ビルディングオートメーションシステム（BAS）をサイバー攻撃から守る

サイバーセキュリティの課題：

ビルディングオートメーションシステムのデータにアクセスして業務に役立てつつ保護する方法

目次

はじめに 3
OSIsoftについて 4
「自分は大丈夫」 5
• Googleオーストラリア本社 5
• 設備機器管理を営む某企業 6
• 米国国防総省 6
• カジノ所有者 6
サイバーリスクが増加する理由 7
1. データアクセスへの期待が高まっていること 7
2. データ量の増加に伴い、データへのアクセスニーズが高まっていること 7
3. ビル管理システムにはサイバーセキュリティ対策がないことが多い 8
4. ビルシステムが攻撃対象になっている 8
5. ハッカーたちはさらに高度化している 9
リスクを回避する 10
• 産業用制御システムの専門家から学ぶ 10
• 状況認識レベルをあげる 11
• イベントに関するデータを分析する 11
• イベントフレームと通知の管理 11
• セキュリティレイヤーを使う 12
• より多くのことを疑問視する 12
結論 13

はじめに

現在のビルディングオートメーションシステム(以下BAS)は、重要なデータを収集、利用、提供しつつもデータを保護しなければならないというサイバーセキュリティの課題に直面しています。この問題には、二面性があります。商業・企業ビルの設備から得られるデータは、かつてないほど豊富になり、こうしたデータが持つ価値への認識は高まっているのは良い点です。一方で、BASデータとその機能は、不正使用や盗難のリスクに晒されており、かつてないほどに脆弱化しているのが厄介な点です。しかし、データを活用しつつ、保護する方法はいくつかあります。

本書では、設備管理責任者が知っておくべきサイバーセキュリティリスクについて解説します。近年、こうしたリスクがどのように増加してきたのか、そしてデータがハッキングされた場合、設備の利用者や所有者にどのような影響の可能性があるのかについて説明します。第二部では、サイバーセキュリティの専門家が、リスクを回避する方法についての知見を提案します。また、BASとそのデータを、ハッカーや妨害者、その他の悪意のある行為者たちから確実に守るために、従業員やパートナーに要求すべきことについても明確にします。

OSIsoftについて

OSIsoftは石油精製や電力発電、鉱業、プラント工場、組み立て製造業やプロセス製造業界向けのデータインフラストラクチャであるPI Systemを提供し、ミッションクリティカルな業務をサポートし、業務データを活用した意思決定を支援することから始まりました。PI Systemは、オペレーションに関わるデータをリアルタイムに収集し、処理内容に応じてコンテキスト化して保管し、視覚化することで、データを必要とする「人」と、「必要なデータ」と「知見を生み出すツール」をつなげます。

