ZJTP20234171575

ManageEngine Firewall Analyzer

スタートアップガイド

2024年改訂

■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 6
1.1 Firewall Analyzerについて 6
1.2 本ガイドについて 6
1.3 本ガイドの目的と対象読者 6
2 動作環境 6
2.1 ハードウェア要件 7
2.2 OS要件 8
2.3 Webブラウザー要件 8
2.4 ポート要件 9
3 FWAのセットアップ 9
3.1 インストーラーのダウンロード 9
3.2 インストール手順（Windows） 9
3.3 インストール手順（Linux） 17
3.4 アンインストール手順 21
4 起動と停止 22
4.1 起動、停止に関する注意事項 22
4.2 Windows（起動） 22
4.3 Windows（停止） 23
4.4 Linux（起動） 24
4.5 Linux（停止） 25
5 初期設定 25
5.1 Webクライアントへのアクセス 25
5.2 ライセンス適用（保守ユーザー向け） 26
5.3 ログインパスワードの更新とメールサーバー設定 28
5.4 装置登録 29
5.4.1 FWAにsyslogを直接転送 30
5.4.2 ファイルインポート 31
5.5 アーカイブ設定 36
6 レポート 38
6.1 FWAレポート 38
6.1.1 イントラネット設定 41
6.2 プロキシレポート 42
6.3 VPNレポート 43
6.4 カスタムレポート（スケジュールレポート） 45

6.4.1 スケジュール設定方法 45
6.4.2 レポートフィルター 46
6.4.3 レポートタイプ 47
7 アラートプロファイル設定 48
7.1 通知テンプレートの作成 48
7.2 アラートプロファイルの作成 49
7.3 通常アラート 50
7.4 異常アラート 51
7.5 帯域 52
7.6 SNMP設定 53
8 アラート 55
8.1 アラート 55
8.2 可用性アラート 56
8.3 セルフ監視 57
9 ルール管理 58
9.1 装置ルール設定 58
9.2 ルール管理 63
9.2.1 概要 64
9.2.2 最適化 65
9.2.3 クリーンアップ 66
9.2.4 並べ替え 67
9.2.5 影響 68
9.2.6 管理 71
9.2.7 比較 73
9.2.8 期限切れ通知 74
10 コンフィグバックアップ 75
10.1 コンフィグバックアップのスケジュール設定手順 76
10.2 バックアップ監査 77
10.3 比較 78
11 ログ検索 79
11.1 生ログ設定 79
11.2 生ログ検索 80
11.3 集約検索 82
12 ユーザー管理とロール権限 83
12.1 ユーザー管理 83
12.2 ロール権限 86
12.3 パスワードポリシー 87

13　各メニュータブの説明 88
13.1　ダッシュボード 88
13.1.1 ダッシュボードの新規作成 89
13.1.2 ウィジェットの追加、編集、削除 91
13.2　インベントリ 92
13.2.1 スナップショット画面 93
13.3　アラート 95
13.4　レポート 95
13.5　ルール管理 96
13.6　コンプライアンス 96
13.7　検索 96
13.8　ツール 97
13.9　設定 97
13.10 サポート(米国) 98
14　お問い合わせ窓口と関連資料 98
14.1　お問い合わせ窓口 98
14.2　関連資料 99

1 はじめに

1.1 Firewall Analyzerについて

ManageEngine Firewall Analyzerは、マルチベンダーのUTM・ファイアウォール、プロキシサーバーのログを収集し、一元的に管理するツールです。

収集したログの統計的な可視化や、特定のログを検知した際のアラート発報、ファイアウォールに設定されているルールの整理、管理を実現します。

1.2 本ガイドについて

本ガイドでは、Firewall Analyzer（以下、FWA）のインストール方法から導入時に必要な初期設定、製品機能の概要について記載します。
本ガイドは、ビルド12.7.124（2024年1月24日リリース）をもとに作成しています。

FWAのリリースビルドについては、以下をご参照ください。
https://www.manageengine.jp/products/Firewall_Analyzer/support.html#eol

本ガイドに記載の範囲は、FWAの基本的な操作方法です。
一部機能は、本ガイドでは取り扱っておりません。

FWAのユーザーマニュアルは、以下をご参照ください。
https://www.manageengine.jp/products/Firewall_Analyzer/help/

1.3 本ガイドの目的と対象読者

本ガイドは、FWA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 動作環境

2.1 ハードウェア要件

最小のハードウェア要件は、以下の通りです。

- CPU：Quad Core 3.5 GHz/ 8 threads以上
- メモリ：8GB以上
- ハードディスク：90GB以上

FWAではログの流量やログの保存期間に応じて、サイジング情報を設定しています。
サイジングの目安は以下をご確認ください。
※ログ流量=1秒間のパケット数

メモリ要件

ログ流量	メモリ
500ログ/秒まで	8GB
500ログ/秒以上	16GB

ハードディスク（保存期間）

ログ流量	1日	1週間	1か月	3か月	6か月	1年間
500ログ/秒	12GB	38GB	100GB	210GB	320GB	630GB
100ログ/秒	18GB	65GB	150GB	400GB	720GB	1.2TB
300ログ/秒	40GB	150GB	440GB	1TB	1.5TB	2.5TB
500ログ/秒	90GB	300GB	720GB	1.8TB	3.4TB	6TB
1000ログ/秒	180GB	640GB	1.4TB	3.5TB	6TB	10.5TB
2000ログ/秒	364GB	1.31TB	3.03TB	7.2TB	13.5TB	21.1TB
3000ログ/秒	546GB	1.97TB	4.5TB	10.8TB	20.3TB	31.6TB

※上記のサーバーサイジングは、OSリソースを考慮しておりません。
※ハードディスクサイズ：アーカイブ + インデックス + データベースサイズ = 合計サイズ
※製品のご利用に際し、専用サーバーでご利用いただくことを推奨しています（その他のアプリケーションが同サーバー上で稼働している場合、十分なリソースを確保できない場合があります）。
※ご購入前に、評価版でのご利用環境の検証を推奨します。
※対象装置のsyslogを、サードパーティーのsyslogサーバー経由でFWAサーバーに転送することは非推奨の構成です。トラブルシューティングの状況に応じて、対象装置から

の直接転送（弊社推奨構成）をご案内する場合がございますので、あらかじめご了承ください。
※FWAの機能で、ログ流量を確認することができます。
https://www.manageengine.jp/support/kb/Firewall_Analyzer/?p=2189

2.2 OS要件

FWAのOS要件は、以下の通りです。

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Red Hat Enterprise Linux 8～9.4
- CentOS Stream 9
- Ubuntu Server 20.04 LTS
- Ubuntu Server 22.04 LTS

※64bit版をご利用ください。
※評価期間中のみ、クライアントOSを使用することが可能ですが、スペックや稼働状況によって動作が遅くなる可能性がございます。なお、**本番の運用環境では上記のサーバーOSをご利用ください。**
※AWSやAzureなどのクラウド環境、VMwareやHyper-V、XenServerなどの仮想化環境上でも、上記対応OS上であれば運用可能です。ただし、性能に関しては、必ず評価版を利用して製品性能を十分に検証した上で、お客様の性能要件を満たすか確認してください。

2.3 Webブラウザー要件

FWAのWebUIにアクセスする際は、以下のブラウザーをご利用ください。

- Google Chrome（最新版）
- Mozilla Firefox（最新版）
- Microsoft Edge（最新版）

2.4 ポート要件

FWAで使用するポート番号について、以下の表をご確認ください。

用途	ポート番号
WebUI接続	8060/8061（TCP） HTTP/HTTPS
DB接続 （PostgreSQL）	13306（TCP）
SSHD	22（TCP）
syslogサーバー	1514（UDP）
ログファイルのインポート	21（FTP：TCP） 22（SFTP/SCP：TCP）

3 FWAのセットアップ

3.1 インストーラーのダウンロード

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

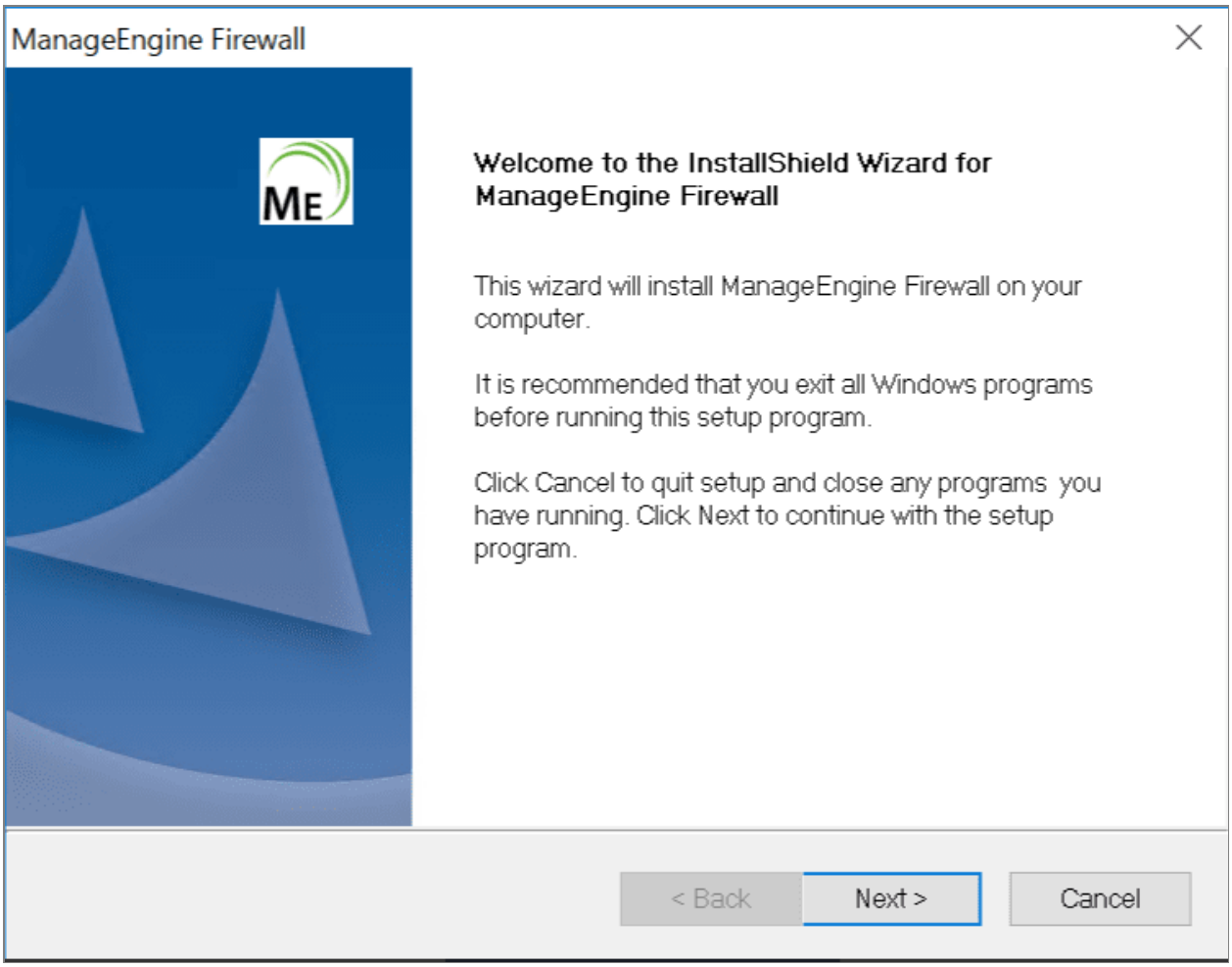
> インストール後30日間は、評価版としてすべての機能を使用できます。30日の評価期間が終了後、正規ライセンスを適用しない場合、自動的に停止します。

3.2 インストール手順（Windows）

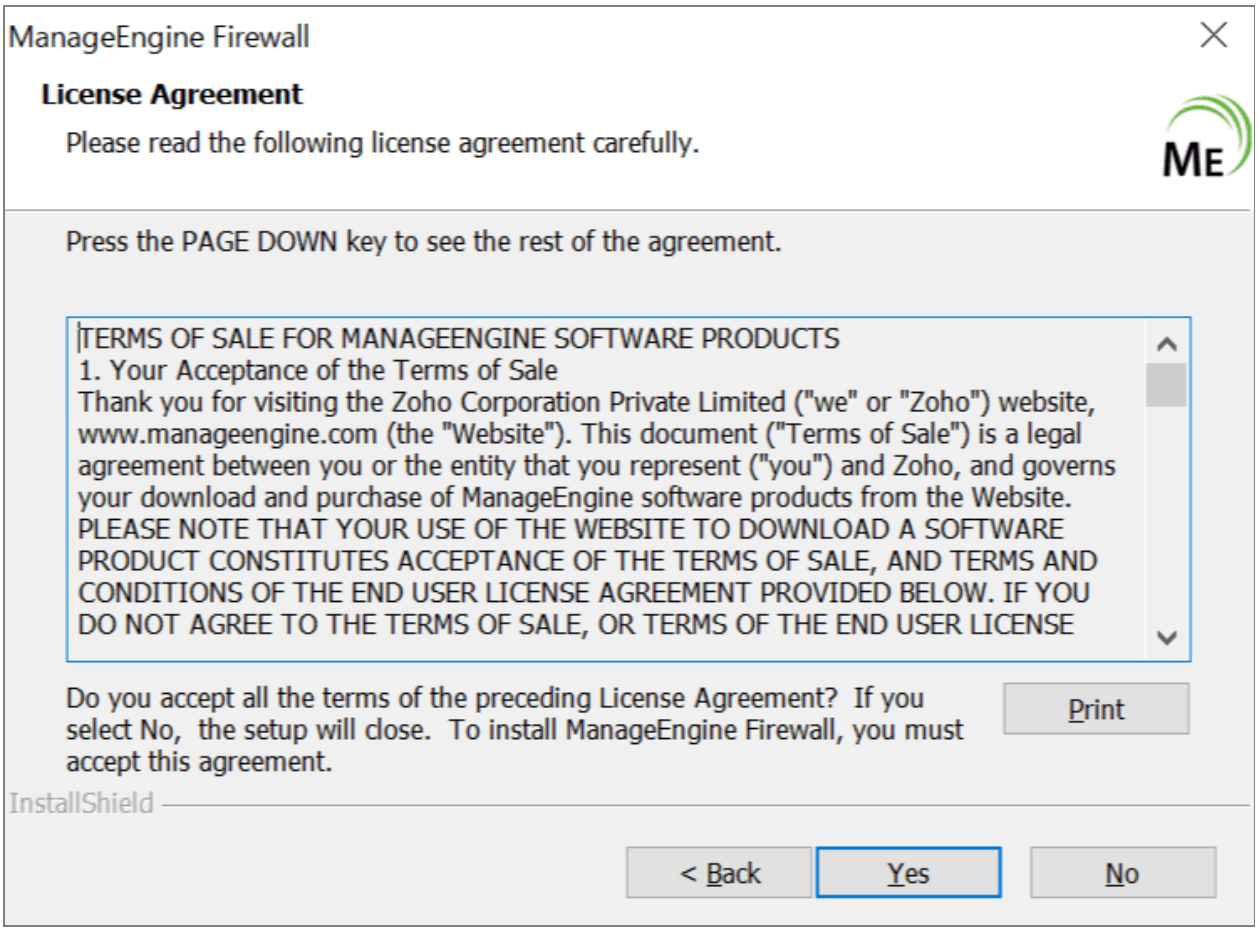
インストーラーファイルをダウンロード後、
以下の手順で、Windows環境にFWAをインストールします。

1. インストーラーファイル「ManageEngine_FirewallAnalyzer_64bit.exe」を、インストールサーバーに配置

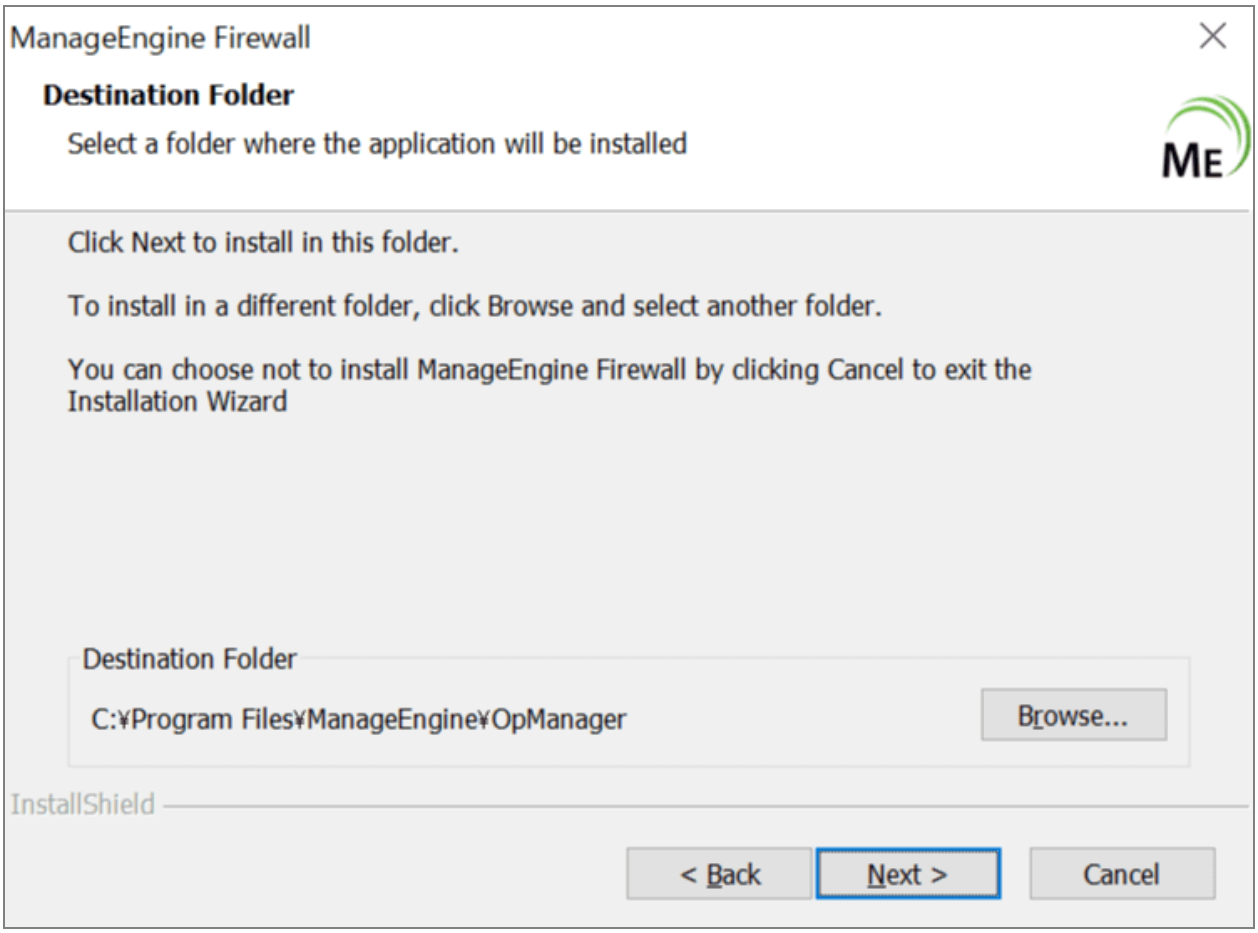
2. 右クリックから管理者権限で実行
   以下、インストールウィザードに沿ってインストールを行います。



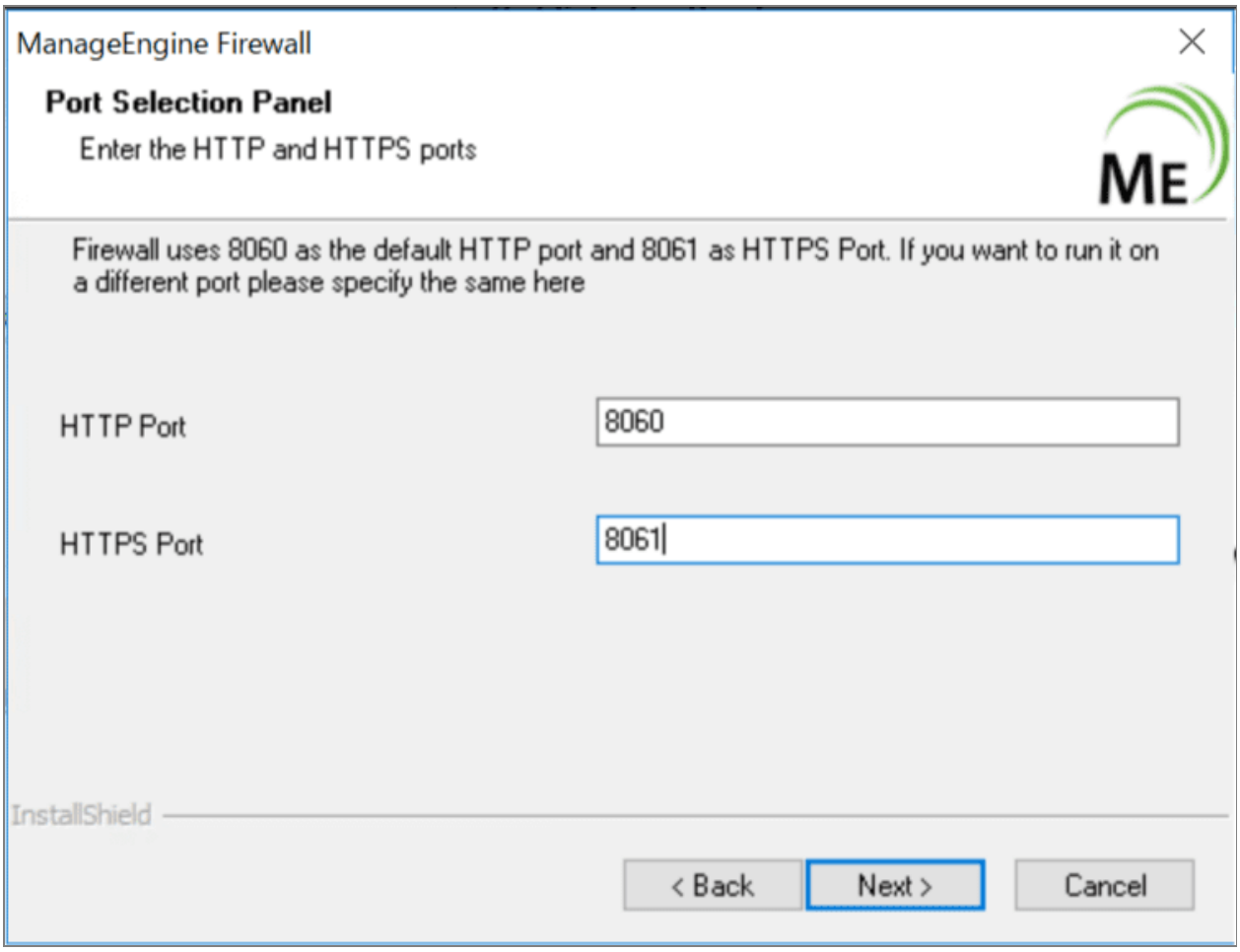
3. ライセンス条項（英語）を承諾後、［Yes］をクリック



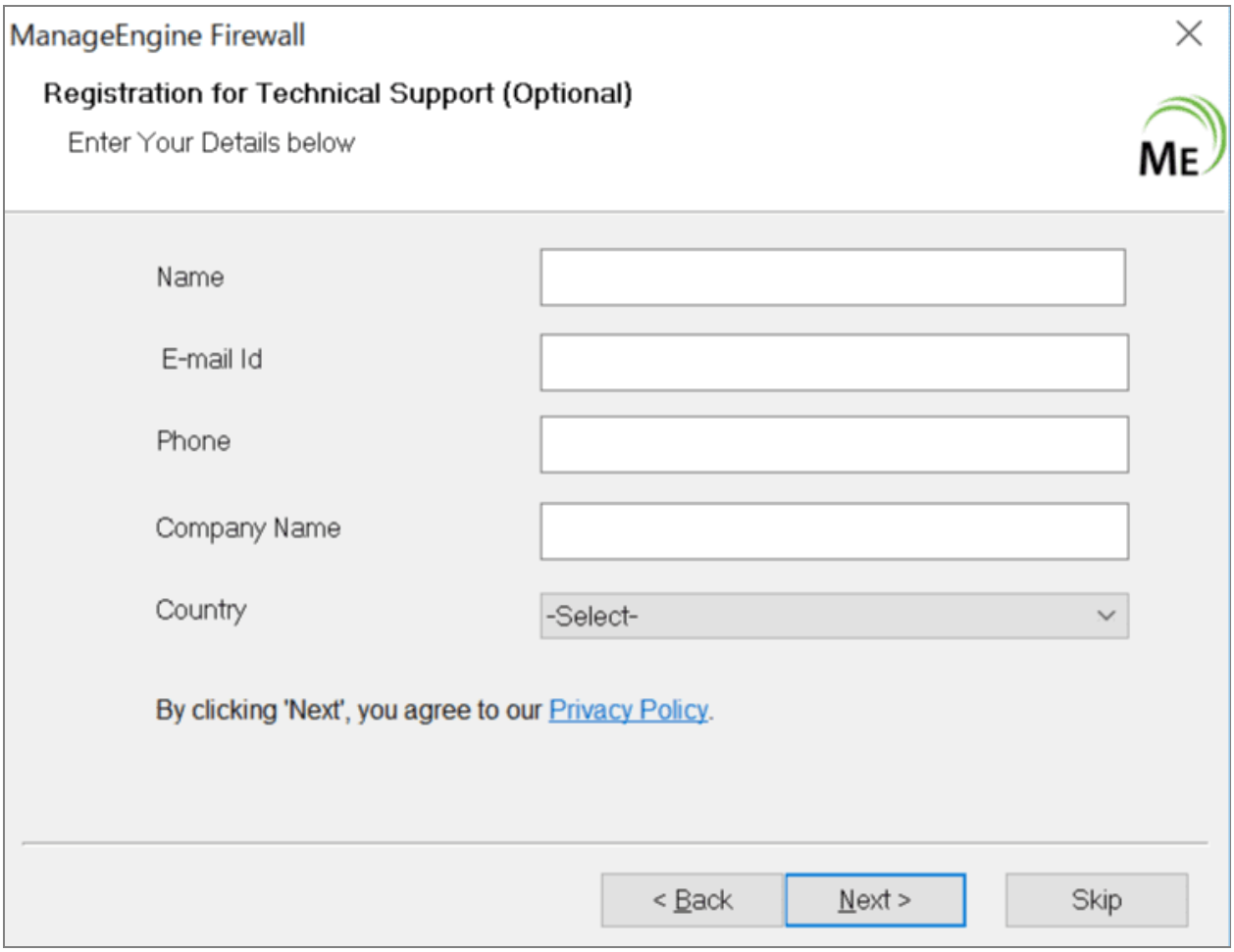
4. インストールディレクトリパスを指定
   デフォルトでは、「C:\Program Files\ManageEngine\OpManager」にインストールされます。



