NEC

WebSAM

Network Flow Analyzer 3.4
リファレンスマニュアル

WebSAM

NFA00MJ0340-01

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。

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、Microsoft Edge、Internet Explorer、Microsoft 365、Office 365、および、その他のマイクロソフト製品の名称は、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。
- 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 3.4 (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 の機能および操作の詳細について説明しています。NFA の持つ機能を最大限に引き出し、効果的に運用するために、本書を活用してください。

本書の構成

本書の構成は、以下の通りです。表の対象者を参考にして読み進めてください。

表　本書の構成

Admin NFA の管理者　User NFA のすべての利用者

タイトル	内容	対象者
「第 1 章　製品概要と基本操作（1 ページ）」	NFA の製品概要と Web コンソールの基本的な操作方法について説明します。	User
「第 2 章　運用前の環境設定（24 ページ）」	NFA の運用に入る前に必要となる環境設定の方法について説明します。	Admin
「第 3 章　運用時の各種設定（53 ページ）」	NFA の運用に入ってから必要に応じて行う環境設定の方法について説明します。	Admin
「第 4 章　運用操作（97 ページ）」	NFA の運用時の操作方法について説明します。	User
「第 5 章　システムメンテナンス（135 ページ）」	NFA のメンテナンス方法について説明します。	Admin
「付録 B　トラブルシューティング（190 ページ）」	NFA のトラブルシューティング方法について説明します。	Admin
「C.1　製品が利用するポート番号の一覧（195 ページ）」	NFA が利用するポート番号のデフォルト値について説明します。	Admin
用語集 (「A - Z（198 ページ）」,「あ - わ（201 ページ）」)	NFA の各種機能および本書で使用している用語、略語について説明します。	User

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。

表　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　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。 `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。

表　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
WebSAM Network Flow Analyzer Security Monitoring ライセンス	Security Monitoring ライセンス

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 製品概要と基本操作 1

1.1 製品概要 2
1.1.1 製品の特長 2
1.1.2 機能概要 3
1.1.3 システム構成 7

1.2 Web コンソールの基本操作 9
1.2.1 Web コンソールを使用するための準備を行う 10
1.2.1.1 NFA サーバーと時刻を同期する 10
1.2.1.2 Web ブラウザーのセキュリティ設定を確認する 10
1.2.1.3 Web ブラウザーに SSL サーバー証明書をインポートする 11
1.2.2 Web コンソールにアクセスする 11
1.2.3 Web コンソール構成 12
1.2.4 ウィジェットの種類 15
1.2.5 ウィジェットを操作する 18
1.2.5.1 ドリルダウン分析を行う 18
1.2.5.2 グラフの表示項目をフィルタリングする 19
1.2.5.3 折れ線グラフの表示をズームインする 20
1.2.5.4 IP アドレス表示をホスト名表示に変換する 21
1.2.5.5 グラフの種類を変更する 21
1.2.6 個人設定の内容を更新する 22

第 2 章 運用前の環境設定 24

2.1 ライセンスを管理する 25
2.1.1 ライセンスの種類 25
2.1.2 ライセンスを管理する 25
2.1.2.1 ライセンスを登録する 27
2.1.2.2 ライセンスを削除する 28

2.2 システムの環境設定を行う 28
2.2.1 エクスポーター情報の登録ポリシーを設定する 29
2.2.2 SNMP 情報取得パラメーターのデフォルト値を設定する 30
2.2.3 SNMP トラップの通知先を設定する 31

2.3 エクスポーターを管理する 36
2.3.1 エクスポーターの情報を自動で登録する 38
2.3.2 エクスポーターの情報を手動で登録する 40
2.3.2.1 エクスポーターを追加する 40
2.3.2.2 管理対象のインターフェイスを追加する 42
2.3.3 エクスポーターの情報を更新、削除する 43
2.3.3.1 エクスポーターの情報を更新する 43
2.3.3.2 管理対象のインターフェイスの情報を更新する 45
2.3.3.3 エクスポーターの情報を削除する 46
2.3.3.4 管理対象のインターフェイスの情報を削除する 46
2.3.4 インターフェイスライセンスの割り当て状況を一括で更新する 47

2.4 ユーザーを管理する 47
2.4.1 ユーザーの種類 47
2.4.2 ユーザー情報を操作する 48

2.4.2.1 ユーザーを追加する 49
2.4.2.2 ユーザー情報を更新する 51
2.4.2.3 ユーザー情報を削除する 52

第 3 章 運用時の各種設定 53

3.1 複数インターフェイスのフローを集計し分析する 54
3.1.1 IF グループについて 54
3.1.2 IF グループを操作する 55
3.1.2.1 IF グループを追加する 56
3.1.2.2 IF グループを更新する 57
3.1.2.3 IF グループを削除する 57

3.2 複数の宛先または送信元のフローを集計して分析する 58
3.2.1 エンドポイントグループについて 58
3.2.2 エンドポイントグループを操作する 58
3.2.2.1 エンドポイントグループを追加する 60
3.2.2.2 エンドポイントグループを更新する 61
3.2.2.3 エンドポイントグループを削除する 61

3.3 固有のアプリケーション通信を識別する 62
3.3.1 アプリケーション定義について 62
3.3.2 アプリケーション定義を操作する 63
3.3.2.1 アプリケーション定義を追加する 65
3.3.2.2 アプリケーション定義を更新する 69
3.3.2.3 アプリケーション定義を削除する 74
3.3.3 アプリケーション定義での少量フローの分析について 74

3.4 特定フローをしきい値で監視する 75
3.4.1 しきい値監視について 76
3.4.2 しきい値監視エントリを操作する 76
3.4.2.1 しきい値監視エントリを追加する 78
3.4.2.2 しきい値監視エントリを更新する 82
3.4.2.3 しきい値監視エントリを削除する 84

3.5 ローデータの外部出力設定を行う 85

3.6 セキュリティ観点でフローを分析・監視する 87
3.6.1 セキュリティ監視について 87
3.6.2 セキュリティ監視設定を操作する 90
3.6.2.1 セキュリティ監視設定を追加する 93
3.6.2.2 セキュリティ監視設定を更新する 95
3.6.2.3 セキュリティ監視設定を削除する 95

第 4 章 運用操作 97

4.1 現在のネットワーク状況を確認する 98
4.1.1 ダッシュボードについて 98
4.1.2 ダッシュボード表示画面を操作する 98
4.1.3 ダッシュボード定義を操作する 100
4.1.3.1 ダッシュボード定義を追加する 102
4.1.3.2 ダッシュボード定義を更新する 105
4.1.3.3 ダッシュボード定義を削除する 108

4.2 エクスポーターごとにフローの詳細を分析する 108
4.2.1 エクスポーター分析について 108

4.2.2 エクスポーター分析画面を操作する 109
4.2.3 分析の条件と表示するウィジェットについて 115
4.3 蓄積データや分析結果を外部に出力する 117
4.3.1 蓄積データをコマンドで CSV ファイルに出力する 117
4.3.2 分析結果を画面から CSV ファイルで出力する 117
4.4 ローデータを確認する 121
4.5 フローレートを確認する 124
4.6 イベント情報を確認する 126
4.6.1 しきい値超過、回復イベントの発生履歴を確認する 126
4.7 セキュリティ監視の検知結果を確認する 128
4.8 ユーザーの操作履歴を確認する 133
第 5 章 システムメンテナンス 135
5.1 システムの環境をメンテナンスする 136
5.1.1 バージョン情報を確認する 136
5.1.2 サービスを起動、停止する 137
5.1.3 製品が利用する通信ポート番号を変更する 138
5.1.4 フロー情報の記録処理方式を変更する 140
5.1.5 Microsoft 365 通信定義の自動更新を停止する 142
5.1.6 Web サーバーの URL を変更する 143
5.1.7 環境設定をバックアップ、リストアする 144
5.1.7.1 環境設定をバックアップする 146
5.1.7.2 環境設定のバックアップをリストアする 146
5.1.8 全データをバックアップ、リストアする 147
5.1.8.1 全データをバックアップする 148
5.1.8.2 全データのバックアップをリストアする 149
5.1.9 証跡ログの保持期間を変更する 150
5.2 フローデータの管理について 151
5.2.1 フローデータの保持期間と丸め処理について 151
5.2.2 ディスク使用量の見積もり方法 152
5.2.3 保持するフロー数の上限を変更する 154
5.2.4 フローの保持期間を変更する 155
5.2.5 丸め処理の基準時刻を変更する 155
付録 A コマンドリファレンス 157
A.1 nfa_ssl_keytool 157
A.2 nfa_flow_export 161
A.2.1 パラメーター設定ファイルの形式 168
A.2.2 出力 CSV ファイルの形式 171
A.2.3 使用例 174
A.3 nfa_application_conf 176
A.3.1 インポートおよびエクスポートのファイル形式 179
A.3.2 使用例 183
A.4 nfa_reload_dnssetting 184
A.5 保守ツール 185

A.5.1 nfa_diskcheck.....185
A.5.2 nfatech ログ採取コマンド.....187

付録 B トラブルシューティング.....190

B.1 Web コンソールに接続できない.....190
B.2 ダッシュボード画面のウィジェットでグラフが表示されない.....190
B.3 ダッシュボード画面のウィジェットでグラフの表示が遅延する.....191
B.4 各種設定処理に失敗する.....192
B.5 エクスポーターを削除しても、復活してしまう.....192
B.6 ウィジェットにて、ホスト名表示ができない.....193
B.7 Web コンソールのレイアウトが崩れてしまう.....194
B.8 **ページの有効期限が切れているか、不正なリクエストです**のエラーが表示される.....194

付録 C 製品が利用するシステムリソース.....195

C.1 製品が利用するポート番号の一覧.....195

付録 D 他システムとの連携設定.....196

D.1 UNIVERGE PF6800 Web GUI との連携設定.....196

用語集.....198

第 1 章
製品概要と基本操作

NFA の製品概要と Web コンソールの基本的な操作方法について説明します。

目次

1.1 製品概要 2
1.2 Web コンソールの基本操作 9

1.1　製品概要

NFA の製品概要について説明します。

1.1.1　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。

1.1.2　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。

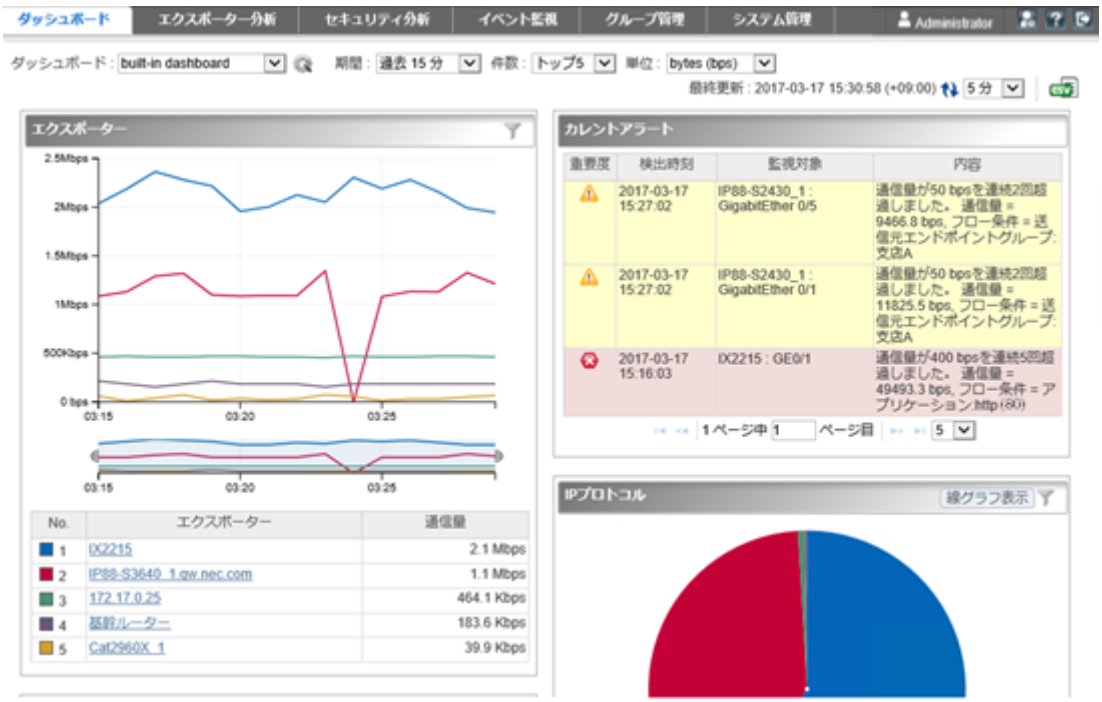

図 1-1　ダッシュボード表示

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 1-2　エクスポーター分析

セキュリティ分析

- 受信したフロー情報をセキュリティの観点で分析・監視し、DoS/DDoS やスキャンの攻撃の疑いを検知することができます。
- 検知の履歴はイベントとして確認することができ、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。
- 本機能を利用するためには Security Monitoring ライセンスが必要です。

図 1-3　インシデント履歴

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 1-4　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 1-5　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/ドメイン	種別	操作
tcpmux	1	TCPまたはUDP	任意	製品定義	
rje	5	TCPまたはUDP	任意	製品定義	
echo	7	TCPまたはUDP	任意	製品定義	
discard	9	TCPまたはUDP	任意	製品定義	
systat	11	TCPまたはUDP	任意	製品定義	
daytime	13	TCPまたはUDP	任意	製品定義	
qotd	17	TCPまたはUDP	任意	製品定義	
msp	18	TCPまたはUDP	任意	製品定義	
chargen	19	TCPまたはUDP	任意	製品定義	
ftp-data	20	TCPまたはUDP	任意	製品定義	
ftp	21	TCPまたはUDP	任意	製品定義	
ssh	22	TCPまたはUDP	任意	製品定義	
telnet	23	TCPまたはUDP	任意	製品定義	
smtp	25	TCPまたはUDP	任意	製品定義	
O365-Exchange	80, 443, 587, 143, 993, 995, 25	TCP	13.107.6.152-13.107.6.153, 13.107.18.10-13.107.18.11, 13.107.128.0-13.107.131.255, 23.103.160.0-23.103.175.255, 40.96.0.0-40.103.255.255, 40.104.0.0-40.105.255.255, 52.96.0.0-52.99.255.255, 131.253.33.215, 132.245.0.0-132.245.255.255, 150.171.32.0-150.171.35.255, 204.79.197.215, outlook.office.com, outlook.office365.com, r1.res.office365.com,...	製品定義	

図 1-6　アプリケーション定義

1.1.3　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 1-7 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、エクスポーター、エンドポイントで構成されます。

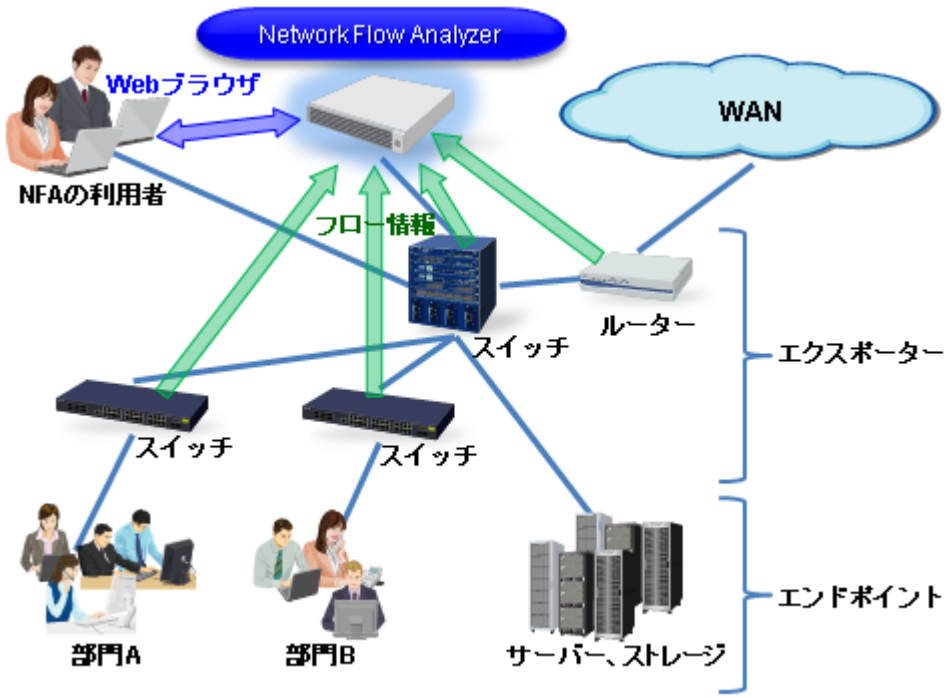

図 1-7　システム構成図

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。

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 1-8 統合運用時のシステム構成例（9 ページ）」に示します。

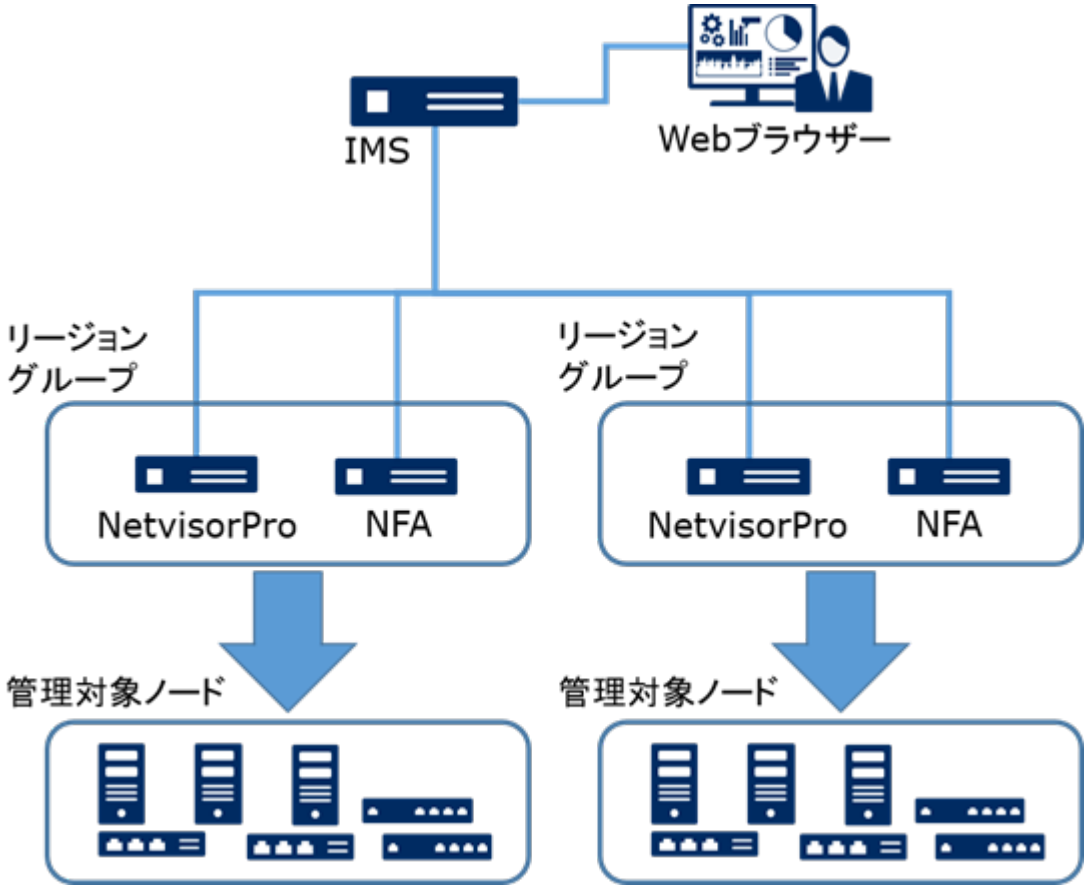

図 1-8　統合運用時のシステム構成例

「図 1-8 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(エクスポーター)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(エクスポーター)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。

1.2　Web コンソールの基本操作

NFA を操作する場合は、まず、Web ブラウザーを用いて NFA の Web コンソールに接続します。ここでは、NFA の Web コンソールに接続する方法および、Web コンソールの基本的な操作について説明します。

1.2.1　Web コンソールを使用するための準備を行う

Web ブラウザーから NFA の Web コンソールを使用するための準備作業について説明します。

Web コンソールにアクセスする前に、Web ブラウザー側の設定作業を行います。これらの作業は最初の 1 回だけ行う必要があります。

1.2.1.1　NFA サーバーと時刻を同期する

Web コンソールを操作するマシンと NFA サーバーの時刻を一致させます。

Web コンソール上の時刻と NFA サーバーの時刻が不一致だと、表示上の時刻がずれているように見える場合があります。

運用開始前に、Web コンソールを操作するマシンの時刻を、NFA サーバーに一致するように設定してください。

ヒント

NTP サービスなどを利用し、常に時刻のずれがないようにしておくことをお勧めします。

1.2.1.2　Web ブラウザーのセキュリティ設定を確認する

NFA の Web コンソールを使用するために必要な、Web ブラウザーのセキュリティ設定について説明します。

Web コンソールにアクセスするためには、Web ブラウザーで、JavaScript と Cookie が有効になっている必要があります。

サポートしている Web ブラウザーは、初期設定で JavaScript と Cookie は有効になっており、特別な設定なく使用することができます。設定を変更している場合は、NFA を使用するのに適切な設定かどうか確認してください。

また、Windows Server で[**セキュリティ強化の構成**]を「有効」にしている場合は「Windows Server での設定（11 ページ）」の設定が必須となります。

Google Chrome の設定確認

Google Chrome の設定画面で確認を行います。[**詳細設定**]以下にある、[**プライバシーとセキュリティ**]セクションで確認を行うことができます。詳細な設定手順については、Google Chrome のヘルプを参照してください。

- [**プライバシーとセキュリティ**]セクション

  JavaScript の実行が許可されていること、Cookie を保存する設定になっていることを確認します。

Windows Server での設定

[**セキュリティ強化の構成**]を「有効」にしている場合は、インターネット オプションダイアログの設定で、「信頼済みサイト」に「about:blank」を追加してください。

1.2.1.3　Web ブラウザーに SSL サーバー証明書をインポートする

NFA にアクセスするために必要な SSL サーバー証明書を、Web ブラウザーにインポートします。

使用する SSL サーバー証明書に自己署名形式を選択した場合、証明書を Web ブラウザーにインポートすることで、NFA に安全にアクセスすることができます。

ヒント

認証局に証明書を発行してもらう場合でも、認証局によっては、Web ブラウザーに認証局のルート証明書をインポートするよう、指示がある場合があります。その場合は、認証局からの指示に従ってください。

- Microsoft Edge および Google Chrome の場合は、以下の手順を実施します。
  1. 「A.1　nfa_ssl_keytool（157 ページ）」の `exportcert` コマンドで、インポート可能な証明書 (.cer ファイル) を生成します。
  2. `nfa_ssl_keytool exportcert` で作成した証明書ファイルを、Web ブラウザーが動作するマシン上でダブルクリックします。
  3. 表示された証明書ダイアログで、[**証明書のインストール**]ボタンをクリックします。

     [**証明書のインポートウィザード**]が表示されます。[**次へ**]ボタンをクリックします。
  4. [**証明書をすべて次のストアに配置する**]を選択し、[**参照**]ボタンをクリックします。
  5. 証明書ストアの選択ダイアログで、「信頼されたルート証明書機関」を選択し、[**OK**]ボタンをクリックします。
  6. [**次へ**]ボタンをクリックします。
  7. [**完了**]ボタンをクリックします。
  8. 自己署名のため、セキュリティ警告が表示されますが、[**はい**]ボタンをクリックします。

  正しくインポートされましたというダイアログが表示されれば、証明書のインポートは完了です。

1.2.2　Web コンソールにアクセスする

Web ブラウザーから NFA の Web コンソールに接続する手順について説明します。

Web コンソールにアクセスするために、以下の手順を実行します。

1. Web ブラウザーで以下の URL を指定し、Web コンソールのログイン画面を起動します。

https://<NFA サーバーのドメイン名(FQDN)>/nfa/

ホスト名 (FQDN) は、SSL サーバー証明書の作成時に入力した名前に一致している必要があります。一致していない場合、不正な証明書として警告が表示されます。

ヒント

Web コンソールにアクセスするためには、URL に指定した NFA サーバーのドメイン名(FQDN)に対して、名前解決が可能な環境である必要があります。

2. ユーザー名、パスワードを入力し、Web コンソールにログインします。

Web コンソールへのログインが成功すると、ユーザーごとに設定したダッシュボード画面を表示します。

⚠ 注意

- Web コンソールへのログイン、および、操作に関する注意事項を以下に示します。
  - 初回ログイン後に、必ず、admin ユーザーのパスワードを変更してください。

    パスワードの変更は、画面右上の[**個人設定**]ボタンから表示される個人設定画面で行います。
  - パスワード誤りを連続で 5 回検出した場合、当該ユーザーの情報はロック状態となり、当該ユーザーでのログインは、10 分間できなくなります。
  - NFA の設定情報の操作(追加、変更、削除など)を、複数の Web コンソールで同時に行うことはできません。
  - Web コンソールにログインしてから 30 分間何も操作しなかった場合は、自動でログアウトし、次の操作のタイミングでログイン画面に遷移します。

    ただし、ダッシュボード画面、エクスポーター分析画面、イベント一覧画面において、更新間隔に、1 分、5 分、15 分のいずれかを指定している場合は、自動でのログアウトは行われません。
- IMS コンポーネントの Web コンソールとのシングルサインオン動作を有効にしている場合の注意事項を以下に示します。
  - IMS コンポーネントにおいて、NFA と同一名のユーザーを登録しておく必要があります。同一名のユーザーに対してのみ、シングルサインオンが有効に動作します。
  - ログイン時において、NFA の Web コンソールに対する URL を指定していても、IMS コンポーネントの Web コンソールのログイン画面が表示されます。ログインが成功すると、自動的に、NFA の Web コンソール画面に遷移します。
  - IMS コンポーネントが停止している状態では、NFA の Web コンソールにアクセスできない場合があります。この場合は、以下の URL を指定して、NFA の Web コンソールに対するログイン画面を表示し、ログインしてください。

    https://<NFA サーバーのドメイン名(FQDN)>/nfa/login

1.2.3　Web コンソール構成

NFA の Web コンソールの構成について説明します。

NFA の Web コンソールは、「図 1-9 Web コンソールの構成（13 ページ）」で示す領域で構成されています。

図 1-9　Web コンソールの構成

タイトル領域

製品名と共に、製品ライセンスおよびコードワードの登録状況を示すメッセージを必要に応じて通知します。

メインメニュー領域

各メニュー、操作ボタンを表示します。

- メインメニュー（NFA の機能カテゴリ）
  - [**ダッシュボード**]タブ

    ダッシュボード画面の表示や設定に関する操作画面を表示します。
  - [**エクスポーター分析**]タブ

    分析対象のエクスポーターを絞り込んで、詳細な通信量の分析を行うためのエクスポーター分析画面を表示します。
  - [**セキュリティ分析**]タブ

    受信したフロー情報をセキュリティの観点で分析するための画面を表示します。
  - [**イベント監視**]タブ

    通信量に対するしきい値監視の設定や、しきい値監視によるしきい値超過、回復のイベントの発生履歴を確認するための画面を表示します。
  - [**グループ管理**]タブ

    ダッシュボード画面やエクスポーター分析画面での分析や表示で利用するエンドポイントのグルーピング、および、エクスポーターのインターフェイスのグルーピングを行うための設定画面や現在のグループ設定状況を示す一覧画面を表示します。

- [**システム管理**]タブ

  エクスポーターおよびそのインターフェイスを管理する画面や NFA にログイン可能なユーザー情報を管理する画面などシステム全体に関係する設定、管理を行うための画面を表示します。

  ヒント

  管理者権限を持つユーザーでログインした場合にのみ[**システム管理**]タブを表示します。

- ユーザー名表示
  - ログインしているユーザー名を表示します。ここでは、ユーザー設定で[**表示名**]に指定した値を表示します。ユーザーの追加操作の際に、[**表示名**]の指定を行わなかった場合は、[**ユーザー名**]の指定値を表示します。
- 操作ボタン
  - [**個人設定**]ボタン

    ログインしているユーザーの[**表示名**]や[**パスワード**]などユーザーの個人設定に関する設定変更のための画面を表示します。

    ヒント

    初回のログイン時に、パスワードの変更を行うことを推奨しています。

  - [**ヘルプ**]ボタン

    NFA のヘルプを表示します。

  - [**ログアウト**]ボタン

    Web コンソールからログアウトします。

サブメニュー領域

選択したメインメニューに関係するサブメニューがある場合に表示します。

通知領域

操作に関する情報や入力値の不正に関するエラーなどの情報を通知します。

機能操作領域

選択したメインメニュー、サブメニューに合わせた操作画面を表示します。

フッター領域

現在接続している NFA のバージョン情報やコピーライトの情報を表示します。

1.2.4　ウィジェットの種類

ダッシュボード画面およびエクスポーター分析画面では、通信状況の様々な分析結果を項目ごとのウィジェットとして表示します。ここでは、NFA がサポートするウィジェットの種類について説明します。

ウィジェットは表示する内容から大きく 3 つのタイプに分類することができます。

折れ線グラフ表示タイプ

分析結果として、指定期間における各項目の通信量の推移を折れ線グラフで表示します。また、一覧表示で、指定期間における各項目の通信量の順位を表示します。通信量の単位は、bps または、pps を選択することができます。

以下のウィジェットがこのタイプに属します。

- 通信量分析ウィジェット

表 1-1　通信量分析ウィジェット

ウィジェットの種類	説明
エクスポーター	通信量の多いエクスポーターを表示します。 エクスポーターの通信量は、そのエクスポーターが持つインターフェイスの通信量の合計値です。
入力インターフェイス	入力側の通信量の多いインターフェイスを表示します。
出力インターフェイス	出力側の通信量の多いインターフェイスを表示します。

- 送信元、宛先分析ウィジェット

表 1-2　送信元、宛先分析ウィジェット

ウィジェットの種類	説明
送信元 IP アドレス	通信量の多い送信元 IP アドレスを表示します。 ウィジェット内の表示において、送信元 IP アドレスは、ホスト名表示に切り替えることができます。
宛先 IP アドレス	通信量の多い宛先 IP アドレスを表示します。 ウィジェット内の表示において、宛先 IP アドレスは、ホスト名表示に切り替えることができます。
カンバセーション	通信量の多いカンバセーション(2 点間の通信)を表示します。 ウィジェット内の表示において、通信を行う 2 つのエンドポイントの IP アドレスは、ホスト名表示に切り替えることができます。
送信元エンドポイントグループ	通信量の多い送信元エンドポイントグループを表示します。
宛先エンドポイントグループ	通信量の多い宛先エンドポイントグループを表示します。
送信元 AS	通信量の多い送信元 AS(Autonomous System)を表示します。 AS は番号で表示します。
宛先 AS	通信量の多い宛先 AS(Autonomous System)を表示します。 AS は番号で表示します。

折れ線グラフ表示タイプのウィジェットのイメージを「図 1-10 折れ線グラフ表示タイプのウィジェット（16 ページ）」に示します。

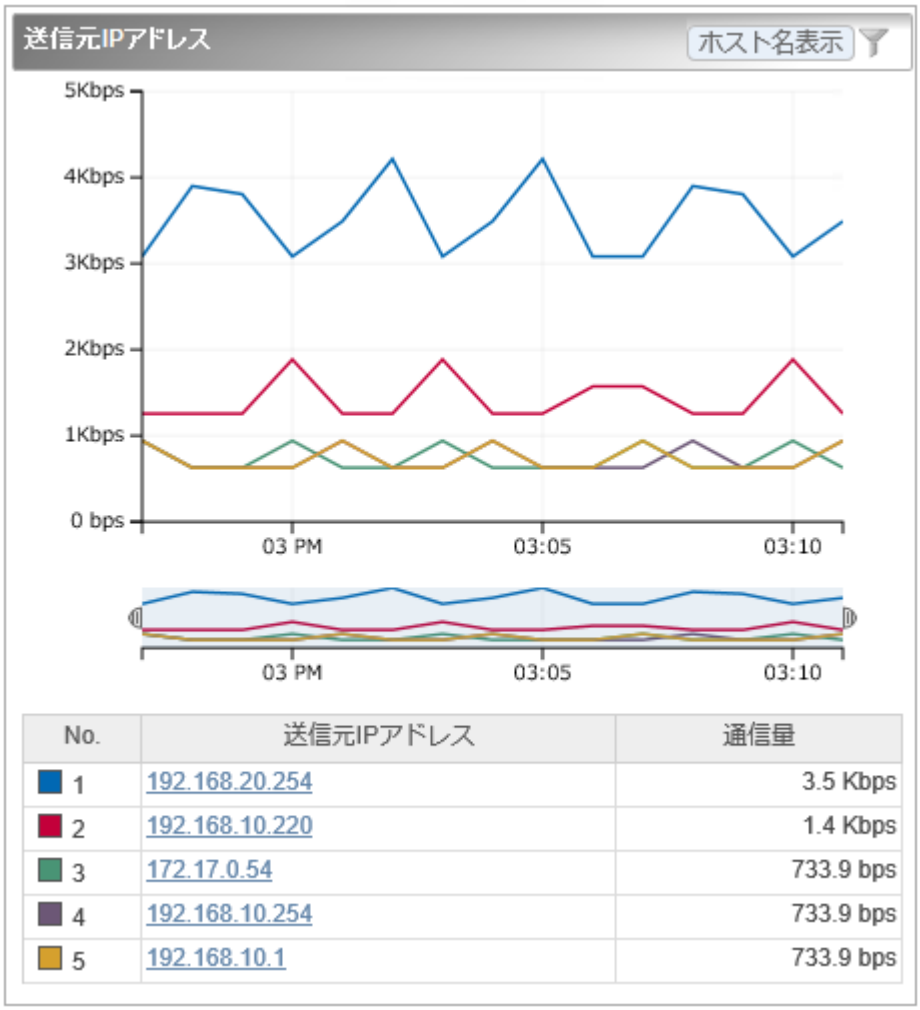

図 1-10　折れ線グラフ表示タイプのウィジェット

円グラフ/折れ線グラフ表示タイプ

分析結果を円グラフまたは折れ線グラフのどちらかで表示することができます。

- 円グラフ

  指定期間における各項目の通信量が、全体の通信量に対しどれくらいの割合を占めているのかを表示します。また、一覧表示で、指定期間における各項目の通信量の順位を表示します。通信量の単位は、bytes または、packets を選択することができます。

- 折れ線グラフ

  分析結果として、指定期間における各項目の通信量の推移を折れ線グラフで表示します。また、一覧表示で、指定期間における各項目の通信量の順位を表示します。通信量の単位は、bps または、pps を選択することができます。

以下のウィジェットがこのタイプに属します。

表 1-3　円グラフ/折れ線グラフ表示タイプのウィジェット

ウィジェットの種類	説明
アプリケーション	通信量の多いアプリケーションを表示します。
IP プロトコル	通信量の多い IP プロトコルを表示します。
DSCP	通信量の多い DSCP 値を表示します。

円グラフ/折れ線グラフ表示タイプのウィジェットのイメージを「図 1-11 円グラフ/折れ線グラフ表示タイプのウィジェット（17 ページ）」に示します。

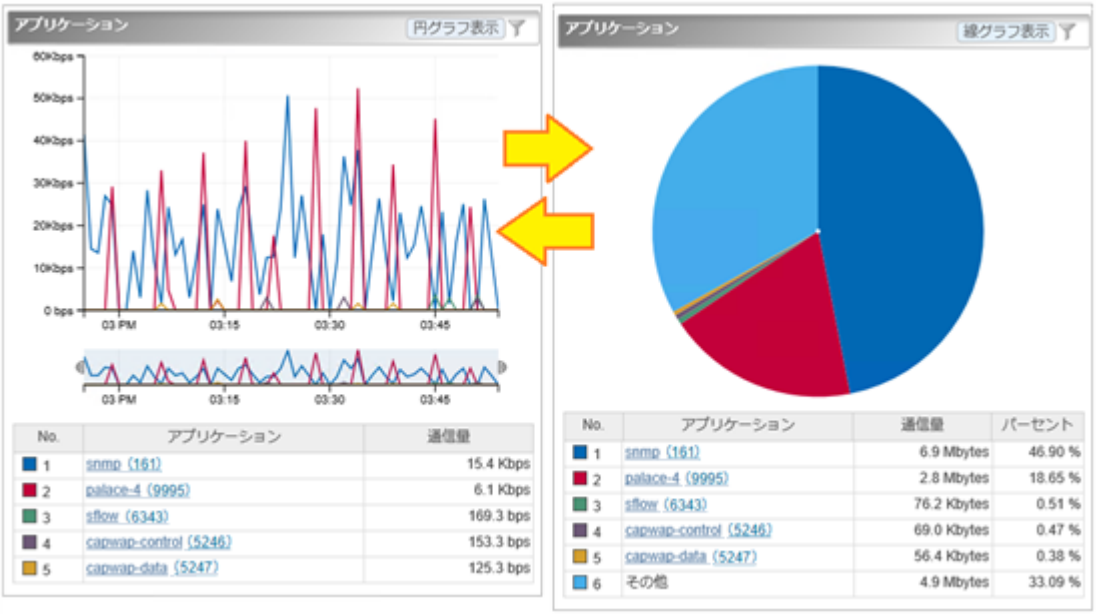

図 1-11　円グラフ/折れ線グラフ表示タイプのウィジェット

一覧表示タイプ

通信状況に関連する情報を一覧で表示します。

以下のウィジェットがこのタイプに属します。

表 1-4　一覧表示タイプのウィジェット

ウィジェットの種類	説明
カレントアラート	現在発生中のアラートイベントを表示します。

一覧表示タイプのウィジェットのイメージを「図 1-12 一覧表示タイプのウィジェット（18 ページ）」に示します。

カレントアラート

重要度	検出時刻	監視対象	内容
	2017-03-17 15:27:02	IP88-S2430_1 : GigabitEther 0/5	通信量が50 bpsを連続2回超過しました。 通信量 = 9466.8 bps, フロー条件 = 送信元エンドポイントグループ: 支店A
	2017-03-17 15:27:02	IP88-S2430_1 : GigabitEther 0/1	通信量が50 bpsを連続2回超過しました。 通信量 = 11825.5 bps, フロー条件 = 送信元エンドポイントグループ: 支店A
	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 (80)

1 ページ中 1 ページ目　5

図 1-12　一覧表示タイプのウィジェット

1.2.5　ウィジェットを操作する

折れ線グラフ表示タイプ、および、円グラフ/折れ線グラフ表示タイプのウィジェットに対しては、ドリルダウン分析や表示項目のフィルタリング表示の操作が行えます。

折れ線グラフ表示タイプ、または円グラフ/折れ線グラフ表示タイプを折れ線グラフで表示したウィジェットでは、グラフのズームイン表示が行えます。

また、エンドポイントの情報を IP アドレスで表示するウィジェットにおいては、IP アドレスのホスト名変換表示が行えます。

円グラフ/折れ線グラフ表示タイプのウィジェットに対しては、グラフを円グラフまたは折れ線グラフで表示することができます。

ヒント

[**線グラフ表示**]ボタンをクリックすると線グラフ、[**円グラフ表示**]ボタンをクリックすると円グラフに切り替わります。

1.2.5.1　ドリルダウン分析を行う

折れ線グラフ表示タイプおよび円グラフ/折れ線グラフ表示タイプのウィジェットにおいて、一覧に表示する項目のリンクをクリックし、分析条件の絞り込みを行っていくことができます。ここでは、その操作手順について説明します。

ダッシュボード画面に表示するウィジェットから詳細な分析を行っていく場合や、エクスポーター分析画面での分析結果に対し、直感的な操作でフィルター条件を追加していきたい場合に本操作を行います。

1. 対象ウィジェットの一覧表示部分で項目のリンクをクリックします。

ヒント

ダッシュボード画面の複数エクスポーターに対するウィジェットから操作した場合は、分析対象のエクスポーター、および、インターフェイスを選択するための画面を表示します。この場合は、分析対象のエクスポーター、もしくは、インターフェイスをクリックで選択します。

2. エクスポーター分析画面の[**フィルター条件**]にクリックした項目が追加されます。

分析結果が更新されたことを確認してください。

操作例

ダッシュボード画面から、「拠点接続ルーター」のインターフェイス「0/1」を流れる送信元 IP アドレス「192.168.1.100」の通信をドリルダウン分析する場合の操作例を以下に示します。

1. ダッシュボード画面の「送信元 IP アドレス」のウィジェットから、送信元 IP アドレス「192.168.1.100」のリンクをクリックします。
2. エクスポーター分析画面に遷移し、[**分析対象の候補一覧**]が表示されます。

   このとき、[**フィルター条件**]には、送信元 IP アドレス/ホスト名=「192.168.1.100」が指定され、[**分析対象の候補一覧**]には、この条件に該当するフローを監視しているエクスポーターおよびインターフェイスの名前とその通信量が表示されます。
3. [**分析対象の候補一覧**]で、「拠点接続ルーター」のインターフェイス「0/1」のリンクをクリックします。
4. エクスポーター分析画面には、以下の条件に該当するフローを分析する各種ウィジェットが表示されます。

   [対象エクスポーター]

   拠点接続ルーター

   [対象インターフェイス]

   0/1

   [フィルター条件]

   送信元 IP アドレス/ホスト名=「192.168.1.100」

1.2.5.2　グラフの表示項目をフィルタリングする

折れ線グラフ表示タイプおよび円グラフ/折れ線グラフ表示タイプのウィジェットでは、フィルタリングの機能を用いることで、現在の表示項目の一部を表示対象から除外することができます。ここでは、その操作手順について説明します。

本操作は、Top N 表示のうちの一部の項目を一時的に非表示にし、注目したい項目のみを残してグラフを見やすくしたい場合に行います。

例えば、Top 20 の表示に対し、10 位から 20 位の項目を比較したい場合に、1 位から 9 位までの項目を除外してグラフを見やすくします。

1. 対象ウィジェットの [**フィルター指定**]ボタンをクリックします。
2. 分析対象フィルタリングダイアログで、分析対象項目のチェックボックスをオフにし、分析対象から外します。
3. [**OK**]ボタンをクリックし、フィルター指定を反映します。

ウィジェットの表示内容が変化します。

- 折れ線グラフ表示タイプのウィジェットの場合

  分析対象の項目のみに変化します。

- 円グラフ/折れ線グラフ表示タイプのウィジェットの場合

  分析対象の項目の合計の通信量に対する割合の表示に変化します。

1.2.5.3　折れ線グラフの表示をズームインする

折れ線グラフ表示タイプのウィジェットにおいて、指定期間の全体を示す折れ線グラフの時間幅を狭めることで、グラフを拡大表示することができます。ここでは、その操作手順について説明します。