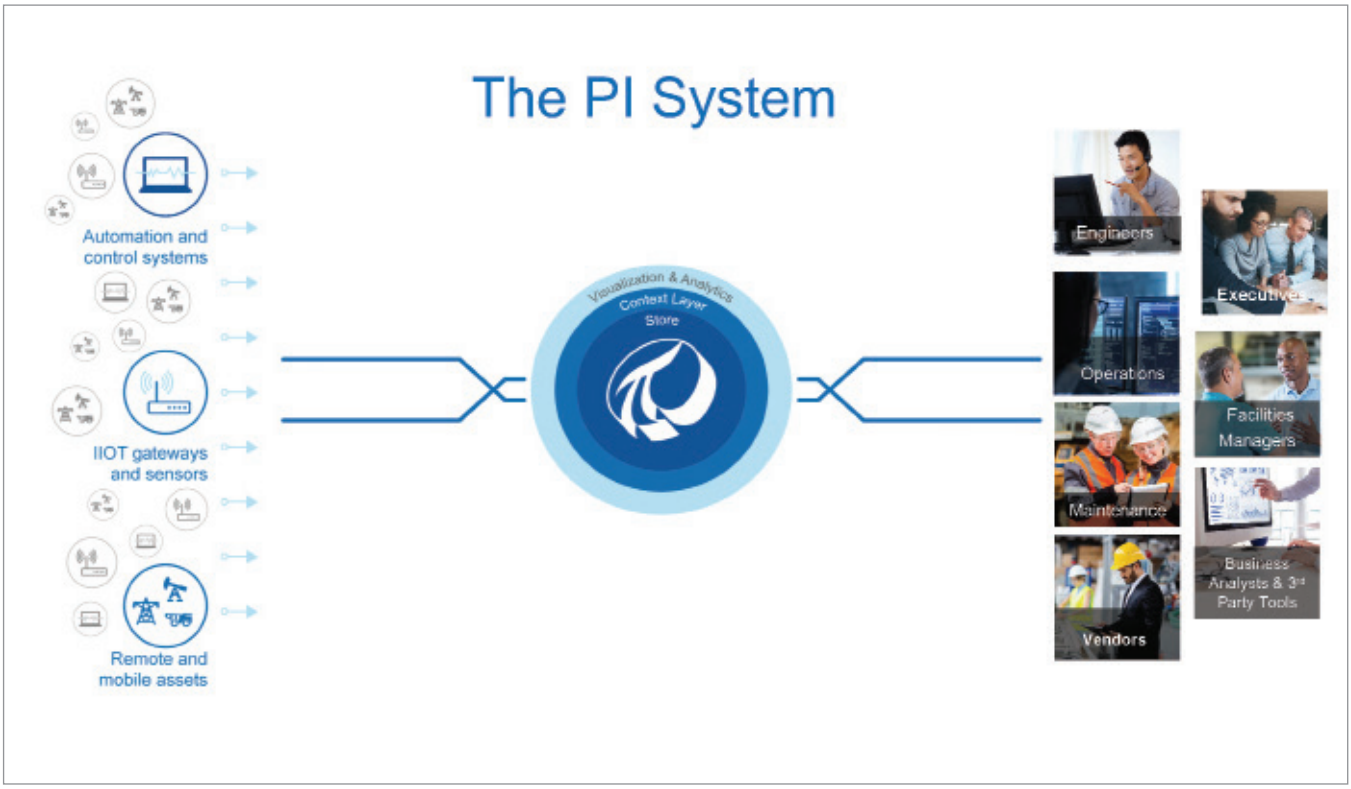
OSIsoftは製造業におけるサイバーセキュリティ分野で長年の経験があり、設備データの取り扱いに関する最新の知識とベストプラクティスを有しています。

PI Systemは、流入したばかりのデータストリームを体系化して、意味のある付加情報を加えることで、高度な分析ツールで簡単に使えるデータに変換します。

PI Systemは、設備管理としてBASやエネルギー計測、ビルのIoT機器などの数多くの異なる設備からデータを自動的に取り込んで保管します。

データを自動的に収集することで、データの信頼性が高まり、属人的なデータ収集よりもスピーディに作業が完了し、リアルタイムな分析や意思決定が可能になります。

OSIsoft PI System — 実績のあるデータインフラストラクチャのアプローチ



PI Systemは、ポートフォリオ全体からデータを収集し、そのデータを標準化、統合することで、異なるアプリケーションやプラットフォーム間でセキュアに共有できるようになります。

「自分は大丈夫」

例えば、職場で銃撃事件が起こる、あるいは天災に見舞われるような最悪の事態は、自分たちの身には降りかからないと思うのが人間の性です。サイバーセキュリティの侵害も、同じことです。まさか自分たちが被害にあうことなど想像もしたくないでしょう。しかし、設備防災訓練や襲撃からの避難訓練の重要性と同じように、今ではBASサイバーセキュリティとデータ保護は必要不可欠であるということ、そしてその責任はIT部門でも会計部門でもないことに管理者たちは気づき始めています。
たとえ、「うちのビルはスマートビルディング」ではないと思っていたとしても、BASは、次から次へとさまざまな設備に接続し、豊富なデータを持っています。あなたの所有するビルには、インテリジェントな空調・換気システム、スマートTV付きの会議室、インターネット接続された照明、その他のIoT機器があるかもしれません。こうしたすべてのシステム、機器、接続が、ハッカーの攻撃対象であり、攻撃のためのツールになり得るのです。

今日では、設備・機器に関わるサイバーセキュリティの脅威が当たり前のように報道されています。過去数年間に起きた次の4つの事件は、設備・機器に対する脅威の凄まじさと規模を物語っています。

