ビル設備における
サイバーセキュリティ
セルフチェックシート
設問項目ガイド

CICS
Construction Industry and Cyber Security

2023年7月

独立行政法人情報処理推進機構
産業サイバーセキュリティセンター
中核人材育成プログラム　第６期生
建設業とサイバーセキュリティ

目次

第1章 はじめに

1.1. 本書の目的

住宅やオフィスビル、病院、道路、橋梁など私たちが毎日生活する上で様々な建築物や設備、インフラを利用しています。しかし、近年、サイバー攻撃技術の高度化に加え、様々なシステムがネットワークに繋がり発展していく中、2010年イランの核燃料施設へのサイバー攻撃として使用されたマルウェア「Stuxnet」の登場以降、制御システムへのサイバー攻撃のリスクも高まっています。私たちが日常的に利用し、照明や空調、エレベータなど多くの制御系機器を有するビル分野も例外ではなく、2016年ラッペーンランタでのDDoS攻撃による暖房停止や2021年ドイツのオフィスビルでのBAS機器ロック事件のように、ビルに対するサイバー攻撃も実際に発生しています。

本書は、「ビル設備におけるサイバーセキュリティ セルフチェックシート」の補足文章であり、各設問で問われている内容について、その設問の「背景・目的」、その設問が達成されなかった場合に「想定されるリスク」、その設問の解説やその設問を達成するための施策例を記載した「内容解説・施策例」の3項目で解説しています。

また、本書では、ビル分野、特にオフィスビルのビル設備におけるサイバーセキュリティの重要性を理解し、対策を検討・実施するために必須となる観点を整理しています。オフィスビルの設計や建設、運用に関わる様々な「ステークホルダ」と「ビルのライフサイクル（各段階・フェーズ）」におけるサイバーセキュリティ対策に焦点を当てた構成としています。

オフィスビルのライフサイクルを「設計・仕様」、「建設」、「竣工」、「運用」、「改修・廃棄」の5つと、どのフェーズにも共通する項目を加えて、計6つに分類しています。さらに、主なオフィスビルに関わるステークホルダを「発注者・ビルオーナー・ビル管理会社」、「設計事務所」、「建設会社（ゼネコン）」、「設備協力会社（サブコン）」、「メーカー・ベンダー」の5つに分類しています。

それぞれの段階・フェーズとステークホルダに対するサイバーセキュリティ対策を示すことで、読者にビル設備に必要なサイバーセキュリティの視点や知識を提供することを目指しています。

ビルのライフサイクルにおける段階・フェーズ

1. 共通
2. 「設計・仕様」段階
3. 「建設」段階
4. 「竣工」段階
5. 「運用」段階
6. 「改修・廃棄」段階

ステークホルダ

1. 発注者/権利者
   ・ビルオーナー・ビル管理会社
   :ビルの管理・運用を行う立場や、ビルの仕様変更や更新の権利を持つ会社に加え、ビルの利用者であるテナント入居企業
2. 設計事務所
   :ビルの設計（意匠・構造・設備）・監理を行う立場の会社
3. 建設会社(元請・ゼネコン)
   :ビル全体の工事を管理する立場の会社
4. 設備協力会社(サブコン)
   :ビルの設備工事の管理や、設備システムの工事・構築をする立場の会社
5. メーカー・ベンダー
   :ビル設備を構成する機器・システムを製造・販売する立場の会社

1.2. 対象とする読者

ビルのライフサイクル（設計・仕様検討から運用、廃棄まで）において、ステークホルダは、発注者であるビルオーナーや、設計監理を行う設計者、ビルの建設工事一式を請け負う建設会社（元請）以外にも、ビルを実際に維持管理する運用管理会社、そのビルを利用するテナント入居者と多種多様であり、業種も異なることが多いです。また、テナントオフィスビルにおけるC工事では、発注者はテナント入居者となることも多く、ビルのライフサイクル、その段階によって、ステークホルダも変化します。

そのため、ビルオーナー、ビル管理者、テナント入居者、ビル設計者、ゼネコン・サブコンの施工管理等の担当者、設備機器メーカーの開発担当者等 、ビルのライフサイクルに関わるステークホルダといった幅広い読者を対象としています。

1.3. 対象とする範囲

ビルには、大規模、中小規模といった規模による区分や、新築ビル、既存ビルといった建設・利用の段階による区分、さらにオフィスビルや商業施設、ホテル、病院などの用途による区分が存在します。これらの区分や条件、環境が複合的に組み合わさり、ビルが設計、建設、運用維持管理されているため、意匠、構造の設計や基準が異なるだけでなく、ビル設備の構成や運用管理体制、運用規模等の条件も異なります。 サイバーセキュリティ対策においても、条件が異なるビルに適用できる・実施すべきセキュリティレベルの判断は異なってきます。

利用区分・形態や条件により必要となるセキュリティレベルも異なってくるため、本書で対象とするビルは、事務所（自社オフィスビルおよびテナントオフィスビル）で、中央監視システムを導入しているビルとしています。
しかし、オフィスビルも店舗や飲食店が入居するような例も多く、このような複合オフィスビルに対しても、各種条件を踏まえて、セキュリティ要件を整理、検討するために本書を活用いただくことも想定しています。

本書の対象となるビル設備とは、建築基準法上の建築設備（建築物に設ける電気、ガス、給水、排水、換気、暖房、冷房、消火、排煙若しくは汚物処理の設備又は煙突、昇降機若しくは避雷針をいう。）としています。
また、上記ビル設備の管理・運用を行うための制御システム（OT：Operational Technology）であるビル設備システムとは、受変電制御システム、照明制御システム、熱供給制御システム、給排水制御システム、空調制御システム、昇降機制御システム、防災監視システムに加え、防犯・入館管理システム、監視カメラシステム、これらを統合的に監視・管理するための中央監視、統合管理システム（BAS：Building Automation System）等としています。

最近では、IoT機器を活用したスマートビル向けに「統合ネットワーク※」の取り組みが進んできています。本書では、テナントやビル利用者向けのサービスとして提供されるITシステムやOAシステムは対象外としていますが、全ての設備やセンサーが1つにつながる統合ネットワークの採用に伴い、利便性が大きくなる反面、BASに対するサイバー攻撃のリスクも大きくなると考えられるため、統合ネットワークを採用しているスマートビルにおいては、より一層の検討が必要です。

※統合ネットワーク：BA（Building Automation）ネットワークと一般のPCやWi-Fi等で利用するLAN・OA（Office Automation）ネットワーク等を統合したネットワーク

1.4. 設問ごとの対象

「ビル設備におけるサイバーセキュリティ セルフチェックシート」における各設問の対象となるステークホルダは、「発注者/権利者・ビルオーナー・ビル管理会社」、「設計事務所」、「建設会社（ゼネコン）」、「設備協力会社（サブコン）」、「メーカー・ベンダー」としています。
各設問で想定している主な読者、ステークホルダは以下の表1に示すとおりです。

ただし、以下の表1で「○」が付いていないステークホルダも業務形態や契約内容によっては、主体的に検討、実施する必要があったり、間接的もしくは副次的に関わることも想定されるため、留意が必要です。

表1：設問ごとの対象者一覧表　　【凡例】○：主な対象者として想定

段階	No.	対象者（ステークホルダ）				
		発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー
1.「共通」	1	○	○	○	○	○
	2	○	○	○	○	○
	3	○	○	○	○	○
	4	○	○	○	○	○
	5	○	○	○	○	○
2.「設計・仕様」	1	○	○			
	2	○	○			
	3	○	○			○
	4	○	○			○
	5	○	○			○
3.「建設」	1	○		○	○	
	2	○		○	○	
	3	○		○	○	
	4	○		○	○	
	5	○		○	○	○
	6	○		○	○	○
4.「竣工」	1	○	○	○	○	○
	2	○	○	○	○	
	3	○	○	○	○	○
	4	○			○	○
	5	○		○	○	
5.「運用」	1	○			○	○
	2	○			○	○
	3	○				
	4	○				
	5	○				
	6	○			○	○
	7	○				
	8	○				
	9	○				
	10	○				
	11	○				
	12	○				
	13	○				
	14	○				○
	15	○				
6.「改修・廃棄」	1	○	○	○	○	○
	2	○		○	○	
	3	○	○	○	○	
	4	○		○	○	○
	5	○		○	○	○

1.5. 本書の構成

第2章「設問項目ガイド」では、別資料の「ビル設備におけるサイバーセキュリティセルフチェックシート」記載の設問項目について、それぞれ内容を解説しています。セルフチェックシートの設問で不明な内容があった際や、より具体的な検討を行う際の参考資料として、ご確認ください。

また、付属資料として、本書作成にあたり参考とした資料・ガイドライン一覧の「参考資料」と本書で使用されている用語を説明した「用語集」の2つを付属しています。

1.6. 免責事項

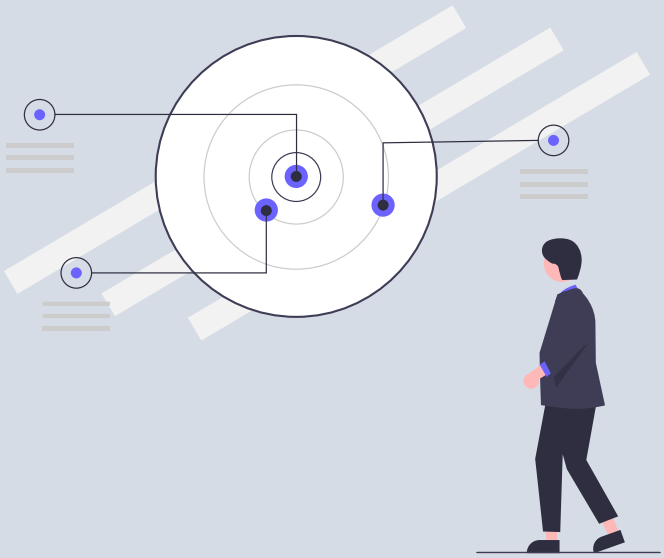
- 本書は単に情報として提供され、内容は予告なしに変更される場合があります。
- 発行元の許可なく、本書の記載内容を複写、転載することを禁止します。
- 本プロジェクトは、本書の使用に起因して生じるすべての直接的、間接的、付随的又は結果的損害、利益の損失等に関し、法的原因の如何を問わず何らの責任も負いません。

1.7. 注意事項

- 本書の内容は本プロジェクトの見解に基づいております。独立行政法人情報処理推進機構（IPA）および作成者の所属企業、本書の作成にご協力いただいた企業の見解を反映するものではありません。

第2章
設問項目ガイド

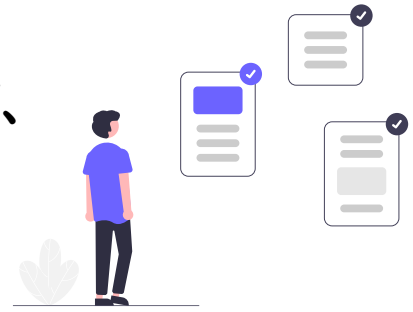
1. 共通
2. 「設計・仕様」段階
3. 「建設」段階
4. 「竣工」段階
5. 「運用」段階
6. 「改修・廃棄」段階



対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

サイバーセキュリティリスクに関して各関係者の役割と責任を明確にした上で、サイバーセキュリティリスク管理体制が構築されていますか？



■ 背景・目的

システム等のセキュリティインシデント発生時、迅速かつ的確に対応できることは、被害や損害を最小限に抑えることにつながるため、事前に事故時の対応体制・対応方法を明確化をしておく必要があります。
サイバーセキュリティリスクについて、ビルに関わるステークホルダそれぞれの役割と責任範囲を明確にした上で、ビル設備システムの状況監視やインシデント発生後に迅速な対応が取れる体制を構築すること大切です。
また、責任の所在が不明確であることが原因で起こる企業間のトラブルを防ぐ必要があります。

■ 想定されるリスク

サイバーセキュリティのインシデントが発生した際に、誰がどの範囲で責任を負うかが明確でなく対応が遅れることにより、利用者のビルに対する信頼性や世間からの社会的信用が失墜するだけでなく、ビルを安全に操業することが出来なくなる可能性があります。

■ 内容解説・施策例

サイバーセキュリティに関して各社・各組織において、その役割と責任を明確にすることは、ビルのライフサイクルマネジメントの観点から、効率的に維持保全・運用管理を行うために必要です。

各ステークホルダの役割と責任を明確にするための施策としては、第一にサイバーセキュリティリスク管理体制の構築があげられます。管理体制の構築にあたっては、以下のような施策があります。

- ビルオーナーやビル管理会社以外にも設計事務所や建設会社など、ビルのライフサイクルに関わる企業・関係者各々で、経営層、CISO（最高情報セキュリティ責任者）、戦略マネジメント層、システム担当者の役割と責任に基づき、組織一丸となった対応が必要であることを踏まえ、自社の実態に応じた体制を構築する。
- 内部統制を機能させる観点から、サイバーセキュリティ対策の有効性や報告に関する信頼性を確保するために、関係者それぞれの役割を体制内で明確化する。
- CISO等は、組織内全ての事業領域を包含したサイバーセキュリティリスク管理体制を構築し、それぞれの役割における責任範囲を明確にする。
- CISO等が、組織内に設置された経営リスクに関する委員会に参加する。
- 取締役、監査役はサイバーセキュリティリスク管理体制が適切に構築、運用されているかを定期的に監査する。
- サイバーセキュリティ対策遂行に求められる責任や専門性、人的資源の状況に応じて、「組織内の要員で対応すべきもの」と「外部の専門サービスに委託すべきもの」とで、切り分けを行う。
- セキュリティ・バイ・デザインの観点から、ビルの建設、運用・維持管理の体制構築においても、設計・仕様段階からサイバーセキュリティ対策を考慮し、運用・管理体制を構築する。

これら施策を各社・各組織で実施し、サイバーセキュリティ対策の責任主体を明確化することで、各社・各組織の自らが担うべき役割を理解し、対策漏れが生じないようにします。

加えて、自社や自組織内での責任範囲を明確化するだけでなく、サプライチェーンやビルのライフサイクルに関係する複数の企業・組織間での責任範囲についても明確化します。

さらに各社・各組織間の役割・責任範囲について、契約書やセキュリティポリシーにおいて文書化することは、組織内の構成員・職員への伝達だけでなく、客観的な評価を行うためにも有用です。客観的な評価により、現状の課題を解消する改善活動にも活かすことができます。

参考資料・ガイドライン

- サイバーセキュリティ経営ガイドライン（指示2：サイバーセキュリティリスク管理体制の構築）
  【経済産業省、（独）情報処理推進機構】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

ステークホルダ間で利用するITシステムやPC・スマートデバイス等の情報機器、図面等機密情報の取り扱いについて情報セキュリティポリシーに基づき対策を講じていますか？

■ 背景・目的

発注者と設計事務所、建設会社間で利用する情報共有基盤、クラウドシステムなどのITシステムやPC・スマートデバイスなどの情報機器には、計画書や企画書、BIM・CADで作成した設計情報、契約情報、財務情報など重要情報が保管されることが多く、これら機密情報の保護は必須です。

また、組織間の業務上の繋がりを悪用して次の攻撃の踏み台とするサイバー攻撃手法の「サプライチェーン攻撃」においては、セキュリティ対策が脆弱な取引先や委託先企業が標的となり、攻撃を受けます。特に異なる企業間で利用するITシステムや図面の取り扱い方法、機密情報のやり取りについては、事前に情報セキュリティポリシーを検討する必要があります。

■ 想定されるリスク

特に異なる企業間でITシステムを使用するケースにおいて、各社固有の情報セキュリティポリシーに従い、運用すると、一定の水準に達していない企業があった場合、その企業から攻撃を受け、設計情報や契約、財務情報などの機密情報に不正アクセスされ、情報漏えいにつながる恐れがあります。

中でもBIMデータなどの設計情報は設計・建設段階でより効率的に作業できるだけでなく、設計・建設中に作成された情報を記録して、ビルの運用・維持管理の業務にも役立ちます。
しかし、一度、設計情報が漏えいすると、建設するビルの入退室管理システムや、その方法、鍵管理などの物理セキュリティ対策、ビル設備システムの構成やアクセス制御方法、運用管理方法などの論理セキュリティ対策も漏えいし、ビルへの脅威増大につながります。

■ 内容解説・施策例

ビルを設計、建設し、維持管理するうえで、各ステークホルダ間で利用するITシステムや情報機器、図面等機密情報の取り扱いについて定めた情報セキュリティポリシーが必要です。

「情報セキュリティポリシー」は、組織全体での理念や指針である「基本方針」と基本方針を実現するための規則である「対策基準」、対策基準ごとに実施すべき対策の内容を手順として記載した「実施手順」の3つで構成されます。

情報セキュリティポリシーの策定手順は、業態、組織規模、目的、予算、期間などによって大きく異なりますが、代表的な策定手順としては、以下の手順があります。

1. 情報セキュリティポリシー策定の組織決定（責任者、担当者の選出）
2. 目的、情報資産の対象範囲、期間、役割分担などの決定
3. 策定スケジュールの決定
4. 基本方針の策定
5. 情報資産の洗い出し、リスク分析とその対策
6. 対策基準と実施内容の策定

また、特に複数の企業が1つの場所（施工現場および現場事務所）で作業する建設現場では、情報セキュリティを維持するための体制として、情報セキュリティマネジメントシステムを構築します。

情報セキュリティマネジメントシステムの構築フローは以下になります。

1. 情報セキュリティポリシーの策定
2. 情報セキュリティ管理体制の整備
3. 情報資産管理台帳の作成

建設現場の情報セキュリティ管理体制は、現場内の最高責任者である現場所長と現場所長が任命するセキュリティ責任者、セキュリティ担当者、およびその他現場の管理下で業務に従事する者で構成されます。

さらに、情報資産管理台帳の作成では、建設現場で業務上取り扱う業務情報全般、顧客や関係者の個人情報、PC、スマートデバイス、プリンタなどの情報機器全般（情報資産）を洗い出し、情報資産ごとに重要度を判断し、管理者・保管場所・現場閉所時の取扱い等を決定し、情報資産管理台帳として整備します。

構築した情報セキュリティマネジメントシステムが情報セキュリティ対策の実効性を確保していくためには、定期的に運用状況を確認し、改善を行っていくことが重要となります。

参考資料・ガイドライン

- 中小企業の情報セキュリティ対策ガイドライン 【（独）情報処理推進機構】
- 建設現場における情報セキュリティガイドライン 【（一社）日本建設業連合会】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

委託先・取引先等を含めたサプライチェーン全体のリスクを把握し、対策を実施していますか？

■ 背景・目的

委託先や取引先との関係において、セキュリティレベルを互いに確認し合うことは、セキュリティ対策が脆弱な取引先や委託先企業が標的となるサプライチェーン攻撃の脅威やサプライチェーンセキュリティを考える上で重要です。

組織としてリスクの程度や重要性を把握し、適切な対策ができるようになるため、サプライチェーン全体のセキュリティレベルを底上げすることができます。

■ 想定されるリスク

委託先や取引先とのサプライチェーン上で、サイバーセキュリティ対策が脆弱なところから個人情報や機密データの漏えいが発生するリスクがあります。情報漏えいが発端で、何らかの問題や損害賠償請求などの経済的な損失を負う可能性があります。

また、漏えいした情報を悪用もしくは、脆弱なセキュリティレベルの企業からビルの設備システムへ侵入を許してしまった場合、ビル機能を停止させてしまう危険性が高まります。

■ 内容解説・施策例

サイバーセキュリティにおける委託先等の取引先を含めたサプライチェーン全体の状況把握および、その対策として、実施すべき内容には以下に示すものがあります。

- グループ企業や委託先との取引、その連携先におけるサイバーセキュリティリスクへの対策状況を把握する。
- 委託先等サプライチェーン上の企業の合意のもと、各企業が実施すべきサイバーセキュリティ対策を定め、監査やその報告内容を通じて、その実効性を確認する。
- 委託先等の取引先との契約で合意したサイバーセキュリティリスクに関する役割と責任範囲に基づいて、適切な対策が講じられていることを確認する。
- 過剰な対策や形骸化した対策とならないよう、委託先等サプライチェーン内で扱う情報の機密性や重要性のランク別に実施すべき対策を決定する。

これら実施内容については、「単品受注生産」や「重層下請（ピラミッド）構造」と言った建設業界特有の事情や、サプライチェーン内での役割、相手先の対応能力等の状況に応じて、決定されます。

加えて、サプライチェーン上で発生するリスクについては、その発生確率と発生時の影響を定量的に評価し、その結果に応じて対策を定め、実行します。

特に事業影響の大きいリスク対策について、抜本的対策が必要になる場合は、経営・マネジメント層で実施する必要があります。

また、サプライチェーンにおけるサイバーセキュリティ対策について、委託先等取引先の対策状況の報告や、そのサプライチェーンを構成する各要素およびリスク状況の変化を継続的に監視し、異常を検知した内容から、リスク評価やサイバーセキュリティ対策の内容を見直し、改善を行います。

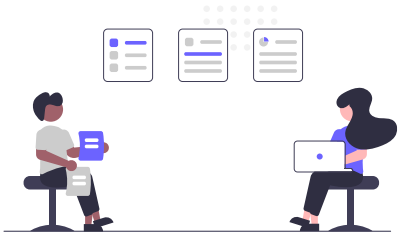
参考資料・ガイドライン

- サイバーセキュリティ経営ガイドライン（指示9：ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策 ）【経済産業省、（独）情報処理推進機構】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

