大容量スパムメール対策を実現する AXのセキュアメールソリューション

THE APPLICATION PLATFORM

ソリューションブリーフ
AXシリーズ

■ 増加するスパムメールに対する課題

いまや電子メールは個人や企業を問わず、コミュニケーションインフラとして定着しており、スマートフォンやネットブックなど、様々なクライアントの普及によりその利用環境も大きく広がっています。その一方で、電子メールの活用に伴うセキュリティのリスクも急速に高まっており、情報漏洩、ウイルス、ワーム、スパイウェア、フィッシング、ボット、スパムなどメールを媒介とする脅威はますます多様化しています。スパムメールは、全世界でやり取りされている電子メールの約90%を占めていると言われており、企業活動におけるセキュリティリスクの上昇や生産性の低下、サーバリソースの浪費を招いています。サービスプロバイダにとっては、スパムメールの被害を広げてしまうリスクや、大量のスパムメール処理によるサービスパフォーマンスの低下など、ビジネスに大きな影響を与える深刻な問題になっています。メールフィルタなどによる現行のセキュリティ対策だけでは、現在、そして今後も増加するトラフィックに対して十分なパフォーマンスを維持するのは困難です。もし、スパムフィルタと連携して大量のトラフィックに耐えるセキュリティ対策を行うことができれば、スパムフィルタの負荷は軽減され、よりハイパフォーマンスで安定したメールサービス環境を構築することができるようになります。

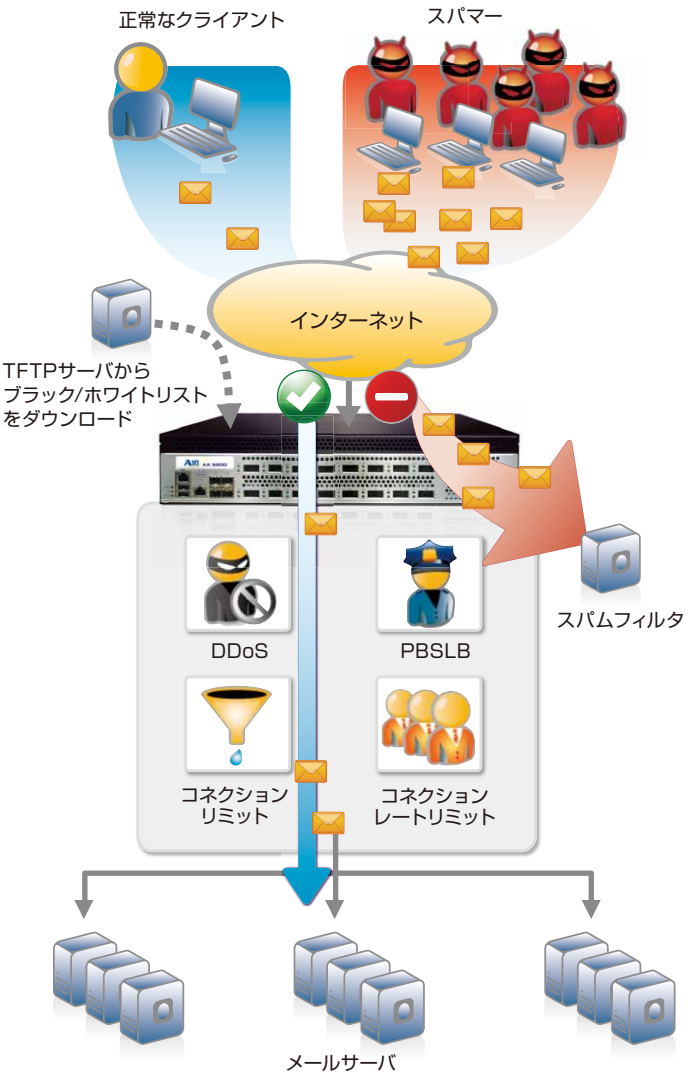
■ AXシリーズによる大容量スパムメール対策

A10ネットワークスのアプリケーションプラットフォームAXシリーズは、マルチコア・マルチCPUに最適化されたA10の独自OS (ACOS: Advanced Core Operating System)と64ビット対応の専用ハードウェアにより業界最高峰のパフォーマンスを実現します。既存のスパムメール対策製品と、ハイパフォーマンスなAXシリーズのPBSLB機能とを組み合わせることによって、高速で大容量なスパム対策ソリューションを提供することが可能です。PBSLB機能に加えて、AXシリーズのDDoS対策機能、コネクションリミット機能を併用することにより、サイト全体にわたるセキュリティも高めることができます。

