Netskopeの導入でテナントを可視化
クラウドを安心して活用できる環境を構築

導入事例 +

JALグループのIT中核会社として、航空オペレーションに欠かせないシステムの開発から運用、保守までを手がけるJALインフォテック。そのノウハウはJALグループ内にとどまらず、空港管理会社や他業種・他業界でも広く活用されています。一方、クラウドの活用にともない「データの可視化」という課題に直面してきた同社は、Netskopeを導入。課題を解消し「安心感」を手に入れる一方、Netskopeをより一層活用することでさらなるセキュリティ強化を目指しています。

境界型セキュリティの限界が露呈
クラウドを前提としたセキュリティ構築が課題に

JALインフォテックの業務は、JALグループにおける航空オペレーション向けシステムの開発・運用・保守が中心です。航空会社ではお客さまの予約をはじめ、航空貨物の取り扱いや航空機の整備・運航、客室乗務員のスケジュール調整など、あらゆる業務がITで運用されているため、同社が果たす役割は非常に重要なものとなっています。またJALグループ内で培ったノウハウは、空港管理会社向けの業務システム、一般企業向けのコールセンターシステムやIT資産管理ソフトウェアにも生かされています。

このようにグループ内外で幅広いIT関連業務を行うJALインフォテックにとって、避けて通れないのがクラウドの利用と、それにともなうセキュリティの問題です。サイバーセキュリティ戦略の策定を担当している八谷嘉則氏は、同社が抱えていた課題についてこのように語ります。

「当社では、これまで境界防御型を前提としたセキュリティシステムを運用していました。しかしGmailやMicrosoft365が導入されてクラウドにデータが出るようになると、出て行くデータをどう保護するかが課題になります」。

同じ課題を抱える他社との意見交換を通して、CASBの存在を認識していたという八谷氏。しかし実際にCASBの導入に踏み切った背景には、もうひとつの理由があります。サイバーセキュリティ戦略の責任者である小泉和也氏が、当時を振り返りこのように語ります。

「きっかけになったのはコロナです。急遽VPNを増強して境界型のセキュリティを継続しようとしたのですが、在宅勤務への急激なシフトでビデオ会議利用など想定以上のトラフィックが発生することで、VPNやインターネット接続部分がボトルネックになりました。VPN依存のセキュリティ対策でクラウド利用の拡大自体が無理であることが分かり、CASBの導入を加速することになりました」。

JAL INFOTEC

組織概要

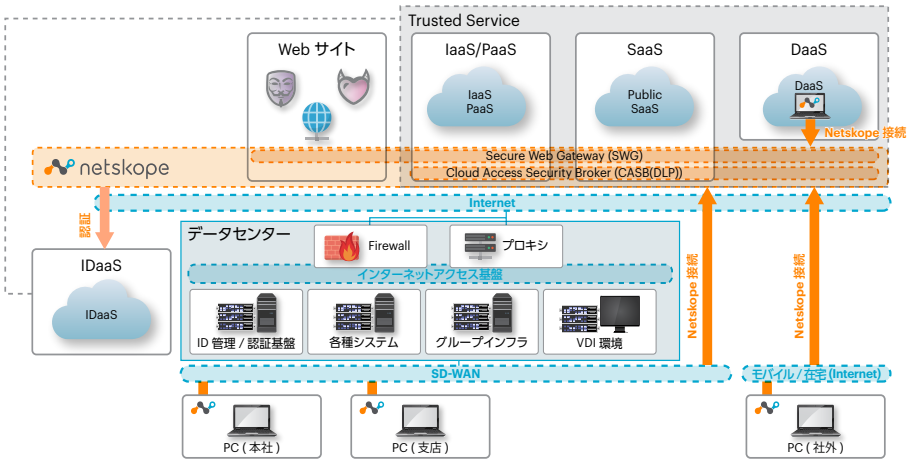
業界	地域	設立	従業員数
テクノロジー	グローバル	1978年	975名 (2023年10月1日現在)

株式会社JALインフォテック
(現:JALデジタル株式会社)
https://www.jalinfotec.co.jp/

株式会社JALインフォテック
サービス事業本部
IT基盤事業部
セキュリティ統制部　部長
小泉 和也氏

株式会社JALインフォテック
サービス事業本部
IT基盤事業部
セキュリティ統制部
セキュリティ戦略グループ
マネージャー
八谷 嘉則 氏

システム構成図



業界で評価が高いNetskopeに注目
「テナントが見えること」が導入の決め手に

2020年にCASB導入に向けて動き出したJALインフォテック。コロナ禍に後押しされた形ではあるものの「もともとこのタイミングでセキュリティ戦略を立てる予定だった」と八谷氏は語ります。とはいえセキュリティ担当の人員が限られていたこともあり、プライオリティをつけて年次で進めていくことにしたそうです。

