できるようにする。 （区画内に設置した空調制御機器への操作履歴管理を行う）
(5)	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。
62	保守用持込み端末		
(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。
(2)	USB 等の外部媒体経由で、端末が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使用可能となっている。	・使用できる外部媒体等をあらかじめ限定した運用を徹底する。 （外部媒体等を安易に利用できないようにする。）
			・使用できる外部媒体等をあらかじめ限定した運用を徹底する。 （外部媒体等を安易に利用できないようにする。）

空調システムに関連して、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のセキュリティーインシデント、リスク源、セキュリティポリシー（対策要件）は、基本的に共通編の要件をそのまま適用可能である。共通編については付録 B に紹介しているので、あわせて参考にして欲しい。

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、空調システムに関連する設備について、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 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、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。

付録 A　空調システムの種類

空調方式は、暖房時や冷房時に使う熱源システムの設置場所により、セントラル空調方式と個別分散空調方式に分類される。セントラル空調方式では、空調対象（ビル）全体の熱源を一カ所にまとめて設置する。大規模ビルでは地下に、中小規模ビルでは屋上に熱源機器を設置する。一方、個別分散空調方式では、熱源機（室外機）と空調機（室内機）の間隔の制限から、中小規模ビルでは、熱源を屋上にまとめて設置、あるいはビル周辺の半地下や地上に分散して設置する。大規模ビルでは、各フロアの周辺部に熱源機（室外機）の設置場所を設け、フロア毎に空調機（室内機）を設置することで、個別分散空調方式を実現している。

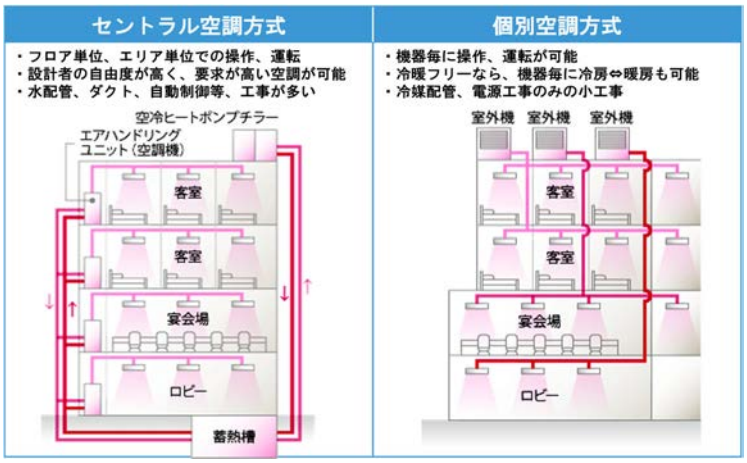


図　付録 A-1　セントラル空調と個別分散空調方式

空調システムでは、熱搬送媒体として、一般的には空気、水、冷媒が使われる。セントラル空調方式では、空気、水が用いられ、個別分散空調方式では、冷媒が用いられる。

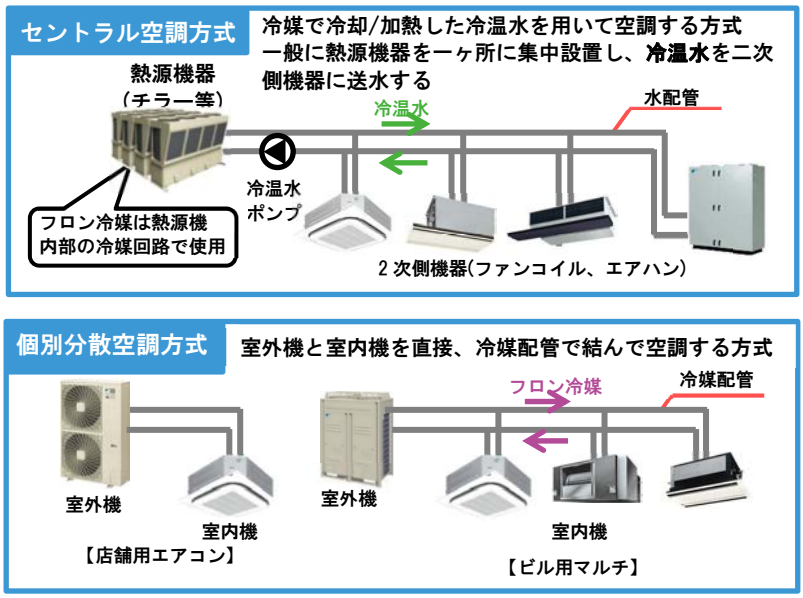


図　付録 A-2　熱搬送媒体の違い

付録 B　参考文献

「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」
経済産業省／サイバーセキュリティ課

本ガイドライン（個別編：空調システム）に対する、上位のガイドラインとなるものであり、ビルシステムを構成する全てのサブシステムにおける共通的なセキュリティ対策が含まれた共通編である。一方、本ガイドラインは空調サブシステムに特化したサイバーセキュリティ対策について記述したものであり、ビルシステム全体に共通する要件については、共通編を併せて参照して欲しい。
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_building/20190617_report.html

なお、参考のため、共通編で示したビルシステムにおけるリスクと対策ポリシーの表を下記に再掲する。

１．全体管理

システム全体の構成情報や組織体制、教育など、場所によらない要素について、セキュリティインシデント、リスク源、セキュリティポリシー（対策要件）のセットでまとめたものが下表である。

表 付録 B- 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。

	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. 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。
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。

	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)	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かったり、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・セキュリティー関連教育を含む・教育場所を明記）

２．機器ごとの管理策

場所ごと、機器ごとの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　付録 B- 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。

	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
(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。
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。

	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。
(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。

	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)	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。
(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。

	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
(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。
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。

	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)	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。
(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。
(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。

	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
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。
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。