GOOGLEオーストラリア本社

2013年、2人のセキュリティ調査員が調べたところによると、Googleがオーストラリア、シドニーに所有するWharf 7オフィスのビル管理システム（BMS）にハッキングできることが判明しました。
同社のBMSのプラットフォームを作ったメーカーは、既知の脆弱性に対処するためのパッチをリリースしていましたが、Googleのコントロールシステムには、まだ実装されていませんでした。
この事態を発見した調査員たちは、システムの管理者パスワードが誰でも想像がつくような一般的なものであったことから、ビルの空調・換気システムを制御するコントロールパネルにアクセスできたということです。このパスワードを使えば、フロアーや屋根の青写真だけでなく、水道配管図といったデータにまでアクセス可能でした。

設備機器管理を営む某企業

2016年、IBMの調査員は、米国全土で20以上のビルを運営する某設備管理会社に対して侵入テストを実施しました。その結果、ひとつのビルのセンサーや温度自動調整器を制御するビルオートメーションシステムのファームウェアにいくつかの欠陥があることが判明しました。調査員たちは、BASへのアクセス権を得て、同社のセントラルサーバーへのアクセスを試みました。

調査員たちがその時に居た場所からインターネット経由で同社のコーポレイトサーバーへアクセスすることは、保護レイヤーによって阻止されましたが、その後、同社の駐車場へ移動して、そこから無線ゲートウェイで接続してみたところ、データセンターが入っているビルを含むすべてのビルの環境制御システムにアクセスできたのです。つまり、冷却システムをオフにして、サーバーをシャットダウンすることも可能だったということです。

米国国防総省

2018年、国防総省Department of Diffence（以下、DoD）は、DoDの設備機器コントロールシステムに関する脆弱性と検出、記録、是正措置の実装にかかるコストは、今後4年間でおよそ2億5,000万ドルを超えると議会に報告しました。本報告書によると、現在の覚書や指示書で検討されているすべての要件を完遂するためには、軍事サービスの1案件につき1,100万～9,600万ドルのコストがかかり、さらに「最重要システムとして現在評価と是正措置が行われているシステム以外でさらにシステムの脆弱性が発見された場合は、コストはさらに上昇する可能性が高い」と述べられています。

カジノ所有者

最近行われたウォールストリート誌主催のCEOカンファレンスにおいて、出席者たちは、次のことを学びました。ビルの温度自動調整器や冷却装置、CCTVカメラ、換気・空調システムなどのIoT機器が、いかに脆弱で、ハッカーたちによるデータの盗難やオペレーションの中断リスクがあるかということです。
ひとつの例として、サイバーセキュリティ企業のCEOであるDarktrace 氏は、次のように述べました。「ハッカーたちは、カジノのロビーにあった水槽用の温度自動調整器（インターネット接続）から侵入して、カジノの最優良顧客に関するデータを盗んだのです。」

ハッカーたちは、スマート温度自動調整器を使って、カジノのITネットワークにアクセスしました。温度自動調整器をブリッジにして、Wi-Fiネットワークに接続し、大金を儲けた顧客に関するデータをクラウドから盗み出したのです。

サイバーリスクが増加する理由

設備機器の運用に関連するサイバーセキュリティリスクの増加には、5つの傾向が見られます。

1. データアクセスへの期待が高まっていること

カジノの水槽に置かれていたスマート温度自動調整器の例は、ほとんどすべての物理的対象が「スマート」になり、ネットワークに接続されていることを示唆しています。家電がますます賢くなることは、つまりこれまでの予想を超える脅威とデバイスが、日々、従業員とともに入り込んでくるということです。

今日ではNestやAmazon Echo、SonyのHUISのようなホームオートメーションシステムを使い慣れている居住者や上層幹部が増えています。 そして彼らは、職場も同様にスマートなビルであることを期待します。ボタンひとつで、会議室の照明を調節し、空調・換気システムのエネルギー効率を把握したいと思っています。

消費者のテクノロジーに対する期待の高まりを受けて、同様のテクノロジーが、商業・企業ビルへと適用されます。

データにアクセスしたいという期待は、商業・企業ビルをよりスマートにしようという気運に拍車をかけます。そしてアクセスが可能になることで、コネクティッド・デバイスが、攻撃対象となる範囲を広げてしまうのです。

