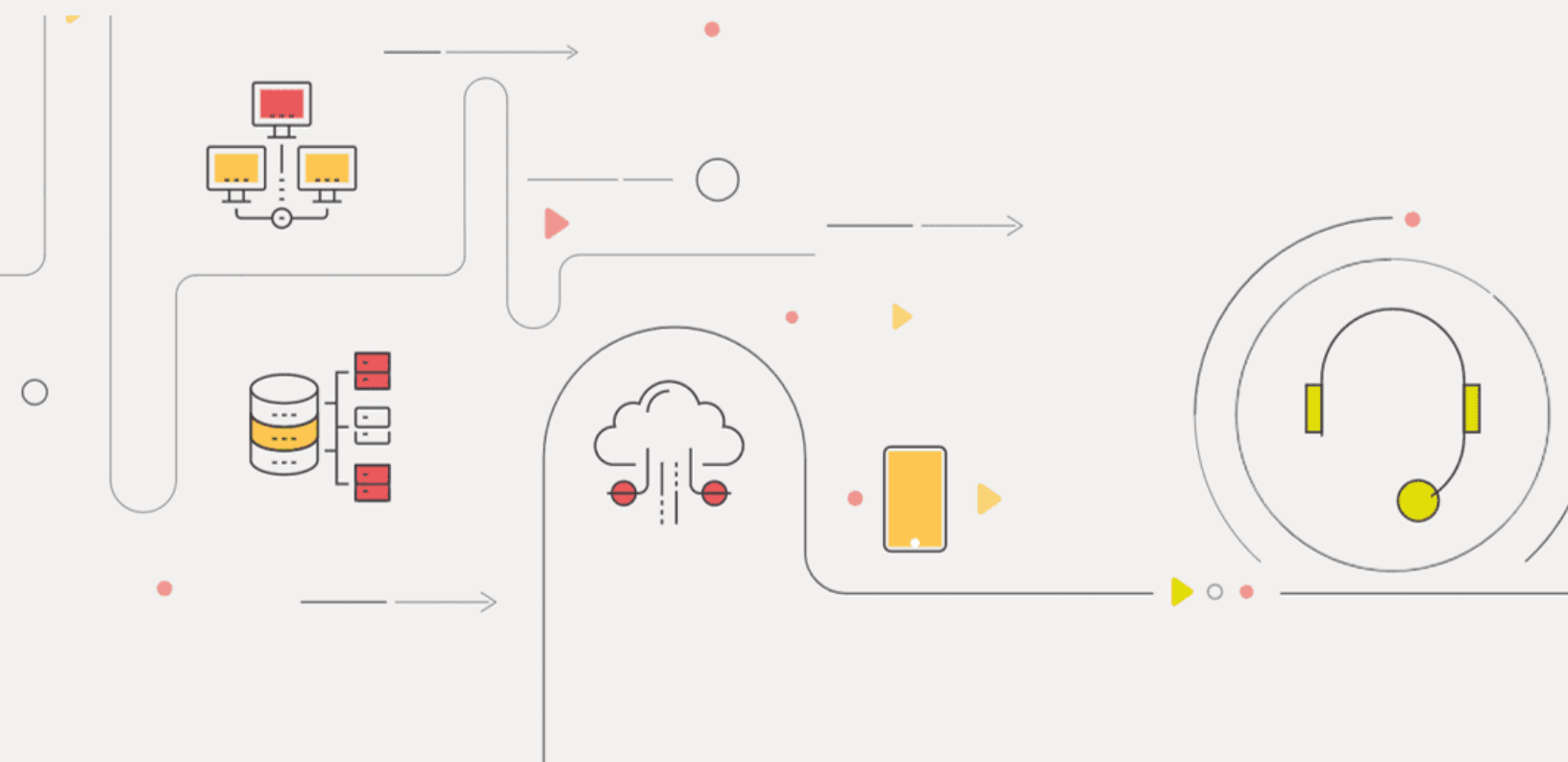


ManageEngine Network Configuration Manager



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、ZOH0 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	Network Configuration Manager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	7
2.1	ハードウェア要件	7
2.2	OS要件	7
2.3	Webブラウザ要件	8
2.4	ポート要件	8
3	NCM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	26
5.1	Webクライアントへのアクセス	26
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	装置追加	30
5.4.1	ディスカバリー	30
5.4.2	手動追加	31
5.4.3	インポート機能による追加	31
5.4.4	装置グループ	33
5.5	認証情報の登録	33
5.5.1	手動登録	33
5.5.2	認証プロファイル	34
5.5.3	認証ルール	35
6	コンフィグバックアップ	36

6.1	手動バックアップ	36
6.2	スケジュールバックアップ	37
7	コンフィグ参照とエクスポート	39
7.1	参照方法	39
7.2	ベースライン世代	40
7.3	差分比較	41
7.4	除外条件の設定	45
7.4.1	Line Exclude	45
7.4.2	Block Exclude	46
7.5	コンフィグエクスポート	47
7.6	コンフィグ世代や操作履歴の保存設定	49
8	コンフィグ変更検出の設定	51
8.1	リアルタイム変更検出	51
8.2	変更通知設定	52
9	コンフィグ変更	54
9.1	コンフィグレットの実行	54
9.1.1	コンフィグレット作成手順	54
9.1.2	コンフィグレット実行	55
9.1.3	コンフィグレットの管理	57
9.1.4	コンフィグレットの実用例	57
9.2	ターミナル	59
9.3	コンフィグアップロード	62
10	ファームウェアの脆弱性の確認	64
10.1	各種レポートについて	64
10.2	脆弱性DBの同期	67
11	コンプライアンスチェック	68
11.1	ルールの作成	68
11.2	ルールグループの作成	71
11.3	ポリシーの作成	71
11.4	コンプライアンスチェックの実行	72
12	スケジュール設定	73
12.1	スケジュールタイプ	73
12.2	スケジュールの追加	74
13	ユーザー管理とロール権限	76
13.1	ユーザー管理	76
13.2	ロール権限	78
13.3	パスワードポリシー	80

14	各メニュータブの説明.....	82
14.1	ダッシュボード.....	82
14.1.1	ダッシュボードの新規作成.....	83
14.1.2	ウィジェットの追加、編集、削除.....	84
14.2	インベントリ.....	86
14.2.1	スナップショット画面.....	88
14.3	コンフィグ自動化.....	89
14.4	ファームウェアの脆弱性.....	90
14.5	コンプライアンス.....	90
14.6	アラート.....	90
14.7	ツール.....	91
14.8	設定.....	91
14.9	レポート.....	92
14.10	サポート.....	92
15	お問い合わせ窓口と関連資料.....	93
15.1	お問い合わせ窓口.....	93
15.2	関連資料.....	94

1 はじめに

1.1 Network Configuration Managerについて

ManageEngine Network Configuration Managerは、マルチベンダー環境におけるネットワーク装置の、コンフィグレーション管理を自動化するNCM（Network Configuration Management）ツールです。

ルーター、スイッチ、ファイアウォール等を対象に、コンフィグ自動バックアップ、変更管理、世代管理、ハードウェア情報管理等を実現し、ネットワーク管理者の負担を削減します。

1.2 本ガイドについて

本ガイドでは、Network Configuration Manager（以下、NCM）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。

NCM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/Network_Configuration_Manager/support.html#eol

本ガイドに記載の範囲は、NCM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。

NCM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/Network_Configuration_Manager/help/

1.3 本ガイドの目的と対象読者

本ガイドは、NCM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構成（管理台数50台）は、以下の通りです。

- CPU : 2.0GHz Dual-Core以上
- メモリ : 4GB以上
- ハードディスク : 100GB以上

管理台数毎のサーバーサイジングの目安は、以下をご確認ください。

管理台数	CPU	メモリ	HDD
1台～50台	2.0GHz Dual-Core以上	4GB	100GB
51台～200台	2.3GHz Dual-Core以上	4GB以上	150GB
201台～500台	2.5GHz Dual-Core以上	8GB	200GB
501台～2000台	3.0GHz Quad-Core以上	8～16GB	300GB
2001台～5000台	3.0GHz Quad-Core以上	16～32GB	300～500GB

※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。

※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おります（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）。

2.2 OS要件

NCM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

NCM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

NCM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	方向	ポート	プロトコル
コンフィグ転送	双方向	22	SCP UDP
	双方向	69	TFTP TCP
syslog変更検出	NW装置 → NCM	514	SYSLOG UDP
WebUI接続	Webクライアント → NCM	8060/8061	HTTP/HTTPS TCP
DB接続 (PostgreSQL)	-	13306	TCP

3 NCM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/Network_Configuration_Manager/download.html

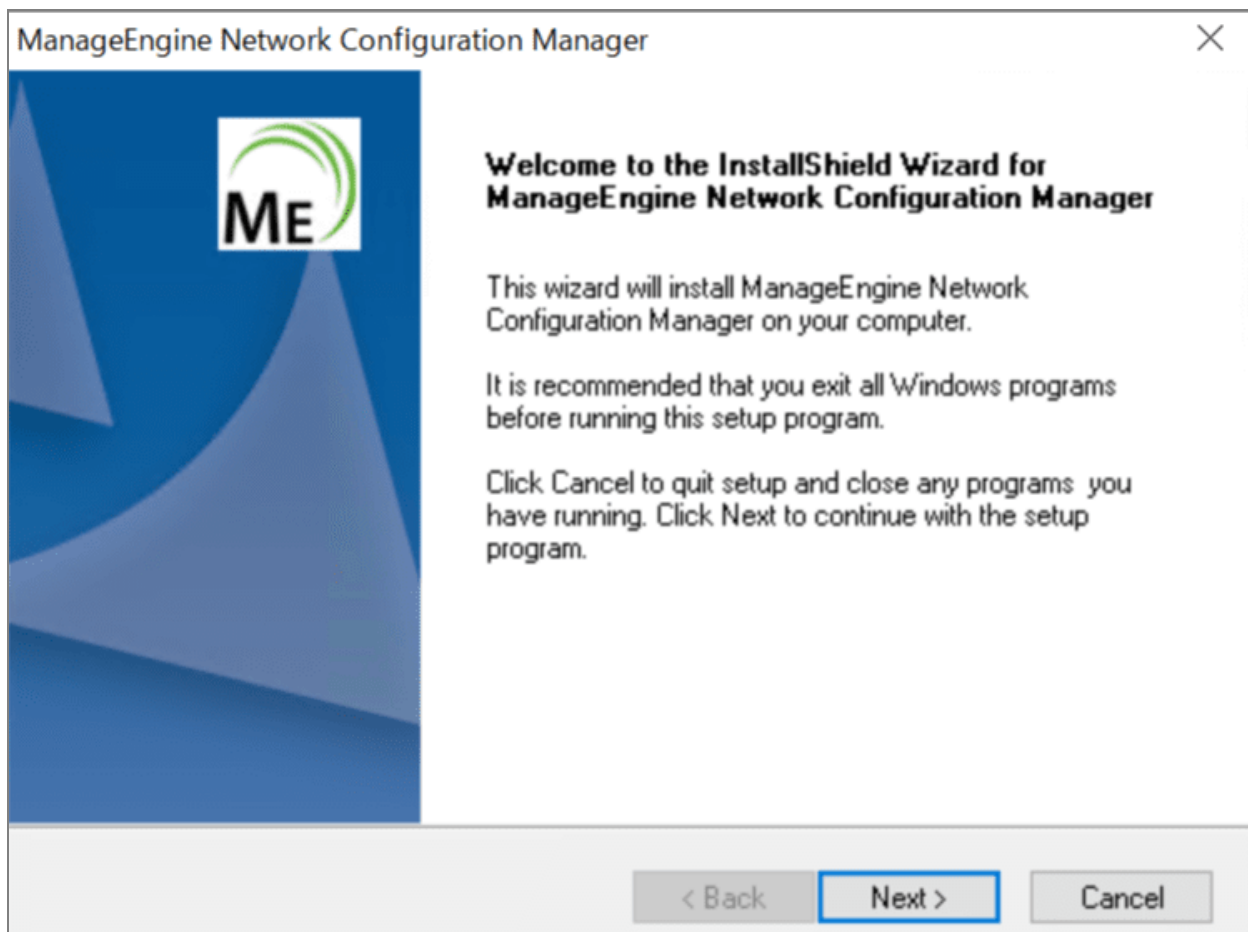
- ・ インストール後30日間は、評価版としてすべての機能を使用できます。30日の評価期間が終了後、正規ライセンスを適用しない場合、自動的に無料版にダウングレードします（管理可能台数2台）。
- ・ 以降のインストール手順でNCMをインストール後、ログイン後のUI [サポート] → [インストール情報] → [インストールディレクトリ] から、ディレクトリパスを確認することができます。詳細は以下のページをご参照ください。

https://www.manageengine.jp/support/kb/Network_Configuration_Manager/?p=4594

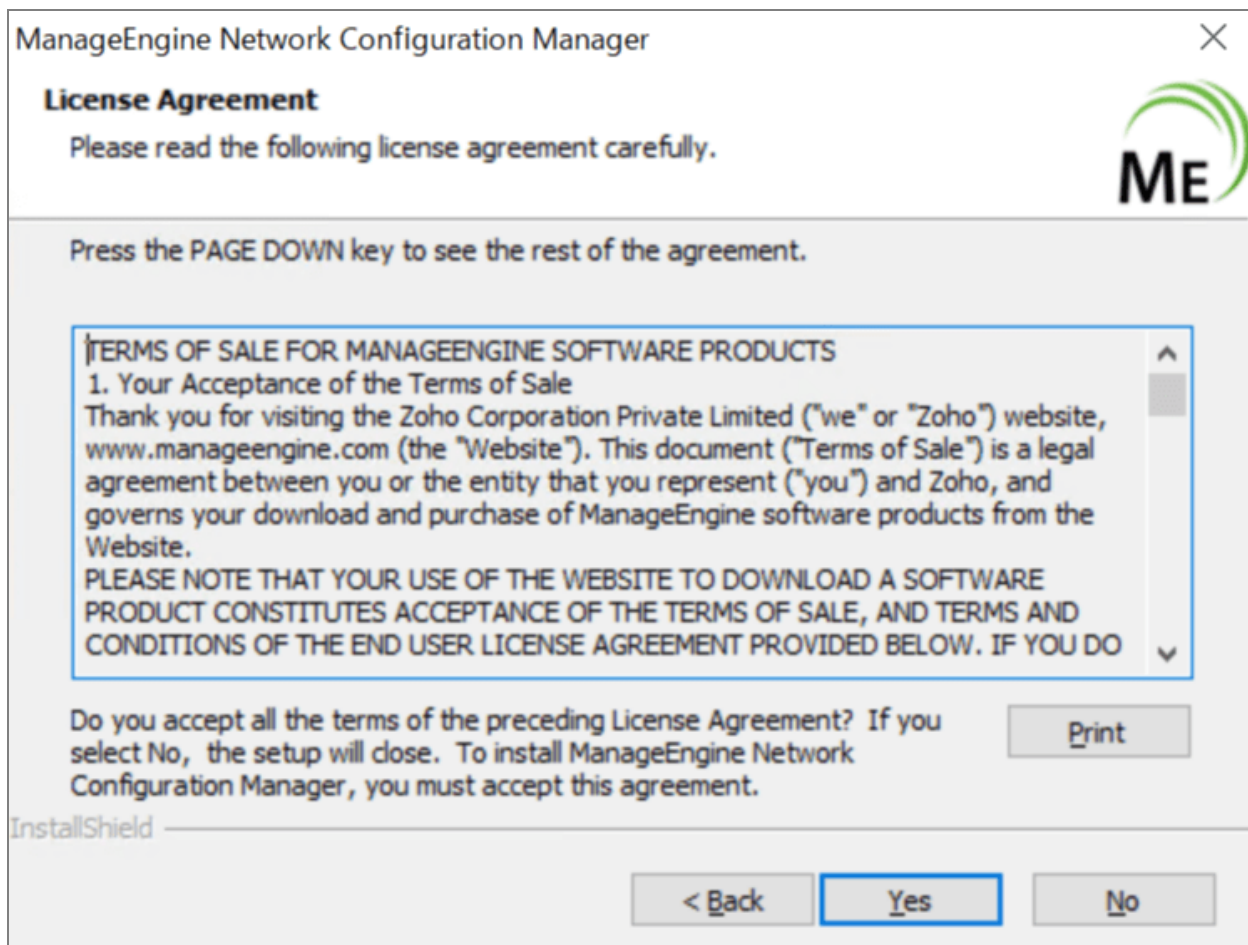
3.2 インストール手順（Windows）

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NCMをインストールします。

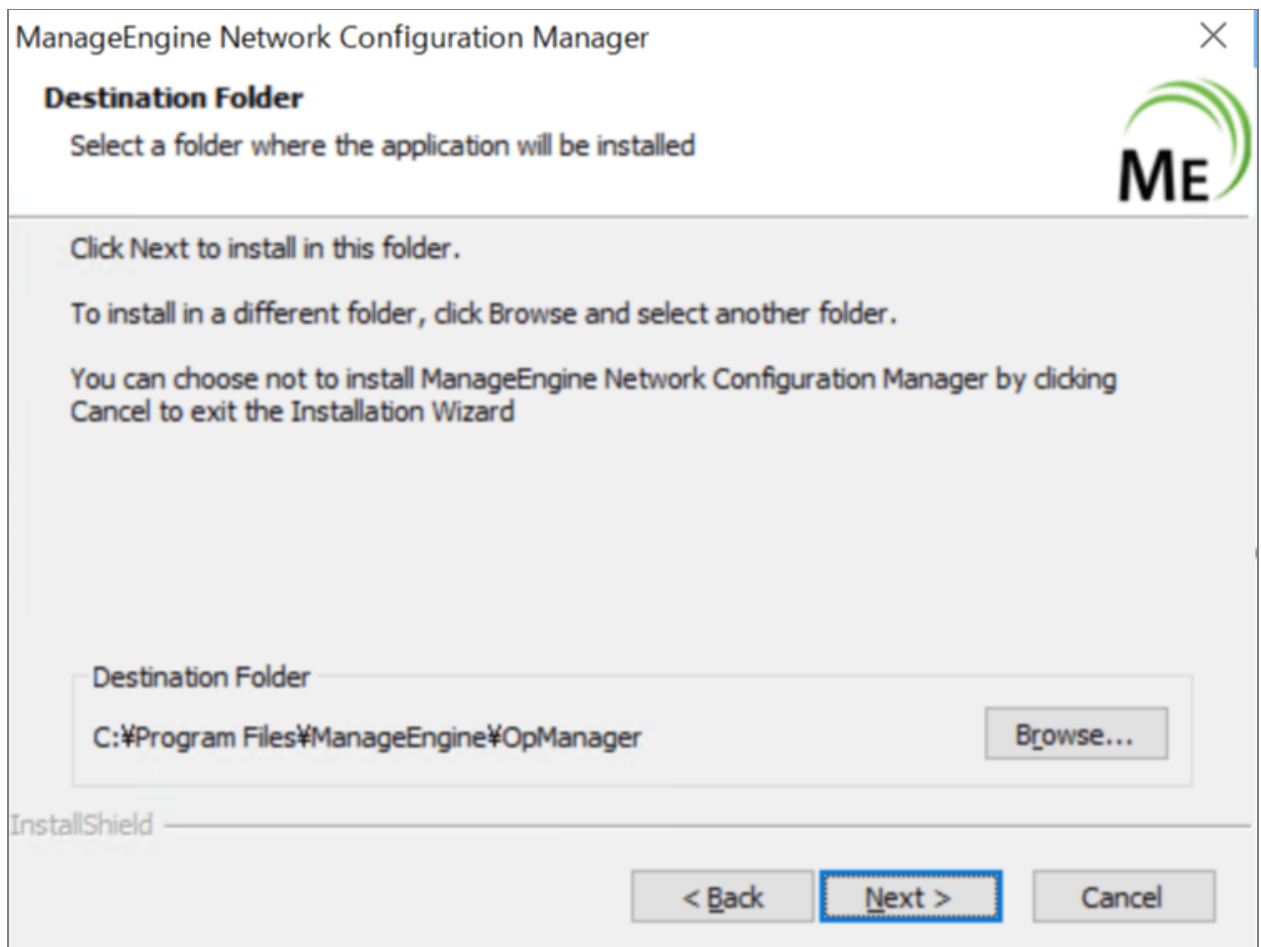
1. インストーラーファイル「
ManageEngine_NetworkConfigurationManager_64bit.exe」を、インストールサーバーに配置
2. 右クリックから管理者権限で実行
以下、インストールウィザードに沿ってインストールを行います。



