NEC

WebSAM

Network Flow Analyzer 3.2
スタートアップガイド

WebSAM

著作権

商標

はじめに

このたびは、WebSAM Network Flow Analyzer 3.2 (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。

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（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。	Admin
「第 3 章　インストール後の環境設定（38 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 4 章　基本操作（52 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（66 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。	Admin
「付録 A　コマンドリファレンス（68 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。	Admin
「付録 B　トラブルシューティング（77 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。	Admin

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。

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　表記規則

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

本書では、以下の略称を用いて記述しています。

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

NFA の製品概要について説明します。

目次

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。

1.2　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。

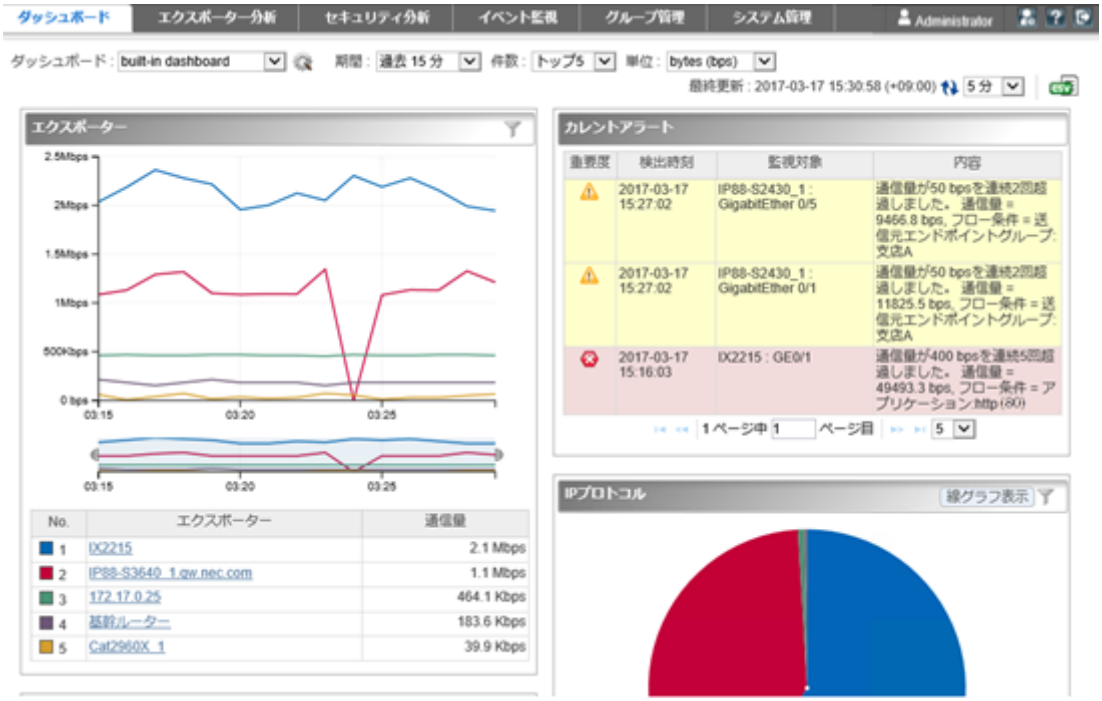

図 1-1　ダッシュボード表示