2. データ量の増加に伴い、データへのアクセスニーズが高まっていること

ポンプ、バルブ、化粧室の自動ペーパータオルなど、ビル用の商品はかつてないほどに範囲が広がり、さらにデータを収集して共有化する能力を持ち始めています。BACnetやModbusなどの通信プロトコルが、かつては互換性のなかったビル管理システムと接続するようになり、またビルのIoTセンサーはかつてないほど大量のデータを生成しています。再生可能エネルギーシステムやエネルギー貯蓄装置、マイクログリッドのような新しいテクノロジーと同様に、アクセス制御や給水／排水処理システム、電子制御の保全管理システムもさらに有用なデータを生成しています。

データに価値があれば、それにアクセスして活用したいという需要が生まれます。そうすると、ハッカーの侵入口が開いたということになります。ビル管理者には、非常に頭の痛い問題です。

データの価値を引き出すためには、データへのアクセスが不可欠です。現在利用できる分析範囲は、BASの能力をはるかに超えています。BASのデータをマイニングすれば、発見できなかったような問題を知ることができます。ビルの資産データは、外部から取得できるリアルタイムなデータと組み合わせたり、あるいはアルゴリズムを使って新たな主要業績評価指標（KPI）を計算することも可能なのです。

同時に上層幹部が組織全体のデータへアクセスできることに慣れてきたことで、データへの需要も高まっています。経営幹部たちは、消費エネルギーを抑えてコストを削減し、規制報告書の要件を満たし、あるいは買収・合併に伴う財務要件に対応するために、ビルのデータを使いたいと要求しています。

ビル制御システムに効果的なサイバーセキュリティ対策がなければ、脆弱で攻撃される可能性があることになり、データ共有の問題が発生します。社内ネットワークあるいはインターネット経由でデータを共有するすべてのチャネルに、サイバーリスクの可能性があります。設備機器データにアクセスしたいという需要が高まれば、脆弱性も同様に高くなるのです。

3. ビル管理システムにはサイバーセキュリティ対策がないことが多い

残念ながら、設備機器のサイバーセキュリティ対策は、増加し続けるデータ量に追いついていないのが現状です。ビルディングファシリティコントロールシステム社の、ディレクターFred Gordy氏によると、BASは従来、利便性を念頭に設置されてきました。例えば、Webブラウザーからシステムにリモートアクセスすれば、ビル管理者やベンダーは時間もコストも節約できます。その当時、BASのセキュリティは最重要事項ではなかったために、IT部門はこうしたシステムとは無関係で、あるいは関わりたくないと考えており、保護された状態ではありませんでした。もしネットワークが分離されておらず、パスワードも変更されず、その他の保護対策がなされてなければ、インターネットはリスクを招くチャネルとなります。

2016年にBuilding Operating Management誌が設備機器の経営幹部を対象に行った調査によると、回答者のわずか28%が、すべてのBASのパスワードを定期的に変更していることが明らかになりました。さらに17%が、サイバーセキュリティに関して知識がある、あるいは非常に造詣が深いと答えたのです。

今日の設備機器管理部門は、システムが不正アクセスされているかもしれないという状況認識がないことが多いです。本調査では、回答者の35%が、BASがハッキングの対象になった可能性すら検知した確証がないと答えています。

4. ビルシステムが攻撃対象になっている

従来、オペレーションに関わるデータは、会計システムや自動投票機から得られるデータのようには重要視されてきませんでした。10年前のビルシステムは、今ほど脆弱ではありませんでした。なぜなら、システムが生成するデータはめったに共有化されることもアクセスされることもなく、誰も躍起になって探し出そうとしていなかったからです。しかし、今日では、エネルギー管理システムのデータをもとにコストを削減し、設備機器の問題について通知を受け取り、タイムリーかつ正確なシステム情報をもとに保全価値を高めることが可能になり、データは業務の効率化においてますます不可欠な存在となっています。

残念なことに、オペレーショナルデータをすべて盗み出すこと、あるいは保護されていないオペレーショナルシステムに侵入してコンピュータの処理能力をハイジャックすることの価値に、犯罪的なハッカーたちも気づいているのです。

