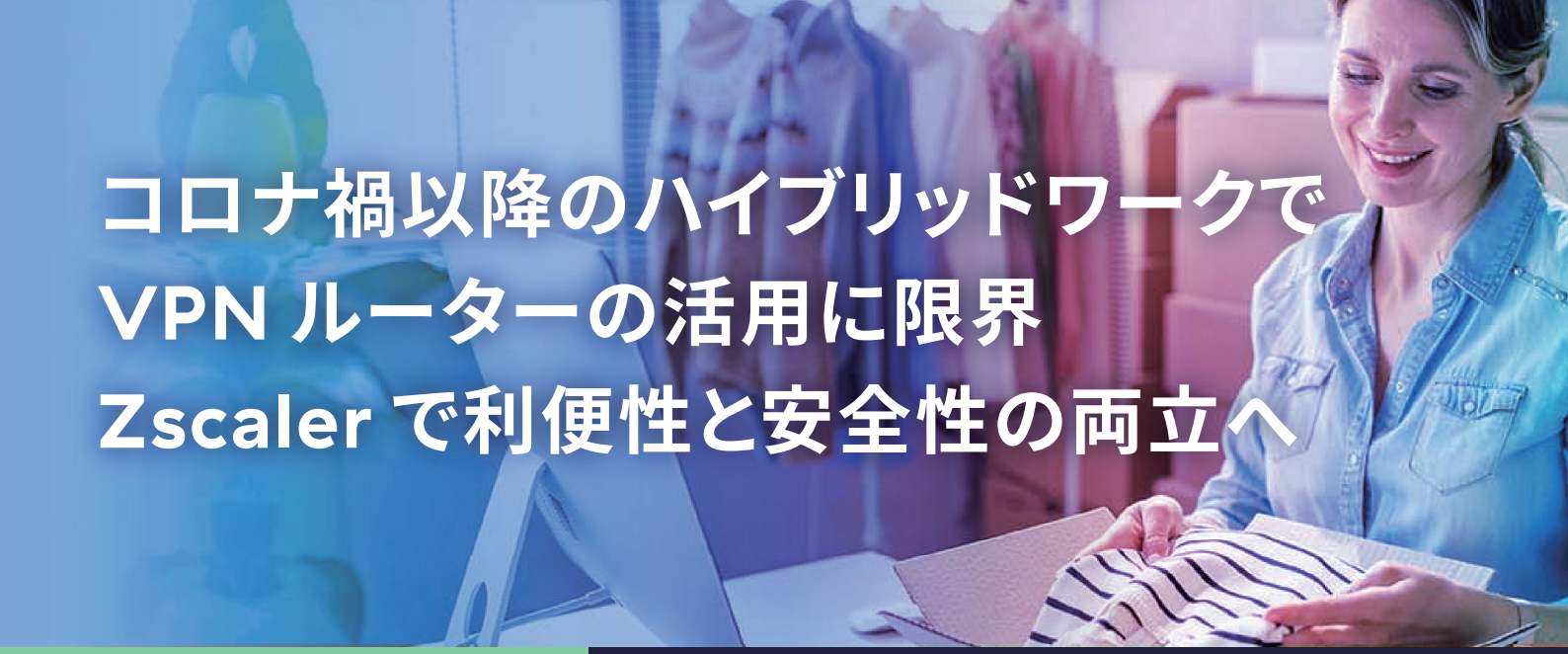

コロナ禍以降のハイブリッドワークで VPN ルーターの活用に限界 Zscaler で利便性と安全性の両立へ

主な課題

・コロナ禍のハイブリッドワークでVPNによる帯域圧迫が顕著に。一方で、全通信のログを取得しながらシャドーITの可視化を行うなどセキュリティ対策の強化も望まれていた。最新ツールを利用できる自由度とセキュリティ強化の両立を目指す必要があった

効果

・Zscaler導入後は、VPN利用時にあった切り替えがなくなり、利便性を向上

・全通信のログ取得やシャドーITの把握ができることで、セキュリティインシデントへの対応を正確かつスピーディに

・ネットワーク遅延の原因をすぐに切り分けられるようになったほか、BCP対策としても期待されている

“ハイブリッドワークを支えるセキュリティとして VPNに代わるソリューションを求めていました”

