

WebSAM
Network Flow Analyzer 1.1
スタートアップガイド

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

はじめに

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

本書では、NFA のインストールおよび環境設定、基本的な操作方法について説明しています。NFA の環境構築のための作業を行う前に、本書をよくお読みください。

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。



NFA の管理者



NFA のすべての利用者

本書の構成

タイトル	内容	対象者
「第 1 章 製品概要 (1 ページ)」	NFA の製品概要について説明します。	USER
「第 2 章 インストール (14 ページ)」	NFA のセットアップ手順について説明します。	NFA
「第 3 章 インストール後の環境設定 (32 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。	NFA
「第 4 章 基本操作 (42 ページ)」	NFA の Web コンソールの基本的な操作について説明します。	USER
「第 6 章 アンインストール (55 ページ)」	NFA をアンインストールする手順について説明します。	NFA
「付録 A. コマンドリファレンス (57 ページ)」	NFA のセットアップに関係するコマンドの詳細について説明します。	NFA
「付録 B. トラブルシューティング (61 ページ)」	NFA のセットアップ作業に関するトラブルシューティング方法について説明します。	NFA

本書の表記規則

本書では、注意すべき事項や補足事項について、以下の表記を用います。

注意補足事項の表記

表記	説明
注意	製品機能の設定、操作を行う上で守らなければならない事柄や特に注意すべき点を示します。

表記	説明
ヒント	知っておくと役に立つ便利な情報を示します。

本書では、以下の表記規則に従って記述しています。

表記規則

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

本製品は、デフォルトでは、以下のディレクトリにインストールします。

デフォルトのインストール先:

/opt/nec/nfa

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

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

目次

第1章 製品概要	1
1.1 製品の特長	2
1.2 機能概要	3
1.3 動作環境	6
1.3.1 システム構成	6
1.3.2 システム要件	7
1.3.3 フローデータの管理について	8
1.3.3.1 フローデータの保持期間と丸め処理について	8
1.3.3.2 ディスク使用量の見積もり方法	9
1.3.3.3 保持するフロー数の上限を変更する	11
1.3.3.4 フローの保持期間を変更する	12
1.4 製品ライセンスとインターフェイスライセンス	13
第2章 インストール	14
2.1 導入までの流れ	15
2.2 事前準備を行う	15
2.2.1 インストールパラメーターの設計を行う	15
2.2.2 インストール先の環境確認を行う	18
2.3 インストール処理を実行する	18
2.4 SSL サーバー証明書を準備する	20
2.4.1 自己署名証明書を準備する	20
2.4.2 公的な認証局が発行する証明書を準備する	22
2.4.3 他で作成した証明書を使用する	24
2.5 製品が利用する通信ポート番号を確認する	24
2.5.1 製品が利用するポート番号の一覧	25
2.5.2 製品が利用する通信ポート番号を変更する	25
2.6 ファイアウォールの設定を変更する	27
2.7 Web サーバーに関する追加の設定	29
2.7.1 Web サーバーログの自動削除設定	29
2.8 サービスを起動する	30
第3章 インストール後の環境設定	32
3.1 Web コンソールを使用するための準備を行う	33
3.1.1 サーバーと時刻を同期する	33
3.1.2 Web ブラウザーのセキュリティ設定を確認する	33

3.1.3 Web ブラウザーに SSL サーバー証明書をインポートする	35
3.2 Web コンソールにアクセスする	36
3.3 システムの環境設定を行う	37
3.4 製品ライセンスを登録する	38
3.5 エクスポートの装置側設定を行う	40
3.6 ユーザーを追加する	41
第 4 章 基本操作.....	42
4.1 Web コンソール構成.....	43
4.2 ウィジェットの種類.....	45
4.3 ウィジェットを操作する	48
4.3.1 ドリルダウン分析を行う	48
4.3.2 グラフの表示項目をフィルタリングする	50
4.3.3 折れ線グラフの表示をズームインする	50
4.3.4 IP アドレス表示をホスト名表示に変換する	51
4.4 個人設定の内容を更新する	52
第 5 章 アップグレード.....	53
5.1 アップグレードする	54
第 6 章 アンインストール.....	55
6.1 アンインストールにおける注意事項.....	56
6.2 製品をアンインストールする	56
付録 A. コマンドリファレンス	57
A.1 nfa_ssl_keytool	57
付録 B. トラブルシューティング	61
B.1 インストーラー実行時のエラーと対策	61
B.2 サービス起動時のエラーと対策	62

第 1 章

製品概要

NFA の製品概要について説明します。

目次

1.1 製品の特長	2
1.2 機能概要	3
1.3 動作環境	6
1.4 製品ライセンスとインターフェイスライセンス	13

1.1 製品の特長

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

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

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

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

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

簡単な操作でドリルダウン分析が可能

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

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

操作例:

1. 各インターフェイスを流れる通信量の表示から、特定のインターフェイス(仮に Ethernet1/1)を選択します。
(選択した Ethernet1/1 を流れる通信の表示に絞り込まれます。)
2. 各アプリケーションの通信量の表示から特定のアプリケーション(仮に http)を選択します。
3. Ethernet1/1 を流れる http 通信量に関する分析結果が表示されます。

表示内容の自由なカスタマイズ機能を提供

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

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

カスタマイズ例:

