RISE with SAP 向け Zscaler Private Access (ZPA)

RISE with SAP 環境でネイティブに利用可能な
業界初かつ唯一のゼロトラスト アクセス ソリューション

ソリューションの概要

市場の課題

SAP製品は、財務、会計、販売、サプライ チェーン、調達、製造、人事などの領域にわたるビジネスの中核プロセスの管理を支援しています。複数の部門にわたってデータを一元化し、ビジネス情報やプロセス管理を合理化することを目的として設計されており、組織の円滑な運営を可能にしています。

ビジネス上の重要な機能を担っているため、SAPソリューションには知的財産、財務記録、個人データ、サプライ チェーン情報などの機密性の高いビジネスデータが含まれています。その結果、データの暗号化、身代金の要求、業務の妨害を目論むサイバー犯罪者やスパイ集団、ハクティビストから価値の高いターゲットと見なされています。

SAPシステムが侵害されると、業務が完全に停止し、生産、財務報告、サービス提供が妨げられ、重大な財務損失、企業イメージの低下、規制違反による罰金につながる可能性があります。

従来、SAPシステムへのアクセスは、オフィス内から標準的なマルチプロトコル ラベル スイッチング(MPLS)ネットワークを通じて行われていました。しかし、クラウドの採用とハイブリッド ワークの台頭により、現在ほとんどの組織では仮想プライベートネットワーク(VPN)を介してリモート ユーザーがこれらのシステムにアクセスできるようにしています。

残念ながら、従来のネットワーク中心のアクセス アプローチは、設計上安全ではありません。攻撃対象領域が大幅に増加し、アプリケーションやデータが侵入や侵害を受けやすくなることが知られているほか、SAPユーザーと業務に不可欠なSAPシステムの間でフェイルセーフな接続を確保するうえでは信頼性に欠け、適切とはいえません。

現在、オンプレミスのSAPシステムを運用している組織には、厳しいタイムリミットがあり、SAP ECCは2027年までにサポート終了となる予定です。言うまでもありませんが、ITリーダーやビジネス リーダーにとっては、入念な計画を行ったうえで従来のSAPシステムからRISE with SAPなどのクラウドベースのS/4HANAに移行することが急務となっています。

SAPの移行とビジネス トランスフォーメーションを安全に実現するためには、ユーザーとアプリを直接接続するゼロトラスト アーキテクチャーに基づくセキュアアクセス テクノロジーを採用し、アクセス手法を最新化することを検討する必要もあります。このようなアプローチは、セキュリティ リスクの軽減、運用の複雑さの排除、ネットワーク中心のVPNに関連するパフォーマンスのボトルネック解消に効果を発揮します。

RISE with SAP 向け Zscaler Private Access (ZPA)

Zscaler Private Access™ (ZPA) を利用することで、組織が移行のどの段階にあっても、すべての SAP アプリケーションへのアクセスを効率化できます。画期的な新しい統合の一環として、Zscaler は RISE with SAP 環境内でゼロトラスト アクセス サービスをネイティブに統合する唯一のサイバーセキュリティ ベンダーとして SAP に認定されました。

これは、SAP のお客様の RISE クラウド環境内で ZPA をネイティブにプロビジョニングし、各種基準に完全に準拠したゼロトラスト接続を提供することで実現されています。SAP でホストされ、ネイティブに統合された ZPA サービスは、Zscaler Zero Trust Exchange™ へのアウトバウンド接続を作成し、従業員とパートナーの両方にユーザーからアプリへの直接アクセスを提供します。

ZPA は、独自のインサイドアウト接続モデルに従って、ユーザーと SAP アプリケーション間でポリシーベースの排他的な接続を動的に仲介します。さらに、Zero Trust Exchange の統合データ保護機能によって、RISE with SAP のお客様は重要な SAP データを保護し、GDPR、HIPAA などのさまざまな規制基準を確実に順守できます。

