資料９

ビル分野における
サイバーセキュリティガイドライン開発

Jan/14/2021

マカフィー株式会社 佐々木　弘志

McAfee

アジェンダ

目的：
先行するビル分野SWGのセキュリティガイドライン開発の経緯や内容を紹介することで、宇宙産業SWGでの検討の方向性やアウトプットイメージの参考とする。

1. ビルシステムのセキュリティガイドライン開発の背景

2. サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）

3. ビルシステムのセキュリティガイドラインの概要・特徴

ビルシステムのセキュリティ
ガイドライン開発の背景

ビルシステムに対するセキュリティ脅威の増大

ビルシステムのオープン化

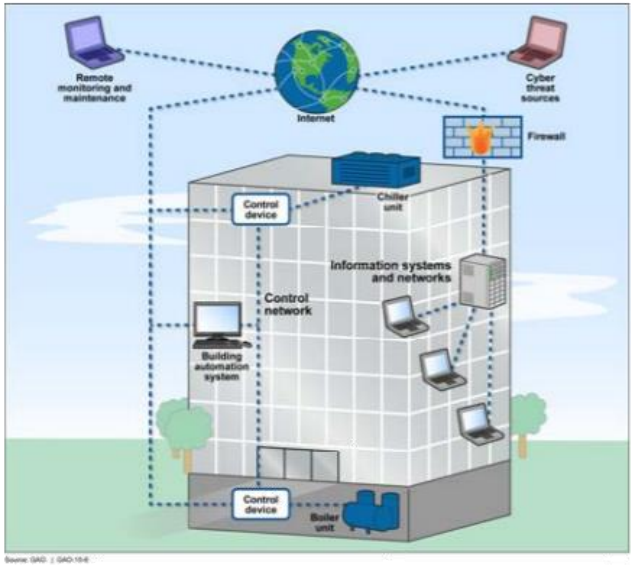


図 2-3　空調等をインターネット経由で遠隔から管理する例

ビルシステムに対する脅威

ビル管理システムで多く用いられている通信プロトコル（BACnet）のポートスキャンを観測（2014）

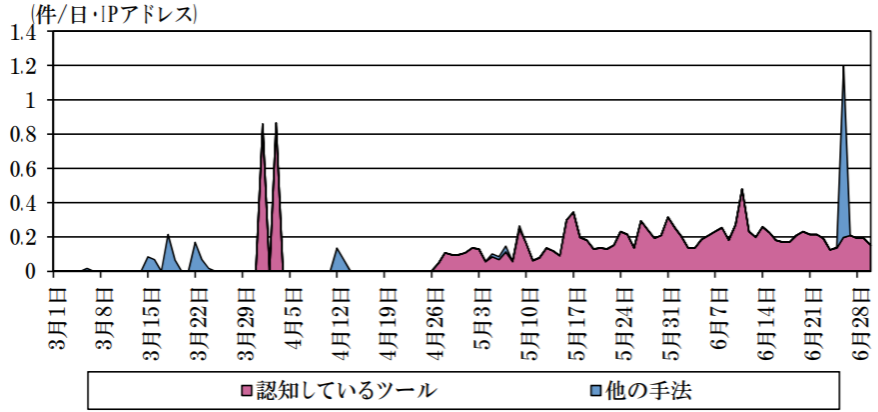


図2-1　BACnet システムの探索と考えられるアクセス件数の推移
(3月1日～6月30日)

リモートメンテナンス等の利便性追求のため、ビルシステムがオープン化
⇒　サイバー攻撃を受けやすい環境になっている

https://www.meti.go.jp/press/2019/06/20190617005/20190617005_01.pdf　警察庁発表：https://www.npa.go.jp/cyberpolice/detect/pdf/20140911.pdf

