NEC

# WebSAM

# Network Flow Analyzer 1.1

## リリースメモ

WebSAM

# 著作権



# 輸出時の注意

本製品を輸出する場合には、外国為替および外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上、必要な手続きをお取りください。

なお、ご不明な場合は、弊社担当営業にお問合せください。

# 商標

# はじめに

このたびは、WebSAM Network Flow Analyzer 1.1 (以降、NFA と略記します) をお買い求めいただき、誠にありがとうございます。NFA では、ネットワークを流れる通信のフロー情報を分析することで、様々な通信の状況を可視化することができます。

本書では、NFA のリリース項目、および、NFA のインストールメディアの収録内容について説明しています。NFA をご使用になる前に本書の内容を確認してください。

# 本書の表記規則

本書では、注意すべき事項や補足事項について、以下の表記を用います。

**注意補足事項の表記**

| 表記 | 説明 |
|---|---|
| **⚠ 注意** | 製品機能の設定、操作を行う上で守らなければならない事柄や特に注意すべき点を示します。 |
| **ヒント** | 知っておくと役に立つ便利な情報を示します。 |

本書では、以下の表記規則に従って記述しています。

**表記規則**

| 表記 | 説明 | 例 |
|---|---|---|
| [] | ダイアログ、タブ、メニュー、項目名、ボタンなどの画面要素を示します。 | [**ダッシュボート**]タブ、[**OK**]ボタン |
| <*userinput*> | ユーザー環境により変化する項目、および入力値を示します。 | <*%インストールディレクトリ%*>、<*filepath*> |
| `configuration file` | 設定ファイルの記述内容を示します。 | 以下の値を設定します。<br>`port = 27120` |
| `command line` | コマンドライン操作を示します。 | 以下のコマンドを実行します。<br>`$ rpm -q nec-nfa-controller` |

本製品は、デフォルトでは、以下のディレクトリにインストールします。

**デフォルトのインストール先:**

```
/opt/nec/nfa
```

本書では、上記のインストール先を<*%インストールディレクトリ%*>と記述します。インストール先を変更している場合は、適宜読み替えてください。

インストールの際に、本製品で管理するデータの格納先をインストール先とは異なるディレクトリに設定することができます。本書では、この場合のデータの格納先を<*%データディレクトリ%*>と記述します。インストール先とデータ格納先を分離していない場合は、<%

*データディレクトリ%>と<%インストールディレクトリ%>*は、同じディレクトリを指します。

# 目次

# 第 1 章
# メディア構成

インストールメディアの収録内容について示します。

## 目次

# 1.1　ディレクトリ構成

インストールメディア内のディレクトリ構成について説明します。

- nfa-release.pdf (本書)
- nfa-install (インストーラー)
- nfa-upgrade (アップグレードインストーラー)
- conf/, lib/, rpm/ (インストール関連ファイル)
- doc/ (「1.2　ドキュメント一覧（2 ページ）」参照)
  - nfa-startup.pdf
  - nfa-reference.pdf
  - nfa-oss-license.pdf
  - oss-source/ (同梱オープンソースソフトウェアのソースコード)
- tools/
  - flow-Analyzer.mib (NFA の MIB オブジェクト定義ファイル)
  - diskcheck/ (ディスク使用量をチェックするサンプルスクリプト)

# 1.2　ドキュメント一覧

インストールメディア内に収録している NFA のドキュメントについて説明します。

**表 1-1　NFA のドキュメント一覧**

| タイトル (ファイル名) | 概要 |
|---|---|
| WebSAM Network Flow Analyzer 1.1 リリースメモ<br>( nfa-release.pdf ) | NFA 1.1 のリリース内容を示したドキュメント(本書)です。 |
| WebSAM Network Flow Analyzer 1.1 スタートアップガイド<br>( nfa-startup.pdf ) | NFA 1.1 のセットアップ方法を示したマニュアルです。<br>新規インストールや、古いバージョンからのアップグレード (バージョンアップ) の手順を記載しています。 |
| WebSAM Network Flow Analyzer 1.1 リファレンスマニュアル<br>( nfa-reference.pdf ) | NFA 1.1 の操作マニュアルです。 |
| WebSAM Network Flow Analyzer 1.1 オープンソースソフトウェアのライセンス条文<br>( nfa-oss-license.pdf ) | NFA 1.1 が利用しているオープンソースソフトウェアのライセンス条文および著作権表示です。 |

# 第 2 章
# 製品概要

NFA の製品概要について説明します。

## 目次

# 2.1　製品の特長

NFA では、ネットワークを流れる通信のフロー情報を、直感的で簡単な操作で分析していき、通信状況を様々な視点で可視化することができます。

NFA は、どこから、どこ宛に、何の通信が、どれだけ行われているのか を細かく分析、表示することで、ネットワークの安定運用をサポートします。

## フロー情報(NetFlow、IPFIX、sFlow)から通信状況を詳細に分析

ネットワークの通信状況を調べる方法として、一般的に SNMP が多く用いられています。しかし、SNMP では、スイッチやルーターの各インターフェイスを流れる通信量を調べることはできても、その通信量の内訳を調べることは困難です。

NFA では、SNMP ではなく、フロー情報(NetFlow、IPFIX、sFlow)を用いて通信状況を分析します。フロー情報を用いた分析により、SNMP では調べることができなかった、どこから、どこ宛に何の通信がどれだけ行われているのかの通信量の内訳を細かく調べることが可能です。通信状況を詳細に把握することで、ネットワーク障害の原因調査やキャパシティ管理業務を効率的に行えるようになります。

## 簡単な操作でドリルダウン分析が可能

NFA では、画面上のグラフ、一覧の情報をクリック 1 つで、簡単に絞り込んでいくことができます。

例えば、以下のように、画面に表示した情報に対し、直感的で簡単な操作を行っていくことで、より細かな通信状況を即座に確認していくことができます。

操作例:

