

LogicVein

The logo for LogicVein features the text "LogicVein" in a bold, black, sans-serif font. Below the text is a stylized graphic consisting of two overlapping, horizontal, teardrop-shaped loops. The left loop is blue and the right loop is red, with a white space between them where they overlap.



 **ThirdEye**

The logo for ThirdEye features a circular icon on the left containing a stylized eye shape. To the right of the icon, the text "ThirdEye" is written in a bold, sans-serif font. "Third" is in black and "Eye" is in red.

ユーザーズマニュアル

目次

第 1 章	はじめに	9
1.1	ThirdEye について	9
1.2	ThirdEye のエディションについて	10
1.3	動作環境	11
1.4	使用ポート一覧	12
第 2 章	インストール	13
2.1	インストールする	13
2.1.1	VMware ESXi へのデプロイ	13
2.1.2	Windows Hyper-V へのデプロイ	15
2.2	ネットワークを設定する	21
2.3	ライセンスを適用する	23
2.4	初期設定(詳細設定)	24
第 3 章	ログイン/ログアウト	25
3.1	ログインする	25
3.2	ログアウトする	25
第 4 章	画面構成	26
4.1	画面の構成と各部の役割	26
4.1.1	メインタブ構成	26
4.1.2	グローバルメニュー構成	27
4.1.3	マップ画面構成	27
第 5 章	基本設定	28
5.1	クレデンシャルを設定する	28
5.1.1	共通のクレデンシャルを設定する	28
5.1.2	機器ごとにクレデンシャルを設定する	31
5.2	デバイスを追加する	34
5.2.1	1 台ずつ登録する	34
5.2.2	ネットワーク上のデバイスを登録する	35
5.2.3	Excel ファイルからインポート登録する	38
5.3	監視設定をする	40
5.3.1	異常を検知した時のアクションを設定する	40
5.3.2	Ping 監視を設定する	44
5.3.3	SNMP 情報を収集する Enterprise Suite	47
5.3.4	しきい値を設定して監視する	49
5.3.5	SNMPトラップを監視する(OID 指定)	51
5.3.6	SNMPトラップを監視する(すべて)	54
5.3.7	モニターセットを使用して多数の機器に対して監視設定をする	56
5.4	マップを設定する	59

5.4.1	マップを作成する.....	59
5.4.2	マップにデバイスを挿入する.....	61
5.4.3	トポロジーマップを作成する.....	64
5.4.4	カスタムフィールドを使用したロケーションマップを作成する.....	67
5.4.5	オブジェクトのアイコンを設定する.....	69
5.4.6	2つのオブジェクトの間を線で結ぶ.....	72
5.4.7	リンク線にインタフェースを紐付ける.....	74
5.4.8	アイコンのラベルやリンク線の表示形式を設定する.....	77
5.4.9	マップのデフォルトのデバイスラベル形式を変更する.....	79
5.4.10	マップの背景画像を設定する.....	80
5.4.11	マップの階層構造を設定する.....	82
5.5	ダッシュボードを作成する.....	84
5.5.1	ダッシュボードを追加する.....	84
5.5.2	ダッシュボードを切り替える.....	86
5.5.3	ウィジェットを追加する.....	87
5.5.4	ダッシュボードを削除する.....	89
5.5.5	ダッシュボードの編集メニュー.....	90
5.5.6	ウィジェットの編集メニュー.....	91
第6章	運用操作.....	92
6.1	障害対応.....	92
6.1.1	障害が発生しているデバイスを確認する.....	92
6.1.2	障害内容を確認する.....	94
6.1.3	障害対応後、インシデントを「解決済み」にする.....	95
6.2	SNMPで収集したデータを確認する 	96
6.2.1	コンソールからグラフを表示する.....	96
6.2.2	Excelファイルへエクスポートする.....	98
6.2.3	ダッシュボードレポートを発行する.....	99
6.2.4	ダッシュボードレポートを定期的にメールで送信する.....	99
6.3	デバイスのコンフィギュレーションを取得する 	101
6.3.1	使用する前の確認事項.....	101
6.3.2	バックアップを実行する.....	101
6.3.3	バックアップ後のステータスについて.....	103
6.3.4	取得したコンフィグを確認する.....	104
6.3.5	コンフィグの比較.....	105
6.3.6	コンフィグバックアップを無効にする.....	106
6.4	デバイスにSSH/Telnet接続をする.....	107
6.4.1	使用する前の準備.....	107
6.4.2	ターミナルを起動する.....	109

6.4.3	操作ログを確認する	Enterprise	Suite	110
6.5	リアルタイムで Ping を実行する			111
6.6	デバイスのインターフェースの Up/Down 状態を確認する			112
6.7	登録されている機器からの SNMP トラップを確認する			114
6.8	受信した Syslog を確認する	Enterprise	Suite	115
6.9	監視を一時的に停止する(非監視設定)			117
6.9.1	手動で非監視にする			117
6.9.2	スケジュールで非監視にする			119
6.9.3	非監視のデバイスを検索する			121
6.10	ジョブ管理	Enterprise	Suite	122
6.10.1	ジョブの作成			123
6.10.2	ジョブ履歴			126
6.10.3	ジョブ承認機能			126
6.10.4	過去のジョブ履歴を確認する			132
6.11	監視設定を解除する			133
6.11.1	モニターを削除する			133
6.11.2	マップからオブジェクト(デバイス/マップ)を削除する			134
6.11.3	マップを削除する			136
6.11.4	デバイスを削除する			137
6.11.5	ジョブを削除する			138
第 7 章	詳細設定			139
7.1	いろいろな監視設定をする			139
7.1.1	Web サイトの監視する	Enterprise	Suite	139
7.1.2	TCP ポートを監視する	Enterprise	Suite	141
7.1.3	計算式を使用した監視をする			143
7.1.4	トラップ受信時に特定のトラップインシデントを自動でクリアする			146
7.1.5	トラップに含まれる値でアクションを変える			147
7.2	Agent-D を使用した監視	Enterprise	Suite	151
7.2.1	Windows にインストールする			151
7.2.2	Linux にインストールする			155
7.2.3	CPU 監視			159
7.2.4	メモリ監視			164
7.2.5	HDD 監視			167
7.2.6	プロセス監視			170
7.2.7	Windows サービス監視			176
7.2.8	テキストログ監視			179
7.2.9	Windows イベントログ監視			183
7.2.10	Syslog 監視			191

7.3	MIB をコンパイルする	198
7.4	デバイスの EOL/EOS 管理 Suite	199
7.4.1	手動設定	200
7.4.2	自動設定	201
7.5	コンプライアンスの概要 Suite	203
7.5.1	ルール	204
7.5.2	コンプライアンスポリシー	209
7.5.3	自動修復機能.....	214
7.6	ドラフトコンフィギュレーション Suite	228
7.6.1	ドラフトコンフィギュレーションの作成	228
7.6.2	プレーンテキストからドラフトコンフィギュレーションをインポートする	230
7.6.3	ドラフトをエクスポートする	230
7.6.4	ドラフトを削除する.....	230
7.6.5	ドラフト同士の比較.....	231
7.6.6	ドラフトコンフィギュレーションをデバイスに適用する	231
7.7	チェンジアドバイザ Suite	232
7.7.1	チェンジアドバイザを用いてコマンドを実行する	233
7.8	閲覧ツール.....	234
7.8.1	DNS ルックアップ.....	234
7.8.2	IOS Show コマンド.....	234
7.8.3	IP ルーティングテーブル	235
7.8.4	Ping	235
7.8.5	SNMP システム情報	235
7.8.6	インタフェース概要	236
7.8.7	トレースルート.....	236
7.8.8	ポートマップ.....	236
7.8.9	ライブの ARP テーブル.....	236
7.9	変更ツール Suite	237
7.9.1	MOTD バナーの設定	237
7.9.2	NTP サーバ	237
7.9.3	SNMP コミュニティストリング	238
7.9.4	SNMP トラップホスト.....	238
7.9.5	Syslog ホスト.....	238
7.9.6	VLAN のポート割当て	239
7.9.7	インタフェース設定	239
7.9.8	コマンドランナー	240
7.9.9	ASA OS ソフトウェア配布	241
7.9.10	IOS ソフトウェア配布.....	242

7.9.11	NEC WA ソフトウェア配布	243
7.9.12	OS イメージ	244
7.9.13	OS イメージファイルの取得	244
7.9.14	Yamaha RT ファームウェアの配布	245
7.9.15	スタティックルートの追加	246
7.9.16	スタティックルートの削除	246
7.9.17	Enable Password の変更	247
7.9.18	VTY Password の変更	247
7.9.19	ユーザアカウントの削除	247
7.9.20	ユーザアカウントの追加	247
7.9.21	ローカルユーザパスワードの変更	248
7.10	バルクチェンジの概要 Suite	249
7.10.1	バルクチェンジジョブを作成する	249
7.11	ユーザを登録する	254
7.11.1	権限を追加する	254
7.11.2	ユーザを追加する	259
7.11.3	ユーザ情報を変更する	261
7.11.4	ログイン中のユーザのパスワードを変更する	262
7.11.5	Active Directory または RADIUS サーバと連携する	263
7.11.6	ユーザのセッションタイムアウトを設定する	268
7.11.7	ユーザを削除する	269
7.11.8	権限を削除する	270
7.12	データ保存期間を変更する	271
7.13	メールサーバを設定する	272
7.14	SNMP トラップ送信を設定する Enterprise Suite	274
7.15	カスタムデバイスフィールドのカラム名を変更する	276
7.16	ホスト名に sysName を使用する	277
7.17	Syslog ファイルの保存期間/サイズを設定する Enterprise Suite	278
7.18	Syslog ファイルを外部ストレージに保存する Enterprise Suite	279
7.19	メモテンプレートを編集する	284
7.20	右クリックメニューに特定の URL を追加する	285
7.21	ライセンスを更新する	287
7.22	オンラインでアップデートをする	288
7.23	バージョン(リビジョン)を確認する	289
7.24	プロキシサーバを使用する	290
7.25	Zero-Touch (オプション) Suite	291
7.25.1	Zero-Touch 要求条件	292
7.25.2	Zero-Touch タイプの選択	293

7.25.3	DHCP サーバ.....	294
7.25.4	コンフィギュレーションの配布.....	297
7.25.5	新規導入デバイスを扱う際の注意.....	305
7.25.6	3G ネットワークあるいは VPN 付きモバイルルータ経由での配布.....	305
7.25.7	デバイスを手元で設定してから遠隔地に送付する場合.....	306
7.25.8	ブートストラップコードの配布.....	307
第 8 章	システムバックアップ／復元.....	308
8.1	自動でシステムバックアップを実行する.....	308
8.2	手動でシステムバックアップを実行する.....	309
8.3	システムバックアップの保有数を変更する.....	310
8.4	外部ストレージに保存する.....	311
8.5	復元する.....	313
第 9 章	再起動／シャットダウン.....	316
第 10 章	アンインストール.....	317
10.1	アンインストールする.....	317
第 11 章	お問い合わせ.....	318
第 12 章	巻末資料.....	319
12.1	ICMP ポーリングについて.....	319

改訂履歴

版数	発行日	改訂内容
第 1 版	2022 年 4 月 20 日	初版発行

第1章 はじめに



本書は、ネットワーク障害監視ソフトウェア「ThirdEye」のマニュアルです。ThirdEye の各種設定や操作方法について説明します。

1.1 ThirdEye について





ThirdEye は、小規模ネットワーク環境から大規模ネットワーク環境まで、幅広くご利用いただけるネットワーク障害監視ツールです。ThirdEye では、以下のことができます。

- ポーリング監視 (ICMP Ping、SNMP ポーリング)
- SNMPトラップ監視
- しきい値監視
- インシデント管理 (重大度、ステータス、優先度、担当者、イベント集約)
- ダッシュボード管理 (統計情報のグラフ表示、ウィジェットのカスタマイズ)
- インベントリ管理 (表示のカスタマイズ、ソート、検索)
- マップ管理 (階層構造の設定、マップのツリー表示、インシデント通知、L2 マップの自動描画)
- 監視項目のセット・テンプレート登録
- 統計情報のエクスポート
- 非監視期間の設定
- ターミナルプロキシによる証跡管理
- インシデント更新時の E メール通知
- プライベート MIB のコンパイル
- コンフィギュレーションバックアップと世代管理
- ネットワーク機器 (ルータ/スイッチ/ファイアウォールなど) の設定変更
- Syslog 監視

1.2 ThirdEye のエディションについて

ThirdEye には、「Suite」、「Enterprise」、「Basic」の 3 つのエディションがあります。エディションによって、使用できる機能が異なります。エディションの違いによる機能差は、以下の【エディションによる主な機能比較表】をご参照ください。また、本書では最上位エディションである「Suite」をベースにすべての機能を説明しており、「Basic」や「Enterprise」では使用できない機能があります。特定のエディションでしか使用できない機能には、各説明項目のタイトルに  /  のようなアイコンが表示されています。

【アイコンの種類】

- 3 エディション共通で使用可能 …  または、アイコンなし
- Basic で使用可能 … 
- Enterprise で使用可能 … 
- Suite で使用可能 … 

【エディションによる主な機能比較表】

機能		Basic	Enterprise	Suite
ディスカバリ		○	○	○
監視	ICMP	○	○	○
	SNMP	×	○	○
	SNMPトラップ	○	○	○
	HTTP/HTTPS	×	○	○
	TCP ポート	×	○	○
	vCenter	×	○	○
	VMware Guest	×	○	○
	VMware Host	×	○	○
	Xen Server	×	○	○
	Agent-D	×	○	○
	Syslog 監視	×	○	○
非監視	手動	○	○	○
	スケジュール	○	○	○
アクション/通知機能	インシデント	○	○	○
	メール	○	○	○
	コマンド実行	○	○	○
	トラップ送信	○	○	○
	ジョブ実行	×	×	○
コンフィグ管理	コンフィグバックアップ	×	○	○
	世代管理	×	○	○
	比較	×	○	○
	エクスポート	×	○	○
コンフィグ変更	バルクチェンジ	×	×	○
	復元	×	○	○
	変更ツール	×	×	○
	ドラフトコンフィグ	×	×	○
ターミナルプロキシ	Telnet/SSH 接続	○	○	○
	操作履歴の保存	×	○	○
ダッシュボード	追加	○	○	○

機能		Basic	Enterprise	Suite
	共有	○	○	○
	ウィジェット	○	○	○
	レポート	×	○	○
インシデント		○	○	○
ジョブ		×	○	○
コンプライアンス		×	×	○
レポート		×	○	○
MIB コンパイル		○	○	○
Zero-touch(オプション)		×	×	○

1.3 動作環境

ThirdEye は、バーチャルアプライアンスとして提供され、以下の 2 つのプラットフォームをサポートしています。

- VMWare ESXi (バージョン 7.0 以上)
- Windows Hyper-V (Windows server 2016 以降)
- Amazon Web Services ※1
- Nutanix AHV
- Linux KVM

ThirdEye を使用するには、次の環境が必要です。

項目	推奨	デフォルト	最小
ハードディスク	HDD1: 8 GB HDD2: 50 GB 以上	HDD1: 8 GB HDD2: 50 GB	HDD1: 8 GB HDD2: 50 GB
HDD プロビジョニング	シン または シック	シン または シック	シン または シック
メモリ	8 GB 以上	16 GB	8 GB
CPU	仮想 CPU 8 個(コア) 以上	仮想 CPU 16 個(コア)	仮想 CPU 4 個(コア)

その他特記事項

※ HDD プロビジョニングタイプは、シン/シックのいずれのタイプもサポートされています。

1.4 使用ポート一覧

ThirdEye が通信に使用するポートを以下に示します。ファイアウォール経由でデバイスにアクセスする必要がある場合は、ファイアウォールの通信設定を変更し、必要なポートが解放されるようにしてください。

機能	プロトコル	ポート	UDP /TCP	通信方向
Zero-Touch	DHCP	67	UDP	ThirdEye (←) 送信先
		68	UDP	ThirdEye (→) 送信先
	HTTP	80	TCP	ThirdEye (←) 送信先
	TFTP	69	UDP	ThirdEye (←) 送信先
	ICMP	-	-	ThirdEye (←) 送信先
自動ディスカバリ	SSH, Telnet	22,23	TCP	ThirdEye (→) 送信先
	SNMP	161	UDP	ThirdEye (→) 送信先
	ICMP	-	-	ThirdEye (→) 送信先
設定の送信 (コンフィギュレーション の復元)	SSH, Telnet	22,23	TCP	ThirdEye (→) 送信先
	TFTP	69	UDP	ThirdEye (←) 送信先
	FTP	20,21	TCP	ThirdEye (←) 送信先
変更ツールによる設定	SSH, Telnet	22,23	TCP	ThirdEye (→) 送信先
Trap 送信	SNMP Trap	162	UDP	ThirdEye (→) 送信先
SNMP 監視	SNMP	161	UDP	ThirdEye (→) 送信先
Trap 受信	SNMP Trap	162	UDP	ThirdEye (←) 送信先
リアルタイム変更検知	Syslog	514	UDP	ThirdEye (←) 送信先
バックアップ*	SSH, Telnet	22, 23	TCP	ThirdEye (→) 送信先
	SNMP	161	UDP	ThirdEye (→) 送信先
	TFTP	69	UDP	ThirdEye (←) 送信先
	FTP	20,21	TCP	ThirdEye (←) 送信先
ターミナルプロキシ	SSH	2222	TCP	ThirdEye (←) クライアント PC
	SSH, Telnet	22, 23	TCP	ThirdEye (→) 送信先
Web ターミナル	HTTPS	443	TCP	ThirdEye (←) クライアント (GUI)
	SSH, Telnet	22, 23	TCP	ThirdEye (→) 送信先
クライアント	HTTPS	443	TCP	ThirdEye (←) クライアント (GUI)
外部認証機能	LDAP	389	TCP	ThirdEye (→) 認証サーバ
	RADIUS	1812	UDP	ThirdEye (→) 認証サーバ

* 使用するプロトコルの適切な設定は、使うデバイスの種類によります。

例えば、IOS デバイスの場合、「CLI (Telnet, SSH)のみ、あるいは CLI と TFTP の両方」など

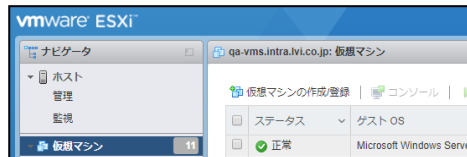
第2章 インストール

2.1 インストールする

2.1.1 VMware ESXi へのデプロイ

VMware ESXi へのデプロイ手順について説明します。ここでは ESXi 6.5 を使用した場合を例に説明します。

1. Web UI にログインし、仮想マシンから「仮想マシンの作成/登録」をクリックします。



2. 「OVF ファイルまたは OVA ファイルから仮想マシンをデプロイ」を選択し、「次へ」をクリックします。



3. 任意の仮想マシン名を入力後、OVA ファイル「lvi-core-****-appliance.ova」をドラッグ・アンド・ドロップし、「次へ」をクリックします。



4. ストレージを選択し「次へ」をクリックします。



5. デployするネットワークとディスクのプロビジョニングを選択し「次へ」をクリックします。



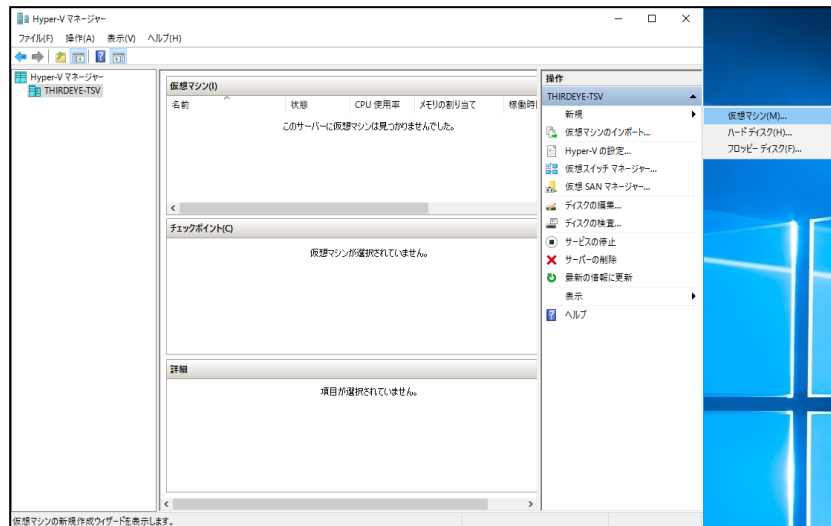
6. 「完了」をクリックします。



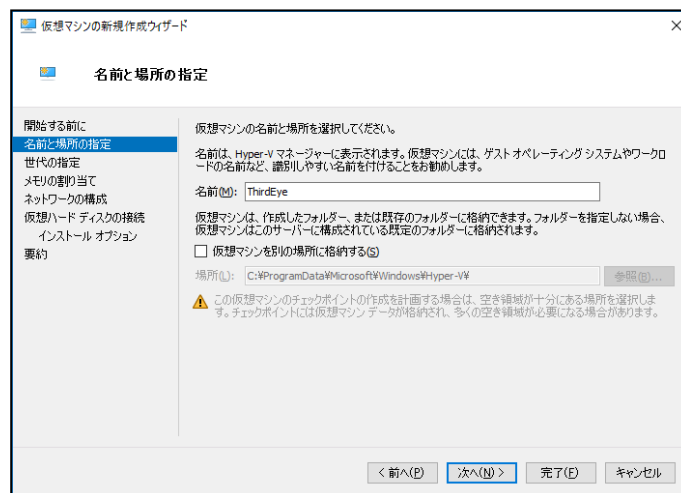
2.1.2 Windows Hyper-V へのデプロイ

Windows Hyper-V へのデプロイ手順について説明します。ここでは Windows Server 2016 を使用した場合を例に説明します。

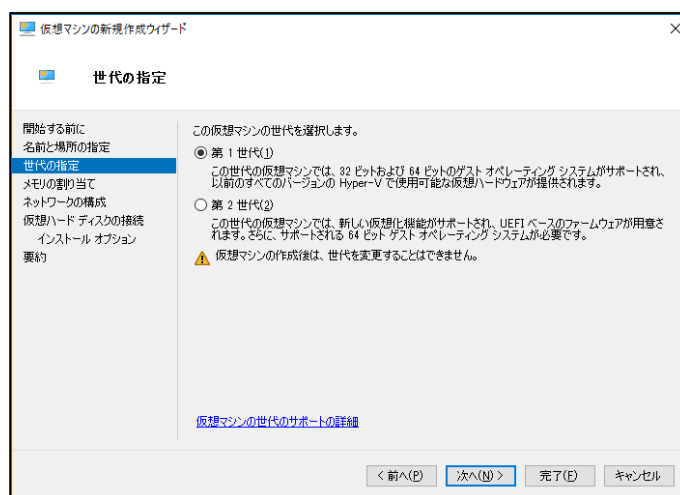
1. Hyper-V マネージャーを起動し、「新規」→「仮想マシン」をクリックします。



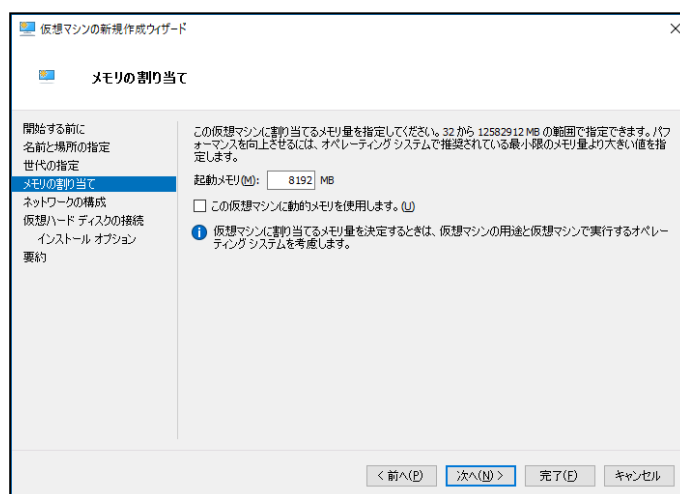
2. 仮想マシンの名前を入力し、「次へ」をクリックします。



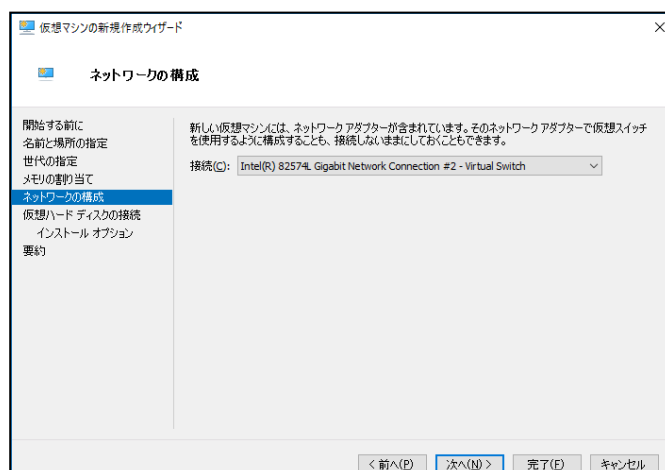
3. 「第 1 世代」を選択し、「次へ」をクリックします。



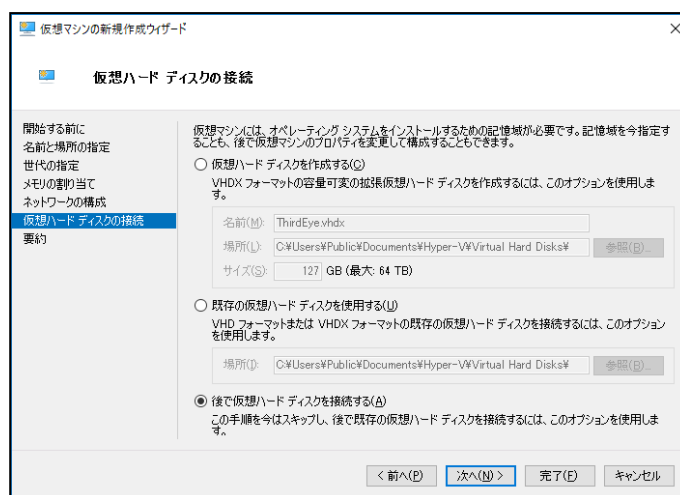
4. 起動メモリを設定し、「次へ」をクリックします。



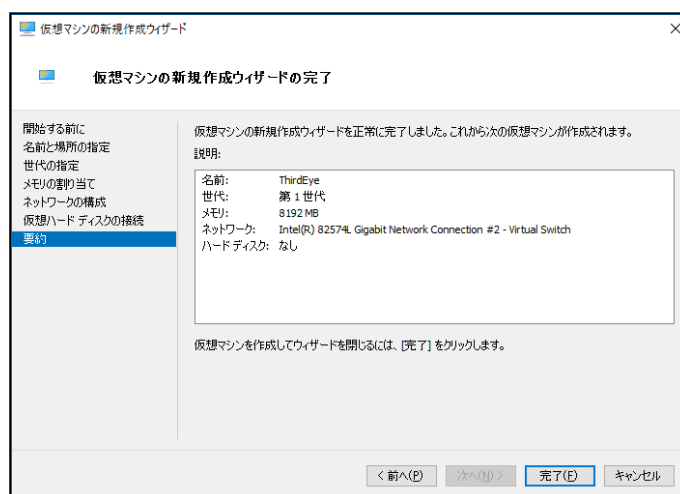
5. 接続先に使用する仮想スイッチを選択し、「次へ」をクリックします。



6. 「後で仮想ハードディスクを接続する」を選択し、「次へ」をクリックします。



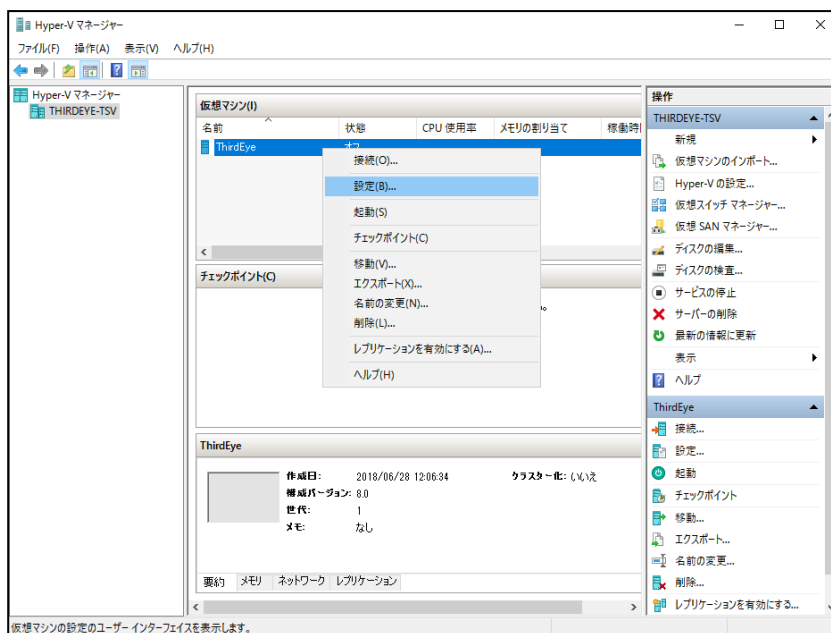
7. 「完了」をクリックします。



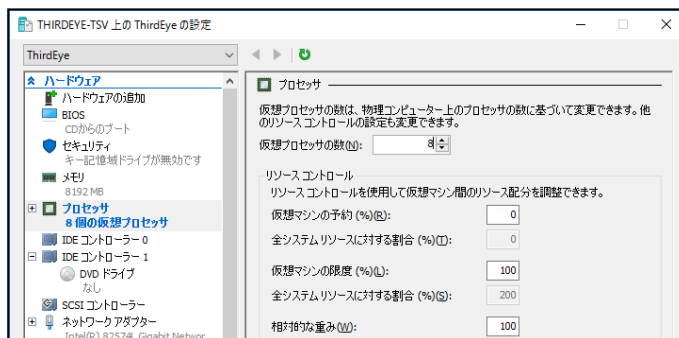
以上で仮想マシンが作成されます。

続いて、2 つの VHDX ファイルを作成した仮想マシンに割り当てます。

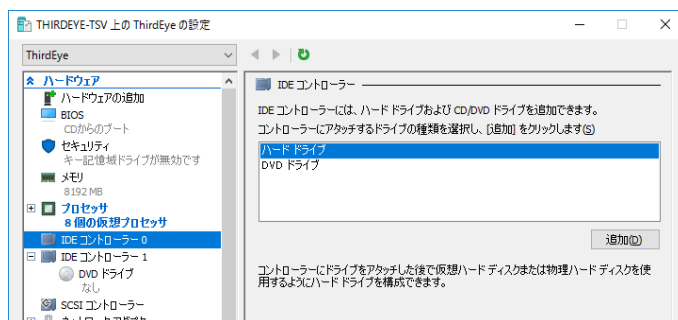
8. 作成した仮想マシンを右クリックし、「設定」をクリックします。



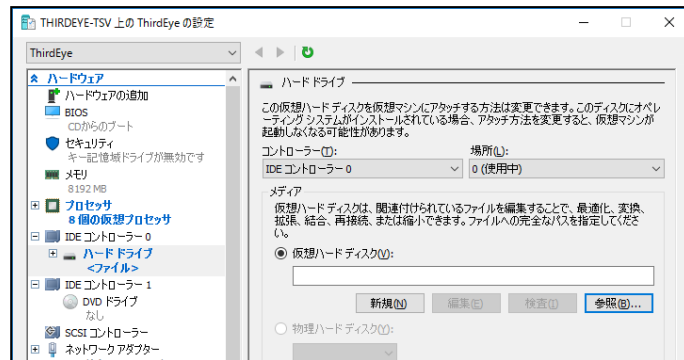
9. 「プロセッサ」を選択し、「仮想プロセッサ数」を変更します。



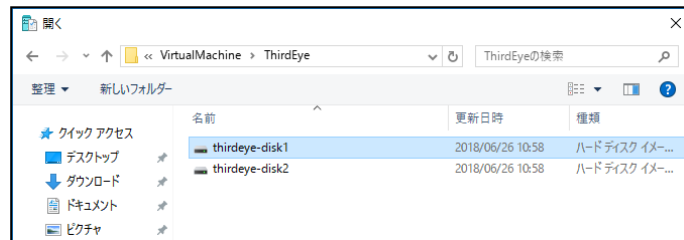
10. 「IDE コントローラー 0」を選択し、「追加」をクリックします。



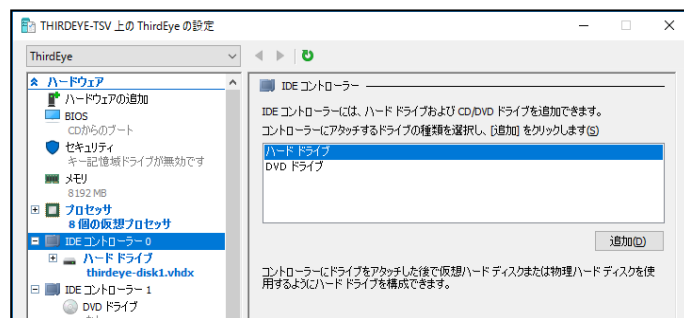
11. 「参照」をクリックします。



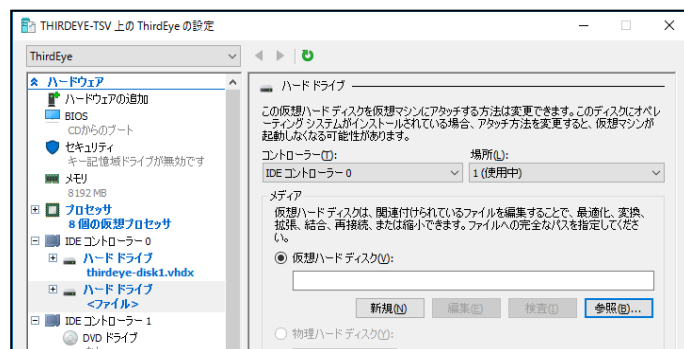
12. 「disk1」を追加し、「OK」をクリックします。



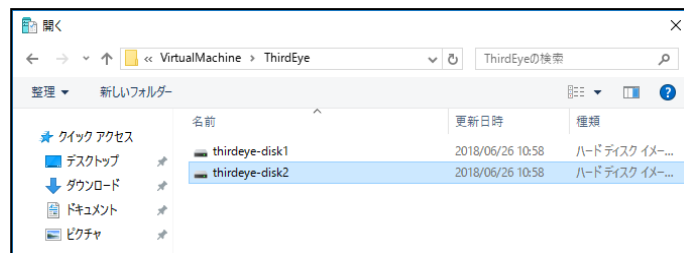
13. 再度、「IDE コントローラー 0」を選択し、「追加」をクリックします。



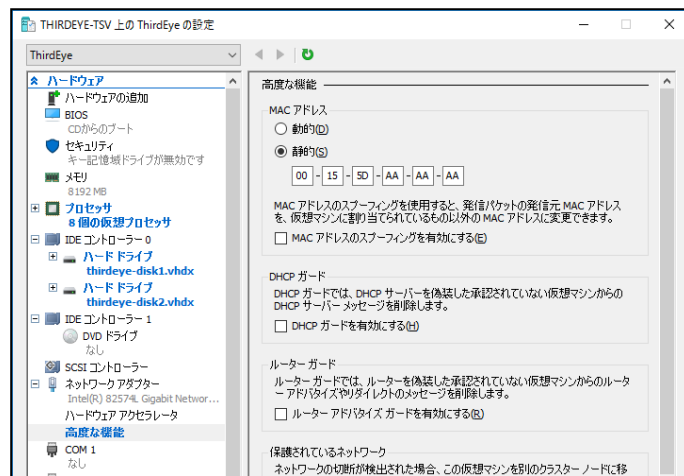
14. 「参照」をクリックします。



15. 「disk2」を追加し、「OK」をクリックします。



16. ネットワークアダプタ内の「高度な機能」をクリックし、MAC アドレスを「静的」に変更します。



補足

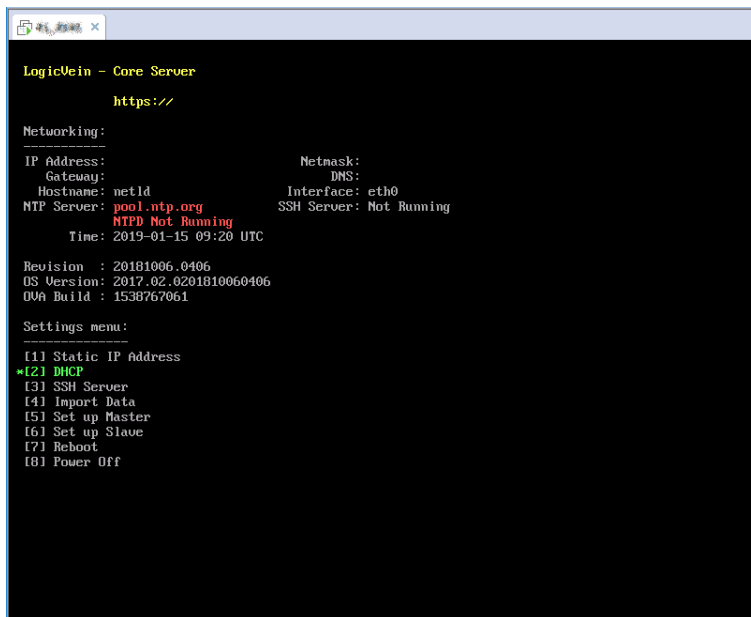
本製品のライセンスは MAC アドレスで管理されています。仮想マシンに割り当てられた MAC アドレスが変更されないように、MAC アドレスを「静的」に設定することをおすすめします。

2.2 ネットワークを設定する

ネットワーク設定では、ThirdEye に付与するホスト名や IP アドレスなどを設定します。デフォルトでは、DHCP から IP アドレス等を取得します。DHCP サーバがない環境では、以下の手順で各種設定を行います。

※ネットワーク設定は、仮想マシンコンソール上でキーボードを使って操作します。

1. キーボードの「1」キーを押し[Static IP Address]を選択します。



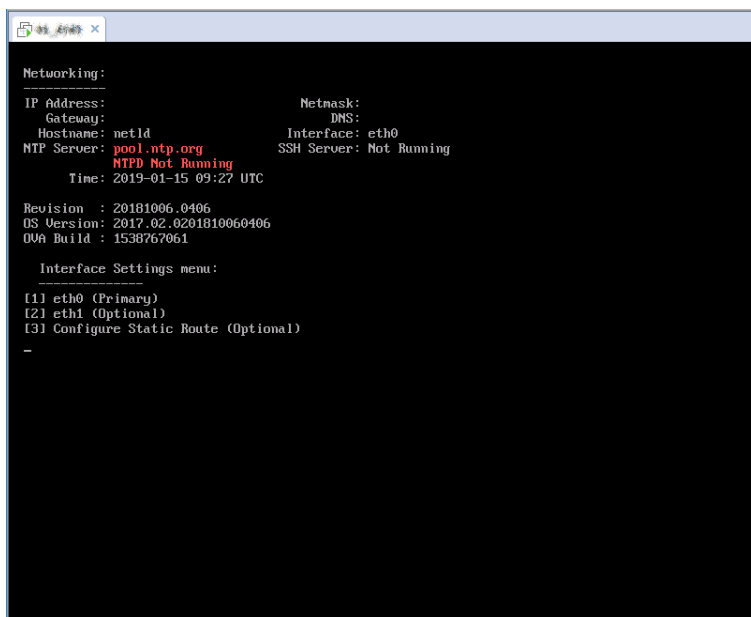
```
LogicVein - Core Server
https://

Networking:
IP Address:                               Netmask:
Gateway:                                   DNS:
Hostname: net1d                           Interface: eth0
NTP Server: pool.ntp.org                   SSH Server: Not Running
MTPD Not Running
Time: 2019-01-15 09:20 UTC

Revision : 20181006.0406
OS Version: 2017.02.0201810060406
OVA Build : 1538767061

Settings menu:
[1] Static IP Address
*[2] DHCP
[3] SSH Server
[4] Import Data
[5] Set up Master
[6] Set up Slave
[7] Reboot
[8] Power Off
```

2. キーボードの「1」キーを押し[eth0 (Primary)]を選択します。



```
Networking:
IP Address:                               Netmask:
Gateway:                                   DNS:
Hostname: net1d                           Interface: eth0
NTP Server: pool.ntp.org                   SSH Server: Not Running
MTPD Not Running
Time: 2019-01-15 09:27 UTC

Revision : 20181006.0406
OS Version: 2017.02.0201810060406
OVA Build : 1538767061

Interface Settings menu:
[1] eth0 (Primary)
[2] eth1 (Optional)
[3] Configure Static Route (Optional)
-
```

3. 以下のネットワーク設定項目が順に表示されます。キーボードで値を入力し、「Enter」キーを押して次へ進みます。

項目	説明	必須項目
Hostname	仮想アプライアンスで使用するホスト名	必須
NTP Server	仮想アプライアンスで使用する NTP サーバのアドレス (IP アドレスまたはホスト名)	必須
IP Address	仮想アプライアンスで使用する IP アドレス	必須
Netmask	上記 IP アドレスのサブネットマスク	必須
Gateway	ゲートウェイの IP アドレス	必須
DNS 1/2	DNS サーバの IP アドレス	—

注意

仮想マシンコンソールでのキーボード配列は英語配列です。

4. 確認メッセージが表示されます。キーボードの「Y」キーを押し設定を保存します。

```

Networking:
IP Address:                               Netmask:
Gateway:                                   DNS:
Hostname: netld                             Interface: eth0
NTP Server: pool.ntp.org                     SSH Server: Not Running
Time: 2019-01-15 09:25 UTC

Revision : 20181006.0406
OS Version: 2017.02.0201810060406
OVA Build : 1538767061

Interface Settings menu:
[1] eth0 (Primary)
[2] eth1 (Optional)
[3] Configure Static Route (Optional)

Enter STATIC network settings:
-----
Hostname: thirdeye
NTP Server: 192.168.0.3
IP Address: 192.168.30.41
Netmask: 255.255.255.0
Gateway: 192.168.30.254
DNS 1:
DNS 2:

Do you want to SAVE and APPLY these settings? (y/N) [default: N] _

```

設定は以上です。設定後、サービスが自動的に再起動します。

2.3 ライセンスを適用する

ライセンスを適用し、製品をアクティベートします。

1. Web ブラウザで、ThirdEye のアドレスを入力し、アクセスします。

`https://<Address>/`

※<Address>には、IP アドレスまたは FQDN(Fully Qualified Domain Name)を指定します。

2. ライセンス認証画面が表示されます。アクティベーションキー または シリアルナンバー をコピー&ペーストして入力し、[認証]をクリックします。

- インターネットに接続できない場合 :アクティベーションキー
- インターネット接続できる場合 :シリアルナンバー(25桁の英数字で構成された番号)



サービスが自動的に再起動し、ライセンス適用は完了します。

2.4 初期設定(詳細設定)

ライセンスを適用後、初回アクセス時に[詳細設定]画面が表示されます。この画面では、admin ユーザのパスワードやメールサーバを設定できます。

詳細設定

adminユーザ設定

adminユーザのメールアドレス:

adminユーザのログインパスワード:

パスワードの再入力:

ロケール設定

メール送信時の言語: 言語:

メール送信時のタイムゾーン: タイムゾーン:

サーバ設定

ブラウザタブの表示名:

メール等のリンクアドレスに使用するホスト名またはIPアドレス:

メール設定

SMTPサーバのホスト名またはIPアドレス:

メール送信時のメールアドレス:

メール送信時の差出人名:

カテゴリー	項目	必須項目
admin ユーザ設定	admin ユーザのメールアドレス	—
	admin ユーザのログインパスワード	必須
ロケール設定	メール送信時の言語	—
	メール送信時のタイムゾーン	—
サーバ設定	ブラウザタブの表示名	—
	メール等のリンクアドレスに使用するホスト名または IP アドレス	—
メール設定	SMTP サーバのホスト名または IP アドレス	—
	メール送信時のメールアドレス	—
	メール送信時の差出人名	—

注意	<p>パスワードを設定するには、以下の条件を満たしている必要があります。</p> <ul style="list-style-type: none"> • 8文字以上であること • 推測されやすい文字列(人名や固有名詞、辞書に載っている単語、よく使われるパスワード)でないこと • 同じ文字の繰り返しやわかりやすい並びの文字列でないこと
-----------	---

設定後、[保存]をクリックし、ログイン画面に進みます。

第3章 ログイン/ログアウト

ログイン/ログアウトするには、以下の手順に従ってください。

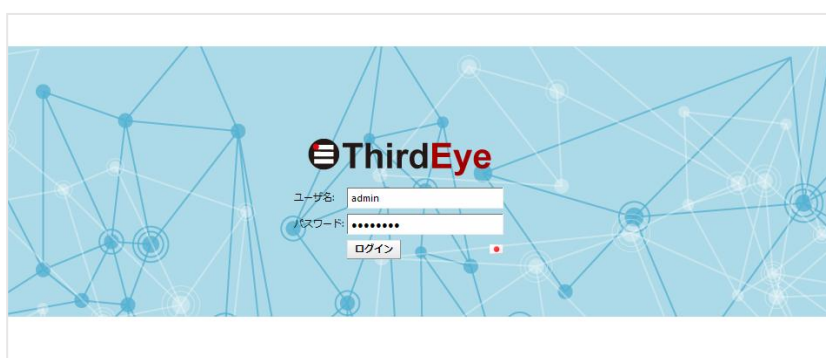
3.1 ログインする

1. Web ブラウザで、ThirdEye のアドレスを入力し、アクセスします。

https://<Address>/

※<Address>には、IP アドレスまたは FQDN(Fully Qualified Domain Name)を指定します。

2. ログイン画面で、ユーザ名・パスワードを入力し、ログインします。

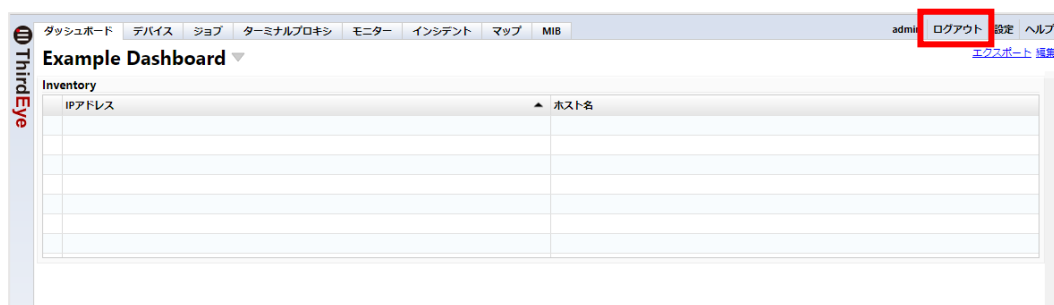


※新規インストールの場合、「[2.4 初期設定](#)」で admin ユーザのパスワードを設定しています。

ログインすると、ThirdEye のトップ画面が表示されます。

3.2 ログアウトする

1. 画面右上にある[ログアウト]をクリックします。



ログアウトすると、ThirdEye のログイン画面が表示されます。

第4章 画面構成

4.1 画面の構成と各部の役割

ThirdEye の画面構成について説明します。



No.	名称	説明
①	メインタブ	メイン画面を切り替えるタブです。
②	メイン画面	メインタブで選択したタブに対応する画面が表示されます。
③	グローバルメニュー	画面右上に固定表示されるメニューです。

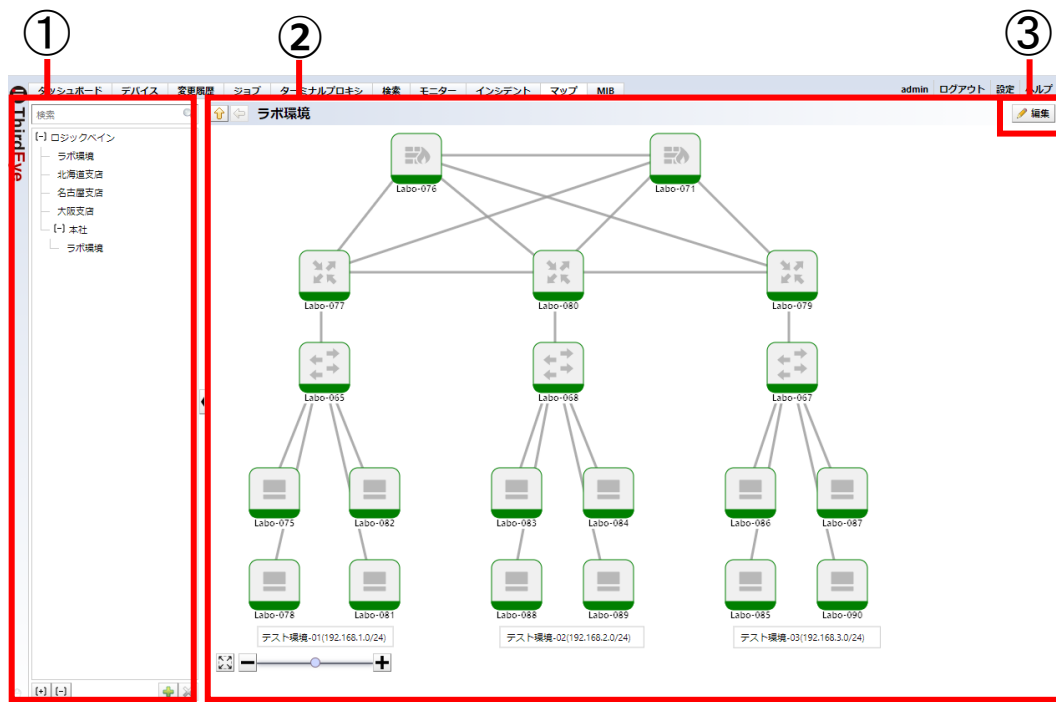
4.1.1 メインタブ構成

タブ	エディション	説明
ダッシュボード	共通	ダッシュボードを表示します。詳しくは、「5.5 ダッシュボードを作成する」を参照してください。
デバイス	共通	登録されているデバイスをインベントリ(一覧表)として表示します。
変更履歴	Enterprise Suite	コンフィギュレーションの変更履歴を表示します。
ジョブ	Enterprise Suite	ジョブの一覧を表示します。
ターミナルプロキシ	Enterprise Suite	デバイスにターミナルで接続したときの記録の一覧を表示します。
検索	Enterprise Suite	スイッチポート検索と ARP 検索、インタフェース検索を行うことができます。
コンプライアンス	Suite	デバイスのコンフィグに
モニター	共通	監視設定を行います。
インシデント	共通	インシデントの一覧を表示します。
マップ	共通	マップを表示します。マップでは、マップの作成、編集、削除を行うことができます。
MIB	共通	MIB の検索、閲覧を行います。

4.1.2 グローバルメニュー構成

項目	説明
ユーザ名	現在のログインユーザ名が表示されます。
ログアウト	ThirdEye からログアウトします。
設定	各種設定（[サーバ設定]）画面が表示されます。
ヘルプ	ヘルプメニューが表示されます。

4.1.3 マップ画面構成



No.	名称	説明
①	マップツリー	マップをツリー形式で表示します。
②	マップ	選択されたマップを表示します。
③	編集	マップの編集モードに移行します。

第5章 基本設定

ここでは、ThirdEye で監視を行うための基本的な設定について説明します。

5.1 クレデンシャルを設定する

監視対象機器から SNMP を使用して監視する場合、または、コンフィギュレーションを取得する場合は、監視対象機器に設定されているクレデンシャル(SNMP コミュニティやユーザ名、パスワード)を ThirdEye に設定する必要があります。クレデンシャルは、デバイスタブの[インベントリ]→[クレデンシャル]で設定します。

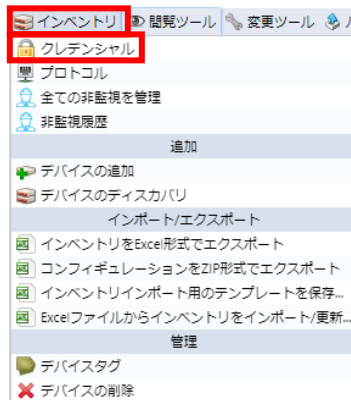
クレデンシャルの設定方法は、「ダイナミック」と「スタティック」の 2 通りあります。


項目	説明
ダイナミック	アドレス範囲に対し、共通のクレデンシャルを設定します。 監視対象機器に共通のクレデンシャルを設定している場合に使用すると便利です。 ※1つのネットワークグループに、最大3つまでクレデンシャルを登録できます。
スタティック	IP アドレス単位で、クレデンシャルを設定します。 監視対象機器ごとに異なるクレデンシャルを設定している場合に使用します。

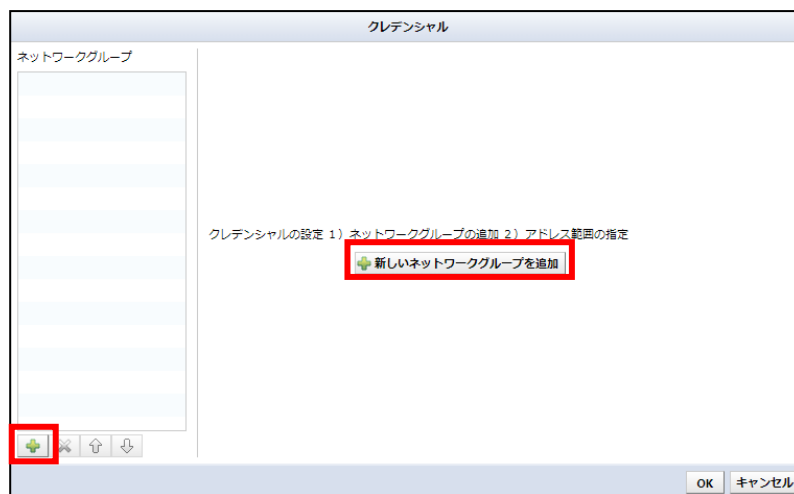
5.1.1 共通のクレデンシャルを設定する

監視対象機器に共通のクレデンシャルを設定している場合は、「ダイナミック」を使用して設定します。

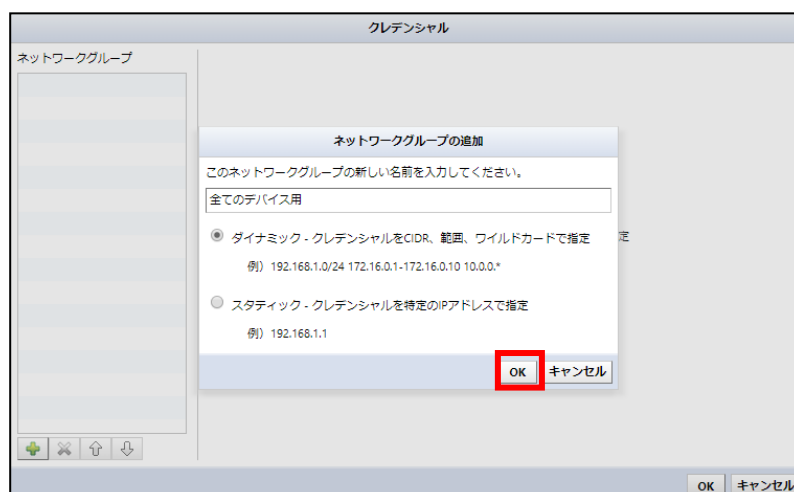
1. [デバイス]タブを選択し、[インベントリ]→[クレデンシャル]の順にクリックします。




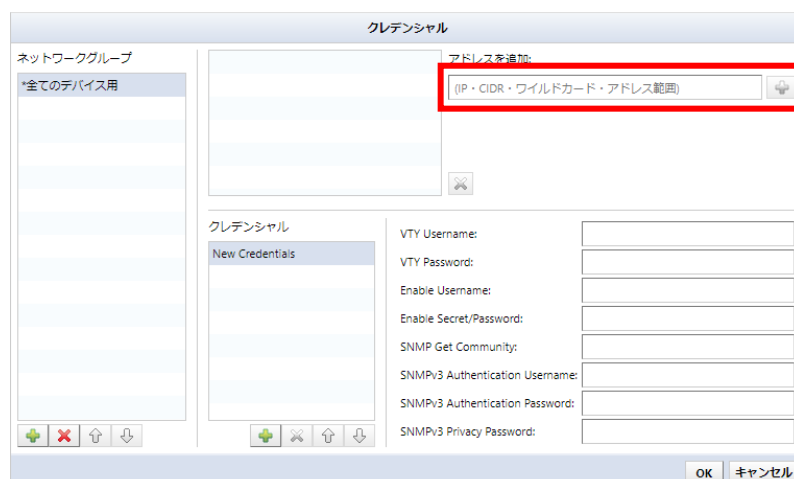
2. [ (追加)] または [新しいネットワークグループを追加] をクリックします。



3. ネットワークグループ名を入力し、[ダイナミック]を選択して[OK]をクリックします。



4. [アドレスを追加]欄にネットワークグループのアドレス範囲を入力し、[ (追加)] をクリックします。



5. 各項目を設定します。

項目	説明
VTY Username /VTY Password	ネットワーク機器にログインする際に必要なユーザ名/パスワードを入力します。
Enable Username /Enable Secret/Password	イネーブルモードに入る為のユーザ名/パスワードを入力します。
SNMP Get Community	SNMP Get リクエスト時に使用する SNMP コミュニティ入力します
SNMPv3 Authentication Username	SNMPv3 で定義された、認証ユーザ名を入力します
SNMPv3 Authentication Password	SNMPv3 で定義された、コミュニティに対するパスワード入力します
SNMPv3 Privacy Password	SNMP による通信の際、暗号化に用いられるパスワード入力します

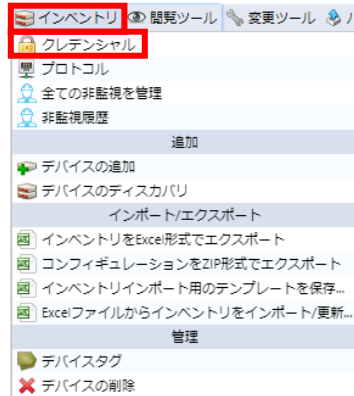
※必要のない項目は、入力を省略することが可能です。


6. [OK]をクリックし、設定を保存します。

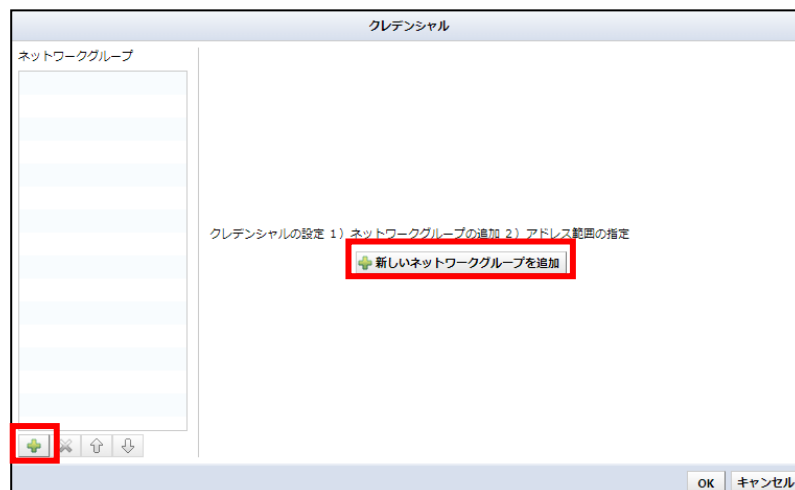
5.1.2 機器ごとにクレデンシャルを設定する

監視対象機器ごとに異なるクレデンシャルを設定している場合は、「スタティック」を使用して設定します。

1. [デバイス]タブを選択し、[インベントリ]→[クレデンシャル]の順にクリックします。




2. [ (追加)]または[新しいネットワークグループを追加]をクリックします。



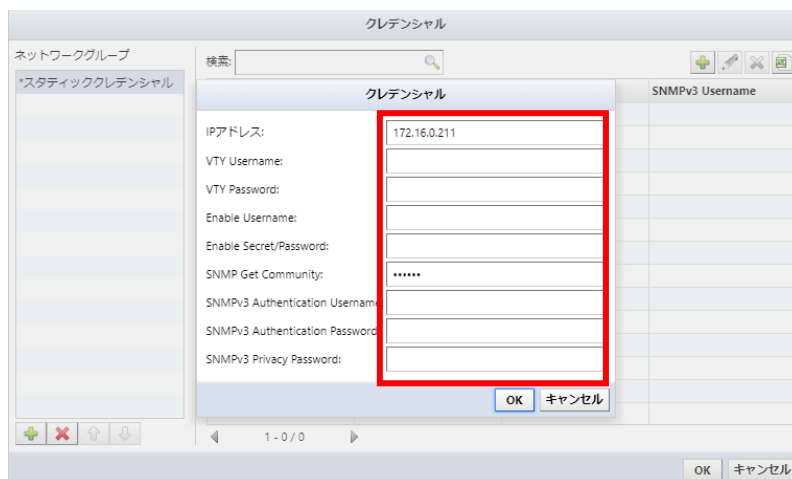
3. ネットワークグループ名を入力し、[スタティック]を選択して[OK]をクリックします。



4. [ (追加)]をクリックします。



5. IP アドレスを入力し、各項目を設定します。



項目	説明
IP アドレス	ネットワーク機器の IP アドレスを入力します。
VTY Username /VTY Password	ネットワーク機器にログインする際に必要なユーザ名/パスワードを入力します。
Enable Username /Enable Secret/Password	イネーブルモードに入る為のユーザ名/パスワードを入力します。
SNMP Get Community	SNMP Get Request を実行する際に使用する SNMP コミュニティを入力します。
SNMPv3 Authentication Username	SNMPv3 で定義されている認証ユーザ名を入力します。
SNMPv3 Authentication Password	SNMPv3 で定義されているコミュニティのパスワードを入力します。
SNMPv3 Privacy Password	SNMP で通信する際、暗号化に使用するパスワードを入力します。

※必要のない項目は、入力を省略することが可能です。

6. [OK]をクリックします。

7. [OK]をクリックし、設定を保存します。

IPアドレス	VTY Username	Enable Username	SNMPv3 Username
172.16.0.211			

5.2 デバイスを追加する

ThirdEye にデバイスを追加する場合、次のいずれかの方法を使用します。

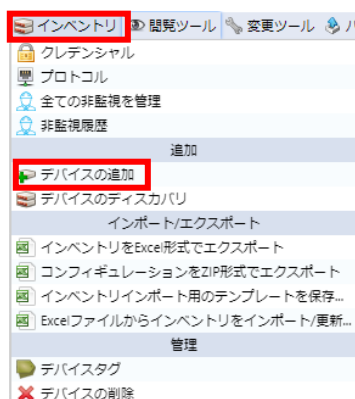
項目	説明
手動	デバイスの IP アドレスを直接入力し、デバイスを追加します。追加は 1 台ずつ行います。
ディスカバリ	指定された IP アドレスの範囲内にあるデバイスを自動的に検出し、追加します。
インポート	デバイスデータを XLSX ファイルから読み込む機能です。インポート用のテンプレートファイルをエクスポートし、そのファイルに監視対象機器の情報を記入します。

注意

デバイス追加時に、デバイスはマップに表示されません。デバイスをマップ上にオブジェクトとして表示する場合は、デバイスをマップに追加してください。マップへの追加方法は「[5.4.2 マップにデバイスを挿入する](#)」を参照してください。

5.2.1 1 台ずつ登録する

1. [デバイス]タブを選択し、[インベントリ]→[デバイスの追加]の順にクリックします。



2. 追加するデバイスの IP アドレスを入力し、[OK]をクリックします。

デバイスの追加

IPアドレス:

アダプタを識別できないSSHホストにLinuxアダプタを割り当てる

項目	説明
アダプタを識別できない SSH ホストに Linux アダプタを割り当てる	コンフィグバックアップのためのアダプタを認識できない場合に、Linux アダプタを割り当てます。

ThirdEye が監視対象機器から情報収集を完了すると、追加されたデバイスがデバイス一覧に追加されます。

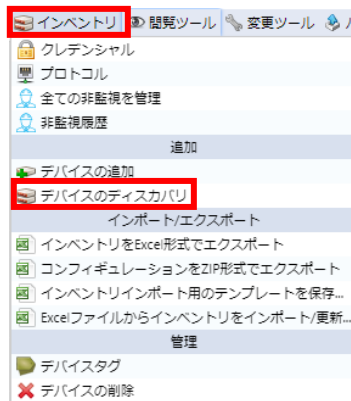


IPアドレス	ホスト名	ハードベンダー	モデル	デバイスタイプ	シリアル番号	トレイト
172.16.0.211	ISR4321.intra.lvi.co.jp-1	Cisco	ciscoISR4321			http icmp ncm

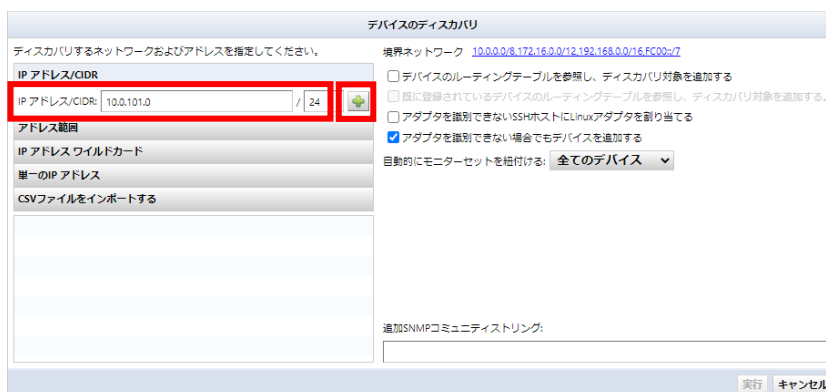
※対象の IP アドレスと通信できない場合でもデバイスは追加されますが、ホスト名やインタフェース情報は取得できません。

5.2.2 ネットワーク上のデバイスを登録する

1. [デバイス]タブを選択し、[インVENTORY]→[デバイスのディスカバリ]の順にクリックします。



2. ディスカバリする IP アドレス範囲を指定し、[+] (追加) をクリックします。



デバイスのディスカバリ

ディスカバリするネットワークおよびアドレスを指定してください。

境界ネットワーク 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, FC02::7

IP アドレス/CIDR

IP アドレス/CIDR: 10.0.101.0 / 24 [+]

アドレス範囲

IP アドレス ワイルドカード

単一の IP アドレス

CSV ファイルをインポートする

デバイスのルーティングテーブルを参照し、ディスカバリ対象を追加する

既に登録されているデバイスのルーティングテーブルを参照し、ディスカバリ対象を追加する。

アダプタを識別できない SSH ホストに Linux アダプタを割り当てる

アダプタを識別できない場合でもデバイスを追加する

自動的にモニターセットを相付ける: 全てのデバイス

追加SNMPコミュニティストリング:

実行 キャンセル

項目	説明
デバイスのルーティングテーブルを参照し、ディスカバリ対象を追加する	発見されたデバイスのルーティングテーブルを参照してディスカバリ対象ネットワークを追加します。
既に登録されているデバイスのルーティングテーブルを参照し、ディスカバリ対象を追加する。	既に登録されているデバイスがある場合、登録されているデバイスのルーティングテーブルを参照してディスカバリ対象ネットワークを追加します。
アダプタを識別できない SSH ホストに Linux アダプタを割り当てる	コンフィグバックアップのためのアダプタを認識できない場合に、Linux アダプタを割り当てます。
アダプタを識別できない場合でもデバイスを追加する	アダプタを認識できない場合でも、デバイスを追加します。
自動的にモニターセットを紐付ける	発見したデバイスに対して、選択したモニターセットを割り当てます。

3. 画面左下に入力情報が追加されます。[実行]をクリックします。

デバイスのディスカバリ

ディスカバリするネットワークおよびアドレスを指定してください。

境界ネットワーク 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16,FC00::/7

IP アドレス/CIDR

IP アドレス/CIDR: /

アドレス範囲

IP アドレス ワイルドカード

単一の IP アドレス

CSV ファイルをインポートする

10.0.101.0/24

追加SNMPコミュニティストリング:

デバイスのルーティングテーブルを参照し、ディスカバリ対象を追加する

既に登録されているデバイスのルーティングテーブルを参照し、ディスカバリ対象を追加する。

アダプタを識別できない SSH ホストに Linux アダプタを割り当てる

アダプタを識別できない場合でもデバイスを追加する

自動的にモニターセットを紐付ける: 全てのデバイス

実行 キャンセル

4. ディスカバリが開始され、画面下にディスカバリの結果が表示されます。

ThirdEye

ダッシュボード デバイス ジョブ ターミナルプロキシ モニター インシデント マップ MIB admin ログアウト 設定 ヘルプ

IP/ホスト名検索: 詳細検索

IPアドレス	ホスト名	トレイト
10.0.101.1	LVIGW-c3650.intra.lvi.co.jp-1	icmp snmp
10.0.101.2	LVIGW-c3650.intra.lvi.co.jp-2	icmp snmp
10.0.101.3	LVIGW-c3650.intra.lvi.co.jp-3	icmp snmp
10.0.101.4	LVIGW-c3650.intra.lvi.co.jp-4	icmp snmp
10.0.101.5	LVIGW-c3650.intra.lvi.co.jp-5	icmp snmp
10.0.101.6	LVIGW-c3650.intra.lvi.co.jp-6	icmp snmp
10.0.101.7	LVIGW-c3650.intra.lvi.co.jp-7	icmp snmp
10.0.101.8	LVIGW-c3650.intra.lvi.co.jp-8	icmp snmp
10.0.101.9	LVIGW-c3650.intra.lvi.co.jp-9	icmp snmp
10.0.101.10	LVIGW-c3650.intra.lvi.co.jp-10	icmp snmp

1 - 254 / 254

1ページあたりの表示件数: 254

インタラクティブ ディスカバリ (2019/09/03 17:55)

ステータスサマリ

- 254 アドレスをスキャンしました
- 254 ノードが発見されました

再ディスカバリオプション

- ワーニングが発生したアドレス
- 未検出のアドレス
- 全てのアドレス

実行

ステータス	IPアドレス	ホスト名	トレイト
成功	10.0.101.151	LVIGW-c3650.intra.lvi.co.jp-151	icmp snmp
成功	Cisco IOS		
成功	10.0.101.169	LVIGW-c3650.intra.lvi.co.jp-169	icmp snmp
成功	Cisco IOS		
成功	10.0.101.248	LVIGW-c3650.intra.lvi.co.jp-248	icmp snmp
成功	Cisco IOS		
成功	10.0.101.158	LVIGW-c3650.intra.lvi.co.jp-158	icmp snmp
成功	Cisco IOS		
成功	10.0.101.165	LVIGW-c3650.intra.lvi.co.jp-165	icmp snmp
成功	Cisco IOS		
成功	10.0.101.75	LVIGW-c3650.intra.lvi.co.jp-75	icmp snmp
成功	Cisco IOS		

ディスカバリが完了すると、発見されたデバイスが自動的に ThirdEye に追加されます。

ディスカバリには「境界ネットワーク」という設定があり、ディスカバリの対象範囲を「境界ネットワーク」に指定された範囲に制限することができます。「境界ネットワーク」には、デフォルトでいくつかの範囲が指定されていますので、必要に応じて「境界ネットワーク」を編集してください。

デバイスのディスカバリ

ディスカバリするネットワークおよびアドレスを指定してください。

境界ネットワーク 10.0.0.0/8,172.16.0.0/12,192.168.0.0/16,FC00::/7

IPアドレス/CIDR デバイスのルーティングテーブルを参照し、ディスカバリ対象を追加する

デバイスのディスカバリ

ディスカバリするネットワークおよびアドレスを指定

IPアドレス/CIDR

IPアドレス/CIDR:

アドレス範囲

IPアドレス ワイルドカード

単一のIP アドレス

CSVファイルをインポートする

ディスカバリの境界ネットワークを編集

次の境界ネットワークを利用してディスカバリを実行します。ディスカバリはこれらのネットワークに含まれるアドレスに対して実行されます。

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16
- FC00::/7

IPアドレス/CIDR: /

OK キャンセル

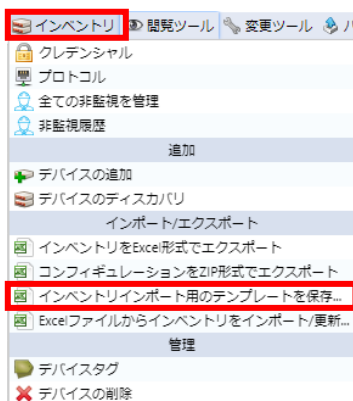
実行 キャンセル

補足

5.2.3 Excel ファイルからインポート登録する

監視対象機器の情報を Excel ファイルからインポートすることができます。インポート用のテンプレートが用意されているので、事前にテンプレートファイルをエクスポートし、そのファイルに監視対象機器の情報を記入してインポートしてください。

1. [デバイス]タブを選択し、[インベントリ]→[インベントリインポート用のテンプレートを保存]をクリックします。



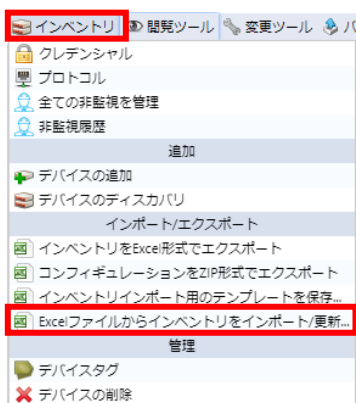
2. ファイルを開く画面が表示されます。「ファイルを保存する」を選択し、[OK]をクリックします。
※ファイル名は「ThirdEye-inventory-template.xlsx」となり、XLSX ファイル形式で保存されます。

3. 保存したファイルを編集し、以下の項目に情報を入力し、上書き保存します。

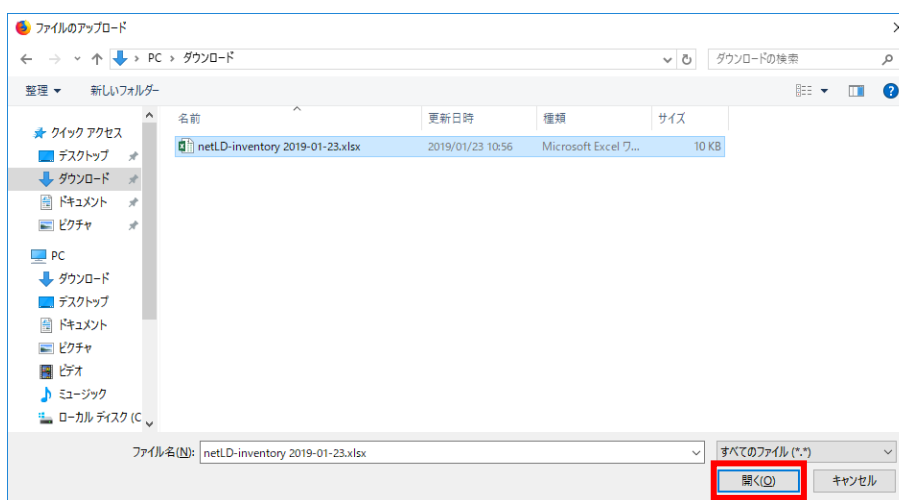
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	IP Address	Network	Adapter ID	Hostname	Type	Vendor	Model	OS Version	Serial Number	Memo	End Of Sale	End Of Life	Custom 1	Custom 2	Custom 3	Custom 4	Custom 5
2	172.16.0.1	Default		Demo-01													
3	172.16.0.2	Default		Demo-02													
4	172.16.0.3	Default		Demo-03													
5	172.16.0.4	Default		Demo-04													
6	172.16.0.5	Default		Demo-05													
7	172.16.0.6	Default		Demo-06													
8	172.16.0.7	Default		Demo-07													
9	172.16.0.8	Default		Demo-08													
10	172.16.0.9	Default		Demo-09													
11	172.16.0.10	Default		Demo-10													
12																	

項目	説明	必須項目	入力例
IP Address	デバイスの IP アドレスを入力します。	必須	192.168.1.10
Network	機器を追加したいネットワーク名を選択します。	必須	Default
Adapter ID	デバイスのアダプタを選択します。 ※現在のバージョンでは、この項目を指定する必要はありません。	—	Cisco IOS
Hostname	デバイスのホスト名を入力します。	—	
End Of Sale	販売終了日を「yyyy/mm/dd」の形式で入力します。	—	2022/1/1
End Of Life	サポート終了日を「yyyy/mm/dd」の形式で入力します。	—	2022/12/31
Custom 1～5	「カスタムデバイスフィールド」の情報を入力します。	—	

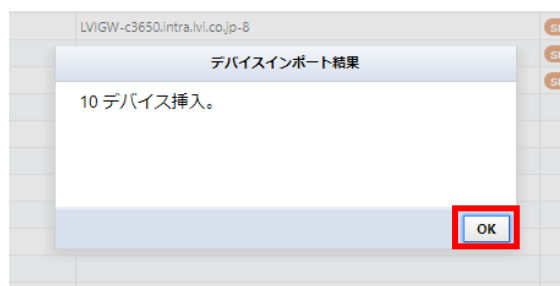
4. [インベントリ]→[Excel ファイルからインベントリをインポート/更新]の順にクリックします。



5. ファイル選択ダイアログが表示されます。編集したファイルを選択し、[開く]をクリックします。



6. 確認メッセージが表示されます。[OK]をクリックします。



5.3 監視設定をする

SNMPを使用した情報収集や ICMP Ping を使用した監視など、監視対象機器を監視する方法はいくつかあります。ここでは、基本的な監視設定の流れを記載しています。

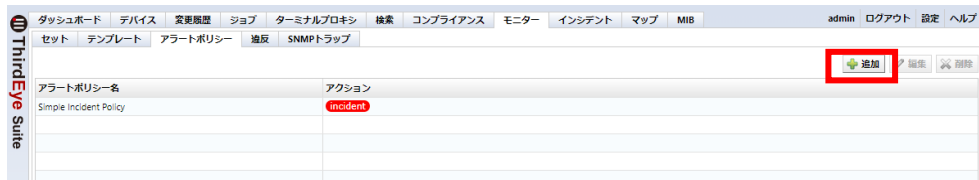
監視を始めるまでの流れは、以下のとおりです。

- ① アクションの設定(アラートポリシー機能)
- ② 監視項目の設定(モニター機能)
- ③ しきい値などトリガー設定(トリガー機能)

5.3.1 異常を検知した時のアクションを設定する

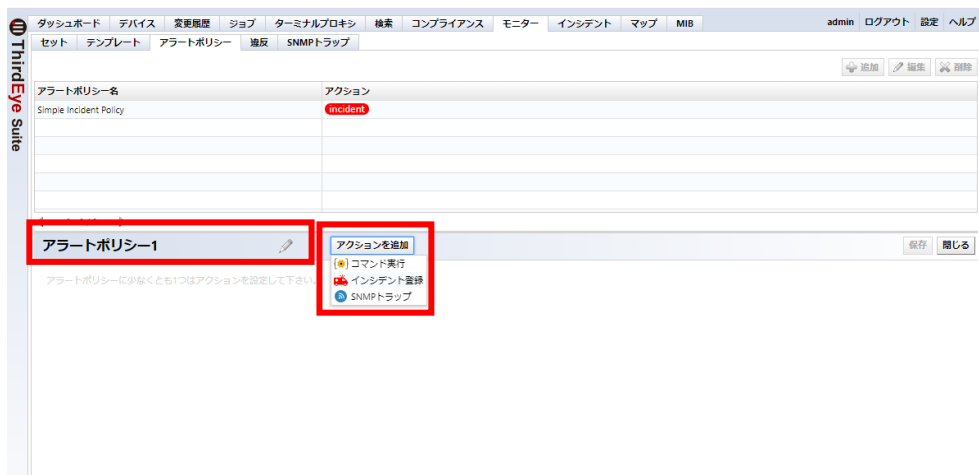
異常を検知した場合のアクションには、インシデント登録/メール送信、プログラム実行、SNMPトラップの3つの方法があります。アクション設定は、[モニター]タブ配下の[アラートポリシー]タブで設定します。以下に新しいアラートポリシーを作成する手順を記載します。

1. [モニター]→[アラートポリシー]を選択し、[追加]をクリックします。



2. アラートポリシー名を入力します。[アクションを追加]をクリックし、アクションを選択します。

※アクションは、複数追加することができます。



【アクション内容】

項目	使用可能エディション	説明
コマンド実行	共通	障害検知時にリモートホスト上でコマンドを実行します。
インシデント登録	共通	障害検知時にインシデント登録とメール送信を実行します。
SNMPトラップ	共通	障害検知時に SNMPトラップを送信します。
ジョブ実行	Suite	登録されているジョブを実行します。

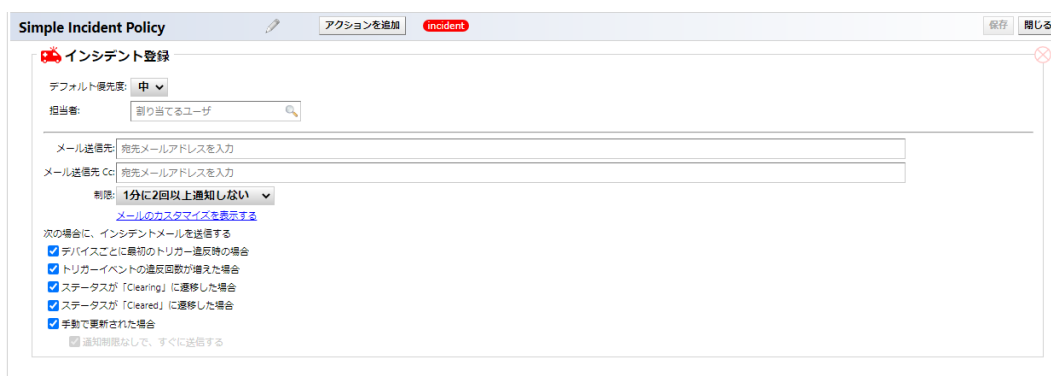
3. [保存]をクリックし、[閉じる]をクリックします。



以上でアラートポリシーの設定は完了です。以下に、それぞれのアクションについて説明します。

(1) インシデント登録

インシデント登録では、障害発生時にインシデントを作成します。また、Eメール送信先/Ccにメールアドレスを入力することで、メールを送信することが可能です。



項目	説明
デフォルト優先度	インシデント登録時の優先度を指定します。
担当者	インシデントの担当者を指定します。 ※メールアドレスを登録したユーザアカウントが担当者に指定されている場合、インシデントが更新されると、そのユーザアカウントのメールアドレスに更新が通知されます。
メール送信先	インシデントのメール送信先を設定します。 ※未入力の場合は、メールを送信しません。
メール送信先 Cc	CCのメール送信先を設定します。 ※未入力の場合は、メールを送信しません。
制限	メールで通知するタイミングを指定します。(初期値:1分以内2回以上通知しない)
メールのカスタマイズを表示する	件名、前文、末文をカスタマイズできます。
デバイスごとの最初のトリガー違反時の場合	デバイス単位で、初回違反時にメールを送信します。
トリガーイベントの違反回数が増えた場合	違反回数が増加した場合にメールを送信します。
ステータスが「Clearing」に遷移した場合	ステータスが自動的に「Clearing」に遷移した場合にメールを送信します。
ステータスが「Cleared」に遷移した場合	ステータスが自動的に「Cleared」に遷移した場合にメールを送信します。
手動で更新された場合	インシデントが手動で更新された場合にメールを送信します。

項目	説明
通知制限なしで、すぐに送信する	インシデントが手動で更新された場合、上記「制限」の設定に関わらず、すぐにメールを送信します。

※メール送信をするには、あらかじめメールサーバを設定する必要があります。メールサーバの設定については、「7.13 メールサーバを設定する」を参照してください。

(2) SNMPトラップ

障害発生時に、他の NMS や警報装置等にトラップを送信することができます。

項目	説明
トラップ送信先	障害発生時に送信される SNMP トラップの送信先を指定します。
トラップコミュニティ名	送信される SNMP トラップのコミュニティ名を指定します。
デバイスごとの最初のトリガー違反時にのみ実行	デバイス単位で、初回違反時に SNMP トラップを送信します。
トリガーイベントの違反回数が増えた場合	違反回数が増加した場合に SNMP トラップを送信します。
ステータスが「Clearing」に遷移した場合	ステータスが自動的に「Clearing」に遷移した場合に SNMP トラップを送信します。
ステータスが「Cleared」に遷移した場合	ステータスが自動的に「Cleared」に遷移した場合に SNMP トラップを送信します。

ThirdEye から送信されるトラップは以下のとおりです。

項目	説明	
トラップ名	triggerViolation	
トラップ OID	1.3.6.1.4.1.45654.2.1.1	
トラップに含まれる変数	thirdEyeDeviceUuid	障害が発生した機器の UUID (ThirdEye 内部で使用)
	thirdEyeDeviceIpAddress	障害が発生した機器の IP アドレス
	thirdEyeManagedNetwork	障害が発生した機器が所属する管理ネットワーク (ThirdEye で使用)
	thirdEyeDeviceHostname	障害が発生した機器のホスト名
	thirdEyeMessage	インシデントのメッセージ
	thirdEyeMeasurement	監視内容
	thirdEyeSeverity	インシデントの重大度
	thirdEyeDeviceCustom1	障害が発生した機器のカスタム 1 の内容
	thirdEyeDeviceCustom2	障害が発生した機器のカスタム 2 の内容
	thirdEyeDeviceCustom3	障害が発生した機器のカスタム 3 の内容
	thirdEyeDeviceCustom4	障害が発生した機器のカスタム 4 の内容
	thirdEyeDeviceCustom5	障害が発生した機器のカスタム 5 の内容
	thirdEyeClearStatus	違反のステータス (not_cleared/clearing/cleared)
	thirdEyeOccurrenceCount	違反カウント
thirdEyeFirstViolation	最初の違反 (True/False)	
thirdEyeSeverityEnum	インシデントの重大度の番号	

(3) コマンド実行

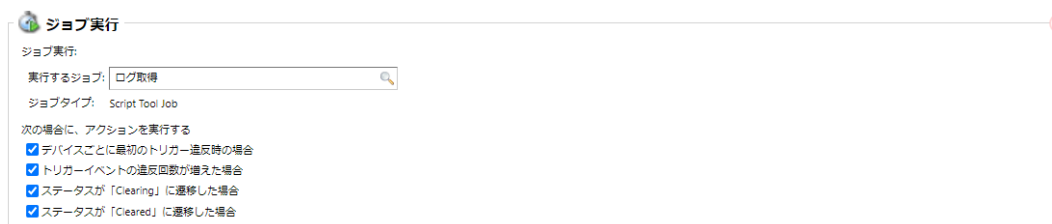
リモートホストからプログラムを実行できます。指定したリモートホストに SSH ログインし、リモートホストから指定したコマンドを実行します。