サイバーセキュリティリスクやその取り組み状況について、情報を収集し、ビルに関わるステークホルダ間で情報共有を行っていますか？



■ 背景・目的

サイバーセキュリティ対策として、属する業界団体やセキュリティコミュニティから出される最新情報の収集や共有の重要性、必要性について、これまでも広く謳われています。
加えて、最新のサイバー攻撃被害を回避したり、被害を最小限に抑えるために、単独でこれらの情報を収集することは限界があります。

日々、高度化・複雑化する最新のサイバー攻撃手法に対抗するためには、ビルに関わるステークホルダ間で、サイバーセキュリティに関する情報共有ができる組織的な繋がりが必要です。

■ 想定されるリスク

情報共有に慎重な場合、他の組織や業界との情報交換が十分に行われず、新たな視点や攻撃手法に対する認識が不足する可能性があります。
ビル設備システムに対して予防策や適切な対策を実施することができず、サイバー攻撃を受けるリスクが増大する可能性があります。

■ 内容解説・施策例

サイバーセキュリティに関する情報（サイバーセキュリティリスクの近況やその取り組み・対策）を収集し、それらの情報を建設するビルに関わるステークホルダ間で、共有・開示を促進するためにの施策例としては、以下に示すものがあります。

- 情報の入手と提供、双方向の情報共有を通じて、社会全体・業界全体のサイバー攻撃の防御につなげ、情報を入手するだけでなく、業界団体のセキュリティ組織等で積極的に情報を提供する。
- ビルに関わるステークホルダとのコミュニケーションや、広報による一般向けの情報開示等の機会において、サイバーセキュリティに関する取組・対策状況の情報開示に積極的に取り組む。
- 「サイバー攻撃被害に関わる情報の共有・公表ガイダンス」を参考に、サイバーセキュリティ専門組織との情報共有や被害に関わる情報の公表を行う際の観点について、理解し、インシデント発生時に備える。※1
- IPA （独）情報処理推進機構や（一社）JPCERTコーディネーションセンター等による脆弱性情報や注意喚起情報、セキュリティ関連製品・サービスの事業者等とのコミュニケーションを自社のサイバーセキュリティ対策に活かす。
- CSIRT間における情報共有や、日本シーサート協議会、業界・業種内でのセキュリティ情報共有組織（ISAC）等のコミュニティ活動への参加による情報収集等を自社のサイバーセキュリティ対策に活かす。
- IPAに対し、告示（コンピュータウイルス対策基準、コンピュータ不正アクセス対策基32 準）に基づき、マルウェア情報や不正アクセス情報についての届出を行う。※2
- インシデント発生時、JPCERTコーディネーションセンターにインシデントに関する情報提供を行い、必要に応じて調整を依頼する。※3
- 中小企業の場合は、商工会議所、商工会等を通じて、地元・地域内で情報共有を行うことのできる相手を確保する。

参考資料・ガイドライン

- サイバーセキュリティ経営ガイドライン（指示10：サイバーセキュリティに関する情報の収集、共有及び開示の促進 ） 【経済産業省、（独）情報処理推進機構】

※文中URL
1. サイバー攻撃被害に関わる情報の共有・公表ガイダンス
   https://www.nisc.go.jp/pdf/council/cs/kyogikai/guidance2022_honbun.pdf
2. （独）情報処理推進機構 「届出・相談・情報提供」
   https://www.ipa.go.jp/security/outline/todoke-top-j.html
3. JPCERTコーディネーションセンター 「JPCERT/CCに依頼する」
   https://www.jpcert.or.jp/menu_reporttojpcert.html

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

設計変更やシステムの構成変更がある場合、その変更内容と手順が定められたサイバーセキュリティ要件・ポリシーに準拠していることを確認していますか？

■ 背景・目的

「設計・仕様」段階に関わらず「建設」段階、「運用」段階等、ビルのライフサイクルを通して、変更の大小はありますが、設計内容やシステム構成の変更は発生します。
そういった変更に際しては、どの段階においても一定のセキュリティレベルを維持するために、定めたサイバーセキュリティ要件・ポリシーに準拠しているかを確認する必要があります。

特に軽微な変更ほど、サイバーセキュリティ要件の確認を行わず適用するケースも考えられ、その1つの小さな変更が、システム全体に対する脆弱性を作り出し、サイバー攻撃につながることも考えられます。

■ 想定されるリスク

設計やシステム構成変更の内容がサイバーセキュリティ要件・ポリシーに準拠していることを確認せずに適用した場合、軽微な変更であったとしても、ビル設備システム全体の脅威につながるようなリスクを含んでいる可能性もあります。

特に、後付けで当初の設計にないIoT機器・センサー類を接続、設置することで、IoT機器からビル設備システムに対して外部からの侵入を許したり、内装工事で内壁のレイアウトを変更することで物理的にアクセス可能な範囲・エリアが意図せず拡大してしまうなど、ビルおよびビル設備システム全体のセキュリティに影響がないか注意が必要です。

■ 内容解説・施策例

設計やシステム構成を変更する際は、管理台帳やシステム構成図への反映や定期的な見直しを行い、最新の状態で管理していくことが、ビル設備システムを含む制御システムを理解するとともに、脅威や脆弱性の特定の一助にもなります。

また、その変更がビル設備システムの性能監視や遠隔監視を行うような変更・機能追加の提案である場合は特に、定めたサイバーセキュリティ要件・ポリシーを確認し、より慎重に判断する必要があります。

その提案がサイバーセキュリティ要件・ポリシーへの準拠が確認され、受け入れられたとなった場合でも、遠隔監視・操作ができるようになるとサービス不能攻撃（DoS）によるサービス停止や不正アクセスによるデータ窃取など、サイバー攻撃で悪用されうる攻撃対象領域（Attack Surface）が増える点に注意が必要が想定されます。

遠隔監視・操作機能を追加した際の対策確認の内容例としては、以下があります。
「設計・仕様」段階等、これまでに一度検討・実施されている内容の可能性もありますが、設計、システム構成の変更に伴い、再度、対策状況を確認し、ルールやポリシーの徹底を周知する必要があります。

遠隔監視・操作機能追加時の対策・確認例としては、以下に示すものがあります。

1. ファイアウォールを導入し、通信制御によりネットワークを分離（区画化）する。
2. 1.に加え、許可する通信を制限し、最小化する。
3. システムの操作者や操作可能範囲を限定する。
4. ID・パスワード管理を徹底させる。
   ID・パスワード管理例：
   1. 1つのIDを複数人で共用しない。
   2. 工場出荷状態の初期パスワードから変更する。
   3. 英大文字小文字+数字+記号を使った10桁以上のパスワードや推測されづらいパスワードを設定する。
   4. 複数のシステムやサービスで同じパスワードを使い回さない。
5. 一定時間経過後、自動ログアウトする機能を設け、ログイン状態を継続させない。
6. 上記1.～4.の内容が実際に機能しているか（通信制御が行われているか）を定期的に確認・検査する。

加えて、意匠設計、特に動線計画や物理セキュリティに関わる計画・設計が変更となれば、重要な機器が設置された室・空間には特定の人間以外はアクセスできないようになっているか警備・監視体制などの運用方法も含め、確認が必要です。

特に配線経路となるEPSやMDF・IDF室、空調機械室等が共用部に位置することも計画上多く、注意が必要です。

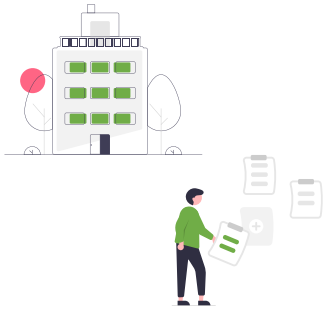
参考資料・ガイドライン

- Resilience and Cyber Security of Technology in the Built Environment
  【IET (The Institution of Engineering and Technology：英国工学技術学会)】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

建設するビルおよびビル設備システムのレジリエンスに関する要件について検討していますか？



■ 背景・目的

2011年に発生した東日本大震災以降、建築構造物やインフラに対するレジリエンス、BCP（事業継続計画）、BCM（事業継続マネジメント）に大きな関心が向けられるようになり、ビルオーナーやビルの管理者会社は、自然災害だけでなく人為災害も含めた災害全体のビル使用者への影響を最小限に抑える必要性があります。

また、耐震性、免震・制振構造のような建物の構造的なレジリエンス要件の検討以外にも、建物環境においてビル設備システムのレジリエンス要件についても検討が必要です。
ビル設備システムにおけるレジリエンスの必要性は、一般的にはビルの運用用途（一般オフィスビル、商業施設、病院、ホテル等）によって変わり、具体的な対策は、立地条件や事業の性質、規制・法的要件、事業への影響を考慮して検討されます。

■ 想定されるリスク

大地震等の自然災害が発生すると、建物自体の倒壊のような物理的な損傷の他、ビル内の電気、空調、衛生、通信設備が停止する可能性があります。
復旧不可能な損傷や障害、長期間の機能停止が発生すると、ビジネスそのものに対して大きな影響を及ぼす恐れがあります。
例えば、電気等の主要なビル設備システムが停止することにより、ビルの利用に支障が出るだけでなく、ビルの安全性やセキュリティに対するリスクが高まる可能性もあります。

また、人為災害により引き起こされた設備システムの停止でも、同じく、ビルの利用に支障が出たり、ビルの安全性やセキュリティに対するリスクが高まる可能性があります。

■ 内容解説・施策例

「設計・仕様」段階において、まず設計、建設するビル個別の用途の特性を考慮して、対象ビルの機能継続、レジリエンスに関わる目標設定を行う必要があります。

地震、台風等自然災害の多い日本において、高いレジリエンス性能を有する建物にするためには、耐震性や浸水への対応性確保に加え、災害等によりライフラインが途絶した際の対応性確保も必要です。
災害等でライフラインが途絶した際の対応性確保を行う方法として、代替機器等を考慮した設備計画や系統の設定など、以下に示すものがあります。

＜電気設備＞
- 防災用電源の活用（十分な防災用燃料の備蓄、間欠運転に耐える回路構成、系統電源供給の多重化、非常用発電と防災用発電の連携等）
- 太陽光等を活用した防災用電源による自立化

＜給排水・衛生設備（消火設備を含む）＞
- 水源多様化（防災用井戸、雨水利用等による自立化）
- 機能維持に有効な負荷低減（節水化、超々節水等）
- 排水機能の維持（排水の一次貯留、排水再利用等）

＜空調・換気設備＞
- 機能維持に有効な設備の負荷低減（電力を用いない通風・換気、パッシブデザイン等）

また、被災によるライフライン途絶時に対象ビルの機能を維持するためには、平時から以下の内容を検討し、準備が必要です。

- 建築物各部の点検および継続使用の可否を判断するための手順を明確化し、関係者に周知する。
- 軽微な補修・調整、被災部分の安全確保等に必要な資材等を備蓄する。
- 設備停止、ライフライン途絶に備え、適切な規模を備蓄する。
- 代替設備の運転、仮設電源・水源等の接続等の手順を明確化し、関係者に周知する。

上記の内容は、防災拠点となる建築物の対応例ですが、一般の共同住宅やオフィス等、防災拠点建築物ではない建築物・ビルでも、レジリエンス力の高いビル、被災後の継続使用・BCP（事業継続計画）等を考える上で、重要です。

参考資料・ガイドライン

- Resilience and Cyber Security of Technology in the Built Environment
  【IET (The Institution of Engineering and Technology：英国工学技術学会)】
- 防災拠点等となる建築物に関わる機能継続ガイドライン（新築版）【国土交通省住宅局】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

建設するビルおよびビル設備システムのサイバーセキュリティ対策の検討・企画に必要な要件について整理していますか？

■ 背景・目的

「2016年フィンランド・ラッペーンランタでのDDoS攻撃による暖房停止」や「2021年ドイツのオフィスビルでのBAS機器ロック事件」のように、建物、設備システムに対するサイバー攻撃も実際に発生しています。

ビルおよびビル設備システムに対する適切なサイバーセキュリティ対策を検討するためには、ビルの仕様を検討する段階で、適切なサイバーセキュリティ要件を整理することが重要です。

そこで、サイバーセキュリティ要件を整理するには、資産管理やアクセス制御などの防御技術の観点以外にも、サイバー攻撃の兆候を早期に発見する検知方法やインシデント発生時の対応方法、事業を継続、早期に回復させるための復旧方法を検討し、計画する必要があります。

また、サイバーセキュリティとレジリエンスに関する要件には依存関係があり、サイバーセキュリティ要件は、レジリエンス要件と合わせて検討する必要があります。

重大な障害や災害に対処できない場合、建物のサイバーセキュリティに対しても重大な影響を及ぼす可能性があります。

■ 想定されるリスク

サイバーセキュリティ対策を企画・検討するにあたり、必要な要件について整理できていない場合、実施するサイバーセキュリティ対策が不十分な内容になるだけでなく、過度な対策となるなど、重要度の高い設備・システムに対して、適切な対策を実施できない恐れがあります。

特にスマートビル等で採用される「統合ネットワーク」と呼ばれる複数のシステムが共通して利用するネットワークを採用した場合、サイバー攻撃・サイバーセキュリティについて検討していないビルでは、サイバー攻撃を受けた際、照明や空調と言ったビル設備システムの停止に留まらず、ITシステム側にも攻撃が及ぶ可能性があり、ビルの入居テナントが業務利用しているITシステム基盤への被害も想定されます。

■ 内容解説・施策例

建設するビルおよびビル設備システムのサイバーセキュリティ対策検討や企画に必要な要素は以下に示すものがあります。

1．経営目標等の整理

建設するビルの設備システムのサイバーセキュリティ対策に関わる経営・事業目標（事業拡張、事業継続等）がどのようになっているか整理します。

特に、事業継続計画（BCP）が策定されているかは重要であるため、その内容については確認する必要があります。もし、BCPがない、整備されていない場合、有事の際にビル利用者への影響が懸念されるため、担当部署とともにBCP策定を検討します。

BCPの策定にあたり、サイバー攻撃に対する対応や復旧計画の観点も重要です。

2．外部要件の整理

建設するビルの設備システムのサイバーセキュリティ対策に関わる外部要件（セキュリティ法規制、標準規格、ガイドライン準拠、国・自治体・業界からの要求、市場・顧客・取引先からや、サプライチェーン上の要求等）がどのようになっているか整理します。

また、外部要件の整理では、標準規格・ガイドライン等から、どのようなサイバーセキュリティ脅威・リスクがあるかについて、認識することが重要です。

3．内部要件/状況の整理

建設するビルの設備システムのサイバーセキュリティ対策に関わる内部要件（セキュリティポリシーなどの方針、システム面、運用・維持管理面、改修面等）や体制が、現状どのようになっているか、今後どのようにしたいかを整理します。

また、実際にビルの維持管理を行うビル管理会社まで含めたビルのサイバーセキュリティを進めていく上での体制が不明確である場合、この内部要件・状況整理の段階でサイバーセキュリティに対する考え方を整理し、サイバーセキュリティ対策を推進するための体制やルール・手順等を整備します。そして、それら整備した体制やルール・手順の内容から実施計画を立案し、関係各所に対して周知・教育等を行います。

参考資料・ガイドライン

- 工場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
  【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)工場サブワーキンググループ】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

建設するビルおよびビル設備システムに対するサイバーセキュリティを把握していますか？

■ 背景・目的

建設するビルとその設備システムに対して、最悪の被害・障害につながる災害などの環境的脅威や人為的脅威であるセキュリティ上の脅威、脆弱性を把握し、考えうるリスクを評価します。
そして、そのリスク発生への対応を検討することが必要です。

ビル設備システムへの脅威（自然災害によるライフライン途絶、マルウェア感染、不正アクセス、誤操作、内部不正など）、脆弱性（電源設備のメンテナンス不足、不適切なパスワード管理など）、影響度（高い、低い）を把握し、最終的なリスク対応を検討します。
その検討を通じて、各構成要素の対策優先順位を行うことで、必須で実施すべき対策や効果の高い対策を特定することができます。

■ 想定されるリスク

ビルやビル設備システムの構成要素（設備・ネットワーク機器等）に対する脅威・脆弱性の把握やリスク対策を行わない場合、受容できないリスクが残り、想定外の損失を被ったり、ビジネスそのものに対して大きな影響を及ぼす恐れがあります。
過度な対策により通常の業務遂行、運用に支障をきたすなどの不都合が生じる恐れもあります。

■ 内容解説・施策例

主にビル設備システムの稼働に影響を与える脅威の例としては以下に示すものがあります。

- 機器の盗難、システム・機器に対する破壊・不正操作

  物理侵入によるシステム・機器の破壊・盗難・不正操作、ネットワーク経由の侵入または内部からの不正通信を利用したシステム・機器の破壊・盗難・不正操作
- 設備の異常な制御や停止

  設備の不正な制御や停止、設備へ異常負荷をかけての停止、設備の安全制御機能停止
- データ盗難・漏えい

  USBメモリへの不正コピー、不正なサーバへのアップロード、パケットの盗聴
- データ改ざん・破壊

  データやプログラムの改ざん・消去、設定値の悪意ある変更、パケットの改ざん
- 可用性低下

  ネットワーク停止、リソース（ハードディスク容量、CPU処理速度、メモリ容量等）不足
- 外部への攻撃の踏み台として利用

  外部のサーバ/ネットワークへの攻撃
- システム・機器の障害・故障

  電源の停電・瞬断、電源設備および空調設備・通信機器・サーバ・PCの障害・故障
- 従業員、保守要員（設備ベンダ）の過失

  マルウェアに感染した機器の接続、設定/操作ミス
- 施設や作業環境の脅威

  漏電、火気不始末等による火災、近隣からの延焼、電磁波による電子機器の損傷
- 自然環境の脅威

  大雨・洪水による浸水・漏水、地震などによる機器の転倒・落下・損傷、落雷・洪水・地震による停電・瞬断、火災による機器・設備等の消失

また、各ビル設備システム資産に対する評価と攻撃者視点での実際の攻撃シナリオの評価の観点から、2つのリスク分析手法があります。

1． 資産ベースのリスク分析

保護対象となるビル設備システムを構成する各資産を対象に、その重要度、上記のような想定される脅威の発生可能性、脅威に対する脆弱性の3つを評価指標として、リスクを評価します。

2． 事業被害ベースのリスク分析

対象の事業やサービス（ここでは、照明・空調、監視システム等のビル設備）に対して、事業被害とそのレベル、事業被害を引き起こす攻撃手順の発生可能性、攻撃に対する脆弱性の3つを評価指標として、リスクを評価します。

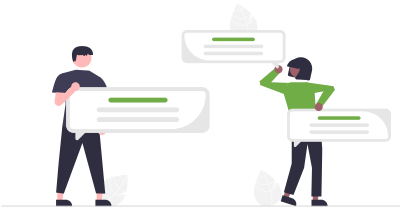
参考資料・ガイドライン

- 工場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
  【産業サイバーセキュリティ研究会 WG1(制度・技術・標準化)工場サブワーキンググループ】
- 制御システムのセキュリティリスク分析ガイド【(独)情報処理推進機構】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

ビル設備システムに対する脅威分析の結果や想定されるリスク等を考慮した上で、サイバーセキュリティ対策を検討していますか？



■ 背景・目的

サイバーセキュリティを考える上で、リスクがなくなることはなく、サイバーセキュリティ対策に充てられるリソース（費用・人員）も限られています。
そのため、サイバーセキュリティ対策には、限られたリソースの中でも、ある程度の網羅性を持ちつつ、重要度・優先度の高い対策から実施していくことが重要です。

サイバーセキュリティ対策として、運用方法や監査、インシデント管理・対応に関する「組織的な対策」や、従業員への教育や内部不正を防ぐための対応に関する「人的な対策」、機器の盗難、攻撃者の重要エリア侵入を防ぐための対応に関する「物理的な対策」、マルウェア感染や不正アクセスを防ぐための対応に関する「技術的な対策」を検討する必要があります。

■ 想定されるリスク

「設計・仕様」段階で検討されていない対策は、特に「技術的な対策」と「物理的な対策」はビル建設の工程が進むほど、対策実施が難しくなります。
また、設計する設備システムに対する脅威・脆弱性の分析やリスクの特定を行わない場合と同様に、それらに対するサイバーセキュリティ対策を検討しない場合、リスクの高い部分に必要な対策を講じられていなかったり、過度な対策となる可能性があります。

■ 内容解説・施策例

ビル設備システムのサイバーセキュリティ対策を検討するにあたり、初めにサイバーセキュリティ対策の方針を策定します。方針の策定後、これまで整理、把握してきたビルおよびビル設備システムに対する脅威・リスクをサイバーセキュリティ対策と結びつけながら、検討を進めます。

対象のビルや自社の置かれた環境、ステークホルダ等に応じて、対策の費用対効果も考慮しながら、必要なサイバーセキュリティ対策をより具体的に検討します。
対策内容としては、「組織的な対策」「技術的な対策」、「物理的な対策」、「人的な対策」の4つに分類され、以下に示すものがあります。

＜組織的な対策＞
- 運用、セキュリティに関するマニュアル・ルールの整備
- インシデント発生時の対応計画およびインシデント対応体制の構築
- インシデント発生後の復旧計画および復旧体制の構築

