Flowmon

V.9.00.10 ガイド

平成 30 年 1 月 30 日

Ver.9.00.10 対応

オリゾンシステムズ株式会社

目次

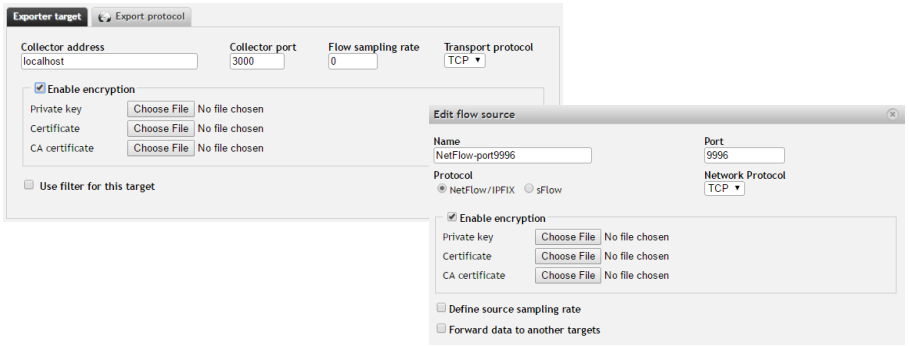
1. はじめに

本資料は、Flowmon コレクタ・プローブ及び Flowmon ADS の ver.9 における新機能についてご紹介しております。

2. Flowmon コレクタ・プローブ ver.9 の新機能

2. 1. セキュリティの強化

TLS3.1 に対応し、よりセキュリティが強化されました。
また、フローデータの TCP-TLS 暗号化転送の実現により、拠点からデータセンターまたはクラウドへ安全にフローデータを収集し、暗号化によるフローデータエクスポートと他のコレクタへのデータ転送(複製)が可能となりました。
結果、クラウド環境における Flowmon のご利用がサポート可能となりました。
今後、Flowmon の AWS に対応したモジュールのご提供開始も予定されており、Flowmon をご利用いただける環境がより広がって参ります。



2. 2. ネットワークパフォーマンスモニタリング & 診断の拡張

2. 2. 1. サードベンダの IPFIX 拡張解析のサポート

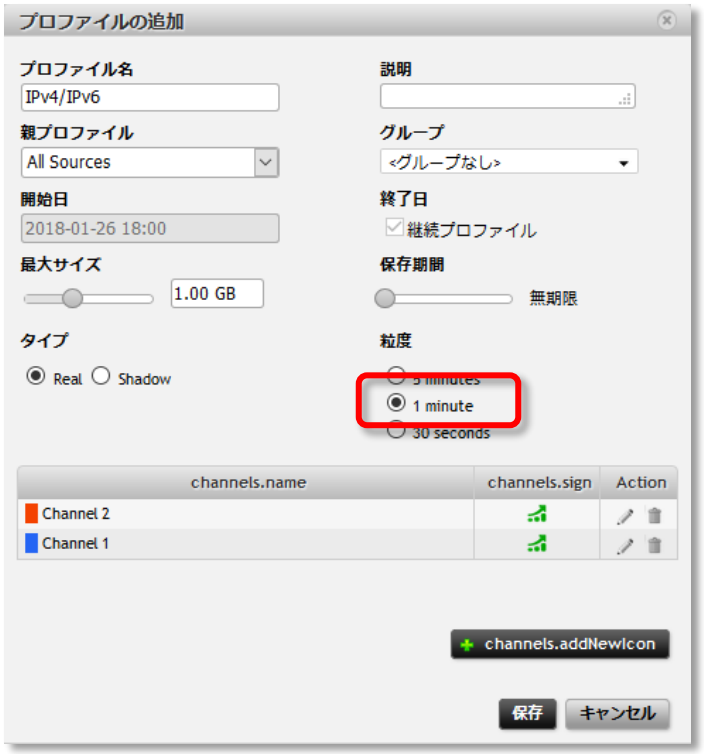
これまでの Flowmon プローブでの IPFIX 拡張解析に加え、サードベンダーの IPFIX 拡張解析がサポート可能となりました。

- Cisco (AVC HTTP)
- Gigamon (HTTP, DNS)
- IXIA
- VMWare NSX (rule ID, vmUUID, vnicIndex)

