

ネットワークとアプリケーションの障害対応、セキュリティの強化を目指しNetScout nGeniusを導入

学習院大学 様

ネットワークの利用状況をリアルタイムに可視化
 詳細な分析によりトラブル対応やセキュリティ対策を支援

事例のポイント

■ 学習院大学様の課題

- ネットワーク障害に対応するため、障害範囲をリアルタイムで可視化したい
- 回線帯域がひっ迫した際、Web会議等のどのアプリケーションが占有しているかわからない

■ 課題解決の成果

- ネットワーク／アプリケーション障害の範囲、期間、原因を調べることができる
- 収集したパケットをセキュリティインシデント調査の証跡にできる
- レポート機能を使い、日々のネットワーク運用状況を可視化できる

■ 導入ソリューション NetScout nGenius

「NetScout nGeniusはフォレンジックに加え、高度なネットワーク／アプリケーション可視化の機能を備えている点が決め手となりました。われわれが抱えているさまざまな課題を一気に解決できると考えたからです」

計算機センター 村上 登志男 氏

背景・課題

オンライン授業の普及などの理由により、ネットワークの安定運用の重要性が高まる
 端末側でのセキュリティ対策が実施できず、ネットワーク側でのセキュリティ対策が必要に

幕末の京都に設けられた公家の教育機関を起源とする学習院大学では、1877年の創立以来、学生生徒の個性を育み、国際的な視野の広さを養う教育が行われてきた。現在は「学習院大学グランドデザイン2039」のもと、同大学の歴史と伝統を継承しつつ、これに基づいた豊かな人間性を備え、積極的、創造的に社会に貢献する人材を育成することに取り組んでいる。

同大学の計算機センターは、情報処理に関する教育研究を行うための大学附置研究施設として発足。教育用PC約800台(大学分)をはじめとする各種IT機器／設備の運用管理に加え、学生向けのITリテラシ

一講座や夏期講習会・研究会を主催するなど、学生・教職員の教育・研究を幅広く支えている。

同センターは組織的には学習院大学に属しているものの、管理対象となるITインフラの範囲は広く、大学に加え幼稚園、初等科、中等科、高等科、女子中・高等科、女子大学まで、学校法人学習院が設置するすべての教育研究機関に及ぶ。そして同センターにおいて、ITインフラの構築・運用や、新入生などを対象としたITリテラシー教育を担っているのが、城所弘泰氏、磯上貞雄氏、村上登志男氏の3氏だ。

「教職員からの問い合わせはヘルプデスクのスタッフに対応してもらっていますが、実際にITインフラを運用し、トラブルなどがあった場合に原因の調査や対応を行うのはわれわれ3人です。少人数で業務を回しているため常に忙しい状況ですが、特にITインフラのリプレースの時期はやることも多く、大変な思いをしています」(城所氏)

「オンライン授業の普及などの理由により、ネットワー

お客様プロフィール



学習院大学

所在地：東京都豊島区目白1-5-1
 URL：https://www.univ.gakushuin.ac.jp

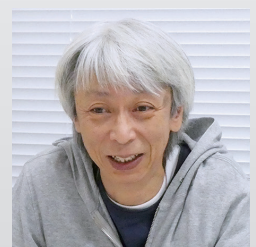
1877年創立。法学部・経済学部・文学部・理学部・国際社会科学部の5学部および大学院で構成された私立総合大学である。教育目標は「ひろい視野 たくましい創造力 ゆたかな感受性」。自ら課題を発見し、その解決に必要な方策を提案・遂行する力を十分に身につけた人材を育成することを使命に、学生の個性を尊重しながら、文理両分野にわたる広義の基礎教育と多様な専門教育を有機的につなげる教育を行っている。



学習院大学
 計算機センター
 村上 登志男 氏



学習院大学
 計算機センター
 城所 弘泰 氏



学習院大学
 計算機センター
 磯上 貞雄 氏

クの安定運用、セキュリティの強化が一段と求められることになりました。その一環として、ネットワークのパケットを収集・分析するフォレンジック製品についても、より深い議論が行われることになったのです。当大学では20年近く前からフォレンジック製品を導入していたのですが、パケットを詳細に分析する機能が無く、障害時には都度大量のパケットを確認する必要があり、障害対応に多くの稼働がかかっていました。そこで、こうした問題を解決できる製品を検討することにしたのです」(城所氏)

解決策と効果

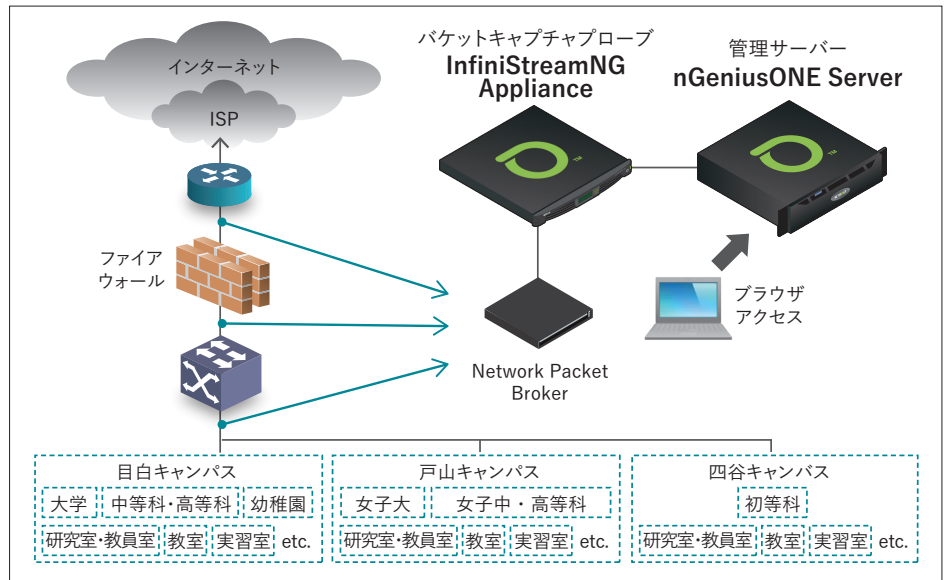
フォレンジックに加え高度なネットワーク可視化を評価
セキュリティ対策やトラブル対応を支援