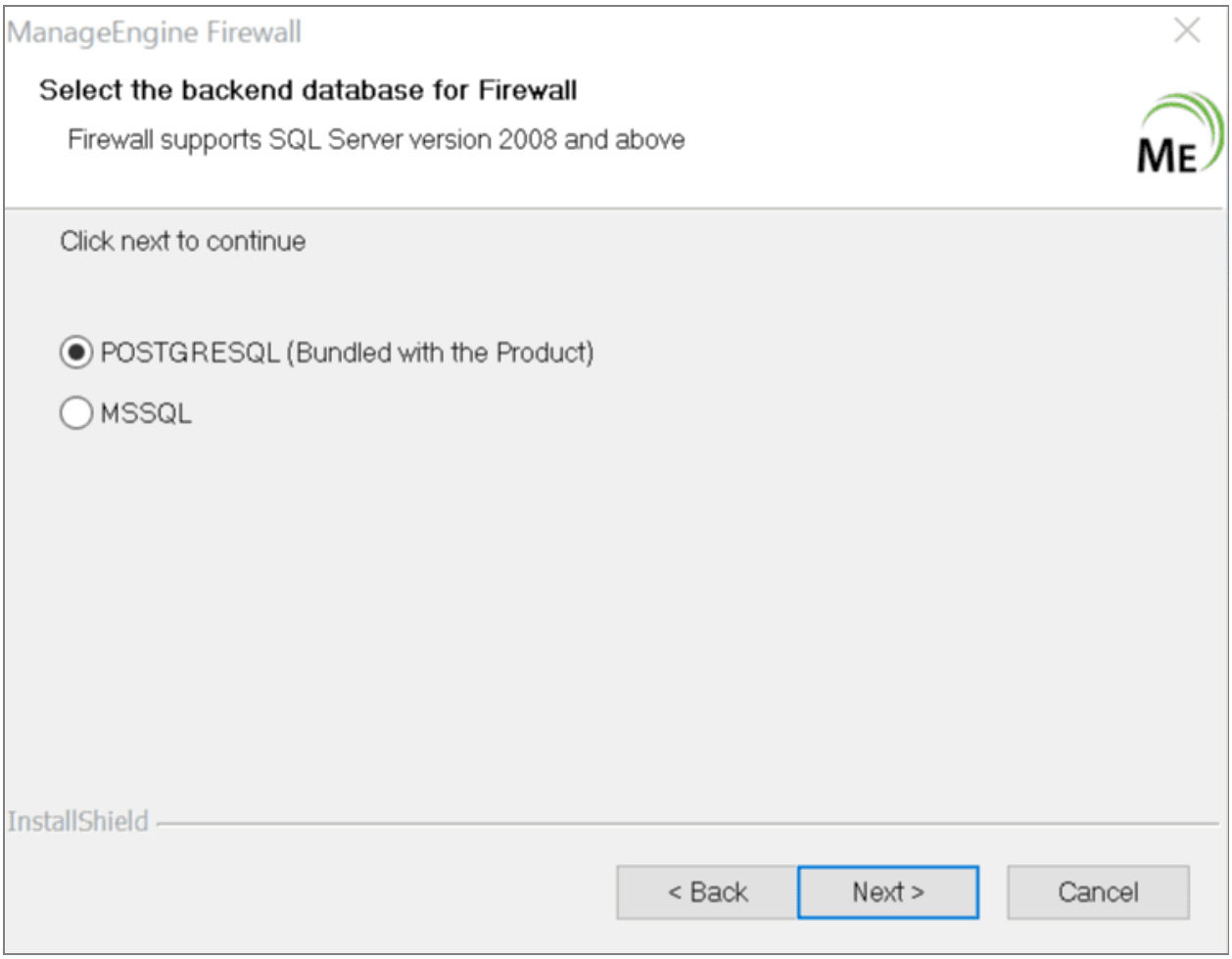
5. WebUIに接続するためのWebサーバー用ポート番号を指定
   デフォルトポート番号：8060（HTTP）、8061（HTTPS）



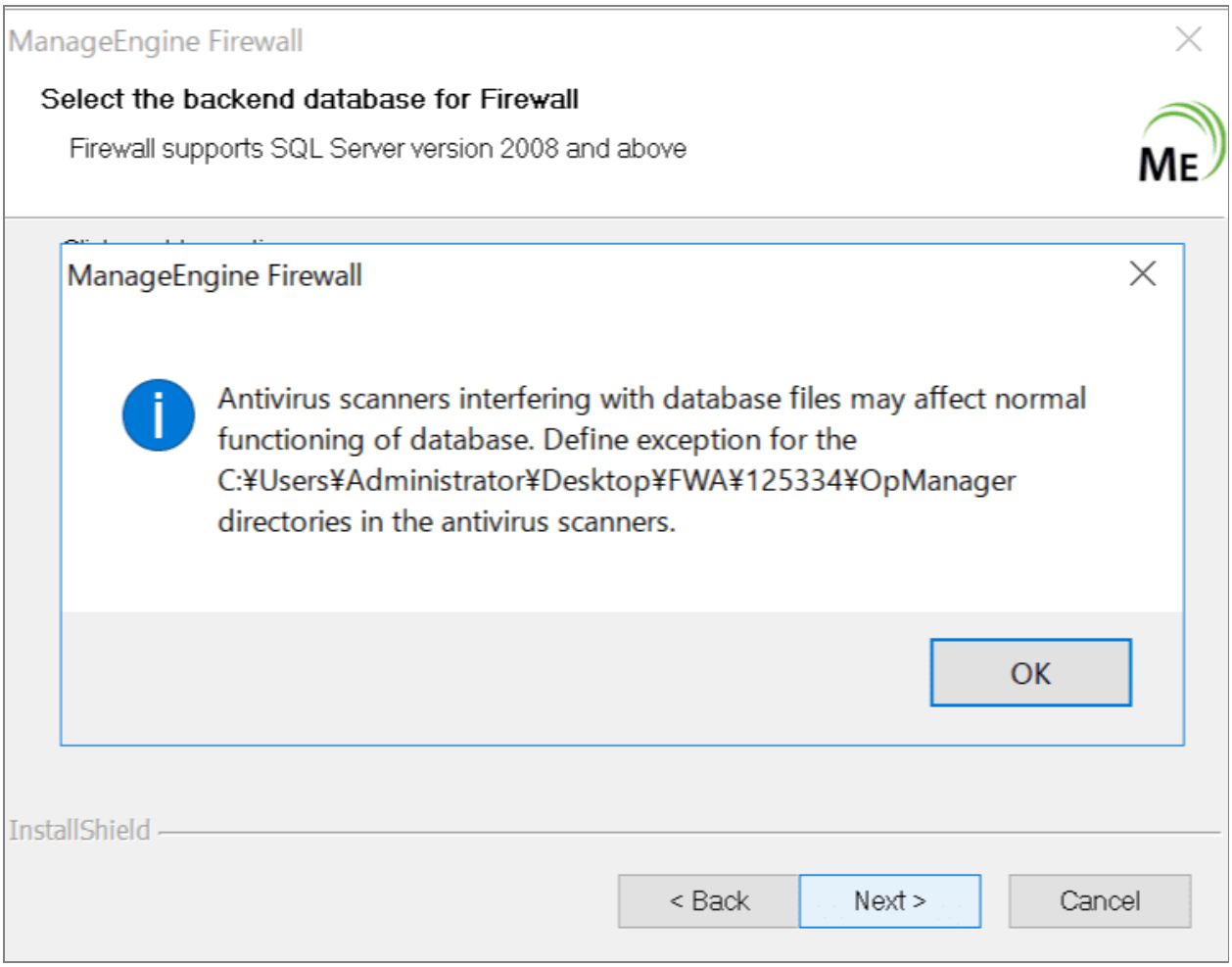
6. お客様情報（Registration for Technical Support）を入力
※スキップ可



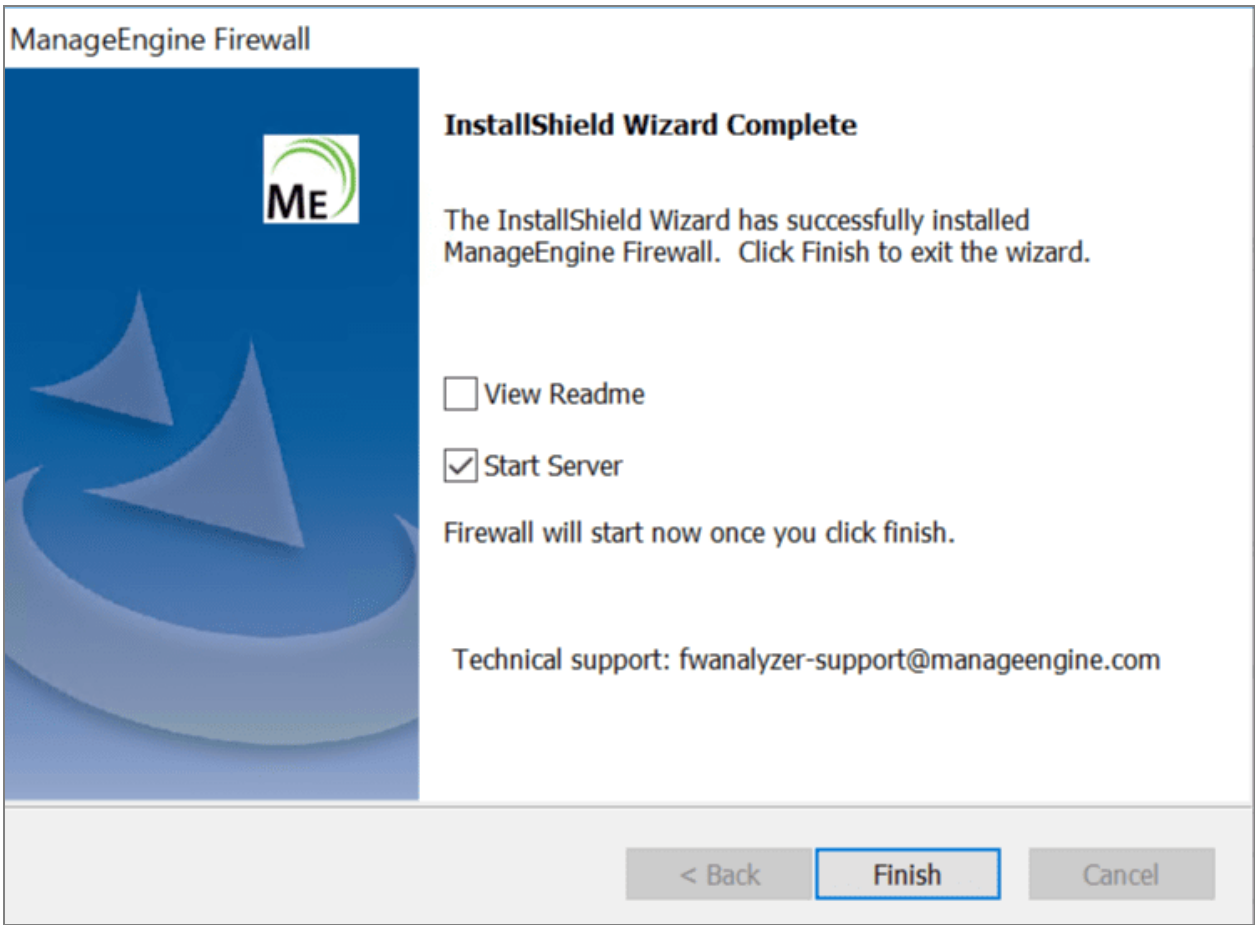
7. 使用するデータベースを選択し、［Next］をクリック
   FWAには、PostgreSQLがバンドルされています。
   ※MS SQLを選択する場合、お客様の方で別途ご用意してください。



8. アンチウイルスソフトに関するダイアログを確認
   インストールサーバー上で、アンチウイルスソフトやバックアップソフトを使用する場合、データベースの動作に影響を及ぼす可能性があるため、インストールディレクトリ「ManageEngine」全体をアンチウイ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。



9. ［InstallShield Wizard Complete］が表示されると、インストール完了です。
［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FWAが起動します。



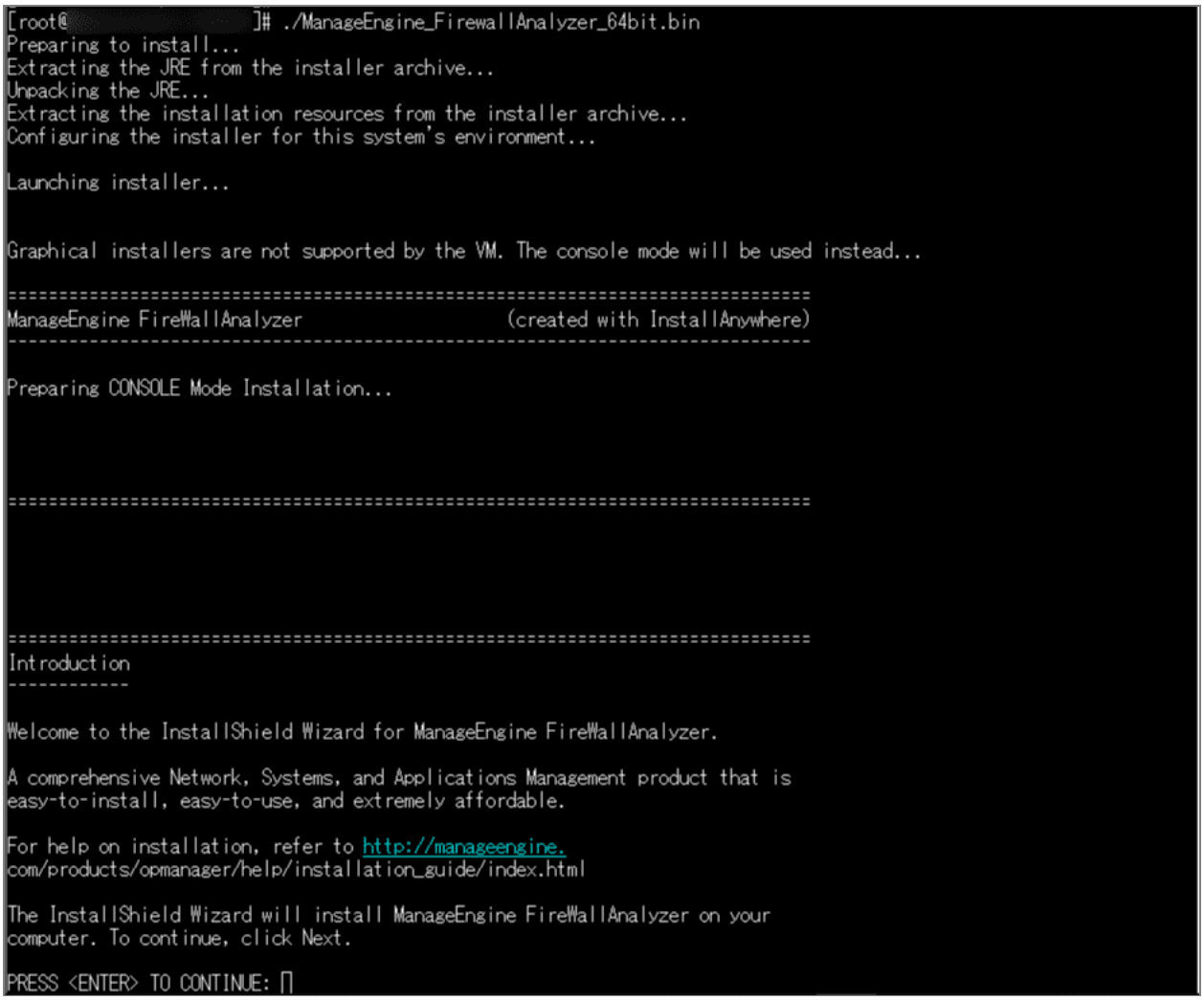
3.3 インストール手順（Linux）

インストーラーファイルをダウンロード後、
以下の手順で、Linux環境にFWAをインストールします。

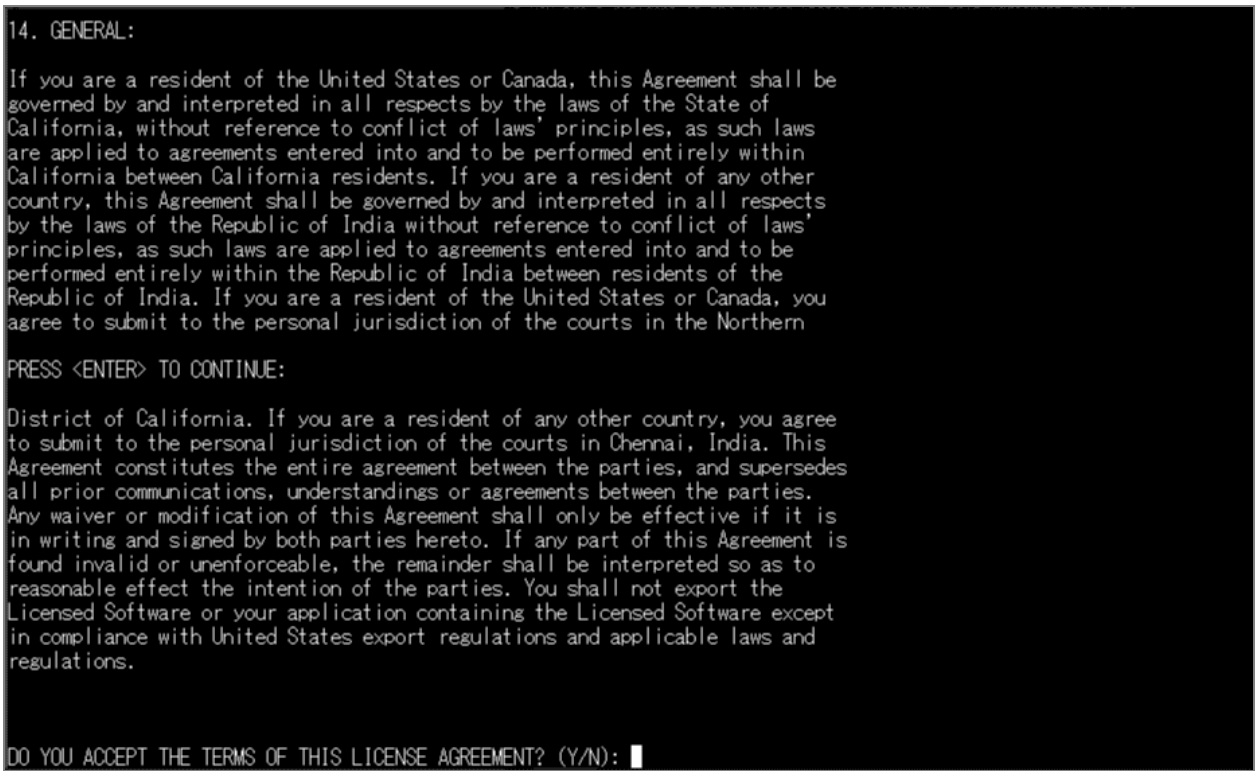
1. インストーラーファイル「ManageEngine_FirewallAnalyzer_64bit.bin」を、インストールサーバーに配置

