

CA Spectrum®

Network Configuration Manager ユーザ ガイ
ド
リリース 9.3



このドキュメント（組み込みヘルプシステムおよび電子的に配布される資料を含む、以下「本ドキュメント」）は、お客様への情報提供のみを目的としたもので、日本CA株式会社（以下「CA」）により隨時、変更または撤回されることがあります。

CAの事前の書面による承諾を受けずに本ドキュメントの全部または一部を複写、譲渡、開示、変更、複本することはできません。本ドキュメントは、CAが知的財産権を有する機密情報です。ユーザは本ドキュメントを開示したり、(i) 本ドキュメントが関係するCAソフトウェアの使用についてCAとユーザとの間で別途締結される契約または(ii) CAとユーザとの間で別途締結される機密保持契約により許可された目的以外に、本ドキュメントを使用することはできません。

上記にかかわらず、本ドキュメントで言及されているCAソフトウェア製品のライセンスを受けたユーザは、社内でユーザおよび従業員が使用する場合に限り、当該ソフトウェアに関連する本ドキュメントのコピーを妥当な部数だけ作成できます。ただしCAのすべての著作権表示およびその説明を当該複製に添付することを条件とします。

本ドキュメントを印刷するまたはコピーを作成する上記の権利は、当該ソフトウェアのライセンスが完全に有効となっている期間内に限定されます。いかなる理由であれ、上記のライセンスが終了した場合には、お客様は本ドキュメントの全部または一部と、それらを複製したコピーのすべてを破棄したことを、CAに文書で証明する責任を負います。

準拠法により認められる限り、CAは本ドキュメントを現状有姿のまま提供し、商品性、特定の使用目的に対する適合性、他者の権利に対して侵害のないことについて、黙示の保証も含めいかなる保証もしません。また、本ドキュメントの使用に起因して、逸失利益、投資損失、業務の中断、営業権の喪失、情報の喪失等、いかなる損害（直接損害か間接損害かを問いません）が発生しても、CAはお客様または第三者に対し責任を負いません。CAがかかる損害の発生の可能性について事前に明示に通告されていた場合も同様とします。

本ドキュメントで参照されているすべてのソフトウェア製品の使用には、該当するライセンス契約が適用され、当該ライセンス契約はこの通知の条件によっていかなる変更も行われません。

本ドキュメントの制作者はCAです。

「制限された権利」のもとでの提供：アメリカ合衆国政府が使用、複製、開示する場合は、FAR Sections 12.212、52.227-14 及び 52.227-19(c)(1)及び(2)、ならびに DFARS Section 252.227-7014(b)(3) または、これらの後継の条項に規定される該当する制限に従うものとします。

Copyright © 2013 CA. All rights reserved. 本書に記載された全ての製品名、サービス名、商号およびロゴは各社のそれぞれの商標またはサービスマークです。

CA Technologies 製品リファレンス

このガイドは、以下の製品に関するものです。

- CA Spectrum® (CA Spectrum)
- CA Spectrum® NCM (Network Configuration Manager)
- CA Spectrum® Report Manager (Report Manager)
- CA Service Desk

CAへの連絡先

テクニカルサポートの詳細については、弊社テクニカルサポートの Web サイト (<http://www.ca.com/jp/support/>) をご覧ください。

目次

第 1 章: はじめに	11
Network Configuration Manager の機能	11
Network Configuration Manager へのアクセス	13
重要な用語.....	14
設定のタイプ.....	16
ランニング コンフィギュレーション	16
スタートアップ コンフィギュレーション	16
設定ファイル.....	16
サポートされているデバイス	17
デバイス認定データベースへのアクセス	17
デバイス ファミリ	20
Network Configuration Manager によるデバイス ファミリの特定方法.....	20
Cisco IOS デバイス	20
Cisco NX OS デバイス	21
Juniper JUNOS デバイス	22
拡張ユーティリティ	23
Network Configuration Manager の前提条件	24
通信モード	24
SSH v2 のサポート	25
Cisco デバイス および SCP	25
デバイス設定変更の未承諾通知	25
デバイストラップ	26
デバイスマIB オブジェクト	27
グローバルコレクション	27
保守モード	28
Network Configuration Manager レポート パック	28
第 2 章: Network Configuration Manager の設定	29
Network Configuration Manager の設定	29
一般設定の実行.....	29
設定履歴設定の選択.....	30
設定変更アラート設定の選択.....	32
承認ワークフロー.....	33
TFTP サーバの設定	36

FTP サーバの設定	41
リモート TFTP または FTP サーバを使用する場合の考慮事項	43
単一デバイスの TFTP または FTP サーバの指定	44
デバイス設定エクスポートの設定を選択	45
デバイスファミリの設定	47
デバイスファミリ一般設定の設定	47
デバイスファミリ通信モードの設定	48
デバイスファミリ マスクの設定	49
通知トラップ設定の設定	51
单一のデバイスの設定によるデバイスファミリ設定の上書き	54
单一のデバイス上の Network Configuration Manager へのアクセス	54
单一のデバイスにおける Network Configuration Manager の有効化または無効化	54
单一のデバイスでの未承諾デバイス設定キャプチャの設定	55
单一デバイスの設定変更アラート設定の指定	56
单一のデバイス上での通信モード設定	57
单一のデバイス上でのマスク設定	59
Network Configuration Manager 拡張ユーティリティ	60
サポートされている操作	61
カスタムデバイスファミリの作成	62
デバイスファミリへのデバイスの配置	64
拡張ユーティリティのスクリプト設定	65
Perl モジュール	72
スクリプトのインポートおよびエクスポート	78
スクリプトのバックアップおよび履歴の管理	81
カスタマイズされたトラップ	81
第 3 章: グローバル同期タスク	83
グローバル同期について	83
Enterasys/Riverstone SSR デバイスについて	84
グローバル同期の設定	84
グローバル同期のスケジュール	85
オンデマンド グローバル同期タスクの実行	87
单一デバイスの設定履歴の表示	87
2つの設定の比較	90
参照設定の指定	91
設定アラーム	92
参照とランニング コンフィギュレーションの差異の表示	93
スタートアップとランニング コンフィギュレーションの表示	93
グローバル同期タスク結果の表示	94

Report Manager からの Network Configuration Manager レポート	94
Report Manager オプション	95
Report Manager でネットワーク設定管理レポートの生成.....	96
第 4 章: Network Configuration Manager のデバイスレベルのタスク	99
設定の手動によるキャプチャ	99
単一デバイスへの設定の手動アップロード	100
承認が不要.....	100
単一デバイスに設定をアップロード (承認が必要)	103
第 5 章: Network Configuration Manager バルク タスク	105
アップロード タスクの作成.....	105
Enterasys/Riverstone SSR デバイスによるアップロード タスクへの応答の決定	108
同期 タスクの作成.....	109
スタートアップへの保存 タスクを作成	111
第 6 章: ファームウェア アップロード	113
ファームウェア アップロードについて	113
権限.....	114
デバイス ファームウェアの転送設定の設定	115
Cisco フラッシュ パーティション 情報の表示	116
ファームウェア ロード タスクの作成	117
再ロード タスクの作成	121
再ロード キャンセル タスクの作成	124
デバイス ファームウェアのロード スクリプト	125
第 7 章: タスクの管理	127
グローバル コレクションとタスクの関連付け	127
新しいタスクの関連付け.....	127
既存タスクの関連付け	128
バルク タスクのスケジュール	130
再利用可能なタスク	131
タスクのスケジュール	131
タスクの開始と停止	134
タスクの開始.....	135
タスクの停止.....	136
タスクの再開.....	136

タスクを削除.....	137
タスク情報の表示.....	137
リアルタイムでタスク結果を表示.....	137
すべてのバルク タスクの重大な統計の表示.....	138
バルク タスクの詳細な統計の表示.....	138
タスクの状態とステータス値.....	139
タスクの状態.....	139
タスク ステータス.....	140
第 8 章: Network Configuration Manager のポリシー	141
Network Configuration Manager のポリシーについて.....	141
單一行ポリシー.....	142
複数行ブロック ポリシー.....	143
ポリシーの作成.....	144
ポリシー条件.....	147
修正アクションのために推奨されるアップロード	155
違反を表示.....	158
非準拠デバイスの修復.....	167
ポリシー テーブルからの非準拠デバイス修復	167
ポリシー違反アラームからの非準拠デバイスの修復	168
ポリシーの管理.....	169
ポリシーの編集.....	169
ポリシーの有効化および無効化.....	170
グローバル コレクションにポリシーを適用	170
ポリシーの削除.....	171
ポリシー情報の表示.....	172
ポリシーの詳細の表示.....	172
すべてのポリシーの重大な統計の表示.....	172
単一のデバイスに適用されるすべてのポリシーの重大な統計の表示	173
グローバル コレクションに適用されるポリシーの重大な統計の表示	173
複数行ブロック ポリシーの例.....	174
シナリオ.....	174
はじめに.....	175
ポリシーの定義.....	177
ポリシーの保存およびテスト	183
違反の監視.....	189

付録 A: サポートされているデバイス

191

Cisco 対応デバイス.....	191
Cisco 対応デバイス.....	215
Cisco 対応デバイス.....	222
Cisco CAT 対応デバイス	224
Cisco NX OS をサポートしているデバイス	226
Enterasys 対応デバイス	227
Enterasys/Riverstone SSR 対応デバイス	230
Extreme 対応デバイス	232
Foundry 対応デバイス.....	237
Juniper 対応デバイス	248
Lancom がサポートされているデバイス.....	250
Nortel Baystack のサポートされているデバイス	250
Nortel Passport 対応デバイス	251

付録 B: Network Configuration Manager イベント

253

Network Configuration Manager イベントについて.....	253
デバイス上で生成されたイベント	253
設定変更.....	253
設定変更イベントの相関.....	254
スタートアップコンフィギュレーションとランニングコンフィギュレーションの比較	255
参照設定とランニングコンフィグレーションの比較	255
ポリシーに準拠/非準拠のデバイス	256
ポリシー アラーム生成イベントに非準拠のデバイス	256
キャプチャ成功/失敗	257
アップロード成功/失敗	257
アップロード失敗アラーム生成イベント	258
スタートアップへの書き込み成功/失敗	258
デバイス上の NCM 有効化/無効化	258
NCM 無効化、操作の不実行	259
デバイス ファームウェアのロード	259
デバイス ファミリでのデバイスの追加/削除	259
ポリシーで生成されたイベント	260
ポリシー有効/無効	260
変更済みポリシー	260
ポリシーの違反者	260
違反ポリシー、アラーム生成イベント	260

グローバル同期、キャプチャ、アップロードおよびスタートアップへの書き込みタスクで生成されたイベント	261
スケジュール済み/スケジュールされていないタスク	261
起動、停止、完了、一部完了したタスク	261
タスクが一部完了したアラーム生成イベント	262
設定マネージャアプリケーションで生成されたイベント	262
グローバル未承諾通知	262
デバイスファミリ上で生成されたイベント	263
付録 C: Network Configuration Manager 権限	265

第1章：はじめに

この章では、Network Configuration Manager（NCM）についての概要を説明します。

このセクションには、以下のトピックが含まれています。

[Network Configuration Manager の機能 \(P. 11\)](#)

[Network Configuration Manager へのアクセス \(P. 13\)](#)

[重要な用語 \(P. 14\)](#)

[設定のタイプ \(P. 16\)](#)

[サポートされているデバイス \(P. 17\)](#)

[デバイス認定データベースへのアクセス \(P. 17\)](#)

[デバイスファミリ \(P. 20\)](#)

[拡張ユーティリティ \(P. 23\)](#)

[Network Configuration Manager の前提条件 \(P. 24\)](#)

[通信モード \(P. 24\)](#)

[デバイス設定変更の未承諾通知 \(P. 25\)](#)

[グローバルコレクション \(P. 27\)](#)

[保守モード \(P. 28\)](#)

[Network Configuration Manager レポートパック \(P. 28\)](#)

Network Configuration Manager の機能

設定管理は、ネットワークを構成する単一のデバイスやデバイス ファミリの設定を識別および監視するプロセスです。デバイスにはルータ、ハブ、およびスイッチが含まれます。

CA Spectrum Network Configuration Manager を使用すると、以下の利点があります。

- ネットワーク問題の解決にかかる時間を減らすことにより、ネットワークの稼働時間を増加させる。
- 反発するトラブルシューティングおよび修正が必要なネットワーク問題の発生を減らすことにより、ネットワーク サポートコストを削減する。
- システム全体にわたる変更の管理時間を減らすことにより、ネットワーク運用コストを削減する。

ネットワーク上の各デバイスは、特定のサービスを提供するよう設定されます。デバイスの操作方法およびカスタマイズされた方法についての詳細は、その設定に含まれています。

Network Configuration Manager では、以下のタスクを実行できます。

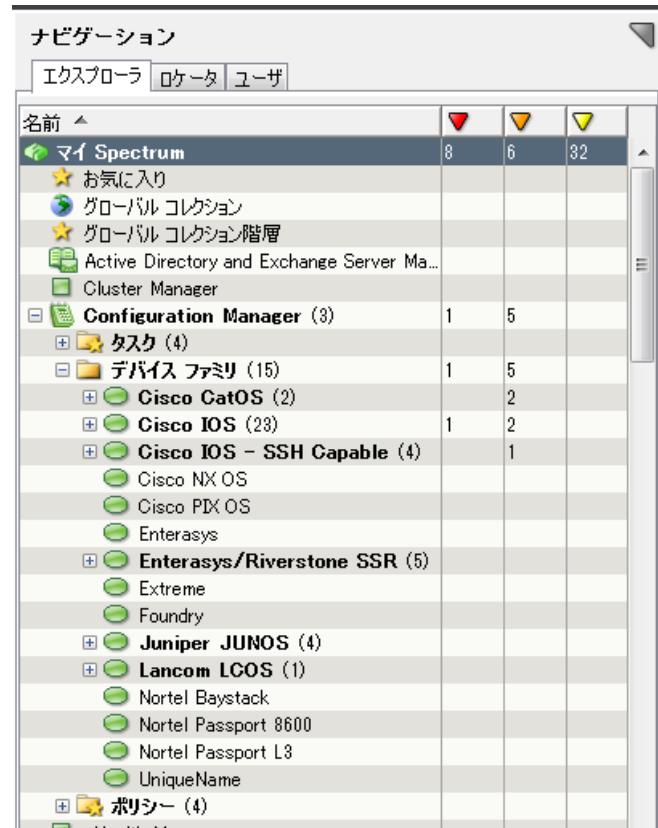
- CA Spectrum または OneClick でモデリングされたサポート対象デバイスの設定を管理。
- ネットワーク デバイス設定をキャプチャし、CA Spectrum データベースに保管。
- ランニングとスタートアップのコンフィギュレーションの比較。
- Perl 設定スクリプトのアップロード。
- フームウェアのロード。
- 設定のエクスポート。
- 同じファミリ タイプで 1 つ以上のデバイスの設定をロードおよびマージ。

注: コンテンツのマージでは、既存ファイルに情報が追加されます（上書きまたはリストアは行われません）。

- デバイス上で正しい設定が実行されていることを確認。
- デバイス設定の信頼性を確実にするために、自動キャプチャおよびポリシーのスケジュールを設定。
- デバイス設定の確認により、パフォーマンスの問題を検出。
- 比較およびトラブルシューティング用のネットワーク デバイス設定の履歴管理。
- 設定のコンテンツを監視し、デバイスのコンテンツが準拠していることを確認するためのポリシー作成。

Network Configuration Manager へのアクセス

OneClick コンソールから Network Configuration Manager にアクセスするには、[エクスプローラ] タブから設定マネージャを選択します。



[設定マネージャ] ノードを展開すると、デバイス ファミリ ビュー、ポリシー ビュー、およびタスク ビューが表示されます。

注: OneClick の詳細については、「オペレータ ガイド」を参照してください。

重要な用語

以下の用語は、Network Configuration Manager を理解するために重要です。

承認ワークフロー

実装される前に承認を受信するには、Network Configuration Manager によって開始される設定変更を必要とします。承認ワークフローは、承認プロセスで CA Service Desk チケットまたは CA Spectrum 許可権限を使用するようセットアップできます。

バルクタスク

バルクタスクは複数のデバイスで実行できるタスクです。次のバルクタスク、アップロード、同期、スタートアップへの保存、ファームウェアロードタスク、再ロード、および再ロードキャンセルが使用可能です。

デバイスマリ

デバイス設定にアクセスする共通のメソッドを共有するデバイスのグループです。 Network Configuration Manager が標準でサポートするデバイスは、自動的にデバイスマリに配置されます。拡張ユーティリティを使用し、さらにデバイスマリを作成できます。

グローバル同期タスク

スケジュールを使用して Network Configuration Manager が有効化されているネットワーク上のすべてのデバイスのランニングコンフィギュレーションを収集します。ネットワーク全体にわたってサポートされているすべてのデバイスから、設定をキャプチャする期間および繰り返し頻度を選択します。ネットワーク上のすべてのデバイスの設定をキャプチャすることによって、ランニングコンフィギュレーションの履歴を管理できます。

ファームウェアロードタスク

ファームウェアを Cisco IOS および Cisco IOS - SSH Capable デバイスにアップロードします。

Network Configuration Manager のポリシー

設定内のコンテンツを監視し、デバイスのコンテンツが準拠しているかを検証します。ポリシーは、デバイスのホスト設定で特定の側面を指定します。ホスト設定ファイルがデバイス用にキャプチャされるたびに、ポリシーが確認および比較されます。ポリシーに違反するデバイスではアラームが生成され、半自動的に修復することができます。デバイスで設定変更がある場合、ポリシーが準拠しているかが確認されます。

参照設定

参照用の基準として役立つデバイス設定です。他の設定を参照設定と比較できます。現在の設定が参照と異なる場合、デバイスでアラームを生成できます。

再ロードタスク

ファームウェアがアップロードされた後、デバイスを再ロードします。このタスクは Cisco IOS および Cisco IOS - SSH Capable デバイスに使用できます。

再利用可能タスク

実行された後に保持されるタスクは、再定義せずに再度複数回実行できます。また、反復するスケジュールを作成し、事前に決められた時間で再利用可能なタスクを実行することもできます。

スタートアップへの保存タスク

現在のランニングコンフィギュレーションを、1つまたは複数の選択されたデバイスのスタートアップコンフィギュレーションに書き込みます。デバイスの設定は NVRAM (不揮発性ランダムアクセスメモリ) に保存されます。このタスクは複数のデバイスで実行できます。

単一のデバイス

CA Spectrum が監視しているネットワーク内のデバイスの表記です。単一のデバイスを設定した場合、すべてのグローバルデバイスマトリクスの設定より優先されます。

同期タスク

ネットワーク上の選択されたデバイスについて、ポリシーに準拠しているデバイス設定をキャプチャおよび検証し、結果をリアルタイムで表示します。同期タスクでデバイス設定がキャプチャされる場合、デバイスに関連するすべてのポリシーに対して設定が確認されます。このタスクは複数のデバイスで実行できます。

アップロード タスク

新しいコンテンツを、1つまたは複数の選択されたデバイスのランニング コンフィギュレーションにマージします。このタスクは複数のデバイスで実行できます。

設定のタイプ

以下のセクションでは、デバイスのさまざまな設定について説明します。

ランニング コンフィギュレーション

ランニング コンフィギュレーションは、デバイスにロードされている設定のバージョンであり、デバイスが現在どのように動作するかが定義されます。ランニング コンフィギュレーションのみが、現在のランタイム セッションに有効です。

スタートアップ コンフィギュレーション

スタートアップ コンフィギュレーションは、デバイスに格納されている設定のバックアップ バージョンです。デバイスが再起動された場合、スタートアップ コンフィギュレーションが使用されます。デバイスによっては、プライマリおよびセカンダリのスタートアップ コンフィギュレーションが存在します。デバイスでは起動時に、前回のランニング コンフィギュレーションがスタートアップ コンフィギュレーションのコピーで置き換えられます。

設定ファイル

設定ファイルには、デバイスの製造元によるランニング コンフィギュレーションの属性のサブセットが含まれます。多くのデバイスでは、Network Configuration Manager による完全な設定ファイルのキャプチャが可能です。キャプチャされた設定ファイルは編集することができます。

サポートされているデバイス

Network Configuration Manager では、以下のベンダーのデバイス ファミリをすぐに使用できます。

- Cisco
- Enterasys
- Enterasys
- Riverstone SSR
- Extreme
- Foundry
- Juniper
- Lancom
- Nortel (Baystack および Passport)

これらのデバイス ファミリのいずれかに当てはまらないデバイスは、Network Configuration Manager 拡張ユーティリティを使用して設定できます。

デバイス認定データベースに照会することによって、すべてのサポートされているデバイスのリストを取得できます。デバイス認定データベースにアクセスするには、[CA サポート Web サイト](#)に移動します。CA Spectrum 製品ページの「参考資料」セクションには、「Device and Technology Certification」へのリンクが含まれています。詳細については、「認定ユーザガイド」を参照してください。

デバイス認定データベースへのアクセス

CA テクニカルサポート Web サイトのアプリケーションでは、すべての CA Spectrum 認定デバイスについて検索できます。CA Spectrum が特定のデバイスモデルをサポートするかどうかを判別し、ファームウェアのバージョンおよびリリースによってフィルタできます。また、デバイスが簡易認定または拡張認定でサポートされているかどうかを確認できます。

次の手順に従ってください:

1. [CA サポート オンラインの Web サイト](#)に移動します。
2. CA Spectrum 製品ページにアクセスします。

3. [Recommended Reading] リンクをクリックします。
4. [Device and Technology Certification] リンクをクリックします。
5. そのページで、[Search engine] リンクをクリックします。
Certification Web Database Search アプリケーションが表示されます。
6. [Product Line] ドロップダウンリストから Spectrum 製品を選択します。

Record	System Object Identifier	Support Level
Cisco : 1100AP	1.3.6.1.4.1.9.1.507	ENHANCED
Cisco : 1200-1220AP	1.3.6.1.4.1.9.1.474	ENHANCED
Cisco : 1210-1230AP	1.3.6.1.4.1.9.1.525	ENHANCED
Cisco : 1240AP	1.3.6.1.4.1.9.1.685	ENHANCED
Cisco : 1250AP	1.3.6.1.4.1.9.1.758	ENHANCED
Cisco : 1300AP	1.3.6.1.4.1.9.1.565	ENHANCED
Cisco : 1400AP	1.3.6.1.4.1.9.1.533	ENHANCED

7. デバイスを見つけるために必要に応じて、以下の検索条件フィールドに入力します。

Certified Vendors

CA Spectrum が認定した 1 つ以上のデバイスを製造する企業または組織。ベンダー フィルタは、選択したベンダーによって所有または取得されたすべてのデバイスに検索を限定します。

Keyword Search

各デバイスのデバイスタイプ名フィールドを検索します。キーワード検索は、デバイスタイプ名フィールドに特定のキーワードが含まれるすべてのデバイスに検索を限定します。

System Object Identifier

システム オブジェクト ID またはシステム オブジェクト ID の一部を検索します。入力したシーケンスが含まれるデバイスがすべて返されます。

たとえば、1.3.6.1.4.1.9.1.685 は Cisco 1240AP デバイスを示します。

注: 一意のシステム オブジェクト ID を持たないデバイスもあります。さらに、一部のデバイスにはシステム オブジェクト ID がありません。

Support Level

CA Spectrum 認定サポートの現在のレベルを示します。2 レベルの認定サポートを利用可能です。詳細については、「概要」トピックを参照してください。

8. [Search Database] ボタンをクリックして、検索条件に基づく検索を開始します。

1 行に 1 つのデバイスの結果が表示されます。このレベルの詳細には、デバイス名およびモデル、システム オブジェクト ID、およびサポート レベルが含まれます。

9. 結果テーブルの特定のエントリをクリックします。

次のように、選択したデバイスに関する詳細情報が表示されます。

Cisco : 1240 AP

Device Information

	Device Name: 1240 AP
	System Object Identifier: 1.3.6.1.4.1.9.1.685

Version Support History

SPECTRUM 9.1:

	Release	Firmware	Model Type	Support Level
	Initial	AP 12.2 (IOS)	AironetIOS	ENHANCED

SPECTRUM 9.0:

	Release	Firmware	Model Type	Support Level
	Initial	AP 12.2 (IOS)	AironetIOS	ENHANCED

SPECTRUM 8.1:

	Release	Firmware	Model Type	Support Level
	Initial	AP 12.2 (IOS)	AironetIOS	ENHANCED

デバイス ファミリ

Network Configuration Manager のサポートを受けるには、デバイス ファミリとデバイスを関連付ける必要があります。標準でサポートされているデバイスは、自動的に適切なデバイス ファミリに割り当てられます。デバイスは、単一のデバイス ファミリにのみ属することができます。

Network Configuration Manager デバイス ファミリは、アクセス方法を設定するための一元的な場所を提供します。アクセス方法は他のファミリ メンバからデバイス設定にアクセスするために使用されます。ローカルデバイスでデバイス ファミリの設定を上書きできます。詳細については、「[デバイス ファミリの設定 \(P. 47\)](#)」を参照してください。

Network Configuration Manager の拡張ユーティリティでは、オンデマンドでさらにデバイス ファミリを作成できます。これにより、Network Configuration Manager は拡張され、さらにデバイスおよびベンダーをサポートできます。手動でさらにデバイス ファミリを作成し、手動でユーザが作成したデバイス ファミリにデバイスを移動する詳細については、「[拡張ユーティリティ \(P. 23\)](#)」を参照してください。

Network Configuration Manager によるデバイス ファミリの特定方法

Network Configuration Manager は、標準でサポートされるデバイスのデバイス ファミリを自動的に特定します。通常、この決定はベンダーに基づいて行われます。詳細については、「[サポートされているデバイス \(P. 191\)](#)」を参照してください。

Cisco IOS デバイス

以下のデバイス ファミリが Cisco IOS デバイスに存在します。

- Cisco IOS - SSH Capable (SSH/SCP 通信モード対応)
- Cisco IOS (SSH/SCP 通信モード非対応)

Cisco IOS - SSH Capable ファミリにデバイスを配置するには、以下の条件を満たす必要があります。

- デバイス記述子は、12.2 (18) 以上のファームウェア バージョンを示す必要があります。
- 機能セットには、SCP で必要とされる暗号化機能を備えたデバイスを示す「K9」という文字が含まれている必要があります。
- デバイスへの SSH アクセスは、ディスクバリ時に禁止を解除する必要があります。

注: デバイスへの SSH アクセスがディスクバリ時にブロックされる場合（例：ファイアウォール）、Cisco IOS デバイス ファミリにデバイスを入れます。

たとえば、以下に記述されているデバイスは Cisco IOS - SSH Capable ファミリに配置されます。

```
Cisco IOS Software, 7200 Software (C7200-JK9S-M), Version 12.3(14)T6,  
RELEASE SOFTWARE (fc2)  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2006 by Cisco Systems, Inc.  
Compiled Thu 05-Jan-06 05:36 by dchih
```

以下に記述されているデバイスは、Cisco IOS ファミリに配置され、SSH/SCP を使用して設定を取得することはできません。

```
Cisco Internetwork Operating System Software  
IOS (tm) C2600 Software (C2600-J1S3-M), Version 12.3(17a), RELEASE  
SOFTWARE (fc2)  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2005 by cisco Systems, Inc.  
Compiled Mon 12-Dec-05 1
```

Cisco NX OS デバイス

Cisco NX OS デバイスは、Net::SSH::Expect モジュールを使用するスクリプトによってサポートされています。Cisco NX OS デバイスを標準でサポートするために、これらのモジュールで Perl の領域をセットアップする必要があります。

Perl の環境をセットアップする詳細については、「[Perl モジュール \(P. 72\)](#)」を参照してください。

Juniper JUNOS デバイス

Network Configuration Manager では JUNOScript API を使用し、JUNOS デバイスと通信します。具体的には、以下のとおり JUNOScript API マージ コマンドは、アップロードを実行するために使用されます。

```
<load-configuration format="text" action="merge">
```

JUNOScript サポートは、JUNOScript バージョン 6.3R1 を使用して開発されました。JUNOScript API の新しいリリースは通常、後方互換性があります。

JUNOScript API コマンドは、JUNOS CLI コマンドと異なります。その結果、Network Configuration Manager のアップロードでは、アップロードを成功させるために正しい形式を使用する必要があります。

詳細については、JUNOScript API の Juniper のドキュメント Web サイトを参照してください。

例: JUNOScript API 形式の使用

以下の例は、JUNOS CLI コマンドラインから入力されたコマンドと JUNOScript API からのコマンドの違いを示します。コマンドはデバイスから snmp の場所フィールドを削除します。

テストデバイスには、以下の設定テキストのブロックがあります。これは snmp 場所フィールドの値を「Boston」に設定しています。

```
snmp {  
    name jun2300-96.4;  
    description "Juniper J2300 w/ JUNOS 9.0R4 built 2008-11-18 18:55:38 UTC";  
    location Boston;
```

以下のコマンドは JUNOS CLI コマンドラインから使用し、このデバイス上の snmp 場所フィールドを削除できます。

```
admin@jun2300-96.4# delete snmp location
```

以下の Network Configuration Manager アップロードは、デバイスから snmp 場所フィールドを削除します。

```
snmp {  
    delete: location;  
}
```

どちらの操作も同等です。ただし、JUNOScript API 構文が Network Configuration Manager アップロードで使用される必要があります。

拡張ユーティリティ

Network Configuration Manager の拡張ユーティリティでは、Network Configuration Manager の機能を標準サポート以上に拡張できます。拡張ユーティリティで、以下のタスクを実行できます。

- オンデマンドでさらにデバイスファミリを作成します。その後、Perl のスクリプトを使用して、これらの追加のデバイスファミリを設定し、より多くのデバイスで Network Configuration Manager 機能を拡張できます。デバイスファミリを作成する詳細については、「[カスタムデバイスファミリの作成 \(P. 62\)](#)」を参照してください。スクリプトを設定する詳細については、「[拡張ユーティリティのスクリプト設定 \(P. 65\)](#)」を参照してください。
- Network Configuration Manager がデバイス上で実行する操作で Perl スクリプトを使用して、さらにデバイスおよびベンダーを管理します。スタートアップコンフィギュレーションのキャプチャおよび書き込みなどの操作です。また、この操作にはランニングコンフィギュレーションのキャプチャまたはアップロードが含まれます（デバイスファームウェアのアップロード、デバイスの再ロード、およびデバイス上の再ロード操作のキャンセル）。スクリプトは、Network Configuration Manager 内でそれぞれの操作用に設定できます。カスタマイズされたスクリプトを使用してこれらの操作を実行する詳細については、「[Network Configuration Manager の拡張ユーティリティ \(P. 60\)](#)」を参照してください。
- インストール用にカスタマイズされたトラップ設定を作成します。これは設定変更イベント情報を相關するために使用できます。詳細については、「[設定通知トラップ設定 \(P. 51\)](#)」を参照してください。

Network Configuration Manager の前提条件

Network Configuration Manager を実行し、管理されたネットワークでデバイス設定の実行履歴をアクティブに保持するには、以下の手順を実行します。

- SNMP を使用している場合、読み取り/書き込みコミュニティ文字列でデバイスをモデリングします。 詳細については、「[IT インフラストラクチャのモデリング/管理 - 管理者ガイド](#)」を参照してください。
- SSH を使用する場合、デバイスで SCP が有効になっていることを確認します。 詳細については、「[通信モード \(P. 24\)](#)」を参照してください。

通信モード

以下の表は、Network Configuration Manager でサポートされているデバイスをサポートする通信モードを示しています。列内の「X」は、通信モードがそのデバイス ファミリでサポートされていることを示します。Perl スクリプトがデバイスと通信する唯一の方法である場合、スクリプトで使用されるメソッドについて通知されます。

SNMP/TFTP 通信モードを使用するデバイスでキャプチャおよびロードの設定を有効化するには、「[TFTP サーバの設定 \(P. 36\)](#)」を参照してください。

デバイス ファミリ	SNMP/TFTP	Telnet/FTP	SSH/SCP	SSH/TFTP	Perl
Cisco CatOS	X			X	
Cisco IOS	X	X			X
Cisco IOS-SSH Capable	X	X	X		X
Cisco NX OS					SSH
Cisco PIX OS					Telnet
Enterasys	X				X
Enterasys/Riverstone SSR	X				X
Extreme	X				X
Foundry	X				X
Juniper JUNOS			X		X

デバイス ファミリ	SNMP/TFTP	Telnet/FTP	SSH/SCP	SSH/TFTP	Perl
Lancom LCOS					TFTP/ Telnet
Nortel Baystack				X	X
Nortel Passport 8600	X				X
Nortel Passport L3	X				X

SSH v2 のサポート

Network Configuration Manager では、SSH v2 のみがサポートされます。SSH v1 はサポートされません。SSH v1 のみがサポートされる Cisco デバイスは、Cisco IOS - SSH Capable ファミリに自動的に配置されません。

Network Configuration Manager では、SSH v1 のみをサポートする Juniper デバイスはサポートされません。

SSH v2 をサポートするには、Cisco または Juniper のデバイスでファームウェアをインストールまたは更新します。「[デバイス ファミリにデバイスを配置 \(P. 64\)](#)」の手順に従って、デバイスを追加します。

Cisco デバイス および SCP

SSH 通信モードを使用するには、Cisco デバイスでセキュア コピー (SCP) が有効になっている必要があります。

SCP の詳細については、<http://www.cisco.com> で Cisco IOS セキュア コピー機能のドキュメントを参照してください。

デバイス設定変更の未承諾通知

Network Configuration Manager は、変更が発生した直後にデバイス設定のキャプチャを試みます。設定変更の未承諾通知は、変更が発生したデバイスから送信されるトラップまたは MIB オブジェクトのいずれかになります。

設定が変更された場合、一部のデバイスは SNMP トラップを送信します。その後、SpectroSERVER がキャプチャを実行してデータベースに設定を保存し、更新された設定データを提供します。Network Configuration Manager ポリシーは、最新の設定キャプチャに対してテストされます。 詳細については、「[デバイストラップ \(P. 26\)](#)」を参照してください。

選択した情報はこれらの設定トラップ通知から解析し、ホスト設定テーブルで表示できます。 詳細については、「[設定通知トラップ設定 \(P. 51\)](#)」を参照してください。

SNMP トラップを送信する代わりに、または送信に加えて、一部のデバイスでは MIB 属性を更新して設定変更の信号を送信します。 次に、SpectroSERVER は MIB をポーリングして、属性の変更が認識されると新しい設定をキャプチャします。 詳細については、「[デバイスマIBオブジェクト \(P. 27\)](#)」を参照してください。

Network Configuration Manager では、サポートされているデバイスのサブセット上で通知を監視します。 Network Configuration Manager を拡張して、その他のサポートされているデバイスからトラップおよび MIB オブジェクトをさらに監視することができます。

デバイス設定変更の未承諾通知を有効化すると、ネットワーク上のデバイスの最新更新済み設定キャプチャが提供されます。 この機能を無効化し、ネットワークパフォーマンスを低下させる可能性のある TFTP 転送を含む不要なキャプチャを回避できます。 詳細については、「[一般設定の設定 \(P. 29\)](#)」および「[単一のデバイスで未承諾デバイス設定キャプチャの設定 \(P. 55\)](#)」を参照してください。

デバイストラップ

Network Configuration Manager では、以下の 2 つのトラップがサポートされています。

- Cisco: ciscoConfigManEvent 1.3.6.1.4.1.9.9.43.2
- Juniper: jnxCmCfgChange 1.3.6.1.4.1.2636.4.5

これらのトラップのどちらかを受信すると、CA Spectrum ではイベント 0x00821029 が生成されます。 このイベントによって、Network Configuration Manager によるキャプチャの実行がトリガれます。 他のサポートされているデバイスのキャプチャをトリガする場合は、そのイベントにさらに設定変更トラップをマッピングします。

デバイス MIB オブジェクト

設定変更が発生した場合、Network Configuration Manager は特定されるモデル属性によって MIB オブジェクトをポーリングします。この機能は、以下の MIB オブジェクトをサポートする Cisco デバイスおよび Juniper デバイスでサポートされています。

- CISCO-CONFIG-MAN-MIB: ccmHistoryRunningLastChanged
1.3.6.1.4.1.9.9.43.1.1.1
- JUNIPER-CFGMGMT-MIB: jnxCmCfgChgLatestTime 1.3.6.1.4.1.2636.3.18.1.2

他のサポートされているデバイスに属性ポーリング メカニズムを拡張できます。Model Type Editor を使用し、設定変更通知をポーリングする属性を作成し、それをポーリングされた属性にします。次に、新しく作成されたポーリングされた属性の属性 ID に Config_Change_AttrID 属性 (0x12bf8) の値を設定します。その後、Network Configuration Manager ではこの属性の設定変更通知を監視し、キャプチャを実行します。

グローバルコレクション

グローバルコレクションにより、ネットワーク デバイスの表示を管理できます。グローバルコレクションには、複数のベンダーからのデバイスが含まれます。バルク タスクを実行する場合、または Network Configuration Manager ポリシーを作成する場合、グローバルコレクションが役立ちます。

グローバルコレクションの詳細については、「IT インフラストラクチャのモデリング/管理 - 管理者ガイド」を参照してください。

詳細情報:

- [グローバルコレクションとタスクの関連付け \(P. 127\)](#)
- [グローバルコレクションにポリシーを適用 \(P. 170\)](#)

保守モード

保守モードにあるすべてのデバイスで、Network Configuration Manager が無効化されます。デバイスが保守モードであるかどうかを確認するには、[エクスプローラ] タブからデバイスを選択し、[情報] タブをクリックします。一般情報画面の下に、[保守モード] オプションがあります。このオプションが「はい」に設定されている場合、デバイスは保守モードになっています。

Network Configuration Manager レポート パック

Network Configuration Manager のレポート オプションは、CA Spectrum Report Manager のネットワーク設定管理レポートパックに含まれています。Report Manager では、多数のレポート コンテンツ、形式、およびレポート構成オプションが提供されます。デバイス設定変更に関心のある組織のさまざまな対象読者に対して、適切なタイプおよび範囲の情報でレポートを生成できます。

詳細については、「[Report Manager からの Network Configuration Manager レポート \(P. 94\)](#)」および「Report Manager ユーザ ガイド」を参照してください。

第 2 章: Network Configuration Manager の設定

このセクションには、以下のトピックが含まれています。

[Network Configuration Manager の設定 \(P. 29\)](#)

[デバイス ファミリの設定 \(P. 47\)](#)

[単一のデバイスの設定によるデバイス ファミリ設定の上書き \(P. 54\)](#)

[Network Configuration Manager 拡張ユーティリティ \(P. 60\)](#)

Network Configuration Manager の設定

このセクションでは、Network Configuration Manager の基本設定について説明します。

一般設定の実行

初期設定をいくつか選択し、Network Configuration Manager が設定キャプチャを実行し、変更イベントを相關する方法を決定します。

次の手順に従ってください:

1. [エクスプローラ] タブで [設定マネージャ] を選択します。
コンテンツ画面の [情報] タブに、情報および設定が表示されます。
2. 一般設定サブビューを展開します。
一般設定オプションが表示されます。
3. 必要に応じて、以下の一般設定オプションを変更します。

未承諾デバイス設定キャプチャ

デバイスから未承諾通知の受信時に、そのデバイスの設定をキャプチャすることを Network Configuration Manager で有効化または無効化します。設定変更の未承諾通知は、Network Configuration Manager が変更を監視しているトラップまたは MIB オブジェクトのいずれかになります。

相関イベント期間(秒)

設定変更イベントが相関している期間を指定します。この期間中に発生する特定のデバイスに使用されるすべての設定変更イベントは、単一のイベントに結合されます。

デフォルト : 120

新しくモデリングされたデバイスの設定をキャプチャ

グローバル レベルでネットワーク上に新しくモデリングされたデバイスを処理する方法を指定します。利用可能な値は以下のとおりです。

次のグローバル同期時

グローバル同期スケジュールに従って、新しくモデリングされたデバイスをキャプチャします。

キャプチャしない

新しくモデリングされたデバイス上の Network Configuration Manager を無効にします。 Network Configuration Manager の機能を有効にするには、デバイス上で Network Configuration Manager を手動で有効化します。

即時

グローバル同期の実行を待機することなく、新しくモデリングされたデバイスを（モデリングされた時点で）即座にキャプチャします。

タスクワークの待ち行列サイズ

各 CA Spectrum ホスト上で並行して処理されるデバイスの最大数を指定します。

実行中のタスクを手動で停止する場合、停止コマンドを受信した後に現在キューにあるすべてのデバイスが処理されます。

デフォルト : 10

設定履歴設定の選択

以下の手順では、キャプチャされた設定のストレージを制御する方法について説明します。デバイスごとに保存される設定数、または時間の長さのいずれかによって、キャプチャされた設定を保持できます。

重要: キャプチャされた設定を格納する方法を指定する場合、SpectroSERVER データベースへの影響を検討します。あまりにも多くの設定が保持される場合、設定ファイルモデルで SpectroSERVER データベースを満たすことができます。

次の手順に従ってください:

1. [エクスプローラ] タブで [設定マネージャ] を選択します。
コンテンツ画面の [情報] タブに、情報および設定が表示されます。
2. 設定履歴サブビューを展開します。
キャプチャされた設定の停止方法を制御するために使用されるオプションが表示されます。
3. 以下のオプションのいずれかを選択します。
 - **デバイスごとに格納される最大設定数を指定します。** このオプションでは、指定された数に基づくデバイスごとにキャプチャされた設定を格納します。

デバイスごとの最大格納設定数

デバイスごとに格納される設定の最大数を指定します。たとえば、数値が 25 の場合、デバイスごとに最新の 25 件の設定が CA Spectrum データベースに存在することを示します。

デフォルト: 25

- **設定が保存される最大日数を指定します。** このオプションでは、時間に基づくキャプチャされた設定を格納します。

ホスト設定が保存される最大日数

破棄される前に、ホスト設定が保存される最大日数を指定します。

注: 設定がキャプチャされる頻度によっては、長い期間を指定すると、SpectroSERVER データベースが設定ファイルモデルで満たされる可能性があります。

デフォルト: 30 (日)

デバイスごとの最小格納設定数

デバイスごとに格納されるホスト設定の最小数を指定します。設定がこの最小値で残すには古くなり継続できない場合も、設定は保持されます。

デフォルト: 5

設定変更アラート設定の選択

設定変更アラート設定は、アラームをトリガする設定変更イベントと、生成されるアラームのタイプを制御します。 設定変更アラート設定を選択し、表示されるアラームを決定できます。

次の手順に従ってください:

1. [エクスプローラ] タブで [設定マネージャ] を選択します。
コンテンツ画面の [情報] タブに、情報および設定が表示されます。
2. 設定変更アラート サブビューを展開します。
設定変更アラート オプションが表示されます。
3. 必要に応じて、以下の [設定変更アラート] オプションを変更します。

アラート モード

アラームをトリガするイベントを指定します。

変更時のアラーム

アラームは設定変更のみに対して生成されます。

参照違反時のアラーム

アラームは参照設定違反のみに対して生成されます。

参照違反時または変更時のアラーム

アラームは参照設定違反および設定変更の両方に対して生成されます。

アラームなし

アラームはどの設定変更に対しても生成されません。

デフォルト：アラームなし

参照違反アラート タイプ

参照設定違反が発生した場合に生成されるアラームまたはイベントのタイプを指定します。既存の比較マスクは、現在の設定と参照設定の大きな違いを確定するために使用されます。現在の設定が参照設定に一致する場合、参照違反アラームは自動的にクリアされます。

参照設定を設定する詳細については、「[参照設定の指定 \(P. 91\)](#)」を参照してください。

有効な値は、重大、メジャー、マイナーのアラームおよびイベントのみです。

デフォルト：イベントのみ

設定変更アラートタイプ

設定変更が発生した場合に生成されるアラームまたはイベントのタイプを指定します。

有効な値は、重大、メジャー、マイナーのアラームおよびイベントのみです。

デフォルト：イベントのみ

承認ワークフロー

承認ワークフローでは、処理される前に Network Configuration Manager が承認を受信することによって開始される設定変更を必要とします。承認ワークフローでは、承認プロセスで CA Service Desk チケットまたは CA Spectrum 許可権限を使用するようセットアップできます。

このセクションでは、承認ワークフロー オプションを設定する方法について説明します。また、OneClick 承認ワークフロー モードが有効な場合のタスクを承認する方法についても説明します。

タスクを使用して設定変更を開始する詳細については、「[Network Configuration Manager デバイス レベル タスク \(P. 99\)](#)」および「[Network Configuration Manager バルク タスク \(P. 105\)](#)」を参照してください。

注：詳細については、「CA Spectrum および CA Service Desk 統合ガイド」を参照してください。

ワークフロー オプションの設定

承認ワークフローでは、処理される前に Network Configuration Manager が承認を受信することによって開始される設定変更を必要とします。承認の要求および処理方法を決定するには、承認ワークフロー オプションを設定します。

次の手順に従ってください:

1. [エクスプローラ] タブで [設定マネージャ] を選択します。
コンテンツ画面の [情報] タブに、情報および設定が表示されます。
2. ワークフロー サブビューを展開します。
承認ワークフロー オプションが表示されます。
3. 必要に応じて、以下の承認ワークフロー設定を変更します。

承認ワークフロー モード

デバイスを変更するすべての操作に対して承認が必要かどうかを指定します。これらの操作には、アップロード、スタートアップへの保存、ファームウェアのロード、再ロード、および再ロード キャンセルのタスクが含まれます。

無効

Network Configuration Manager で開始される設定変更が承認を必要としないことを示します。

ServiceDesk

Network Configuration Manager で開始される CA Service Desk で承認を取得する必要がある設定変更を指定します。タスクが作成された場合、CA Service Desk チケットが生成されます。承認された場合、タスクは処理できる状態に配置されます。

このオプションが選択されている場合、[設定] ボタンは有効です。[設定] ボタンをクリックし、ServiceDesk ワークフロー設定ページを呼び出します。ここでは、以下のフィールドに初期値を設定できます。

エラー タイプ: エラー タイプの値は、CA Spectrum で統合使用するために Service Desk で設定されます。これらの値の詳細については、「CA Service Desk 実装ガイド」を参照してください。

承認済みステータス、拒否ステータス、キャンセルステータス、承認待機ステータス：さまざまなステータスの値をエラータイプによって使用できます。ステータスの値は、CA Spectrum との統合用に CA Service Desk で設定されます。これらの値をセットアップする詳細については、「CA Spectrum および CA Service Desk 統合ガイド」を参照してください。

注: Service Desk 承認が有効で、タスクを作成するユーザに [タスク承認者] 権限がある場合、CA Service Desk 承認は任意です。 詳細については、「[Network Configuration Manager 権限 \(P. 265\)](#)」を参照してください。

OneClick

[タスク承認者] 許可のあるユーザによって開始または承認された場合にのみ処理できる、Network Configuration Manager で開始される設定変更を指定します。

デフォルト：無効

承認プロセスに設定変更を含める

設定コンテンツを承認要求に含めるかどうかを指定します。

デフォルト：いいえ

注: ユーザには、このオプションを有効にする [承認要求から設定変更を非表示] 権限が必要です。 詳細については、「[Network Configuration Manager 権限 \(P. 265\)](#)」を参照してください。

OneClick のタスクを承認

OneClick 承認ワークフロー モードが有効な場合、[タスク承認者] 権限のあるユーザは OneClick コンソールからタスクを承認する必要があります。

注: また、電子メール通知からのタスクを承認または拒否できます。 タスクに対して承認が要求される場合、電子メールは生成され、承認用にタスク承認者に送信されます。 電子メールに含められたリンクからタスクを承認または拒否できます。 適切なリンクを選択します。 タスクが承認または拒否されるかどうかを反映し、状態が更新されます。

次の手順に従ってください:

1. [エクスプローラ] タブの [設定マネージャ] の下にある [タスク] フォルダで「タスク」を選択します。

使用可能なタスクがコンテンツ画面の[リスト]タブに表示されます。

2. タスクを右クリックし、右クリックメニューから必要に応じて、[タスクの承認]、[タスクの拒否]、または[承認要求のキャンセル]を選択します。

タスクの状態は、タスクがそれぞれ [承認済み]、[拒否]、または [キャンセル] のいずれであるかを反映して更新されます。

TFTP サーバの設定

このセクションでは、SpectroSERVER システムで Trivial File Transfer Protocol (TFTP) サーバを開始する方法について説明します。TFTP でコンフィギュレーションファイルが転送されます。このプロセスは以下の 2 つの手順から構成されます。

