ソリューションの概要

Zscaler Resilience™

ブラックアウト、ブラウンアウト、壊滅的な障害の発生時における中断のない事業継続性の確保

IT リーダーの最重要課題となった事業継続性

働き方の変化に伴い、事業継続性は IT リーダーにとって最優先事項になりつつあります。現在、IT リーダーはミッションクリティカルなサービスの中断を防ぎ、継続的な生産性向上に集中的に取り組むことが求められています。適切なツール、プロセス、テクノロジーを使用することで、IT 部門は災害発生時においても組織の全機能を迅速かつ簡単に復元できます。

ストレージ、コンピューティング、セキュリティをクラウドから提供するサービスに移行した組織は、柔軟でスケーラブルなシステム、事業継続性の向上、IT コストと複雑さの軽減を実現しています。このようなメリットがあっても、多くの組織が自然災害、物理的攻撃、国家規模での脅威などの惨事に備え、事業継続性を最適化する方法を模索しています。

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事業継続性を確保するための包括的な機能セットです。Zscaler Resilience は、Zscaler Zero Trust ExchangeTM の高度なアーキテクチャー上に構築されており、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提供します。顧客側がコントロールする Zscaler のディザスター リカバリー機能は、堅牢なフェイルオーバー オプションと組み合わせることで、あらゆる障害シナリオにおける組織の事業継続計画の取り組みをサポートすると同時に、業界で最も回復力に優れたセキュリティ クラウドとしての位置づけを確立します。

なぜクラウド レジリエンスが必要なのか

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、スケーリング イベント、サービスの障害などによって通常のビジネス アクティビティー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ためにも、ミッションクリティカルなアプリケーション (Saas、社内、プライベート) へのユーザー トラフィックは常に流れている必要があります。中断の原因としては、クラウド内の障害またはアプリケーションへの接続障害が考えられます。クラウド レジリエンスには、クラウド自身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

クラウドの回復力により、クラウド自体が効果的なインフラストラクチャー上に構築され、日常のビジネス機能を支える強力な運用プロセスが確保されます。Zscaler のクラウドは、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します。顧客とのやり取り、接続の喪失、パフォーマンスの低下が発生することはありません。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、ユーザーがアプリケーションやデータにアクセスできるよう、その可用性と接続手段によって変わります。クラウドへのアクセスが中断された場合、アプリケーションへの代替の最適パスを見つける必要があります。この最適化には手動または自律的なアクションがあり、ネットワーク パフォーマンスの低下から完全な停止に至るまでのさまざまな障害に対処するために適用できます。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セットです。