項目	説明
リモート SSH ホスト	コマンドを実行するリモートホスト(外部サーバ)を指定します。
ポート	SSH 接続に使用するポート番号。
ユーザ名	リモートホストへのログインに使用されるユーザ。
パスワード	リモートホストへのログインに使用されるユーザのパスワード。
コマンド	リモートホストで実行するコマンド。
デバイスごとの最初のトリガー違反時のみ実行	デバイス単位で、初回違反時にコマンドを実行します。
トリガーイベントの違反回数が増えた場合	違反回数が増加した場合にコマンドを実行します。
ステータスが「Clearing」に遷移した場合	ステータスが自動的に「Clearing」に遷移した場合にコマンドを実行します。
ステータスが「Cleared」に遷移した場合	ステータスが自動的に「Cleared」に遷移した場合にコマンドを実行します。

(4) ジョブ実行 Suite

リモートホストからプログラムを実行できます。指定したリモートホストに SSH ログインし、リモートホストから指定したコマンドを実行します。



項目	説明
実行するジョブ	実行するジョブのジョブ名を入力します。
デバイスごとの最初のトリガー違反時のみ実行	デバイス単位で、初回違反時にコマンドを実行します。
トリガーイベントの違反回数が増えた場合	違反回数が増加した場合にコマンドを実行します。
ステータスが「Clearing」に遷移した場合	ステータスが自動的に「Clearing」に遷移した場合にコマンドを実行します。
ステータスが「Cleared」に遷移した場合	ステータスが自動的に「Cleared」に遷移した場合にコマンドを実行します。

5.3.2 Ping 監視を設定する

Ping 監視を行うには、ICMP モニターを追加します。

ThirdEye の初期設定では、モニターセット「Default」が自動的に適用される設定が有効になっています。そのため、手動またはディスカバリで追加された監視対象機器には、「ICMP Ping (Default)」というモニターが自動的に割り当てられ、追加直後から Ping 監視が始まります。

ここでは、以下の条件のモニターを監視対象機器に追加する手順を記載します。

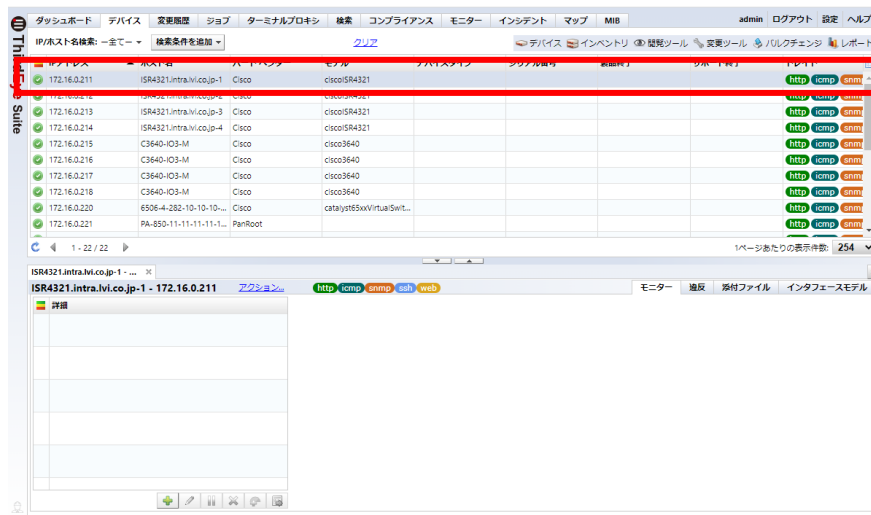
【条件】


監視間隔: 5 分

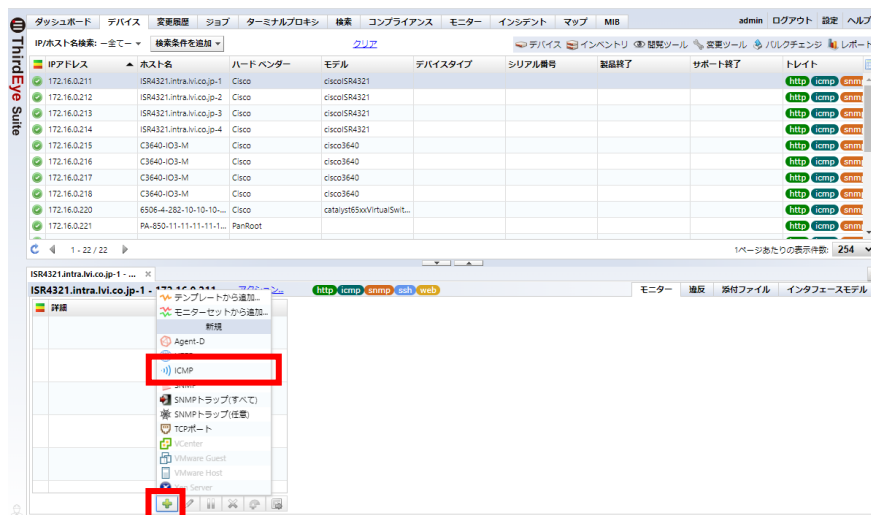
アラート条件: 10 分間に 2 回、応答が無い場合

※ThirdEye の ICMP ポーリングの詳細は「[12.1 ICMP ポーリングについて](#)」を参照してください。

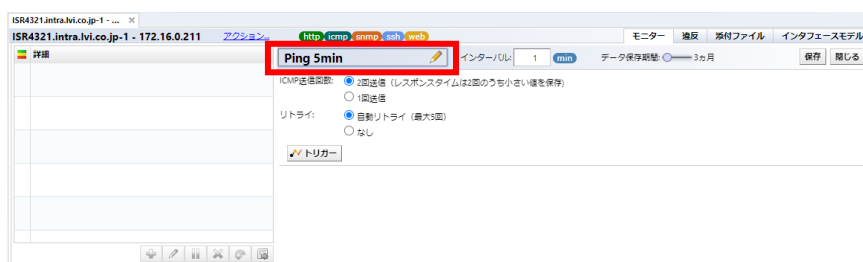
1. [デバイス]タブの監視対象機器一覧から、モニターを設定する機器をダブルクリックします。



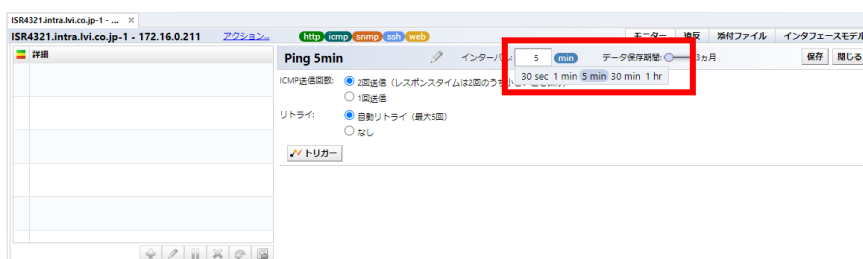
2. 左下の[ (追加)]をクリックし、「ICMP」をクリックします。



3. 任意のモニター名を入力します。



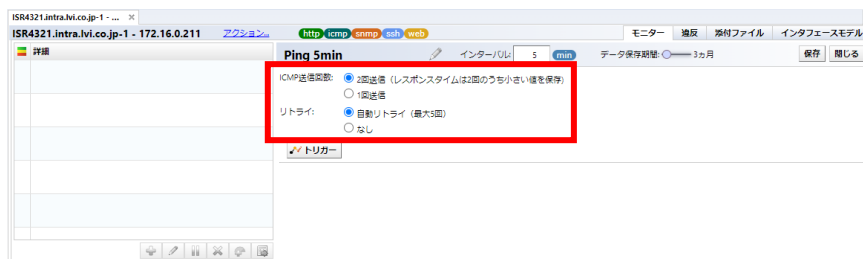
4. インターバルを指定します。



5. データ保存期間を「3ヵ月/6ヵ月/12ヵ月」から指定します。



6. ICMP 送信回数とリトライを選択します。



7. [トリガー]をクリックし、[レスポンス確認]をクリックします。



8. 以下の項目を入力します。



項目	説明
期間	処理を実行するための期間を設定します。(最小値:1分) 定められた期間内に何回失敗(カウント)したらポリシーに定義された処理を実行するのか、カウントの基準となる期間。
カウント	設定期間内に何回失敗したら処理を実行するかを設定します。(最小値:1)
アラートポリシー	アラートポリシーを指定します。
重大度	重大度を次の中から選択します。(初期値:ワーニング) 「エマージェンシー」、「アラート」、「クリティカル」、「エラー」、「ワーニング」、「通知」、「情報」、「デバッグ」 重大度とアイコンの枠線/ステータスアイコンの対応表は、 こちら を参照してください。
メッセージ	障害検知時に表示されるメッセージを設定します。 ※メッセージを表示させるためには、アラートポリシーに「インシデント登録」アクションが定義されている必要があります。

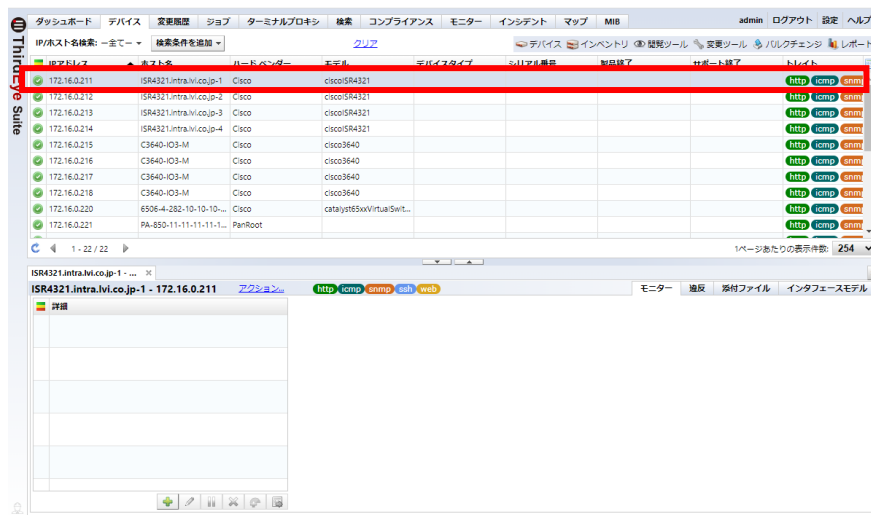
9. [保存]をクリックします。



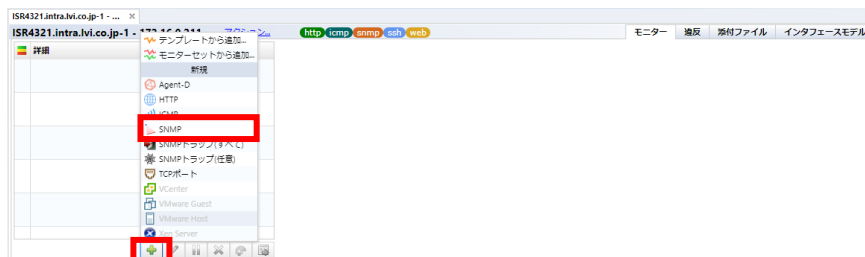
5.3.3 SNMP 情報を収集する Enterprise Suite

監視対象機器から CPU 使用率やトラフィック量といった MIB 情報を取得するためには、SNMP モニターを追加します。ここでは、監視対象機器に対して以下の Cisco 社機器の CPU 使用率 (cpmCPUTotal1minRev) を取得する手順を記載します。

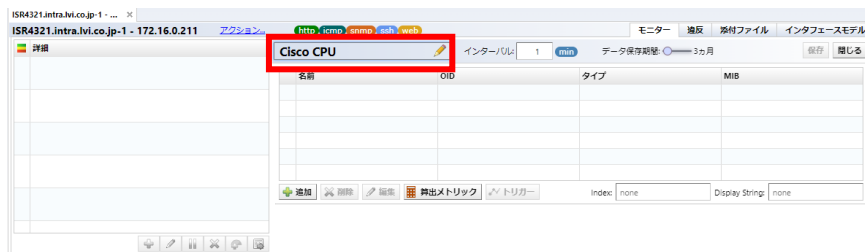
1. [デバイス]タブの監視対象機器一覧から、モニターを設定する機器をダブルクリックします。



2. 左下の[+] (追加)をクリックし、「SNMP」をクリックします。



3. 任意のモニター名を入力します。



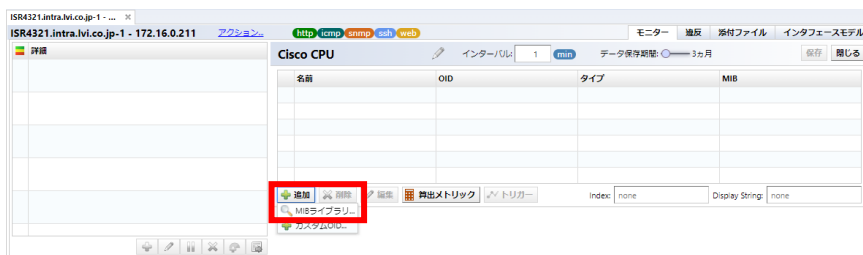
4. インターバルを指定します。



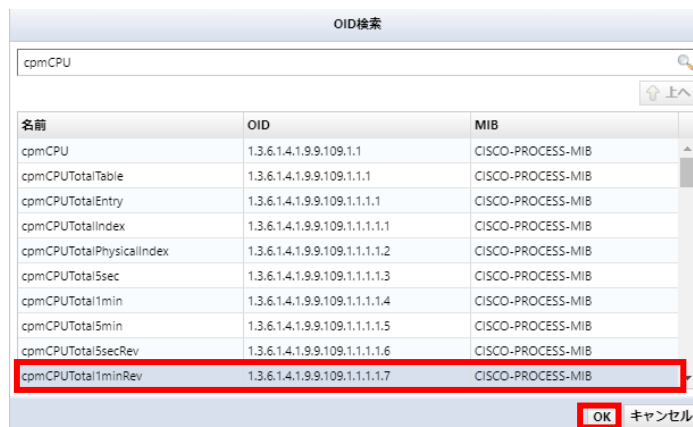
5. データ保存期間を「3ヶ月/6ヶ月/12ヶ月」から指定します。



6. [ (追加)] をクリックし、[MIB ライブラリ] をクリックします。



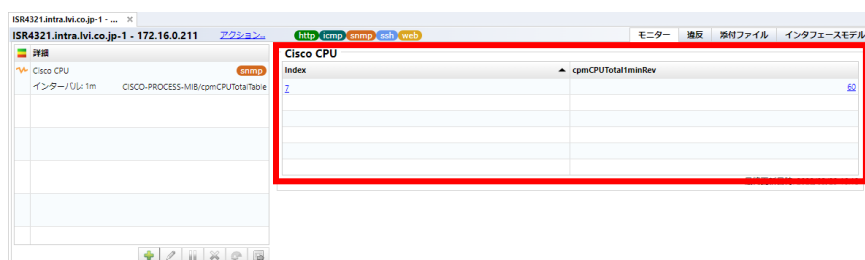
7. OID 検索に MIB の OID または名前を入力し、追加する MIB を選択して、[OK] をクリックします。



8. [保存]をクリックします。



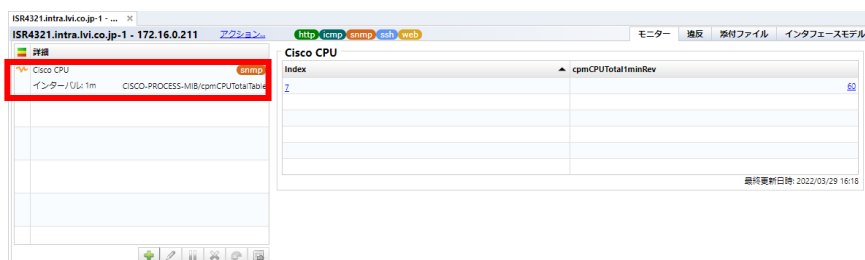
保存後、データ収集が開始され正常に取得できればデバイス詳細画面にデータが表示されます。



5.3.4 しきい値を設定して監視する

取得するデータに対してしきい値を設定し、違反時にアラートをあげることができます。ここでは、「[5.3.3 SNMP 情報を収集する](#)」で作成した SNMP モニターに対して、しきい値を設定します。

1. 詳細テーブルから、しきい値を設定するモニターをダブルクリックまたは[編集]をクリックします。

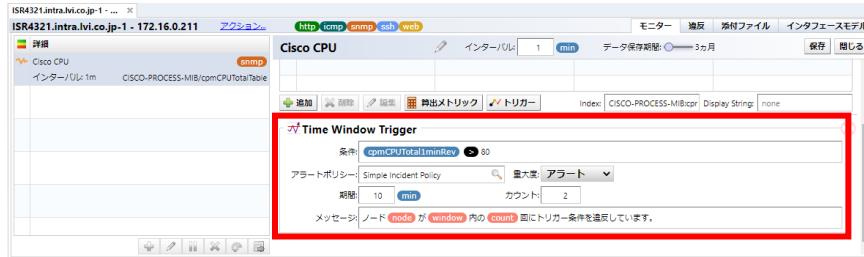


2. [トリガー]をクリックし、[期間]をクリックします。



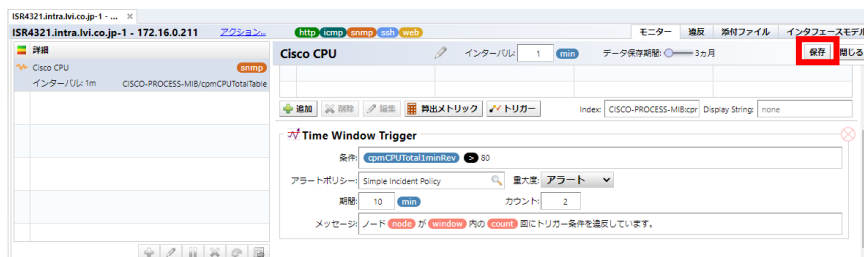
3. 以下の項目を入力します。

以下の画像は、CPU 使用率が 80%を超えた場合にアラート発報するように設定された例です。



項目	説明
条件	以下の項目を使って、条件を指定することができます。 <ul style="list-style-type: none"> • is (等しい) • is not (等しくない) • > (より小さい、右の値のほうが小さい) • < (より大きい、右の値のほうが大きい) • contains (含む) • not contains (含まない)
アラートポリシー	アラートポリシーを指定します。
重大度	重大度を次の中から選択します。(初期値:ワーニング) 「エマージェンシー」、「アラート」、「クリティカル」、「エラー」、「ワーニング」、「通知」、「情報」、「デバッグ」 重大度とアイコンの枠線/ステータスアイコンの対応表は、 こちら を参照してください。
期間	処理を実行するための期間を設定します。(最小値:30 秒) 定められた期間内に何回失敗(カウント)したらポリシーに定義された処理を実行するのか、カウントの基準となる期間。
カウント	設定期間内に何回失敗したら処理を実行するかを設定します。(※最小値:1)
メッセージ	処理を実行するときのメッセージを設定する。

4. [保存]をクリックします。

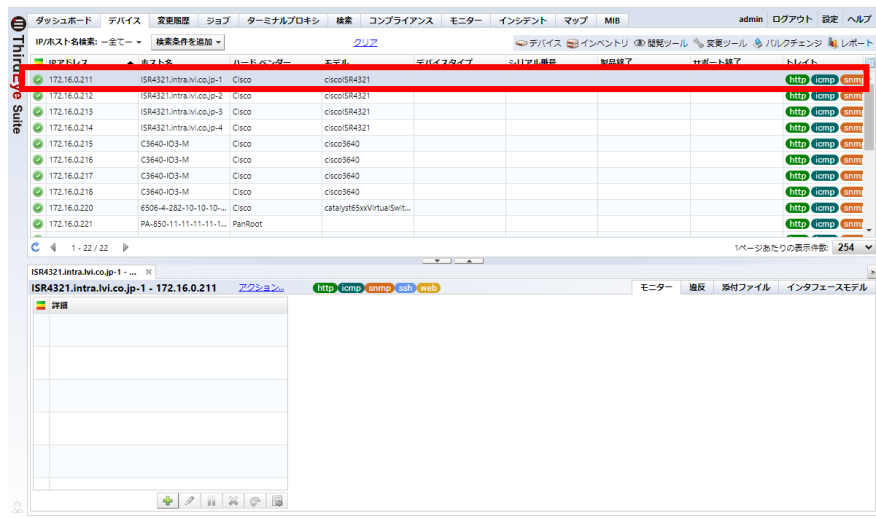



5.3.5 SNMPトラップを監視する(OID 指定)

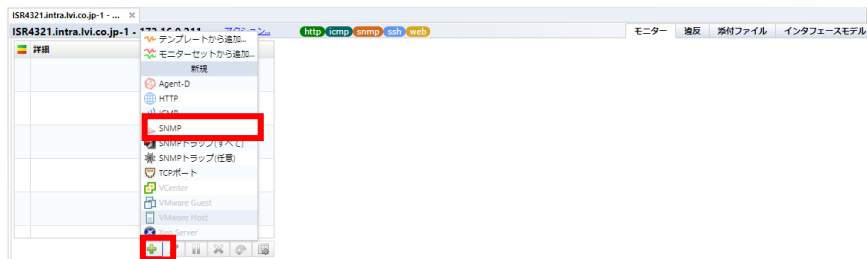
指定された SNMP トラップを対象として監視を行います。監視したい SNMP トラップの OID をあらかじめ設定しておくことで、該当する SNMP トラップを受信した時に、その設定に基づいたアクションを実行できます。SNMP トラップごとに異なるアクションを構成したい場合に設定します。

※すべての SNMP トラップを対象として監視を行う方法もあります。詳しくは、「[5.3.6 SNMP トラップを監視する\(すべて\)](#)」を参照してください。

1. [デバイス]タブの監視対象機器一覧から、モニターを設定する機器をダブルクリックします。



2. 左下の[追加]をクリックし、「SNMPトラップ(任意)」をクリックします。



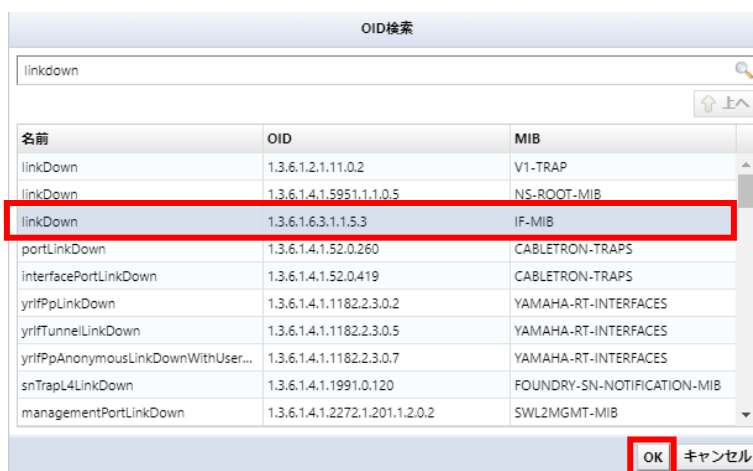
3. 任意のモニター名を入力します。



4. [MIB ライブラリ]をクリックします。



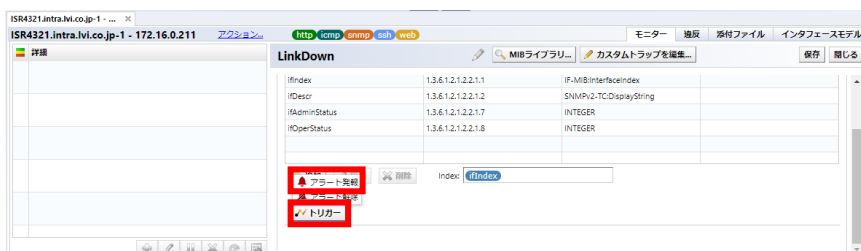
5. OID 検索にトラップ OID または名前を入力し、監視するトラップを選択し、[OK]をクリックします。



6. 障害発生時のメッセージを入力します。



7. [トリガー]をクリックし、[アラート発報]をクリックします。



8. 以下の項目を入力します。



項目	説明
条件	<p>[トリガーに以下の条件を指定する]にチェックを入れると、以下の項目を使って、条件を指定することができます。</p> <ul style="list-style-type: none"> • is (等しい) • is not (等しくない) • > (より小さい、右の値のほうが小さい) • < (より大きい、右の値のほうが大きい) • contains (含む) • not contains (含まない)
アラートポリシー	アラートポリシーを指定します。
重大度	<p>重大度を次の中から選択します。(初期値: ワーニング) 「エマージェンシー」、「アラート」、「クリティカル」、「エラー」、「ワーニング」、「通知」、「情報」、「デバッグ」 重大度とアイコンの枠線/ステータスアイコンの対応表は、こちらを参照してください。</p>

9. [保存]をクリックします。

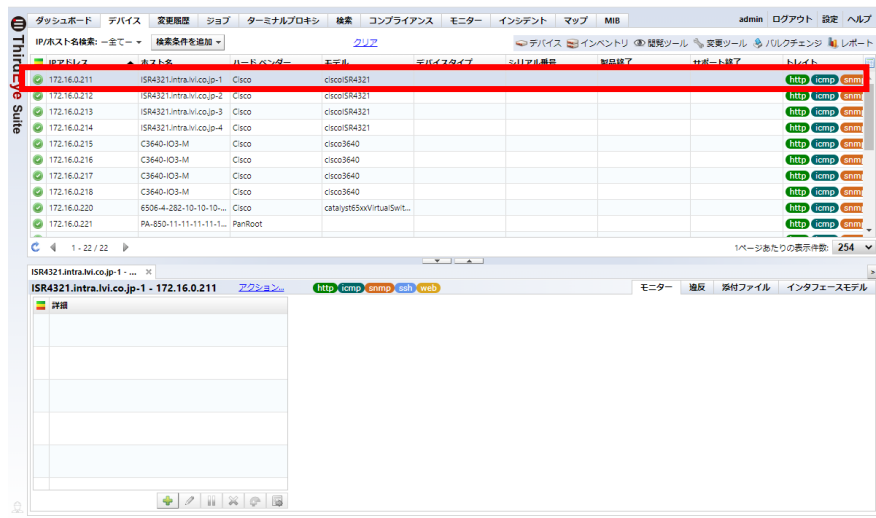


5.3.6 SNMPトラップを監視する(すべて)

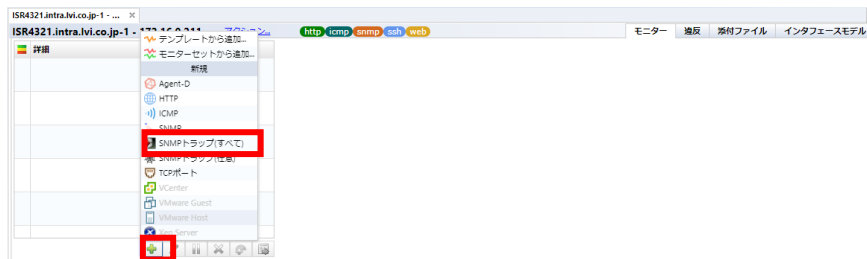
すべての SNMP トラップを対象として監視を行います。「SNMP トラップ(すべて)」をあらかじめ設定しておくことで、SNMP トラップを受信した時に、設定に基づいた共通のアクションを実行できます。監視対象のトラップがはっきりと決まっていない場合、または、すべての SNMP トラップを監視してインシデント登録したい場合に使用すると便利です。

なお、「SNMP トラップ(すべて)」設定は、監視したいトラップ OID を指定する「SNMP トラップ(任意)」設定と併用できます。併用した場合、「SNMP トラップ(任意)」設定が優先されます。

1. [デバイス]タブの監視対象機器一覧から、モニターを設定する機器をダブルクリックします。



2. 左下の[+] (追加)をクリックし、「SNMP トラップ(すべて)」をクリックします。



3. 任意のモニター名を入力します。



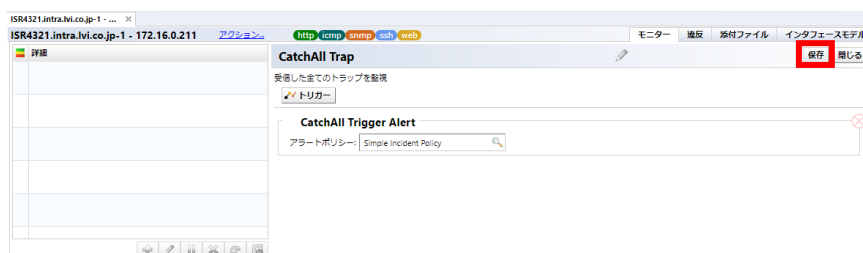
4. [トリガー]をクリックし、[Catch All Trap Alert]をクリックします。



5. アラートポリシーを指定します。



6. [保存]をクリックします。



以上の設定により、監視対象機器から受信したすべての SNMP トラップに対して、アラートを発報するようになります。

5.3.7 モニターセットを使用して多数の機器に対して監視設定をする

ThirdEye のモニター設定には、複数のモニターを 1 つにまとめて構成する「モニターセット」という機能があります。「モニターセット」を使用することで、構成されたモニターを一度に多数のデバイスに適用することができます。

1. [モニター]→[セット]を選択し、[追加]をクリックします。



2. モニターセット名を入力し、[OK]をクリックします。

モニターセットを作成

モニターセット名:

新しくデバイスが追加された際に、このモニターセットを自動的に適用する。

OK
キャンセル

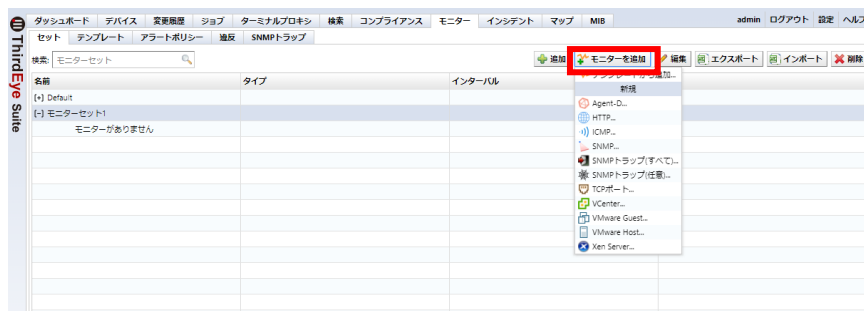
項目	説明
新しくデバイスが追加された際に、このモニターセットを自動的に適用する。	このモニターセットに含まれるモニターを、デバイスを追加した時に自動的に割り当てます。

3. 作成したモニターセットを選択します。



4. [モニターを追加]をクリックし、監視項目を設定します。

※モニターの作成方法は、個別のモニター設定と同じ方法で追加できます。



項目	説明
テンプレートから追加	[テンプレート]に、作成されているモニターテンプレートの中からモニターを追加します。
Agent-D	Agent-D のモニターを追加します。
HTTP	http または https に対する監視するモニターを追加します。
ICMP	ICMP Ping によるモニターを追加します。
SNMP	MIB テーブルから監視する MIB オブジェクトを指定し監視するモニターを追加します。
SNMPトラップ(すべて)	すべての SNMPトラップを監視するモニターを追加します。
SNMPトラップ(任意)	指定された SNMPトラップを監視するモニターを追加します。
TCP ポート	指定された TCP ポートに対する監視するモニターを追加します。
VCenter	vCenter のリソース情報を取得するモニターを追加します。
VMware Guest	vCenter 経由で、VMware ゲストのリソース情報を取得するモニターを追加します。
VMware Host	vCenter 経由で、VMware ホストのリソース情報を取得するモニターを追加します。
Xen Server	Citrix Xen Server のメモリ使用状況を確認するモニターを追加します。

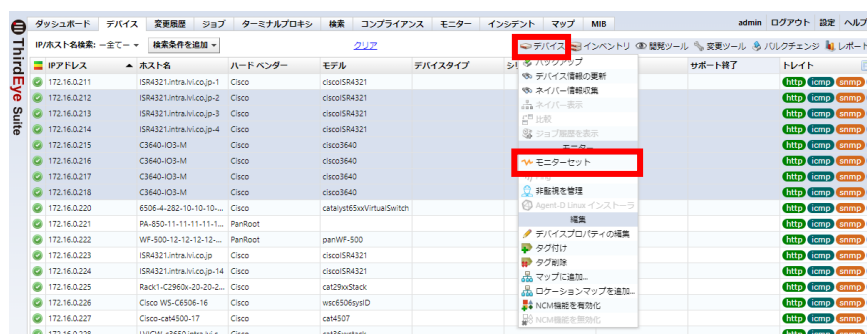
【モニター追加後の画面例】

名前	タイプ	インターバル	詳細
(-) モニターセット1			
Cisco CPU	SNMP	1m	CISCO-PROCESS-MIB/cpmCPUTotal
ICMP Ping	ICMP	30s	ICMP echo
Link-down Trap	SNMPトラップ(任意)	n/a	IF-MIB/linkDown
Link-up Trap	SNMPトラップ(任意)	n/a	IF-MIB/linkUp
インタフェース使用量 (64bit)	SNMP	1m	IF-MIB/IFTable

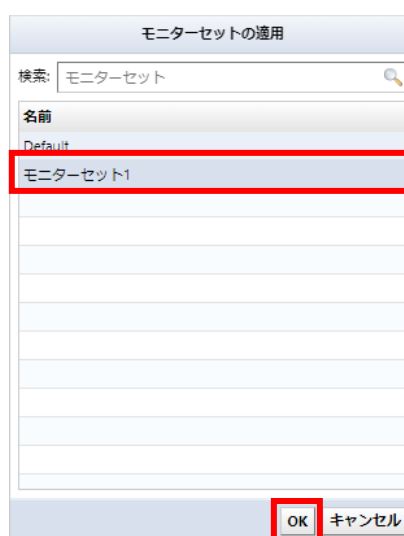
5. [デバイス]タブを選択し、モニターセットを割り当てるデバイスを選択します。

IPアドレス	ホスト名	ハードベンダー	モデル	デバイスタイプ	シリアル番号	製品終了	サポート終了	トレイト
172.16.0.211	ISR4321.intra.nico.jp-1	Cisco	ciscoSR4321					http icmp snmp
172.16.0.212	ISR4321.intra.nico.jp-2	Cisco	ciscoSR4321					http icmp snmp
172.16.0.213	ISR4321.intra.nico.jp-3	Cisco	ciscoSR4321					http icmp snmp
172.16.0.214	ISR4321.intra.nico.jp-4	Cisco	ciscoSR4321					http icmp snmp
172.16.0.215	C3640-03-M	Cisco	cisco3640					http icmp snmp
172.16.0.216	C3640-03-M	Cisco	cisco3640					http icmp snmp
172.16.0.217	C3640-03-M	Cisco	cisco3640					http icmp snmp
172.16.0.218	C3640-03-M	Cisco	cisco3640					http icmp snmp
172.16.0.220	6506-4-282-10-10-10...	Cisco	catalyst6506VirtualSwitch					http icmp snmp
172.16.0.221	PA-850-11-11-11-11...	PanRoot						http icmp snmp
172.16.0.222	WF-500-12-12-12-12...	PanRoot	panWF-500					http icmp snmp
172.16.0.223	ISR4321.intra.nico.jp	Cisco	ciscoSR4321					http icmp snmp
172.16.0.224	ISR4321.intra.nico.jp-14	Cisco	ciscoSR4321					http icmp snmp

6. [デバイス]→[モニターセット]の順にクリックします。



7. 適用したいモニターセットを選択し、[OK]をクリックします。



以上の操作で、モニターセットの適用は完了です。

デバイス詳細表示領域の左にある[詳細]欄には、監視中のモニターが一覧で表示されます。デバイスをダブルクリックして展開し、モニターが[詳細]欄に反映されているかを確認できます。



5.4 マップを設定する

マップは、ネットワーク構成を視覚的に管理するための表示機能です。監視対象機器をオブジェクトとしてマップに追加することで、デバイスの障害状況を視覚的に表示することができます。

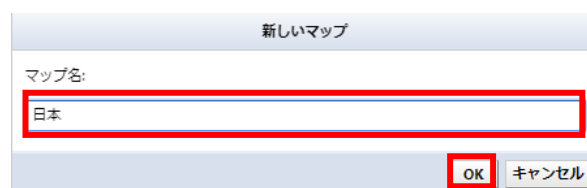
5.4.1 マップを作成する

マップ階層を表すマップオブジェクトを作成します。複数のマップオブジェクトを作成し、階層構造の監視マップを作成することもできます。

1. 画面左下にある[ (作成)]をクリックします。



2. [新しいマップ]画面が表示されます。マップ名を入力し、[OK]をクリックします。

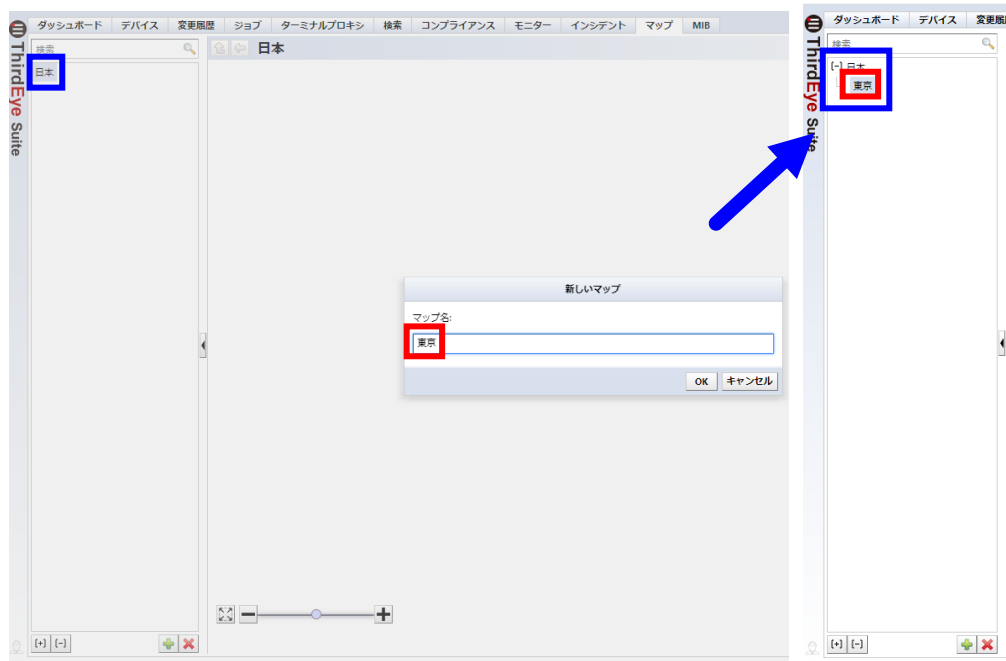


3. 画面左側のマップ一覧に、保存したマップが表示されます。



画面左側のマップ一覧で、マップを選択した状態で新しいマップを作成すると、選択したマップの下位階層に新しいマップを作成できます。

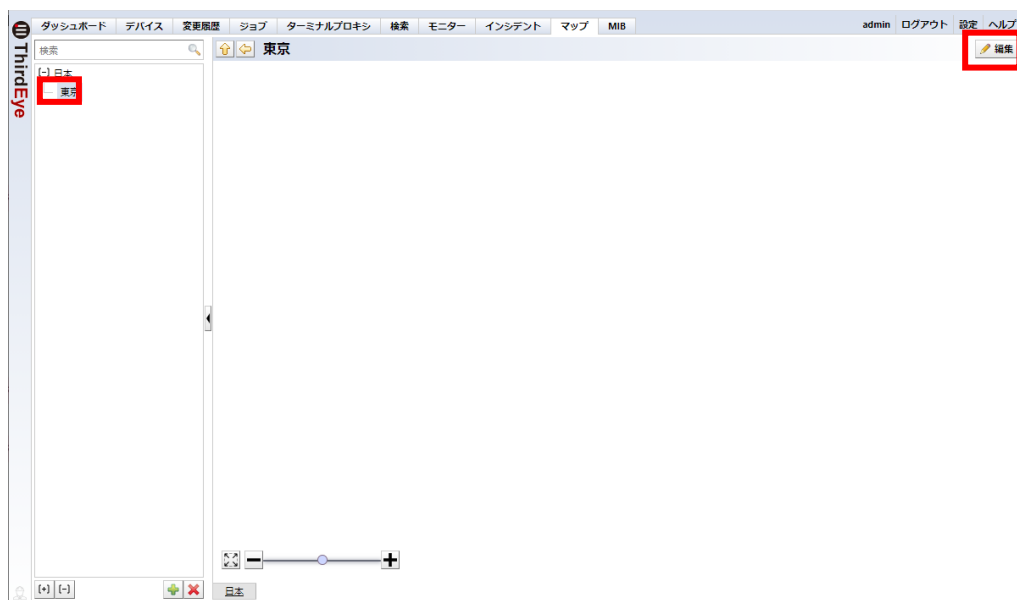
補足



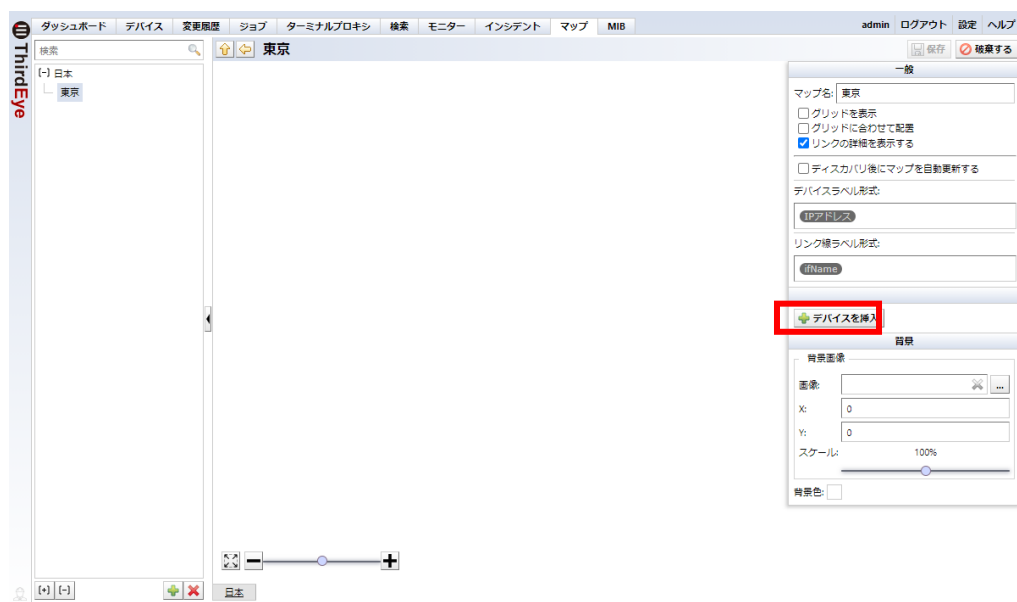
5.4.2 マップにデバイスを挿入する

マップオブジェクトの上にデバイスオブジェクトを配置します。

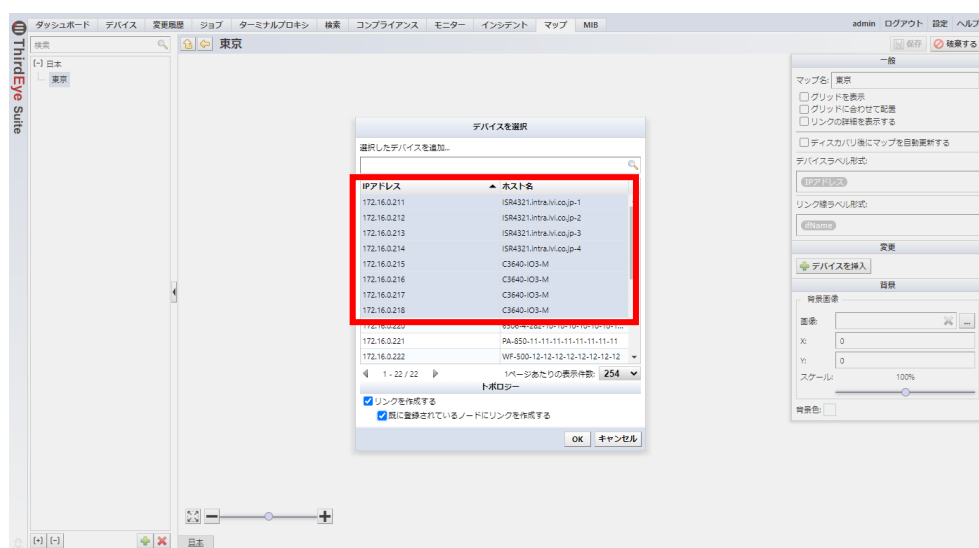
1. 画面左側のマップ一覧から、デバイスを追加するマップをダブルクリックで開き、[編集]をクリックします。



2. [デバイスを挿入]をクリックします。

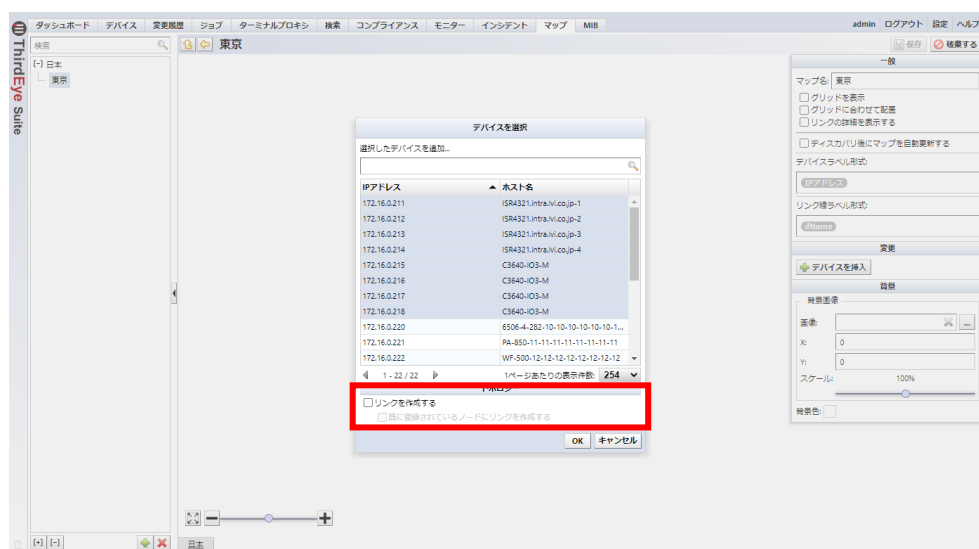


3. マップに挿入するデバイスを選択します。

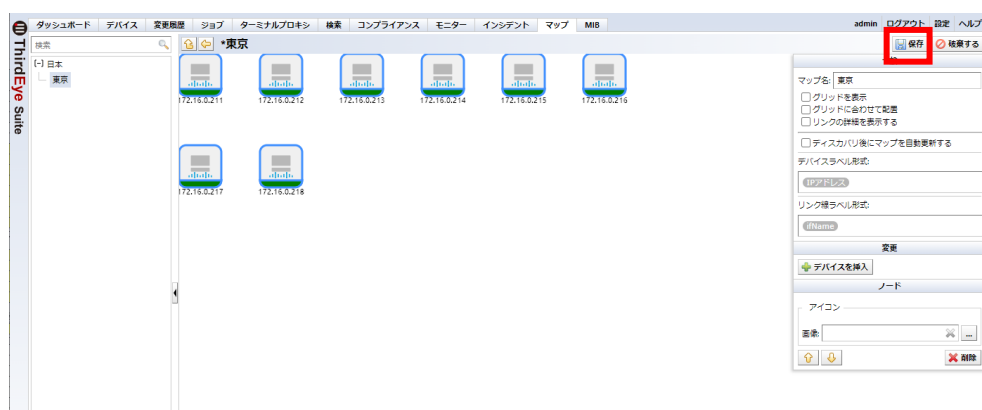


4. [リンクを作成する]のチェックを外し、[OK]をクリックします。

※[リンクを作成する]は、ARP/MAC アドレステーブルなどの情報に基づいて、L2 マップを自動作成する機能です。詳しくは、「[5.4.3 トポロジーマップを作成する](#)」を参照してください。



5. デバイスオブジェクトが挿入されます。[保存]をクリックし、編集を完了します。



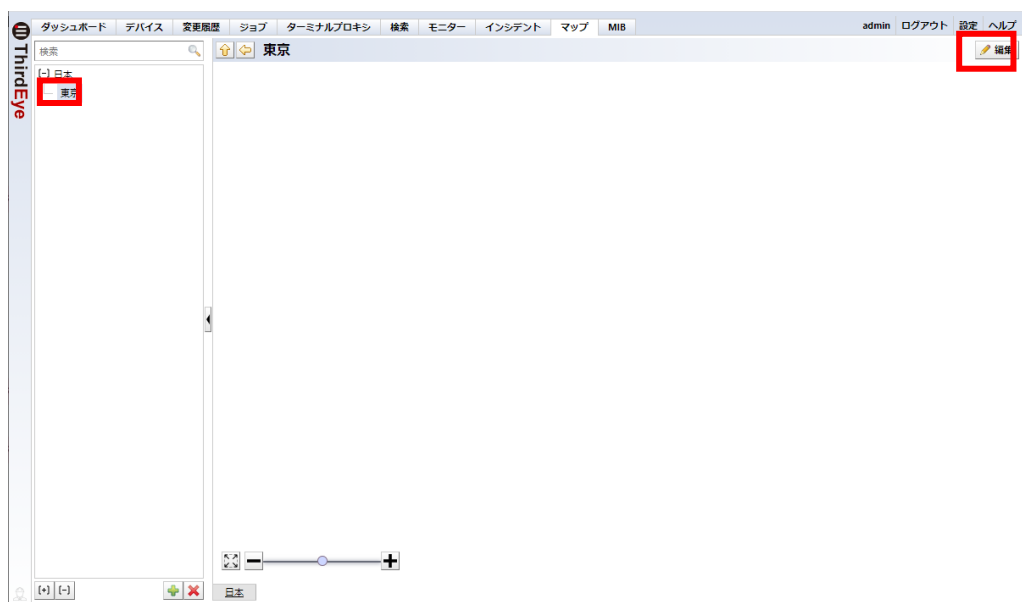
5.4.3 トポロジーマップを作成する

リビジョン 20210730.0146 から、ARP/MAC アドレステーブル、CDP、LLDP の情報に基づいて L2 マップを自動作成する機能が実装されました。これらの情報は、デバイスの追加時やデバイス情報の更新時に、SNMP を使用して取得されます。

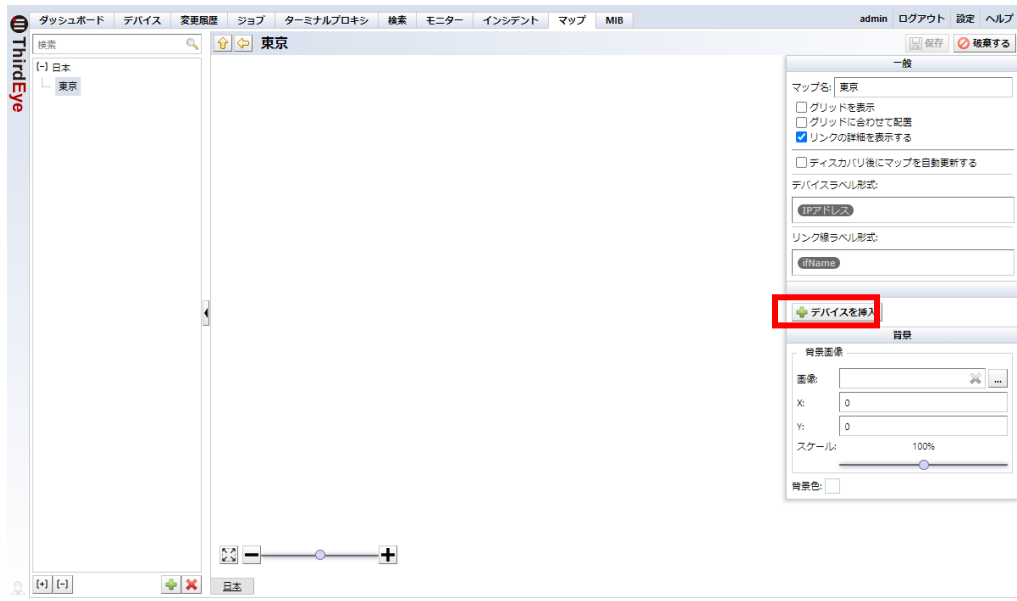
トポロジー機能を利用する場合の注意事項

- SNMP ポーリングを使用してデバイスから情報を取得する必要があります。
- トポロジー機能を利用したマップは、情報取得時の情報に基づいて作成されます。トポロジーマップの構成情報が、常に最新であるとは限りません。

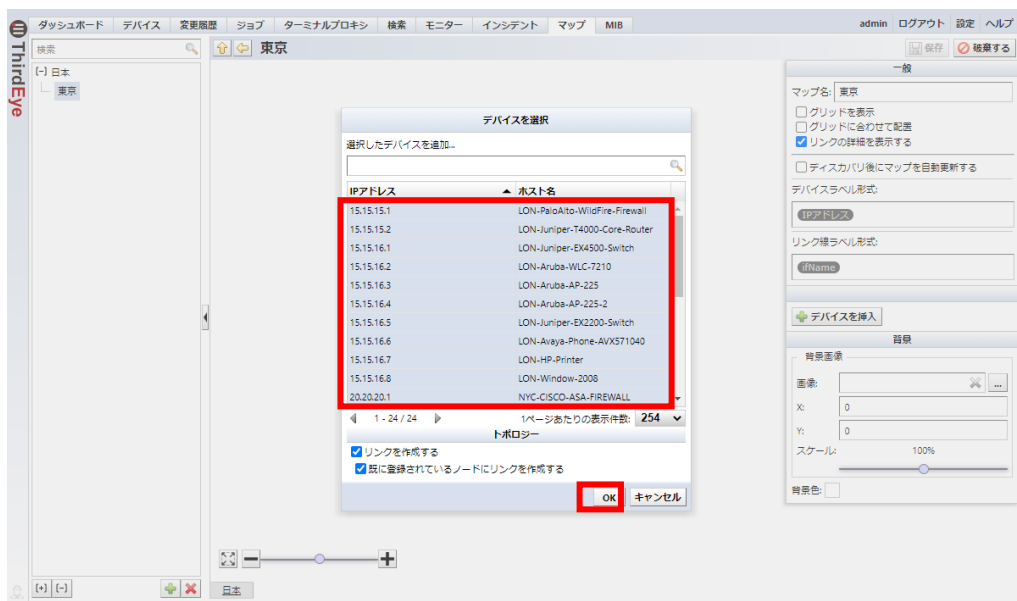
1. 画面左側のマップ一覧から、デバイスを追加するマップをダブルクリックし、[編集]をクリックします。



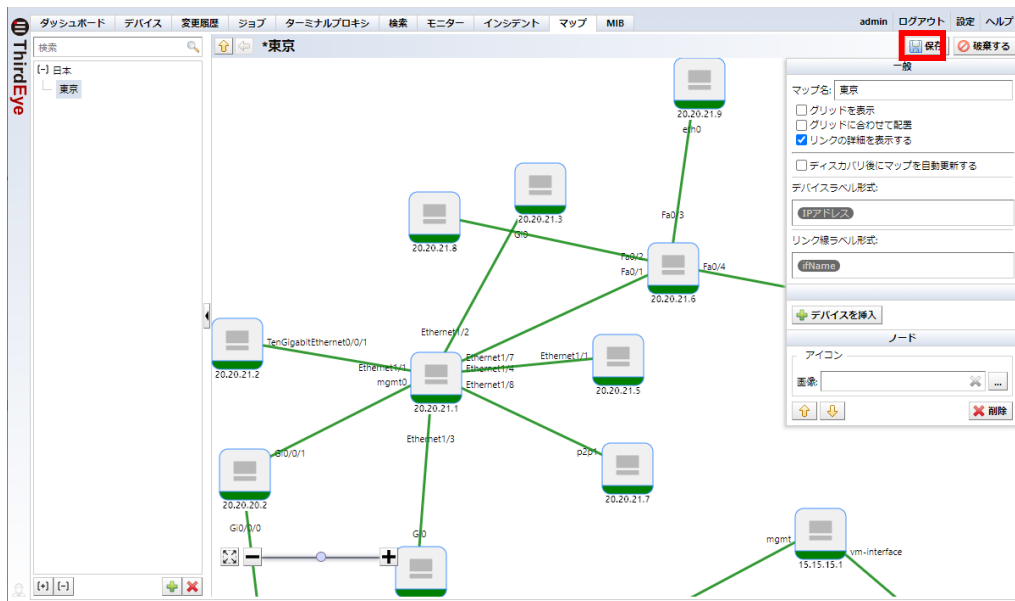
2. [デバイスを挿入]をクリックします。



3. マップに挿入するデバイスを選択し、[リンクを作成する]にチェックを入れて[OK]をクリックします。



4. デバイスオブジェクトが挿入されます。[保存]をクリックし、編集を完了します。



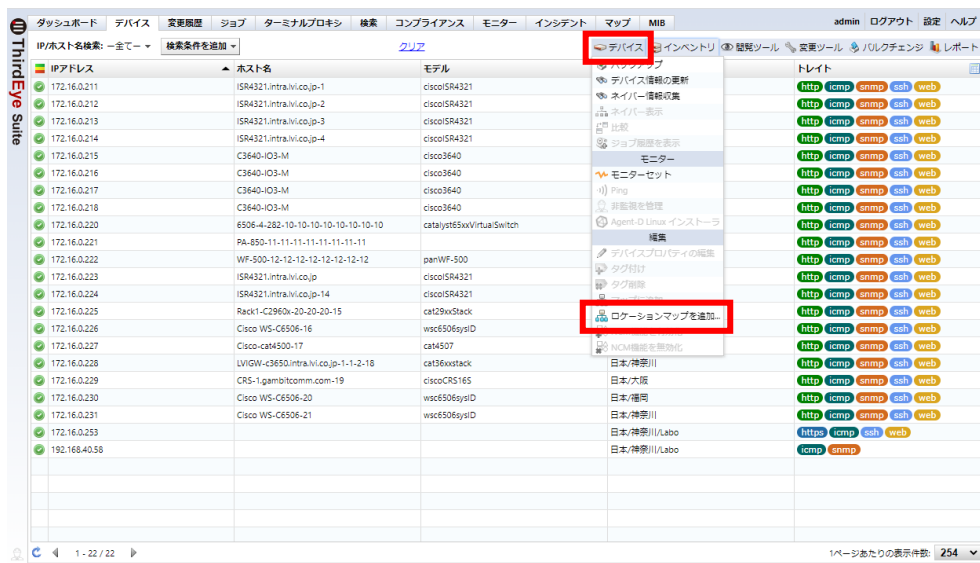
5.4.4 カスタムフィールドを使用したロケーションマップを作成する

カスタムフィールドの情報を使用して、マップを作成することができます。

【カスタムフィールドの設定イメージ】

IPアドレス	ホスト名	モデル	カスタム 1
172.16.0.211	ISR4321.intra.lvi.co.jp-1	ciscoSR4321	日本/東京
172.16.0.212	ISR4321.intra.lvi.co.jp-2	ciscoSR4321	日本/神奈川
172.16.0.213	ISR4321.intra.lvi.co.jp-3	ciscoSR4321	日本/大阪
172.16.0.214	ISR4321.intra.lvi.co.jp-4	ciscoSR4321	日本/福岡
172.16.0.215	C3640-IO3-M	cisco3640	日本/東京
172.16.0.216	C3640-IO3-M	cisco3640	日本/神奈川
172.16.0.217	C3640-IO3-M	cisco3640	日本/大阪
172.16.0.218	C3640-IO3-M	cisco3640	日本/福岡
172.16.0.220	6506-4-282-10-10-10-10-10-10	catlyst65xxVirtualSwitch	日本/東京
172.16.0.221	PA-850-11-11-11-11-11-11-11		日本/大阪
172.16.0.222	WF-500-12-12-12-12-12-12-12	panWF-500	日本/福岡
172.16.0.223	ISR4321.intra.lvi.co.jp	ciscoSR4321	日本/東京
172.16.0.224	ISR4321.intra.lvi.co.jp-14	ciscoSR4321	日本/神奈川
172.16.0.225	Rack1-C2960x-20-20-20-15	cat29xxStack	日本/大阪
172.16.0.226	Cisco WS-C6506-16	wsc6506sysID	日本/福岡
172.16.0.227	Cisco-cat4500-17	cat4507	日本/東京
172.16.0.228	LVI6W-c3650.intra.lvi.co.jp-1-1-2-18	cat36xxstack	日本/神奈川
172.16.0.229	CRS-1.gambitcomm.com-19	ciscoCRS165	日本/大阪
172.16.0.230	Cisco WS-C6506-20	wsc6506sysID	日本/福岡
172.16.0.231	Cisco WS-C6506-21	wsc6506sysID	日本/神奈川
172.16.0.253			日本/神奈川/Labo
192.168.40.58			日本/神奈川/Labo

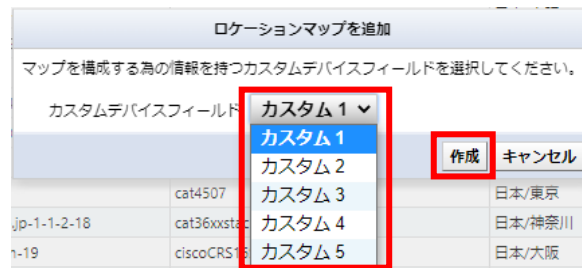
1. [デバイス]タブを選択し、[デバイス]→[ロケーションマップを追加]の順にクリックします。



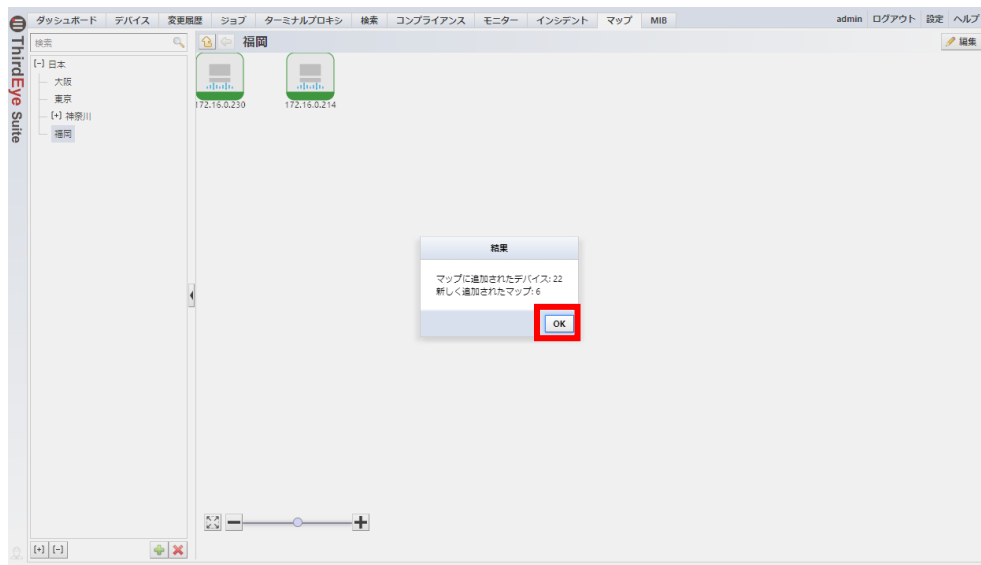
補足

デバイスを選択することで、選択したデバイスを対象にロケーションマップを作成することができます。

2. カスタムフィールドを選択し、[作成]をクリックします。



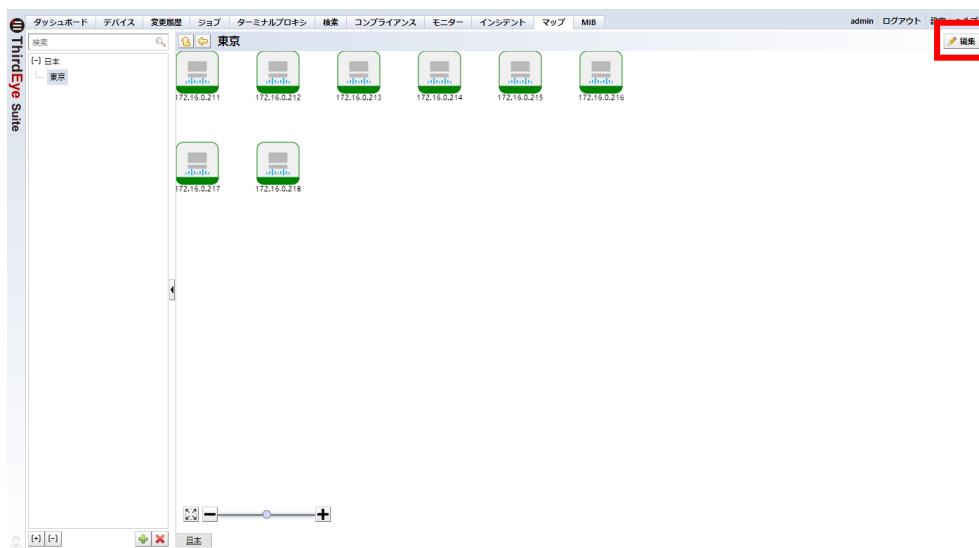
3. [OK]をクリックします。



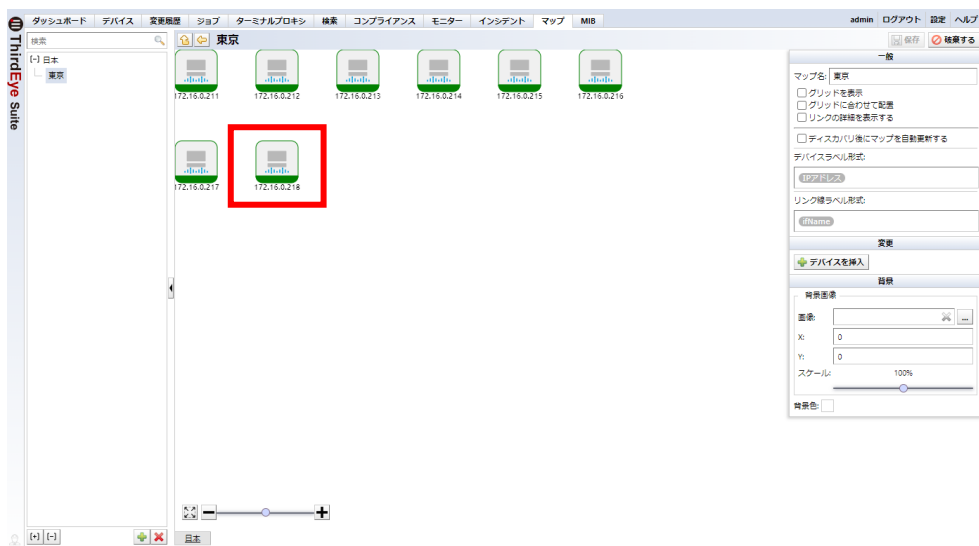
5.4.5 オブジェクトのアイコンを設定する

オブジェクトのアイコンを変更できます。

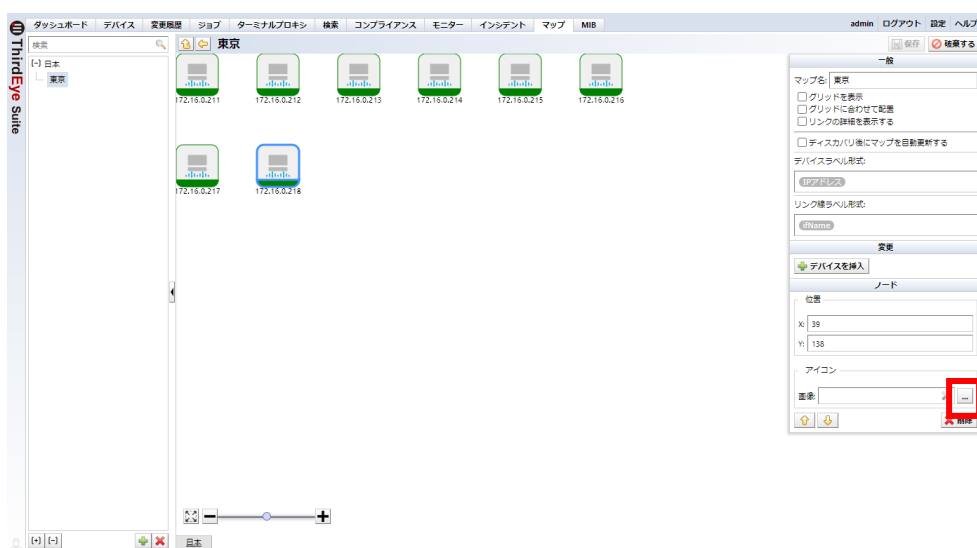
1. マップをダブルクリックで開き、[編集]をクリックします。



2. アイコンを設定したい対象のオブジェクトを選択します。



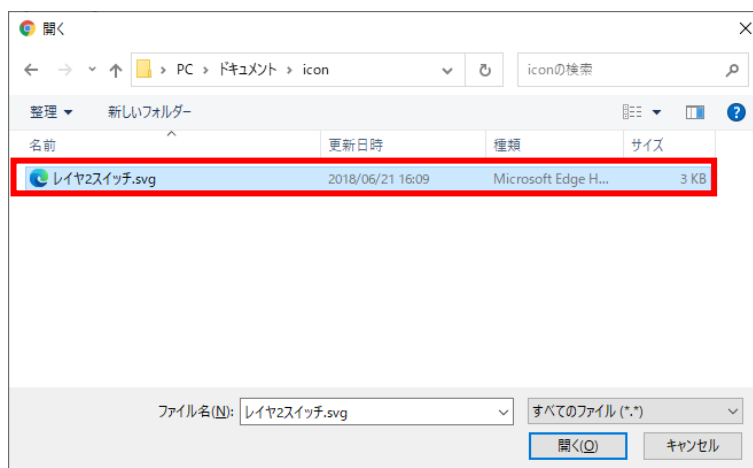
3. 編集メニューの中から、ノードセクションの[画像]欄の右にある[...]をクリックします。



4. ファイルの選択画面が表示されます。[] をクリックし、ファイルをアップロードします。



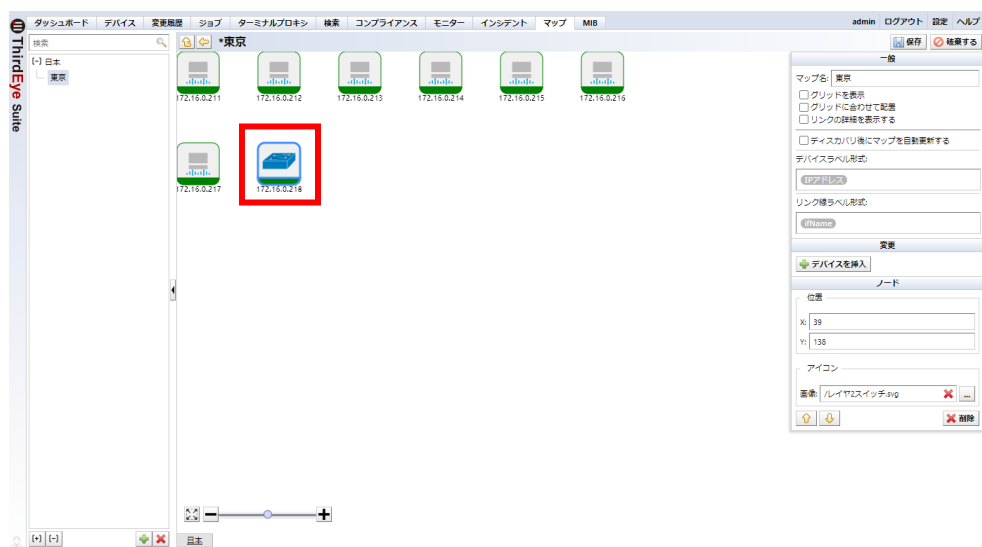
5. アップロードするアイコンを選択します。



6. アイコン画像に設定したいファイルを選択し、[OK]をクリックします。



7. オブジェクトのアイコンが選択した画像に変更されます。

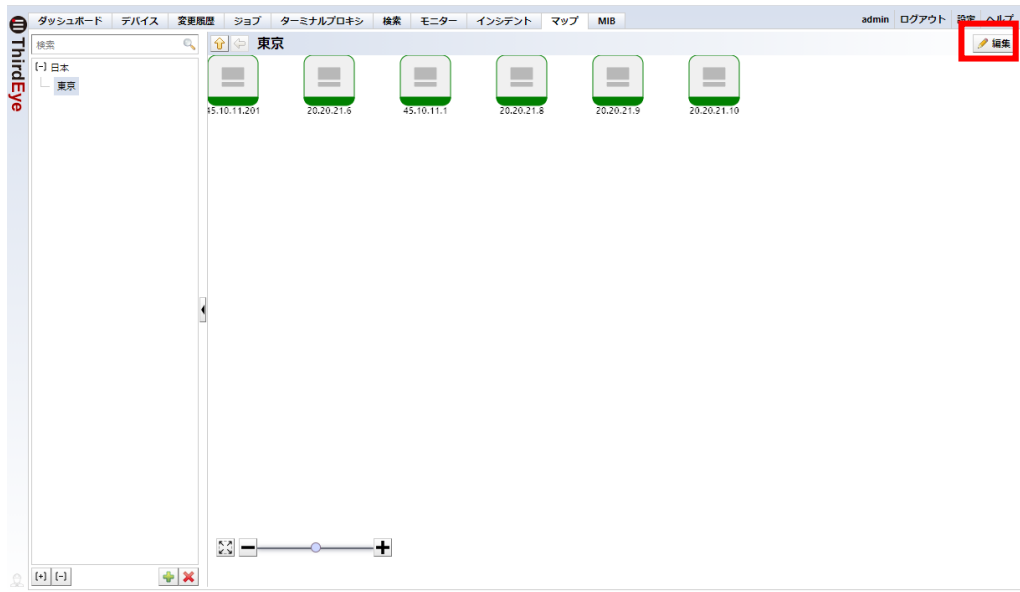


5.4.6 2つのオブジェクトの間を線で結ぶ

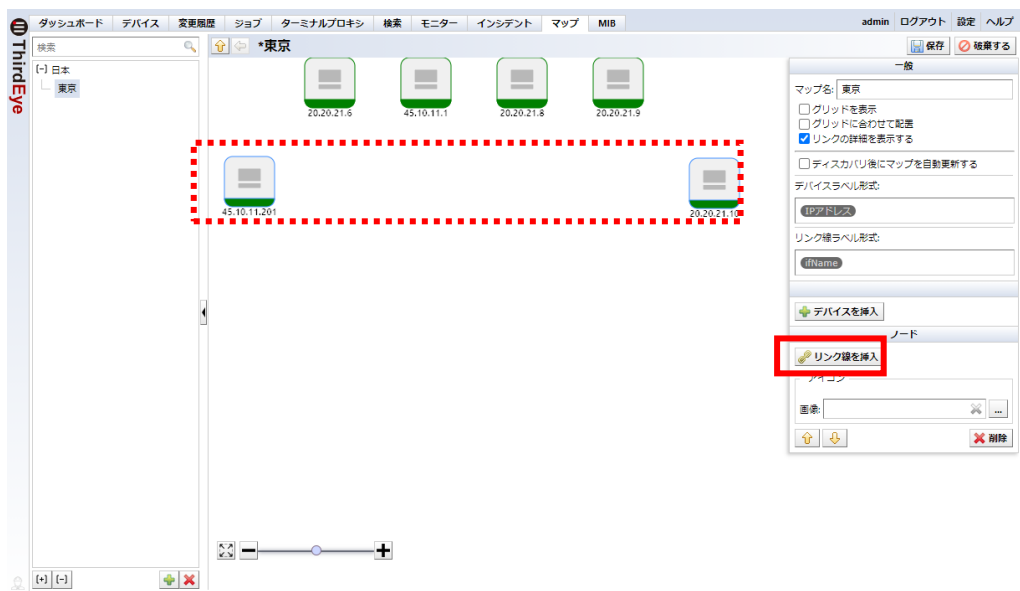
マップやデバイスなどのオブジェクト同士をリンク線でつなぐことができます。

※リンク線の太さは変更できません。

1. マップをダブルクリックで開き、[編集]をクリックします。

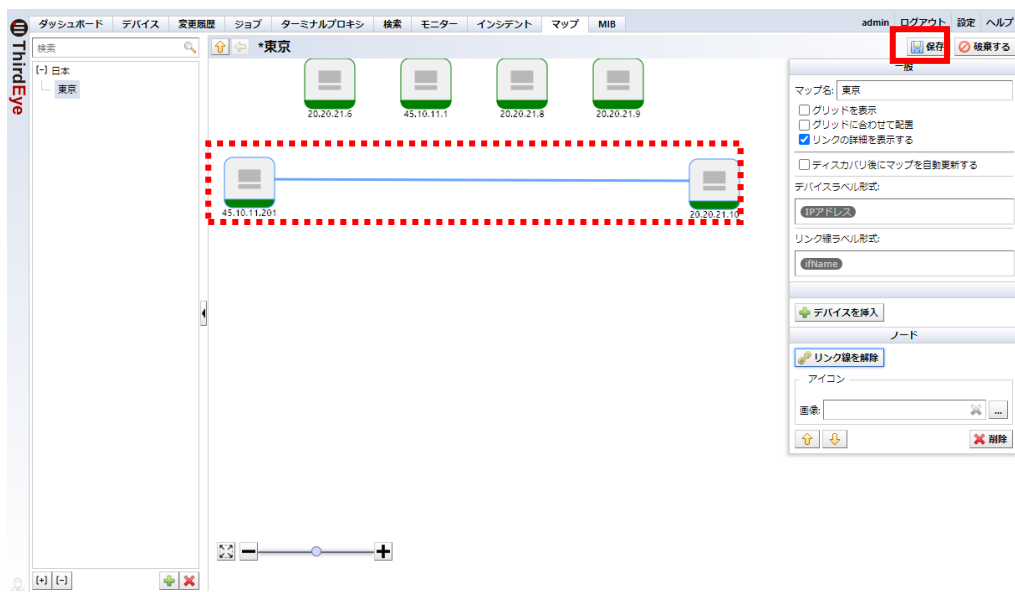


2. キーボードの「Ctrl」キーを押しながら、リンク線でつなぐ2つのデバイスをクリックし選択します。デバイスが選択された状態で[リンク線を挿入]をクリックします。



3. リンク線が挿入されます。[保存]をクリックし、編集を完了します。

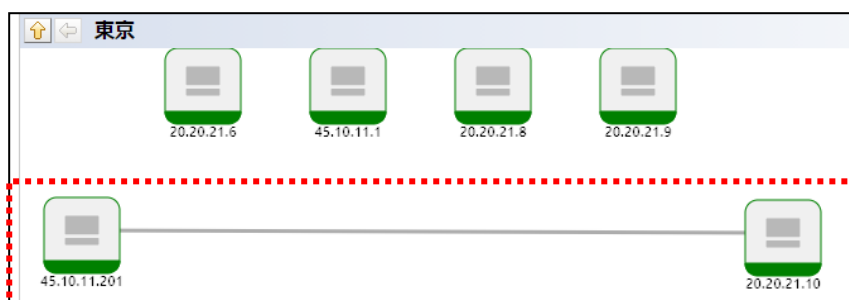
※リンク線を削除する場合は、2つのデバイスを選択した状態で[リンク線を解除]をクリックします。



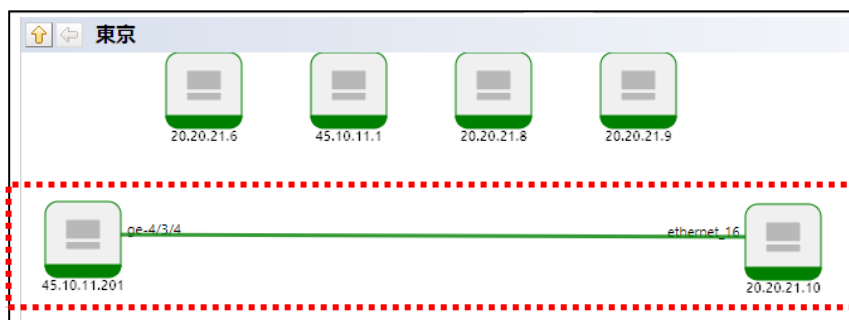
5.4.7 リンク線にインタフェースを紐付ける

リビジョン 20210730.0146 から、リンク線にデバイスのインタフェースを紐付けることができます。リンク線にデバイスのインタフェースを紐付けることで、そのデバイスのインタフェースで障害(LinkDownトラップやトラフィック量のしきい値超過など)が発生した場合に、障害イベントの重大度に応じて、デバイスオブジェクトに加えてリンク線の色が変化するようになります。

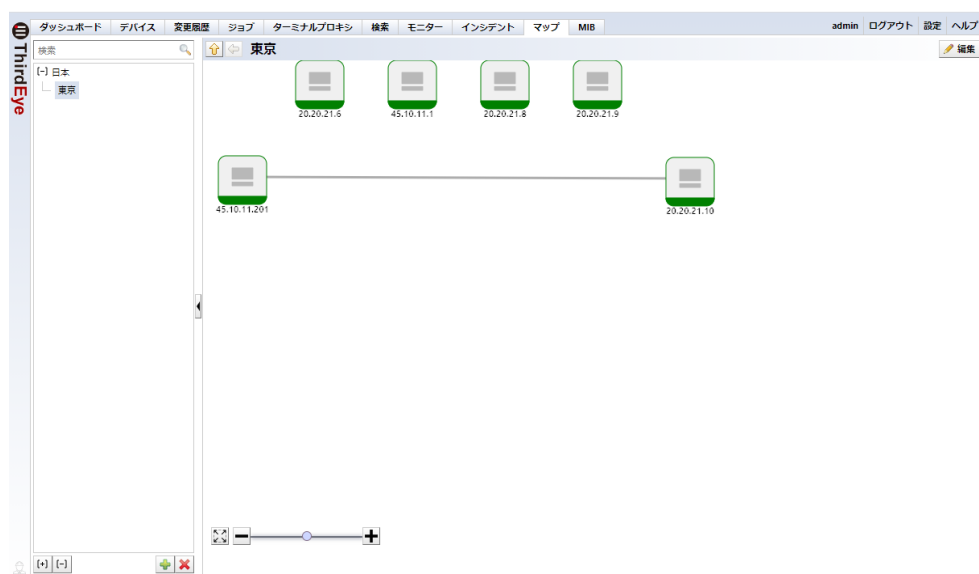
【リンク線にデバイスのインタフェースを紐付けていない状態】



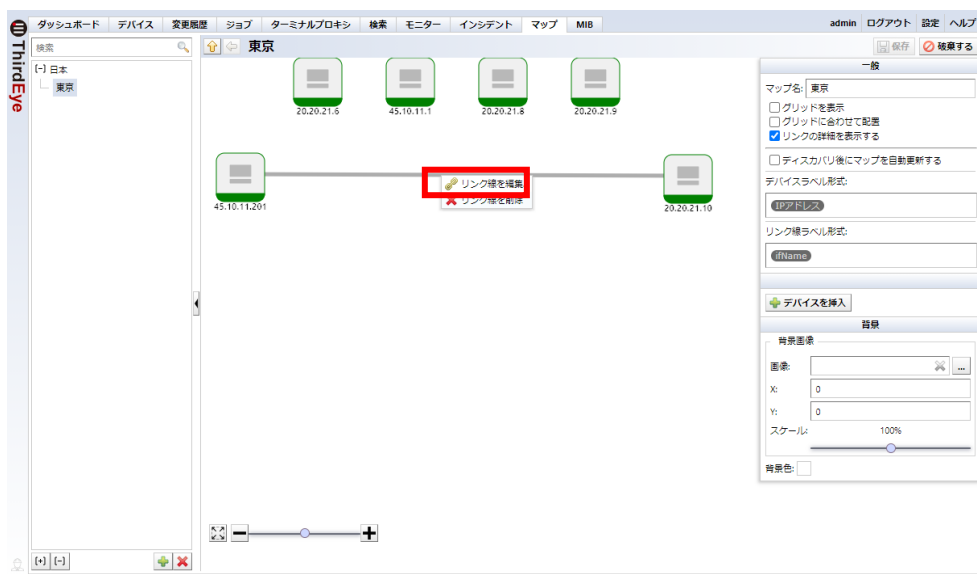
【リンク線にデバイスのインタフェースを紐付けた状態】



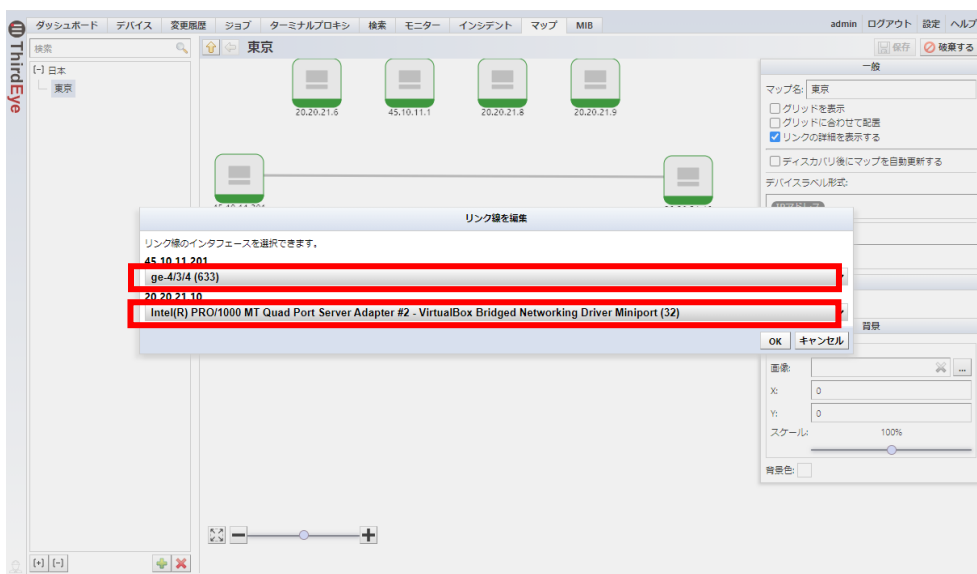
1. マップをダブルクリックで開き、[編集]をクリックします。



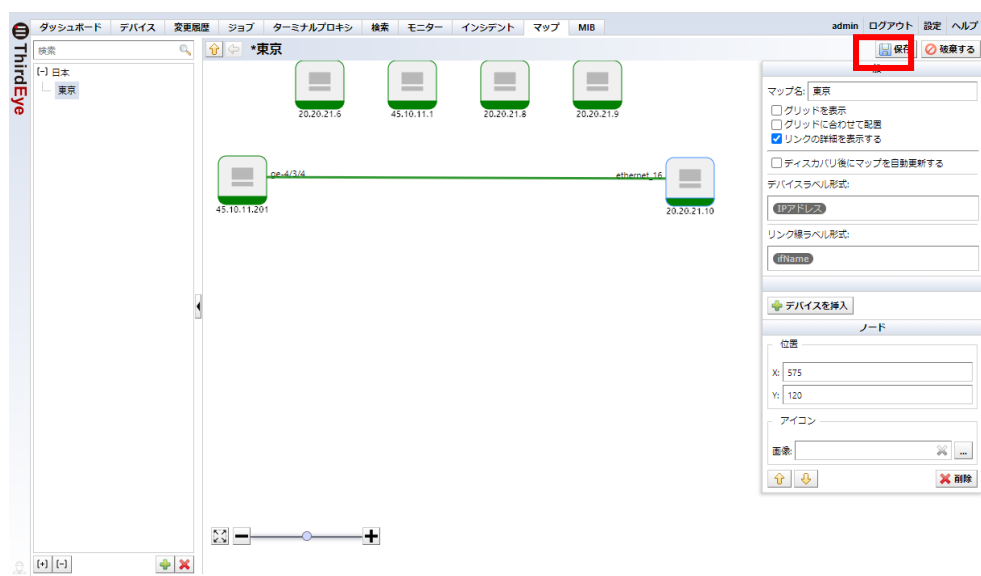
2. リンク線を右クリックし、[リンク線を編集]をクリックします。



3. 各デバイスのプルダウンメニューからインターフェースを選択し、[OK]をクリックします。

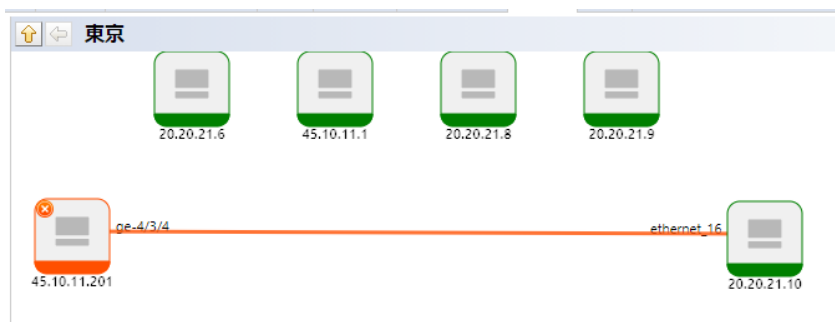


4. [保存]をクリックします。



以上で、リンク線とインタフェースの紐付けは完了です。

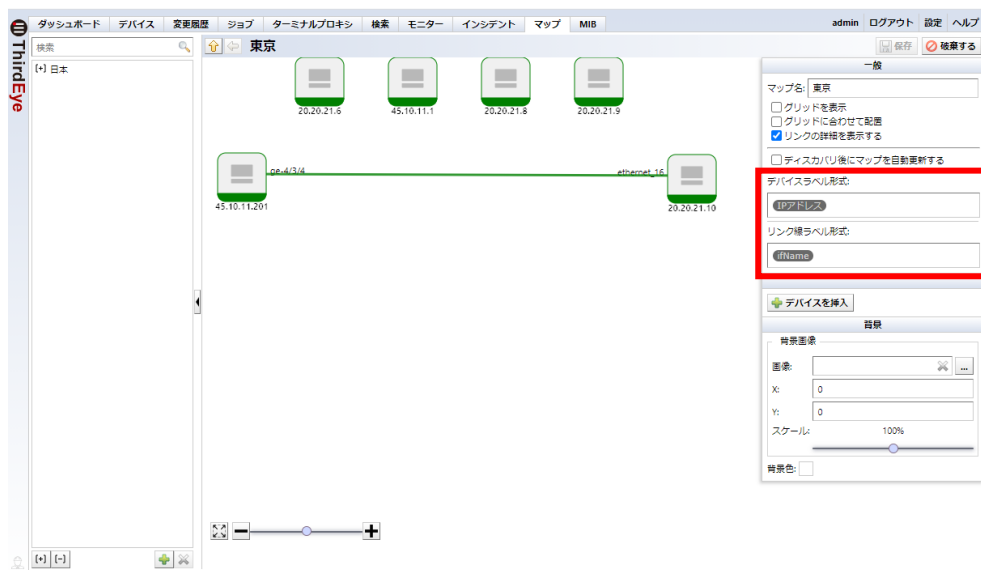
これにより、紐付けられたデバイスのインタフェースで違反が発生すると、デバイスオブジェクトに加えてリンク線の色が変化します。



