報道資料

SoftBank Technology

2018年4月10日

オフィスビルへのサイバー攻撃を想定した実証実験により、建物設備システムにおける脆弱性を発見

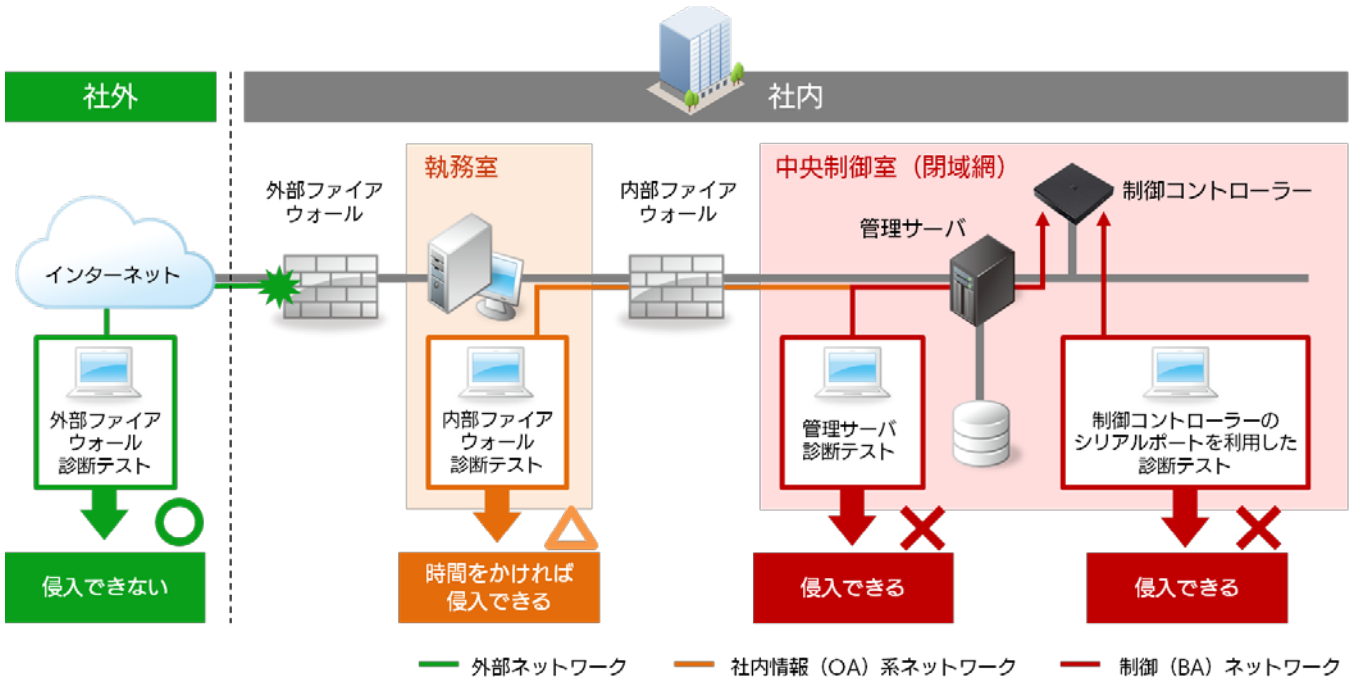
～ビルディングオートメーションシステム向けのセキュリティソリューションの開発を推進～

ソフトバンク・テクノロジー株式会社
サイバートラスト株式会社

ソフトバンク・テクノロジー株式会社（本社：東京都新宿区、代表取締役社長：阿多 親市、以下 SBT）とサイバートラスト株式会社（本社：東京都新宿区、代表取締役社長：眞柄 泰利、以下サイバートラスト）は、株式会社竹中工務店（本社：大阪市中央区、社長：宮下正裕、以下竹中工務店）と共同でビルディングオートメーションシステム（以下、BA と称する）※1 における設備環境を対象としたセキュリティ脆弱性診断の実証実験を実施しました※2。

その結果、社内情報（OA）系ネットワーク経由ならびに、閉域網での運用を前提とした制御（BA）ネットワーク自体からのサイバー攻撃では脆弱性が検出されました。これにより、制御（BA）ネットワーク上のサーバ（例えば、空調サブシステム等）類や機器への不正侵入、またはマルウェアを感染させることで電力システム、空調システム、照明システムなどをダウンさせるといった被害を及ぼす可能性があることが判明しました。

今回の結果を受け、SBT とサイバートラストの 2 社は竹中工務店と共同で、BA 設備環境へのセキュリティ対策として、社内情報（OA）ネットワーク経由ならびに、閉域網での運用を前提とした制御（BA）ネットワーク自体からの侵入に加えて、機器への物理的な攻撃も想定した対策を講じる必要があることを踏まえて、BA 向けセキュリティソリューションの開発を推進します。



＜実証実験結果イメージ図＞

■実証実験結果

本実証実験で実施したペネトレーションテスト※3の結果は以下のとおりです。

① 社内情報（OA）系ネットワークから閉域網での運用を前提とした制御（BA）ネットワークへの侵入可否：
実証実験では、社内情報（OA）系ネットワークから閉域網での運用を前提とした制御（BA）ネットワークへの侵入はできなかったが、時間を掛けて攻撃を実施することで、侵入される可能性があることが判明しました。

② 閉域網での運用を前提とした制御（BA）ネットワーク上のサーバ/機器に対しての侵入、攻撃：
制御（BA）ネットワークにアクセスがあった場合、対象システムが被害を受ける可能性があることが判明しました。

③ 設備を制御するコントローラ機器自体の評価：
省エネモニター（ディスプレイ）などの攻撃を受けることを前提に設計されていない機器に、一部セキュリティ機能が乏しい部分があり、これを踏み台にされることによりビル制御機器に被害を及ぼす可能性があることが判明しました。