1. 各インターフェイスを流れる通信量の表示から、特定のインターフェイス(仮に Ethernet1/1)を選択します。

   (選択した Ethernet1/1 を流れる通信の表示に絞り込まれます。)

2. 各アプリケーションの通信量の表示から特定のアプリケーション(仮に http)を選択します。

3. Ethernet1/1 を流れる http 通信量に関する分析結果が表示されます。

## 表示内容の自由なカスタマイズ機能を提供

NFA では、可視性の向上を図るために表示内容を自由にカスタマイズすることができます。

例えば、以下のように、運用環境に合わせて、表示、分析のカスタマイズを行っていくことで、ネットワークの状況を正確に把握できるようになります。

カスタマイズ例:

- NFA にログインするユーザー毎に、ダッシュボード(メイン画面)で表示するグラフや一覧の内容を定義し、運用することができます。
- 独自の業務アプリケーション通信の定義や IP アドレスの範囲指定による部門の定義を行うことで、分析結果をより分かり易く表現することができます。

# 2.2　機能概要

NFA が提供する機能概要について説明します。

## ダッシュボード

- NFA にログインしたユーザーが担当するネットワーク範囲について、現在の通信状況やイベント発生状況をリアルタイムに表示します。
- 表示するすべての分析結果を CSV ファイル形式で外部出力することができます。
- グラフや一覧を表示する構成要素である[**ウィジェット**]をドラッグ&ドロップの操作で自由に配置でき、ユーザー毎の運用に合わせたダッシュボード定義を簡単に作成することができます。

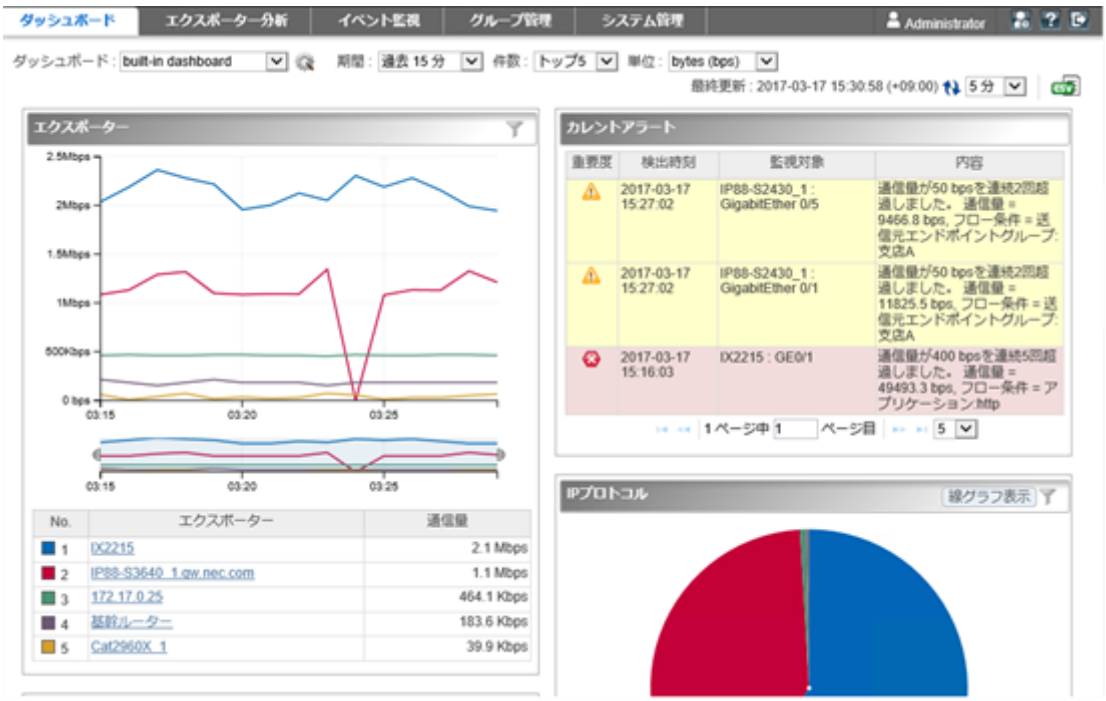



**図 2-1　ダッシュボード表示**

## エクスポーター分析

- フロー情報を送信してくるエクスポーターやそのインターフェイスを絞りこんで、詳細な通信状況を分析することができます。

- 現在の通信状況だけではなく、過去の通信状況も分析することができ、中長期的な通信状況の変化の推移を確認することができます。
- ダッシュボード画面と同様に、各分析結果を CSV ファイル形式で外部出力することができます。