5.4.8 アイコンのラベルやリンク線の表示形式を設定する

マップ上のデバイスオブジェクトの下側に表示される文字列(ラベル)やリンク線の表示形式を、マップ単位でカスタマイズできます。

1. マップをダブルクリックで開き、[編集]をクリックします。
2. [デバイスラベル形式]および、[リンク線ラベル形式]の設定を変更します。



各ラベル形式に使用できるオブジェクトは、以下のとおりです。任意の文字列を指定することもできます。

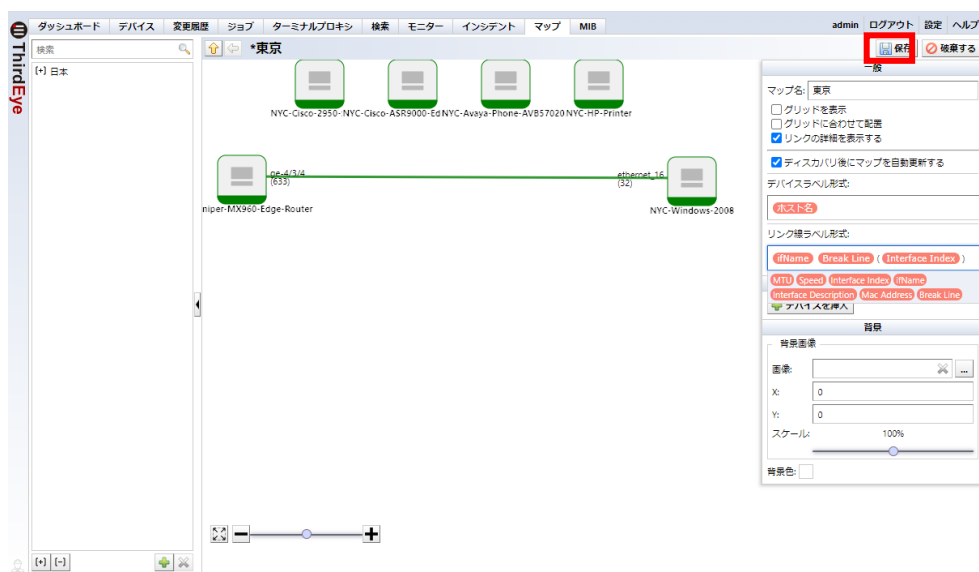
【デバイスラベル形式】

項目	説明
IP アドレス	デバイスの IP アドレスを表示する。(初期値)
ホスト名	デバイスのホスト名を表示する。
ネットワーク	デバイスのネットワークを表示する。
アダプタ	デバイスのアダプタを表示する。
デバイスタイプ	デバイスのデバイスタイプを表示する。
ハードベンダー	デバイスのハードベンダーを表示する。
ソフトベンダー	デバイスのソフトベンダーを表示する。
OS バージョン	デバイスの OS バージョンを表示する。
シリアル番号	デバイスのシリアル番号を表示する。
カスタム 1	デバイスの カスタム 1 の情報を表示する。
カスタム 2	デバイスの カスタム 2 の情報を表示する。
カスタム 3	デバイスの カスタム 3 の情報を表示する。
カスタム 4	デバイスの カスタム 4 の情報を表示する。
カスタム 5	デバイスの カスタム 5 の情報を表示する。
改行	ラベルに改行を挿入する。

【リンク線ラベル形式】

項目	説明
ifName	ifName の値を表示する。(初期値)
Interface Index	ifIndex を表示する。
Interface Description	ifDescr を表示する。
MTU	ifMtu を表示する。
Speed	ifSpeed を表示する。
Mac Address	ifPhysAddress を表示する。
改行	ラベルに改行を挿入する。

3. [保存]をクリックし、編集を完了します。



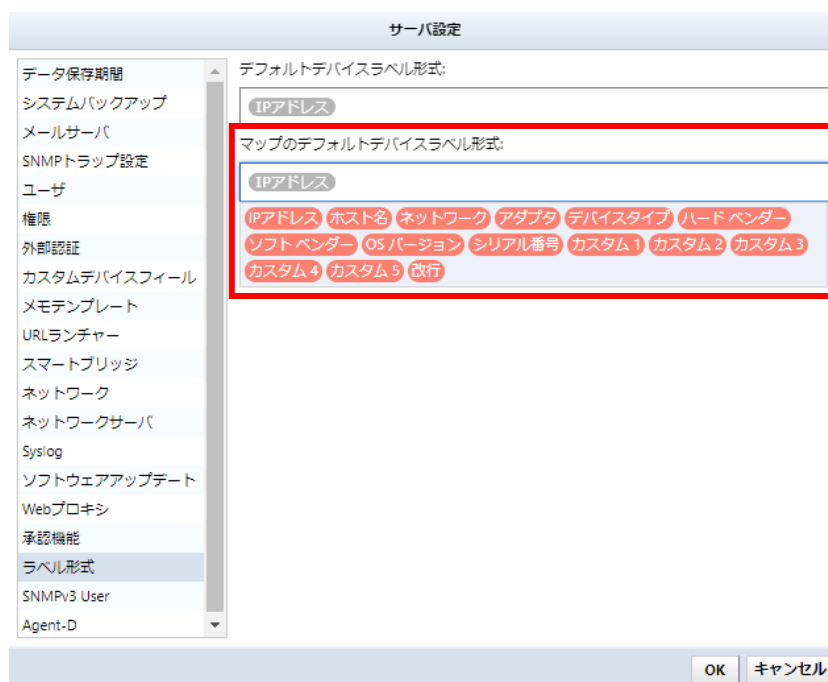
5.4.9 マップのデフォルトのデバイラベル形式を変更する

新しいマップを作成する時の、デフォルトのデバイラベル形式を指定することができます。変更後に作成するマップは、設定内容が自動的に反映されます。変更しても、作成済みのマップには反映されません。

1. グローバルメニューの[設定]をクリックします。



2. [ラベル形式]をクリックし、「マップのデフォルトデバイラベル形式」にラベル形式を設定します。



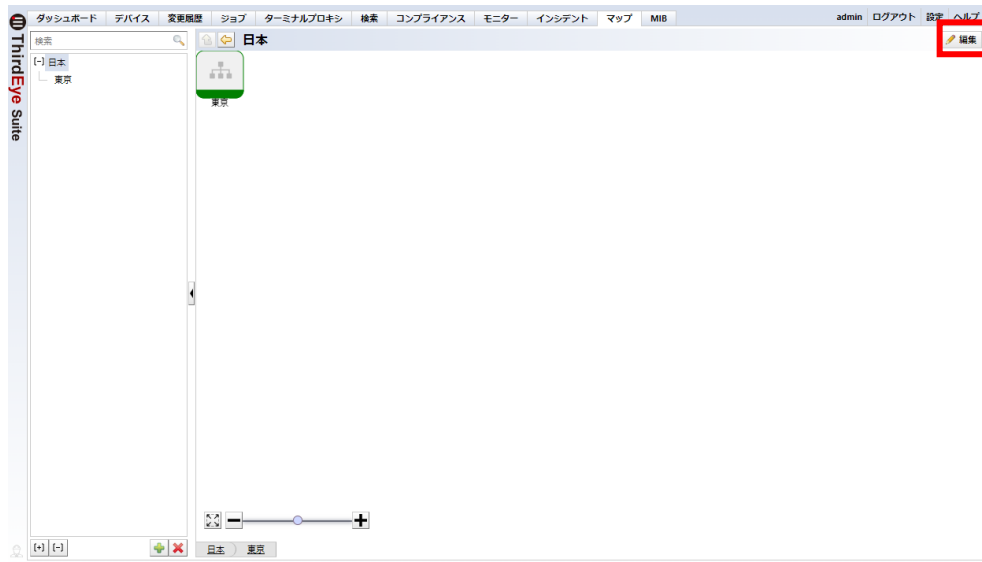
補足

グレーで表示される「IP アドレス」は、初期値であることを意味します。「デフォルトデバイラベル形式」は、マップに加えて、Live Ping 機能のラベル形式に使用されます。

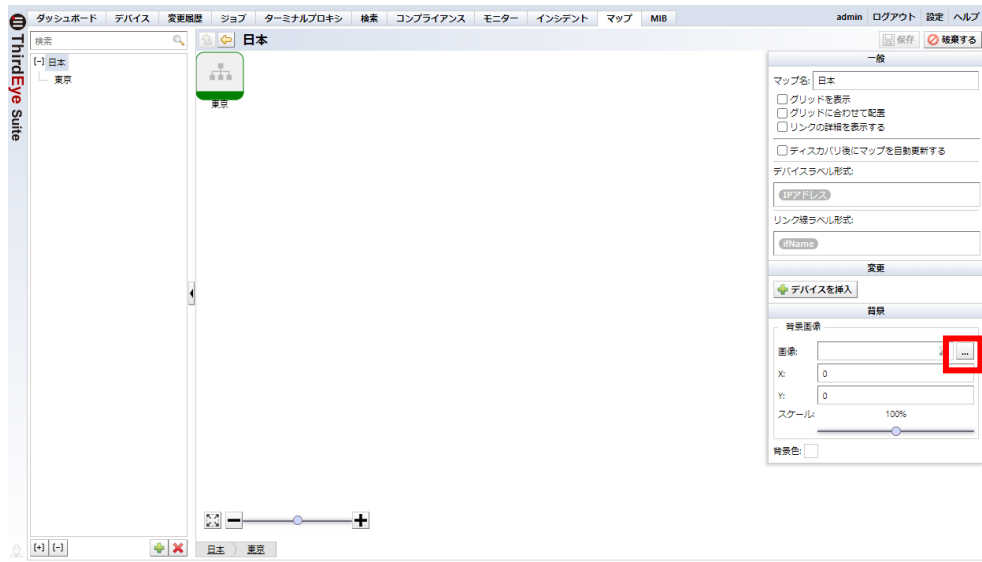
5.4.10 マップの背景画像を設定する

マップの[編集]メニューから、背景画像を設定できます。

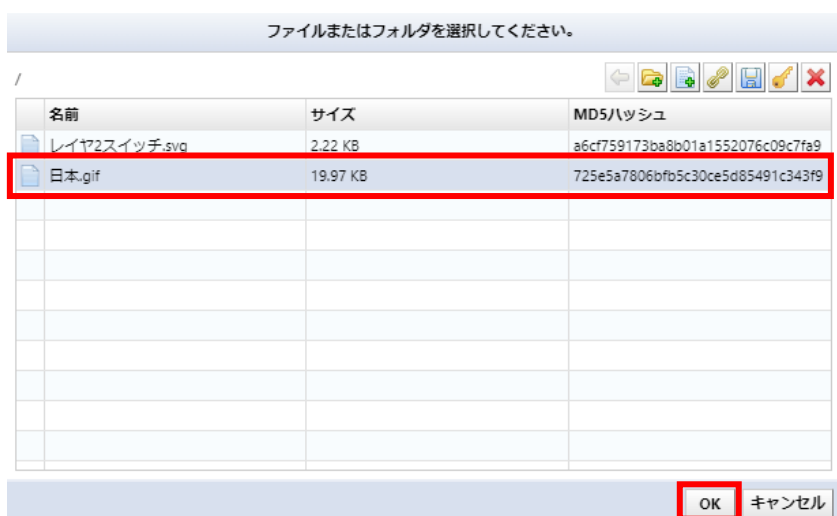
1. マップをダブルクリックで開き、[編集]をクリックします。



2. 画面右側の設定メニューの中から、背景セクションの[画像]欄の右にある[⋮]をクリックします。



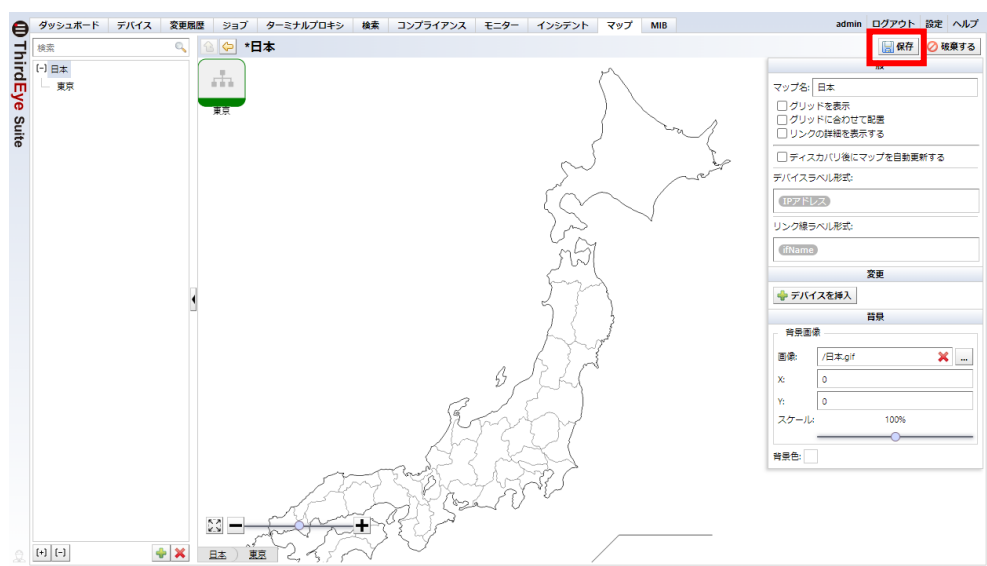
3. ファイルの選択画面が表示されます。背景画像に設定したいファイルを選択し、[OK]をクリックします。



補足

クライアントのファイルを ThirdEye サーバにアップロードすることができます。
[]をクリックすると、クライアント側のファイル選択ダイアログが表示されます。
アップロードするファイルを選択し、[開く]をクリックしてください。

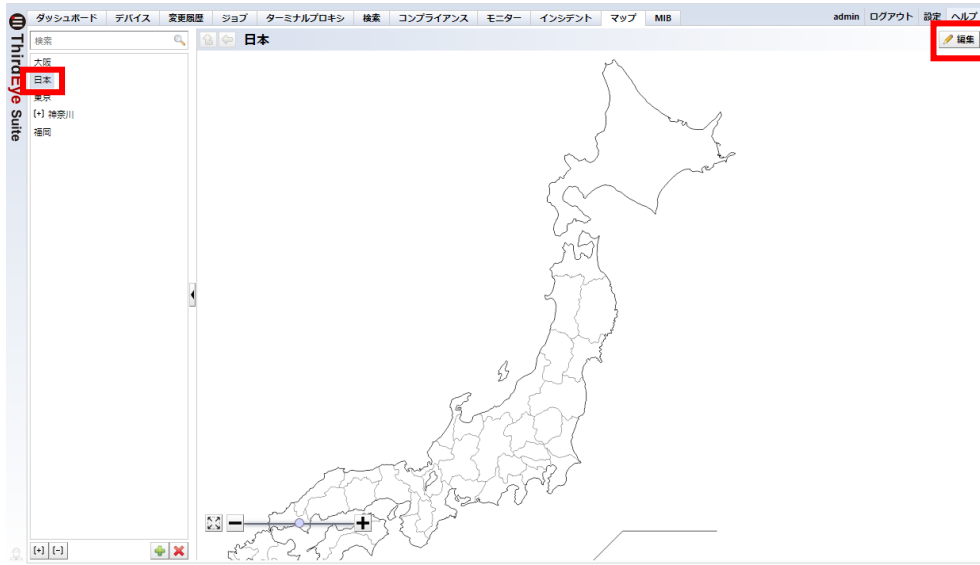
4. [保存]をクリックし、編集を完了します。



5.4.11 マップの階層構造を設定する

マップを階層構造で表示する場合は、階層構造の上位階層マップに下位階層マップを挿入することで構成できます。

1. 画面左側のマップ一覧から、上位階層になるマップをダブルクリックで開き、[編集]をクリックします。



2. マップ画面上で右クリックします。右クリックメニューから[マップを挿入]を選択します。



3. 下位階層として挿入するマップを選択し、[OK]をクリックします。

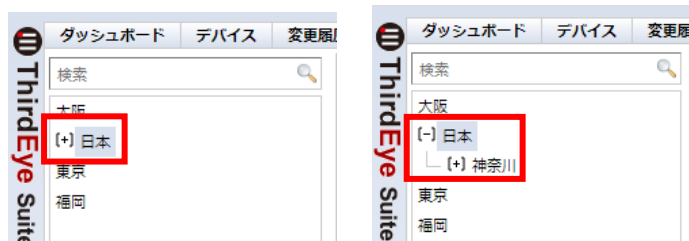


4. 下位階層のマップのオブジェクトが挿入されます。[保存]をクリックし、編集を完了します。



階層構造が作られると、画面左側のマップ一覧がツリー表示に変わります。

マップ名の左にある記号[+]/[-]をクリックすることで、マップの展開や折りたたみが可能です。



5.5 ダッシュボードを作成する


ダッシュボードは、画面にさまざまな項目を埋め込んで1つの監視画面を構成できるインターフェースです。埋め込まれている各項目を「ウィジェット」と呼びます。ユーザは、新しくダッシュボードを作成したり、ウィジェットを追加・並び替えたりできます。



5.5.1 ダッシュボードを追加する

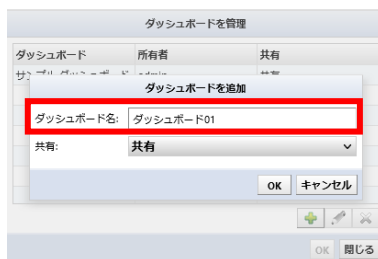
1. [ダッシュボード]タブの下の "ダッシュボード名" (下図では、"サンプル ダッシュボード" の部分)をクリックし、[ダッシュボードの管理]を選択します。



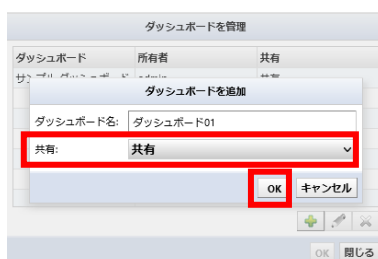
2. [ (追加)]をクリックします。



3. ダッシュボード名を入力します。



4. 共有でダッシュボードのタイプを選択し、[OK]をクリックします。



共有	説明
共有	他のユーザが閲覧できるダッシュボードを追加する。
プライベート	作成したユーザのみが閲覧できるダッシュボードを追加する。

5. ダッシュボードが一覧に追加されます。
6. [閉じる]をクリックし、[ダッシュボードを管理画面]を閉じます。

5.5.2 ダッシュボードを切り替える

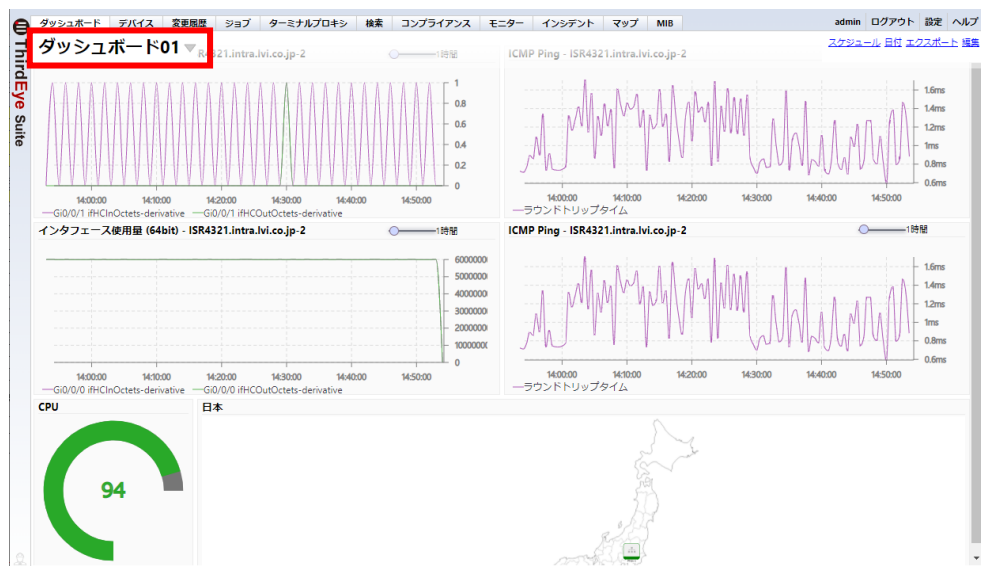
1. [ダッシュボード]タブの下の "ダッシュボード名" (下図では、" サンプル ダッシュボード" の部分) をクリックし、[ダッシュボードの管理]を選択します。



2. 切り替えたいダッシュボードを選択し、[OK]をクリックします。



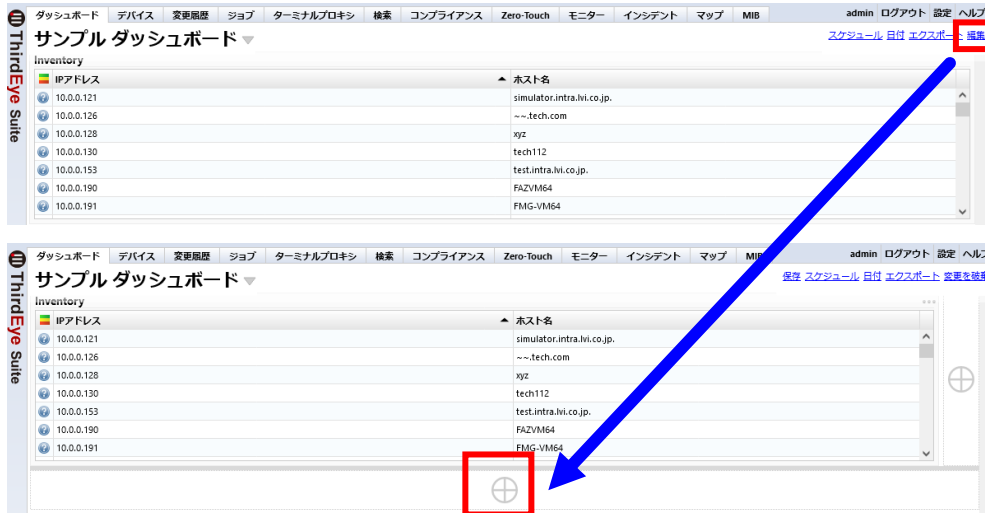
3. 選択したダッシュボード画面に切り替わります。




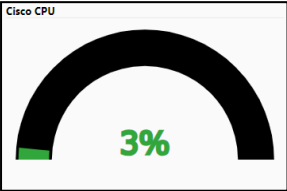
5.5.3 ウィジェットを追加する


ウィジェットは、ダッシュボードにコンテンツを表示させる構成要素です。ウィジェットをダッシュボードに追加しておく、見たい情報にすぐにアクセスすることができます。

ダッシュボードの画面右上にある[編集]から[⊕ (追加)]をクリックすると、ウィジェットを追加できます。



追加できるウィジェットの種類は、以下のとおりです。


ウィジェットの種類	説明
インベントリ	<p>インベントリを表示する。</p>  <p>※最大表示数は 100 件です。100 件を超える場合は、[デバイス]タブから確認できます。</p>
メーター	<p>メーターグラフを表示する。</p> <p>【デフォルト】  【温熱性】 </p>
折れ線グラフ	<p>折れ線グラフを表示する。</p> 

ウィジェットの種類	説明																																																																
<p>マップ</p>	<p>マップを表示する。</p> <div data-bbox="416 264 1035 707" style="border: 1px solid black; padding: 5px;"> <p>map01</p>  </div>																																																																
<p>違反</p>	<p>違反を表示する。</p> <div data-bbox="416 763 1398 927" style="border: 1px solid black; padding: 5px;"> <p>違反</p> <table border="1"> <thead> <tr> <th>IPアドレス</th> <th>ホスト名</th> <th>メッセージ</th> <th>Index</th> <th>回復日時</th> <th>発生回数</th> <th>作成日時</th> <th>更新日時</th> </tr> </thead> <tbody> <tr> <td>192.168.41.49</td> <td></td> <td>No response from node 192.168.41.49</td> <td>cleared</td> <td>21/12/21 11:50:52</td> <td>4</td> <td>21/12/21 11:47:22</td> <td>21/12/21 11:50:52</td> </tr> <tr> <td>192.168.41.49</td> <td></td> <td>No response from node 192.168.41.49</td> <td>cleared</td> <td>21/12/13 12:17:53</td> <td>6</td> <td>21/12/13 12:12:53</td> <td>21/12/13 12:17:53</td> </tr> <tr> <td>192.168.41.49</td> <td></td> <td>No response from node 192.168.41.49</td> <td>cleared</td> <td>21/12/13 12:10:53</td> <td>1</td> <td>21/12/13 12:08:23</td> <td>21/12/13 12:10:53</td> </tr> <tr> <td>192.168.41.46</td> <td></td> <td>Node 192.168.41.46 reported linkDown on interface 5</td> <td>cleared</td> <td>21/12/13 11:54:25</td> <td>1</td> <td>21/12/13 11:43:33</td> <td>21/12/13 11:54:25</td> </tr> <tr> <td>192.168.41.46</td> <td></td> <td>Node 192.168.41.46 reported linkDown on interface 6</td> <td>6</td> <td></td> <td>1</td> <td>21/12/13 11:44:03</td> <td>21/12/13 11:44:03</td> </tr> <tr> <td>192.168.41.46</td> <td></td> <td>Node 192.168.41.46 reported linkDown on interface 6</td> <td>cleared</td> <td>21/12/13 11:44:00</td> <td>6</td> <td>21/12/13 11:42:32</td> <td>21/12/13 11:44:00</td> </tr> <tr> <td>192.168.41.46</td> <td></td> <td>Node 192.168.41.46 reported linkDown on interface 2</td> <td>cleared</td> <td>21/12/13 11:41:18</td> <td>2</td> <td>21/12/13 11:04:49</td> <td>21/12/13 11:41:18</td> </tr> </tbody> </table> </div>	IPアドレス	ホスト名	メッセージ	Index	回復日時	発生回数	作成日時	更新日時	192.168.41.49		No response from node 192.168.41.49	cleared	21/12/21 11:50:52	4	21/12/21 11:47:22	21/12/21 11:50:52	192.168.41.49		No response from node 192.168.41.49	cleared	21/12/13 12:17:53	6	21/12/13 12:12:53	21/12/13 12:17:53	192.168.41.49		No response from node 192.168.41.49	cleared	21/12/13 12:10:53	1	21/12/13 12:08:23	21/12/13 12:10:53	192.168.41.46		Node 192.168.41.46 reported linkDown on interface 5	cleared	21/12/13 11:54:25	1	21/12/13 11:43:33	21/12/13 11:54:25	192.168.41.46		Node 192.168.41.46 reported linkDown on interface 6	6		1	21/12/13 11:44:03	21/12/13 11:44:03	192.168.41.46		Node 192.168.41.46 reported linkDown on interface 6	cleared	21/12/13 11:44:00	6	21/12/13 11:42:32	21/12/13 11:44:00	192.168.41.46		Node 192.168.41.46 reported linkDown on interface 2	cleared	21/12/13 11:41:18	2	21/12/13 11:04:49	21/12/13 11:41:18
IPアドレス	ホスト名	メッセージ	Index	回復日時	発生回数	作成日時	更新日時																																																										
192.168.41.49		No response from node 192.168.41.49	cleared	21/12/21 11:50:52	4	21/12/21 11:47:22	21/12/21 11:50:52																																																										
192.168.41.49		No response from node 192.168.41.49	cleared	21/12/13 12:17:53	6	21/12/13 12:12:53	21/12/13 12:17:53																																																										
192.168.41.49		No response from node 192.168.41.49	cleared	21/12/13 12:10:53	1	21/12/13 12:08:23	21/12/13 12:10:53																																																										
192.168.41.46		Node 192.168.41.46 reported linkDown on interface 5	cleared	21/12/13 11:54:25	1	21/12/13 11:43:33	21/12/13 11:54:25																																																										
192.168.41.46		Node 192.168.41.46 reported linkDown on interface 6	6		1	21/12/13 11:44:03	21/12/13 11:44:03																																																										
192.168.41.46		Node 192.168.41.46 reported linkDown on interface 6	cleared	21/12/13 11:44:00	6	21/12/13 11:42:32	21/12/13 11:44:00																																																										
192.168.41.46		Node 192.168.41.46 reported linkDown on interface 2	cleared	21/12/13 11:41:18	2	21/12/13 11:04:49	21/12/13 11:41:18																																																										
<p>テーブル</p>	<p>テーブルを表示する。</p> <div data-bbox="416 987 1398 1151" style="border: 1px solid black; padding: 5px;"> <p>テーブル</p> <table border="1"> <thead> <tr> <th>IPアドレス</th> <th>ホスト名</th> <th>indexName</th> <th>ifInOctets-derivative</th> <th>ifOutOctets-derivative</th> </tr> </thead> <tbody> <tr> <td>10.0.0.126</td> <td>test123</td> <td>GigabitEthernet1</td> <td>183120</td> <td>25314</td> </tr> <tr> <td>10.0.0.126</td> <td>test123</td> <td>GigabitEthernet2</td> <td>0</td> <td>0</td> </tr> <tr> <td>10.0.0.126</td> <td>test123</td> <td>GigabitEthernet3</td> <td>170426</td> <td>0</td> </tr> <tr> <td>10.0.0.126</td> <td>test123</td> <td>VirtualPortGroup0</td> <td>0</td> <td>0</td> </tr> <tr> <td>10.0.0.126</td> <td>test123</td> <td>Null0</td> <td>0</td> <td>0</td> </tr> </tbody> </table> </div>	IPアドレス	ホスト名	indexName	ifInOctets-derivative	ifOutOctets-derivative	10.0.0.126	test123	GigabitEthernet1	183120	25314	10.0.0.126	test123	GigabitEthernet2	0	0	10.0.0.126	test123	GigabitEthernet3	170426	0	10.0.0.126	test123	VirtualPortGroup0	0	0	10.0.0.126	test123	Null0	0	0																																		
IPアドレス	ホスト名	indexName	ifInOctets-derivative	ifOutOctets-derivative																																																													
10.0.0.126	test123	GigabitEthernet1	183120	25314																																																													
10.0.0.126	test123	GigabitEthernet2	0	0																																																													
10.0.0.126	test123	GigabitEthernet3	170426	0																																																													
10.0.0.126	test123	VirtualPortGroup0	0	0																																																													
10.0.0.126	test123	Null0	0	0																																																													
<p>文字列</p>	<p>文字列を表示する。</p> <div data-bbox="416 1211 526 1406" style="border: 1px solid black; padding: 5px;"> <p>文字列</p> <p>1.50</p> </div>																																																																

5.5.4 ダッシュボードを削除する

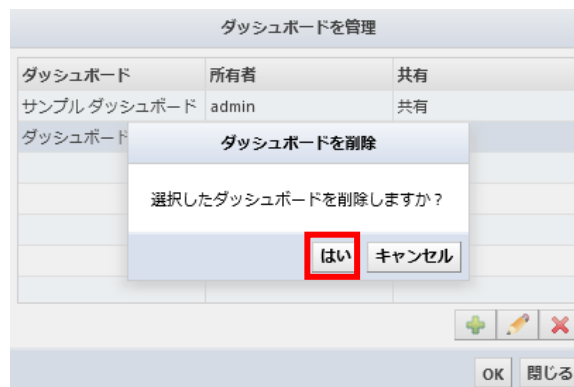
1. [ダッシュボード]タブの下の "ダッシュボード名" (下図では、" サンプル ダッシュボード" の部分) をクリックし、[ダッシュボードの管理]を選択します。



2. 削除したいダッシュボードを選択し、[ 削除] をクリックします。



3. 確認メッセージが表示されます。[はい] をクリックします。



5.5.5 ダッシュボードの編集メニュー

【通常時】



【編集時】



項目		説明
スケジュール	Enterprise Suite	・ダッシュボードの PDF レポートを E メール送信するようにスケジュールします。 ※スケジュールは、「インベントリ」、「折れ線グラフ」のウィジェットが対象です。
日付	Enterprise Suite	ダッシュボードの折れ線グラフの表示期間を一括で変更できます。 ※日付は、「折れ線グラフ」のウィジェットが対象です。
エクスポート	Enterprise Suite	表示しているダッシュボードの PDF レポートを作成します。 ※エクスポートは、「インベントリ」、「折れ線グラフ」のウィジェットが対象です。
編集	共通	ダッシュボードの編集モードに移行します。
保存	共通	ダッシュボードの変更内容を保存し、編集モードから戻ります。
変更を破棄	共通	ダッシュボードの編集モードを中止します。
⊕ (追加)	共通	ダッシュボードにウィジェットを追加します。

5.5.6 ウィジェットの編集メニュー

ダッシュボードの編集モード中は、ウィジェットを追加/編集/削除することができます。



項目	説明
...	ウィジェットタイトルの右側に表示される三点リーダー(「...」)のマーク。 「...」をクリックすると、ウィジェットの編集メニューが表示されます。
編集	ウィジェットを編集します。
削除	ウィジェットを削除します。

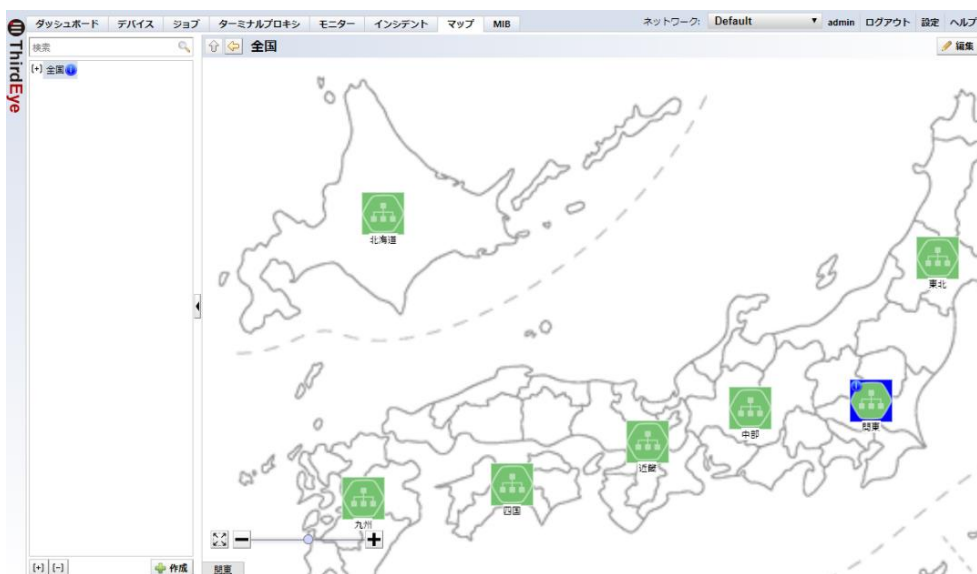
第6章 運用操作

ここでは、日々の運用で使用する操作を記載しています。

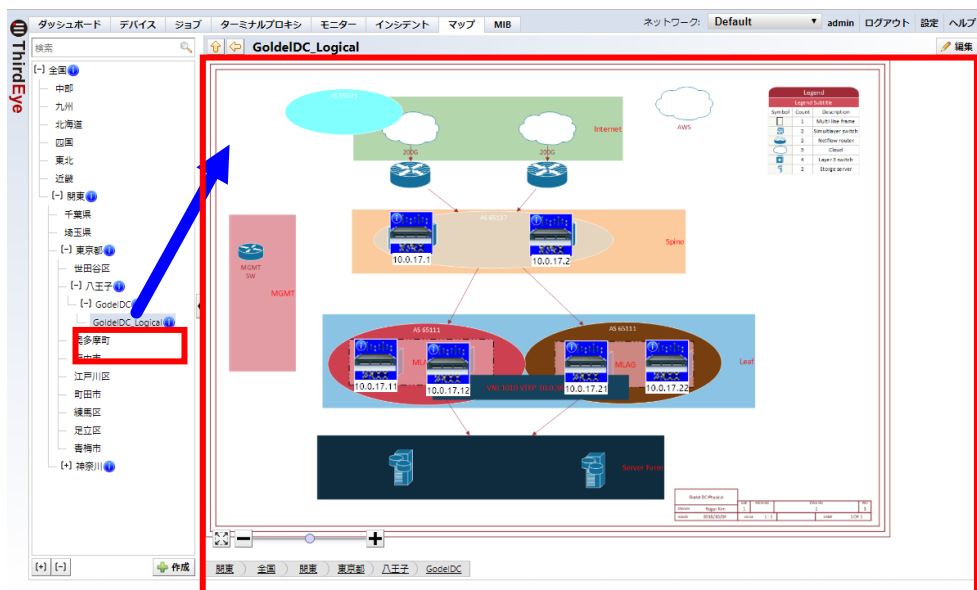
6.1 障害対応

6.1.1 障害が発生しているデバイスを確認する

デバイスの障害を検知すると、マップ上のオブジェクトの枠色がモニターに設定されている重大度に応じた色に変化し、重大度を表すステータスアイコンがオブジェクトの左上に表示されます。下位階層にあるオブジェクトでステータスが変わると、上位階層のマップオブジェクトに反映されます。この動作は、ダッシュボードにウィジェットとして登録しているマップにおいても同じです。



マップオブジェクトをダブルクリックすると下の階層に遷移します。また、マップツリーを使用することで目的のマップを表示することができます。



メモ:

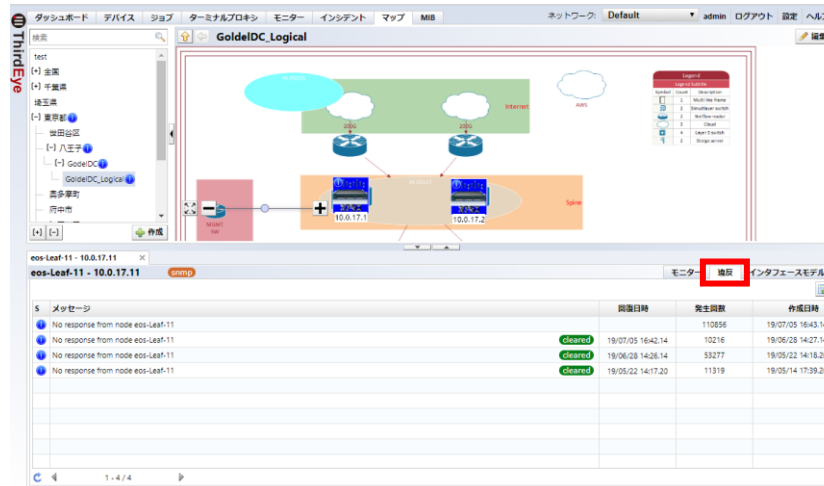
重大度別に表示されるステータスアイコンとオブジェクト枠色のイメージは、以下の通りです。

重大度	ステータスアイコン	オブジェクト (イメージ)
エマージェンシー (Emergency)		
アラート (Alert)		
クリティカル (Critical)		
エラー (Error)		
ワーニング (Warning)		
通知 (Notice)		
情報 (Info)		
デバッグ (Debug)		

※1つのデバイスで複数のインシデントが発生している場合、もっとも高い重大度が表示されます。

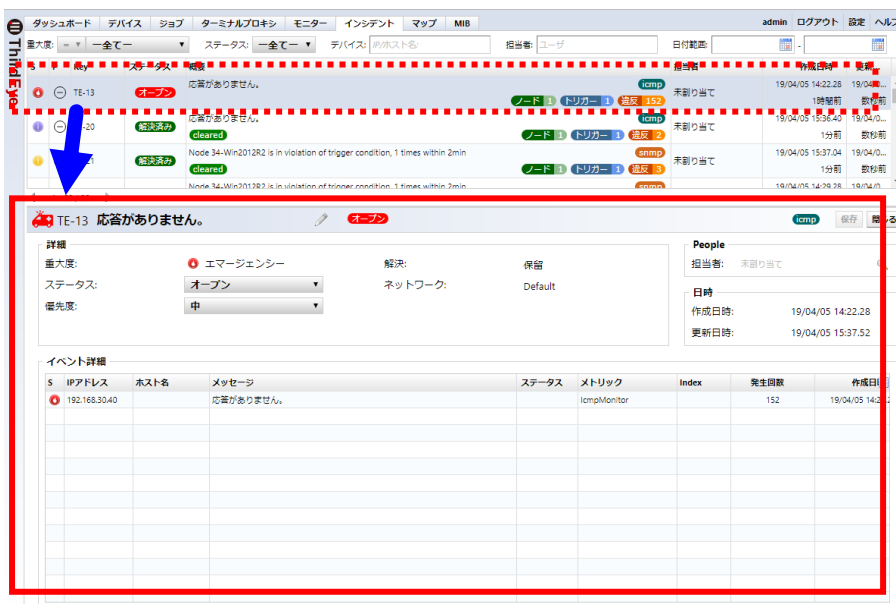
6.1.2 障害内容を確認する

障害が発生している箇所を特定したら、障害内容を確認します。障害が発生したデバイスをダブルクリックすると、デバイス詳細画面が表示されます。デバイス詳細画面の[違反]タブでは、そのデバイスでこれまで発生した障害を確認することができます。



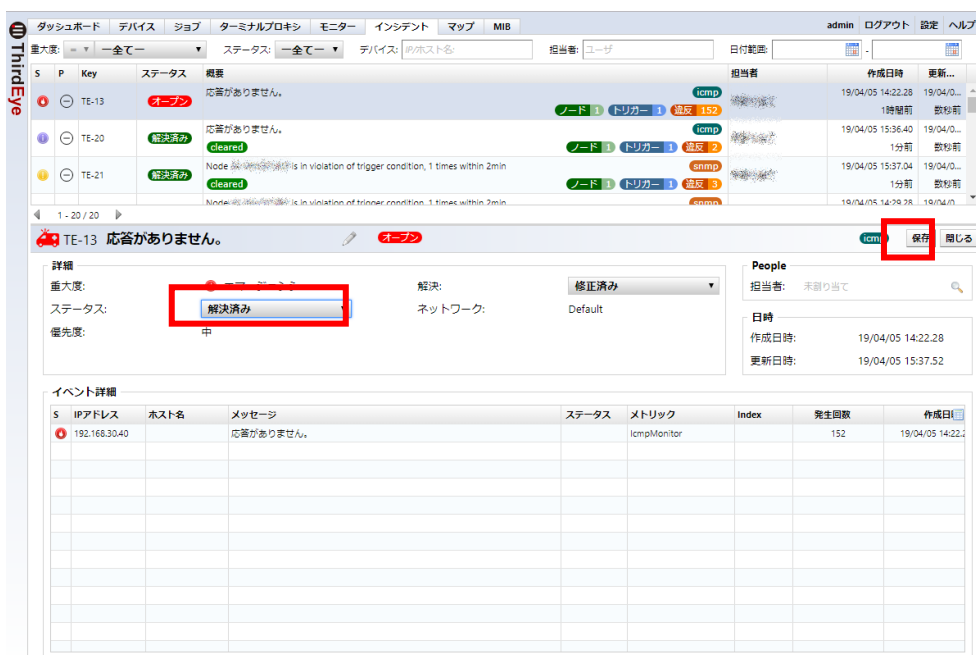
この障害の内容は、[インシデント]タブで確認することができます。[インシデント]タブでは、モニターに割り当てられたアラートポリシー設定に基づき最初に検知された違反イベントが、インシデントとして作成されます。各インシデントには、自動的に一意のインシデント番号が採番されます。ただし、同じアラートポリシーで構成された同じモニターによって検知された違反イベントは、インシデントを重複させないために、同じオープンインシデントに集約されます。同じオープンインシデントの集約は、インシデントのステータスが「解決済み」として保存されるまで継続されます。なお、ユーザはインシデントを削除することはできません。

1. 確認したいインシデント行をダブルクリックします。
2. 画面下側にインシデント詳細画面が表示されます。イベント詳細でイベント内容を確認します。



6.1.3 障害対応後、インシデントを「解決済み」にする

障害の対処が完了したら、インシデントをクローズします。[ステータス]のプルダウンメニューから[解決済み]を選択し、[保存]をクリックします。



ステータスの表示が「解決済み」に変更され、クローズ処理は完了します。[閉じる]をクリックし、インシデント詳細画面を閉じます。



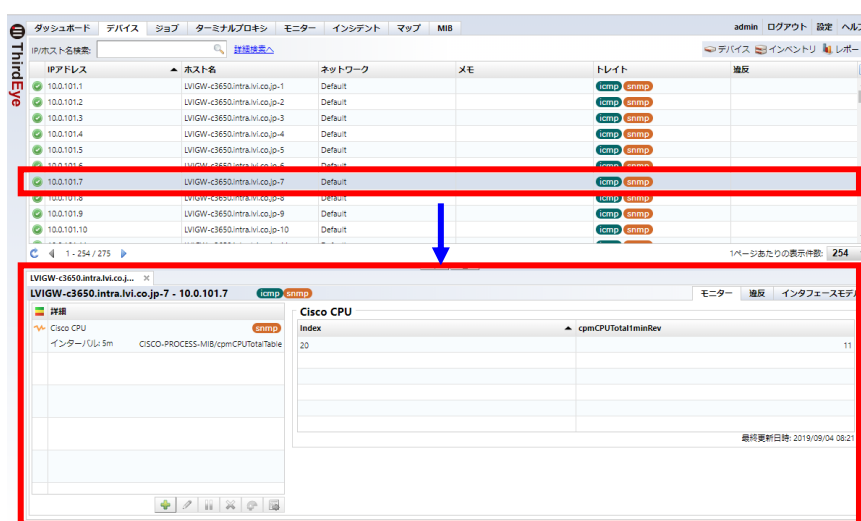
6.2 SNMP で収集したデータを確認する Enterprise Suite

SNMP モニターで収集したデータは、データベースに保存されます。過去のデータからグラフを作成したり、Excel ファイルにエクスポートすることができます。

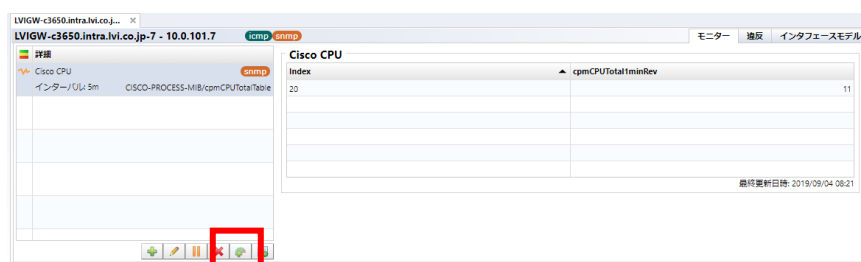
6.2.1 コンソールからグラフを表示する

SNMP で収集されたデータは、ダッシュボードにグラフウィジェットを追加することで確認できます。ダッシュボードの追加手順は、「[5.5.1 ダッシュボードを追加する](#)」で説明していますが、デバイス詳細画面からダッシュボードにグラフウィジェットを追加することもできます。

1. [デバイス]タブの監視対象機器一覧から、モニターを設定する機器をダブルクリックします。



2. モニター詳細から、データを確認するモニターを選択し、[ダッシュボードに追加]をクリックします。



3. ウィジェットを追加するダッシュボードを選択します。

ダッシュボードウィジェットを追加

ダッシュボード: Example Dashboard

メトリック	Index
<input type="checkbox"/> Example Dashboard	
<input type="checkbox"/> ダッシュボード01	
<input type="checkbox"/> ダッシュボード02	

フィルタ

追加 キャンセル

4. グラフに追加するメトリックとインデックスを選択し、[OK]をクリックします。

※取得するデータによっては、「Index」が表示されず、「メトリック」のみが表示される場合があります。

ダッシュボードウィジェットを追加

ダッシュボード: ダッシュボード01

メトリック	Index
<input checked="" type="checkbox"/> cpmCPUTotal1minRev	<input checked="" type="checkbox"/> 20

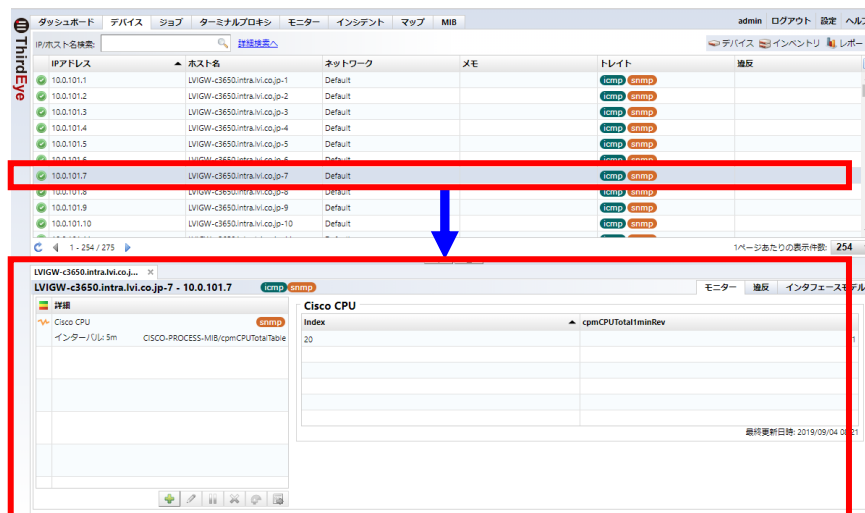
フィルタ


追加 キャンセル

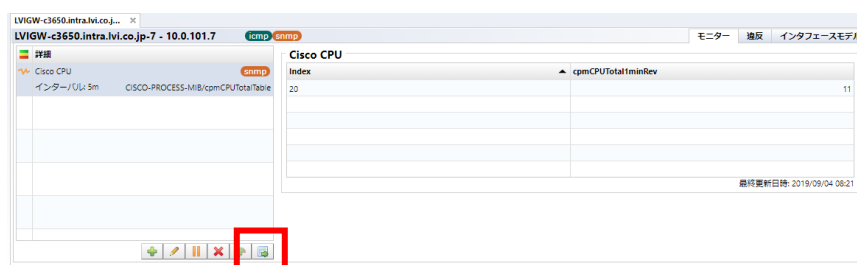
6.2.2 Excel ファイルへエクスポートする

SNMP で収集したデータは、Excel ファイルにエクスポートすることができます。

1. [デバイス]タブの監視対象機器一覧から、モニターを設定する機器をダブルクリックします。



2. モニター詳細から、データを確認するモニターを選択し、[ (エクスポート)] をクリックします。



3. ファイル名とデータエクスポート期間を入力し、[保存] をクリックします。

データエクスポート

ファイル名: LVIGW-c3650.intra.lvi.co.jp-7-Cisco-CPU.xlsx

開始日: 2019/09/03 8 10

終了日: 2019/09/04 8 32

保存 **キャンセル**

保存をクリック後、Excel ファイルがダウンロードされます。

6.2.3 ダッシュボードレポートを発行する

ウィジェットで表示されている「インベントリ」、「折れ線グラフ」を対象に、PDF ファイルにエクスポートすることができます。

ダッシュボードの画面右上にある[エクスポート]をクリックすると、エクスポートすることができます。



6.2.4 ダッシュボードレポートを定期的にメールで送信する

ダッシュボードレポートを定期的にメール送信することができます。

※メールを送信するには、まずメールサーバを設定する必要があります。メールサーバの設定については、「[7.13 メールサーバを設定する](#)」を参照してください。

1. [スケジュール]をクリックします。



2. [スケジュール]画面が表示されます。[+] (追加)をクリックします。



3. [Eメール スケジュール]画面が表示されます。各項目を入力/選択します。

項目	説明
To/Cc	メール送信先アドレスを入力します。
範囲指定	レポート表示期間の範囲を指定します。 <ul style="list-style-type: none"> 24 時間以内 週間以内 30 日以内 昨日 (00:00:00～23:59:59) 先週 (月曜日～日曜日) 先月 (月初～月末) 日付範囲 (ユーザが任意の期間を指定)
スケジュール	レポートを発行するスケジュールを指定する。
時間帯	レポートを発行するタイムゾーンを指定します。
フィルタ	実行時間のフィルタ設定を指定します。 ※フィルタの設定は、「ジョブ管理」で設定をします。
保存	設定を保存します。
キャンセル	設定を破棄し、前の画面に戻ります。

4. [保存]をクリックします。

6.3 デバイスのコンフィギュレーションを取得する Enterprise Suite

ThirdEye では、Net LineDancer(コンフィグ管理ツール)の一部の機能を使用することができます。デバイスのコンフィギュレーションを取得することを「(コンフィグ)バックアップ」と呼びます。コンフィグバックアップは、ThirdEye がデバイスに SSH または Telnet で接続し、show コマンドや tftp コマンドなどを使用してコンフィグを取得します。

6.3.1 使用する前の確認事項

コンフィグをバックアップするには、以下の要件が満たされていることを確認してください。

- デバイスにログインするためのログインユーザ名やパスワードが設定されていること。
「5.1 クレデンシャルを設定する」を参照して、クレデンシャルが設定済みであることを確認してください。
- コンフィグバックアップが可能な機種であること。
コンフィグバックアップの対応機種については、下記の資料を参照してください。
https://www.lvi.co.jp/NetLD/pdf/adapter_list.pdf
- NCM 機能が有効であること。
コンフィグバックアップの対象は、トレイトカラムに「ncm」が表示されているデバイスです。



IPアドレス	ホスト名	アダプタ	ハードベンダー	モデル	デバイスタ...	シリアル番号	トレイト
10.0.0.250	cisco1921aboo.intra.lvi.co.jp	Cisco IOS					telnet ssh nmap ncm

6.3.2 バックアップを実行する

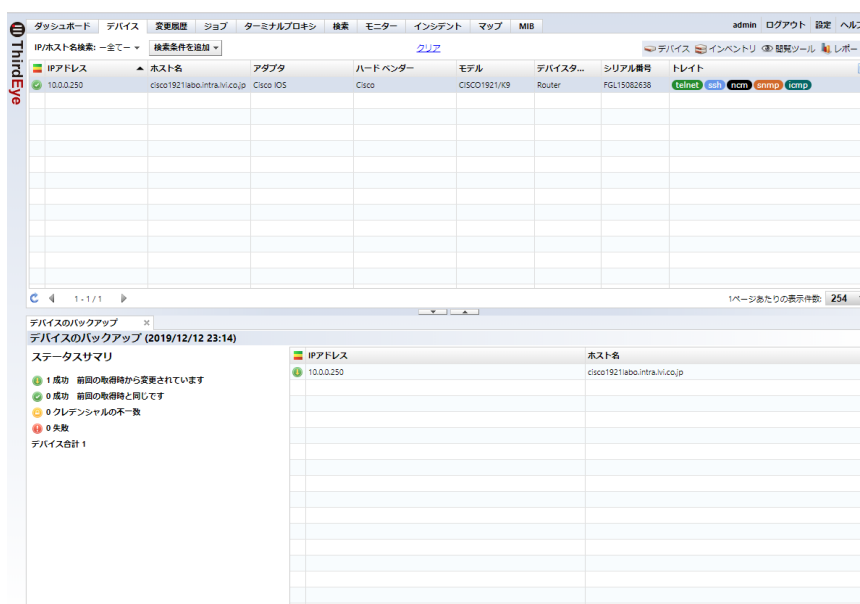
バックアップを実行するには、対象のデバイスを選択し、デバイスメニューから[バックアップ]をクリックします。
(デバイスが選択されていない場合は、NCM 機能が有効なデバイスを対象に実行します)



IPアドレス	ホスト名	アダプタ	ハードベンダー	モデル	デバイスタ...	シリアル番号	トレイト
10.0.0.250	cisco1921aboo.intra.lvi.co.jp	Cisco IOS					telnet ssh nmap ncm

- バックアップ
- デバイスプロパティの更新
- スワイチングの管理
- スワイチングの表示
- 比較
- ジョブ履歴を表示
- モニター
- モニターセット
- nmap
- 構築
- デバイスプロパティの編集
- タグ付け
- タグ削除
- Enable ncm trait
- Disable ncm trait

バックアップを実行すると、画面下に実行結果が表示されます。










バックアップ実行時のステータスサマリー一覧は以下のとおりです。

アイコン	説明
	バックアップ成功、変更あり。 前回バックアップしたものとデバイス上のコンフィギュレーションとの間に差分が検知された場合に表示されます。初めてのバックアップの際にも表示されます。
	バックアップ成功、変更なし。 デバイス上のコンフィグデータが前回バックアップした内容と同じ場合に表示されます。
	クレデンシャルの不一致のため、バックアップ失敗。 登録されているクレデンシャルが誤っています。右に表示される結果をクリックすると、バックアップで使用したクレデンシャルが表示されます。インベントリ→クレデンシャルの設定を確認してください。
	バックアップ失敗。 コンフィギュレーションが取得できませんでした。アイコンをダブルクリックすると、詳細が表示されます。

6.3.3 バックアップ後のステータスについて

バックアップ後、デバイスビューの左側に表示される、ステータスアイコンが変化します。バックアップステータスで用されるアイコンは以下の通りです。

アイコン	ステータス	状態説明
	バックアップ完了	コンフィギュレーション取得が正常に完了しています。
	コンフィギュレーション不一致	デバイスの running-config と startup-config に差分があります。アイコンをダブルクリックすると、比較結果が表示されます。
	クレデンシャルの不一致	登録されているクレデンシャルではログインができずバックアップが失敗しています。クレデンシャル設定を確認してください。
	バックアップ失敗	何らかの原因でバックアップが失敗しています。
	バックアップ未実行	バックアップが実行されていません。
	ワーニング	このデバイスは、障害度がワーニングに設定されたコンプライアンスポリシーに違反しています。
	エラー	このデバイスは、障害度がエラーに設定されたコンプライアンスポリシーに違反しています。

ステータスカラムに表示されるアイコンは、モニター設定のトリガーで設定した重大度とバックアップステータスの中で優先度が高いアイコンが表示されます。

ステータス	重大度ステータス	バックアップステータス
エマージェンシー		
アラート		
バックアップ失敗		
クリティカル		
クレデンシャル不一致		
エラー		
コンフィグ不一致		
ワーニング		
通知		
情報		
デバッグ		
バックアップ未実行		
通常		

高
↑
優先度
↓
低

6.3.4 取得したコンフィグを確認する

取得したコンフィグは、デバイス詳細画面から確認できます。

The screenshot shows the Cisco Prime Network Manager interface. The top navigation bar includes 'ダッシュボード', 'デバイス', '変更履歴', 'ジョブ', 'ターミナルプロキシ', '検索', 'モニター', 'インシデント', 'マップ', 'MIB', 'admin', 'ログアウト', '設定', and 'ヘルプ'. The main content area displays details for a device with IP address 10.0.0.250, host name 'cisco1921labo.intra.lvi.co.jp', and model 'CISCO1921/K9'. A table of configuration files is highlighted with a red box:


変更検知日時	コンフィギュレーション	変更日時	サイズ	ユーザー
2019/12/12 23:14	/running-config	2019/12/12 23:14	4167	n/a
	/startup-config	2019/12/12 23:14	4167	n/a
	/vlan.dat	2019/12/12 23:14	916	n/a

コンフィグをダブルクリックすることで内容を確認することができます。

The screenshot shows the configuration content for the selected device, displayed in a terminal window. The configuration is as follows:

```
2019/12/12 23:14
1 version 15.4
2 service timestamps debug datetime msec
3 service timestamps log datetime msec
4 no service password-encryption
5
6 hostname Cisco1921
7
8 boot-start-marker
9 boot-end-marker
10
11
12 enable secret 5 $1*x1Th4bcnrSP5pJxmVc0hFF92M/
13
14 aaa new-model
15
16
17
18
19
20
21
22 aaa session-id common
23
24
25
26
```


6.3.5 コンフィグの比較

2つのコンフィグを選択して[ (比較ボタン)]をクリックすると、コンフィグを比較できます。

※「Ctrl」キーを押しながら選択すると、複数選択ができます。

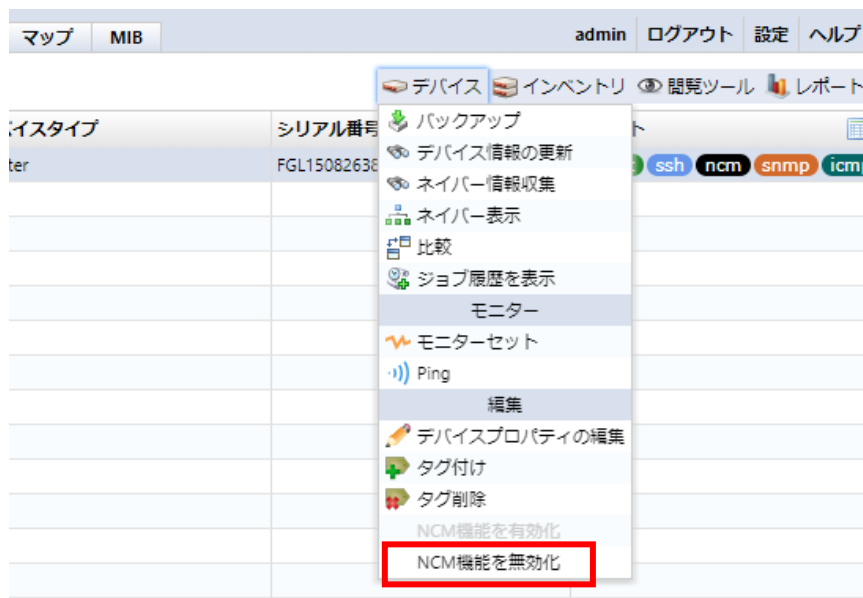


コンフィグを比較すると、コンフィギュレーションの差分が色付きで強調表示されます。差分の種類ごとに異なる色で表示するようになっており、赤色は削除された部分、黄色は変更された部分、緑色は追加された部分を表します。

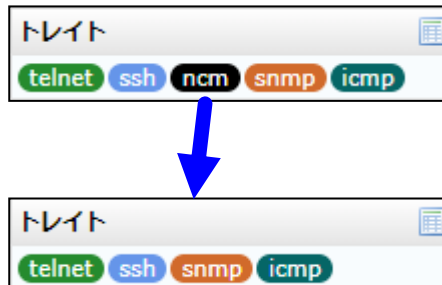


6.3.6 コンフィグバックアップを無効にする

コンフィグバックアップに対応した機種でも、コンフィグを取得しない場合には NCM 機能を無効にすることでバックアップ対象から外すことができます。NCM 機能を無効にするには、インベントリで対象デバイスを選択し、デバイスメニュー内の [NCM 機能を無効化] をクリックします。



NCM 機能を無効にすると、トレイトに ncm が表示されなくなります。



NCM 機能を有効にするには、対象デバイスを選択し、デバイスメニュー内の [NCM 機能を有効化] をクリックします。

6.4 デバイスに SSH/Telnet 接続をする

デバイス一覧やマップから監視対象機器に対して、SSH/Telnet 接続することができます。この機能を「ターミナルプロキシ」と呼びます。ターミナルプロキシを使用すると、ターミナル上で実行されたコマンドや出力結果が自動的に保存されます。

6.4.1 使用する前の準備

ターミナルプロキシを使用するためには、以下の準備が必要です。

- 操作する端末に Tera Term をインストール
ターミナルプロキシは、操作している PC の Tera Term を呼び出します。
- ブラウザインテグレーションのインストール
ThirdEye に接続しているブラウザと Tera Term を紐付ける必要があります。

この準備は、ターミナルプロキシを初めて起動したときに表示される画面から行うことができます。以下に、[Step 2] の「ブラウザインテグレーション」のインストール手順を記載します。Tera Term のインストールについては、Tera Term のマニュアルをご確認ください。

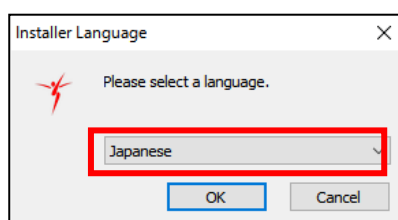
1. [インストールインテグレーション]をクリックし、ttinstall.exe をダウンロードします。



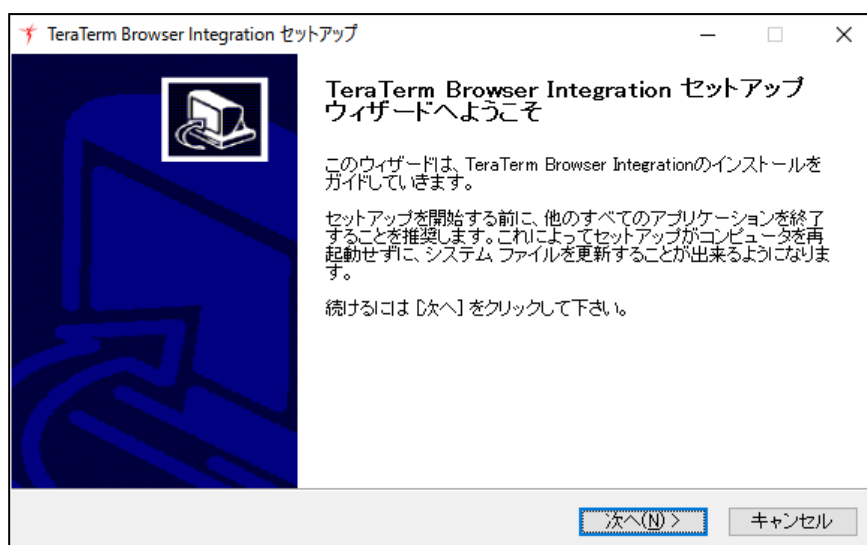
2. ダウンロードした ttinstall.exe を実行します。



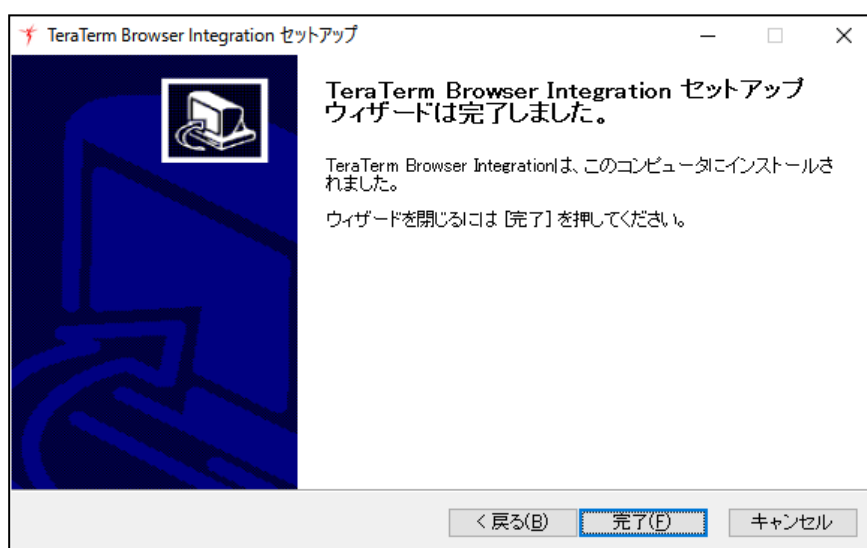
3. 表示言語を選択し、[OK]をクリックします。



4. [次へ]をクリックします。



5. [完了]をクリックします。



以上で準備が完了します。

補足

[Step 2]の「ブラウザインテグレーション」については、ブラウザのキャッシュをクリアしたり ThirdEye をアップデートしたりすると、再設定が必要になる場合があります。

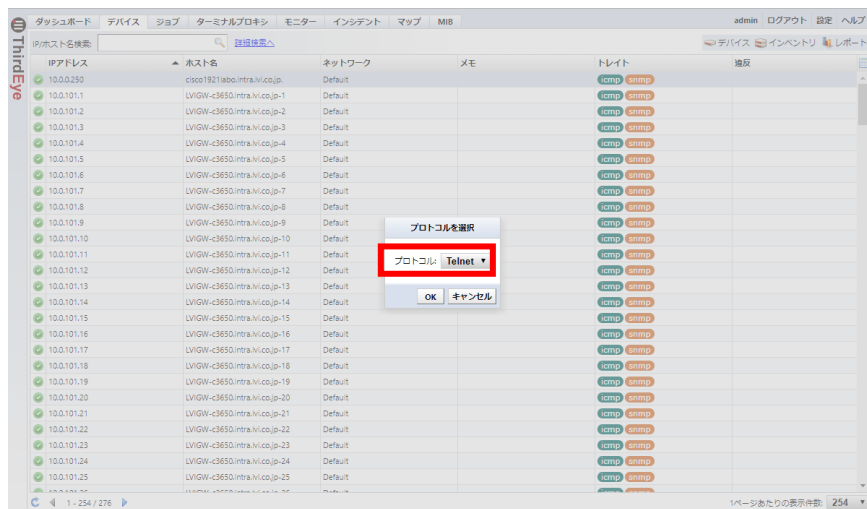
6.4.2 ターミナルを起動する

1. [デバイス]タブを選択します。
2. ターミナル接続対象のデバイスを右クリックし、[ターミナルを起動]を選択します。



3. [プロトコルを選択]画面が表示されます。接続時のプロトコルを選択し、[OK]をクリックします。

※すでにコンフィグバックアップが完了しているデバイスには表示されません。



4. ターミナルソフト「Tera Term」の起動が完了し、デバイスのログイン画面が表示されます。

```
192.168.40.222 - netLD VT
File Edit Setup Control Window Help
Welcome to Net LineDancer - Sep 4, 2019, 12:48:43 AM UTC
Resolving device 10.0.0.250...
Connecting to device 10.0.0.250...

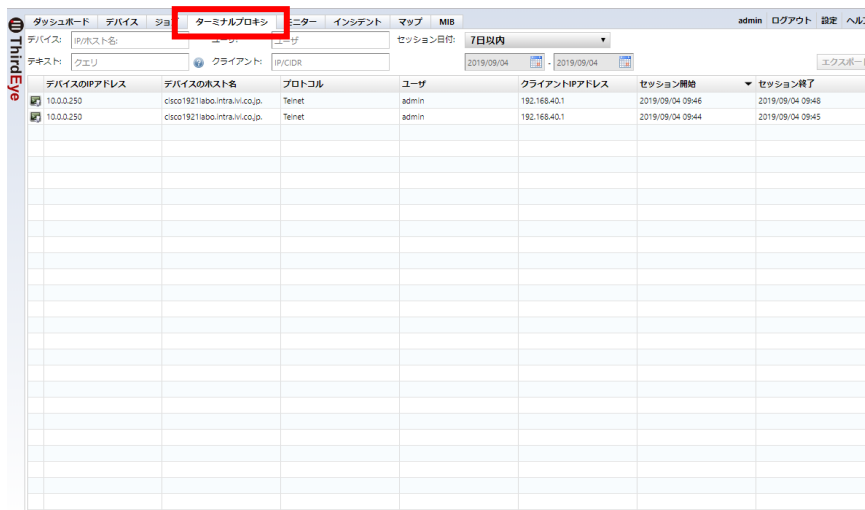
User Access Verification
Username: lvi
Password:
Cisco1921>en
Password:
Cisco1921#show ver
Cisco1921#show version
Cisco IOS Software, C1900 Software (C1900-UNIVERSALK9-M), Version 15.4(3)M5, RE
LEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1988-2016 by Cisco Systems, Inc.
Compiled Tue 09-Feb-16 02:36 by prod_rel_team

ROM: System Bootstrap, Version 15.0(1r)M9, RELEASE SOFTWARE (fc1)

Cisco1921 uptime is 5 weeks, 6 days, 22 hours, 40 minutes
System returned to ROM by reload at 02:25:09 UTC Wed Jul 24 2019
System image file is "usbflash0:c1900-universalk9-mz.SPA.154-3.M5.bin"
Last reload type: Normal Reload
```

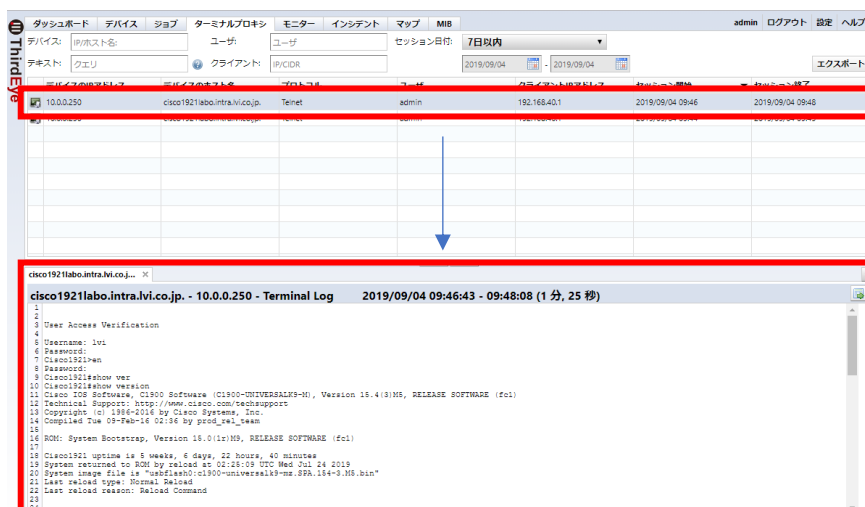
6.4.3 操作ログを確認する Enterprise Suite


1. [ターミナルプロキシ]タブを選択します。



2. 一覧から閲覧したいログをダブルクリックします。

※接続中のセッションログを確認することはできません。



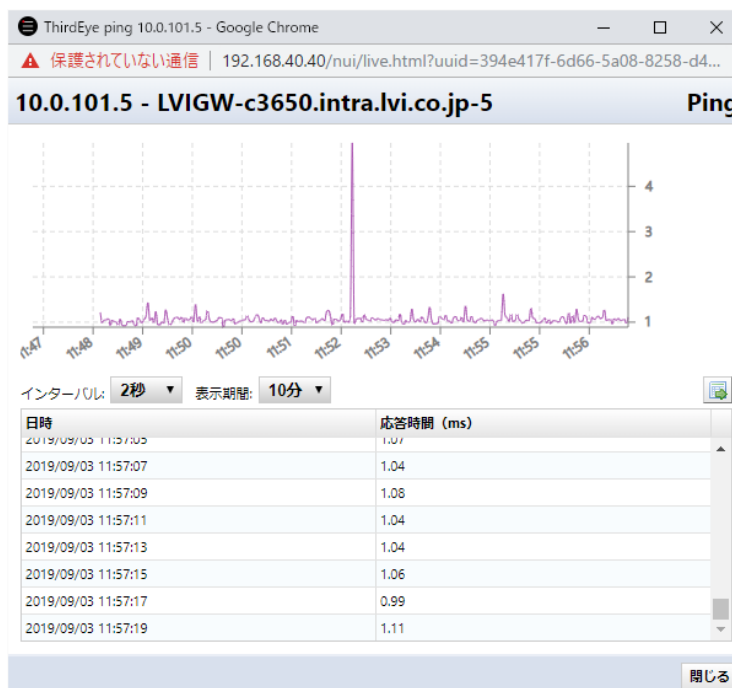
ログ画面右上にある  (エクスポート) をクリックすると、セッションデータをテキストファイルとして保存できます。なお、ファイル名は「ThirdEye-termlogs YYYY-MM-DD.zip」となり、ZIP ファイル形式でまとめられます。「YYYY-MM-DD」は保存した年月日を表します。


6.5 リアルタイムで Ping を実行する

デバイス一覧やマップから監視対象機器に対して、右クリックメニューから Ping を実行することができます。送信間隔は、起動時は2秒間隔ですが、Ping を実行後に表示される画面から変更することができます。



Ping をクリックすると、以下の画面が表示され Ping の結果が表示されます。

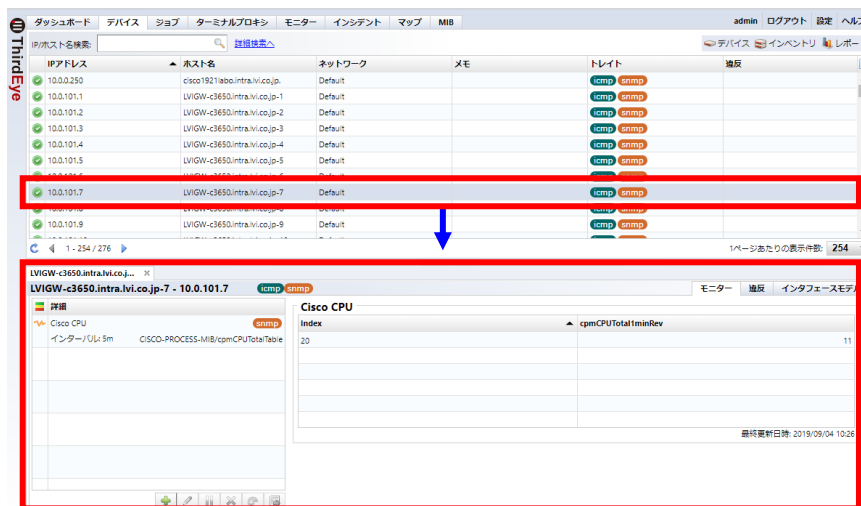


画面右にある[] (エクスポート) をクリックすると、Ping の結果を CSV ファイルにエクスポートできます。

6.6 デバイスのインタフェースの Up/Down 状態を確認する

デバイス詳細画面では、デバイスのインタフェースの状態を確認することができます。この機能を使用するためには、監視対象機器と SNMP 通信ができる必要があります。

1. [デバイス]タブの監視対象機器一覧から、モニターを設定する機器をダブルクリックします。



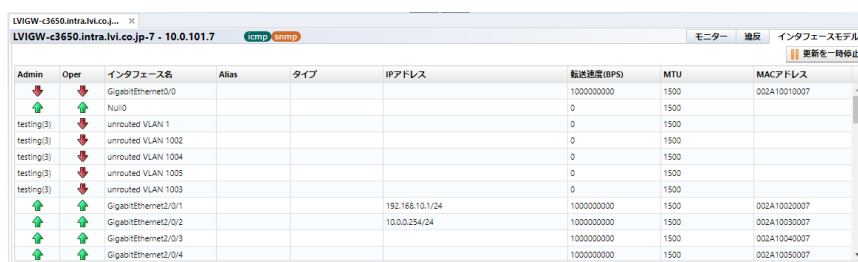
2. デバイス詳細画面内の[インタフェース]タブをクリックします。



3. [自動更新]をクリックします。



4. 監視対象機器のインタフェースの情報を定期的に取得し、現在の状態を確認することができます。



Admin	Oper	インタフェース名	Alias	タイプ	IPアドレス	転送速度(BPS)	MTU	MACアドレス
	↓	GigabitEthernet0/0				1000000000	1500	002A10010007
	↑	Null0				0	1500	
testing(3)	↓	unrouted VLAN 1				0	1500	
testing(3)	↓	unrouted VLAN 1002				0	1500	
testing(3)	↓	unrouted VLAN 1004				0	1500	
testing(3)	↓	unrouted VLAN 1005				0	1500	
testing(3)	↓	unrouted VLAN 1003				0	1500	
	↑	GigabitEthernet2/0/1			192.168.10.1/24	1000000000	1500	002A10020007
	↑	GigabitEthernet2/0/2			10.0.0.254/24	1000000000	1500	002A10030007
	↑	GigabitEthernet2/0/3				1000000000	1500	002A10040007
	↑	GigabitEthernet2/0/4				1000000000	1500	002A10050007

停止するには、デバイス詳細画面を閉じるか、[更新を一時停止]をクリックします。

6.7 登録されている機器からの SNMP トラップを確認する

ThirdEye にデバイスとして登録されている監視対象機器から送信された SNMP トラップは、[モニター]タブ→[SNMP トラップ]タブから確認することができます。また、検索機能を使用することで、特定のデバイスから送信された SNMP トラップのみを表示することができます。

日時	IPアドレス	ホスト名	OID	メッセージ
19/09/03 12:08:59	10.0.101.14	LVIGW-c3650.intra.vi.co.jp-14	linkDown	sysUpTimeInstance: 45 days, 22:38:41.42, 1.3.6.1.2.1.2.2.1.1.8: 8, 1...
19/09/03 12:08:59	10.0.101.71	LVIGW-c3650.intra.vi.co.jp-71	linkDown	sysUpTimeInstance: 45 days, 22:38:40.96, 1.3.6.1.2.1.2.2.1.1.8: 8, 1...
19/09/03 12:08:59	10.0.101.17	LVIGW-c3650.intra.vi.co.jp-17	linkDown	sysUpTimeInstance: 45 days, 22:38:42.48, 1.3.6.1.2.1.2.2.1.1.8: 8, 1...
19/09/03 12:08:59	10.0.101.22	LVIGW-c3650.intra.vi.co.jp-22	linkDown	sysUpTimeInstance: 45 days, 22:38:41.34, 1.3.6.1.2.1.2.2.1.1.8: 8, 1...
19/09/03 12:08:59	10.0.101.30	LVIGW-c3650.intra.vi.co.jp-30	linkDown	sysUpTimeInstance: 45 days, 22:38:41.24, 1.3.6.1.2.1.2.2.1.1.8: 8, 1...
19/09/03 12:08:59	10.0.101.79	LVIGW-c3650.intra.vi.co.jp-79	linkDown	sysUpTimeInstance: 45 days, 22:38:40.89, 1.3.6.1.2.1.2.2.1.1.8: 8, 1...
19/09/03 12:08:59	10.0.101.25	LVIGW-c3650.intra.vi.co.jp-25	linkDown	sysUpTimeInstance: 45 days, 22:38:42.43, 1.3.6.1.2.1.2.2.1.1.8: 8, 1...
19/09/03 12:08:59	10.0.101.87	LVIGW-c3650.intra.vi.co.jp-87	linkDown	sysUpTimeInstance: 45 days, 22:38:40.82, 1.3.6.1.2.1.2.2.1.1.8: 8, 1...
19/09/03 12:08:59	10.0.101.38	LVIGW-c3650.intra.vi.co.jp-38	linkDown	sysUpTimeInstance: 45 days, 22:38:41.12, 1.3.6.1.2.1.2.2.1.1.8: 8, 1...
19/09/03 12:08:59	10.0.101.33	LVIGW-c3650.intra.vi.co.jp-33	linkDown	sysUpTimeInstance: 45 days, 22:38:42.38, 1.3.6.1.2.1.2.2.1.1.8: 8, 1...
19/09/03 12:08:59	10.0.101.46	LVIGW-c3650.intra.vi.co.jp-46	linkDown	sysUpTimeInstance: 45 days, 22:38:41.03, 1.3.6.1.2.1.2.2.1.1.8: 8, 1...
19/09/03 12:08:59	10.0.101.95	LVIGW-c3650.intra.vi.co.jp-95	linkDown	sysUpTimeInstance: 45 days, 22:38:40.74, 1.3.6.1.2.1.2.2.1.1.8: 8, 1...
19/09/03 12:08:59	10.0.101.54	LVIGW-c3650.intra.vi.co.jp-54	linkDown	sysUpTimeInstance: 45 days, 22:38:40.92, 1.3.6.1.2.1.2.2.1.1.8: 8, 1...
19/09/03 12:08:59	10.0.101.62	LVIGW-c3650.intra.vi.co.jp-62	linkDown	sysUpTimeInstance: 45 days, 22:38:40.81, 1.3.6.1.2.1.2.2.1.1.8: 8, 1...
19/09/03 12:08:59	10.0.101.103	LVIGW-c3650.intra.vi.co.jp-103	linkDown	sysUpTimeInstance: 45 days, 22:38:40.69, 1.3.6.1.2.1.2.2.1.1.8: 8, 1...
19/09/03 12:08:59	10.0.101.41	LVIGW-c3650.intra.vi.co.jp-41	linkDown	sysUpTimeInstance: 45 days, 22:38:42.33, 1.3.6.1.2.1.2.2.1.1.8: 8, 1...
19/09/03 12:08:59	10.0.101.70	LVIGW-c3650.intra.vi.co.jp-70	linkDown	sysUpTimeInstance: 45 days, 22:38:40.70, 1.3.6.1.2.1.2.2.1.1.8: 8, 1...
19/09/03 12:08:59	10.0.101.111	LVIGW-c3650.intra.vi.co.jp-111	linkDown	sysUpTimeInstance: 45 days, 22:38:40.61, 1.3.6.1.2.1.2.2.1.1.8: 8, 1...
19/09/03 12:08:59	10.0.101.78	LVIGW-c3650.intra.vi.co.jp-78	linkDown	sysUpTimeInstance: 45 days, 22:38:40.56, 1.3.6.1.2.1.2.2.1.1.8: 8, 1...
19/09/03 12:08:59	10.0.101.86	LVIGW-c3650.intra.vi.co.jp-86	linkDown	sysUpTimeInstance: 45 days, 22:38:40.39, 1.3.6.1.2.1.2.2.1.1.8: 8, 1...
19/09/03 12:08:59	10.0.101.49	LVIGW-c3650.intra.vi.co.jp-49	linkDown	sysUpTimeInstance: 45 days, 22:38:42.27, 1.3.6.1.2.1.2.2.1.1.8: 8, 1...
19/09/03 12:08:59	10.0.101.13	LVIGW-c3650.intra.vi.co.jp-13	linkDown	sysUpTimeInstance: 45 days, 22:38:41.43, 1.3.6.1.2.1.2.2.1.1.8: 8, 1...
19/09/03 12:08:59	10.0.101.119	LVIGW-c3650.intra.vi.co.jp-119	linkDown	sysUpTimeInstance: 45 days, 22:38:40.52, 1.3.6.1.2.1.2.2.1.1.8: 8, 1...
19/09/03 12:08:59	10.0.101.94	LVIGW-c3650.intra.vi.co.jp-94	linkDown	sysUpTimeInstance: 45 days, 22:38:40.32, 1.3.6.1.2.1.2.2.1.1.8: 8, 1...
19/09/03 12:08:59	10.0.101.127	LVIGW-c3650.intra.vi.co.jp-127	linkDown	sysUpTimeInstance: 45 days, 22:38:40.43, 1.3.6.1.2.1.2.2.1.1.8: 8, 1...
19/09/03 12:08:59	10.0.101.102	LVIGW-c3650.intra.vi.co.jp-102	linkDown	sysUpTimeInstance: 45 days, 22:38:40.18, 1.3.6.1.2.1.2.2.1.1.8: 8, 1...

