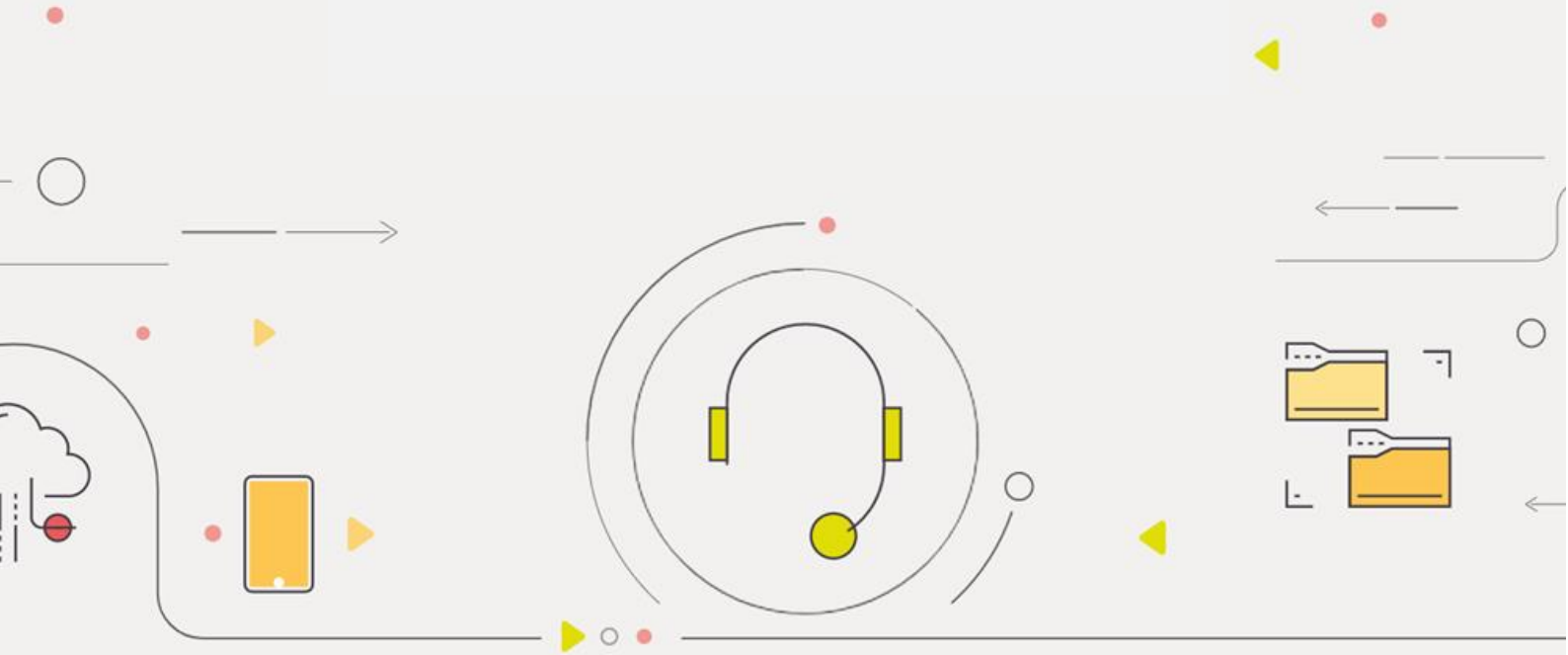
ZJTP20227201202

ManageEngine NetFlow Analyzer



スタートアップガイド

■著作権について
本ガイドの著作権は、ゾーホージャパン株式会社が所有しています。

■注意事項
本ガイドの内容は、改良のため、予告なく変更することがあります。
ゾーホージャパン株式会社は本ガイドに関しての一切の責任を負いかねます。
当社はこのガイドを使用することにより引き起こされた偶発的もしくは間接的な損害についても責任を負いかねます。

■商標一覧
文中の社名、商品名等は各社の商標または登録商標である場合があります。
Windows は、米国およびその他の国における米国 Microsoft Corp.の登録商標です。
ManageEngine は、ZOHO Corporation Pvt.Ltd 社の登録商標です。
なお、本ガイドでは、(R)、TM 表記を省略しています。

目次

1　はじめに

1.1　NetFlow Analyzer について

ManageEngine NetFlow Analyzer は Web UI を備えたトラフィック解析ツールです。
NetFlow、sFlow、NetStream、J-Flow、IPFIX、AppFlow、cflow などが生成、出力するフローデータを受信し解析することで、詳細なトラフィック情報を表示します。
フローデータには、監視対象インターフェースを通過するネットワークトラフィックの詳細情報が含まれます。
NetFlow Analyzer はこの情報を処理して、監視対象のネットワーク装置を通過するパケットの IP アドレスやアプリケーション、ポートなどの送信元/宛先情報を表示します。
オンデマンド、もしくはスケジュール生成が可能なレポート機能も豊富に搭載しており、定量的な根拠に基づいたトラフィック情報の分析や帯域のキャパシティプランニングにもご活用いただけます。

1.2　本スタートアップガイドについて

- 本ガイドは NetFlow Analyzer Professional Edition ビルド 12.7.124 の基本的な使い方について記載しています。Enterprise Edition については記載していません。
  Enterprise Edition の概要は、以下のページをご参照ください。
  https://www.manageengine.jp/products/NetFlow_Analyzer/Enterprise-Edition.html
- フローデータを NFA に送信するために必要な、ネットワーク装置のコンフィグ設定については記載しておりません。
- NetFlow Analyzer Professional Edition を以降、NFA と表記します。
- 本製品をインストールしたホームディレクトリを［NFA_HOME］と表記します。
  ※デフォルトのホームディレクトリは次の通りです。
  Windows：C:¥Program Files¥ManageEngine¥OpManager
  Linux：/opt/ManageEngine/OpManager
- NetFlow、sFlow などのデータをフローデータと表記します。
- インターフェースを IF と表記します。

1.3　本ガイドの目的と対象読者

本ガイドは、NFA を購入された方やこれから評価版を使用される方が、本製品の概要を手早く理解し、ご利用を開始するまでの学習時間を短縮することを目的としています。

2　事前準備

2.1　サポート対象装置の確認

監視対象とするネットワーク装置は、フロープロトコルに対応している必要があります。NFA の対応フローデータは次の通りです。

NetFlow	sFlow 他
NetFlow（v5,v7,v9）, NetFlow-Lite（受信側のみ）,Flexible NetFlow	sFlow（v2,v4,v5）, NBAR, CBQoS, J-Flow, IPFIX, AppFlow, cflow, NetStream, rflow

以下のリンクからフロープロトコル対応装置の参考情報をご案内しておりますが、フロープロトコル対応状況は装置ベンダーやメーカー、管理者様へご確認いただくようお願いいたします。
https://www.manageengine.jp/products/NetFlow_Analyzer/supported-devices.html

フロープロトコル非対応装置については、NetFlow Generator を用いた監視が可能です。NetFlow Generator の詳細は、以下のページをご参照ください。
https://www.manageengine.jp/products/NetFlow_Analyzer/help/nps.html

2.2　保持データの理解

NFA は 3 種類のデータ（ローデータ、履歴データ、トラフィックデータ）を保持します。

	ローデータ	履歴データ	トラフィックデータ
概要	・監視対象装置から受信したほぼそのままのフローデータ ・アプリケーションやポート情報を含むトラフィック情報を 1 分間粒度で保持	・時間経過とともにローデータを平均化かつ圧縮した軽量データ ・時間経過とともに表示時間粒度が増加 ・トラフィックの傾向把握やトップ通信の詳細分析が可能	・1 分毎のトラフィック情報（容量、速度、帯域使用率、パケット数）を保持する軽量データ ・ローデータを保持していない期間でも、トラフィック情報を 1 分間粒度表示
表示時間粒度	1 分間	10 分間 1 時間 6 時間 24 時間 1 週間	1 分間
保持期間	デフォルトで最長 1 週間	無期限	最長 1 年間
保持データ	送信元 IP 宛先 IP 送信元ポート 宛先ポート アプリケーション DSCP プロトコル ToS TCP フラッグ ネクストホップ AS パケット数 容量 NBAR2（対応装置から受信している場合）	送信元 IP 宛先 IP 送信元ポート アプリケーション DSCP プロトコル ToS パケット数 容量 NBAR2（対応装置から受信している場合）	パケット数 容量

※ローデータの長期保存を最長 6 か月間にする「高性能レポートエンジン（HighPerf）オプション」の詳細は、以下のページをご参照ください。
https://www.manageengine.jp/products/NetFlow_Analyzer/help/high-perf.html
※保持データの詳細は、以下のページをご参照ください。
https://www.manageengine.jp/support/kb/NetFlow_Analyzer/?p=983
※NFA が受信したフローデータは暗号化されデータベース内に格納されるため、外部への出力ができない仕様です。
※フローデータを受信することでのみ、データを取り込むことが可能です。それ以外の方法で外部データをデータベースに取り込むことはできません。

本ガイドを読み進めるにあたり、ポイントとなる内容は以下の通りです。
「1 週間以内の厳密な調査と監視には、受信したフローデータ情報をほぼそのまま保持しているローデータのご利用を推奨します。一方、ローデータは多くの HDD 容量を必要とします。そのため長期間の調査と監視には、必要十分なデータを期間幅軸で平均化（10 分～1 週間）して表示する、軽量な履歴データ（無期限の保持が可能）のご利用を推奨します。履歴データの平均化対象には、送信元/宛先 IP やアプリケーション、ポートやプロトコル情報などが含まれますが、トラフィックの容量、速度、帯域使用率、パケット数情報は、軽量なトラフィックデータ（1 年間の保持が可能）を用いた 1 分間粒度での表示が可能です。ローデータを保持しない環境でも、履歴データとトラフィックデータを用いて、トラフィックを十分に監視いただけます。
なおシステム要件の算出には、ローデータの保持期間を考慮する必要があります。ローデータは 3 日~1 週間分保持されることが多いです。」

2.3 「運用設計上の注意点」の確認

NFA インストールサーバーのシステム要件は、ローデータの保持期間とフローレート（受信フローデータ数/秒）を基に確定することが可能です。
フローレートは、インストールした NFA に監視対象を追加した後、確認が可能となります。また NFA 運用後もフローレート値は変動します。
その為、NFA インストールサーバーのスペック（HDD 容量、CPU（コア数と GHz 数）、メモリー（GB））について、今後拡張する必要が出てくる可能性がある旨をあらかじめご留意ください。
NFA 運用後も、システム要件の準拠状況を定期的にご確認ください。
システム要件の算出方法は「5.5 システム要件の確定と見直し」をご確認ください。

NFA インストールサーバーは、NFA 専用のサーバーをご用意ください。
アンチウィルスソフトやデータバックアップツールをインストールしている場合は、NFA インストールフォルダーを必ずスキャン対象またはバックアップ対象から除外してください。
上記以外の「運用設計上の注意点」は以下のリンクからご案内をしております。必ずご確認ください。
https://www.manageengine.jp/products/NetFlow_Analyzer/operational-design.html

2.4　システム要件の確認

ローデータの保持期間を 1 週間、と想定した場合の最小システム要件は次の通りです。
CPU：2.4 GHz Quad Core Processor（GHz が 2.4 以上、コア数が 4 以上）
メモリー：4GB
HDD 空き容量：925GB（製品起動用 200GB+履歴データ用 200GB+ローデータ用 525GB）
以降、「5.5 システム要件の確定と見直し」で算出されるスペックと差分がある場合、増強対応をお願いいたします。

その他、サポート OS、サポート Web ブラウザー、ポート要件は以下の通りです。

サポート OS	Windows Server 2022 Windows Server 2019 Windows Server 2016 Ubuntu Server 14～22.04 LTS Red Hat Enterprise Linux 7～9.1 CentOS Stream 9 CentOS 7
サポート Web ブラウザー	Google Chrome（推奨/最新版） Mozilla Firefox（最新版） Microsoft Edge（最新版）

用途	デフォルトのポート番号	プロトコル	説明	方向
Web サーバーポート（HTTP）	8060	TCP	Web ブラウザーから NFA サーバーへの接続時に使用される Web ポート	受信
Web サーバーポート（HTTPS）	8061	TCP	Web ブラウザーから NFA サーバーへの接続時に使用される Web ポート（HTTPS）	受信

フローデータ待ち受けポート	9996	UDP	ネットワーク装置から送付されるフローデータを受信するリスニングポート	受信
DB ポート	13306	TCP	NFA がデフォルトでバンドルする PostgreSQL データベースへの接続時に使用されるポート	送受信
MSSQL	1433	TCP	Microsoft SQL データベースに接続する際に使用されるポート	-
SNMP	161	UDP	ネットワーク装置情報を取得や、SNMP ベースの NBAR を設定時に使用されるポート	送受信
Wrapper ポート	32000～32999	TCP	-	送受信
JVM	31000～31999	TCP	Wrapper への接続時に使用されるポート	送受信

上記以外の「システム要件」は以下のリンクからご案内をしております。必ずご確認ください。
https://www.manageengine.jp/products/NetFlow_Analyzer/system-requirements.html

2.5　インストーラーの取得

Windows または Linux 用のインストーラーは、以下のリンク先からダウンロードしてください。
https://www.manageengine.jp/products/NetFlow_Analyzer/download.html

インストール後 30 日間は、評価版としてすべての機能を使用できます。30 日の評価期間が終了後、正規ライセンスを適用しない場合、自動的に無料版にダウングレードします（管理可能 IF 数：2IF）。

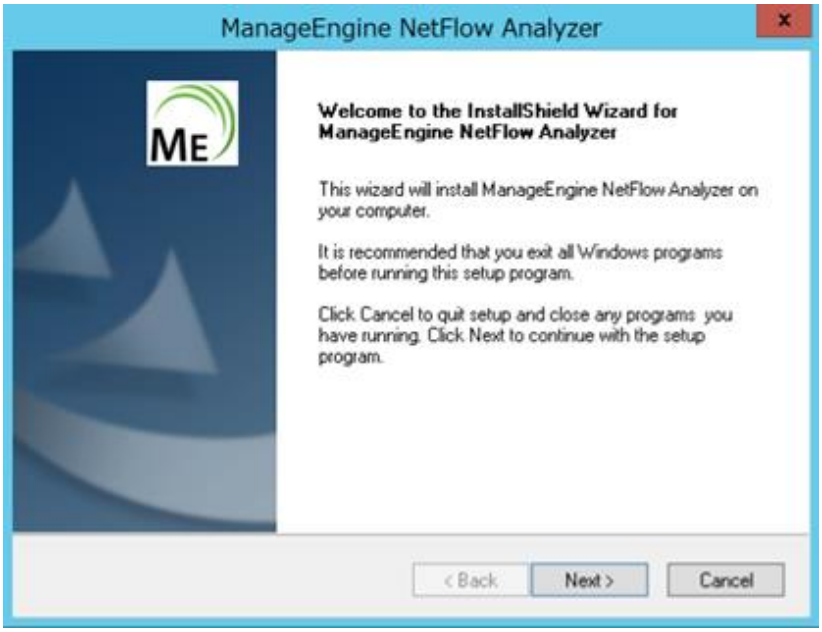
3　インストール/アンインストールと起動/停止

3.1　インストール手順 - Windows

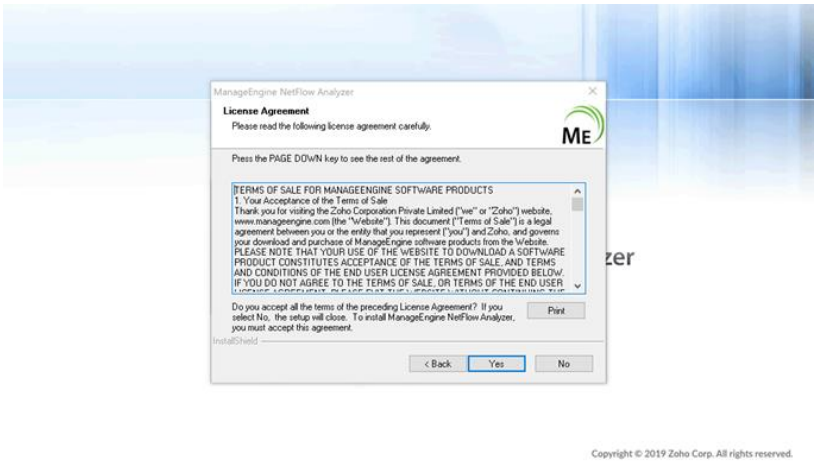
1. インストーラーファイル「ManageEngine_NetFlowAnalyzer_64bit.exe」を、インストールサーバーに配置