あらゆる障害シナリオに対応する回復力

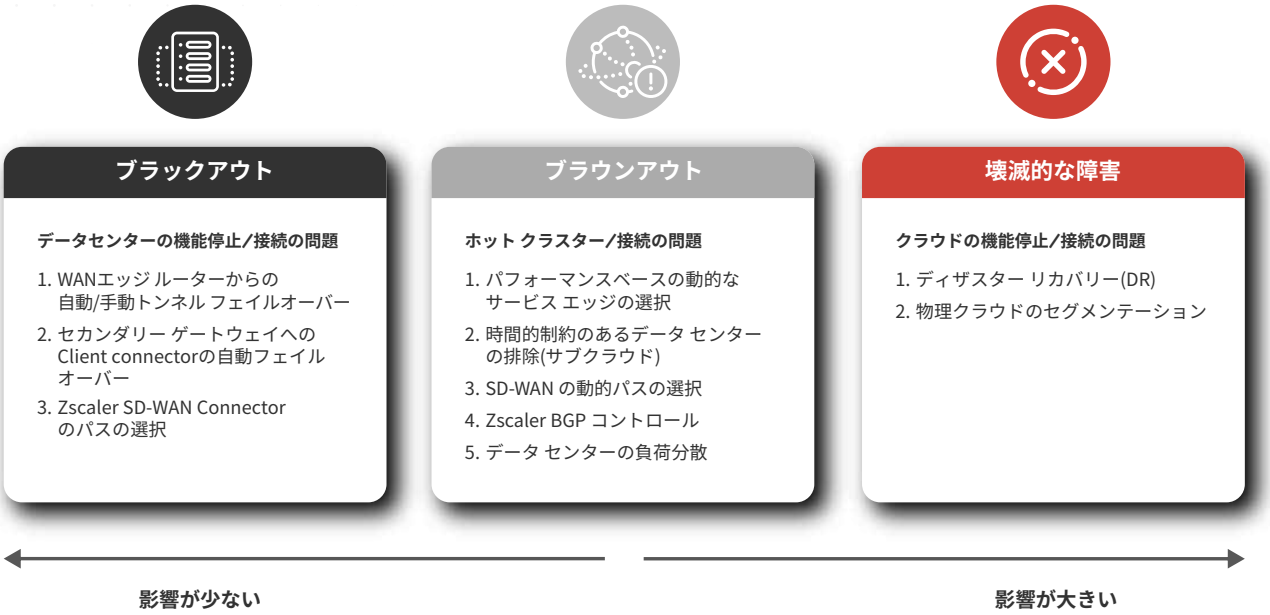

図 1: 障害シナリオに対応するためのさまざまなオプション

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。ノードのクラッシュまたはディスクの問題が個々の障害の主な原因であると考えられます。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の問題を招く可能性があります。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 エクセレンスは、軽微な障害をバックグラウンドで管理し、顧客とのやり取りを最小限に抑えながら、継続的な生産性を確保するため、こうした問題を防ぐことができます。

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

災害が発生した場合にも、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 アクセスを許可しながら 重要なセキュリティ ポリシーを適用

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

Zscaler Zero Trust Exchange のアーキテクチャーと オペレーショナル エクセレンスを 活用することで、ブラックアウト、ブラウンアウト、壊滅的な障害を簡単に対処

コストと複雑性の削減

旧式のバックアップ インフラや オンプレミスの VPN にかかるコストを排除しながら、重要なアプリにアクセスできないことで発生するビジネスの中断や生産性の低下を回避

ブラックアウト

データ センターの機能停止 (2022 年 1 月に発生した Interxion London 施設での機能停止など) またはキャリア / トランジット プロバイダーの機能停止などの深刻な接続問題は、影響を受けた 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ブラックアウトのシナリオとみなされます。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、単一キャリアの損失やその他の接続問題が発生した場合の機能停止を最小限に抑えるのに非常に効果的です。復旧にかかる時間に関係なく、影響を受けたデータ センターのサービスをそれ以上利用できないという事態を引き起こします。

業務を継続するには、顧客はトラフィックを近接する Zscaler のセカンダリー データ センターに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。

事業継続性とは、起こりうるさまざまな障害シナリオを考慮して対策を立てることです。Zscaler が誇るワールドクラスのインフラストラクチャーは、100% の可用性を提供できるように設計されています。

SD-WAN デバイスを使用したオフィスからのトラフィック

ルーティング /SD-WAN デバイスを使用してオフィスからトラフィックを送信する場合、Zscaler の展開に関するベスト プラクティスに従い、プライマリー IPsec/GRE トンネルに到達できない場合に備えてバックアップ IPsec/GRE トンネルを確保する必要があります。フェイルオーバーを発動させる手段は、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 は、アクティブなトンネルが到達不能になったり、レイテンシー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)、セカンダリー回線のバックアップ トンネルに自動的にフェイルオーバーできます。より原始的なデバイスでは、バックアップ トンネルを手動で有効にする必要があります。プライマリー データ センターが復旧したら、顧客の責任でスイッチバックを行います。

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 はトンネルの両エッジをコントロールして、アプリ プロファイルの PAC ファイルのロジックを使用しながらプライマリー 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。Zscaler Client Connector は到達可能になった時点で、プライマリー ゲートウェイに戻ります。場合によっては、PAC ファイルを手動で変更してフェイルオーバーを発動させることもできます。

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、収益と生産性の両方の点で大きな損失を被る可能性が出てきます。IT 部門がブラウンアウトを認識して解決に向けた作業に取りかかる前にユーザーがその兆候を指摘した場合、ユーザーのストレスがたまる状況に陥り、すべての作業が滞る可能性があります。ブラックアウトへの対処に加えて、Zscaler は以下の方法でブラウンアウトの問題を緩和します。