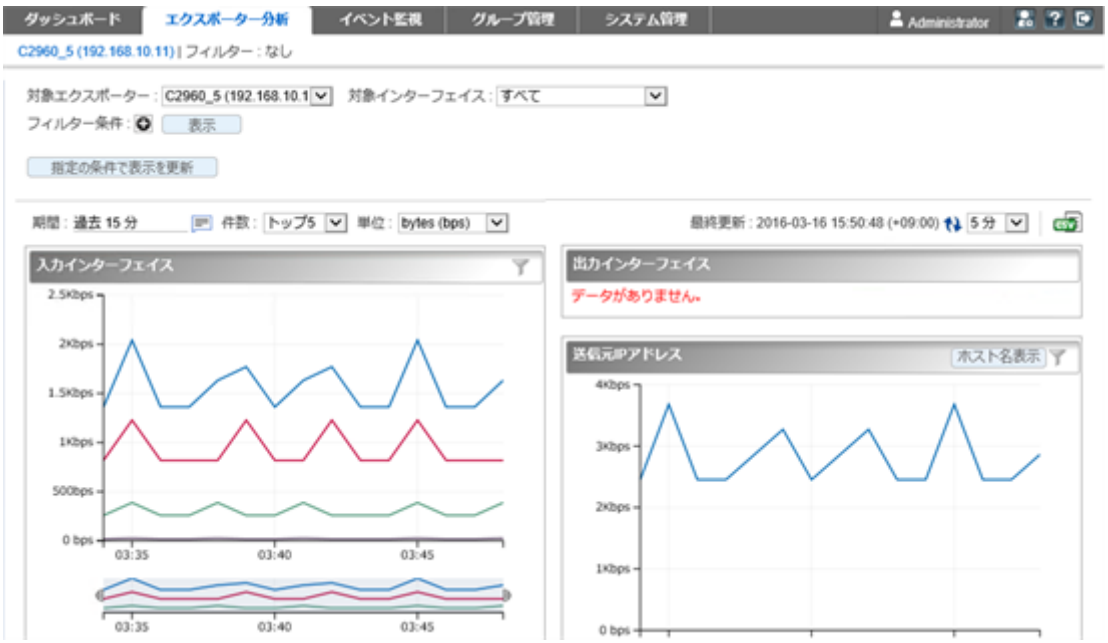



**図 2-2　エクスポーター分析**

## イベント監視

- 送信元や宛先の IP アドレス、アプリケーションなどの条件で絞り込んだ通信量に対し、しきい値監視を行うことができます。
- しきい値超過、回復に関するイベントの発生履歴を一覧で表示します。ダッシュボード画面にカレントアラートウィジェットを配置した場合は、現在のイベントの発生状況をダッシュボード画面で見ることができます。
- しきい値超過、回復のイベントは、SNMP トラップ形式で、別の管理システムに送信することができます。


**図 2-3　イベント一覧**

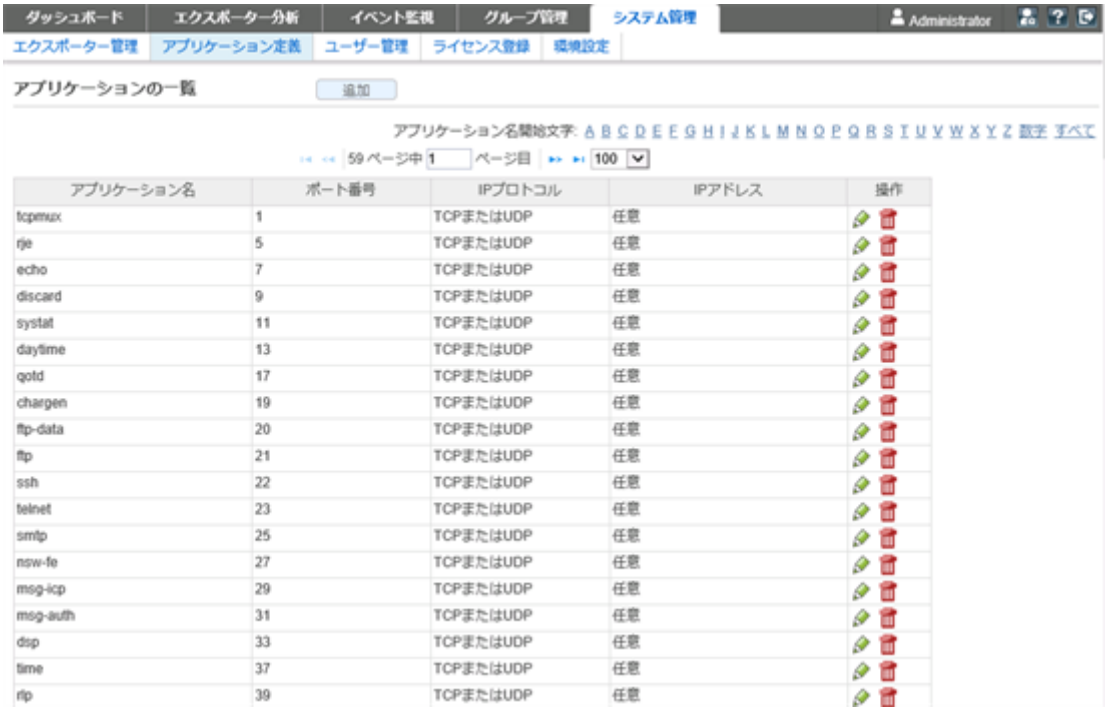
## グループ管理

- 通信のエンドポイント(送信元、または宛先)である複数の IP アドレスまたはネットワークアドレスを部門単位などでグルーピングすることで、グループ単位での通信量の分析を行うことができます。
- LAG(Link Aggregation)を構成する複数のインターフェイスをグルーピングすることで、1 つの LAG インターフェイスとして通信量を分析することができます。


**図 2-4　エンドポイントグループ一覧**

## システム管理

- 通信状況の分析で利用するアプリケーションの定義を行うことができます。アプリケーションの定義は、IP プロトコルとポート番号の組み合わせの情報に送信元、または、宛先にあたる IP アドレスを組み合わせることで、細分化したアプリケーション定義を行うことができます。
- フロー情報を送信するエクスポーターやそのインターフェイスの情報、ライセンスの割り当て状況を一覧で管理することができます。
- NFA にログインするユーザーのパスワードやデフォルトで表示するダッシュボードの定義の情報を管理することができます。




| アプリケーション名 | ポート番号 | IPプロトコル | IPアドレス | 操作 |
|---|---|---|---|---|
| tcpmux | 1 | TCPまたはUDP | 任意 | |
| rje | 5 | TCPまたはUDP | 任意 | |
| echo | 7 | TCPまたはUDP | 任意 | |
| discard | 9 | TCPまたはUDP | 任意 | |
| systat | 11 | TCPまたはUDP | 任意 | |
| daytime | 13 | TCPまたはUDP | 任意 | |
| qotd | 17 | TCPまたはUDP | 任意 | |
| chargen | 19 | TCPまたはUDP | 任意 | |
| ftp-data | 20 | TCPまたはUDP | 任意 | |
| ftp | 21 | TCPまたはUDP | 任意 | |
| ssh | 22 | TCPまたはUDP | 任意 | |
| telnet | 23 | TCPまたはUDP | 任意 | |
| smtp | 25 | TCPまたはUDP | 任意 | |
| nsw-fe | 27 | TCPまたはUDP | 任意 | |
| msg-icp | 29 | TCPまたはUDP | 任意 | |
| msg-auth | 31 | TCPまたはUDP | 任意 | |
| dsp | 33 | TCPまたはUDP | 任意 | |
| time | 37 | TCPまたはUDP | 任意 | |
| rlp | 39 | TCPまたはUDP | 任意 | |

