ビルディングオートメーションシステム（BAS）のサイバーセキュリティ

ビルディングオートメンションシステムを安全に保つための最善の方法と実践的なアプローチ

コネクテッドビル（スマートビル）におけるリスク軽減

注：トレインは、ここで提示されている事実と提案の正確性を確認していますが、最終的な設計および適用の決定はお客様のご判断にゆだねられます。

デジタル化された現代においては、サイバーセキュリティの脅威がどこにでも存在します。インターネット検索を行うとき、オンライン購入をするとき、または金融取引を完了するとき、機密情報を守ることが常に頭に浮かびます。ITの専門家は、ビジネスシステムを管理し保護するために細心の注意を払っています。

では、あなたのスマートビルディングシステムを監視しているのは誰でしょうか？

ビルディングオートメーションシステム（BAS）は、商業ビルの所有者や居住者にとって大きな運用上の利点を提供します。BASは、室内環境の質（IEQ）を効果的に管理し、エネルギー効率を最適化するためのアプリケーションやインターフェースを提供します。

しかし、インターネットに接続されたシステムであるため、従来のIT資産と同様のサイバーリスクを 共有しています。適切な注意を払えば、これらのリスクは管理可能です。 ここでは、BASサイバーセキュリティの最善の方法をご紹介します。

ヒント:
BAS セキュリティは他のITシステムと同様に厳重に注意を払うべきです。

よくある質問と懸念事項

BAS プロバイダーとしてトレインは毎年数千の建物およびIT専門家と協業していますが、お客様から以下のような質問や懸念を繰り返しいただくことがあります。

- BASをサイバーセキュリティの脅威から守るためにどのように設計すればよいですか？
- 施設内の他のシステムとBASシステムが最も安全に連携する方法は何ですか？
- BASへのアクセスを安全に提供するにはどうすればよいですか（現場およびリモートの両方で）？
- サービスプロバイダーに安全なアクセスを提供することは可能ですか？そのリスクは何ですか？
- BASが安全であることをどのように確信できますか？
- 安全なBASを維持するために具体的にどのような行動を取るべきですか？

BASサイバーセキュリティの3つの重要な領域

BAS業界の専門家は、これらの一般的な質問や懸念に対処しています。良いニュースとして、安全なBASシステムを設計、設置、維持するための非常に実用的なベストプラクティスがあります。

これらのベストプラクティスは、主に3つのカテゴリーに分類されます。

1. **隔離 –** BASを他のビジネスシステムから分離し、インターネットから隔離し、不正な物理的アクセスから保護する独立したエンティティとして設計します。
2. **安全なアクセス –** 従業員やサービスプロバイダーに対して、安全な現場およびリモートアクセスを提供するプロセスを確立します。
3. **運用と保守 –** 設定されたプロトコルを確立し、それに従い、システムとソフトウェアの定期的なメンテナンスを行うことで、長期的なセキュリティを維持します。

更に詳しく見ていきましょう

隔離

適切に設計されたビルオートメーションシステムは、他のシステムから十分に分離され、不正な人員によるアクセスを防ぐ必要があります。隔離は、いくつかの明確なカテゴリーに分けることができます。

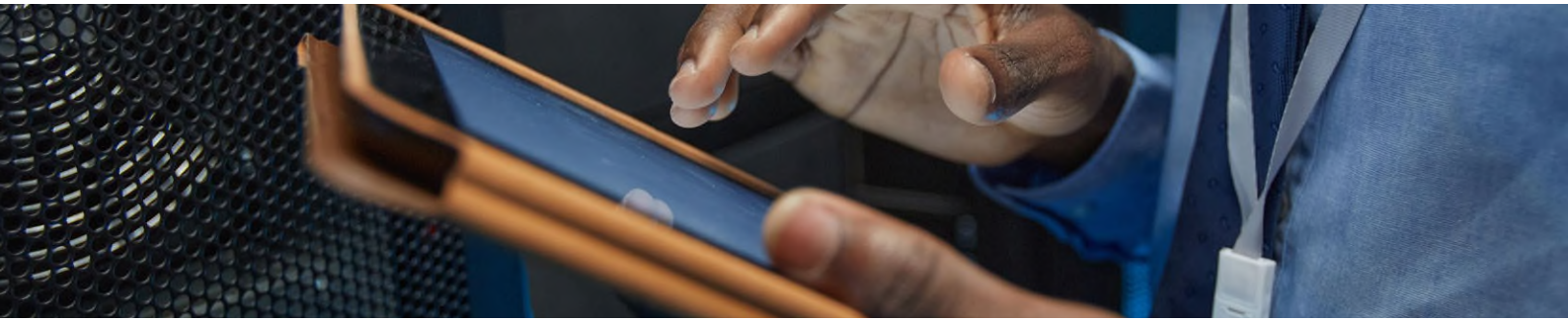
物理的隔離 BASシステムへのアクセスは、認可された従業員およびサービスプロバイダーに厳しく制限されるべきです。解決策としては、主要なBASハードウェアを施錠された部屋（例えば、電気室）に保管し、BASの運用および管理に使用されるワークステーションへのアクセスを制御することが挙げられます。

