zscaler™

ZSCALER

ゼットスケーラーの銀行/金融サービスでの利用

コンテンツ

01 急速に変化するテクノロジとビジネスの環境

02 デジタルトランスフォーメーションの現状

03 成功するデジタル、失敗するデジタル

04 従来型のインフラストラクチャ：
推進要素か阻害要素か

05 セキュリティとユーザエクスペリエンスの両立

06 SASEとゼロトラストによるセキュリティ
とユーザエクスペリエンスの両立

07 ゼットスケーラーの紹介

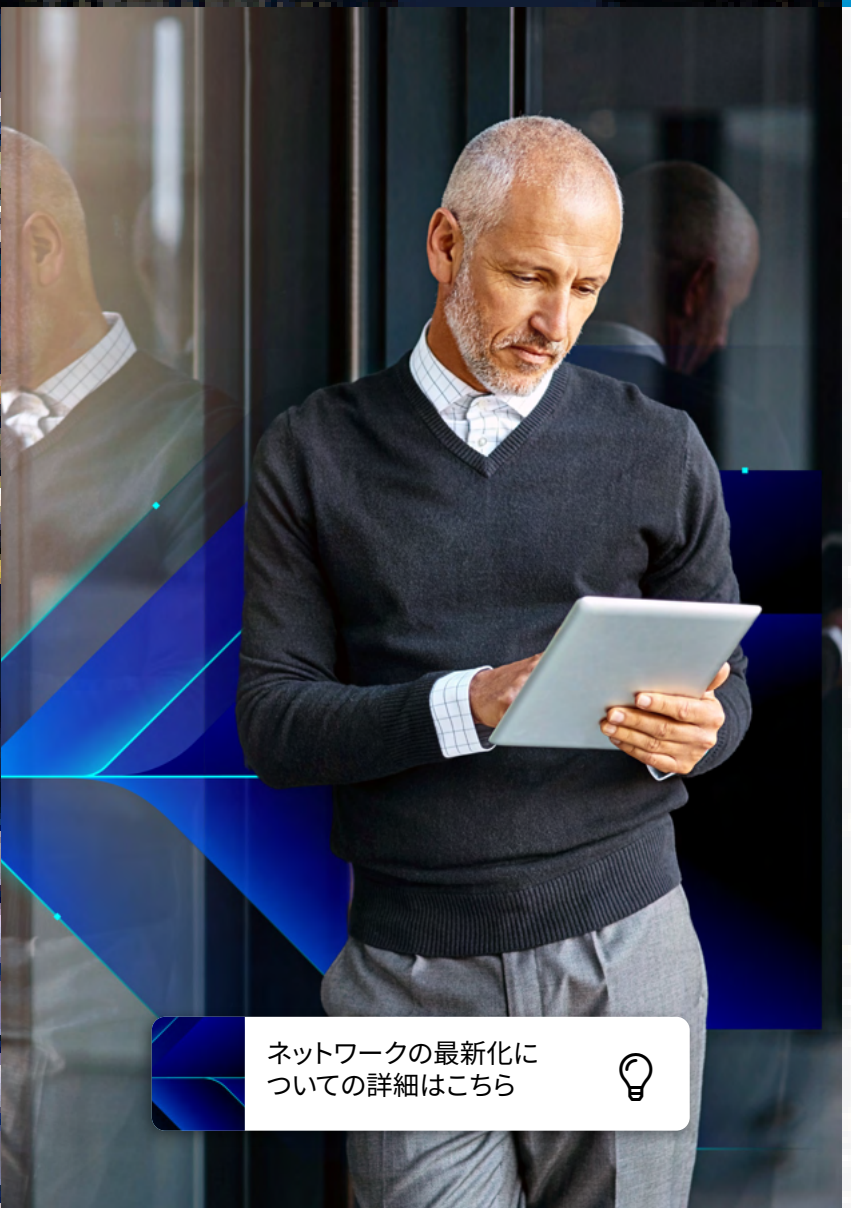
08 合併・買収

09 デジタルトランスフォーメーションで次
に何を目指すか？

10 今すぐ行動すべき理由

1 急速に変化するテクノロジ環境

世界がどのような破壊的効果に見舞われようとも、世界の現状を表す最も適切かつ定量的で高感度のバロメータが金融サービス分野の健全性であることに変わりありません。



ネットワークの最新化についての詳細はこちら

急速に変化する国際経済情勢を勝ち抜き、発展するために、この分野では、包括的かつ戦略的なアプローチを採用して自らが生まれ変わり、クラウドコンピューティング、あらゆる場所でのモバイルの利用、人工知能（AI）による自動化といった最新のテクノロジを活用した新たなFinTechプラットフォームが採用されてきました。

