# 全てのユーザー、アプリケーション、ロケーションを網羅するクラウドベースのセキュアアクセス

## Silver PeakとZscalerにより、ゼロタッチプロビジョニングでユーザー、アプリケーション、デバイス、ロケーションを問わず、セキュリティポリシーの適用を自動化

### クラウドファーストセキュリティの課題

**予測不能なアプリケーションパフォーマンス**
トラフィックの優先順位付けや、ビジネスドリブンのセキュリティポリシーの適用機能の欠如により、アプリケーションパフォーマンスが低下してしまいます

**時間を要し、ミスを招きやすいポリシー構成により実装が遅延**
常に変化するクラウドアプリケーションは、各ロケーションでルータやファイアウォールの手動による継続的な再構成が必要となります

**一貫性のないポリシー適用**
膨大なサイト数を横断したセキュリティポリシー定義を一貫して維持することは、非常に大変な作業になります

### ソリューションメリット

**ビジネスクリティカルなアプリケーションへの迅速かつセキュアなアクセス**
ビジネスクリティカルなアプリケーションを優先することにより、最高品質のユーザーエクスペリエンスを提供します

**新たなサイトやアプリケーションの実装を加速**
一元化されたポリシー定義や真のゼロタッチプロビジョニングにより、新たな支社の立上げやアプリケーションの実装を加速させ、M&Aの迅速な進行を可能にします

**全てのユーザーに対して一貫したビジネスおよびセキュリティポリシーを世界規模で適用**
セキュリティおよびクラウドアプリケーションの自動アップデートにより、全てのロケーションを横断した最適なネットワークとセキュリティポリシー適用を実現します

## 概要

アプリケーションがクラウドに移行し続けていることで、トラフィックパターンが変化してきており、新たなWAN（広域ネットワーク）アプローチおよびセキュリティモデルが求められています。全てのアプリケーションが企業のデータセンターでホスティングされていた時代では、支社からのトラフィックはMPLS回線を使用して全てデータセンターにバックホールされ、セキュリティサービススタック全般がデータセンターの出口ポイントで実行されていたため、支社では基本的なセキュリティサービスで十分足りていました。

今日の最先端企業では、データセンター、パブリックあるいはプライベートクラウドなど、あらゆる場所でアプリケーションがホスティングされており、あるいは無数のSaaS（サービスとしてのソフトウェア）プロバイダより提供を受けています。ユーザーは場所やデバイスを問わず、ブローバンドインターネットを含め多様なWANトランスポートを通じてアプリケーションにアクセスしているため、セキュリティモデルやITの課題が複雑化しています。さらにIoTデバイスの拡大もセキュリティの課題の増加に拍車をかけています。

また、企業のセキュリティ境界の分散も攻撃サーフェスの増加につながっており、企業を脅威から保護するための高度なセキュリティサービスに対するニーズが大幅に高まっているのが現状です。

企業が各支社で次世代ファイアウォールを実装する方法もありますが、こうしたモデルは維持するのが困難だと言えます。ハードウェアは非常に高価で、専用のセキュリティアプライアンスをそれぞれの支社に実装し、管理するにも多くのIT人材が必要になります。さらに、支社からのアプリケーショントラフィックには、サンドボックス、侵入防止（IPS）、データロス防止、SSLインスペクションなど、脅威や脆弱性から企業を守るには高度なセキュリティコントロールが求められます。

こうしたセキュリティやコストの問題に対応するために、Zscaler™ などが提供する一元的にオーケストレートされたクラウドホスト型セキュリティサービスが台頭し、急成長を続けています。アプリケーションアウェアかつビジネスドリブンのSilver Peak Unity EdgeConnect™ SD-WANエッジプラットフォームに補完された Zscaler Cloud Security Platformでは、強力なセキュアアクセスサービスエッジ（SASE）ソリューションを提供しており、企業を脅威から保護し、コストを抑制しつつ最高レベルのアプリケーションパフォーマンスとユーザーエクスペリエンスを実現します。