2. 以下のコマンドを参考に、インストーラーファイルに実行権限を付与
   コマンド：chmod a+x <file-name>

3. 以下を実行し、インストールを開始
   ./ManageEngine_NetworkConfigurationManager_64bit.bin

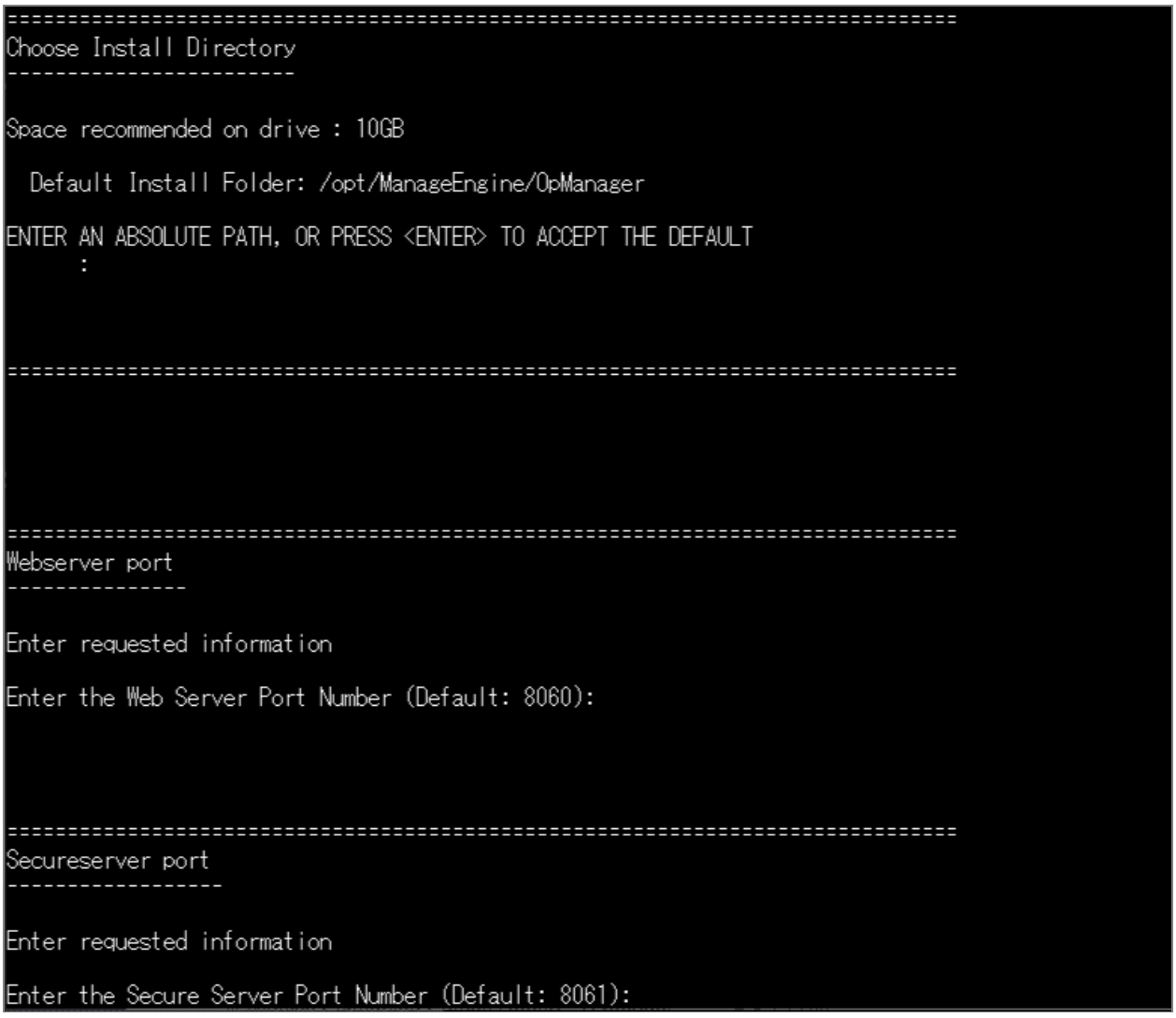


4. ライセンス条項（英語）を確認後、［Y］を入力して続行

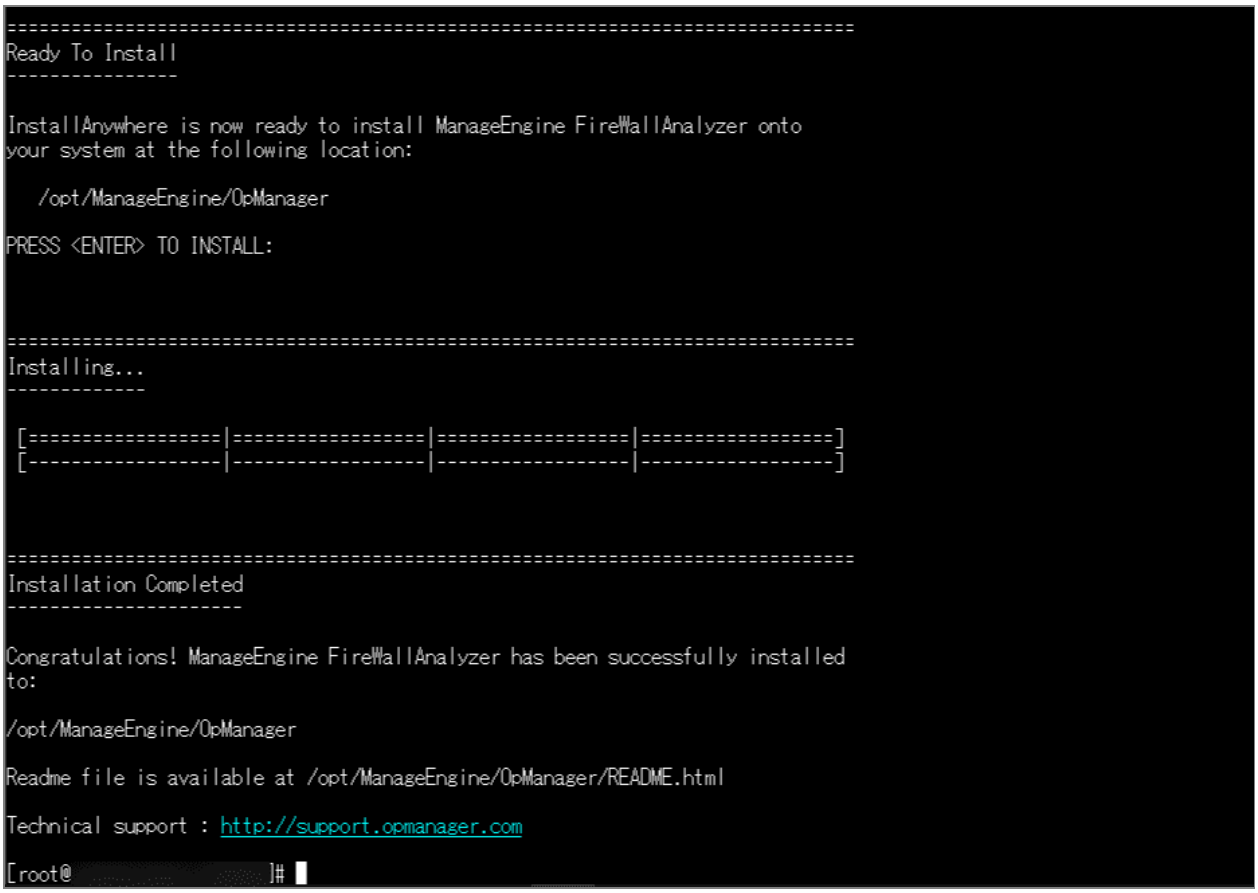


5. お客様情報（Registration for Technical Support）を任意に入力
   ※［N］を入力し、スキップ可

6. インストールディレクトリパスとWebUIに接続するためのWebサーバー用ポート番号を指定
   ・デフォルトパス：/opt/ManageEngine/OpManager
   ・デフォルトポート番号：8060（HTTP）、8061（HTTPS）



7. インストール情報を確認し、Enterをクリック
「Firewall Analyzer has been successfully installed」が表示されると、インストール完了です。



3.4 アンインストール手順

起動停止方法は、以降の「4起動と停止」をご参照ください。

Windowsの場合

以下の手順で、アンインストールを実施します。

1. FWA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 Firewall 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、インストールディレクトリ「ManageEngine」を削除

※インストールディレクトリ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。

Linuxの場合

以下の手順でアンインストールを実施します。

1. FWAを停止
2. インストールディレクトリ「ManageEngine」を削除

4 起動と停止

4.1 起動、停止に関する注意事項

- 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FWAを停止した上で実施するようお願いします。
- 製品が停止されていない状態でのサーバー停止は、製品データベースの破損につながる恐れがあります。
- アプリケーション起動/停止、サービス起動/停止は、いずれか1つの方法で実施してください。
  アプリケーション起動を実施した場合には、アプリケーション停止を、
  サービス起動を実施した場合には、サービス停止の実施をお願いします。

4.2 Windows（起動）

※タスクマネージャーで、以下のプロセスが稼働していないことを事前に確認してください。

・java.exe
・wrapper.exe
・postgres.exe
・FirewallAnalyzer TrayIcon / OpManager TrayIcon

アプリケーション起動

1. コマンドプロンプトを管理者権限で起動
2. FWAインストールディレクトリ/bin/に遷移
3. 「run.bat」を実行
   モジュールの読み込みが開始されます。

読み込みが完了すると、以下のようなメッセージが表示されます。

> Server started in :: ［37028 ms］
> Connect to: ［http://localhost:8060］

HTTPSによる接続の場合は、以下のメッセージが表示されます。

> Server started in :: ［37028 ms］
> Connect to: ［https://localhost:8061］

サービス起動

インストール手順に沿ってインストールすると、FWAはWindowsサービスとして自動で登録されます。

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、services.mscより［サービス］を起動
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。

4.3 Windows（停止）

アプリケーション停止

1. コマンドプロンプトを管理者権限で起動
2. FWAインストールディレクトリ/bin/に遷移
3. 以下2つのコマンドを順に実行
   shutdown.bat
   stopPgSQL.bat

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、services.mscより［サービス］を起動
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
・FirewallAnalyzer TrayIcon / OpManager TrayIcon

4.4 Linux（起動）

アプリケーション起動

1. 管理者権限（root）で、インストールサーバーにアクセス
2. FWAインストールディレクトリ/bin/に遷移
3. 「./run.sh」を実行
   モジュールの読み込みが開始されます。

読み込みが完了すると、以下のようなメッセージが表示されます。

```
Server started in :: ［37028 ms］
Connect to: ［http://localhost:8060］
```

HTTPSによる接続の場合は、以下のメッセージが表示されます。

```
Server started in :: ［37028 ms］
Connect to: ［https://localhost:8061］
```

サービス起動

以下の手順で、サービス登録および起動を行います。

1. 管理者権限（root）で、インストールサーバーにアクセス
2. FWAインストールディレクトリ/bin/に遷移
3. 以下のコマンドを実行し、サービスとして登録
   ./linkAsService.sh
4. 以下のコマンドを参考に起動
   systemctl start OpManager.service

起動後のステータスは、以下のコマンドで参照します。
systemctl status OpManager.service

4.5 Linux（停止）

アプリケーション停止

1. 管理者権限（root）で、インストールサーバーにアクセス
2. FWAインストールディレクトリ/bin/に遷移
3. 以下2つのコマンドを順に実行
   ./shutdown.sh
   ./stopPgSQL.sh

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. 以下のコマンドを参考に停止
   systemctl stop OpManager.service

停止後のステータスは、以下のコマンドで参照します。
systemctl status OpManager.service

5 初期設定

5.1 Webクライアントへのアクセス

FWAを起動後、Webクライアントへアクセスします。

1. 「2.3 Webブラウザー要件」に記載のブラウザーを開き、以下のいずれかのURLでアクセス
   http://<ホスト名/サーバーIPアドレスまたはlocalhost>:8060
   https://<ホスト名/サーバーIPアドレスまたはlocalhost>:8061
   ※「8060」および「8061」はデフォルトのポート番号です。
2. 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
   デフォルト：admin/admin

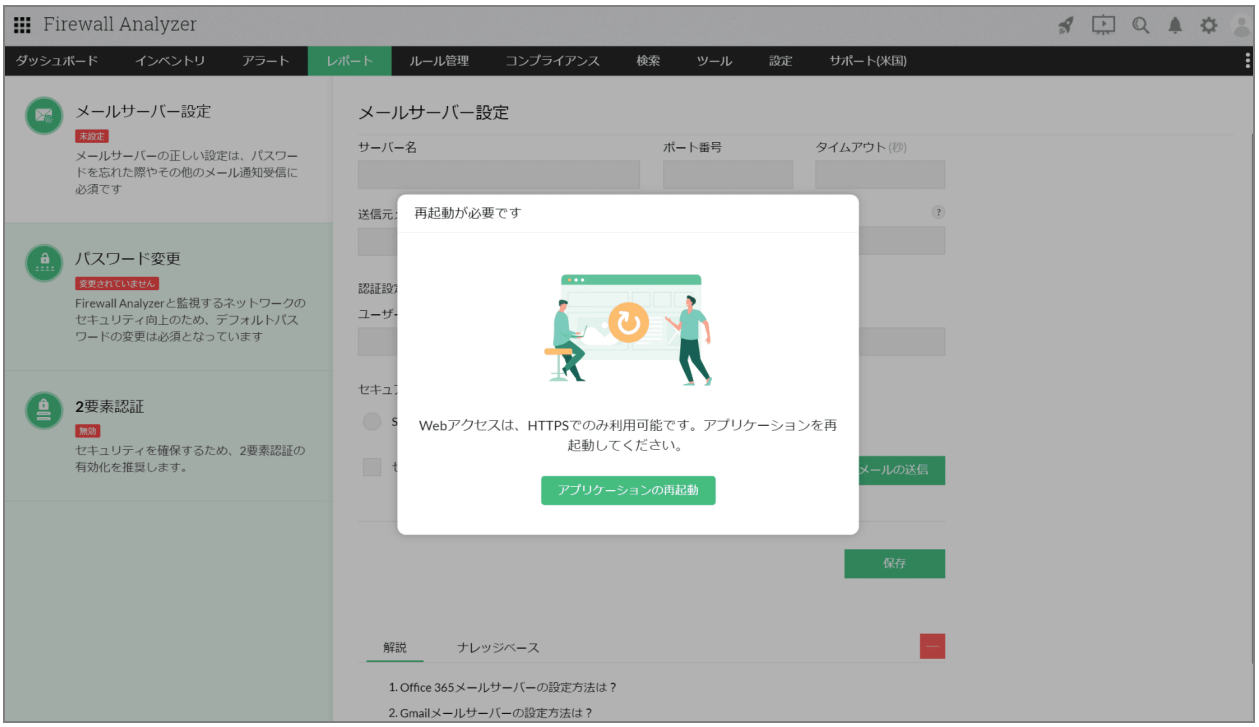
5.2 ライセンス適用（保守ユーザー向け）

FWA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。

ライセンスファイルを受領後、以下の手順でライセンス適用を行います。

1. FWA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］をクリックし、適用

ライセンスファイルを初めて適用すると、HTTPSの有効化および反映のための再起動を強制するメッセージが表示されます。［アプリケーションの再起動］をクリックし製品を再起動後、HTTPSを使用して製品UIにアクセスしてください。



再起動後、メールサーバー設定、adminユーザーのデフォルトパスワードの変更、2要素認証の有効化を推奨する画面が表示されます。

その後、画面右上のシルエットアイコンの［製品］タブでご契約情報（ライセンスタイプ、会社名、監視可能装置数、有効期限等）を確認してください。

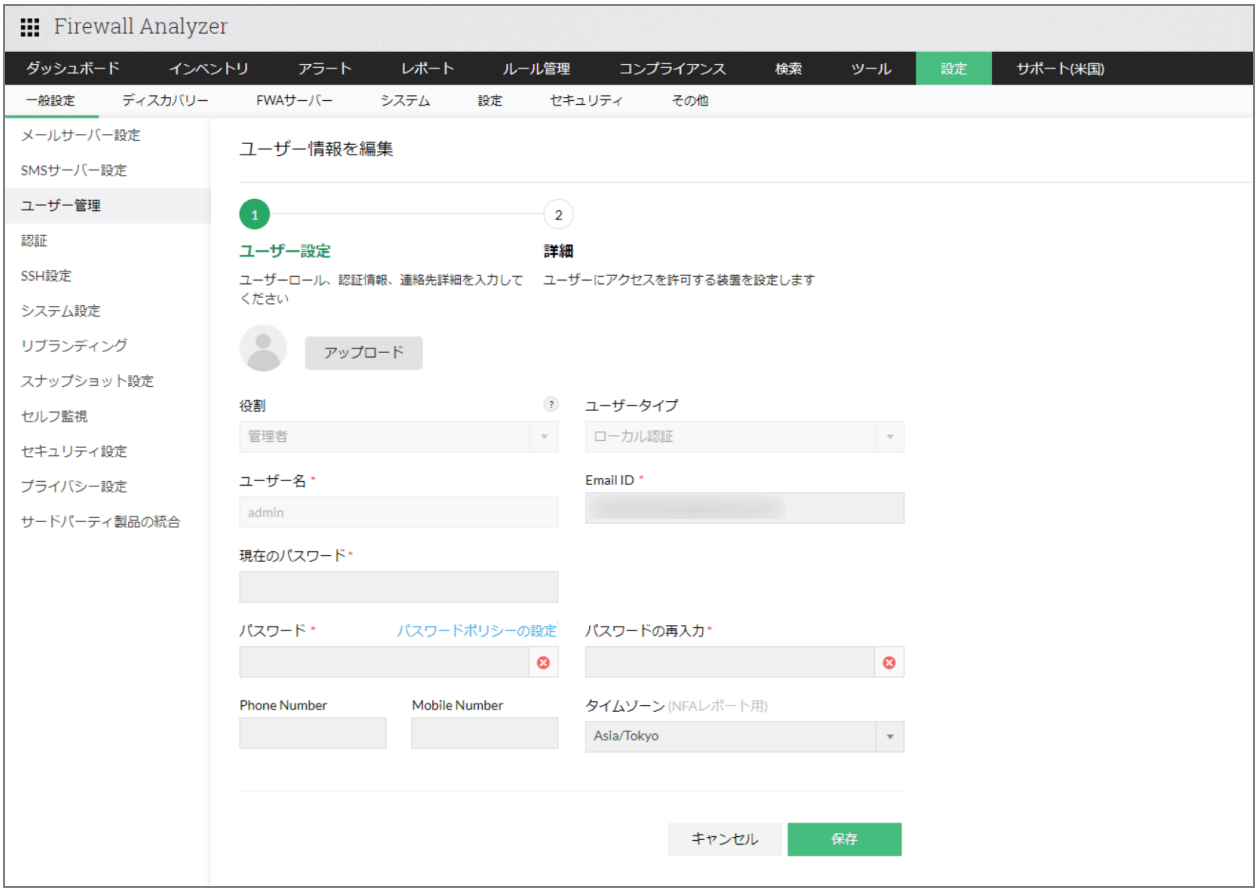
・ご契約内容およびライセンス発行に関するご不明点は、当社ライセンス担当窓口までご連絡ください。
連絡先：jp-license@zohocorp.com
・［設定］→［一般設定］→［セキュリティ設定］→［SSL設定］でHTTPS接続を無効化することができます。無効化後、製品を再起動します。

5.3 ログインパスワードの更新とメールサーバー設定

FWAにログイン後、adminユーザーアカウントのログインパスワードの更新とメールサーバーの設定を実施します。
※保守ユーザーの場合、ライセンスファイルを適用後に以降の設定が強制されます。

ログインパスワードの変更について

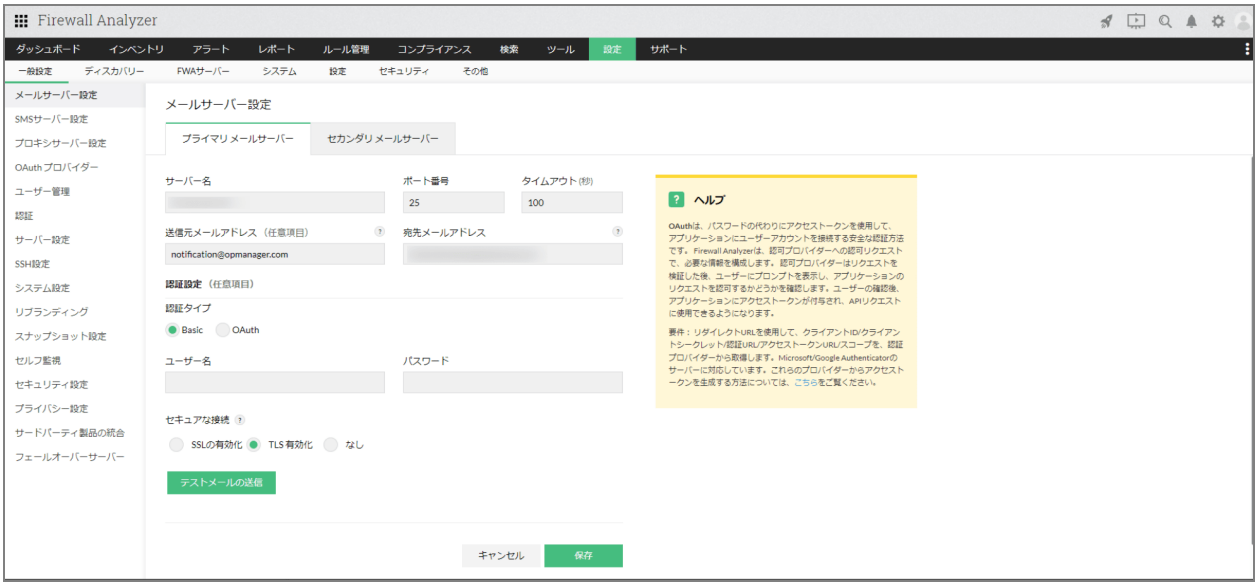
［設定］→［一般設定］→［ユーザー管理］→［ユーザー］画面でadminユーザーをクリックし、新規のパスワードを設定してください。



※評価版をご利用の場合、デフォルトパスワードを変更せず7日間以上ログインしていないと、アカウントがロックされログインできなくなります。

メールサーバー設定について

［設定］→［一般設定］→［メールサーバー設定］画面で、ご利用環境のメールサーバーを設定します。
［テストメールの送信］オプションより、設定したメールサーバーの有効性を確認するためのテストを行うことができます。



■メールサーバーを設定する目的
・定期的なレポートファイルをメールで受信
・特定の条件に該当するログを検知した際のアラートメール通知
・ログインパスワードを失念した場合、ログイン画面の［パスワードを忘れた場合］より、指定したメールアドレス宛にパスワードリセット用リンクを通知

■保守ユーザーの場合
ライセンスファイルを適用後、メールサーバー設定およびパスワード更新専用の画面が自動で表示されます。

5.4 装置登録

FWAに装置を登録する方法は以下の2つがあります。

- FWAにsyslogを直接転送

管理対象装置のsyslog転送先として、FWAのインストールサーバーを指定します。

- ファイルインポート
  管理対象装置のsyslogファイルをインポートします。

FWAがログを受信後、［インベントリ］→［装置］画面に自動で装置が追加されます。
※新規インストール後はUIにアクセスすると、装置追加方法のポップアップが表示されますが、上記1つ目の方法による装置追加を推奨しています。

5.4.1　FWAにsyslogを直接転送

管理対象装置からsyslogを直接転送する場合、以下の2点を設定します。

- syslogサーバー設定（FWA側の設定）
- syslog転送の設定（管理対象装置側の設定）

FWAのsyslogサーバー設定は以下の手順で実施します。

1. ［設定］→［FWAサーバー］→［syslogサーバー］を表示
2. 画面右上の［追加］をクリック
3. 任意のプロファイル名、使用するsyslog用ポート番号を入力
4. 設定を保存後、プロファイル名、ポート番号が［syslogサーバー］一覧に追加されることを確認

> ステータスが［アップ］になっていることを確認してください。［ダウン］の場合、サーバー上で既にポートが占有されている状態のため、ポートの開放または別ポート番号の追加が必要です。

その後管理対象装置側で、syslog転送先（FWAのインストールサーバー/ポート番号）を設定します。
以下のページでは各ベンダーごとに参考となる設定内容を記載していますが、
コマンドや設定内容の詳細については、ご利用のベンダー様にご確認ください。

・管理対象装置の設定
https://www.manageengine.jp/products/Firewall_Analyzer/help/firewall-devices_configuration.html

> ※サードパーティベンダーのsyslogサーバーを中継して転送する構成は、弊社では推奨していません。FWAで問題が発生した際の調査状況に応じて、それ以上の調査が叶わず、FW装置からFWAへの直接転送（弊社推奨構成）をご案内する場合がございますので、あらかじめご了承ください。

