ManageEngine
NetFlow Analyzer

ネットワーク VS アプリケーション

アプリケーションから見る!
トラフィックの監視と制御

ゾーホージャパン株式会社

目次

アプリケーションのパフォーマンスを向上させるために、アプリケーションまたはそのホストサーバーを最適化する担当者様は少なくないでしょう。ネットワークは、アプリケーションの提供速度に大きく起因するため、アプリケーション提供に大きな役割を果たします。基盤となるネットワークに問題がある場合やサーバー設定の最適さ、、またはアプリケーションの最適さによって、アプリケーションの配信速度は影響されます。

従来のネットワークとアプリの監視手法からの脱却

アプリケーションを最適化するのではなく、ネットワークの観点からアプリケーションのパフォーマンスと配信に関する問題を分析します。ネットワーク管理者は、アプリケーション配信の最適化のため LAN と WAN のトラフィックを可視性し、問題の要因を見つけ改善する必要があります。

不適切な帯域幅管理

アプリケーションやユーザー毎の帯域使用状況の監視と可視化ができないと、ネットワーク管理者は帯域幅が十分であるかどうか、または追加の帯域を契約する必要があるかどうか判断できません。また、追加の帯域を契約したとしても長期的な問題解決にはなりません。最初に帯域を可視化し、ビジネスに必要なアプリケーションとそうではないアプリケーションのどちらがより多くの帯域幅を消費しているかを特定し、それに応じて帯域幅を割り当てる必要があります。

ビジネスクリティカルなアプリケーションの優先順位

ビジネスクリティカルなアプリケーションを優先できている企業は多くありません。その結果、ネットワークはベストエフォート型ですべてのアプリケーションを配信しようとします。このため、ネットワーク輻輳時にすべてのトラフィックがブロックされる可能

性が高くなります。このような問題を回避するには、QoS ポリシーを定義してトラフィックに優先順位を付ける必要があります。

動作が遅いホップ

パケットは複数のホップを通過して利用者に到達します。いずれかのホップに長い待ち時間がかかると、アプリケーションの応答時間が長くなり、利用者から不満があがります。このようなクリティカルパスを監視し、待ち時間/パケットロス/ジッタなどを見つける必要があります。

ネットワークを脅かす攻撃や悪意のあるトラフィック

ハッカーはネットワークにジャンクトラフィックを送り、ネットワークとアプリケーションのパフォーマンスを低下させようとします。悪意のあるトラフィックが発生している場合、リアルタイムで識別してブロックできる可能性があるので、ネットワークにアクセスしているトラフィックが正常であるかどうかの監視を実施する必要があります。

アプリケーションから見るトラフィック分析

基本的なネットワーク監視やトラフィック分析は行っているが、それをアプリケーション配信と関連させている企業は多くありません。ネットワークとアプリケーションは異なるレイヤーですが、アプリケーション配信がネットワークに依存していることを再認識する必要があります。ネットワークのパフォーマンス低下やジャンクトラフィックの大量発生は、アプリケーション配信に影響を与えます。そのため、アプリケーションの視点からネットワークトラフィックを分析および制御するのに役立つネットワークトラフィック分析ソフトウェアが必要です。このようなソフトウェアは管理者の課題解決におおいに役立つものと考えられます：

1. より多くの帯域幅を使用しているアプリケーションを特定
2. ビジネスに必要なアプリケーションに優先順位を付ける
3. WAN 全体に広がる帯域のボトルネックを調査
4. 根本原因を見つけるためのフォレンジック分析
5,攻撃や侵入を防ぐ

