ケーススタディ

Taniumの情報収集の圧倒的スピードを体感 約5,000台の端末の脆弱性を排除する “リアルタイム衛生管理”を実現

和歌山県
Wakayama Prefecture

和歌山県

業種
地方自治体

人口
891,620人（2023年10月1日時点）

所在地
和歌山県和歌山市

導入ソリューション
Tanium Core, Deploy, Patch, Comply, Threat Response, Discover, Impact, Enforce（一部）

Taniumの導入効果

- 全端末を一元管理して脆弱性を排除する“リアルタイム衛生管理”を実現
- 端末情報の可視化とパッチ配信の自動化で、端末の管理業務を大幅に効率化
- ネットワークの負荷を軽減し、回線の細い拠点へのパッチ配信時間を短縮

和歌山県では、総務省のガイドラインに都度対応してきたことで、セキュリティシステムの肥大化と管理運用の負担が大きな課題となっていた。2022年、その克服を目指してセキュリティ対策を再整備しTaniumを導入した同県は、5,000台以上の端末を一元管理して脆弱性を排除する“リアルタイム衛生管理”を実現。ソフトウェアのバージョンアップ作業の大幅効率化など、多大な成果を挙げている。

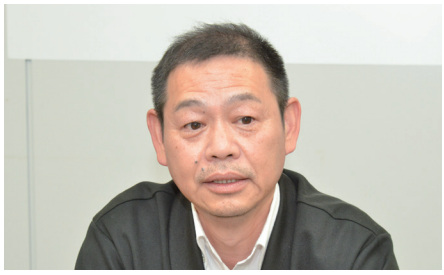
管理・運用の負担軽減を目指し、セキュリティ対策を再整備

和歌山県では、本庁と出先機関である振興局などを高速回線で結ぶ「きのくにe-ねっと」を整備し、快適な通信環境のもとで行政業務が行われている。2004年度に運用が始まったこの情報ハイウェイは、現在では県内全市町村や関係機関などでも活用されており、県全体として欠かせない情報基盤となっている。

このような先進的な取り組みを進める中で、多岐にわたるセキュリティ対策も実施してきた。担当部署である情報基盤課が中心となり、情報漏洩・不正アクセス対策として、端末側でデータを保持しないシンクライアントシステムを2005年から採用し、以降もファイル暗号化や振る舞い検知などのシステム・機器を随時導入。並行して、職員のPCの整備や、その他の情報通信インフラの管理を日頃から徹底するなど、先進的かつきめ細かなセキュリティ対策に取り組んできた。

ただ、それでも課題は数多くあった。同課ネットワーク班長の菊山和明氏は、「総務省のガイドラインに対応するために、都度個別のシステムや機器を追加していました。結果として、システム全体が肥大化して管理運用が煩雑になる、セキュリティのアラートを一元的に管理できない、インシデント発生時のログ確認に手間取る、といった問題が発生していました」と話す。

そうした中で大きな転機となったのが、総務省の「地方公共団体における情報セキュリティポリシーに関するガイドライン」の改定だ。情報基盤課は、改定によりエンドポイント対策とログ管理システムの導入が必須の要件となったことを受け、この際セキュリティ対策を総合的に再整備し、システム肥大化の抑止と管理運用の負担軽減を図ることを決断。ネットワークにつながる端末をすべて一律に監視でき、操作性の高いシステムを導入したいと考え、Taniumの検討を開始した。



総務部 行政企画局 情報基盤課
ネットワーク班長 菊山 和明氏

エンドポイントの状態を可視化して脆弱性を把握・管理できるTaniumを導入すれば、“リアルタイム衛生管理”を実現し、長年の課題を解消できると考えました

和歌山県 総務部 行政企画局
情報基盤課 ネットワーク班長
菊山 和明氏

検証でTaniumの圧倒的スピードを体感

Taniumに注目した理由について菊山氏は、「従来のセキュリティ対策で特に不足していたのが、いわゆる“リアルタイム衛生管理（サイバーハイジーン）”です。エンドポイントの状態を可視化して脆弱性を把握・管理するTaniumを使えば、リアルタイム衛生管理を実現できると考えました」と語る。