ビルシステムに対するセキュリティ脅威の増大

ビルシステムへのサイバー脅威事例と被害（想定も含む）

攻撃内容	発生事象	（想定）被害
ビル照明ハッキング	MITの学生が学内ビルの屋外から見える窓の照明を使って巨大なテトリスゲームにした。	学生による実験のため実害はなし。しかし、照明システムを遠隔制御することで、重要なイベント・会議中に照明を落とすなどの攻撃が可能である。
収容所の警備システムハッキング	マイアミの収容所の収容房の扉がリモート解除されて、収容されていた対立ギャング同士の抗争事件に発展した。	収容所内のギャングの諍いによる囚人・看守の負傷。もし外部へ続く扉が開錠されていれば、脱獄が起こっていたかもしれない。
ビルの暖房設備へのDDoS攻撃	フィンランドのビルの暖房が数時間にわたって停止した	ビル内の人への健康被害。11 月のフィンランドは外気温マイナス 2 度の環境であった。
ホテルのカードキー発行システムランサムウェア感染	オーストリアの 4つ星ホテルで、客室のカードキー発行システムの操作が不可能となった。	客室扉の施錠、開錠が不可能となり、宿泊客が閉め出される事態が発生した。結果、宿泊代の返金等の補償、一定期間ホテルを閉館して、鍵システムの刷新を行うなど多くの費用が発生した。
インターネットカメラのハッキング	日本国内各地で、インターネットカメラの画面が書き換えられた。（追記：ストリーミング映像が一般公開されるケースもあった。）	監視カメラの監視機能の喪失、映像記録の信ぴょう性の低下、カメラの映像が漏えいすることによるプライバシーの侵害、それに伴う訴訟の可能性もある。