＜技術的な対策＞
- ネットワークの論理的・物理的な分割
- 通信データ制限：ファイアウォール（FW）、侵入検知・防止システム（IDS・IPS）の導入
- 利用者制限：ネットワーク機器やセキュリティ機器のID／パスワード、認証設定
- 通信監視・制御：通信状況可視化・監視、侵入検知システム（IDS）、侵入防止システム(IPS)の導入、フィルタリング
- 構成管理：接続機器の管理（OS・ファームウェアのバージョン、IP・MACアドレス、利用プロトコル、利用ポート番号）
- 脆弱性対策：機器やシステム、ソフトウェアに対する脆弱性情報の収集・診断、対策（ソフトウェア更新、パッチ適用等）
- ログ取得：ログ取得・連携、分析の仕組み、体制の構築
- セキュリティソフト、ウイルス対策ソフトの導入
- 外付けのセキュリティ機器の導入

＜物理的な対策＞
- 地震などによる機器の転倒・落下防止対策
- 不正侵入者や内部不正者による機器の盗難防止対策
- 盗難された機器により、ビル設備システムに侵入し攻撃されることを防止する対策
- 盗難された記憶デバイスにより、内部に保存された情報を利用されないための、データ暗号化などの仕組みの構築
- 不要なインタフェース／ポート(LAN、USB など)の物理的又は論理的な閉塞
- 防災センター（中央監視室）、電気室等の重要な構成機器を設置したや部屋への入室制限、入退管理システムの導入
- 監視カメラの設置
- 外部からの侵入だけでなく、内部からの侵入（内部不正）まで含めた管理・監視体制の構築

＜人的な対策＞
- 従業員や委託先など、ビルの運用・維持管理に関わる関係者へのセキュリティ教育・訓練

参考資料・ガイドライン

- 工場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
  【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） 工場サブワーキンググループ】
- ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン
  【産業サイバーセキュリティ研究会 ワーキンググループ1（制度・技術・標準化） ビルサブワーキンググループ】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

検討したサイバーセキュリティ要件や対策が、設計図書（設計図や仕様書）に記載されていますか？

■ 背景・目的

基本計画・基本設計段階では、発注者からの要望を聞いた上で、各種法規制や様々な条件を整理し、仕様書や基本設計図書、説明書を作成し、認識のすり合わせを行います。
その後、実施設計段階では、出来上がった基本設計をもとに、現場の施工業者が、工事に着工できるよう詳細部分まで設計を行うことで、最終的な見積と工事内容が確定し、建設会社との工事請負契約と自治体への建築確認申請が可能となります。

設計者は、発注者から提示されたサイバーセキュリティ対策要件をもとに、より具体的な対応策・実装策に落とし込み、これらの実装策を提供可能なメーカー・ベンダー等との調整を踏まえ、設計案として、発注者への提案や設計図書を作成する必要があります。

■ 想定されるリスク

検討したサイバーセキュリティ対策や要件が、特に実施設計の段階で、図面、仕様書等に記載されていない場合、その後の「建設」段階以降も対策が取られず、対策漏れにつながる恐れがあります。

図面や仕様書に示されていない対策、特に機器の盗難、攻撃者の重要エリアへの侵入を防ぐための入退室管理などの「物理的な対策」や、マルウェア感染や不正アクセスを防ぐための対策などの「技術的な対策」はビル建設の工程が進むほど、工期・費用の面からも対応、実施が難しくなります。

■ 内容解説・施策例

これまで検討してきたサイバーセキュリティ要件や対策について、設計者との打合せで認識合わせを行います。設計図書として設計図や仕様書に記載するサイバーセキュリティ対策の例としては、以下に示すものがあります。

＜物理的な対策＞
- 入退室を登録（事前および都度）して管理する仕組みを入れる。
- 物理的なバリア等を設け、許可された者以外が触れることを困難にする。
- 作業員の作業状況を常時監視する仕組みを入れる。
- サーバ類専用の室、区画を設け、機器を設置する。
- 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。
- 利用しない空USBポートやネットワークスイッチ等の空ポートは物理的に閉塞する。
- 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・ロックする。
- 配線の縦ルート上に人の立ち入る保護区域の施錠管理を行う。
- 配線の横ルートで天井裏などの隠蔽部に敷設する場合や機器を隠蔽部に設置する場合は施錠可能な点検口を設ける。
- ビルシステム主装置以降の縦配線は専用区画に配線し、専用区画内に機器（コントローラなど）を設置する。

＜技術的な対策（システム構成面での対策）＞

1. 全体管理策
   - 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、各管理設備の稼動履歴等、資産管理システムまた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。
   - 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定める。
   - ランサムウェアやサイバー攻撃の横展開に備え、オンラインバックアップだけでなく、オフラインバックアップ方法も定める。
   - 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、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。

2. ネットワークに関する対策
   - システムごとにネットワークセグメントを分離する。
   - 利用システムの動作上必要なネットワークセグメント間の通信は、必要な通信のみ許可する。
   - 外部ネットワークとの接続点にはファイアウォール（FW）を設置し、利用システムの動作に必要な最小限の通信のみを許容する。
   - 運用段階での引込回線を管理するため、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。
   - 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にデータの交換を行う。
   - アクセス制御の実装方式を検討し、設計に反映する。
   - 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上で発注する。
   - 接続端末を制限する仕組みを導入し、通常使用しないパケットの通信は許可しない。
   - 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、解析を行うシステムを導入し、機器やネットワークの状態を監視する。

3. 機器に関する対策
   - システムへのログイン管理等により、許可された者以外の操作を制限する。
   - 操作者を人単位で特定・限定できる機能（生体認証、IDカード、ID/PW等）を入れる。
   - ログ情報取得システムを導入する。
   - 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。
   - 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。
   - 保守用端末はその建物専用のものを納入し、ウィルス検疫やパッチなど適切に管理されたものを使用する。

参考資料・ガイドライン

- 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
  【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】

設問No.3-1

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

建設現場や現場事務所内でのPC・スマートデバイス等の情報機器や図面の取り扱いに関する情報セキュリティ教育を建設作業員向けに実施していますか？

■ 背景・目的

建設現場の情報セキュリティを維持するために、建設現場において「情報セキュリティ基本方針」を制定し、情報セキュリティ管理体制を整備し、情報資産を調査・分類した情報資産管理台帳を作成する必要があります。

また、建設現場にはゼネコンなどの元請施工者だけでなく、発注者や設計者、協力会社や資機材メーカー担当者等、多くの関係者が出入りします。それに加え、工事の進捗情況により関係者が入れ替わっていくため、一般的なオフィス環境よりも特に情報漏えいのリスクが大きいと言えます。
このような環境にある中、情報セキュリティ基本方針やポリシー、ルールを策定しても、それを利用する従業員・建設作業員がルールを守らなければ、被害が発生する確率は大きくなるため、情報漏えいの危険性や情報セキュリティの重要性を理解し、ルールを守るよう、従業員・建設作業員への徹底した教育が重要です。

■ 想定されるリスク

建設現場において情報セキュリティ基本方針やポリシーを定めても、従業員や建設作業員がその情報セキュリティポリシーを理解していない場合、図面等の機密情報や従業員・工事関係者の個人情報といった情報漏えいが発生する恐れがあります。
また、以下の建設業界の情報セキュリティ5大脅威を引き起こす原因としては、本人の認識不足やルール違反と共に会社側の教育・指導不足があげられます。事故の発生により、発注者の信用失墜や損害賠償などに繋がり、経営上の大きなリスクとなります。

建設業界の「情報セキュリティ」5大脅威

1. パソコン等の情報機器紛失・盗難
2. ブログ等SNSへの投稿による現場写真の漏えい
3. 図面等重要書類の紛失・盗難による情報漏えいと事故報告遅延
4. メール誤送信による図面データ等の漏えい
5. 標的型攻撃メールによるコンピュータウィルス（ランサムウェア）感染

■ 内容解説・施策例

建設現場内の情報セキュリティ最高責任者である現場所長または情報セキュリティ責任者は、発注者と締結した契約書の秘密保持や情報セキュリティ関連事項を確認し、その内容を協力会社との下、請負契約または委託先との業務委託契約の特記事項、条件書などに明記して契約を締結します。
そして、これらの内容について、情報セキュリティ教育を定期的・継続的に実施する必要があります。

情報セキュリティ責任者および情報セキュリティ担当者の役割として、現場構成員である元請職員や建設現場作業員等、建設工事関係者全員に対して、朝礼、定例会議、協議会等において、情報セキュリティ教育を年1回以上の頻度で実施することがあげられます。

主な教育内容
- （各社の）情報セキュリティポリシー概要
- 建設現場でのセキュリティの必要性
- 現場事務所のルール、手順
- 情報セキュリティ事故の事例やその対応方法と再発防止策
- 利用者が行うこと、行ってはいけないこと

教育方法として、日本建設業連合会発行の動画コンテンツやリーフレット、ポスター等が活用できます

- 情報セキュリティに関するガイドライン・教育資料集
  https://www.nikkenren.com/kenchiku/ict/security/guideline.html
  【（一社）日本建設業連合会 ICT推進部会 情報セキュリティ専門部会】

また、情報セキュリティ責任者の役割として、上記の関係者への教育以外にも、「協力会社・委託先が情報セキュリティ基本方針に基づき、情報セキュリティに関する具体的なルールや手順を遵守できるかのチェック」があります。
基準を満たしていない場合は、協力会社や委託先に対し改善要求を行い、対応状況を確認する必要があります。

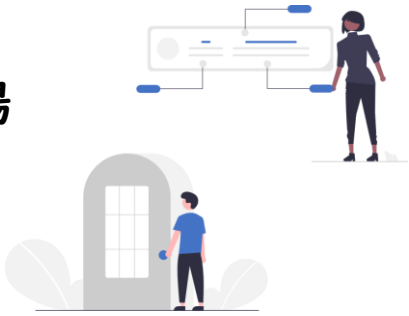
参考資料・ガイドライン

- 建設現場における情報セキュリティガイドライン【一般社団法人 日本建設業連合会】
- 元請会社における情報セキュリティガイドライン【一般社団法人 日本建設業連合会】
- 協力会社における情報セキュリティガイドライン【一般社団法人 日本建設業連合会】
- 建設業界の「情報セキュリティ」5大脅威
  https://www.nikkenren.com/kenchiku/ict/security/movie.html#a1

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

建設現場に出入りする業者・作業員に対して身元確認や建設現場への入退場管理を行っていますか？



■ 背景・目的

建設現場では、現場監督が現場を管理し、その配下で様々な専門技術を持った作業員が集まり、工事を進めていきますが、工程により必要な技術が異なるため、建設工事期間中は様々な会社に所属する作業員が出入りします。

業者・作業員に対して、身元確認や建設現場への入退場管理を行う目的として、建設現場では危険を伴う作業もあり、現場監督は一人ひとりの安全を確保するために現場で作業を行っている作業員を特定し、作業員情報を管理することがあげられます。
しかし、部外者が建設現場に侵入した際に、機器の窃盗・盗難や事故の他、サイバー攻撃につながる行為を防止することも建設するビルおよびビル設備システムに対するサイバーセキュリティ対策として、重要な項目となります。

■ 想定されるリスク

建設現場への入退場を管理していない場合、部外者が容易に建設現場に出入りでき、現場で利用する機材・機器の窃盗、設計・工事情報の漏えいにつながる恐れがあります。

また、悪意を持った部外者に加え、特に注目度の高い建設プロジェクトの場合、建設現場に出入りする業者の中に攻撃者が紛れていることも想定されます。
そういった攻撃者が建設現場内に侵入することにより、情報漏えいの他、現場で利用している仮設システムや本設の設置済み機器・システムに対して、不正操作や不正デバイスの接続を行ったり、運用段階でサイバー攻撃を行うための下準備を行うことも考えられます。

■ 内容解説・施策例

入退場管理の業務負荷とコストは大きいですが重要です。管理方法は、就労届や作業員名簿、入館証などで作業員の身元確認を実施する方法と顔認証等生体認証システムを用いたデジタル管理もあります。

さらに重要な機器や設備の設置作業実施時は必ず元請社員やサブコン社員の立会いを行うとより強固になります。
注意点として、建設現場へ不定期に入場することになる搬入業者やベンダー関連業者は抜け漏れが生じやすいので気を付ける必要があります。
また、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）などを取り締まります。

現場事務所内においても、必要な情報セキュリティレベルによって分類し、その分類に応じて対策を実施します。

- 情報セキュリティエリアの分類（例）

	分類	必要な対策	例
レベル1 エリア	入室（館）の抑止機能があり、かつ無断入室（館）禁止表示等により、第3者の立ち入りが制限されているエリア。	利用目的を明確にする。エリア出入り口に無断入室禁止等の表示を行う。	現場事務所内の共有スペース、会議室、応接室等。
レベル2 エリア	従業員以外の出入りが禁止されているエリア。 もしくは常時施錠されたキャビネット・引き出し等。	部屋の場合は、原則的に常時施錠する。専用の部屋でない場合は、必ずパーティションなどで区分けをし、従業員が常駐・監視して、従業員以外の出入りを禁止する。 キャビネット・引き出しの場合は常時施錠する。	従業員の執務スペースや、施錠されたキャビネット・引き出し等。
レベル3 エリア	アクセス権限が規定され、かつ許可された者以外が利用する場合はアクセス記録が取られている常時施錠のエリア、書庫・金庫等。	入室する者が限定された部屋では、常時施錠し、その鍵は特定の個人が管理する。限定された者以外が入室する場合はアクセス記録を取る。書庫・金庫の場合も常時施錠し、その鍵は特定の個人が管理する。	施錠された所長室や、書庫・金庫等。

【出典：建設現場における情報セキュリティガイドライン　3. 1現場事務所のエリア分類と情報セキュリティ対策】

また、建設現場も、現場事務所と施工場所が同じ敷地内にある場合もあれば、別々の場所にある場合もあります。
特に、現場事務所と施工場所が別々の場所にある場合では、詰所と呼ばれる建設作業員の休憩・待機所や会議室が施工場所の敷地内に仮設で用意されることが多いです。
詰所でもPCやスマートデバイス、プリンタ等の情報機器を使用するため、現場事務所内と同じく、セキュリティレベルに応じて扉やキャビネット、ロッカーを施錠するなどして、機器の盗難や情報漏えいに注意する必要があります。

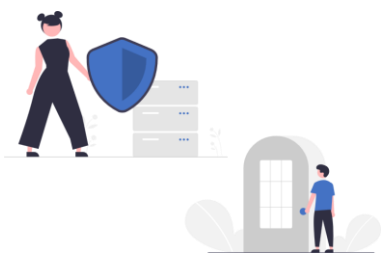
参考資料・ガイドライン

- 建設現場における情報セキュリティガイドライン【一般社団法人 日本建設業連合会】
- 元請会社における情報セキュリティガイドライン【一般社団法人 日本建設業連合会】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

ビル設備機器設置後やシステム導入後、ビル設備機器設置箇所の施錠および鍵管理、入退室管理を行っていますか？



■ 背景・目的

防災センター(中央監視室)や電気室内にはビル設備システムを制御・設定するための重要な機器が設置されています。

また、ビル設備システムを制御・設定する機器が設置された、これらの室内では保護すべき機密情報が取り扱われている場合も多くあります。
「運用」段階からだけではなく、「建設」段階においても、ビル設備システムの制御機器への許可されない操作や機密情報の漏えいを防止するために、なるべくビル設備システム設置後から、防災センターや電気室の扉や機器を設置したラックの扉は施錠し、各室への入退室は許可された者のみに制限することが重要です。

■ 想定されるリスク

建設段階でも、悪意を持った者が防災センター（中央監視室）や電気室内に入室すると、防災センターや電気室内の機器への物理的アクセスが可能となり、不正操作や情報漏えい、機器の物理的破壊、盗難などの被害を受ける恐れがあります。

また、関係者以外の人間が防災センターや電気室内に入室することにより、不用意な操作や変更、不正デバイスの設置などが行われ、「運用」段階に入ってビル設備システムの操業に影響を及ぼす可能性があります。
その結果、ビル設備システムの異常動作や停止などの事態に陥る恐れがあります。

■ 内容解説・施策例

特に「建設」段階における防災センター(中央監視室)や電気室のようなビル設備システムを制御・設定するための重要な機器が設置される室・空間に必要な対策としては、以下に示すものがあります。

- 就労届や作業員名簿、新規入場者アンケートにて、作業員の身元確認を実施した上で、作業実施時は必ず元請社員の立会いのもと行う。

- 重要な機器が設置される室・空間の入退室を制限するために物理的な鍵や電子錠で施錠管理を徹底する。

  電子錠はカードキー、バイオメトリクス（指紋認証や顔認識など）、パスコードなどの認証手法があります。

- 重要な機器設置後の室・空間への入退室管理ルールが変更となる場合、現場入場中の作業者や新規入場者に対して周知するようにする。

- 重要な機器が設置される室・空間への入退室は、ITシステムまたは紙等の管理台帳において、入退室者の識別結果、入退室時間等を元請社員等の管理者が記録できるようにする。

- 重要な機器が設置される室・空間が施錠可能な状態から機器の設置を行うことが望ましいですが、建設工程の問題上、扉の施錠が難しい場合、部外者が簡単に入れない、もしくは、重要な機器まで到達できない・触れられないような仕組みを構築する。

  機器設置後、設置した室の扉がまだ取り付けられていない、扉の締め切りができないような場合の代替策として、以下のような施策例があります。

  - 制御盤やラックの扉だけでも施錠する
  - 機器の空きポートは設置時までに閉塞しておく
  - 事前開封が行われたかの有無を確認できる梱包で保管しておく
  - 定期的な現場巡回を行う
  - 仮設の監視カメラを設置する

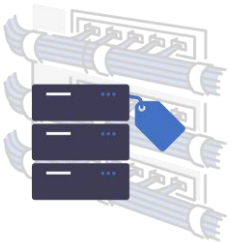
参考資料・ガイドライン

- 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
  【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】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

ビル設備システム機器が情報系システム機器等の別システムの機器と同じラックに設置されている場合、各機器がどのシステムのものであるかを（タグやシールなどで）分かるようにしていますか？



■ 背景・目的

サーバ室や異なるシステムのサーバラックが混在し、多くの機器が設置されている環境では、機器やケーブルの取り違えが発生する恐れもあります。
このような環境下で、システムメンテナンスや機器更新を行うと作業ミスが発生しやすくなり、システムの安全性、および可用性に影響する大きなリスクとなる恐れがあります。

ITシステムのネットワークには、一般利用者が日常的に使用するPC などのウイルス感染リスクの高い機器が接続されています。
ITシステムのネットワークにビル設備システムを含む制御システムが誤接続されると、情報系システムネットワーク内のウイルス感染した機器から、接続した制御システムがウイルスに感染し、システムの運転に影響を及ぼす恐れがあります。

機器設置の段階から、ビル設備システムの構成機器やネットワークケーブルには、タグやシールなどラベルを取り付け、ビル設備システムの機器であることを明示し、ITシステムと間違われないよう、注意喚起することで、誤接続を防ぐ効果があります。

■ 想定されるリスク

システムメンテナンス・機器更新時に他システムとの混同が原因で、誤操作や誤接続が行われると、照明や空調と言ったビル設備システムが停止したり、動作に異常が発生したりする可能性があります。

また、ビル設備システムがITシステムのネットワークに誤接続されると、ビル設備システムの機器がウイルスに感染し、ビル設備システムの運転に影響を及ぼす恐れがあります。

■ 内容解説・施策例

特にビル設備システム機器が情報系システム機器等の別システムの機器と同じラックに設置されている場合における、「建設」段階から誤操作・誤接続を防止する対策として、以下に示すものがあります。

1. 別ラックに分割して設置および施錠管理を行う
   管理区分(ITシステム、電力制御・空調制御のビル設備システムなど) ごとに別の場所や別ラックに搭載し、別々の鍵で施錠管理します。
   場所・ラックを物理的に分離し、機器への物理的アクセスを制限することで、誤接続などの人為的ミス防止以外に物理的なアクセス権の区分が可能です。
   ただし、設計内容によっては、物理的に別の場所での管理や、異なるラックを設置することが、難しい場合もあるため、「設計・仕様」段階等、あらかじめ検討しておくことが重要です。

2. ラベル表示を行う
   電力制御・空調制御などのビル設備システムの機器やケーブルであることを、タグやシールなどのラベルで表示、明示します。ラベルの内容として、「無断操作禁止」などと記載すると、作業員に対する注意喚起にもつながります。
   また、「建設」段階における管理者（元請職員、サブコン職員）の連絡先や異常時の対応方法を記載し、無断操作や不正操作を防止します。
   ラベルには、赤色系などの注意を引く色を使用するとより効果的になります。

3. 空きポート・端子を閉塞する
   作業員による誤接続や悪意を持った者からの不正端末接続を防止するために、空きポートや空き端子は、物理的に閉塞します。
   また、ラベルには「接続禁止」などと表示し、取り付け、注意喚起を行います。

4. 電源スイッチなどのスイッチ類を封印する
   電源スイッチなどの誤操作を防止するために、ラベルなどを使用し、注意喚起を行います。
   また、ラベルには「操作禁止」などと表示し、取り付けるとより効果的になります。

5. ネットワークケーブルの色分けを行う
   システム構成や物理配線の状況にもよりますが、物理的に別々の場合やVLAN等で仮想的にネットワークが分離しているような場合でも、接続するネットワークごとに違う色のケーブルを使用することで、誤接続を防止します。