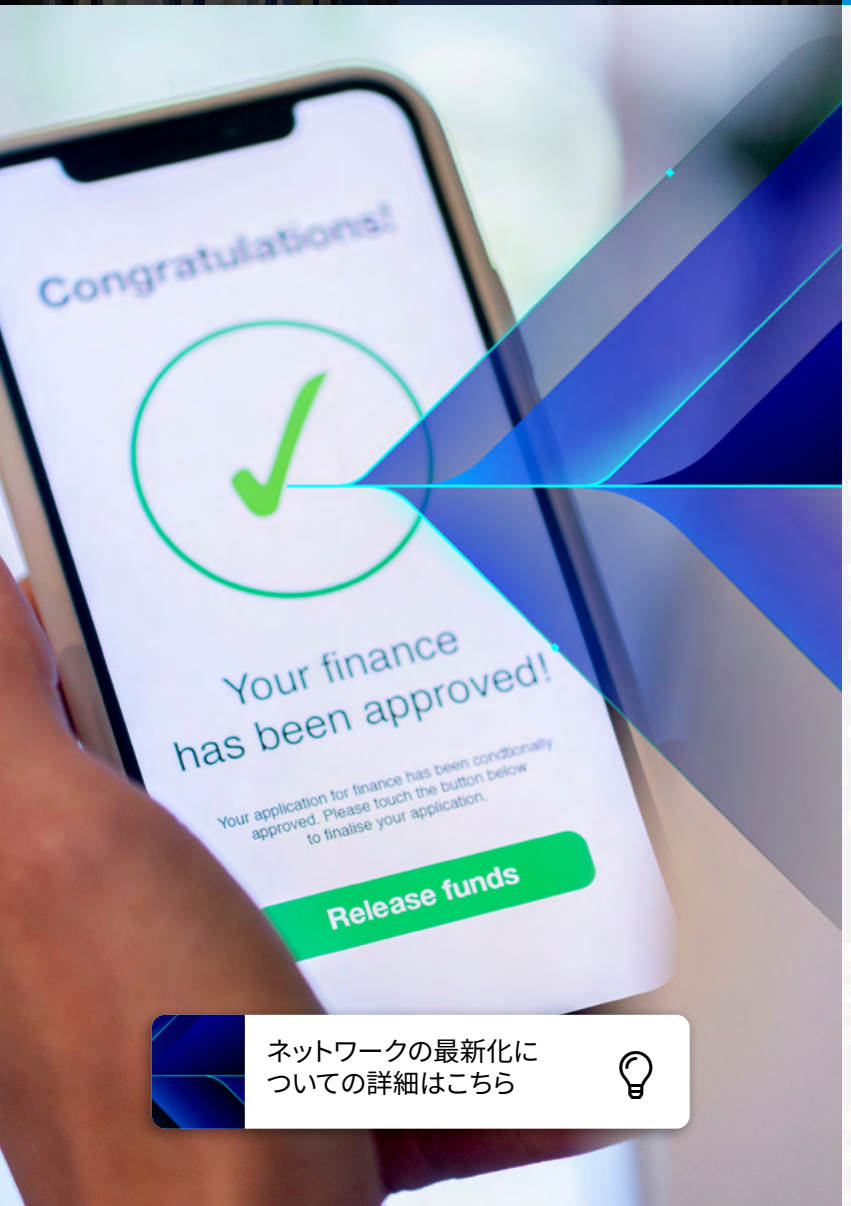
2020年までは、ミレニアル世代の若者が非接触型のタップ方式の支払いシステムなどの新しいテクノロジの普及を主導してきましたが、その動きが広がり、今ではすべての年齢層に非接触型の利便性が知られるようになりました。もちろん、新型コロナウイルスの感染拡大も、オンラインバンキングとキャッシュレスの社会への移行を加速させる大きな要因となりました。

