

# 病院ネットワークのセキュリティ強化 アプリケーション可視化・制御により 病院情報システムのリスク回避を実現

甲状腺疾患専門病院として名高い東京・表参道の伊藤病院。電子カルテを中心とする診療系情報システムと一般業務系情報システムを同じ基幹ネットワーク上で運用する同病院は、ネットワークのリプレースを機にさらなるセキュリティ強化を目的として次世代ファイアウォール「PA-500」を導入した。同機によるアプリケーションの可視化およびウイルス被害や、情報漏えいリスクの高いアプリケーションの制御を実現することで、更なる病院情報ネットワークの安全な運用を目指している。

## 院内ネットワークのセキュリティ強化に向けてPA-500を導入

東京・表参道の一等地で60床を有する伊藤病院は、1937年の開院以来、甲状腺疾患の専門病院として一貫して医療を提供している。27名の常勤医はすべて甲状腺疾患専門医で構成され、甲状腺疾患専門病院の中でも屈指の知名度を持つ。それを示すように、他の病院・診療所からの紹介患者も多い。診療圏は東京都内、関東全域にとどまらず全国に及び、韓国など海外からも患者が診断を仰ぎに訪れるという。外来患者は1日約1,000人に上り、血液検査、エコー、CTからアイソトープなど検査から治療・調剤まで同病院で完結できる体制を整え、来院のその日に検査、治療方針が決定できることを特長としている。

伊藤病院は、以前から伊藤公一院長自身が病院のIT化を推進しており、電子カルテシステムをはじめとする医療情報システムを積極的に導入している。また、一般業務系（情報系）システムについてもグループウェア、Google Appsによるメールシステムなども先進的に取り入れてきた。こうした基幹業務系および一般業務系は1つの基幹ネットワークを論理的にセグメントで分離し、約250台の診療端末、一般業務端末で利用されている。このネットワークは2002年に構築されたが、ネットワーク機器の更新時期を迎えたことと、その後にさまざまなシステムが導入され拡張の必要があったことから今回のネットワーク更改に至った。ネットワーク更改の大きな要件の1つがセキュリティ強化であり、エンドポイントセキュリティの導入とともに、外部ネットワーク境界におけるPA-500の導入だった。

「診療系システムと一般業務系システムは分離されていますし、端末は共有しているものの、一部一般業務系アプリケーションは仮想デスクトップで稼働させるなど、患者情報にかかわるセキュリティは担保されています。しかし、USBやWebサイト経由のウイルス被害、ファイル共有のWinMXなど、情報漏えいリスク対策は従来以上に強化する必要がありました」。事務部システム管理主任の齋藤功氏は、PA-500導入に至った経緯をこう述べる。

## アウトバウンドのトラッキングとアプリケーション制御を目的に導入

PA-500導入の背景には、医療機関においてファイル共有ソフトによる情報漏えいが問題となっていることがあげられる。当院では、職員には同様のソフトの利用禁止の誓約書を取っているものの、論理的に確実に使用をブロックしなかったことが直接的にある。それに加え、Webサイト経由のウイルス被害や情報漏えいリスクの高いWeb利用を制御するために、まずはトラフィックを可視化し、トラッキングすることが大きな目的だった。

齋藤氏は、病院のコンプライアンスに基づくセキュリティ制御をするためにネットワーク境界でのセキュリティ製品を探していたところ、ネットワークインフラのリプレースを依頼したイ

IT HOSPITAL



### 伊藤病院

東京都渋谷区神宮前 4-3-6  
<http://www.ito-hospital.jp/>

### 分野

医療機関

### 導入背景

- 基幹ネットワークのリプレースにあわせたセキュリティ強化
- 情報漏えい対策としてのファイル共有ソフトのブロック
- ウイルス被害を未然に防ぐ通信のトラッキング
- セキュリティ強化のためのアプリケーション可視化・制御

### ソリューション

- アウトバウンド通信におけるアプリケーションファイアウォール機能、URLフィルタリング機能などにより、アプリケーション可視化・制御

「アプリケーションをカテゴリベースで可視化・制御でき、しかも使いやすく、わかりやすいGUIであることから、PA-500を選定しました」



齋藤 功氏  
伊藤病院  
事務部  
システム管理主任

ンテグレートからパロアルトネットワークス製品の提案を受け、その採用に至ったものだが、選定した理由を次のように語る。

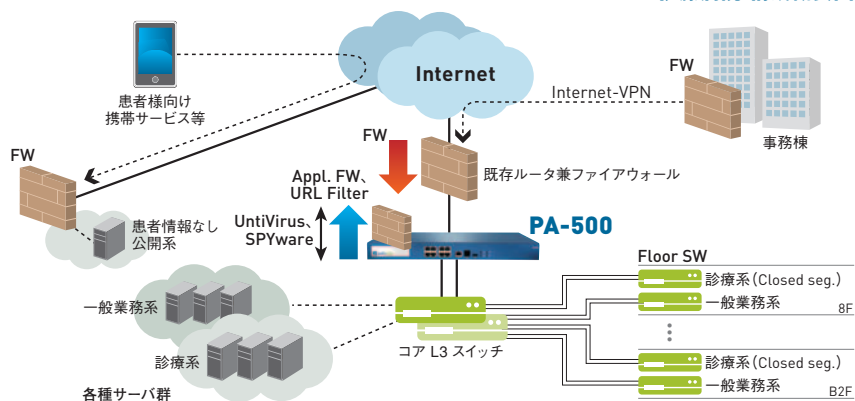
「ファイル共有ソフトをはじめ、増加するネットワークアプリケーションをカテゴリベースで可視化・制御できる能力が優れていたこと。その設定やネットワークの利用状況をドリルダウンでチェックする際に非常にわかりやすいGUIであったこと。また、URLフィルタリングや各種の脅威検出の機能を利用しても性能が落ちないということを知り、ネットワークリプレースの総予算の中で十分なコストパフォーマンスを発揮してくれると判断したからです」(齋藤氏)。

### トラフィックの可視化・把握により対策手段が明確に

PA-500の導入によって、当初の目的であるファイル共有ソフトの利用はブロックされ、そのリスクは回避できた。あわせて、Web経由のウイルスのトラッキング、オンラインストレージなど情報漏えいにつながる危険性のあるアプリケーションの利用などが完全に可視化され、次のステップであるアプリケーション制御へのプロセスが見えてきたという。トラフィックの把握が容易になったことに対して、「業務に関係ないと思われるサイトの利用が把握できたことや、オンラインストレージやファイル預りサービスが職員によってどう使われているか認識できました。オンラインストレージなどの利用頻度によって業務効率上で必要であるなら、それに代わる安全なアプリケーションを提供する必要があります。その判断をする上でアプリケーション可視化は非常に役立ちます。また、事務部門がある隣のビルからインターネットVPNを使ってグループウェアシステムにアクセスしていますが、PA-500はそうしたエクストラネット的なセグメントの可視化にも有効であると理解できました」と齋藤氏は指摘する。

現在、PA-500はファイアウォール機能付きルータの下に透過型で配置されており、ルータ兼ファイアウォールがインバウンド側のセキュリティを、PA-500がアウトバウンド側の通信を制御している。今後、徐々にファイアウォール機能付きルータのファイアウォールポリシーをPA-500に移行し、既存機器の更新時には既存ルータを取り外し、PA-500をインターネット直結の機器として利用することも検討している。また、電子カルテシステムはベンダーによるVPNを使ったりリモートメンテナンスが行われていることや、隣接の事務棟からのアクセスも多いことから、障害に備えた冗長化構成にする方針でもある。

伊藤病院 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