学習院大学は、2021年夏よりフォレンジック製品のリプレースに向けた作業を開始。7月に取引のあるベンダー各社に対しRFIを提示、9月下旬に「10Gbps回線のフルパケットをロスなく蓄積できること」などの要件をRFPとしてまとめた。このRFPに対して複数社から提案があり、検討の結果、2製品が最終候補として残ったが、要件を満たしている上に、高度なネットワーク可視化の機能を備えていることが評価され、「NetScout nGenius」が採用されることになった。

採用の理由だが、当時はコロナ禍に対応するため、Web会議システムを使ったオンライン授業が始まっていた。これに伴い、「接続が切れやすい」「ネットワークが急に遅くなった」といった問い合わせが増えていたのだが、こうしたトラブルの原因を究明し、迅速に解消するためには、ネットワークの利用状況をリアルタイムで可視化できる機能が重要と考えたのである。

この点、NetScout nGeniusはネットワーク上を流れるデータをキャプチャし、リアルタイムで解析することが可能なので、ネットワーク障害を早期に発見でき、回復までの時間を大きく短縮できる。さらに、長期間にわたるパケットを大容量ストレージに記録し、インシデントが発生した際に証拠を保全・解析するフォレンジック機能も備えている。

同大学がNetScout nGeniusを実際に導入してみたところ、ネットワークの可視化については期待以上の効果があり、さまざまなシーンで役に立つことが分かった。例えば、学生の利用がほとんどない時期・時間帯にもかかわらず、外部との通信量が増えたことがあったのだが、NetScout nGeniusのダッシュボードを使って調べて見ると、欧州のホスティングサーバーが攻撃前の偵察を行っていることが判明した。



「かなり巧妙な手口が使われていたため、NetScout nGeniusがなければ分からなかったかもしれません」(磯上氏)

一方で、可視化した結果、正常な利用であることが判明したこともある。ある建物から大量のトラフィックが流れ、ネットワークが混み合うということがあった。これを調べてみると、発信元は研究室、宛先は国立の研究所であったことから、学術用のデータをアップロードしていただけと判断できた。「やり取りされるデータのほとんどが暗号化されていますが、送信元や宛先、パケット長などが分かるため、いつ、どこで、なにが起きたのかをダッシュボードで調べることができ、原因を特定することが可能です。当初の課題であった『接続が切れやすい』『ネットワークが急に遅くなった』といったトラブルについても、発生時の学内の利用状況をモニタリングすることで、原因がキャンパス側ではなく、サービスの提供元であるということが判明しました」(磯上氏)

今後の展望

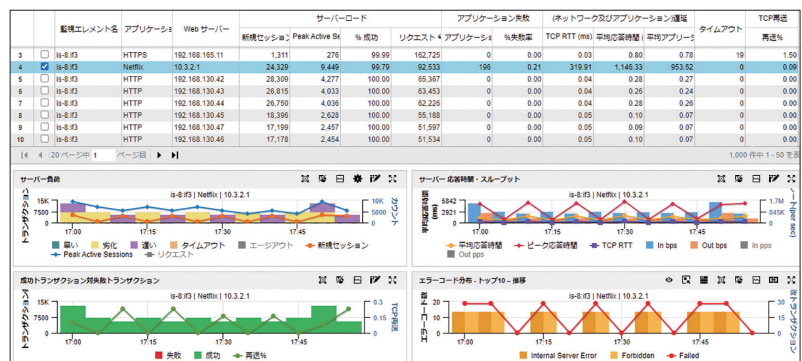
大学特有のネットワーク事情に対応するため
NetScout nGeniusをより使いこなしたい

「大学のネットワーク管理においては、イントラネットよりインターネットに近い意識が必要になります。そうした事情を踏まえた上で、快適さと安全性を両立させるためにも、NetScout nGeniusをさらに使いこなしていきたいと考えています」(村上氏)

その意味でも、計算機センターは従来のファイアウォールや境界防御などでは検知できないリスクに対応可能なNDR (Network Detection and Response) も早くから導入しているが、SCSKが扱っているパケットキャプチャ型NDR製品「NetScout Omnis Cyber Intelligence (OCI)」の導入も今後検討していくとのことだ。

学習院大学は今後もSCSKの支援を受けつつ、より快適で安全なキャンパスLANを実現すべく取り組みを進めていく。

HTTP 通信の品質統計の表示例



通信毎のセッション数、トランザクション数、遅延、パケットの再送、エラーコードの発生数とその内訳などの統計やセッションログ(XDR)情報も表示可能
キャプチャ画像は試験環境のものであり、実際の通信ではございません



SCSK株式会社

- ソリューションの詳細情報・お問い合わせ先
ネットワークプロダクト第二部
▶ URL : <https://www.scsk.jp/sp/netscout/>
- 本件に関するお問い合わせ先
▶ Mail : netscout-staff@scsk.jp

● 本リーフレット記載の会社名、製品名は各社の商標、または登録商標です。なお、本文中や図版には®マーク、TMマークを表記していません。
● 記載されているロゴ、文章、図版その他を無断で転載、複製、再利用することを禁止します。
● 本リーフレット記載されている情報は制作時点の内容であり、予告なしに変更することがございます。予めご了承ください。