In partnership with

Johnson Controls

Booz | Allen | Hamilton

サイバースマートビルディング

コネクティビティとオートメーションへの投資を守るために

2017年2月

エグゼクティブサマリー

もはや現実のものになったスマートビルのリスクとベネフィット

21世紀に入り、スマートビルはもはやオプションではなく、必然になりました。素早くタイムリーな対応を可能にするスマートビル環境は、ビルのデータを活用してオペレーションを最適化し、設備コストの低減を図ると同時に、安全性やサスティナビリティを高めます。また、リアルタイムでテナントや居住者のニーズに対応する一方で、エネルギー効率を最大限に高めます。そしてHVAC（冷暖房空調機器）制御、データネットワーク、電源管理といった内部システムと外部ネットワークを接続し、ビルの管理・監視オペレーションを一層効率化します。

ビルの所有者や運営事業者、管理者はこれまで、スマートビルの性能を機能性や効率性、コスト、信頼性、品質といった基準に基づいて評価し、設備投資を判断してきました。しかし、これからはサイバーセキュリティも評価項目に含める必要があります。ビルのデータやオペレーションシステムへのアクセスが増えるにつれ、スマートビル環境の安全性の課題も増加します。エネルギーのリモート分析や二酸化炭素排出量の監視などの新たな機能は、大きなメリットをもたらす一方で、テナントにサイバーリスクをもたらし、企業の利益を脅かす可能性もあります。

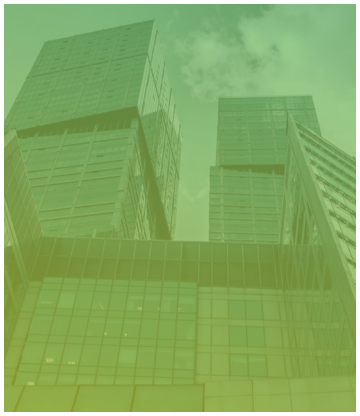
もはやビルは、単にスマートであるだけでなく、サイバースマートでなければならないのです。

ジョンソンコントロールズのグローバルプロダクト担当プレジデント、ビル・ジャクソンは、先頃発表した米国土安全保障省とのビルオートメーションシステムのためのサイバーセキュリティに関するパートナーシップに関し、「現在、そして将来のサイバー脅威に対する防御のためには、ビルオートメーションや制御システムの安全な設計や開発、導入が求められます」と述べています。

サイバー脅威の攻撃者たちは、ビルオートメーションやセキュリティシステムなどのクリティカルな環境を標的に攻撃を仕掛ける意思も能力もあることを実証しています。インターネットに接続されたすべての製品そのものに攻撃価値があるわけではありませんが、こうした機器が侵入口となって、より機密性の高いデータやシステムが侵害される可能性があります。例えば、ハッカーたちはHVAC業者の認証情報や決済システムの脆弱性を悪用して小売企業のネットワークに入り込み、最終的にクレジットカード情報を引き出しています。接続されたセンサーやデバイスの数が増えるにつれて、攻撃者たちはビルの自動制御システムを通じてより多くのデータやクリティカルな情報にアクセスできるようになり、脅威はかつてないほど高まります。しかし懸念すべきは情報漏えいだけではありません。自動制御システムがコントロールする対象はますます増加し、サイバー犯罪によって物理的な被害を受ける危険性も高まっているのです。

産業界や公共機関に与える影響

国家、州、地方など、あらゆるレベル企業や行政、地方自治体まで、あらゆるレベルの公共機関で、ビル制御システムへのサイバー脅威に対する対応策は、大幅な進展を遂げています。米国国防省が発行した統一施設基準（Unified Facilities Criteria: UFC）には、次のように記載されています。「制御システムの設計や導入段階でサイバーセキュリティを要件として含めることは、設計および建設コストの増大につながるものの、こうしたセキュリティコントロールを設計段階でなく設計後や施工後に導入する場合に比べれば、導入コストは抑えられる。従来の制御システムにはサイバーセキュリティは考慮されていなかったため、こうした要件の追加はコスト増にはなるが、セキュリティを高めることができる。設計後に導入する場合に比べると設計時に導入する方がコストは低くなる」



SFから現実へ：スマートビルに対して想定されるサイバー攻撃

コネクティビティ（他システムへの高い接続性）やオートメーションは無限の可能性を生み出しますが、適切なセキュリティ対策がなければ、スマートビルはサイバー攻撃のリスクにさらされてしまいます。例えば次のようなシナリオが考えられます。