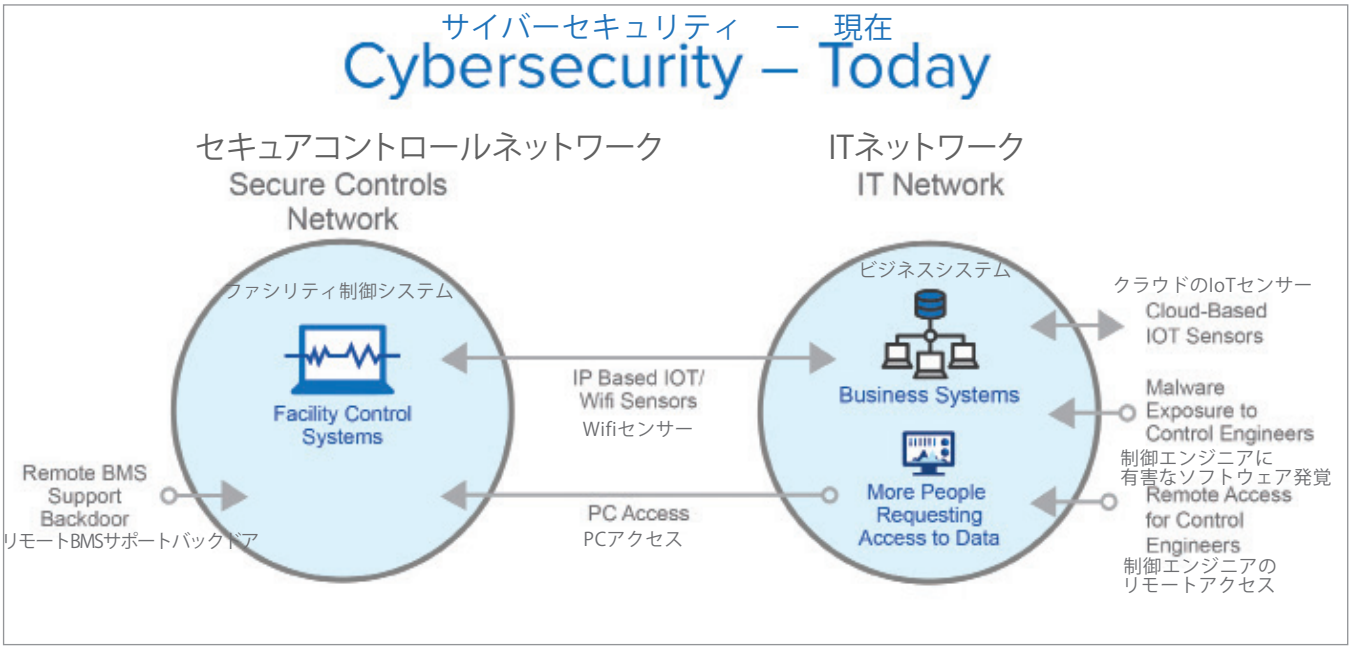
ハッカーたちが通常業務を意図的に妨害し、保全部門のパソコンやBASにアクセスすれば、ミッションクリティカルなシステムを不能化し、人々が仕事を遂行できないようにすることが可能です。例えば、高層オフィスビルの中で、ビジネスを止めるためにハッカーがやるべきことは、ただひとつ、防火設備やエレベーターシステムを不能にして、社員たちがビルに居られなくなるようにすればよいのです。

Ismail Sadiron / Shutterstock.com

5. ハッカーたちはさらに高度化している

サイバーセキュリティの知識は、急速に進化しています。ハッカーたちが多くのBASに簡単にアクセスできるのは恐ろしいことです。インターネットに接続されている機器を検索する初のサーチエンジンであるShodan.io を使えば、5分間検索するだけで、複数のビル管理システムへのログイン画面が表示されます。

