IT標準規格によるコネクテッド照明システムの保護

マイケル・スクルラ

照明やビル技術の統合を専門とする人々は、IT標準規格を採用して統合型スマートシステムを保護することにより、デバイスセキュリティにおける通信の抜け穴やギャップを塞ぐことができる。

4000万件のクレジットカードやデビットカードの番号が流出した2013年の米ターゲット社（Target）のデータ流出事件は、情報技術（IT）システムとビル運用技術（OT）システムを接続することのリスクを浮き彫りにした。「より洗練された種類のサイバー犯罪が、小売業界に初めてもたらされた事例だった。当社だけでなく、小売業界全体に注意喚起を促すものだった」と、ターゲット社の最高情報セキュリティ責任者を務めるリッチ・アゴスチノ氏（Rich Agostino）は、2020年のNational Retail Federation Big Show（全米小売協会主催の展示会）で述べた[1]。

この事件をおそらくきっかけとして、セキュリティパラメータの再分析と、小売セキュリティに関する現時点での絶対的基準の確立に向けた、かつてない規模の取り組みに小売業界は乗り出すことになった。攻撃者は、リモートビル管理及び監視システムを介して、最初のアクセスを獲得していた。情報漏洩は、電子メールによる初歩的なフィッシングによっても発生していた。詳細な調査によって、エッジデバイスセキュリティのポリシーと機能の認証が甘かったこと、また、サプライチェーンセキュリティに関する従業員トレーニングが不十分だったことが、明らかになった[2]。

それ以来、攻撃面（アタックサーフェス、攻撃対象領域）を小さく抑えることによって予期せぬやり取りを制限することを目的とした、セキュリティ設計が行われている。IoTによってこの攻撃面の潜在的範囲がどれだけ広く拡大されるかを、ネットワークセキュリティ専門家が理解したためである。IoTセキュリティは複雑である。エコシステムは目まぐるしく変化し、その飛躍的な成長によって、IoTは新たな攻撃にさらされることになる。照明とビルシステムを統合型（コンバージド）ネットワークに接続する専門家は、そうしたリスクを理解し、実証されたITセキュリティ対策を講じることによって、セキュリティギャップを緩和する必要がある。

通信システムにおける潜在的脆弱性の特定

商業施設の照明システムには必ず、通信ネットワークと、センサ、照明器具、照明制御のためのユーザーインタフェースといったインテリジェントなシステム要素が含まれている。照明ネットワーク技術は、独占的である場合が多いが、インターネットに通常は接続されている、パブリック（またはセミパブリック）ネットワークとのインタフェースを持つのが一般的である。このインタフェースは、独占的な部分をデジタル通信の標準規格に変換する、ブ

リッジまたはゲートウェイを介して実装される。標準規格として最も一般的なのは、イーサネットとTCP/IPスタックである。オープンな接続性の利点は、そうした標準規格を通じて他のシステムやデバイスと接続できるという、その本質的な能力にある。しかし、その本質的な「標準」の通信理念が、実質的に攻撃対象領域を生成する。

この攻撃対象領域は、通信媒体に大きく依存する。無線データ転送は、照明器具に組み込まれた短距離で低消費電力の通信デバイスや、以前は有線で接続されていた外部制御機器（壁スイッチ、モーションセンサ、調光器など）で、一般的に利用されている。この場合、通信は通常、本質的に独占的なものである。照明業界ではこれまでに、Zigbee、Wi-Fi、Bluetoothなどの標準規格が確実に導入されている（bit.ly/3ys6axrとbit.ly/3oyMgLPを参照）。しかし、それらの通信は、上流でゲートウェイまたはブリッジによって符号化されて、前述のパブリックまたはセミパブリックのネットワークにつながるイーサネットに送られる場合が多い。

照明システムをイーサネットに接続するのは避けたほうが良いというのが、一般的な見解だが、これが実行可能なケースは稀である。デジタル化されたこの時代において、ビルシステムの接続性には、高いレベルの効率、利便性、オートメーション、持続可能性、管理が求められる。照明技術は、単なる照明にとどまらない多くの役割を果たすことができるが、メーカーは、シンプルで安全で適切に構築された、他のビルシステムやITシステムとの相互接続方法を提供する必要がある。法的責任とは別に、メーカーは、ソリューションのセキュリティを提供する責任を負うことになる。