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

1.2 機能概要

NFA が提供する機能概要について説明します。

ダッシュボード

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

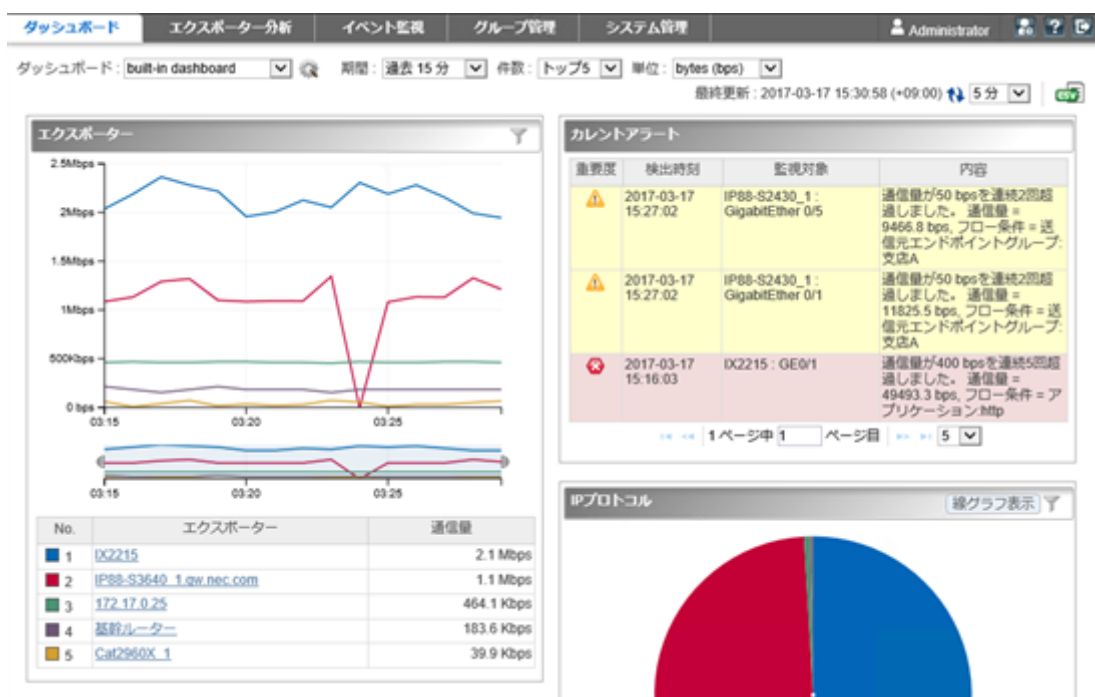


図 1-1 ダッシュボード表示

エクスポート分析

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

- 現在の通信状況だけではなく、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。

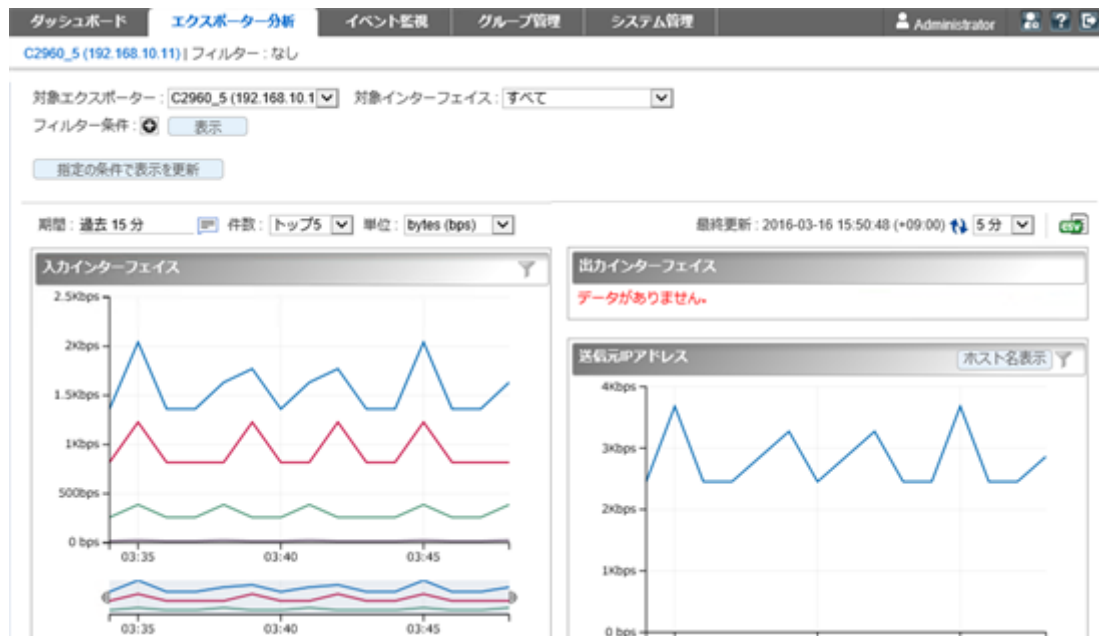


図 1-2 エクスポーター分析

イベント監視

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

ダッシュボード

エクスポート分析

イベント監視

グループ管理

システム管理

Administrator

イベント一覧

しきい値監視エントリ一覧

イベントの一覧

最終更新: 2017-03-17 15:19:34 (+09:00) 1分

1ページ中 1ページ目 100

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

図 1-3 イベント一覧

グループ管理

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

ダッシュボード

エクスポート分析

イベント監視

グループ管理

システム管理

Administrator

エンドポイントグループ一覧

IPグループ一覧

エンドポイントグループの一覧

追加

エンドポイントグループ名	IPアドレス	操作
人事部	192.168.3.1-192.168.3.100	 
営業部	192.168.3.101-192.168.3.200	 
広報部	192.168.2.0/255.255.255.0	 
支店A	172.17.0.0/255.255.255.0	 
支店B	172.17.4.0/255.255.255.0	 
経理部	192.168.1.0/255.255.255.0	 
開発部	192.168.4.0/255.255.255.0	 

図 1-4 エンドポイントグループ一覧

システム管理

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

ダッシュボード

エクスポーター分析

イベント監視

グループ管理

システム管理

Administrator

エクスポーター管理

アプリケーション定義

ユーザー管理

ライセンス登録

環境設定

アプリケーションの一覧

追加

アプリケーション名開始文字: A B C D E E G H I J K L M N O P Q R S T U V W X Y Z 数字 すべて

59 ページ中 1

ページ目

100































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

図 1-5 アプリケーション定義

1.3 動作環境

NFA の動作環境について説明します。

1.3.1 システム構成

NFA のシステム構成について説明します。

NFA の運用環境は、「[図 1-6 システム構成図 \(7 ページ\)](#)」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。

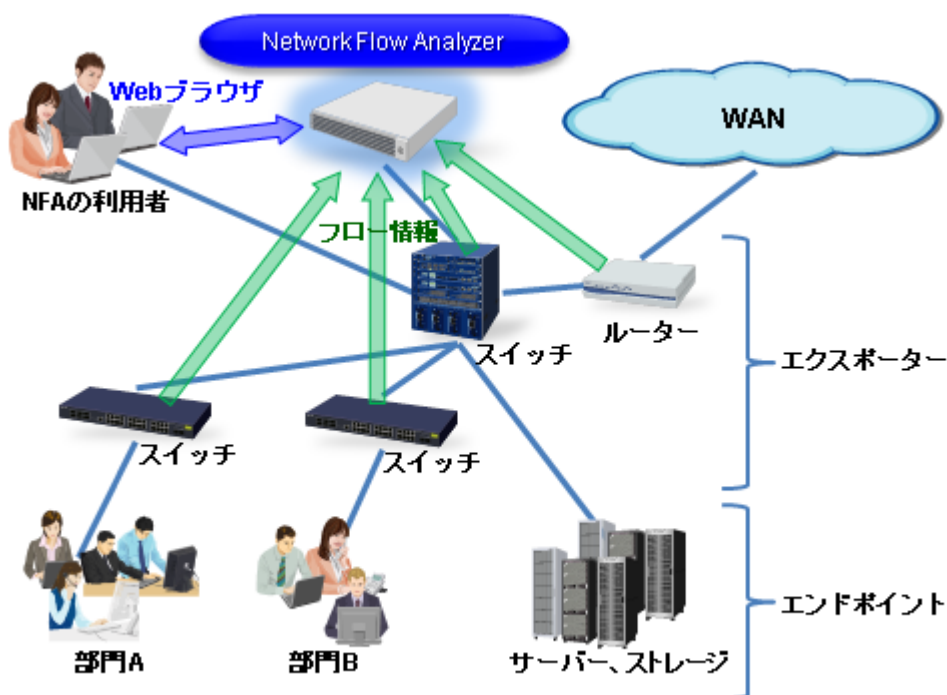


図 1-6 システム構成図

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

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

ヒント

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

1.3.2 システム要件

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

表 1-1 サーバーのシステム要件

項目	内容
CPU	Intel クアッドコア Xeon 以上、または同等の互換プロセッサを推奨
システムメモリ	最低 4GB 以上 (8GB 以上を推奨)
ディスク容量	インストールディレクトリ: 5GB 以上

項目	内容
	データディレクトリ: 最低 100GB 以上 データディレクトリに必要なサイズの見積りは、「 1.3.3.2 ディスク使用量の見積もり方法 (9 ページ) 」を参照してください。
OS	<ul style="list-style-type: none"> Red Hat Enterprise Linux 6 (x86_64) Red Hat Enterprise Linux 7 (x86_64)
フロープロトコル	<ul style="list-style-type: none"> NetFlow (v5、v9) IPFIX sFlow (v4、v5) NetFlow、IPFIX はサンプリングにも対応

表 1-2 Web ブラウザーの要件

項目	内容
対応ブラウザ	Windows 上で動作する以下のブラウザ <ul style="list-style-type: none"> Internet Explorer 11 Mozilla Firefox 38 以上 Google Chrome 48 以上
CPU	Intel Core i3 以上、または同等の互換プロセッサを推奨
システムメモリ	1GB 以上

ヒント

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

1.3.3 フローデータの管理について

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

1.3.3.1 フローデータの保持期間と丸め処理について

NFA では、大量のフローデータを限られたディスク容量の中で長期間保持するために、受信したフローデータを以下の「[表 1-3 フローデータの粒度と保持期間 \(8 ページ\)](#)」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 1-3 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

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
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。

1.3.3.2 ディスク使用量の見積もり方法

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

フローデータの蓄積、管理に必要なディスク使用量は、NFA が管理するエクスポートの台数、および、フローの発生頻度に関係しています。また、「[1.3.3.1 フローデータの保持期間と丸め処理について \(8 ページ\)](#)」で示した通り、フローデータに対する保持期間、および単位時間ごとの最大フロー数は、NFA で規定されています。そのため、フローデータの蓄積に必要なディスク使用量の目安は、これらを踏まえた計算式から算出することができます。

注意

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

具体的な算出方法を以下に説明します。

1. NFA で管理するエクスポートの台数を確認します。
今後の運用において増加する予定があれば、最終的な管理数を明確にします。
2. フローの保持期間を確認し、ディスク容量算出で使用する係数を以下の計算式から算出します。

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

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

計算結果の小数点以下は切り上げてください。

保持期間がデフォルト値のままであれば、係数は 2970 となります。

ヒント

フローデータに対する保持期間の変更については、「[1.3.3.1 フローデータの保持期間と丸め処理について \(8 ページ\)](#)」を参照してください。

3. 運用環境におけるフローの発生頻度(1 分間の平均フロー数)を確認します。
フローの発生頻度は、運用環境において 1 分間に平均何セッションの通信が発生しているのかをおおよその数値で求めます。
4. 以下の計算式にあてはめて、ディスク容量の目安を算出します。

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

- N: NFA が管理するエクスポートの台数
手順 1 で確認した値を代入して計算します。
- P: NFA の保持期間に影響を受ける係数
手順 2 で確認した値を代入して計算します。
- L: 単位時間ごとに保持する最大フロー数
デフォルトでは、最大で上位 1,000 フローを保持するため、1,000 を指定します。

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、「[1.3.3.3 保持するフロー数の上限を変更する \(11 ページ\)](#)」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

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

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

1.3.3.3 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、エクスポート、単位時間ごとに上位1,000フローを保持します。