本操作は、全体の表示設定で指定したグラフの表示期間の範囲で、更に時間幅を指定して、グラフを拡大表示します。通信状況の詳細を拡大して細かく確認していきたい場合に本操作を行います。

1. 下側の全体を表示する折れ線グラフ(レンジセレクターと呼ぶ)を選択します。
2. レンジセレクターの左右のカーソルをドラッグ&ドロップで移動し、時間幅を調節します。

   表示位置をさらに調整する場合は以下の操作を行います。

   - レンジセレクターの左右のカーソルをドラッグ&ドロップで移動し、時間幅を調整します。
   - レンジセレクターの指定エリアをドラッグ&ドロップし、時間幅自体を移動させます。
   - レンジセレクターの指定エリア外をクリックして時間指定を解除し、新しく時間幅をドラッグ&ドロップで指定します。

   ヒント

   - 時間指定の解除時は、レンジセレクターの左右のカーソルが非表示になります。レンジセレクター内で、ドラッグ&ドロップの操作で時間幅の指定を行うと、再び、カーソルが表示されます。

- 時間指定を解除せずに、単に時間外のエリアをドラッグして、時間幅を指定することもできます。

上側の折れ線グラフの表示を指定した範囲で拡大表示されます。また、一覧に表示する通信量、およびその順位についても指定した範囲に対する情報で表示します。

1.2.5.4　IP アドレス表示をホスト名表示に変換する

エンドポイントの情報を IP アドレスで表示するウィジェットにおいて、表示するエンドポイントの IP アドレスをホスト名に変換し表示することができます。ここでは、その操作手順について説明します。

エンドポイントを示す IP アドレスをホスト名に変換するためには、エンドポイントのホスト名と IP アドレスを管理する DNS(Domain Name System)に対し、NFA がネットワークを介してホスト名を問い合わせできる環境である必要があります。

ヒント

- DNS に登録されていないエンドポイントについては、ホスト名の問い合わせが行えないため、本操作を行っても IP アドレス表示のままになります。
- 本操作で変換されるホスト名は、本操作を実施した時点でのホスト名ではなく、分析対象のフロー情報を受信した時点に DNS から取得したホスト名です。そのため、過去の通信状況を分析する場合に、当時と現在のホスト名が異なっている場合は、当時のホスト名で表示します。

本操作を実施することで、通信のエンドポイントの状況把握が行いやすくなります。

1. 対象ウィジェットの[**ホスト名表示**]ボタンをクリックします。
2. エンドポイントを示す IP アドレスがホスト名に変化します。

   当該ウィジェットの一覧表示部分を確認してください。

元の IP アドレス表示に戻す場合は、[**IP アドレス表示**]ボタンをクリックします。

1.2.5.5　グラフの種類を変更する

円グラフ/折れ線グラフ表示タイプにおいては、円グラフを折れ線グラフ、または折れ線グラフを円グラフに変更することができます。ここではその操作手順について説明します。

本操作を実施することで、1 つの画面で、特定のプロトコル観点で時系列に沿ってフローを分析したり、指定した期間のフローの割合を分析することができます。

ヒント

グラフ表示タイプを変更できるウィジェットの種類は、以下の 3 つです。

- [**アプリケーション**]ウィジェット
- [**IP プロトコル**]ウィジェット
- [**DSCP**]ウィジェット

1. 対象ウィジェットの[**折れ線グラフ表示**]ボタンまたは[**円グラフ表示**]ボタンをクリックします。
2. 対象ウィジェット内のグラフが[**円グラフ表示**]または[**折れ線グラフ**]に変更されます。

⚠ 注意

ここで行った変更は、別の画面に移動するか、F5 キーを押して画面を更新することによりデフォルトのグラフに変更されます。

デフォルトのグラフの種類を変更する方法については、「4.1.3.2　ダッシュボード定義を更新する（105 ページ）」を参照してください。

1.2.6　個人設定の内容を更新する

NFA の Web コンソールにログインしたユーザーが自身のログインパスワードを含むユーザー情報を更新する際の手順について説明します。

ヒント

[**ユーザー名**]、および、[**アクセスレベル**]については、変更することができません。

1. 個人設定画面を表示します。

   メインメニュー領域の[**個人設定**]ボタンをクリックします。
2. 表示された個人設定画面で内容を変更します。
   - [**表示名**]

     画面上の表示用のユーザーの名前を指定します。最大文字数は 32 文字です。

     以下に示す文字は指定することができません。

     - 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
     - 先頭および末尾への半角スペース

     省略した場合は、[**ユーザー名**]で指定した名前を表示名としても使用します。
   - [**デフォルトのダッシュボード**]

     ログインした時に、最初に表示するダッシュボード定義の名前を選択します。
   - [**パスワード変更**]

     チェックボックスをオンにし、[**旧パスワード**]欄に現在のパスワードを指定します。

     [**新パスワード**]欄、および、[**パスワード再入力**]欄には、新しいパスワードを指定します。

     パスワードは、以下の文字を組み合わせて、8~64 文字の文字数で指定します。

     - 半角英大文字
     - 半角英小文字

- 半角数字
- 半角スペース と 以下の記号

  ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

パスワードには、上記の 4 種類の文字のうち、3 種類以上の文字を含んでいる必要があります。また、過去 10 回分のパスワードとは異なっている必要があります。

3. 変更内容を確認し、[**OK**]ボタンをクリックします。

第 2 章
運用前の環境設定

NFA の運用に入る前に必要となる環境設定の方法について説明します。

目次

2.1 ライセンスを管理する 25
2.2 システムの環境設定を行う 28
2.3 エクスポーターを管理する 36
2.4 ユーザーを管理する 47

2.1　ライセンスを管理する

NFA のライセンスについて説明します。

2.1.1　ライセンスの種類

NFA のライセンスの考え方について説明します。

製品ライセンス

製品ライセンスとは、NFA 製品を有効にするためのライセンスのことを指します。

NFA のインストール直後は機能制限のあるトライアル版として動作します。トライアル版では、管理対象として、エクスポーターの 2 つのインターフェイスしか登録できません。製品ライセンスを登録すると機能制限が解除され、ライセンス内容に応じた製品機能が利用できるようになります。

インターフェイスライセンス

インターフェイスライセンスとは、フロー情報の受信可否を判断するための、管理対象のエクスポーターのインターフェイスに割り当てるライセンスのことを指します。インターフェイスに割り当てることができるインターフェイスライセンスの数は、登録した製品ライセンスの内容により、最大数が決まります。

Security Monitoring ライセンス

Security Monitoring ライセンスとは、セキュリティ分析機能を利用するための監視設定に対して割り当てるライセンスのことを指します。割り当てることができる Security Monitoring ライセンスの数は、登録したライセンスの内容により、最大数が決まります。例えば、"WebSAM Network Flow Analyzer Security Monitoring (5 監視ライセンス版)"を登録した場合は、5 つのセキュリティ監視設定を行うことができます。セキュリティ監視設定の詳細については、「3.6.1　セキュリティ監視について（87 ページ）」を参照してください。

2.1.2　ライセンスを管理する

ライセンスを管理するためのライセンス登録画面について説明します。

ライセンス登録画面

登録済みのライセンスキーの情報確認、および、ライセンスの登録操作を行います。

ライセンス登録画面は、[**システム管理**] >[**ライセンス登録**] をクリックして表示します。

図 2-1　ライセンス登録画面

機能操作領域

- [**ライセンス追加**]ボタン

  ライセンスキーを登録します。本ボタンをクリックすると、ライセンスの追加画面が表示されます。

ライセンスキーの一覧

- [**番号**]

  登録したライセンスキーを管理する番号です。

- [**製品型番**]

  ライセンスキーの登録時に入力したライセンスキーに対する製品型番を表示します。

- [**ライセンスキー**]

  登録したライセンスキーの値を表示します。

- [**状態**]

  ライセンスの登録状態を表示します。

  [**コードワード未登録**]が表示されている場合は、[**有効期限**]の日付に達するまでにコードワードの登録を行ってください。有効期限を過ぎた場合は、ライセンスキーが無効になり、製品が利用できなくなります。

- [**有効期限**]

  登録されているライセンスキー定義に対する有効期限の情報を表示します。

- [**操作**]

  登録されているライセンスキーに対する操作ボタンを表示します。

  - [**コードワード登録**]ボタン

    コードワードの登録画面を表示します。表示された画面でライセンスキーに対するコードワードの登録を行うことができます。

⚠ 注意

[**状態**]欄が[**コードワード登録済み**]の場合、本ボタンは無効な状態で表示されます。

- [**詳細**]ボタン

  ライセンスキーの詳細画面を表示します。表示された画面でライセンスキーに関する詳細情報を確認することができます。

- [**削除**]ボタン

  登録したライセンス情報を削除します。

ライセンスの一覧

ライセンスキーの一覧で登録したライセンスキーについて、下記の情報を表示します。

- [**ライセンス名称**]

  有効になったライセンス名を表示します。

- [**数量**]

  有効になったライセンスの数量を表示します。

- [**ライセンスキー番号**]

  ライセンスキーの一覧の[**番号**]に対応するライセンスキーの番号を表示します。

2.1.2.1　ライセンスを登録する

ライセンスを有効にする手順について説明します。

事前に、登録するライセンスキーが記載されたコードワード申請用紙を手元に準備しておいてください。

ライセンスの登録は、以下の 3 つの手順で行います。

1. ライセンスキーの登録
2. コードワード発行窓口へのコードワードの発行依頼
3. コードワードの登録

この 3 つの手順に対する詳細な操作手順について説明します。

1. ライセンスキーを登録します。
   a. ライセンス登録画面を表示します。

      [**システム管理**] >[**ライセンス登録**] をクリックします。

   b. [**ライセンス追加**]ボタンをクリックします。

      ライセンスの追加画面が表示されます。

   c. コードワード申請用紙に記載された製品型番、ライセンスキーを入力します。

d. 入力内容を確認し、[**登録**]ボタンをクリックします。

登録処理が正常に完了すると、ライセンスの追加画面の[**コードワード申請コード**]欄にコードワード申請コードが表示されます。

2. コードワードの発行申請を行います。

表示されたコードワード申請コードを使用して、コードワード発行申請を行います。申請方法の詳細は、コードワード申請用紙に記載されています。

ヒント

コードワード申請コードは、ライセンス登録画面で対象ライセンスキーの[**詳細**]ボタンをクリックすることで、再度表示できます。

コードワードは、申請から数日以内に送付されます。

3. コードワードを登録します。

a. ライセンス登録画面で、対象ライセンスキーの[**コードワード登録**]ボタンをクリックします。

コードワードの登録画面が表示されます。

b. [**コードワード**]欄に入手したコードワードを入力します。

c. 入力内容を確認し、[**登録**]ボタンをクリックします。

登録処理が正常に完了するとライセンス登録画面に戻ります。ライセンスキーの一覧の当該ライセンスキーの[**状態**]の表示が、[**コードワード登録済み**]に変わったことを確認してください。

2.1.2.2　ライセンスを削除する

登録済みのライセンスを削除する操作について説明します。

誤ってライセンスキーを登録してしまった場合や、登録済みのライセンスキーを別システムに移行する場合に、ライセンスの削除操作を行います。

1. ライセンス登録画面を表示します。

[**システム管理**] >[**ライセンス登録**] をクリックします。

2. ライセンスキーの一覧で、対象ライセンスキーの[**削除**]ボタンをクリックします。

3. 表示された削除確認ダイアログで内容を確認します。

4. [**OK**]ボタンをクリックし、削除を実行します。

2.2　システムの環境設定を行う

管理対象のエクスポーター情報 (エクスポーター、およびそのインターフェイスの情報) を NFA に登録する前に行っておくべき、環境設定について説明します。

NFA の運用を開始する前に、管理対象のエクスポーター情報の登録に関する以下の環境設定を行います。

- エクスポーター情報の登録ポリシーの設定

  管理対象となるエクスポーター情報を NFA に登録するポリシーとして、以下の 2 つがあります。

  - フロー情報の受信契機による自動登録

    受信したフロー情報から、エクスポーター、および、インターフェイスに関する情報を取得し、管理対象として NFA に自動登録します。このとき、インターフェイスライセンスの割り当て処理も自動で行います。

  - 手動登録

    管理対象となるエクスポーター、および、インターフェイスの情報登録やインターフェイスライセンスの割り当てをすべて手動で行います。

  自動登録が選択されている場合でも、エクスポーターの手動登録はいつでも自由に行うことができます。

  ヒント

  デフォルト設定では、フロー情報の受信契機による自動登録が有効になっています。

- SNMP 情報取得パラメーターのデフォルト値の設定

  NFA では、管理対象のエクスポーターのホスト名やインターフェイスの情報をエクスポーターの MIB から SNMP を用いて取得します。

  SNMP 情報取得パラメーターのデフォルト値を設定しておくと、個々のエクスポーターに対するパラメーター設定が不要になります。また、フロー情報の受信契機による自動登録の処理において、このパラメーターを用いて SNMP 情報の自動取得が行えるようになります。

2.2.1　エクスポーター情報の登録ポリシーを設定する

管理対象のエクスポーター情報(エクスポーター、およびそのインターフェイスの情報)の登録ポリシーの設定方法について説明します。

本操作では、フロー情報の受信時に、エクスポーター情報を自動登録するのか、しないのかの登録ポリシーを設定します。

ヒント

- デフォルト設定では、エクスポーター情報を自動登録する設定になっています。
- エクスポーター情報を自動登録する設定を行った場合は、エクスポーター情報の自動登録時に、インターフェイスライセンスの割り当ても自動で行います。

1. 環境設定画面を表示します。

[**システム管理**] >[**環境設定**] をクリックします。

2. 以下のいずれかを選択します。
   - [**フロー受信を契機に自動で登録する**]
   - [**手動で登録する**]
3. 設定内容を確認し、[**保存**]ボタンをクリックします。

2.2.2　SNMP 情報取得パラメーターのデフォルト値を設定する

エクスポーター、および、インターフェイスにおける SNMP 情報取得を行う場合に必要な、SNMP パラメーターのデフォルト値の設定方法について説明します。

NFA では、エクスポーター情報を登録する場合に、SNMP を用いてエクスポーターの MIB から、ホスト名(sysName)やインターフェイス名(ifName)などの情報を取得します。

本設定を行うことで、エクスポーターごとに SNMP パラメーターの設定を行う作業が不要になります。また、フロー情報の受信契機によるエクスポーター情報の自動登録時に、SNMP 情報取得も合わせて自動で行うことができます。

本操作を実施する前に、運用環境のエクスポーターに設定している SNMP パラメーターの値を確認しておいてください。

ヒント

運用環境に配置するエクスポーター側の SNMP パラメーター(SNMP バージョン、ポート番号、SNMP コミュニティ名)の値については、運用環境で統一した値で設定しておくことを推奨します。

1. 環境設定画面を表示します。

   [**システム管理**] >[**環境設定**] をクリックします。
2. [**エクスポーター情報取得パラメーター**]の各入力欄に対し、エクスポーター側の設定と同じ値を指定します。
   - [**SNMP バージョン**]

     プルダウンメニュー([**1**] / [**2c**])から選択します。デフォルト値は[**2c**]です。
   - [**ポート番号**]

     0～65535 の範囲で半角数字を指定します。デフォルト値は「161」です。SNMP のポート番号は、一般的には、「161」 を利用します。
   - [**SNMP コミュニティ名**]

     最大文字数は 255 文字で、以下の文字を指定することができます。デフォルト値は「public」です。
     - 半角英数字
     - 半角スペース

- 以下の記号

  ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

3. 設定内容を確認し、[**保存**]ボタンをクリックします。

2.2.3　SNMP トラップの通知先を設定する

監視機能によって発生したイベントの内容を SNMP トラップで別の運用管理システム(SNMP マネージャー)に送信することができます。ここでは、SNMP トラップの通知を行う場合に必要な通知先情報の設定手順について説明します。

指定した通知先に、イベント情報を SNMP トラップで送信することができます。本機能は、しきい値監視機能、または、セキュリティ監視機能において、SNMP トラップによりイベントを通知する設定を行った場合に動作します。

しきい値監視機能の操作については、「3.4.2.1　しきい値監視エントリを追加する（78 ページ）」、「3.4.2.2　しきい値監視エントリを更新する（82 ページ）」を参照してください。

セキュリティ監視機能の操作については、「3.6.2.1　セキュリティ監視設定を追加する（93 ページ）」、「3.6.2.2　セキュリティ監視設定を更新する（95 ページ）」を参照してください。

1. 環境設定画面を表示します。

   [**システム管理**] >[**環境設定**] をクリックします。

2. [**SNMP トラップ通知の設定**]の各入力欄に対し、適切な値を指定します。

   ここで指定した送信先に、トラップが送信されます。

   - [**SNMP バージョン**]

     送信する SNMP トラップに対する SNMP バージョンをプルダウンメニュー([**1**] / [**2c**])から選択します。デフォルト値は[**2c**]です。

   - [**SNMP コミュニティ名**]

     SNMP トラップに対する SNMP コミュニティ名を指定します。最大文字数は 255 文字で、以下の文字を指定することができます。デフォルト値は「public」です。

     - 半角英数字
     - 半角スペース
     - 以下の記号

       ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

   - [**宛先ポート番号**]

     宛先となるポート番号を指定します。0～65535 の範囲で半角数字を指定します。デフォルト値は「162」です。

   - [**宛先 IP アドレス**]

     SNMP トラップの宛先となる IPv4 アドレスを指定します。

3. 設定内容を確認し、[**保存**]ボタンをクリックします。

NFA が送信する SNMP トラップの内容は以下の通りです。NFA の SNMP トラップを受信する SNMP マネージャー側の仕様に従い、SNMP マネージャー側での受信設定を行ってください。

- しきい値監視機能
  - nfaTrafficThreshExceeded

    通信量のしきい値超過を示します。

Enterprise :	.1.3.6.1.4.1.119.2.3.239.2	
Generic Trap :	6	
Specific Trap :	1	
Variable Bindings :	nfaEventOccurTime :	イベントの発生日時
	nfaEventOccurExpAddr :	エクスポーターの IP アドレス
	nfaEventOccurExpIfIndex :	エクスポーターの ifIndex
	nfaEventOccurExpName :	エクスポーターの名前
	nfaEventOccurExpIfName :	エクスポーターのインターフェイスの名前
	nfaEventOccurEntryName :	監視エントリの名前
	nfaEventLevel :	重要度
	nfaThreshFlowConditions :	監視対象のフロー条件
	nfaThreshConfData :	しきい値
	nfaThreshConfTimes :	連続発生回数の設定値
	nfaThreshConfUnit :	しきい値と実測値の単位
	nfaThreshMeasuredData :	実測値
	nfaThreshFlowDirection :	通信の方向

  - nfaTrafficThreshCleared

    通信量のしきい値超過状態から回復したことを示します。

Enterprise :	.1.3.6.1.4.1.119.2.3.239.2	
Generic Trap :	6	
Specific Trap :	2	
Variable Bindings :	nfaEventOccurTime :	イベントの発生日時
	nfaEventOccurExpAddr :	エクスポーターの IP アドレス
	nfaEventOccurExpIfIndex :	エクスポーターの ifIndex
	nfaEventOccurExpName :	エクスポーターの名前
	nfaEventOccurExpIfName :	エクスポーターのインターフェイスの名前
	nfaEventOccurEntryName :	監視エントリの名前
	nfaEventLevel :	重要度(information(1)を通知)
	nfaThreshFlowConditions :	監視対象のフロー条件
	nfaThreshConfData :	しきい値

	nfaThreshConfUnit :	しきい値と実測値の単位
	nfaThreshMeasuredData :	実測値
	nfaThreshFlowDirection :	通信の方向

- nfaThreshStopped

  しきい値監視エントリの監視停止操作により、しきい値超過状態から回復したことを示します。

Enterprise :	.1.3.6.1.4.1.119.2.3.239.2	
Generic Trap :	6	
Specific Trap :	5	
Variable Bindings :	nfaEventOccurTime :	イベントの発生日時
	nfaEventOccurExpAddr :	エクスポーターの IP アドレス
	nfaEventOccurExpIfIndex :	エクスポーターの ifIndex
	nfaEventOccurExpName :	エクスポーターの名前
	nfaEventOccurExpIfName :	エクスポーターのインターフェイスの名前
	nfaEventOccurEntryName :	監視エントリの名前
	nfaEventLevel :	重要度(information(1)を通知)
	nfaThreshFlowConditions :	監視対象のフロー条件
	nfaThreshConfData :	しきい値
	nfaThreshConfUnit :	しきい値と実測値の単位
	nfaThreshFlowDirection :	通信の方向

- セキュリティ監視機能
  - nfaSecurityDdosDetected

    DDoS 検知によるインシデントの検出を示す。

Enterprise :	.1.3.6.1.4.1.119.2.3.239.2	
Generic Trap :	6	
Specific Trap :	6	
Variable Bindings :	nfaEventOccurTime :	イベントの発生日時
	nfaEventOccurExpAddr :	エクスポーターの IP アドレス
	nfaEventOccurExpIfIndex :	エクスポーターの ifIndex
	nfaEventOccurExpName :	エクスポーターの名前
	nfaEventOccurExpIfName :	エクスポーターのインターフェイスの名前
	nfaEventLevel :	重要度
	nfaSecurityDetectionRule :	検知ルール名
	nfaSecurityDstIP :	被疑となったフローの宛先 IP アドレス
	nfaSecurityDirection :	通信の方向
	nfaSecurityIncidentID :	インシデント ID

- nfaSecurityDdosCleared

  DDoS 検知によるインシデントのイベントが回復されたことを示す。

Enterprise :	.1.3.6.1.4.1.119.2.3.239.2	
Generic Trap :	6	
Specific Trap :	7	
Variable Bindings :	nfaEventOccurTime :	イベントの発生日時
	nfaEventOccurExpAddr :	エクスポーターの IP アドレス
	nfaEventOccurExpIfIndex :	エクスポーターの ifIndex
	nfaEventOccurExpName :	エクスポーターの名前
	nfaEventOccurExpIfName :	エクスポーターのインターフェイスの名前
	nfaEventLevel :	重要度(information(1)を通知)
	nfaSecurityIncidentID :	インシデント ID

- nfaSecurityDdosAutoCleared

  DDoS 検知によるインシデントのイベントが、インシデント情報の削除に伴って自動的に回復されたことを示す。

Enterprise :	.1.3.6.1.4.1.119.2.3.239.2	
Generic Trap :	6	
Specific Trap :	8	
Variable Bindings :	nfaEventOccurTime :	イベントの発生日時
	nfaEventOccurExpAddr :	エクスポーターの IP アドレス
	nfaEventOccurExpIfIndex :	エクスポーターの ifIndex
	nfaEventOccurExpName :	エクスポーターの名前
	nfaEventOccurExpIfName :	エクスポーターのインターフェイスの名前
	nfaEventLevel :	重要度(information(1)を通知)
	nfaSecurityIncidentID :	インシデント ID

- nfaSecurityScanDetected

  スキャン検知によるインシデントの検出を示す。

Enterprise :	.1.3.6.1.4.1.119.2.3.239.2	
Generic Trap :	6	
Specific Trap :	9	
Variable Bindings :	nfaEventOccurTime :	イベントの発生日時
	nfaEventOccurExpAddr :	エクスポーターの IP アドレス
	nfaEventOccurExpIfIndex :	エクスポーターの ifIndex
	nfaEventOccurExpName :	エクスポーターの名前
	nfaEventOccurExpIfName :	エクスポーターのインターフェイスの名前
	nfaEventLevel :	重要度

	nfaSecurityDetectionRule :	検知ルール名
	nfaSecuritySrcIP :	被疑となったフローの送信元 IP アドレス
	nfaSecurityDirection :	通信の方向
	nfaSecurityIncidentID :	インシデント ID

- nfaSecurityScanCleared

  スキャン検知によるインシデントのイベントが回復されたことを示す。

Enterprise :	.1.3.6.1.4.1.119.2.3.239.2	
Generic Trap :	6	
Specific Trap :	10	
Variable Bindings :	nfaEventOccurTime :	イベントの発生日時
	nfaEventOccurExpAddr :	エクスポーターの IP アドレス
	nfaEventOccurExpIfIndex :	エクスポーターの ifIndex
	nfaEventOccurExpName :	エクスポーターの名前
	nfaEventOccurExpIfName :	エクスポーターのインターフェイスの名前
	nfaEventLevel :	重要度(information(1)を通知)
	nfaSecurityIncidentID :	インシデント ID

- nfaSecurityScanAutoCleared

  スキャン検知によるインシデントのイベントが、インシデント情報の削除に伴って自動的に回復されたことを示す。

Enterprise :	.1.3.6.1.4.1.119.2.3.239.2	
Generic Trap :	6	
Specific Trap :	11	
Variable Bindings :	nfaEventOccurTime :	イベントの発生日時
	nfaEventOccurExpAddr :	エクスポーターの IP アドレス
	nfaEventOccurExpIfIndex :	エクスポーターの ifIndex
	nfaEventOccurExpName :	エクスポーターの名前
	nfaEventOccurExpIfName :	エクスポーターのインターフェイスの名前
	nfaEventLevel :	重要度(information(1)を通知)
	nfaSecurityIncidentID :	インシデント ID

ヒント

NFA が送信する SNMP トラップの形式を定義した MIB ファイルはインストールメディア内の以下のパスに収録しています。

- `/NFA/tools/flow-Analyzer.mib`

2.3　エクスポーターを管理する

管理対象のエクスポーター情報(エクスポーター、および、そのインターフェイスの情報)を管理する方法について説明します。

エクスポーター管理画面

エクスポーターを NFA に管理対象として登録するには、以下の 2 つの方法があります。

- 「2.3.1　エクスポーターの情報を自動で登録する（38 ページ）」
- 「2.3.2　エクスポーターの情報を手動で登録する（40 ページ）」

ここでは、上記のいずれかの方法で登録したエクスポーター情報を管理するエクスポーター管理画面について説明します。

エクスポーター管理画面は、[**システム管理**] >[**エクスポーター管理**] をクリックして表示します。

図 2-2　エクスポーター管理画面

機能操作領域

- [**追加**]ボタン

  エクスポーターを新規に登録します。本ボタンをクリックすると、エクスポーター追加画面が表示されます。

- [**すべて展開**]ボタン

  すべてのエクスポーターに対する[**インターフェイス一覧**]を展開して表示します。

- [**すべて折りたたむ**]ボタン

  すべてのエクスポーターに対する[**インターフェイス一覧**]を折りたたんで表示します。

- [**DNS 情報取得**]ボタン

  DNS に問い合わせを行い、すべてのエクスポーターのホスト名(ドメイン名)を取得します。

- [**SNMP 情報取得**]ボタン

  すべてのエクスポーターから SNMP を用いて、ホスト名(sysName)、および、管理対象のインターフェイス名(ifName)を取得します。

- [**インターフェイスライセンス**]

  現在のインターフェイスライセンスの割り当て状況を表示します。

- [**ライセンス変更反映**]ボタン

  インターフェイスライセンスの割り当て状況に対する変更内容を反映します。

- [**直近 7 日間の全体のフローレートの最大値**]

  直近の 7 日間における全エクスポーターの最大フローレート合計値とその日時を表示します。

エクスポーターの一覧

- [**エクスポーター名**]

  管理対象のエクスポーターの名前を表示します。

  ▸ボタン、または、▾ボタンをクリックすると、当該エクスポーターの[**インターフェイス一覧**]の表示の展開、または、折りたたみを行います。

- [**インターフェイス一覧**]

  管理対象のインターフェイスの情報を表示します。

  - [**インターフェイス名**]チェックボックス

    インターフェイスライセンスの割り当て状況を示します。

    * チェック: オン

      ライセンスが割り当てられています。

    * チェック: オフ

      ライセンスが割り当てられていません。

  - [**編集**]ボタン

    インターフェイスの登録内容を変更します。本ボタンをクリックすると、インターフェイス編集画面が表示されます。

  - [**削除**]ボタン

    インターフェイスの情報を削除します。

- [**IP アドレス**]

  管理対象のエクスポーターの IP アドレスを表示します。

- [**フローレートの最大値(計測時刻)**]

  直近の 7 日間におけるフローレートの最大値とその日時を表示します。表示するフローレートは、1 分間に発生したフロー数となります。

- [**最終受信時刻**]

  エクスポーターからフローデータを最後に受信した日時を表示します。

- [**操作**]

  登録されているエクスポーターに対する操作ボタンを表示します。

  - [**編集**]ボタン

    エクスポーターの登録内容を変更します。本ボタンをクリックすると、エクスポーター編集画面が表示されます。

  - [**削除**]ボタン

    エクスポーター情報を削除します。

  - [**インターフェイス追加**]ボタン

    インターフェイスを新規に登録します。本ボタンをクリックすると、インターフェイス追加画面が表示されます。

2.3.1　エクスポーターの情報を自動で登録する

NFA では、管理対象のエクスポーターの情報を、フロー情報の受信を契機に自動登録することができます。

エクスポーター情報を自動登録する場合は、[**エクスポーター情報の自動登録ポリシー**]において、自動登録設定が選択されている必要があります。詳細は、「2.2.1　エクスポーター情報の登録ポリシーを設定する（29 ページ）」を参照してください。

自動登録処理では、受信したフロー情報をもとに以下の情報を自動で登録します。

- エクスポーターの識別情報
- 分析対象のインターフェイス情報
- インターフェイスライセンスの割り当て

エクスポーターの識別情報の登録

- フロー情報の送信元 IP アドレスをエクスポーターの IP アドレスとして登録します。

  NFA に、すでに同じ IP アドレスのエクスポーターが登録されていた場合は、登録済みと判断し、エクスポーターの登録処理は行いません。

- 新規のエクスポーターの登録の場合は、DNS(Domain Name System)に問い合わせを行い、FQDN(完全修飾ドメイン名)形式のホスト名を登録します。
- エクスポーター側で SNMP を有効にしている場合は、SNMP を用いて、エクスポーターの MIB からホスト名(sysName)を取得し、登録します。この SNMP 情報取得においては、「2.2.2　SNMP 情報取得パラメーターのデフォルト値を設定する（30 ページ）」で指定した SNMP パラメーターを使用します。

ヒント

自動登録されたエクスポーターの表示名は、下記の優先順位で表示を行います。

1. ホスト名 (DNS)
2. ホスト名 (SNMP sysName)
3. IP アドレス

分析対象のインターフェイス情報の登録

- NFA では、エクスポーター側でのフロー情報の出力設定において、インターフェイスの入力(IN)側の通信をフローの分析対象にしていることを想定しています。そのため、NFA では、受信したフロー情報の入力(IN)側を示すインターフェイスの識別子(ifIndex)を分析対象のインターフェイスとして NFA に登録します。

  NFA に、すでに、同じエクスポーターの ifIndex 値として登録されていた場合は、登録済みと判断し、インターフェイス情報の登録処理は行いません。
- エクスポーター側で SNMP を有効にしている場合は、SNMP を用いて、エクスポーターの MIB からインターフェイス名(ifName)を取得し、登録します。この SNMP 情報取得においては、「2.2.2　SNMP 情報取得パラメーターのデフォルト値を設定する（30 ページ）」で指定した SNMP パラメーターを使用します。

  ifName の値を取得できた場合は、各画面でのインターフェイス名の表示を ifName の名前で表示します。ifName の値が取得できない場合は、ifIndex<ifIndex 値> の形式でインターフェイス名を表示します。

⚠ 注意

エクスポーター側でのフロー情報の出力設定において、インターフェイスの出力(OUT)側の通信をフローの分析対象にしている場合は、エクスポーター情報の自動登録処理は正しく動作しません。この場合は、手動で登録情報を更新してください。

インターフェイスライセンスの割り当て

- NFA が分析対象のインターフェイスと判断する入力(IN)側のインターフェイスに対し、インターフェイス情報の登録処理と同時にインターフェイスライセンスの割り当て処理を行います。

- 割り当て可能なインターフェイスライセンスがない場合は、割り当て処理は行いません。

ヒント

インターフェイスライセンスの割り当て処理まで正常に完了した場合に、当該フロー情報を NFA に蓄積、管理します。ライセンス数の超過により、インターフェイスライセンスの割り当てが行えなかった場合は、受信したフロー情報を破棄します。

2.3.2　エクスポーターの情報を手動で登録する

エクスポーターの情報は、手動であれば、NFA にいつでも登録することができます。

手動で登録する場合は、エクスポーター管理画面で以下のエクスポーター情報を登録します。

- エクスポーターの識別情報

  エクスポーターの一覧の[**追加**]ボタンをクリックし、登録作業を行います。詳細は、「2.3.2.1　エクスポーターを追加する（40 ページ）」を参照してください。

- 分析対象のインターフェイス情報

  エクスポーターの一覧の[**インターフェイス追加**]ボタンをクリックし、登録作業を行います。詳細は、「2.3.2.2　管理対象のインターフェイスを追加する（42 ページ）」を参照してください。

  ヒント

  手動登録したインターフェイスに対しては、フロー情報の受信、分析を行うために、別途、インターフェイスライセンスの割り当て操作を行う必要があります。

2.3.2.1　エクスポーターを追加する

エクスポーターの識別情報を NFA に登録するための手順について説明します。

1. エクスポーター管理画面を表示します。

   [**システム管理**] >[**エクスポーター管理**] をクリックします。

2. [**追加**]ボタンをクリックします。

3. 表示されたエクスポーター設定画面で適切な値を指定します。

   - [**表示名**]

     エクスポーターの表示名を指定します。最大文字数は 32 文字です。

     以下に示す文字は指定することができません。

     - 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
     - 先頭および末尾への半角スペース

NFA の各画面では、ここで入力した表示名でエクスポーターを表示します。省略した場合は、以下の優先順位で表示します。

a. ホスト名 (DNS)

b. ホスト名 (SNMP sysName)

c. IP アドレス

- [**IP アドレス**]

  フロー情報の送信元となる IPv4 アドレスを指定します。他のエクスポーターと重複した IP アドレスを指定することはできません。

- [**SNMP 設定**]

  エクスポーター側の SNMP 設定内容に合わせて以下の 3 つのパラメーターを入力します。

  - [**SNMP バージョン**]

    プルダウンメニュー([**空欄(省略)**] / [**1**] / [**2c**])から選択します。

  - [**ポート番号**]

    0～65535 の範囲で半角数字を指定します。SNMP のポート番号は、一般的には、161 を利用します。

  - [**SNMP コミュニティ名**]

    最大文字数は 255 文字で、以下の文字を使って指定します。

    * 半角英数字
    * 半角スペース
    * 以下の記号

      ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

  3 つのパラメーターは、省略可能です。省略したパラメーターは、環境設定画面で指定したデフォルト値で動作します。詳細は、「2.2.2　SNMP 情報取得パラメーターのデフォルト値を設定する（30 ページ）」を参照してください。

4. 必要に応じてエクスポーターのサンプリング率を設定します。

- [**サンプリング率の手動設定**]

  NetFlow または IPFIX パケットを送信するエクスポーターにのみ有効な設定です。サンプリング動作をしているのにサンプリング率の通知を行えないエクスポーターの場合や、サンプリング率を手動で指定したい場合に使用します。

  [**サンプリング率**]を指定した場合、エクスポーターから受信したフロー情報に、指定したサンプリング率をかけた値を計算し、実際の通信量と判断します。

  - [**サンプリング率**]

* 空 (指定しない)

  デフォルト値です。

  エクスポーターから通知されるサンプリング率を利用します。

* 1 以上の整数値

  指定したサンプリング率を利用します。

- [**エクスポーターからの通知を使用する**]

  * チェック : オン

    エクスポーターから通知されるサンプリング率を利用します。

    デフォルトはチェック:オンです。

  * チェック : オフ

    チェックをオフにすることで[**サンプリング率**]欄が有効になります。

    サンプリング率を手動で設定する場合に使用します。

ヒント

- sFlow パケットには必ずサンプリング率が含まれています。このため、sFlow パケットを送信するエクスポーターを自動登録した場合、[**サンプリング率**]を手動で設定することはできません。
- NFA1.0 からのバージョンアップを行った場合、バージョンアップ前に登録されていたすべてのエクスポーターは[**エクスポーターからの通知を使用する**]がオンの状態になります。

5. 設定内容を確認し、[**OK**]ボタンをクリックします。

2.3.2.2　管理対象のインターフェイスを追加する

分析対象のインターフェイス情報を NFA に登録するための手順について説明します。

1. エクスポーター管理画面を表示します。

   [**システム管理**] >[**エクスポーター管理**] をクリックします。

2. エクスポーターの一覧で、対象エクスポーターの[**インターフェイス追加**]ボタンをクリックします。

3. 表示されたインターフェイス設定画面で適切な値を指定します。

   - [**インデックス (SNMP ifIndex)**]

     分析対象のインターフェイスを示す ifIndex の値を指定します。1 以上の半角数字を指定します。

   - [**表示名**]

     インターフェイスの表示名を指定します。最大文字数は 32 文字です。

以下に示す文字は指定することができません。

- 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
- 先頭および末尾への半角スペース

NFA の各画面では、ここで指定した表示名でインターフェイスを表示します。

省略した場合は、下記の優先順位でインターフェイス名を表示します。

a. ifName

b. ifIndex<ifIndex 値>

4. 設定内容を確認し、[**OK**]ボタンをクリックします。

2.3.3　エクスポーターの情報を更新、削除する

NFA に登録したエクスポーターの情報は、エクスポーター管理画面で、登録情報の更新や削除を行うことができます。

2.3.3.1　エクスポーターの情報を更新する

NFA に登録したエクスポーターの情報を更新するための手順について説明します。

ヒント

[**IP アドレス**]については、変更することができません。

1. エクスポーター管理画面を表示します。

   [**システム管理**] >[**エクスポーター管理**] をクリックします。

2. エクスポーターの一覧で、対象エクスポーターの[**編集**]ボタンをクリックします。

   エクスポーター編集画面が表示されます。

3. エクスポーター編集画面で変更したい項目の入力値を変更します。

   - [**表示名**]

     エクスポーターの表示名を指定します。最大文字数は 32 文字です。

     以下に示す文字は指定することができません。

     - 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
     - 先頭および末尾への半角スペース

     NFA の各画面では、ここで入力した表示名でエクスポーターを表示します。省略した場合は、以下の優先順位で表示します。

     a. ホスト名 (DNS)

     b. ホスト名 (SNMP sysName)

c. IP アドレス

- [**ホスト名 (DNS)**]

  情報を更新する場合は、[**DNS 情報取得**]ボタンをクリックします。情報が取得できなかった場合は、何も表示しません。

- [**ホスト名 (SNMP sysName)**]

  情報を更新する場合は、[**SNMP 情報取得**]ボタンをクリックします。情報が取得できなかった場合は、何も表示しません。

- [**SNMP 設定**]

  エクスポーター側の SNMP 設定内容に合わせて以下の 3 つのパラメーターを入力します。

  - [**SNMP バージョン**]

    プルダウンメニュー([**空欄(省略)**] / [**1**] / [**2c**])から選択します。

  - [**ポート番号**]

    0～65535 の範囲で半角数字を指定します。SNMP のポート番号は、一般的には、161 を利用します。

  - [**SNMP コミュニティ名**]

    最大文字数は 255 文字で、以下の文字を使って指定します。

    * 半角英数字
    * 半角スペース
    * 以下の記号

      ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

  3 つのパラメーターは、省略可能です。省略したパラメーターは、環境設定画面で指定したデフォルト値で動作します。詳細は、「2.2.2　SNMP 情報取得パラメーターのデフォルト値を設定する（30 ページ）」を参照してください。

4. 必要に応じてエクスポーターのサンプリング率を設定します。

- [**サンプリング率の手動設定**]

  NetFlow または IPFIX パケットを送信するエクスポーターにのみ有効な設定です。サンプリング動作をしているのにサンプリング率の通知を行えないエクスポーターの場合や、サンプリング率を手動で指定したい場合に使用します。

  [**サンプリング率**]を指定した場合、エクスポーターから受信したフロー情報に、指定したサンプリング率をかけた値を計算し、実際の通信量と判断します。

  - [**サンプリング率**]

    * 空 (指定しない)

デフォルト値です。

エクスポーターから通知されるサンプリング率を利用します。

* 1 以上の整数値

指定したサンプリング率を利用します。

- [**エクスポーターからの通知を使用する**]

* チェック : オン

エクスポーターから通知されるサンプリング率を利用します。

デフォルトはチェック:オンです。

* チェック : オフ

チェックをオフにすることで[**サンプリング率**]欄が有効になります。

サンプリング率を手動で設定する場合に使用します。

ヒント

- sFlow パケットには必ずサンプリング率が含まれています。このため、sFlow パケットを送信するエクスポーターを自動登録した場合、[**サンプリング率**]を手動で設定することはできません。
- NFA1.0 からのバージョンアップを行った場合、バージョンアップ前に登録されていたすべてのエクスポーターは[**エクスポーターからの通知を使用する**]がオンの状態になります。

5. 変更内容を確認し、[**OK**]ボタンをクリックします。

2.3.3.2　管理対象のインターフェイスの情報を更新する

NFA に登録したインターフェイス情報を更新するための手順について説明します。

更新することができる項目は、以下の通りです。

- [**表示名**]

1. エクスポーター管理画面を表示します。

   [**システム管理**] >[**エクスポーター管理**] をクリックします。

2. エクスポーターの一覧で、対象インターフェイスの[**編集**]ボタンをクリックします。

   インターフェイスの編集画面が表示されます。

3. インターフェイスの編集画面で[**表示名**]欄の入力値を変更します。

   - [**表示名**]

     インターフェイスの表示名を指定します。最大文字数は 32 文字です。

     以下に示す文字は指定することができません。

- 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
- 先頭および末尾への半角スペース

NFA の各画面では、ここで指定した表示名でインターフェイスを表示します。

省略した場合は、下記の優先順位でインターフェイス名を表示します。

a. ifName

b. ifIndex:<ifIndex 値>

インターフェイスの名前 (SNMP ifName) を更新する場合は、[**SNMP 情報取得**]ボタンをクリックします。

4. 変更内容を確認し、[**OK**]ボタンをクリックします。

2.3.3.3　エクスポーターの情報を削除する

NFA に登録したエクスポーターの情報を削除するための手順について説明します。

⚠ 注意

本操作を行うと、削除対象のエクスポーターの下記の情報も削除します。

- すべてのインターフェイス情報。
- すべてのインターフェイスに対して蓄積した、フロー情報。

1. エクスポーター管理画面を表示します。

   [**システム管理**] >[**エクスポーター管理**] をクリックします。

2. エクスポーターの一覧で、対象エクスポーターの[**削除**]ボタンをクリックします。
3. 表示された削除確認ダイアログで内容を確認します。
4. [**OK**]ボタンをクリックし、削除を実行します。

