

## Cisco Traffic Anomaly Detector XT 5600



### 製品概要

Cisco® Traffic Anomaly Detector XT 5600 は、各種サービス プロバイダー、企業、政府機関、教育・研究機関等のネットワークを、Distributed Denial of Service (DDoS; 分散型サービス拒否) 攻撃やその他のサイバー攻撃から防御するための完璧なソリューションです。これにより、攻撃が業務に悪影響を与える前に、すばやく抑制サービスを起動して攻撃をブロックできます。

特許を取得した独自の Multiverification Process (MVP) アーキテクチャに基づく Cisco Traffic Anomaly Detector XT では、最新の動作分析および攻撃識別テクノロジーを利用して、あらゆるタイプのサイバー攻撃を早い段階で検出して識別できます。

Cisco Traffic Anomaly Detector XT では、Web サーバや e- コマース アプリケーション サーバといった保護対象となるデバイスへ向かうトラフィックを常時モニタすることにより、「正常な」動作状態を示す詳細なプロファイルが個々のデバイスに対して作成されます。Cisco Traffic Anomaly Detector XT は、フロー単位でプロファイルと比較し、プロファイルと異なる動作を検出すると、それを攻撃の兆候とみなして対応します。この対応オプションには、オペレータに警告を送って手動で対応できるようにする、既存の管理システムを起動する、Cisco Guard XT DDoS 軽減対策アプライアンスを起動してただちに抑制サービスを開始する、などがあります。

Cisco Traffic Anomaly Detector XT と Cisco Guard XT を組み合わせれば、業界で最も包括的な DDoS 防御システムを実現できます。Cisco Traffic Anomaly Detector XT および Cisco Guard XT は、MVP アーキテクチャに基づき、適正なトランザクションに影響を与えることなく不正な攻撃フローを検出/ルート変更/隔離/除去することにより、ネットワークおよびビジネスクリティカルなトラフィックを確実に保護できます。

### アプリケーション

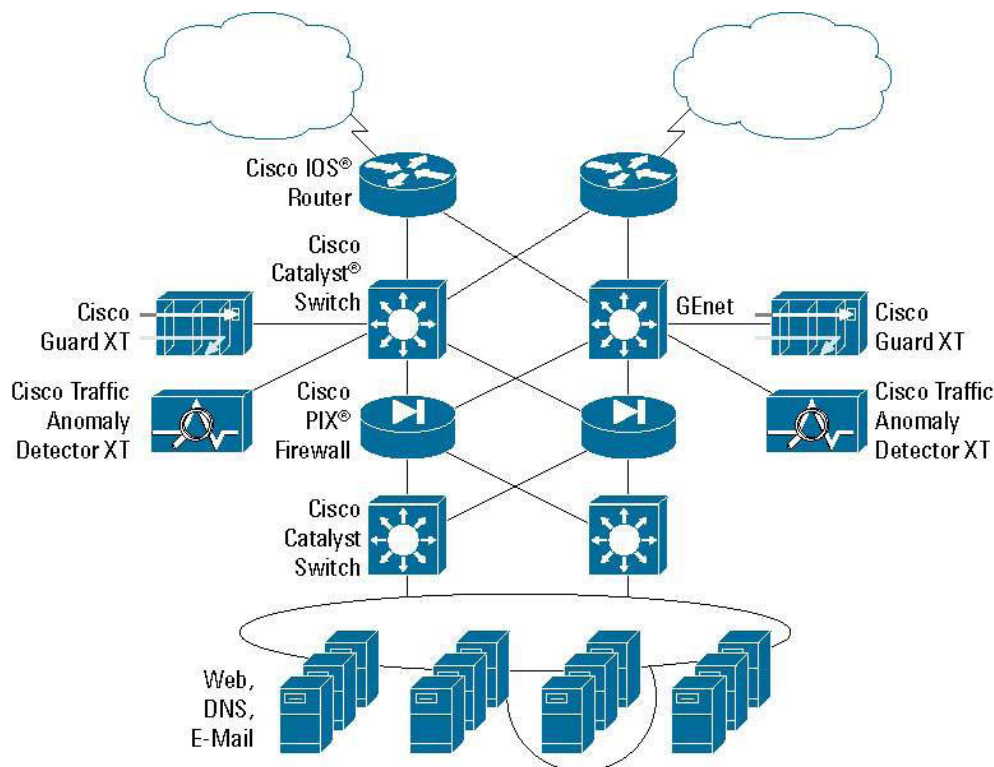
サイバー攻撃はますます増加しており、オンライン ビジネスが直面する脅威の中でも、とりわけ DDoS 攻撃が急速な増加を示しています。こうした攻撃は、単に世間の注目を集めることを目的とした破壊行為から、特定の標的の業務を混乱させるために計画された集中攻撃まで、とどまることなく悪質化しており、多くのビジネスを崩壊寸前に追い込んでいます。