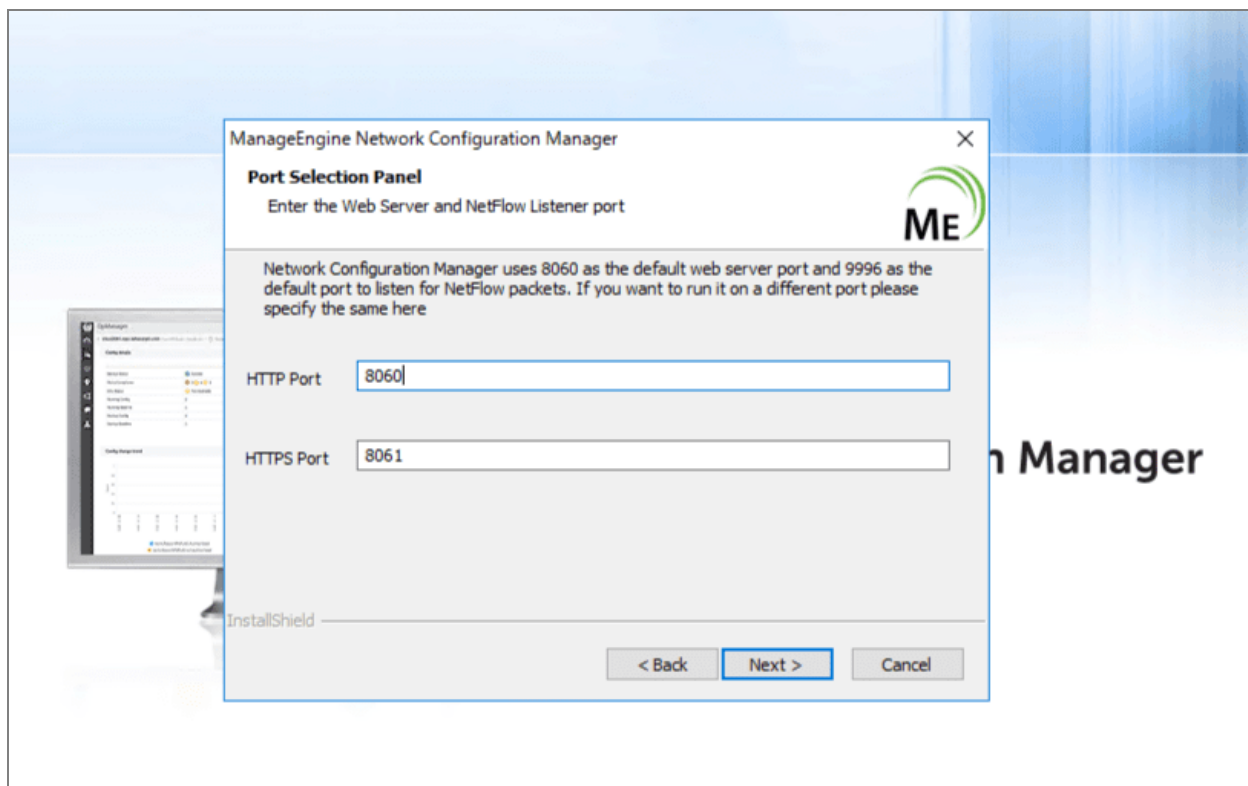
3. ライセンス条項（英語）を承諾後、 [Yes] をクリック



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

ManageEngine Network Configuration Manager ×

Registration for Technical Support (Optional)

Enter Your Details below



Name

E-mail Id

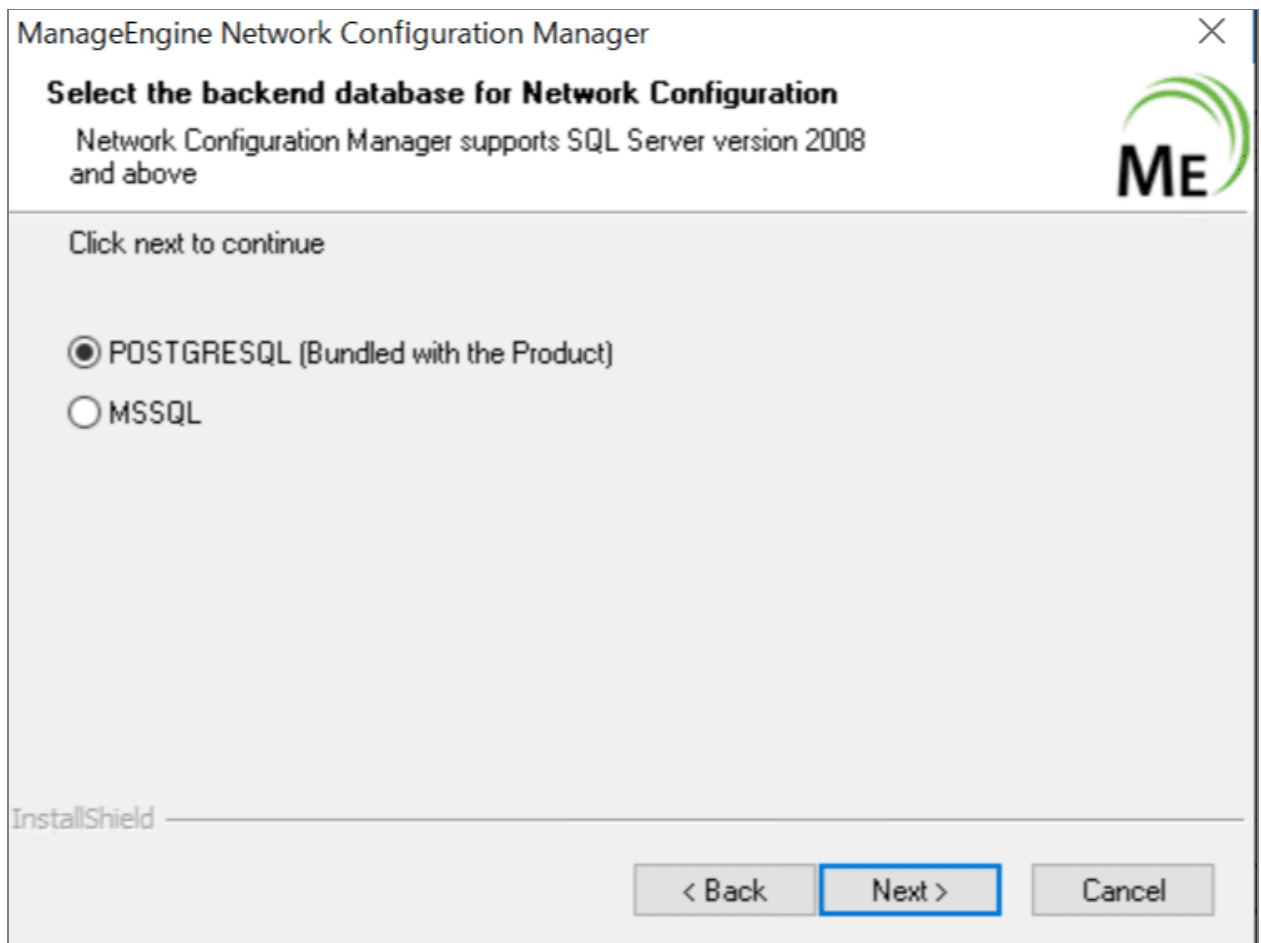
Phone

Company Name

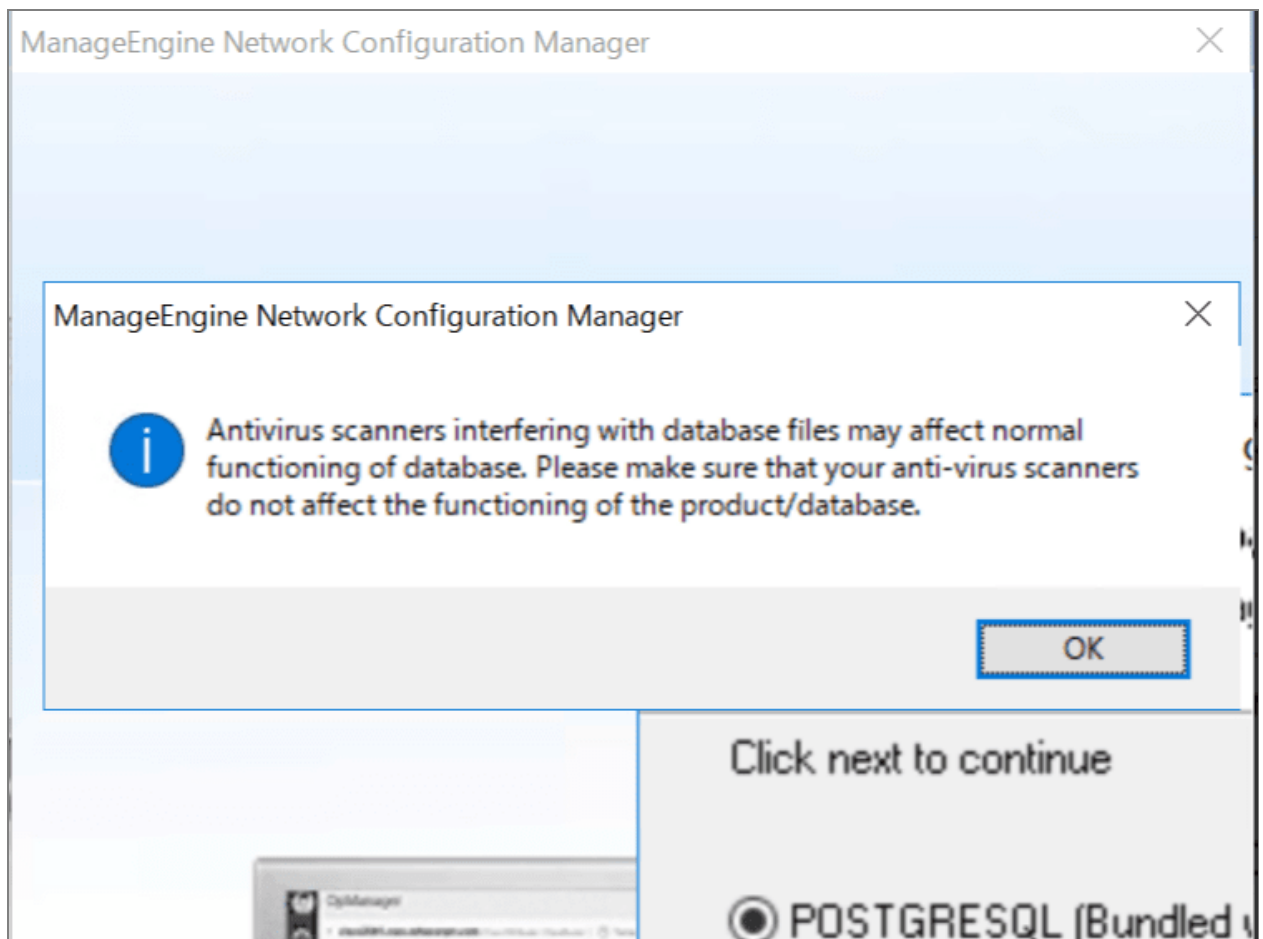
Country

By clicking 'Next', you agree to our [Privacy Policy](#).

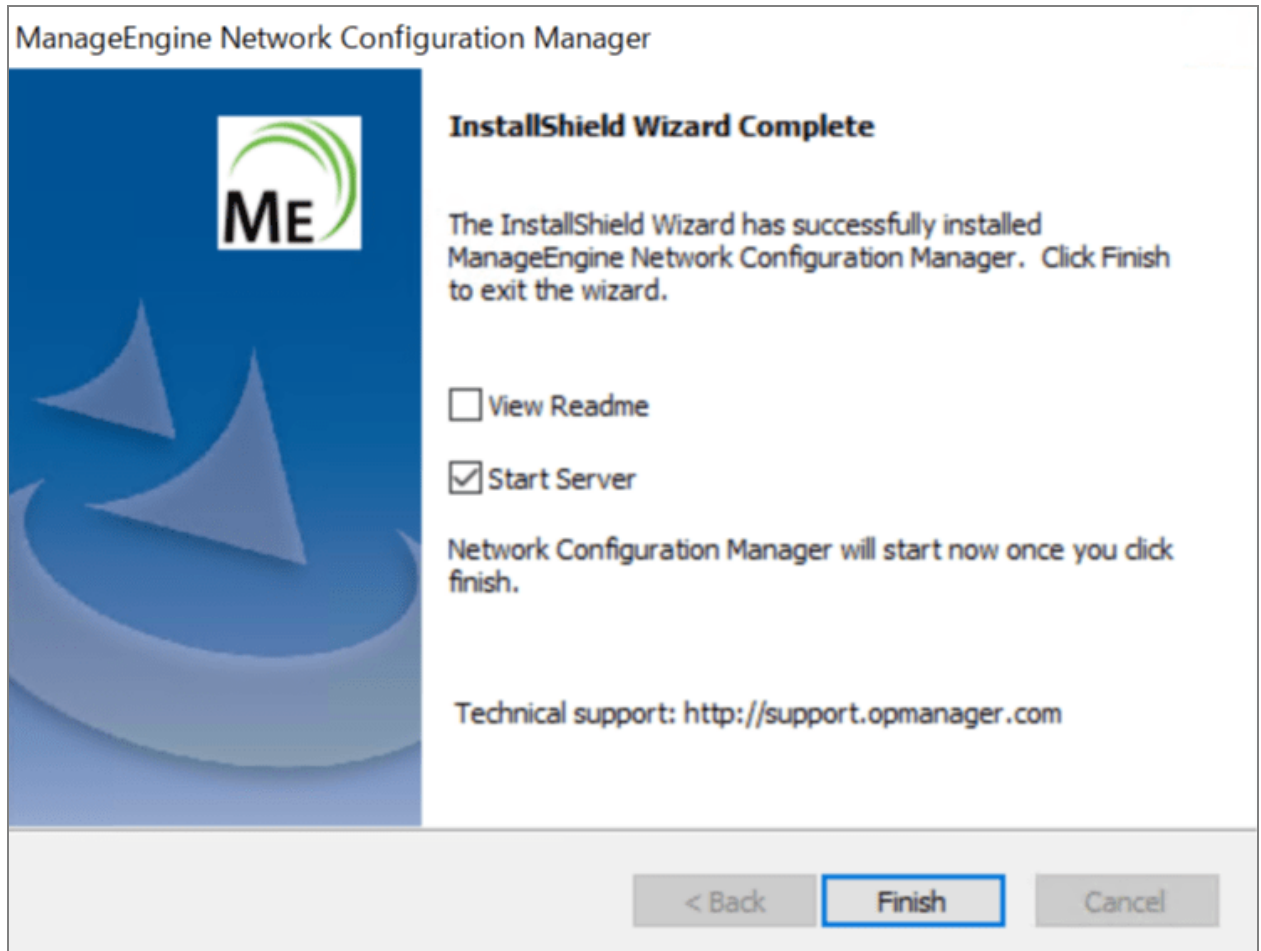
7. 使用するデータベースを選択し、[Next] をクリック
NCMには、PostgreSQLがバンドルされています。
※MS SQLを選択する場合、お客様の方で別途ご用意してください。



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NCM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NCMをインストールします。

1. インストーラーファイル「
ManageEngine_NetworkConfigurationManager_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

```

[root@centos-tmpl ~]# ./ManageEngine_NetworkConfigurationManager_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...

Graphical installers are not supported by the VM. The console mode will be used instead...

=====
ManageEngine Network Configuration Manager      (created with InstallAnywhere)
=====

Preparing CONSOLE Mode Installation...

=====

=====
Introduction
=====

Welcome to the InstallShield Wizard for ManageEngine Network Configuration
Manager

A comprehensive Network, Systems, and Applications Management product that is
easy-to-install, easy-to-use, and extremely affordable.

For help on installation, refer to
https://www.manageengine.com/network-monitoring/installing\_opmanager.html

The InstallShield Wizard will install ManageEngine Network Configuration
Manager on your computer. To continue, click Next.

PRESS <ENTER> TO CONTINUE: █

```

4. ライセンス条項（英語）を確認後、[Y]を入力して続行

14. GENERAL:

If you are a resident of the United States or Canada, this Agreement shall be governed by and interpreted in all respects by the laws of the State of California, without reference to conflict of laws' principles, as such laws are applied to agreements entered into and to be performed entirely within California between California residents. If you are a resident of any other country, this Agreement shall be governed by and interpreted in all respects

PRESS <ENTER> TO CONTINUE:

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): ☐

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)

```
Choose Install Directory
-----

Space recommended on drive : 10GB

Default Install Folder: /opt/ManageEngine/OpManager

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

=====

=====

Webserver port
-----

Enter requested information

Enter the Web Server Port Number (Default: 8060):

=====

Secureserver port
-----

Enter requested information

Enter the Secure Server Port Number (Default: 8061):
```

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


```

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

Please review the following before continuing:

Product Name:
    ManageEngine Network Configuration Manager

Install Folder:
    /opt/ManageEngine/OpManager

Disk Space Information (for Installation Target):
    Required: 642.89 MegaBytes
    Available: 131,658.05 MegaBytes

PRESS <ENTER> TO CONTINUE:

=====
Installing...
=====

[=====|=====|=====|=====]
[-----|-----|-----|-----]

=====
Installation Completed
=====

Congratulations! ManageEngine Network Configuration Manager has been
successfully installed to:

/opt/ManageEngine/OpManager

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

Technical support : http://support.opmanager.com

```

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. NCM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 Network Configuration Manager」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. NCM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NCM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
- ・ NetworkConfigurationManager 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. NCM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、NCM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、service.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. NCMインストールディレクトリ/OpManager/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、service.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
- ・ NetworkConfigurationManager 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. NCMインストールディレクトリ/OpManager/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、サービス登録ならびに起動を行います。

1. 管理者権限（root）で、インストールサーバーにアクセス
2. インストールディレクトリ/OpManager/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. NCMインストールディレクトリ/OpManager/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

NCMを起動後、Webクライアントへアクセスします。

1. 「2.3 Webブラウザ要件」に記載のブラウザを開き、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）