2. インストーラーを管理者権限で実行後、ウィザード形式によりインストールを実施

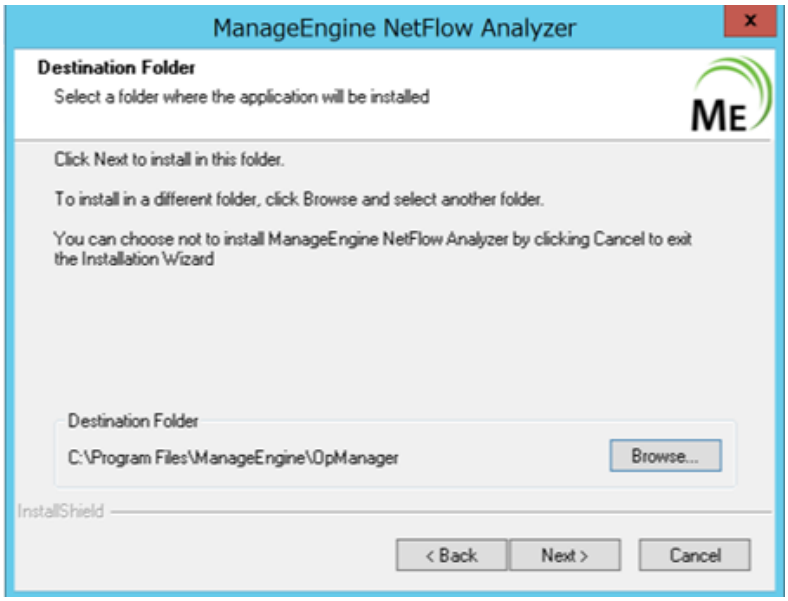
3. ［Next］をクリック



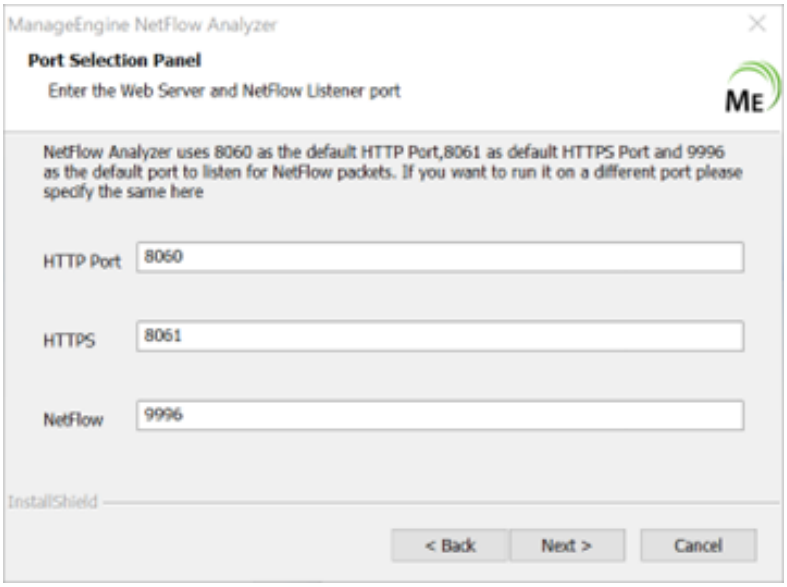
4. License Agreement（ライセンス条項）に承諾後、［Yes］をクリック



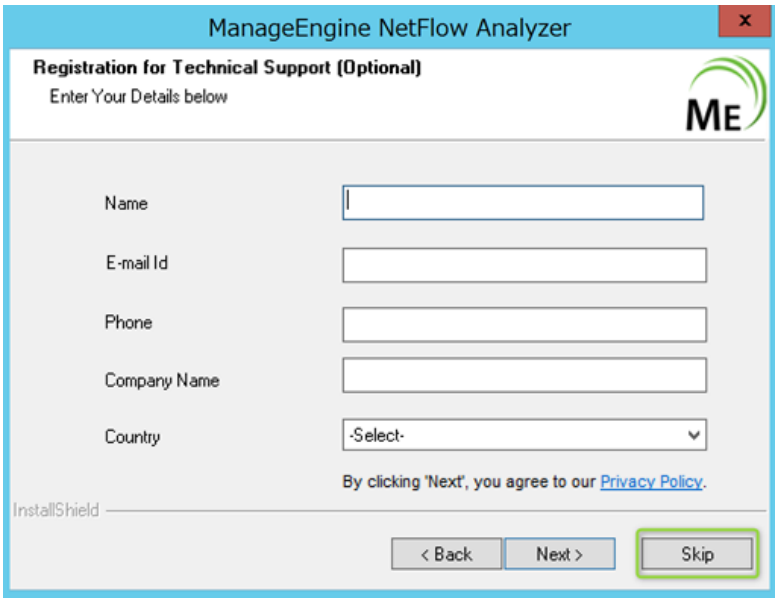
5. インストールディレクトリを選択し、［Next］をクリック
※デフォルトは C:¥Program Files¥ManageEngine¥OpManager



6. Web サーバーのポート番号を指定し、［Next］をクリック
※希望のポートを指定可能
※ブラウザー用 HTTP ポートと HTTPS ポート、そしてフローデータ待ち受けポートのデフォルト値はそれぞれ 8060、8061、9996
※ポート情報は、NFA ログイン後［設定］→［一般設定］→［サーバー設定］から再設定が可能

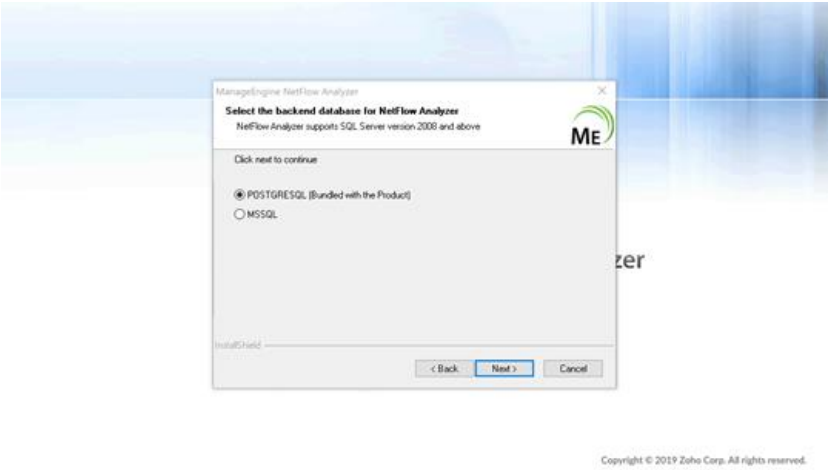


7. ［Skip］をクリックし、テクニカルサポート情報の入力をスキップ

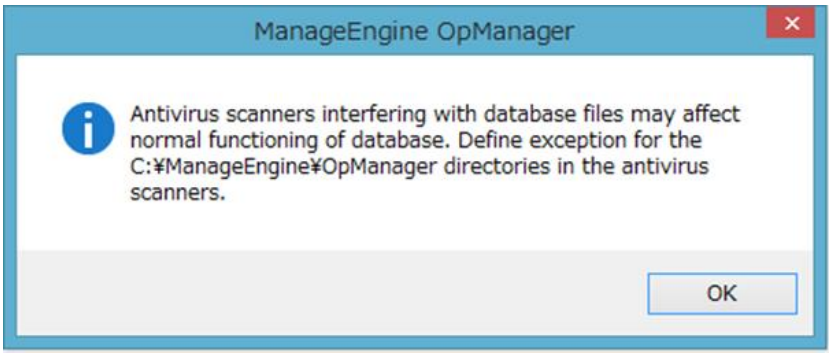


8. インストールが終了するまで待機

9. 使用するデータベースを選択し、［Next］をクリック
※NFA には PostgreSQL がバンドルされています。
※MS SQL を選択する場合、お客様の方で別途ご用意してください。

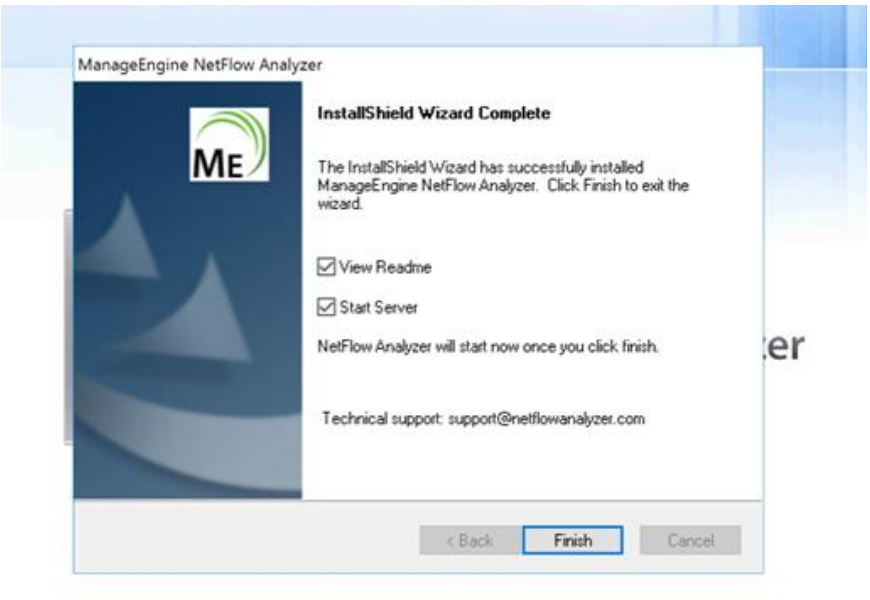


10. 内容を確認し［OK］をクリック
※アンチウィルスソフトやバックアップソフトを使用している場合、データベースの動作に影響を及ぼす可能性がありますので、［NFA_HOME］をアンチウィルスソフトやバックアップソフトの対象から除外してください。



11. ［InstallShield Wizard Complete］の表示を確認

［Start Server］にチェックを入れた状態で［Finish］をクリックすると、サービスとして NFA が起動します。



3.2　インストール手順 - Linux

1. インストーラーファイル「ManageEngine_NetFlowAnalyzer_64bit.bin」を、インストールサーバーに配置

2. ManageEngine_NetFlowAnalyzer_64bit.bin に実行権限を付与

```
[root@centos-tmpl ~]# cd /home/
[root@centos-tmpl home]# ls
ManageEngine_NetFlowAnalyzer_64bit.bin
[root@centos-tmpl home]# chmod 777 ManageEngine_NetFlowAnalyzer_64bit.bin
[root@centos-tmpl home]# ls
ManageEngine_NetFlowAnalyzer_64bit.bin
[root@centos-tmpl home]#
```

3. ManageEngine_NetFlowAnalyzer_64bit.bin を管理者（root）権限で実行

```
[root@centos-tmpl home]# ./ManageEngine_NetFlowAnalyzer_64bit.bin
Preparing to install...
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...

Launching installer...
```

4. Enter を押しながら Introduction と License Agreement（ライセンス条項）を確認

```
===============================================================================
Introduction
------------

Welcome to the InstallShield Wizard for ManageEngine NetFlowAnalyzer


NetFlow Analyzer uses Cisco NetFlow, sFlow, J-Flow etc. to provide valuable
information on what applications are using bandwidth, who is using them, and
where traffic is headed in the network.
Such information is useful for network analysis,troubleshooting, network
auditing, usage-based billing, and more.

For help on installation, refer to
https://www.manageengine.com/products/netflow/help/installing-and-starting.
html

The InstallShield Wizard will install ManageEngine NetFlowAnalyzer on your
computer. To continue, click Next

PRESS <ENTER> TO CONTINUE:
```

5. License Agreement（ライセンス条項）に承諾後 y を入力

```
PRESS <ENTER> TO CONTINUE:

California between California residents. If you are a resident of any other
country, this Agreement shall be governed by and interpreted in all respects
by the laws of the Republic of India without reference to conflict of laws'
principles, as such laws are applied to agreements entered into and to be
performed entirely within the Republic of India between residents of the
Republic of India. If you are a resident of the United States or Canada, you
agree to submit to the personal jurisdiction of the courts in the Northern
District of California. If you are a resident of any other country, you agree
to submit to the personal jurisdiction of the courts in Chennai, India. This
Agreement constitutes the entire agreement between the parties, and supersedes
all prior communications, understandings or agreements between the parties.
Any waiver or modification of this Agreement shall only be effective if it is
in writing and signed by both parties hereto. If any part of this Agreement is
found invalid or unenforceable, the remainder shall be interpreted so as to
reasonable effect the intention of the parties. You shall not export the
Licensed Software or your application containing the Licensed Software except
in compliance with United States export regulations and applicable laws and
regulations.



DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N): y
```

6. n を入力しテクニカルサポートの入力をスキップ

```
================================================================================
ManageEngine NetFlowAnalyzer
----------------------------



Do you want to register for technical support?(Y/N) (Default: Y): n
```

7. インストールパスを確認し Enter

※パスを入力することでインストール先を変更可能

※デフォルトは/opt/ManageEngine/OpManager

```
================================================================================
Choose Install Folder
---------------------

Space recommended on drive : 10GB

  Default Install Folder: /opt/ManageEngine/OpManager

ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
      :
```

8. Web サーバーHTTP ポートと HTTPS ポートを確認し Enter を入力
   ※希望のポートを指定可能
   ※ブラウザー用 HTTP ポートと HTTPS ポートのデフォルト値はそれぞれ 8060、8061
   ※ポート情報は、NFA ログイン後［設定］→［一般設定］→［サーバー設定］から再設定が可能

```
================================================================================
Webserver port
---------------

Enter requested information

Enter the HTTP Port Number (Default: 8060):




================================================================================
Secure server port
------------------

Enter requested information

Enter the HTTPS Port Number (Default: 8061):
```

9. NetFlow 待ち受け（リッスン）ポートを確認し Enter
   ※NetFlow 待ち受けポートを指定可能
   ※ポート情報は、NFA ログイン後［設定］→［一般設定］→［サーバー設定］から再設定が可能

```
================================================================================
NetFlow Listener Port
---------------------

Enter requested information

Enter the NetFlow Listener Port  (Default: 9996):
```

10. インストール状況を確認し Enter

```
================================================================================
Pre-Installation Summary
------------------------

Please review the following before continuing:

Product Name:
    ManageEngine NetFlowAnalyzer

Install Folder:
    /opt/ManageEngine/OpManager

Disk Space Information (for Installation Target):
    Required:  656.38 MegaBytes
    Available: 144,202.74 MegaBytes

PRESS <ENTER> TO CONTINUE:
```

11. インストールの完了を確認

```
================================================================================
Installation Completed
----------------------

Congratulations! ManageEngine NetFlowAnalyzer has been successfully installed
to:

/opt/ManageEngine/OpManager

Readme file is available at /opt/ManageEngine/OpManager/README.html


Technical support :  support@netflowanalyzer.com
```

3.3　アンインストール - Windows

1. NFA を停止後、Windows サーバーの［コントロールパネル］→［プログラムと機能］を表示

2. 「ManageEngine NetFlow Analyzer」を選択し、アンインストールを実行

3. アンインストール処理が完了後、インストールフォルダー「ManageEngine」を削除
   ※インストールフォルダーを削除できない場合には、タスクマネージャーから関連プロセスを停止させた後、削除してください。

3.4　アンインストール - Linux

1. NFA を停止

2. インストールディレクトリ「ManageEngine」を削除

3.5　起動と停止に関する注意事項

1. 定期点検やメンテナンス等により、サーバーを再起動する場合、事前に NFA を停止した上で実施するようお願いします。

2. NFA を停止していない状態で突発的にサーバーが停止すると、製品データベースが破損する可能性があります。

3. サービス起動を実施した場合にはサービス停止を、バッチ起動を実施した場合にはバッチ停止を、いずれかの対応をお願いします。

3.6　起動手順 - Windows

サービス起動（推奨）

1. Windows の［コントロールパネル］→［管理ツール］→［サービス］を選択
   ※［管理ツール］が見つからない場合は、service.msc より［サービス］を起動してください。

2. サービス一覧に「ManageEngine OpManager」が存在することを確認

3. サービス「ManageEngine OpManager」を選択し、「サービスの開始」をクリック
   ※しばらくして WebUI にアクセスできるようになります。