https://www.meti.go.jp/press/2019/06/20190617005/20190617005_01.pdf　資料内の事例をもとに作成

ビルシステムの特徴

超長期の運用 （システム/10-20年）	複数フェーズの ライフサイクル	マルチステーク ホルダー	多種多様な ビルの種類

図 3-12　ビルのライフサイクルを意識した対策が必要

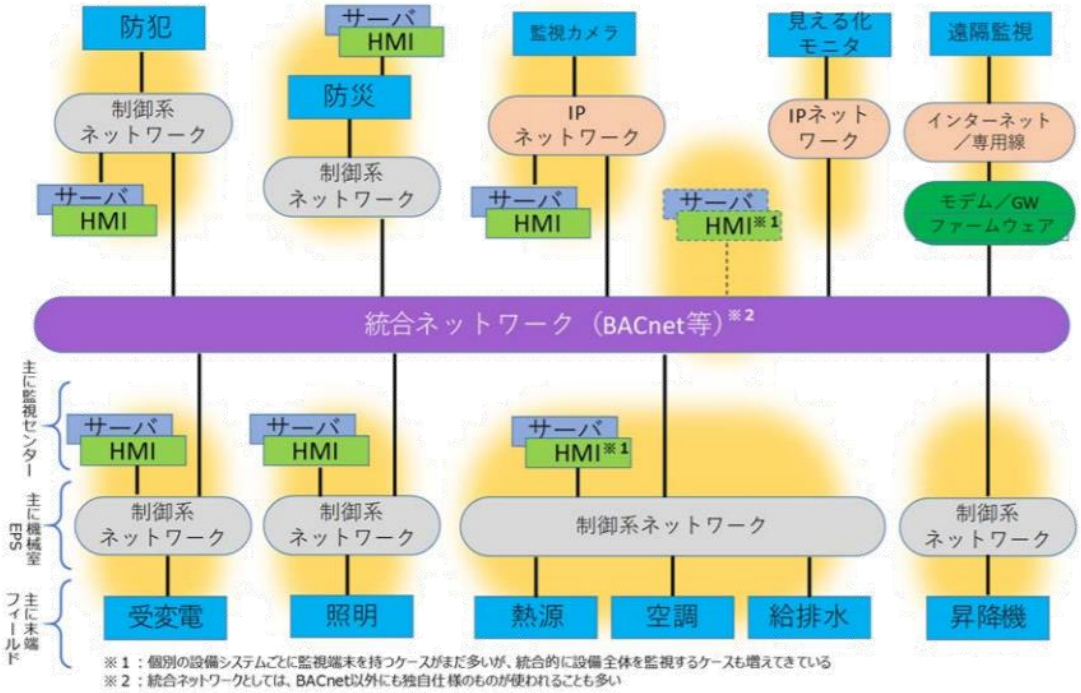


図 3-3　ビルシステムの標準的なモデル（全体像）

https://www.meti.go.jp/press/2019/06/20190617005/20190617005_01.pdf

ビルシステムのセキュリティガイドライン開発の背景まとめ

ビルシステムの環境変化

技術革新・利便性向上

・**インターネット接続機会が増加**

サイバー脅威の進化

・世界的に、ビルシステムを対象にした**サイバー攻撃が発生**
・ビルシステム**特有の通信手順**も攻撃対象となってきた

ビルならではの事情

・ビルシステムは、そのライフサイクルにおいて、**多様な関係者が関与する構造**であるためサイバーセキュリティ対策を**統合管理する体制を組織しずらい**

ビルシステムの多様な関係者が**共通して参照できるサイバーセキュリティ対策**の必要性

サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）

サプライチェーンリスク管理が政策の重要課題に

経済産業省より「サイバーフィジカルセキュリティ対策フレームワーク（CPSF）v1.0」公開

欧米において強化される『サプライチェーン』サイバーセキュリティへの要求

参考：産業サイバーセキュリティ研究会第1回にて配布

- **米国、欧州は、サプライチェーン全体に及ぶサイバーセキュリティ対策を模索。**

【米国】

- 2017年、**サイバーセキュリティフレームワーク**（NIST策定のガイドライン）**に、『サイバーサプライチェーンリスクマネジメント』を明記へ**
- 2017年末、**防衛調達に参加する全ての企業に対してセキュリティ対策（SP800-171の遵守）を義務化**

【欧州】

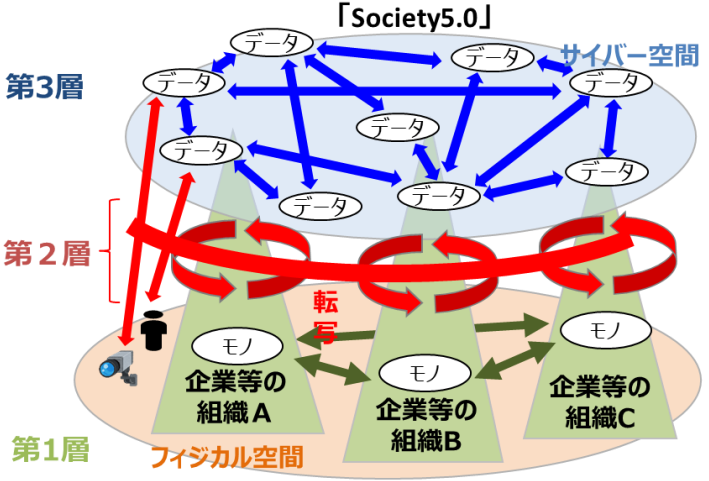
- 2016年、**エネルギー等の重要インフラ事業者に、セキュリティ対策を義務化（NIS Directive）**
- 2017年、**単一サイバーセキュリティ市場を目指し、ネットワークに繋がる機器の認証フレームの導入検討を発表**
- **EUの顧客データを扱う企業に対するデータ処理制限等の新たな義務（GDPR）を2018年から適用**
- **ドイツにおいてルーターのテクニカルガイドラインを作成中**

セキュリティ要件を満たさない事業者、製品、サービスは

グローバルサプライチェーンからはじき出されるおそれ

日本：産業サイバーセキュリティ研究会立ち上げ（2018年３月）
WGでフレームワークを策定・公開（2019年4月18日）

業界単位のSWG（ビル、電力、防衛産業、自動運転、スマートホーム）が設立



http://www.meti.go.jp/committee/kenkyukai/shoujo/sangyo_cyber/wg_1/pdf/001_06_00.pdf