それと同時に、テクノロジの進歩によって、これまでの常識を覆す競合企業の参入も可能になりました。スマートフォンを利用し、電子決済を積極的に活用するeコマースが消費者に受け入れられるようになったことから、新しいスタイルを踏襲した金融機関が参入し始めているのです。

住宅ローンの検討、保険の規約や投資計画の検索、あるいは預金口座からの単なる資金移動のいずれを目的とする場合であるかにかかわらず、デジタルでの実行が標準として急速に定着しつつあります。市場のダイナミズムと新たに加わった選択肢によって、厳しい要求を突きつける顧客が増加し、ユーザごとにカスタマイズされ、付加価値のある、リアルタイムでシームレスなユーザエクスペリエンスが求められるようになりました。

2 デジタルトランスフォーメーションの現状

デジタルイノベーションとビジネスアジリティは、新規顧客の獲得、得意分野での市場シェアの拡大、新しいビジネス分野での成長の機会への対応の鍵となります。



しかしながら、成熟した金融機関の中心は今なおコアシステムであり、多くの場合に長年をかけて広範囲にわたってカスタマイズされてきた独自のオンプレミステクノロジを基盤とするものであるため、様々な要素が相互に依存し、多くの階層のIT機能が連携しています。金融関連の法規制、ガバナンスの管理、データプライバシーに関する法律がクラウド導入の主な阻害要因であるとされることを考えれば、ほとんどの金融サービス機関でパブリッククラウドが提供する効率性やアジリティの活用に時間がかかっているのは、当然とも言えるでしょう。

金融関連の規制当局は早い段階から、セキュリティやプライバシーの観点からのクラウドコンピューティングの利用に関する標準やガイダンスの制定を進めてきました。これにより、クラウドによる法規制のコンプライアンスが可能になったため、金融機関は、イノベーションを損なうことなく、リスク管理、データの整合性、機密性に対する効果的なアプローチを開発できるようになりました。

現在、ほとんどの金融機関がハイブリッド環境で一部の従来型のインフラストラクチャを運用していますが、クラウドが着実に定着し、ERPから、市場データ、CRM調査、販売資料、市場評価分析までのあらゆるプラットフォームやアプリケーションがIT環境で利用されるようになっています。FINRA認定の簡単なトレーニングがオンラインに移行し、**FINRAそのもののアプリケーションも100%クラウドに移行しました**.

2020年にヨーロッパ・中東・アフリカの600人のCIOを対象にゼットスケーラーが実施した調査によると、金融サービス分野でデジタルトランスフォーメーションが順調に進んでいることがわかりました。現在、多くの組織がクラウドファースト戦略を採用しており、複数のパブリッククラウドやSaaS（Security as a Service）のアプリケーションを顧客向けソリューション、バックオフィスの運用、金融エコシステムのパートナー（シャドーバンク、フィンテックプロバイダなど）との統合を利用しています。

この調査では、3分の2の企業が **50%のアプリケーションをクラウドに移行し、4分の1の企業が75%のアプリケーションをクラウドに移行したと回答しています。**

ネットワークの最新化についての詳細はこちら

3 成功するデジタル、失敗するデジタル

金融サービスの一等地の店舗からオンラインへの進化に伴い、プロバイダは、かつてはさまざまな支店で提供していた対面の顧客サービスと同じレベルをオンラインに形を変えてそのまま提供しようとする過程で、課題に直面しています。

顧客を失うリスクを軽減するため、カスタマエクスペリエンスは、ほとんどの金融機関で常に最上位のビジネス優先事項となってきました。サービスが正しくシームレスに提供されれば、顧客はさらに多くを求め、多くのサービスを利用し、新しいサービスを購入する可能性も高くなります。正しくない、遅い、あるいは信頼が欠如したサービスを提供すれば、すぐに顧客に見放されてしまいます。

進歩的な金融サービス機関は、将来や業界の動向に常に注視し、5G、AI、ブロックチェーン、RPA（ロボットプロセスオートメーション）、IoT（モノのインターネット）の幅広い分野での利用を取り入れたテクノロジに注目しています。

