CASE STUDY

日本電気株式会社：
全世界26万台の端末をTaniumで一元管理し、サイバーハイジーンを徹底

会社名

日本電気株式会社

業種

情報・通信

従業員数

連結 約10万人

本社所在地

東京都港区

導入ソリューション

Tanium Cloud Core
Discover
Patch
Deploy
Asset
エンタープライズサービス

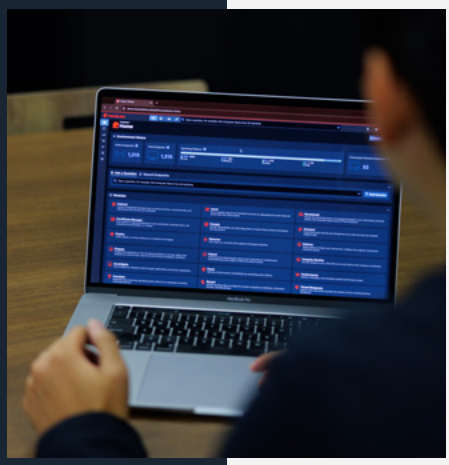
日本電気株式会社（以下、NEC）は、全世界の約26万台の端末の状況や脆弱性をTaniumで可視化して管理。パッチ配信にかかる時間を以前の2週間から4～5日に短縮し、非管理端末を検出して管理下に置くなど、大規模な環境でサイバーハイジーンを徹底している。

NECは、社会価値創造型企業として「Orchestrating a brighter world」というメッセージを掲げている。安全・安心に代表されるさまざまな社会価値を提供し、社会の中で人々が豊かに生きることをサポートすることが同社の使命。中期経営計画に記されたDX推進プランでも、社内で実現したDXを社会へと還元することがうたわれており、中でもセキュリティは最重要事項のひとつとして位置づけられている。

実際に、セキュリティソリューションの提供は同社の強みであり、社内ITにおいてもセキュリティに力を入れてきた。自ら活用することでソリューションの強みを知り、ノウハウを得た上で顧客に提案できるというメリットもある。エンドポイント管理施策は2002年にスタート。国内企業の中でも先駆的な取り組みを進めてきた。

「当社では26万台を超えるデバイスを管理しておりますが、IT資産の稼働状況や脆弱性を常に正確かつ最新の状態で把握し続けることは、極めて高度な運用が求められる課題です。しかしながら、エンドポイント管理は、サイバーリスクの最小化および事業継続性の確保に直結する重要な要素であり、経営リスクの観点からも優先的に取り組むべき領域と認識しています。」と、NEC Corporate Executive CISOの淵上 真一氏は語る。

NECグループのすべての端末を一元管理



Taniumの導入当時に抱えていた課題は、大きく3つあった。セキュリティ対策として脆弱性を正確に把握すること、IT資産管理を徹底しどこにどんな端末があるのかを把握すること、そしてパッチ適用などの現場の作業負荷を軽減することだ。

これらの課題を解決すべく、NISTサイバーセキュリティフレームワークをベースに課題を洗い出し、対策の方向性を明確化したところ、NECグループのすべての端末を一元管理するソリューションとしてTaniumが最適だと判断し、導入に至ったという。

負荷を大幅に軽減し管理を強化

Tanium導入後の変化について、CISO統括オフィス長の田上岳夫氏は「以前はパッチの配信に2週間ほどかかっていましたが、Taniumを使うことで4〜5日へと短縮できました。パッチはサイレントに適用でき、プロセスも見直したことで、現場の工数も15分の1以下に削減できました」と話す。

以前のツールでは、配信したことは記録されているものの、適用されたかどうかまではわからなかったが、Taniumを使えばパッチの適用状況に加え、さまざまな情報を取得できる。「"パッチが確実に適用されている"ことも確認できるようになりました。Taniumを使えばさまざまな情報をすばやく取得でき、まさに"かゆい所に手が届くソリューション"です」。

シャドーITが可視化できることもTaniumのメリットだ。CISO統括オフィスマネージャーの林杏奈氏は、「ネットワーク上にあるデバイスなら、存在の把握だけでなく、だれがその端末を管理しているのかを確認して管理下に置くことができます。これを実現することも、Taniumを導入した目的の一つでした」と話す。

このように、非管理端末を洗い出し、管理対象とすることで、社内全体の脆弱性管理体制を大きく向上させることができる。さらに管理端末の脆弱性把握能力も格段に向上した。たとえば、以前はZoomやEdgeなどの脆弱性対応調査に24時間以上を要していたが、今では5分程度で社内全体の脆弱性を把握できる。

セキュリティ対応の迅速化と業務効率アップ

NECにとって、Tanium導入の最大のメリットの一つは「セキュリティ対応の迅速化」だ。 Tanium導入以前は、特定の脆弱性に関するエンドポイントアプリケーションの調査に24時間以上を要することもあった。しかし現在では、同様の調査をわずか5分で完了できる。

