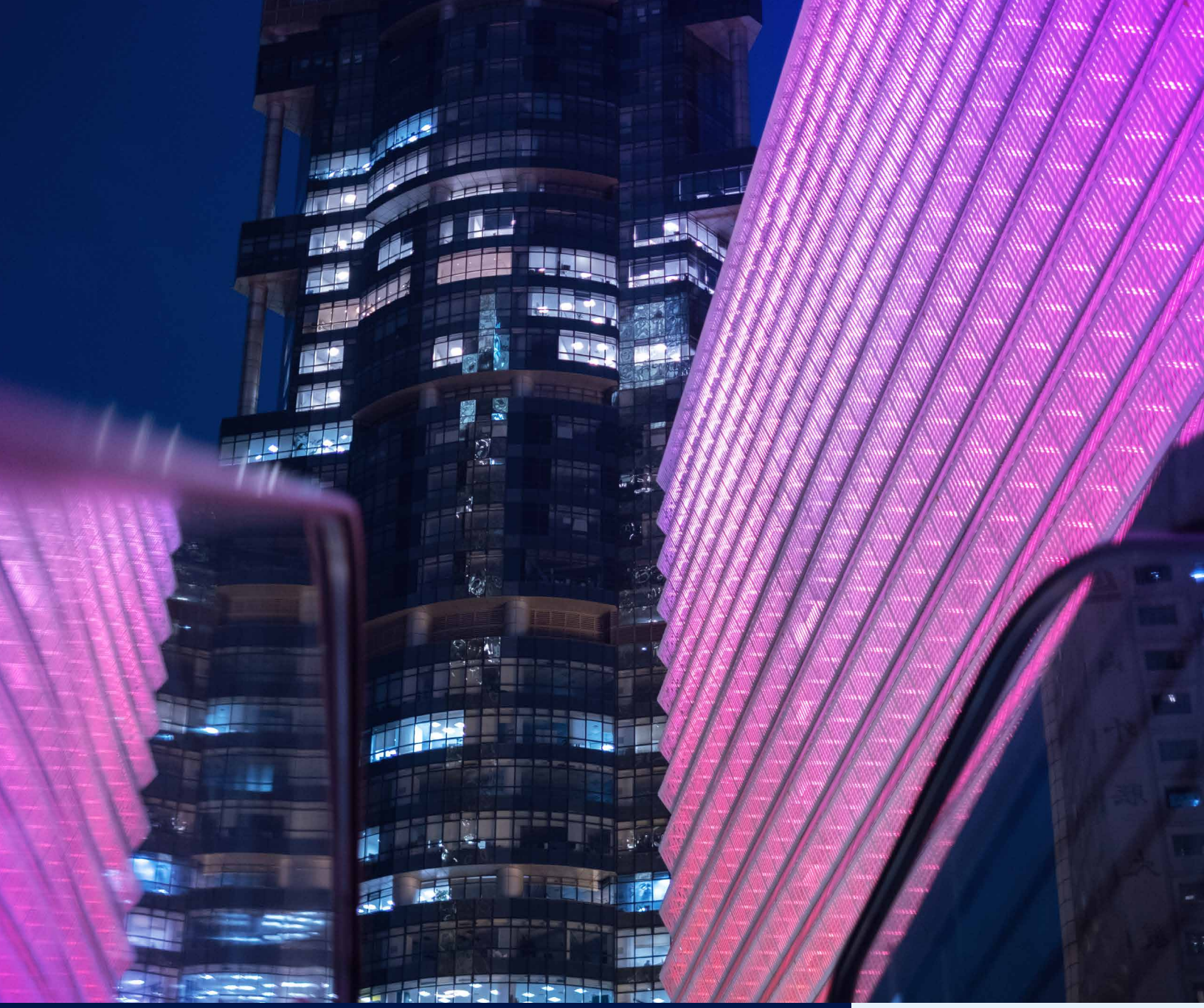


Zscaler Resilience™

ブラックアウト、ブラウンアウト、
壊滅的な障害に効果的に対処しながら、
中断のない事業継続性を確保

© 2024 Zscaler, Inc.All rights reserved.

