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

全体版

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

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（全体版）

段階	No.	設問	✓	設問項目ガイド対応ページ
1．「共通」	1	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？		7
	2	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？		9
	3	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？		11
	4	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？		13
	5	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？		15
2．「設計・仕様」	1	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？		17
	2	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？		19
	3	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？		21
	4	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？		23
	5	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？		25
3．「建設」	1	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？		27
	2	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？		29
	3	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？		31
	4	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？		33
	5	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？		35
	6	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？		37
4．「竣工」	1	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？		39
	2	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？）		41
	3	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？		43
	4	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？		45
	5	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？		47

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（全体版）

段階	No.	設問	✓	設問項目ガイド対応ページ
5．「運用」	1	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？		49
	2	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？		51
	3	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？		53
	4	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？		55
	5	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？		57
	6	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？		59
	7	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？		61
	8	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？		63
	9	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？		65
	10	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？		67
	11	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？		69
	12	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？		71
	13	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？		73
	14	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？		75
	15	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？		77
6．「改修・廃棄」	1	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？		79
	2	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？		81
	3	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？		83
	4	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？		85
	5	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？		87

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	○		○	○	○