５．ライフサイクルを考慮したセキュリティ対応策（別紙）

1.全体管理

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)
01.構成情報／管理情報														
011.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。														
0111.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。														
			0111P1	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。	0111P1-M1	設計図書の特記仕様にシステム構成図を記載する。 システム全体構成の更新履歴、管理設備ごとの稼動履歴等、資産管理システム又は設備機器管理システムを利用した運用管理を行う仕様を明記する。	0111P1-M1B1	納品されるシステム構成品（設備）が設計仕様（同等品でも）と異なる場合、その内容を明記してシステム構成図を作成する	0111P1-M1C1	システム構成図と現場機器が合致しているかの確認を行い、引渡す。	0111P1-M1O1	変更が発生する都度、システム構成図を最新に更新して常に最新に保つ。	0111P1-M1R1	システム構成が更新や改修時に変更があった部分を最新の情報にシステム構成図を改め、古い構成図は廃棄処理を確認する。
02.バックアップデータ／事業継続														
021.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。														
0211.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。														
			0211P1	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。	0211P1-M1	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。			0211P1-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。	0211P1-M1O1	運用開始前に、バックアップデータからの復旧再インストールが行えることを確認する。 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。 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。	0211P1-M1R1	改修時のバックアップデータ廃棄を行う。
022.システムの脆弱性をついた攻撃を受ける。														
0221.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。														
			0221P1	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。	0221P1-M1	設計図書の特記仕様にシステムの脆弱性対策について記載する。 システム全体の接続性を担保した上での、必要なアップデート／パッチが適用されている機器であることを仕様に明記する。			0221P1-M1C1	システム全体の接続性を担保した上での、必要なアップデート／パッチが適用されている機器であることを確認し引渡す。	0221P1-M1O1	ビル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適用の可否と時期を検討すること。		
03.会社／要員の管理														
031.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。														
0311.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。														
			0311P1	システム構築要件に教育訓練について明記する。	0311P1-M1	発注主側の運転管理者教育について、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）			0311P1-M1C1	竣工引渡し時にシステム操作説明を行う際、合わせてセキュリティについても説明を実施すること。	0311P1-M1O1	ビルシステムの運用会社選定（委託先選定）にあたって、その責任範囲を発注要件に組み込む。 ・管理・運用組織への継続的セキュリティ啓発／監査を実施する。 ・ビルシステム引渡し前に運転要員相当数に十分な操作訓練期間を設ける。 ・ビルシステムの運転権限者の登録情報を発注者と共有できる。 ・自社（運用会社）の定められた人以外の操作者に対し（保守作業者など）定めた手順を確認し記録する。 ・発注主に対し運転記録・保管記録類の定期報告要件がある（日常正常時・不具合対応時）。		
032.ビルシステムが内部作業員等から攻撃を受ける。														
0321.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。														
			0321P1	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。	0321P1-M1	システム構築要件を明示する。 就労届や作業員名簿にて、作業員の身元確認を実施すること。また作業実施時は必ず元請社員の立会いを行うこと。	0321P1-M1B1	作業場所が施錠可能な状況から機器の搬入据付を行なう。 やむを得ず、搬入する場合、事前開封が行なわれたかの有無が確認できる梱包をして保管。 就労届や作業員名簿にて、作業員の身元確認を実施すること。また作業実施時は必ず元請社員の立会いを行うこと。 定期的な現場巡回を行い、不審者や不審行動（不要な撮影等）などを取り締まる。	0321P1-M1C1	元請け社員以外の作業箇所記録を保管し、発注主に報告可能な状態とする。	0321P1-M1O1	保守作業のための来館者は事前届出を行い、入館時に身元確認をし作業域への入室を許可する。		

1.全体管理

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)
04.体制構築等														
041.攻撃等への対応が効果的にできず、被害が拡大する。														
0411.十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。														
			0411P1	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。	0411P1-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。					0411P1-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。		
042.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。														
0421.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。														
			0421P1	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。	0421P1-M1	設計過程で、セキュリティ知識を持った有識者の監修を受けること。			0421P1-M1C1	構築後セキュリティ知識を持った有識者の監修を受け、証明を得ること。	0421P1-M1O1	竣工引渡し時の監査の内容に変化がないか定期的な確認を行う。		
043.攻撃への初動対応が遅れ、被害が拡大する。														
0431.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。														
			0431P1	入場前に適切にセキュリティ対策を実施する。	0431P1-M1	作業者の入場者教育実施時にセキュリティ教育を実施する。	0431P1-M1B1	作業者の入場者教育実施時にセキュリティ教育を実施する。			0431P1-M1O1	保守員の教育を徹底し、訓練を実施し防御のレベルを上げる。		
044.攻撃への対応が体系的に実施できず、被害が拡大する。														
0441.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。														
			0441P1	設計要件・運用要件を明記する。	0441P1-M1	定期的なセキュリティ監査を行い、セキュリティ管理体制を維持することを設計要件に盛り込む。					0441P1-M1O1	定期・不定期のセキュリティー診断を行う。インシデント対応時の連絡体制を含むセキュリティ管理体制を構築し、適切に運用管理する。		
045.攻撃に対する対応手順が分からず、被害が拡大する。														
0451.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。														
			0451P1	緊急時の対応手順要件について明記する。	0451P1-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。					0451P1-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。		
046.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。														
0461.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。														
			0461P1	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）			0461P1-B1	竣工引渡し時にシステム操作説明を行う際、合わせてシステム運用管理についても教育を実施すること。			0461P1-O1	ビルシステムの稼動状況やログを定期的に確認することの重要性についての教育を行う。		

