データ シート

Zscaler Privileged Remote Access for OT and IIoT Systems

産業用システムおよびデバイスへの高速かつ安全な直接アクセス

Zscaler Privileged Remote Access は、VPN やエージェントに頼ることなく、さまざまな現場や工場など、あらゆる場所の運用技術 (OT) およびインダストリアル IoT (IIoT) 資産への高速かつ安全な直接アクセスを可能にします。

工場の生産性を最大化し、ベンダー / 請負業者のリスクを最小化

リモート アクセスは、スマート ファクトリーの生産監視と予知保全には欠かせません。現場の技術者やサードパーティー ベンダーは、工場 / 現場の資産にリモートで接続し、機械のデータを確認することで、リアルタイムで機器の監視、トラブルシューティング、修理を行い、工場の稼働時間と効率を最大限に高める必要があります。

リモート ユーザーはこれまで、こうした資産に仮想プライベート ネットワーク (VPN) を介して接続してきましたが、VPN は管理が煩雑なうえ、固有のセキュリティ上の欠陥を抱えています。VPN を使用した従来のリモート アクセス アプローチは、ネットワーク内のすべての人を信頼し、必要以上にアクセス権を付与する「城と堀」のアーキテクチャーを基盤としており、これを悪用する攻撃者に簡単に侵害される可能性があります。

OT セキュリティの課題

- **ランサムウェア攻撃による中断のリスクを抱える従来の OT 環境：**攻撃者は外部に公開された脆弱な OT 資産を発見し、悪用することができます。

メリット

- **稼働時間の向上とリスクの低減**
  ゼロトラスト接続により、ベンダー / 請負業者が機器への接続や修理を速やかに行えるようになり、ダウンタイムとリスクを最小化
- **工場と従業員の安全性の向上**
  OT ネットワークや OT システムをインターネットから不可視化することで、攻撃者による発見と悪用、生産プロセスの妨害を阻止
- **優れたユーザー エクスペリエンスの提供**
  従来の VPN の煩わしさを伴わず、リモート ワーカーやサードパーティーが簡単にアクセス可能
- **OT/IT の統合の加速**
  ゼロトラスト セキュリティを OT および IIoT に拡張し、インダストリー 4.0 の取り組みを加速

ほとんどの OT システムは、ベンダーが提供するセキュリティ パッチを必要な頻度で取得しておらず、定期的な更新のために十分なダウンタイムを設けていません。

- **大きな運用上のオーバーヘッドを伴う VPN：**通常、VPN にはインバウンド ポートが必要なため、ユーザーのアクセスを制限するにはファイアウォールの頻繁な変更が必要です。従来のアプライアンス ベースの特権アクセス管理 (PAM) 製品と組み合わせて使用される場合もありますが、これによって複雑さは増大する一方、ランサムウェア対策として十分な効果は得られません。
- **自由なラテラル ムーブメントを可能にする過剰なアクセス権：**VPN は、ユーザーの管理対象外エンドポイントを直接 OT ネットワークに接続するため、ランサムウェアやマルウェアが工場の環境に持ち込まれるリスクが高まります。
- **拡張性と高速かつシームレスなユーザー エクスペリエンスを提供できない従来のアーキテクチャー：**VPN クライアントは煩わしく、動作が遅いうえ、互いに競合するケースが多いため、リモートの技術者が複数のノート PC を操作したり、さまざまな OT 機器にアクセスするために大きなコストをかけて現場を訪問したりする必要があります。

こうした課題は、最終的に工場のダウンタイムを引き起こし、工場の作業員や機器に物理的な安全上のリスクをもたらす可能性があります。OT の運用担当者は、VPN に代わる安全で信頼性の高いソリューションとして、ゼロトラスト セキュリティに関心を寄せています。

Zscaler Privileged Remote Access

Zscaler Privileged Remote Access は、さまざまな現場や工場など、あらゆる場所の OT および IIoT デバイスへの高速かつ安全で信頼性の高い接続を可能にするクラウド型ゼロトラスト アクセス ソリューションです。ZPA プラットフォームを基盤とする特権リモート アクセスにより、リモート ワーカーやサードパーティー ベンダーは、RDP、SSH、VNC を使用した機密性の高い生産システムへのクライアントレス リモート デスクトップ アクセスが可能になります。管理対象外のデバイスにクライアントをインストールしたり、ジャンプ ホストや VPN にログインしたりする必要はありません。