ソリューションの概要

IT リーダーの最重要課題となった事業継続性

働き方が変化し、事業継続性が最優先事項になるにつれ、ミッションクリティカルなサービスの中断を防ぎながら生産性を維持することが IT リーダーの大きな課題となっています。適切なツール、プロセス、テクノロジーを使用すれば、IT 部門は災害発生時においても組織のあらゆる機能を迅速かつ簡単に復元できます。

多くの組織がストレージ、コンピューティング、セキュリティといった主要な領域にクラウド型サービスを導入し、システムの柔軟性と拡張性の向上、事業継続性の強化、そして IT コストと複雑さの軽減を実現しています。このようにクラウド型サービスには多くのメリットがありますが、自然災害、物理的な攻撃、国家規模での脅威などに対処するには、堅牢な事業継続性も必要です。

Zscaler Resilience は、ブラックアウト、ブラウンアウト、壊滅的な障害などが発生した際にも事業継続性を確保するための包括的な機能を提供します。Zscaler Zero Trust Exchange™ の高度なアーキテクチャーに基づいて構築された Zscaler Resilience は、オペレーショナル エクセレンスを活用して常に高い可用性と保守性を確保します。お客様側で管理される Zscaler のディザスター リカバリー機能と堅牢なフェイルオーバー オプションを組み合わせて使用すれば、あらゆる障害シナリオにおいても大きな中断なく業務を継続できるようになります。この包括的な機能により、Zscaler のセキュリティ クラウドは、業界で最も安全で回復力に優れたクラウドとなっています。

クラウド レジリエンスが必要な理由

ビジネス リーダーは生産性を最大限に高めるための環境づくりに注力しています。接続の問題、需要の増加、サービスの障害などによって通常のビジネス業務が中断された場合でも、IT 部門は事業や生産性の継続性を確保する必要があります。

事業継続性を確保するには、ミッションクリティカルなアプリケーション (SaaS アプリ、社内アプリ、プライベート アプリなど) へのユーザー トラフィックが常に流れている必要がありますが、クラウド内の障害やアプリケーションへの接続障害などが発生し、中断する場合があります。クラウド レジリエンスには、クラウド自体とクラウドに対する回復力の両方が含まれます。

クラウドの回復力

クラウドの回復力とは、強固なインフラと効果的なプロセスを備えたクラウドを構築し、日常業務を効率的に処理しながら、予期せぬ問題や中断からも迅速に復旧できるようにすることです。Zscaler クラウドは、軽微な障害 (ノードのクラッシュ、ディスクの問題など) の多くを自律的に処理するため、お客様が介入することなく接続とパフォーマンスが維持されます。処理能力と冗長性をオーバープロビジョニングする Zscaler の堅牢な専用ハードウェア システムは、回復力の高い基盤を提供します。

クラウドに対する回復力

クラウドに対する回復力は、包括的なクラウド レジリエンス ソリューションに不可欠な要素です。クラウドへの接続は、クラウドの可用性と、ユーザーがアプリケーションやデータにアクセスする接続手段に依存します。クラウドへのアクセスが中断された場合、お客様はアプリケーションへの代替パスを見つけることで接続を最適化し、手動または自動化された方法を適用して、ネットワーク パフォーマンスの低下や完全な停止などのさまざまな問題に対処する必要があります。Zscaler Resilience は、軽微なものから壊滅的なものまで、あらゆる障害が発生した際に事業継続性を確保するための包括的な機能を提供します。

© 2024 Zscaler, Inc. All rights reserved.

あらゆる障害シナリオに対応する回復力



図 *1:* 障害シナリオに対応するためのさまざまなオプション

軽微な障害

軽微な障害にはパフォーマンスの不具合、互換性の問題、運用上または品質上の問題など、重大な障害ではないものが含まれます。このような個別の障害は、ノードのクラッシュやディスク関連の問題によって発生する場合がほとんどです。発生頻度が最も高く、気づかれにくい軽微な障害ですが、スピードの低下、運用上の問題、ユーザーのストレスなどにつながる可能性があります。回復力に優れたZscalerのクラウド アーキテクチャーとオペレーショナル エクセレンスにより、軽微な障害による業務の中断が防止されます。障害が発生した場合はバックグラウンドで自動的に管理されるため、お客様はほとんど介入することなく、生産性を維持できます。