2.機器ごとの管理策　1.ネットワーク（クラウド、情報系NW、BACnet等）

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)
10.ネットワーク														
101.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。														
1011.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。														
			1011P1	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。	1011P1-M1	システムごとにネットワークセグメントを分離する。			1011P1-M1C1	ネットワーク設計どおりにセグメントが分離されていることを確認する。	1011P1-M1O1	ネットワークの変更時にセグメントが分離されていることを確認する。		
					1011P1-M2	システム・ネットワークの規模が大きい場合、単一システム内においてもセグメントを分離する。			1011P1-M2C1	ネットワーク設計どおりにセグメントが分離されていることを確認する。	1011P1-M2O1	ネットワークの変更時にセグメントが分離されていることを確認する。		
102.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。														
1021.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。														
			1021P1	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。	1021P1-M1	収容システムの動作上必要なネットワークセグメント間通信は、必要な通信のみ許可する。			1021P1-M1C1	ネットワーク設計どおりに必要な通信以外が制限されていることを確認する。	1021P1-M1O1	ネットワークの変更時にセグメント間で必要な通信以外が制限されることを確認する。		
103.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。														
1031.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。														
			1031P1	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。	1031P1-M1	外部ネットワークとの接続点にはファイアウォールを設置し、収容システムの動作に必要不可欠な最小限の通信のみを許容する。			1031P1-M1C1	ネットワーク設計どおりに必要な通信以外が制限されていることを確認する。	1031P1-M1O1	外部ネットワークとの接続は運用責任者が統制し、収容システムの動作に必要不可欠な最小限の通信のみが許容され、不正な外部ネットワーク接続がないことを定期的に点検する。		
104.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。														
1041.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。														
			1041P1	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。	1041P1-M1	運用フェーズにおけるの引込回線の管理性を高めるため、外部接続回線の入線経路や回線引込エリアを規定（制限）する。			1041P1-M1C1	設計図書に記載されていない外部接続回線が設置されていないことを確認する。	1041P1-M1O1	運用責任者が外部接続回線の設置状況を定期的に点検し、不正な回線が引き込まれていないことを確認する。		
					1041P1-M2	施工者や入居者が許可なく回線を敷設できない運用ルールを定める。					1041P1-M2O1	施工者や入居者が許可なく回線を敷設できない運用ルールを徹底する。		
11.クラウドサーバ・Webサーバ														
111.外部ネットワーク接続経由で侵入を受ける。														
1111.外部接続機器のセキュリティ対策が十分ではない。														
			1111P1	外部からのアクセスに制限を設ける。	1111P1-M1	外部との境界にはDMZを置き内部と外部で直接アクセスはせず、データの交換を行う。			1111P1-M1C1	外部アクセスが制限されていることを確認する。	1111P1-M1O1	許可されたアクセスのみ実施されていることを定期的に確認する。	1111P1-M1R1	廃棄時にはネットワーク機器の設定データ（管理者パスワードを含んで）を消去するか物理的に破壊しアクセスできないようにする。
					1111P1-M2	境界にファイアウォールを立て、かつプロキシサーバを立てて外部とのアクセスは間接アクセスとする。								
					1111P1-M3	境界にファイアウォールを設ける。								
112.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。														
1121.Web公開システムの脆弱性対策が十分ではない。														
			1121P1	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。	1121P1-M1	アクセス制御の実現方式を検討し、設計に反映する。			1121P1-M1C1	設計どおりに通信制限が行われていることを確認する。	1121P1-M1O1	利用者（入居者等）の変更の都度、システムのアクセス制御に関する設定変更を行う。		
					1121P1-M2	インターネット公開システム収容セグメントのセキュリティ確保に関する技術的対策を検討し、設計に反映する。					1121P1-M2O1	セキュリティリスクアセスメント等の機会を用いて、技術的対策の有効性を定期的に点検する。		
113.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。														
1131.発注側がリスクを把握していない。														
			1131P1	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。	1131P1-M1	クラウドサービスの約款を確認し、必要なセキュリティレベルについて合意したうえで発注する。								