業界唯一の OT および IIoT 向けのゼロトラスト アクセス ソリューションとして、Zscaler Privileged Remote Access は以下のようなメリットを提供します。

稼働時間と生産性の向上

インラインのゼロトラスト セキュリティによる直接接続により、ユーザーは機器への接続と修理をすばやく行えるようになり、ダウンタイムを最小限に抑えられます。また、速度低下やコストの増加を招く従来の VPN や PAM 製品を介したバックホールを排除できます。

工場と従業員の安全性の向上

インサイドアウト接続によって、OT ネットワークとシステムがインターネットから不可視化されるため、生産プロセスを混乱させようとする悪意のある人物に資産が発見されたり、悪用されたりすることはありません。

卓越したユーザー エクスペリエンスの実現

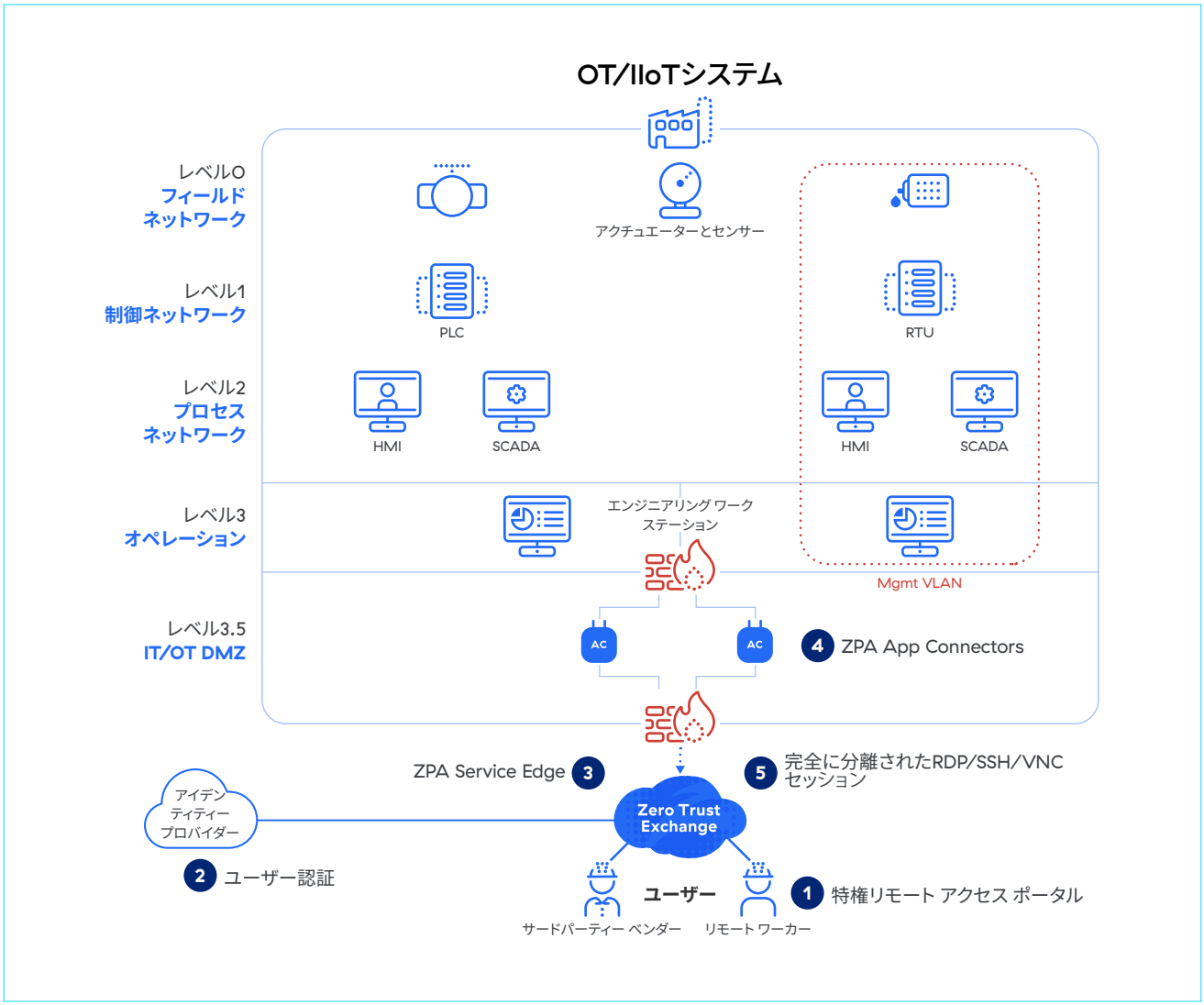
Web ブラウザーからクライアントレスでアクセスできるため、リモート ワーカーだけでなく、サードパーティーのベンダーや請負業者も従来の VPN のような煩わしさを感じることなく、OT システムに簡単にアクセスできます。