CPSFをもとにした業界別のセキュリティガイドライン開発

ビルSWGによる
ガイドライン策定経緯

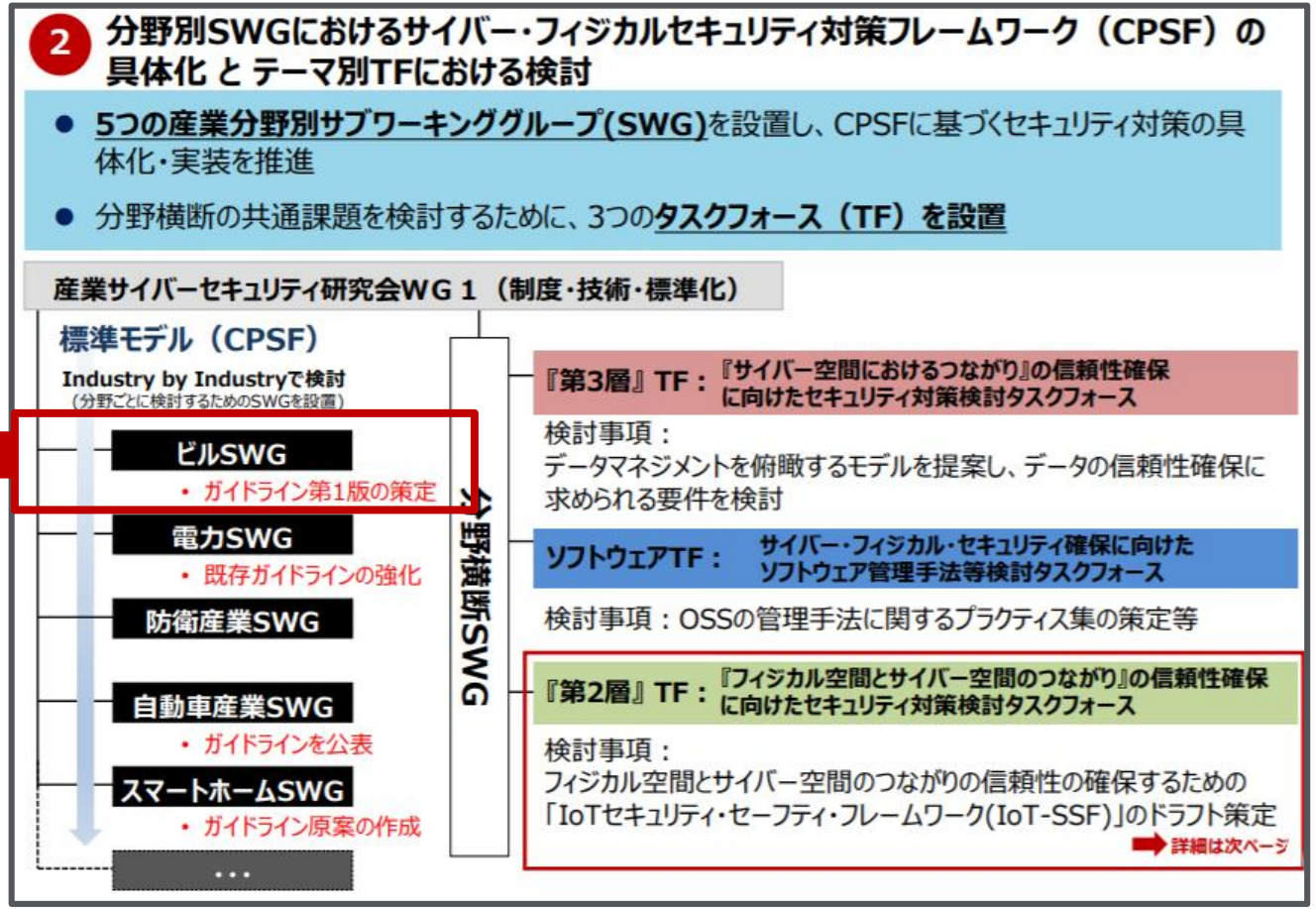
2017年12月：
産業サイバーセキュリティ研究会発足

2018年2月：
ビルSWG発足
ビルオーナー等含む業界のステークホルダーが参画

2018年10月：
ガイドラインβ版公開

2019年４月：
標準モデル（CPSF）公開

2019年6月：
ガイドライン第1版公開
（SWG発足から約1年4ヶ月）



https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/005_03_00.pdf

CPSFの概念と使い方

第Ⅰ部：コンセプト

サイバー・フィジカル・システムの
「3層構造」
「6つの構成要素」

第Ⅱ部：ポリシー

各層や要素を考慮した**リスク評価**及び**対策要件**を洗い出し

第Ⅲ部：メソッド

具体的な対策の検討
（リスクとマッピング）

＜三層構造と６つの構成要素＞
サイバー・フィジカル一体型社会のセキュリティのためにCPSFで提示した新たなモデル

- CPSFでは、産業・社会の変化に伴うサイバー攻撃の脅威の増大に対し、リスク源を適切に捉え、検討すべきセキュリティ対策を漏れなく提示するための新たなモデル（**三層構造**と**６つの構成要素**）を提示。