これらのテクノロジの採用、実装、展開の進展がCovid-19のパンデミックの影響で突如として停止することになり、このことは、あらゆるレベルの商業分野や組織の開発戦略に多大で破壊的な影響を与えました。あらゆる組織が短期間で方向転換を迫られ、ビジネス継続性の確保に重点的に取り組む必要がありました。数日以内にほとんどのIT部門が課題に直面し、プロジェクトの優先順位を見直し、作業を加速させることで、プロジェクト管理を習得し、地域や世界の経済を動かし続けなければならなくなりました。オフィスやブランチで働いていた何千人もの担当者がリモートワークに移行し、**キャッシュレスの支払方法やその他の形式のリモートプロセスが**当初の予想より早い時期に展開されました。

ネットワークの最新化についての詳細はこちら

4 従来型のインフラストラクチャ：推進要素か阻害要素か

金融サービス機関はデジタルトランスフォーメーションの一環としてクラウドやモバイルの採用を進め、大きな進歩を遂げましたが、進化によっていくつかの新たな課題に直面することにもなりました。

日常業務に今も利用されている既存の投資は、耐用年数をできるだけ引き伸ばすことで、最大限のROIを達成しようとすることもよくあります。問題は、従来型のインフラストラクチャは、今日のクラウドやモバイルの世界のトランザクション、分析、処理の要求に対応するように設計されていない点にあります。そういった不備がパンデミックによって表面化することになりました。

パンデミック前は、ほとんどの金融サービス部門の担当者が支店やオフィス環境で働いていました。少数の担当者が外出先での打ち合わせや在宅勤務などの目的でVPN（仮想プライベートネットワーク）やVDI（仮想デスクトップインタフェース）を利用し、組織の中核である金融システムや保険システムに接続していました。しかしながら、今回のパンデミックにより、IT部門は、外出が制限されてしまった多数のリモートワーカーによる安全なリモートアクセスを可能にするという課題に直面しました。

モバイルの担当者はビジネスシステムやクラウドアプリケーションにアクセスできましたが、VPNは大半のスタッフが使用することを前提に設計されていないだけでなく、ロードバランサ、DDoS、ファイアウォール、VPNコンセントレータなどの積み重ねられたアプライアンスをトラフィックが通過しなければなりません。既存のネットワークと従来型のインフラストラクチャ、複数のアプライアンスを経由してトラフィックをバックホールすると、レイテンシが発生し、ユーザの不満が募り、生産性が低下します。最悪の場合、従業員がセキュリティポリシーやVPNコントロールを回避するようになり、セキュリティ脆弱性につながります。

VDIテクノロジにより、リモートユーザがBYOD（個人所有デバイスの業務利用）を使用して中核システム、電子メール、その他のアプリケーションに接続しつつ、データの漏洩や盗難などの古くからある問題を軽減できるようになりました。これらのソリューションは、セットアップが難しく、メンテナンスにコストがかかるだけでなく、範囲を超えて使用されるようになり、パンデミックが続く中でセキュリティリスクが増大することにもなりました。

