株式会社 TKC 様

約１万か所の全国会計事務所の業務生産性向上支援を目指し、TKC 全国会会員に向けたインターネットブレイクアウトによるユーザエクスペリエンス向上と安全性確保の両立を短期間で実現

「富士通とシスコと当社の連携がうまく機能し、お客様に特に意識させることもなくサービスの機能を強化し、業務効率化支援が実現しました。」

株式会社 TKC
執行役員システム開発研究所副所長
兼　技術研究・開発支援センター長
魚谷 仁司氏

全国の会計事務所と地方公共団体に専門特化した情報サービスを展開している株式会社 **TKC**（以下、**TKC**）。「自利利他」を社是として社会的責任を強く意識した事業展開を行う同社は今回、**TKC** 全国会会員に提供する「セキュリティゲートウェイサービス」の機能強化策として **Cisco Umbrella** をベースとした富士通の **DNS** セキュリティを導入。インターネットブレイクアウト方式による快適なアクセス性と、**DNS** セキュリティによる安全性強化を実現した。

導入事例概要

導入製品	DNS セキュリティソリューション

課題 1	課題 2	課題 3
アクセス集中による遅延を解消、セキュリティを強化し、顧客である会計事務所の業務生産性向上に貢献したい	既存環境への影響を最小限にとどめ、コストを抑えて早期にサービス提供したい	約１万か所の全国会計事務所への展開を、顧客の負荷を最小限に、かつ短期間で実現したい

効果 1	効果 2	効果 3
センター集約型からインターネットブレイクアウト方式に変更し、快適なアクセス性と DNS セキュリティによる安全性強化	**クラウド型サービスを採用することで、クライアントレスでの導入が実現でき、早期の導入とコスト抑制**	**各会計事務所側ルータの設定変更自動プログラムを開発し、検討開始から 2 ヶ月という短期間で全体の約 7 割に展開**

導入の背景

ネットワークトラフィック増大に伴い、センター集約型セキュリティ構成の改善が求められた

株式会社 **TKC**
執行役員
システム開発研究所副所長
兼 技術研究・開発支援センター長
魚谷 仁司氏

執行役員 システム開発研究所副所長 兼 技術研究・開発支援センター長の魚谷仁司氏は、同社の事業およびその役割について「当社は 1966 年の創業以来、会計事務所と地方公共団体の 2 つの分野に専門特化した情報サービスを展開し、わが国の情報産業界に確固たる地位を築いてきました。会計事務所の社会的使命の達成とその関与先企業の健全な発展を支援するという目的のもと、現在約 9,900 の TKC 会員事務所（TKC 全国会に所属する税理士・公認会計士事務所）にオンラインシステムを提供し、60 万社を超える関与先企業の決算申告を支えています。この分野は、会計・税務の専門知識と深い経験が必要であり、常に法令に完全準拠した専門的なシステムを提供しなくてはなりません。税理士、公認会計士、地方公務員の業務遂行を、情報通信技術を活用しながら支援し、社会の発展に寄与していくのが当社の役割だといえます。その中では当社が、自前でリソースの確保が難しい TKC 会員事務所の情報システム部門であるという意識で活動しています。」と語る。

この思想はセキュリティ対策にも貫かれていると、システム開発研究所技術研究・開発支援センター IT ソリューション技術部長の長川英司氏は次のように話す。「秘匿情報を多く取り扱う会計事務所においてもデータ消失や漏えいを回避するため、新たな脅威への対策が求められています。