NCM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. NCM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。

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

NCM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〕 → 〔ユーザー管理〕 → 〔ユーザー〕 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〕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。

Network Configuration Manager

ダッシュボード インベントリ コンフィグ自動化 ファームウェアの脆弱性 コンプライアンス アラート ツール 設定 レポート サポート

一般設定 装置管理 ディスカバリ ユーザー管理 認証 タグ 一般 連携 PCI

メールサーバー設定

プライマリメールサーバー セカンダリメールサーバー

サーバー名 ポート番号 タイムアウト (秒)

25 100

送信元メールアドレス (任意項目) 宛先メールアドレス

notification@opmanager.com

認証設定 (任意項目)

認証タイプ

☒ Basic ☐ OAuth

ユーザー名 パスワード

セキュアな接続

☐ SSLの有効化 ☒ TLS有効化 ☐ なし

テストメールの送信

ヘルプ

OAuthは、パスワードの代わりにアクセストークンを使用して、アプリケーションにユーザーアカウントを接続する安全な認証方法です。Network Configuration Managerは、認可プロバイダーへの認可リクエストで、必要な情報を構成します。認可プロバイダーはリクエストを検証した後、ユーザーにプロンプトを表示し、アプリケーションのリクエストを認可するかどうかを確認します。ユーザーの確認後、アプリケーションにアクセストークンが付与され、APIリクエストに使用できるようになります。

要件：リダイレクトURLを使用して、クライアントID/クライアントシークレット/認証URL/アクセストークンURL/スコープを、認証プロバイダーから取得します。Microsoft/Google Authenticatorのサーバーに対応しています。これらのプロバイダーからアクセストークンを生成する方法については、[こちら](#)をご覧ください。

キャンセル 保存

■メールサーバーを設定する目的

- ・ 定期的なレポートをメールで受信
- ・ コンフィグ変更を検出した際のリアルタイムなメール通知を実施
- ・ 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〕から、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ならびにパスワード更新専用の画面が自動で表示されます。

5.4 装置追加

NCMに装置を追加する方法は以下の3つがあります。

- ディスカバリー機能で、ネットワーク内のSNMP対応装置を一括追加
- 手動追加
- ファイルインポートによる追加

追加された装置は、[インベントリ] → [装置] で確認できます。

5.4.1 ディスカバリー

■ ディスカバリー機能を使用する際の前提条件

- ・ SNMPに対応している装置に使用できます。
- ・ [設定] → [装置管理] → [sysObjectIDファインダー] に、追加する装置のsysObjectIDが事前に追加されている必要があります。

以下の手順で、装置を追加します。

1. [設定] → [ディスカバリー] を表示し、[ネットワークディスカバリー] をクリック
2. 以下の中からディスカバリー方法を選択
 - ・ IP/ホスト名：単一の装置を追加
 - ・ IPレンジ：IPアドレスの範囲を指定して追加
 - ・ CSVファイル：CSVファイルをインポートして追加
3. 認証設定からSNMPプロファイルを任意に作成
デフォルトでは、コミュニティ「Public」が追加されています。
4. [ディスカバリー] をクリック

Network Configuration Manager

ダッシュボード インベントリ コンフィグ自動化 ファームウェアの脆弱性 コンプライアンス アラート ツール 設定 レポート サポート(米国)

一般設定 装置管理 ディスカバリ ユーザー管理 認証 タグ 一般 連携 PCI

ネットワークのディスカバリ

☐ IP/ホスト名 ☒ IPレンジ ☐ CSVファイル

☒ v4 ☐ v6

開始IPアドレス
[] - [] - [] - []

終了IPアドレス
[] - [] - [] - []

サブネットマスク
255.255.255.0

認証情報 +

検索

☐ すべて選択

☐ Public

☐ te.st

ディスカバリ

ディスカバリーの実施結果は、[設定] → [ディスカバリー] → [ディスカバリーレポート] から参照できます。

5.4.2 手動追加

対象装置がSNMPに対応していない場合や設定できない場合に、手動で装置を追加することができます。

1. [インベントリ] → [装置] に移動し、画面右上の [+] マークをクリック
2. 追加する装置のホスト名またはIPアドレス、装置のベンダー、装置テンプレート、シリーズ/モデルを入力し、[追加] をクリック

5.4.3 インポート機能による追加

事前に作成したテキストファイルをインポートし、装置を追加することができます。

■フォーマット

<ホスト名/IPアドレス>,<装置テンプレート名>,<シリーズ>,<モデル>

例：

Catalyst2900,Cisco IOS Switch,2900,2924
192.168.111.11,Cisco IOS Router,800,805

1. [インベントリ] → [装置] に移動し、画面右上の [+] マークをクリック
2. [テキストファイルから装置をインポート] → [参照] をクリックし、テキストファイルをインポート

非SNMP装置の追加

×

アクションを選択:

☐ 装置追加 ☒ テキストファイルから装置をインポート

ファイルの場所

参照

キャンセル

インポート

メモ:

テキストファイルから装置をインポートする場合は、次のフォーマットとなっていることを確認してください: (カラム名はフォーマット通りの順、また、それぞれのエントリはカンマ(,)で区切ります) 1行ごとに入力します

フォーマット

<ホスト名/IPアドレス>,<装置テンプレート名>,<シリーズ>,<モデル>

5.4.4 装置グループ

［インベントリ］に追加された装置を、目的や管理構成にあわせてグループ化します。

1. ［インベントリ］ → ［グループ］ を表示
2. 画面右上の［+］をクリック
3. 装置グループ名を任意に入力し、以下の4つの項目からグループ化する装置を選択
 - ・ 装置グループ（Device Group）：既に作成されている装置グループから選択
 - ・ 装置（Devices）：インベントリ画面に追加されている装置リストより個別に選択
 - ・ 基準（Criteria）：ホスト名やIPアドレス、ベンダー等、作成基準となる条件をプルダウン形式で選択
 - ・ インポート（Import）：既に追加されている装置のIPアドレスをテキストファイルで指定しインポート
4. ［保存］をクリック

- ・ ［パブリックグループとする］の選択の有無により、装置グループは「Public」または「Private」として作成されます。
- ・ デフォルトでは、プライベートグループとして作成され、許可されたユーザーのみ装置グループを閲覧できます。
- ・ 装置グループをすべてのユーザーに閲覧可能とする場合には、パブリックグループとして作成します。
- ・ パブリックグループとして一度作成すると、プライベートに戻すことはできません。

5.5 認証情報の登録

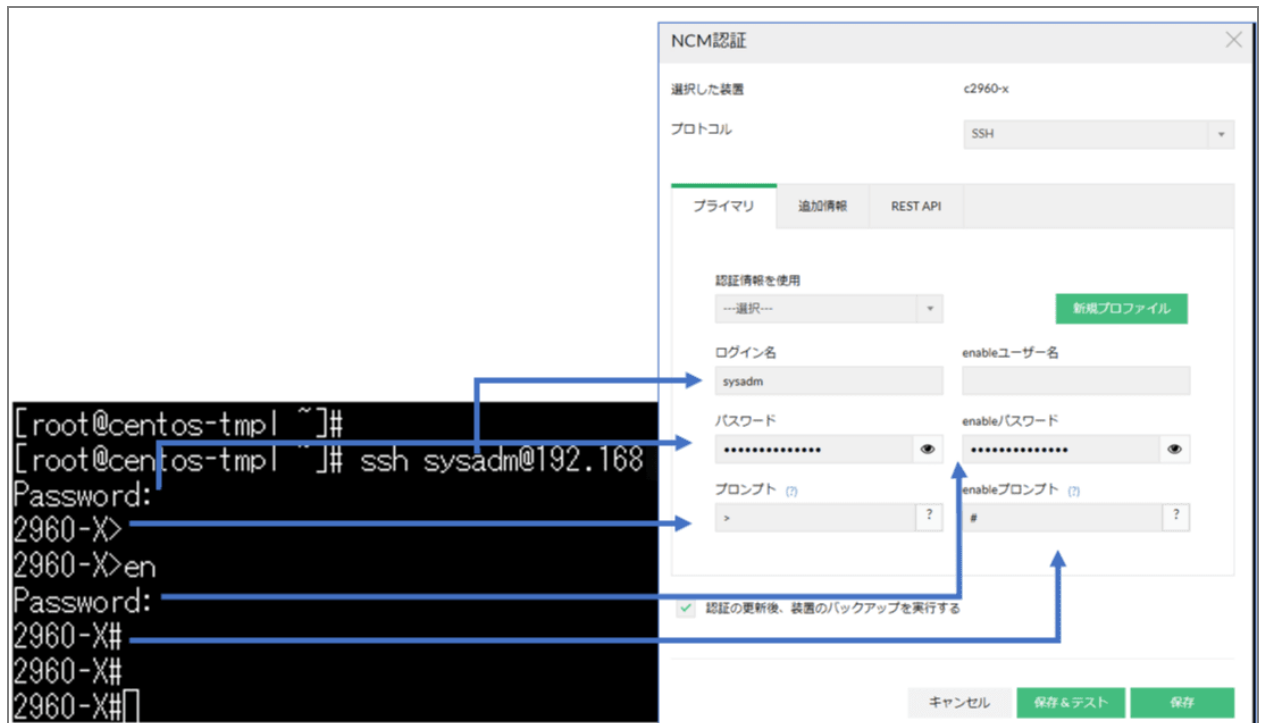
装置を追加後、対象装置とNCM間の通信を確立するために、対象装置の認証情報を登録します。

5.5.1 手動登録

1. ［インベントリ］ → ［装置］ に遷移
2. 対象装置のホスト名左の鍵アイコンをクリックし、［NCM認証］を表示

3. 以下の各情報を入力

プロトコル、プライマリ認証情報（ログイン名、パスワード、プロンプト、enable情報）



「保存とテスト」をクリックすることで、入力した認証情報の有効性をテストします。

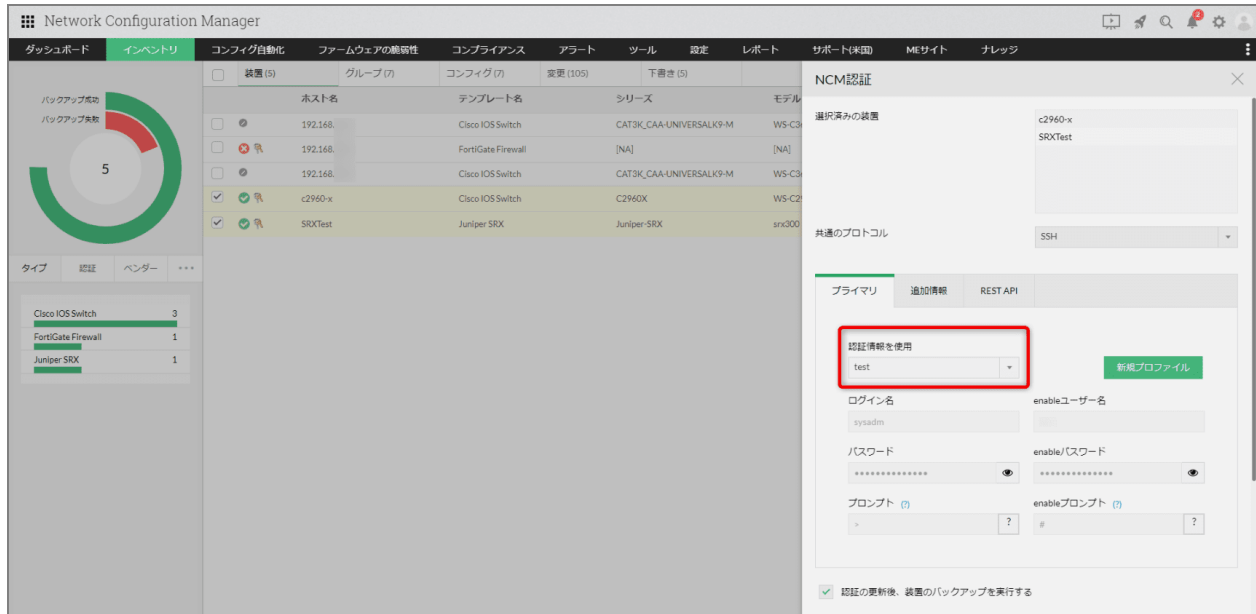
5.5.2 認証プロファイル

複数の装置で共通の認証情報を設定している場合には、認証プロファイルを作成して一括で適用することができます。

1. 「コンフィグ自動化」→「認証設定」→「認証プロファイル」を開き、画面右上の「+」をクリック
2. 「認証情報の追加」で、任意のプロファイル名を入力し、以下の認証タイプより認証情報を入力
 - ・ Telnet認証
 - ・ SSH認証
 - ・ SNMP

認証プロファイルを作成後、以下の手順で適用します。

1. [インベントリ] → [装置] で、認証プロファイルを適用する複数の装置にチェック
2. 画面右上の [...] より、[NCM認証] を選択
3. [NCM認証] で、装置が選択されていることを確認し、プロトコルを選択
4. [プライマリ] タブの [認証情報を使用] で、作成した認証プロファイルを選択



5.5.3 認証ルール

認証ルール機能を使用して、ディスカバリー時に認証プロファイルを自動で適用するフローを設定することができます。

1. [コンフィグ自動化] → [認証設定] → [認証ルール] 右上の [+] をクリック
2. 任意のルール名を入力
3. [条件の設定] を選択し、認証プロファイルを適用する装置の条件（ホスト名や IP アドレス、ベンダーなど）を設定
4. プロトコル、認証プロファイルをプルダウンより選択
5. [ルールの有効化] にチェックを入れ、保存

Network Configuration Manager

ダッシュボード インベントリ **コンフィグ自動化** ファームウェアの脆弱性 コンプライアンス アラート ツール 設定 レポート サポート(米国)

認証ルールを追加

ルール名
test

説明

装置の選択
● 条件の設定 ○ 装置グループ

条件選択

条件	操作	値	追加
1 IPアドレス	次の文字列で始まる	192.168	+
2 ベンダー	次に等しい	Cisco	+

条件の設定 パターン
(1 AND 2)

プロトコル
SSH

認証プロファイル
test_cat1

☒ ルールの有効化

キャンセル 保存

認証ルールの実行履歴は、[コンフィグ自動化] → [認証設定] → [監査詳細] に表示されます。

6 コンフィグバックアップ

認証情報を設定した装置との通信を確立した後、コンフィグをバックアップします。

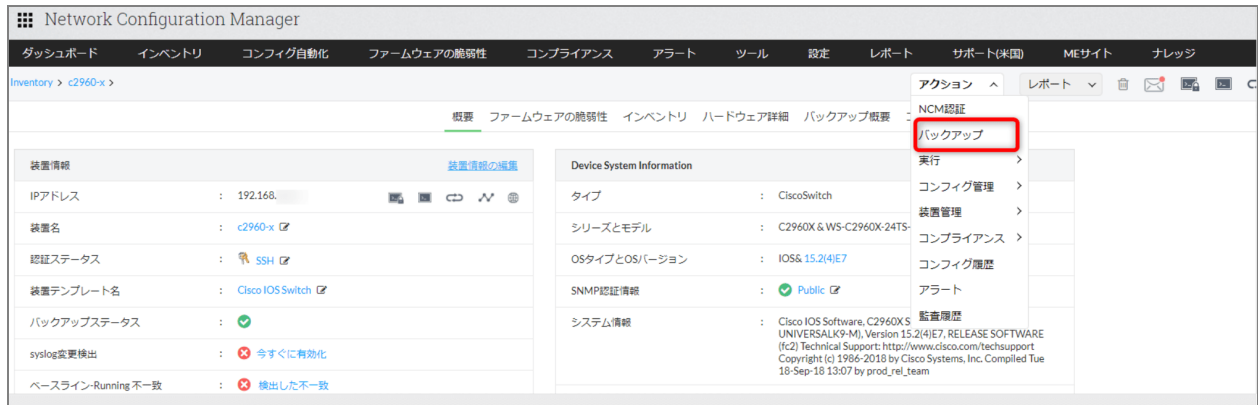
6.1 手動バックアップ

単一装置に対してバックアップを行う場合

1. [インベントリ] → [装置] で、対象装置をクリック
2. スナップショット画面上部の [アクション] → [バックアップ] をクリック

バックアップが正常に終了すると、[最新操作] のステータスが [Backup] となり、緑色のマークで表示されます。

バックアップに失敗すると、赤色のマークが表示されます。



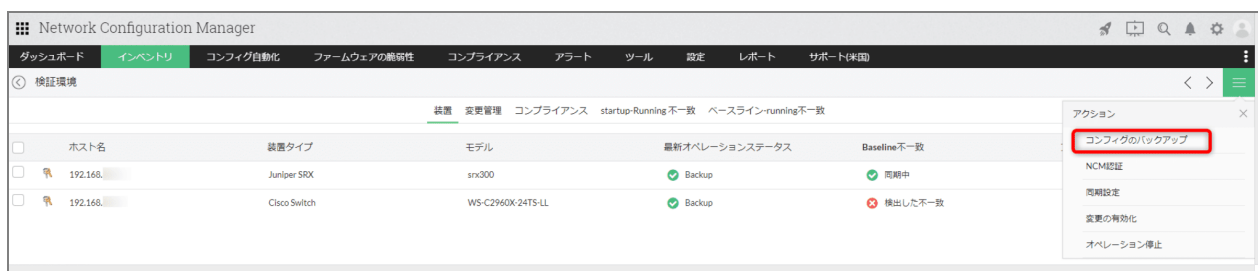
複数装置や装置グループに対してバックアップを行う場合

- ・ 複数装置を指定してバックアップを実行する手順

1. [インベントリ] → [装置] で、対象装置ホスト名の左のチェックボックスにチェック
2. 画面右上に表示される [...] → [バックアップ] を選択

- ・ 装置グループに対してバックアップを実行する手順

1. [インベントリ] → [グループ] → 対象の装置グループをクリック
2. 画面右上の [=] → [コンフィグのバックアップ] をクリック



6.2 スケジュールバックアップ

スケジュールを作成して、コンフィグバックアップの実行を自動化します。

1. [コンフィグ自動化] → [スケジュール] を表示

- 画面右上の [+] アイコンをクリック
- 任意のスケジュール名を入力し、スケジュールタイプ [Configuration Backup] を選択
- バックアップを実行する対象の装置グループまたは装置を選択

Network Configuration Manager

ダッシュボード インベントリ **コンフィグ自動化** ファームウェアの脆弱性 コンプライアンス アラート ツール 設定 レポート サポート(米国)

スケジュールの追加

スケジュール名
コンフィグバックアップ

スケジュールタイプ
Configuration Backup

Device Group
装置グループ:
社内検証機器

Devices

レポート通知 ? ☒ メール ☐ レポートの保存

メールで通知する
(カンマ(,)を使用して複数アドレスを指定します)

メール件名

メモ: レポートには、個人情報が含まれることがあります。レポートは、設定した受信者に、スケジュール通り、送信されます。受信者を設定する際は、十分に、留意ください

☐ バックアップが失敗した場合に通知 ☐ 通知から設定の変更箇所を除外する

- メール通知を任意に設定
※レポートの保存では、NCMインストールディレクトリ
/OpManager/schedule_results/backup/配下に.html形式で保存されます。
- スケジュールを実行する周期（毎時、日次、週次、月次、1回）を指定し [保存]

Network Configuration Manager

ダッシュボード

インベントリ

コンフィグ自動化

ファームウェアの脆弱性

コンプライアンス

アラート

ツール

設定

レポート

サポート(米国)

スケジュールの追加

レポート通知 ?

