NetVizura
製品ガイド

Rev 1.0
2019年 12月02日

目次

はじめに

NetVizuraは、複数モジュールが組み合わさった製品です。現在２種類の有償モジュールから構成されています。各モジュール、インストーラーは共通でWEB GUIも共通となり、横断的な利用が可能となっております。

- NetFlow Analyzer(NFA) ・・・社内に配置するだけで、直ぐに社内ネットワークの「見える化」を実現するフローコレクターです。

- EventLog Analyzer(ELA) ・・・ネットワーク機器、サーバーからのログ及びSNMPトラップを収集するSyslogサーバーです。NFAと組み合わせることで、xFlow, Syslog, SNMP Trapを利用した横断的な問題解析が可能です。

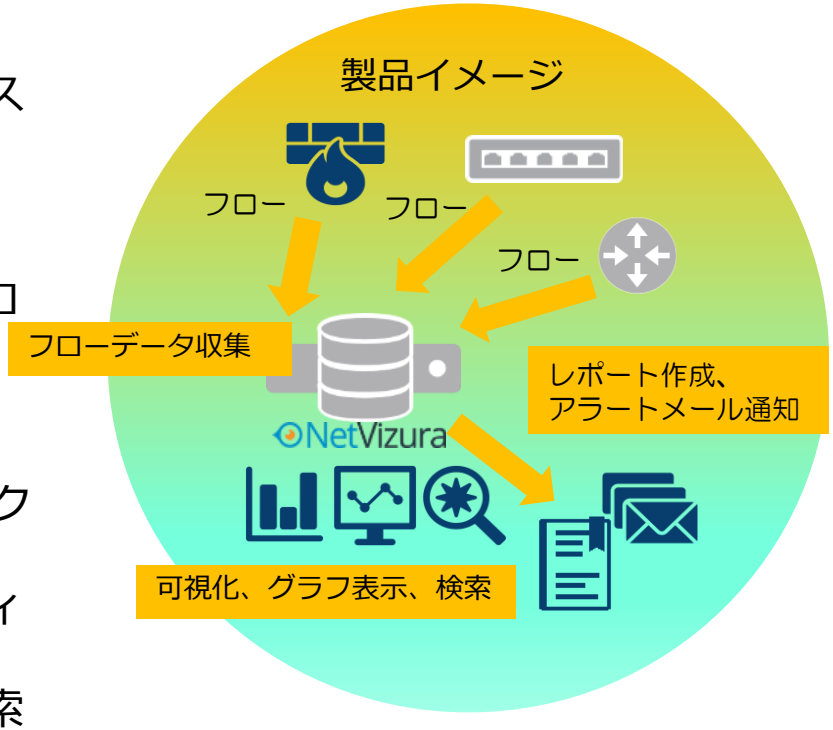
本製品ガイドでは、NFAを説明した後にELAを紹介いたします。ELAは単独販売はしておらず、NFAの購入が前提となっておりますので、ご注意ください。

1.NFAの概要

NetVizura NetFlow Analyzer(以降、NetVizura NFA)は、フローデータの収集・分析が簡単で、ネットワークの異常原因を早期発見出来ます。

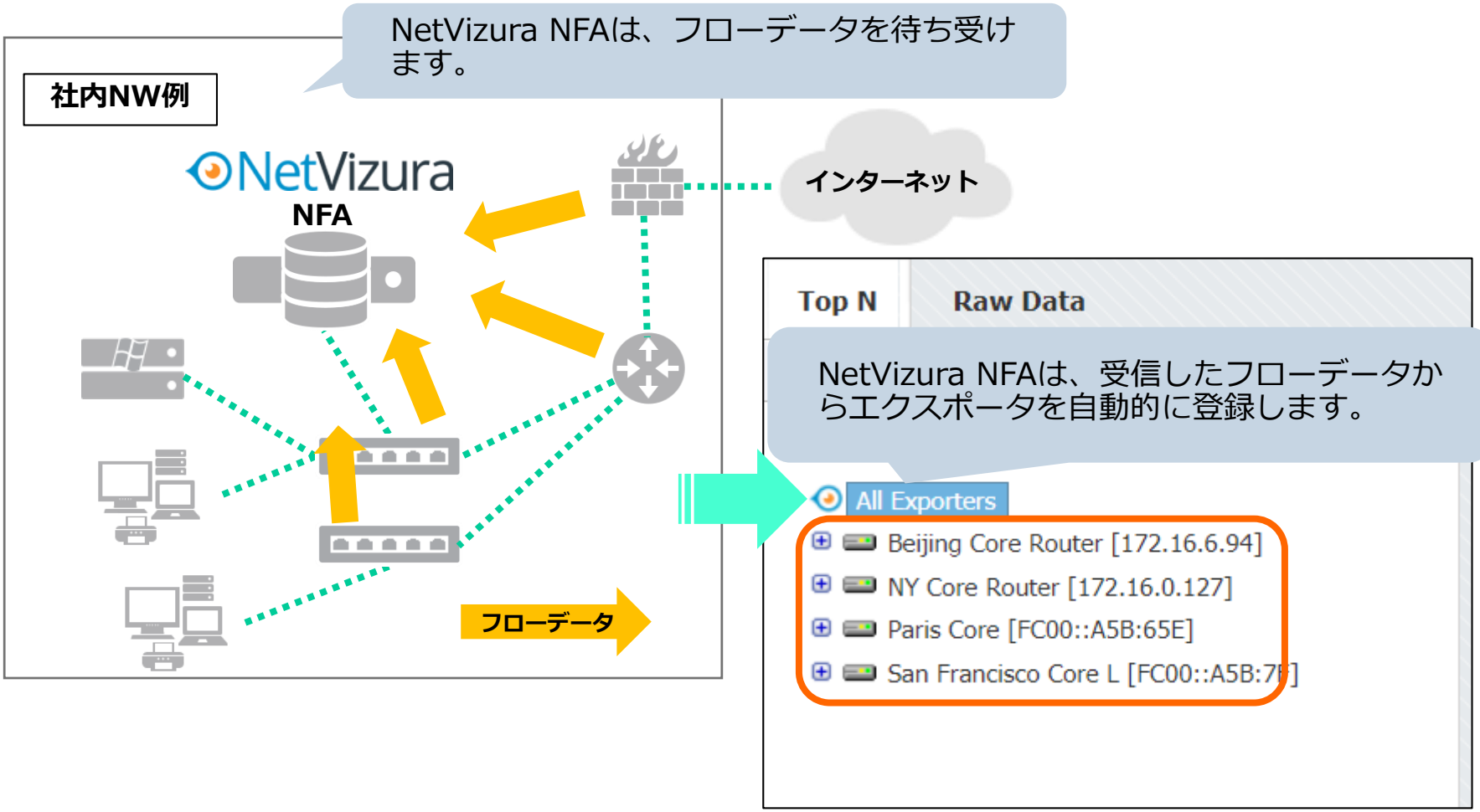
NetVizura NFAのここがポイント！

- 低価格サブスクリプションとアプライアンス製品販売をラインナップ
- 1秒間当たり50,000フローの収集処理能力
- Cisco Netflow v5/v9、IPFIX、NSEL、sFlow v5やCisco Netflow互換の多彩なプロトコルをサポート
- 分かりやすいWEB GUIで5W(どこ、だれ、いつ、何、なぜ)を支援
- Syslogと連携した特定ユーザのトラフィック表示
- サブネットを個別定義したカスタムトラフィックごとのアラーム設定
- フローデータのローデータ表示、データ検索、ソート、CSV出力機能