5.4.2　ファイルインポート

ログ転送の他、対象装置のログファイルをインポートして取り込む方法があります。
以下の手順でログファイルをインポートします。

1. ［設定］→［システム］→［ログファイルのインポート］を表示
2. 画面右上の［ログのインポート］をクリック
3. 以下のオプションよりインポートタイプを選択し、インポートを実施
   ・ローカルホスト
   ・リモートホスト

ローカルホスト

FWAに接続している端末上（インストールサーバー含む）にログファイルが存在する場合、本オプションよりインポートを実施します。

ローカルホスト画面では、以下の3つのオプションから選択します。

- ファイル

項目	説明

ファイルの場所	ローカル内に保管されているファイルの場所を指定します。 テキストファイルまたはZipファイルをインポート可能です。 ※ファイルサイズ：最大1GB
未解析/ジャンクレコードは無視する	FWAで解析不可なログが含まれている場合、そのレコードはスキップし、解析可能なレコードのみを参照します。
次を仮想ファイアウォールとする（※）	仮想ファイアウォールと物理ファイアウォールを分ける際に使用します。 チェックがない場合、インポートされる装置は物理装置として識別されます。
ログファイルを既存の装置にマッピング	インポート対象の装置がFWAに既に追加されている場合、対象装置にマージするようインポートします。

- スケジュール

項目	説明
ファイルの場所	ローカル内に保管されているファイルの場所（パス含む）を指定します。
時間間隔（分）、開始	ファイルの参照間隔と開始時刻を指定します。
動的にファイル名を変更する	日時等、インポート対象のファイル名が動的に変化する場合にチェックを入れ、ファイル名の変更パターンを入力します。
未解析/ジャンクレコー	FWAで解析不可なログが含まれている場合、そのレコードはス

ドは無視する	キップし、解析可能なレコードのみを参照します。
次を仮想ファイアウォールとする（※）	仮想ファイアウォールと物理ファイアウォールを分ける際に使用します。 チェックがない場合、インポートされる装置は物理装置として識別されます。
ログファイルを既存の装置にマッピング	インポート対象の装置がFWAに既に追加されている場合、対象装置にマージするようインポートします。

- ディレクトリ

項目	説明
ファイルの場所	ファイルが保管されているディレクトリパスを指定
未解析/ジャンクレコードは無視する	FWAで解析不可なログが含まれている場合、そのレコードはスキップし、解析可能なレコードのみを参照します。
次を仮想ファイアウォールとする（※）	仮想ファイアウォールと物理ファイアウォールを分ける際に使用します。 チェックがない場合、インポートされる装置は物理装置として識別されます。

インストールサーバー上から直接FWAのWebUIにアクセスした場合、［スケジュール］と［ディレクトリ］オプションが表示されます。 リモート端末から接続した場合、これら2つのオプションは表示されません。

リモートホスト

ログファイルがローカル端末上ではなくリモート端末上にある場合、本オプションよりインポートを実施します。

リモートホスト画面では、以下の項目を指定します。

項目	説明
ホスト名/IPアドレス	リモート端末のホスト名もしくはIPアドレスを入力
ユーザー名、パスワード	リモート端末にアクセスするための認証情報を入力
プロトコル	アクセス時のプロトコルを選択 ・FTP ・SFTP/SSH
ポート	プロトコル選択時に自動的にポートが反映されます。必要に応じて変更してください。
時間間隔（分）、開始	ファイルの参照間隔と開始時刻を指定します。
ファイルの場所	リモート端末に保管されているファイルの場所を指定

	※ファイルサイズ：最大2GB
動的にファイル名を変更する	日時等、インポート対象のファイル名が動的に変化する場合にチェックを入れ、ファイル名の変更パターンを入力します。
未解析/ジャンクレコードは無視する	FWAで解析不可なログが含まれている場合、そのレコードはスキップし、解析可能なレコードのみを参照します。
次を仮想ファイアウォールとする（※）	仮想ファイアウォールと物理ファイアウォールを分ける際に使用します。 チェックがない場合、インポートされる装置は物理装置として識別されます。
ログファイルを既存の装置にマッピング	インポート対象の装置がFWAに既に追加されている場合、対象装置にマージするようインポートします。

（※）
［次を仮想ファイアウォールとする］オプションは、VDOMのsyslogファイルをインポートする場合に有効化します。
・FWAに既に装置が追加されている場合
本オプションを有効化し、FWAに追加されている既存装置のIPアドレスを入力してインポートしてください。
・FWAに装置が追加されていない場合
初めにVDOMのsyslogファイルをインポートし装置追加を行います。それ以降は本オプションを有効化の上、追加した装置のIPアドレスを入力してVDOMのsyslogファイルをインポートしてください。

※本オプションを有効化した場合、IPアドレスの入力が必須です。IPアドレスの入力なしにインポートを実施すると、エラーが発生します。
※入力したIPアドレスが、FWAの［インベントリ］画面に存在しない場合、新規装置として追加されます。

5.5 アーカイブ設定

FWAは管理対象装置のログを受信後、インストールディレクトリ内にアーカイブファイルを作成し、定期的にZip化します。
本設定では、受信したログの保存期間やZipファイルの作成間隔を設定します。

・設定画面
［設定］→［システム］→［アーカイブファイル］→［アーカイブ設定］

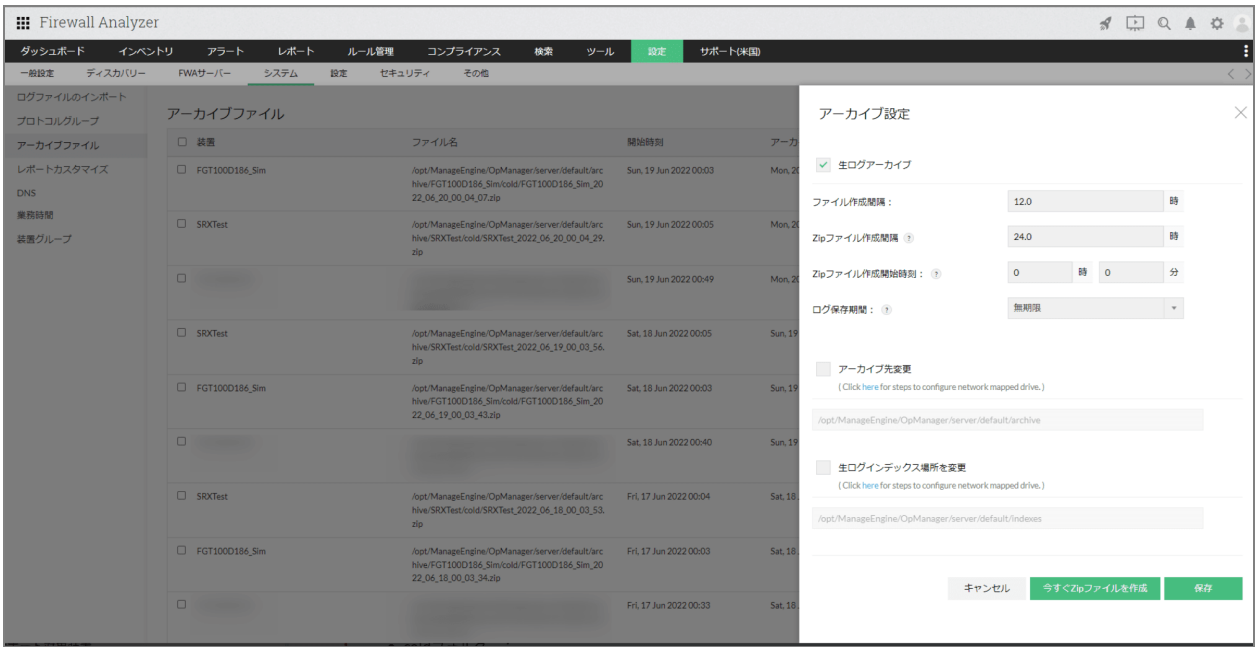
アーカイブ設定画面には、以下の設定項目があります。

項目	説明
ファイル作成間隔	管理対象装置からsyslogを受信し、ログファイルを作成する間隔を指定します。 作成されたアーカイブファイルは、アーカイブ先のhotフォルダーに保存されます。 ※デフォルト：12時間
Zipファイル作成間隔	ディスク容量の圧迫を防ぐために、ログファイルのZip化を行う間隔を指定します。 作成されたZipファイルは、アーカイブ先のcoldフォルダーに保存されます。 ※デフォルト：24時間

Zipファイル作成開始時刻	Zipファイル作成の開始時刻 ※デフォルト：0時0分
ログ保存期間	受信した生ログの保存期間を指定します。 期間：1週間、1か月、2か月、3か月、6か月、1年、無期限 ※デフォルト：無期限 ※本設定は、［設定］→［設定］→［データ保存］の［ログアーカイブ］期間と連動しています。
アーカイブ先変更	生ログのアーカイブファイルの保存先を設定します。 チェックを入れると保存先を変更できます。 デフォルト：ManageEngine/OpManager/server/default/archive
生ログインデックス場所を変更	生ログのインデックスファイルの保存先を設定します。 チェックを入れると保存先を変更できます。 デフォルト：ManageEngine/OpManager/server/default/indexes
今すぐZipファイルを作成	アーカイブ先のhotフォルダーに保存されているアーカイブファイルを、即時的にZip化します

アーカイブ先（archiveフォルダー配下）には、管理対象装置ごとにフォルダーが作成されており、さらに以下の3つのフォルダーが存在します。

・hotフォルダー
ログを受信してからZipファイルが作成されるまでの最新の生ログが保存されます。
・coldフォルダー
hotフォルダーの生ログデータをZip化したZipファイルが保存されます。
・warmフォルダー
データ参照時に、対象期間の生ログデータを一時的に保管します。1日経過するとwarmフォルダーからは削除されます。



6 レポート

FWAでは、ファイアウォールやプロキシサーバーから受信したログを解析し、各種レポートタイプごとに解析データを可視化します。
FWAに実装されている各種レポートタイプについて記載します。

6.1 FWAレポート

［レポート］→［FWAレポート］では、以下のレポートタイプが実装されています。

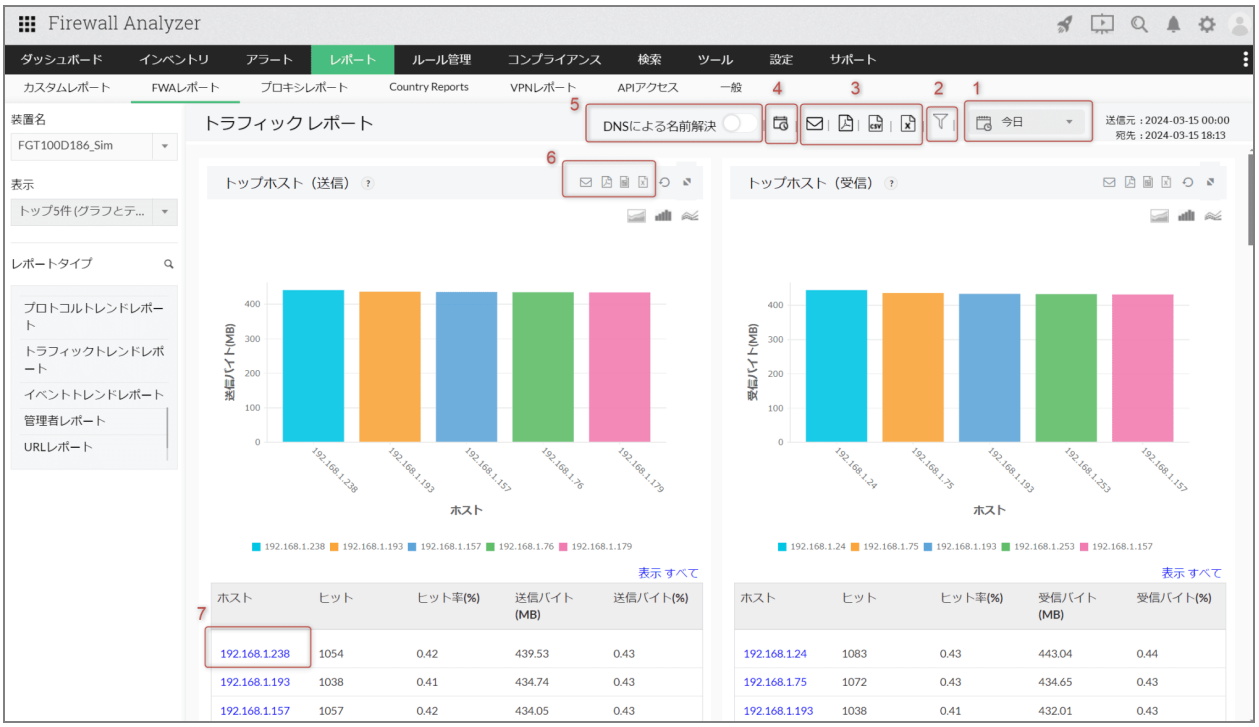
レポートタイプ	説明
トラフィックレポート	ファイアウォールを通過（permit/accept）した送受信トラフィック量に基づいた帯域使用率を表示します。
プロトコル使用レポート	ファイアウォールを通過（permit/accept）してトラフィックを生成しているプロトコルグループの帯域幅使用率を表示します。
Web使用レポート	ファイアウォールを通過（permit/accept）してトラフィックを生成しているプロトコルグループの内、Webプロトコルグループ

	に特化した帯域幅使用率を表示します。
メール使用レポート	ファイアウォールを通過（permit/accept）してトラフィックを生成しているプロトコルグループの内、メールプロトコルグループに特化した帯域幅使用率を表示します。
FTP使用レポート	ファイアウォールを通過（permit/accept）してトラフィックを生成しているプロトコルグループの内、ファイル転送プロトコルグループに特化した帯域幅使用率を表示します。
Telnet使用レポート	ファイアウォールを通過（permit/accept）してトラフィックを生成しているプロトコルグループの内、Telnetプロトコルグループに特化した帯域幅使用率を表示します。
ストリーミング・チャットサイトレポート	ファイアウォールを通過（permit/accept）してトラフィックを生成しているプロトコルグループの内、ストリーミングとチャットサイト通信に関する帯域幅使用率を表示します。 事前に、後述のイントラネット設定を行う必要があります。
イベント概要レポート	ファイアウォールが生成したイベント（重要度）の概要を表示します。
ファイアウォールルールレポート	使用頻度の高いルールや使用されていないルール情報を表示します。
受信・送信トラフィックレポート	インバウンドトラフィック（LANに流入するトラフィック）とアウトバウンドトラフィック（LANから出力されるトラフィック）を分離している場合のトラフィック状況を表示します。 事前に「6.1.1 イントラネット設定」を行う必要があります。
イントラネットレポート	内部ホスト（LAN内部のホスト）からのトラフィック情報を表示します。 事前に「6.1.1 イントラネット設定」を行う必要があります。

インターネットレポート	外部ホスト（LAN外部のホスト）からのトラフィック情報を表示します。 事前に「6.1.1 イントラネット設定」を行う必要があります。
セキュリティレポート	ファイアウォールに設定されているルールによって拒否（Deny）された通信を表示します。
ウイルスレポート	ウイルスに関する通信に特化してログ情報を表示します。
攻撃レポート	攻撃に関する通信に特化してログ情報を表示します。
Spamレポート	Spamに関する通信に特化してログ情報を表示します。
プロトコルトレンドレポート	各プロトコルグループごとに、使用状況のトレンドを時系列で表示します。
トラフィックトレンドレポート	通信量のトレンドを時系列で表示します。
イベントトレンドレポート	イベント数のトレンドを時系列で表示します。
管理者レポート	ファイアウォールのログイン、ログオフ、ログイン拒否に関連するレポートを表示します。
URLレポート	syslogに含まれるURLのカテゴリを取得し、許可、拒否状況をカテゴリ単位で表示します。

FWAレポート画面では、以下の各操作を実行することができます。
以下、トラフィックレポート例

1. 出力日時の変更
   ※トレンドレポートでは、日時指定はできません。
2. 送信元、宛先、プロトコルに関するフィルター設定
   ※画面左上の［装置名］で［すべての装置］を選択した場合は表示されません。
3. レポート全体のPDF、XLSX、CSVファイル出力、メール送信
4. スケジュール出力設定
5. DNSによる名前解決（インストールサーバーからアクセス可能なDNSサーバーにDNS解決を行います）
6. レポート内のウィジェット単位のPDF、XLSX、CSVファイル出力、メール送信
7. 通信の詳細確認（該当ホストやプロトコルを深掘りして、詳細な通信内容を表示します）



6.1.1　イントラネット設定

組織のネットワーク環境におけるIPアドレス（LAN）を、イントラネットとインターネットに区別するための設定を行います。

・設定画面
［設定］→［設定］→［イントラネット］

［イントラネット設定］画面では、FWAに追加されている装置が一覧で表示されます。
装置個別または画面右上の［全装置設定］より、複数装置に一括で設定することができます。

対象装置を指定後、イントラネットとして設定するネットワーク範囲を以下の項目より指定します。

- IPアドレス
  単一のホスト/IPアドレスを指定します。

- IPネットワーク
  特定のネットワークを設定する場合に、IPアドレスと対応するサブネットマスクを指定します。

- IPレンジ
  IPアドレスを範囲指定する場合に、開始と終了のIPアドレス、対応するサブネットマスクを指定します。

6.2 プロキシレポート

プロキシサーバーのアクセスログを、各カテゴリに分けて収集、可視化します。
［レポート］→［プロキシレポート］では、以下の各レポートタイプが実装されています。

レポートタイプ	説明
URLレポート	プロキシサーバーのログに含まれるURLとそのカテゴリ情報をレポート化します。
プロキシ使用レポート	プロキシサーバーのキャッシュとステータスコードの使用情報について表示します。
Webサイト詳細レポート	プロキシサーバー経由でアクセスした、Webサイト、ドメイン、Webページなどの情報を表示します。
トップトーカーレポート	プロキシサーバー経由で通信を行っている上位のホストとユーザー情報（LAN/WAN）を表示します。

［FWAレポート］と同様に、［プロキシレポート］でも以下の各操作を実施します。

1. 出力日時の変更
2. 送信元、宛先、プロトコルに関するフィルター設定
3. レポート全体のPDF、XLSX、CSVファイル出力、メール送信
4. レポート内のウィジェット単位のPDF、XLSX、CSVファイル出力、メール送信
5. スケジュール出力設定
6. DNSによる名前解決（インストールサーバーからアクセス可能なDNSサーバーにDNS解決を行います）
7. 通信の詳細確認（該当ホストやサイトを深掘りして、詳細な通信内容を表示します）

6.3 VPNレポート

収集したVPNログを各カテゴリに分けて可視化します。
［レポート］→［VPNレポート］には、以下の各レポートタイプが実装されています。

レポートタイプ	説明
アクティブVPNユーザー	リアルタイムでVPN通信を行っているアクティブなユーザーを表

レポート	示します。
VPNセッションレポート	VPN通信が発生したユーザーとそのセッション情報を表示します。
トップユーザーレポート	VPN接続の回数（ヒット数）が多いユーザー情報を表示します。
VPN Usageレポート	VPN接続が行われていたアクティブなセッション数を時系列の折れ線グラフとして表示します。
VPN Statusレポート	アクティブVPNユーザーレポートが、指定した期間におけるオンラインのVPN情報（ユーザー名、IP、VPN接続時刻、経過時間）を表示するのに対し、 VPN Statusレポートでは、時間軸のアクティブVPNユーザーのセッション数を表示します。
VPN概要レポート	一定の期間（日、1時間）のVPNセッション数に焦点をあて、 VPN使用状況を表示します。
VPNレポート	ファイアウォール経由のVPN通信に関するユーザー（上位のユーザー、VPN接続失敗ユーザー）や使用統計などの情報を表示します。
VPNトレンドレポート	VPN接続に成功した一定期間のセッション数に関して、折れ線グラフの時系列形式でセッション数を表示します。 ※既にセッションがクローズしているVPNセッションが表示対象です。
アクティブVPNトレンドレポート	VPNトレンドレポートと同様、VPN接続に成功した一定期間のセッション数に関して、折れ線グラフの時系列形式でセッション数を表示します。 ※VPNトレンドレポートの場合、既にセッションがクローズして

	いるVPNセッションを表示対象としますが、本レポートの場合、一定の時間帯でVPNセッションがアクティブなセッション数を表示します。

6.4 カスタムレポート（スケジュールレポート）

FWAに実装されている各種レポートタイプをスケジュールで定期出力します。

6.4.1　スケジュール設定方法

以下の手順で設定します。

1. ［レポート］→［カスタムレポート］→［レポートプロファイル］右上の［追加］をクリック
2. プロファイル名を任意に入力し、対象装置を選択
3. レポートフィルターを任意に指定
4. 出力するレポートタイプを選択
   ※［ウィジェットのカスタマイズ］で［はい］を選択することで、レポート内の任意のウィジェットを指定することができます。

5. スケジュールを［有効］にし、レポートタイプ（PDF、CSV、XLS）を選択
6. レポートを生成するスケジュール（毎時、日次、週次、月次、1回、カスタム）を設定
7. メール通知を任意に設定
   ※メール通知を行う場合には、事前に「5.3メールサーバー設定」を設定してくだ

さい。

8. 設定を保存
   ※保存後、レポートプロファイル一覧に、設定したプロファイルが追加されていることを確認してください。

・設定したスケジュールは、［レポート］→［カスタムレポート］→［スケジュールリスト］で、ステータスを有効化/無効化できます。

・レポートファイルの保存先は、［設定］→［その他］→［ユーザー設定］→［スケジュールレポート保存場所］で指定します。

6.4.2　レポートフィルター

カスタムレポートでプロファイルを作成する際に指定するフィルターを設定します。
フィルター内容は、包含または除外から選択し、プロトコル、送信元/宛先IPアドレス、イベント、ユーザー情報を条件に指定します。
レポートフィルター設定により、出力するレポートに含める情報やレポートから除外する情報を指定します。

レポートフィルター機能は、カスタムレポートの他に、FWAレポート、プロキシレポート、VPNレポートの画面上からも指定できます。

6.4.3　レポートタイプ

各種レポートに含まれる情報（プロトコル、URL、イベント、VPN、ルール、攻撃、ウイルス、Spam、ホスト、サーバー）に関して、必要な情報のみを選択し、レポートに出力することができます。

レポートの表示形式は、グラフとテーブル、グラフ、テーブルから選択することができ、グラフを選択した場合には、さらに円グラフや棒グラフを選択することができます。

作成したレポートタイプは、カスタムレポートのレポートプロファイル追加画面のレポート一覧に表示されます。

7 アラートプロファイル設定

セキュリティ対策や通信の監視を目的に、条件に合致したログイベントが発生した際に管理者にアラートを通知します。

7.1 通知テンプレートの作成

アラート発生時のアクションを事前にテンプレートとして定義し、アラートプロファイルを作成する際に使用します。

1. ［設定］→［その他］→［通知テンプレート］右上の［追加］をクリック
2. 作成するテンプレートタイプを選択
   メール、チャット（Slack連携）、syslogプロファイル、トラッププロファイル等
3. 通知先など、各テンプレートタイプに応じた必要項目を入力し、保存
   ※以下はメール通知の設定例です。