2.3.3.4　管理対象のインターフェイスの情報を削除する

NFA に登録したインターフェイス情報を削除するための手順について説明します。

1. エクスポーター管理画面を表示します。

   [**システム管理**] >[**エクスポーター管理**] をクリックします。

2. エクスポーターの一覧で、対象インターフェイスの[**削除**]ボタンをクリックします。
3. 表示された削除確認ダイアログで内容を確認します。
4. [**OK**]ボタンをクリックし、削除を実行します。

2.3.4　インターフェイスライセンスの割り当て状況を一括で更新する

NFA に登録しているインターフェイスに対し、一括で、インターフェイスライセンスの割り当て状況を更新することができます。

更新後のインターフェイスライセンスの割り当て数が、割り当て可能数を超えないことを事前に確認してください。

- NFA では、インターフェイスライセンスを割り当てているインターフェイスのフロー情報のみを受信し、蓄積します。
- 本操作で、インターフェイスライセンスの割り当てを解除した場合は、エクスポーター情報の自動登録を許可している場合であっても、自動でインターフェイスライセンスの割り当てが行われることはありません。

1. エクスポーター管理画面を表示します。

   [**システム管理**] >[**エクスポーター管理**] をクリックします。

2. エクスポーターの一覧で、[**すべて展開**]ボタンをクリックします。

   すべてのエクスポーターのインターフェイス情報が表示されます。

3. インターフェイスライセンスの割り当て状況を変更します。

   [**インターフェイス一覧**]のチェックボックスを切り替えます。

   - チェック : オン

     インターフェイスライセンスを割り当てます。

   - チェック : オフ

     インターフェイスライセンスの割り当てを解除します。

   インターフェイスライセンスの割り当て状況を変更した場合、当該インターフェイスの欄の色が変わります。

4. 変更内容を確認し、[**ライセンス変更反映**]ボタンをクリックします。

2.4　ユーザーを管理する

NFA の Web コンソールにログインするユーザーの管理について説明します。

2.4.1　ユーザーの種類

NFA のユーザーに対し、アクセスレベルを設定することで、操作範囲を制限することができます。

ユーザーのアクセスレベルには、管理者 と オペレーター の 2 種類があります。

管理者

NFA が提供するすべての画面、機能の操作を行うことができます。

オペレーター

参照操作を基本とします。NFA の設定操作については、フローの分析操作に関係する一部を除き、操作を制限しています。

具体的な制限内容は以下の通りです。

表 2-1　オペレーターの操作可能範囲

メインメニュー	操作	備考
[**ダッシュボード**]タブ	○	すべての操作を行うことができます。ただし、ダッシュボード定義に対する編集、削除の操作は、自身が作成した定義のみに制限されます。
[**エクスポーター分析**]タブ	○	-
[**イベント監視**]タブ	△	しきい値監視の設定操作を行うことはできません。
[**グループ管理**]タブ	△	エンドポイントグループ、および、IF グループの設定操作を行うことはできません。
[**システム管理**]タブ	×	表示しません。
[**個人設定**]ボタン	○	-
[**ヘルプ**]ボタン	○	-
[**ログアウト**]ボタン	○	-

2.4.2　ユーザー情報を操作する

NFA のユーザー情報を管理するユーザー管理画面について説明します。

ユーザー管理画面

ユーザーの一覧では、登録済みのユーザーの情報確認、および、登録操作を行います。

ユーザー管理画面は、[**システム管理**] >[**ユーザー管理**] をクリックして表示します。

図 2-3　ユーザー管理画面

機能操作領域

- [**追加**]ボタン

  ユーザーを新規に登録します。本ボタンをクリックすると、ユーザー追加画面が表示されます。

ユーザーの一覧

- [**ユーザー名**]

  登録しているユーザーを識別するための名前を表示します。

- [**表示名**]

  ログイン時に表示するユーザー表示名の設定値を表示します。

- [**アクセスレベル**]

  ユーザーのアクセスレベル(管理者、オペレーター)を表示します。

- [**デフォルトのダッシュボード**]

  ログイン時に最初に表示するデフォルトのダッシュボード定義の名前を表示します。

- [**最終ログイン**]

  ユーザーが最後にログインした日時を表示します。

- [**操作**]

  登録されているユーザーに対する操作ボタンを表示します。

  - [**編集**]ボタン

    ユーザーの登録内容を変更します。本ボタンをクリックすると、ユーザー編集画面が表示されます。

  - [**削除**]ボタン

    登録済みのユーザーを削除します。

    注意

    - 初期状態から登録されている「admin」ユーザーは削除できません。（本ボタンを表示しません。）
    - ユーザーがログインしているとき、本ボタンは無効な状態で表示されます。

2.4.2.1　ユーザーを追加する

新規にユーザーを登録する手順について説明します。

1. ユーザー管理画面を表示します。

   [**システム管理**] >[**ユーザー管理**] をクリックします。

2. ユーザーの一覧の[**追加**]ボタンをクリックします。
3. 表示されたユーザー追加画面で適切な値を指定します。
   - [**ユーザー名**]

     NFA 内で一意に識別できるユーザーの名前を指定します。最大文字数は 255 文字です。指定可能な文字は、半角英数字、ハイフン(-)、アンダーバー(_)、ドット(.)、アットマーク(@)、アポストロフィ(')です。
   - [**表示名**]

     画面上の表示用のユーザーの名前を指定します。最大文字数は 32 文字です。

     以下に示す文字は指定することができません。

     - 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
     - 先頭および末尾への半角スペース

     省略した場合は、[**ユーザー名**]で指定した名前を表示名としても使用します。
   - [**初期パスワード**]

     登録するユーザーの初期パスワードを指定します。以下の文字を組み合わせて、8~64 文字の文字数で指定します。

     - 半角英大文字
     - 半角英小文字
     - 半角数字
     - 半角スペース と 以下の記号

       ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

     パスワードには、上記の 4 種類の文字のうち、3 種類以上の文字を含んでいる必要があります。
   - [**パスワード再入力**]

     [**初期パスワード**]で指定したものと同じパスワードを指定します。
   - [**アクセスレベル**]

     [**管理者**]、[**オペレーター**]のいずれかを選択します。
   - [**デフォルトのダッシュボード**]

     ユーザーがログインした時に、最初に表示するダッシュボード定義の名前を選択します。
4. 設定内容を確認し、[**OK**]ボタンをクリックします。

2.4.2.2　ユーザー情報を更新する

ユーザーの登録情報を更新する手順について説明します。

ヒント

[**ユーザー名**]については、変更することができません。

1. ユーザー管理画面を表示します。

   [**システム管理**] >[**ユーザー管理**] をクリックします。

2. ユーザーの一覧で、対象ユーザーの[**編集**]ボタンをクリックします。

3. 表示されたユーザー編集画面で内容を変更します。

   - [**表示名**]

     画面上の表示用のユーザーの名前を指定します。最大文字数は 32 文字です。

     以下に示す文字は指定することができません。

     - 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
     - 先頭および末尾への半角スペース

     省略した場合は、[**ユーザー名**]で指定した名前を表示名としても使用します。

   - [**アクセスレベル**]

     [**管理者**]、[**オペレーター**]のいずれかを選択します。

   - [**デフォルトのダッシュボード**]

     ユーザーがログインした時に、最初に表示するダッシュボード定義の名前を選択します。

   - [**パスワード変更**]

     チェックボックスをオンにし、[**新パスワード**]欄、および、[**パスワード再入力**]欄に、新しいパスワードを指定します。パスワードは、以下の文字を組み合わせて、8~64 文字の文字数で指定します。

     - 半角英大文字
     - 半角英小文字
     - 半角数字
     - 半角スペース と 以下の記号

       ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~

     パスワードには、上記の 4 種類の文字のうち、3 種類以上の文字を含んでいる必要があります。また、過去 10 回分のパスワードとは異なっている必要があります。

4. 変更内容を確認し、[**OK**]ボタンをクリックします。

2.4.2.3　ユーザー情報を削除する

ユーザーを削除する手順について説明します。

1. ユーザー管理画面を表示します。

   [**システム管理**] >[**ユーザー管理**] をクリックします。

2. ユーザーの一覧で、対象ユーザーの[**削除**]ボタンをクリックします。
3. 表示された削除確認ダイアログで内容を確認します。
4. [**OK**]ボタンをクリックし、削除を実行します。

第 3 章
運用時の各種設定

NFA の運用に入ってから必要に応じて行う環境設定の方法について説明します。

目次

3.1 複数インターフェイスのフローを集計し分析する 54
3.2 複数の宛先または送信元のフローを集計して分析する.....58
3.3 固有のアプリケーション通信を識別する 62
3.4 特定フローをしきい値で監視する.....75
3.5 ローデータの外部出力設定を行う.....85
3.6 セキュリティ観点でフローを分析・監視する 87

3.1　複数インターフェイスのフローを集計し分析する

NFA では、分析対象とする複数の物理インターフェイスをエクスポーター側の設定に合わせて、論理的な 1 つのインターフェイスとしてグルーピングする IF グループ機能を提供しています。

3.1.1　IF グループについて

IF グループの利用方法について説明します。

IF グループの利用用途

エクスポーター側の仕様によっては、複数の物理インターフェイスを LAG(Link Aggregation) などの設定により、1 つの論理的なインターフェイスとしてまとめる構成をとることができます。しかし、エクスポーター側では、論理的な 1 つのインターフェイスに対するフロー情報を送信することができないため、通常は、物理インターフェイスごとのフロー情報に対する分析しか行うことができません。

エクスポーター側のインターフェイス設定と同じように、NFA 側でも論理的な 1 つのインターフェイスとして、フロー情報を分析したい場合に、IF グループを用います。

IF グループでまとめたインターフェイスに対し可能な操作内容

NFA では、IF グループでまとめたインターフェイスを通常のインターフェイスと同等に取り扱います。そのため、IF グループでまとめたインターフェイスに対しても通常のインターフェイスと同様に以下の操作を行うことができます。

- ダッシュボード画面、および、エクスポーター分析画面の[**通信量 (入力インターフェイス)**]ウィジェット、[**通信量 (出力インターフェイス)**]ウィジェットで、IF グループのインターフェイスに対する通信量を確認することができます。
- ダッシュボード画面、および、エクスポーター分析画面で、[**対象インターフェイス**]に IF グループのインターフェイスを指定すると、IF グループのインターフェイスの通信量に対する各種ウィジェットでの分析結果を確認することができます。
- IF グループのインターフェイスの通信量に対し、しきい値監視を設定することができます。

ヒント

- IF グループは、同一のエクスポーターのインターフェイスに対してのみグルーピングが行えます。異なるエクスポーターのインターフェイスをグルーピングすることはできません。
- 1 つのインターフェイスを複数の IF グループに所属させることはできません。

- IF グループでグルーピングしたインターフェイスを削除した場合は、自動的に、IF グループからも削除されます。

3.1.2　IF グループを操作する

IF グループ一覧画面について説明します。

IF グループ一覧画面

登録済みの IF グループの内容確認、および、登録操作を行います。

IF グループ一覧画面は、[**グループ管理**] >[**IF グループ一覧**] をクリックして表示します。

図 3-1　IF グループ一覧画面

機能操作領域

- [**追加**]ボタン

  IF グループを新規に登録します。本ボタンをクリックすると、IF グループ追加画面が表示されます。

  ⚠ 注意

  ユーザーのアクセスレベルがオペレーターの場合は、本ボタンを表示しません。

IF グループの一覧

- [**IF グループ名**]

  IF グループの名前を表示します。

- [**エクスポーター**]

  グルーピングしたインターフェイスを保有するエクスポーターの名前を表示します。

- [**インターフェイス**]

  IF グループに属するインターフェイスの名前を表示します。

- [**操作**]

  登録されている IF グループに対する操作ボタンを表示します。

  - [**編集**]ボタン

IF グループの登録内容を変更します。本ボタンをクリックすると、IF グループ編集画面が表示されます。

- [**削除**]ボタン

  登録済みの IF グループを削除します。

注意

ユーザーのアクセスレベルがオペレーターの場合は、[**操作**]列を表示しません。

3.1.2.1　IF グループを追加する

新規に IF グループを登録する手順について説明します。

1. IF グループ一覧画面を表示します。

   [**グループ管理**] >[**IF グループ一覧**] をクリックします。

2. [**追加**]ボタンをクリックします。

3. 表示された IF グループ追加画面で適切な値を指定します。

   - [**IF グループ名**]

     IF グループに対する名前を指定します。最大文字数は 32 文字です。

     以下に示す文字は指定することができません。

     - 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
     - 先頭および末尾への半角スペース

   - [**対象エクスポーター**]

     NFA に登録しているエクスポーターをプルダウンメニューから選択します。

   - [**対象インターフェイス**]

     [**対象エクスポーター**]を選択すると表示されます。チェックボックスをオンにし、グルーピング対象のインターフェイスを選択します。

     チェック: オン

     グルーピング対象に追加します。

     チェック: オフ

     グルーピング対象から除外します。

     ヒント

     すでに他の IF グループに所属しているインターフェイスは、[**対象インターフェイス**]には表示しません。

4. 設定内容を確認し、[**OK**]ボタンをクリックします。

3.1.2.2　IF グループを更新する

IF グループの登録情報を更新する手順について説明します。

ヒント

[**対象エクスポーター**]については、変更することができません。

1. IF グループ一覧画面を表示します。

   [**グループ管理**] >[**IF グループ一覧**] をクリックします。

2. IF グループの一覧で、対象 IF グループの[**編集**]ボタンをクリックします。

3. 表示された IF グループ編集画面で内容を変更します。

   - [**IF グループ名**]

     IF グループに対する名前を指定します。最大文字数は 32 文字です。

     以下に示す文字は指定することができません。

     - 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
     - 先頭および末尾への半角スペース

   - [**対象インターフェイス**]

     チェックボックスを切り替え、グルーピング対象のインターフェイスを選択します。

     チェック: オン

     グルーピング対象に追加します。

     チェック: オフ

     グルーピング対象から除外します。

4. 変更内容を確認し、[**OK**]ボタンをクリックします。

3.1.2.3　IF グループを削除する

IF グループを削除する手順について説明します。

1. IF グループ一覧画面を表示します。

   [**グループ管理**] >[**IF グループ一覧**] をクリックします。

2. IF グループの一覧で、対象 IF グループの[**削除**]ボタンをクリックします。

3. 表示された削除確認ダイアログで内容を確認します。

4. [**OK**]ボタンをクリックし、削除を実行します。

3.2　複数の宛先または送信元のフローを集計して分析する

NFA では、通信のエンドポイントとなる複数の送信元 IP アドレス、または、宛先 IP アドレスをグルーピングし、グループ単位で通信量の分析を行うことができるエンドポイントグループ機能を提供しています。

3.2.1　エンドポイントグループについて

エンドポイントグループの利用方法について説明します。

エンドポイントグループの利用用途

部門間、または、拠点間をつなぐネットワークの通信負荷を調べる場合に、個々のエンドポイントの通信量を 1 つ 1 つ調べていく方法では、多くの作業工数が発生してしまい、全体的な通信内容の傾向を調べることも困難です。

このような場合に対応するため、NFA では、複数のエンドポイントをグルーピングして、グループごとの通信量を集計し、また、その集計した通信に対する内訳などを詳しく分析することができるエンドポイントグループ機能を提供しています。

エンドポイントグループ機能を用いることで、部署や拠点などのネットワークを利用する組織単位での通信傾向を把握することができるようになり、部門間、または、拠点間を結ぶネットワークのキャパシティ管理業務に役立てることができます。

エンドポイントグループに対し可能な操作内容

NFA では、エンドポイントグループ機能を用いて、以下の分析操作を行うことができます。

- ダッシュボード画面、および、エクスポーター分析画面の[**送信元エンドポイントグループ**]ウィジェット、[**宛先エンドポイントグループ**]ウィジェットで、エンドポイントグループごとの通信量を確認することができます。
- エクスポーター分析画面の[**フィルター条件**]で、[**送信元エンドポイントグループ**]または、[**宛先エンドポイントグループ**]を指定すると、エンドポイントグループの通信に対する各種ウィジェットでの分析結果を確認することができます。
- エンドポイントグループの通信量に対し、しきい値監視を設定することができます。

3.2.2　エンドポイントグループを操作する

エンドポイントグループ一覧画面について説明します。

エンドポイントグループ一覧画面

登録済みのエンドポイントグループの内容確認、および、登録操作を行います。

エンドポイントグループ一覧画面は、[**グループ管理**] >[**エンドポイントグループ一覧**] をクリックして表示します。

図 3-2　エンドポイントグループ一覧画面

機能操作領域

- [**追加**]ボタン

  エンドポイントグループを新規に登録します。本ボタンをクリックすると、エンドポイントグループ追加画面が表示されます。

  ⚠ 注意

  ユーザーのアクセスレベルがオペレーターの場合は、本ボタンを表示しません。

エンドポイントグループの一覧

- [**エンドポイントグループ名**]

  エンドポイントグループの名前を表示します。

- [**IP アドレス**]

  エンドポイントグループに属する IP アドレス、IP アドレス範囲、ネットワークアドレスの情報を表示します。

- [**操作**]

  登録されているエンドポイントグループに対する操作ボタンを表示します。

  - [**編集**]ボタン

    エンドポイントグループの登録内容を変更します。本ボタンをクリックすると、エンドポイントグループ編集画面が表示されます。

  - [**削除**]ボタン

    登録済みのエンドポイントグループを削除します。

⚠ 注意

ユーザーのアクセスレベルがオペレーターの場合は、操作列を表示しません。

3.2.2.1　エンドポイントグループを追加する

新規にエンドポイントグループを登録する手順について説明します。

1. エンドポイントグループ一覧画面を表示します。

   [**グループ管理**] >[**エンドポイントグループ一覧**] をクリックします。

2. [**追加**]ボタンをクリックします。

3. 表示されたエンドポイントグループ追加画面で適切な値を指定します。

   - [**エンドポイントグループ名**]

     エンドポイントグループに対する名前を指定します。最大文字数は 32 文字です。

     以下に示す文字は指定することができません。

     - 記号: , ! " $ ' * + ; < = > ? \ ^ ` { | } ~
     - 先頭および末尾への半角スペース

   - [**対象 IP アドレス**]

     グルーピング対象とするエンドポイントの IP アドレス条件を指定します。以下の条件のうち 1 つ以上を指定する必要があります。

     - 操作ボタン
       * [**追加**]ボタン

         対象 IP アドレスの条件指定のための入力欄を追加します。

       * [**削除**]

         対象 IP アドレスグループ対象の条件指定のための入力欄を削除します。

     - [**IP アドレス**]

       対象のエンドポイントの IPv4 アドレスを 1 つ指定します。

     - [**IP アドレス範囲**]

       対象のエンドポイントの IPv4 アドレスの範囲を指定します。

     - [**ネットワークアドレス**]

       対象エンドポイントの属するネットワークアドレスとネットマスクを指定します。

4. 設定内容を確認し、[**OK**]ボタンをクリックします。

3.2.2.2　エンドポイントグループを更新する

エンドポイントグループの登録情報を更新する手順について説明します。

1. エンドポイントグループ一覧画面を表示します。

   [**グループ管理**] >[**エンドポイントグループ一覧**] をクリックします。

2. エンドポイントグループの一覧で、対象のエンドポイントグループ名の[**編集**]ボタンをクリックします。

3. 表示されたエンドポイントグループ編集画面で内容を変更します。

   - [**エンドポイントグループ名**]

     エンドポイントグループに対する名前を指定します。最大文字数は 32 文字です。

     以下に示す文字は指定することができません。

     - 記号: , ! " $ ' * + ; < = > ? \ ^ ` { | } ~
     - 先頭および末尾への半角スペース

   - [**対象 IP アドレス**]

     グルーピング対象とするエンドポイントの IP アドレス条件を指定します。以下の条件のうち 1 つ以上を指定する必要があります。

     - 操作ボタン
       * [**追加**]ボタン

         対象 IP アドレスの条件指定のための入力欄を追加します。

       * [**削除**]

         対象 IP アドレスグループ対象の条件指定のための入力欄を削除します。

     - [**IP アドレス**]

       対象のエンドポイントの IPv4 アドレスを 1 つ指定します。

     - [**IP アドレス範囲**]

       対象のエンドポイントの IPv4 アドレスの範囲を指定します。

     - [**ネットワークアドレス**]

       対象エンドポイントの属するネットワークアドレスとネットマスクを指定します。

4. 変更内容を確認し、[**OK**]ボタンをクリックします。

3.2.2.3　エンドポイントグループを削除する

エンドポイントグループを削除する手順について説明します。

1. エンドポイントグループ一覧画面を表示します。

[**グループ管理**] >[**エンドポイントグループ一覧**] をクリックします。

2. エンドポイントグループの一覧で、対象のエンドポイントグループ名の[**削除**]ボタンをクリックします。
3. 表示された削除確認ダイアログで内容を確認します。
4. [**OK**]ボタンをクリックし、削除を実行します。

3.3　固有のアプリケーション通信を識別する

NFA では、個々のアプリケーション通信を識別するためのアプリケーション定義機能を提供しています。

アプリケーション定義では、識別条件として一般的に用いられている通信のポート番号と IP プロトコルの条件に加えて、システム固有のアプリケーション通信を識別するために、送信元、または、宛先の IP アドレス、または、ドメインの条件を設定することができます。

3.3.1　アプリケーション定義について

アプリケーション定義の利用方法について説明します。

アプリケーション定義の利用用途

アプリケーションの通信量を分析するためには、そのアプリケーション通信を識別する条件を定義する必要があります。アプリケーション通信の識別方法としては、通信のポート番号と IP プロトコルの情報を見て識別することが一般的です。例えば、http の通信では、80 番ポートを利用した TCP または UDP の通信かどうかで識別することができます。しかし、アプリケーションの仕様によっては、http 通信と同じポート番号、IP プロトコルを利用していたり、http 通信を利用してサービス提供するアプリケーションだったりする場合があります。このような場合には、正確なアプリケーション通信の識別が困難なため、精度の高い通信量分析が行えません。

このような場合に対応するため、NFA では、ポート番号と IP プロトコルの識別条件だけではなく、更に、通信の送信元、または、宛先の IP アドレス、または、ドメインを識別条件に加えたアプリケーション定義を行うことができます。

例えば、特定の業務サーバーが、http 通信を利用した業務サービスを提供していた場合において、この業務サービスの通信と一般的な http 通信とを別々のアプリケーション通信として扱い、それぞれの通信量分析を行うことができるようになります。

アプリケーション定義に対し可能な操作内容

NFA では、アプリケーション定義を追加していくことで、以下の分析操作を行うことができます。

- ダッシュボード画面、および、エクスポーター分析画面の[**アプリケーション**]ウィジェットで、定義したアプリケーションを含むアプリケーションごとの通信量を確認することができます。
- エクスポーター分析画面の[**フィルター条件**]で[**アプリケーション**]に定義したアプリケーション名を指定すると、当該アプリケーションの通信に対する分析結果を各種ウィジェットで確認することができます。
- 定義したアプリケーションの通信量に対し、しきい値監視を設定することができます。

3.3.2　アプリケーション定義を操作する

アプリケーション定義画面について説明します。

アプリケーション定義画面

登録済みのアプリケーション定義の内容確認、および、登録操作を行います。

アプリケーション定義画面は、[**システム管理**] >[**アプリケーション定義**] をクリックして表示します。

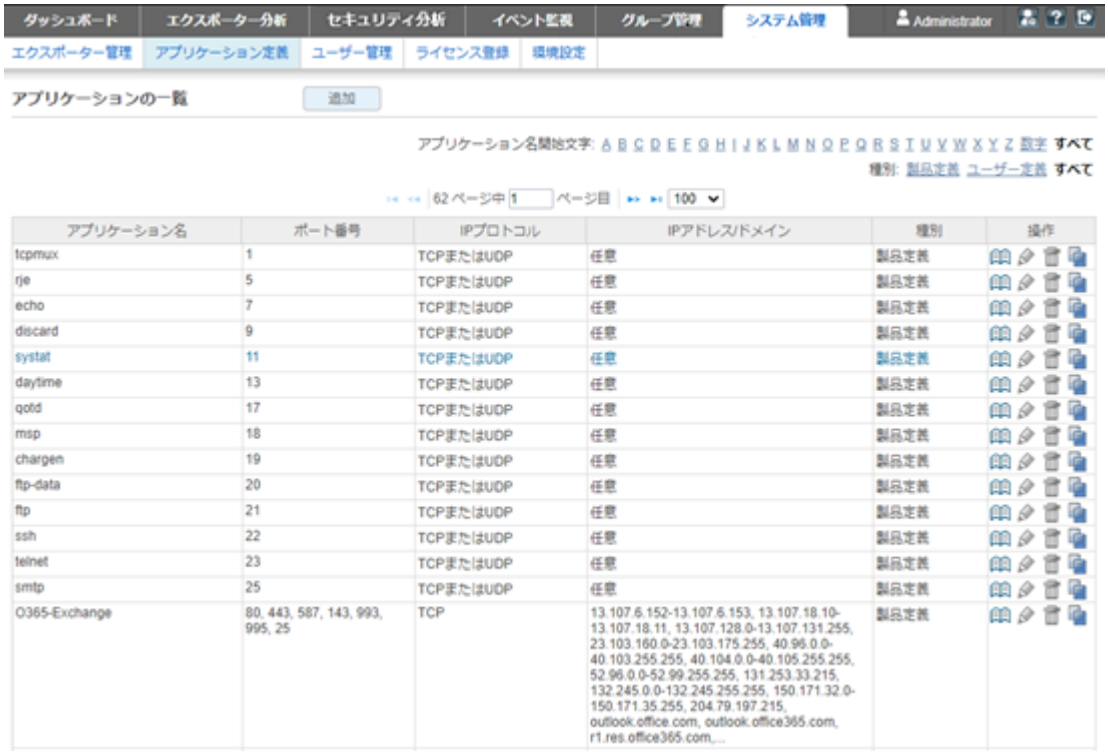

図 3-3　アプリケーション定義画面

ヒント

NFA では、アプリケーション定義として、2025 年 2 月時点で IANA で管理されていたアプリケーションのうち、ポート番号と IP プロトコルの組み合わせで一意にアプリケーションを特定できる定義を標準で取り込んでいます。

機能操作領域

- [**追加**]ボタン

  アプリケーション定義を新規に登録します。本ボタンをクリックすると、アプリケーション追加画面が表示されます。

  ヒント

  アプリケーション定義の追加は、nfa_application_conf コマンドを利用することでも行うことができます。nfa_application_conf コマンドについては、「A.3　nfa_application_conf（176 ページ）」を参照してください。

- [**アプリケーション名開始文字**]

  アプリケーション名の先頭が英数字のものを絞り込んで表示します。「すべて」を選択した場合は、アプリケーション名での絞り込みは行いません。

- [**種別**]

  NFA が提供する[**製品定義**]か、または、ユーザーが作成した[**ユーザー定義**]かで絞り込んで表示します。「すべて」を選択した場合は、種別での絞り込みは行いません。

ヒント

[**アプリケーション名開始文字**]と[**種別**]の両方を指定した場合は、両方の条件を満たす(AND 条件)アプリケーション定義を表示します。

アプリケーションの一覧

- [**アプリケーション名**]

  アプリケーションの名前を表示します。

- [**ポート番号**]

  当該アプリケーションの通信で利用するポート番号を表示します。

- [**IP プロトコル**]

  当該アプリケーションの通信で利用する IP プロトコルを表示します。

- [**IP アドレス/Domain**]

  当該アプリケーションの通信を識別するための IP アドレス条件(特定の IP アドレス、IP アドレス範囲、ネットワークアドレス)、または、ドメイン条件を表示します。

- [**種別**]

  当該アプリケーション定義の種別を表示します。

  - [**製品定義**]

    NFA が標準で提供するアプリケーション定義であることを示します。

  - [**ユーザー定義**]

ユーザーが作成したアプリケーション定義であることを示します。

ヒント

少量フローとして分析するアプリケーション定義には[**少量フローとして分析**]アイコンが表示されます。詳細は「3.3.3　アプリケーション定義での少量フローの分析について（74 ページ）」を参照してください。

- [**操作**]

登録されているアプリケーションに対する操作ボタンを表示します。

- [**詳細**]ボタン

  アプリケーション定義の詳細情報を表示します。本ボタンをクリックすると、アプリケーション詳細画面が表示されます。

- [**編集**]ボタン

  アプリケーション定義の登録内容を変更します。本ボタンをクリックすると、アプリケーション編集画面が表示されます。

  [**ユーザー定義**]のアプリケーション定義に対してのみクリックすることができます。

- [**削除**]ボタン

  登録済みのアプリケーション定義を削除します。

  [**ユーザー定義**]のアプリケーション定義に対してのみクリックすることができます。

- [**コピー**]ボタン

  既存のアプリケーション定義の内容をコピーして、新たなアプリケーション定義を作成します。本ボタンをクリックすると、アプリケーション追加画面が表示されます。

ヒント

アプリケーション定義の更新、削除は、`nfa_application_conf` コマンドを利用することでも行うことができます。`nfa_application_conf` コマンドについては、「A.3　nfa_application_conf（176 ページ）」を参照してください。

3.3.2.1　アプリケーション定義を追加する

新規にアプリケーション定義を追加する手順について説明します。

アプリケーション定義は、以下の 2 つの方法で追加することができます。

- アプリケーション定義画面から 1 つずつ定義を追加する
- `nfa_application_conf` コマンドを利用して複数定義を一括で追加する

ここでは、アプリケーション定義画面から 1 つずつ定義を追加する方法について説明します。

nfa_application_conf コマンドを利用して複数定義を一括で追加する方法については、「A.3　nfa_application_conf（176 ページ）」を参照してください。

1. アプリケーション定義画面を表示します。

   [**システム管理**] >[**アプリケーション定義**] をクリックします。

2. [**追加**]ボタンをクリックします。

3. 表示されたアプリケーション追加画面で適切な値を指定します。

   - [**アプリケーション名**]

     アプリケーションに対する名前を指定します。最大文字数は 32 文字です。

     以下に示す文字は指定することができません。

     - 記号: , ! " $ ' * + ; < = > ? \ ^ ` { | } ~
     - 先頭および末尾への半角スペース

   - [**種別**]

     表示は、必ず、[**ユーザー定義**]となります。

   - [**高度な設定**]

     高度な設定を行うかどうかを指定します。

     [**無効**]を選択した場合は、以下の項目を指定します。

     - [**ポート番号**]

       アプリケーションが利用する送信元、または、宛先のポート番号を指定します。0～65535 の範囲で半角数字を指定します。

       複数のポート番号を指定する場合は、コンマ(,)で区切って指定します。

       ポート番号の範囲を指定する場合は、以下の形式で指定します。

       <開始ポート番号>-<終了ポート番号>

       2 つのエンドポイント(送信元、宛先)のいずれかで指定する必要がありますが、[**IP プロトコル**]の入力値に、[**TCP**]、[**UDP**]、[**TCP または UDP**]の 3 つ以外を指定した場合は、両方のエンドポイント(送信元、宛先)で省略することができます。

     - [**IP プロトコル**]

       アプリケーションが利用する IP プロトコルをプルダウンメニューから選択します。

ヒント

TCP と UDP の両方を利用するアプリケーションに対しては、[**TCP または UDP**]を選択すると、TCP と UDP の両方の通信量を集計した分析結果を得ることができます。

- [**IP アドレス/ドメイン**]

アプリケーションの識別条件として送信元、または、宛先に対する IP アドレス、または、ドメインの条件を指定します。

以下のいずれかを選択します。

* [**任意の IP アドレス/ドメイン**]

  アプリケーションの識別において、IP アドレス、または、ドメインの条件を設定しない場合に選択します。

* [**特定の IP アドレス/ドメイン**]

  アプリケーションの識別のための条件を 1 つ以上指定します。

  + 操作ボタン

    - [**追加**]ボタン

      条件指定のための入力欄を追加します。

    - [**削除**]

      条件指定のための入力欄を削除します。

  + [**IP アドレス**]

    IPv4 アドレスを 1 つ指定します。

  + [**IP アドレス範囲**]

    IPv4 アドレスの範囲を指定します。

  + [**ドメイン**]

    ドメインを 1 つ指定します。最大文字数は、255 文字です。指定可能な文字は、半角英数字、ハイフン(-)、ドット(.)、アスタリスク(*)です。

    アスタリスク(*)はワイルドカードの意味となり、以下のように指定します。

```
*.nec.com
abc.*.nec.com
```

    アスタリスク(*)のみの指定やアスタリスク(*)を 2 つ以上指定することはできません。

    ⚠ 注意

    アスタリスク(*)を用いた指定を行う場合、対象のドメイン名は、IP アドレスからの逆引きで解決できる必要があります。

[**有効**]を選択した場合は、アプリケーションを識別するための条件として以下の項目を指定します。

- [**通信の方向**]
  * [**指定しない**]

    送信元、宛先の[**ポート番号**]、[**IP アドレス/ドメイン**]を意識しない条件を指定する場合に選択します。

  * [**指定する**]

    送信元、宛先の[**ポート番号**]、[**IP アドレス/ドメイン**]を明確に指定する場合に選択します。

    [**送信元**]、[**宛先**]のどちらか一方だけを指定することも可能です。

- [**IP プロトコル**]

  アプリケーションが利用する IP プロトコルをプルダウンメニューから選択します。

  ヒント

  TCP と UDP の両方を利用するアプリケーションに対しては、[**TCP または UDP**]を選択すると、TCP と UDP の両方の通信量を集計した分析結果を得ることができます。

- [**ポート番号**]

  アプリケーションが利用する送信元、または、宛先のポート番号を指定します。0～65535 の範囲で半角数字を指定します。

  複数のポート番号を指定する場合は、コンマ(,)で区切って指定します。

  ポート番号の範囲を指定する場合は、以下の形式で指定します。

  <開始ポート番号>-<終了ポート番号>

  2 つのエンドポイント(送信元、宛先)のいずれかで指定する必要がありますが、[**IP プロトコル**]の入力値に、[**TCP**]、[**UDP**]、[**TCP または UDP**]の 3 つ以外を指定した場合は、両方のエンドポイント(送信元、宛先)で省略することができます。

- [**IP アドレス/ドメイン**]

  アプリケーションの識別条件として送信元、または、宛先に対する IP アドレス、または、ドメインの条件を指定します。

  以下のいずれかを選択します。

  * [**任意の IP アドレス/ドメイン**]

    アプリケーションの識別において、IP アドレス、または、ドメインの条件を設定しない場合に選択します。

  * [**特定の IP アドレス/ドメイン**]

アプリケーションの識別のための条件を 1 つ以上指定します。

+ 操作ボタン
  - [**追加**]ボタン

    条件指定のための入力欄を追加します。
  - [**削除**]

    条件指定のための入力欄を削除します。

+ [**IP アドレス**]

  IPv4 アドレスを 1 つ指定します。

+ [**IP アドレス範囲**]

  IPv4 アドレスの範囲を指定します。

+ [**ドメイン**]

  ドメインを 1 つ指定します。最大文字数は、255 文字です。指定可能な文字は、半角英数字、ハイフン(-)、ドット(.)、アスタリスク(*)です。

  アスタリスク(*)はワイルドカードの意味となり、以下のように指定します。

```
*.nec.com
abc.*.nec.com
```

  アスタリスク(*)のみの指定やアスタリスク(*)を 2 つ以上指定することはできません。

  ⚠ 注意

  アスタリスク(*)を用いた指定を行う場合、対象のドメイン名は、IP アドレスからの逆引きで解決できる必要があります。

- [**少量フローとして分析する**]

  当該アプリケーション定義に一致するフローを少量フローとして分析する対象とするかどうかを指定します。詳細は「3.3.3　アプリケーション定義での少量フローの分析について（74 ページ）」を参照してください。

アプリケーションを識別するための条件は、[**条件を追加する**]の[**追加**]ボタンをクリックすることで追加することができます。また、[**条件を削除する**]の[**削除**]ボタンをクリックすることで、削除することができます。

4. 設定内容を確認し、[**OK**]ボタンをクリックします。

3.3.2.2　アプリケーション定義を更新する

アプリケーション定義の登録情報を更新する手順について説明します。

アプリケーション定義は、以下の 2 つの方法で更新することができます。

- アプリケーション定義画面から 1 つずつ定義を更新する
- `nfa_application_conf` コマンドを利用して複数定義を一括で更新する

ここでは、アプリケーション定義画面から 1 つずつ定義を更新する方法について説明します。

`nfa_application_conf` コマンドを利用して複数定義を一括で更新する方法については、「A.3　nfa_application_conf（176 ページ）」を参照してください。

1. アプリケーション定義画面を表示します。

   [**システム管理**] >[**アプリケーション定義**] をクリックします。

2. アプリケーションの一覧で、対象のアプリケーション名の[**編集**]ボタンをクリックします。

3. 表示されたアプリケーション編集画面で内容を変更します。

   - [**アプリケーション名**]

     アプリケーションに対する名前を指定します。最大文字数は 32 文字です。

     以下に示す文字は指定することができません。

     - 記号: , ! " $ ' * + ; < = > ? \ ^ ` { | } ~
     - 先頭および末尾への半角スペース

   - [**種別**]

     表示は、必ず、[**ユーザー定義**]となります。

   - [**高度な設定**]

     高度な設定を行うかどうかを指定します。

     [**無効**]を選択した場合は、以下の項目を指定します。

     - [**ポート番号**]

       アプリケーションが利用する送信元、または、宛先のポート番号を指定します。0～65535 の範囲で半角数字を指定します。

       複数のポート番号を指定する場合は、コンマ(,)で区切って指定します。

       ポート番号の範囲を指定する場合は、以下の形式で指定します。

       <開始ポート番号>-<終了ポート番号>

       2 つのエンドポイント(送信元、宛先)のいずれかで指定する必要がありますが、[**IP プロトコル**]の入力値に、[**TCP**]、[**UDP**]、[**TCP または UDP**]の 3 つ以外を指定した場合は、両方のエンドポイント(送信元、宛先)で省略することができます。

     - [**IP プロトコル**]

アプリケーションが利用する IP プロトコルをプルダウンメニューから選択します。

ヒント

TCP と UDP の両方を利用するアプリケーションに対しては、[**TCP または UDP**]を選択すると、TCP と UDP の両方の通信量を集計した分析結果を得ることができます。

- [**IP アドレス/ドメイン**]

アプリケーションの識別条件として送信元、または、宛先に対する IP アドレス、または、ドメインの条件を指定します。

以下のいずれかを選択します。

* [**任意の IP アドレス/ドメイン**]

  アプリケーションの識別において、IP アドレス、または、ドメインの条件を設定しない場合に選択します。

* [**特定の IP アドレス/ドメイン**]

  アプリケーションの識別のための条件を 1 つ以上指定します。

  + 操作ボタン

    • [**追加**]ボタン

      条件指定のための入力欄を追加します。

    • [**削除**]

      条件指定のための入力欄を削除します。

  + [**IP アドレス**]

    IPv4 アドレスを 1 つ指定します。

  + [**IP アドレス範囲**]

    IPv4 アドレスの範囲を指定します。

  + [**ドメイン**]

    ドメインを 1 つ指定します。最大文字数は、255 文字です。指定可能な文字は、半角英数字、ハイフン(-)、ドット(.)、アスタリスク(*)です。

    アスタリスク(*)はワイルドカードの意味となり、以下のように指定します。

```
*.nec.com
abc.*.nec.com
```

    アスタリスク(*)のみの指定やアスタリスク(*)を 2 つ以上指定することはできません。

⚠ 注意

アスタリスク(*)を用いた指定を行う場合、対象のドメイン名は、IP アドレスからの逆引きで解決できる必要があります。

[**有効**]を選択した場合は、アプリケーションを識別するための条件として以下の項目を指定します。

- [**通信の方向**]
  * [**指定しない**]

    送信元、宛先の[**ポート番号**]、[**IP アドレス/ドメイン**]を意識しない条件を指定する場合に選択します。

  * [**指定する**]

    送信元、宛先の[**ポート番号**]、[**IP アドレス/ドメイン**]を明確に指定する場合に選択します。

    [**送信元**]、[**宛先**]のどちらか一方だけを指定することも可能です。

- [**IP プロトコル**]

  アプリケーションが利用する IP プロトコルをプルダウンメニューから選択します。

  ヒント

  TCP と UDP の両方を利用するアプリケーションに対しては、[**TCP または UDP**]を選択すると、TCP と UDP の両方の通信量を集計した分析結果を得ることができます。

- [**ポート番号**]

  アプリケーションが利用する送信元、または、宛先のポート番号を指定します。0～65535 の範囲で半角数字を指定します。

  複数のポート番号を指定する場合は、コンマ(,)で区切って指定します。

  ポート番号の範囲を指定する場合は、以下の形式で指定します。

  <開始ポート番号>-<終了ポート番号>

  2 つのエンドポイント(送信元、宛先)のいずれかで指定する必要がありますが、[**IP プロトコル**]の入力値に、[**TCP**]、[**UDP**]、[**TCP または UDP**]の 3 つ以外を指定した場合は、両方のエンドポイント(送信元、宛先)で省略することができます。

- [**IP アドレス/ドメイン**]

  アプリケーションの識別条件として送信元、または、宛先に対する IP アドレス、または、ドメインの条件を指定します。

  以下のいずれかを選択します。

  * [**任意の IP アドレス/ドメイン**]

アプリケーションの識別において、IP アドレス、または、ドメインの条件を設定しない場合に選択します。

* [**特定の IP アドレス/ドメイン**]

  アプリケーションの識別のための条件を 1 つ以上指定します。

  + 操作ボタン

    - [**追加**]ボタン

      条件指定のための入力欄を追加します。

    - [**削除**]

      条件指定のための入力欄を削除します。

  + [**IP アドレス**]

    IPv4 アドレスを 1 つ指定します。

  + [**IP アドレス範囲**]

    IPv4 アドレスの範囲を指定します。

  + [**ドメイン**]

    ドメインを 1 つ指定します。最大文字数は、255 文字です。指定可能な文字は、半角英数字、ハイフン(-)、ドット(.)、アスタリスク(*)です。

    アスタリスク(*)はワイルドカードの意味となり、以下のように指定します。

    ```
    *.nec.com
    abc.*.nec.com
    ```

    アスタリスク(*)のみの指定やアスタリスク(*)を 2 つ以上指定することはできません。

    ⚠ 注意

    アスタリスク(*)を用いた指定を行う場合、対象のドメイン名は、IP アドレスからの逆引きで解決できる必要があります。

- [**少量フローとして分析する**]

  当該アプリケーション定義に一致するフローを少量フローとして分析する対象とするかどうかを指定します。詳細は「3.3.3　アプリケーション定義での少量フローの分析について（74 ページ）」を参照してください。

アプリケーションを識別するための条件は、[**条件を追加する**]の[**追加**]ボタンをクリックすることで追加することができます。また、[**条件を削除する**]の[**削除**]ボタンをクリックすることで、削除することができます。