- システムを TFTP サーバとして設定する。この手順はプラットフォームによって異なります。
- OneClick で TFTP 設定を指定する。

分散 SpectroSERVER (DSS) 環境がある場合、TFTP サーバが Network Configuration Manager 機能を有効にするために、すべての SpectroSERVER で実行されている必要があります。

サポートされるデバイスファミリ通信モードについては、「[通信モード \(P. 24\)](#)」を参照します。

注: 適切なコミュニティ名（読み取り/書き込み）を使用して、ネットワークの各デバイスが正しくモデリングされていることを確認します。

TFTP サーバとしてシステムをセットアップ

このセクションでは、TFTP サーバとしてシステムをセットアップする方法について説明します。手順はプラットフォームによって変わります。

TFTP をサポートする Solaris バージョン 10 または 11 システムの設定

以下の手順では、TFTP をサポートするために Solaris（バージョン 10 または 11）システムをセットアップします。

次の手順に従ってください：

1. `root` としてログインします。
2. 以下のコマンドを使用して、`/tftpboot` ディレクトリを作成し、すべてのユーザにディレクトリの読み取り/書き込み権限を与えます。

```
mkdir /tftpboot  
chmod 777 /tftpboot
```

注：TFTP サーバは SpectroSERVER ホスト システム以外のシステムで実行できます。ただし、SpectroSERVER コンピュータは TFTP サーバのルートディレクトリにアクセスできる必要があり、SpectroSERVER コンピュータ上のルートディレクトリは TFTP サーバと共有される必要があります。詳細については、「[リモート TFTP または FTP サーバを使用する場合の考慮事項 \(P. 43\)](#)」を参照してください。

3. `/etc/services` ファイルに TFTP エントリが含まれていることを確認します。エントリを検索するには、以下のコマンドを入力します。

```
cd /etc  
grep tftp services
```

`/etc/services` ファイルに以下のエントリが示されます。

```
tftp      69/udp
```

このエントリが表示されない場合、サービス ファイルを編集して [ホスト特有の機能] セクションに追加します。

4. `/etc/inetd.conf` ファイル内で以下の行を検索し、行頭のシャープ記号 (#) を削除してコメント解除します。

```
#tftp dgram udp6 wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
```

5. エントリが `-s /tftpboot` オプションで終わることを確認します。この最後に `tftp` ディレクトリ（この場合、`/tftpboot`）を指定します。

6. `inetconv` コマンドを実行します。

7. tftp サービスが有効であることを確認します。

```
svcs | grep tftp
```

以下のレスポンスが表示されます。

```
online Apr_10 svc:/network/tftp/udp6:default
```

8. システムが TFTP サーバとして設定されている場合、TFTP 転送を利用できるようにデバイスが読み取り/書き込みコミュニティ文字列でモーリングされていることを確認します。
9. 「[TFTP 設定](#) (P. 40)」に説明されているとおり、OneClick の TFTP 設定を設定します。

TFTP をサポートする Linux システムの設定

以下の手順では、TFTP をサポートするために Linux システムをセットアップします。

次の手順に従ってください:

1. root としてログインします。
2. 以下のコマンドを実行して、システムに TFTP サーバがインストールされていることを確認します。

```
% rpm -q tftp-server
```

以下のメッセージは、TFTP サーバがインストールされていることを示します。

```
tftp-server-<version>.EL3.1
```

上記のメッセージが表示されない場合、TFTP サーバがインストールされていません。以下の手順を実行します。

- a. TFTP パッケージは Redhat の Web サイト (<http://www.redhat.com>) からダウンロードします。
- b. 以下のコマンドを実行します。

```
% rpm -i <package.rpm>
```
- c. 以下の手順に従って、Red Hat の Web サイトから rpm パッケージをインストールします。

3. 以下のコマンドを使用して、/tftpboot ディレクトリを作成し、すべてのユーザにディレクトリの読み取り/書き込み権限を与えます。

```
mkdir /tftpboot
chmod 777 /tftpboot
```

注: TFTP サーバは SpectroSERVER ホストシステム以外のシステムで実行できます。ただし、SpectroSERVER コンピュータは TFTP サーバのルートディレクトリにアクセスできる必要があり、SpectroSERVER コンピュータ上のルートディレクトリは TFTP サーバと共有される必要があります。詳細については、「[リモート TFTP または FTP サーバを使用する場合の考慮事項 \(P. 43\)](#)」を参照してください。

4. /etc/xinetd.d ディレクトリに移動します。

5. tftp と名付けられたファイルを以下のように編集します。

```
Set disable=no
```

6. ファイルを保存して閉じます。

7. 以下のコマンドのいずれか 1 つを実行し、xinetd サービスを再起動します。

- % service xinetd restart

以下のメッセージが表示されます。

```
Stopping xinetd  OK
Starting xinetd  OK
```

または

- % killall -HUP xinetd

8. TFTP サーバが稼働していることを確認します。

注: 検証の 1 つのメソッドでは、Network Configuration Manager キャプチャを実行します。TFTP タイムアウトエラー /event 0x821001 を受信した場合、TFTP は稼働していません。

9. 「[TFTP 設定 \(P. 40\)](#)」に説明されているとおり、OneClick の TFTP 設定を設定します。

Windows 上の TFTP サーバ

TFTP サーバは、通常 Windows で使用できません。任意のデバイス ファミリに対して TFTP 通信モードを使用する場合、TFTP サーバをセットアップします。複数の無料または商用アプリケーションが使用できます。

リモート ホスト上の TFTP サーバを Network Configuration Manager で使用するには、「[リモート TFTP または FTP サーバを使用する場合の設定 \(P. 43\)](#)」を参照してください。

TFTP をサポートする Windows システムを設定するには、「[TFTP 設定 \(P. 40\)](#)」に述べられている手順を完了します。このプロシージャの手順は、インストールするすべての TFTP サーバに適用できます。

Windows で TFTP サーバを設定する方法

このセクションでは、OneClick で TFTP を設定する方法について説明します。

注: この手順を実行する前に、システムが TFTP サーバとして設定されていることを確認します。詳細については、「[システムを TFTP サーバとしてセットアップ \(P. 36\)](#)」を参照してください。

次の手順に従ってください:

1. [エクスプローラ] タブで [設定マネージャ] を選択します。
コンテンツ画面の [情報] タブに、情報および設定が表示されます。
2. TFTP 設定サブビューを展開します。
TFTP 設定テーブルが表示されます。
3. 必要に応じて、以下を変更します。 [設定] をクリックして特定のフィールドを編集し、完了したら Enter キーを押します。

デフォルト TFTP ホスト

ランドスケープ用の TFTP サーバ IP アドレス。デフォルトでは SpectroSERVER を実行しているホスト システム。

このフィールドでは、TFTP サーバの IP アドレスをグローバルに変更できます。リモート ホストを使用する場合の考慮事項については、「[リモート TFTP または FTP サーバを使用する場合の考慮事項 \(P. 43\)](#)」を参照してください。

注: 属性 DefaultTftpHost は、属性エディタで設定できます。

デフォルト TFTP ディレクトリ

TFTP が実行されているパス名。 [設定] をクリックして、以下のように有効な TFTP サーバのパスを入力します。

- Unix システムの場合、/tftpboot
- Windows の場合、C:\win23app\SPECTRUM\NCM\tftp

注: TFTP サーバは SpectroSERVER ホストシステム以外のシステムで実行できます。ただし、SpectroSERVER コンピュータは TFTP サーバのルートディレクトリにアクセスできる必要があり、SpectroSERVER コンピュータ上のルートディレクトリは TFTP サーバと共有される必要があります。詳細については、「[リモート TFTP または FTP サーバを使用する場合の考慮事項 \(P. 43\)](#)」を参照してください。

TFTP 転送タイムアウト(秒)

TFTP 転送がタイムアウトするまでの時間。[設定] をクリックし、TFTP サーバと接続する場合のタイムアウト値(秒)を指定します。デフォルトは 50 秒で、これはデータ転送の間隔が 50 秒であることを示します。

ランドスケープ

CA Spectrum ランドスケープ (表示のみ)。

FTP サーバの設定

SpectroSERVER システムでローカル FTP サーバを使用できるように、Network Configuration Manager を設定します（サポートされているデバイスファミリ通信モードについては、「[通信モード \(P. 24\)](#)」を参照してください）。

ファイル転送に FTP を使用するデバイスを展開している場合は、FTP サーバを設定します。プラットフォーム用のネイティブ FTP サーバをインストールおよび設定することをお勧めします。Windows プラットフォームの場合、以下のリンクにネイティブ FTP サービスのインストールおよび設定方法が説明されています。

- Windows Server 2008 :
[http://technet.microsoft.com/en-us/library/cc732769\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc732769(WS.10).aspx)
- Windows Server 2012 :
<http://www.c-sharpcorner.com/UploadFile/cd7c2e/how-to-install-ftp-server-on-windows-server-2012/>

次の手順に従ってください:

1. [エクスプローラ] タブで [設定マネージャ] を選択します。
コンテンツ画面の [情報] タブに、情報および設定が表示されます。
2. FTP 設定サブビューを展開します。
FTP 設定テーブルが表示されます。
3. 必要に応じて、以下の設定を変更します。 [設定] をクリックして特定のフィールドを編集し、Enter キーを押します。

デフォルト FTP ホスト

ランドスケープ用の FTP サーバの IP アドレス。デフォルトでは、SpectroSERVER はこのホストシステムで実行されます。

このフィールドでは、FTP サーバの IP アドレスをグローバルに変更できます。詳細については、「[リモート TFTP または FTP サーバを使用する場合の考慮事項 \(P. 43\)](#)」を参照してください。

注: 属性 DefaultFtpHost はこの値を表します。これは属性エディタで設定できます。

FTP ユーザ名

FTP ユーザ名。

FTP パスワード

FTP パスワード。

デフォルト FTP ディレクトリ

FTP が実行されているパス名。

注: FTP サーバは SpectroSERVER ホスト システム以外のシステムで実行できます。ただし、特定の要件がディレクトリに適用されます。詳細については、「[リモート TFTP または FTP サーバを使用する場合の考慮事項 \(P. 43\)](#)」を参照してください。

ランドスケープ

CA Spectrum ランドスケープ（表示のみ）。

リモート TFTP または FTP サーバを使用する場合の考慮事項

デフォルトで SpectroSERVER を実行しているホスト システムは、TFTP および FTP サーバの両方に使用するホスト システムでもあります。ただし、別のホスト システムで実行されるように TFTP または FTP サーバをセットアップすることができます。

別のホストでグローバルに実行されるように TFTP または FTP サーバをセットアップするには、「[TFTP 設定 \(P. 40\)](#)」および「[FTP サーバの設定 \(P. 41\)](#)」で述べられているデフォルトの [TFTP/FTP ホスト] およびデフォルトの [TFTP/FTP ディレクトリ] フィールドを使用します。また、「[单一デバイスの TFTP または FTP の指定 \(P. 44\)](#)」で説明されたとおりに属性エディタを使用して、ホストのデフォルト値を上書きすることもできます。

注: デバイスによって TFTP および FTP サーバ ホスト システムを上書きできますが、TFTP および FTP のディレクトリ設定はランドスケープ全体に適用されます。

SpectroSERVER が実行されるローカル システムの代わりに TFTP または FTP サーバにリモート ホストを使用する場合、以下の点を考慮します。

- 指定された TFTP および FTP ディレクトリのどちらも、CA Spectrum ホスト システムからローカルでアクセスできる必要があります。
SpectroSERVER を実行するコンピュータで TFTP または FTP サーバのルート ディレクトリを共有します。
 - Unix システムの場合、リモート ディレクトリを読み取り/書き込み nfs マウントを使用してマウントする必要があります。

- パス名を指定する場合、UNC パスのみを使用します。ローカル変数またはローカルにマップされたディレクトリは許可されません。たとえば、ホスト「tftpserver」の共有フォルダ「tftpboot」にアクセスするには、デフォルト TFTP ディレクトリとして UNC パスの ¥¥tftpserver¥tftpboot を指定します。
- Windows システムで、UNC パスはユーザ名およびパスワードを必要としませんが、読み取り/書き込み権限が必要です。
注: マップされたドライブはサポートされないため、ネットワーク ドライブのマッピングおよびユーザ名とパスワードの提供は要件から回避されません。

單一デバイスの TFTP または FTP サーバの指定

以下の手順では、デバイス レベルで TFTP または FTP サーバの個別のホストシステムを指定する方法について説明します。

注: ランドスケープにグローバルに TFTP または FTP ホストを設定するには、「[TFTP 設定 \(P. 40\)](#)」および「[FTP サーバの設定 \(P. 41\)](#)」でそれぞれ説明されたとおりに、デフォルトの [TFTP ホスト] およびデフォルトの [FTP ホスト] フィールドを使用します。デバイスによって TFTP および FTP サーバホストシステムを上書きできますが、TFTP および FTP のディレクトリ設定はランドスケープ全体に適用されます。

次の手順に従ってください:

1. [エクスプローラ] タブで、別のホストシステムで TFTP または FTP サーバを使用するデバイスを選択します。
2. コンテンツ画面で [リスト] タブを選択し、デバイスを選択します。
3. ツールメニューから [ユーティリティ] を選択し、[属性エディタ] を選択します。
属性エディタが表示されます。
4. [ユーザ定義] フォルダを選択し、[追加] をクリックします。
[属性セレクタ] ウィンドウが表示されます。

5. [属性セレクタ] ウィンドウの [フィルタ] フィールドに「host」と入力します。NCM_FTP_Host および NCM_TFTP_Host の属性を選択し、[OK] をクリックします。

これで、これら 2 つの属性が [ユーザ定義] フォルダの下に表示されました。

6. NCM_FTP_Host および NCM_TFTP_Host の両方の属性を選択し、追加矢印をクリックします。

変更できる値が右ペインに表示されます。

7. 各属性を以下の値に変更します。

変更なし

チェックボックスをオフにして、残りのフィールドを有効にします。

IP アドレス

TFTP および FTP プロトコルを実行するホストシステムの IP アドレスを入力します。

注: NAT を使用する場合、パブリック IP アドレスを使用します。

デフォルトとして設定

選択されている場合、新しく作成されたすべてのデバイスがこの値を自動的に継承します。

8. [OK] をクリックします。確認ダイアログボックスが開いたら、[はい] をクリックします。

[属性編集結果] ページに変更の結果が表示されます。

9. [閉じる] をクリックします。

デバイス設定エクスポートの設定を選択

Network Configuration Manager を設定して、履歴のアーカイブ用にデバイス設定をテキストファイルにエクスポートできます。このファイルシステムを CA Spectrum および OneClick の外部で手動で管理する必要があります。

次の手順に従ってください:

1. [エクスプローラ] タブで [設定マネージャ] を選択します。
コンテンツ画面の [情報] タブに、情報および設定が表示されます。
2. 設定のエクスポート サブビューを展開します。
3. [設定のエクスポート] の横にある [設定] をクリックします。デフォルトは「エクスポートしない」です。以下のオプションから 1 つを選択します。

固有の設定のみエクスポート

デバイス設定が以前キャプチャされた設定と異なる場合にのみエクスポートされます。

固有およびグローバル同期設定のエクスポート

デバイス設定が以前キャプチャされた設定、またはグローバル同期にあるものと異なる場合にのみエクスポートされます。たとえば、グローバル同期を毎日実行するように設定した場合、デバイスごとに 1 つのファイルが毎日生成されます。詳細については、「[グローバル同期について \(P. 83\)](#)」を参照してください。

エクスポート設定が [設定のエクスポート] の横に表示されます。

4. [エクスポートディレクトリ] 列で [設定] をクリックします。次に、UNIX (Solaris/Linux) および Windows 用の設定テキストファイルをエクスポートするローカルディレクトリを指定します。エクスポートファイル名は、デバイス名およびタイムスタンプを使って名付けられます。設定テキストファイルをネットワーク共有にエクスポートする場合、ディレクトリに UNC パスを指定します。たとえば、`¥Shared_Server¥Export¥ExportFiles` などです。
5. Enter キーを押します。

エクスポートディレクトリが表示されます。

デバイス ファミリの設定

デバイス ファミリは、Network Configuration Manager とデバイス ファミリ内のデバイスとのインタラクションを設定するための一元的な場所を提供します。デバイス ファミリに対して作成された設定は、ファミリに含まれるすべてのデバイスで有効になります。デバイス ファミリ設定は、ローカル デバイス レベルで上書きすることができます。詳細については、「[单一デバイスを設定してデバイス ファミリ設定を上書き \(P. 54\)](#)」を参照してください。

デバイス ファミリの設定にアクセスするには、[エクスプローラ] タブの [デバイス ファミリ] からデバイス ファミリを選択します。次に、コンテンツ画面で [情報] タブを選択します。デバイス ファミリ設定が表示されます。

拡張ユーティリティを使用して Perl スクリプトを設定することにより、サポートされている Network Configuration Manager の操作についてデバイスとのインタラクションを処理することができます。詳細については、「[Network Configuration Manager の拡張ユーティリティ \(P. 60\)](#)」を参照してください。

デバイス ファミリ一般設定の設定

一般設定サブビューには、設定マネージャの設定が含まれています。設定マネージャでは、デバイス ファミリ全体のタスクを無効にできます。設定マネージャが無効に設定されている場合、Network Configuration Manager の操作は、このデバイス ファミリに含まれるデバイスのいずれにおいても実行されません。

注: デバイス ファミリのいずれかのデバイスで操作を必要とする場合、設定マネージャはローカル デバイス レベルで無効にすることもできます。詳細については、「[单一デバイスを設定してデバイス ファミリ設定を上書き \(P. 54\)](#)」を参照してください。

次の手順に従ってください:

1. 「Network Configuration Manager デバイス ファミリ設定へのアクセス」に説明されているとおりにデバイス ファミリ設定に移動し、一般設定サブビューを開きます。

選択されたデバイス ファミリの一般設定が表示されます。

2. [設定マネージャ] の隣の [設定] をクリックし、デバイス ファミリに対して Network Configuration Manager タスクおよび機能を有効または無効にします。デフォルトでは、Configuration Manager マネージャは有効です。

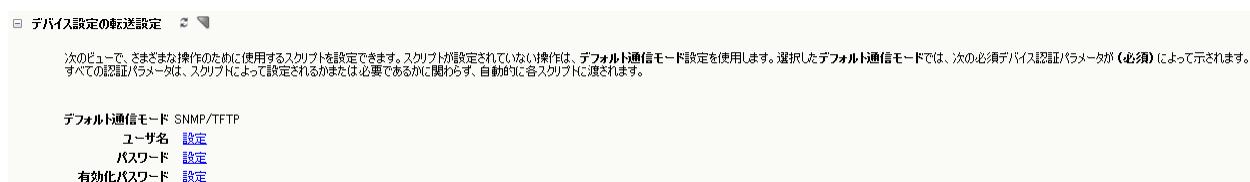
Network Configuration Manager とのデバイス ファミリの通信状態は、設定マネージャの隣に表示されます。

デバイス ファミリ通信モードの設定

標準でサポートされているすべてのデバイス ファミリには通信モードがあり、Network Configuration Manager が関連するデバイスと対話する方法を決定しています。デフォルトでサポートされる一部のデバイス ファミリでは、複数の通信モードから選択できます。選択された通信モードによって、デバイス ユーザ名、パスワード、および有効化パスワードが必要になる場合があります。

同じユーザ名、パスワードおよび有効化パスワードを使用してファミリのどのデバイスにもアクセスできない場合、ローカルデバイス側でユーザ名およびパスワードを上書きできます。詳細については、「[单一デバイスを設定してデバイス ファミリ設定を上書き \(P. 54\)](#)」を参照してください。

以下のイメージには、デバイス設定の転送設定サブビューに表示される、デフォルト通信モード設定が表示されています。



次の手順に従ってください:

1. [エクスプローラ] タブの [デバイス ファミリ] からデバイス ファミリを選択し、コンテンツ画面の [情報] タブを選択します。
デバイス ファミリ設定が表示されます。
2. デバイス設定の転送設定サブビューを展開します。
デバイス ファミリの通信モード設定が表示されます。

3. 選択されたデバイス ファミリにはデフォルト通信モードを選択します。

選択された通信モードが [デフォルト通信モード] の横に表示されます。

4. 必要に応じて、以下のフィールドを変更します。

ユーザ名

デバイスにアクセスするユーザ名を指定します。

パスワード

デバイスにアクセスするためのパスワードを指定します。

パスワードの有効化

デバイス（Cisco IOS、Cisco IOS-SSH Capable および Foundry デバイスのみに対応）の設定に使用する 2 番目のパスワードを指定します。

選択されたデバイス ファミリの通信モードが設定されました。

デバイス ファミリ マスクの設定

デバイス ファミリのマスクは、デバイス設定コンテンツを設定の比較から除外したり、機密情報を権限のないユーザから隠したりするために設定します。マスク設定については、以降のセクションで説明します。

デバイス ファミリ比較マスク

比較マスクは、履歴設定との比較時にデバイス設定コンテンツを隠すための正規表現のリストです。比較マスクの正規表現に一致するデバイス設定ファイルの行は、設定ファイルの比較時に無視されます。 Network Configuration Manager では事前定義済みマスクのリストが提供され、[比較マスク] の隣のウインドウに表示されます。

マスクを追加および削除できます。

マスク設定は、ローカルデバイス レベルで上書きできます。 詳細については、「[单一デバイスを設定してデバイス ファミリ設定を上書き \(P. 54\)](#)」を参照してください。

デバイス ファミリの表示マスクの追加

表示マスクは、デバイス設定ファイル全体を表示する OneClick 権限のないユーザから、デバイス設定コンテンツを隠す正規表現のリストです。マスクされない設定の表示権限は、[表示マスク] フィールドのコンテンツを表示するために必要です。この設定を使用し、権限のないユーザからパスワードまたはその他のコンテンツを隠します。ローカルデバイスレベルで設定されているマスクを上書きできます。

次の手順に従ってください:

1. 比較マスクまたは表示マスクで [追加] を選択します。
[追加] ダイアログ ボックスが表示されます。
2. 選択されたデバイス ファミリのマスクを入力します。たとえば、コメント行の場合は [!#] を入力します。任意の正規表現を入力します。
3. [OK] をクリックします。
マスク用に入力したコンテンツが表示されます。デバイス ファミリのすべてのデバイスにマスクが設定されました。
4. 前の手順を繰り返し、さらにマスクを入力します。

ローカル デバイスでデバイス ファミリ設定を上書きする詳細については、「[デバイス ファミリ設定を上書きする単一デバイスの設定 \(P. 54\)](#)」を参照してください。

マスクの入力

デバイス ファミリ内のすべてのデバイスに適用されるマスクを入力できます。

次の手順に従ってください:

1. 比較マスクまたは表示マスクで [追加] を選択します。
[追加] ダイアログ ボックスが表示されます。
2. 選択されたデバイス ファミリのマスクを入力します。たとえばコメント行の場合は、[#] を入力するか、何らかの正規表現を入力します。
3. [OK] をクリックします。
マスク用に入力したコンテンツが表示されます。これで、デバイス ファミリのすべてのデバイスにマスクが設定されました。

通知トラップ設定の設定

デバイスからのトラップ通知に基づいて自動的にデバイス設定をキャプチャするように、CA Spectrum を設定できます。インストール用にこれらのトラップ設定をカスタマイズできます。デバイスからの設定変更トラップ通知から解析され、ホスト設定テーブルに表示される情報を指定します。Network Configuration Manager ではこれらの設定を使用し、イベントを特定のデバイス用に結合するために設定変更イベント情報を相関させます。

注: 未承諾デバイス設定キャプチャ設定では、デバイスの自動設定キャプチャを制御します。この機能の詳細については、「[デバイス設定変更の未承諾通知 \(P. 25\)](#)」を参照してください。

トラップ形式情報はデバイス ファミリによって異なります。Cisco CatOS、Cisco IOS、Cisco IOS - SSH Capable、および Juniper JUNOS デバイス ファミリには、すぐに使えるサポートが提供されます。以下の例には、Cisco IOS - SSH Capable デバイス ファミリでデフォルトとなる Syslog トラップを表示しています。

```
Configured from {SOURCE} by {USER} on {LOCATION}
Configured from {LOCATION} by {SOURCE}
```

以下の変数は、トラップメッセージから解析され、ホスト設定テーブルに表示される情報を表します。

SOURCE

ホスト設定テーブルの [ソース] 列に対応します。

USER

変更が加えられた際にデバイスでログインしていたユーザを示します。この値はホスト設定テーブルの [デバイス ユーザ] 列に対応します。

LOCATION

ホスト設定テーブルの [場所] 列に対応します。

また、Syslog サーバからのトラップメッセージがデフォルト以外の形式である場合、追加のメッセージ形式を指定することもできます。

デバイス ファミリの設定

以下のイメージでは、テーブルの列を含めて、Cisco IOS - SSH Capable に使用するホスト設定テーブルを示しています。

The screenshot displays two windows from the Network Configuration Manager interface.

The top window shows a table titled "コンテンツ:cis7505-96.11.ca.com - タイプ: Cisco7505". The table lists four hosts with columns for Status, Name, Network Address, Security Domain, Manufacturer, Model Class, MAC Address, Type, and Landscaping. The hosts are categorized by color: green for normal, orange for major, and red for critical.

状態	名前	ネットワーク アドレス	セキュア ドメイン	製造元	モデル クラス	MAC アドレス	タイプ	ランドスケープ
正常	cis7505-96.1..	138.42.94.141	Directly Managed	Cisco Syste..	Switch-Router	00:02:7dd5fb:0:20	Cisco7505	g11n833-v71(0x3200000)
重大	cis7204-96.6..	138.42.94.202	Directly Managed	Cisco Syste..	Switch-Router	00:07:0dbdfc:0:0	Cisco7204V..	g11n833-v71(0x3200000)
正常	newcis7606-..	138.42.94.449	Directly Managed	Cisco Syste..	Switch-Router	00:24:97:2f:05:80	Cisco 7606s	g11n833-v71(0x3200000)
正常	cis7606-96.3..	138.42.94.249	Directly Managed	Cisco Syste..	Switch-Router	00:1cb0:c9:e9:0:0	Cisco 7606s	g11n833-v71(0x3200000)

The bottom window shows a detailed log entry for "コンポーネント詳細:cis7505-96.11.ca.com - タイプ: Cisco7505". The log table has columns for キャプチャ時間, 行変更, 参照, ランニングヒストアップの比較, 最終検証時間, NCM モード, NCM ユーザ, デバイス ユ.., ソース, and 場所. The log details a series of configuration changes made by user "nozhi02" on July 12, 2013, at various times between 2:25:59 and 3:01:08 JST.

キャプチャ時間	行変更	参照	ランニングヒストアップの比較	最終検証時間	NCM モード	NCM ユーザ	デバイス ユ..	ソース	場所
2013/07/12 2:25:59 JST	1	変更内容	差異を表示	2013/07/12 3:01:08 ..SSH	nozhi02	Unknown	Unknown	Unknown	
2013/07/12 2:28:36 JST	1	変更内容		2013/07/12 2:24:44 ..SSH	nozhi02	Unknown	Unknown	Unknown	
2013/07/12 2:21:44 JST	1	変更内容		2013/07/12 2:22:18 ..SSH	nozhi02	Unknown	Unknown	Unknown	
2013/07/12 2:19:19 JST	1	変更内容		2013/07/12 2:20:35 ..SSH	nozhi02	Unknown	Unknown	Unknown	
2013/07/12 2:14:56 JST	2	変更内容		2013/07/12 2:18:04 ..SSH	nozhi02	Unknown	Unknown	Unknown	
2013/07/11 2:37:32 JST	0			2013/07/12 2:13:39 ..					

The log content shows the configuration changes made on July 11, 2013, at 2:37:32 JST, including service timestamps and no service password-encryption settings.

情報は、デバイス トラップ、Syslog のトラップおよびイベント、Network Configuration Manager 内部、および一般変更イベントにマッピングされた他のトラップに基づいて関連しています。 Network Configuration Manager 一般設定の相関イベント期間パラメータは、設定変更イベントが関連している時間を決定します。 詳細については、「[一般設定の設定 \(P. 29\)](#)」を参照してください。

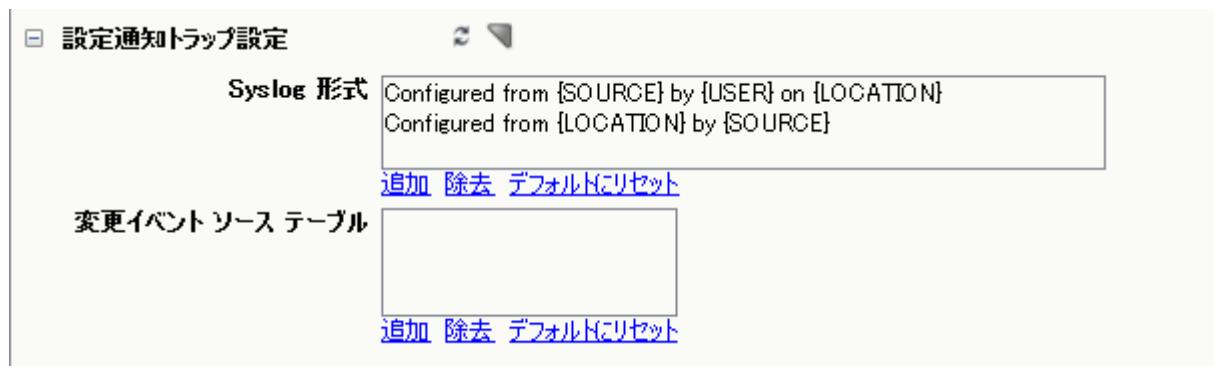
イベント メッセージの詳細については、「[Network Configuration Manager のイベント \(P. 253\)](#)」を参照してください。

デバイス ファミリの通知トラップ設定を設定します。

次の手順に従ってください:

1. 「Network Configuration Manager デバイス ファミリ設定へのアクセス」に説明されているとおりにデバイス ファミリ設定に移動し、設定通知トラップ設定サブビューを展開します。

選択されたデバイス ファミリの設定通知トラップ設定が表示されます。このサブビューは、Syslog サーバから受信するトラップの基本形式で設定されます。以下のイメージでは、Cisco IOS デバイス ファミリのデフォルト設定を示しています。



2. Syslog 形式を追加するには、以下の手順を実行します。
 - a. [Syslog 形式] ボックスの下にある [追加] をクリックします。
[追加] ダイアログ ボックスが表示されます。
 - b. {} 内のメッセージから解析できる列固有の情報でトラップメッセージの形式を入力し、[OK] をクリックします。
新しい Syslog 形式がボックスに追加されます。
3. [変更イベント ソース テーブル] にエントリを追加するには、以下の手順を実行します。
 - a. [変更イベント ソース テーブル] ボックスの下にある [追加] をクリックします。
[追加] ダイアログ ボックスが表示されます。
 - b. [ソース インデックス エントリ] を入力し、[OK] をクリックします。
新しいエントリがテーブルに追加されます。

单一のデバイスの設定によるデバイス ファミリ設定の上書き

このセクションでは、関連するデバイス ファミリの設定が上書きされるように単一のデバイスを設定する方法について説明します。ほとんどのデバイス ファミリ設定は、ローカルデバイス レベルで上書き可能です。

单一のデバイス上の Network Configuration Manager へのアクセス

单一のデバイス用の Network Configuration Manager は、Network Configuration Manager サブビューで利用可能です。

次の手順に従ってください:

1. [エクスプローラ] タブでデバイスを選択します。
コンテンツ画面の [情報] タブに、情報および設定が表示されます。
2. ページを下方向にスクロールし、Network Configuration Manager サブビューを展開します。

Network Configuration Manager のデバイス設定オプションが表示されます。

ここで選択した設定はデバイス ファミリ設定に上書きされます。

单一のデバイスにおける Network Configuration Manager の有効化または無効化

すべての Network Configuration Manager の操作は、ローカルデバイスで無効にすることができます。この設定をデバイスで有効にするには、Network Configuration Manager が関連するデバイス ファミリで有効にされている必要があります。詳細については、「[デバイス ファミリ一般設定の設定 \(P. 47\)](#)」を参照してください。

次の手順に従ってください:

1. 「[单一デバイスの Network Configuration Manager 設定へのアクセス \(P. 54\)](#)」で説明されているように、Network Configuration Manager サブビューを展開します。

Network Configuration Manager のデバイス設定オプションが表示されます。

2. [設定マネージャ] の横にある [設定] をクリックし、Network Configuration Manager のタスクおよび機能を有効または無効にします。
注: Network Configuration Manager はデフォルトで有効です。
Network Configuration Manager との現在の通信状態は、[設定マネージャ] の隣に表示されます。

单一のデバイスでの未承諾デバイス設定キャプチャの設定

未承諾デバイス設定キャプチャは、ローカルデバイスで有効化または無効化できます。

注: このローカル設定を有効にするには、未承諾デバイス設定キャプチャがグローバルに有効化されている必要があります。

詳細については、「[デバイス設定変更の未承諾通知 \(P. 25\)](#)」を参照してください。

次の手順に従ってください:

1. 「[单一デバイスの Network Configuration Manager 設定へのアクセス \(P. 54\)](#)」で説明されているように、Network Configuration Manager サブビューを開きます。
Network Configuration Manager のデバイス設定オプションが表示されます。
2. [未承諾デバイス設定キャプチャ] の横にある [設定] をクリックして、自動デバイス キャプチャを有効または無効にします。
[未承諾デバイス設定キャプチャ] の横に値が表示されます。

単一デバイスの設定変更アラート設定の指定

設定変更アラート設定は、ローカル デバイスで有効化または無効化できます。

次の手順に従ってください:

1. 「[単一デバイスの Network Configuration Manager 設定へのアクセス](#) (P. 54)」で説明されているように、Network Configuration Manager サブビューを展開します。
Network Configuration Manager のデバイス設定オプションが表示されます。
2. ローカル設定変更アラート サブビューを展開します。
ローカル設定変更アラート オプションが表示されます。
3. 「ローカル設定変更アラート設定の使用」の隣の [設定] をクリックし、グローバル設定を上書きします。
値が「ローカル設定変更アラート設定の使用」の隣に表示されます。
4. 必要に応じて、以下の [設定変更アラート] オプションを変更します。

アラート モード

アラームをトリガするイベントを指定できます。

変更時のアラーム

設定変更のみに対してアラームをトリガします。

参照違反時のアラーム

参照設定違反のみに対してアラームをトリガします。

参照違反時または変更時のアラーム

参照設定違反および設定変更の両方に対してアラームをトリガします。

アラームなし

どの設定変更に対してもアラームをトリガしません。

デフォルト： アラームなし

参照違反アラートタイプ

参照設定違反が発生した場合に生成されるアラームまたはイベントのタイプを指定します。既存の比較マスクは、現在の設定と参照設定の大きな違いを確定するために使用されます。現在の設定が参照設定に一致する場合、参照違反アラームは自動的にクリアされます。

参照設定を設定する詳細については、「[参照設定の指定 \(P. 91\)](#)」を参照してください。

有効な値は、重大、メジャー、マイナーのアラームおよびイベントのみです。

デフォルト：イベントのみ

設定変更アラートタイプ

設定変更が発生した場合に生成されるアラームまたはイベントの唯一のタイプを指定します。

有効な値は、重大、メジャー、マイナーのアラームおよびイベントのみです。

デフォルト：イベントのみ

单一のデバイス上での通信モード設定

標準でサポートされているすべてのデバイスに通信モードがあり、Network Configuration Manager がデバイスと対話する方法を決定します。標準でサポートされている一部のデバイスでは、複数の通信モードから選択することができます。選択された通信モードによっては、デバイス ユーザ名、パスワード、および有効化パスワードが必要になる場合があります。

デバイス ファミリの通信モードを設定する詳細については、「[デバイス ファミリ通信モードの設定 \(P. 48\)](#)」を参照してください。

以下は、ローカル通信設定サブビューの例です。

The screenshot shows the 'Local Communication Settings' sub-view. It includes sections for mode selection and authentication. The mode selection section has a note about priority over device family mode settings. The authentication section lists fields for local user name, password, and enable password.

ローカル通信モード設定の使用 無効 設定
ローカルのデフォルト通信モード SNMP/TFTP 設定

ローカル認証設定の使用 無効 設定
ローカル ユーザ名 設定
ローカル パスワード 設定
ローカル有効化パスワード 設定

单一のデバイスで通信モードを設定

次の手順に従ってください:

1. 「[单一デバイスの Network Configuration Manager 設定へのアクセス](#) (P. 54)」で説明されているように、Network Configuration Manager サブビューを展開します。

Network Configuration Manager のデバイス設定オプションが表示されます。

2. ローカル通信設定サブビューを展開します。

ローカル通信設定オプションが表示されます。使用可能なオプションは、デバイスタイプによって異なります。

3. 必要に応じて、以下の [通信設定] オプションを変更します。

ローカル通信モード設定の使用

[ローカルのデフォルト通信モード] でデバイス ファミリ通信モードを上書きするかどうかを指定します。

注: スクリプトがデバイス ファミリ上の操作に設定されている場合、[ローカルのデフォルト通信モード] はその操作に使用されません。

ローカルのデフォルト通信モード

デバイスで複数の通信モードから選択できる場合、通信モードを指定します。

ローカル認証設定の使用

デバイス ファミリ認証設定を上書きするかどうかを指定します。有効な場合、[ローカルユーザ名] および [ローカルパスワード] フィールドに指定された値が使用されます。

ローカル ユーザ名

デバイスにアクセスするユーザ名を指定します。

ローカル パスワード

デバイスにアクセスするためのパスワードを指定します。

ローカル有効化パスワード

デバイス (Cisco IOS、Cisco IOS-SSH Capable および Foundry デバイスのみに対応) の設定に使用する 2 番目のパスワードを指定します。

選択されたデバイスのローカル通信設定オプションが設定されます。

单一のデバイス上でのマスク設定

マスクは、スクリプトの内容を設定の比較から除外したり、機密情報を権限のないユーザから隠したりするために設定します。ローカルデバイスレベルで設定されたマスクにより、そのデバイスが関連するデバイス ファミリのマスク設定が上書きされます。单一のデバイスのマスク設定については、以降のセクションで説明します。

比較マスク

比較マスクは、履歴設定との比較時にデバイス設定コンテンツを隠すための正規表現のリストです。比較マスクの正規表現に一致するデバイス設定ファイルの行は、設定ファイルの比較時に無視されます。Network Configuration Manager では事前定義済みマスクのリストが提供され、[比較マスク] の隣のウィンドウに表示されます。ローカルデバイスのマスクにより、デバイス ファミリのマスク設定が上書きされます。

表示マスク

表示マスクは、デバイス設定ファイル全体を表示する OneClick 権限のないユーザから、デバイス設定コンテンツを隠す正規表現のリストです。[表示マスク] フィールドのコンテンツには、[マスクされない設定の表示] 権限のあるオペレータのみがアクセスできます。マスクを使用し、権限のないユーザからパスワードまたはその他のコンテンツを隠します。ローカルデバイスのマスクにより、デバイス ファミリのマスク設定が上書きされます。

[マスクされない設定の表示] 権限の詳細については、「[Network Configuration Manager 権限 \(P. 265\)](#)」を参照してください。

单一デバイスのマスクを入力

单一のデバイスにマスクを入力できます。

次の手順に従ってください:

1. 「[单一デバイスの Network Configuration Manager 設定へのアクセス \(P. 54\)](#)」で説明されているように、Network Configuration Manager サブビューを展開します。

Network Configuration Manager のデバイス設定オプションが表示されます。

2. ローカルマスク設定サブビューを展開します。
ローカル比較および表示マスク オプションが表示されます。
3. [ローカル比較マスクの使用] または [ローカル表示マスクの使用] の隣の [設定] をクリックし、デバイス ファミリ 設定を上書きします。
値がオプションの隣に表示されます。
4. [比較マスク] または [ローカル表示マスク] で [追加] を選択します。
[追加] ダイアログ ボックスが表示されます。
5. 選択されたデバイスのマスクを入力します。たとえばコメント行の場合は、[!#] を入力するか、何らかの正規表現を入力します。
6. [OK] をクリックしてエントリを適用します。
マスク用に入力したコンテンツが表示されます。これで、選択されたデバイスにマスクが設定されました。
7. さらにマスクを入力するには、手順 4 から手順 6 を繰り返します。

Network Configuration Manager 拡張ユーティリティ

Network Configuration Manager 拡張ユーティリティでは、Network Configuration Manager の基本機能を拡張できます。 Network Configuration Manager がデバイスで実行する操作に Perl スクリプトを使用して、デバイス ファミリを作成し、追加のデバイスおよびベンダーを管理できます。 トランク設定をカスタマイズし、設定変更イベント情報を相関させるために使用できます。

以下のセクションでは、 Network Configuration Manager サポートを拡張するために拡張ユーティリティを使用する方法について説明します。

サポートされている操作

Network Configuration Manager 拡張ユーティリティでは、Perl スクリプトを使用することにより、追加のデバイスおよびベンダーに対して Network Configuration Manager を拡張できます。 Network Configuration Manager の拡張は、Network Configuration Manager がデバイス上で実行する操作に対して Perl スクリプトを提供することによって可能になります。以下のリストでは、これらの操作の概要について説明します。

スタートアップ コンフィギュレーションのキャプチャ

デバイスのスタートアップ コンフィギュレーションをキャプチャします。

ランニング コンフィギュレーションのキャプチャ

デバイスのランニング コンフィギュレーションをキャプチャします。

ランニング コンフィギュレーションのアップロード

指定されたコンテンツをデバイスのランニング コンフィギュレーションにアップロードおよびマージします。

スタートアップ コンフィギュレーションの書き込み

現在のデバイスのランニング コンフィギュレーションを、スタートアップ コンフィギュレーションに書き込みます。

デバイス再ロード

デバイスを再起動します。

再ロード キャンセル

デバイスでスケジュールされた再起動をキャンセルします。

デバイス フームウェアのロード

デバイス上で、指定されたファームウェア イメージのロードを開始します。

スクリプトは、オンデマンドで作成されたデバイス ファミリ内でそれぞれの操作用に設定できます。スクリプトが設定されていない操作はいずれも、任意のデバイス ファミリおよびそれに含まれるすべてのデバイスでサポートされていない操作として処理されます。

Cisco PIX OS の標準デバイス ファミリは、Network Configuration Manager のサポート拡張にスクリプトがどのように使われるかについて例を提供します。（これらの例となるスクリプトでは、Net::Telnet perl モジュールで IPv6 はサポートされていません。）

また、このユーティリティでは Perl のスクリプトを使用し、標準デバイス ファミリに属しているデバイスとの Network Configuration Manager のインタラクションを変更することもできます。

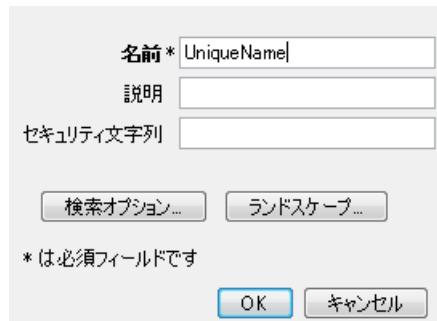
カスタム デバイス ファミリの作成

Network Configuration Manager では、標準で Cisco、Enterasys、Enterasys/Riverstone SSR、Extreme、Foundry、Juniper、Lancom、Nortel Baystack、および Nortel Passport デバイス ファミリをサポートしています。Network Configuration Manager の拡張ユーティリティでは、カスタムのデバイス ファミリを作成できます。

次の手順に従ってください：

1. ナビゲーション画面の [エクスプローラ] タブで設定マネージャを開します。
2. [デバイス ファミリ] を右クリックし、[デバイス ファミリの作成] を選択します。

以下に示すように、[デバイス ファミリの作成] ダイアログ ボックスが表示されます。



3. [名前] フィールドに、固有の名前を入力します。
4. (オプション) 説明およびセキュリティ文字列を入力します。
5. (オプション) [ランドスケープ] ボタンをクリックし、デバイス ファミリを配置するランドスケープを選択します。

6. 特定のデバイスを検索するには、[検索オプション] ボタンをクリックします。

[検索オプション] ダイアログ ボックスが表示されます。デバイス ファミリは、グローバルコレクションと同様に、手動でファミリに追加された静的メンバと、指定された検索条件を使用して自動的に追加された動的メンバの両方を所有することができます。詳細については、「管理者ガイド」を参照してください。

注: 1つのデバイスは、1つのデバイス ファミリのみに所属できます。同じデバイスに適用される検索条件が複数のデバイス ファミリに含まれている場合、最初にその検索を実行したデバイス ファミリにデバイスが含まれます。

7. 完了したら、[OK] をクリックします。

デバイス ファミリが作成され、ナビゲーション画面の [エクスプローラ] タブにある [デバイス ファミリ] に表示されます。これで静的メンバが追加できます。

デバイス ファミリへのデバイスの配置

Network Configuration Manager では、標準でサポートされるデバイスが自動的にファミリに割り当てられます。現在デバイス ファミリに関連付けられているデバイスは、ユーザが作成したデバイス ファミリに手動で移動させる必要があります。メンバシップを定義する検索条件を含む手動で作成されたデバイス ファミリには、デバイス ファミリにすでに属しているデバイスは取り込まれません。検索条件で新しいデバイスを取り込むには、デバイスがどのデバイス ファミリのメンバーにもなっていない状態である必要があります。

デバイス ファミリにデバイスを配置するための複数のオプションがあります。手動で関連付けを作成できます。

次の手順に従ってください:

1. デバイスを見つけます。
2. デバイスを右クリックし、[追加先] から [デバイス ファミリ] を選択します。
[デバイス ファミリの選択] ダイアログ ボックスが表示されます。
3. 選択されたデバイスに関連付けるデバイス ファミリを選択します。

適切なデバイス ファミリが表示されない場合、[作成] をクリックしてカスタムデバイス ファミリを作成します。詳細については、「[カスタムデバイス ファミリの作成 \(P. 62\)](#)」を参照してください。

これでデバイスは選択されたデバイス ファミリに関連付けられます。

定義された検索条件を使用して、手動で作成されたデバイス ファミリを強制的に更新できます。

次の手順に従ってください:

1. ナビゲーション画面のデバイス ファミリを右クリックします。
2. [デバイス ファミリを更新] を選択します。
現在、デバイス ファミリに属していない場合、デバイス ファミリは検索条件に一致するすべてのデバイスを検索し追加します。

デバイス ファミリ検索条件の詳細については、「[カスタムデバイス ファミリの作成 \(P. 62\)](#)」を参照してください。

また、標準でサポートされたデバイス ファミリの 1 つにデバイスをリストアすることもできます。

次の手順に従ってください:

1. 現在、デバイス ファミリに関連付けられていないデバイスを右クリックします。
2. [再設定]、[NCM デバイス ファミリの再評価] を選択します。

重要: Cisco PIX デバイスでは、NCM デバイス ファミリの再評価機能はサポートされていません。

Network Configuration Manager はデバイスを再評価し、すぐに使用できるデバイス ファミリに属する必要があるかを特定します。

配置が適切であることを Network Configuration Manager が特定する場合、デバイスはデバイス ファミリに追加されます。

注: 手動で作成されたデバイス ファミリに存在しているデバイス上の NCM デバイス ファミリの再評価アクションは有効になりません。

標準でサポートされるデバイス ファミリの詳細については、「[サポートされているデバイス \(P. 191\)](#)」を参照してください。

拡張ユーティリティのスクリプト設定

OneClick を使用して、Network Configuration Manager スクリプトでインタラクションをすべて実行します。 Network Configuration Manager では、CA Spectrum 環境内のすべてのスクリプト管理を処理します。 利用可能なスクリプト記述のオプションについては、以降のセクションで説明します。

スクリプト記述の注意事項

Network Configuration Manager の操作用にスクリプトが設定されると、このスクリプトはファミリ内のすべてのデバイスに使用されます。たとえば、スクリプトが Cisco IOS SSH Capable デバイス ファミリでサポートされているすべての操作に設定された場合、デバイス ファミリの通信モード設定およびローカルデバイスで上書きされた通信モードは無効になります。この例では、Cisco IOS SSH Capable デバイス ファミリに含まれるすべてのデバイス上のすべての Network Configuration Manager の操作に対するスクリプトが使用されます。

Network Configuration Manager の操作のサブセットのみに設定されたスクリプトがある場合、Network Configuration Manager では、スクリプトが設定されていない操作にデバイス ファミリで選択、またはローカルデバイスで上書きされた通信モードが使用されます。

ユーザ名、パスワード、および有効化パスワードは、コマンドライン パラメータとして常にスクリプトに送信されます。デバイス ファミリで指定されている値は、ローカルデバイスで上書きされていない限り使用されます。上書きされている場合は、ローカルで上書きされた値が使用されます。