2.機器ごとの管理策　1.ネットワーク（クラウド、情報系NW、BACnet等）

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)
12.情報系端末（オフィス系端末）														
	121.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。													
		1211.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。												
			1211P1	外部からのアクセスに制限を設ける。	1211P1-M1	外部との境界にはDMZを置き内部と外部で直接アクセスはせず、データの交換を行う。			1211P1-M1C1	外部アクセスが制限されていることを確認する。	1211P1-M1O1	許可されたアクセスのみ実施されていることを定期的に確認する。	1211P1-M1R1	廃棄時にはネットワーク機器の設定データ（管理者パスワードを含んで）を消去するか物理的に破壊しアクセスできないようにする。
					1211P1-M2	境界にファイアウォールを立て、かつプロキシサーバを立てて外部とのアクセスは間接アクセスとする。								
					1211P1-M3	境界にファイアウォールを設ける。								
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）														
	131.外部ネットワーク接続経由で攻撃を受ける。													
		1311.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。												
			1311P1	外部からのアクセスに制限を設ける。	1311P1-M1	外部との境界にはDMZを置き内部と外部で直接アクセスはせず、データの交換を行う。			1311P1-M1C1	外部アクセスが制限されていることを確認する。	1311P1-M1O1	許可されたアクセスのみ実施されていることを定期的に確認する。	1311P1-M1R1	廃棄時にはネットワーク機器の設定データ（管理者パスワードを含んで）を消去するか物理的に破壊しアクセスできないようにする。
					1311P1-M2	境界にファイアウォールを立て、かつプロキシサーバを立てて外部とのアクセスは間接アクセスとする。								
					1311P1-M3	境界にファイアウォールを設ける。								
14.ビルシステム間相互接続														
	141.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。													
		1411.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。												
			1411P1	正当な端末以外にアクセスしない、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。	1411P1-M1	接続端末を制限する仕組みを導入し、通常使わないパケットは流さない。			1411P1-M1C1	許可された端末へのアクセスしかできない事を確認する 予め許可されたパケット以外は流されないことを確認する。	1411P1-M1O1	許可されたアクセスのみ実施されていることを定期的に確認する。	1411P1-M1R1	廃棄時には許可常用情報を完全消去する。

2.防災センター（中央監視室）

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)
20.防災センター（中央監視室）														
201.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。														
2011.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。														
			2011P1	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。	2011P1-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）			2011P1-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。	2011P1-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。	2011P1-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。
					2011P1-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）			2011P1-M2C1	上に同じ。	2011P1-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。	2011P1-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。
					2011P1-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）					2011P1-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。	2011P1-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。
			2011P2	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。	2011P2-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）			2011P2-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。	2011P2-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。	2011P2-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。
					2011P2-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）			2011P2-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。	2011P2-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。	2011P2-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。
					2011P2-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）					2011P2-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。	2011P2-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。
											2011P2-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。		
202.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。														
2021.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。														
			2021P1	作業員の作業状況を常時監視する仕組みを入れる。	2021P1-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）			2021P1-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。	2021P1-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。	2021P1-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。
					2021P1-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）					2021P1-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。	2021P1-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。
			2021P2	許可された作業員以外が作業できない仕組みを入れる。	2021P2-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。			2021P2-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れたり、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。	2021P2-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。	2021P2-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。
					2021P2-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。			2021P2-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。	2021P2-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。	2021P2-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。