より多くの帯域幅を使用しているアプリケーションを特定

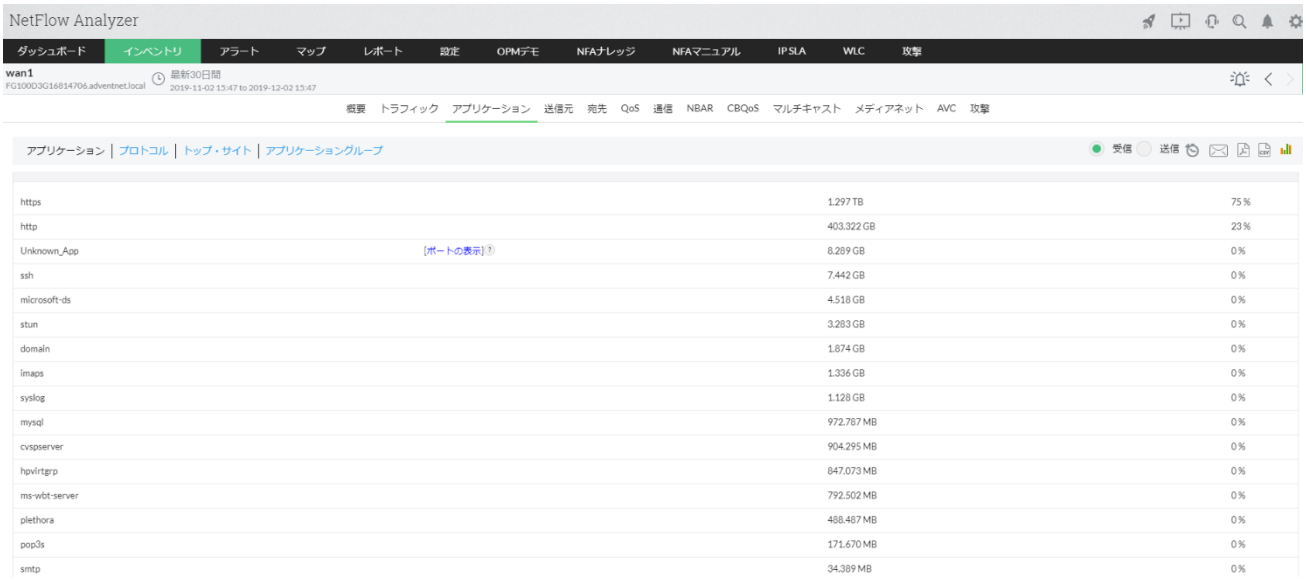
SNMP によるトラフィック監視では、インターフェース/ポートを流れるトラフィックの総量を監視することができます。アプリケーションの一覧とその帯域消費率を特定するには、より詳細な監視が必要です。

■アプリケーションから見る！トラフィックの監視と制御

ルーターやスイッチで機能する NetFlow や sFlow などのプロトコルにより生成されるデータを「フローデータ」と呼びます。
フローデータにはトラフィックに関する情報だけでなく、アプリケーションの一覧や各アプリケーションの帯域消費率に関する情報も含みます。
このフローデータを活用するソフトウェアを「フローコレクター」と呼びますが、ManageEngine では「NetFlow　Analyzer」というフローコレクターを提供しています。

NetFlow Analyzer は、NetFlow や sFlow 等によって生成されるフローデータを受信し見やすい形に整えることで、手軽な帯域分析を支援します。Cisco NBAR などの技術も活用し、ネットワーク経由でアクセスするアプリケーションを識別し、アプリケーションとそれらが消費する帯域幅に関する詳細な情報を提供します。これにより、ビジネスクリティカルなアプリケーションと非ビジネスクリティカルなアプリケーションが帯域の何パーセントを使用しているかを正確に把握できます。また、最も帯域を消費しているデバイスやユーザーを見つけるのにも役立ちます。

アプリケーションから見る！トラフィックの監視と制御



ビジネスに必要なアプリケーションに優先順位を付ける

QoS ポリシーは、アプリケーションがどのように帯域幅（高優先度、ベストエフォート、スカベンジャークラス）を優先するかを定義します。組織で使用されているビジネスクリティカルなアプリケーション、または利用者に提供されるアプリケーションやリアルタイム性を求められる音声/ビデオ通信のほとんどは、「最優先」に該当します。それほど重要ではないその他のアプリケーションは、ベストエフォートとして定義されます。例えば、Facebook、Twitter などのソーシャルアプリケーションはスカベンジャークラス（くず拾い）に定義されるべきです。優先順位が設定されていない場合、ネットワークはすべてのアプリケーションを配信するためにベストエフォート型のアプローチを取ります。その結果、ビジネスクリティカルなアプリケーションと非ビジネスクリティカルなアプリケーションの両方が同じ優先順位で提供されます。

