

WebSAM
Network Flow Analyzer 1.0

リリースメモ

著作権

本書に記載する内容の著作権は、日本電気株式会社に帰属します。本書の内容の一部、または、全部を日本電気株式会社の書面による許可なくコピー、改変することを禁止しています。

本書の内容には、日本電気株式会社が開示するすべての情報を掲載していない場合、または、他の方法で開示している情報と表現が異なっている場合があります。また、本書の内容は、将来、予告なしに変更または、廃止する場合がありますので、あらかじめご承知おきください。

本書を制作するにあたり、正確さを期するために万全の注意を払っておりますが、日本電気株式会社は、本書の内容に関し、その正確性、有用性、確実性、その他のいかなる保証もいたしません。また、日本電気株式会社は、本書の技術的、もしくは、編集上の間違いや欠落について、一切の責任を負いません。

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

- NEC、NEC ロゴは、日本およびその他の国における日本電気株式会社の商標および登録商標です。
- Microsoft、Internet Explorer は、米国 Microsoft Corporation の米国およびその他の国における登録商標です。
- Linux は Linus Torvalds 氏の米国およびその他の国における登録商標です。
- Red Hat は Red Hat Software, Inc. の商標または登録商標です。
- Intel、Xeon、Intel Core は、Intel Corporation の米国ならびに他の国における商標または登録商標です。
- Cisco、IOS、Catalyst は、Cisco Systems, Inc. およびその関連会社の米国ならびに他の国における登録商標です。
- 本製品には、Visigoth Software Society (<http://www.visigoths.org/>) によって開発されたソフトウェアが含まれています。
- そのほかの会社名ならびに商標名は各社の商標または登録商標です。
- 本文中では™や® は明記していません。

はじめに


このたびは、WebSAM Network Flow Analyzer 1.0 (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。	[ダッシュボード]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。 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。 \$ rpm -q nec-nfa-controller

本製品は、既定では、以下のディレクトリにインストールします。

既定のインストール先:

/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	1
1.1 ディレクトリ構成	2
1.2 ドキュメント一覧	2
第2章 製品概要	3
2.1 製品の特長	4
2.2 機能概要	5
第3章 動作環境	9
3.1 システム構成	10
3.2 システム要件	11
3.3 フローデータの管理について	11
3.3.1 フローデータの保持期間と丸め処理について	11
3.3.2 ディスク使用量の見積もり方法	12
第4章 新規機能・強化した機能	14
4.1 本バージョンでのリリース内容	15
第5章 注意制限事項	16
5.1 エクスポート側の設定に対する注意制限事項	17
5.1.1 SNMP ifIndex 持続性のための設定	17
5.1.2 NetFlow v9 利用のための設定	17
5.1.3 IPv6 通信のフロー分析について	18
5.2 Internet Explorer 9 利用時の注意制限事項	18

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.....	2
1.2 ドキュメント一覧.....	2

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)
- conf/ (インストール関連ファイル)
- lib/ (インストール関連ファイル)
- rpm/ (インストールファイル)
- 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)

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 1.0 リリースメモ (nfa-release.pdf)	NFA 1.0 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 1.0 スタートアップ ガイド (nfa-startup.pdf)	NFA 1.0 のセットアップ方法を示したマニュアルです。
WebSAM Network Flow Analyzer 1.0 リファレンスマ ニュアル (nfa-reference.pdf)	NFA 1.0 の操作マニュアルです。
WebSAM Network Flow Analyzer 1.0 オープンソース ソフトウェアのライセンス条文 (nfa-oss-license.pdf)	NFA 1.0 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	4
2.2 機能概要	5

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、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、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 では調べることはできなかった、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。