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。

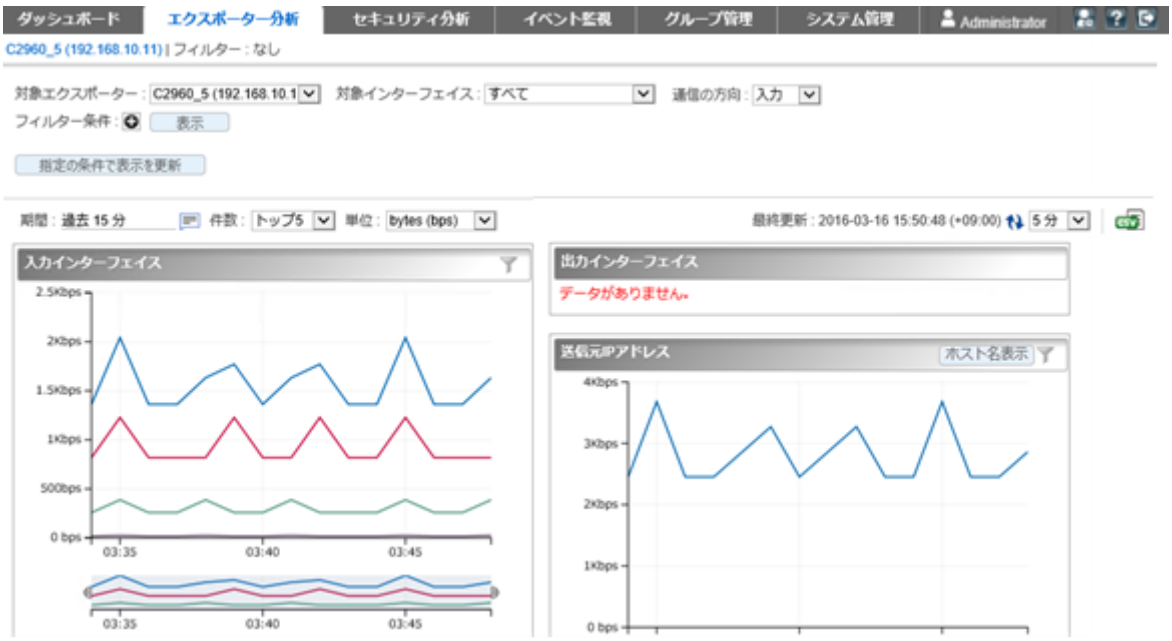

図 1-2　エクスポーター分析

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。

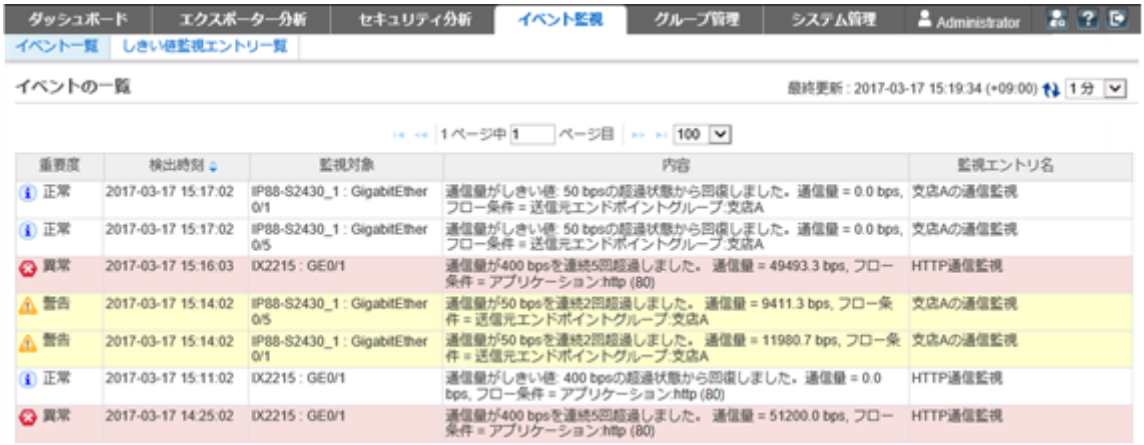

図 1-4　イベント一覧

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。

図 1-6　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 のシステム構成

NFA の運用環境は、「図 1-7 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。

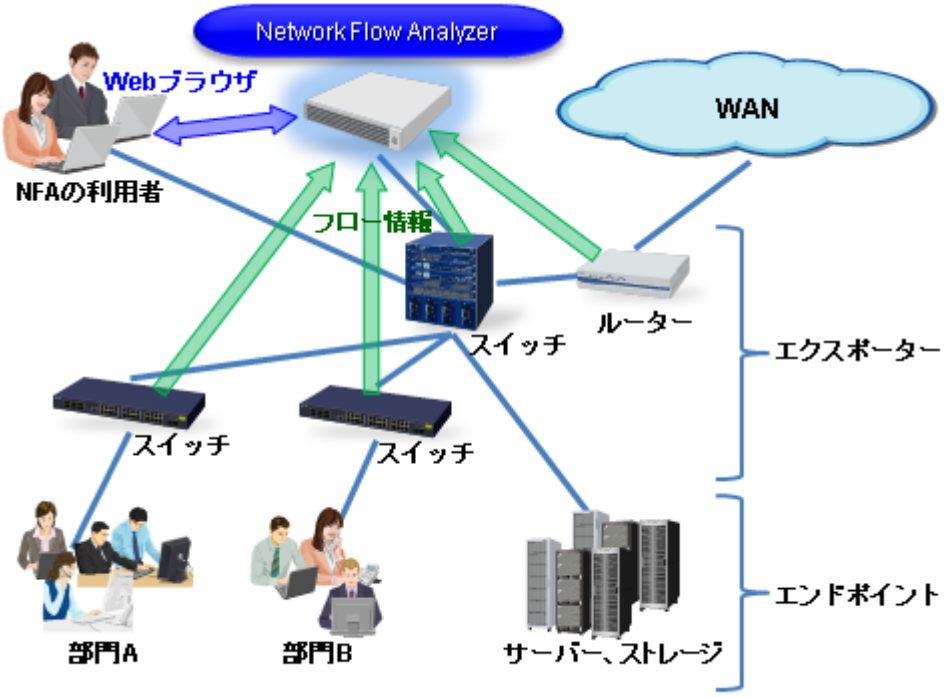

図 1-7　システム構成図

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（8 ページ）」に示します。

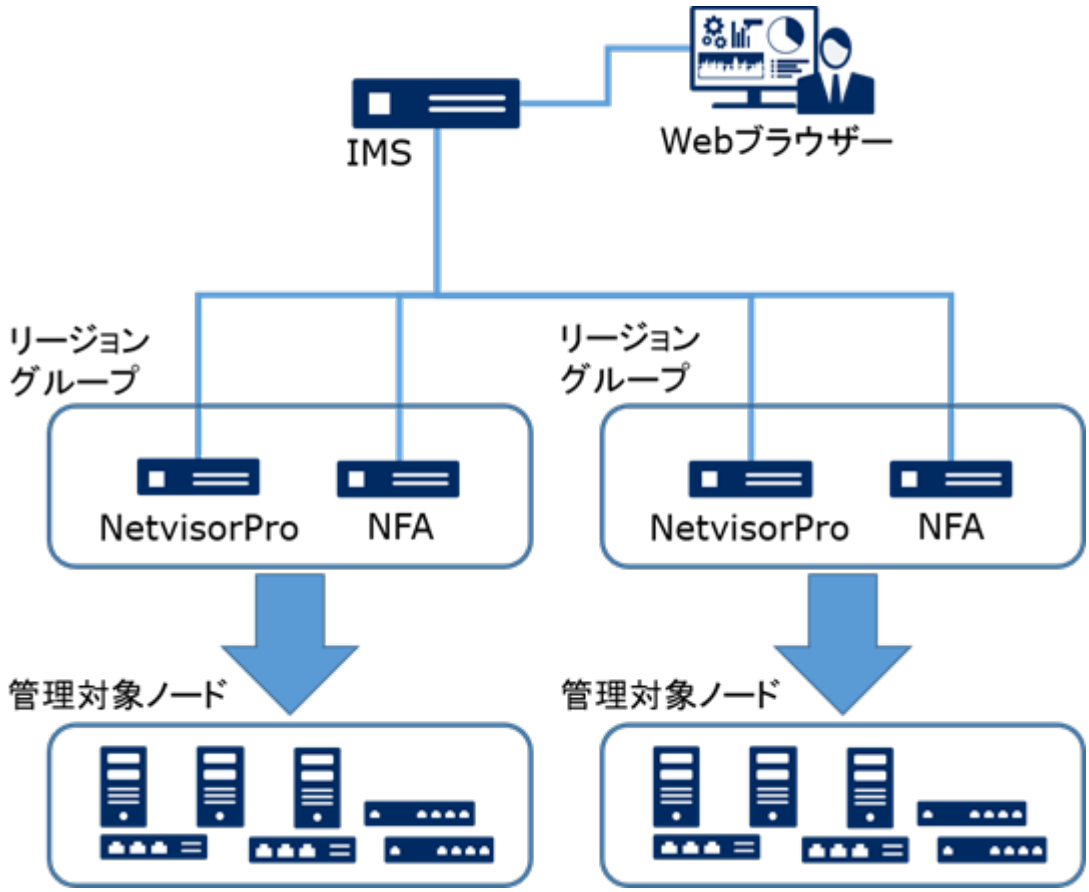

図 1-8　統合運用時のシステム構成例

「図 1-8 統合運用時のシステム構成例（8 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。

1.3.2　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 注 1
システムメモリ	最低 4GB 以上 (16GB 以上を推奨) 注 1
ディスク容量	インストールディレクトリ: 5GB 以上
	データディレクトリ: 最低 100GB 以上 注 2 注 3 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（11 ページ）」を参照してください。
OS	• Red Hat Enterprise Linux 9 (x86_64) 注 4 注 6 (9.2 以上をサポート) • Red Hat Enterprise Linux 8 (x86_64) 注 5 注 6
フロープロトコル	• NetFlow (v5、v9) • IPFIX • sFlow (v4、v5) NetFlow、IPFIX はサンプリングにも対応