2.NFAシステム導入イメージ

各NW機器からNetVizura NFA宛てに、フローデータを送信する設定を行ってください。



3.NFA特長 1 – すぐ見える化

NetVizura NFAは、ターゲットNW機器のトラフィック分析を直ぐに開始することができます。

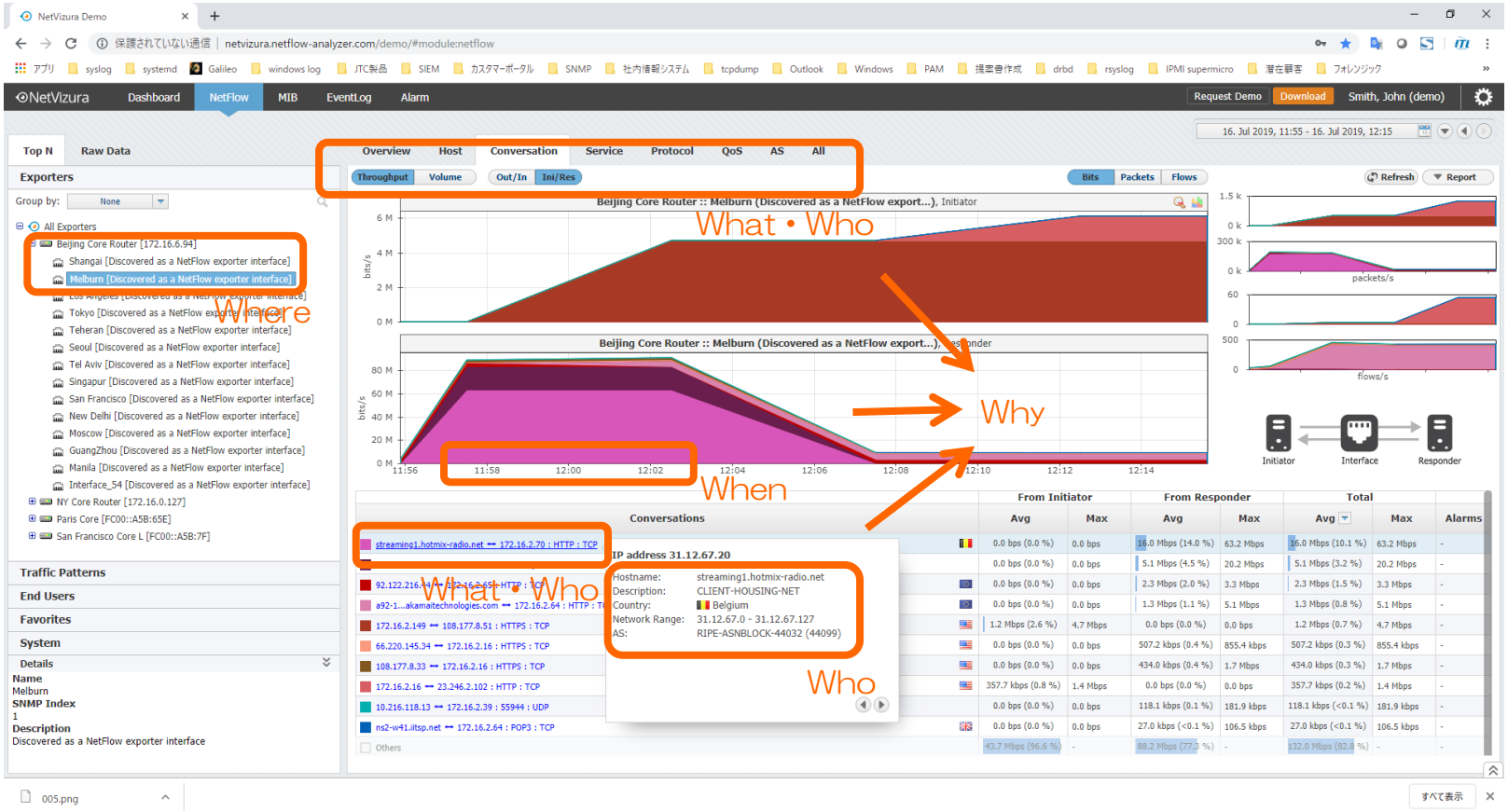
- ✓ 通常、インストールからデータ表示まで 30分程度で完了します。

インストールからトラフィックグラフ表示までの手順：

1. NetVizura NFAをインストールします。
   インターネット環境に繋がったサーバ上で、インストールシェルを実行します。
2. ターゲットNW機器のフロー設定を行います。
   NetVizura NFAにフローデータを送信する設定を行います。トラフィック分析を行いたいターゲットNW機器にログインし、フローエクスポート設定を行います。
3. NetVizura NFAの初期セットアップを行います。
   Web GUIにアクセスし、初期セットアップウィザードの指示に従っていくつかの設定（管理ユーザー、メールサーバー、エクスポータ、サブネットなど）を行います。

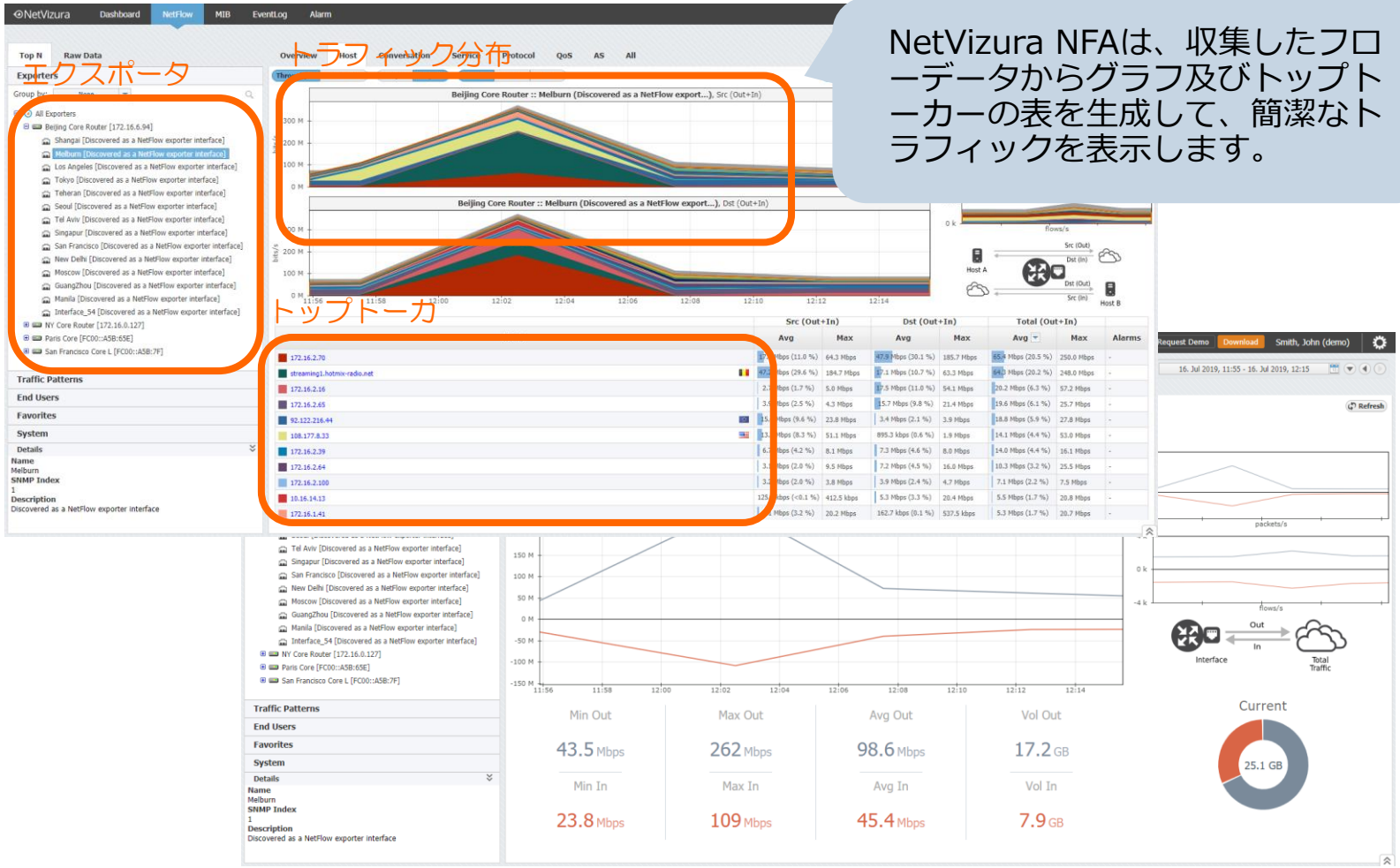
3.NFA特長 2 – 5W追跡をサポート

NetVizura NFAは、標準で出力されるデータ及びフィルター機能を組み合わせることによって、どのホストが？いつ？どこの機器のどのIFで？どのサービスで?なぜそのような通信を？といった5W情報の追跡を強力にサポートします。