2. 2. 2. 1 分粒度プロファイル

※本機能は、ver.9.01.00 以降搭載予定です。

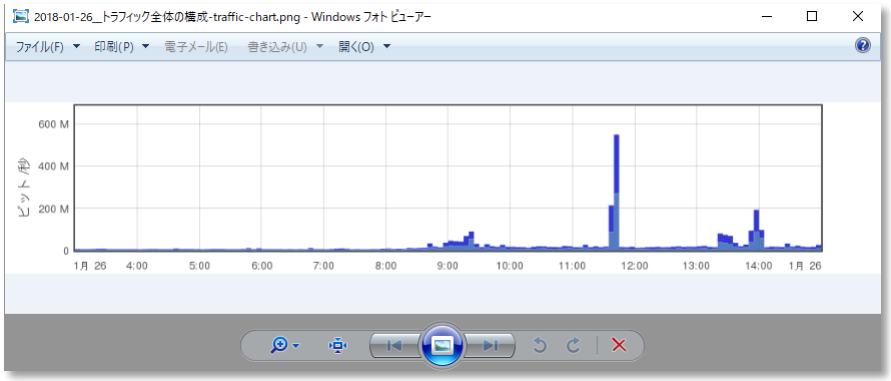
1 分粒度のプロファイルがご利用可能となりました。
これにより、解析の目的や用途により、30 秒、1 分、5 分と粒度を選択し、最適な粒度での解析を行っていただくことが可能となります。