内部ネットワークの隔離 ビルオートメーションシステム（BAS）は、他のIT資産と非常に似ています。BASネットワークは、不要なリスクを軽減するために、必要な通信のみを許可し、その他の通信はすべて禁止するべきです。BASは、別の物理ネットワークにインストールするか、論理的な隔離を利用することができます。一般的な例としては、仮想LAN（VLAN）があります。

ヒント:
ITスタッフに相談しましょう。彼らはネットワークの設置や運用に関する意思決定について、適切な隔離を維持するための最善の方法を知っています。

インターネットの隔離 ビルオートメーションシステム（BAS）は、不正アクセスを防ぐためにインターネットから適切に隔離されるべきです。通常、これはファイアウォール（ルーター）を使用して、BASネットワークを外部からのインターネットアクセスから隔離することで実現されます。

ヒント: ファイアウォールを設定してBASのアウトバウンドトラフィックを許可することで、Trane Connect™リモートアクセスのような安全なリモートアクセスソリューションを利用できるようにし、サービス担当者の生産性を向上させることができます。



安全なアクセス

BASを利用する施設スタッフやサービスプロバイダーが適切にアクセスできるようにすることが重要です。セキュリティ対策は、現場およびリモートのすべてのユーザーインターフェースを網羅する必要があります。

ユーザー認証情報 BASでは通常、複数のユーザーアカウントが必要であり、それぞれのアカウントには個々の役割に応じた必要な機能に限定された権限が設定されています。専任のシステム管理者がシステム全体へのフルアクセス権を持つべきです。新しいユーザーアカウントの設定やアクセスレベルの決定（閲覧のみ、または限定された項目の閲覧および変更）は、その管理者のみが行うべきです。

オンサイトアクセス ベストプラクティスのセキュリティは、上記で述べたユーザー認証情報と組み合わせて、BASが存在するネットワークへのアクセスを制限することで実現されます。ユーザーがネットワークにアクセスできる場合、通常、BASにはウェブブラウザでを使用してURLまたはIPアドレスを介してアクセスします。

リモートアクセス リモートアクセスを使用することで、適切な人員がどこからでもシステムにアクセスできるようにします。「人員」には、貴社の従業員だけでなく、サービスプロバイダーの従業員も含まれます。リモートアクセスには、上記で述べたユーザー認証情報に加えて、追加のセキュリティ層が必要です。

インターネットから安全にBASにアクセスするための一般的な方法が２つあります。

1) セキュアリモートアクセスポータル この方法では、セキュアなアクセスを制御する別のサーバー（通常はクラウド上）を使用し、ユーザーがサイトへのアクセスをリクエストできるようにします。このタイプのソリューションは通常、以下のように機能します：

- BASシステムは、顧客ネットワークまたは別のセルラー接続を介してポータルに安全に接続します。
- 顧客ネットワークが使用される場合、アウトバウンドポートのみが使用され、インバウンドポートは開かれません。
- セルラー接続が使用される場合、ファイアウォールやプライベートセルラーネットワークなどの複数の方法を使用して安全な接続を確立します。
- ユーザーはポータルにアクセスして、1つ以上のサイトへのアクセスをリクエストできます。ポータルでのユーザー認証（ユーザー認証情報、許可されたサイト）が必要です。
- ポータルは、ユーザーが許可されたサイトへの安全なアクセスを提供します。
- ポータルは、ウェブブラウザ、モバイルアプリ、サービスツールアクセスの組み合わせをサポートする場合があります。

2) 仮想専用通信網（VPN） 施設のITスタッフは、従業員やサービス業者にBASネットワークへのリモートアクセスを提供するためにVPNを設定できます。この際、セキュリティ対策に特に注意が必要です。外部のサービスプロバイダーにVPNアクセスを許可する場合、BASネットワークの隔離レベルによっては、他のシステムへのアクセスが許可されてしまう可能性があります。