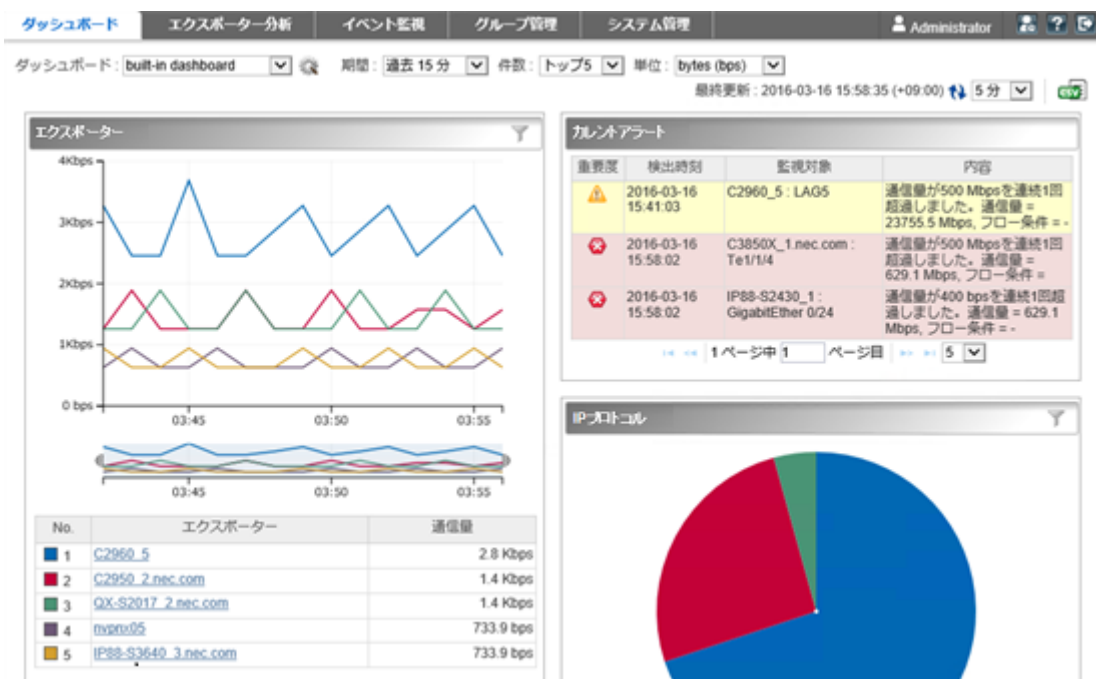


図 2-1 ダッシュボード表示

エクスポート分析

- フロー情報を送信してくるエクスポート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。

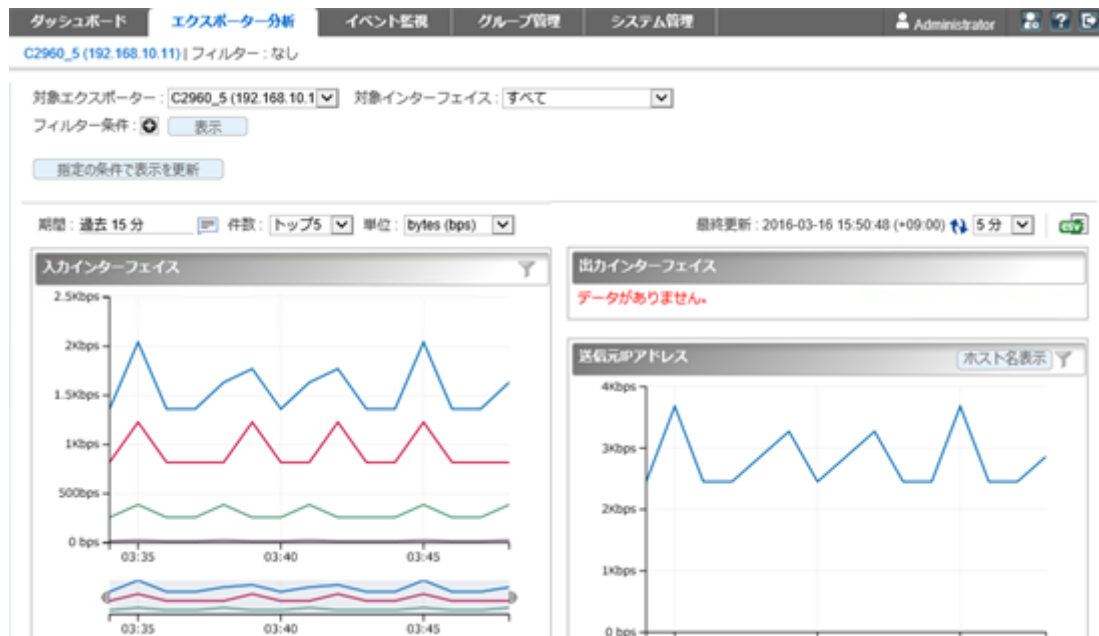


図 2-2 エクスポーター分析

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。

ダッシュボード

エクスポート分析

イベント監視

グループ管理

システム管理

Administrator

?

🔍

イベント一覧

しきい値監視エントリー一覧

イベントの一覧

最終更新: 2016-03-16 16:17:43 (+09:00)