3.NFA特長 3 - わかりやすい画面

NetVizura NFAは、シンプルかつ分かりやすくデータを表示します。



3.NFA特長 4 – 様々なフロー形式

NetVizura NFAは、様々なフロー形式を標準サポートします。

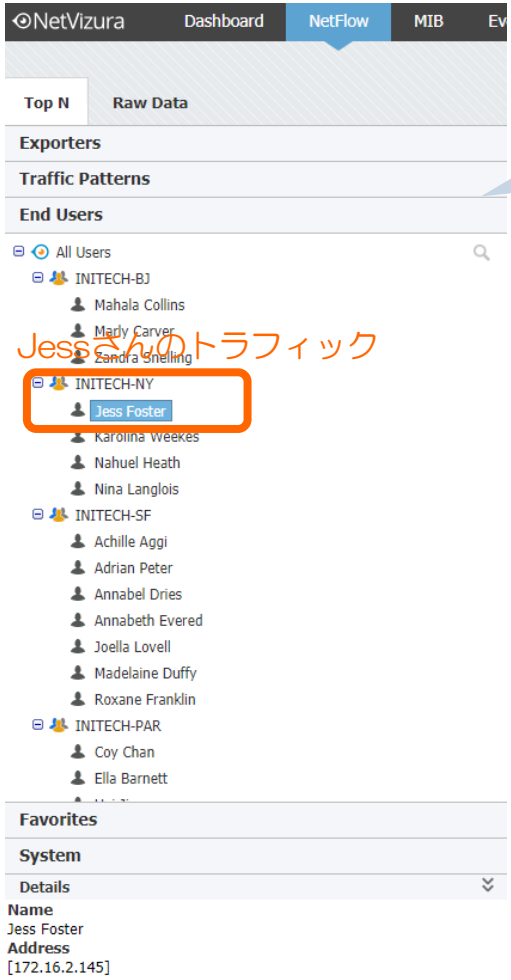
NetVizura NFAサポートプロトコル：

項番	サポートプロトコル
1	Cisco NetFlow version5
2	Cisco NetFlow version9
3	IPFIX
4	NSEL
5	sFlow version 5
6	その他： Cisco NetFlow version5とCisco NetFlow version9に互換性のあるプロトコル

* フローのエクスポータ設定および対象フロープロトコルの形式・バージョンは、各メーカサイトをご参照ください。また、ご購入前に 評価版でお試しいただくか、弊社まで対応状況をお問合せください（お問合せいただく際は、ターゲット装置のファームウェア情報、型番をご提供ください）。

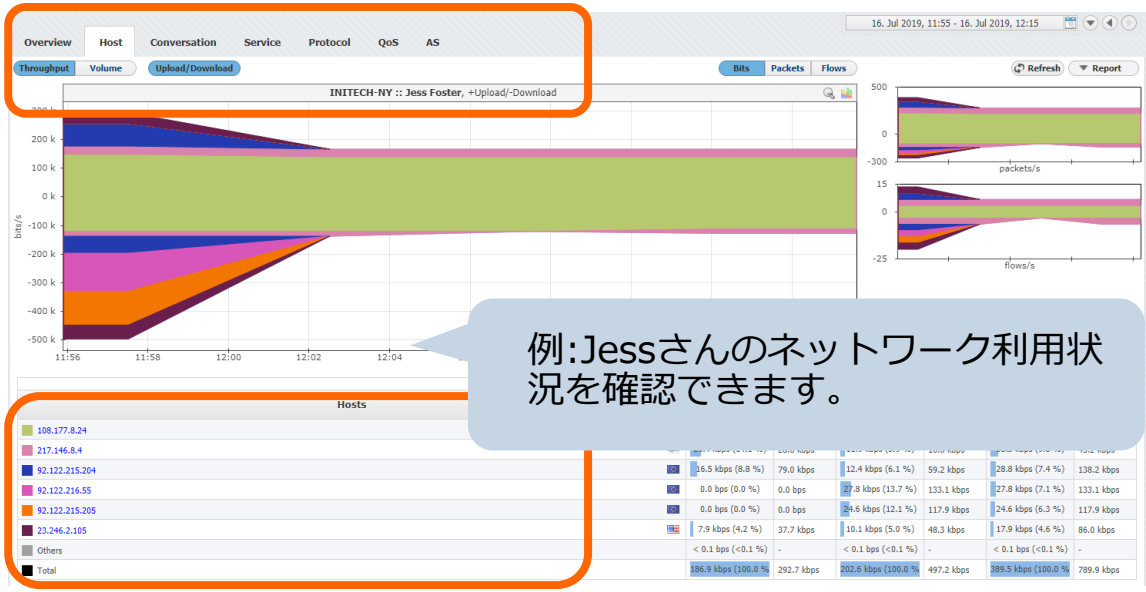
3.NFA特長 5 – エンドユーザ統計

NetVizura NFAは、Active Direcory(AD)のイベントログと連携してエンドユーザごとのトラフィック分析をサポートします。



Jessさんのトラフィック

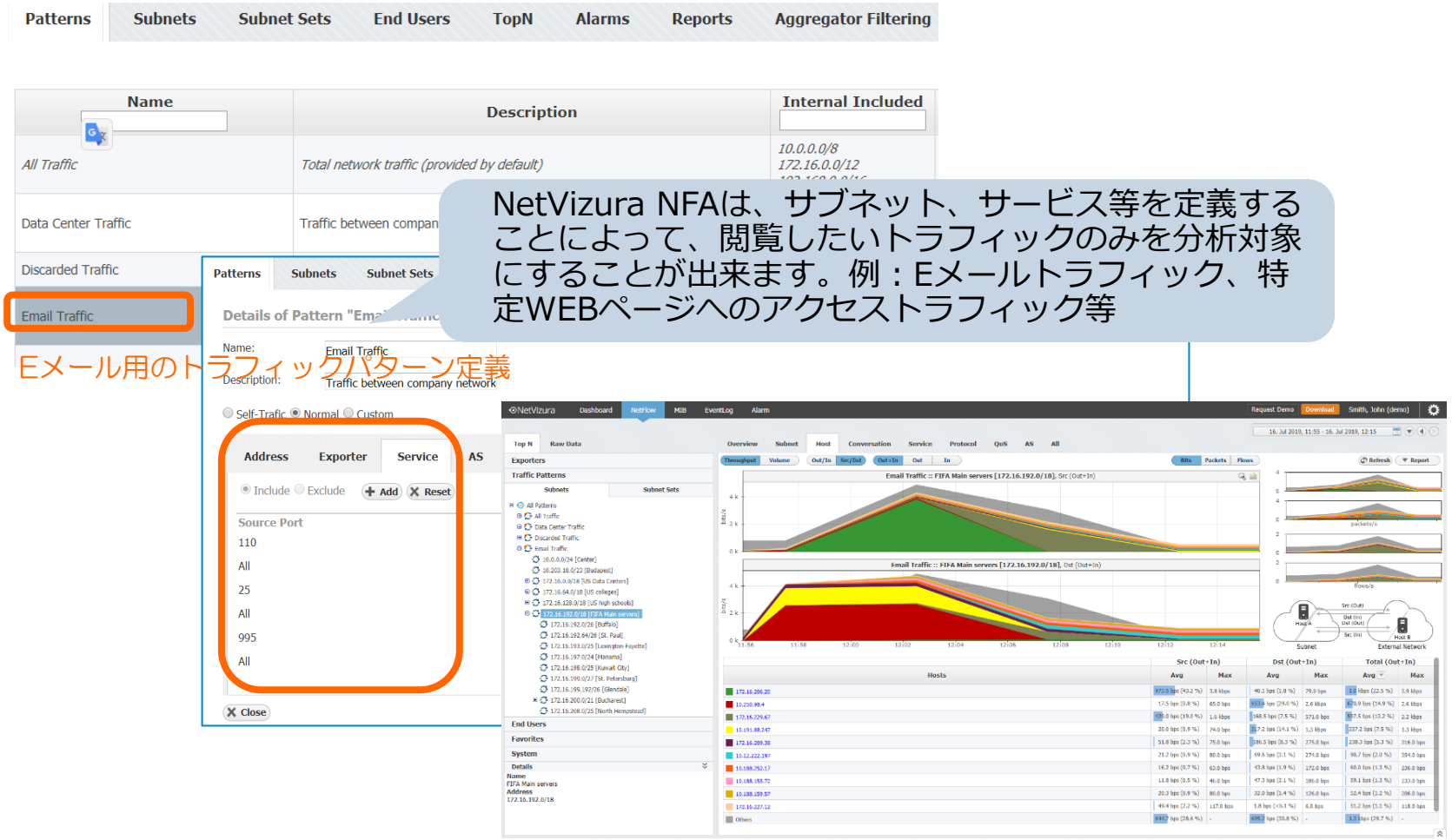
NetVizura NFAとADが連携することで、ドメインユーザごとのトラフィック表示が可能となります。



