

DXC Technologyが
バーチャルファースト戦略を推進：
わずか90日でゼロトラスト
ネットワークアクセスに移行

DXC Technologyは、Zscaler Zero Trust Exchangeを活用して、世界13万人以上のユーザーにインターネットやSaaSへの安全なアクセスを提供し、業務効率向上を実現



課題

- DXCの世界中の従業員が使用するインターネットやSaaSのトラフィックを保護する
- 帯域幅の表示や管理をリアルタイムで行う
- オンプレミスからゼロトラストセキュリティモデルへ移行する



成果

- 13万人以上という規模の大きなビジネスのセキュリティを確保し、3か月で400億件以上のトランザクションと1,982テラバイトのトラフィックを処理
- セキュリティ体制を強化して、3か月で13億件のポリシー違反を防止し、920万件の脅威をブロック
- 暗号化されたトラフィックに潜む脅威を90日間で160万件検出してブロックし、ビジネスリスクを低減
- わずか90日で導入を実現し、バーチャルファーストの目標を推進



「Zscalerから得たプラスの成果は、当社だけではなく、デジタルトランスフォーメーションへの取り組みを始めるお客様のメリットにもなっています」

— **Mike Baker**

DXC Technology、グローバルCISO

ゼロトラストでモダンワークプレイスを先導

DXC Technologyは、エンタープライズITサービスのグローバルリーダーとして、従業員にとって非常に優れた雇用主であるだけでなく、お客様にとっても卓越したビジネスパートナーであることを目指しています。競争の激しい現代のビジネス環境でこれらの目標を達成するには、オフィス内かリモートかを問わずに協業できる支援が必要です。

DXCの従業員がバーチャルファーストの働き方を実現するには、従来のファイアウォールやVPNといった境界型セキュリティから脱却する必要があります。このためDXCは、ゼロトラストアーキテクチャへの移行に際して、世界最大のインライン型セキュリティクラウドプラットフォームであるZscaler Zero Trust Exchangeを採用しました。これにより、世界中の従業員と企業のお客様が安全に協働できるリモートワーク環境が実現しました。

Zscalerは、ゼロトラストセキュリティモデルの5つの柱（ID、デバイス、ネットワーク、データ、アプリケーションとワークロード）を完全にサポートし、きめ細かな制御とポリシーによって、データ中心のアプローチを提供します。DXCのグローバル最高情報セキュリティ責任者であるMike Bakerは、この取り組みについて次のように説明しています。「私たちは当初、特定のセキュリティユースケース向けとしてZero Trust Exchangeを採用しました。しかし、私たちが手にしたものが当社の成長を支える強力なプラットフォームであることをすぐに実感しました。そこからZscalerとの協業体制を築いてきましたが、この協業がDXCと当社のお客様の未来の働き方を変革するでしょう。当社のプログラムが現代の脅威ランandscapeによる課題に合わせて成熟および進化している中でZscalerと協力することが、ゼロトラストの目標達成を可能にしています」



「人に関する観点としては、リモートワークを優先し、場所を問わずに従業員が安全に働けるように、必要なプロセスやテクノロジーの採用または変更を検討しています。Zero Trust Exchangeを選択したことで、ゼロトラストの取り組みを支える適切なテクノロジーを導入できたと確信しています」

— **Suresh Gumma**
DXC Technology,
副CISO

ゼロトラストが未来の働き方をサポート

エンタープライズITサービスのグローバルリーダーであるDXCは、セキュリティ対策の選択肢が無数にあることでお客様が直面する課題や、リモートワークの実現には考え方の根本的な転換が必要であることを理解しています。DXCは、安全なリモートワークのために、従来のロケーション中心のモデルを捨て、ID中心のアプローチを採用する必要がありました。

ゼロトラストモデルは、IDや、デバイス、データ、アプリケーションを保護するための最も包括的な方法です。DXCの副CISOであるSuresh Gummaは、ゼロトラストを、セキュリティプログラムの全体像を明確に示す戦略的な枠組みとして捉えるようチームに働きかけました。「ゼロトラストは、人、プロセス、テクノロジーを統合し、利便性を損なわない優れたユーザー体験を提供しながらセキュリティを確保できる、すばらしいアプローチです」