これ以外にも、ハッカーたちがビル制御システムを見つけて不正アクセスするために使えるMaltegoやZoomEyeなどのツールや技術が存在します。組織が、リスクと脆弱性を知り、それらを無力化する一方で、ハッカーたちはシステムを悪用するさらに新しい方法を試しています。サイバーセキュリティのトレーニングおよび認定プログラムを提供する最大規模の組織であるSANS Instituteによると、2018年に発見された新しい脆弱性のある分野のひとつが、データリポジトリ／クラウド上のデータであることがわかりました。コラボレーションのために、莫大なコードリポジトリをオンライン上で公開するソフトウェアアプリケーション、クラウドに保管されているミッションクリティカルなテラバイト規模のデータが、攻撃者の共通のターゲットになっています。ハッカーたちは、こうしたインフラストラクチャのパスワード、暗号鍵、アクセストークン、機密データを探しています。



多くのビルオートメーションシステムは、エンタープライズITネットワーク上にあり、複数のアクセスポイントを解放していることから、制御システムがサイバー攻撃に対して脆弱なまま放置されています。

リスクを回避する

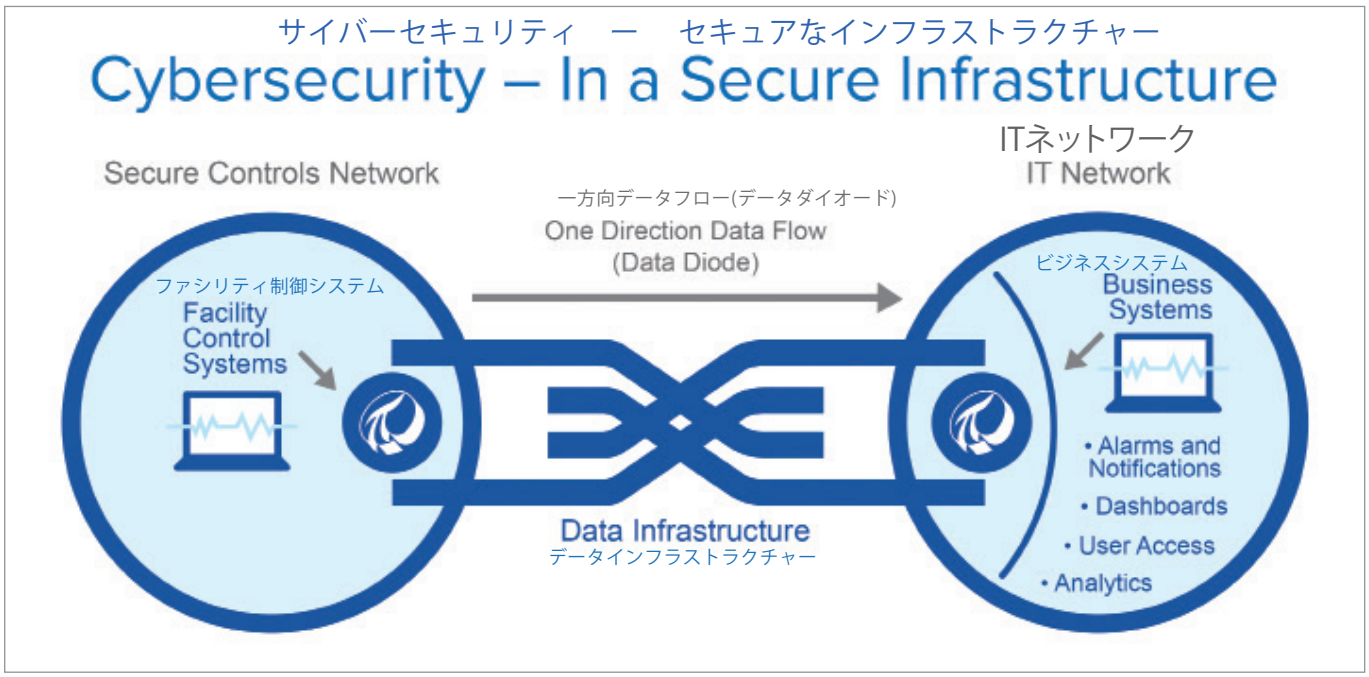
このようにビルディングシステムとそのデータに数多くのリスク分野がある中で、どうすればリスクを回避することができるでしょうか？次に示すのは、システムの機密性を確保するための4つのアクションアイテムと、設備機器の管理チームおよびパートナー企業に問いただすべき質問事項をリスト化したものです。