例:Jessさんのネットワーク利用状況を確認できます。

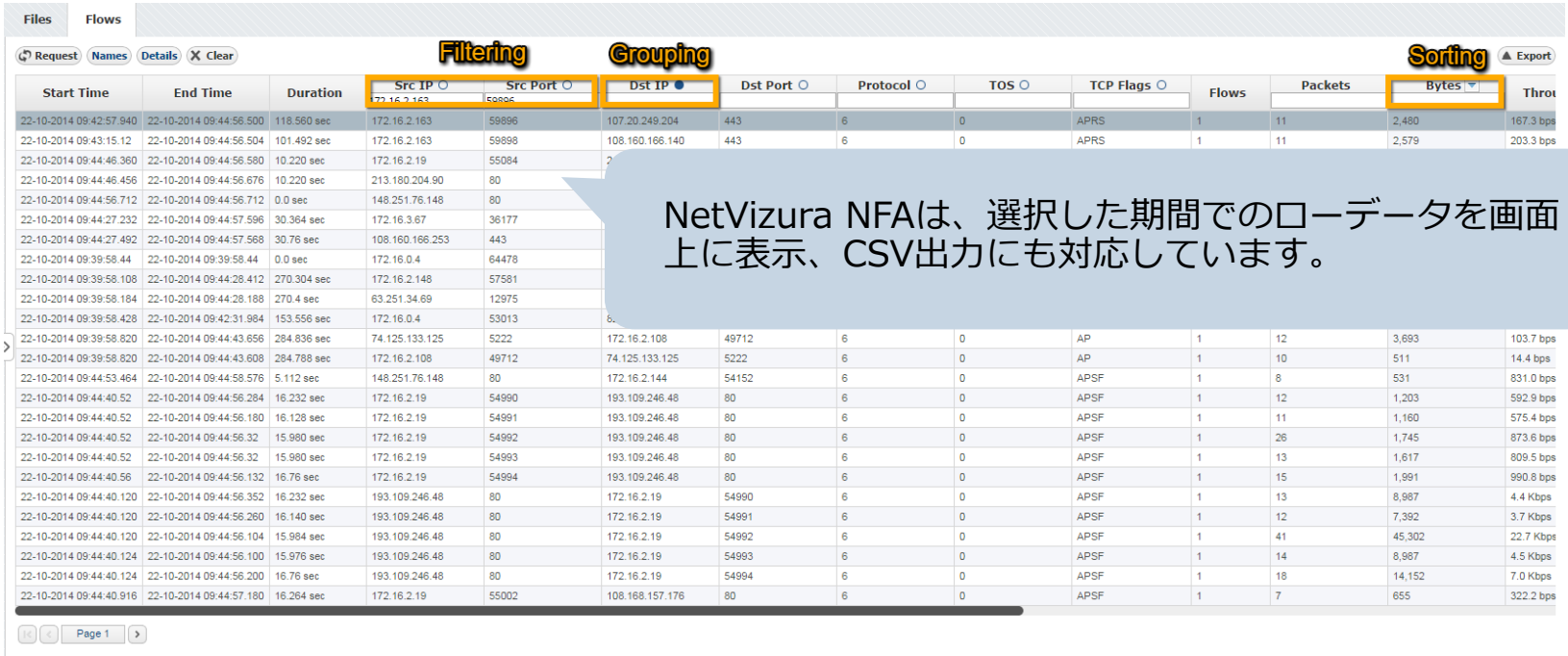
3.NFA特長 6 – カスタムトラフィック

NetVizura NFAは、NW管理者が定義したルールによって監視に必要なトラフィックだけを限定して表示することが出来ます。



3.NFA特長 7 – ローデータ表示

NetVizura NFAは、収集したフローデータのローデータを検索・ソート・CSV出力することが出来ます。ローデータを利用してより詳細なトラフィック分析が可能です。



Start Time	End Time	Duration	Src IP	Src Port	Dst IP	Dst Port	Protocol	TOS	TCP Flags	Flows	Packets	Bytes	Throu
22-10-2014 09:42:57.940	22-10-2014 09:44:56.500	118.560 sec	172.16.2.163	59896	107.20.249.204	443	6	0	APRS	1	11	2,480	167.3 bps
22-10-2014 09:43:15.12	22-10-2014 09:44:56.504	101.492 sec	172.16.2.163	59898	108.160.166.140	443	6	0	APRS	1	11	2,579	203.3 bps
22-10-2014 09:44:46.360	22-10-2014 09:44:56.580	10.220 sec	172.16.2.19	55084	2								
22-10-2014 09:44:46.456	22-10-2014 09:44:56.676	10.220 sec	213.180.204.90	80									
22-10-2014 09:44:56.712	22-10-2014 09:44:56.712	0.0 sec	148.251.76.148	80									
22-10-2014 09:44:27.232	22-10-2014 09:44:57.596	30.364 sec	172.16.3.67	36177									
22-10-2014 09:44:27.492	22-10-2014 09:44:57.568	30.76 sec	108.160.166.253	443									
22-10-2014 09:39:58.44	22-10-2014 09:39:58.44	0.0 sec	172.16.0.4	64478									
22-10-2014 09:39:58.108	22-10-2014 09:44:28.412	270.304 sec	172.16.2.148	57581									
22-10-2014 09:39:58.184	22-10-2014 09:44:28.188	270.4 sec	63.251.34.69	12975									
22-10-2014 09:39:58.428	22-10-2014 09:42:31.984	153.556 sec	172.16.0.4	53013	8								
22-10-2014 09:39:58.820	22-10-2014 09:44:43.656	284.836 sec	74.125.133.125	5222	172.16.2.108	49712	6	0	AP	1	12	3,693	103.7 bps
22-10-2014 09:39:58.820	22-10-2014 09:44:43.608	284.788 sec	172.16.2.108	49712	74.125.133.125	5222	6	0	AP	1	10	511	14.4 bps
22-10-2014 09:44:53.464	22-10-2014 09:44:58.576	5.112 sec	148.251.76.148	80	172.16.2.144	54152	6	0	APSF	1	8	531	831.0 bps
22-10-2014 09:44:40.52	22-10-2014 09:44:56.284	16.232 sec	172.16.2.19	54990	193.109.246.48	80	6	0	APSF	1	12	1,203	592.9 bps
22-10-2014 09:44:40.52	22-10-2014 09:44:56.180	16.128 sec	172.16.2.19	54991	193.109.246.48	80	6	0	APSF	1	11	1,160	575.4 bps
22-10-2014 09:44:40.52	22-10-2014 09:44:56.32	15.980 sec	172.16.2.19	54992	193.109.246.48	80	6	0	APSF	1	26	1,745	873.6 bps
22-10-2014 09:44:40.52	22-10-2014 09:44:56.32	15.980 sec	172.16.2.19	54993	193.109.246.48	80	6	0	APSF	1	13	1,617	809.5 bps
22-10-2014 09:44:40.56	22-10-2014 09:44:56.132	16.76 sec	172.16.2.19	54994	193.109.246.48	80	6	0	APSF	1	15	1,991	990.8 bps
22-10-2014 09:44:40.120	22-10-2014 09:44:56.352	16.232 sec	193.109.246.48	80	172.16.2.19	54990	6	0	APSF	1	13	8,987	4.4 Kbps
22-10-2014 09:44:40.120	22-10-2014 09:44:56.260	16.140 sec	193.109.246.48	80	172.16.2.19	54991	6	0	APSF	1	12	7,392	3.7 Kbps
22-10-2014 09:44:40.120	22-10-2014 09:44:56.104	15.984 sec	193.109.246.48	80	172.16.2.19	54992	6	0	APSF	1	41	45,302	22.7 Kbps
22-10-2014 09:44:40.124	22-10-2014 09:44:56.100	15.976 sec	193.109.246.48	80	172.16.2.19	54993	6	0	APSF	1	14	8,987	4.5 Kbps
22-10-2014 09:44:40.124	22-10-2014 09:44:56.200	16.76 sec	193.109.246.48	80	172.16.2.19	54994	6	0	APSF	1	18	14,152	7.0 Kbps
22-10-2014 09:44:40.916	22-10-2014 09:44:57.180	16.264 sec	172.16.2.19	55002	108.168.157.176	80	6	0	APSF	1	7	655	322.2 bps

Page 1

4.他社類似製品比較

NetVizura NFAと他社類似製品との比較は以下の通りです。NFAの特長として、多彩な販売形態と低価格、必要な問題分析能力があります。

比較項目	NetVizura NFA	P社	S社	N社
問題分析能力	○	△ ※IFごとに表示不可、グラフ時間軸なし	○	△ ※Queryによるテキスト表示のみ
表示データの種類	○	△ ※QOS,AS表示なし	○	△ ※QOS,AS表示なし
日本語GUI	×	○	○	×
販売形態	①ライセンス販売 △ ②サブスクリプション販売 ○ ③アプライアンス販売 ○	①ライセンス販売 ○ ②サブスクリプション販売 × ③アプライアンス販売 ○	①ライセンス販売 ○ ②サブスクリプション販売 × ③アプライアンス販売 ×	①ライセンス販売 ○ ②サブスクリプション販売 × ③アプライアンス販売 ×
価格	○	○	×	×
性能限界	○ 50,000fps	○ 10,000fps	○ 50,000fps	× メーカ発表なし
マルチプラットフォーム	○	×	×	○