DXCのセキュリティアーキテクチャは、米国サイバーセキュリティ・インフラストラクチャセキュリティ庁(CISA)のゼロトラスト成熟度モデル(ZTMM)をはじめとする主要な標準に基づいており、ゼロトラストによるモダナイゼーションへの包括的なアプローチを提供します。DXCは、ZTMMとそれを支えるテクノロジーを採用し、きめ細かな制御を行うことで、場所やデバイスを問わず、データやリソースへの不正アクセスを防止しています。

「人に関する観点としては、リモートワークを優先し、場所を問わずに従業員が安全に働けるように、必要なプロセスやテクノロジーの採用または変更を検討しています。Zero Trust Exchangeを選択したことで、ゼロトラストの取り組みを支える適切なテクノロジーを導入できたと確信しています」とGummaは語ります。

安全なインターネット接続により、可視性とセキュリティ体制を向上

60か国以上の大企業を支援しているDXCの従業員は、13万人を超えています。従業員は毎日DXCの環境にリモート接続しており、機密データに対しては、安全なアクセスと認証が求められます。セキュリティチームは、ユーザーがこれらの環境にどのようにアクセスしているかを詳細に可視化するだけでなく、データ損失やマルウェアの拡散を防ぐために、トラフィックを一貫した方法で保護する必要がありました。

DXCは、インターネットとSaaSアプリケーションへのアクセスを保護するため、クラウドネイティブなZscaler Internet Access (ZIA)を導入しました。ZIAは、Zscaler Zero Trust Exchangeの中核部分であり、あらゆるデバイスやあらゆる場所からのSaaSアプリケーションへの接続と、インテリジェントなトラフィックルーティングを可能にします。

ZIAを使用することで、DXCはTLS/SSLトラフィックを大規模かつ高速に検査できるようになり、高度な攻撃やマルウェアを検出して防止し、データ損失をリアルタイムで阻止できるようになりました。DXCは、暗号化されたトラフィックに潜む脅威のリスクを劇的に低減し、3か月の間に160万件の脅威を検出してブロックしました。

また、DXCはZscaler Sandboxを活用することで、未知の脅威や不審なファイルをインテリジェントに検出、隔離、分析し、すべてのユーザーとデバイスに対する侵害を防止しています。毎日数兆件にものぼるシグナルを元にしたリアルタイムのセキュリティアップデートが行われ、悪意のあるものと無害のものが識別されます。無害であるとすでに判断されているファイルはほぼ即座に提供されることで、DXCのユーザーの安全性も生産性も確保されます。

「ゼロトラストは、人、プロセス、テクノロジーを統合する、素晴らしいアプローチです」

— Mike Baker

DXC Technology, グローバルCISO

さらに、Zscaler Bandwidth Controlによって詳細なポリシー設定が可能となるため、DXCのITチームは重要なビジネスアプリケーションを優先し、ユースケースに応じて帯域幅を最適化できるようになりました。「セキュリティチームは、Zscalerのダッシュボードから、デバイスや、アプリケーション、ネットワークのパフォーマンスと使用状況をリアルタイムで可視化できます。これらの深いインサイトと指標により、私たちはリスクを定量化し、DXCのセキュリティ体制を経営陣に説明できるようになりました。これは、以前には不可能だったことです」とGummalは説明します。

クロスプラットフォーム統合によりゼロトラスト戦略を拡大

DXCのセキュリティチームは、エンドポイントデバイスの可視化と管理のためにCrowdStrikeを導入したあと、脅威インテリジェンスをエンドポイントからアプリケーションまで統合して活用するために、ZscalerをCrowdStrikeと統合しました。DXCは、自社が管理するデバイスに対して、CrowdStrike Zero Trust Assessment (ZTA)の動的スコアに基づいてアプリケーションへのアクセスを許可またはブロックするポリシーをZIAから構成できます。ZTAスコアはZscalerに連携され、デバイスのセキュリティ状態に基づいてそのアクセスポリシーがリアルタイムで変更されます。

