

セキュリティを脅かす“野良IoT”撲滅のための処方箋

IoT時代に求められるセキュリティ—その実現が運用の利便性も高める

あらゆるモノがインターネットにつながる IoT 時代において懸念されるリスクは、管理が行き届かない野良 IoT デバイスの存在だ。セキュリティを危険にさらす課題にどう対処すべきなのか。本稿で、1つの解決策を提示する。

リスクだらけの野良 IoT デバイス その解決は喫緊の課題

あらゆるモノがインターネットとつながっていく時代にあつて、野良 IoT デバイスの存在が懸念事項として指摘されている。野良 IoT デバイスとは、管理が行き届かずに放置されている機器のこと。ソフトウェアに関わる脆弱性が発見されても放置されたままのため、それを踏み台として同デバイスとつながったシステムなどに侵入されてしまう危険が伴う。実際、セキュリティ専門機関などにより数々の侵入事例も報告されている。

国内では「個人情報保護法」の改正、海外に目を向ければ「EU データー一般保護規則（GDPR）」の施行などを背景に、今や企業にとってセキュリティは避けて通れない問題だ。社内システムにどれほど気を配っていたとしても、IoT デバイスへの対策が抜け落ちていては対策が不十分と指摘されかねない。

そもそも野良 IoT デバイスが発生する要因は、運用管理に手間とコストを要すること。本来、機器を野良化させな

いたためには担当者による適切な管理、脆弱性やバグ発生時のリアルタイム対応などを求められる。だが、IoT デバイスは遠隔地や足を踏み入れにくい環境などに設置されることが多く、その管理には時間はもちろん、人件費や交通費などのコストもかさむ。さらに、設置場所が多様化しているため、管理できる範囲を超えてしまっているのだ。

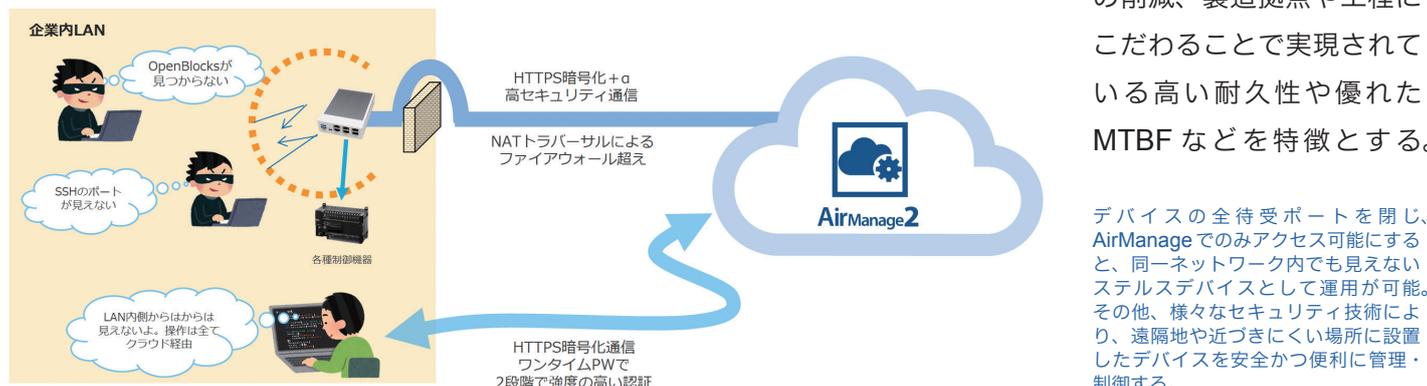
セキュア環境で遠隔管理を実現 OpenBlocks IoT ゲートウェイ

裏を返せば、リアルタイムに管理できる仕組みを持つ IoT デバイスならば、これらの課題を解決し IoT システムを安全かつ便利に運用できることになる。この点、野良 IoT の撲滅を掲げる、ぶらっとホームの IoT ゲートウェイ「OpenBlocks IoT シリーズ」には特筆すべき技術が盛り込まれている。

OpenBlocks IoT ゲートウェイは、モノとインターネットをつなぐ仕組みを、ユーザー側でいかに効率的に実現できるかを徹底追求した製品。IoT システムの構築・運用に必要な機能がモジュール化されたパッケージソフトウェア

「FW3」による開発工数の削減、製造拠点や工程にこだわることで実現されている高い耐久性や優れた MTBF などの特徴とする。

デバイスの全待受ポートを閉じ、AirManageでのみアクセス可能にすると、同一ネットワーク内でも見えないステルスデバイスとして運用が可能。その他、様々なセキュリティ技術により、遠隔地や近づきにくい場所に設置したデバイスを安全かつ便利に管理・制御する。