トラップをダブルクリックすると、トラップの詳細を表示することができます。また、表示されているトラップは、[エクスポート]ボタンをクリックして CSV ファイルにエクスポートすることができます。

SNMPトラップ詳細

```
sysUpTimeInstance: 45 days, 22:52:32.69, ifIndex: 8, ifDescr: GigabitEthernet2/0/1, ifAdminStatus: 1, ifOperStatus: 2, 1.3.6.1.6.3.1.1.4.1.0: 1.3.6.1.6.3.1.1.5.3
```

オブジェクト	値
sysUpTimeInstance	45 days, 22:52:32.69
ifIndex	8
ifDescr	GigabitEthernet2/0/1
ifAdminStatus	1
ifOperStatus	2
1.3.6.1.6.3.1.1.4.1.0	1.3.6.1.6.3.1.1.5.3

[閉じる](#)

6.8 受信した Syslog を確認する Enterprise Suite

Rev. 20221026.0600 から[Syslog]タブで syslog を確認できるようになりました。

[ダウンロード]ボタンをクリックすると、syslog ファイルをダウンロードできます。

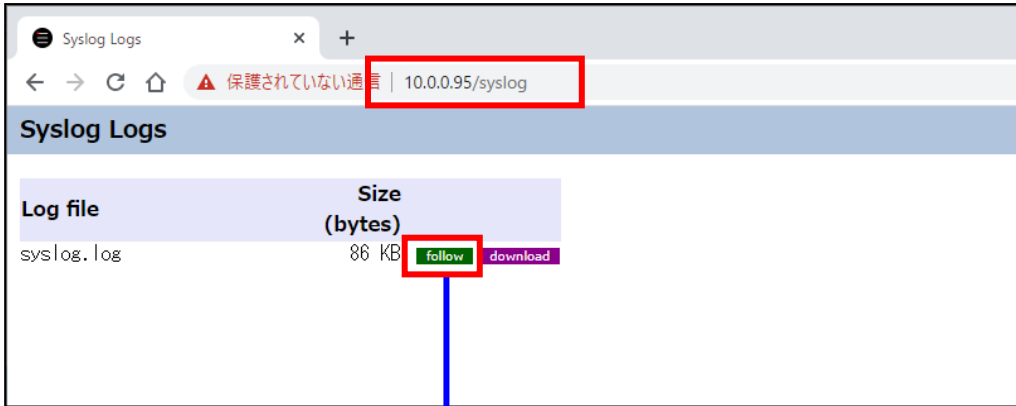
[表示]ボタンをクリックすると、ブラウザ上で syslog を参照できます。

The screenshot displays the Syslog management interface in ThirdEye Suite. At the top, there are navigation tabs for 'ダッシュボード', 'デバイス', '変更履歴', 'ジョブ', 'ターミナルプロキシ', '検索', 'コンプライアンス', 'モニター', 'インシデント', 'マップ', and 'MIB'. Below these is a sub-menu with 'セット', 'テンプレート', 'アラートポリシー', '違反', 'SNMPトラップ', and 'Syslog'. The main area shows a table with two columns: 'ファイル名' (File Name) and 'ファイルサイズ' (File Size). The table lists 'syslog.log' (1 MB) and 'syslog.log.1.gz' (428 KB). To the right of the table are 'ダウンロード' (Download) and '表示' (View) buttons. Below the table is a log viewer for 'Log: syslog.log' with 'Clear' and 'Mark' buttons. The log content shows various system messages, including 'Packet dropped due to input queue full' and 'net1d27 backup 10.0.0.234@default starting'.

Rev. 20221026.0600 以前のバージョンで ThirdEye で受信した Syslog を確認するには、「https://<ThirdEyeIP or Hostname>/syslog」にアクセスします。アクセスすると、以下の画面が表示されます。

[follow]ボタンをクリックすると、ブラウザ上で Syslog を参照できます。

[download]ボタンをクリックすると、syslog ファイルをダウンロードできます。



Log: syslog.log

Clear Mark

Time	Source	Destination	Message
2022-10-01T11:02:50.483185+00:00	LOCAL7.ERR	10.0.0.126	<187:2019: *Oct 1 11:02:19.367: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:03:23.905289+00:00	LOCAL7.ERR	10.0.0.128	<187:2018: *Oct 1 11:02:19.366: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:03:50.726869+00:00	LOCAL7.ERR	10.0.0.126	<187:1985: *Oct 1 20:03:22.819 JST: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:04:23.850119+00:00	LOCAL7.ERR	10.0.0.126	<187:2020: *Oct 1 11:03:14.205: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:04:51.351342+00:00	LOCAL7.ERR	10.0.0.126	<187:1986: *Oct 1 20:04:22.878 JST: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:05:24.675174+00:00	LOCAL7.ERR	10.0.0.126	<187:2021: *Oct 1 11:04:14.819: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:05:51.723911+00:00	LOCAL7.ERR	10.0.0.126	<187:2021: *Oct 1 11:04:14.819: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:06:25.143139+00:00	LOCAL7.ERR	10.0.0.126	<187:1987: *Oct 1 20:05:23.598 JST: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:06:52.143139+00:00	LOCAL7.ERR	10.0.0.126	<187:2022: *Oct 1 11:05:15.202: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:07:25.071918+00:00	LOCAL7.ERR	10.0.0.126	<187:2022: *Oct 1 11:05:15.202: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:07:53.348136+00:00	LOCAL7.ERR	10.0.0.126	<187:1988: *Oct 1 20:06:23.917 JST: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:08:25.165109+00:00	LOCAL7.ERR	10.0.0.126	<187:2023: *Oct 1 11:06:15.924: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:08:55.693164+00:00	LOCAL7.ERR	10.0.0.126	<187:2023: *Oct 1 11:06:15.924: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:09:25.159061+00:00	LOCAL7.ERR	10.0.0.126	<187:1989: *Oct 1 20:07:23.986 JST: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:09:55.939030+00:00	LOCAL7.ERR	10.0.0.126	<187:2024: *Oct 1 11:07:16.834: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:10:25.738185+00:00	LOCAL7.ERR	10.0.0.126	<187:2024: *Oct 1 11:07:16.834: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:10:55.882015+00:00	LOCAL7.ERR	10.0.0.126	<187:1990: *Oct 1 20:08:24.074 JST: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:11:25.783781+00:00	LOCAL7.ERR	10.0.0.126	<187:1990: *Oct 1 20:08:24.074 JST: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:11:56.118849+00:00	LOCAL7.ERR	10.0.0.126	<187:1992: *Oct 1 20:10:24.658 JST: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:12:26.493245+00:00	LOCAL7.ERR	10.0.0.126	<187:2027: *Oct 1 11:10:19.453: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:12:56.021052+00:00	LOCAL7.ERR	10.0.0.126	<187:2027: *Oct 1 11:10:19.453: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:13:27.965381+00:00	LOCAL7.ERR	10.0.0.126	<187:1993: *Oct 1 20:11:24.718 JST: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:14:00.426419+00:00	LOCAL7.ERR	10.0.0.126	<187:2028: *Oct 1 11:11:19.585: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:14:27.385476+00:00	LOCAL7.ERR	10.0.0.126	<187:2028: *Oct 1 11:11:19.585: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:15:00+00:00	LOCALD.INFO	127.0.0.1	<134>Oct 1 11:15:00 netId27 backup 10.0.0.234@default starting
2022-10-01T11:15:02+00:00	LOCALD.INFO	127.0.0.1	<134>Oct 1 11:15:02 netId27 Exiting task of type 'backup' for 10.0.0.234@default.
2022-10-01T11:15:28+00:00	LOCALD.INFO	127.0.0.1	<134>Oct 1 11:15:02 netId27 backup 10.0.0.234@default completed successfully.
2022-10-01T11:15:28.699484+00:00	LOCAL7.ERR	10.0.0.128	<187:1997: *Oct 1 20:15:27.821 JST: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:17:01.806040+00:00	LOCAL7.ERR	10.0.0.126	<187:1998: *Oct 1 20:16:27.855 JST: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:17:29.580761+00:00	LOCAL7.ERR	10.0.0.126	<187:2033: *Oct 1 11:16:25.270: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:18:01.861776+00:00	LOCAL7.ERR	10.0.0.126	<187:2033: *Oct 1 11:16:25.270: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:18:29.627167+00:00	LOCAL7.ERR	10.0.0.126	<187:1989: *Oct 1 20:17:28.500 JST: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:18:58.024116+00:00	LOCAL7.ERR	10.0.0.126	<187:2034: *Oct 1 11:17:25.326: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:19:02.089592+00:00	LOCAL7.ERR	10.0.0.126	<187:2034: *Oct 1 11:17:25.326: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:19:29.983305+00:00	LOCAL7.ERR	10.0.0.126	<187:2000: *Oct 1 20:18:26.547 JST: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:20:02.126086+00:00	LOCAL7.ERR	10.0.0.126	<187:2035: *Oct 1 11:18:26.492: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:20:02.126086+00:00	LOCAL7.ERR	10.0.0.126	<187:2035: *Oct 1 11:18:26.492: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
2022-10-01T11:20:31.064689+00:00	LOCAL7.ERR	10.0.0.126	<187:2001: *Oct 1 20:19:28.904 JST: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
			<187:2036: *Oct 1 11:18:26.583: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full
			<187:2002: *Oct 1 20:20:29.987 JST: *SNMP-3-INPUT_OFULL_ERR: Packet dropped due to input queue full

Following

6.9 監視を一時的に停止する(非監視設定)

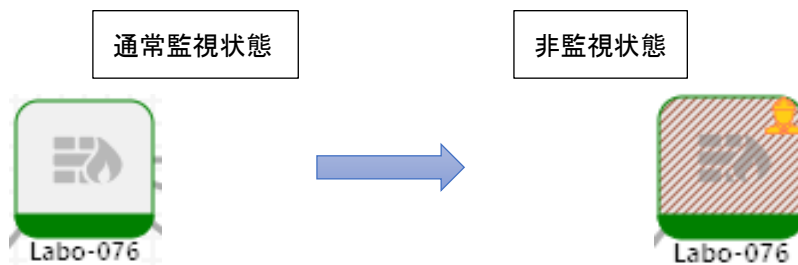
監視を停止することを「非監視」と呼びます。監視対象機器を非監視状態にすると、その機器で監視イベントが発生しても、障害イベントを検知しなくなります。この機能は、メンテナンス時などに監視を一時的に停止したい場合に有効です。

非監視の設定方法は、「[6.9.1 手動で非監視にする](#)」と「[6.9.2 スケジュールで非監視にする](#)」の2通りあります。

注意

rev.20201203.0810 以降、[ジョブ]タブにあった非監視機能は、[デバイス]タブから操作するように変更されました。

デバイスを非監視状態にすると、マップ上のオブジェクトの外観が次のように変化します。

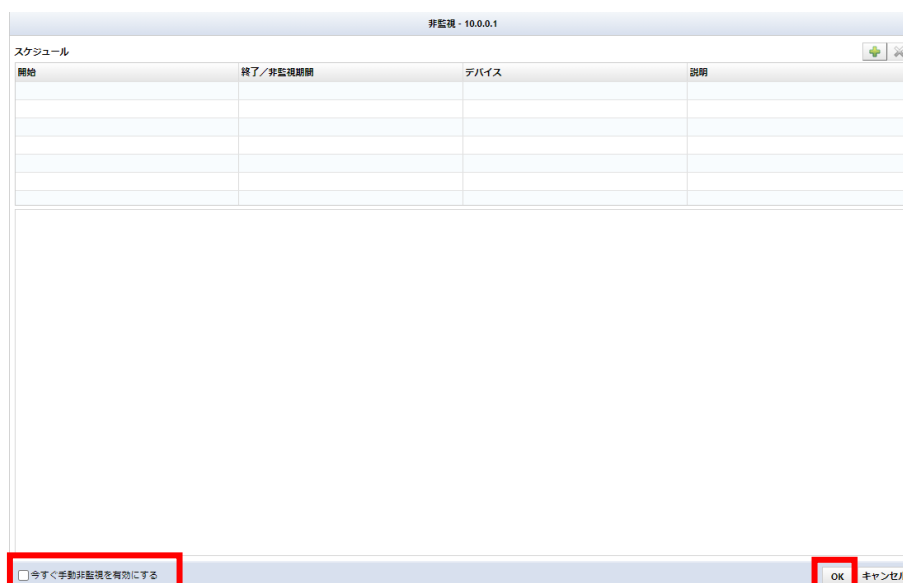


6.9.1 手動で非監視にする

1. [デバイス]タブを開き、非監視状態にしたいデバイスを選択して右クリックします。
※「Ctrl」キーを押しながら選択すると、複数選択ができます。
2. [非監視を管理]をクリックします。

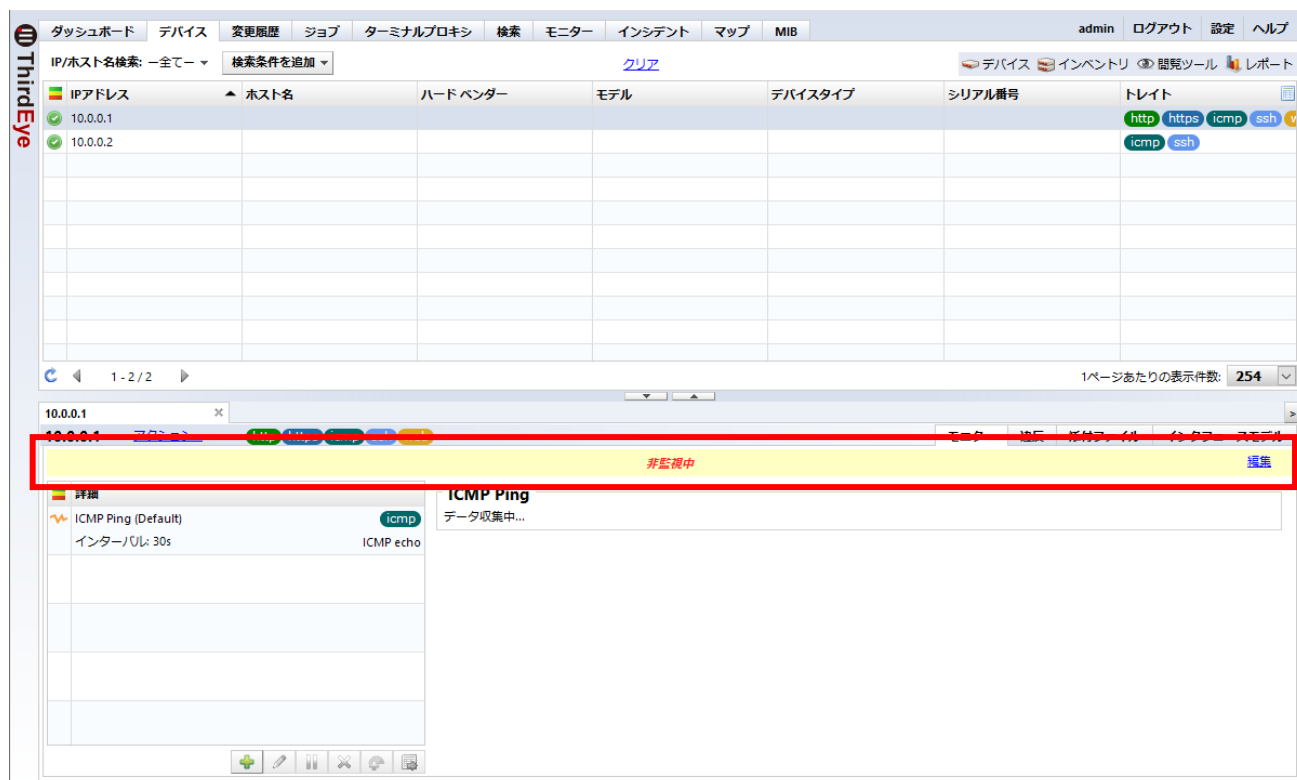


3. 「今すぐ手動非監視を有効にする」にチェックを入れ、[OK]をクリックします。



以上で操作は完了です。

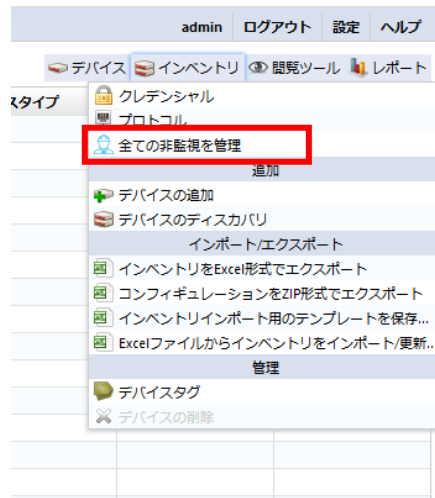
デバイスをダブルクリックしてデバイスビューを表示すると、[モニター]タブに **非監視中** と表示されていることを確認できます。




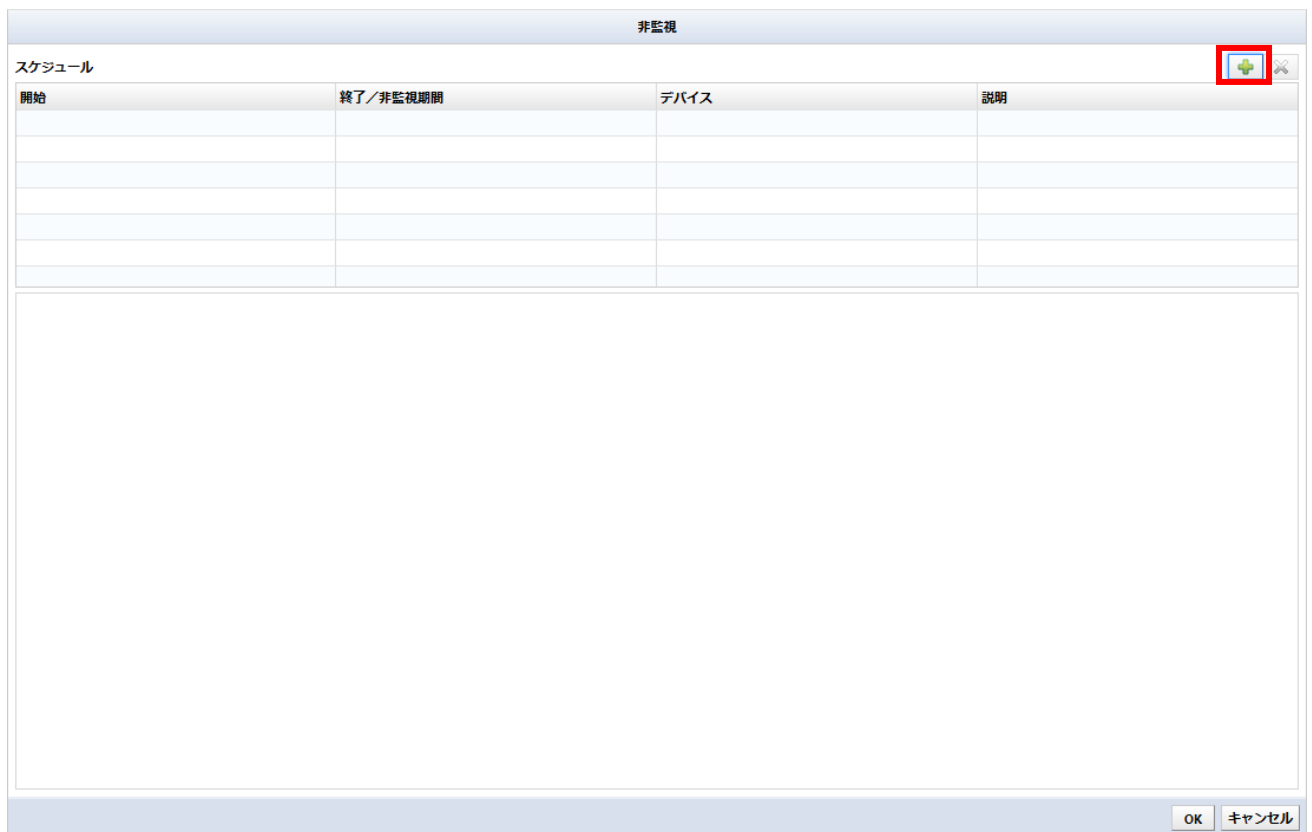
非監視状態を解除する場合は、上記[手順 3]で「今すぐ手動非監視を有効にする」のチェックをはずし、[OK]をクリックしてください。

6.9.2 スケジュールで非監視にする

1. [デバイス]タブを開き、[インベントリ]→[全ての非監視を管理]をクリックします。



2. [ (追加)]ボタンをクリックします。



3. 非監視のスケジュールと対象のデバイスを設定します。

開始	終了/非監視期間	デバイス	説明
2021/03/12 16:14	2021/03/12 17:14 (60分)	全てのデバイス	

スケジュール 時間帯: (GMT+09:00) 東京 説明

開始: 一度 日単位 週単位 月単位 クーロン

16 : 14 2021/03/12

非監視期間: 1 hr 終了: 17 : 14 2021/03/12

デバイス

全てのデバイス 検索 静的リスト

OK キャンセル

メニュー項目	項目	説明
スケジュール	開始	以下 5 種類の実行スケジュールから、非監視を開始するスケジュールを選択します。 <ul style="list-style-type: none"> 一度・・・時刻に設定されている日時に 1 度だけ実行する 日単位・・・n 日毎に実行する(起点は当月 1 日) 週単位・・・特定の曜日に実行する 月単位・・・指定した月毎に実行する クーロン・・・クーロン形式で指定した日時に行する
	非監視期間	非監視期間を指定します。 期間の単位は「min」「hr」「day」から変更できます。 ※終了の日は、実行スケジュールが「一度」の場合のみ指定できる
説明		非監視スケジュールの説明を入力します。
デバイス		非監視スケジュールの実行対象となるデバイスを指定します。 <ul style="list-style-type: none"> 全てのデバイス・・・全てのデバイスを対象にする 検索・・・指定された検索に該当するデバイスのみを対象にする 静的リスト・・・指定されたデバイスのみを対象にする

4. [OK]をクリックします。

以上の操作で、スケジュールの設定時間に応じて非監視状態になります。

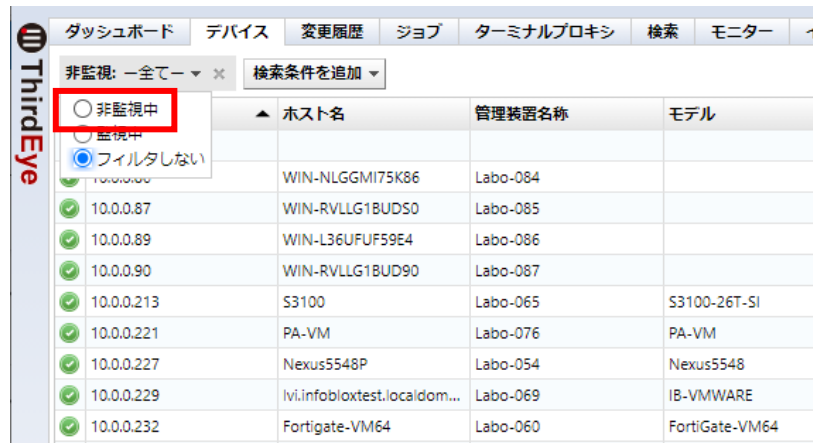
6.9.3 非監視のデバイスを検索する

デバイスタブの検索条件を使用して、非監視状態のデバイスを検索することができます。

1. [デバイス]タブを開き、[検索条件を追加]→[非監視]をクリックします。



2. [非監視中]を選択します。



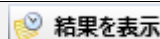
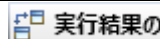


以上の操作で、非監視中のデバイスの一覧が表示されます。

6.10 ジョブ管理 Enterprise Suite

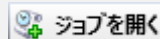

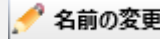

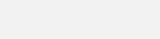
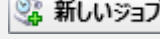
ジョブタブでは、ジョブを作成、編集、管理そして実行が出来ます。一つのジョブは、定期的に自動実行するように設定されたコマンドの集まりです。ジョブのトリガーとは、定期的な実行を引き起こすきっかけになる条件のことです。たとえば、1月1日の正午、五分ごと、毎月の最初の月曜日などです。一つのジョブには複数のトリガーを与えることが出来、与えるトリガーを調整することで、ジョブを実行する頻度を制御できます。

ジョブタブは2つのサブタブ、ジョブ履歴タブとジョブ管理タブから成り立ちます。ジョブ履歴サブタブでは、過去のジョブ実行の結果を見ることが出来ます。自動的に実行されたものも手動で実行したものも、共にここに表示されます。

ジョブ履歴サブタブでは、以下のボタンがあります。

項目	説明
 結果を表示	選択したジョブの実行結果を開きます。
 実行結果の比較	選択した2つのジョブの結果を比較します。
 キャンセル	選択した実行中のジョブを中止します。
 ジョブ承認ログ	ジョブ承認ログを表示します。

一方、ジョブ管理サブタブでは、ジョブの新規作成、作成済みジョブのプロパティ確認、編集などの実際の作業を行うことが可能です。登録されているジョブをダブルクリックすれば、編集画面が開きます。いくつかのボタンが提供されています。

項目	説明
 ジョブを開く	選択したジョブのプロパティを開きます。
 削除	選択したジョブを削除します。
 名前の変更	選択したジョブの名前を変更します。
 すぐに実行	選択したジョブを即時に実行します。
 新しいジョブ	新規ジョブを作成します。ツール/ディスカバリ/ネイバー/バックアップ/バルクチェンジ/レポートのジョブを追加できます。
 フィルタの設定	クローン形式のフィルタを登録します。

6.10.1 ジョブの作成

ジョブは、ジョブ管理→新しいジョブ以下のサブメニューから作成できます。このサブメニューには様々な種類のジョブが登録されていますが、どの種類のジョブでもその作成の大まかな流れは変わりません。メニューから種類を選んだ後、ジョブを作るには、

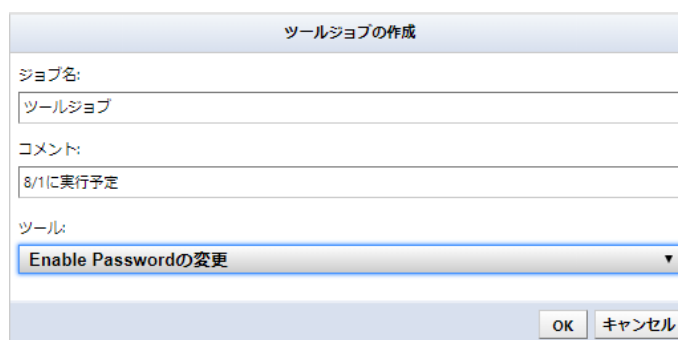
1. まずジョブ名を決め、使う機能を選びます。
2. 必要なパラメータを入力します。
3. 対象デバイスを選びます。
4. 最後に、ジョブのトリガー(実行頻度)を入力します。

以下では、試しにジョブを一つ作り、その様子を画面ごとに実際に示して説明を行います。新しいジョブ→ツールをクリックしてみましょう。

1. ジョブ名を決め、機能を選ぶ

まずは、好きな名前でもジョブ名を与えます。コメント欄には、後に他人がわかりやすいコメントを付け加えると良いでしょう。

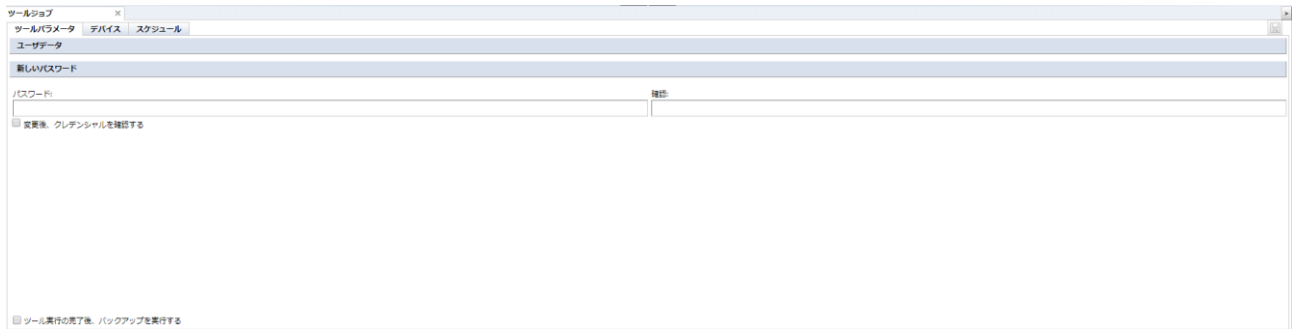
次に、ツールを選びます。デバイスタブのツールメニュー→閲覧ツールと変更メニューで使うことのできるツールはほぼすべて選ぶことが出来ます。今回はイネーブルパスワードの変更を選んでみましょう。OK ボタンを押すと、ステータスペインに新しいタブが開かれます。



ツールジョブの作成	
ジョブ名:	ツールジョブ
コメント:	8/1に実行予定
ツール:	Enable Passwordの変更
OK キャンセル	

2. 必要なパラメータを入力

次に、開かれた新しいタブで、必要なパラメータを入力します。(新しいタブは更にサブタブに分かれており、ツールパラメータサブタブがデフォルトで開かれているはずです。)イネーブルパスワードの変更を選んだので、入力すべきツールパラメータはパスワード、確認、ツール実行の完了後、バックアップを実行します。



3. 対象デバイスを選ぶ


画面のメインペインにはジョブタブが、ステータスペインには新しいジョブの設定タブ(その中にはツールパラメータサブタブ)が開かれているはずです。

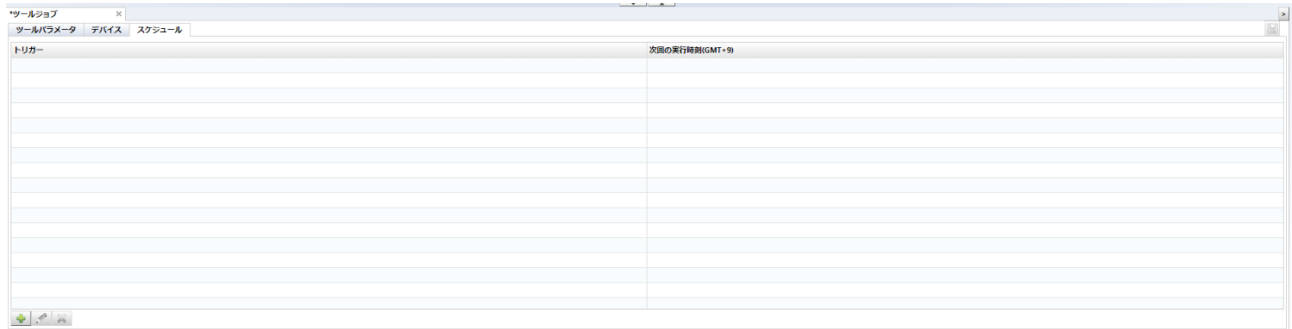
ステータスペインでデバイスサブタブを選んでください。詳細検索機能と似た画面が表示されます。ただし、この画面には すべてのデバイス、検索、静的リストというラジオボタンがあります。



検索オプションを使う場合の注意としては、検索はジョブ実行時に行われるという事です。デバイスビューの検索で現れたものが固定されて追加されるものではありません。ジョブを実行するときと同じ条件で検索を行い、その結果に対してジョブを実行します。そのため、インベントリに新しいデバイスが追加され、かつそのデバイスがジョブ作成時の検索クエリにマッチした場合、ジョブはその新しいデバイスにも実行されます。この性質はうまく使えば便利ですが、間違えると想定外のデバイスにジョブを実行することになります。この点に留意してください。

4. トリガーを追加する

最後に、トリガーを追加します。ステータスペインをスケジュールサブタブに移動させてください。下部、左の  ボタンから、新しいトリガーを追加することができます。



日付や繰り返し頻度を設定し、トリガーを作ります。すべての入力が終わったら、保存ボタンを押してください。

トリガー

名前:

一度
 日単位
 週単位
 月単位
 クーロン


繰り返し間隔 日ごと

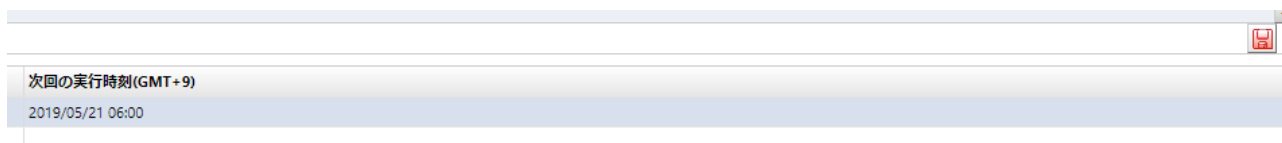
繰り返し間隔の値に1以外の数値を設定した場合、そのスケジュールの開始点は常に各月の1日からとなります。例: 繰り返し間隔 = 2の場合 → 自動ディスクパリは開始月の1日から始まり、3日、5日・・・の間隔で起動します。

時間帯:

フィルタ:

項目	説明
名前	トリガーの名称
時刻	ジョブを実行する時刻、日付
スケジュール単位	以下 5 種類の実行スケジュールを選択 一度・・・時刻に設定されている日時に 1 度だけ実行する 日単位・・・n 日毎に実行する(起点は当月 1 日) 週単位・・・特定の曜日に実行する 月単位・・・指定した月毎に実行する クーロン・・・クーロン形式で指定した日時に実行する
時間帯	タイムゾーン
フィルタ	「フィルタの設定」で登録されているスケジュールフィルタを選択します。このフィルタにマッチしたタイミングは、トリガーから取り除かれます。




最後に、ステータスペインの右上にある ボタンを押してジョブ設定を保存することを忘れないようにしてください。未保存の変更が存在したままになってしまいます。



6.10.2 ジョブ履歴

[ジョブ]→[ジョブ履歴]サブタブでは、過去のジョブ実行履歴が一覧で表示されます。過去のジョブの実行状況は、ジョブが成功したか失敗したかのステータスとともに記録されています。

ステータスアイコンは、ジョブ履歴一覧の左側に表示されます。ステータスアイコンとその意味は次のとおりです。

アイコン	説明
	全てのデバイスに正常に接続できました。
	一部のデバイスで処理が失敗しました。
	全てのデバイスで処理が失敗しました。

ジョブ履歴の保存期間を設定する方法については、「[7.12 データ保存期間を変更する](#)」を参照してください。

6.10.3 ジョブ承認機能

承認機能とは、申請者が作成・編集したジョブを、上長などの承認者が承認することで実行可能になる機能です。承認を得ていないジョブは、実行できなくなります。この機能を利用することで、誤操作の防止やコンプライアンス強化など、セキュアな運用を実現できます。

※この承認機能は、ネットワーク機器の設定を変更するジョブに対してのみ有効です。

承認の流れ

1. 申請者がジョブを作成・編集し、[承認要求]を行う(承認依頼)
2. 承認担当者が、該当ジョブ内の[ジョブ承認ログ]から承認依頼を確認する。
3. 問題がなければ[承認]を行う。問題があれば確認画面から[却下]または[コメント]を行い、申請者へ連絡する。
4. [承認]が行われたら、申請者は該当ジョブを実行する。

(1) 承認機能の権限を設定する

登録済みの権限に対して、承認者の設定をします。設定された権限を割り当てられたユーザが、ジョブの承認を行うことができます。

1. [設定]をクリックします。
2. [権限]を選択し、対象の権限を選択します。
3. 権限内容を指定し、[OK]をクリックします。

承認機能に関する権限は、以下の2つの権限内容です。

権限	説明
ツールの実行を承認する権限。	承認要求(承認依頼)されたジョブを承認することができる権限。
承認なしにツールを実行する権限。	承認要求(承認依頼)することなく、ジョブを実行することができる権限。

■承認者の権限を設定する場合、「ツールの実行を承認する権限。」にチェックを入れます。

The screenshot shows the 'Server Settings' dialog box. On the left, a list of settings is visible, with '権限' (Permissions) selected. The main area shows a list of roles: Administrator, approver, and requester. The 'approver' role is selected. Below the role list, there are several checkboxes for permissions. The checkbox for 'ツールの実行を承認する権限。' (Tool execution approval) is checked. Other permissions like 'ツールの実行を許可する。' (Allow tool execution) and '承認なしにツールを実行する権限。' (Allow tool execution without approval) are unchecked. At the bottom, there are buttons for '全て選択' (Select all), '全ての選択を解除' (Deselect all), 'OK', and 'キャンセル' (Cancel).

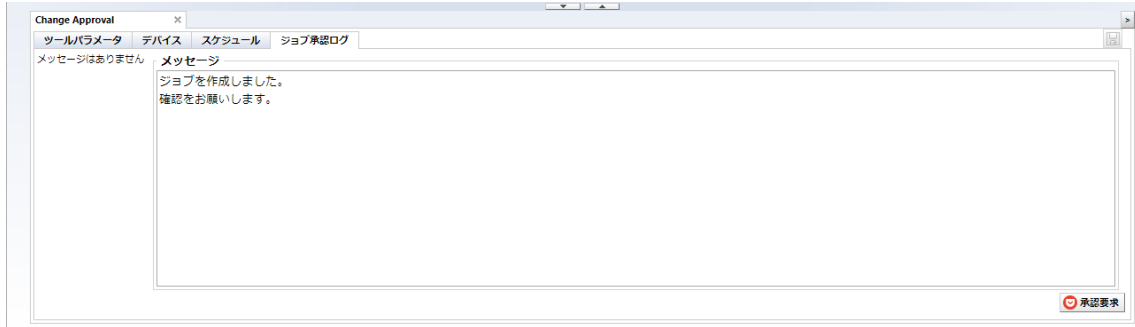
■申請者の権限を設定する場合、「ツールの実行を承認する権限。」のチェックをはずします。

The screenshot shows the 'Server Settings' dialog box. On the left, a list of settings is visible, with '権限' (Permissions) selected. The main area shows a list of roles: Administrator, approver, and requester. The 'requester' role is selected. Below the role list, there are several checkboxes for permissions. The checkbox for 'ツールの実行を承認する権限。' (Tool execution approval) is unchecked. Other permissions like 'ツールの実行を許可する。' (Allow tool execution) and '承認なしにツールを実行する権限。' (Allow tool execution without approval) are checked. At the bottom, there are buttons for '全て選択' (Select all), '全ての選択を解除' (Deselect all), 'OK', and 'キャンセル' (Cancel).

(2) 承認要求を申請する(ジョブを申請する)

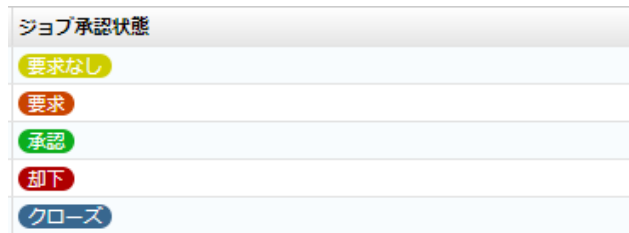
申請者はジョブを作成・編集する際に、承認要求を申請することができます。

1. ジョブを作成・編集します。
2. [ジョブ承認ログ]タブを開き、メッセージ欄にメッセージを入力し、[承認要求]をクリックします。



申請が完了すると、[ジョブ承認状態]カラムに「要求」と表示されます。

■ [ジョブ承認状態]カラムの表示例



■ [ジョブ承認状態]カラムの表示内容一覧

ジョブ承認状態	説明
要求なし	ジョブ承認要求が設定されていません。
要求	ジョブ実行承認が要求されています。
承認	ジョブ実行が承認されています。
却下	ジョブ承認要求が却下されています。
クローズ	ジョブがクローズされています。このステータスは以下の場合に設定されます。 <ul style="list-style-type: none">• ジョブの実行• 管理者/ジョブ要求者によるクローズ ※クローズされたジョブを実行したい場合は、再度承認要求を行う必要があります。

(3) 承認要求を承認する(ジョブを承認する)

承認者は、申請者から申請されたジョブ(承認要求)を承認することができます。

1. [ジョブ管理]タブを開きます。

2. 承認要求されたジョブを開きます。

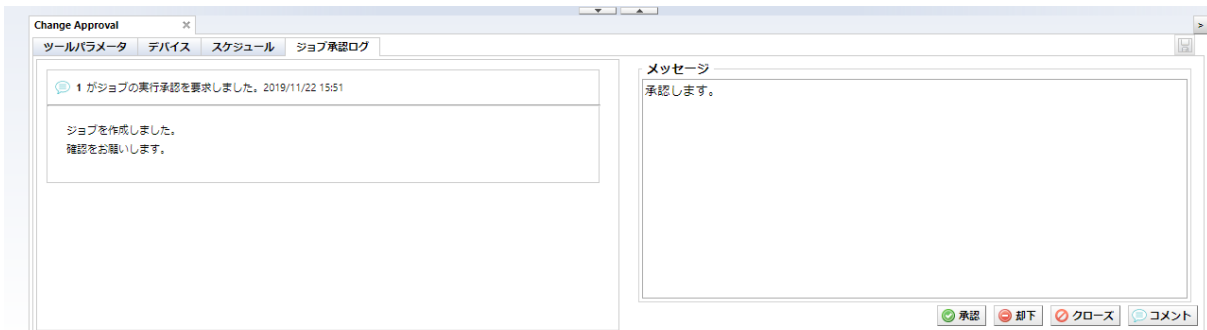
[ジョブ管理]画面上部にある「ジョブ実行承認状態」から、表示するジョブをフィルタできます。



3. ジョブ内容を確認し、[ジョブ承認ログ]タブを開きます。

4. メッセージ欄にメッセージを入力し、[承認]をクリックします。

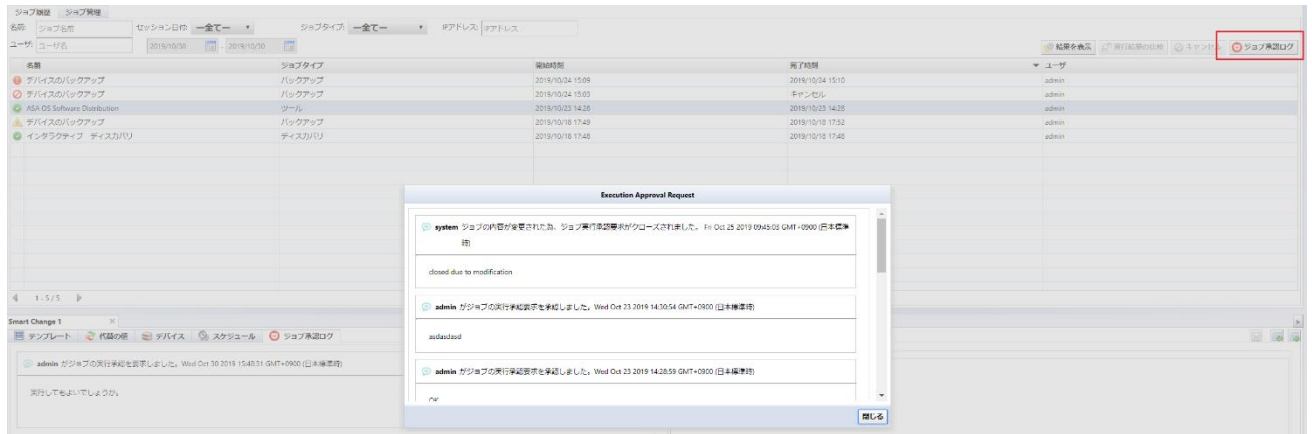
問題があれば、メッセージ欄にメッセージを入力し、[却下]または[コメント]をクリックします。



(4) 承認までの記録を確認する

[ジョブ履歴]画面で、対象ジョブを選んで[ジョブ承認ログ]をクリックすると、承認までの記録(メッセージ)を確認することができます。

※[ジョブ承認ログ]ボタンは、承認後に実行されたジョブの場合にのみ有効になります。



(5) 承認機能の通知

ジョブの申請、実行、完了時に SNMPトラップまたは該当のジョブ関係者へメールによる通知を行うことができます。

➤ SNMPトラップ設定

サーバ設定画面の SNMPトラップ設定から、承認イベント発生時にトラップを送信します。

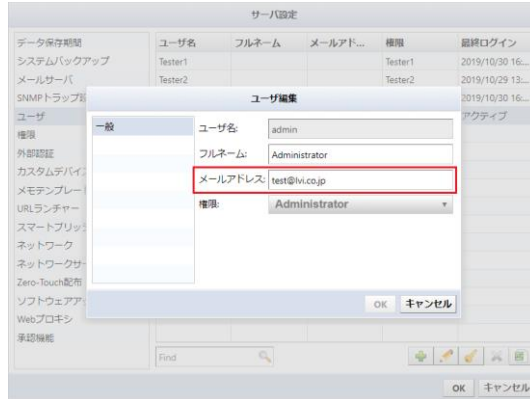
ジョブの要求/実行/承認/却下/クローズ時にトラップが送信されます。



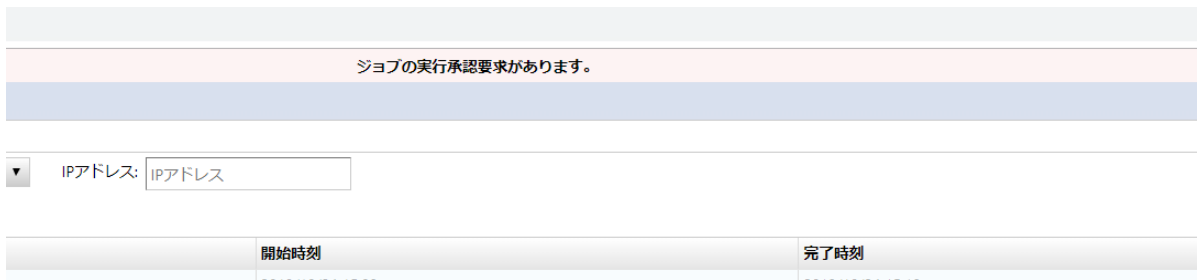
➤ メール送信

サーバ設定画面のユーザ編集でメールアドレスを設定することで、承認イベント発生時にメールを送信することができます。ジョブの要求/実行/承認/却下/クローズ時にメールが送信されます。

メール送信を行うためには、事前にメールサーバを設定しておく必要があります。

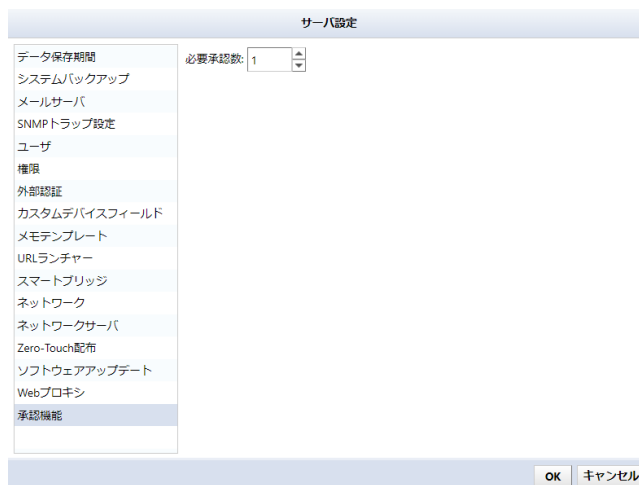


また、ジョブの承認要求がある場合、画面上部に以下のようなバナーが表示されます。



(6) 必要承認数を変更する

申請者が作成・編集したジョブを実行できるようになるまでに必要な承認数を指定できます。必要承認数の設定は、[設定]→[承認機能]より設定できます。設定可能な範囲は、1～3です。



6.10.4 過去のジョブ履歴を確認する

ジョブ履歴は、[ジョブ]タブ→[ジョブ履歴]から確認でき、これまでに実行されたジョブが表示されます。ジョブタイプには、レポート/ディスカバリ/ネイバー/バックアップ/Agent-D/ツールがあり、「いつ」、「誰が」、「何をした」という情報が記録されます。また、レポートのジョブについてはダブルクリックをすることで発行されたレポートを閲覧することが可能です。

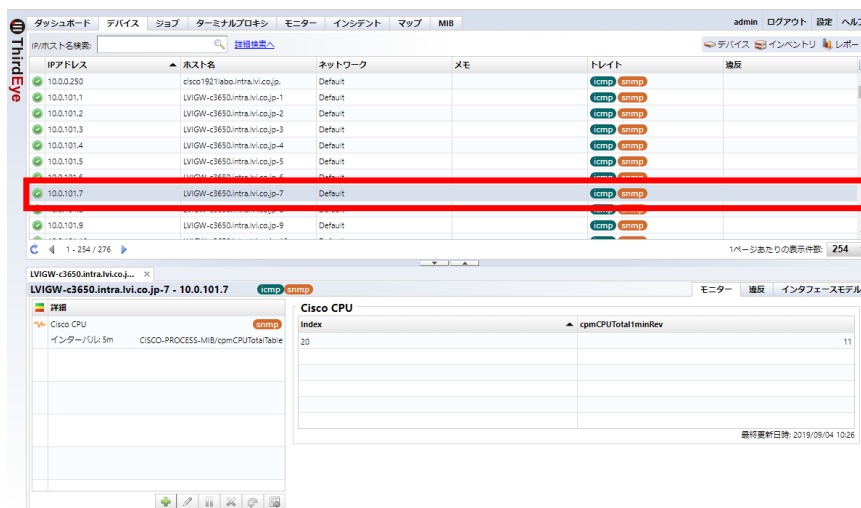
【カラム一覧】

項目	説明
名前	ジョブの名前が表示されます。
ジョブタイプ	ジョブの種類が表示されます。
開始日時	ジョブを実行した開始日時が表示されます。
完了日時	ジョブを完了した完了日時が表示されます。
ユーザ	ジョブを実行したユーザ名が表示されます。

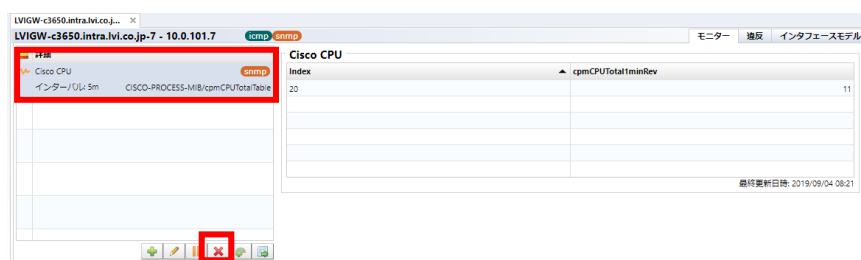
6.11 監視設定を解除する

6.11.1 モニターを削除する

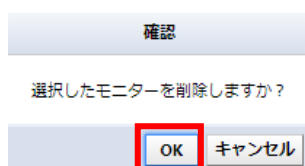
1. [デバイス]タブの監視対象機器一覧から、モニターを設定する機器をダブルクリックします。



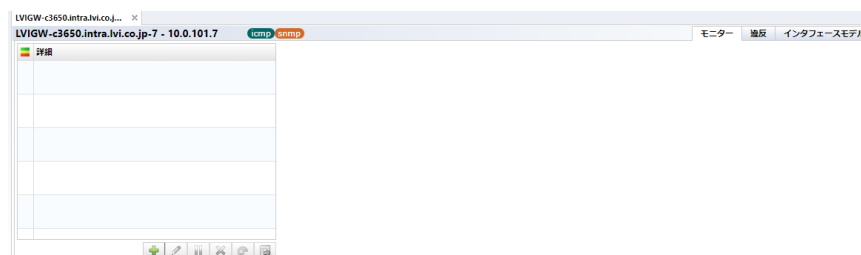
2. モニター詳細から削除するモニターを選択し、[削除]をクリックします。



3. 確認画面で[OK]をクリックします。

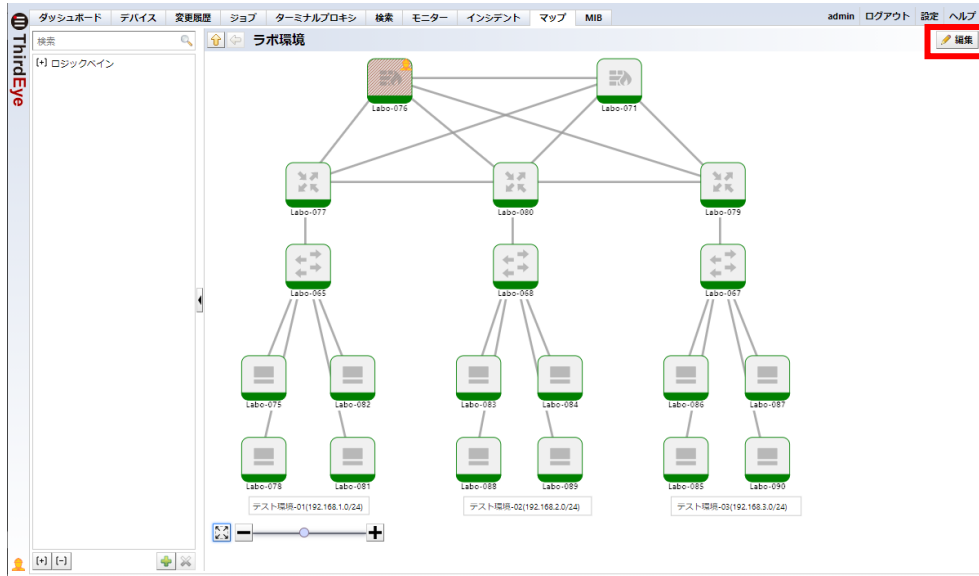


モニター詳細からモニターが削除され、データ収集が中止されます。

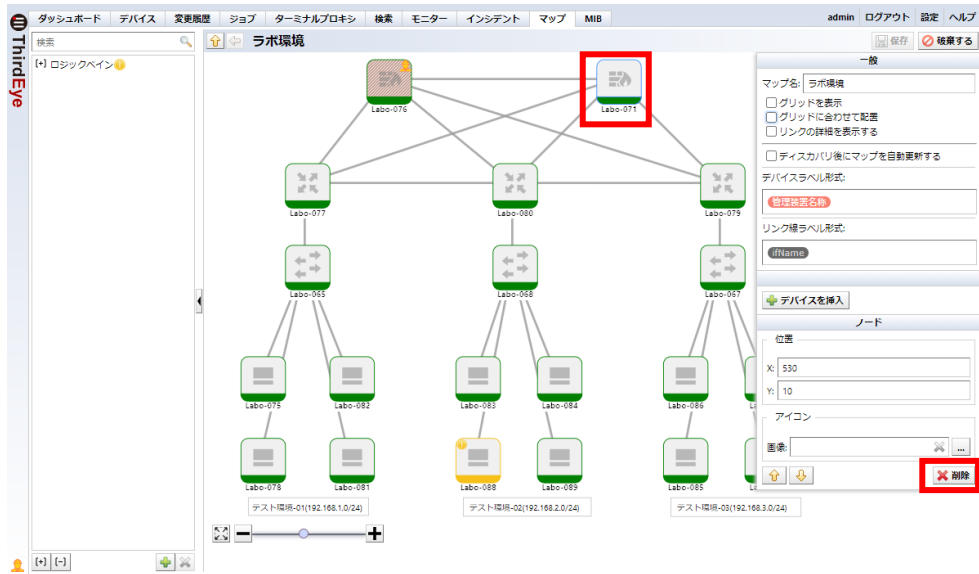


6.11.2 マップからオブジェクト(デバイス/マップ)を削除する

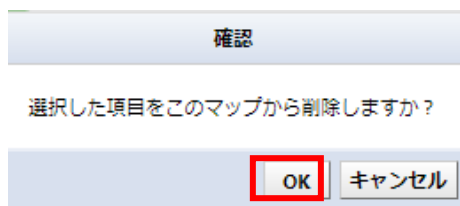
1. 画面左側のマップ一覧からマップをダブルクリックで開き、[編集]をクリックします。



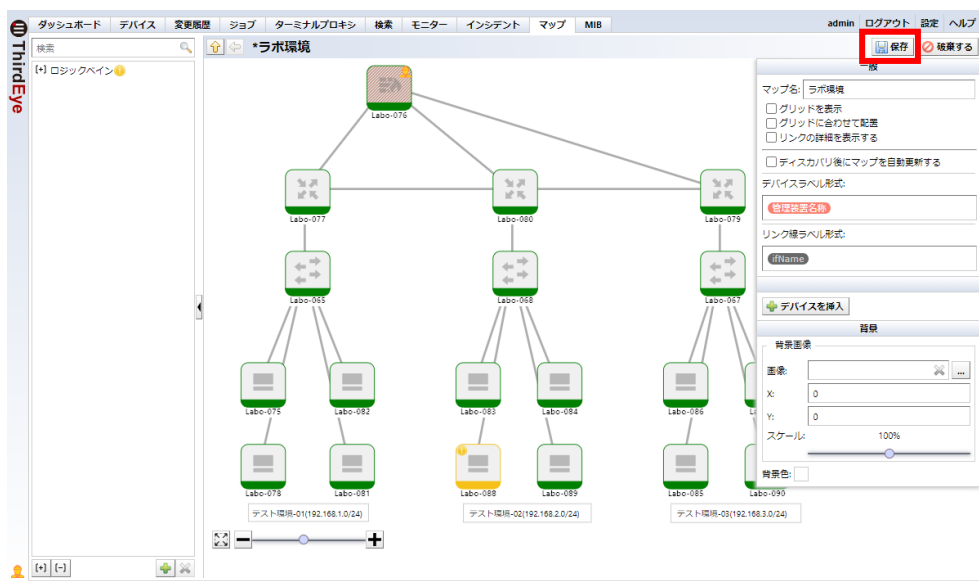
2. 削除したいオブジェクトを選択し、[削除]をクリックします。



3. 確認メッセージが表示されます。[OK]をクリックします。

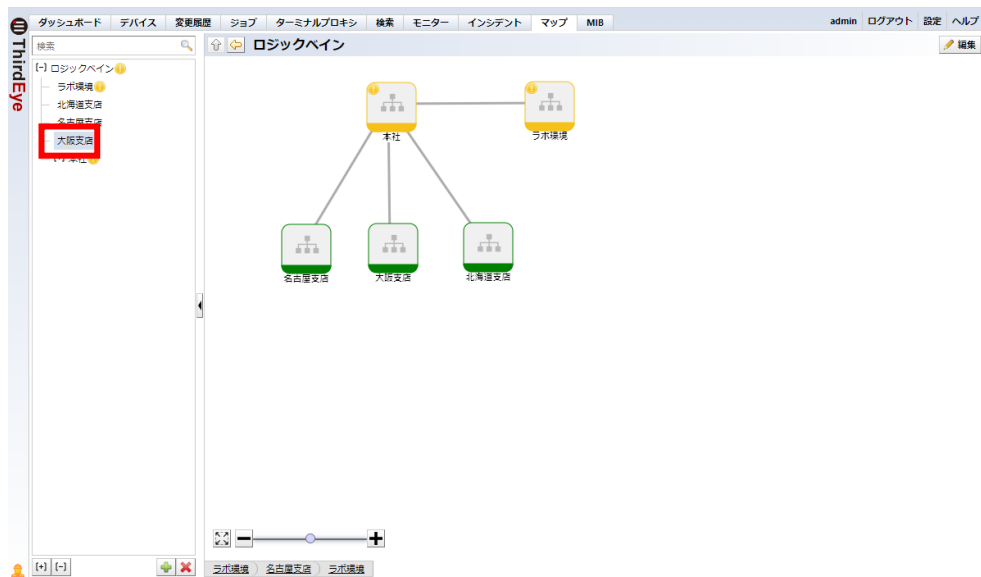



4. デバイスが削除されます。[保存]をクリックし、編集を完了します。

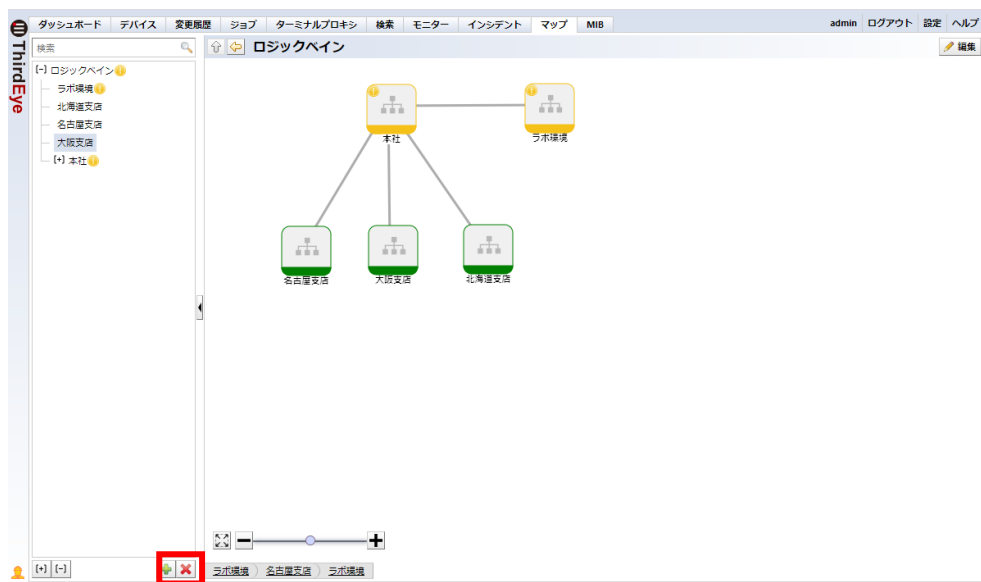


6.11.3 マップを削除する

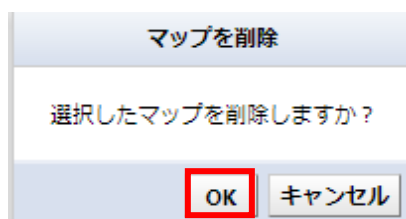
1. マップツリーから削除したいマップを選択します。



2. 左下の[ (削除)]をクリックします。

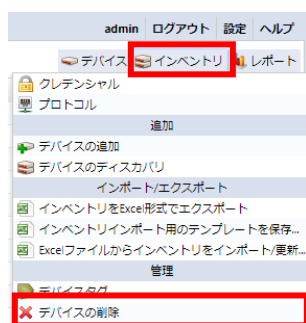


3. 確認メッセージが表示されます。[OK]をクリックします。



6.11.4 デバイスを削除する

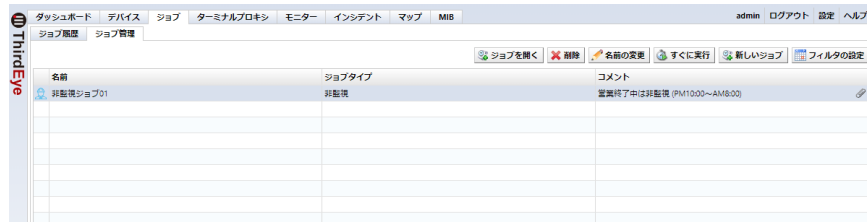
1. [デバイス]タブで削除したいデバイスを選択します。※複数選択可
2. デバイスを選択した状態で、[インベントリ]→[デバイスの削除]の順にクリックします。



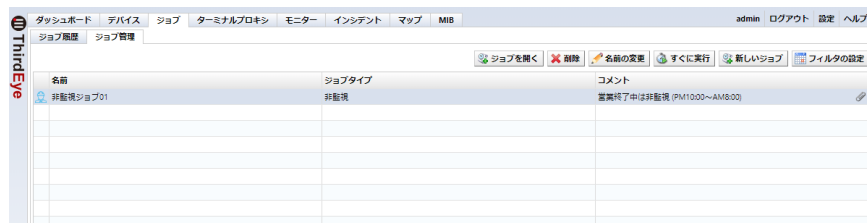
3. 確認メッセージが表示されます。[はい]をクリックします。

6.11.5 ジョブを削除する

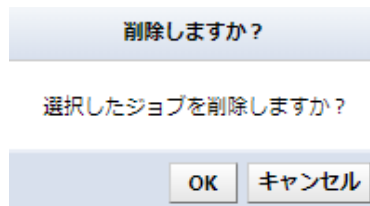
1. [ジョブ]タブ→[ジョブ管理]をクリックします。



2. 削除するジョブを選択し、[削除]をクリックします。



3. 確認画面で[はい]をクリックします。



ジョブ管理一覧から、選択したジョブが削除されます。



第7章 詳細設定

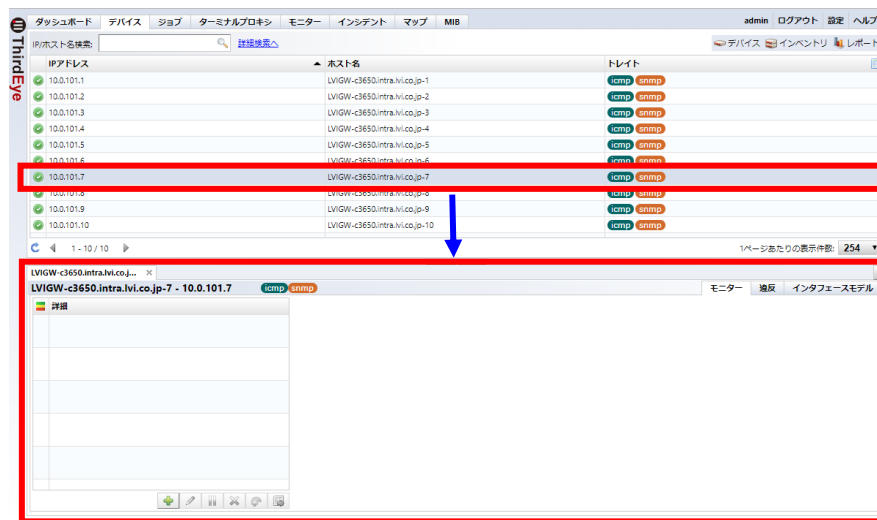
ここでは、ThirdEye のバックアップやグローバル設定、基本設定より詳細な監視設定を紹介します。

7.1 いろいろな監視設定をする

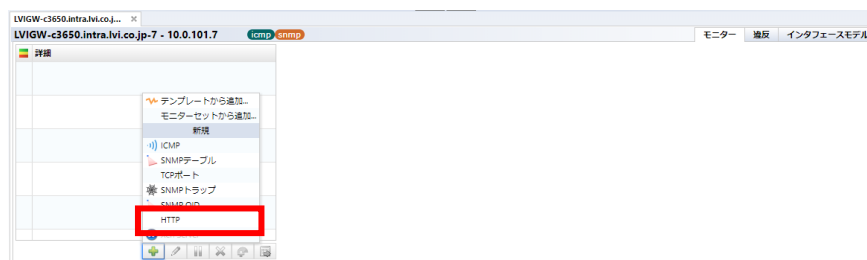
7.1.1 Web サイトの監視する Enterprise Suite

HTTP リクエストを送信し、Web ポートの監視や特定のサイトの監視を行うことができます。

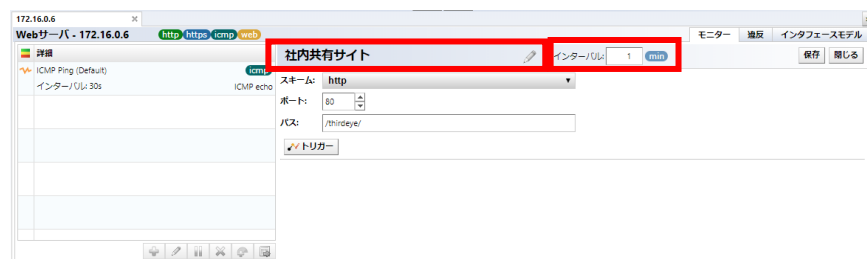
1. [デバイス]タブの監視対象機器一覧から、モニターを設定する機器をダブルクリックします。



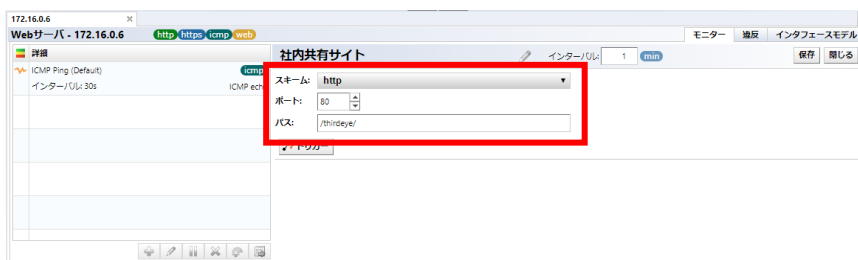
2. 左下の[+] (追加) をクリックし、「HTTP」をクリックします。



3. 任意のモニター名とインターバルを設定します。

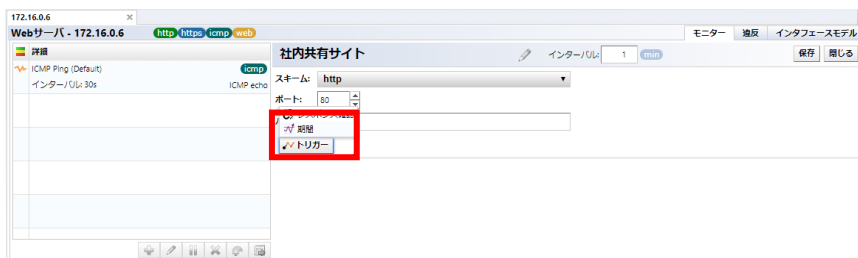


4. 以下の項目を入力します。



項目	説明
スキーム	HTTP または HTTPS を選択します。
ポート	Web ポートを指定します。
パス	監視するサイトのパスを入力します。

5. [トリガー]をクリックし、[期間]をクリックします。

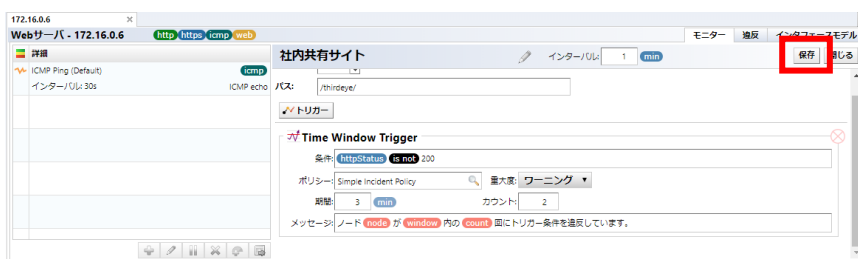


6. 各項目を設定します。

以下の画面の条件では、ステータスコードが「200」以外の場合がアラート対象になります。
 ※各項目の詳細については、「5.3.4 しきい値を設定して監視する」を参照してください。



4. [保存]をクリックします。




保存後、リクエストが開始され正常に取得できればデバイス詳細画面にデータが表示されます。



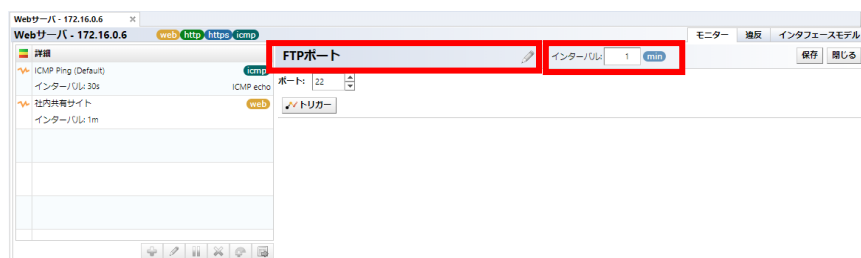
7.1.2 TCP ポートを監視する Enterprise Suite

TCP ポートに syn メッセージを送信し、応答があるかを確認することができます。

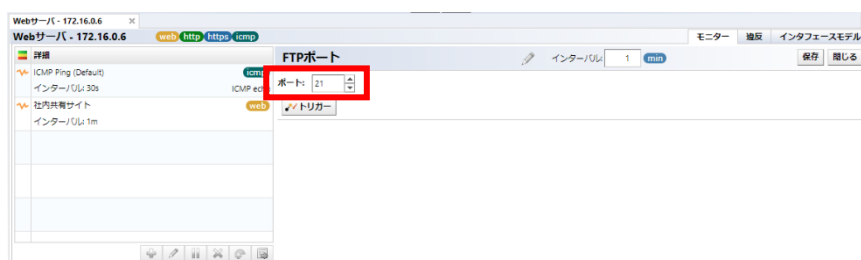
1. 左下の[ (追加)]をクリックし、「TCP ポート」をクリックします。



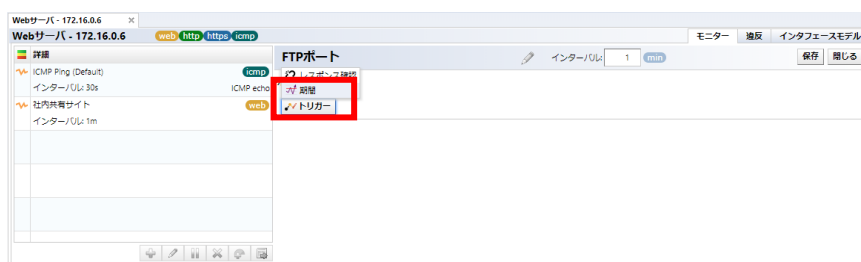
2. 任意のモニター名とインターバルを設定します。



3. 監視するポート番号を設定します。

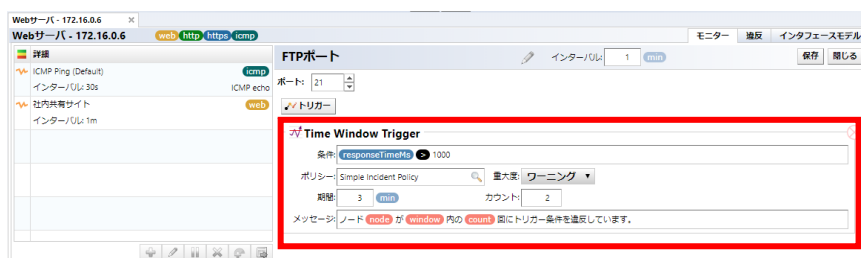


4. [トリガー]をクリックし、[期間]をクリックします。

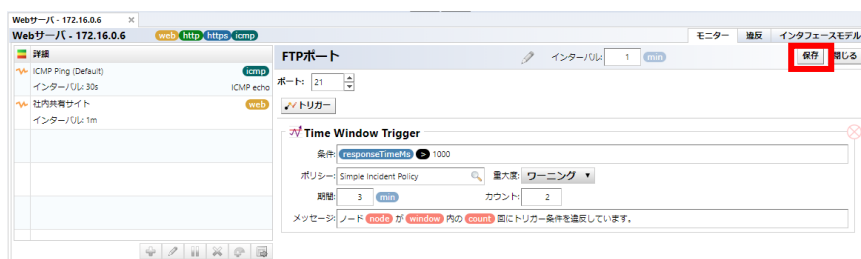


5. 各項目を設定します。

以下の画面の条件では、レスポンスが 1000 ミリ秒より大きい場合がアラート対象になります。
※各項目の詳細については、「5.3.4 しきい値を設定して監視する」を参照してください。



6. [保存]をクリックします。



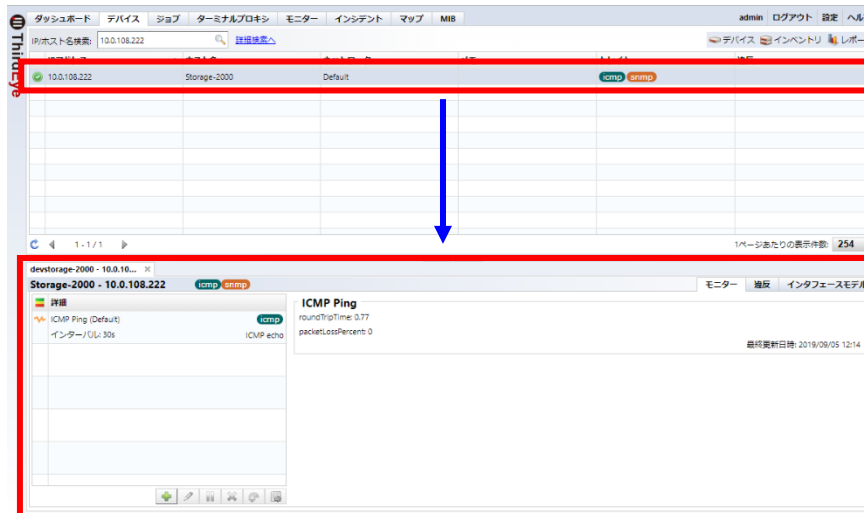
保存後、リクエストが開始され正常に取得できればデバイス詳細画面にデータが表示されます。



7.1.3 計算式を使用した監視をする

ThirdEye では、カスタム計算式を使用して取得したデータを自動で計算することができます。例えば、標準 MIB である HOST-RESOURCE-MIB にはサーバのディスクのサイズと使用量の MIB はありますが、使用率(%)の MIB はありません。カスタム計算式を使用することで、ディスクのサイズと使用量を計算して使用率を出すことができます。ここでは、HOST-RESOURCE-MIB を例に手順を記載します。

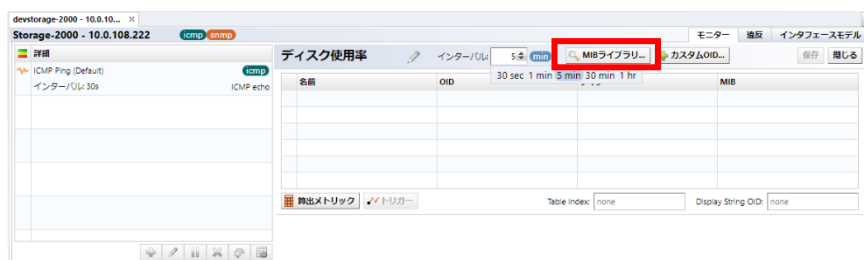
1. [デバイス]タブの監視対象機器一覧から、モニターを設定する機器をダブルクリックします。



2. 左下の[+] (追加)をクリックし、「SNMP テーブル」をクリックします。
3. 任意のモニター名とインターバルを設定します。



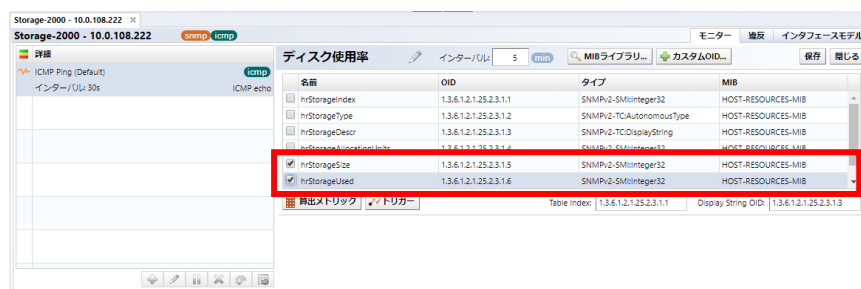
4. [MIB ライブラリ]をクリックします。



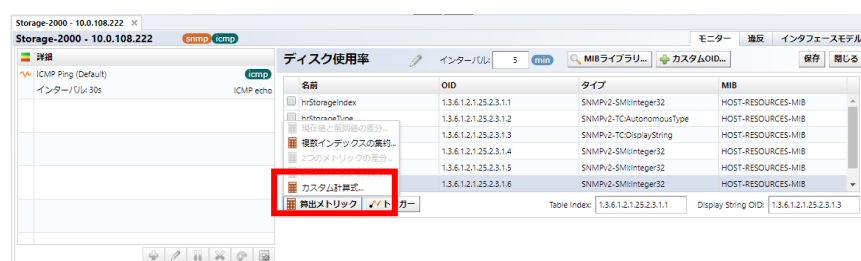
- OID 検索に「hrstorage」と入力し、検索結果から「hrStorageTable」を選択し[OK]をクリックします。



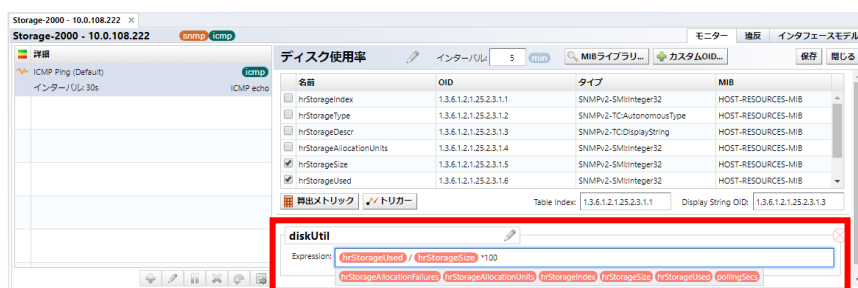
- テーブルから「hrStorageSize/hrStorageUsed」にチェックを入れます。



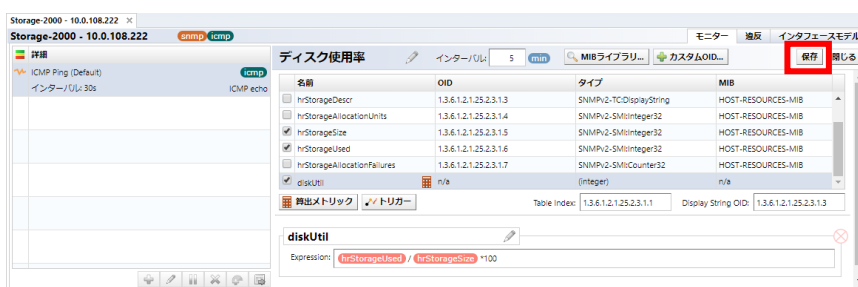
- [算出メトリック]→[カスタム計算式]をクリックします。



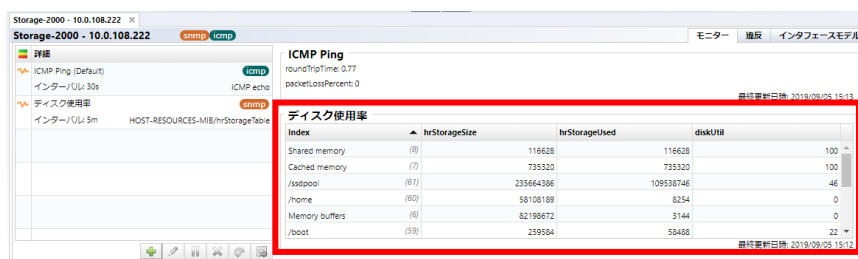
8. 名前と計算式を入力します。



9. [保存]をクリックします。



保存後、データ収集が開始され結果が表示されます。

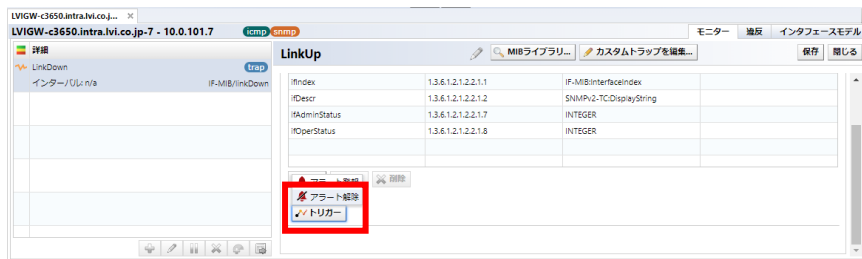


カスタム計算式を使用しても、計算後の値に対して、しきい値を設定することができます。しきい値設定については、[「5.3.4 しきい値を設定して監視する」](#)を参照してください。

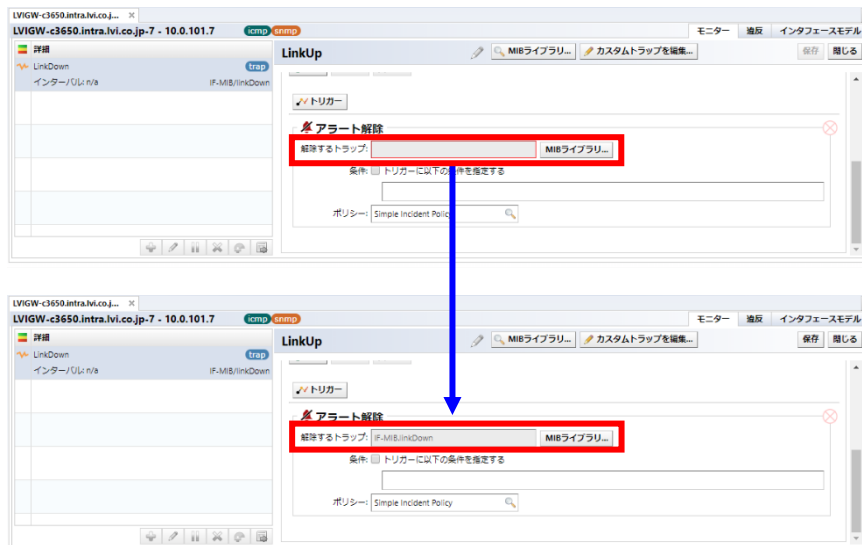
7.1.4 トラップ受信時に特定のトラップインシデントを自動でクリアする

関係関係にあるトラップを受信した際に、自動で障害をクリアし、マップ上のアイコンの色やステータスアイコンを通常の状態に戻すことができます。例えば、LinkDownトラップと LinkUpトラップです。LinkDownトラップを受信し障害としてインシデントが発生した後、LinkUpトラップを受信した時点で LinkDownトラップをクリアします。