ガバナンス制御によるリスクの軽減

クラウドベースのセッション記録、ストリーミング再生、セッション監視、許可制のアクセスにより、サードパーティーのリモート アクセス セッションを完全に監視、制御します。

仕組み

特権リモート アクセスによって、管理者、リモート技術者、ベンダー、請負業者は、VPN やエンドポイント エージェントを使わずに OT/IIoT システムに安全にアクセスし、完全なサイバー脅威対策と運用の保護を実現できます。



1 ユーザーが HTML5 対応の任意のブラウザー (Chrome、Safari、Edge など) から特権リモート アクセス ポータルにログオンします。

2 設定された SAML/OIDC アイデンティティー プロバイダーを介してユーザーが認証、承認され、承認されたコンソールがポータルに表示されます。

3 Zero Trust Exchange の一部である ZPA の最寄りのサービス エッジにユーザー セッションがルーティングされます。

4 OT 環境に展開された Zscaler App Connector が、Zscaler Zero Trust Exchange へのアウトバウンド接続を開始します。SSH/RDP/VNC ポートをネットワーク外に公開する必要はありません。

5 ユーザーが OT システムへの分離された SSH/RDP/VNC セッションをリクエストします。Zero Trust Exchange は、ユーザーのセキュリティ ポリシーとアクセス ポリシーに従って、ユーザーのコンソールと対応する App Connector 間の接続を仲介します。

App Connector と OT システムの間で SSH/RDP/VNC 接続が開始され、ユーザーのコンソール セッションにピクセル データがストリーミングされます。これにより、OT システムとリモート技術者間でのネットワーク接続が不要になります。

主要な機能

HTML5 対応ブラウザー経由のクライアントレスアクセス	内部および外部のユーザーを、RDP、SSH、VNC を使用する対象システムに完全に分離した形で接続し、管理対象外のエンドポイントや信頼されていないネットワークからの接続を可能にします。サードパーティーのユーザーがデータに安全にアクセスできるようにしながら、コピー、貼り付け、ローカルの管理対象外デバイスとの間でのアップロードやダウンロードをブロックします。
完全に分離されたクライアントレスの RDP、SSH、VNC セッション	サードパーティーのユーザーが、クライアントをインストールしたり、VPN を経由したりすることなく、管理対象外デバイスで HTML5 対応のブラウザーを使用して OT システムにアクセスできるようになります。
ネットワーク変更の回避	IP アドレスの重複がある場合でも、コストのかかる手作業でのネットワーク アドレス変換を行うことなく、複数のサイトにまたがるシステムへのアクセスを可能にします。工場からのアウトバウンド接続は 1 つだけとなるため、ファイアウォールの定期的な変更も回避できます。
攻撃対象領域の排除	承認されたユーザーと特定のデバイスの間に 1 つの安全なセグメントを作成することで、インターネットや許可されていないユーザーから OT システムを不可視化します。また、OT ネットワークへのすべてのインバウンド接続を排除します。
ユーザーのアイデンティティーに基づく OT アクセス	強力なネイティブのポリシー エンジンを使用して、ユーザー、デバイス、コンテンツ、アプリケーションのリスク ポスチャーに基づいたアクセス ポリシーを継続的に検証し、認証されたユーザーのみが生産システムにアクセスできるようにします。
期限付きアクセス	特定のシステムやデバイスへのアクセスを特定の時間に制限します。時間帯と曜日を追加して、有効な時間をさらに制限し、常時アクセスのオーバープロビジョニングを防ぎます。

