

Zscaler の製造業向けソリューション

Purdue モデルにゼロトラストを導入

ソリューションの概要

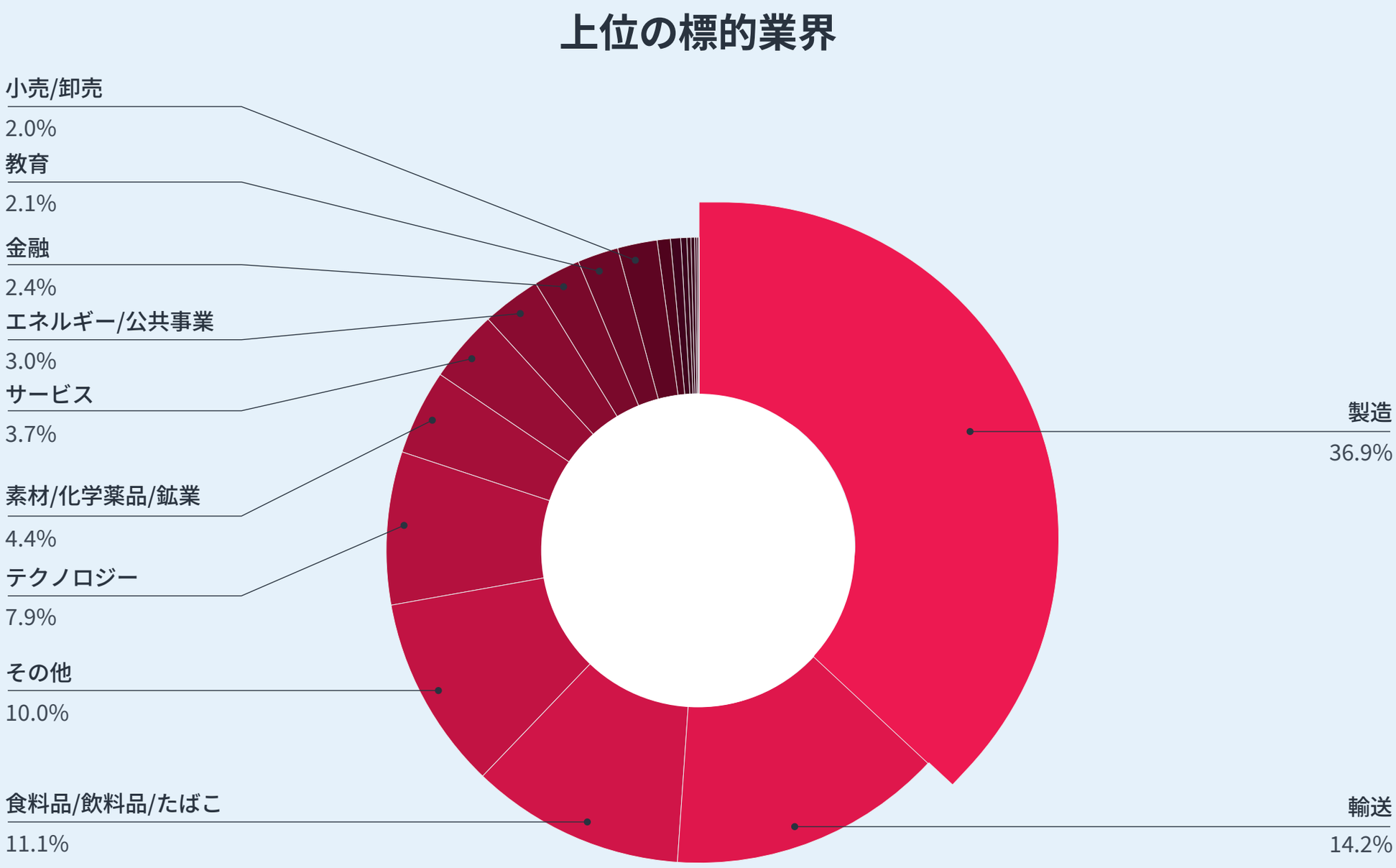
©2025 Zscaler, Inc. All rights reserved.

工場には新たなアプローチによる OT システム保護が必要

世界中の製造企業が、生産ラインを強化するために、スマート ロボット、すべての機械への IoT センサーの取り付け、クラウドベースの分析、工場フロア全体のデジタル ツインなどを導入しています。目標はシンプルです。生産高の向上、ダウンタイムの短縮、そして 24 時間体制の生産を実現する予測メンテナンスです。

しかし、多くの組織は、想定とは異なる現実を認めています。新たな接続のたびに OT の攻撃対象領域が拡大し、ひとたび攻撃者に侵入されると、影響を受けるリスクが大幅に高まるのです。その原因となるのは古い OS、フラットなネットワーク、OT に対する可視性の低さです。工場の変革を続けるには、工場のセキュリティ アーキテクチャーを再構築する必要があります。

