

P2Pアプリケーションの正確な検出・制御を実現 キャンパスネットワーク特有の要件に応える 統合ゲートウェイセキュリティを実現したPA-4050

国立大学法人 信州大学は、県内に分散する5つのキャンパスを結ぶネットワークとSINET (学術情報ネットワーク)との境界に、全学部を統合するゲートウェイセキュリティとして次世代ファイアウォール「PA-4050」を導入した。学部や部局などによって異なるポリシー運用が要求されるキャンパスネットワーク特有の要件に対して、仮想システム機能によるセキュリティシステムの統合化を実現するとともに、従来は不十分だったP2Pアプリケーションの確実な制御を可能するなど、柔軟でセキュアなキャンパスネットワークを構築した。



国立大学法人 信州大学

(写真は長野市 工学部キャンパス)

長野県松本市旭 3-1-1

<http://www.shinshu-u.ac.jp/>

分野

教育機関

導入背景

- SINET接続のギガ化に対応するパフォーマンス
- 異なるポリシー運用を行うVRFの統合
- P2Pアプリケーション(ファイル交換ソフト)の確実な検出・ブロック

ソリューション

- App-ID機能によるアプリケーションの可視化とP2Pアプリケーションの確実な制御
- アプリケーション制御と認証ネットワークを連携したユーザーの挙動監視
- 仮想システム(VSYS)機能による部局ごとの異なるポリシー運用の実現

ポリシーの異なる部局のネットワークを統合管理

信州大学は、長野県内に5つのキャンパスに分散した8学部からなる総合大学である。キャンパス間は平均40km離れており、北は長野市から南は南箕輪キャンパスまで、学内ネットワークは県下全域に及んでいる。総合情報処理センター(長野市)は、これらのキャンパスおよびキャンパス間ネットワークの運用や各種サーバによるサービスを提供している。

かつて学内のネットワークは、全学のネットワークの他に教育学部や医学部、図書館など各部局がそれぞれ同大学のグローバルIPアドレス下に独自のネットワーク(VRF)を構築していた。2006年にこれらの部局ネットワークのファイアウォールやセキュリティ装置を統合し、総合情報処理センターが統括するゲートウェイシステムへと移行した。その際に、SINET(学術情報ネットワーク)接続のギガ対応、ファイル交換ソフト使用禁止に基づいてP2Pアプリケーションを検出できるIPS/IDS機能を持つファイアウォールを導入・運用してきた。しかしながら、導入した統合セキュリティ装置のP2Pアプリケーション検出精度の低さ、異なるポリシー運用を行う既設のVRFの仮想システムに制限があるなどの問題を抱えていた。そこで、この統合セキュリティ装置に代わって導入されたのが、次世代ファイアウォールの「PA-4050」だ。

P2Pアプリケーションの確実な検出・制御を実現

以前に運用していたIPS/IDS機能を持つファイアウォールはP2Pアプリケーションを検出してもIPアドレスでしか検出できない上、検出できてもアプリケーションのカテゴリ分類が大雑把であり、防止したいファイル交換ソフトとは違うアプリケーションであったりと、その検出精度に問題があったという。

「P2Pアプリケーションの使用禁止は学長命令であったため確実に検出・ブロックしたかったのですが、以前のIPS/IDSベースのファイアウォールでは検出の精度が低く、検出パターンを見て現場に赴いた担当者がデータをフィードバックして分析しないと、使用を禁止しているファイル交換ソフトなのかどうか判別ができませんでした。PA-4050では、ファイルシェアリング、P2Pアプリケーションといったようにサブカテゴリが充実している上、アプリケーションを正確に識別する能力が高く、WinnyやShareazeなどをブロックし、Skypeは許可するなどのきめ細かい制御が可能になりました」。総合情報処理センターの准教授 鈴木彦文氏は、PAシリーズのアプリケーション識別機能(App-ID)の精度の高さをこう述べる。