主なポイント

- **RISE with SAP へのクラウド移行中のアクセスの合理化：**ZPA は、RISE with SAP への移行中に SAP アプリへの一貫したユーザー アクセスを提供します。
- **VPN を使用しないセキュア リモート アクセス：**この統合により、VPN を使用せずにあらゆる場所の従業員やパートナーに SAP への安全な接続を提供できます。
- **ユーザーとアプリのセグメンテーション：**ユーザーのアクセス パターンに基づいて、アプリのセグメンテーションに関する推奨事項を自動生成し、ゼロトラストの原則に基づいてユーザーとアプリ間できめ細かいアクセス ポリシーを施行します。
- **完全なインライン トラフィック検査と情報漏洩防止：**SAP アプリケーションのペイロード全体にインラインでセキュリティ検査を実行し、既知および未知の脅威を特定、ブロックするとともに、業務に不可欠なデータを保護します。

この統合の細かい意味合いについて理解を深めるには、その固有の特性を掘り下げ、RISE with SAP についても知る必要があります。

RISE with SAP の概要

RISE with SAP は、SAP のサブスクリプションベースの Business Transformation as a Service (BTaaS) パッケージで、従来のオンプレミスの ERP ソリューションからクラウドベースの ERP ソリューションへの移行を簡素化します。完全管理型の移行サポートに加え、包括的なインフラ、テクニカル サポート、トランスフォーメーション ツールを組織に提供しています。

組織は RISE を利用することで、AWS や GCP、Azure などのハイパースケーラーでホストされるクラウド ERP ソリューションである SAP S/4HANA のプライベート クラウド エディション (PCE) に SAP ECC を移行します。サブスクリプションには、SAP の技術管理サービスが含まれています。RISE のお客様は、SAP が管理するインフラとサービスを利用しながら、ERP の構成とアップグレードの制御を維持できます。

RISE with SAP との統合における Zscaler 独自の強み

Zscaler は、特に RISE with SAP の移行において、他のセキュア リモート アクセス ソリューションとは異なり、ZPA Application Connector を RISE クラウド内でネイティブに直接プロビジョニングすることで価値を提供します。

ゼロトラスト アクセスの機能を RISE with SAP 内に直接プロビジョニングする革新的なアプローチにより、基盤となる OS への依存やハードウェアの仮想化の必要性を排除しながら、ユーザーとアプリ間でポリシーベースの安全な接続を実現します。

RISE with SAP 向け ZPA は、増減するハイブリッド ワークの需要の変動に合わせて動的に拡張できます。ZPA のクラウド ネイティブなプロビジョニングによって、Kubernetes などのオーケストレーション ツールのメリットを活用しながら、リソース使用率や自己修復機能を改善し、運用負荷を削減することが可能です。

ZPA は、従来のネットワーク アクセスのアプローチに頼ることなく、あらゆる SAP アプリケーションへのゼロトラスト アクセスを実現します。S/4HANA への移行時にもシームレスに動作し、RISE with SAP では独自の機能を提供します。