注

1. 仮想化環境で運用する場合、オーバーコミットの影響を受けずに、確実に指定した CPU リソース、および、メモリリソースが利用できるように、仮想化基盤の設定を行ってください。
2. 製品仕様上、ハードディスクへのアクセスが頻繁に行われます。利用環境に合わせて、「SAS 15,000rpm」などのアクセス性能の高いハードディスクを利用することを強く推奨します。また、「RAID 5」,「RAID 50」,「RAID 10」 のいずれかの構成で運用することを推奨します。
3. 仮想化環境で運用する場合、他の仮想マシンの動作の影響を受けて、ハードディスクへの十分なアクセス性能が得られない場合があります。SSD (Solid State Drive) を利用するなどして、ハードディスクへの十分なアクセス性能を確保してください。
4. 以下のパッケージをインストールする必要があります。
   - python3
   - bzip2
   - chkconfig
   - initscripts
5. 以下のパッケージをインストールする必要があります。
   - python3
   - bzip2
6. SELinux を無効（disabled）に設定する必要があります。

表 1-2　Web ブラウザーの要件

項目	内容
対応ブラウザー	Windows 上で動作する以下のブラウザー • Microsoft Edge 104 以上 • Google Chrome 104 以上

項目	内容
CPU	Intel Core i3 以上、または同等の互換プロセッサを推奨
システムメモリ	1GB 以上

ヒント

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

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（10 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
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、「1.3.3.1　フローデータの保持期間と丸め処理について（10 ページ）」で示した通り、フローデータに対する保持期間、および単位時間ごとの最大フロー数は、NFA で規定されています。そのため、フローデータの蓄積に必要なディスク使用量の目安は、これらを踏まえた計算式から算出することができます。