**図 2-5　アプリケーション定義**

# 第 3 章
# 動作環境

NFA の動作環境について説明します。

## 目次

# 3.1　システム構成

NFA のシステム構成について説明します。

NFA の運用環境は、「図 3-1　システム構成図（10 ページ）」に示した通り、NFA をインストールしたサーバー(NFA サーバー)、および、NFA の利用者の端末のほか、エクスポーター、エンドポイントで構成されます。

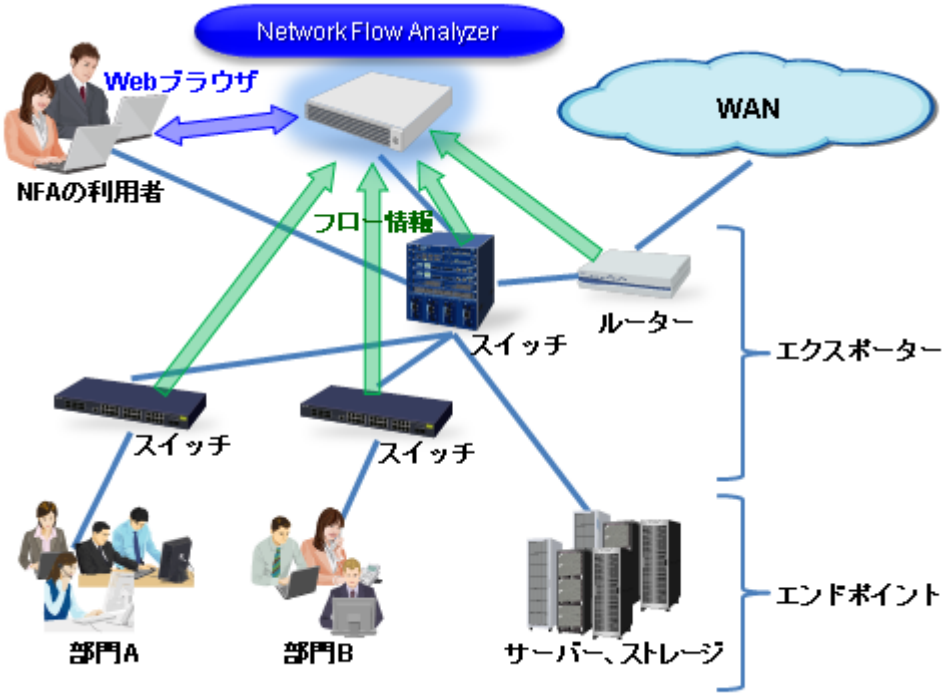



**図 3-1　システム構成図**

NFA は、フロー情報を受信・蓄積するフローコレクターとしての役割と、蓄積したフロー情報から通信状況を分析するフローアナライザーとしての役割の 2 つを持ちます。また、NFA の利用者向けの画面を提供する Web サーバーの機能も内蔵しています。NFA では、フローコレクター部分を 「コレクター」 (collector)、フローアナライザー部分と Web サーバーを合わせて 「コントローラー」 (controller) と呼びます。

NFA の利用者は、手元にある端末から Web ブラウザーを起動して、NFA の Web コンソールに接続します。

## ヒント

- NFA では、ネットワークに接続し、通信を行う端末やサーバーなどの機器のことを総称してエンドポイントと呼んでいます。
- エンドポイント間の通信内容をフロー情報に変換し、NFA に送信することができるスイッチやルーターなどの機器のことを総称してエクスポーターと呼んでいます。

# 3.2　システム要件

NFA の動作に必要なシステム要件、および、サポート環境について以下に示します。

**表 3-1　サーバーのシステム要件**

| 項目 | 内容 |
|---|---|
| CPU | Intel クアッドコア Xeon 以上、または同等の互換プロセッサを推奨 |
| システムメモリ | 最低 4GB 以上 (8GB 以上を推奨) |
| ディスク容量 | インストールディレクトリ: 5GB 以上 |
| | データディレクトリ: 最低 100GB 以上 |
| OS | • Red Hat Enterprise Linux 6 (x86_64)<br>• Red Hat Enterprise Linux 7 (x86_64) |
| フロープロトコル | • NetFlow (v5、v9)<br>• IPFIX<br>• sFlow (v4、v5)<br>NetFlow、IPFIX はサンプリングにも対応 |

**表 3-2　Web ブラウザーの要件**

| 項目 | 内容 |
|---|---|
| 対応ブラウザー | Windows 上で動作する以下のブラウザー<br>• Internet Explorer 11<br>• Mozilla Firefox 38 以上<br>• Google Chrome 48 以上 |
| CPU | Intel Core i3 以上、または同等の互換プロセッサを推奨 |
| システムメモリ | 1GB 以上 |

**ヒント**

- ブラウザーに最新の修正プログラムを適用した上でご利用いただくことを推奨します。修正プログラム未適用の場合、一部機能が正常動作しない場合があります。
- ブラウザーによっては、Unicode のサロゲートペア文字が 2 文字として扱われることがあります。この場合、各入力欄に実際に入力できる文字数は少なくなります。

# 3.3　フローデータの管理について

NFA では、受信したフローデータをデータベースを用いて管理しています。ここでは、フローデータの管理の仕組みについて説明します。

## 3.3.1　フローデータの保持期間と丸め処理について

NFA では、大量のフォローデータを限られたディスク容量の中で長期間保持するために、受信したフローデータを以下の「表 3-3　フローデータの粒度と保持期間（12 ページ）」で示す単位時間ごとに集約(丸め処理)し、データの粒度を変えて保持しています。また、NFA で