5.NFA製品ラインナップ

NetVizura NFAの製品ラインナップ(サブスクリプション)は以下のとおりです：

ライセンス	最大受信フロー(fps)	CPU規格	RAMサイズ	HDD規格と容量
50fps	50fps	シングルコア 2.0GHz以上	2GB以上	5GB以上
500fps	500fps	シングルコア 2.0GHz以上	3GB以上	10GB以上
5,000 fps	5,000fps	デュアルコア 2.0GHz以上	4GB以上	120GB SAS/SSDでRAID0/ストライプ方式RAID推奨
50,000fps	50,000fps	オクタコア2.0GHz以上	8GB以上	2.4TB SAS/SSDでRAID0/ストライプ方式RAID推奨
50,000fps以上	弊社までお問い合わせください			

* ライセンス列記載の各fps値は、そのライセンスで監視できる最大のfps値です。例えば、50fpsラインセンスでそれを超えたフローデータはドロップされます。ご購入前に 評価版を実環境にインストールし、通常時の負荷状態と最大値をご取得頂くことを推奨いたします。

5.NFA製品ラインナップ-2

NetVizura NFAの製品ラインナップ(アプライアンス製品)は以下のとおりです：

製品名称	最大受信(fps)	CPU規格	RAMサイズ	HDD規格と容量
BlueVault io-B(50fps)	50fps	Intel Core i3	4GB	512GB SSD
BlueVault io-B(500fps)	500fps	Inter Core i3	4GB	512GB SSD
BlueVault io-R(500fps)	500fps	Intel Core i3	8GB	1TB SATA RAID1
BlueVault io-R(5,000fps)	5,000fps	Inter Core i3	8GB	1TB SATA RAID1

* 製品名称に記載のあるfps以下であれば追加ライセンスなしでご利用頂けます。

* BlueVault io-B及びio-Rのハードウェア仕様(CPU規格、RAMサイズ、HDD規格と容量)は、2019年7月現在の情報となります。こちらの仕様は予告なく変更することがございますので、ご購入前に必ず弊社までお問合せください。

5.NFA製品ラインナップ-3

必要なライセンスパッケージは「fps(フロー/秒)の数」で決定します。

- ✓ ライセンスパッケージ（=fps数）を決定するには、
  概算見積りをする場合、PC１台１fps～1.5fpsで計算するといった方法があります。また、正確にfpsを測定するにはターゲットNW装置でfpsをカウントする必要があります。カウント方法は、評価版をインストールしカウントするのが確実となります。
- ✓ 製品価格は、価格表をご覧ください。
  価格表ダウンロードページ： https://www.jtc-i.co.jp/contact/pcontact.php

6.参考）フローとは

フローとは、２つのノード間セッションの初めから終わりまでの一連の通信のことです。送信元、宛先IPアドレス、ポート、プロトコルなど属性が同じものが１つのフローとしてカウントされます。また、フローを発呼するNW機器を本ドキュメントでは、エクスポータと呼びます。

従来のSNMPでは追跡出来なかったユーザとアプリケーションごとのトラフィック分析が可能となり、かつDPIより収集するデータ量が少ないこと、導入・運用コストが低いにも関わらず既存トラフィック分析・将来インフラ設計に有用なデータを簡単に収集出来るため、近年再び注目されているプロトコルとなります。

各ベンダー様々なフロー形式がありますので、ご利用のNW機器の型番、ファームウェアのバージョンを確認し、どのプロトコルがエクスポート可能かを先ずはご確認ください。

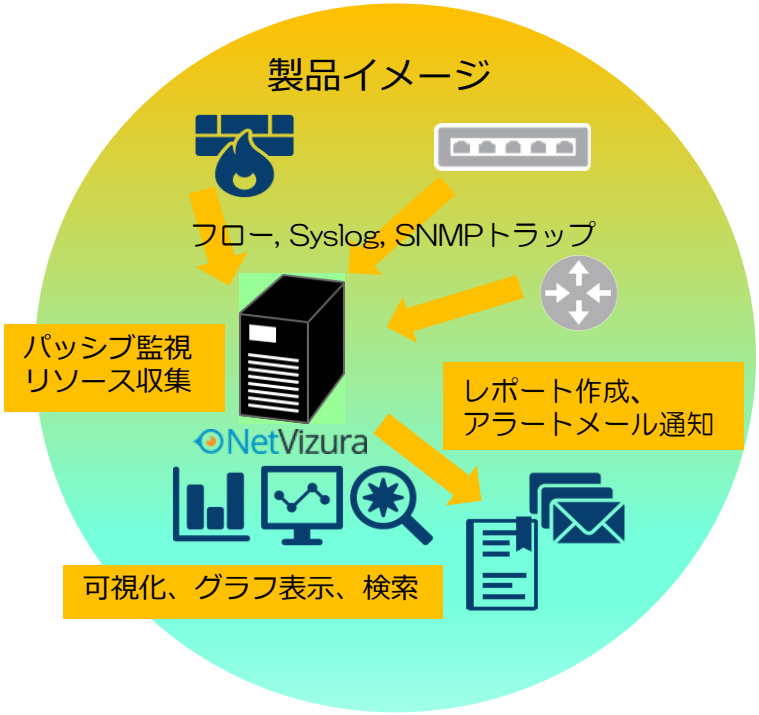
＊プロトコルの種類に関しては、本ドキュメントの特長4 様々なフロー形式をご参照ください。エクスポータ設定および対象フロープロトコルの形式・バージョンは、各メーカサイトをご参照ください。また、本製品ご購入前に 評価版でお試しいただくか、弊社まで対応状況をお問合せください（お問合せいただく際は、ターゲット装置のファームウェア情報、型番をご提供ください）。

7.NetVizura ELAの概要

NetVizura EventLog Analyzer(以降、NetVizura ELA)は、Syslog, SNMPトラップ収集・分析ソフトウェアです。フローデータを収集・分析するNetVizura NFAと組み合わせて横断的な障害検知・分析を可能とし、ネットワークの異常原因を早期発見出来ます。

NetVizura ELAのここがポイント！

- 低価格サブスクリプションとアプライアンス製品販売をラインナップ
- パッシブ監視のオールインワンソリューション※NFAと組み合わせた場合
- BSD-syslog, IETF-syslog両対応
- 分かりやすいWEB GUIで5W(どこ、だれ、いつ、何、なぜ)を支援
- 文字列、重要度、ログ種別を定義・組み合わせたアラームを柔軟に設定可能

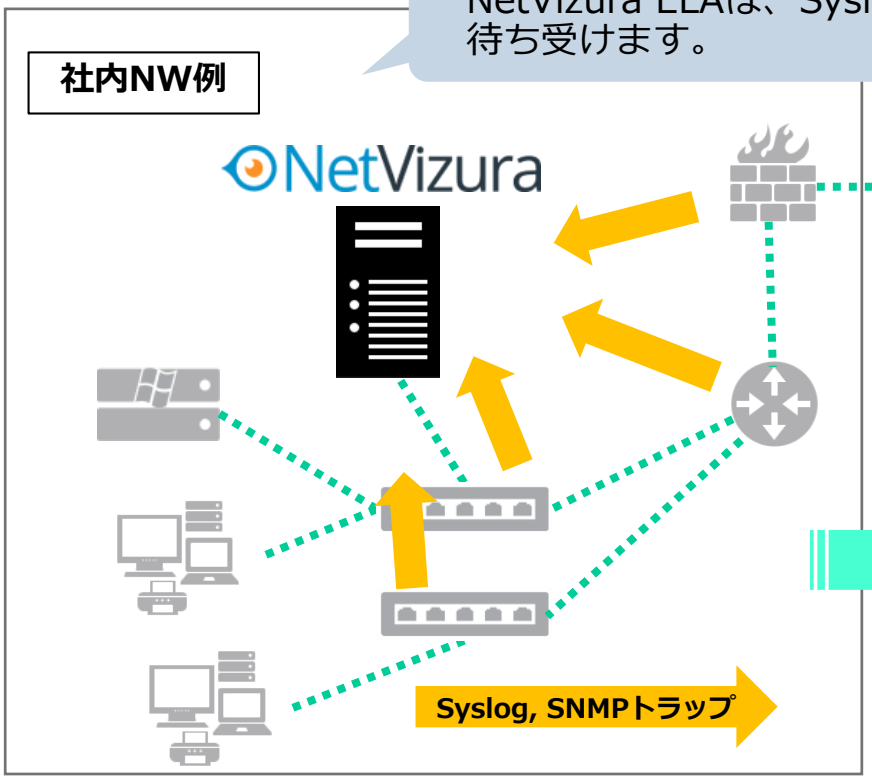


＊NetVizura ELAのみのご利用は、現在取り扱っておりません。NetViuzra NetFlow Analyzerご購入のお客様が、本製品利用の対象ユーザーとなります。