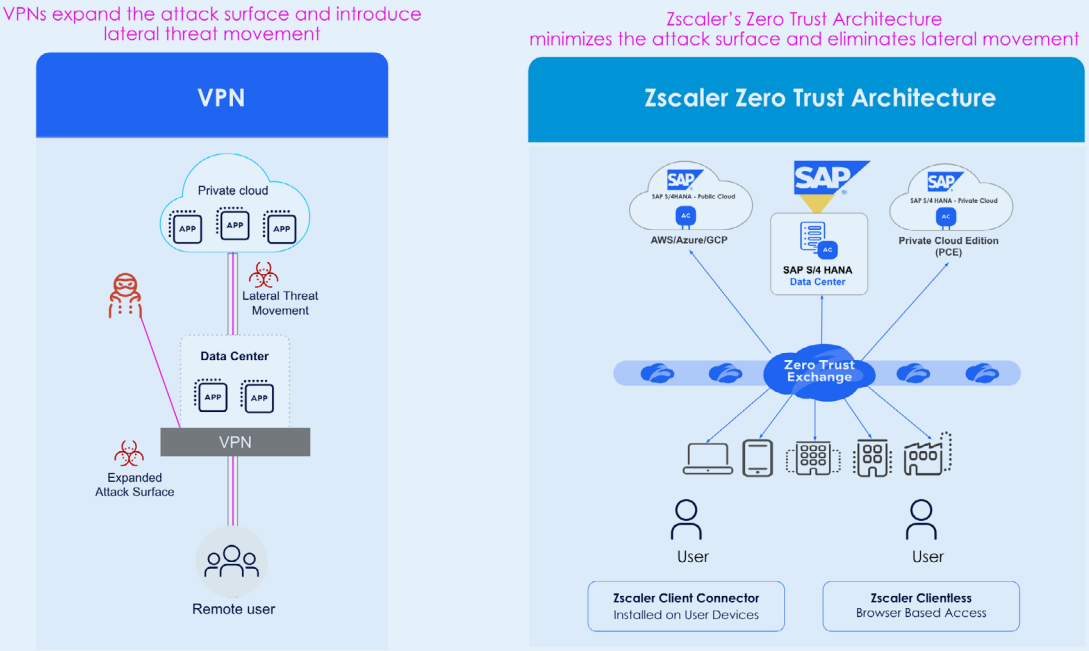

図 1: VPN と Zscaler のゼロトラスト アーキテクチャーの比較

従業員とパートナーのための合理的かつ安全なリモート アクセス

ハイブリッド ワークの台頭により、従業員やユーザーはどこからでも SAP アプリケーションにアクセスできる環境を必要としています。そのため、ユーザーから業務に不可欠な SAP システムへの安全かつ一貫性した接続の重要性がこれまで以上に高まっています。これまで投資してきた SAP から RISE with SAP クラウドへの移行を計画している場合や移行中の場合は、特に重要です。

多くの組織は、接続を確保するために従来のネットワーク アクセスのアプローチに依存しています。しかし、このアプローチは設計上、本質的に安全ではありません。ユーザーは過剰な信頼を付与され、SAP アプリケーションの機密情報も含め、ネットワーク全体に制限なくアクセスできます。また、トラフィックをデータ センターにヘアピンすることで、接続にレイテンシーが発生し、ユーザー エクスペリエンスに悪影響が出る傾向があります。

ZPA は、「決して信頼せず、常に検証する」というゼロトラストの原則に従い、ユーザーのアイデンティティーとデバイスのセキュリティに基づいて特定の SAP アプリケーションへのアクセスのみを提供し、VPN などの従来のネットワーク アクセスのアプローチに代わって、よりきめ細かい安全な接続を実現します。

ZPA は、独自のインサイドアウト接続モデルに従って、許可された SAP ユーザーと特定の SAP アプリケーションの間でポリシーベースの接続を仲介します。さらに、Zero Trust Exchange のデータ保護機能は、機密情報に対する包括的な可視性と制御を実現し、SAP アプリケーション内の重要なデータの保護と、GDPR、HIPAA などの規制基準の順守において極めて重要な役割を果たします。

SAP 向け ZPA は S/4HANA でシームレスに動作し、ネイティブに展開された SAP の ZPA サービスにより、RISE with SAP でも独自の形で機能します。

従業員向けのクライアントベースのゼロトラスト アクセス

Zscaler は、RISE with SAP 環境内に ZPA Application Connector を直接プロビジョニングする独自の機能を提供します。

ZPA App Connector は、RISE with SAP のお客様のネットワークから Zscaler クラウドへの安全なアウトバウンド接続を提供する、軽量の仮想アプライアンスです。セキュア ゲートウェイとして機能し、Zero Trust Exchange プラットフォームへの暗号化されたアウトバウンド TLS 接続を確立することで、SAP アプリケーションへのアクセスを可能にします。

これにより、ユーザーを SAP アプリケーションに接続するためのインバウンド アクセスやパブリック IP は不要になります。接続のアウトバウンドな性質は、潜在的な脅威にさらされる可能性を最小限に抑えるセキュリティ上の重要な特徴といえます。TLS 接続が確立されると、SAP アプリケーションとユーザー間のすべてのトラフィックがマイクロトンネル化され、トランザクションの安全性とプライバシーが確保されます。

