Cybersecurity Summary

Trane® Connect™ | リモートアクセス

Trane Connectとは?

Trane Connect は、Tracer®ビルディングオートメーションシステム（BAS）の認証されたユーザーが、Traneのクラウド環境にアクセスできるようにするソフトウェア・アズ・ア・サービス（SaaS）です。

建物のファイアウォール内にある Tracer コントローラーから、最初に外部に向けて開始される安全な接続を確立することで、Trane Connectを通じたリモートアクセスが実現されます。

Building Automation System（BAS）へのリモートアクセスは、認証済みユーザー（主に企業のサービスエンジニア）に対して、施設設備を遠隔から構成変更・運用管理・保守作業を実施するための高度な柔軟性を提供します。これにより、作業の迅速化、運用コストの最適化、そして高いセキュリティレベルを確保した遠隔サポートが可能となります。

動作の仕組み

エンドポイントセキュリティ

Tracer BAS（Tracer® SC+、SC、ならびに各種レガシーコントローラ）は、Trane Cloud との連携を行うようにネットワーク設定を構成することが可能です。クラウドとの通信には、現行製品群ではWebSocketプロトコルを採用し、レガシー Trane コントローラではOpenVPNを用いることで、暗号化されたトンネルを介したセキュアな通信路を確立します。このアーキテクチャにより、標準化された方式で、シンプルでありながら高いセキュリティを備えた接続性を提供することができます。

Trane Connectのセキュリティ対策

- Tracer BAS コントローラとTrane Cloud間にセキュアな通信チャネルを確立し、最新のTLS／SSL 暗号化を適用することで、施設へのリモートアクセス機能を安全に提供します。
- 既存のファイアウォール設定を最小限の変更で運用可能な、セキュア接続向けソリューションです。
- 現行のBAS コントローラでは、WebSocket／OpenVPN 通信において TCP 443 を利用したアウトバウンド接続を使用します。
- レガシー Tracer BASコントローラでは、OpenVPN による UDP 1194 ポートを用いたアウトバウンド接続を使用します。
- 256-bit AESの暗号化レベルを採用しています。
- Tracer BASコントローラはクラウド側への全ての通信セッションを内部ネットワークから外向きに開始し、セキュアなリモートアクセス経路の確立を実現します。
- リモートアクセスの確立には、クラウドレイヤーと Tracer BAS コントローラの双方における厳格なユーザー認証および認可プロセスが要求されます。これらは 3 ステップの手順として実装されています。

