

# アプリケーションの可視化・制御をベースにセキュリティリスクを低減 複合的な脅威防御でセキュリティ向上を実現 建設会社の安全なネットワーク利用を支える

全国各地でインフラ整備や住宅、再開発などの都市機能整備に関わり、地域社会の活性化に貢献する東急建設。ネットワークのゲートウェイシステムの更新を機に、ファイアウォールをはじめ複数のセキュリティ機器を統合してコスト削減を実現するとともに、新たな脅威に対してアプリケーションの可視化・制御をベースにネットワーク利用の安全性を向上させた。そのソリューションとして採用されたのが、次世代ファイアウォールPA-2050である。

## トラフィック増大に対応する性能確保、セキュリティ向上を目的にリプレース

総合建設業(ゼネコン)準大手、東急建設は1946年の創業以来、半世紀以上にわたり全国各地でインフラ整備や住宅、再開発などの都市機能整備に関わり、地域社会の活性化に貢献してきた。特に東急グループの一員として鉄道関連工事を軸として東急沿線地域の開発、商業施設の建設などで多くの実績を積んでいる。現在も渋谷駅東口・東急文化会館跡地周辺開発、二子玉川東地区の再開発(二子玉川ライズ開発プロジェクト)、たまプラーザ駅周辺再開発などのビックプロジェクトに携わっている。

同社は東京・渋谷の本社をはじめ、全国主要都市に12の支店を持ち、さらに全国の工事現場の数百カ所に作業所があり、これらを結ぶネットワークは事業の重要なインフラとなっている。また、建設業では共同企業体(JV)としてプロジェクトを進めることがあるが、その際、同業他社のPCを自社ネットワークに接続させることが日常的に行われている。そのため以前から、安全性と利便性の両立が担保されたセキュリティ環境が必要とされている。「作業事務所内はJV各社のPCが1つのLANで構成されています。各社がそれぞれルーターを設置してアクセスに対するセキュリティは担保されているものの、自社ネットワークと他社のPCがつながっていてもいい環境が建設会社のネットワークには求められています」。管理本部情報システム部システムセンター長 吉村典之氏は、ネットワーク環境の特殊性を指摘する。

こうしたセキュリティレベルのさらなる向上に加えて、同社では2004年に導入したファイアウォールやルーター、プロキシサーバーなどのセキュリティ・ネットワークシステムの老朽化が進み、トラフィックの急増に対して機器の性能が追いつかない状態になっていた。また、複数のサーバー、セキュリティソフトで構成された旧システムは、運用負荷が大きく、ソフトウェアライセンスの更新やハードウェアの保守など高額の運用コストも課題だった。

## アプリケーションの可視化・制御による脅威防御の先進性を評価

2010年4月にリプレースの本格的な検討を開始し、トラフィックのボトルネックを解消するとともに、5年後のトラフィック増加に対しても性能を維持できること、セキュリティ機能を統合することにより運用負荷とコスト削減を実現することを要件としてベンダーに提案を依頼した。ところが、そのUTMへのリプレースを中心とする提案は、アンチウイルスなどのセキュリティ機能を使用するとスループットの低下が著しく、要件を満たすためにはハイグレードのモデルを導入する必要があった。結果的にアンチウイルスとURLフィルタリングは従来システムのバージョンアップという提案で、満足できるものでなかった。そこで、システムセンターでインフラを担当する前保俊洋氏は、以前から注目していた次世代ファイアウォールについて、同製品の販売パートナーに提案を持ちかけ、実機検証を経て導入に至ったものである。

「最近では80番ポートを使用するアプリケーションが増加しており、従来のファイアウォールのようにポート番号とプロトコルだけでトラフィックを制御しきれなくなっているため、次世代ファイアウォールのアプリケーションの可視化・制御機能に大きな魅力を感じました。また、ファイア



### 東急建設株式会社

東京都渋谷区渋谷1-16-14 渋谷地下鉄ビル  
<http://www.tokyu-cnst.co.jp/>

### 分野

土木建設業

### 導入背景

- 複数の機器で構成されるゲートウェイシステムの老朽化、トラフィック増大に伴うアクセス性能の低下
- プロトコルとポート制御で対応できない新たな脅威となり得る通信への対応
- 複数のシステムを運用することによる、運用負荷とコストの負担