バッチ起動

1. コマンドプロンプトを管理者権限で起動

2. ［NFA_HOME］ /bin フォルダーに移動

3. run.bat を実行
   起動が開始すると、NFA のモジュール起動状態が表示されます。
   すべてのモジュールが起動すると、以下のメッセージが表示されます。
   Server started in :: ［58338 ms］
   Connect to: ［http://localhost:ポート番号］

3.7　起動手順 - Linux

サービス起動（推奨）

1. root 権限でインストールサーバーにログイン

2. ［NFA_HOME］/bin ディレクトリに移動
   ［root@centos］# cd /opt/ManageEngine/OpManager/bin/

3. linkAsService.sh コマンドを実行
   ［root@centos bin］# sh linkAsService.sh

4. systemctl start OpManager.service コマンドを実行
   ［root@centos bin］# systemctl start OpManager.service

シェル起動

1. ［NFA_HOME］ /bin ディレクトリに移動

2. run.sh を root 権限で実行

NFA を起動したシェルターミナルを閉じた場合、NFA が停止します。
ターミナルへの定常ログインが難しい場合は、サービスを介した起動/停止を推奨します。

3.8 停止手順 - Windows

サービス停止

1. Windows の［コントロールパネル］→［管理ツール］→［サービス］を選択
   ※管理ツールが見つからない場合は、service.msc より［サービス］を起動してください。

2. サービス一覧に「ManageEngine OpManager」が存在することを確認

3. サービス「ManageEngine OpManager」を選択し、「サービスの停止」をクリック
   ※停止後、タスクマネージャーで以下のプロセスが残存していないことを確認してください。
   ・java.exe
   ・wrapper.exe
   ・postgres.exe
   ・NetFlowAnalyzerTrayIcon / OpManagerTrayIcon

バッチ停止

1. コマンドプロンプトを管理者権限で起動

2. ［NFA_HOME］/bin ディレクトリに移動

3. 以下 2 つのコマンドを順に実行
   shutdown.bat
   stopPgSQL.bat
   ※停止後、タスクマネージャーで以下のプロセスが残存していないことを確認してください。
   ・java.exe
   ・wrapper.exe
   ・postgres.exe
   ・NetFlowAnalyzerTrayIcon / OpManagerTrayIcon

4. 手順 4.を実施後、プロセスが残存する場合、プロセス詳細から手動で強制終了（kill）

3.9 停止手順 - Linux

サービス停止

1. 管理者権限（root）で、インストールサーバーにアクセス

2. 以下のコマンドを実行
   systemctl stop OpManager.service

   ※停止後のステータスは、以下のコマンドでステータスをご参照いただけます。
   systemctl status OpManager.service

シェル停止

1. 管理者権限（root）で、インストールサーバーにアクセス

2. ［NFA_HOME］/bin ディレクトリに移動

3. 以下 2 つのコマンドを順に実行
   ./shutdown.sh
   ./stopPgSQL.sh

   ※停止後のステータスは、以下のコマンドでステータスをご参照いただけます。
   systemctl status OpManager.service

4　ログインと初期設定

4.1　ログイン

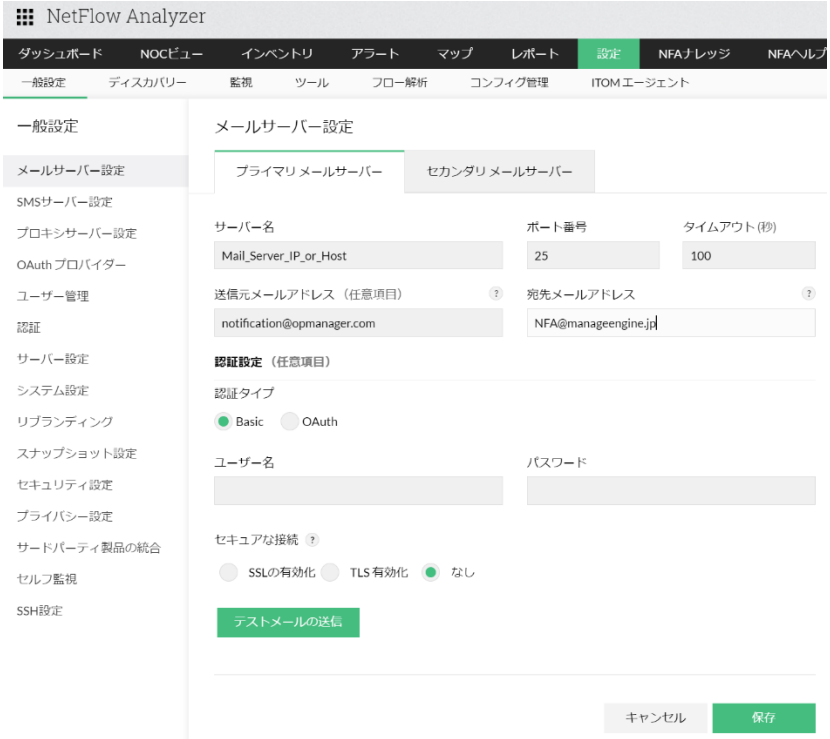
1. Webクライアントへのアクセス
   「2.4 システム要件の確認」に記載のブラウザーを開き、以下のURLでアクセス
   http://<ホスト名/サーバーIPアドレスまたはlocalhost>:<ポート番号>
   もしくはhttps://<ホスト名/サーバーIPアドレスまたはlocalhost>:<ポート番号>

2. NFA へのログイン
   ログイン画面の表示を確認後、ユーザー名/パスワードを入力
   ※ユーザー名/パスワードの初期値は admin/admin

4.2　初期設定

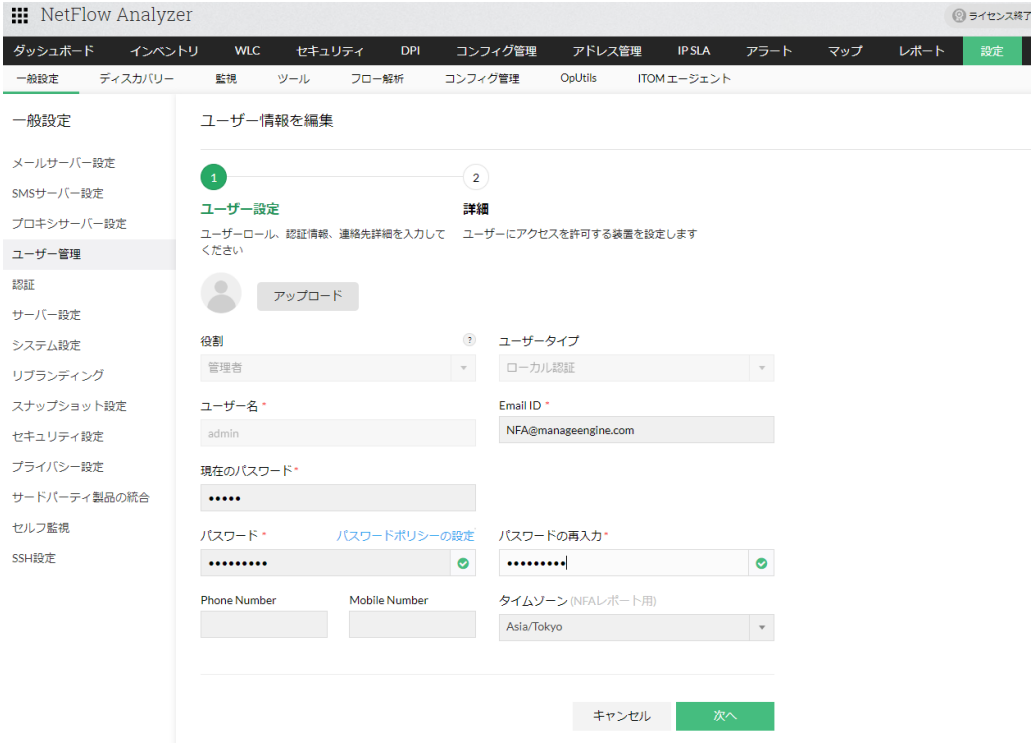
1. 初回のみ表示されるガイド（はじめに：3 手順）を閉じる

2. メールサーバーを設定
   ［設定］→［一般設定］→［メールサーバー設定］で、各項目を入力し［保存］をクリック



3. admin ユーザー情報を更新

［設定］→［一般設定］→［ユーザー管理］→［ユーザー］タブ で、［admin］をクリックし、メールアドレスとパスワードを更新

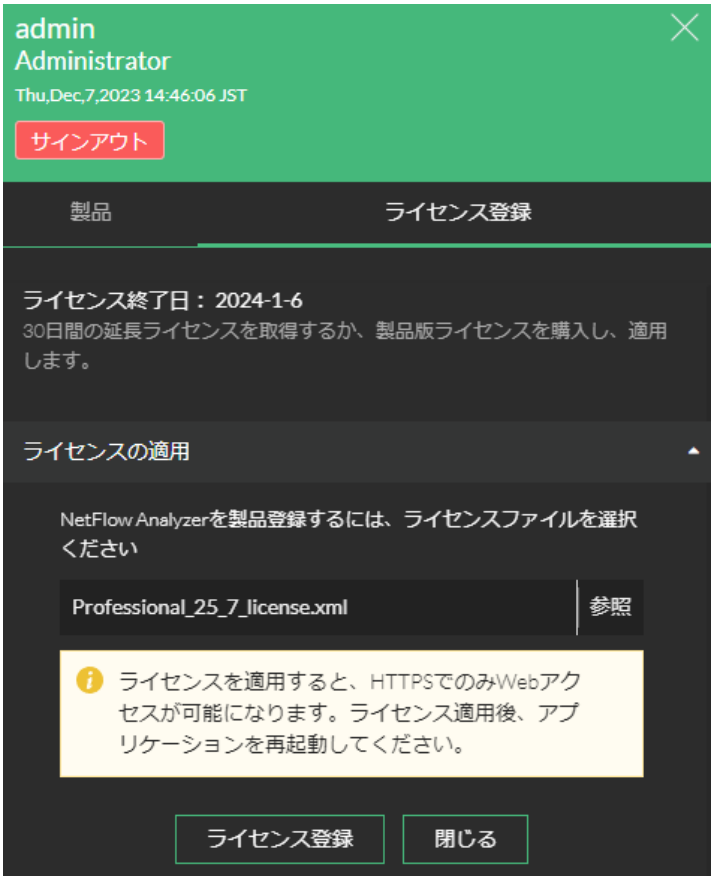


4. ライセンス適用（保守ユーザー向け）

NFA をご契約したユーザー様には、当社ライセンス担当よりご契約内容に応じたライセンスファイル（.xml）をご提供します。

ライセンファイルを受領後、以下の手順でライセンス適用を行います。

1. NFA にログイン後、画面右上のシルエットアイコンをクリック
2. ［ライセンス登録］タブをクリックし、［参照］で、適用するライセンスファイルを選択
3. ［ライセンス登録］をクリック



メッセージ「ライセンスファイルを適用しました」の表示を確認し、［製品］タブでご契約情報（ライセンスタイプ、会社名、インターフェースの最大数、有効期限等）を確認してください。

※ライセンスファイル適用時の挙動について、以下のページをご参照ください。

https://www.manageengine.jp/products/NetFlow_Analyzer/help/licensing.html#beh

※ご契約内容およびライセンス発行に関するご不明点は、当社ライセンス担当窓口までご連絡をお願いします。

ライセンス担当窓口：jp-license@zohocorp.com

5. 機能の表示設定 1

画面右上の［設定（歯車）アイコン］→［表示するモジュール］で、［コンフィグ管理］［アドレス管理］のチェックを外して［保存］をクリック

※［パケット解析］は Network Packet Sensor を介したオプション機能です。
　詳細について、以下のページをご参照ください。

https://www.manageengine.jp/products/NetFlow_Analyzer/help/nps.html

6. 機能の表示設定 2

［設定］→［一般設定］→［システム設定］→［ベンチマーク］で、［リモートデスク

トップ/ターミナル］を［無効］と選択し［保存］をクリック

7. 機能の表示設定 3
［設定］→［一般設定］→［システム設定］→［クライアント設定］で、［製品プロモーション］［製品アシストのお知らせ］［チャットサポート］［他の製品のおすすめ］を［無効］化、さらに［デフォルトダッシュボードからウィジェットを追加 / 削除できるようにする］［DB クエリ］を［有効］と選択し［保存］をクリック

8. NFA を運用するうえでのセキュリティベストプラクティスを確認
※セキュリティベストプラクティスについて、以下をご参照ください。
https://www.manageengine.jp/products/NetFlow_Analyzer/help/security_best_practices.html

9. NFA へのログインアカウントを作成
［設定］→［一般設定］→［ユーザー管理］→［ユーザー追加］で、NFA へのログインユーザーアカウントを作成
※権限の詳細やロール作成について、以下のページをご参照ください。
https://www.manageengine.jp/products/NetFlow_Analyzer/help/user-management-settings.html
※標準のアカウント数は、デフォルトの admin ユーザーを含めて 2 ユーザーまでです。
それ以上の追加は、追加 X ユーザーオプションが必要です。
https://www.manageengine.jp/products/NetFlow_Analyzer/help/options.html

10. NFA インストールサーバーのセルフ監視
［設定］→［一般設定］→［セルフ設定］で監視頻度としきい値を設定し、NFA インストールサーバーのパフォーマンス通知を有効化

5　装置の追加と設定

5.1　装置の追加

NFA は、フローデータを受信した際にフローデータを送付する装置と IF を登録し、監視を自動的に開始します。
装置からフローデータを送付するには、装置に直接ログインいただきベンダー様やメーカー様が提供するフロープロトコルを有効化する推奨コンフィグを設定してください。
以下、留意事項です。

- ［インベントリ］→［装置］→［装置追加］、［インベントリ］→［装置］→ 画面右上の［+］アイコン、さらに［設定］→［ディスカバリー］から移動する［フローのエクスポート］のご利用はお控えいただくようよろしくお願い申し上げます。

- フローデータの送付先 IP アドレスとポートは、それぞれ NFA インストールサーバー IP アドレスと NFA で設定中のリスニングポート（デフォルト値 9996）です。
  リスニングポートは、NFA ログイン後［設定］→［一般設定］→［サーバー設定］から確認/変更いただけます。

- フロープロトコルを有効化していないインターフェースが表示される場合があります。
  監視が不要なインターフェースは［設定］→［フロー解析］→［ライセンス管理］から管理対象外に設定してください。
  ※事象の詳細について、以下のページをご参照ください。
  https://www.manageengine.jp/support/kb/NetFlow_Analyzer/?p=2698

- インターフェース ifindex-1 が表示される場合があります。3.と同様に管理対象外に設定してください。
  ※事象の詳細について、以下のページをご参照ください。.
  https://www.manageengine.jp/support/kb/NetFlow_Analyzer/?p=4278

- フロープロトコル非対応装置も、NetFlow Generator を用いて監視が可能です。
  ※NetFlow Generator の詳細について、以下のページをご参照ください。
  https://www.manageengine.jp/products/NetFlow_Analyzer/help/nps.html

- フロープロトコルを有効化していないインターフェースが表示される場合があります。
  ※事象の詳細について以下のページをご参照ください。
  https://www.manageengine.jp/support/kb/NetFlow_Analyzer/?p=2434

5.2 SNMP を介した監視対象装置/インターフェース情報の取得

監視対象の装置/IF 名と速度値情報を SNMP で取得可能な場合、以下の手順で NFA 上に反映させることが可能です。

1. ［設定］→［ディスカバリー］→［認証設定］→［認証情報の追加］に移動

2. 装置の SNMP 情報を入力し［保存］をクリック

3. ［インベントリ］→［装置］に移動

4. 該当装置名左のボックスをチェック → 画面右上の［・・・］→［SNMP 認証情報の関連付け］に移動

5. 手順 1.と 2.で作成した装置の SNMP 認証を選択 →［テストと関連付け］をクリック後
任意の［インターフェース名タイプ］を選択し、［保存］をクリック