攻撃の手法も巧妙になっています。攻撃者は、適正な要求であるかのように偽装したり、送信元 ID を盗用したり、脆弱化させた「ゾンビ」ホストを何台も使用してインターネット データ センターや既存の防御システムに大量のトラフィックを処理させたりして、不正なトラフィック フローの識別とブロックを事実上不可能にします。

Cisco Traffic Anomaly Detector XT と Cisco Guard XT を組み合わせれば、企業、ホスティングセンター、政府機関、教育・研究機関、およびサービス プロバイダー環境を DDoS 攻撃から保護する、完璧な検出および軽減対策ソリューションを実現できます。Traffic Anomaly Detector XT は、既知の「正常な」動作と異なる振る舞いを検出することによって攻撃されている可能性を検知すると、攻撃対象のデバイスへ向かうトラフィックのみをルート変更し、検査するように Guard XT に警告します。他のトラフィックは通常どおりに伝送されるので、業務全体への影響は抑えられ、1 台の Guard XT で多数のデバイスやゾーンを保護できます。

ルート変更されたトラフィックは、Cisco Guard XT を経由します。Cisco Guard XT は、サービスプロバイダー、企業、官庁・教育・研究機関ネットワークの入口となるアクセス ポイントから ISP のバックボーンとのピアリング ポイントに至るまで、ネットワーク内の任意の場所に設置できますが、通常はクリティカル パスから離して配置されます。このルート変更されたトラフィックに対して詳細な検査が行われ、「不正な」フローと適正なトランザクションとが識別され、分離されます。攻撃パケットは識別され、除去されますが、適正なトラフィックは元の宛先へと転送されるので、正しいユーザとトランザクションは常にネットワークを通過でき、最大限のアベイラビリティが保証されます。

図 1



## 主な機能と利点

### 識別と学習

Cisco Traffic Anomaly Detector XT は、クリティカル パスから離して設置され、ギガビット ライン レートのトラフィック フローをミラーリングしてモニタすることによって、貴重なスイッチやルータのリソースを消費することなく、保護対象となる各デバイスについて「正常な」動作の詳細なプロファイルを作成します。

動作ベースの高度な異常検出テクノロジーを利用する Cisco Traffic Anomaly Detector XT は、グローバル レベルおよび個々のセッション レベルの両方で、プロファイルとの比較によって異常動作を検出するという方法で、既知の攻撃だけでなく未知の (Day Zero) 攻撃も含めてあらゆるタイプの攻撃を極めて正確に識別できます。接続ごとの精細な状態分析をすべてのパケットについて実行することにより、巧妙な低レートのサーバ リソース枯渇攻撃から、分散した数万ものゾンビによって仕掛けられる大規模な攻撃まで、最も捕捉しにくい高度な攻撃を高速かつ包括的に検出して識別できます。

Traffic Anomaly Detector XT には、動作識別エンジンも装備されているため、プロファイルを継続的に更新する必要はなく、スタティックなシグニチャ ベースの検出方式で問題になる多数の警告や誤検出も少なくなります。さらに、Cisco Traffic Anomaly Detector XT には、そのまますぐに使用できる設定済みのデフォルト プロファイルが付属しています。自動学習機能を使用すれば、推奨設定が作成されるので、オペレータはチューニングの参考にすることができます。

さらに、セッション状態コンテキストによって適正なセッション トラフィックが識別され、セッションを悪用した攻撃を特定できるので、不正な動作に対する一層の保護を提供します。

### ハイパフォーマンス

高いパフォーマンスを持つ Cisco Traffic Anomaly Detector XT は、ギガビット ライン レートのフローをモニタでき、同じ攻撃であればデバイスあたり 10 万を超える送信元を十分に識別できるので、大規模で大容量の環境を分散型の攻撃から保護できます。

さらに、ミラーリングされたトラフィックに対するマルチステージ分析によって、最も捕捉しにくい低レートの攻撃でも迅速に識別できます。Cisco Traffic Anomaly Detector XT は、データ センターのなかで保護対象となるリソースに近いダウンストリーム側に配置すれば、最大限の保護を提供します。また、検出範囲を広げるために、Cisco Guard XT 付近のアップストリーム側に配置することも可能です。

### レポートと管理

Cisco Traffic Anomaly Detector XT では、Web ベースの GUI (グラフィカル ユーザ インターフェイス) \*を使用してわかりやすく情報を表示できるので、設定、運用、および攻撃の識別と分析が簡略化されます。

複数レベルにわたるリアルタイムの履歴レポート機能によって、ネットワーク オペレータ、セキュリティ管理者、およびクライアントは、攻撃の検出、ポリシーの設定、および攻撃の軽減対策に役立つ詳細な情報を得られます。また、レポートの統計情報はテキスト ファイルにエクスポートして、バックエンドでカスタマイズしたり、あとで検討したりするために利用できます。

また、Cisco Traffic Anomaly Detector XT では、攻撃への対応をすみやかに開始できるように、ネットワーク オペレータや Cisco Guard XT に対して事前警告を発するように設定できます。Cisco Guard XT に警告を送信することで、自動抑制サービスによる迅速な阻止も可能です。さら