逆に、ユーザーが SAP アプリケーションへのアクセスをリクエストすると、ユーザーのデバイスにインストールされている軽量エージェントである Zscaler Client Connector (ZCC) がそのリクエストを傍受し、Zero Trust Exchange にマイクロトンネルで送信します。Zero Trust Exchange は、ユーザーのリクエストを評価し、RISE with SAP のお客様のセキュリティ ポリシーに従ってユーザーのアイデンティティーとデバイスの状況を検証します。検証後、Zero Trust Exchange が App Connector に指示し、SAP アプリケーションへの安全な接続が確立されます。

ZPA は、特定のユーザーとアプリケーション間でのみトラフィックをルーティングすることで、セキュリティが確保されていない直接接続を防止します。ユーザーとアプリ間のマイクロセグメンテーションを適用することで、各ユーザーのアクセスを他のユーザーから分離し、ゼロトラスト セキュリティ モデルに準拠します。複数のユーザーが同じ SAP アプリケーションにアクセスする場合、トラフィックは暗号化された個々のマイクロトンネルにセグメント化されます。これにより、不正アクセスやネットワーク上でのラテラル ムーブメントが防止され、1 つの接続が侵害されても他のユーザーや SAP アプリケーションに影響が及ぶことはありません。

外部パートナー向けのブラウザーベースのゼロトラスト アクセス

ZPA は、管理対象外デバイスを使用してアクセスしている可能性があるサードパーティー ユーザー、請負業者、SAP ユーザーに対して、SAP アプリケーションへのブラウザーベースのアクセスも提供しています。このようなシナリオでは、ZPA のブラウザーベースのアクセス機能によって、要求された特定の SAP アプリケーションにユーザーを安全に接続します。ユーザーのデバイスに ZCC エージェントをインストールする必要はありません。

ブラウザーベースのオプションで SAP アプリケーションにアクセスする場合のプロセスは以下のとおりです。

1. **ユーザー認証：**ユーザーは、SAP アプリケーションに関連付けられた特定の URL に移動します。ZPA がユーザーを組織のアイデンティティー プロバイダー (IdP) にリダイレクトし、認証を行います。
2. **ポリシーの施行：**認証が成功すると、ZPA はユーザーのアイデンティティーとコンテキストに基づいてアクセス ポリシーを施行し、許可されたユーザーのみが SAP アプリケーションにアクセスできるようにします。
3. **アプリケーションへのアクセス：**ZPA は、S/4HANA でネイティブに展開された App Connector を通じて、ユーザーのブラウザーと要求された SAP アプリケーション間に安全なインサイドアウト接続を確立します。この方法により、アプリケーションがインターネットに対して不可視化された状態が維持され、攻撃対象領域が減少します。

ZPA が提供するブラウザーベースのアクセスは、ネットワーク経由ではなく特定の SAP アプリケーションに直接接続することで、セキュリティを強化し、ネットワーク内でのラテラル ムーブメントのリスクを最小限に抑えます。このアプローチにより、ユーザーはどこからでも業務に不可欠なアプリケーションにシームレスかつ安全にアクセスできます。

内部ユーザーやサードパーティー ユーザーによる SAP の機密データの流出防止

Zero Trust Exchange の統合データ保護機能によって、RISE with SAP のお客様は重要な SAP データを流出から保護し、GDPR、HIPAA などのさまざまな規制基準を確実に順守できます。

さらに、Zscaler のクラウド ブラウザー分離 (CBI) によって、サードパーティーはクラウドでホストされている仮想ブラウザーを介して SAP アプリケーションに安全にアクセスし、安全な視覚コンテンツのみをデバイスにストリーミングできます。読み取り専用アクセスを提供するゼロトラスト ポリシーを適用して、ダウンロード / アップロードを防止し、機密データをマスクし、管理対象外デバイスでコードが実行されないようにします。これにより、ネットワークの公開やデータ流出のリスクを排除しながら、制御された安全なアクセスを実現できます。