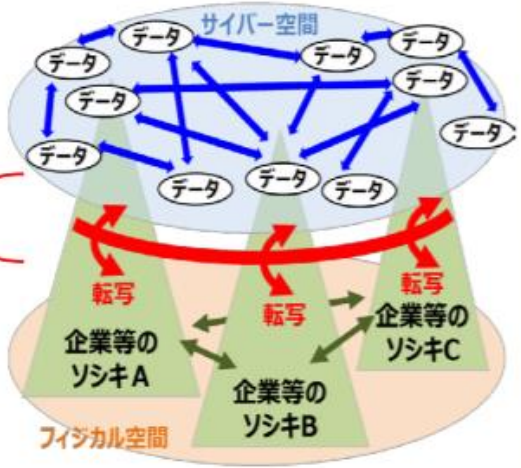
三層構造

「Society5.0」における**産業社会を３つの層に整理**し、セキュリティ確保のための信頼性の基点を明確化

サイバー空間におけるつながり
【第３層】
自由に流通し、加工・創造されるサービスを創造するための**データの信頼性**を確保

フィジカル空間とサイバー空間のつながり
【第２層】
フィジカル・サイバー間を正確に**“転写”する機能の信頼性**を確保
（現実をデータに転換するセンサーや電子信号を物理運動に転換するコントローラ等の信頼）

企業間のつながり
【第１層】
適切な**マネジメントを基盤に各主体の信頼性**を確保



６つの構成要素

対策を講じるための単位として、**サプライチェーンを構成する要素を６つに整理**

構成要素	定義
ソシキ	• バリュークリエイションプロセスに参加する企業・団体・組織
ヒト	• ソシキに属する人、及びバリュークリエイションプロセスに直接参加する人
モノ	• ハードウェア、ソフトウェア及びそれらの部品 操作する機器を含む
データ	• フィジカル空間にて収集された情報及び共有・分析・シミュレーションを通じて加工された情報
プロシージャ	• 定義された目的を達成するための一連の活動の手続き
システム	• 目的を実現するためにモノで構成される仕組み・インフラ