2.防災センター（中央監視室）

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)
21.HMI/HIM														
211.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。														
2111.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。														
			2111P1	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。	2111P1-M1	操作者を人単位で特定／限定できる機能を入れる ・生体認証、IDカード、ID/PW等			2111P1-M1C1	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。	2111P1-M1O1	登録の管理が必要になる。 破棄については定期監査を実施。 システム的な定期チェック。 IDカードは、パスワードの管理は個人単位で行う。		
					2111P1-M2	操作者を特定の集団に限定する機能を入れる。 ・IDカード、ID/PW等			2111P1-M2C1	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。	2111P1-M2O1	登録の管理が必要になる。 破棄については定期監査を実施。 システム的な定期チェック。 IDカードは、パスワードの管理はグループ単位でしっかりする。		
											2111P1-O1	入室管理（個人を特定した入退室の管理）をする。 （レベル高：相互監視体制＋記録、レベル中：どちらかが入る）		
212.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。														
2121.端末やシステムの権限管理や作業監視が十分でない。														
			2121P1	作業員の作業状況を常時監視する仕組みを入れる。	2121P1-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）			2121P1-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。	2121P1-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。	2121P1-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。
					2121P1-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）					2121P1-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。	2121P1-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。
			2121P2	許可された作業員以外が作業できない仕組みを入れる。	2121P2-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。			2121P2-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れたり、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。	2121P2-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。	2121P2-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。
					2121P2-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。			2121P2-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。	2121P2-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。	2121P2-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。
213.侵入者にシステム情報を探られ攻撃が拡大する。														
2131.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。														
			2131P1	アクセスログ、操作履歴を適切に管理する	2131P1-M1	操作履歴、ログ情報の記録と解析の仕組みを導入する アクセスログを閲覧する権限を管理する			2131P1-M1C1	共通：設計通りの機能が入っているか検査する	2131P1-M1O1	操作履歴、ログ情報の記録と解析の仕組みが正常に機能しているか、定期的に確認する。 権限管理が適切に管理・運用できているか、定期的に点検する。		
214.不正侵入に対する状況解析が困難で対策が遅れる。														
2141.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。														
			2141P1	各種ログ情報の導入とログ解析の仕組みを導入する。	2141P1-M1	ログ情報取得システムを導入する。			2141P1-M1C1	ログ取得、解析のシステムが動作していることを確認する。	2141P1-M1O1	必要に応じてログ情報の解析を行う。 アラーム発生時の行動指針を作成し教育訓練を定期的に実施する。	2141P1-M1R1	廃棄前に取得したログ情報を完全に消去する。 ログを何処で取っているか解析されないようにログ取得機能を消去若しくはオフする。 IPアドレスも予め定められた値に変更する。
215.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。														
2151.システムの運用監視が十分でない。														
			2151P1	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。	2151P1-M1	IDS（侵入検知システム）、UTM（統合脅威管理）等を導入する。 ログの取得、解析システムを導入し機器やネットワークの状態を監視する。			2151P1-M1C1	ネットワーク監視の仕組みが導入され正しく動作していることを確認する。	2151P1-M1O1	ログを必要に応じて解析し、異常の有無を確認する。 ネットワーク監視やログ解析により異常と判断されたときに実施する行動マニュアルを作成し教育訓練を行う。	2151P1-M1R1	ネットワーク監視機器の構成情報やログ情報は完全に消去する。
216.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。														
2161.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。														
			2161P1	工場出荷前及び引渡し前に事前検疫を実施する。			2161P1-B1	工場出荷前にウィルス検疫を実施する。	2161P1-C1	竣工引渡し前にウィルス検疫を実施する。	2161P1-O1	定期的にウィルス検疫し、記録を取る。		

2.防災センター（中央監視室）

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)
217.侵入者にシステム内部を探られ、不正な操作をされる。														
2171.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。														
			2171P1	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。	2171P1-M1	操作者、管理者などの権限管理できる機能を入れる。 操作者にはシステムの内部構造が見えないようにする。 データの閲覧や操作の権限を管理する。			2171P1-M1C1	共通：設計通りの機能が入っているか検査する。	2171P1-M1O1	権限管理が有効に機能しているか定期的に検査する。		
218.システムの脆弱性をついた攻撃を受ける。														
2181.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。														
			2181P1	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。	2181P1-M1	適切なアップデートやパッチ適用が可能な機能を有する機器を導入する。	2181P1-M1B1	工場出荷前に、その時点で脆弱性情報に対して、適切に対応できているか確認する。	2181P1-M1C1	竣工引渡し前に、その時点で脆弱性情報に対して、適切に対応できているか確認する。	2181P1-M1O1	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。	2181P1-M1R1	サービスされないソフトウエアが生じたら、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。
											2181P1-M1O2	脆弱性の情報を収集し、把握しておく。		
219.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。														
2191.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。														
			2191P1	外部媒体等を安易に利用できないようにする。	2191P1-M1	利用しない空USBポートは治具でふさぐ。 HIM本体を施錠できるケースやラックに収納する。	2191P1-M1B1	現場搬入後、引渡しまで防犯管理を実施する。	2191P1-M1C1	利用しない空USBポートは治具でふさぐ。	2191P1-M1O1	利用しない空USBポートは利用できない状態か、定期的に確認する		
			2191P2	外部媒体等を事前検疫してから利用する。					2191P2-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。	2191P2-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。		
22.保守用持ち込み端末														
221.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。														
2211.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。														
			2211P1	保守用端末は適切に管理されたものを使う。	2211P1-M1	保守用端末はその建物専用のものを納入する。	2211P1-M1B1	保守用端末も、工場出荷時にウイルス検疫を実施する。	2211P1-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。	2211P1-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。 ウイ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。	2211P1-R1	サービスされないソフトウエアが生じたら、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
					2211P1-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			2211P1-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	2211P1-M2O1	保守用端末を持ち込む際、事前にウイルス検疫を実施するものとする ウイ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		
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）														
231.不正端末を接続され、マルウェアを送り込まれる。														
2311.空きポートが接続可能な状態で放置されている。														
			2311P1	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。	2311P1-M1	スイッチ等の未使用ポートを物理的にロックする。 可能ならスイッチ等の未使用ポートを動作させない構成情報を導入する。 利用しているポートから容易にケーブルを抜かれないように物理的に保護する。 （ケーブルロックの仕組みの導入やポートがある機器は鍵付ラック内や高度セキュリティエリア内に設置する。） 空きポートが利用された場合、それを特定できるようにする。			2311P1-M1C1	ネットワーク機器の未使用ポートが利用できないことを確認する。	2311P1-M1O1	定期的に未使用ポートのチェックを行う。 未使用ポートを利用する場合の承認プロセスを確立する。		