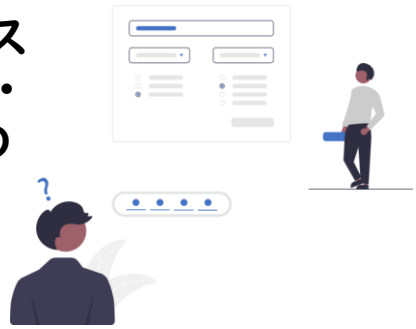
参考資料・ガイドライン

- J-CLICS STEP I／STEP2（ICSセキュリティ自己評価ツール）
  【JPCERTコーディネーションセンター（JPCERT/CC）】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

ビル設備システムや機器のログインパスワードについて、定められたパスワード・ポリシーに従い、出荷時（デフォルト）のパスワードから変更していますか？



■ 背景・目的

ビル設備システムを含む制御システムに限らず、PCや制御装置などの多くは、パスワードによって厳重に管理され、システムへの不正アクセスを防止するための対策が施されています。

一方、制御システム関連の機器は構成上複雑な認証システムを導入・構築することが難しいことも多く、パスワードさえ分かれば、システムへのアクセスが可能となり、重要なデータの読取りや制御装置を不正にコントロールできる可能性があります。特に攻撃者はシステム全体にアクセスできる管理者用のパスワードを狙い、不正アクセスを試みます。
ビル設備システムを含む制御システムやルーター、ネットワークスイッチといったネットワーク機器のパスワードおよびパスワードの管理は対象システムへの攻撃を防ぐために、強度の高いパスワードの設定や運用方法などを定めたパスワード・ポリシーを策定することが重要です。

また、機器出荷時のパスワードがそのままの状態であった場合（デフォルトのパスワードのまま）、機器のメーカーホームページ等、出荷時のパスワードがインターネット上で公開されていることも多く、容易に推測される恐れもあり、パスワード・ポリシーに準拠した内容で、新しいパスワードに変更しておくことが重要です。

■ 想定されるリスク

パスワード・ポリシーが策定されていない場合、パスワードの適切な設定や管理が行われず、特に簡単なパスワードは推測されたり、漏えいしているパスワードリストを利用した辞書攻撃や総当たり攻撃のリスクが高くなります。

パスワードが漏えいすると、ビル設備システムに不正アクセスされ、操業データなどの重要な情報を盗み取られたり、ビル設備システムのプログラムコードや設定値（パラメータ）を書き換えられたりする恐れがあります。
その結果、空調の設定温度の変更や電力の供給停止等、ビル設備システムの挙動が不正に変更され、システムが停止すれば、莫大な損害が発生する可能性があります。

■ 内容解説・施策例

通常、システムの設定変更や接続変更は、管理者のみが行うようにしますが、管理者パスワードは、デフォルト値から変更せずに使用していると、容易に攻撃されてしまう恐れがあるので、変更することをお奨めします。

「設計・仕様」段階のなるべく早い段階で、ビル設備システム含む制御システムで使用するパスワードの設定、変更などの管理方法について、パスワード・ポリシーを策定する必要があります。策定したパスワード・ポリシーについては、「建設」段階において、確実に実施・遵守されていることを確認する必要があります。

ただし、「設計・仕様」段階でパスワード・ポリシーを要件として盛り込んでおくことが望ましいですが、既存ビル等、既に運用されているビルでは、システムの仕様や運用状況などの理由でパスワード・ポリシーが適用できない場合が考えられます。その場合、入退室管理や施錠管理などの物理セキュリティ施策を強化して、許可されない人員の物理アクセス面からシステムを保護します。

1. パスワード・ポリシーの作成
   パスワード・ポリシーを策定し、文書化します。パスワード・ポリシーの内容例として、以下に示す要件があります。

   ① 以下の条件を満たすパスワードを使用する。
   - 覚えられる文字列を使用する。(メモなどを参照しなければ入力できないような文字列は使用しない。メモが漏えいするリスクがあります。)
   - 一般の辞書に記載されている文字列(英単語、辞書に記載されている単語のローマ字表記など)やパスワード設定に多く使用される文字列(例:password、qwerty)などは使用しない。
   - パスワード設定する当人に関係し、他人も容易に知り得るような情報(名前、誕生日、電話番号、車のナンバーなど) から推測できる文字列を使用しない。
   - 英小文字、英大文字、数字、記号(例:@, !, #, $)の4 種類を組合せた文字列を使用する。
   - 可能な限り文字列を長くする(10文字以上推奨)。但し、対象機器に設定できるパスワードの最大長が10文字未満の場合は、最大長の文字数とする。

   ② パスワードを他人に教えたり、共有したりしない。

   ③ パスワードは使い回さない。(複数のシステムで同じパスワードを設定しない。)

   ④ パスワードが他人に知られた可能性がある場合(流出時)、即時変更する。

   ⑤ 管理用パスワードは機密情報として厳重管理を徹底する。

2. パスワード・ポリシーの遵守
   従業員等システムを利用する職員がパスワード・ポリシーに記載された内容を理解し遵守する。

   ① パスワードの設定ルールの遵守

   ② パスワードの有効期限の遵守

   ③ パスワード情報の管理方法の遵守

   ④ 技術的施策の実施

   ⑤ パスワード・ポリシーに関する啓発・教育の徹底

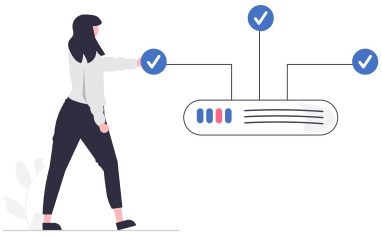
参考資料・ガイドライン

- J-CLICS STEP1／STEP2(ICSセキュリティ自己評価ツール)
  【JPCERTコーディネーションセンター(JPCERT/CC)】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

事前にビル設備システムネットワークに接続する機器がウイルスに感染していないことを確認していますか？



■ 背景・目的

USBメモリやハードディスク、CD、DVD、磁気テープなどの記録媒体、またはノートPCやスマートデバイスなどの情報機器は、ウイルス感染のリスクがある経路となる可能性があります。

近年、これらの機器を通じて、感染が広まるケースが増えており、特にビル設備システムを含む制御システムを標的にしたウイルスも確認されています。
そのため、ビル設備システムやビル設備ネットワークに機器を接続する際には、あらかじめウイルスチェックなどの手順を定め、実施し、注意を払うことが必要です。

■ 想定されるリスク

ビル設備システムの機器がウイルスに感染すると、ビル設備システムの運用に重大な影響が及び、業務停止などの深刻な問題が生じる可能性があります。

ウイルス感染によって、機密情報の漏えいやシステムおよびデータの損傷などの被害を受ける危険性が存在します。さらに、ウイルスの駆除には、システムの停止や再インストールなどが必要になる場合もあり、企業にとって膨大なコスト負担が発生します。
その結果、企業イメージやビルのブランドイメージが低下する可能性もあります。

■ 内容解説・施策例

制御システム、ITシステム問わず、接続される機器は、所定のウィルス対策・検疫を受けたもののみとルールを決める必要があります。
また、工場出荷前にウィルス検疫を実施するなど、ビル設備システムのネットワークに接続する前までには、これから接続する機器がウイルスに感染していないことを証明、確認する必要があります。

さらに、ウイルス対策例としては、以下に示すネットワーク経由での感染対策、持込み媒体経由での感染対策、制御システムPC上での対策などの施策があります。
ウイルス対策の方法によっては、システムの動作に悪影響を及ぼす可能性がありますので、対策の計画、実施にあたっては、制御システムベンダに問い合わせて、ベンダの推奨する方法で行うことをお奨めします。

1．ネットワーク経由での感染対策
　ネットワーク経由でのウイルス感染を防止する対策として、不要なネットワーク接続の除去、常時使用しないネットワーク接続の切断（ネットワーク機器の電源OFF など）、ファイアウォールの設置や設定強化などがあります。

2．持ち込み媒体経由での感染対策
　USB メモリや持ち込みPC経由でのウイルス感染を防止する対策として、媒体持ち込みの制限、媒体内の不要なファイルの削除、持ち込み時のウイルスチェックなどがあります。

3．制御システムPC上での対策
　制御システムPC上でのウイルス対策として、機器の施錠管理、不要接続ポート（USB ポートやネットワークポート）の閉塞、常時使用しない機器の切断（電源OFF など）、ウイルス対策ソフトの導入、アプリケーションホワイトリストの設定、OS やソフトウエアのアップデート・設定強化などがあります。

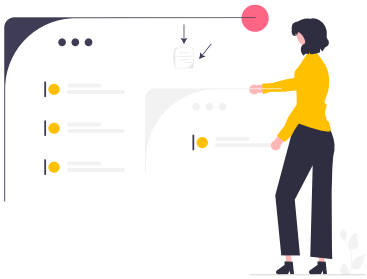
参考資料・ガイドライン

- J-CLICS STEP I／STEP2（ICSセキュリティ自己評価ツール）
  【JPCERTコーディネーションセンター（JPCERT/CC）】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

ビル設備ネットワークに接続している機器（サーバ、クライアント端末、ネットワーク機器等）の管理台帳とシステム構成図が作成されていますか？



■ 背景・目的

ビルの維持管理やビル設備システムに関連したビジネスリスクの発生回避、また発生時の迅速な対応のためには、ビジネスリスクをもたらす要因を正確に分析・評価し、適切な対応策を検討・実施することが重要です。
そのためには、ビル設備システムのシステム構成を把握し、定期的にビル設備システム（OSやソフトウエアを含む）の棚卸と評価を実施します。

そして、どんなシステムが存在しているか、機能や重要な業務、設置場所、所有者、サポート担当者などを記載した管理台帳を作成し、竣工時の最新状態を管理しておくことが重要です。

システムの最新の状態が管理されていると、「運用」段階において、想定されるリスクに対するサポート担当者への迅速な対応や早期復旧方法を把握でき、ビジネスリスクを最小限に抑えることができます。

■ 想定されるリスク

ビル設備システムの管理台帳・システム構成図がない、または最新の状態で管理されていない（システム構成への変更を管理台帳に反映してない）場合、停電、故障、地震、火事のような障害・災害（自然災害のみならず、不正アクセスなどの人的災害を含む）への対策が不十分となる恐れがあります。
また、システム構成変更時に本来不要な対応が発生したり、不具合発生時に原因追求までの遅延や対策漏れなどにより、ビジネスそのものへ大きな影響を及ぼす恐れがあります。

■ 内容解説・施策例

竣工引き渡し時までに現地の機器設置や配線の状況を踏まえ、ビル設備ネットワークに接続している機器（サーバ、クライアント端末、ネットワーク端末）など構成要素を洗い出し、管理台帳、システム構成図、データフロー図等を作成します。

ビルの規模や設計にもよりますが、ビル設備システムを構成する機器の数は大量になることも多いため、資産管理ツールなどのツール・システムを用いて自動的に資産管理する方法が望ましいです。ただし、各種要件等により、手作業による台帳作成や資産管理を行う際は、機器の確認に時間を要することや、確認漏れが発生する可能性があることに留意が必要です。

資産管理台帳に記載する情報として以下のような項目があります。

- 機器、ソフトウエアの管理 責任者（資産の所有者、管理者名など）
- 機器、ソフトウエアの形態（形式、バックアップメディア、ライセンスなど）
- 機器、ソフトウエアの接続状況（使用インターフェース、IPアドレス、MACアドレス、接続機器名、接続図、VLAN設定情報、通信ポート、通信プロトコルなど）
- 機器、ソフトウエアにおける変更記録（設定変更、バージョンアップなど）
- 機器、ソフトウエアの情報（メーカー、シリアル・製造ナンバー、形式など）
- 設置（保管）状況
- 設置（保管）場所
- 設置（保管）期間
- 利用用途
- 利用者範囲
- システムアカウント所有者リスト
- 破棄方法
- 災害やインシデント発生時の復旧に必要な情報
- 他のシステムなどとの依存関係
- ネットワーク機器を含めたネットワーク構成図

また、システム構成図・ネットワーク構成図に記載する情報としては、以下のような項目があります。

- ネットワーク機器との接続状況（物理的な構成）
- 通信方向とその通信プロトコル（論理的な構成）

資産間のデータの流れを明確化するためにデータマトリックスとデータフロー図を作成します。

- データマトリックス：データフローの有無と方向を記載した表。
- データフロー図：矢印を用いてデータフローを記した図。データフローをシステム構成図に直接記入すると、システム全体の仕組みが把握しやすくなります。

さらに資産管理ツール等を用いて効率的に資産情報を収集することに加え、各機器の脆弱性についても管理することが望ましいです。

参考資料・ガイドライン

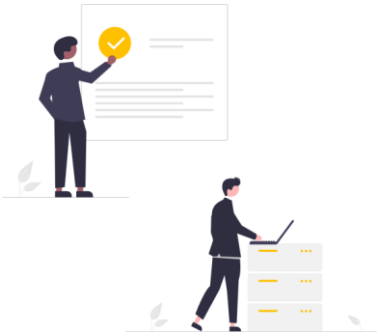
- 工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン
  【産業サイバーセキュリティ研究会 ワーキンググループ1（制度・技術・標準化） 工場サブワーキンググループ】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

設計図やシステム構成図、仕様書通りに現場機器が設置、配線されていることを確認していますか？

（設計図・仕様書等に記載がない機器・配線が取り付けられていませんか？）



■ 背景・目的

ビル設備システム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という問題が運用時に発生しないよう、竣工検査時にシステム構成図（設計図）と現場機器が合致していることを確認し、引き渡す必要があります。

また、予定された計画や設計、構成にない機器が接続されていないことを確認することで、建設時の誤りに気づくだけでなく、不正な機器の設置・配線がないかや、外部との不正な通信が発生していないか等を確認することができます。

さらに、設計変更はVE（Value Engineering）提案などもあり、たびたび発生します。
設計・仕様の変更に伴い、当然、現場で設置・設定する機器も変更となりますが、その変更内容は最終的に竣工図書（竣工図、検査記録、機器の仕様書等）に記載する必要があります。

■ 想定されるリスク

竣工検査時に設計図や仕様書通りに現場機器が設置されていることを確認しない場合、ビル設備システムの最新の構成情報が把握できていない状態になる恐れがあります。
最新のシステム構成情報が管理できていない状態で運用段階に入ると、もし不具合があった場合に、どの時点から設計情報と現場の機器設置の状態が乖離したか、把握が難しくなるだけでなく、サイバー攻撃の検知・復旧対応や、その事後対応にも影響が出る恐れがあります。

■ 内容解説・施策例

竣工前には、試運転調整や性能検査、消防完了検査、総合連動試験等の設計や基準を満たしているかどうか確認する各種検査・試験があります。

設備の種別により検査内容は異なりますが、メーカーの工場でも実施する様々な検査に合格した機器・材料は、さらに現場で加工・設置されます。
性能検査では、システムとして設計仕様通りの性能が発揮できるかを検査します。性能検査と同じく竣工前までに、現場で加工・設置された機器が設計仕様通りに設置されているかや、設計や計画にない配線・配管の有無についても確認します。
また、検査・試験における注意点として、建設中・試験中に登録された情報が機器やシステムに残っていないか確認し、破棄されている必要があります。

検査により、現場で加工・設置された機器が設計仕様通りに設置されていない場合、現地のやり直し工事や、施工図・機器完成図の再修正が必要です。
設計や計画にない配線・配管が有る場合は、対象の配線・配管の撤去や施工図・機器完成図の再修正が必要となります。
もし、軽微な変更でも、その内容が竣工図書等に反映されていない場合、現地のやり直し工事が発生したり、竣工図や機器完成図の再修正が必要となる等、発注者とのトラブルにつながります。

サイバーセキュリティに関する現場と設計図についての確認項目の例としては、以下に示すものがあります。

- 竣工図は実際の状態と食い違いがないよう修正ができているか。
- 竣工図の部屋名、機器名称・番号・仕様などは実際のものとあっているか。
- 機器完成図の機器番号・名称などは竣工図の記載と整合がとれているか。
- 備品・予備品種類・数量は一覧表と整合がとれているか。

加えて、竣工図書は建物のメンテナンスや不具合が発生した場合に利用するため、竣工図書と実際の状況との相違には注意が必要です。

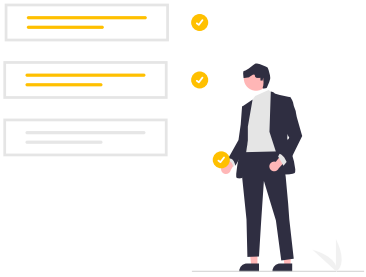
参考資料・ガイドライン

- 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
  【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】
- 設備工事ポイントシート（若手向け） 13-3 竣工図書・備品・メーター読合せ
  https://www.nikkenren.com/kenchiku/jfcc_setsubi/pointsheet/mokuji.html
  【一般社団法人 日本建設業連合会】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

竣工検査時、機器の設定やネットワーク設計に事前に定めたサイバーセキュリティ対策が実施されているか検査を実施していますか？



背景・目的

ビル内のネットワークを物理的又は論理的に分離することは、ビル設備システムの一部に起きたウイルス感染などのサイバー攻撃が、ビル内のネットワーク経由で拡大していくのを防ぐために重要です。

竣工検査時に各システムごとにネットワークセグメントを分離することや、セグメント間の通信を最小限に制限すること、と言った設計・構成、設定などのネットワーク設計時に定めたサイバーセキュリティ対策が実際に実施されているか、機能しているかを確認する必要があります。

想定されるリスク

竣工検査時に機器の設定やネットワーク設計等の事前に定めたサイバーセキュリティ対策が実施されているかについて検査していない場合、サイバー攻撃を受けた際に当初想定したサイバーセキュリティ対策が機能しない恐れがあります。

サイバー攻撃を受け、機器の設定やネットワークの設定が設計と異なっていたり、セキュリティ対策設定が無効化になっていると、サイバー攻撃により設定を変更されたのか、それとも元々無効化された状態で運用を続けていたのかの判別が難しくなり、サイバー攻撃の検知・対応・復旧のプロセスに影響を与える可能性があります。

■ 内容解説・施策例

設計・仕様や建設の段階で定めた機器の設定やネットワーク設計等の事前に定めたサイバーセキュリティ対策について、竣工検査時、実際に実施されているかの確認内容としては以下に示すものがあります。

＜物理面での対策＞

- 入場者に関して、継続登録者、一時登録者で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。
- IT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を確認する。
- 防災センター（中央監視室）等の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。
- 防災センター（中央監視室）等の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。
- 現場搬入後、引渡しまで施錠管理を実施する。
- 装置等に鍵などで施錠があるものは、施錠し管理されているか確認する。

＜技術的な対策（システム構成面での対策）＞

1. 全体管理策
   - 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確認する。
   - 元請社員以外の作業箇所記録を保管しているか確認する。
   - 防災センター（中央監視室）等の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。
   - 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。
   - 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。
   - 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。
   - 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。
2. ネットワークに関する対策
   - 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。
   - 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。
   - 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。
   - 外部アクセスが制限されていることを確認する。
   - 許可された端末へのアクセスしかできないことを確認する
   - あらかじめ許可されたパケット以外は通信できないことを確認する。
   - 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。
3. 機器に関する対策
   - 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。
   - 竣工引渡し前にウィルス検疫を実施する。
   - 利用しない空USBポートや未使用ポートは治具等で物理的にふさぎ、利用できないこと確認する。
   - 保守用端末も、竣工引渡し時にウィルス検疫を実施する。

参考資料・ガイドライン

- 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
  【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】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

竣工引渡し後、「運用」段階におけるビル設備システムおよびシステム上で稼働しているアプリケーションの脆弱性対応やセキュリティパッチ適用等について、運用に入るまでに関係者間で打合せを行っていますか？

背景・目的

ビル内のネットワークを物理的または論理的に分離することは、ビル設備システムの一部に起きた竣工後の運用段階でビル設備システムやシステム上で稼働しているアプリケーションに脆弱性が発見されることがあります。
その脆弱性対応として、OSやアプリケーションのアップデート、セキュリティパッチの適用などがありますが、いかに脆弱性を早く発見し、脆弱性に対処するかが、サイバーセキュリティ対策として重要となります。

そのためにも、運用段階に入る前の竣工引き渡し時に脆弱性の対応方法について、関係者間で打合せを行い、確認しておく必要があります。

想定されるリスク

運用段階に入る前にビル設備システムおよびシステム上で稼働しているアプリケーションの脆弱性対応について、打合せ・確認を行わなかった場合、脆弱性についての認識が不十分で、システム内に脆弱性が残ったままの状態となり、システムの脆弱性をついた攻撃を受ける恐れがあります。

また、脆弱性対応として、OSやアプリケーションのアップデート、セキュリティパッチの適用を行いますが、ベンダーの提供する情報をもとにテストやパッチの適用状態の確認を行わないなど対応方法・手順が確立されていないと、システムやアプリケーションの動作に不具合が出ることや、アップデートやセキュリティパッチが上手く実施できないといった問題が発生する可能性もあります。

■ 内容解説・施策例

「運用」段階に入る前までにアプリケーションの脆弱性対応やセキュリティパッチ適用について、関係者間で打合せを行うにあたり、以下の点を考慮します。

1. 脆弱性情報やセキュリティパッチ情報の入手方法についてビル設備システムベンダーに確認する。
   - ビル設備システムに対する脆弱性情報やセキュリティパッチ情報の入手方法について、ビル設備システムベンダーに事前確認し、セキュリティパッチが発行された場合、速やかに情報が得られるようにします。脆弱性情報に関しては、情報の入手手順に加え、入手頻度を定めておくのも必要です。
   - システムベンダ等からセキュリティパッチ情報が発行された場合には、対象のシステムや機器に対するセキュリティパッチ適用の必要性や影響を確認します。

