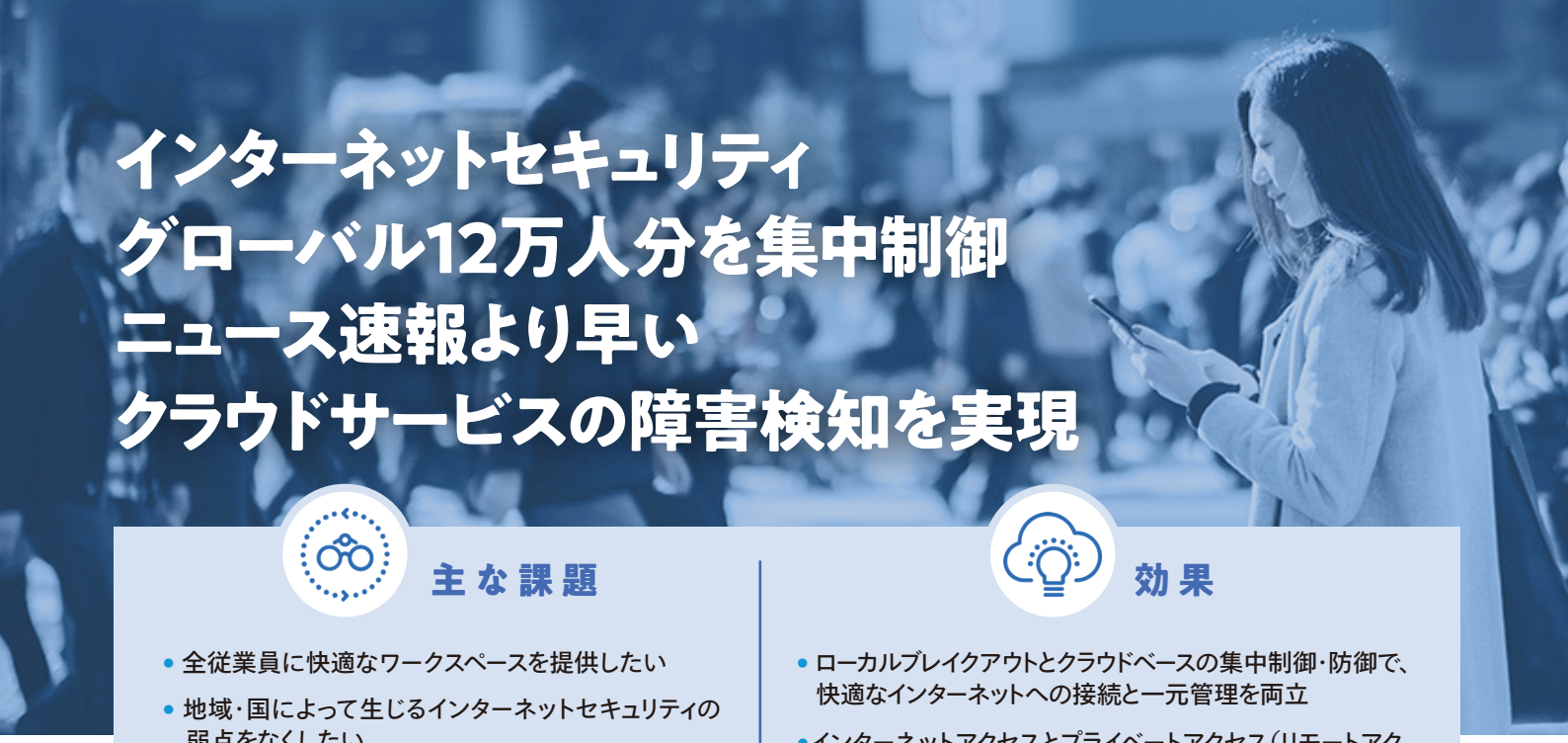


インターネットセキュリティ グローバル12万人分を集中制御 ニュース速報より早い クラウドサービスの障害検知を実現

主な課題

- 全従業員に快適なワークスペースを提供したい
- 地域・国によって生じるインターネットセキュリティの弱点をなくしたい
- 国内で実現した先進的な施策を素早くグローバル展開したい
- クラウド・テレワークへのシフトによって「いつ、どこで、何が」起きたか把握できなくなっていた