## アプリケーションのクラウドへの移行により、WANとセキュリティのトランスフォーメーションを促進

企業はアプリケーションをクラウドに移行する際にいくつかの課題に直面します。最高レベルのパフォーマンスを実現するためには、ユーザーはクラウドホスト型およびSaaSアプリケーションにインターネット上からダイレクトに接続するべきです。しかしながら、これにより支社における攻撃サーフェスが増加してしまい、強力なセキュリティ対策を施さない限り、企業を脅威と脆弱性に晒すことになってしまいます。

ルータや個々のファイアウォールに基づくデバイス中心モデルは、ハブ＆スポークアーキテクチャを採用しており、全てのインターネット宛トラフィックを本社にバックホールし、次世代ファイアウォールによって検査されています。このバックホールは高価なMPLS帯域を消費し、遅延をもたらすとともにアプリケーションパフォーマンスを損ねることになります。代替策として、企業は次世代ファイアウォールを各支社に実装することもできますが、ITをさらに複雑化し、コストも高騰してしまいます。

## クラウドファーストITセキュリティの課題

**場所やデバイスを問わず業務をこなせるWAN：**クラウドファースト戦略を実行する上で、IT部門は新たなセキュリティの課題に直面します。ユーザーは支社のみならず、自宅、ホテル、喫茶店などあらゆる場所からクラウドおよびSaaSアプリケーションにアクセスします。さらにIoTデバイスの急増もセキュリティを困難なものにしています。こうした課題に対応するには、企業はユーザーがいる場所に関係なく同等のセキュリティサービスソリューションを提供し、接続環境を問わず全てのユーザーに対して高速かつセキュアなエクスペリエンスを提供する必要があります。

**全てのアプリケーションは同質ではない：**VoIPなどのSaaSサービスは、ジッター（送信遅延の揺らぎ）に敏感で堅牢なセキュリティ対策が施されているため、企業にとってリスクはさほどありません。ユーザーをこのようなアプリケーションにダイレクトに接続することで最善のユーザーエクスペリエンスを提供することができます。しかしながら、その他のクラウドあるいはWebベースのアプリケーションは、さほどセキュアではなく、企業を脅威に晒すか知的財産（IP）の漏洩をもたらし、より高度なセキュリティインスペクションが必要かもしれません。例えば、従業員が不注意で、または悪意を持ってFacebookのメッセージで企業の知的財産を転送してしまうかもしれません。あるいは、企業ポリシーで全てのトラフィックにSSLインスペクションまたはユーザー認証を適用しているにもかかわらず、ゲストWi-Fiトラフィックだけが除外されているかもしれません。こうした例外対策は自動的かつ一貫して漏れなく企業全体にわたり適用し、企業ネットワークのセキュリティを確保し、感染を防ぐ必要があります。IT部門はビジネス要件に沿って、または意図的にアプリケーション、ユーザー、ロケーション、デバイスに基づき、きめ細かなセキュリティポリシーをサポートしなければなりません。

**アプリケーションと脆弱性は常に変化する：**SaaSアプリケーションの定義やアクセスするためのIPアドレスのレンジは常に変化しており、特にMicrosoft Office 365などの著名なSaaSアプリケーションや、RingCentralなどのUCaaSアプリケーション、またはFacebookやInstagramなどの娯楽アプリはなおさらです。現在、企業のセキュリティを脅かす新たな脅威が日々100万件近く発見されています[1]。そこでWANおよびセキュリティは継続的に適応していく必要がありますが、これを自動化することでIT部門は頻繁な変更にも対応することができ、

[1] https://www.webarxsecurity.com/website-hacking-statistics-2018-february/

ビジネスクリティカルなアプリケーションにセキュアかつ途切れのないアクセスを提供することが可能になります。

**新たな支社の立上げとアプリケーションの迅速な実装：**今日のグローバルマーケットで競争優位性を保つためには、IT部門は新たなアプリケーションの実装と新規サイトのオンライン化を迅速に行う必要があります。ルータ、個別のファイアウォール、そしてMPLS接続に基づく従来のWANモデルで新規サイトを立ち上げる場合、一般的には3ヵ月以上の期間を要します。他の企業を買収するしないにかかわらず、ビジネスの成長に合わせ、アプリケーションの要件を満たすためには、企業は新たなWANおよびセキュリティサービスをゼロタッチプロビジョニングにより実装を自動化する能力が求められています。