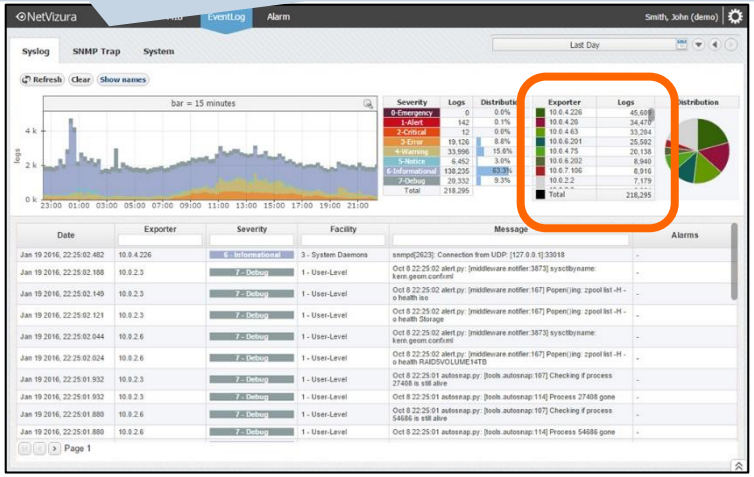
8.ELAシステム導入イメージ

各NW機器からNetVizura宛てに、Syslog, SNMPトラップを送信する設定を行ってください。

NetVizura ELAは、Syslog,SNMPトラップを待ち受けます。

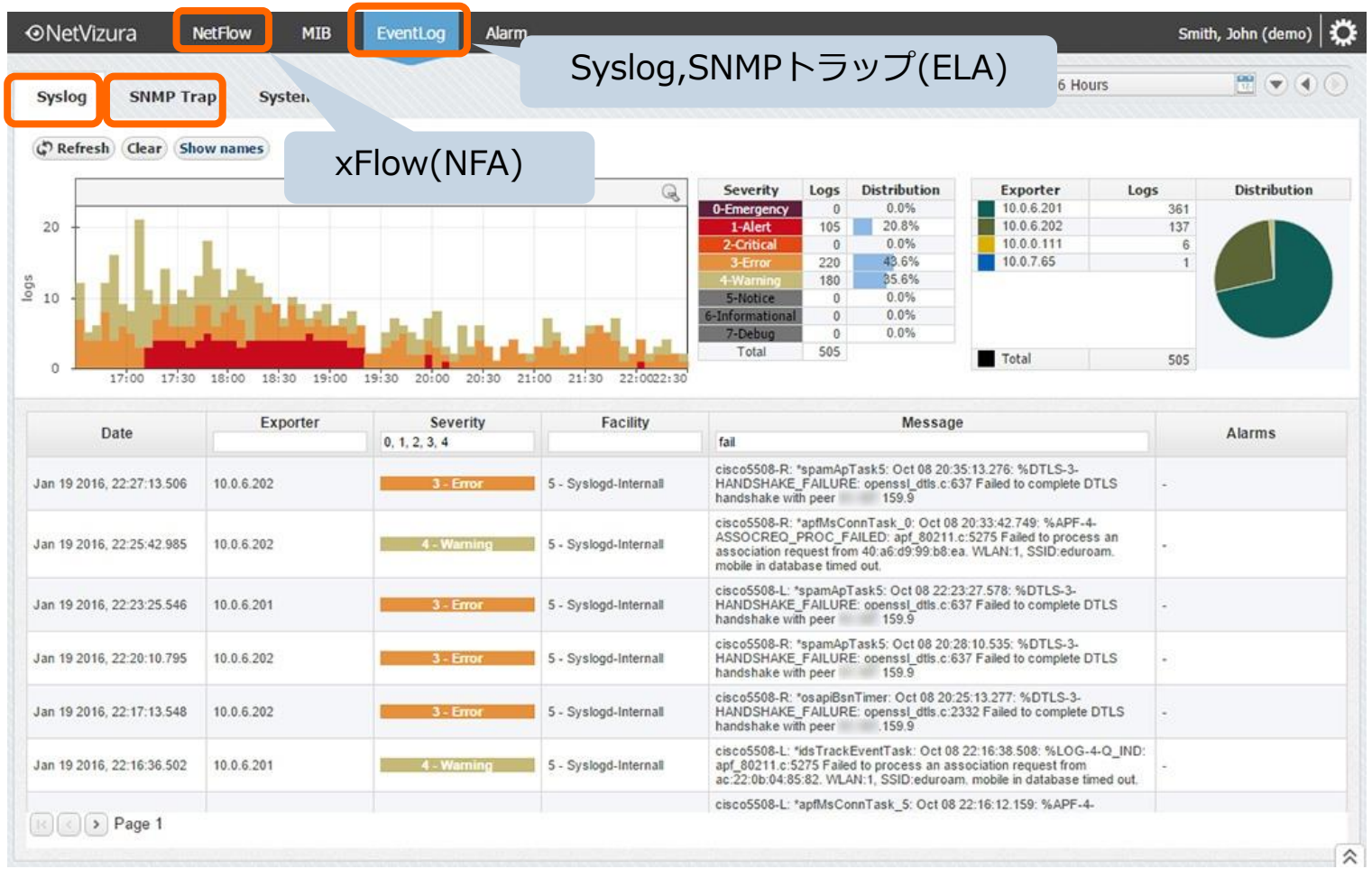


NetVizuraは、受信したSyslog/SNMPトラップからエクスポータを自動的に登録します。



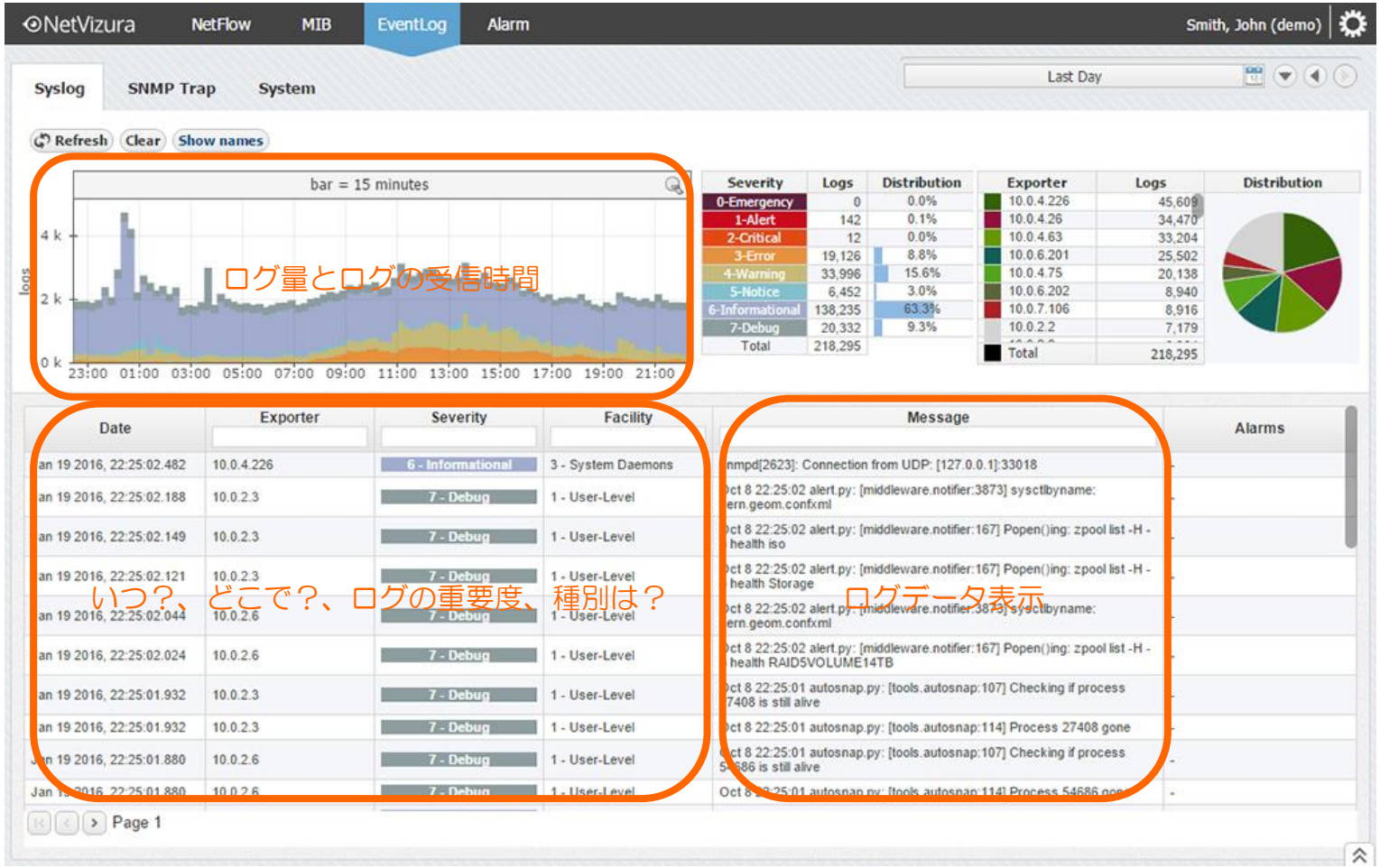
9.ELA特長 1 – パッシブ監視の統合

NetVizura ELAは、NFAとの同時利用でパッシブ監視(xFlow, Syslog, SNMPトラップ)をオールインワンで実現します。



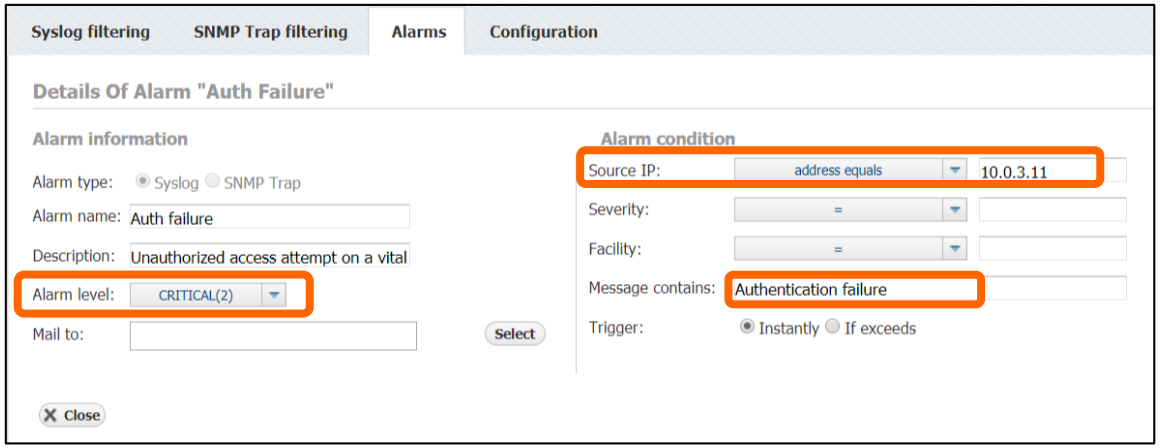
9.ELA特長 2 – 見やすい画面

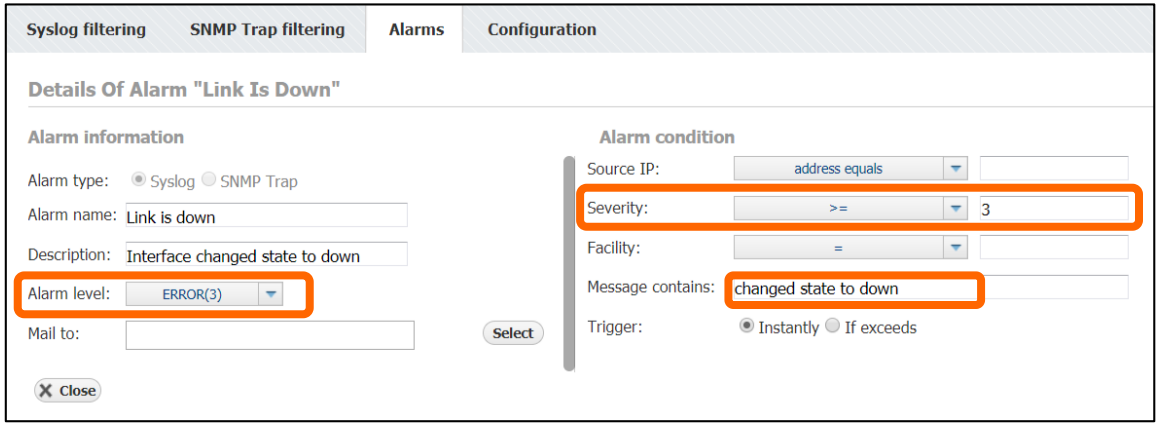
NetVizura ELAは、シンプルなグラフとログ、SNMPトラップの表示で運用者にデータを分かりやすく見える化します



9.ELA特長 3 – 柔軟なアラーム設定

NetVizura ELAは、送信元IPアドレス、ログの重要度、種別、ログメッセージに含む文字列を設定してアラーム発報が可能です。また、アラームレベルにより重要度を再定義出来ます。





10.ELA製品ラインナップ

NetVizura ELAの製品ラインナップ(サブスクリプション)は以下のとおりです：

xFlow/syslog 受信量	ルータ台数		
	3台以下	20台以下	100台以下
小 ↕ 大	50fps,3exp※ (NFAのみの購入)	50fps,20exp (NFA+ELAの購入)	-
	500fps,3exp※ (NFAのみの購入)	500fps,20exp (NFA+ELAの購入)	500fps,100exp (NFA+ELAの購入)
	5,000fps,3exp※ (NFAのみの購入)	5,000fps,20exp (NFA+ELAの購入)	5,000fps,100exp (NFA+ELAの購入)

※ NFA のみのご購入も可能です。つまり、Syslog 受信の要件がなければ、ELA をご購入いただく必要はございません。その場合でも、ELA の 3exp 迄の Syslog 受信機能は無料でご提供となります。

注意） expは「エクスポータ≒ルーター」のことです。fps は「flow per second」、mps は「message per second」の意味となります。
サブスクリプション記載の各 fps値 及び exp値は、そのライセンスで監視できる最大の fps値、exp値となります。
