

WebSAM
Network Flow Analyzer 2.0

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。
- Google Chrome は、Google Inc. の登録商標または商標です。
- Firefox は、Mozilla Foundation の米国およびその他の国における登録商標または商標です。
- 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 2.0 (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

本書では、以下の略称を用いて記述しています。

略称表現

正式表記	略称表現
WebSAM Network Flow Analyzer	NFA
WebSAM Integrated Management Server	IMS
WebSAM NetvisorPro V	NetvisorPro

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 製品概要	1
1.1 製品の特長	2
1.2 機能概要	3
第 2 章 動作環境	7
2.1 システム構成	8
2.2 システム要件	9
2.3 フローデータの管理について	10
2.3.1 フローデータの保持期間と丸め処理について	10
2.3.2 ディスク使用量の見積もり方法	11
第 3 章 ドキュメント一覧	14
第 4 章 リリース内容	15
4.1 バージョン 2.0 でのリリース内容	16
4.1.1 IMS コンポーネントによる統合運用	16
4.1.2 DSCP によるフロー分析	16
4.1.3 バージョン 2.0 における修正項目	17
4.2 バージョン 1.1 でのリリース内容	18
4.2.1 フローデータのエクスポート機能	18
4.2.2 フローデータ保持期間の動的変更対応	18
4.2.3 しきい値監視機能の性能向上	19
4.2.4 対応フロープロトコルの強化	19
4.2.5 グラフ表示タイプの切り替え機能	19
4.2.6 バージョン 1.1 における仕様変更	20
4.2.6.1 分析結果の CSV ファイル出力内容の変更	20
4.2.7 バージョン 1.1 における修正項目	23
第 5 章 注意制限事項	25
5.1 エクスポート側の設定に対する注意制限事項	26
5.1.1 SNMP ifIndex 持続性のための設定	26
5.1.2 NetFlow v9 利用のための設定	26
5.1.3 IPv6 通信のフロー分析について	27