4. 変更内容を確認し、[**OK**]ボタンをクリックします。

3.3.2.3　アプリケーション定義を削除する

アプリケーション定義を削除する手順について説明します。

アプリケーション定義は、以下の 2 つの方法で削除することができます。

- アプリケーション定義画面から 1 つずつ定義を削除する
- `nfa_application_conf` コマンドを利用して複数定義を一括で削除する

ここでは、アプリケーション定義画面から 1 つずつ定義を削除する方法について説明します。

`nfa_application_conf` コマンドを利用して複数定義を一括で削除する方法については、「A.3　nfa_application_conf（176 ページ）」を参照してください。

削除操作は、[**種別**]が[**ユーザー定義**]のアプリケーション定義に対してのみ行うことができます。

1. アプリケーション定義画面を表示します。

   [**システム管理**] >[**アプリケーション定義**] をクリックします。

2. アプリケーションの一覧で、対象のアプリケーション名の[**削除**]ボタンをクリックします。
3. 表示された削除確認ダイアログで内容を確認します。
4. [**OK**]ボタンをクリックし、削除を実行します。

3.3.3　アプリケーション定義での少量フローの分析について

少量のフローを監視・分析するためのアプリケーション定義の利用方法について説明します。

アプリケーション定義での少量フローの分析の利用用途

NFA では、フローデータを長期間保持するために、受信したフローデータに対して丸め処理を行い、通信量の多い上位のフローに着目した監視・分析を行います。

その弊害として、上位に含まれないが重要な少量のフローや、通信量がしきい値以下になったことを検知するような監視において、下位のフローを正確に監視・分析することができません。

このような場合には、アプリケーション定義の少量フローの分析設定が有効です。少量フローの分析設定を行うことで、当該アプリケーションに合致するフローを丸め処理の対象外とすることができます。それにより、アプリケーション定義を監視対象とした下位のフローを正確に監視・分析することができます。

少量フローの分析設定を行うアプリケーション定義は、以下の条件に合致する必要があります。

- 送信元のポート番号または宛先のポート番号のどちらか一方でも指定されていること
- 送信元の IP アドレス/ドメインと宛先の IP アドレス/ドメインの両方が設定されていること
- ポート番号が単一の指定であること
- IP アドレスが範囲指定でないこと
- ドメインにアスタリスク(*)を含まないこと
- 条件が 1 つだけ設定されていること

設定の方法については「3.3.2.1　アプリケーション定義を追加する（65 ページ）」を参照してください。

⚠ 注意

- 少量フローの分析設定によって丸め処理の対象外となるのは 1 分単位のデータ粒度のみです。1 分粒度以降の丸め処理では、少量フローの分析設定によって保持された下位のフローも処理の対象となります。

  また、少量フローの分析設定によって保持された下位のフローはエクスポーター分析画面でのみグラフに表示されます。

- 少量フローの分析設定により、丸め処理を行わずに保管するフロー情報が増えすぎた場合、ディスク使用量や性能に影響が出る可能性があります。

  目安として、少量フローの分析設定を行うアプリケーション定義の数は最大 50 個程度を推奨しています。

  また、少量フローの分析設定により集約せずに保持するフローの量は、集約された通常のフローの量の 10%以下となるようにしてください。以下のファイルを参照することで 10%を超えているかどうかを確認することができます。

  このファイルには、集約せずに保持するフローの比率が 10%を超えた場合に、対象時刻やエクスポーターの IP アドレスと共に集約されずに保持されたフローの量が出力されます。

  ファイル：

  `<%データディレクトリ%>/collector/flowrate_log/nfa_collector_low_app_flowrate.csv`

  ログ：

```
time,exporter id,ip address,low app flow,additional save rate
    2022-01-13 13:51,1001,192.168.10.1,142,14.2%
```

3.4　特定フローをしきい値で監視する

NFA では、エンドポイント間の通信における特定のフローに対し、通信量のしきい値監視を行うことができます。

3.4.1　しきい値監視について

しきい値監視の利用方法について説明します。

しきい値監視の利用用途

エンドポイント間の特定の通信に対し、突発的な通信量の増加を目視で検知することは困難です。分析対象となる多くのフローがある中で、常に目視で、状況を観察する運用は、作業工数の面から非現実的だと言えます。

このような場合に対応するため、NFA では、エンドポイント間の通信に対し、様々な観点でしきい値を設定し、監視する機能を提供しています。例えば、特定のアプリケーション通信に対してや、特定の宛先 IP アドレスに対する通信に対しての監視設定が行えます。

しきい値監視の機能概要

NFA のしきい値監視機能では、以下の操作を行うことができます。

- 以下のフロー条件を指定して、これに該当するフローの通信量に対し、しきい値監視を行うことができます。
  - 送信元、または、宛先 IP アドレス
  - 送信元、または、宛先エンドポイントグループ
  - 送信元、または、宛先 AS 番号
  - アプリケーション
  - IP プロトコル
  - DSCP

  ヒント

  送信元 IP アドレスとアプリケーションの条件を組み合わせるなど複数条件の指定が可能です。

- しきい値超過の判定は、1 分間隔で、指定した条件に該当するフローの 1 分平均の通信量に対し行います。
- しきい値超過の発生状況を、[**イベント監視**]タブのイベント一覧画面で確認することができます。また、現在発生中のしきい値超過の状況については、ダッシュボード画面の[**カレントアラート**]ウィジェットでも確認することができます。
- しきい値超過、回復の検知時に、そのイベント情報を SNMP トラップで他の運用管理システム(SNMP マネージャー)に送信することができます。

3.4.2　しきい値監視エントリを操作する

しきい値監視エントリ一覧画面について説明します。

しきい値監視エントリ一覧画面

登録済みのしきい値監視エントリの内容確認、および、登録操作を行います。

しきい値監視エントリ一覧画面は、[**イベント監視**] >[**しきい値監視エントリ一覧**] をクリックして表示します。

図 3-4　しきい値監視エントリ一覧画面

機能操作領域

- [**追加**]ボタン

  しきい値監視エントリを新規に登録します。本ボタンをクリックすると、しきい値監視エントリ追加画面が表示されます。

- [**監視状態を変更**]ボタン

  しきい値監視エントリの実行状態に対する変更内容を反映します。

⚠ 注意

ユーザーのアクセスレベルがオペレーターの場合は、本領域の操作ボタンを表示しません。

しきい値監視エントリの一覧

- [**実行**]

  しきい値監視エントリの監視状態を表示します。

  チェック: オン

  監視が開始中であることを示します。

  チェック: オフ

  監視が停止中であることを示します。

- [**エントリ名**]

  しきい値監視エントリの名前を表示します。

- [**フロー条件**]

  監視対象とするフロー条件を表示します。

- [**しきい値**]

  しきい値超過の判定条件(しきい値、連続発生回数)を表示します。

- [**監視対象**]

  フローを監視するエクスポーターおよび、そのインターフェイス名を表示します。

- [**方向**]

  監視対象としている通信フローの向きを表示します。

- [**操作**]

  登録されているしきい値監視エントリに対する操作ボタンを表示します。

  - [**詳細**]ボタン

    しきい値監視エントリの詳細情報を表示します。本ボタンをクリックするとしきい値監視エントリ詳細画面が表示されます。

  - [**編集**]ボタン

    しきい値監視エントリの登録内容を変更します。本ボタンをクリックすると、しきい値監視エントリ編集画面が表示されます。

  - [**削除**]ボタン

    登録済みのしきい値監視エントリを削除します。

注意

ユーザーのアクセスレベルにより、操作ボタンの表示が異なります。

- 管理者

  監視が開始中([**実行**]欄のチェック: オン)のしきい値監視エントリは、[**詳細**]ボタンのみ操作できます。その他のボタンは無効な状態で表示されます。

- オペレーター

  [**詳細**]ボタンのみ操作できます。その他のボタンは表示されません。

3.4.2.1　しきい値監視エントリを追加する

新規にしきい値監視エントリを登録する手順について説明します。

1. しきい値監視エントリ一覧画面を表示します。

   [**イベント監視**] >[**しきい値監視エントリ一覧**] をクリックします。

2. [**追加**]ボタンをクリックします。

3. 表示されたしきい値監視エントリ追加画面で適切な値を指定します。

   - [**エントリ名**]

     しきい値監視エントリに対する名前を指定します。最大文字数は 64 文字です。

以下に示す文字は指定することができません。

- 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
- 先頭および末尾への半角スペース

• [**フロー条件を指定する**]

条件を指定する場合、チェックボックスをオンにします。

また、監視対象とするフローを識別するための条件をプルダウンメニュー([**アプリケーション**] / [**送信元 IP アドレス/ホスト名**] / [**宛先 IP アドレス/ホスト名**] / [**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**] / [**送信元 AS 番号**] / [**宛先 AS 番号**] / [**IP プロトコル**] / [**DSCP**])から選択し、値を設定します。

ヒント

[**送信元 IP アドレス/ホスト名**]と[**アプリケーション**]の条件を組み合わせるなど複数条件の指定が可能です。

送信元 IP アドレス/ホスト名、宛先 IP アドレス/ホスト名に指定できるホスト名は FQDN の形式で指定してください。また、ホスト名の指定にはワイルドカードを表すアスタリスク(*)を含めることができます。

• [**監視対象のインターフェイス**]

どのインターフェイスを経由する通信に対してしきい値監視を行うのか、エクスポーターおよびインターフェイスを指定します。

- [**通信の方向**]

  監視対象とする通信フローの向きを指定します。

  * [**入力**]

    指定インターフェイスにおける入力方向の通信フローを監視対象とします。

  * [**出力**]

    指定インターフェイスにおける出力方向の通信フローを監視対象とします。

  * [**双方向**]

    指定インターフェイスにおける双方向の通信フローの合計値を監視対象とします。

- [**すべて展開**]ボタン

  [**選択済み**]欄、または、[**選択候補**]欄のツリー表示をすべて展開して表示します。

- [**すべて折りたたむ**]ボタン

[**選択済み**]欄、または、[**選択候補**]欄のツリー表示をすべて折りたたんで表示します。

- [**<<追加**]ボタン

  [**選択候補**]欄で選択したインターフェイスを監視対象として[**選択済み**]欄に追加します。

- [**削除>>**]ボタン

  [**選択済み**]欄で選択したインターフェイスを監視対象から削除します。

• [**しきい値設定**]

しきい値超過の判定条件を指定します。

- [**測定値**]

  * [**不等号**]

    [**>**] : 測定値が、しきい値を超えた値の場合にしきい値超過と判定します。

    [**≧**] : 測定値が、しきい値と同じ、または、超えた値の場合にしきい値超過と判定します。

    [**<**] : 測定値が、しきい値を下回った値の場合にしきい値超過と判定します。

    [**≦**] : 測定値が、しきい値と同じ、または、下回った値の場合にしきい値超過と判定します。

  * [**しきい値**]

    しきい値を指定します。0～99999 の範囲で半角数字を指定します。

  * [**単位**]

    しきい値で指定した数値に対する単位をプルダウンメニュー（[**bps**] / [**Kbps**] / [**Mbps**] / [**Gbps**] / [**Tbps**]）から選択します。

- [**連続発生回数 *N***]

  しきい値超過が連続で何回発生した場合にイベント通知を行うのかを指定します。1～1000 の範囲で半角数字を指定します。

ヒント

しきい値監視機能は、丸め処理によって集約された後の通信量の多いフローを対象として監視を行います。そのため、監視対象のフローが丸め処理の対象となった場合には正確な監視を行うことができません。

このような場合には、監視対象のフローをアプリケーションとして定義し、かつ少量フローの分析設定を行うことで、当該フローが集約の対象外となり、正確な監視を行うことができます。

特に、通信量が少ないフローの監視や、下回りを検知する監視においては、少量フローの分析設定を行ったアプリケーション定義を監視するようにしてください。

- [**通知設定**]

  しきい値超過の判定時のイベント通知内容を指定します。

  - [**イベント重要度**]

    しきい値超過のイベントの重要度をプルダウンメニュー([**警告**] / [**異常**])から選択します。

  - [**SNMP トラップによりイベントを通知する**]

    当該しきい値監視エントリで発行するイベントを SNMP トラップ送信する場合、チェックボックスをオンにします。

    ヒント

    SNMP トラップを送信するためには、環境設定画面で送信先に関する設定を行っておく必要があります。詳細は、「2.2.3　SNMP トラップの通知先を設定する (31 ページ)」を参照してください。

4. 設定内容を確認し、[**OK**]ボタンをクリックします。

⚠ 注意

NFA では、指定した条件に該当するフローの 1 分平均の通信量に対し、1 分間隔でしきい値超過の判定処理を行っています。

大量の監視項目を設定した場合は、すべてのしきい値超過の判定処理が 1 分以内に行えず、適切なしきい値監視が行えない状態になる可能性があります。

設定できる監視項目数は、管理するエクスポーターの台数やフローの受信数、マシンスペック等の環境に依存します。ここでの監視項目数とは、各しきい値監視エントリで指定したインターフェイス数の合計値のことを指します。例えば、以下の内容のしきい値監視エントリを設定していた場合、監視項目数は、「7」です。

- エントリ名: エントリ 01

  監視対象インターフェイス:

  - ルーター A のインターフェイス 0/1, 0/2
  - ルーター B のインターフェイス 0/1, 0/2

  エントリ 01 の監視項目数 = 「4」

- エントリ名: エントリ 02

  監視対象インターフェイス:

  - ルーター A のインターフェイス 0/2
  - ルーター C のインターフェイス 0/1, 0/2

  エントリ 02 の監視項目数 = 「3」

設定されている監視項目数で、しきい値判定処理が適切に動作しているかを確認するには、以下のファイルに次のようなログが出力されないことを確認してください。「skipped」というログが出ていれば、処理が 1 分以内に行えなかったことを示しているので、設定されている監視項目数が多すぎる可能性があります。

ファイル :

<%インストールディレクトリ%>/controller/log/com.nec.nfa.threshold.information.log

ログ：

```
2016-12-13 14:51:32.755 INFO   15974 15  threshold monitoring time:
1481608292, 120 entries will be skipped.
```

3.4.2.2　しきい値監視エントリを更新する

しきい値監視エントリの登録情報を更新する手順について説明します。

ヒント

[**エントリ名**]については、変更することができません。

1. しきい値監視エントリ一覧画面を表示します。

   [**イベント監視**] >[**しきい値監視エントリ一覧**] をクリックします。

2. しきい値監視エントリの一覧で、登録情報を更新したいしきい値監視エントリに対する[**編集**]ボタンをクリックします。

3. 表示されたしきい値監視エントリ編集画面で内容を変更します。

   - [**フロー条件を指定する**]

     条件を指定する場合、チェックボックスをオンにします。

     また、監視対象とするフローを識別するための条件をプルダウンメニュー([**アプリケーション**] / [**送信元 IP アドレス/ホスト名**] / [**宛先 IP アドレス/ホスト名**] / [**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**] / [**送信元 AS 番号**] / [**宛先 AS 番号**] / [**IP プロトコル**] / [**DSCP**])から選択し、値を設定します。

     ヒント

     [**送信元 IP アドレス/ホスト名**]と[**アプリケーション**]の条件を組み合わせるなど複数条件の指定が可能です。

     送信元 IP アドレス/ホスト名、宛先 IP アドレス/ホスト名に指定できるホスト名は FQDN の形式で指定してください。また、ホスト名の指定にはワイルドカードを表すアスタリスク(*)を含めることができます。

   - [**監視対象のインターフェイス**]

     どのインターフェイスを経由する通信に対してしきい値監視を行うのか、エクスポーターおよびインターフェイスを指定します。

     - [**通信の方向**]

       監視対象とする通信フローの向きを指定します。

       * [**入力**]

指定インターフェイスにおける入力方向の通信フローを監視対象とします。

* [**出力**]

  指定インターフェイスにおける出力方向の通信フローを監視対象とします。

* [**双方向**]

  指定インターフェイスにおける双方向の通信フローの合計値を監視対象とします。

- [**すべて展開**]ボタン

  [**選択済み**]欄、または、[**選択候補**]欄のツリー表示をすべて展開して表示します。

- [**すべて折りたたむ**]ボタン

  [**選択済み**]欄、または、[**選択候補**]欄のツリー表示をすべて折りたたんで表示します。

- [**<<追加**]ボタン

  [**選択候補**]欄で選択したインターフェイスを監視対象として[**選択済み**]欄に追加します。

- [**削除>>**]ボタン

  [**選択済み**]欄で選択したインターフェイスを監視対象から削除します。

• [**しきい値設定**]

しきい値超過の判定条件を指定します。

- [**測定値**]

  * [**不等号**]

    [**>**] : 測定値が、しきい値を超えた値の場合にしきい値超過と判定します。

    [**≧**] : 測定値が、しきい値と同じ、または、超えた値の場合にしきい値超過と判定します。

    [**<**] : 測定値が、しきい値を下回った値の場合にしきい値超過と判定します。

    [**≦**] : 測定値が、しきい値と同じ、または、下回った値の場合にしきい値超過と判定します。

  * [**しきい値**]

    しきい値を指定します。0～99999 の範囲で半角数字を指定します。

  * [**単位**]

    しきい値で指定した数値に対する単位をプルダウンメニュー（[**bps**] / [**Kbps**] / [**Mbps**] / [**Gbps**] / [**Tbps**]）から選択します。

- [**連続発生回数 *N***]

  しきい値超過が連続で何回発生した場合にイベント通知を行うのかを指定します。1～1000 の範囲で半角数字を指定します。

ヒント

しきい値監視機能は、丸め処理によって集約された後の通信量の多いフローを対象として監視を行います。そのため、監視対象のフローが丸め処理の対象となった場合には正確な監視を行うことができません。

このような場合には、監視対象のフローをアプリケーションとして定義し、かつ少量フローの分析設定を行うことで、当該フローが集約の対象外となり、正確な監視を行うことができます。

特に、通信量が少ないフローの監視や、下回りを検知する監視においては、少量フローの分析設定を行ったアプリケーション定義を監視するようにしてください。

- [**通知設定**]

  しきい値超過の判定時のイベント通知内容を指定します。

  - [**イベント重要度**]

    しきい値超過のイベントの重要度をプルダウンメニュー([**警告**] / [**異常**])から選択します。

  - [**SNMP トラップによりイベントを通知する**]

    当該しきい値監視エントリで発行するイベントを SNMP トラップ送信する場合、チェックボックスをオンにします。

    ヒント

    SNMP トラップを送信するためには、環境設定画面で送信先に関する設定を行っておく必要があります。詳細は、「2.2.3　SNMP トラップの通知先を設定する (31 ページ)」を参照してください。

4. 変更内容を確認し、[**OK**]ボタンをクリックします。

3.4.2.3　しきい値監視エントリを削除する

しきい値監視エントリを削除する手順について説明します。

1. しきい値監視エントリ一覧画面を表示します。

   [**イベント監視**] >[**しきい値監視エントリ一覧**] をクリックします。

2. しきい値監視エントリの一覧で、削除したいしきい値監視エントリに対する[**削除**]ボタンをクリックします。

3. 表示された削除確認ダイアログで内容を確認します。

4. [**OK**]ボタンをクリックし、削除を実行します。

3.5　ローデータの外部出力設定を行う

NFA が受信したすべてのフローデータを、集約前の状態で外部出力するための設定について説明します。

NFA では、フロー数の上限値の設定に従い、通信量の少ないフローデータを 1 つに集約してデータベースに記録しています。

本設定を行うことで、集約処理などの加工を行う前のフローデータをローデータとして外部出力することができます。外部出力したローデータは、簡易的なネットワークフォレンジックとして活用することができます。

本設定後、ローデータは以下のように出力されます。

- 指定ディレクトリの下に各エクスポーターのディレクトリを作成し、15 分毎に自動出力します。
- 15 分間に発生した通信フローのローデータを CSV ファイルへ 10 万件/ファイルで分割して記録し、bzip2 を用いて 1 つにまとめて圧縮します。
- ローデータには、DNS から得られる送信元、および、宛先 IP アドレスに対するドメイン名や NFA が付加するアプリケーションなどの情報は含まれていません。
- ローデータには、NFA の Web コンソールでは表示していない、各フローの TCP フラグの情報が含まれています。

ローデータの外部出力によるディスク使用量は、以下の計算式を用いて見積もりを行うことができます。本設定を行う前に、十分なディスク空き容量があることを確認してください。

- 1 エクスポーターのディスク使用容量 [Bytes] = F × 215 × C × D × 24 × 60
  - F: 当該エクスポーターの 1 分間のフロー数(フローレート)
  - C: ローデータの圧縮率

    「0.06」 を指定して計算します。
  - D: ローデータの保持期間の日数

例:

フローレートが約 300,000 件/分のエクスポーター 5 台のローデータを 1 年間保持する場合

300,000 × 215 × 0.06 × 365 × 24 × 60 × 5 ≒ 9.25 TBytes

⚠ 注意

ローデータを外部出力するためには、一時記録用データベースへの書き込みを有効にしておく必要があります。詳細は、「5.1.4　フロー情報の記録処理方式を変更する（140 ページ）」を参照してください。

1. root ユーザーで NFA サーバーにログインします。

2. NFA のサービスを停止します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ctl.sh stop
```

3. 設定ファイル (collector.conf) を開きます。

   <%データディレクトリ%>/collector/conf/collector.conf

   設定ファイルが存在しない場合は、新規に作成してください。

   ヒント

   collector.conf は、フロー情報の受信用の通信ポート番号の設定変更などでも活用する設定ファイルです。

4. 設定ファイル (collector.conf) に、ローデータの外部出力に関するパラメーターを追記し、保存します。

   指定形式:

```
rawdata.auto-export.output-directory = <Output_Directory>
rawdata.auto-export.retention-days = <Days>
```

   ***Output_Directory*:**

   ローデータを出力するディレクトリのパスを指定します。

   本パラメーターが指定されていない、または、設定値が不正な場合は、ローデータの外部出力は行われません。

   ⚠ 注意

   本パラメーターには、NFA の <%インストールディレクトリ%> および <%データディレクトリ%> 配下のパスは指定しないでください。

   ***Days*:**

   出力したローデータの保持期間の日数を指定します。

   ヒント

   設定ファイル (collector.conf) に本パラメーターを指定していない場合は、以下のパラメーターを指定した場合と同様の動作となります。

```
rawdata.auto-export.retention-days = 1095
```

5. NFA のサービスを起動します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ctl.sh start
```

サービス起動後、ローデータの外部出力に関する設定内容が NFA に反映されます。

3.6　セキュリティ観点でフローを分析・監視する

NFA では、受信したフロー情報をセキュリティの観点で分析・監視し、DoS/DDoS やスキャンの攻撃の疑いを検知することができます。

⚠ 注意

本機能を利用するためには Security Monitoring ライセンスが必要です。

3.6.1　セキュリティ監視について

セキュリティ監視の利用方法について説明します。

セキュリティ監視の利用用途

NFA のセキュリティ監視機能では受信したフローの情報を元に、DoS/DDoS やスキャンの攻撃の疑いを検知する機能を提供しています。

一般的に、このようなネットワークのセキュリティ監視は IDS/IPS を用いてネットワークの境界を重点的に監視しますが、NFA では専用のセキュリティ製品を導入しなくても、エクスポーター単位に様々な監視箇所でセキュリティ観点での簡易的な監視を行うことができます。

セキュリティ監視の機能概要

- 監視対象のインターフェイスを通るフローに対して、2 種類の監視・検知(DoS/DDoS 攻撃またはスキャンの疑いの監視・検知)を行うことができます。

  それぞれの種類ごとに、以下の検知ルールを利用して監視を行うことができます。

  - DoS/DDoS 攻撃の疑いの監視・検知

    DoS/DDoS を検知するルールは以下の通りです。

    * SYN フローの監視

      TCP の接続要求を行う SYN パケットをサーバーに大量に送信し、サーバーのリソースを枯渇させる攻撃を検知します。

      この攻撃は一般的に"SYN Flood"と呼ばれます。

      宛先 IP ごとに、TCP フラグの値が SYN のみの TCP パケットの数をしきい値により監視します。

    * TCP SYN/ACK フローの監視

      踏み台(リフレクター)などを用いて SYN/ACK パケットをサーバーに大量に送信し、サーバーのリソースを枯渇させる攻撃を検知します。

      この攻撃は一般的に"SYN ACK リフレクション"と呼ばれます。

宛先 IP ごとに、TCP フラグの値に SYN と ACK を含み、かつ FIN を含まないペイロード長が短い TCP パケットの数をしきい値により監視します。

* TCP FIN フローの監視

  TCP の切断要求を行う FIN パケットのみをサーバーに大量に送信し、サーバーのリソースを枯渇させる攻撃を検知します。

  この攻撃は一般的に"FIN Flood"と呼ばれます。

  宛先 IP ごとに、TCP フラグの値が FIN のみの TCP パケットの数をしきい値により監視します。

* TCP RST フローの監視

  TCP 通信の中断を行う RST パケットのみをサーバーに大量に送信し、サーバーのリソースを枯渇させる攻撃を検知します。

  この攻撃は一般的に"Stream Flood"と呼ばれます。

  宛先 IP ごとに、TCP フラグの値に RST を含む TCP パケットの数をしきい値により監視します。

- スキャンの疑いの監視・検知

  スキャンを検知するルールは以下の通りです。

* TCP SYN スキャン

  TCP の接続要求を行う SYN パケットを任意のホスト、任意のポートに送信し、サーバーからの応答に応じてポートの利用状態を把握する走査行為を検知します。

  送信元 IP ごとに、TCP フラグの値が SYN のみの TCP パケットが送信された宛先の数(宛先 IP と宛先ポートの組み合わせ)をしきい値により監視します。

* TCP FIN スキャン

  TCP の切断要求を行う FIN パケットを任意のホスト、任意のポートに送信し、サーバーからの応答に応じてポートの利用状態を把握する走査行為を検知します。

  送信元 IP ごとに、TCP フラグの値が FIN のみの TCP パケットが送信された宛先の数(宛先 IP と宛先ポートの組み合わせ)をしきい値により監視します。

* TCP FIN/URG/PSH スキャン

  矛盾した TCP フラグの値(FIN/URG/PSH)のパケットを任意のホスト、任意のポートに送信し、サーバーからの応答に応じてポートの利用状態を把握する走査行為を検知します。

  この攻撃は一般的に"クリスマスツリースキャン"と呼ばれます。

送信元 IP ごとに、TCP フラグの値に FIN/URG/PSH をすべて含む、ペイロード長が短い TCP パケットが送信された宛先の数(宛先 IP と宛先ポートの組み合わせ)をしきい値により監視します。

* TCP NULL スキャン

  TCP フラグの値が 0(NULL)である異常なパケットを任意のホスト、任意のポートに送信し、サーバーからの応答に応じてポートの利用状態を把握する走査行為を検知します。

  送信元 IP ごとに、TCP フラグの値が 0 の TCP パケットが送信された宛先の数(宛先 IP と宛先ポートの組み合わせ)をしきい値により監視します。

- 監視は、条件に一致した被疑となるフローが 1 分間にどれだけ発生したかを監視し、設定されたしきい値を超えた場合にインシデントとして検知します。
- 検知されたインシデントは、イベント発行により通知されます。発行されたイベントは利用者によるインシデントの確認操作に連動して回復されます。
- インシデントの詳細な内容は、発行されたイベントのリンクから遷移できるインシデント詳細画面で確認することができます。
- インシデントの検知状況は、[**イベント監視**]タブのイベント一覧画面で確認することができます。また、未確認のインシデントの検知状況については、ダッシュボード画面の[**カレントアラート**]ウィジェットでも確認することができます。
- インシデントのイベントの発生、回復は、SNMP トラップで他の運用管理システム(SNMP マネージャー)に送信することができます。

ヒント

- 監視を行うための設定は、監視対象のインターフェイスと検知の種類の組ごとに設定します。監視を行う設定の数だけ Security Monitoring ライセンスが必要となります。

  例えば、以下の監視を行う場合、必要な Security Monitoring ライセンスは 3 となります。

  - ルーター A のインターフェイス 0/1 での DDoS 検知
  - ルーター A のインターフェイス 0/1 でのスキャン検知
  - ルーター A のインターフェイス 0/2 での DDoS 検知
- フローは入力、出力インターフェイスの組み合わせの単位で監視されます。逆向きのフローは別々に監視されます。
- 監視対象に、サンプリングによるモニタリングを行うエクスポーターを指定した場合、検知の精度が低下する可能性があります。

⚠ 注意

- 監視対象のエクスポーターの総数が多い場合、性能に影響が出る可能性があります。Security Monitoring ライセンスを割り当てるエクスポーターの総数は 10 台以下にしてください。

3.6.2　セキュリティ監視設定を操作する

セキュリティ監視設定一覧画面について説明します。

セキュリティ監視設定一覧画面

登録済みのセキュリティ監視設定の内容確認、および、登録操作を行います。

セキュリティ監視設定一覧画面は、[**セキュリティ分析**] をクリックして表示します。

図 3-5　セキュリティ監視設定一覧画面

機能操作領域

- [**Security Monitoring ライセンス**]

  現在の Security Monitoring ライセンスの割り当て状況を表示します。

- [**監視状態を変更**]ボタン

  セキュリティ監視設定の[**状態**]に対する変更内容をシステムに反映します。

⚠ 注意

ユーザーのアクセスレベルがオペレーターの場合は、本領域の操作ボタンを表示しません。

DDoS 検知

- [**追加**]ボタン

  DDoS 検知設定を追加します。

- [**状態**]

  監視状態を表示します。

チェックボックスの操作は[**監視状態を変更**]をクリックすることで反映されます。

チェック: オン

監視が開始中であり、Security Monitoring ライセンスが割り当てられていることを示します。

チェック: オフ

監視が停止中であり、Security Monitoring ライセンスが割り当てられていないことを示します。

- [**エクスポーター**]

監視対象のエクスポーター名を表示します。

- [**インターフェイス**]

監視対象のインターフェイス名を表示します。

- [**検知ルール**]

設定されている検知ルールを表示します。

- [**操作**]

登録されている DDoS 検知設定に対する操作ボタンを表示します。

  - [**詳細**]ボタン

    DDoS 検知設定の詳細情報を表示します。本ボタンをクリックすると DDoS 検知設定詳細画面が表示されます。

  - [**編集**]ボタン

    DDoS 検知設定の登録内容を変更します。本ボタンをクリックすると、DDoS 検知設定編集画面が表示されます。

  - [**削除**]ボタン

    登録済みの DDoS 検知設定を削除します。

⚠ 注意

ユーザーのアクセスレベルにより、操作ボタンの表示が異なります。

- 管理者

  状態が開始中([**実行**]欄のチェック: オン)の DDoS 検知設定は、[**詳細**]ボタンのみ操作できます。その他のボタンは無効な状態で表示されます。

- オペレーター

  [**詳細**]ボタンのみ操作できます。その他のボタンは表示されません。

スキャン検知

- [**追加**]ボタン

  スキャン検知設定を追加します。

- [**状態**]

  監視状態を表示します。

  チェックボックスの操作は[**監視状態を変更**]をクリックすることで反映されます。

  チェック: オン

  監視が開始中であり、Security Monitoring ライセンスが割り当てられていることを示します。

  チェック: オフ

  監視が停止中であり、Security Monitoring ライセンスが割り当てられていないことを示します。

- [**エクスポーター**]

  監視対象のエクスポーター名を表示します。

- [**インターフェイス**]

  監視対象のインターフェイス名を表示します。

- [**検知ルール**]

  設定されている検知ルールを表示します。

- [**操作**]

  登録されているスキャン検知設定に対する操作ボタンを表示します。

  - [**詳細**]ボタン

    スキャン検知設定の詳細情報を表示します。本ボタンをクリックするとスキャン検知設定詳細画面が表示されます。

  - [**編集**]ボタン

    スキャン検知設定の登録内容を変更します。本ボタンをクリックすると、スキャン検知設定編集画面が表示されます。

  - [**削除**]ボタン

    登録済みのスキャン検知設定を削除します。

⚠ 注意

- 監視対象のエクスポーターの総数が多い場合、性能に影響が出る可能性があります。Security Monitoring ライセンスを割り当てるエクスポーターの総数は 10 台以下にしてください。

- ユーザーのアクセスレベルにより、操作ボタンの表示が異なります。
  - 管理者

    状態が開始中([**実行**]欄のチェック: オン)のスキャン検知設定は、[**詳細**]ボタンのみ操作できます。その他のボタンは無効な状態で表示されます。
  - オペレーター

    [**詳細**]ボタンのみ操作できます。その他のボタンは表示されません。

3.6.2.1　セキュリティ監視設定を追加する

新規に DDoS 検知設定またはスキャン検知設定を登録する手順について説明します。

1. セキュリティ監視設定一覧画面を表示します。

   [**セキュリティ分析**] をクリックします。
2. DDoS 検知またはスキャン検知の[**追加**]ボタンをクリックします。
3. 表示された DDoS 検知設定追加画面またはスキャン検知設定追加画面で適切な値を指定します。
   - [**検知ルール**]

     検知を行うルールを選択します。

     しきい値は 1～1,000,000,000,000 を指定できます。必要に応じてデフォルト値を適切な値に変更してください。
   - [**監視対象のインターフェイス**]

     どのインターフェイスを経由する通信に対して監視を行うのか、エクスポーターおよびインターフェイスを指定します。
     - [**すべて展開**]ボタン

       [**選択済み**]欄、または、[**選択候補**]欄のツリー表示をすべて展開して表示します。
     - [**すべて折りたたむ**]ボタン

       [**選択済み**]欄、または、[**選択候補**]欄のツリー表示をすべて折りたたんで表示します。
     - [**<<追加**]ボタン

       [**選択候補**]欄で選択したインターフェイスを監視対象として[**選択済み**]欄に追加します。
     - [**削除>>**]ボタン

       [**選択済み**]欄で選択したインターフェイスを監視対象から削除します。

ヒント

以下のインターフェイスは選択候補に表示されません。

- 既に検知設定が行われているインターフェイス。
- インターフェイスライセンスが割り当てられていないインターフェイス。
- IF グループでまとめたインターフェイス。

- [**通知設定**]

  インシデントの発生時のイベント通知内容を指定します。

  - [**イベント重要度**]

    インシデントの発生時のイベントの重要度をプルダウンメニュー([**警告**] / [**異常**])から選択します。

  - [**SNMP トラップによりイベントを通知する**]

    当該検知設定で発行するイベントを SNMP トラップ送信する場合、チェックボックスをオンにします。

    ヒント

    SNMP トラップを送信するためには、環境設定画面で送信先に関する設定を行っておく必要があります。詳細は、「2.2.3　SNMP トラップの通知先を設定する (31 ページ)」を参照してください。

4. 設定内容を確認し、[**OK**]ボタンをクリックします。

ヒント

- 複数のインターフェイスを選択した状態で追加を行った場合、インターフェイスごとに設定が登録されます。

⚠ 注意

セキュリティ監視機能では、監視対象に指定されたインターフェイスを通るすべてのフローに対し、1 分間隔で分析、集計を行い検知の判定処理を行っています。

マシンスペックやフローの受信数によってはすべての検知の判定処理が 1 分以内に行えず、適切な監視が行えない状態になる可能性があります。

設定されている監視の設定で、検知の判定処理が適切に動作しているかを確認するには、以下のファイルに次のようなログが出力されないことを確認してください。「skipped」というログが出ていれば、処理が 1 分以内に行えなかったことを示しているので、設定の見直しを行ってください。

ファイル：

<%*インストールディレクトリ*%>/controller/log/security-monitoring.log

ログ：

```
2023-10-23   15:52:31.755   INFO        15980   15      Skipped   monitoring.
[ExporterID=1012, TargetTime=2023-10-23 15:51]
```

上記のログが繰り返し出力されている場合は、監視対象となっているエクスポーターの数やインターフェイスの数を減らし、負荷を軽減してください。

3.6.2.2　セキュリティ監視設定を更新する

DDoS 検知設定またはスキャン検知設定の登録情報を更新する手順について説明します。

1. セキュリティ監視設定一覧画面を表示します。

   [**セキュリティ分析**] をクリックします。

2. セキュリティ監視設定一覧で、登録情報を更新したい検知設定に対する[**編集**]ボタンをクリックします。

3. 表示された DDoS 検知設定編集画面またはスキャン検知設定編集画面で内容を変更します。

   - [**検知ルール**]

     検知を行うルールを選択します。

     しきい値は 1～1,000,000,000,000 を指定できます。必要に応じてデフォルト値を適切な値に変更してください。

   - [**通知設定**]

     インシデントの発生時のイベント通知内容を指定します。

     - [**イベント重要度**]

       インシデントの発生時のイベントの重要度をプルダウンメニュー([**警告**] / [**異常**])から選択します。

     - [**SNMP トラップによりイベントを通知する**]

       当該検知設定で発行するイベントを SNMP トラップ送信する場合、チェックボックスをオンにします。

       ヒント

       SNMP トラップを送信するためには、環境設定画面で送信先に関する設定を行っておく必要があります。詳細は、「2.2.3　SNMP トラップの通知先を設定する (31 ページ)」を参照してください。

4. 変更内容を確認し、[**OK**]ボタンをクリックします。

3.6.2.3　セキュリティ監視設定を削除する

DDoS 検知設定またはスキャン検知設定を削除する手順について説明します。

1. セキュリティ監視設定一覧画面を表示します。

   [**セキュリティ分析**] をクリックします。

2. セキュリティ監視設定一覧で、削除したい検知設定に対する[**削除**]ボタンをクリックします。
3. 表示された削除確認ダイアログで内容を確認します。
4. [**OK**]ボタンをクリックし、削除を実行します。

第 4 章
運用操作

NFA の運用時の操作方法について説明します。

目次

4.1 現在のネットワーク状況を確認する 98
4.2 エクスポーターごとにフローの詳細を分析する 108
4.3 蓄積データや分析結果を外部に出力する 117
4.4 ローデータを確認する 121
4.5 フローレートを確認する 124
4.6 イベント情報を確認する 126
4.7 セキュリティ監視の検知結果を確認する 128
4.8 ユーザーの操作履歴を確認する 133

4.1　現在のネットワーク状況を確認する

NFA では、ログインしたユーザーが、担当するネットワーク範囲の現在の状況を即座に把握できるように、ダッシュボード機能を提供しています。

4.1.1　ダッシュボードについて

ダッシュボードの利用方法について説明します。

ダッシュボードの利用用途

ダッシュボードは、管理担当のネットワーク範囲が、現在どのような通信状況になっているのかを即座に確認できるホーム画面として提供しています。

ダッシュボードでは、担当するネットワーク範囲の全体状況を見渡すような運用を想定しており、複数のエクスポーターの各インターフェイスを流れる通信状況を比較、分析することや、担当するネットワーク範囲でのしきい値超過発生状況を確認することができます。また、全体の通信傾向から、フロー条件を絞り込んでいき、より詳細な分析へとドリルダウンしていく、最初の画面としても活用できます。

ダッシュボードで可能な操作内容

NFA が提供するダッシュボードでは、以下の分析操作を行うことができます。

- 各ウィジェットで複数のエクスポーターの各インターフェイスの通信に対し、通信量の比較、分析を行うことができます。
- NFA にログインするユーザーごとに最初に表示するダッシュボード内容を自由に定義することができます。
- 運用中にネットワークの状況に合わせて、登録済みの他のダッシュボード定義に切り替えて、フローの状況を確認することができます。
- 各ウィジェットの一覧のリンクをクリックし、分析条件を絞り込んだ状態でエクスポーター分析画面にジャンプ(ドリルダウン分析)することができます。
- 各ウィジェットでの分析結果を CSV ファイル形式で外部出力することができます。

4.1.2　ダッシュボード表示画面を操作する

ダッシュボード画面について説明します。

ダッシュボード画面

各種ウィジェットにより、分析対象のエクスポーターおよびインターフェイスを流れる現在の通信状況を確認することができます。

ダッシュボード画面は、NFA へのログイン後、最初に表示されます。また、[**ダッシュボード**]タブをクリックすることでも表示することができます。

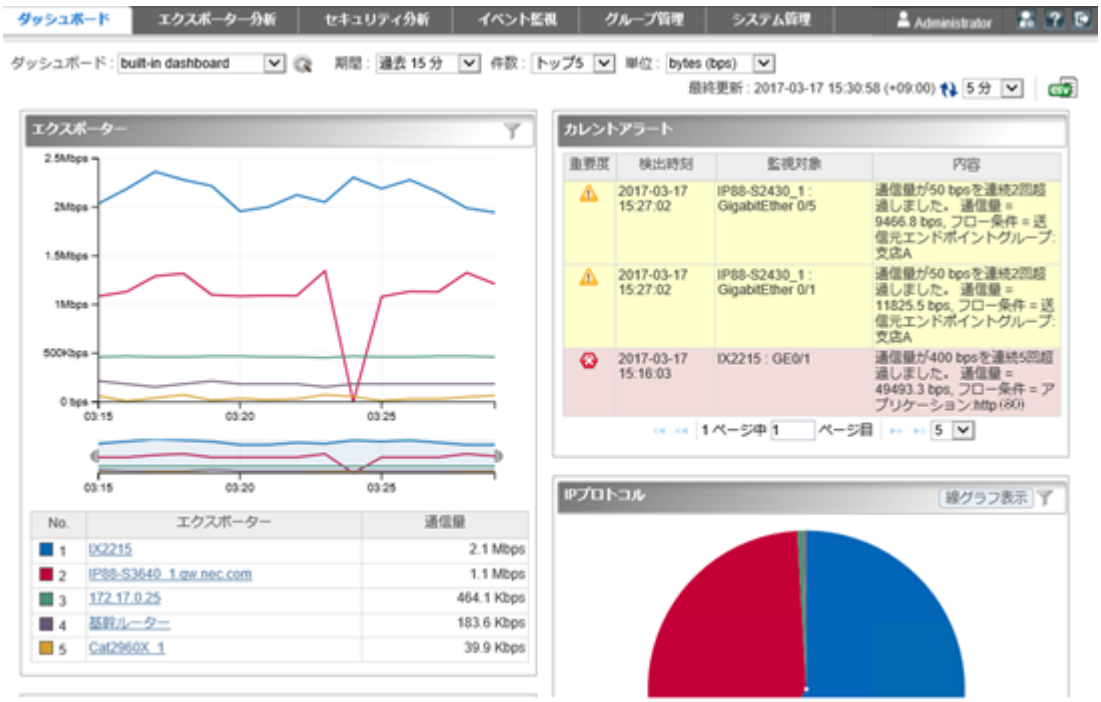

図 4-1　ダッシュボード表示画面

機能操作領域

- [**ダッシュボード名**]