1. 医薬品製造や食品加工など、厳密な温度調節が求められる工場での冷暖房機能を停止する
2. 企業ビル内のHVACシステムの冷房設定を操作し、事業に大幅な中断を引き起こして生産性を失わせる
3. データセンターの冷却機能や電力管理機能をシャットダウンし、IT機器を破壊して基幹業務アプリケーションをオフライン状態にする
4. インターネットに接続された物理セキュリティシステムへの不正アクセスを得て、動的攻撃を可能にする

「スマートビルは優れた投資先ですが、サイバースマートビルへの投資はさらに素晴らしい事業機会をもたらします。セキュリティなしでは、コネクティビティやオートメーションによる変革の真の恩恵は受けることができないでしょう。サイバーセキュリティを導入することでお客様や自社の利益を守ることができるのです」

-ブーズ・アレン・ハミルトン　バイスプレジデント　セダー・ラバーレ氏

SANSの「2016 State of Industrial Control System (ICS) Security Survey」（ICSセキュリティ動向調査）によると、回答者の67%は制御システムに対する深刻もしくは高度な脅威を認識しており、この割合は2015年の43%から上昇しています。極めて複雑なシステムが統合されることで、攻撃者にとってスマートビルは標的としての価値が高まっており、今やスマートビルはこうした戦いの最前線に立たされています。

今こそ行動を起こす時

コネクティビティやオートメーションはサイバー攻撃にとっての侵入ポイントを生み出し、安全や事業継続性、品質やプライバシーに影響を与える危険性があります。しかし、こうしたリスクがあるからと言ってイノベーションの歩みを止めるわけにはいきません、むしろサイバーセキュリティに適切に対処することで、投資は確実に保証できるでしょう。

そこで求められるのが、従来の発想からの転換です。サイバーセキュリティは企業にとってのお荷物でも単なるITの問題でもなく、間違っても脅しの手口などではありません。サイバーセキュリティはスマートビル事業を発展させていくための推進要素であり、うまくすれば自社の投資を保証し、コネクティビティ（他システムへの高い接続性）による変革からもたらされる恩恵をしっかりと受け取れるだけの能力を、確約してくれるものなのです。

ジョンソンコントロールズとブーズ・アレン・ハミルトンでは、何も手を打たずにいれば企業は競争力を失っていくことを実感してきました。スマートビル環境の中でサイバー戦略やテクノロジー分析を実現してきた経験を通じて、ビルのデータが持つ力をスマートかつ安全に活用していくことの重要性を認識しています。そこで本白書では、サイバースマートビルを実現していくために役立つ重要な見解をまとめています。

第一ステップはスマートビルシステムを評価し、導入する際に戦略を定義し、投資を確実に保護することのできる適切なパートナーとの連携を図ることです。ここには問題点の定義、サイバーセキュリティを会社の優先課題にすることやリスクマネジメント意識改革、ビルのライフサイクルを通じたサイバー機能の統合も含まれます。

ビルが「会話する」

スマートビルは、デジタルデバイスやネットワーク、アプリケーションがWebを介してつながることによって、現在の利用状況や天候予測をもとに、自動的に室温を変えたり、立ち入り禁止区域の入口で、監視カメラに見知らぬ人が映るとビル管理者に警告で知らせたり、エネルギー使用量を最適化し、制御トラブルを未然に防いだりすることができます。

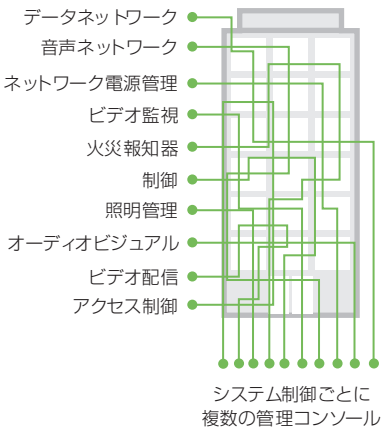
実世界とデジタル世界の窓口として、スマートビルテクノロジーは、コネクティビティやオートメーション、オープンアーキテクチャー、相互運用性を中核機能として、ビルや企業、テナントや居住者まで、有用なデータを共有し、トータルパフォーマンスを最適化します。これまで別々に存在していたシステム（下図参照）を一体化することによって、スマートビルはかつてないパワーを得て、有効性や効率性を高めます。IoT（Internet of Things）センサーやデバイスを導入することによって、新たなデータ源からオートメーションシステムに情報を提供し、効率化のための分析的洞察が可能になります。これによって、ビル管理や運用に関する多様なシステムをすべて統合し、一元化したアクセスが実現します。