第 1 章

製品概要

NFA の製品概要について説明します。

目次

1.1 製品の特長	2
1.2 機能概要	3

1.1 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。

1.2 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。

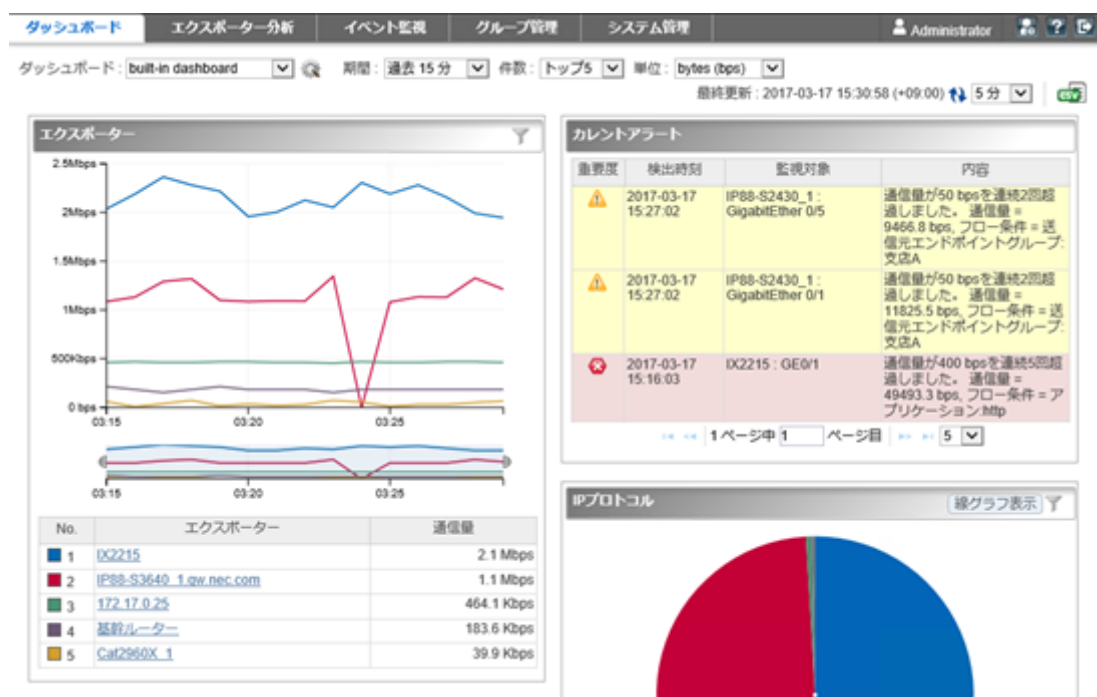


図 1-1 ダッシュボード表示

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。

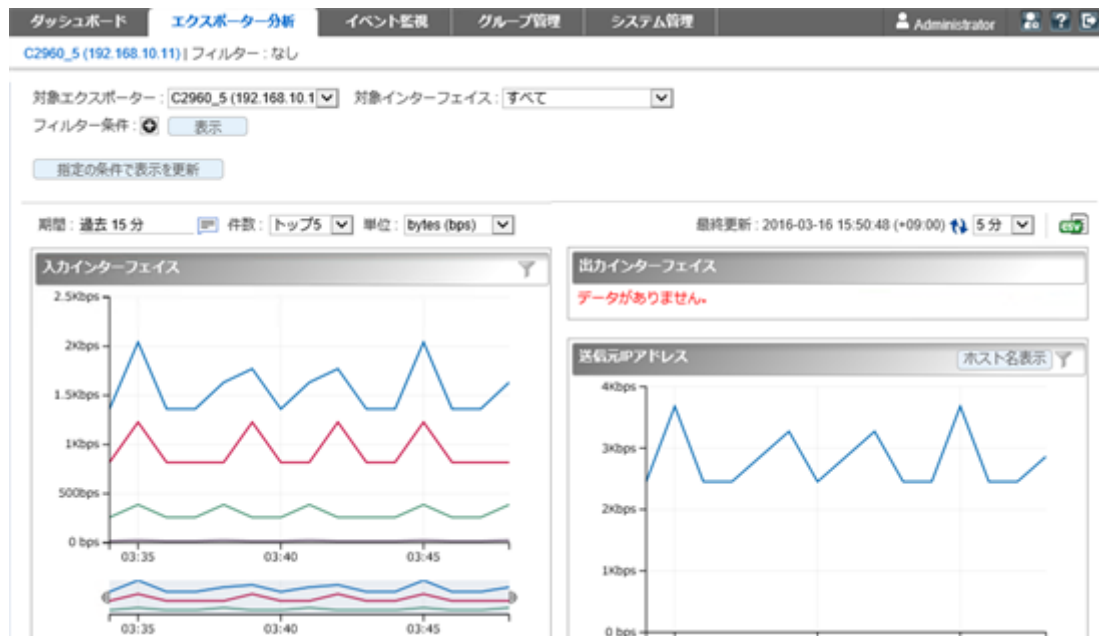


図 1-2 エクスポーター分析

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一覧

イベントの一覧

最終更新: 2017-03-17 15:19:34 (+09:00)

1分

1ページ中 1

ページ目

100

重要度	検出時刻	監視対象	内容	監視エントリ名
 正常	2017-03-17 15:17:02	IP88-S2430_1: GigabitEthernet 0/1	通信量がしきい値 50 bpsの超過状態から回復しました。通信量 = 0.0 bps, フロー条件 = 送信元エンドポイントグループ: 支店A	支店Aの通信監視
 正常	2017-03-17 15:17:02	IP88-S2430_1: GigabitEthernet 0/5	通信量がしきい値 50 bpsの超過状態から回復しました。通信量 = 0.0 bps, フロー条件 = 送信元エンドポイントグループ: 支店A	支店Aの通信監視
 異常	2017-03-17 15:16:03	IX2215: GE0/1	通信量が400 bpsを連続5回超過しました。通信量 = 49493.3 bps, フロー条件 = アプリケーション: http	HTTP通信監視
 警告	2017-03-17 15:14:02	IP88-S2430_1: GigabitEthernet 0/5	通信量が50 bpsを連続2回超過しました。通信量 = 9411.3 bps, フロー条件 = 送信元エンドポイントグループ: 支店A	支店Aの通信監視
 警告	2017-03-17 15:14:02	IP88-S2430_1: GigabitEthernet 0/1	通信量が50 bpsを連続2回超過しました。通信量 = 11980.7 bps, フロー条件 = 送信元エンドポイントグループ: 支店A	支店Aの通信監視
 正常	2017-03-17 15:11:02	IX2215: GE0/1	通信量がしきい値 400 bpsの超過状態から回復しました。通信量 = 0.0 bps, フロー条件 = アプリケーション: http	HTTP通信監視
 異常	2017-03-17 14:25:02	IX2215: GE0/1	通信量が400 bpsを連続5回超過しました。通信量 = 51200.0 bps, フロー条件 = アプリケーション: http	HTTP通信監視