メール

レポートの保存

メールで通知する

メール件名

(カンマ(,)を使用して複数アドレスを指定します)

メモ: レポートには、個人情報が含まれることがあります。レポートは、設定した受信者に、スケジュール通り、送信されます。受信者を設定する際は、十分に、留意ください

バックアップが失敗した場合に通知

通知から設定の変更箇所を除外する

コンフィグの変更があった場合に通知する

毎時

日次

週次

月次

1回

週次実行

日曜

月曜

火曜

水曜

木曜

金曜

土曜

実行

12

時

00

分

キャンセル

保存

7 コンフィグ参照とエクスポート

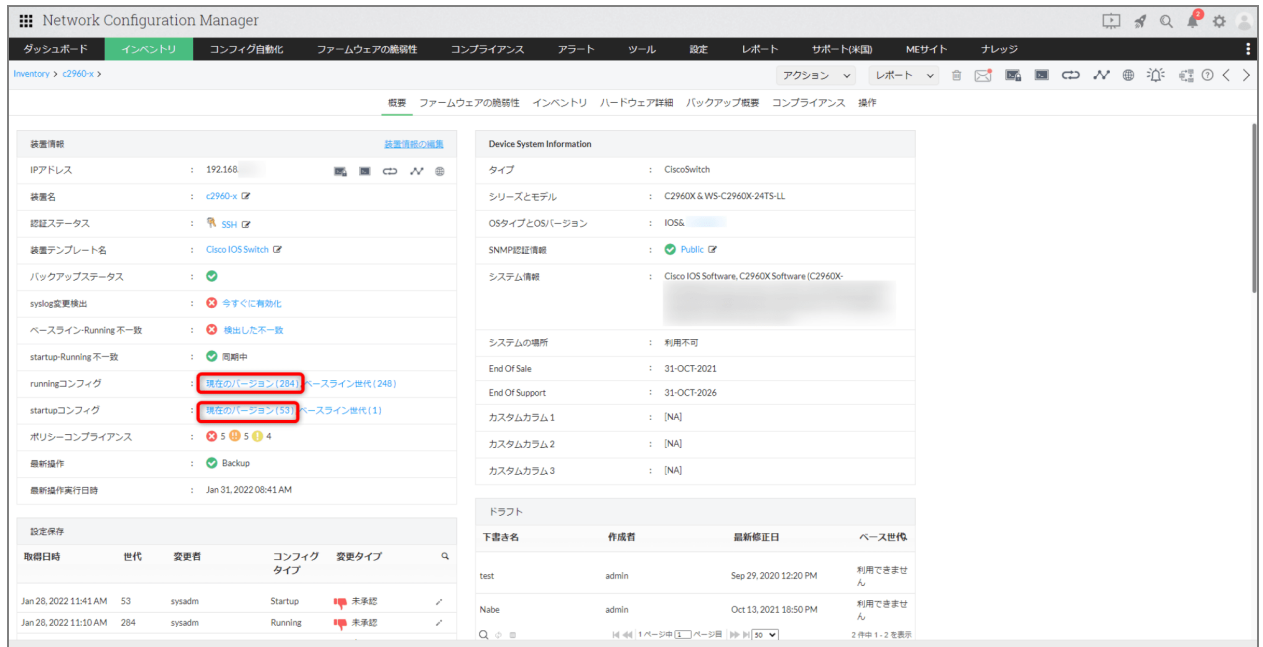
バックアップで取得したコンフィグの参照方法と、テキストファイルとしてコンフィグファイルをエクスポートする方法について記載します。

7.1 参照方法

バックアップで取得したコンフィグは、以下の手順で参照します。

1. [インベントリ] → [装置] 一覧で、対象装置のホスト名をクリック
2. スナップショット画面 [概要] タブを表示
3. [装置情報] ウィジェットから、runningコンフィグまたはstartupコンフィグの [現在のバージョン] リンクをクリック

(C) ZOH0 Japan Corporation. All rights reserved.



4. [コンフィグレーションの表示] アイコンをクリックし、コンフィグ情報を表示



7.2 ベースライン世代

コンフィグ変更後などの運用において、安定性のあるコンフィグ世代（ベース世代）を指定することができます。

ベースとなるコンフィグ世代を設定することにより、障害時など、安全なコンフィグ世代に戻す際に役立つほか、コンフィグ変更が発生した際の差分比較にも使用します。

ベースラインのコンフィグ世代は、デフォルトで第1世代（バックアップを取得した最

初のコンフィグ世代) に設定されます。
以下の手順でベースライン世代を変更します。

1. [インベントリ] → [装置] 一覧で、対象装置のホスト名をクリック
2. スナップショット画面 [概要] タブを表示
3. [設定保存] ウィジェットから対象のコンフィグ世代をクリック
4. コンフィグの内容を確認後、画面右上の [≡] より [ベースラインとして設定] をクリック



[設定] → [一般] → [クライアント/サーバー設定] の [Automatically set newly generated configuration as Baseline] を有効化すると、最新のコンフィグ世代を自動でベースライン世代に設定します。

7.3 差分比較

取得したコンフィグの世代間やベースラインコンフィグとの差分を確認します。
NCMでは、以下の特定のコンフィグ世代を2つ並べて差分を比較することができます。

- RunningコンフィグとStartupコンフィグとの比較
- 直前で取得したコンフィグ世代との比較
- ベースラインコンフィグ世代との比較
- 他装置のコンフィグとの比較

RunningコンフィグとStartupコンフィグとの比較

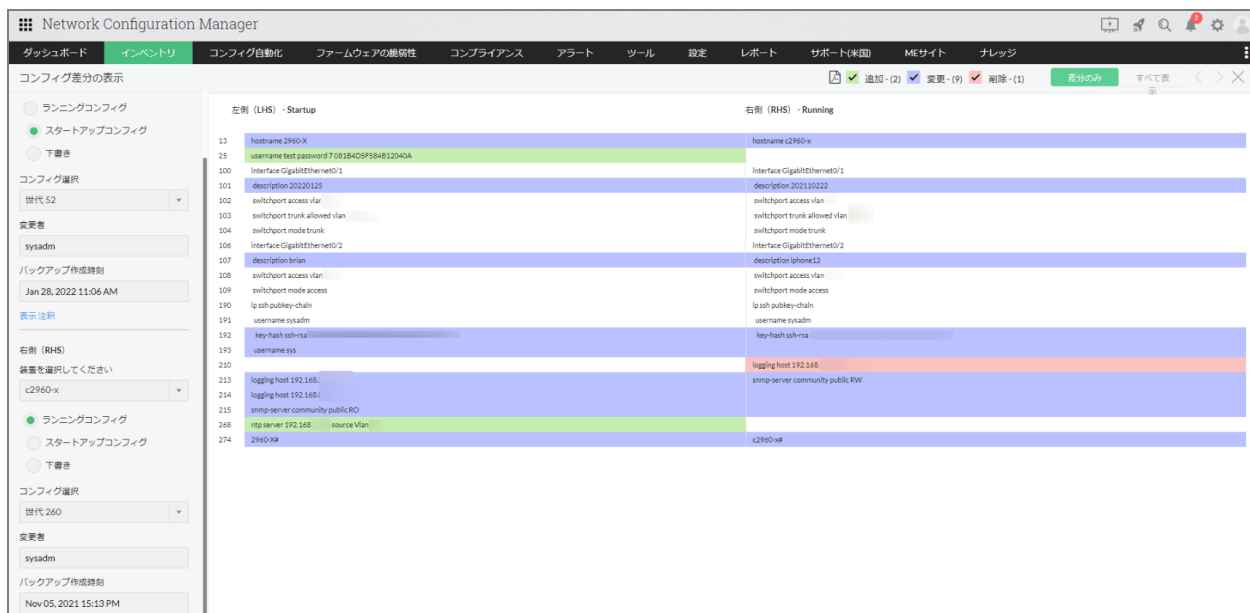
取得したRunningとStartupコンフィグに差分がある場合、スナップショット画面[概要]タブ→[装置情報]ウィジェットの[Startup-Running不一致]のステータスが、[検出した不一致]と表示されます。
※差分がない場合、[同期中]と表示されます。

The screenshot displays the 'Network Configuration Manager' interface. The left sidebar shows the 'Inventory' tab selected. The main content area is divided into two panels. The left panel, titled '装置情報' (Device Information), lists various system details. The 'startup-Running不一致' (Startup-Running Inconsistency) status is highlighted with a red box and shows a green checkmark and the text '同期中' (Synchronizing). The right panel, titled 'Device System Information', provides details about the device, including its type (CiscoSwitch), series (C2960X & WS-C2960X-24TS-LL), OS version (IOS), and system information (Cisco IOS Software, C2960X Software (C2960X-)).

項目	値
IPアドレス	192.168
装置名	c2960-x
認証ステータス	SSH
装置テンプレート名	Cisco IOS Switch
バックアップステータス	成功
syslog変更検出	未検出
ベースライン-Running不一致	検出した不一致
startup-Running不一致	同期中
runningコンフィグ	現在のバージョン(284), ベースライン世代(248)
startupコンフィグ	現在のバージョン(53), ベースライン世代(1)
ポリシーコンプライアンス	5 5 4
最新操作	Backup
最新操作実行日時	Jan 31, 2022 08:41 AM

下書き名	作成者	最新修正日	ベース世代
test	admin	Sep 29, 2020 12:20 PM	利用できません
Nabe	admin	Oct 13, 2021 18:50 PM	利用できません

[検出した不一致] をクリックすると、差分ページが表示されます。



- ・ 差分ページでは、追加、変更、削除が色分けで表示されます。
- ・ 画面上部より、[差分のみ] または [すべて表示] を選択して表示します。

直前で取得したコンフィグ世代、ベースラインコンフィグ世代との比較

スナップショット画面で最新のコンフィグ世代を選択し、
以下をクリックすることで、各コンフィグ世代との差分を表示します。

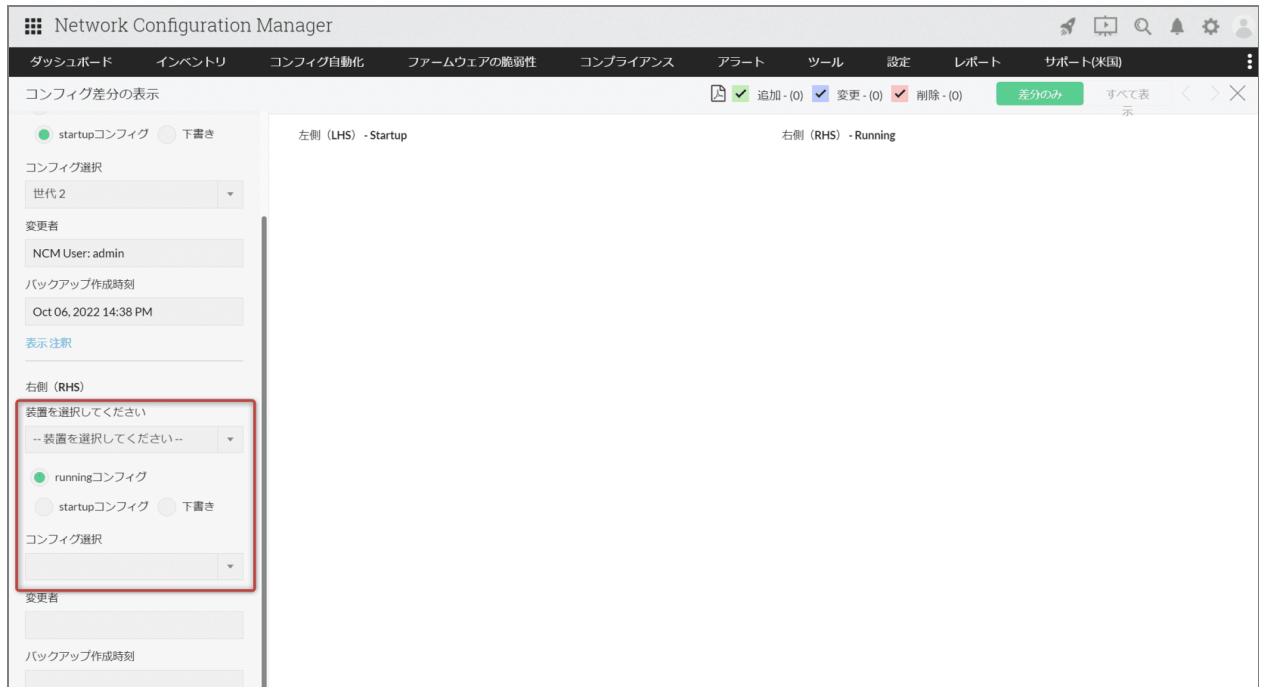
- 以前の世代との比較
- ベースラインと比較



他装置のコンフィグとの比較

他装置の特定のコンフィグ世代と比較します。

1. スナップショット画面より任意のコンフィグ世代を表示
2. 画面右上の [≡] より、[他のコンフィグと比較] を選択
3. 差分比較画面左にある「右側 (RHS)」の [--装置を選択してください--] より、比較対象装置とコンフィグタイプ、世代を選択



7.4 除外条件の設定

コンフィグを表示するたびに動的に変動する値が含まれている場合、バックアップ取得時に、それらも差分として毎回検出されます。

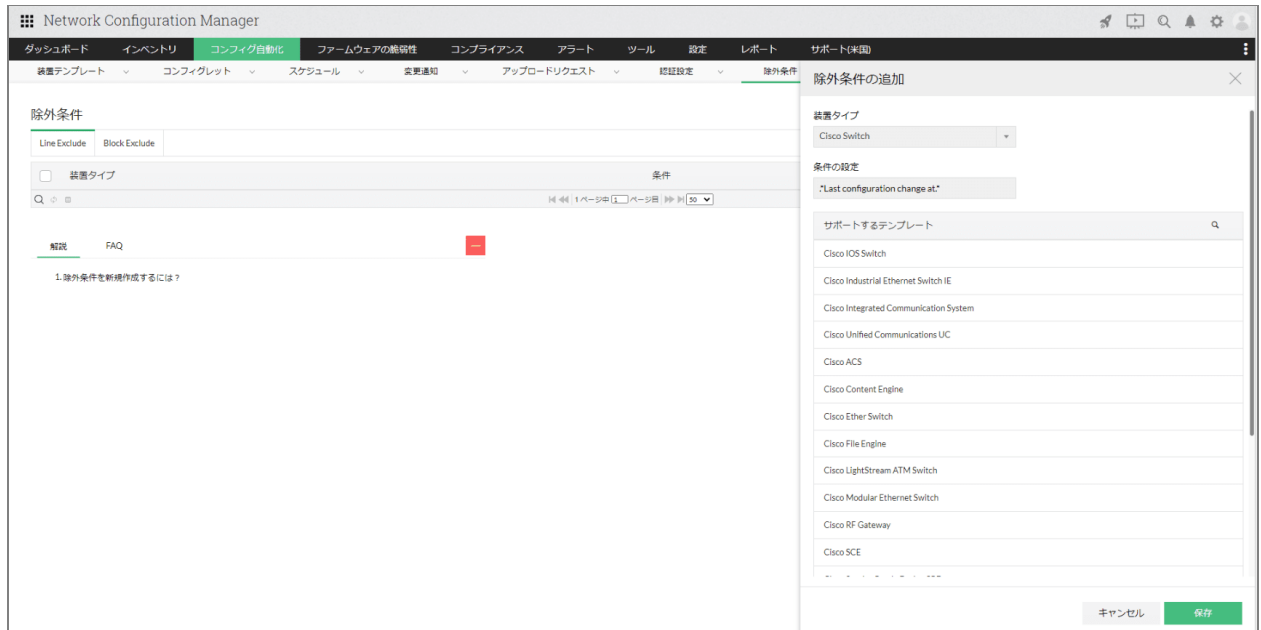
除外条件機能により、差分の検出対象から除外するコンフィグを設定します。

7.4.1 Line Exclude

特定の1行のコンフィグに対して、除外設定をします。

1. [コンフィグ自動化] → [除外条件] → [Line Exclude]
2. 画面右上の [+] をクリック
3. 装置タイプをプルダウンから選択

装置タイプを選択すると、対応する装置テンプレートの一覧が表示されます。



4. [条件の設定] に除外条件を設定し、保存

除外条件例

・ 例1

コンフィグ確認時に先頭に表示される「Last configuration change at 13:40:09 UTC Sun Aug 24 2014 by username」という文字列を除外する場合

.*Last configuration change at.*

・ 例2

コンフィグ表示の際の「building configuration」を除外する場合

.*Building.*

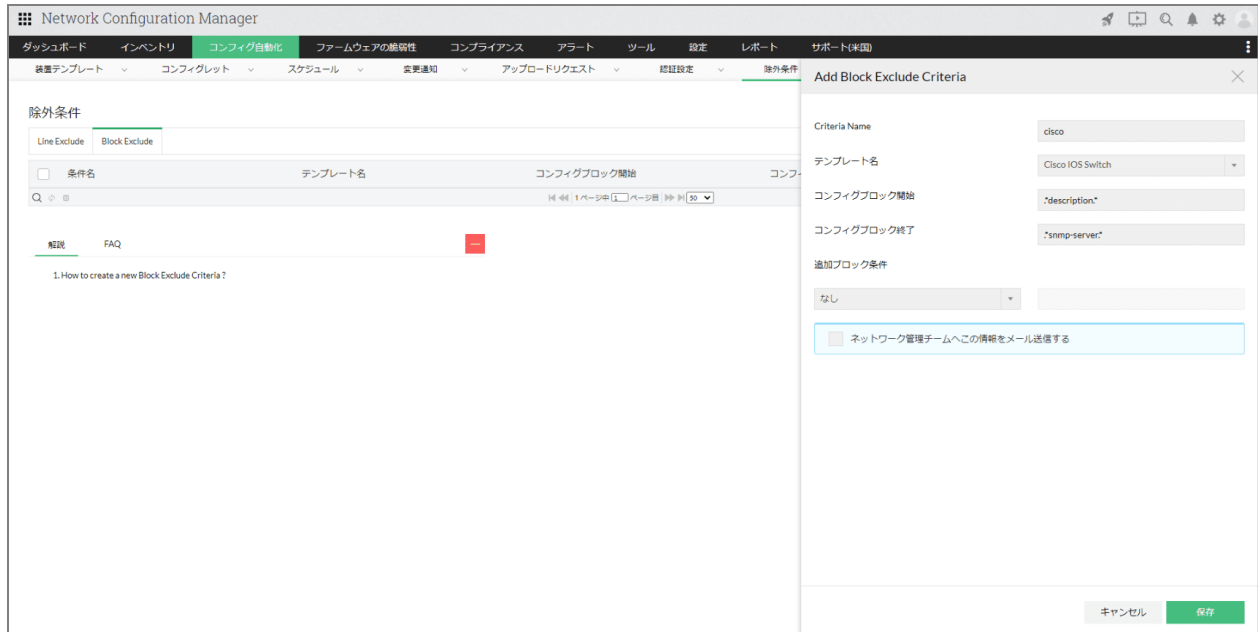
7.4.2 Block Exclude

開始コンフィグブロックと終了コンフィグブロックを設定し、ブロック間のコンフィグを差分対象から除外します。

※設定した開始、終了コンフィグ間以外のコンフィグを変更した場合に、差分として検出されます。

1. [コンフィグ自動化] → [除外条件] → [Block Exclude]