1. LinkDownトラップのモニターを作成します。
2. LinkUp用のSNMPトラップモニターを作成します。
3. [トリガー]をクリックし、[期間]をクリックします。



4. 解除するトラップの[MIBライブラリ]をクリックし、LinkDownトラップを追加します。



5. [保存]をクリックします。

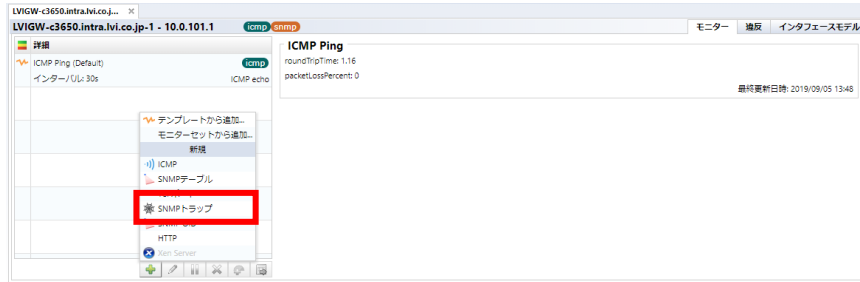


7.1.5 トラップに含まれる値でアクションを変える

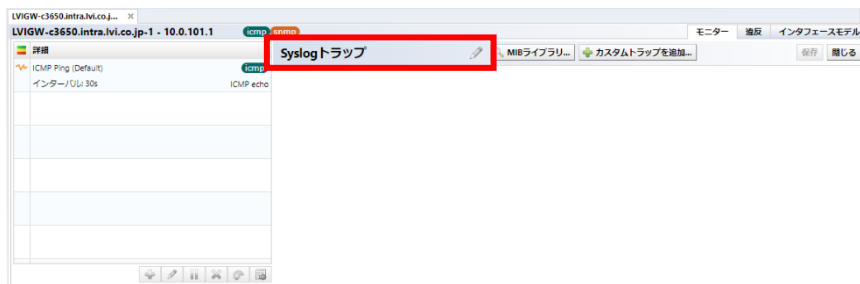
監視対象機器は、トラップを送信する際に様々な情報をトラップに入れて送信します。その内容によっては、障害として検知したくない場合もあります。ThirdEye では、条件指定してフィルタリングすることができます。

以下の例では、Cisco 社機器の Syslogトラップを使用してトラップをフィルタリングしています。

1. SNMPトラップモニターを追加します。



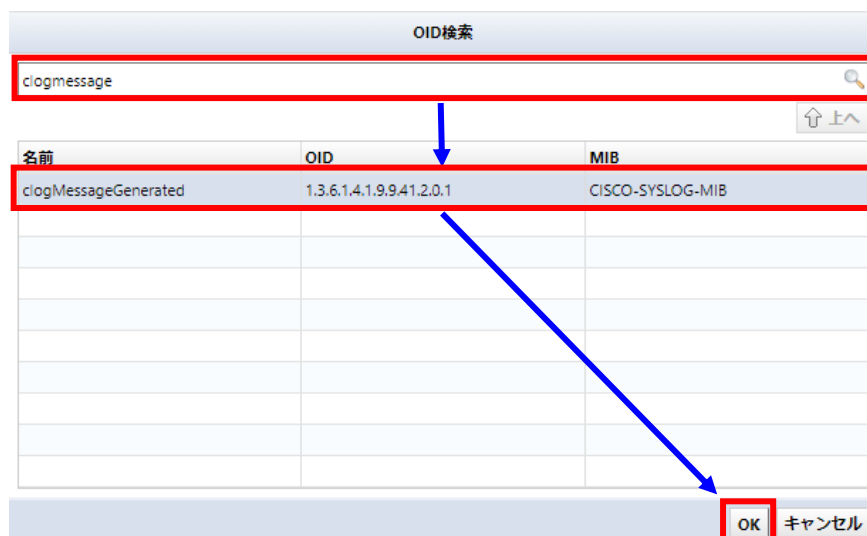
2. 任意のモニター名を表示します。



3. [MIB ライブラリ]をクリックします。

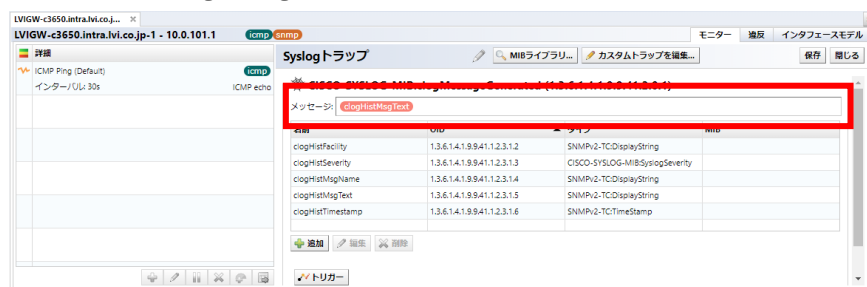


- OID 検索に「clogmessage」と入力し、検索結果から「clogMessageGenerated」を選択し[OK]をクリックします。

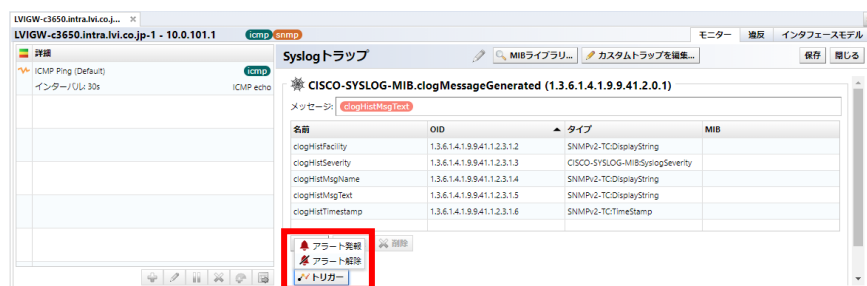


- 障害発生時のメッセージを入力します。

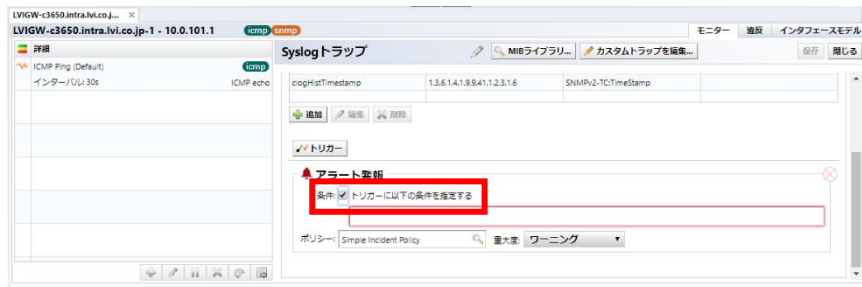
※以下では、トラップに含まれる clogHitMsgText(メッセージ内容)を表示します。



- [トリガー]をクリックし、[アラート発報]をクリックします。



7. 「条件」にチェックを入れます。



8. 赤枠に「条件」を入力します。



上記例では、clogHistSeverity が error 以上(emergency、alert、critical)、かつ clogHistMsgText の値に「LogicVein」が含まれない場合がアラート対象となります。

メモ:なぜ「clogHistSeverity < error」が emergency、alert、critical となるのか？

機器から clogHistSeverity の情報が送信される時、値には「数字」で送信されます。ThirdEye では、MIB 定義に基づいて 数字 を 文字列 に変換して表示します。MIB ファイルから clogHistSeverity の定義を確認すると、右記のように記載されています。この場合の条件式は、「clogHistSeverity < 4(error)」となるため、アラート対象が 4 より小さい emergency (1)、alert (2)、critical (3) が条件に該当することになります。

```
SYNTAX INTEGER
{
  emergency(1),
  alert(2),
  critical(3),
  error(4),
  warning(5),
  notice(6),
  info(7),
  debug(8)
}
```

9. ポリシーと重大度を設定します。



10. [保存]をクリックします。



7.2 Agent-D を使用した監視 Enterprise Suite

Agent-D は、サーバ監視のための SNMP エージェントです。Windows または Linux ベースの OS に Agent-D をインストールすることで、サーバの CPU やメモリ、ログなどを監視できるようになります。

7.2.1 Windows にインストールする

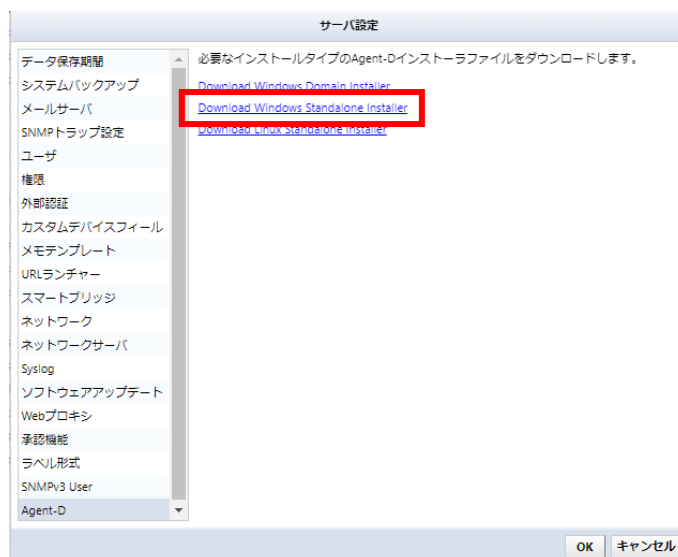
(1) Agent-D を手動でインストールする

ThirdEye からインストーラをダウンロードし、任意の Windows サーバにインストールします。サポートされている Windows OS は、Windows Server 2016/2019 です。

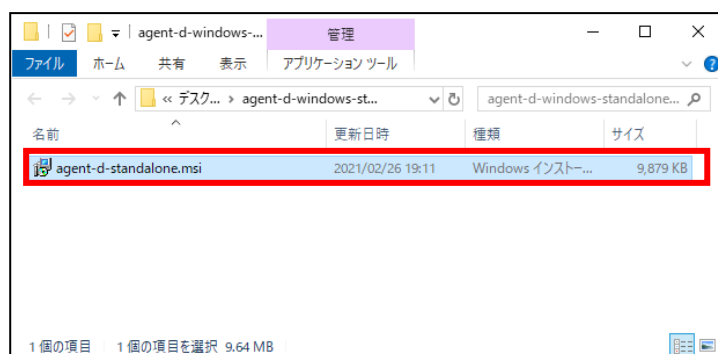
1. グローバルメニューの[設定]をクリックします。



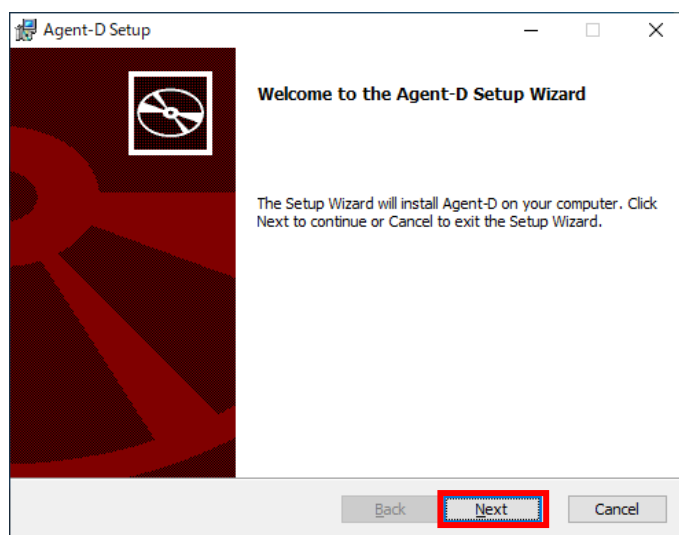
2. [Agent-D]をクリックし、[Download Windows Standalone Installer]をクリックします。



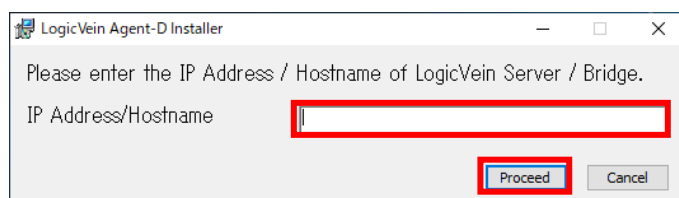
3. ダウンロードしたファイルをインストールする Windows サーバにコピーします。
4. ダウンロードしたファイルを解凍し、「agent-d-standalone.msi」をダブルクリックして実行します。



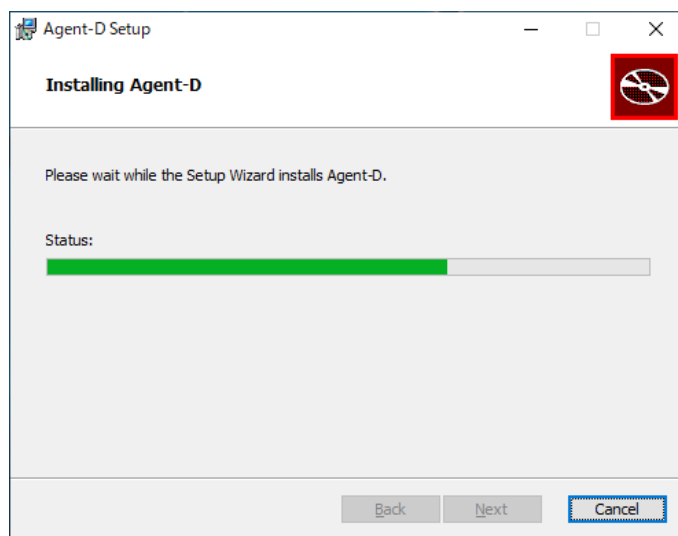
5. [Next]をクリックします。



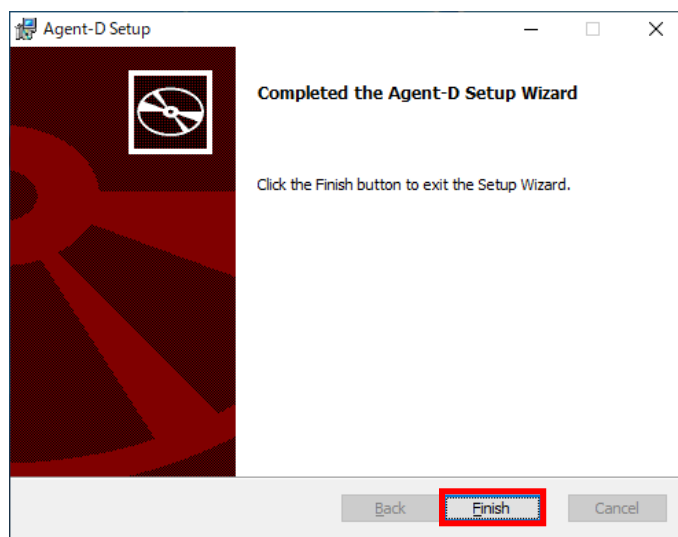
6. ThirdEye の IP アドレスまたはホスト名を入力し、[Proceed]をクリックします。



7. インストールが開始されます。

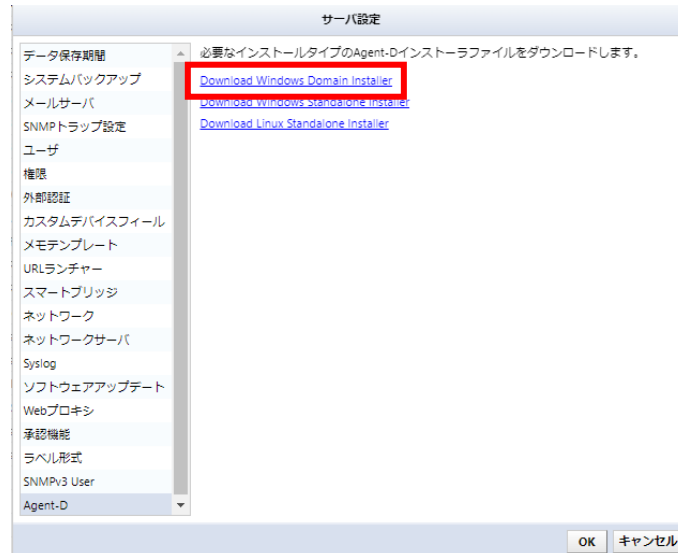


8. [Finish]をクリックします。



(2) ドメインコントローラーのグループポリシーを利用して、Agent-D を配布およびインストールする

新規または既存の Active Directory のグループポリシーを使用して、複数のサーバ上に一括して Agent-D をインストールできます。グローバルメニューの[設定]→[Agent-D]→[Download Windows Domain Installer]をクリックすると、MSI ファイルをダウンロードできます。



詳細については Microsoft Docs の案内をご確認ください。

Microsoft Docs:「グループ ポリシーを使用してソフトウェアをリモートでインストールする」

<https://docs.microsoft.com/ja-jp/troubleshoot/windows-server/group-policy/use-group-policy-to-install-software>

7.2.2 Linux にインストールする

(1) ThirdEye から Agent-D を配布およびインストールする

Linux の場合、ThirdEye から Linux に SSH 接続できる環境であれば、Agent-D を ThirdEye のメニューからインストールできます。

1. SSH 接続するための認証情報(ユーザ名/パスワード)を設定します。

※追加方法については、「[5.1 クレデンシャルを設定する](#)」を参照してください。以下の画像は、ダイナミッククレデンシャルを使用した場合の一例です。

クレデンシャル

ネットワークグループ

- Linux credential
- Default

192.168.40.200

192.168.40.59

アドレスを追加:

(IP・CIDR・ワイルドカード・アドレス範囲)

クレデンシャル

New Credentials

VTY Username: lviAdmin

VTY Password:

Enable Username:

Enable Secret/Password:

SNMP Get Community:

SNMPv3 Authentication Username:

SNMPv3 Authentication Password:

SNMPv3 Privacy Password:

OK キャンセル

2. 監視対象の Linux デバイスを追加します。

※追加方法については、「[5.2 デバイスを追加する](#)」を参照してください。以下の画像は、1 台ずつ登録する場合の一例です。

デバイスの追加

IPアドレス: 192.168.40.200

アダプタを識別できないSSHホストにLinuxアダプタを割り当てる

OK キャンセル

3. 監視対象の Linux デバイスが選択された状態で、デバイスメニューの[Agent-D Linux インストーラ]をクリックします。

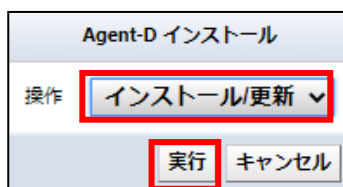


[Agent-D Linux インストーラ]がグレーアウトして選択できない場合、選択しているデバイスに Linux アダプタが割り当てられていない可能性があります。対象デバイスに Linux アダプタが割り当てられていることを確認してください。デバイスメニューの[デバイスプロパティの編集]から確認できます。

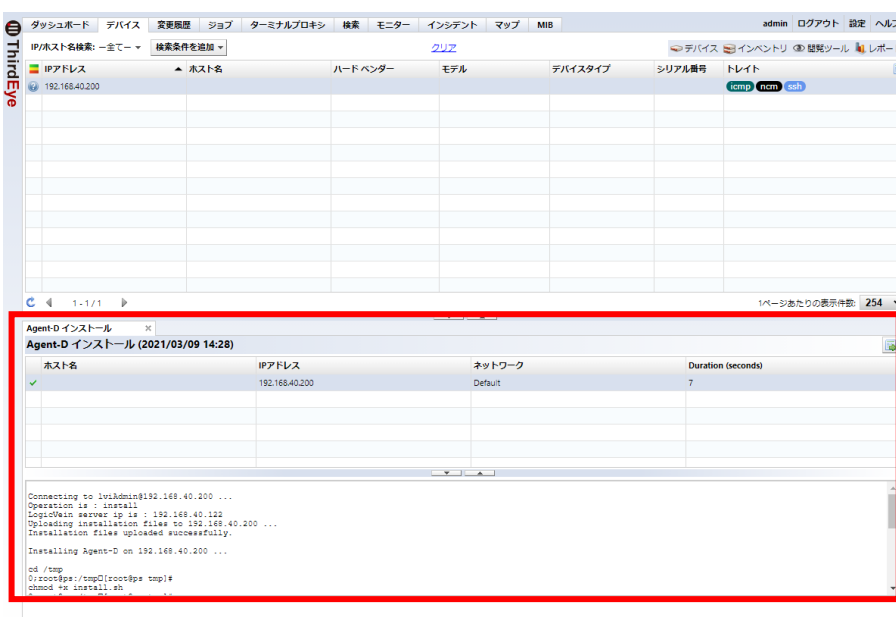
補足



4. [インストール/更新]を選択し、[実行]をクリックします。



5. インストールが実行され、画面下半分に結果が表示されます。



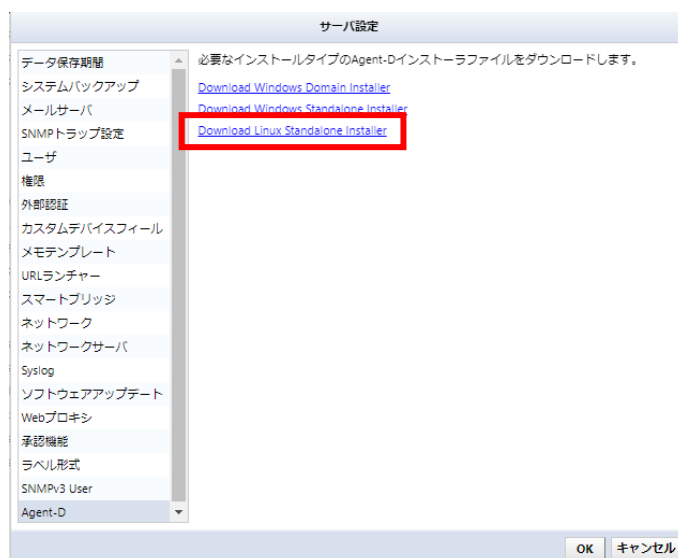
(2) Agent-Dを手動でインストールする

ThirdEye からインストーラをダウンロードし、任意の Linux にインストールします。サポートされている OS は、RedHat Linux 7/8、CentOS 7/8、Ubuntu です。

1. グローバルメニューの[設定]をクリックします。



2. [Agent-D]をクリックし、[Download Linux Standalone Installer]をクリックします。



3. ダウンロードしたファイルをインストール先の Linux サーバにコピーします。
4. unzip コマンドを使用してダウンロードしたファイルを解凍します。

```
[lviAdmin@fcent8 ~]$ unzip agent-d-linux-installer.zip
Archive: agent-d-linux-installer.zip
  inflating: uninstall.sh
  inflating: telegraf.sudoers
  inflating: telegraf.service
  inflating: telegraf.logrotate
  inflating: telegraf.conf
  inflating: telegraf.bin
  inflating: telegraf-wrapper
  inflating: telegraf-revision
  inflating: install_common.sh
  inflating: install.sh
  inflating: init.sh
[lviAdmin@fcent8 ~]$ ls
agent-d-linux-installer.zip  install.sh          telegraf-revision  telegraf.bin      telegraf.logrotate  telegraf.sudoers
init.sh                     install_common.sh  telegraf-wrapper  telegraf.conf     telegraf.service    uninstall.sh
[lviAdmin@fcent8 ~]$
```

5. install.sh を実行します。

```
[lviAdmin@fcent8 ~]$ sudo sh install.sh
Enter LogicVein server IP address: 192.168.40.112
Source IP address: 192.168.40.59
Adding Agent-D user...
Copying Agent-D files...
Agent-D files copied successfully.

Starting Agent-D service...
Created symlink /etc/systemd/system/multi-user.target.wants/telegraf.service → /usr/lib/systemd/system/telegraf.service.
Redirecting to /bin/systemctl restart telegraf.service
Checking Agent-D status...

Redirecting to /bin/systemctl status telegraf.service
Agent-D service started successfully.

Agent-D installation successful.
[lviAdmin@fcent8 ~]$
```

6. ThirdEye の IP アドレスを入力し、「Enter」キーを押します。

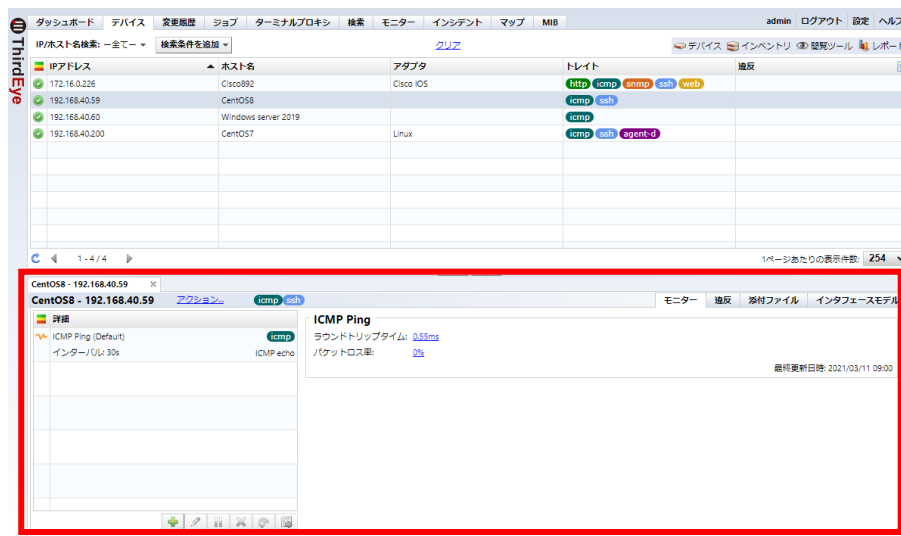
7.2.3 CPU 監視


Agent-D を使用して、インストールされているサーバの CPU 情報を取得します。CPU 使用率などにしきい値を設定することで、しきい値を超過した時にアラートを発報することができます。[モニター]→[テンプレート]には、あらかじめ以下のテンプレートが CPU 監視用のモニターとして登録されています。

- Linux CPU Stats
- Windows CPU Stats

ここでは、[Agent-D]→[Linux CPU]プラグインを CentOS デバイスのモニターとして設定する場合を例に説明します。モニターセットを利用する場合は、「[5.3.7 モニターセットを使用して多数の機器に対して監視設定をする](#)」を参照してください。

1. モニターを設定するデバイスをダブルクリックし、デバイス詳細を開きます。



2. [ (追加)] をクリックし、[Agent-D] をクリックします。



- 任意のモニター名を入力し、[インターバル]および[データ保存期間]を設定します。



- [Plugin Library...]をクリックします。



- [Linux CPU]を選択し、[OK]をクリックします。

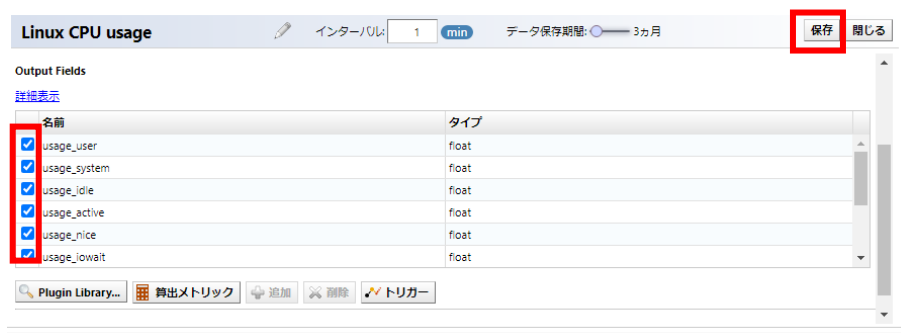


6. Plugin Config で取得する項目にチェックを入れます。



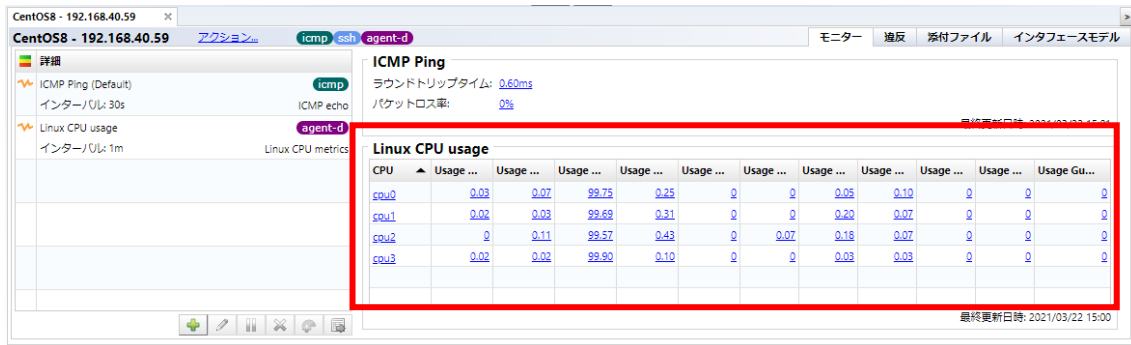
項目	説明
生の CPU 時間メトリックを収集します (collect_cpu_time)	CPU が使用された時間を収集します。チェックがない場合は、Output fields で time_から始める Field にチェックを入れても値は表示されません。
生の非アイドル CPU 状態の合計を計算して表示します (report_active)	Idle/guest/guest_nice 以外の値の合計値を算出します。チェックがない場合は、Output fields で time_active/usage_active にチェックを入れても値は表示されません。

7. Output Fields で取得する項目にチェックを入れ、[保存]をクリックします。



補足 Agent-D の [Output Fields] では、一般的な監視項目にデフォルトでチェックが入っています。その他の監視項目を表示するには、[詳細表示]をクリックします。

以上で、Agent-D から CPU の情報が送信され、デバイス詳細で確認することができます。



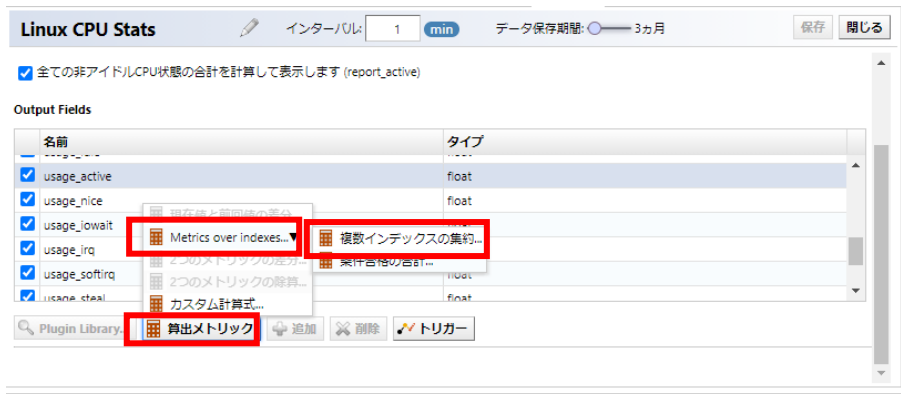
(1) CPU 全体の使用率を取得する

Agent-D の CPU モニターは、コア毎の情報を取得します。CPU 全体の使用率を取得するためには、算出メトリックを使用します。

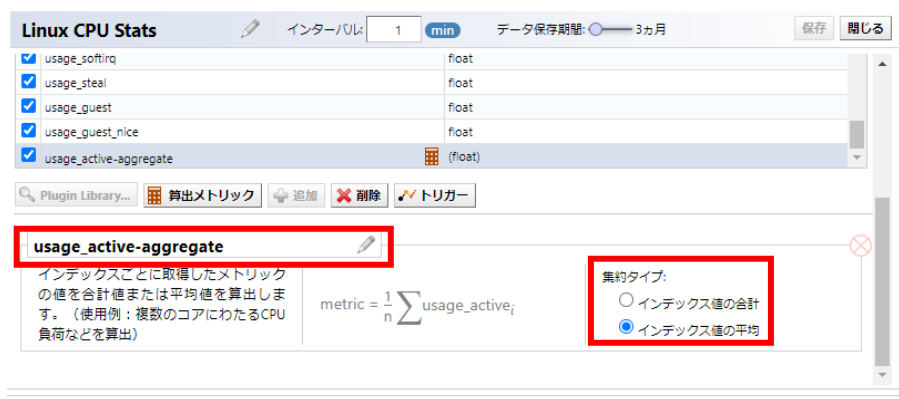
1. CPU モニターをダブルクリックで開きます。
2. [usage_active]を Output Fields からクリックします。



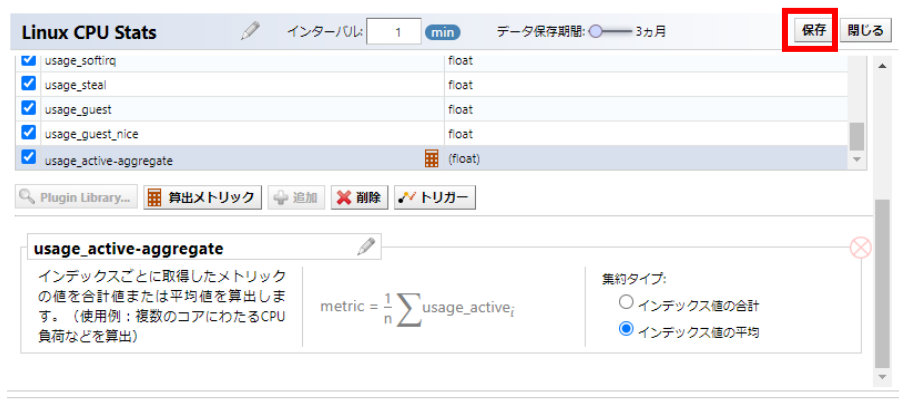
3. [算出メトリック]→[Metrics over indexes]→[複数インデックスの集約]をクリックします。



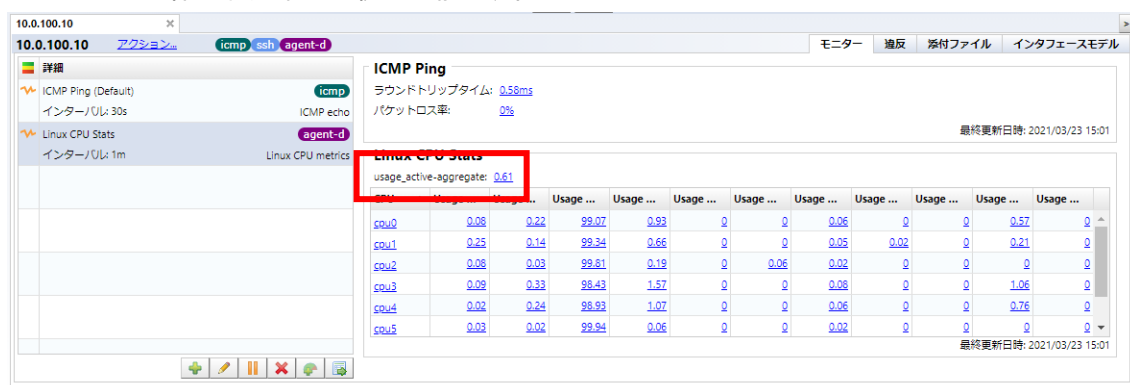
4. メトリック名(ここでは usage_active-aggregate)を分かりやすい名前に変更し、集約タイプを選択します。



5. [保存]をクリックします。



以上で、各インデックス(各コア)の usage_active を集約した値を表示することができます。これに対してしきい値を設定することで CPU 全体の利用率の監視が可能です。



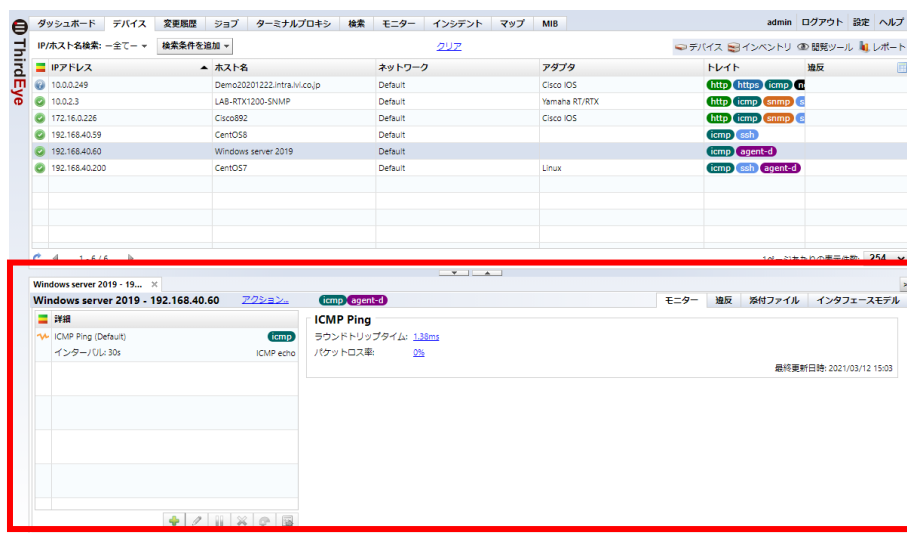
7.2.4 メモリ監視

Agent-D を使用して、インストールされているサーバのメモリ情報を取得します。メモリ使用率などにしきい値を設定することで、しきい値を超過した時にアラートを発報することができます。[モニター]→[テンプレート]には、あらかじめ以下のテンプレートがメモリ監視用のモニターとして登録されています。

- Linux Memory Stats
- Windows Memory Stats

ここでは、[Agent-D]→[Windows Memory]プラグインを Windows サーバのモニターとして設定する場合を例に説明します。モニターセットを利用する場合は、「[5.3.7 モニターセットを使用して多数の機器に対して監視設定をする](#)」を参照してください。

1. モニターを設定するデバイスをダブルクリックし、デバイス詳細を開きます。



2. [ (追加)] をクリックし、[Agent-D] をクリックします。



3. 任意のモニター名を入力し、[インターバル]および[データ保存期間]を設定します。



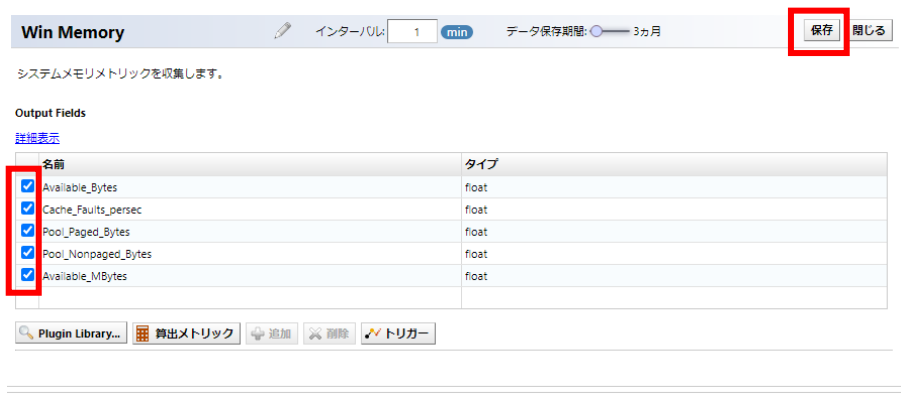
4. [Plugin Library...]をクリックします。



5. [Windows Memory]を選択し、[OK]をクリックします。

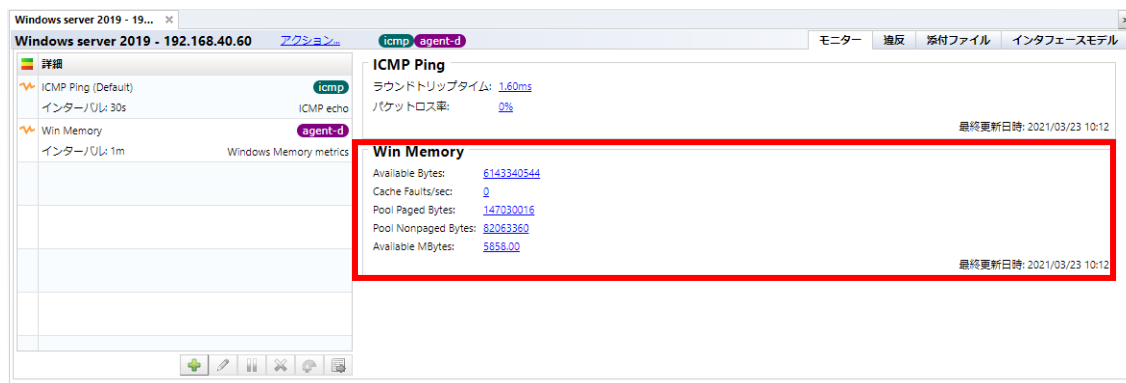


6. [Output Fields]でデータを取得する項目にチェックを入れ、[保存]をクリックします。



補足 Agent-D の[Output Fields]では、一般的な監視項目にデフォルトでチェックが入っています。その他の監視項目を表示するには、[詳細表示]をクリックします。

以上で、Agent-D からメモリの情報が送信され、デバイス詳細で確認することができます。



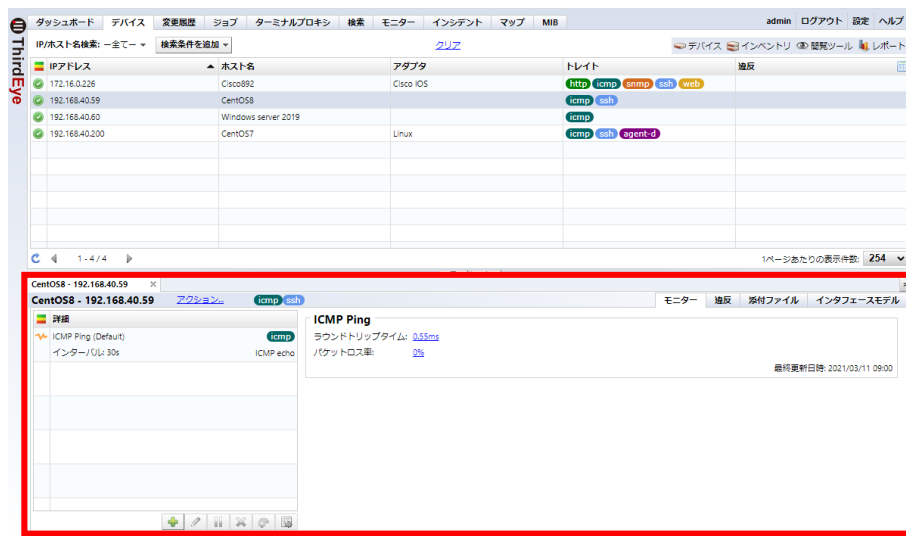
7.2.5 HDD 監視

Agent-D を使用して、インストールされているサーバの HDD 情報を取得します。HDD の空き容量や使用率などにしきい値を設定することで、しきい値を超過した時にアラートを発報することができます。[モニター]→[テンプレート]には、あらかじめ以下のテンプレートが HDD 監視用のモニターとして登録されています。

- Linux Disk Stats
- Windows Disk Stats

ここでは、[Agent-D]→[Linux Disk]プラグインを CentOS デバイスのモニターとして設定する場合を例に説明します。モニターセットを利用する場合は、「[5.3.7 モニターセットを使用して多数の機器に対して監視設定をする](#)」を参照してください。

1. モニターを設定するデバイスをダブルクリックし、デバイス詳細を開きます。



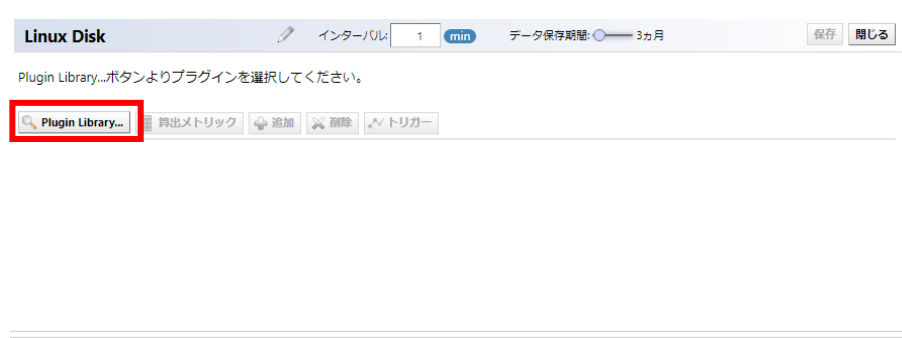
2. [ (追加)] をクリックし、[Agent-D] をクリックします。



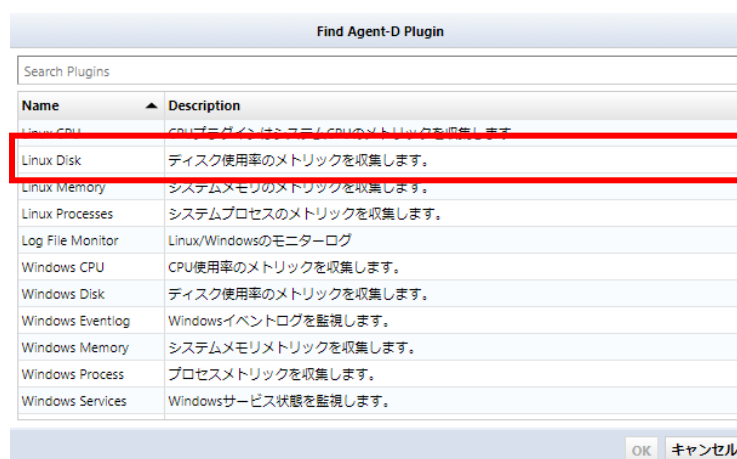
3. 任意のモニター名を入力し、[インターバル]および[データ保存期間]を設定します。



4. [Plugin Library...]をクリックします。

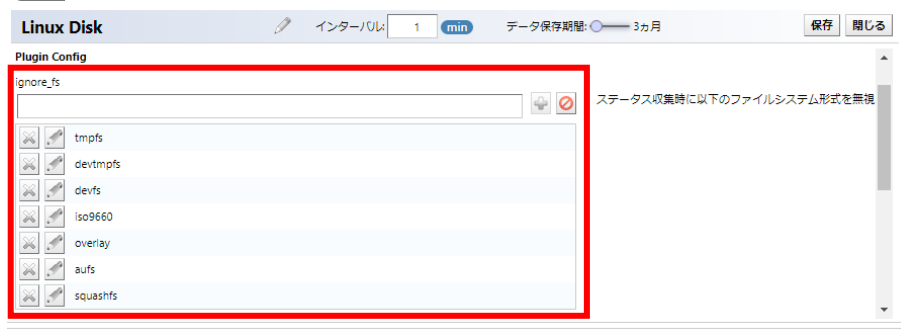


5. [Linux Disk]を選択し、[OK]をクリックします。

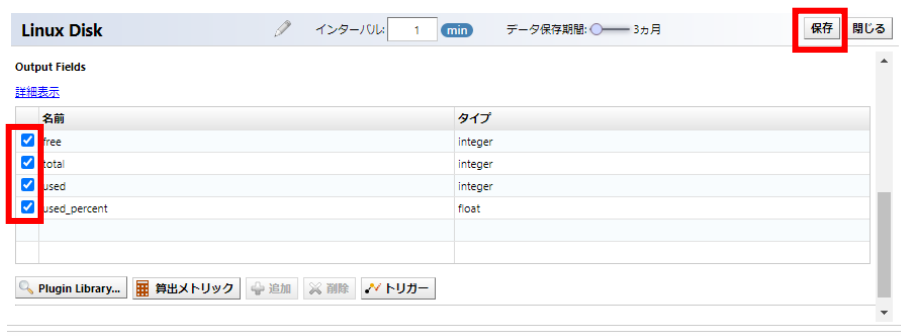


6. [ignore_fs]欄で、データ収集から除外するファイルシステムを指定します。

※除外リストには、あらかじめいくつかのファイルシステムが設定されています。必要に応じて[+] (追加)、[-] (削除)で編集します。

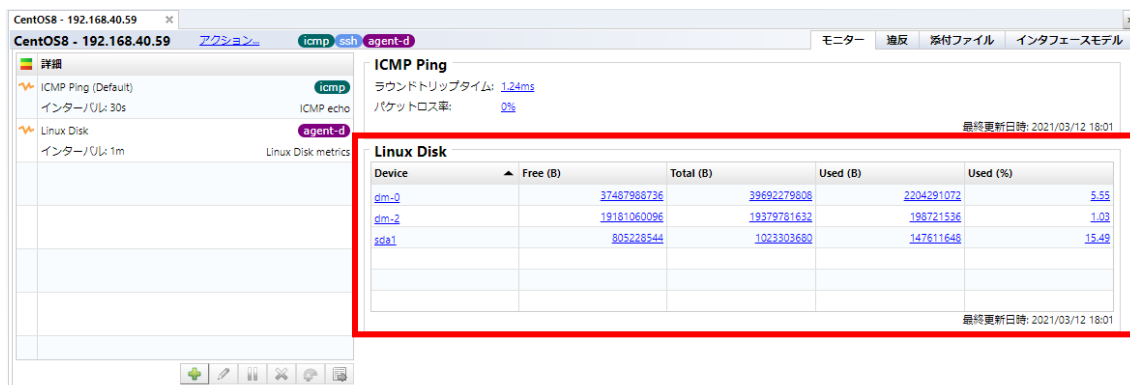


7. [Output Fields]で取得する項目にチェックを入れ、[保存]をクリックします。



補足 Agent-D の [Output Fields] では、一般的な監視項目にデフォルトでチェックが入っています。その他の監視項目を表示するには、[詳細表示]をクリックします。

以上で、Agent-D から HDD の情報が送信され、デバイス詳細で確認することができます。



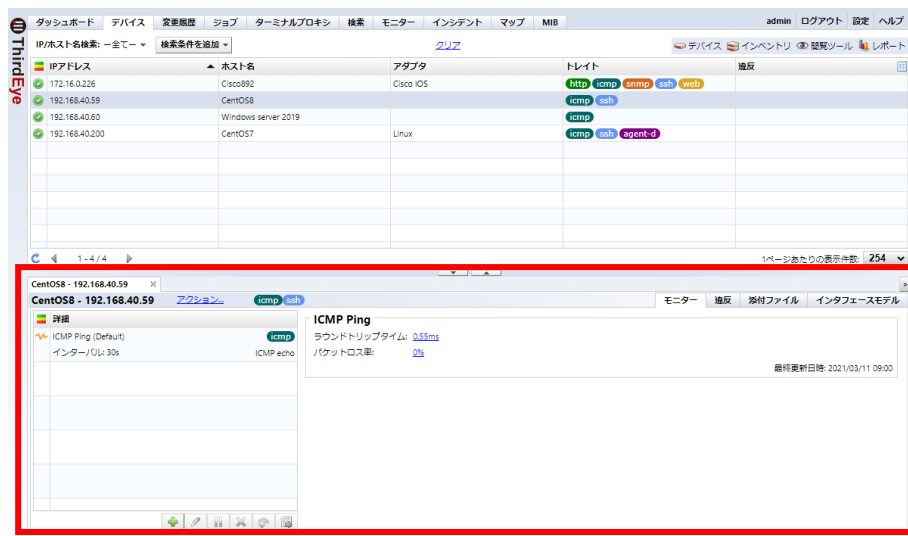
7.2.6 プロセス監視

Agent-D を使用して、インストールされているサーバのプロセスの情報を取得します。プロセスのステータスやメモリ使用量などにしきい値を設定することで、しきい値を超過した時にアラートを発報することができます。[モニター]→[テンプレート]には、あらかじめ以下のテンプレートがプロセス監視用のモニターとして登録されています。

- Linux Process Stats
- Windows Process Stats

ここでは、[Agent-D]→[Windows Process]プラグインを Windows サーバのデバイスのモニターとして設定する場合を例に説明します。モニターセットを利用する場合は、「[5.3.7 モニターセットを使用して多数の機器に対して監視設定をする](#)」を参照してください。

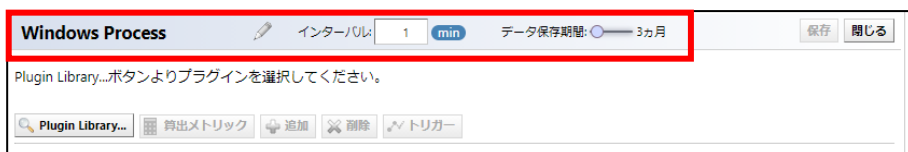
1. モニターを設定するデバイスをダブルクリックし、デバイス詳細を開きます。



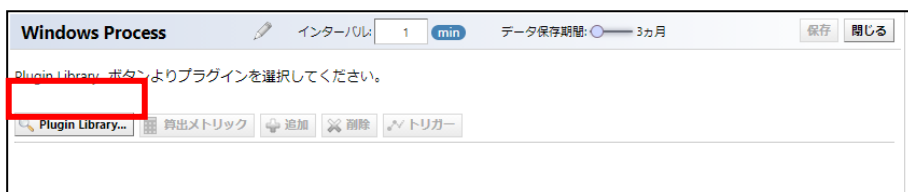
2. 追加をクリックし、[Agent-D]をクリックします。



3. 任意のモニター名を入力し、[インターバル]および[データ保存期間]を設定します。



4. [Plugin Library...]をクリックします。

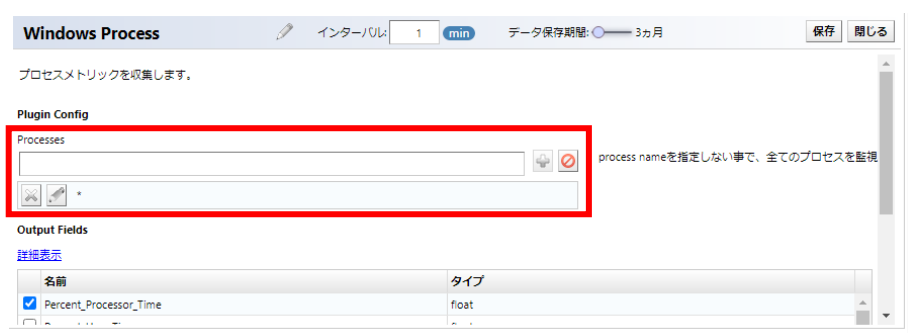


5. [Windows Process]を選択し、[OK]をクリックします。

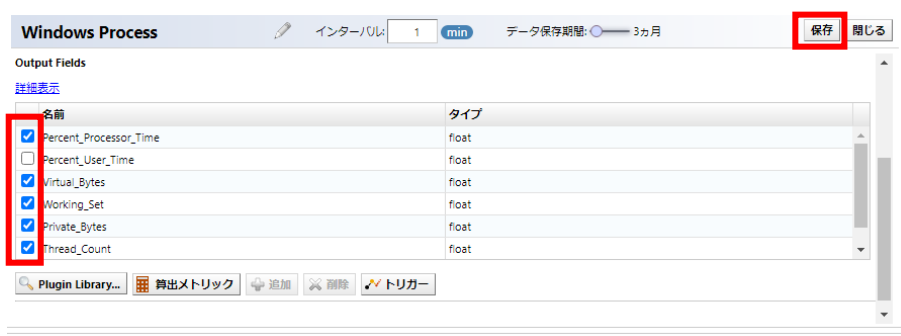


6. 特定のプロセスに関する情報のみをモニター表示したい場合は、[Processes]欄に対象のプロセス名を入力して追加します。入力しない場合は、全てのプロセスのデータが収集されます。

※通常、このパラメータはデフォルト設定のままです。

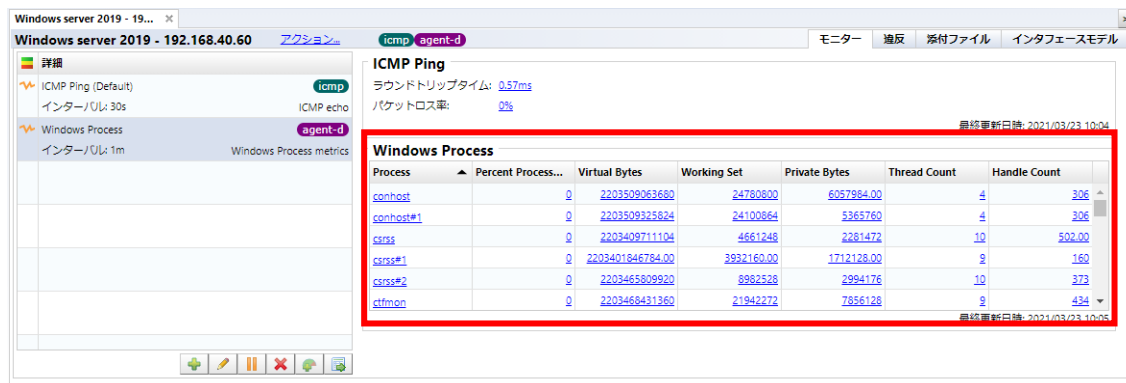


7. [Output Fields]で取得する項目にチェックを入れ、[保存]をクリックします。



補足 Agent-D の[Output Fields]では、一般的な監視項目にデフォルトでチェックが入っています。その他の監視項目を表示するには、[詳細表示]をクリックします。

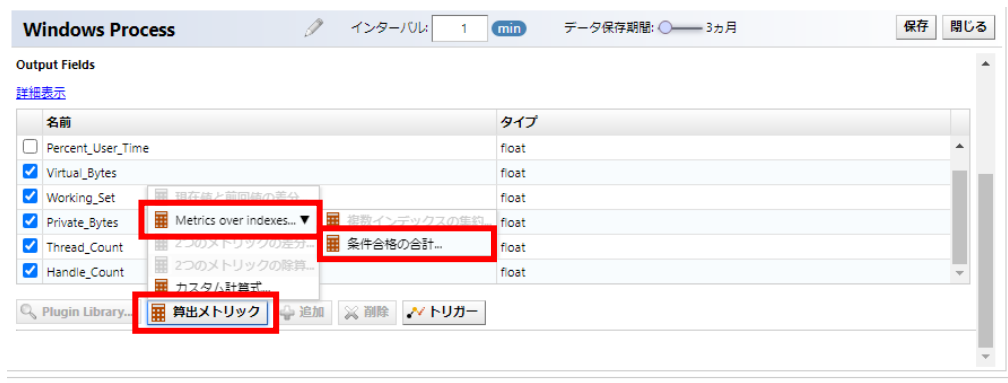
以上で、Agent-D からプロセスの情報が送信され、デバイス詳細で確認することができます。



(1) プロセス数を監視する

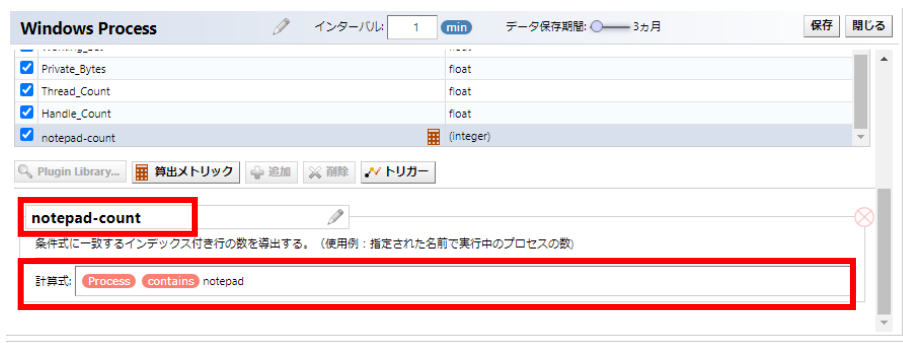
実行中のプロセス数を監視する場合、プロセス数をカウントするためのメトリックを追加する必要があります。

1. プロセスのモニターをダブルクリックで開きます。
2. [算出メトリック]→[Metrics over indexes]→[条件合格の合計]の順にクリックします。



3. count メトリック名を分かりやすい名前に変更し、計算式を設定します。

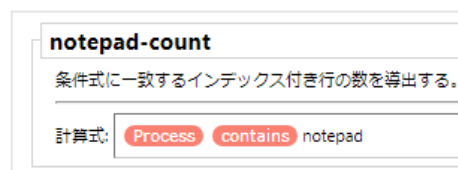
(下図では、メトリック名が初期値の「count-metric」から「notepad-count」に変更しています)



- Windows の場合、プロセス名は「Process」に対して設定します。

(設定例)

計算式: **Process** **contains** {プロセス名}



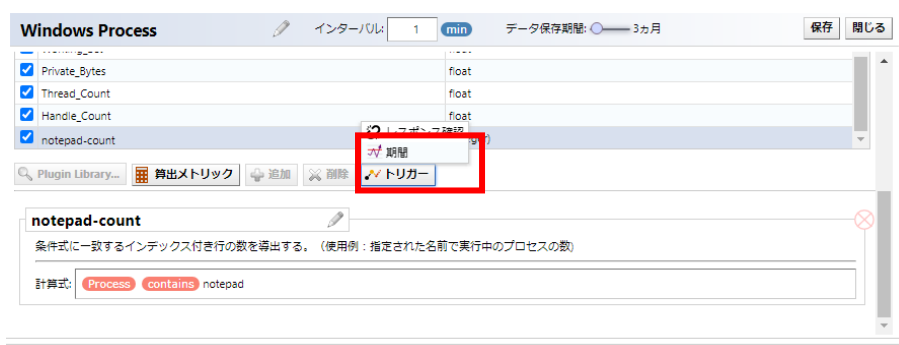
- Linux の場合、プロセス名は「process_name」に対して設定します。

(設定例)

計算式: **process_name** **contains** {プロセス名}



4. [トリガー]→[期間]をクリックします。



5. 作成した *count* メトリックを使用して条件を設定します。



項目	説明
条件	<p>以下の項目を使って、条件を指定することができます。</p> <ul style="list-style-type: none"> • is (等しい) • is not (等しくない) • > (より小さい、右の値のほうが小さい) • < (より大きい、右の値のほうが大きい)

6. そのほかの項目(アラートポリシー/重大度/期間/カウント/メッセージ)を設定します。



項目	説明
期間	処理を実行するための期間を設定します。(最小値: 1 分) 定められた期間内に何回失敗(カウント)したらポリシーに定義された処理を実行するのか、カウントの基準となる期間。
カウント	設定期間内に何回失敗したら処理を実行するかを設定します。(最小値: 1)
アラートポリシー	アラートポリシーを指定します。
重大度	重大度を次の中から選択します。(初期値: ワーニング) 「エマージェンシー」、「アラート」、「クリティカル」、「エラー」、「ワーニング」、「通知」、「情報」、「デバッグ」
メッセージ	障害検知時に表示されるメッセージを設定します。 ※メッセージを表示させるためには、アラートポリシーに「インシデント登録」アクションが定義されている必要があります。

7. [保存]をクリックします。



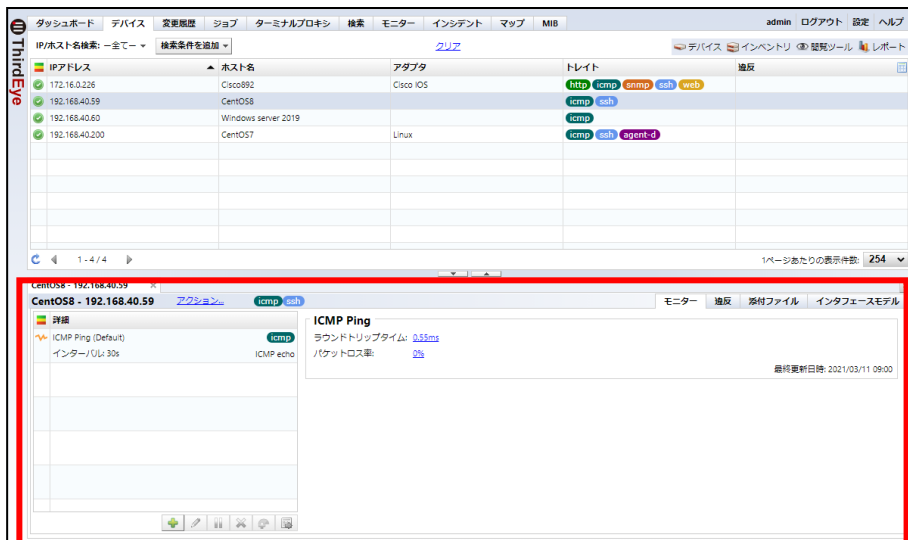
7.2.7 Windows サービス監視


Agent-D を使用して、インストールされている Windows サーバの Windows サービスの情報を取得します。サービスのステータスにしきい値を設定することで、しきい値を超過した時にアラートを発報することができます。[モニター]→[テンプレート]には、あらかじめ以下のテンプレートが Windows サービス監視用のモニターとして登録されています。

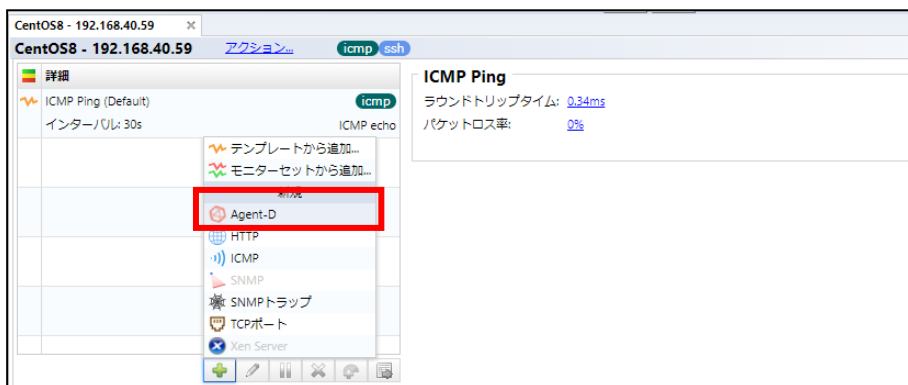
- Windows Service Status

ここでは、[Agent-D]→[Windows Services]プラグインを Windows サーバのデバイスのモニターとして設定する場合を例に説明します。モニターセットを利用する場合は、「[5.3.7 モニターセットを使用して多数の機器に対して監視設定をする](#)」を参照してください。

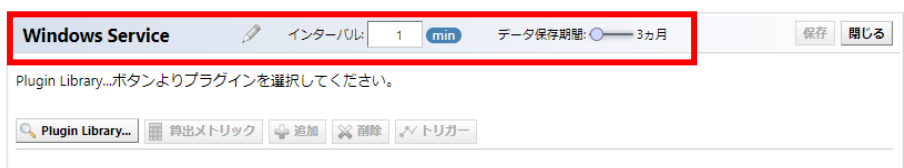
1. モニターを設定するデバイスをダブルクリックし、デバイス詳細を開きます。



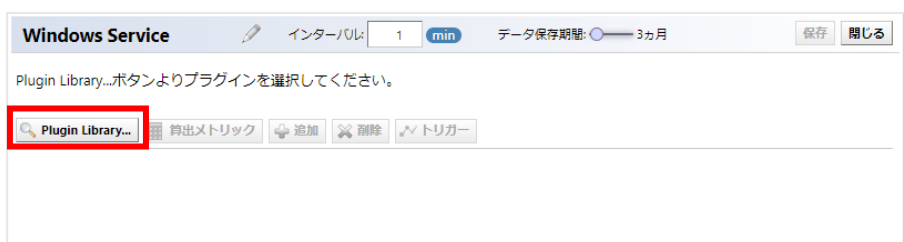
2. [ (追加)] をクリックし、[Agent-D] をクリックします。



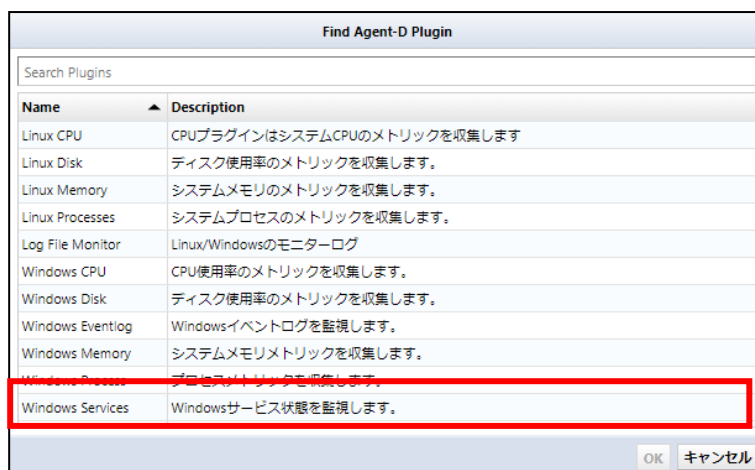
3. 任意のモニター名を入力し、[インターバル]および[データ保存期間]を設定します。



4. [Plugin Library...]をクリックします。

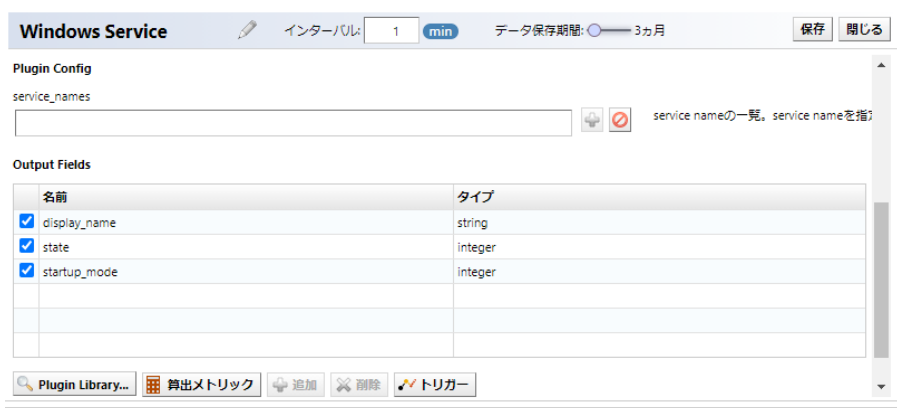


5. [Windows Services]を選択し、[OK]をクリックします。

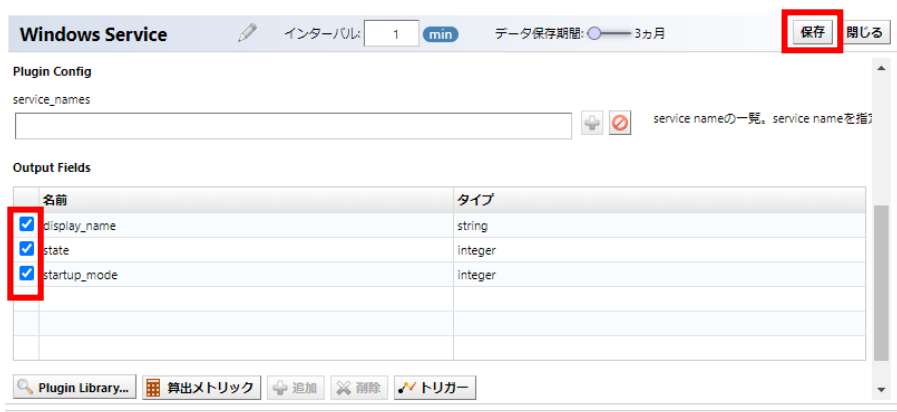


6. 特定のプロセスに関する情報のみをモニター表示したい場合は、[service_names]欄に対象のサービス名を入力して追加します。入力しない場合は、全てのサービスのデータが収集されます。サービス名は完全一致です。(大文字小文字の区別はありません)

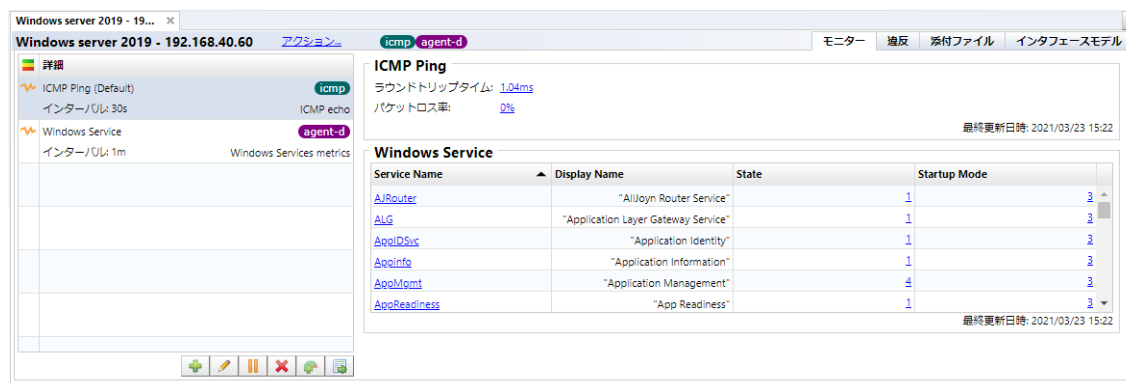
※通常、このパラメータはデフォルト設定のまま構いません。



7. [Output Fields]で取得する項目にチェックを入れ、[保存]をクリックします。



以上で、Agent-D からサービスの情報が送信され、デバイス詳細で確認することができます。



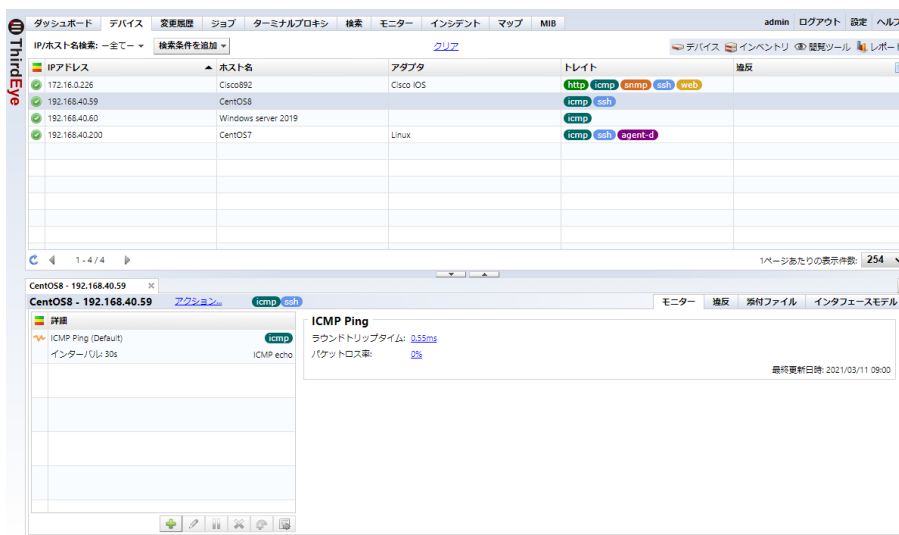
7.2.8 テキストログ監視

Agent-D を使用して、インストールされているサーバのログ情報を取得します。特定の文字列を含むログを検出した時にアラートを発報することができます。[モニター]→[テンプレート]には、あらかじめ以下のテンプレートがログ監視用のモニターとして登録されています。

- Linux Syslog Monitor
- Windows Log File Monitor

ここでは、[Agent-D]→[Log File Monitor]プラグインを Linux デバイスのモニターとして設定する場合を例に説明します。

1. モニターを設定するデバイスをダブルクリックし、デバイス詳細を開きます。



2. [ (追加)] をクリックし、[Agent-D] をクリックします。



3. 任意のモニター名を入力し、[インターバル]および[データ保存期間]を設定します。

The screenshot shows a configuration window for a monitor. The path is `/var/logs/messges`. The interval is set to 1 min. The data retention period is set to 3 months. There are buttons for '保存' (Save) and '閉じる' (Close). Below the path, there is a message: 'Plugin Library...ボタンよりプラグインを選択してください。' (Please select a plugin from the Plugin Library... button). There are also buttons for 'Plugin Library...', '算出メトリック' (Calculation Metric), '追加' (Add), '削除' (Delete), and 'トリガー' (Trigger).

4. [Plugin Library...]をクリックします。

The screenshot shows the same configuration window as above. The 'Plugin Library...' button is highlighted in red.

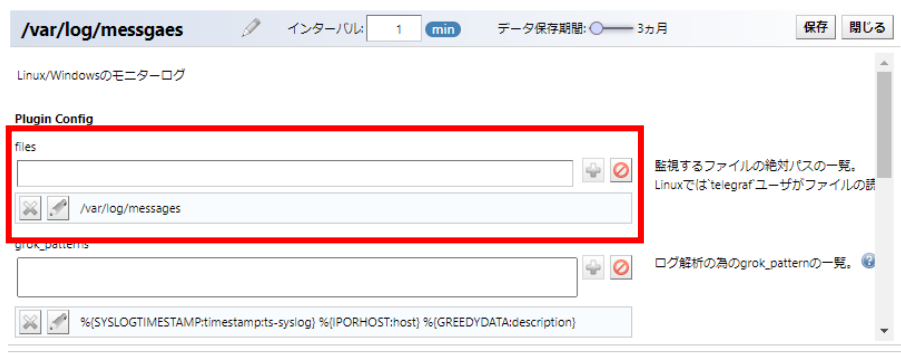
5. [Log Fie Monitor]を選択し、[OK]をクリックします。

The screenshot shows a dialog box titled 'Find Agent-D Plugin'. It has a search bar and a table of plugins. The 'Log File Monitor' plugin is highlighted in red.

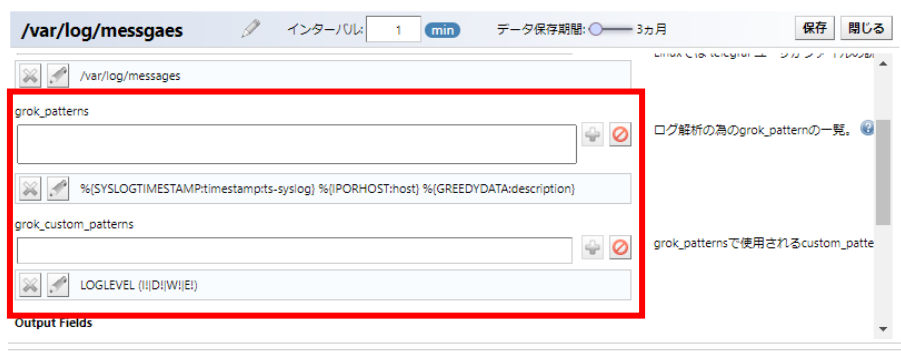
Name	Description
Linux CPU	CPUプラグインはシステムCPUのメトリックを収集します
Linux Disk	ディスク使用率のメトリックを収集します。
Linux Memory	システムメモリのメトリックを収集します。
Linux Processor	システムプロセスのメトリックを収集します
Log File Monitor	Linux/Windowsのモニターログ
Windows CPU	CPU使用率のメトリックを収集します。
Windows Disk	ディスク使用率のメトリックを収集します。
Windows Eventlog	Windowsイベントログを監視します。
Windows Memory	システムメモリメトリックを収集します。
Windows Process	プロセスメトリックを収集します。
Windows Services	Windowsサービス状態を監視します。

6. [files]欄に監視するログファイルを絶対パスで追加します。

※Agent-D プログラムが対象のログファイルを読み取れるように、事前にセキュリティ設定を行う必要があります。Windows では「SYSTEM」ユーザとして実行され、Linux では「telegraf」ユーザとして実行されます。



7. grok_patterns および grok_cusom_patterns を入力します。



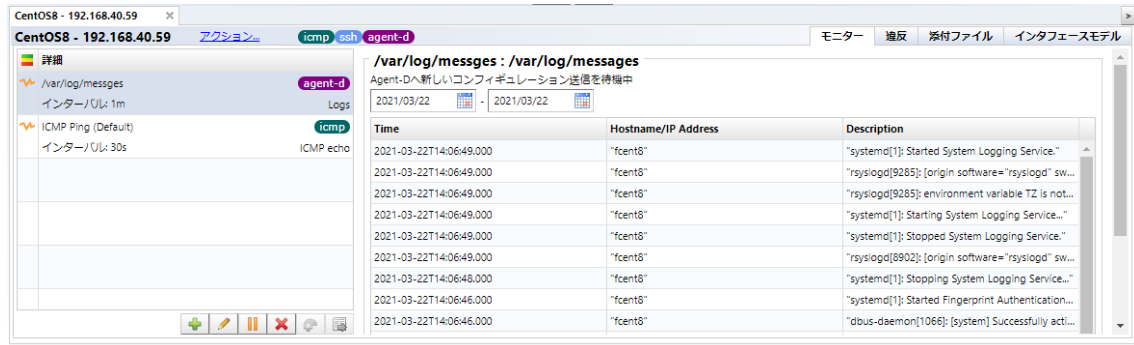
項目	説明
grok_patterns	<p>grok_pattern を使用して、1 行のログを分割し、指定した field と一致した文字を入れるための式を入力します。</p> <p>grok_pattern とは、 「<code>%(PATTERN_NAME:FIELD_NAME:MODIFIER(option))</code>」で構成され、正規表現を定義した PATTERN_NAME にマッチした内容を FIELD_NAME に入れます。</p> <p>例: ログメッセージ「Aug 20 11:15:40 192.168.0.1 ERROR systemd: Started Hostname Service.」</p> <p>式: <code>%(SYSLOGTIMESTAMP:timestamp)¥s%(IPORHOST:iporhost)¥s %[LOGLEVEL:level]¥s%(GREEDYDATA:message)</code></p> <ul style="list-style-type: none"> 「Aug 20 11:15:40」を SYSLOGTIMESTAMP というパターンを使用して times という field に値を保存する。 grok_pattern: <code>%(SYSLOGTIMESTAMP:timestamp)</code> 「192.168.0.1」を IPORHOST というパターンを使用して iporhost という field に値を保存する。 grok_pattern: <code>%(IPORHOST:iporhost)</code> 「ERROR」を LOGLEVEL というパターンを使用して level という field に値を保存する。 grok_pattern: <code>%(LOGLEVEL:level)</code>

項目	説明
	<ul style="list-style-type: none"> 「systemd: Started Hostname Service.」を GREEDYDATA というパターンを使用して message という field に値を保存する。 grok_pattern: %{GREEDYDATA:message}
grok_cusom_patterns	<p>grok_pattern で使用する PATTERN_NAME を新たに定義することができます。以下の構文で作成します。</p> <p>PATTERN_NAME (正規表現)</p>

8. [Output Fields]で取得する項目にチェックを入れ、[保存]をクリックします。



以上で、Agent-D からログ情報が送信され、デバイス詳細で確認することができます。

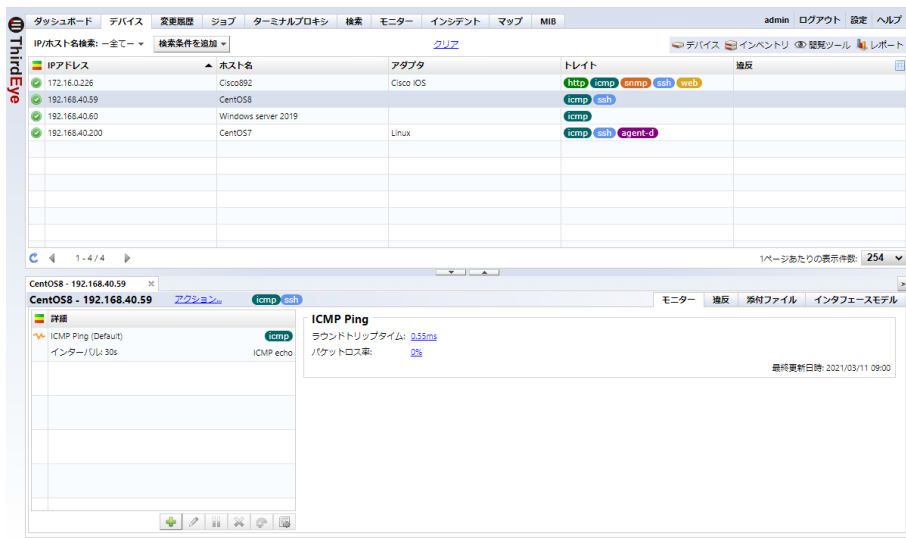



7.2.9 Windows イベントログ監視

Agent-D を使用して、インストールされている Windows サーバの Windows イベントログ情報を取得します。特定の文字列を含むイベントログを検出した時にアラートを発報することができます。[モニター] → [テンプレート] には、あらかじめ以下のテンプレートが Windows イベントログ監視用のモニターとして登録されています。

- Windows Event Log Monitor

1. モニターを設定するデバイスをダブルクリックし、デバイス詳細を開きます。



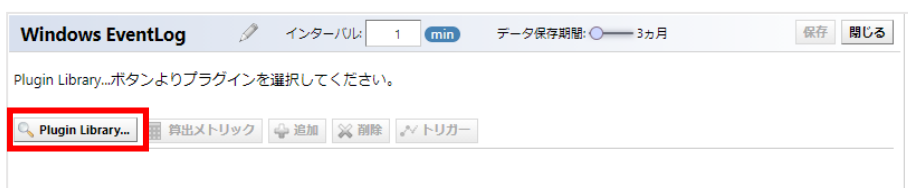
2. [ (追加)] をクリックし、[Agent-D] をクリックします。



3. 任意のモニター名を入力し、[インターバル]および[データ保存期間]を設定します。



4. [Plugin Library...]をクリックします。



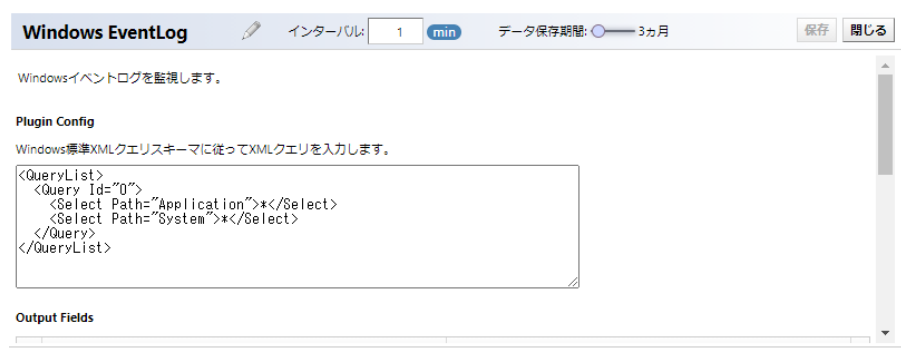
5. [Windows Eventlog]を選択し、[OK]をクリックします。



6. 監視するイベントログにチェックを入れます。



- 「高度な設定を使用」をクリックすると XML 形式で指定することができます。



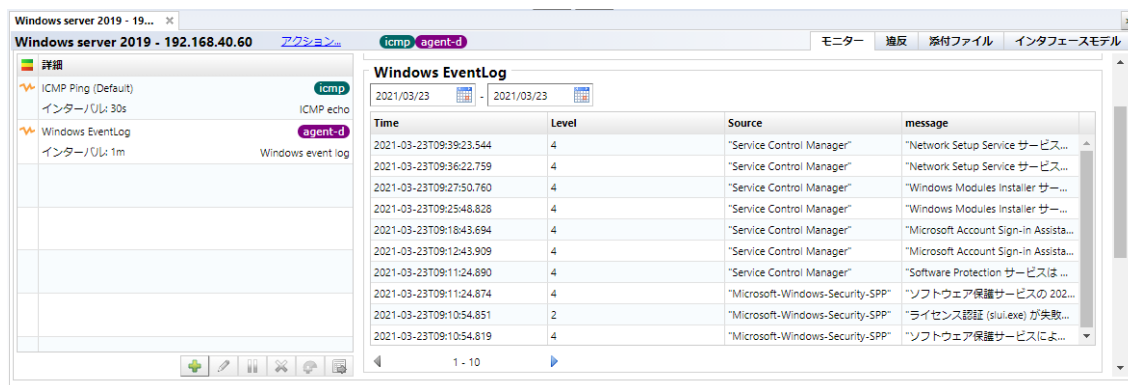
7. [Output Fields] で取得する項目にチェックを入れます。



8. [保存] をクリックします。



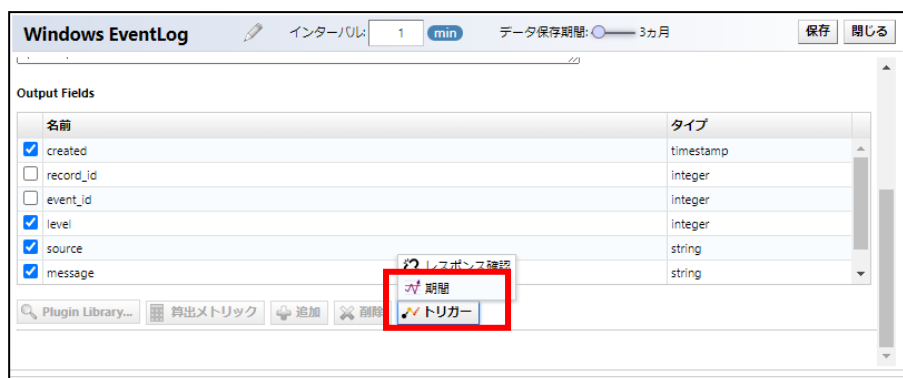
以上で、Agent-D からイベントログの情報が送信され、デバイス詳細で確認することができます。



(1) 任意の文字列が含まれる場合にアラート発報する

Windows イベントログの[全般]タブの内容は、Agent-D「Windows Eventlog」プラグインの「message」フィールドに表示されます。この「message」フィールドに特定の文字列が含まれるというフィルタ条件を設定することで、Windows イベントログに任意の文字列が含まれている場合にアラート発報させることができます。

1. イベントログのモニターをダブルクリックで開きます。
2. [トリガー]→[期間]をクリックします。



3. Agent-D の「message」を使用して条件を設定します。



項目	説明
条件	<p>以下の項目を使って、条件を指定することができます。</p> <ul style="list-style-type: none"> contains (含む) <p>※ そのほかの条件式(「is」, 「is not」, 「>」, 「<」, 「not contains」)を選択できますが、特定の文字列を含む条件を設定する場合は「contains」を使用してください。</p>

4. そのほかの項目(アラートポリシー/重大度/期間/カウント/メッセージ)を設定します。



項目	説明
期間	処理を実行するための期間を設定します。(最小値:1分) 定められた期間内に何回失敗(カウント)したらポリシーに定義された処理を実行するのか、カウントの基準となる期間。
カウント	設定期間内に何回失敗したら処理を実行するかを設定します。(最小値:1)
アラートポリシー	アラートポリシーを指定します。
重大度	重大度を次の中から選択します。(初期値:ワーニング) 「エマージェンシー」、「アラート」、「クリティカル」、「エラー」、「ワーニング」、「通知」、「情報」、「デバッグ」
メッセージ	障害検知時に表示されるメッセージを設定します。 ※メッセージを表示させるためには、アラートポリシーに「インシデント登録」アクションが定義されている必要があります。

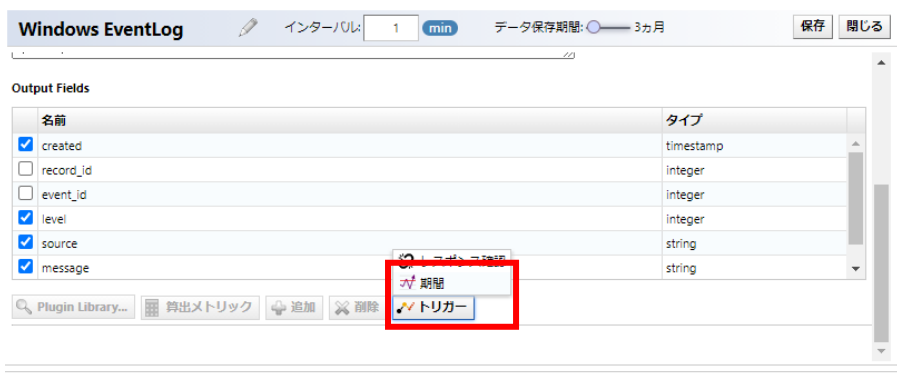
5. [保存]をクリックします。



(2) 特定のレベル以上のログが発生した場合にアラート発報する

「重大」や「エラー」など、特定のログレベルのイベントが Windows イベントログで発生した場合にアラート発報させることができます。ここでは、ログレベルが「エラー」以上のイベントが発生した時にアラート発報させる設定を例に説明します。

1. イベントログのモニターをダブルクリックで開きます。
2. [トリガー]→[期間]をクリックします。

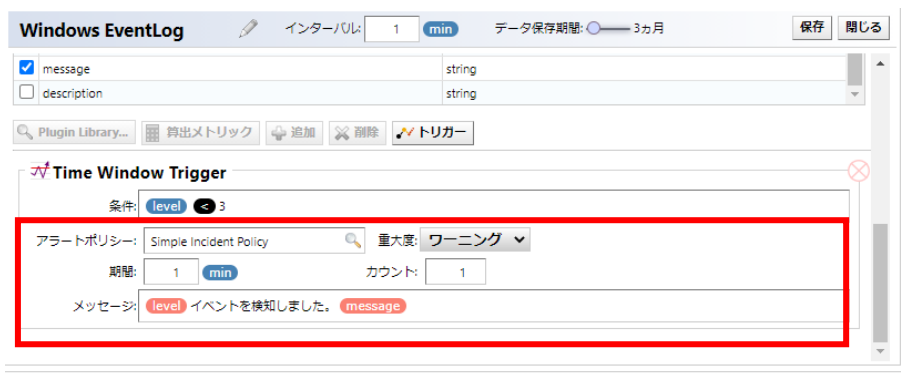


3. Agent-D の「level」を使用して条件を設定します。



項目	説明
条件	以下の項目を使って、条件を指定することができます。 is (等しい) is not (等しくない) > (より小さい、右の値のほうが小さい) < (より大きい、右の値のほうが大きい)

4. そのほかの項目(アラートポリシー/重大度/期間/カウント/メッセージ)を設定します。



項目	説明
期間	処理を実行するための期間を設定します。(最小値: 1 分) 定められた期間内に何回失敗(カウント)したらポリシーに定義された処理を実行するのか、カウントの基準となる期間。
カウント	設定期間内に何回失敗したら処理を実行するかを設定します。(最小値: 1)
アラートポリシー	アラートポリシーを指定します。
重大度	重大度を次の中から選択します。(初期値: ワーニング) 「エマージェンシー」、「アラート」、「クリティカル」、「エラー」、「ワーニング」、「通知」、「情報」、「デバッグ」
メッセージ	障害検知時に表示されるメッセージを設定します。 ※メッセージを表示させるためには、アラートポリシーに「インシデント登録」アクションが定義されている必要があります。

5. [保存]をクリックします。

The screenshot shows the configuration interface for a Windows EventLog trigger. At the top, there is a header bar with the title "Windows EventLog", a search icon, and fields for "インターバル" (Interval) set to "1 min" and "データ保存期間" (Data retention period) set to "3ヶ月" (3 months). A "保存" (Save) button is highlighted with a red box, and a "閉じる" (Close) button is next to it. Below the header, there is a table with two rows: "message" (checked) and "description" (unchecked), both with a type of "string". Below the table, there are buttons for "Plugin Library...", "导出メトリック" (Export metrics), "追加" (Add), "削除" (Delete), and "トリガー" (Trigger). The main configuration area is titled "Time Window Trigger" and contains several fields: "条件" (Condition) set to "level" with a dropdown arrow and "3"; "アラートポリシー" (Alert policy) set to "Simple Incident Policy" with a search icon and "重大度" (Severity) set to "ワーニング" (Warning); "期間" (Period) set to "1 min" and "カウント" (Count) set to "1"; and "メッセージ" (Message) set to "level イベントを検知しました。" (level Event detected.) with a "message" button.

