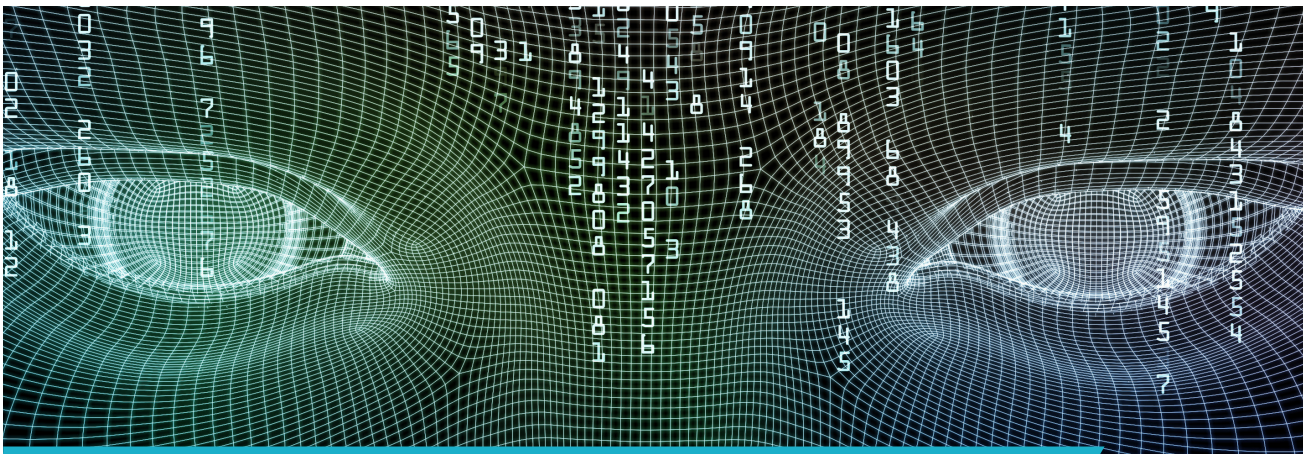
ixia

WHITE PAPER



効率的なセキュリティ対策実現のポイントは、インターネットの“縮小”？

日々、高度化し増えるサイバー攻撃。数々のセキュリティ対策製品を導入しても、警告が多過ぎて管理者が対応しきれなくなる可能性がある。その問題をトラフィックに注目して解決する方法がある。

膨大な警告に悩まされるセキュリティ管理者

私たちの企業活動には、もはやインターネットは欠かせない存在となっている。しかし、インターネットに散在するサイバー攻撃の脅威が、ビジネスを脅かす原因となっているのは疑いようがない。そうしたリスクを軽減し、有事に備えるために、一般的な組織ではできる限りのセキュリティ対策を実施していることだろう。

企業ネットワークは、膨大な数の攻撃トラフィックを日々受け取っている。その多くは、ゲートウェイに設置された数々のセキュリティツールで防ぐことができている。しかしながら、それらを管理するセキュリティ担当者やトラフィックをチェックするデバイスは、もはや限界に近い状態に追い込まれている。

攻撃トラフィックのほとんどは、セキュリティデバイスが適切に検知して、管理者へ警告する。あらゆる攻撃に対処するため、次世代ファイアウォールやIPS（侵入防止システム）、アンチマルウェア／アンチスパム、コンテンツフィルタリングなどを定番のセキュリティデバイスを導入している企業は少なくない。また、サンドボックスやDDoS防御、情報漏えい防止といった新しい技術を導入していれば、その分だけ警告の種類が増えることになる。その上、膨大な攻撃トラフィックが流れ込んでくれば、警告が多過ぎて管理者が対応しきれなくなる恐れがある。セキュリティデバイスに掛かる負荷が上昇し、誤検知や検出漏れが発生する可能性も高まるだろう。

膨大なアラートを効率よく処理するためにセキュリティイベント管理（SEIM）ツールを駆使する方法もある。しかし、こうしたツールは高価であるし、誤検知や検知漏れを完全に追跡できるわけではない。軽微な問題であっても警告がやむことはなく、むしろ管理者を“アラート疲れ”に追いやっている。