PAシリーズは、アプリケーションプロトコルの検出、プロトコルのデコード、シグネチャ、動作分析などによって高い精度でアプリケーションを検出することができ、ポリシー制御によって不正なアプリケーションをブロックし、適切なアプリケーション管理ができる。

「PA-4050は、オープンなネットワーク環境を前提に、個別のポリシー運用というキャンパスネットワーク特有の要件に対応するとともに、P2Pアプリケーションの確実な制御を実現しました」



鈴木彦文氏
信州大学 准教授
総合情報処理センター

「PA-4050は、スペック通りの処理能力を発揮する上に、アプリケーション識別能力が高いため、学内からのオンラインゲームへのアクセスやボット系パソコンのブロックなど、さまざまなアプリケーション制御への期待は大きい」(鈴木氏)と強調する。

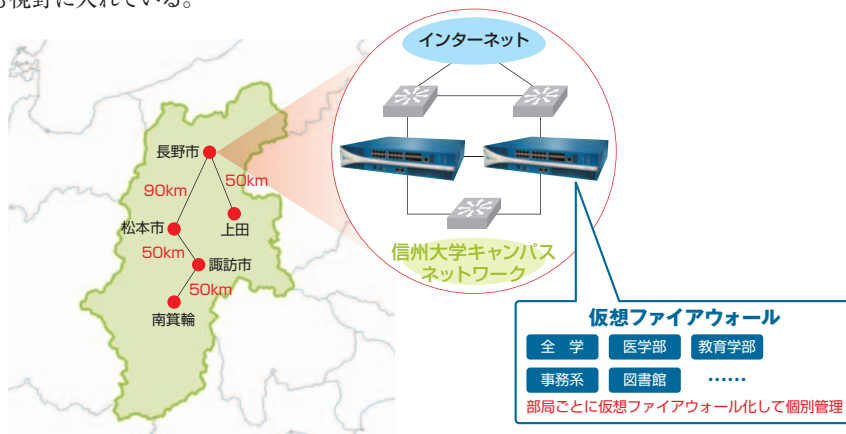
また、PAシリーズはIPアドレスとユーザー情報を動的にマッピングしてユーザーの活動を可視化することができるが、総合情報処理センターでは今年度中に認証ネットワークと連携してユーザーの挙動を可視化することを計画している。これにより、アプリケーション利用とユーザー情報をひも付け、確実なアプリケーション制御を実施していくという。

仮想システムを使った個別のポリシー運用にも柔軟に対応

もう1つのセキュリティ要件である部局ごとに異なるポリシー運用を統合的に管理することに対しても、PA-4050は十分に機能を発揮できると期待している。従来のセキュリティ装置ではマルチテナントサービスが可能な仮想システム (VSYS) は5つのセグメントにしか対応できていなかったが、PA-4050では標準で25の仮想システム (最大125まで拡張可能) を構築できる。

「これまでは、全学・医学部・教育学部・事務系・図書館の5つのVRFをVSYSに割り当てていましたが、その他の学部、さらには学科によって独自のポリシーで運用したいという要求があります。オープンなネットワーク環境を前提に、学部や部局によって異なるポリシー運用が要求されるキャンパスネットワーク特有の要件に対して、PA-4050は十分に応える機能・性能を備えています。今後は、各VRFの担当者にそれぞれ管理権限も委譲して、部局に合ったポリシー運用を進めていきたい」(鈴木氏) という。

また、信州大学はSINETノード機関であるため他大学も接続しているほか、さまざまな産学共同組織とネットワークを結んでいる。ある大学からはファイアウォール運用も含めてSINET接続を依頼されており、今後は他大学や組織に対して、仮想システムによるファイアウォール機能だけでなく、ユーザー認証と連携したネットワーキングサービスを提供していくことも視野に入れている。



パロアルトネットワークス

E-mail: InfoJapan@paloaltonetworks.com

www.paloaltonetworks.jp