産業用制御システムの専門家から学ぶ

今日の商業・企業ビルは、サイバーセキュリティの点で産業用設備に後れを取っていますが、ビル管理システムと産業用SCADAシステムとの間には似ている点が多くあります。つまり、産業用システムのサイバーセキュリティの専門家から学ぶべき点は多いのです。

重要でありながらも十分に保護されていなかった産業用システムが世界中でサイバー攻撃を受けて注目を集めたことは、結果的には新しい発見、ベストプラクティスの改良、学ぶべき教訓となりました。それらを、今日の商業・企業ビルの設備機器に適用し、データアクセスを可能にしながらも、制御機能へのアクセスを保護することができます。

OSIsoftは、産業用設備機器の分野をスタートに、現在ではNIST（米国国立標準技術研究所）やNCCoE（官民連携R&Dセンター）や他の組織と連携して、製造業の制御システムのセキュリティを改善するプロジェクトに参加しています。さらに最近では、NISTやNCCoEと提携し、サイバーセキュリティ技術やさまざまな業界におけるビジネスケースの開発と適用を推進しています。同組織は、どこにでも適用できる標準化されたサイバーセキュリティソリューションを広く展開しようと取り組んでいます。OSIsoftのPI Systemは、すでにボストンのMITやNASAのラングレー研究所、ハーバード大学メディカルスクール、米国国立衛生研究所、メリーランド大学カレッジパーク校で採用され、セキュアな発電と消費エネルギーデータへのアクセスを実現しています。



PI Systemのデータインフラストラクチャー。データ収集と配信ネットワークから制御システムネットワークを分離しています。

状況認識レベルをあげる

OSIsoftは、かつてNCCoEと共同で、NISTのサイバーセキュリティ・プラクティスガイド、特別号（Cybersecurity Practice Guide-Special Publication 1800-7）を作成しました。これは、公益事業を営む企業の状況認識レベルを評価、改善するためのガイドブックです。設備管理システムの管理者の状況認識レベルが向上すれば、例えばコジェネレーションのようなエネルギー供給システムや水処理施設、あるいはBASのようなビルシステムであっても、リアルタイムにデータをモニタリングして、問題を検知して修繕し、問題を未然に回避し、オペレーションを最適化することができます。また、状況認識能力は、ネットワークの保護、サイバー犯罪に関わるリスクの回避にも不可欠です。何が起こっているのかを把握できなければ、侵害されたことに気づかないからです。

イベントに関するデータを分析する

データ分析を行い、「イベント」を明確に特定し、通知する機能を使ってリアルタイムなデータをコンテキスト化することで、状況認識能力をさらにレベルアップすることができます。イベントとは、始まりと終わりがあるものは何でも対象になります。空調・換気システムのスタートアップとシャットダウン、部屋を使用している時間、あるいは大学などのキャンパス全体の停電などもイベントになります。このように注意すべきイベントが検知された時に、関係者にアラートを発して通知するのです。

PI System を使ってデータ分析するのは簡単です。データポイントや付加価値の計算、さらに実施すべきアクションの提案など、すでに必要な機能が組み込まれていますので、問題を診断し、オペレーションを最適化することで、コストを削減することができます。PI System のイベントフレームは、イベントの開始時間と終了時間、継続時間、同時に発生している他のイベントやデータをキャプチャします。どういったケースで通知するかについては、ユーザー定義でルールを設定し、特定のイベントが発生した時に、メールを送るのか、あるいはWebサービスにリクエストを送るのかを決めることができます。また、通知を受け取った後のアクション、例えば、送信時間や承認、コメント入力、上層部への報告などの履歴は、今後の詳細な検査に使う時に取り出せるように保管されます。このように、一連のイベントをキャプチャし、分析することが可能です。

セキュリティレイヤーを使う

サイバーセキュリティの専門家たちは、重層化することで最善のセキュリティ効果が得られることに同意しています。原子力発電工場の制御システムを、普通のITネットワーク上で稼働させるべきでないように、BASもITネットワーク上で稼働させるべきではありません。

PI Systemのユーザーが使っているのは、ネットワーク制御システムをデータ収集や配信ネットワークから隔離しているひとつのレイヤーです。つまり、設備機器データにアクセスするためには、ひとつのパスワードで保護された扉がひとつしかないということです。PI Systemは、BASを脅威に晒すことなく、データにアクセスすることを可能にします。