図 1-3 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

システム管理

Administrator



エンドポイントグループ一覧

IP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
人事部	192.168.3.1-192.168.3.100	 
営業部	192.168.3.101-192.168.3.200	 
広報部	192.168.2.0/255.255.255.0	 
支店A	172.17.0.0/255.255.255.0	 
支店B	172.17.4.0/255.255.255.0	 
経理部	192.168.1.0/255.255.255.0	 
開発部	192.168.4.0/255.255.255.0	 

図 1-4 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。

ダッシュボード	エクスポーター分析	イベント監視	グループ管理	システム管理	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](#) [すべて](#)

59 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
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	 
rip	39	TCPまたはUDP	任意	 

図 1-5 アプリケーション定義

第2章

動作環境

NFA の動作環境について説明します。

目次

2.1 システム構成	8
2.2 システム要件	9
2.3 フローデータの管理について	10

2.1 システム構成

NFA のシステム構成について説明します。

NFA のシステム構成

NFA の運用環境は、「図 2-1 システム構成図 (8 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。

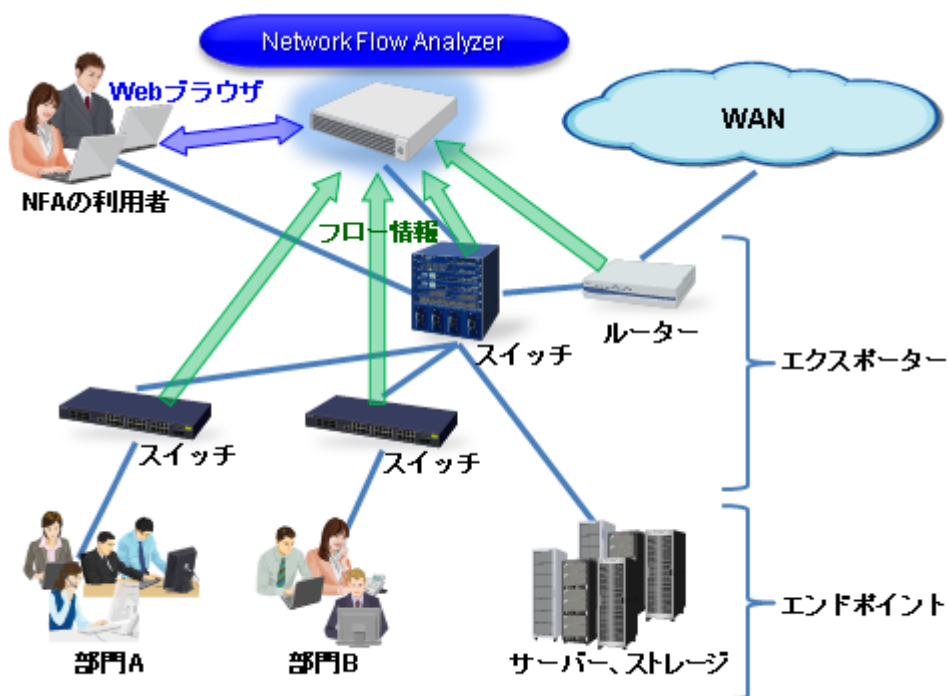


図 2-1 システム構成図

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。

IMS コンポーネント利用時のシステム構成

IMS コンポーネントを利用することで、複数配置した NFA の統合運用や、NFA と NetvisorPro との統合運用が可能になります。統合運用時のシステム構成例を「[図 2-2 統合運用時のシステム構成例 \(9 ページ\)](#)」に示します。