そこで、そもそも分析すべきトラフィックを少なくするという新しい考え方を提案するのが、イクシアコミュニケーションズの「ThreatARMOR」である。

分析すべきトラフィックと分析する必要のないトラフィック

ThreatARMORは、ファイアウォールやIPS、アンチマルウェアといったセキュリティデバイスを配置する“セキュリティインフラ”を挟みこむように配置するゲートウェイデバイスである。インターネットから入ってくるトラフィック、あるいは企業ネットワークから外に出るトラフィックを事前にチェックし、セキュリティインフラで分析する必要のないものを排除する。

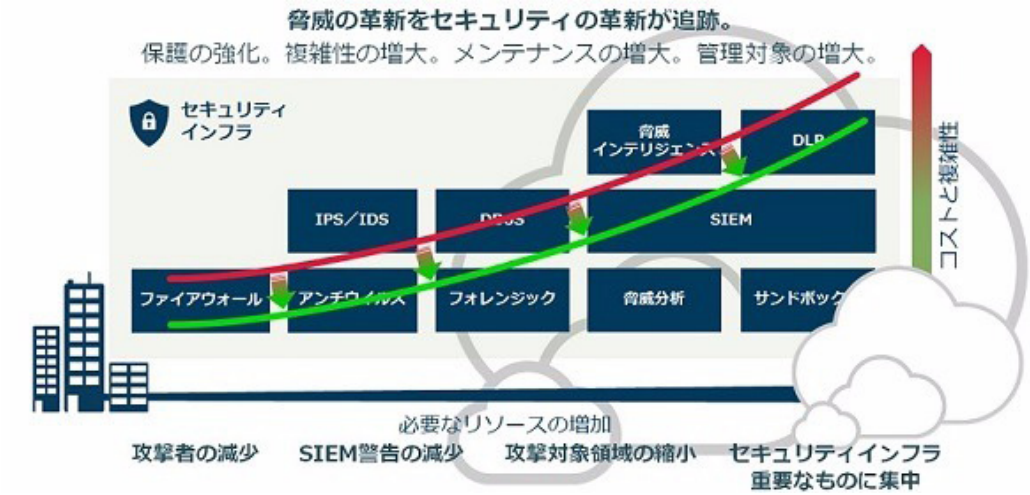
イクシアコミュニケーションズ 公共・エンタープライズ営業部 部長の野澤さゆり氏は、この技術・仕組みを「**インターネットを縮小するもの**」と表現する。

もともとイクシアコミュニケーションズは、セキュリティベンダー向けのテストデバイスを開発してきた。その経験を基に、専門の「ATI」（Application and Threat Intelligence）開発センターを設置して、攻撃の手口や防御の手法を長年にわたって研究し、知見を蓄積してきた。そうした知見は、世界各国に「脅威情報プログラム」として提供しており、ThreatARMORでも活用されている。

いわゆるシグネチャベースの検知ではないため、非常に高速な分類が可能で、ネットワークに負荷を掛けることもない。また、特殊な情報構造を採用しており誤検知が起きる心配もない。セキュリティインフラに負荷が掛かるトラフィックを大幅に削減でき、無駄の多いインターネットを効率よく縮小するというわけだ。

イクシアコミュニケーションズ
野澤氏

「実はThreatARMORが見ているのは、トラフィックのIPアドレスのみです。既に攻撃者が利用していたり、ハイジャックしていたり、一般的に利用するものとして登録されていなかったりするIPアドレスからのトラフィックをバッサリと切ることで、本当に価値のあるトラフィックのみに分析を集中できるようになるのです」（野澤氏）



インターネットを縮小することでセキュリティコストと複雑性を下げることができる

分析すべきトラフィックをさらに最適化して無駄をなくす

ThreatARMORでインターネットを縮小したとしても、分析すべきトラフィックは決して少ないとはいえない。より効率的で効果的なセキュリティ分析をするためには、トラフィックの状態や内容に合わせて、最適な分析手法を割り当てればよいはずだ。