7.2.10 Syslog 監視

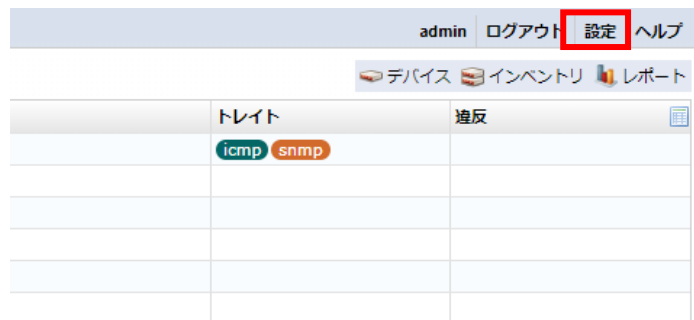
Agent-D を使用して、ThirdEye に転送される Syslog 情報を取得します。特定の文字列を含むイベントログを検出した時にアラートを発報することができます。[モニター]→[テンプレート]には、あらかじめ以下のテンプレートが Syslog 監視用のモニターとして登録されています。

- ThirdEye Syslog Monitor

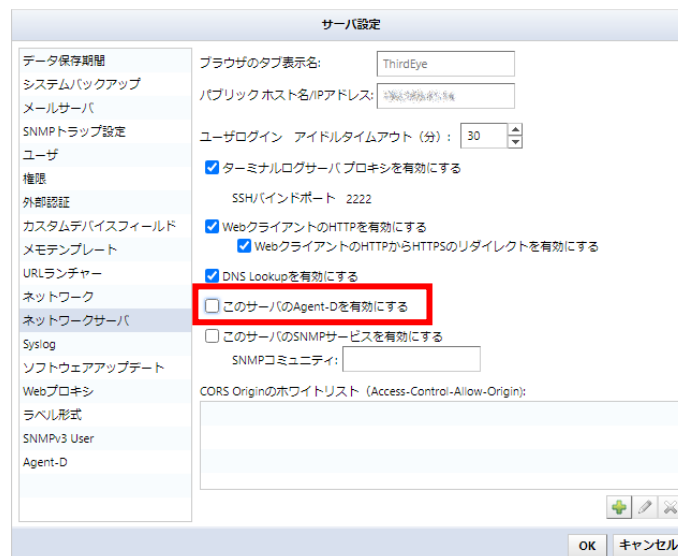
Agent-D は ThirdEye にあらかじめインストールされていますが、デフォルトでは無効になっています。ThirdEye 自身の Agent-D の有効/無効を変更する場合、ThirdEye を再起動する必要があります。

ここでは、ThirdEye 自身の Agent-D を有効にし、[テンプレート]→[ThirdEye Syslog Monitor]をモニターとして設定する場合を例に説明します。

1. [設定]をクリックします。



2. [ネットワークサーバ]を選択し、[このサーバの Agent-D を有効にする]にチェックを入れ、[OK]をクリックします。

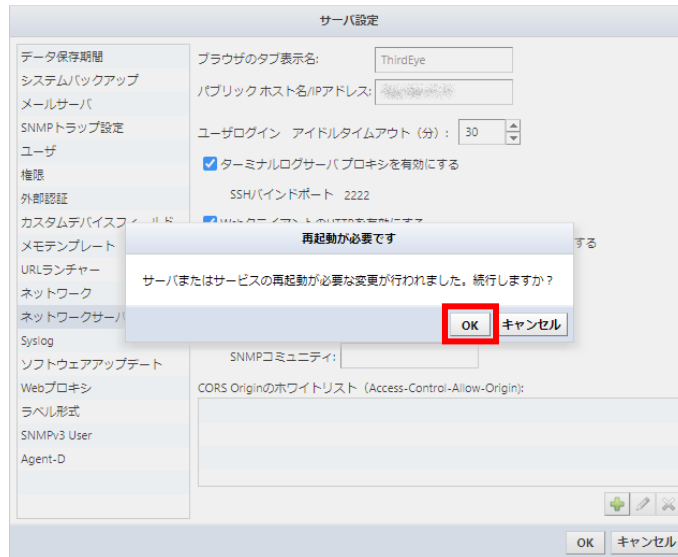


- 再起動の確認画面で[OK]をクリックします。

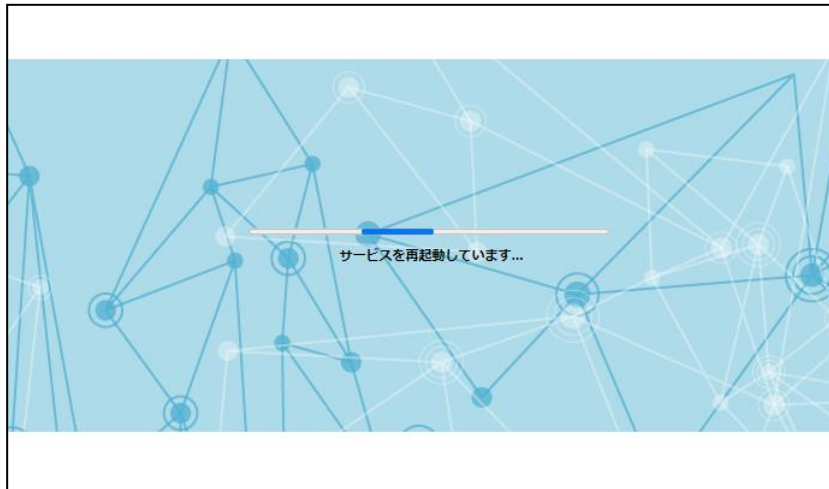
[再起動が必要です]

サーバまたはサービスの再起動が必要な変更が行われました。続行しますか？

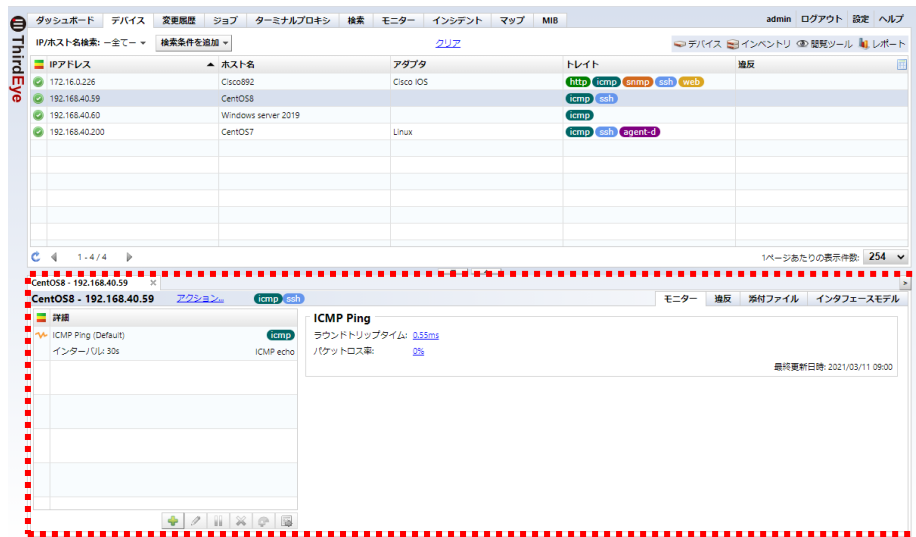
※設定を反映させるには、ThirdEye を再起動する必要があります。[OK]をクリックすると、ThirdEye が自動的に再起動します。




- 「サービスを再起動しています...」のメッセージを確認し、数分待ちます。



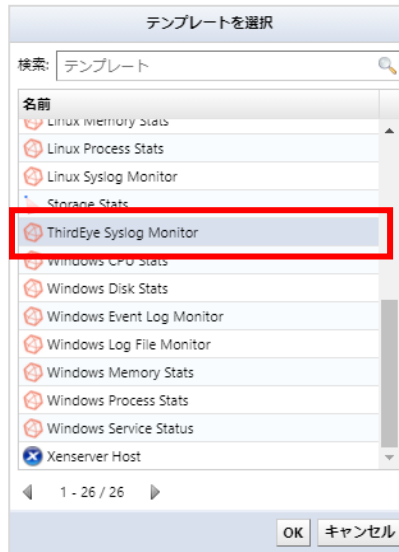
5. ログイン画面が表示されます。ログイン後、デバイスタブをクリックします。
6. [インベントリ]→[デバイス追加]から ThirdEye 自身の IP アドレスを監視対象機器として登録します。
7. ダブルクリックし、デバイス詳細を開きます。



8. [ (追加)] をクリックし、[テンプレートから追加] をクリックします。



9. [ThirdEye Syslog Monitor]を選択し、[OK]をクリックします。

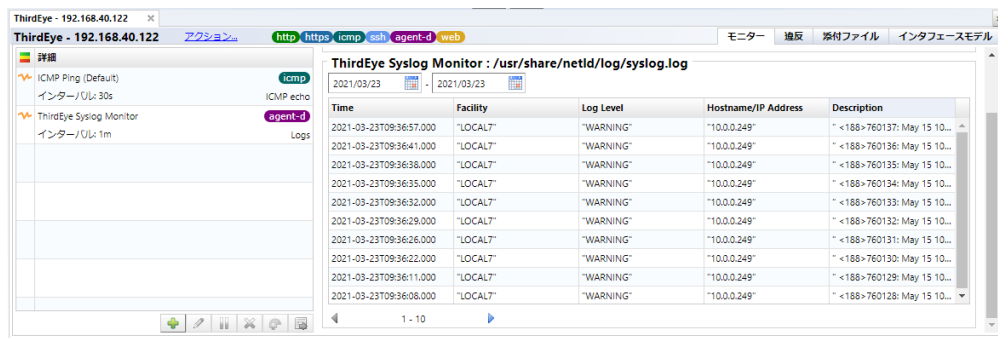


10. [Output Fields]で取得する項目にチェックを入れ、[保存]をクリックします。

※テンプレートにすでに設定されている[files]や[grok_patterns]の設定を変更する必要はありません。



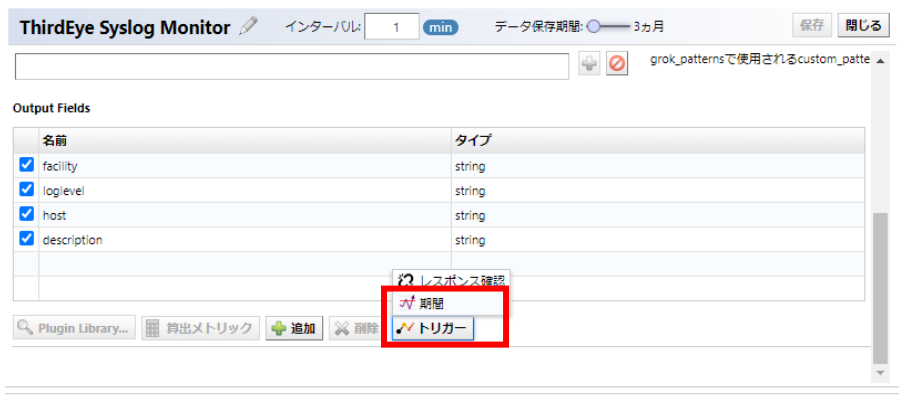
以上で、ThirdEye に送信された Syslog 情報が取得できます。Syslog のメッセージは「description」field に表示されます。



(1) 任意の文字列が含まれる場合にアラート発報する

Syslog メッセージの内容は、Agent-D「Log File Monitor」プラグインの「description」フィールドに表示されます。この「description」フィールドに特定の文字列が含まれるというフィルタ条件を設定することで、Syslog メッセージに任意の文字列が含まれている場合にアラート発報させることができます。

1. [ThirdEye Syslog Monitor]モニターをダブルクリックで開きます。
2. [トリガー]→[期間]をクリックします。



3. 「description」を使用して条件を設定します。



項目	説明
条件	以下の項目を使って、条件を指定することができます。 <ul style="list-style-type: none">• contains (含む) ※ そのほかの条件式(「is」, 「is not」, 「>」, 「<」, 「not contains」)を選択できますが、特定の文字列を含む条件を設定する場合は「contains」を使用してください。

4. そのほかの項目（アラートポリシー/重大度/期間/カウント/メッセージ）を設定します。

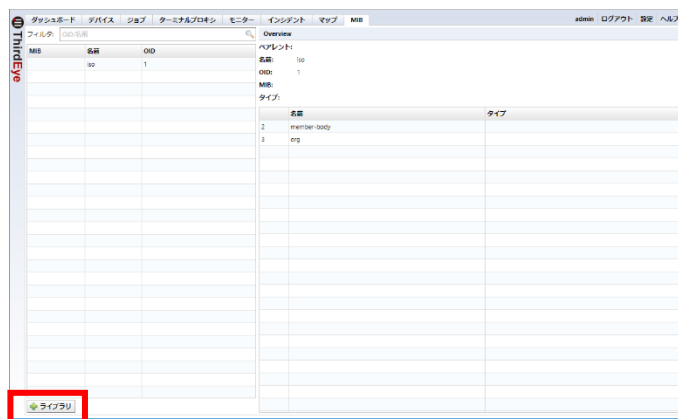
項目	説明
期間	処理を実行するための期間を設定します。(最小値: 1 分) 定められた期間内に何回失敗(カウント)したらポリシーに定義された処理を実行するのか、カウントの基準となる期間。
カウント	設定期間内に何回失敗したら処理を実行するかを設定します。(最小値: 1)
アラートポリシー	アラートポリシーを指定します。
重大度	重大度を次の中から選択します。(初期値: ワーニング) 「エマージェンシー」、「アラート」、「クリティカル」、「エラー」、「ワーニング」、「通知」、「情報」、「デバッグ」
メッセージ	障害検知時に表示されるメッセージを設定します。 ※メッセージを表示させるためには、アラートポリシーに「インシデント登録」アクションが定義されている必要があります。

5. [保存]をクリックします。

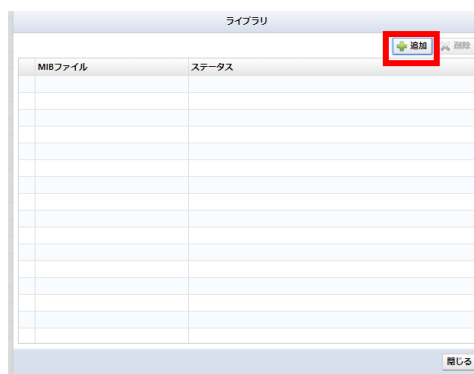
7.3 MIB をコンパイルする

ThirdEye にコンパイルされていない MIB ファイル追加することができます。


1. MIB 画面の左下にある[ライブラリ]をクリックします。

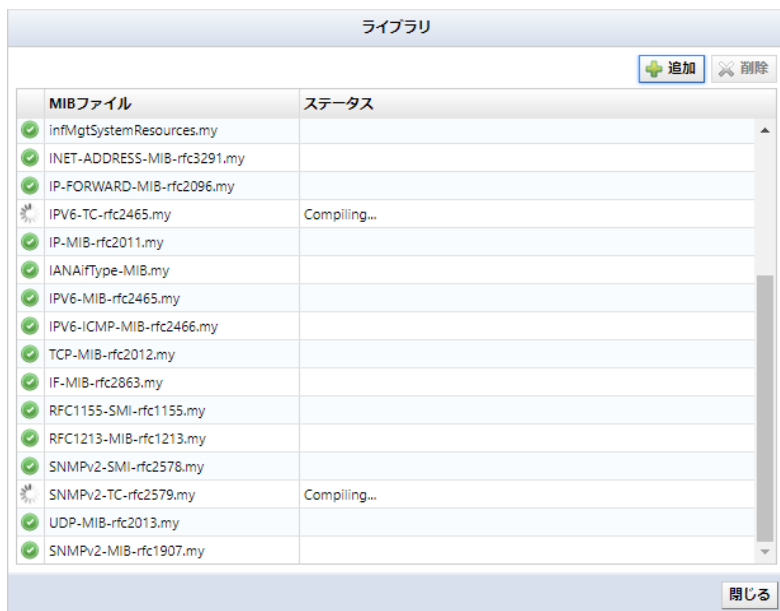


2. ライブラリ画面が表示されます。[追加]をクリックします。



3. ファイル選択ダイアログが表示されます。コンパイルする MIB ファイルを選択し、[開く]をクリックします。

MIB ファイルが一覧に表示され、MIB ファイルの左に[ (緑)]が表示されるとコンパイルは完了です。



7.4 デバイスの EOS/EOL 管理 Suite

EOS/EOL を管理するために、インベントリに「製品終了 (EOS)」「サポート終了 (EOL)」の列が追加されました。EOS/EOL 情報は、手動または Excel ファイルからのインポートで設定が可能であるほか、Cisco デバイスのみ Cisco Support API を利用して自動設定が可能です。

IPアドレス	ホスト名	ネットワーク	アダプタ	モデル	デバイスタイプ	ハードベンダー	OSバージョン	シリアル番号	製品終了	サポート終了
10.0.0.112	test	Default	Cisco IOS	CSR1000V	Router	Cisco	15.4(1)S4	929NCJ6ODJE	2022/12/31	2024/03/31
10.0.0.153	test.intra.hvi.co.jp	Default	Cisco IOS	CSR1000V	Router	Cisco	15.4(1)S4	9A0HFQVZf6	2022/12/31	2024/03/31
10.0.0.126	tech126	Default	Cisco IOS	CSR1000V	Router	Cisco	15.4(1)S4	9E0UQZVW9E	2022/12/31	2024/03/31
10.0.0.128	tech1281	Default	Cisco IOS	CSR1000V	Router	Cisco	15.4(1)S4	9I4P8735EIN	2022/12/31	2024/03/31
10.0.0.124	tech	Default	Cisco IOS	CSR1000V	Router	Cisco	15.4(1)S4	9V0INVIMGX0	2022/12/31	2024/03/31
10.0.0.223	CSR1000v	Default	Cisco IOS	CSR1000V	Router	Cisco	15.4(1)S4	9V7J6ZVFX83	2022/12/31	2024/03/31
10.0.0.149	csr1000v_inspection	Default	Cisco IOS	CSR1000V	Router	Cisco	15.4(1)S4	9WP7N6JVP3M	2022/12/31	2024/03/31
10.0.3.249	test20220802	Default	Cisco IOS	WS-C3650-24TS	Switch	Cisco	03.06.06E	FDO2027E0MF		
10.0.6.249	test20220802	Default	Cisco IOS	WS-C3650-24TS	Switch	Cisco	03.06.06E	FDO2027E0MF		
10.0.3.254	test20220728	Default	Cisco IOS	CISCO1921/K9	Router	Cisco	15.4(3)M5	FGL15082638		
10.0.0.250	1921CiscoRouter	Default	Cisco IOS	CISCO1921/K9	Router	Cisco	15.4(3)M5	FGL15082638		
10.0.0.227	Nexus5548P	Default	Cisco Nexus	Nexus5548	Switch	Cisco	7.1(4)N1(1)	55143708V7		
10.0.0.154	tech	Default	Cisco IOS	discoCSR1000v	Router	Cisco			2022/12/31	2024/03/31
10.0.0.101	RouterM.hvi.local	Default	Cisco IOS	discoCSR1000v	Router	Cisco			2022/12/31	2024/03/31
192.168.1.10	Rack1-C2960x	Default	Cisco IOS	cat2960xStack	Switch	Cisco			2022/12/31	2024/03/31
192.168.1.30	Cisco_WLC	Default	Cisco AireSpace C...	disco5500Wlc	Switch	Cisco			2022/12/31	2024/03/31
172.16.0.221	ISR4321.intra.hvi.c...	f	Cisco IOS	discoISR4321	Router	Cisco			2022/12/31	2024/03/31

7.4.1 手動設定

(1) 手順

1. EOS/EOLを取得する機器を選択します。

IPアドレス	ホスト名	ネットワーク	アダプタ	モデル	デバイスタイプ	ハードベンダー	OSバージョン	シリアル番号	製品終了	サポート終了
10.0.0.112	test	Default	Cisco IOS	CSR1000V	Router	Cisco	15.4(1)54	929NC160DIE		
10.0.0.153	test.intra.lvi.co.jp	Default	Cisco IOS	CSR1000V	Router	Cisco	15.4(1)54	940HFGQZ2F6		
10.0.0.126	tech126	Default	Cisco IOS	CSR1000V	Router	Cisco	15.4(1)54	9E0UQZVW9E		
10.0.0.128	tech1281	Default	Cisco IOS	CSR1000V	Router	Cisco	15.4(1)54	94P8735EIN		
10.0.0.124	tech	Default	Cisco IOS	CSR1000V	Router	Cisco	15.4(1)54	9V0INVIMG0X		
10.0.0.223	CSR1000v	Default	Cisco IOS	CSR1000V	Router	Cisco	15.4(1)54	9V7J6ZWFYB3		
10.0.0.149	csr1000v_inspection	Default	Cisco IOS	CSR1000V	Router	Cisco	15.4(1)54	9P7N6UV9P3M		

2. デバイスメニューから「デバイスプロパティの編集」をクリックします。

デバイスタイプ	ハードベンダー	アクション	備考	製品終了	サポート終了
Router	Cisco	バックアップ			
Router	Cisco	デバイス情報の更新	ODJE		
Router	Cisco	デバイス情報収集	QZ2F6		
Router	Cisco	デバイス表示	VK9E		
Router	Cisco	ジョブ履歴を表示	5EIN		
Router	Cisco	モニター	IMG0X		
Router	Cisco	モニターセットの適用...	/FYB3		
Router	Cisco	ping	IVP3M		
Switch	Cisco	非監視を管理	7EOMF		
Switch	Cisco	Agent-0 Linux インストーラ	7EOMF		
Router	Cisco	デバイスプロパティの編集	2638		
Router	Cisco	CiscoデバイスのEOS/EOL情報の収集	2638		
Switch	Cisco		8V7		

3. 製品終了とサポート終了の日付を選択し保存をクリックします。

デバイスの編集

アダプタ: Cisco IOS

製品終了: 2023/03/31

サポート終了: 2024/03/31

カスタムフィールド

リース契約終了... クリックして編集

設置場所: クリックして編集

連絡先: クリックして編集

トポロジデモ追... クリックして編集

最終作業日時: クリックして編集

保存 キャンセル

以上の手順により、カラムに設定した日付が表示されるようになります。

IPアドレス	ホスト名	ネットワーク	アダプタ	モデル	デバイスタイプ	ハードベンダー	OSバージョン	シリアル番号	製品終了	サポート終了
10.0.0.112	test	Default	Cisco IOS	CSR1000V	Router	Cisco	15.4(1)54	929NC160DIE	2023/03/31	2024/03/31
10.0.0.153	test.intra.lvi.co.jp	Default	Cisco IOS	CSR1000V	Router	Cisco	15.4(1)54	940HFGQZ2F6	2023/03/31	2024/03/31
10.0.0.126	tech126	Default	Cisco IOS	CSR1000V	Router	Cisco	15.4(1)54	9E0UQZVW9E	2023/03/31	2024/03/31
10.0.0.128	tech1281	Default	Cisco IOS	CSR1000V	Router	Cisco	15.4(1)54	94P8735EIN	2023/03/31	2024/03/31
10.0.0.124	tech	Default	Cisco IOS	CSR1000V	Router	Cisco	15.4(1)54	9V0INVIMG0X	2023/03/31	2024/03/31
10.0.0.223	CSR1000v	Default	Cisco IOS	CSR1000V	Router	Cisco	15.4(1)54	9V7J6ZWFYB3	2023/03/31	2024/03/31
10.0.0.149	csr1000v_inspection	Default	Cisco IOS	CSR1000V	Router	Cisco	15.4(1)54	9P7N6UV9P3M	2023/03/31	2024/03/31

7.4.2 自動設定

(1) 前提条件

- 使用している ThirdEye がインターネットに接続できること
- Cisco Smart Net Total Care にアクセスするための、事前に Cisco アカウントでログインし、API キーとシークレットコードを取得する必要がある

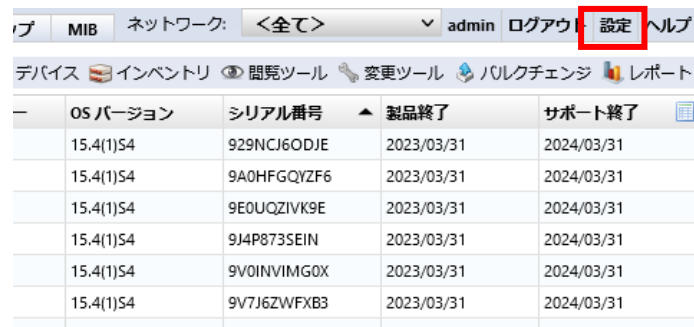
※有効な Cisco Smart Net Total Care (SNTC)が必要です。

※API の取得について、以下を参照してください。

<https://developer.cisco.com/docs/support-apis/#!user-onboarding-process>

(2) 手順（オンライン環境）

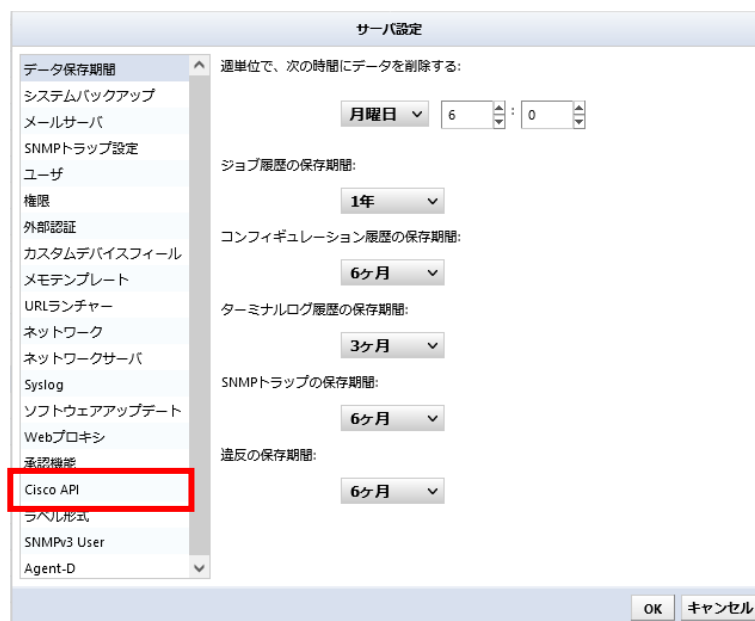
1. 設定をクリックします。



The screenshot shows a web interface with a top navigation bar containing 'MIB', 'ネットワーク: <全て>', 'admin', 'ログアウト', '設定', and 'ヘルプ'. Below the navigation bar is a menu with 'デバイス', 'インベントリ', '閲覧ツール', '変更ツール', 'パルクチェンジ', and 'レポート'. The main content area is a table with columns: 'OS バージョン', 'シリアル番号', '製品終了', and 'サポート終了'. The table contains several rows of device information.

OS バージョン	シリアル番号	製品終了	サポート終了
15.4(1)S4	929NCJ6ODJE	2023/03/31	2024/03/31
15.4(1)S4	9A0HFGQYZF6	2023/03/31	2024/03/31
15.4(1)S4	9E0UQZIVK9E	2023/03/31	2024/03/31
15.4(1)S4	9J4P873SEIN	2023/03/31	2024/03/31
15.4(1)S4	9V0INVIMG0X	2023/03/31	2024/03/31
15.4(1)S4	9V7J6ZWFXB3	2023/03/31	2024/03/31

2. Cisco API をクリックします。



The screenshot shows the 'サーバ設定' (Server Settings) dialog box. The left sidebar contains a list of settings categories, with 'Cisco API' highlighted in red. The main area of the dialog box contains several configuration options with dropdown menus and input fields:

- データ保存期間: 週単位で、次の時間にデータを削除する: 月曜日 6 : 0
- ジョブ履歴の保存期間: 1年
- コンフィギュレーション履歴の保存期間: 6ヶ月
- ターミナルログ履歴の保存期間: 3ヶ月
- SNMPトラップの保存期間: 6ヶ月
- 違反の保存期間: 6ヶ月

At the bottom of the dialog box are 'OK' and 'キャンセル' buttons.

- API キーとシークレットコードを入力し、OK をクリックします。

サーバ設定

データ保存期間
システムバックアップ
メールサーバ
SNMPトラップ設定
ユーザ
権限
外部認証
カスタムデバイスフィード
メモテンプレート
URLランチャー
ネットワーク
ネットワークサーバ
Syslog
ソフトウェアアップデート
Webプロキシ
承認機能
Cisco API
ラベル形式
SNMPv3 User
Agent-D

Cisco Client Id: qvpf68esdmcwvnrdrv58nmzuagaer
Cisco Client Secret: NBZPffPuzPtvePSEAM8xbxP2aergaer

OK キャンセル

- EOS/EOL を取得する機器を選択します。

IPアドレス	ホスト名	ネットワーク	アダプタ	モデル	デバイスタイプ	ハードベンダー	OSバージョン	シリアル番号	製造終了	サポート終了
10.0.0.112	test	Default	Cisco IOS	CSR1000V	Router	Cisco	15.4(1)54	929WCJ6ODJE	2023/03/31	2024/03/31
10.0.0.153	test.intra.hi.co.jp	Default	Cisco IOS	CSR1000V	Router	Cisco	15.4(1)54	9A0HFGQVZF6	2023/03/31	2024/03/31
10.0.0.126	tech126	Default	Cisco IOS	CSR1000V	Router	Cisco	15.4(1)54	9E0UQZVW9E	2023/03/31	2024/03/31
10.0.0.128	tech1281	Default	Cisco IOS	CSR1000V	Router	Cisco	15.4(1)54	944P8735EIN	2023/03/31	2024/03/31
10.0.0.124	tech	Default	Cisco IOS	CSR1000V	Router	Cisco	15.4(1)54	9V0INVIMGOX	2023/03/31	2024/03/31
10.0.0.223	CSR1000v	Default	Cisco IOS	CSR1000V	Router	Cisco	15.4(1)54	9V7J6ZWF9B3	2023/03/31	2024/03/31
10.0.3.249	test20220802	Default	Cisco IOS	WS-C3650-24TS	Switch	Cisco	03.06.06E	FDO2027EOMF		
10.0.6.249	test20220802	Default	Cisco IOS	WS-C3650-24TS	Switch	Cisco	03.06.06E	FDO2027EOMF		
10.0.3.254	test20220728	Default	Cisco IOS	CISCO1921K9	Router	Cisco	15.4(9)M5	FGL15082638		
10.0.0.250	1921CiscoRouter	Default	Cisco IOS	CISCO1921K9	Router	Cisco	15.4(9)M5	FGL15082638		
10.0.0.227	Nexus5548P	Default	Cisco Nexus	Nexus5548	Switch	Cisco	7.1(H)(N11)	SS1143708V7		

- デバイスメニューから「Cisco デバイスの EOS/EOL 情報の収集」をクリックします。

インシデント マップ MIB ネットワーク: <全て>

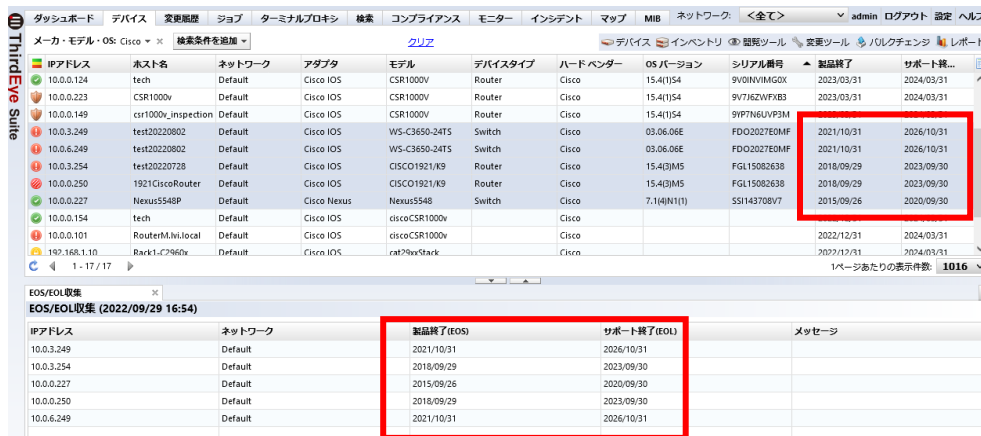
デバイス インベントリ 閲覧ツール 変更

バックアップ
デバイス情報の更新
ネイバー情報収集
ネイバー表示
比較
ジョブ履歴を表示
モニター
モニターセットの適用...
Ping
非監視を管理
Agent-D Linux インストーラ
編集
CiscoデバイスのEOS/EOL情報の収集
タグ付け
タグ削除

6. 以下の画面で「はい」をクリックします。



以上の手順により、自動で EOS/EOL 情報を取得し、カラムに登録します。



(3) 手順 (オフライン環境)

ThirdEye がインターネットに接続できない場合、Cisco サーバーから販売終了日を取得することはできません。ただし、インベントリを csv ファイルとしてエクスポートして、Cisco サービスへのインポートに使用できます。その後、Cisco サービスから csv ファイルをエクスポートし、ThirdEye にインポートしてサポート終了日を更新できます。Cisco サービスでは、エクスポートファイルに販売終了日が含まれないことに注意してください。

Cisco サービスへのインポートに使用できる csv ファイルをエクスポートするには、インベントリメニューから「インベントリを CSV 形式でエクスポート」を選択してください。



7.5 コンプライアンスの概要 Suite

コンプライアンスポリシーを設定することで、意図しない設定がデバイスのコンフィギュレーションに設定されていることが自動的に確認することができます。自動的に検出するためには、コンプライアンス

スルールを作成する必要があります。ルールは、以下の4つのマッチング条件を用いて構成されます。

- 一致した場合、対象外
- 一致しない場合、対象外
- 一致した場合、違反
- 一致しなかった場合、違反

それぞれの条件は一つの検索文字列を持っており、与えられたコンフィギュレーションがその文字列にマッチするかを調べます。コンプライアンスルールを集めたものは ルールセットと呼びます。ルールセットもまた、自由に作成することができます。

さらに、もっと大きな単位でコンプライアンスを管理するために、ポリシーというものが備わっています。ポリシーはルールセットを複数組み合わせることで作られますが、加えてそれを適用するデバイスのリストや、違反の重大さ(エラーまたは警告または通知)、違反の履歴などの情報も持っています。

7.5.1 ルール

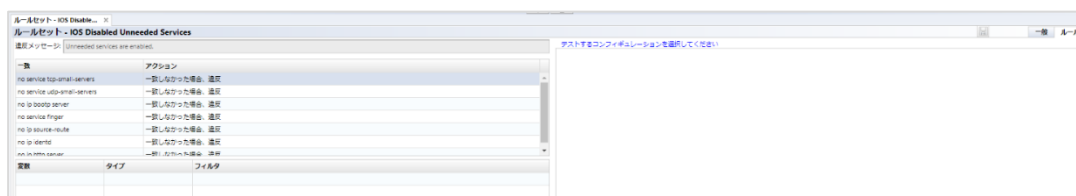
(1) ルールセットタブ

ルールセットタブは、ルールセットを管理します。

デバイス	変更履歴	ジョブ	ターミナルプロキシ	検索	コンプライアンス	Zero-Touch
コンプライアンスポリシー ルールセット						
+ 作成 📄 コピー ✖ 削除						
ルールセット	アダプタ	コンフィギュレーション				
IOS Session Idle Timeout	Cisco IOS	/running-config				
IOS Secure Enable Passwords	Cisco IOS	/running-config				
IOS SSH-only Restricted Access	Cisco IOS	/running-config				
IOS Interface Auto-Duplex/Speed	Cisco IOS	/running-config				
IOS Disabled Unneeded Services	Cisco IOS	/running-config				
IOS Telnet Restricted Access	Cisco IOS	/running-config				

ルールサブタブ

ルールセットサブタブでそれぞれのルールセットをダブルクリックすると、その内容がステータスペインの新たなタブに表示されます。新しいタブには2つのサブタブ、一般サブタブとルールサブタブがあります。



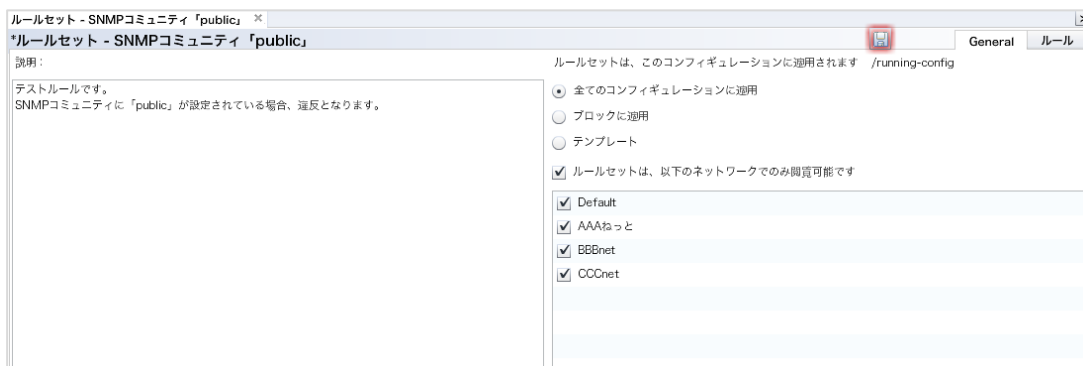
項目	説明
違反メッセージ	ルールに違反した場合に表示されるメッセージを入力します。

項目	説明
開始/終了	「一致」項目で指定された文字列を検索する範囲を指定します。この欄は、一般サブタブで「ブロックに適用」が選択された場合に表示されます。
一致	検索される文字列を指定します。文字列を「~(チルダ)」で挟むことで変数化することができます。 例: interface gigabitEthernet ~INT_NUM~
アクション	マッチングの条件を選択します。 一致しない場合、対象外 一致した場合、対象外 一致しなかった場合、違反 一致した場合、違反
変数	「一致」項目で指定する文字列に変数を使用した場合の値が表示されます。
タイプ	マッチする可能性のある4つのタイプを指定します。タイプにマッチしない場合、検索条件から外れます。 テキスト : すべてのテキストがマッチします。 IP アドレス : IP アドレスを表す文字列のみにマッチします。 ホスト名 : ホスト名にマッチします。 ワード : 単語にマッチします。 正規表現 : 正規表現を使用してマッチする文字列をさがします。
フィルタ	検索する文字列や値を入力します。*が入力された場合、「どのような値でも良い」という意味になります

一般サブタブ

一般サブタブは、ルールの説明や適用範囲を設定するタブです。ルールに対する説明を書くことは、後のメンテナンスの上で重要です。現在の管理者が退職した場合を考えてみてください。コンプライアンスを適切に管理するためには、後任の者が書かれたルールを理解しなくてはなりません。一般的には、ルールの定義だけからそのルールの目的を推測することは極めて難しいことです。どのようなことが起こっても安定したメンテナンスを行うために、ルールには最悪でも最低限の説明を加え、出来ればわかりやすい説明を加えます。

現在選択しているルールの説明を加えることができる他、ルール自体の設定を行うことも出来ます。




項目	説明
説明	ルールの説明を入力します。

項目	説明
全てのコンフィギュレーションに適用	コンフィギュレーション全体にルールを適用します。
ブロックに適用	コンフィギュレーションをブロック単位に分け、ブロック単位でルールを適用します。
テンプレート	コンフィギュレーションをテンプレート上から1行ずつ比較し、差分がある場合は違反になります。
ルールセットは、以下のネットワークでのみ閲覧可能です	チェックを有効にした場合、ルールの適用対象となるネットワークが制限されます。

(2) 新規ルールの作成

ここでは、スクリーンショットを交えて新規ルールの作成方法をお伝えします。例として Cisco IOS のデバイスコンフィギュレーションで SNMP コミュニティ設定が“public”である場合に違反を発生させてみましょう。

1. コンプライアンス→ルールセットタブで  ボタンをクリックします。



ルールセット	アダプタ	コンフィギュレーション
IOS Session Idle Timeout	Cisco IOS	/running-config
IOS Secure Enable Passwords	Cisco IOS	/running-config
IOS SSH-only Restricted Access	Cisco IOS	/running-config
IOS Interface Auto-Duplex/Speed	Cisco IOS	/running-config
IOS Disabled Unneeded Services	Cisco IOS	/running-config
IOS Telnet Restricted Access	Cisco IOS	/running-config

2. ルールの名前、対象アダプタ(機種の分類)、どちらのコンフィギュレーションに適用するルールであるか(running-config か startup-config か)を選び、OK ボタンをクリックします。



ルールセット


名前:

アダプタ:

コンフィギュレーション:

OK キャンセル

3. 違反メッセージ欄に、違反検出時に表示されるメッセージを入力します。

この例では、メッセージは「SNMP コミュニティに「public」が設定されています」です。終わったら、 ボタンを押してください。

*ルールセット - SNMPコミュニティ「public」

違反メッセージ SNMPコミュニティに「public」が設定されています

一致	アクション

+ ✖ ⬆ ⬇

変数	タイプ	フィルタ

- 一致に、違反となるテキストを入力し、アクションで「一致した場合、違反」を選択します。

*ルールセット - SNMPコミュニティ「public」

違反メッセージ SNMPコミュニティに「public」が設定されています

一致	アクション
snmp-server community public ~mode~	一致した場合、違反

+ ✖ ⬆ ⬇

変数	タイプ	フィルタ
mode	text	

- 作成したルールをテストする場合、テストするコンフィギュレーションを選択してくださいをクリックして、インベントリからコンフィギュレーションを選択してください。

ルールセット - SNMPコミュニティ「public」

違反メッセージ SNMPコミュニティに「public」が設定されています

一般 ルール

[テストするコンフィギュレーションを選択してください](#)

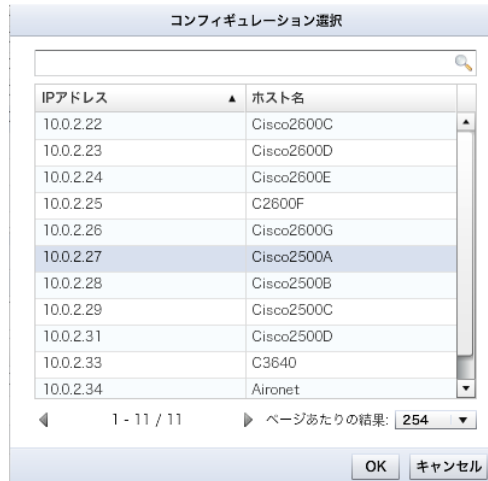
一致	アクション
snmp-server community public ~mode~	一致した場合、違反

+ ✖ ⬆ ⬇

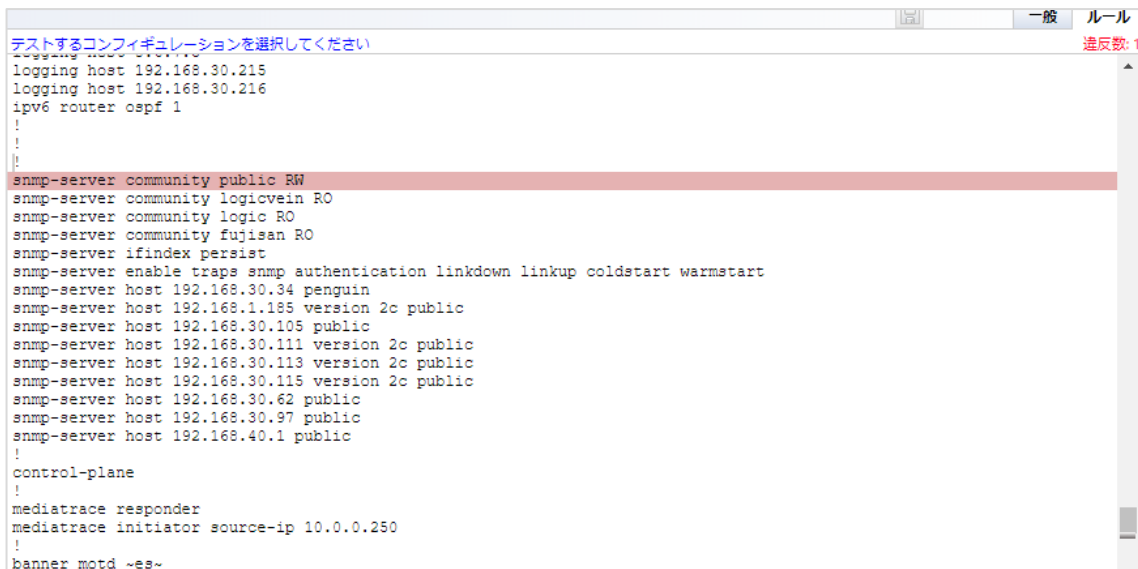
変数	タイプ	フィルタ
mode	テキスト	

6. ルール作成時に選択したアダプタに当てはまるデバイスのリストがコンフィギュレーション選択ウィンドウに一覧表示されます。

この列では、始めに選択した IOS アダプタに合致するデバイスのみが表示されます。



このテキストルールに対して違反が検索され、そしてもし違反が見つければ赤で表示されます。終わったら、次の章でこのルールセットからポリシーを作りましょう。



7.5.2 コンプライアンスポリシー

(1) コンプライアンスポリシータブ

コンプライアンスポリシータブは次のサブタブからなります。

コンプライアンスポリシー		ルールセット		
コンプライアンスポリシー	適用デバイス	違反しているデバイス	違反	適合

デバイスサブタブ

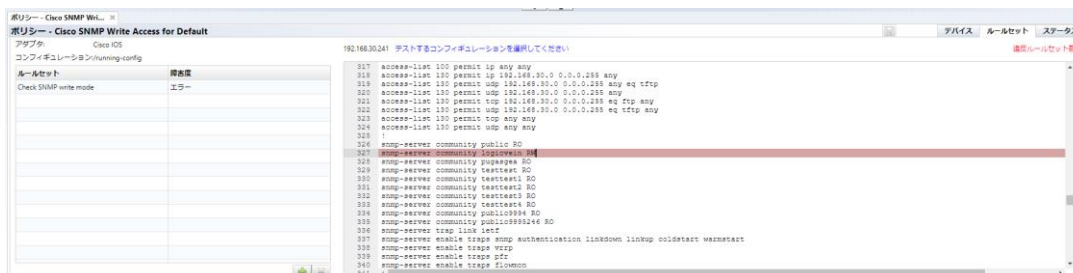
このタブは、ポリシーをどのデバイスに適用するかを選択します。入力インターフェースは、ジョブ管理のものと同じです。静的リスト、検索、すべてのデバイスの3つの方法を用い、タブ切り替えテクニックを適宜用いてデバイスを選択します。

ポリシー - Junosポリシー		
ポリシー - Junosポリシー		
<input type="radio"/> 全てのデバイス <input type="radio"/> 検索 <input checked="" type="radio"/> 静的リスト		
IPアドレス	ホスト名	ネットワーク
10.0.3.254	SRX-240	192.168.40.152

項目	説明
全てのデバイス	全てのデバイスにポリシーを適用します。
検索	検索条件に一致したデバイスにポリシーを適用します。
静的リスト	「デバイス」タブで選択して追加したデバイスにポリシーを適用します。

ルールセットサブタブ

このタブでは、作ったルールセットをポリシーに登録します。



項目	説明
アダプタ	ポリシーを適用するアダプタを表示しています。
コンフィギュレーション	ポリシーを適用するコンフィギュレーションを表示しています。
ルールセット	ポリシーに追加したルールです。
障害度	障害のレベルを、エラーまたはワーニングから選択できます。ポリシー違反時に表示されるアイコンが異なります。

(2) 新規ポリシーの作成

先程作成したルールセットを用いて、Cisco IOS デバイスコンフィギュレーション用のポリシーを作成してみましょう。

1. コンプライアンス→コンプライアンスポリシータブにて **+ 作成** ボタンをクリックします。



2. ポリシー名、対象アダプタ、コンフィギュレーションの種類を入力し、OK をクリックします。

ポリシー

名前：

アダプタ：

コンフィギュレーション：

3. デバイスサブタブにて、この例では検索を選択します。


The screenshot shows the 'Policy - IOS Policy' configuration window with the 'Device' sub-tab selected. The window contains several input fields for configuration parameters, including IP/CIDR, Admin IP, Hostname, Section name, EOS, EOL, System name, and Installation Date, all of which are filled with wildcards. There are also radio buttons for logical operators (AND/OR), a model field, a version dropdown, a MAC address field, and a configuration text field. A 'Tags' section is visible with Tag A, Tag B, and Tag D.

このデバイスサブタブでの検索、静的リストなどの動作と設定方法は、ジョブ管理タブで行う動作・設定方法と全く同じです。結果としてジョブ管理タブで行うのと同様に、検索ルールを用いた時には違反チェックが起動するたびに対象デバイスが検索され、そのデバイスにのみ違反チェックが行われます。ポリシー作成時の検索結果が保存されるわけではない事に注意してください。

4. ステータスペインのルールセットサブタブにて、 ボタンをクリックします。

The screenshot shows the 'Policy - IOS Policy' configuration window with the 'Rule Set' sub-tab selected. The window displays a table of rule sets with columns for 'Rule Set' and 'Severity'. The table lists several rule sets, including 'IOS Session Idle Timeout', 'IOS Secure Enable Passwords', and 'IOS SSH-only Restricted Access'. A 'Test Configuration' button is visible.

ルールセット	障害度
IOS Session Idle Timeout	エラー
IOS Secure Enable Passwords	エラー
IOS SSH-only Restricted Access	ワーニング

ルールセットを選択し  ボタンを押してください。この例では、SNMP コミュニティ「public」と IOS セキュア Enable Password ルールを選択しました。

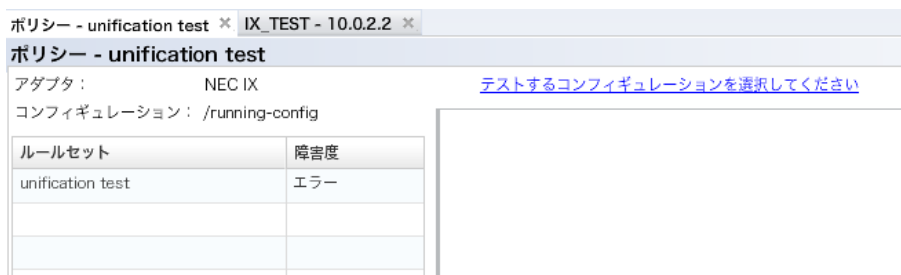
The screenshot shows the 'Add Rule Set' dialog box. The dialog box contains a list of rule sets to be added, including 'IOS Disabled Unneeded Services', 'IOS Interface Auto-Duplex/Speed', 'IOS SSH-only Restricted Access', 'IOS Secure Enable Passwords', 'IOS Session Idle Timeout', 'IOS Telnet Restricted Access', and 'SNMP Community 'public''. The 'Add' and 'Cancel' buttons are visible at the bottom.

このウィンドウに現れるルールは、そのアダプタタイプが現在のポリシーのアダプタタイプにマッチするものに限られます。全くルールが表示されない場合には、ポリシーかルールのアダプタタイプを見直してください。

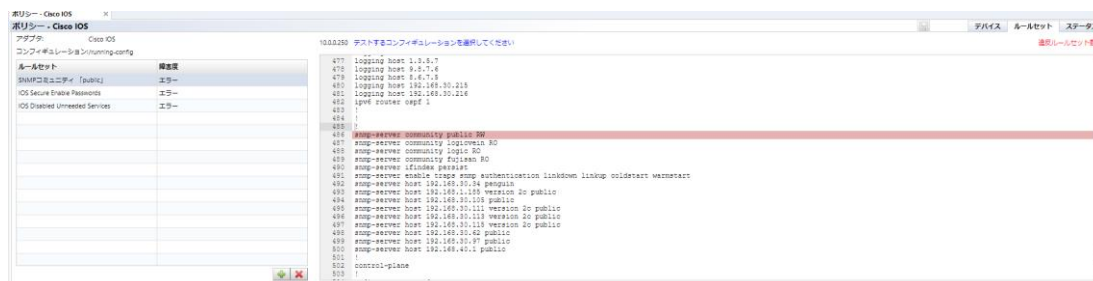
ルールの障害度を選択します。ルールセットごとに異なる障害度を設定することができます。



ポリシーをテストするには、「テストするコンフィギュレーションを選択してください」をクリックし、コンフィギュレーションを選択してください。(ルールセットのテストで行った手順と同じです。)



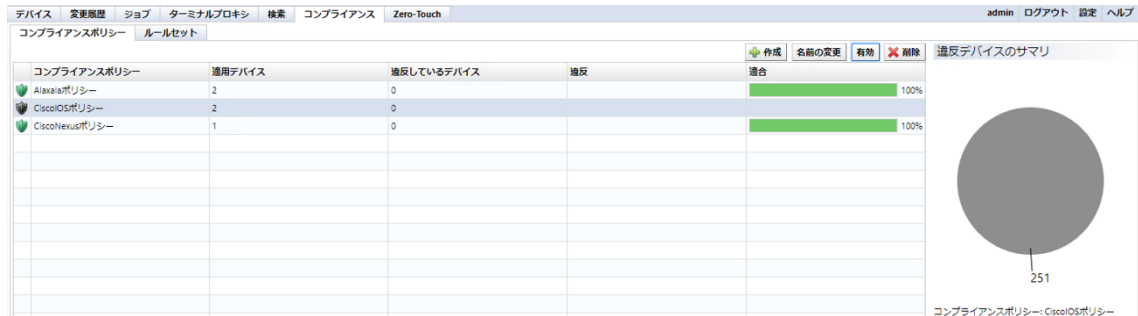
このテストルールに対して違反が検索され、そしてもし違反が見つければ赤で表示されます。テスト結果を確認したら、次はポリシーを有効化しましょう。ポリシーを作成しただけでは、違反チェックは行われません。



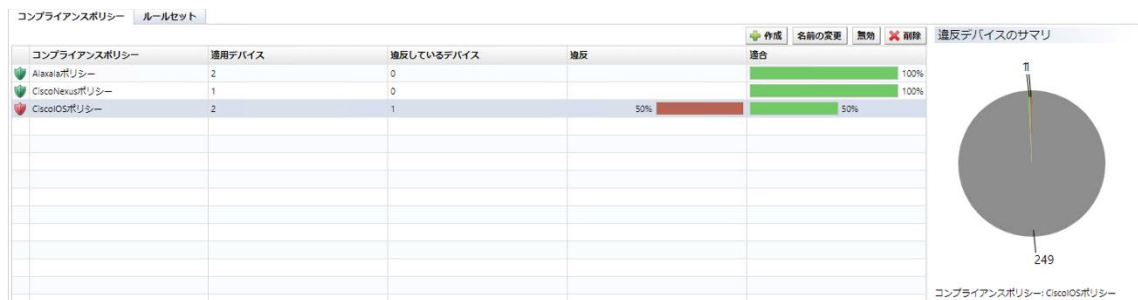
(3) 作成したポリシーの適用

ポリシーを作成したら、次にポリシーを有効化する必要があります。メインペインにコンプライアンス →コンプライアンスポリシーサブタブが開かれていることを確認してください。

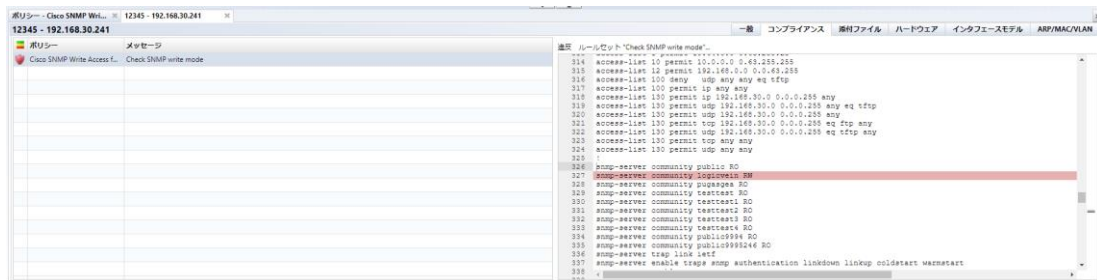
ポリシーを選択した状態で有効ボタンを押してください。右の違反デバイスのサマリに円グラフが表示され、違反状況が一目でチェックできます。



ポリシー違反のあるデバイスがあった場合には、ポリシーのアイコンが変化します。その障害度に応じて、オレンジのワーニング、あるいは赤いエラーアイコンが表示されます。



変化したアイコンをダブルクリックしましょう。すると、ステータスペインにステータスサブタブが開かれます。このサブタブには、違反の詳細が書かれています。



違反アイコンはデバイスビューにも表示されます。アイコンをダブルクリックすれば、違反の詳細を知ることができます。

7.5.3 自動修復機能

コンプライアンス機能とバルクチェンジ機能を合わせることで、コンプライアンス違反を検知した場合に、予め指定したバルクチェンジジョブを自動で実行することができます。これにより、即時にコンプライアンス違反を解消することができます。

設定の流れ

1. バルクチェンジジョブの作成

コンプライアンス違反が発生した際に実行するバルクチェンジジョブを作成します。

2. コンプライアンス違反のルールを作成

違反ルールを作成し、ルールとバルクチェンジジョブを紐付けします。

3. コンプライアンスポリシーの作成

コンプライアンスルールとデバイスを紐付け、検知する設定をします。

以下では、設定例を使用して設定方法を説明します。

(1) ケース1: SNMP コミュニティ設定にて Read-Write 権限の使用を禁止している場合

1. ジョブ->ジョブ管理に移動し、新しいジョブ->バルクチェンジを選択します。



2. ジョブ名、コメント(オプション)を入力します。

バルクチェンジジョブの作成

ジョブ名:
SNMPコミュニティ設定

コメント:
Read-Only設定

アダプタ: Cisco IOS

ジョブで設定されているデバイス全てに、共通の代替値を設定する
 ジョブで設定されているデバイスごとに、ユニークな代替値を設定する

OK キャンセル

3. 適用するデバイスのアダプタを選択し OK をクリックします。

※ルールセットとの紐付けに使用します。

バルクチェンジジョブの作成

ジョブ名:
SNMPコミュニティ設定

コメント:
Read-Only設定

アダプタ: Cisco IOS

ジョブで設定されているデバイス全てに、共通の代替値を設定する
 ジョブで設定されているデバイスごとに、ユニークな代替値を設定する

OK キャンセル

4. テンプレートに実行するコマンドを入力します。

*SNMPコミュニティ設定

テンプレート | 代替の値 | デバイス | スケジュール | ジョブ承認ログ

代替値

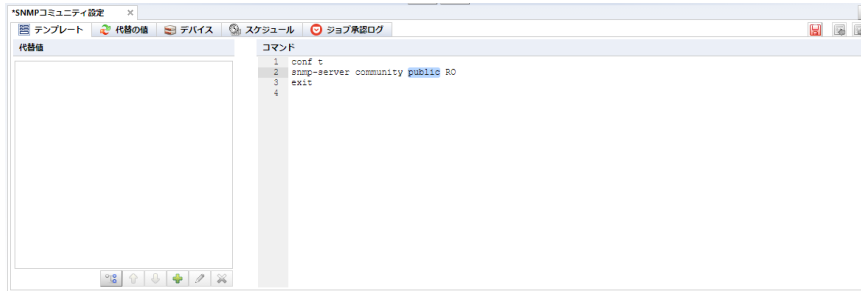
コマンド

```
1 conf t
2 snmp-server community public RO
3 exit
4
```

5. 変数化する箇所を選択し、+をクリックします。

※変数化せずにこのままコマンドを実行する場合は、この手順をスキップします。

※今回のケースでは、コミュニティ名はコンフィグから取得する為、コミュニティ名の部分を変数化します。



6. 変数名を入力し、OK をクリックします。

代替値の追加

選択: public

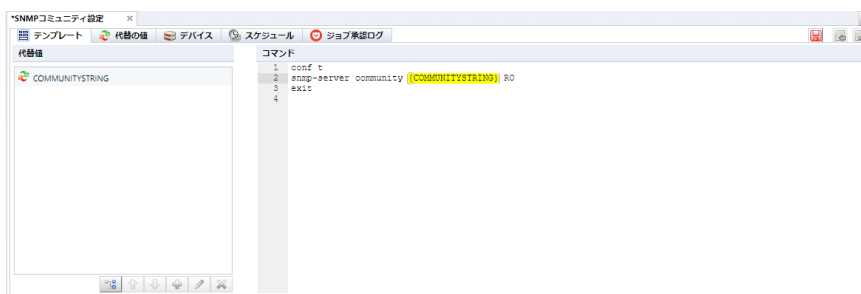
名前: COMMUNITYSTRING

タイプ: テキスト

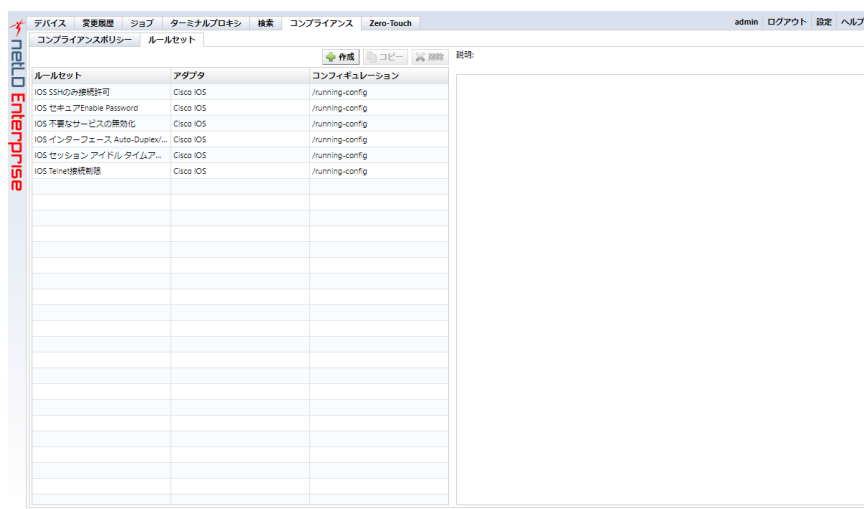
選択した値をデフォルトとして使用する

OK キャンセル

7. 保存します。



8. コンプライアンス→ルールセットに移動し、作成をクリックします。



9. ルール名を入力し、およびアダプタを選択し、OK をクリックします。

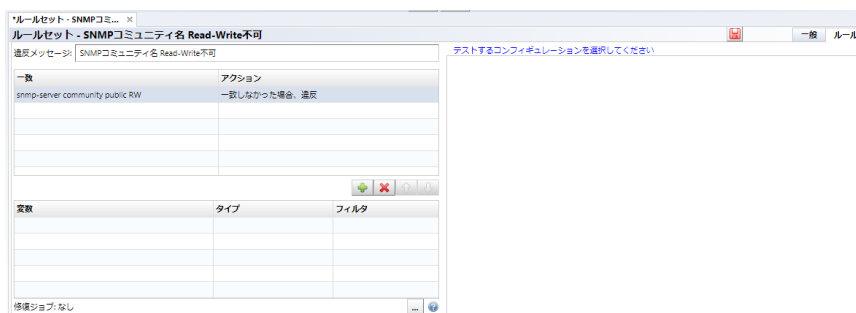
※アダプタはバルクチェンジ作成時に選択したアダプタを選択してください。

The screenshot shows the 'ルールセット' (Rule Set) configuration dialog box. The fields are filled as follows:

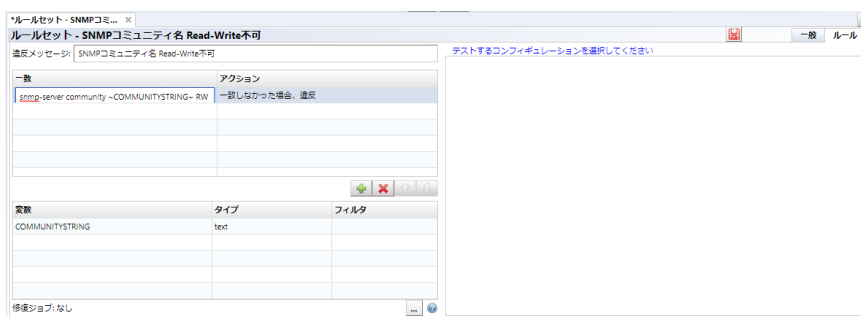
- 名前: SNMPコミュニティ名 Read-Write不可
- アダプタ: Cisco IOS
- コンフィギュレーション: /running-config

Buttons: OK, キャンセル

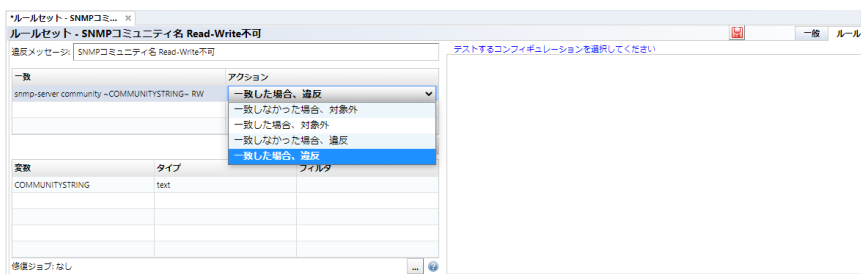
10. +をクリックし、一致条件を追加します。



11. コミュニティ名の部分をバルクチェンジの変数名に指定し「~」で挟みます。

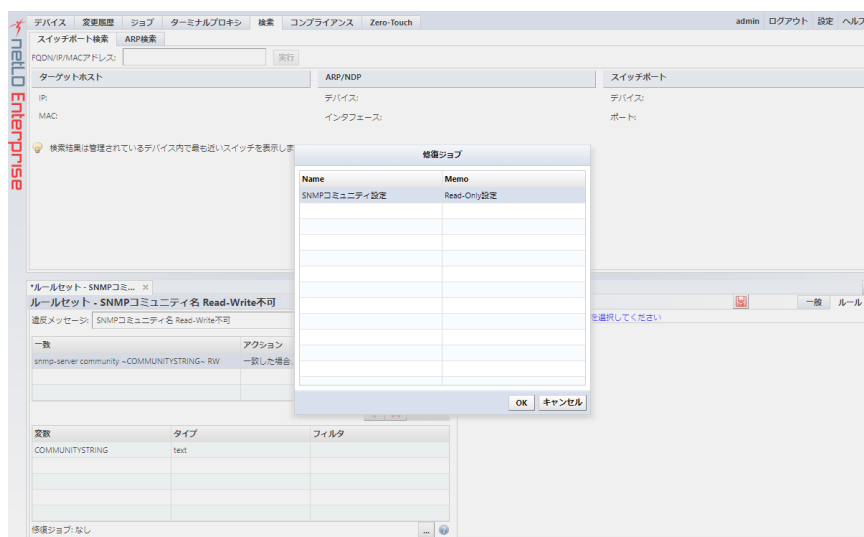


12. アクションを「一致した場合、違反」に設定します。

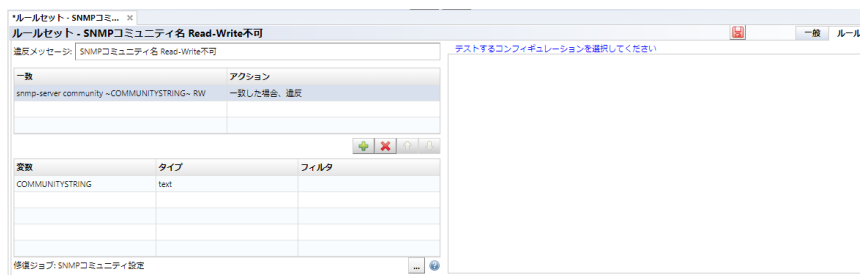


13. 修復ジョブの「…」をクリックし、違反時に実行するバルクチェンジジョブを指定します。

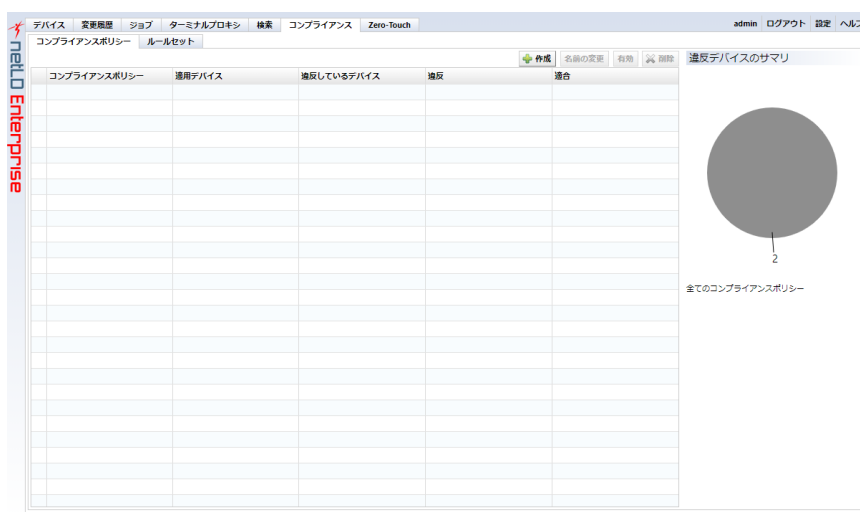
※指定できるジョブは1つです。



14. 設定を保存します。



15. コンプライアンス→コンプライアンスポリシーに移動し、作成をクリックします。



16. 名前を入力後、アダプタおよび対象のコンフィギュレーションファイルを選択し、OK をクリックします。

コンプライアンスポリシー

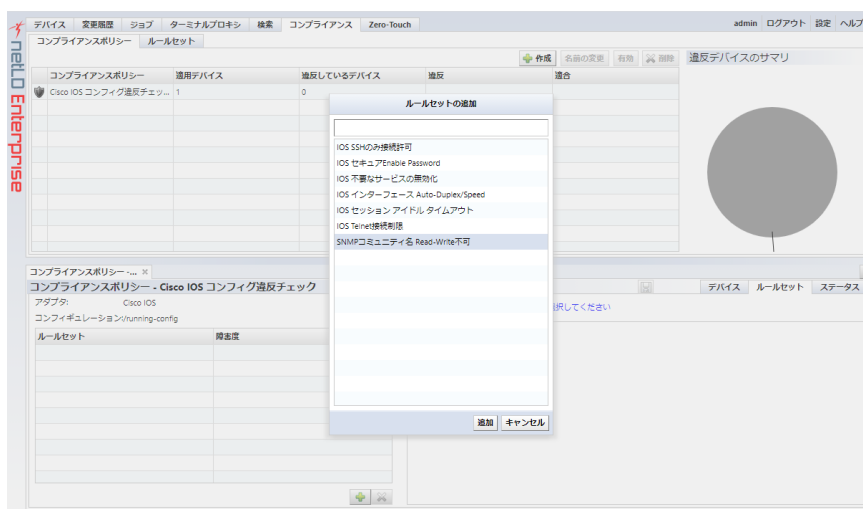
名前:

アダプタ:

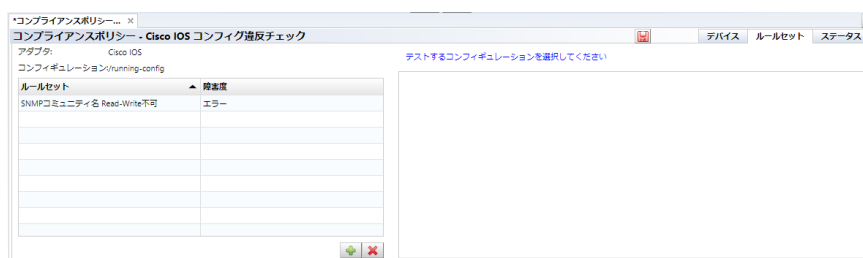
コンフィギュレーション:

OK キャンセル

17. +をクリックし、ルールセットを追加します。



18. 保存をクリックします。

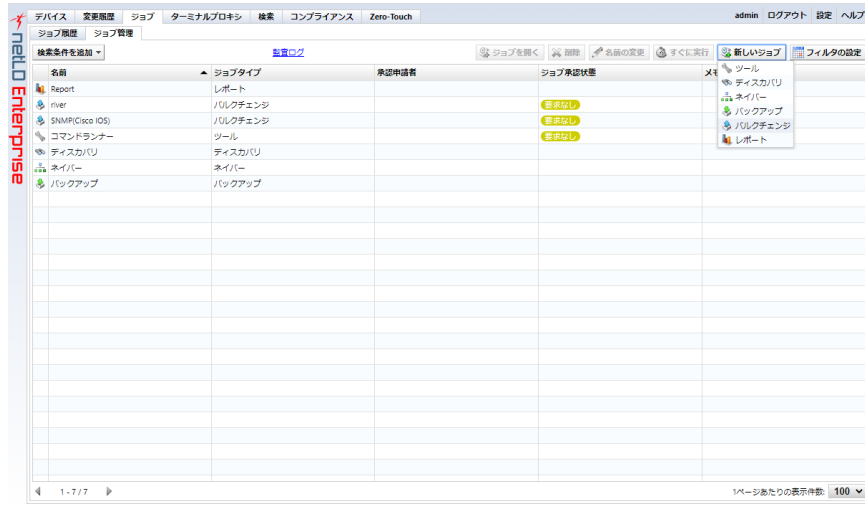


19. 作成したコンプライアンスポリシーを選択し、「有効」をクリックします。



(2) ケース 2: インタフェースにアクセスリストが追加されていない場合

1. ジョブ->ジョブ管理に移動し、新しいジョブ->バルクチェンジを選択します。



2. ジョブ名、コメント(オプション)を入力します。

バルクチェンジジョブの作成

ジョブ名:
アクセスリスト(ネットワーク指定)

コメント:
ラボ環境ネットワークのみアクセス可能

アダプタ: Cisco IOS

ジョブで設定されているデバイス全てに、共通の代替値を設定する
 ジョブで設定されているデバイスごとに、ユニークな代替値を設定する

OK キャンセル

3. 適用するデバイスのアダプタを選択し OK をクリックします。

※ルールセットとの紐付けに使用します。

バルクチェンジジョブの作成

ジョブ名:
アクセスリスト(ネットワーク指定)

コメント:
ラボ環境ネットワークのみアクセス可能

アダプタ: Cisco IOS

ジョブで設定されているデバイス全てに、共通の代替値を設定する
 ジョブで設定されているデバイスごとに、ユニークな代替値を設定する

OK キャンセル

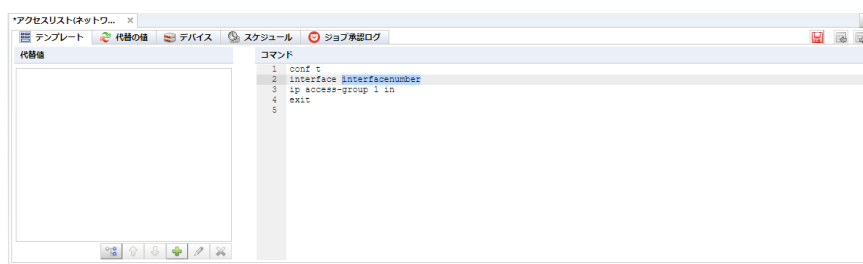
4. テンプレートに実行するコマンドを入力します。



5. 変数化する箇所を選択し、+をクリックします。

※変数化せずにこのままコマンドを実行する場合は、この手順をスキップします。

※今回のケースでは、コミュニティ名はコンフィグから取得する為、コミュニティ名の部分を変数化します。



6. 変数名を入力し、OK をクリックします。

代替値の追加

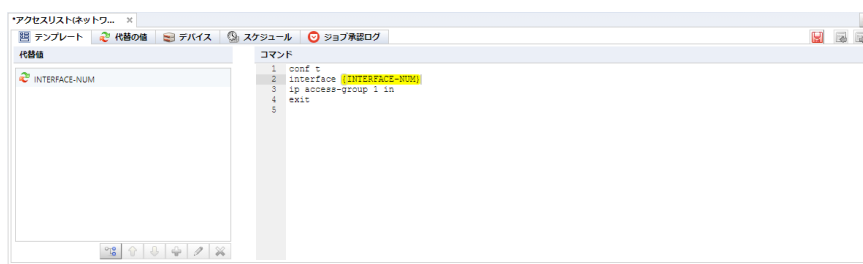
選択: interfacenumber

名前:

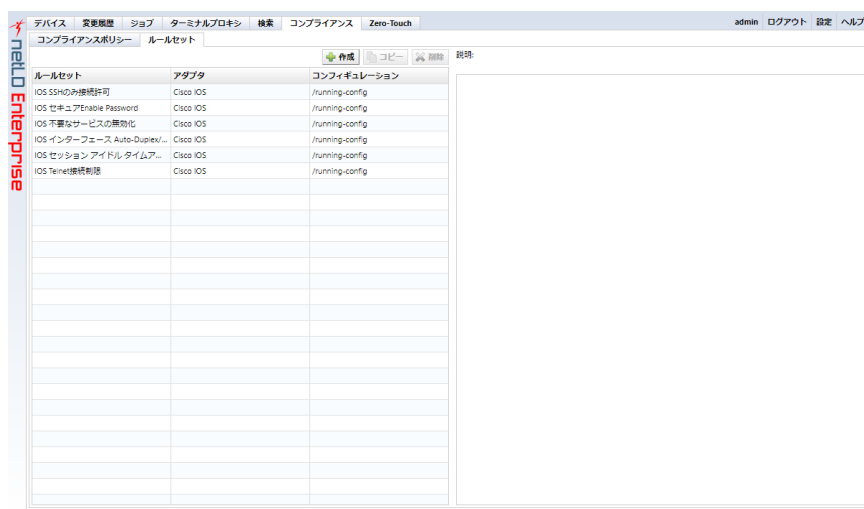
タイプ: テキスト

選択した値をデフォルトとして使用する

7. 保存します。



8. コンプライアンス→ルールセットに移動し、作成をクリックします。



9. ルール名を入力し、およびアダプタを選択し、OK をクリックします。

※アダプタはバルクチェンジ作成時に選択したアダプタを選択してください。

ルールセット

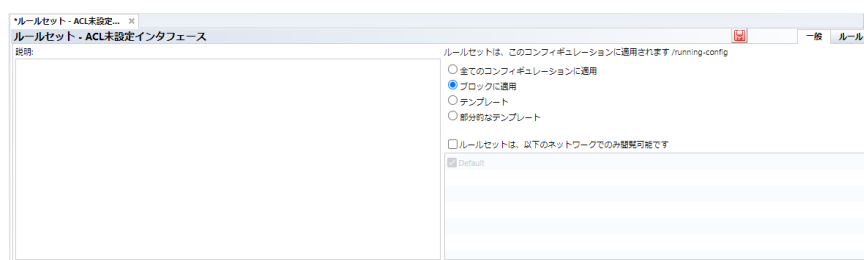
名前:
ACL未設定インタフェース

アダプタ:
Cisco IOS

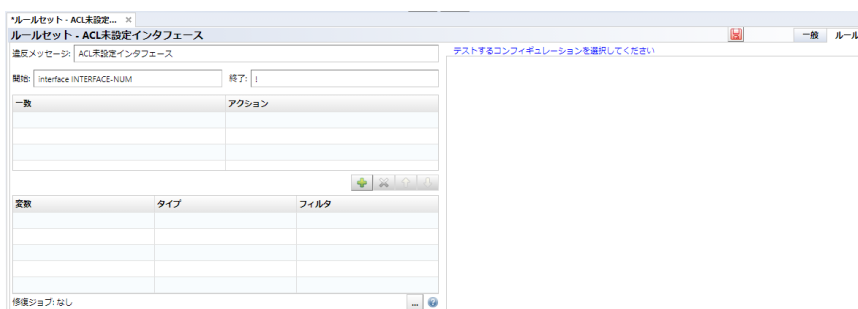
コンフィギュレーション:
/running-config

OK キャンセル

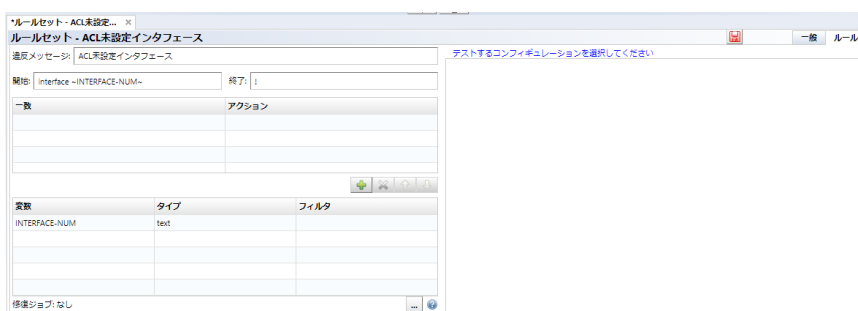
10. 一般タブに移動し、「ブロックに適用」を選択します。



11. ルールを適用するブロックを「開始/終了」で指定します。

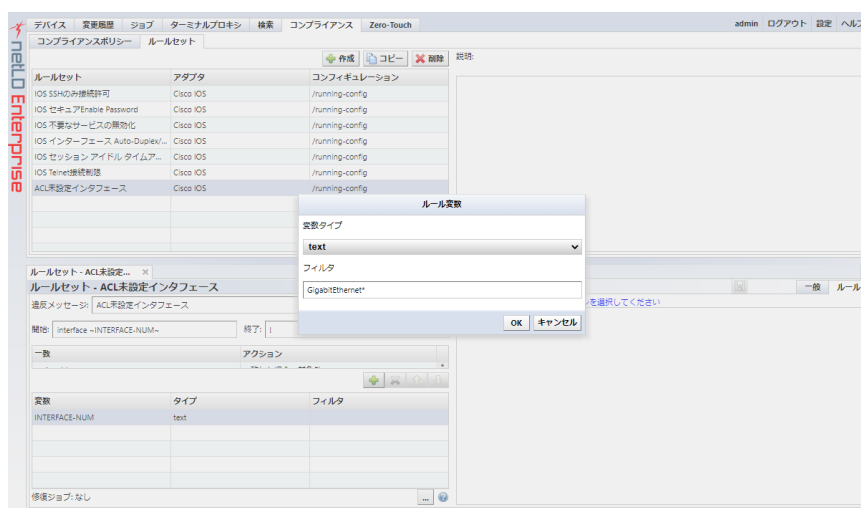


12. インタフェース番号の部分を変数名に指定し「~」で挟みます。

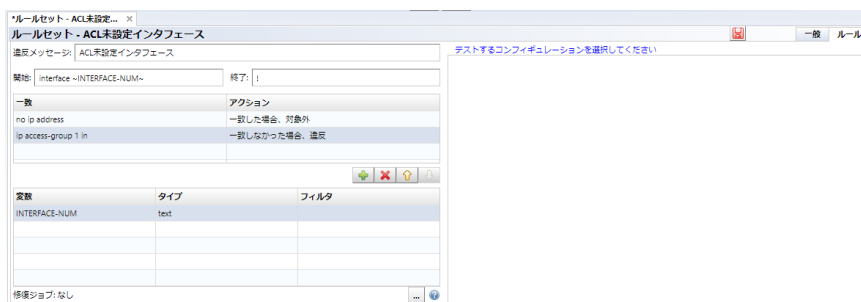


13. 追加された変数をダブルクリックし、テキストフィルタを追加します。

※今回は GigabitEthernet のインタフェースを対象とするため、「GigabitEthernet*」を指定します。

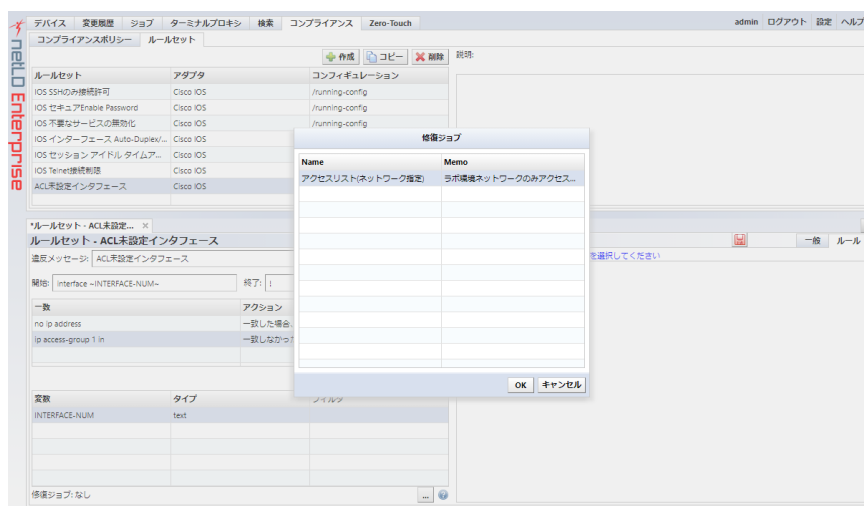


14. +をクリックし、一致条件を追加します。

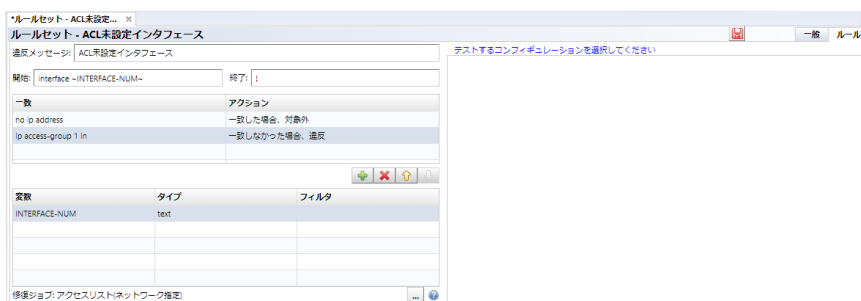


15. 修復ジョブの「…」をクリックし、違反時に実行するバルクチェンジジョブを指定します。

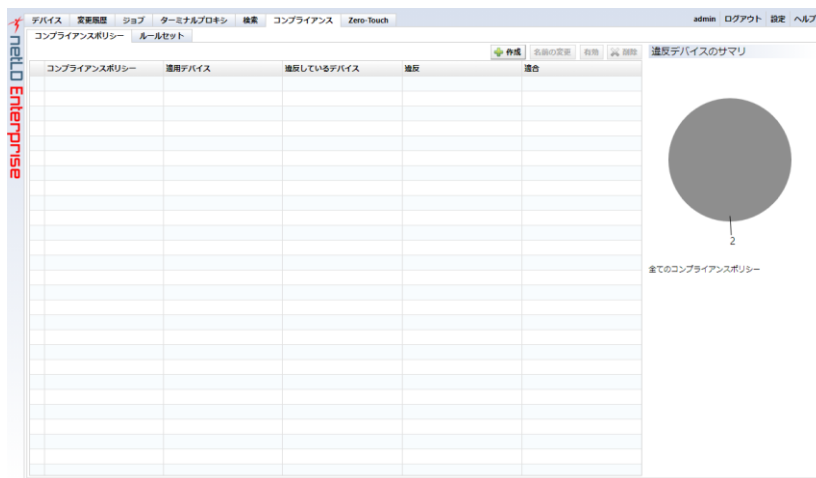
※指定できるジョブは1つです。



16. 設定を保存します。



17. コンプライアンス→コンプライアンスポリシーに移動し、作成をクリックします。

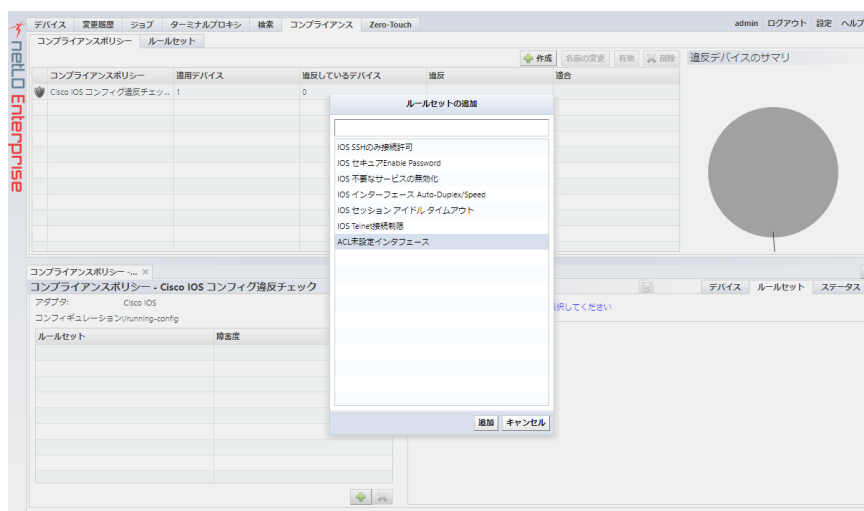


18. 名前を入力後、アダプタおよび対象のコンフィギュレーションファイルを選択し、OK をクリックします。

The screenshot shows a configuration dialog box titled 'コンプライアンスポリシー'. It contains the following fields and options:

- 名前:** A text input field containing 'Cisco IOS コンフィグ違反チェック'.
- アダプタ:** A dropdown menu with 'Cisco IOS' selected.
- コンフィギュレーション:** A dropdown menu with '/running-config' selected.
- Buttons:** 'OK' and 'キャンセル' (Cancel) buttons at the bottom right.