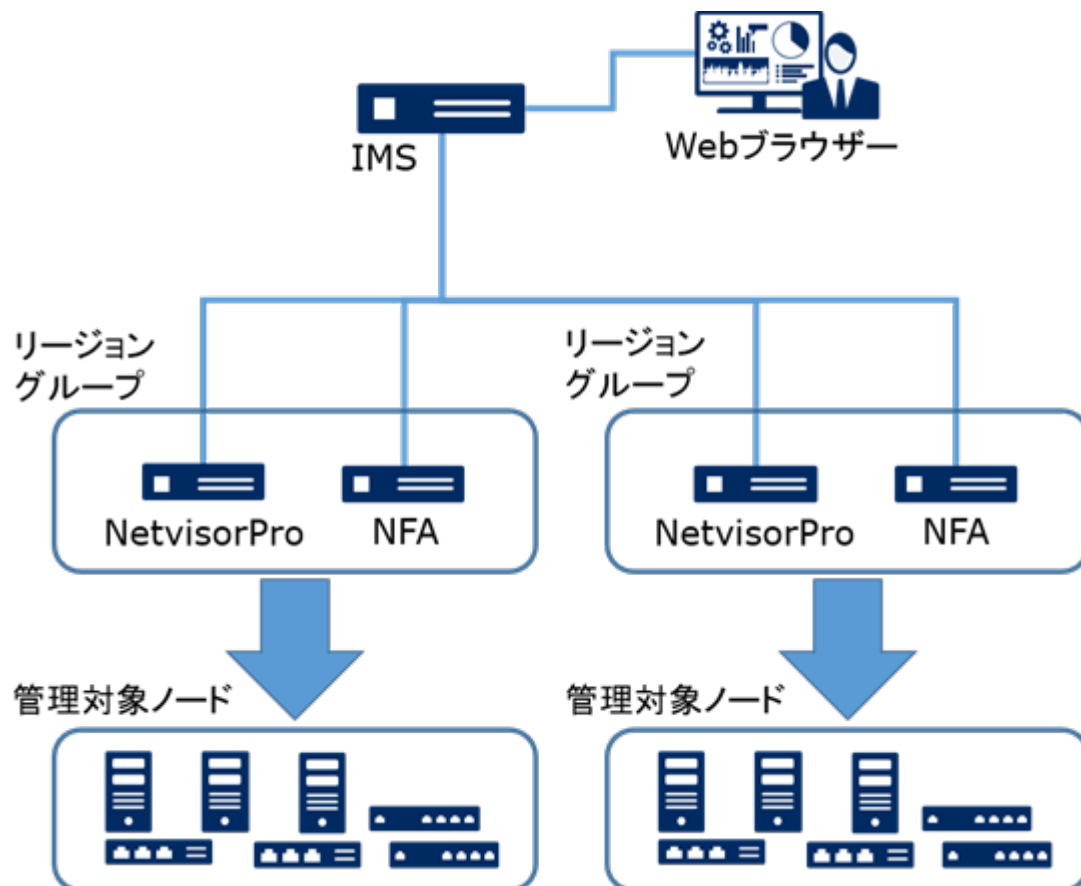


図 2-2 統合運用時のシステム構成例

「[図 2-2 統合運用時のシステム構成例 \(9 ページ\)](#)」に示すように、同一ノード(エクスポート)を管理する NFA と NetvisorPro は、リージョンというグループでグルーピングします。IMS コンポーネントの Web コンソールでは、同一リージョングループ内の各製品が管理する同一ノード(エクスポート)の情報を統合して表示します。

ヒント

NFA と IMS コンポーネントとを同じサーバーにインストールすることができます。ただし、この場合、操作に対する応答が遅いなどの問題が発生する可能性があります。十分に検証した上で、運用を開始してください。また、可能な限り、別のサーバーに分散してインストールする構成を推奨します。

2.2 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 2-1 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 注 1
OS	<ul style="list-style-type: none"> Red Hat Enterprise Linux 6 (x86_64) 注 2 Red Hat Enterprise Linux 7 (x86_64)
フロープロトコル	<ul style="list-style-type: none"> NetFlow (v5、v9) IPFIX sFlow (v4、v5) NetFlow、IPFIX はサンプリングにも対応

注

1. 製品仕様上、ハードディスクへのアクセスが頻繁に行われます。利用環境に合わせて、「SAS 15,000rpm」などのアクセス性能の高いハードディスクを利用することを推奨します。
2. バージョン 6.6 以上の OS での動作をサポートします。

表 2-2 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 11 Mozilla Firefox 60 以上 Google Chrome 71 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。

2.3 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。

2.3.1 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、受信したフローデータを以下の「表 2-3 フローデータの粒度と保持期間 (11 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 2-3 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。

2.3.2 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、「2.3.1 フローデータの保持期間と丸め処理について (10 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。