🔄

なし

1

ページ中

1

 ページ目

100

重要度	検出時刻	監視対象	内容	監視エントリー名
異常	2016-03-16 15:58:02	C2960_2.nec.com : Fa0/1	通信量が500 Mbpsを連続5回超過しました。通信量 = 629.1 Mbps, フロー条 件 = -	HTTP通信監視
異常	2016-03-16 15:58:01	C2960_1.nec.com : Fa0/11	通信量が500 bpsを連続5回超過しました。通信量 = 1021.1 Mbps, フロー条 件 = -	HTTP通信監視
異常	2016-03-16 15:58:01	C2950_2.nec.com : LAG1	通信量が500 Mbpsを連続5回超過しました。通信量 = 1572.7 Mbps, フロー 条件 = -	HTTP通信監視
正常	2016-03-16 15:44:03	C2960_5 : LAG5	通信量のアラートが監視停止により回復されました。	支店Aの通信監視
正常	2016-03-16 15:44:03	C2960_5 : LAG3	通信量がしきい値 400 Mbpsの超過状態から回復しました。通信量 = 818.1 bps, フロー条件 = -	支店Aの通信監視
警告	2016-03-16 15:43:03	C2960_5 : LAG3	通信量が400 Mbpsを連続4回超過しました。通信量 = 1227.2 Mbps, フロー 条件 = -	支店Aの通信監視
警告	2016-03-16 15:41:03	C2960_5 : LAG5	通信量が400 Mbpsを連続4回超過しました。通信量 = 1361.1 Mbps, フロー 条件 = -	支店Bの通信監視

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。

ダッシュボード

エクスポート分析

イベント監視

グループ管理

システム設定

Administrator

?

エンドポイントグループ一覧

IFグループ一覧

エンドポイントグループの一覧

追加

エンドポイントグループ名	IPアドレス	操作
営業部	192.168.3.1/255.255.255.0	 
広報部	192.168.2.1/255.255.255.0	 
支店A	172.17.0.0/255.255.252.0	 
支店B	172.17.4.0/255.255.252.0	 
総務部	192.168.1.1/255.255.255.0	 
開発部	192.168.4.1/255.255.255.0	

図 2-4 エンドポイントグループ一覧

システム設定

- 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ト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。

ダッシュボード	エクスポート分析	イベント監視	グループ管理	システム設定	Administrator
エクスポーター管理	アプリケーション定義	ユーザー管理	ライセンス登録	環境設定	

アプリケーションの一覧 [追加](#)

アプリケーション名開始文字: [A](#)[B](#)[C](#)[D](#)[E](#)[F](#)[G](#)[H](#)[I](#)[J](#)[K](#)[L](#)[M](#)[N](#)[O](#)[P](#)[Q](#)[R](#)[S](#)[T](#)[U](#)[V](#)[W](#)[X](#)[Y](#)[Z](#) [数字](#) [特殊文字](#)

56 ページ中 1 ページ目 100













































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
lcpmux	1	TCPまたはUDP	任意	 
rtmp	1	DDP	任意	 
nbt	2	TCPまたはUDP	任意	 
compressnet	2	DDP	任意	 
rje	5	TCPまたはUDP	任意	 
zip	6	DDP	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	 
netstat	15	TCP	任意	 
qold	17	TCPまたはUDP	任意	 
misp	18	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	 
lmp	24	TCPまたはUDP	任意	 
smtp	25	TCPまたはUDP	任意	 
nsw-le	27	TCPまたはUDP	任意	 
msg-icp	29	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	10
3.2 システム要件	11
3.3 フローデータの管理について	11

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、エクスポート、エンドポイントで構成されます。

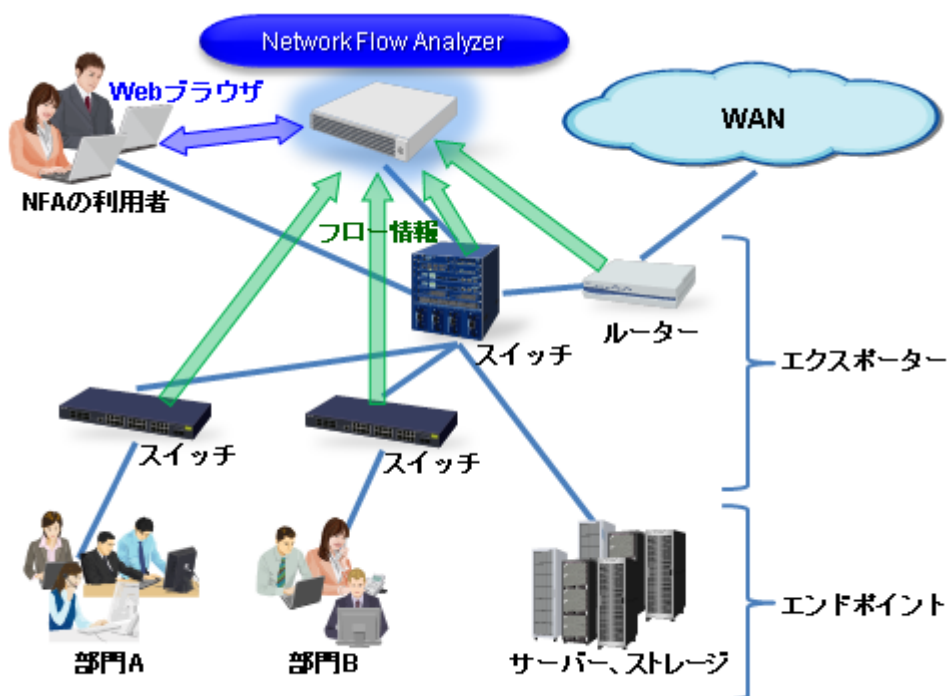


図 3-1 システム構成図

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トと呼んでいます。

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	<ul style="list-style-type: none"> Red Hat Enterprise Linux 6 (x86_64) Red Hat Enterprise Linux 7 (x86_64)
フロープロトコル	NetFlow (v5、v9)、sFlow (v4、v5)