2. 画面右上の [+] をクリック
3. 条件名を任意に入力
4. 適用する装置テンプレート名をプルダウンから選択
5. コンフィグブロック開始、コンフィグブロック終了に、コンフィグ行を入力し保存



7.5 コンフィグエクスポート

バックアップで取得したコンフィグは、NCMのデータベースに暗号化した状態で保存され、UI上に表示されます。

本項では、取得したコンフィグをテキスト形式でエクスポートする方法を記載します。

最新のコンフィグ世代を一括でエクスポートする方法

1. [設定] → [一般] → [コンフィグのエクスポート] を表示
2. エクスポートの実行スケジュールを以下から選択
実施しない、日次、週次、月次
3. スケジュール実行する場合、実行間隔と完了時のメール通知先を設定
4. 対象装置を選択し、以下のチェックボックスを任意に選択
 - ・ 失敗した際に通知
 - ・ すべてのコンフィグを同じフォルダーに入れてください

5. 「出力先」に、テキストファイルを保存するフォルダーパスを入力し保存

- ・スケジュールを設定せず即時的にエクスポートする場合、「今すぐコンフィグをエクスポート」をクリックします。

- ・スケジュール実行で通知機能を使用するには、事前にメールサーバー設定を行う必要があります。

「5.3ログインパスワードの更新とメールサーバー設定」参照

- ・「すべてのコンフィグを同じフォルダーに入れてください」を選択しない場合、ベンダー/対象装置ごとにフォルダーを分割してコンフィグファイルをエクスポートします。

Network Configuration Manager

ダッシュボード インベントリ コンフィグ自動化 ファームウェアの脆弱性 コンプライアンス アラート ツール 設定 レポート サポート(米国)

一般設定 装置管理 ディスカバリ ユーザー管理 タグ 一般 連携 PCI

基本設定

クライアント/サーバー設定 データベース管理 DB同期設定 **コンフィグのエクスポート** 履歴のエクスポート サードパーティ syslogサーバー トラブルチケット設定 SNMPトラップ

☒ 実行しない ☐ 日次 ☐ 週次 ☐ 月次

このオプションを選択するとスケジュールを無効化します

出力先

/opt/ManageEngine/OpManager/config_backup

宛先フォルダー名の記載箇所 2022-01-27

今すぐコンフィグをエクスポート 保存

特定のコンフィグ世代をエクスポートする場合

1. 「インベントリ」→「装置」で対象装置をクリック
2. 装置概要画面「概要」タブの「設定保存」ウィジェットから、対象のコンフィグ世代をクリック
3. コンフィグ内容を確認し、画面右上の「≡」→「コンフィグのエクスポート」をクリック



7.6 コンフィグ世代や操作履歴の保存設定

NCMで保持するコンフィグ世代数や操作履歴の日数を設定します。

[設定] → [一般] → [データベース管理] で、以下の各項目を設定します。

- 次の日数より古い装置操作履歴を削除
レポートや装置概要画面に表示される操作履歴の保持日数を設定します。
デフォルト：無制限
- 最新バージョンを維持
バックアップで取得したコンフィグの保持世代数を設定します。
デフォルト：無制限
※チェックを付けると、「次の日数より古い設定を削除」は設定できません。
- 次の日数より古い設定を削除
バックアップの実施日時をもとに、指定した日数を経過したコンフィグ世代を削除します。
デフォルト：無制限
※チェックを付けると、「最新バージョンを維持」は設定できません。
- 次の日数後、syslogメッセージのトレンドデータを削除します
データベースに保管される毎分のsyslogメッセージ数の情報を削除します。
syslogメッセージ数は、syslogフラッディング検知機能（※）で使用されます。
デフォルト：30日
- 次の日数後、ファームウェア脆弱性の履歴データを削除

〔レポート〕配下にある以下2つのレポートタイプの脆弱性データを削除します。

- ・脆弱性修正トレンドレポート
- ・脆弱性履歴レポート

デフォルト：30日

- ユーザー監査クリーンアップを有効化

〔レポート〕 → 〔Vulnerability & ユーザーレポート〕 → 〔ユーザー監査〕レポートのデータが、DBクリーンアップにより削除されます。

デフォルト：チェックなし

- DBクリーンアップの時刻

上記各設定のクリーンアップ時刻を設定します。

デフォルト：毎日午前2時



(※)

「syslogフラッディング検知機能」では、特定装置から200syslog/2分を受信した場合に、syslog受信を2時間ブロックします。

ブロックされた装置は、〔設定〕 → 〔装置管理〕 → 〔送信したsyslogをブロックされたホスト〕に表示されます。必要に応じて画面右上の〔削除〕からブロックを解除できます。

「syslogフラッディング検知機能」を使用しない場合、[設定] → [一般] → [クライアント/サーバー設定] で、[syslogの受信をブロック] のチェックを外して保存してください。

8 コンフィグ変更検出の設定

コンフィグ変更が発生した際に、いち早く検知し、現在のコンフィグ内容を確認することが重要です。

NCMでは、対象装置のコンフィグが変更された際に、syslogメッセージをもとにリアルタイムで変更を検出し、自動でバックアップを実施します。
また変更検知と同時に、メール送信などの通知アクションを実行する機能が実装されています。

8.1 リアルタイム変更検出

本機能を使用して、予期せぬコンフィグ変更をリアルタイムで検出し、最新コンフィグを自動取得します。

以下の手順でリアルタイム変更検出を有効化、無効化します。

- ・事前に[NCM認証]による認証が確立している必要があります。
- ・対象装置に適用されている装置テンプレートが、[Syslog変更検出の有効化/無効化]に対応している必要があります。[コンフィグ自動化] → [装置テンプレート] → [CLI装置テンプレート]より、装置テンプレートを確認してください。

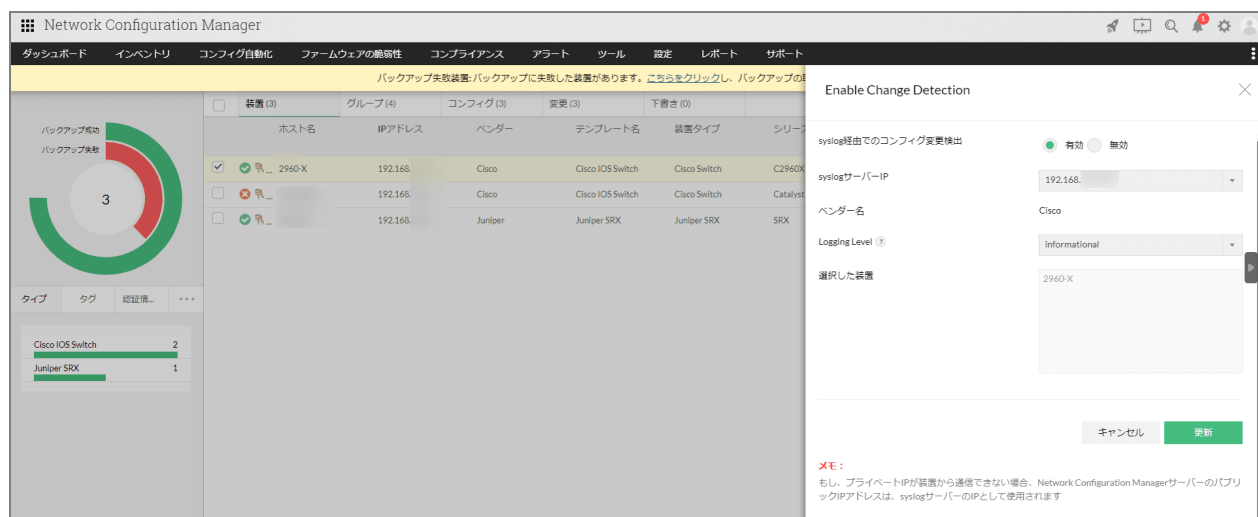
1. [インベントリ] → [装置] で、変更検出を有効化する装置名左のチェックボックスにチェック
2. 画面右上の[・・・]より、[変更の有効化]をクリック
3. [syslog経由でのコンフィグ変更検出]が有効になっていることを確認
 - ・NCMにはsyslogサーバーがバンドルされており、デフォルトではそのIPが指定されています。
 - ・syslogサーバーのIPアドレスを変更する場合、[設定] → [一般設定] →

「[サーバー設定]」の「syslogサーバー」から変更可能です（※変更後、サーバーの再起動が必要です）。

4. syslogサーバーのIPアドレスを選択
5. 「Logging Level」を指定し、選択している装置に誤りがないことを確認
6. 「更新」ボタンをクリック

装置テンプレートに実装されているコマンドをもとに、syslogメッセージを転送するコンフィグ変更が行われます。

※syslog変更検出機能を無効化する場合には、上記手順3.で「syslog経由でのコンフィグ変更検出」を無効として更新してください。



8.2 変更通知設定

コンフィグバックアップやリアルタイム変更検出機能でコンフィグの差分を検知した際に、特定のアクションを実行して通知する機能が実装されています。

NCMでは、以下の5つのアクションから選択することができます。

- メール設定
指定した任意のメールアドレスに通知します。
- SNMPトラップの送信
特定のホストに、SNMPv2トラップを送信します。
- syslogメッセージの送信
特定のsyslogサーバーへ、syslogメッセージを送信します。
- トラブルチケットの作成

ManageEngine ServiceDesk Plusと連携し、ヘルプデスクにトラブルチケットを作成します。

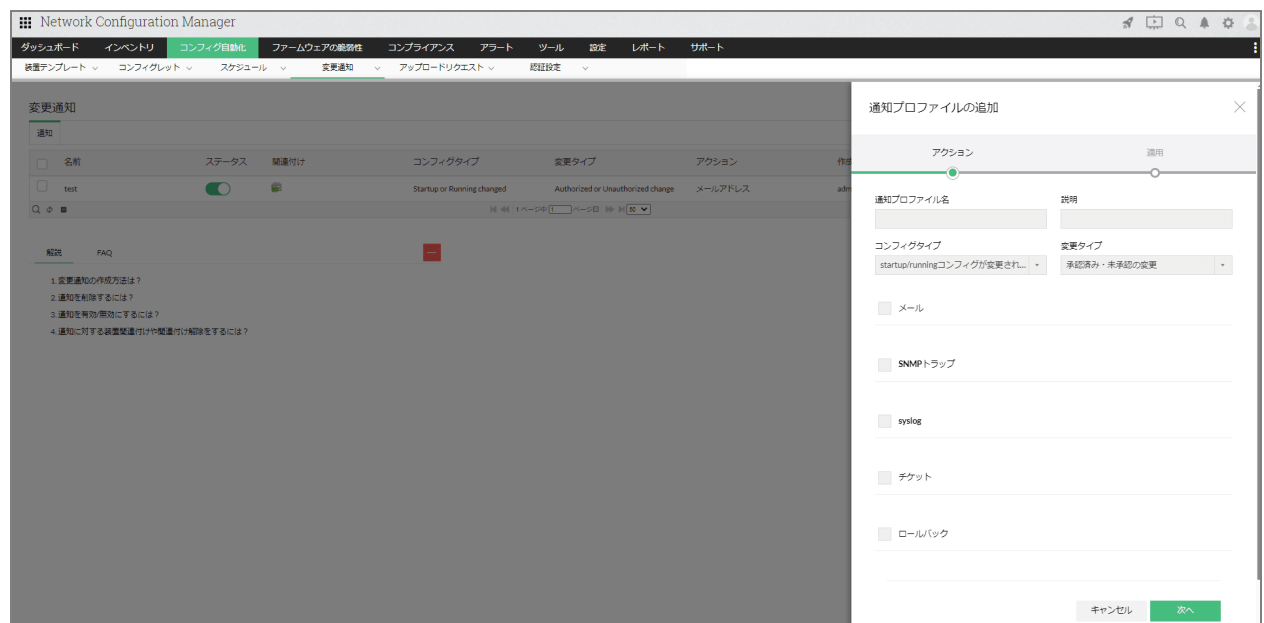
- ロールバック

直前のコンフィグ世代またはベースライン世代にコンフィグを戻します。

※プロトコル「TFTP」に対応している必要があります。

メールアクションを例に、以下の手順で設定します。

1. [コンフィグ自動化] → [変更通知] を開き、画面右上のプラスアイコンをクリック
2. 任意の通知プロファイル名を入力
3. コンフィグタイプのプルダウンより、以下のいずれかを選択
 - ・ StartupまたはRunningコンフィグが変更された場合
 - ・ Runningコンフィグが変更された場合
 - ・ Startupコンフィグが変更された場合
4. 変更タイプのプルダウンより、以下のいずれかを選択
 - ・ 承認済み/未承認の変更
 - ・ 未承認の変更
 - ・ 承認済みの変更
5. メールアクションを選択し、[次へ]



6. 特定の装置または装置グループを指定し、[保存]

保存した変更通知設定は、[コンフィグ自動化] → [変更通知] 一覧に追加されます。一覧から、有効化、無効化、削除ができます。

9 コンフィグ変更

以下の複数の方法で、NCMから対象装置のコンフィグを変更することができます。

- コンフィグレット
- ターミナル
- コンフィグアップロード

9.1 コンフィグレットの実行

複数装置に同じコマンドを投入する場合や、特定の時間帯にコンフィグ変更を行う場合、
コンフィグレット機能で、投入するコマンドセットを事前に作成し、特定の装置に特定の時間帯に投入するよう設定します。

コンフィグレット機能で使用するモードには、以下の3つがあります。

モード	概要
ファイル転送モード	「TFTP」でコンフィグをアップロードします。 ※対象装置ならびに適用されている装置テンプレートが、プロトコル「TFTP」に対応している必要があります。
スクリプト実行モード	CLIベースでコマンドを実行します。 ※実行するコマンドが1行の場合や、コマンド実行後にプロンプト情報（#、>など）が変化しない場合に使用します。
アドバンスドスクリプト実行モード	コマンドラインで装置に接続して、一連のコマンドを実行する際、プロンプト情報（#、>など）が変化する場合に使用します。 例：OSイメージファイルのアップロード

9.1.1 コンフィグレット作成手順

以下の手順で、コンフィグレットを作成します。

1. [コンフィグ自動化] → [コンフィグレット] → [CLIコンフィグレット] 右上の[+]をクリック
2. [コンフィグレットの追加] で、任意のコンフィグレット名を入力し、実行モードを選択
3. [ベンダー] で、Allまたは特定のベンダー名を選択
コンフィグレット実行時に該当のベンダー装置のみを表示し、装置選択を簡略化します。
4. [コンフィグレット内容] に、投入予定のコマンドを入力
変数の入力も可能です（例：snmp-server community %COMMUNITY% RO）。
変数を含むコマンドを追加した場合、コンフィグレット実行の際、変数に指定する値を要求されます。
5. [コンフィグバックアップ] にチェックを入れ、保存

The screenshot shows the 'Network Configuration Manager' interface. The top navigation bar includes 'ダッシュボード', 'インベントリ', 'コンフィグ自動化' (highlighted), 'ファームウェアの脆弱性', 'コンプライアンス', 'アラート', 'ツール', '設定', 'レポート', and 'サポート(米国)'. The main section is titled 'コンフィグレットの追加'. It contains several input fields: '名前' (Name) with a text box, '実行モード' (Execution Mode) with a dropdown menu set to 'スクリプト実行モード', 'ベンダー' (Vendor) with a dropdown menu set to 'All', and '説明' (Description) with a text box. Below the description field is a light blue informational box with the following text: 'メモ：変数名「NO_ENTER」や「NO_RESPONSE」は、システムで定義されており、使用できません。通常の変数は、「LV」や「for」で書き始めることができません。ループ変数には必ず「LV」で始まる名前をつけてください' (Note: Variable names 'NO_ENTER' and 'NO_RESPONSE' are defined in the system and cannot be used. Normal variables cannot start with 'LV' or 'for'. Loop variables must start with 'LV'). Below this box is the 'コンフィグレット内容' (Configlet Content) section with a large text area.

9.1.2 コンフィグレット実行

作成したコンフィグレットは、コンフィグレットの一覧ページに追加されます。
単一装置または複数装置に対して、コンフィグレットを実行します。

1. [コンフィグ自動化] → [コンフィグレット] → [CLIコンフィグレット] を表示
2. 実行対象のコンフィグレットで[実行]をクリック



3. コンフィグレットを実行する装置または装置グループを選択
4. [実行前後にコンフィグのバックアップを実行する] にチェックを入れ、実行



コンフィグレットで変数を定義する場合、以下のオプションから選択します。

- ・すべての装置へ同じ値
コンフィグレットを実行する装置に、共通の変数を指定する場合に選択します。
例として、'%COMMUNITY%'では、値として「public」を指定できます。
- ・それぞれの装置へ異なる値
複数装置に個別の変数を指定する場合に選択します。

このオプションを選択した場合、以下のフォーマットに沿ったテキストファイルまたはCSVファイルをインポートします。

フォーマット : RESOURCE,<VARIABLENAME>,<VARIABLENAME>

例 :

RESOURCE,IPADDRESS,MGMTINTERFACE

de-host,192.168.122.2,vlan-mgmt

9.1.3 コンフィグレットの管理

作成したコンフィグレットの編集、削除は、以下の操作で実施します。

編集手順

1. [コンフィグ自動化] → [コンフィグレット] → [CLIコンフィグレット] を表示
2. 編集対象のコンフィグレットをクリック
3. [コンフィグレットの編集] で任意の変更を加え、保存

削除手順

1. [コンフィグ自動化] → [コンフィグレット] → [CLIコンフィグレット] を表示
2. 対象のコンフィグレットを確認し、アクションから削除アイコンをクリック
3. [選択したコンフィグを除外しますか?] というメッセージを確認後、[OK] をクリックし削除
コンフィグレット名左のチェックボックスにチェックを入れ、ページ上部の削除アイコンから複数のコンフィグレットを一括で削除することもできます。

9.1.4 コンフィグレットの実用例

スクリプト実行モードとアドバンスドスクリプト実行モードの実用例を下記に記載します。

スクリプト実行モード

- パスワードを変更
configure terminal
enable password xxxx
exit
- 複数装置にNTPサーバーを指定
configure terminal
ntp server 192.168.x.x
exit

アドバンスドスクリプト実行モード

- 再起動コマンドの実行例
再起動コマンドを実行時に、装置のコマンドラインでyes/no応答がある場合
<command prompt='(y/n)'>execute reboot</command>
<command prompt='NO_RESPONSE'>y</command>
- OSイメージファイルのアップロード
コマンド実行の流れは以下の通りです（※TFTPで転送されます）。
1.投入するOSイメージファイルをTFTPサーバーに配置
2.OSイメージファイルをフラッシュメモリにコピーするためのコマンドを実行
3.TFTPサーバーのIPアドレスを指定
4.フラッシュメモリにコピーするソースファイル名を指定
5.コピー先のファイルを指定