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. 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。

$$\text{保持期間係数 } P = P1 \times 60 + P2 \times 6 + P3 \times 24 + P4 \times 4 + P5 + P6 \div 7$$

- 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、「[2.3.1 フローデータの保持期間と丸め処理について \(10 ページ\)](#)」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。

$$\text{ディスク使用量の目安[MB]} = (N + 5) \times P \times L \times 0.000415 + A \times 0.15 + 10,000 \text{ [MB]}$$

- 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。
- 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

エクスポートの台数が 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。

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

第3章 ドキュメント一覧

本バージョンで提供する NFA のドキュメントについて説明します。

表 3-1 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 2.0 リリースメモ (nfa-release.pdf)	NFA 2.0 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 2.0 スタートアップ ガイド (nfa-startup.pdf)	NFA 2.0 のセットアップ方法を示したマニュアルです。 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 2.0 リファレンスマ ニュアル (nfa-reference.pdf)	NFA 2.0 の操作マニュアルです。
WebSAM Network Flow Analyzer 2.0 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 2.0 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 2.0 でのリリース内容	16
4.2 バージョン 1.1 でのリリース内容	18

4.1 バージョン 2.0 でのリリース内容

NFA2.0 において、機能追加、修正した内容を説明します。

4.1.1 IMS コンポーネントによる統合運用

WebSAM Integrated Management Server (IMS)コンポーネントを利用することで、複数配置した NFA の統合運用や、NFA と NetvisorPro との統合運用が可能になりました。

IMS コンポーネントが提供する Web コンソールを用いることで、以下の運用を行うことができます。

- 複数の NFA で運用している環境において、各 NFA のウィジェットを1つのダッシュボードに並べて配置することができます。これにより、管理対象となるネットワーク全体の状況を簡単に把握することができます。
- NetvisorPro による SNMP 監視の状況と NFA が収集したフロー情報を同時に確認することができます。これにより、ネットワーク障害の原因調査をスムーズに行うことができます。
- IMS コンポーネントが提供する Web コンソールから、NFA の Web コンソールをシングルサインオンで起動することができます。これにより、2つの Web コンソールをシームレスに操作することができます。

上記以外にも IMS コンポーネントを利用することで、NFA のしきい値監視で検知したしきい値超過のイベントを、メール送信や任意のコマンドで通報することができます。

4.1.2 DSCP によるフロー分析

NFA 2.0 では、フロー情報に含まれている DSCP の値を用いたフロー分析が行えるようになりました。

DSCP 値を用いてフロー情報を分析することで、以下のような通信状況の確認を行うことができます。

- 経路上を流れるパケットに対し、意図した QoS 設定(DSCP によるマーキング)が行われているかの確認
- QoS 設定(DSCP の設定)を行ったことによる通信状況の変化の確認
- DSCP による優先度ごとの通信量の確認

具体的に DSCP によるフロー分析が行える機能は、以下の通りです。

- ダッシュボード表示

円グラフ/折れ線グラフ表示タイプの[**DSCP**]ウィジェットが追加されました。各 DSCP 値(PHB)ごとの通信量の状況を確認することができます。

- エクスポーター分析

[DSCP]ウィジェットで、フロー情報の分析結果を確認することができます。また、フィルター条件として DSCP 値(PHB)を指定することで、特定の DSCP 値(PHB)に対する通信量や通信内容を確認することができます。

- しきい値監視

しきい値監視の対象となるフローの条件として、DSCP 値(PHB)を指定することができます。

- CSV ファイル出力

ダッシュボード画面、および、エクスポート分析画面で表示する[DSCP]ウィジェットで表示するフロー情報を他のウィジェットと同様に CSV ファイル形式で外部出力することができます。

