５．ライフサイクルを考慮したセキュリティ対応策（別紙）

6.空調システム

機器	インシデント	リスク源	No.	セキュリティポリシー	対応策									
					No.	設計・仕様(Method/Measure)：	No.	建設(Building)	No.	竣工検査(Completion inspection)	No.	運用(Operation)	No.	改修・廃棄(Reforming)
60.空調システム														
	601.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。													
		6011.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。												
			6011P1	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。	6011P1-M1	空調機専用の室、区画を設け、機器を設置する。			6011P1-M1C1	共通：設計通りになっているか検査する。 建築中／試験中の登録情報が破棄されていることを確認する。	6011P1-M1O1	定期的に、登録状況と入退室状況を確認し、継続登録者の見直しを行う。		
			6011P2	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。	6011P2-M1	空調機類を収納する機械室若しくは区画は施錠可能なこと。			6011P2-M1C1	共通：設計通りになっているか検査する。	6011P2-M1O1	鍵の管理を適切に行う。		
	602.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。													
		6021.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。												
			6021P1	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。	6021P1-M1	空調システムを二重化し、空調専用コントローラを併設する。					6021P1-M1O1	定期的に併設機器への切り替え、動作確認を実施する。		
					6021P1-M2	居室単位に個別リモコンを設置する。 緊急時のみに使用する場合は、管理者以外が操作できない場所に設置する。					6021P1-M2O1	定期的に個別リモコンによる居室単位での操作確認を行う。		
			6021P2	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。	6021P2-M1	空調システムを二重化し、空調専用コントローラを併設する。					6021P2-M1O1	定期的に併設機器への切り替え、動作確認を実施する。		
					6021P2-M2	居室単位に個別リモコンを設置する。 緊急時のみに使用する場合は、管理者以外が操作できない場所に設置する。					6021P2-M2O1	定期的に個別リモコンによる居室単位での操作確認を行う。		
			6021P3	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。）	6021P3-M1	システム設計にあたってリスクアセスメントを実施し、必要な運用計画を立案すること。					6021P3-M1O1	運用計画に基づいたリスクアセスメントを適宜実施する。		
			6021P4	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。）	6021P4-M1	緊急時の対応手順、関係者間の連絡手順についてマニュアル化し、竣工引渡し時に説明を行うことを設計要件に書き込む。					6021P4-M1O1	ビル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（関係者間の連絡手順を含む）を整備する。		
	603.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。													
		6031.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。												
			6031P1	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。	6031P1-M1	ネットワーク停止時間と収集するデータと収集間隔を想定し、空調専用コントローラにデータ保持機能を用意する。 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 システムバックアップ周期と操作権限者を定める。その上で、バックアップデータの取得・保管方法と再インストール方法を作成。			6031P1-M1C1	定められた方法で、システムバックアップデータが作成されることを確認する。 その上で、作成されたバックアップデータが有効に再インストールできるか確認しバックアップデータをマニュアルとともに引渡す。	6031P1-M1O1	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。 収集データの欠損が問題になる時間以内の間隔で、サーバにデータバックアップを実施する。 バックアップデータの保管場所管理の定期的確認を行う。	6031P1-M1R1	改修時のバックアップデータ廃棄を行う。