2.防災センター（中央監視室）

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)
24.システム管理用サーバ（ビルシステム主装置）														
				241.所定の作業員以外による不正操作が行われる。										
				2411.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。										
			2411P1	適切に管理された専用の室、区画の中に機器を設置する。	2411P1-M1	サーバ類専用の室、区画を設け、機器を設置する。			2411P1-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。	2411P1-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。		
			2411P2	区画内のラックやケースは施錠管理を行う。	2411P2-M1	サーバ類を収納するラックやケースは施錠できるタイプのものとする。			2411P2-M1C1	共通：設計通りになっているか検査する。	2411P2-M1O1	カギの管理を適切に行う。		
				242.所定の作業員以外による不正操作が行われる。										
				2421.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。										
			2421P1	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。	2421P1-M1	サーバ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）			2421P1-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。	2421P1-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。	2421P1-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。
				243.侵入者にシステム情報を探られ攻撃が拡大する。										
				2431.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。										
			2431P1	アクセスログを記録する機能を入れる。	2431P1-M1	閲覧する権限を管理する。 システムログサーバを設置する。			2431P1-M1C1	共通：設計通りの機能が入っているか検査する。	2431P1-M1O1	権限管理が適切に管理できているか、定期的に点検する。 システムログサーバが動作しているか、定期的に確認する。		
				244.不正侵入に対する状況解析が困難で対策が遅れる。										
				2441.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。										
			2441P1	各種ログ情報の導入とログ解析の仕組みを導入する。	2441P1-M1	ログ情報取得システムを導入する。			2441P1-M1C1	設置端末全てに対してマルウエア対策を施す。 ログ取得、解析のシステムが動作していることを確認する。	2441P1-M1O1	必要に応じてログ情報の解析を行う。 アラーム発生時の行動指針を作成し教育訓練を定期的に実施する。	2441P1-M1R1	廃棄前に取得したログ情報を完全に消去する。 ログを何処で取っているか解析されないようにログ取得機能を消去若しくはオフする。 IPアドレスも予め定められた値に変更する。
				245.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。										
				2451.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。										
			2451P1	不正なアクセスや操作を確認する仕組みを入れる。	2451P1-M1	IDS（侵入検知システム）、UTM（統合脅威管理）等を導入する。 ログの取得、解析システムを導入し機器やネットワークの状態を監視する。			2451P1-M1C1	ネットワーク監視の仕組みが導入され正しく動作していることを確認する。	2451P1-M1O1	ログを必要に応じて解析し、異常の有無を確認する。 ネットワーク監視やログ解析により異常と判断されたときに実施する行動マニュアルを作成し教育訓練を行う。	2451P1-M1R1	ネットワーク監視機器の構成情報やログ情報は完全に消去する。
				246.不正な命令を実行してしまい、不正な動作をさせられる。										
				2461.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。										
			2461P1	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。	2461P1-M1	接続先相手を限定する機能を導入する。			2461P1-M1C1	接続先相手を限定する機能が正常に動作するか、本来のシステムの動作に影響がないか検査する。	2461P1-M1O1	接続先相手を限定する機能が正常に動作するか、定期的に検査を実施する。	2461P1-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。
				247.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。										
				2471.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。										
			2471P1	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。	2471P1-M1	製品出荷時に単体でのウィルスチェックを行う。			2471P1-M1C1	竣工検査時にシステム全体でのウィルスチェックを行う。	2471P1-M1O1	システム全体のウィルスチェックを適宜行う。		
				248.侵入者にシステム内部を探られ、不正な操作をされる。										
				2481.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。										
			2481P1	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。	2481P1-M1	操作者、管理者などの権限管理できる機能を入れる。 操作者にはシステムの内部構造が見えないようにする。 データの閲覧や操作の権限を管理する。			2481P1-M1C1	共通：設計通りの機能が入っているか検査する。	2481P1-M1O1	権限管理が有効に機能しているか定期的に検査する。		