パフォーマンスベースの動的なサービス 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 の正常性に依拠します。エンドツーエンドの HTTP 接続では、レイテンシーを算出する際に双方のゲートウェイに対して継続的に ping を実行してから最終判断へと移ります。これにより、Zscaler はブラウンアウトのシナリオに効果的に対処するためのレイテンシーベースのデータ センターを選択します。

お客様がコントロールするデータ 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もう 1 つの方法は、図 3 に示すように、顧客側のコントロールによるデータ センターの選択です。例えば、ロサンゼルス空港で発生した SaaS アプリケーションのピアリングの問題 (解決に数時間かかる) など、データ センターで機能の問題が発生した場合は、管理ポータルで該当するデータ センターをサブクラウドから除外できます。次に、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 ゲートウェイをフェッチして、新しいデータ センターへの Z トンネルを確立します。このような顧客側がコントロールするデータ センターの除外には時間的な制約があり、事前に決められた時間が経過すると元の選択したデータ センターに戻ります。

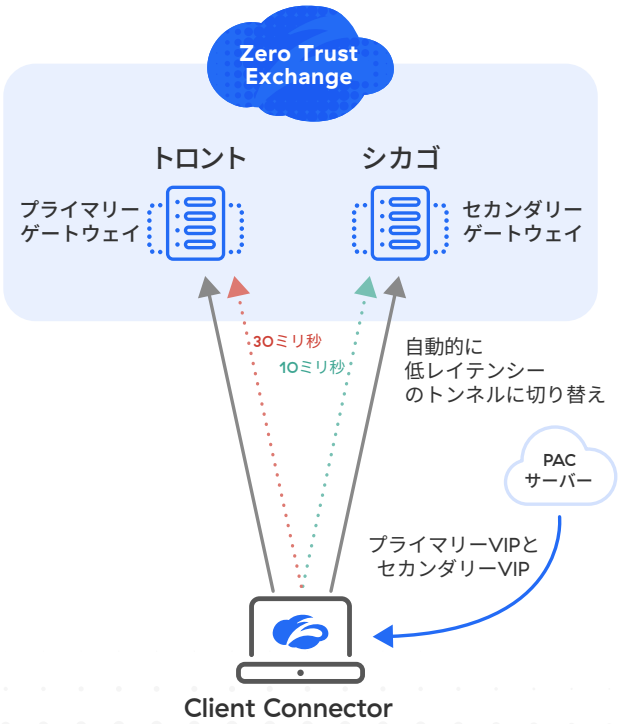

図 2: パフォーマンスベースの動的なサービス エッジの選択

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
Zscaler が直接コントロールできないルーティング / SD-WAN デバイスを使用してオフィスからトラフィックを送信する場合、顧客のオプションはエッジ デバイスの機能に制限されます。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できます。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できます。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 コントロール
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。