■ PBSLB (Policy Based Server Load Balancing)機能

AXシリーズは、スパムフィルタよりも先にトラフィックを受信し、最初の防御壁として高速なスパムの振り分けを実現します。

AXシリーズのPBSLB(Policy Based Server Load Balancing)を使用すれば、第三者機関で公開されているブラックリスト/ホワイトリスト(BWリスト)を振り分けのポリシとして活用し、送信元のIPアドレスを基に事前に定義したアクション(パケットの破棄・コネクションのリセット・特定サーバグループへのリダイレクト)を高速に実行することが可能です。PBSLBで使用するBWリストには、IPv6を使用することも可能なため、IPv6ホストからのアクセスに対してもポリシを適用することができます。PBSLBは、AXシリーズに設定された仮想IPアドレス毎に定義することができるため、メールサーバのグループ毎に異なるポリシを個別に設定することが可能です。これにより、サービスレベルの異なるメールサービスを提供することができます。AXシリーズのPBSLBは、ブラックリスト/ホワイトリストに、最大で800万のホストアドレス、64,000のサブネットアドレスを設定することが可能であるため、精度の高いシステムを構成することができます。

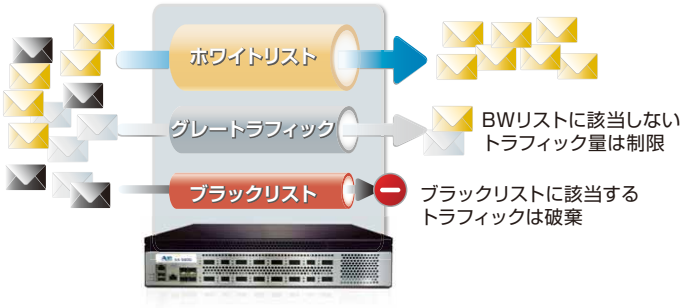


大容量で高速なスパムメール対策を実現する
PBSLBソリューション

■ 急増するトラフィックからのサーバ保護

AXシリーズは、送信元クライアントからの最大コネクション数を制限するコネクションリミットや秒間当りのコネクション数を制限するコネクションレートリミットをサポートしています。これらの機能をPBSLBと同時に利用することで、例えば、送信元IPアドレスがBWリストに該当しないグレーなメールのトラフィック量を抑え、ホワイトリストに該当する正当なトラフィックを多く通過させるなど、ポリシ毎にトラフィックを制限することが可能となり、正規の使用者にとって快適なメール環境を実現できます。

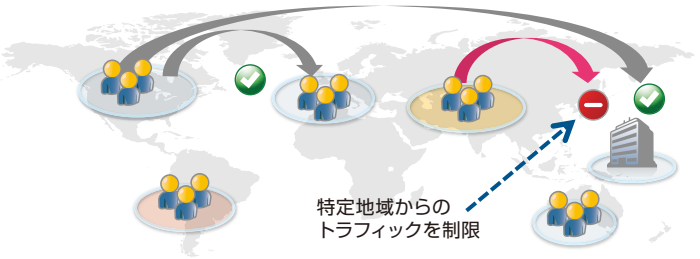
スパムメールの80%以上はボット化したホストから送信されていると言われており、メールサーバは、ボットのフラッディング攻撃によるサーバダウンの危険に常にさらされています。AXシリーズを導入することによって、メールサーバに到達するはずだったボットの攻撃を、AXが持つSyn-CookieなどのDDoS対策機能により、サーバの直前で防御するため、サーバダウンの可能性を最小限に抑えることができます。