**WANパフォーマンスとセキュリティの課題を解決：**クラウドが普及し、アクティブWANトランスポートとしてブロードバンドインターネットや4G/LTEサービスの利用が増加する中で、IT部門はセキュリティ、ネットワーク、アプリケーションパフォーマンスの課題解決がさらに困難になっています。それでも常時接続やハイパフォーマンスのアプリケーションに対するエンドユーザーの期待はこれまで以上に高まっています、企業のIT部門は迅速なトラブルシューティングを可能にするツールを活用することで、ビジネスへの対応力を向上させる必要があります。

こうした課題を解決するにはWANおよびWANセキュリティインフラモデルの再構築が必要となります。

## クラウドファーストの時代に即したSASE

デジタルトランスフォーメーションは、アプリケーションのデータセンターからクラウドへの移行を促し、従来のネットワークとセキュリティのアーキテクチャを時代遅れのものにしました。ガートナーは、こうした新たなパラダイムに対応するために設計された製品／サービスを表すSASE（セキュアアクセスサービスエッジ）という言葉を生み出しました。WAN機能を、セキュリティWebゲートウェイ（SWG）、クラウドアクセスセキュリティブローカー（CASB）、FWaaS（サービスとしてのファイアウォール）、そしてゼロトラストネットワークアクセス（ZTNA）といった総合的なネットワークセキュリティ機能と統合することにより、デジタルトランスフォーメーションに求められるダイナミックなセキュアアクセスをサポートすることが可能になります。SASEの主要な設計原理は、支社からかさばるハードウェアを取り除き、WAN管理や包括的なセキュリティサービススタックを含むクラウドネイティブサービスに移行させることにあります。このようなアーキテクチャにより、パフォーマンス、可用性、アジリティ、そしてコストのバランスを取ることが可能になります。

Silver PeakとZscalerは、それぞれWANエッジとセキュリティインフラソリューションのリーダーであり、今日のクラウドファーストの企業が直面する新たなビジネスニーズに独自に対応するSASEアーキテクチャを提供します。

## Silver PeakとZscalerで実現するセキュアWANアクセス

Zscaler Internet Access™ などのクラウドホスト型セキュリティサービスは、クラウドファースト企業向けに従来とは異なる優れたセキュリティを提供するために誕生しました。Zscalerでは集中管理の下、次世代ファイアウォール、アクセスコントロール、IPS、サンドボックス、UTM、URLフィルタリング、DLP、CASB、リモートブラウザ分離など、包括的なセキュリティスタックをサポートしており、全てのユーザーに対して均一のプロテクション機能と一貫したポリシー適用を膨大なサイトを横断して提供しています。また、物理的なセキュリティアプライアンスの購入、実装、管理は不要となっています。

クラウドホスト型セキュリティサービスとアプリケーションアウェアでビジネスドリブンのEdgeConnectプラットフォームを組合せることにより、支社のWANエッジインフラを合理化することができます。企業はもはや各支社に高価で管理が複雑な次世代ファイアウォールを実装する必要がなくなります。

**きめ細かいセキュリティポリシー適用：**Silver Peak First-packet iQ™ アプリケーション認識機能により、インテリジェントなきめ細かいトラフィック操作が可能になります。これに、業務目的に沿ったきめ細かなセキュリティポリシー適用を加えることで、全てのアプリケーションの最高レベルのパフォーマンスを提供しつつ、組織の安全を守ることができます。例えば、以下のようなビジネスドリブンのセキュリティポリシーを適用することができます：

1. 企業のデータセンターでホスティングされているアプリケーショントラフィックをダイレクトに本社に送信
2. UCaaSトラフィックのみをプロバイダのクラウドサービスに送信
3. プロバイダのクラウドまたはWebサービスに送信する前に、Salesforce、Facebook、YouTube、Box、Webブラウズトラフィックなどのインターネット宛トラフィックを、全てZscalerのクラウドPOPに送信してインスペクションを実行