2.防災センター（中央監視室）

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)
	249.システムの脆弱性をついた攻撃を受ける。													
		2491.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。												
			2491P1	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。	2491P1-M1	適切なアップデートやパッチ適用が可能な機能を有する機器を導入する。			2491P1-M1C1	工場出荷前及び引渡し前に、その時点で脆弱性情報に対して、適切に対応できているか確認する。	2491P1-M1O1	脆弱性の情報を定期的に収集する。 USBタイプの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。	2491P1-M1R1	サービスされないソフトウエアが生じたら、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。
											2491P1-M1O2	脆弱性の情報を収集し、把握しておく。		
	2410.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。													
		24101.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。												
			24101P1	外部媒体等を安易に利用できないようにする。	24101P1-M1	利用しない空USBポートは治具でふさぐ。 ビルシステム主装置本体を施錠できるケースやラックに収納する。			24101P1-M1C1	利用しない空USBポートは治具でふさぐ。 現場搬入後、引渡しまで施錠管理を実施する。 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。	24101P1-M1O1	利用しない空USBポートは利用できない状態か、定期的に確認する。 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。		
			24101P2	外部媒体等を事前検疫してから利用する。					24101P2-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。	24101P2-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。		

3.機械室／制御盤ボックス

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)
30.機械室														
	301.所定の作業員以外による不正操作が行われる。													
		3011.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。												
			3011P1	機械室は施錠可能とする。	3011P1-M1	入退場者をシステムを使って登録・管理する仕組みを入れる。					3011P1-M1O1	入室可能な人員の登録・削除をタイムリーに行う。 登録・削除とも責任者によるダブルチェックを行う。 入室登録されていない人員が入室する際には、入室者の氏名・入退室時間を記録し、係員が常時付き添う。		
					3011P1-M2	施錠可能とする。					3011P1-M2O1	鍵の貸出・返却については(常時貸出を含む)、都度責任者の承認を得るものとし、氏名・貸出時刻・返却時刻を記録する。 鍵の紛失がすぐに気付く様式で鍵を保管する。 鍵を紛失した場合の報告・対応手順を策定する。 入室する際には、都度入室者の氏名・入退室時刻を記入する。 入退室に関する記録については、日々責任者が確認するとともに、年数回の監査を行う。 入室登録されていない人員が入室する際には、入室者の氏名・入退室時間を記録し、係員が常時付き添う。		
31.コントローラ（DDC、PLC等）														
	311.侵入者にシステム情報を探られ攻撃が拡大する。													
		3111.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。												
			3111P1	ログを適切に管理可能な機器・システムを導入する。	3111P1-M1	操作履歴、ログ情報の記録と解析の仕組みを導入する。 アクセスログを閲覧する権限を管理する。			3111P1-M1C1	共通：設計通りの機能が入っているか検査する。	3111P1-M1O1	操作履歴、ログ情報の記録と解析の仕組みが正常に機能しているか、定期的に確認する。 権限管理が適切に管理・運用できているか、定期的に点検する。		
		312.不正侵入に対する状況解析が困難で対策が遅れる。												
		3121.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。												
			3121P1	各種ログ情報の導入とログ解析の仕組みを導入する。	3121P1-M1	ログ情報取得システムを導入する。			3121P1-M1C1	設置端末全てに対してマルウエア対策を施す。 ログ取得、解析のシステムが動作していることを確認する。	3121P1-M1O1	必要に応じてログ情報の解析を行う。 アラーム発生時の行動指針を作成し教育訓練を定期的に実施する。	3121P1-M1R1	廃棄前に取得したログ情報を完全に消去する。 ログを何処で取っているか解析されないようにログ取得機能を消去若しくはオフする。 IPアドレスも予め定められた値に変更する。
	313.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。													
		3131.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。												
			3131P1	不正なアクセスや操作を確認する仕組みを入れる。	3131P1-M1	IDS（侵入検知システム）、UTM（統合脅威管理）等を導入する。 ログの取得、解析システムを導入し機器やネットワークの状態を監視する。			3131P1-M1C1	ネットワーク監視の仕組みが導入され正しく動作していることを確認する。	3131P1-M1O1	ログを必要に応じて解析し、異常の有無を確認する。 ネットワーク監視やログ解析により異常と判断されたときに実施する行動マニュアルを作成し教育訓練を行う。	3131P1-M1R1	ネットワーク監視機器の構成情報やログ情報は完全に消去する。
	314.不正な命令を実行してしまい、不正な動作をさせられる。													
		3141.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。												
			3141P1	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。	3141P1-M1	ネットワーク機器にホワイトリスト機能を導入し、不正な通信を排除する。	3141P1-M1B1	・ホワイトリスト機能は、工場試験時に設定を行い、機能が正常に動作するかどうかを工場段階で検査を行う。 ・上記設定にあたっては、交換予備機まで含める。	3141P1-M1C1	竣工検査時にホワイトリスト機能が正常に動作するか確認する。	3141P1-M1O1	納品物にすべての機器のMACアドレスリストを含める ネットワーク内の不正通信を常時監視する。		
	315.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。													
		3151.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。												
			3151P1	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。	3151P1-M1	製品出荷時に単体でのウィルスチェックを行う。			3151P1-M1C1	システム全体がマルウエア感染がないことを確認する。	3151P1-M1O1	脆弱性の情報を定期的に収集し、把握しておく。 適宜、システム全体がマルウェア感染していないことを確認する。		
	316.侵入者に容易にアクセスされ、不正操作をされる。													
		3161.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。												
			3161P1	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。			3161P1-B1	工場出荷時にデフォルトのID・パスワードから変更する。	3161P1-C1	竣工時にID・パスワードのリストを納入する。	3161P1-O1	運用時にID・パスワードのリストを適切に管理する。		