nfa_flow_export コマンドでは、出力する CSV ファイルに対し、今まで出力していた項目に加えて、DSCP 値(PHB)が追加されています。

4.1.3 バージョン 2.0 における修正項目

バージョン 2.0 で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 (8u131 へ更新)
 - Apache Tomcat (8.5.35 へ更新)
 - Apache Struts2 (2.3.36 へ更新)
 - Apache Commons FileUpload (1.3.3 へ更新)
 - Apache Commons Collections (3.2.2 へ更新)
 - Apache Commons BeanUtils (1.9.3 へ更新)
 - Apache Commons Logging (1.2 へ更新)
2. エクスポートの表示名、エンドポイントグループ名、アプリケーション名に"その他"という名前を設定した場合に、[エクスポート]ウィジェット、[送信元/宛先エンドポイントグループ]ウィジェット、[アプリケーション]ウィジェットにおいて、名前としての"その他"に対し、リンクが設定されない問題を修正しました。
3. サービスの停止時に、nfa_collector プロセスが異常終了する場合がある問題を修正しました。
4. sFlow のエクスポートにおいて、送信側のフローに対するモニタリングを設定した場合に、当該エクスポートから取得したフロー情報に対するグラフ表示が正しく行えない場合がある問題を修正しました。
5. 受信したフローデータを蓄積するデータベースのデータサイズが肥大化する場合がある問題を修正しました。

4.2 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。

4.2.1 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。

4.2.2 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ト数を増加したり、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、運用の目的に合わせた設定変更を行うことができます。

4.2.3 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

4.2.4 対応フロープロトコルの強化

NFA1.1 において、NetFlow サンプル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 サンプルング

エクスポーターが、NetFlow Lite などのサンプル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。サンプル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ルング率が含まれている場合は、自動でサンプル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。サンプル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ル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。

4.2.5 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。

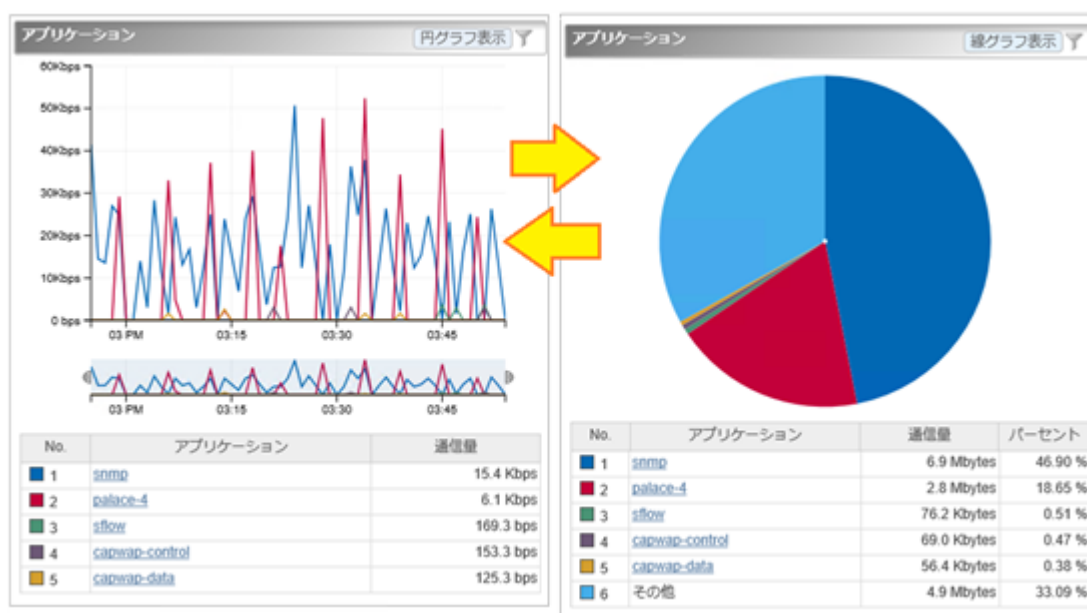


図 4-1 円グラフ/折れ線グラフ表示タイプのウィジェット

4.2.6 バージョン 1.1 における仕様変更

バージョン 1.1 で変更された仕様について説明します。

4.2.6.1 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

エクスポート分析画面での 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

- エクスポート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

- エクスポート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
- エクスポート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

4.2.7 バージョン 1.1 における修正項目

バージョン 1.1 で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. エクスポート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. エクスポート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. エクスポート分析画面での[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くなる場合がある問題を修正しました。
 6. エクスポート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. 複数のエクスポートに対して、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。
 - 当該エクスポートが sFlow エクスポートの場合、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

NFA2.0 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	26
--------------------------------	----

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須な情報です。

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須な情報です。

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 2.0 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。

WebSAM
Network Flow Analyzer 2.0
リリースメモ

NFA00RJ0200-01

2019 年 01 月 01 版 発行

日本電気株式会社

© NEC Corporation 2014 - 2019