

# 社内ネットワークのさらなるセキュリティ強化 アプリケーション可視化と脅威からの総合的な防御により 自由なネット利用環境を維持しながらセキュリティを強化

1万人近い芸能人・有名人が利用し国内最大のブログサービスやアバターコミュニティ、モバイルゲームなどを提供する「Ameba」の運営で知られるサイバーエージェント。社内ネットワークで頻りにウイルスが検出されたことをきっかけに、クライアントセキュリティに加えた多段的なセキュリティ環境を構築するために次世代ファイアウォールのPAシリーズを導入した。同ソリューションのアプリケーション可視化・制御や総合的な脅威防止機能により、より高いレベルのセキュリティを強化しつつ、社員の自由なネット利用環境を維持した。

## 多段的なレイヤーでの対策でセキュリティを強化

サイバーエージェントは、「Ameba」やモバイルソーシャルアプリ、スマートフォンアプリなどのインターネットメディア事業、インターネット広告代理事業を中心に1998年の設立以来、急成長を遂げてきたインターネット総合サービス企業である。特に同社の知名度を一躍高めたのが「Ameba」サービスだ。各種調査で国内最大のブログサービスとされ、芸能人や有名人などのタレントプロガーが多いことでも有名な「アメバブログ」、自分そっくりのアバターでチャットやゲームを楽しむ「アメバピグ」、モバイルサービス「Ameba モバイル」など多彩なサービスを展開し、今では月間2500万人以上が「Ameba」サービスを利用している。また、創業以来の主要事業であるインターネット広告代理事業は国内トップクラスを誇る一方、最近はソーシャルメディアに対してケータイやスマートフォン向けアプリを多数提供している。

同社の社員は、仕事柄その多くが多数のソーシャルメディアを日常業務の中で利用している。ソーシャルメディアを感染経路に悪用するマルウェアも多く、セキュリティリスクもある。「最近ではURLを簡素化したショートURLが使われているためにドメインが推測できず、注意していても悪意のあるページに飛ばされ、知らないうちにマルウェアをダウンロードさせられることも。2010年初め頃、クライアントセキュリティソフトで、そうした脅威が大量に検出される事態が起きました。既存のクライアントアンチウイルスでは不十分と感じ、多段的な対策によるセキュリティ強化の必要性が高まっていました」。同社の社内ネットワークインフラの担当者である高場大樹氏は、次世代ファイアウォールであるPAシリーズ導入の背景をこう述べる。

## アプリケーションの可視化、特定通信のみ遮断する機能を評価

高場氏がウイルスやスパイウェア対策の基本として考えていたことは、「感染しない」「拡散しない」「社外に出さない」の3つ。このうち「感染しない」対策はクライアントセキュリティソフトで実施しているため、「拡散しない」「社外に出さない」という点を重点にした提案依頼を各社に持ちかけた。特に既存アンチウイルスソフトの定期スキャンだけでもユーザーの業務に影響があるため、「ユーザーに体感値なく、セキュリティレベルの向上を実現したい」という条件を付けた。

依頼した各社からの提案は、IPS(侵入防止システム)やUTM(統合脅威管理)アプライアンス導入を指向するものが多かったというが、その中の1社にPAシリーズによる提案があった。高場氏自身がインターネットなどで知ったパロアルトネットワークスの次世代ファイアウォールに興味を示していたことも、その提案の拠りどころとなったようだ。

製品選定の検討にあたって、それぞれ実機を借り受けて約2週間にわたって検証を行った。検討の結果、採用に至ったのがPAシリーズだったが、その選定理由を高場氏は次のように述べる。

「他社のUTMはファイアウォールの強化版というイメージを払拭しきれず、またIPSによる対策は脅威となる通信をクライアントで検出すると、そのPC自体をネットワークから遮断するような仕組



## 株式会社サイバーエージェント

東京都渋谷区道玄坂一丁目12番1号 渋谷マークシティ  
<http://www.cyberagent.co.jp/>

## 分野

インターネット総合サービスプロバイダー

## 導入背景

- 日常的にソーシャルメディアや海外サイトなどを自由に使う業務環境
- クライアントセキュリティソフトで多数のウイルス、スパイウェアを検出
- 多段的な対策によるネットワークセキュリティ強化

## ソリューション

- アンチウイルス、IPS機能などによるネットワーク境界でのマルウェア対策
- アプリケーションの可視化・制御による脅威通信のブロックおよび予防的対策の体制構築
- Panoramaによる18台のPAシリーズの一元管理