  登録済みのダッシュボード定義をプルダウンメニューから選択します。ダッシュボードで表示する分析内容を切り替えることができます。

- [**ダッシュボード管理**]ボタン

  登録済みのダッシュボード定義の内容を確認したり、ダッシュボード定義を追加、更新、削除します。本ボタンをクリックすると、ダッシュボード管理画面が表示されます。

- [**期間**]

  分析対象とするフローの分析期間をプルダウンメニュー（[**過去 15 分**] / [**過去 30 分**] / [**過去 1 時間**] / [**過去 6 時間**] / [**過去 24 時間**] / [**過去 48 時間**] / [**過去 72 時間**]）から選択します。デフォルト値は[**過去 15 分**]です。

- [**件数**]

  ダッシュボードの各ウィジェットで表示する上位データの表示件数をプルダウンメニュー([**トップ 5**] / [**トップ 10**] / [**トップ 20**])から選択します。デフォルト値は[**トップ 5**]です。

ただし、円グラフ/折れ線グラフのウィジェットの場合、指定件数以下の項目をまとめて「その他」として表示します。よって、グラフ上の表示項目数は、「指定件数+1」件になります。

- [**単位**]

  ダッシュボードの各ウィジェットで表示する通信量の表示単位をプルダウンメニュー([**bytes (bps)**] / [**packets (pps)**])から選択します。デフォルト値は[**bytes (bps)**]です。

- [**最終更新**]

  最終の更新日時を表示します。

- [**更新**]ボタン

  ダッシュボード上のすべてのウィジェットの分析結果を最新の内容に更新します。

- [**更新間隔**]

  ダッシュボードの各ウィジェットの分析結果表示の更新間隔をプルダウンメニュー([**1 分**] / [**5 分**] / [**15 分**] / [**なし**])から選択します。デフォルト値は[**5 分**]です。

- [**CSV 出力**]

  ダッシュボード上のすべてのウィジェットの分析結果を CSV ファイル形式で出力します。詳細は、「4.3.2　分析結果を画面から CSV ファイルで出力する（117 ページ）」を参照してください。

ウィジェット表示領域

ウィジェットを表示します。ダッシュボードに表示する各ウィジェットの操作については、「1.2.5　ウィジェットを操作する（18 ページ）」を参照してください。

4.1.3　ダッシュボード定義を操作する

ダッシュボード管理画面について説明します。

ダッシュボード管理画面

登録済みのダッシュボード定義の内容確認、および、登録操作を行います。

ダッシュボード管理画面は、ダッシュボード画面の[**ダッシュボード管理**]ボタンをクリックして表示します。

図 4-2　ダッシュボード管理画面

機能操作領域

- [**追加**]ボタン

  ダッシュボード定義を新規に登録します。本ボタンをクリックすると、ダッシュボード追加画面が表示されます。

ダッシュボードの一覧

- [**ダッシュボード名**]

  ダッシュボード定義に対する名前を表示します。

  ヒント

  ✔マークは、ログインしているユーザーの[**デフォルトのダッシュボード**]で設定しているダッシュボード定義であることを示します。

- [**説明**]

  ダッシュボードの定義内容に対する説明を表示します。

- [**操作**]

  登録されているダッシュボードに対する操作ボタンを表示します。

  - [**編集**]ボタン

    ダッシュボード定義の登録内容を変更します。本ボタンをクリックすると、ダッシュボード編集画面が表示されます。

  - [**削除**]ボタン

    登録済みのダッシュボード定義を削除します。

  - [**コピー**]ボタン

    既存のダッシュボード定義の内容をコピーして、新たなダッシュボード定義を作成します。本ボタンをクリックすると、ダッシュボード追加画面が表示されます。

  ⚠ 注意

  ユーザーのアクセスレベルにより、操作ボタンの表示が異なります。

- 管理者

  初期状態から登録されている「built-in dashboard」は、[**コピー**]ボタンのみ操作できます。その他のボタンは無効な状態で表示されます。

- オペレーター

  ログインしているユーザーが作成したダッシュボード定義のみ、すべての操作が行えます。

  他のユーザーが作成したダッシュボード定義は、[**コピー**]ボタンのみ操作できます。その他のボタンは表示されません。

4.1.3.1　ダッシュボード定義を追加する

新規にダッシュボード定義を登録する手順について説明します。

1. ダッシュボード管理画面を表示します。

   ダッシュボード画面の[**ダッシュボード管理**]ボタンをクリックします。

2. [**追加**]ボタンをクリックします。

   ヒント

   既存のダッシュボード定義をもとに新しいダッシュボード定義を作成したい場合は、ダッシュボードの一覧から、もとになるダッシュボード定義の[**コピー**]ボタンをクリックし、ダッシュボード追加画面を表示します。

3. 表示されたダッシュボード追加画面で適切な値を指定します。

   - [**ダッシュボード名**]

     ダッシュボード定義に対する名前を指定します。最大文字数は 32 文字です。

     以下に示す文字は指定することができません。

     - 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
     - 先頭および末尾への半角スペース

   - [**説明**]

     当該ダッシュボード定義の利用目的や内容に関する説明を任意の文字で指定します。最大文字数は 1024 文字です。

   - [**表示のデフォルト設定**]

     当該ダッシュボード定義でダッシュボードを表示した直後の表示設定に対するデフォルト値を指定します。

     - [**期間**]

       分析対象とするフローの分析期間をプルダウンメニュー（[**過去 15 分**] / [**過去 30 分**] / [**過去 1 時間**] / [**過去 6 時間**] / [**過去 24 時間**] / [**過去 48 時間**] / [**過去 72 時間**]）から選択します。デフォルト値は[**過去 15 分**]です。

- [**件数**]

  各ウィジェットで表示する上位データの表示件数をプルダウンメニュー（[**トップ 5**] / [**トップ 10**] / [**トップ 20**]）から選択します。デフォルト値は[**トップ 5**]です。

- [**単位**]

  各ウィジェットで表示する通信量の表示単位をプルダウンメニュー（[**bytes (bps)**] / [**packets (pps)**]）から選択します。デフォルト値は[**bytes (bps)**]です。

- [**描画更新間隔**]

  各ウィジェットの分析結果表示の更新間隔をプルダウンメニュー（[**1 分**] / [**5 分**] / [**15 分**] / [**なし**]）から選択します。デフォルト値は[**5 分**]です。

4. ウィジェットを追加します。

   a. [**ウィジェット追加**]ボタンをクリックし、ウィジェットの追加ダイアログを表示します。

   b. ダッシュボードに追加したいウィジェットのチェックボックスをオンにします。

      選択できるウィジェットの詳細については、「1.2.4　ウィジェットの種類（15 ページ）」を参照してください。

   c. 設定内容を確認し、[**OK**]ボタンをクリックします。

      選択したウィジェットがダッシュボード追加画面に反映されます。

ヒント

1 つのダッシュボード定義に追加できるウィジェットの最大数は 20 です。

5. ウィジェットの表示タイトルや分析対象を細かく指定します。

   a. ウィジェットの[**編集**]ボタンをクリックし、ウィジェット設定画面を表示します。

   - [**表示タイトル**]

     ウィジェットに対するタイトルを指定します。最大文字数は 32 文字です。

     以下に示す文字は指定することができません。

     - 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
     - 先頭および末尾への半角スペース

     デフォルト値はウィジェットの種類名です。

   - [**件数**]

     [**件数**]をプルダウンメニュー（[**デフォルト設定を使う**] / [**トップ 5**] / [**トップ 10**] / [**トップ 20**]）から選択します。デフォルト値は[**トップ 5**]です。

     特定のウィジェットで、ダッシュボード追加画面の[**表示のデフォルト設定**]で指定したものと異なる件数で表示させたい場合に指定します。

- [**分析対象**]

  以下から選択します。

  - [**すべてのエクスポーター**]

    NFA に登録しているすべてのエクスポーターのすべてのインターフェイスが分析対象となります。

  - [**特定のエクスポーター**]

    NFA に登録しているエクスポーターの中から分析対象を選択します。

    [**選択候補**]欄から分析対象としたいエクスポーターを選択し、[**追加**]ボタンをクリックします。

  - [**特定のインターフェイス**]

    NFA に登録しているインターフェイスの中から分析対象を選択します。

    [**選択候補**]欄から分析対象としたいエクスポーターのインターフェイスを選択し、[**追加**]ボタンをクリックします。

    ヒント

    「エクスポーター」ウィジェットには表示されません。

- [**通信の方向**]

  分析対象に[**特定のインターフェイス**]を選択した場合には、監視対象とする通信フローの向きを指定できます。

  - [**入力**]

    指定インターフェイスにおける入力方向の通信フローを監視対象とします。

  - [**出力**]

    指定インターフェイスにおける出力方向の通信フローを監視対象とします。

  - [**双方向**]

    指定インターフェイスにおける双方向の通信フローの合計値を監視対象とします。

b. 設定内容を確認し、[**OK**]ボタンをクリックします。

6. ウィジェットに表示するグラフのタイプを設定します。

   ウィジェットの[**線グラフ表示**]/[**円グラフ表示**]ボタンをクリックし、グラフ表示タイプを設定します。

   ヒント

   ウィジェットの種類によっては、[**線グラフ表示**]/[**円グラフ表示**]ボタンは表示されません。

[**線グラフ表示**]ボタンをクリックすると線グラフ、[**円グラフ表示**]ボタンをクリックすると円グラフに切り替わります。

7. ウィジェットの表示を調整します。
   - ウィジェットの配置を変更する場合

     ウィジェットにカーソルを重ねてドラッグし、移動先でドロップします。
   - 不要なウィジェットを削除する場合

     ウィジェットの[**削除**]ボタンをクリックします。
8. 設定内容を確認し、[**OK**]ボタンをクリックします。

4.1.3.2　ダッシュボード定義を更新する

ダッシュボード定義の登録情報を更新する手順について説明します。

1. ダッシュボード管理画面を表示します。

   ダッシュボード画面の[**ダッシュボード管理**]ボタンをクリックします。
2. ダッシュボードの一覧で、対象のダッシュボード名の[**編集**]ボタンをクリックします。
3. 表示されたダッシュボード編集画面で内容を変更します。

   以下のすべての項目の変更を行うことができます。
   - [**ダッシュボード名**]

     ダッシュボード定義に対する名前を指定します。最大文字数は 32 文字です。

     以下に示す文字は指定することができません。
     - 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
     - 先頭および末尾への半角スペース
   - [**説明**]

     当該ダッシュボード定義の利用目的や内容に関する説明を任意の文字で指定します。最大文字数は 1024 文字です。
   - [**表示のデフォルト設定**]

     当該ダッシュボード定義でダッシュボードを表示した直後の表示設定に対するデフォルト値を指定します。
     - [**期間**]

       分析対象とするフローの分析期間をプルダウンメニュー（[**過去 15 分**] / [**過去 30 分**] / [**過去 1 時間**] / [**過去 6 時間**] / [**過去 24 時間**] / [**過去 48 時間**] / [**過去 72 時間**]）から選択します。デフォルト値は[**過去 15 分**]です。
     - [**件数**]

各ウィジェットで表示する上位データの表示件数をプルダウンメニュー（[**トップ 5**] / [**トップ 10**] / [**トップ 20**]）から選択します。デフォルト値は[**トップ 5**]です。

- [**単位**]

  各ウィジェットで表示する通信量の表示単位をプルダウンメニュー（[**bytes (bps)**] / [**packets (pps)**]）から選択します。デフォルト値は[**bytes (bps)**]です。

- [**描画更新間隔**]

  各ウィジェットの分析結果表示の更新間隔をプルダウンメニュー（[**1 分**] / [**5 分**] / [**15 分**] / [**なし**]）から選択します。デフォルト値は[**5 分**]です。

4. ウィジェットを追加します。

   a. [**ウィジェット追加**]ボタンをクリックし、ウィジェットの追加ダイアログを表示します。

   b. ダッシュボードに追加したいウィジェットのチェックボックスをオンにします。

   選択できるウィジェットの詳細については、「1.2.4　ウィジェットの種類（15 ページ）」を参照してください。

   c. 設定内容を確認し、[**OK**]ボタンをクリックします。

   選択したウィジェットがダッシュボード追加画面に反映されます。

5. ウィジェットの表示タイトルや分析対象を変更します。

   a. ウィジェットの[**編集**]ボタンをクリックし、ウィジェット設定画面を表示します。

   - [**表示タイトル**]

     ウィジェットに対するタイトルを指定します。最大文字数は 32 文字です。

     以下に示す文字は指定することができません。

     - 記号: ! " $ ' * + ; < = > ? \ ^ ` { | } ~
     - 先頭および末尾への半角スペース

     デフォルト値はウィジェットの種類名です。

   - [**件数**]

     [**件数**]をプルダウンメニュー（[**デフォルト設定を使う**] / [**トップ 5**] / [**トップ 10**] / [**トップ 20**]）から選択します。デフォルト値は[**トップ 5**]です。

     特定のウィジェットで、ダッシュボード追加画面の[**表示のデフォルト設定**]で指定したものと異なる件数で表示させたい場合に指定します。

   - [**分析対象**]

     以下から選択します。

     - [**すべてのエクスポーター**]

NFA に登録しているすべてのエクスポーターのすべてのインターフェイスが分析対象となります。

- [**特定のエクスポーター**]

  NFA に登録しているエクスポーターの中から分析対象を選択します。

  [**選択候補**]欄から分析対象としたいエクスポーターを選択し、[**追加**]ボタンをクリックします。

- [**特定のインターフェイス**]

  NFA に登録しているインターフェイスの中から分析対象を選択します。

  [**選択候補**]欄から分析対象としたいエクスポーターのインターフェイスを選択し、[**追加**]ボタンをクリックします。

ヒント

「エクスポーター」ウィジェットには表示されません。

- [**通信の方向**]

  分析対象に[**特定のインターフェイス**]を選択した場合には、監視対象とする通信フローの向きを指定できます。

  - [**入力**]

    指定インターフェイスにおける入力方向の通信フローを監視対象とします。

  - [**出力**]

    指定インターフェイスにおける出力方向の通信フローを監視対象とします。

  - [**双方向**]

    指定インターフェイスにおける双方向の通信フローの合計値を監視対象とします。

b. 設定内容を確認し、[**OK**]ボタンをクリックします。

6. ウィジェットに表示するグラフのタイプを変更します。

   ウィジェットの[**線グラフ表示**]/[**円グラフ表示**]ボタンをクリックし、グラフ表示タイプを設定します。

ヒント

ウィジェットの種類によっては、[**線グラフ表示**]/[**円グラフ表示**]ボタンは表示されません。

[**線グラフ表示**]ボタンをクリックすると線グラフ、[**円グラフ表示**]ボタンをクリックすると円グラフに切り替わります。

7. ウィジェットの表示を調整します。

- ウィジェットの配置を変更する場合

  ウィジェットにカーソルを重ねてドラッグし、移動先でドロップします。

- 不要なウィジェットを削除する場合

  ウィジェットの[**削除**]ボタンをクリックします。

8. 変更内容を確認し、[**OK**]ボタンをクリックします。

4.1.3.3　ダッシュボード定義を削除する

ダッシュボード定義を削除する手順について説明します。

1. ダッシュボード管理画面を表示します。

   ダッシュボード画面の[**ダッシュボード管理**]ボタンをクリックします。

2. ダッシュボードの一覧で、対象のダッシュボード名の[**削除**]ボタンをクリックします。
3. 表示された削除確認ダイアログで内容を確認します。
4. [**OK**]ボタンをクリックし、削除を実行します。

4.2　エクスポーターごとにフローの詳細を分析する

NFA では、エクスポーター、および、そのインターフェイスを指定し、フローの監視箇所を特定した上で、フローの詳細分析を行っていきます。ここでは、現在、過去のフローの詳細を分析するためのエクスポーター分析機能について説明します。

4.2.1　エクスポーター分析について

エクスポーター分析の利用方法について説明します。

エクスポーター分析の利用用途

エクスポーター分析では、特定のエクスポーター、または、インターフェイスに焦点をあて、そこを経由する通信の詳細なフローを分析します。また、ダッシュボードでの分析とは異なり、現在の状況だけではなく、過去にさかのぼって、フローの状況を確認することができます。

エクスポーター分析は、ダッシュボードでの全体状況の観察時に異常を検出し、その原因をドリルダウンして調査したい場合や、ネットワークの障害の発生時に、発生当時の通信状況を詳しく確認する場合に活用します。

エクスポーター分析で可能な操作内容

NFA が提供するエクスポーター分析では、以下の分析操作を行うことができます。

- 過去の特定の日時を指定して、一定期間のフローを詳細に分析することができます。
- 複数のフィルター条件(例えば、送信元 IP アドレス/ホスト名やアプリケーションなど)を指定してフローを絞り込み、詳細な分析を行っていくことができます。フィルター条件の指定は、各ウィジェットの一覧のリンクをクリックでも行うことができます。
- 各ウィジェットでの分析結果を CSV ファイル形式で外部出力することができます。

4.2.2　エクスポーター分析画面を操作する

エクスポーター分析画面について説明します。

エクスポーター分析画面

フローを特定するための様々な条件を指定していくことで、フローの詳細な状況を分析していくことができます。

エクスポーター分析画面は、[**エクスポーター分析**]タブをクリックして表示します。

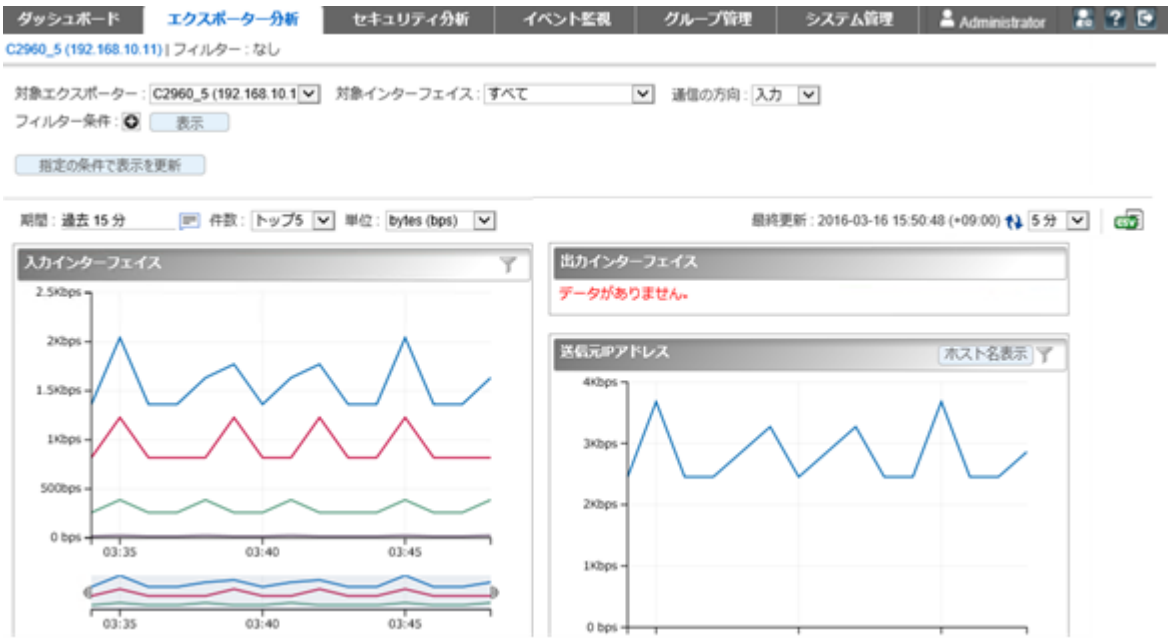

図 4-3　エクスポーター分析画面

機能操作領域

- 分析対象
  - [**対象エクスポーター**]

    分析対象のエクスポーターを選択します。
  - [**対象インターフェイス**]

    [**対象エクスポーター**]で選択したエクスポーターにおける分析対象のインターフェイスをプルダウンメニューから選択します。

- [**通信の方向**]

  [**対象インターフェイス**]で選択したインターフェイスに対して、監視対象とする通信フローの向きを指定できます。

  * [**入力**]

    選択したインターフェイスにおける入力方向の通信フローを監視対象とします。

  * [**出力**]

    選択したインターフェイスにおける出力方向の通信フローを監視対象とします。

  * [**双方向**]

    選択したインターフェイスにおける双方向の通信フローの合計値を監視対象とします。

ヒント

インターフェイスライセンスの割り当てが行われているエクスポーターおよびインターフェイスが選択対象となります。

- [**フィルター条件**]

分析対象のフローを絞り込みたい場合に指定します。

- 操作ボタン

  * [**追加**]ボタン

    [**フィルター条件**]の入力欄を追加します。この場合、追加した条件をすべて満たす(AND 条件)フローを分析対象とします。

  * [**削除**]

    [**フィルター条件**]の入力欄を削除します。

  * [**表示**]/ [**非表示**]ボタン

    [**フィルター条件**]の表示を、表示したり、非表示にしたりすることができます。

    各ウィジェットで分析結果を表示する際に、画面のスペースをできる限り、分析結果の表示にあてたい場合に活用します。

- 条件指定

  以下の条件を指定できます。

  * [**送信元 IP アドレス/ホスト名**]

    指定した IP アドレスまたはホストからの通信に絞って、以下の観点で分析します。

    + どの IP アドレス宛の通信が多いのか

+ 何のアプリケーションの通信が多いのか
+ 何の IP プロトコルを利用した通信が多いのか
+ どの DSCP 値(PHB)の通信が多いのか

* [**宛先 IP アドレス/ホスト名**]

  指定した IP アドレスまたはホスト宛の通信に絞って、以下の観点で分析します。

  + どの IP アドレスからの通信が多いのか
  + 何のアプリケーションの通信が多いのか
  + 何の IP プロトコルを利用した通信が多いのか
  + どの DSCP 値(PHB)の通信が多いのか

* [**送信元エンドポイントグループ**]

  指定したエンドポイントグループに属する IP アドレスからの通信に絞って、以下の観点で分析します。

  + グループ内のどの IP アドレスからの通信が多いのか
  + どの IP アドレス宛の通信が多いのか
  + 何のアプリケーションの通信が多いのか
  + 何の IP プロトコルを利用した通信が多いのか
  + どの DSCP 値(PHB)の通信が多いのか

* [**宛先エンドポイントグループ**]

  指定したエンドポイントグループに属する IP アドレス宛の通信に絞って、以下の観点で分析します。

  + グループ内のどの IP アドレス宛の通信が多いのか
  + どの IP アドレスからの通信が多いのか
  + 何のアプリケーションの通信が多いのか
  + 何の IP プロトコルを利用した通信が多いのか
  + どの DSCP 値(PHB)の通信が多いのか

* [**アプリケーション**]

  指定したアプリケーションの通信に絞って、以下の観点で分析します。

  + どの IP アドレスからの通信が多いのか
  + どの IP アドレス宛の通信が多いのか
  + どの DSCP 値(PHB)の通信が多いのか

* [**IP プロトコル**]

  指定した IP プロトコルの通信に絞って、以下の観点で分析します。

  + どの IP アドレスからの通信が多いのか
  + どの IP アドレス宛の通信が多いのか
  + 何のアプリケーション通信が多いのか
  + どの DSCP 値(PHB)の通信が多いのか

* [**DSCP**]

  指定した DSCP の通信に絞って、以下の観点で分析します。

  + どの IP アドレスからの通信が多いのか
  + どの IP アドレス宛の通信が多いのか
  + 何のアプリケーション通信が多いのか
  + 何の IP プロトコルを利用した通信が多いのか

* [**送信元 AS 番号**]

  指定した AS 番号のネットワークからの通信に絞って、以下の観点で分析します。

  + どの AS 番号のネットワークへの通信が多いのか
  + どの IP アドレスからの通信が多いのか
  + どの IP アドレス宛の通信が多いのか
  + 何のアプリケーションの通信が多いのか
  + 何の IP プロトコルを利用した通信が多いのか
  + どの DSCP 値(PHB)の通信が多いのか

* [**宛先 AS 番号**]

  指定した AS 番号のネットワークへの通信に絞って、以下の観点で分析します。

  + どの AS 番号のネットワークからの通信が多いのか
  + どの IP アドレスからの通信が多いのか
  + どの IP アドレス宛の通信が多いのか
  + 何のアプリケーションの通信が多いのか
  + 何の IP プロトコルを利用した通信が多いのか
  + どの DSCP 値(PHB)の通信が多いのか

ヒント

- 1 つの入力欄に対し、複数の値をコンマ(,)区切りで指定することができます。この場合、指定した値のどれか 1 つでも該当すれば(OR 条件)、分析対象のフローと判断します。
- 各条件の入力欄の最大文字数は、255 文字です。
- 送信元 IP アドレス/ホスト名、宛先 IP アドレス/ホスト名に指定できるホスト名は FQDN の形式で指定してください。また、ホスト名の指定にはワイルドカードを表すアスタリスク(*)を含めることができます。

- [**指定の条件で表示を更新**]ボタン

  指定した条件に該当するフローの分析結果を表示します。

  分析結果として表示するウィジェットの種類は、指定したフィルター条件の内容で変化します。詳細は、「4.2.3　分析の条件と表示するウィジェットについて（115 ページ）」を参照してください。

表示設定領域

分析対象とする期間や表示件数などの表示に関する条件を指定します。

以下の設定項目のいずれかの値を変更すると分析結果を更新します。

- 分析期間
  - [**期間**]

    ボタンをクリックし、表示された画面で分析期間を指定します。

    * [**既定の期間から選択**] (デフォルト値)

      分析期間をプルダウンメニュー（[**過去 15 分**] / [**過去 30 分**] / [**過去 1 時間**] / [**過去 6 時間**] / [**過去 24 時間**] / [**過去 48 時間**] / [**過去 72 時間**]）から選択します。デフォルト値は[**過去 15 分**]です。

    * [**特定の日時と期間を指定**]

      起点となる日時と分析期間を指定します。デフォルト値は「一時間前」から「現在時刻まで」になります。

      1. 分析期間の起点となる日付を指定します。入力欄への直接入力するか、ボタンから指定します。
      2. 起点となる時刻をプルダウンメニューから選択します。起点となる時刻は、日付の指定内容によって選択できる時刻が以下のように変わります。

表 4-1　起点の日付に対する指定可能な時刻

指定した日付	指定可能な時刻
今日、または、昨日	0:00 を基準に 1 時間単位で時刻指定が可能
2 日前から 3 日前	0:00 を基準に 6 時間単位で時刻指定が可能

指定した日付	指定可能な時刻
4 日以上前	時刻指定不可

3. 分析期間をプルダウンメニューから選択します。NFA が保持しているフローデータの粒度に合わせて、NFA が適切な選択肢を提示します。

- [**件数**]

  各ウィジェットで表示する上位データの表示件数を([**トップ 5**] / [**トップ 10**] / [**トップ 20**])から選択します。デフォルト値は[**トップ 5**]です。

- [**単位**]

  各ウィジェットで表示する通信量の表示単位をプルダウンメニュー([**bytes (bps)**] / [**packets (pps)**])から選択します。デフォルト値は[**bytes (bps)**]です。

- 表示の更新と外部出力

  分析内容の更新操作や外部出力を行うことができます。

  - [**最終更新**]

    最終の更新日時を表示します。

  - [**更新**]ボタン

    すべてのウィジェットの分析結果を最新の内容に更新します。

  - [**更新間隔**]

    各ウィジェットの分析結果表示の更新間隔をプルダウンメニュー([**1 分**] / [**5 分**] / [**15 分**] / [**なし**])から選択します。デフォルト値は[**5 分**]です。

  - [**CSV 出力**]

    すべてのウィジェットの分析結果を CSV ファイル形式で出力することができます。詳細は、「4.3.2　分析結果を画面から CSV ファイルで出力する（117 ページ）」を参照してください。

ウィジェット表示領域

指定した条件に該当するフローに対する分析結果を表示します。分析結果を示すウィジェットに対しては、以下の操作を行うことができます。

- 「1.2.5.1　ドリルダウン分析を行う（18 ページ）」
- 「1.2.5.2　グラフの表示項目をフィルタリングする（19 ページ）」
- 「1.2.5.3　折れ線グラフの表示をズームインする（20 ページ）」
- 「1.2.5.4　IP アドレス表示をホスト名表示に変換する（21 ページ）」

4.2.3　分析の条件と表示するウィジェットについて

エクスポーター分析画面において、[**フィルター条件**]や[**通信の方向**]を指定した場合に表示するウィジェットの種類について説明します。

エクスポーター分析画面では、以下の 5 つの観点で分析結果を表示します。分析結果の表示内容は、[**フィルター条件**]や[**通信の方向**]の指定内容により変化します。

インターフェイスごとの通信量分析

[**フィルター条件**]の値に合致するフローの通信量を、以下のウィジェットでインターフェイスごとに表示します。

- [**入力インターフェイス**]ウィジェット
- [**出力インターフェイス**]ウィジェット

ヒント

- [**通信の方向**]として、[**入力**]を指定した場合

  [**入力インターフェイス**]ウィジェットの分析結果のみを表示します。
- [**通信の方向**]として、[**出力**]を指定した場合

  [**出力インターフェイス**]ウィジェットの分析結果のみを表示します。

エンドポイント観点での通信量分析

[**フィルター条件**]の値に合致するフローに対し、以下のウィジェットでフローのエンドポイントの観点で分析します。

- [**送信元 IP アドレス**]ウィジェット
- [**宛先 IP アドレス**]ウィジェット
- [**カンバセーション**]ウィジェット

ヒント

- [**フィルター条件**]として、[**送信元 IP アドレス/ホスト名**]、または、[**宛先 IP アドレス/ホスト名**]のどちらか 1 つを指定した場合

  指定条件の対向のエンドポイントに対する通信量を分析します。例えば、[**送信元 IP アドレス/ホスト名**]を指定した場合は、[**宛先 IP アドレス**]ウィジェットの分析結果のみを表示します。
- [**フィルター条件**]として、[**送信元 IP アドレス/ホスト名**]、および、[**宛先 IP アドレス/ホスト名**]の両方を指定した場合

  フローのカンバセーションが特定されるため、エンドポイント観点での通信量分析は行いません。

通信種別観点での通信量分析

[**フィルター条件**]の値に合致するフローに対し、以下のウィジェットで通信の種別(アプリケーション、IP プロトコル、DSCP)の観点で分析します。

- [**アプリケーション**]ウィジェット
- [**IP プロトコル**]ウィジェット
- [**DSCP**]ウィジェット

ヒント

- [**フィルター条件**]として、[**IP プロトコル**]を指定した場合

  指定した IP プロトコルを利用するアプリケーションの通信量の分析のみを実施します。
- [**フィルター条件**]として、[**アプリケーション**]を指定した場合

  フローの通信種別が特定されるため、通信種別観点での通信量分析は行いません。

エンドポイントグループ観点での通信量分析

[**フィルター条件**]に[**送信元エンドポイントグループ**]、または、[**宛先エンドポイントグループ**]を指定した場合は、指定条件の対向のエンドポイントグループに対する通信量を以下のウィジェットで分析します。

- [**送信元エンドポイントグループ**]ウィジェット
- [**宛先エンドポイントグループ**]ウィジェット

ヒント

- [**フィルター条件**]として、[**送信元エンドポイントグループ、**]および、[**宛先エンドポイントグループ**]の両方を指定した場合

  フローのエンドポイントグループ間が特定されるため、エンドポイントグループ観点での通信量分析は行いません。

AS 観点での通信量分析

[**フィルター条件**]に[**送信元 AS 番号**]、または、[**宛先 AS 番号**]を指定した場合は、指定条件の対向の AS に対する通信量を以下のウィジェットで分析します。

- [**送信元 AS**]ウィジェット
- [**宛先 AS**]ウィジェット

ヒント

- [**フィルター条件**]として、[**送信元 AS 番号、**]および、[**宛先 AS 番号**]の両方を指定した場合

  フローの AS 間が特定されるため、AS 観点での通信量分析は行いません。

4.3　蓄積データや分析結果を外部に出力する

NFA では、データベースに蓄積しているフローデータを CSV ファイルとして出力するコマンドと、ウィジェットで表示したフローの情報を Web コンソールを用いて CSV ファイルに出力する機能を提供しています。

nfa_flow_export コマンド

`nfa_flow_export` コマンドを実行することで、蓄積している詳細なフローデータを CSV ファイルとして外部出力することができます。

Web コンソールからの CSV 出力機能

ダッシュボード画面、および、エクスポーター分析画面の各ウィジェットで分析表示したフローの情報を、CSV ファイルとして外部出力することができます。

4.3.1　蓄積データをコマンドで CSV ファイルに出力する

データベースに蓄積されたフローデータは、`nfa_flow_export` コマンドを用いることで、CSV ファイル形式で外部出力することができます。

本コマンドは、CSV ファイルへ出力するフローデータの種類と粒度、および対象とする期間などを指定して、実行します。データの種類は、大きく分けて、エクスポーター 1 台に着目した詳細なフローデータと、全エクスポーターの情報をまとめたネットワーク全体のフローデータの 2 つの種類があります。

また、本コマンドを cron などに登録することにより、定期的に CSV ファイルに出力するよう構成することもできます。

詳細は、「A.2　nfa_flow_export（161 ページ）」や「A.2.3　使用例（174 ページ）」を参照してください。

4.3.2　分析結果を画面から CSV ファイルで出力する

ダッシュボード画面、および、エクスポーター分析画面の各ウィジェットの分析結果を CSV ファイル形式で外部出力する手順について説明します。

1. フロー情報の分析画面を表示します。
   - ダッシュボード画面を表示する場合、[**ダッシュボード**]タブをクリックします。
   - エクスポーター分析画面を表示する場合は、[**エクスポーター分析**]タブをクリックします。
2. フロー分析のための条件指定を行います。

   各ウィジェットの分析結果が表示されます。

3. ウィジェット表示領域の右上の[**CSV 出力**]をクリックします。

   画面に表示している各ウィジェットの分析結果をまとめた ZIP ファイルのダウンロードが開始されます。

ヒント

ダウンロードするファイルは以下の名前になります。

- ダッシュボード画面の場合:

  `DashboardCSV_<yyyymmdd-hhmmss>.zip`

- エクスポーター分析画面の場合:

  `ExporterAnalysisCSV_<yyyymmdd-hhmmss>.zip`

*<yyyymmdd-hhmmss>*は、出力操作を行った NFA サーバーの日時を表す値になります。

4. ダウンロードした ZIP ファイルの内容を確認します。

   ZIP ファイルを解凍し、画面上のすべてのウィジェットに対応する CSV ファイルが含まれていることを確認します。

   ウィジェットと CSV ファイルの対応状況は、CSV ファイル名から判断することができます。CSV ファイルの命名規則は以下の通りです。

   <識別 ID>_<ウィジェット番号>_<ウィジェット名>_<グラフ種別>`.csv`

   - 識別 ID

     NFA が、画面上のウィジェットを一意に識別するために内部で付与する ID を示します。

   - ウィジェット番号およびウィジェット名

     ウィジェットの種類に対応した番号と名前を示します。対応状況は以下の通りです。

表 4-2　ウィジェット種別に対応するウィジェット番号およびウィジェット名

ウィジェットの種類	ウィジェット番号	ウィジェット名
エクスポーター	1	Exporters
入力インターフェイス	2	InInterfaces
出力インターフェイス	3	OutInterfaces
送信元 IP アドレス	20	SourceIPAddresses
宛先 IP アドレス	21	DestinationIPAddresses
カンバセーション	23	Conversations
送信元エンドポイントグループ	40	SourceEndpointGroups
宛先エンドポイントグループ	41	DestinationEndpointGroups
送信元 AS	30	SourceAS
宛先 AS	31	DestinationAS
アプリケーション	13	Applications

ウィジェットの種類	ウィジェット番号	ウィジェット名
IP プロトコル	14	IPProtocols
カレントアラート	50	CurrentAlerts
DSCP	81	DSCP

- グラフ種別

  CSV ファイルに含まれるデータの表示種別を示します。表示種別の説明を以下に示します。

表 4-3　グラフ種別の説明

グラフ種別	説明
line	折れ線グラフ表示データであることを示します。
pie	円グラフ表示データであることを示します。
table	一覧表示データであることを示します。

5. CSV ファイルの内容を確認します。

   CSV ファイルの形式は以下の通りです。

表 4-4　CSV ファイル内容の形式

行数	項目	説明
1	Date	CSV ファイルの出力操作を行った日時を示します。
2	CsvType	どの画面から出力された CSV ファイルなのかを示します。 • Dashboard ダッシュボード画面から出力したことを示します。 この場合、出力時のダッシュボード定義の名前も合わせて出力します。 • ExporterAnalysis エクスポーター分析画面から出力したことを示します。
3	Widget	分析処理を行ったウィジェットの情報を示します。出力形式は以下の通りです。 <ウィジェット番号>,<ウィジェット名>,<グラフ種別>
4	StartingTime	出力したデータの分析期間の開始日時を示します。 [**カレントアラート**]ウィジェットの場合は、必ず「-」になります。
5	EndingTime	出力したデータの分析期間の終了日時を示します。 [**カレントアラート**]ウィジェットの場合は、必ず「-」になります。
6	Interval(minutes)	折れ線グラフにおけるデータのプロット間隔を分単位で示します。 円グラフ表示、および一覧表示のデータの場合は、必ず「-」になります。
7	Unit	出力データの単位を示します。単位は以下のいずれかになります。 bytes、bps、packets、pps、-
8	StartingPosition	実際のデータが出力されている行番号を示します。

行数	項目	説明
9	TargetType	分析対象の種別を示します。 • Exporters 分析対象がエクスポーターであることを示します。 • Interfaces(<通信の方向>) 分析対象がインターフェイスであることを示します。 通信の方向は以下の形式で出力します。 - Inbound 入力方向の通信フローが対象であることを示します。 - Outbound 出力方向の通信フローが対象であることを示します。 - Bi-Direcion 双方向の通信フローが対象であることを示します。
10	Exporters または Interfaces	分析対象のエクスポーター、または、インターフェイスの名前を示します。複数ある場合は、コンマ(,)区切りで表現します。 インターフェイスの場合は、以下のように表現します。 <エクスポーター名>:<インターフェイス名> すべてのエクスポーターのインターフェイスを対象にしている場合は、以下のように表現します。 (All)
11	FilterCount	エクスポーター分析画面で指定したフィルター条件の個数を示します。 ダッシュボード画面から CSV 出力した場合は、本項目の行を出力しません。
~N	<フィルター条件>	「FilterCount」項目の値が「0」以外の場合は、以降の行で、フィルター条件の内容を 1 行ずつ以下の形式で出力します。 <フィルター条件>,<設定値> フィルター条件は以下のように表現しています。 • SourceIPAddress [**送信元 IP アドレス/ホスト名**]フィルター条件であることを示します。 • DestinationIPAddress [**宛先 IP アドレス/ホスト名**]フィルター条件であることを示します。 • SourceEndpointGroup [**送信元エンドポイントグループ**]フィルター条件であることを示します。 • DestinationEndpointGroup [**宛先エンドポイントグループ**]フィルター条件であることを示します。 • SourceAS [**送信元 AS 番号**]フィルター条件であることを示します。 • DestinationAS [**宛先 AS 番号**]フィルター条件であることを示します。 • Application [**アプリケーション**]フィルター条件であることを示します。 • IPProtocol [**IP プロトコル**]フィルター条件であることを示します。

行数	項目	説明
		• DSCP [**DSCP**]フィルター条件であることを示します。
N+1	空行	実際のデータを出力する行と区切るため、空行を挿入します。
N+2	WidgetTitle	分析処理を行ったウィジェットのタイトルを示します。 ダッシュボード画面から出力した場合は、12 行目に本項目を出力し、ダッシュボード定義でユーザーが指定したウィジェットのタイトルを出力します。
N+3	<データラベル>	出力データの内容を示すラベルを以下の形式で出力します。 Time,<項目>,...
N+4	<データ>	データラベルに対応するデータをコンマ(,)区切りで出力します。

ヒント

CSV ファイル中に出力する時刻情報は、UNIX 時刻形式で出力します。

⚠ 注意

CSV ファイルによる分析結果の出力では、原則として Web コンソールに表示されている分析結果のグラフと同一の時間範囲のデータが出力されます。ただし、カレントアラートについては、Web コンソールの表示更新タイミングとの兼ね合いで、画面上はまだ表示されていないが、内部的には新しいアラートが発生している場合があります。このような場合は、CSV 出力を行った時点でのカレントアラートが出力されるため、CSV ファイルに出力されたカレントアラートの内容が、Web コンソール上での表示と異なる場合があります。

4.4　ローデータを確認する

受信したすべてのフローデータを集約前のローデータとして外部出力することができます。ここでは、外部出力されたローデータの確認方法について説明します。

ローデータを外部出力するためには、事前設定が必要になります。詳細は、「3.5　ローデータの外部出力設定を行う（85 ページ）」を参照してください。

ローデータには、NFA の Web コンソールでは表示していない、各フローの TCP フラグの情報や sFlow に含まれている Ethernet フレームタイプ、Ethernet タイプ、VLAN タグの情報が含まれています。また、通信量の少ないフローに対するデータも記録されています。そのため、ローデータは、簡易的なネットワークフォレンジックとして活用することができます。

⚠ 注意

ローデータには、DNS から得られる送信元、および、宛先 IP アドレスに対するドメイン名の情報は含まれていません。また、NFA が付加するアプリケーション、インターフェイスグループ、エンドポイントグループの情報も含まれていません。

ローデータの出力先

ローデータは、設定ファイル (collector.conf) で指定した出力先ディレクトリ配下に以下の構成で出力されます。

ローデータは、15 分毎に以下の構成で自動出力されます。

- *<Output_Directory>/<IP_Address>/YYYY-MM/*

  RawFlow_*<IP_Address>*_*<FlowType>*_IPv4_*YYYY-MM-DD_HH-MM*.tar.bz2

  上記の圧縮ファイルを解凍した場合、以下のような構成となります。

  - RawFlow_*<IP_Address>*_*<FlowType>*_IPv4_*YYYY-MM-DD_HH-MM/*

    RawFlow_*<IP_Address>*_*<FlowType>*_IPv4_*YYYY-MM-DD_HH-MM*_*<index>*.csv

  Output_Directory

  設定ファイル (collector.conf) で指定した出力先ディレクトリ

  IP_Address

  エクスポーターの IP アドレス

  FlowType

  フロープロトコルの種別

  - sFlow: sFlow によるフローデータを記録していることを示します。
  - NetFlow: NetFlow、または、IPFIX によるフローデータを記録していることを示します。

  index

  出力ファイルの識別番号

  1 ファイルあたり 10 万件のフローデータが記録され、出力ファイルの数に合わせて *index* が付与されます。

  出力ファイルの「 *YYYY-MM-DD_HH-MM* 」は、フローを記録する起点となる日時を示します。例えば、「2022-10-14_09-30」の場合は、2022 年 10 月 14 日 9 時 30 分から 15 分間受信したフローに対するローデータであることを示します。