ネットワークの最新化についての詳細はこちら

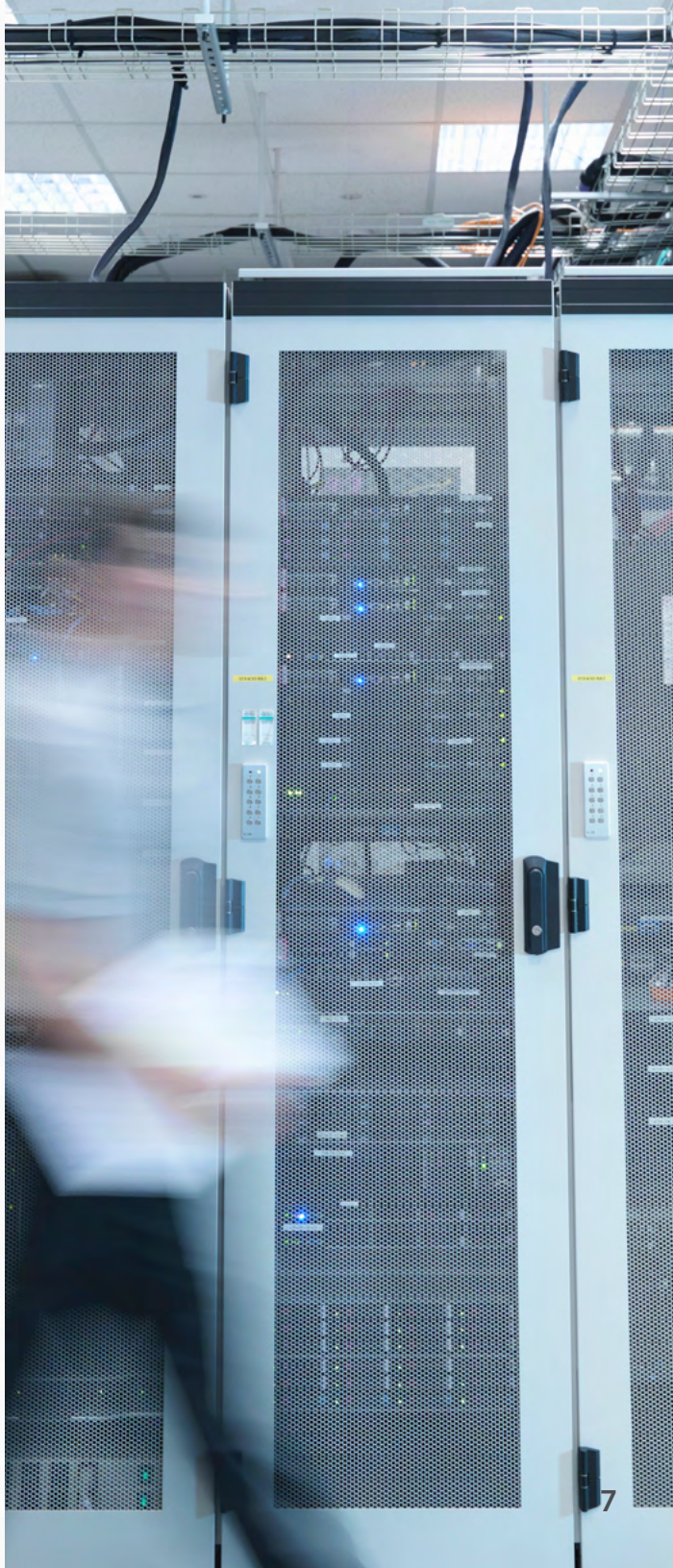
IT部門は通常、インフラストラクチャを追加することで低パフォーマンスのネットワークの問題を解決しますが、この方法では、複雑さやコストが追加されるだけでなく、セキュリティリスクも増大します。このやり方をいつまでも続ければ、アジリティやイノベーションが損なわれ、競争力が低下してしまいます。

この傾向がこの数か月間にCovid-19によって加速し、大半の従業員がリモートワークに移行し、金融サービス業界でもMicrosoft 365の導入が加速しました。

結果として、次のような問題が発生しました。

- VPNベースのリモートアクセスソリューションは、ビジネスに必要なサービスレベルを提供できず、レイテンシとユーザエクスペリエンスが低下した
- リモートコンピュータをオンネットワークにするVPNベースのリモートアクセスは、エンドポイント感染の主なベクトルであることが古くから知られているが、在宅勤務の増加によってさらに状況が悪化している
- Microsoft 365は多くのやり取りが発生するプロトコルであるため、許容可能なサービスレベルを提供するには、高帯域幅と低レイテンシが必要になる
- 「ハブ&スポーク」アーキテクチャの拡張には、多額のコストがかかり、最終的には必要なSLAを提供できなくなる
- 既存のセキュリティアーキテクチャの対象領域の拡大により、特にトロイの木馬攻撃に対する脆弱性が高くなり、内部関係者の脅威を完全に保護することもできない

多くのIT担当者は、ハブ&スポークアーキテクチャでは今日の分散型クラウドやモバイル環境に対応できず、リモートユーザのサポートが困難で、ネットワークトラフィックの増加に合わせて拡張できないことに気付いています。けれども、アーキテクチャのトランスフォーメーションのニーズを上昇させる理由は、従来型のインフラストラクチャの保護の課題とコストだけではありません。IT部門は、多様化する動的で複雑な環境で様々な新しいイノベーションを可能にするアーキテクチャを設計し、実装する必要があります。その目標は、自然言語の理解と処理、ビッグデータの収集、パターンの識別、解釈、理解、論証、助言をリアルタイムに実現し、次世代のガイド付き学習、運用テクノロジ、ロボティクス、ウェアラブルなどをサポートできるデジタル環境を構築することにあります。