例えば、50fps,20exp ラインセンスを購入の場合、50fps を超過するとドロップします。また、20exp を超えたログ受信もドロップします。
ご購入前に 評価版を実環境にインストールし、通常時の負荷状態と最大値をご取得頂くことを推奨いたします。

10.ELA製品ラインナップ-2

NetVizuraアプライアンスio-Bの販売パターンは、以下の通りです：

販売パターン	ライセンス	最大性能 NetFlow(fps)	最大性能 Syslog(mps)	備考
BlueVault io-B(50fps,3exp)	NFA:50fps ELA:3exp(free)	50fps	500mps ※3exp迄	NFA,ELA同時利用時
BlueVault io-B(50fps,20exp)	NFA:50fps ELA:20exp	50fps	500mps ※20exp迄	NFA,ELA同時利用時
BlueVault io-B(500fps,3exp)	NFA:500fps ELA:3exp(free)	500fps	500mps ※3exp迄	NFA,ELA同時利用時
BlueVault io-B(500fps,20exp)	NFA:500fps ELA:20exp	500fps	500mps ※20exp迄	NFA,ELA同時利用時

＊ELAの単独利用販売はございません

10.ELA製品ラインナップ-3

NetVizura

NetVizuraアプライアンスio-Rの販売パターンは、以下の通りです：

販売パターン	ライセンス	最大性能 NetFlow(fps)	最大性能 Syslog(mps)	備考
BlueVault io-R(500fps,3exp)	NFA:500fps ELA:3exp(free)	500fps	1,000mps ※3exp迄	NFA,ELA同時利用時
BlueVault io-R(500fps,20exp)	NFA:500fps ELA:20exp	500fps	1,000mps ※20exp迄	NFA,ELA同時利用時
BlueVault io-R(500fps,100exp)	NFA:500fps ELA:100exp	500fps	1,000mps ※100exp迄	NFA,ELA同時利用時
BlueVault io-R(5,000fps,3exp)	NFA:5,000fps ELA:3exp	5,000fps	1,000mps ※3exp迄	NFA,ELA同時利用時
BlueVault io-R(5,000fps,20exp)	NFA:5,000fps ELA:20exp	5,000fps	1,000mps ※20exp迄	NFA,ELA同時利用時
BlueVault io-R(5,000fps,100exp)	NFA:5,000fps ELA:100exp	5,000fps	10,00mps ※100exp迄	NFA,ELA同時利用時

