

キャンパスネットワークのシンプル化を推進しつつセキュリティを強化 UTMからセキュリティ機能を統合した 次世代ファイアウォールへリプレース

駒澤大学は、キャンパスネットワークシステムの更改を機にパロアルトネットワークスの次世代ファイアウォールを導入した。ゲートウェイおよび内部ファイアウォールとして運用してきた9台のUTMを次世代ファイアウォール「PAシリーズ」にリプレース。システム更改のテーマである“システムのシンプル化によるコスト削減の実現”を、セキュリティ機能の統合化と運用機器の物理的な削減によって達成した。また、次世代ファイアウォールの特徴であるアプリケーションの可視化・制御というアプローチにより、キャンパスネットワークの自由な利用環境とセキュリティ強化を両立した。

サービスレベル、セキュリティレベルを維持しながらコスト削減を狙う

駒澤大学は、1882年に近代教育を行う大学として開校して以来、128年間にわたり多くの人材を各界に送り出してきた。仏教の教えと禅の心を現代的教育に活かしていくことを建学の理念とし、7学部7研究科に1万6,000人の学生を擁する総合大学である。

同大学のキャンパスネットワークシステム「KOMAnet」は、総合情報センター（所長：金山智子教授）によって管理され、約1万9,000人の学生および教職員に広く利用されている。5年ごとにシステム更改をしてきたKOMAnetだが、2011年度の更改ではサービスレベル、セキュリティレベルを保ちながらコスト削減が大きなテーマだった。「今回の更改では仮想化によるサーバ統合で物理サーバのコスト削減を図りましたが、セキュリティシステムにおいてもセキュリティレベルを維持しながらシステム構成をシンプル化し、運用負荷を減らすとともにコストをいかに削減するかが課題でした」（総合情報センター情報ネットワーク課課長 成田早苗氏）。

また、ネットワークの脅威がP2Pをはじめとするアプリケーションベースのセキュリティリスクが高まっていることを背景に、情報漏えい防止に向けたアプリケーションレベルの制御が求められるようになっていた。

システム構成のシンプル化という点では、従来ゲートウェイおよび教育研究系・学生系セグメントと事務系セグメント間で運用してきたUTMをリプレースすることだった。「ゲートウェイのUTMは、アンチウイルスやIPS機能を稼働させるとパフォーマンスが著しく低下するため、ファイアウォールとしてのみ運用。一方、内部ファイアウォールとして使っていたUTMは主にアンチウイルスに利用していましたが、やはりパフォーマンスの問題によりロードバランサー下で計7台を運用していました」（運用・保守を担当する独立系の情報サービス会社、SRAの分銅淳至氏）と述べ、ゲートウェイでのセキュリティ機能を統合・シンプル化し、かつ運用台数を削減して運用負荷の軽減とコスト削減すること、さらにアプリケーションレベルでのアクセス制御を可能にするというのがリプレースの要件だった。

脅威防御機能を稼働してもスループットが低下しないPAシリーズを採用

従来の一般的なUTMはセキュリティ機能を統合化しながらも、アンチウイルスやIPSなどスキャンエンジンを稼働するとスループットが著しく低下する。しかし、PAシリーズは、シングルパス・パラレルプロセッシング（SP3）アーキテクチャにより、マルチギガビットレベルのデータフローに対しセキュリティ、脅威防御、URLフィルタリング機能などを提供するパフォーマンスを持つ。

「次世代ファイアウォールは、セキュリティ強化の要件として挙げたアプリケーションベースの制御が可能であることに加え、防御機能を稼働させてもスループットがほとんど落ちないことを高く評価しました。また、IPアドレス単位でなく、名前解決ベースでポリシー設定できる点にも魅力を感じていました」（分銅氏）と次世代ファイアウォールを採用した理由を述べる。