この値は、インストール後の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ト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。

- エクスポート管理画面にて、各エクスポートの[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、エクスポート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。エクスポート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
```

1.3.3.4 フローの保持期間を変更する

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、「[1.3.3.1 フローデータの保持期間と丸め処理について（8 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

この保持期間を変更する手順について説明します。

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。

1.4 製品ライセンスとインターフェイスライセンス

NFA の製品ライセンスとインターフェイス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。

第2章 インストール

NFA のインストール手順について説明します。

目次

2.1 導入までの流れ.....	15
2.2 事前準備を行う	15
2.3 インストール処理を実行する	18
2.4 SSL サーバー証明書を準備する	20
2.5 製品が利用する通信ポート番号を確認する	24
2.6 ファイアウォールの設定を変更する	27
2.7 Web サーバーに関する追加の設定	29
2.8 サービスを起動する	30

2.1 導入までの流れ

NFA を導入するまでの作業の流れについて説明します。

インストール作業の流れを、「表 2-1 インストール作業の流れ (15 ページ)」に示します。

表 2-1 インストール作業の流れ

項番	概要	説明
1	インストールパラメーターの決定	「2.2.1 インストールパラメーターの設計を行う (15 ページ)」 インストール作業に必要なパラメーターを確認し、その値を決定します。
2	インストール先の環境確認	「2.2.2 インストール先の環境確認を行う (18 ページ)」 ディスクの空き容量や、OS のカーネルパラメーターの値が適正であるかどうか確認します。
3	インストーラーの実行	「2.3 インストール処理を実行する (18 ページ)」 インストールメディアに収録されたインストーラーを実行し、NFA をインストールします。
4	SSL サーバー証明書の準備	「2.4 SSL サーバー証明書を準備する (20 ページ)」 NFA には、HTTPS でアクセスします。HTTPS 通信用に、SSL サーバー証明書を用意します。 証明書は、自身で署名を行う自己署名証明書と、公的な認証局に発行してもらう証明書の 2 種類があります。どちらかを選択して準備します。
5	使用するポート番号の確認	「2.5 製品が利用する通信ポート番号を確認する (24 ページ)」 NFA の使用するポート番号が、NFA サーバー上の他のソフトウェアの使用するポート番号と干渉しないことを確認します。
6	ファイアウォールの設定	「2.6 ファイアウォールの設定を変更する (27 ページ)」 NetFlow、IPFIX、sFlow のパケット受信や、外部との HTTPS 通信を行うために、ファイアウォールの設定を変更します。
7	Web サーバーの追加設定	「2.7 Web サーバーに関する追加の設定 (29 ページ)」 必要に応じて、NFA の Web サーバーに関する追加の設定を行います。
8	サービスの起動	「2.8 サービスを起動する (30 ページ)」 NFA のサービスを起動し、Web ブラウザーからアクセスできることを確認します。

2.2 事前準備を行う

NFA をインストールする前の準備作業について説明します。

2.2.1 インストールパラメーターの設計を行う

インストール作業に先立ち、作業に必要なパラメーターを準備します。

製品を動作させるのに必要なカーネルパラメーター

NFA を動作させるためには、以下のカーネルパラメーターの要件を満たす必要があります。

表 2-2 カーネルパラメーターの要件

パラメーター名	説明
kernel.shmmax	各プロセスが使用できる共有メモリーの最大サイズです。バイト単位で指定します。 NFA では、256MB 以上の値を設定する必要があります。 最大の性能を引き出すために、2GB 以上の値を設定することを強く推奨します。

インストーラー実行時に必要なパラメーター

インストーラーを実行する際に必要なパラメーターを説明します。

表 2-3 インストーラー実行時に必要なパラメーター

パラメーター名	説明	デフォルト値
インストールディレクトリ	製品の実行ファイルをインストールするディレクトリです。 最大で 128 文字まで指定することができます。半角英数字、および "_", "-", "." のみ使用可能です。	/opt/nec/nfa
データディレクトリ	フロー情報や設定などのデータを保存するディレクトリです。 最大で 128 文字まで指定することができます。半角英数字、および "_", "-", "." のみ使用可能です。 インストールディレクトリとは別の場所を指定することを推奨します。 データディレクトリには、受信したフローデータを全て蓄積します。管理するエクスポーターの台数によっては、非常に多くの空き容量を必要とします。 必要な容量の計算は、「 1.3.3.2 ディスク使用量の見積もり方法 (9 ページ) 」を参照してください。	/opt/nec/nfa

SSL 証明書の作成に必要なパラメーター

NFA への HTTPS 通信用で使用する SSL サーバー証明書を作成するために、SSL サーバー証明書に関するパラメーター、および証明書の識別名 (Distinguished Name) に関するパラメーターを準備する必要があります。

SSL サーバー証明書を公的な認証局に発行してもらう場合、使用する認証局によっては、鍵の暗号化アルゴリズムや識別名など、一部のパラメーターに条件が指定されている場合があります。事前に、認証局が提示している条件を確認してください。

表 2-4 SSL サーバー証明書に関するパラメーター

パラメーター名	説明	デフォルト値
キーストアのパスワード	SSL サーバー証明書を格納するキーストアのパスワードです。	なし
秘密鍵のパスワード	SSL サーバー証明書の秘密鍵のパスワードです。	なし
エントリーの別名	SSL サーバー証明書を格納するエントリーの表示名です。	tomcat

パラメーター名	説明	デフォルト値
	特別な理由がない限り、デフォルト値をそのまま使用することをお勧めします。	
鍵の暗号化アルゴリズム	SSL サーバー証明書の鍵の暗号化アルゴリズムです。 自己署名証明書を利用する場合など、通常はデフォルト値のままで問題ありません。指定可能な値の詳細は「 A.1 nfa_ssl_keytool (57 ページ) 」を参照してください。	RSA
生成する鍵のサイズ	SSL サーバー証明書の鍵のサイズです。 自己署名証明書を利用する場合など、通常はデフォルト値のままで問題ありません。指定可能な値の詳細は「 A.1 nfa_ssl_keytool (57 ページ) 」を参照してください。	2048
署名アルゴリズム	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です。 通常はデフォルト値のままで問題ありません。指定可能な値の詳細は「 A.1 nfa_ssl_keytool (57 ページ) 」を参照してください。 公的な認証局に証明書を発行してもらう場合、発行依頼時に指定できる場合があります。詳細は、認証局にお問い合わせください。	SHA256withRSA
自己署名証明書の有効期限	自己署名証明書を利用する場合に指定する、証明書の有効期限です。作成時点からの有効日数を指定します。 公的な認証局に証明書を発行してもらう場合、通常、有効期限は認証局により決められるため、この値を準備する必要はありません。	3650 日 (約 10 年)

表 2-5 SSL サーバー証明書の識別名 (Distinguished Name) に関するパラメーター

パラメーター名	説明	例
サーバーの FQDN	NFA サーバーの完全修飾ドメイン名 (FQDN) です。SSL サーバー証明書の Common Name に相当します。 NFA にアクセスする全ての Web ブラウザーはこのドメイン名を URL に指定してアクセスするため、全ての Web ブラウザーが解決可能な名前である必要があります。	nfa.nec.com
部署名	製品を所有し運用する組織の部署名です。SSL サーバー証明書の Organizational Unit に相当します。	IT Operation Division
組織名	製品を所有し運用する組織の名称です。SSL サーバー証明書の Organizational Name に相当します。 通常、法律上の正式な英文組織名称を指定します。	NEC Corporation
市区町村名	製品を所有し運用する組織の属する市区町村の名前です。SSL サーバー証明書の Locality に相当します。 例えば、東京都港区の場合は Minato-ku と指定します。	Minato-ku
都道府県名	製品を所有し運用する組織の属する都道府県の名前です。SSL サーバー証明書の State に相当します。 例えば、東京都の場合は Tokyo と指定します。	Tokyo
国コード	製品を所有し運用する組織が属する国のコード名です。SSL サーバー証明書の Country に相当します。 日本の場合は、通常、JP と指定します。	JP

2.2.2 インストール先の環境確認を行う

NFA をインストールするサーバーの環境が、インストール要件を満たしているか確認します。

確認するのは、次の2点です。

- カーネルパラメーターの値は要件を満たしているか
 - ディスクの空き容量は十分か
1. カーネルパラメーター `kernel.shmmax` の値がインストール要件を満たしているか確認します。

