Zscaler Zero Trust Automation の概要

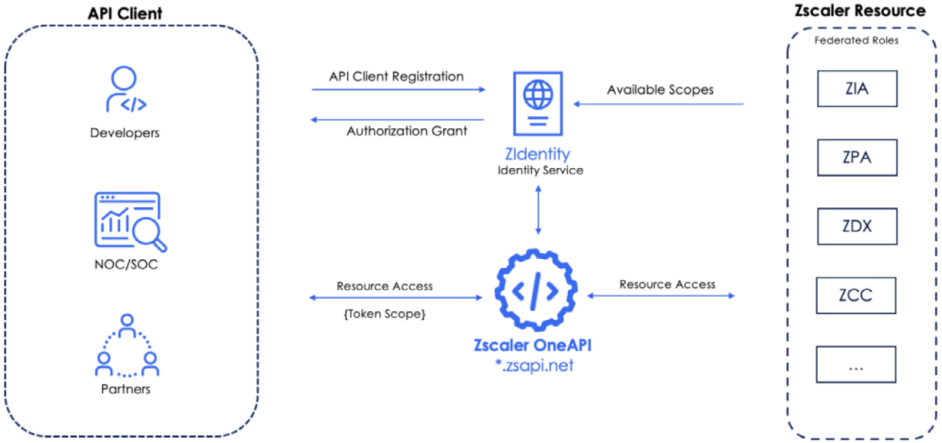
管理が必要な IT 製品やアプリケーションが増えるにつれ、多くの組織がユーザー コンソールを介した手動管理から自動化ソリューションに移行しています。自動化は、ますます複雑化する IT システムをより効果的に管理し、コストのかかるセキュリティ侵害を招く恐れのあるヒューマン エラーのリスクを削減することで、IT 部門をサポートします。

AI がコードの作成や日常業務の自動化にますます利用される中、自動化はすでに新しい形の IT 管理者として役割を果たしています。Zscaler はこうした傾向を反映し、オートメーション エンジニア向けに特別に設計された自動化サービスである OneAPI を開発しました。

Zscaler の自動化

Zscaler は API ファーストの戦略を採用しているため、すべてのサービスと機能が API を介してアクセスおよび設定できるように構築されています。セキュリティ エンジニアが長年使用してきた Zscaler の Web コンソールは、API を介してバックエンドでやり取りします。この Web コンソールに加えて、Zscaler の新たな API ファースト アーキテクチャーにより、オートメーション エンジニアはコードベースのワークフローを通じて Zscaler ソリューションを効率的に導入、管理できるようになります。

Zscaler は OneAPI を開発することで API ファースト戦略を強化し、より優れたセキュリティ機能を提供するとともに、オートメーション エンジニアの運用効率をさらに向上させます。



Zscaler OneAPI

Zscaler OneAPI は、Zscaler プラットフォーム用の単一のプログラミング インターフェイスです。このシンプルなアプローチにより、Zscaler ソリューションの導入、展開、保守が迅速化されます。OneAPI によって自動化が新たな IT 管理者になるため、アイデンティティー管理、監査、可視化、変更制御といった複数の機能を API クライアントが利用できるようになります。

グローバルに展開された Zscaler OneAPI は、分散型のクラウド ネイティブ プラットフォームを使用することで、低遅延と高可用性を実現します。API コールはデータ主権に関する要件を順守しながら、最も近いデータセンターまたはリージョンにルーティングされます。

©2025 Zscaler, Inc. All rights reserved.

OAuth 2.0

API クライアントは、大まかな粒度ときめ細かな粒度の両方のロールベース アクセス制御 (RBAC) をサポートする OAuth 2.0 標準を使用して認証および承認されます。これらの制御により、セキュリティ部門は自動化に対して、人間の管理者と同じ責任基準を適用できます。すべての API コールは、API クライアントのアイデンティティーでログに記録され、完了するまで追跡されます。すべてのアクティビティーは監査でき、人間のユーザーと同様に API クライアントに対して行動制限を適用することも可能です。

ZIdentity の API クライアント

OneAPI は、Zscaler の ZIdentity を統合したアイデンティティー プラットフォームを利用し、API クライアントのアイデンティティー登録と継続的な管理を行います。ZIdentity をすでに使用する組織は、API クライアントを個別にアクティベーションしたりプロビジョニングしたりする必要はなく、人間のユーザーと同じように構成できます。ZIdentity は、API クライアントに許可されるスコープを決定する中心的な機関として機能し、これらのスコープはいつでも調整できます。監査ログとリクエスト ID はシステム全体で追跡および記録されるため、システムは完全な可視性と制御を確保できます。

Zscaler Zero Trust Automation を導入すべき理由

	問題：	Zscaler の解決策：
スピードとスケーラビリティーの課題	▪ セキュリティ インシデントや規制により、ゼロトラストの迅速な導入が必要 ▪ 購入から導入までの時間が非常に長い ▪ M&A に伴う組織の迅速な統合 ▪ フランチャイズや支社への展開が必要	▪ 異なる製品間での反復的な手順を削減 ▪ テンプレートの使用で、特定のニーズに合わせて実装を迅速化
複雑さの課題	▪ ポイント製品やポイント ソリューションによって管理が複雑化 ▪ 複雑さによってセキュリティ ギャップのリスクが増大 ▪ 個人や部門間で責任が分離されていないため、セキュリティ部門に責任が集中	▪ 新しいフレームワークを活用して、複数の部門でポリシー策定の責任を共有 ▪ API に RBAC を実装 ▪ ポリシーと例外に対する責任を共有 ▪ ビジネス部門とアプリ開発者が必要なセキュリティ ポリシーを作成できるようにすることで、セキュリティ部門の負荷を軽減
リソースの最適化	▪ タイプミス、テストのエラー、更新時のミスといったヒューマンエラーのリスク ▪ (インターネット アクセスの中断) ▪ 単調な作業により従業員の職務満足度が低下 十分に活用されていない高額な人材	▪ 展開前のコード レビューを実施 ▪ ロール バックが必要な場合に備えてコードに復元ポイントを提供 ▪ 防御の最前線として自動化を有効化 (事前予防的な対応、例：UEBA アラートが再認証し、サンドボックスを実行) ▪ エンジニアがより挑戦的でやりがいのある仕事に集中できる環境を構築

©2025 Zscaler, Inc. All rights reserved.

Zscaler OneAPI は自動化を管理者にすることで、導入や統合にかかる時間を短縮し、ヒューマン エラーの可能性を減らすと同時に、組織のセキュリティを強化します。OneAPI は、マイクロセグメンテーションの実装、環境の監査、担当部門の投資収益率の最適化などの強力な機能を提供します。

OneAPI による Zscaler プラットフォームの自動化の詳細は、zscaler.jp にアクセスするか、Zscaler アカウント チームにご相談ください。
エンジニア向けの詳細は、次のヘルプ サイトをご覧ください：https://help.zscaler.com/ja/oneapi

zscaler™ | Experience your world, secured.™

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 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 SASE 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™、Zero Trust Exchange™、Zscaler Internet Access™、ZIA™、Zscaler Private Access™、ZPA™、**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