は、データの粒度ごとに保持期間を設けており、保持期間を超えたデータを破棄します。保持期間はユーザーが変更することもできます。

**表 3-3　フローデータの粒度と保持期間**

| データの粒度(単位時間) | デフォルトの保持期間 | 保持期間の変更可能範囲 |
|---|---|---|
| 1 分 | 24 時間 | 2～168 時間 |
| 10 分 | 72 時間 | 12～336 時間 |
| 60 分 | 14 日間 | 4～60 日間 |
| 6 時間 | 60 日間 | 14～365 日間 |
| 24 時間 | 365 日間 | 60～1095 日間 |
| 7 日 | 1095 日間 | 365～2190 日間 |

フローデータの集約処理では、単位時間ごとに以下の 7 つのフローキーがすべて同一のフローデータを集約して 1 つにまとめます。

1. 送信元 IP アドレス
2. 宛先 IP アドレス
3. 送信元ポート番号
4. 宛先ポート番号
5. IP プロトコル
6. ToS バイト(DSCP)
7. 入力インターフェイス

さらに、NFA では、フローデータの蓄積に必要なディスク使用量を一定に抑えるため、上記の集約処理に加えて、以下のような処理を行います。

- 単位時間ごとに、通信量の多い上位 1,000 フローまでのデータのみを詳細な分析対象として管理します。
- 上位 1,000 フローに含まれない下位のフローデータについては、「その他」のフローとして、集約して管理します。

## 3.3.2　ディスク使用量の見積もり方法

受信したフローデータを蓄積、管理するために必要なディスク使用量の見積もり方法について説明します。

フローデータの蓄積、管理に必要なディスク使用量は、NFA が管理するエクスポーターの台数、および、フローの発生頻度に関係しています。また、「3.3.1　フローデータの保持期間と丸め処理について（11 ページ）」で示した通り、フローデータに対する保持期間、および単位時間ごとの最大フロー数は、NFA で規定されています。そのため、フローデータの蓄積に必要なディスク使用量の目安は、これらを踏まえた計算式から算出することができます。

### ⚠ 注意

エクスポーターの台数が多い場合など、フローデータのサイズは非常に大きくなるため、ディスクの空き容量が枯渇する可能性があります。ディスクが枯渇すると、新規のフローデータが受信できない他、全体として正常に動作できなくなります。ディスク容量が枯渇しないよう、最大フロー数は、少し余裕を持たせて計算することを推奨します。

具体的な算出方法を以下に説明します。

1. NFA で管理するエクスポーターの台数を確認します。

   今後の運用において増加する予定があれば、最終的な管理数を明確にします。

2. フローの保持期間を確認し、ディスク容量算出で使用する係数を以下の計算式から算出します。

   保持期間係数 P = P1 × 60 + P2 × 6 + P3 × 24 + P4 × 4 + P5 + P6 ÷ 7

   - P1: 1 分粒度データの保持期間(単位：時)
   - P2: 10 分粒度データの保持期間(単位：時)
   - P3: 60 分粒度データの保持期間(単位：日)
   - P4: 6 時間粒度データの保持期間(単位：日)
   - P5: 24 時間粒度データの保持期間(単位：日)
   - P6: 7 日粒度データの保持期間(単位：日)

   計算結果の小数点以下は切り上げてください。

   保持期間がデフォルト値のままであれば、係数は 2970 となります。

   #### ヒント

   フローデータに対する保持期間の変更については、「3.3.1　フローデータの保持期間と丸め処理について（11 ページ）」を参照してください。

3. 運用環境におけるフローの発生頻度(1 分間の平均フロー数)を確認します。

   フローの発生頻度は、運用環境において 1 分間に平均何セッションの通信が発生しているのか をおおよその数値で求めます。

4. 以下の計算式にあてはめて、ディスク容量の目安を算出します。

   ディスク使用量の目安[MB] = ( N + 5 ) × P × L × 0.000415 + A × 0.15 + 10,000 [MB]

   - N: NFA が管理するエクスポーターの台数

     手順 1 で確認した値を代入して計算します。

   - P: NFA の保持期間に影響を受ける係数

     手順 2 で確認した値を代入して計算します。

   - L: 単位時間ごとに保持する最大フロー数

デフォルトでは、最大で上位 1,000 フローを保持するため、1,000 を指定します。

- A: NFA が受信した 1 分間の平均フロー数

  手順 3 で確認した値を代入して計算します。

## 計算例

エクスポーターの台数が 50 台 、フローデータに対する保持期間・単位時間ごとの最大フロー数がデフォルト値、1 分間の平均フロー数が 600,000 フローの場合は、以下のような計算結果になります。

- N = 50
- P = 2,970 (24 × 60 + 72 × 6 + 14 × 24 + 60 × 4 + 365 + 1095 ÷ 7)
- L = 1,000
- A = 600,000
- ディスク使用量の目安 = ( 50 + 5 ) × 2,970 × 1,000 × 0.000415 + 600,000 × 0.15 + 10,000 ≒ 163.9GB

# 第 4 章
# リリース内容

リリース内容について説明します。

## 目次

# 4.1　バージョン 1.1 でのリリース内容

NFA1.1 において、機能追加、修正した内容を説明します。

## 4.1.1　フローデータのエクスポート機能

データベースに蓄積したフローデータを CSV ファイルとして出力する `nfa_flow_export` コマンドを追加しました。

本コマンドにより、蓄積したフローデータを粒度を落とすことなく、外部ファイルとして長期保存することができます。

本コマンドを用いた主な運用例は以下になります。

- 詳細な過去のデータを外部ファイルとして長期保存する。
- コマンドを cron などから呼び出すことより、分析レポート作成の元になるデータを定期的に生成する。
- 外部の運用管理ソフトウェアから本コマンドを呼び出すことにより、インシデント発生時の通信状況や、イベントの詳細を自動で保存する。