主なメリット

従来のネットワーク アクセス ソリューションによって SAP アプリケーションへのリモート アクセスを可能にすると、攻撃対象領域の大幅な増加という課題が生じ、業務に不可欠なアプリが侵害を受けやすくなるとともに、パフォーマンスの低下とレイテンシーの問題も引き起こし、ユーザー エクスペリエンスが低下します。対照的に、ZPA は SAP システムを使用する組織に複数のメリットを提供します。

- **SAP ユーザー (従業員およびパートナー)** は、移行の段階を問わず、あらゆる SAP アプリケーションへの高速かつ安全で信頼性の高いアクセスを利用できます。
- **SAP アプリケーション**へのアクセスはインサイドアウト接続を介して安全に行われるため、アプリケーションがインターネットにさらされることはありません。
- **SAP アプリケーション**を不可視化し、到達不能にすることで、攻撃の影響範囲やラテラル ムーブメントを最小限に抑えます。
- **RISE with SAP のお客様**は、従来のネットワーク アクセス技術への投資に伴うコストと複雑さに対処する必要がなくなります。

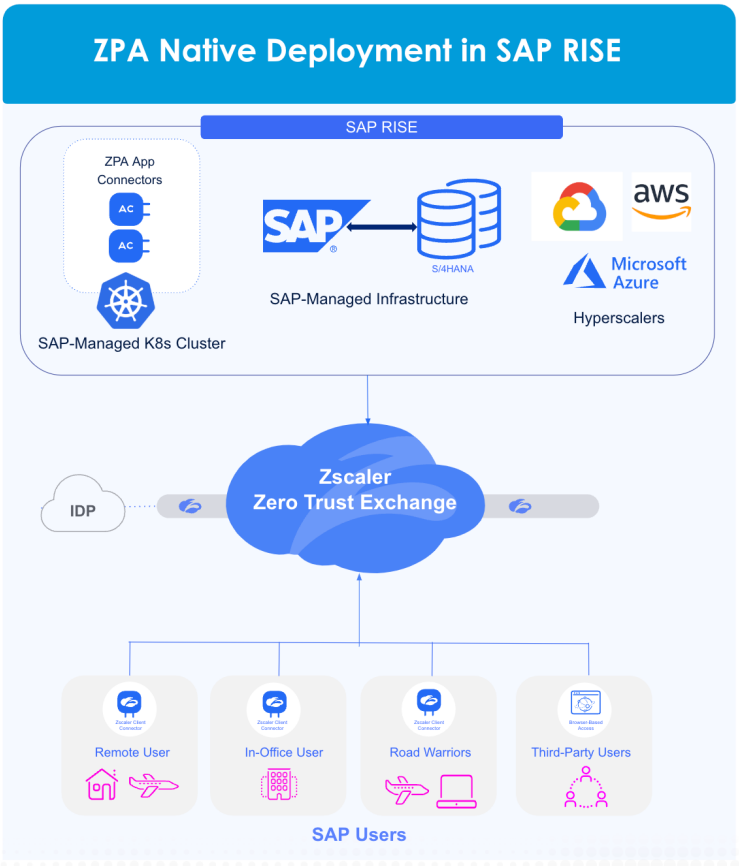

図 2. RISE with SAP 環境にネイティブに展開される ZPA

RISE with SAP 内での ZPA のネイティブな統合

サーバーとネットワークの管理は、仮想化 (通常は仮想マシン [VM] を使用) からコンテナー化 (軽量コンテナーを使用) に移行しています。VM と比較すると、コンテナーは移植性やセキュリティに優れ、管理しやすく、迅速なアプリケーション提供が可能な点で好まれています。

Kubernetes は、最も人気のあるコンテナー オーケストレーション プラットフォームの一つです。これを利用することで、並列依存関係のない分離環境内でアプリケーションを実行できます。SAP のクラウド ERP はクラウド ネイティブで、Kubernetes によってオーケストレーションされます。