デフォルトのスクリプトコマンド ライン パラメータ

デフォルトでは、Network Configuration Manager は各スクリプトにパラメータを以下に示された順序で提供します。スクリプトでこれらのパラメータが使用されない場合でも、スクリプトはこれらのパラメータを受け入れるように書かれている必要があります。

- デバイス IP。
- アップロードするコンテンツを含むファイルの絶対ファイル名（アップロード操作のみ）。
- デバイス ユーザ名。
- デバイス パスワード。
- デバイス 有効化パスワード。

追加のスクリプトコマンド ライン パラメータ

オプションで、サポートされた操作のそれぞれに、追加のコマンド ライン パラメータを無制限に設定することができます。追加されたパラメータは、コマンド ラインで、デフォルトの一連のパラメータの後にスクリプトに渡されます。これらのパラメータは、「[追加のスクリプト パラメータ]」リスト内に表示されている順序で受け渡されます。

ランニング コンフィギュレーションアップロードおよびデバイス ファームウェアのロード操作では、追加のコマンド ライン パラメータを使用して、実行時にユーザに対して値を確認するプロンプトが表示されるように設定できます。ラベルおよびデフォルト値を実行時のプロンプトで表示することもできます。

エラー コードのマッピング

Network Configuration Manager では、スクリプトによって返されたゼロ以外の整数値をテキスト形式のエラーメッセージにマッピングする機能が提供され、エラーが発生した場合にはそのメッセージが OneClick に表示されます。これによって、スクリプトの作成者は障害モードの詳細情報を提供することができます。

スクリプト エラーの処理

Network Configuration Manager がスクリプトに基づく操作の成功をレポートするには、スクリプトはゼロの値を返す必要があります。スクリプトによりゼロ以外の値が返された場合、Network Configuration Manager では操作が失敗したものと想定されます。

STDERR バッファ内で返される他のエラー詳細

スクリプトがゼロ以外の値を返した場合、上記のエラーマッピングに加えて、Network Configuration Manager では STDERR バッファでスクリプトによって返された出力も検索されます。コンテンツが見つかると、OneClick に追加のエラー情報として表示されます。

設定スクリプトの入力

Network Configuration Manager は、以下の操作に Perl スクリプトを使用できます。

スタートアップ コンフィギュレーションのキャプチャ

このスクリプトでは、STDOUT バッファにデバイスのスタートアップ コンフィギュレーションを返す必要があります。バッファに返されるすべてのコンテンツは、デバイスのスタートアップ コンフィギュレーションであると見なされます。

ランニング コンフィギュレーションのキャプチャ

このスクリプトでは、STDOUT バッファにデバイスのランニング コンフィギュレーションを返す必要があります。バッファに返されるすべてのコンテンツは、デバイスのランニング コンフィギュレーションであると見なされます。

ランニング コンフィギュレーションのアップロード

このスクリプトは、絶対ファイル名パラメータによって識別されるファイルを読み取ります（詳細については、「[デフォルトのスクリプトコマンドラインパラメータ \(P. 66\)](#)」を参照）。その後、ファイルのコンテンツをデバイスのランニング コンフィギュレーションにアップロードおよびマージします。

スタートアップ コンフィギュレーションの書き込み

このスクリプトにより、デバイスのランニング コンフィギュレーションがスタートアップ コンフィギュレーションに書き込まれます。

デバイス再ロード

このスクリプトはデバイスを再起動します。

再ロード キャンセル

このスクリプトは、デバイスで保留中またはスケジュールされた再起動をキャンセルします。

デバイス フームウェアのロード設定

このスクリプトはデバイス上に新しいファームウェアイメージをアップロードし、このファームウェアイメージを使用して、デバイスを再ロードするために必要なすべての操作を実行します。

これらの操作に設定スクリプトを選択できます。

次の手順に従ってください:

1. [エクスプローラ] タブでデバイス ファミリを選択します。
コンテンツ画面の [情報] タブに、情報および設定が表示されます。
2. デバイス設定の転送設定サブビューを開きます。
スクリプト操作サブビューが表示されます。
注: Cisco IOS および Cisco IOS - SSH Capable デバイス ファミリの場合、デバイス フームウェアのロードスクリプトは、デバイス フームウェアの転送設定サブビューに存在します。
3. 適切なスクリプト操作サブビューを開きます。
使用可能なスクリプト設定フィールドが表示されます。

4. スクリプト名の隣の [設定] をクリックします。

[スクリプトの選択] ダイアログ ボックスが、以下の例のように表示されます。

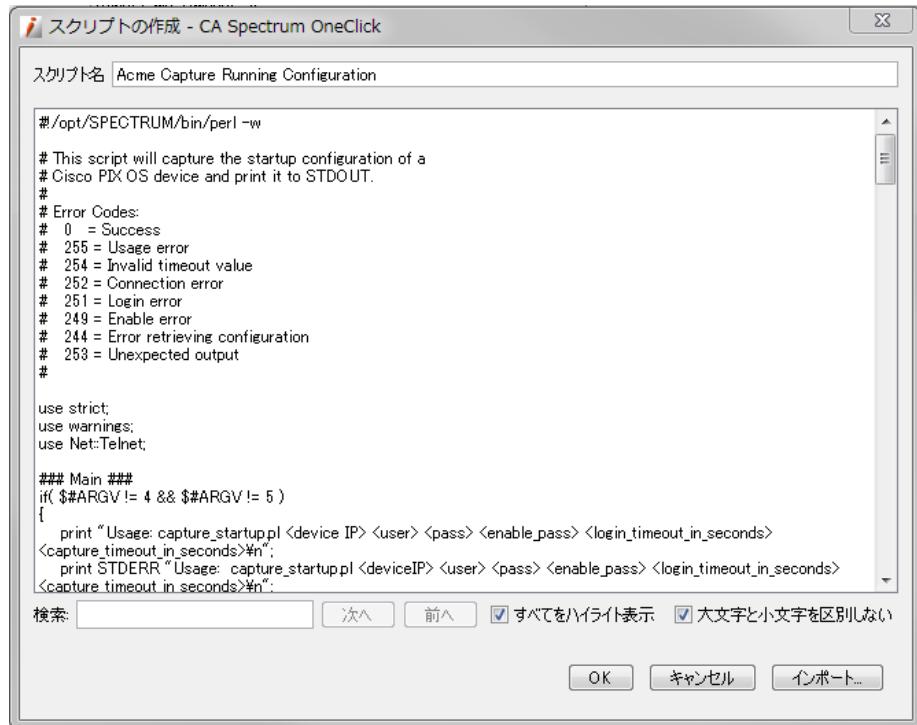


5. 以下のいずれかの手順を実行します。

- 使用するスクリプトが使用可能な場合、スクリプトを選択して [OK] をクリックし、手順 10 に移動します。
- 選択されたデバイス ファミリのスクリプトをまだ作成していない場合、[作成] をクリックしてアップロードまたは作成します。

6. [スクリプト名] フィールドに、スクリプトの一意の名前を入力します。スクリプト名の下のフィールドにスクリプトを貼り付けるか、[インポート] をクリックしてシステムのローカルに保存されている設定ファイルをインポートします。

以下の例のとおり、スクリプトコンテンツが [スクリプト名] フィールドの下のフィールドに表示されます。



7. (オプション) 必要に応じて、スクリプトコンテンツを編集します。または、[検索] フィールドに条件を入力し、スクリプトファイルで特定の行を見つけます。
8. スクリプトのインポートおよび設定が完了したら、[OK] をクリックします。
[スクリプトの選択] ダイアログ ボックスにスクリプト名が表示されます。
9. スクリプトを選択し、[OK] をクリックします。
スクリプトがロードされ、[スクリプトの内容] フィールドに表示されます。
10. その他のスクリプトパラメータを追加します。

注: 詳細については、「[追加のスクリプトコマンドラインパラメータ \(P. 66\)](#)」を参照してください。

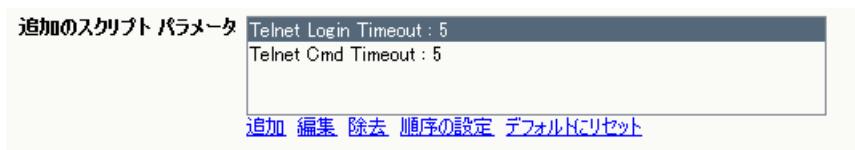
11. [追加のスクリプトパラメータ] フィールドの下にある、[追加] をクリックします。

[追加] ダイアログボックスが表示されます。

- パラメータ名および値を入力します。操作が [アップロード]、またはタスクが [ファームウェアのロード] である場合、パラメータを設定して実行時に値を確認するプロンプトを表示させることができます。

- [OK] をクリックします。

以下の例のとおり、パラメータが [追加のスクリプトパラメータ] フィールドに表示されます。



12. エラー コードのマッピングを追加します。詳細については、「[エラー コードのマッピング \(P. 67\)](#)」を参照してください。

13. [エラー コードのマッピング] フィールドの下にある、[追加] をクリックします。

[追加] ダイアログボックスが表示されます。

14. [エラー コード] フィールドにエラー コード、および [エラーメッセージ] フィールドに対応するメッセージを入力し、[OK] をクリックします。

以下の例のとおり、エラー コードが [エラー コードのマッピング] フィールドに表示されます。

エラー コードのマッピング	
255	→ Usage error
254	→ Invalid timeout value
252	→ Connection error
251	→ Login error
249	→ Enable error
追加 編集 除去	

これで設定スクリプトを実行できます。

Perl モジュール

CA Spectrum には標準で提供される Perl スクリプトを実行するのに必要なすべての Perl モジュール (Windows/Solaris プラットフォーム用) が付属しています。以下に示します。

- Net::Telnet

さらに CA Spectrum には、拡張ユーティリティ用にスクリプトを開発するのに役立つ可能性のある Perl モジュールも付属しています。該当するスイッチを以下に示します。

- Net::SSH
- Net::SSH::Expect
- Expect
- Net::TFTP
- Net::SCP
- Net::FTP

CA Spectrum に付属の Perl モジュールは以下で確認できます。

/opt/SPECTRUM/lib/perl5

重要: Perl モジュールが正常にコンパイルおよびインストールされていない場合、エラーまたはその他の望ましくない動作が発生する可能性があります。

SSH ベースの Perl スクリプトを Network Configuration Manager の操作に使用

Network Configuration Manager の操作に使用する CA Spectrum で標準のスクリプトベースのサポートは、Net::Telnet モジュールに基づいています。SSH ベースのスクリプトを Network Configuration Manager の操作に使用する場合

- **Windows および Solaris -** CA Spectrum には完全な Perl インストールおよび Net::SSH::Expect モジュールが含まれています。
- **Linux -** システムの個別の場所に Perl をインストールし、Perl を使用するため CA Spectrum を設定する必要があります。

この Perl のインストールおよび CA Spectrum での設定は、DSS のランドスケープごとに行う必要があります。SSH ベースのスクリプトを使用するようモデリングされたデバイスのある各ランドスケープで、Perl をセットアップする必要があります。

注: カスタム Perl インストールを使用すると CA Spectrum で設定してから、CA Spectrum の標準スクリプトを継続して使用する場合、カスタム Perl 領域に Net::Telnet perl モジュールをインストールする必要があります。このモジュールは www.cpan.org からダウンロードおよびインストールできます。そうでない場合、CA Spectrum の標準スクリプトは失敗します。

SSH ベースのスクリプトをセットアップするには、プラットフォームに固有の手順に従います。

Windows の場合

1. Perl をインストールします。

CA Spectrum には Cygwin の完全な Perl のバージョンが付属しているため、Net::SSH::Expect モジュールに基づくスクリプトを使用する場合、さらにインストールする必要はありません。

他のモジュールに基づくスクリプトを使用する場合、使用しているモジュールに応じて、以下のいずれかを完了します。

- Perl モジュールが Cygwin 以外に Perl のバージョンと互換性のある場合、SpectroSERVER マシン上に特定の Perl をインストールして、特定の Perl モジュールをインストールし、特定の Perl インストールを使用するために CA Spectrum を設定することをお勧めします。
(「[カスタム Perl インストールを使用する CA Spectrum の設定 \(P. 76\)](#)」を参照してください)
- インストールする Perl モジュールが Cygwin の Perl のみと互換性があり、それが変更モジュール（つまり、C ライブラリのコンパイルが不要）である場合、CA Spectrum の Perl インストールに追加できます。<Module_Name>.pm ファイルを \$SPECROOT/NT-Tools/SRE/lib/perl5/site_perl/5.8 に配置するだけです。
- インストールする Perl モジュールが Cygwin の Perl のみと互換性があり、C ライブラリのコンパイルが必要な場合、このモジュールはコンパイルされ、CA Spectrum に付属している必要があります。この拡張機能要求については、CA Spectrum サポートに連絡してください。

2. SSH ベースの Perl モジュールおよび SSH プログラムをインストールします。

CA Spectrum には、Net::SSH::Expect (およびそれに必要な) モジュールおよび ssh プログラム (Net::SSH::Expect に必要) が付属しています。このモジュールを使用してスクリプトを開発する方法の手順については、www.cpan.org にある Net::SSH::Expect のドキュメントを確認してください。

3. カスタム Perl インストールを使用するために CA Spectrum を設定します。

CA Spectrum の Perl はこの目的でセットアップされるため、カスタム Perl インストールを使用するために CA Spectrum を設定する必要はありません。

Solaris の場合

Solaris 上の CA Spectrum には、上述の Perl のモジュールが付属しています。CA Spectrum に付属しているもの以外の Perl モジュールを使用するには、カスタム領域に Perl をインストールする必要があります。

1. Perl をインストールします。

Perl は Solaris のさまざまなバージョンで使用可能です。Sun Freeware (www.sunfreeware.com) から特定の Solaris バージョン用にコンパイルされた Perl をダウンロードできます。Perl v5.8.8 はテストされています。Net::SSH::Expect perl モジュールと互換性があります。

注: SunOS には自身のバージョンの Perl (v5.005) を付属している可能性があります。しかし、通信に必要な一部のモジュールと非互換性問題が発生する可能性があるため、このバージョンを Network Configuration Manager スクリプト用に使用することは推奨されません。

2. SSH ベースの Perl モジュールおよび SSH プログラムをインストールします。

Net::SSH::Expect モジュールを使用する場合、必要な操作は ssh プログラムをセットアップするだけです。

Net::SSH::Expect モジュールには、ssh ユーティリティがインストールされていることが必要です。システムにユーティリティが含まれていない場合、OpenSSH パッケージをインストールすることにより www.sunfreeware.com からダウンロードおよびインストールすることができます。

追加のモジュールを使用する場合、www.cpan.org からダウンロードできます。

必ず上記でインストールしたカスタム Perl の領域にこれらのモジュールをインストールします。

以下のようにモジュールをインストールしている場合、Perl バイナリのフルパスを指定することでこれを実行できます。

```
<PERL_FULL_PATH>/perl Makefile.pl
```

注: 一部の Perl モジュールは C/C++ コード ライブラリに依存します。このようなモジュールをインストールするには、ライブラリにリンクできるように gcc コンパイラをインストールする必要があります。これも www.sunfreeware.com から取得できます。

3. カスタム Perl インストールを使用するために CA Spectrum を設定します。

「[カスタム Perl インストールを使用する CA Spectrum の設定 \(P. 76\)](#)」を参照して、上記の手順 1 で Perl をインストールした領域を CA Spectrum で指し示します。

Linux の場合

1. Perl をインストールします。

OS にはすでに Perl がインストールされています (/usr/bin/ を確認します)。この事前にインストールされた Perl は、Network Configuration Manager のスクリプトに使用できます。

2. SSH ベースの Perl モジュールおよび SSH プログラムをインストールします。

Net::SSH::Expect モジュール、依存するモジュール、および ssh ユーティリティをダウンロードおよびインストールする必要があります。

Net::SSH::Expect の依存関係ツリーは以下のとおりです。

Net::SSH::Expect -> Expect -> IO::Pty

ここで「->」は「必要とする」関係を表します。

www.cpan.org からこれらのモジュールをすべてダウンロードできます。

必ず上記でインストールしたカスタム Perl の領域にこれらのモジュールをインストールします。

以下のようにモジュールをインストールしている場合、Perl バイナリのフルパスを指定することでこれを実行できます。

```
<PERL_FULL_PATH>/perl Makefile.pl
```

注: 一部の Perl モジュールは C/C++ コードライブラリに依存します。このようなモジュールをインストールするには、ライブラリにリンクできるように gcc コンパイラをインストールする必要があります。最新の gcc パッケージを追加するために rpm を使用して、gcc コンパイラをインストールできます。

3. カスタム Perl インストールを使用するために CA Spectrum を設定します。

「[カスタム Perl インストールを使用する CA Spectrum の設定 \(P. 76\)](#)」を参照して、上記の手順 1 で Perl をインストールした領域を CA Spectrum で指し示します。

カスタム Perl インストールを使用する CA Spectrum の設定

デフォルトでは、CA Spectrum は付属の Perl を使用するように設定されています。CA Spectrum に付属されていない追加の Perl モジュールを Perl 領域にインストールしており、それを使用する場合、カスタム Perl インストールを使用するために CA Spectrum を設定できます。これをセットアップするには、OneClick の [エクスプローラ] タブで設定マネージャ モデルをクリックします。情報ビューで、Perl 設定サブビューを開きます。ランドスケープごとに Perl ディレクトリ設定に含まれるテーブルを検索します。

カスタム Perl ディレクトリを指定するには、[カスタム Perl を使用] オプションを有効にする必要があります。それを行わないと、CA Spectrum に付属しているデフォルト Perl が使用されます。特定の SpectroSERVER システムでインストールしたカスタム Perl の場所に CA Spectrum を指定できます。

次の手順に従ってください:

1. 指定のランドスケープで、[カスタム Perl を使用] を有効に設定します。
2. カスタム Perl の領域の使用を有効にすると、カスタム Perl ディレクトリを指定します。

注: カスタム Perl のディレクトリには、perl.exe (Windows) または Perl プログラム (Solaris/Linux) が含まれるディレクトリのフルパス名が含まれている必要があります。

たとえば、Perl プログラムが /usr/local/bin/ に配置されている場合、カスタム Perl ディレクトリを /usr/local/bin/ として指定する必要があります。

注: カスタム Perl のインストールを使用するために CA Spectrum を設定すると、CA Spectrum デフォルトスクリプトを使用することを続行できます。しかし、カスタム Perl の領域には Net::Telnet Perl モジュールがインストールされている必要があります。このモジュールは www.cpan.org からダウンロードおよびインストールできます。それを行わないと、CA Spectrum デフォルトスクリプトは失敗します。

カスタム Perl 領域の使用を無効にし、デフォルトの CA Spectrum Perl を使用できます。

[カスタム Perl を使用] を無効 (CA Spectrum のデフォルトを使用) に設定します。カスタム Perl 領域の使用を無効にした場合、カスタム Perl ディレクトリを表示または編集することはできません。ただし、[カスタム Perl を使用] を再度有効にした場合、以前に指定したカスタム Perl ディレクトリがリストアされます。

追加の Perl モジュールの使用

優先の Perl モジュールに基づくスクリプトを使用する場合、使用される領域に Perl モジュールをインストールする必要があります。

Windows の場合

使用するモジュールによって 3 つのオプションがあります。

- Perl モジュールが Cygwin 以外に Perl のバージョンと互換性のある場合、SpectroSERVER マシン上に特定の Perl をインストールして、特定の Perl モジュールをインストールし、特定の Perl インストールを使用するため CA Spectrum を設定することをお勧めします。（「[カスタム Perl インストールを使用する CA Spectrum の設定 \(P. 76\)](#)」を参照してください）。
- インストールする Perl モジュールが Cygwin の Perl のみと互換性があり、それがテキストベースのモジュール（つまり、C ライブラリのコンパイルが不要）である場合、CA Spectrum の Perl インストールに追加できます。 <Module_Name>.pm ファイルを \$SPECROOT/NT-Tools/SRE/lib/perl5/site_perl/5.8 に配置するだけです。

- インストールする Perl モジュールが Cygwin の Perl のみと互換性があり、C ライブラリのコンパイルが必要な場合、このモジュールはコンパイルされ、CA Spectrum に付属している必要があります。この拡張機能要求については、CA Spectrum サポートに連絡してください。

Solaris および Linux の場合

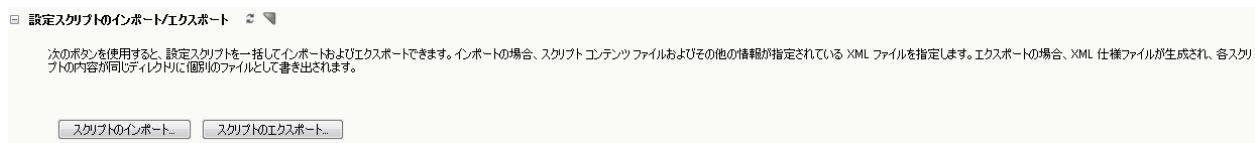
SpectroSERVER に個別の領域に Perl をインストールし、その Perl を使用して必要な Perl モジュールをインストールし、Perl インストール領域を使用するために CA Spectrum を設定する必要があります。Perl をインストールすると、インストールする特定の Perl モジュールのインストール手順を参照してください。その後、「[カスタム Perl インストールを使用する CA Spectrum の設定 \(P. 76\)](#)」を参照してください。Net::SSH::Expect モジュールに基づくスクリプトを使用する方法の詳細については、「[Network Configuration Manager 操作に使用する SSH ベースの Perl スクリプトの使用 \(P. 72\)](#)」を参照する可能性があります。ただし、任意の Perl モジュールを統合するガイドラインとして手順を使用する場合があります。

スクリプトのインポートおよびエクスポート

Network Configuration Manager では、スクリプトを一括してインポートおよびエクスポートできます。スクリプトは、OneClick クライアントを実行しているホストサーバのファイルシステムにエクスポート、またはファイルシステムからインポートされます。

スクリプトをエクスポートするには、以下の手順を実行します。

1. ナビゲーション画面で [設定マネージャ] を選択します。
2. コンテンツ画面で [情報] タブを選択します。
情報および設定が表示されます。
3. 設定スクリプトのインポート/エクスポート サブビューを展開します。
[スクリプトのインポート] ボタンおよび [スクリプトのエクスポート] ボタンが表示されます。



4. [スクリプトのエクスポート] をクリックします。
[エクスポートするスクリプトの選択] ダイアログ ボックスが表示されます。
5. エクスポートされるスクリプトを選択します。または、複数のスクリプトを選択します。
[名前を付けて保存] ダイアログ ボックスが表示されます。
6. 保存する場所を選択し、エクスポート時に自動的に生成される XML 仕様ファイルの名前を入力します。エクスポート処理では、指定された名前および拡張子 .pl を使用して、選択された各 Perl スクリプトにファイルが生成されます。またエクスポート処理では、エクスポートされたスクリプトのリストおよびそれぞれのエラーマッピング情報を含む XML 仕様ファイルも生成されます。その後、この XML 仕様ファイルは、同じまたは異なる CA Spectrum 環境上でスクリプトをインポートするのに使用できます。

選択された Perl スクリプトは、指定した場所にエクスポートされます。

スクリプトをインポートするには、以下の手順を実行します。

1. ナビゲーション画面で [設定マネージャ] を選択します。
2. コンテンツ画面で [情報] タブをクリックします。
情報および設定が表示されます。
3. 設定スクリプトのインポート/エクスポート サブビューを展開します。
[スクリプトのインポート] ボタンおよび [スクリプトのエクスポート] ボタンが表示されます。
4. [スクリプトのインポート] をクリックします。
[開く] ダイアログ ボックスが開きます。
5. Network Configuration Manager にインポートされる Perl スクリプトを記述する XML 仕様ファイルを選択します。事前に CA Spectrum からエクスポートされたスクリプトをインポートしている場合、エクスポート時に生成された XML 仕様ファイルを使用できます。

また XML 仕様ファイルは、以下の例に示されるフォーマットに従って手動で生成することもできます。

```
<scripts>
  <script>
    <file-name>ABC_Vendor_Capture_Running_Configuration.pl</file-name>
    <display-name>ABC ベンダー キャプチャ ランニング コンフィギュレーション
  </display-name>
    <error-message errorCode="255">使用方法</error-message>
    <error-message errorCode="99">無効な有効化パスワード</error-message>
    <error-message errorCode="98">予期しないレスポンス</error-message>
    <error-message errorCode="97">無効な Telnet タイムアウト値</error-message>
  </script>
  <script>
    <file-name>XYZ_Vendor_Capture_Running_Configuration.pl</file-name>
    <display-name>XYZ ベンダー キャプチャ ランニング コンフィギュレーション
  </display-name>
    <error-message errorCode="255">使用方法</error-message>
    <error-message errorCode="99">レスポンスのタイム アウト</error-message>
    <error-message errorCode="50">接続エラー</error-message>
  </script>
  <script>
    <file-name>XYZ_Vendor_Capture_Startup_Configuration.pl</file-name>
    <display-name>XYZ ベンダー キャプチャ スタートアップ コンフィギュレーション
  </display-name>
  </script>
</scripts>
```

file-name

インポートされる Perl ファイルの名前。インポート時に、XML 仕様ファイルと同じディレクトリにファイルが置かれている必要があります。

display-name

このスクリプトを識別するために OneClick で使用される名前。

error-message

(オプション) エラーが発生する場合、スクリプトによって OneClick に表示されるエラーメッセージに返されるエラー コード のマッピングを示します。それぞれのスクリプトに複数のエラーメッセージ エレメントを指定することができます。

Perl スクリプト XML がインポートされました。デバイス ファミリで Network Configuration Manager の操作を設定すると、スクリプトが利用可能になります。

注: インポート処理では、スクリプトとデバイス ファミリの関連付けは行われません。

スクリプトのバックアップおよび履歴の管理

スクリプトは CA Spectrum データベースにモデルとして格納されているため、CA Spectrum でバックアップが実行されるたびにバックアップされます。スクリプトのエクスポート機能により、Network Configuration Manager のスクリプトの追加バックアップおよび履歴の追跡手段が提供されます。これにより、容易にアクセスし、必要に応じて CA Spectrum にインポートして戻すことができます。

カスタマイズされたトラップ

インストール用にカスタマイズされたトラップ設定を設定して、Network Configuration Manager の機能を拡張できます。これらの設定を使用し、イベントを特定のデバイス用に結合するために設定変更イベント情報を相關させます。これらの設定はデバイス ファミリ レベルで設定されます。詳細については、「[設定通知トラップ設定 \(P. 51\)](#)」を参照してください。

第3章：グローバル同期タスク

この章では、Network Configuration Manager を使用して、ネットワーク上でグローバル同期タスクを設定する方法について説明します。グローバル同期タスクの実行時に、Network Configuration Manager によりすべてのデバイス設定がキャプチャおよび保存されます。

注: Network Configuration Manager のポリシーを設定する前に、デバイス設定をキャプチャしておくことをお勧めします。

このセクションには、以下のトピックが含まれています。

- [グローバル同期について \(P. 83\)](#)
- [グローバル同期の設定 \(P. 84\)](#)
- [グローバル同期のスケジュール \(P. 85\)](#)
- [オンデマンド グローバル同期タスクの実行 \(P. 87\)](#)
- [単一デバイスの設定履歴の表示 \(P. 87\)](#)
- [2つの設定の比較 \(P. 90\)](#)
- [参照設定の指定 \(P. 91\)](#)
- [設定アラーム \(P. 92\)](#)
- [グローバル同期タスク結果の表示 \(P. 94\)](#)
- [Report Manager からの Network Configuration Manager レポート \(P. 94\)](#)

グローバル同期について

[グローバル同期] タスクでは、Network Configuration Manager を有効にしたネットワーク上のデバイス用のランニング コンフィギュレーションが収集されます。このタスクが定期的に実行されるようにスケジュールできます。ネットワーク全体にわたりサポートされているすべてのデバイスから設定をキャプチャする期間および頻度を選択できます。たとえば、毎日午後 9 時から午前 5 時までの間にデバイス設定をキャプチャする、などです。ネットワーク上のすべてのデバイスの設定をキャプチャすることによって、ランニング コンフィギュレーションの履歴を管理できます。

グローバル同期を設定して、スタートアップコンフィギュレーションがランニングコンフィギュレーションと同じであるかどうかを確認できます。これらの設定が異なる場合にアラームを生成するように Network Configuration Manager を設定できます。グローバル同期はスタートアップコンフィギュレーションをキャプチャし、ランニングコンフィギュレーションと比較して変更箇所を検出します。スタートアップおよびランニングのコンフィギュレーションの説明については、「[コンフィギュレーションのタイプ \(P. 16\)](#)」を参照してください。

注: また、ネットワーク上で選択されたデバイスのランニングコンフィギュレーションを収集し、自動同期タスクを作成して結果をリアルタイムで表示することもできます。詳細については、「[同期タスクの作成 \(P. 109\)](#)」を参照してください。

Enterasys/Riverstone SSR デバイスについて

Enterasys/Riverstone SSR デバイス上で実行された設定キャプチャでは、ランニングコンフィギュレーションではなくスタートアップコンフィギュレーションが取得されます。そのため、Network Configuration Manager によって管理されているデバイス設定履歴は、SSR デバイス上のスタートアップコンフィギュレーションの履歴です。SSR デバイスが Network Configuration Manager の設定アップロードを処理する方法の詳細については、「[Enterasys/Riverstone SSR デバイスによるアップロードタスクへの応答方法の決定 \(P. 108\)](#)」を参照してください。

グローバル同期の設定

スケジュールなどのグローバル同期の設定を設定します。グローバル同期は、[エクスプローラ] タブのタスクの下に表示されるグローバル同期タスクによって実行されます。

次の手順に従ってください:

1. [エクスプローラ] タブで [設定マネージャ] を選択します。
コンテンツ画面の [情報] タブに、情報および設定が表示されます。
2. グローバル同期サブビューを展開します。
グローバル同期オプションが表示されます。

- 必要に応じて、以下のオプションを変更します。

グローバル同期スケジュール

グローバル同期タスクのスケジュールを指定します。[スケジュール] ボタンをクリックし、デフォルトスケジュールを選択またはカスタムスケジュールを作成する [スケジュールの選択] ダイアログボックスにアクセスします。グローバル同期タスクをスケジュールする詳細については、「[グローバル同期のスケジュール \(P. 85\)](#)」を参照してください。

同期タスクが割り当て時間内に完了しなかった場合、タスクアラームを生成

グローバル同期タスクが正しく完了しなかった場合、アラームによって通知されるマイナー、メジャー、または重大アラームを指定します。多くのデバイスを管理し、スケジュールされたグローバル同期を定期的に実行している場合、同期タスクはスケジュールされた期間の終わりに停止します。これは設定のキャプチャにより低速リンクの帯域幅が消費されるためです。

NCM が無効になったデバイスとデバイス ファミリを含める

[失敗デバイスリスト] に Network Configuration Manager が無効になったデバイスを含めるかどうかを指定します。

デフォルト：はい

スタートアップとランニングのコンフィギュレーションが等しいことを検証

ネットワークのデバイスのスタートアップ コンフィギュレーションと現在のランニング コンフィギュレーションを比較する場合、このオプションを有効にします。

スタートアップ コンフィギュレーションが異なる場合、デバイスアラームを生成

ランニング コンフィギュレーションと異なるスタートアップ コンフィギュレーションを持ったデバイス用のアラームを生成する場合は、マイナー、メジャー、または重大アラームを指定します。

グローバル同期のスケジュール

グローバル同期をスケジュールして、ネットワーク上にあるすべてのデバイス用のランニング コンフィギュレーションを自動的に収集できます。デバイスはランダムな順序で処理されます。

スケジュールされたグローバル同期が割り当て時間内に完了しない場合、次回の実行時に、前回処理されなかったデバイスからランダムに処理が開始されます。次に、残りのすべてのデバイスがランダムな順序で処理されます。

重要: CA Spectrum ランドスケープが複数のタイムゾーンに存在する場合、「1回限り」のグローバル同期をスケジュールしないでください。このタイプのタスクを実行すると、最も早いタイムゾーンのみでグローバル同期が実行されます。

次の手順に従ってください:

1. エクスプローラで、タスク フォルダ内のグローバル同期タスクを選択します。
2. コンテンツ画面で [リスト] タブを選択します。
3. ツールバーの [スケジュール] ボタンをクリックします。
[スケジュールの作成] ダイアログ ボックスが表示されます。
4. 以下のいずれかの手順を実行します。
 - デフォルト スケジュールを選択して、[OK] をクリックします。
 - カスタム スケジュールを作成します。 [作成] をクリックし、スケジュールのオプションを指定して [OK] をクリックします。

カスタム スケジュールは使用可能なスケジュールのリストに追加されます。新しいスケジュールを選択して、[OK] をクリックします。

グローバル同期タスクがスケジュールされました。スケジュールがリストテーブルの [スケジュール] 列に表示され、[スケジュール] アイコンがタスク フォルダのタスクの隣に表示されます。

オンデマンド グローバル同期タスクの実行

グローバル同期タスクを実行して、ネットワーク上にあるすべてのデバイス用のランニング コンフィギュレーションを収集します。デバイスはランダムな順序で処理されます。

次の手順に従ってください:

1. エクスプローラで、タスク フォルダ内のグローバル同期タスクを選択します。
2. コンテンツ画面で [リスト] タブを選択します。
3. [選択したタスクの開始] アイコンをクリックします。

[同期タスク結果] ダイアログ ボックスには、処理されたデバイスおよびグローバル同期の結果のリストが示されます。

単一デバイスの設定履歴の表示

OneClick で单一のデバイスの設定履歴を表示することができます。ネットワーク デバイスに設定をアップロードする詳細については、「[单一のデバイスへの設定を手動アップロード \(P. 100\)](#)」を参照してください。

次の手順に従ってください:

1. [エクスプローラ] タブでデバイスを選択します。
2. コンテンツ画面で [リスト] タブが選択されていることを確認し、コンポーネント詳細画面で [ホスト設定] タブを選択します。

以下の詳細がホスト設定テーブルに表示されます。

キャプチャ時間

デバイスでこの行の設定が最初にキャプチャされた時刻 (M-DD-YYY HH:MM:SS) がリストされます。

キャプチャ実行者

タスクを設定する CA Spectrum OneClick ユーザを示します。

行変更

デバイス上の以前の設定と比較する場合、関連する変更行の数がリストされます。関連する変更には行の追加、行の削除、行の変更が含まれます。無関係の変更は比較マスクに一致するすべての行です。比較マスクはデバイスファミリ用のマスク設定で管理されます。詳細については、「[デバイスファミリマスクの設定 \(P. 49\)](#)」を参照してください。

行変更の合計

デバイス上の以前の設定と比較し、変更された行（関連および無関係）の合計数がリストされます。変更が検出された場合、変更のハイパーリンクが表示されます。

参照

このデバイス用の参照設定を示します。

ランニングとスタートアップの比較

スタートアップおよびランニングのコンフィギュレーションファイルの設定の差異が表示されます（該当する場合）。差異が存在する場合、[差異を表示] ハイパーリンクが表示されます。

最終検証時間

デバイス上にその設定が存在していることを Network Configuration Manager が最後に検証した時刻（M-DD-YYY HH:MM:SS）がリストされます。

最終検証ユーザ

デバイスにアクセスした最後のユーザを示します。

NCM モード

変更が Network Configuration Manager で開始された場合、デバイスに新しい設定コンテンツを転送するのに使用されるメソッドを示します。

NCM ユーザ

Network Configuration Manager を使用して、デバイスで設定変更を開始した CA Spectrum ユーザを示します。

デバイス ユーザ

デバイスにアクセスし、設定変更を作成したユーザを示します。

ソース

設定変更のソースを識別します。

場所

設定変更の場所を識別します。

違反ポリシー

この設定変更の後に違反していたポリシーを示します。

準拠ポリシー

この設定変更の後に準拠していたポリシーを示します。

Network Configuration Manager によって 1 つまたは複数の変更が検出されると、新しい列が作成されます。

- ホスト設定テーブルの行を選択します。

キャプチャされたホスト設定コンテンツが、テーブルの下にあるボックスに表示されます。

- (オプション) ホスト設定テーブルの [行変更] 列で (該当する場合) 変更のハイパーキークをクリックし、選択されたデバイスの設定に追加、削除および変更された行、および無関係の行を表示します。

[設定の差異] ダイアログボックスが表示されます。強調表示されたテキストは、以下の色を使用してステータスを示します。

- 緑 - 追加された行を表します。
- 赤 - 削除された行を表します。
- 青 - 変更された行を表します。
- 灰色 - 無関係な行を表します。無関係の変更は比較マスクに一致する行です。

注: [次へ] または [前へ] をクリックし、ファイル内の差異を移動します。

5. (オプション) ホスト設定テーブルの [ランニングとスタートアップの比較] 列で (該当する場合) [差異の表示] ハイパーリンクをクリックし、追加、削除および変更された行、および無関係の行を表示します。

[ランニングとスタートアップの比較] ダイアログ ボックスには、キャプチャされたデバイスのランニング コンフィギュレーション ファイルとスタートアップ コンフィギュレーション ファイルの差異が示されます。スタートアップ コンフィギュレーションは右側の列に表示されます。強調表示されたテキストは、前の手順でリストされた色を使用してステータスを示します。

2つの設定の比較

異なるデバイスに属していても、2つのあらゆるホスト設定を比較できます。

次の手順に従ってください:

1. [エクスプローラ] タブでデバイスを選択します。
2. コンテンツ画面で [リスト] タブが選択されていることを確認し、コンポーネント詳細画面で [ホスト設定] を選択します。
3. 比較するホスト設定テーブルの設定を右クリックし、[比較の開始] を選択します。
4. 比較に含める2番目の設定を選択します。同じデバイス用の設定を選択するか、または [エクスプローラ] タブで別のデバイスを選択します。その設定情報がホスト設定テーブルに表示されることを確認します。

5. ホスト設定テーブル内の比較に含める 2 番目の設定を右クリックし、[<name_of_first_configuration> と比較] を選択します。
[設定の差異] ダイアログボックスが表示されます。強調表示されたテキストは、以下の色を使用してステータスを示します。
 - 緑 - 追加された行を表します。
 - 赤 - 削除された行を表します。
 - 青 - 変更された行を表します。
 - 灰色 - 無関係な行を表します。無関係の変更は比較マスクに一致する行です。

注: [次へ] または [前へ] をクリックし、ファイル内の差異を移動します。

参照設定の指定

関連するアラームを持ったデバイス用の参照設定を指定できます。現在の設定が参照と大きく異なると Network Configuration Manager が判断するたびに、デバイスでアラームが生成されます。

注: アラーム設定の詳細については、「[設定変更アラートの設定 \(P. 32\)](#)」を参照してください。

次の手順に従ってください:

1. [エクスプローラ] タブでデバイスまたはデバイス ファミリを選択します。
コンテンツ画面で [リスト] タブが選択されていることを確認します。
 2. 参照としてその最新の設定を設定した [リスト] タブで 1 つ以上のデバイスを選択します。
 3. 選択内容を右クリックし、[NCM 参照設定のセット] を選択します。
確認ダイアログボックスが表示されます。
 4. [はい] を選択します。
- 最新の設定が選択した各デバイスの参照として設定されます。ホスト設定テーブルの [参照] フィールドには、チェックおよび参照を設定したユーザが表示されます。

また、手動で参照設定を指定できます。

次の手順に従ってください:

1. [エクスプローラ] タブでデバイスを選択します。

コンテンツ画面で [リスト] タブが選択されていることを確認し、コンポーネント詳細画面で [ホスト設定] を選択します。

2. 参照として使用する設定を右クリックし、[参照の設定] を選択します。

設定はこのデバイス用の参照設定として指定されます。チェックおよび参照を設定したユーザが、ホスト設定テーブルの [参照] フィールドに表示されます。

設定した後に、参照設定仕様を変更または削除することができます。1つの設定のみをデバイス用の参照設定として設定できます。すでに設定されている別の設定で [参照の設定] または [NCM [参照設定の設定] オプションを使用する場合、元の設定が自動的にクリアされ、新しい設定が指定した参照設定になります。参照設定をクリアするには、ホスト設定テーブルで設定のメニューを右クリックし、[参照の設定解除] コマンドを使用します。

設定アラーム

特定の設定変更が発生した場合にトリガされるアラームを指定できます。このセクションでは、アラームをトリガした設定間の差異を表示する方法について説明します。

設定変更アラームをトリガするタイミングを決定する詳細については、「[設定変更アラートの設定 \(P. 32\)](#)」および「[単一デバイスの設定変更アラート設定の指定 \(P. 56\)](#)」を参照してください。

参照とランニング コンフィギュレーションの差異の表示

[アラーム詳細] タブで単一のデバイス用の参照とランニングの差異を表示および比較できます。

次の手順に従ってください:

1. [エクスプローラ] タブで、デバイス、デバイス ファミリ、またはグローバル コレクションを選択します。
2. コンテンツ画面で [アラーム] タブを選択します。
選択されたアイテムのアラームが表示されます。
3. [アラーム タイトル] 列に「参照および現在のランニング コンフィギュレーションが異なります」と表示するアラームを選択します。
4. コンポーネント詳細画面で [アラーム詳細] タブを選択します。
アラーム詳細が表示されます。
5. [差異を表示] ハイパーリンクをクリックします。

設定の差異画面には、キャプチャされたデバイス用の参照と現在のランニング ファイルの差異が表示されます。参照設定は右側の列に表示されます。

スタートアップとランニング コンフィギュレーションの表示

[アラーム詳細] タブで単一デバイス用のスタートアップとランニング コンフィギュレーションの差異を表示および比較できます。

次の手順に従ってください:

1. [エクスプローラ] タブで、デバイス、デバイス ファミリ、またはグローバル コレクションを選択します。
2. コンテンツ画面で [アラーム] タブを選択します。
デバイス、デバイス ファミリ、またはグローバル コレクションのアラームが表示されます。

3. [アラーム タイトル] 列に「スタートアップおよびランニングのコンフィギュレーションが異なります」と表示するアラームを選択します。
4. コンポーネント詳細画面で [アラーム詳細] タブを選択します。
アラーム詳細が表示されます。
5. [差異を表示] ハイパーリンクをクリックします。
[ランニングとスタートアップの比較] 画面には、キャプチャされたデバイスのランニングコンフィギュレーションファイルとスタートアップコンフィギュレーションファイルの差異が示されます。
スタートアップコンフィギュレーションは左側の列に表示されます。

グローバル同期タスク結果の表示

グローバル同期が失敗および成功したデバイスのリストを表示できます。

注: [失敗デバイスリスト] に無効な Network Configuration Manager を持つデバイスを含めるかどうかを制御できます。 詳細については、「[グローバル同期の設定 \(P. 84\)](#)」を参照してください。

次の手順に従ってください:

1. [設定マネージャ] を展開し、[エクスプローラ] タブで [タスク] を選択します。
2. [グローバル同期タスク] を選択します。
コンテンツ画面の [情報] タブに、情報および結果が表示されます。
3. [フィルタ] フィールドに名前、タイプ、状態、またはデバイスファミリを入力し、結果リストをフィルタします。

Report Manager からの Network Configuration Manager レポート

Network Configuration Manager のレポートオプションは、CA Spectrum Report Manager のネットワーク設定管理レポートパックに含まれています。 Report Manager では、多数のレポートコンテンツ、形式、およびレポート構成オプションが提供されます。 その結果、デバイス設定変更に関心のある組織のさまざまな対象読者に対して、適切なタイプおよび範囲の情報でレポートを生成できます。

Report Manager オプション

Report Manager は、以下の Network Configuration Manager レポートの生成および管理用に複数のオプションを提供します。

- 最新のテスト結果を表示するためにオンデマンドのレポートを生成。
- 1回限りまたは定期的なテスト レポート生成スケジュールを設定。
- スケジュール済みテスト レポートを Report Manager で保持する期間、および保持するレポート数を指定。
- スケジュール済みテスト レポートの電子メール受信者を指定。
- 別の Report Manager ユーザ用にテスト レポートのスケジュールを設定。
- PDF、テキスト、および表計算形式でレポートを発行。

注: Report Manager 機能の詳細については、「Report Manager ユーザ ガイド」を参照してください。

以下のレポートを使用できます。

設定変更: すべて

設定変更があるすべてのデバイス用の変更のサマリを表示します。行はそれぞれ、その設定変更を説明するデータと関連付けられるデバイスを表します。

設定変更: グループ

指定されたグローバルコレクションでデバイス用の変更のサマリを表示します。行はそれぞれ、その設定変更を説明する、ロールアップされた統計と関連付けられるデバイスを表します。

設定変更: 個別デバイス

指定されたデバイスに設定変更のリストを表示します。行はそれぞれ、変更の時間、変更したユーザ、および変更された行数を表示します。さらに、行にはそれぞれ、現在の設定と前の設定の間の差異を表示する Java アプレットへの Web リンクが含まれます。

設定イベント ログ 詳細: すべて

Network Configuration Manager アクティビティのある CA Spectrum 内のすべてのデバイスおよびモデル用イベントのリストを逆の年代順に表示します。リストのエントリにはそれぞれ、IP アドレス（該当する場合）、イベントテキスト、イベントコード、およびイベント作成者が含まれます。

設定イベント ログ 詳細: グループ

指定されたグローバルコレクション用の Network Configuration Manager アクティビティのあるすべてのデバイスおよびモデル用イベントのリストを逆の年代順に表示します。リストのエントリにはそれぞれ、IP アドレス（該当する場合）、イベントテキスト、イベントコード、およびイベント作成者が含まれます。

設定イベント ログ 詳細: 選択したデバイスまたはモデル

Network Configuration Manager アクティビティのある指定されたデバイスまたはモデルのイベントのリストを逆の年代順に表示します。リストのエントリにはそれぞれ、IP アドレス（該当する場合）、イベントテキスト、イベントコード、およびイベント作成者が含まれます。

トップ N 設定変更: すべて

「トップ N」が現在の並べ替え条件に基づくレコードの最大数として定義されている、設定変更がある「トップ N」デバイスの変更のサマリを表示します。レコードはそれぞれ、その設定変更を説明する、ロールアップされた統計と関連付けられるデバイスを表します。

トップ N 設定変更: グループ

グローバルコレクションに設定変更がある「トップ N」デバイスの変更のサマリを表示します。「トップ N」は現在の並べ替え条件に基づくレコードの最大数として定義されます。レコードはそれぞれ、その設定変更を説明する、ロールアップされた統計と関連付けられるデバイスを表します。

Report Manager でネットワーク設定管理レポートの生成

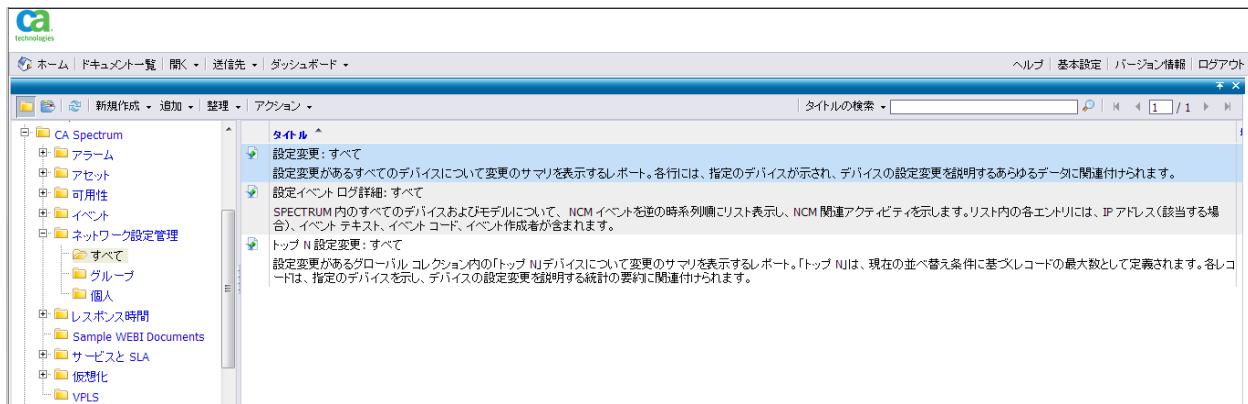
CA Spectrum Report Manager を使用して、ネットワーク設定管理レポートを生成できます。

注: 以下の例では、ネットワーク設定管理レポートの概要および Report Manager で使用可能な機能のみを説明します。詳細については、「Report Manager ユーザ ガイド」を参照してください。

次の手順に従ってください:

- 生成するテストのタイプを選択します。

以下のイメージでは、ネットワーク設定管理レポートオプションを示します。



- レポートを設定します。日時範囲のオプションを選択し、レポートタイトルとサブタイトルを提供して、ランドスケープを選択します。

- [レポートの表示] をクリックし、レポートを生成します。

レポートが表示されます。以下のイメージでは、レポート結果の例を示します。

The screenshot shows the generated report titled "SPECTRUM 設定変更:すべて". The report header includes the title and a sub-instruction: "設定変更があるすべてのデバイスについて変更のサマリを表示します。".