2. セキュリティパッチを適用する手順についてビル設備システムベンダーに確認する。
   - ビル設備システムに対するセキュリティパッチ適用の手順についてビル設備システムベンダーに事前確認し、ベンダー推奨の手順がある場合は、その手順を確認しておきます。

3. セキュリティパッチ適用時のリスク対策を検討する。
   - セキュリティパッチ適用によってビル設備システムが異常になる可能性もあるため、その対処方法として以下の点を考慮します。

     ① セキュリティパッチ適用時に使用する記録媒体やPCのウイルスチェックを徹底する。

     ② セキュリティパッチが正規のルートで入手したものか・改ざんされていないか確認を徹底する。

     ③ セキュリティパッチ適用前にシステムのバックアップを実施する。

     ④ システム稼働に対する影響が少ない機器から段階的にセキュリティパッチを適用する。

参考資料・ガイドライン

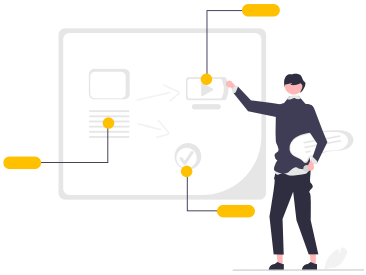
- J-CLICS STEP I／STEP2（ICSセキュリティ自己評価ツール）
  【JPCERTコーディネーションセンター（JPCERT/CC）】

設問No.4-5

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

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関する説明を実施していますか？



■ 背景・目的

竣工引渡し時には、システムの操作説明を行いますが、その際、ビル設備システムなどの説明するシステムのセキュリティ対策についても説明を行うことは、ビルの運用管理者・担当者への教育・意識醸成のために必要です。

設計、構築されたビル設備システムのセキュリティ対策が運用段階で上手く機能するためにも、そのシステムを運用・管理する担当者に対して説明を行うことは、平時および緊急時対応のための準備の一環となります。

■ 想定されるリスク

竣工引渡し時にシステム操作説明を行う際にセキュリティについて説明を実施していない（説明を受けていない）場合、サイバー攻撃等でビル設備システムへの被害が発生した際に、ビルの運用管理者・担当者が迅速な対応ができず、初動対応が遅れ、被害が拡大する恐れがあります。

■ 内容解説・施策例

竣工引き渡し段階では、主にビル管理者（ビル管理会社）に対して、建物設備取扱説明・保守管理説明を行います。

システム全体の概要説明や日常管理（運用）を主体とした説明内容となりますが、ビル設備の知識が無い方でも理解できるよう、わかりやすい操作説明とする必要があります。
運用管理上や機能上、安全上、重要な内容を説明することは、適切なビルの運用・維持管理を行い、不具合を回避することにもつながるため、ビル管理者など使用者目線に立って、取扱説明書の作成、説明を行います。

その説明の際、導入されているセキュリティ対策やセキュリティ機器とその設定内容、運用上必要となる対応・注意点など、セキュリティに関する内容についても合わせて説明を行います。
セキュリティに関する内容も説明を行うことにより、サイバー攻撃によるインシデント発生時の初動対応やその後の復旧を速やかに行うことができます。

説明するセキュリティに関する内容の例としては、以下に示すものがあります。

- 運用、セキュリティに関するマニュアル・ルールについて
- インシデント発生時の対応計画およびインシデント対応体制について
- インシデント発生後の復旧計画および復旧体制について

参考資料・ガイドライン

- 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
  【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】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

ビル設備システムで利用している機器やシステム構成を把握し、変更履歴を含め最新の状態を管理していますか？

■ 背景・目的

ビルの維持管理やビル設備システムに関連するビジネスリスクを回避し、ビジネスリスクの発生時には、迅速に対応するために、正確な要因の分析と評価が重要です。これらに基づき、適切な対策を検討して実施する必要があります。

ビル設備システムのシステム構成を把握し、特に運用段階では、定期的にビル設備システム全体（OSやソフトウェアを含む）の監査と評価を行うことが重要です。さらに、設備機器やシステムなどの資産情報、機能、重要な業務、設置場所、所有者・管理者、サポート担当者などを記録した資産管理台帳を作成し、竣工時の最新状態を管理します。

資産管理台帳によってシステムの最新状態が把握されると、「運用」段階において、予想される影響や被害、サポート担当者への迅速な連絡などのインシデント対応、早期復旧方法が把握できるようになり、ビジネスリスクを最小限に抑えることにつながります。

■ 想定されるリスク

もし、ビル設備システムの資産管理台帳やシステム構成図が存在しないか、最新の状態で管理されていない場合、停電、故障、地震、火事などの障害・災害（自然災害や不正アクセスなどの人為的災害を含む）に対する対策が不十分になる可能性があります。

さらに、システム構成の変更が管理台帳に正しく反映されていない場合、本来不要な対応が発生する可能性や、不具合・インシデント発生時の原因追求までに要する時間の遅延、対策の見落としが生じる恐れがあります。これにより、ビジネス全体に大きな影響が及ぶ可能性があります。

■ 内容解説・施策例

ビル設備システムで利用している機器やシステム構成を把握する管理策として、以下に示すものがあります。

<資産管理台帳の作成および管理>

ビル設備システムを構成する機器などの資産の管理台帳を作成します。
（竣工図書等の納品物に管理台帳がある場合でも、その内容と現地の状況に差異がないか、改めて確認が必要です。）

資産管理台帳は、各機器・システムに対する脅威やその脆弱性を把握し、それらに起因する障害が発生した場合のリスクを把握するために使用します。そのため、資産管理台帳を作成する際、ビル設備システムに関係する全ての機器やシステムの情報を洗い出し、その重要度を設定しておきます。

資産管理台帳に記載する情報としては、以下の項目があげられます。

- 機器、システムの管理 責任者（資産の所有者、管理者名など）
- 機器、システムの形態（形式、バックアップメディア、ライセンスなど）
- 機器、システムの接続状況（使用インターフェース、IPアドレス、MACアドレス、接続機器名、接続図、VLAN設定情報、通信ポート、通信プロトコルなど）
- 機器、システムにおける変更記録（設定変更、バージョンアップなど）
- 機器、システムの情報（メーカー、シリアル・製造ナンバー、形式など）
- 機器設置（保管）状況
- 機器設置（保管）場所
- 機器設置（保管）期間
- 対象機器やシステムの利用用途
- 対象機器やシステムの利用者範囲
- システムアカウント所有者リスト
- 機器やシステム、それら内部に保存されたデータの破棄・廃棄方法
- 災害やインシデント発生時の復旧に必要な情報
- 他のシステムなどとの依存関係
- ネットワーク機器を含めたネットワーク構成図

システム構成を変更する際には、資産管理台帳への反映や定期的な見直しを確実に行い、最新の状態で管理していくことが、対象のビル設備システムへの理解につながり、脅威や脆弱性の把握に役立ちます。

参考資料・ガイドライン

- J-CLICS STEP1／STEP2（ICSセキュリティ自己評価ツール）
  【JPCERTコーディネーションセンター（JPCERT/CC）】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

ビル設備システムに対する脅威や脆弱性について、定期的に情報収集し、ウイルス対策やセキュリティパッチ適用等の対応を行っていますか？

■ 背景・目的

ビル設備システムを含む制御システムに脆弱性や問題、不具合が発見された場合、メーカーやシステムベンダーからセキュリティパッチやOS・ファームウェアアップデートなどの対策が発行されます。
システムを安全な状態に保つためには、対策情報を迅速に入手して対応する、脆弱性対応が重要です。
脆弱性情報の入手方法やセキュリティパッチが発行された際の対応手順については、平常時から確認しておきます。

また、対応作業に際して発生するウイルス感染や動作不全などを考慮して、作業前にシステムのバックアップを取得し、一度に全機器に対して適用するのではなく、いくつかに分割し、動作確認を行いながら適用するなどの対策手順を作成します。

■ 想定されるリスク

セキュリティパッチやアップデートが適用されていない場合、システムが攻撃の影響を受けやすくなったり、急な停電や空調停止などビル設備システムの動作が不安定になったり、稼働しない状態になったりする恐れがあります。

また、セキュリティパッチやアップデートの適用作業が正しい手順で行われていないと、作業時にウイルス感染したり、セキュリティパッチ自体の不具合によってシステムが異常な状態になったりする恐れがあります。
なお、セキュリティパッチやアップデートが適用されたとしても、別のシステムやインストールされているアプリケーションのバージョンなどの依存関係により、不具合が発生する恐れがあります。

■ 内容解説・施策例

セキュリティパッチの適用検討と実施にあたり考慮する点は、以下に示すものがあります。

1. セキュリティパッチの情報入手方法について、ビル設備システムベンダーに確認する。
   - ビル設備システムに対する脆弱性情報やセキュリティパッチ情報の入手方法について、ビル設備システムベンダーに事前確認し、セキュリティパッチが発行された場合、速やかに情報が得られるようにします。脆弱性情報に関しては、情報の入手手順に加え、入手頻度を定めておくのも必要です。
   - システムベンダー等からセキュリティパッチの情報が発行された場合には、対象のシステムや機器に対するセキュリティパッチの適用の必要性や影響を確認します。

2. セキュリティパッチを適用する手順について、ビル設備システムベンダーに確認する。
   - ビル設備システムに対するセキュリティパッチの適用の手順について、ビル設備システムベンダーや構築したサブコン等に事前確認し、推奨の手順がある場合は、その手順を確認しておきます。
   - パッチの適用状況については事前に把握し、未適用パッチに対しては適用する計画を定めます。実施するためには自動化ツールの活用等も考慮し、パッチ管理を行うことが必要です。
   - ビル設備システムはクローズドな環境で構築・運用されることも多く、サポートが終了していたり、各メーカー・ベンダーの保証から外れていることも想定されます。その場合、特に危険度・緊急度が高い脆弱性が発見された際は、仮想パッチを含むセキュリティパッチの適用について、ベンダーとの調整が必要となります。

3. セキュリティパッチ適用時のリスク対策を検討する。
   - セキュリティパッチ適用によってビル設備システムが異常になる可能性もあるため、その対処方法として以下の点を考慮します。

     ① セキュリティパッチ適用時に使用するUSBメモリやCD/DVD、HDDなどの記録媒体やPCのウイルスチェックは徹底する。
     ② セキュリティパッチ適用前にシステムのバックアップを実施する。
     ③ 稼働への影響が小さい機器から段階的にセキュリティパッチを適用する。

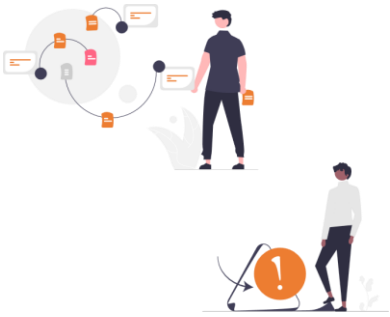
参考資料・ガイドライン

- J-CLICS STEP I／STEP2（ICSセキュリティ自己評価ツール）
  【JPCERTコーディネーションセンター（JPCERT/CC）】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

ビル設備システムに対するサイバーセキュリティリスクを把握し、そのリスクに対応するための計画（リスク対応計画）を策定していますか？



■ 背景・目的

ビル設備システムの管理者は、運用・維持管理しているビル設備システムへの脅威と脆弱性を継続的に把握し、考えられるサイバーセキュリティリスクを評価します。
そして、そのリスク発生への対応を検討することが必要です。

例として、ビル設備システムへの脅威には何があるのか？（自然災害によるライフライン途絶や停電、不正アクセス、誤操作、内部不正など）、脆弱性は何があるのか？（電源設備のメンテナンス不備、不適切なパスワード管理、物理アクセスの容易度など）、影響度はどの程度なのか？（高い、低い、ビル全体に影響する、別拠点まで影響する）を把握した上で、最終的なリスク対応を検討します。

ただし、ビル設備システムに限らず、脅威や脆弱性は日々変化していくため、継続的に情報を更新し、リスク検討を行う必要があります。
その検討を通じて、システムや機器などの各構成要素に対する対策の優先順位を決めることにもつながります。

■ 想定されるリスク

ビルやビル設備システムの構成要素に対する脅威・脆弱性の把握やリスク対策を行わない場合、受容できないリスクが残り、想定外の損失を被ったり、ビジネスそのものに対して大きな影響を及ぼす恐れがあります。
過度な対策により通常の業務遂行、運用に支障をきたすなどの不都合が生じる恐れもあります。

また、脅威や脆弱性は日々変化し、それに伴いリスク対応方法も変化していくため、継続的にリスク対策を行わない場合、最新の脅威や脆弱性に対応できず、攻撃を受け、被害が発生する恐れがあります。

■ 内容解説・施策例

サイバーセキュリティリスクの把握・特定は、重要な経営判断が必要です。さらに、把握・特定したリスクに対して、その影響度に従い、リスク低減、リスク回避、リスク移転のためのリスク対応計画が必要となります。

サイバー・フィジカル・セキュリティ対策フレームワーク（以下CPSF）のリスク評価における対策要件では、以下のように記載されています。

CPSF（対策要件ID：CPS.RA-6）のリスク評価における対策要件

- リスクアセスメントに基づき、発生し得るセキュリティリスクに対する対応策の内容を明確に定め、対応の範囲や優先順位を整理した結果を文書化する。

リスクアセスメント（リスク評価）の結果に基づいてリスク対応を計画し、文書化することが求められています。また、対策例として、CPSFでは以下の項目がBasicとAdvanceでレベル別に記載されています。

<Basic>

- 組織は、リスクアセスメントの結果を考慮して、対象とするリスクへの対応策を選定する。
- 組織は、セキュリティリスク対応の実施計画を策定する。
- セキュリティリスクの受容について、リスク所有者の承認を得る。

<Advance>

- 組織は、セキュリティリスク対応のプロセスについての文書化した情報を安全に保管する。
- 組織は、リスクアセスメントの結果に応じて対応策を選定する際、実施する対応策及び当該対応策を採用する理由を文書化することが望ましい。
- 組織は、対応策の適用等に関して、セキュリティリスク対応計画を策定し、リスク所有者の承認を得る。
- 組織は、セキュリティリスク対応計画をレビューし、当該計画が自組織全体のリスクマネジメント戦略における優先順位に適合しているかどうかを確認する。

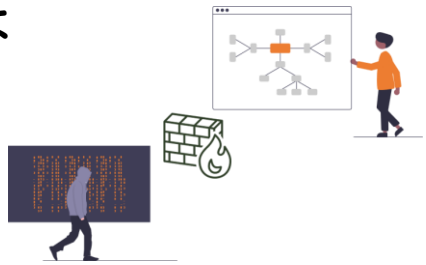
参考資料・ガイドライン

- J-CLICS STEP I ／STEP2（ICSセキュリティ自己評価ツール）
  【JPCERTコーディネーションセンター（JPCERT/CC）】
- サイバー・フィジカル・セキュリティ対策 フレームワーク
  【経済産業省 商務情報政策局 サイバーセキュリティ課】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

ビル設備システムネットワークと他ネットワークとの分離を行い、その境界にはファイアウォールを設置し、不要な通信は遮断していますか？



■ 背景・目的

ネットワーク接続は、必要な通信手段でありますが、同時にサイバー攻撃やウイルスの侵入経路にもなりえます。そのため、ビル設備システムを含む制御システムのネットワークは、イントラネットやインターネットなどの外部ネットワークに接続しない方が安全ではあります。

しかし、最近では、複数のシステムを遠隔で管理・監視するケースだけでなく、ビル内情報通信インフラ構築に伴うイニシャルコストの低減や、ITシステムで求められる高信頼ネットワークをビル管理システムでの活用を目的に、個別に構築していたビル設備システムとITシステムのネットワークをIPで統合するケースも増えています。

ビル設備システムのネットワークをITシステム等の他ネットワークに接続する場合には、通信仕様や接続仕様を把握した上で、ネットワークの境界にファイアウォールを設置して、必要な通信のみを通過させる必要があります。

■ 想定されるリスク

ファイアウォールを設置せずにビル設備システムネットワーク内から、外部ネットワークとの接続を行うと、セキュリティ対策が十分でない外部ネットワークに接続された情報系端末経由で、外部からの攻撃を受けたり、ウイルス感染したりします。

また、ビル設備システムの一部に起きたマルウェア感染が、ビル設備システム間の相互接続経由で容易に拡大していく恐れもあります。

■ 内容解説・施策例

技術的なサイバーセキュリティ対策としてファイアウォールの導入は効果が期待できますが、適切に設定・運用されていない場合、システムの異常動作や、期待した効果が得られないことにつながる可能性があります。

既に運用しているビル設備システムのネットワーク間にファイアウォールを設置・設定する場合には、想定した動作や通信制御を行うために事前の十分な調査・検討を行うことが重要です。

ネットワーク分離やファイアウォール設置における実施内容の例としては以下に示すものがあります。

1．他のネットワークとの接続の必要性の精査

ビル設備システムネットワークをイントラネット・インターネットなどの情報系ネットワークや他のネットワークと接続すると、他ネットワークから攻撃や侵入を受ける恐れがあります。
特にデジタルサイネージや監視カメラのネットワークといった異なるビル制御システムや機器のネットワークを接続する場合は注意が必要です。他のネットワークとの通信を行う場合には、接続の必要性を再検討し、必要のなくなった接続や通信は放置せずに廃止し、抜線するなど取り外しを行います。

2．最小範囲でのネットワーク構成の検討

他のネットワークとの接続の必要性を精査した結果、接続が必要となる場合、サイバーセキュリティリスクを低減するために、なるべく最小範囲で各ネットワークを区画する構成（ネットワーク区画化およびセグメント化、DMZ設置）にする必要があります。（ネットワーク分離によるネットワーク構成の変更は、本来、ネットワーク設計の段階から検討するべき内容になります。）

3．ファイアウォールの設置・通信制御

他のネットワークと接続する場合は、そのネットワークとの境界にファイアウォールを設置して必要な通信のみを通過させ、不要な通信は遮断するようにします。ファイアウォールの設置には、以下の点に注意が必要です。

- ビル設備機器ベンダーやメーカーに推奨構成や設定を問い合わせ、確認する。

  ファイアウォールでビル設備システム関連の通信を通過させる場合は、資産管理台帳のシステム構成図から確認できない等、現状把握が難しい場合、ビル設備機器ベンダーやメーカーに利用機器の通信仕様（通信プロトコル、通信ポート）を問い合わせます。
  ベンダー推奨のファイアウォール機器や設定がある場合にはその機器・設定を使用します。

- ファイアウォールを攻撃者の不正アクセスや不正通信から保護する。

  ファイアウォールの設定変更や接続変更は、システム管理者等、許可された者のみが行うようにします。そのため、ファイアウォールは施錠可能なラックなどに格納して物理的にアクセス・操作できないようにします。
  ネットワーク経由（遠隔）での設定機能はオフにして、極力使用しないようにすることで、遠隔からの攻撃のリスクを下げることができます。
  また、ファイアウォールの設定変更を行うために必要な管理者パスワードは、デフォルトのパスワードから変更せずに使用していると、機器のメーカーや型番がわかると容易に推測されてしまう恐れがあるため、変更が必要です。

参考資料・ガイドライン

- J-CLICS STEP１／STEP2（ICSセキュリティ自己評価ツール）
  【JPCERTコーディネーションセンター（JPCERT/CC）】
- 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
  【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】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

ビル設備システムへのアクセス許可やリモートアクセスの制限を行っていますか？

■ 背景・目的

ビル設備システムを含む制御システムにリモート接続することには、ウイルス感染、情報漏えい、外部からの不正な操作などのリスクが存在します。
ビル設備システムの機器自体ではメールやWebへのアクセスが機能制限されている場合でも、それらの機能を持つPCやサーバがビル設備システムの機器と接続されている状態では、インターネット経由でビル設備システムの機器にアクセスする手段が確立されています。

ビル設備システムが他の拠点の設備システムと通信したり、クラウド環境で複数の拠点を一元管理する場合でも、インターネット回線を使用しており、同様のリスクが生じます。

適切な対策を講じるためには、ビル設備システムへのアクセス許可を管理し、リモート接続の範囲を最小限に制限した上で、接続時に必要な承認手順を設けるなど、ウイルス感染や情報漏えいを防止する対策を厳格に実施することが重要です。

■ 想定されるリスク

ビル設備システムへのアクセス許可がない場合、悪意のある第三者から不正操作が行われる恐れがあるのと、運用担当者による内部不正の検知ができない恐れもあります。

また、リモート接続により、外部から防災センター（中央監視室）や電気室内のビル設備システム・機器へのアクセスが可能となります。
その結果、ウイルス感染、不正操作や情報漏えいなどの被害を受ける恐れがあります。

■ 内容解説・施策例

BACnet/IP等のプロトコルを使用したビル設備システムネットワークの IP化に伴い、従来は個別に構築していた設備ごとのシステムを相互に接続し、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ため、以下に示すリモートアクセスに関する管理対策例を実施し、厳密に管理する必要があります。