作成した CSV ファイルは外部の表計算ソフトに取り込むことで、自由に編集・分析することができます。CSV の作成は、分析を行いたい期間を指定したり、前回コマンドを実行した続きから CSV ファイルを出力するなど、運用に合わせた柔軟な操作が可能です。

本機能はコマンドラインのため、Web ブラウザーを必要とせずに実行することができます。

## 4.1.2　フローデータ保持期間の動的変更対応

NFA では、大量のフローデータを長期間保持するために、一定の期間ごとにデータを集約し、データの粒度を変えて保持しています。NFA1.1 では、この保持期間を変更できるように機能強化を行いました。

保持期間のデフォルト値と、変更可能な保持期間の範囲は以下の通りです。

**表 4-1　フローデータの粒度と保持期間**

| データの粒度(単位時間) | デフォルトの保持期間 | 保持期間の変更可能範囲 |
|---|---|---|
| 1 分 | 24 時間 | 2～168 時間 |
| 10 分 | 72 時間 | 12～336 時間 |
| 60 分 | 14 日間 | 4～60 日間 |
| 6 時間 | 60 日間 | 14～365 日間 |
| 24 時間 | 365 日間 | 60～1095 日間 |
| 7 日 | 1095 日間 | 365～2190 日間 |

保持期間の変更は運用を停止することなく実施することが可能です。このため、運用中に監視エクスポーター数を増加したり、大量のフローデータを格納したことによりディスクの空き容量が少なくなった場合でも、保持期間を変更することで対処を行うことができます。

また、保持期間の設定は、データの粒度毎に異なる値を設定することができます。例えば、詳細なフローデータの保持期間を増加し、粒度の粗いフローデータの保持期間を短くするといった、運用の目的に合わせた設定変更を行うことができます。

### 4.1.3　しきい値監視機能の性能向上

しきい値監視機能の処理性能を向上しました。NFA1.0 では監視項目数を 150 項目以下にすることを推奨していましたが、NFA1.1 にてしきい値監視機能の処理を改善し、より多くの監視ができるようになりました。

弊社検証では、以下の環境で監視項目数 2000 が動作することを確認しています。

**表 4-2　監視項目数 2000 の動作実績環境**

| 項目 | 内容 |
|---|---|
| CPU | Intel E5-2630v3(2.40 GHz) * 8 コア |
| システムメモリ | 64GB |
| ディスク | 2.5 型 SAS (15000rpm) |
| OS | Red Hat Enterprise Linux 7.3 (x86_64) |
| フロー数 | 20000 フロー/秒 |

### 4.1.4　対応フロープロトコルの強化

NFA1.1 において、NetFlow サンプリングに対応しました。また新規フロープロトコルとして IPFIX に対応しました。

#### NetFlow サンプリング

エクスポーターが、NetFlow Lite などのサンプリングした情報を送信した場合でも、フロー情報を分析できるように強化を行いました。サンプリング率はエクスポーターごとに手動で設定することができます。受信したフロー情報にサンプリング率が含まれている場合は、自動でサンプリング率を読み込みこともできます。

#### IPFIX

対応フロープロトコルに IPFIX を追加しました。サンプリングされたフロー情報を受信した場合でも手動でサンプリング率を設定することで、適切にフローデータを分析することができます。

### 4.1.5　グラフ表示タイプの切り替え機能

アプリケーション、IP プロトコルのウィジェットについては、円グラフと折れ線グラフの両方で表示できるように強化しました。

NFA1.0 では、アプリケーション、IP プロトコルのウィジェットは円グラフとしてのみ表示できましたが、NFA1.1 からは、円グラフと折れ線グラフの両方で表示できるように機能強化を行いました。

これにより、アプリケーション観点や、IP プロトコル観点で、時系列に沿ってフローを分析することができるようになります。

円グラフと折れ線グラフの切り替えは、ダッシュボード画面やエクスポーター分析画面から、動的に行うことができます。

ダッシュボード画面においては、円グラフと折れ線グラフのどちらをデフォルトのグラフとして表示するかを定義することができます。また、ウィジェットを複数定義することにより、円グラフと折れ線グラフを並べて表示することもできます。

