2023 年 6 月 9 日
パナソニック ホールディングス株式会社
東京建物株式会社

国内初※1、ビルオートメーション向け通信規格 BACnet/IP®の制御コマンドレベル監視に対応

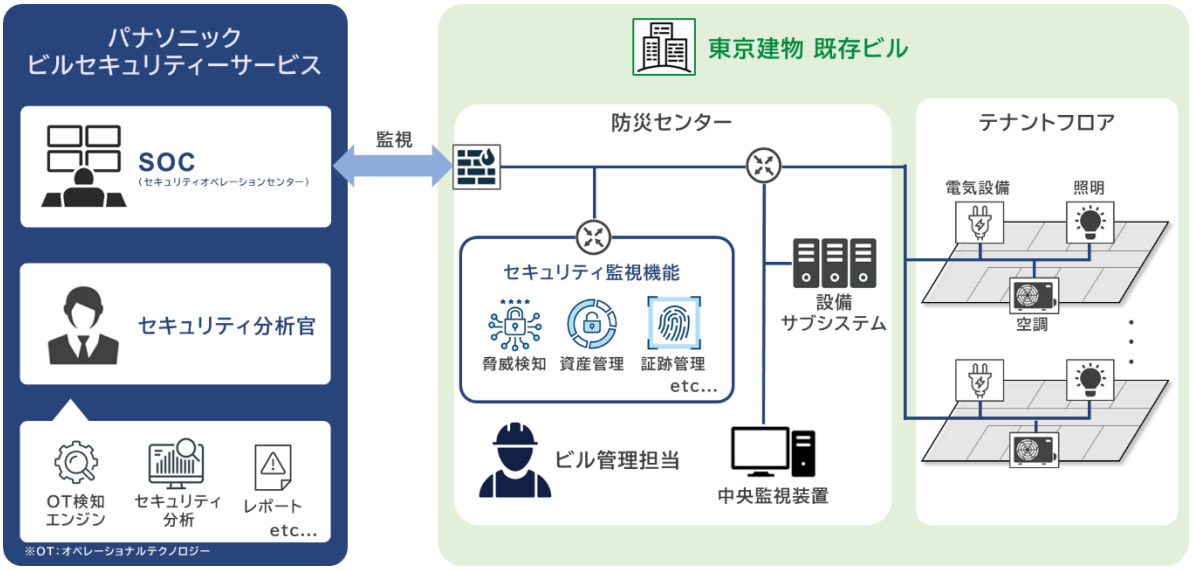
ビル向けサイバーセキュリティ監視サービスを既存ビルに本格導入

パナソニック ホールディングス株式会社（本社：大阪府門真市、代表取締役 社長執行役員 グループ CEO 楠見雄規、以下「パナソニック ホールディングス」）と東京建物株式会社（本社：東京都中央区、代表取締役 社長執行役員 野村均、以下「東京建物」）は、ビルオートメーションシステムのサイバー・フィジカル・セキュリティ対策に向け連携しており、今般、パナソニック ホールディングスが提供するビルオートメーションシステム向けサイバーセキュリティ監視サービスを首都圏にある東京建物の既存ビルに本格導入し、サービスを開始しました。

本サイバーセキュリティ監視サービスは、本格導入される商用サービスとして国内初となる※1BACnet/IP® ※2 プロトコルの制御コマンドレベルでの監視に対応しており、既存ビルに対しても設備への影響を最小限に抑えながら導入することが可能です。パナソニック ホールディングスが保有するビルセキュリティ監視の技術・ノウハウを用いることで、ビルに導入した脅威検知機能が検出したイベントの原因分析と影響分析を行い、ビルの運営者やテナントにとって重大なサイバー攻撃や異変が生じていることを素早く運営者に連絡し、対処することが可能となります。

本格導入するビル向けサイバーセキュリティ監視サービスの構成

本サイバーセキュリティ監視サービスでは、BACnet/IP®を用いるビルオートメーションシステムネットワークやネットワーク機器から情報を取得する構成を採用しています。