表 3-2 Web ブラウザーの要件

項目	内容
対応ブラウザ	Windows 上で動作する以下のブラウザ <ul style="list-style-type: none"> Internet Explorer 9 以上 Mozilla Firefox 38 以上 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、一定の保存期間ごとに、データを集約(丸め処理)し、データの粒度を変えて保持しています。ここでは、フローデータの粒度に対する保持期間とその丸め処理の詳細について説明します。

NFA では、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し、データの粒度を変えて管理しています。また、NFA

では、データの粒度ごとに保持期間を規定しており、保持期間を超えたデータを破棄します。

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)	保持期間
1 分	24 時間
10 分	72 時間
60 分	14 日間
6 時間	60 日間
24 時間	1 年間
7 日	3 年間

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

ヒント

- NFA では、フローデータの蓄積に必要なディスク使用量を最小にするため、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。
- NFA では、内部処理用の集約していない生のフローデータを 24 時間保持しています。

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トの台数、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 \(11 ページ\)](#)」で示したとおり、単位時間ごとのフローデータに対する保持期間、および、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。

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ト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. 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。

3. 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。

$$\text{ディスク使用量の目安[MB]} = (N + 5) \times L \times 1.6[\text{MB}] + A \times 0.15[\text{MB}]$$

- N: NFA が管理するエクスポートの台数

手順 1 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フローデータの最大フロー数

通常は、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。

注意

- 最大フロー数を変更した場合は、変更した値を参考にして計算してください。
- エクスポート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。

- A: NFA が受信した 1 分間の平均フロー数

手順 2 で確認した値を代入して計算します。

計算例

エクスポートの台数が 50 台、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。

$$(50 + 5) \times 1,000 \times 1.6[\text{MB}] + 600,000 \times 0.15[\text{MB}] = 178\text{GB}$$

第4章

新規機能・強化した機能

NFA1.0におけるリリース内容について説明します。

目次

4.1 本バージョンでのリリース内容	15
--------------------------	----

4.1 本バージョンでのリリース内容

本バージョンは、NFA の最初のリリースになります。製品が提供する機能については、[「2.2 機能概要 \(5 ページ\)」](#)を参照してください。

第 5 章

注意制限事項

NFA1.0 における注意制限事項について説明します。

目次

5.1 エクスポート側の設定に対する注意制限事項	17
5.2 Internet Explorer 9 利用時の注意制限事項	18

5.1 エクスポート側の設定に対する注意制限事項

エクスポート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、エクスポート側の設定を行う必要があります。

エクスポートを再起動すると、エクスポートの仕様によっては、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。

エクスポートの仕様によっては、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、エクスポートの 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。

以下にエクスポート側での 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

エクスポート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、エクスポート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、エクスポート側の設定において、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ト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. エクスポート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要な情報です。
3. エクスポート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要な情報です。

以下にエクスポート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

エクスポートの設定を行うコマンドは、機種によって異なります。必ず、エクスポート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 1.0 では、IPv6 通信のフローの分析に対応していません。

エクスポート側の設定において、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、エクスポート側の設定において、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。

5.2 Internet Explorer 9 利用時の注意制限事項

Internet Explorer 9 利用時の注意制限事項について説明します。

画面の自動更新によるメモリー使用量の増加

ダッシュボード画面やエクスポーター分析画面を表示する際に、[更新間隔]を[なし]以外に設定して自動更新を有効にしていると、Internet Explorer プロセスの使用メモリーが自動更新のたびに増加する場合があります。そのため、長期間放置しておくで大量のメモリーを消費し、動作が不安定になる場合があります。

増大した使用メモリーは、別画面に移動するか、F5 キーを押して画面を更新することで解放されます。ダッシュボード画面やエクスポーター分析画面を長時間表示する場合は、数時間に 1 回程度、別の画面に移動するか、F5 キーを押して画面を更新してください。

ヒント

この問題は、Internet Explorer 10 以降では発生しません。

WebSAM
Network Flow Analyzer 1.0
リリースメモ

NFA00RJ0100-04

2016 年 06 月 04 版 発行

日本電気株式会社

© NEC Corporation 2014 - 2016