保存した通知テンプレートは、［通知テンプレート］画面の一覧に追加されます。

7.2 アラートプロファイルの作成

通知テンプレートを作成後、以下の手順でアラートプロファイルを作成します。

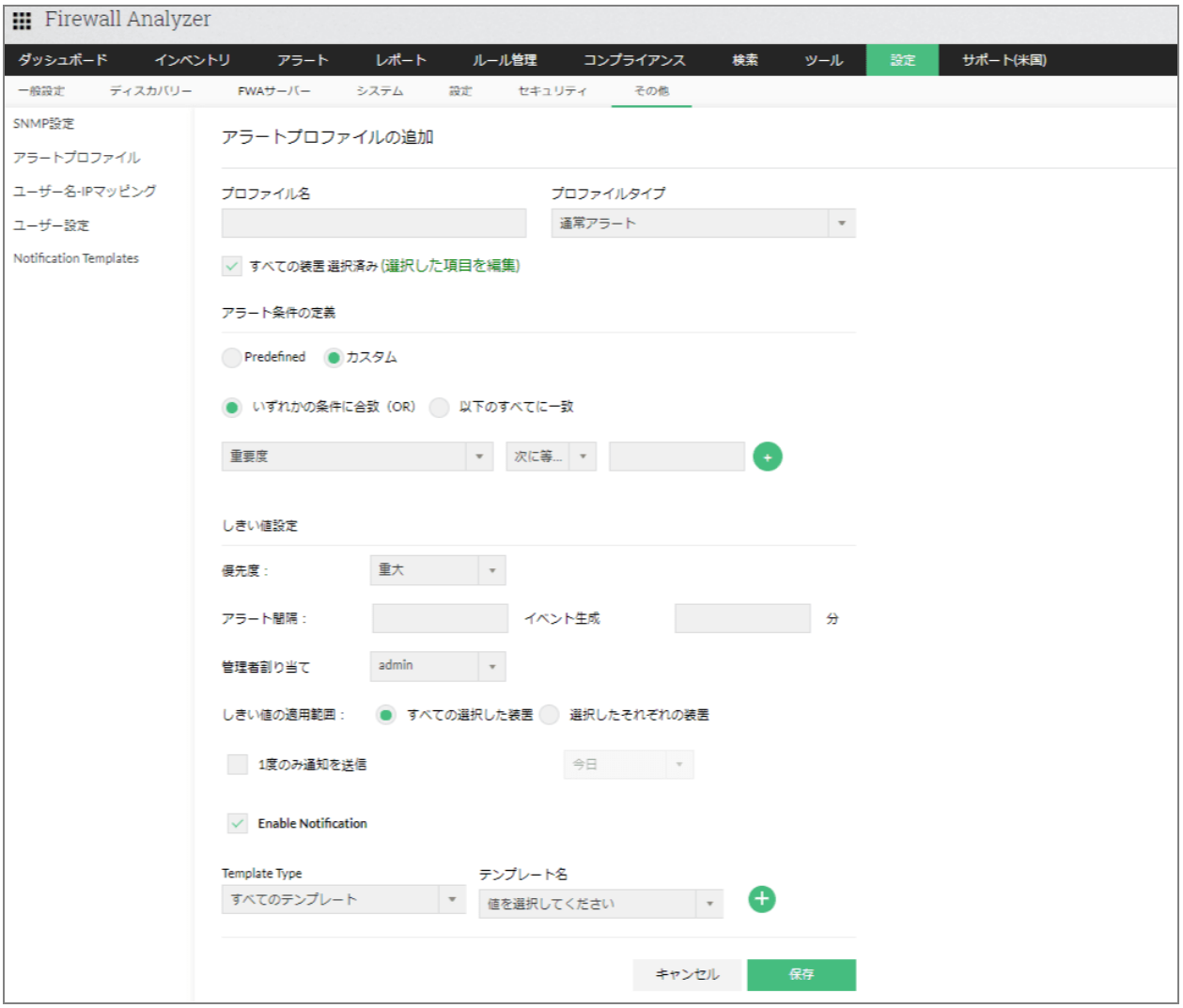
1. ［設定］→［その他］→［アラートプロファイル］右上の［追加］をクリック
2. プロファイル名を任意に入力
3. プロファイルタイプを以下から選択
   ・通常アラート
   ・異常アラート
   ・帯域
   ※各プロファイルタイプについては、後述の内容をご確認ください。
4. プロファイルを適用する対象装置を選択
   ※デフォルトではすべての装置が選択されています。
5. ［アラート条件の定義］で以下のいずれかを選択

・カスタム：任意の条件を指定します。
・事前定義：各種イベントタイプ（VPN、重要度、攻撃、セキュリティ、ウイルス、SPAM、管理）に対して、事前にアラート条件を実装しています。

6. ［しきい値設定］の項目でアラートの優先度、アラート間隔を設定
7. 1度のみ通知を送信
   アラート発生時に毎回通知を行うか、任意のタイミングで1度のみ通知するか選択します。
8. 通知を有効にする
   ［通知テンプレート］機能で作成したテンプレートを選択します。

7.3 通常アラート

アラート条件を任意にカスタマイズして設定します。
※前述、「アラートプロファイルの作成」に記載の内容と同様の手順で作成します。



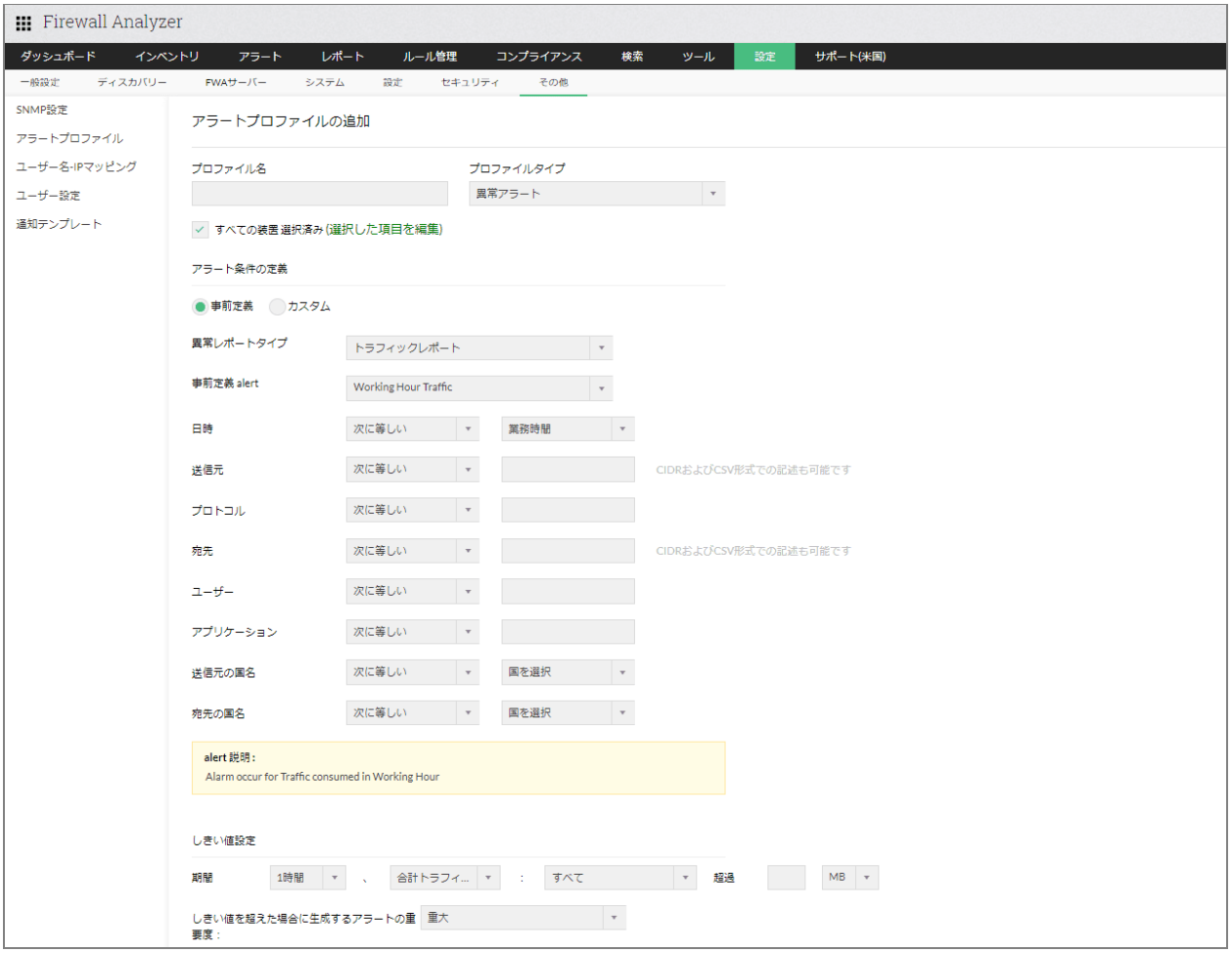
7.4 異常アラート

NBA（Network Behavior Analysis：ネットワーク動作解析) のようにトラフィックの何らかの異常を検知する場合に選択します。
前述、「アラートプロファイルの作成」の手順4以降の流れを記載します。

1. 対象装置を選択
2. ［アラート条件の定義］で以下の中からレポートタイプを選択し、各条件を設定
   ・トラフィックレポート
   ・攻撃レポート
   ・ウイルスレポート
   ・VPNレポート

・URLレポート
・ルールレポート

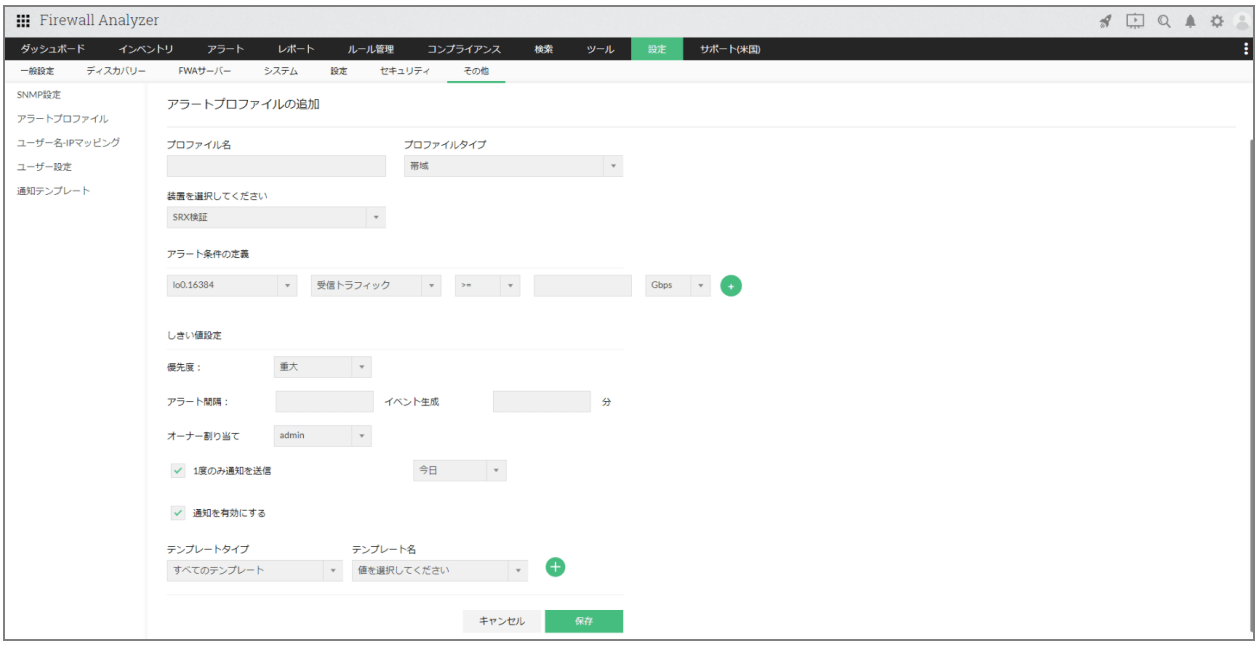
3. しきい値設定
   対象期間や重要度、異常の有無を確認する時間間隔を指定
4. 1度のみ通知を送信
   アラート発生時に毎回通知を行うか、任意のタイミングで1度のみ通知するか選択します。
5. 通知を有効にする
   ［通知テンプレート］機能で作成したテンプレートを選択します。



7.5 帯域

対象装置のインターフェースで使用する帯域の異常を検知します。
前述、「アラートプロファイルの作成」の手順4以降の流れを記載します。

1. 対象装置を選択
2. アラート条件の定義
   ・対象のインターフェース
   ・トラフィックタイプ（受信トラフィック、送信トラフィック、合計トラフィック）
   ・トラフィックの条件、値
3. しきい値設定
   ・優先度
   ・アラート間隔
   ・1度のみ通知を送信（任意）
   ・通知を有効にする（任意）



> 帯域アラートを設定するには、後述の「7.6 SNMP設定」を事前に登録する必要があります。

7.6 SNMP設定

FWAでSNMP設定を有効化することにより、以下の機能でSNMPを使用した情報取得を行います。

- ダッシュボード
  ファイアウォールライブトラフィック、ファイアウォールインターフェースライブトラフィック

- インベントリ
  ［帯域］→［ライブトラフィック］

- 帯域アラート
  ［設定］→［その他］→［アラートプロファイル］

> ダッシュボード、インベントリ配下の上記データについては、syslogの情報をもとにデータ表示することも可能です。
> SNMP設定を有効にすることで、SNMPをもとに帯域データが取得されます。

以下の手順でSNMP設定を有効化します。

1. ［設定］→［その他］→［SNMP設定］画面右上の［追加］をクリック
2. 以下の各情報を設定
   ・装置名：SNMP設定を行う対象装置を選択
   ・SNMPバージョン：v1/v2/v3から選択
   ※v3を選択すると、さらに認証設定を入力する画面が表示されます。
   ・SNMPコミュニティ：対象装置に設定されているSNMPコミュニティ名を入力
   ・SNMPポート：SNMPポート番号を入力
3. インターフェースライブレポートにチェックし、更新間隔（1分/5分/10分）を選択（任意）
4. ［テスト］をクリックし、入力したSNMP情報に誤りがないことを確認し［保存］

8 アラート

FWAで発報されたアラートの確認画面について記載します。

8.1 アラート

「7 アラートプロファイル設定」を設定後、条件に該当するログを検知すると、［アラート］タブにアラートが発報され、一覧で表示されます。
その他「8.3 セルフ監視」により発生したアラートも同様にアラート一覧に追加されます。

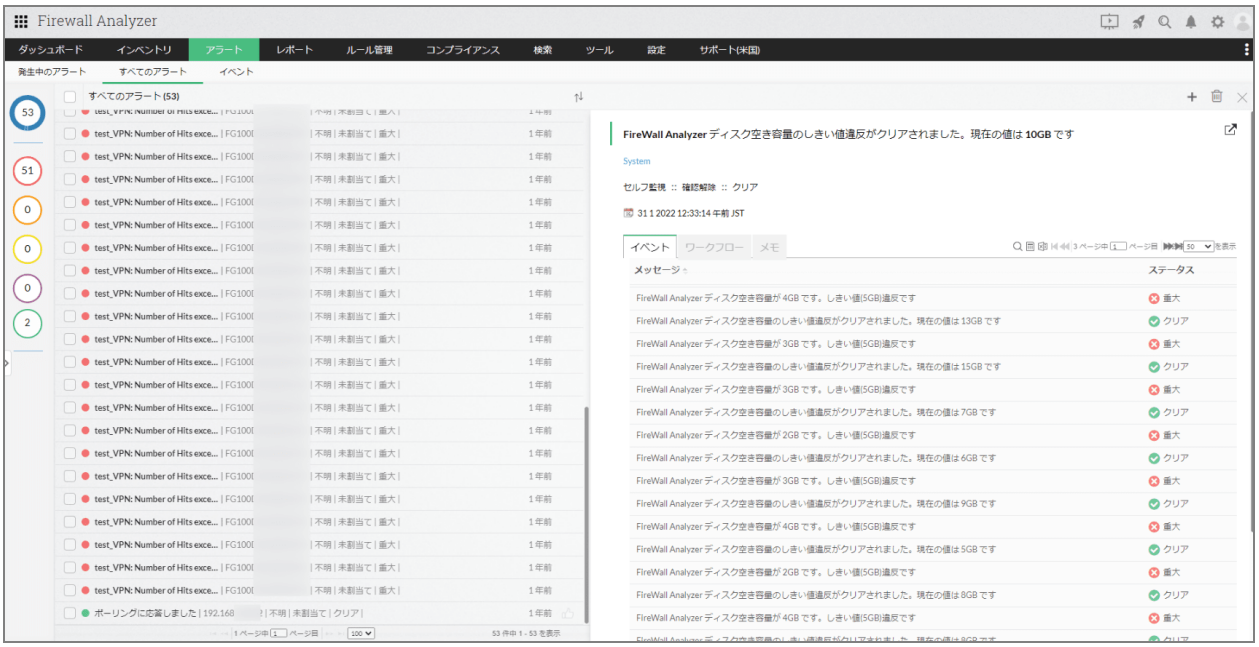
アラートは、アラートプロファイル設定で指定したアラートの重要度に応じて、色分けで表示されます。
画面左の重要度のアイコンをクリックすることで、重要度に該当するアラートのみが表示されます。
アラートタブには以下の3つのタブが存在します。

- 発生中のアラート
  アラートプロファイルやセルフ監視により発生したアラートの内、アラートがクリアされていない、発生中のアラートを一覧で表示します。

- すべてのアラート
  アラートプロファイルやセルフ監視により発生したすべてのアラートを一覧で表

示します。セルフ監視のしきい値違反やクリアは、1つのアラートとして集約されます。

- イベント
  アラートプロファイルやセルフ監視により発生したすべてのアラートを一覧で表示します。セルフ監視のしきい値違反やクリアのアラートは、個々のイベントとして表示されます。



対象のアラートをクリックすることで、アラートが発生するトリガーとなった通信情報や条件が表示されます。

8.2 可用性アラート

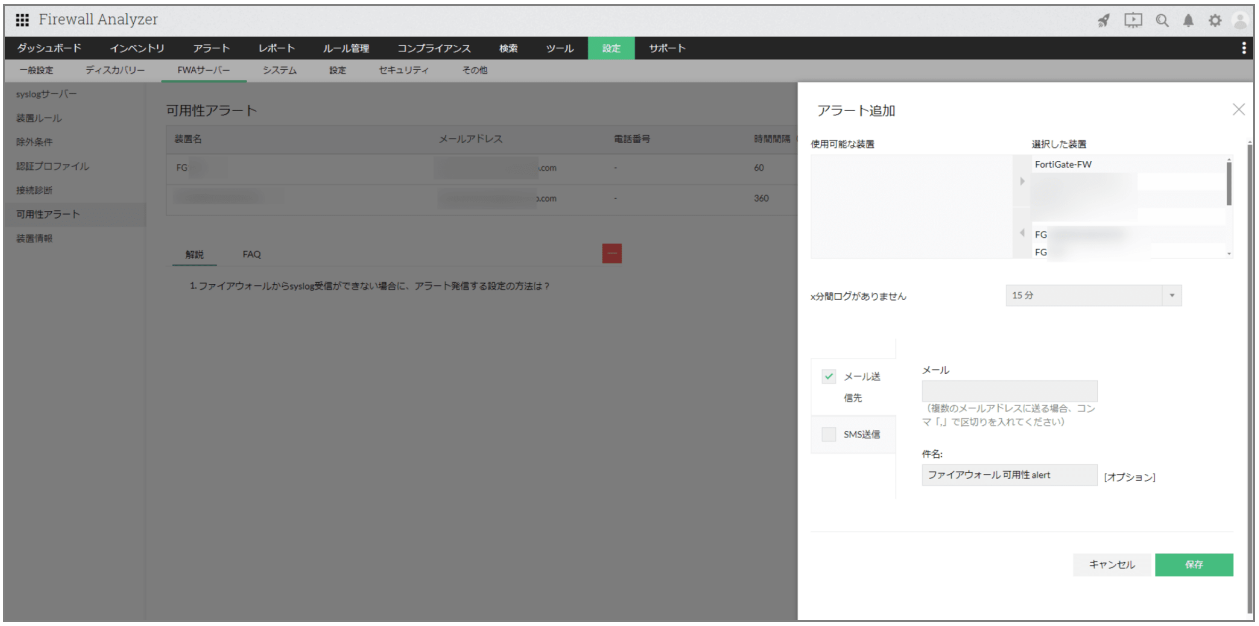
対象装置から一定時間ログを受信していない場合に、アラートを発報し管理者にメール通知します。

以下の手順で、可用性アラートを設定します。

1. ［設定］→［FWAサーバー］→［可用性アラート］を表示し、画面右上の［追加］をクリック

2. 以下の各項目を設定
   ・対象装置
   ・x分間ログがありません（15分、30分、1時間、2時間、6時間、12時間、1日）
   ※指定した時間、対象装置からログ受信がない場合に、アラートを発報します。
   ・アラート発生時のアクション（メール送信）
3. 各項目を設定後、［保存］をクリック

> ・可用性アラートが発報された際は、指定したアクション（メール送信）のみが実行され、FWA上の［アラート］には表示されません。
> ・メール通知アクションの設定にあたり、事前にメールサーバー設定を実施してください。



8.3 セルフ監視

FWAのインストールサーバー自体のCPUやディスク空き容量を監視します。

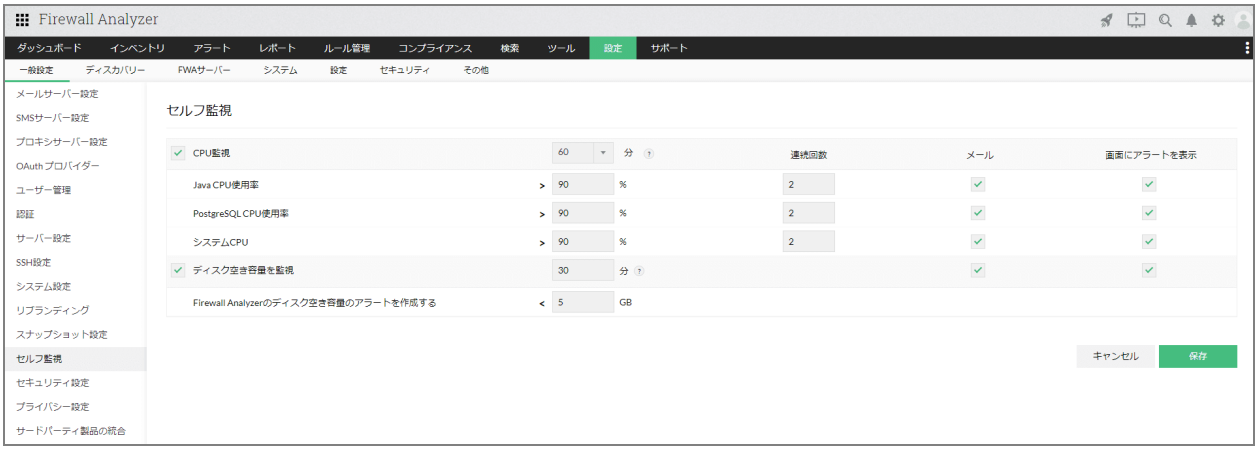
［設定］→［一般設定］→［セルフ監視］画面で、以下の各項目を設定します。

CPU監視

- 監視間隔（5分/10分/15分/30分/60分）
- Java CPU使用率 （しきい値%、連続回数、メール通知、アラート表示）
- PostgreSQL CPU使用率 （しきい値%、連続回数、メール通知、アラート表示）
- システムCPU （しきい値%、連続回数、メール通知、アラート表示）

ディスク空き容量

- 監視間隔（任意の分数を設定指定）
- Firewall Analyzerのディスク空き容量のアラートを作成する（しきい値GB）



9 ルール管理

ファイアウォールに設定されている既存ルール（ポリシー）の関連性を可視化し、ルール設定を最適化します。
また、新規ルールを追加する際、既存ルールとの関連性を事前に把握するために使用します。