スパムメールの量を抑えて正当なメールを多く通過させる
PBSLB+コネクションリミット機能

■ 特定地域からの攻撃対策

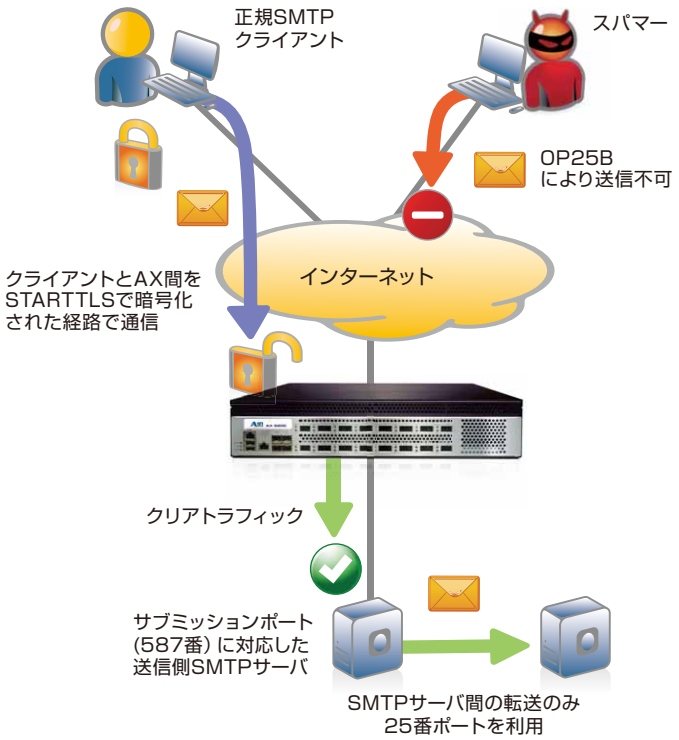
AXシリーズは、特定の地域からのアクセスに対してコネクション数を制限したり、アクセスを拒否したりすることができます。AXシリーズのGeo-Location機能では、アクセスしてくるユーザのIPアドレスを基に、地域情報とIPアドレスを関連づけたデータベースを参照してユーザがいる地域を特定します。このGeo-Location機能とコネクションリミットやACLを組み合わせることで、特定の地域からのトラフィックを制御することができます。このデータベースは、サードパーティから提供されるものをCSVでインポートして利用することができます。カスタマイズも可能で、ユーザ独自のデータベースを構築することもできます。



特定地域からのアクセスを制限する Geo-Location機能

■ スパムメールの被害拡大を防ぐ対策

現在、サービスプロバイダでは、スパムメールの被害拡大を防ぐ対策としてOP25B(Outbound Port25 Blocking)とともにサブミッションポート(Port 587)の利用が進んでいます。AXシリーズは、サブミッションポートを利用するSMTPのクライアントとサーバ間の暗号化経路を提供するSTARTTLSの機能をサポートしています。AXがSSLプロキシとして暗号化トラフィックの終端・復号化を実行することで、メールサーバの負荷を軽減させ、パフォーマンスを向上させます。



メールサーバの負荷を軽減するAXのSTARTTLS機能

■ AXによるハイパフォーマンスなセキュアメール環境

A10ネットワークスのAXシリーズは、最先端のマルチコア・マルチCPU技術を独自OSである「ACOS」アーキテクチャで最適化することにより、柔軟なトラフィック制御を実行しながらも、業界最高峰のパフォーマンスを実現しています。AXシリーズの圧倒的なパフォーマンスは、増加するスパムトラフィックにも十分対応可能であり、同時にメールサーバの負荷を軽減します。これにより、メールサービスの停止を回避し、サービスを継続して提供できます。AXシリーズを導入することにで、よりハイパフォーマンスで安定したメールサービス環境を構築することができるようになります。

A10 Networks
A10ネットワークス株式会社
〒105-0001 東京都港区虎ノ門4-3-20 神谷町MTビル 16階
TEL: 03-5777-1995　FAX: 03-5777-1997
Email: jinfo@a10networks.com
http://www.a10networks.co.jp

お問い合わせ