11.NetVizuraシステム要件

NetVizura(ELA+NFA)の推奨システム要件は以下の通りです：

	推奨仕様
CPU	Quad Core 3.0GHz以上
メモリ	4GB以上 ※秒間の受信性能要件によって、要求仕様は異なります。詳細は、弊社迄ご連絡ください
ディスク	1.6TB SASもしくはSSD*1 *1 RAID 0もしくは、他ストライピング方式のRAID構成推奨。また、古いフローデータのアーカイブの為に追加のストレージも推奨します。ログの保管要件によって、ディスクサイズは変化します。サイジングに関する詳細は、弊社迄ご連絡ください
OS	• CentOS 7 (64bit) • Ubuntu 18.04 LTS(64bit)

注意） 本推奨仕様は、以下の条件のもと計算しております。要件によって計算式は変わってきますのでご注意ください。
ELA: 20expを秒間500mpsとして計算 約1.5TB
NFA: 500fps。NetFlow Rawデータ保存期間 30日、NetFlowデーターベース保存期間 365日として計算 約100GB

11.NetVizuraシステム要件-2

NetVizura

ライセンス	50fps	50fps, 20exp	500fps	500fps,20exp	500fps,100exp	5,000fps	5,000fps,20exp	5,000fps,100exp	50,000fps	50,000fps,20exp	50,000fps,100exp
CPU規格	シングルコア2.0Ghz以上	クアッドコア3.0Ghz以上	シングルコア2.0Ghz以上	クアッドコア3.0Ghz以上	オクタコア3.6Ghz以上	デュアルコア2.0Ghz以上	クアッドコア3.0Ghz以上	オクタコア3.6Ghz以上	オクタコア2.0Ghz以上	オクタコア3.6Ghz以上	オクタコア3.6Ghz以上
RAMサイズ	2GB以上	4GB以上	4GB以上	8GB以上	8GB以上	4GB以上	8GB以上	8GB以上	8GB以上	16GB以上	16GB以上
HDD規格と容量	12GB以上	1.6TB SAS/SSDでRAID0/ストライプ方式RAID推奨	120GB以上	1.6TB SAS/SSDでRAID0/ストライプ方式RAID推奨	3.1TB SAS/SSDでRAID0/ストライプ方式RAID推奨	1.2TBSAS/SSDでRAID0/ストライプ方式RAID推奨	2.7TB SAS/SSDでRAID0/ストライプ方式RAID推奨	4.2TB SAS/SSDでRAID0/ストライプ方式RAID推奨	21TB SAS/SSDでRAID0/ストライプ方式RAID推奨	22.5TB SAS/SSDでRAID0/ストライプ方式RAID推奨	24TB SAS/SSDでRAID0/ストライプ方式RAID推奨

注意） 本推奨仕様は、以下の条件のもと計算しております。要件によって計算式は変わってきますのでご注意ください。
NetFlow Rawデータ保存期間 30日、NetFlow及びSyslogデーターベース保存期間 365日として計算

12. EventReporterとの連携

NetVizura NFAは、EventReporterと連携してActive Directoryのドメインユーザごとのトラフィックを可視化出来ます。

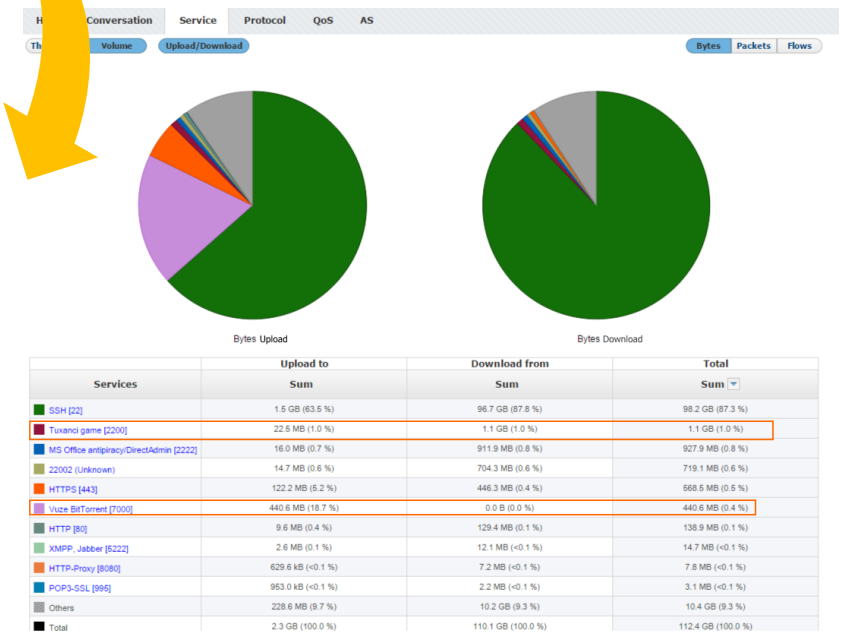
Active Directory

syslog送信

NetVizura
NA

EventReporterは、ログオンイベントのみをNetVizuraへsyslog送信

特定ユーザのトラフィック画面



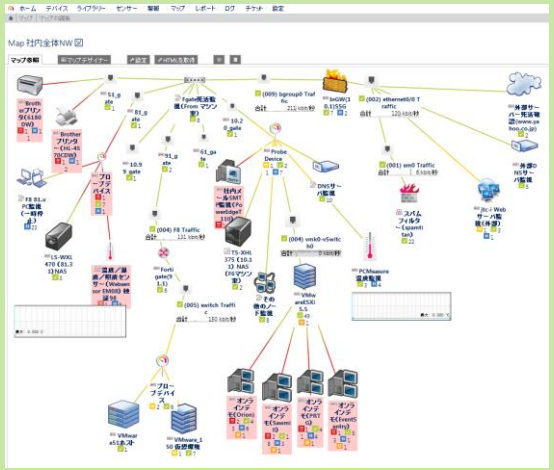
特定アカウントの通信状況がまるわかりに！！

12.PRTGとNetVizura同時利用

NetVizura NFAは、PRTGのNetFlowセンサーでは可視化出来ないIFごとのトラフィック監視やカスタムトラフィックによる特定のトラフィックを可視化出来ます。PRTGでサービス死活監視、NetVizura NFAにフローデータを任せてください。そして、御社ネットワーク見える化のレベルを１段向上してください。

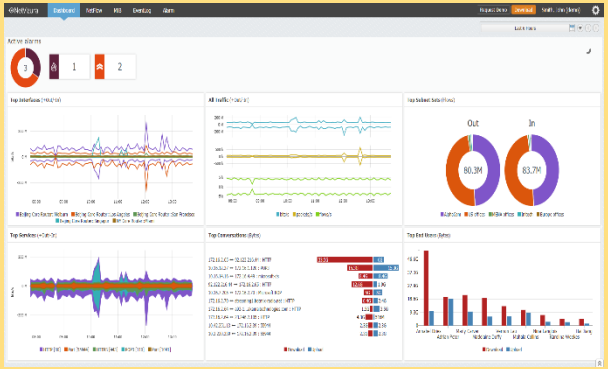
PRTG

PRTGは、サービスの死活監視



NetVizura

NFAは、フローデータによるトラフィック分析



13.評価とお問合せ

NetVizura

製品の評価について

- ✓ 評価版インストーラを下記ソフトウェアダウンロードページから
  ダウンロードしてご利用ください：

  ソフトウェアダウンロード： https://www.jtc-i.co.jp/support/download/

- ✓ すべての機能を３０日間無料でご利用いただけます。
- ✓ 本製品は日本語ユーザーインターフェイスに対応していません。日本語
  ユーザーインターフェイスの利用をご希望の場合は、
  弊社までご相談ください。

  お問合せ：https://www.jtc-i.co.jp/contact/scontact.php

- ✓ ライセンスを登録すると製品版として動作します。

製品のお問合せについて

- ✓ 製品ご購入前のお問合せ先：
  https://www.jtc-i.co.jp/contact/scontact.php
- ✓ 製品ご購入後のお問合せ先：カスタマーポータル
  https://www.jtc-i.co.jp/support/customerportal/

ジュピターテクノロジー株式会社

【本社】
〒183-0023
東京都府中市宮町2-15-13　第15三ツ木ビル8Ｆ
TEL：042-358-1250　FAX：042-360-6221

【大阪営業所】
〒530-0001
大阪府大阪市北区梅田1-1-3 大阪駅前第3ビル11Ｆ
TEL：06-6131-8471　FAX：06-6131-8472

E-Mail: sales@jtc-i.co.jp
URL: https://www.jtc-i.co.jp/