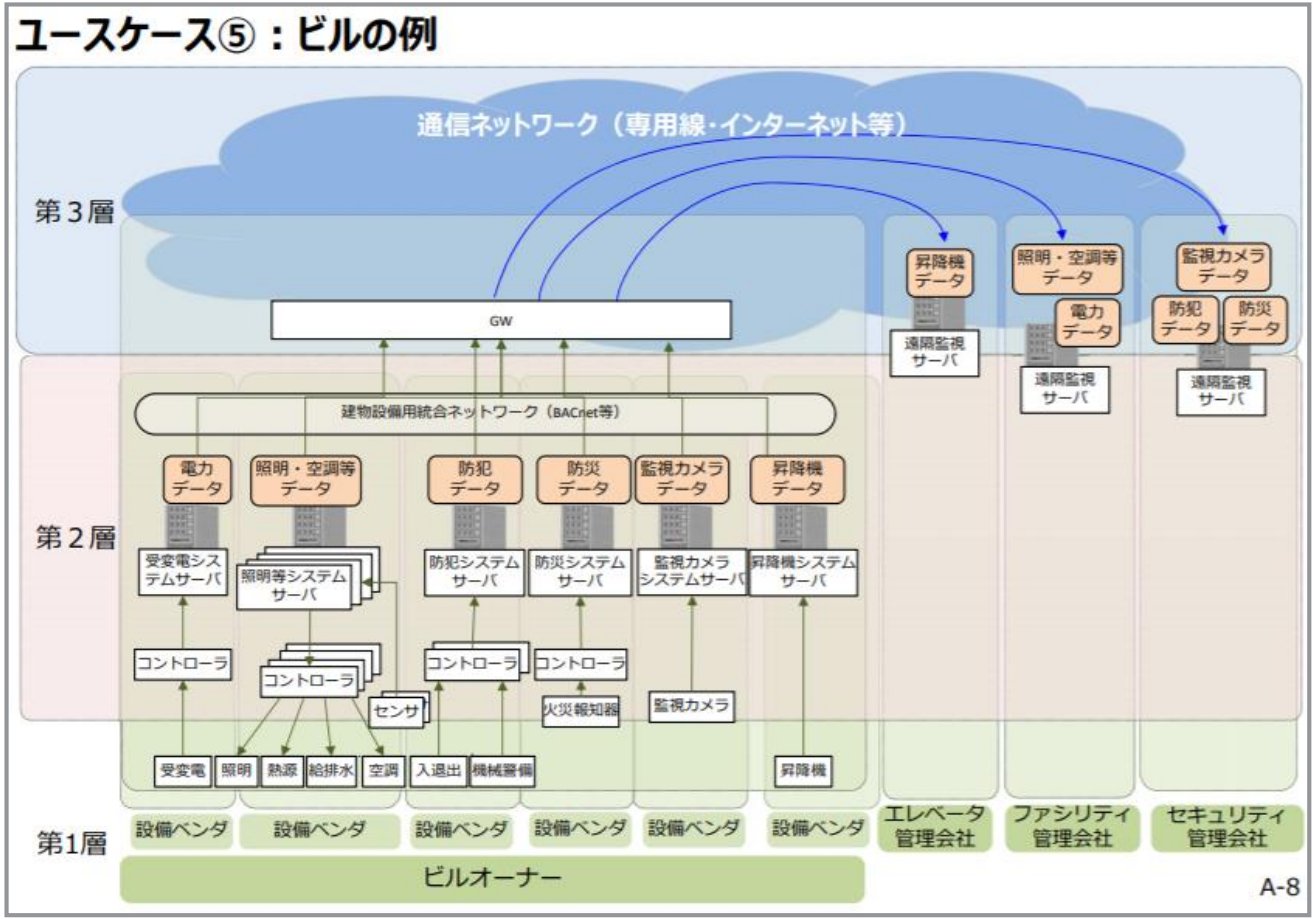
https://www.meti.go.jp/press/2019/04/20190418002/20190418002-1.pdf

CPSFのユースケース：ビルシステムの３層構造

CPSFの特徴

個別の組織ではなく、**マルチステークホルダーが関わるシステム全体を捉えた**フレームワークである。

様々な産業分野に共通で適用可能な**「フレームワーク」であるため、**セキュリティ対策を示すガイドラインは、個別の産業分野における**セキュリティリスクに応じて**検討する必要がある。