2.3. レポート機能の追加

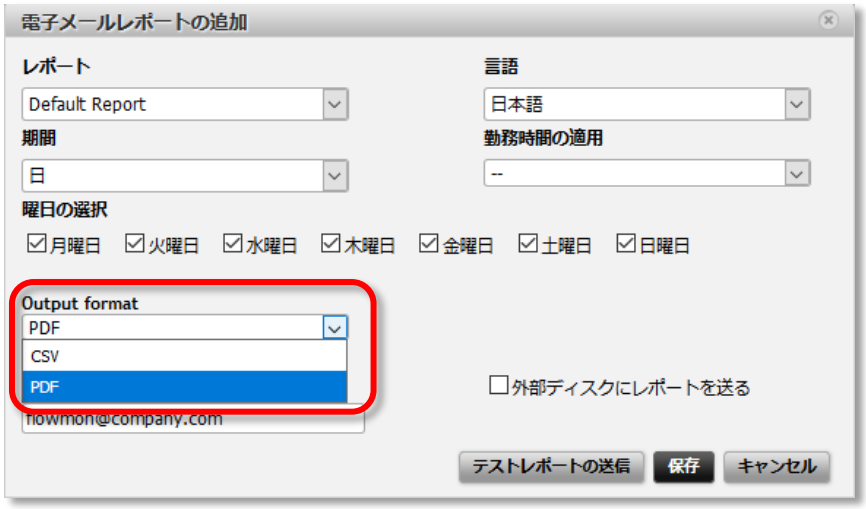
2.3.1. チャプタ画像の保存

レポートに挿入されたグラフ画像を画像として保存することができるようになり、Flowmon でのレポート結果が他の資料でも活用していただきやすくなりました。



2.3.2. CSV ファイルでのレポート送信

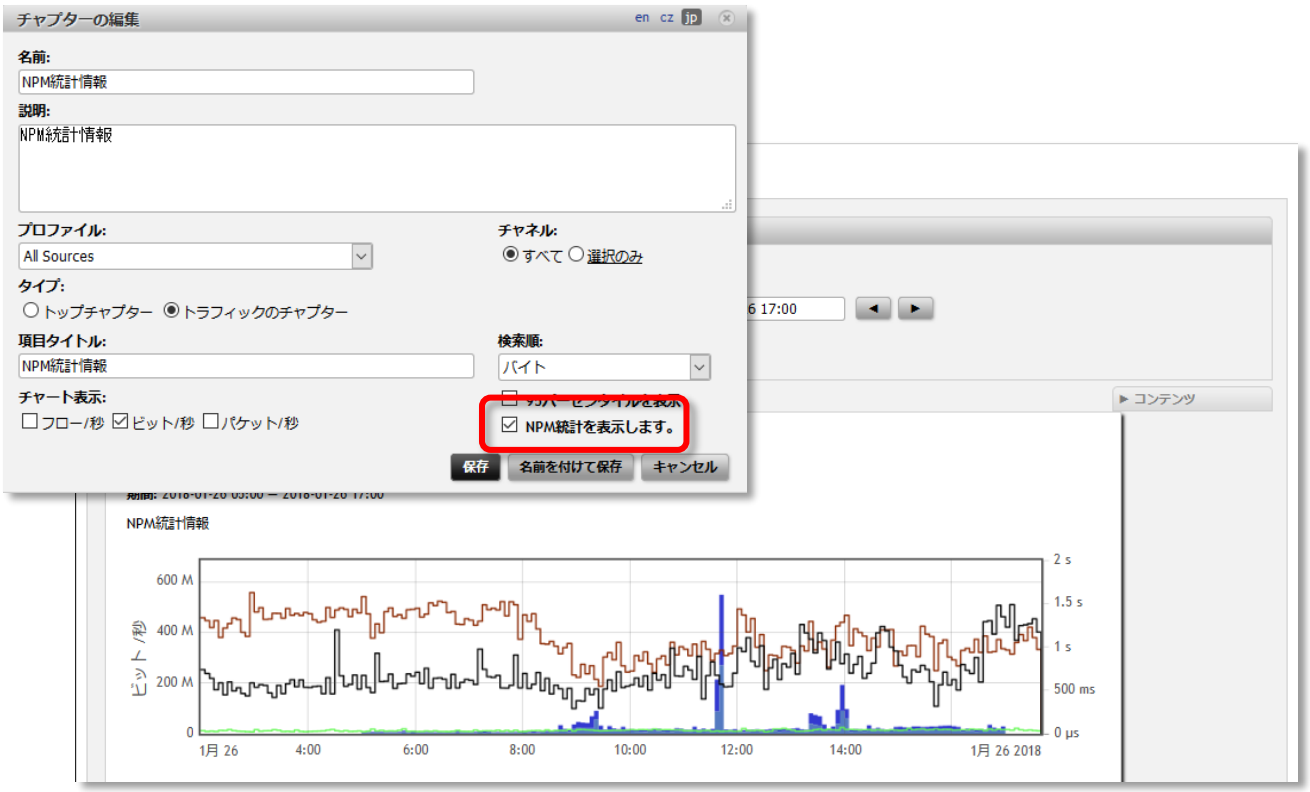
定期的にメール送信や外部ディスクへ保存する「電子メールレポート」の形式に、これまでの PDF 形式に加え、CSV 形式が選択可能となりました。



2.3.3. NPM グラフの表示

※本機能は、ver.9.01.00 以降搭載予定です。

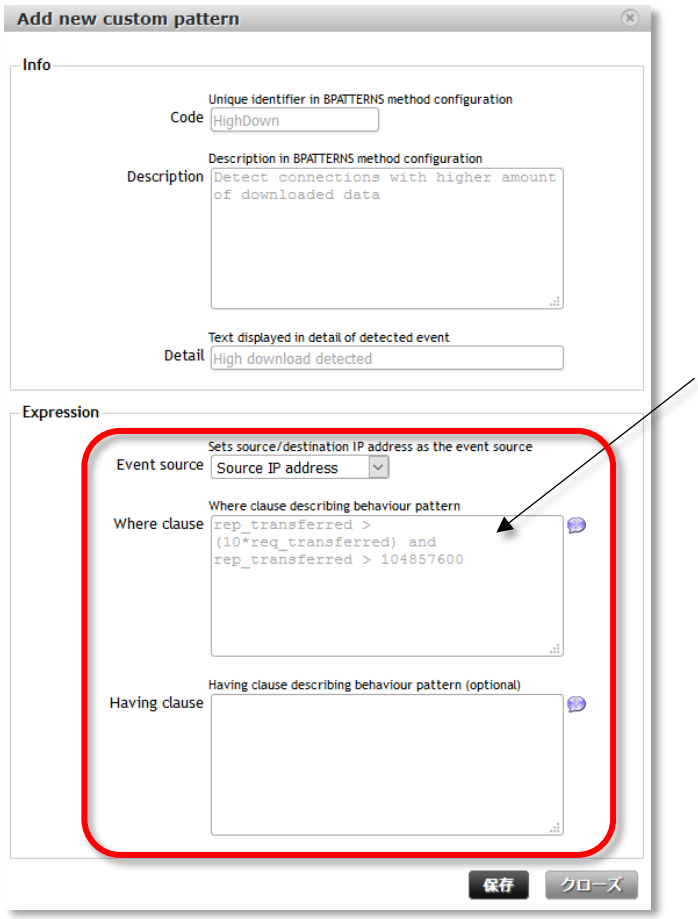
解析画面でのみ表示が可能であった NPM のグラフが、レポートでも表示可能となりました。