3.機械室／制御盤ボックス

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)
317.システムの脆弱性をついた攻撃を受ける。														
3171.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。														
			3171P1	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。	3171P1-M1	適切なアップデートやパッチ適用が可能な機能を有する機器を導入する。			3171P1-M1C1	工場出荷前及び引渡し前に、その時点で脆弱性情報に対して、適切に対応できているか確認する。	3171P1-M1O1	脆弱性の情報を定期的に収集する。 USBタイプの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。	3171P1-M1R1	サポートされないソフトウエアが生じたら、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。
											3171P1-M1O2	脆弱性の情報を定期的に収集し、把握しておく。		
318.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。														
3181.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。														
			3181P1	外部媒体等を安易に利用できないようにする。	3181P1-M1	利用しない空USBポートは治具でふさぐ。 HIM本体を施錠できるケースやラックに収納する。			3181P1-M1C1	利用しない空USBポートは治具でふさぐ。 現場搬入後、引渡しまで施錠管理を実施する。 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。	3181P1-M1O1	利用しない空USBポートは利用できない状態か、定期的に確認する。 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。		
			3181P2	外部媒体等を事前検疫してから利用する。					3181P2-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。	3181P2-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。		
			3181P3	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。					3181P3-C1	外部持込端末を接続する場合は、ウィルス検疫等確認したものに限る	3181P3-O1	外部持込端末を接続する場合は、ウィルス検疫等確認したものに限る。		
32.ネットワーク機器（ファイアウォール、ルータ、スイッチ）														
321.不正端末を接続され、マルウェアを送り込まれる。														
3211.空きポートが接続可能な状態で放置されている。														
			3211P1	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	3211P1-M1	スイッチ等の未使用ポートを物理的にロックする。 可能ならスイッチ等の未使用ポートを動作させない構成情報を導入する。 利用しているポートから容易にケーブルを抜かれないように物理的に保護する。 （ケーブルロックの仕組みの導入やポートがある機器は鍵付ラック内や高度セキュリティエリア内に設置する。） 空きポートが利用された場合、それを特定できるようにする。			3211P1-M1C1	ネットワーク機器の未使用ポートが利用できないことを確認する。	3211P1-M1O1	定期的に未使用ポートのチェックを行う。 未使用ポートを利用する場合の承認プロセスを確立する。		
33.ゲートウェイ機器														
331.不正な命令を実行してしまい、不正な動作をさせられる。														
3311.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。														
			3311P1	ネットワーク上に、通信先を制限する仕組みを導入する	3311P1-M1	MAC認証やIPアドレス制限を設ける。			3311P1-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。	3311P1-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。		
34.各種制御盤・分電盤														
341.所定の作業員以外による不正操作が行われる。														
3411.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。														
			3411P1	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。	3411P1-M1	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。					3411P1-M1O1	鍵の貸出・返却については(常時貸出を含む)、都度責任者の承認を得るものとし、氏名・貸出時刻・返却時刻を記録する。 特に、常時貸出者の異動に伴う鍵の返却は迅速に行うものとする。		