Zscaler の Threatlabz による最新の IoT/OT レポートによると、IoT に対するマルウェア攻撃のうち 36% を製造業が受けており、これは全業界で最大となっています。



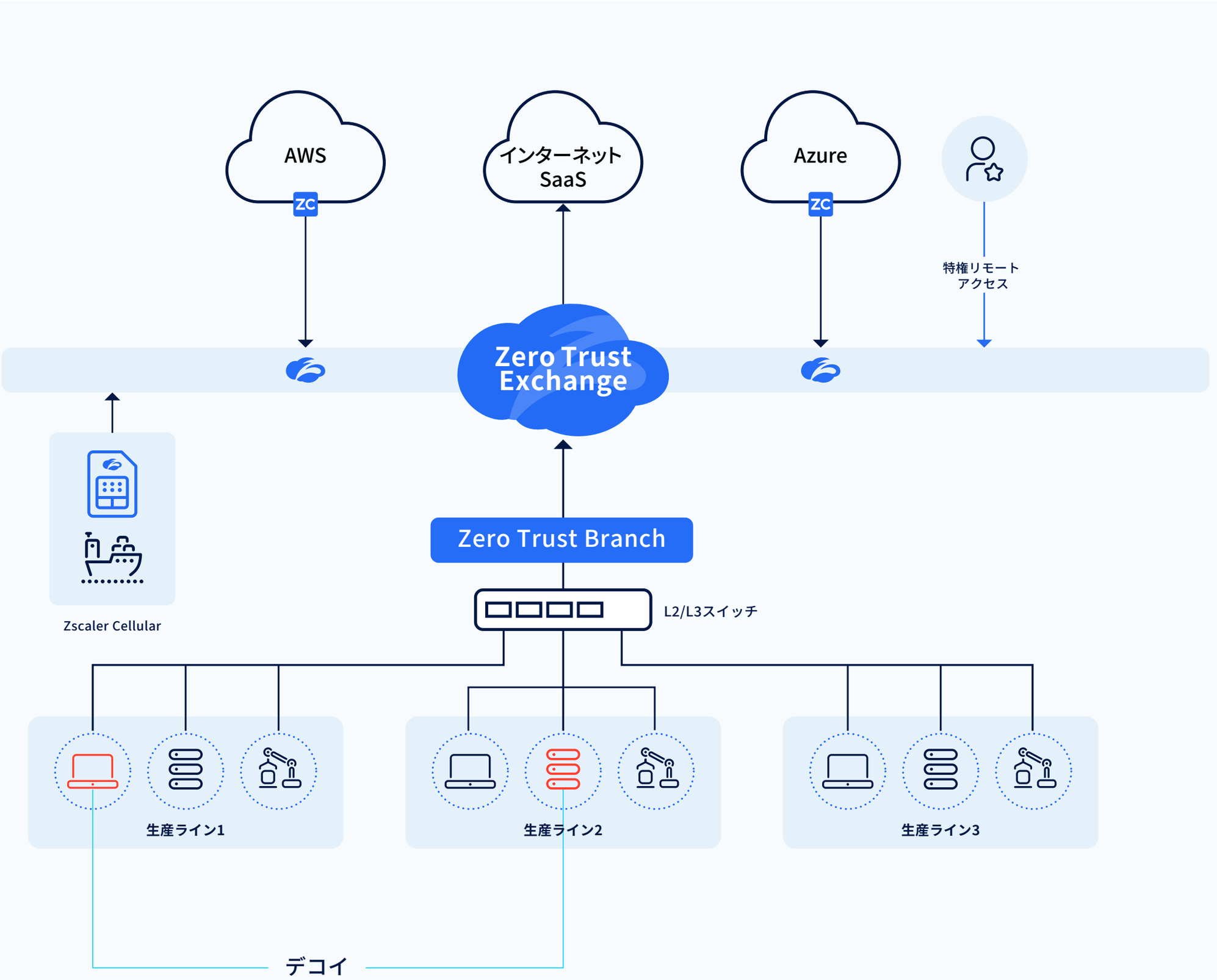
業界別の標的分布

©2025 Zscaler, Inc. All rights reserved.

工場内外のすべてのユーザーと デバイスへのゼロトラストの拡張

セキュリティ部門は、製造と産業環境を保護するために、すべてのユーザーとデバイスのやり取りが検査され、最小特権ポリシーに従って施行されることを確認する必要があります。Zscaler のゼロトラスト アプローチは OT 専用に構築されており、工場運営全体で安全なアクセス、セグメンテーション、接続を実現します。

- 技術者やサードパーティーが重要な OT システムにアクセスする際には VPN 不要のアクセスを提供
- きめ細かな東西のセグメンテーションを適用し、脅威のラテラル ムーブメントを防止
- OT システムをクラウドやデータ センターに安全に接続し、分析を実施
- トラック、キオスク、POS スキャナーなどのセルラーの OT システムにゼロトラストを拡張
- 攻撃者を早期に検出し、権限昇格を防止



工場向けゼロトラスト アーキテクチャー

©2025 Zscaler, Inc. All rights reserved.