Zscaler Resilience の主なメリット

中断のないセキュリティによる事業継続性

不測の事態が起こった際も、重要なセキュリティ ポリシーを適用しながら、インターネット、SaaS、プライベート アプリへのゼロトラスト アクセスを維持できます。

あらゆる障害シナリオに対応するシームレスなエクスペリエンス

クラス最高のアーキテクチャーおよびZero Trust Exchange のオペレーショナル エクセレンスによって、ブラックアウト、ブラウンアウト、壊滅的な障害に簡単に対処できます。

コストと複雑さの軽減

重要なアプリへの接続トラブルによるビジネスの中断や生産性の低下を回避しながら、従来型のバックアップ インフラやオンプレミス VPN にかかるコストを排除できます。

© 2024 Zscaler, Inc. All rights reserved.

ブラックアウト

2022 年 1 月に Interxion のロンドン施設で発生したようなデータ センターの機能停止やキャリア / トランジット プロバイダーの接続障害などの深刻な接続中断により、影響を受ける Zscaler のデータ センターに組織がトラフィックを転送できない状況がブラックアウトのシナリオに該当します。Zscaler の冗長アーキテクチャーは、複数のプロバイダーとインターネット エクスチェンジ (IX) を備えたキャリアニュートラルなデータ センターを活用することで、個別のキャリア障害や接続の問題による障害を最小限に抑えます。ただし、データ センターが中断した場合、影響を受けたお客様は、復旧が完了するまでその特定のデータ センターのサービスを利用できません。

業務を継続するには、お客様は近接する Zscaler のセカンダリー データ センターにトラフィックをリダイレクトする必要があります。Zscaler はキャリア プロバイダーとデータ センター プロバイダーを組み合わせて使用することで、特定のサプライヤーからの中断を効果的に軽減し、セカンダリー データ センターを利用できるようにします。また、一時的に追加される負荷をサポートするために、データ センターの予備容量をオーバープロビジョニングして維持します。

事業継続性を確保するには、さまざまな障害シナリオを想定した綿密な計画が必要です。
Zscaler の優れたインフラは、100% の可用性を確保するように特別に構築されています。

SD-WAN デバイスを使用したオフィスからのトラフィック

オフィスから SD-WAN またはルーティング デバイスを使用してトラフィックを送信する場合、プライマリー IPsec/GRE トンネルが利用できなくなった場合のフェイルオーバーに備えて、事前にバックアップ IPsec/GRE トンネルを設定しておくことが推奨されます。フェイルオーバーの実行方法は、デバイスの機能やネットワークの設計によって異なります。例えば、デュアル インターネット回線を備えた SD-WAN では、アクティブなトンネルが利用できなくなったり、遅延のしきい値を超えたりすると (L7 正常性チェックが有効になっている場合)、バックアップ トンネルへのフェイルオーバーが自動的に実行されます。一方、機能が限定的なデバイスでは、手動フェイルオーバーが必要になる場合があります。プライマリー データセンターが再び利用可能になった後、プライマリートンネルに切り替えるのはお客様の責任となります。

Zscaler Client Connector を使用したトラフィック

Zscaler Client Connector を使用してトラフィックを送信する場合、Zscaler はトンネルの両端を制御します。プライマリー ゲートウェイが利用できなくなった場合は、アプリ プロファイルの PAC ファイルで定義されたロジックに基づいてプライマリー ゲートウェイからセカンダリー ゲートウェイに自動的にフェイルオーバーします。プライマリー ゲートウェイに再びアクセスできるようになると、Zscaler Client Connector はプライマリー ゲートウェイに切り替えます。必要に応じて、PAC ファイルを手動で変更してフェイルオーバー動作を制御することもできます。

ブラウンアウト

通常、ブラウンアウトとは、ネットワーク サービスの品質が意図せず、または予期せず低下した状態を指します。ブラウンアウトへの対処を誤ると、収益や生産性の低下につながる恐れがあります。ユーザーがブラウンアウトの兆候を指摘し、IT 部門がそれを認識して対応を開始するまでに時間がかかる場合、ユーザーの不満を引き起こすだけでなく、業務の進捗に遅れが生じる可能性もあります。ブラックアウトへの対応に加え、Zscaler は以下の方法を通じてブラウンアウトの問題を緩和します。

© 2024 Zscaler, Inc. All rights reserved.