Report details:

- レポート期間: 2013/07/10 0:00:00 ~ 2013/07/11 0:00:00

設定変更:すべて					
デバイス名	デバイス IP	デバイス タイプ	設定変更	行変更の合計	最終変更の時間
138.42.96.10	138.42.96.10	IP Device	7	11	2013/07/10 1:34:21 AM
138.42.96.11	138.42.96.11	IP Device	2	3	2013/07/10 7:24:37 AM
138.42.96.12	138.42.96.12	IP Device	2	5	2013/07/10 1:34:07 PM

4. [デバイス名] のハイパーリンクをクリックし、デバイス レベルで結果を確認します。

以下のイメージでは、例を示します。このビューから [変更を表示] ハイパーリンクをクリックし、選択したデバイスの設定に追加、削除および変更される行、および無関係の行を表示できます。

The screenshot shows a report titled "SPECTRUM" with a sub-section "設定変更: 個別デバイス". The report details configuration changes for a specific device over a period from July 10, 2014, to July 11, 2013. The table lists the following information:

変更時間	行変更	詳細	NCM モード	NCM ユーザ	デバイス ユーザ	ソース	場所
2013/07/10 01:34:21 PM	1	変更内容	N/A	N/A	WEB	console	vty0 (172.18.248.132)
2013/07/10 01:27:03 PM	1	変更内容	N/A	N/A	WEB	console	vty0 (172.18.248.132)
2013/07/10 01:33:33 PM	5	変更内容	N/A	N/A	admin	Unknown	vty1 (172.18.92.34)
2013/07/10 01:01:39 PM	1	変更内容	N/A	N/A	Unknown	snmp	172.18.92.21
2013/07/10 08:45:47 AM	1	変更内容	N/A	N/A	admin	console	vty0 (172.18.92.34)
2013/07/10 07:16:37 AM	1	変更内容	N/A	N/A	WEB	snmp	vty1 (172.18.92.200)
2013/07/10 06:17:10 AM	1	変更内容	N/A	N/A	Unknown	Unknown	Unknown

第 4 章: Network Configuration Manager のデバイスレベルのタスク

この章では、Network Configuration Manager を使用して、ネットワーク内でデバイスの設定を手動でキャプチャ、エクスポート、およびアップロードする方法について説明します。

このセクションには、以下のトピックが含まれています。

[設定の手動によるキャプチャ \(P. 99\)](#)

[單一デバイスへの設定の手動アップロード \(P. 100\)](#)

設定の手動によるキャプチャ

Network Configuration Manager は、変更が発生した直後にデバイス設定のキャプチャを試みます。設定変更の未承諾通知は、変更が発生したデバイスから送信されるトラップまたは MIB オブジェクトのいずれかになります。未承諾通知を受信する場合、SpectroSERVER はキャプチャを実行しデータベースに設定を保存して、更新された設定データを提供します。また、手動で OneClick のデバイス設定をキャプチャできます。

次の手順に従ってください:

1. [エクスプローラ] タブで単一のデバイスを選択します。
コンテンツ画面の [リスト] タブにデバイスが表示されます。
2. コンポーネント詳細画面で [ホスト設定] タブを選択します。
前回のキャプチャの結果が表示されます。
3. 設定のキャプチャアイコンをクリックします。
キャプチャの結果が表示されます。リスト内に新しい設定が表示されるか、現在の設定について最終検証時間が更新されます。

單一デバイスへの設定の手動アップロード

コンフィギュレーションファイルをネットワーク上の単一のデバイスに手動でアップロードできます。アップロードされるコンフィギュレーションファイルは、既存のコンフィギュレーションファイルにマージされます。この機能を利用して、新たにインストールされたデバイスまたは代替/スタンバイ状態のリモートデバイスを迅速にオンラインにすることが可能です。

Juniper JUNOS デバイス ファミリのデバイスにアップロードする場合、JUNOScript API 形式を使用します。詳細については、「[Juniper JUNOS デバイス \(P. 22\)](#)」を参照してください。

注: バルク アップロードタスクを作成して、設定をアップロードし、リアルタイムの結果を表示できます。詳細については、「[アップロードタスクの作成 \(P. 105\)](#)」を参照してください。

承認が不要

単一のデバイスにデバイス設定をアップロードするプロセスは、承認ワークフローが有効かどうかによって異なります。以下の手順では、承認を必要としない場合のプロセスについて説明します。

注: ワークフロー承認オプションの詳細については、「[ワークフローの設定 \(P. 33\)](#)」を参照してください。

次の手順に従ってください:

1. [エクスプローラ] タブで単一のデバイスまたはデバイス ファミリを選択します。

コンテンツ画面の [リスト] タブに、選択されたデバイス ファミリに関連付けられた 1 つまたは複数のデバイスが表示されます。

2. コンポーネント詳細画面で [ホスト設定] タブを選択します。

前回のキャプチャの結果が表示されます。

3. [アップロード] アイコンをクリックします。

注: 承認が必要な場合、[承認必須] ダイアログ ボックスが表示されます。[承認必須 (P. 103)] に移動し、承認要求を作成します。

選択されたデバイスの最後に認識された設定情報を示す、設定のアップロード画面が表示されます。例は以下のとおりです。

```
Last configuration change at 11:11:28 EST Mon Jun 10 2013 by admin
version 12.2
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
hostname cis7204-96.6
boot-start-marker
boot system disk0:c7200-adventuresek9-mz.122-33.SRE4bin
boot system disk0:c7200-jk9s-mz.124-25ebin
warm-reboot count 10 uptime 10
boot-end-marker
security passwords min-length 1
logging console errors
enable secret 5 $1$zDGm$H3f9xVvzMZ26X0eTxyl1
aaa new-model

aaa group server tacacs+ TAC
server 138.42.249.194
aaa authentication login default group tacacs+ enable
aaa authentication ppp default local
aaa authorization config-commands
aaa authorization exec default group tacacs+ local none
aaa authorization commands 1 default group tacacs+ local none
aaa authorization commands 15 default group tacacs+ local none
```

4. 以下のオプションの手順のいずれかを実行します。
 - (オプション) 必要に応じて、設定コンテンツを編集します。
 - (オプション) [検索] フィールドに条件を入力し、設定ファイルで指定された行を見つけて、アップロードする前にコンテンツの変更または確認を行います。
 - [スタートアップにも保存] を選択し、この設定をスタートアップコンフィギュレーションに書き込みます。これで再起動時に、デバイスに設定ファイルをロードするようになります。

注: この機能は Cisco、Foundry、および Nortel Passport L3 デバイスでのみサポートされています。
 - [開く] をクリックして、システム上でローカルに保存されている、以前にエクスポートされた設定ファイルをインポートします。
 - このコンフィギュレーションファイルをテキストまたは html 形式で保存およびエクスポートする場合、[名前を付けて保存] をクリックします。
5. [アップロード] をクリックし、コンフィギュレーションファイルを選択されたデバイスにアップロードします。

処理が完了すると、「設定のアップロードが成功しました。」というメッセージが表示されます。

注: スケジューリングタスクは、バルク タスクで使用可能な機能です。アップロードタスクをスケジュールする場合は、「[Network Configuration Manager のバルク タスク \(P. 105\)](#)」を参照してください。

單一デバイスに設定をアップロード(承認が必要)

承認ワークフローが有効な場合、処理するために設定変更を承認する必要があります。承認後に実行できるアップロード要求用のタスクを作成することで、これは実行されます。

注: 承認ワークフロー オプションの詳細については、「[ワークフローの設定](#)(P. 33)」を参照してください。

次の手順に従ってください:

1. [エクスプローラ] タブで单一のデバイスまたはデバイス ファミリを選択します。
コンテンツ画面の [リスト] タブに、選択されたデバイス ファミリに関連付けられた 1 つまたは複数のデバイスが表示されます。
2. コンポーネント詳細画面で [ホスト設定] タブを選択します。
前回のキャプチャの結果が表示されます。
3. [アップロード] アイコンをクリックします。
[承認必須] ダイアログ ボックスが表示されます。
4. [はい] をクリックして操作を続行します。
[NCM タスクを作成] が表示されます。
5. 以下のようにタスクを作成します。
 - a. [名前] フィールドに、固有の名前を入力します。

注: Network Configuration Manager ではデフォルトの名前 (<タスク タイプ>.YY-MM-DD_HH:MM.<ユーザ名>) が提供されます。たとえば、Upload.2006-10-17_15:48:04.Administrator などです。

- b. [説明] フィールドに、タスクの説明を入力します。
- c. 実行された後にタスクを使用可能にする場合、[再利用可能タスク] を選択します。
- d. [編集] をクリックし、[コンテンツのアップロード] ボックス内のデバイス設定にアップロードおよびマージするコンテンツを指定します。[開く] をクリックして、テキスト ファイルからコンテンツをインポートすることもできます。変更した後に [別名で保存] をクリックし、txt または html でこの設定ファイルを保存およびエクスポートすることができます。

- e. (オプション) [検索] フィールドに条件を入力し、設定ファイルで特定の行を見つけます。
 - f. [スタートアップへのコミット] を選択して（該当する場合）、新しいコンテンツがマージされた後でランニング コンフィギュレーション全体をスタートアップ コンフィギュレーションにコピーします。
 - g. [失敗時にデバイスにアラーム] を選択し、タスクが失敗した各デバイス上にアラームを生成します。
 - h. [承認の要求] をクリックします。
[承認必須] ダイアログ ボックスが表示されます。
6. ユーザを選択し、[タスク承認者] に電子メールアドレスを入力して、タスクの説明を入力し（オプション）、[OK] をクリックして要求を生成します。
- 確認ダイアログ ボックスが表示され、要求の作成に成功したことを示します。電子メールはタスク承認者に送信され、生成されたタスクは [エクスプローラ] タブのタスク フォルダに表示されます。
- 注: 電子メールの設定の詳細については、「管理者ガイド」を参照してください。
7. 承認ステータスを確認し、「[タスクの開始 \(P. 135\)](#)」の説明に従ってタスクを実行します。

第 5 章: Network Configuration Manager バルクタスク

この章では、Network Configuration Manager でオンデマンドのバルクのアップロードタスク、同期タスク、およびスタートアップへの保存タスクを作成する方法について説明します。これらのタスクでは、ホスト設定のキャプチャおよびアップロードによりデバイスとの対話が行われます。単一のデバイスまたはデバイスのリストに対して、随時実行可能なタスクを作成できます。これらのオンデマンドタスクは、同じ設定を (IP アドレスなどわずかな差異で) ネットワーク上の複数のデバイスにロールアウトする場合に役立ちます。

タスクは再利用可能として定義することができます。再利用可能なタスクは実行後も保持され、再度実行することができます。タスクが再利用可能でない場合、一度実行されると [ロストファウンド] ビューに送信され、24 時間以内にページされます。

このセクションには、以下のトピックが含まれています。

[アップロードタスクの作成 \(P. 105\)](#)

[同期タスクの作成 \(P. 109\)](#)

[スタートアップへの保存タスクを作成 \(P. 111\)](#)

アップロードタスクの作成

自動的にアップロードタスクを作成し、バルク設定のアップロードを実行します。バルクアップロードタスクでは、新しいコンテンツが 1 つまたは複数の選択されたデバイスの実行コンフギュレーションにマージされます。デバイスはランダムな順序で処理されます。

重要: Enterasys/Riverstone SSR デバイスにアップロードしている場合は、このタスクを続行する前に [「Enterasys/Riverstone SSR デバイスによるアップロードタスクへの応答方法の決定 \(P. 108\)」](#) を参照してください。

Juniper JUNOS デバイス ファミリのデバイスにアップロードしている場合、JUNOScript API 形式を使用する必要があります。詳細については、[「Juniper JUNOS デバイス \(P. 22\)」](#) を参照してください。

次の手順に従ってください:

1. [エクスプローラ] タブで、单一デバイス、デバイス ファミリ、グローバル コレクション、検索結果エントリ、またはコンテナ（ユニバースなど）を選択します。
2. [リスト] タブをクリックし、アップロード タスクを実行するデバイスを選択します。
3. ツールバーの [NCM タスクの作成] アイコンからアップロード タスクを選択します。
[アップロード タスク] ダイアログ ボックスが表示されます。
注: 選択されたデバイスが [許可] タブに表示されない場合、[禁止] をクリックし、Network Configuration Manager のタスクから無効化されているデバイスまたは必要な権限のないデバイスを表示します。
4. [続行] をクリックします。
[タスクの作成] ダイアログ ボックスが表示されます。
5. 以下のようにタスク情報を入力します。
 - a. (オプション) [名前] フィールドに一意の名前を入力します。
注: Network Configuration Manager ではデフォルトの名前 (<タスク タイプ>.YY-MM-DD_HH:MM.<ユーザ名>) が提供されます。たとえば、Upload.2006-10-17_15:48:04.Administrator などです。
 - b. (オプション) [説明] フィールドに、タスクの説明を入力します。
 - c. [再利用可能タスク] を選択し、タスクを再利用可能にします。
 - d. [編集] をクリックし、[コンテンツのアップロード] ボックス内のデバイス設定にアップロードおよびマージするコンテンツを指定します。[開く] をクリックして、テキスト ファイルからコンテンツをインポートすることもできます。変更した後に [別名で保存] をクリックし、txt または html でこの設定 ファイルを保存およびエクスポートすることができます。
 - e. [検索] フィールドに条件を入力し、設定 ファイル内の特定の行を見つけます。
 - f. [スタートアップへのコミット] を選択して（該当する場合）、新しいコンテンツがマージされた後でランニング コンフィギュレーション全体をスタートアップ コンフィギュレーションにコピーします。

-
-
-
-
-
- - g. [失敗時にデバイスにアラーム] を選択し、タスクが失敗した各デバイス上にアラームを生成します。
6. 承認が必要な場合（[承認の要求] ボタンで示される）、以下の手順を実行します。
 - a. [承認の要求] をクリックします。
[承認必須] ダイアログボックスが表示されます。
 - b. ユーザを選択し、[タスク承認者] に電子メールアドレスを入力して、タスクの説明を入力し（オプション）、[OK] をクリックして要求を生成します。
確認ダイアログボックスは、要求が正常に作成されたことを示します。電子メールのメッセージはタスク承認者に送信され、生成されたタスクは [エクスプローラ] タブのタスク フォルダに表示されます。
注: 電子メールの設定の詳細については、「管理者ガイド」を参照してください。
 - c. 承認ステータスを確認し、「[タスクの開始 \(P. 135\)](#)」の説明に従ってタスクを実行します。
注: 承認ワークフロー オプションの詳細については、「[ワークフローの設定 \(P. 33\)](#)」を参照してください。
7. 承認が必要でない場合（[保存] ボタンで示される）
 - a. [保存] をクリックします。
[タスクが保存されました] ダイアログボックスが表示されます。
 - b. 以下のいずれかの手順を実行します。
 - [アップロード] をクリックし、選択されたデバイスにタスクをアップロードします。
[アップロードタスク結果] ダイアログボックスが表示され、生成されたタスクは [エクスプローラ] タブのタスク フォルダに表示されます。結果ダイアログボックスの詳細については、「[リアルタイムでタスク結果を表示 \(P. 137\)](#)」を参照してください。

- [スケジュール] をクリックして、将来の実行に備えてタスクをスケジュールします。スケジューリングについては、「[タスクのスケジュール \(P. 131\)](#)」で説明されます。
そのタスクは保存され、そのスケジュールに従って実行されます。
- [閉じる] をクリックしタスクを保存します。これは後日実行できます。設定マネージャの下にある [エクスプローラ] タブの [タスク] から選択することによって、タスクを編集および実行できます。

Enterasys/Riverstone SSR デバイスによるアップロード タスクへの応答の決定

Enterasys/Riverstone SSR デバイスは、設定のアップロードに常時応答するわけではありません。デバイスによっては、ランニング コンフィギュレーションおよびスタートアップ コンフィギュレーションの両方が、アップロードされたコンテンツと置き換えられます。または、アップロードされたコンテンツがランニング コンフィギュレーションおよびスタートアップ コンフィギュレーションの両方にマージされる場合もあります。Enterasys/Riverstone SSR デバイス上で実行された設定キャプチャでは、ランニング コンフィギュレーションではなくスタートアップ コンフィギュレーションが取得されます。そのため、ランニングおよびスタートアップのコンフィギュレーションを確認するために、Enterasys ファームウェアを実行しているデバイスをテストすることをお勧めします。

次の手順に従ってください:

1. 検索結果または [エクスプローラ] タブ内のコンテナ（ユニバースなど）から、単一の SSR デバイスを選択します。
2. コンテンツ画面で [リスト] タブをクリックします。
3. コンポーネント詳細画面で [ホスト設定] タブをクリックします。
事前にキャプチャされた設定が表示されます。
4. 設定のキャプチャアイコンを選択し、選択されたデバイスの現在の設定をキャプチャします。
5. [アップロード] アイコンを選択します。
[設定のアップロード] 画面が表示されます。現在のスタートアップ コンフィギュレーションのコンテンツが下部ペインに表示されます。

6. [設定のアップロード] 画面で既存の設定を編集します。たとえば、以下のロケーション行の値を削除（または行を削除）します。
`system set location "値"`
 7. もう一度 [アップロード] アイコンを選択し、変更されたデバイス設定をアップロードします。もう一度設定のキャプチャアイコンを選択し、デバイスから新しい設定をキャプチャします。
- この場所が新たにキャプチャされた設定に存在しない場合は、デバイスによってランニングコンフィギュレーションおよびスタートアップコンフィギュレーションの両方がアップロードされたコンテンツに（マージではなく）置き換えられていることがわかります。

同期タスクの作成

自動同期タスクを作成し、ネットワーク上の選択されたデバイスのポリシーに準拠しているデバイス設定をキャプチャおよび検証し、結果をリアルタイムで表示します。同期タスクがデバイス設定をキャプチャする場合、デバイスに関連するすべてのポリシー、および指定されていれば、デバイススタートアップコンフィギュレーションに対して設定を確認します。デバイスはランダムな順序で処理されます。

Network Configuration Manager ポリシーの詳細については、「[Network Configuration Manager ポリシー \(P. 141\)](#)」を参照してください。

バックグラウンドモードでグローバル同期タスクを実行する詳細については、「[グローバル同期について \(P. 83\)](#)」を参照してください。

次の手順に従ってください：

1. [エクスプローラ] タブで、单一デバイス、デバイスファミリ、グローバルコレクション、検索結果エントリ、またはコンテナ（ユニバースなど）を選択します。
2. コンテンツ画面の [リスト] タブをクリックし、同期タスクに含めるデバイスを選択します。

3. ツールバーの [NCM タスクの作成] アイコンから [同期タスク] をクリックします。

[デバイスの選択: 同期タスク] ダイアログ ボックスが表示されます。

注: 選択されたデバイスが [許可] タブに表示されない場合、[禁止] をクリックして、Network Configuration Manager のタスクから無効化されているか必要な権限を持たないデバイスを表示させます。

4. 以下のようにタスク情報を入力します。

- a. [名前] フィールドに、固有の名前を入力します。

注: Network Configuration Manager ではデフォルトの名前 (<タスクタイプ>.YY-MM-DD_HH:MM.<ユーザ名>) が提供されます。たとえば、Sync.2010-09-09_15:48:04.Administrator などです。

- b. [説明] フィールドに、タスクの説明を入力します。
 - c. [スタートアップが異なる場合にデバイスでアラーム] および適切な重大度を選択し、キャプチャされた設定がスタートアップコンフィギュレーションと異なる各デバイスでアラームを生成させます。
 - d. [スケジュールの編集] をクリックし、将来の実行に備えてタスクをスケジュールします。スケジューリングについては、「[タスクのスケジュール \(P. 131\)](#)」で説明されます。
 - e. [再利用可能タスク] を選択し、タスクを再利用可能にします。

5. 以下のいずれかの手順を実行します。

- [保存] をクリックしタスクを保存します。これは後日実行できます。Configuration Manager の下にある [エクスプローラ] タブのタスクから選択することによって、タスクを実行できます。

- [同期タスクを今すぐ実行] をクリックします。

[同期タスク結果] ダイアログ ボックスが表示され、生成されたタスクは [エクスプローラ] タブのタスク フォルダに表示されます。詳細については、「[リアルタイムでタスク結果を表示 \(P. 137\)](#)」を参照してください。

スタートアップへの保存タスクを作成

スタートアップへの自動保存タスクを作成し、1つ以上の選択されたデバイスのスタートアップコンフィギュレーションに現在のランニングコンフィギュレーションを書き込みます。デバイスの設定は NVRAM（不揮発性ランダムアクセスメモリ）に保存されます。

デバイスはランダムな順序で処理されます。

次の手順に従ってください:

1. [エクスプローラ] タブで、單一デバイス、デバイス ファミリ、グローバルコレクション、検索結果エントリ、またはコンテナ（ユニバースなど）を選択します。
2. コンテンツ画面の [リスト] タブをクリックし、アップロードするデバイスを選択します。
3. ツールバーの [NCM タスクの作成] アイコンから [スタートアップへの保存タスク] をクリックします。

[スタートアップへの保存タスク] ダイアログ ボックスが表示されます。

注: 選択されたデバイスが [許可] タブに表示されない場合、[禁止] をクリックし、Network Configuration Manager のタスクから無効化されているデバイスまたは必要な権限のないデバイスを表示します。

4. 以下のようにタスク情報を入力します。
 - a. (オプション) [名前] フィールドに一意の名前を入力します。
注: Network Configuration Manager ではデフォルトの名前 (<タスクタイプ>.YY-MM-DD_HH:MM.<ユーザ名>) が提供されます。たとえば、WriteStartup.2006-10-17_15:48:04Administrator などです。
 - b. (オプション) [説明] フィールドに、タスクの説明を入力します。
 - c. [再利用可能タスク] を選択し、タスクを再利用可能にします。
5. 承認が必要な場合（[承認の要求] ボタンで示される）、以下の手順を実行します。
 - a. [承認の要求] をクリックします。
[承認必須] ダイアログ ボックスが表示されます。

- b. ユーザを選択し、[タスク承認者]に電子メールアドレスを入力して、タスクの説明を入力し（オプション）、[OK]をクリックして要求を生成します。

確認ダイアログ ボックスは、要求が正常に作成されたことを示します。電子メールはタスク承認者に送信され、生成されたタスクは [エクスプローラ] タブのタスク フォルダに表示されます。

注: 電子メールの設定の詳細については、「管理者ガイド」を参照してください。

- c. 承認ステータスを確認し、「[タスクの開始 \(P. 135\)](#)」の説明に従ってタスクを実行します。

注: 承認ワークフロー オプションの詳細については、「[ワークフローの設定 \(P. 33\)](#)」を参照してください。

6. 承認が必要でない場合は、以下の手順のいずれかを実行します。

- [スケジュール] をクリックして、将来の実行に備えてタスクをスケジュールします。スケジューリングについては、「[タスクのスケジュール \(P. 131\)](#)」で説明されます。

- [保存] をクリックします。

タスクは将来の実行に備えて保存されます。

- [スタートアップへの保存タスクを今すぐ実行] をクリックします。

[スタートアップへの保存タスク結果] ダイアログ ボックスが表示され、生成されたタスクは [エクスプローラ] タブのタスク フォルダに表示されます。詳細については、「[リアルタイムでタスク結果を表示 \(P. 137\)](#)」を参照してください。

注: タスク デバイス上の「スタートアップとランニングのコンフィギュレーションが異なります」のどのアラームも、このタスクによって自動的にクリアされます。 詳細については、「[スタートアップおよびランニング コンフィギュレーションの差異の表示 \(P. 93\)](#)」を参照してください。

第6章: ファームウェア アップロード

このセクションでは、Cisco IOS および Cisco IOS - SSH Capable デバイスのファームウェアをアップロードする方法について説明します。ファームウェアのアップロードは、以下の 2 つのメソッドのどちらかによって実行できます。

- ファームウェア ロード タスクの使用
- 拡張ユーティリティのスクリプトの使用

重要: ファームウェアのアップロードは高度なユーザの機能であり、上級の知識を必要とします。誤ってデバイス ファームウェアを変更すると、稼働していない状態のデバイスに残る可能性があります。

このセクションには、以下のトピックが含まれています。

[ファームウェア アップロードについて \(P. 113\)](#)

[権限 \(P. 114\)](#)

[デバイス ファームウェア の転送設定の設定 \(P. 115\)](#)

[Cisco フラッシュ パーティション情報の表示 \(P. 116\)](#)

[ファームウェア ロード タスクの作成 \(P. 117\)](#)

[再ロード タスクの作成 \(P. 121\)](#)

[再ロード キャンセル タスクの作成 \(P. 124\)](#)

[デバイス ファームウェア のロード スクリプト \(P. 125\)](#)

ファームウェア アップロードについて

スクリプトが存在する場合、ファームウェア アップロードがサポートされ、このスクリプトが使用されます。スクリプトが存在せず、デバイスが CISCO-FLASH-MIB をサポートする場合、MIB が使用されます。

ファームウェア アップロードは特定のタスクを正常に、および特定の順番で転送を成功させるために実行する必要があります。このセクションでは、これらのタスクおよびファームウェアのアップロード プロセスについて説明します。

注: これらのタスクは「[ファームウェア ロード タスクの作成 \(P. 117\)](#)」で説明された「ファームウェア ロード タスク」、またはカスタム スクリプトによって処理されます。

タスクは次のとおりです。

1. サーバからデバイスにファームウェアイメージをアップロードします。デバイスは、既知のサーバ（イメージサーバ）から指定されたフルッシュまたはファイルシステム名にファームウェアイメージをロードするように指示される必要があります。このアップロードは、イメージファイルおよびネットワーク帯域幅のサイズによって完了するまでに数分から数時間かかります。
2. デバイスにブートコマンド設定をアップロードします。以下の3つの手順で発生します。
 - a. 設定をキャプチャします。現在の設定に新しいコマンドを挿入できるように、設定をキャプチャする必要があります。
 - b. 変更をアップロードします。
 - c. NVRAMに書き込みます。起動時にデバイスが指定されたイメージを再ロードするように、変更された設定をスタートアップに書き込む必要があります。
3. スクリプトの再ロードを実行します。再ロードコマンドはモードを有効にするために直接書き込まれており、設定の一部ではありません。

必要に応じて、システムはデフォルトプロトコルまたは上書きスクリプトを各フェーズで使用します。

重要: これらの手順のいずれかでエラーが発生した場合、ロールバックは行われません。デバイスは最後に成功した状態のままでです。

権限

これらのセクションで説明されたとおりにファームウェアをアップロードする場合、以下の Network Configuration Manager の権限が必要な可能性があります。

- デバイスファームウェアのロード
- デバイス再ロード
- 再ロードのスケジュール

詳細については、「[Network Configuration Manager 権限 \(P. 265\)](#)」を参照してください。

デバイス フームウェアの転送設定の設定

このセクションでは、デバイスにフームウェアイメージを転送するために使用するプロトコルおよびサーバ設定を設定する方法について説明します。これらの設定はデバイスファミリ レベルで作成され、デバイス フームウェアの転送設定サブビューに存在します。これは Cisco IOS および Cisco IOS - SSH Capable デバイスファミリのみで使用可能です。これらのデバイスファミリのデバイスは CISCO-FLASH-MIB をサポートします。

注: フームウェアアップロードは、Cisco IOS および Cisco IOS - SSH Capable デバイスファミリにおいて標準でサポートされます。他のすべてのデバイスについては、拡張ユーティリティを使用して [デバイス フームウェアのロード] スクリプトを指定できます。詳細については、「[Network Configuration Manager の拡張ユーティリティ \(P. 60\)](#)」を参照してください。

次の手順に従ってください:

1. [エクスプローラ] タブのデバイス ファミリから Cisco IOS または Cisco IOS - SSH Capable デバイス ファミリを選択します。
情報および設定が、コンテンツ画面の [情報] タブに表示されます。
2. デバイス フームウェア転送設定サブビューを展開します。
フームウェア転送オプションでは、サーバからフームウェアイメージ転送を設定できるようになり、また、カスタム スクリプトが提供されます。
3. 以下のいずれかの手順を実行します。
 - 必要に応じて、[フームウェアイメージ転送プロトコル] を変更します。
 - [デバイス フームウェアのロード] スクリプトを入力します。
スクリプトを入力する詳細については、「[設定スクリプトの入力 \(P. 67\)](#)」を参照してください。

重要: スクリプトが存在する場合、[フームウェアイメージ転送プロトコル] に指定されるものにかかわらず、スクリプトが使用されます。

Cisco フラッシュ パーティション情報の表示

正常に新しいファームウェア イメージをデバイスにアップロードするには、イメージをサポートするのに十分なディスク領域が必要です。このセクションでは、ファームウェアアップロードを試行する前に、デバイス上で使用可能なリソースを確認する便利な方法について説明します。

注: [NCM タスクの作成] ダイアログ ボックスの [パーティションの表示] ボタンを使用して [ファームウェア ロード タスク] を作成している場合、デバイス用のパーティション情報を表示することもできます。 詳細については、「[ファームウェア ロード タスクの作成 \(P. 117\)](#)」を参照してください。

Cisco フラッシュ パーティション情報を表示する方法

1. [エクスプローラ] タブのデバイス ファミリで、Cisco IOS または Cisco IOS - SSH Capable デバイス ファミリのいずれかのデバイスを選択します。

コンテンツ画面の [情報] タブに、デバイスの情報および設定が表示されます。

2. Cisco フラッシュ パーティション サブビューを展開します。

以下の情報が表示されます。

名前

パーティション名。

ファイルの数

パーティション内のファイル数。

空き容量

パーティションで使用可能な容量。アップロードされる新しいファームウェア イメージをサポートするのに十分なディスク空き容量が必要です。

合計容量

パーティションに割り当てられた合計容量。

ファームウェア ロード タスクの作成

このセクションでは、ファームウェア ロード タスクを作成する方法について説明します。これは Cisco IOS および Cisco IOS - SSH Capable デバイスにファームウェアをアップロードするのに使用されます。

注: このタスクを完了するには、新しいファームウェアイメージをアップロードするデバイスの場所を指定する必要があります。ターゲット場所には新しいイメージをサポートできる十分なスペースが必要です。タスクを作成する前にデバイス上の使用可能なリソースを確認するには、「[Cisco フラッシュパーティション情報の表示 \(P. 116\)](#)」を参照してください。

次の手順に従ってください:

1. [エクスプローラ] タブのデバイス ファミリで、Cisco IOS または Cisco IOS - SSH Capable デバイス ファミリのいずれかのデバイスを選択します。
2. コンテンツ画面の [リスト] タブをクリックし、ファームウェア ロード タスク用のデバイスを選択します。
3. ツールバーの [NCM タスクの作成] アイコンから [ファームウェア ロード タスク] を選択します。

[デバイスの選択: ファームウェア ロード タスク] ダイアログ ボックスが開きます。

注: 選択されたデバイスが [許可] タブに表示されない場合、[禁止] をクリックして、Network Configuration Manager タスクから無効化されているか必要な権限を持たないデバイスを表示させます。

4. [続行] をクリックします。
[NCM タスクの作成] ダイアログ ボックスが表示されます。
5. 以下のようにタスクを作成します。

- a. [名前] フィールドに、固有の名前を入力します。

注: Network Configuration Manager ではデフォルトの名前 (<タスク タイプ>.YY-MM-DD_HH:MM.<ユーザ名>) が提供されます。たとえば、LoadFirmware.2006-10-17_15:48:04.Administrator などです。

- b. [説明] フィールドに、タスクの説明を入力します。
- c. [再利用可能タスク] を選択し、タスクを再利用可能にします。

- d. 以下のイメージ情報を入力します。

ファームウェア イメージ名

イメージサーバ上のファームウェアイメージのファイル名。

宛先

デバイス上に置かれるイメージのファイル名。サーバ上のものと同じ名前であることが多く、値はオート フィルされます。

ブートコマンド

ブートするイメージの名前。これは宛先名でオート フィルされます。

デフォルト : boot system flash

バックアップ ブートコマンド

エラーが発生する場合に、ブートするイメージの名前。デバイスで現在ブート可能なイメージに設定される必要があります。これは宛先名でオート フィルされます。

デフォルト : boot system flash

ファームウェア アップロード後にデバイスを再ロード

選択された場合、[再ロード情報] フィールドは有効であり、ファームウェア アップロードが成功した後にデバイスが再ロードされます。

パーティションの表示

[パーティションの表示] をクリックし、[デバイス パーティション] ダイアログボックスを表示します。これはデバイスで使用可能なリソースを表示します。ターゲット場所には新しいイメージをサポートできる十分なスペースが必要です。

- e. 以下の再ロード情報を入力します（該当する場合）。

今すぐ再ロード

[今すぐ再ロード] を選択すると、ファームウェア アップロードに成功した直後にデバイスを再ロードします。このオプションが選択されていない場合は、[タイミング] フィールドを使用して再ロードをスケジュールします。

スタートアップにも保存(変更された場合)

ランニング コンフィギュレーションが変更されたのに保存されていない場合、再ロードが開始される前にスタートアップにコピーするかどうかを示します。

Telnet ログインタイムアウト

デバイスへのログインを試行している間に、telnet 接続に使用されるタイムアウト値（秒単位）。

Telnet コマンド タイムアウト

telnet 接続でコマンドを実行しようとする間に使用されるタイムアウト値（秒単位）。

- f. [サーバ設定] をクリックして [サーバ設定の編集] ダイアログボックスで以下を入力し、デバイス ファミリ レベルで設定された転送設定を上書きします。

プロトコル

使用されるプロトコル。

サーバアドレス

デバイスがファームウェアイメージをコピーするイメージ転送サーバアドレス。

タイムアウト(秒)

デバイスがファームウェアイメージサーバからのコピーに失敗するまでのタイムアウト期間。

イメージ ディレクトリ

ファイルが使用されるイメージ転送サーバのサブディレクトリ。

注: イメージサーバのルートディレクトリからのイメージが使用されない場合、これが必要になる可能性があります。

ユーザ名

イメージ転送サーバにより必要とされるユーザ名。

注: これは指定されたプロトコルでは必要とされない可能性があります。

パスワード

イメージ転送サーバにより必要とされるパスワード。

注: これは指定されたプロトコルでは必要とされない可能性があります。

6. 承認が必要な場合（[承認の要求] ボタンで示される）、以下の手順を実行します。

- a. [承認の要求] をクリックします。

[承認必須] ダイアログ ボックスが表示されます。

- b. ユーザを選択し、[タスク承認者] 用の電子メール アドレスを入力します。

- c. (オプション) タスクの説明を入力し、[OK] をクリックして要求を生成します。

確認ダイアログ ボックスは、要求が正常に作成されたことを示します。電子メールのメッセージはタスク承認者に送信され、生成されたタスクは [エクスプローラ] タブのタスク フォルダに表示されます。

注: 電子メール設定の詳細については、「管理者ガイド」を参照してください。

- d. 承認ステータスを確認し、「[タスクの開始 \(P. 135\)](#)」の説明に従ってタスクを実行します。

注: 承認ワークフロー オプションの詳細については、「[ワークフローの設定 \(P. 33\)](#)」を参照してください。

7. 承認が必要でない場合（[保存] ボタンで示される）

- a. [保存] をクリックします。

[タスクが保存されました] ダイアログ ボックスが表示されます。

b. 以下のいずれかを実行します。

- [ファームウェアのアップロード] をクリックし、タスクを処理します。
[ファームウェア ロードタスク結果] ダイアログ ボックスが表示され、生成されたタスクは [エクスプローラ] タブのタスク フォルダに表示されます。 詳細については、「[リアルタイムでタスク結果を表示 \(P. 137\)](#)」を参照してください。
- [スケジュール] をクリックして、将来の実行に備えてタスクをスケジュールします。スケジューリングについては、「[タスクのスケジュール \(P. 131\)](#)」で説明されます。
タスクは保存され、スケジュールに従って実行されます。
- [閉じる] をクリックしタスクを保存します。これは後日実行できます。設定マネージャの下にある [エクスプローラ] タブの [タスク] から選択することによって、タスクを編集および実行できます。

再ロードタスクの作成

再ロードタスクを作成し、ファームウェアがアップロードされた後にデバイスを再ロードします。このタスクは Cisco IOS および Cisco IOS - SSH Capable デバイスに使用できます。

注: 再ロードタスクにより提供される機能は、ファームウェア ロードタスクでもオプションで使用可能です。

次の手順に従ってください:

1. [エクスプローラ] タブのデバイス ファミリで、Cisco IOS または Cisco IOS - SSH Capable デバイス ファミリのいずれかのデバイスを選択します。
2. コンテンツ画面で [リスト] タブをクリックし、再ロードタスク用のデバイスを選択します。

3. 再ロードタスクを選択し、ツールバーの [NCM タスクの作成] アイコンからタスクを再ロードします。

[デバイスの選択: 再ロードタスク] ダイアログボックスが開きます。

注: 選択されたデバイスが [許可] タブに表示されない場合、[禁止] をクリックし、Network Configuration Manager のタスクから無効化されているデバイスまたは必要な権限のないデバイスを表示します。

4. 承認が必要な場合（[承認の要求] ボタンで示される）、以下の手順を実行します。

- a. [承認の要求] をクリックします。

[承認必須] ダイアログボックスが表示されます。

- b. ユーザを選択し、[タスク承認者] 用の電子メールアドレスを入力します。

- c. (オプション) タスクの説明を入力し、[OK] をクリックして要求を生成します。

確認ダイアログボックスは、要求が正常に作成されたことを示します。電子メールのメッセージはタスク承認者に送信され、生成されたタスクは [エクスプローラ] タブのタスクフォルダに表示されます。

注: 電子メール設定の詳細については、「管理者ガイド」を参照してください。

- d. 承認ステータスを確認し、「[タスクの開始 \(P. 135\)](#)」の説明に従ってタスクを実行します。

承認された後にタスクを開始する場合、[再ロードタスク] ダイアログボックスが表示されます。

注: 承認ワークフロー オプションの詳細については、「[ワークフローの設定 \(P. 33\)](#)」を参照してください。

5. 承認が必要でない場合は、[再ロードタスクを今すぐ実行] をクリックします。

[再ロードタスク] ダイアログボックスが表示されます。

6. 以下のようにタスクを作成します。
 - a. 以下の再ロード情報を入力します。

今すぐ再ロード

[今すぐ再ロード] を選択すると、すぐにデバイスを再ロードします。このオプションが選択されていない場合は、[タイミング] フィールドを使用して再ロードをスケジュールします。

ウォーム

ウォーム再ロードします（NVRAM へのイメージのコピーおよび解凍をスキップ）。

スタートアップにも保存(変更された場合)

ランニング コンフィギュレーションが変更された場合、再ロードが開始される前にスタートアップにコピーするかどうかを示します。

Telnet ログインタイムアウト

デバイスへのログインを試行している間に、telnet 接続に使用されるタイムアウト値（秒単位）。

Telnet コマンドタイムアウト

telnet 接続でコマンドを実行しようとする間に使用されるタイムアウト値（秒単位）。

- b. [OK] をクリックします。

[デバイス再ロードタスク結果] ダイアログボックスが表示され、生成されたタスクは [エクスプローラ] タブのタスク フォルダに表示されます。 詳細については、「[リアルタイムでタスク結果を表示 \(P. 137\)](#)」を参照してください。

再ロード キャンセル タスクの作成

再ロード キャンセル タスクは、デバイスでスケジュールされた保留中の再起動をキャンセルするために使用されます。このタスクは Cisco IOS および Cisco IOS - SSH Capable デバイスに使用できます。

次の手順に従ってください:

1. [エクスプローラ] タブのデバイス ファミリで、Cisco IOS または Cisco IOS - SSH Capable デバイス ファミリからデバイスを選択します。
2. コンテンツ画面で [リスト] タブをクリックし、再ロード タスク用のデバイスを選択します。
3. ツールバーの [NCM タスクの作成] アイコンから [再ロード タスク]、[再ロード キャンセル タスク] を選択します。

[デバイスの選択: 再ロード キャンセル タスク] ダイアログ ボックスが表示されます。

注: 選択されたデバイスが [許可] タブに表示されない場合、[禁止] をクリックして、Network Configuration Manager タスクから無効化されているか必要な権限を持たないデバイスを表示させます。

4. 承認が必要な場合（[承認の要求] ボタンで示される）、以下の手順を実行します。
 - a. [承認の要求] をクリックします。
[承認必須] ダイアログ ボックスが表示されます。
 - b. ユーザを選択し、[タスク承認者] 用の電子メール アドレスを入力します。
 - c. (オプション) タスクの説明を指定します。
 - d. [OK] をクリックして、要求を生成します。

確認ダイアログ ボックスは、要求が正常に作成されたことを示します。電子メールのメッセージはタスク承認者に送信され、生成されたタスクは [エクスプローラ] タブのタスク フォルダに表示されます。

注: 電子メール設定の詳細については、「管理者ガイド」を参照してください。

- e. 承認ステータスを確認し、「[タスクの開始 \(P. 135\)](#)」の説明に従つてタスクを実行します。

注: 承認ワークフロー オプションの詳細については、「[ワークフローの設定 \(P. 33\)](#)」を参照してください。

5. 承認が必要でない場合は、以下のタスクのいずれかを実行します。

- [スケジュール] をクリックして、将来の実行に備えてタスクをスケジュールします。スケジューリングについては、「[タスクのスケジュール \(P. 131\)](#)」で説明されます。
- [保存] をクリックします。
タスクは将来の実行に備えて保存されます。この手順を終了します。
- [再ロード キャンセル タスクを今すぐ実行] をクリックします。
[デバイス再ロード キャンセル タスク結果] ダイアログ ボックスが表示され、生成されたタスクは [エクスプローラ] タブのタスク フォルダに表示されます。詳細については、「[リアルタイムでタスク結果を表示 \(P. 137\)](#)」を参照してください。

デバイス フームウェアのロード スクリプト

デバイス フームウェア ロード スクリプトは、フームウェア ロード タスク (CISCO-FLASH-MIB をサポートする Cisco デバイス用のみ) の MIB ベースの内部サポートの代わりに、デバイスで指定されたフームウェア イメージのロードを開始するために使用できます。スクリプトを使用する詳細については、「[Network Configuration Manager の拡張ユーティリティ \(P. 60\)](#)」を参照してください。

第 7 章: タスクの管理

このセクションには、以下のトピックが含まれています。

[グローバルコレクションとタスクの関連付け \(P. 127\)](#)

[バルクタスクのスケジュール \(P. 130\)](#)

[タスクの開始と停止 \(P. 134\)](#)

[タスク情報の表示 \(P. 137\)](#)

[タスクの状態とステータス値 \(P. 139\)](#)

グローバルコレクションとタスクの関連付け

タスクはグローバルコレクションと関連付けることができます。グローバルコレクションとタスクを関連付けることによって、実行時にタスクタイプをサポートするコレクションのすべてのメンバでタスクが実行されます。初期タスク作成中またはタスクがすでに存在するようになった後に、グローバルコレクションとタスクを関連付けることができます。

注: [NCM タスクにグローバルコレクションを含める] 権限は、ユーザがグローバルコレクションとタスクを関連付けるのに必要です。権限の詳細については、「[Network Configuration Manager 権限 \(P. 265\)](#)」を参照してください。

詳細情報:

[グローバルコレクション \(P. 27\)](#)

新しいタスクの関連付け

タスクを作成する場合、グローバルコレクションとタスクを関連付けることができます。

次の手順に従ってください:

1. [エクスプローラ] タブでグローバルコレクションノードを選択します。

定義されたグローバルコレクションのリストが、コンテンツ画面の [リスト] タブに表示されます。

注: グローバルコレクションが存在しない場合、続行する前に 1 つ作成する必要があります。 詳細については、「IT インフラストラクチャのモデリング/管理 - 管理者ガイド」を参照してください。

2. [リスト] タブで、タスクを関連付けるグローバルコレクションを選択します。

グローバルコレクションは強調表示され、[NCM タスクの作成] アイコンが有効化されます。

3. [NCM タスクの作成] アイコンをクリックし、作成するタスクを選択して、このグローバルコレクションに関連付けます。

タスク用の [デバイスの選択] ダイアログ ボックスが表示されます。

4. タスクに応じて、「[Network Configuration Manager のバルク タスク](#) (P. 105)」または「[ファームウェアアップロード](#) (P. 113)」で述べられたとおりにタスクの作成を続行します。

完了した場合

- 新しいタスクがグローバルコレクションの [情報] タブの NCM タスク サブビューに表示されます。
- 新しいタスクが [エクスプローラ] タブのタスク フォルダに表示されます。 タスク用の [情報] タブを表示する場合、タスクが関連付けられるグローバルコレクションがグローバルコレクション サブビューに表示されます。

タスクが実行される場合、実行時にタスク タイプをサポートするグローバルコレクションのすべてのメンバで実行されます。

既存タスクの関連付け

グローバルコレクションと既存のタスクを関連付けることができます。 また、[タスクの作成中に関連付ける](#) (P. 127) こともできます。 以下の手順は、別のグローバルコレクションを既存のタスクに追加またはコレクションを削除するために使用できます。

次の手順に従ってください:

1. [エクスプローラ] タブの [設定マネージャ] の下の [タスク] フォルダからタスクを選択します。
タスク用の情報がコンテンツ画面の [情報] タブに表示されます。
2. グローバルコレクションサブビューを展開します。
選択されたタスクと関連付けられているグローバルコレクションがテーブルに表示されます。
3. テーブルの上の [グローバルコレクションの追加/削除] アイコンをクリックします。
[タスクメンバエディタ] ダイアログボックスが表示されます。
4. [使用可能なグローバルコレクション] ペイン (右側) からグローバルコレクションを選択します。矢印を使用し、このタスクと関連付けられる [関連するグローバルコレクション] ペイン (左側) へ移動します。
[関連するグローバルコレクション] ペインにあるグローバルコレクションはこのタスクと関連付けられます。
5. [保存] をクリックして、後続の確認ダイアログボックスで [はい] をクリックします。
関連するグローバルコレクションがテーブルに表示されます。タスクが実行される場合、実行時にタスクタイプをサポートする、関連するグローバルコレクションのすべてのメンバで実行されます。

バルク タスクのスケジュール

バルク タスクはスケジュールできます。タスクの作成時またはタスクが実行された後（再利用可能なタスクの場合）のいずれかに、スケジューリングを実行できます。

次のタスクをスケジュールできます： [アップロード タスク] 、 [同期 タスク] 、 [スタートアップへの保存タスク] 、 [ファームウェア ロード タスク] および [再ロード キャンセル タスク] 。

注: 再ロード タスクはこのメカニズムを使ってスケジュールすることはできません。代わりに、デバイスの内部スケジューリング メカニズムが使用されます。再ロード操作を実行するためにスクリプトを定義する場合、スクリプトでは再ロード タスクをスケジュールするデバイスのスケジューリング メカニズムを活用する必要があります。 詳細については、「[設定スクリプトの入力 \(P. 67\)](#)」を参照してください。

タスクはスケジュールの 1 つのみに関連付けることができます。新しいスケジュールの指定時に既存のスケジュールがタスクにある場合、前のスケジュールが削除されます。繰り返しのタスクを手動で削除する必要があります。自動的にクリーンアップは実行されません。

タスクは基本的に配布されます。「ローカル」のタスクはそれぞれ、ローカル ランドスケープのローカル タイム ゾーンに基づいてスケジュールされた時間に実行されます。推奨されるベスト プラクティスは、同じタイム ゾーン 設定で動作しているすべての SpectroSERVER を持つことです。

[成功デバイスリスト] および [失敗デバイスリスト] テーブルの [完了時刻] 列には、タスク操作が特定のデバイスで試行されたタイミングが示されます。この機能によって、異なるタイム ゾーンで複数のランドスケープのある DSS でタスクが実行される時間を判断するのに役立ちます。

注: バルク タスクをスケジュールするには、Network Configuration Manager の NCM タスク スケジュール 権限が必要です。

再利用可能なタスク

再利用可能なタスクを定義すると、再定義しないでタスクを複数回保存および実行できます。また、繰り返しのスケジュールを作成し、事前に決められた時間で自動的にタスクを実行することもできます。