### ソリューション

- ユーザーベースのポリシー設定によってネットワーク上のアプリケーションの可視化・制御
- App-ID、Content-IDによる複数の防御機能の統合で、運用負荷とコスト削減の実現
- 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る高いスループットと複数のセキュリティ機能の両立



東急建設が導入したPA-2050

「社内に安全なファイル共有・転送の仕組みを作り、アプリケーション制御機能によりファイル転送サービスの利用を禁止するなど、潜在するリスクの低減が実現できると期待しています」



吉村典之 氏  
管理本部情報システム部  
システムセンターセンター長

「80番ポートを利用するアプリケーションの制御に、次世代ファイアウォールの大きな魅力を感じます」



前保俊洋 氏  
管理本部情報システム部  
システムセンター

ウォール機能に加えて、アンチウイルスや URL/ データフィルタリング、IPS など複数のセキュリティ機能を使用してもスループットの低下がほとんど見られず、コスト削減も実現できます」(前保氏)と採用の理由を述べる。

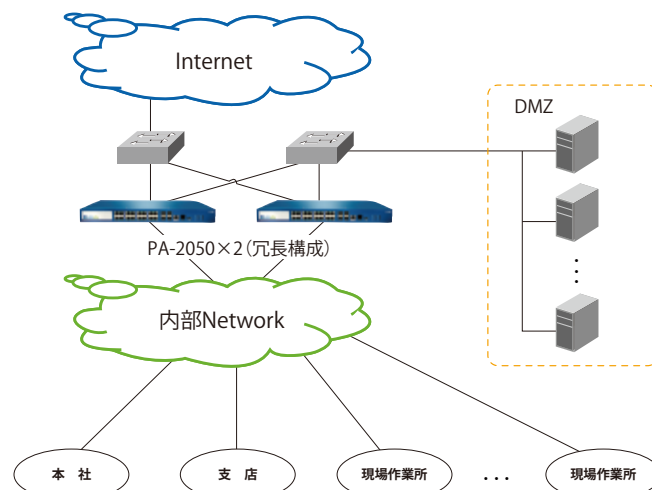
### トラフィックの確実な認識と制御でセキュリティリスクを低減

導入した PA-2050(冗長構成)によって、従来のルーター、ファイアウォール、アンチウイルスサーバー、URL フィルタリングサーバーを機能統合できたため、年間数百万円のコスト削減を実現。ボトルネックが解消され業務に影響を与えるような遅延もなくなった。期待したアプリケーションの可視化・制御機能については、「可視化・制御可能なアプリケーション数が多いことに加えて検出の精度も高く、セキュリティリスクとなる危険性がある VPN ソフトや P2P アプリケーション、Web サイトに埋め込まれたアプリケーションを確実に把握できるようになりました」と前保氏。脅威となり得る通信をプロアクティブに防御できる態勢ができ、利用されているアプリケーションがネットワーク帯域どの程度占有しているか把握できるようになったことで、各種セキュリティ施策やシステム投資計画に活かすことができるようになったという。

また、アプリケーション可視化・制御をユーザー ID にひも付けて実施できることにより、外部の LDAP で認証が必要な電子入札ソフトの利用において、従来のファイアウォールで不可能だった DHCP 環境での個別ポリシーの適用が、利用ユーザーのみに適用して通信が可能になり、クリティカルな通信の安全性が高まったと指摘する。

建設会社では顧客や協力会社と CAD 図面など大容量データを頻繁にやり取りする。従来は Web サービスのオンラインストレージやファイル転送サービスを使用するケースが多かったが、機密性の高いデータのやり取りには好ましいとはいえない。吉村氏は、「今後、社内に安全なファイル共有・転送の仕組みを構築し、アプリケーション制御で外部のオンラインストレージサービスやファイル転送サービスの利用を禁止することにより、セキュリティ対策を強化したい」と述べ、アプリケーション可視化・制御をベースにしたネットワーク利用の安全性向上に大きな期待を寄せている。

### 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