⚠ 注意

- エクスポー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（43 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、「1.3.3.1　フローデータの保持期間と丸め処理について（10 ページ）」を参照してください。

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

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

4. 以下の計算式にあてはめて、ディスク容量の目安を算出します。

   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、「3.3　保持するフロー数の上限を変更する（42 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

1.4　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。

ヒント

本バージョンでは、割り当てることができる Security Monitoring ライセンスの数は 5 となっています。

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

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。

ヒント

複数の NFA、または、NFA と NetvisorPro を統合する場合は、別途、IMS コンポーネントをインストールする必要があります。詳細は、「WebSAMNetwork Management Web コンソール スタートアップガイド」を参照してください。

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（16 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 I/O 性能、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（20 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（22 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（27 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（30 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	動作環境の追加設定	「2.7　動作環境の追加設定を行う（32 ページ）」 必要に応じて、 NFA の動作環境に対する追加の設定を行います。
8	IMS コンポーネント利用のための設定	「2.8　IMS コンポーネント利用のための設定を行う（34 ページ）」 IMS コンポーネントを利用した統合運用を行う場合の設定を行います。 IMS コンポーネントを利用しない場合は、設定不要です。
9	サービスの起動	「2.9　サービスを起動する（36 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 (11 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
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。 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。	tomcat
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（68 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（68 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（68 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

パラメーター名	説明	例
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

IMS コンポーネント利用時に必要なパラメーター

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。

IMS コンポーネントを利用する場合に、設定作業で必要となるパラメーターを説明します。

表 2-6　IMS コンポーネントの利用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
ims.application-instance-id (manager id)	IMS コンポーネントが、接続する NFA を識別するために必要な ID を半角英数字で指定します。 本パラメーターは、IMS コンポーネント側の設定ファイル (ims-conf.ini) の設定値と一致させる必要があります。	未定義
ims.msgqueue.host (ims ip address)	IMS コンポーネントをインストールするサーバーの IPv4 アドレスを指定します。 IMS コンポーネントをクラスタシステムにインストールしている場合は、クラスタシステムのフローティング IP を指定します。	127.0.0.1
ims.msgqueue.port (port number)	IMS コンポーネントの Message Queue との通信で利用する通信ポート番号を指定します。	28110
ims.webserver.base-url (ims web url)	IMS コンポーネントが提供する Web コンソールにアクセスするための URL を指定します。 本パラメーターは、ブラウザー側および NFA 側からアクセス可能な URL を指定する必要があります。	http://localhost
ims.sso.enabled	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するかどうかを以下のように指定します。 • true : シングルサインオンの動作を有効にします。 • false : シングルサインオンの動作を無効にします。	false

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 3 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

- ディスクの I/O 性能は十分か

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を確認します。

```
# 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を確認します。

   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（11 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。

3. インストール先となるディスクの I/O 性能が十分かを確認します。

   a. インストールメディアに収録されている `fio` コマンドをサーバーの任意の場所に配置します。

   `fio` コマンド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/fio`

   b. `fio` コマンドを用いて、random write の性能を測定します。

   以下のように `fio` コマンドを実行します。

```
# fio -filename=<%測定対象のディスクのパス%>/fio -direct=1
-rw=randwrite -bs=8k -size=20G -numjobs=5 -group_reporting
-name=randomwrite
```

*<%測定対象のディスクのパス%>*には、NFA をインストールする際に、データディレクトリとして指定予定のパスを指定します。

上記のコマンドでは、指定パスに fio ディレクトリを作成し、そのディレクトリ内に、8KB のブロックサイズでデータを書き込むことで、ディスクの I/O 性能を測定します。

c. `fio` コマンドによるディスクの I/O 性能の測定結果を確認します。

コマンドの実行後、出力内容の以下の部分を読み取ります。

- `write:` から始まる行の IOPS 値、および BW 値(スループット)
- `lat (usec):` から始まる行の、avg の値(レイテンシー平均値)

以下に出力例を示します。