1. Tracer BAS コントローラが、通信セッションを確立するための初期ハンドシェイクを主導的に実行します。

2. Trane Cloud*側において、ユーザーの認証資格およびアクセス権限を厳密に検証します。

3. Tracer BAS* コントローラに対して、ユーザー資格情報を用いた直接認証を行います。

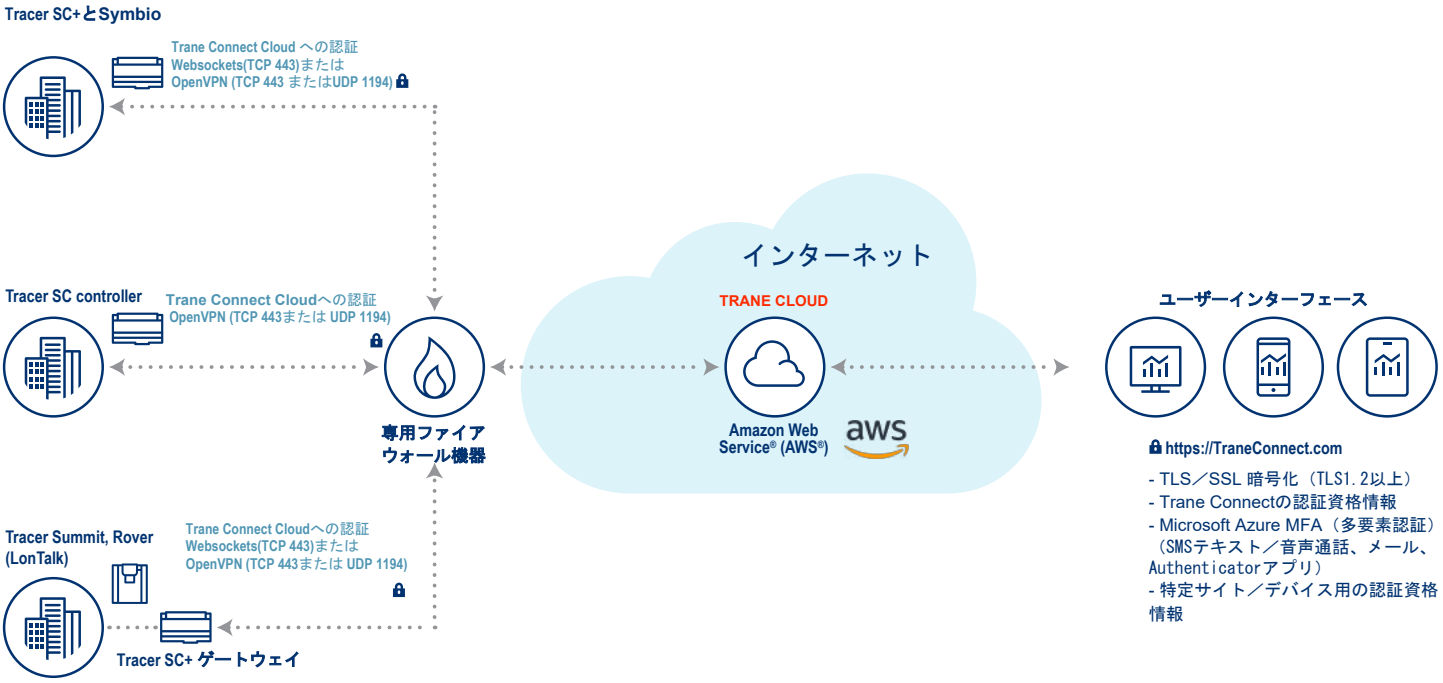
***注**：有効なユーザー資格情報が必須となります。

Trane Connect を用いたリモートアクセスにおけるファイアウォール要件：

·ポート443（TCP）–アウトバウンド通信
·ポート 1194（UDP）–アウトバウンド通信

TRANE TECHNOLOGIES

ネットワークセキュリティ



1. ユーザーがTracerBASコントローラをTraneCloud 上に登録します。
この処理は、前述の通り、３段階のプロセスによって実行されます。
2. ユーザーは Trane Connectポータルを介して自身を認証し、Tracer BAS コントローラへのアクセスを確立します。
これは、Tracer BAS コントローラに対して構成されたセキュアトンネルへアクセスする唯一の手段です。
3. Trane Connect は、Microsoft® Azure® が提供する組み込みの多要素認証（MFA）を使用しています。
すべての通信は、TLS 1.2 以上の最新の TLS／SSL 暗号化によって保護されています。
4. Trane Connect のリモートアクセスセッションが確立された後、ユーザーは各 Tracer BASコントローラへアクセスするために、ログイン認証情報を個別に入力する必要があります。
5. ユーザーが各Tracer BAS コントローラからログアウトすると、Trane Connect のリモートアクセスセッションは都度無効化されます。
6. Trane Cloudサーバーは、Trane Connect の管理インターフェースを通じて、リモートアクセス操作のトラッキングおよびログ記録を実施します。

データプライバシー

Trane Technologies™Company, LLC（以下「Trane Technologies」）は、個人のプライバシーを尊重し、顧客、従業員、取引業者、消費者、ビジネスパートナー、その他関係者から寄せられる信頼を重視しています。
トレインテクノロジープライバシーポリシーの詳細は以下のリンクからご確認ください。
https://www.tranetechnologies.com/en/index/privacy-policy.html.

データセキュリティ

Trane Tracer BAS コントローラおよび Trane Cloud によるデータ利用は、HVACマシンデータのみに限定されています。HVACマシンデータとは、手動入力を伴わず、製品または提供されたサービスから自動的に生成・収集されるデータを指します。これには、HVAC システムの物理的測定値および運転状態に関連するデータが含まれ、例えば温度、湿度、圧力、HVAC機器の動作状況などが該当します（これらに限定されない）。

HVAC マシンデータには、個人データは一切含まれません。
また、本書においては、仮に Trane のコントロール製品またはホスト型アプリケーションの利用者が、製品内で作成するアカウントに自身の氏名（例：firstname.lastname@address.com）を使用した場合であっても、当該氏名は個人データには該当しないものとします。

HVAC マシンデータは、Trane によって以下の目的で利用される場合があります。
(a) 製品およびサービス利用者に対し、より高品質なサポートサービスや製品を提供するため (b) Trane の規約および条件への適合性を評価するため (c) 製品およびサービス利用者の集計的特性や行動に関する統計分析その他の分析を行うため (d) ユーザーデータおよびその他情報のバックアップ、ならびにリモートサポートやデータ復旧を実施するため (e) 各種技術分析を提供または実施するため（エンジニアリング分析、故障解析、保証分析、エネルギー分析、予測分析、サービス分析、製品使用状況分析、その他必要な分析。これらの履歴や傾向分析を含むが、これらに限定されない）(f) 製品または提供サービスの利用者のニーズを把握し、それに対応するため。

Trane Connectで利用される基盤技術

WebSocket プロトコルは、クライアントからのリクエストを必要とせずにサーバーからクライアントへデータを送信できる標準化された仕組みを提供することで、リアルタイムデータ転送を実現します。
Trane はWebSocket Secure（wss://）を採用しており、TLS 1.2 以上の暗号化を伴うTCP 443番ポートを使用してTrane Cloudへのセキュアな接続を確立します。
なお、WebSocket プロトコルはIETF によりRFC 6455 として標準化されています。

OpenVPN は、仮想プライベートネットワーク（VPN）技術を実装するソフトウェアアプリケーションであり、ルーティングまたはブリッジ構成におけるポイントツーポイント接続やサイト間接続、リモートアクセス接続をセキュアに構築するために用いられます。
OpenVPN は、SSL/TLS を利用した鍵交換を行う独自のセキュリティプロトコルを使用しています。

TRANE

トレイントレイン・テクノロジーズ（Trane Technologies、ニューヨーク証券取引所上場、NYSE:TT）は、グローバル・クライメート・イノベーター（世界的気候改革者）です。暖房、換気、空調・制御システムサービス、部品など、豊富な製品群を通して快適で省エネな室内環境を創出します。詳しくは jp.trane.com または trane technologies.com をご覧ください。

BAS-SLB072-JP
09/19/2023