システムはIP（インターネット・プロトコル）ネットワーク上で動作し、相互に一体となって高度なオートメーション機能やリモートコネクティビティ機能を提供します。さらにクラウド対応のシステムによって、スマートビルシステムにはアクセシビリティやスケーラビリティが加わり、コストを低減します。

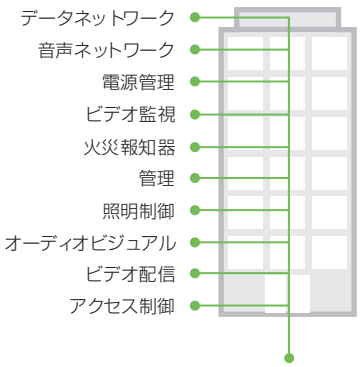
コネクティビティやオートメーションの性能を高めることで、膨大なビジネスの価値が提供されます。広範なイノベーションが可能になるだけでなく、限定的な統合であっても大きな価値を生み出すことができます。しかし、こうしたデジタルの継続的な進化はサイバーセキュリティの懸念を広範にもたらすことにもなり、スマートビルのオーナー、運用会社、管理者はこの点に真剣に取り組む必要があります。

スマートビルは、さまざまな運用システムを1つのネットワークのもとにまとめ、ビルオーナーや管理会社はビル運営を一元化し、効率化することができます。

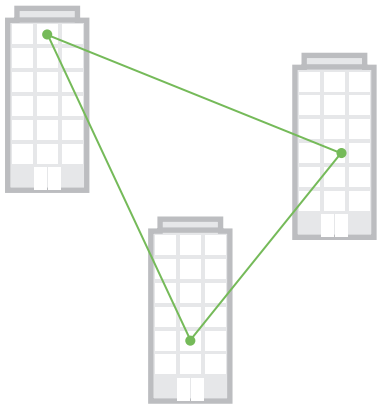
複数の独自技術によるシステム ▶ 単一ネットワーク ▶ 複数ネットワーク接続のビル



システム制御ごとに
複数の管理コンソール



ローカル&遠隔で多機能な
中央監視コンソール



コネクティビティにサイバーリスクはつきもの

米国土安全保障省の産業制御システムセキュリティ担当機関ICS-CERTは、2015年のレポートの中で、重要インフラ関係者の74%が、ネットワークに接続された制御システムは、さまざまなインフラを通じてセキュリティの脅威にさらされている可能性が高まっている[1]、と答えていることを報告しています。さらに、サイバーセキュリティ上、こうした急速な脆弱性の拡大によって、スマートビルの所有者や運用事業者、管理者には適切な防御措置を講じる必要性が生じ、実行されない場合にはビジネスリスクに直面することにも言及しています。

ホワイトハッカーや研究者が発見したリスクや脆弱性は、手順が整わないまま情報開示されています。ハッカーが悪用してDDoS（分散型サービス拒否）攻撃を仕掛けたり、犯罪者が脆弱なデータストリームを探し出して、その情報を売って利益を得るリスクがあります。また、国家支援組織が機密性の高い企業情報や個人情報を入手したり、テロリスト集団が重要なシステムを破壊したり、安全上の問題を生み出すリスクもあります。こうしたリスクは全て何マイルも離れた場所からもたらされるのです。

サイバー脅威を巡る最近の動向からは、さまざまなサイバー攻撃が、次第にビルオートメーションシステムなど制御システムのインフラを標的にするようになっていることを、明らかに示しています。制御システムを標的としてカスタマイズされたマルウェアが増加しているだけでなく、ビルに関連するサイバー脅威環境は、さまざまな攻撃者や攻撃のベクトル、多彩な手口を通じて拡大しています。

最近の報道を見れば、こうしたシナリオがもはや未来絵図ではなくなっていることがわかります。攻撃者がスマートビルへの攻撃意図と能力を兼ね備えていることを示すニュースは枚挙にいとまがありません。

研究者が大手インターネット検索プロバイダーのビル制御システムをハッキング[2]

セキュリティを専門とする研究者たちが、パッチが適用されていない大手インターネット検索プロバイダーの脆弱なビル制御システムをハッキングし、コントロールパネルの管理者アクセス権を入手することに成功しました。実行こそされなかったものの、オペレーティングシステム全体を制御することも可能な状態でした。

ハイテク装備の中国ホテルでハッカーが数百室の客室制御ネットワークに侵入[3]