セキュリティに関するIT標準規格に従い、エッジベースのセキュリティを提供することによって、セキュリティプレーンのサイズを制限することが、簡単な解決策である。ITにおいて一般的に使われる「エッジ」という語は、一般的なIT手段によって相互に接続される領域にあるあらゆるものを指し、「エッジデバイス」は、家庭用サーモスタットから、商業施設にある照明やモーションセンサに至るまでの、インターネットに接続されるあらゆるものを指す。

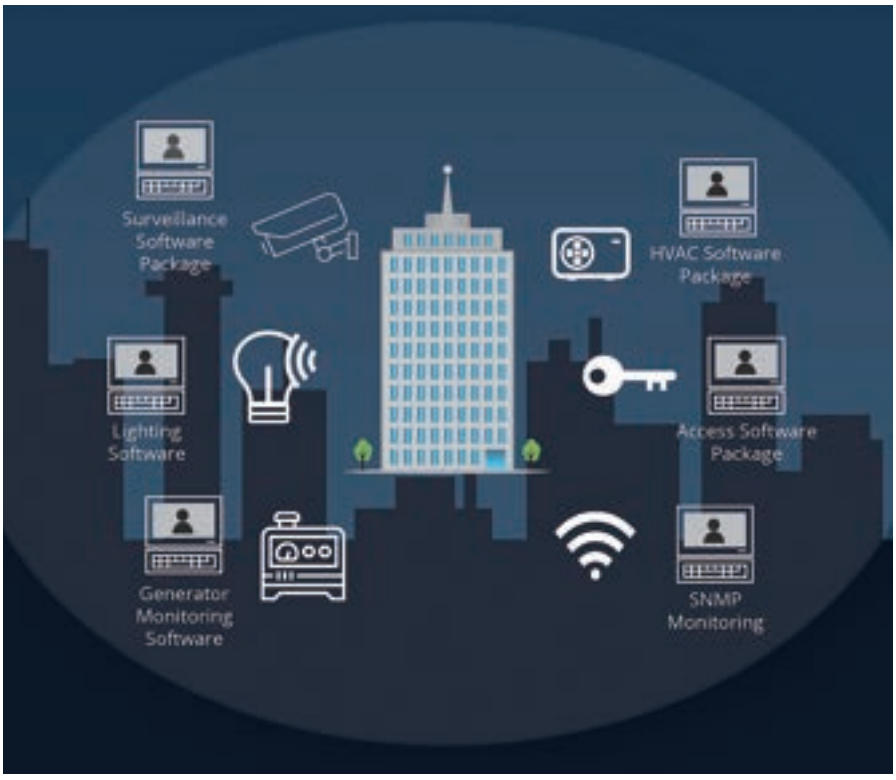
施設のすべての物流、運用、システムが、情報技術（IT）と運用技術（OT）を統合した戦略によって管理され、共通のIT標準規格を順守することが理想的である（本稿の図はすべて、ラディックスIoT社提供）。

セキュリティを第一とする標準規格とポリシー

2021年の時点で、100億台を超えるIoTデバイスが運用されており[3]、その数は2030年までに、254億台を超えると予想されている。技術進歩によってイーサネットは、商業ビルシステムの最前線に押し出された。ビル運用システムと照明システムを、それぞれ別のネットワークにサイロ化するのは、もはや実用的ではない。PoE（Power over Ethernet）照明の導入は増加しており、運用と保守を容易にするための統一されたシステムを求める声は高まっている。それは、コスト管理上の理由から、ビジネスネットワークを利用するビル技術に対する需要を生み出している（bit.ly/3ifAwMu）。