Fred Gordy氏によると、他のセキュリティレイヤーは、すべての社内ユーザーやベンダーがそれぞれに独自のユーザー名を持ち、その認証情報を誰ともシェアできないことを保証するものです。また、アクセス権限のある人やシステムに接続されているデバイスを目録化し、パスワードが定期的に変更されていることを確かめることも重要です。

さらにGordy氏によると、設備管理会社の経営陣たちは、彼らが管理するBASがパブリックIPを所有しているかどうか調査し、もしそうであれば、そこから外してファイアーウォール内にシステムを置くべきだと述べています。リモートアクセスが必要であれば、最も低コストでリモートアクセスが可能なソリューションを選択することです。この2つのステップを実行するだけでも、貴社の制御システムはShodanのような検索エンジンにヒットしなくなります。

より多くのことを疑問視する

次に挙げるのは、疑問視しておくべき質問事項です：

- データや制御がどのようにビジネス目標の達成能力を弱体化させているか、考えたことがありますか？
- セキュリティの進化にどのように追随していますか？
- BAS関連のどのようなセキュリティパラメーターがありますか？
- システム管理をサードパーティベンダーに任せていますか？また彼らはリモート接続していますか？
- オペレーショナルデータを外部のデータソースと組み合わせて使っていますか？もしそうであれば、それにはどのようなリスクが伴いますか？
- エネルギー消費データをどのように集めていますか？
- サイバーセキュリティ上のイベントが発生した場合に検知することはできますか？過去6か月間で検知したことはありますか？
- サイバーセキュリティ上のイベントが検知された場合、すばやく行動できますか？次のステップを決めるのは誰ですか？
- 保護すべきデータは何だと思われますか？データアセットの目録化を実施したことはありますか？
- 貴社のシステムやデータを保護するために、ベンダーやパートナーはどのようなサポートを提供していますか？

最も重要な次のステップは、チームメンバーに疑問を投げかけ、さらに彼らがそれをパートナーに投げかけるように徹底することです。

結論

データを利用する量、頻度、方法が増え続けるにつれて、ビルの管理方法も変革しています。データを活用すれば、ビルをよりコスト効果的に運営し、居住者の快適さを高め、システムが停止しないようにすばやく対策を取ることができます。さらに、組織の成長にとって必要な人材を魅了して採用し、維持することもできます。また、ビル設備の経営幹部たちは、インターネット接続された次世代のスマートデバイスに伴うリスクに対処できなければなりません。

PI Systemは、サイバーセキュリティ・スマートなビルの基盤となります。データインフラストラクチャーとして、分散したソースからのデータを標準化、統合、一元管理するためのセキュアな手段を提供します。

ABOUT OSIsoft

OSIsoftはデータを通して人々が世界を変革することを支援します。す。OSIsoftのPI System は、センサーや製造機器、その他機器からキャプチャしたデータを、情報豊富な知見へとリアルタイムに変えることで、生産性の向上、重要な意思決定、新製品の開発を支援します。1,000社を超える先進的な公共事業、最大規模の石油・天然ガス企業の90%、フォーチュン500に選ばれる工業企業の65%が PI Systemに信頼を寄せており、ビジネスに最大限に活かしています。PI Systemは、全世界で20億をこえるデータストリームを管理しています。さらに詳しくは、osisoft.comをご覧ください。

PI Systemのお客様がどのように設備機器を改善しているのかについては、explore.osisoft.com/l/facilitiesをご覧ください。
また、OSIsoftおよびPI Systemの詳細については、explore.osisoft.com/l/osisoft-and-pi-systemをご覧ください。

メールでのお問い合わせはこちら：smartbuildings@osisoft.com
日本語でのお問い合わせはこちら：marketingjapan@osisoft.com

Corporate Headquarters:
1600 Alvarado Street
San Leandro, CA 94577, USA
Contact us at +1 510.297.5800

OSIsoft Japan株式会社:
〒160-0022　東京都新宿区新宿4-1-6
JR新宿ミライナタワー8F
代表 03-6709-8545

WPBASEN4-1152019