6.空調システム

機器	インシデント	リスク源	No.	セキュリティポリシー	対応策									
					No.	設計・仕様(Method/Measure)：	No.	建設(Building)	No.	竣工検査(Completion inspection)	No.	運用(Operation)	No.	改修・廃棄(Reforming)
61. 空調専用コントローラ														
	611.メーカークラウドへのアクセスの際に、サイバー攻撃を受ける。													
		6111.メーカー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。												
			6111P1	メーカークラウド、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。	6111P1-M1	メーカークラウド、空調専用コントローラ間で、適切な認証方式を導入する。又は専用回線を導入する。			6111P1-M1C1	ネットワーク設計通り適切な認証方式を採用しているか、又は専用回路を用いているかを確認する。	6111P1-M1O1	認証方式が攻撃に対して十分であるかを定期的に確認する。あるいは、認証方式を実現しているソフトウェアの脆弱性を監視し、必要に応じて対応を検討する。	6111P1-M1R1	「設計・仕様」に同様。その時点で最適な仕組みに入れ替える。
			6111P2	メーカークラウド、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。	6111P2-M1	メーカークラウド、空調専用コントローラ間で、適切な暗号方式によりデータの暗号化を導入する。又は専用回線を導入する。万一の漏洩に備え、通信上のデータは必要最低限に限定する。			6111P2-M1C1	ネットワーク設計通り適切な暗号化方式を採用しているか、又は専用回路を用いているかを確認する。	6111P2-M1O1	暗号方式が攻撃に対して十分であるかを定期的に確認する。あるいは、暗号化方式を実現しているソフトウェアの脆弱性を監視し、必要に応じて対応を検討する。	6111P2-M1R1	「設計・仕様」に同様。その時点で最適な仕組みに入れ替える。
	612.USB経由や、外部アクセスにより不正接続や攻撃を受ける。													
		6121.一般ユーザーが、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。												
			6121P1	ウィ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）	6121P1-M1	MAC認証やIPアドレス制限を設ける。			6121P1-M1C1	通信先の制限が機能しているかを確認する。 納品時にすべての機器のMACアドレス・IPアドレスのリストを納入する。	6121P1-M1O1	ログ情報を定期的に確認し、許可したアドレス以外からアクセスされていないことを確認する。 運用時にMACアドレス・IPアドレスのリストを適切に管理する。		
			6121P2	ウィ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。）	6121P2-M1	スイッチ等の空きポートについては、不正利用ができない様、専用モジュラジャックガード等を取付ける。 インテリジェントスイッチ等のソフトウェアにてポート利用制限の設定が可能なものには、その利用制限の設定を行う。	6121P2-M1B1	システム構築業者以外の第三者の不正アクセスを防ぐため、建設中に配線の損傷が無いように管理し、機器が据え付けられた後はEPSの施錠管理を行う。	6121P2-M1C1	スイッチ等の空きポートについては、専用モジュラジャックガード等の取付けがあるか確認する。 インテリジェントスイッチ等のソフトウェアにてポート利用制限の設定が利用制限の設定通りであるか確認する。	6121P2-M1O1	作業者の作業後に、運用者がスイッチ空ポートの専用治具が決められた箇所にあるか、点検時の確認を行う。	6121P2-M1R1	スイッチ更新時にも空ポート管理を更新前と同様な対応を行う。
					6121P2-M2	利用しない空きUSBポート等は治具でふさぐ。	6121P2-M2B1	現場搬入後、引渡しまで防犯管理を実施する。	6121P2-M2C1	利用しない空USBポート等は治具でふさぐ。	6121P2-M2C1O1	利用しない空USBポート等は利用できない状態か、定期的に確認する。		
									6121P2-M2C2	USBを接続する場合は、ウィルス検疫等確認したものに限る。 外部媒体も使用する場合も同じ。	6121P2-M2C2O1	USBを接続する場合は、ウィルス検疫等確認したものに限る。 外部媒体も使用する場合も同じ。		
	613.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。													
		6131.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。												
			6131P1	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。	6131P1-M1	ネットワーク停止時間と収集するデータと収集間隔を想定し、空調専用コントローラにデータ保持機能を用意する。 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 システムバックアップ周期と操作権限者を定める。その上で、バックアップデータの取得・保管方法と再インストール方法を作成。			6131P1-M1C1	定められた方法で、システムバックアップデータが作成されることを確認する。 その上で、作成されたバックアップデータが有効に再インストールできるか確認しバックアップデータをマニュアルとともに引渡す。	6131P1-M1O1	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。 収集データの欠損が問題になる時間以内の間隔で、サーバにデータバックアップを実施する。 バックアップデータの保管場所管理の定期的確認を行う。	6131P1-M1R1	改修時のバックアップデータ廃棄を行う。