5.3　監視対象装置/インターフェース情報の手動更新

監視装置の装置/IF 名と速度値を SNMP で取得できない場合、手動で設定することが可能です。

装置名の手動更新

1.　［インベントリ］→［装置］に移動

2.　該当装置名左のボックスをチェック → 画面右上の［・・・］→［装置編集］に移動

3.　［ユーザー定義名］で任意の表示名を入力し［保存］をクリック
※半角英数字と_（アンダーバー）をご利用ください。

IF 名と速度値の手動更新

1.　［インベントリ］→［インターフェース］→ 該当 IF 名をクリック→［概要］タブに移動

2.　画面右上の［編集］文字をクリック

3.　インターフェース名や帯域情報を入力
※受信/送信帯域は 1Mbps がデフォルト設定されています。使用率 100%の問題について、以下のページをご参照ください。
https://www.manageengine.jp/support/kb/NetFlow_Analyzer/?p=252

5.4 データ保持設定

データの種類については「2.2 保持データの理解」をご参照ください。
NFA で管理される主要データのお勧め保持設定をご案内します。

1. ［設定］→［フロー解析］→［ストレージ設定］に移動

2. ［ローデータ］タブで以下を設定し、［保存］をクリック
   2.1 ［ローデータ］ ＝ ［ON］
   2.2 ［ローデータ保持期間］ ＝ ［3 日］もしくは［1 週間］
   ※NFA インストールサーバースペックを考慮の上、選択してください。
   ※高性能レポートエンジンオプションをご利用いただくことで、ローデータの保持期間を 6 か月まで延長が可能です。
   2.3 ［空きディスク容量が設定値以下で古いローデータを削除］ ＝ ［30%］
   ※1 時間に 1 度、ディスクの空き容量を確認し、設定したしきい値よりも空き容量が少ない場合、しきい値を上回るまで、古いローデータが 1 時間分ずつ削除されます。
   ※NFA インストールサーバーの HDD に余裕のある場合、値を小さくしてください。
   2.4 ［最新 2 時間のレポートに集約データを使用］ ＝ ［OFF］

3. ［履歴データ］タブで以下を設定し、［保存］をクリック
   3.1 ［保持するトップレコード数］ ＝ ［300］
   3.2 ［データの保持］ ＝ ［無期限］

4. ［トラフィックデータ］タブで以下を設定し、［保存］をクリック
   4.1 ［データの保持］ ＝ ［1 年］

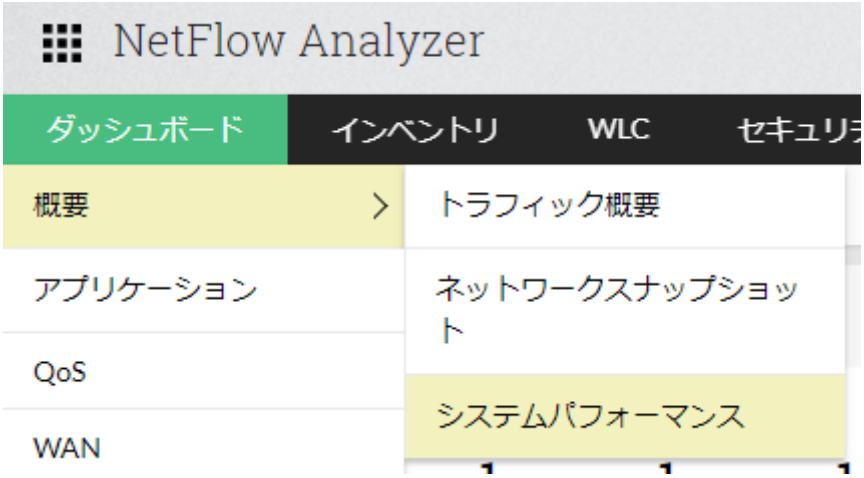
5. ［AS］タブで以下を設定し、［保存］をクリック
   5.1 ［AS データの収集］ ＝ ［IP ベース AS］
   ※フローデータの IP アドレスと IANA データベースを紐づけ AS（Autonomous System）情報を表示します。

5.5　システム要件の確定と見直し

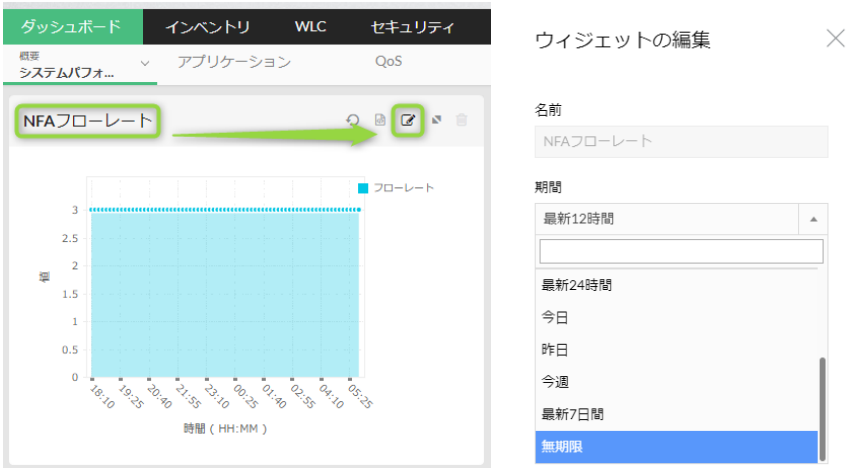
「5.1 装置の追加」と「5.4 データ保持設定」の対応後、NFA インストールサーバーのシステム要件（CPU/メモリー/HDD）を確定いただけます。
以下の算出方法をご確認の上、システム要件への準拠状況の見直し、および不足分の増強をご対応ください。

なお OS や web ブラウザー要件、ポート要件やその他注意事項は、「2.3「運用設計上の注意点」の確認」と「2.4 システム要件の確認」をご参照ください。

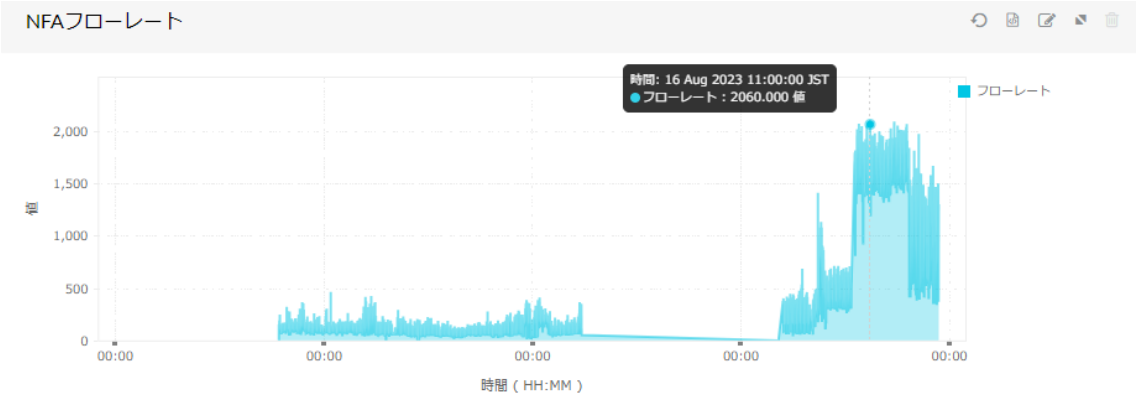
1.　［ダッシュボード］→［概要］→［システムパフォーマンス］に移動



2.　［NFA フローレート］ウィジェット内の編集アイコンをクリック →［期間］で［無期限］を選択し［保存］をクリック



3. 表示されるフローレートの瞬間最高値を確認



4. ［設定］→［フロー解析］→［ストレージ設定］→［ローデータ］タブで設定中のローデータの保持期間を確認

以降はシステム要件ホームページをご参照の上、システム要件を確定します。
※https://www.manageengine.jp/products/NetFlow_Analyzer/system-requirements.html

5. CPU の確定
以下の表からフローレートに応じた CPU（GHz とコア数）をご参照いただき、CPU 要件としてください

0～3,000	2.4 GHz Quad Core Processor 以上
3,001～6,000	3.2 GHz Quad Core Processor 以上
6,001～9,000	
9,001～10,000	
10,001～25,000	
25,001～50,000	
50,001～75,000	
75,001～100,000	

※高性能レポートエンジン（HighPerf）オプションをご利用の場合、以下が対象となります。

0～10,000	3.5 GHz 以上かつ 8 core/16 threads 以上
10,001～25,000	
25,001～50,000	
50,001～75,000	3.5 GHz 以上かつ 16 core/32 threads 以

75,001～100,000	上

6. メモリーの確定

以下の表からフローレートに応じたメモリー（GB）をご参照のうえ、メモリー要件としてください。

0～3,000	4GB
3,001～6,000	6GB
6,001～9,000	8GB
9,001～10,000	16GB
10,001～25,000	18GB 以上
25,001～50,000	20GB 以上
50,001～75,000	22GB 以上
75,001～100,000	24GB 以上

※高性能レポートエンジン（HighPerf）オプションをご利用の場合、以下が対象となります。

0～10,000	24GB
10,001～25,000	
25,001～50,000	24GB 以上
50,001～75,000	32GB 以上
75,001～100,000	

7. HDD の確定

以下 7.1、7.2、7.3 の値を合計し HDD 要件としてください。

例：7.1 が 200GB、7.2 が 225GB、7.3 が 3,500GB の場合、合計 3,925GB

7.1 製品起動&DB インストール用 HDD 空き容量は 200GB（Professional Edition）

7.2 履歴データ用 HDD 空き容量を以下の表からご参照ください。

0～3,000	200GB
3,001～6,000	
6,001～9,000	
9,001～10,000	
10,001～25,000	225GB
25,001～50,000	250GB
50,001～75,000	300GB

75,001～100,000	350GB

7.3 ローデータ用 HDD 空き容量/日を以下の表からご参照いただき、ローデータ保持日数と掛け算（×）してください。

例 1：フローレート 2,000、ローデータ保持期間 3 日の環境

75GB×3 日= 225GB

例 2：フローレート 12,000、ローデータの保持期間 2 週（14 日）、高性能レポートエンジン（HighPerf）オプション有りの環境

250GB×14 日=3,500GB

0～3,000	75GB
3,001～6,000	150GB
6,001～9,000	225GB
9,001～10,000	250GB
10,001～25,000	ローデータ保持非推奨
25,001～50,000	
50,001～75,000	
75,001～100,000	

※高性能レポートエンジン（HighPerf）オプションをご利用の場合、以下が対象となります。

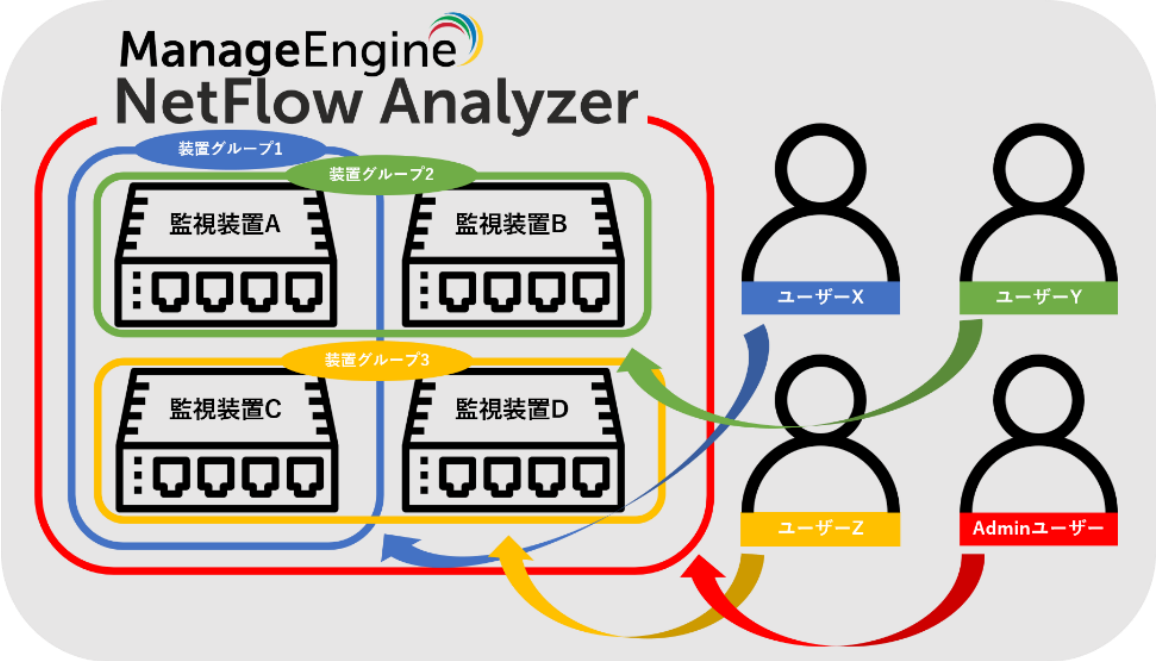
0～10,000	100GB
10,001～25,000	250GB
25,001～50,000	500GB
50,001～75,000	750GB 読み込み&書き込み速度 350MiB/秒 以上
75,001～100,000	1000GB 読み込み&書き込み速度 500MiB/秒 以上

※システム要件の算出例について、以下のページをご参照ください。

https://www.manageengine.jp/products/NetFlow_Analyzer/system-requirements.html#example

5.6 監視グループの作成 - 装置グループ

装置グループは、NFA の監視対象装置を任意にまとめたグループです。
作成した装置グループをユーザーアカウントに割り当てることで、グルーピングされた装置のトラフィック情報の閲覧権限を該当ユーザーアカウントに付与することが可能です。
admin ユーザーは、全ての監視対象装置の情報を表示することが可能です。



- グループの作成手順
  1. ［設定］→［フロー解析］→［グループ設定］→［装置グループ］に移動

  2. 画面右上の［追加］をクリック

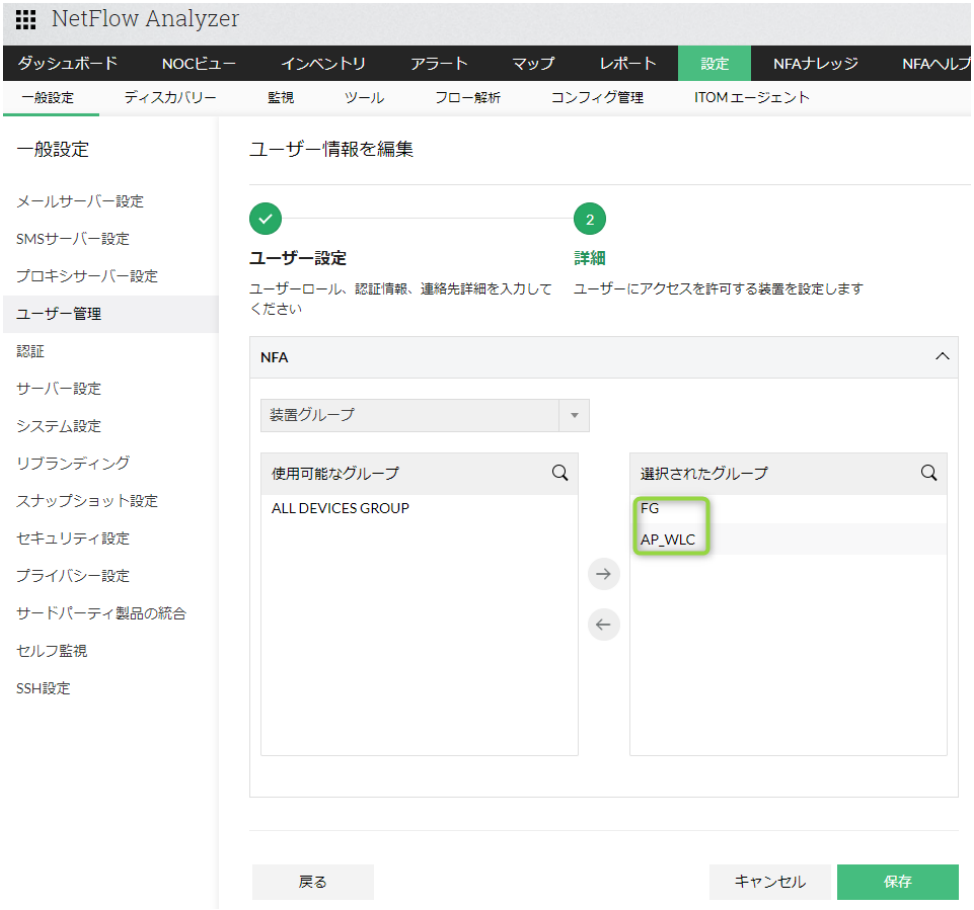
  3. 任意グループ名と説明、グループ化する装置を選択し保存
     ※グループ名に（）や※などの全角記号を利用しないでください。