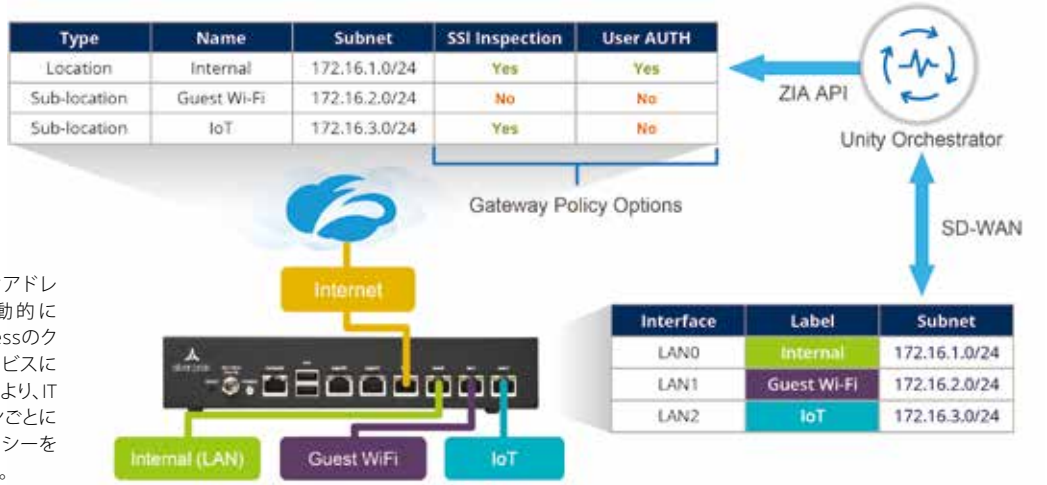


図1：サブロケーションアドレスとサブネットが自動的にZscaler Internet Accessのクラウドセキュリティサービスにマッピングされることにより、IT部門でサブロケーションごとに独自のセキュリティポリシーを定義することができます。

**アプリケーション、ユーザー、デバイスレベルでコントロール：**Silver PeakとZscaler APIの連携により、IT部門はZscalerの一連のセキュリティポリシーを各支社に適用することができます。また状況により、支社内の特定のアプリケーション、ユーザー、デバイスごとに異なるセキュリティポリシー適用が必要になる場合、ゲートウェイオプション機能により、サブロケーションに例外を定義することが可能になります（図1参照）。さらに以下のようなポリシーを定義することができます：

1. 企業のトラフィックにSSLインスペクションを適用
2. ネットワークにアクセスするIoTデバイスにSSLインスペクションを適用（ユーザー認証は実行しない）
3. ゲストWi-Fiアクセスはプライバシーの問題上SSLインスペクションは適用しない

**集中管理：**Silver PeakとZscalerの連携ソリューションは支社のWANインフラをシンプル化するだけでなく、集中管理を可能にします。真のゼロタッチプロビジョニングにより、ゲートウェイオプションやロケーション／サブロケーションルールを含む、全てのポリシーを一度に定義し、全サイトに自動的に適用することができます。これにより、僅か数分で膨大な数のサイトに新たなポリシーを実装することが可能になります。新たなサイトのオンライン化またはポリシーの変更やアップデートも同様に容易に行うことができます。一元管理のポリシー構成とアドミニストレーションにより、個別のファイアウォール設置モデルで必要となるデバイスごとの構成が不要となり、人為的ミスも最小限に止めることが可能になります。結果として、きめ細かいエンドツーエンドのセキュリティポリシー適用を実現することができます。

**立上げを完全に自動化：**Silver PeakとZscalerは、クラウドセキュリティサービスの立上げをシンプル化するために提携しました。EdgeConnect SD-WANアプライアンスと近接型のZscaler Enforcement Node（ZEN）PoP間のIPsecトンネル構成を完全に自動化することで、各支社での時間のかかる手作業によるIPsecトンネルの定義を排除することができます。Zscalerポータルのロケーション情報は、Silver Peak Unity Orchestrator™ から「学習」し、最寄りのプライマリおよびバックアップのZEN PoPと支社を接続するために活用されます（図2参照）。