```
# cat /proc/sys/kernel/shmmax
68719476736
```

表示された値はバイト単位です。上記の例では **64GB** となり、変更は不要です。

もし、**32MB (33554432)** などの小さな値が表示された場合は、最低 **256MB** 以上 (推奨値 **2GB** 以上) の値に変更してください。カーネルパラメーターの変更作業は、OS のマニュアルを参照の上で実施してください。

2. インストール先のディスク空き容量が十分か確認します。
 - a. NFA が必要とするディスク容量を計算します。

ディスク容量の計算方法の詳細は、「[1.3.3.2 ディスク使用量の見積もり方法 \(9 ページ\)](#)」を参照してください。

- b. インストール先のディスクの空き容量を確認します。

ディスク空き容量の確認は、`df` コマンドを使用して調べることができます。

```
# df -h
Filesystem              Size  Used Avail Use% マウント位置
/dev/mapper/vg_nfa-lv_root
                        22T   1.8T   19T    9% /
tmpfs                    16G    0    16G    0% /dev/shm
/dev/sda1                 485M   32M   429M    7% /boot
```

表示されたマウント位置から、空き容量 (**Avail**) の値を確認してください。

この例では、`/opt/nec/nfa` にインストールする場合、インストール先には **19TB** の空き容量があります。

空き容量が足りない場合は、インストール先を変更するか、ディスクを増設してください。

2.3 インストール処理を実行する

インストールメディアに収録されているインストーラーを実行し、NFA をインストールします。

1. CD-ROM ドライブにインストールメディアを挿入し、CD-ROM をマウントします。

ここでは、CD-ROM のマウントポイントを/media として説明します。別の場所にマウントした場合は、適宜読み替えてください。

2. 次のコマンドを実行して、インストーラーを起動します。

```
# /media/nfa-install
```

3. インストールディレクトリのパスを入力するプロンプトが表示されるので、パスを入力します。

```
Input installation path [default: /opt/nec/nfa]
>
```

1 行目の右にはデフォルト値が表示されます。デフォルト値から変更しない場合は、何も入力せずに Enter キーを押します。

4. データディレクトリのパスを入力するプロンプトが表示されるので、パスを入力します。

```
Input data installation path [default: /opt/nec/nfa]
>
```

1 行目の右にはデフォルト値が表示されます。デフォルト値から変更しない場合は、何も入力せずに Enter キーを押します。

5. 入力したパスを確認し、インストールを開始します。

インストールディレクトリとデータディレクトリのパスを入力すると、入力したパスが表示されます。入力したパスに間違いがなければ、y を入力し Enter キーを押します。

```
----- Confirmation -----
Installation path      : /opt/nec/nfa
Data Installation path : /opt/nec/nfa
-----

Is it OK to install? (y/n): y
```

y を入力すると、インストール処理が開始されます。

n を入力すると、パスを入力するプロンプトが再度表示され、インストール先を修正することができます。

次のメッセージが表示されれば、インストール処理は完了です。

```
Installing controller ... done
Installing collector  ... done
```

インストール処理の途中でエラーが発生した場合は、エラーメッセージが表示されます。エラーメッセージが表示された場合は、「[B.1 インストーラー実行時のエラーと対策 \(61 ページ\)](#)」を参照し、対処を行ってください。

2.4 SSL サーバー証明書を準備する

NFA には HTTPS でアクセスします。この HTTPS 通信に、SSL サーバー証明書を準備します。

SSL サーバー証明書には、次の 2 種類があります。

- 自己署名証明書
- 公的な認証局に発行してもらう証明書

また、NFA では、Java keytool などを使って、他で作成した証明書を流用して使用することもできます。

それぞれの場合の準備手順を説明します。

- 「[2.4.1 自己署名証明書を準備する \(20 ページ\)](#)」
- 「[2.4.2 公的な認証局が発行する証明書を準備する \(22 ページ\)](#)」
- 「[2.4.3 他で作成した証明書を使用する \(24 ページ\)](#)」

⚠ 注意

サポートする証明書の形式は、Java keytool で扱える形式と同等の、X.509 形式の証明書です。この形式は多くの認証局がサポートしている形式ですが、ご利用予定の認証局がサポートしているかどうか、念のため事前に確認してください。

2.4.1 自己署名証明書を準備する

NFA で使用する SSL サーバー証明書として、自己署名証明書を作成する手順を説明します。

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 \(57 ページ\)](#)」を参照してください。

作成した証明書は、NFA にアクセスするすべての Web ブラウザーに配布、インストールします。

1. 次のコマンドを実行して、鍵のペア (公開鍵と非公開鍵) を生成し、鍵に対する証明書を作成します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ssl_keytool genkeypair
```

鍵と証明書を格納するキーストアのパスワードや、証明書の識別名、鍵のパスワードに関する情報を入力していきます。

- `[]` 内にはデフォルト値が表示されています。何も入力せず Enter キーを押すと、デフォルト値が使用されます。
- 鍵のパスワード (key password) の入力では、何も入力せず Enter キーを押すと、キーストアと同じパスワードが設定されます。

```

What is your server domain name? (FQDN)
[nfa.nec.com]:
What is the name of your organizational unit?
[Unknown]: IT Operation Division
What is the name of your organization?
[Unknown]: NEC Corporation
What is the name of your City or Locality?
[Unknown]: Minato-ku
What is the name of your State or Province?
[Unknown]: Tokyo
What is the two-letter country code for this unit?
[Unknown]: JP
Is CN=nfa.nec.com, OU=IT Operation Division, O=NEC Corporation,
L=Minato-ku, ST=Tokyo, C=JP correct?
[No]: yes
Enter key password for <tomcat>
(RETURN if same as keystore password):

```

ヒント

- `nfa_ssl_keytool` コマンドは、いくつかの引数を取ることができます。鍵のアルゴリズムやサイズ、有効期限などを変更したい場合は、「[A.1 nfa_ssl_keytool \(57 ページ\)](#)」を参照し、オプション引数を指定してください。

鍵のアルゴリズムを ECDSA、鍵のサイズを 256bit に設定する場合の実行例:

```

# cd /opt/nec/nfa/controller/bin
# ./nfa_ssl_keytool genkeypair -keyalg EC -keysize 256

```

- 鍵の内容を変更して再度作成するには、`nfa_ssl_keytool delete` コマンドを実行してから再度 `nfa_ssl_keytool genkeypair` コマンドを実行するか、`nfa_ssl_keytool genkeypair` コマンドを最初とは異なる `-alias` を指定して実行します。

コマンドの詳細は、「[A.1 nfa_ssl_keytool \(57 ページ\)](#)」を参照してください。

作成された証明書は、自己署名された状態になります。

2. 次のコマンドを実行し、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。

コマンドの実行に成功すると、指定したファイルにバイナリー符号化方式の証明書が出力されます。

`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、「[3.1.3 Web ブラウザーに SSL サーバー証明書をインポートする \(35 ページ\)](#)」を参照してください。

2.4.2 公的な認証局が発行する証明書を準備する

NFA で使用する SSL サーバー証明書として、公的な認証局に署名済み証明書を発行してもらう手順を説明します。

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 \(57 ページ\)](#)」を参照してください。

サポートする証明書の形式は、Java `keytool` で扱える形式と同等の、X.509 形式の証明書です。この形式は多くの認証局がサポートしている形式ですが、ご利用予定の認証局がサポートしているかどうか、念のため事前に確認してください。

1. 次のコマンドを実行して、鍵のペア (公開鍵と非公開鍵) を生成し、鍵に対する証明書を作成します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ssl_keytool genkeypair
```

鍵と証明書を格納するキーストアのパスワードや、証明書の識別名、鍵のパスワードに関する情報を入力していきます。

- [] 内にはデフォルト値が表示されています。何も入力せず Enter キーを押すと、デフォルト値が使用されます。
- 鍵のパスワード (key password) の入力では、何も入力せず Enter キーを押すと、キーストアと同じパスワードが設定されます。

```
What is your server domain name? (FQDN)
[nfa.nec.com]:
What is the name of your organizational unit?
[Unknown]: IT Operation Division
What is the name of your organization?
[Unknown]: NEC Corporation
What is the name of your City or Locality?
[Unknown]: Minato-ku
What is the name of your State or Province?
[Unknown]: Tokyo
What is the two-letter country code for this unit?
[Unknown]: JP
Is CN=nfa.nec.com, OU=IT Operation Division, O=NEC Corporation,
L=Minato-ku, ST=Tokyo, C=JP correct?
[No]: yes
Enter key password for <tomcat>
(RETURN if same as keystore password):
```

ヒント

- `nfa_ssl_keytool` コマンドは、いくつかの引数を取ることができます。鍵のアルゴリズムやサイズ、有効期限などを変更したい場合は、「[A.1 nfa_ssl_keytool \(57 ページ\)](#)」を参照し、オプション引数を指定してください。

鍵のアルゴリズムを ECDSA、鍵のサイズを 256bit に設定する場合の実行例:

```
# cd /opt/nec/nfa/controller/bin
# ./nfa_ssl_keytool genkeypair -keyalg EC -keysize 256
```

- 鍵の内容を変更して再度作成するには、nfa_ssl_keytool delete コマンドを実行してから再度 nfa_ssl_keytool genkeypair コマンドを実行するか、nfa_ssl_keytool genkeypair コマンドを最初とは異なる -alias を指定して実行します。

コマンドの詳細は、「[A.1 nfa_ssl_keytool \(57 ページ\)](#)」を参照してください。

2. 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 <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。

3. 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。

4. 認証局から署名済み証明書が届いたら、まずは、認証局のルート証明書をインポートします。

ルート証明書は、NFA サーバー上にファイルとして保存し、次のコマンドでインポートできます。

```
# <%インストールディレクトリ%>/controller/bin/nfa_ssl_keytool
importcert -alias <alias> <filename>
```

<alias>には任意の名前を指定できます。ルート認証局の名前など、分かりやすい名前を指定してください。

認証局によっては、ルート証明書の他に中間証明書のインポートが必要になる場合があります。インポートする証明書の詳細は、認証局にお問い合わせください。

5. ルート証明書や中間証明書をインポートした後に、署名済みの自身の証明書をインポートします。

自身の証明書のインポートにも、nfa_ssl_keytool importcert コマンドを使用します。次のように、-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。

NFA サーバー側の証明書の準備は、これで完了です。

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。

2.4.3 他で作成した証明書を使用する

NFA で使用する SSL サーバー証明書として、他で作成した証明書を流用して使用する手順を説明します。

事前に JKS (Java KeyStore) 形式のキーストアを準備し、キーストア内に有効な鍵と証明書を作成しておいてください。また、準備したキーストアのファイルは、NFA サーバー上に配置しておいてください。

1. 次のテキストファイルを開きます。

```
<%データディレクトリ%>/controller/conf/tomcat.properties
```

ファイルが存在しない場合は新規作成します。ファイルのエンコーディングは UTF-8 にしてください。

2. 以下の内容を tomcat.properties ファイルに記載します。

```
nfa.tomcat.https.keyAlias = 鍵を含むエントリの別名
nfa.tomcat.https.keyPass = 鍵のパスワード
nfa.tomcat.https.keystoreFile = キーストアファイルの絶対パス
nfa.tomcat.https.keystorePass = キーストアのパスワード
```

注意

tomcat.properties ファイルに、外部のキーストアを使用する設定を記載した場合、nfa_ssl_keytool コマンドは使用できなくなります。代わりに、Java keytool コマンドなどを直接使用して管理してください。

Java keytool コマンドは、NFA サーバー上にもインストールされています。

```
<%インストールディレクトリ%>/controller/jre/bin/keytool
```

自己署名証明書の場合などは、バイナリー符号化形式の証明書 (.cer) を出力し、Web ブラウザーにインポートしてください。

2.5 製品が利用する通信ポート番号を確認する

NFA では、外部との通信、および製品内部の通信のために、いくつかの通信ポートを利用します。

NFA サーバー内で、他の製品と利用する通信ポート番号が重複していないことを確認します。

まず、NFA が利用する通信ポート番号一覧を説明します。利用するポート番号が他の製品と重複していた場合は、NFA が利用するポート番号か、他の製品が利用するポート番号のいずれかを変更してください。

2.5.1 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 2-6 NFA が利用する通信ポート番号一覧 (外部通信) (25 ページ)」、「表 2-7 NFA が利用する通信ポート番号一覧 (内部通信) (25 ページ)」に示します。

表 2-6 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。

表 2-7 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。

2.5.2 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。

利用するポート番号が他の製品と重複していた場合は、NFA が利用するポート番号か、他の製品が利用するポート番号のいずれかを変更する必要があります。

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. 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 2-8 通信ポート番号の設定ファイルと設定項目 (外部通信) (25 ページ)」、「表 2-9 通信ポート番号の設定ファイルと設定項目 (内部通信) (26 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。

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。

表 2-8 通信ポート番号の設定ファイルと設定項目(外部通信)

用途	設定項目
HTTPS 通信	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 設定ファイル collector/conf/collector.conf 指定形式 netflow.port = 9995

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。

表 2-9 通信ポート番号の設定ファイルと設定項目(内部通信)

用途	設定項目
フローデータ DB 通信	<ul style="list-style-type: none"> 設定ファイル collector/conf/flowdb.conf 指定形式 flowdb.port = 27100
	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 設定ファイル controller/conf/controller.properties 指定形式 systemdb.port = 27110
	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 設定ファイル controller/conf/event.properties 指定形式 eventdb.port = 27120

用途	設定項目
	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 設定ファイル controller/conf/controller.properties 指定形式 message.server.port = 27200
	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 設定ファイル collector/conf/nfalog.conf 指定形式 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。

- 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。

- NFA のサービスを起動します。

```
# /etc/init.d/nec-nfa-service start
```

すでに起動していた場合は、まず/etc/init.d/nec-nfa-service stop で停止してから、/etc/init.d/nec-nfa-service start で起動してください。

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。

2.6 ファイアウォールの設定を変更する

NFA の利用する通信ポートが、ファイアウォールによってブロックされないように、ファイアウォールの設定を変更します。

NFA サーバー上でオープンして利用する通信ポートのデフォルト値は、「表 2-10 NFA が利用する通信ポート番号一覧 (外部通信) (28 ページ)」、「表 2-11 NFA が利用する通信ポート番号一覧 (内部通信) (28 ページ)」の通りです。また、NFA から外部への通信で使用するポートのデフォルト値は、「表 2-12 NFA から外部への宛先ポート番号 デフォルト値一覧 (28 ページ)」の通りです。

これらのポート番号がファイアウォールによってブロックされないよう、ファイアウォールの設定を変更します。

表 2-10 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。

表 2-11 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。

表 2-12 NFA から外部への宛先ポート番号 デフォルト値一覧

名称	ポート番号	プロトコル	方向	用途
SNMP Get	161	UDP	OUT	NFA サーバーからエクスポートへの SNMP 通信で使用する宛先ポート番号です。 このポート番号は、Web コンソール上の設定で、エクスポート単位に変更できます。
SNMP Trap	162	UDP	OUT	NFA サーバーから外部のネットワーク管理製品への SNMP トラップ送信で使用する宛先ポート番号です。 このポート番号は、Web コンソール上の設定で変更できます。

ここでは、ファイアウォールに iptables や firewalld を利用している場合の設定例を説明します。

他のファイアウォールソフトウェアやネットワーク経路上のファイアウォールに関しては、各製品のマニュアルを参照してください。

「2.5.2 製品が利用する通信ポート番号を変更する (25 ページ)」の手順などにより利用するポート番号を変更している場合は、設定例中のポート番号を適宜読み替えてください。

- `iptables` を利用している場合は、`/etc/sysconfig/iptables` を編集します。

以下は編集後のファイルの一例です。記載方法の詳細については、OS の提供するマニュアルを参照してください。

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT
-A INPUT -p udp -m udp --dport 6343 -j ACCEPT
-A INPUT -p udp -m udp --dport 9995 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
COMMIT
```

下線部が追記した部分です。

ファイルの編集後は、設定を有効にするために `iptables` サービスを再起動してください。

- `firewalld` を利用している場合は、次のようにコマンドを実行します。

```
# firewall-cmd --permanent --add-port=443/tcp
# firewall-cmd --permanent --add-port=6343/udp
# firewall-cmd --permanent --add-port=9995/udp
# firewall-cmd --reload
```

`firewalld` の詳細は OS の提供するマニュアルを参照してください。

2.7 Web サーバーに関する追加の設定

NFA の Web サーバーに関する追加の設定について説明します。

2.7.1 Web サーバーログの自動削除設定

NFA の Web サーバーに関するログを定期的に自動削除するための設定について説明します。

NFA の Web コンソールに対するアクセスログおよび Web サーバー自身の動作ログは、以下のディレクトリに蓄積されます。

<インストールディレクトリ>/controller/tomcat/logs/

このディレクトリ内の以下のログについては自動ではローテーションおよび削除はされません。必要に応じて、`cron` などを利用して古いログを自動的に削除するように設定してください。

- localhost_access_log.yyyy-mm-dd.txt
- catalina.yyyy-mm-dd.log

yyyy-mm-dd は、NFA サーバーの日付を表します。例えば、localhost_access_log.2016-04-01.txt は、2016/4/1 の Web コンソールに対するアクセスログファイルです。

設定例

以下は、30 日以上経過したログファイルを、毎日深夜 1 時にチェックして削除する cron 設定の例です。

```
0 1 * * * /usr/bin/find /opt/nec/nfa/controller/tomcat/logs/
-type f -regex '^.*\.[0-9]+-[0-9]+-[0-9]+\.(txt|log)$'
-mtime +30 -exec /bin/rm -f {} \;
```