- ユーザーアカウントへ装置グループを割り当てる手順
  1. admin ユーザーで NFA にログイン

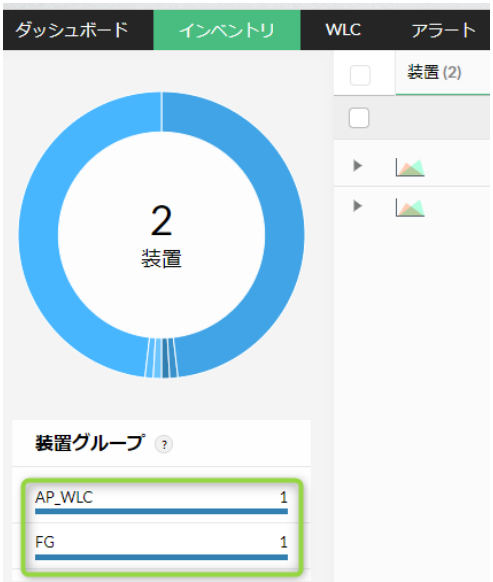
  2. ［設定］→［一般設定］→［ユーザー管理］→ 任意のユーザー名をクリック

  3. ［ユーザー設定］画面で［次へ］をクリック

4. ［詳細］画面で、割り当てる装置グループを［使用可能なグループ］から［選択されたグループ］へ移動し、［保存］をクリック



5. 該当のユーザーアカウントでログイン後、4.で選択した装置グループの装置が［インベントリ］→［装置］に表示されることを確認



5.7　監視グループの作成 - インターフェースグループ

IF グループは、監視対象インターフェースを装置横断でまとめ、監視対象とするグルーピング機能です。
まとめたインターフェース群のトラフィック情報を［インベントリ］から閲覧することが可能です。
また、作成した IF グループをユーザーアカウントに割り当てることで、該当 IF グループのトラフィック情報の閲覧権限を該当ユーザーアカウントに付与することも可能です。

- グループの作成手順
  1. ［設定］→［フロー解析］→［グループ設定］→［インターフェースグループ］に移動

  2. 画面右上の［追加］をクリック

  3. 任意グループ名と説明、グループ化する IF を選択し保存
     ※グループ名に（）や※などの全角記号を利用しないでください。

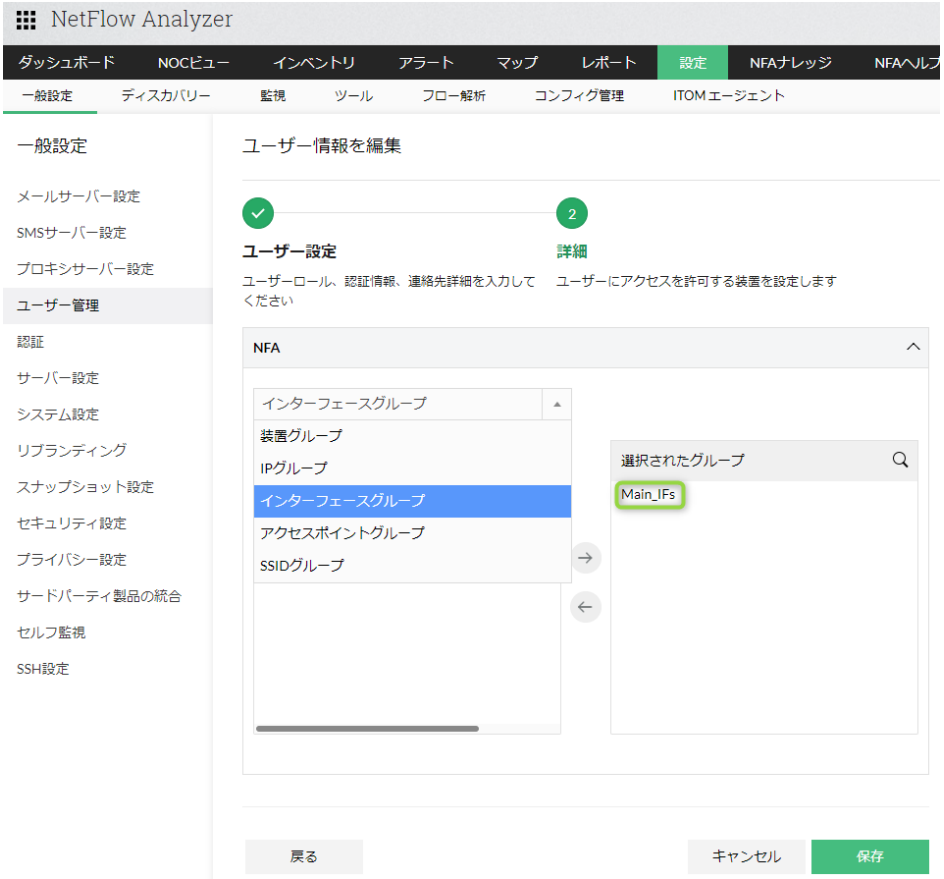
- ユーザーアカウントへ IF グループを割り当てる手順
  1. admin ユーザーで NFA にログイン

  2. ［設定］→［一般設定］→［ユーザー管理］→ 任意のユーザー名をクリック

  3. ［ユーザー設定］画面で［次へ］をクリック

  4. ［詳細］画面で［インターフェースグループ］項目を選択

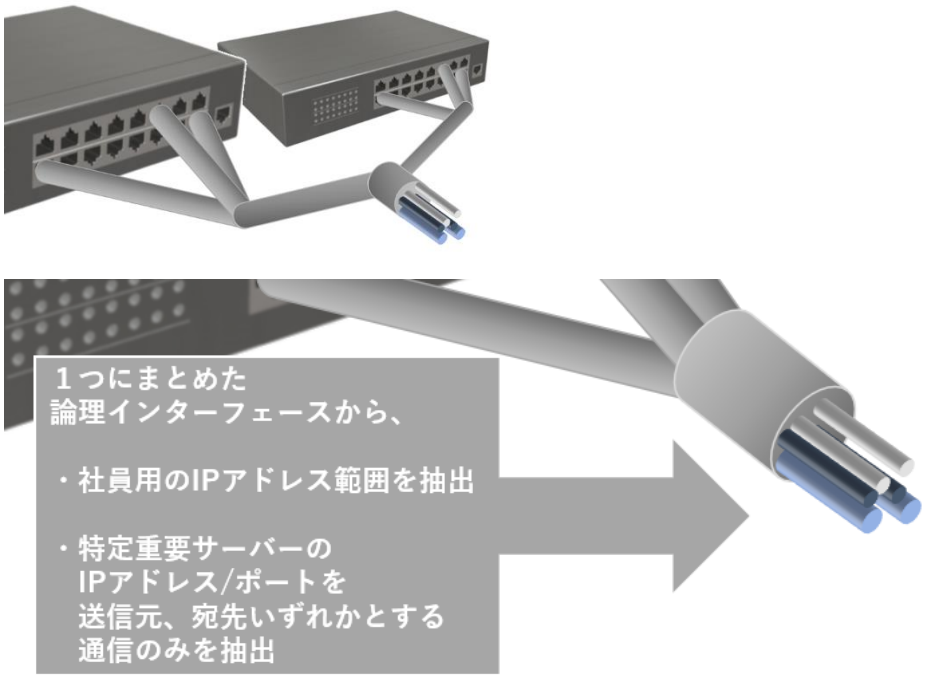
5. 監視対象 IF グループを［使用可能なグループ］から［選択されたグループ］へ移動し、［保存］をクリック



6. 該当のユーザーアカウントでログイン後、5.で選択した IF グループが［インベントリ］→［グループ］→［インターフェースグループ］に表示されることを確認

5.8　監視グループの作成 - IP グループ

IP グループは、任意 IF に対して IP アドレスやポート/プロトコル、DSCP 値の包含/除外条件でフィルタリングをするグループ機能です。
例えば基幹 IF（複数指定が可能）に対して、社員に割り当てている IP アドレス範囲を条件指定することで、社員通信のみを表示する IP グループを作成いただけます。



また、作成した IP グループをユーザーアカウントに割り当てることで、該当 IP グループのトラフィック情報の閲覧権限を該当ユーザーアカウントに付与することも可能です。

- グループの作成手順
  1. ［設定］→［フロー解析］→［グループ設定］→［IP グループ］に移動

  2. 画面右上の［追加］をクリック

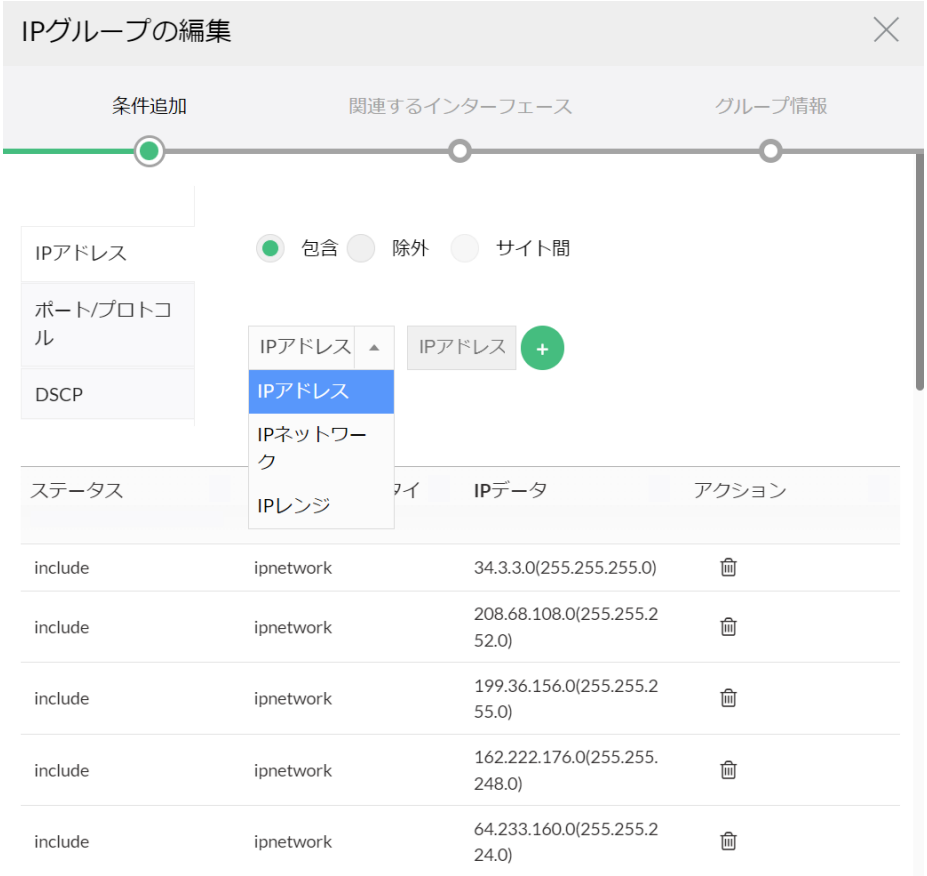
  3. グループの条件を指定、［+］アイコンで追加し［次へ］をクリック

     IP アドレス：
     ［包含］/［除外］/［サイト間］条件で IP アドレス（単一）/IP ネットワーク（サブネットマスク）/IP レンジ（範囲）を指定

     ポート/プロトコル：

プルダウンメニューからプロトコルを、入力画面に入力した任意ポート番号を条件に指定

DSCP：
プルダウンメニューから DSCP 値を条件に指定



4. 任意グループ名と説明、グループ化する IF を選択し保存
   ※グループ名に（）や※などの全角記号を利用しないでください。
   ※関連ナレッジ
   Zoom トラフィック監視：
   https://www.manageengine.jp/support/kb/NetFlow_Analyzer/?p=5776
   作成したグループの活用例：
   https://www.manageengine.jp/support/kb/NetFlow_Analyzer/?p=3826