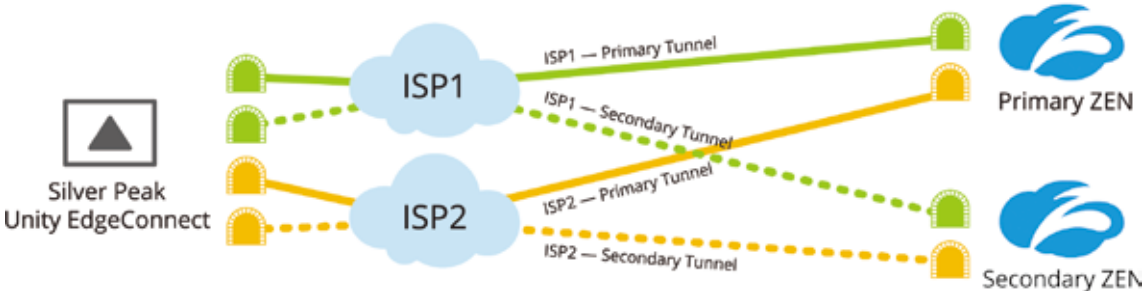


図2：一貫した最適パスの選定により、最高レベルのSaaS品質と99.999%の可用性を実現

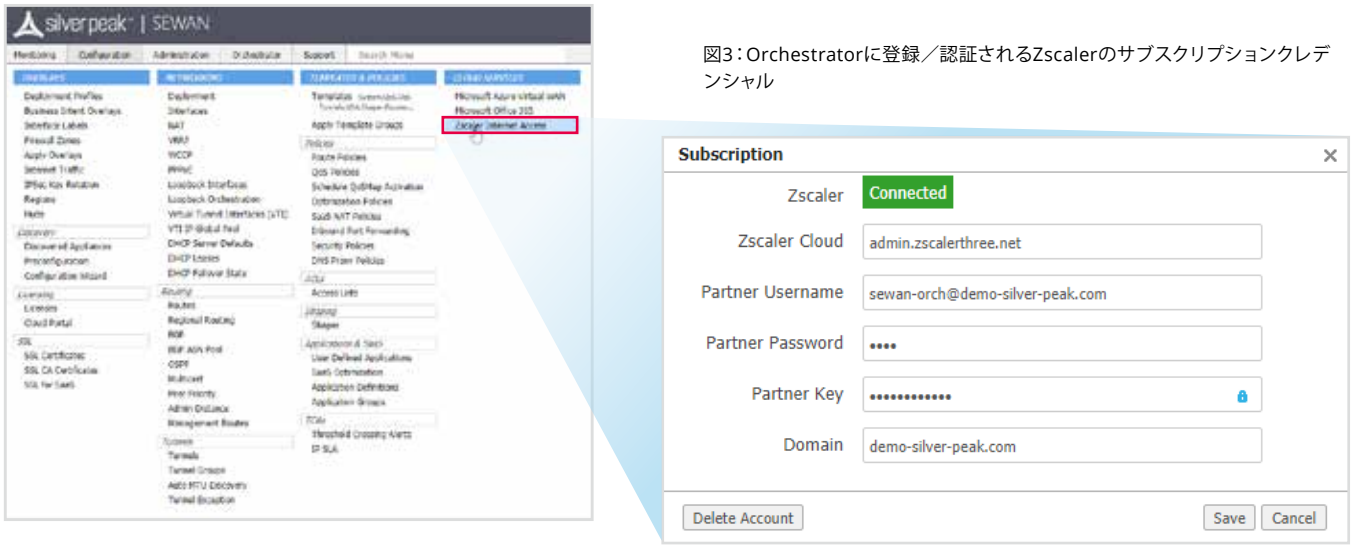


図3：Orchestratorに登録／認証されるZscalerのサブスクリプションクレデンシャル

Unity OrchestratorコンソールからZscalerのサブスクリプションクレデンシャル（図3参照）を認証し、ZEN PoPに接続する支社を選択します。次にOrchestratorが各支社と最寄りのプライマリ／セカンダリZEN PoPとの間で、プライマリおよび任意のセカンダリIPsecトンネルを自動で構成することにより、最高品質レベルのクラウドアプリケーションパフォーマンスを提供することができます。各EdgeConnectアプライアンスが備えるIP SLAエンジンが継続的に全てのIPsecトンネルのヘルス状態を監視します。ヘルスチェックでは各ZEN PoPにおける特定のテストポイントの状態を測定し、必要に応じてバックアップノードにトラフィックを自動的にリダイレクトします。また、新たなZEN PoPが支社の近くで有効になった場合、トンネル構成が自動でアップデートされることにより、Silver Peak/Zscalerソリューションで一貫した適応が可能となり、ユーザーに常に最善のアプリケーションパフォーマンスを提供することができます。