タスクをスケジュールする詳細については、「[タスクのスケジュール \(P. 131\)](#)」を参照してください。

注: 繰り返しのスケジュールのないタスクは、再利用可能なタスクとして自動的に作成されます。

[再利用可能タスク] オプションがタスク作成中に指定された場合、タスクは再利用可能として指定されます。

タスクは以下の領域で再利用可能として識別できます。

- コンテンツ画面のリストテーブルの [再利用可能] フィールド
- コンポーネント詳細画面の [情報] タブの [一般タスク情報] 内

タスクのスケジュール

タスクをスケジュールすることにより、タスクを定義し、それを実行する将来の日付と時間を指定できます。タスクをスケジュールし、1回限りまたは繰り返して実行します。タスク作成時にスケジュールをセットアップできます。[スケジュール] または [スケジュールの編集] ボタンを使用します。または、再利用可能なタスクについては、いつでもスケジュールをセットアップできます。

注: [ホスト設定] タブから実行されたタスクはスケジュールできません。

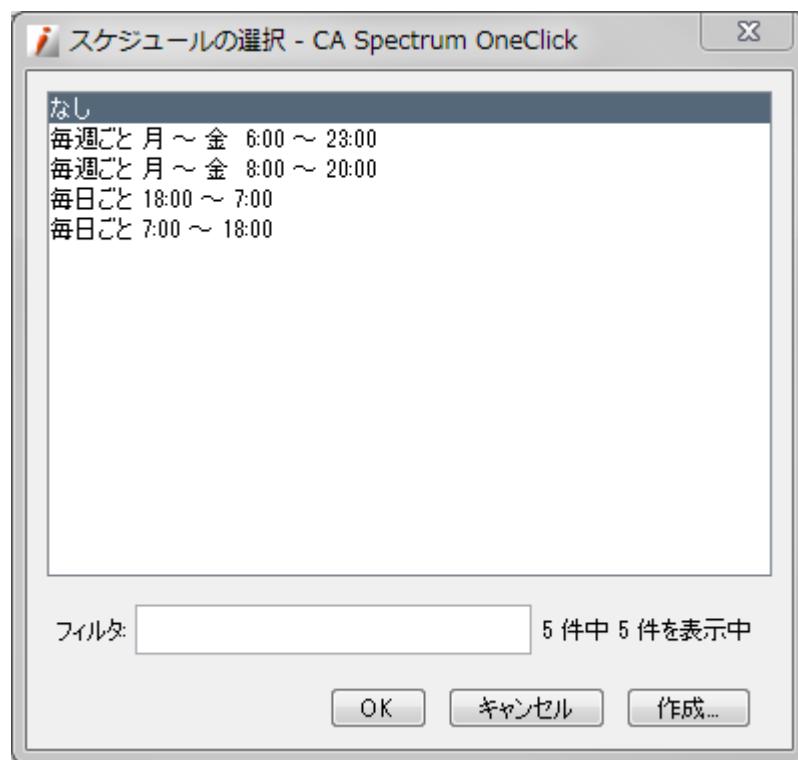
次の手順に従ってください:

1. 次のいずれかのタスクを作成するには、「[Network Configuration Manager バルクタスク \(P. 105\)](#)」および「[ファームウェアアップロード \(P. 113\)](#)」で概説された手順に従います: [アップロードタスク]、[同期タスク]、[スタートアップへの保存タスク]、[ファームウェアロードタスク]、および[再ロードキャンセルタスク]。

[スケジュール] または [スケジュールの編集] ボタンが、作成ダイアログボックスに表示され、ここで使用できます。

注: 承認ワークフローが有効な場合、タスクの作成中に [スケジュール] ボタンは使用できません。承認されたタスクのみをスケジュールできます。タスクが作成された後、スケジュールをセットアップする必要があります。手順は以下のとおりです。

2. [スケジュール] または [スケジュールの編集] ボタンを選択します。
[スケジュールの選択] ダイアログボックスは、以下のイメージのように表示されます。



3. 以下のいずれかの手順を実行します。

- デフォルトスケジュールを選択して、[OK]をクリックします。
- カスタムスケジュールを作成します。[作成]ボタンをクリックし、スケジュールオプションを指定して[OK]をクリックします。カスタムスケジュールがリストに追加されます。新しいスケジュールを選択して、[OK]をクリックします。

タスクがスケジュールされました。スケジュールが[スケジュール]ボタンの隣に表示されます。

注: タスク用のスケジュールを削除するには、[なし]のデフォルトスケジュールを選択します。

4. このタスクを複数回実行する場合、[再利用可能タスク]を選択します。前の手順で繰り返しのスケジュールを指定した場合、タスクは再利用可能なタスクとして作成される必要があります。

注: 再利用可能なタスクは自動的にクリーンアップされません。

5. 以下のいずれかの手順を実行します。

- タスクを保存します。スケジュールを指定しており、後で[タスク]フォルダの[リスト]タブからタスクを実行する場合、[保存]ボタンをクリックします。タスクは関連するスケジュール(ある場合)で作成されます。
- タスクを実行します。タスクをすぐに実行する場合、[実行]ボタンをクリックします。

タスクは保存され、[エクスプローラ]の[タスク]フォルダに、[スケジュール済みタスク]アイコンと共に表示されます。

スケジュール情報は、コンテンツ画面のリストテーブルの[スケジュール]フィールドおよびコンポーネント詳細画面の[情報]タブの[一般タスク情報]内で使用可能です。

また、以下のいずれかの理由で、タスクを作成した後にスケジュールを作成または変更することもできます。

- 繰り返しで実行するようにタスクをセットアップする前に、タスクを十分にテストします。
- 承認を必要とするタスクが承認されるまでスケジュールできないため、まずはタスクを作成して、承認されるのを待つ必要があります。
- サイトの状況は、スケジュール変更を必要とするように変更されました。

次の手順に従ってください:

1. [エクスプローラ] でタスクを選択し、コンテンツ画面で [リスト] タブを選択します。
拒否されたすべてのタスクが表示されます。
2. スケジュールを作成または変更するタスクを選択します。スケジューリングに適格なタスクは、以下の条件を満たしている必要があります。
 - タスクが実行されるには適格である必要があります。タスクが再利用可能なタスク（再利用可能 = はい）であるか、再利用可能でない場合、これはまだ実行されていません（非アクティブ状態）。
 - 承認ワークフローが有効な場合、タスクは承認状態である必要があります。

スケジュールできる場合、ツールバーの [スケジュール] ボタンはタスクに対して有効です。

注: [スケジュール] ボタンが有効でない場合は、適格性条件が満たされるかを確認します。
3. [スケジュール] ボタンをクリックします。
[スケジュールの作成] ダイアログボックスが表示されます。
4. スケジュールを選択または作成します。

タスクの開始と停止

このセクションでは、タスクを開始、停止、再開、および削除する方法について説明します。

タスクの開始

この手順では、すでに作成されたタスクを開始する方法について説明します。タスクがまだ実行されておらず再利用可能な場合、または再利用可能なタスクではなく、まったく実行されていない場合、タスクを開始できます。承認が有効な場合、タスクは [承認済み] の状態である必要があります。

注: 実行される前に、承認を必要とするどの設定変更タスクも承認される必要があります。

次の手順に従ってください:

1. [エクスプローラ] タブの [設定マネージャ] の下にあるタスク ビューからタスクを選択します。

2. コンテンツ画面で [リスト] タブを選択します。

タスクに関する情報はリストテーブルに表示されます。[状態] 列の [承認待機] の値は、要求が生成されているが承認されていないことを示します。[承認済み] の値は、要求が承認されており実行できることを示します。

3. 開始するタスクを選択します。

タスクを開始できる場合、[開始] ボタンは有効です。

4. [選択したタスクの開始] アイコンをクリックし、タスクを実行します。

タスクに情報が必要な場合は、そのタスクのセクションを参照してください。そうでない場合、タスクは開始され、[タスクの状態] の値が更新されます。

タスクによっては、結果ダイアログ ボックスが表示されます。詳細については、「[リアルタイムでタスク結果を表示 \(P. 137\)](#)」を参照してください。

タスクの停止

実行中のタスクを停止できます。

次の手順に従ってください:

1. [エクスプローラ] タブで [設定マネージャ] の下にある [タスク] を選択します。
2. コンテンツ画面で [リスト] タブをクリックし、タスクを選択します。
注: 実行中の状態にあるタスクのみを停止できます。
3. ツールバーの [選択したタスクの停止] アイコンをクリックします。
タスクは停止され、 [タスクの状態] の値が更新されます。

タスクの再開

タスクが停止されており、残存デバイスリストにデバイスが残っている場合、タスクは再開できます。タスクを再開する場合、Network Configuration Manager は残りリストにあるそれらのデバイスで操作を実行しようとするだけです。以前に成功または失敗し、残りリストから削除されたデバイスでは操作は再試行されません。

次の手順に従ってください:

1. [エクスプローラ] タブで [設定マネージャ] の下にある [タスク] を選択します。
2. コンテンツ画面で [リスト] タブをクリックし、再開するタスクを選択します。
注: [残り] 列に正の値で表されているように、デバイスが残っているタスクのみを再開できます。
3. ツールバーの [選択したタスクの再開] アイコンをクリックします。
タスクは開始され、 [開始] の値が更新されます。

タスクを削除

OneClick のタスクを削除できます。

注: 実行中または編集ロックされているタスクは削除できません。

次の手順に従ってください:

1. [エクスプローラ] タブで [設定マネージャ] の下にある [タスク] を選択します。
2. コンテンツ画面で [リスト] タブをクリックし、削除するタスクを選択します。
3. ツールバーの [選択したタスクの削除] アイコンをクリックします。
[削除の確認] ダイアログボックスが表示されます。
4. 削除するには、[はい] をクリックします。
選択されたタスクが削除されます。

タスク情報の表示

このセクションでは、作成および実行されたタスク用の情報を表示する方法について説明します。

リアルタイムでタスク結果を表示

アップロード、同期、スタートアップへの保存、ファームウェアロードタスク、または再ロードキャンセルタスクを開始した後、結果ダイアログボックスが表示されます。タスクの名前、状態、タイプ、およびステータス（保留、失敗、または成功）が、[結果] タブに表示されます。失敗した場合、結果が [失敗の原因] フィールドに表示されます。

注: タスクの統計は、10 秒間のポーリングサイクルで更新されます。

タスクが実行されている間、結果ダイアログ ボックスで以下を実行できます。

- [コンテンツ] タブをクリックし、アップロード中のコンテンツを表示します。
注: [コンテンツ] タブは、[アップロードタスク結果] ダイアログ ボックスおよび[ファームウェアロードタスク結果] ダイアログ ボックスのみで使用できます。
- [停止] をクリックし、タスクをキャンセルします。タスクは進行中のすべてのデバイスの処理を終了します。その後、残りのデバイスの処理も停止されます。
- [閉じる] をクリックし、バックグラウンドでタスクを実行します。

すべてのバルクタスクの重大な統計の表示

すべてのバルクタスクの重大な統計を同時に表示できます。

次の手順に従ってください:

1. [エクスプローラ] タブで [設定マネージャ] の下にある [タスク] を選択します。
2. コンテンツ画面で [リスト] タブを選択します。
すべてのバルクタスクの統計が表示されます。

バルクタスクの詳細な統計の表示

単一のバルクタスクの詳細な統計を表示するには、別の手順を実行します。

次の手順に従ってください:

1. [タスク] フォルダからタスクを選択します。
2. コンテンツ画面で [情報] タブをクリックします。
タスクの情報が表示されます。

タスクの状態とステータス値

[タスクの状態] (状態) および [タスク ステータス] の値は、タスクの実行における現在の段階を示します。タスク結果または統計を表示する場合、[タスクの状態] (状態) および [タスク ステータス] を使用できます。これらのビューにアクセスするには、「[タスク情報の表示 \(P. 137\)](#)」を参照します。

タスクの状態

[タスクの状態] (状態) の値には以下があります。

承認済み

承認ワークフロー モードはこのタスクに対して有効になっています。タスクは適切なタスク承認者により承認されており、実行できます。

承認待ち

承認ワークフロー モードはこのタスクに対して有効になっています。このタスクの要求は生成されていますが、まだ承認されていません。

完了

タスクは正常に実行されており、再利用可能です。繰り返しのスケジュールが設定され、少なくとも一度は実行されたことのあるタスクは、この状態になります。

完了 - 廃棄待ち

タスクは実行されており、再利用可能です。タスクは 24 時間以内にページされます。

拒否

承認ワークフロー モードはこのタスクに対して有効になっています。このタスクの要求は生成され、適切なタスク承認者によって拒否されました。

非アクティブ

タスクはスケジュールされていますが、まだ実行されていません。

初期化中

CA Spectrum 内のタスク準備が開始されています。

実行中

タスクは現在実行中です。この状態のタスクは停止できます。

停止中

タスクは開始され、ユーザによって停止されました。

タスクステータス

可能な [タスクステータス] 値を以下に示します。

失敗

タスクは正常に完了しませんでした。結果は [失敗の原因] フィールドに表示されます。

保留

タスクは現在実行中です。この状態のタスクは停止できます。

成功

そのタスクは正常に完了しました。

第 8 章: Network Configuration Manager の ポリシー

このチャプタでは、Network Configuration Manager のポリシーを作成および設定する方法について説明します。Network Configuration Manager ポリシーではコンフィギュレーションのコンテンツを監視し、デバイスコンテンツが準拠していることを確認します。

注: Network Configuration Manager のポリシーを設定する前に、設定をキャプチャしておくことをお勧めします。ネットワークでグローバル同期タスクをセットアップするには、「[グローバル同期タスク \(P. 83\)](#)」を参照してください。

このセクションには、以下のトピックが含まれています。

[Network Configuration Manager のポリシーについて \(P. 141\)](#)

[ポリシーの作成 \(P. 144\)](#)

[非準拠デバイスの修復 \(P. 167\)](#)

[ポリシーの管理 \(P. 169\)](#)

[ポリシー情報の表示 \(P. 172\)](#)

[複数行ブロック ポリシーの例 \(P. 174\)](#)

Network Configuration Manager のポリシーについて

Network Configuration Manager ポリシーは、デバイス ホスト設定のコンテンツを監視するために使用される条件を定義します。デバイス ホスト設定ファイルがキャプチャされるたびに、ポリシーが確認および比較されます。ポリシーに違反するデバイスではアラームを生成し、修復を受けることができます。

ポリシーを作成し、単一のデバイスおよびグローバルコレクションに適用することができます。グローバルコレクションに適用される場合、ポリシーはデバイス ファミリごとにすべてのグローバルコレクションメンバーに強制適用されます。グローバルコレクションをセットアップする詳細については、「[Network Configuration Manager およびグローバルコレクション \(P. 27\)](#)」を参照してください。

2つのタイプのポリシー（單一行ポリシーおよび複数行ブロック ポリシー）を作成できます。次のセクションで説明します。

注: Enterasys/Riverstone SSR デバイスで実行される設定キャプチャでは、ランニング コンフィギュレーションではなくスタートアップ コンフィギュレーションが提供されます。そのため、デバイスが Network Configuration Manager のポリシーに準拠しているかどうかを判断する場合、スタートアップ コンフィギュレーションが使用されます。SSR デバイスが Network Configuration Manager の設定アップロードを処理する方法の詳細については、「[Enterasys/Riverstone SSR デバイスによるアップロードタスクへの応答方法の決定 \(P. 108\)](#)」を参照してください。

單一行ポリシー

單一行ポリシーは、現在定義済みのホスト設定とポリシー定義を1行ずつ比較します。ホスト設定のデータの各行は、ポリシーに対して分析されます。設定全体にわたる單一のコマンドの存在を確認する場合に、このタイプのポリシーは役立ちます。

例

すべてのスイッチで http を有効にする必要があるという規制がサイトにあるとします。設定内の以下を使用してスイッチがオンラインになります。

```
#http configuration  
set ip http server disable  
set ip http port 80
```

このデバイスがサイト規制に準拠するには、「set ip http server disable」を「set ip http server enable」にする必要があります。この状況を識別し修正するには、單一行ポリシーを作成して、設定に「set ip http server enable」の行があるかどうかを確認できます。この行が設定にない場合、条件を修復できるようにアラームを生成することを指定できます。アラームからポリシー違反を表示できます。また、修正済みのコンテンツをアップロードするタスクをスケジュールすることによりデバイスを修復するオプションがあります。

複数行ブロック ポリシー

複数行ブロック ポリシーは、現在定義済みのホスト設定とポリシーを 1 ブロックずつ比較します。ポリシーは、ポリシーと現在のホスト設定の間に対応するブロックに一致させようとします。ブロックは開始と終了のタグで指定されます。制限を付けているブロック内のデータのみがポリシーによって分析されます。インターフェース設定などの設定テキストのブロックの設定を監視している場合、このタイプのポリシーが役立ちます。ほとんどのデバイスには複数のインターフェースがあり、個別のインターフェースに使用する一意の設定が同じ設定ファイルに表示されます。

ブロック ポリシーを強制適用する場合、使用可能な 2 つのオプションがあります。設定コンテンツは、ポリシー条件の事前定義済みセットと比較できます。また、設定履歴の前の設定または参照設定と比較できます。

前の設定または参照設定と比較する場合、変更、追加、または削除された行が識別されます。前の設定または参照設定との比較は、ブロックのコンテキストで発生する変更を強調表示するのに役立ちます。指定されたブロックの外部で発生する変更は、マスクされた変更または無関係な変更として示されます。

事前定義済みポリシー条件と比較する場合、条件に違反する行が強調表示されます。ブロック内で並べ替えられた行も強調表示される可能性があります。

例

説明に表示された「shutdown」という単語によって識別されている特定のインターフェースをシャットダウンするとします。以下の方法で複数行ブロック ポリシーを定義することによって、このようなデバイスを識別できます。

- 指定されたコンテンツとの比較。ポリシー定義として説明に「shutdown」を含まないすべてのインターフェースを検索できます。これにより、ポリシーの違反者として説明に「shutdown」を含むすべてのインターフェースを強調表示します。
- 別の設定との比較。キャプチャが発生するごとに新しくキャプチャされた設定を参照設定と比較することによって、コンテンツを監視できます。「shutdown」がインターフェース用の説明に追加される場合、それは参照設定に一致しないため、ポリシーの違反者として強調表示されます。

デバイスが識別された後、シャットダウンコマンドは修正アクションに推奨されたアップロードの一部として、シャットダウン用にマークされたインターフェースに対して容易に発行できます。

この例の実装については、「[複数行ブロック ポリシーの例 \(P. 174\)](#)」に詳細が述べられています。

ポリシーの作成

ポリシーは、デバイスホスト設定のコンテンツを監視するために使用する条件を定義します。ポリシーを作成し、単一のデバイスおよびグローバルコレクションに適用することができます。2つのタイプのポリシー（單一行ポリシーおよび複数行ブロック ポリシー）を作成できます。以下の手順では、Network Configuration Manager ポリシーを作成する方法について説明します。

注: 例は「[複数行ブロック ポリシーの例 \(P. 174\)](#)」で提供されています。

次の手順に従ってください:

1. [エクスプローラ] タブで単一のデバイスを選択します。
デバイス用の情報がコンテンツ画面の [情報] タブに表示されます。
2. ネットワーク設定ポリシー サブビューを展開します。
ネットワーク設定ポリシーテーブルが表示されます。
3. [ポリシーの作成] アイコンをクリックします。
[ポリシー タイプの選択] ダイアログ ボックスが表示されます。
4. 作成する以下のポリシーのタイプをクリックします。
 - **單一行ポリシー。** 一度に設定の單一行のみが比較されるポリシーを作成します。 [NCM プロファイルの作成] ダイアログ ボックスが表示されます。
 - **複数行ブロック ポリシー。** ブロックに制限を付けることによって、ホストの設定が比較されるポリシーを作成します。 [NCM ブロック ポリシーの作成] ダイアログ ボックスが表示されます。
5. [ポリシー ID] セクションで、ポリシーの名前および説明を入力します。

6. ダイアログボックスの [ポリシー条件] セクションで、以下のようにポリシー条件を設定します。
 - 単一行ポリシーについては、「[単一行ポリシー条件 \(P. 147\)](#)」を参照してください。
 - 複数行ブロックポリシーについては、「[複数行ブロックポリシー条件 \(P. 147\)](#)」を参照します。
7. ダイアログボックスの [ポリシーアクション] セクションで、以下の手順を実行します。
 - a. 以下のようにアラーム条件を入力します。

違反時にデバイスにアラーム

デバイスがこのポリシーに非準拠である場合、デバイスにアラームを生成するかどうかを示します。これは各非準拠デバイスの単一アラームであり、[アラーム] タブで表示可能です。アラームの重大度（重大、メジャー、マイナー）を選択することもできます。このオプションを使用するには、ポリシーを有効にする必要があります。

違反時にポリシーにアラーム

少なくとも 1 つのデバイスが非準拠である場合、ポリシーにアラームを生成するかどうかを示します。これは単一ポリシーでの単一アラームであり、[アラーム] タブで表示可能です。アラームの重大度（重大、メジャー、マイナー）を選択することもできます。このオプションを使用するには、ポリシーを有効にする必要があります。

- b. 修正アクションのために推奨されるアップロードを入力します。
 - 単一行ポリシーについては、「[単一行ポリシーの修正アクション \(P. 156\)](#)」を参照してください。
 - 複数行ブロックポリシーについては、「[複数行ブロックポリシーの修正アクション \(P. 156\)](#)」を参照します。
 - c. [スタートアップへのコミット] オプションを選択し、新しいコンテンツがマージされた後に、ランニングコンフィギュレーション全体をスタートアップコンフィギュレーションにコピーするかどうかを示します。
8. [保存] をクリックします。

[NCM ポリシーの保存] または [NCM ブロックポリシーの保存] ダイアログボックスが表示されます。

9. [続行] をクリックします。

注: [終了] をクリックするとポリシーは非アクティブ化され、デバイスがこのポリシーに準拠しているかどうかは確認されません。ただし、[エクスプローラ] タブの [ポリシー] から選択することにより、後でポリシーを有効化できます。

[NCM ポリシーのテスト] または [NCM ブロック ポリシーのテスト] ダイアログ ボックスが表示されます。CA Spectrum データベース内の 1 つ以上のデバイス用に格納された設定に対して、ポリシーがテストされます。ポリシー結果（必要に応じて修正アクションを含む）は、確認用に表示されます。ポリシーのテスト中は、アラームは生成されません。

10. デバイスが非準拠の場合

- デバイスが非準拠である理由に関する情報を得るために [違反を表示] をクリックします。

[違反を表示] ダイアログ ボックスが表示されます。 [違反を表示] ダイアログ ボックスの詳細については、「[単一行ポリシー違反 \(P. 159\)](#)」または「[複数行ブロック ポリシー違反 \(P. 160\)](#)」を参照してください。

- [閉じる] をクリックします。

11. [修復] をクリックし、正しいコンテンツをデバイスにアップロードおよびマージしてポリシーに準拠させます。 詳細については、「[ポリシー テーブルから非準拠デバイスを修復 \(P. 167\)](#)」を参照してください。

注: 修正アクションが提供されている場合にのみ修復は有効です。

12. [ポリシーの有効化] を選択すると、データベース内の設定を確認することにより、および該当する場合は必要に応じてアラームを生成することにより、即座にこのポリシーが適用されます。

注: [ネットワーク設定ポリシー] ダイアログ ボックスからポリシーを有効化（または無効化）することもできます。 詳細については、「[ポリシー テーブルからポリシーの有効化および無効化 \(P. 170\)](#)」を参照してください。

13. [完了] をクリックします。

ポリシー条件

指定できるポリシー条件のタイプは、單一行ポリシーと複数行ブロックポリシーで異なります。このセクションでは、定義したポリシーのタイプに従ってポリシー条件を指定する方法について説明します。このセクションには、以下のトピックが含まれます。

- [單一行ポリシー条件 \(P. 147\)](#)
- [複数行ブロック ポリシー条件 \(P. 147\)](#)
- [\[ポリシー条件\] ダイアログ ボックス \(P. 153\)](#)

單一行ポリシー条件

單一行ポリシーの比較条件を指定するには、以下の手順に従います。

單一行ポリシーの条件を指定する方法

1. [ポリシー条件] セクションの [NCM ポリシーの作成] ダイアログ ボックスで [追加] をクリックし、比較の条件を作成します。
[ポリシー条件] ダイアログ ボックスが開きます。
2. [\[ポリシー条件\] ダイアログ ボックス \(P. 153\)](#) の説明に従って、ポリシー条件を設定します。
[ポリシー条件] ダイアログ ボックスが完了した後、新しい比較の条件がテーブルに表示されます。
3. さらに条件を追加または既存の条件を変更するには、[追加]、[編集] および [削除] ボタンを使用します。

このダイアログ ボックスの残り（ポリシーの保存中を含む）は、「[ポリシーの作成 \(P. 144\)](#)」で説明されています。

複数行ブロック ポリシー条件

複数行ブロック ポリシーを定義している場合、条件の 2 つのタイプ（ブロック定義条件および比較条件）を指定する必要があります。ブロック定義条件ではブロックの開始および終了を構成するものを定義します。比較条件は現在のホスト設定に対する比較に使用されるコンテンツを定義します。

このセクションではこの条件を定義する方法について説明し、以下のトピックが含まれます。

- [ブロックについて \(P. 148\)](#)
- [複数行ブロック ポリシー条件の指定 \(P. 149\)](#)
- [指定されたコンテンツと比較 \(P. 150\)](#)
- [ブロック一致の比較対象: 参照設定または前の設定 \(P. 152\)](#)

ブロックについて

複数行ブロック ポリシーを使用する場合、デバイス用のホスト設定ファイルのブロックを構成するものを確認する必要があります。Cisco IOS - SSH Capable デバイスの以下の例では、以下に似たブロックが各インターフェースに存在しています。このブロックは、「*interface name*」の行およびコメント文字「!」で区切られます。

```
interface Loopback0
description "test 123"
ip address 138.42.96.6 255.255.255.255
ip pim sparse-dense-mode
no ip route-cache cef
no ip route-cache
ipv6 address 2002:8A2A:5E12:8A2A:6006::1/128
ipv6 enable
ipv6 rip IPv6-1 enable
!
```

ポリシーを定義する場合、この情報が使用されます。ブロック ポリシー用語で、このブロックは以下によって定義されます。

開始タグ : *interface name* (名前)

終了タグ : !

ブロックの開始および終了を構成するものを定義するには、テキストまたは正規表現のいずれかを使用できます。開始または終了のタグとして適格であるかを判断する場合、2つのオプションの違いについて、以下で説明します。

注: [開始タグ] および [終了タグ] として定義された値は、ブロックの一部として含まれます。

テキストの使用

テキストを使用する場合、一致するテキストが含まれる行全体がそのフィールドに一致します。たとえば、テキストタイプの「interface」を開始タグとして使用する場合、「interface」という単語が含まれるすべての行に一致し、ブロック用の開始行として見なされます。

正規表現(Regex)の使用

正規表現を使用する場合、正規表現パターン（および行全体ではない）の完全一致のみがこのフィールドに一致します。たとえば、終了タグとして「interface abc」を指定した場合、「interface abc」までのコンテンツのみが、ブロックの終了として見なされます。代わりに「interface abc.*」を指定した場合（ここでの「.*」は正規表現のワイルドカードのパターンであり、1列の中でどの文字にも一致します）、「interface abc」に一致する行全体がブロックの終了として見なされます。

複数行ブロック ポリシー条件の指定

以下の手順では、複数行ブロック ポリシーの条件を指定する方法について説明します。

次の手順に従ってください:

1. [ポリシー条件] セクションの [NCM ブロック ポリシーの作成] ダイアログボックスで、以下のブロック定義条件を指定します。

ブロックの開始および終了を構成するものを定義するには、テキストまたは正規表現のいずれかを使用できます。2つのオプションの違いの追加説明については、「[ブロックについて \(P. 148\)](#)」を参照してください。

注: [開始タグ] および [終了タグ] として定義された値は、ブロックの一部として含まれます。

開始タグ

比較に使用されるブロックの開始を指定する文字を指定します。ブロックの開始を識別するために、ポリシーはホスト設定内でこの区切り文字タグを探します。テキストまたは正規表現のボタンの選択で示されるとおり、値はテキスト形式または正規表現になります。以下の例は「interface」を表す正規表現です。

(?m)^interface .*

この例を使用して、ポリシーは「interface」で始まる行を探します。

終了タグ

比較に使用されるブロックの終了を指定する文字を指定します。ブロックの終了を識別するために、ポリシーはホスト設定内でこの区切り文字タグを探します。[テキスト] または [正規表現] ボタンの選択で示されているとおり、値はテキスト形式または正規表現になります。以下の例は、「!」という文字を表す正規表現です。

(?m)^!.*

この例を使用して、ブロックの終了を示すために、ポリシーはブロックの開始の後にある最初のコメント文字（「!」）を探します。

2. [比較条件] セクションで、以下のいずれかのオプションを選択します。

- 指定されたコンテンツと比較

ポリシーがこのポリシーで指定されたユーザ定義のコンテンツに対して現在のホスト設定を比較することを指定します。 詳細については、「[指定されたコンテンツと比較 \(P. 150\)](#)」を参照してください。

- ブロック一致の比較対象

ポリシーが前の設定または参照設定からのコンテンツと現在のホスト設定を比較することを指定します。 詳細については、「[ブロック一致の比較対象: 参照設定または前の設定 \(P. 152\)](#)」を参照してください。

このダイアログ ボックスの残り（ポリシーの保存中を含む）は、「[ポリシーの作成 \(P. 144\)](#)」で説明されています。

指定されたコンテンツと比較

複数行ブロック ポリシーを定義する場合、現在の設定の各ブロックで確認されるコンテンツを明示的に指定できます。 この手順では、複数行ブロック ポリシーでユーザ定義の条件をセットアップする方法について説明します。

ユーザ定義の比較条件をセットアップする方法

1. [指定されたコンテンツと比較] オプションが選択された [NCM ブロック ポリシーの作成] ダイアログ ボックスで、[順序] を指定します。使用可能なオプションは以下のとおりです。

順序なし

現在のホスト設定と比較する場合、考慮されない条件の順序を示します。ポリシーの違反はコンテンツのみに基づいて発生します。

順序の保持(追加行を許可)

指定されたコンテンツがポリシーに準拠するように指定された順序で表示される必要があることを示します。ただし、追加のコンテンツは指定されたコンテンツの間に散在することを許可されます。指定されたコンテンツの一部が設定に存在しない場合、または異なる順序で存在する場合、ポリシー違反が発生します。ポリシーは一致しない行を無視します。

順序の保持(追加行なし)

ポリシーに準拠するために、指定されたコンテンツは指定された順序で隣り合うように表示される必要があると示します。設定ブロックが指定されたコンテンツと完全に一致しない場合、ポリシー違反が発生します。指定されたコンテンツによって明示的に定義されていないブロック コンテンツの追加行では、ポリシー違反が発生します。

2. [追加] をクリックし、比較の条件を作成します。
[ポリシー条件] ダイアログ ボックスが表示されます。
3. [\[ポリシー条件\] ダイアログ ボックス](#) (P. 153) の説明に従って、ポリシー条件を設定します。
[ポリシー条件] ダイアログ ボックスを閉じた後、新しい比較の条件がテーブルに表示されます。ホスト設定と比較時に保持される順序を指定している場合、テーブル内の条件の順序が使用されます。
4. さらに条件を追加または既存の条件を変更するには、[追加]、[編集] および [削除] ボタンを使用します。

ブロック一致の比較対象: 参照設定または前の設定

複数行ブロック ポリシーを定義する場合、ポリシーが現在のホスト設定を以前にキャプチャされた設定または参照設定として保存されたコンテンツと比較することを指定できます。コンテンツはブロックごとに比較されます。この手順では、コンテンツを参照または以前にキャプチャされた設定のいずれかと比較するポリシーをセットアップする方法について説明します。

注: ポリシーをテストする場合、参照設定または前の設定がデバイス用に存在する必要があります。そうでない場合、テスト不可のポリシー ステータスの結果となります。

参照設定または前の設定とコンテンツを比較する方法

1. [ブロック一致の比較対象] オプションが選択された [NCM ブロック ポリシーの作成] ダイアログ ボックスで、コンテンツを比較する設定のタイプを指定します。使用可能なオプションは以下のとおりです。

前の設定

現在のホスト設定が最も新しくキャプチャされた設定とブロックごとに比較されることを示します。

参照設定

現在のホスト設定が参照として指定された設定とブロックごとに比較されることを示します。参照設定を設定する詳細については、「[参照設定の指定 \(P. 91\)](#)」を参照してください。

参照設定または前の設定

現在のホスト設定が保存された設定とブロックごとに比較されることを示します。最初に、ポリシーは参照設定を探します。参照設定が特定のデバイスに設定されていない場合、ブロック コンテンツは以前の既知の設定と比較されます。

注: ポリシーのテスト時に参照設定または前の設定がデバイス用に存在しない場合、テスト不可のポリシー ステータスの結果となります。

2. (オプション) 以下の手順を実行して、ブロック ID を指定します。

ブロック ID は 2 つの設定間にに対応するブロックに一致させるために使用されます。ブロック内から特定のテキストを選択して、ブロック ID として使用できます。たとえば、2 つの設定間で「interface Loopback n 」とラベルの付いたインターフェースを比較するには、ブロック ID として「interface Loopback.*」を特定する必要があります。

ブロック ID が指定されていない場合、ブロックの最初の行がブロック ID として使用されます。ほとんどの場合、このデフォルトは 2 つの設定間で一致するブロックを識別するのに十分です。

- a. [詳細設定] をクリックします。

[ブロック ID の指定] ダイアログ ボックスが表示されます。

- b. ブロック ID および値がテキストまたは正規表現のどちらであるかを指定します。

「interface」で始まる対応する行に一致する正規表現の例を以下に示します。

```
(?m)^interface .*
```

対応するブロックに一致させるためにインターフェースの名前のみ（行全体ではなく）が使用される場合に、「interface name」を表す正規表現の例を以下に示します。

```
(?m)^interface ([a-z]|A-Z|0-9|/)*
```

注: 正規表現を使用する場合、正規表現をキャプチャするグループはブロック ID を選択するために活用されます。これは高度な正規表現の概念です。正規表現を使用する場合、キャプチャ グループ 1 がブロック ID として使用されます。この例では、グループ 1 は ([a-z]|A-Z|0-9|/)* であり、インターフェースの名前を識別します。

複数ブロック ポリシーでテキストおよび正規表現を使用する詳細については、「[ブロックについて \(P. 148\)](#)」を参照してください。

- c. [OK] をクリックします。

[ブロック ID] ダイアログ ボックスが閉じます。

[ポリシー条件] ダイアログ ボックス

この手順では、[ポリシー条件] ダイアログ ボックスを完了する方法について説明します。これは單一行および複数行ブロック ポリシーの比較条件を定義するために使用されます。ユーザが特定するコンテンツは、デバイスのホスト設定ファイルがキャプチャされるたびに、確認および比較されます。[ポリシー条件] ダイアログ ボックスは、[NCM ポリシーの作成] ダイアログ ボックスから呼び出されます。

[ポリシー条件]ダイアログ ボックスを使用して条件を定義する方法

1. ポリシーの比較タイプを選択します。利用可能な比較タイプは以下のとおりです。

指定の行を含む

ホスト設定ファイルに、指定されたすべての行が含まれることを示します。条件を満たす場合、ポリシーに準拠しており、許可されます。

指定の行を含まない

ホスト設定ファイルに、指定された行が含まれないことを示します。条件を満たす場合、ポリシーに準拠しており、許可されます。

指定の語句を含む

ホスト設定ファイルに、これらの語句や記号が含まれることを示します。条件を満たす場合、ポリシーに準拠しており、許可されます。

指定の語句を含まない

ホスト設定ファイルに、これらの語句や記号が含まれないことを示します。条件を満たす場合、ポリシーに準拠しており、許可されます。

指定の正規表現に一致する

ホスト設定ファイルが、これらの正規表現に一致することを示します。一致する場合、ポリシーに準拠しており、許可されます。

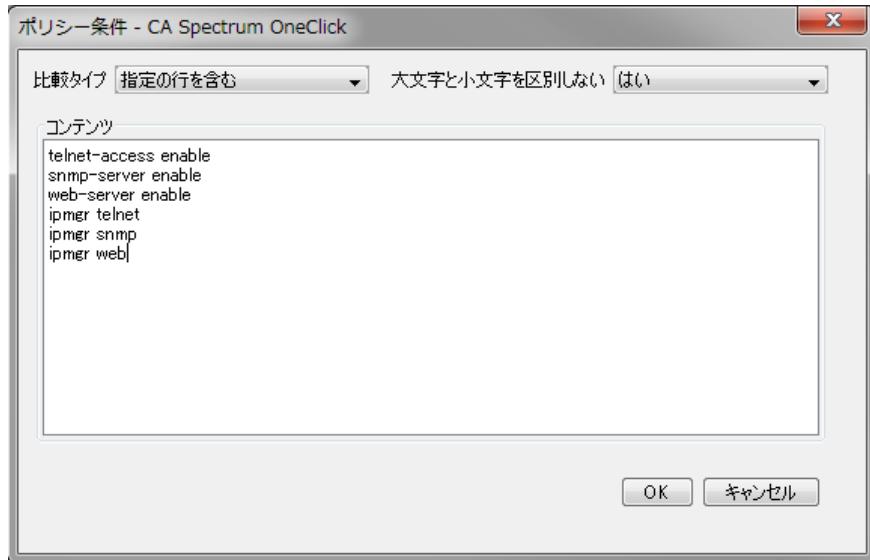
指定の正規表現に一致しない

ホスト設定ファイルが、これらの正規表現に一致しないことを示します。一致しない場合、ポリシーに準拠しており、許可されます。

2. 入力するコンテンツの大文字または小文字を無視するかどうかを指定します。

注: 正規表現を使用する場合、この設定は使用できません。

3. [コンテンツ] ボックス内をクリックし、コンテンツ（全行、サブ文字列、または正規表現）を入力します。以下はその一例です。



4. [OK] をクリックします。

[ポリシー条件] ダイアログ ボックスが閉じ、新しい条件がテーブルに表示される [NCM ポリシーの作成] または [NCM ブロック ポリシーの作成] ダイアログ ボックスに戻ります。

修正アクションのために推奨されるアップロード

修正アクションのために推奨されたアップロードのセットアップは、單一行と複数行ブロック ポリシーでわずかに異なります。このセクションでは、定義されたポリシーのタイプに従って、修正アクションを設定する方法について説明します。このセクションには、以下のトピックが含まれます。

- [單一行ポリシーの修正アクション \(P. 156\)](#)
- [複数行ブロック ポリシーの修正アクション \(P. 156\)](#)

單一行ポリシーの修正アクション

單一行ポリシーの修正アクションのために推奨されるアップロードには、デバイスをポリシーに準拠させる、ランニングコンフィギュレーションに一度マージされたコンテンツの指定が含まれます。この手順では、このコンテンツをセットアップする方法について説明します。

單一行ポリシーの修正アクションを入力する方法

1. [修正アクションのための推奨アップロード] グループの下にある、[編集] をクリックします。
注: [開く] をクリックしてテキストファイルからコンテンツをインポートすることもできます。
[修正アクションの編集] ダイアログボックスが表示されます。
2. 非準拠デバイスを修復する1行または複数行を入力します。これはデバイスをこのポリシーに準拠させる、ランニングコンフィギュレーションに一度マージされたコンテンツです。
3. [OK] をクリックします。
[修正アクションの編集] ダイアログボックスが閉じ、修正行が表示されます。

複数行ブロックポリシーの修正アクション

複数行ブロックポリシーの修正アクションのために推奨されるアップロードには、デバイスをポリシーに準拠させる、ランニングコンフィギュレーションに一度マージされたコンテンツの指定が含まれます。性質によりブロックポリシーが非準拠データの複数ブロックまたは発生を処理するため、それに応じてこれを処理するために修正アクションをセットアップする必要があります。この手順では、このコンテンツをセットアップする方法について説明します。

複数行ブロック ポリシーの修正アクションを入力する方法

- 違反が発生した各ブロックに影響を与える修正アクションを必要とする場合、[各違反ブロックに対して繰り返す] を選択します。チェックを解除した場合、修正アクションは最初に違反しているブロックのみにそのままアップロードされます。
- [修正アクションのための推奨アップロード] グループの下にある、[編集] をクリックします。

注: [開く] をクリックしてテキストファイルからコンテンツをインポートすることもできます。

[修正アクションの編集] ダイアログ ボックスが表示されます。

- 非準拠デバイスを修復する 1 行または複数行を入力します。これはデバイスをこのポリシーに準拠させる、ランニング コンフィギュレーションに一度マージされたコンテンツです。[抽出されたコンテンツの挿入] ボタンを使用し、修正アクションに <extracted_text> タグを挿入します。ポリシーが実行された場合、これはブロック固有のコンテンツで置換されます。修正アクションの例を以下に示します。

```
interface <extracted_text>
description "policy violation detected on <extracted_text> by Spectrum"
!
```

重要: 特に修復アクションが繰り返される場合、修復テキストは有効であり、完全なデバイス設定ステートメントである必要があります。たとえば、前の例の終了から「!」が省略された場合、修正アクションは正しく実装されない可能性があり、予期しない結果が発生する可能性があります。これはステートメントが正しく終了されないためです。説明は新規行の文字または「!」の文字を含む新しい行で終了する必要があります。

- [抽出されたコンテンツの設定] をクリックします。
[抽出されたコンテンツの編集] ダイアログ ボックスが表示されます。
- 各ブロックから抽出されるコンテンツを入力し、テキストまたは正規表現 (Regex) のいずれかを選択します。
 - テキストの場合、<extracted_text> タグが修正アクションで見つかる任意の場所に、この値が挿入されます。
 - 正規表現の場合、<extracted_text> タグが修正アクションで見つかる任意の場所に、評価された正規表現から返された値が挿入されます。

「interface *name*」を表す正規表現の例を以下に示します。

(?m)^interface ([a-z]|A-Z|0-9||/|)*

この例を使用して、ポリシーは各ブロックからインターフェースの名前を抽出し、修正アクションに挿入します。

注: 複数ブロック ポリシーでのテキストおよび正規表現を使用する詳細については、「[複数行ブロック ポリシー \(P. 143\)](#)」を参照してください。

6. [OK] をクリックします。

[修正アクションの編集] ダイアログ ボックスが閉じ、修正行が表示されます。

違反を表示

デバイスが非準拠である場合、[違反を表示] ダイアログ ボックスには理由に関する情報が提供されます。呼び出されるダイアログ ボックスおよび示される情報は、ポリシー定義に基づいて変わります。このセクションには、以下のトピックが含まれます。

- [単一行ポリシー違反 \(P. 159\)](#)
- [複数行ブロック ポリシー違反 \(P. 160\)](#)

單一行ポリシー違反

すべての單一行ポリシーに対する違反は、[違反を表示] ダイアログ ボックスに表示されます。

以下の例では、デバイスの設定に含まれていないため、ポリシー違反が発生している必要な特定のコマンドが表示されます。

The screenshot shows a window titled "Violation Display - CA Spectrum OneClick". The main pane displays a configuration file with several lines highlighted in red, indicating they are violations. The highlighted lines include:

```
!
! Last configuration change at 11:11:28 EST Mon Jun 10 2013 by admin
!
version 12.2
no service pad
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
!
hostname cis7204-96.6
!
boot-start-marker
boot system disk0:c7200-adventuresek9-mz.122-33.SRE4.bin
boot system disk0:c7200-jk9s-mz.124-25e.bin
warm-reboot count 10 uptime 10
boot-end-marker
!
```

Below the configuration file, there is a status bar with the text "行の合計数: 644 違反行: 0 現在の行: 0 次へ 前へ".

The bottom pane is titled "現在のブロックの欠落行: 6" and contains the following red-highlighted text:

```
telnet-access enable
snmp-server enable
web-server enable
ipmgr telnet
ipmgr snmp
ipmgr web
```

At the bottom right of the dialog box is a "閉じる" (Close) button.