```
randomwrite:   (g=0):   rw=randwrite,   bs=(R)   4096B-4096B,   (W)
4096B-4096B,
 (T) 4096B-4096B, ioengine=psync, iodepth=1
...
fio-3.15
Starting 5 processes
Jobs: 1 (f=1): [w(1),_(4)][99.9%][w=23.5MiB/s][w=6009 IOPS][eta 00m:
07s]
randomwrite: (groupid=0, jobs=5): err= 0: pid=14996: Tue Jan 21
18:14:55 2020
  write: IOPS=2669, BW=10.4MiB/s (10.9MB/s)(100GiB/9819695msec)
    clat (usec): min=38, max=16726k, avg=1867.65, stdev=30805.21
     lat (usec): min=38, max=16726k, avg=1867.85, stdev=30805.21
    clat percentiles (usec):
 （以下略）
```

NFA においては、以下の 2 つの指標が、記載している値以上であることを推奨します。

- IOPS (Input Output Per Second): 1900
- スループット: 15 MiB/s

ヒント

すべてのエクスポーターのフローレートの合計が 6,000,000 フロー/分となるようなフローデータを NFA で処理する場合は、 以下に示すディスク I/O 性能を確保する必要があります。

- IOPS (Input Output Per Second): 2,335 以上
- スループット: 18.2 Mib/s 以上

性能測定の完了後、`fio` コマンドが作成した fio ディレクトリは削除してください。

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. インストールメディアの ISO イメージをマウントします。

   ここでは、インストールメディア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. インストーラーを起動します。

   インストール先の OS に合わせて、以下のコマンドを実行します。

   - Red Hat Enterprise Linux 9 (x86_64)

     ```
     # /media/NFA/Linux/nfa-install-rhel9
     ```

   - Red Hat Enterprise Linux 8 (x86_64)

     ```
     # /media/NFA/Linux/nfa-install-rhel8
     ```

   ヒント

   インストーラーの起動後、途中で中止したい場合は、Ctrl+C を入力することで、中止することができます。

   ⚠ 注意

   インストール先の OS に対応していないコマンドを実行した場合は、インストール処理が失敗するため注意してください。

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、インストール処理を開始します。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。

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

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

⚠ 注意

開始後は、Ctrl+C などで処理を中断しないでください。

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（77 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 通信用に、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（22 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（24 ページ）」
- 「2.4.3　他で作成した証明書を使用する（26 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（68 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。

```
Enter keystore password:
Re-enter new password:
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
```

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（68 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 コマンドを実行します。

  コマンドの詳細は、「A.1　nfa_ssl_keytool（68 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（40 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（68 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。

```
Enter keystore password:
Re-enter new password:
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
```

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（68 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` コマンドを実行します。

  コマンドの詳細は、「A.1　nfa_ssl_keytool（68 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 -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。

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 PKCS12 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。

ヒント

Java KeyStore (JKS) 形式のキーストアを使用することもできます。JKS 形式のキーストアを使用する場合は、後述する設定ファイルの編集で、nfa.tomcat.https.keystoreType の値に JKS を指定してください。

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
nfa.tomcat.https.keystoreType = PKCS12
```

⚠ 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 2-7 NFA が利用する通信ポート番号一覧 (外部通信)（27 ページ）」、「表 2-8 NFA が利用する通信ポート番号一覧 (内部通信)（28 ページ）」に示します。

表 2-7　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。 詳細は、「2.7.2　Microsoft 365 定義更新用の通信でプロキシサーバーを利用する（33 ページ）」を参照してください。

表 2-8　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 2-9 通信ポート番号の設定ファイルと設定項目(外部通信)（28 ページ)」、「表 2-10 通信ポート番号の設定ファイルと設定項目(内部通信)（29 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 2-9　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

用途	設定項目
	netflow.port = 9995

表 2-10　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

用途	設定項目
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 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。

3. 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。

ヒント

ポート番号の変更内容は、NFA のサービス起動時に反映されます。

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 2-11 NFA が利用する通信ポート番号一覧 (外部通信)（30 ページ)」、「表 2-12 NFA が利用する通信ポート番号一覧 (内部通信)（31 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 2-13 NFA から外部への宛先ポート番号 デフォルト値一覧（31 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 2-11　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。

名称	ポート番号	プロトコル	方向	用途
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。 詳細は、「2.7.2　Microsoft 365 定義更新用の通信でプロキシサーバーを利用する（33 ページ）」を参照してください。

表 2-12　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 2-13　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ターへの 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、エクスポーター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 firewalld や iptables 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（28 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。

- 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。

- 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。

2.7 動作環境の追加設定を行う

NFA の動作環境に対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。

2.7.2 Microsoft 365 定義更新用の通信でプロキシサーバーを利用する

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ための通信において、プロキシサーバーを利用するための設定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 を利用して、マイクロソフトのサイト 「endpoints.office.com」 にアクセスします。

NFA からマイクロソフトのサイトへの通信において、プロキシサーバーを利用する必要がある場合は、以下の設定を行います。

1. root ユーザーで NFA サーバーにログインします。
2. 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。

3. 設定ファイル (controller.properties) に、プロキシサーバーを利用するためのパラメーターを追記し、保存します。

   指定形式:

   ```
   https.proxy.host = <proxy server name>
   https.proxy.port = <port number>
   https.proxy.user = <username>
   https.proxy.password = <password>
   ```

   ***<proxy server name>*:**

利用するプロキシサーバーのドメイン名を指定します。

***<port number>*:**

利用するプロキシサーバーのポート番号を指定します。

***<username>*:**

プロキシ認証で利用するユーザー名を指定します。プロキシ認証を行わない場合は設定不要です。

***<password>*:**

プロキシ認証で利用するパスワードを指定します。プロキシ認証を行わない場合は設定不要です。

ヒント

プロキシ認証は、Basic 認証と Digest 認証に対応しています。

設定例:

```
https.proxy.host = proxysrv.nec.com
https.proxy.port = 8080
```

サービス起動後、設定内容が NFA に反映されます。

2.8　IMS コンポーネント利用のための設定を行う

IMS コンポーネントを利用し、複数の NFA、または、NFA と NetvisorPro との統合運用をする場合に行う設定について説明します。

ヒント

IMS コンポーネントを利用しない場合、本設定は不要です。

IMS コンポーネントを利用する場合、以下の 3 つの設定を行います。

- IMS コンポーネントのセットアップ

  IMS コンポーネントのインストールや NFA からの接続を許可するための IMS コンポーネントの設定を行います。

  詳細は、「WebSAM Network Management Web コンソール スタートアップガイド」を参照してください。

- IMS コンポーネントとの接続設定

  IMS コンポーネントと接続するための NFA 側の設定を行います。

- シングルサインオンのための設定

  IMS コンポーネントの Web コンソールから、シングルサインオンで、NFA の Web コンソールにアクセスできるようにするための設定を NFA 側で行います。