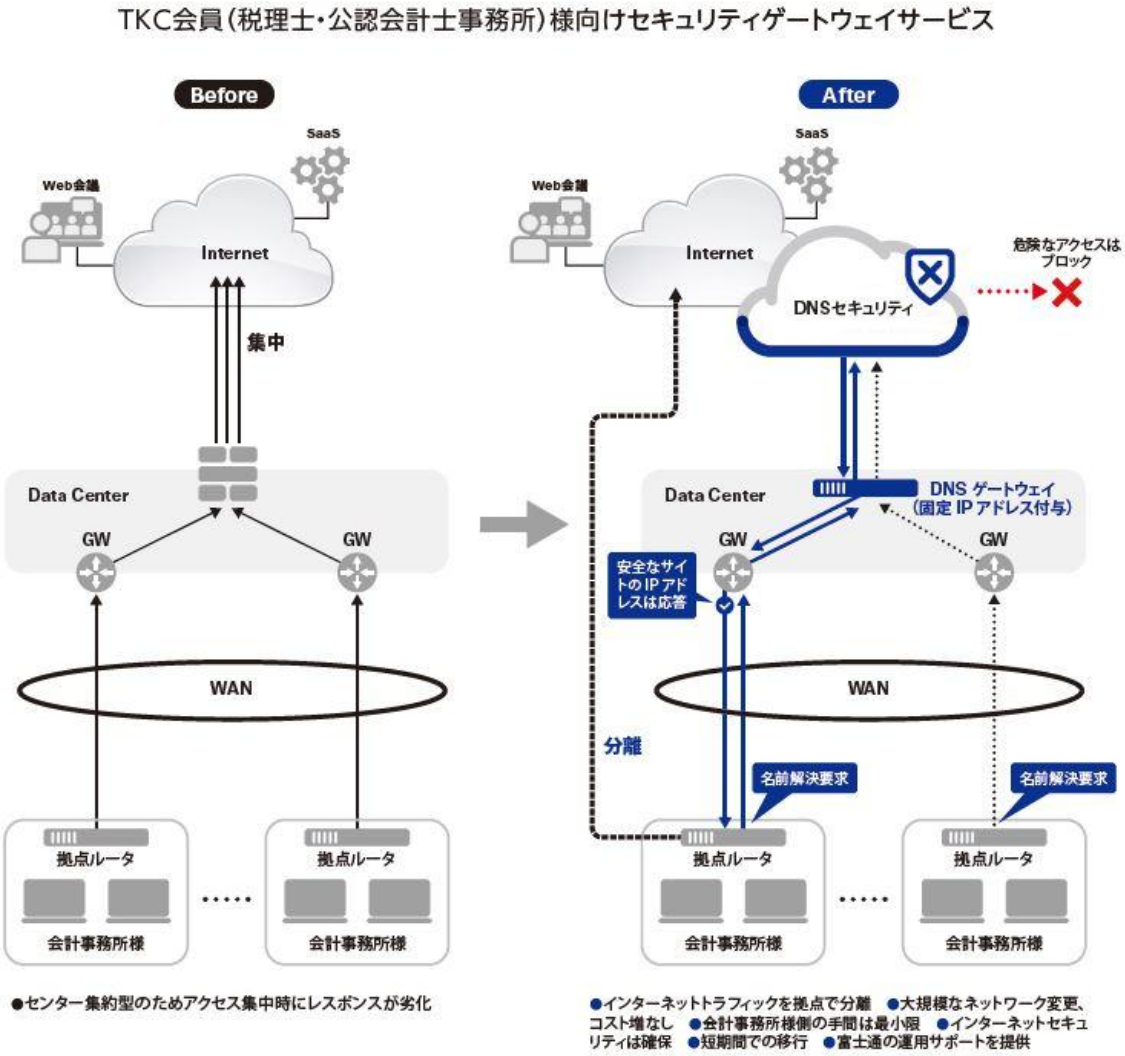
そこで当社では、一般的なウイルス対策ソフトでは検知することが難しい新種のウイルスを振る舞いから検知するサービス、IPA が提供する『情報セキュリティ 5 か条』（注 1）の項目をチェックし、ソフトウェアの脆弱性などの課題を可視化するサービスなどを組み合わせ、『TKC サイバーセキュリティサービス』として会員の方々に無償で提供しています。」

そして今回は、同社ネットワークサービスの 1 つである「セキュリティゲートウェイサービス」の強化に取り組んだ（図）。長川氏は、今回の強化策の背景をこう説明する。「従来のすべてのインターネット通信を当社のデータセンター経由で行うセンター集約型のセキュリティ構成は、トラフィックが集中するとレスポンスが遅延してしまう課題がありました。また、増加する SSL 暗号通信のチェック対策も懸案でした。2019 年頃からゼロトラストセキュリティ、SASE（注 2）などの概念に基づく製品が登場し、導入検討を重ねていたさなか、コロナ禍を受けて働き方が大きく変わり、テレワークや研修オンライン化などでトラフィックが急増。そこでデータセンター経由のインターネットアクセスを、各会計事務所側のルータからダイレクトに接続するインターネットブレイクアウト方式に変更することとし、その前提でいかにセキュリティ性を維持するか、具体策の検討に入りました。」