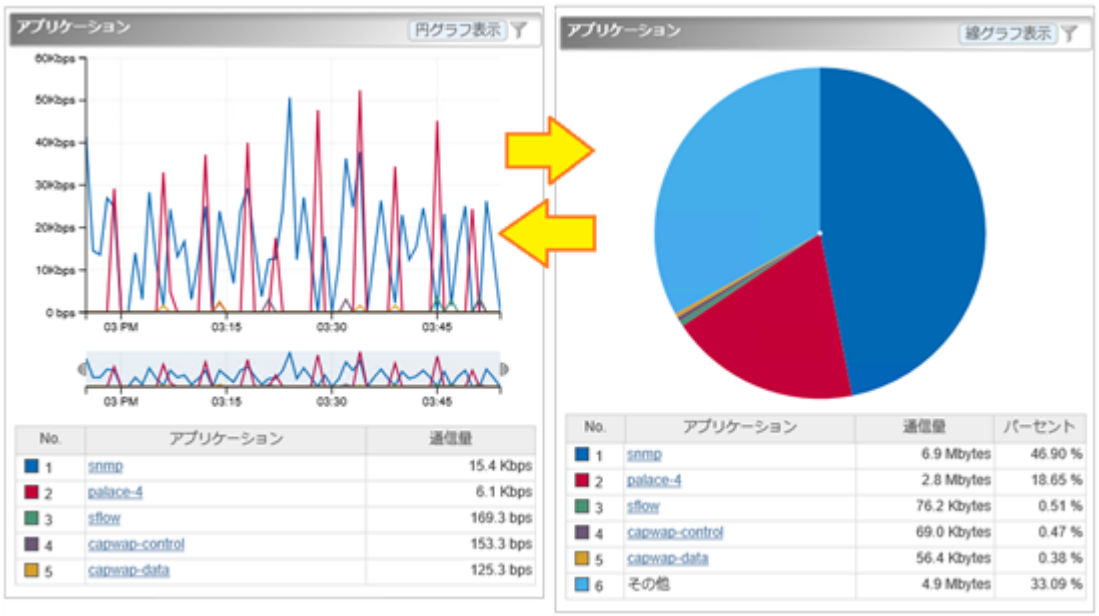



**図 4-1　円グラフ/折れ線グラフ表示タイプのウィジェット**

## 4.1.6　仕様変更

仕様が変更された内容を説明します。

### 4.1.6.1　分析結果の CSV ファイル出力内容の変更

ダッシュボード画面やエクスポーター分析画面からの CSV 出力に関する仕様を、以下のように変更しました。

#### ファイル名に関する変更点

- ダウンロードファイル名

エクスポーター分析画面での CSV 出力によるダウンロードファイル名の接頭辞を以下のように変更しました。

| 変更前 | 変更後 |
|---|---|
| ExporterAnalyzeCSV_ | ExporterAnalysisCSV_ |

- CSV ファイル名

  ダウンロードした zip ファイルに含まれる CSV ファイル名のうち、ウィジェットの名称にあたる部分を変更しました。

| 変更前 | 変更後 |
|---|---|
| ExporterTraffic | Exporters |
| InterfaceInputTraffic | InInterfaces |
| InterfaceOutputTraffic | OutInterfaces |
| srcIPAddress | SourceIPAddresses |
| dstIPAddress | DestinationIPAddresses |
| Conversation | Conversations |
| srcEndPointGroup | SourceEndpointGroups |
| dstEndPointGroup | DestinationEndpointGroups |
| srcAS | SourceAS |
| dstAS | DestinationAS |
| Application | Applications |
| IPProtocol | IPProtocols |
| CurrentAlert | CurrentAlerts |

## CSV ファイルの内容に関する変更点

- 一部の項目名を変更しました。
  - 共通

| 変更前 | 変更後 |
|---|---|
| StartTime | StartingTime |
| EndTime | EndingTime |
| Exporter | Exporters |
| Interface | Interfaces |
| FlowFilterCount | FilterCount |
| WidgetName | WidgetTitle |

  - エクスポーター分析画面から出力されるウィジェット名称

| 変更前 | 変更後 |
|---|---|
| ExporterTraffic | Exporters |
| InterfaceInputTraffic | InInterfaces |

| 変更前 | 変更後 |
|---|---|
| InterfaceOutputTraffic | OutInterfaces |
| srcIPAddress | SourceIPAddresses |
| dstIPAddress | DestinationIPAddresses |
| Conversation | Conversations |
| srcEndPointGroup | SourceEndpointGroups |
| dstEndPointGroup | DestinationEndpointGroups |
| srcAS | SourceAS |
| dstAS | DestinationAS |
| Application | Applications |
| IPProtocol | IPProtocols |
| CurrentAlert | CurrentAlerts |

- エクスポーター分析画面でフロー条件を指定した場合の項目名

| 変更前 | 変更後 |
|---|---|
| srcIPAddress | SourceIPAddress |
| dstIPAddress | DestinationIPAddress |
| srcEndPointGroup | SourceEndpointGroup |
| dstEndPointGroup | DestinationEndpointGroup |
| srcAS | SourceAS |
| dstAS | DestinationAS |

- 一部の項目の値の出力形式を変更しました。
  - 以下の項目に出力される時刻情報を UNIX 時刻形式に変更しました。
    - Date
    - StartingTime
    - EndingTime
    - <データ行中の時刻を表す値>
  - Exporters 項目について、すべてのエクスポーターを表す値を変更しました。

| 変更前 | 変更後 |
|---|---|
| (all) | (All) |

  - Exporters および Interfaces 項目について、エクスポーター名に IP アドレスを付与するよう変更しました。

| 変更前 | 変更後 |
|---|---|
| Exporter-001 | Exporter-001 (192.168.10.1) |

  - 削除されたインターフェイス、エンドポイントグループまたはアプリケーションを出力する場合の表現を変更しました。 対象ウィジェットは下記の通りです。

        * 入力インターフェイス
        * 出力インターフェイス
        * 送信元エンドポイントグループ
        * 宛先エンドポイントグループ
        * アプリケーション

| 変更前 | 変更後 |
|---|---|
| deleted | (deleted) |

    - 対象のフローデータが存在しない場合に、「No Data」を出力するように改善しました。 対象ウィジェットは下記の通りです。
        * アプリケーション
        * IP プロトコル
    - エクスポーター分析画面からの出力時の CsvType の値を変更しました。

| 変更前 | 変更後 |
|---|---|
| ExporterAnalyze | ExporterAnalysis |

- データ行の一部について、値の出力形式を変更しました。
    - 「その他」の名称を変更しました。 対象ウィジェットは下記の通りです。
        * アプリケーション
        * IP プロトコル

| 変更前 | 変更後 |
|---|---|
| (Other) | Others |

    - カレントアラートウィジェットのデータラベル名を変更しました。

| 変更前 | 変更後 |
|---|---|
| OccurredTime,Severity,Target,Detail | Severity,DetectionTime,Targets,Content |

### 4.1.7　修正項目

修正された問題の一覧を記載します。

1. 以下の OSS を、バグ修正取り込みのために更新しました。
    - Java Runtime (8u121 へ更新)
    - Apache Tomcat (8.0.39 へ更新)
    - Apache Struts2 (2.3.32 へ更新)
    - Apache Commons BeanUtils (1.9.2 へ更新)
    - Apache Commons FileUpload (1.3.2 へ更新)

- Log4j2 (2.5 へ更新)
- PostgreSQL (9.2.14 へ更新)
- SQLite3 (3.10.2 へ更新)
- ICU (58.2 へ更新)