<command prompt=']? '>copy tftp : flash:</command>
<command prompt=']? '>%TFTP_SERVER_IP%</command>
<command prompt=']? '>%SOURCE_FILE_NAME%</command>
<command prompt='confirm'>%DESTINATION_FILE_NAME%</command>
<command timeout='120' suffix='\$NO_ENTER'>y</command>
- TFTPサーバーへ現在のOSイメージファイルをバックアップ
コマンド実行の流れは以下の通りです。
1.使用するコマンド：copy flash <filename> tftp
 <filename>：現在のOSイメージファイルの場所（パス）
2.TFTPサーバーのIPアドレスを指定

3.コピー先のファイルを指定

```
<command prompt=']?'>copy flash:/%SOURCE_FILE_NAME% tftp</command>
```

```
<command prompt=']?'>%TFTP_SERVER_IP%</command>
```

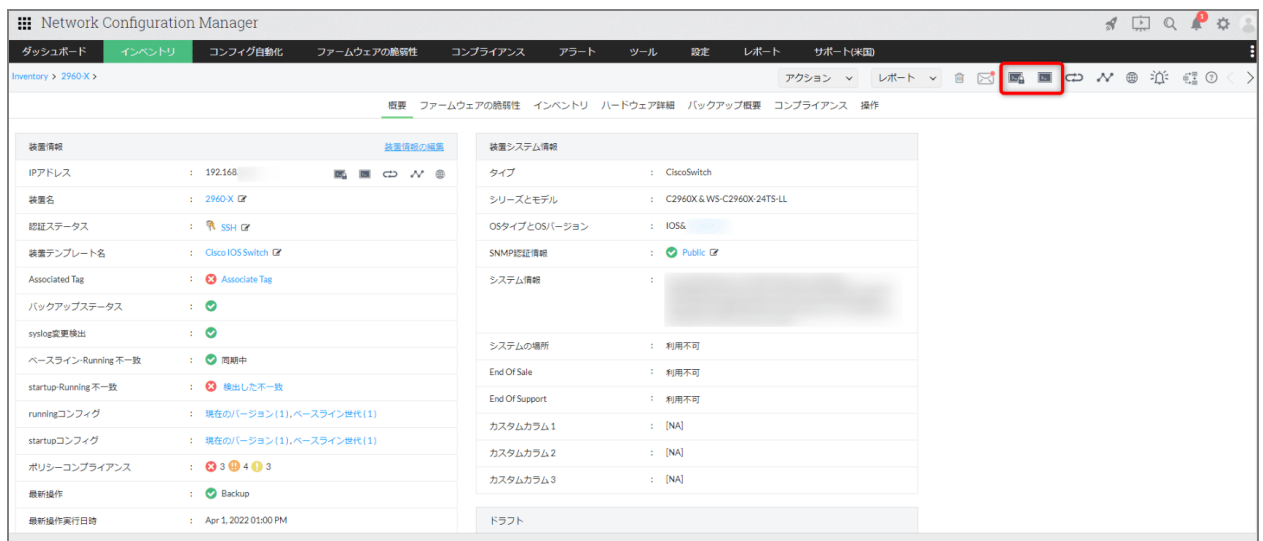
```
<command timeout='70'>%DESTINATION_FILE_NAME%</command>
```

9.2 ターミナル

ターミナル機能では、CLIベースによるコンフィグ操作を装置個別に行います。

ターミナル機能は、以下の2つの画面から使用することができます。

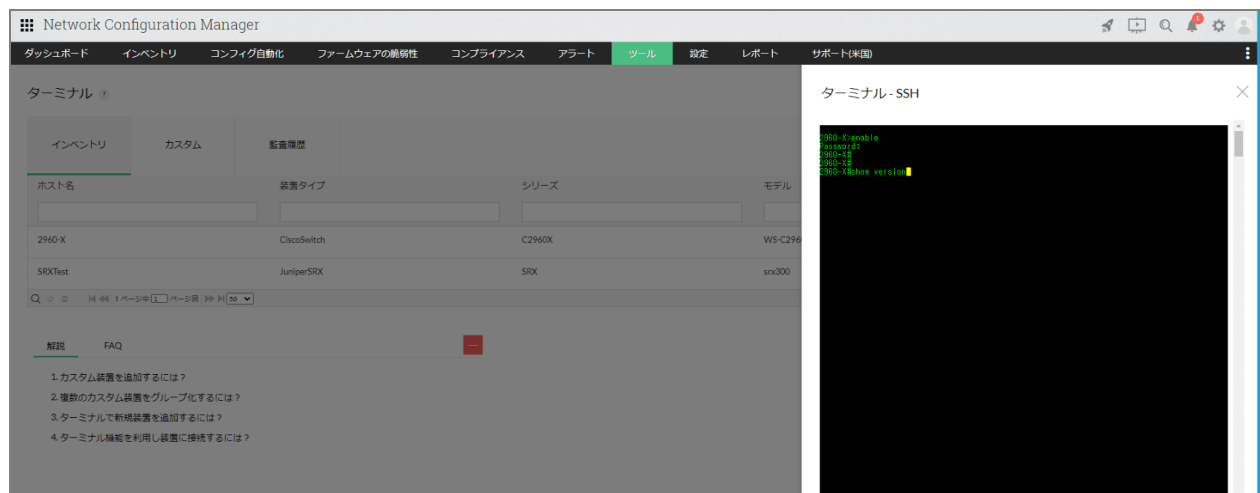
1. [インベントリ] → [装置] → スナップショット画面右上のターミナルアイコン



2. [ツール] → [ターミナル] → [インベントリ] → 対象装置のターミナルアイコン



SSHまたはTelnetアイコンをクリックすることで、以下のようなターミナル画面が表示されコマンド操作を行います。



- ・対象装置の認証情報（NCM認証）を事前に設定している場合、上記のようなターミナル画面が自動で表示されます。
- ・認証情報（NCM認証）を未設定の場合、アイコンをクリック後、認証情報を入力する画面が表示されます。

ターミナル機能（カスタム）

Linux環境などの環境にターミナル接続を行うことができます。

1. [ツール] → [ターミナル] → [カスタム] タブを表示し、画面右上の [追加]

をクリック

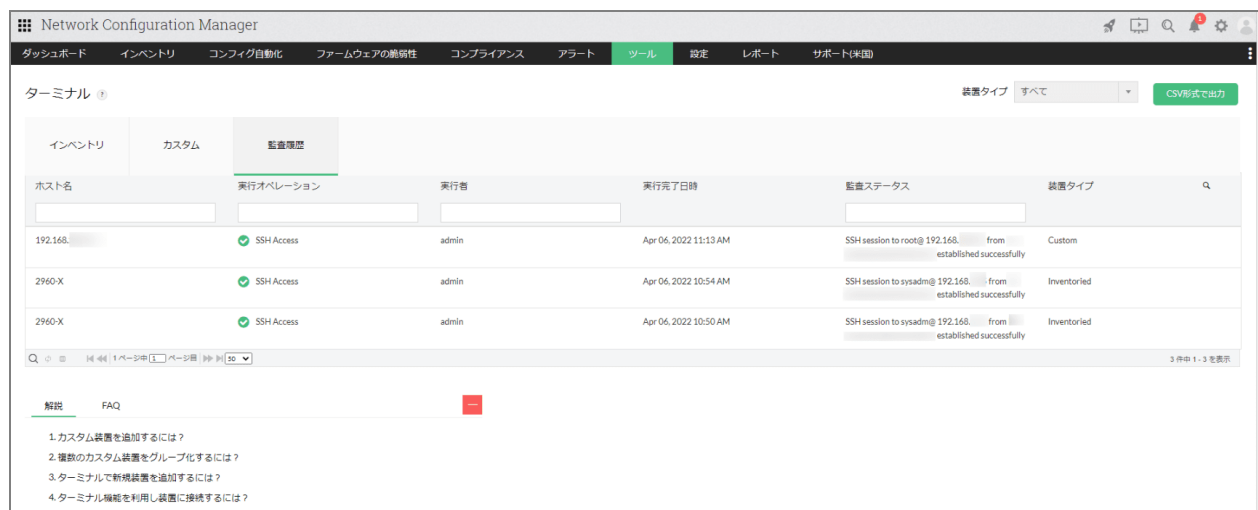
2. リモートホストのIPアドレス、ポート番号、ログイン名/パスワード、プロンプト情報を入力
3. ターミナル装置グループの項目で「+」をクリックし、接続するホストのグループ名を任意に入力し追加
4. 追加したターミナル装置グループを選択し、閲覧権限（自身のみ、管理者、すべてのユーザー）を選択の上、「保存」



ターミナル機能（監査履歴）

ターミナル機能を経由して行ったコマンド操作やその出力内容は、「監査履歴」に自動で記録されます。

ホスト名をクリックし、操作履歴を参照します。



9.3 コンフィグアップロード

アップロードでは、NCMから対象装置にコンフィグを転送します。コンフィグ全体のアップロードや一部のコンフィグのみをアップロードすることができます。

- ・Startupコンフィグにアップロードする場合、コンフィグ全体の内容が記載されている状態で投入してください。

- ・対象装置の認証プロトコルで、「TFTP」または「SCP」が選択されていない場合には以下のメッセージが表示され、アップロードを実行することができません。

「コンフィグアップロードはサポートされていません。TFTP/SCP/SFTPのいずれかのプロトコルを選択してください」

コンフィグ全体をアップロード

1. [インベントリ] → [装置] で対象装置をクリック
2. スナップショット画面 [設定保存] やベースライン世代から、アップロード対象のコンフィグを表示
3. 画面右上の [≡] → [アップロード] をクリック



4. アップロード対象のコンフィグタイプ (Startup/Runningコンフィグ) を選択し、実行タイミング (即時/スケジュール) を指定
5. [アップロード] をクリックし、選択したコンフィグ世代全体をアップロード



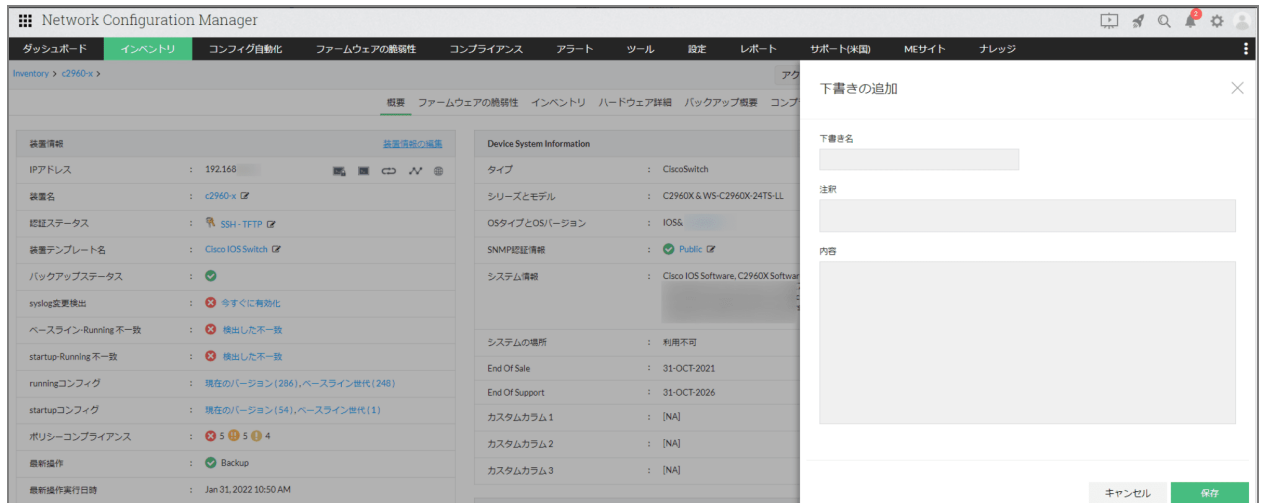
コンフィグファイルの編集（下書き作成）

Startup/Runningコンフィグの取得履歴から任意の世代を選択して、下書きとして編集します。

1. [インベントリ] → [装置] で対象装置をクリック
2. スナップショット画面上部の [アクション] のドロップダウンより、[コンフィグ管理] → [下書きの追加] をクリック



3. 下書き名、注釈、内容（投入するコンフィグ）を記載して保存
保存した下書きは、[概要] タブ → [ドラフト] に追加されます。



4. 追加した下書きをクリックし、内容を確認の上、[≡] → [アップロード] をクリック
5. アップロード対象のコンフィグタイプ（Startup/Running）、投入タイミング（即時/スケジュール）を指定しアップロード

10 ファームウェアの脆弱性の確認

管理対象装置にインストールされているファームウェアバージョンに潜む、脆弱性情報（CVE ID、ベーススコア、関連URLなど）を装置単位で確認します。

10.1 各種レポートについて

NCMの「ファームウェアの脆弱性」機能では、コンフィグバックアップの実行により取得したファームウェアバージョンに潜む脆弱性情報を一覧で表示します。

・ サポート対象ベンダー

Cisco、Juniper、Fortinet、Palo Alto、HP、Aruba、Arista、Dell、Citrix、MikroTik、CheckPoint、F5、Symantec（Blue Coat）、Infoblox、Riverbed、Huawei、NETGEAR、HPE、Juniper（NetScreen）

すべての脆弱性

管理対象装置のファームウェアバージョンに潜む以下の脆弱性情報を一覧で表示しま

す。

- CVE ID
- ベーススコア
- 重要度
- 影響を受ける装置数
- 参照URL

ホスト名右のステータスの項目より、脆弱性（CVE ID）ごとに対応状況を選択できます。

The screenshot shows the 'Network Configuration Manager' interface. At the top, there's a navigation bar with tabs like 'ダッシュボード', 'インベントリ', 'コンフィグ自動化', 'ファームウェアの脆弱性' (selected), 'コンプライアンス', 'アラート', 'ツール', '設定', 'レポート', and 'サポート(米国)'. Below this, there are summary cards for '脆弱性総数' (51), 'Criticalな脆弱性 (CVSS基準)' (2), 'エクスプロイト可能' (0), and '検出した脆弱性' (51). A search bar and filters for '重要度' (critical, important, moderate, low) are present. The main content area displays a table of CVEs. The first entry is 'CVE-2020-1614' with a base score of 10 and critical severity. Below the table, a dropdown menu for 'ステータス' (Status) is open, showing options: 'レポート済み' (Reported), 'レポート済み' (Reported), '確認済み' (Confirmed), '解決策を計画中' (Solution in progress), '解決済み' (Resolved), and '脆弱性の対象外' (Out of scope of vulnerability). The table columns are 'ホスト名', 'ベンダー', '世代', 'シリーズ', and 'モデル'. The first row shows '192.168', 'Juniper', '15.1X49-D50.3', 'SRX', and 'srx300'.

露出装置

脆弱性の影響を受ける「装置」に焦点をおき、該当装置に関する以下の情報を一覧表示します。

- ホスト名
- ベンダー
- 世代（ファームウェアバージョン）
- シリーズ
- モデル
- 脆弱性の数

ホスト名左の [▼] をクリックすると、該当するCVE IDのリストが、ベーススコアの
高いIDから順に表示されます。

The screenshot shows the 'Network Configuration Manager' interface. At the top, there's a navigation bar with tabs: ダッシュボード, インベントリ, コンフィグ自動化, **ファームウェアの脆弱性**, コンプライアンス, アラート, ツール, 設定, レポート, サポート(米国). Below this is a sub-bar with: すべての脆弱性, 露出装置, 配布バージョン, 脆弱性DBの同期, 高度なCVE検索.

Summary cards at the top show: 2 影響を受けた装置総数, 2 Criticalな装置 (CVSS基準), 0 エクスプロイト可能, 51 検出した脆弱性 (最新7日間).

Filters: エクスプロイトステータス: ☒ すべて ☐ エクスプロイト; 装置グループ: All Devices Group; 重要度: **すべて** critical Important Moderate Low; 更新をリクエスト.

ホスト名	ベンダー	世代	シリーズ	モデル	脆弱性の数
▼ 192.168.1.1	Juniper	15.1X49-D50.3	SRX	srx300	1
CVE ID ベーススコア 重要度 脆弱性タイプ エクスプロイト					
CVE-2020-1614 10 重大 利用できません [NA]					
▼ 192.168.1.2	Cisco	15.2(4)E7	C2960X	WS-C2960X-24TS-LL	50
CVE ID ベーススコア 重要度 脆弱性タイプ エクスプロイト					
CVE-2007-5552 9.3 重大 利用できません [NA]					
CVE-2017-6743 8.8 Important 利用できません [NA]					
CVE-2019-16009 8.8 Important 利用できません [NA]					

配布バージョン

脆弱性の影響を受ける「世代（ファームウェアバージョン）」に焦点をおき、該当の
ファームウェアバージョンに関する以下の情報を一覧表示します。

- ベンダー
- 世代（ファームウェアバージョン）
- 脆弱性の数
- 装置数

各ホスト名左の [▼] をクリックすると、各ファームウェアバージョンに該当するホス
ト情報とCVE ID情報のリストが、ベーススコアの高いIDから順に表示されます。

Network Configuration Manager						
ダッシュボード	インベントリ	コンフィグ自動化	ファームウェアの脆弱性	コンプライアンス	アラート	ツール
設定	レポート	サポート(中国)				
すべての脆弱性	露出装置	配布バージョン	脆弱性DBの同期	高度なCVE検索		
51 脆弱性総数	2 影響を受けた装置総数	0 エクスプロイト可能	51 検出した脆弱性 (最新7日間)			
エクスプロイトステータス: <input checked="" type="radio"/> すべて <input type="radio"/> エクスプロイト	装置グループ: All Devices Group	重要度: <input checked="" type="radio"/> すべて <input type="radio"/> critical <input type="radio"/> Important <input type="radio"/> Moderate <input type="radio"/> Low	更新をリクエスト			
ベンダー	世代	脆弱性の数	装置数			
▼ Cisco	15.2(4)E7	50	1			
ホスト名	CVE ID	ベーススコア	重要度	脆弱性タイプ	シリーズ	モデル
192.168	CVE-2007-5552	9.3	重大	利用できません	C2960X	WS-C2960X-24TS-LL
192.168	CVE-2017-4743	8.8	Important	利用できません	C2960X	WS-C2960X-24TS-LL
192.168	CVE-2019-16009	8.8	Important	利用できません	C2960X	WS-C2960X-24TS-LL
192.168	CVE-2020-3217	8.8	Important	利用できません	C2960X	WS-C2960X-24TS-LL
192.168	CVE-2017-3864	8.6	Important	利用できません	C2960X	WS-C2960X-24TS-LL
192.168	CVE-2020-3228	8.6	Important	利用できません	C2960X	WS-C2960X-24TS-LL
192.168	CVE-2015-0586	7.8	Important	利用できません	C2960X	WS-C2960X-24TS-LL
192.168	CVE-2015-0592	7.8	Important	利用できません	C2960X	WS-C2960X-24TS-LL
192.168	CVE-2020-3200	7.7	Important	利用できません	C2960X	WS-C2960X-24TS-LL
▶ Juniper	15.1X49-D50.3	1	1			

10.2 脆弱性DBの同期

Zoho Corporationが管理している脆弱性データベースと、脆弱性情報を同期する設定をします。

- ・同期は指定した時刻に日次で行われます。

デフォルト：午前2時

- ・脆弱性情報の自動同期を行うには、インターネット環境が必要です。

インターネット接続がないクローズドな環境の場合、[手動インポート]機能により、「vulnerability_dump_new.dat」ファイルをインポートすることで情報を更新することができます。インターネット接続可能な環境でファイルをダウンロードし、インポートを実施してください。