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 センターにプロアクティブにリダイレクトできます。

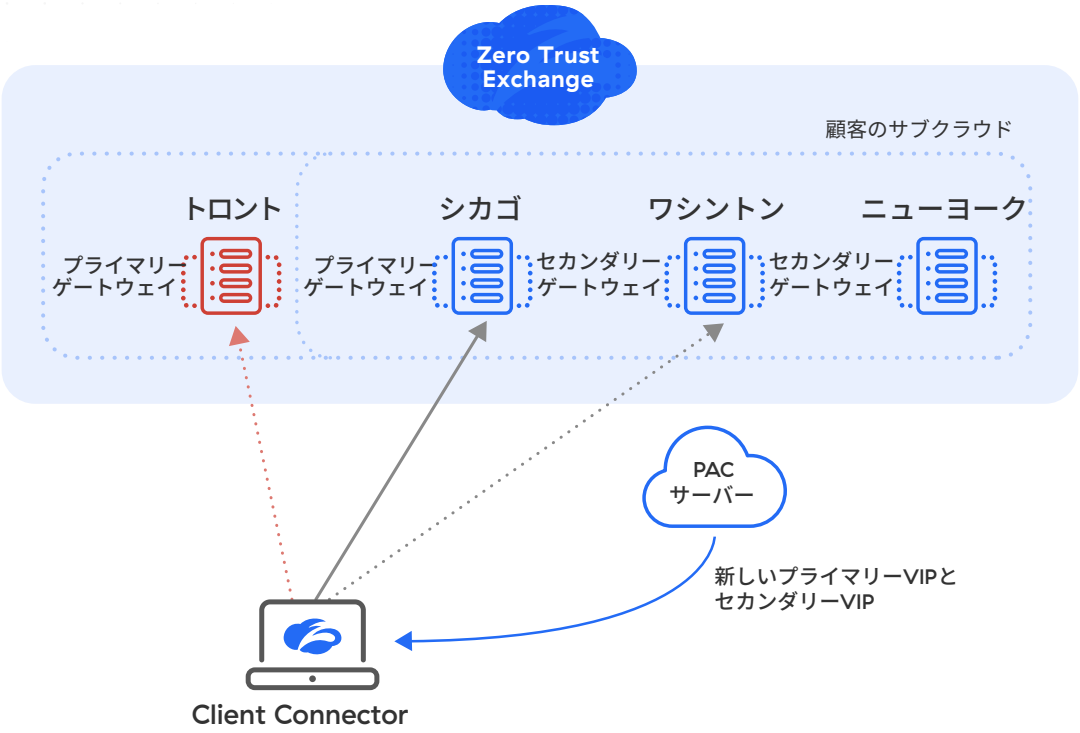

図 3: お客様のコントロールによるデータ センターの除外

壊滅的な障害

ZIA/ZPA 向けのディザスター リカバリー機能

Zscaler が提供するクラウド向けのディザスター リカバリー (DR) 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。

Zscaler のディザスター リカバリーは顧客側がコントロールする事業継続性ソリューションであり、Zscaler のクラウドに影響を与える可能性のある壊滅的な事象が発生した場合でも組織の運用を維持します。

ディザスター リカバリーは、DNS TXT レコードの更新によって開始されます。図 4 に示されているように、DR フェイルオーバーが開始されると、ディザスター リカバリーは、接続場所を問わずミッションクリティカルなプライベート /SaaS アプリケーションやインターネットにアクセスするためのパスをユーザーに提供します。

Zscaler のディザスター リカバリーでは、Zscaler のグローバルなクラウドが機能停止した際に、どのビジネス クリティカルなプライベート アプリケーションまたは SaaS アプリケーションにユーザーがアクセスできるかを、顧客がコントロールできます。

ユーザーは、Zscaler Private Access™ (ZPA™) Private Service Edge(Zscaler のクラウドがローカルに実装されたバージョン) を介して重要なプライベート アプリケーションに接続します。そして、AWS S3 インスタンスに保存されたポリシーで定義された重要な SaaS アプリケーションとインターネットに接続します。Zscaler Client Connector がインストールされていれば、誰でもディザスター リカバリーを使用でき、顧客が開始した DNS ベースの DR トリガーを通じて、ディザスター リカバリーを有効化するタイミングを決定およびコントロールできます。

プライベート アプリケーションへの安全なアクセスを実現するために、管理者は、Zscaler の管理ポータルで重要なアプリケーション セグメント、App Connector グループ、ZPA Private Service Edge グループの DR を構成して、グローバルな ZPA クラウド インフラストラクチャーに影響を与える災害が発生した場合にも事業継続性を確保できます。

お客様が指定する重要なアプリケーションへのアクセス

ZPA UI ダッシュボードでは、災害時の事業継続に不可欠なアプリケーションを事前に識別して、DR イベント中にユーザーがそのアプリケーションに確実にアクセスできるようにします。

Zscaler Internet Access™ (ZIA™) を介してインターネット上のアプリケーションに安全にアクセスするために、管理者はディザスター リカバリーのために次のオプションから選択できます (これらのコントロールは Zscaler Client Connector を介して提供され、Zscaler のポータルで構成されます)。

- **フェイル オープン：**万が一、Zscaler Cloud の機能が停止した場合、ユーザーは直接インターネットにアウトバウンド接続されることになります。しかし、これには、すべてのユーザーがセキュリティの制限なしで、インターネット上のあらゆる Web サイトに自由にアクセスできるというリスクが伴います。
- **コントロールされたフェイル オープン – Zscaler で定義されたインターネットの接続先リストへのアクセス：**ユーザーは、Web 上の最も一般的で重要なアプリケーション (Office 365、Google Workspace など) にアクセスできます。Zscaler は AWS でホストされているこのリストを維持しているため、Zscaler Cloud が停止から復旧している間でも利用できます。顧客はこのリストに独自のインターネット Web サイトを追加でき、リストにない Web サイトはブロックされ、Zscaler Client Connector を介してユーザーのエンドポイントで適用されます。Zscaler Client Connector はこのリストを定期的にダウンロードして、常に最新で正確な状態を保ちます。
- **フェイル クローズ：**セキュリティを非常に重要視していて、ZIA を使用していない際にユーザーがインターネットにアクセスすることを望まない場合は、すべてのアクセスを停止することができます。

