TANIUM

CIS Controlsに準拠するための“可視化”プラットフォームで資産管理から脆弱性対策までワンストップで対応

SAISON INFORMATION SYSTEMS

株式会社セゾン情報システムズ

業種
情報・通信業

従業員数
約700人

本社所在地
東京都港区

導入商品
Asset・Discover・Patch・Deploy・Comply・Enforce

Taniumの導入効果

- グローバル標準のガイドラインCIS Controlsへの準拠をサポート
- 約1,800台の端末をほぼ完全に可視化
- KPIと現状を数値化し経営層に報告することが可能に
- 可視化から設定、変更までワンストップで幅広く対応

株式会社セゾン情報システムズ（以下、セゾン情報システムズ）は、MFT(Managed File Transfer Suites)市場において国内シェアトップ、グローバルシェアでも4位につけるソフトウェアHULFT（ハルフト）で知られるシステムインテグレーター。Taniumを活用して約1,800台の端末とソフトウェアを“可視化”し、管理を効率化した。

ランサムウェアの脅威に対応するために

セゾン情報システムズは、そのシステムインテグレーション事業に加え、国内シェア7割超のファイル転送ツール「HULFT」で有名だ。1993年にメインフレームとC/S環境のデータ連携を可能にするミドルウェアとして誕生したHULFTはその後も進化し続け、現在は次世代クラウド型データ連携プラットフォーム「HULFT Square（ハルフトスクエア）」が企業のDX基盤として注目を集めている。

デジタル産業に身を置くセゾン情報システムズにとって、セキュリティは身近な脅威だ。受注したプロジェクトを進めるにあたっては常にセキュリティを念頭に置く必要があり、ソフトウェア開発に際しても安心・安全は大前提となる。

さまざまな脅威が発生する中で、経営層からもランサムウェアへの対策を求められていた。そして、ランサムウェアに対して最も有効な防衛策は、脆弱性対策だ。そのため、セゾン情報システムズでは、OSやソフトウェアの最新パッチを速やかに適用することを最優先課題として、すべての社員と端末管理者、自社ネットワークにアクセスできる協力会社の社員などに対して適切なタイミングで警告していた。しかしながら、「まさにいま、実際に適用されているかどうか」を確認することは難しかった。デジタルの会社であり、社員のITリテラシーは高い。とはいえ、開発環境の端末なども多数あり、不安は残っていた。

コーポレートデベロップメントセンター
QM推進室 松村 章宏氏

DXを推進する会社ですから、セキュリティを優先して便利な使い方に制限をかけるのはNG。Taniumを活用して安心して利用できるゼロトラスト環境の整備を進めていきます

コーポレートデベロップメントセンター
QM推進室 SIS-CSIRT 阿部 正朝氏

「不安」という雰囲気を「課題」として顕在化させるために、不安の要素を言語化することは有益だ。セゾン情報システムズでは、まずは「守るべきものを明確にしたい」と考えた。そのためには、ハードウェアとソフトウェアのリアルタイムかつ完全な資産管理をワンストップで実現できるソリューションが必要だった。

コーポレートデベロップメントセンター QM推進室 松村 章宏氏は、「グローバル企業としてさらなる成長を遂げるためには、セキュリティについてもグローバルな規格に対応しておく必要がありました」と話す。「そこで、クラウドと親和性の高いCIS Controlsへの準拠を目指すことになり、守るべき対象を明確にするために、IT資産をリアルタイムに棚卸して管理するためのソリューションを検討することになりました」

コーポレートデベロップメントセンター
QM推進室 SIS-CSIRT 阿部 正朝氏

約1,800端末をほぼ完全に可視化

複数のソリューションを検討した結果、セゾン情報システムズが選んだのはTaniumだった。検討したソリューションをCIS ControlsのBasic 6項目と照らし合わせたところ、求められる要件を最も充たしていたのがTaniumだったのだ。PoCを実施し、2020年夏に導入を決定した。メンテナンスの手間がかからないクラウド版のTanium Cloudを採用しスピーディに導入を進め、実際に利用しながら運用設計を実施して、運用手順書などのドキュメント類を整備し、徐々に本格運用へと移行した。

当初は脆弱性を抱えている端末が想定より多く、中でもWindowsの月次パッチが未適用の端末が目立ったという。コーポレートデベロップメントセンター QM推進室 SIS-CSIRT 阿部 正朝氏は、「すべてを可視化できたことで、本腰を入れて脆弱性を撲滅する取り組みを進めることができました」と話す。いまでは約1,800端末をほぼ完全に可視化し、パッチの適用率を大幅に改善することができた。

「協力会社さんの持ち込みPCを含めて、すべての可視化を実現しました。非管理端末は3%程度で、そのほとんどは新規導入の端末です。そのため、完全にゼロにするのは難しいのですが、検証環境のサーバなども管理者が登録してくれるようになってきたことで、常にクリーンな状態を保てています」（阿部氏）

ワンストップで幅広く対応

Taniumを使えば、可視化から設定・変更までワンストップで幅広く対応できることも大きなメリットだった。リソースが限られる中で、可能な限りTaniumを使って自動化を実装している。また担当者がセキュリティ設定を行う際に、CIS Benchmarksガイドラインに準拠する運用プロセスを確立しやすくなった。

そして状況の可視化は数値化にもつながり、経営層に対して、リアルな数字に基づくレポートを提供できるようになった。管理下にある端末の割合や、脆弱性を抱えている端末の割合およびその理由などを定期的に報告しており、以前より的確に状況を説明することが可能になった。

「いまでは“Taniumは優れた可視化ソリューション”として社内に認知されています。状況を可視化できたことで、スタートラインに立てました。これからも脆弱性対応を進め、ハイジーンを強化していきたいと考えています」（松村氏）

今後は、海外の子会社への展開も視野に入っている。そのために、ネットワークも見直し、グローバルで共通化する方向にある。阿部氏は、「ゼロトラストネットワークへの移行を真剣に検討していて、すでにゼロトラストの考え方をセキュリティ方針策定の中心に置いています。弊社はDXを推進する会社ですから、セキュリティを優先して便利な使い方に制限をかけるという方向性はありえません。その上で、守るべきものをきちんと守ります。今後もTaniumを活用して、安心して利用できるゼロトラスト環境の整備を進めていきます」と話してくれた。

お問い合わせ
TANIUM
タニウム合同会社
〒100-0004　東京都千代田区大手町２丁目６－４ 常盤橋タワー25階
https://www.tanium.jp
jpmarketing@tanium.com

©2023 Tanium, Inc. All rights reserved. Tanium は Tanium, Inc. の登録商標です。その他の社名、製品名、サービス名は各社の商標または登録商標です。