5 セキュリティとユーザエクスペリエンスの適切なバランス

銀行、保険会社、その他の金融サービス機関は当然ながら、膨大な量の顧客の資金や財務情報を保持し、管理しています。

犯罪者より常に先行し、金融関連の厳格な法規制を常に順守するという絶え間なく進化する課題を抱えているため、金融機関がサイバーセキュリティに最も多くの予算を投入していることは驚きではありません。

新しいデジタル開発は、脆弱性を悪用しようとする犯罪者に新たな機会を与えることになります。従業員に宛てたフィッシングメールが成功すれば数秒で認証情報が攻撃者の手に渡り、情報漏洩やランサムウェア攻撃、あるいはその両方の標的になる恐れがあります。しかしながら、ユーザエクスペリエンスを損なうことなく、中核となるビジネスプロセスとアプリケーションをモバイルやリモートの従業員がコスト効率の高い方法で安全に利用できるようにするにはどうすればよいのでしょうか。

複数のセキュリティ手順が必要な方法では、ユーザエクスペリエンスが大きく損なわれ、顧客や従業員が不満を感じ、生産性が大きく低下する可能性があります。IT部門の責任者は、セキュリティとユーザエクスペリエンスはどちらも提供できるものではあるものの、両方を同時に達成するのは容易ではないと認識しています。

Zscaler Zero Trust Exchange の詳細はこちら

6 SASEとゼロトラストによるセキュリティとユーザエクスペリエンスの両立

SASE（セキュアアクセスサービスエッジ）は、アプリ、デバイス、ユーザが従来のネットワーク境界の外を移動することに起因するセキュリティの課題を解決する、ガートナーによって定義されたセキュリティモデルです。

Zscaler Zero Trust Exchange
の詳細はこちら

SASEアーキテクチャは、包括的なWAN機能にセキュアWebゲートウェイ、CASB、FaaS（Firewall-as-a-Service）、ZTNA（ゼロトラストネットワークアーキテクチャ）などのネットワークセキュリティ機能を組み合わせることで、デジタルエンタープライズの動的なセキュアアクセスのニーズをサポートします 。

従来のネットワークアクセスとは異なり、ゼロトラスト適応型ビジネスは、ブローカ接続を処理し、ユーザ、デバイス、場所、アプリに基づいてアクセスを許可することで、ユーザをオンネットワークにすることなく、あらゆる場所で働く許可されたユーザに高速で安全なアクセスを提供します。ZTNAでは、Webは信頼されないトランスポートとなり、アプリケーションへのアクセスは、サードパーティプロバイダがコントロールする中間クラウドサービスまたは自らがホスティングするサービスを経由します。

このモデルでは従来のVPNのハードウェアや面倒なプロセスが不要になるため、シームレスなプロセスが実現し、ユーザエクスペリエンスが向上します。

ZTNAは、リソースへのコントロールされたアクセスを提供し、接続を強化し、アプリケーションをインターネットに直接公開する必要性を排除し、攻撃対象領域を少なくします。パンデミックを契機に多くの組織に採用され、リモートや自宅で働く従業員も本社で働く従業員と同じレベルのセキュリティコントロールで中核となるアプリケーションにアクセスできるようにする目的で利用されるようになりました。ZTNAは今日、企業が全社的に採用するベストプラクティスの標準になりつつあります。データセンタ、プライベートアプリ、パブリッククラウドのいずれにユーザがアクセスし、オフィスあるいはリモートのどちらで働く場合も、同じユーザエクスペリエンスが実現します。

ZERO TRUST EXCHANGE

ゼットスケーラーのZero Trust Exchangeは、ビジネスポリシーを使用して、ユーザ、デバイス、アプリケーションを任意のネットワーク経由で安全に接続する、専用に設計されたクラウドベースのSASEプラットフォームです。高速かつ安全でスケーラブルなこのプラットフォームは、組織におけるセキュリティの優先事項とユーザエクスペリエンスを両立させ、クラウドを利用した安全なビジネスの遂行を可能にします。

7 ゼットスケーラーを選択すべき理由 — はじめに

仮想通貨を処理する新しい金融サービスソリューションの開発、新しい境界を超えたサービスの提供、不正の防止、あるいは新しい法規制のコンプライアンスプロセスの管理のいずれを目的とする場合であっても、金融サービス機関は、堅牢性、アジリティ、スケーラビリティを備えた最新プラットフォームを採用し、イノベーションを加速させて競争力を強化することで、自らの戦略を推進する必要があります。