その中でも、野良 IoT 対策の特筆ポイントが、FW3アーキテクチャの1つとして搭載されたリモート管理サービス「AirManage」である。

セキュリティを高める 秀逸なステルス技術

AirManage は、遠隔地に設置した OpenBlocks IoT ゲートウェイをネットワーク経由で管理できるクラウドベースのアプリケーション。IoT ゲートウェイへの新規ソフトウェアの追加による機能拡張、ソフトウェアのバージョンアップ、脆弱性が発見された場合のセキュリティ修正プログラムの適用などの操作を現地に行くことなく即座に実行できる。時間指定アップデートや設定ファイルを自動で変更するリコンフィグ、設定ファイルを3世代前まで自動保存する設定バックアップ、ログ取得など機能も多彩で管理に必要な操作はすべて Web 画面上で行える。

しかも、IoT ゲートウェイごとに設定操作できただけでなく、複数デバイスを単位とした一括管理にも対応してい

るので機器数が増えても安心だ。

OpenBlocks IoT ゲートウェイの秀逸な点はセキュリティの高さ。遠隔管理の実現にはデバイスのポートを常時開く仕組みが一般的だが、OpenBlocks IoT シリーズではゲートウェイの全待受ポートを閉じた状態で、クラウド経由の AirManage によるアクセスのみを可能とすることにより、同一ネットワーク内でもデバイスが見えないステルス運用が可能となる。つまり、サイバー攻撃者にも発見されないため、セキュリティ性がきわめて高い。

さらに、AirManage と OpenBlocks IoT ゲートウェイとの通信はすべて HTTPS による暗号化に加えて、SSH ポートフォワード（トンネリング）技術により安全な通信環境が担保されている。また、管理コンソールへのログインではワンタイムパスワードによる2段階認証を採用することで、不正アクセスを防ぐ。

セキュアなネットワーク環境で実現される管理の利便性と機能の拡張性を特徴とする OpenBlocks IoT ゲートウェイは、中部電力や阪神電気鉄道などインフラ系企業や

通信系事業者、研究機関といった特に信頼性が重視される分野で採用されている。

野良 IoT 対策はもちろん、本格運用を視野に入れた TCO などの視点からも OpenBlocks IoT シリーズは有効だと考えている。

管理コンソールの操作性に配慮。画面から各 IoT ゲートウェイの Web ベース UI にアクセスして、AirManage 経由で設定の変更と確認を可能にした。

有効	ノード名	場所	カテゴリ	パッケージ Ver.	有効期限	ステータス	ダウンロード	更新	アクション
<input type="checkbox"/>	BX_SENSOR_DEMO	技術部冷蔵庫の上	obsbxstretch	openbl: 3.3.1-1 (3.3.0-13)	2030/12/31	% 更新あり(DL待機中)	02:04	ダウンロード直後	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	H_SHI_EX1_TEST	技術部冷蔵庫の上	obsbxstretch	openbl: 3.4.0-8 (3.3.0-13)	2030/12/31	% 更新あり(DL待機中)	02:00	ダウンロード直後	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	H_SHI_VX1_1GES	技術部東側換気機ラック	obsvxstretch	openbl: 3.3.1-1 (3.3.0-13)	2030/12/31	% 未接続	02:00	ダウンロード直後	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	H_SHI_VX2_AI_DEMO	4階南側のガラス壁貼り付け	obsvxstretch	openbl: 3.3.1-1 (3.3.0-13)	2030/12/31	% 更新あり(DL待機中)	02:07	ダウンロード直後	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	H_SHI_VX2_TEST		obsvxstretch	openbl: 3.4.0-8 (3.3.0-13)		% 更新あり(指示待ち)	手動	手動	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/>	VX_MOTION_CAMERA	技術部ドアの前	obsvxstretch	openbl: 3.3.3-1 (3.3.0-13)	2030/12/31	% 更新あり(DL待機中)	02:00	ダウンロード直後	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

ぷらっとホーム株式会社

〒102-0073 東京都千代田区九段北4-1-3 日本ビルディング九段別館3F
お問い合わせ TEL. 03-5213-4370 FAX. 03-3221-3766 E-mail. sales@plathome.co.jp
<https://www.plathome.co.jp/>

すべての製品名、サービス名、会社名、ロゴは、各社の商標、または登録商標です。製品の仕様・性能は予告なく変更する場合がありますので、ご了承ください。

2 セキュリティを脅かす“野良 IoT”撲滅のための処方箋