ヒント: BASは、インターネットから直接アクセスできる状態（例：公開IPアドレスと開放ポート）にしてはいけません。

ヒント: セキュアリモートアクセスポータルを使用することで、オンサイトおよびリモートアクセスの両方が可能です。この単一のアクセス方法により、VPNの設定やメンテナンスが不要となり、IT管理が簡素化されます。
また、ユーザーにとっては、オンサイトでもオフサイトでも一貫したアクセスが可能になります。

運用と保守

BASシステムが適切に隔離され、安全なアクセスが定義され実装された後は、システムを注意深く維持管理する必要があります。サイバーセキュリティのベストプラクティスは、その効果を維持するために継続的な注意が必要です。
以下にいくつかの重要な考慮事項を示します。

ユーザーIDとパスワードのベストプラクティス

不正なログイン情報の使用は、悪意のある行為者によく利用される手法です。強力で安全なユーザーIDとパスワードを割り当てることの重要性は、いくら強調してもしすぎることはありません。適切なアクセス制御とユーザー管理を注意深く維持する必要があります。

- **強力なパスワードを使用する**：推測されやすいパスワードの使用を避けます。優れたBASシステムは、パスワードの強度に関するルールを設定し 、遵守させます。
- **パスワードを共有しない：**残念ながら、これは非常によくあることです。不正なユーザーがアクセスする最も可能性の高い方法の一つです。すべての認可されたユーザーには、固有のIDとパスワードを割り当てるべきです。これにより、誰がいつシステムにログインしたかを追跡できます。
- **サービスプロバイダーには一時的なパスワードを提供する：**サービスプロバイダーや組織外の他の人に付与されるログイン情報には厳しい制限を設けるべきです。契約作業が完了したら、すぐにアクセスを削除します。特定の場合には、信頼できるサービスパートナーに対して、変更を一時的に許可するために簡単にアップグレードできる「読み取り専用」のアクセスを恒久的に割り当てることが許容される場合があります。
- **アクセスが不要になったユーザーを削除する**：非常に重要です。従業員が組織を離れた場合や、サービスプロバイダーとの契約が終了した場合は、彼らのログイン情報を削除します。すべてのシステムアクセスポイントをブロックします。

ヒント:
Active Directoryサービスを利用可能な場合、従業員はActive Directoryサービスによって認証されます。これにより、従業員は業務用のパスワードを使用してBASにアクセスすることができます。また、会社を退職した従業員がメインシステムから削除されると、BASへのアクセスがブロックされることも保証されます。

システムおよびソフトウェアのメンテナンス

適切にインストールされたシステムでも、一貫したメンテナンスがなければセキュリティを維持できません。施設の所有者や運営者は、BASシステムを最新の状態に保ち、安全に運用するための計画を持つ必要があります。
すべてのBASシステムには、以下の定期的なメンテナンスが必要です。

- **定期的なソフトウェア更新**：今日のデジタル世界では、新たなサイバー脅威に対する最新の保護を提供するために、ソフトウェアを頻繁に更新する必要があります。ソフトウェアを最新の状態に保たないと、リスクが増大します。多くのBASプロバイダーは、最低でも年に一度、または新たな脆弱性が発見された場合にはさらに頻繁に更新を行います。更新があればすぐに対応し定期的なソフトウェア更新の計画を立てましょう。

- **インターネット隔離のテスト**：ファイアウォールの設定が変更されることは珍しくありません。BASがインターネットに露出していないかを定期的にテストし、継続的なシステムメンテナンスの一環として行います。早期発見がリスク軽減の鍵です。

- **ユーザー認証情報の確認**：BASシステム内のすべてのユーザーのログイン認証情報を定期的に確認するスケジュールを設定します。リストにあるすべてのユーザーが、付与されたアクセスレベルを引き続き必要としているかを確認します。アクセスが不要になったユーザーを削除します。

ヒント: 社内に専門知識がない場合は、サービスプロバイダーに依頼してサイバーセキュリティの維持を支援してもらうことができます。

トレインは、お客様のシステムを確実に保護するために一歩先を行きます。

サイバーセキュリティは、トレインのすべてのコネクテッドソリューションにおいて優先事項です。トレインはお客様のITチームと緊密に連携し、トレインのコネクテッドビルディング管理システムがリスクに対して強化され、認可されたユーザーに安全なアクセスを提供できるよう支援します。以下は、トレインが提供する人気のあるソリューションで、システムのセキュリティを容易に保つのに役立ちます。