またDXCは、ユーザーの認証や、使用が認められているアプリケーションへのパートナーおよび従業員によるアクセス権を検証するために、Oktaを導入しました。セキュリティチームは、ZscalerとOktaを統合し、IDレベルでの完全なゼロトラストソリューションを実現しました。OktaがユーザーのIDを検証すると、Zscalerはデバイスのトラフィックを検査して、最小権限アクセスの原則に沿い、IDとコンテキストに基づいて、必要なリソースのみへのアクセスを許可します。ZscalerとOktaの統合により、DXCのユーザーはどこからでも高速かつ安全に、インターネットやSaaSアプリケーションにアクセスできます。これらの統合によるインテリジェンスと保護を組み合わせることで、セキュリティチームは以前よりも自信を持って行動できるようになりました。

「ZscalerがWebとSaaSのトラフィックを可視化し、CrowdStrikeがエンドポイントを管理し、OktaがID層として機能することで、インシデント発生時に的確な調査を実施できる豊富なツールを活用できるため、DXCのセキュリティチームの対応はさらに迅速になりました」とBakerは説明します。

DXCは、優秀なテクノロジー人材の採用と定着という目標を達成するため、ユーザー体験の向上を優先事項としてきました。DXCは、従業員が世界中のどこからでも同じように安全かつシームレスに、インターネットやSaaSアプリケーションにアクセスできるようにしたいと考えています。



従業員の定着率、採用状況、生産性が向上

DXCは、優秀なテクノロジー人材の採用と定着という目標を達成するため、ユーザー体験の向上を優先事項としてきました。DXCは、従業員が世界中のどこからでも同じように安全かつシームレスに、インターネットやSaaSアプリケーションにアクセスできるようにしたいと考えています。ユーザー体験の向上に加え、DXCのゼロトラストへの移行は採用活動にもプラスの影響をもたらしています。「Zscalerのおかげで、ユーザーがどこからでも簡単に作業できるようになり、DXCが世界中のあらゆる場所から人材を採用する取り組みに役立っています。一貫したエクスペリエンスと信頼性は、DXCに競争上の確かな優位性をもたらしています」とBakerは説明します。「誰もがバーチャルファースト環境の柔軟性を気に入っているのです」

安全で安心な業務環境を維持するために、DXCは不要なWebサイトや不適切なWebサイトへのアクセスをブロックしています。「ユーザーは、会社のデバイスを私的に利用し、不要なサイトで帯域幅を消費してしまうことがあります。Zscalerは、不適切なサイトや悪意のあるサイトをブロックするほか、人事部門によるポリシー設定を可能とすることで、インシデントや、承認されていないコンテンツへのアクセスを防止できるようにしています」とBakerは述べます。「これによってセキュリティが強化されるだけでなく、生産性も大幅に向上しました」

知識を共有し、お客様の信頼を獲得

DXCは、ZIAを導入した直後に、展開したZero Trust Exchangeを、お客様のZscaler環境と共存し通信できるように構成しました。DXCの従業員は、数回クリックするだけでお客様のリソースへシームレスかつ安全に接続でき、ITモダナイゼーションプロジェクトでの協働を実現できます。「私たちは当初、DXCを保護するためにZscalerに投資しました。しかし、当社がお客様と同じセキュリティレベルで保護されていると伝わることで、お客様から寄せられる信頼感が高まったことにすぐに気付きました」とBakerは言います。「さらに私たちは、自社での展開を通じて得た知識を活用することで、セキュリティ関連のお客様によるZscalerのゼロトラスト実装の導入や管理を支援できるようになりました。Zero Trust Exchangeプラットフォームから得たプラスの成果は、当社だけではなく、デジタルトランスフォーメーションへの取り組みを始めるお客様のメリットにもなっています」