6.空調システム

機器	インシデント	リスク源	No.	セキュリティポリシー	対応策											
					No.	設計・仕様(Method/Measure)：	No.	建設(Building)	No.	竣工検査(Completion inspection)	No.	運用(Operation)	No.	改修・廃棄(Reforming)
614.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。														
6141.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。														
			6141P1	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。	6141P1-M1	防災センター（中央監視室）の入場者をシステムを使って登録（事前、都度）・管理する仕組みを入れる。 （全面的に情報システムによる方法）			6141P1-M1C1	入場者に関し、継続登録者、一時登録者を分けて事前登録できること、一時登録者を都度登録できることを確認する。	6141P1-M1O1	入場者は継続登録者、一時登録者ともに事前に、必ずシステム登録する。定期的に、登録状況と入退室状況を確認し、継続登録者の見直しを行う。	6141P1-M1R1	「設計・仕様」に同様。その時点で最適な仕組みに入れ替える。
					6141P1-M2	防災センター（中央監視室）の入場者をシステムを使って登録（事前、都度）する仕組みと紙台帳等（都度）で管理する仕組みを組み合わせて導入する。 （情報システムと手動運用を組み合わせる方法）			6141P1-M2C1	上に同じ。	6141P1-M2O1	入場者は継続登録者、一時登録者ともに事前に、システム登録することを基本とする。紙台帳を利用する場合も事前登録を必須とするとともに、定期的にシステム及び紙台帳への登録状況と入退室状況を確認し、運用の不備の確認や見直しを行う。	6141P1-M2R1	全面的にシステム化する方法の採否について検討を行う。全面システム化が困難な場合でも、情報システムと手動運用を組み合わせる方法の採用を検討する。
					6141P1-M3	防災センター（中央監視室）の入場者を紙台帳等を使って登録（事前、都度）・管理する仕組みを入れる。 （全面的に手動運用による方法）					6141P1-M3O1	入場者は継続登録者、一時登録者ともに事前に、紙台帳への登録を実施する。定期的に紙台帳への登録状況と入退室状況を確認し、運用の不備の確認や見直しを行う。	6141P1-M3R1	全面的にシステム化する方法の採否について検討を行う。全面システム化が困難な場合には、情報システムと手動運用を組み合わせる方法の採用についても検討する。現状の全面的に手動運用による方法を採用する場合でも、セキュリティ確保上の課題を減らす方法について検討を行う。
			6141P2	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。	6141P2-M1	（ICカード等の）システムにより、入退室者の識別と入退室時間を自動的に管理できる仕組みを入れる。 （情報システムにより自動管理する方法）			6141P2-M1C1	予め入退室の事前予約ができ（継続登録者は登録期間や入退室可能曜日等の条件、一時登録者は入退室可能日時等）、情報システムに予約登録された者のみが、登録された情報の範囲（場所、期間等）において、入退室ができ、入退室者の識別結果と入退室時間が記録されることを確認する。また、登録情報の範囲外の者、事前登録の無い者の入室を排除又は警告できることを確認する。 ※一時入場者も事前登録が必要。	6141P2-M1O1	入退室の状況はシステムによって自動的に記録される。 入退室の状況と記録の状況が正しいか、警報の発生状況やその後の処理の状況、システムの抜けを突いた運用がされていないか定期的に確認をする。問題点や不備が確認された場合には運用等の見直しを行う。	6141P2-M1R1	「設計・仕様」に同様。その時点で最適な仕組みに入れ替える。
					6141P2-M2	予め入退室管理者を定め、入退室者の識別と入退室時間をその場でチェックし、管理できる仕組みを入れる。 （情報システム又は紙台帳等により手動管理する方法）			6141P2-M2C1	情報システム又は紙等の管理台帳において、入退室者の識別結果、入退室時間等を管理者が記録できるようになっていること。	6141P2-M2O1	入退室管理者が、事前の登録状況のチェックを行い、登録が無ければ登録を行い、入退室の事実を確認して、情報システム又は紙台帳への記録を行う。 事前の登録状況と都度登録の状況、情報システム又は紙台帳への入退室の記録状況を定期的に確認し、記録や運用の不備の確認や見直しを行う。	6141P2-M2R1	入退室を自動管理する方法の採否について検討を行う。自動管理をしない場合でも、現状が手動管理の場合には、情報システムによる管理への移行を検討する。情報システム化が困難な場合でも、手動運用の中で、セキュリティ確保上の課題を減らす方法について検討を行う。
					6141P2-M3	鍵を貸与された入退室権限保持者が、入退室の都度、自ら入退室時間等を記録する仕組みを入れる。部外者が入退室する際には、入退室権限保持者が同伴し、部外入退室者の識別情報と入退室時間を記録する仕組みを入れる。 （全面的に手動管理する方法）					6141P2-M3O1	入退室権限保持者が、入退室の都度、自ら入退室時間等を紙台帳へ記録する。同伴者がいる場合には、その記録も行う。 勤務録やメンテナンス記録と、紙台帳への入退室の記録状況を定期的に確認し、記録や運用の不備の確認や見直しを行う。	6141P2-M3O1R1	入退室を自動管理する方法の採否について検討を行う。自動管理をしない場合でも、情報システムによる管理への移行を検討する。情報システム化が困難な場合でも、手動運用の中で、セキュリティ確保上の課題を減らす方法について検討を行う。
											6141P2-M3O2	都度入場者（臨時の作業員や見学者など、ICカード不保持者）の入退室にあたっては、入退室管理者（入退室権限保持者）が必ず付きそう。		
6142.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。														
			6142P1	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）	6142P1-M1	空調機専用の室、区画を設け、機器を設置する。			6142P1-M1C1	共通：設計通りになっているか検査する。 建築中／試験中の登録情報が破棄されていることを確認する。	6142P1-M1O1	定期的に、登録状況と入退室状況を確認し、継続登録者の見直しを行う。		
			6142P2	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）	6142P2-M1	空調機類を収納するラックやケース若しくは区画は施錠可能なこと。			6142P2-M1C1	共通：設計通りになっているか検査する。	6142P2-M1O1	カギの管理を適切に行う。		