NFA 側で行う設定は、以下の設定ファイル (controller.properties) を更新することで行います。

設定ファイル:

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

ヒント

- 設定ファイル (controller.properties) が存在しない場合は、新規に作成してください。
- 設定ファイル (controller.properties) の更新内容は、NFA のサービス起動時に反映されます。

⚠ 注意

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 (controller.properties) 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。

IMS コンポーネントとの接続設定

設定ファイル (controller.properties) の以下のパラメーターを編集し、上書きして保存します。

```
ims.application-instance-id = <manager id>
ims.msgqueue.host = <ims ip address>
ims.msgqueue.port = <port number>
```

<manager id>

IMS コンポーネントが、接続する NFA を識別するための ID を指定します。

本パラメーターは、IMS コンポーネント側の設定ファイル (ims-conf.ini) の設定値と一致させる必要があります。

<ims ip address>

IMS コンポーネントをインストールするサーバーの IPv4 アドレスを指定します。

IMS コンポーネントをクラスタシステムにインストールしている場合は、クラスタシステムのフローティング IP を指定します。

<port number>

IMS コンポーネントの Message Queue との通信で利用する通信ポート番号を指定します。

本パラメーターは、デフォルトの通信ポート番号を変更した場合に、修正が必要になります。

設定例:

```
ims.application-instance-id = nfa01
ims.msgqueue.host = 192.168.1.200
ims.msgqueue.port = 28110
```

シングルサインオンのための設定

設定ファイル (controller.properties) の以下のパラメーターを編集し、上書きして保存します。

```
ims.webserver.base-url = <ims web url>
ims.sso.enabled = <true|false>
```

<ims web url>

IMS コンポーネントが提供する Web コンソールにアクセスするための URL を指定します。

⚠ 注意

本パラメーターは、ブラウザー側および NFA 側からアクセス可能な URL を指定する必要があります。

<true|false>

シングルサインオンの動作を有効にするかどうかを以下のように指定します。

- true : シングルサインオンの動作を有効にします。
- false : シングルサインオンの動作を無効にします。

ここでは、「true」を指定します。

設定例:

```
ims.webserver.base-url = http://ims.nec.com
ims.sso.enabled = true
```

2.9 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。

   ```
   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（78 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

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　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。

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 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（40 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。

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。

- 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（68 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。

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（39 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

- 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

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、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
```

3.4　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、「1.3.3.1　フローデータの保持期間と丸め処理について（10 ページ）」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。

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、以下の設定ファイルにおいて、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。

- 設定ファイル:

  `<%`***データディレクトリ***`%>/collector/conf/collector.conf`
- 設定パラメーター:

```
rawdb.switch = 1
```

ヒント

設定ファイル (collector.conf) に `rawdb.switch` の指定がない場合は、「1」を指定した場合と同じ動作(一時記録用データベースへの書き込みが有効)となります。

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。

```
# /etc/init.d/nec-nfa-service 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。

```
# /etc/init.d/nec-nfa-service 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　エクスポーターの情報取得のための設定を行う

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 のデフォルトの設定では、未知のエクスポーターからフロー情報を受信すると、そのエクスポーター情報 (エクスポーター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ター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。

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

- エクスポーターの DNS 上の名前 (FQDN)
- エクスポーターの 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、エクスポーターの 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、エクスポーターの 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。

3.7　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。

3.8　エクスポーターの装置側設定を行う

エクスポーター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 にエクスポーターからのフロー情報を集めるには、次の設定をエクスポーター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、各エクスポーター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（28 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。

   エクスポーターを再起動すると、エクスポーターの仕様によっては、分析対象のインターフェイスに対応する ifIndex の値が変化する場合があります。この場合、NFA では、

分析箇所のインターフェイスの特定が正しく行えないため、分析結果も正しく表示することができなくなります。

このようなエクスポーターについては、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. NetFlow v9、IPFIX の場合は、特定フィールドタイプを含むフローレコード定義の作成を行います。

   NFA では、NetFlow v9、および、IPFIX において、特定フィールドタイプを含むフローレコードのみをサポートしています。NetFlow v9、または、IPFIX を利用する場合は、エクスポーター側の設定において、以下のフィールドタイプを含むフローレコード定義の作成を行います。