に、SNMP(簡易ネットワーク管理プロトコル)の MIB(管理情報ベース)に準拠しているので、デバイス、保護ゾーン、および攻撃のすべてのレベルの統計情報を、標準ベースの管理システムで利用できます。

\* 英語 GUI のみの提供となります。

## まとめ

サービス プロバイダー、ホスティング センター、企業、政府機関、教育・研究機関向けに設計された Cisco Traffic Anomaly Detector XT と Cisco Guard XT DDoS 軽減対策アプライアンスを組み合わせれば、最も悪質な攻撃に直面しても業務の継続性を保護できるだけのセキュリティ ソリューションを実現できます。これにより、貴重な事業資産に強固なアベイラビリティと保護を保証できるため、ユーザは競争上、大幅な優位性を得られます。

## 製品仕様

表 1 製品仕様

メモリ	2 GB DDRAM
ハードドライブ	80 GB
インターフェイス	ギガビット イーサネット × 2 100BASE-T × 2(管理用)
電源装置	デュアル 110 ~ 220 V、350 W
重量	28.2 kg/62 ポンド
高さ	8.53 cm/3.36 インチ
幅	44.5 cm/17.5 インチ
奥行	69.9 cm/27.5 インチ
動作温度	10 ~ 35°C(50.0 ~ 95.0°F)
保管温度	10 ~ 43°C(50.0 ~ 109.4°F)
湿度	動作時: 8 ~ 80% 保管時: 8 ~ 80%
ラックマウント	可能
管理	セキュア Web ベース GUI CLI: コンソール、Telnet、SSH Cisco(Riverhead) SNMP MIB および MIB II TACACS+ Syslog
認定規格	UL 認定 CE FCC ルール Part 15 準拠
攻撃に対する保護	<ul style="list-style-type: none"> <li>● スプーフィングおよび非スプーフィング攻撃 <ul style="list-style-type: none"> <li>◦ TCP(SYN、SYN-ACK、ACK、FIN、フラグメント)</li> <li>◦ UDP(ランダム ポート フラッド、フラグメント)</li> <li>◦ ICMP(到達不可能、エコー、フラグメント)</li> <li>◦ DNS</li> </ul> </li> <li>● クライアント攻撃 <ul style="list-style-type: none"> <li>◦ 非アクティブおよびすべての接続</li> <li>◦ HTTP Get フラッド</li> </ul> </li> <li>● BGP 攻撃</li> </ul>

## 発注情報

表 2 発注情報

製品名	製品番号	SMARTnet 番号
Cisco Traffic Anomaly Detector XT 5600 (LC コネクタ付き 1000BASE-SX マルチモード光ファイバ ポート、デュアル AC 電源、RAID を装備)	ADX-5600-MMF-A-K9	CON-SNT-ADX5600M
Cisco Traffic Anomaly Detector XT アプライアンス 5.0	SC-ADX-5.0-K9	

シスコ製品の購入方法の詳細は、「[購入案内](#)」を参照してください。

## テクニカル サポート サービス

お客様が大規模な組織であるか、営利企業であるか、またはサービス プロバイダーであるかにかかわらず、シスコは、お客様のネットワーク投資の収益を最大限に高めることをお約束します。シスコでは、各種のテクニカル サポート サービスを提供しており、ご使用のシスコ製品で動作を効率化し、高いアベイラビリティを維持し、最新のシステム ソフトウェアを活用できるように支援しています。

シスコのテクニカル サポート サービスでは、以下のような機能を提供して、ネットワーク投資の保護と、業務上重要なアプリケーションを実行しているシステムのダウンタイムの最小化を実現しています。

- シスコのネットワーク専門家がオンラインと電話でサポート
- 障害または問題が発生した場合の単なる対応策ではなく、ネットワーク運用には不可欠の一部としてソフトウェアのアップデートとアップグレードを常時提供することにより、予防的なサポート環境を実現
- シスコの技術的知識とリソースをお客様の要求に応じて提供
- お客様の技術スタッフのリソースを育成することにより、生産性を向上
- リモート テクニカル サポートに加えてオンサイトのハードウェア交換サービスを提供
- シスコのテクニカル サポート サービスには、次のものがあります。
  - Cisco SMARTnet<sup>®</sup> サポート
  - Cisco SMARTnet オンサイト サポート
- シスコ ソフトウェア アプリケーション サービス (Software Application Support および Software Application Support plus Upgrades)

詳細は、次のサイトをご覧ください。<http://www.cisco.com/jp/services/>

©2007 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、およびCisco Systemsロゴは、Cisco Systems, Inc.またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用はCiscoと他社との間のパートナーシップ関係を意味するものではありません。(0701R)

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ株式会社

〒107-0052 東京都港区赤坂2-14-27 国際新赤坂ビル東館

<http://www.cisco.com/jp>

お問い合わせ先(シスコ コンタクトセンター)

<http://www.cisco.com/jp/go/contactcenter>

0120-092-255 (通話料無料)

電話受付時間：平日 10:00～12:00、13:00～17:00

お問い合わせ先