3. Flowmon ADS ver.9 の新機能

3.1. ユーザ定義のふるまいパターン

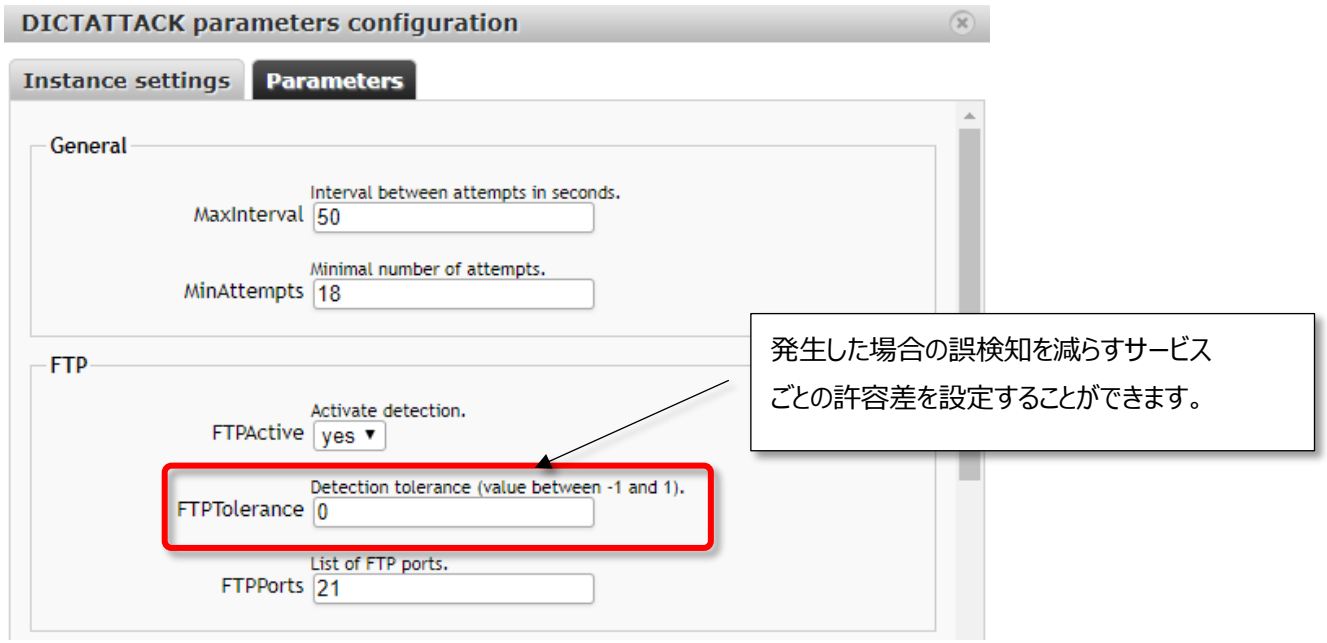
FlowmonADS による検知をよりお客様の環境に合わせて行っていただくため、お客様にてふるまい検知パターンを作成することが可能になりました。これにより、特定のユースケースやシナリオに焦点を当てた検出や、異なる環境での検出等、問題に対して迅速に、より複雑な検出ルールを作成することができ、上級ユーザの要求にも応えることができます。



- イベントソースは送信元、送信先 IP アドレスを選択することができます。
- 国別や OS を直接 GUI から設定することができます。

3. 2. 広範囲な辞書攻撃の検知

FTP, HTTP, IMAP, POP3 , SMTP, VNC, RDP, Samba, SSH, Telnet 等のさまざまなサービスに対応し、Flowmon ADS をユニバーサル検知メソッドとして機能させることが可能です。
また、攻撃を検出するポートを設定可能となりました。



4. お問い合わせ

バージョンアップにおいて問題が発生した場合や本マニュアルの不明点などにつきましては下記までご連絡ください。

- 連絡先
  オリゾンシステムズ株式会社
  ORIZON Systems Co. LTD.
  東京都新宿区新宿 6-27-56 新宿スクエア 7F
  E-mail：flowmon-support@orizon.co.jp