ローデータファイルの形式

圧縮ファイルには、15 分間のフローデータを記録する CSV ファイルが含まれています。この CSV ファイル、および、記録されているローデータの形式は以下の通りです。

- 文字コード: UTF-8
- 改行コード: LF
- 出力形式:

出力するデータ項目を「表 4-5 CSV ファイルの列一覧（123 ページ）」に示します。各項目を順番に、コンマ(,)区切りで出力します。また、各値をダブルクォー テーション(")で囲んで出力します。

表 4-5　CSV ファイルの列一覧

列番号	列名	説明
1	recv_time	フローデータの受信時刻。 NFA サーバーのタイムゾーンを基準とし、*YYYY-MM-DD hh:mm:ss* の形式で示します。
2	src_address	フローの送信元となるエンドポイントの IP アドレス。
3	dst_address	フローの宛先となるエンドポイントの IP アドレス。
4	nexthop	フローの Next Hop IP アドレス。 INGRESS の設定でフローを採取した場合やエクスポーターが宛先となっているフローなどでは値がありません。
5	input	フローが入力方向で通過したインターフェイスの ifIndex 値。
6	output	フローが出力方向で通過したインターフェイスの ifIndex 値。 INGRESS の設定でフローを採取した場合やエクスポーターが宛先となっているフローなどでは値がありません。
7	packets	フローのパケット数。
8	octets	フローの L3 レイヤーパケットの合計オクテット数 (バイト数)。
9	first	フローの最初のパケットを処理した時のエクスポーターの sysUpTime。 sysUpTime は、起動してからの経過時間を 1/100 秒で表します。
10	last	フローの最後のパケットを処理した時のエクスポーターの sysUpTime。 sysUpTime は、起動してからの経過時間を 1/100 秒で表します。 **ヒント** 以下の計算により、フローの継続時間を求めることができます。 **フローの継続時間** `[ms] = (last - first) ÷ 10`
11	src_port	TCP、または、UDP の送信元ポート番号。 TCP、および、UDP 以外のフローの場合は値がありません。
12	dst_port	TCP、または、UDP の宛先ポート番号。 TCP、および、UDP 以外のフローの場合は値がありません。
13	tcp_flags	フローに含まれている TCP フラグ。 TCP フラグの情報を文字列と論理和で示します。 例: "SYN/ACK/PSH (0x1a)"
14	protocol	IP プロトコル。
15	tos	ToS 値(DSCP+IP Preference)。 10 進数で値を示します。 **ヒント** DSCP 値は以下の計算によって求めることができます。

列番号	列名	説明
		`DSCP値 = ToS値 ÷ 4`
16	src_as	フローの送信元 AS 番号。
17	dst_as	フローの宛先 AS 番号。
18	src_mask	フローの送信元 IP アドレスに対するサブネットマスク。 CIDR (Classless Inter-Domain Routing) 値で示します。
19	dst_mask	フローの宛先 IP アドレスに対するサブネットマスク。 CIDR (Classless Inter-Domain Routing) 値で示します。
20	frametype	Ethernet フレームタイプ。 sFlow で受信したフローの場合にのみ値を出力します。
21	ethertype	Ethernet タイプ。 sFlow で受信したフローの場合にのみ値を出力します。
22	vlan_tag	VLAN タグの ID。 sFlow で受信したフローの場合にのみ値を出力します。

4.5　フローレートを確認する

監視対象となるネットワークを流れる通信フローの流量(フローレート)の確認方法について説明します。

フローレートは、NFA の諸元と運用状況を比較確認する場合などで活用することができます。

ヒント

NFA におけるフローレートとは、1 分間に発生したエンドポイント間の通信フローの数のことを指します。

フローレートは、以下の 2 つの方法で確認することができます。

- エクスポーター管理画面のエクスポーターの一覧の情報から確認する

  直近 7 日間におけるエクスポーター全体、および、エクスポーター毎のフローレートの最大値とその発生日時の情報を表示します。

- フローレートを記録するログファイルの内容から確認する

  各エクスポーターの 1 分単位のフローレートの記録を CSV ファイルに記録しています。

エクスポーター管理画面で表示するフローレート情報については、「2.3　エクスポーターを管理する（36 ページ）」を参照してください。

ここでは、フローレートを記録するログファイルについて説明します。

ログファイルの出力先

フローレートのログファイルは、以下のディレクトリに日単位のファイルで出力します。

- 出力先ディレクトリ:

  `<%データディレクトリ%>/collector/flowrate_log/`

- ファイル名:

  nfa_collector_flow_rate_*yyyy-mm-dd*.csv

本ログファイルの保持期間は 30 日です。30 日を過ぎたログファイルは自動的に削除されます。

ログファイルの形式

NFA が出力するフローレートのログファイルの形式は以下の通りです。

- 文字コード: UTF-8
- 改行コード: LF
- 出力形式:

  ```
  time,exporter id,ipaddress,flow rate,flow template status
  ```

  - time (時刻):

    フローレートを記録した時刻情報を示します。

  - exporter id (エクスポーター ID):

    NFA が内部で管理するエクスポーターの ID を示します。

  - ipaddress (エクスポーターの IP アドレス):

    エクスポーターの IP アドレスを示します。

  - flow rate (フローレート):

    1 分間のフローレートの値を示します。

  - flow template status (フローの解析エラーの情報):

    NetFlow version 9 のパケット解析時に、テンプレートレコードの情報が不足しフローの解析が行えなかった場合に *template error* を表示します。

    ヒント

    エラーが表示された場合には、テンプレートレコードを定期的に(10 分間隔程度を目安に)受信できるようにエクスポーターの設定等を見直してください。

出力例:

```
time,exporter id,ipaddress,flow rate,flow template status
2022-10-14 13:51,1001,192.168.10.1,168231,
```

```
2022-10-14 13:51,1002,172.17.1.1,254220,
2022-10-14 13:52,1001,192.168.10.1,161649,template error
2022-10-14 13:52,1002,172.17.1.1,281135,
```

4.6　イベント情報を確認する

NFA が検知したイベントの発生状況は、イベント一覧画面で確認することができます。

4.6.1　しきい値超過、回復イベントの発生履歴を確認する

イベント一覧画面の表示内容について説明します。

イベント一覧画面

NFA が検出したしきい値超過やその回復などを示すイベントの発生履歴を表示します。

NFA では、最新のイベントを 1 万件まで保持します。

イベント一覧画面は、[**イベント監視**] >[**イベント一覧**] をクリックして表示します。

図 4-4　イベント一覧画面

表示設定領域

表示の更新については、以下の項目の表示、操作を行うことができます。

- [**最終更新**]

  最終の日時を表示します。

- [**更新**]ボタン

  ダッシュボード上のすべてのウィジェットの分析結果を最新の内容に更新します。

- [**更新間隔**]

  [**イベント一覧**]の更新間隔をプルダウンメニュー([**1 分**] / [**5 分**] / [**15 分**] / [**なし**])から選択します。デフォルト値は[**1 分**]です。

イベントの一覧

- ページ移動ボタン

  保持するイベントの情報を複数のページに分けて表示します。表示ページについては、以下の操作を行うことができます。

  - ページの切り替えボタン

    * ボタン

      1 ページ目(最新情報)を表示します。

    * ボタン

      現在表示しているページの 1 ページ前のページを表示します。

    * ボタン

      現在表示しているページの 1 ページ後のページを表示します。

    * ボタン

      最後のページを表示します。

  - [**表示ページ入力**]欄

    指定したページの情報を表示します。

  - [**表示件数**]

    1 ページに表示するイベントの件数をプルダウンメニュー([**50**] / [**100**] / [**250**] / [**500**] [**1000**])から選択します。デフォルト値は[**100**]です。

- イベント一覧

  - [**重要度**]

    イベントに対する重要度を以下の 3 つで表現します。

    * 異常

    * 警告

    * 正常

  - [**検出時刻**]

    NFA がイベントを検出した日時を表示します。

  - [**監視対象**]

    イベントを検出した監視箇所となるエクスポーター、および、インターフェイスの名前を表示します。

  - [**内容**]

    イベントの内容を表示します。

- [**監視エントリ名**]

  イベントを検出した監視エントリの名前を表示します。

ヒント

[**重要度**]、[**検出時刻**]の項目名の欄をクリックすることで、現在表示中のデータを並びかえることができます。

4.7　セキュリティ監視の検知結果を確認する

セキュリティ監視によって検知されたインシデントの確認方法について説明します。

セキュリティ監視によって検知されたインシデントはインシデント詳細画面で確認することができます。

ヒント

インシデントの情報は最大 1000 件まで保存され、古いインシデント情報は自動的に削除されます。

インシデント詳細画面

セキュリティ監視によって検知した DDoS またはスキャンの攻撃の疑いの詳細情報を表示します。

イベント一覧画面またはダッシュボード画面の[**カレントアラート**]ウィジェットに表示されたセキュリティ監視の検知、回復のイベントの[**内容**]のインシデント ID のリンクをクリックし、インシデント詳細画面を表示します。

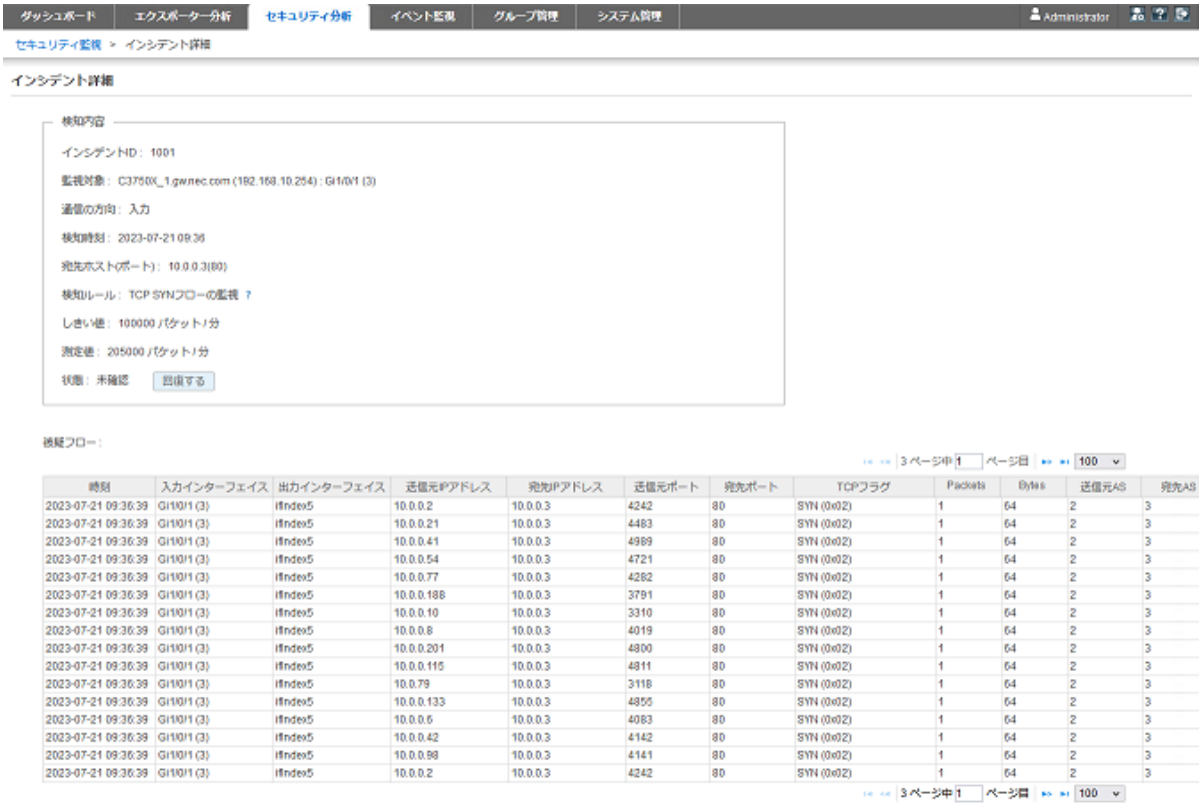

図 4-5　インシデント詳細画面

検知内容表示領域

表示の更新については、以下の項目の表示、操作を行うことができます。

- [**インシデント ID**]

  検知したインシデントを一意に識別するために内部で付与する ID を表示します。

- [**監視対象**]

  インシデントを検知した監視箇所となるエクスポーター、および、インターフェイスの名前を表示します。

- [**通信の方向**]

  検知の対象となった通信フローの向きを示します。

  - [**入力**]

    監視対象のインターフェイスにおける入力方向の通信フローで検知されたことを示します。

  - [**出力**]

    監視対象のインターフェイスにおける出力方向の通信フローで検知されたことを示します。

- [**検知時刻**]

インシデントを検知した時刻を表示します。 1 分以上継続的に検知された場合には検知されていた期間を表示します。

- [**宛先ホスト(ポート)**]

  攻撃対象として検知されたホストの IP アドレスとポート番号を表示します。

- [**送信元ホスト**]

  攻撃元として検知されたホストの IP アドレスを表示します。

  この項目はスキャン検知の場合に表示されます。

- [**検知ルール**]

  検知ルールを表示します。

- [**しきい値**]

  しきい値を表示します。

- [**測定値**]

  実際の測定値を表示します。

- [**状態**]

  当該インシデントの確認状態を表示します。

  インシデントが発生した際には未確認状態です。未確認状態の場合には[**回復する**]ボタンをクリックすることで回復状態となります。

  回復操作を行った場合、当該インシデントの検知イベントの回復状態が回復済となります。

被疑フローの一覧

- ページ移動ボタン

  被疑となったフローを複数のページに分けて表示します。表示ページについては、以下の操作を行うことができます。

  - ページの切り替えボタン

    * ⏮ボタン

      1 ページ目(最新情報)を表示します。

    * ◀◀ボタン

      現在表示しているページの 1 ページ前のページを表示します。

    * ▶▶ボタン

      現在表示しているページの 1 ページ後のページを表示します。

    * ⏭ボタン

最後のページを表示します。

- [**表示ページ入力**]欄

  指定したページの情報を表示します。

- [**表示件数**]

  1 ページに表示するイベントの件数をプルダウンメニュー([**100**] / [**250**] / [**500**] / [**1000**])から選択します。デフォルト値は[**100**]です。

• 被疑フロー

- [**時刻**]

  フローの受信時刻を表示します。

- [**入力インターフェイス**]

  フローの入力側のインターフェイス名を表示します。

- [**出力インターフェイス**]

  フローの出力側のインターフェイス名を表示します。

- [**送信元 IP アドレス**]

  フローの送信元 IP アドレスを表示します。

- [**宛先 IP アドレス**]

  フローの宛先 IP アドレスを表示します。

- [**送信元ポート**]

  フローの送信元ポートを表示します。

- [**宛先ポート**]

  フローの宛先ポートを表示します。

- [**TCP フラグ**]

  TCP ヘッダに含まれるコントロールフラグの論理和を表示します。。

  <*フラグ名*>(<*フラグ値*>)の形式で表示します。

  フラグ値は FIN=0x01, SYN=0x02, RST=0x04, PSH=0x08, ACK=0x10, URG=0x20, ECE=0x40, CWR=0x80, NS=0x0100 として、ON になっているフラグの論理和が 16 進数表記で出力されます。

- [**Packets**]

  フローの通信量(オクテット数)を表示します。

- [**Bytes**]

  フローの通信パケット数を表示します。

- [**送信元 AS**]

フローの送信元 AS 番号を表示します。

- [**宛先 AS**]

  フローの宛先 AS 番号を表示します。

- [**IP プロトコル**]

  フローの IP プロトコル名を表示します。

- [**TOS**]

  フローの TOS (Type Of Service) フィールド値を表示します。

  10 進数表記で出力されます。

- [**Nexthop**]

  フローの Nexthop の IPv4 アドレスを表示します。

- [**送信元 Mask**]

  フローの送信先 IPv4 アドレスのサブネットマスク値を表示します。

- [**宛先 Mask**]

  フローの宛先 IPv4 アドレスのサブネットマスク値を表示します。

- [**First**]

  フローの最初のパケットを処理した時のエクスポーターの sysUpTime を表示します。

  sysUpTime は、起動してからの経過時間を 1/100 秒で表します。

- [**Last**]

  フローの最後のパケットを処理した時のエクスポーターの sysUpTime を表示します。

  sysUpTime は、起動してからの経過時間を 1/100 秒で表します。

- [**Frametype**]

  Ethernet フレームのタイプを表示します。

  「Ethernet 2」、「IEEE802.3 SNAP」、「IEEE802.3 RAW」、「IEEE802.3 LLC」のいずれかの文字列で出力されます。

  sFlow の場合にのみ値が表示されます。

- [**Ethertype**]

  Ethernet フレームのタイプ値を表示します。

  16 進数表記で出力されます。

  sFlow の場合にのみ値が表示されます。

- [**VLAN タグ**]

フローの VLAN ID を表示します。

sFlow の場合にのみ値が表示されます。

4.8　ユーザーの操作履歴を確認する

NFA では、各ユーザーのログイン、ログアウトの履歴を証跡ログとして記録しています。

証跡ログを活用することで、誰がどのような頻度でネットワークフローの状況を確認しているかを追跡調査することができます。

証跡ログは以下のパスにテキストファイルとして出力されます。また、証跡ログは、以下のファイル名で、日ごとに記録するファイルが切り替わります。

出力パス

<%*データディレクトリ*%>/controller/auditlog/

ファイル名

audit_log.*YYYY-MM-DD*.txt

証跡ログの詳細なフォーマットについては、「証跡ログフォーマット（133 ページ）」を参照してください。

証跡ログファイルの保持期間のデフォルト値は、3 年間(1095 日間)となっています。保持期間の変更方法については、「5.1.9　証跡ログの保持期間を変更する（150 ページ）」を参照してください。

ヒント

証跡ログファイルは、任意のテキストエディターを用いて参照することができます。

証跡ログフォーマット

証跡ログは、以下のフォーマットで、1 操作に対し 1 行で記録されます。

```
<操作日時>\t<操作>\t<結果>\t<ユーザー名>\t<本文>
```

\t : タブ文字を示します。

<操作日時>

操作を行った日時を示します。以下の形式となります。

- YYYY-MM-DD HH:mm:ss.SSS

<操作>

操作の種類を示します。以下となります。

- 情報

<結果>

操作の結果を示します。以下のいずれかとなります。

- 成功
- 失敗

<ユーザー名>

操作を行ったユーザー名を示します。

システムの動作によるログやログインの失敗などでユーザー名が特定できなかった場合のログでは、「(none)」となります。

<本文>

操作の具体的な内容を示します。

以下に証跡ログの出力例を示します。

```
2023-09-02 17:49:20.002  情報  成功  admin  ログインしました。(ユーザー名=admin)
```

```
2023-09-02 17:50:15.021  情報  成功  admin  ログアウトしました。(ユーザー名=admin)
```

```
2023-09-02 17:51:12.338  情報  失敗  admin  ログインに失敗しました。(ユーザー名=admin)
```

第 5 章
システムメンテナンス

NFA のメンテナンス方法について説明します。

目次

5.1 システムの環境をメンテナンスする.....136
5.2 フローデータの管理について.....151

5.1　システムの環境をメンテナンスする

システムの環境をメンテナンスする手順について説明します。

5.1.1　バージョン情報を確認する

バージョン情報を確認する手順について説明します。

NFA の動作に関して、NEC カスタマーサポートセンターに問い合わせを行う場合や、NEC カスタマーサポートセンターから入手したアップデートモジュールを適用する場合に、運用中の NFA の正確なバージョン情報を確認する必要があります。

バージョンを確認するには、Web コンソールから確認する方法と、コマンドから確認する方法があります。Web コンソールが開けない環境、状態の場合はコマンドからバージョンを確認してください。

- Web コンソールから確認する

  1. NFA の Web コンソールに接続します。
  2. フッター領域のバージョン情報を確認します。すべての画面で確認できます。

     表示形式は以下の通りです。

     WebSAM Network Flow Analyzer <バージョン番号>-<リリース番号>

     例: バージョン「1.0.0」、リリース番号「16」の場合

図 5-1　バージョン情報表示

- コマンドから確認する

  1. NFA サーバーにログインします。(root ユーザーである必要はありません。)
  2. 以下のコマンドを実行します。

```
$ rpm -q nec-nfa-controller
```

  1. 表示結果からバージョン情報を確認します。

     表示形式は以下の通りです。

nec-nfa-controller-<バージョン番号>-<リリース番号>.x86_64

例: バージョン「1.0.0」、リリース番号「16」の場合

```
$ rpm -q nec-nfa-controller
nec-nfa-controller-1.0.0-16.x86_64
```

5.1.2　サービスを起動、停止する

NFA が動作するサーバー上で、NFA のサービスを手動で起動、停止する手順について説明します。

NFA のサービスは、OS の起動、停止に連動して、自動で起動、停止します。

NFA のメンテナンスのため、OS を起動したまま、NFA のサービスのみを停止したり、再び起動したい場合は、NFA が提供する以下のコマンドで制御することができます。

<%*インストールディレクトリ*%>/controller/bin/nfa_ctl.sh

コマンドは、NFA サーバーに root ユーザーでログインして実行する必要があります。

- サービスを起動する場合、引数 start を付けてコマンドを実行します。

  NFA の全てのデーモンプロセスの起動に成功すれば、コマンドは戻り値として 0 を返します。

  ```
  # <%インストールディレクトリ%>/controller/bin/nfa_ctl.sh start
  ```

- サービスを停止する場合、引数 stop を付けてコマンドを実行します。

  NFA の全てのデーモンプロセスの停止に成功すれば、コマンドは戻り値として 0 を返します。

  ```
  # <%インストールディレクトリ%>/controller/bin/nfa_ctl.sh stop
  ```

- 引数 status を付けてコマンドを実行すれば、サービスの状態を確認することができます。

  ```
  # <%インストールディレクトリ%>/controller/bin/nfa_ctl.sh status
  ```

  サービスが起動していれば、次のようなメッセージを表示します。また、コマンドは戻り値として 0 を返します。

  ```
  systemdb (pid 12340) is running...
  eventdb (pid 12341) is running...
  controller (pid 12342) is running...
  web server (pid 12343) is running...
  flowdb (pid 12344) is running...
  logserver (pid 12345) is running...
  collector (pid 12346) is running...
  ```

  サービスが停止していれば、次のようなメッセージを表示します。また、コマンドは戻り値として 3 を返します。

```
systemdb is stopped
eventdb is stopped
controller is stopped
web server is stopped
flowdb is stopped
logserver is stopped
collector is stopped
```

5.1.3　製品が利用する通信ポート番号を変更する

NFA が利用するポート番号を変更する手順を説明します。

NFA が利用するポート番号については、「C.1　製品が利用するポート番号の一覧（195 ページ）」を参照してください。

NFA が利用する各ポート番号の変更手順は、以下の通りです。

1. root ユーザーでログインします。
2. NFA のサービスを停止します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ctl.sh stop
```

3. 変更したいポート番号に対する設定ファイルを変更し、上書きして保存します。

   設定ファイルについては、「表 5-1 通信ポート番号の設定ファイルと設定項目(外部通信)（138 ページ）」、「表 5-2 通信ポート番号の設定ファイルと設定項目(内部通信)（139 ページ）」を参照してください。当該の設定ファイルが存在しない場合は、ファイルを新規に作成してください。

表 5-1　通信ポート番号の設定ファイルと設定項目(外部通信)

設定ファイルは<%データディレクトリ%>配下に格納されています。

用途	設定項目

HTTPS 通信	• 設定ファイル
	`controller/conf/tomcat.properties`
	• 指定形式
	`nfa.tomcat.https.port = 443`

sFlow パケット受信	• 設定ファイル
	`collector/conf/collector.conf`
	• 指定形式
	`sflow.port = 6343`

NetFlow パケット、
IPFIX パケット受信
	• 設定ファイル
	`collector/conf/collector.conf`
	• 指定形式
	`netflow.port = 9995`

表 5-2　通信ポート番号の設定ファイルと設定項目(内部通信)

設定ファイルは<%データディレクトリ%>配下に格納されています。

用途	設定項目
フローデータ DB 通信	• 設定ファイル collector/conf/flowdb.conf • 指定形式 `flowdb.port = 27100`
	• 設定ファイル collector/conf/flowdb-extra.conf • 指定形式 `port = 27100`
システム管理 DB 通信	• 設定ファイル controller/conf/controller.properties • 指定形式 `systemdb.port = 27110`
	• 設定ファイル controller/conf/systemdb-extra.conf • 指定形式 `port = 27110`
イベント管理 DB 通信	• 設定ファイル controller/conf/event.properties • 指定形式 `eventdb.port = 27120`
	• 設定ファイル controller/conf/eventdb-extra.conf • 指定形式 `port = 27120`
コントローラー制御通信	• 設定ファイル controller/conf/controller.properties • 指定形式 `message.server.port = 27200`
	• 設定ファイル collector/conf/collector.conf • 指定形式 `controller.port = 27200`
コレクターログサービス通信	• 設定ファイル collector/conf/nfalog.conf • 指定形式

用途	設定項目
	`Port = 27210`

⚠ 注意

- 1 つの項目について 2 つ以上の設定ファイルが記載されているポートは、すべての設定ファイルを同時に編集し、同じ値を設定してください。関連する設定ファイル間でポート番号が異なると、正常に動作しません。
- パラメーターの末尾に不要なスペースが含まれている場合、末尾のスペースも含めてパラメーター値と判断するため、意図した通りの処理が行えません。

  設定ファイルの保存前に、パラメーター末尾に不要なスペースが含まれていないことを確認してください。

4. 必要に応じて、ファイアウォールの設定を見直します。

   特に外部通信用のポート番号は、ファイアウォールによってブロックされている場合が多いため、ポート番号変更の際には、ファイアウォールの設定が適切かどうか、確認してください。

5. NFA のサービスを起動します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ctl.sh start
```

   サービス起動後、ポート番号の変更内容が NFA に反映されます。

5.1.4　フロー情報の記録処理方式を変更する

受信したフロー情報の記録処理の方式を環境条件に合わせて変更することで、ディスク I/O 負荷を低減することができます。

既定の処理では、受信したフロー情報をすべて一時記録用データベースに記録し、その後、1 分間のフローデータとして集約処理(丸め処理)を実施してから、フローデータ管理用データベースに記録しています。

定常的に受信するフロー情報が多く、かつ、NFA サーバーのディスク I/O 性能が十分ではない環境においては、フローデータの記録処理に時間がかかり、メモリ使用量が増加し続ける場合があります。このような場合は、一時記録用データベースへの記録処理を停止し、メモリ上で集約処理を行ったフローデータを直接、フローデータ管理用データベースに記録する方式に変更することで、大幅にディスク I/O 負荷を減らすことができます。

以下の手順で記録方式を変更します。

1. root ユーザーで NFA サーバーにログインします。
2. NFA のサービスを停止します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ctl.sh stop
```

3. 設定ファイル (collector.conf) を開きます。

<%データディレクトリ%>/collector/conf/collector.conf

設定ファイルが存在しない場合は、新規に作成してください。

ヒント

collector.conf は、フロー情報の受信用の通信ポート番号の設定変更などでも活用する設定ファイルです。

4. 設定ファイル (collector.conf) に、フロー情報の記録処理の方式切り替えのためのパラメーターを追記し、保存します。

指定形式:

```
rawdb.switch = <0|1>
```

0 :

受信したフロー情報を一時記録用データベースへ書き込む処理は行わず、メモリ上で保持して、集約処理(丸め処理)を行う方式です。

ディスク I/O 性能が十分ではない環境の場合に指定します。

⚠ 注意

一時記録用データベースへ書き込んだデータは、現状、24 時間保持する仕様となっています。このデータは、ローデータの外部出力機能やセキュリティ分析機能において利用しています。また、将来の機能強化においても活用する可能性があります。本パラメーターに「0」を指定した場合は、それらの機能の利用ができない場合がある点に注意してください。

1 :

受信したフロー情報を一時記録用データベースへ書き込み、データベースのデータを元に、集約処理(丸め処理)を行う方式です。

通常は、こちらを選択します。

ヒント

設定ファイル (collector.conf) に本パラメーターを指定していない場合は、以下のパラメーターを指定した場合と同様の動作となります。

```
rawdb.switch = 1
```

5. NFA のサービスを起動します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ctl.sh start
```

サービス起動後、フロー情報の記録処理方式の変更内容が NFA に反映されます。

5.1.5　Microsoft 365 通信定義の自動更新を停止する

Microsoft 365 (Office 365) の通信を識別するアプリケーション定義内容を自動更新する処理を停止する手順について説明します。

アプリケーション定義の自動更新処理は、マイクロソフトが提供している REST API を利用します。

Microsoft 365 (Office 365) の通信に対する分析が不要な場合、または、NFA からマイクロソフトのサイトへの通信が行えない環境の場合は、以下の手順で自動更新処理を停止させてください。

1. root ユーザーで NFA サーバーにログインします。
2. NFA のサービスを停止します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ctl.sh stop
```

3. 設定ファイル (controller.properties) を開きます。

   `<%データディレクトリ%>/controller/conf/controller.properties`

   設定ファイルが存在しない場合は、新規に作成してください。

   ヒント

   controller.properties は、NFA が利用する通信ポート番号の設定変更や IMS コンポーネントとの接続設定でも活用する設定ファイルです。

4. 設定ファイル (controller.properties) に、自動更新処理を停止するためのパラメーターを追記し、保存します。

   指定形式:

```
application.auto-update.o365.enable = <false|true>
```

   false:

   Microsoft 365 (Office 365) の通信に対するアプリケーション定義内容の自動更新を停止します。

   true:

   Microsoft 365 (Office 365) の通信に対するアプリケーション定義内容を自動更新します。

   設定ファイル (controller.properties) に本パラメーターを指定していない場合は、「true」を指定した場合と同様に動作します。

   ここでは、自動更新を停止させるため、「false」を指定します。

```
application.auto-update.o365.enable = false
```

5. NFA のサービスを起動します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ctl.sh start
```

サービス起動後、設定内容が NFA に反映されます。

5.1.6　Web サーバーの URL を変更する

NFA にアクセスする URL を変更する手順を説明します。

NFA にアクセスする URL のうち、ドメイン名 (FQDN) は変更することができます。ドメイン名を変更した場合、SSL サーバー証明書の中のドメイン名 (識別名の CN) を変更する必要があります。

SSL サーバー証明書に関する操作は、製品が提供する `nfa_ssl_keytool` コマンドを使用します。詳細は、「A.1　nfa_ssl_keytool（157 ページ）」を参照してください。

1. root ユーザーで NFA サーバーにログインします。
2. 次のコマンドを実行し、出力されたメッセージの中から Owner 情報を確認します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ssl_keytool list -v
```

実行例:

```
# cd /opt/nec/nfa/controller/bin
# ./nfa_ssl_keytool list -v | grep '^Owner'
Owner: CN=nfa.nec.com, OU=IT Operation Division, O=NEC Corporation,
 L=Minato-ku, ST=Tokyo, C=JP
```

3. `nfa_ssl_keytool selfcert` コマンドを`-dname`, `-dns` オプション付きで実行し、識別名を更新します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ssl_keytool selfcert
 -dname <dname> -dns <FQDN>
```

確認した Owner 情報のうち、ドメイン名に関係する CN の値を変更して実行します。

実行例:

```
# ./nfa_ssl_keytool selfcert -dname "CN=new-nfa.nec.com,
 OU=IT Operation Division, O=NEC Corporation, L=Minato-ku,
 ST=Tokyo, C=JP" -dns new-nfa.nec.com
```

4. 公的な認証局に証明書を発行してもらっていた場合、証明書の再発行を依頼します。
   a. 次のコマンドを実行し、認証局に送付するための証明書署名要求 (CSR) をファイルに出力します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ssl_keytool
 certreq -dns <FQDN> <filename>
```

   指定したファイルに、CSR の内容がテキストで出力されます。

   b. 証明書署名要求 (CSR) を認証局に提出します。

nfa_ssl_keytool certreq コマンドで出力した CSR ファイルの内容を、認証局に提出します。

認証局は、CSR の内容を元に、証明書に署名し、返送します。署名済み証明書の返送には、認証局によっては数日かかる場合があります。

c. 認証局から返送された署名済み証明書をインポートします

nfa_ssl_keytool importcert コマンドを、-alias オプションは指定せずに実行します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ssl_keytool
 importcert <filename>
```

実行時に Failed to establish chain from reply というメッセージが表示された場合、証明書のチェーンが解決できなかったことを表しています。認証局のルート証明書や中間証明書がインポートされていない可能性があります。認証局に、インポートが必要な証明書を問い合わせてください。

5. NFA のサービスを再起動します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ctl.sh stop
# <%インストールディレクトリ%>/controller/bin/nfa_ctl.sh start
```

6. 自己署名証明書を使用している場合、nfa_ssl_keytool exportcert コマンドで、Web ブラウザーにインポートするための証明書をファイルに出力します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ssl_keytool exportcert
 <filename>
```

<*filename*>には任意のファイル名を指定できますが、Web ブラウザー側で簡単に証明書をインポートするために、ファイルの拡張子に.cer を指定することを強く推奨します。

nfa_ssl_keytool exportcert コマンドで出力した証明書ファイルは、NFA にアクセスするすべての Web ブラウザーに配布し、インポートしてください。Web ブラウザーに証明書をインポートすることで、NFA の Web サーバーに成りすますフィッシング攻撃などを予防することができます。

Web ブラウザーに証明書をインポートする方法は、「1.2.1.3　Web ブラウザーに SSL サーバー証明書をインポートする（11 ページ）」を参照してください。

NFA サーバー側の証明書の更新作業は、これで完了です。

公的な認証局に証明書を発行してもらった場合でも、使用する認証局によっては、Web ブラウザー側に別途、認証局の証明書をインストールするなどの作業が必要となる場合があります。詳細は、認証局の指示に従ってください。

5.1.7　環境設定をバックアップ、リストアする

NFA の環境設定バックアップ、およびそのリストアについて説明します。

環境設定のバックアップにより、NFA で設定を行った情報がバックアップできます。このバックアップからリストアすることで、バックアップ時点の環境設定に戻すことができます。

環境設定のバックアップには、以下の情報は含まれません。

- 蓄積したフローデータ
- 発生したイベントデータ
- 登録したライセンス情報

上記のデータは、リストアされないため、リストア先の環境の情報がそのまま残ります。

ヒント

蓄積したフローデータやイベントデータも含めてバックアップする方法もあります。詳細は「5.1.8　全データをバックアップ、リストアする（147 ページ）」を参照してください。

環境設定のバックアップは、全てのデータをバックアップする方法とは異なり、NFA のサービスを起動した状態で実施することができます。

リストアに関する注意事項

- バックアップ情報には、ライセンス情報は含まれていません。そのため、バックアップを取得した環境とリストア先の環境で登録されているライセンスに差がある場合は、リストアの前に、リストア先環境にバックアップ元の環境と同じ種類のライセンスを同じ数だけ登録してください。

  ライセンスの管理についての詳細は、「2.1　ライセンスを管理する（25 ページ）」を参照してください。

- バックアップしたデータは、同じバージョンの NFA にのみリストアすることができます。
- バックアップ元の環境とリストア先の環境で、NFA のドメイン名 (Web サーバーにアクセスするための URL) が異なる場合、SSL サーバー証明書を修正する必要があります。
- バックアップ元の環境とリストア先の環境で、カーネルパラメーター kernel.shmmax の値を揃えるか、リストア先の環境の値をバックアップ元の環境より大きく設定してください。

  バックアップ元の環境よりもリストア先の環境の kernel.shmmax の値が小さい場合は、リストア完了後にサービスが起動できない場合があります。

- 登録されているエクスポーターなどの情報は、システム単位で異なる内部 ID で管理されており、フローデータもその内部 ID を元に管理されています。そのため、バックアップ元の環境と異なるシステムにリストアする場合、リストア先の環境に蓄積していたフローデータの情報が、本来の情報とは異なる内容で表示される場合があります。

  リストア先は、同一システムにするか、インストール直後のフローデータが蓄積していない環境とすることをお勧めします。

5.1.7.1　環境設定をバックアップする

NFA の環境設定をバックアップする手順について説明します。

環境設定のバックアップは、NFA のサービスを起動した状態でも実施することができます。

1. root ユーザーで NFA サーバーにログインします。
2. 次のコマンドを実行します。

```
# cd <%インストールディレクトリ%>/controller/bin
# ./nfa_backup <path>
```

引数<*path*>には、バックアップを出力するディレクトリを指定します。

エラーメッセージが表示されず、コマンドが正常終了すると、指定した出力先ディレクトリにバックアップファイルが生成されています。

生成されたバックアップディレクトリは、他の記録媒体に退避するなどして、大切に保管してください。

5.1.7.2　環境設定のバックアップをリストアする

NFA の環境設定バックアップをリストアする手順について説明します。

バックアップのリストアは、NFA のサービスを停止した状態で実施する必要があります。

リストアに関して、いくつか注意事項があります。事前に、「リストアに関する注意事項（145 ページ）」を参照してください。

リストア作業を開始する前に、「5.1.7.1　環境設定をバックアップする（146 ページ）」で取得したバックアップディレクトリを NFA サーバーに配置しておく必要があります。

ヒント

「5.1.8.1　全データをバックアップする（148 ページ）」で取得したバックアップディレクトリを使用することもできます。その場合、フローデータやイベントデータはリストアされず、環境設定情報のみがリストアされます。

1. root ユーザーで NFA サーバーにログインします。
2. NFA のサービスを停止します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ctl.sh stop
```

3. 次のコマンドを実行し、NFA の環境設定をリストアします。

```
# cd <%インストールディレクトリ%>/controller/bin
# ./nfa_restore <path>
```

引数<*path*>には、バックアップが格納されているディレクトリを指定します。

エラーメッセージが表示されず、コマンドが正常終了すると、リストアは完了です。

⚠ 注意

OS や Python のバージョンによっては、実行時に警告(Warning)が表示される場合がありますが、リストアは正常に実施されるため問題はありません。

4. バックアップ元の環境とリストア先の環境で、NFA のドメイン名 (Web サーバーにアクセスするための URL) が異なる場合は、SSL サーバー証明書の更新作業を行います。

   作業手順は、「5.1.6　Web サーバーの URL を変更する（143 ページ）」を参照してください。

5. NFA のサービスを起動します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ctl.sh start
```

5.1.8　全データをバックアップ、リストアする

環境設定、蓄積データの一括バックアップ、およびそのリストアについて説明します。

環境設定および蓄積データの一括バックアップにより、NFA で設定を行った情報と蓄積したフローデータ、イベントデータを全てバックアップすることができます。このバックアップからリストアすることで、バックアップ時点の状態に戻すことができます。

なお、登録されたライセンス情報はバックアップされません。ライセンス情報だけは、バックアップ時点の状態に復元はされず、リストア先の環境の情報がそのまま残ります。

ヒント

蓄積したフローデータやイベントデータを含めずに環境設定のみバックアップする方法もあります。詳細は「5.1.7　環境設定をバックアップ、リストアする（144 ページ）」を参照してください。

全データのバックアップは、環境設定のバックアップとは異なり、NFA のサービスを起動した状態で実施することはできません。

バックアップに関する注意事項

- エクスポーターの台数が多い環境や、フローが多い環境では、バックアップするデータのサイズが数百 GB から数 TB になることがあります。バックアップデータの出力先や保存先の空き容量は十分確保した上で作業してください。
- バックアップのデータサイズが数百 GB から数 TB と非常に大きくなる場合、バックアップ処理に数時間から数十時間かかる場合があります。

リストアに関する注意事項

- バックアップしたデータは、同じバージョンの NFA にのみリストアすることができます。

- バックアップのデータサイズが数百 GB から数 TB と非常に大きい場合、リストア処理に数時間から数十時間かかる場合があります。
- バックアップ情報には、ライセンス情報は含まれていません。そのため、バックアップを取得した環境とリストア先の環境で登録されているライセンスに差がある場合は、リストアの前に、リストア先環境にバックアップ元の環境と同じ種類のライセンスを同じ数だけ登録してください。

  ライセンスの管理についての詳細は、「2.1　ライセンスを管理する（25 ページ）」を参照してください。
- バックアップしたデータは、同じバージョンの NFA にのみリストアすることができます。
- バックアップ元の環境とリストア先の環境で、NFA のドメイン名 (Web サーバーにアクセスするための URL) が異なる場合、SSL サーバー証明書を修正する必要があります。
- バックアップ元の環境とリストア先の環境で、カーネルパラメーター kernel.shmmax の値を揃えるか、リストア先の環境の値をバックアップ元の環境より大きく設定してください。

  バックアップ元の環境よりもリストア先の環境の kernel.shmmax の値が小さい場合は、リストア完了後にサービスが起動できない場合があります。

5.1.8.1　全データをバックアップする

環境設定、蓄積データを一括してバックアップする手順を説明します。

全データの一括バックアップは、NFA のサービスを停止した状態でのみ実施することができます。

バックアップに関して、いくつか注意事項があります。事前に、「バックアップに関する注意事項（147 ページ）」を参照してください。

1. root ユーザーで NFA サーバーにログインします。
2. バックアップ対象の現在のサイズを確認します。

   次のコマンドを実行し、サイズを確認してください。

   ```
   # du -sm <%データディレクトリ%>/{controller,collector}/{conf,db}
   ```

   結果は、個々のディレクトリ単位に MB 単位で表示されます。表示された数字を合算してください。

   実行例:

   ```
   # du -sm /opt/nec/nfa/{controller,collector}/{conf,db}
   1       /opt/nec/nfa/controller/conf
   92      /opt/nec/nfa/controller/db
   1       /opt/nec/nfa/collector/conf
   1016208 /opt/nec/nfa/collector/db
   ```

この例では、最大で約 993GB 程度のバックアップサイズになります。

3. NFA のサービスを停止します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ctl.sh stop
```

4. 次のコマンドを実行します。

```
# cd <%インストールディレクトリ%>/controller/bin
# ./nfa_backup -full <path>
```

引数<*path*>には、バックアップを出力するディレクトリを指定します。見積もったバックアップサイズに対して、十分な空き容量があるディスクを指定するように注意してください。

エラーメッセージが表示されず、コマンドが正常終了すると、指定した出力先ディレクトリにバックアップファイルが生成されています。

⚠ 注意

バックアップのサイズによっては、コマンドの完了までに数時間から数十時間かかる場合があります。

5. NFA のサービスを起動します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ctl.sh start
```

生成されたバックアップディレクトリは、他の記録媒体に退避するなどして、大切に保管してください。

5.1.8.2　全データのバックアップをリストアする

環境設定、蓄積データのバックアップをリストアする手順を説明します。

バックアップのリストアは、NFA のサービスを停止した状態で実施する必要があります。

リストアに関して、いくつか注意事項があります。事前に、「リストアに関する注意事項（147 ページ）」を参照してください。

リストア作業を開始する前に、「5.1.8.1　全データをバックアップする（148 ページ）」で取得したバックアップディレクトリを NFA サーバーに配置しておく必要があります。