効果

- ローカルブレイクアウトとクラウドベースの集中制御・防御で、快適なインターネットへの接続と一元管理を両立
- インターネットアクセスとプライベートアクセス（リモートアクセス）の経路分離と集中制御により通信を最適化
- 端末→社内、自宅ネットワーク→インターネット→クラウドの通信品質を区間ごとにHop by Hopで見える化し、「いつ、どこで、何が」起きているかを可視化。障害対応の迅速化を実現

“システムはクラウド、働く場所はリモートに分散する中、安全性の強化が求められました”

従業員の快適さやビジネス継続性よりも機能制限・部分最適が求められた古い基盤から脱却するため、ネットワークもクラウドにシフトしました

田中 夏生 氏, CISSP

日本電気株式会社
コーポレートIT・デジタル部門
CISO統括オフィス
ネットワークセキュリティグループ長
兼 働き方DX開発センター
ネットワークサービスグループ長
ディレクター

グローバルで約12万人の従業員を擁するNECグループでは、従業員の安全性と利便性を両立する信頼性の高いネットワークインフラを実現する一環として、Zscalerのソリューションを活用。インターネットへのアクセスを保護する「Zscaler Internet Access（ZIA）」、プライベートアクセスを保護する「Zscaler Private Access（ZPA）」に続き、端末からクラウドまでを監視する「Zscaler Digital Experience（ZDX）」を導入した。セキュリティ機能をクラウド上に集約することで、国内外に分散する人・データ・ITリソースを集中的かつ一元的に監視・制御できるようにした。同時に、ビジネスに欠かせないWeb会議などクラウドサービスの稼働状況を可視化し、従業員のデジタルエクスペリエンスにかかわる障害の早期検知と対応を可能にした。また、ZIAによるフィルタリング・脅威防御の状況をサイバーセキュリティダッシュボードで全社員に公開、セキュリティカルチャー変革に活用している。

Orchestrating a brighter world

NEC

日本電気株式会社

https://jpn.nec.com/

本社所在地：東京都港区芝5-7-1
従業員数：連結118,527名(2023年3月末現在)
業種：ICT

導入ソリューション

Zscaler Zero Trust Exchange™
Zscaler Internet Access™
Zscaler Private Access™
Zscaler Digital Experience™

zscaler™

利便性と安全性を両立できるインフラと運用体制を整備

働きがいの実感を高めていく「Smart Work 2.0」を推進しているNECは、新たな働き方として社員が働く時間と場所を自律的にデザインし、リモートとリアルを最適に組み合わせるハイブリッドワークを定着させてきた。グループ全体で12万人に上る従業員の働く場所やデータ、ITリソースがグローバルに分散する中で、いかに集中的に監視・制御できるかが重要である。そのためには、ビジネスの安全性と利便性を両立させるかがポイントだった。

そこでNECグループでは、従業員のクラウド活用を促進する利便性と、分散するリソースを集中制御する安全性を両立するためのビジネスインフラ基盤を従来的な推定ベースの信頼でなくゼロトラスト志向で真に信頼のおける「Truly Trusted Network」としてグローバルな運用体制の整備を進めてきた。例えば、オフィスとテレワーク、クラウドとオンプレミスの違いがセキュリティリスクや従業員のストレスにならないためのアクセス環境の整備や、グローバルでのトラフィック監視や障害対応などの取り組みを進めている。

Truly Trusted Networkではゼロトラストの考え方に基づき「ハイブリッドワークのビジネスインフラ環境を安全性・可用性の両面で真に信頼できる(Truly Trustedな)状態にシフトすることを目標にネットワーク整備を進めています」(図1)とNECグループ全体のネットワークセキュリティ基盤の導入・展開を担う田中 夏生氏は説明する。