アプリケーションから見る！トラフィックの監視と制御

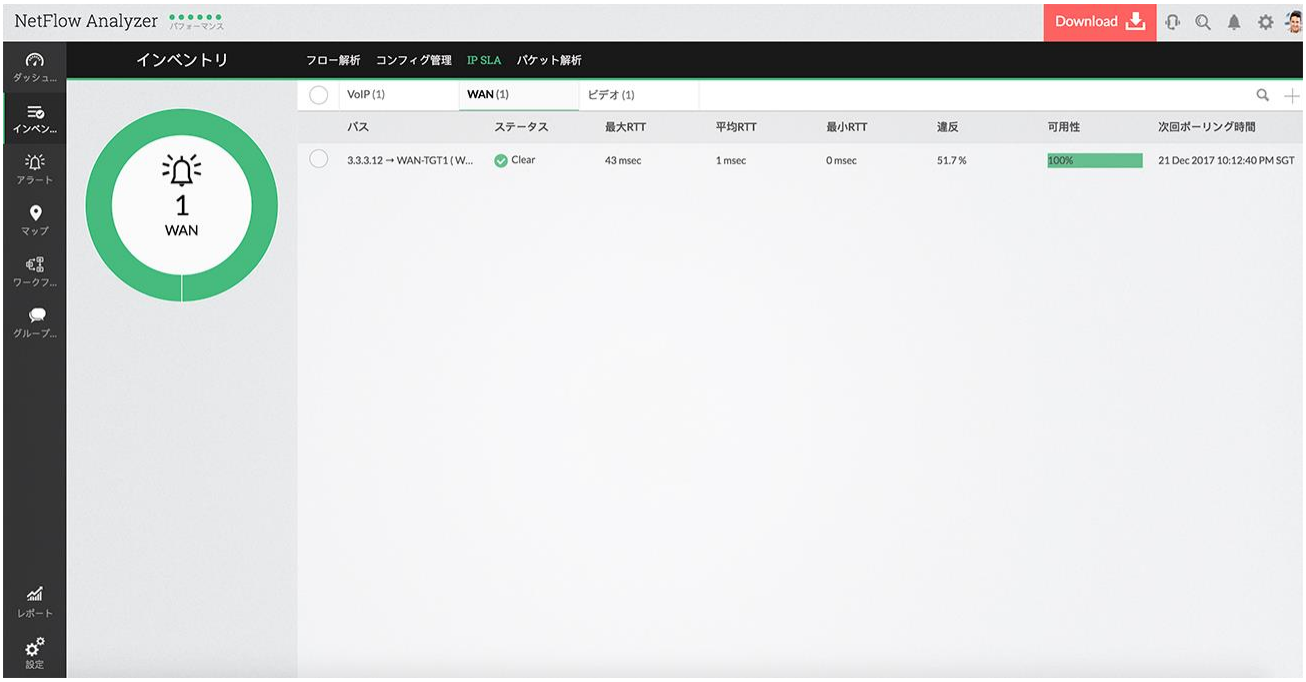
ここで QoS ポリシーが役立ちます。ビジネスクリティカルなアプリケーションの帯域利用を優先し、帯域を効率的に利用します。NetFlow Analyzer を使用すると、QoS ポリシーの監視および検証ができ、Qos ポリシー設定の前後を比較するのにも役立ちます。

WAN **全体の帯域幅のボトルネックを検出**

アプリケーションの利用者とその管理場所は遠く離れていることが多く、利用時に発生するパケットは複数のホップを通過していきます。そのため、利用者がよりスムーズにアプリケーション利用できるように、各ホップでの待ち時間は最小限に抑える必要があります。ただし、各ホップは複数のトラフィック処理やパケット転送、ルーティングなどに時間がかかることがあるため、常に可能とは限りません。このような状態は遅延を増大させ、アプリケーションの配信に影響を及ぼします。

■アプリケーションから見る！トラフィックの監視と制御

NetFlow Analyzer では、Cisco IP SLA の監視により、テストパケットをシミュレートして、WAN リンクの待ち時間、ジッタ、およびパケットロスレベルを定期観測します。待ち時間、ジッタ、またはパケットロスを事前把握することができ、パフォーマンスデータの分析や問題が大きくなる前に対策を施すことができます。