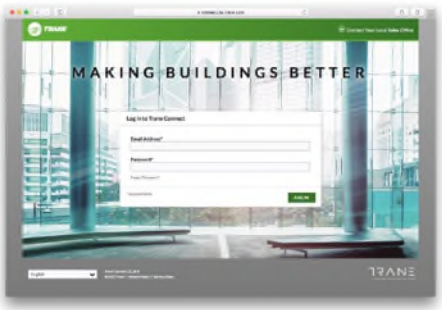
安全なセルラー接続

BASシステムへのインターネットアクセスに課題がありますか？BASシステムをビジネスネットワークから隔離する必要がありますか？トレインは、お客様のニーズに合わせた複数のセルラー接続オプションを提供しています。最も人気のあるオプションは、プラグアンドプレイのトレインUSBセルラーモジュールで、トレインBASシステムとTrane Connectセキュアリモートアクセス間のプライベートで暗号化された通信を提供します。

Trane Connect™ セキュアリモートアクセス

トレインのクラウドベースのカスタマーポータルは、リモート監視や定期メンテナンスのために、トレインBASへの安全なリモートアクセスを提供します。その他の利用可能なサービスに加えて、Trane Connect セキュアリモートアクセスはウェブブラウザとトレインのモバイルアプリスイートをサポートしているため、どこからでも簡単にトレインBASシステムにアクセスできます。

従業員やサービスプロバイダーにアクセス認証情報を提供することができます。管理者権限があれば、アクセス認証情報とサイト権限を持つ人々のリストを自分で管理できます。すべての場合において、建物レベルのBASシステムのパスワードは追加のセキュリティ層として維持されます。



Trane Connect セキュアリモートアクセスの特徴

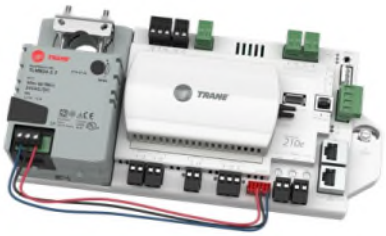
- ネットワークまたは別のセルラー接続を介して、建物からクラウドへの安全な接続。
- Trane ConnectレベルおよびBASシステムレベルでのユーザーアクセス制御。
- 認可されたユーザーは、PC、タブレット、または電話を使用して、ウェブブラウザまたはトレインのモバイルアプリスイートを介してBASシステムにアクセス可能。

サービス契約

BASシステムを安全かつ最新の状態に保つことは、継続的な優先事項です。新たなサイバーリスクが常に出現しています。BASソフトウェアを最新の状態に保つことは、安全なシステムを維持するための重要な要素です。システムは定期的にテストされ、安全性を確認する必要があります。また、ユーザーアクセス認証情報（パスワードなど）も定期的に見直し、管理する必要があります。トレインは、建物とBASシステムを最適なパフォーマンスと継続的なセキュリティで維持するために、オンサイトおよびコネクテッドサービスを含むさまざまなサービス契約を提供しています。

制御関連製品のセキュリティ

Tracer® SC+やSymbio®ユニットコントロールを含むトレインの制御関連製品は、暗号化、複数層のアクセス制御、認証などのツールを使用して、インシデントからデータを保護するように設計されています。トレインは、複雑なサイバーセキュリティ機能を標準装備で提供しています。



TRANE

Learn more at jp.trane.com

トレイン・ジャパン株式会社

本　社

〒141-0021　東京都品川区上大崎4-5-37 本多電機ビル5F
（営　業　部）　Tel.03-5435-6442　Fax.03-5435-6440
（サービス部）　Tel.03-5435-6443　Fax.03-5435-6440

大阪事業所

〒577-0848　大阪府東大阪市岸田堂西2-10-28
（営　業　部）　Tel.06-6726-4550　Fax.06-6224-1271
（サービス部）　Tel.06-6726-4563　Fax.06-6224-1271

広島事業所

〒739-2102　広島県東広島市高屋町杵原1312-2
Tel.06-6726-4563　Fax.06-6224-1271

九州事業所

〒861-8038　熊本県熊本市東区長嶺東8-13-47
Tel.050-3662-3410　Fax.096-349-7075

宮城出張所

〒981-3117　宮城県宮城郡利府町花園3-24-1
（サービス部）　Tel.022-369-3849　Fax.022-369-3849

BAS-SLB135-JP
03/2025