1. root ユーザーで NFA サーバーにログインします。
2. NFA のサービスを停止します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ctl.sh stop
```

3. 次のコマンドを実行し、NFA の環境設定をリストアします。

```
# cd <%インストールディレクトリ%>/controller/bin
# ./nfa_restore -full <path>
```

引数<*path*>には、バックアップが格納されているディレクトリを指定します。

エラーメッセージが表示されず、コマンドが正常終了すると、リストアは完了です。

⚠ 注意

- バックアップのサイズによっては、コマンドの完了までに数時間から数十時間かかる場合があります。
- OS や Python のバージョンによっては、実行時に警告(Warning)が表示される場合がありますが、リストアは正常に実施されるため問題はありません。

4. バックアップ元の環境とリストア先の環境で、NFA のドメイン名 (Web サーバーにアクセスするための URL) が異なる場合は、SSL サーバー証明書の更新作業を行います。

   作業手順は、「5.1.6　Web サーバーの URL を変更する（143 ページ）」を参照してください。

5. NFA のサービスを起動します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ctl.sh start
```

5.1.9　証跡ログの保持期間を変更する

ユーザーの操作履歴を記録する証跡ログの保持期間を変更する手順について説明します。

証跡ログの保持期間のデフォルト値は、3 年間(1095 日間) となっています。証跡ログの保持期間を変更したい場合は、以下の操作を行います。

ヒント

証跡ログ 1 件のデータサイズは、約 300 Bytes です。1 日の証跡ログの件数を 1,000 件と仮定した場合、1 日分のデータサイズは約 300 KBytes となります。この値を目安に、設定変更後のディスク使用量において問題がないことを事前に確認することを推奨します。

1. root ユーザーで NFA サーバーにログインします。
2. NFA のサービスを停止します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ctl.sh stop
```

3. 設定ファイルの内容を変更し、上書きして保存します。

   設定ファイルと変更のための指定形式は以下の通りです。

   - 設定ファイル

     <%データディレクトリ%>/controller/conf/controller.properties

   - 指定形式

```
auditlog.max-duration = <保持日数>
```

<*保持日数*>で指定した日数分のデータを保持します。ここには、1~5000 の数値を指定することができます。

4. NFA のサービスを起動します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ctl.sh start
```

サービスの起動後、保持期間の変更内容が NFA コンポーネントに反映されます。

5.2　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。

5.2.1　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 5-3 フローデータの粒度と保持期間（151 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 5-3　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。

5.2.2　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、「5.2.1　フローデータの保持期間と丸め処理について（151 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。
- 以下で説明する見積もり内容には、ローデータを外部出力した際に必要となるディスク容量は含まれていません。ローデータを外部出力する運用を実施する場合は、「3.5　ローデータの外部出力設定を行う（85 ページ）」の内容を参照し、ローデータの外部出力で必要となるディスク容量の見積もりも行ってください。

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、「5.2.1　フローデータの保持期間と丸め処理について（151 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。

     ヒント

     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。最大フロー数の変更については、「5.2.3　保持するフロー数の上限を変更する（154 ページ）」を参照してください。

   - 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

5.2.3　保持するフロー数の上限を変更する

保持するフロー数の上限を変更する方法について説明します。

NFA では、デフォルトの動作として、エクスポーター、単位時間ごとに上位 1,000 フローを保持します。

この値は、設定により変更できます。

⚠ 注意

フロー数の上限値を大きくすると、NFA サーバーに対する負荷が増加します。よって、管理するエクスポーターの台数やフローの受信数、マシンスペック等の環境によっては、定常的に高負荷となり、NFA が正常に動作しない場合があります。

実際の動作環境にて 1 日以上運用させた状態で、以下のような観点で、正常に稼働することをご確認ください。

- エクスポーター管理画面にて、各エクスポーターの[**最終受信時刻**]に遅れが発生していないこと。
- ダッシュボード画面、エクスポーター分析画面にてフローデータが参照できること。

1. 環境設定画面を表示します。

   [**システム管理**] >[**環境設定**] をクリックします。

2. [**フローデータの上限数**]の入力欄に対し、保持するフローデータの上限数を設定します。

   フロー数の上限値は 1,000～10,000 の範囲で指定します。エクスポーターの台数を基準とした場合、以下の数値を目安にしてください。

   1 台～10 台

   上位 10,000 フロー

   11 台～20 台

   上位 6,000 フロー

   21 台～30 台

   上位 3,000 フロー

   31 台以上

   拡張は推奨しません。

ヒント

- 以下の設定ファイルを編集することにより上限数を変更することもできます。ファイルが存在しない場合は、新規に作成してください。なお、[**システム管理**] >[**環境設定**] から変更した場合、本設定ファイルの内容は上書きされます。
- ファイルの編集後は、設定を有効にするために NFA サービスを再起動してください。
- `<%データディレクトリ%>/controller/conf/flowdb.properties`
- 以下の 6 つの設定で指定されている値を、すべて同じ値に変更します。

```
flowdb.table.record.limit.1 = 1000
flowdb.table.record.limit.2 = 1000
flowdb.table.record.limit.3 = 1000
flowdb.table.record.limit.4 = 1000
flowdb.table.record.limit.5 = 1000
flowdb.table.record.limit.6 = 1000
```

5.2.4　フローの保持期間を変更する

フローデータの保持期間を変更する方法について説明します。

NFA では、「5.2.1　フローデータの保持期間と丸め処理について（151 ページ）」に基いて、フローデータをデータベースに保持する期間が決められています。

ヒント

フロー数やフローの保持期間の上限値を小さくしてから実際にデータが削除されるまでに、数分から 40 分程度の時間を要します。

1. 環境設定画面を表示します。

   [**システム管理**] >[**環境設定**] をクリックします。

2. [**フローデータの保持設定**]の各入力欄に対し、保持するフローデータの保持期間を設定します。

   指定する保持期間は上から順番に長い期間を設定する必要があります。例えば[**1 分粒度データ**]の保持期間に 36 時間を指定した場合は、[**10 分粒度データ**]は 36 時間以上の期間を設定する必要があります。

5.2.5　丸め処理の基準時刻を変更する

保持するフローデータの丸め処理を行う基準時刻を変更する方法について説明します。

NFA では、フローデータを長期間保持するために、「5.2.1　フローデータの保持期間と丸め処理について（151 ページ）」に基いて、データの粒度を変えて保持しています。データの粒度を変えるための丸め処理は、設定された基準時刻に基づいて実行されます。基準時刻は、NFA のインストール時に、サーバーのタイムゾーン設定を元に設定されます。

1. root ユーザーで NFA サーバーにログインします。

2. NFA のサービスを停止します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ctl.sh stop
```

3. 設定ファイル (collector.conf) を開きます。

   <%データディレクトリ%>/collector/conf/collector.conf

   設定ファイルが存在しない場合は、新規に作成してください。

ヒント

collector.conf は、フロー情報の受信用の通信ポート番号の設定変更などでも活用する設定ファイルです。

4. 設定ファイル (collector.conf) に、以下のパラメーターを追記し、保存します。

   指定形式:

```
collector.aggregation-offset = <±HHMM>
```

±HHMM :

UTC (協定世界時：Coordinated universal time) からのオフセットを指定します。

ヒント

設定ファイル (collector.conf) に本パラメーターを指定していない場合で、かつ、タイムゾーン設定が日本時間となっているサーバーにおいては、以下のパラメーターを指定した場合と同様の動作となります。

```
collector.aggregation-offset = +09:00
```

5. NFA のサービスを起動します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ctl.sh start
```

サービス起動後、丸め処理に対する基準時刻の変更内容が NFA に反映されます。

付録 A　コマンドリファレンス

NFA の提供するコマンドについて説明します。

A.1　nfa_ssl_keytool

HTTPS 通信で使用する SSL サーバー証明書の作成および管理を行うコマンドです。

このコマンドは、Java keytool コマンドの機能を本製品向けに使いやすい形で提供するラッパーコマンドです。本コマンドから使用できる機能は、Java keytool コマンドの一部のみです。また、引数の名前や意味は、Java keytool コマンドに合わせています。

Java keytool コマンドとの相違点は次の通りです。

- 最初の引数に `genkeypair` などのサブコマンド名を指定します。サブコマンドの引数名の先頭に - は付きません。
- 本コマンドでは、キーストアの形式は PKCS12 固定です。また、キーストアのパスは<%*データディレクトリ*%>/`controller/conf/server.keystore` 固定です。
- `genkeypair` サブコマンドを実行すると、キーストアのパスワード、キーストア内のエントリーの別名、鍵のパスワードが以下のファイルに記録されます。

  <%*データディレクトリ*%>/`controller/conf/tomcat.properties`

  ファイルに記録された各種情報は、各種サブコマンドで`-storepass`、`-alias` オプションを省略した際に自動で使用されます。そのため、引数の指定数を最小限に抑えてコマンドを実行することができます。
- `-keyalg`、`-validity` オプションのデフォルト値が異なります。
- `initstore` という独自のサブコマンドを実装しています。

パス

<%*インストールディレクトリ*%>/`controller/bin/nfa_ssl_keytool`

形式

```
nfa_ssl_keytool genkeypair [-help] [-storepass PASS] [-alias ALIAS]
    [-keyalg KEYALG] [-keysize KEYSIZE] [-sigalg SIGALG]
    [-validity DAYS] [-dname DNAME] [-dns DNS]
```

```
nfa_ssl_keytool selfcert [-help] [-storepass PASS] [-alias ALIAS]
    [-sigalg SIGALG] [-validity DAYS] [-dname DNAME] [-dns DNS]
```

```
nfa_ssl_keytool certreq [-help] [-storepass PASS] [-alias ALIAS]
    [-dns DNS] FILE
```

```
nfa_ssl_keytool importcert [-help] [-storepass PASS] [-alias ALIAS] FILE
```

```
nfa_ssl_keytool exportcert [-help] [-storepass PASS] [-alias ALIAS] FILE
```

```
nfa_ssl_keytool list [-help] [-storepass PASS] [-alias ALIAS] [-rfc | -v]
```

```
nfa_ssl_keytool delete [-help] [-storepass PASS] [-alias ALIAS]
```

```
nfa_ssl_keytool initstore [-help]
```

```
nfa_ssl_keytool -help
```

説明

各サブコマンドの意味は次の通りです。

- `genkeypair`

  鍵のペア (公開鍵および関連する非公開鍵) を生成し、キーストアに格納します。また、Web サーバーが生成した鍵を使用するための情報を以下のファイルに書き出します。

  `<%`***データディレクトリ***`%>/controller/conf/tomcat.properties`

- `selfcert`

  キーストアエントリーの鍵に対する自己署名証明書を作成します。

- `certreq`

  PKCS#10 形式を使って証明書署名要求 (CSR) を生成します。

- `importcert`

  ファイルから証明書または証明書チェーンを読み取り、キーストアに格納します。

- `exportcert`

  証明書をキーストアから読み取り、バイナリ符号化方式の証明書としてファイルに格納します。

- `list`

  特定のキーストアエントリー、またはキーストア全体の内容を表示します。

- `delete`

  キーストアから特定のエントリーを削除します。

- `initstore`

  キーストアファイルを削除します。

引数

-storepass *PASS*

キーストアのパスワードを指定します。

`genkeypair` サブコマンドの実行時に省略した場合は、コマンド実行中にパスワードの入力が求められます。それ以外のサブコマンドの実行時に省略した場合は、tomcat.properties ファイルから読み取った値を使用します。

-alias *ALIAS*

キーストア内のエントリーの別名を指定します。

`genkeypair` サブコマンドの実行時に省略した場合は、デフォルト値の「tomcat」が使用されます。また、`list` サブコマンドの実行時に省略した場合は、すべてのエントリーが対象になります。それ以外のサブコマンドの実行時に省略した場合は、tomcat.properties ファイルから読み取った値を使用します。

-keyalg *KEYALG*

鍵の暗号化アルゴリズムを指定します。「RSA」、「DSA」、「EC」などを指定することができます。デフォルトは「RSA」です。

`-keyalg`、および`-sigalg` に指定できるアルゴリズム一覧は、Java 暗号化アーキテクチャ (JCA) リファレンス・ガイド を参照してください。

-keysize *KEYSIZE*

生成する鍵のサイズを指定します。

指定可能な値およびデフォルト値は、Java keytool の仕様に準拠しています。

-sigalg *SIGALG*

自己署名証明書に署名を付けるときに使うアルゴリズムを指定します。

指定するアルゴリズムは、`-keyalg` と互換性のあるものでなければなりません。指定可能な値およびデフォルト値は、Java keytool の仕様に準拠しています。

-validity *DAYS*

自己署名証明書が有効と見なされる日数を指定します。0 ～ 365000 が指定できます。デフォルトは 3650 (約 10 年) です。

-dname *DNAME*

自己署名証明書の issuer フィールドと subject フィールドとして使う X.500 識別名を指定します。

識別名を指定しなかった場合は、コマンド実行中に識別名の入力を求められます。

-dns *DNS*

証明書の Subject Alternative Name 拡張領域に登録する FQDN を指定します。

genkeypair サブコマンドでは、指定しなかった場合は証明書の Common Name が使用されます。

-new *NEWPASS*

キーストアまたは鍵のパスワードを変更する際に、変更後のパスワードを指定します。

省略した場合は、コマンド実行中にパスワードの入力が求められます。

-rfc

list サブコマンドの出力形式指定オプションです。出力可能符号化方式で証明書の内容が出力されます。

-v オプションと同時に指定することはできません。

-v

list サブコマンドの出力形式指定オプションです。人間が読むことのできる形式で、証明書の内容詳細が出力されます。

-rfc オプションと同時に指定することはできません。

-help

コマンド全体、または各コマンドの使用方法を表示します。

戻り値

成功時には 0 を返します。失敗時には 0 以外の値を返します。

ヒント

バージョン 2.0 以前で作成したキーストアの形式は、Java KeyStore (JKS) となります。JKS 形式を利用している場合、以下のサブコマンドが追加で使用できます。

```
nfa_ssl_keytool storepasswd [-help] [-storepass PASS] [-new NEWPASS]
```

```
nfa_ssl_keytool keypasswd [-help] [-storepass PASS] [-alias ALIAS]
    [-keypass KEYPASS] [-new NEWPASS]
```

- storepasswd

  キーストアのパスワードを変更します。

- keypasswd

  キーストアエントリーの鍵パスワードを変更します。

また、各サブコマンドに-keypass オプションが指定できます。

-keypass *KEYPASS*

鍵のパスワードを指定します。

genkeypair サブコマンドの実行時に省略した場合は、コマンド実行中にパスワードの入力が求められます。それ以外のサブコマンドの実行時に省略した場合は、tomcat.properties ファイルから読み取った値を使用します。

A.2　nfa_flow_export

データベース内に蓄積されたフローデータを外部の CSV ファイルに出力するコマンドです。

本コマンドは、CSV ファイルへ出力するフローデータの種類と粒度、および対象とする期間などを指定して、実行します。

- 対象とするデータの種類

  データの種類は、大きく分けて以下の 2 つの種類があります。

  - エクスポーター 1 台に着目した詳細なフローデータ
  - 全エクスポーターの情報をまとめた、ネットワーク全体のフローデータ

    ネットワーク全体のフローデータは、エクスポーターおよびインターフェイスの通信量、送信元/宛先 IP アドレス、アプリケーション、IP プロトコル、ToS(DSCP)、送信元/宛先 AS 番号の 6 種類から選択します。

- 対象とするデータの粒度

  NFA では一定の期間ごとに、フローデータを集約(丸め処理)し、データの粒度を変えて保持しています。どの粒度のデータを出力するかも、パラメーターとして指定します。データの粒度と丸め処理の詳細は、「5.2.1　フローデータの保持期間と丸め処理について（151 ページ）」を参照してください。

- 対象とする期間

  出力するデータの開始日時と終了日時を指定して、データを出力します。

  また、定期的に繰り返し実行するためのモードとして、前回出力時の終了時刻以降のデータを出力するという指定の方法もあります。

データの種類や粒度、期間の他には、出力するフローデータを条件によって絞り込む指定(フィルタリング)や、CSV ファイルの出力先などを指定します。

コマンドのパラメーターの指定方法は、コマンドの引数として直接指定する方法と、パラメーターを設定ファイルに記載して指定する方法の 2 通りがあります。コマンドの引数として直接指定する場合は、1 回の実行で出力するフローデータは 1 種類になります。設定ファイルを用いると、1 回の実行で複数種類のフローデータの CSV ファイルを出力することができます。

出力される CSV ファイルの形式は、「A.2.2　出力 CSV ファイルの形式（171 ページ）」を参照してください。

パス

<%*インストールディレクトリ*%>/collector/bin/nfa_flow_export

形式

```
nfa_flow_export -type DATATYPE -level { 1 | 2 | 3 | 4 | 5 | 6 }
    {-period START END | -continue} -out OUTDIR [OPTIONS...]
```

```
nfa_flow_export -file FILEPATH
```

```
nfa_flow_export -help
```

引数 (パラメーターをコマンド引数で指定する場合)

-type *DATATYPE*

出力するデータタイプを指定します。指定必須です。指定できるデータタイプは以下です。

- exporter *EXPORTER*[:*INTERFACE*]

  指定したエクスポーターおよびそのインターフェイスのフローデータを出力します。`exporter` キーワードに続いて、エクスポーターを指定します。エクスポーターに続いて「:」およびインターフェイスを指定することで、特定インターフェイスに限定したデータを出力することもできます。

  エクスポーター、インターフェイスはそれぞれ 1 つのみ指定可能です。エクスポーターやインターフェイスの指定には、表示名の他に IP アドレスや ifIndex 値、IF グループ名なども使用できます。詳細は「値の指定書式に関する補足（167 ページ）」を参照してください。

- traffic

  全エクスポーターとインターフェイスの通信量に関するフローデータを出力します。

- ipaddr

  ネットワーク全体の IP アドレス(通信エンドポイント)に関するフローデータを出力します。

- app

  ネットワーク全体のアプリケーションに関するフローデータを出力します。

- ipprot

  ネットワーク全体の IP プロトコルに関するフローデータを出力します。

- tos

  ネットワーク全体の ToS(DSCP)値に関するフローデータを出力します。

- as

  ネットワーク全体の AS 番号に関するフロー情報を出力します。

-level { 1 | 2 | 3 | 4 | 5 | 6 }

エクスポートするデータの粒度をレベルを表す 1～6 の数値で指定します。指定必須です。

レベルとデータの粒度の関係は「フローデータの粒度と指定可能期間の関係（164 ページ）」を参照してください。

-period *START　END*

出力するフローデータの期間の開始日時および終了日時を指定します。`-period` または`-continue` のいずれか一方を指定します。両方同時に指定はできません。

日時は、yyyymmdd または yyyymmddhhmm[ss] の形式で指定します。

`-level` に指定したレベルに応じて、開始日時と終了日時の幅に制限があります。詳細は「フローデータの粒度と指定可能期間の関係（164 ページ）」を参照してください。

-continue

前回実行時に出力した最後のフローデータから現在時刻までのフローデータを出力する場合に指定します。`-continue` または`-period` のいずれか一方を指定します。両方同時に指定はできません。

`-out` で指定したディレクトリに対する初回実行時には、実行時刻の記録のみ行い、フローデータは出力しません。次回実行時からフローデータを出力します。

`-level` に指定したレベルに応じて、一度の`-continue` 実行で出力できる期間に制限があります。詳細は「フローデータの粒度と指定可能期間の関係（164 ページ）」を参照してください。

-out

出力先ディレクトリを指定します。指定必須です。

絶対パスまたは相対パスの指定が可能です。指定するディレクトリは事前に作成しておく必要があります。

-filter *CONDITIONS*

出力するフローデータを絞り込む条件を指定します。条件を指定すると、その条件に該当するフローデータのみ出力されます。

詳細な指定方法は「フィルター条件の指定方法（165 ページ）」を参照してください。

-full

画面には表示されない、詳細なフロー情報も含めて出力します。出力内容の変化については、「A.2.2　出力 CSV ファイルの形式（171 ページ）」を参照してください。

`-type` に `exporter` を指定した場合に使用できるオプションです。

-limit *N*

1 回の実行で出力するフローデータの件数の最大値を指定します。通信量(byte 単位)の多いフローデータから順に出力し、指定件数を超えるフローデータは出力しません。

指定しない場合は、出力件数の制限を行いません。

-limit-by-packet

`-limit` オプションで件数制限する際の出力優先度を、通信量(byte 単位)の多い順から、通信パケット数が多い順に変更します。

-line *N*

CSV ファイル 1 つに出力する最大行数を指定します。指定しない場合は、1 ファイルあたり 65,535 行まで出力します。指定できる最大値は 1,048,575 です。

出力するデータが 1 つのファイルに収まらない場合は、ファイルを分割します。分割されたファイルは、ファイル名末尾が _001.csv、_002.csv のように連番になります。

-no-header

指定すると、CSV ファイル中の 1 行目にヘッダーフィールド行を出力しません。

引数 (パラメーターを設定ファイルで指定する場合)

-file *FILE*

パラメーターを記載した設定ファイル(パラメーター設定ファイル)を指定して、本コマンドを実行します。

パラメーター設定ファイルを使用することで、1 回のコマンドで複数の対象に対し一括でデータ出力することができます。対象が多数の場合は、パラメーター設定ファイルを準備して実行することを推奨します。

パラメーター設定ファイルの形式については、「A.2.1　パラメーター設定ファイルの形式（168 ページ）」を参照してください。

引数 (その他)

-help

コマンドの使用方法を表示します。

戻り値

成功時には 0 を返します。失敗時には 0 以外の値を返します。

フローデータの粒度と指定可能期間の関係

フローデータは、データの粒度ごとにレベルを分けて保持しています。本コマンドの `-period` で指定できる最小時間幅・最大時間幅は、レベルごとに決まっています。同様に、`-continue` で実行する際に一度に出力できる最大時間幅もレベルごとに決まっています。

「表 A-1 フローデータの粒度と指定可能期間の対応表（165 ページ）」に、レベルごとの最小時間幅および最大時間幅を示します。

表 A-1　フローデータの粒度と指定可能期間の対応表

レベル	データの粒度(単位時間)	最小時間幅	最大時間幅
1	1 分	1 分	60 分
2	10 分	10 分	12 時間
3	60 分	60 分	3 日
4	6 時間	6 時間	14 日
5	24 時間	24 時間	60 日
6	7 日	7 日	365 日

`-period` で指定する時間幅は、これらの値の範囲に収まるように指定してください。例えば、2017/4/1 の 10:00 からレベル 1 の最大時間幅(60 分)でデータを出力する場合は、`-period 201704011000 201704011059` と指定します。

`-continue` で定期的に出力する場合は、最大時間幅の半分程度の間隔で繰り返し実行することを推奨します。また、最後の実行から最大時間幅を超える期間が空いた場合は、`-continue` による繰り返し実行の間隔を一時的に狭めると、より迅速に最新時刻に追いつくことができます。

ヒント

`-continue` を指定してのコマンドが、フローデータが存在しない期間に対して実行されると、フローデータが存在する期間の最古のデータから CSV ファイルへ出力されます。例えば、保持期間がデフォルトで、レベル 1 のデータに対する実行が最後の出力から 30 時間空いた状況を考えます。この状況で`-continue` を指定してコマンドを実行すると、保持期間(24 時間)を超えているため、フローデータが存在する 24 時間前から 23 時間前までの 60 分間のフローデータを CSV ファイルに出力します。この場合も、`-continue` を指定してのコマンド実行を連続して行うことで、迅速に最新時刻に追いつくことができます。

データの保持期間に関する詳細は、「5.2.1　フローデータの保持期間と丸め処理について（151 ページ）」を参照してください。

フィルター条件の指定方法

フィルター条件は、フィルターの名前と条件に指定する値を「=」で結合して指定します。「=」の前後には空白を入れません。

指定できるフィルター条件は以下の通りです。

- exporter=*EXPORTER*[:*INTERFACE*][,*EXPORTER*[:*INTERFACE*]...]

  エクスポーターでフィルタリングを行います。エクスポーターに続いて「:」およびインターフェイスを指定することで、特定インターフェイスに限定してフィルタリングします。

エクスポーターやインターフェイスの指定には、表示名の他に IP アドレスや ifIndex 値、IF グループ名なども使用できます。詳細は「値の指定書式に関する補足（167 ページ）」を参照してください。

`-type` が `traffic`、`ipaddr`、`app`、`ipprot`、`tos`、`as` の場合に有効なフィルターです。

- srcip=*IPADDR*[,*IPADDR*...]

  送信元 IP アドレスでフィルタリングを行います。

  `-type` が `exporter` または `ipaddr` の場合に有効なフィルターです。

- dstip=*IPADDR*[,*IPADDR*...]

  宛先 IP アドレスでフィルタリングを行います。

  `-type` が `exporter` または `ipaddr` の場合に有効なフィルターです。

- srcendpt=*GROUP*[,*GROUP*...]

  送信元エンドポイントグループ名でフィルタリングを行います。

  `-type` が `exporter` または `ipaddr` の場合に有効なフィルターです。

- dstendpt=*GROUP*[,*GROUP*...]

  宛先エンドポイントグループ名でフィルタリングを行います。

  `-type` が `exporter` または `ipaddr` の場合に有効なフィルターです。

- app=*APPLICATION*[,*APPLICATION*...]

  アプリケーション名でフィルタリングを行います。

  `-type` が `exporter` または `app` の場合に有効なフィルターです。

- ipprot=*PROTOCOL*[,*PROTOCOL*...]

  IP プロトコルでフィルタリングを行います。IP プロトコル名または IP プロトコル番号が指定できます。

  `-type` が `exporter` または `ipprot` の場合に有効なフィルターです。

- dscp=*DSCP*[,*DSCP*...]

  DSCP 値(PHB)でフィルタリングを行います。DSCP 値(6 桁の 2 進数)または PHB が指定できます。

  `-type` が `exporter` または `tos` の場合に有効なフィルターです。

- srcas=*AS*[,*AS*...]

  送信元 AS 番号でフィルタリングを行います。

  `-type` が `exporter` または `as` の場合に有効なフィルターです。

- dstas=*AS*[,*AS*...]

  宛先 AS 番号でフィルタリングを行います。

-type が exporter または as の場合に有効なフィルターです。

それぞれの条件の右辺は、コンマ区切りで複数並べることで、いずれかの値に一致する場合に出力する、という OR 条件でフィルタリングを行えます。コンマの前後には空白を入れずに指定します。

また、複数の条件をスペースで区切って指定することで、すべての条件に一致する場合に出力する、という AND 条件でフィルタリングを行えます。

値の指定書式に関する補足

- エクスポーターの指定

  本コマンドでエクスポーターを指定する箇所では、表示名、または IP アドレスが指定できます。

  エクスポーター名に含まれうる文字のうち、コロン(:) は、インターフェイス指定との区切り文字として特別な意味を持つので、コロンそのものを含める場合は、コロンの直前に「\」を挿入してエスケープする必要があります。

  ヒント

  bash などのシェルでは、コマンドライン上で「\」を入力すると、特殊なエスケープ文字として処理され、文字として認識されない場合があります。その場合、指定の名前全体をクオート文字(' ' や " ")で囲うことで、正しく指定できます。

  例) エクスポーター名が Asystem:exporter1 の場合

  ```
  # ./nfa_flow_export -type exporter 'Asystem\:exporter1:GBE0/1' ...
  ```

- インターフェイスの指定

  本コマンドでインターフェイスを指定する箇所では、表示名、または ifIndex 値が指定できます。また、IF グループ名も指定できます。

  インターフェイス名についても、エクスポーター名と同様に、コロン(:)が特別な意味を持つので、コロンそのものを含める場合は、コロンの直前に「\」を挿入してエスケープする必要があります。

- IP プロトコルの指定

  本コマンドで入力可能な IP プロトコル名および IP プロトコル番号は、IANA が公開している Protocol Numbers の定義に準拠しています。IP プロトコル名の指定では、大文字、小文字は区別されます。

  http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml [*1]

- フィルター条件の値の指定

*1　この URL は、2021 年 9 月現在のものです。

フィルター条件の値(右辺)は、コンマ区切りで複数の値を指定することができます。条件値にコンマそのものを含める場合は、コンマの直前に「\」を挿入してエスケープする必要があります。

- コマンドラインからの空白を含む値の指定

  エクスポーター名やインターフェイス名、フィルター条件の値など、空白文字を含む値をコマンドラインから指定すると、空白文字が引数の切れ目として認識され、意図通りの値が指定できません。

  指定する値に空白文字が含まれる場合は、値全体をクオート文字(' ' や " ")で囲みます。

注意事項

- 本コマンドを実行するためには、NFA サービスが起動している必要があります。また、本コマンドは、root ユーザーのみ実行できます。
- エクスポーターを表示名で指定する際、同じ表示名を持つエクスポーターが複数存在すると、対象を一意に特定できないため、エラーとなります。重複する表示名を持つエクスポーターを指定する場合は、表示名の代わりに IP アドレスで指定するか、表示名が重複しないように名前を変更してください。

  同様に、1 つのエクスポーターに属するインターフェイスと IF グループの表示名が重複している場合も、そのインターフェイス表示名を指定すると、対象を一意に特定できずエラーとなる場合があります。この場合は、表示名の代わりに ifIndex 値を指定するか、表示名が重複しないように名前を変更してください。
- 数字のみからなる名前を持つ IF グループを指定すると、インターフェイスの ifIndex 値の指定と区別が付かず、意図通りに指定できない場合があります。指定する IF グループには、数字以外の文字を含む名前をあらかじめ設定してください。
- 本コマンドを実行すると、`-out` で指定したディレクトリ内に、CSV ファイルの他に nfa_flow_export.dat というファイルが作成されます。このファイルには、出力の対象や最後に出力したデータの時刻などの実行情報が記録されます。このファイルを削除すると`-continue` による継続出力が意図通りに動作しません。

A.2.1　パラメーター設定ファイルの形式

`nfa_flow_export` コマンドの`-file` 引数に渡すパラメーター設定ファイルの形式について説明します。

ファイルフォーマット

入力ファイルは、以下の規則に従って作成してください。

- パラメーター設定ファイルは、UTF-8 エンコーディングで記載します。

ヒント

設定ファイルに記載できる文字は、コマンドを実行する環境のロケールに依存します。UTF-8 ロケールでコマンドを実行することで、すべての UTF-8 文字が使用できます。

- 各行の先頭が「#」から始まる行は、コメント行として扱われ、無視されます。
- 出力データの単位で、設定を構成します。

  大括弧 [ ] 内に任意の設定名を記載し、それ以降の行に、コマンドライン引数で設定できる内容を記載します。大括弧 [ ] から次の [ ] までをセクションと呼びます。セクションの設定名は、ファイル内で一意である必要があります。
- セクション内には、コマンドライン引数に相当する設定を、1 行に 1 つずつ記載します。記載する設定は、***パラメーター名 ： 値*** の形式です。パラメーター名には、コマンドライン引数名の先頭から「-」を除いた名前を指定します。値は、コマンドライン引数に指定する内容と同じです。例えば、`-type exporter` *エクスポーター名*に相当する内容を記載するには、`type : exporter` ***エクスポーター名***と記載します。

  `-continue` や`-full` などの値を持たないオプション引数を指定するには、値に「on」と記載します。値が「on」であれば、そのオプションが設定されます。値に「off」と記載すると、そのパラメーターは設定されていないものとして扱われます。
- DEFAULT という名前のセクションは、特別なセクションとして扱われます。

  DEFAULT セクションに設定した内容は、他のすべてのセクションのデフォルト値として扱われます。例えば、すべての設定に対して同じ期間(period)を指定したい場合は、DEFAULT セクションに `period` パラメーターを記載することで、他のセクションに `period` パラメーターを記載しなくても実行することができます。

  なお、`out` パラメーターは DEFAULT セクションに記載することができません。各セクションにそれぞれ記載する必要があります。

値の指定書式に関する補足

ファイルに記載するパラメーターの値は、基本的にはコマンドライン引数に設定する値と同じですが、以下の違いがあります。

- フィルター条件の複数指定

  コマンドライン引数で`-filter` に複数種のフィルター条件を指定する場合、空白文字で区切って指定します。一方、パラメーター設定ファイルに複数のフィルター条件を書く場合は、空白文字ではなく改行で区切ります。また、改行後の行は先頭を空白文字からはじめます。具体例は「記載例（170 ページ）」を参照してください。
- 「%」を含む値の指定

  「%」を含む値を指定するには、「%%」と二重に記載する必要があります。
- 空白文字を含む値の指定

コマンドライン引数とは異なり、空白を含む値を指定する場合でも、クオート文字で囲う必要はありません。

その他、コマンドライン引数の指定と同様に、以下の文字を使用する場合はエスケープが必要です。

- エクスポーター名やインターフェイス名にコロン(:)そのものを含める場合は、コロンの直前に「\」を挿入してエスケープする必要があります。
- フィルター条件の値にコンマ(,)そのものを含める場合は、コンマの直前に「\」を挿入してエスケープする必要があります。

記載例

以下は、2017/4/1 10:00 から 30 分間分のレベル 1 (1 分粒度) のフローデータを、3 台のエクスポーターについて出力する設定例です。

```
[DEFAULT]
period : 201704011000 201704011029
level : 1

[Router01]
type : exporter Router01
out : /csvdata/Router01/

[Router02]
type : exporter Router02
out : /csvdata/Router02/

[Router03]
type : exporter Router03
out : /csvdata/Router03/
```

以下は、1 つのデータタイプに対し、複数の異なるフィルター条件を指定して、繰り返し実行する場合の設定例です。

```
[DEFAULT]
continue : on
level : 2
type : ipaddr

[src/dst address: Router01 (1)]
# Router01 上でキャプチャされた、宛先：192.168.0.10 に関するフロー
out : /csvdata/ipaddr-Router01-1/
filter : exporter=Router01
  dstip=192.168.0.10

[src/dst address: Router01 (2)]
# Router01 上でキャプチャされた、宛先：192.168.0.20 に関するフロー
out : /csvdata/ipaddr-Router01-2/
filter : exporter=Router01
  dstip=192.168.0.20

[src/dst address: Router02 GBE0/1]
```

```
# Router02, Gigabitethernet0/1 上でキャプチャされたフロー
out : /csvdata/ipaddr-Router02-if01/
filter : exporter=Router02:Gigabitethernet0/1

[src/dst address: Router02 GBE0/2]
# Router02, Gigabitethernet0/2 上でキャプチャされたフロー
out : /csvdata/ipaddr-Router02-if02/
filter : exporter=Router02:Gigabitethernet0/2
```

A.2.2　出力 CSV ファイルの形式

nfa_flow_export コマンドが出力する CSV ファイルの形式について説明します。

出力ファイル名

出力されるファイル名の命名規則は以下の通りです。

*<yyyymmddhhmmss>*_<***データタイプ***>_<***連番***>.csv

- *yyyymmddhhmmss*

  コマンドの実行を開始した日時です。

- *データタイプ*

  -type に指定したデータタイプ名です。

  exporter を指定した場合は、データタイプ名(exporter)の代わりに、指定したエクスポーターの名前になります。また、インターフェイスも指定していた場合は、インターフェイスの名前も付与されます。エクスポーターやインターフェイスの名前のうち、ファイルシステムで使用できない文字は「_」に置換されます。

- *連番*

  3 桁の連番です。001 から始まります。一度に出力されるデータ数が多い場合は 001、002、003 と複数ファイルに分割されます。

例) エクスポーター Router の、インターフェイス Gigabitethernet1/1 を対象とした場合

20170401100147_Router_Gigabitethernet1_1_001.csv

出力フォーマット

CSV ファイルの構成は以下の通りです。

- 文字エンコーディングは UTF-8 で出力されます。
- 1 行目は、項目名の書かれたヘッダーフィールド行です。

  -no-header オプションを指定して実行した場合は、ヘッダーフィールド行は省略され、1 行目からフローデータが出力されます。

- 2 行目以降は、フローデータが出力されます。フローデータは日時の昇順に出力されます。

「表 A-2 CSV ファイルの列一覧（172 ページ）」に、出力列の一覧を示します。また、出力列はデータタイプによって異なります。データタイプと出力列の対応を「表 A-3 データタイプ別の出力列一覧（173 ページ）」に示します。

表 A-2　CSV ファイルの列一覧

列名	説明
DATE	NFA がフローを受信した時刻。 受信時刻は、データの粒度(単位時間)で切り捨てられます。
EXPORTER	フローを検出したエクスポーター名。 フィルター条件「exporter」に対応します。
BYTES	フローの通信量(オクテット数)。
PKTS	フローの通信パケット数。
PROTOCOL	IP プロトコル名。 名前が定義されていない場合は、IP プロトコル番号を出力されます。 フィルター条件「ipprot」に対応します。
TOS	TOS (Type Of Service) フィールド値。 10 進数表記で出力されます。
TCP_FLAGS	TCP ヘッダに含まれるコントロールフラグの論理和。 FIN=0x01, SYN=0x02, RST=0x04, PSH=0x08, ACK=0x10, URG=0x20, ECE=0x40, CWR=0x80, NS=0x0100 として、ON になっているフラグの論理和が 16 進数表記で出力されます。
L4_SRC_PORT	送信元ポート番号。
IPV4_SRC_ADDR	送信元 IPv4 アドレス。 フィルター条件「srcip」に対応します。
SRC_MASK	送信先 IPv4 アドレスのサブネットマスク値。
INPUT_IF	エクスポーター上の入力インターフェイス名。 IF グループに該当する場合は、IF グループ名が出力されます。 フィルター条件「exporter」のインターフェイス指定に対応します。
L4_DST_PORT	宛先ポート番号。
IPV4_DST_ADDR	宛先 IPv4 アドレス。 フィルター条件「dstip」に対応します。
DST_MASK	宛先 IPv4 アドレスのサブネットマスク値。
OUTPUT_IF	エクスポーター上の出力インターフェイス名。 IF グループに該当する場合は、IF グループ名が出力されます。 フィルター条件「exporter」のインターフェイス指定に対応します。
IPV4_NEXT_HOP	次の転送先ルーターの IPv4 アドレス。
SRC_AS	送信元 AS 番号。 フィルター条件「srcas」に対応します。
DST_AS	宛先 AS 番号。 フィルター条件「dstas」に対応します。
FRAMETYPE	Ethernet フレームのタイプを表す文字列。

列名	説明
	「Ethernet 2」、「IEEE802.3 SNAP」、「IEEE802.3 RAW」、「IEEE802.3 LLC」のいずれかの文字列で出力されます。
ETHERTYPE	Ethernet フレームのタイプ値。 16 進数表記で出力されます。
VLAN_TAG	VLAN ID。
APP	アプリケーション名。 フィルター条件「app」に対応します。
SRC_ENDPOINT_GROUP	送信元エンドポイントグループ名。 フィルター条件「srcendpt」に対応します。
DST_ENDPOINT_GROUP	宛先エンドポイントグループ名。 フィルター条件「dstendpt」に対応します。
SRC_HOSTNAME	送信元 IPv4 アドレスに該当する FQDN 名。
DST_HOSTNAME	宛先 IPv4 アドレスに該当する FQDN 名。
DSCP	DSCP 値(PHB)。 対応する PHB がない値の場合は、6 桁の 2 進数で出力します。

ヒント

NFA では、単位時間ごとに保持するフローデータの上限数が決まっており、上限を超えたフローデータは「その他」としてまとめられます。「その他」のフローは、DATE、BYTES、PKTS の列以外が空欄となり、単位時間ごとの最後のデータとして出力されます。

フローデータの丸め処理については、「5.2.1　フローデータの保持期間と丸め処理について（151 ページ）」も参照してください。

表 A-3　データタイプ別の出力列一覧

列名	exporter	exporter (-full)	traffic	app	ipaddr	ipprot	as	tos
DATE	Y	Y	Y	Y	Y	Y	Y	Y
EXPORTER			Y	Y	Y	Y	Y	Y
BYTES	Y	Y	Y	Y	Y	Y	Y	Y
PKTS	Y	Y	Y	Y	Y	Y	Y	Y
PROTOCOL	Y	Y				Y		
TOS	Y	Y						Y
TCP_FLAGS		Y						
L4_SRC_PORT	Y	Y						
IPV4_SRC_ADDR	Y	Y			Y			
SRC_MASK		Y						
INPUT_IF	Y	Y	Y	Y	Y	Y	Y	Y
L4_DST_PORT	Y	Y						
IPV4_DST_ADDR	Y	Y			Y			
DST_MASK		Y						
OUTPUT_IF	Y	Y	Y	Y	Y	Y	Y	Y

列名	exporter	exporter (-full)	traffic	app	ipaddr	ipprot	as	tos
IPV4_NEXT_HOP		Y						
SRC_AS	Y	Y					Y	
DST_AS	Y	Y					Y	
FRAMETYPE		Y						
ETHERTYPE		Y						
VLAN_TAG		Y						
APP	Y	Y		Y				
SRC_ENDPOINT_GROUP	Y	Y			Y			
DST_ENDPOINT_GROUP	Y	Y			Y			
SRC_HOSTNAME		Y			Y			
DST_HOSTNAME		Y			Y			
DSCP	Y	Y						Y

A.2.3　使用例

nfa_flow_export コマンドの使用例を説明します。

特定のエクスポーターについて指定期間のフローデータを出力する

エクスポーター Router01 の全インターフェイスを対象として、1 時間粒度の詳細なフローデータを 2017/4/1～4/2 の 2 日分出力するには、以下のコマンドを実行します。

```
# mkdir -p /nfa-csv
# /opt/nec/nfa/collector/bin/nfa_flow_export -type exporter Router01
    -period 20170401 20170402 -level 3 -full -out /nfa-csv/
```

コマンドを実行すると、/nfa-csv ディレクトリに CSV ファイルが出力されます。

全エクスポーターの情報をまとめたネットワーク全体のフローデータを定期的に出力する

すべてのエクスポーターの情報をまとめたネットワーク全体のフローデータとして、エクスポーターおよびインターフェイスの通信量、送信元/宛先 IP アドレス、アプリケーション、IP プロトコル、ToS(DSCP)、送信元/宛先 AS 番号の 6 つの種類を出力できます。これらを対象として、1 分粒度のフローデータを定期的に出力するには、まず以下のファイルを作成します。

```
[DEFAULT]
continue : on
```

```
level : 1

[Traffic]
type : traffic
out : /nfa-csv/traffic

[Endpoint IP Address]
type : ipaddr
out : /nfa-csv/ipaddr

[Application]
type : app
out : /nfa-csv/app

[IP protocol]
type : ipprot
out : /nfa-csv/ipprot

[DSCP]
type : tos
out : /nfa-csv/dscp

[AS number]
type : as
out : /nfa-csv/as
```