Zscalerのソリューションで業務利用の利便性を向上させ 安全性の担保も同時に実現しました。

栗原 寛昇 氏

BASE株式会社 Corporate Infosys Group マネージャー

ネットショップ作成サービス「BASE」、購入者向けショッピングサービス「Pay ID」、オンライン決済サービス「PAY.JP」（※）等の企画・開発・運営をするBASE。「BASE」は誰でも簡単にネットショップが作成できることから2023年末時点で210万を超えるショップに利用が広がっている。コロナ禍を機に全社的なWFH（Work from home）をスタート、現在までオフィス出社とWFHのハイブリッドワークを継続している。そこで課題として浮上したのが自宅からリモートアクセスのためのVPNの扱い。VPNによる帯域圧迫のため、業務によってVPNを接続/切断する必要が生じた。そこでBASEグループではZscalerソリューションを導入、VPNを経由しない通信でもログを取得できる安全性と利便性を兼ね備えたIT基盤を構築した。

※「PAY.JP」は100%子会社のPAY株式会社が提供しています。

zscaler™

BASE

BASE株式会社

https://binc.jp/

本社所在地：東京都港区六本木三丁目2-1 住友不動産六本木グランドタワー
従業員数：274名（連結 / 2023年12月31日現在）
業種：Webサービス企画・開発・運営

導入ソリューション

Zscaler Zero Trust Exchange™
Zscaler Internet Access™（ZIA™）
Zscaler Private Access™（ZPA™）
Zscaler Digital Experience™（ZDX™）

コロナ以降のリモートアクセス対応 VPNルーター利用からの脱却が課題

簡単にネットショップを作成できる「BASE」をはじめとしたWebサービスを提供するBASE。同社でCorporate Infosys Groupマネージャーを務める栗原 寛昇氏は、「コロナ禍ではEC（電子商取引）サイトのサービスへの需要が急激に高まり、反響は非常に大きなものでした。引き続き、多くのオーナーにご利用いただいています」と堅調なビジネス成長の状況を語る。

BASEでは、従来から一部の営業担当者向けにVPNルーターを使ったリモートアクセス環境を提供していたが、コロナ時代を迎えて全社に拡張して活用することになった。「全社への拡張と従業員数の増加からVPNによって帯域が圧迫し、VPNルーターを入れ替えても接続が不安定な状況となっていました」（栗原氏）。

実際、VPNで社内システムに接続しながら、Web会議などを行うと帯域の圧迫から通信の遅延などの不具合が生じるようになった。また、「Web会議中はVPNを切る」といった運用を求めたため、業務中にVPNの接続・切断を繰り返すことになり、従業員の不満や生産性の低下につながっていった。BASE エンジニアの濵谷 淳氏は、「VPNを使うとすべてのトラフィックが会社のネットワークを経由するために、帯域を圧迫していました」と語る。

そこで、セキュリティ機能とネットワーク機能を1つのクラウドサービスに統合させるSASE（Secure Access Service Edge）の検討を始めたという。

「会社のネットワークを経由しない外部のVPNを用いる場合、通信ログが取れなくなります。ハイブリッドワークを推奨する以上、どこで作業していてもログが取れる状態を維持していくべきと考え、セキュリティ強化も考慮してSASEを検討したのです」（濵谷氏）。

エンジニアが安心して最新ツールを使える 便利かつ安全な環境を目指す

SASEの導入には、もう1つ狙いがあったと濵谷氏は語る。「BASEはIT系の企業で、エンジニアが多くいます。ITツールやSaaSの利用に基本的には制限を設けておらず、新しいものを検証してほしいというスタンスです。これは開発の自由度が高い一方で、野良SaaSの利用など会社として管理できないシャドーITの存在にもつながります。これらを可視化して、状況を把握したい思いがありました」

情報漏洩対策としても、ITツールの利用ログが取れていれば、ツール側とユーザー側の問題を切り分けることができる。BASE システムエンジニアの武内 将毅氏は、「SASEの導入でアクセスログを監視されるのでは？という現場の危惧はありました。しかし、社員を守るためにも状況を把握する必要があることを説明して、理解を広めていきました」と振り返る。

“IT企業として最新テクノロジーは必須 開発の自由度とシャドーIT可視化の両立が必要でした”