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

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

---

*1　個々のフィールドタイプは必須ではありませんが、特別な理由が無い限りエクスポータ側でフローレコードに含める設定を行ってください。
フローレコードに該当情報が存在しない場合は任意値(ゼロ)として扱います。 そのため、該当する widget が表示されない等の結果となり、フローを正しく分析出来ない場合があります。

*2　エクスポーター側でフローレコードに含める設定を必ず行ってください。ライセンスを正しく付与するために必須な情報です。

*3　エクスポーター側でフローレコードに含める設定を必ず行ってください。フローの通信量を統計分析するために必須な情報です。

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

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

3.9　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。

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

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（53 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。

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 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 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。

ウィジェットの種類	説明
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 4-2 折れ線グラフ表示タイプのウィジェット（56 ページ）」に示します。

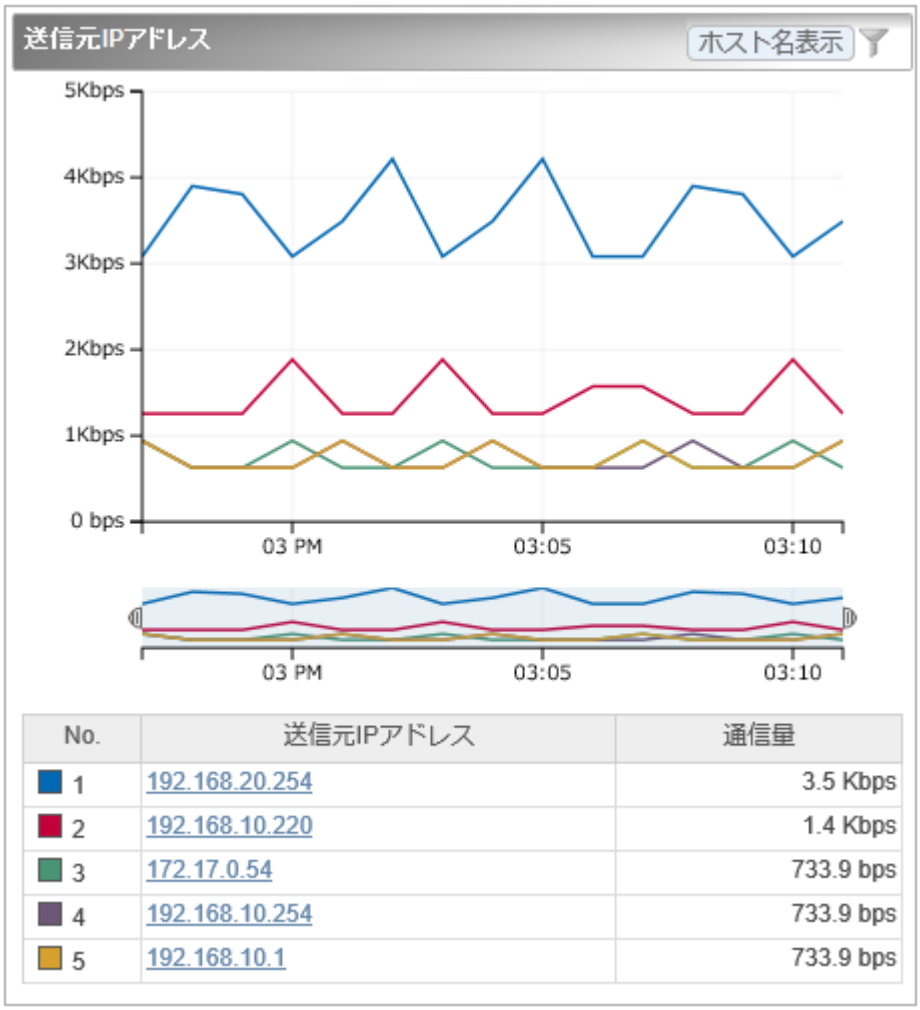

図 4-2　折れ線グラフ表示タイプのウィジェット

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。
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 4-3 円グラフ/折れ線グラフ表示タイプのウィジェット（57 ページ）」に示します。