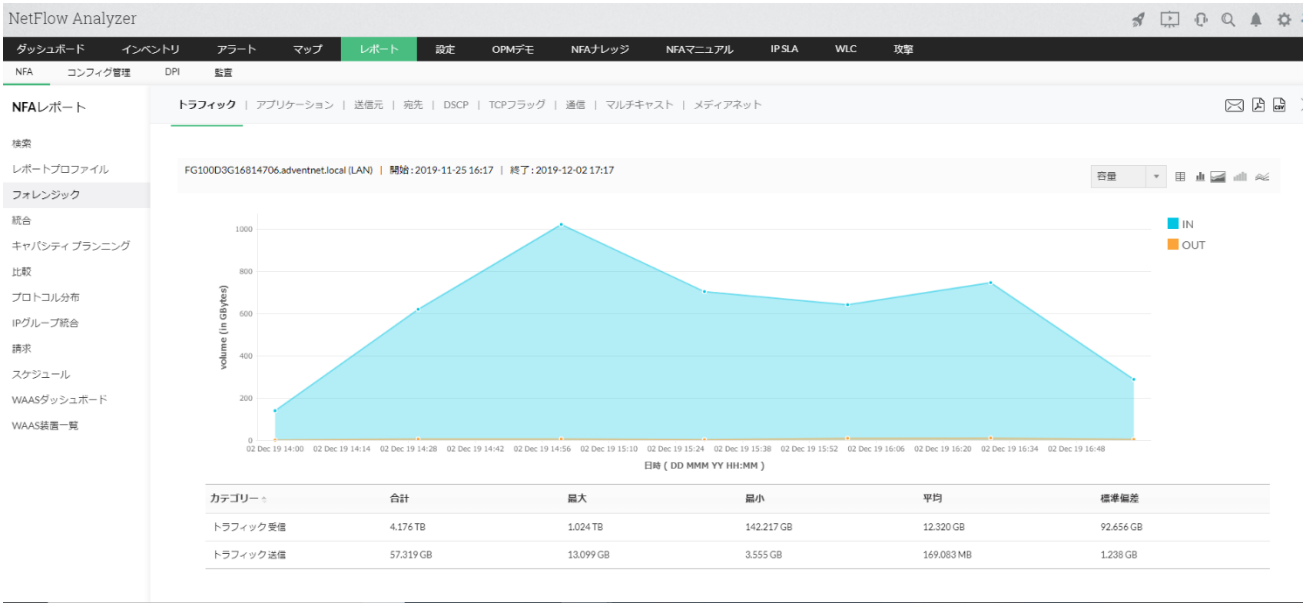
根本原因を見つけるためのフォレンジック分析

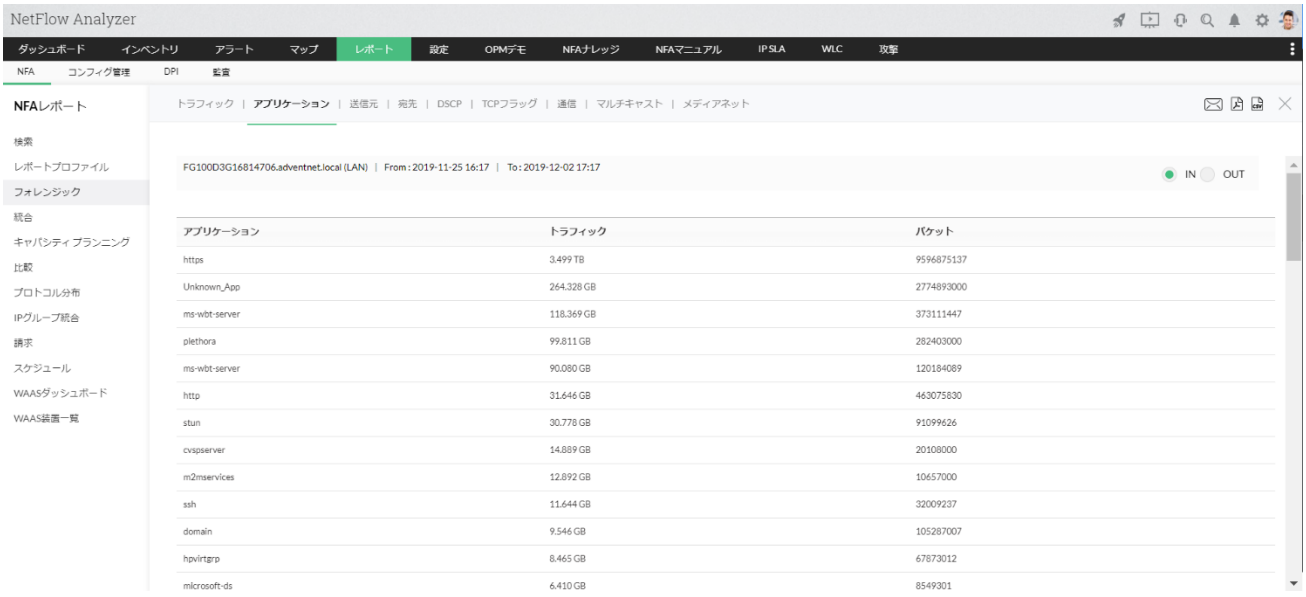
問題を迅速に解決することよりも重要なことは、根本的な原因を突き止め再発を防ぐことです。根本原因を見つけるための詳細な分析には膨大な量のデータを分析し、誰が、いつ、何を、そしてなぜ行っていたのかを把握する必要があります。これには広範囲に渡るレポートの生成と入念な分析が必要です。