次にZscaler ZEN PoPに転送するアプリケーショントラフィックの取扱いポリシーを選択し、適切なプライマリ／セカンダリトラフィックを構成画面に「ドラッグ＆ドロップ」します（図4参照）。一般的に、UCaaSなどのホワイトリストのトラフィックを除く全てのインターネット宛トラフィックがこれ該当します。以降のポリシー変更はOrchestratorで容易にアップデートして全てのロケーションに展開することができます。

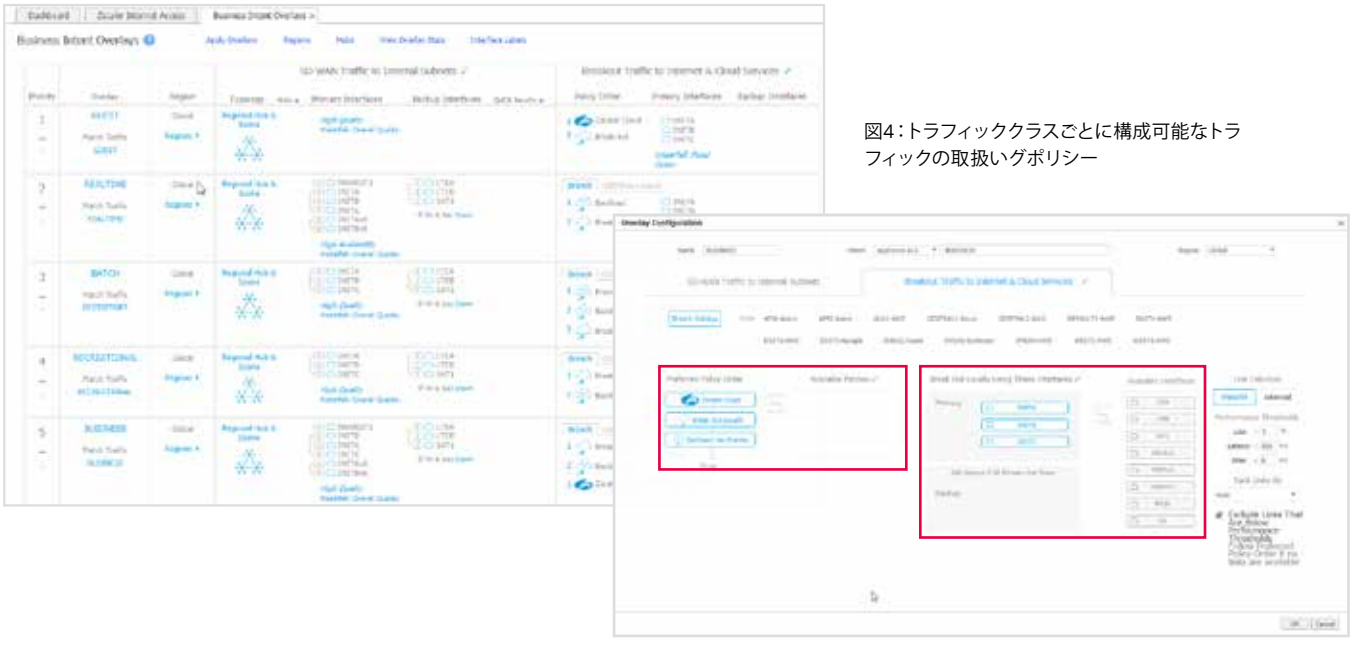

図4：トラフィッククラスごとに構成可能なトラフィックの取扱いグポリシー

Silver Peakは、Zscaler APIを活用してSD-WANファブリック内の支社を最寄りのプライマリ／任意のセカンダリZEN PoPに接続するためのプロセスを連携／自動化しています。この連携により、多くのサイトが数分で自動的に接続されるため、IT運用コストを劇的に節約することができます（図5参照）。また、SD-WANを横断する一貫したポリシー適用といった付加価値ももたらし、企業を脅威や脆弱性から保護します。