- ユーザーアカウントへ IP グループを割り当てる手順

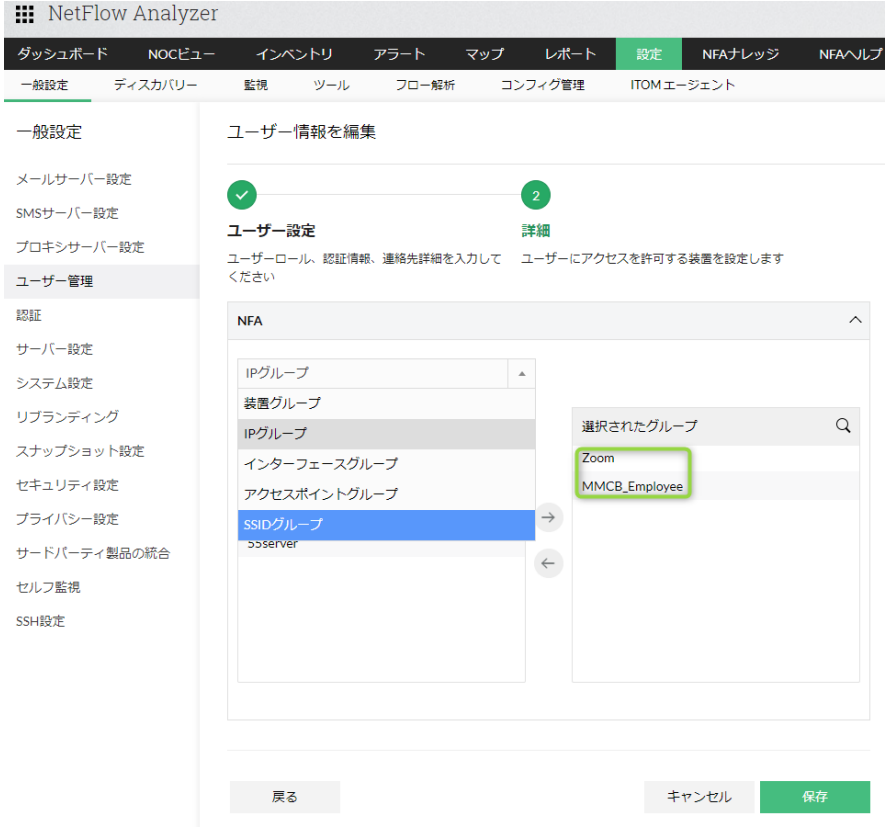
1. admin ユーザーで NFA にログイン

2. ［設定］→［一般設定］→［ユーザー管理］→ 任意のユーザー名をクリック

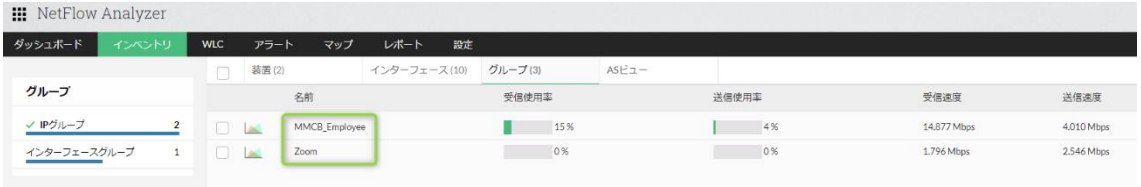
3. ［ユーザー設定］画面で［次へ］をクリック

4. ［詳細］画面で［IP グループ］項目を選択

5. 監視対象 IF グループを［使用可能なグループ］から［選択されたグループ］へ移動し、［保存］をクリック

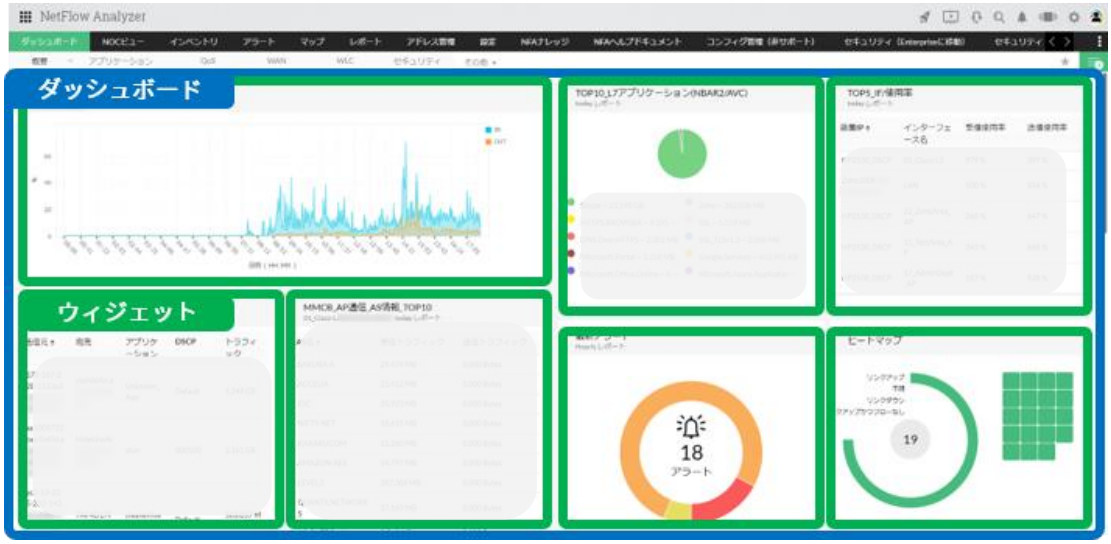


6. 該当のユーザーアカウントでログイン後、5.で選択した IP グループが［インベントリ］→［グループ］→［IP グループ］に表示されることを確認



5.9　ダッシュボードの作成

ダッシュボードは、任意の監視項目を一画面で統括的に表示するビュー機能です。
NFA が保持する各種情報を細分（ウィジェット）化し、任意に配置することが可能です。



ダッシュボード作成手順は以下の通りです。

1. ［ダッシュボード］→［カスタム］→［新規ダッシュボードの作成］に移動

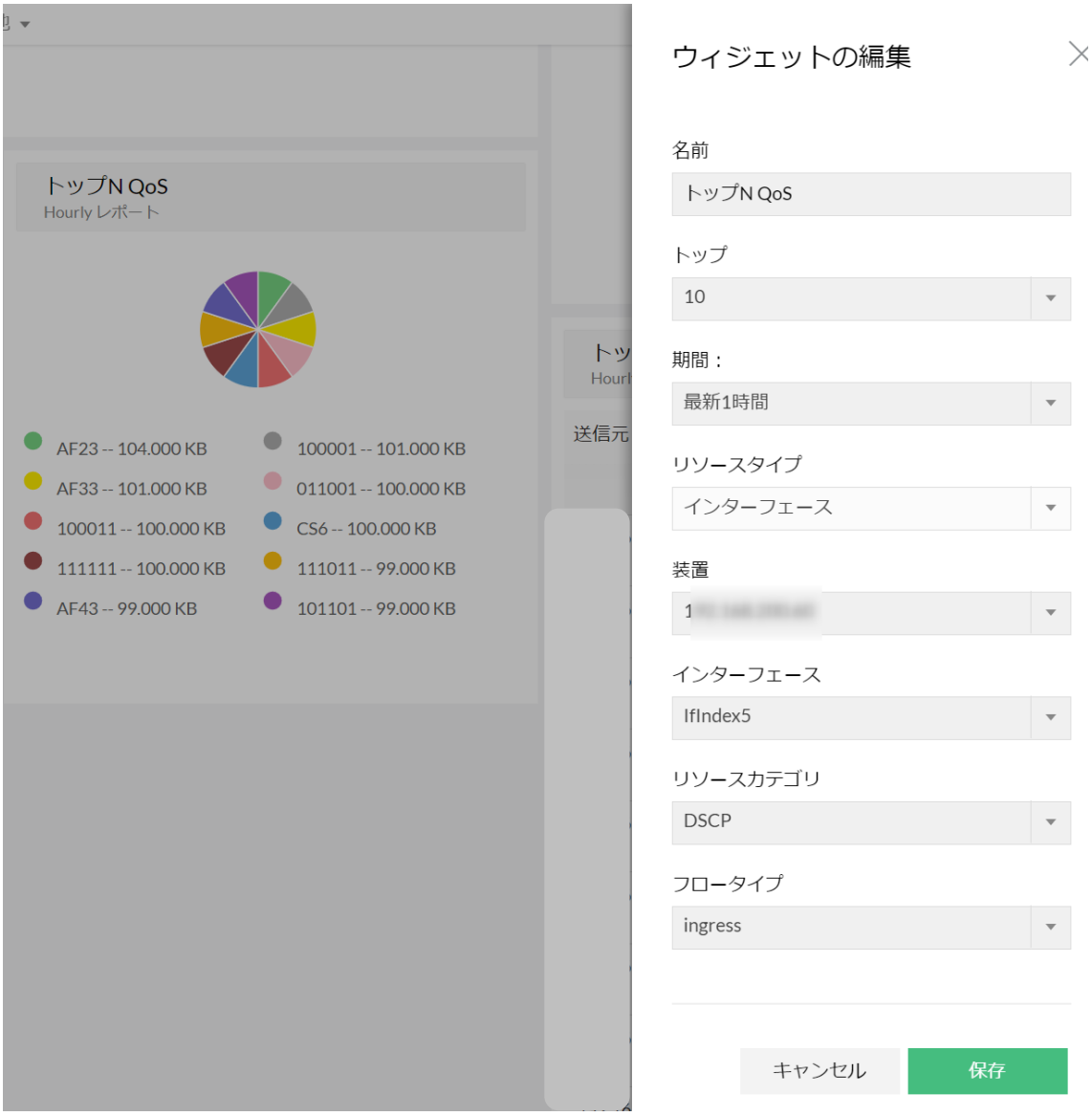
2. 任意の名前を入力し［次へ］をクリック

3. ［フロー解析］配下から、作成ダッシュボードで表示するウィジェットを選択し［次へ］をクリック
   ※選択したウィジェットはそれぞれ 1 つずつ追加されます、2 つ目以降はダッシュボードが完成後に追加してください。

4. ダッシュボードを表示するユーザーを選択し［作成］をクリック
   ※管理者権限ユーザーは全てのダッシュボードを表示可能

5. ［ダッシュボード］→［カスタム］→ 作成したダッシュボードに移動

6. 各ウィジェット右上の編集アイコン　からデータ表示の対象（IF/IP グループ/IF グループなど）や表示期間、ウィジェット名を編集



7. 画面右上の★アイコンをクリック
以降は製品へのログイン時に、★アイコンをクリックしたダッシュボードがデフォルト表示されるようになります。

5.10 アラートプロファイル設定 - 通知テンプレートの作成

アラートプロファイルでは、アラート発生条件となるしきい値を設定し、違反を検知した際に発報することが可能です。発報方法は、事前に［通知テンプレート］で設定いただく必要があります。

1. ［設定］→［フロー解析］→［通知テンプレート］に移動

2. ［追加］をクリック

3. テンプレートタイプを選択
   ※SMS（メールベース SMS/SMS 送信）はご利用いただけません。

テンプレート情報を入力

メール（メール送信による通知）
1. 任意テンプレート名を入力
2. 任意送信元/宛先/CC 先メールアドレスを入力
3. メール形式を選択（推奨：両方）
4. 件名/メッセージを編集
5. ［テスト実行］でメールの受信を確認
6. ［保存］をクリック

チャット（発報時に、連携する Slack 上でメッセージとして通知）
※［設定］→［一般設定］→［サードパーティ製品の統合］→［Slack］の事前設定が必要です。
1. 任意テンプレート名を入力
2. 宛先をチャンネル/メンバーから選択し、プルダウンメニューから該当の紐づけ先を選択
3. 件名/説明を編集
   ※プルダウンメニューから変数をクリックすることで、各内容が件名/説明（メッセージ）に反映されます。
4. ［保存］をクリック

プログラム実行（発報時にプログラムコマンドを実行）
※コマンドは［NFA_HOME］/bin から実行されます。
1. 任意テンプレート名を入力
2. コマンドを入力
3. プログラム引数を入力
   ※［引数変数］のプルダウンメニューから変数をクリックすることで、各内容が［プログラム引数］に反映されます。
4. コマンド実行結果でエラー/出力から任意の内容を選択
5. ［保存］をクリック

チケットログ（発報時に、連携するチケット管理サービス（SDP など）にアラート内容をチケット起票）
※［設定］→［一般設定］→［サードパーティ製品の統合］でチケット管理サービスの事前設定が必要です。
1. 任意テンプレート名を入力
2. 利用サービスとの紐づけを設定
3. 件名/説明を入力
   ※プルダウンメニューから変数をクリックすることで、各内容が件名/説明に反映されます。
4. ［保存］をクリック

Web アラート（製品 UI 上で音声アラートを発報）
1. 任意テンプレート名を入力
2. 音声アラートを発報させる対象ユーザーを役割の一覧から選択
3. 音声（サウンド）をプルダウンメニューから選択
4. ［保存］をクリック

syslog プロファイル（発報時に syslog を送信）
1. 任意テンプレート名を入力
2. syslog の送付対象となる宛先ホスト/ポートを入力
3. severity（重要度）とメッセージを入力
   ※プルダウンメニューから変数をクリックすることで、各内容が severity/メッセージに反映されます。
4. ［保存］をクリック

トラッププロファイル（発報時に SNMP トラップを送信）

1. 任意テンプレート名を入力
2. トラップの送付対象となる宛先ホスト/ポート/（SNMP）バージョン/コミュニティを入力
3. varbind を入力
   ※プルダウンメニューから変数をクリックすることで、各内容が varbind に反映されます。
4. ［保存］をクリック

webhook の実行（発報時に webhook を実行）

1. 任意テンプレート名を入力
2. webhook の詳細を入力

項目	説明
hook URL	webhook の URL 及び、メソッドのタイプを入力します。 ※GET 以外のメソッドを指定する場合は、更に以下の詳細を入力します。 **データタイプ** リクエストのデータタイプを入力します。 ※指定するデータタイプごとに、以降の入力する項目が異なります。 **ペイロードタイプ**（データタイプが raw の時に表示されます。） ペイロードタイプを入力します。 **コンテンツ body**（データタイプが raw の時に表示されます。） 指定したペイロードタイプに沿って、リクエストの body を入力します。 変数を利用する場合はリストアイコン をクリックします。 ※フロー情報は「NetFlow 変数」から、アラートの情報は「NFA アラート条件」 **カスタムパラメーター**（データタイプが raw 以外の時に表示されます。） URL にクエリパラメーターを付与する場合に入力します。 変数を利用する場合はリストアイコン をクリックします。
リクエストヘッダー	リクエストヘッダーが入力されていない場合は、適切なリクエストヘッダーを入力します。

ユーザーエージェント ※任意	必要に応じて、ユーザーエージェント情報を入力します。
タイムアウト値	サーバーから応答が無かった場合のタイムアウト値を入力します。

3. ［保存］をクリック

5.11 アラートプロファイル設定 - アラートプロファイルの作成

1. ［設定］→［フロー解析］→［アラートプロファイル］→［リアルタイム］に移動

2. ［追加］をクリック

3. 項目を入力し、［保存］をクリック

プロファイル名	-	必須/作成後変更不可
説明	-	任意
出力対象	-	監視インターフェースや各種グループの任意対象を選択
アラート条件	-	トラフィックタイプを受信/送信/送受信から選択
しきい値とアクションの定義	「使用率」「ボリューム（容量)」「速度」「パケット数」から選択 ※一律して比較しやすい為、「使用率」の採用を推奨します。	以下の順で定義 ＞（超過）もしくは＜（不足)、しきい値、発生回数 、時間間隔、重要度（注意/警告/重大)、通知手段（全てのテンプレート)、作成済みテンプレート ［+］アイコンをクリックすることで複数の条件を定義可能
時間フィルター	週末（土日）の除外/タイムゾーン/業務時間フィルター	任意選択 ※［業務時間フィルター］で設定した時間範囲のみをレポートの監視対象とします。

5.12 名前解決 - 事前設定 - DHCP ログファイル

DHCP ログや DNS を介して、NFA が表示する IP アドレスをホスト名や MAC アドレスに名前解決（変換）して表示することが可能です。

前提
NFA が参照する DHCP ログに関しまして、IP アドレスと名前を［Assign］で紐づけ、［Renew］で更新、［Release］で解放と認識し、NFA が処理します。

認識可能なログのサンプルは以下の通りです。
ID,Date,Time,Description,IP Address,Host Name,MAC Address
10,08/25/23,07:49:32,Assign,192.1.1.2,DESKTOP-Test.local,F01DBCA4B6DC
10,08/25/23,07:49:32,Renew,192.1.1.3,DESKTOP-Test.local,F01DBCA4B6DC,
10,08/25/23,07:49:32,Release,192.1.1.3,DESKTOP-Test.local,F01DBCA4B6DC,

DHCP ログファイル、DNS サーバーの事前設定の後、総合的な紐づけ設定をご案内します。

1. ［設定］→［フロー解析］→［IP マッピング］→［DHCP］→［インポート］に移動

2. 任意プロファイル名を入力し、 ［リモートホスト］を選択
   ※［ローカルホスト］から手動で DHCP ログファイルを読み込ませることも可能です。

3. ［ホスト名/IP アドレス］ に DHCP サーバーのホスト名または IP アドレスを入力

4. ［ユーザー名］［パスワード］に認証 ID/パスワードを入力

5. ［プロトコル］を選択し、［ポート］が自動入力されることを確認
   ※例えば［ポート］［プロトコル］それぞれ［21］［FTP］が入力されていることを確認してください。

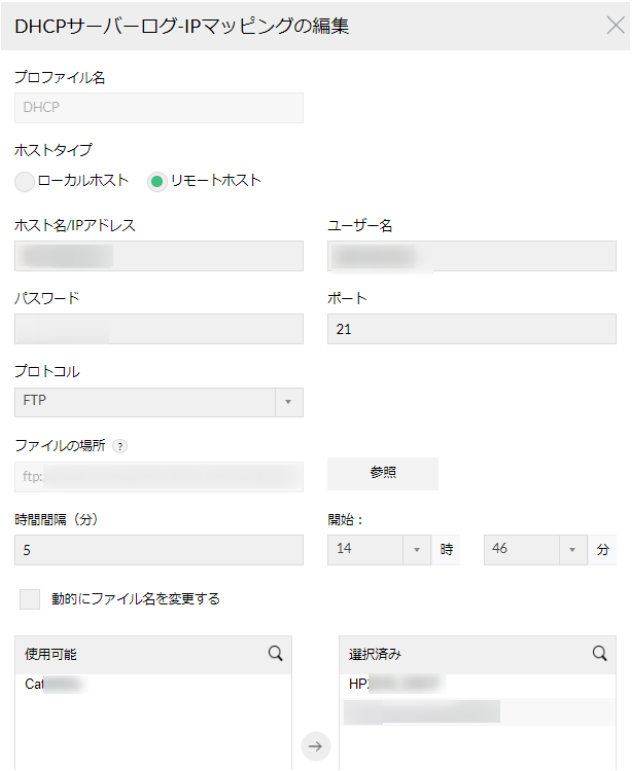
6. ［参照］から、上記で認識された DHCP サーバーにログインし、DHCP ログファイルを選択

7. ［時間間隔］に任意分数を入力

※「10（分）」などが一般的です。

8. ［開始］に任意時間を指定
※直近の指定時間から設定した時間間隔毎に、DHCP ログの差分確認が実行されます。

9. 紐づけを設定する監視対象装置を［選択済み］に移動
※別の DHCP ログ設定で設定済みの装置は選択肢として表示されません。



10. ［保存］をクリック

5.13 名前解決 - 事前設定 - DNS サーバー

「5.12 名前解決 – 事前設定 –DHCP ログファイル」に引き続き、DNS サーバーの事前設定をご案内します。

1. ［設定］→［フロー解析］→［基本設定］→［DNS］に移動

2. ［タイムアウト］［リトライ回数］を任意に指定
   ※それぞれ 3000（ミリ秒）/1（回）が一般的です。

3. ［DNS サーバー参照］で［カスタム］を選択し、紐づける DNS サーバーを最大 3 つまで［+］アイコンを用いて追加
   ※［プライマリ］はローカルサーバーから DNS 名を取得します。
   ※［セカンダリ］はローカルサーバーから DNS 名を逆引きで取得します。