2. UNIVERGE PF6800 Ver. 6.3 の WebGUI からの Network Flow Analyzer の画面起動が失敗する問題を修正しました。
3. エクスポーター分析画面の期間の指定において、起点の日時を現在時刻から 1 時間以内に設定し、かつ期間を「現在時刻まで」に設定した場合に、分析結果に起点の日時に指定した時刻の 1 分前のデータが含まれてしまう問題を修正しました。
4. エクスポーター分析画面の期間の指定における[**特定の日時と期間を指定**]にて、期間に「現在時刻まで」以外を選択した際に、指定された期間と、分析結果として表示される期間が異なる(指定された期間に対して、分析結果の期間が 1 つの単位時間の分だけ余分に表示される)問題を修正しました。

   単位時間についてはリファレンスガイドの「フローデータの保持期間と丸め処理について」をご参照ください。
5. エクスポーター分析画面での[**特定の日時と期間を指定**]の期間に「現在時刻まで」を指定し、表示された分析結果の画面で CSV 出力を実行した場合に、蓄積データの切り替えのタイミングによって線グラフのウィジェットのデータ粒度が画面上の粒度よりも細かくなる場合がある問題を修正しました。
6. エクスポーター分析画面の分析期間の指定において、起点の日付を現在時刻の 3 日前に指定した場合に、時刻指定ができない（プルダウンリストが選択できない）場合がある問題を修正しました。
7. 複数のエクスポーターに対して、DNS 情報取得または SNMP 情報取得が同時に実行されると、情報取得に失敗する、または、実際には情報取得が成功しているにも関わらず画面上に失敗と表示される場合がある問題を修正しました。
8. イベント一覧画面の表示処理性能を改善し、大量にイベントが登録されている場合でも、数秒で表示できるようになりました。
9. 入力側インターフェイスの識別子(IN ifIndex)の値が有効でない(0 もしくは値が含まれない)フローを受信した場合に発生する次の問題を修正しました。
   - 当該エクスポーターが sFlow エクスポーターの場合、グラフの値が 0 で表示される。
   - フローデータの集約(丸め処理)において、受信したフローを別のフローと同一とみなし集約してしまうため、グラフ表示の値が不正となる。

# 第 5 章
# 注意制限事項

NFA1.1 における注意制限事項について説明します。

## 目次

# 5.1　エクスポーター側の設定に対する注意制限事項

エクスポーター側の設定に対する注意制限事項について説明します。

## 5.1.1　SNMP ifIndex 持続性のための設定

NFA でフローを正しく分析するためには、分析対象のインターフェイスに対応する ifIndex の値が変化しないように、エクスポーター側の設定を行う必要があります。

エクスポーターを再起動すると、エクスポーターの仕様によっては、分析対象のインターフェイスに対応する ifIndex の値が変化する場合があります。この場合、NFA では、分析箇所のインターフェイスの特定が正しく行えないため、分析結果も正しく表示することができなくなります。

エクスポーターの仕様によっては、ifIndex 値を再起動後も持続するための設定が行える場合があります。運用を開始する前に、必ず、エクスポーターの ifIndex 値の持続性に関する仕様を確認し、ifIndex 値の持続性のための設定を行ってください。

以下にエクスポーター側での ifIndex 値の持続性のための設定例 (Cisco Catalyst 6500 シリーズ) を示します。

```
(config)# snmp-server ifindex persist
```

**⚠ 注意**

エクスポーターの設定を行うコマンドの仕様は、機種によって異なります。必ず、エクスポーター側の設定マニュアルを確認し、設定作業を実施してください。

## 5.1.2　NetFlow v9 利用のための設定

NFA は、NetFlow v9 について、特定のフォーマットのみをサポートしています。

NetFlow v9 を利用する場合は、エクスポーター側の設定において、以下のフィールドタイプを含むフローレコード定義の作成を行ってください。

1. 送信元 IP アドレス / 宛先 IP アドレス 注 1
2. 送信元ポート番号 / 宛先ポート番号 注 1
3. IP プロトコル 注 1
4. ToS バイト(DSCP) 注 1
5. 入力インターフェイス / 出力インターフェイス 注 2
6. フローのバイト数、パケット数 注 3

**注**

1. 個々のフィールドタイプは必須ではありませんが、特別な理由が無い限りエクスポータ側でフローレコードに含める設定を行ってください。

フローレコードに該当情報が存在しない場合は任意値(ゼロ)として扱います。 そのため、該当する widget が表示されない等の結果となり、フローを正しく分析出来ない場合があります。

2. エクスポーター側でフローレコードに含める設定を必ず行ってください。

   ライセンスを正しく付与するために必須な情報です。

3. エクスポーター側でフローレコードに含める設定を必ず行ってください。

   フローの通信量を統計分析するために必須な情報です。

---

以下にエクスポーター側でのフローレコードの設定例(Cisco Catalyst 3850 シリーズ)を示します。

```
(config)# flow record NetFlow-record
(config)# match ipv4 tos
(config)# match ipv4 protocol
(config)# match ipv4 source address
(config)# match ipv4 destination address
(config)# match transport source-port
(config)# match transport destination-port
(config)# collect interface input
(config)# collect interface output
(config)# collect counter bytes long
(config)# collect counter packets long
(config)# collect timestamp sys-uptime first
(config)# collect timestamp sys-uptime last
```

**⚠ 注意**

エクスポーターの設定を行うコマンドは、機種によって異なります。必ず、エクスポーター側の設定マニュアルを確認し、設定作業を実施してください。

---

## 5.1.3　IPv6 通信のフロー分析について

NFA 1.1 では、IPv6 通信のフローの分析に対応していません。

エクスポーター側の設定において、IPv6 通信のフローを監視対象とした場合、NFA では、そのフローデータを処理することができません。

不要な通信を避けるため、エクスポーター側の設定において、IPv6 通信のフローを監視対象としないように設定してください。

**WebSAM**
**Network Flow Analyzer 1.1**
**リリースメモ**

**NFA00RJ0110-01**

**2017 年 03 月 01 版 発行**

**日本電気株式会社**