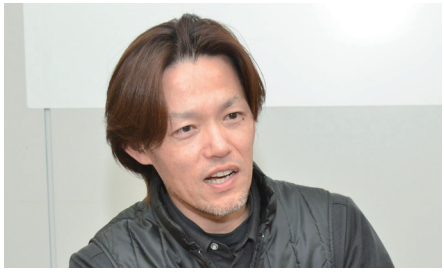
とはいえ、懸念もあった。先述の通り、同県では全職員のPCにシンクライアントシステムを導入し、処理のほとんどをサーバ側で行っている。そのため、職員の利用する約4,600台のPCの中には、低スペックのものが多く含まれている。また県内には、ネットワーク回線の細い山間部の拠点なども点在している。そうした環境下でも新システムが問題なく稼働するのか、という不安があったのだ。

そこで、検討の段階でエンドポイント数などの条件の近い他の環境下で検証を実施。必要な情報を取得できるか、アプリの配信が可能かなどを確認した上で、他の候補製品と比較し、Taniumが理想的であると評価した。同課主任の岩田雄一郎氏は、「端末の情報収集にかかる時間が桁違いに速かったです。他の製品では翌朝までかかることが、ものの数分で終わってしまう。スペックの低いPCや細い回線でも問題なく稼働することを確認できたため、仕様書作成の参考になりました」と話す。

導入作業は、同県のエンドポイントセキュリティシステム基盤構築及び賃貸借業務を落札した伊藤忠テクノソリューションズ株式会社（CTC）を中心に、2022年4月に開始。業務用のソフトウェアの移行作業などを含め、当初の想定通り同年9月末に完了し、同年10月に新たなセキュリティ対策を施したシステムの稼働を開始した。

5,000台の端末でリアルタイム衛生管理を実現

Taniumの導入によって、同県のセキュリティ対策は格段に進化した。端末のログデータを可視化・分析するSplunkと組み合わせることで、OS・ソフトウェアのバージョンなどの情報を収集し、パッチを自動で配信して常に最新の状態に保つ。ネットワークに新たに接続された端末や、パフォーマンスの異常を自動検出して分析し、速やかに適切な対応をとる。情報基盤課によって整備された端末はもとより、ネットワークに接続されたすべての端末を一元管理し、脆弱性を排除する、まさに思い描いた通りの“リアルタイム衛生管理”を実現できたのだ。



総務部 行政企画局 情報基盤課
主任 岩田 雄一郎氏

総務部 行政企画局 情報基盤課
副主査 岡田 泰典氏

それにともない、システムの管理運用の効率は飛躍的に向上した。たとえば各端末のソフトウェアのバージョンアップについては、従来、ユーザーが各自パッチをダウンロードして実行していたため、トラブルが発生するたびに情報基盤課に問い合わせがきて、対応を求められていた。しかし、Taniumの導入後は、パッチの90%以上は、ユーザが作業することなく自動で適用できるようになり、例外的なケースのみ情報基盤課が対処すれば済むようになった。

同課副主査の岡田泰典氏は、「課の担当者は3名しかいないので、以前は職員以外のものを含め5,000台以上の端末を個別に監視するのが大変で、問い合わせの電話があるたびに、本来の仕事が止まってしまいました。今は管理画面で各端末の状態をひと目で把握でき、ユーザーサポートの作業に手をとられることもほとんどなくなりました」と喜ぶ。パッチの適用に関しては、ユーザー側ではほぼ100%、管理側でも80%程度、作業を削減できた実感があるという。また、なんらかの問題が発生した際にも、端末のログデータを迅速に収集して分析し、要因を簡単に特定できるようになったことも大きな進歩だ、と菊山氏は指摘する。

岩田氏は最後に、今後の展開についてこう話した。「従来のWSUSを利用したWindowsのパッチ配信は、回線の細い拠点への配信に時間がかかります。そこで、Taniumで検証を行ったところ、独自技術のリニアチェーンにより、ネットワークに負荷をかけずに配信できることがわかりました。このように、今後もTaniumの活用の幅を広げ、管理運用作業のさらなる効率化を進めていきたいと考えています」

※所属・役職等はインタビュー当時の情報です。

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

©2024 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。