4. ［保存］をクリック

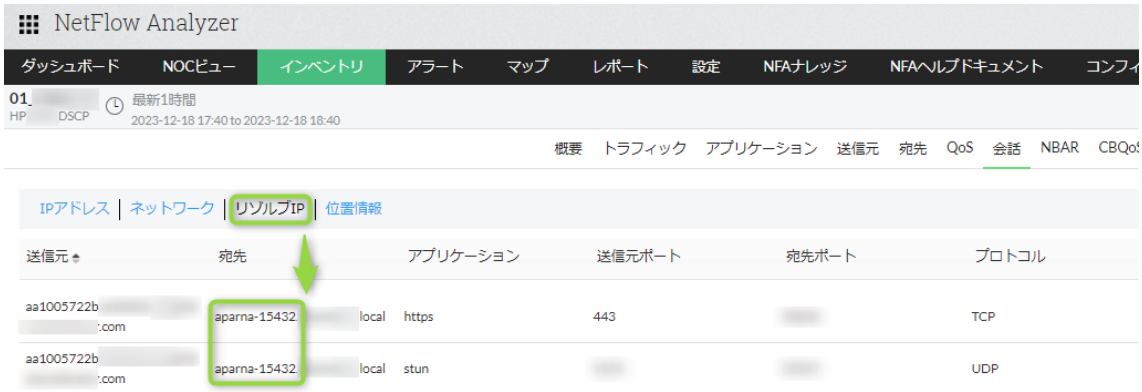
5.14 名前解決 - 紐づけ設定

「5.12 名前解決 – 事前設定 –DHCP ログファイル」と「5.13 名前解決 – 事前設定 – DNS サーバー」の設定内容を NFA に紐づけ設定します。

1. ［設定］→［フロー解析］→［基本設定］→［IP 解決］に移動

2. ［リゾルブ IP］で［デフォルト］または［オンデマンド］を選択
   ※［デフォルト］を選択すると、名前解決が常に行われたレポートが出力されます。
   ※［オンデマンド］を選択すると、名前解決が必要なレポートに対して都度手動の操作が必要となります。
   ※レポートの生成速度などパフォーマンスへの影響を考慮し［オンデマンド］のご利用を推奨しております。

3. ［IP 解決方法］で［DHCP サーバーログ］と［DNS］のみをチェックし、［保存］をクリック
   ※設定していない項目のチェックを必ず外してください。
   ※チェック項目の上から順に名前解決が優先されます。
   ※DHCP ログの名前解決情報はデータベース内に残る為、過去データを表示する際もその時々の名前解決を用いた表示が可能です。
   ※名前解決表示の例
   ［インベントリ］→［インターフェース］→ 任意インターフェース →［会話］→［リゾルブ IP］で、名前解決情報をご確認いただけます。

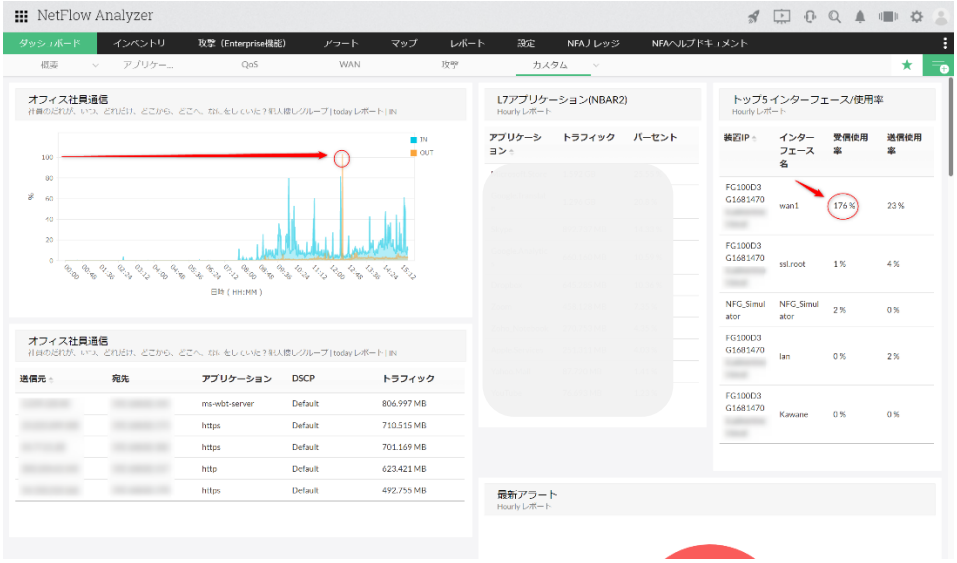


6　運用と監視

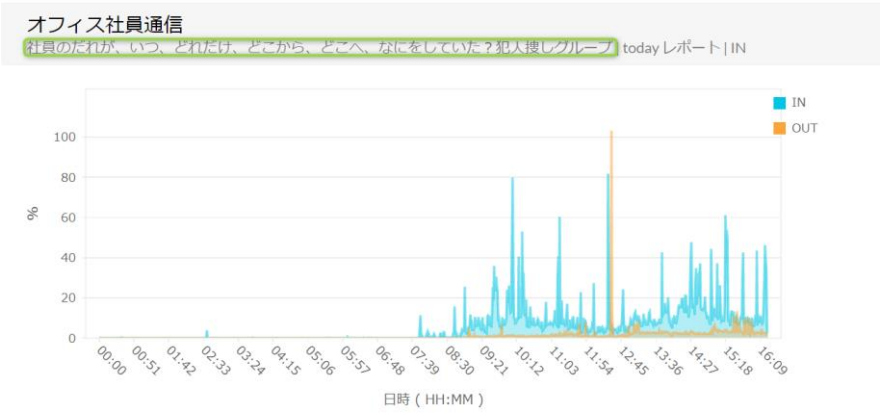
6.1　ダッシュボード

製品ログイン後、「5.9 ダッシュボードの作成」で作成したダッシュボードが表示されます。該当のダッシュボード画面で通信の問題状況を認識し、原因を特定する手順を紹介します。

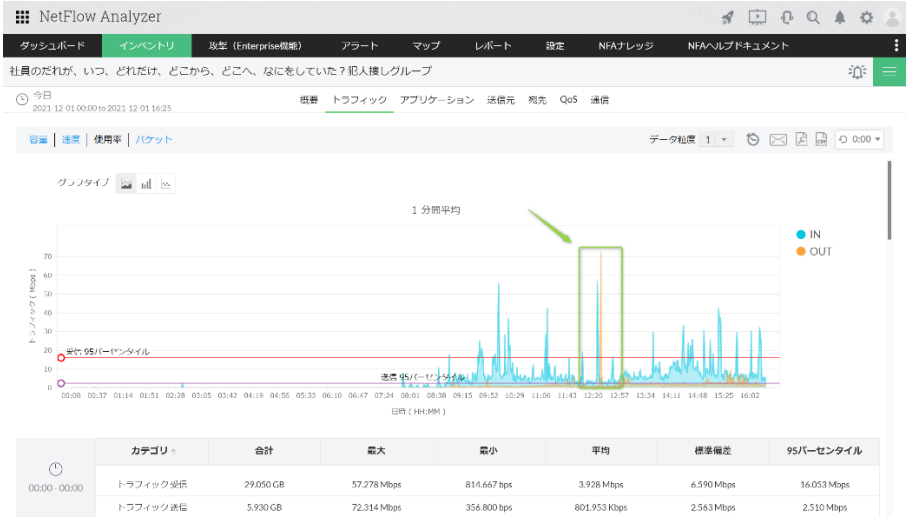
1. ［ダッシュボード］に表示される画面から通信状況を確認
   例：使用率が 100%に近くないか、もしくは超過していないか、大容量のトラフィックが発生していないか



2. ウィジェット名下の監視対象をクリックし、関連したページに移動
   ※以下の画像は IP グループを対象にしたトラフィックウィジェットの例です。



3. グラフ内の確認したい箇所をドラッグし期間を抽出
※抽出する期間幅は最短でも 19 分間以上にしてください。19 分間未満の場合、データポイントの仕様上［会話］情報が表示されない場合があります。
※画面右上の時計アイコンから任意期間の指定が可能です。



4. ［会話］→［受信/送信］ラジオボタン →［リゾルブ IP］に移動
※［受信/送信］ラジオボタンの内、［受信］がデフォルトで選択されています。
※通信情報は、トラフィック容量の大きい順で表示されます。
※ユーザーやサーバーの通信状況を把握し、気になる通信の原因を特定いただけます。

※IP グループを用いたダッシュボードの構築や、通信内訳情報の確認方法について、以下のページをご参照ください。
https://www.manageengine.jp/support/kb/NetFlow_Analyzer/?p=6585

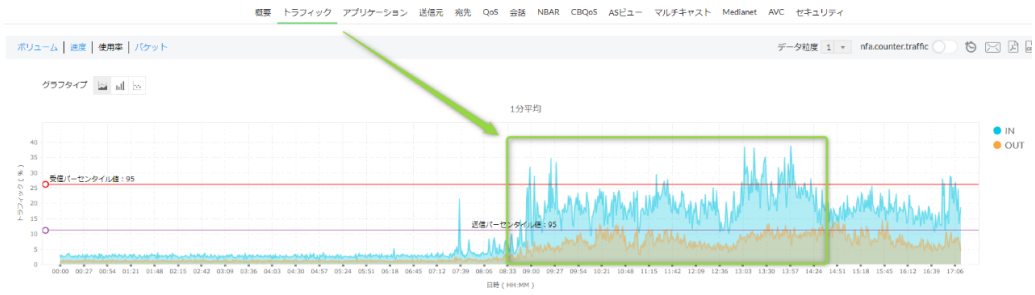
6.2　インベントリ - インターフェース

監視対象 IF 一覧の使用率状況から通信の問題を認識し、原因を特定する手順を紹介します。

1. ［インベントリ］→［インターフェース］に表示される受信/送信使用率などを確認
   例：使用率が 100%に近くないか、もしくは超過していないか、大容量のトラフィックが発生していないか
   ※使用率表示の注意事項について「5.3 監視対象装置/IF 情報の手動更新」で紹介しています。

2. 確認したいインターフェース名をクリック

3. ［トラフィックタブ］で確認したい箇所をマウスドラッグし、監視対象期間幅を抽出
   ※抽出する期間幅は最短でも 19 分間以上にしてください。19 分間未満の場合、データポイントの仕様上［会話］情報が表示されない場合があります。
   ※画面左上の時計アイコンから任意期間の指定が可能



4. ［会話］→［受信/送信］ラジオボタン →［リゾルブ IP］に移動
※［受信/送信］ラジオボタンの内、［受信］がデフォルトで選択されています。
※通信情報は、トラフィック容量の大きい順で表示されます。
※ユーザーやサーバーの通信状況を把握し、気になる通信の原因を特定いただけます。

※インベントリ機能を用いた「遅延報告への切り分け例と原因特定方法」について、以下のページをご参照ください。
https://www.manageengine.jp/support/kb/NetFlow_Analyzer/?p=6787

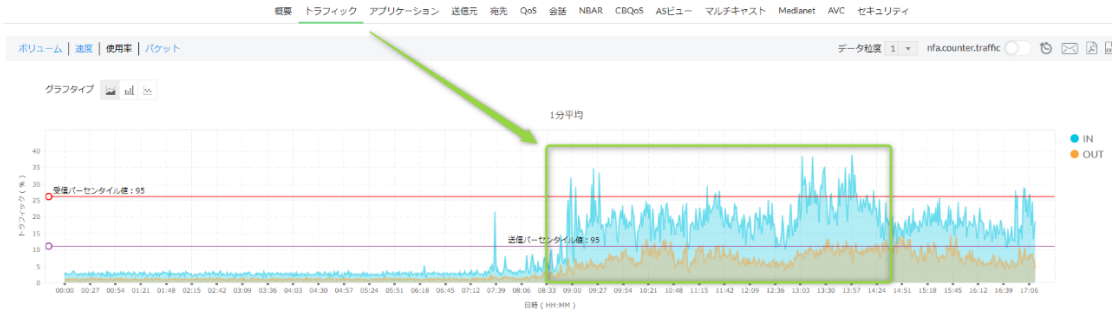
6.3　インベントリ - IP グループ

作成した IP グループ一覧の使用率状況から通信の問題を認識し、原因を特定する手順を紹介します。
※IP グループの作成手順は「5.8 監視グループの作成 – IP グループ」で紹介しています。

1. ［インベントリ］→［IP グループ］に表示される受信/送信使用率などを確認
   例：使用率が 100%に近くないか、もしくは超過していないか、大容量のトラフィックが発生していないか

2. 確認したい IP グループ名をクリック

3. ［トラフィックタブ］で確認したい箇所をマウスドラッグし、監視対象期間幅を抽出
   ※抽出する期間幅は最短でも 19 分間以上にしてください。19 分間未満の場合、データポイントの仕様上［会話］情報が表示されない場合があります。
   ※画面左上の時計アイコンから任意期間の指定が可能



4. ［会話］→［受信/送信］ラジオボタン →［リゾルブ IP］に移動
※［受信/送信］ラジオボタンの内、［受信］がデフォルトで選択されています。
※通信情報は、トラフィック容量の大きい順で表示されます。
※ユーザーやサーバーの通信状況を把握し、気になる通信の原因を特定いただけます。

※Zoom アプリケーションのトラフィック監視を例とした「XML ファイルを用いた IP グループの設定と活用」方法について、以下のページをご参照ください。
https://www.manageengine.jp/support/kb/NetFlow_Analyzer/?p=5776

6.4　レポート - 概要

NFA ではインターフェースや作成グループを対象に様々なレポートを作成できます。

レポート	説明
検索	検索条件に基づいたレポート情報を生成します。
レポートプロファイル	オリジナルフィルターと出力したいトラフィックレポートを任意に組み合わせ、生成レポートの型を定義し情報を出力する、カスタマイズ性の高いレポートです。
フォレンジクス	ローデータを参照し詳細情報を出力するレポートです。
お気に入りレポート	出力したフォレンジクスレポート画面右上の☆アイコンから、レポートの生成条件をお気に入りレポートとして保存します。 お気に入りレポートから、再度その条件で最新のレポートを出力できます。
統合	監視対象とするインターフェースやグループ情報の通信情報を統合的に表示するレポートです。各監視対象の概要通信情報を提供します。
比較	複数の監視対象を同じ期間で、もしくは単一の監視対象を複数の期間でレポート化します。
プロトコル分布	インターフェースやグループを対象に、帯域使用率トップ N プロトコル情報をレポート化します。
インベントリレポート	インターフェースやグループを対象に、条件に絞ったトラフィック情報をレコード形式で表示します。
パーセンタイルレポート	パーセンタイル値に基づいて詳細なトラフィック情報を提供します。
LAN WAN レ	LANIP 間、もしくは LANIP と WANIP 間の送信/受信トラフィックを

ポート	レポート化します。
位置情報レポート	Geolocation(位置情報)毎の通信情報をレポート化します。
課金	帯域監視からユーザー課金や部署間のコスト付け替えに必要な情報を提供します。
予測	トラフィック情報の傾向から将来予測をレポートとして提供します。
スケジュール	単発、もしくは日次/週次/月次単位で指定したレポートを自動作成し、必要に応じてメール送付する機能です。

以降、代表的なレポートである「統合」「フォレンジクス」「比較」「スケジュール」についてご案内します。その他のレポートタイプについては、以下のマニュアルご参照ください。
https://www.manageengine.jp/products/NetFlow_Analyzer/help/reports-netflow-analyzer-12-user-guide.html

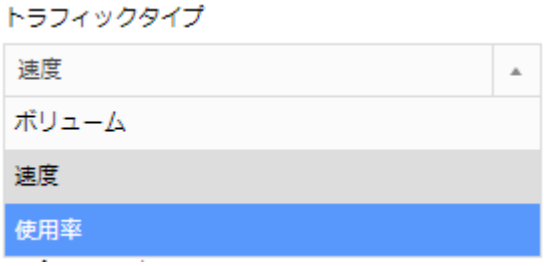
6.5　レポート - 統合

統合レポートは、インターフェース、インターフェースグループ、または IP グループの通信の概要を表示するレポートです。レポートの生成手順は以下の通りです。

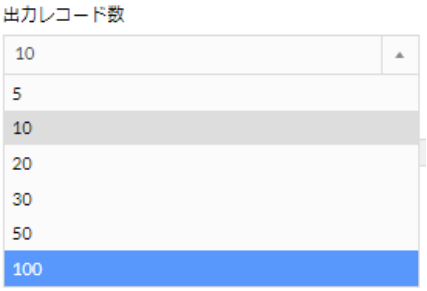
1.　［レポート］→［NFA］→［統合］に移動

2.　出力対象を指定

3.　出力するトラフィックタイプを速度/ボリューム/使用率から選択



4.　出力レコード数（出力データのトップ N 数）を選択
※10 を選択するとトップ 10 のデータが表示されます。
※データ数が少ない場合、選択した数字よりも少ないトップ N 数でデータが表示されます。