宿泊者のためにネットワークアクセスを提供していた中国の5つ星ホテルでは、倫理的ハッカーが高度に自動化されたホテルの客室ネットワークに侵入し、建物内にある何百もの同タイプの客室を制御可能な状態にしていました。もし適切な安全措置が講じられていなければ、照明や冷暖房、デジタルキーといった制御システムが操作され、宿泊客の個人情報が盗み出されていたかも知れません。

IoTデバイスが史上最悪のサイバー攻撃の標的に[4]

DNSプロバイダーの米Dyn社を標的にした過去最大規模のDDoS攻撃は、欧米で多数のインターネットユーザーを巻き込んだ重大な障害を引き起こしました。攻撃はボットネットを通じて実行され、マルウェアに感染したIPカメラやデジタルレコーダー、プリンターなど、インターネットに接続された大量のデバイスで構成されていました。同様の機器類はスマートビルの至る所に設置されており、攻撃対象となるリスクがあることを示しています。

対応遅れによりスマートビルからの撤退を余儀なくされたホテル

オーストラリアにある4つ星クラスの高級ホテルは最近、続けざまにサイバー攻撃の被害にあいました。4度目の攻撃の後、ホテルは電子キーカードシステムがランサムウェアに感染し、宿泊客の到着時にスタッフがルームキーをプログラムできなくなっていることを発表しました。ビットコインでの「身代金」を何度も支払った後、ホテルの経営者はルームキーオートメーションを止め、100年前のホテル開業時に使っていたものと同様の物理キーに戻すことを決定しました。スマートイノベーションの導入にあたっては、適切なサイバー防御が取られているかどうかが、極めて重要なのです。[5]

リスクの新たな様相

「今、そして未来のサイバー脅威に対する防御のためには、ビルオートメーションや制御システムのセキュアな設計、開発、導入が要求される」

–ジョンソンコントロールズ グローバル製品担当バイスプレジデント ビル・ジャクソン

サイバーリスクに対応するために、ビルオーナー、オペレーター、管理者は新たな挑戦を受け入れなければなりません。スマートビルと企業ITの保護にはある種共通の原則がありますが、大きな違いもあります。ビルのセキュリティ保護はどのような点に特徴があり、新たな課題とはどのようなものでしょうか?

サイバーインシデントの影響ははるかに深刻

あなたが直面するのはかつてない挑戦です。単に情報漏えいやITサービスの中断だけでなく、被害は物理的損失にも及ぶようになっています。システムをIPネットワークに接続し、外部アクセスやクラウドとつながるようになると、サイバー脅威はビジネスオペレーションの安全性にも及び、ビジネスの停止を招く危険性もあります。

複数世代にまたがる旧来のビルインフラが可能性を制限

ビルには多大な設備投資が行われます。毎年のように取り替えるスマートフォンとは異なり、こうした資本資産は何十年も続くことを前提に組み立てられます。ほんの5年ほど前まで、設計の段階ではセキュリティのことなどほとんど考えられていませんでした。現在存在しているのは、新旧入り交じったインフラです。このような多様なスマートビル環境に追加導入できるようなセキュリティ対策には、限界があります。

「プラグアンドプレイ」ですべてを解決できるようなソリューションなど存在しない

スマートビル環境の安全を確保するためには、リスクベースの計画、セキュリティアーキテクチャー、テクノロジー、プロセス、スキルなど、さまざまなアプローチを融合する必要があります。ITセキュリティの世界では、ベンダーがこうしたアプローチをうまく体系化してパッケージにしてくれますが、ビルオートメーションシステムにはあてはまりません。なぜなら、ビル設備はそれぞれ用途や規模に応じて、個別にカスタマイズされたシステムや機器が設置される傾向が強く、その設備投資にかかる費用が膨大なため、実際にはいろいろな世代のシステムが混在しているケースが多くあるからです。このような状況に対し、適切なセキュリティソリューションを設計するためには、さまざまなパズルのピースをうまくはめ込めるだけの、優れた経験や技術力を持っている必要があります。

ひとりでは何もできない

サイバーセキュリティに関わるステークホルダーは、ITに精通した人ばかりではなく、ビジネスや企業の壁をはるかに超えた場所に存在します。多彩な経験や専門知識を統合し、多方面のステークホルダーを一体化させることこそ、複雑さを増す一方のリスク環境でセキュリティを確保する唯一の方法です。(次ページ参照)

スマートビルへの投資から得られる可能性を最大限に実現するためには、進化し続けるサイバーリスクから投資を保護しなければなりません。つまり、ビル環境の独自性を受け入れ、適切なステークホルダーを取り込んでいくことが、ビルにフォーカスしたサイバー脅威の急速な拡大を凌ぐ対応を取っていくためには有効だということです。