リアルタイムのパフォーマンス指標に基づく Zscaler 側でのサービス エッジの選択

Zscaler Client Connector は、プライマリーとセカンダリーの ZIA Service Edge 間における最適なパスを選択します。図 2 に示すように、地理的な距離ではなく、各 ZIA Service Edge の正常性を考慮します。Zscaler では、エンドツーエンドの HTTP 接続を使用して遅延が測定されますが、これは、両方のゲートウェイに継続的に ping を送信し、応答にかかる時間をチェックすることで行われます。このデータに基づいて、Zscaler は最適なデータ センターを選択するため、ブラウンアウトなどの状況にも効果的に対処できます。

顧客側でのデータ センターの除外

ブラウンアウト発生時に事業継続性を維持するために、お客様側でデータ センターを除外する方法もあります (図 3)。例えば、ロサンゼルスのデータ センターなどで問題が発生した場合 (解決までに時間がかかる SaaS アプリケーションへの接続の問題など)、お客様は管理ポータルを使用してそのデータ センターを一時的に除外することができます。除外されると、Zscaler Client Connector は新しいプライマリー ゲートウェイとセカンダリー ゲートウェイを取得して、それらのデータ センターへの Z トンネルを確立します。ここで重要なのは、この除外は一時的なものであるということです。一定期間が経過すると、システムは元の データセンターの使用に戻ります。

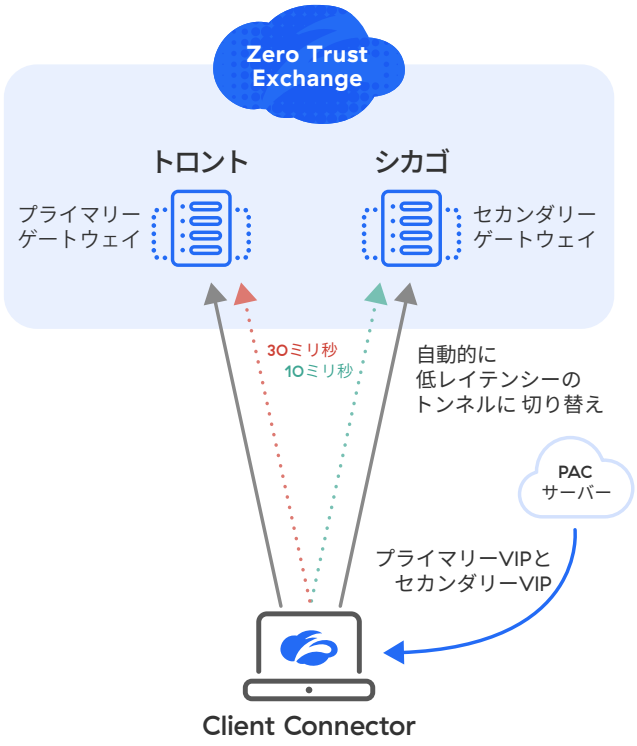


図 2: パフォーマンスベースの動的なサービス エッジの選択

ブラウンアウト対応ルーティング デバイスからのトンネル フェイルオーバー

オフィスからのトラフィックの送信にルーティング デバイスや SD-WAN デバイスを使用している場合、Zscaler はそれらのデバイスがトラフィックをどのように処理するかを直接制御することはできないため、ブラウンアウトへの対応はデバイスの機能と性能に完全に依存します。例えば、SD-WAN ルーターは、Zscaler のプローブ エンドポイントへの L7 正常性チェックに基づく独自のアルゴリズムを使用して、サービスの低下を検出します。ブラウンアウトの可能性が検出されると、SD-WAN デバイスは同じリンクまたはセカンダリー リンク上のバックアップ トンネルに自動的にフェイルオーバーします。正常性チェックでの結果が良好になると、デバイスはプライマリー トンネルに戻ります。