https://www.meti.go.jp/press/2019/04/20190418002/20190418002-2.pdf

ビルシステムのセキュリティガイドラインの概要・特徴

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の構成

目的・対象範囲・
対象読者
（はじめに）

脅威・
環境変化
（2章）

対策の基本的な考え方（３章）

対策要件
（4章）

ライフサイクルごとの対策要件
（5章：別紙表）

対策要件 → 設計・仕様 → 建設 → 竣工検査 → 運用 → 改修・廃棄

対応策													
インシデント起因機器	インシデント起因リスク源	No.	セキュリティポリシー	No.	設計・仕様(Method/Measure)：	No.	建設(Building)	No.	竣工検査(Completion inspection)	No.	運用(Operation)	No.	改修・廃棄(Reforming)
01.構成情報／管理情報													
011.ビルシステムへの被害発生時に、被害確認が遅れ、復旧作業の支障となる。													
0111.ビルの構成情報が最新状態に管理できておらず、機器の最新の接続関係が把握できない。													
		0111P1	構築システム構成図（設計時）に対し、引渡し時のシステム構成図を竣工引渡し書類として作成するように"設計仕様"に加える。 システム全体構成（外部接続先を含む）の最新状態を常に把握できるようにする。	1P1-	設計図書の特記仕様にシステム構成図を記載する。 システム全体構成の更新履歴、管理設備ごとの稼動履歴等、資産管理システム又は設備機器管理システムを利用した運用管理を行う仕様を明記する。	0111P1-M1B1	納品されるシステム構成品（設備）が設計仕様（同等品でも）と異なる場合、その内容を明記してシステム構成図を作成する	0111P1-M1C1	システム構成図と現場機器が合致しているかの確認を行い、引渡す。	0111P1-M1O1	変更が発生する都度、システム構成図を最新に更新して常に最新に保つ。	0111P1-M1R1	システム構成が更新や改修時に変更があった部分を最新の情報にシステム構成図を改め、古い構成図は廃棄処理を確認する。
02.バックアップデータ／事業継続													
021.適切なバックアップデータがなく、ビルシステムへの被害発生時に復旧作業の支障となる。													
0211.バックアップが取られていない、又はバックアップの範囲や対象が適切でない。													
		0211P1	システムバックアップ方法を運用側と確認の上でバックアップ方法を設計時に仕様を組み込む。 管理ポイントや運転スケジュール等、システムを運用するにあたって必要なデータについては、バックアップを取得する機能を具備する。	1P1-	システムバックアップ周期と操作権限者を定める。その上で、バックアップデータの取得・保管方法と再インストール方法を作成。			0211P1-M1C1	定められた方法で、システムバックアップデータが作成されることを確認する。その上で、作成されたバックアップデータが有効に再インストールできるか確認しバックアップデータをマニュアルとともに引渡す。	0211P1-M1O1	運用開始前に、バックアップデータからの復旧再インストールが行えることを確認する。 バックアップデータの保管場所管理の定期的確認を行う。 管理ポイントや運転スケジュール等、システムを運用するにあたって必要なデータについては、バックアップを取得する。	0211P1-M1R1	改修時のバックアップデータ廃棄を行う。