支社を保護するIPsecトンネルの確立の全自動化に加えて、Silver Peak/Zscalerソリューションは、インターネット宛トラフィックにギガビットスピードの帯域幅を必要とする、主要な支社をサポートする柔軟性も持ち合わせています。Orchestratorで一元的に構成し、これらのロケーションと最寄りのプライマリ／セカンダリZEN PoP間のGREトンネルを監視します。

## Silver Peak + Zscaler = 優れたビジネス成果

Silver Peak self-driving wide area network™（自律型WAN）プラットフォームとZscaler Cloud Security Platformにより、クラウドとダイレクトにつながる支社のプロビジョニングとセキュリティ保護を僅か数分で完了させることができます。最終的に、迅速な実装、最適なパフォーマンス、そしてクラウドアプリケーションにおける最高レベルのエンドユーザーエクスペリエンス、および常時変動する業務要件に一貫して適応するセキュアなSD-WAN接続がもたらされることで、企業は既存および将来的なクラウドへの投資から多くの効果を期待することができます。これにより、IT部門のコスト削減と運用のシンプル化につながります。また、エンドユーザーは必要とするビジネスクリティカルなアプリケーションへの高速、安全、そして途切れのないアクセスが可能になります。

- クラウドのメリットを存分に生かすセキュアアクセスサービスエッジ（SASE）アーキテクチャを提供することでビジネスのアジリティとITのシンプル化を実現します
- 支社のWANとセキュリティインフラを合理化し、個別のルータや次世代ファイアウォール、そして無数のオンプレミスデバイスを不要にしつつ、社外勤務が当たり前になった世界でセキュリティの向上を図ることができます
- 99.999%の可用性でビジネスクリティカルなアプリケーションに高速かつ安全にアクセスすることが可能となり、業務の全般的な生産性とユーザーエクスペリエンスの向上を可能にします