緊急アクセスのためのジャストインタイム ユーザー プロビジョニング	緊急アクセスのためのサードパーティー ユーザーのプロビジョニング、管理、プロビジョニング解除の負担を軽減します。
資格情報の Vault	RDP、SSH、VNC を使用するシステムにアクセスするための認証情報を Zscaler の Vault に安全に保管します。ユーザーを SAML のアイデンティティーにマッピングするとともに、さまざまな基準を使用して OT システムの資格情報を対象システムに挿入し、OT システムの資格情報のサードパーティーとの共有を避けます。
転送ファイル向けのインライン ウイルス対策と高度なクラウド サンドボックス	対象システムに転送されたファイルのインライン ウイルス スキャンと、高度なクラウド サンドボックスでの実行により、ランサムウェアとマルウェアを阻止します。
セッションの録画とストリーミング再生	改ざん防止処理を施した録画データを、データ主権が確保されたクラウドに保存します。録画データは、ロールベースのアクセス制御に基づきオンデマンドでストリーミングできます。
セッションの監視	ライブ PRA セッションを監視して、ベンダーの技術者を監督し、工場のリスクを最小限に抑えます。偶発的なものか悪意によるものかを問わず、セッションを即座に終了して、中断の原因となる行為を阻止できます。
許可制のアクセス	画面共有、マウスとキーボードの操作によって、技術者との共有 PRA セッションをホストします。
マイクロ テナント	サブテナントへの委任管理者アクセスにより、ロールベースのきめ細かいアクセス制御を提供します。

ライセンス

価格は一意の OT アプリケーション (RDP、SSH、VNC を使用する対象システム) の数に基づきます。

ソリューションの機能	PRA Essentials	PRA Advanced
	提供されるもの：PRA システム / コンソール 10 件につき 1 組の App Connector。 公正使用制限：10 GB/ システム / 月 (ZPA テナント全体でのデータ使用量)。 システムは、RDP、SSH、VNC の特権コンソールとして定義	
SSH、RDP、VNC の完全なプロトコル分離	✓	✓
対話型認証	✓	✓
クリップボード制御 (テキストのコピーと貼り付け)	✓	✓
Advanced Cloud Sandbox[1] を使用したサンドボックス化されたファイル転送	✓	✓
ジャストインタイム / 期限付きアクセス	✓	✓
資格情報の Vault とインジェクション		✓
緊急アクセス		✓
クラウド セッションの録画と再生		✓
セッションの監視		✓
許可制のアクセス		✓

1. Advanced Cloud Sandbox を含んだ ZIA テナントが必要です。
2. 緊急ユーザーは ZPA ユーザー ライセンス数にカウントされません。各四半期におけるアクティブな一意の緊急ユーザー数は、ZPA プラットフォームのユーザー数を超えてはなりません。
3. セッションの録画はクラウドに 365 日間保存されます (テナント全体で 10 時間 / システム / 月の録画を含む)。

PRA Essentials は ZPA Business Edition の一部として含まれ、PRA Advanced は ZPA Transformation Edition および Unlimited Editions の一部として含まれています。対象システムの上限は合計 10 件です。追加のライセンスを購入することで、容量を拡張することができます。インライン クラウド サンドボックスを利用するには、Advanced Cloud Sandbox 機能を含んだ Zscaler Internet Access テナントが必要です。

技術仕様

Zscaler のコンポーネント	サポートするプラットフォームとシステム
特権リモート アクセス	対象システム：Windows ── RDP または VNC Linux/Unix ── SSH または VNC OIDC/SAML IdP ── ZIdentity、Microsoft Azure、Okta[1]
App Connector	VMware vSphere Hypervisor arm64 および amd64 プラットフォーム用 Docker コンテナー Zscaler Branch Connector Device

1. 緊急アクセスは Okta でのみサポートされています。

OT および IIoT におけるゼロトラスト セキュリティのメリット

従来、OT 環境は外界から物理的に隔離された状態にありましたが、デジタル化が進みインターネットに接続されるようになり、マルウェアやランサムウェア、サプライ チェーン攻撃の影響を受けやすくなってきています。これらはシステムの中断を引き起こし、従業員を危険にさらす恐れがあります。ファイアウォールや VPN などの従来の境界型セキュリティ対策で OT 資産を侵害から保護するだけでは、もはや十分ではありません。ゼロトラストは予定外のダウンタイムを防ぎ、産業システムの生産性を最大化するための鍵となります。

- **攻撃対象領域の最小化：**公開されたポートを不要にすることで、OT および IIoT システムを攻撃者に対して不可視化します。
- **ラテラル ムーブメントの排除：**ユーザーと OT システムが同一のネットワーク上で接続されないようにすることで、マルウェア攻撃やランサムウェア攻撃の拡散を防ぎます。
- **OT/IT の統合の加速：**リモート管理のスピードとアジリティーを維持しながら、OT システムを安全に接続、管理します。

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com/jp