9.1 装置ルール設定

［ルール管理］機能を使用するために、対象装置のルール、コンフィグ情報を事前に取得する必要があります。

装置ルールの取得は、［設定］→［FWAサーバー］→［装置ルール］画面右上の［追加］より実施します。

取得方法には以下の3つがあります。

- CLIベース
- ファイルインポート
- API

> ベンダーごとの使用可能な方法については、以下のサポートページをご確認ください。
> https://www.manageengine.jp/products/Firewall_Analyzer/SupportedFW.html#rule_management

以下の手順で装置ルールを設定します。

CLIベース

1. ［装置選択］より対象装置を選択し、取得方法［CLI］を選択
2. 対象装置に接続する認証情報（プロトコル、IPアドレス、ログイン名、パスワード等）を入力し、［テスト］をクリック

3. 検証に成功後、［ルール/コンフィグ取得をスケジュール］を任意に設定
   以下の例では毎日0時00分に、最新情報を自動で取得します。

ファイルインポート

1. ［装置選択］より対象装置を選択し、取得方法［ファイル］を選択
2. ルール情報を含むファイルまたはコンフィグ情報を含むファイルを各インポートオプションから選択し、インポートを実施

API

1. ［装置選択］より対象装置を選択し、取得方法［API］を選択
2. 対象装置のAPI管理サーバーのURL、認証情報（ユーザー名、パスワード）を入力

装置ルール設定を保存後、一覧に取得状況が追加されます。

9.2 ルール管理

「9.1 装置ルール設定」を実施後、［ルール管理］タブより、
ファイアウォールのルール情報に関する各種レポートを確認します。

> ベンダーごとのサポート対象機能は、以下のページをご参照ください。
> https://www.manageengine.jp/products/Firewall_Analyzer/SupportedFW.html#rule_management

9.2.1　概要

ファイアウォールからルール情報を取得し、現在の設定情報の概要を表示します。
［サマリ］タブでは、以下の各統計情報が表示されます。

レポートタイプ	説明
合計ルール数	該当ファイアウォールで設定されている全てのルール数
許可ルール数	該当ファイアウォールで設定されている全ての許可ルール数
拒否ルール数	該当ファイアウォールで設定されている全ての拒否ルール数
ファイアウォール受信ルール数	該当ファイアウォールで設定されているインバウンド（受信）ルール数
ファイアウォール送信ルール数	該当ファイアウォールで設定されているアウトバウンド（送信）ルール数
無効ルール数	無効（非アクティブ）になっているルール数
ロギングが無効のルール数	ロギング設定が無効になっているルール数
「any」から「any」への許可ルール数	通信を無制限に許可しているルール数
「any」サービスを許可しているルール数	サービス「any」を設定しているルール数
双方向ルールカウント	方向（送信元と宛先）の値のみが異なり、他項目の値は同一なルール数

［セキュリティルールタブ］では、ファイアウォールに設定されているルール情報（ルール番号/ID、送信元、宛先、送信インターフェース、宛先インターフェース、サービス、アクション）を一覧で表示します。

［オブジェクト詳細］タブでは、ファイアウォールに設定されているオブジェクト情報（ネットワークオブジェクト、サービスオブジェクト）を一覧で表示します。

一覧で表示されるルールの順番は、ファイアウォールのCLIベースで設定されているルールの順番に沿って表示されます。

9.2.2　最適化

ファイアウォールに設定されているルールの相関関係や使用状況に応じて、最適なルール構成を確認します。
以下の各タイプごとに情報を参照します。

タイプ	説明
ポリシー異常	ルール間の相関性を解析し、設定の最適化をサポートします。 カテゴリ別（冗長性/一般化/相関（コリレーション）/シャドウ/グループ）に、相関性や重複状況を表示します。
ルールの提案	過度な許可ルール（permit/any）に対して、ルールの使用状況に

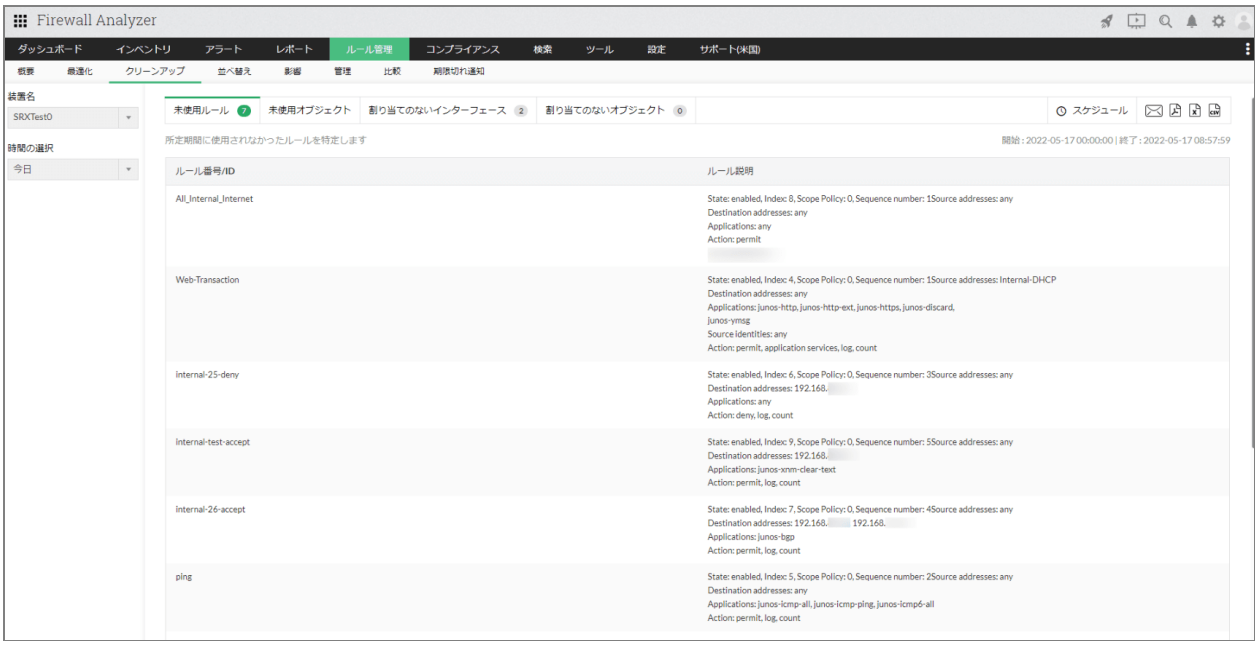
	もとづいた推奨設定を表示します。
ポリシーのチューニング	許可ルールのみを表示し、一定期間に使用されているルール情報をもとにチューニング内容を表示します。
オブジェクト使用	選択した期間に受信したsyslogに応じて、使用されたネットワークオブジェクト/サービスオブジェクトの概要を表示します。 また、未使用のネットワークオブジェクト/サービスオブジェクトも表示します。
重複オブジェクト	同じIPアドレス/サービスを持つが、オブジェクト名が異なるネットワーク/サービスオブジェクトを対象に、重複しているオブジェクト情報を一覧で表示します。

9.2.3　クリーンアップ

ファイアウォールに設定されているものの、一定期間使用されていないルールやオブジェクト、インターフェース情報を表示します。
以下の各タイプごとに情報を参照します。

タイプ	説明
未使用ルール	一定期間に使用されなかったルール番号/ID、ルール説明（送信元、宛先、アクション等）を一覧で表示します。
	ファイアウォールに設定されているルール内の未使用のオブジェ

未使用オブジェクト	クトについて、該当のルール名、オブジェクトタイプ、未使用オブジェクト数、未使用比率（%）を一覧で表示します。
割り当てのないインターフェース	ルールに割り当てられていない未使用のインターフェース情報（インターフェース名、IPアドレス、タイプ、モード、許可されたサービス、Vdom、ARP転送）を一覧で表示します。
割り当てのないオブジェクト	ルールに割り当てられていないオブジェクト情報（オブジェクト名、オブジェクト詳細、タイプ）を一覧で表示します。



9.2.4　並べ替え

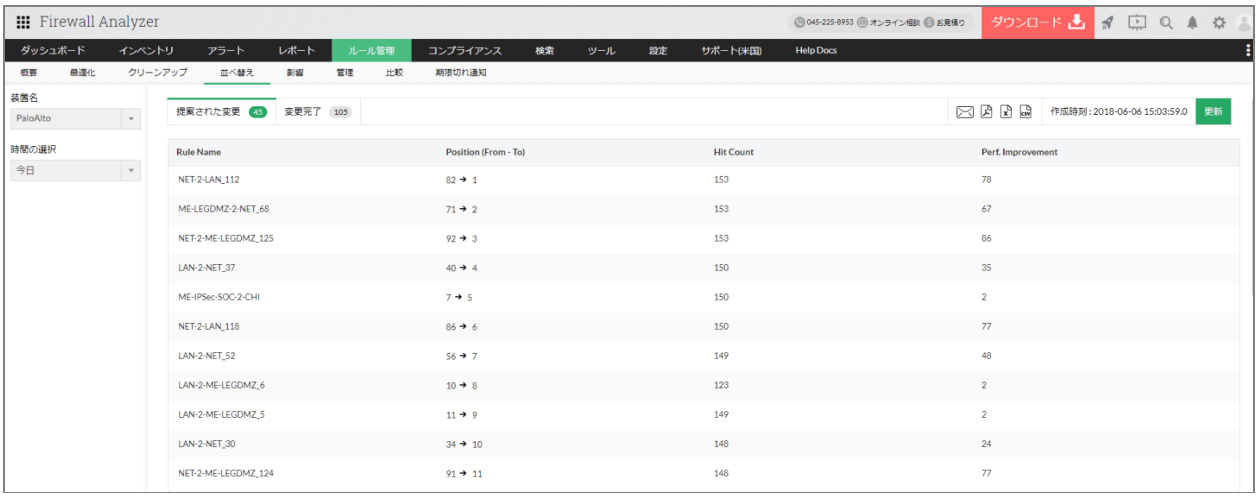
使用頻度の多いルールの順番を上位に配置することで、ファイアウォール自体の負荷を低減させることにつながります。
本レポートでは、使用されるルールのヒット数に応じて、最適なルールの配置を提案します。
以下の各タイプごとに情報を参照します。

タイプ	説明
	FWAが対象のファイアウォールから受信するsyslogに含まれる

提案された変更	ルールのヒット数をもとに、現在のポジションからどこのポジションに配置することが適切か表示します。
変更完了	ファイアウォールに設定されているルール内の未使用のオブジェクトについて、該当のルール名、オブジェクトタイプ、未使用オブジェクト数、未使用比率（%）を一覧で表示します。

・並べ替えレポートでは、ルール配置の提案のみを行い、FWAからファイアウォールに対する設定変更は行いません。

・ルールに値が設定されていない場合、並べ替え提案の解析プロセスで、解析対象外となります。



9.2.5　影響

ファイアウォールに新規ルールを追加する際、既存ルールとの関係や影響範囲を事前に把握することが重要です。
本機能では、新規に追加予定のルールと既存ルールの関連性を表示します。

以下の流れで影響分析レポートからルールの関連性を確認します。

1. 追加予定のルール情報をレポートとして作成
2. レポートから既存ルールとの関連性を確認

1.追加予定のルール情報をレポートとして作成

［ルール管理］→［影響］画面で対象装置を選択し、［影響分析］より以下の各情報を入力

項目	説明
ポリシーでのルール	任意のルール名
ポジション	新規ルールの配置予定の位置を選択
ソース	ファイアウォールに設定されている送信元オブジェクトまたはIPアドレスを指定
宛先	ファイアウォールに設定されている宛先オブジェクトまたはIPアドレスを指定
送信インターフェース	送信元のインターフェースゾーン
宛先インターフェース	宛先のインターフェースゾーン
サービス	サービス名を選択
アクション	ルールのアクションを選択（Allow/Deny）
ブラックリストにしているIPアドレスファイルを検討対象にする	組織内で重要視しているIPアドレスリストが存在する場合に、txtまたはcsv形式のファイルを選択
最初に、オブジェクトの重複確認をする	重複確認を行うルール数を選択（通常はALL）

2.レポートから既存ルールとの関連性を確認

生成したレポートには、以下の情報が表示されます。

項目	説明
ルールのインパクト詳細	［影響分析］で設定したルール情報を表示します。
異常詳細	既存ルールとの重複がある場合に表示されます。
ルール並べ替えの提案	既存ルールのヒット数から新規ルールの配置をサポートします。
このルールは、許可の範囲が広くとられています	Anyを含む場合や、許可設定しているオブジェクトが多い場合に、高リスクであることを警告します。
セキュリティ脅威の詳細	設定したサービスやインターフェースのセキュリティリスクレベルやCVE情報を表示します。
ブラックリスト（要注意）のIPアドレス分析	新規ルールにブラックリストとして指定したIPアドレスが含まれているか表示します。

リスクがあるポート情報	設定したサービス、インターフェースのセキュリティリスク（CVE情報）を表示します。
複数ルールにおけるオブジェクトの重複性	追加予定のサービス、送信元/宛先IPアドレスの各オブジェクトと既存ポリシーとの重複性を表示します。

9.2.6　管理

CLIまたはAPIで接続を確立しているファイアウォールに対して、FWAから、オブジェクトやルールの追加/編集/削除を行います。
以下の各タブごとに、オブジェクトの編集や変更を実施します。

タブ	説明
ネットワークオブジェクト	ネットワークオブジェクトの追加やファイアウォールに設定されている既存オブジェクトの編集や削除を行います。 ● ローカルオブジェクト ネットワークオブジェクトの追加設定を行います。 ● ファイアウォールオブジェクト 既存で設定されているネットワークオブジェクトを編集します。 追加、編集したオブジェクトは、ローカルオブジェクトまたは、［レビュー&送信］タブに追加されます。 ※この時点では、ファイアウォールに変更は反映されません。
サービスオブジェクト	サービスオブジェクトの追加やファイアウォールに設定されている既存オブジェクトの編集/削除を行います。 ● ローカルオブジェクト サービスオブジェクトの追加設定を行います。 ● ファイアウォールオブジェクト 既存で設定されているサービスオブジェクトを編集します。

	追加、編集したオブジェクトは、ローカルオブジェクトまたは、［レビュー&送信］タブに追加されます。 ※この時点では、ファイアウォールに変更は反映されません。
セキュリティルール	ルールの追加や対象装置に設定されている既存ルールの編集/削除を行います。 ● ローカルルール 新規ルールの追加設定を行います。 ● ファイアウォールルール 既存で設定されているルールを編集します。 追加、編集したルールは、ローカルルールまたは、［レビュー&送信］タブに追加されます。 ※この時点では、ファイアウォールに変更は反映されません。
レビュー&送信	新規追加、編集、削除予定のオブジェクトやルールは、それぞれ［ローカルオブジェクト］と［ローカルルール］に追加されます。加えて、［レビュー&送信］タブにも追加されます。 ［レビュー&送信］タブで、対象のオブジェクトまたはルールにチェックを入れて、画面右上の［送信］をクリックすることで、対象のファイアウォールに設定を送信します。 編集や削除もこのタブから実行できます。
Rule Approval	ルールやオブジェクトの変更の際に、Administrator権限のFWAユーザー間で承認プロセスを実現します。 ユーザーが変更リクエストを送信し、承認者が承認、拒否、投入を行います。
コミット	Palo AltoまたはCheck Pointを管理対象装置としている場合、［レビュー&送信］タブで送信したオブジェクトやルールは、［コミット］タブに移動します。 ［コミット］または［インストールポリシー］より、設定を送信します。

Palo AltoまたはCheck Pointをご利用の場合には、以下ページに記載の手順に沿って、変更内容の送信およびコミットを実施してください。
https://www.manageengine.jp/products/Firewall_Analyzer/help/firewall-rule-administration.html#review_send

9.2.7　比較

ファイアウォールの2つのコンフィグファイル、または異なるRunningコンフィグバージョン（世代）間における、ルールセットの差分を表示します。
追加、変更、削除ポイントを色別に比較します。
以下の各項目ごとに、差分を確認します。

項目	説明
コンフィグファイル間	2つの同一ベンダー/モデルのコンフィグファイルをインポートし、ルールセットを比較します。
コンフィグファイルと最新runningコンフィグ	ファイアウォールのコンフィグファイルをインポートし、現在稼働しているルールセット（FWAで取得したRunningコンフィグ）との比較を行います。
runningコンフィグの世代間	ファイアウォールのコンフィグ設定が変更され、コンフィグバージョン（世代）がFWA上に追加されている場合に、変更されたルールセットを差分として表示します。

・ファイアウォールのコンフィグが変更された場合、［コンプライアンス］→［変更管理］に世代が追加されます。

・コンフィグ世代の差分が、基本設定のみ（ルールセットに関する差分がない）場合、本機能による比較はできません。

9.2.8　期限切れ通知

ファイアウォールに設定されているルールの有効期限やスケジュール情報を一覧で表示します。
以下の各タブごとに、アクティブなルールや今後アクティブになるルール、既に期限が切れているルールなどを表示します。

項目	説明
すべてのスケジュールルール	週次のスケジュールや、特定の期間の1回のみのスケジュールなど、ファイアウォールに設定されているスケジュールルールを一覧で表示します。
アクティブルール	スケジュールルールの内、現在アクティブ状態のルールを一覧で表示します。また、アクティブなルールの期限が切れた場合に、通知する機能も搭載されています。 ［自分に通知］では、対象ルールの期限切れ確認時間（日次）や、期限切れになる前後の通知日を指定することができます。 ※繰り返しルールには設定できません。
予定ルール	今後のスケジュールで、アクティブになるルールを一覧で表示します。
期限切れルール	設定されたスケジュールに則り、既に有効期限が切れたルールを一覧で表示します。
繰り返しルール	週次や日次スケジュールなど、定期的にアクティブになるよう設定されているルールを一覧で表示します。

9.2.9　リスク

ファイアウォールに設定されているルールを分析し、脆弱なリスクが存在するルールをレベル別に表示します。
以下の各タブごとに、対象装置に潜む脆弱性を確認します。

タブ	説明
概要	各リスクレベルの合計数やリスク数のトレンドを色別に表示します。
ルール	各ルールごとに、該当するリスク内容を表示します。 ・ルール表示 ルール名/IDを基準に、該当するリスクレベルとその数を一覧で表示します。 リスク数をクリックすると、ルールに関連するリスク情報と対策のための推奨事項を確認することができます。 ・リスク表示 リスクレベルを基準に、リスク情報と該当のルール数を一覧で表示します。 リスク情報をクリックすると、該当のルール一覧が表示されます。 誤検知としてマークが必要なルールには、［誤検知をマーク］により該当ルールをホワイトリストとして追加することができます。 ※誤検知としてマークしたルールは、［除外ルール］から確認できます。

10 コンフィグバックアップ

ファイアウォールのコンフィグを定期的にバックアップし、差分を比較します。

> ・事前に［装置ルール］を設定している必要があります。
> ・本機能のサポート対象ベンダーは、以下のページをご参照ください。
> https://www.manageengine.jp/products/Firewall_Analyzer/SupportedFW.html#complia

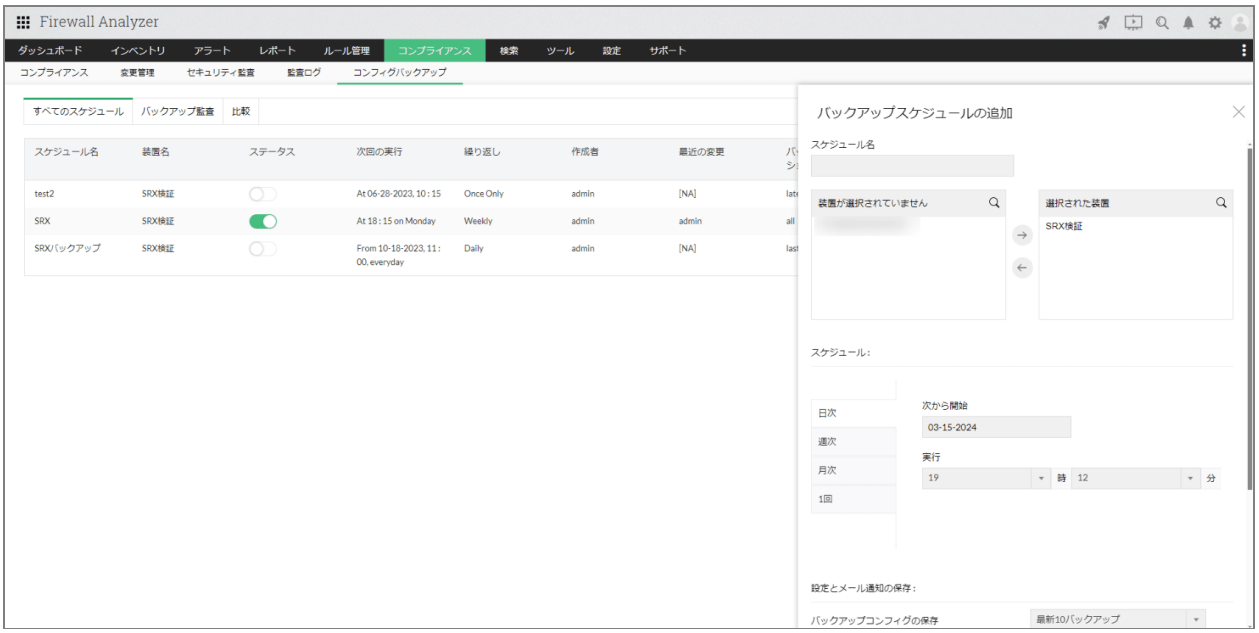
> nce

・設定画面
［コンプライアンス］→［コンフィグバックアップ］

10.1　コンフィグバックアップのスケジュール設定手順

以下の手順で、スケジュール設定を行います。

1. ［コンプライアンス］→［コンフィグバックアップ］→［すべてのスケジュール］を表示
2. 画面右上の、［バックアップスケジュールの追加］をクリック
3. 任意のスケジュール名を入力し、バックアップ対象の装置を選択
4. コンフィグバックアップを実施する周期を選択
   選択可能な周期：日次、週次、月次、1回
5. ［設定とメール通知の保存］の項目で、保存するコンフィグ世代数、メール通知を設定
   選択可能なコンフィグ世代数：最新3バックアップ、最新5バックアップ、最新10バックアップ、最新バックアップ、すべてのバックアップ
   ※週次、月次を選択した場合、［すべてのバックアップ］項目を選択できます。
   ※1回を選択した場合、最新バックアップのみが選択可能です。
   ※メール通知を有効化した場合、指定したメールアドレスにコンフィグバックアップの実行ステータス（成功、失敗）を通知します。
6. ［保存］より、設定を保存
   保存すると、［すべてのスケジュール］の一覧に設定内容が表示されます。



10.2　バックアップ監査

スケジュールによるコンフィグバックアップの取得日時やステータス、取得したコンフィグファイルのダウンロードを行います。

以下の項目を選択し、参照するデータを指定します。

- 装置名
- スケジュールタイプ（すべてのスケジュール、日次、週次、月次、1回）
- 時間の選択（今日、最新24時間、最新7日間、最新30日間、カスタム）

［コンフィグファイル］のダウンロードリンクより、取得したコンフィグファイルをテキスト形式でダウンロードします。
［比較］では、取得した別世代のルールまたはコンフィグとの比較を行います。