本格導入するビル向けサイバーセキュリティ監視サービスの構成図

サービスの背景

近年のオフィスビルでは、各種センサーや照明・空調・電力制御システムをビルオートメーションネットワークに接続して情報を収集し分析することで、照度・室温等を最適化したオフィス空間の提供やエネルギー利用の最適制御を実現する事例が増えてきています。それに伴い、ビルオートメーションネットワーク内の機器の相互通信や、外部サーバが提供する機能の活用のためにインターネットとの通信を行う必要性が出ています。これらの通信がインターネットを介した遠隔からのサイバー攻撃を可能にしてしまうリスクや、マルウェアに感染した機器からビルオートメーションネットワークを介して他の機器に感染させてしまいビルオートメーションシステムが正しく稼働しなくなるリスクに直結しています。例として、2016 年にはフィンランドのビルが DDoS 攻撃※3を受けて暖房システムが機能停止した事例や、2017 年にはオーストリアのホテルの客室ドア開閉システムがランサムウェア※4 に感染し一時閉館に追い込まれた事例などが報告されています。

このような背景から、経済産業省は 2019 年 6 月に「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第 1 版」を、2023 年 4 月には同ガイドラインの第2版を公開し、ビルオーナーを始め建設会社、各種設備機器ベンダ、保守会社等のビルに関わる事業者にサイバー・フィジカル・セキュリティ対策の要請を行っております。

サービスの主な特徴

今回本格導入するサービスの主な特徴は以下の通りです。

- ビル内の既存設備の稼働に殆ど影響することなく導入、運用することが可能であり、各種設備機器のベンダにも依存しないため、新規・既存問わず幅広いビルに導入可能です。
- 東京建物から提供を受けたビルオートメーションシステムネットワーク内の設備資産の情報とリアルタイム監視により得られた設備情報とを突合することで各設備資産のリアルタイムの稼働情報を更新し、攻撃監視に役立てています。
- オペレーショナルテクノロジー（OT）の脅威検知に秀でた脅威検知機能の導入と、ビルセキュリティ監視の知見を持つパナソニック ホールディングスのセキュリティ分析官が分析を行います。これにより異常な通信パターンや不審なアクティビティを素早く検出し、適切な対策をとることが可能になります。また、検出された脅威情報は速やかに東京建物の関連部署やビル管理会社に共有され、緊急時には迅速な対応を実現します。
- 証跡管理機能がビル内の通信ログを収集、蓄積することで発生した脅威の前後の記録に遡って詳細な分析を行うことが可能です。サイバー攻撃に限らず故障や操作ミスなどに起因する事象であってもログを残しているため原因の特定などに役立てることができます。
- 脅威が発生した際の分析レポートだけではなく、定期的にレポートを発行し、監視対象システムに生じている変化や改善すべき状況などを可視化しご提案することができます。

サイバー攻撃は最終目的到達までに対象システムで準備をするプロセスを踏むことも多いため、これらの取り組みによりビルオートメーションシステムのサイバーセキュリティ対策が強化されることで、サイバー攻撃の未然防止やビル設備のダウンタイム最小化といった効果を得られます。また、今回のサービスでは日々のビル管理業務等の運用により生じた

ビルオートメーションシステムネットワーク内の変化を検出・報告されることとなるため、サイバーハイジーン※5 や効率的な設備保全を実現することができます。

今後の展開

パナソニック ホールディングスと東京建物は、今後もビルのサイバー・フィジカル・セキュリティ対策の実現に向けて連携し、ビルを利用されるお客様の更なる安全・安心・快適なビル環境づくりを目指します。

以上

※1：2023 年 6 月 9 日　パナソニック ホールディングス株式会社調べ
※2：BACnet®は、ASHRAE の米国およびその他の国における登録商標または商標
※3：システムの処理性能を大幅に超える大量のデータを送信し機能不全を引き起こす攻撃
※4：感染したコンピュータのデータを暗号化して利用できない状態とし、復旧と引き換えに金銭を要求する悪意のあるソフトウェア
※5：組織のデジタルシステムとネットワークの健全性とセキュリティを維持するために設計された一連の慣行と対策

【関連情報】
ビルオートメーションシステム向けサイバーセキュリティソリューションの実証実験を開始
https://news.panasonic.com/jp/press/jn200114-1