管理対策例

1. リモートアクセスに関するルールを定める
   リモートアクセスを行うための申請手順やその承認手順、リモートアクセスの権限削除の手順について規定します。
2. リモートアクセスを監視し、指定されたプロトコルや許可された接続のみに制限する
   リモートアクセスの開始や終了後、定期的に通信機器やアクセス先の機器のログを取得、確認し、不正な通信がないかや、ルールが遵守されているか確認します。
3. リモートアクセスにはMFA（多要素認証）を使用する。
   ユーザIDとパスワードだけでリモートアクセスを許可するのではなく、MFAを利用することで、ユーザIDとパスワードの知識情報に加え、スマートデバイスやFIDOセキュリティキーなどの所持情報および指紋、顔などの生体情報で認証を行い、不正アクセスを防止します。
4. リモートアクセスにはVPN等暗号化されたネットワークを使用する
   リモートアクセスを行うためには、VPNや専用線を使用して、通信は暗号化し、リモートアクセス通信の機密性と完全性を保護します。
5. 指定された接続元からしか、リモートアクセスできないよう制限する
   外部のどこからでもリモートアクセスできないよう、指定した接続元からしかリモートアクセスできないよう制限します。
6. ジャンプサーバ（踏み台サーバ）とファイル検疫サーバを経由してリモートアクセスする
   ジャンプサーバとは、目的のサーバにログインするために中継サーバです。
   始めにジャンプサーバにログインし、その後、ジャンプサーバからリモートアクセスを行います。
   ファイル検疫サーバでは、マルウェアに感染していなか、セキュリティ対策ソフトのパターンファイルは最新か、不要なアプリケーションがインストールされていないか等を検査し、問題がないアクセスだけ許可します。
7. 特権コマンドの実行やリモートアクセスによる機密情報へのアクセスは制限・禁止にする
   特権コマンドなどの通常のユーザが利用しないようなコマンドや不必要なコマンドは無効化するなどして、制限・禁止します。
   リスク低減のため、不要なリモートアクセスからの機密情報へのアクセスも、制限・禁止します。
8. 認可されたリモートコマンドのみを実行し、認可されていないコマンドは拒否する
   あらかじめ認可（許可）されたコマンドのみを実行可能とし、認可されていないコマンドが入力された場合は、そのコマンドを拒否する設定を行います。
9. 一定時間・期間経過後、リモートアクセスが切断・無効化される仕組みを導入する
   一定時間・期間、応答がない場合や、経過した場合にリモートアクセスの接続を切断します。

参考資料・ガイドライン

- J-CLICS STEP I／STEP2（ICSセキュリティ自己評価ツール）
  【JPCERTコーディネーションセンター（JPCERT/CC）】
- SP 800-53 Rev.5 Security and Privacy Controls for Information Systems and Organizations【米国国立標準技術研究所（NIST）】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

ビルの運用担当者や、システムメンテナンスを行う人員等がビル設備システムで利用するアカウント・アクセス権について、棚卸し等の管理を定期的に行っていますか？

■ 背景・目的

ビル設備システムの操作権限は、必要な者に対してのみ制限され、システム管理者によって、捜査権限の付与が許可されます。
定期的に操作権限が付与されたアカウントが、適切な権限設定となっているか確認する必要があります。

ビルの運用に関わるスタッフやシステムメンテナンス担当者が増減したり、退職したりした場合、または役割や責任が変わった場合には、操作権限を持つメンバーに変更がある可能性があります。そのため、利用されているアカウントの確認を行い、権限の設定が正確であることを確認する必要があります。

■ 想定されるリスク

ビル設備システムにおいて、適切なアカウントやパスワードの管理が行われていない場合、退職者や操作権限の必要がなくなったメンバーのアカウントが残ったままになる可能性があります。
これにより、不正アクセスによる業務の妨害や機密情報の漏えいが発生し、ビジネス全体に深刻な影響を及ぼす危険性があります。

■ 内容解説・施策例

海外で既に報告されている制御システムのインシデントの中には、組織の所属中に不正を行う内部不正の事例以外にも、過去所属していた職員が、所属中に得た知識や情報を悪用して、退職後に外部から不正を行うといった事例もあることから、技術的、物理的対策に加えて、運用面の対策（人的対策）が必要となります。

対策例としては、以下に示すものがあります。

1. ビル設備システムで使用が許可されているアカウントや使用が禁止されているアカウントについて規定し、文書化する。

2. ビル設備システムで使用するアカウントの管理者を設定する。

3. アカウントの作成・削除や役割・権限の追加・削除する際の承認、廃棄手順と言ったアカウント管理ポリシーを定める。

4. アカウントの割り当てやそのアカウントで使用できる役割・権限（アクセス権）は必要最小限とする。

5. 共有アカウントおよびグループアカウントの定めたポリシー・ルール以外での使用は制限する。

6. アカウントの使用を監視する。

7. 退職や異動等でアカウントやアクセス権が不要になった場合は、アカウント管理者に通知し、利用していたアカウントやデバイスの適切な棚卸を実施する。

8. 職員の退職や異動があった際、その内容が自動的に反映され、アカウントやアクセス権が削除されるよう、アカウント管理の仕組みやプロセスと連携させる。

9. 定期的に定めたアカウント管理方法やポリシーが適切かどうか見直す。

参考資料・ガイドライン

- J-CLICS STEP1／STEP2（ICSセキュリティ自己評価ツール）
  【JPCERTコーディネーションセンター（JPCERT/CC）】
- SP 800-53 Rev.5 Security and Privacy Controls for Information Systems and Organizations【米国国立標準技術研究所（NIST）】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

防災センター（中央監視室）などの重要なビル設備システムや構成機器を設置した室・空間への入退室は、許可された関係者だけに限られていますか？

■ 背景・目的

防災センター（中央監視室）や電気室内にはビル設備システムを制御・設定するための重要な機器が設置されています。
また、これらの室内では、人命に関わる防災設備関連の機器が有る他、保護すべき機密情報が取り扱われている場合もあります。

ビル設備システムの制御機器への許可されない操作や機密情報の漏えいを防止するために、防災センターや電気室内への入退室は許可された者のみに制限することが重要です。

もし、業務上、訪問者やメンテナンス作業等で外部の方が入室する必要がある場合は、常に入室権限を持った関係者が付き添い、不要または不正な操作、機密情報の撮影・複製および持出しなどを防止することが重要です。

■ 想定されるリスク

悪意を持った人物が防災センターや電気室に侵入すると、物理的なアクセスが可能となり、防災センターや電気室の機器に対して不正な操作、情報漏えい、機器の物理破壊や盗難などの被害が発生する危険性があります。
また、関係者以外の人々が防災センターや電気室に入ることで、不適切な操作や変更、不正なデバイスの設置などが行われ、ビル設備システムの運用に影響を及ぼす可能性があります。
その結果、ビル設備システムが異常動作したり停止したりする危険性が存在します。

■ 内容解説・施策例

防災センター等の重要なビル設備システム構成機器が設置された部屋への入退室は、特定の職員・関係者等に制限し、入退室管理を行う必要があります。
入退室管理を行う際に検討する内容の例として、以下に示すものがあります。

1. 重要なビル設備システム構成機器が設置された部屋への入退室や機器の持ち込み等、物理アクセスに関するポリシー・手順を策定し、文書化する。

2. 策定した物理アクセスに関するポリシー・手順は、職員や関係者等に周知し、徹底させる。

3. 重要な機器がある部屋への物理的アクセスについて、アクセスが許可された職員・関係者のアクセスリストを作成し、定期的なリストの内容を見直す。

4. アクセスリストに含まれる職員・関係者は、IDカードや暗証番号、顔認証等の生体認証による認証装置を用いて個人の認証を行い、入退室を許可する。

5. 重要な機器がある部屋への物理アクセス（入退室）が不要となった職員・関係者は、アクセスリストから削除する。入退室に必要な鍵やIDカード等のデバイスの返却・破棄を徹底する。

6. 入退室に関して、時間、場所、入退室者、作業内容等のログを取得する。

7. 入室時の職員・関係者等の作業・行動を監視する仕組み（監視カメラ等）を導入する。

8. 一時的に入退室する来訪者等については、対象の部屋入室に関する承諾書に署名を得た上で、アクセスリストに含まれる職員・関係者が同伴し、来訪者の行動を制限、管理する。

9. 鍵、IDカード等の物理アクセスに必要なデバイスの管理を徹底する。

参考資料・ガイドライン

- J-CLICS STEP1／STEP2（ICSセキュリティ自己評価ツール）
  【JPCERTコーディネーションセンター（JPCERT/CC）】
- SP 800-53 Rev.5 Security and Privacy Controls for Information Systems and Organizations【米国国立標準技術研究所（NIST）】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

ビル設備システム機器・端末に許可されていないUSBメディアやネットワークケーブル等が不用意に接続されないよう保護措置を取っていますか？

■ 背景・目的

USBメモリやハードディスク、CD、DVD、磁気テープなどの記録媒体、またはノートPCやスマートデバイスなどの情報機器は、ウイルス感染のリスクがある経路となる可能性があります。

近年、これらの機器を通じて、感染が広まるケースが増えており、特にビル設備システムを含む制御システムを標的にしたウイルスも確認されています。
そのため、ビル設備システムやビル設備ネットワークに機器を接続する際には、あらかじめウイルスチェックなどの手順を定め、実施し、注意を払うことが必要です。

加えて、セキュリティポリシーで許可されていないUSBメモリ等の記録媒体の接続を禁止するだけでなく、USBポートやLANポートを物理的に閉鎖する・挿入できなくすると言った保護措置を取るなど、今後はより一層の警戒・対策が必要です。

■ 想定されるリスク

ビル設備システムの機器がウイルスに感染すると、ビル設備システムの運用に重大な影響が及び、業務停止などの深刻な問題が生じる可能性があります。
ビル設備システムで利用している機器・PCに対して、不正なキーボード入力を行うツールもあり、そのツールの使用により攻撃コマンドが送信される恐れもあります。

ウイルス感染によって、機密情報の漏えいやシステムおよびデータの損傷などの被害を受ける危険性が存在します。さらに、ウイルスの駆除には、システムの停止や再インストールなどが必要になる場合もあり、企業にとって膨大なコスト負担が発生します。
その結果、企業イメージやビルのブランドイメージが低下する可能性もあります。

■ 内容解説・施策例

ビル設備システム機器や端末に許可されていないUSBメディアやネットワークケーブル等が接続されないようにする対策例としては、以下に示すものがあります。

1. USBやネットワーク等の不要ポートの閉塞
   対策強度別に以下の対策があります。
   1. 端子キャップを取り付ける
   2. 1.に加えて、ソフトにより閉塞する（サービスの停止、USBのデバイスクラス制限等）
   3. 2.に加えて、ハードにより閉塞する（完全に利用を不可にする）

2. USBメディアやHDDなどのメモリデバイス利用に関するポリシー・手順を策定、文書化する。

3. 策定したメモリデバイス利用に関するポリシー・手順は、職員や関係者等に周知し、徹底させる。

4. USBメディアやHDDなどのメモリデバイスを使用する際は、その必要性とリスクを確認する。

5. 許可されたメモリデバイスのみを利用する。

6. メモリデバイス等へのコピーは、最小限のデータのみ行う。

7. メモリデバイスに対して、保存データがウイルス感染していなか、ウイルスチェックし、Windowsの自動実行機能（AutoRun）などの機能を無効化してから、利用する。

8. メモリデバイスの使用後は、フォーマットなどで初期化し、データを完全に削除する。

9. ネットワーク機器に対して、許可されていないネットワークケーブルが接続された際に、アラートをあげる仕組みを導入する。

10. 既に接続されているネットワークケーブル等が抜かれないようない仕組みを入れる。

参考資料・ガイドライン

- J-CLICS STEP1／STEP2（ICSセキュリティ自己評価ツール）
  【JPCERTコーディネーションセンター（JPCERT/CC）】
- 工場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
  【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） 工場サブワーキンググループ】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

ビルテナント（入居者）が契約する外部接続回線や設置する機器について定期的に点検し、不正な回線の引き込みや不正な機器の接続がないことを確認していますか？

■ 背景・目的

ビルテナント（入居者）が契約したITシステム用の外部接続回線や設置機器などをビル管理者側でも把握することは、外部ネットワーク接続経由での不正接続や攻撃を防ぐためにも重要です。

ビルテナント（入居者）の入居時に、ビル全体に影響を与えるような工事の他、外部回線引き込みはビル管理者の許可が必要とするなど、運用ルールを定め、管理する必要があります。

■ 想定されるリスク

ビルへの引き込み回線の管理が不十分で、ビルテナント（入居者）が勝手に不正な外部回線を引き込まれた場合、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恐れがあります。

また、一部のテナントで発生した障害やサイバー攻撃の被害が、不正に引き込まれた外部回線を通じて、別テナントや別システム、別拠点に対しても拡大する可能性もあります。

■ 内容解説・施策例

ビルへの引き込み回線の管理が不十分である場合、テナント入居者等がビル管理者の承認を得ず不正な外部回線を引き込まれる可能性があるため、検討・実施する対策内容としては、以下に示すものがあります。

1. 施工者やテナント入居者が許可なくインターネット回線等を敷設できない運用ルールを策定し、契約を結ぶなどし、運用ルールを徹底させる。

2. ビルの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。

3. ビル共用部にあるEPSやMDF・IDFで回線引き込み作業等がある場合、事前にビルオーナーやビル管理者の許諾を得た上で、実施する。

4. ビル共用部にあるEPSやMDF・IDFで、テナント入居者が利用する回線引き込み等の工事を行う際、当該工事に立ち合い、不正な機器や回線が引き込まれないよう監視する。

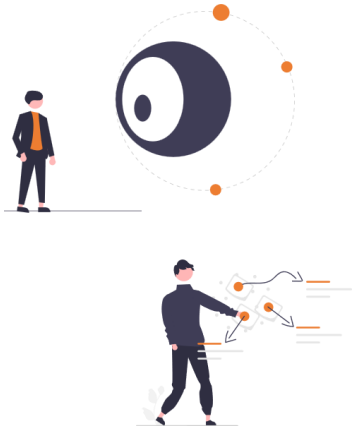
5. 特に統合ネットワークを採用しているビルにおいて、テナント入居者側で敷設する回線や機器がビル全体の設備システムに影響がないか確認する。
（C工事の内容が、共用部やビル全体に影響を及ぼすような場合も確認が必要です。）

参考資料・ガイドライン

- 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
【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】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー



ビル設備システムついて、平常時からシステムの稼働状況やログを確認、分析し、監視を行っていますか？

■ 背景・目的

ビル設備システムの異常を早期に検知するためには、ビル設備システムの稼働状況やログを定期的に確認し、分析することが非常に重要です。

定期的な稼働状況の監視とログの分析により、ビル設備システムに問題が発生する前に異常を察知することができます。また、問題が生じた場合でも、迅速にサポート担当者と連携して対応するために必要な情報を収集することができます。これにより、ビル設備システムの運用に悪影響を及ぼすリスクを最小限に抑えることができます。

日常的にビル設備システムのCPU負荷、メモリ使用量、ハードディスクの空き容量、ネットワークの通信状況などを確認し、ビル設備システムのOSが生成するログを注意深く監視することで、異常な兆候を素早く察知する体制を整える必要があります。
また、関係者全体の意識も重要であり、異常を見逃さずに対処できるような担当者の意識向上を図る必要があります。

■ 想定されるリスク

ビル設備システムを定期的に確認しないと、正常な状態と異常な状態を正確に判断できず、異常の兆候を見逃してしまう可能性があります。

このような状況では、異常を早期に検知することができず、最終的にはビル設備システムの運用に重大な影響を及ぼすような操業停止などの深刻な問題に直面する可能性があります。

■ 内容解説・施策例

ビル設備システムの異常を早期発見するためには、平常時からログやシステムの稼働状況について確認し、正常な状態を把握しておくことが必要です。システムの監視における施策例としては、以下に示すものがあります。

1. ビル設備システムの監視対象を定め、監視手順を策定し、継続的に監視を行う。

2. 戦略に従って継続的監視を実装する。

3. ビル設備システム全体のセキュリティイベントのアラートを一元化管理して収集する。

4. PCやサーバ上の OS 、アプリケーションログなどを監視するホストベース侵入検知システム（IDS）を導入する。

5. 対象のネットワークを流れるパケットを監視するネットワーク侵入検知システム（IDS）を導入する。

6. ネットワーク機器からネットワークトラフィックフローログやネットワークトラフィックを収集する。

7. 監視状況に応じて、セキュリティイベントの警告の閾値を定期的に調整する。

8. 機密情報を保管する端末やリモート管理端末（コマンドライン等）から監査ログを収集する。

参考資料・ガイドライン

- J-CLICS STEP1／STEP2（ICSセキュリティ自己評価ツール）
  【JPCERTコーディネーションセンター（JPCERT/CC）】
- CIS Critical Security Controls version8
  【CIS(Center for Internet Security)】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

サイバーセキュリティインシデントが発生した際に運用を継続するための対応計画が策定されていますか？

■ 背景・目的

不審なアクセスを検知した場合、迅速に対処することが運用を継続する上で重要です。迅速な対処により、重要なデータ漏えいや制御プログラムの不正な改ざん、システムの停止などの被害を回避することができます。

サイバーセキュリティインシデントの検知、封じ込め、根絶といった手順に加えて、インシデントへの対応においては、ステークホルダとのコミュニケーションも重要です。不審なアクセスを検知した際や攻撃が発生した際には、迅速かつ正確な対応が求められます。

ビルの運用・維持管理においても、サイバーセキュリティインシデントに対する対応計画の策定が重要であり、不正アクセスなどのサイバー攻撃に対して効果的に対処できる体制を整えることが必要です。

■ 想定されるリスク

サイバーセキュリティインシデント発生時の運用を継続するための対応計画が策定されていない場合、攻撃等への対応が効果的にできなかったり、対応手順がわからず、被害が拡大する恐れがあります。
また、対応計画が不十分だと、運用時のセキュリティ管理体制も不十分となる可能性が高くなり、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、被害が拡大する恐れもあります。

■ 内容解説・施策例

サイバーセキュリティインシデントが発生した際に運用継続ができるよう事前に対応計画を策定しおく必要があります。
インシデント対応については、以下の流れになります。

以下のガイドを参考に作成
（参考元ガイド：JDCC「建物設備システムリファレンスガイド（第三版）（インシデント対応・セキュリティソリューション編）」）

またインシデント対応計画や、その中で検討すべき施策例としては、以下に示すものがあります。

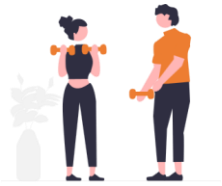
1. ビル設備システムに対するインシデント対応に関して、ポリシーと手順を策定し、文書化する。
2. インシデント対応に関する対応体制を整備する。
3. セキュリティインシデントを報告する必要がある関係者の連絡先を収集し、管理する。
4. ビル設備の設定等、定期的なシステムのバックアップ取得および封じ込めの対応方針を検討する。
5. 職員や関係者がセキュリティインシデントを報告するための組織全体の基準を策定する。
6. インシデント対応時に連絡・報告する手段を検討し、利用できるようにする。

参考資料・ガイドライン

- 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
  【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】
- CIS Critical Security Controls version8
  【CIS(Center for Internet Security)】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サプコン）	メーカー ベンダー



ビルの運用担当者に対して、ビル設備システムのセキュリティ監視手順やインシデント対応手順についての教育・訓練を定期的に実施していますか？

■ 背景・目的

ビル設備システムのセキュリティ監視手順やインシデント対応手順についてビルの運用管理者・担当者に教育・訓練を行うことは、地震や火災などの避難訓練と同様、事前に一連のプロセスを体験するために重要です。

また、インシデント発生時の対応方法を理解し、定期的にその方法(手順)を用いて訓練するだけでなく、教育・訓練内容についても最新の情報・情勢に合った内容に更新し、実施することが重要です。

■ 想定されるリスク

セキュリティインシデントを監視し、警告や異常時の対応手順を備えていても、それらを実際に経験したことがない担当者にとっては、実際のサイバー攻撃発生時などに適切な対応を行うことは難しいです。

サイバー攻撃を検知しても、適切な対応策を講じることなく時間だけが経過し、被害が拡大する可能性もあります。
さらに、誤った対応を行うと、二次的な被害やさらなる問題を引き起こす可能性もあります。

■ 内容解説・施策例

ビルの運用担当者に対して定期的に行うビル設備システムのセキュリティ監視手順やインシデント対応手順についての教育・訓練の内容の例として、以下に示すものがあります。

I．監視手順の理解
サイバーセキュリティにおける監視は、ログの監視から物理的な監視、例えば不審な配線やネットワーク機器の接続など、さまざまな項目を対象とします。
組織の監視手順に基づいて、以下に挙げるような監視項目を実施します。

＜主な監視事項＞

- ファイアウォールやネットワーク機器、サーバ等のログイン記録およびイベントログ
- ログインおよびログアウト時間
- 各機器・システムへのログインに必要なアカウントやパスワードの変更履歴
- アクセス権限のないユーザのアクセスログ
- 統合監視システム等のビル設備システムにおける各種操作ログ
- 侵入検知システム（IDS）・侵入防止システム（IPS）のログ
- 防災センター（中央監視室）など、重要なビル設備機器が設置された部屋への入退室記録および作業記録
- 配線やネットワーク機器（ファイアウォール、ルータやスイッチングHUBなど）の接続状況
- ネットワーク負荷の状況変化
- 不正プロセスの動作可否

2．警報発生時や異常時の訓練
実際のビル設備システムで、インシデント対応の訓練を行うことは、現在稼働しているシステムへの影響が懸念されるため、訓練用に別途、実際の環境と同じ環境を設けることが理想的です。しかし、訓練用に別環境を用意することが難しい場合、実システムへの影響がない、または、影響が限定的となるよう、配慮して、訓練する必要があります。
大規模な訓練や演習の実施は制限が多く、難しいため、机上でインシデント対応のマニュアルを確認するような訓練と組み合わせて実施すると、より効果的です。

