

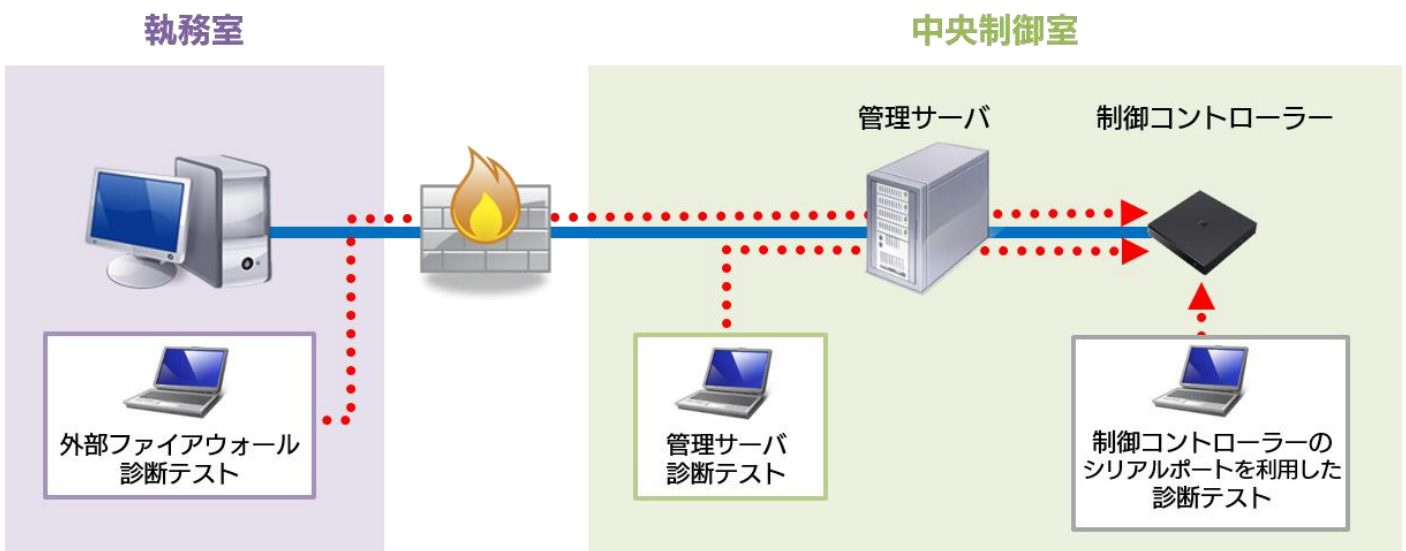
オフィスビルへのサイバー攻撃を想定した実証実験を開始

～ビルオートメーションシステムにおけるセキュリティ課題の顕在化と対策の実施～

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：阿多 親市、以下サイバートラスト）は、株式会社竹中工務店（本社：大阪府中央区、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※¹（以下ビルオートメーション）における IoT 機器のセキュリティ脆弱性診断の実証実験を行うことをお知らせします。

本実証実験では、竹中工務店所有のビルオートメーションシステム関連装置や社内システムからビルオートメーションへの侵入を試み、不正アクセスや情報漏えいを想定した脆弱性診断を行います。



脆弱性診断のイメージ図

■実証実験の背景

昨今、さまざまな機器がインターネットに繋がり、IoT 機器として家電や社会インフラなど多くの場面で使用されています。今後も IoT に対する社会的ニーズが強まることが予想され、総務省は、2020 年までに IoT 機器が 300 億個に増大すると発表※²しています。

建物においても、空調設備や電気設備、各種センサーなどさまざまな機器がネットワークに繋がり、建物の IoT 化が進んでいます。これらはビルオートメーションとして、建物全体のエネルギー省力化に寄与しており、改正省エネ法への対応や IoT 機器の普及によって今後も建物に対するエネルギー省力化の要求および市場規模が増大すると予測されています※³。

しかしながら、機器がインターネットに繋がることで、今までサイバー攻撃の対象ではなかった機器が攻撃の対象となり、IoT 機器の脆弱性を利用した乗っ取りや利用停止といった被害の報告があがっています。これを受け総務省は 2017 年 9 月に重要 IoT 機器に対する脆弱性診断の実施※⁴や、2017 年 10 月には IoT セキュリティの総合対策の公表※⁵をするなど、IoT 機器に対するセキュリティ対策が本格化されてきています。

こうした中、3社はビルオートメーションのIoT脆弱性セキュリティ診断を行い、ビルオートメーションにおけるIoT機器のセキュリティ課題を顕在化し、対策方法の検討を行います。

■各社の役割

・SBT

ビルオートメーション全般に向けた脆弱性の仮説立案と脆弱性診断後の機器レベルからネットワークレベル、遠隔監視までの対策およびソリューションの提供。

・サイバートラスト

IoT脆弱性診断の実施、結果レポートと対策の検討。

サイバー演習手順、評価の技術支援と重要機器などへの高セキュリティ対策の提供。

・竹中工務店

ビルオートメーションにおけるセキュリティ注力点の調査および検討と実環境での脆弱性診断実施。

脆弱性診断後の対策検討および今後の新規建築物などに向けたセキュリティ対策実装検討。

■診断概要

不正アクセスや情報漏えい対策として、デバイスや制御コントローラ、ネットワークに潜む脆弱性や潜在要因を検出します。

実証実験の実施期間は2017年11月から2017年12月までを予定しています。

主な診断項目（予定）

1.入出力処理に関する調査	各種サブシステムや制御コントローラに対するセンシング情報への不正アクセス、パラメータ改ざんなど
2.認証に関する調査	ログインフォーム、ログインエラーメッセージ、ログイン・個人情報の送受信など
3.認可に関する調査	権限昇格、権限のない情報へのアクセスなど
4.制御に関する調査	PLCや制御コントローラ（制御盤）、中央管理室設備に対する起動・停止や乗っ取り、不正制御可否
5.外部ポートに関する調査	デバイスのシリアルポートから侵入、悪意のあるコード挿入、漏えい可否など

■今後について

SBTとサイバートラスト、竹中工務店は本実証実験の結果をもとに、共同でビルオートメーションのセキュリティ対策を強化し、ビルオートメーションをはじめとしたEMS（エネルギー管理システム）市場のセキュリティ意識の向上に努めていきます。

※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（電気設備や空調設備、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する。

※2 総務省発表『平成29年版 情報通信白書』：<http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h29/html/nc133100.html>

※3 富士経済：『BEMS、BAS、ESP、FEMS エネルギーソリューションの国内市場を調査』：<https://www.fuji-keizai.co.jp/market/16081.html>

※4 総務省発表『IoT機器に関する脆弱性調査等の実施』：http://www.soumu.go.jp/menu_news/s-news/02ryutsu03_04000088.html

※5 総務省発表『IoTセキュリティ総合対策』の公表』：http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000126.html

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（皆口、吉田、與儀）

TEL：03-6892-3063 / Email：sbt-pr@tech.softbank.co.jp

※本リリースに記載されている会社名、製品名、サービス名は、当社または各社、各団体の商標もしくは登録商標です。