



今日、セキュリティに対する脅威は、その種類、数、被害の深刻さにおいて日々増しており、特に、IPセキュリティへの対策は、インターネットアプリケーションサービスを取り扱う企業にとって非常に重要です。

認証とデータセキュリティ実現のために、EAPOL (802.1x) 関連のユーザー認証、PPP、暗号化方式 (IPsec、TLS、SSL) 等のプロトコル運用をデバイスが設計されていますが、いずれも、セキュリティ、高回復性、堅牢性が不十分なために悪意の第三者から攻撃の標的にされるリスクを潜んでいます。

ネットワーク機器メーカー (NEM)、サービスプロバイダー、システムインテグレーター、エンタープライズは、常に「最新の脅威に対応できるセキュリティ対策」を施しながら「最適なネットワークパフォーマンス」を確保するために、継続的な脆弱性テストが不可欠です。

また、ファイアウォール、侵入検知および防止システム (IDS/IPS)、ゲートウェイアンチウィルス、IPSecゲートウエ

イ等の「セキュリティ系デバイス」は、定期的にアップデートさせて、常に最新の防御環境を備える必要があります。

イクシアのIxLoad-Attackでは、ネットワークで運用中のデバイスをマルウェアやDDoS攻撃から防御します。

IxLoad-Attack

- 脆弱性、マルウェア、高性能型のDDoS攻撃を含むライブラリを継続的にアップデートすることで、これらの脅威に対するネットワーク防御の強化、脅威検出機能の検証テスト、セキュリティ装置の精度の報告を行います。
- エミュレーションできる通常のアプリケーショントラフィックと共に、攻撃をシミュレーションできます。これにより、攻撃系トラフィックと正常系トラフィックの混在環境を作り、「ネットワークセキュリティ装置」に攻撃を行いつつ、スループット性能を測定できます。

製品	説明
IxLoad-Attack	<ul style="list-style-type: none"> 標準で6,000種類の攻撃トラフィックをシミュレーション可能 攻撃パターンを任意にカスタマイズ可能 フルラインレートでのDDoS攻撃を生成 定期的な定義ファイルの更新サービス(攻撃パターンの種類を増加可能) 同じポートで正常系、攻撃系トラフィックを混在可能 IPSecトンネル上でも攻撃トラフィックを生成可能

This material is for informational purposes only and subject to change without notice. It describes Ixia's present plans to develop and make available to its customers certain products, features, and functionality. Ixia is only obligated to provide those deliverables specifically included in a written agreement between Ixia and the customer.