アプリケーションから見る！トラフィックの監視と制御

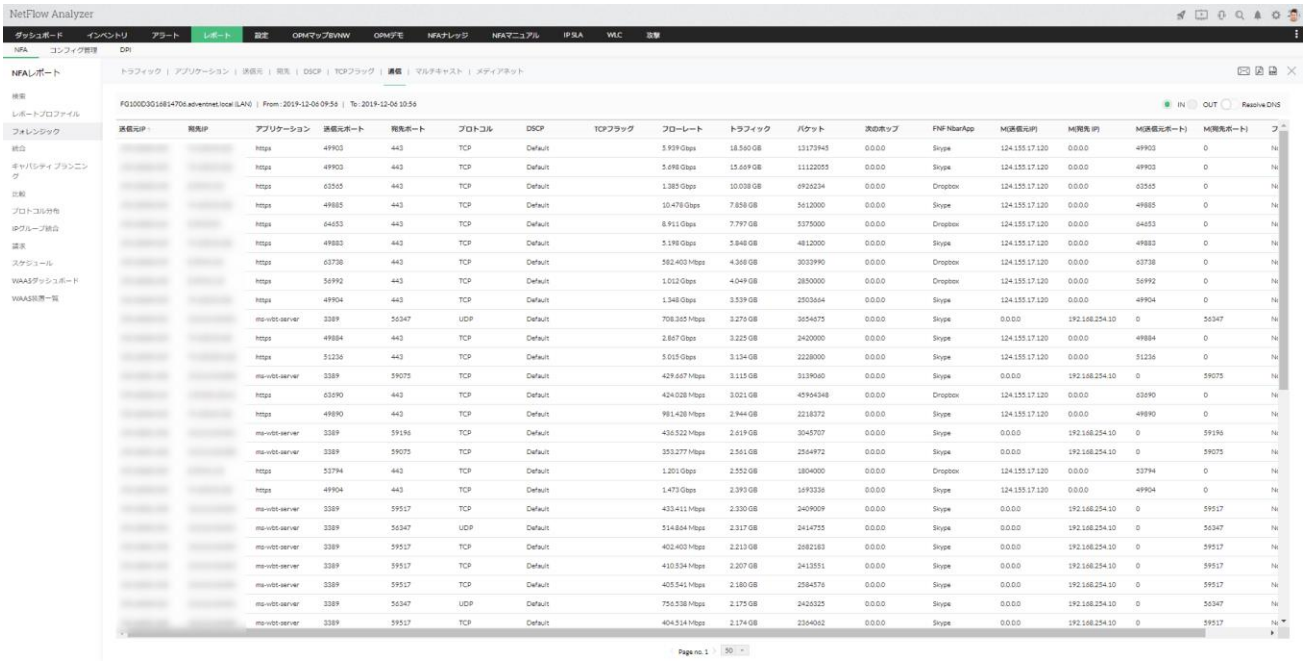
NetFlow Analyzer は、フォレンジックレポートにより上記のような分析を支援します。この機能では、過去に遡って必要なデータを収集し、レポートを生成します。

