

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

01 ビルのサイバーセキュリティ対策 には何が必要？

組織的対策

物理的対策

技術的対策

人的対策



02 ビルのサイバーセキュリティの現状

ビル設備・設備システムに対する攻撃事例

DDoS攻撃による
暖房停止

BAS機器のロック

カードキーシステムの
ランサムウェア被害

ビル設備・設備システムが
抱える課題

- ・ 超長期の運用
- ・ 長いライフサイクルにおける複数の段階
- ・ マルチステークホルダー
- ・ 多種多様なビル形態



03 セルフチェックシートで対策状況をCheck

上記のビル設備・設備システムが抱えるサイバーセキュリティの課題を踏まえて対策を解決するため、本セルフチェックシートを使用して、対象ビルの設備・システムに対するサイバーセキュリティ対策の状況を確認できます。

※セルフチェックシート記載の各設問は、必須要件ではありません。自社や対象ビルの要件・環境に対して必要な対策を検討・実施するためにご活用ください。

04 セルフチェックシートの特徴

1

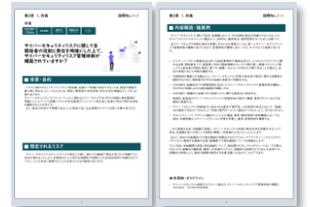
“ライフサイクル”
“ステークホルダー”
ごとに設問を整理

ビルのライフサイクルにおける段階とその段階に関わるステークホルダーごとに、設問の対象を設定！

自社に関連する内容を重点的に確認し、対策の検討・実施にご活用ください。

2

“設問項目ガイド”に
詳細な内容を記載



セルフチェックシートの設問に関して、その「背景・目的」、「想定リスク」、「内容解説・施策例」を設問項目ガイドに記載！

セルフチェックシートと併せてご利用ください。

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

使用
方法

01 本書の構成

- ① セルフチェックシート本体
- ② 設問項目ガイド

上記の2部で本書は構成されています。

1



2



02 各段階でセルフチェックシートの設問をCheck ✓

セルフチェックシートの設問項目は、ビルのライフサイクルの段階ごとに記載しています。各段階ごとに、各ステークホルダー企業の担当者が各項目に対する対策の検討・実施状況を確認します。どのステークホルダーが？どの段階に？何を検討・実施する必要があるのか？を記載しています。

ビルのライフサイクルにおける段階

1. 共通(全段階に共通して必要な項目)
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

ステークホルダーの分類

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
(元請・ゼネコン)

設備協力会社
(サブコン)

メーカー
ベンダー

03 設問項目ガイドで詳細をCheck ✓

セルフチェックシートの設問項目について、不明点等がある場合、設問項目ガイドの内容を確認します。

「設問項目ガイド」記載内容 3項目

背景・目的

セルフチェックシートの設問項目の背景と目的について説明しています。

想定されるリスク

セルフチェックシートの設問項目が検討・実施されていなかった(達成できていなかった)場合に想定されるリスク例を説明しています。

内容解説・施策例

セルフチェックシートの設問項目を達成するうえで、重要な内容や施策例を説明しています。