エンドポイントにおけるソフトウェアのパッチ適用も大幅な効率化を実現した。従来はパッチの展開に最大14日を要していたが、Taniumにより最短4日まで短縮することができた。さらに、パッチの適用状況をリアルタイムで可視化できるため、従来よりも確実なパッチ管理を実現している。

> Taniumの導入により、対応スピードの向上、業務効率の改善、生産性の向上という三拍子が揃いました。
>
> 日本電気株式会社 Corporate Executive CISO
> **淵上 真一氏**

ServiceNowとの連携により脆弱性対策を加速

TaniumとServiceNowの連携により、IT資産および脆弱性情報の統合管理と、エンドポイントにおける重大な脆弱性の早期検出を加速する取り組みも行われている。Taniumが脆弱性を検知し、ServiceNowが自動で対応を指示することで、人的ミスを防ぎ、対応の迅速化と正確性を実現した。これにより、脆弱性の検知から対応指示までの時間を平均7分の1に短縮できた。

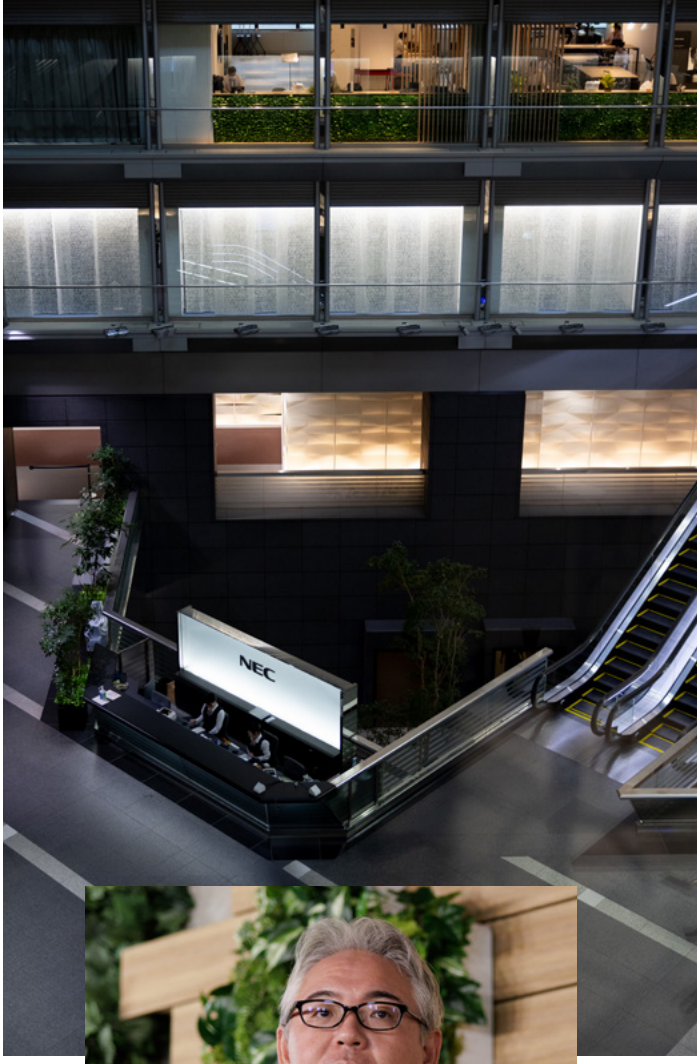
さらに、Taniumのデータを活用したサイバーセキュリティダッシュボードを構築し、リスクの変化をリアルタイムで把握・管理する体制を整備することで、長期的な課題と即時対応が求められるインシデントを明確に区別し、的確な意思決定を可能にしている。

「Taniumの導入により、対応スピードの向上、業務効率の改善、生産性の向上という三拍子が揃いました」と淵上氏は語っている。

社内ノウハウを活かし外販も展開

NECは自社で導入したTaniumのソリューションの外部販売も行っており、NECの統合エンドポイント管理基盤（UEM）として、独自のノウハウや周辺ツールとの連携を含めて顧客に提案している。

セキュリティ事業統括部の山水 佳紀氏は「NECでは端末の"利用者情報"と"管理者情報"を入力するとTaniumで情報を収集する独自ツールをセットで提供することもできます」と話す。自グループでの導入経験を生かしたコンサルティングにも力を入れ、社内の成果を社会へと還元するショウケースのひとつとしたい考えだ。



Taniumの導入効果

全世界26万台の端末をTanium Cloudで一元管理し、サイバーハイジーンを徹底。脆弱性の把握にかかる時間を90％以上短縮し、現場の作業負荷の大幅軽減を実現した。

- 世界26万台の端末をTanium Cloudで一元管理
- 全社のPCの状態や脆弱性を5分ですばやく把握
- パッチの配信にかかる時間を2週間から4〜5日へ短縮
- 現場担当者の作業負担を15分の1以下に
- ServiceNowとの連携により脆弱性の検知から対応指示までの時間を7分の1に短縮

TANIUM

The Power of Certainty.™

Visit us at www.tanium.jp and follow us on Facebook and X.