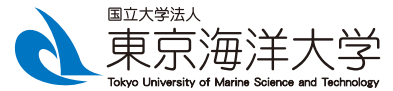


ユーザー事例 Success Story

東京海洋大学
Linux環境の
稼働監視

Red Hat Insightsにより、 RHEL環境の監視を実現。 セキュリティ対応上の指標も獲得



2003年10月に東京商船大学と東京水産大学が統合して誕生した東京海洋大学。学部としては海洋科学部4学科と海洋工学部3学科を有し、翌2004年4月に国立大学法人東京海洋大学となった。同大学では2015年10月、情報処理センターシステムの更新プロジェクトを開始、学内の情報システム基盤を刷新すると同時に、Red Hat Enterprise Linux (RHEL) 環境のモニタリングを検討。その際に導入し、効果を上げているのがRed Hat Insightsだ。

背景

学内の情報システム基盤を刷新、 1つのデータセンターに集約

2つの大学を前身に持つ東京海洋大学は、越中島地区と品川地区の2カ所にキャンパスを置いているが、両キャンパス間は「SINET5」と呼ばれる学術情報ネットワークで繋がれており、大学として1つのネットワーク網が形成されている。こうした大学の基盤となるネットワーク環境や学内のメールサーバー、DNSサーバー、Webサーバーなどで構成されるシステム(情報処理センターシステム)および教育システムの構築、運用管理を担っているのが情報処理センターだ。

同センターでは、2005年から5年に1回の頻度で情報処理センターシステムのリプレースを行っており、2015年10月に3期目の更新プロジェクトに着手した。当時の状況を、国立大学法人東京海洋大学 情報処理センター 助教の室田朋樹氏は、次のように説明する。

「情報処理センターシステムは、全学生と教職員が利用する大規模な情報システム基盤です。世の中のトレンドへの対応や最新テクノロジーの取り込みなども加味して、5年に1度リプレースを行っています。今回は、越中島地区と品川地区の各々にあったメールサーバーなどのシステムを1つのデータセンターに集約して統合化を図り、新たな取り組みとしてディザスタリカバリ対策も行うことになりました。併せて学術情報ネットワークSINET5への接続も10Gbpsに増強することになりました」。

プロジェクトの開始にあたっては、政府調達の手続きに則って2015年9月中旬に開札が行われ、システムインテグレータのテクマトリックスが落札した。

課題

セキュリティ上の漏れを塞ぐため RHEL環境の見える化を図りたい

情報処理センターシステムに含まれるメール

サーバーやDNSサーバー、Webサーバーは全てRed Hat Enterprise Linux (RHEL) ベースのLinux環境だが、Windows環境も一部混在している。講義でExcelなどを使用することもあり、教室で学生が使用する端末はWindowsマシンだからだ。

「ただしWindowsはLinuxに置き換える対象というものではなく、あくまで使い分けが前提です。ユーザーがアクセスするメールサーバーやWebサーバー、教室の端末を除く認証基盤など、重要なシステムはすべてRHELの環境の中に組み込まれています」(室田氏)。

今回、情報処理センターシステムの更新プロジェクトを始めるにあたり、室田氏は以前から抱えていた課題も併せて解決したかったという。それが、RHEL環境の稼働状況を見える化することだった。

「これまで、適切にパッチが当たっているかどうかなどきちんと管理できておらず、これをそのままにしておくことは大きなセキュリティリスクだと考えたのです。『セキュリティ上の漏れを塞ぎたい』というのが最大の動機で、システム全体をリプレースする今回のタイミングで、この課題も解決したいと考えました」。

システム要件

監視ツールの投入で システムの稼働に影響しないか

以前からRHEL環境の見える化を図りたいと考えていた室田氏は、日頃から各種メディアやソリューションベンダーのサイトなどを閲覧して、適切な解決策がないかを模索していた。そんな折、レッドハットが2015年6月に発表したオンライン経由のシステム分析サービス「Red Hat Insights」の情報に辿り着いたという。

Red Hat Insightsは、RHEL環境の定期的な情報収集とレポートを行うツールで、障害に対して事前に予防的な対策を打つことを可能にしてくれるものだ。対象となるOSはRHEL 6とRHEL 7

で、ユーザー企業がRHELのサブスクリプションを持っていれば、物理環境/仮想環境を問わず、10システムまでは追加費用なしで利用できる。

「Red Hat Insightsの存在を知り、今回のプロジェクトを担当してもらうことになったテクマトリックスにその情報を伝えて、まず無償で利用できる評価用のRed Hat Insightsを使ってみて、システム稼働に不具合が出ないかを検証してもらうことにしました」。