Zscaler ソリューションのコンポーネント

特権リモート アクセス

サードパーティーやリモート技術者が、任意のブラウザーを介して RDP/SSH/VNC の宛先にエージェントレスで安全に接続できるようにします。

主な機能

クリップボードの制御
ゼロトラスト ポリシーに基づいてコピー / 貼り付け機能を制限し、機密データを保護します。

監査とガバナンス制御
セッションの録画、セッションの共有、許可制のアクセスにより、サードパーティーのリスクを軽減します。

資格情報 Vault とマッピング
対象システムの資格情報をクラウドの Vault に保存し、マッピング ポリシーを通じてアクセスを共有します。

期限付きアクセスとジャストインタイム アクセス
メンテナンス ウィンドウを計画的に設定し、緊急メンテナンス時には JIT アクセスを提供します。

ゼロトラスト セグメンテーション

OT システムのマイクロセグメンテーションを行い、OT システムと OT/IT システム間の通信を確実に許可されたもののみにするポリシーを施行します。

きめ細かなマイクロセグメンテーション
サポートされている OT システムを 1 つのセグメントに分離します (/32 を使用)。

デバイスの検出と分類
OT デバイスを自動的に検出、分類します。

ランサムウェアのキル スイッチ
既定のポリシーを適用してインシデント対応を自動化し、OT システムを段階的に制限します。

ポリシーの施行
デバイスの種類やタグに基づいてデバイスを自動的にグループ化し、東西トラフィックに対してポリシーを施行します。

©2025 Zscaler, Inc. All rights reserved.

OT への安全なアクセス

カメラ、センサー、モニター、キオスク、その他の OT システムをクラウド アプリケーションとインターネットに安全に接続させます。リスクの高いまたは悪意のあるアプリや URL との通信をブロックします。

ゼロタッチ プロビジョニング 事前定義済みのテンプレートを使用し、完全に自動化されたゼロタッチの展開を活用します。	**統合されたゼロトラスト ポリシー** IoT/OT がプライベート アプリやインターネットにアクセスする際、検査し、ポリシーを施行します。
きめ細かなポリシーの施行 ユーザー / デバイスの地域、場所、アクセスされた URL、機密データなどに基づいて、ポリシーを施行します。	**セルラーのゼロトラスト接続** トラック、キオスク、掘削装置などのセルラーデバイスのゼロトラスト接続を簡単に実現します。

Zscaler Deception

既存の防御を回避した OT 脅威を、デコイを使って検出します。侵害されたユーザーを検出し、ラテラル ムーブメントを阻止するとともに、ランサムウェアや悪意のある内部関係者から保護します。

ラテラル ムーブメントの検出 PLC や SCADA のデコイ システムを展開し、攻撃者のラテラル ムーブメントの試みを検出します。	**侵害前の検出** 脅威アクターが攻撃前に環境を偵察している際に、正確なアラートを受信できます。
クラウド ネイティブで導入 Zscaler Private Access (ZPA) との統合を通じて、デコイの作成、ホスト、配信を可能にします。	**ネットワーク構成は不要** VLAN トランキング、SPAN ポート、GRE トンネルから脱却し、トラフィックをデコイにルーティングします。

©2025 Zscaler, Inc. All rights reserved.

Zscaler の主な特長

セキュリティ ギャップの解消

工場内外のすべての環境に、一貫したゼロトラスト ポリシーを施行します。

ダウンタイムの低減

既存の OT 環境の中断を最小限に抑えてゼロトラスト セグメンテーションを施行し、ラテラル ムーブメントによるダウンタイムのリスクを軽減します。

コストと複雑性の軽減

工場内にシンプルな Purdue モデルのセキュリティ アーキテクチャーを使用することで、ファイアウォールや NAC、VPN、VDI、マイクロセグメンテーション ツールを削減または統合します。

Zscaler について

Zscaler (NASDAQ: ZS) は、より効率的で、俊敏性や回復性に優れたセキュアなデジタル トランスフォーメーションを加速しています。Zscaler Zero Trust Exchange™ プラットフォームは、ユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界 150 拠点以上のデータ センターに分散された SSE ベースの Zero Trust Exchange™ は、世界最大のインライン型クラウド セキュリティ プラットフォームです。詳細は、**zscaler.com/jp** をご覧いただくか、Twitter で **@zscaler** をフォローしてください。

© 2025 Zscaler, Inc. All rights reserved. Zscaler™ および **zscaler.com/jp/legal/trademarks** に記載されたその他の商標は、米国および / または各国の Zscaler, Inc. における (i) 登録商標またはサービス マーク、または (ii) 商標またはサービス マークです。その他の商標はすべて、それぞれの所有者に帰属します。

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

Zero Trust Everywhere