19. +をクリックし、ルールセットを追加します。



20. 保存をクリックします。



21. 作成したコンプライアンスポリシーを選択し、「有効」をクリックします。




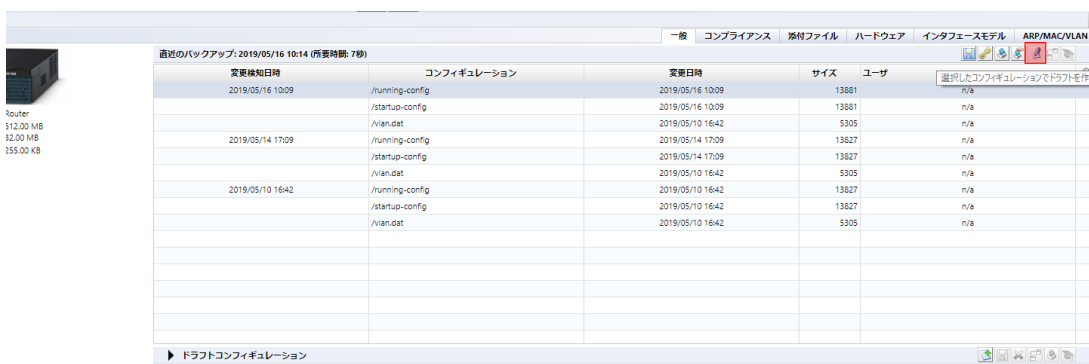
7.6 ドラフトコンフィギュレーション Suite

ドラフトコンフィギュレーションとは、バックアップ履歴と独立に保存されたコンフィギュレーションのことです。その性質はバックアップされた普通のコンフィグ履歴と殆ど同じですが、いくつか追加要素があります。たとえば、それぞれに名前を与えることができ、外部のプレーンテキストに保存すること、およびインポートすることが可能です。この機能は、同じデバイスコンフィギュレーションを何度か再利用する場合に便利です。

7.6.1 ドラフトコンフィギュレーションの作成

ドラフトコンフィギュレーションは、既存のコンフィギュレーション履歴からコピーして作ることが出来ます。

1. 対象デバイスをダブルクリックしてコンフィグ履歴を開いてください。
2. ドラフトコンフィギュレーションのベースとなるものを選択し、 ボタンをクリックします。



3. ドラフトコンフィギュレーションの名前を入力し、OK をクリックします。

ドラフトコンフィギュレーション

ファイル名:

4. 作成されたドラフトコンフィギュレーションをダブルクリックします。

最近のバックアップ: 2019/05/16 10:14 (所要時間: 7秒)

変更検知日時	コンフィギュレーション	変更日時	サイズ	ユーザ
2019/05/16 10:09	/running-config	2019/05/16 10:09	13881	n/a
	/startup-config	2019/05/16 10:09	13881	n/a
	/vlan.dat	2019/05/10 16:42	5305	n/a
2019/05/14 17:09	/running-config	2019/05/14 17:09	13827	n/a
	/startup-config	2019/05/14 17:09	13827	n/a
	/vlan.dat	2019/05/10 16:42	5305	n/a
2019/05/10 16:42	/running-config	2019/05/10 16:42	13827	n/a

ドラフト	最終変更	サイズ	ユーザ
sample-config	2019/05/20 14:50	13881	admin

5. コンフィギュレーションを編集し、 ボタンをクリックします。

```

sample-config
1 version 15.4
2 service timestamps debug datetime msec
3 service timestamps log datetime msec
4 no service password-encryption
5 !
6 hostname Cisco1921
7 !
8 boot-start-marker
9 boot-end-marker
10 !
11 !
12 enable secret 5 $1$xiIh$bfnrSP8pJzxWVtOhFF9AN/
13 !
14 no aaa new-model

```

```

sample-config
1 version 15.4
2 service timestamps debug datetime msec
3 service timestamps log datetime msec
4 no service password-encryption
5 !
6 hostname Cisco1921labo
7 !
8 boot-start-marker
9 boot-end-marker
10 !
11 !
12 enable secret 5 $1$xiIh$bfnrSP8pJzxWVtOhFF9AN/
13 !
14 no aaa new-model

```

```

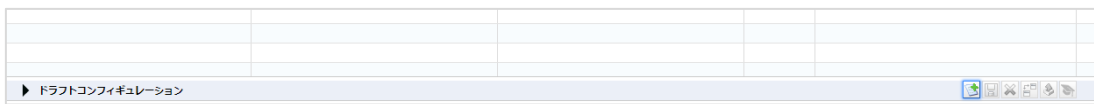
sample-config@10.8.8.250
sample-config
1 version 15.4
2 service timestamps debug datetime msec
3 service timestamps log datetime msec
4 no service password-encryption
5 !
6 hostname Cisco1921labo
7 !
8 boot-start-marker
9 boot-end-marker
10 !
11 !
12 enable secret 5 $1$xiIh$bfnrSP8pJzxWVtOhFF9AN/
13 !
14 no aaa new-model
15 !
16 !

```

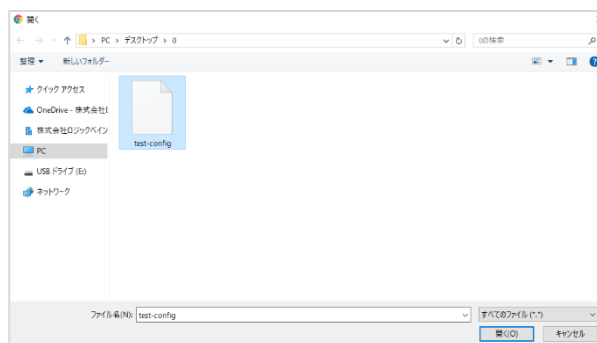
7.6.2 プレーンテキストからドラフトコンフィギュレーションをインポートする

テキストエディタ等で編集したコンフィギュレーションをインポートすることで、ドラフトコンフィギュレーションを作成することができます。まず、デバイスビューで対象デバイスをダブルクリックし、コンフィグ履歴を表示してください。

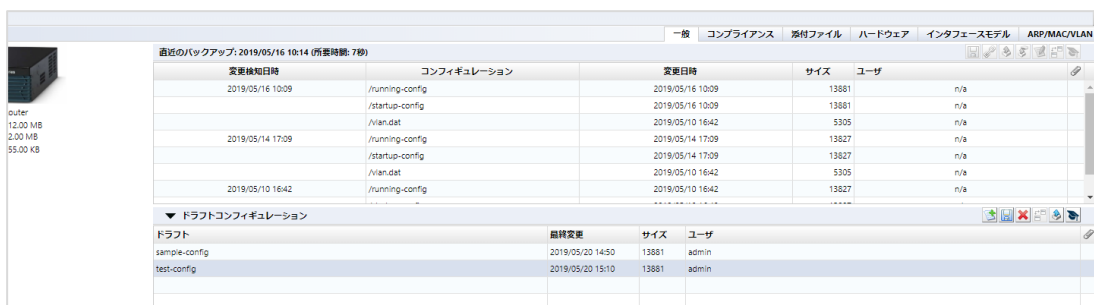
1. ステータスペインで  ボタンを押してください。



2. インポートするファイルを選択し、「開く」をクリックします。



テキストファイルの内容がインポートされ、ドラフトコンフィギュレーションが作成されます。

A screenshot of a configuration history table. The table has columns for '変更後日時' (After Change Date), 'コンフィギュレーション' (Configuration), '変更日時' (Change Date), 'サイズ' (Size), and 'ユーザ' (User). The table shows several rows of configuration changes. At the bottom, there is a section for 'ドラフトコンフィギュレーション' (Draft Configuration) with a sub-table showing the newly imported 'test-config' draft.


変更後日時	コンフィギュレーション	変更日時	サイズ	ユーザ
2019/05/16 10:09	/running-config	2019/05/16 10:09	13881	n/a
	/startup-config	2019/05/16 10:09	13881	n/a
	/vlan.dat	2019/05/10 16:42	9305	n/a
2019/05/14 17:09	/running-config	2019/05/14 17:09	13827	n/a
	/startup-config	2019/05/14 17:09	13827	n/a
	/vlan.dat	2019/05/10 16:42	9305	n/a
2019/05/10 16:42	/running-config	2019/05/10 16:42	13827	n/a

ドラフト	最終変更	サイズ	ユーザ
sample-config	2019/05/20 14:50	13881	admin
test-config	2019/05/20 15:10	13881	admin


7.6.3 ドラフトをエクスポートする

エクスポートするには  ボタンを押してください。

7.6.4 ドラフトを削除する

削除するには  ボタンを押してください。

7.6.5 ドラフト同士の比較

コンフィギュレーションを比較するには  ボタンを押します。ドラフトコンフィグでも、通常のコンフィグと同様の比較機能を使用することができます。詳しくは、「[6.3.5 コンフィグの比較](#)」を参照してください。




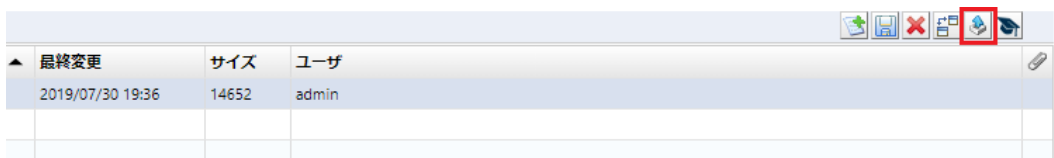
変更検知日時	コンフィギュレーション	変更日時	サイズ	ユーザ
2019/07/29 13:14	/running-config	2019/07/29 13:14	14652	n/a
	/startup-config	2019/07/29 13:14	14652	n/a
	/vian.dat	2019/06/25 17:55	916	n/a
2019/06/27 15:05	/running-config	2019/06/27 15:05	14022	n/a
	/startup-config	2019/06/27 15:05	14088	n/a
	/vian.dat	2019/06/25 17:55	916	n/a
2019/06/25 17:55	/running-config	2019/06/25 17:55	13883	n/a

ドラフト	最終変更	サイズ	ユーザ
test1	2019/07/30 19:36	14652	admin

7.6.6 ドラフトコンフィギュレーションをデバイスに適用する

ドラフトの比較と同じく、ドラフトの適用もバックアップコンフィグの適用(復元)と同じ手順で行うことができます。ただし、ただ一点異なる点が生じます。

アップロードするドラフトコンフィギュレーションを選び、 ボタンを押してください。



最終変更	サイズ	ユーザ
2019/07/30 19:36	14652	admin

running-config と startup-config のどちらにアップロードするかを選択してください。この点が履歴のアップロードとの唯一の相違点です。(履歴のアップロードでは、running-config は running-config に、startup-config は startup-config にそれぞれアップロードされます。)

ドラフトの挿入

投入予定のコンフィギュレーション:


OK を押してアップロードを開始してください。

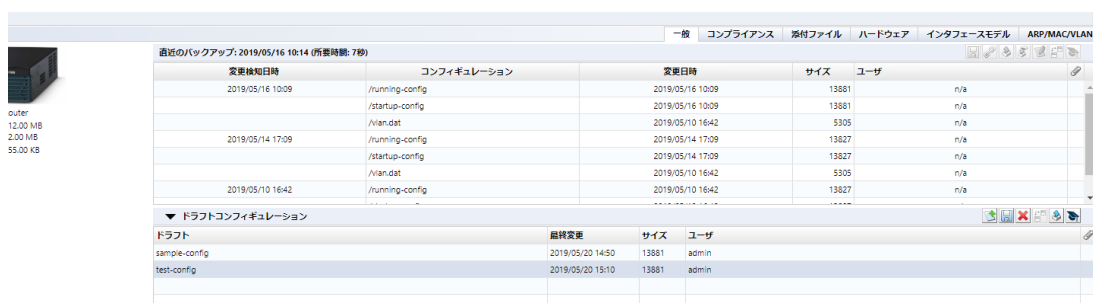
コンフィギュレーションの復元

コンフィギュレーションの復元中

7.7 チェンジアダバイザ Suite

チェンジアダバイザは、現在のコンフィグと指定されたコンフィグを読み込み、前者を後者に変更するために必要な設定変更コマンドを出力してくれる機能です。(この機能は一部デバイスでは使用出来ません。)

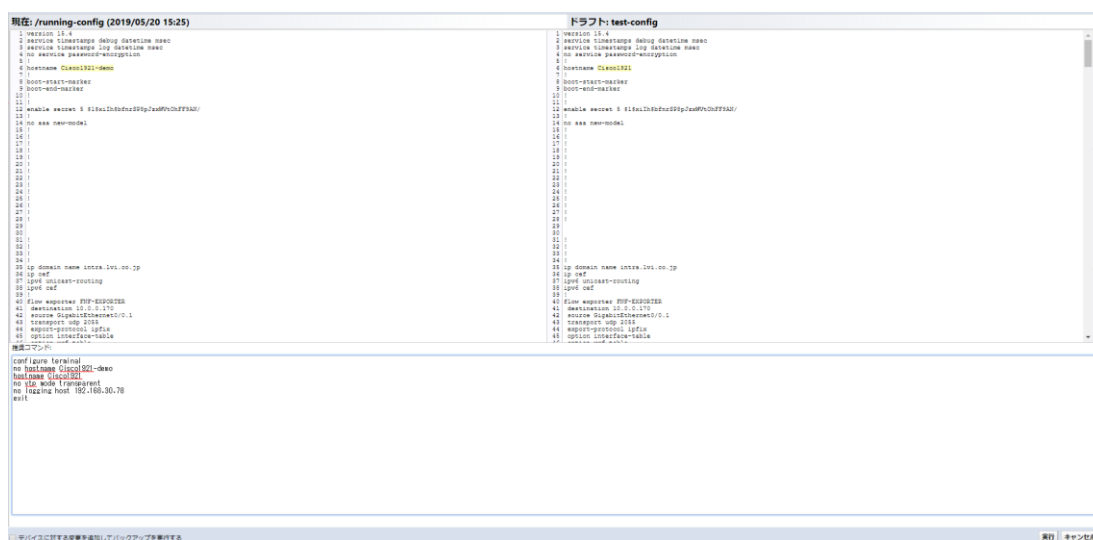
1. デバイスビューでデバイスをダブルクリックしてください。
2. コンフィギュレーション履歴あるいはドラフトから、コンフィグを選んでください。
3.  ボタンを押してください。



変更後日時	コンフィギュレーション	変更日時	サイズ	ユーザ
2019/05/16 10:09	/running-config	2019/05/16 10:09	13881	n/a
	/startup-config	2019/05/16 10:09	13881	n/a
	/vlan.dat	2019/05/10 16:42	5305	n/a
2019/05/14 17:09	/running-config	2019/05/14 17:09	13827	n/a
	/startup-config	2019/05/14 17:09	13827	n/a
	/vlan.dat	2019/05/10 16:42	5305	n/a
2019/05/10 16:42	/running-config	2019/05/10 16:42	13827	n/a

ドラフト	最終変更	サイズ	ユーザ
sample-config	2019/05/20 14:50	13881	admin
test-config	2019/05/20 15:10	13881	admin

4. チェンジアダバイザが起動し、下側のペインでコマンドが提示されます。



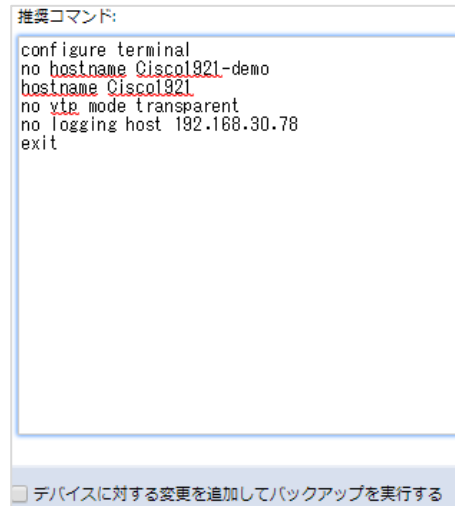
```
現在: /running-config (2019/05/20 15:25)
1 version 15.6
2 REVVIEW timestamps debug datetime msec
3 REVVIEW timestamps log datetime msec
4 no REVVIEW password-encryption
5 !
6 hostname Cisco321-0000
7 boot-start-marker
8 boot-end-marker
9 !
10 !
11 !
12 enable secret 5 $1ilal2h8dnu$Pp2aW0h0uFF3A2/
13 !
14 no aaa new-model
15 !
16 !
17 !
18 !
19 !
20 !
21 !
22 !
23 !
24 !
25 !
26 !
27 !
28 !
29 !
30 !
31 !
32 !
33 !
34 !
35 !
36 ip domain name lvsr.lvs.co.jp
37 !
38 !
39 ip route 0.0.0.0 0.0.0.0 192.168.80.78
40 !
41 !
42 !
43 !
44 !
45 !
46 !
47 !
48 !
49 !
50 !
51 !
52 !
53 !
54 !
55 !
56 !
57 !
58 !
59 !
60 !
61 !
62 !
63 !
64 !
65 !
66 !
67 !
68 !
69 !
70 !
71 !
72 !
73 !
74 !
75 !
76 !
77 !
78 !
79 !
80 !
81 !
82 !
83 !
84 !
85 !
86 !
87 !
88 !
89 !
90 !
91 !
92 !
93 !
94 !
95 !
96 !
97 !
98 !
99 !
100 !

ドラフト: test-config
1 version 15.6
2 REVVIEW timestamps debug datetime msec
3 REVVIEW timestamps log datetime msec
4 no REVVIEW password-encryption
5 !
6 hostname Cisco321
7 boot-start-marker
8 boot-end-marker
9 !
10 !
11 !
12 enable secret 5 $1ilal2h8dnu$Pp2aW0h0uFF3A2/
13 !
14 no aaa new-model
15 !
16 !
17 !
18 !
19 !
20 !
21 !
22 !
23 !
24 !
25 !
26 !
27 !
28 !
29 !
30 !
31 !
32 !
33 !
34 !
35 !
36 ip domain name lvsr.lvs.co.jp
37 !
38 !
39 ip route 0.0.0.0 0.0.0.0 192.168.80.78
40 !
41 !
42 !
43 !
44 !
45 !
46 !
47 !
48 !
49 !
50 !
51 !
52 !
53 !
54 !
55 !
56 !
57 !
58 !
59 !
60 !
61 !
62 !
63 !
64 !
65 !
66 !
67 !
68 !
69 !
70 !
71 !
72 !
73 !
74 !
75 !
76 !
77 !
78 !
79 !
80 !
81 !
82 !
83 !
84 !
85 !
86 !
87 !
88 !
89 !
90 !
91 !
92 !
93 !
94 !
95 !
96 !
97 !
98 !
99 !
100 !

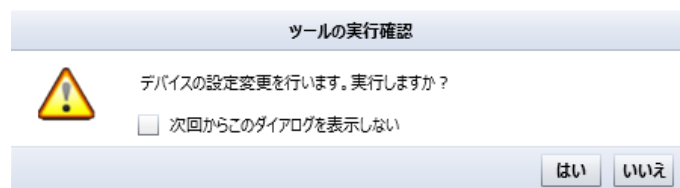
config terminal
no hostname Cisco321-0000
hostname Cisco321
no ip route 0.0.0.0 0.0.0.0 192.168.80.78
ip route 0.0.0.0 0.0.0.0 192.168.80.78
exit
```


7.7.1 チェンジアドバイザーを用いてコマンドを実行する

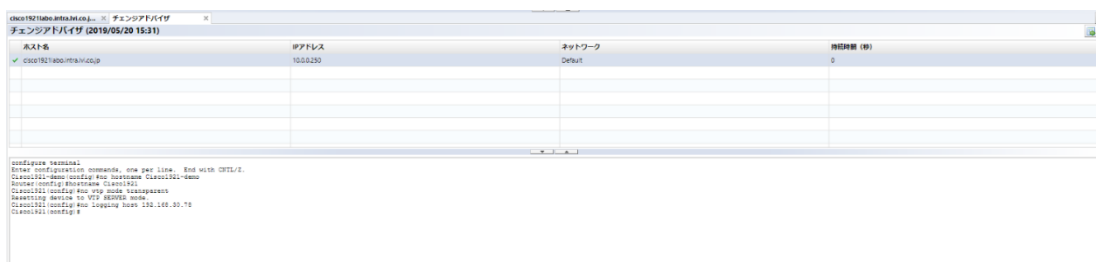
チェンジアドバイザーの出力したコマンドをデバイスで実行することが出来ます。提示されたコマンドを実行する前に、実行するコマンドを一度確認してください。不適切なコマンドがあった場合には、出力されたコマンドを直接編集することが出来ます。



その後、実行を押してください。はいを押して進みます。




コマンドを実行後、結果を確認することが出来ます。チェンジアドバイザーの実行結果・履歴はジョブ履歴にも表示されます。



コンフィギュレーションの復元やドラフトコンフィギュレーションのアップロードでは、主な通信プロトコルは TFTP です。したがって、復元およびアップロード機能は TFTP の実装されていないデバイスでは利用不可です。一方、チェンジアドバイザー機能は CLI ログイン (telnet/SSH) さえサポートしていれば利用できます。CLI ログインはほとんどの機種がサポートしておりますので、アップロードが利用不可能な環境でも、チェンジアドバイザーの機能を用いて代用することが出来ます。

7.8 閲覧ツール

閲覧ツールメニューから使用可能な機能は、選択したデバイスのリアルタイムの状況を知ることができます。検出された結果はまとめて CSV としてエクスポートすることも可能です。閲覧ツールを用いるときにはステータスペインに専用のタブが開かれるので、エクスポートは、その常に右上にある  ボタンから行うことができます。



7.8.1 DNS ルックアップ

デバイスの DNS 名前解決情報を表示します。



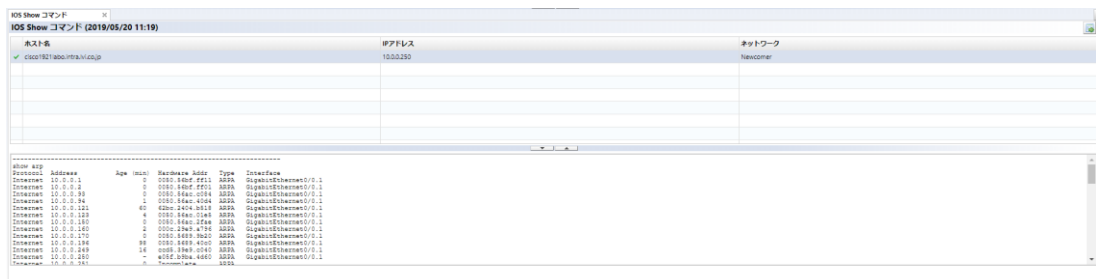
ホスト名	IPアドレス	ネットワーク	DNS名前解決
✓ S3100	10.0.3.8	192.168.40.152	S3100.intra.lvi.co.jp
✓ SI-R-220D	10.0.3.13	192.168.40.152	SI-R-220D.intra.lvi.co.jp
✓ SI-R_G100	10.0.3.15	192.168.40.152	SI-R-80brin.intra.lvi.co.jp
✓ SI-R-80brin	10.0.3.14	192.168.40.152	SI-R_G100.intra.lvi.co.jp
✓ SI-R_G200_1	10.0.3.12	192.168.40.152	SI-R_G200_1.intra.lvi.co.jp
✓ SR-S224TC2-Fujitsu	10.0.3.253	192.168.40.152	SR-S224TC2-Fujitsu.intra.lvi.co.jp
✓ Laco-1921	10.0.3.57	192.168.40.152	Laco-1921.intra.lvi.co.jp
✓ SRX-240	10.0.3.254	192.168.40.152	SRX-240.intra.lvi.co.jp

7.8.2 IOS Show コマンド

デバイスの IOS Show コマンドの結果を表示します。ただしこのコマンドは Cisco IOS と互換性のあるデバイス上でしか実行できません。はじめに実行する show コマンドをリストから選択し、実行を押すとコマンドが発行されます。



IOS Show コマンドを用いて、選択したデバイスに show arp コマンドを実行した際の結果画面が表示されます。



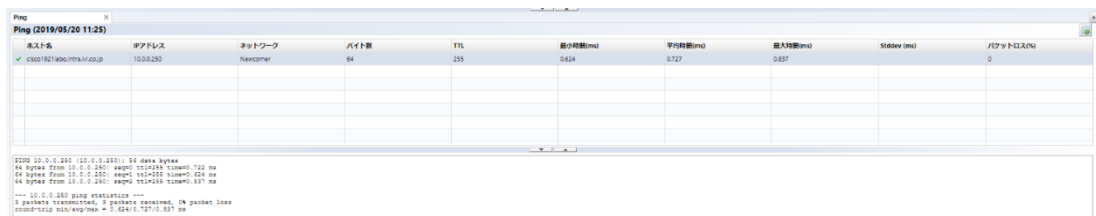
7.8.3 IP ルーティングテーブル

デバイスのルーティングテーブルを表示します。なお、この機能はデバイスを複数選択した状態では実行することができません。



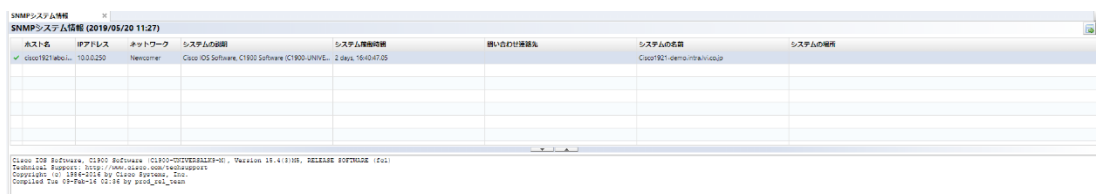
7.8.4 Ping

デバイスに対して Ping を実行し、レスポンスを確認します。



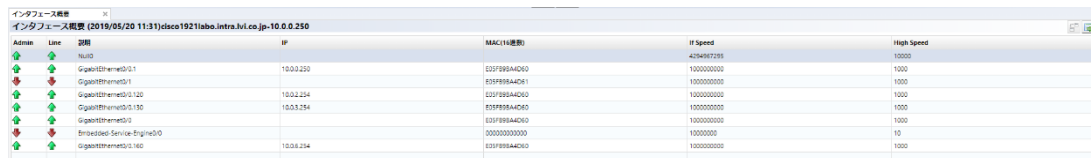
7.8.5 SNMP システム情報

デバイスの SNMP システム情報を表示します。



7.8.6 インタフェース概要

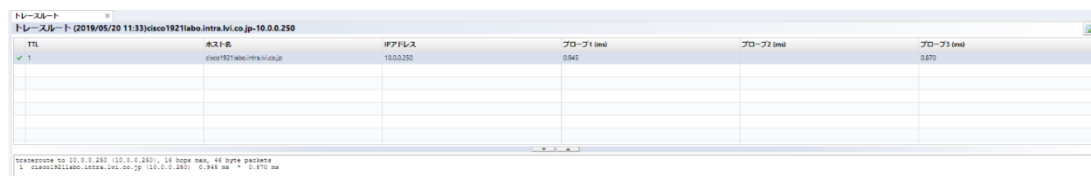
デバイスの各インタフェースの開閉状態、IP アドレス等の詳細情報を表示します。なお、この機能はデバイスを複数選択した状態では実行することができません。



Admin	Line	名前	IP	MAC(16進数)	IF Speed	High Speed
🟢		Null0			4294967295	1000
🟢		GigabitEthernet0/1	10.0.2.200	E37F98A4D60	1000000000	1000
🟢		GigabitEthernet0/1		E5F989A4D61	1000000000	1000
🟢		GigabitEthernet0/1:20	10.0.2.214	E27F98A4D60	1000000000	1000
🟢		GigabitEthernet0/1:80	10.0.2.214	E5F989A4D60	1000000000	1000
🟢		GigabitEthernet0/0		E37F98A4D60	1000000000	1000
🟢		Embedded-Service-Engine0/0		000000000000	1000000000	10
🟢		GigabitEthernet0/1:60	10.0.2.214	E37F98A4D60	1000000000	1000

7.8.7 トレースルート

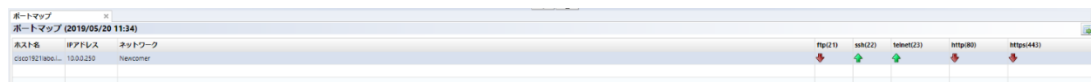
デバイスに対してトレースルートを行い、レスポンスを表示します。なお、この機能はデバイスを複数選択した状態では実行することができません。



TTL	ホスト名	IPアドレス	プローブ1 (ms)	プローブ2 (ms)	プローブ3 (ms)
1	cisco1921labo.intra.lvi.co.jp	10.0.2.200	0.941		0.870

7.8.8 ポートマップ

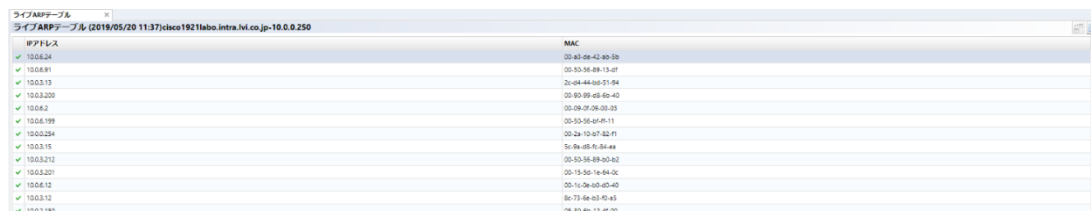
デバイスのポート開閉情報を表示します。



ホスト名	IPアドレス	ネットワーク	Tftp(21)	Ssh(22)	Telnet(23)	Http(80)	Https(443)
cisco1921labo...	10.0.2.200	Networker	🔴	🟢	🟢	🔴	🔴

7.8.9 ライブの ARP テーブル

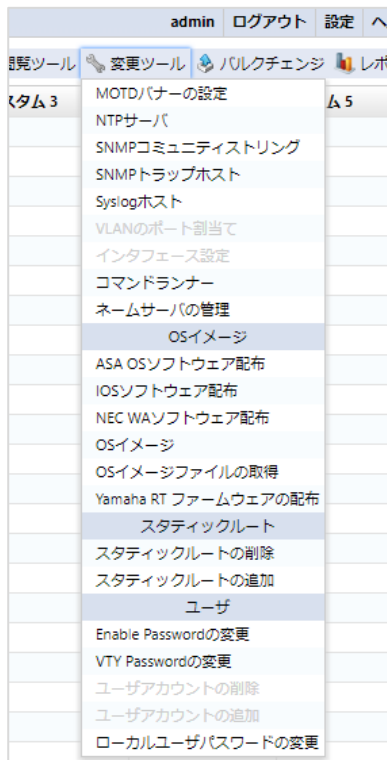
ARP テーブルのライブステータスを表示します。なお、この機能はデバイスを複数選択した状態では実行することができません。



IPアドレス	MAC
10.0.2.24	00-00-00-00-00-00
10.0.897	00-50-56-8F-05-0F
10.0.310	20-00-44-00-00-00
10.0.200	00-80-80-80-80-80
10.0.2	00-08-00-20-00-00
10.0.199	00-50-56-8F-05-11
10.0.204	00-20-10-07-02-F1
10.0.10	50-00-00-00-00-00
10.0.212	00-50-56-8F-00-02
10.0.201	00-10-00-10-00-00
10.0.12	00-10-00-00-00-00
10.0.12	00-70-00-00-00-00
10.0.180	00-00-00-00-00-00

7.9 変更ツール Suite

変更ツールメニューは、選択したデバイスのコンフィグを変更することに関連する操作を集めています。この章では、この変更ツールサブメニューにあるそれぞれの機能を上から順に解説していきます。



7.9.1 MOTD バナーの設定

デバイスのログインバナーを設定します。

MOTDバナーの設定

ログインバナー

Welcome to LogicVein Network

ツール実行の完了後、バックアップを実行する

7.9.2 NTP サーバ

NTP サーバをデバイスに追加/削除します。

NTPサーバ

追加するNTPサーバ

削除するNTPサーバ

ツール実行の完了後、バックアップを実行する

7.9.3 SNMP コミュニティストリング

デバイスに対して、SNMP コミュニティを追加/削除します。

SNMPコミュニティストリング	
新しいコミュニティ名	
コミュニティ名	<input type="text" value="public"/>
アクセスタイプ	<input type="text" value="RO"/>
コミュニティ名を消す	
コミュニティ名	<input type="text" value="lvi"/>
アクセスタイプ	<input type="text" value="RO"/>
<input type="checkbox"/> ツール実行の完了後、バックアップを実行する	<input type="button" value="実行"/> <input type="button" value="キャンセル"/>

7.9.4 SNMP トラップホスト

デバイスに対して、SNMP トラップホスト設定を追加/削除します。NMS 新規導入の一括設定に威力を発揮します。

SNMPトラップホスト	
新しいトラップホスト名	
トラップホスト名/アドレス	<input type="text" value="public"/>
新しいコミュニティ名	
コミュニティ名	<input type="text" value="192.168.0.100"/>
アクション (追加/削除)	<input type="text" value="add"/>
<input type="checkbox"/> ツール実行の完了後、バックアップを実行する	<input type="button" value="実行"/> <input type="button" value="キャンセル"/>

7.9.5 Syslog ホスト

デバイスに対して、Syslog ホストを追加/削除します。

Syslogホスト	
追加するロギングホスト	<input type="text" value="192.168.0.100"/>
削除するロギングホスト	<input type="text"/>
<input type="checkbox"/> ツール実行の完了後、バックアップを実行する	<input type="button" value="実行"/> <input type="button" value="キャンセル"/>

7.9.6 VLAN のポート割当て

デバイスのアクセスポートに対して、VLAN ポートの設定を実行します。なお、この機能はデバイスを複数選択した状態では実行することができません。

画面のインタフェースを選択してくださいから、VLAN 設定対象のインタフェースを選択(複数選択可)し、VLAN を選択してください。欄から割り当てる VLAN を選択して OK ボタンをクリックします。

VLANのポート割当て

インタフェースを選択してください

Embedded-Service-Engine0/0
GigabitEthernet0/0
GigabitEthernet0/1
GigabitEthernet0/0/0

VLANを選択してください

Name	Number
default	1
fddi-default	1002
token-ring-default	1003
fddinet-default	1004
trnet-default	1005

ツール実行の完了後、バックアップを実行する 実行 キャンセル

7.9.7 インタフェース設定

デバイスインタフェースの Admin Status を変更します。なお、この機能はデバイスを複数選択した状態では実行することができません。

「インタフェースを選択してください」欄から、Admin Status を変更するインタフェースを選択(複数選択可)し、プルダウンメニューで Up/Down を選択して「実行」ボタンをクリックします。

インタフェース設定

インタフェースを選択してください

Admin	Interface
down	Embedded-Service-Engine0/0
up	GigabitEthernet0/0
up	GigabitEthernet0/1
up	GigabitEthernet0/0/0

選択したインタフェースをUp/Downする UP

ツール実行の完了後、バックアップを実行する 実行 キャンセル

7.9.8 コマンドランナー

コマンドランナーは、複数のデバイスに同一の操作を繰り返し行う時に便利なツールです。たとえば、100 行以上のコマンドを沢山のデバイスに一度に実行できます。行うことのできるコマンドは、コンフィギュレーションのダウンロードやアップロードが含まれます。必要な項目を入力後、実行ボタンを押してください。

コマンドランナー

このデバイスに対して実行するコマンドを指定してください

デフォルトの正規表現より優先する

応答タイムアウト(秒): 60

ツール実行の完了後、バックアップを実行する

実行 キャンセル

デフォルトの正規表現より優先するという欄は、特定のタイプのプロンプトにマッチする正規表現を指定します。マッチされるプロンプトは、シェルスクリプトで言えば PS1 変数のようなものです。この欄を指定する必要があるのは、あるコマンドが通常と異なるプロンプトを用いた返答をする場合です。たとえば、一部のインタラクティブなコマンドは通常『<username>#』で始まるプロンプトではなく、よりシンプルな『<』で始まるコマンドを用いて次の入力を促してくるかもしれません。その場合には、それを正規表現 ^< (行頭の<)で指定する必要があります。そうしなくては、コマンドの出力結果とプロンプトを区別することができなくなってしまいます。

7.9.9 ASA OS ソフトウェア配布

Cisco ASA のデバイスに対して OS をリモート配布することができます。本機能を使用するには、予め OS を保存しておく必要があります。保存方法の詳細については「[7.9.12 OS イメージ](#)」を参照してください。

ASA OSソフトウェア配布

転送するASA OSイメージファイルを選択してください... ...

flash転送先

オプション

既存のイメージをflashから削除する

新しいイメージでブートする

イメージ転送後にリロードする

ツール実行の完了後、バックアップを実行する

実行 キャンセル

項目	説明
転送する ASA OS イメージファイルを選択してください	右側の [...] ボタンを押すと、登録してある OS イメージをブラウザするウィンドウが現れますので、アップロードするイメージを選択してください。
flash 転送先	デバイスの備える記憶ドライブを指定します。
既存のイメージを flash から削除する	---
新しいイメージでブートする	イメージ転送後、新しいイメージでブートする
イメージ転送後にリロードする	イメージ転送後、新しいイメージでリロードする

7.9.10 IOS ソフトウェア配布

Cisco IOS のデバイスに対して IOS をリモート配布することができます。本機能を使用するには、予め IOS を保存しておく必要があります。保存方法の詳細については「[7.9.12 OS イメージ](#)」を参照してください。

IOSソフトウェア配布

転送するIOSイメージファイルを選択してください...

flash転送先

オプション

flashディレクトリ先

flashパーティション先

既存のイメージをflashから削除する

新しいイメージでブートする

イメージ転送後にリロードする

空き容量の事前チェック

ツール実行の完了後、バックアップを実行する

項目	説明
転送する IOS イメージファイルを選択してください	右側の [...] ボタンを押すと、登録してある OS イメージをブラウザするウィンドウが現れますので、アップロードするイメージを選択してください。
flash 転送先	デバイスの備える記憶ドライブを指定します。機種によって、flashusbflash0nvram など、指定できる内容が異なります。
flash ディレクトリ先	転送先ドライブ・パーティション内のディレクトリ。ディレクトリが存在しないときは、指定した名前のディレクトリが自動で生成されます。
flash パーティション先	転送先ドライブのパーティション。指定されたパーティションが存在しない場合にはコマンドは失敗します。
既存のイメージを flash から削除する	---
新しいイメージでブートする	イメージ転送後、新しいイメージでブートする
イメージ転送後にリロードする	イメージ転送後、新しいイメージをリロードする
メモリ要件の事前チェック(DRAM)	http://cisco.com にて投入するイメージの DRAM 容量を確認し、入力してください。イメージの投入前に、デバイスに十分な空き容量があるかどうかを確認します
ツールの完了後、バックアップを実行する	---


7.9.11 NEC WA ソフトウェア配布

NEC WA ソフトウェアをリモート OS 配布することができます。本機能を使用するには、予め WA ソフトウェアを保存しておく必要があります。保存方法の詳細については「[7.9.12 OS イメージ](#)」を参照してください。




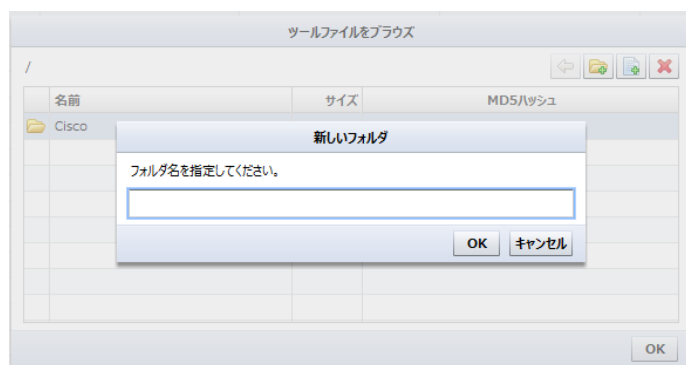
項目	説明
flash ディレクトリ先	転送先のディレクトリ
既存のイメージを flash から削除する	既存のイメージを flash から削除する
新しいイメージでブートする	イメージ転送後、新しいイメージでブートする設定をする
イメージ転送後にリロードする	イメージ転送後にリロードする

7.9.12 OS イメージ

ソフトウェア配布に使用する OS イメージをサーバのファイルシステム上に保存します。 ボタンをクリックし、OS イメージファイルを追加します。



 ボタンを押すと、サーバのファイルシステム上にディレクトリを追加できます。



OS イメージがリストに追加されたら、OK ボタンを押します。

OS イメージの追加には時間がかかる場合があります。時間がかかりすぎる場合、または追加されない場合は、指定したディレクトリを確認し、再度ファイルの追加を試みてください。

7.9.13 OS イメージファイルの取得

指定したデバイスから OS イメージをダウンロードしてデータベースに保存します。ダウンロードしたイメージは後に再びアップロードすることができます。

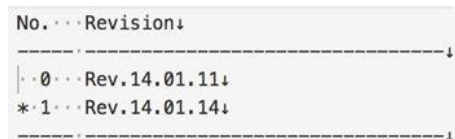


7.9.14 Yamaha RT ファームウェアの配布

Yamaha RT ソフトウェアをリモート OS 配布することができます。本機能を使用するには、予め Yamaha RT ソフトウェアを保存しておく必要があります。保存方法の詳細については「[7.9.12 OS イメージ](#)」を参照してください。

項目	説明
ファームウェアファイルを選択	対象のファームウェアファイルを選択
ファームウェアのリビジョンアップ先のエリアを指定	複数のファームウェアをサポートする機種では ROM エリア番号(1,0)を選択可能。指定しない場合は稼働中のファームウェアがアップグレードされる。
現在稼働中のファームウェアファイルを内蔵フラッシュにコピー	複数ファームウェアをサポートする機種で稼働中のファームウェアのバックアップを行う※1
アップグレードする前に設定を保持し、アップグレード用一時設定を導入	ファームウェアのアップロードを行う前に設定を保存して、コマンドを実行※2
最小限の空きメモリ	設定したメモリを超えた場合にファームウェアアップグレードを中止させることが可能※3
最大待機時間	ネットワークの通信遅延が多い環境で待機時間を指定
ツール実行の完了後、バックアップを実行する	ファームウェア配布時に Yamaha 機器はデバイスの仕様として再起動を行います。チェックを入れることでバックアップを実行しますが、デバイスの再起動中の為に失敗します。

※1: 以下の場合は Rev.14.01.14 が稼働中の為、このファームウェアのバックアップが行われます。



複数のファームウェアをサポートしない機種でこのチェックを行った場合、ファームウェアのアップグレードは中止されます。また、リビジョンアップ先の ROM 番号と稼働中のファームウェアの ROM 番号が同じ場合にもアップグレードは中止されます。

※2: 下記のコマンドが実行されます。

```
login timer [timer]
```

```
show config | grep "tftp host"
```

```
tftp host [ThirdEye IP]
```

※3: 以下のメモリ使用量の場合、80 を設定する事でファームウェアアップグレードは中止されます。

```
CPU: ... 0%(5sec) ... 0%(1min) ... 0%(5min) ... Memory: 82% used
Packet-buffer: ... 0%(small) ... 0%(middle) ... 7%(large) ... 0%(huge) used
```

7.9.15 スタティックルートの追加

必要な情報を入力し、実行を押すと、ルートが追加されます。

スタティックルートの追加	
デスティネーション	
デスティネーションアドレス (IPアドレス)	10.0.100.0
デスティネーションサブネットマスク (IPマスク)	255.255.255.0
ゲートウェイ	
ゲートウェイアドレス (IPアドレス)	10.0.0.30
<input type="checkbox"/> ツール実行の完了後、バックアップを実行する	
<input type="button" value="実行"/> <input type="button" value="キャンセル"/>	

7.9.16 スタティックルートの削除

既存のスタティックルート設定を選択して削除します。

スタティックルートの削除		
スタティックルートを選択		
ゲートウェイ	宛先マスク	宛先アドレス
10.0.0.250	24	10.0.2.0
10.0.0.211	24	10.0.3.0
10.0.0.51	16	10.128.0.0
192.168.0.247	24	192.168.20.0
<input type="checkbox"/> ツール実行の完了後、バックアップを実行する		
<input type="button" value="実行"/> <input type="button" value="キャンセル"/>		

7.9.17 Enable Password の変更

デバイスの Enable Password または Enable Secret の設定を変更します。Enable Password が設定されている場合は Enable Password が変更され、Enable Secret が設定されている場合は Enable Secret が変更されます。両方が設定されている場合は Enable Secret が変更されます。

Enable Passwordの変更	
ユーザーデータ	
新しいパスワード	
パスワード: *****	確認: *****
<input type="checkbox"/> ツール実行の完了後、バックアップを実行する	実行 キャンセル

7.9.18 VTY Password の変更

デバイスの VTY Password の設定を変更します。

VTY Passwordの変更	
ユーザーデータ	
新しいパスワード	
パスワード: *****	確認: *****
<input type="checkbox"/> ツール実行の完了後、バックアップを実行する	実行 キャンセル

7.9.19 ユーザアカウントの削除

デバイスに設定されている既存のユーザアカウントを削除します。なお、この機能はデバイスを複数選択した状態では実行することができません。

ユーザアカウントの削除	
ユーザーデータ	
ユーザ名	logicvein
<input type="checkbox"/> ツール実行の完了後、バックアップを実行する	実行 キャンセル

7.9.20 ユーザアカウントの追加

デバイスに新規ユーザアカウントを追加します。なお、この機能はデバイスを複数選択した状態では実行することができません。

ユーザアカウントの追加	
ユーザーデータ	
ユーザ名	logicvein
パスワード	*****
ユーザ権限	SU
<input type="checkbox"/> ツール実行の完了後、バックアップを実行する	実行 キャンセル

7.9.21 ローカルユーザパスワードの変更

デバイスに設定されているユーザアカウントのパスワードを変更します。

ローカルユーザパスワードの変更	
ユーザデータ	
ユーザ名	logicvein
新しいパスワード	
パスワード: *****	確認: *****
<input type="checkbox"/> ツール実行の完了後、バックアップを実行する	<input type="button" value="実行"/> <input type="button" value="キャンセル"/>

7.10 バルクチェンジの概要 Suite

バルクチェンジ機能はコマンドランナーと似た機能ですが、より柔軟な機能を備えています。固定された一つのコマンドを発行する代わりに、コマンドをテンプレート化したものを作り、テンプレート変数を設けてデバイスごとに変数の値を変えることができます。

例えば、デバイスのパスワードを変更したいが、それぞれのデバイスに違うパスワードを設定したい場合、コマンドランナーではそれぞれのデバイスに対してジョブを実行する必要があります。

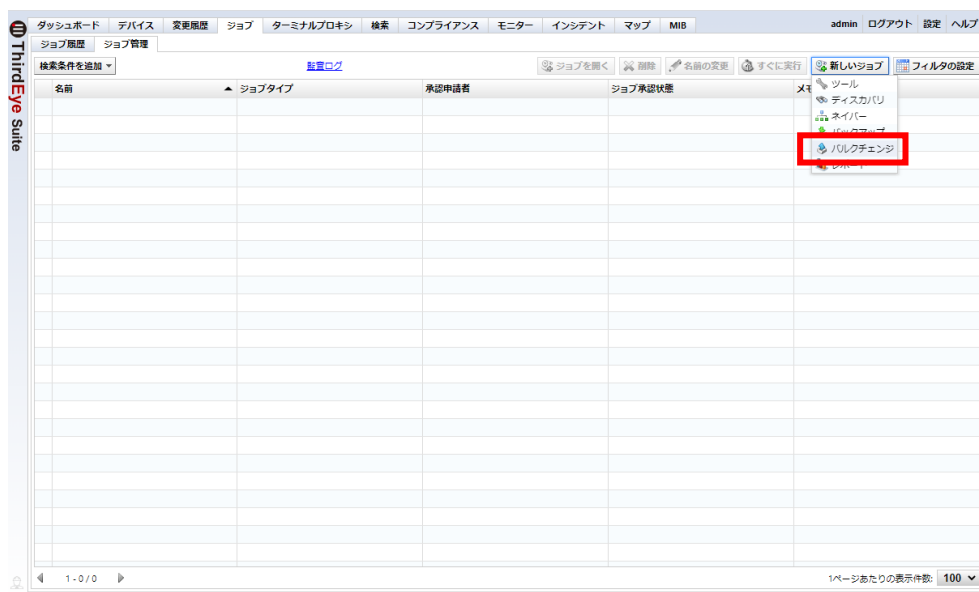
しかし、バルクチェンジを使用することで、パスワードを変数化し、それぞれのデバイスに別の値を割り振ることで、1回のジョブで違ったパスワードで設定をすることができます。

7.10.1 バルクチェンジジョブを作成する

バルクチェンジジョブは「ジョブ管理」から作成できます。ジョブの作成方法は「[6.10 ジョブ管理](#)

Enterprise Suite」を参照してください。

1. [ジョブ]タブ→[ジョブ管理]をクリックし、[新しいジョブ]→[バルクチェンジ]をクリックします。



2. ジョブ名、コメントを入力し、機能を選択し、[OK]をクリックします。

バルクチェンジジョブの作成

ジョブ名:
Cisco Enable/パスワード一括変更

コメント:
Enable/パスワード一括変更

修復ジョブを設定する

ジョブで設定されているデバイス全てに、共通の代替値を設定する

ジョブで設定されているデバイスごとに、ユニークな代替値を設定する

OK キャンセル

タイプ	説明
ジョブ名	バルクチェンジジョブの名前を入力します。
コメント	バルクチェンジジョブのコメント(説明)を入力します。
修復ジョブに設定する	バルクチェンジジョブを修復ジョブとして使用するかどうかを選択します。 選択された場合、追加でアダプタを選択します。
ジョブで設定されているデバイス全てに、共通の代替値を設定する または、 ジョブで設定されているデバイスごとに、ユニークな代替値を設定する	どちらか、1つを選択します。コマンドを実行する時に変数に同じ値を入れて実行するか違う値を入れて実行するか選択することができます。

3. テンプレートで、ベースとなるコマンドを入力します。

*Cisco Enable/パスワード... ※

テンプレート 代替の値 デバイス スケジュール ジョブ承認ログ


代替値

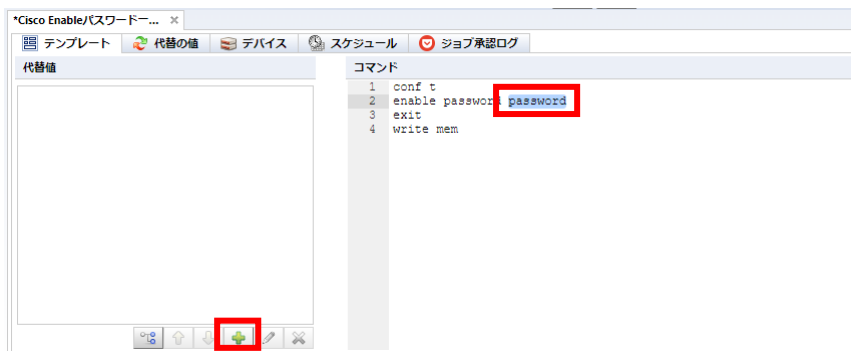
コマンド

```

1 conf t
2 enable password password
3 exit
4 write mem

```

4. 代替値として変更する部分を選択し、 ボタンをクリックします。



5. 代替値の名前を入力し、タイプを選択します。

代替値の追加

選択: password

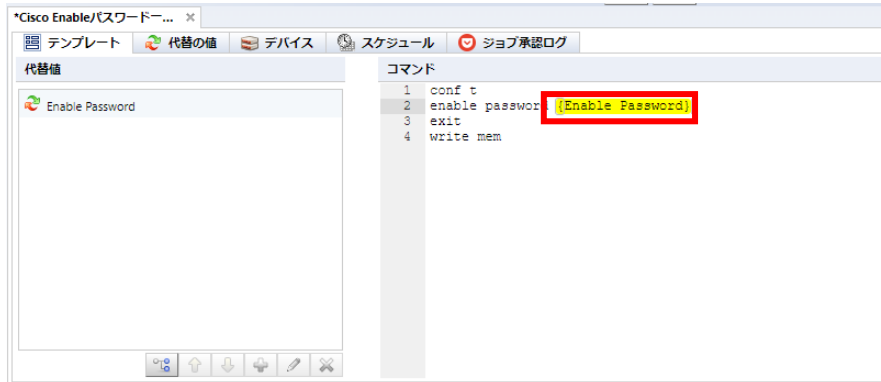
名前:

タイプ: テキスト

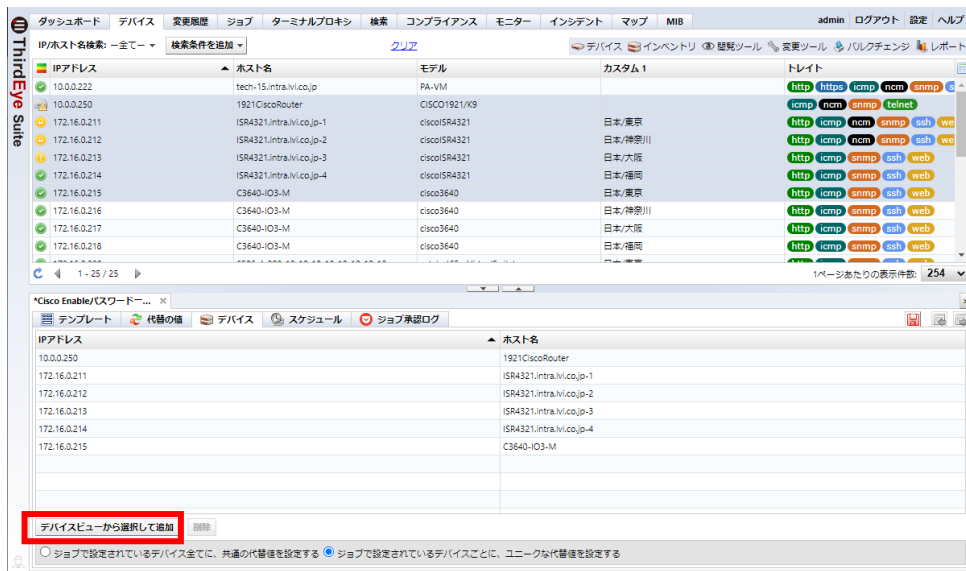
選択した値をデフォルトとして使用する

タイプ	説明
テキスト	任意のテキスト
IP アドレス	IP アドレス。正しい IPv4 あるいは IPv6 フォーマット以外の値が入力された時には、エラーが通知されます。
ホスト名	ホスト名
IP アドレスまたはホスト名	IP アドレスあるいはホスト名
選択	代替値入力の際に、ドロップダウンリストから選ぶようになります。予め設定した値しか入力されなくなるので安全です。
条件選択	有効か無効かを選ぶチェックボックスを設けます。無効と指定されたデバイスでは、その代替値は空白の文字列になります。

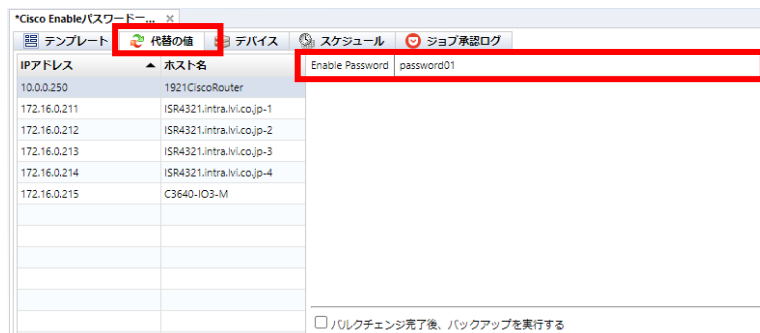
変数化された部分は黄色に表示されます。





6. デバイスタブで実行するデバイスを追加します。



7. 代替の値タブで、値を入力します。




代替データはエクセルファイルを用いてインポート/エクスポート出来ます。右上の  (エクスポート) あるいは  (インポート) を用いてください。

8. スケジュールタブでトリガーを追加します。

詳しくは、「6.10 ジョブ管理 **Enterprise** **Suite**」を参照してください。



9.  ボタンを押してジョブを保存します。



7.11 ユーザを登録する

ThirdEye にログインするユーザを作成します。ユーザに権限を割り当てることで、ユーザが実行できる操作を制限することができます。ThirdEye では、複数の権限を組み合わせることで、細かく指定することができます。

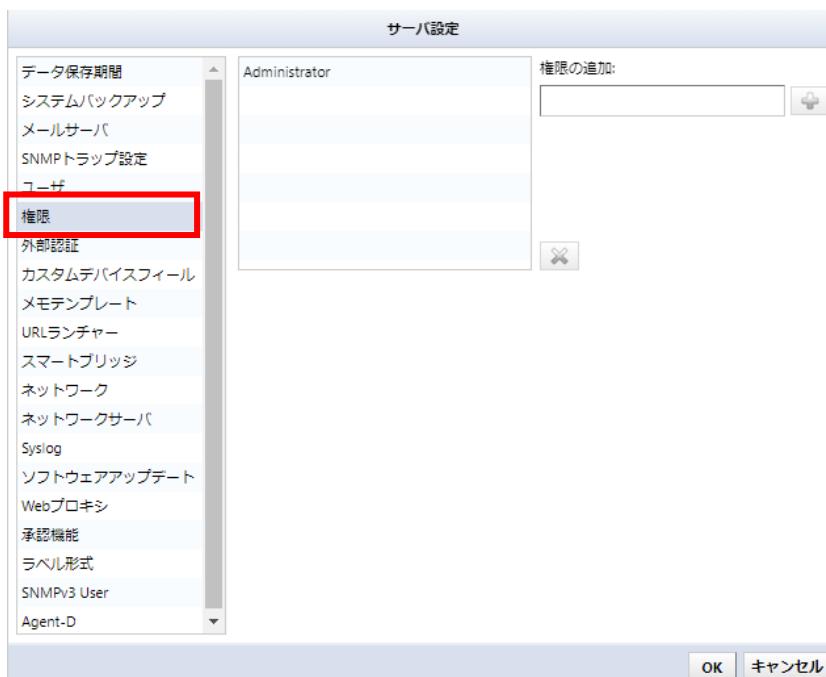
ユーザと権限の設定は、グローバルメニューの[設定]から設定することができます。



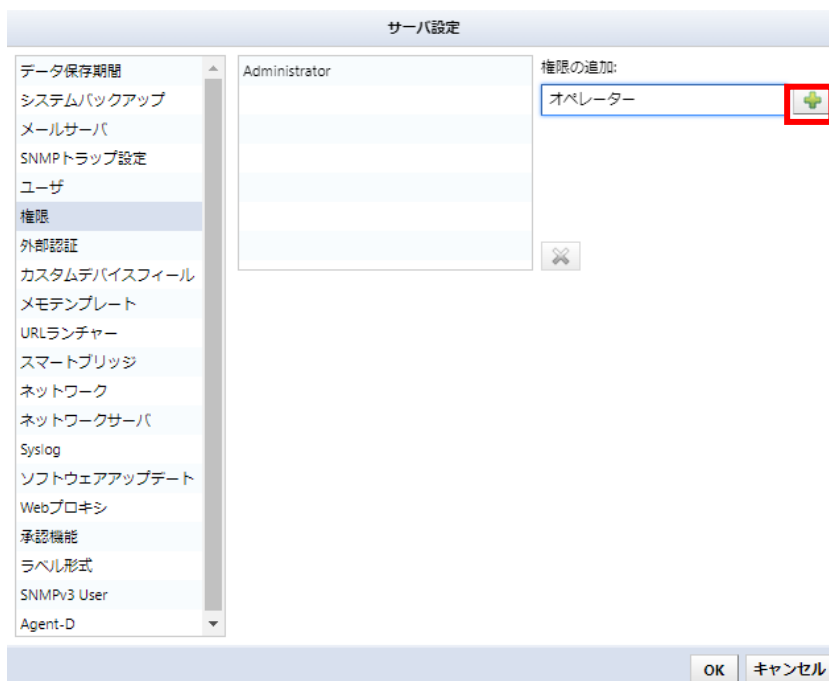
7.11.1 権限を追加する

※すべての実行権限も持つ「Administrator」が登録されています。「Administrator」権限を削除することはできません。

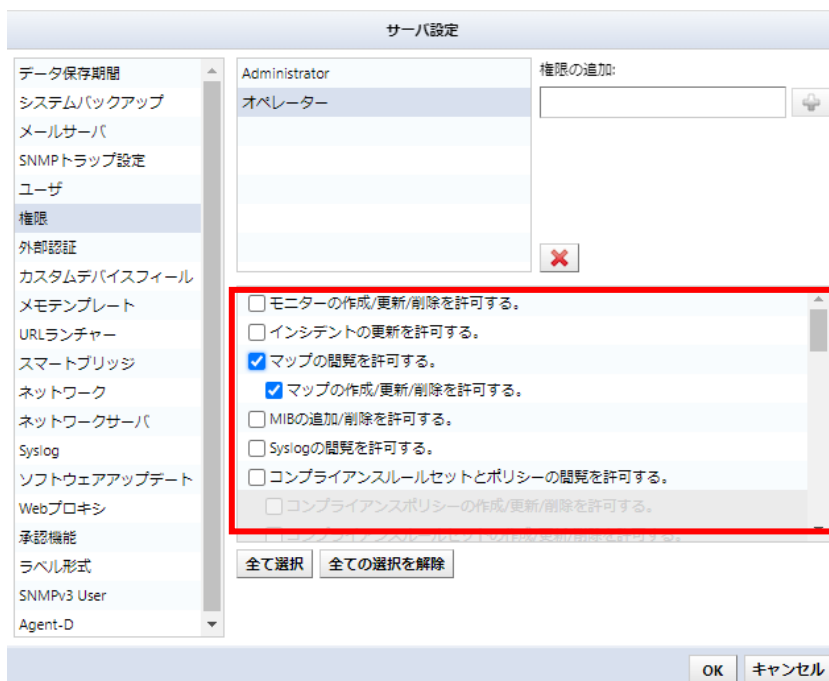
1. [権限]をクリックします。



2. [権限の追加]欄に権限名を入力し、[+] (追加) をクリックします。



3. 権限名が一覧に追加され、選択された状態に変化します。画面右下の権限項目から、必要な項目にチェックを付けます。



【権限項目一覧】

権限項目		説明
モニターの作成/更新/削除を許可する。	共通	モニターの作成/更新/削除ができます。
インシデントの更新を許可する。	共通	インシデントを更新できます。
マップの閲覧を許可する。	共通	マップを閲覧できます。
マップの作成/更新/削除を許可する。	共通	マップの作成/更新/削除ができます。 (※「マップの閲覧を許可する。」に付随する権限)
MIB の追加/削除を許可する。	共通	MIB の追加/削除ができます。
Syslog の閲覧を許可する。	Enterprise Suite	デバイスから送信される Syslog を閲覧できます。
コンプライアンスルールセットとポリシーの閲覧を許可する。	Suite	コンプライアンスタブを閲覧できます。
コンプライアンスポリシーの作成/更新/削除を許可する。	Suite	コンプライアンスポリシーの作成/更新/削除ができます。 (※「コンプライアンスルールセットとポリシーの閲覧を許可する。」に付随する権限)
コンプライアンスルールセットの作成/更新/削除を許可する。	Suite	コンプライアンスルールの作成/更新/削除ができます。 (※「コンプライアンスルールセットとポリシーの閲覧を許可する。」に付随する権限)
コンフィギュレーションの閲覧を許可する。	Enterprise Suite	デバイスから取得したコンフィグを閲覧できます。
クレデンシャル及びプロトコル設定を許可する。	共通	クレデンシャルとプロトコルを設定できます。
インベントリ内デバイス情報の作成/更新/削除を許可する。	共通	インベントリ内デバイス情報の作成/更新/削除ができます。
カスタムフィールド名の設定を許可する。	共通	カスタムデバイスフィールドの名前を変更できます。
インベントリ内デバイスへのタグ適用、解除を許可する。	共通	インベントリ内デバイスへのタグ適用、解除ができます。
ドラフトコンフィギュレーションの閲覧を許可する。	Suite	ドラフトコンフィギュレーションを閲覧できます。
ドラフトコンフィギュレーションの作成/更新/削除を許可する。	Suite	ドラフトコンフィギュレーションの作成/更新/削除ができます。 (※「ドラフトコンフィギュレーションの閲覧を許可する。」に付随する権限)
スケジュールのフィルタ設定を許可する。	Enterprise Suite	スケジュールのフィルタ設定ができます。
バックアップジョブの実行を許可する。	Enterprise Suite	バックアップジョブを実行できます。
バックアップジョブの作成/更新/削除を許可する。	Enterprise Suite	バックアップジョブの作成/更新/削除ができます。 (※「バックアップジョブの実行を許可する。」に付随する権限)
ディスカバリの実行を許可する。	共通	ディスカバリを実行できます。
ディスカバリジョブの作成/更新/削除を許可する。	Enterprise Suite	ディスカバリジョブの作成/更新/削除ができます。 (※「ディスカバリの実行を許可する。」に付随する権限)
ツールの実行を許可する。	Enterprise Suite	ツールを実行できます。
ツールの作成/更新/削除を許可する。	Enterprise Suite	ツールの作成/更新/削除ができます。 (※「ツールの実行を許可する。」に付随する権限)

権限項目		説明
ツールの実行を承認する権限。	Enterprise Suite	承認が必要なジョブに対して、承認を行うことができます。 (※「ツールの実行を許可する。」に付随する権限)
承認なしにツールを実行する権限。	Enterprise Suite	承認を必要としないジョブを作成でき、実行することができます。 (※「ツールの実行を許可する。」に付随する権限)
バルクチェンジジョブの実行を許可する。	Suite	バルクチェンジジョブを実行することができます。 (※「ツールの実行を許可する。」に付随する権限)
バルクチェンジジョブの作成/更新/削除を許可する。	Suite	バルクチェンジジョブの作成/更新/削除ができます (※「バルクチェンジジョブの実行を許可する。」に付随する権限)
デバイスコンフィギュレーション変更ツールの実行を許可する。	Suite	変更ツールを実行することができます。 (※「ツールの実行を許可する。」に付随する権限)
レポートの実行を許可する。	Enterprise Suite	レポートを実行できます。
レポートの作成/更新/削除を許可する。	Enterprise Suite	レポートの作成/更新/削除ができます。 (※「レポートの実行を許可する。」に付随する権限)
コンフィギュレーション復元ジョブの実行を許可する。	Enterprise Suite	コンフィギュレーション復元ジョブを実行できます。
Agent-D インストーラの実行を許可する。	Enterprise Suite	Agent-D インストーラを実行できます。
ネイバー情報収集ジョブの実行を許可する。	Enterprise Suite	ネイバー情報収集ジョブを実行できます。
ネイバー情報収集ジョブの作成/更新/削除を許可する。	Enterprise Suite	ネイバー情報収集ジョブの作成/更新/削除ができます。 (※「ネイバー情報収集ジョブの実行を許可する。」に付随する権限)
URL ランチャーの作成/更新/削除を許可する。	共通	URL ランチャーの作成/更新/削除ができます。
メモの作成/更新/削除を許可する。	共通	メモの作成/更新/削除ができます。
管理ネットワークの作成/更新/削除を許可する。	Enterprise Suite	管理ネットワークの作成/更新/削除ができます。
セキュリティの設定を許可する。	共通	セキュリティの設定ができます。
インベントリタグの作成/更新/削除を許可する。	共通	インベントリタグの作成/更新/削除ができます。
ターミナルサーバ プロキシ経由でのログインを許可する。	共通	ターミナルサーバ プロキシ経由でのログインができます。
ターミナルサーバ プロキシ経由での自動ログインを許可する。	Enterprise Suite	ターミナルサーバ プロキシ経由での自動ログインができます。 (※「ターミナルサーバ プロキシ経由でのログインを許可する。」に付随する権限)
enable mode に直接自動ログインを許可する。	Enterprise Suite	enable mode に直接自動ログインができます。 (※「ターミナルサーバ プロキシ経由での自動ログインを許可する。」に付随する権限)
他のユーザのターミナルアクセスログ閲覧を許可する。	Enterprise Suite	他のユーザのターミナルアクセスログを閲覧できます。
ターミナルアクセスログ閲覧の削除を許可する。	Enterprise Suite	ターミナルアクセスログの削除ができます。 (※「他のユーザのターミナルアクセスログ閲覧を許可する。」に付随する権限)

4. [OK]をクリックします。

サーバ設定

権限の追加:

権限


モニターの作成/更新/削除を許可する。
 インシデントの更新を許可する。
 マップの閲覧を許可する。
 マップの作成/更新/削除を許可する。
 MIBの追加/削除を許可する。
 Syslogの閲覧を許可する。
 コンプライアンスルールセットとポリシーの閲覧を許可する。
 コンプライアンスポリシーの作成/更新/削除を許可する。
 コンプライアンスルールセットの作成/更新/削除を許可する。

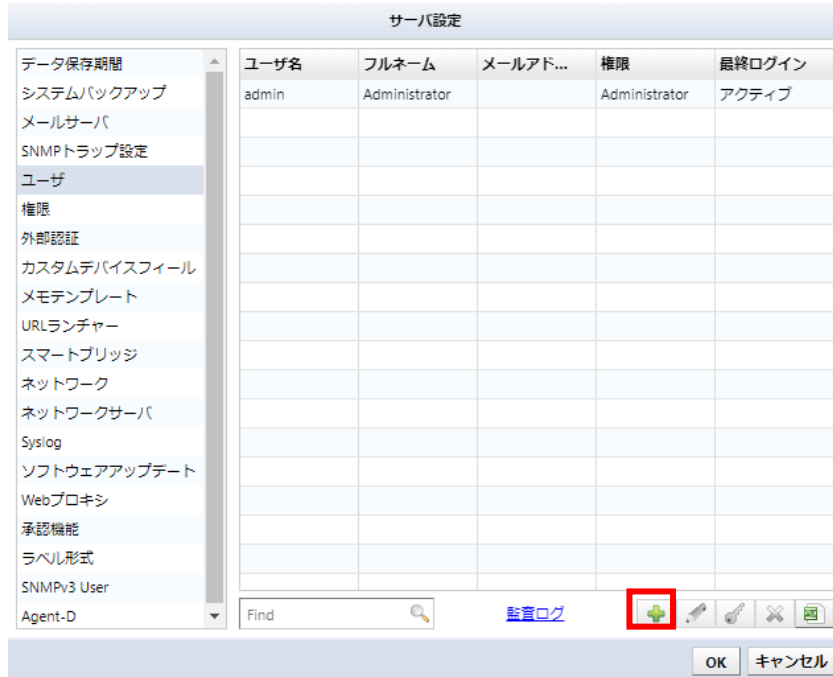
全て選択 全ての選択を解除

OK キャンセル

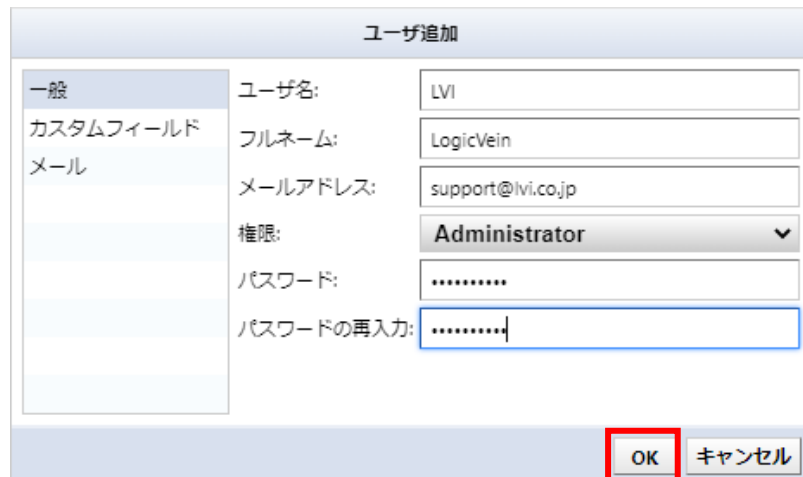
7.11.2 ユーザを追加する

※「admin」ユーザがあらかじめ登録されています。「admin」ユーザは、削除することができません。

1. [ (追加)]をクリックします。

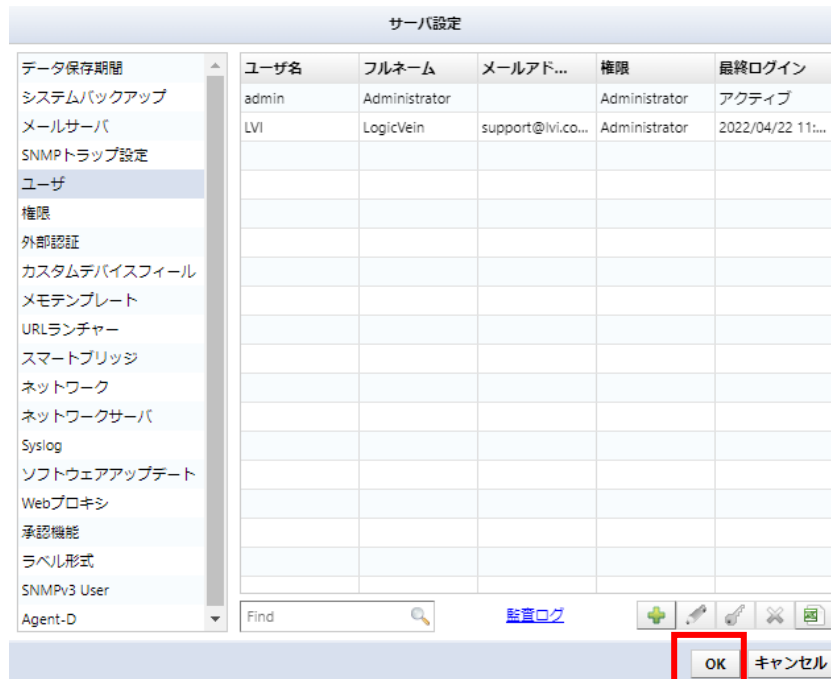


2. ユーザ追加画面が表示されます。項目を入力し、[OK]をクリックします。



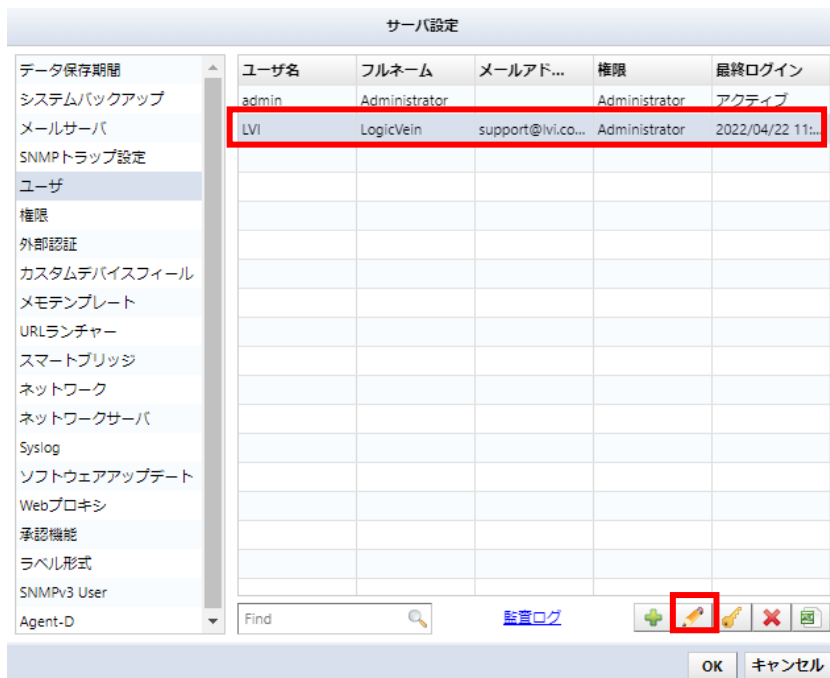
カテゴリ	項目	説明	必須
一般	ユーザ名	ユーザ名を入力します。	必須
	フルネーム	ユーザのフルネームを入力します。	—
	メールアドレス	ユーザのメールアドレスを入力します。	—
	権限	ユーザの権限を選択します。「7.11.1 権限を追加する」で設定した権限をプルダウンメニューから選択できます。	必須
	パスワード	ユーザのパスワードを設定します。 ※パスワードを設定するには、以下の条件を満たしている必要があります。 <ul style="list-style-type: none"> 8文字以上であること 推測されやすい文字列(人名や固有名詞、辞書に載っている単語、よく使われるパスワード)でないこと 同じ文字の繰り返しやわかりやすい並びの文字列でないこと 	必須
カスタムフィールド	カスタム 1~5	ユーザが閲覧可能なカスタムデバイスフィールドを選択します。 ※表示される項目名は、「7.15 カスタムデバイスフィールドのカラム名を変更する」の設定に基づき変化します。	—
メール	インシデントメール	インシデントメールを曜日/時間によって制限する場合に、設定します。	—

3. [OK]をクリックします。



7.11.3 ユーザ情報を変更する

1. 編集したいユーザを選択し、[ (編集)] をクリックします。




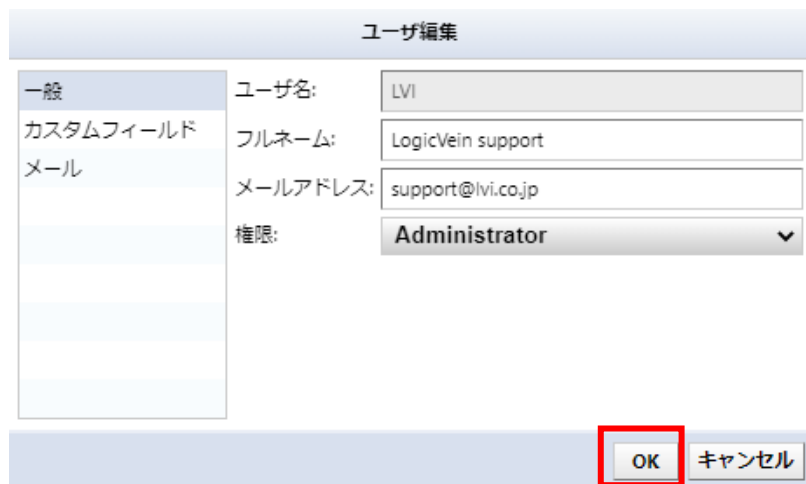
ユーザ名	フルネーム	メールアドレス...	権限	最終ログイン
admin	Administrator		Administrator	アクティブ
LVI	LogicVein	support@lvi.co...	Administrator	2022/04/22 11:...