例えば、Webサービスの通信を深く分析したいのに、その部分をファイアウォールやIPSに通す必要はないだろう。また、コンテンツフィルタリングツールが、通信プロトコルについて分析することはできない。

そこで役に立つのがイクシアコミュニケーションズの「Vision ONE」だ。SSL暗号化通信や仮想化環境にも対応し、ネットワークトラフィックを完全に可視化（見える化）して、効率のよいセキュリティ分析をできるようにするソリューションである。

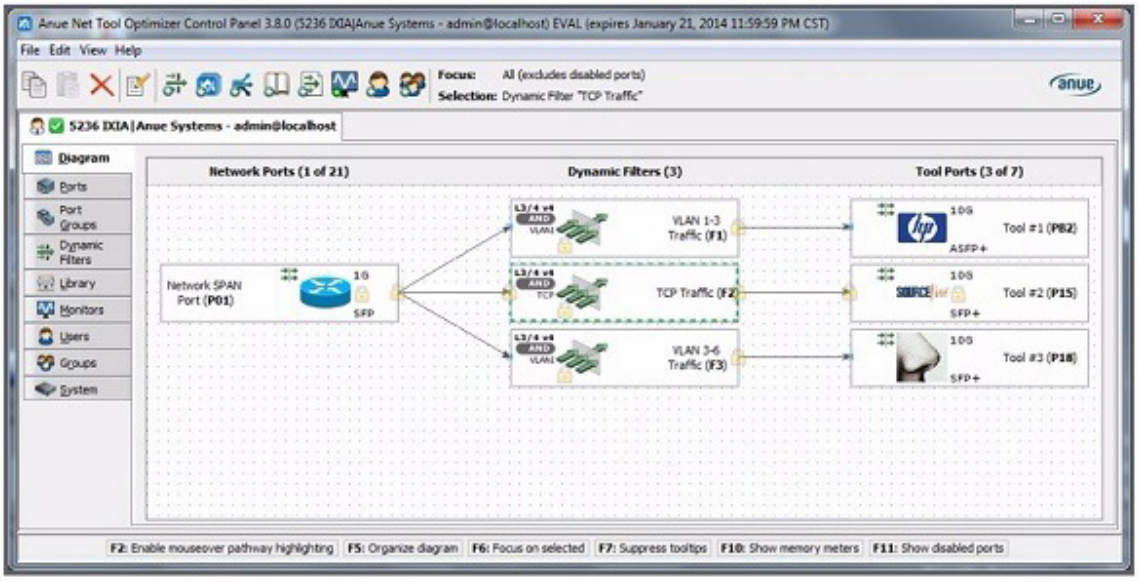
上述のATI開発センターでは、テスト用に攻撃を模したトラフィックを開発すると同時に、実環境のトラフィックについても深く研究してきた経験を持つ。そうして培ってきた知見を応用して開発された高精度なトラフィック分析技術が、Vision ONEに実装されている。

Vision ONEは、分析に不要な箇所を取り除く「パケットトリミング」や個人情報が解析ツールへ取り込まれないようにする「データマスキング」といった機能を駆使して、最適な状態でセキュリティデバイスへデータを渡すことができる。1つのトラフィックを複数のツールへダイナミックに振り分けたり、冗長化されたデバイスに多数のトラフィックをロードバランシングしたりすることも可能だ。

イクシアコミュニケーションズの西形氏

こうしたフィルタリングルールは、ユーザーが自由に設定することができるが、イクシアコミュニケーションズは画期的な手法を選択した。GUIでアイコンを並べて必要な情報を入れるだけで、自動的にルールが生成されるようにしたのだ。