導入のポイント

インターネットブレイクアウト方式に変更し、快適なアクセス性と DNS セキュリティによる安全性強化を実現

各会計事務所から直接インターネットにアクセスするインターネットブレイクアウトを採用することで、各種のクラウドサービスおよび TKC ネットワーク経由で利用する業務アプリケーションの帯域確保が可能になる一方、データセンターのセキュリティ設備を経由しなくなることでインターネット向け通信に既存のセキュリティ機能が適用されなくなるリスクが生じる。この解決策として同社が採用したのが、富士通の DNS セキュリティだ。



これはシスコが提供するクラウド型 DNS セキュリティ Cisco Umbrella をベースとした、富士通のセキュリティサービスだ。TKC は創業当初から富士通とのつながりが深く、富士通が提供する企業向けネットワークサービス「FENICS」の開発時からのメインユーザーでもある。本プロジェクトも TKC と富士通の両社が連携し、検討が進められた。

長川氏は数あるセキュリティ製品から本サービスを採用した理由を、次のように語る。「クラウド型で提供され、機器の調達や構築が必要なく、コストを抑えての導入が可能であることに加えて、本サービスには他社製品と比較して 2 つの優位性がありました。1 つはサービスの安定性。従来のセキュリティ装置よりチェックが甘くなっては本末転倒ですから、新旧の仕組みをつないで細かく検証しました。具体的には新たな仕組みでは検知のみを、停止は従来の仕組み側で行って、通信ログを比較しました。その結果、双方で特性の違いはありましたが、新しい仕組みでも高い検知率が確認でき、問題ないことが判明しました。もう 1 つは導入後のサポート。セキュリティ製品には必ず過剰検知という課題を伴います。その際にシスコ側と連携し、どのような復旧処

理を行ってくれるかを富士通に確認しました。その結果、過剰検知だった場合は通信停止の速やかな解除や正当な理由の報告を受けるなど、納得いくフローを提示いただけたことで、採用に踏み切りました。」

株式会社 **TKC**
システム開発研究所
技術研究・開発支援センター
IT ソリューション技術部長
長川 英司 氏

本サービスの実装にあたっての最大の課題が、利用者である各会計事務所のインターネット接続が動的 IP アドレス方式である点。そのため、当初はローミングクライアント方式での導入が検討されたが、数万に上るユーザ側の端末へのインストール作業を伴うため、顧客側の業務に多大な影響が及ぶ懸念があった。

この解決策として富士通は、固定グローバル IP アドレスを付与した DNS ゲートウェイ装置をデータセンター内に配置。Cisco Umbrella に対する名前解決要求（DNS クエリ処理）はこの DNS ゲートウェイ装置経由で行い、インターネットへのアクセスは各事務所からのインターネットブレイクアウトにて実行する仕組みを開発した。これにより、ローミングクライアントのインストール不要で、Cisco Umbrella のセキュリティポリシーが全利用者に適用される。

もう 1 つの導入時のハードルが、全国の会計事務所に 1 万台近く設置されているルータの設定変更。前述の通り会計事務所側は動的な IP アドレス方式のため、一括での設定変更ができない。約 150 台を対象に事前調査したところ、計 19 パターンの設定仕様が必要なことが判明した。長川氏はこの課題を乗り越えた方策について、次のように話す。「当社側の全国の SE が訪問して 1 台ずつ設定変更を行うことも検討しましたが、コロナ禍ではそれも難しい状況でした。そこで、計 19 パターンの設定を自動で行う独自プログラムを開発しました。センター側から各ルータにアクセス、各 IP アドレスの体系を読み取った上で、必要な更プログラムを判別してそれぞれの会計事務所の希望した時間に更新するものです。これにより、当社側だけでなく利用されるお客様側の負荷を最小限に、かつ短期間での設定変更が実現しました。」