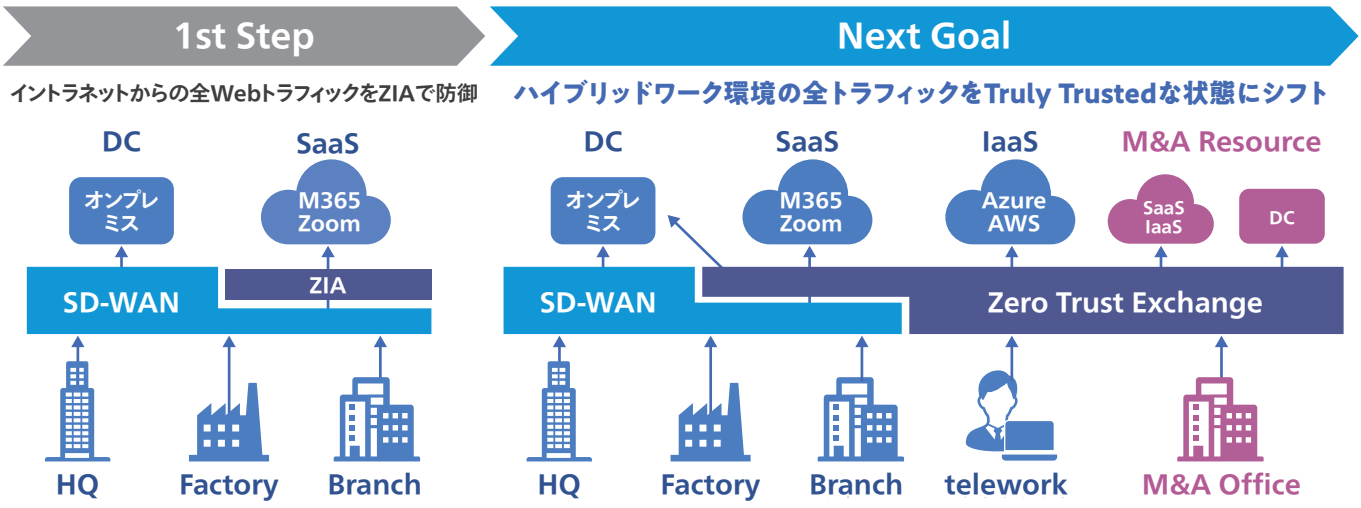
サイバー攻撃に対する安全性と従業員の利便性を両立

Truly Trusted Networkの実現に向けてネットワークセキュリティの整備を段階的に進めている同社は、第1弾として2018年4月にインターネットアクセスを防御するための「Zscaler Internet Access(ZIA)」を導入。国内と海外にある全拠点からSaaS(Microsoft 365、Zoom、Box、Salesforce)を含むインターネットへのアクセスすべてを、ZIAを介する形に整備した。

このZIAの導入により、セキュリティの向上とユーザーエクスペリエンスの向上を実現。セキュリティ面ではサイバー攻撃への対策を強化し、各拠点からのWebトラフィックに対し、ZIAのWebフィルタやサンドボックス、APT(脅威対策)機能を活用している。また、そのログはグローバルのSIEM基盤上に集められ、常にリスク解析の対象となっている。例えばマルウエアと外部サーバーの不正な通信を検知した場合、日本とシンガポールの混成チームからなるグローバルCSIRTが即座に通信を遮断し被害の拡大を抑制、被害を受けた従業員に対しては迅速に被害調査・対策を実施するグローバルなレジリエンス対応を可能にした。

ユーザーエクスペリエンスに関しては、昼休み時間に頻繁に発生していたWebレスポンスの遅延を、Zscalerの潤沢かつ継続的に強化されるリソースを活用することで大幅に改善。ブラウザの表示待ちを60～70%を短縮し、国内の通信速度としてはZIA導入前にはおよそ1Gbpsであったものが、導入直後には

図1. NECのゴールイメージ



zscaler™

3Gbps、現在は約30Gbpsにまで向上しているという。さらに「ZIAの導入でSSL暗号通信を可視化できるので、かつてのように事前申請することなくSNSや動画サイトの閲覧が可能になるなど、アクセスできるコンテンツの拡大にも貢献しています」と田中氏は成果を語った。

ストレスなくSaaS/DCの安全な接続を実現
多数VPN装置の脆弱性対応の負担から解放

ZIAに続く第2弾として、2020年10月から利用を開始したのが自社データセンター（DC）やIaaSへ安全にリモートアクセスできる「Zscaler Private Access（ZPA）」である。

NECグループではかつて国内・海外の各拠点にマルチベンダーのVPN装置を配置していた。しかし、多くの国では持ち出されたPCのSaaSへの通信を防御する仕組みを入れず、社内向けのVPNと同時接続できる構成であったため、防御されていないインターネット通信を経由して社内が攻撃されるリスクがあった。

VPN接続時はDC上のSWG（Secure Web Gateway）で強制的に防御するケースもあったがその場合は「SaaS通信が遅くなる」「DCの回線が圧迫される」といった課題が存在していた。またVPN装置の脆弱性が発見された場合、各国にある機器で対策をとる必要があり、大きな負担と対策完了までのリスクが生じていた。これをZPAで解消したのだ。「Zscalerのソリューションにより、リモートアクセスの性能問題の解消と安全性を両立しています」と田中氏は評価する。