「IoTデバイスのメーカーにはサイバーセキュアな設計、開発、導入.が必要です。一方、IoTデバイスのユーザーは、そうしたデバイスにおけるセキュリティを最優先に考える必要があるのです」

–ジョンソンコントロールズ グローバル・プロダクト・セキュリティ担当ディレクター ジェイソン・ロッセロット (CSOオンライン2016年10月25日「IoTマシンの台頭」)

建物のサイバーセキュリティを支える主要ステークホルダー

社外ステークホルダー

ビルオーナー： 確実な投資のためには、サイバーセキュリティがリスクマネジメントの中核に据えられるべきであると主張する。

ビル管理者： サイバー技術をビル管理システムや日常業務へどのように取り込んでいくのかを決定する上で、中心的な役割を担う。

コンサルティングエンジニア： 技術的にビルの構造にどのようにセキュリティを組み入れていくべきかを指示する。

建築家： サイバー脅威軽減のため、設計段階で物理的なセキュリティや安全性における優先順位を決定する。

建設業者： 主要なビルテクノロジーについて、サイバーセキュリティに対応するパートナーやサプライヤーを特定し契約する。

インテグレーター： サイバー対応で多彩なビル技術を完全に統合できる、適切なベンダーやパートナーを組み合わせて連携体制を整備する。

メーカー： 設計から構築・販売・メンテナンスを通じ、スマートビルのためのデバイスやシステムのセキュアな製品ライフサイクルを実行する。

新規市場参入者： スマートビル向け機能を搭載した新製品やサービスを導入するが、現実にサイバーリスクをもたらす可能性があり慎重な検討を要する。

入居者／テナント： サイバースマートビルのさまざまな機能から日常的に恩恵を受けるが、自らの不注意がリスクにつながるため注意が必要。

来訪者： スマートビルでのセキュアな体験をすれば賛同者となりうるが、基準以下の場合には不要な注目を集める要因となる。

社内ステークホルダー

法務、安全&プライバシー: 規制当局のサイバーおよびプライバシー関連要件を判断する。

購買・調達: サイバーセキュリティ対応のサプライヤー、ベンダーの獲得プロセスを推進する。

マーケティングおよび広報: 顧客や社内のステークホルダーにサイバーセキュリティに関するメッセージを発信する。

リスクマネジメント: 戦略的リスクの優先順位決定や、サイバーセキュリティ投資ポートフォリオ全体を通じた影響についての指針を提供する。

財務: セキュリティ対策投資に関する優先順位付けや、指針の提供についてキーインフルエンサーとして機能する。

IT: 社内テクノロジーをスムーズに稼動させると同時に、一般的にはサイバーセキュリティの現状を全社的に把握する任務を負う。

監査: サイバーセキュリティが関連法規と社内ポリシーの両方を遵守して運用されているかどうかを精査する。

危機管理&事業継続性: セキュリティを含めたインシデント管理のための企業の基幹機能を担う。

具体的なアクション

リスクは現実のものとなりました。しかし、セキュリティについてパニックを起こす必要はありません。コスト削減、効率化、利便性などビルオートメーションの導入がもたらすビジネス価値は甚大です。導入を中断したりせず、投資を保護し、可能性を最大化する策を考えましょう。

スマートなアプローチはまず、自社を取り巻くリスク状況に基づいて一貫したアクションを取るための戦略やフレームワークを構築することから始まります。ジョンソンコントロールズでは、課題を組み立て、素早く勝利をつかみ、実際に状況を好転させていくための5段階の基本的なステップを推奨しています。

1. 具体的な課題を注視し、方向性を探る

サイバーセキュリティに関して、ビルオペレーターや管理者にとっては軍隊の意思決定方法が大いに参考になります。ゼロからのインフラ設計、既存ビルシステムのセキュリティ確保にはまず、自社のスマートビルにとってどの要素が最も重要な意味を持つのか優先順位を決定する必要があります。それはネットワークに接続した物理セキュリティシステムでしょうか？　オンプレミスのデータセンターの連続稼動時間を確実にすることでしょうか？　あらゆるセキュリティについて最高水準の保証を得る余裕はないにしろ、自社のビジネスにとって何が重要なのか、しっかりと優先順位をつけることが大切です。そこから、攻撃可能な対象領域をマッピングし、攻撃者の観点に立って攻撃の侵入経路を想定します。そして、サイバー脅威インテリジェンスを取り込むことで、別の攻撃者が実際に自社のインフラを標的にする見込みを把握します。こうした体系的なプロセスを総合して現実のサイバーリスクがどのようなものであるかを理解し、それぞれに合わせたマップを用意して対応措置を取ることが可能になります。