導入の効果

約 2 か月で 7 割に展開完了、アクセス性改善に加え脅威傾向の把握によるセキュリティ対策強化も実現

本サービスは、2021 年 12 月下旬より提供を開始。事前の取り組みが功を奏し、開始から約 2 か月間という短期間で全国約 1 万台のルータの約 70%の設定変更が完了。その後も順次作業を進め、2022 年 6 月末に全台の設定変更が完了し、サービスが利用されている。

長川氏は今回のプロジェクトの成果を、次のように評価する。「検討開始からサービス提供まで約 2 か月というスピード感は、クラウドサービスならではの価値だと思います。ちょうど 12 月から 3 月という会計事務所の繁忙期にサービス展開が重なったのですが、この間、1 件の事故もなく無事に設定変更が完了し、従来よりも安全、快適にネットワークやアプリケーションをご利用いただけるようになりました。従来に比べ、過剰検知や誤検知でアクセスできないといったヘルプデスクへの問い合わせも少なく、そうした事態になった際も富士通がシスコと連携してすぐに原因を究明、対処してくれるため、以前よりも対応が早くなりました。アクセスできない場合も明確な理由をお客様にご説明できることで、満足度も高くなりました。」

富士通では TKC 側から問い合わせがあると、シスコの TAC（注 3）や Talos（注 4）と連携し、過剰検知や誤検知の場合は通信停止を解除、正当な理由がある場合は、その理由を回答する。要する期間も中 1 日程度と、従来よりも早期での対応が実現している。

また、長川氏はその他の成果として通信状況と脅威傾向の可視化を挙げる。「従来は我々が直接、管理画面を確認することができず、すべて富士通から報告を受けていましたが、本サービスではダッシュボードから、当社側でもリアルタイムに状況が把握できます。通信ログからブロックされた対象のサイトがわかることで脅威の傾向が把握でき、安心です。『Emotet（エモテット）』と呼ばれるウイルスへの感染を狙う攻撃メールが騒がれたときも被害が及ぶことなく、成果を実感しました。」

魚谷氏は総評として「そもそもセキュリティサービスはご利用になる側からすると何も変化がなく、プラスの効果は特に意識もされない部分なのですが、万一業務に支障を来たすことになれば、多大なご迷惑をおかけするマイナスの事態となります。その意味で今回のプロジェクトは、お客様に特に意識させることもなくサービスの機能を強化し、業務効率化支援が実現しました。これも富士通とシスコが当社とうまく連携していただいたおかげだと思います。」と語る。

今後の展望

フラットでシンプルなネットワーク化で顧客に安心、安全な業務環境を提供したい

最後に魚谷氏は、今後の展望と富士通への期待について、次のように結んだ。「当社では今後、ゼロトラストの考え方を基本とし、従来の閉域網からオープンかつフラットでシンプルなネットワークに変えて行こうと検討しています。富士通とは創業以来長いお付き合いがあり、我々のお客様の業務全般を支援するという思想や企業文化も理解していただいています。これからもそうした背景を汲み取った上で、当社会員の皆様が安全に、安心してビジネスが展開できるテクノロジーやサポートの提案に、期待しています。」

脚注

注 1　IPA 情報セキュリティ 5 か条
注 2　SASE：Secure Access Service Edge の略
注 3　Cisco TAC：Technical Assistance Center/シスコのお客様、パートナー、および代理店に対するテクニカル サポート サービス
注 4　Cisco Talos：250 人を超えるセキュリティ専門家が所属する世界最大規模のデータ解析を行っている脅威インテリジェンス組織

株式会社 TKC 様

本社所在地　栃木県宇都宮市鶴田町 1758 番地
設立　1966 年 10 月 22 日
従業員数　2,398 名
URL　https://www.tkc.jp/

［2022 年 9 月 7 日掲載］

本事例中に記載の肩書きや数値、固有名詞等は取材日現在のものであり、このページの閲覧時には変更されている可能性があることをご了承ください。

お問い合わせ先

製品・サービスについてのお問い合わせはコチラ
富士通株式会社　〒211-8588　神奈川県川崎市中原区上小田中 4-1-1