ゼットスケーラーのSASEベースのZero Trust Exchange**は、世界中に分散する150を超えるデータセンタを利用して10年以上にわたって運用されてきた、世界最大のインラインクラウドセキュリティプラットフォームであり、1日に1億件以上の脅威をブロックしています。このプラットフォームは、1日に1,500億以上のトランザクションと1億7,500万のセキュリティアップデートを処理しており、これは全世界で処理されるGoogle検索の10倍に相当します。**

ゼットスケーラーは、金融サービスの分野で豊富な実績を誇り、500以上の金融サービス分野のお客様、米国の銀行の上位10行中6行、ヨーロッパの銀行の上位10社中7行、オーストラリアの銀行の上位5行中2行が自社の金融インフラストラクチャでゼットスケーラーのZero Trust Exchangeを利用しています。ゼットスケーラーは全業種において、Forbes 2000の上位企業の450社を含む、185か国の4,500のお客様の信頼されるパートナーです。ゼットスケーラーのZero Trust Exchangeは、あらゆる場所のユーザ、デバイス、アプリケーションをビジネスポリシーを私用して安全に接続することで、サイバー攻撃やデータ損失から何千ものお客様を保護しています。

このプラットフォームの主なメリットは、既存のアーキテクチャに追加することでデジタルトランスフォーメーションが瞬時に加速し、効率的かつ安全で顧客中心のスケーラブルなサービスを提供できる点にあります。

- **効率性：**ITを簡素化し、複雑さを軽減し、コストを削減します。
- **セキュリティ：**複数の部門のセキュリティポスチャの単一ビューを提供することで、耐障害性とセキュリティポスチャを強化し、データ損失やセキュリティリスクを軽減します。
- **顧客中心：**WFA（Work From Anywhere）環境をサポートし、処理能力を向上させ、レイテンシを短縮し、一貫性あるユーザエクスペリエンスを提供することで、生産性の向上を実現します。
- **スケーラビリティ：**デジタルイノベーションを支援し、デジタルトランスフォーメーションを加速させ、成長を可能にする、アジリティを備えた最新プラットフォームです。

Zscaler Zero Trust Exchange
の詳細はこちら

ナショナルオーストラリア銀行（NAB）は、オーストラリア、ニュージーランド、アジアの一部、英国、米国で事業を展開し、資産管理を含む銀行/金融関連の商品やサービスを統合して提供しています。

Covid-19のロックダウンに直面した同行は、従業員の在宅勤務を短期間で可能にし、900万人以上の顧客へのサービスの提供を継続する必要がありました。

NABでEGMインフラストラクチャ、クラウド、ワークプレイスを担当するSteve Day氏は、次のように述べています。「Covid-19のパンデミック以前は、5,000人を超える従業員にリモートワークは認められていませんでした。コンタクトセンタの従業員が自宅で問い合わせの電話に対応できるようにし、アプリやデータストアへのリモートアクセスを可能にする方法をすぐに見つけなければなりませんでした。これらすべてを、通常の4倍の電話による問い合わせを処理しながら進める必要がありました」

NABはゼットスケーラーを導入し、コールセンタチームを含む32,000人以上の従業員に安全なリモートアクセスを提供する作業をわずか3週間で完了しました。NABはゼロトラストの採用により、将来の運用をサポートするインフラストラクチャを構築しつつ、コストと攻撃対象領域を削減することができました。

「ゼロトラストには2つの大きなメリットがあります。1点目として、社内のネットワークをわけて運用する必要がなくなるため、大幅なコスト削減が実現します。新しいモデルでは、オフィスにおいてもパブリックインターネットアクセスのみを提供しています。2点目として、高価なセキュリティインフラストラクチャをインストールすることなく、すべてのデータとアプリケーションを行内の環境から削除して、攻撃対象領域を少なくすることで、セキュリティポスチャを強化できました。安全なネットワークインフラストラクチャを手に入れることができたため、現在の危機的な状況のみならず、正常に戻った後のNABのサポートにも役立ちます」