作成したファイルを /nfa-csv/flowexport.conf として保存します。

続いて、out パラメーターに設定したディレクトリを作成します。

```
# mkdir /nfa-csv
# cd /nfa-csv
# mkdir traffic app ipaddr ipprot dscp as
```

準備ができたら、cron などに nfa_flow_export コマンドを定期的に実行するように設定します。

以下は、cron を使用して 30 分ごとに実行する設定例です。

```
0,30 * * * *    /opt/nec/nfa/collector/bin/nfa_flow_export
    -file /nfa-csv/flowexport.conf
```

毎時 0 分、30 分に、/nfa-csv ディレクトリの下のサブディレクトリに、それぞれ CSV ファイルが作成されます。

cron の設定に関する詳細は、OS の提供するマニュアルを参照してください。

ヒント

nfa_flow_export コマンドは、出力した CSV ファイルの管理は行いません。出力した CSV ファイルは、定期的に外部サーバーに移動するなどしてディスク容量を圧迫しないように運用する必要があります。

過去から現在までのフローデータを連続出力する

例えばネットワーク遅延調査を目的として、過去から現在までのフローデータを連続して出力し、外部に保存しておくこともできます。

以下は、2017/4/1 10:00 の時点からはじめて、2017/4/1 0:00 からの 1 分粒度のフローデータをすべて出力する例です。

1. 1 回目の実行は、-period を使用して 60 分間のデータを出力します。

```
# mkdir /nfa-csv
# /opt/nec/nfa/collector/bin/nfa_flow_export -type exporter Router01
    -period 201704010000 201704010059 -level 1 -full -out /nfa-csv/
```

2. 1 回目の実行から時間を開けず、2 回目を実行します。2 回目以降の実行は、-period ではなく-continue を使用することで、前回実行の続きのデータから出力することができます。

```
# /opt/nec/nfa/collector/bin/nfa_flow_export -type exporter Router01
    -continue -level 1 -full -out /nfa-csv/
```

   2 回目の実行では、2017/4/1 1:00 から 60 分間のデータが出力されます。

3. 現在時刻に追いつくまで、繰り返し-continue で実行します。

   1 回の実行で、60 分間のデータが出力されていきます。

ヒント

現在時刻に追いついた後も、cron などで定期的に実行することで、さらに継続して出力することが可能です。

A.3　nfa_application_conf

NFA に登録しているアプリケーション定義の内容を外部ファイルに出力 (エクスポート) したり、外部ファイルから複数のアプリケーション定義を NFA へ一括で追加、更新、削除 (インポート) するコマンドです。

本コマンドでは、アプリケーション定義の内容を JSON ファイル形式で取り扱います。ファイル形式の詳細については、「A.3.1　インポートおよびエクスポートのファイル形式（179 ページ）」を参照してください。

パス

<%*インストールディレクトリ*%>/controller/bin/nfa_application_conf

形式

```
nfa_application_conf import [-help] [-silent] [-unformatted]
 [-log LOGFILE] FILE
```

```
nfa_application_conf export [-help] [-silent] [-unformatted]
 [-type SYSTEM|USER] FILE
```

```
nfa_application_conf -help
```

説明

各サブコマンドの意味は次の通りです。

- import

  FILE で指定したファイルの内容を元に、NFA へのアプリケーション定義の追加、更新、削除を行います。

  FILE で指定したファイルの内容に対しては、コマンド処理のはじめにフォーマットチェックが実施されます。フォーマットチェックでエラーが検出された場合は、すべてのアプリケーション定義に対し、インポート処理は行われません。

  フォーマットチェックでエラーがない場合は、インポート処理が行われますが、以下に合致するアプリケーション定義に対しては、インポート処理が行われません。

  - 追加対象のアプリケーション定義の名前が、既存のアプリケーション定義と重複している
  - 更新、または、削除対象のアプリケーション定義が NFA に登録されていない

  上記の原因でインポートされなかったアプリケーション定義は、エラーレコードファイルに出力されます。

  ヒント

  - エラーレコードファイルは、インポートファイルと同じディレクトリに作成され、インポートファイルの名前に".error_*yyyymmddhhmmss*"を付加したファイル名となります。
  - エラーレコードファイルのエラー箇所を修正することで、エラー定義に対するインポートファイルを効率的に作成することができます。

- export

  FILE で指定したファイルに NFA のアプリケーション定義を JSON 形式で出力します。

引数

-silent

非対話モード(サイレントモード)で実行します。

非対話モードの場合、コマンド実行中の動作確認が表示されず、コマンド実行中の入力操作はなく、以下の動作となります。

- import の場合

  運用ログがすでに存在している場合、上書きします。

- export の場合

  FILE で指定したファイルがすでに存在している場合、上書きします。

-unformatted

- import の場合

  エラーとなったアプリケーション定義の JSON データをプログラムで処理しやすいように、インデント、および、改行を含まない形式でエラーレコードファイルに出力します。

- export の場合

  アプリケーション定義の JSON データをプログラムで処理しやすいように、インデント、および、改行を含まない形式でファイルに出力します。

-log *LOGFILE*

インポート処理の実行内容を記録する運用ログファイルの出力先を指定します。*LOGFILE* には、絶対パス、または、相対パスの指定が可能です。

本オプションを指定していない場合は、以下のデフォルトパスに出力されます。

- <%*インストールディレクトリ*%>/controller/log/nfa_application_conf/import_log_*yyyymmddhhmmss*.log

-type SYSTEM または USER

[**製品定義**]のアプリケーション定義のみをエクスポート対象とする場合は、-type SYSTEM を指定します。

[**ユーザー定義**]のアプリケーション定義のみをエクスポート対象とする場合は、-type USER を指定します。

本オプションを指定していない場合は、[**製品定義**]、および、[**ユーザー定義**]の両方のアプリケーション定義をエクスポート対象とします。

FILE

- import の場合

  アプリケーション定義を記述したインポートファイルを絶対パス、または、相対パスで指定します。

- export の場合

  アプリケーション定義を出力するエクスポートファイルを絶対パス、または、相対パスで指定します。

-help

コマンドの使用方法を表示します。

戻り値

戻り値	種別	説明
0	正常	正常終了
2	異常	ファイルの入出力に失敗した
4	異常	コマンドの引数が不正
9	異常	インポートファイルのフォーマットが不正
10	異常	内部エラー
11	異常	指定したファイルまたはディレクトリが存在しない
100	警告	一部のアプリケーション定義のインポートに失敗した
101	警告	ユーザー操作(CTRL+C など)により、途中で処理を中断した

注意事項

- 以下のメッセージが出力され、インポート処理が開始された後に、CTRL+C でコマンドを停止させても、NFA 内でのインポート処理は継続されます。

```
Importing is in progress.
```

A.3.1　インポートおよびエクスポートのファイル形式

`nfa_application_conf` コマンドのインポートファイル、および、エクスポートファイルのファイル形式について説明します。

ファイル形式

`nfa_application_conf` コマンドで処理する各ファイルは以下の形式となります。

- 文字コード: UTF-8
- 改行コード: LF
- 出力ファイルの権限: 644 (rw-r--r--)
- インポートファイル、および、エラーレコードファイルのデータ形式:

```
{
    "add-applications" :  [ APPLICATION ] | null,
    "edit-applications" : [ APPLICATION ] | null,
    "delete-applications" : [ number ] | null
}
```

プロパティ	型	説明
add-applications	list [APPLICATION]	リスト形式で、追加するアプリケーション定義(APPLICATION)を指定します。 アプリケーション定義(APPLICATION)の詳細は、「APPLICATION（180 ページ）」を参照してください。 id または、type を指定していた場合、その値を無視して処理を行います。 追加するアプリケーション定義がなければ、null を指定するか、または、プロパティ自体を省略します。
edit-applications	list [APPLICATION]	リスト形式で、更新するアプリケーション定義(APPLICATION)を指定します。 アプリケーション定義(APPLICATION)の詳細は、「APPLICATION（180 ページ）」を参照してください。 id を識別子として、アプリケーション定義の更新処理を行います。 type を指定していた場合、その値を無視して処理を行います。 更新するアプリケーション定義がなければ、null を指定するか、または、プロパティ自体を省略します。
delete-applications	list [number]	削除するアプリケーション定義の id を指定します。 id を識別子として、アプリケーション定義の削除処理を行います。 削除するアプリケーション定義がなければ、null を指定するか、または、プロパティ自体を省略します。

- エクスポートファイルのデータ形式:

```
{
    "data" : [ APPLICATION ],
    "count" : number
}
```

プロパティ	型	説明
data	list [APPLICATION]	リスト形式でエクスポートしたアプリケーション定義(APPLICATION)の内容を示します。 アプリケーション定義(APPLICATION)の詳細は、「APPLICATION（180 ページ）」を参照してください。
count	number	エクスポートされたアプリケーション定義の数を示します。

APPLICATION

APPLICATION オブジェクトの形式を以下に示します。

```
{
    "id" : number,
    "name" : string,
    "type" : “SYSTEM” | “USER”,
    "conditions" : [ CONDITION ],
    "low-flow-monitoring" : true | false
}
```

プロパティ	型	説明
id	number	アプリケーション定義を識別するための ID。 インポート処理でのアプリケーション定義の更新、削除において利用します。
name	string	アプリケーション定義の名前。 最大文字数は 32 文字です。 以下に示す文字は指定することができません。 • 記号: , ! " $ ' * + ; < = > ? \ ^ ` { | } ~ • 先頭および末尾への半角スペース 他のアプリケーション定義の名前と同じ名前をつけることはできません。
type	string	アプリケーション定義の種別。 • "SYSTEM" : [**製品定義**]であることを示します。 • "USER" : [**ユーザー定義**]であることを示します。
conditions	list [CONDITION]	アプリケーション通信を識別するための条件情報。 1 つ以上の条件(CONDITION)を指定する必要があり、複数条件が指定されている場合は、OR 条件となります。 条件(CONDITION)の詳細は、「CONDITION（181 ページ）」を参照してください。
low-flow-monitoring	bool	少量フローとして分析するかどうかを表す情報。 詳細は「3.3.3　アプリケーション定義での少量フローの分析について（74 ページ）」を参照してください。

CONDITION

CONDITION オブジェクトの形式を以下に示します。

```
{
    "ip-protocol" : string,
    "endpoint1" : DETAILED_CONDITION | null,
    "endpoint2" : DETAILED_CONDITION | null,
    "src" : DETAILED_CONDITION | null,
    "dst" : DETAILED_CONDITION | null
}
```

プロパティ	型	説明
ip-protocol	string	アプリケーションが利用する IP プロトコル名。 指定可能な IP プロトコル名は、「指定可能な IP プロトコル（183 ページ）」を参照してください。 インポート処理においては、大文字、小文字を区別しません。
endopint1	DETAILED_CONDITION	通信の方向を指定しない場合のエンドポイントの詳細条件(DETAILED_CONDITION)。 詳細条件(DETAILED_CONDITION)の詳細は、「DETAILED_CONDITION（182 ページ）」を参照してください。 src、および、dst とは、同時に指定することはできません。 条件がない場合は、null を指定するか、または、プロパティ自体を省略します。

プロパティ	型	説明
endpoint2	DETAILED_CONDITION	通信の方向を指定しない場合のエンドポイントの詳細条件(DETAILED_CONDITION)。 詳細条件(DETAILED_CONDITION)の詳細は、「DETAILED_CONDITION（182 ページ）」を参照してください。 src、および、dst とは、同時に指定することはできません。 条件がない場合は、null を指定するか、または、プロパティ自体を省略します。
src	DETAILED_CONDITION	通信の方向を指定する場合の送信元の詳細条件(DETAILED_CONDITION)。 詳細条件(DETAILED_CONDITION)の詳細は、「DETAILED_CONDITION（182 ページ）」を参照してください。 endopint1、および、endpoint2 とは、同時に指定することはできません。 条件がない場合は、null を指定するか、または、プロパティ自体を省略します。
dst	DETAILED_CONDITION	通信の方向を指定する場合の宛先の詳細条件(DETAILED_CONDITION)。 詳細条件(DETAILED_CONDITION)の詳細は、「DETAILED_CONDITION（182 ページ）」を参照してください。 endopint1、および、endpoint2 とは、同時に指定することはできません。 条件がない場合は、null を指定するか、または、プロパティ自体を省略します。

DETAILED_CONDITION

DETAILED_CONDITION オブジェクトの形式を以下に示します。

```
{
    "port" : string | null,
    "ip-address" : [ string ] | null,
    "domain" : [ string ] | null
}
```

プロパティ	型	説明
port	string	アプリケーションが利用するポート番号。 ポート番号は、0～65535 の範囲の半角数字となりますが、複数のポート番号が条件となる場合は、コンマ(,)で区切って表現したり、以下の形式で範囲を表現します。 **<開始ポート番号>-<終了ポート番号>** ip-protocol が、"TCP"、"UDP"、"TCP/UDP"のいずれかの場合は、必ず指定します。 条件がない場合は、null を指定するか、または、プロパティ自体を省略します。
ip-address	list [string]	アプリケーションの識別条件となる送信元、または、宛先の IP アドレス。

プロパティ	型	説明
		192.168.0.1 のような IPv4 アドレス形式で指定します。また、IP アドレスの範囲指定の場合は、以下の形式となります。 `<開始IPv4アドレス>-<終了IPv4アドレス>` 複数条件が指定されている場合は、OR 条件となります。domain の条件が指定されている場合も OR 条件となります。
domain	list [string]	アプリケーションの識別条件となる送信元、または、宛先のドメイン名。 最大文字数は、255 文字です。 指定可能な文字は、半角英数字、ハイフン(-)、ドット(.)、アスタリスク(*)です。アスタリスク(*)のみの指定やアスタリスク(*)を 2 つ以上指定することはできません。 複数条件が指定されている場合は、OR 条件となります。ip-address の条件が指定されている場合も OR 条件となります。

指定可能な IP プロトコル

アプリケーション定義で IP プロトコルとして指定可能なプロトコル名を以下に示します。

ヒント

TCP/UDP は、[**TCP または UDP**]のことを意味しています。

```
TCP/UDP, HOPOPT, ICMP, IGMP, GGP, IPv4, ST, TCP, CBT, EGP, IGP,
BBN-RCC-MON, NVP-II, PUP, ARGUS, EMCON, XNET, CHAOS, UDP, MUX,
DCN-MEAS, HMP, PRM, XNS-IDP, TRUNK-1, TRUNK-2, LEAF-1, LEAF-2, RDP,
IRTP, ISO-TP4, NETBLT, MFE-NSP, MERIT-INP, DCCP, 3PC, IDPR, XTP,
DDP, IDPR-CMTP, TP++, IL, IPv6, SDRP, IPv6-Route, IPv6-Frag, IDRP,
RSVP, GRE, DSR, BNA, ESP, AH, I-NLSP, SWIPE, NARP, MOBILE, TLSP,
SKIP, IPv6-ICMP, IPv6-NoNxt, IPv6-Opts, 61, CFTP, 63, SAT-EXPAK,
KRYPTOLAN, RVD, IPPC, 68, SAT-MON, VISA, IPCV, CPNX, CPHB, WSN, PVP,
BR-SAT-MON, SUN-ND, WB-MON, WB-EXPAK, ISO-IP, VMTP, SECURE-VMTP,
VINES, TTP, NSFNET-IGP, DGP, TCF, EIGRP, OSPFIGP, Sprite-RPC, LARP,
MTP, AX.25, IPIP, MICP, SCC-SP, ETHERIP, ENCAP, 99, GMTP, IFMP, PNNI,
PIM, ARIS, SCPS, QNX, A/N, IPComp, SNP, Compaq-Peer, IPX-in-IP, VRRP,
PGM, 114, L2TP, DDX, IATP, STP, SRP, UTI, SMP, SM, PTP, ISISoverIPv4,
FIRE, CRTP, CRUDP, SSCOPMCE, IPLT, SPS, PIPE, SCTP, FC, RSVP-E2E-IGNORE,
MobilityHeader, UDPLite, MPLS-in-IP, manet, HIP, Shim6, WESP, ROHC
```

A.3.2　使用例

`nfa_application_conf` コマンドの使用例を説明します。

`nfa_application_conf` コマンドは、アプリケーション定義のみをバックアップしたい場合や他の環境で動作する NFA のアプリケーション定義をコピーしたい場合などで利用することができます。

具体的な使用例を以下に示します。

[ユーザー定義]のアプリケーション定義のみをエクスポートする

-type USER オプションを指定して以下のようにコマンドを実行します。

```
# mkdir -p /nfa-app
# /opt/nec/nfa/controller/bin/nfa_application_conf export -type USER /nfa-app/user.json
```

コマンドを実行すると、/nfa-app ディレクトリの user.json ファイルに[**ユーザー定義**]のアプリケーション定義のみが出力されます。

他の NFA にアプリケーション定義をコピーする

「[**ユーザー定義**]のアプリケーション定義のみをエクスポートする」の操作を実施し、コピー元の NFA から[**ユーザー定義**]のアプリケーション定義をエクスポートします。

/nfa-app/user.json の data プロパティのデータを元にインポートファイルの add-applications プロパティのデータを作成します。

作成したインポートファイルをコピー先となる NFA へ配置し、以下のようにコマンドを実行します。

```
# /opt/nec/nfa/controller/bin/nfa_application_conf import import.json
```

上記において、すでに同名のアプリケーション定義が存在していた場合は、当該アプリケーション定義の処理がエラーとなります。この場合は、edit-applications プロパティのデータとして、当該アプリケーション定義データを記載して、インポート処理を再度実行してください。

A.4　nfa_reload_dnssetting

OS の DNS サーバーの設定を NFA に動的に反映するためのコマンドです。

NFA サービスが起動している状態で、OS の DNS サーバー設定(resolv.conf)の変更を行った場合、本コマンドを実行することで、NFA サービスの再起動をせずに設定変更を NFA に反映することができます。

パス

<%*インストールディレクトリ*%>/collector/bin/nfa_reload_dnssetting

形式

```
nfa_reload_dnssetting
```

戻り値

成功時には 0 を返します。失敗時には 0 以外の値を返します。

A.5　保守ツール

NFA の運用維持や障害調査のためのログ採取を行うツールについて説明します。

A.5.1　nfa_diskcheck

ディスク使用率を監視し、しきい値を超えた場合にメールや syslog を用いてユーザーに通知することができるコマンドです。

本コマンドを cron 等で定期実行することにより、NFA が使用するディスクの使用状況を簡易的に監視することができます。

ヒント

本コマンドは、NFA の動作とは独立しており、簡易的にディスク使用率を監視するためのものです。詳細な監視や異常時のきめ細かな通報処理を行いたい場合は、WebSAM SystemManager G などの監視製品を利用することを推奨します。

パス

`<%`*インストールディレクトリ*`%>/collector/bin/diskcheck/nfa_diskcheck`

形式

```
nfa_diskcheck
```

説明

監視対象とするディスクやしきい値、通知手段については、コマンドと同じパスに配置されている設定ファイル(nfa_diskcheck.conf)を用いて指定します。本コマンドを実行する前に、必ず、設定ファイル(nfa_diskcheck.conf)を編集し、 監視内容を指定してください。

⚠ 注意

設定ファイル(nfa_diskcheck.conf)は、`nfa_backup` コマンドによるバックアップの対象外です。必要に応じて個別にバックアップを行ってください。

設定ファイル(nfa_diskcheck.conf) のパラメーター

設定ファイル(nfa_diskcheck.conf)で指定する `nfa_diskcheck` コマンドのパラメーター内容を「表 A-4 コマンドパラメーター（186 ページ）」に示します。

省略可能なパラメーターの指定を省略した場合は、デフォルト値で処理が行われます。

表 A-4　コマンドパラメーター

パラメーター名	説明	デフォルト値
detect_path	ディスク使用率を監視するパス。 絶対パスで指定します。 本パラメーターは、必ず、指定してください。	
threshold_value	ディスク使用率のしきい値 [%]。 本パラメーターは、必ず、指定してください。	
syslog_notify	しきい値超過時の syslog 通知の実行フラグ。 True: syslog での通知を行います。 False: syslog での通知を行いません。	True
syslog_name	syslog で通知するプログラム名。	nfa_diskcheck
syslog_severity	通知する syslog の重要度。 以下のいずれかを指定することができます。 debug, info, notice, warn, err, crit, alert, emerg	warn
syslog_message	syslog で通知するメッセージ。 syslog_notify = True の場合は、必ず、指定してください。	
mail_notify	しきい値超過時のメール通知の実行フラグ。 メールの文字コードは、UTF-8 です。	True
smtp_server	メールサーバーのドメイン名(FQDN)、もしくは、IP アドレス。 mail_notify = True の場合は、必ず、指定してください。	
smtp_port	メール送信で利用するポート番号。	25
smtp_username	SMTP 認証に用いるユーザー名。 smtp_username、または、smtp_password が省略されていた場合は、SMTP 認証を利用しません。	SMTP 認証を利用しない
smtp_password	SMTP 認証に用いるパスワード。 smtp_username、または、smtp_password が省略されていた場合は、SMTP 認証を利用しません。	SMTP 認証を利用しない
mail_to	メールの宛先アドレス。 コンマ(,)区切りで複数指定することができます。 mail_notify = True の場合は、必ず、指定してください。	
mail_cc	メールの複写先アドレス。 コンマ(,)区切りで複数指定することができます。 本パラメーターは省略することができます。	
mail_from	メールの送信元アドレス。 mail_notify = True の場合は、必ず、指定してください。	
mail_subject	メールの件名。 mail_notify = True の場合は、必ず、指定してください。	
mail_body	メールの本文。 mail_notify = True の場合は、必ず、指定してください。	

以下のパラメーターに対しては、監視処理で取得した情報を置換文字列として埋め込むことが可能です。

- syslog_message
- mail_subject
- mail_body

使用可能な置換文字列を「表 A-5 置換文字列（187 ページ）」に示します。

例:

```
syslog_message = High disk usage. The disk usage been {disk_usage}%.
```

表 A-5　置換文字列

置換文字列	説明
{disk_size}	監視対象ディスクの全体容量 [MB]。
{used}	監視対象ディスクの使用量 [MB]。
{available}	監視対象ディスクの空き容量 [MB]。
{disk_usage}	監視対象ディスクの使用率 [%]。
{detect_path}	監視対象ディスクのパス (detect_path の設定値)。
{date_time}	ディスク利用率の取得日時。 *YYYY-MM-DD hh:mm:ss(TimeZone)*の形式となります。

戻り値

成功時には 0 を返します。失敗時には 0 以外の値を返します。

A.5.2　nfatech ログ採取コマンド

NFA の運用で障害が発生した場合に、原因調査で必要なログを採取するためのツールについて説明します。

NFA の運用で障害が発生した場合は、NFA が提供するログ採取ツールを使用してログを採取し、NEC カスタマーサポートセンターへ送付してください。

NFA では、以下の 3 つのログ採取ツールを提供しています。状況に合わせて使い分けてください。

- `nfatech.sh` コマンド

  様々な事象の調査で必要となるログを採取するコマンドです。基本的には、本コマンドを使用してログを採取します。

  採取するログの内容は以下の通りです。

  - NFA が動作する OS 関連の情報
  - NFA の動作ログ
  - NFA の設定ファイル

  - NFA のプロセス情報
  - NFA のデータベース情報 (システム設定、イベント件数、テーブル構成の情報)

- nfatech_minimal.sh コマンド

  障害調査で必要となる最小限のログを採取するコマンドです。ディスクの空き容量が少ない場合は、本コマンドを使用してログを採取します。

  採取するログの内容は以下の通りです。

  - NFA が動作する OS 関連の情報
  - NFA の動作ログ (各処理のリソース利用に関する統計情報は除く)
  - NFA の設定ファイル
  - NFA のプロセス情報

- nfatech_core.sh コマンド

  NFA プロセスのコアダンプファイルを採取するためのコマンドです。NFA プロセスが異常終了する事象が発生した場合に、nfatech.sh コマンド、または、nfatech_minimal.sh コマンドと共に本コマンドを使用します。

  採取するログの内容は以下の通りです。

  - NFA プロセスのコアダンプファイル

パス

<%*インストールディレクトリ*%>/controller/bin/nfatech/nfatech.sh

<%*インストールディレクトリ*%>/controller/bin/nfatech/nfatech_minimal.sh

<%*インストールディレクトリ*%>/controller/bin/nfatech/nfatech_core.sh

形式

```
nfatech.sh [-help] [-n] [-o Directory]
```

```
nfatech_minimal.sh [-help] [-n] [-o Directory]
```

```
nfatech_core.sh [-help] [-n] [-o Directory]
```

説明

ログを採取し、指定したディレクトリに 1 つの圧縮ファイルとして出力します。

出力ファイル名は以下となります。

- nfatech-*YYYYmmdd-HHMMSS*.tar.bz2

ディレクトリの指定を行っていない場合は、カレントディレクトリに出力します。

引数

-n

ログ採取で必要となるディスク容量の見積もりを行い、出力先のディスク容量が十分かを確認します。

-n オプションを指定した場合は、ログ採取処理は行いません。

-o *Directory*

採取したログの出力先を指定します。

Directory には、絶対パス、または、相対パスの指定が可能です。*Directory* で指定したディレクトリが存在していない場合は作成します。

-help

コマンドの使用方法を表示します。

戻り値

成功時には 0 を返します。失敗時には 0 以外の値を返します。

付録 B　トラブルシューティング

NFA をご利用いただく上で想定されるトラブルと、その対処方法について説明します。

B.1　Web コンソールに接続できない

事象

所定の URL を指定して Web コンソールに接続しようとしたが、以下のような画面が表示され、接続できない。

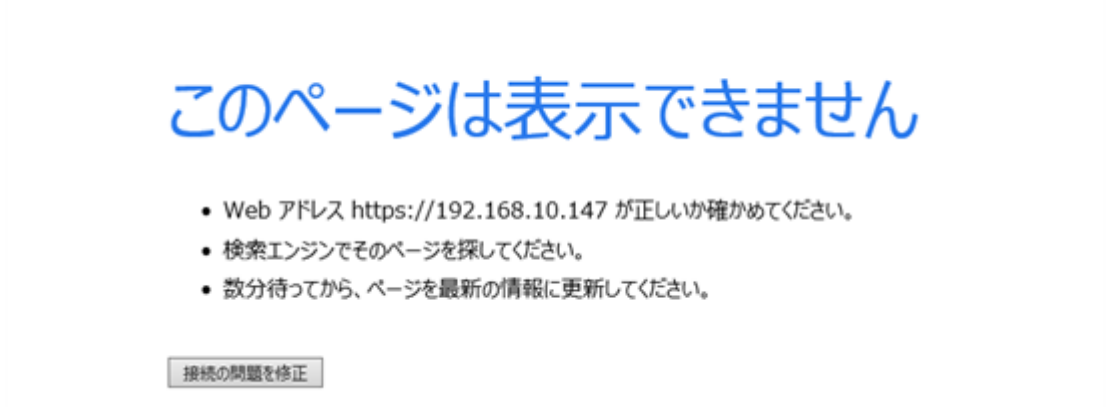

図 B-1　画面例

原因

NFA サーバー上で、NFA のサービスが起動していないことが考えられます。

対処

NFA のサービスを再起動してください。操作については、「5.1.2　サービスを起動、停止する（137 ページ）」を参照してください。

B.2　ダッシュボード画面のウィジェットでグラフが表示されない

事象

ダッシュボードのグラフが表示されるすべてのウィジェットにおいて、**データの取得に失敗しました、データがありません**と表示され、グラフが表示されない。

図 B-2　画面例

原因 1

NFA サーバー上で、フローコレクターが動作していないことが考えられます。

対処 1

NFA のサービスを再起動してください。操作については、「5.1.2　サービスを起動、停止する（137 ページ）」を参照してください。

原因 2

Web コンソールが動作するクライアントマシンと NFA サーバーの時刻が大きくずれているために、蓄積されたフローデータが正しく参照できていないことが考えられます。

対処 2

Web コンソールが動作するクライアントマシンと NFA サーバーの時刻を合わせてください。

B.3　ダッシュボード画面のウィジェットでグラフの表示が遅延する

事象

ダッシュボードの各ウィジェットにおいて、一部の期間のグラフデータが即時に表示されず、数分以上の時間がたってから表示される。

原因

NFA のフローコレクターにおいて、受信したフロー情報のデータベース書き込みに時間がかかっていることが原因だと考えられます。

NFA のフローコレクターは、フロー情報の受信頻度に対し、データベースへの書き込み処理が遅い場合は、メモリに受信したフロー情報を一時的に蓄積します。その後、受信したフロー情報をすべてデータベースへ書き込む仕様です。各ウィジットでは、データベースへの

書き込み処理が完了したデータしかグラフ表示できないため、表示が遅延する場合があります。

対処

一時的な表示遅延であれば、そのままの状態で運用いただいて問題ありません。

特定時間帯において、必ず遅延が発生し運用に支障が生じている場合は、「5.1.4　フロー情報の記録処理方式を変更する（140 ページ）」の手順に沿って、一時記録データベースへの書き込みを停止することで解決できる場合があります。

本事象は、フロー情報の受信頻度とディスク I/O 性能のバランスが崩れていることが起因しています。そのため、フローを送信するエクスポーター数を削減したり、高性能のディスクの利用に切り替えるなど運用環境を見直すことも効果があります。

B.4　各種設定処理に失敗する

事象

各種設定処理を実行した際、**失敗しました**というエラーが表示されて、設定処理が失敗する。

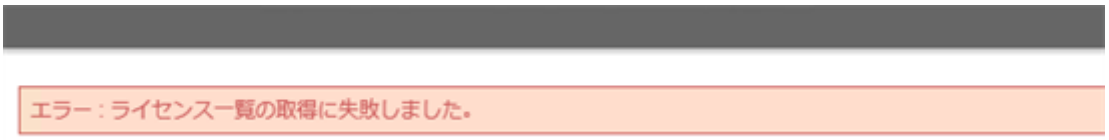

図 B-3　画面例

原因

NFA サーバー上で、サービスの一部が動作していないことが考えられます。

対処

NFA のサービスを再起動してください。操作については、「5.1.2　サービスを起動、停止する（137 ページ）」を参照してください。

B.5　エクスポーターを削除しても、復活してしまう

事象

エクスポーターを削除しても、当該エクスポーターからのフロー受信契機で再度エクスポーターが登録されてしまう。

原因

自動登録機能がオンになっていることが考えられます。

この場合、エクスポーターを削除したとしても、その後で再度当該エクスポーターからのフローを受信すれば、再度エクスポーターが登録されてしまいます。

対処

以下のいずれかの対処が必要です。

- エクスポーター側で、フローの送信設定を止める。
- NFA 側で、エクスポーターの自動登録機能をオフにする。

  操作の詳細については、「2.2.1　エクスポーター情報の登録ポリシーを設定する（29 ページ）」を参照してください。

B.6　ウィジェットにて、ホスト名表示ができない

事象

フローの受信し始めているはずだが、5 分以上たたないとホスト名表示ができない。

原因

ホスト名の取得は、DNS サーバーに負荷がかからないよう考慮して名前解決を行っているため、最大 5 分程度の時間がかかる場合があります。よって、これは仕様通りの動作になります。

対処

なし。

なお、DNS サーバー側の設定が正しく行えているかを確認するためには、フローコレクターのマシン上で `nslookup` や `ping` などのコマンドを実行することで、ホスト名が解決できるかどうか確認することができます。

以下は、`nslookup` コマンドの実行例です。

```
$ nslookup 192.168.10.100
```

B.7　Web コンソールのレイアウトが崩れてしまう

事象

Web コンソールのレイアウトが崩れてしまう。

原因

ご利用の Web ブラウザーが、サポート対象のバージョンではないことが考えられます。

対処

NFA がサポートしているバージョンの Web ブラウザーをご利用ください。

- Microsoft Edge 104 以上
- Google Chrome 104 以上

B.8　ページの有効期限が切れているか、不正なリクエストですのエラーが表示される

事象

設定の変更などを行おうとすると、**ページの有効期限が切れているか、不正なリクエストです**のエラーが表示される。

原因

別の画面にて、他の設定を実施中であることが考えられます。

対処

設定情報を操作する場合は、NFA に対する同時操作を行わないようにしてください。

付録 C　製品が利用するシステムリソース

製品が利用するシステムリソースについて説明します。

C.1　製品が利用するポート番号の一覧

製品が利用するポート番号のデフォルト値について説明します。

NFA が外部との通信、および内部での通信において利用するポート番号を、「表 C-1 NFA が利用する通信ポート番号一覧 (外部通信)（195 ページ）」、「表 C-2 NFA が利用する通信ポート番号一覧 (内部通信)（195 ページ）」に示します。

表 C-1　NFA が利用する通信ポート番号一覧 (外部通信)

名称	ポート番号	プロトコル	方向	用途
HTTPS 通信ポート	443	TCP	IN	HTTPS 通信ポートです。
sFlow パケット受信ポート	6343	UDP	IN	sFlow パケット受信ポートです。
NetFlow、IPFIX パケット受信ポート	9995	UDP	IN	NetFlow パケット、IPFIX パケットの受信ポートです。
O365 定義更新用通信ポート	443	TCP	OUT	Microsoft 365 (Office 365)に対するアプリケーション定義を自動更新するための「endpoints.office.com」との通信用ポートです。 **ヒント** プロキシサーバーを利用して通信することが可能です。

表 C-2　NFA が利用する通信ポート番号一覧 (内部通信)

名称	ポート番号	プロトコル	方向	用途
フローデータ DB 通信ポート	27100	TCP	IN	フローデータ管理用データベースへの通信ポートです。
システム管理 DB 通信ポート	27110	TCP	IN	システム管理用データベースへの通信ポートです。
イベント管理 DB 通信ポート	27120	TCP	IN	イベント管理用データベースへの通信ポートです。
コントローラー制御通信ポート	27200	TCP	IN	コントローラープロセス制御への通信ポートです。
コレクターログサービス通信ポート	27210	UDP	IN	コレクタープロセスのログサービスへの通信ポートです。

これらのポート番号はすべて変更することができます。利用するポート番号の変更手順は、「5.1.3　製品が利用する通信ポート番号を変更する（138 ページ）」を参照してください。

付録 D　他システムとの連携設定

NFA と他システムとを連携させるための設定方法について説明します。

D.1　UNIVERGE PF6800 Web GUI との連携設定

UNIVERGE PF6800(以降、PFC と略記します)の Web GUI から NFA の Web コンソールに、ログイン認証なしに接続するための設定方法について説明します。

本設定を行うことで、PFC の Web GUI からシームレスに NFA を操作することができるようになります。

ヒント

- 本設定により NFA と連携が行える PFC のバージョンは、6.1 以上です。
- 以下に示す NFA 側の連携設定と合わせて、PFC 側でも連携設定を行う必要があります。
  PFC 側の設定手順については、PFC の「Web GUI 利用者マニュアル」を参照してください。

1. NFA のサービスを停止します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ctl.sh stop
```

2. 以下の設定ファイルを編集します。ファイルが存在しない場合は、新規に作成してください。

   `<%データディレクトリ%>/controller/conf/sso.properties`

   設定ファイルの記述形式は以下の通りです。

```
sso.ipaddr.n = <PFCのIPv4アドレス>
sso.username.n = <ユーザー名>
```

   - *n*

     1 からの連番で、この番号を増やすことで、複数の定義を行うことができます。

   - *<PFC の IPv4 アドレス>*

     PFC の運用管理用の NIC(eth0 等)に設定している IPv4 アドレスを指定します。

   - *<ユーザー名>*

     NFA にログインする NFA のユーザーの名前を指定します。

     *<ユーザー名>*に指定したユーザーが、NFA に登録されていない場合は、NFA への接続はできません。ただし、下記の場合は admin ユーザーで接続します。

     - *<ユーザー名>*に何も指定しない場合
     - 「sso.username.n = 」の定義自体を省略した場合

3. NFA のサービスを起動します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ctl.sh start
```

設定例

PFC1(192.168.10.1)、PFC2(192.168.10.2)が冗長構成をとっているシステムにおいて、NFA にユーザー名「PFC_User」でログインする場合の設定を以下に示します。

```
sso.ipaddr.1 = 192.168.10.1
sso.username.1 = PFC_User
sso.ipaddr.2 = 192.168.10.2
sso.username.2 = PFC_User
```

用語集

A - Z

■ A

■ AS

AS(Autonomous System/自律システム)とは、RFC 1930 で定義されている、インターネットなどの大規模な TCP/IP ネットワーク内に、ある各組織が保有・運用する自律したネットワークのことを示します。

この自立したネットワークを識別するために AS 番号が用いられており、各国の NIC(Network Information Centre)によって管理されています。

■ D

■ DNS

DNS(Domain Name System)とは、ネットワーク上のホスト名、あるいは、ドメイン名と IP アドレスとの対応状況を管理するためのシステムのことを指します。

■ DSCP

DSCP(Differentiated Services Code Point)とは、パケットに優先度を付けるための仕組みのことを指します。IP ヘッダー内の ToS フィールド(8bit)のうち、6bit を利用し、64 段階の優先度を指定することができます。

■ F

■ FQDN

FQDN(Fully Qualified Domain Name/完全修飾ドメイン名)とは、ドメイン名、サブドメイン名、ホスト名等を省略せずにすべて記述したドメイン名のことを示します。

■ I

■ IANA

IANA(Internet Assigned Numbers Authority)とは、インターネットに関連する様々な番号(IP アドレス、プロトコル番号、ポート番号など)を管理している組織のことを指します。

■ ifIndex

SNMP によるネットワーク管理において最も利用されている識別子の 1 つで、物理インターフェイスや論理インターフェイスに関連付けられる一意の識別番号のことを指します。

NFA では、フロー情報のインターフェイスの識別において ifIndex 値を利用しています。

■ ifName

装置の物理インターフェイス、または、論理インターフェイスの名前を記録する MIB のオブジェクト名のことを指します。

■ IF グループ

複数インターフェイスを通るフロ-を集計し分析したい場合に用いるグルーピング機能のことを指します。

IF グループは、LAG(Link Aggregation)構成の複数のインターフェイスをグルーピングして、１つの LAG インターフェイスとしてフローを分析する場合に用いることを想定しています。

■ IP プロトコル

NFA では、IP ヘッダ中のプロトコル番号 (IP Protocol Number)で示されるプロトコルのことを指しており、具体的には、TCP、UDP、ICMP などの総称としています。

■ IPFIX

IPFIX(IP Flow Information Export)とは、ネットワークの通信状況をモニタリングするための技術で、NetFlow version 9 をもとにして拡張された IETF 標準技術です。

■ L

■ LAG

LAG(Link Aggregation Group)とは、複数の物理的なインターフェイスを仮想的に束ね、あたかも 1 本のインターフェイスであるかのように扱う技術のことで、IEEE P802.3ad で規定されています。

■ M

■ MIB

MIB(Management Information Base)とは、SNMP で管理可能なネットワーク装置が、自分の状態を外部に知らせるために公開する管理情報のことで、RFC 1156 および、RFC 1213 で規定

されています。MIB の情報は、外部から SNMP を用いて、オブジェクト名を指定して値を参照することができます。

■ N

■ NetFlow

米国 Cisco Systems, Inc.が開発したネットワークの通信状況をモニタリングするための技術で、RFC3954 でバージョン 9 の仕様が公開されています。

NetFlow では、IP ベースの通信情報のみを対象としており、また、通信パケットのモニタリング方法としてフルモードとサンプリングモードの 2 つを提供しています。

■ NFA

WebSAM Network Flow Analyzer の略称です。

■ P

■ PHB

PHB(Per Hop Behavior)とは、DSCP 値に対応するパケット転送処理の振る舞い定義のことを指します。

■ S

■ sFlow

米国 InMon Corp.が開発したネットワークの通信状況をモニタリングするための技術で、RFC3176 でバージョン 4 の仕様が公開されています。

sFlow では、特定の割合で通信パケットをサンプリングし、その情報を統計分析することで、全体の通信量を算出する仕組みを提供しています。

NFA では、スイッチ、ルーター側でサンプリングし、生成したフロー情報(sFlow パケット)を受信して、その情報を統計分析することで通信量の算出を行います。

■ SNMP

SNMP(Simple Network Management Protocol)とは、RFC1157 で規定されているネットワーク管理のためのプロトコルです。

SNMP を用いることで、TCP/IP ネットワークに接続するネットワーク装置に対し、ネットワーク経由で監視や管理を行うことができます。

NFA では、SNMP v1、v2c を用いてエクスポーターの名前やインターフェイス情報を取得します。

■ SNMP トラップ

能動的に自分の状態を通知するための SNMP が提供する仕組みのことを指します。

NFA では、しきい値監視で検出したイベントを外部に通知する方法として SNMP トラップを用いています。

■ sysName

装置のホスト名を記録する MIB のオブジェクト名のことを指します。sysName の値は、装置のコンフィグにより設定することができます。

■ T

■ ToS

ToS(Type of Service)とは、IP ヘッダーを構成するフィールドの 1 つで、パケット転送を行う各装置に対し、パケットの処理方法を伝えるために利用します。

あ - わ

■ あ

■ ウィジェット

ダッシュボード画面、および、エクスポーター分析画面の構成要素の 1 つで、グラフや一覧の表示機能を提供します。

■ エクスポーター

NFA では、フロー(sFlow、NetFlow、IPFIX)パケットを送信することができるスイッチやルーターなどの装置、または、ソフトウェアの総称としてエクスポーターという表現を用います。

■ エンドポイント

ネットワークに接続し、様々な通信を行うパソコンなどのネットワーク端末の総称のことを示します。NFA では、クライアントだけではなく、サーバーも含め、エンドポイントと表現します。

■ エンドポイントグループ

通信のエンドポイントとなる複数の送信元アドレス、または、宛先アドレスのフローを集計し、分析したい場合に用いるグルーピング機能のことを指します。

エンドポイントグループは、部署内の IP アドレス帯をグルーピングして部署ごとのフローの分析を行う場合などに利用することを想定しています。

■ か

■ カンバセーション

NFA では、特定の 2 点間の通信のやり取りのことをカンバセーションと表現します。

■ は

■ フロー

エンドポイント間の通信の流れのこと、または、この通信の流れをエクスポーターでモニタリングし生成した情報(sFlow、NetFlow、IPFIX)のことを指します。

■ フローレート

NFA では、1 分間に発生したエンドポイント間の通信の流れの数のことを指します。

■ ポート番号

TCP/IP の通信を行う際に通信先のプログラムを特定するための番号のことを指します。

■ ら

■ ローデータ

NFA では､時間や通信量の多さによる集約処理を行う前に記録されたフローデータのことを指します。

WebSAM
Network Flow Analyzer 3.4
リファレンスマニュアル

NFA00MJ0340-01

2025 年 5 月 01 版 発行

日本電気株式会社

© NEC Corporation 2014-2025