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。

2.8 サービスを起動する

インストールが正常に完了すると、NFA のサービスを起動することができます。

NFA のサービスは、起動スクリプト (System V init スクリプト) を直接実行するか、OS を再起動することで起動することができます。

ここでは、起動スクリプトを実行してサービスを起動する方法を説明します。

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て、サービスを起動します。

```
# /etc/init.d/nec-nfa-service start
```

正常に起動すると、次のようなメッセージが表示されます。

- Red Hat Enterprise Linux 6 の場合

```
Starting systemdb:      [ OK ]
Starting eventdb:      [ OK ]
Starting controller:   [ OK ]
Starting web server:   [ OK ]
Starting flowdb:       [ OK ]
Starting log server:   [ OK ]
Starting collector:    [ OK ]
```

サービスには複数のデーモンプロセスが含まれているため、複数行出力されます。

- Red Hat Enterprise Linux 7 の場合

```
Starting nec-nfa-service (via systemctl): [ OK ]
```

正常に起動できなかったプロセスは、[OK]の代わりに[NG]と表示されます。

3. 次のコマンドを実行して、デーモンプロセスが確かに起動していることを確認します。

```
# /etc/init.d/nec-nfa-service status
```

正常に起動していると、*name (pid process_id) is running* が、各プロセスごとに表示されます。

```
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...
```

4. 次のコマンドを実行して、**Web** サーバーの待ち受けポートが開いていることを確認します。

```
# ss -an | grep 443
```

443 は、**Web** サーバーのデフォルトの待ち受けポート番号です。

Web サーバーが正常に起動していると、次のように、443 番ポートが **LISTEN** 状態になっています。

```
LISTEN      0          100          :::443          :::*
```

正常に起動できなかった場合、「[B.2 サービス起動時のエラーと対策 \(62 ページ\)](#)」を参照し、対処してください。

第3章 インストール後の環境設定

NFA のインストール後に必要な環境設定の方法について説明します。

目次

3.1 Web コンソールを使用するための準備を行う	33
3.2 Web コンソールにアクセスする	36
3.3 システムの環境設定を行う	37
3.4 製品ライセンスを登録する	38
3.5 エクスポーターの装置側設定を行う	40
3.6 ユーザーを追加する	41

3.1 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。

3.1.1 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。

3.1.2 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。

サポートしているブラウザは、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 \(35 ページ\)](#)」の設定が必須となります。

Internet Explorer の設定確認

Internet Explorer の設定確認はインターネット オプションダイアログで行います。Internet Explorer の画面上で Alt+T キーを押し、表示されたメニューから[**インターネット オプション**]を選択してください。各タブの詳細な設定手順については、Internet Explorer のヘルプを参照してください。

- ・ [セキュリティ]タブ
 - 「信頼済みサイト」への登録
- NFA サーバーの URL を、「信頼済みサイト」に登録します。

ヒント

「信頼済みサイト」に登録したくない場合は、NFA サーバーが「制限付き」サイト以外に分類されるように設定を行ってください。

- JavaScript の有効化

「信頼済みサイト」の[レベルのカスタマイズ]で、[アクティブ スクリプト]の設定が「有効にする」になっていることを確認します。

- [プライバシー]タブ

NFA サーバーの属するゾーンが「インターネット」の場合、Cookie を承諾する設定となっていることを確認してください。

ヒント

- NFA サーバーの属するゾーンが「信頼済みサイト」または「ローカル イン트라ネット」の場合、Cookie はブロックされません。
 - NFA サーバーの属するゾーンが「制限付きサイト」の場合、Cookie は常にブロックされ、Web コンソールは使用できません。
-

Mozilla Firefox の設定確認

Mozilla Firefox のオプション設定画面で確認を行います。詳細な設定手順については、Mozilla Firefox のヘルプを参照してください。

- [プライバシー]パネル

[履歴]の設定で、サイトから送られてきた Cookie を保存する設定になっていることを確認します。

Google Chrome の設定確認

Google Chrome の設定画面で確認を行います。画面下部の[詳細設定を表示]をクリックし、[プライバシー]セクションの[コンテンツの設定]ボタンをクリックします。表示されたコンテンツの設定ダイアログ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。

- [Cookie]

Cookie を保存する設定になっていることを確認します。

- [JavaScript]

JavaScript の実行が許可され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。

3.1.3 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。

⚠ 注意

証明書を Web ブラウザーにインポートせず、警告が出ている状態のままで利用すると、Internet Explorer ではまれに不正動作(ページが表示できなかったり、画面上の操作が行えないなど)が発生します。証明書をインポートしてご利用になることを強くお勧めします。

- Internet Explorer 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 \(57 ページ\)](#)」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。

- Mozilla Firefox の場合は、以下の手順を実施します。
 1. Web ブラウザーで以下の URL にアクセスします。

`https://<NFA サーバーのドメイン名(FQDN)>/nfa/`

ヒント

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。

安全な接続ではない旨の警告が表示されます。

2. **[エラー内容]**ボタンをクリックし、表示された**[例外を追加]**ボタンをクリックします。
3. セキュリティ例外の追加ダイアログで、**[次回以降もこの例外を有効にする]**にチェックがあることを確認の上で、**[セキュリティ例外を承認]**ボタンをクリックします。

⚠ 注意

セキュリティ例外を追加する際は、追加する証明書の内容が正しいことをよく確認の上で実行してください。

ログイン画面が表示されれば、証明書のインポートは完了です。

3.2 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。

事前に「[3.1 Web コンソールを使用するための準備を行う \(33 ページ\)](#)」に記載の、Web ブラウザーの設定を行っておく必要があります。

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。

初期ユーザー名は「admin」、初期パスワードは「password」です。

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

- 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。
- 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、エクスポート分析画面、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。

3.3 システムの環境設定を行う

管理対象のエクスポート情報 (エクスポート、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 のデフォルトの設定では、未知のエクスポートからフロー情報を受信すると、そのエクスポート情報 (エクスポートおよびインターフェイスの情報) を自動で登録します。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。

ヒント

フロー情報の受信時にエクスポート情報を自動登録しないように設定することもできます。この自動登録のポリシーは、環境設定画面から設定できます。環境設定画面を開くには、[システム管理]>[環境設定]をクリックします。

エクスポート情報を自動登録する際、NFA は、以下の情報を自動で収集し、エクスポート情報として登録します。

- エクスポートの DNS 上の名前 (FQDN)
- エクスポートの SNMP 上の名前 (sysName)
- インターフェイスの名前 (ifName)

FQDN の情報は、NFA サーバーの名前解決機構に従って、エクスポートの IP アドレスを変換し、取得します。

sysName、および ifName については、SNMP 情報取得パラメーターのデフォルト値をあらかじめ登録しておくことで、そのパラメーターでの SNMP 通信により、エクスポート側の MIB から情報を取得します。

ここでは、SNMP 情報取得パラメーターのデフォルト値を設定する手順を説明します。

本操作を実施する前に、運用環境のエクスポート側に設定している 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ト側の 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. [エクスポート情報取得パラメーター]の各入力欄に対し、エクスポート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。

3.4 製品ライセンスを登録する

製品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。

製品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。

3.5 エクスポートの装置側設定を行う

エクスポートの装置側設定を変更し、NetFlow、IPFIX や sFlow 情報を NFA に送ったり、SNMP で情報を取得できるようにします。

NFA にエクスポートからのフロー情報を集めるには、次の設定をエクスポート装置上で行う必要があります。

- NetFlow、IPFIX または sFlow 情報を NFA サーバーに送信する設定
- SNMP による情報取得を有効にする設定

具体的な設定方法は、各エクスポートの装置マニュアルを参照してください。

以下に、装置側で設定が必要な項目の概要を説明します。

1. フロー情報の送信先を NFA サーバーの IP アドレスに設定します。また、送信先ポート番号を、NetFlow、IPFIX の場合は 9995 に、sFlow の場合は 6343 に設定します。

ヒント

「[2.5.2 製品が利用する通信ポート番号を変更する \(25 ページ\)](#)」の手順で NetFlow、IPFIX や sFlow の受信ポート番号を変更している場合は、変更後のポート番号に合わせて装置側の設定を行ってください。

2. 必要に応じて、インターフェイスの `ifIndex` を固定化 (持続) する設定を行います。

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

このようなエクスポートについては、再起動後もインターフェイスの `ifIndex` を保持するように設定を行ってください。

Cisco IOS におけるコンフィグ例:

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

3. NetFlow、IPFIX の場合は、アクティブフローのキャッシュタイムアウトを 1 分に設定します。

Cisco IOS におけるコンフィグ例:

```
(config)# ip flow-cache timeout active 1
```

4. sFlow の場合は、カウンターサンプルを送信する間隔を 1 分に設定します。

NEC UNIVERGE IP8800/S シリーズにおけるコンフィグ例:

```
(config)# sflow polling-interval 60
```