すべての單一行ポリシーの [違反を表示] ダイアログ ボックスには、以下の情報が含まれます。

設定

任意の違反が発生した行を強調表示して、その全体でキャプチャされたホスト設定を表示します。

行の合計数

設定ファイル内の行の合計数を提供します。

違反行

ポリシーに違反する行の合計数を提供します。

現在の行

設定ファイル内の現在の場所を提供します。

次へ

次の違反にすぐに進めます。

前へ

前の違反に戻れます。

現在のブロックの欠落行: *total_number_of_lines*

設定ファイルで見つからなかったポリシーで定義された行を表示します。

注: 単一行ポリシーの場合、1つのブロックのみです。

複数行ブロック ポリシー違反

複数行ブロック ポリシーで比較に使用できる2つのタイプの条件があります。ユーザ定義の条件および保存された設定からのコンテンツです。そのため、表示される [違反を表示] ダイアログ ボックスは、表示される違反コンテンツによって異なります。

特定のコンテンツと比較した時の違反

ユーザ定義の条件が複数行ブロック ポリシーの比較に使用される場合、違反は [違反ブロックの表示] ダイアログ ボックスに表示されます。

現在のホスト設定がユーザ定義の条件と比較される、複数行ブロック ポリシーの [違反ブロックの表示] ダイアログ ボックスの例を以下に示します。

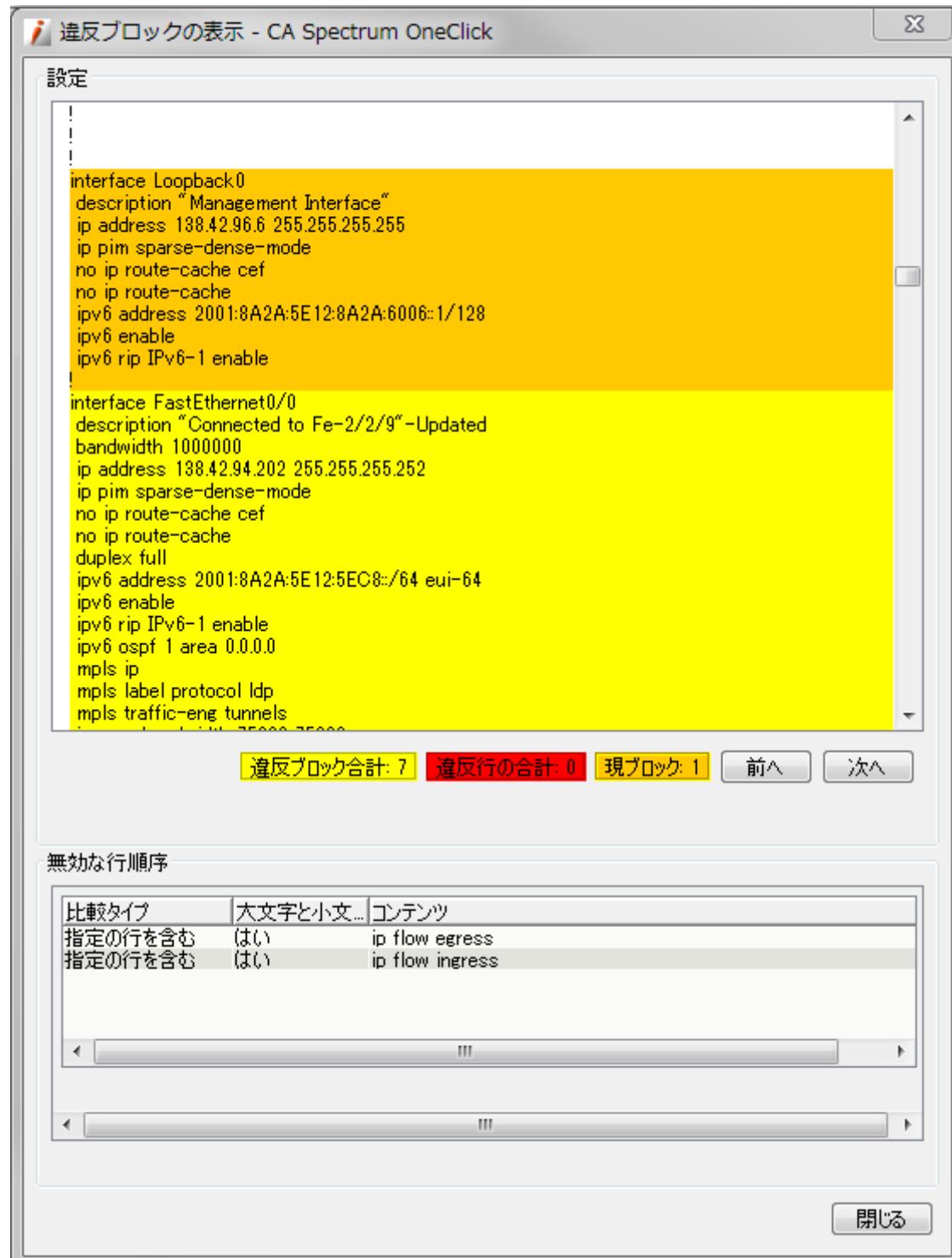
この例では、各インターフェース設定に「`duplex auto`」がなく、「`no ip route-cache`」があることを確認するために、ポリシーをセットアップしています。違反は以下のように特定されます。



次の例では、以下のコマンドが表示され、また以下の順序で表示される場合に、設定は準拠しているとするようにポリシーはセットアップされています。

```
ip flow egress  
ip flow ingress
```

コマンドが表示されますが、以下のイメージのとおり正しい順序でないため、現在の設定はこのポリシーに違反します。



[違反ブロックの表示] ダイアログ ボックスには、違反に応じて以下の情報が含まれる場合があります。

設定

任意の違反が発生した行を以下のように強調表示して、その全体でキャプチャされたホスト設定を表示します。

- **赤** - これらの行には違反が含まれます。
ブロックは色によって識別できます。
- **オレンジ** - これらの行は現在のブロックを構成します。
- **黄色** - これらの行は現在のブロック以外のブロックに含まれています。

違反ブロック合計

違反を含むブロックの合計数を提供します。

違反行の合計

ポリシーに違反する行の合計数を提供します。

現ブロック

設定ファイル内の現在の場所を提供します。区別できるブロックは識別用に番号が付けられています。

前へ

違反を含む前のブロックに戻ることができます。

次へ

違反を含む次のブロックにすぐに進むことができます。

現在のブロックの欠落行: *total_number_of_lines*

設定ファイルで見つからなかったポリシーで定義された行を表示します。

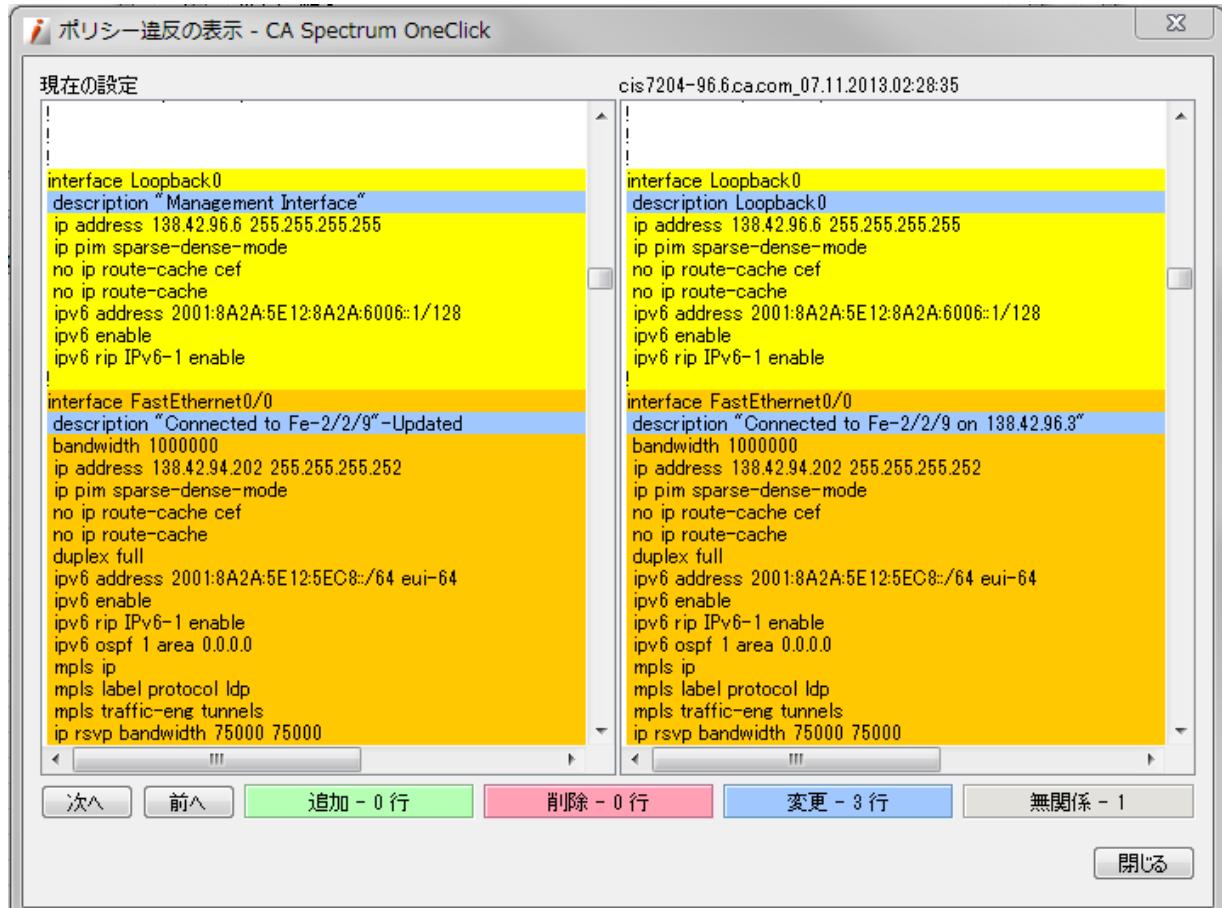
無効な行順序

設定ファイルの表示順に違反しているコンテンツ条件を表示します。

別の設定と比較した時の違反

保存された設定が複数行ブロック ポリシーの比較に使用される場合、違反は [ポリシー違反の表示] ダイアログ ボックスに表示されます。

現在のホスト設定が参照設定と比較され、行が変更された（そのため、ポリシー違反が発生している）場合、複数行ブロック ポリシーの [ポリシー違反の表示] ダイアログ ボックスの例を以下に示します。



現在のホスト設定は左ペインにあり、参照設定は右側に表示されます。2つの設定の差異は以下のキーに従って強調表示されます。

差異を含むブロックは全体に強調表示され、以下の色で区別できます。

- 黄色 - 違反が発生しているブロックを構成する行を表します。
- オレンジ - 違反が発生しているブロックを構成する行を表します。

差異を示す個々の行は、以下のように示します。

- 緑 - 追加された行を表します。
- 赤 - 削除された行を表します。
- 青 - 変更された行を表します。
- 灰色 - 異なる行ですが、制限を付けるブロックの外にあります。

[次へ] または [前へ] をクリックし、ファイル内の差異間を移動します。

非準拠デバイスの修復

ポリシーのセットアップ時に非準拠デバイスを修復するのに加え、違反が発生した後に、非準拠デバイスの修復を開始することもできます。このセクションには、以下のトピックが含まれます。

- [ポリシー テーブルからの非準拠デバイス修復 \(P. 167\)](#)
- [ポリシー違反アラームからの非準拠デバイスの修復 \(P. 168\)](#)

ポリシー テーブルからの非準拠デバイス修復

単一のデバイスまたはグローバルコレクションを選択して、ポリシー テーブルからポリシーを確認および修復することができます。たとえば、非準拠デバイスを修復できます。

次の手順に従ってください:

1. [エクスプローラ] タブで、個々のデバイスまたは設定済みポリシーのあるグローバルコレクションを選択します。
2. コンテンツ画面で [情報] タブを選択します。
デバイスまたはグローバルコレクションに関する情報が表示されます。
3. ネットワーク設定ポリシーを展開します。
ネットワーク設定ポリシー テーブルが表示されます。非準拠デバイスのあるポリシーは、[違反者] 列の値がゼロ以外になります。
4. 非準拠デバイスがあるポリシーを選択し、[修復ダイアログ ボックスを開く] アイコンをクリックします。
[違反デバイスを修復] ダイアログ ボックスが表示されます。

5. [コンテンツ] タブをクリックし、修復を実行するためにアップロードするコンテンツを表示します。
6. [違反を表示] をクリックして、各デバイスの違反を表示します。
7. [修復] をクリックします。
[タスクを作成しています] ステータス ボックスが表示されます。
[アップロードタスク結果] ダイアログ ボックスには、操作の結果が表示されます。

ポリシー違反アラームからの非準拠デバイスの修復

違反を表示して正しいコンテンツをデバイスにアップロードまたはマージし、[アラーム詳細] タブのポリシーに準拠させることができます。ポリシー違反アラームから直接、非準拠デバイスを修復します。

次の手順に従ってください:

1. [エクスプローラ] タブで、個々のデバイス、設定済みポリシーのあるグローバルコレクション、または(ポリシーノードから) ポリシーを選択します。
2. コンテンツ画面の [アラーム] タブで、[アラーム タイトル] 列内に「NCM ポリシー違反」と示されているアラームを選択します。
3. コンポーネント詳細画面の [アラーム詳細] タブで、[違反の詳細を表示] をクリックします。
[違反デバイスを修復] ページが表示されます。
4. [コンテンツ] をクリックして、修復を実行するためにアップロードするコンテンツを表示します。 [違反を表示] をクリックして、各デバイスの違反を表示します。
[違反を表示] ページが表示されます。
5. [修復] をクリックします。
[タスクを作成しています] のステータス ボックスに続いて、[アップロードタスク結果] ページが表示されます。

ポリシーの管理

ポリシーが作成された後に、編集、有効化または無効化、グローバルコレクションへの適用、および削除を行うことができます。このセクションには、以下のトピックが含まれます。

- [ポリシーの編集 \(P. 169\)](#)
- [ポリシーの有効化および無効化 \(P. 170\)](#)
- [グローバルコレクションにポリシーを適用 \(P. 170\)](#)
- [ポリシーの削除 \(P. 171\)](#)

ポリシーの編集

既存の Network Configuration Manager ポリシーを編集することができます。ポリシーの編集後、ポリシーを保存して有効化する必要があります。

ポリシーを編集する方法

1. [エクスプローラ] タブの [ポリシー] ノードの下にあるポリシーを選択します。
2. コンテンツ画面で [リスト] タブを選択します。
ポリシーのリストが表示されます。
3. ポリシーを選択し、ツールバーの [編集] アイコンをクリックします。
[NCM ポリシーの編集] ダイアログ ボックスが表示されます。
4. 必要に応じて変更を加え、[保存] をクリックします。

ポリシーが無効になります。「[ポリシーテーブルからポリシーの有効化および無効化 \(P. 170\)](#)」で説明されるようにポリシーを有効にします。

注: 必要に応じて、グローバルコレクションを選択して [情報] タブをクリックし、関連するポリシーを編集することにより、ポリシーの編集が可能です。または、個々のデバイスを選択して [情報] タブをクリックし、[ネットワーク設定ポリシー] をクリックして、関連するポリシーを編集することもできます。

ポリシーの有効化および無効化

Network Configuration Manager ポリシーは、ポリシー テーブルから有効および無効にすることができます。

次の手順に従ってください:

1. [エクスプローラ] タブの [ポリシー] ノードの下にあるポリシーを選択します。
2. コンテンツ画面の [リスト] タブを選択します。
ポリシーのリストが表示されます。
3. ポリシーを選択し、[選択したポリシーの有効化] アイコンをクリックします。
ポリシーを有効にすると、すべての非準拠デバイスおよび違反ポリシーに指定したアラームがただちに表示されます。
4. (オプション) ポリシーを選択して [選択したポリシーの無効化] アイコンをクリックし、そのポリシーを無効にします。
ポリシーを無効化すると、非準拠デバイスおよび違反があったポリシーの既存アラームが即座にクリアされます。

注: また、グローバルコレクションまたは個々のデバイスを選択することにより、ポリシーを有効および無効にすることもできます。 [情報] タブを使用し、関連するポリシーを管理します。

グローバルコレクションにポリシーを適用

ポリシーが作成された後、グローバルコレクションに適用できます。ポリシーがグローバルコレクションに適用される場合、ポリシーはデバイスファミリごとにすべてのグローバルコレクションメンバに強制適用されます。

グローバルコレクションにポリシーを適用する方法

1. [エクスプローラ] タブでグローバルコレクションを選択します。
グローバルコレクションの情報がコンテンツ画面の [情報] タブに表示されます。
2. ネットワーク設定ポリシー サブビューを展開します。
ネットワーク設定ポリシー テーブルが表示されます。

3. [グローバルコレクションに対するポリシーの追加/削除] アイコンをクリックします。
[グローバルコレクションに対するポリシーの追加/削除] ダイアログボックスが表示されます。
4. このグローバルコレクションに強制適用するポリシーを選択し、[適用先] ウィンドウに移動します。
注: [作成] ボタンを使用して、このダイアログボックスから直接ポリシーを作成することもできます。
5. [OK] をクリックします。
適用されるポリシーはネットワーク設定ポリシーテーブルに表示され、デバイスファミリごとのすべてのグローバルメンバに強制適用されます。

詳細情報:

[グローバルコレクション \(P. 27\)](#)

ポリシーの削除

必要がなくなったポリシーを削除するには、[エクスプローラ] タブの[ポリシー] から該当するポリシーを右クリックし、[削除] を選択します。

注: オプションで、グローバルコレクションを選択して [情報] タブをクリックし、関連するポリシーを削除することにより、ポリシーを削除できます。また、個々のデバイスを選択して [情報] タブをクリックし、[ネットワーク設定ポリシー] をクリックして、関連するポリシーを削除することもできます。

ポリシー情報の表示

このセクションではポリシー情報を表示する方法について説明し、以下のトピックが含まれます。

- [ポリシーの詳細の表示 \(P. 172\)](#)
- [すべてのポリシーの重大な統計の表示 \(P. 172\)](#)
- [グローバルコレクションに適用されるポリシーの重大な統計の表示 \(P. 173\)](#)
- [単一のデバイスに適用されるすべてのポリシーの重大な統計の表示 \(P. 173\)](#)

ポリシーの詳細の表示

Network Configuration Manager ポリシーのコンポーネント詳細を表示できます。

次の手順に従ってください:

1. 関連するポリシーがある [エクスプローラ] タブで、単一のデバイスまたはグローバルコレクションを選択します。
2. コンテンツ画面で [情報] タブをクリックします。

選択したデバイスまたはグローバルコレクションの情報および設定が表示されます。

3. [ネットワーク設定ポリシー] を展開し、[選択したモデルのコンポーネント詳細を表示します] をクリックします。

選択されたポリシーのコンポーネント詳細画面が表示されます。

注: [エクスプローラ] タブの [ポリシー] からポリシーを選択してこの画面にアクセスすることもできます。

すべてのポリシーの重大な統計の表示

[エクスプローラ] タブの [設定マネージャ] の下にある [ポリシー] を選択し、コンテンツ画面の [リスト] タブを選択することにより、ポリシーの重大な統計を表示できます。

すべてのポリシーの統計が表示されます。

単一のデバイスに適用されるすべてのポリシーの重大な統計の表示

单一のデバイスに適用されるポリシーの重大な統計を表示できます。

次の手順に従ってください:

1. デバイスを選択して、[情報] タブをクリックします。
デバイスについての情報が表示されます。
2. [ネットワーク設定ポリシー] を選択します。
单一のデバイスに適用されるすべてのポリシーの統計が表示されます。

グローバルコレクションに適用されるポリシーの重大な統計の表示

グローバルコレクションに適用されるポリシーの重大な統計を表示できます。

次の手順に従ってください:

1. [エクスプローラ] タブで既存のグローバルコレクションを選択します。コンテンツ画面の [情報] タブを選択します。
コンテンツ画面に情報が表示されます。
2. [ネットワーク設定ポリシー] を選択します。
コレクションに適用されるすべてのポリシーの統計が表示されます。

複数行ブロック ポリシーの例

このセクションでは、複数行ブロック ポリシーの使用方法の例を示します。同じユースケースは 2 つの異なる方法（指定されたコンテンツと比較、および別の設定と比較による）に実装されます。

注: このセクションで提供されるコンテンツは、高いレベルでサンプルユースケースを提供することを目的としています。このセクションで参照された概念またはアイテムの追加情報については、適切な親トピックを参照してください。

このセクションには、以下のトピックが含まれます。

- [シナリオ \(P. 174\)](#)
- [はじめに \(P. 175\)](#)
- [ポリシーの定義 \(P. 177\)](#)
- [ポリシーの保存およびテスト \(P. 183\)](#)
- [違反の監視 \(P. 189\)](#)

シナリオ

説明に含まれる「shutdown」という単語によって識別された特定のインターフェースをシャットダウンするとします。以下の方法で複数行ブロック ポリシーを定義することによって、このようなデバイスを識別できます。

- 指定されたコンテンツとの比較。ポリシー定義として説明に「shutdown」を含まないすべてのインターフェースを検索できます。これにより、ポリシーの違反者として説明に「shutdown」を含むすべてのインターフェースを強調表示します。
- 別の設定との比較。キャプチャが発生するごとに新しくキャプチャされた設定を参照設定と比較することによって、コンテンツを監視できます。「shutdown」がインターフェース用の説明に追加される場合、それは参照設定に一致しないため、ポリシーの違反者として強調表示されます。

デバイスが識別された後、シャットダウン コマンドは修正アクションに推奨されたアップロードの一部として、シャットダウン用にマークされたインターフェースに対して容易に発行できます。

はじめに

ポリシーの定義を始める前に、以下の手順を実行する必要があります。

- ブロックを構成するものを特定します。
- 参照設定を確立します（参照設定と比較する場合）。

デバイス用にキャプチャされたホスト設定の確認により、この情報を収集できます。グローバル同期タスク、同期タスクおよび、[設定をキャプチャ] アイコンを使用して、設定はキャプチャされます。

デバイス用にキャプチャされたホスト設定を表示する方法

1. [エクスプローラ] タブでデバイスを選択します。
2. コンテンツ画面で [リスト] タブが選択されていることを確認し、コンポーネント詳細画面で [ホスト設定] を選択します。
3. 表示するキャプチャされたホスト設定のホスト設定テーブルで行をクリックします。

キャプチャされたホスト設定が、テーブルの下のボックスに表示されます。

注: 詳細については、「[单一デバイスの設定履歴を表示 \(P. 87\)](#)」を参照してください。

ブロックを構成するものの特定

以下のイメージでは、デバイス用の設定ファイルの一部を示します。このデバイス上の各インターフェースに同様の形式があり、開始タグおよび終了タグによって区切られていることが確認できます。また、数個のインターフェースの説明に「shutdown」の表示があることに注目します。

```
interface Loopback0
description "Management Interface"
bandwidth 1000000
ip address 172.22.96.5 255.255.255.255
ip pim sparse-dense-mode
ipv6 address FFFE:8A2A:5E12:8A2A:6005::1/128
ipv6 enable
ipv6 rip IPv6-1 enable
!
interface Loopback1
description "Multicast RP Interface #1 shutdown"
ip address 172.22.96.23 255.255.255.255
ip pim sparse-dense-mode
!
interface Loopback2
description "Multicast RP Interface #2 shutdown"
ip address 172.22.96.40 255.255.255.255
```

検索: 次へ 前へ すべてをハイライト表示 大文字と小文字を区別しない

ブロック ポリシー用語で、この例の各ブロックは以下によって定義されます。

開始タグ : interface

終了タグ : !

参照設定を確立します(参照設定と比較する場合)。

「デバイス用にキャプチャされたホスト設定を表示する方法」で概説された手順を使用し、デバイス用の理想的な設定を含むホスト設定を識別して、参照設定としてこの設定を指定します。参照設定を設定する詳細については、「[参照設定の指定 \(P. 91\)](#)」を参照してください。

注: 参照設定の代わりに、比較用に最後のキャプチャされた設定を使用することもできます。

以下のイメージでは、参照設定として使用される設定ファイルの一部を示します。この設定にはどのインターフェースの説明にも「shutdown」が含まれないことに注意してください。

2013/07/11 2:37:32 JST - nozhi02 - CA Spectrum OneClick

```
interface Loopback0
description "Management Interface" ━━━━━━ 説明
bandwidth 1000000
ip address 172.22.96.5 255.255.255.255
ip pim sparse-dense-mode
ipv6 address FFFE:8A2A:5E12:8A2A:6005::1/128
ipv6 enable
ipv6 rip IPv6-1 enable
!
interface Loopback1
description "Multicast RP Interface #1" ━━━━━━ 説明
ip address 172.22.96.23 255.255.255.255
ip pim sparse-dense-mode
!
interface Loopback2
description "Multicast RP Interface #2" ━━━━━━ 説明
ip address 172.22.96.40 255.255.255.255
ip pim sparse-dense-mode
!
```

検索: 次へ 前へ すべてをハイライト表示 大文字と小文字を区別しない

名前を付けて保存... 閉じる

詳細情報:

- [グローバル同期タスク](#) (P. 83)
 - [同期タスクの作成](#) (P. 109)
 - [設定の手動によるキャプチャ](#) (P. 99)
 - [参照設定の指定](#) (P. 91)

ポリシーの定義

ブロックを構成するものを確立し、(必要に応じて) 参照設定を指定した後、複数行ブロック ポリシーを定義できます。

複数行ブロック ポリシーを作成し、その後以下のセクションを含む [NCM ブロック ポリシーの作成] ダイアログ ボックスを呼び出すには、「[ポリシーの作成 \(P. 144\)](#)」で概説された手順を参照してください。

- ポリシー ID
- ポリシー条件
- ポリシー アクション

これらのセクションはそれぞれ別々に説明されます。

注: 「[ポリシーの作成 \(P. 144\)](#)」セクションでは、このセクションで示されたそれぞれのフィールドの詳細な追加情報を利用できます。

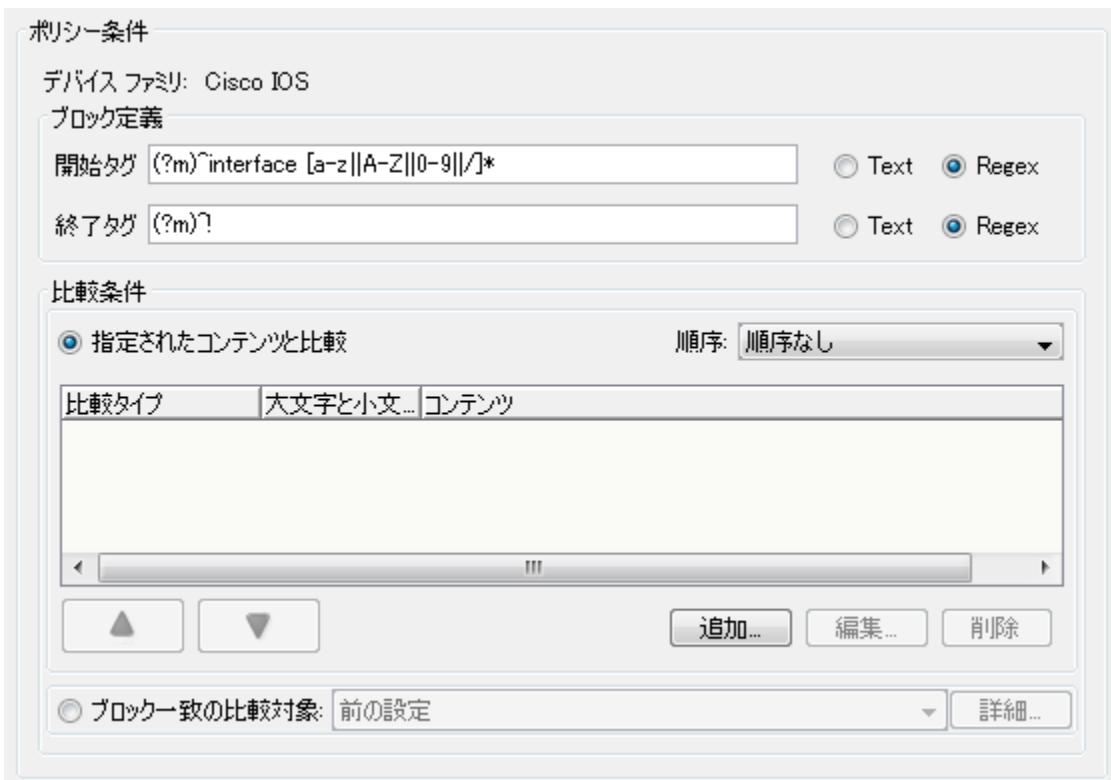
ポリシー ID

ポリシー ID の情報はポリシーを識別します。これらのフィールドを使用し、サイトに配置された標準に従ってポリシーの名前を指定します。

ポリシー ID	
名前	Shutdown
説明	User this policy to shutdown earmarked dev

ポリシー条件

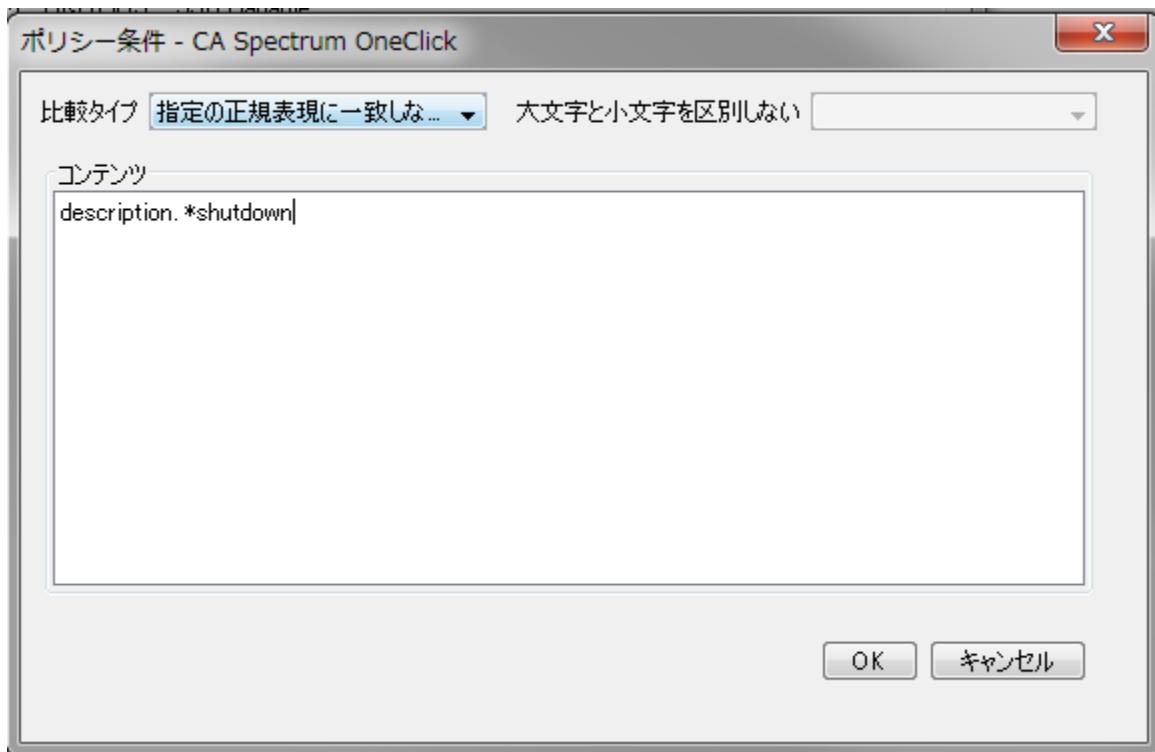
[ポリシー条件] 情報は、以下のイメージに示されるとおり、ブロック区切りフィールドおよび比較条件を定義します。



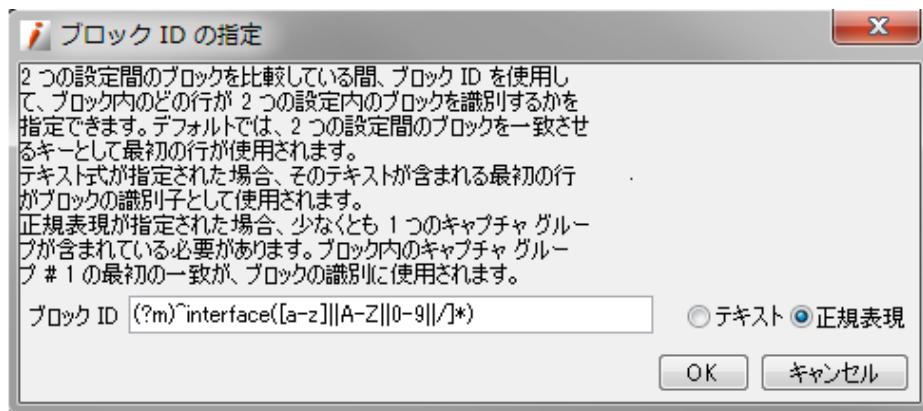
- ブロック定義。** [開始タグ] および [終了タグ] フィールドは、ブロックの最初および最後を識別するために使用される文字列を定義します。この例では、正規表現の値は「*interface name*」の文字列で始まり、「!」の文字で終わる各ブロックを指定するために使用されます。これらの値はブロックの一部として含まれています。
- 比較条件。** このセクションは、新しくキャプチャされた設定がポリシーに対して評価されるメソッドを制御します。特定の条件、ユーザ定義の条件、または別の設定に対する設定を比較するかどうかを指定できます。

注: 条件のセットを 1 つのみ、单一ポリシーに含めることができます。デモンストレーション目的としてのみ、両方の条件のセットがここに表示されます。

- [指定されたコンテンツと比較] のオプションは、ポリシーが有效地にされた後にキャプチャされる各設定がユーザ定義の条件と比較されるということを示します。[追加] ボタンをクリックし、[ポリシー条件] ダイアログ ボックスを表示します。以下のイメージでは、「description」で始まり、「shutdown」を含んでいる行を探す条件を示します。このポリシーが実行される場合、説明に「shutdown」を含むインターフェースは違反者として識別されます。

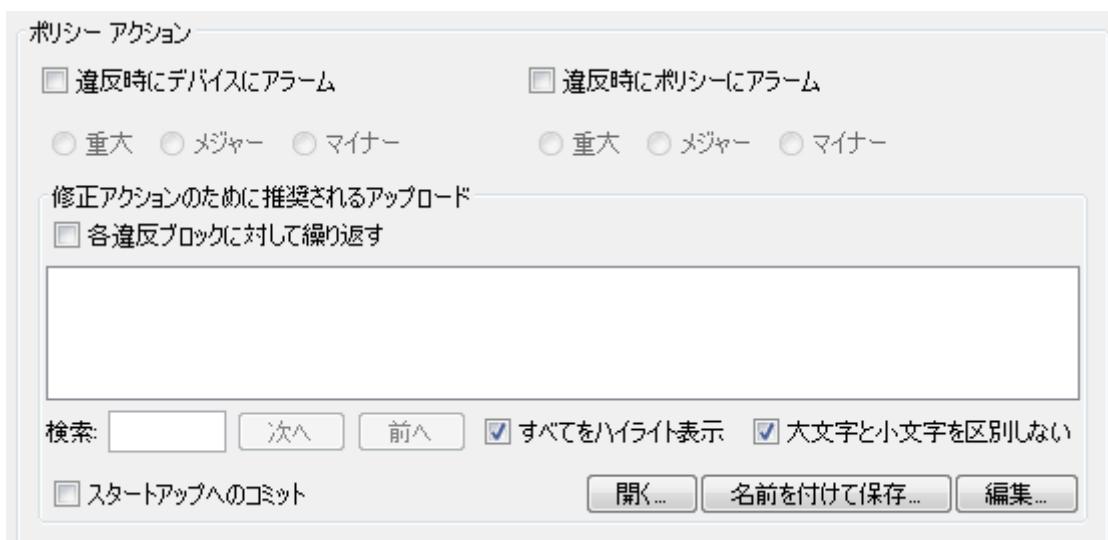


- [ブロック一致の比較対象: 参照設定] のオプションは、ポリシーが有効になった後にキャプチャされる各設定が、デバイス用の参照設定として指定された設定と比較されるということを示します。[詳細] ボタンをクリックし、ブロック ID を指定します。これは現在の設定と参照設定（指定された場合は前の設定）の間に対応するブロックに一致させるために使用されます。以下の例は、「interface name」に基づいて照合されます。



ポリシー アクション

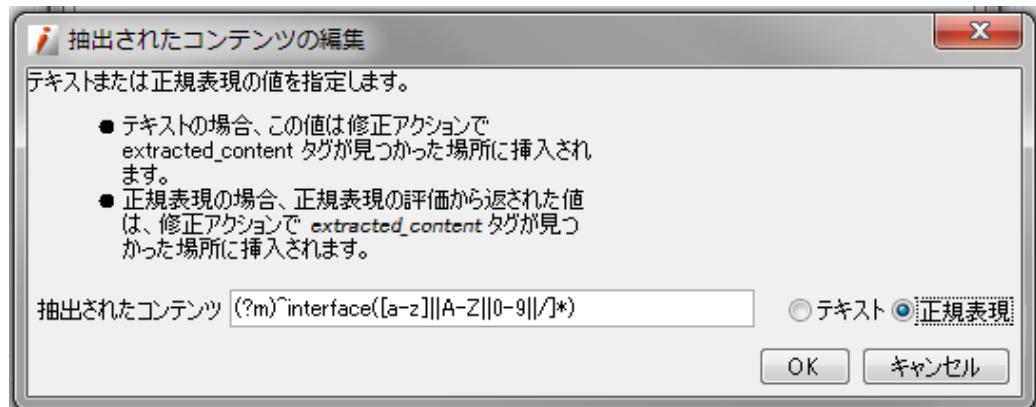
[ポリシー アクション] オプションでは、アラームが生成される方法を定義し、アップロードされるその修正アクションが非準拠である必要があります。以下のイメージでは、このセクション（すでに入力済み）について示され、その後説明されます。



- 違反が発生するタイミングに使用するアラームの基本設定を指定します。アラームはデバイス、ポリシーまたは両方と関連付けることができます。
- [修正アクションのために推奨されるアップロード]を定義するには、[編集] ボタンをクリックし、[修正アクションの編集] ダイアログ ボックスを表示します。ボックスに、デバイスにアップロードされるコンテンツを入力します。以下のイメージでは、デバイスに変更した説明およびシャットダウン コマンドをアップロードするコンテンツを示します。



この例では、ポリシーの実行時に、`<extracted_text>` タグはブロック固有コンテンツにより置換されます。修正アクションにこのタグを挿入するには、[抽出されたコンテンツの挿入] ボタンを使用します。タグを置換するために使用されるものを設定するには、[抽出されたコンテンツの設定] ボタンをクリックします。これで以下のダイアログボックスを開きます。



この例では、インターフェースの名前が各ブロックから抽出され、修正アクションコンテンツを作成するために使用されます。

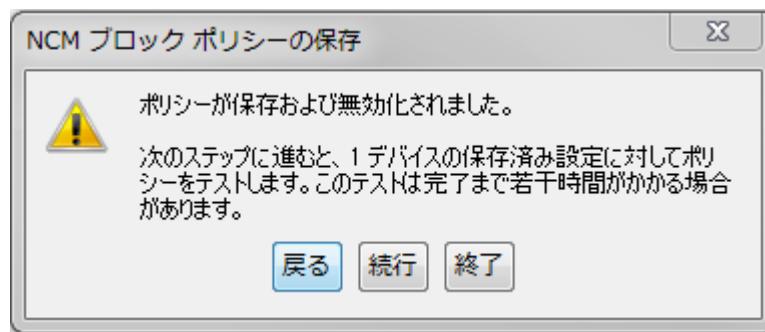
修正アクションコンテンツが定義された後に、[修正アクションのために推奨されるアップロード] ボックスに表示されます。違反が発生するごとにこの変更が行われる必要のある場合、[各違反ブロックに対して繰り返す] オプションを選択します。空白のままの場合、変更は最初の発生に対してのみ行なわれます。

ポリシーの保存およびテスト

ポリシーが最初に定義された後、予期したとおり確実に動作するように、有効化される前にテストされる必要があります。

ポリシーのテストを続行するには、[NCM ブロック ポリシーの作成] ダイアログ ボックスの [保存] をクリックし、設定を保存します。次のイメージで示されるとおり、その後の [保存] ダイアログ ボックスで、[続行] をクリックしてポリシーをテストします。

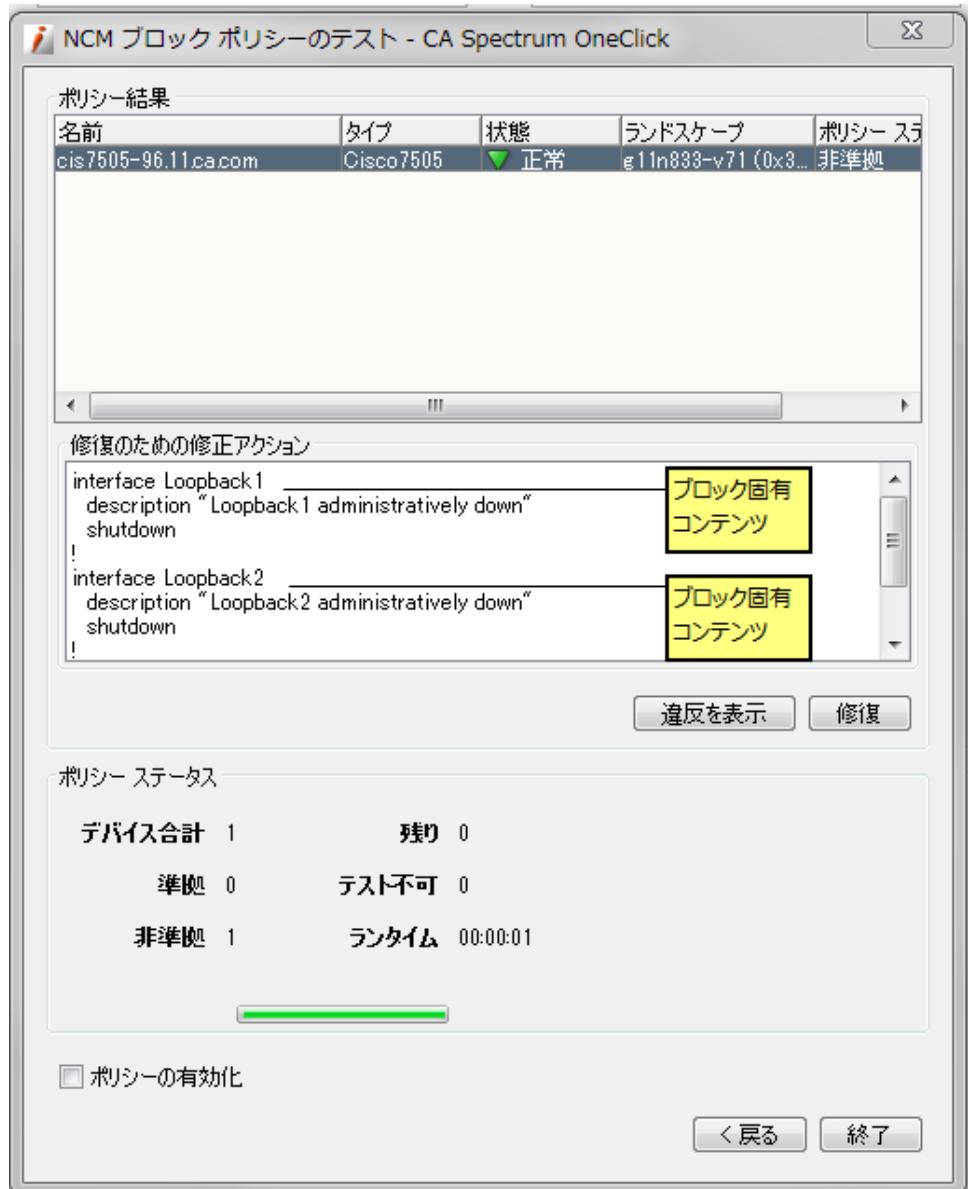
注: ポリシーディレクションに追加の変更を加えるために [戻る] を選択することもできます。 [終了] をクリックする場合、ポリシーが保存されますが無効となります。



[NCM ブロック ポリシーのテスト] ダイアログ ボックスが開き、テストが開始され、ステータスバーはその進捗状況を示します。テスト中に現在の設定はキャプチャされ、ポリシーで指定された条件と比較されます。ブロックはブロック ID に基づいて一致し、対応するブロックのコンテンツが比較されます。

注: 含まれるデバイス数によって、テストは完了に少し時間がかかる場合があります。

ポリシーのテストが完了している場合、ポリシー結果は以下のように表示されます。



この例のように非準拠が検出された場合、影響を受けたデバイスの数が [ポリシー ステータス] セクションにレポートされます。また、これが定義されている場合、修正アクションも表示されます。<extracted_text> タグがブロック固有のコンテンツで置換されていることを確認します。

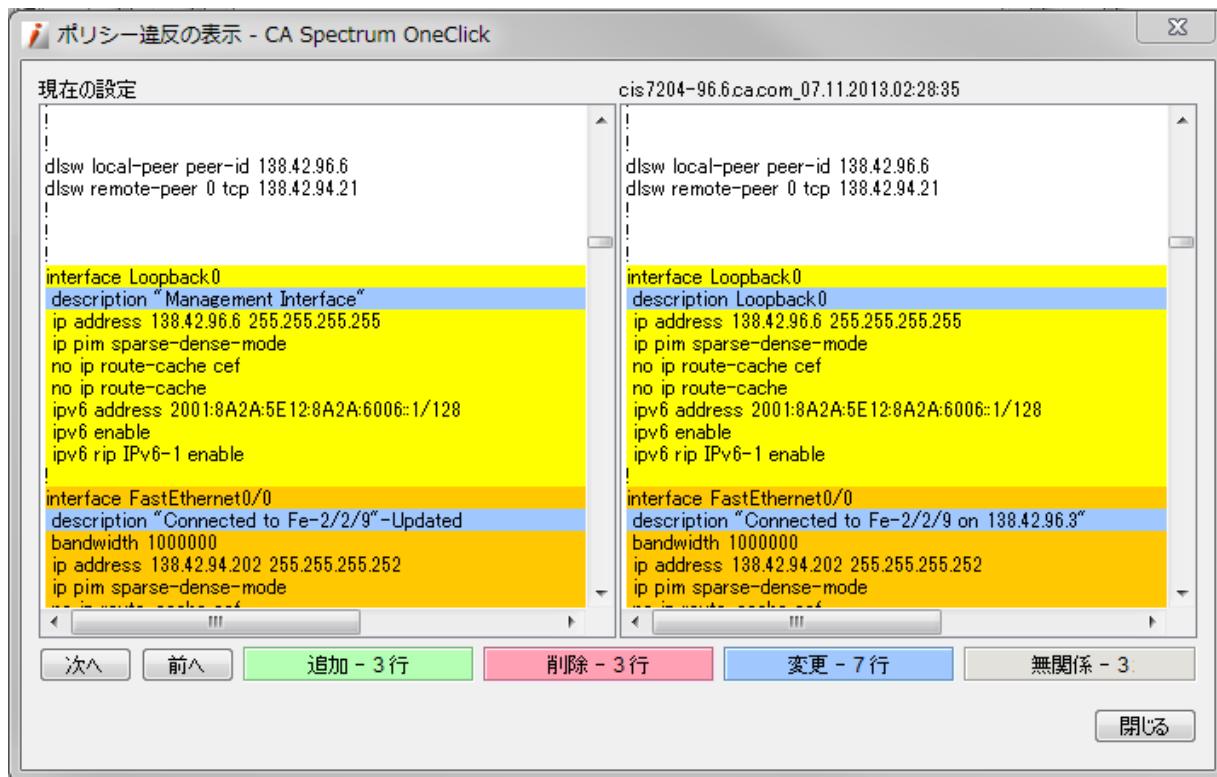
テストが完了した後、テストダイアログボックスから以下の手順を実行できます。

- ポリシー違反を表示するには、[違反を表示] をクリックします。ダイアログボックスが表示され、違反が示されます。
 - 比較条件に指定されたコンテンツを使用した場合、以下のイメージのように [違反ブロックの表示] ダイアログボックスが表示されます。ブロックはそれぞれ色によって区別され、違反している行は強調表示されます。この例では、「description」で始まり、「shutdown」が含まれている行が、違反として識別されます。[次へ] および [前へ] ボタンを使用して、違反をスクロールできます。



- 比較条件に別の設定を使用した場合、以下のイメージのように【ポリシー違反の表示】ダイアログボックスが表示されます。ブロックはそれぞれ色によって区別され、差異は強調表示されます。この例では、インターフェースの2つの説明コンテンツは、参照として定義されたものに一致しません。【次へ】および【前へ】ボタンを使用して、違反をスクロールできます。

重要: 参照設定に対して比較している場合、適用されない場所で意図せずに修正アクションを実行しないように、必ず差異をそれぞれ確認してください。



- ポリシー違反を修正し、これによりデバイスを準拠させるには、【修復のための修正アクション】ボックスで概説されたとおり、【修復】をクリックしてコンテンツをアップロードします。【アップロードタスク結果】ダイアログボックスで表示されたタスクの結果で、アップロードタスクは作成および実行されます。

- テストの結果に満足している場合、「ポリシーの有効化」オプションを選択し、このポリシーに基づいて自動監視およびアラーム生成を開始します。そうでない場合は、[戻る] をクリックしてポリシー定義を変更できます。[終了] をクリックした場合、ポリシーは保存されますが有効にはなりません。

違反の監視

ポリシーが有効化された後、キャプチャされた設定を監視し、指定したアクションに基づいて任意の違反に対してアラートを生成します。ポリシー違反によって生成されたアラームには、「NCM ポリシー違反」のアラーム タイトルがあります。以下のイメージでは、この例のポリシーに基づいて生成されたアラームを示しています。

The screenshot shows two windows from the Cisco Network Configuration Manager (NCM) interface.