2. サイロ化した従来の体制を忘れること　ー　サイバーセキュリティに求められるのは部門横断型のチーム構成

サイバーリスクにしっかりと対応するためには、全社的な参画や積極的な関与が必要です。通常、ITやサイバーセキュリティ、ファシリティ部門にはリスク管理を主導するだけの専門的なノウハウとアクセス権があります。1つのユニットとして一丸となった協力体制を敷くには、社内外のさまざまなステークホルダーをまとめる必要もあります。社外では、サイバーセキュリティを重視し、大幅な投資を行うビジネスパートナーやベンダーと協力することになります。ここでは、適切なポリシーや製品、サービス、人材にコミットし、間違いなく信頼できるパートナーと連携する必要があります。特に、セキュリティは付け足しではなく、サードパーティの価値提案の中で主要テーマとして取り上げられている必要があります。

3. 企業文化の変革　ー　サイバースマートビルの重要性を明確に主張する

社内のリーダーシップコミュニティおよび社内外のステークホルダーがサイバースマートビルの重要性を強く認識しなければなりません。たとえトップクラスのチーム、専門的能力、最先端のテクノロジーソリューションを揃えても、サイバーセキュリティは組織全体の協力体制とサポートがなければ成功しません。スマートビルのオーナー、運用会社、管理者はサイバーセキュリティと自社のビジネスの将来が本質的に結びついていることを理解した上で企業文化を構築する必要があります。ROI（投資対効果）やセキュリティにおけるそれぞれの役割を含めて、この問題に正しく取り組むことの重要性をしっかり話し合いましょう。

また、幹部から新入社員まで、全社的に参画意識を持たせるための適切なメカニズムを検討しましょう。ビジネスチャンスとリスクについてのコンセンサスを形成する

ミリタリーグレードのセキュリティをスマートビルに適用

連邦政府や軍施設、金融機関、医薬品企業、病院、ハイテク企業や研究機関などでは、低遅延性やシステムの整合性は最重要課題であり、こうした環境では高度なセキュリティや強固なネットワークエンジンの導入は不可欠です。

ジョンソンコントロールズのビルオートメーションシステム（BAS）開発チームはこうしたニーズを実感し、官民双方の顧客と連携してBASアプリケーションのためにミリタリーグレードのクラス最高のセキュリティを開発しました。

その成果として先ごろ発表されたのが、*Metasys*®セキュアネットワークオートメーションエンジン（NAE-S）です。この新しいエンジンはサイバー脅威に対する防御性能を高めた製品を提供し、新たな機能を組み込んだネットワークを構築して重要なインフラをサイバー攻撃から保護するよう設計されています。このエンジンに搭載された暗号化モジュールは、不正ユーザーが機密情報にアクセスできないよう、ネットワーク上を行き来するデータを暗号化します。この機能が新たに加わったことで、ネットワーク上で動的な認証が可能になり、プロトコル通信の安全が確保されます。同時にビルオペレーションの制御に用いられるBAS内で攻撃を受ける可能性のあるルートの安全性も確保し、一般的なハッキングの手口に対して真のエンドツーエンドの防御を提供します。

ためには、説明会やリスク教育、演習などが有効です。ある意味、最も困難な作業であると同時に最も根本的な部分でもあります。

4. スマートビルの導入を妨げるのではなく、実現するための正しい能力を身につける。

ただサイバーセキュリティを導入するだけでは攻撃に対する完璧な措置が講じられたとは言えません。テクニカルソリューションはパズルの重要なピースではあるものの、人材やプロセスへの投資もバランス良く導入していかなければなりません。スマートビルのライフサイクル全体を通じてサイバーセキュリティを組み入れ、プロセスに負荷がかかり過ぎないよう気をつけなければなりません。そのためにはどのような中核機能が有効なのでしょうか?