5. 装置の SNMP バージョンを 1 または 2c に設定します。
6. 装置の SNMP Get のコミュニティ名を設定します。

3.6 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 32 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任意の文字で指定します。最大文字数は 32 文字です。先頭および末尾に半角スペースを指定することはできません。

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、8~32 文字の文字数で指定します。

- 半角英数字
- 半角スペース
- 以下の記号

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

- [パスワード再入力]

[初期パスワード]で指定したものと同一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。

第4章

基本操作

NFA の基本的な操作について説明します。

目次

4.1 Web コンソール構成.....	43
4.2 ウィジェットの種類.....	45
4.3 ウィジェットを操作する	48
4.4 個人設定の内容を更新する	52

4.1 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 4-1 Web コンソールの構成 \(43 ページ\)](#)」で示す領域で構成されています。



図 4-1 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。

- **[エクスポート分析]タブ**

分析対象のエクスポートを絞り込んで、詳細な通信量の分析を行うためのエクスポート分析画面を表示します。

- **[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ト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、エクスポート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

エクスポート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。

4.2 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ト分析画面では、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 4-1 通信量分析ウィジェット

ウィジェットの種類	説明
エクスポート	通信量の多いエクスポートを表示します。 エクスポートの通信量は、そのエクスポートが持つインターフェー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 4-2 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。
カンパセーション	通信量の多いカンパセーション(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。

ウィジェットの種類	説明
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 4-2 折れ線グラフ表示タイプのウィジェット \(46 ページ\)](#)」に示します。

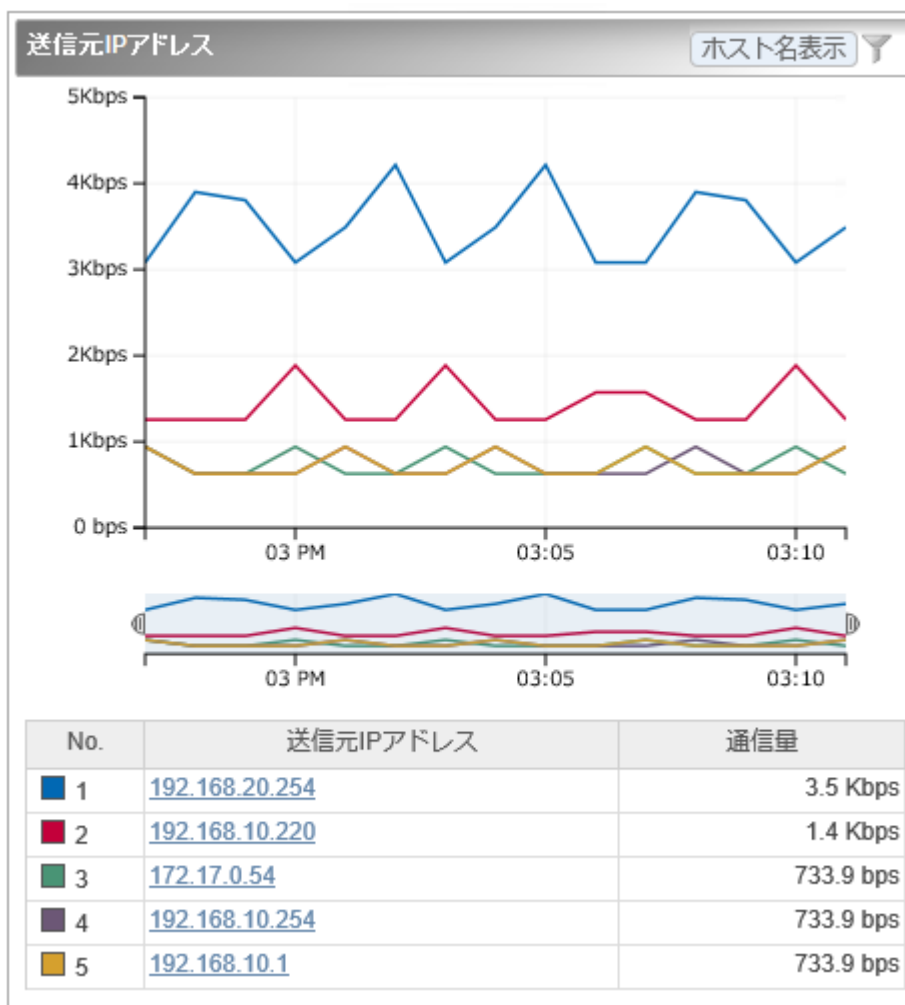


図 4-2 折れ線グラフ表示タイプのウィジェット

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 4-3 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。

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 4-3 円グラフ/折れ線グラフ表示タイプのウィジェット \(47 ページ\)](#)」に示します。

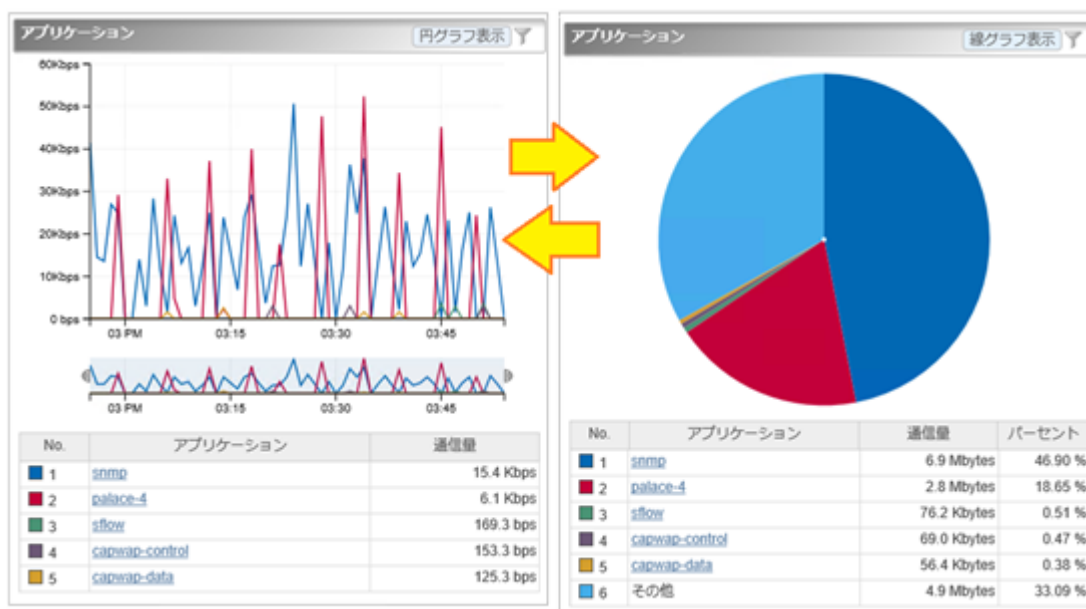


図 4-3 円グラフ/折れ線グラフ表示タイプのウィジェット

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 4-4 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 4-4 一覧表示タイプのウィジェット \(48 ページ\)](#)」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




 1 ページ中 1 ページ目  5 

図 4-4 一覧表示タイプのウィジェット

4.3 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。

4.3.1 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、エクスポート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]を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=「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=「192.168.1.100」

4.3.2 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。

4.3.3 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(レンジセクターと呼ぶ)を選択します。
2. レンジセ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。

- ・ レンジセレクト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、レンジセレクトの左右のカーソルが非表示になります。レンジセレクト内で、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。

4.3.4 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で 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。

注意

ホスト名表示に変換した場合、エクスポーター分析画面へのリンクは表示されません。

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。

4.4 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任意の文字で指定します。最大文字数は 32 文字です。先頭および末尾に半角スペースを指定することはできません。

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、8~32 文字の文字数で指定します。

- 半角英数字
- 半角スペース
- 以下の記号

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

3. 変更内容を確認し、[OK]ボタンをクリックします。

第5章 アップグレード

NFA のアップグレード手順について説明します。

目次

5.1 アップグレードする	54
---------------------	----

アップグレードにより、古いバージョンから最新バージョンへ更新されます。

5.1 アップグレードする

インストールメディアに収録されているインストーラを実行し、NFA をアップグレードします。

1. CD-ROM ドライブにインストールメディアを挿入し、CD-ROM をマウントします。

ここでは、CD-ROM のマウントポイントを /media として説明します。別の場所にマウントした場合は、適宜読み替えてください。

2. アップグレード前に、NFA のサービスを停止します。

```
# /etc/init.d/nec-nfa-service stop
```

3. 次のコマンドを実行して、インストーラーを起動します。

```
# /media/nfa-upgrade
```

4. 表示されたバージョン番号を確認し、アップグレードを開始します。

各機能コンポーネントの現在のバージョンが左に、アップグレード後のバージョンが右の [] 内に表示されます。バージョン番号に間違いがなければ、y を入力し Enter キーを押します。

```
Network Flow Analyzer version 1.1.0-7 Upgrade Installer

----- Confirmation -----
Controller : 1.0.0-19  -> [ 1.1.0-7 ]
Collector  : 1.0.0-19  -> [ 1.1.0-7 ]
-----

Is it OK to upgrade? (y/n): y
```

y を入力すると、インストール処理が開始されます。

n を入力すると、インストール処理は中止されます。

次のメッセージが表示されれば、アップグレードの適用は完了です。

```
Upgrading controller ... done
Upgrading collector  ... done
```