Red Hat Insightsを選んだ決め手

システム稼働状況を可視化でき 大学/システムインテグレータの双方に有用

室田氏からの依頼を受けたテクマトリックス株式会社 ネットワークセキュリティ事業部 第二技術部 ネットワークインテグレーション課 課長の太田拓也氏は、早速Red Hat Insightsの検証を開始する。

「依頼の内容は『Red Hat Insightsを導入することで、システム運用上、何か問題がないかを確認してほしい』。5年間の運用を行う上で、サービス利用者である大学とサービス提供者であるテクマトリックスの双方にメリットがあるかどうかを判断してほしい』というものでした。そこで我々はRed Hat Insightsをテスト環境に入れて運用してみたのですが、まずシステム稼働上はまったく問題ありませんでした」(太田氏)。

またRed Hat Insightsが発行するレポートによって、監視対象のシステムの状態や対応策がよく分かることが明らかになった。

「Red Hat Insightsのレポート画面では、問題の種類と重要度が分類されており、影響を受けるシステムや対応方法まで確認することができます。これは1日1回更新され、レポート結果にアップデートがある場合は週一度の自動配信メールで教えてくれます。そこで東京海洋大学様には、『システム稼働上まったく問題なく、大学様とテクマトリックスの双方にとって実

Linux環境の稼働監視の流れ

01 背景

学内の情報システム基盤を刷新、1つのデータセンターに集約

- 5年ごとに情報処理センターシステムを刷新
- 2つのキャンパスのシステムを統合

02 課題

セキュリティ上の漏れを塞ぐためRHEL環境の見える化を図りたい

- パッチ適用の管理などが徹底していなかった
- 刷新のタイミングでこのリスクを解消したい

03 システム要件

監視ツールの投入でシステム全体の稼働に影響しないか

- 無償版を使って稼働状態を検証
- 検証作業はパートナー企業に依頼

04 Red Hat Insightsを選んだ決め手

システム稼働状況を可視化でき、大学/システムインテグレータの双方に有用

- レポートでシステムの状態や対応策を把握できる
- アップデートもメールで通知

に有用なツールだと思う」とご報告したのです(太田氏)。

Red Hat Insightsを導入したメリット1 パッチ更新など、対応優先度が明確に 対応漏れの不安も払拭

Red Hat Insightsから出されるレポートは、見つけた問題がセキュリティ上の問題なのか、パフォーマンス上の問題なのか、あるいは安定性に関わるものなのかといった問題の種類と、その対応重要度まで教えてくれる。

「例えばセキュリティパッチの更新が必要だという時、重要度に関係なく同一レポート内に一覧で出されてしまうと、すべてに対応するのはかなり大変ですし、対応漏れの恐れもある。しかしRed Hat Insightsで受け取るレポートには、問題の種類だけでなく、その重要度が明瞭に、しかもワークアラウンドを含めた対応策まで記されています。実際のシステムにどんな影響があり、どれくらい対応優先度が高いのか、という情報が明確に整理され提供されるのはとても便利です。対応漏れの心配も払拭されました(室田氏)。

現在、Red Hat Insightsは問題発見のためのルールを150~160ほど持っており、このルールに則ってシステムを監視している。ユーザー側では、重要度によりレポートをフィルタすることも可能だ。

Red Hat Insightsを導入したメリット2 システムセキュリティ上で 対応判断の拠り所となる指標ができた

またRed Hat Insightsの導入で得られたもう1つの大きなメリットとして、Red Hat Insightsから受け取るレポートが、システムセキュリティ上の対応を判断する際の拠り所となる指標になった点があるという。

「通常、システムに何か問題がないかを調べる時は、運用管理者がシステムをコマンドで叩き、レッド

ハットのセキュリティのページを確認し、CVE(Common Vulnerabilities and Exposures)も見つづ、ワークアラウンドがないかを検索して…、といった作業を行います。この工程が、Red Hat Insightsのレポートによって大幅に削減されました。Red Hat Insightsがデイリーでシステムをスキャンしていて、例えばこの環境にはこんな脆弱性があり、その理由はこのパッケージがここに入っているためだ、といった詳細まで教えてくれるのです。さらにワークアラウンドがある場合には、その情報の所在まで分かるようになっていきます。このレポートを拠り所に、CVEの情報や一般的な対処方法も確認したうえで、最終的な対応策を判断しています(太田氏)。

東京海洋大学ではシステム運用をテクマトリックスに委託しているが、Red Hat Insightsから出されるレポートは、自社運用しているユーザー企業にとってももちろん有用だ。

「レッドハットがOSの稼働状況をチェックしてくれて、何か問題があれば教えてくれるというのは、ユーザーにとって大きな安心感に繋がります。またRed Hat Insightsのレポートは、システムインテグレータと話す際の共通言語にもなる。パートナー企業との意思疎通もスムーズになったと感じています(室田氏)。