- ・同期機能を無効化する場合、[設定] → [一般] → [DB同期設定]の[データベースとのファームウェア脆弱性情報の同期を無効にする]にチェックを入れ、保存してください。



11 コンプライアンスチェック

管理対象装置に設定されているコンフィグが、組織や業界の標準に準拠または違反しているかどうか確認します。

11.1 ルールの作成

コンプライアンスチェックを実施するために、コンフィグに存在すべき行や存在すべきではない行を定義します。

※デフォルトで複数のルールが定義されています。

1. [コンプライアンス] → [ルール] 右上のプラスアイコンをクリック
2. 以下の中から条件レベルを選択し、条件とするコンフィグ内容を設定
 - ・ 簡易条件
 - ・ 高度な条件
 - ・ 高度なカスタム条件



3. 任意のルール名、説明を入力し、違反の重要度（重大、やや重大、警告）を指定の上、設定を保存



以下は、各条件タイプの説明です。

条件タイプ	説明
簡易条件	コンフィグに、指定した1行または複数行が含まれているか確認します。

	<p>例 :</p> <p>コンフィグに次の行がすべて含まれているかどうかを確認</p> <pre>snmp-server community public RO snmp-server community private RW</pre>
高度な条件	<p>正規表現を使用してより複雑な条件を指定することができます。</p> <p>例 :</p> <p>コンフィグにenable secret設定がされているかどうかを確認</p> <pre>enable secret 5 \$1\$3Jcu\$Sb3</pre>
高度なカスタム条件	<p>ブロック単位で開始行と終了行のコンフィグを定義し、その範囲内のコンフィグ行を対象に、コンプライアンスチェックを実施します。</p> <ul style="list-style-type: none"> ● シングルラインブロック : 単一行の開始ブロック、追加ブロック条件を指定しチェックを行います。 ● マルチラインブロック : ブロック開始行と終了行の条件を指定し、ブロック単位でチェックを行います。 <p>例 :</p> <p>descriptionがすべてのインターフェースブロックに記載されているか確認</p> <pre>interface FastEthernet0/0 description branch office 1 connectivity ip address 192.168.118.32 255.255.255.0 service-policy output Stream ! interface FastEthernet0/1 description branch office 2 connectivity ip address 192.168.118.32 255.255.255.0 service-policy output Stream !</pre> <p>ブロック開始 : interface ブロック終了 : !</p>

	追加ブロック条件：次の値を含まない_shutdown 条件：次の値を含む_description
--	---

11.2 ルールグループの作成

作成したルールをグループとして集約します。

1. [コンプライアンス] → [ルールグループ] 右上のプラスアイコンをクリック
2. 任意のルールグループ名、説明を入力し、グループに含めるルールを選択し、保存

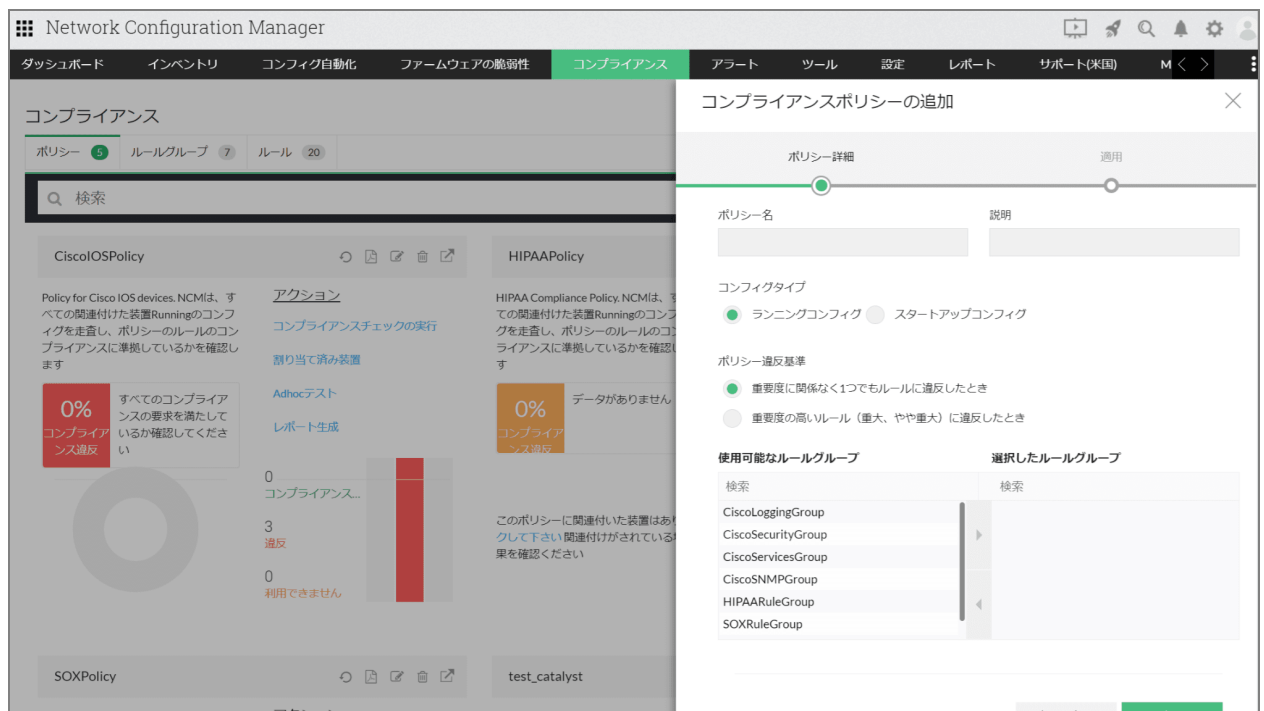


11.3 ポリシーの作成

作成したルールグループをもとに、コンプライアンスチェックを実施する対象装置を関連付けます。

1. [コンプライアンス] → [ポリシー] 右上のプラスアイコンをクリック
2. 任意のポリシー名、説明を入力し、コンプライアンスチェックを実行するコンフィグタイプ（Runningコンフィグ/Startupコンフィグ）を選択
3. ポリシー違反とする基準として、以下のいずれかを選択
 - ・ 重要度に関係なく1つでもルールに違反したとき
 - ・ 重要度の高いルール（重大、やや重大）に違反したとき

4. コンプライアンスチェックに使用するルールグループを選択して、[次へ]



5. 実行対象の装置または装置グループを指定し、保存

11.4 コンプライアンスチェックの実行

作成したコンプライアンスポリシーは、[コンプライアンス] → [ポリシー] 一覧に追加されます。

ウィジェットの[コンプライアンスチェックの実行]をクリックすると、関連付けられた装置に対してコンプライアンスチェックが実行されます。

実行結果に応じて、以下のステータスが表示されます。

- ポリシーに準拠している場合：緑のステータス
- ポリシーに違反している場合：赤のステータス

ウィジェット上のパーセンテージをクリックし、コンプライアンスポリシーに設定されているルールごとの準拠状況を確認します。



12 スケジュール設定

スケジュール設定により、コンフィグバックアップやコンフィグレットの実行など、NCMで行う各操作を定期的に行うよう自動化します。

12.1 スケジュールタイプ

スケジュールで設定できるスケジュールタイプは下記の通りです。

スケジュールタイプ	機能
コンフィグバックアップ	特定の装置または装置グループを対象に、コンフィグバックアップを実行します。
レポート生成	特定の装置または装置グループを対象に、ネットワークレポート、コンフィグレポート、Nipperレポート、脆弱性レポートなどを作成します。
コンプライアンスチェック	特定の装置または装置グループを対象に、コンプライアンスチェックを実行します。
コンフィグレット実行	特定の装置または装置グループを対象に、指定したコンフィグレットを実行します。
装置ディスカバリー	指定したIPアドレス範囲を対象に、ディスカバリーを実行します。

コンフィグ同期	特定の装置または装置グループを対象に、RunningコンフィグとStartupコンフィグを同期します。
PCIレビュー	特定の装置または装置グループを対象に、PCIレビューを実施します。

12.2 スケジュールの追加

以下の手順でスケジュールを設定します。

※例として、コンフィグバックアップのスケジュール設定を記載します。

1. [コンフィグ自動化] → [スケジュール] を表示し、右上の [＋] アイコンをクリック
2. 任意の [スケジュール名] を入力し、[スケジュールタイプ] のドロップダウンから [Configuration Backup] を選択
3. 対象の装置または装置グループを選択
4. スケジュールの実行間隔（毎時、日次、週次、月次、1回）を指定して保存

レポート通知について

- ・メール：指定したメールアドレスにスケジュールの実行結果が通知されます。
- ・レポートの保存：NCMインストールディレクトリ/schedule_results/配下に、各スケジュールタイプごとの実行結果が.htmlファイルで保存されます。

スケジュールの追加

スケジュール名

test

スケジュールタイプ

Configuration Backup

Device Group

Devices

装置グループ:

All Devices Group

レポート通知 ?



メール



レポートの保存

メールで通知する

メール件名

(カンマ(,)を使用して複数アドレスを指定します)

メモ: レポートには、個人情報が含まれることがあります。レポートは、設定した受信者に、スケジュール通り、送信されます。受信者を設定する際は、十分に、留意ください



バックアップが失敗した場合に通知



通知から設定の変更箇所を除外する



コンフィグの変更があった場合に通知する

毎時

日次

週次

月次

1回

週次実行

日曜

月曜

火曜

水曜

木曜

金曜

土曜

実行

12



時

00



分

13 ユーザー管理とロール権限

NCM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、有償のオプションです）。

13.1 ユーザー管理

[設定] → [ユーザー管理] → [ユーザー] で、ユーザーを作成します。
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
NCMであらゆる操作を実行する権限があります。装置の追加や削除、コンフィグ変更などの操作が可能です。
- オペレーター
NCMの操作に制限がある権限です。コンフィグ変更（コンフィグレット実行、アップロード）を行う際は、管理者のユーザーアカウントへ申請を行い、管理者が承認しない限り変更はできません。

操作権限の詳細は、以下のページをご参照ください。

https://www.manageengine.jp/products/Network_Configuration_Manager/help/rolebased-access-control-v12.html

以下の手順で新規ユーザーを作成します。

1. [設定] → [ユーザー管理] 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）
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]

Network Configuration Manager

ダッシュボード インベントリ コンフィグ自動化 ファームウェアの脆弱性 コンプライアンス アラート ツール 設定 レポート サポート

一般設定 装置管理 ディスカバリ ユーザー管理 認証 タグ 一般 連携 PCI

ユーザー情報を編集

1 ユーザー設定 2 詳細

ユーザーロール、認証情報、連絡先詳細を入力してください ユーザーにアクセスを許可する装置を設定します

アップロード

ロール --ロールを選択-- ユーザータイプ ローカル認証

ユーザー名 * ZOH0 Email ID *

パスワード * パスワードポリシーの設定 パスワードの再入力 *

Phone Number Mobile Number タイムゾーン (NFAレポート用) Asia/Tokyo

キャンセル 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]

Network Configuration Manager

ダッシュボード インベントリ コンフィグ自動化 ファームウェアの脆弱性 コンプライアンス アラート ツール 設定 レポート サポート

一般設定 装置管理 ディスカバリ ユーザー管理 認証 タグ 一般 連携 PCI

ユーザー情報を編集

1 ユーザー設定 2 詳細

ユーザーロール、認証情報、連絡先詳細を入力してください ユーザーにアクセスを許可する装置を設定します

コンフィグ管理

すべての装置 全ての装置へのアクセスを許可

特定の装置を選択

装置グループの選択

Select Tag

コンフィグレットグループ 全てのコンフィグレットグループにアクセスできます

戻る キャンセル 保存

- ・ ローカル認証

NCM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。

- ・ RADIUS認証

RADIUS認証を使用して、NCM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/Network_Configuration_Manager/help/radius-server-settings-v12.html

- ・ AD認証

AD認証を使用して、NCM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/Network_Configuration_Manager/help/adding-domain-v12.html

13.2 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（読み取り/書き込み、読み取り、アクセス許可なし）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] → [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ならびにその説明を記入
3. [共通設定]、[ネットワークコンフィグ管理] の項目から、権限に付与する内容を選択し、[保存] をクリック

※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] の一覧に追加されます。

Network Configuration Manager

ダッシュボード インベントリ コンフィグ自動化 ファームウェアの脆弱性 コンプライアンス アラート ツール 設定 レポート サポート(米国)

一般設定 ユーザー管理 タグ 一般 連携 PCI

Add Role

名前
レポート参照

説明
レポート参照権限のみ

キャンセル 保存

共通設定

Modules	Read/Write	Read	No Access
全般設定	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
アラート	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ダッシュボード	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
レポート	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
ツールセット	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

ネットワークコンフィグ管理

Modules	Read/Write	Read	No Access
装置管理	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
コンフィグ自動化	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

ロール画面で選択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/Network_Configuration_Manager/help/role_feature.html#Operation_list

追加したロール権限は、[設定] → [ユーザー管理] → [ユーザー] で新規にユーザーを作成する際に、[ロール]に表示されるようになります。

Network Configuration Manager

ダッシュボード

インベントリ

コンフィグ自動化

ファームウェアの脆弱性

コンプライアンス

アラート

ツール

設定

レポート

サポート

一般設定

装置管理

ディスカバリ

ユーザー管理

認証

タグ

一般

連携

PCI

ユーザー情報を編集

1

2

ユーザー設定

詳細

ユーザーロール、認証情報、連絡先詳細を入力してください

ユーザーにアクセスを許可する装置を設定します

アップロード

ロール

ユーザータイプ

--ロールを選択--

--ロールを選択--

管理者

オペレーター

レポート権限

ローカル認証

Email ID *

パスワードの再入力 *

Phone Number

Mobile Number

タイムゾーン (NFAレポート用)

Asia/Tokyo

キャンセル

次へ

13.3 パスワードポリシー

NCM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や動作を設定します。

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。

Network Configuration Manager

ダッシュボード
インベントリ
コンフィグ自動化
ファームウェアの脆弱性
コンプライアンス
アラート
ツール
設定
レポート
サポート(米国)

一般設定
装置管理
ディスクバリ
ユーザー管理
認証
タグ
一般
連携
PCI

ユーザー管理

ユーザー
ロール
パスワードポリシー

メモ：
この設定は「ローカル認証」のユーザーにのみ適用されます [詳細はこちらを参照ください](#)

最短パスワード長
5

パスワードの履歴を記録する
3
パスワード

パスワードとユーザー名は同一にはできません
有効

パスワードを忘れた場合
有効

ユーザーアカウントのロックアウトポリシー
有効

ログイン失敗の最大試行回数
5

ロックアウト期間
2
分

キャンセル
保存

各パラメーターについて、以下の表に記載します。

パラメーター	説明
最短パスワード長	パスワードの最短長を指定します。 最短5文字、最長100文字まで指定できます。
パスワードの履歴を記録する	過去に設定したパスワードの重複を防ぐことを目的に、指定した履歴数に応じて、過去に使用したパスワードを再設定できないようにします。
パスワードとユーザー名は同一にはできません	有効化すると、パスワードとユーザー名に同一の値を設定できなくなります。
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］の表示を有効化/無効化します。
ユーザーアカウントのロックアウトポリシー	有効化すると、以下の「ログイン失敗の最大試行回数」ならびに「ロックアウト期間」を設定できるようになります。
ログイン失敗の最大試行回数	ログインの失敗を許容する回数を指定します。
ロックアウト期間（分）	ログイン失敗の最大試行回数に達した場合のロックアウト時間（分）を指定します。

14 各メニュータブの説明

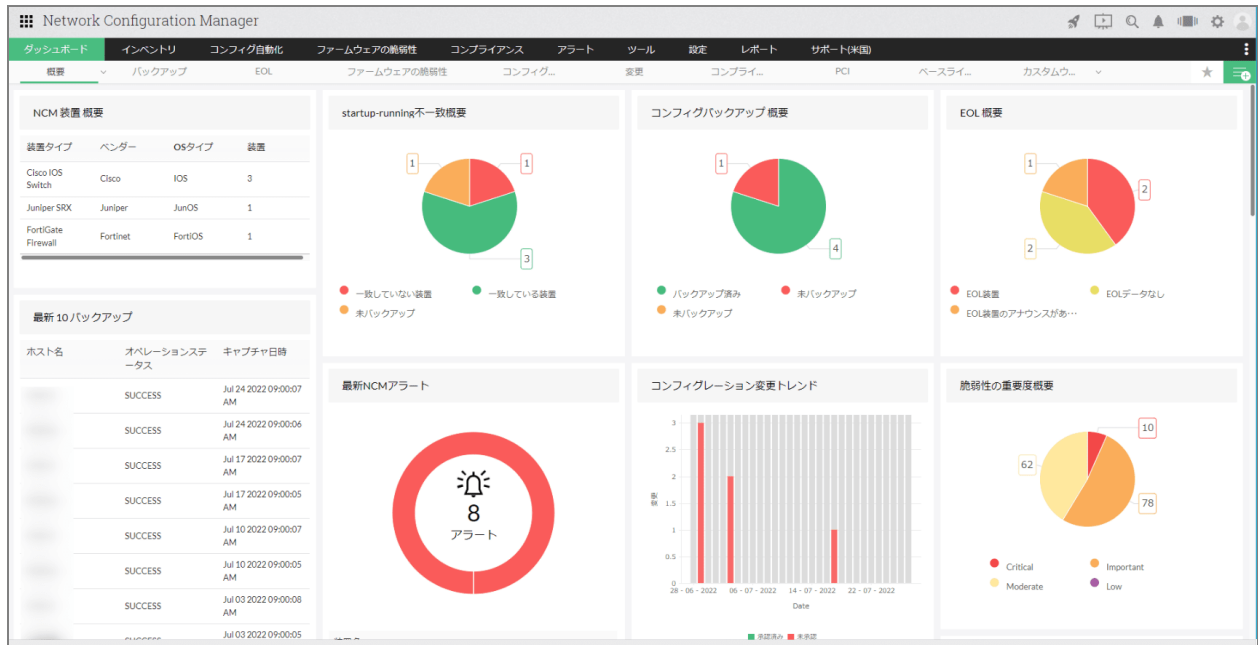
NCMにログイン後の画面上部に、各メニュータブが存在します。
各メニュータブで表示される情報や操作可能な機能について記載します。

14.1 ダッシュボード

NCM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、管理対象装置やコンフィグ管理の状況を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。