SAP のクラウド ネイティブな ERP とのシームレスな統合を可能にするために、ZPA サービスは、RISE のお客様のプライベート クラウド環境で SAP が管理する Kubernetes クラスター内でネイティブに実行できるように設計されています。Zscaler は、この画期的な方法での展開を実現したことで、SAP のお客様の独自のクラウド ネイティブ RISE 環境内から、基準に完全に準拠した形でゼロトラスト アクセスを提供できるようになりました。

SAP でホストされる ZPA App Connector の RISE with SAP 環境での展開

SAP が管理する RISE のお客様専用 Kubernetes (K8s) クラスター：RISE のお客様には、SAP アプリケーション ワークロードとセキュリティに関するお客様固有の要件に合わせて調整された、SAP が管理する専用の K8s クラスターが提供されます。これにより、SAP が管理する K8s クラスター内で ZPA App Connector をプロビジョニングし、RISE with SAP クラウドで実行されている SAP アプリケーションに対して、基準に完全に準拠したゼロトラスト接続を行えるようになります。

SAP が管理するクラウド インフラ：SAP は、Kubernetes クラスターやホスト OS、その他のコンポーネントを含め、クラウド内の基盤インフラ スタックを RISE のお客様に代わって完全に管理します。また、高可用性、稼働時間、レジリエンスを確保し、自動でのディザスター リカバリーを可能にするための技術メンテナンス サービスを提供します。

RISE with SAP のお客様が制御する ZPA テナント：RISE のお客様は、インフラ管理を SAP に任せつつも、Zscaler Cloud Admin Portal を介して ZPA テナントを完全に制御できます。このポータルから、組織固有のセキュリティ要件に基づいて、ユーザー管理とセキュア アクセス ポリシー、そしセキュリティ基準の設定を行えます。

Zscaler ZPA-CS サービスの共有責任モデル：
現在の RISE with SAP のお客様が Zscaler ZPA-CS サービスを使用するには、まず SAP からサービスを注文し、次に ZPA App Connector のライセンスとプロビジョニング キーを Zscaler から直接注文する必要があります。

- RISE のお客様の ZPA 管理者は、SAP にプロビジョニング キーを提供します。次に、SAP が RISE のお客様の S/4HANA PCE のクラウド ERP 環境に App Connector のプロビジョニング キーをインストールします。
- インストール後、SAP は ZPA App Connector の基本的な管理と保守を担当し、RISE のお客様の ZPA 管理者は ZPA テナントに対する完全な制御の維持を担当します。

主なメリット

SAP アプリケーションへの安全な接続を確立するために、VM を使用してゼロトラスト アクセスなどのサービスを展開すると、運用オーバーヘッドの増加、スケーラビリティーの低下、プロビジョニングの複雑化などの課題が発生します。
VM とは対照的に、SAP でホストされるクラウドネイティブ環境で ZPA を展開することで、次のようなメリットを得られます。

移植性とパフォーマンス：
SAP がホストする ZPA App Connectors は、OS やハイパーバイザーに依存しません。基盤となる OS への依存やハードウェアの仮想化の必要性を排除しながら、さまざまなクラウド環境で一貫して実行でき、ZTNA サービスの応答時間を短縮できます。

スケーラビリティーと最適化：
SAP がホストする ZPA App Connector は、ごく短時間で運用を開始し、需要の変動に合わせてすばやく動的に拡張できます。簡単なプロビジョニングが可能で、ZTNA の接続を簡素化できます。

リソース使用率とコスト：SAP がホストする ZPA App Connector は軽量で、Kubernetes などのオーケストレーション ツールを活用することで、リソース使用率や自己修復機能を改善し、運用負荷を削減します。