安全なインターネット アクセスから 強力な協業へ

DXCとZscalerの協業の成功は、セキュリティソリューションのリーダーである2社の強固な連携につながりました。

「Zscalerは、主要な協業パートナーとして、DXCの事業と目標を深く理解してくれています。Zscalerの経営陣とも、強力な関係を築いてきました。同社の丁寧な対応や細部への配慮は、この規模のベンダーとしては珍しいほどです」とBakerは述べます。「当社は、このプラットフォームによってリスクを大幅に低減できました。この成果を踏まえ、さらなる関係拡大の機会に向けて、私たちはZscalerと連携し続けています」

高度な機能でバーチャル ファースト戦略を成熟化

DXCは、強化されたセキュリティ体制や、大幅なリスク軽減、戦略的イノベーションを基盤に、Zscalerのさらなる機能の活用も検討しています。

お客様のデータの保護を最優先に掲げるDXCのセキュリティチームは、自社のデータ保護機能を強化するために、Zscaler Data Protectionの導入を検討しています。Zscaler Data Protectionは、リモートユーザーと、ユーザーがアクセスするSaaSアプリケーションやパブリッククラウドアプリケーションを追跡しながら、エンドポイント、インライン、クラウドにわたって一貫性のある統合的なデータ保護を提供します。データは、機械学習による革新的なデータ検出を活用することで、自動的に検出および分類されます。DXCは、Zscaler Data Protectionによって、データの挙動とリスクを的確に把握できるようになります。特に、ユーザーが機密性の高い顧客情報を取り扱っている際に役立ちます。

DXCは、自社のユーザーや、アプリケーション、資産、テクノロジーパートナーとの広範なエコシステムにわたるサイバーリスクを定量化し可視化するために、Zscaler Risk360™の導入も検討しています。Risk360は、DXCのZscaler環境、外部ソース、およびZscaler ThreatLabzによるセキュリティ調査から得られるデータを組み合わせることで、DXCのリスク露出状況に関する詳細ビューや、是正のための実用的なインサイト、財務への潜在的影響、サイバーリスクの管理と意思決定に役立つ経営層向けレポートを提供します。



「Zscalerは、主要な協業パートナーとして、DXCの事業と目標を深く理解してくれています。Zscalerの経営陣とも、強力な関係を築いてきました。同社の丁寧な対応や細部への配慮は、この規模のベンダーとしては珍しいほどです」

— Mike Baker
DXC Technology、
グローバルCISO



「私たちは当初、特定のセキュリティユースケース向けとしてZero Trust Exchangeを採用しました。しかし、私たちが手にしたものが当社の成長を支える強力なプラットフォームであることをすぐに実感しました」

— Mike Baker
DXC Technology、
グローバルCISO

従業員、お客様、組織のために貢献

DXCがバーチャルファースト企業になるという目標を達成するには、世界中の13万人を超えるリモート従業員によるインターネットトラフィックを保護する、シームレスな方法が必要でした。このため、始めにZIAをわずか90日で導入し、現在ではあらゆる場所とデバイスからのインターネットアクセスとSaaSアクセスを保護しています。

すべてのWebトラフィックを可視化したことで、DXCは帯域幅制御ポリシーを細かく設定しています。これにより、重要なビジネスアプリケーションを優先して、すべてのトラフィックをリアルタイムに保護し、深いインサイトによって世界中の物理的な資産や拠点を最適化しています。DXCは、Zscaler Zero Trust Exchangeを活用し、安全なモダンワークプレイスを実現しています。

詳細はこちら

dxc.com/jp/ja/offerings/security

お問合せと最新情報:
dxc.com/jp/ja/contact-us



DXC Technologyについて

DXC Technology (NYSE: DXC) は、最新のIT環境への刷新、データアーキテクチャの最適化、パブリック・プライベート・ハイブリッドクラウド全体に渡るスケーラビリティとセキュリティを実現しながら、ミッションクリティカルなシステムを支え、グローバルに広がるお客様のビジネスをご支援します。DXCは、競争力や業務パフォーマンス、顧客体験価値のさらなる向上といった課題に挑む世界大手企業のお客様の信頼を獲得しています。DXCがどのようにお客様の成功と従業員の成長を実現しているかについてはDXC.comをご覧ください。日本における取組についてはDXC.com/jpをご覧ください。