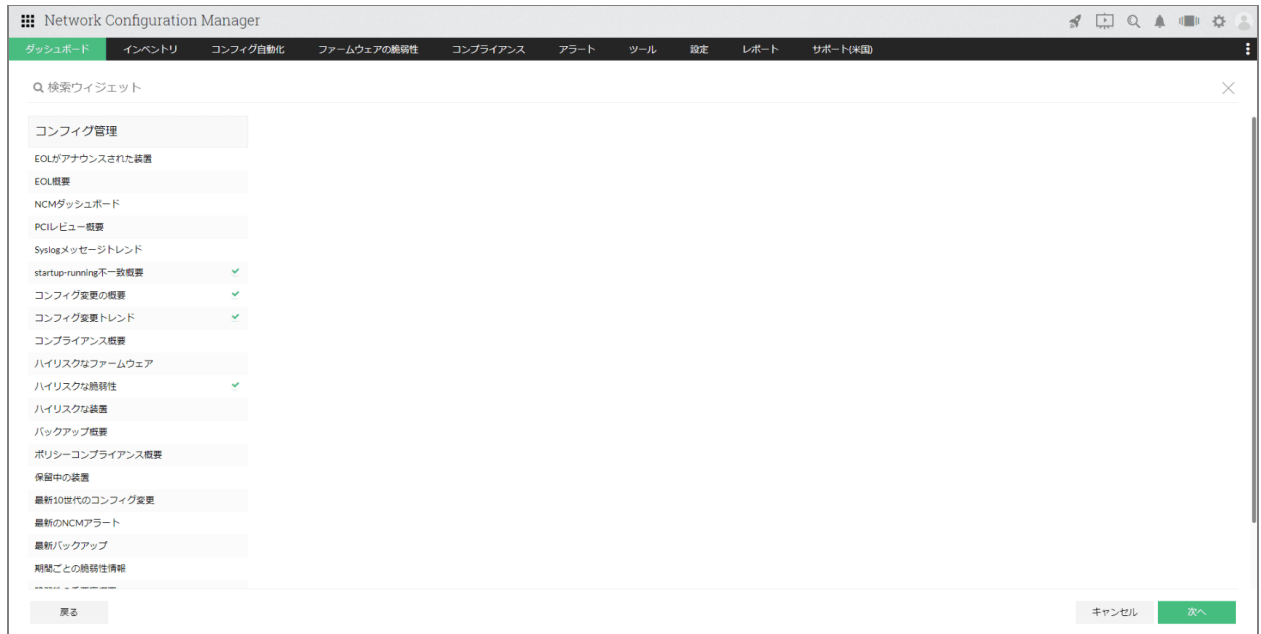
タブ名	機能
概要	管理装置の概要やコンフィグバックアップ、変更履歴など、全体の状況を表示します。
バックアップ	コンフィグバックアップの履歴やスケジュール状況など、コンフィグバックアップ状況に関する情報を表示します。
EOL	EOLを迎えている装置やEOLのアナウンスがあった装置など、EOLに関する情報を表示します。
ファームウェアの脆弱性	管理対象装置のファームウェアに潜む脆弱性情報（CVE IDや重要度など）を表示します。
コンフィグ不一致	StartupコンフィグとRunningコンフィグの同期状況を表示します。
変更	コンフィグの変更日時や対象装置の情報など、コンフィグの変更状況を表示します。
コンプライアンス	コンプライアンス機能の実行結果（準拠、違反）の状況を表示します。
PCI	PCIレビューの依頼状況（依頼日時、レビュー者、レビューステータス）を表示します。
ベースライン対ランニングコンフリクト	管理対象装置のベースラインコンフィグとRunningコンフィグの不一致状況を表示します。



14.1.1 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。

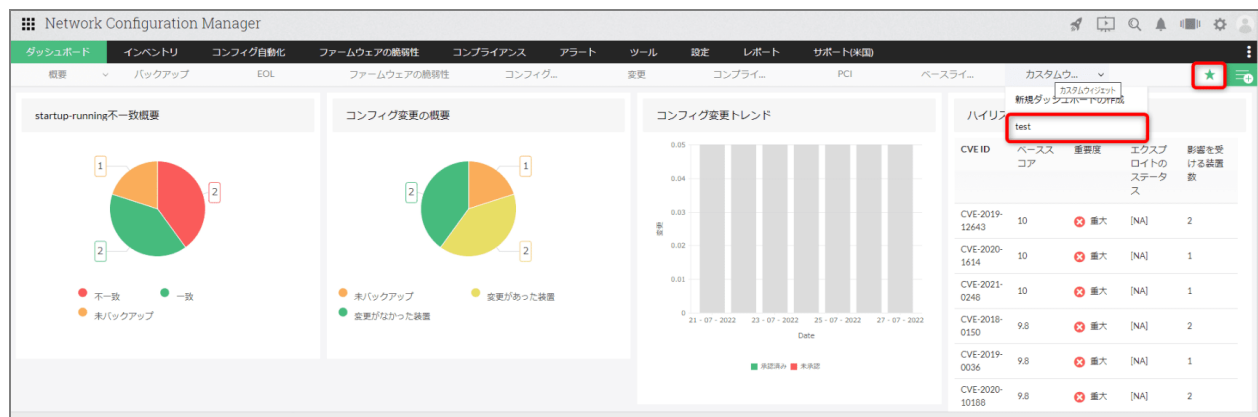
1. ダッシュボード画面右上の「+」をクリック
2. 「ダッシュボードを追加」をクリック
3. 任意のダッシュボード名、説明を入力し、「次へ」をクリック
※ダッシュボード名に、特殊文字や空白は使用できません。
4. ダッシュボードに追加するウィジェットを選択し、「次へ」をクリック



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選択し、[作成] をクリック

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。

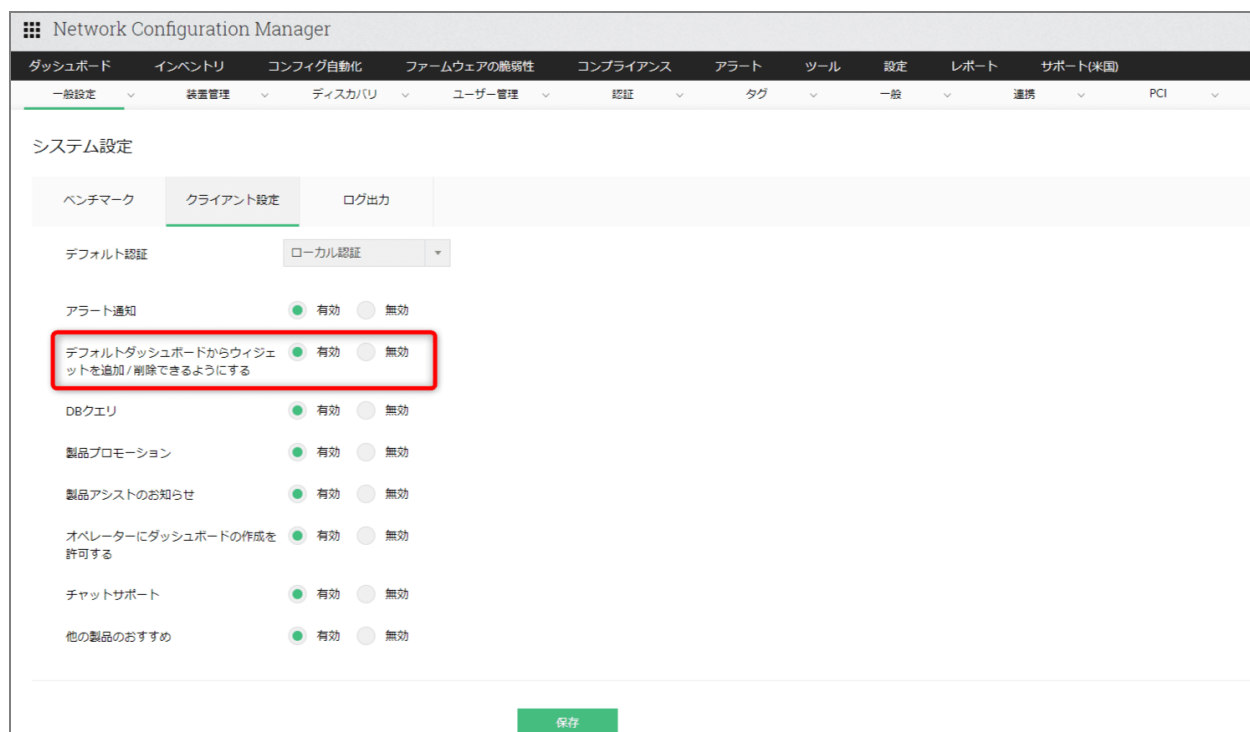
また、ダッシュボードを表示し、画面右上の[★]をクリックすると、デフォルトダッシュボードとして設定することができます。



14.1.2 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
に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] 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

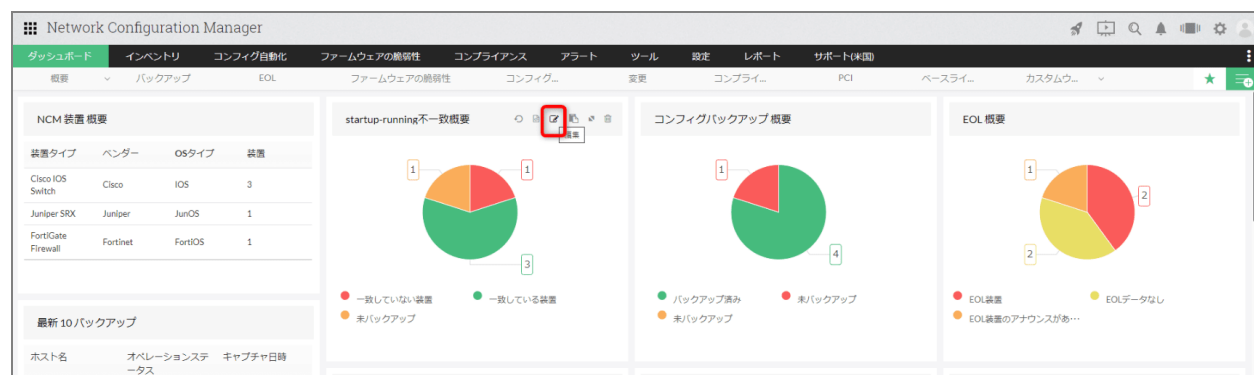
集] アイコンから編集を行います。

※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、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。



14.2 インベントリ

NCMに追加した装置の確認や装置グループの作成、コンフィグ参照など、各管理対象装置についてより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	NCMに追加した装置の一覧を表示します。 ホスト名、装置テンプレート名、シリーズ、モデル、最新操作ステータス、コンフィグ不一致、コンプライアンスステータスなど、各情報を表示します。

	<p>ホスト名をクリックすると、対象装置のスナップショット画面が表示されます。詳細は「14.2.1 スナップショット画面」を参照ください。</p>
グループ	<p>NCMに追加した装置をグループ化します。</p> <p>デフォルトで、すべての装置グループ、バックアップ失敗グループ、Ciscoルーターグループ、Ciscoスイッチグループが実装されています。</p> <p>詳しくは、「5.4.4 装置グループ」を参照ください。</p>
コンフィグ	<p>コンフィグバックアップで取得したコンフィグ情報を一覧で表示します。</p> <p>ホスト名、IPアドレス、世代数、取得日時、変更者、コンフィグタイプ（Startup/Running）、変更タイプ（未承認、承認済み）などの情報を表示します。</p> <p>ホスト名をクリックすると、対象装置の各コンフィグ世代を表示し、更にその世代をクリックすることで、コンフィグ内容を参照することができます。</p>
変更	<p>各装置のコンフィグ変更情報を一覧で表示します。</p> <p>取得日時、ホスト名、IPアドレス、世代数、変更者、コンフィグタイプ（Startup/Running）、変更タイプ（未承認、承認済み）などの情報を表示します。</p> <p>画面左上の時計アイコンより、表示する期間を指定します。</p>
下書き	<p>コンフィグ変更（アップロード）用に作成した下書きの一覧が表示されます。</p> <p>ホスト名、下書き名、作成者、最新修正日、ベース世代、コンフィグタイプなどの情報を表示します。</p> <p>下書きを一から作成した場合、ベース世代とコンフィグタイプのステータスは「利用できません」となります。</p> <p>下書きについては、「9.3 コンフィグアップロード」を参照してください。</p>

装置、コンフィグ、変更、下書きタブでは、画面下部の「表示カラム選択」より表示するカラムを選択できます。

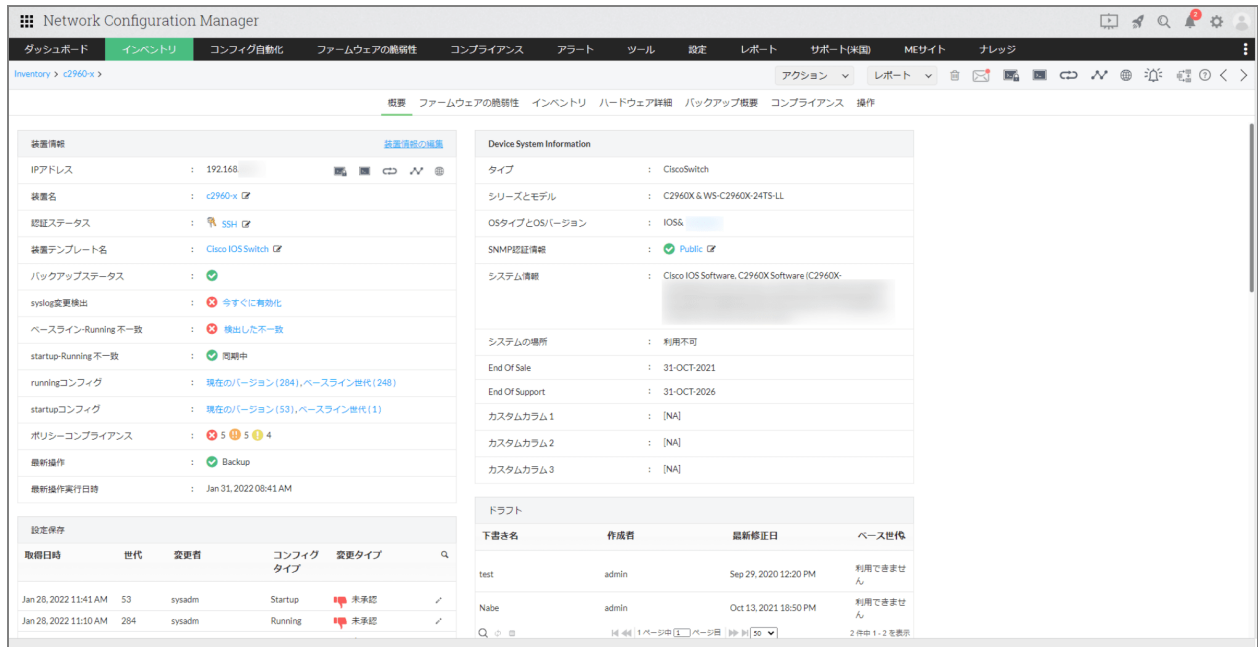
14.2.1 スナップショット画面

［インベントリ］ → ［装置］ 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	対象装置やコンフィグの不一致、操作情報などを表示します。 ［設定保存］ウィジェットより、取得したコンフィグ世代の参照や差分比較を行うことができます。
ファームウェアの脆弱性	対象装置のファームウェアに潜む脆弱性情報（CVE ID、脆弱性タイプ、ベーススコア、重要度）を一覧で表示します。 CVE IDをクリックし、参考URLなどより詳細な情報を表示します。
インベントリ	対象装置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、アップ/ダウン、受信/送信速度）や設定されているVLAN情報を一覧で表示します。
ハードウェア詳細	対象装置のハードウェア情報（RAMサイズ、MACアドレス、OSイメージファイル名、シリアル番号など）を表示します。
バックアップ概要	Startup/Runningコンフィグやベースラインコンフィグの不一致状況、直近1週間のバックアップ実行状況、コンフィグ変更状況を表示します。
コンプライアンス	対象装置に該当するコンプライアンスポリシーの準拠/違反状況（ホスト名、ポリシー名、重大レベル、最終チェック日）を表示します。 ポリシー名をクリックし、各ルールごとに状況を確認することができます。
操作	最新のバックアップ履歴（ホスト名、実行ステータス、実行日時、本文、実行者）と操作履歴（ホスト名、実行操作名、実行者、実行完了日時、ステータス）を一覧で表示します。

スナップショット画面上部の［アクション］から、認証情報の編集やコンフィグバックアップ、コンフィグレットの実行、レポート生成など各アクションを実行することができます。



14.3 コンフィグ自動化

コンフィグ管理を自動化する各種設定を行います。

タブ名	説明
装置テンプレート	バックアップ/アップロードコマンドやコンフィグ同期コマンドなど、コンフィグ管理を行う上で必要なコマンドセットが実装されているテンプレートを管理します。 NCMを装置に追加する際に、装置テンプレートが適用されます。
コンフィグレット	複数の装置に共通のコマンドを投入する場合や、特定の時間帯にコンフィグ変更を行う場合に、コマンドセットを事前に作成しておき、任意の装置に任意の時間にコマンドを投入します。 詳細は、「9.1 コンフィグレットの実行」を参照してください。
スケジュール	コンフィグバックアップやコンフィグレットの実行、コンフィグ同期などの操作を、特定の周期で実行するようスケジュール化します。 詳細は、「12 スケジュール設定」を参照してください。
変更通知	特定の装置や装置グループを対象に、コンフィグ変更を検知した際のアクション（メール通知、SNMPトラップ、syslog転送など）を設定します。 詳細は、「8.2 変更通知設定」を参照してください。

アップロードリクエスト	オペレーター権限、一部のロール権限のユーザーがコンフィグ変更（コンフィグレットの実行やコンフィグアップロード）を管理者権限のユーザーに依頼した際の、各ステータスを確認します（保留中、承認済み、拒否）。
認証設定	認証プロファイルや認証ルールを設定します。 認証ルールでは、装置追加時に、条件に一致した装置に対して認証プロファイルを自動適用するよう設定することができます。 詳細は、「5.5 認証情報の登録」を参照してください。
除外条件	コンフィグの差分対象から除外するコンフィグ行やコンフィグブロックを設定します。 詳細は、「7.4 除外条件の設定」を参照してください。

14.4 ファームウェアの脆弱性

取得した各装置のファームウェアに潜む脆弱性情報を一覧で表示します。

装置やバージョンを基準に、該当する脆弱性情報とそのベーススコア（重大度）、参考URLを一覧で表示します。

詳しくは、「10 ファームウェアの脆弱性の確認」の章をご参照ください。

14.5 コンプライアンス

管理対象装置に設定されているコンフィグが、組織や業界の標準に準拠または違反しているか、コンプライアンスチェック機能を使用して確認します。

任意のルールとポリシーを作成し、準拠状況を確認することができます。

詳しくは、「11 コンプライアンスチェック」の章をご参照ください。

14.6 アラート

コンフィグ変更の発生やコンフィグバックアップ失敗などのイベントを、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。



14.7 ツール

ターミナル機能や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。



14.8 設定

メールサーバー設定や装置ディスカバリー、ユーザー管理など、NCMを運用する上で必要な各種設定を行います。



14.9 レポート

管理対象装置のハードウェアやファームウェア情報、コンフィグ変更や Startup/Running コンフィグの同期状況、脆弱性やEOLなどの各種情報をレポートとして参照します。

各レポートは、PDF、CSV形式、メール送付（PDF）により出力することができます。
※一部のレポートタイプでは、XLSX形式に対応しています。



14.10 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。



15 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ならびに、NCM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。

15.1 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>

保守ユーザー様は、下記のお客様専用サイト「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>

15.2 関連資料

オンラインユーザーマニュアル

https://www.manageengine.jp/products/Network_Configuration_Manager/help/

ナレッジベース

https://www.manageengine.jp/support/kb/Network_Configuration_Manager/

リリース関連情報

https://www.manageengine.jp/products/Network_Configuration_Manager/help/release_info.html

簡易版スタートアップガイド

https://www.manageengine.jp/products/Network_Configuration_Manager/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>

・ Network Configuration Manager製品ページ

https://www.manageengine.jp/products/Network_Configuration_Manager/