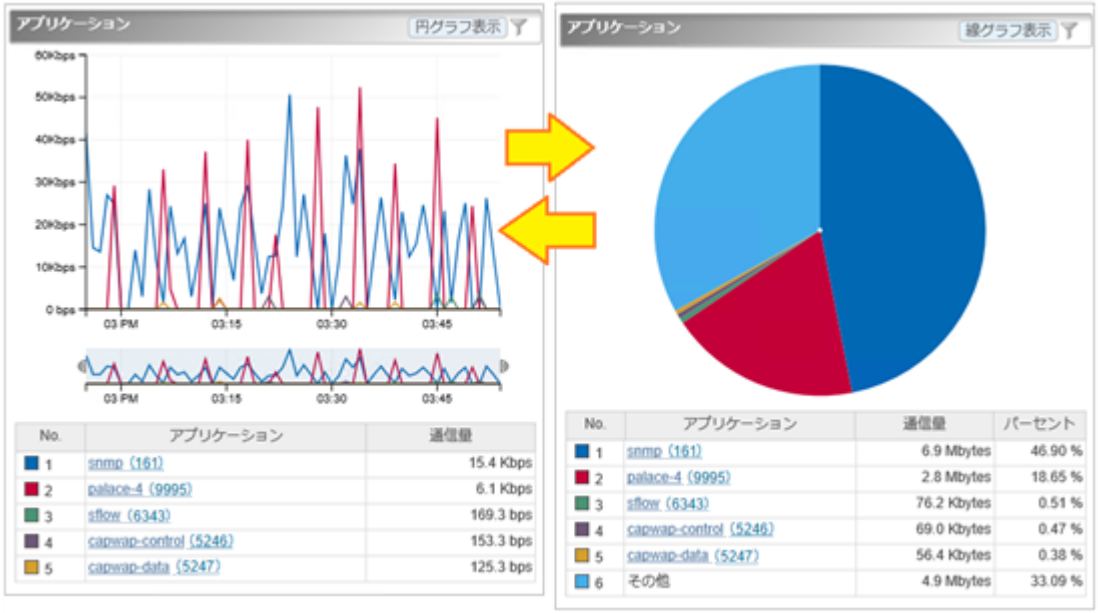

図 4-3　円グラフ/折れ線グラフ表示タイプのウィジェット

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（58 ページ）」に示します。

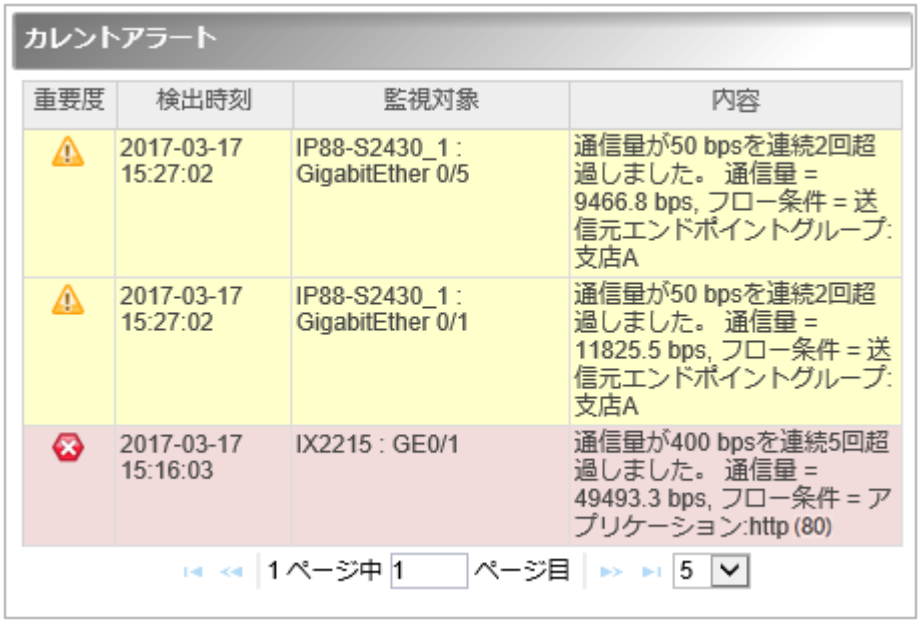

図 4-4　一覧表示タイプのウィジェット

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=「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。

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。

   ⚠ 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 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

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 を古いバージョンから最新バージョンへ(アップグレード)します。

1. インストールメディアの ISO イメージをマウントします。

   ここでは、インストールメディア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. インストーラーを起動します。

   インストール先の OS に合わせて、以下のコマンドを実行します。

   - Red Hat Enterprise Linux 9 (x86_64)

```
# /media/NFA/Linux/nfa-upgrade-rhel9
```

   - Red Hat Enterprise Linux 8 (x86_64)

```
# /media/NFA/Linux/nfa-upgrade-rhel8
```

⚠ 注意

インストール先の OS に対応していないコマンドを実行した場合は、アップグレード処理が失敗するため注意してください。

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、アップグレード処理を開始します。n を入力すると、アップグレード処理は中止されます。

```
Network Flow Analyzer version 3.2.0-6 Upgrade Installer

----- Confirmation ---------------------
Controller : 3.1.0-8  -> [ 3.2.0-6 ]
Collector  : 3.1.0-8  -> [ 3.2.0-6 ]
----------------------------------------

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

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（77 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
```

ヒント

アップグレード後に、IMS コンポーネントとの接続設定を追加することもできます。設定方法は「2.8　IMS コンポーネント利用のための設定を行う（34 ページ）」を参照してください。

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

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　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.2.1　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-1 コマンドパラメーター（73 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-1　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-2 置換文字列（74 ページ）」に示します。

例:

```
syslog_message = High disk usage. The disk usage been {disk_usage}%.
```

表 A-2　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.2.2　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

ヒント

本コマンドは、インストールメディアにも収録しています。インストール処理でエラーが発生した場合は、インストールメディア内のコマンド類をコピーして配置し、nfatech.sh コマンド、または、nfatech_minimal.sh コマンドを用いてログを採取してください。

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 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 *XXX*MB 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（22 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（22 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 3.2
スタートアップガイド

NFA0LSJ0320-01

2023 年 10 月 01 版 発行

日本電気株式会社