Red Hat Insightsを導入したメリット3 運用管理の工数を大幅に削減、 コスト削減の可能性にも期待

さらに、Red Hat Insightsの導入で問題対応が迅速化したことで運用管理の工数が大幅に削減し、オペレータの負荷も減ることで、今後運用コストの削減も期待できるという。

「Red Hat Insightsの導入効果を定量的に測るのはなかなか難しいのですが、今後Red Hat Insightsをベースとした問題対応が定型業務化し、例えばこんな問題にはこんな対策を取るというガイドライン



国立大学法人東京海洋大学
情報処理センター 助教
室田 朋樹 氏



テクマトリックス株式会社
ネットワークセキュリティ事業部
第二技術部
ネットワークインテグレーション課
課長
太田 拓也 氏

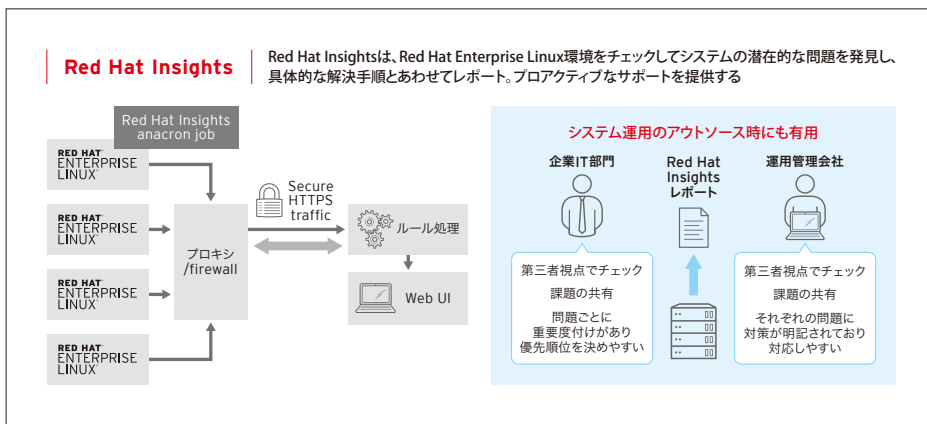
を用意できれば、Windows Updateのような高水準なセキュリティ対策に近づけていくことができるのではないかと。そうなればオペレータの数を減らすことができ、運用コストも削減できる。最終的には、そんな可能性も期待できるのではないかと考えています(室田氏)。

「Red Hat Insightsは、比較的経験の浅いエンジニアでも監視業務を行うことを可能にしてくれるので、監視対象のシステムが100台あるいは200台と広がってもスケールしやすいソリューションだと思います。我々の運用チームでは、今後、他のシステムでもぜひ使いたいと高く評価しています(太田氏)。

今後の展望/レッドハットへの期待 メールでの情報提供をより詳細に することでさらなる利便性向上を期待

東京海洋大学では現在、RHEL環境下で約30のシステムが稼働している。同大学は無償版でカバーできる10システムに加えて、残り20システムの監視については有償版のライセンスを購入した。無償版と有償版とで提供される機能自体には全く差異はなく、無償版ではレポートを参照する機能のみ利用できるが、有償版では不明点や質問などをレッドハットのサポートに問い合わせることができる。また確認されるものではないが、機能拡張の要望をサポートに送ることも可能だ。

「Red Hat Insightsから提供されるレポートは実に有用で、1日1回、専用画面の情報が更新されるのでユーザーとしては安心です。またこの画面はテクマトリックスとも共有しているので、何か気になる点があれば、すぐに話し合うこともできる。レポートにアップデートがあった時は週単位のメールで教えてくれますが、欲を言えば、特にアップデートがなくともメールの報告があり、システムが問題なく稼働していると確認できればより安心ですね。また今後はメールに数行でも簡単な説明があると、より利便性も高まると思います(室田氏)。



05 Red Hat Insightsを導入したメリット1
パッチ更新など、対応優先度が明確に。対応漏れの不安も払拭

- 問題の切り分けと対応優先度が明瞭
- レポートの内容はユーザー側で設定可能

06 Red Hat Insightsを導入したメリット2
システムセキュリティ上で対応判断の拠り所となる指標ができた

- レポートがリスクを判断する際の1つの拠り所に
- パートナー企業との意思疎通もスムーズに

07 Red Hat Insightsを導入したメリット3
運用管理の工数を大幅に削減、コスト削減の可能性にも期待

- レポートの活用がオペレータの負荷軽減に繋がる
- 経験の浅いエンジニアでも監視業務が可能に

08 今後の展望/レッドハットへの期待
メールでの情報提供をより詳細にすることでさらなる利便性向上を期待

- すべてのRHEL環境監視のために有償版も購入
- メールによるさらなる情報提供にも期待