5. ［レポートを選択］から、生成するレポートに表示させたい項目を選択

6. データの表示期間を選択

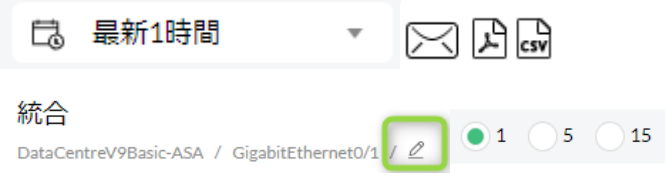
7. ［業務時間フィルター］/［週末の除外］を任意に設定

※［業務時間フィルター］で設定した時間範囲のみをレポートの監視対象とします。

※［週末の除外］オプションの「週末」は「土曜日と日曜日（固定）」を指します。

8. ［レポート生成］をクリック

※作成したレポート画面右上のアイコンから、表示時間の調整や PDF/CSV レポートの出力、メール添付での PDF レポート送付やレポート生成条件の調整、トラフィックデータの時間粒度が可能



6.6 レポート - フォレンジクス

フォレンジクスレポートは、ローデータを用いて IF の詳細情報を表示するレポートです。ローデータを保持している期間であれば、発生する全通信を分単位で表示することが可能です。ローデータの保持期間については「5.4 データ保持設定」をご確認ください。
レポートの生成手順は以下の通りです。

1. ［レポート］→［NFA］→［フォレンジクス］に移動

2. ［出力対象］で、監視対象を選択

3. ［条件定義］で出力データの条件を指定
   ※条件を指定しない場合は、全データを表示します。
   ※［+］アイコンで任意の条件を追加できます。

4. 全条件に対する［いずれかの条件に合致（or）/すべての条件に合致（and)］を選択

5. ［期間］で、データの表示期間を選択
   ※ローデータの保持期間内の値を指定してください。

6. ［業務時間フィルター］/［週末の除外］を任意に設定
   ※［業務時間フィルター］で設定した時間範囲のみをレポートの監視対象とします。
   ※［週末の除外］オプションの「週末」は「土曜日と日曜日（固定）」を指します。

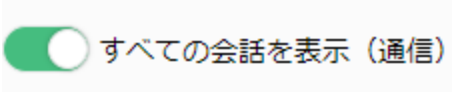
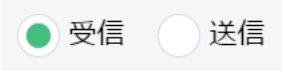
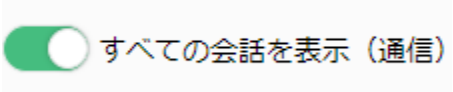
7. ［レポート生成］をクリック

生成レポート内、画面右上のアイコンから、お気に入りレポートに追加/PDF/CSV レポートの出力、さらにメールに PDF レポートを添付し特定の宛先に送付することが可能です。

通信情報が表示されるタブは、［トラフィック/アプリケーション/送信元/宛先/QoS/TCP フラッグ/次のホップ（ネクストホップ）/会話/AS ビュー/マルチキャスト/メディアネット］です。

タブ	詳細
トラフィック	受信/送信トラフィック情報を表示します。［ボリューム/速度/使用率/パケット（数）］から表示データ種類を変更できます。
アプリケーション	受信/送信アプリケーション情報を、トラフィック量/パケット数と共に表示します。

	アイコン 受信 送信 から受信/送信情報を表示切替することが可能です。 各アプリケーション名をクリックすることで、詳細通信情報を確認することが可能です。
送信元/宛先	受信/送信（IF で受信する通信/送信される通信） 送信元/宛先（各通信の送信元/宛先）情報を、トラフィック量/パケット数と共に表示します。 ※特定インターフェースで受信したパケットの送信元情報を「送信元受信レポート」、受信したパケットの宛先情報を「宛先受信レポート」、特定インターフェースから送信したパケットの送信元情報を「送信元送信レポート」、送信した宛先情報を「宛先送信レポート」とそれぞれ表示しています。 アイコン 受信 送信 から受信/送信情報を表示切替することが可能です。 ［リゾルブ IP］から、名前解決を実施することが可能です。 各項目をクリックすることで、それぞれの詳細通信情報を確認することが可能です。
QoS	受信/送信 DSCP/ToS 情報を、トラフィック量/パケット数と共に表示します。 アイコン 受信 送信 から受信/送信情報を表示切替することが可能です。 各 DSCP/ToS 値をクリックすることで、それぞれの詳細通信情報を確認することが可能です。
TCP フラグ	TCP フラグ値が受信フローデータに含まれる場合、値を表示します。 TCP フラグ名をクリックすることで、TCP フラグ値ごとの通信情報も表示します。 アイコン 受信 送信 から受信/送信情報を表示切替することが可能です。
次のホッ	フローデータに含まれる nexthop 情報が含まれる場合、値を表示します。

プ	IP アドレスをクリックすることで、ネクストホップ IP ごとの通信情報も表示します。 アイコン  から受信/送信情報を表示切替することが可能です。
AS ビューー	AutonomousSystem データを表示します。 アイコン  から受信/送信情報を表示切替することが可能です。
会話	送信元/宛先が一対の通信情報を受信/送信毎に表示します。 アイコン  から受信/送信情報を表示切替することが可能です。 ［リゾルブ IP］から、名前解決を実施することが可能です。 アイコン  を有効化することで、受信中の MAC アドレス情報を表示することが可能です。
マルチキャスト	マルチキャスト情報を表示します。 アイコン  から受信/送信情報を表示切替することが可能です。 ［リゾルブ IP］から、名前解決を実施することが可能です。
Medianet	Cisco Medianet 機能をご利用の場合、取得した情報を表示します。 アイコン  から受信/送信情報を表示切替することが可能です。 ［リゾルブ IP］から、名前解決を実施することが可能です。 アイコン  を有効化することで、受信中の MAC アドレス情報を表示することが可能です。

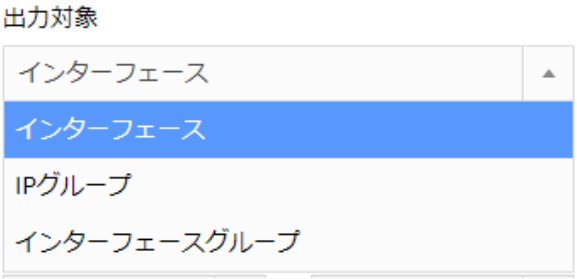
6.7　レポート - 比較

比較レポートは、複数の監視対象を同じ期間で、もしくは同一の監視対象を異なる期間で比較表示するレポートです。

［複数の監視対象/同じ期間］の比較レポートの生成手順は以下の通りです。

1. ［レポート］→［NFA］→［比較］→［複数の監視対象/同じ期間］に移動

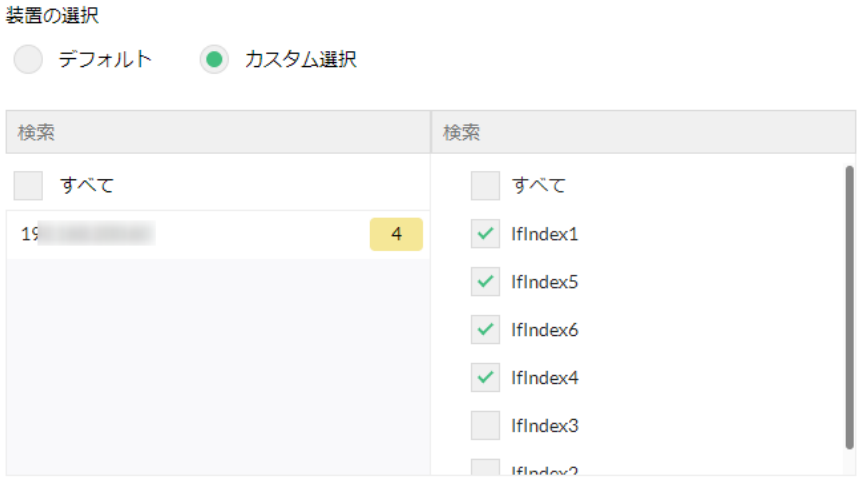
2. ［出力対象］で、監視対象を選択



3. ［デフォルト］ラジオボタンから、比較する対象のトップ N 値（5/10/20）と、参考基準（トラフィック（量）/95 パーセンタイル、受信/送信/両方（送受信合計））を選択

> NFA における「N パーセンタイル」値とは、表示中データポイントの値（速度/容量/使用率/パケット）を昇順で並べ、上位(100-N)［%］の個数の値を除いた中で一番大きなデータポイントの値です。
>
> 仮に、グラフの速度値が以下のように 20 データポイントで表示されている場合の 95 パーセンタイル値の基準をご紹介します。
> 10,63,51,64,92,120,72,83,69,66,12,77,46,74,36,82,42,54,75,89（単位 Mbps）
>
> 全データポイントの値を昇順で並べます
> 10,12,36,42,46,51,54,63,64,66,69,72,74,75,77,82,83,89,92,120（単位 Mbps）
>
> 95%は 19/20 なので 20 データポイントのうち 19 番目のデータポイント値"92"を抽出します。
>
> 95 パーセンタイル横軸の基準は 92Mbps となります。

もしくは、［カスタム選択］ラジオボタンから、比較対象とする対象を選択



4. ［データ粒度を選択］

5. ［期間］で、データの表示期間を選択

6. ［業務時間フィルター］/［週末の除外］を任意に設定

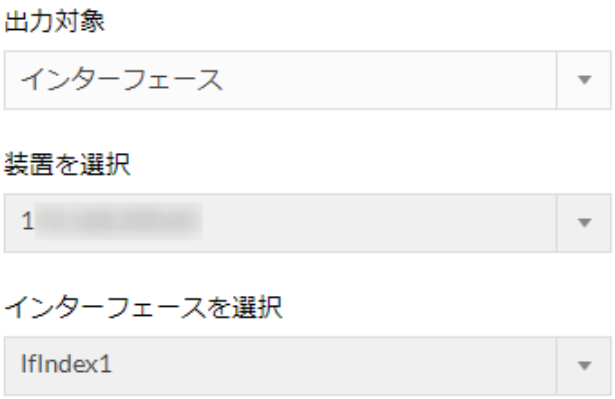
※［業務時間フィルター］で設定した時間範囲のみをレポートの監視対象とします。
※［週末の除外］オプションの「週末」は「土曜日と日曜日（固定)」を指します。

7. ［レポート生成］をクリック
※作成したレポート画面上部のアイコンから、表示時間の調整や PDF/CSV レポートの出力、メール添付での PDF レポート送付やレポート生成条件の調整が可能

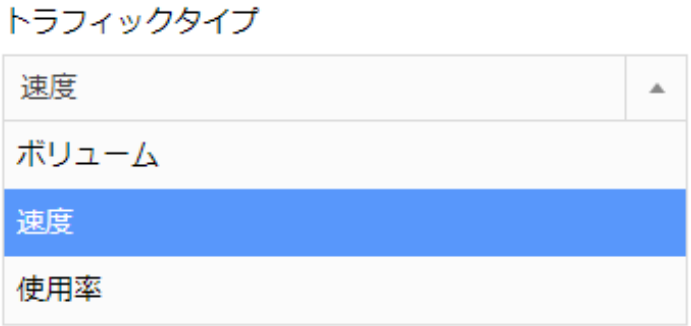
［同一の監視対象/異なる期間］の比較レポートの生成手順は以下の通りです。

1. ［レポート］→［NFA］→［比較］→［同一の監視対象/異なる期間］に移動

2. ［出力対象］で、監視対象を選択

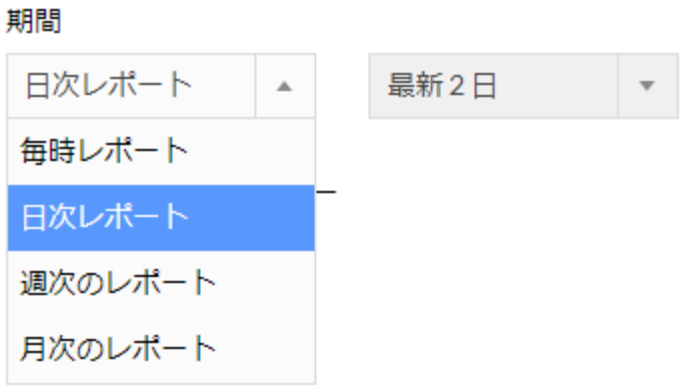


3. ［トラフィックタイプ］を選択



4. ［データ粒度を選択］

5. ［期間］で、データの表示期間を選択



6. ［業務時間フィルター］/［週末の除外］を任意に設定
※［業務時間フィルター］で設定した時間範囲のみをレポートの監視対象とします。
※［週末の除外］オプションの「週末」は「土曜日と日曜日（固定)」を指します。

7. ［レポート生成］をクリック
※作成したレポート画面上部のアイコンから、表示時間の調整や PDF/CSV レポートの出力、メール添付での PDF レポート送付やレポート生成条件の調整が可能

6.8 レポート - スケジュール

スケジュールレポートは、1 度のみ、もしくは日次、週次、月次といった任意のタイミングでレポートを生成し、レポートファイルの保管や特定のメールアドレスにレポートを送付する機能です。

例：
・統合レポート：毎日の特定 IP グループ通信概要情報を PDF レポートで出力し、管理者へメール送付
・比較レポート：毎週金曜日に、各曜日の特定 IF トラフィック推移を PDF レポートで出力、管理者へメール送付
・フォレンジクスレポート：毎日の特定 IF 通信詳細情報を CSV レポートで出力し、管理者いへメール送付

1. ［レポート］→ ［NFA］ →［スケジュール］→［スケジュールの追加］に移動

2. 任意のタブを選択
   ※フォレンジクスレポートは［インターフェース/アクセスポイント］タブでのみ利用可能

3. 任意のスケジュールプロファイル名を入力
   ※プロファイル（スケジュール）名には半角英数字と_（アンダーバー）をご利用ください。

4. レポートタイプを指定
   ※［統合］［比較］［フォレンジクスレポート］など

5. 監視対象を選択

6. レポート形式を PDF/CSV から指定

7. スケジュールの実行タイミングを設定
   ※スケジュールレポートを複数作成する場合、各スケジュールの実行タイミングに関して 5～10 分以上の間隔を空ける必要があります。
   ※［週末の除外］オプションの「週末」は「土曜日と日曜日（固定）」を指します。

8. ［メール通知］オプションを設定

9. をクリックし、任意の項目を設定
※フォレンジクスレポートには［表示を増やす］オプションはありません。

10. ［保存］をクリック

11. スケジュール生成されるレポートを［レポート］→ ［NFA］ →［スケジュール］や受信メールの添付で確認

7　お問い合わせ窓口と関連資料

7.1　お問い合わせ窓口

製品に関する技術サポートやその他お問い合わせについては、以下のページをご確認ください。

評価版ユーザーのお問い合わせ
https://www.manageengine.jp/support/trial.html

製品購入後（保守ユーザー）のお問い合わせ
https://www.manageengine.jp/support/purchased.html

保守ユーザーは、下記の保守ユーザー専用ポータル「ManageEngine Community」よりお問い合わせください。

・ManageEngine Community
https://adcommunity.manageengine.jp/jsp/login.jsp

・ManageEngine Community マニュアル
https://jpmeuser.wiki.zoho.com/Me-Community.html

価格、お見積りなどの営業に関するお問い合わせ
https://www.manageengine.jp/purchase/

その他のお問い合わせ
https://www.manageengine.jp/contact.html

7.2 関連資料

オンラインユーザーマニュアル
https://www.manageengine.jp/products/NetFlow_Analyzer/help/

ナレッジベース
https://www.manageengine.jp/support/kb/NetFlow_Analyzer/

リリース関連情報
https://www.manageengine.jp/products/NetFlow_Analyzer/help/release_info.html

オプション
https://www.manageengine.jp/products/NetFlow_Analyzer/help/options.html

簡易版スタートアップガイド
https://www.manageengine.jp/products/NetFlow_Analyzer/startup-guide.html

製品提供元

ゾーホージャパン株式会社
〒220-0012
神奈川県横浜市西区みなとみらい 3-6-1 みなとみらいセンタービル 13 階

ホームページ：https://www.zoho.co.jp

NetFlow Analyzer 製品ページ：
https://www.manageengine.jp/products/NetFlow_Analyzer/