「一般的なフィルタリングツールでは、コマンドラインからコンフィグを1行ずつ入力するため、非常に大変な思いをしているはずです。あるユーザーでは、試行錯誤しながら4時間かけて、やっと1つのフィルタリングを設定できたというケースもありました。Vision ONEでは、同じルール設定を10分で完了できたと高く評価しています」と、イクシアコミュニケーションズ システムエンジニアリング部 システムエンジニアの西形 渉氏は自信を見せる。

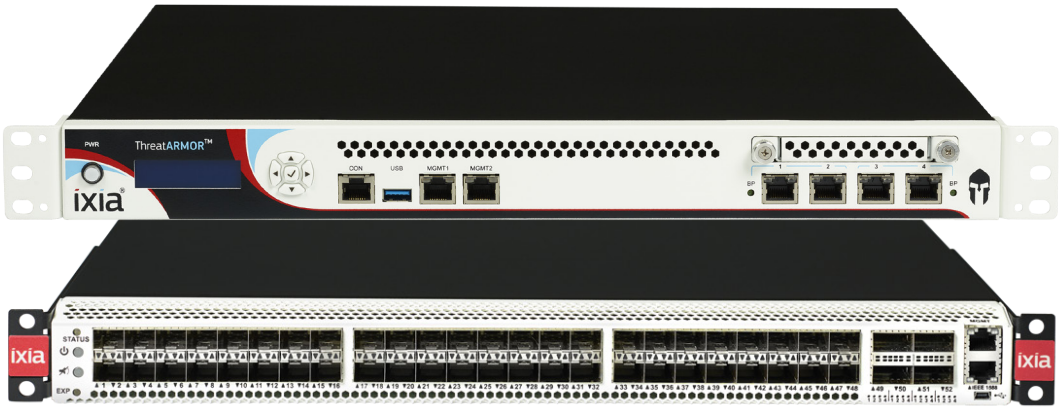


もしフィルタリングルールがオーバーラップする場合、非常に複雑なコンフィグを何行も間違えずに入力していかなければならない。Vision ONEの管理インタフェースであれば、オーバーラップも自動的に処理して、パケットロスのないルールを設定できるというわけだ。

ThreatARMORとVision ONEを組み合わせることにより、ハイパフォーマンスなセキュリティデバイスを導入する必要が無くなり、セキュリティインフラの機能を最大化することが可能となる。管理者は、人でなければ対処できないインシデントに集中し、迅速かつ的確な対応を取れるようになるだろう。“セキュリティインフラと運用の最適化”という新しいレイヤーを設けるソリューションといえる。

さらにイクシアコミュニケーションズは、10Gbps対応ThreatARMORやスケールアウト対応のVision ONEなどを発表し、よりさまざまな環境に適合するソリューションとして継続的に開発する意向だ。

「今後、国内企業を狙った脅威がさらに増加すると予想されています。どんなに小さな企業でも、膨大な攻撃トラフィックにさらされることになります。その多くは、ThreatARMORによって排除することが可能です。まずはインターネットを縮小することから始めてみてはいかがでしょうか」
（西形氏）



イクシアコミュニケーションズ株式会社
〒160-0023 東京都新宿区西新宿6-24-1
西新宿三井ビル11F
TEL: 03-5326-1948
:salesjapan@ixiacom.com | jp.ixiacom.com

IXIA WORLDWIDE HEADQUARTERS
26601 AGOURA RD.
CALABASAS, CA 91302

(TOLL FREE NORTH AMERICA)
1.877.367.4942

(OUTSIDE NORTH AMERICA)
+1.818.871.1800
(FAX) 1.818.871.1805
www.ixiacom.com

IXIA EUROPEAN HEADQUARTERS
IXIA TECHNOLOGIES EUROPE LTD
CLARION HOUSE, NORREYS DRIVE
MAIDENHEAD SL6 4FL
UNITED KINGDOM
SALES +44.1628.408750
(FAX) +44.1628.639916

IXIA ASIA PACIFIC HEADQUARTERS
101 THOMSON ROAD,
#29-04/05 UNITED SQUARE,
SINGAPORE 307591

SALES +65.6332.0125
(FAX) +65.6332.0127