## サイバーエージェントが導入した



PA-500



PA-2020

「PA は脅威となる特定の通信のみをブロックでき、予防的なセキュリティ体制を構築しつつ、自由なネット利用の環境を維持できました」



高場 大樹 氏  
サイバーエージェント  
人事部 全社人事グループ  
ワークプレイスクリエイティブチーム  
シニアスタッフ

みがほとんど。それに対し、脅威となる特定の通信のみをブロックする PA シリーズを高く評価しました。また、あらゆるアプリケーション通信を詳細に解析し、可視化・制御できること。しかも、アプリケーションを利用しているユーザーレベルで、それが可能な点に多くの可能性を感じました」(高場氏)。

また、高場氏は検証機を使ってみて、グラフィカルな管理用ユーザーインターフェースが優れていることも好評価。特にアプリケーションの種別、あるいはユーザーごとに通信をドリルダウンして分析する操作が非常にわかりやすいと指摘する。

導入されたシステムは、スループット 500Mbps (脅威防御使用時 200Mbps) の PA-2020 が 8 台、スループット 250Mbps (脅威防御時 100Mbps) の PA-500 が 10 台。本社ビルやデータセンターなど主要拠点 4 カ所に PA-2020 を、地方拠点 5 カ所に PA-500 を、それぞれ既存ファイアウォールの下に冗長化して設置。アプリケーション可視化・制御、アンチウイルス、IPS の各セキュリティ機能を利用している。また、すべての PA シリーズの集中管理するために、データセンターに Panorama を導入・運用している。

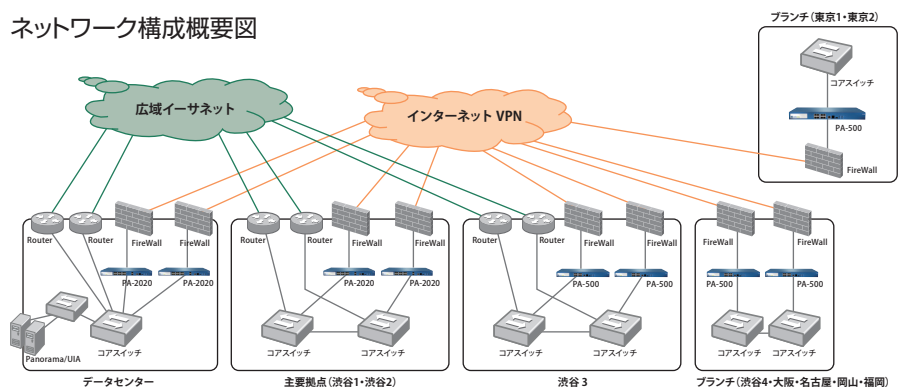
### アプリケーション通信の把握・制御で予防的なセキュリティ体制を構築

PA シリーズ導入後、クライアント側でウイルスやスパイウェアが検出されることはほとんどなく、社内ネットワークに拡散されることもないという。「導入後、1 カ月ほど PA シリーズ側で大量メール送信型ウイルスや悪質なアドウェアなど数件検出しましたが、その後はほとんどありません。社員に体感値がなく、セキュリティレベルが向上し、脅威を広めない、出さないという目的も達成できました」(高場氏) とし、ネットワークの脅威を多段的に防御する環境が実現したことに非常に満足しているという。

また、Panorama による全デバイスの管理・監視、アプリケーション通信の多角的な可視化・分析、パターンファイルやシグネチャのアップデート管理などが一元的にできるため、管理負荷もさほど増えず、逆にクライアント側の感染に伴うサポートが減少し、運用負担が減少した。

今後、高場氏はアプリケーションの可視化・制御機能を存分に使いこなしたいという。「Active Directory と連携させているので、ユーザーごと、あるいはユーザーグループごとに制御ポリシーを適用して、P2P アプリケーションなど危険性の高い通信をコントロールするなどして、安全な通信を確保したいですね」(高場氏)。基本的に自由なネット利用の環境を維持しつつ、PA シリーズで社員のアプリケーション利用状況を把握して、予防的なセキュリティ体制を構築していきたいと述べる。また、既存のファイアウォールとインターネット VPN 機能も PA シリーズに統合し、シンプルなセキュリティインフラを目指したいと展望する。

### 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