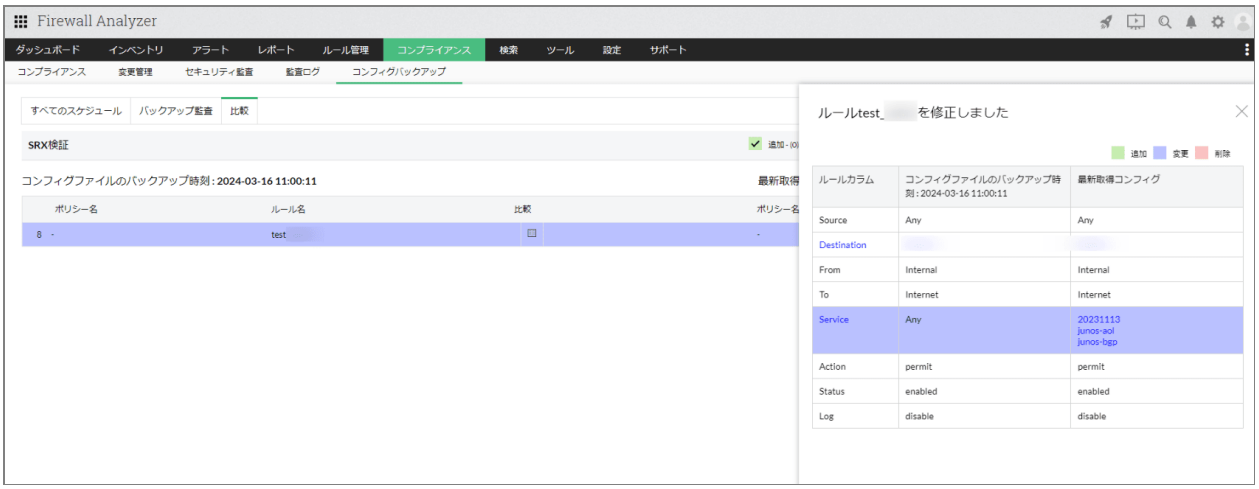
10.3　比較

スケジュールバックアップで取得したコンフィグ情報をもとに、ルールまたはコンフィグに焦点をあて、差分比較を行います。

比較対象に関する以下の情報を指定します。

- 装置名：比較対象の装置を選択
- 比較規準：ルールまたはコンフィグを選択
- スケジュールタイプ：比較を行うスケジュールタイプを選択
- 時間の選択：取得したコンフィグ期間を選択
  今日、最新24時間、最新7日間、最新30日間、カスタム
- 比較するコンフィグのバックアップ日次：取得したコンフィグを選択（取得した日時で表示されます）
- 対象：比較対象のコンフィグを選択（取得した日時で表示されます）
  ※［最新コンフィグ］は、その場で最新のコンフィグを取得し比較対象とします。

ルールまたはコンフィグに差分がある場合には、以下のような差分ページが表示され、差分内容の詳細を確認します。



11 ログ検索

11.1　生ログ設定

FWAが受信する生ログのインデックス設定を実施します。

デフォルトでは、［セキュリティログのインデックスのみ］が有効化されています。後述の「11.2 生ログ検索」で、トラフィックログの検索を行う場合には、［トラフィックとセキュリティログのインデックス］を選択して、設定を保存します。

選択した項目に応じて、生ログ検索画面で表示されるオプションが異なります。

［セキュリティログのインデックスのみ］を選択した場合

- タイプ検索
  ファイアウォールの生ログ
- VPNの生ログ
- ウイルス/攻撃の生ログ
- 装置管理の生ログ
- 拒否の生ログ

［トラフィックとセキュリティログのインデックス］を選択した場合

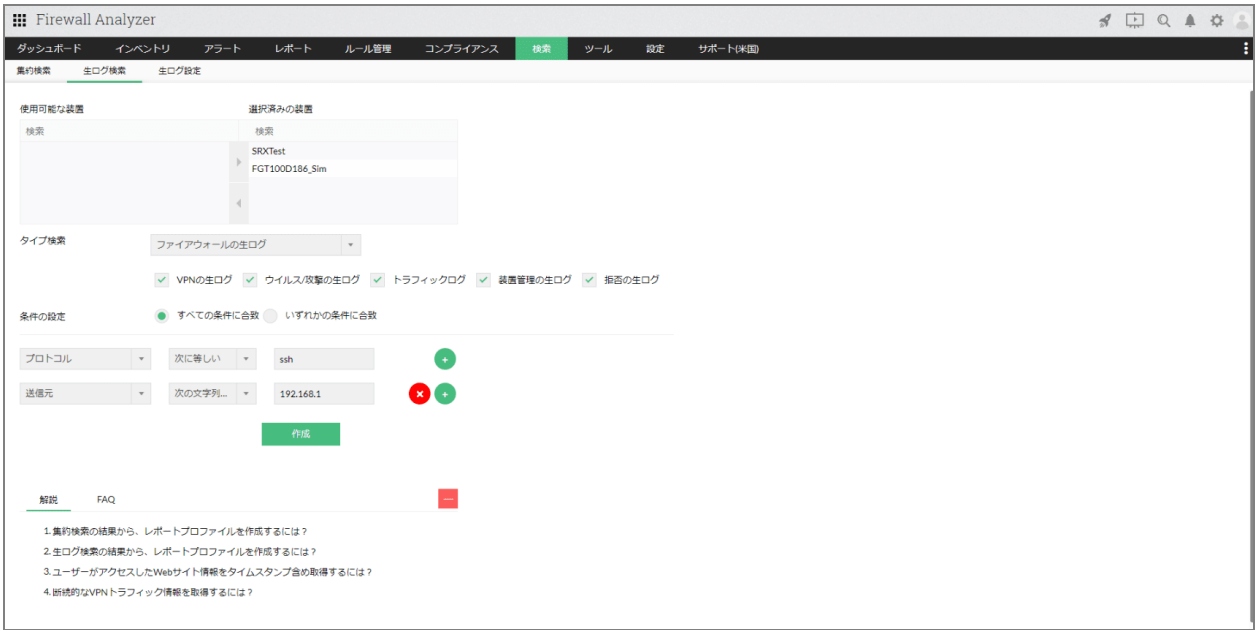
- タイプ検索

ファイアウォールの生ログ
プロキシの生ログ
不明なプロトコル

- VPNの生ログ
- ウイルス/攻撃の生ログ
- トラフィックログ
- 装置管理の生ログ
- 拒否の生ログ

11.2　生ログ検索

FWAが受信した生ログに対して複数の検索条件を指定し、該当ログを検索します。



タイプ検索には、以下の種類があります。

- ファイアウォールの生ログ
- プロキシの生ログ
- 不明なプロトコル

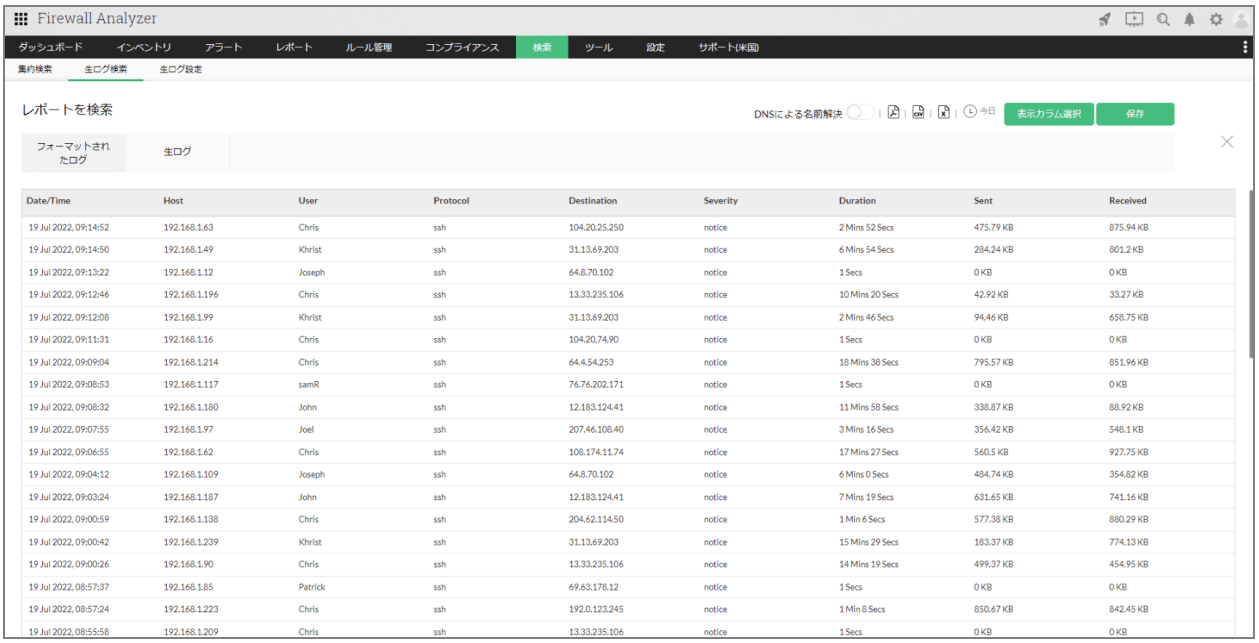
また、生ログタイプとして、以下のチェック項目が実装されています。

- VPNの生ログ
- ウイルス/攻撃の生ログ
- トラフィックログ
- 装置管理の生ログ
- 拒否の生ログ

検索条件を指定し［作成］をクリックすると、検索条件に該当する生ログ情報が表示されます。
※プラスアイコンをクリックし、複数の検索条件を指定することも可能です。

検索後は、［フォーマットされたログ］または［生ログ］タブから確認します。

- フォーマットされたログ
  生ログを日時やホスト、ユーザーなど、各カラムごとに分け、視覚的に分かりやすい形式で表示します。
- 生ログ
  FWAが受信したログを、加工せずそのままの状態（生ログ）で表示します。



・画面上部の［保存］より、検索した条件をプロファイルとして保存することができます。
※保存したプロファイルは、［レポート］→［カスタムレポート］のプロファイル一覧

に追加され、次回以降、保存した条件で検索することができます。
※［スケジュール］を有効化することで、検索条件に対する検索結果を定期出力します。

・［フォーマットされたログ］タブを表示し、画面上部の［表示カラム選択］から、一覧に表示するカラム情報を選択することができます。
※選択可能なカラムは11個までです。

11.3　集約検索

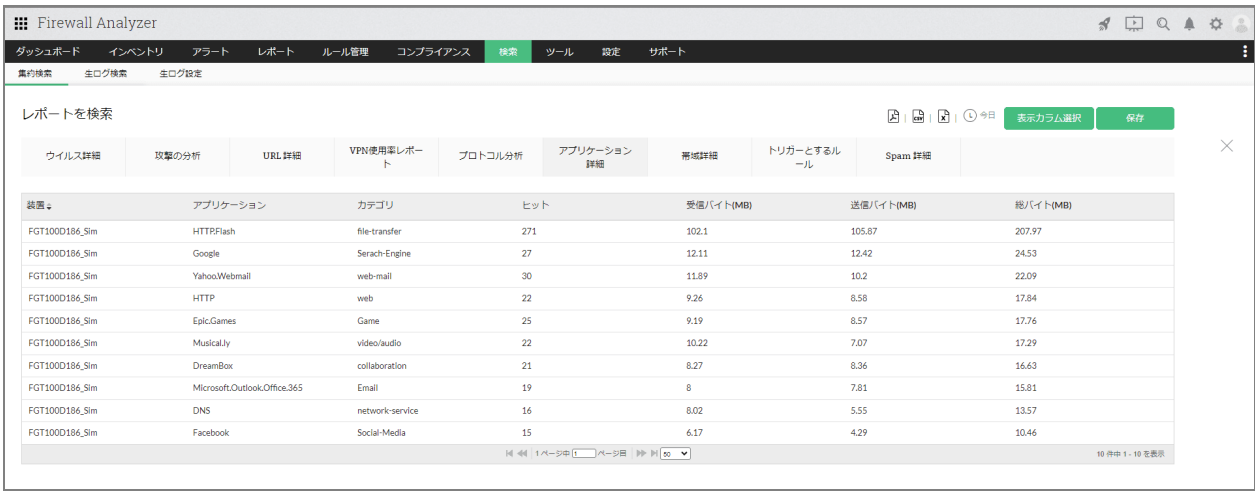
FWAのデータベースに集約されたデータをもとに、データ検索を行います。
検索画面で、対象装置の選択と検索条件を指定します。

検索条件を指定し［作成］をクリックすると、検索条件に該当するログ情報が表示されます。
※プラスアイコンをクリックし、複数の検索条件を指定することも可能です。

検索結果は、以下のタイプごとに表示されます。

- ウイルス詳細
- 攻撃の分析
- URL詳細
- VPN使用率レポート
- プロトコル分析
- アプリケーション詳細

- 帯域詳細
- トリガーとするルール
- Spam詳細（Spam Detail）



画面上部の［保存］より、検索した条件をプロファイルとして保存することができます。
保存したプロファイルは、［レポート］→［カスタムレポート］のプロファイル一覧に追加され、次回以降、保存した条件で検索を行うことができます。

12 ユーザー管理とロール権限

FWAを複数人で管理する場合に、ユーザーアカウントごとに権限を作成して付与することができます。
※標準で使用可能なユーザーアカウント数は、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、オプションです）。

12.1　ユーザー管理

［設定］→［一般設定］→［ユーザー管理］→［ユーザー］画面で、ユーザーアカウントを作成します。
デフォルトで、以下の2つの権限が実装されています。

- 管理者

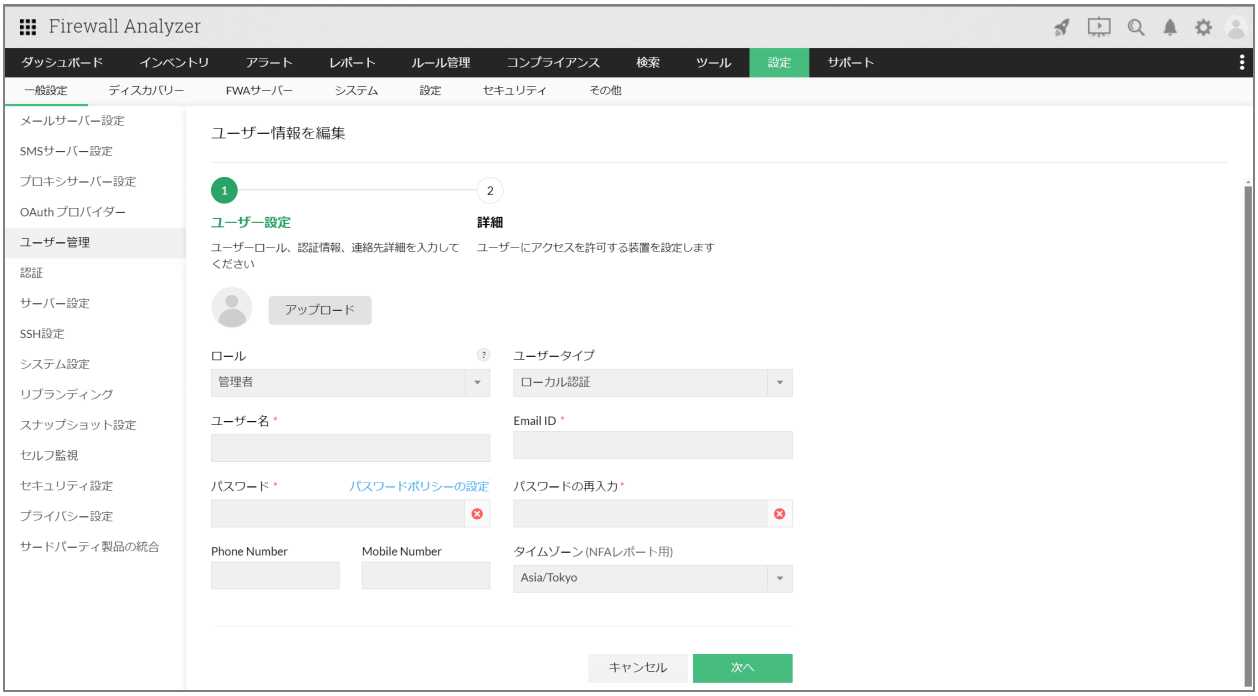
FWAであらゆる操作を実行する権限があります。

- オペレーター
  FWAで操作制限のある権限です。ユーザー管理機能の操作など、設定タブ配下の表示項目が制限されます。

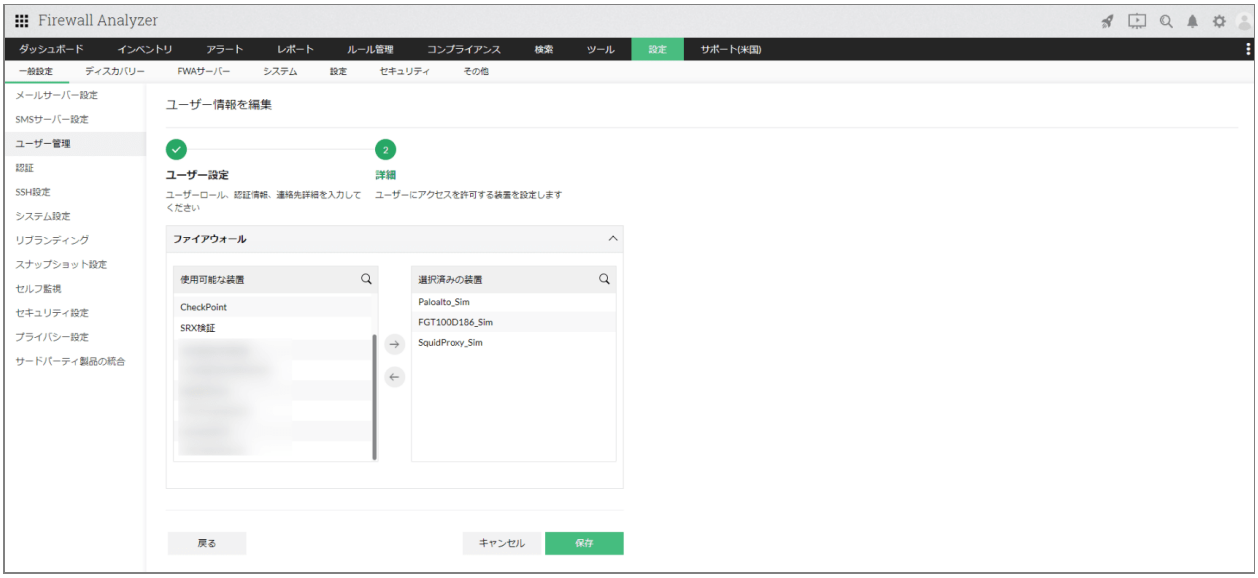
操作権限の詳細については、以下のページをご参照ください。
https://www.manageengine.jp/products/Firewall_Analyzer/help/user-management-settings.html#create_users

以下の手順でユーザーアカウントを作成します。

1. ［設定］→［一般設定］→［ユーザー管理］→［ユーザー］右上の［ユーザー追加］をクリック
2. ［ロール］で、作成するユーザーの権限を選択（管理者、オペレーター、作成したロール権限）
   ※ロール権限については、次章を確認してください。
3. ［ユーザータイプ］で、認証タイプを以下より選択
   ・ローカル認証
   ・RADIUS認証
   ・AD（Active Directory）認証
4. ユーザー名、パスワード、対象ユーザーのメールアドレスを入力し、［次へ］



5. ユーザーに割り当てる装置または装置グループを選択し、保存



・ローカル認証
FWAで独自に作成、管理するユーザーアカウントです。ローカル認証の場合、パスワードポリシーを任意に設定することができます。
※パスワードポリシーの設定は、「12.3 パスワードポリシー」をご確認ください。

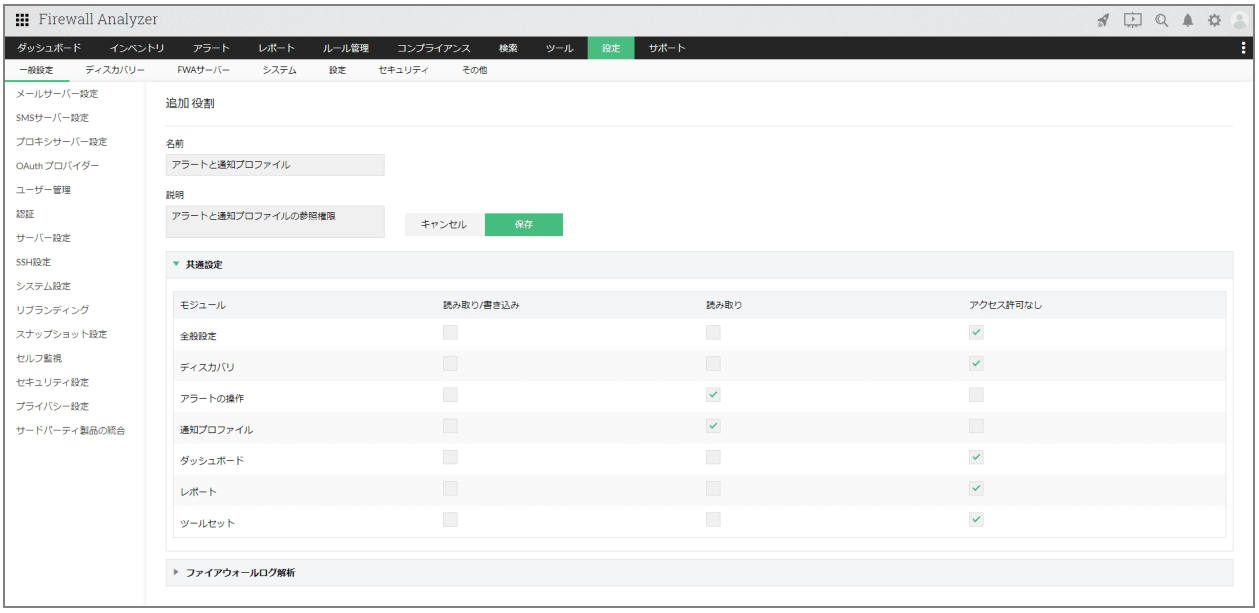
・RADIUS認証
RADIUS認証を使用して、FWAにログインするユーザーアカウントを作成します。 導入しているRADIUSサーバーの設定が必要です。RADIUSサーバーの設定については、以下のページをご参照ください。
https://www.manageengine.jp/products/Firewall_Analyzer/help/user-management-settings-radius.html

・AD認証
AD認証を使用して、FWAにログインするユーザーアカウントを作成します。 導入しているドメインサーバーの設定が必要です。ドメインサーバーの設定については、以下のページをご参照ください。
https://www.manageengine.jp/products/Firewall_Analyzer/help/user-management-settings-ad.html

12.2　ロール権限

管理者、オペレーター権限に加え、任意の権限名と各機能の権限（Read/Write、Readのみ、アクセス権なし）を付与した独自の権限を作成します。
作成手順は以下の通りです。

1. ［設定］→［一般設定］→［ユーザー管理］→［ロール］を表示し、画面右上の［Add Role］をクリック
2. 権限名として任意の［名前］およびその［説明］を記入
3. ［共通設定］、［ファイアウォールログ解析］の項目から、権限に付与する操作を選択し、［保存］
   ※操作権限は、読み取り/書き込み、読み取り、アクセス許可なしから選択します。
   ※権限を保存すると、［ロール］画面の一覧に追加されます。