https://www.meti.go.jp/press/2019/06/20190617005/20190617005_02.pdf

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　5章抜粋

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

機器	インシデント	リスク源	No.	セキュリティポリシー	対応策 No.	設計・仕様(Method/Measure)：	No.	建設(Building)	No.	竣工検査(Completion inspection)	No.	運用(Operation)	No.	改修・廃棄(Reforming)
10.ネットワーク														
101.ビルシステムの一部に起きたマルウェア感染が、ビル内のネットワーク経由で容易に拡大していく。														
1011.ビル内のネットワークに様々なビル設備機器が混在して接続され、マルウェアの感染拡大防止を意識した管理がされていない。														
			1011P1	ビル内のネットワークをセキュリティポリシーに基づいて物理的又は論理的に分離する。	1011P1-M1	システムごとにネットワークセグメントを分離する。			1011P1-M1C1	ネットワーク設計どおりにセグメントが分離されていることを確認する。	1011P1-M1O1	ネットワークの変更時にセグメントが分離されていることを確認する。		
					1011P1-M2	システム・ネットワークの規模が大きい場合、単一システム内においてもセグメントを分離する。			1011P1-M2C1	ネットワーク設計どおりにセグメントが分離されていることを確認する。	1011P1-M2O1	ネットワークの変更時にセグメントが分離されていることを確認する。		
102.ビルシステムの一部に起きたマルウェア感染が、ビル内のネットワーク経由で容易に拡大していく。														
1021.ビル内のネットワークでやり取りされる通信が適切に管理されておらず、リモートからの不正侵入の防止を意識した管理がされていない。														
			1021P1	ビル内のネットワークにおいては、セグメント間通信を必要最小限に制限する。	1021P1-M1	収容システムの動作上必要なネットワークセグメント間通信は、必要な通信のみ許可する。			1021P1-M1C1	ネットワーク設計どおりに必要な通信以外が制限されていることを確認する。	1021P1-M1O1	ネットワークの変更時にセグメント間で必要な通信以外が制限されることを確認する。		
103.管理外の外部ネットワーク接続経由でマルウェア感染や不正侵入を受ける。														
1031.保守等の理由で外部接続が知らぬ間に取り付けられたり、外部との通信ポートが開けられたりするのを十分に管理・制限できていない。														
			1031P1	不正接続の有無を定期的に点検する。 外部との接続や通信はファイアウォール等により必要最小限に制限する。	1031P1-M1	外部ネットワークとの接続点にはファイアウォールを設置し、収容システムの動作に必要不可欠な最小限の通信のみを許容する。			1031P1-M1C1	ネットワーク設計どおりに必要な通信以外が制限されていることを確認する。	1031P1-M1O1	外部ネットワークとの接続は運用責任者が統制し、収容システムの動作に必要不可欠な最小限の通信のみが許容され、不正な外部ネットワーク接続がないことを定期的に点検する。		
104.管理外の外部ネットワーク接続経由で不正接続や攻撃を受ける。														
1041.ビルへの引き込み回線の管理が不十分で、勝手に不正な外部回線を引き込まれる。														
			1041P1	ビル内に設置する外部接続回線を管理し、不明回線の有無等を定期的に点検する。	1041P1-M1	運用フェーズにおける⇔引込回線の管理性を高めるため、外部接続回線の入線経路や回線引込エリアを規定（制限）する。			1041P1-M1C1	設計図書に記載されていない外部接続回線が設置されていないことを確認する。	1041P1-M1O1	運用責任者が外部接続回線の設置状況を定期的に点検し、不正な回線が引き込まれていないことを確認する。		
					1041P1-M2	施工者や入居者が許可なく回線を敷設できない運用ルールを定め					1041P1-M2O1	施工者や入居者が許可なく回線を敷設できない運用ルールを徹底		

ガイドラインを参考とし、各ライフサイクルにおけるステークホルダーが協力して
リスクに応じたセキュリティ対策を実施する

https://www.meti.go.jp/press/2019/06/20190617005/20190617005_02.pdf

参考）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

ガイドライン目次・大構成	概要
1. はじめに	ガイドライン策定の目的、適用範囲、対象読者、位置づけ、ガイドライン全体の構成
2. ビルシステムを巡る状況の変化	ビルの制御システムの特徴、脅威の増大、ビルシステムにおけるサイバー攻撃事例、サイバー攻撃された場合の影響
3. ビルシステムにおけるサイバーセキュリティ対策の考え方	ビルシステムのセキュリティ対策を検討する上で必要なビルのシステム構成、特徴、ライフサイクルを考慮した対策の考え方
4. ビルシステムにおけるリスクと対応ポリシー	ビルシステムにおいて想定されるセキュリティインシデントに対するリスク源（原因）とそれに対する対策要件を表形式で整理
5. ライフサイクルを考慮したセキュリティ対応策	4章で示した対策要件をビルシステムのライフサイクルごとの対策に展開して表形式で整理（別紙）
付録A：用語集	ガイドライン内で使用する主にサイバーセキュリティに関する用語の説明
付録B：JDCC の建物設備システムリファレンスガイドとの関係	日本データセンター協会『建物設備システムリファレンスガイド』と本ガイドラインとの関係性の説明
付録C：サイバー・フィジカル・セキュリティ対策フレームワークの考え方と、サイバー・ フィジカル・セキュリティ対策フレームワークの考え方を踏まえたビルシステムにおける ユースケース	サイバー・フィジカル・セキュリティ対策フレームワークの考え方の概要説明と、その考え方をビルシステムのユースケースに適用した場合の考え方
付録D：参考文献	本ガイドラインでは参照していないものも含めて、ビルシステムのセキュリティ対策に関連する国内外の取組みやガイドライン等を紹介
別紙：ライフサイクルを考慮したセキュリティ対応策	ガイドライン本体の５章の中身

https://www.meti.go.jp/press/2019/06/20190617005/20190617005_01.pdf 資料内の目次をもとに作成


McAfee™
Together is power.