■今後の展開

本実証実験の結果をもとに、BA/FA（Factory Automation）/PA（Process Automation）向け設備セキュリティソリューションの共同開発を推進し、新設・既設を問わず、BA をはじめとした EMS（エネルギーマネジメントシステム）市場や Industrie 4.0 を前提とした Smart Factory 市場におけるセキュリティ意識の向上に努め、安心・安全の高いオートメーション化を推進していきます。

（※1）ビルディングオートメーションシステム：ビルにある多種多様な設備（電力設備や空調設備、防災・防犯設備、エレベーターなどの機械設備）の機器の監視・管理・制御などを総合的に行う情報システム。機器の運用状況の監視や運用情報の記録・管理を統合的に行うことで、ビル内の安全性確保や、省エネの促進、防犯強化や管理業務の省力化などを実現可能にします。

（※2）本実証実験では、サイバートラストと「IoT/制御システムペネトレーションテスト」を提供する株式会社ベルウクリエイティブ（本社：東京都中央区日本橋、代表取締役：大和田 利郎）が共同でセキュリティ脆弱性診断を実施しています。

（※3）ペネトレーションテスト：ネットワークに接続されているシステムに対して、様々な手法で侵入を試みるテスト。主な調査項目として、DoS 攻撃（サービス拒否攻撃）を受けた際の耐久レベルや、実際に侵入された場合に他のコンピュータや外部ネットワークへ与える影響度合いなどがあります。

報道関係者様向け お問い合わせ窓口	ソフトバンク・テクノロジー株式会社 コーポレートコミュニケーショングループ（吉田、與儀）
	TEL：03-6892-3063 / Email：sbt-pr@tech.softbank.co.jp

別紙

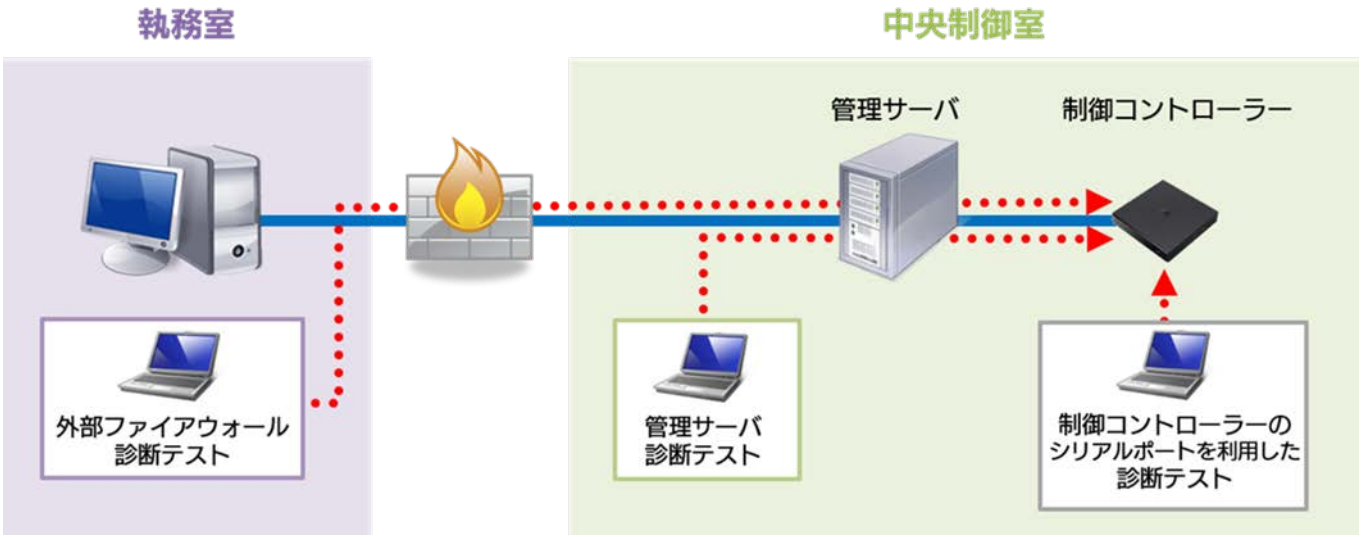
参考リリース）オフィスビルへのサイバー攻撃を想定した実証実験を開始
http://www.softbanktech.co.jp/corp/news/press/2017/046/

■実証実験概要

本実証実験では、竹中工務店所有ビルの制御システム関連装置や社内システムから制御（BA）ネットワークへの侵入を試み、不正アクセスやデータ改ざん、サービス停止を想定したペネトレーションテストを行いました。不正アクセス、情報漏えい、データ改ざん、サービス停止攻撃などの脅威から、オフィスビルに設置されているデバイスや設備を制御するコントローラ機器、ネットワークに潜む脆弱性を検出し、実際に侵入、攻撃を試みた上で、悪用の可能性及びオフィスビルのリスクについても調査しました。
今回の結果を受け、竹中工務店では対策を検討・実施しています。

＜ペネトレーションテスト対象及び観点＞
① 社内情報（OA）系ネットワークから閉域網での運用を前提とした制御（BA）ネットワークへの侵入可否
② 閉域網での運用を前提とした制御（BA）ネットワーク上のサーバ/機器に対しての侵入、攻撃
③ 設備を制御するコントローラ機器自体の評価

＜実施期間＞ 2017 年 11 月～2017 年 12 月末。



＜脆弱性診断のイメージ図＞

報道関係者様向け お問い合わせ窓口	ソフトバンク・テクノロジー株式会社 コーポレートコミュニケーショングループ（吉田、與儀）
	TEL：03-6892-3063 / Email：sbt-pr@tech.softbank.co.jp