「初年度はEDRの整備から始めました。メール経由でエンドポイントにデータが届くため、エンドポイントのセキュリティを強化したいと考えたためです。CASBの導入はその次のタイミングとしました」。

CASB製品の選定にあたり、八谷氏が参考にしたのはガートナー社が発行する「マジック・クアドラント」。掲載されていたセキュリティ製品の中から、

- 日本にセールスのチャネルがあること
- 市場でもある程度のシェアを確保していること
- リーダー格の企業にも認められている製品であること

以上の要件を満たすソリューションを探した結果、Netskopeにたどり着きました。その後はNetskopeをベンチマークにして、他社製品を比較するという流れで検討を進めたそうです。

当初より「選ぶならNetskopeだろう」（八谷氏）と感じていたというものの、実際に選定の決め手となったのは「テナントの可視化」でした。

「たとえばGmailの場合、URLをいくら引いてみてもGmailであることしか分かりません。ですがNetskopeだとそれがプライベートのGmailなのか、あるいは自社なのか他社なのか、テナントまできちんと識別できます。Gmailに限らず、各クラウドサービスでテナントが見えるという点に重きを置いて評価を行いました」。

加えてデコードしたSSL通信とDLPと組み合わせることで、データの中身を見た上で「取り扱ってはいけないような情報」を検知できることも高く評価したと、八谷氏は語ります。

Netskopeが原因のトラブルは一切なし！
データの流れとテナントの可視化が安心感に

JALインフォテックがNetskopeを導入したのは2022年5月のこと。前年から社内での簡単なPoCと販売代理店の協力による本格的なPoCを実施し、同社が求める仕様をきちんと満たしていることは十分に確認していたといいます。「本格導入の直後は証明書系の問い合わせが度々発生しましたが、Netskopeが原因のトラブルは発生していません」と八谷氏は語ります。

PoCではSSLデコードした結果がきちんと可視化されているか、SWGの中でセキュリティリスクのあるサイトがリアルタイムにブロックされるかを確認しました。さらにNetskopeのクライアントがVDI環境でも動くかどうかを確認しました。

本格導入後もPoCで確認した通りの性能が発揮されていると語る八谷氏。ユーザーがセキュリティリスクに該当するサイトにアクセスした場合でも、それをきちんとトラッキングでき、止められているといいます。

「SWGは実環境で運用しないと、誤・過検知などの評価が難しいと認識しており、本番運用には不安がありましたが懸念は杞憂に終わりました。またグループ内で競合製品も運用しており個別の悪性URL情報等を入手しますが、確認するとNetskopeのセキュリティリスクカテゴリに既に登録されており、自動的に接続をコントロールできているという点で、大きな安心感を持てるようになりました」。

またクラウドサービス間のデータの動き、たとえばJALインフォテックが契約しているストレージサービスからクライアントのストレージにデータを渡すような場合でも、

- どのユーザーがどのようなデータを流しているか
- だれ（どのテナント）がデータを受け取ったか

というところまで可視化されるため、「やはり運用している側として安心」できると八谷氏は語ります。

CSPM導入や構成管理の取り組みが今後の課題
クラウド時代に最適化したセキュリティ環境へ

テナントの可視化と、クラウド上のデータの流れの可視化に成功したJALインフォテック。しかしセキュリティ対策はまだ終わりではありません。八谷氏は「今後は、IaaS/Paas/SaaSに対するセキュリティ対策が必要だと感じています。CSPM/SSPMの導入など、構成管理の部分でどのように取り組んでいくかがポイントですね」と語ります。

今後はNetskopeのさらなる活用を含め、システムの再構築やパラメーターのチューニングを通して、クラウド時代に最適化されたセキュリティ環境を構築したいと考えています。

*株式会社JALインフォテック（現：JALデジタル株式会社）、2023年9月時点の事例です。

netskope

SASEのグローバルリーダーであるネットスコープは、ゼロトラストを原則としてAI/MLを活用したデータ保護を行っています。サイバー脅威から企業を守り、セキュリティとパフォーマンスを妥協することなく両立し最適化に導きます。1つのプラットフォームで新たなエッジネットワークの構築、リスクの低減、そしてあらゆるクラウド、ウェブ、アプリケーション通信において卓越した可視性を提供します。詳しくはnetskope.com/jpをご覧ください。