4.配線経路（MDF室、EPS、天井裏ラック）

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)
40.MDF室／EPS／天井裏ラック														
401.不正端末を接続され、マルウェアを送り込まれる。														
4011.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。														
			4011P1	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。	4011P1-M1	配線の縦ルート上に人の立ち入る保護区域を施錠管理とする。 【A：入室の個人特定が施錠管理で行なえる方式のIDカードで開錠する電気錠方式＋扉の開閉状態を監視可能とする（スイッチストライク）】 【B：（鍵の貸し出し管理）＋扉の開閉状態を監視可能とする（スイッチストライク）】 【C：施錠管理（鍵の貸し出し管理のみ）】	4011P1-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。	4011P1-M1C1	装置等に鍵などで施錠があるものは、施錠し引渡す。	4011P1-M1O1	設計・仕様に対応して、以下の方式で施錠管理を行う。 A：入室の個人特定が施錠管理で行なえる方式のIDカードで開錠する電気錠方式＋扉の開閉状態を監視可能とする。 B：（鍵の貸し出し管理）＋扉の開閉状態を監視可能とする。 C：施錠管理（鍵の貸し出し管理のみ）。		
					4011P1-M2	配線の横ルートで天井裏などの隠蔽場所に敷設する場合や機器を隠蔽場所に設置する場合は施錠可能な点検口を設ける。	4011P1-M2B1	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。	4011P1-M2C1	装置等に鍵などで施錠があるものは、施錠し引渡す。	4011P1-M2O1	施錠管理（鍵の貸し出し管理のみ）を行う。		
					4011P1-M3	ビルシステム主装置以降の縦配線は専用区画に配線する。 専用区画に機器（コントローラなど）を設置する。 【A：強電系配線と分離した施錠可能な専用EPSに配線し、機器を設置する】 【B：強電系配線と共用EPSに配線するが配線は配管・ダクト・蓋鍵付きケーブルラックに配線する。機器は収納盤に納め施錠する。】	4011P1-M3B1	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。	4011P1-M3C1	装置等に鍵などで施錠があるものは、施錠し引渡す。	4011P1-M3O1	専用区画の第三者アクセスの立ち入りを、事前申告を基に管理する。		
41.内部に置かれたネットワーク機器（スイッチ類）														
411.所定の作業員以外による不正操作が行われる。														
4111.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。														
			4111P1	適切に管理された専用の室、区画の中に機器を設置する。	4111P1-M1	サーバ類専用の室、区画を設け、機器を設置する。			4111P1-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。	4111P1-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。		
			4111P2	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。	4111P2-M1	機器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。			4111P2-M1C1	共通：設計通りになっているか検査する。	4111P2-M1O1	鍵の管理を適切に行う。		
412.不正端末を接続され、マルウェアを送り込まれる。														
4121.空きポートが接続可能な状態で放置されている。														
			4121P1	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。	4121P1-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。	4121P1-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。	4121P1-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を取付けが、決められた箇所にあるか確認する。 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。	4121P1-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。	4121P1-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。
					4121P1-M2	利用しない空きUSBポートは治具でふさぐ。	4121P1-M2B1	現場搬入後、引渡しまで防犯管理を実施する。	4121P1-M2C1	利用しない空USBポートは治具でふさぐ。	4121P1-M2C1O1	利用しない空USBポートは利用できない状態か、定期的に確認する。		
									4121P1-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。	4121P1-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。		

5.末端装置が置かれる場所

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)
50.末端装置														
	501.不正端末を接続され、マルウェアを送り込まれる。													
		5011.空きポートが接続可能な状態で放置されている。												
			5011P1	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。	5011P1-M1	やむを得ず、スイッチ類を設置する場合はスイッチ空ポートを治具(専用モジュラージャック）等であらかじめ塞ぐ。 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。	5011P1-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。	5011P1-M1C1	設計時の状態であるかの確認が行われ、空ポートにフィールドで試験などを行った状況がないか確認する。 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。	5011P1-M1O1	保守点検などでスイッチ類に対して作業が行われる場合は事前事後確認を行う。	5011P1-M1R1	一部の設備更新などの場合には事前に更新製品の仕様確認を行うこと。
	502.不正な命令を実行してしまい、不正な動作をさせられる。													
		5021.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。												
			5021P1	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。	5021P1-M1	利用者認証設定及び利用者ごとの利用権限設定を行う。 生体、IDカード＋パスワード等の認証機能を施す。	5021P1-M1B1	設営や構築時のID、パスワード等の漏洩がない様、厳重に管理を行う。	5021P1-M1C1	構築時のID、パスワードについては抹消したことを確認し、客先の要望する新たなID、パスワードを設定し引渡す。	5021P1-M1O1	不定期（人事異動）や定期的な認証方法の管理を行う（生体認証、IDカード管理、パスワード管理を行う）。	5021P1-M1R1	システム更新時には旧システムのパスワード体系を引き継がず新たな体系で行う。 廃棄機器については、ＩＤ、パスワード等の設定情報の抹消を行う。