ITツールやSaaSの利用に制限は設けていない分、 野良SaaS利用などの状況把握が求められていました。

濵谷 淳 氏

BASE株式会社 Corporate Infosys Group エンジニア

zscaler™

製品の検討段階では、Zscaler製品以外にも7製品ほど説明やデモの紹介を受けたという。その上で、固定IPでSaaSなどにアクセスできる要件や、ユーザーインタフェースの使い勝手を調べて絞り込んだ。最終的にはZscalerともう1製品が残り、検証することになった。検証での評価について、濵谷氏はこう語る。

「エンジニアについては、サービスやサイトを制限なく使えるようにする必要があります。しかしプレ導入したZscalerの競合製品では、エンジニアが使うGitHubやDockerなどでエラーが出てしまい、その都度、除外設定する状況になりました。作業が大変なだけでなく、これではセキュリティの担保ができません。一方のZscaler製品はトラブルなく動きました」。開発系の現場にはZscalerが適していることを実感したという。

さらに、プレ導入したことでZscalerの使いやすさや融通の効きやすさも実感した。「レポートの機能が豊富で、特別な手間をかけず、いつでもレポートを見られます。例えばCTO（最高技術責任者）向けのレポートがデフォルトで用意されていて、加工の手間がかからないことは大変ありがたい点でした」（武内氏）。

VPNの切り替えがなく利便性向上
トラブル切り分けからBCP対策まで効果

BASEでは2023年にZscalerを検証環境から本格導入へと進めていった。リモートアクセスのセキュリティをVPNからZscaler Private Access™（ZPA）によるクラウドサービスに移行。また、社内とインターネットのアクセスをZscaler Internet Access™（ZIA）で制御することで、シャドーITの把握を行う。これらにより、すべての通信のログが取得でき、セキュリティインシデントへの対応や予測が可能になった。さらにZscaler Digital Experience™（ZDX）により、ユーザーエクスペリエンスの調査やベンチマークを可能にした。

栗原氏は、「社員からは、業務でVPNを切り替える必要がなくなって楽になったという声を多くもらっています」と語る。武内氏も「Zscaler導入後、VPNの障害や遅延に関する問い合わせがなくなりました」と安定した稼働についても評価する。

ZDXの導入効果も上がっている。「ネットワークが遅延した際、原因が自宅かオフィスか、SaaS側なのかということがZDXですぐに確認できるので、明確な指示ができるようになりました。もちろんレスポンスも高めることができました」（武内氏）。

当初は狙っていなかったメリットも生じている。「ビルの保守点検で停電になるケースが年に数回ありますが、そうしたときに従来はVPNルーターが動かず、24時間稼働している部署の業務に支障がありました。Zscaler移行後は、ビル施設の稼働状況にかかわらず業務を継続できます。これは障害時や緊急時のBCP（事業継続計画）の面から、有効だと考えています」（濵谷氏）。

情報漏洩対策への取り組みも進む。クレジットカード番号などの漏洩をパターンマッチングで止めるDLP（Data Loss

*“ネットワーク遅延の問い合わせにも
原因がすぐに分かり、明確な返答が可能になりました”*

*ZDXでは、ネットワーク遅延も原因がどこにあるのか
すぐに切り分けられます。*

武内 将毅 氏

BASE株式会社 Corporate Infosys Group エンジニア

zscaler™

Prevention）ソリューションの導入で、情報の安全性を確保する。Zscalerの DLPでは、流出する情報がクレジットカード番号やマイナンバーなどの機密情報である場合に流出を防止できる。このEDMを導入することで、自社が持つクレジットカードなどの情報の流出を強固に防ぐ備えを作ります」（武内氏）。

今後は、Zscaler製品との連携によるエンドポイントセキュリティの強化や、多方面のログデータから脅威を自動検出して通知するSIEM（Security Information and Event Management）ソリューションの導入も視野に入る。また、ネットワーク経由に限らず、クライアント端末経由の機密データの可視化並びに漏洩対策を実現するZscaler Endpoint DLPの導入も検討している。「当社が提供するサービスは、ショップオーナー様や購入者様のEC・決済をサポートしているため、国内外のどこに拠点があっても業務ができることが求められます。どこでどんなデバイスをつないでもセキュリティが担保されてログが収集できる環境が必要です」（濵谷氏）。こうした環境を整えていくためにも、Zscalerの将来性に期待を寄せている。

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 ZeroTrust Exchangeは、ユーザ、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、何千人も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で動作するSASE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.jpをご覧いただくか、Twitterで@zscalerをフォローしてください。