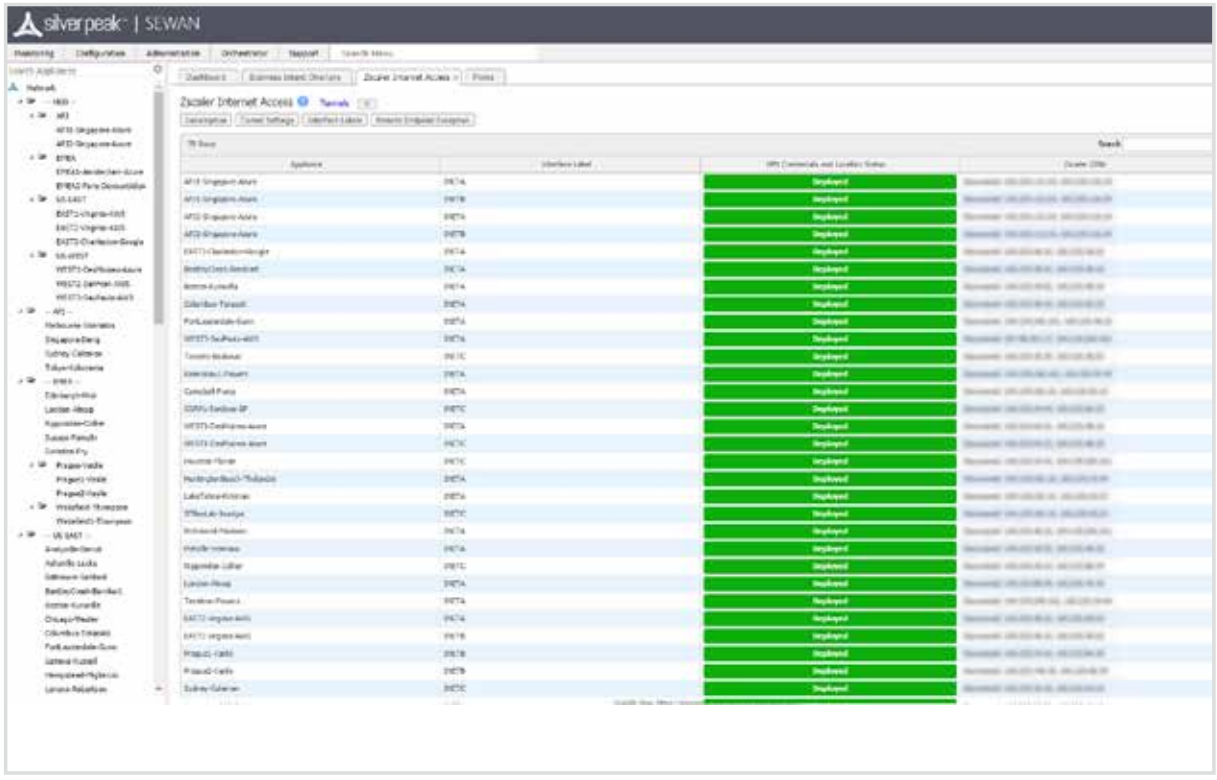


図5：数分で各SD-WAN支社が最寄りのZscaler ZEN PoPに自動的に接続

- 自動化された実装と真のゼロタッチプロビジョニングにより迅速かつ安全に新たな支社を立ち上げることで、ビジネスアジリティの向上と売上の加速を実現します
- 容易な変更、人為的ミスの削減、迅速なトラブルシューティングにより、IT部門のビジネスへの対応能力を強化することができます
- セキュリティ要件を一度に集中的に定義するだけで、全ての従業員、ゲスト、デバイス、ロケーションに対して最適なセキュリティを自動的に提供することができます
- 業務要件に応じてカスタマイズされたきめ細かいネットワークおよびセキュリティポリシーにより、リスクを最小限に止めることが可能になります
- ネットワークおよびアプリケーションのトラブルシューティング、並びに日常的なフィールドサポート／ヘルプデスクコールに要する時間を短縮することができます
- 高価なMPLSサービスへの依存度を最小限に止め、コスト高なセキュリティアプライアンスを排除することができます
- WANとセキュリティを刷新し、より優れたパフォーマンス、信頼性、コントロール、経済性により、クラウドへの投資から多くの効果を得ることが可能になります

## Zscalerについて

Zscalerにより、組織はモバイル／クラウドファーストの時代に合わせて、ネットワークとアプリケーションを安全に利用することが可能になります。Zscalerのクラウドデリバリサービスでは、包括的な脅威対策機能と高速なユーザーエクスペリエンスを提供しつつ、デバイス、ロケーション、ネットワークを問わず、ユーザーをアプリケーションやクラウドサービスにセキュアに接続することができます。コスト高な複雑なゲートウェイアプライアンスは不要です。詳細はzscaler.comまたはTwitter @zscalerをご覧下さい。

## Silver Peakについて

Silver PeakはSD-WANのグローバルリーダーとして、クラウドおよびデジタルトランスフォーメーションへの投資から最大限の価値を引き出し、最新のWAN構築を実現するネットワーキングソフトウェアを提供しています。Unity EdgeConnect SD-WANエッジプラットフォームでは自律型のWANを提供し、ビジネスニーズに適応するために継続的に学習することで、企業ユーザーやIT部門に最高品質のエクスペリエンスをもたらします。EdgeConnectプラットフォームは従来のルータを不要とし、SD-WAN、ファイアウォール、セグメンテーション、ルーティング、WAN最適化、そしてアプリケーションの可視化とコントロールを1つの一元管理プラットフォームに集約しています。EdgeConnect SD-WANエッジプラットフォームは、これまで世界100ヵ国以上で2,000社超のグローバル企業に導入されています。


**企業名**

Silver Peak Systems 合同会社
〒 150-8512
東京都渋谷区桜丘町 26-1
セルリアンタワー 15 階

**電話番号**

TEL：03-5456-5049

**オンライン**

Eメール：info@silver-peak.com
Webサイト：www.silver-peak.com





SP-SB-SECURE-SD-WAN-WITH-ZSCALER-JP-051820