

全日本空輸株式会社

社内にタスクフォースチームを立ち上げ、世界中の3万台の端末を東京から管理

全日本空輸株式会社(以下、ANA)は、タニウムのソリューションを全面的に採用し、全世界の事業所、空港カウンター、および社内業務で使用するWindows端末約3万台の最新状況を迅速に把握できる体制を整えた。業務アプリの配信にタニウムを活用することで、業務コストの大幅な削減も成し遂げている。



脅威に侵入された後に いかに迅速に対処できるか

ANAグループの行動指針で真っ先に出てくる言葉は、「安全」だ。人とものを運ぶ航空運送事業者として、安全な運航はすべてに優先する。その姿勢はITにおいても同様だ。全世界で約3700万人におよぶ顧客の個人情報や蓄積する情報プラットフォームの保護はもちろんだが、最も注力すべきは空港カウンターに置かれた端末や従業員に貸与するPCなどのIT資産、標的型攻撃やランサムウェアなどの脅威は、保護の脆弱な端末を入り口にするケースが多いためだ。

2010年代に入ったころから、端末のセキュリティ事情は大きく変わってきた。脅威の多様化が進み、ゼロデイ攻撃も頻発するようになった。そうすると、静的なパターンファイルによるウイルス駆除では間に合わなくなる。ANAでは常に最先端の対策を実施してきたが、このような急速に移りゆくトレンドを精緻に把握した上で、将来の脅威とその対策のありべき姿を見据えることになった。

デジタル変革室 企画推進部 担当部長 和田 昭弘氏は、「端末の挙動を見極めて不審なところがあれば知らせてくれる振る舞い検知型のツールも導入しました。しかし、脅威も進化しており、極力不審な動きをせずに感染を広げるものもあります。防御壁を突破し、振る舞い検知をすり抜ける脅威にも対処する“衛生管理”の必要性に気づき、タニウムを採用しました」と話す。

瞬時に“今の状態”をつかむ

ANAがタニウムを使用し始めたのは2016年。当時は、EDRという言葉もまだ一般化しておらず、多くの企業は“防御”に関心を寄せていた。その中で同社は、「万全の防御はするが、それで完璧とは言えない。侵入された後にいかに迅速に脅威を発見し、対応するかが問われる」という立場で方針を策定したことになる。タニウムを世界中の支社、空港カウンター、従業員のPCなど、ほぼすべての端末に展開し、東京のセキュリティ拠点から一括監視できるようにしたのだ。

導入後ほどなく、その成果を華々しく示す出来事があった。2017年5月、ランサムウェアのWannaCryが世界中の企業を震え上がらせた。最新のセキュリティパッチを適用しているPCは被害を免れたが、世界中で数十万台のパッチ未適用PCが感染し、名だたるグローバル企業も被害を受けた。事の大きさが報じられると、ANAは即座にタニウムを使って世界中の端末を検査。1時間とかわからず、すべてが安全であることがわかったため、被害がなかったことをまとめて迅速に経営層に報告することができた。

もちろん、日常的に発生する小さなインシデントには都度対応しており、タニウムの価値を感じるシーンも多かった。そのため、同社は「タニウムでやれること」の範囲を拡大していく。データの配布やソフトウェアのインストールなど、タニウムのソリューションをフル活用して業務効率を高めているのだ。

企業プロフィール

1952年の創業以来、安全運航を第一に航空運送サービスを提供してきたANAはお客様の満足度にもこだわるためDX推進に力を注ぎ、2018年に「攻めのIT経営銘柄」、2019年に「DXグランプリ」、2020年は「DX認定」「IT賞」を獲得。コロナがもたらす人々の行動変容により、航空需要の「量」と「質」の変化が予想されることから、ANAグループのビジネス・モデルを変革し、グループ全体の事業ポートフォリオを見直すことで、感染症の再来にも耐え得る強靱な企業グループに生まれ変わろうとしている。

導入製品

Tanium Core
ITオペレーション
リスクとセキュリティの製品

導入効果

全世界の事業所、空港カウンター、および社内業務で使用するWindows端末3万台にタニウムを導入。端末の最新情報を瞬時に取得して瞬時に対策を取る態勢を整えた。コロナ禍における在宅勤務者のユーザビリティとセキュリティをどちらも確保するために活用するなど、さまざまな成果を挙げている。