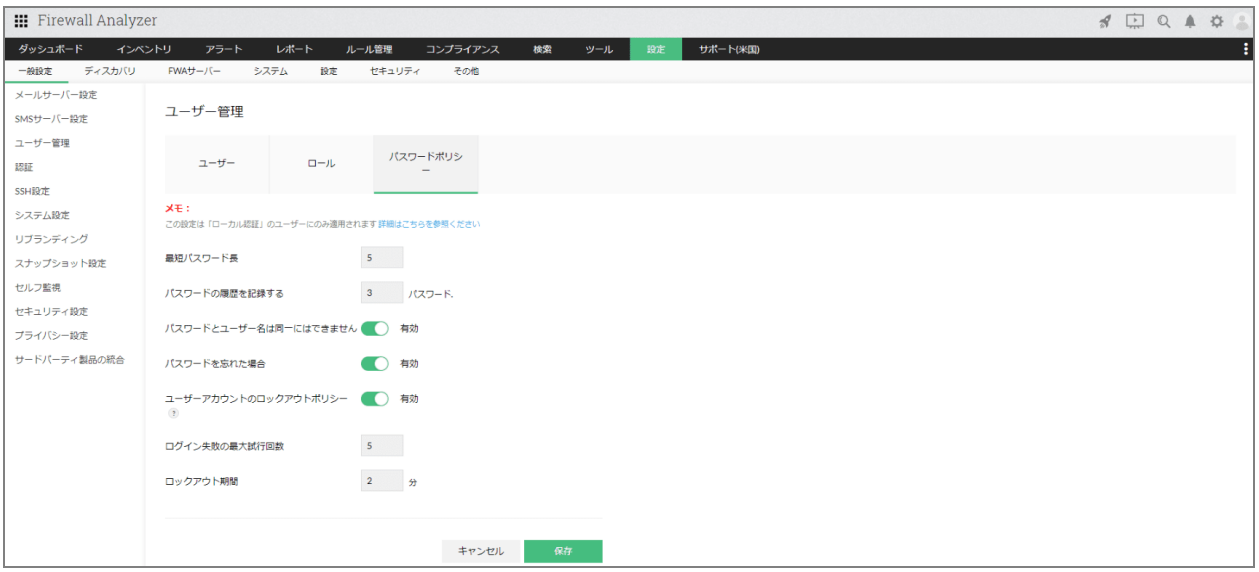


追加したロール権限は、［設定］→［一般設定］→［ユーザー管理］→［ユーザー］でユーザーを作成または編集する際の［ロール］に表示されるようになります。

> ロール機能で作成可能な操作権限については、以下のページをご参照ください。
> https://www.manageengine.jp/products/Firewall_Analyzer/help/role_feature.html#Operation_list

12.3　パスワードポリシー

FWAにログインして操作を行うユーザーアカウントの「パスワードレベル」を設定します。
ご利用環境のセキュリティレベルに応じて、ポリシー変更を実施してください。
※ローカル認証で追加したユーザーを対象にポリシーが適用されます。



各パラメーターについて、以下の表に記載します。

項目	説明
最短パスワード長	設定可能な最短パスワードの長さを設定 デフォルト：5
パスワードの履歴を記録する	パスワードを変更時に、過去数回の同パスワードの使用を不可に設定
パスワードとユーザー名は同一にはできません	ユーザー名、パスワードを同一にしない場合、有効に設定
パスワードを忘れた場合	ログイン画面で、［パスワードを忘れた場合］オプションを表示/非表示に設定

ユーザーアカウントのロックアウトポリシー	複数回ログインに失敗した場合のロック設定
ログイン失敗の最大試行回数	ロックアウトポリシーを有効にした際の最大試行回数を設定（デフォルト5回）
ロックアウト期間	ロックアウトポリシーを有効にした際のロック時間を設定（デフォルト2分）

13 各メニュータブの説明

FWAの画面上部に、各メニュータブが存在します。
各タブで表示される情報や操作可能な機能について記載します。

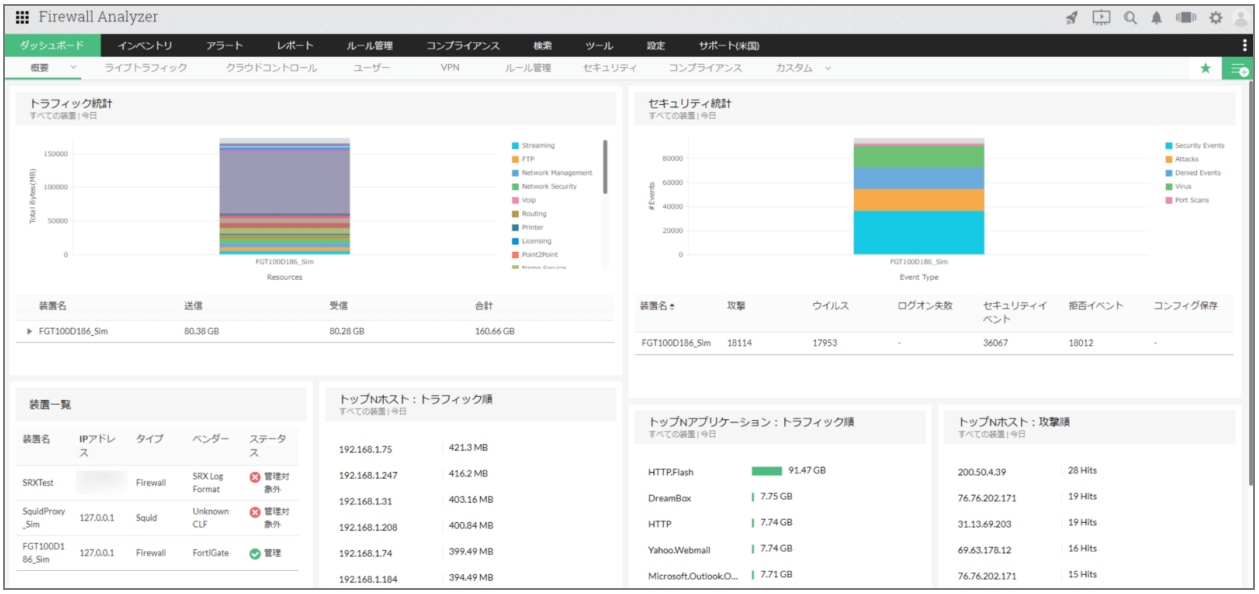
13.1　ダッシュボード

FWAにログイン後に表示されるホーム画面です。
ダッシュボードで表示する項目（ウィジェット）を任意にカスタマイズすることで、管理対象装置の一覧や装置、ホストごとのトラフィック状況を1つの画面で把握します。

ダッシュボードには、以下のタブが存在します。

タブ名	機能
概要	管理対象装置の一覧やホスト、アプリケーションごとのトラフィック状況など、全体の状況を表示します。
ライブトラフィック	装置またはインターフェースごとに、In/Outのトラフィックをリアルタイムのグラフで表示します。
クラウドコントロール	ファイアウォールを通過するクラウドサービスの使用状況を表示します。

ユーザー	通信を行っているユーザーに焦点をあて、アクセス状況を表示します。
VPN	ファイアウォールを通過するVPN通信のトラフィック使用率、VPNグループとユーザー情報を表示します。
ルール管理	ファイアウォールに設定されているルールを最適化するための情報（シャドーイング、冗長性、相関性、グループ化、一般化）を表示します。
セキュリティ	攻撃、ウイルス、SPAM通信など、ファイアウォールを通過しようとする通信の内、セキュリティに関連するデータを表示します。
コンプライアンス	業界の各セキュリティ標準や監査要件に対する、ファイアウォールに設定されているコンフィグの準拠状況を表示します。



13.1.1 ダッシュボードの新規作成

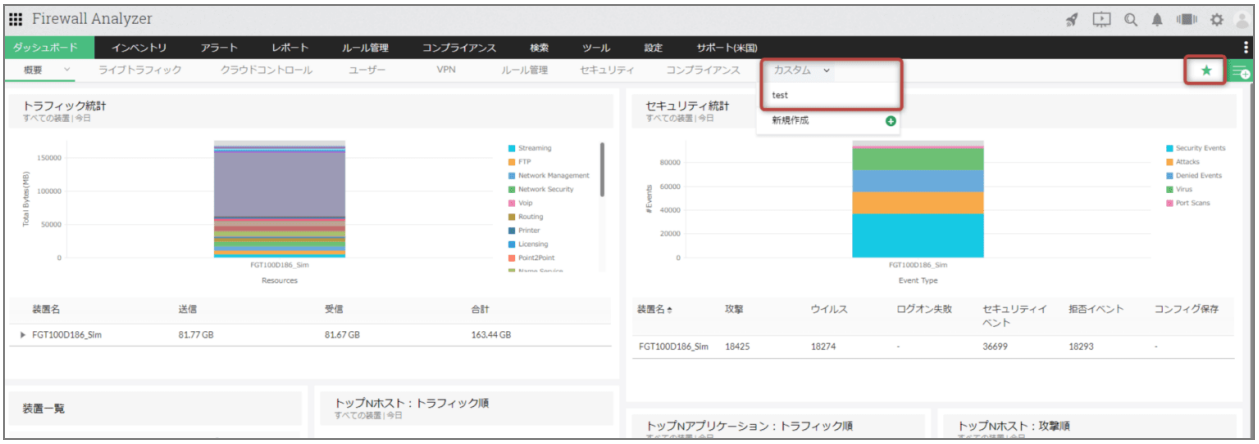
以下の手順で新規ダッシュボードを作成します。

1. ダッシュボード画面右上の［+］をクリック

2. ［ダッシュボードを追加］をクリック
3. 任意のダッシュボード名、説明を入力し、［次へ］をクリック
   ※ダッシュボード名に、特殊文字や空白は使用できません。
4. ダッシュボードに追加するウィジェットを選択し、［次へ］をクリック

5. ダッシュボードの参照を許可するユーザーアカウントを任意に選択し、［作成］

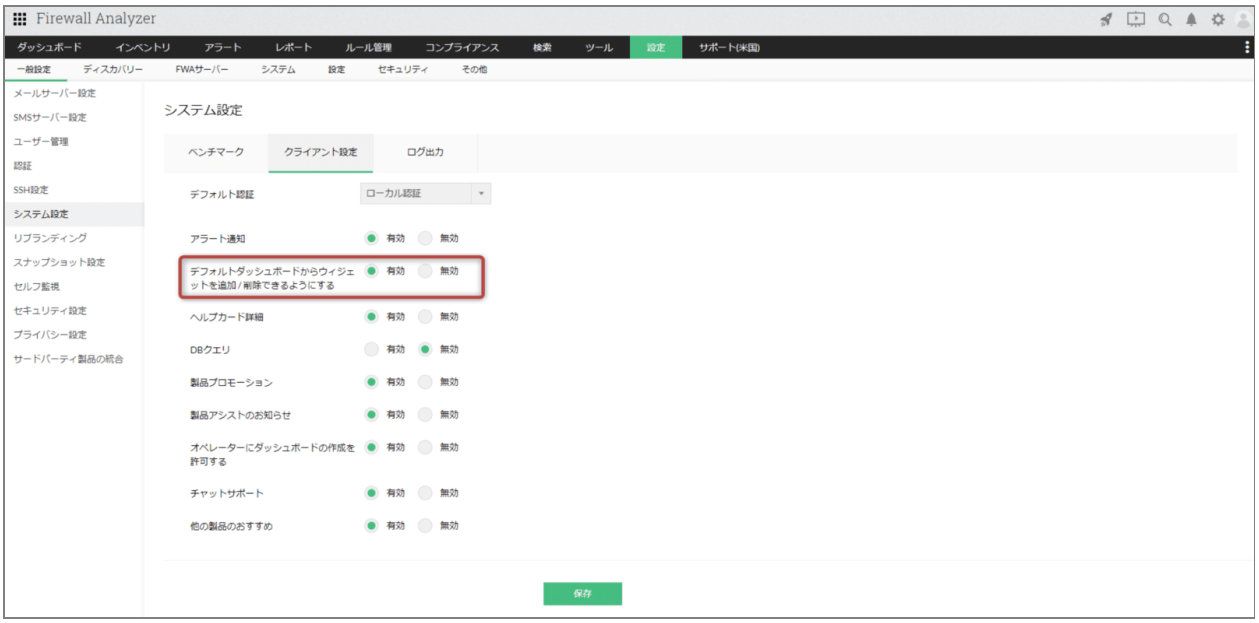
作成したダッシュボードは、［ダッシュボード］→［カスタムウィジェット］タブから選択できます。
また、ダッシュボードを表示し、画面右上の［★］をクリックすると、デフォルトダッシュボードとして設定することができます。



13.1.2 ウィジェットの追加、編集、削除

ウィジェットの追加

デフォルトダッシュボードにウィジェットを追加するためには、事前設定が必要です。
［設定］→［一般設定］→［システム設定］→［クライアント設定］より、
［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］を有効化して保存してください。



上記設定を保存後、［ダッシュボード］画面右上の［+］アイコンより、表示中のダッシュボードに任意のウィジェットを追加します。

ウィジェットの編集、削除

ウィジェットに表示する情報を変更する際は、ウィジェットにカーソルをあて、［編集］アイコンから編集を行います。

※編集できる内容はウィジェットごとに異なり、ウィジェット名やデータ表示対象期間、データ表示数、対象装置などを指定することができます。

ウィジェットを削除する際は、同様に対象のウィジェットにカーソルをあて、［削除］アイコンから削除します。

> ダッシュボード内で、ウィジェットを任意の位置に配置したり、大きさを変更することができます。
> 参照する頻度の高いウィジェットを上部に配置しておくことで、より迅速に情報を把握します。

13.2　インベントリ

FWAに追加した装置や使用ユーザーの確認、トラフィックの多い通信状況の参照など、
管理対象装置から受信したログ情報にもとづいた詳細な情報を確認することができます。

［インベントリ］には、以下のタブが存在します。

タブ名	説明
装置	FWAに追加されている装置の一覧を表示します。 装置の名前、ライセンス（管理/非管理）、IPアドレス タイプ、ベンダー、アップ/ダウンリンク速度、イントラネット/SNMP設定の各情報を表示します。
インターフェース	FWAに追加された装置のログから取得したインターフェース情報を表示します。 インターフェース名をクリックすることで、帯域や発生した通信を表示します。

ユーザー	FWAに追加された装置のログから取得したユーザー情報を表示します。 ユーザー名をクリックすることで、対象ユーザーに関する詳細な通信状況を表示します。
クラウドサービス	FWAに追加された装置のログから取得したクラウドサービス情報を表示します。 クラウドサービス名をクリックすることで、帯域や使用ユーザー情報を表示します。
使用ルール	装置でトリガーとして使用されたルール情報（許可/拒否、ヒット数、トラフィック数）を表示します。 ルール名をクリックすることで、ルールのトリガーとなった通信情報を表示します。

13.2.1 スナップショット画面

［インベントリ］→［装置］画面で装置をクリックすると、スナップショット画面が表示されます。

本画面では、対象装置に関する詳細な情報を参照することができます。

タブ名	説明
概要	装置情報に加え、受信、送信のトラフィック量を表示します。 アップリンク/ダウンリンクの値を編集アイコンから変更することができます。
帯域	受信、送信のライブトラフィックを表示します。グラフによる時系列データと、最小、最大、平均のトラフィック値を算出したデータが表示されます。 グラフ上をクリックすることで、該当の時間帯の通信状況（送信元、ユーザー、宛先、時刻、ルール番号/ID、プロトコル、重要度、期間、送受信バイト）を一覧で表示します。
トップ10	トラフィックの多い通信を対象に、ホスト、宛先、プロトコルグループ、内部サーバー、外部サイト、会話（通信）を一覧で表示します。 対象のホストやプロトコルグループをクリックすることで、より詳細な通信情報を表示することができます。
サイト	通信許可、拒否されたWebサイト（URL）情報を表示します。

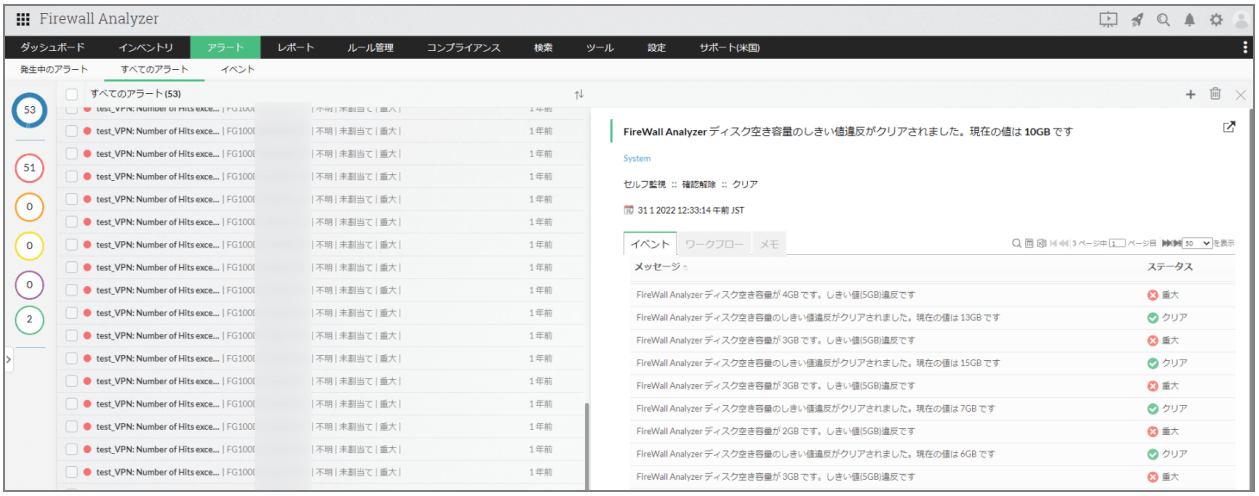
	該当のURL、ヒット数、ヒット率(%)、総バイト(MB)を一覧で確認します。
アプリケーション	対象装置を介して発生した通信のうち、アプリケーション情報を表示します。 アプリケーション名またはカテゴリ名をクリックすることで、該当のアプリケーションを使用しているより詳細な通信情報が表示されます。
ルール	対象装置で許可、拒否された上位のルール（ポリシー）番号を表示します。 ルール番号をクリックすることで、ルールのヒット数や、ルールに該当した通信の情報が表示されます。
セキュリティ	攻撃やウイルス、拒否された送信元、宛先ホスト情報など、セキュリティに関連する情報を一覧で表示します。 攻撃名やホスト名をクリックすることで、該当の通信の詳細（ホスト、宛先、プロトコルなど）が表示されます。
VPN	対象装置を介して発生したVPN通信の情報（アクティブVPNユーザー、VPNセッション、上位VPNレポート）を一覧で表示します。 一覧では、ユーザー名やVPN通信の開始/終了時刻、経過時間、送信/受信量などが表示されます。
ウイルス	プロキシサーバーを経由したウイルス情報を表示します。 ※プロキシサーバーの画面で表示されます。
使用	プロキシサーバーの使用状況（キャッシュコード、ピアステータス、HTTPステータスコード、HTTP操作）を表示します。 ※プロキシサーバーの画面で表示されます。

・アプリケーションレポートのサポート対象は、以下の通りです。
Check Point、Cisco Firepower、FortiGate、Juniper SRX、Palo Alto、SonicWall、Sophos XG、WatchGuard

・「app」レコードを含むsyslogデータを解析対象とします。

13.3　アラート

アラートプロファイルやセルフ監視で発生したイベントを、アラートとして一覧で表示します。
アラートの発生状況から、問題が発生している装置やそのイベント内容を把握します。



13.4　レポート

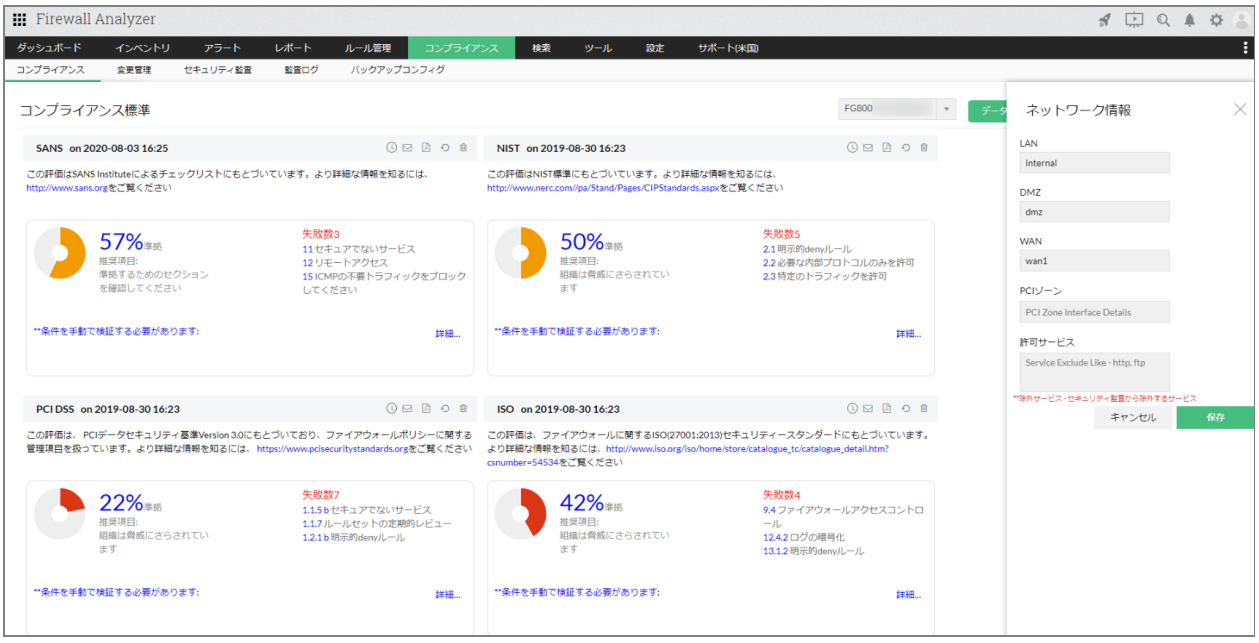
カスタムレポートやFWAレポート、プロキシレポートなど、各種レポートを表示、ファイル出力します。
詳しくは、「6 レポート」の章をご参照ください。

13.5　ルール管理

ファイアウォールに設定されているルールについて、
既存ルール間の関連性や新規ルールを追加する際の重複性などを確認し、
最適なルール設定をサポートします。
詳しくは、「9 ルール管理」の章をご参照ください。

13.6　コンプライアンス

ファイアウォールに設定されているルールやコンフィグについて、
SANSやPCI-DSSなどの各業界のセキュリティ標準に対する準拠状況や、コンフィグバックアップ、変更管理を実施します。
コンフィグバックアップについては、「10 コンフィグバックアップ」の章をご参照ください。



13.7　検索

任意の検索条件を指定し、該当のログを特定します。

生ログベースの検索と、データベースの集約データを対象とした検索を行います。
詳しくは、「11 ログ検索」の章をご参照ください。

13.8　ツール

Ping、MACアドレス/DNS解決、syslog転送など、各種ツール機能を使用することができます。

13.9　設定

メールサーバー設定やユーザー管理、ログファイルのインポート、アラートプロファイル設定など、FWAを運用する上で必要となる各種設定を行います。

13.10 サポート

本ページは、主に本社サポートやマニュアル（英語）への案内が表示されます。
［コミュニティと詳細］の項目では、インストール環境情報やアップグレード履歴を確認することができます。

> 日本国内における正規のサポート窓口や関連資料については、次章をご確認ください。

14 お問い合わせ窓口と関連資料

日本国内における正規のお問い合わせ窓口および、FWAのユーザーガイドやナレッジベースなどの関連資料について記載します。

14.1　お問い合わせ窓口

製品に関する技術サポート窓口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窓口
https://www.manageengine.jp/support/trial.html

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

保守ユーザー様は、下記のお客様専用ポータル「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窓口
https://www.manageengine.jp/purchase/

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

14.2　関連資料

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

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

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

簡易版スタートアップガイド
https://www.manageengine.jp/products/Firewall_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

・Firewall Analyzer製品ページ
https://www.manageengine.jp/products/Firewall_Analyzer/