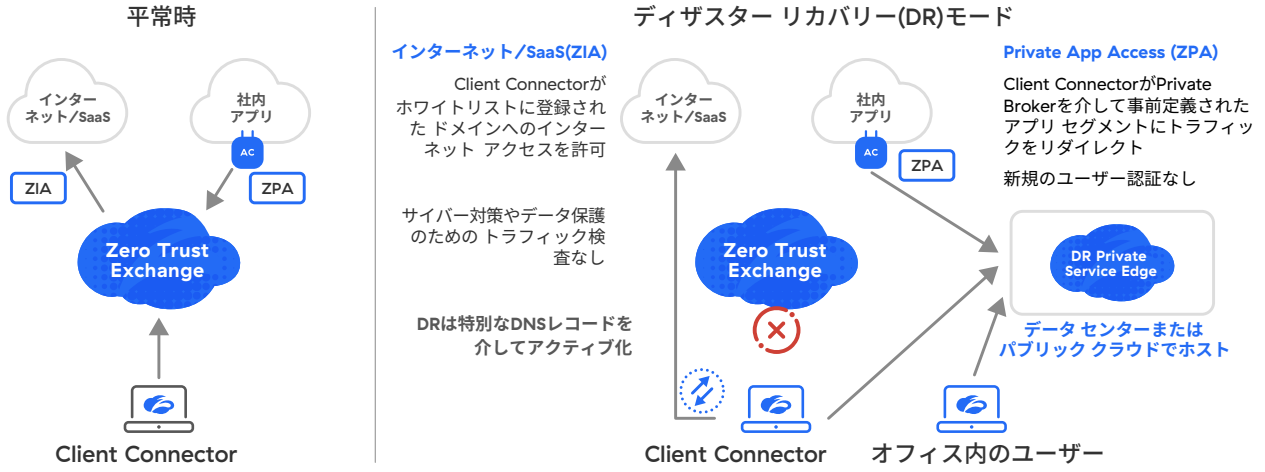

図 4: Zscaler のミッションクリティカルなサービス向けのディザスター リカバリー

ディザスター リカバリーを有効にすると、グローバルな Zscaler のクラウド インフラストラクチャーに影響を与えるような災害が発生した場合でも、事業継続性を確保でき、世界中のどこからでもユーザーが重要なアプリケーションにシームレスにアクセスできるようになります。

通常の運用では、ミッションクリティカルなアプリケーションへのアクセスは Zero Trust Exchange を介して仲介されます。災害が発生した場合、プライベート アプリへのすべての接続は、顧客のデータ センターまたはプライベート クラウドにローカルにインストールされた ZPA Private Service Edge を介して仲介されます。そして、インターネットや SaaS アプリケーションへのすべての接続は AWS S3 バケットに保存されたポリシーを通じて適用されます。これにより、災害時のシームレスなユーザー エクスペリエンスが実現します。Zscaler Cloud の機能が復元すると、製品は通常の動作に戻り、ゼロトラスト セキュリティと Zero Trust Exchange を介した接続を最大限に活用できます。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サポートします。Zscaler のプラットフォームは、比類のないセキュリティとシームレスなユーザー エクスペリエンスにより、事業継続性のための完全な柔軟性を提供します。

Zscaler Resilience はプラットフォームの一部として組み込まれているため、外部サービスを追加することなく、プラットフォーム内で冗長性を確保できます。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できるよう尽力しています。

Zscaler のディザスター リカバリーが持つ主なメリット

- 災害発生時の事業中断を最小限に抑制
- ブラック スワン現象の最中でも、ミッションクリティカルなアプリケーションへのアクセスを確保・Zscaler によってアプリケーション 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 DR 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.jp/resilience をご確認ください。

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