6.空調システム

機器	インシデント	リスク源	No.	セキュリティポリシー	対応策									
					No.	設計・仕様(Method/Measure)：	No.	建設(Building)	No.	竣工検査(Completion inspection)	No.	運用(Operation)	No.	改修・廃棄(Reforming)
615.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。														
6151.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。														
			6151P1	作業員の作業状況を常時監視する仕組みを入れる。	6151P1-M1	作業員の行動を常時記録する仕組みを入れる。 （システムによる記録）			6151P1-M1C1	防災センター（中央監視室）内で実際に作業員の作業状況を常時監視、記録することができ、監視の死角がないことを確認する。	6151P1-M1O1	記録はシステムによって自動的に行われる。 システムによる記録状況を定期的に確認し、記録システムの不具合の発生や作業員の不審行動の有無等を確認する。	6151P1-M1R1	作業員の不審行動を自動で検知し、警報を発するシステムの導入を検討する。困難な場合でも、行動記録システムのより最適な記録に向けた見直しを行う。
					6151P1-M2	日報等で他の作業員の不審行動を記録できるようにする。 （作業員相互の牽制）					6151P1-M2O1	日報を定期的に確認し、作業員の不審行動の有無を確認する。	6151P1-M2R1	作業員の不審行動を自動で検知し、警報を発するシステムの導入や、作業員の行動を記録システムの導入を検討する。新規システムの導入が困難な場合でも、作業員同士の相互牽制をより最適なものとし、追加的な監視の導入に向けた見直しを行う。
			6151P2	許可された作業員以外が作業できない仕組みを入れる。	6151P2-M1	物理的なバリアを設け、許可された者以外が触れることを困難にする。			6151P2-M1C1	防災センター（中央監視室）内で実際に許可された以外のエリアに入ることができたり、許可されたスイッチ盤や操作端末に触れることができないことを確認する。	6151P2-M1O1	防災センター（中央監視室）内の作業状況を定期的に確認し、作業員が無関係なシステムに近づけない仕組みが正しく運用されていることを確認する。確認の結果、課題点等があれば、運用や仕組みの改善を行う。	6151P2-M1R1	「設計・仕様」に同様。その時点で最適な仕組みに入れ替える。
					6151P2-M2	システムへのログイン管理等により、許可された者以外が操作することを困難にする。			6151P2-M2C1	防災センター（中央監視室）内で実際に許可された以外の端末やシステムにログインができないことを確認する。	6151P2-M2O1	防災センター（中央監視室）内の作業状況を定期的に確認し、作業員が無関係なシステムを操作できない仕組みが正しく運用されていることを確認する。確認の結果、課題点等があれば、運用や仕組みの改善を行う。	6151P2-M2R1	「設計・仕様」に同様。その時点で最適な仕組みに入れ替える。
62.保守用持込み端末														
621.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。														
6211.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。														
			6211P1	保守用端末は適切に管理されたものを使う。	6211P1-M1	保守用端末はその建物専用のものを納入する。	6211P1-M1B1	保守用端末も、工場出荷時にウィルス検疫を実施する。	6211P1-M1C1	保守用端末も、竣工引渡し時にウィルス検疫を実施する。	6211P1-M1O1	保守用端末はその建物専用のものとし、持ち出しさせない運用とする。 脆弱性の情報を定期的に収集する。 ウィルス検疫ツール等で、定期的に検査する。 定期的にOS、ミドルウエア、アプリケーション等にパッチをあてる、安定性が確保された範囲で最新のものに更新する。	6211P1-R1	サービスされないソフトウェアが生じたら、システムを最新のものに更新する。 若しくは廃棄を検討する。
					6211P1-M2	保守用端末はウィルス検疫やパッチなど適切に管理されたものを使う			6211P1-M2C1	保守用端末を持ち込む際、事前にウィルス検疫を実施するものとする	6211P1-M2O1	保守用端末を持ち込む際、事前にウィルス検疫を実施するものとする。 ウィルスソフトを常駐させ、常にチェックする。 OS、ドライバ等をオンラインで更新する。		
622.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。														
6221.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。														
			6221P1	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。）	6221P1-M1	利用しない空USBポート等は治具でふさぐ。 接続先機器を施錠できるケースやラックに収納する。	6221P1-M1B1	現場搬入後、引渡しまで防犯管理を実施する。	6221P1-M1C1	利用しない空USBポート等は治具でふさぐ。	6221P1-M1O1	利用しない空USBポート等は利用できない状態か、定期的に確認する。		
			6221P2	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。 （外部媒体等を事前検疫してから利用する。）					6221P2-C1	USBを接続する場合は、ウィルス検疫等確認したものに限る。 外部媒体も使用する場合も同じ。	6221P2-O1	USBを接続する場合は、ウィルス検疫等確認したものに限る。 外部媒体も使用する場合も同じ。		