5. そして、オペレーション開始

今日存在する脅威についてあらゆる面を確認したからと言って、将来への備えができたわけではありません。ここで止まってしまっては、コンプライアンス重視のアプローチによって、これまで述べてきたことの全てが阻害される可能性もあります。私たちが相手にしているのは進化し続ける「敵」であり、この敵に打ち勝つためにはセキュリティの専門的知識が必要です。監査担当チームはコンプライアンスや有効性について外部からの評価を行ってくれます。しかし、あなたの任務はリスクに焦点を当てて、会社の資産を守ることです。社内外のインテリジェンスを継続的に監視し、変化し続けるリスクプロファイルを把握します。常に先手を打てるよう、ビルオートメーション機器メーカーや分析サービスプロバイダーなど、製品セキュリティへの取り組みを実践している協力企業を見つけ、進化に対応できるようにすることで、この先何年も、安心して眠りにつけるようになるでしょう。

ライフサイクルのフェーズ	サイバー能力と概要	コア機能のチェックリスト
取得	**セキュリティ要件の検討** あらゆる仕様プロセスの一環にセキュリティソリューションを含めること。ベンダーや技術パートナーと協力して、ネットワーク接続するあらゆるスマートビルソリューションの中核部分としてセキュリティに優先的に取り組むこと。ベンダーに既存ネットワークとのどのような統合を求めるのかを定義し、ビルオートメーションシステムのための別のネットワークセグメントをできるだけ活用できるようにすることが望ましい。システム改修の機会に最新のセキュリティプロトコルを導入。ビルのライフサイクルを通じたセキュリティのオペレーション予算を明確に示せるよう準備しておくこと。	▫ 安全規程 ▫ コンプライアンス ▫ 計画・設計
	評価 セキュリティベンダーとそのソリューションを評価するための一貫した評価フレームワークを構築する。セキュアな設計やコーディングを実践するプログラムを実際に提示することができ、製品の脆弱性の発見、改善、パッチの適用を適切なタイミングで確実に行える成熟した脆弱性管理プログラムを持った企業を選択することが好ましい。コストのようにビジネス上の要請事項がセキュリティの問題に優先される可能性があることを認識しておくこと。このため、セキュリティの持つ意味や新旧システムの統合による得失評価のための枠組みを設計すること。ただし、アドオンのセキュリティ制御については、特定されたリスクを最少化するために柔軟に選択できるようにすること。	▫ サードパーティによるリスク管理 ▫ リスクアセスメント
導入	**セキュリティの組み込み** ビルオートメーションシステムを安全に導入し、ガイドラインに従って自社のIT部門と連携していく方法について、ベンダーの提案内容を把握したうえで、自社のコンプライアンスやリスクのニーズに基づいて制御機能を追加する方法を検討する。設計は重要であるものの、セキュアなネットワーク設計や遠隔アクセス機能の分野においては、リスクを監視し最少化するためにシステムをどのように構築して導入していくのかが重要になる。	▫ セキュリティアーキテクチャー ▫ IDおよびアクセス管理 ▫ 情報保護 ▫ プロダクトコードの安全性強化と検証
運用およびメンテナンス	**定期アップデート** ソフトウェアのサブスクリプションサービスや、インテグレーターとの予防保全契約を継続。制御システムメーカーは通常、導入以降のパッチの提供を行うため、自社システムのソフトウェアを常に最新の状態にしておくことがサイバースマートビルを維持していく上で重要。ベンダーによるセキュリティアップデートの提供機関やシステムのサポート期間をしっかりと把握し、システム寿命が終了する前に入れ替えが行えるよう、出口戦略を確実に用意しておくこと。	▫ 脆弱性管理 ▫ サービスレベルアグリーメント（SLA）
	検証、監視および対応 リスクを知ること。ネットワークに何が接続されているのか、常に状況を認識しておくこと。自社のエコシステム内のあらゆるドメインを通じてセキュリティの成熟度を識別する評価フレームワークを策定し、導入すること。入念かつ定期的に自社が構築した想定シナリオや技術的脆弱性についてストレステストを実行すること。継続的に監視を行い、指針をもとにインシデントの兆候を探ること。あらかじめ設定したトリガー基準に基づいて、問題の優先順位や重要度を決定すること。必要に応じて全社的な対応を指揮し、顧客の信頼を維持すると同時に、ベンダーと協力して適切な修正措置を取ること。	▫ アセット管理 ▫ セキュリティ監視 ▫ レッドチーム編成 ▫ 脅威インテリジェンス ▫ インシデント対応 ▫ 演習

今こそ行動を開始する絶好の好機

スマートビル業界には積極的にサイバーリスクに取り組めるチャンスがあり、同時にそうする義務もあります。世界的にスマートコミュニティやスマートシティの展開が進み、今後、課題は増加する一方です。スマートビルへの投資から本当の意味でのリターンを得られるかどうかは、世界中にまん延する複雑なサイバー課題への取り組み方にかかっています。適切に対処することで、ブランドを守れるだけでなく、自社のテナントや来訪者の安全、プライバシーを保護することができます。

