NEWS RELEASE

東京建物

2020 年 1 月 14 日

報道関係各位

東京建物株式会社
パナソニック株式会社

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

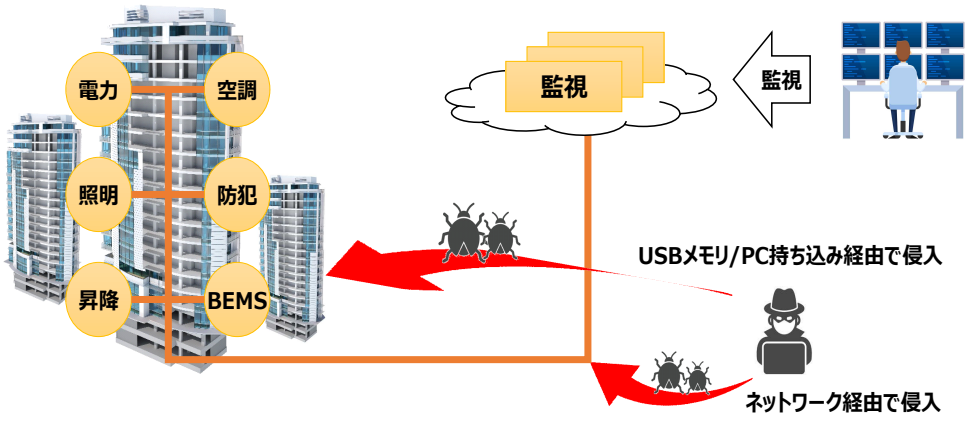
東京建物株式会社（本社：東京都中央区、代表取締役 社長執行役員 野村均、以下「東京建物」）とパナソニック株式会社（本社：大阪府門真市、代表取締役社長 津賀一宏、以下「パナソニック」）は、ビルオートメーション（BA）システムのサイバー・フィジカル・セキュリティ対策に向け、パナソニックが開発中である BA システム向けサイバーセキュリティソリューションの実証実験を首都圏にある東京建物の既存ビルで実施することに合意しました。

今回の実証実験ではサイバー・フィジカル・セキュリティ対策を行うために設備資産の調査を行い、サイバー攻撃のリスク評価を行います。さらに、設備資産の調査において収集した通信データに BA システムの攻撃データを模した通信を紛れ込ませたサイバー攻撃のシミュレーションデータを生成します。これをパナソニックが保有する AI 技術を活用したサイバー攻撃検知ソフトウェアに入力し、疑似サイバー攻撃の通信を検知可能か、実証実験を行います。

・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 BA 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。また、ビル管理業務の効率化のため、複数ビルをインターネットで接続し同一拠点から遠隔で監視する運用も行われつつあります。これら BA システムの高度化により利便性が高まる反面、インターネットを介した遠隔からのサイバー攻撃により BA システムが正しく稼働しなくなるリスクも高まっています。例えば、2016 年にはフィンランドにあるビルが DDoS 攻撃(※1)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にあるホテルの客室ドア開閉システムがランサムウェア(※2)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。

このような背景のもと、2019 年 6 月に経済産業省は「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。



・実証実験の概要

従来、BA システムは設備機器ベンダの独自プロトコルが主流で機器間の連携が困難でしたが、ビル設備を統合的に監視・制御する必要性から 2003 年にオープンな国際標準規格である BACnet®（Building Automation and Control Networking Protocol）が策定され、今日では BA システムにおけるデファクトスタンダードとして利用されています。これにより、低コストで異なるベンダの設備機器を連携させることが可能となってきました。しかし、BACnet はオープン仕様であり攻撃者側も容易に仕様を入手・理解することが可能であるため、攻撃の難易度は下がる傾向にあります。一方で、ビルは竣工してから数十年にわたって 24 時間体制でシステムを安定稼働させ、ビルの利用者へ空調、照明やセキュリティなどの機能を提供し続ける必要があります。安定した稼働を最優先する運用下においては、Windows®のような汎用 OS のセキュリティ脆弱性が発見された場合であっても、対策がシステム全体へ悪影響を与えないか慎重に見極める必要があります。これらの検証には時間を要する場合が多く、一般的に迅速に対策を導入することは難しい傾向にあります。

こういった課題に対応するため、パナソニックでは将来の BA システムに求められるサイバーセキュリティソリューションの開発を進めています（表 1）。BA システムのサイバー・フィジカル・セキュリティ対策を行うためには、対象システムにどういった設備資産が存在し、どういった運用がなされているかを可視化した上で、サイバー攻撃のリスク評価を行う必要があります。今回、パナソニックは東京建物の既存ビルに対してこのリスク評価を実施していきます。具体的には BA システムの設備資産・運用といった設備資産調査を通じてシステムの脆弱性やサイバー攻撃が行われやすい攻撃ポイントを特定します。長年にわたるパナソニックの IoT 製品へのペネトレーションテスト(※3)で培ってきた攻撃者視点に基づくセキュリティ脅威分析を実施することで、BA システムのセキュリティリスクを可視化します。このリスクの可視化においては、運用稼働中の BA ネットワークを流れる通信データを収集し、伝送されている制御コマンドを分析することで現在の運用状況を踏まえた精度の高いリスクの分析を行うことを目指していきます。

この取組みにより、サイバー攻撃によるビルやテナントが被る被害を可視化することができるため、サイバー・フィジカル・セキュリティ対策の優先度付けを行うことが可能となり、ビルのセキュリティ性能評価に向けた対策ロードマップを策定することが可能となります。

表 1：BA システム向けサイバーセキュリティソリューション

メニュー	概要
セキュリティリスク分析	・設備資産調査、攻撃シナリオの検討 ・セキュリティリスクの分析、重要度判定
セキュリティ対策の設計・導入支援	・セキュリティリスクに対する対策提案 ・残存リスクに対する監視方式提案 ・セキュリティ対策ロードマップ策定支援
セキュリティ遠隔監視	・残存リスクに対するセキュリティ異常兆候監視 ・定期的な監視レポート
セキュリティインシデント対策支援	・原因調査・対策支援

昨今の標的型攻撃と呼ばれる高度なサイバー攻撃を想定した場合、インターネットからのサイバー攻撃対策だけでは不十分であり、BA システムに悪意のあるソフトウェアが侵入したことをいち早く検知する IDS（Intrusion Detection System）製品の導入が重要です。ただし、社会的に BA システムに対する IDS 製品の性能を評価する手法やデータが十分に存在しておらず、ビルの所有者や管理者が適切な製品を選定出来ないといった課題がありました。

この課題に対応するため、今回のリスク評価において重大なリスクを引き起こす可能性があるサイバー攻撃を特定し、このサイバー攻撃を模した疑似通信データを既存ビルから収集した通信データに混入させることで IDS 製品の評価用データを生成します。また、パナソニックが開発中の AI 技術を活用したビル向けサイバー攻撃検知ソフトウェアが、疑似サイバー攻撃を検出できるか実証実験を実施します。

・今後の展開

東京建物とパナソニックは、実証実験で得られた知見をもとに、ビルのサイバー・フィジカル・セキュリティ対策にむけたソリューション開発で連携し、ビルに入居されてい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。

※1：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
※2：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
※3：既知の攻撃技術を用いて攻撃対象に侵入を試みることで脆弱性が存在しないか検証すること

以上