Top Window (Alarm List):

Shows a list of alarms for device "cis7204-96.6.ca.com" (Cisco 7204VXR). There are two entries:

重大度	日付/時刻	名前	ネットワーク アドレス	セキュア ドメイン	タイプ	アラーム タイトル	ランドスケープ
メジャー	2013/07/09 20:56:24 JST	cis7204-96.6.ca...	138.42.94.202	Directly Managed	Cisco7204V...	高い CPU 使用率	g1In833-v71 (0x3200000)
マイナー	2013/07/12 5:18:56 JST	cis7204-96.6.ca...	138.42.94.202	Directly Managed	Cisco7204V...	NCM ポリシー違反	g1In833-v71 (0x3200000)

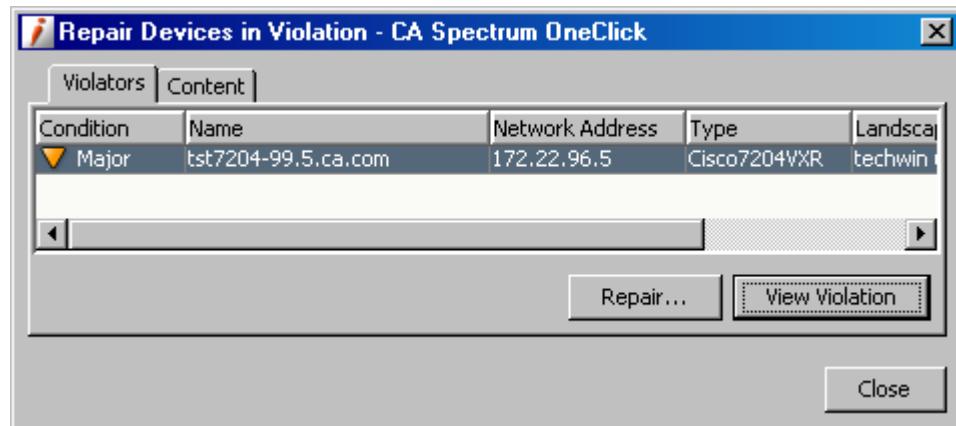
Bottom Window (Alarm Detail):

Shows details for the "NCM ポリシー違反" alarm. The summary states: "2013/07/12 5:18:56 JST 設定マネージャ - デバイス cis7204-96.6.ca.com は、ランドスケープ g1In833-v71 上でポリシー Upload に違反しました。この違反の重大度はマイナーです。"

The detailed view includes:

- Severity:** マイナー
- Root Cause:** このデバイス上のホスト設定はユーザ定義ポリシーに違反しています。
- Reasons:**
 - 1) デバイス設定はローカルで変更されました。
 - 2) このポリシーに違反する設定がデバイスにアップロードされました。
 - 3) デバイスがリブートされ、このポリシーに違反しているスタートアップ コンフィギュレーションがロードされました。
- Action:**
 - 1) 設定を点検してください。
 - 2) 推奨された修正処置をアップロードします。
 - 3) デバイス設定の変更がスタートアップ コンフィギュレーションに保存されていることを確認してください。

アラーム詳細から [違反の詳細を表示] をクリックできます。これにより [違反デバイスを修復] ダイアログ ボックスが以下のように開きます。



このダイアログ ボックスから使用可能なボタンを使用し、ポリシーのテスト中に記述されたとおり、違反を表示または非準拠を修復できます。

注: 非準拠デバイス用のコンテンツ画面のネットワーク設定ポリシーテーブルからこのダイアログ ボックスを起動することもできます。 詳細については、「[ポリシー テーブルから非準拠デバイスを修復 \(P. 167\)](#)」を参照してください。

付録 A: サポートされているデバイス

このセクションには、以下のトピックが含まれています。

[Cisco 対応デバイス \(P. 191\)](#)

[Cisco 対応デバイス \(P. 215\)](#)

[Cisco 対応デバイス \(P. 222\)](#)

[Cisco CAT 対応デバイス \(P. 224\)](#)

[Cisco NX OS をサポートしているデバイス \(P. 226\)](#)

[Enterasys 対応デバイス \(P. 227\)](#)

[Enterasys/Riverstone SSR 対応デバイス \(P. 230\)](#)

[Extreme 対応デバイス \(P. 232\)](#)

[Foundry 対応デバイス \(P. 237\)](#)

[Juniper 対応デバイス \(P. 248\)](#)

[Lancom がサポートしているデバイス \(P. 250\)](#)

[Nortel Baystack のサポートしているデバイス \(P. 250\)](#)

[Nortel Passport 対応デバイス \(P. 251\)](#)

Cisco 対応デバイス

CA Spectrum Network Configuration Manager は、以下の Cisco デバイスをサポートします。サポートされている Catalyst デバイスのリストについては、「[Cisco 対応 Catalyst デバイス \(P. 215\)](#)」を参照してください。PIX Firewall デバイスのリストについては、「[Cisco 対応 PIX ファイアウォールデバイス \(P. 222\)](#)」を参照してください。

この表には例が示されます。デバイスサポートの最新情報については、[CA デバイス認定データベースにアクセス \(P. 17\)](#)してください。

Perl スクリプトがデバイスで唯一の通信手段である場合、スクリプトメソッドが提供されます。

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
CiscoDSC9216K 9	1.3.6.1.4.1.9.1.521	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Cisco677i	1.3.6.1.4.1.9.1.363	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco741	1.3.6.1.4.1.9.1.94	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco742	1.3.6.1.4.1.9.1.95	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco743	1.3.6.1.4.1.9.1.96	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco744	1.3.6.1.4.1.9.1.97	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco751	1.3.6.1.4.1.9.1.81	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco752	1.3.6.1.4.1.9.1.82	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco753	1.3.6.1.4.1.9.1.83	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco761	1.3.6.1.4.1.9.1.98	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco762	1.3.6.1.4.1.9.1.99	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco765	1.3.6.1.4.1.9.1.102	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco766	1.3.6.1.4.1.9.1.103	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco771	1.3.6.1.4.1.9.1.126	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco772	1.3.6.1.4.1.9.1.127	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco775	1.3.6.1.4.1.9.1.128	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco776	1.3.6.1.4.1.9.1.129	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Cisco801	1.3.6.1.4.1.9.1.212	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco802	1.3.6.1.4.1.9.1.213	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco802J	1.3.6.1.4.1.9.1.295	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco803	1.3.6.1.4.1.9.1.214	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco804	1.3.6.1.4.1.9.1.215	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco804J	1.3.6.1.4.1.9.1.296	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco805	1.3.6.1.4.1.9.1.245	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco806	1.3.6.1.4.1.9.1.384	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco811	1.3.6.1.4.1.9.1.395	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco813	1.3.6.1.4.1.9.1.396	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco826	1.3.6.1.4.1.9.1.322	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco826QuadV	1.3.6.1.4.1.9.1.321	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco827	1.3.6.1.4.1.9.1.284	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco827H	1.3.6.1.4.1.9.1.446	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco827QuadV	1.3.6.1.4.1.9.1.270	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco828	1.3.6.1.4.1.9.1.382	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

Cisco 対応デバイス

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Cisco831	1.3.6.1.4.1.9.1.497	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco836	1.3.6.1.4.1.9.1.499	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco837	1.3.6.1.4.1.9.1.495	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco871	1.3.6.1.4.1.9.1.571	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco877	1.3.6.1.4.1.9.1.569	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco878	1.3.6.1.4.1.9.1.570	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco1000	1.3.6.1.4.1.9.1.40	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco1003	1.3.6.1.4.1.9.1.41	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco1004	1.3.6.1.4.1.9.1.44	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco1005	1.3.6.1.4.1.9.1.49	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco1020	1.3.6.1.4.1.9.1.43	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco1401	1.3.6.1.4.1.9.1.206	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco1407	1.3.6.1.4.1.9.1.249	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco1417	1.3.6.1.4.1.9.1.250	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco1502	1.3.6.1.4.1.9.1.161	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco1503	1.3.6.1.4.1.9.1.160	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Cisco1538M	1.3.6.1.4.1.9.1.224	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco1548M	1.3.6.1.4.1.9.1.225	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco1601	1.3.6.1.4.1.9.1.113	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco1602	1.3.6.1.4.1.9.1.114	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco1603	1.3.6.1.4.1.9.1.115	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco1604	1.3.6.1.4.1.9.1.116	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco1605	1.3.6.1.4.1.9.1.172	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco1701ADSL BRI	1.3.6.1.4.1.9.1.550	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco1710	1.3.6.1.4.1.9.1.200	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco1711	1.3.6.1.4.1.9.1.538	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco1712	1.3.6.1.4.1.9.1.539	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco1720	1.3.6.1.4.1.9.1.201	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco1721	1.3.6.1.4.1.9.1.444	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco1750	1.3.6.1.4.1.9.1.216	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco1751	1.3.6.1.4.1.9.1.326	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco1760	1.3.6.1.4.1.9.1.416	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

Cisco 対応デバイス

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Cisco1801	1.3.6.1.4.1.9.1.638	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco1811	1.3.6.1.4.1.9.1.641	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco1812	1.3.6.1.4.1.9.1.642	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco1841	1.3.6.1.4.1.9.1.620	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2000	1.3.6.1.4.1.9.1.10	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2102	1.3.6.1.4.1.9.1.15	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2202	1.3.6.1.4.1.9.1.16	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2500	1.3.6.1.4.1.9.1.13	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2501	1.3.6.1.4.1.9.1.17	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2502	1.3.6.1.4.1.9.1.18	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2503	1.3.6.1.4.1.9.1.19	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2504	1.3.6.1.4.1.9.1.20	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2505	1.3.6.1.4.1.9.1.21	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2506	1.3.6.1.4.1.9.1.22	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2507	1.3.6.1.4.1.9.1.23	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2508	1.3.6.1.4.1.9.1.24	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Cisco2509	1.3.6.1.4.1.9.1.25	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2501FRAD FX	1.3.6.1.4.1.9.1.165	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2501LANF RADFX	1.3.6.1.4.1.9.1.166	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2502LANF RADFX	1.3.6.1.4.1.9.1.167	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2510	1.3.6.1.4.1.9.1.26	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2511	1.3.6.1.4.1.9.1.27	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2512	1.3.6.1.4.1.9.1.28	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2513	1.3.6.1.4.1.9.1.29	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2514	1.3.6.1.4.1.9.1.30	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2515	1.3.6.1.4.1.9.1.31	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2516	1.3.6.1.4.1.9.1.42	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2517	1.3.6.1.4.1.9.1.67	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2518	1.3.6.1.4.1.9.1.68	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2519	1.3.6.1.4.1.9.1.69	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2520	1.3.6.1.4.1.9.1.70	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2521	1.3.6.1.4.1.9.1.71	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Cisco2522	1.3.6.1.4.1.9.1.72	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2523	1.3.6.1.4.1.9.1.73	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2524	1.3.6.1.4.1.9.1.74	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2525	1.3.6.1.4.1.9.1.75	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2610	1.3.6.1.4.1.9.1.185	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2610M	1.3.6.1.4.1.9.1.418	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2610XM	1.3.6.1.4.1.9.1.466	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2611	1.3.6.1.4.1.9.1.186	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2611M	1.3.6.1.4.1.9.1.419	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2611XM	1.3.6.1.4.1.9.1.467	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2612	1.3.6.1.4.1.9.1.187	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2613	1.3.6.1.4.1.9.1.195	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2620	1.3.6.1.4.1.9.1.208	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2620XM	1.3.6.1.4.1.9.1.468	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2621	1.3.6.1.4.1.9.1.209	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2621XM	1.3.6.1.4.1.9.1.469	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Cisco2650	1.3.6.1.4.1.9.1.319	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2650XM	1.3.6.1.4.1.9.1.470	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2651	1.3.6.1.4.1.9.1.320	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2651XM	1.3.6.1.4.1.9.1.471	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2691	1.3.6.1.4.1.9.1.413	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2801	1.3.6.1.4.1.9.1.619	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2811	1.3.6.1.4.1.9.1.576	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2821	1.3.6.1.4.1.9.1.577	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco2851	1.3.6.1.4.1.9.1.578	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco3000	1.3.6.1.4.1.9.1.6	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco3101	1.3.6.1.4.1.9.1.32	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco3102	1.3.6.1.4.1.9.1.33	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco3103	1.3.6.1.4.1.9.1.34	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco3104	1.3.6.1.4.1.9.1.35	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco3202	1.3.6.1.4.1.9.1.36	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco3204	1.3.6.1.4.1.9.1.37	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Cisco3220	1.3.6.1.4.1.9.1.553	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco3250	1.3.6.1.4.1.9.1.479	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco3620	1.3.6.1.4.1.9.1.122	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco3640	1.3.6.1.4.1.9.1.110	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco3660	1.3.6.1.4.1.9.1.205	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco3661Ac	1.3.6.1.4.1.9.1.338	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco3661Dc	1.3.6.1.4.1.9.1.339	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco3662Ac	1.3.6.1.4.1.9.1.340	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco3662AcCo	1.3.6.1.4.1.9.1.342	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco3662Dc	1.3.6.1.4.1.9.1.341	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco3662DcCo	1.3.6.1.4.1.9.1.343	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco371098-HP 001	1.3.6.1.4.1.9.1.625	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco371098-HP .3.1.1	1.3.6.1.4.1.11.2.3.7.11.33	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco3725	1.3.6.1.4.1.9.1.414	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco3745	1.3.6.1.4.1.9.1.436	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco3825	1.3.6.1.4.1.9.1.543	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Cisco3845	1.3.6.1.4.1.9.1.544	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco4000	1.3.6.1.4.1.9.1.7	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco4224	1.3.6.1.4.1.9.1.399	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco4500	1.3.6.1.4.1.9.1.14	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco4700	1.3.6.1.4.1.9.1.50	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco6015	1.3.6.1.4.1.9.1.299	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco6100	1.3.6.1.4.1.9.1.251	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco6130	1.3.6.1.4.1.9.1.252	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco6160	1.3.6.1.4.1.9.1.297	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco6200	1.3.6.1.4.1.9.1.192	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco6260	1.3.6.1.4.1.9.1.253	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco6400	1.3.6.1.4.1.9.1.180	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco6400Nrp	1.3.6.1.4.1.9.1.211	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco6400UAC	1.3.6.1.4.1.9.1.464	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7000	1.3.6.1.4.1.9.1.8	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7010	1.3.6.1.4.1.9.1.12	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Cisco7120Ae3	1.3.6.1.4.1.9.1.263	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7120At3	1.3.6.1.4.1.9.1.262	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7120E3	1.3.6.1.4.1.9.1.261	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7120Quadt 1	1.3.6.1.4.1.9.1.259	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7120Smi3	1.3.6.1.4.1.9.1.264	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7120T3	1.3.6.1.4.1.9.1.260	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7140Duala e3	1.3.6.1.4.1.9.1.268	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7140Duala t3	1.3.6.1.4.1.9.1.267	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7140Duale 3	1.3.6.1.4.1.9.1.266	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7140Dualf e	1.3.6.1.4.1.9.1.277	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7140Dual mm3	1.3.6.1.4.1.9.1.269	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7140Dualt 3	1.3.6.1.4.1.9.1.265	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7140Octt1	1.3.6.1.4.1.9.1.276	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7150Dualf e	1.3.6.1.4.1.9.1.355	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7150Dualt 3	1.3.6.1.4.1.9.1.357	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7150Octt1	1.3.6.1.4.1.9.1.356	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Cisco7202	1.3.6.1.4.1.9.1.194	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7204	1.3.6.1.4.1.9.1.125	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7204VXR	1.3.6.1.4.1.9.1.223	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7206	1.3.6.1.4.1.9.1.108	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7206VXR	1.3.6.1.4.1.9.1.222	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
UBR_7246	1.3.6.1.4.1.9.1.179	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7301	1.3.6.1.4.1.9.1.476	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7304	1.3.6.1.4.1.9.1.439	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7401ASR	1.3.6.1.4.1.9.1.403	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7401VXR	1.3.6.1.4.1.9.1.376	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7505	1.3.6.1.4.1.9.1.48	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7507z	1.3.6.1.4.1.9.1.288	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7506	1.3.6.1.4.1.9.1.47	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7507	1.3.6.1.4.1.9.1.45	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7507mx	1.3.6.1.4.1.9.1.290	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7513	1.3.6.1.4.1.9.1.46	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Cisco7513mx	1.3.6.1.4.1.9.1.291	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7513z	1.3.6.1.4.1.9.1.289	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7576	1.3.6.1.4.1.9.1.204	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7603	1.3.6.1.4.1.9.1.401	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7604	1.3.6.1.4.1.9.1.658	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7606	1.3.6.1.4.1.9.1.402	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7609	1.3.6.1.4.1.9.1.509	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco7613	1.3.6.1.4.1.9.1.528	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco9004	1.3.6.1.4.1.9.1.424	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco10005	1.3.6.1.4.1.9.1.437	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco10008	1.3.6.1.4.1.9.1.438	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco10400	1.3.6.1.4.1.9.1.272	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco10720	1.3.6.1.4.1.9.1.397	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco12004	1.3.6.1.4.1.9.1.181	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco12006	1.3.6.1.4.1.9.1.590	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco12008	1.3.6.1.4.1.9.1.182	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Cisco12010	1.3.6.1.4.1.9.1.348	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco12012	1.3.6.1.4.1.9.1.173	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco12016	1.3.6.1.4.1.9.1.273	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco12404	1.3.6.1.4.1.9.1.423	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco12406	1.3.6.1.4.1.9.1.388	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco12410	1.3.6.1.4.1.9.1.394	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco12416	1.3.6.1.4.1.9.1.385	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco3631Co	1.3.6.1.4.1.9.1.425	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoAGS+	1.3.6.1.4.1.9.1.11	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoAPEC	1.3.6.1.4.1.9.1.39	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoAPRC	1.3.6.1.4.1.9.1.38	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoAS5200	1.3.6.1.4.1.9.1.109	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoAS5300	1.3.6.1.4.1.9.1.162	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoAS5350	1.3.6.1.4.1.9.1.313	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoAS5350XM	1.3.6.1.4.1.9.1.679	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoAS5400	1.3.6.1.4.1.9.1.274	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
CiscoAS5400XM	1.3.6.1.4.1.9.1.668	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoAS5800	1.3.6.1.4.1.9.1.188	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoAS5850	1.3.6.1.4.1.9.1.308	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoCacheEngine	1.3.6.1.4.1.9.1.240	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoCrs1Fabric	1.3.6.1.4.1.9.1.739	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoCRS16S	1.3.6.1.4.1.9.1.613	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoCrs18LineCard	1.3.6.1.4.1.9.1.738	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoCRS8S	1.3.6.1.4.1.9.1.643	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoCS500	1.3.6.1.4.1.9.1.9	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoFastHubB_MMFX	1.3.6.1.4.1.9.1.178	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoFastHubB_MMTX	1.3.6.1.4.1.9.1.177	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoFastHub21_6T	1.3.6.1.4.1.9.1.169	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoGS	1.3.6.1.4.1.9.1.1	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoIGESM	1.3.6.1.4.1.9.1.592	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoIGS	1.3.6.1.4.1.9.1.5	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoLocalDirect or	1.3.6.1.4.1.9.1.244	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Cisco MC3810	1.3.6.1.4.1.9.1.286	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cisco MC3810	1.3.6.1.4.1.9.1.157	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoME6340AC A	1.3.6.1.4.1.9.1.713	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoME6340DC A	1.3.6.1.4.1.9.1.714	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoME6340DC B	1.3.6.1.4.1.9.1.715	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoMicroWeb Server2	1.3.6.1.4.1.9.1.176	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoMWR1900	1.3.6.1.4.1.9.1.398	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoMWR1941 DC	1.3.6.1.4.1.9.1.520	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoOlympus	1.3.6.1.4.1.9.1.358	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoOpticalRegenerator	1.3.6.1.4.1.9.1.254	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro316C	1.3.6.1.4.1.9.1.148	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro316T	1.3.6.1.4.1.9.1.147	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro741	1.3.6.1.4.1.9.1.84	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro742	1.3.6.1.4.1.9.1.85	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro743	1.3.6.1.4.1.9.1.86	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro744	1.3.6.1.4.1.9.1.87	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
CiscoPro751	1.3.6.1.4.1.9.1.76	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro752	1.3.6.1.4.1.9.1.77	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro753	1.3.6.1.4.1.9.1.78	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro761	1.3.6.1.4.1.9.1.88	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro762	1.3.6.1.4.1.9.1.89	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro765	1.3.6.1.4.1.9.1.92	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro766	1.3.6.1.4.1.9.1.93	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro1003	1.3.6.1.4.1.9.1.51	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro1004	1.3.6.1.4.1.9.1.52	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro1005	1.3.6.1.4.1.9.1.53	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro1020	1.3.6.1.4.1.9.1.54	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro1601	1.3.6.1.4.1.9.1.117	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro1602	1.3.6.1.4.1.9.1.118	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro1603	1.3.6.1.4.1.9.1.119	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro1604	1.3.6.1.4.1.9.1.120	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro2500PC E	1.3.6.1.4.1.9.1.55	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
CiscoPro2501	1.3.6.1.4.1.9.1.56	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro2502	1.3.6.1.4.1.9.1.130	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro2503	1.3.6.1.4.1.9.1.57	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro2504	1.3.6.1.4.1.9.1.131	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro2505	1.3.6.1.4.1.9.1.58	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro2506	1.3.6.1.4.1.9.1.132	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro2507	1.3.6.1.4.1.9.1.59	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro2508	1.3.6.1.4.1.9.1.133	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro2509	1.3.6.1.4.1.9.1.60	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro2510	1.3.6.1.4.1.9.1.134	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro2511	1.3.6.1.4.1.9.1.61	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro2512	1.3.6.1.4.1.9.1.135	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro2513	1.3.6.1.4.1.9.1.136	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro2514	1.3.6.1.4.1.9.1.62	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro2515	1.3.6.1.4.1.9.1.137	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro2516	1.3.6.1.4.1.9.1.63	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
CiscoPro2517	1.3.6.1.4.1.9.1.138	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro2518	1.3.6.1.4.1.9.1.139	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro2519	1.3.6.1.4.1.9.1.164	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro2520	1.3.6.1.4.1.9.1.104	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro2521	1.3.6.1.4.1.9.1.165	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro2522	1.3.6.1.4.1.9.1.105	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro2523	1.3.6.1.4.1.9.1.140	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro2524	1.3.6.1.4.1.9.1.106	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro2525	1.3.6.1.4.1.9.1.141	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro3116	1.3.6.1.4.1.9.1.149	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro3620	1.3.6.1.4.1.9.1.123	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro3640	1.3.6.1.4.1.9.1.124	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro4500	1.3.6.1.4.1.9.1.166	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoPro4700	1.3.6.1.4.1.9.1.142	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoProtocolTr anslator	1.3.6.1.4.1.9.1.4	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoRPM	1.3.6.1.4.1.9.1.199	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
CiscoRPMPR	1.3.6.1.4.1.9.1.457	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoRpmXf	1.3.6.1.4.1.9.1.440	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoSC3640	1.3.6.1.4.1.9.1.189	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoSN5420	1.3.6.1.4.1.9.1.407	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoSN5428	1.3.6.1.4.1.9.1.475	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoSOHO76	1.3.6.1.4.1.9.1.354	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoSOHO91	1.3.6.1.4.1.9.1.498	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoSOHO97	1.3.6.1.4.1.9.1.496	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoSOHO77	1.3.6.1.4.1.9.1.353	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoSOHO96	1.3.6.1.4.1.9.1.500	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoTrouter	1.3.6.1.4.1.9.1.3	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoTS	1.3.6.1.4.1.9.1.2	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoWS3020Hp q	1.3.6.1.4.1.9.1.748	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoWS3030De I	1.3.6.1.4.1.9.1.749	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoWSC3750G -24PS	1.3.6.1.4.1.9.1.747	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoWSC6504E	1.3.6.1.4.1.9.1.657	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
CiscoWSC6509n eba	1.3.6.1.4.1.9.1.534	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoWSX3011	1.3.6.1.4.1.9.1.112	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoWSX5302	1.3.6.1.4.1.9.1.168	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoWSX6302 Msm	1.3.6.1.4.1.9.1.256	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoURM	1.3.6.1.4.1.9.1.373	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoURM2FE	1.3.6.1.4.1.9.1.374	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CiscoURM2FE2V	1.3.6.1.4.1.9.1.375	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
AP 1130	1.3.6.1.4.1.9.1.618	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
LS_1010	1.3.6.1.4.1.9.1.107	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
LS_1015	1.3.6.1.4.1.9.1.164	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
UBR_7223	1.3.6.1.4.1.9.1.210	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
UBR_7246VXR	1.3.6.1.4.1.9.1.271	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
UBR_904	1.3.6.1.4.1.9.1.191	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
UBR_924	1.3.6.1.4.1.9.1.255	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
UBR_912C	1.3.6.1.4.1.9.1.292	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
UBR_912S	1.3.6.1.4.1.9.1.293	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
UBR_914	1.3.6.1.4.1.9.1.294	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
UBR_925	1.3.6.1.4.1.9.1.316	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
UBR_10012	1.3.6.1.4.1.9.1.317	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
UBR_7111	1.3.6.1.4.1.9.1.344	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
UBR_7111E	1.3.6.1.4.1.9.1.345	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
UBR_7114	1.3.6.1.4.1.9.1.346	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
UBR_7114E	1.3.6.1.4.1.9.1.347	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
UBR_905	1.3.6.1.4.1.9.1.351	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
350 AP	1.3.6.1.4.1.9.1.552	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
1100 AP	1.3.6.1.4.1.9.1.507	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
1210/1230 AP	1.3.6.1.4.1.9.1.525	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
1240 AP	1.3.6.1.4.1.9.1.685	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
1400 AP	1.3.6.1.4.1.9.1.533	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
1300 AP	1.3.6.1.4.1.9.1.565	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
PIX Firewall	1.3.6.1.4.1.9.1.227	いいえ	いいえ	いいえ	Telnet
PIX 506 Firewall	1.3.6.1.4.1.9.1.389	いいえ	いいえ	いいえ	Telnet
PIX 515 Firewall	1.3.6.1.4.1.9.1.390	いいえ	いいえ	いいえ	Telnet
PIX 520 Firewall	1.3.6.1.4.1.9.1.391	いいえ	いいえ	いいえ	Telnet

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
PIX 525 Firewall	1.3.6.1.4.1.9.1.392	いいえ	いいえ	いいえ	Telnet
PIX 535 Firewall	1.3.6.1.4.1.9.1.393	いいえ	いいえ	いいえ	Telnet
PIX 501 Firewall	1.3.6.1.4.1.9.1.417	いいえ	いいえ	いいえ	Telnet
PIX 515E Firewall	1.3.6.1.4.1.9.1.451	いいえ	いいえ	いいえ	Telnet
PIX 506E Firewall	1.3.6.1.4.1.9.1.450	いいえ	いいえ	いいえ	Telnet
cat6500Firewall Sm	1.3.6.1.4.1.9.1.522	いいえ	いいえ	いいえ	Telnet
PIX Firewall Security Module	1.3.6.1.4.1.9.1.674	いいえ	いいえ	いいえ	Telnet
PIX 535sc Firewall	1.3.6.1.4.1.9.1.675	いいえ	いいえ	いいえ	Telnet
PIX 525sc Firewall	1.3.6.1.4.1.9.1.676	いいえ	いいえ	いいえ	Telnet
PIX 515Esc Firewall	1.3.6.1.4.1.9.1.677	いいえ	いいえ	いいえ	Telnet
PIX 515sc Firewall	1.3.6.1.4.1.9.1.678	いいえ	いいえ	いいえ	Telnet
PIX Firewall System Module	1.3.6.1.4.1.9.1.767	いいえ	いいえ	いいえ	Telnet
PIX 515sy Firewall	1.3.6.1.4.1.9.1.768	いいえ	いいえ	いいえ	Telnet
PIX 515Esy Firewall	1.3.6.1.4.1.9.1.769	いいえ	いいえ	いいえ	Telnet
PIX 525sy Firewall	1.3.6.1.4.1.9.1.770	いいえ	いいえ	いいえ	Telnet
PIX 535sy Firewall	1.3.6.1.4.1.9.1.771	いいえ	いいえ	いいえ	Telnet

* IOS < 12.0 = OLD-CISCO-SYSTEM-MIB

** IOS > 12.2(18) 機能「K9」有り

Cisco 対応デバイス

CA Spectrum Network Configuration Manager は、以下の Cisco Catalyst デバイスをサポートします。その他のサポートされている Cisco デバイスについては、「[Cisco 対応デバイス \(P. 191\)](#)」を参照してください。PIX Firewall デバイスのリストについては、「[Cisco 対応 PIX ファイアウォールデバイス \(P. 222\)](#)」を参照してください。

この表には例が示されます。デバイスサポートの最新情報については、[CA デバイス認定データベースにアクセス \(P. 17\)](#)してください。

Perl スクリプトがデバイスで唯一の通信手段である場合、スクリプトメソッドが提供されます。

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Cat116T	1.3.6.1.4.1.9.1.150	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat116C	1.3.6.1.4.1.9.1.151	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat1116	1.3.6.1.4.1.9.1.152	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat1912C	1.3.6.1.4.1.9.1.175	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat2924XL	1.3.6.1.4.1.9.1.183	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat2924CXL	1.3.6.1.4.1.9.1.184	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat2924XLv	1.3.6.1.4.1.9.1.217	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat2640-48TT	1.3.6.1.4.1.9.1.717	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat2948gL3	1.3.6.1.4.1.9.1.275	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat2948gL3Dc	1.3.6.1.4.1.9.1.386	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Cat2960-24TC	1.3.6.1.4.1.9.1.694	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat2960-24TT	1.3.6.1.4.1.9.1.716	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat2960G-24TC	1.3.6.1.4.1.9.1.696	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat2960-48TC	1.3.6.1.4.1.9.1.695	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat297024	1.3.6.1.4.1.9.1.527	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat297024TS	1.3.6.1.4.1.9.1.561	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat2908xl	1.3.6.1.4.1.9.1.170	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat2912LREXL	1.3.6.1.4.1.9.1.370	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat2912MfXL	1.3.6.1.4.1.9.1.221	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat2912XL	1.3.6.1.4.1.9.1.219	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat2916mxl	1.3.6.1.4.1.9.1.171	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat2924CXLv	1.3.6.1.4.1.9.1.218	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat2924MXL	1.3.6.1.4.1.9.1.220	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat295012	1.3.6.1.4.1.9.1.323	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat295024	1.3.6.1.4.1.9.1.324	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat295024C	1.3.6.1.4.1.9.1.325	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Cat2950t24	1.3.6.1.4.1.9.1.359	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat2924LREXL	1.3.6.1.4.1.9.1.369	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat295012G	1.3.6.1.4.1.9.1.427	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat295024G	1.3.6.1.4.1.9.1.428	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat295048G	1.3.6.1.4.1.9.1.429	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat_3500	1.3.6.1.4.1.9.1.111	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat_3508GXL	1.3.6.1.4.1.9.1.246	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat_3512XL	1.3.6.1.4.1.9.1.247	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat_3524XL	1.3.6.1.4.1.9.1.248	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat_3524tXLEn	1.3.6.1.4.1.9.1.287	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat_3548XL	1.3.6.1.4.1.9.1.278	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat355012G	1.3.6.1.4.1.9.1.431	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat355012T	1.3.6.1.4.1.9.1.368	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat355024	1.3.6.1.4.1.9.1.366	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat355048	1.3.6.1.4.1.9.1.367	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat355024Dc	1.3.6.1.4.1.9.1.452	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Cat355024Mmf	1.3.6.1.4.1.9.1.453	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat355024PWR	1.3.6.1.4.1.9.1.485	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat3560_24PS	1.3.6.1.4.1.9.1.563	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat3560G-24PS	1.3.6.1.4.1.9.1.614	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat3560-24TS	1.3.6.1.4.1.9.1.633	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat3560G-24TS	1.3.6.1.4.1.9.1.615	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat3560_48PS	1.3.6.1.4.1.9.1.564	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat3560G-48PS	1.3.6.1.4.1.9.1.616	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat3560-48TS	1.3.6.1.4.1.9.1.634	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat3560G-48TS	1.3.6.1.4.1.9.1.617	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat37xxStack	1.3.6.1.4.1.9.1.516	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat3750Ge12Sfp	1.3.6.1.4.1.9.1.530	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat3750_24ME	1.3.6.1.4.1.9.1.574	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat3750G16TD	1.3.6.1.4.1.9.1.591	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat375024	1.3.6.1.4.1.9.1.511	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat375024T	1.3.6.1.4.1.9.1.514	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Cat375024TS	1.3.6.1.4.1.9.1.513	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat375048	1.3.6.1.4.1.9.1.512	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat4kGateway	1.3.6.1.4.1.9.1.318	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat4000NAM	1.3.6.1.4.1.9.1.575	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat4006	1.3.6.1.4.1.9.1.448	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat4503	1.3.6.1.4.1.9.1.503	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat4510	1.3.6.1.4.1.9.1.537	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat4232L3	1.3.6.1.4.1.9.1.300	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat4506	1.3.6.1.4.1.9.1.502	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat4507	1.3.6.1.4.1.9.1.501	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat4840gL3	1.3.6.1.4.1.9.1.312	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat4908gL3	1.3.6.1.4.1.9.1.298	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat4908gL3Dc	1.3.6.1.4.1.9.1.387	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat4948	1.3.6.1.4.1.9.1.626	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat494810GE	1.3.6.1.4.1.9.1.659	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat5kRsfc	1.3.6.1.4.1.9.1.257	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Cat6kSup720	1.3.6.1.4.1.9.1.557	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat6kGateway	1.3.6.1.4.1.9.1.573	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat6503	1.3.6.1.4.1.9.1.449	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat6513	1.3.6.1.4.1.9.1.400	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat6000	1.3.6.1.4.1.9.1.241	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat6006	1.3.6.1.4.1.9.1.280	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat6009	1.3.6.1.4.1.9.1.281	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat6506	1.3.6.1.4.1.9.1.282	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat6509	1.3.6.1.4.1.9.1.283	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat6kMsfc	1.3.6.1.4.1.9.1.258	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat6kMsfc2	1.3.6.1.4.1.9.1.301	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat6509Sp	1.3.6.1.4.1.9.1.310	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat8510_CSR	1.3.6.1.4.1.9.1.190	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat8510_MSR	1.3.6.1.4.1.9.1.230	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat8515_CSR	1.3.6.1.4.1.9.1.196	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat8515_MSR	1.3.6.1.4.1.9.1.231	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Cat8540_CSR	1.3.6.1.4.1.9.1.203	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat8540_MSR	1.3.6.1.4.1.9.1.202	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat9006	1.3.6.1.4.1.9.1.197	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat9009	1.3.6.1.4.1.9.1.198	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat295024GDC	1.3.6.1.4.1.9.1.472	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat295024S	1.3.6.1.4.1.9.1.430	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat295024SX	1.3.6.1.4.1.9.1.480	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat295024LREG	1.3.6.1.4.1.9.1.484	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat295024LRESt	1.3.6.1.4.1.9.1.482	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat29508LRESt	1.3.6.1.4.1.9.1.483	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat2955C12	1.3.6.1.4.1.9.1.489	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat2955S12	1.3.6.1.4.1.9.1.508	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat2955T12	1.3.6.1.4.1.9.1.488	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat29408TF	1.3.6.1.4.1.9.1.542	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat29408TT	1.3.6.1.4.1.9.1.540	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat295048SX	1.3.6.1.4.1.9.1.560	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

Cisco 対応デバイス

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Cat295048T	1.3.6.1.4.1.9.1.559	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
Cat2950St24LRE 997	1.3.6.1.4.1.9.1.551	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CatExpress500-24LC	1.3.6.1.4.1.9.1.725	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CatExpress500-12TC	1.3.6.1.4.1.9.1.727	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CatExpress500-24PC	1.3.6.1.4.1.9.1.726	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CatExpress500-24TT	1.3.6.1.4.1.9.1.724	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい
CatWsCBS3040F SC	1.3.6.1.4.1.9.1.784	*CISCO-CONFIG-COP Y-MIB	はい	**はい	はい

* IOS < 12.0 = OLD-CISCO-SYSTEM-MIB

** IOS > 12.2(18) 機能「K9」有り

Cisco 対応デバイス

CA Spectrum Network Configuration Manager は、以下の Cisco デバイスをサポートします。サポートされている Catalyst デバイスのリストについては、「Cisco 対応 Catalyst デバイス」を参照してください。

この表には例が示されます。デバイス サポートの最新情報については、[CA デバイス認定データベースにアクセス \(P. 17\)](#)してください。

Perl スクリプトがデバイスで唯一の通信手段である場合、スクリプト メソッドが提供されます。

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
PIX Firewall	1.3.6.1.4.1.9.1.227	いいえ	いいえ	いいえ	Telnet

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
PIX 506 Firewall	1.3.6.1.4.1.9.1.389	いいえ	いいえ	いいえ	Telnet
PIX 515 Firewall	1.3.6.1.4.1.9.1.390	いいえ	いいえ	いいえ	Telnet
PIX 520 Firewall	1.3.6.1.4.1.9.1.391	いいえ	いいえ	いいえ	Telnet
PIX 525 Firewall	1.3.6.1.4.1.9.1.392	いいえ	いいえ	いいえ	Telnet
PIX 535 Firewall	1.3.6.1.4.1.9.1.393	いいえ	いいえ	いいえ	Telnet
PIX 501 Firewall	1.3.6.1.4.1.9.1.417	いいえ	いいえ	いいえ	Telnet
PIX 515E Firewall	1.3.6.1.4.1.9.1.451	いいえ	いいえ	いいえ	Telnet
PIX 506E Firewall	1.3.6.1.4.1.9.1.450	いいえ	いいえ	いいえ	Telnet
cat6500Firewall Sm	1.3.6.1.4.1.9.1.522	いいえ	いいえ	いいえ	Telnet
PIX Firewall Security Module	1.3.6.1.4.1.9.1.674	いいえ	いいえ	いいえ	Telnet
PIX 535sc Firewall	1.3.6.1.4.1.9.1.675	いいえ	いいえ	いいえ	Telnet
PIX 525sc Firewall	1.3.6.1.4.1.9.1.676	いいえ	いいえ	いいえ	Telnet
PIX 515Esc Firewall	1.3.6.1.4.1.9.1.677	いいえ	いいえ	いいえ	Telnet
PIX 515sc Firewall	1.3.6.1.4.1.9.1.678	いいえ	いいえ	いいえ	Telnet
PIX Firewall System Module	1.3.6.1.4.1.9.1.767	いいえ	いいえ	いいえ	Telnet
PIX 515sy Firewall	1.3.6.1.4.1.9.1.768	いいえ	いいえ	いいえ	Telnet
PIX 515Esy Firewall	1.3.6.1.4.1.9.1.769	いいえ	いいえ	いいえ	Telnet
PIX 525sy Firewall	1.3.6.1.4.1.9.1.770	いいえ	いいえ	いいえ	Telnet

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
PIX 535sy Firewall	1.3.6.1.4.1.9.1.771	いいえ	いいえ	いいえ	Telnet

* IOS < 12.0 = OLD-CISCO-SYSTEM-MIB

** IOS > 12.2(18) 機能「K9」有り

Cisco CAT 対応デバイス

以下の表は、CA Spectrum Network Configuration Manager でサポートされている Cisco CAT デバイスを示しています。この表には例が示されます。デバイス サポートの最新情報については、[CA デバイス認定データベースにアクセス](#) (P. 17) してください。

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Cat2926	1.3.6.1.4.1.9.5.35	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
Cat_2948G	1.3.6.1.4.1.9.5.42	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
Cat2948gget x	1.3.6.1.4.1.9.5.62	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
Cat2980ga	1.3.6.1.4.1.9.5.51	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
Cat_2980GS W	1.3.6.1.4.1.9.5.49	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
Cat_4003	1.3.6.1.4.1.9.5.40	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
Cat_4006	1.3.6.1.4.1.9.5.46	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
Cat4503	1.3.6.1.4.1.9.5.58	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Cat_4506	1.3.6.1.4.1.9.5.59	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
Cat4912	1.3.6.1.4.1.9.5.41	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
Cat6knam	1.3.6.1.4.1.9.5.48	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
Cat6503	1.3.6.1.4.1.9.5.56	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
Cat6509neba	1.3.6.1.4.1.9.5.61	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
Cat7603	1.3.6.1.4.1.9.5.53	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
Cat7604	1.3.6.1.4.1.9.5.63	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
Cat7606	1.3.6.1.4.1.9.5.54	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
Cat7609	1.3.6.1.4.1.9.5.55	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
Cat7613	1.3.6.1.4.1.9.5.60	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
CiscoWSC6504E	1.3.6.1.4.1.9.5.64	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
HubCat1400	1.3.6.1.4.1.9.5.6	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
HubCat5000	1.3.6.1.4.1.9.5.7	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
HubCat5002	1.3.6.1.4.1.9.5.29	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
HubCat5500	1.3.6.1.4.1.9.5.17	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
HubCat5505	1.3.6.1.4.1.9.5.34	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい

Cisco NX OS をサポートしているデバイス

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
HubCat5509	1.3.6.1.4.1.9.5.36	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
SwCat1200	1.3.6.1.4.1.9.5.5	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
WS-C6006	1.3.6.1.4.1.9.5.38	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
WS-C6009	1.3.6.1.4.1.9.5.39	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
WS-C6506	1.3.6.1.4.1.9.5.45	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
WS-C6509	1.3.6.1.4.1.9.5.44	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
WS-C6509ne b	1.3.6.1.4.1.9.5.47	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい
WS-C6513	1.3.6.1.4.1.9.5.50	CISCO-CONFIG-COPY -MIB*	いいえ	いいえ	はい

* CATOS < 8.4 = CISCO-STACK-MIB

Cisco NX OS をサポートしているデバイス

以下の表は、CA Spectrum Network Configuration Manager でサポートされている Cisco NX OS デバイスを示しています。

注: Cisco NX OS デバイスは、Net::SSH::Expect モジュールを使用するスクリプトによってサポートされます。Cisco NX OS デバイスを標準でサポートするこれらのモジュールで、Perl の領域をセットアップする必要があります。

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Cisco Nexus 1000V VSM	1.3.6.1.4.1.9.12.3.1.3.840	いいえ	いいえ	いいえ	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Cisco Nexus 2000	1.3.6.1.4.1.9.12.3.1.3.820	いいえ	いいえ	いいえ	はい
Cisco Nexus 5000	1.3.6.1.4.1.9.12.3.1.3.719	いいえ	いいえ	いいえ	はい
Cisco Nexus 7000	1.3.6.1.4.1.9.12.3.1.3.612	いいえ	いいえ	いいえ	はい

Enterasys 対応デバイス

以下の表は、CA Spectrum Network Configuration Manager でサポートされている Enterasys デバイスを示しています。この表には例が示されます。デバイスサポートの最新情報については、[CA デバイス認定データベースにアクセス](#) (P. 17) してください。

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
1G582-09	1.3.6.1.4.1.5624.2.1.35	ENTERASYS-CONF G-MAN-MIB	いいえ	いいえ	はい
1G694-13	1.3.6.1.4.1.5624.2.1.36	ENTERASYS-CONF G-MAN-MIB	いいえ	いいえ	はい
1H582-25	1.3.6.1.4.1.5624.2.1.59	ENTERASYS-CONF G-MAN-MIB	いいえ	いいえ	はい
1H582-51	1.3.6.1.4.1.5624.2.1.34	ENTERASYS-CONF G-MAN-MIB	いいえ	いいえ	はい
1G587-09	1.3.6.1.4.1.5624.2.1.60	ENTERASYS-CONF G-MAN-MIB	いいえ	いいえ	はい
Matrix N	1.3.6.1.4.1.5624.2.1.51	ENTERASYS-CONF G-MAN-MIB	いいえ	いいえ	はい
Matrix N1	1.3.6.1.4.1.5624.2.1.83	ENTERASYS-CONF G-MAN-MIB	いいえ	いいえ	はい
Matrix N3	1.3.6.1.4.1.5624.2.1.53	ENTERASYS-CONF G-MAN-MIB	いいえ	いいえ	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Matrix N5	1.3.6.1.4.1.5624.2.1.79	ENTERASYS-CONFIDENTIAL G-MAN-MIB	いいえ	いいえ	はい
Matrix N7	1.3.6.1.4.1.5624.2.1.52	ENTERASYS-CONFIDENTIAL G-MAN-MIB	いいえ	いいえ	はい
Matrix N ルータ	1.3.6.1.4.1.5624.2.1.70	ENTERASYS-CONFIDENTIAL G-MAN-MIB	いいえ	いいえ	はい
Matrix N スタンドアロン	1.3.6.1.4.1.5624.2.1.77	ENTERASYS-CONFIDENTIAL G-MAN-MIB	いいえ	いいえ	はい
SecureStack A2H124-24	1.3.6.1.4.1.5624.2.1.87	ENTERASYS-CONFIDENTIAL G-MAN-MIB	いいえ	いいえ	はい
SecureStack A2H124-24FX	1.3.6.1.4.1.5624.2.1.91	ENTERASYS-CONFIDENTIAL G-MAN-MIB	いいえ	いいえ	はい
SecureStack A2H124-24P	1.3.6.1.4.1.5624.2.1.88	ENTERASYS-CONFIDENTIAL G-MAN-MIB	いいえ	いいえ	はい
SecureStack A2H124-48	1.3.6.1.4.1.5624.2.1.89	ENTERASYS-CONFIDENTIAL G-MAN-MIB	いいえ	いいえ	はい
SecureStack A2H124-48P	1.3.6.1.4.1.5624.2.1.90	ENTERASYS-CONFIDENTIAL G-MAN-MIB	いいえ	いいえ	はい
SecureStack A2H254-16	1.3.6.1.4.1.5624.2.1.95	ENTERASYS-CONFIDENTIAL G-MAN-MIB	いいえ	いいえ	はい
SecureStack B2G124-24	1.3.6.1.4.1.5624.2.2.314	ENTERASYS-CONFIDENTIAL G-MAN-MIB	いいえ	いいえ	はい
SecureStack B2G124-48	1.3.6.1.4.1.5624.2.2.315	ENTERASYS-CONFIDENTIAL G-MAN-MIB	いいえ	いいえ	はい
SecureStack B2G124-48P	1.3.6.1.4.1.5624.2.2.316	ENTERASYS-CONFIDENTIAL G-MAN-MIB	いいえ	いいえ	はい
SecureStack B2H124-48	1.3.6.1.4.1.5624.2.2.317	ENTERASYS-CONFIDENTIAL G-MAN-MIB	いいえ	いいえ	はい
SecureStack B2H124-48P	1.3.6.1.4.1.5624.2.2.318	ENTERASYS-CONFIDENTIAL G-MAN-MIB	いいえ	いいえ	はい
SecureStack B3G124-24	1.3.6.1.4.1.5624.2.1.100	ENTERASYS-CONFIDENTIAL G-MAN-MIB	いいえ	いいえ	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
SecureStack B3G124-24P	1.3.6.1.4.1.5624.2.1.101	ENTERASYS-CONF1 G-MAN-MIB	いいえ	いいえ	はい
SecureStack B3G124-48	1.3.6.1.4.1.5624.2.1.102	ENTERASYS-CONF1 G-MAN-MIB	いいえ	いいえ	はい
SecureStack B3G124-48P	1.3.6.1.4.1.5624.2.1.103	ENTERASYS-CONF1 G-MAN-MIB	いいえ	いいえ	はい
SecureStack C2G124-24	1.3.6.1.4.1.5624.2.2.283	ENTERASYS-CONF1 G-MAN-MIB	いいえ	いいえ	はい
SecureStack C2G124-48	1.3.6.1.4.1.5624.2.2.284	ENTERASYS-CONF1 G-MAN-MIB	いいえ	いいえ	はい
SecureStack C2G124-48P	1.3.6.1.4.1.5624.2.2.287	ENTERASYS-CONF1 G-MAN-MIB	いいえ	いいえ	はい
SecureStack C2G134-24P	1.3.6.1.4.1.5624.2.2.350	ENTERASYS-CONF1 G-MAN-MIB	いいえ	いいえ	はい
SecureStack C2G170-24	1.3.6.1.4.1.5624.2.2.360	ENTERASYS-CONF1 G-MAN-MIB	いいえ	いいえ	はい
SecureStack C2H124-48	1.3.6.1.4.1.5624.2.2.220	ENTERASYS-CONF1 G-MAN-MIB	いいえ	いいえ	はい
SecureStack C2H124-48P	1.3.6.1.4.1.5624.2.2.286	ENTERASYS-CONF1 G-MAN-MIB	いいえ	いいえ	はい
SecureStack C2K122-24	1.3.6.1.4.1.5624.2.2.285	ENTERASYS-CONF1 G-MAN-MIB	いいえ	いいえ	はい
SecureStack C3G124-24	1.3.6.1.4.1.5624.2.1.96	ENTERASYS-CONF1 G-MAN-MIB	いいえ	いいえ	はい
SecureStack C3G124-24P	1.3.6.1.4.1.5624.2.1.97	ENTERASYS-CONF1 G-MAN-MIB	いいえ	いいえ	はい
SecureStack C3G124-48	1.3.6.1.4.1.5624.2.1.98	ENTERASYS-CONF1 G-MAN-MIB	いいえ	いいえ	はい
SecureStack C3G124-48P	1.3.6.1.4.1.5624.2.1.99	ENTERASYS-CONF1 G-MAN-MIB	いいえ	いいえ	はい
XSR-1805	1.3.6.1.4.1.5624.2.1.32	ENTERASYS-CONF1 G-MAN-MIB	いいえ	いいえ	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
XSR-1850	1.3.6.1.4.1.5624.2.1.45	ENTERASYS-CONFIG-MAN-MIB	いいえ	いいえ	はい
XSR-1800	1.3.6.1.4.1.5624.2.1	ENTERASYS-CONFIG-MAN-MIB	いいえ	いいえ	はい

Enterasys/Riverstone SSR 対応デバイス

以下の表は、CA Spectrum Network Configuration Manager でサポートされている Enterasys/Riverstone SSR デバイスを示しています。この表には例が示されます。デバイスサポートの最新情報については、[CA デバイス認定データベースにアクセス \(P. 17\)](#) してください。

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
DEC 8000	1.3.6.1.4.1.36.2.15.30.1	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
DEC 8600	1.3.6.1.4.1.36.2.15.30.2	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
DEC 2000	1.3.6.1.4.1.36.2.15.30.3	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
OLI-8000	1.3.6.1.4.1.285.9.25	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
OLI-8600	1.3.6.1.4.1.285.9.26	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
OLI-2000	1.3.6.1.4.1.285.9.27	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
CPQ-8000	1.3.6.1.4.1.232.134.1.1	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
CPQ-8600	1.3.6.1.4.1.232.134.1.2	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
CPQ-2000	1.3.6.1.4.1.232.134.1.3	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
6-SSRM-02	1.3.6.1.4.1.52.3.9.33.4.1	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
RS-8000	1.3.6.1.4.1.5567.1.1.1	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
RS-8600	1.3.6.1.4.1.5567.1.1.2	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
RS-2000	1.3.6.1.4.1.5567.1.1.3	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
RS-2100	1.3.6.1.4.1.5567.1.1.4	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
RS-3000	1.3.6.1.4.1.5567.1.1.5	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
IA-1100	1.3.6.1.4.1.5567.1.1.22	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
IA-1200	1.3.6.1.4.1.5567.1.1.23	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
RS-1000	1.3.6.1.4.1.5567.1.1.8	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
IA-1500	1.3.6.1.4.1.5567.1.1.27	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
SSR-8000	1.3.6.1.4.1.52.3.9.20.1.3	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
SSR-8600	1.3.6.1.4.1.52.3.9.20.1.4	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
SSR-2000	1.3.6.1.4.1.52.3.9.33.1.1	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
SSR-2100	1.3.6.1.4.1.52.3.9.33.1.3	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
IA-1000	1.3.6.1.4.1.52.3.9.33.2.8	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
IA-2000	1.3.6.1.4.1.52.3.9.33.2.9	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい

Extreme 対応デバイス

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
XP-2400	1.3.6.1.4.1.5624.2.1.42	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
RS-32000	1.3.6.1.4.1.5567.1.1.6	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
RS-38000	1.3.6.1.4.1.5567.1.1.9	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
SSR-32000	1.3.6.1.4.1.52.10.2	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
ER16	1.3.6.1.4.1.5624.2.1.23	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
BE2800	1.3.6.1.4.1.1456.3.2	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
Terayon ルータ	1.3.6.1.4.1.1456.3.3	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい
5-SSRM-02	1.3.6.1.4.1.5624.2.1.24	CTRON-SSR-CONFIG-MIB	いいえ	いいえ	はい

Extreme 対応デバイス

以下の表は、CA Spectrum Network Configuration Manager でサポートされている Extreme デバイスを示しています。この表には例が示されます。デバイスサポートの最新情報については、[CA デバイス認定データベースにアクセス](#) (P. 17) してください。

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Alpine 3802	1.3.6.1.4.1.1916.2.26	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Alpine 3804	1.3.6.1.4.1.1916.2.20	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Alpine 3808	1.3.6.1.4.1.1916.2.17	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Altitude 300	1.3.6.1.4.1.1916.2.86	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Altitude 350	1.3.6.1.4.1.1916.2.75	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
BlackDiamond 6800	1.3.6.1.4.1.1916.2.8	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
BlackDiamond 6804	1.3.6.1.4.1.1916.2.27	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
BlackDiamond 6808	1.3.6.1.4.1.1916.2.11	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
BlackDiamond 6816	1.3.6.1.4.1.1916.2.24	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
BlackDiamond 8806	1.3.6.1.4.1.1916.2.74	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
BlackDiamond 8810	1.3.6.1.4.1.1916.2.62	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
BlackDiamond 10808	1.3.6.1.4.1.1916.2.56	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
BlackDiamond 12802	1.3.6.1.4.1.1916.2.85	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
BlackDiamond 12804	1.3.6.1.4.1.1916.2.77	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
EnetSwitch 24Port	1.3.6.1.4.1.1916.2.23	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Sentriant CE150	1.3.6.1.4.1.1916.2.83	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit 1	1.3.6.1.4.1.1916.2.1	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit 1iSX	1.3.6.1.4.1.1916.2.19	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit 1iTX	1.3.6.1.4.1.1916.2.14	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい

Extreme 対応デバイス

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Summit 2	1.3.6.1.4.1.1916.2.2	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit 3	1.3.6.1.4.1.1916.2.3	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit 4	1.3.6.1.4.1.1916.2.4	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit 4FX	1.3.6.1.4.1.1916.2.5	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit 5i	1.3.6.1.4.1.1916.2.15	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit 5iLX	1.3.6.1.4.1.1916.2.21	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit 5iTX	1.3.6.1.4.1.1916.2.22	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit 7iSX	1.3.6.1.4.1.1916.2.12	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit 7iTX	1.3.6.1.4.1.1916.2.13	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit 24	1.3.6.1.4.1.1916.2.7	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit 24e2SX	1.3.6.1.4.1.1916.2.41	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit 24e2TX	1.3.6.1.4.1.1916.2.40	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit 24e3	1.3.6.1.4.1.1916.2.25	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit 48	1.3.6.1.4.1.1916.2.6	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit 48i	1.3.6.1.4.1.1916.2.16	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit 48i1u	1.3.6.1.4.1.1916.2.28	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Summit 200-24	1.3.6.1.4.1.1916.2.53	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit 200-24fx	1.3.6.1.4.1.1916.2.70	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit 200-48	1.3.6.1.4.1.1916.2.54	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit 300-24	1.3.6.1.4.1.1916.2.61	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit 300-48	1.3.6.1.4.1.1916.2.55	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit 400-24	1.3.6.1.4.1.1916.2.59	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit 400-24p	1.3.6.1.4.1.1916.2.64	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit 400-24t	1.3.6.1.4.1.1916.2.63	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit 400-48t	1.3.6.1.4.1.1916.2.58	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit Px1	1.3.6.1.4.1.1916.2.30	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit Ver2Stack	1.3.6.1.4.1.1916.2.93	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit X250-24p	1.3.6.1.4.1.1916.2.89	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit X250-24t	1.3.6.1.4.1.1916.2.88	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit X250-24x	1.3.6.1.4.1.1916.2.90	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit X250-48p	1.3.6.1.4.1.1916.2.92	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit X250-48t	1.3.6.1.4.1.1916.2.91	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Summit X450-24t	1.3.6.1.4.1.1916.2.66	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit X450-24x	1.3.6.1.4.1.1916.2.65	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit X450a-24t	1.3.6.1.4.1.1916.2.71	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit X450a-24tDC	1.3.6.1.4.1.1916.2.80	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit X450a-24x	1.3.6.1.4.1.1916.2.84	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit X450a-24xDC	1.3.6.1.4.1.1916.2.82	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit X450a-48t	1.3.6.1.4.1.1916.2.76	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit X450a-48tDC	1.3.6.1.4.1.1916.2.87	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit X450e-24p	1.3.6.1.4.1.1916.2.72	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
Summit X450e-48p	1.3.6.1.4.1.1916.2.79	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
SummitStack	1.3.6.1.4.1.1916.2.67	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
SummitWM 100	1.3.6.1.4.1.1916.2.68	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
SummitWM 200	1.3.6.1.4.1.1916.2.94	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
SummitWM 1000	1.3.6.1.4.1.1916.2.69	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい
SummitWM 2000	1.3.6.1.4.1.1916.2.95	EXTREME-FILETRA NSFER-MIB	いいえ	いいえ	はい

Foundry 対応デバイス

以下の表は、CA Spectrum Network Configuration Manager でサポートされている Foundry デバイスを示しています。この表には例が示されます。デバイスサポートの最新情報については、[CA デバイス認定データベースにアクセス](#) (P. 17) してください。

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
BigIronMG8S w	1.3.6.1.4.1.1991.1.3.32.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
BigIronMG8 Rt	1.3.6.1.4.1.1991.1.3.32.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
BigIronRX4Rt	1.3.6.1.4.1.1991.1.3.40.3.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
BigIronRX4S w	1.3.6.1.4.1.1991.1.3.40.3.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
BigIronRX8Rt	1.3.6.1.4.1.1991.1.3.40.2.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
BigIronRX8S w	1.3.6.1.4.1.1991.1.3.40.2.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
BigIronRX16 Rt	1.3.6.1.4.1.1991.1.3.40.1.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
BigIronRX16 Sw	1.3.6.1.4.1.1991.1.3.40.1.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
BigIronSXL3S w	1.3.6.1.4.1.1991.1.3.37.1.3	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
BigIronSXRx	1.3.6.1.4.1.1991.1.3.37.1.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
BigIronSXSw	1.3.6.1.4.1.1991.1.3.37.1.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
Blron4000Rt	1.3.6.1.4.1.1991.1.3.6.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
Blron4000SI	1.3.6.1.4.1.1991.1.3.6.3	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Blron4000Sw	1.3.6.1.4.1.1991.1.3.6.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
Blron8000Rt	1.3.6.1.4.1.1991.1.3.7.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
Blron8000SI	1.3.6.1.4.1.1991.1.3.7.3	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
Blron15000Rt	1.3.6.1.4.1.1991.1.3.14.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
Blron15000S	1.3.6.1.4.1.1991.1.3.14.3	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
Blron8000Sw	1.3.6.1.4.1.1991.1.3.7.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
Blron15000Sw	1.3.6.1.4.1.1991.1.3.14.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FastIronBBSw	1.3.6.1.4.1.1991.1.3.1.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FastIron2Rt	1.3.6.1.4.1.1991.1.3.8.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FastIron2Sw	1.3.6.1.4.1.1991.1.3.8.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FastIron3Rt	1.3.6.1.4.1.1991.1.3.16.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FastIron3Sw	1.3.6.1.4.1.1991.1.3.16.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FastIronWGSw	1.3.6.1.4.1.1991.1.3.1.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FES2402Sw	1.3.6.1.4.1.1991.1.3.25.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FES2402Rt	1.3.6.1.4.1.1991.1.3.25.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FES4802Rt	1.3.6.1.4.1.1991.1.3.26.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
FES4802Sw	1.3.6.1.4.1.1991.1.3.26.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FES9604Rt	1.3.6.1.4.1.1991.1.3.27.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FES9604Sw	1.3.6.1.4.1.1991.1.3.27.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FES12GCFRt	1.3.6.1.4.1.1991.1.3.28.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FES12GCFSw	1.3.6.1.4.1.1991.1.3.28.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FES2402POE Rt	1.3.6.1.4.1.1991.1.3.29.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FES2402POE Sw	1.3.6.1.4.1.1991.1.3.29.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FES4802POE Rt	1.3.6.1.4.1.1991.1.3.30.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FES4802POE Sw	1.3.6.1.4.1.1991.1.3.30.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424Rt 2	1.3.6.1.4.1.1991.1.3.34.1.1.1.	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424Sw 1	1.3.6.1.4.1.1991.1.3.34.1.1.1.	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424Pre mRt 2	1.3.6.1.4.1.1991.1.3.34.1.1.2.	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424Pre mSw 1	1.3.6.1.4.1.1991.1.3.34.1.1.2.	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424P1X GPremSw 1	1.3.6.1.4.1.1991.1.3.34.1.2.2.	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424P1X GRt 2	1.3.6.1.4.1.1991.1.3.34.1.2.1.	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424P1X GSw 1	1.3.6.1.4.1.1991.1.3.34.1.2.1.	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
FESX424P1X GPremRt 2	1.3.6.1.4.1.1991.1.3.34.1.2.2.	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424P2X GRt 2	1.3.6.1.4.1.1991.1.3.34.1.3.1.	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424P2X GSw 1	1.3.6.1.4.1.1991.1.3.34.1.3.1.	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424P2X GPremRt 2	1.3.6.1.4.1.1991.1.3.34.1.3.2.	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424P2X GPremSw 1	1.3.6.1.4.1.1991.1.3.34.1.3.2.	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX448Rt 2	1.3.6.1.4.1.1991.1.3.34.2.1.1.	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX448Sw 1	1.3.6.1.4.1.1991.1.3.34.2.1.1.	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX448Pre mRt 2	1.3.6.1.4.1.1991.1.3.34.2.1.2.	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX448Pre mSw 1	1.3.6.1.4.1.1991.1.3.34.2.1.2.	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX448P1X GSw 1	1.3.6.1.4.1.1991.1.3.34.2.2.1.	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX448P1X GRt 2	1.3.6.1.4.1.1991.1.3.34.2.2.1.	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX448P1X GPremRt 2	1.3.6.1.4.1.1991.1.3.34.2.2.2.	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX448P1X GPremSw 1	1.3.6.1.4.1.1991.1.3.34.2.2.2.	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX448P2X GRt 2	1.3.6.1.4.1.1991.1.3.34.2.3.1.	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX448P2X GSw 1	1.3.6.1.4.1.1991.1.3.34.2.3.1.	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX448P2X GPremRt 2	1.3.6.1.4.1.1991.1.3.34.2.3.2.	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
FESX448P2X GPremSw	1.3.6.1.4.1.1991.1.3.34.2.3.2. 1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424Fibe rRt	1.3.6.1.4.1.1991.1.3.34.3.1.1. 2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424Fibe rSw	1.3.6.1.4.1.1991.1.3.34.3.1.1. 1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424Fibe rPremRt	1.3.6.1.4.1.1991.1.3.34.3.1.2. 2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424Fibe rPremSw	1.3.6.1.4.1.1991.1.3.34.3.1.2. 1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424Fibe rP1XGRt	1.3.6.1.4.1.1991.1.3.34.3.2.1. 2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424Fibe rP1XGSw	1.3.6.1.4.1.1991.1.3.34.3.2.1. 1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424Fibe rP1XGPremR t	1.3.6.1.4.1.1991.1.3.34.3.2.2. 2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424Fibe rP1XGPremS w	1.3.6.1.4.1.1991.1.3.34.3.2.2. 1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424Fibe rP2XGRt	1.3.6.1.4.1.1991.1.3.34.3.3.1. 2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424Fibe rP2XGSw	1.3.6.1.4.1.1991.1.3.34.3.3.1. 1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424Fibe rP2XGPremR t	1.3.6.1.4.1.1991.1.3.34.3.3.2. 2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424Fibe rP2XGPremS w	1.3.6.1.4.1.1991.1.3.34.3.3.2. 1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX448Fibe rRt	1.3.6.1.4.1.1991.1.3.34.4.1.1. 2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX448Fibe rSw	1.3.6.1.4.1.1991.1.3.34.4.1.1. 1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
FESX448Fibe rPremRt	1.3.6.1.4.1.1991.1.3.34.4.1.2. 2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX448Fibe rPremSw	1.3.6.1.4.1.1991.1.3.34.4.1.2. 1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX448Fibe rP1XGRt	1.3.6.1.4.1.1991.1.3.34.4.2.1. 2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX448Fibe rP1XGSw	1.3.6.1.4.1.1991.1.3.34.4.2.1. 1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX448Fibe rP1XGPremR t	1.3.6.1.4.1.1991.1.3.34.4.2.2. 2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX448Fibe rP1XGPremS w	1.3.6.1.4.1.1991.1.3.34.4.2.2. 1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX448Fibe rP2XGRt	1.3.6.1.4.1.1991.1.3.34.4.3.1. 2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX448Fibe rP2XGSw	1.3.6.1.4.1.1991.1.3.34.4.3.1. 1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX448Fibe rP2XGPremR t	1.3.6.1.4.1.1991.1.3.34.4.3.2. 2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX448Fibe rP2XGPremS w	1.3.6.1.4.1.1991.1.3.34.4.3.2. 1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424POE Rt	1.3.6.1.4.1.1991.1.3.34.5.1.1. 2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424POE Sw	1.3.6.1.4.1.1991.1.3.34.5.1.1. 1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424POE PremRt	1.3.6.1.4.1.1991.1.3.34.5.1.2. 2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424POE PremSw	1.3.6.1.4.1.1991.1.3.34.5.1.2. 1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424POE P1XGSw	1.3.6.1.4.1.1991.1.3.34.5.2.1. 1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
FESX424POE P1XGRt	1.3.6.1.4.1.1991.1.3.34.5.2.1. 2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424POE P1XGPremRt	1.3.6.1.4.1.1991.1.3.34.5.2.2. 2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424POE P1XGPremS w	1.3.6.1.4.1.1991.1.3.34.5.2.2. 1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424POE P2XGRt	1.3.6.1.4.1.1991.1.3.34.5.3.1. 2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424POE P2XGSw	1.3.6.1.4.1.1991.1.3.34.5.3.1. 1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424POE P2XGPremRt	1.3.6.1.4.1.1991.1.3.34.5.3.2. 2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FESX424POE P2XGPremS w	1.3.6.1.4.1.1991.1.3.34.5.3.2. 1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FWSX424Rt	1.3.6.1.4.1.1991.1.3.35.1.1.1. 2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FWSX424Sw	1.3.6.1.4.1.1991.1.3.35.1.1.1. 1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FWSX424P1 XGRt	1.3.6.1.4.1.1991.1.3.35.1.2.1. 2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FWSX424P1 XGSw	1.3.6.1.4.1.1991.1.3.35.1.2.1. 1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FWSX424P2 XGRt	1.3.6.1.4.1.1991.1.3.35.1.3.1. 2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FWSX424P2 XGSw	1.3.6.1.4.1.1991.1.3.35.1.3.1. 1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FWSX448Rt	1.3.6.1.4.1.1991.1.3.35.2.1.1. 2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FWSX448Sw	1.3.6.1.4.1.1991.1.3.35.2.1.1. 1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
FWSX448P1 XGRt	1.3.6.1.4.1.1991.1.3.35.2.2.1. 2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FWSX448P1 XGSw	1.3.6.1.4.1.1991.1.3.35.2.2.1. 1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FWSX448P2 XGRt	1.3.6.1.4.1.1991.1.3.35.2.3.1. 2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FWSX448P2 XGSw	1.3.6.1.4.1.1991.1.3.35.2.3.1. 1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FIron2GCRT	1.3.6.1.4.1.1991.1.3.12.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FIron2GCSw	1.3.6.1.4.1.1991.1.3.12.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FIron2PlusRt	1.3.6.1.4.1.1991.1.3.9.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FIron2PlusS w	1.3.6.1.4.1.1991.1.3.9.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FIron3GCRT	1.3.6.1.4.1.1991.1.3.17.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FIron3GCSw	1.3.6.1.4.1.1991.1.3.17.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FIron400Sw	1.3.6.1.4.1.1991.1.3.22.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FIron400Rt	1.3.6.1.4.1.1991.1.3.22.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FIron4802Rt	1.3.6.1.4.1.1991.1.3.21.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FIron4802SI	1.3.6.1.4.1.1991.1.3.21.3	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FIron4802Sw	1.3.6.1.4.1.1991.1.3.21.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FIron800Rt	1.3.6.1.4.1.1991.1.3.23.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
FIron800Sw	1.3.6.1.4.1.1991.1.3.23.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FIron1500Rt	1.3.6.1.4.1.1991.1.3.24.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FIron1500Sw	1.3.6.1.4.1.1991.1.3.24.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FIronSXrt	1.3.6.1.4.1.1991.1.3.36.1.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FIronSxsw	1.3.6.1.4.1.1991.1.3.36.1.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FIronSxl3Sw	1.3.6.1.4.1.1991.1.3.36.1.3	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FIronSXPrem L3Sw	1.3.6.1.4.1.1991.1.3.36.2.3	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FIronSXPrem Rt	1.3.6.1.4.1.1991.1.3.36.2.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FIronSXPrem Sw	1.3.6.1.4.1.1991.1.3.36.2.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FI2PlusGCSw	1.3.6.1.4.1.1991.1.3.13.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
FI2PlusGCRt	1.3.6.1.4.1.1991.1.3.13.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
NetIronRt	1.3.6.1.4.1.1991.1.3.2.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
NetIron40Gr	1.3.6.1.4.1.1991.1.3.33.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
NetIron400R	1.3.6.1.4.1.1991.1.3.10.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
NetIron800R	1.3.6.1.4.1.1991.1.3.11.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
NIron1500Rt	1.3.6.1.4.1.1991.1.3.15.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
NetIronMLX 4Rt	1.3.6.1.4.1.1991.1.3.44.3.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
NetIronMLX 16Rt	1.3.6.1.4.1.1991.1.3.44.1.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
NetIronMLX 8Rt	1.3.6.1.4.1.1991.1.3.44.2.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
NetIronXMR 16000Rt	1.3.6.1.4.1.1991.1.3.41.1.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
NetIronXMR 8000Rt	1.3.6.1.4.1.1991.1.3.41.2.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
NetIronXMR 4000Rt	1.3.6.1.4.1.1991.1.3.41.3.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
NetIronIMRR t	1.3.6.1.4.1.1991.1.3.39.1.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
NIron4802Rt w	1.3.6.1.4.1.1991.1.3.31.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
ServerIron	1.3.6.1.4.1.1991.1.3.31.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
ServerIronXL	1.3.6.1.4.1.1991.1.3.3.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
SIron400Rt	1.3.6.1.4.1.1991.1.3.18.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
SIron400Sw	1.3.6.1.4.1.1991.1.3.18.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
SIron800Rt	1.3.6.1.4.1.1991.1.3.19.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
SIron800Sw	1.3.6.1.4.1.1991.1.3.19.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
SIron1500Rt	1.3.6.1.4.1.1991.1.3.20.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
SIron1500Sw	1.3.6.1.4.1.1991.1.3.20.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
SIronXLTCS	1.3.6.1.4.1.1991.1.3.3.3	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
SIronLS100R	1.3.6.1.4.1.1991.1.3.42.9.1.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
SIronLS100S	1.3.6.1.4.1.1991.1.3.42.9.1.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
SIronLS300R	1.3.6.1.4.1.1991.1.3.42.9.2.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
SIronLS300S	1.3.6.1.4.1.1991.1.3.42.9.2.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
SIronTM100 Sw 1	1.3.6.1.4.1.1991.1.3.42.10.1.	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
SIronTM100 Sw 2	1.3.6.1.4.1.1991.1.3.42.10.1.	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
SIronTM300 Sw 1	1.3.6.1.4.1.1991.1.3.42.10.2.	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
SIronTM300 Sw 2	1.3.6.1.4.1.1991.1.3.42.10.2.	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
TurbolironSX Sw	1.3.6.1.4.1.1991.1.3.38.1.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
TurbolironSX Rt	1.3.6.1.4.1.1991.1.3.38.1.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
TurbolironSX L3Sw	1.3.6.1.4.1.1991.1.3.38.1.3	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
TurbolironSx PremSw	1.3.6.1.4.1.1991.1.3.38.2.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
TurbolironSX PremRt	1.3.6.1.4.1.1991.1.3.38.2.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
TurbolironSX PremL3Sw	1.3.6.1.4.1.1991.1.3.38.2.3	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
TIron8SIXLG	1.3.6.1.4.1.1991.1.3.5.4	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
TurbolronRt	1.3.6.1.4.1.1991.1.3.4.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
TurbolronSw	1.3.6.1.4.1.1991.1.3.4.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
Turbolron8Rt	1.3.6.1.4.1.1991.1.3.5.2	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
Turbolron8SI	1.3.6.1.4.1.1991.1.3.5.3	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい
Turbolron8Sw	1.3.6.1.4.1.1991.1.3.5.1	FOUNDRY-SN-AGENT -MIB	いいえ	いいえ	はい

Juniper 対応デバイス

以下の表は、CA Spectrum Network Configuration Manager でサポートされている Juniper デバイスを示しています。この表には例が示されます。デバイスサポートの最新情報については、[CA デバイス認定データベースにアクセス](#) (P. 17) してください。

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
EX3200	1.3.6.1.4.1.2636.1.1.1.2.3 0	いいえ	いいえ	はい	いいえ
EX4200	1.3.6.1.4.1.2636.1.1.1.2.3 1	いいえ	いいえ	はい	いいえ
EX8208	1.3.6.1.4.1.2636.1.1.1.2.3 2	いいえ	いいえ	はい	いいえ
EX8216	1.3.6.1.4.1.2636.1.1.1.2.3 3	いいえ	いいえ	はい	いいえ
IRM	1.3.6.1.4.1.2636.1.1.1.2.1 6	いいえ	いいえ	*はい	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
J2300 3	1.3.6.1.4.1.2636.1.1.1.2.1	いいえ	いいえ	*はい	はい
J4300 4	1.3.6.1.4.1.2636.1.1.1.2.1	いいえ	いいえ	*はい	はい
J6300 5	1.3.6.1.4.1.2636.1.1.1.2.1	いいえ	いいえ	*はい	はい
M5	1.3.6.1.4.1.2636.1.1.1.2.5	いいえ	いいえ	*はい	はい
M7i 0	1.3.6.1.4.1.2636.1.1.1.2.1	いいえ	いいえ	*はい	はい
M10	1.3.6.1.4.1.2636.1.1.1.2.4	いいえ	いいえ	*はい	はい
M10i 1	1.3.6.1.4.1.2636.1.1.1.2.1	いいえ	いいえ	*はい	はい
M20	1.3.6.1.4.1.2636.1.1.1.2.2	いいえ	いいえ	*はい	はい
M40	1.3.6.1.4.1.2636.1.1.1.2.1	いいえ	いいえ	*はい	はい
M40e	1.3.6.1.4.1.2636.1.1.1.2.8	いいえ	いいえ	*はい	はい
M160	1.3.6.1.4.1.2636.1.1.1.2.3	いいえ	いいえ	*はい	はい
M320	1.3.6.1.4.1.2636.1.1.1.2.9	いいえ	いいえ	*はい	はい
T320	1.3.6.1.4.1.2636.1.1.1.2.7	いいえ	いいえ	*はい	はい
T640	1.3.6.1.4.1.2636.1.1.1.2.6	いいえ	いいえ	*はい	はい
TX 7	1.3.6.1.4.1.2636.1.1.1.2.1	いいえ	いいえ	*はい	はい

* デバイスは SSH V2 をサポートしている必要があります

Lancom がサポートされているデバイス

以下の表は、CA Spectrum Network Configuration Manager でサポートされている Lancom デバイスを示しています。サポートされたデバイスでは、ファームウェア LCOS 7.58.0045 以上を実行している必要があります。この表には例が示されます。デバイス サポートの最新情報については、[CA デバイス認定データベースにアクセス \(P. 17\)](#) してください。

Perl スクリプトがデバイスで唯一の通信手段である場合、スクリプトメソッドが提供されます。

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
LANCOM 1721 VPN	1.3.6.1.4.1.2356.500.4.1721	いいえ	いいえ	いいえ	Telnet/ TFTP
LANCOM 1751	1.3.6.1.4.1.2356.100.0.1.1751	いいえ	いいえ	いいえ	Telnet/ TFTP
LANCOM 7111	1.3.6.1.4.1.2356.500.2.7111	いいえ	いいえ	いいえ	Telnet/ TFTP
LANCOM 8011	1.3.6.1.4.1.2356.500.2.8011	いいえ	いいえ	いいえ	Telnet/ TFTP

Nortel Baystack のサポートされているデバイス

以下の表は、CA Spectrum Network Configuration Manager でサポートされている Nortel Baystack デバイスを示しています。この表には例が示されます。デバイス サポートの最新情報については、[CA デバイス認定データベースにアクセス \(P. 17\)](#) してください。

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
BayStack450 -24T	1.3.6.1.4.1.45.3.35.1	いいえ	いいえ	*はい	はい
BayStack380 -24T	1.3.6.1.4.1.45.3.45.1	いいえ	いいえ	*はい	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
BayStack420	1.3.6.1.4.1.45.3.43.1	いいえ	いいえ	*はい	はい
BayStack460 -24T	1.3.6.1.4.1.45.3.49.1	いいえ	いいえ	*はい	はい
BayStack470 -48T	1.3.6.1.4.1.45.3.46.1	いいえ	いいえ	*はい	はい
BayStack425 -24T	1.3.6.1.4.1.45.3.57.2	いいえ	いいえ	*はい	はい
BayStack470 -24T	1.3.6.1.4.1.45.3.54.1	いいえ	いいえ	*はい	はい
BayStack551 0-24T	1.3.6.1.4.1.45.3.52.1	いいえ	いいえ	*はい	はい
BayStack551 0-48T	1.3.6.1.4.1.45.3.53.1	いいえ	いいえ	*はい	はい
BayStack552 0-24T-PWR	1.3.6.1.4.1.45.3.59.1	いいえ	いいえ	*はい	はい
BayStack552 0-48T-PWR	1.3.6.1.4.1.45.3.59.2	いいえ	いいえ	*はい	はい
Nortel ERS 5530-24TFD	1.3.6.1.4.1.45.3.65	いいえ	いいえ	*はい	はい

* デバイスは SSH V2 をサポートしている必要があります

Nortel Passport 対応デバイス

以下の表は、CA Spectrum Network Configuration Manager でサポートされている Nortel Passport デバイスを示しています。この表には例が示されます。デバイスサポートの最新情報については、[CA デバイス認定データベースにアクセス](#) (P. 17) してください。

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Passport142 4T	1.3.6.1.4.1.2272.42	SWL2MGMT-MIB	いいえ	いいえ	はい

デバイス名	システム OID	SNMP/TFTP サポート	Telnet サポート	SSH サポート	Perl サポート
Passport164 8	1.3.6.1.4.1.2272.43	SWL2MGMT-MIB	いいえ	いいえ	はい
Passport161 2	1.3.6.1.4.1.2272.44	SWL2MGMT-MIB	いいえ	いいえ	はい
Passport162 4	1.3.6.1.4.1.2272.45	SWL2MGMT-MIB	いいえ	いいえ	はい
Passport861 0	1.3.6.1.4.1.2272.30	RAPID-CITY MIB	いいえ	いいえ	はい
Passport860 6	1.3.6.1.4.1.2272.31	RAPID-CITY MIB	いいえ	いいえ	はい
Passport811 0	1.3.6.1.4.1.2272.32	RAPID-CITY MIB	いいえ	いいえ	はい
Passport810 6	1.3.6.1.4.1.2272.33	RAPID-CITY MIB	いいえ	いいえ	はい
Passport861 0	1.3.6.1.4.1.2272.37	RAPID-CITY MIB	いいえ	いいえ	はい
IntrWanPE1 00	1.3.6.1.4.1.2272.40	RAPID-CITY MIB	いいえ	いいえ	はい
Passport800 6	1.3.6.1.4.1.2272.280887558	RAPID-CITY MIB	いいえ	いいえ	はい
Passport801 0	1.3.6.1.4.1.2272.280887562	RAPID-CITY MIB	いいえ	いいえ	はい

付録 B: Network Configuration Manager イベント

このセクションには、以下のトピックが含まれています。

[Network Configuration Manager イベントについて \(P. 253\)](#)

[デバイス上で生成されたイベント \(P. 253\)](#)

[ポリシーで生成されたイベント \(P. 260\)](#)

[グローバル同期、キャプチャ、アップロードおよびスタートアップへの書き込みタスクで生成されたイベント \(P. 261\)](#)

[設定マネージャアプリケーションで生成されたイベント \(P. 262\)](#)

[デバイスファミリ上で生成されたイベント \(P. 263\)](#)

Network Configuration Manager イベントについて

設定変更がデバイスで発生した場合、イベントが生成されます。指定された相関イベント期間における特定のデバイスのすべてのイベントが組み合わせられます（期間は、設定マネージャの【一般設定】で設定されます）。詳細については、「[一般設定の設定 \(P. 29\)](#)」を参照してください。

情報はデバイス ラップ、Syslog ラップおよびイベント、Network Configuration Manager 内部、および一般変更イベントにマッピングされたその他のラップに基づいて相関されています。この情報はデバイス ファミリによって変わります。Cisco CatOS、Cisco IOS、Cisco IOS - SSH Capable、および Juniper JUNOS デバイス ファミリでは、標準サポートとして提供されます。インストール用にラップをカスタマイズする詳細については、「[設定通知ラップ設定 \(P. 51\)](#)」を参照してください。

デバイス上で生成されたイベント

設定変更

Event0082101b:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 3} 上のタイプ {t} のデバイス {m} で設定変更が検出されました。 (イベント [{e}])

Event00821029:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - 設定変更通知をデバイス {m} から受信しました。 (イベント [{e}])

Event0082105e:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 2} 上のデバイス {m} のランニング コンフィギュレーションが変更されました。 (イベント [{e}])

Event0082105f:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 2} 上のデバイス {m} のランニング コンフィギュレーションが変更されました。 このモデルでアラームが生成されます。 (イベント [{e}])

設定変更イベントの相関

Event0082105a:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 1} 上のタイプ {t} のデバイス {m} から設定変更通知を受信しました。

以下のデバイス トラップが提供されます。

デバイス ユーザ : {S 2}

送信者 : {S 3}

提供されているデバイス トラップ : {S 4}

以下の情報は SPECTRUM によって提供されます。

デバイス ユーザ : {S 2}

Spectrum ユーザ : {S 5}

NCM 通信モード : {S 6}

キャプチャは成功しました : {S 7}

キャプチャ エラー メッセージ : {S 8}

行変更の合計数 : {I 9}

行変更の関連数 : {I 10}

違反ポリシー : {S 11}

準拠ポリシー : {S 12}

現在の設定モデルのモデルハンドル : {H 13}

前の設定モデルのモデルハンドル : {H 14}

スタートアップ コンフィギュレーションとランニング コンフィギュレーションの比較

Event00821024:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 3} 上のデバイス {m} のスタートアップコンフィギュレーションが、ランニングコンフィギュレーションと異なります。 (イベント [{e}])

Event00821025:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 3} 上のデバイス {m} のスタートアップコンフィギュレーションが、ランニングコンフィギュレーションと異なります。。このモデルでマイナーアラームが生成されます。 (イベント [{e}])

Event00821026:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 3} 上のデバイス {m} のスタートアップコンフィギュレーションが、ランニングコンフィギュレーションと異なります。このモデルでメジャー アラームが生成されます。 (イベント [{e}])

Event00821027:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 3} 上のデバイス {m} のスタートアップ設定はその実行中の設定と異なります。このモデルで重大アラームが生成されます。 (イベント [{e}])

Event00821028:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 3} 上のデバイス {m} のスタートアップコンフィギュレーションは、ランニングコンフィギュレーションと同じです。 (イベント [{e}])

参照設定とランニング コンフィグレーションの比較

Event0082105b:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 2} 上のデバイス {m} の参照ランニングコンフィギュレーションが、現在のランニングコンフィギュレーションと異なります。 (イベント [{e}])

Event0082105c:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 2} 上のデバイス {m} の参照ランニングコンフィギュレーションが、現在のランニングコンフィギュレーションと異なります。このモデルでアラームが生成されます。 (イベント [{e}])

Event0082105d:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 2} 上のデバイス {m} の参照ランニングコンフィギュレーションは、そのランニングコンフィギュレーションと同じです。 (イベント [{e}])

ポリシーに準拠/非準拠のデバイス

Event00821016:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - タイプ {t} のデバイス {m} は、ランドスケープ {S 3} 上のポリシー {S 1} に準拠しています。
(イベント [{e}])

Event00821017:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - タイプ {t} のデバイス {m} は、ランドスケープ {S 3} 上のポリシー {S 1} に準拠していません。
(イベント [{e}])

Event00821051:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 1} 上のタイプ {t} のデバイス {m} のホスト設定が、ポリシーに準拠しているかどうかを確認できません。

特定のエラー: {S 2} (イベント [{e}])

Event00821055:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 3} のグローバルコレクション {S 2} からデバイスが削除されたので、タイプ {t} のデバイス {m} は、ポリシー {S 1} に違反しなくなりました。
(イベント [{e}])

Event00821056:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 3} のデバイスファミリ {S 2} からデバイスが削除されたので、タイプ {t} のデバイス {m} は、ポリシー {S 1} に違反しなくなりました。
(イベント [{e}])

Event00821057:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ポリシーが削除されたので、ランドスケープ {S 2} 上のタイプ {t} のデバイス {m} はポリシー {S 1} に違反しなくなりました。
(イベント [{e}])

ポリシーアラーム生成イベントに非準拠のデバイス

Event00821020:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - デバイス {m} は、ランドスケープ {S 3} 上でポリシー {S 1} に違反しました。この違反の重大度はマイナーです。
(イベント [{e}])

Event00821021:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - デバイス {m} は、ランドスケープ {S 3} 上でポリシー {S 1} に違反しました。この違反の重大度はメジャーです。
(イベント [{e}])

Event00821022:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - デバイス {m} は、
ランドスケープ {S 3} 上でポリシー {S 1} に違反しました。この違反の重大度は重大です。 (イベント [{e}])

キャプチャ成功/失敗

Event00821000:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 1} 上のタイプ {t} のデバイス {m} から、ユーザ {u} が開始したホストランニングコンフィギュレーションファイルのキャプチャが成功しました。
(イベント [{e}])

Event00821001:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 1} 上のタイプ {t} のデバイス {m} から、ユーザ {u} が開始したホストランニングコンフィギュレーションファイルのキャプチャが失敗しました。
特定のエラー: {S 3} (イベント [{e}])

Event00821049:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 1} 上のタイプ {t} のデバイス {m} から、ユーザ {u} が開始したホストスタートアップコンフィギュレーションファイルのキャプチャが成功しました。
(イベント [{e}])

Event00821050:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 1} 上のタイプ {t} のデバイス {m} から、ユーザ {u} が開始したホストスタートアップコンフィギュレーションファイルのキャプチャが失敗しました。
特定のエラー: {S 3} (イベント [{e}])

アップロード成功/失敗

Event00821002:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 1} 上のタイプ {t} のデバイス {m} で、ユーザ {u} が開始したホスト設定ファイルのロードが成功しました。 (イベント [{e}])

Event00821003:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 1} 上のタイプ {t} のデバイス {m} で、ユーザ {u} が開始したホスト設定ファイルのロードが失敗しました。
特定のエラー: {S 4} イベント [{e}]

アップロード失敗アラーム生成イベント

Event00821035:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 1} 上のタイプ {t} のデバイス {m} で、ユーザ {u} が開始したホスト設定ファイルのロードが失敗しました。
この失敗の重大度はマイナーです。 (イベント [{e}])

Event00821036:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 1} 上のタイプ {t} のデバイス {m} で、ユーザ {u} が開始したホスト設定ファイルのロードが失敗しました。
この失敗の重大度はメジャーです。 (イベント [{e}])

Event00821037:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 1} 上のタイプ {t} のデバイス {m} で、ユーザ {u} が開始したホスト設定ファイルのロードが失敗しました。
この失敗の重大度は重大です。 (イベント [{e}])

スタートアップへの書き込み成功/失敗

Event00821018:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ユーザ {u} が開始したランドスケープ {S 1} 上のタイプ {t} のデバイス {m} のスタートアップコンフィギュレーションに、ランニングコンフィギュレーションを書き込みました。 (イベント [{e}])

Event00821019:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 1} 上で、タイプ {t} のデバイス {m} のスタートアップコンフィギュレーションにランニングコンフィギュレーションを書き込もうとしましたが、失敗しました。この操作は {S 2} によって開始されました。特定のエラー: {S 3}。 (イベント [{e}])

デバイス上の NCM 有効化/無効化

Event0082102f:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - NCM がデバイス {m} に対して無効になりました。 (イベント [{e}])

Event00821030:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - NCM がデバイス {m} に対して有効になりました。 (イベント [{e}])

NCM 無効化、操作の不実行

Event00821032:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - NCM がモデルデバイスファミリ上で無効になっているので、モデル {m} では要求した NCM 操作は実行されませんでした。 (イベント [{e}])

Event00821033:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - NCM がこのモデル上で無効になっているので、モデル {m} では要求した NCM 操作が実行されませんでした。 (イベント [{e}])

Event00821034:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - このモデルがプロキシモデルなので、モデル {m} では要求した NCM 操作は実行されませんでした。 (イベント [{e}])

デバイス ファームウェアのロード

Event00821053:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 1} 上のタイプ {t} のデバイス {m} のファームウェアのロードが成功しました。コマンドラインパラメータを使用してファームウェアスクリプトを実行しました: {S 3} この操作は {u} によって開始されました。 (イベント [{e}])

Event00821054:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 1} 上のタイプ {t} のデバイス {m} へのファームウェアのロードに失敗しました。特定のエラー: {S 2} コマンドラインパラメータを使用してファームウェアスクリプトを実行しました: {S 3} (イベント [{e}])

デバイス ファミリでのデバイスの追加/削除

Event00821058:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - タイプ {t} のデバイス {m} が、ランドスケープ {S 1} 上のデバイス ファミリ {S 2} に追加されました。 (イベント [{e}])

Event00821059:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - タイプ {t} のデバイス {m} が、ランドスケープ {S 1} 上のデバイス ファミリ {S 2} から削除されました。 (イベント [{e}])

ポリシーで生成されたイベント

ポリシー有効/無効

Event00821014:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - {u} によってポリシー {m} が有効になりました。 (イベント [{e}])

Event00821015:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - {u} によってポリシー {m} が無効になりました。 (イベント [{e}])

Event00821023:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ポリシー {S 1} は無効になりました。このポリシーの違反によって過去に生成されたすべてのアラームがクリアされました。 (イベント [{e}])

変更済みポリシー

Event00821011:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - {u} によってポリシー {m} が変更されました。 (イベント [{e}])

ポリシーの違反者

Event00821012:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 1} 上でポリシー {m} に違反しています。 (イベント [{e}])

Event00821013:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 1} 上でのポリシー {m} への違反が解消されました。 (イベント [{e}])

違反ポリシー、アラーム生成イベント

Event0082101d:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 1} 上でポリシー {m} に違反しています。この違反の重大度はマイナーです。 (イベント [{e}])

Event0082101e:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 1} 上でポリシー {m} に違反しています。この違反の重大度はメジャーです。 (イベント [{e}])

グローバル同期、キャプチャ、アップロードおよびスタートアップへの書き込みタスクで生成されたイベント

Event0082101f:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 1} 上でポリシー {m} に違反しています。この違反の重大度は重大です。 (イベント [{e}])

グローバル同期、キャプチャ、アップロードおよびスタートアップへの書き込みタスクで生成されたイベント

スケジュール済み/スケジュールされていないタスク

Event00821040:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - スケジュール済みのタスク - タイプ {t} のタスク {m} が、ランドスケープ {S 2} 上の {S 1} に対してスケジュールされています。 (イベント [{e}])

Event00821041:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - タスクのスケジュール取り消し - タイプ {t} のタスク {m} に対して、ランドスケープ {S 1} でスケジュールが削除されました。 (イベント [{e}])

起動、停止、完了、一部完了したタスク

Event00821042:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - 開始済みのタスク - {S 1} によって、タイプ {t} のタスク {m} が、ランドスケープ {S 3} 上の {I 2} デバイスで開始されました。 (イベント [{e}])

Event00821043:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - タスクが停止しています - ランドスケープ {S 3} の {S 1} によって、タイプ {t} のタスク {m} が停止しました。 (イベント [{e}])

Event00821045:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - タスク完了 - タイプ {t} のタスク {m} が、ランドスケープ {S 1} 上で処理されたすべてのデバイスで完了しました。デバイスの合計数 {I 2} のうち、{I 3} 件は成功し、{I 4} 件は失敗しました。 (イベント [{e}])

Event00821044:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - 一部のタスクが完了 - タイプ {t} のタスク {m} が、ランドスケープ {S 1} 上で完了しました。未処理デバイスが {I 5} 個あります。デバイスの合計数 {I 2} のうち、{I 3} 件は成功し、{I 4} 件は失敗しました。また、{I 5} 件のデバイスは処理されませんでした。 (イベント [{e}])

タスクが一部完了したアラーム生成イベント

Event00821046:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - 一部のタスクが完了 - タイプ {t} のタスク {m} が、ランドスケープ {S 1} 上で完了しました。未処理デバイスが {l 5} 個あります。デバイスの合計数 {l 2} のうち、{l 3} 件は成功し、{l 4} 件は失敗しました。また、{l 5} 件のデバイスは処理されませんでした。マイナーアラームが生成されました。 (イベント [{e}])

Event00821047:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - 一部のタスクが完了 - タイプ {t} のタスク {m} が、ランドスケープ {S 1} 上で完了しました。未処理デバイスが {l 5} 個あります。デバイスの合計数 {l 2} のうち、{l 3} 件は成功し、{l 4} 件は失敗しました。また、{l 5} 件のデバイスは処理されませんでした。メジャー アラームが生成されました。 (イベント [{e}])

Event00821048:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - 一部のタスクが完了 - タイプ {t} のタスク {m} が、ランドスケープ {S 1} 上で完了しました。未処理デバイスが {l 5} 個あります。デバイスの合計数 {l 2} のうち、{l 3} 件は成功し、{l 4} 件は失敗しました。また、{l 5} 件のデバイスは処理されませんでした。重大アラームが生成されました。 (イベント [{e}])

設定マネージャ アプリケーションで生成されたイベント

Event0082101a:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ランドスケープ {S 1} 上の ncbservice デーモンに接続できません。 (イベント [{e}])

Event0082101c:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - デバイス設定をアーカイブできません。デバイス設定をアーカイブできません。ランドスケープ {S 2} 上のアーカイブディレクトリ {S 1} にファイルを作成できませんでした。 (イベント [{e}])

Event00821052:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - ncbservice デーモンへの接続が回復しました。 (イベント [{e}])

グローバル未承諾通知

Event0082102b:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - 設定変更の未承諾通知に応答する機能が、すべてのランドスケープ上でグローバルに無効になりました。 (イベント [{e}])

Event0082102c:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - 設定変更の未承諾通知に応答する機能が、すべてのランドスケープ上でグローバルに有効になりました。 (イベント [{e}])

デバイス ファミリ上で生成されたイベント

Event0082102d:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - NCM がデバイス ファミリ {m} に対して無効になりました。 (イベント [{e}])

Event0082102e:{d "%w- %d %m-, %Y - %T"} 設定マネージャ - NCM がデバイス ファミリ {m} に対して有効になりました。 (イベント [{e}])

付録 C: Network Configuration Manager 権限

このセクションでは、OneClick ユーザが持つ Network Configuration Manager の権限を示します。デフォルトでは、各権限が有効になっています。

注: 権限を設定する詳細については、「管理者ガイド」を参照してください。

Network Configuration Manager

管理者は Network Configuration Manager アプリケーションを設定できます。これには、設定マネージャノードとデバイスファミリノードから [情報] タブで実行される設定、および各デバイス レベルで実行される Network Configuration Manager の設定が含まれます。また、グローバル同期タスクをスケジュールする機能も含まれています。

ホスト設定のキャプチャ

オペレータに、[ホスト設定] タブからのバルク キャプチャタスクの作成またはオンデマンド キャプチャを許可します。

承認要求から設定変更を非表示

ユーザがワークフロー承認要求に設定コンテンツを含めるかどうか決定できるようにします。

NCM タスクにグローバルコレクションを含める

ユーザがグローバルコレクションと Network Configuration Manager タスクを関連付けられるようにします。コレクションへのアクセス権があることで、ユーザはコレクション内のすべてのメンバに暗黙的にアクセスできるようになります。このアクセス権を使用して、ユーザはこれらのデバイス上に設定のアップロードおよびファームウェアのロードを含め、任意のタスクを実行できます。

デバイスファームウェアのロード

オペレータがデバイスにファームウェアをアップロードできるようになります。

NCM タスクの管理

Network Configuration Manager の「タスク」フォルダへのアクセスを許可します。このフォルダへのアクセス権により、すべての CA Spectrum ランドスケープ上のすべての Network Configuration Manager タスクに 対してグローバルアクセスが提供され、これらすべてを開始、停止、編集、および削除できます。

デバイス再ロード

オペレータがデバイスにファームウェア設定を再ロードできるようになります。

デバイスの修復

オペレータに、非準拠デバイスのポリシー用の指定された修復コンテンツのアップロードを許可します。

ホスト設定をスタートアップに保存

オペレータに、バルクのスタートアップへの保存タスクの作成を許可します。

再ロードのスケジュール

オペレータがデバイスにファームウェア設定の再ロードをスケジュールできるようになります。

NCM タスクのスケジュール

オペレータがバルク タスクをスケジュールできるようになります。

タスク承認者

承認ワークフローの承認認可を制御します。

ServiceDesk

[承認ワークフロー モード] が ServiceDesk に設定されており、ユーザにこの権限がある場合、Service Desk を介した承認の取得は任意です。

OneClick

承認ワークフロー モードが OneClick に設定されており、ユーザに この権限がある場合、ユーザは自分のタスクまたは他のユーザによって開始されたタスクを承認することができます。

ホスト設定のアップロード

オペレータに、[ホスト設定] タブからのバルク アップロード タスクの作成、または自動アップロードを許可します。

キャッシュされたデバイス認証を使用

オペレータに、デバイス ファミリおよび単一のデバイス上書き設定で指定されたユーザ名およびパスワードの使用を許可します。この権限が有効になっている場合、ユーザはタスクが初期化されるたびにユーザ名およびパスワードを入力する必要はありません。この権限が無効になっている場合、タスクを開始する際（たとえば、アップロードやスタートアップへの保存）、デバイス認証のプロンプトが表示されます。

注: この権限がない状態でアップロードやスタートアップへの保存などのバルク タスクを実行している場合、デバイス認証のプロンプトが一回表示されます。その後、これと同じ認証データが、バルク操作が実行されたすべてのデバイスに使用されます。

ホスト設定の表示

オペレータに、ホスト設定へのアクセスを許可します。

NCM ポリシーの表示

Network Configuration Manager の「ポリシー」フォルダへのアクセスを許可します。このフォルダにアクセスすることで、すべての CA Spectrum ランドスケープ上のあらゆる Network Configuration Manager のポリシーへのアクセスが提供され、これらすべてを編集、有効化、無効化、および削除できます。

NCM ポリシーの作成/編集

オペレータに、新規ポリシーの作成または既存ポリシーの編集を許可します。この権限では、ユーザによるポリシーの有効化は許可されません。

NCM ポリシーの有効化/無効化

オペレータに、Network Configuration Manager ポリシーの有効化、無効化、および削除を許可します。

マスクされない設定の表示

オペレータに、ビューマスクによって隠されているコンテンツの表示を許可します。ビューマスクはデバイス ファミリ上に存在し、ローカルデバイスでの上書きが可能です。