今、ここから行動を開始することでサイバー脅威に対して先手を打つことができ、夜中の3時に不吉な電話連絡がかかるようなことを減らせます。ビルのオーナーや事業会社、管理会社にとっては他社との差別化にもつながります。今、私たちはセキュリティの空白地帯にいます。米国国立標準技術研究所（NIST）と国土安全保障省（DHS）では、スマートビルの初期段階におけるベストプラクティス[6]を策定していますが、サイバー規定については未だ、ほとんどの業界で先行する企業は見られません。先手を打てば、セキュリティスタンダードの策定だけでなく、ベンダーやサービスプロバイダーに対して影響力を行使できるチャンスがあります。こうした行動はビジネスにとってもセキュリティにとっても大きな利益になります。

サイバー問題に正面から取り組みましょう。しかし、だからといって必要以上に騒ぎ立てたり、過剰に投資をつぎ込むことはありません。ビルを改修するか、設計段階からスマートビルの導入を検討するのかに関わらず、通常のビジネス同様に今すぐ行動することはできます。まず、フレームワークを定義し、適切なチームを組織することで戦略的にアプローチします。次に、自社の設備の安全性やセキュリティが確保できるような技術管理やリスク管理体制を構築して、計画を実行に移します。この絶好のタイミングを逃す手はありません。

「サイバーセキュリティの脅威によって、商業用ビル制御市場はその様相が変化し、興味深い課題が生まれつつある。ビルのオーナーや管理会社にそうした変化を認識させ、理解させるという作業は依然として難題である。彼らが自社のビルシステムの脆弱性を認識してそのことに対して懸念していたとしても、脅威に対してどのような手を打てばよいのか気が付いてない場合が多い」

2016年9月13日 Forbes誌

1 https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_FY%202015_Annual_Vulnerability_Coordination_Report_S508C.pdf
2 https://www.wired.com/2013/05/googles-control-system-hacked/
3 http://www.scmp.com/news/china/article/1561458/hacker-takes-control-hundreds-rooms-hi-tech-shenzhen-hotel
4 http://www.memoori.com/internet-things-devices-center-biggest-cyber-attack-history/
5 http://www.wired.co.uk/article/austria-hotel-ransomware-true-doors-lock-hackers (2/2/17)
6 http://www.federaltimes.com/articles/nist-unveils-internet-of-things-cybersecurity-guidance ; https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf
7 http://www.forbes.com/sites/pikeresearch/2016/09/13/cybersecurity-and-intelligent-buildings/2/

ブーズ・アレン・ハミルトンについて

ブーズ・アレン・ハミルトンは、100年以上にわたり経営戦略とIT技術の最前線で活躍しています。現在、Fortune　500社番付企業、政府、世界中のNPOに、経営と技術のコンサルティングとエンジニアリングサービスを提供しています。ブーズ・アレン・ハミルトンは、コンサルティング、分析、ミッション運用、技術、システム納入、サイバーセキュリティ、エンジニアリング、イノベーションの専門知識を組み合わせ、最も困難な課題を解決するために、公共および民間部門の顧客と提携しています。
バージニア州マクリーンに本社を置く同社は、世界で22,600名以上の従業員を雇用しており、2016年3月31日までの12ヵ月間の収益は54億1,000万ドルでした。詳細については、BoozAllen.comをご覧ください（NYSE：BAH）。

ジョンソンコントロールズについて

ジョンソンコントロールズは、世界150ヵ国以上のお客様に多様なテクノロジーを提供する業界トップクラスのグローバル多角産業企業です。約13万人の従業員がシームレスに連携し、スマートシティやスマートコミュニティを実現するインテリジェントビル、エネルギー効率化ソリューション、統合インフラ、次世代輸送システムの開発に取り組んでいます。ジョンソンコントロールズのサスティナビリティへの取り組みは、創業のきっかけとなった世界初の電気式室内サーモスタットが発明された1885年にまで遡ります。当社はお客様の成功を支援し、ビル制御やエネルギー貯蔵といった当社の戦略的成長基盤に注力することで、すべてのステークホルダーに向けて価値を創出します。詳細は、www.johnsoncontrols.co.jpをご覧いただくか、またはTwitterで@johnsoncontrolsをフォローしてください。

連絡先

セダー・ラバーレ
バイスプレジデント
labarre_sedar@bah.com

マシュー・ドーン
シニアアソシエイト
doan_matthew@bah.com

連絡先

ジェイソン・ロッセロット
ディレクター
jason.r.rosselot@jci.com

アレックス・ランナー
ディレクター
alex.e.runner@jci.com