RISE with SAP と Zscaler の統合のメリット

- **RISE with SAP へのクラウド移行中のアクセスの合理化：**ZPA は、RISE with SAP への移行中に SAP アプリへの一貫したユーザー アクセスを提供します。
- **VPN を使用しないセキュア リモート アクセス：**この統合により、VPN を使用せずにあらゆる場所の従業員やパートナーに SAP への安全な接続を提供できます。
- **ネイティブ ZPA App Connector のプロビジョニング：**ZPA App Connector は、RISE with SAP (S/4HANA – PCE) の顧客環境内でプロビジョニングされます。クラウド ネイティブな展開により、Zero Trust Exchange への安全なアウトバウンド接続の開始が簡素化され、リソースの効率的な利用、自己修復、オーバーヘッドの削減が実現します。
- **一貫したサービス レベル アグリーメント (SLA):** ZPA App Connector ワークロードを S/4HANA (PCE) ワークロードと並行して実行し、SAP と同じ SLA で可用性、パフォーマンス、応答時間を保証します。
- **攻撃対象領域の最小化：**ZPA はゼロトラストを適用し、ネットワーク全体への接続を提供することなく、ユーザーのアクセスを特定の SAP アプリケーションのみに制限することで、攻撃対象領域を大幅に削減します。
- **ラテラル ムーブメントのリスク軽減：**ユーザーとアプリ間のセグメンテーションと最小特権アクセスに基づく接続により、許可されたユーザーと指定されたアプリケーション間でのみ 1 対 1 のアクセスを確立し、ラテラル ムーブメントを防ぎます。
- **データ保護と各種規制の順守：**Zscaler の統合データ保護機能は、SAP アプリケーションの機密情報に対する包括的な可視性と制御を実現します。これにより、組織はデータを効果的に監視および保護し、GDPR、HIPAA などの規制を順守できます。
- **ユーザー エクスペリエンスの強化：**ネイティブに展開される ZPA App Connector により、ユーザーは基盤システムの移行を気にすることなく利用できます。ユーザーとアプリ間の接続のエクスペリエンスは、デバイスや地理的な場所を問わず一貫性が確保され、従来の SAP アプリからクラウド環境への移行中も中断することなく維持されます。
- **パフォーマンスの向上：**SAP ユーザーは、業務に不可欠な SAP アプリケーションへの高速な直接接続が可能になります。世界中の 160 以上のポイント オブ プレゼンスを活用することで、最短経路でセキュリティを適用し、信頼性の高いアクセスを実現します。
- **事業継続性と高可用性：**インターネット接続が不安定な地域では、ZPA Private Service Edge を利用することで、アクセス ポリシーが数週間キャッシュされ、インターネット接続が失われた場合でも安全な接続と事業継続が可能になります。

RISE with SAP への移行における ゼロトラストによるアクセス合理化とリスク軽減

従来の SAP ECC の展開から RISE with SAP (S/4HANA PCE) への移行を計画する組織が増えるなか、Zscaler はアクセスの合理化とビジネス トランスフォーメーションの保護における主要なパートナーとして SAP と連携しています。

Zscaler Private Access は、従来のネットワーク アクセス ソリューションに代わる強力なサービスとして、ユーザーやアプリの場所を問わず、SAP アプリケーションへの高速で信頼性の高い安全なゼロトラスト アクセスを提供します。

その独自の機能により、攻撃対象領域を大幅に削減し、あらゆる場所のユーザーに優れたエクスペリエンスを提供します。SAP アプリケーションにアクセスするためにユーザー中心の VPN に投資する必要もなくなります。さらに、Zero Trust Exchange プラットフォームの統合データ保護機能は、SAP アプリケーションの機密情報に対する可視性と制御を確保し、効果的なデータ保護とコンプライアンスを実現します。

RISE with SAP 向け ZPA の詳細はこちら >

SAP について
SAP (NYSE: SAP) は、エンタープライズ アプリケーションやビジネス AI のグローバル リーダーとして、ビジネスとテクノロジーをつなぐ役割を担っています。50 年以上にわたり企業の信頼を得て、財務、調達、人事、サプライ チェーン、カスタマー エクスペリエンスなどのビジネスクリティカルな業務を統合し、お客様が最高の成果を実現するために支援しています。詳細については、sap.com をご覧ください。

zscaler™ | Experience your world, secured.™

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 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。

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