> *“ ハイブリッドワークでは、どこで何が起こっているのか障害発生時の切り分けが困難です ”*

Zscalerのソリューションで通信経路を可視化し、迅速な障害の検知・復旧・周知を可能にしています

田中 夏生 氏,CISSP
日本電気株式会社

SaaSの障害の早期検知・可視化で
ビジネスの継続に貢献

クラウドの活用とハイブリッドワークが進む一方、NECでは新たな課題も表面化していた。従業員のIT環境やアクセス先のクラウドサービスが複雑に分散し「どこで何が起こっているのか分からず、障害発生時の切り分けや社内報告もままならないのが実情でした」と田中氏は打ち明ける。例えば従業員からWeb会議にアクセスできないと連絡があった場合、従業員宅のネットワークに問題があるのか、Web会議サービスに問題があるのかすぐに切り分けできず、従業員や経営層に事実に基づいた説明が難しい場面もあった。

こうした課題に対応するために導入したのが「Zscaler Digital Experience（ZDX）」だ。ZDXは従業員の利用状況を正確に監視し、パフォーマンスの最適化や、アプリケーション、ネットワーク、デバイスに起因する問題を迅速に特定して修復するソリューションである。

ZDXでは従業員の端末にインストールされたZscaler Client Connectorとクラウド基盤で、端末からネットワーク、インターネット、クラウドサービスまでの通信経路を監視。「通信経路をHop by Hopにドリルダウンすることにより、どこで何が起きているかを特定できます。そして、実測に基づくダッシュボードの俯瞰情報を使って、障害の発生から復旧までの検知と社内への周知がスピーディに進められるようになりました」と田中氏はZDXによる通信品質の可視化の意義を強調する。

ZDXを導入して間もなく、あるベンダーのクラウドサービスが障害を起こし、Web会議やメール、ストレージなどのアプリケーションが利用できなくなることがあった。「そのときにもZDXにより、外部のニュースで速報として伝えられるより早く社内で障害発生を検知することができました。他のベンダーのWeb会議は問題なく利用できたので、その旨を社内に周知して障害の影響

を最少化するなど、ビジネスの継続に貢献しました」と田中氏はZDXの導入効果を話す。障害情報をいち早く従業員に通知することで「なぜつながらないのか」というストレスを軽減するだけではなく、運用部門への問い合わせを減らすことにもつながっている。

社内周知の迅速化の実例

従来

- 障害発生　1時間後に正式通知
- 復旧　5時間後に正式通知

ZDX導入後

- 障害発生　速報はリアルタイム、20分後に正式通知
- 復旧　速報はリアルタイム、20分後に正式通知

※速報はZDXのAPI経由で監視情報を自動掲載

従業員への周知は、NECが独自に開発したITダッシュボードを活用。SaaSやIaaSなどの監視ツールの結果を表示するほか、APIを用いてクラウドと端末間の通信品質などZDXの情報をほぼリアルタイムに表示することができる。

NECグループでは今後、グローバルな自社DCのクラウド統合やM&Aで取り込んだ企業とのアプリケーション共有などの課題解決に向け、Zscalerのソリューションを活用していくという。

自社の導入実績とノウハウを生かしZscalerソリューションを外販

さらにNECでは、こうしたグループ内における導入実績や活用ノウハウを生かし、Zscalerソリューションの提供も行っている。1つは、ZIAとZPAの導入・構築をパッケージ化したお客様向けのメニューの提供だ。NECセキュリティ事業統括部の長谷川 謙治氏によれば「通常のSIに比べ、低価格かつスピーディに導入できます。Zscalerのソリューションは、社内のオンプレミスと社外のインターネットを同じセキュリティポリシーでガバナンスを効かせられるので、導入したお客様からも高く評価されています」という。

このほかにも、前出の独自開発のITダッシュボードとZDXを組み合わせて提供することも視野に入れており、自社活用を超えて、多くの顧客企業の課題解決にZscalerを活用していく考えだ。

> *“NECグループの導入実績やノウハウに基づく提案が可能です”*
>
> *Zscalerは社内、自宅、外出先を問わず、同じセキュリティポリシーで作業環境を防御できるので安心です*

長谷川 謙治 氏
日本電気株式会社
セキュリティ事業統括部
プロフェッショナル

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 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。