NetFlow Analyzer は、トラフィック、アプリケーション、送信元/宛先 IP アドレス、DSCP など、さまざまな切り口でのデータ分析に役立ちます。





アプリケーションから見る！トラフィックの監視と制御



攻撃や侵入を防ぐ

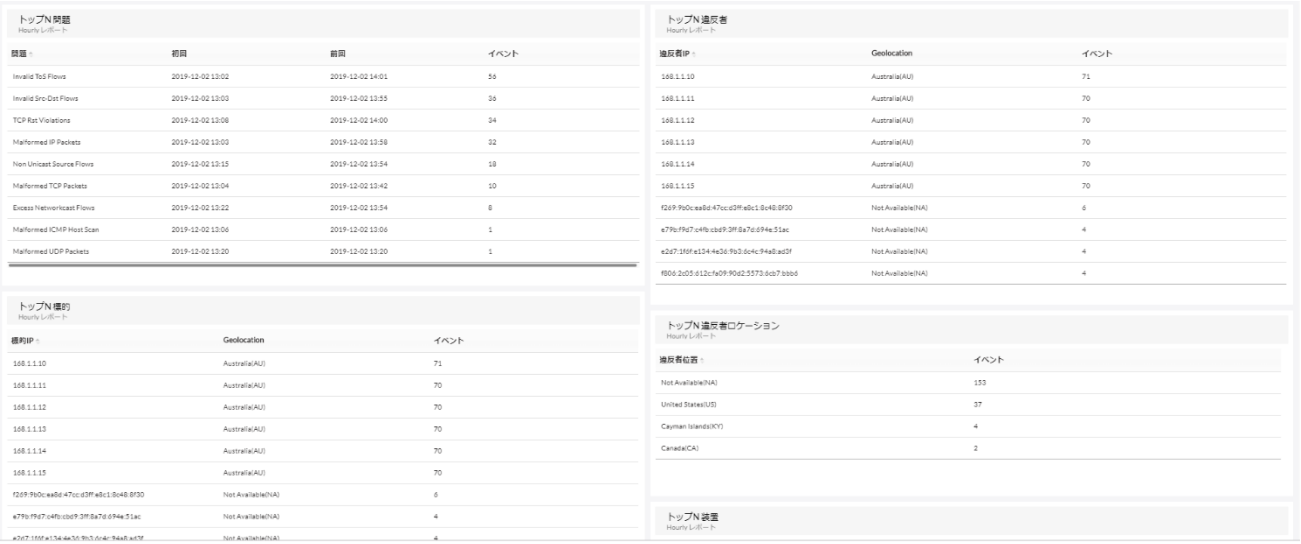
ファイアウォールや侵入検知システム（IDS）の導入にもかかわらず、ハッカーの標的になっている企業は少なくありません。どちらのシステムもパケットのヘッダーを読み取りシグネチャ・マッチングを実行しますが、DDoS やゼロデイアタックなどの高度なセキュリティ攻撃には対応していません。

このような背景により、高度な攻撃からネットワークやデータセンターを保護するのに役立つ高度なセキュリティ分析と保護を必要とする企業が増えてきています。

NetFlow Analyzer では、フローデータを分析してネットワークを攻撃する悪意のあるトラフィックを検出する、フローベースのネットワーク動作異常検出（NBAD）機能を提供しています。悪意のあるトラフィックにルールとパターンを適用して、それらが

■アプリケーションから見る！トラフィックの監視と制御

侵入か攻撃かを識別します。攻撃/セキュリティの脅威を識別し、それらを DDoS、Bad SrcDst、Suspect Flow、Scan/Probe などに分類します。



NetFlow Analyzer によるアプリケーショントラフィックの制御

NetFlow Analyzer は企業の LAN と WAN のトラフィックを可視化し、アプリケーションとそれらの帯域消費に関する情報を提供します。この情報を基に、QoS ポリシーを監視し、ミッションクリティカルなアプリケーションを高い優先度で処理するために必要な変更を加えることができます。LAN や WAN の問題や攻撃はプロアクティブに識別され、利用者が影響を受ける前に修正されます。ネットワークに NetFlow Analyzer を導入し、シームレスなアプリケーション配信のためにネットワークパフォーマンスを向上させましょう。

ManageEngine NetFlow Analyzer について

NetFlow や sFlow などのプロトコルを活用し、ネットワーク帯域の「可視化」を支援するフローコレクター製品です。

NetFlow Analyzer の特徴は以下の通りです。

特徴 1：コストを抑制

アプライアンス製品よりも導入しやすい年間 17.8 万円からの低価格帯

特徴 2：必要充分な機能

ネットワークトラフィックの監視・可視化に必要充分な機能をデフォルトで実装

特徴 3：直感的な管理画面

クリックによるドリルダウンで、障害の原因調査も楽々。直感的な操作でトラフィックの調査も迅速化

お問い合わせ先

ゾーホージャパン株式会社

〒 220-0012

神奈川県横浜市西区みなとみらい 3 丁目 6 番 1 号 みなとみらいセンタービル 13 階

Web : https://www.manageengine.jp/

E-mail : jp-mesales@zohocorp.com（弊社営業宛）

2019 年 12 月発行　ZJMR20191225130

※当 eBook は Zoho corporation で発行されたものをゾーホージャパンが加筆・修正したものです