Zscaler BGP 制御

複数のプロバイダーとインターネット エクスチェンジ (IX) を備えたキャリア ニュートラルなデータ センターである Zscaler の冗長アーキテクチャーは、ブラウンアウト、輻輳、単一のキャリアに関係するその他の問題を最小限に抑えるのに非常に効果的です。Zscaler CloudOps が上流の ISP が最適でないルーティングを行っていることを検出した場合、プライマリー ISP を利用して問題を解決する間、セカンダリー ISP 経由でトラフィックを再ルーティングできます。

Zscaler データ センターの負荷分散

ネットワークの輻輳や特定のデータ センターへの接続に関するその他の問題が発生した場合、Zscaler Client Connector を実行しているクライアントを、統計手法を使用せずに地理的に近い場所のセカンダリー データ センターに予防的にリダイレクトできます。

© 2024 Zscaler, Inc. All rights reserved.

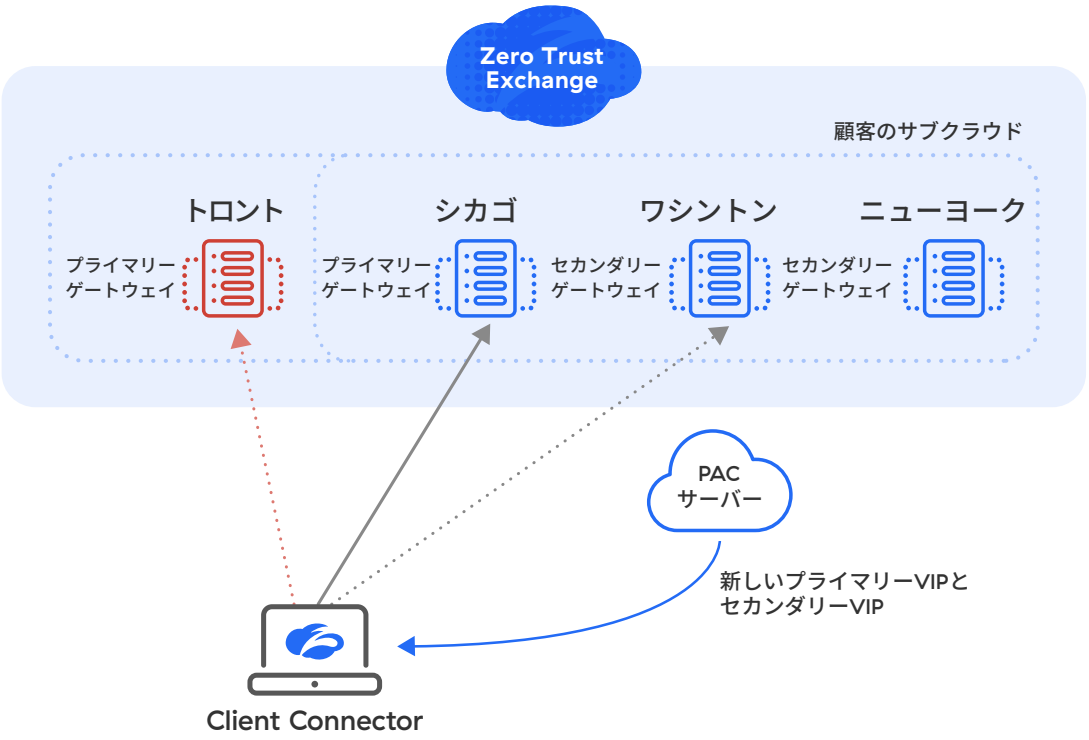


図 3: 顧客側でのデータ センターの除外

壊滅的な障害

ZIA/ZPA 向けの Zscaler Business Continuity

クラウド向けの Zscaler Business Continuity は、ブラック スワン現象が発生している最中でも、ユーザーがミッションクリティカルなアプリケーションにアクセスできるようにし、業務の中断を回避します。

災害時やインフラへのアクセスに問題が生じた際にも、ゼロトラスト セキュリティを維持したまま、アプリケーションに中断なくアクセスできることが極めて重要です。また、特定の業界では、事業継続性を担保するためのコンプライアンス要件や規制基準を満たす必要があります。