EGMインフラストラクチャ、クラウド、ワークプレイスを担当するSteve Day氏は、次のように述べています。「従業員は自宅で自分のPCの電源を入れ、オフィスとまったく同じように仕事を始められます。ログインの手順が追加されることも、セキュリティトークンを使う必要もなく、仕事を進められます」

ナショナルオーストラリア銀行

オーストラリア、メルボルン、ナショナルオーストラリア銀行

nab.com.au

8 合併・買収

Zscaler Zero Trust Exchange
の詳細はこちら

金融サービスは合併、買収、事業売却が一般的な業界ですが、内部のアプリへのユーザによる接続や機密データの保護を担当するネットワークチームやセキュリティチームは、多くの課題に直面します。

多種多様なネットワークのコンバージェンス、重複するIPアドレスの管理、一貫性あるセキュリティ標準の策定は、ITが直面する課題の一部に過ぎません。プロジェクトには時間もリソースも必要で、完了までに数か月から数年を要することも少なくありません。

このような複雑な移行では、速さ、セキュリティ、ユーザエクスペリエンスが何よりも重要です。ゼットスケーラーを選択することで、合併・買収・事業分割プロジェクトが大幅に簡素化されます。

- ソフトウェアを導入し、ユーザをアプリにルーティングするだけです。数分で作業が完了でき、ネットワークの統合はまったく必要ありませんでした。
- 標準化されたセキュリティですべての資産を保護します。承認されたユーザだけにアプリが表示され、ユーザがオンネットワークになることはありません。
- デバイス、アプリ、場所に関係なく、一貫性あるユーザエクスペリエンスでアクセスが提供されます。

9 デジタルトランスフォーメーションで次に何を目指すか？

金融機関はパンデミックへの対応を短期間で可能にしましたが、ITチームやセキュリティチームは当時を振り返り、ニューノーマルへの適応が成功だったことを検証しようとしています。

特定のソリューションの導入が成功すると、デジタルトランスフォーメーションの次の段階に目を向けるようになります。将来のイノベーションを支える最新のインフラストラクチャの構築が、最重要課題となります。

5Gの普及や、金融サービス業界で運用テクノロジ、高度なロボティクス、ウェアラブルなどの顧客中心のイノベーションの採用の増加に伴い、新たな課題やセキュリティの脆弱性が明らかになります。サイバーセキュリティは今後も、金融機関が直面する上位のリスクの1つであり続けるでしょう。

今日のニーズに対応できるだけでなく、世界中の金融機関を支援してリードするビジョンと能力を備えた、信頼できるインフラストラクチャベンダと協力することが、これまで以上に重要になります。

業界のビジョナリであるITリーダーに、デジタルトランスフォーメーションの次の段階について質問しました。

WFA（Work from Anywhere）のリソースをもっと見る

10 今すぐ行動すべき理由

対策を何も講じなければ、インフラストラクチャやMPLSのコストの単純な増加、生産性の低下、あるいはサイバー攻撃からの復旧コストといった形で不利益を被ることになります。

WFA（Work from Anywhere）のリソースをもっと見る

今すぐ行動することで、セキュリティポスチャを直ちに強化し、組織全体のセキュリティを単一ビューで把握しつつ、リモートワークのニューノーマルの効果的なサポートが可能になります 。

それと同時に、将来を見据えたIT投資によってスケーラブルな新しいアーキテクチャへの移行を可能にし、ビジネスの優先事項や新しいイノベーションを加速させることができます。

法規制のコンプライアンス

金融業界の独立系の規制団体が、金融機関や金融サービス業界の効果的かつ一貫性ある規制と監督に取り組んでいます。これらの団体により、業界を代表する組織からの意見に基づき、クラウドテクノロジの採用、CSP（クラウドサービスプロバイダ）へのアウトソーシングのプロセスと実践、クラウドにおけるリスクの管理と測定に向けた原則に基づくアプローチの採用に関するガイダンスと推奨事項が策定されています。

Zscalerーは、堅牢なセキュリティとプライバシー保護と、現在および新たに発生する法規制に関連するリスクとコンプライアンスに対応するサポートを提供することで、お客様のコンプライアンスの取り組みを支援します。さらには、明確な情報とベストプラクティスサポートを提供することで、ゼットスケーラーのソリューションの導入と管理のガバナンスフレームワークへの適合を保証します。

第1版：2021年3月22日

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.jp