IoT接続デバイスのセキュリティ上の問題は、いわゆる「倫理的ハッキング」の実演対象となっている。2017年のIEEE Symposium on Security and Privacy（セキュリティとプライバシーに関するシンポジウム）において研究者らは、スマートランプを乗っ取って制御し、都市全体に拡大する可能性のある連鎖反応を実演した[4]。その研究では、物理的なIoTネットワーク（ランプ）と他の標的の間のギャップを埋めることにより、攻撃者は、家庭用コンピュータ、オフィス、あるいは都市全体に侵入できる可能性があることが示された。

規制当局のポリシーは、デバイスメーカーとシステムインテグレータの両者に求められるセキュリティ対策に影響を与える。その一例が、2021年1月に施行されたカリフォルニア州法であ



データと運用アクセスを保護するには、ビルネットワーク全体で共通して使用される複数のソフトウエア管理システムに対して、ネットワークアーキテクチュアに組み込まれた厳格なセキュリティ制御が必要である。

る。The State of California Bill SB-327は、インターネット接続型デバイスのメーカーに対し、変更されないままになる場合が多いデフォルトのパスワードを廃止することを求めている。その範囲は、医療、自動車、商業ビルシステムにまで拡大されている[5]。この法律では、IoTデバイスを「直接または間接的にインターネットに接続可能な、任意のデバイス、またはその他の物理的オブジェクトで、インターネットプロトコルアドレスまたはBluetoothアドレスが割り当てられているもの」と定義している[6]。照明システムの構造と、より広い世界とのその接続性を考えれば、このポリシーがそれらにも適用されるのは明白である。

これに続いて施行されたのが、IoT Cybersecurity Improvement Act（HR1668）[7]である。これは、すべての米国政府機関によって制御されるIoTデバイスの適切な使用と管理に関する一連の標準規格と指針の公開を、米国立標準技術研究所（National Institute of Standards and Technology：NIST）[8]に求めるものである。この法律はすべての連邦機関に対し、新しい標準規格を満たさないIoTデバイスの調達、取得、使用を禁止している。NISTはまだこの義務を履行していないが、この法律は、連邦政府、州政府、そしておそらくは民間企業の購買行動にも、影響を与えることになるだろう。

上述のNISTの標準規格により、ITシステムと相互に接続されるビルコンポーネントに、ハードウエアのセキュアブートや、セキュアな暗号プロセッサのための標準規格であるTPM（Trusted Platform Module）[9]のサポートなど、IT標準規格を適用することが求められるようになる可能性がある。IT業界では、チップの動作、通信方法、通信内容などを明らかにする権利が主張されている。このような概念が、照明システムの世界にも導入されつつある。サプライチェーンのトレーサビリティに対するその重要性と影響を理解し、IT業界で何度も使われて踏み固められた道をたどることが、非常に重要である。

参考文献

(1) Target Bullseye View, "How Target's Leading the Way in the Industry Through Cybersecurity Collaboration"（Jan. 20, 2020）.
(2) Entech, "Anatomy of a data breach – what we learned from Target"（May 1, 2019）.
(3) B. Jovanovic, "Internet of Things statistics for 2022 - Taking Things Apart," via DataProt（Mar. 8, 2022）.
(4) E. Ronen et al., "IoT Goes Nuclear: Creating a ZigBee Chain Reaction," Proc 2017 IEEE Symp Sec and Privacy（June 26, 2017）.
(5) A. Vigderman, "California Passes Nation's First Cybersecurity Law Addressing Internet of Things," via security. org（Dec. 2, 2020）.
(6) California State Bill SB-327, Information privacy: connected devices（2017–2018）.
(7) 116th U.S. Congress, U.S. Congress HR1668, IoT Cybersecurity Improvement Act of 2020（2019–2020）.
(8) U.S. Congress HR1668, IoT Cybersecurity Improvement Act of 2020（via trackbill.com）.
(9) S. Cheruvu et al., Demystifying Internet of Things Security, New York, apressOpen（2020）.

著者紹介

マイケル・スクルラ（MICHAEL C. SKURLA）は、スマートビルから通信に至るまでのさまざまなマルチサイトインフラの監視と管理を行う商用IoTプラットフォームを提供する、米ラディックスIoT社（Radix IoT）の最高製品責任者。URL: radixiot.com

LEDJ