デジタル変革室 企画推進部 情報セキュリティ・基盤戦略チーム マネージャー 三宅 慎也氏は、「海外拠点の中には、社外へつながるネットワーク速度が256kbpsのところもあります」と話す。タニウムは業務に支障を与えないよう帯域を制限し、決めた帯域内で安定的にファイルを配布できる。細い管を通して1つの端末に完全なデータを送った後に、快適な事業所内ネットワークで事業所内の端末へ順にコピーしていくイメージだ。「実際にはゆっくり確実に送ってくれるわけですが、体感としては“スピーディー”なのです。以前は保守員を派遣し、現地で数日をかけてセットアップすることもありましたが、いまではすべてタニウムで実行しています」。

これは人的負担の削減という成果の1つだが、ほかにもさまざまな面でタニウムは価値を提供している。万一脅威に侵入されても該当する端末をリモートで論理抜線できる安心感、フォレンジックを外部に委託する必要がなくなったことによる業務のスピードアップおよびコスト削減などだ。2021年には、コロナ禍における在宅勤務のユーザビリティとセキュリティをどちらも確保するために、端末のIT管理・運用、有事のインシデント対応にタニウムを活用し始めている。

“ タニウムの価値を引き出すためには、セキュリティとテクノロジーの知識が要求され、実際に運用するとなれば業務知識も必要です。これから育てたいのは、そんなスキルのある人。これら2つの視点を持ち、スピーディーな意思決定もできる人材です

デジタル変革室 企画推進部 情報セキュリティ基盤戦略チーム マネージャー 三宅 慎也 氏

日本を守っていくくらいの気持ちで

ANAでは、三宅氏がリードして“タスクフォースチーム”を機能させ、プロセスの規定やユースケースの拡大など、さまざまな改善活動を適時に行ったことが成功につながった。そして、成果を上げながら適用範囲を拡大したことで、徐々にタニウムを使いこなせるエンジニアも増えてきた。今後はセキュリティをさらに向上させるという視点でセキュリティ運用とIT運用の連動性をさらに高め、常に運用改善を図ることのできる組織モデルを構築したい考えだ。

三宅氏は、「タニウムの価値を引き出すためには、セキュリティとテクノロジーの知識が要求され、実際に運用するとなれば業務知識も必要です。たとえばランサムウェアに感染したPCを発見した場合、システム側の見方で対処しようとするシステム構成から影響範

囲を考え始めてしまいます。しかし、実際には業務をどの順番でどう止めて、影響をどうカバーするのかと考え、そのための対策を迅速に実行する必要が出てきます。これから育てたいのは、そんなスキルのある人。これら2つの視点を持ち、スピーディーな意思決定もできる人材です」と話す。

人を育てながら、タニウムの活用も加速する。現在、Tanium EnforceとTanium Complyを導入中。前者はポリシーに基づくセキュリティパッチの適用に使用し、後者は全端末の脆弱性診断に活用する計画だ。これにより、ANAはタニウムをフルに活用する土台を整えることになる。

和田氏は、「情報漏えいやランサムウェアなど、セキュリティ関連のニュースがメディアを騒がせています。これらはANAグループだけではなく、社会全体として取り組むべき課題です。いつの日かサイバー攻撃がなくなるように、他社様との連携も進めています」と話す。三宅氏は、「その一環として、昨年1年間、企業横断のITセキュリティ研修を受けさせていただきました。セキュリティは、ビジネスで競合する相手とも協力する分野です。これからもコミュニティに貢献し、日本を守っていくくらいの気持ちで取り組んでいきます。そして、そのような機会に、タニウムの使い方を含めて皆と議論していきたいと考えています」と話してくれた。

(右) 全日本空輸株式会社
デジタル変革室 企画推進部 担当部長
和田 昭弘 氏

(左) 全日本空輸株式会社
デジタル変革室 企画推進部
情報セキュリティ基盤戦略チーム マネージャー
三宅 慎也 氏



お問い合わせ



タニウム合同会社
〒141-0021 東京都品川区上大崎3-5-11 目黒ヴィラガーデン5F

<https://www.tanium.jp>
jpmarketing@tanium.com