アップデート処理の途中でエラーが発生した場合は、エラーメッセージが表示されます。エラーメッセージが表示された場合は、「[B.1 インストーラー実行時のエラーと対策 \(61 ページ\)](#)」を参照し、対処を行ってください。

適用後に、NFA のサービスを起動させてください。

```
# /etc/init.d/nec-nfa-service start
```

第 6 章

アンインストール

NFA をアンインストールする手順について説明します。

目次

6.1 アンインストールにおける注意事項.....	56
6.2 製品をアンインストールする	56

6.1 アンインストールにおける注意事項

NFA をアンインストールする際の注意事項について説明します。

製品のアンインストールは、主に `rpm -e` コマンドで行います。

- インストールディレクトリとデータディレクトリを分けてインストールしていた場合、`rpm -e` コマンドではデータディレクトリは削除されません。別途、手動で削除する必要があります。
- インストールディレクトリとデータディレクトリが同じ場合、`rpm -e` コマンドによりすべてのデータが削除されます。
- `rpm -e` コマンドでは、`/etc/init.d/nec-nfa-service` スクリプトはアンインストールされません。アンインストール手順の中で、手動で削除する必要があります。

6.2 製品をアンインストールする

NFA のアンインストール手順について説明します。

1. `root` ユーザーでログインします。
2. 次のコマンドを実行し、NFA のサービスを停止します。

```
# /etc/init.d/nec-nfa-service stop
```

3. 次のコマンドを実行し、製品をアンインストールします。

```
# rpm -e nec-nfa-controller nec-nfa-collector
```

4. 次のコマンドを実行し、サービスの起動スクリプトを削除します。

```
# chkconfig --del nec-nfa-service  
# rm -f /etc/init.d/nec-nfa-service
```

5. インストールディレクトリとデータディレクトリを分けていた場合、データディレクトリを手動で削除します。

以上で、アンインストール作業は完了です。

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 コマンドの詳細は、以下の URL を参照してください。

- <http://docs.oracle.com/javase/jp/8/docs/technotes/tools/unix/keytool.html> *1

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、-keypass 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]
                        [-keypass KEYPASS] [-keyalg KEYALG] [-keysize KEYSIZE] [-sigalg SIGALG]
                        [-validity DAYS] [-dname DNAME]
```

*1 この URL は、2017 年 3 月現在のものです。

```
nfa_ssl_keytool selfcert [-help] [-storepass PASS] [-alias ALIAS]
                        [-keypass KEYPASS] [-sigalg SIGALG] [-validity DAYS] [-dname DNAME]
```

```
nfa_ssl_keytool certreq [-help] [-storepass PASS] [-alias ALIAS]
                        [-keypass KEYPASS] FILE
```

```
nfa_ssl_keytool importcert [-help] [-storepass PASS] [-alias ALIAS]
                           [-keypass KEYPASS] FILE
```

```
nfa_ssl_keytool exportcert [-help] [-storepass PASS] [-alias ALIAS] FILE
```

```
nfa_ssl_keytool storepasswd [-help] [-storepass PASS] [-new NEWPASS]
```

```
nfa_ssl_keytool keypasswd [-help] [-storepass PASS] [-alias ALIAS]
                           [-keypass KEYPASS] [-new NEWPASS]
```

```
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。

- `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。

- `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。

-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。

-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ー API 仕様 & リファレンス](#) ^{*2} 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。

*2 この URL は、2017 年 3 月現在のものです。

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。

-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。

付録 B. トラブルシューティング

NFA のセットアップ作業中に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 インストーラー実行時のエラーと対策

インストーラー実行時に発生するエラーとその対策を説明します。

SHMMAX must be larger than 256 MB

次のようなメッセージが表示された場合、カーネルパラメーター `kernel.shmmax` の値が 256MB より小さく、製品インストール要件を満たしていないのが原因です。

```
ERROR: SHMMAX must be larger than 256 MB.
```

`kernel.shmmax` の値を 256MB (268,435,456 byte) 以上に設定してください。最大の性能を引き出すために、2GB 以上の値に設定することを強く推奨します。カーネルパラメーター値の変更後、再度インストーラーを実行してください。

Non-root user cannot access the install path

次のようなメッセージが表示された場合、インストールディレクトリに非 `root` ユーザーがアクセスする権限がないことが原因です。

```
ERROR: Non-root user cannot access the install path: /opt/nec/nfa
       Check the permission of the install destination.
```

インストールディレクトリとして指定したディレクトリ、およびその途中のディレクトリについて、非 `root` ユーザーがアクセスできるように、`chmod` コマンドなどで設定を行ってください。その後、再度インストーラーを実行してください。

installing package nec-nfa-controller-x.y.z-n.x86_64 needs XXXMB on the / file system

次のようなメッセージが表示された場合、インストールディレクトリに指定したファイルシステム上の空き容量が足りないか、ファイルシステムが書き込み可能でないことが原因です。

```
Installing controller . failed
ERROR: Failed to install controller package: code=1
       installing package nec-nfa-controller-x.y.z-n.x86_64 needs XXXMB
       on the / filesystem.
```

インストールディレクトリには、十分な空き容量を持った書き込み可能な場所を指定してください。空き容量を確保した後、再度インストーラーを実行してください。

Failed to initialize data. Directory exists

次のようなメッセージが表示された場合、データディレクトリに指定したディレクトリ中に、インストール時に作成するディレクトリが既に存在していることが原因です。

```
Installing controller . failed
ERROR: Failed to initialize data.
       Directory exists: /opt/nec/nfa/controller/conf
```

Failed to initialize data が表示されると、その下に、以下のようなリカバリー用のコマンドが表示されます。

```
Try to run the following command later.
/opt/nec/nfa/controller/bin/nfa_init_controller -data /opt/nec/nfa
```

エラーメッセージ中に表示されたディレクトリを削除の上、表示されたコマンドを **root** ユーザーで実行してください。

B.2 サービス起動時のエラーと対策

サービス起動時に発生するエラーとその対策を説明します。

サービス起動時に [NG] が表示された場合

サービス起動時に [NG] が表示された場合、データディレクトリの初期化が正常に行われていない可能性があります。

次の手順で対処を行ってください。

1. 一度、サービスを停止します。

```
# /etc/init.d/nec-nfa-service stop
```

2. 以下のコマンドを実行します。

```
# <%インストールディレクトリ%>/controller/bin/nfa_init_controller
  -data <%データディレクトリ%>
# <%インストールディレクトリ%>/collector/bin/nfa_init_collector
  -data <%データディレクトリ%>
```

データディレクトリが空でない場合、次のようなエラーが表示される場合があります。

```
ERROR: Directory exists: /opt/nec/nfa/controller/conf
```

エラーが表示されたら、表示されたディレクトリを削除の上、再度実行してください。

3. SSL サーバー証明書を作成します。

「[2.4 SSL サーバー証明書を準備する \(20 ページ\)](#)」の手順を実施してください。

4. サービスを再度起動します。

```
# /etc/init.d/nec-nfa-service start
```

Web サーバーの待ち受けポート 443/tcp が存在しないか LISTEN 状態ではない場合

`ss -an | grep 443` などのコマンドで Web サーバーの待ち受けポート 443/tcp の状態を確認しても、開かれたポートが存在しない場合、SSL 証明書が正常に作成されていない可能性があります。

次の手順で対処を行ってください。

1. SSL サーバー証明書を作成します。
「[2.4 SSL サーバー証明書を準備する \(20 ページ\)](#)」の手順を実施してください。
2. サービスを再起動します。

```
# /etc/init.d/nec-nfa-service stop  
# /etc/init.d/nec-nfa-service start
```

OS 起動時にサービスが自動で起動しない場合

手動でサービスを起動することはできるが、OS 起動時にサービスが自動で起動しない場合、`chkconfig` コマンドなどで自動起動設定が変更されている可能性があります。

OS 起動時の自動起動を有効にしたい場合は、次のコマンドを実行し対処を行ってください。

```
# chkconfig nec-nfa-service on
```

WebSAM
Network Flow Analyzer 1.1
スタートアップガイド

NFA0LSJ0110-02

2019 年 07 月 02 版 発行

日本電気株式会社

© NEC Corporation 2014 - 2019