参考資料・ガイドライン

- J-CLICS STEP I／STEP2（ICSセキュリティ自己評価ツール）
  【JPCERTコーディネーションセンター（JPCERT/CC）】
- 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
  【産業サイバーセキュリティ研究会 ワーキンググループI（制度・技術・標準化） ビルサブワーキンググループ】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

ビル設備システムに対してサイバー攻撃を受けた際の復旧計画が策定されていますか？

■ 背景・目的

実際にビル設備システムに対してサイバー攻撃を受けた後の復旧計画は、BCP（事業継続計画）の観点から早期復旧し、事業を継続するためにも重要です。

そのためにも、サイバー攻撃により、影響を受けたシステム・機器に対して、これ以上攻撃者のシステムへの侵害を防ぐ、根絶するための作業や、システム全体を正常な運用状態に回復させるための作業が必要となります。

これらの作業について事前に検討し、復旧計画を策定、いつでも実施できるようにしておく必要があります。

■ 想定されるリスク

ビル設備システムに対してサイバー攻撃を受けた際の復旧計画が策定されていない場合、早期に事業が復旧できず、ビルに入居するテナントに対する被害だけでなく、ビルを運用管理するビジネスそのものへの大きな影響を及ぼす恐れがあります。

また、適切な復旧対応が取れていないことにより、再度攻撃者からサイバー攻撃を受ける恐れもあります。

■ 内容解説・施策例

インシデント対応計画における被害を最小限に抑え、被害を拡大させないために実施する「システムのバックアップ及び封じ込め方針等の検討」では、インシデント発生時に少しでも早く復旧を行う対策として、復旧計画を策定します。
復旧計画の検討内容の例として、以下に示すものがあります。

1. 定期的に設備の設定等のシステムのバックアップを取得する。

2. バックアップの取得方法について、手順を定め、文書化する。
（誰が、いつ、何のバックアップ、いつまで、どのように、どこに保存するか?）

3. 封じ込めを想定したインシデント発生時のネットワーク切断可否、切断した場合のテナント等利用者への影響。これらを考慮した対応方針の策定。
特にネットワーク切断可否においては、インシデント発生箇所や被害拡大の影響に応じて、切断箇所かも変わるため、なるべく詳細に検討しておくべきです。

4. インシデントの原因調査を行うために影響を受けたシステム・機器のログ・データ収集方法を定める。

5. システムの復旧やインシデントの原因調査に必要な関係者の洗い出しと連絡方法の確保を行う。

6. 対外発表や外部組織に対して提出するインシデント報告書や公表文書の作成および報告体制を整備する。

   EUのサイバーレジリエンス法では「インシデント発生後24時間以内に報告義務」があるように、インシデント発生時、そのインシデントの影響を緩和するため、なるべく早期に報告することが重要になります。そのためには、インシデント対応と合わせて、事前に報告書の内容を想定し、報告体制を整備しておくことが重要です。

参考資料・ガイドライン

- 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
  【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】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

ビル設備システムのバックアップデータを定期的に取得していますか？

■ 背景・目的

自然災害やサイバー攻撃の発生等、万が一の事態に備え、ビル設備システムの復旧に必要なデータ（設備設定・パラメータや操業データなど）は、定期的にバックアップを行う必要があります。また、バックアップデータから、想定した目標復旧時間（RTO）や目標復旧地点（RPO）でデータが復元できるかどうかの確認を定期的に行っておくことも必要です。

そのためにもまずは、ベンダーの推奨するバックアップ方法と、その方法でデータが保存されるかを確認しておき、その他資産・システム・データ・の重要度や影響度を考慮して、バックアップ計画を定めておく必要があります。

■ 想定されるリスク

自然災害やサイバー攻撃により、ビル設備システムがシステム機能不全もしくは機能が完全停止した状態になり、その復旧方法として、システムの復元を行う場合が想定されます。

このような場合には、障害・インシデントが起きる前の直近のデータが必要ですが、より短い間隔で定期的にバックアップを行っていれば、より直近のバックアップデータからの復元が可能となりますが、適切な間隔でバックアップされていない場合は、古いバックアップデータから復元することになります。

また、バックアップデータがない場合には、本来の運用状態に復旧するまでに時間や手間がかかるなど、大きな影響を及ぼす恐れがあります。

■ 内容解説・施策例

サイバー攻撃によるインシデントが発生し、その対応・復旧作業として、定期的に設備の設定等システムのバックアップをしておくことは重要です。
ビル設備システムのバックアップデータ取得に関する検討内容の例として、以下に示すものがあります。

1. 定めた目標復旧時間（RTO）や目標復旧地点（RPO）、頻度で設備の設定等、データをバックアップする。

2. 毎回全てのデータをバックアップするフルバックアップや変更・追加されたデータだけをバックアップする差分バックアップなど、バックアップ方法について定める。

3. ランサムウェアやサイバー攻撃の横展開に備え、オンラインバックアップだけでなく、オフラインバックアップ方法も定める。

4. バックアップ媒体の信頼性やバックアップしたデータの完全性を保証するために、定期的にバックアップデータが確実に取り出せることを確認する。

5. インシデント対応訓練等で一部のバックアップデータを用いて、システムが復元できるか検証する。

6. バックアップデータのコピーを別施設・別拠点（物理的）や別システム（論理的）に分離して保管する。

7. バックアップデータの削除・破棄には、2人以上の承認が必要とする（二重認可）手順・ポリシーを策定する。

8. バックアップデータの変更・改ざんや情報漏えいを防ぐために、データの暗号化を行う。

参考資料・ガイドライン

- J-CLICS STEP1／STEP2（ICSセキュリティ自己評価ツール）【JPCERTコーディネーションセンター（JPCERT/CC）】
- SP 800-53 Rev.5 Security and Privacy Controls for Information Systems and Organizations【米国国立標準技術研究所（NIST）】
- CIS Critical Security Controls version8【CIS(Center for Internet Security)】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

ビルの運用・維持管理において、適切にビルの運営・管理ができる仕組みやルール（マネジメントシステム）が実施され、機能していることを定期的に評価していますか？

■ 背景・目的

サイバーセキュリティ施策・対策の効果やその実行性は、組織自体や組織内のポリシーの変更、技術の進歩、新たな攻撃手法の発見などにより、日々変化しています。

サイバーセキュリティ施策・対策は、PDCA（Plan：計画, Do：実行, Check：点検, Action：改善）サイクルを回し、定期的な評価および改善を行っていないと、実効性が下がり、実効性の向上が望めないだけでなく、維持すら難しい状況となります。

また、技術の進歩や社会情勢の変化により、コストが下がったことで、これまでコストの問題で選択できなかった対策方法が選択できようになる場合もあれば、新たな攻撃手法の発見により、既存の対策方法が陳腐化する可能性もあります。

サイバーセキュリティ施策・対策の維持・向上のためにも、ビルの運用・維持管理における仕組みやルール（マネジメントシステム）について、定期的にサイバーセキュリティ対策の評価と見直しを行う管理を行うことで、ビル設備システムのレジリエンス強化にもつながります。

■ 想定されるリスク

利用技術や組織の変化により、既存のサイバーセキュリティ施策やルールが現場の実情に合わなくなり、陳腐化している状態を放置すると、攻撃者の標的になったり、運用上の混乱を引き起こす可能性があります。

このような状況では、ビル設備システムの稼働に悪影響を及ぼすリスクが高まります。さらに、陳腐化したルールや施策をそのまま放置して運用することは、最新のサイバー攻撃に対して効果を発揮できないだけでなく、新たな脆弱性を生み出し、不必要なコストが発生する可能性もあります。

■ 内容解説・施策例

ビルの運用・維持管理における、ビルの運営・管理ができる仕組みやルール（マネジメントシステム）について定めた上で、そのマネジメントシステムが機能していることを定期的に評価し、見直しおよび更新していくことが重要です。

ビルの運用・維持管理におけるマネジメントシステムを評価し、更新していくためには、監査が必要ですが、監査について検討する内容の例として、以下に示すものがあります。

1. ビルの運用・維持管理事業における監査および説明責任、目的や役割について、方針・ポリシーを策定し、文書化する。

2. リスク評価の結果等をもとに監査に必要なログ（監査ログ）や記録として残す監査対象（作業内容・イベント・データ）を定める。

3. 監査ログに含める内容を定める。
   内容例：
   - 発生したイベントのタイプ
   - イベントが発生した日時（タイムスタンプ）、場所
   - イベントの発生源（発生した機器）
   - イベントの結果
   - イベントに関連した内容

4. 監査ログで利用する記憶容量（ストレージ）の容量を監査ログの要件等から定める。

5. 監査ログ取得プロセスで障害発生した際の対応について、定める。

6. 監査ログの内容や監査ログの分析結果を報告し、監査・分析結果の評価を定期的に行う。

7. 監査ログ等、監査に関する情報の保護方法について定める。

8. 監査ログ等、監査に関する情報を保持するために、保持期間や破棄手順などのポリシーを定める。

9. 現在の脅威やリスク評価、及びインシデント発生後の分析に基づき、監査対象のリストを修正する。

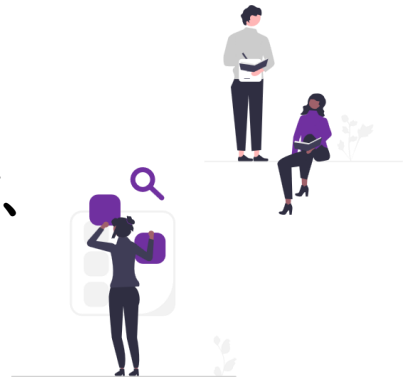
参考資料・ガイドライン

- SP 800-53 Rev.5 Security and Privacy Controls for Information Systems and Organizations【米国国立標準技術研究所（NIST）】
- NIST IR 7628 Revision 1 【米国国立標準技術研究所（NIST）】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

ビルやビル設備システムを改修する際、改修内容やコストに加え、最新のサイバーセキュリティの状況を考慮した上で、サイバーセキュリティ対策を検討していますか？



■ 背景・目的

改修時において、ビルおよびビル設備システムに対する適切なサイバーセキュリティ対策を検討するためには、これまでの「設計・仕様」段階、「運用」段階で検討・実施してきたサイバーセキュリティ要件、サイバーセキュリティポリシーを整理し、改修内容や改修時にかけられるセキュリティ対策コストに加え、日々変化する最新のサイバーセキュリティの状況を考慮する必要があります。

また、改修時に建物用途や居室の用途やレイアウトが変更になることにより、物理セキュリティの要件も変化するため、物理セキュリティ対策についても検討をする必要があります。

■ 想定されるリスク

サイバーセキュリティ対策を検討するあたり、改修後に必要な要件について整理できていない場合、実施するサイバーセキュリティ対策が不十分な内容になるだけでなく、過度な対策となるなど、適切な対策を実施できない恐れがあります。

また、改修に伴うサイバーセキュリティポリシーの変更や最新のサイバーセキュリティ対策を考慮して検討されていないビルでは、最新のサイバー攻撃に対して効果を発揮しないというだけでなく、無駄なコストの原因となります。

■ 内容解説・施策例

まず、設備機器・システムの大規模更新を含むようなビルの改修におけるビルの設備システムのサイバーセキュリティ対策を実施する上での方針を策定します。
方針の策定後、これまで整理、把握してきたビルおよびビル設備システムに対する最新の脅威・リスクをサイバーセキュリティ対策と結びつけながら、検討を進めます。
対象のビルや自社の置かれた環境、改修内容、対策の費用対効果や現状も考慮しながら、必要なサイバーセキュリティ対策をより具体的に検討します。
対策内容としては、以下のような「設計・仕様」段階で検討した内容と同様の内容があげられますが、その検討時点で最適な仕組みやシステムに入れ替え・更新していくことが必要となります。

＜組織的な対策＞
- 運用、セキュリティに関するマニュアル・ルールの整備
- インシデント発生時の対応計画およびインシデント対応体制の構築
- インシデント発生後の復旧計画および復旧体制の構築

＜技術的な対策＞
- ネットワークの論理的・物理的な分割
- 通信データ制限：ファイアウォール（FW）、侵入検知・防止システム（IDS・IPS）の導入
- 利用者制限：ネットワーク機器やセキュリティ機器のID／パスワード、認証設定
- 通信監視・制御：通信状況可視化・監視、侵入検知システム（IDS）、侵入防止システム(IPS)の導入、フィルタリング
- 構成管理：接続機器の管理（OS・ファームウェアのバージョン、IP・MACアドレス、利用プロトコル、利用ポート番号）
- 脆弱性対策：機器やシステム、ソフトウェアに対する脆弱性情報の収集・診断、対策（ソフトウェア更新、パッチ適用等）
- ログ取得：ログ取得・連携、分析の仕組み、体制の構築
- セキュリティソフト、ウイルス対策ソフトの導入
- 外付けのセキュリティ機器の導入

＜物理的な対策＞
- 地震などによる機器の転倒・落下防止対策
- 不正侵入者や内部不正者による機器の盗難防止対策
- 盗難された機器により、ビル設備システムに侵入し攻撃されることを防止する対策
- 盗難された記憶デバイスにより、内部に保存された情報を利用されないための、データ暗号化などの仕組みの構築
- 不要なインタフェース／ポート(LAN、USB など)の物理的又は論理的な閉塞
- 防災センター（中央監視室）、電気室等の重要な構成機、器を設置したや室への入室制限、入退管理システムの導入
- 監視カメラの設置
- 外部からの侵入だけでなく内部からの侵入（内部不正）まで含めた管理・監視体制の構築

＜人的な対策＞
- 従業員や委託先などビルの維持管理に関わる関係者へのセキュリティ教育

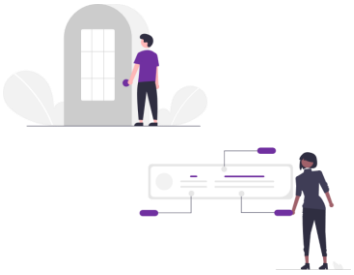
参考資料・ガイドライン

- 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
  【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】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

改修・解体現場に出入りする業者・作業員に対して身元確認や現場への入退場管理を行っていますか？



■ 背景・目的

改修現場および解体現場に出入りする業者・作業員に対して、身元確認や解体現場への入退場管理を行う目的として、特に解体現場では危険を伴う作業であり、現場監督は一人ひとりの安全を確保するために現場で作業を行っている作業員を特定し、作業員情報を管理することがあげられます。

また、廃棄する機器内部にも管理者権限のアカウント情報（ユーザID/パスワード）を含んだ設定データなど機密情報が保存されていることもあります。
身元確認や入退場管理と言った機器の窃盗・盗難や事故の他、サイバー攻撃につながる行為を防止することは解体現場でも人的なサイバーセキュリティ対策として、重要な項目となります。

■ 想定されるリスク

改修現場および解体現場においても入退場を管理していない場合、部外者が容易に現場に出入りでき、現場で利用する機材・機器の窃盗から機器内部に保存された設定データなど機密情報の漏えいにつながる恐れがあります。

また、悪意を持った部外者に加え、改修現場や解体現場に出入りする業者の中に悪意を持った者が紛れていることも想定されます。

■ 内容解説・施策例

改修・解体現場においても入退場管理の業務負荷とコストは大きいですが重要です。
管理方法は、就労届や作業員名簿、入館証などで作業員の身元確認を実施する方法と顔認証等生体認証システムを用いたデジタル管理もあります。

また、1フロアだけの改修工事のように、運営しているビルの一部だけ工事をする場合、ビルへの入館時に腕章や入館証を身に付けるなどし、作業員と見た目でわかるようにします。

さらに、既に重要な機器がある場所では、機器や設備の取り外しや設置の作業実施時、必ず元請社員やサブコン社員の立会いを行うとより強固になります。
改修・解体現場でも不定期に入場することになる搬入業者やベンダー関連業者は抜け漏れが生じやすいので気を付ける必要があります。
また、定期的な現場巡回や作業場所の施錠などを行い、不審者や不審行動（不要な撮影等）などを取り締まります。

また、改修・解体現場においても、現場事務所と施工場所が同じ敷地内にある場合もあれば、別々の場所にある場合もあります。小規模の改修になるほど、現場事務所と施工場所は別々の場所になる傾向にあります。

特に、現場事務所と施工場所が別々の場所にある場合では、詰所と呼ばれる建設作業員の休憩・待機所や会議室が施工場所の敷地や建物内に仮設で用意されることがあります。
詰所でもPCやスマートデバイス、プリンタ等の情報機器を使用するため、現場事務所内と同じく、セキュリティレベルに応じて扉を施錠するなどして、機器の盗難や情報漏えいに注意する必要があります。

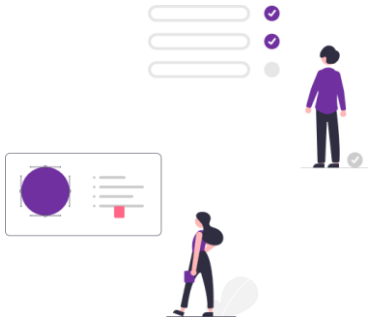
参考資料・ガイドライン

- 建設現場における情報セキュリティガイドライン
- 元請会社における情報セキュリティガイドライン
  【一般社団法人 日本建設業連合会】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

改修後の構成が竣工図書（竣工図、システム構成図、仕様書等）に反映されていることを確認していますか？



■ 背景・目的

改修時も再構築した環境やシステムについて、最終的に竣工図書（竣工図、検査記録、機器の仕様書等）に記載して、納品します。

改修における設計・仕様の内容や改修後の現地の状況が正しく竣工図書に反映されているか確認することは、ビル設備システムの構成情報が最新状態に管理するためにも重要です。

■ 想定されるリスク

ビル設備システムの改修内容が正しく竣工図書に記載されていない、または最新の状態で管理されていない（各種変更を竣工図書に反映してない）場合、障害・災害（不正アクセスなどの人的災害も含む）への対策が不十分になる恐れがあります。

また、適切な復旧対応が取れていないことにより、再度攻撃者からサイバー攻撃を受ける恐れもあります。

■ 内容解説・施策例

改修工事においても、新築工事の際と同様で、改修工事中・試験中に登録された情報が機器やシステムに残っていないか確認し、破棄されている必要があります。

また、軽微な変更でも、その内容が改修における竣工図書等に反映されていない場合、現地のやり直し工事が発生したり、竣工図や機器完成図の再修正が必要となる等、改修工事においても発注者とのトラブルにつながります。

サイバーセキュリティに関する現地の状況と改修図面についての確認項目の例としては、以下のものがあります。

- 竣工図（改修）は実際の状態と食い違いがないよう修正ができているか。
- 竣工図（改修）の部屋名、機器名称・番号・仕様などは実際のものとあっているか。
- 機器完成図の機器番号・名称などは竣工図（改修）の記載と整合がとれているか。
- 備品・予備品種類・数量は一覧表と整合がとれているか。

加えて、竣工図書は建物のメンテナンスや不具合が発生した場合に利用するため、竣工図書と実際の状況との相違には注意が必要です。

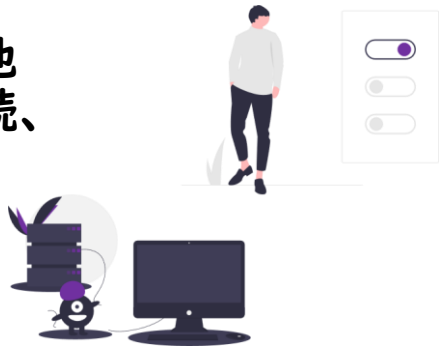
参考資料・ガイドライン

- 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
  【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】
- 設備工事ポイントシート（若手向け）　13-3　竣工図書・備品・メーター読合せ
  https://www.nikkenren.com/kenchiku/jfcc_setsubi/pointsheet/mokuji.html
  【一般社団法人 日本建設業連合会】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

廃棄・撤去するシステムは、撤去時、他のシステムやインターネット等との接続、連携が切断されていますか？



■ 背景・目的

システムの撤去時には、撤去用端末の接続やセキュリティ製品が未更新状態になる等の理由でセキュリティレベルが下がった状態となることがあります。

撤去対象が他のシステムへの侵入口とならないよう、他のシステムとの接続が物理・論理の両面で切断していることを確認する必要があります。もしくは実際の撤去まで他のシステムと切断が出来ない場合、撤去の瞬間まで稼働中のシステムと同等のセキュリティポリシーが適用されている必要があります。

■ 想定されるリスク

撤去にあたり、対象システムのセキュリティレベルが下がった状態となることで、接続している他のシステムへ侵入するための踏み台となってしまう可能性があります。
また、システム撤去後、撤去対象システムと他のシステムの接続点が、他のシステムに対する新たな侵入口となってしまう可能性があります。

■ 内容解説・施策例

廃棄・改修するシステムにおいて、改修・解体時に発生するインフラやシステムに対する変更の影響を考慮した廃棄（解体）計画を策定することが重要になります。

特にビルやビル設備システムの一部を廃棄（解体）を計画する場合は、一定レベルのセキュリティが維持されるよう、廃止に伴うビル設備システム等各種変更の順序や内容を検討する必要があります。
最終的には、事前に計画した内容が実施されているか確認が必要となります。
廃止（解体）計画の内容の例として、ビルやビル設備システムの特性や用途によって異なりますが、以下に示すものがあります。