Zscaler はプライベート事業継続性クラウドをバックアップ オプションとして提供することで、Zscaler のパブリック クラウドに影響を与える恐れのある壊滅的なインシデントが発生した場合でも、組織が業務を継続し、厳格なセキュリティ基準を維持できるようにします。

Zscaler のパブリック クラウドにアクセスできなくなった場合は、事業継続性モードに切り替えることで、ポリシー施行とユーザー認証を継続できます。これらのサービスは Zscaler のパブリック クラウドではなく、お客様がホストする仮想マシン上で実行されるため、セキュリティとアクセスが中断されることはありません。

ZIA 向けの事業継続性

インターネットや SaaS アプリケーションに中断なくアクセスし、規制に順守するために、Zscaler は、お客様がホストする ZIA Private Service Edge とプライベート ポリシー キャッシュで構成されるプライベート事業継続性クラウドにフェイルオーバーできるようにします。

Private Service Edge (PSE) は、Zscaler Client Connector を実行しているユーザーに対して、トラフィック検査やファイアウォール機能などを含む、一貫したトラフィック処理を提供します。障害が発生した場合、この Private Service Edge はお客様のセキュリティ構成のキャッシュ コピーが保持されたプライベート ポリシー キャッシュを使用します。

© 2024 Zscaler, Inc. All rights reserved.

セルフホスト型の機能の展開を希望しない場合は、Zscaler の標準的な事業継続性ソリューションを使用すると、障害発生時でも Web アプリケーションや SaaS アプリケーションに継続的にアクセスできます。このシナリオでは、次のいずれかを選択できます。

フェイル オープン: セキュリティ制限なく、インターネットに自由にアクセスできます。

事前定義された許可リスト： 承認された特定のアプリケーションにアクセスできます。

フェイル クローズ： 障害発生中はインターネットへのすべてのアクセスをブロックします。

ZPA 向けの事業継続性

障害発生時でもプライベート アプリケーションに中断なくアクセスできるように、以下のコンポーネントで構成されるお客様独自のプライベート事業継続性クラウドを構築することも可能です。これらのコンポーネントをグループ化して複数導入すれば、高度な冗長性を確保できます。

Private Cloud Controller: 構成とポリシーを継続的に Zscaler クラウドと同期します。

ZPA Private Service Edge: 組織の環境内で ZPA 機能を提供します。

App Connectors: プライベート サービスへの安全なアクセスを確保します。

ログ レシーバー：他のコンポーネントが生成したログを収集します。

壊滅的な障害が発生した場合、または Zscaler クラウドにアクセスできなくなった場合、ユーザーは Private Cloud Controller に自動的に接続され、そこで認証と ZPA Private Service Edge へのリダイレクトが行われ、安全なアクセスが提供されます。ユーザーが ZPA PSE に接続されると、制御チャネルとデータ チャネルの両方が PSE を介して動作するようになります。