学校法人 駒澤大学

東京都世田谷区駒沢1-23-1
<http://www.komazawa-u.ac.jp/>

分野

教育機関

導入背景

- システム構成のシンプル化によるコスト削減
- アプリケーションレベルのアクセス制御への要求
- ファイル共有ソフト等による情報漏えい防止対策

ソリューション

- 次世代ファイアウォールによるセキュリティ機能の統合化・シンプル化
- アプリケーション可視化・制御による情報漏えい防止およびセキュリティ強化

駒澤大学が導入した



PA-4020



PA-2020



「システム構成をスリム化してコスト削減を図るという課題に対し、次世代ファイアウォールによってセキュリティを強化しながら実現できました」

成田 早苗 氏
駒澤大学 総合情報センター
情報ネットワーク課 課長

「アプリケーションベースの制御が可能であること、脅威防御機能を稼働させてもスループットが低下しない点を高く評価しています」

分銅 淳至 氏
SRA ネットワークシステムサービス本部
ネットワーク運用・構築部 主席

導入した次世代ファイアウォールは、ゲートウェイに PA-4020 を 2 台 (冗長構成) と事務系セグメントとの間に PA-2020 を 2 台 (冗長構成)。PA-4020 はファイアウォール、アンチウイルス、IPS 機能によりインターネットの脅威から KOMAnet 全体を保護している。また、経営情報や人事情報、学生の成績など教務系情報をより強固に守るために、事務系セグメントとの間に PA-2020 を内部ファイアウォールとして運用している。

PA-4020 をゲートウェイに導入したことで、スループットを低下させることなく、アンチウイルスと IPS 機能のより、これまで運用してきた IPS/IDS 装置を排除でき、かつ Web 経由のウイルス対策が可能になった。また、7 台の UTM を 2 台の PA-2020 へリプレースしたことで、導入・運用コストの削減とともに台数削減に伴う運用負荷の軽減を実現している。

また、PA シリーズの User-ID 機能により認証基盤として利用している Active Directory と連携したことで、アプリケーションの可視化や制御において DHCP 環境下でありながら、IP アドレスだけでなくユーザー情報と結びつけた運用監視が可能になった。

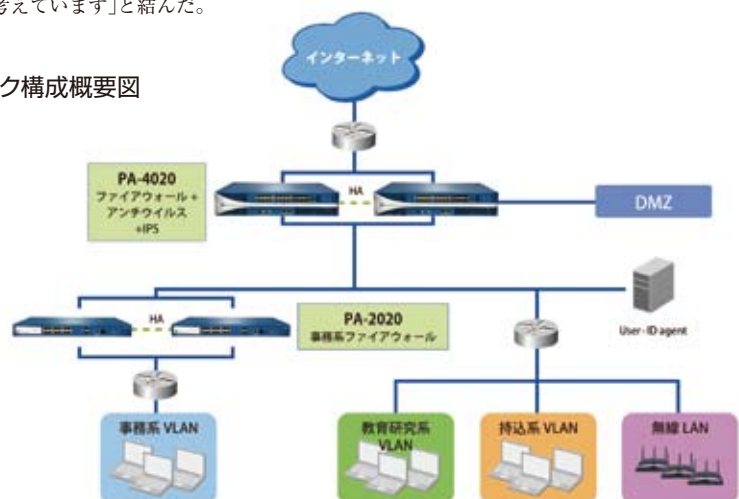
セキュリティ強化とキャンパスネットワークの自由度確保を両立

KOMAnet 更改の最大のテーマだったシステム構成のシンプル化によるコスト削減は、前述のようにゲートウェイの PA-4020 へのセキュリティ機能の統合によって実現され、PA-2020 によって物理的な台数削減を実現により達成できた。

一方、セキュリティ強化の観点では、PA シリーズのアプリケーション可視化・制御により、P2P アプリケーションのコントロールをはじめとして、不正アクセスだけでなく、意図しない情報漏えいに対しても対策強化が実現した。「大学としてのセキュリティ基本規程を策定し、ファイル共有ソフトの原則利用禁止条項を盛り込みましたが、実際の利用実態は完全に把握できず、ネットワーク上の全てを制御できる手段はありませんでした。PA シリーズの導入により、具体的に特定のアプリケーションを制御できるようになったことは大きな効果といえます」(成田氏)。また、基本的に学生や教員の教育・研究に自由に利用できる環境であることがキャンパスネットワークでは重要。「個々のアプリケーションレベルで教職員別、学部別などいろいろなユーザー環境によって通信を制御できることの導入メリットは大きい」(分銅氏)と強調する。

最後に、総合情報センター所長の金山智子氏は、「学生も教員も自由にネットワークを駆使して、安全に情報を活用できる環境を実現できました。それに加えて、企業のように情報を資産としてとらえ保護していこうという、情報に対する価値観、セキュリティに対する教職員や学生のマインドを高めていくことが重要と考えています」と結んだ。

ネットワーク構成概要図



パロアルトネットワークス
E-mail: InfoJapan@paloaltonetworks.com
www.paloaltonetworks.jp