1. 個人を特定できるデータまたはは商業上重要なデータを処理又は保存するために使用されるシステムの撤去および安全な保管、廃棄

2. 当該エリア内にある、その他すべてのIT機器の撤去および安全な保管または廃棄

3. 公衆電気通信ネットワークの接続やサービスの廃止

4. 他の会社または組織の拠点へのネットワークまたは通信リンクの廃止

5. 構築された資産管理システムに対するネットワーク又は通信リンクの廃止

6. 個人を特定できるデータまたは商業上の機密データを含むすべての使用済みメディア、紙記録等の除去および安全な保管または廃棄

7. 機密通信およびネットワークケーブルの経路の変更

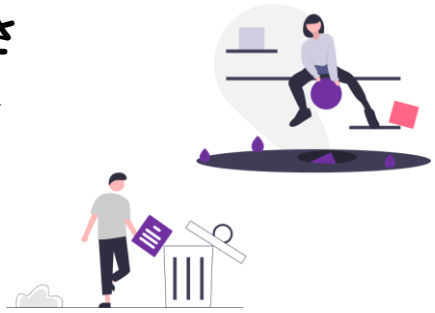
参考資料・ガイドライン

- Code of Practice Cyber Security in the Built Environment 2nd Edition
  【IET (The Institution of Engineering and Technology：英国工学技術学会)】

対象

発注者/権利者 ビルオーナー ビル管理会社	設計事務所	建設会社 （ゼネコン）	設備協力会社 （サブコン）	メーカー ベンダー

ビル設備システム機器は内部に保存された機密データは削除した上で、廃棄されていますか？



■ 背景・目的

ビル設備システムの機器を取り外し、廃棄する際、機器内部には管理者パスワードを含んだ設定データなど機密情報が保存されていることもあり、それらの情報が機器廃棄時に漏えいしないよう、データ削除などを定めた廃棄方法についても規定する必要があります。

また、最終的に規定された廃棄方法が確実に実施され、機器内部のデータが削除し、廃棄されたことを確認する必要があります。

■ 想定されるリスク

機器の廃棄方法について規定していない場合、機器内部に保存されている管理パスワードを含んだ設定データが漏えいする恐れがあります。

機器の設定や構成については、同一企業が管理する複数の拠点でも、同じ設定、同じ構成で構築することも多く、同じ機器を利用している他拠点のビルに対して、漏えいした設定データを悪用したサイバー攻撃につながる可能性もあります。

■ 内容解説・施策例

ビル設備システムとして利用していた機器を廃棄する際の情報漏えいリスクを考慮したポリシー策定や取り決めを行い、その取り決めが確実の実施されているか確認する必要があります。

また、これらの廃棄の取り決めについては、機器・サービスのライフサイクルに関するセキュリティ要件でもあり、どのレベルまで求めるかは機器によっても変わるため、設計・仕様、建設段階での機器の選定、調達時に、あらかじめ検討しておくことが望ましいです。

利用していたサーバやPC内の記録媒体に保存された機密データの廃棄方法は、以下に示すものがあります。

1．物理的に破壊する

HDDや機器自体が故障して通電しない場合に、メディアシュレッダーや穿孔破壊するなどして、物理的に破壊します。

2．データを完全に消去するツールを使用する

① 上書き消去

- ソフトウェアを使用してデータ全体を上書き消去する方法です。
- SSDはメーカーが配布・推奨している専用ツールやコマンドを使って上書きを行います。特にSSDの場合、通常のファイル消去では完全にデータが消去されない可能性があります。

② 磁気消去

- HDDに強力な磁気を照射し、HDD内の磁気記録領域に記録された情報を破壊する方法です。PC上でHDDが認識しないものでもデータ消去が可能で、故障しているHDDのデータ消去も可能です。

データ消去の処理が完了したら、媒体に格納されていたデータの機密性のレベルにもよりますが、シリアル番号や媒体の種類、データ抹消処理方法等を記載した「媒体廃棄証明書」を作成します。実際に、機器・媒体を廃棄する業者（廃棄業者）や機器をレンタル・リースした業者に対しても以下のような依頼をすることも対策として重要です。

1．廃棄業者に処理を依頼する際は機密保持誓約書を締結する

2．廃棄業者に処理を依頼した際は媒体廃棄証明書を受領する

また、HDDなどの記録媒体に保存されるデータ以外の機器内部に保存された個人データ、設定データおよびプライバシに関するデータ等についても削除が必要な点は留意しておく必要があります。

参考資料・ガイドライン

- SP 800-88 rev.1 Guidelines for Media Sanitization
  【米国国立標準技術研究所（NIST）】

謝辞

本書の作成にあたり、独立行政法人 情報処理推進機構 産業サイバーセキュリティセンター中核人材育成プログラムの講師の小林和真先生、目黒有輝先生、並びに情報処理推進機構 中山顕様には、本チェックシートとガイドの元となるプロジェクトのメンター・講師として、ご指導・ご助言、ご支援を賜りました。改めて御礼申し上げます。

そして、本書の作成や本プロジェクトおよびテーマをともに実施した、メンバーの皆様にも感謝を伝えたいと思います。

プロジェクトメンバー

本書は、独立行政法人 情報処理推進機構 産業サイバーセキュリティセンター 中核人材育成プログラムにおける卒業プロジェクト「建設業とサイバーセキュリティ」内のテーマ「ビル設備におけるサイバーセキュリティ」の成果物として作成されました。

【凡例】◎：リーダー、○：サブリーダー、◇：テーマリーダー

	岩田 友臣		上田 祐司
	神田 真人	◎	菊川 智史
◇	小間 誠貴	○	佐藤 恭輔
	甚野 和成		土屋 拓仁
	水田 直人		

メンバー所属企業・協力企業一覧

株式会社アクティオ	アズビル株式会社
エヌ・ティ・ティ・コミュニケーションズ株式会社	株式会社大林組
株式会社きんでん	大成建設株式会社
高砂熱学工業株式会社	日本電気株式会社

付属資料A 参考文献

1. CIS(Center for Internet Security), CIS Critical Security Controls Version8, 2021
2. 技術研究組合制御システムセキュリティセンター(CSSC), ビルシステムにおけるサイバー・フィジカル・セキュリティ対策カタログ, 2022
3. 産業サイバーセキュリティ研究会 ワーキンググループ1(制度・技術・標準化) ビルサブワーキンググループ, ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン, 2023
4. 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) 工場サブワーキンググループ, 工場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, 2022
5. (独)情報処理推進機構, 中小企業の情報セキュリティ対策ガイドライン, 2019
6. (独)情報処理推進機構, 制御システムのセキュリティリスク分析ガイド, 2023
7. 英国工学技術学会(IET), Resilience and Cyber Security of Technology in the Built Environment, 2013
8. 英国工学技術学会(IET), Code of Practice Cyber Security in the Built Environment 2nd Edition, 2014
9. IoT推進コンソーシアム 総務省 経済産業省, IoT セキュリティガイドライン, 2016
10. 日本データセンター協会(JDCC), 建物設備システムリファレンスガイド(第三版)(構築・運用編), 2021
11. 日本データセンター協会(JDCC), 建物設備システムリファレンスガイド(第三版)(インシデント対応・セキュリティソリューション編), 2021
12. (一社)日本建設業連合会, 建設現場における情報セキュリティガイドライン, 2020
13. (一社)日本建設業連合会, 元請会社における情報セキュリティガイドライン, 2020
14. (一社)日本建設業連合会, 協力会社における情報セキュリティガイドライン, 2023
15. (一社)日本建設業連合会, 建設現場ネットワークの構築と運用ガイドライン, 2020
16. (一社)日本建設業連合会, 建設現場におけるスマートデバイス利用に関するセキュリティガイドライン, 2021
17. (一社)日本建設業連合会, 設備工事ポイントシート(若手向け) 13-3 竣工図書・備品・メーター読合せ, 2023
18. JPCERTコーディネーションセンター(JPCERT/CC),J-CLICS STEP1／STEP2(ICSセキュリティ自己評価ツール), 2013
19. 経済産業省 商務情報政策局 サイバーセキュリティ課, サイバー・フィジカル・セキュリティ対策 フレームワーク, 2019
20. 経済産業省、(独)情報処理推進機構, サイバーセキュリティ経営ガイドライン, 2023
21. 国土交通省住宅局, 防災拠点等となる建築物に係る機能継続ガイドライン(新築版), 2019
22. 米国国立標準技術研究所(NIST), Framework for Improving Critical Infrastructure Cybersecurity, 2018
23. 米国国立標準技術研究所(NIST), SP 800-53 Rev.5 – Security and Privacy Controls for Information Systems and Organizations, 2020
24. 米国国立標準技術研究所(NIST), SP 800-82 Rev.2 – Guide to Industrial Control Systems (ICS) Security, 2015
25. 米国国立標準技術研究所(NIST), SP 800-88 Rev.1 – Guidelines for Media Sanitization, 2014
26. 米国国立標準技術研究所(NIST), NISTIR 7628 Rev.1 – Guidelines for Smart Grid Cybersecurity, 2014
27. Telecommunications Industry Association(TIA), SMART BUILDINGS CYBERSECURITY DESIGN APPROACH FOR MULTI-STAKEHOLDER ENVIRONMENTS, 2022
28. アメリカ合衆国エネルギー省(DoE), Facility Cybersecurity Framework(FCF)
29. アメリカ合衆国エネルギー省(DoE), Facility Cybersecurity Capability Maturity Model (F-C2M2)

付属資料B 用語集

用語	意味・解説
Attack Surface	攻撃対象領域とも呼び、サイバー攻撃の対象となりうるIT資産や攻撃点ならびに攻撃経路を指します。
BAS機器	BAS（Building Automation System）機器は、建物の自動化や制御を担当する機器やシステムのことを指す。BAS機器は、建物内の各種設備やシステムを監視・制御し、効率的な運転や快適性の確保を目指します。
BCP (Business Continuity Plan)	企業が自然災害、テロ攻撃、サイバー攻撃などによる被害が発生した場合において、中核となる事業の継続、早期復旧を実現するために、平時及び緊急時における事業継続のため手段等を取り決めておく計画を指す。
BIM (Building Information Modeling)	コンピュータ上に作成した主に3次元の形状情報に加え、室等の名称・面積、材料・部材の仕様・性能、仕上げ等、建築物の属性情報を併せ持つ建物情報モデルを構築するものを指す。
CISO (Chief Information Security Officer)	経営陣の一員、もしくは経営トップからその役を任命された、セキュリティ対策を実施する上での責任者を指す。
C工事	テナント内部の工事など、借り主（テナント入居者）側が発注して行う工事。
DDoS攻撃（Distributed Denial of Service）	ビルシステムに係る機器やサーバが処理できないほどの大量のアクセス要求を多数の端末から一斉に送りつけることで、サービス停止に追い込むサーバ攻撃を意味する。複数台のインターネットに接続された端末が連携して攻撃することが最大の特徴です。
DMZ	直訳すると「非武装地帯」で、ビル内部の内部ネットワークと外部の公衆ネットワークの間に配置されるセグメントやネットワーク領域を指す。 DMZは、ビルシステムの外部からのアクセスを制限し、セキュリティを強化するために使用される。一般的に、インターネットへの公開サービス（ウェブサーバ、メールサーバなど）や外部システムとの接続（VPNゲートウェイ、パートナーシステムなど）は、DMZ内に配置される。ビルシステムの内部ネットワークと外部ネットワークの間に存在するセキュリティ上のバッファゾーンであり、外部からの攻撃や不正アクセスから内部ネットワークを保護する役割を果たす。
EPS	電気配線用の縦シャフトのこと。Electric Pipe Shaft または Electric Pipe Space の頭文字をとったもの。床を電線が貫通する場合に用意される縦穴のことで、電気・通信関係の配線を通すために使われる。
FIDOセキュリティキー	FIDO(Fast IDentity Online)とは、標準規格団体である「FIDO Alliance」が定めた新しい認証の方式。FIDOセキュリティキーは、多要素認証 (MFA)を行うためのデバイスの一種。
IDF室	Intermediate Distribution Frameの略で、電話回線や通信回線の中間配線盤のこと。一般的には、大型オフィスビルなどの1階共用部分や管理人室などに設置されているMDF（主配線盤）から配線され、各階ごとにIDFが設置され、各回線をまとめて管理する。
IDS	Intrusion Detection Systemの略で侵入検知システムのことを指す。通信の監視および管理者への警告を行うためのセキュリティシステム。
IPS	Intrusion Prevention Systemの略で侵入防止システムのことを指す。IDSの機能に加え、通信の遮断まで行うことができるセキュリティシステム。

付属資料B 用語集

用語	意味・解説
MDF室	Main Distributing Frameの略称。電話回線や通信回線の主配線盤のこと。一般的には、大型オフィスビルなどの1階共用部分や管理人室などに設置されている。NTTの収容局から電柱や地下経由で、ビル内のMDFまで必要に応じた配線数を引込んでいる。 事務所ビルや集合住宅等の建物で電話やインターネットの通信回線を室ごとに引き込まなくとも、規模や用途に応じた局線回線を引き込み、建物の内線回線を収容する主たる配線盤のことを言う。
VE（Value Engineering）	コスト削減やパフォーマンスの向上を目的として、プロジェクトや製品の設計や仕様を見直し、より効率的で経済的な解決策を見つける手法。
UTM	Unified Threat Managementの略で、統合脅威管理のことを指す。 ファイアウォール、アンチウイルス、Web（URL）フィルタリング、IDS/IPSといったさまざまなセキュリティ機能を1つのデバイスに集約している。
インシデント	望まない単独もしくは一連のセキュリティ事象、または予期しない単独もしくは一連のセキュリティ事象であって、事業運営を危うくする確率及びセキュリティを脅かす確率が高いもの。
イントラネット	イントラネット(Intranet)とは、内部（intra）とネットワークを意味する（net）を組み合わせた言葉であり、直訳すると「内部ネットワーク」のことを指す。企業内など限られた範囲内で利用可能なネットワーク環境である。
ウィルス検疫	コンピュータシステムやネットワークにおいて、潜在的なマルウェアやウイルスを定期スキャンで検出し、その拡散や被害の防止を目的としたセキュリティ対策の一つ。
サービス不能攻撃（DoS）	悪意ある第三者等が、ソフトウェアの脆弱性を悪用しサーバ装置または通信回線装置のソフトウェアを動作不能にさせることや、サーバ装置、通信回線装置又は通信回線の容量を上回る大量のアクセスを行い、通常の利用者のサービス利用を妨害する攻撃を指す。
サイバーセキュリティ	サイバーセキュリティとは、電子データの漏えい・改ざん等や、期待されていたITシステムや制御システム等の機能が果たされないといった不具合が生じないようにすることを指す。
サイバー攻撃	コンピュータシステムやネットワークに、悪意を持った攻撃者が不正に侵入しデータの窃取・破壊や不正プログラムの実行等を行うことを指す。
サプライチェーン	複数の事業者間での受発注等の契約を介した物や情報のやりとりを行うためのつながりのことを指す。具体的には、部品製造を担う企業とそれらの部品を用いて組立を行う企業との関係にとどまらず、クラウドサービスなど外部のデジタルサービスの利用や、API（アプリケーションプログラムインタフェース）を介したシステム同士の連携などもサプライチェーンに含まれる。
サプライチェーン攻撃	ターゲット企業に直接サイバー攻撃を行うのではなく、セキュリティ対策に弱点がある関連企業や取引先・委託先企業に攻撃を仕掛け、この企業を踏み台としてターゲット企業に不正侵入を行うサイバー攻撃を指す。
ステークホルダ	ビルの計画、設計、建設、運営、メンテナンス、利用に関わる利害関係者のことを指し、様々な側面で影響を及ぼす。 ビルに関わる利害関係者は、オーナー/投資家、開発業者/建設会社、利用者/テナント、管理会社、ファシリティマネージャーなどがある（地域住民、行政機関/規制当局は除く）。
スマートデバイス	スマートフォンやタブレット端末の総称。

付属資料B 用語集

用語	意味・解説
セキュリティコミュニティ	情報共有や協力を通じてセキュリティに関する知識や実践を深めるためのグループやネットワークのことを指す。 主にセキュリティに関連する最新の脅威や攻撃手法、防御策、ベストプラクティスについての情報が共有される。
セキュリティ・バイ・デザイン	情報セキュリティを企画・設計段階から確保するための方策を指す。建物の企画・設計のフェーズからセキュリティ対策を組み込み、サイバーセキュリティ対策を確保しておく概念として、適用することができる。
セキュリティパッチ	発見された情報セキュリティ上の問題を解決するために提供される修正用のファイルを指す。提供元によって、更新プログラム、パッチ、ホットフィクス、サービスパック等名称が異なる。
ネットワークセグメント	ネットワーク内の論理的な区切りのことを指す。ネットワークセグメントは、セキュリティやパフォーマンスの向上、管理の容易化などの目的で使用される。通常、異なるセグメントは異なるネットワークアドレス範囲を持ち、それぞれのセグメントは特定のネットワークリソースやユーザグループにアクセス権を制限することができる。
パケットの通信	データを転送する際に使用される基本的な方法。データはパケットと呼ばれる小さな塊に分割され、それぞれがネットワーク上を独立して転送される。パケット通信では、送信元のコンピュータがデータをパケットに分割し、それぞれにヘッダと呼ばれる制御情報を付加する。ヘッダには、送信元と宛先のIPアドレス、パケットの順序や確認情報などが含まれる。これにより、パケットはネットワーク上を独立して転送され、目的地で再結合される。
パッシブデザイン	空調・換気設備における冷暖房装置の使用を最小限に抑え、自然の風や日射、熱の移動を活用することで、エネルギー効率を向上させることを指す。
ビル設備システム	ビルの管理・運用を行うための制御システムで、受変電、熱供給、空調、給排水、照明、昇降機、防犯、防災、監視カメラ等の各設備の制御システムの総称。
ファイアウォール	あるコンピュータやネットワークと外部ネットワークの境界に設置され、内外の通信を中継・監視し、外部の攻撃から内部を保護するためのソフトウェアや機器、システム等のこと。
マルウェア感染	セキュリティ上の被害を及ぼすウイルス、スパイウエア、ボットなどの悪意をもったプログラムを指す総称 。これらのプログラムは、使用者や管理者の意図に反して（あるいは気づかぬうちに）コンピュータに入り込み悪意ある行為を行う。
ランサムウェア	「Ransom（身代金）」と「 Software（ソフトウェア）」を組み合わせた造語。感染したパソコンのデータを暗号化するなど使用不可能にし、その解除と引き換えに金銭を要求する。さらに新たな攻撃手法として、ターゲットとなる企業・組織内のネットワークへ侵入し、パソコン等の端末やサーバ上のデータを窃取した上で一斉に暗号化してシステムを使用不可能にし、データの復旧に対する金銭要求に加えて、窃取したデータを公開しない見返りの金銭要求も行うなど、二重の脅迫を行う場合もある。
リモート接続	建物内の設備やシステムに対して、物理的にその場にいる必要なく、リモートからアクセスして制御や監視を行うことを指す。リモートモニタリング、リモート制御、遠隔トラブルシューティングが可能です。
レジリエンス	組織や事業への影響を最小限に抑えながら事業を継続する一方で、ある程度の失敗や混乱に耐え、ダイナミックな内部または外部の変化に適応または対応することができる能力の事をいう。

付属資料B 用語集

用語	意味・解説
横ルート	建物や施設内で電気や通信などの信号を伝送するため、同じ階層やフロア内での配線経路として設計される。
縦ルート	建物や施設内で電気や通信などの信号を伝送するため、建物の階層間やフロア間での配線経路として設計される。
縦配線	建物や施設内で電気や通信などの信号を伝送するため、建物の階層間やフロア間での信号伝送を行うための配線をいう。
情報資産	組織内、業務で使用する機器やシステム内の重要な情報のことを指す。情報資産は、機密性、完全性、可用性などの特性を持ち、組織の活動や業務の遂行において価値があるとされます。
脆弱性	1つ以上の脅威によって付け込まれる可能性のある、資産又は管理策の弱点。[JIS Q27000:2014]
標的型攻撃	特定の組織に狙いを絞り、その組織の業務習慣等内部情報について事前に入念な調査を行った上で、様々な攻撃手法を組み合わせ、その組織に最適化した方法を用いて、執拗に行われる攻撃を指す。典型的なものとしては、組織内部に潜入し、侵入範囲を拡大し、重要な情報を窃取又は破壊する攻撃活動が考えられる。これら一連の攻撃活動は、未知の手段も用いて実行されるため、完全に検知及び防御することは困難である。
不正アクセス	許可されていない方法でコンピュータシステムやネットワークに侵入する行為を指す。これは、不正な意図を持つ個人や組織によって行われることがある。
不正機器	組織やネットワークにおいて正当な許可を得ずに使用される機器を指す。例えば、個人所有のスマートフォンやタブレットなどのモバイルデバイス、USBフラッシュドライブや外部ハードドライブ、ワイヤレスルーターまたはアクセスポイント、ゲームコンソールやエンターテイメントデバイス等が該当する。
物理セキュリティ	物理的な手段や対策を用いて建物や施設、資産を保護するためのセキュリティ対策のことを指す。これは、人や機器が物理的にアクセスできる環境におけるセキュリティを強化するために行われる。

改訂履歴

版数	発行日	改訂履歴
第1版	2023年7月1日	初版発行

ビル設備におけるサイバーセキュリティ
セルフチェックシート 設問項目ガイド

2023年7月
独立行政法人情報処理推進機構
産業サイバーセキュリティセンター
中核人材育成プログラム 第6期生
建設業とサイバーセキュリティ