Private Cloud Controller は仮想マシンとして展開され、障害発生時に次のような重要な機能を実行します。

- 認証リダイレクト
- ユーザー リダイレクト
- ログ ストリーミング サービス
- お客様の構成の同期
- お客様のポリシーの同期

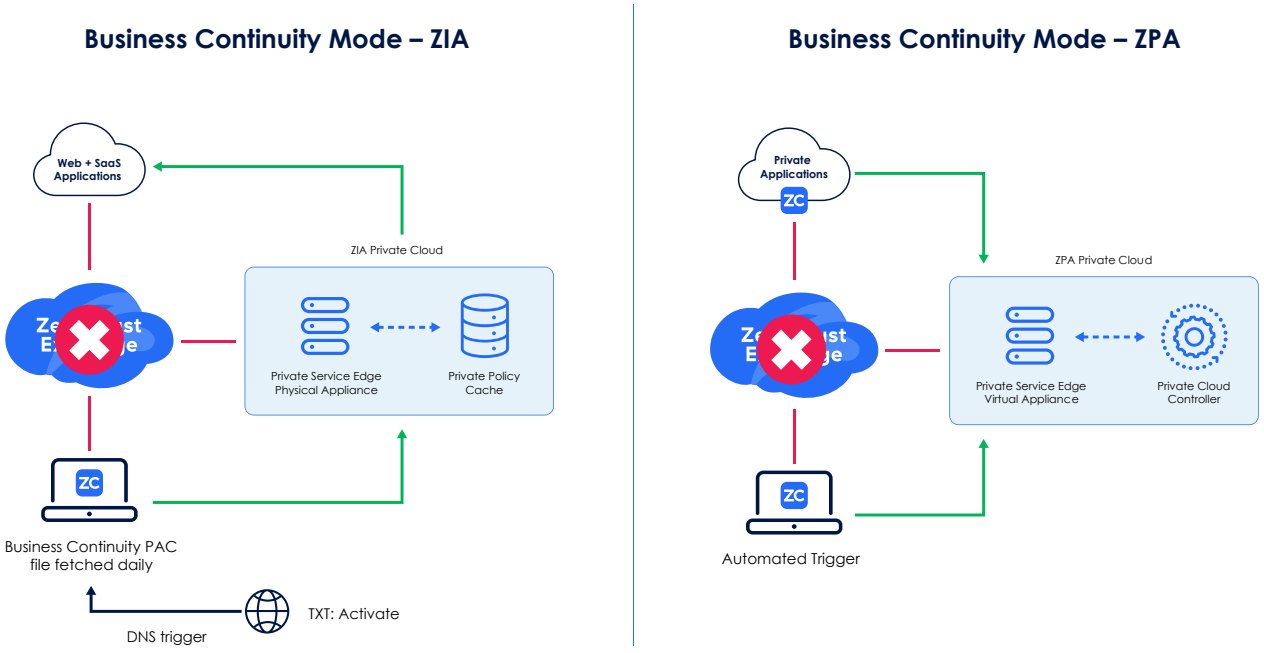


図 4: 完全なセキュリティ態勢を備えた、すべてのアプリにアクセスするためのプライベート事業継続性クラウド

© 2024 Zscaler, Inc. All rights reserved.

エンドポイント向けの事業継続性

通常のエンドポイント (ノートパソコン、コンピューターなど) が誤動作や紛失、侵害など、何らかの理由で利用できなくなるといったケースも組織に壊滅的な影響を及ぼす可能性がある問題の一つです。Zscaler Cloud Browser Isolation を導入することで、BYOD などの管理対象外のエンドポイントからプライベート アプリケーション、Web アプリケーション、SaaS アプリケーションへのブラウザーベースの安全なアクセスを確保できると同時に、情報漏洩のリスクが完全に排除されます。

Zscaler Business Continuity のまとめ

Zscaler クラウドの機能が復元すると、製品は通常の動作を再開し、Zero Trust Exchange の堅牢なゼロトラスト セキュリティと接続機能を最大限に活用します。Zscaler Digital Experience は軽微な障害、ブラウンアウト、ブラックアウトを検出し、ユーザーに重大な影響を与える前に対処できるよう組織をサポートします。Zscaler プラットフォームは、優れたセキュリティとシームレスなユーザー エクスペリエンスを確保しながら、事業継続性のための完全な柔軟性を提供します。

Zscaler Business Continuity は、Zscaler プラットフォームに組み込まれているため、サード パーティー ソリューションを追加することなく、プラットフォーム内で冗長性が提供されます。Zscaler は、Zscaler Resilience ソリューションに継続的に投資することで、ユーザーと IT 部門にシームレスで中断のないエクスペリエンスを提供します。

Zscaler Business Continuity の主なメリット

- 壊滅的なインシデント発生時の事業中断を最小限に抑制
- ブラック スワン現象発生時も業務に不可欠なアプリケーションへのアクセスを確保
- その回復力により、Zscaler のアプリケーション アクセス ソリューションの信頼性が向上
- 通常の運用時とシステム停止時の両方でアプリケーション アクセスを 1 つのプラットフォームで管理することでコストを削減
- 災害時における空白の時間がもたらす生産性の低下を回避することで被害コストを潜在的に削減

Zscaler Resilience の最新情報については、zscaler.com/jp/resilience をご確認ください。

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。

© 2024 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