Buttons: OK, キャンセル

2. ユーザ編集画面が表示されます。編集後、[OK]をクリックします。

※ユーザ名は変更できません。

※パスワードを変更したい場合は、[ (鍵)] から設定します。



一般	ユーザ名:	LVI
カスタムフィールド	フルネーム:	LogicVein support
メール	メールアドレス:	support@lvi.co.jp
	権限:	Administrator

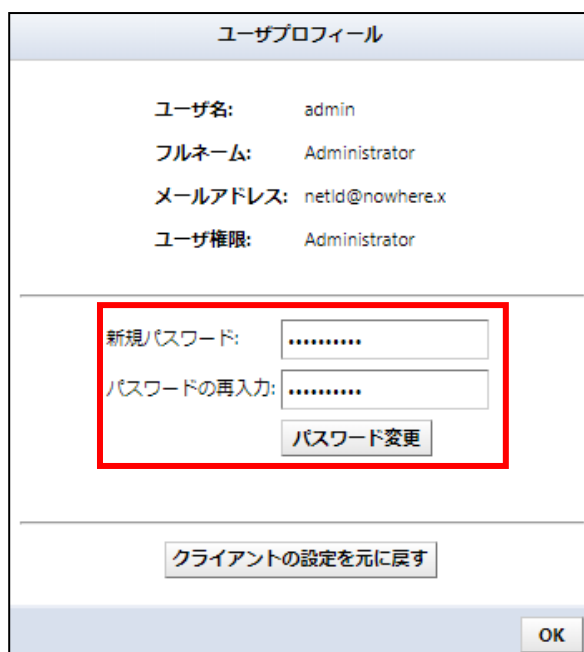
Buttons: OK, キャンセル

7.11.4 ログイン中のユーザのパスワードを変更する

グローバルメニューにあるログインユーザ名からパスワードを変更することができます。ここでは、ユーザ名「admin」のパスワードを変更しています。



新しいパスワードを[新規パスワード]と[パスワードの再入力]に入力します。[パスワード変更]ボタンを押すと、新しいパスワードが登録されます。新規パスワードと再入力された文字列が異なる場合、[パスワード変更]ボタンが有効になりません。

A screenshot of a web interface showing a user profile. The profile information is displayed in a table: 'ユーザ名: admin', 'フルネーム: Administrator', 'メールアドレス: netid@nowhere.x', and 'ユーザ権限: Administrator'. Below the profile information, there is a form for changing the password. The form has two input fields: '新規パスワード:' and 'パスワードの再入力:', both containing masked characters. A red box highlights these two input fields and the 'パスワード変更' button below them. At the bottom of the form, there is a button labeled 'クライアントの設定を元に戻す' and an 'OK' button.

注意

パスワードを設定するには、以下の条件を満たしている必要があります。

- 8文字以上であること
- 推測されやすい文字列(人名や固有名詞、辞書に載っている単語、よく使われるパスワード)でないこと
- 同じ文字の繰り返しやわかりやすい並びの文字列でないこと

7.11.5 Active Directory または RADIUS サーバと連携する

外部認証では、ユーザ情報を管理している認証サーバと連携し、ThirdEye ログインすることができます。これにより、ThirdEye に前もってすべてのユーザを登録する必要がなくなり、導入時の作業や、組織変更時の作業を軽減できます。

外部認証の設定は、グローバルメニューの[設定]→[外部認証]から設定することができます。

(1) RADIUS 連携

RADIUS サーバに **Access-Request** を送信して認証を行います。RADIUS サーバと連携する為には **Access-Accept** に **Filter-Id** をつけて送信するように設定する必要があります。

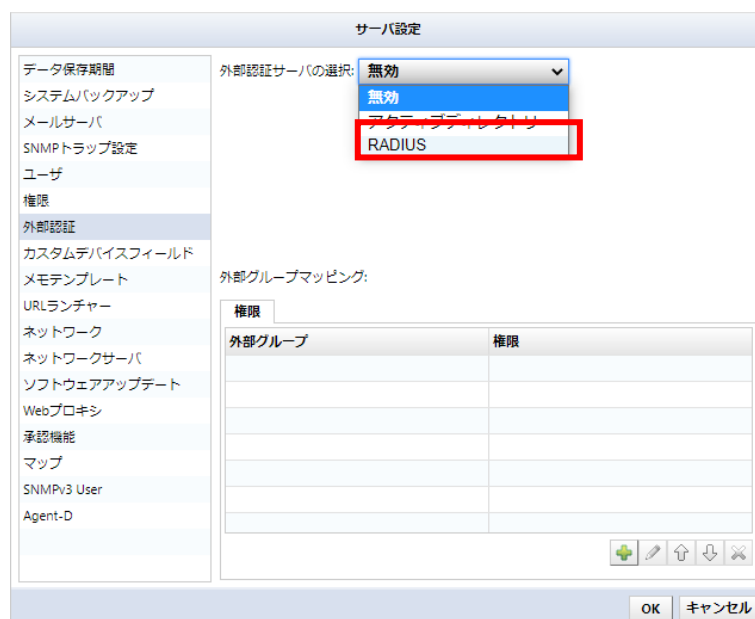
メモ:

以下は FreeRADIUS のユーザ設定のサンプルです。

```
LogicVein  Cleartext-Password := "password"  
Filter-Id += "GROUP"
```

この設定では、「ユーザ名:LogicVein、パスワード:password」の **Access-Request** を受信した場合 **Filter-Id** をセットして **Access-Accept** を送信します。Filter-Id は認証されたユーザが所属するグループとして使用さ

1. [外部認証サーバの選択]を「RADIUS」に変更します。



2. RADIUS サーバの IP アドレス(またはホスト名)と共有シークレットを設定します。

サーバ設定

外部認証サーバの選択: RADIUS

ホスト名: 10.0.0.95 ポート: 1812

共有シークレット: テスト

文字コード: UTF-8

外部グループマッピング:

外部グループ	権限

OK キャンセル

3. 外部グループマッピングの権限を設定します。[+] (追加) から新規追加します。

外部認証

外部グループマッピング:

外部グループ	権限

OK キャンセル

4. RADIUS サーバの Filter-Id に設定されているグループを[外部グループ]に入力し、割り当てる[権限]を選択します。

外部グループマッピング

外部グループ: GROUP

権限: Administrator

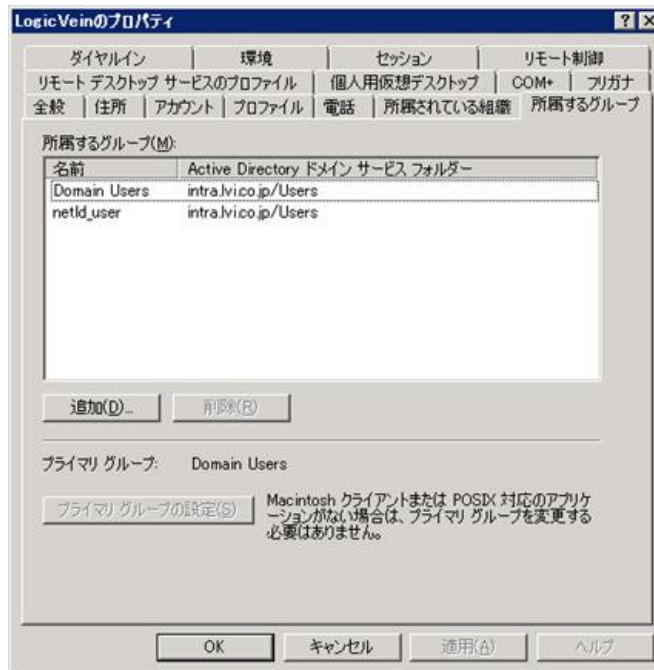
OK キャンセル

以上で RADIUS の設定は完了です。

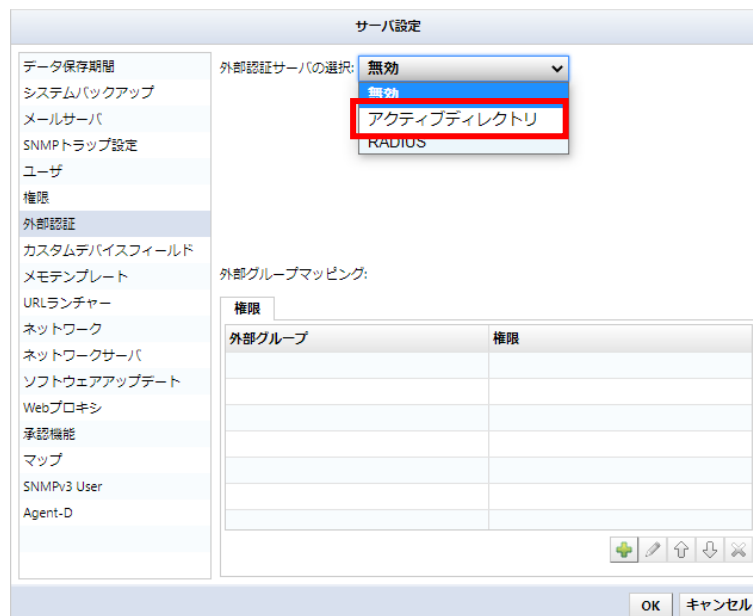
[OK]をクリックして設定を保存し、RADIUS サーバに設定されたユーザでログインします。

(2) Active Directory 連携

Active Directory サーバとの連携では登録されているユーザの所属するグループを使用して権限とネットワークを決定します。



1. [外部認証サーバの選択]を「アクティブディレクトリ」に変更します。



2. ドメイン名と Active Directory サーバの IP アドレス(またはホスト名)を設定します。

サーバ設定

外部認証サーバの選択: アクティブディレクトリ

ドメイン: logicvein.com


IPアドレスまたはホスト名: 192.168.0.3 ポート: 389 テスト

LDAPSを有効にする

タイムアウト(秒): 10

外部グループ	権限

OK キャンセル

3. 外部グループマッピングの権限を設定します  (追加)から新規追加します。

外部認証

外部グループマッピング:

外部グループ	権限

OK キャンセル

4. ユーザが所属するグループを[外部グループ]に入力し、割り当てる[権限]を選択します。

外部グループマッピング

外部グループ: netid_user

権限: Administrator

OK キャンセル

以上でアクティブディレクトリの設定は完了です。

[OK]をクリックして設定を保存し、Active Directory サーバに設定されたユーザでログインします。

(3) 外部認証のテスト

外部認証の設定後、[テスト]から外部認証のテストを行うことができます。

外部グループ	権限
GROUP	Administrator

[認証テスト]ダイアログが表示されたら、認証をテストする[ユーザ名]と[パスワード]を入力し、[テスト]をクリックします。認証に成功すると、下図のように「認証が成功しました」というメッセージが表示されます。

ユーザ名 : LogicVein
パスワード : *****
認証が成功しました

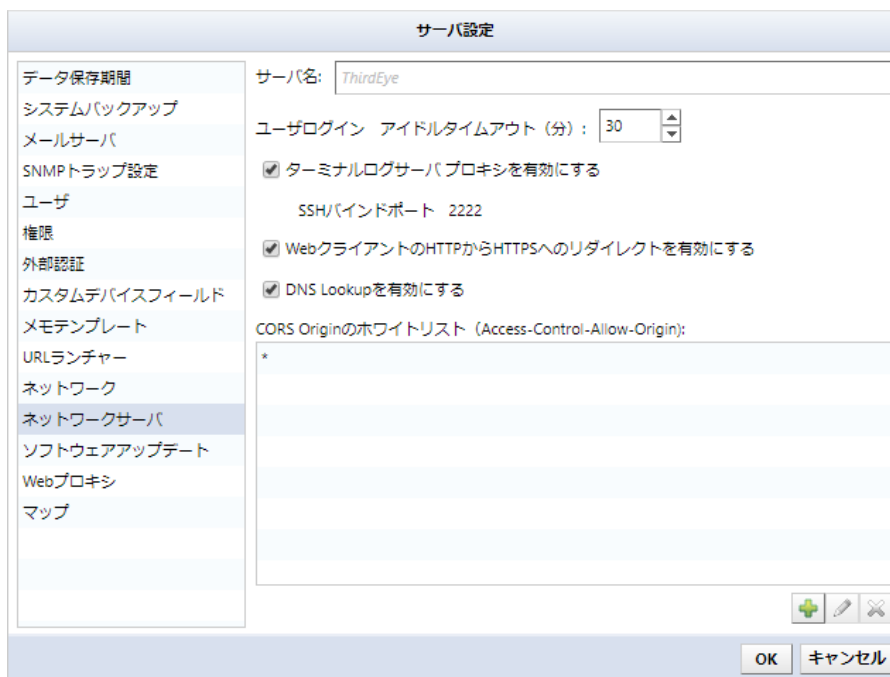
7.11.6 ユーザのセッションタイムアウトを設定する

ThirdEye では、30 分間操作を行わなかったユーザは再度認証が必要になります。この時間を変更するには、以下の手順で設定します。

1. グローバルメニューの[設定]をクリックします。




2. [ネットワークサーバ]をクリックし、「ユーザログイン アイドルタイムアウト」の時間を変更します。※設定可能な範囲: 10~525600(分)

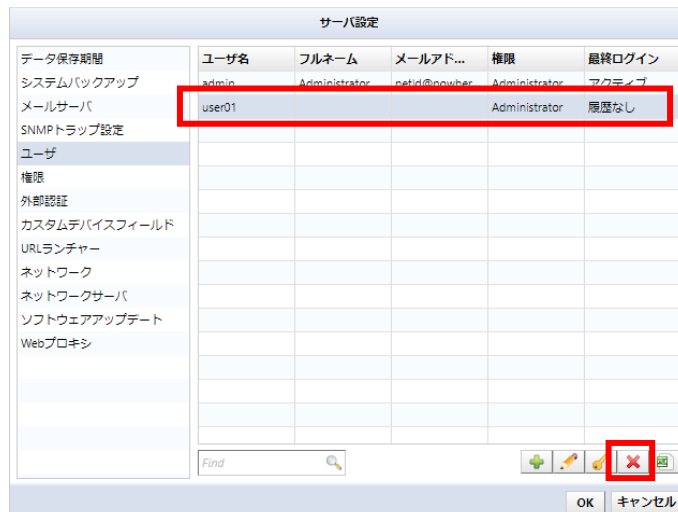


3. [OK]をクリックします。
4. ログアウトして、再度ログインします。

※設定内容を反映するには、ThirdEye からログアウトして、再度ログインする必要があります。

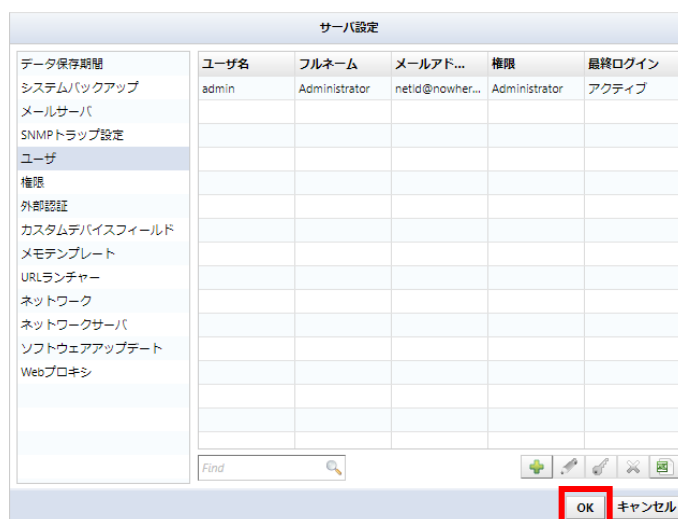
7.11.7 ユーザを削除する

1. 削除したいユーザを選択し、[ (削除)]をクリックします。




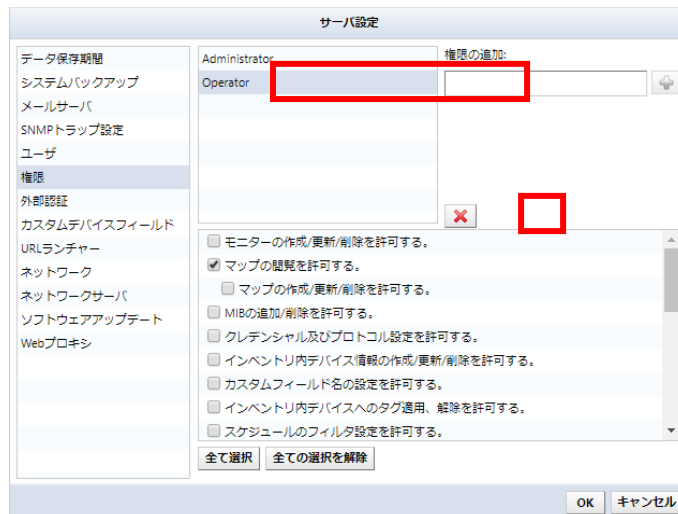
2. ユーザが削除されます。サーバ設定で[OK]をクリックします。

※誤ってユーザを削除した場合は、[キャンセル]をクリックしてください。



7.11.8 権限を削除する

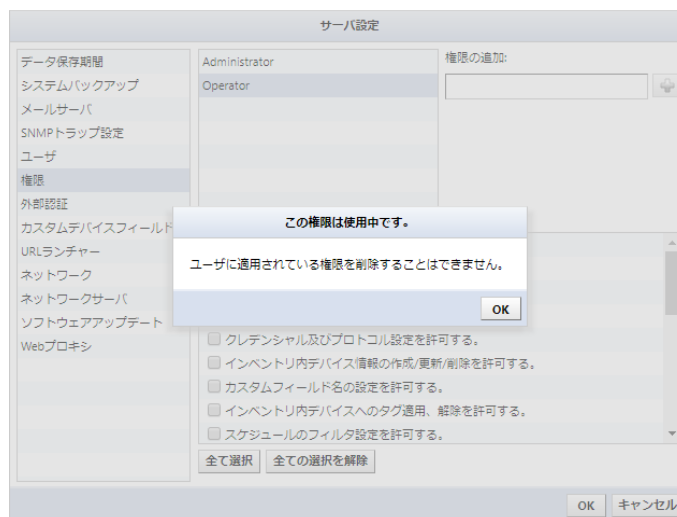
1. 削除したい権限名を選択し、[ (削除)]をクリックします。



2. サーバ設定で[OK]をクリックします。

使用中の権限を削除しようとする、以下のエラーが発生します。

注意



使用されているユーザの権限を割り当て直すなどしてから、削除を実行してください。

7.12 データ保存期間を変更する

データ保存期間では、データの保存期間と自動削除のタイミングを設定します。

項目		説明
週単位で、次の時間にデータを削除する	共通	一定期間経過したデータを、毎週指定された曜日と時間帯に自動的に削除します。(初期値: 月曜日, 6:00) データ保存期間は、以降の項目で指定します。(※ただし、「期限なし」を指定した場合、データは削除されません)
ジョブ履歴の保存期間	Enterprise Suite	[ジョブ]→[ジョブ履歴]タブのデータの保存期間を次の中から指定します。(初期値: 3ヶ月) 「期限なし」、「3ヶ月」、「6ヶ月」、「9ヶ月」、「1年」
コンフィギュレーション履歴の保存期間	Enterprise Suite	各監視対象デバイスのコンフィギュレーションの保存期間を次の中から指定します。(初期値: 期限なし) 「期限なし」、「6ヶ月」、「1年」、「2年」、「3年」、「4年」、「5年」、「6年」、「7年」
ターミナルログ履歴の保存期間	Enterprise Suite	[ターミナルプロキシ]タブのデータの保存期間を次の中から指定します。(初期値: 3ヶ月) 「期限なし」、「3ヶ月」、「6ヶ月」、「9ヶ月」、「1年」、「3年」
SNMPトラップの保存期間	共通	[モニター]→[SNMPトラップ]タブのデータの保存期間を次の中から指定します。(初期値: 期限なし) 「期限なし」、「2週間」、「3ヶ月」、「6ヶ月」、「1年」
違反の保存期間	共通	[モニター]→[違反]タブのデータの保存期間を次の中から指定します。(初期値: 期限なし) 「期限なし」、「2週間」、「3ヶ月」、「6ヶ月」、「1年」

7.13 メールサーバを設定する

メールサーバでは、ThirdEye からメール通知するための SMTP サーバの情報を入力します。障害時にメール送信する場合やダッシュボードレポートを送信する場合には、予め設定する必要があります。

1. グローバルメニューの[設定]をクリックします。



2. [メールサーバ]をクリックし、SMTP サーバの情報を入力します。

項目	説明
ホスト名/IP アドレス	メールサーバのホスト名または IP アドレスを指定します。(初期値: mail)
差出人メールアドレス	メールの送信元(差出人)として表示されるメールアドレスを指定します。(初期値: ThirdEye)
差出人名	メールの送信者名(差出人)として表示される名前を指定します。(初期値: ThirdEye)
サーバ認証あり	メールサーバの認証を設定します。SMTP 認証が必要な場合は、チェックを入れて以下の項目を設定します。(初期値: 無効) メールサーバのユーザ名 … 認証 ID メールサーバのパスワード … 認証パスワード
SMTPS を有効にする	TLS を有効にします。
デフォルトのメール言語	メールの表示言語を設定します。(初期値: 日本語)
デフォルトのメールタイムゾーン	メールのタイムゾーンを設定します。(初期値: (GMT+09:00) 東京)

3. [OK]をクリックします。

サーバ設定

データ保存期間	ホスト名/IPアドレス:	<input type="text" value="mail"/>
システムバックアップ	差出人メールアドレス:	<input type="text" value="netLD"/>
メールサーバ	差出人名:	<input type="text" value="netLD"/>
SNMPトラップ設定	<input type="checkbox"/> サーバ(認証あり)	
ユーザ	<input type="checkbox"/> SMTPSを有効にする	
権限	メールサーバのユーザ名:	<input type="text"/>
外部認証	メールサーバのパスワード:	<input type="password"/>
カスタムデバイスファイル	デフォルトのメール言語	<input checked="" type="radio"/>
メモテンプレート	デフォルトのメールタイムゾーン	(GMT+09:00) 東京
URLランチャー		
スマートブリッジ		
ネットワーク		
ネットワークサーバ		
Syslog		
ソフトウェアアップデート		
Webプロキシ		
承認機能		
ラベル形式		
SNMPv3 User		
Agent-D		

テスト

OK キャンセル


7.14 SNMPトラップ送信を設定する Enterprise Suite

SNMPトラップ設定では、ThirdEye から SNMPトラップを送信するための設定を構成します。トラップを送信する条件やトラップ送信先を設定します。

1. グローバルメニューの[設定]をクリックします。
2. [SNMPトラップ設定]をクリックし、送信対象のイベントにチェックを挿入します。

項目		説明
デバイスのコンフィギュレーション変更検知	Enterprise Suite	前回のバックアップからデバイスのコンフィグが変更されたことを検知した場合、SNMPトラップを送信します。
デバイスの追加と削除	Enterprise Suite	デバイスが追加/削除された場合、SNMPトラップを送信します。
バックアップ失敗	Enterprise Suite	コンフィグバックアップに失敗した場合、SNMPトラップを送信します。
ジョブ失敗	Enterprise Suite	ジョブ実行に失敗した場合、SNMPトラップを送信します。
デバイスのコンプライアンス・ステータス変更検知	Suite	コンプライアンスステータスが変更された場合に、SNMPトラップを送信します。
スマートブリッジの接続状態変更検知	Enterprise Suite	スマートブリッジとコアサーバ間の接続状態が変化した場合、SNMPトラップを送信します。 (※オプションライセンスが有効な場合にのみ表示されます)
監査ログ	Enterprise Suite	ユーザがログイン/ログアウトした場合、SNMPトラップを送信します。

項目		説明
承認イベント発生	Enterprise Suite	ジョブ承認イベントが発生した場合に、SNMPトラップを送信します。
メール送信失敗	Enterprise Suite	メール送信に失敗した場合、SNMPトラップを送信します。
受信したすべてのトラップを転送する	Enterprise Suite	ThirdEye が受信したすべてのトラップを転送します。

3. [ (追加)] をクリックします。
4. トラップ送信先の情報を入力し、[OK] をクリックします。

SNMPトラップホスト

ホスト:

ポート:

バージョン:

SNMPコミュニティストリング:

SNMPトラップホスト

ホスト:

ポート:

バージョン:

SNMPv3 Authentication Username:

SNMPv3 Authentication Password:

SNMPv3 Privacy Password:

SNMPv3 Authentication Protocol:

SNMPv3 Private Protocol:

SNMPv3 EngineID:

項目	説明
ホスト	トラップ送信先の IP アドレスまたはホスト名を入力します。
ポート	トラップ送信先ポートを指定します。(初期値: 162)
バージョン	トラップのバージョンを次の中から指定します。 「1」、「2c」、「3」
SNMP コミュニティストリング	トラップコミュニティ名を入力します。
SNMPv3 Authentication Username	ユーザ認証に使用するユーザ名を入力します。
SNMPv3 Authentication Password	Authentication Username に入力したユーザのパスワードを入力します。
SNMPv3 Privacy Password	暗号化パスワードを入力します。
SNMPv3 Authentication Protocol	認証プロトコルを次の中から指定します。 「SHA」、「SHA224」、「SHA256」、「SHA384」、「SHA512」
SNMPv3 Private Protocol	暗号化プロトコルを次の中から指定します。 「PrivDES」、「PrivAES128」、「PrivAES192」、「PrivAES256」、「Priv3DES」、「PrivAES256-3DES」、「PrivAES192-3DES」
SNMPv3 EngineID	エンジン ID を変更する場合は入力します。(自動で入力されます)

7.15 カスタムデバイスフィールドのカラム名を変更する

カスタムデバイスフィールドでは、デバイスタブや検索で使用するカスタムカラムの名前を設定することができます。

1. グローバルメニューの[設定]をクリックします。
2. [カスタムデバイスフィールド]をクリックします。

設定項目	説明	
データ保存期間	インベントリにある5つのカスタムフィールドで、デバイスに任意の値を付加できます。カスタムフィールドの項目名は、ここで設定してください。	
システムバックアップ		
メールサーバ		カスタム 1: <input type="text"/>
SNMPトラップ設定		カスタム 2: <input type="text"/>
ユーザ		カスタム 3: <input type="text"/>
権限	カスタム 4: <input type="text"/>	
外部認証	カスタム 5: <input type="text"/>	
カスタムデバイスフィールド		
メモテンプレート		
URLランチャー		
ネットワーク		
ネットワークサーバ		
ソフトウェアアップデート		
Webプロキシ		
マップ		

3. 入力欄に任意の表示名を設定し、[OK]をクリックします。

※リビジョン 20220819.0053 から、カスタムデバイスフィールドの追加に対応しました。[追加]ボタンをクリックすることでカスタムデバイスフィールドを追加することができます。

※カスタムデバイスフィールドは、一度追加すると削除できません。

設定項目	説明	
データ保存期間	カスタムフィールドでデバイスに任意の値を付加できます。カスタムフィールドの項目名は、ここで設定してください。	
システムバックアップ		
メールサーバ		カスタム 1: a
SNMPトラップ設定		カスタム 2: b
ユーザ		カスタム 3: c
権限	カスタム 4: カスタム 4	
外部認証	カスタム 5: カスタム 5	
カスタムデバイスフィールド		
メモテンプレート		
URLランチャー		
スマートブリッジ		
ネットワーク		
ネットワークサーバ		
Syslog		
Zero-Touch配布		
ソフトウェアアップデート		
Webプロキシ		
承認機能		
Cisco API		
ラベル形式		

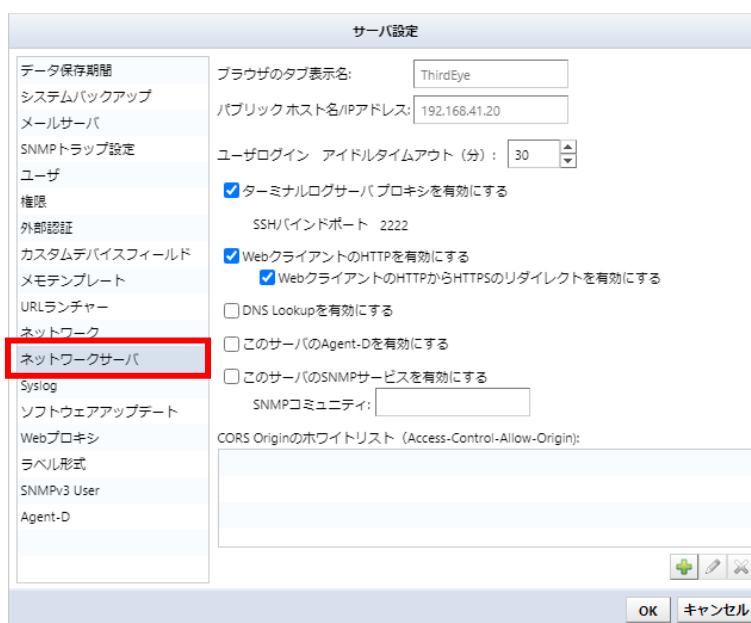
7.16 ホスト名に sysName を使用する

ThirdEye は、DNS サーバからホスト名を取得し、それをデバイスタブに表示します。機器に設定されているホスト名(sysName)を使用するには、以下の設定をします。

1. グローバルメニューの[設定]をクリックします。



2. [ネットワークサーバ]をクリックし、「DNS Lookup を有効にする」のチェックを外します。



3. [OK]をクリックします。

7.17 Syslog ファイルの詳細設定

7.17.1 Syslog ファイルの保存期間/サイズを設定する Enterprise Suite

Syslog ファイルの保存期間を設定します。

1. グローバルメニューの[設定]をクリックします。
2. [Syslog]をクリックし、各項目を設定します。

項目	説明
Syslog サーバを有効にする	Syslog サーバの有効(起動)/無効(停止)を設定します。
ログサイズ(MB)	Syslog ファイルのサイズを指定します。
ログ数	ローテーションされたファイルの保持数を指定します。
維持する日数	ローテーションされたファイルの保持日数を指定します。
時間間隔	Syslog ファイルを指定した時間間隔でローテートします。
Syslog の送信元 IP アドレスをホスト名に変換する(DNS の逆引き)	Syslog の送信元 IP アドレスに対して DNS の逆引きを行い、ホスト名で Syslog ファイルに記録します。

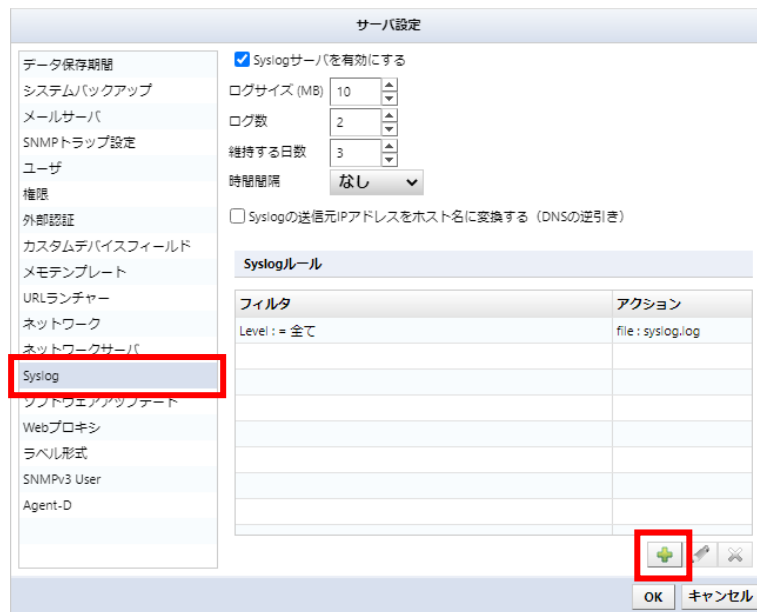
3. [OK]をクリックします。

7.17.2 Syslog ルールを設定する Enterprise Suite

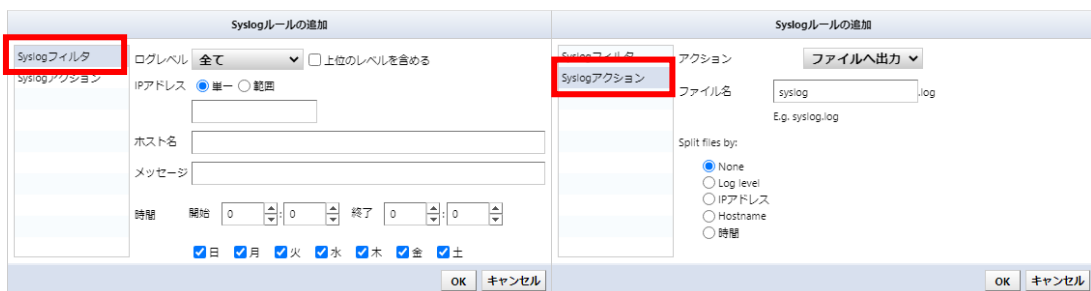
設定された条件に従って、Syslog の出力先を振り分けたり、他のホストに Syslog を転送したり、不要なメッセージを除外したりすることができます。

Syslog ルールを追加するには、次の操作を行います。

1. グローバルメニューの[設定]をクリックします。
2. [Syslog]をクリックし、Syslog ルールで[+] (追加)をクリックします。



3. [Syslog フィルタ]および[Syslog アクション]を設定します。



➤ Syslog フィルタ

項目	説明
ログレベル	Syslog のレベルでフィルタリングします。 [上位のレベルを含める]オプションを有効にすると、選択したレベル以上がフィルタリングの対象になります。
IP アドレス	IP アドレスでフィルタリングします。 [単一]は単一の IP アドレスで、[範囲]は IP 範囲でフィルタリングします。 未入力の場合は、IP アドレスによるフィルタリングを行いません。
ホスト名	ホスト名でフィルタリングします。 未入力の場合は、ホスト名によるフィルタリングを行いません。
メッセージ	指定された文字列を含む Syslog をフィルタリングします。 「メッセージ」欄では、部分一致によるフィルタリングが可能です。大文字/小文字は区別されます。正規表現 (Regex) に基づくフィルタリングには対応していません。 未入力の場合は、メッセージによるフィルタリングを行いません。
時間	時間でフィルタリングします。 開始時間と終了時間で指定された時間内に受信した Syslog がフィルタリングの対象となります。
曜日	曜日でフィルタリングします。

➤ Syslog アクション

アクション	項目	説明
ファイルへ出力	ファイル名	出力する Syslog ファイル名を指定します。
	Split files by	出力される Syslog ファイルを指定単位で分割します。 <ul style="list-style-type: none"> • None: 分割しない • Log Level: ログレベル単位で分割する • IP アドレス: IP アドレスまたはオクテット(第 1,2,3)単位で分割する • Hostname: ホスト名単位で分割する • 時間: 選択した時間単位で分割する
転送	転送形式	転送形式を Syslog と SNMP から選択します。
	転送先 IP アドレス /ホスト名	転送先を指定します。
	ポート	転送先のポート番号を設定します。
	プロトコル	転送プロトコルを UDP または TCP から選択します。 ※転送形式が Syslog の場合に表示
	IP スプーフィング	※転送形式が Syslog の場合に表示
	コミュニティ	SNMP トラップコミュニティを指定します。 ※転送形式が SNMP の場合に表示
破棄	—	Syslog フィルタで指定された Syslog を除外し、Syslog ファイルに記録しなくなります。

4. 設定後、[OK]をクリックします。

Syslogルール追加

Syslogフィルタ
Syslogアクション

アクション: ファイルへ出力

ファイル名: error.log
E.g. error.log

Split files by:
 None
 Log level
 IPアドレス
 Hostname
 時間

OK キャンセル

5. サーバ設定画面で[OK]をクリックします。

サーバ設定

Syslogサーバを有効にする

ログサイズ (MB): 10

ログ数: 2

維持する日数: 3

時間間隔: なし

Syslogの送信元IPアドレスをホスト名に変換する (DNSの逆引き)

Syslogルール

フィルタ	アクション
Level : = 全て	file : syslog.log
Level : = ERROR	file : error.log

OK キャンセル

7.17.3 Syslog ファイルを外部ストレージに保存する Enterprise Suite

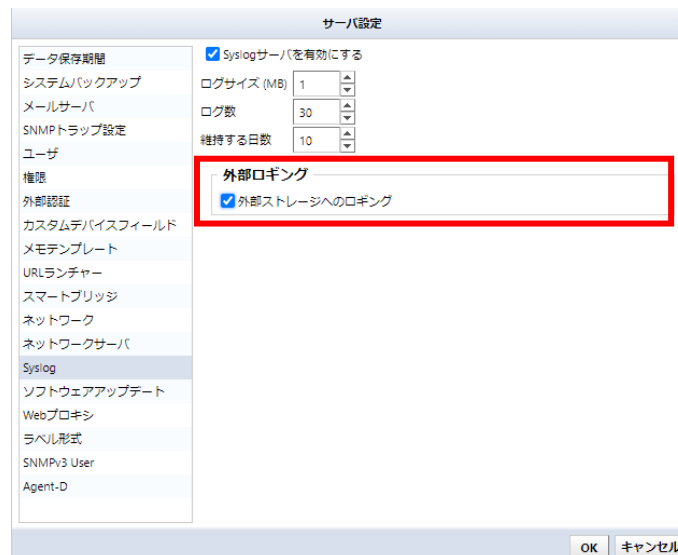
通常、受信した Syslog はローカルの syslog.log ファイルに保存されますが、NFS/SMB サーバと連携することで、外部ストレージに保存することができます。

- ※ 外部ストレージとの連携手順については、「[8.4 外部ストレージに保存する](#)」を参照してください。
- ※ この設定を反映させるには、ThirdEye アプライアンスを再起動する必要があります。再起動中は監視が停止します。

1. グローバルメニューの「設定」をクリックします。

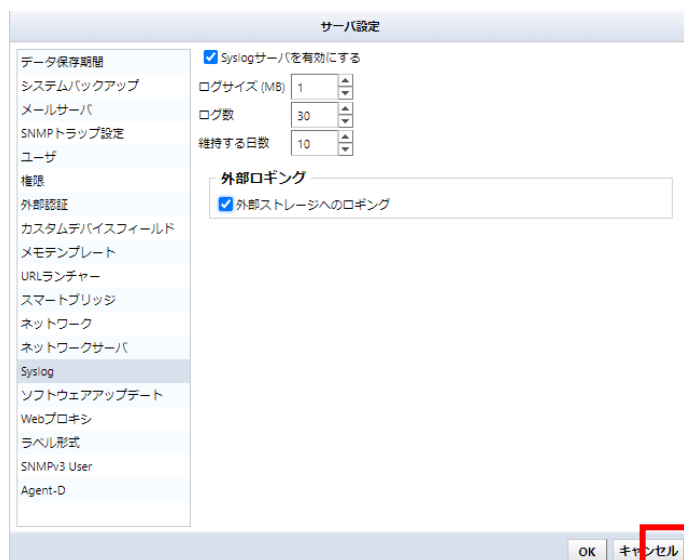


2. 「Syslog」をクリックし、「外部ストレージへのロギング」にチェックをいれます。



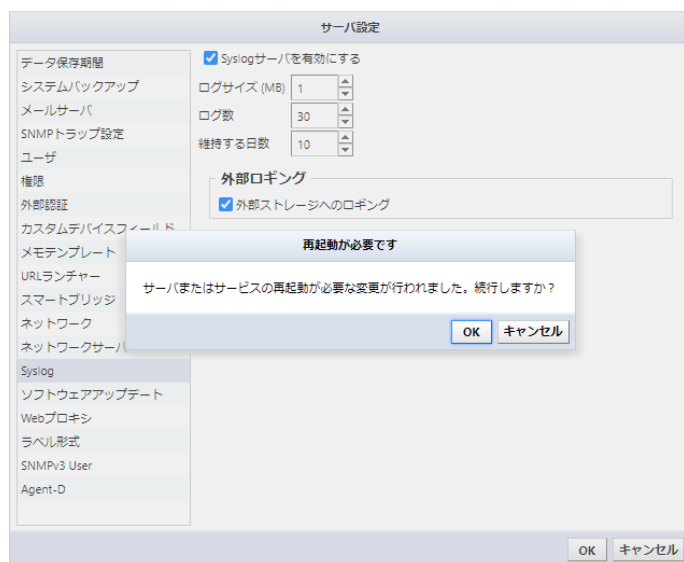
※この「外部ロギング」オプションは、NFS/SMB サーバと連携している場合にのみ表示されます。

3. [OK]をクリックします。



4. 再起動の確認画面で[OK]をクリックします。

※設定を反映させるには、ThirdEye を再起動する必要があります。[OK]をクリックすると、ThirdEye が自動的に再起動します。



補足

syslog.log ファイルの保存先をローカルから外部ストレージに変更すると、ローカルのファイルが外部ストレージにコピーされます。一方、syslog.log ファイルの保存先を外部ストレージからローカルに変更しても、外部ストレージ上のファイルはローカルにコピーされません。
これは、セキュリティ上の理由からサポートされていません。

7.18 メモテンプレートを編集する

メモテンプレートでは、インベントリの「メモ」カラムでデバイスメモを新規作成する時に、自動的に挿入される定型(テンプレート)を設定することができます。

1. グローバルメニューの[設定]をクリックします。



2. [メモテンプレート]をクリックします



項目	説明
フォントサイズ	フォントサイズを変更する。
太字	範囲指定された文字を太字に変更する。
斜字	斜字に変更する。
下線	下線を引く。
テキストの色	文字の色を変更する。
左揃え	文字列の配置を左揃えに設定する。
中央揃え	文字列の配置を中央揃えに設定する。
入力文字数	入力可能な残り文字数。 ※全角／半角にかかわらず、すべて1文字としてカウントされる

3. [OK]をクリックします。

7.19 右クリックメニューに特定の URL を追加する

URL ランチャーは、特定のページに簡単にアクセスするためのショートカット機能です。URL を登録することで、右クリックメニューからページにアクセスできるようになります。

1. グローバルメニューの[設定]をクリックします。



2. [URL ランチャー]をクリックします

The screenshot shows the 'サーバ設定' (Server Settings) dialog box. The 'URLランチャー' (URL Launcher) section is selected in the left sidebar. The main area is titled '新しいURLランチャーの作成' (Create new URL launcher). It contains a '名前:' (Name) field, a 'URL:' field with the value 'http://', and an '追加' (Add) button. To the right, there is a 'URL変数' (URL Variables) list with the following items: ホスト名 (Host name), IPアドレス (IP address), メーカー (Manufacturer), モデル (Model), シリアル番号 (Serial number), and ソフトウェアバージョン (Software version). Below this is a table with columns '名前' (Name) and 'URL'. The table is currently empty. At the bottom right, there are 'OK' and 'キャンセル' (Cancel) buttons.

3. 名前を入力し、URL を指定します。

※名前は右クリックメニューのメニュー名として表示されます。

【URL 変数の説明】

項目	説明	例
ホスト名	デバイスのホスト名を引用する。	ホスト名=thirdeye.co.jp のデバイスを選択した場合、URL の "{device.hostname}" の部分が "thirdeye.co.jp" に置き換えられて実行されます。 http://{device.hostname} ⇒ http://thirdeye.co.jp
IP アドレス	デバイスの IP アドレスを引用する。	IP アドレス=192.168.0.1 のデバイスを選択した場合、URL の "{device.ipAddress}" の部分が "192.168.0.1" に置き換えられて実行されます。 http://{device.ipAddress} ⇒ http://192.168.0.1
メーカー	コンフィグバックアップで取得したメーカー名を引用する	http://{device.hardwareVendor}
モデル	コンフィグバックアップで取得したモデル名を引用する	http://{device.model}
シリアル番号	コンフィグバックアップで取得したシリアル番号を引用する	http://{device.assetIdentity}
OS バージョン	コンフィグバックアップで取得したソフトウェアバージョン引用する	http://{device.osVersion}

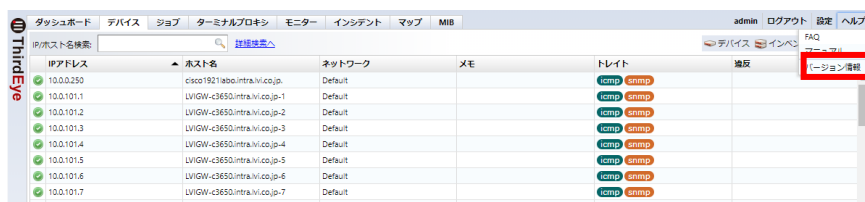
4. [OK]をクリックします。

7.20 ライセンスを更新する

ライセンスのノード数を増やしたりサポート更新したりした場合に、適用されているライセンスを更新する必要があります。ライセンスの更新は、[ヘルプ]→[バージョン情報]から行うことができます。

※この作業は、Administrator 権限を持つユーザのみ行うことができます。

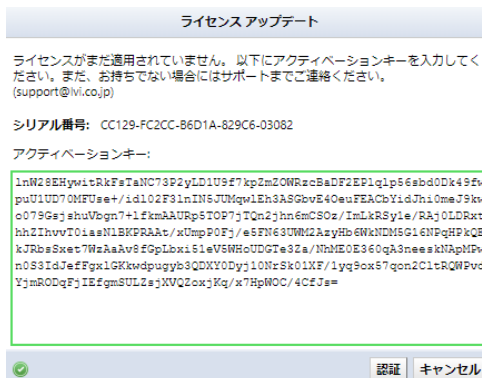
1. グローバルメニューの[ヘルプ]→[バージョン情報]をクリックします。



2. [ライセンス更新]をクリックします。

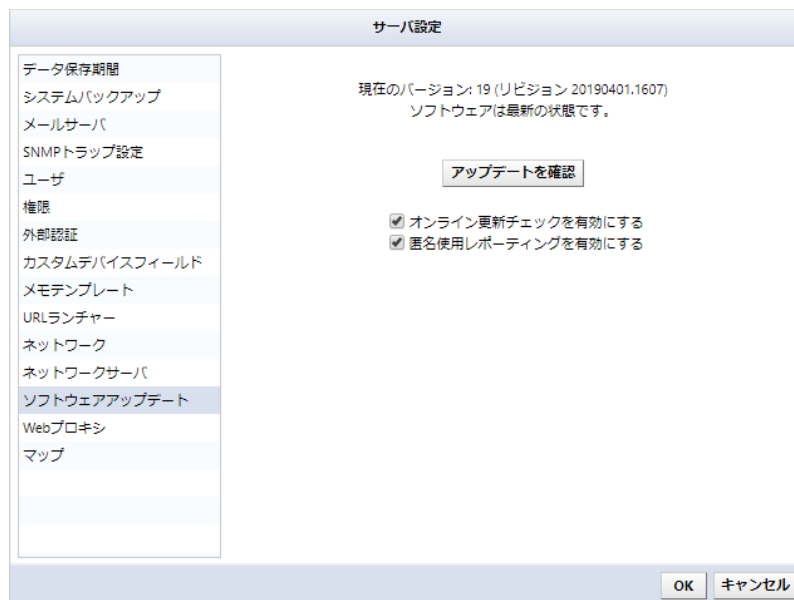


オンライン環境では、自動でライセンス更新がされます。オフライン環境の場合は、アクティベーションキーを入力する画面が表示されます。事前にアクティベーションキーを用意して更新してください。



7.21 オンラインでアップデートをする

ThirdEye をインターネット経由でアップデートをすることができます。ソフトウェアアップデートは、ソフトウェアバージョンのオンラインアップデートに関する設定です。ソフトウェアアップデート設定は、インターネットに接続できる環境でのみ機能します。



項目	説明
アップデートを確認	[アップデートを確認]をクリックすると、更新プログラムの配信をオンラインでチェックします。
オンライン更新チェックを有効にする	[オンライン更新チェックを有効にする]にチェックが入っていると、更新プログラムの配信があるかを定期的に確認します。(初期値:有効)
匿名使用レポートを有効にする	[匿名使用レポートを有効にする]にチェックが入っていると、匿名で利用状況データを送信します。(初期値:有効)

7.22 バージョン(リビジョン)を確認する

現在使用しているバージョン(リビジョン)を確認するには、ヘルプメニューの[バージョン情報]から確認します。



また、仮想マシンのコンソールからも確認することができます。

```
LogicVein - Core Server
https://192.168.40.122
Networking:
-----
IP Address: 192.168.40.122           Netmask: 255.255.255.0
Gateway: 192.168.40.254           DNS: 192.168.0.3 192.168.0.3
Hostname: netld                   Interface: eth0
NTP Server: pool.ntp.org          SSH Server: Running
Time: 2021-03-23 07:54 UTC        Backup: Local
IPv6 Addr: fd14:5839:664d:40:20c:29ff:feb6:baf9
MAC Addr: 00:0C:29:B6:BA:F9

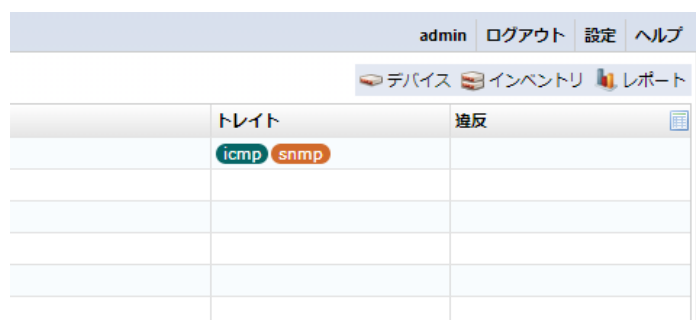
Revision : 20210316.0604
OS Version: 2019.24.0-202103160604
OVA build : 1615874999

Settings menu:
-----
[1] Static IP Address
*[2] DHCP
[3] SSH Server
[4] Import Data
[5] Admin Tools
[6] Reboot
[7] Power Off
```

7.23 プロキシサーバを使用する

プロキシサーバ経由でソフトウェアアップデートやライセンス更新をオンラインで利用する場合、プロキシサーバの情報を設定します。

1. グローバルメニューの[設定]をクリックします。



2. [Web プロキシ]をクリックし、プロキシサーバの情報を入力します。

A screenshot of the 'サーバ設定' (Server Settings) dialog box. The 'プロキシタイプ' (Proxy Type) is set to 'Webプロキシ'. The 'ホスト' (Host) is '192.168.40.200' and the 'ポート' (Port) is '8080'. The 'Realm' is 'logicvein', the 'ユーザ名' (Username) is 'thirdeye', and the 'パスワード' (Password) is 'thirdeye'. A sidebar on the left lists various settings, with 'Webプロキシ' selected. 'OK' and 'キャンセル' (Cancel) buttons are at the bottom right.

項目	説明
プロキシタイプ	プロキシサーバのタイプを次の中から選択します。(初期値:なし) 「なし」、「Web プロキシ」、「SOCKS4 プロキシ」、「セキュア Web プロキシ」
ホスト	プロキシとして使用するサーバの IP アドレスまたはホスト名を指定します。
ポート	プロキシサーバ上のポート番号を指定します。(初期値:8080)
Realm	プロキシの認証レルムを指定します。レルムが必要ない場合は、値を指定しないでください。
ユーザ名	プロキシサーバに送信するユーザ名を指定します。
パスワード	プロキシサーバに送信するパスワードを指定します。

7.24 Zero-Touch (オプション) Suite

Zero-Touch は、物理的に離れたネットワーク上のデバイスにコンフィギュレーションを配布するのに便利なツールです。ツールは Cisco Plug and Play や Cisco Networking Services (CNS)の機能を背景としているので、Zero-Touch はそれらの機能に対応したデバイスでしか用いることができません。

Zero-Touch がコンフィグを配布する形式は主に 3 つあります。

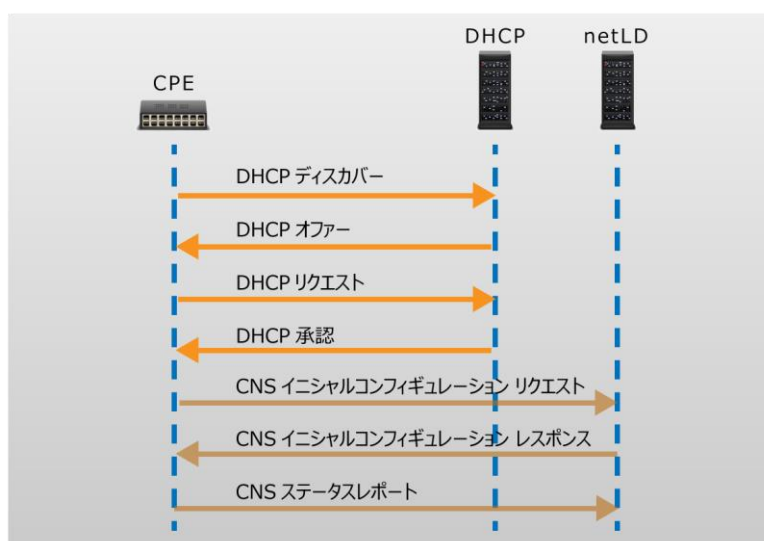
テンプレート:テンプレートベースでコンフィグを配布します。リモートオフィスに新たなデバイスをネットワークに導入する場合に使います。

セルフリカバリ:異常コンフィグを上書きされてしまい、うまく動かなくなってしまったデバイスをリセットするのに便利です。

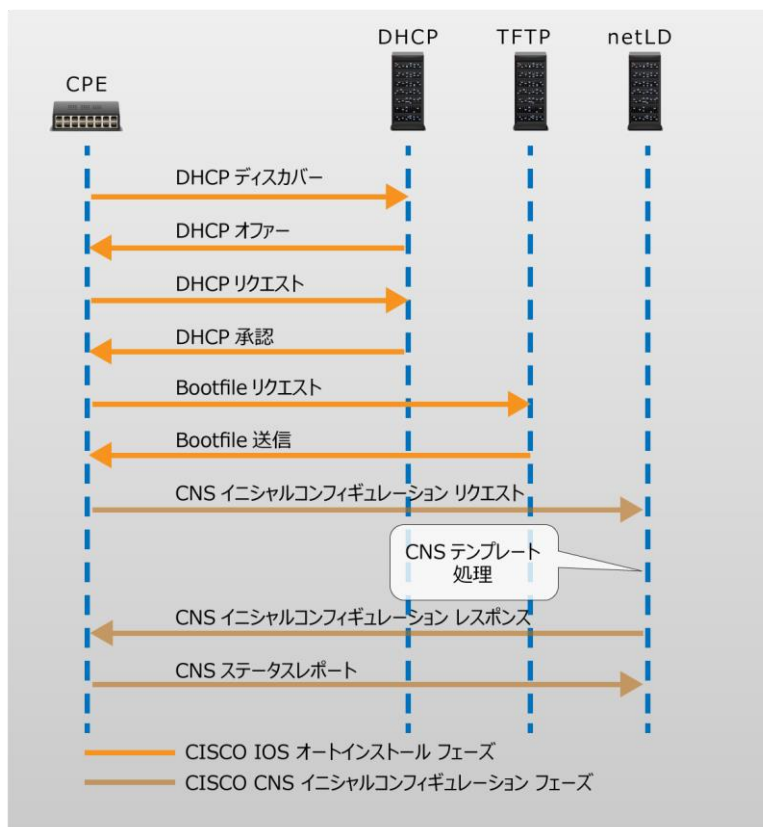
特定デバイスの復元:デバイス装置の更新に便利です。例えば、今まで使われていたデバイスが故障し、同じモデルの別のデバイスに入れ替える場合、それまで使われていた設定を新たなデバイスに書きこむことができます。

ThirdEye Zero-Touch は、以下のようなプロトコルを用いてコンフィギュレーションを配布します。したがって、使用の際にはファイアウォールを適切に設定することが必要となります。

下の図は、PnP を使用した Plug and Play が行う処理の流れを示しています。図を見やすくするために、DHCP、ThirdEye サーバを分割して示して有りますが、これは、3 つのコンピュータを用いるわけではありません。3 つのサーバプログラムはすべて、ThirdEye サーバの動いている一台のコンピュータ上で実行されます。



下の図は、CNS を使用した Plug and Play が行う処理の流れを示しています。PnP を使用した場合と違い DHCP で IP アドレスを取得後、TFTP で Bootfile を取得します。

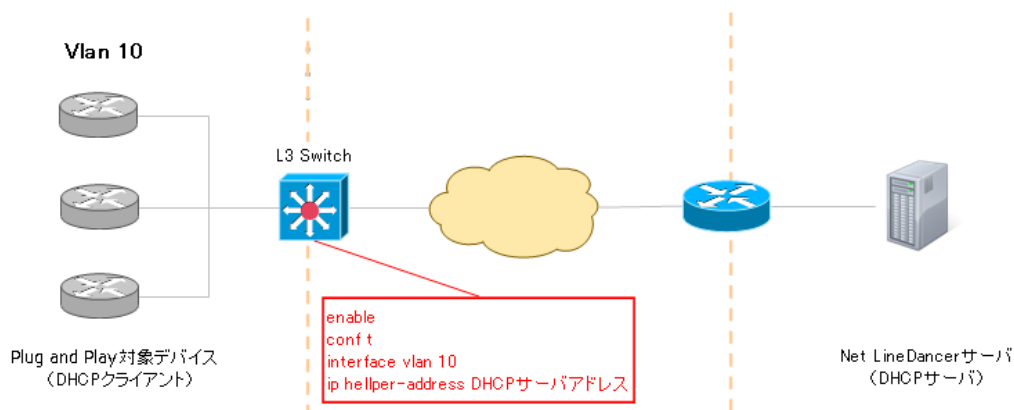


7.24.1 Zero-Touch 要求条件

Zero-Touch を用いるには、以下の条件が整っている必要があります。ご使用前にご確認ください。

- 対象デバイスの IOS のバージョンは、CNS は IOS 12.2 以降、PnP は IOS 15.2(2)以降である必要があります。
- デバイスは startup-config を持っていないはいけません。
- DHCP サーバ - DHCP サーバを ThirdEye 自身に行わせる場合、対象となるデバイスは DHCP の IP アドレス配布が可能なネットワーク内に存在している必要があります。また、対象デバイスが ThirdEye の配布できるネットワークの外に存在している場合は、経路上にあるデバイスに DHCP relay を設定すれば、対象デバイスからの DHCP リクエストを ThirdEye サーバが受信できるようになります。

DHCP リレーの例



7.24.2 Zero-Touch タイプの選択

Zero-Touch のタイプとして Plug and Play と Cisco CNS があります。同時に使用することはできないため、設定→ Zero-Touch 配布と進みます。

これが設定ウィンドウの Zero-Touch セクションです。PnP タイプを選択してください。

サーバ設定

データ保存期間
システムバックアップ
メールサーバ
SNMPトラップ設定
ユーザ
権限
外部認証
カスタムデバイスフィールド
メモテンプレート
URLランチャー
スマートブリッジ
ネットワーク
ネットワークサーバ
Zero-Touch配布
ソフトウェアアップデート
Webプロキシ

PnPタイプ: Plug-and-Play Cisco CNS

PnPサーバ: auto

PnPデバックキングを有効にする

アドレスプール

DHCPサーバを有効にする


リース時間: 5分

アドレスプール	リレーサーバ
Default	無し

OK キャンセル

7.24.3 DHCP サーバ

設定ウィンドウを開き、Zero-Touch セクションにて必要な情報を入力してください。

新たな DHCP プールを設定するには  を押してください。

項目	説明
DHCP サーバを有効にする	ThirdEye がもつ DHCP サーバを利用する場合にはチェックを入れてください。
リース時間	DHCP のリース時間を設定します。

必要な情報を入力し、OK ボタンを押してください。

項目	説明
プール名	作成する DHCP プールの名前を入力
リレーサーバ CIDR	DHCP リレーサーバの存在する IP 範囲を入力
アドレス範囲	配布する IP アドレス範囲を入力(必須)

項目	説明
サブネットマスク	サブネットマスクを入力(必須)
デフォルトゲートウェイ	デバイスのデフォルトゲートウェイを指定
DNS サーバ(オプション)	デバイスからサーバの名前解決を行なうためのDNS サーバを指定

入力が完了しました。

DHCPプールを追加する

プール名:

リレーサーバ CIDR: /

アドレス範囲: -

サブネットマスク:

オーバーライド

デフォルトゲートウェイ:

DNSサーバ:

正しく操作すれば、下の表に新たな項目が追加されるはずですが。

サーバ設定

- データ保存期間
- システムバックアップ
- メールサーバ
- SNMPトラップ設定
- ユーザ
- 権限
- 外部認証
- カスタムデバイスフィールド
- メモテンプレート
- URLランチャー
- スマートブリッジ
- ネットワーク
- ネットワークサーバ
- Zero-Touch配布
- ソフトウェアアップデート
- Webプロキシ

PnPタイプ: Plug-and-Play Cisco CNS

PnPサーバ:

PnPデバックキングを有効にする

アドレスプール

DHCPサーバを有効にする

リース時間

アドレスプール	リレーサーバ	
Default	無し	+
ネットワーク01	192.168.0.100/32	✕

外部の DHCP サーバを使用する

ThirdEye 以外の DHCP サーバを使用する場合には、ThirdEye と通信できる基本的な情報に加え特定のオプションを追加する必要があります。追加するオプションは PnP のタイプにより異なります。

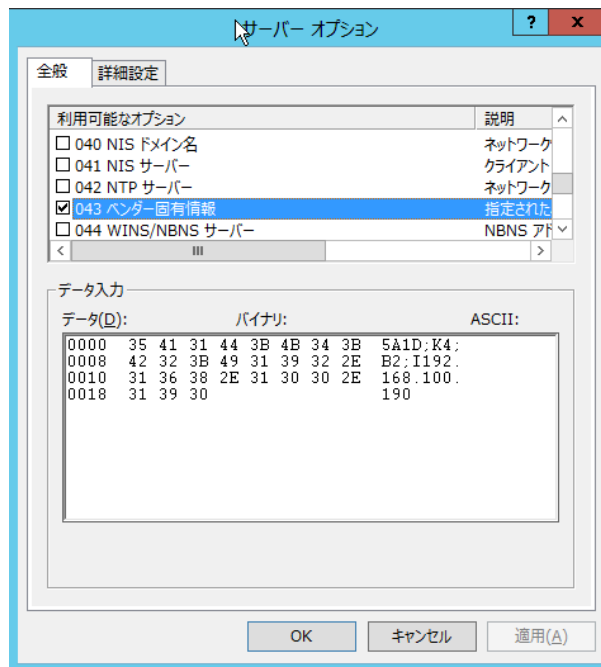
- CNS

オプション 150 またはオプション 6 と 66 どちらも TFTP サーバの情報を渡すオプションです。150 では TFTP サーバの IP アドレスを追加できます。66 では TFTP サーバの名前を追加し 6 で DNS サーバの IP アドレスを追加してデバイスへ渡します。TFTP サーバは ThirdEye を指定する必要があります。Plug and Play が自動で行う処理の流れを示しています。PnP を使用した場合と違い DHCP で IP アドレスを取得後、TFTP で Bootfile を取得します。

- Plug and Play

オプション 43 オプション 43 では、ベンダー固有の情報を追加することができます。

以下の図は Windows の DHCP サーバの設定例です。ASCII 欄に情報を「;」で区切って入力します。



7.24.4 コンフィギュレーションの配布

i. テンプレートベースの配布

大きなネットワークでは、似たようなコンフィグをもつデバイスが沢山あることがよくあります。つまり、コンフィグの違いが IP アドレス、ホスト名、DNS、syslog サーバのアドレスだけであるような場合です。バルクチェンジでは、似たようなコマンドをデバイスごとに柔軟に変化させて送信するためのテンプレートという方法を用いましたが、Zero-Touch では同じテンプレートをコマンドではなくコンフィグにも使うことが出来ます。

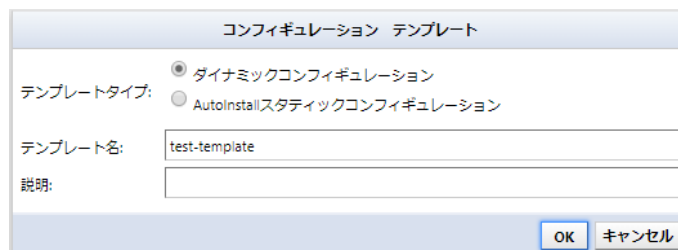
このテンプレートの使い方はすでに解説しているので、ここではその詳細については触れませんが、もしもその章をまだ読んでいない場合は、テンプレートの考え方についてよく理解するためにも、該当する章をお読みになられることを強く推奨いたします。詳しくは、「[7.10 バルクチェンジの概要](#) Suite」を参照してください。

テンプレートを作るためには以下の手順に従ってください。

Zero-Touch → テンプレートタブに移動し、 を押してテンプレートを作成します。



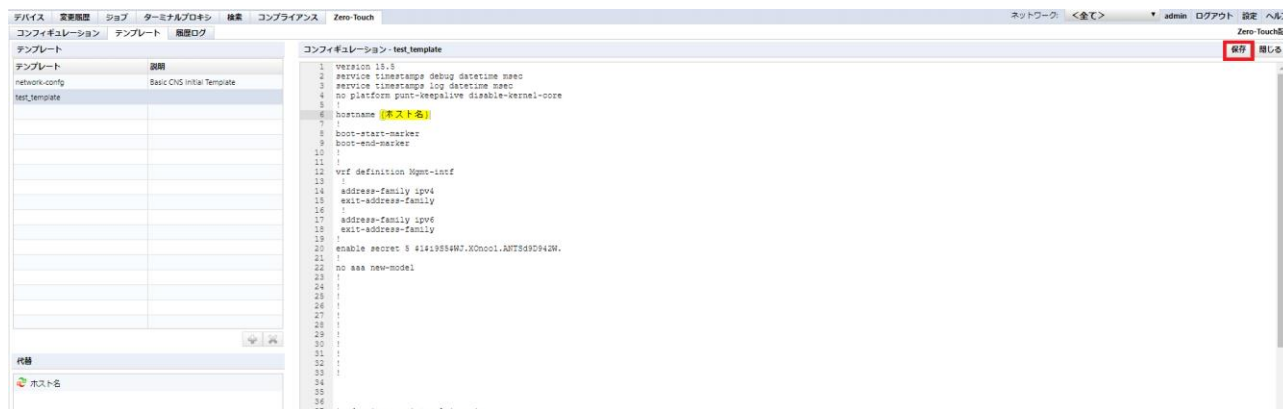
テンプレートタイプにダイナミックコンフィギュレーションを選び、また新たに作るテンプレートの名前をテンプレート名フィールドに入力します。任意で、説明フィールドを記述することができます。終わったら、OK ボタンを押してください。



画面右に大きなテキストエリアが現れます。元となるコンフィギュレーションを、このエリアに入力して下さい。もし Zero-Touch を行う予定のデバイスと同じ機種 of デバイスがインベントリにすでにあるなら、そのデバイスのコンフィギュレーション(例えば start-up config)をコピーし、ここにペーストするのが簡単です。

その後の操作は、「[7.10 バルクチェンジの概要](#) [Suite](#)」で説明したものと同様です。ペーストしたコンフィグに変数を導入し、これをテンプレートにします。


必要な変数をすべて追加したら、テンプレートを保存する必要があります。テキストエリア右上の保存と書かれたボタンをクリックし、作ったテンプレートを保存してください。



デプロイしたコンフィギュレーションをデバイス内に保存したくない場合は、デプロイするコンフィグの `cns config initial...` 文の最後に、`no-persist` オプションを追加してください。

(1) デバイスの登録

さて、これで、Zero-Touchに必要なテンプレートの準備が整いました。次に行うことは、設定の配布先となるデバイスの登録です。対象デバイスごとのテンプレート変数の値を設定する必要もあります。

まず、メインペインをコンフィギュレーションサブタブに移動してください。そこで、Zero-Touch デバイスコンフィギュレーションの  を押してください。





デバイス 変更履歴 ショブ ターミナルプロキシ 検索 コンプライアンス Zero-Touch

コンフィギュレーション テンプレート 履歴ログ

PnPデバイスコンフィギュレーション コンフィギュレーション

デバイスIDまたはテンプレート: 実行

デバイスID	テンプレート
<input checked="" type="checkbox"/> FDO2107A1DL	test_template
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	
<input type="checkbox"/>	

ライブステータス

デバイスID	ステータス

(2) テンプレート変数に入れる値を外部からインポートする

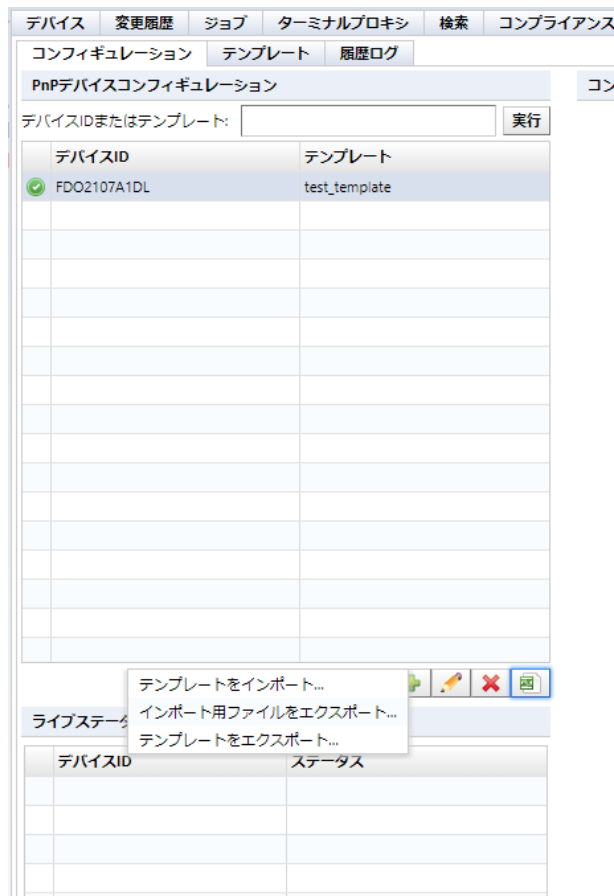
外部にて Excel ファイルで記述されたテーブルを、テンプレートの値として利用することができます。インポートを行うためには、次の手順を追ってください。

Zero-Touch の作業中、デバイスの代替値を入力する所で、閉じるボタンを押してください。



ボタンを押し、サブメニューを表示してください。


現れたメニューからインポート用ファイルをエクスポートあるいはテンプレートをエクスポートメニューから選択してください。



項目	説明
テンプレートをインポート	変数値を格納したエクセルファイルを読み込み、登録します。
インポート用ファイルをエクスポート	値を追記できる空のエクセルシートを出力します。
テンプレートをエクスポート	現在の変数値を反映したエクセルシートを出力します。

出力されたファイルを編集し、テンプレート変数の値を順番に入力していきます。入力後に保存を行うことを忘れないでください。

	A	B	C	D	E	F	G	H	I
1	CNS Device ID	Template	hostname	enable pas	VTY passw	IP address	Mask	community	type
2	FHK134570SY	1812J	1812J	lvi	lvi	192.168.0.1	255.255.255.	(lvi	RW
3									
4									
5									

ThirdEye に戻り、 を再び押し、現れたメニューからテンプレートをインポートを押してください。

コンフィギュレーション
テンプレート
履歴ログ

PnPデバイスコンフィギュレーション
コンフィギュレーション

デバイスIDまたはテンプレート 実行

デバイスID	テンプレート
<input checked="" type="checkbox"/> FHK104780MN	セルフカバリ
<input checked="" type="checkbox"/> TEST	特定デバイスの復元
<input checked="" type="checkbox"/> TESTEST	セルフカバリ
<input checked="" type="checkbox"/> TESTESTEST	Tsune_test

◀ 1 - 1 / 1 ▶
+
✎
✖
📄


ライブステータス

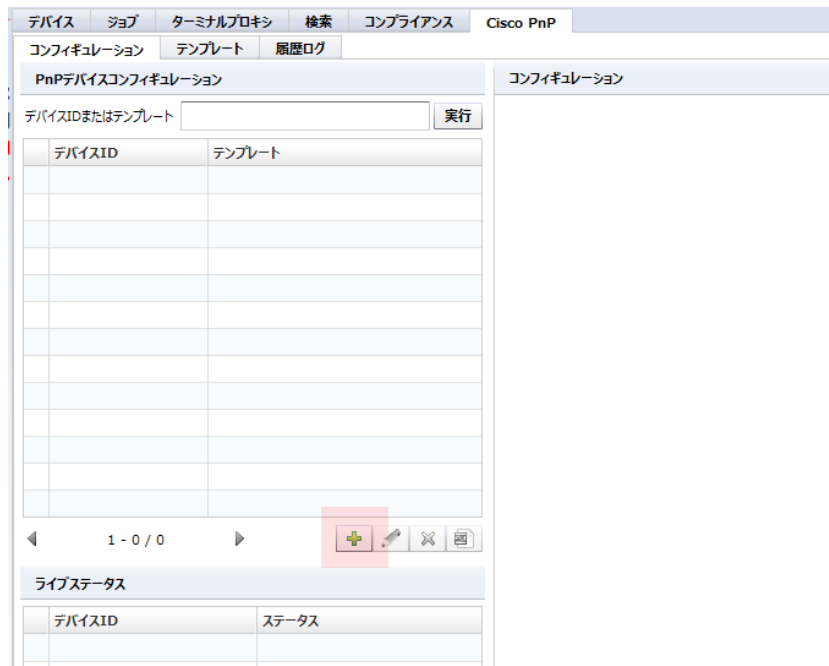
デバイスID	ステータス

- テンプレートをインポート...
- インポート用ファイルをエクスポート...
- テンプレートをエクスポート...

(3) Zero-Touch セルフリカバリ

Zero-Touch は、新たなコンフィギュレーションを送信する代わりに、それまでに ThirdEye 内部に保存されている他のコンフィギュレーションを送信することができます。この機能は、たとえば現在稼働中のデバイスコンフィグがまちがって消去されてしまった場合に有効です。コンフィグが無くなったデバイスは応答しなくなるため、Zero-Touch のような特殊な機能を用いなくては復旧することができません。必要な作業はテンプレートをもちいた Zero-Touch と多くの点で共通です。

まず、メインペインでコンフィギュレーションサブタブに移動してください。そして、を押してください。



デバイスコンフィギュレーションダイアログにて、必要な情報を入力してください。終わったら、OK ボタンを押してください。ただし、配布タイプの項で、セルフリカバリオプションを選択してください。

PnPデバイスコンフィギュレーション	
デバイスID:	FHK104780MN
配布タイプ:	セルフリカバリ
OK キャンセル	


その後、ThirdEye 内に保存されていたコンフィギュレーションデータがデバイスに書き戻されます。その他にテンプレート配信モードと異なる点はありません。

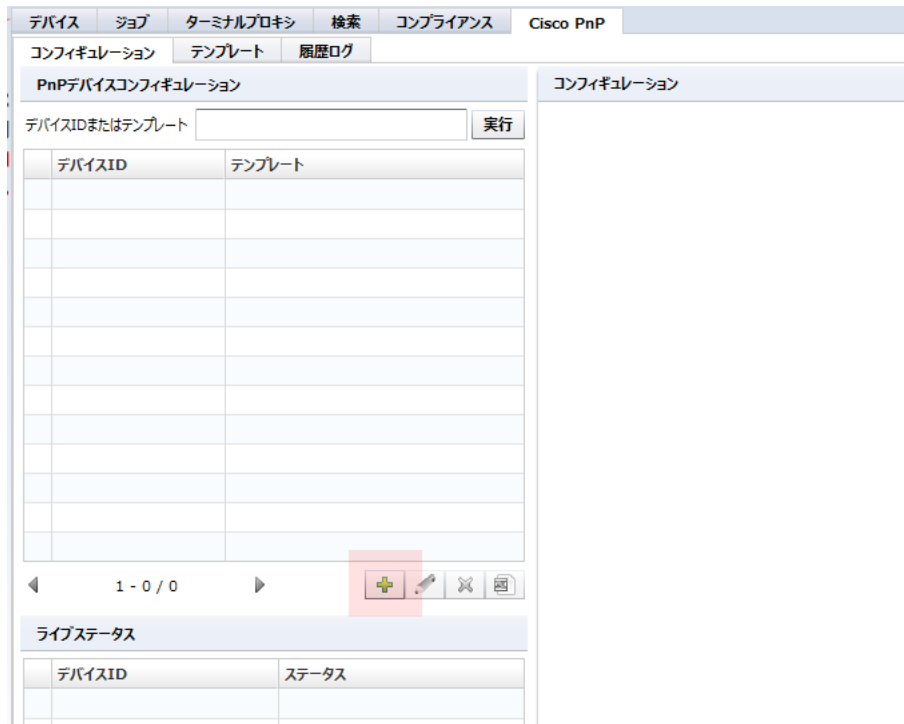
(4) Zero-Touch 特定デバイスの復元

この機能は、古いデバイスを新しいデバイスで入れ替える場合に用います。この機能のおかげで、デバイスが壊れて正常に動かなくなった時でも、新しいデバイスを同じ位置に接続して復旧できます。このモードで Zero-Touch を実行すると、それまで使っていた古いデバイスのコンフィグが新しいデバイスに書かれます。

この機能は、デバイスが遠く離れた位置にあって(別のデータセンターなど)、かつ現地に操作を担当できるものがおらず、直接手で操作することができない時に極めて有効です。Zero-Touch を用いれば、現地のデータセンターの人間にケーブルを挿し込むよう電話で指示できればよく、現地の人間に特殊技能は求められません。その後のデバイス復元などの操作が、現地ではなくネットワーク経由で行われるからです。

セルフリカバリと同様、特定デバイスの復元機能は Zero-Touch テンプレート機能とほぼ同様の操作で行うことができます。

まず初めに、メインペインのコンフィギュレーションサブタブを開き、その中に表示されている  を押してください。



The screenshot shows the Cisco PnP configuration interface. At the top, there are tabs for 'デバイス' (Devices), 'ジョブ' (Jobs), 'ターミナルプロキシ' (Terminal Proxy), '検索' (Search), 'コンプライアンス' (Compliance), and 'Cisco PnP'. Below these are sub-tabs for 'コンフィギュレーション' (Configuration), 'テンプレート' (Template), and '履歴ログ' (History Log). The main content area is titled 'PnPデバイスコンフィギュレーション' (PnP Device Configuration) and 'コンフィギュレーション' (Configuration). It features a search bar for 'デバイスIDまたはテンプレート' (Device ID or Template) and an '実行' (Execute) button. Below this is a table with columns 'デバイスID' (Device ID) and 'テンプレート' (Template). At the bottom of the table, there is a navigation bar with a left arrow, '1 - 0 / 0', a right arrow, and a red box highlighting a green plus sign icon. Below the table is a 'ライブステータス' (Live Status) section with a table for 'デバイスID' (Device ID) and 'ステータス' (Status).

Zero-Touch デバイスコンフィギュレーションダイアログ内で、必要な情報を入力します。配布タイプに、特定デバイスの復元機能を選択してください。完了後、OK ボタンを押してください。

PnPデバイスコンフィギュレーション	
デバイスID:	FHK894572MN
配布タイプ:	特定デバイスの復元
リカバリデバイスID:	FHK221816MN
OK キャンセル	

ここには、リカバリデバイス ID という追加のフィールドがあります。リカバリデバイス ID は一つ目の欄と同じくデバイス ID を指定しますが、この項目には、入れ替え前の古い機器の ID を入力します。

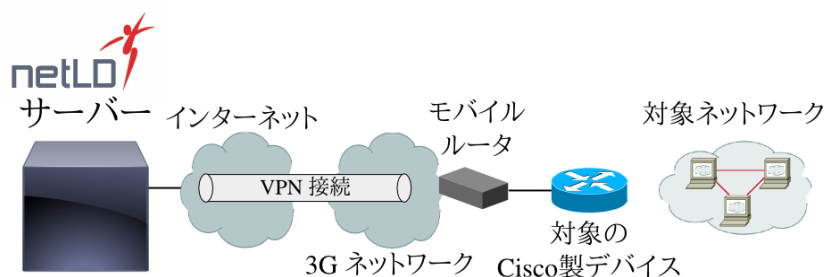
その後、ThirdEye にある、古いデバイス用のコンフィギュレーション情報が、ネットワーク経由で新しいデバイスにアップロードされます。その他の操作方法は Zero-Touch テンプレートの操作方法と同じです。

7.24.5 新規導入デバイスを扱う際の注意

ThirdEye Zero-Touch を用いてコンフィギュレーションをアップロードする際、もしそのデバイスの電源を入れるのが購入してから初めてである場合には、そのデバイスには startup-config が存在しないようにする必要があります。そのようにするためには、ベンダーへのデバイスの発注時に適切な注文オプションを指定してください(例:CCP-CD-NOCF, CCP-EXPRESS-NOCF オプションなど。)

7.24.6 3G ネットワークあるいは VPN 付きモバイルルータ経由での配布

ThirdEye は、コンフィギュレーションを 3G ネットワーク経由で配布することができます。



あるデバイスにコンフィグを配布しないといけないとして、そのデバイスが配置される予定のネットワークで、いくつかのサービスが利用不可である場合を考えてみてください。たとえば、対象のネットワークではインターネットへのアクセスが遮断されているかもしれません。これは、セキュリティを重視しているネットワークでは容易に想像できることです。

遮断は、物理的に接続が無いことが理由のこともあれば、注意深く設定された強力なファイアウォールが稼働しているからかもしれません。デバイスコンフィグの配布のために一時的にファイアウォールを変更するという回答は正しいでしょうか？ セキュリティについて厳格であれば、それが極めてリスクを伴うことだという事はお気づきでしょう。

利用不可であるサービスはインターネットに限りません。DNS や DHCP サービスが利用不可なネットワークもありえます。すべてが静的な IP テーブルで動いているネットワークでは、メンテナンス用のターミナルデバイス挿入する余地すらないかもしれません。

このような問題が起こるのは、主にその対象ネットワークがあなた自身のものでない時です。たとえば、仮に御社がネットワークのメンテナンス事業を受けおっており、対象ネットワークがあなたの顧客のネットワークである場合です。そのような場合は、3G 接続をうまく活用することができます。なぜなら、3G の無線ネットワークを用いてインターネットに接続すれば、対象ネットワークを一切利用することなくデバイスと ThirdEye を接続できるからです。

3G を用いる他の大きな利点としては、次のようなものが挙げられます。

3G 回線からインターネットに接続するためには PPPoE を設定する必要がありません。

3G モバイルルータは再利用できるので、対象ネットワークのあるデータセンターごとに常時準備しておく必要のあるモバイルルータは極少数です。そのため、必要経費は限定的です。

以下の説明では、3G ベースのコンフィグ配布方法について簡単に説明します。

Zero-Touch タブにて、Cisco デバイスにコンフィグを配布するのに必要な設定をあらかじめすべて行なっておきます。つまり、テンプレートを作り、デバイス ID を登録することが含まれます。

モバイルルータの電源を入れ、データセンターへの VPN 接続を有効にします。

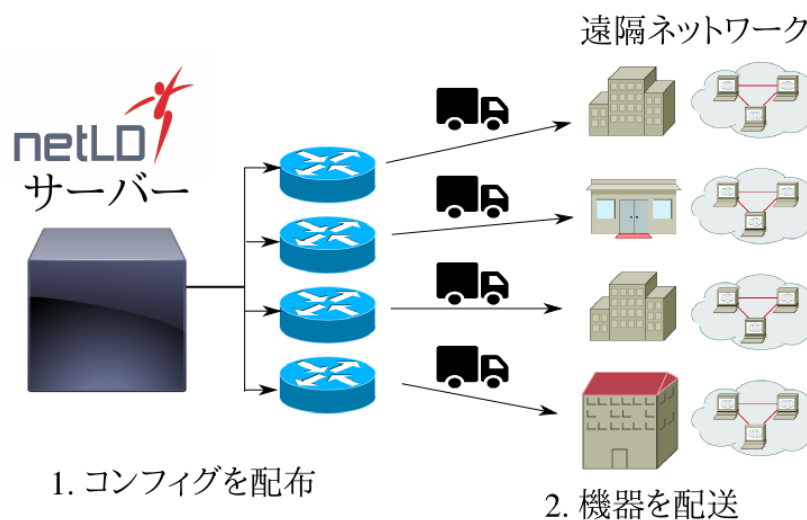
新たな Cisco 製デバイスを モバイルルータに接続します。

ThirdEye がデバイスからのリクエストを自動的に受け取り、コンフィギュレーションを 3G ネットワーク経由で送信します。

配布が終了したあと、電話などで対象ネットワークの近くにいる管理要員に指示し、デバイスにネットワークケーブルを差し込みます。そうすれば、デバイスはデータセンターのネットワークに正しく接続されます。

7.24.7 デバイスを手元で設定してから遠隔地に送付する場合

デバイスを遠隔地に送付するもうひとつの方法は、デバイスを手元で設定してから遠隔地に宅配便で送付する方法です。



ただ単純に、Zero-Touch を用いて手元でデバイスにコンフィグを書き込み、その後デバイスを遠隔地に送付します。この手法の良い点は極めてシンプルでわかりやすいことですが、悪い点は、デバイスを一旦手元に取り寄せるための手間と経費がかかってしまうことです。デバイスを製造元から直接遠隔地に送る必要がある場合には、この手法を使うことはできません。

7.24.8 ブートストラップコードの配布

DHCP の利用が不可能なネットワークでのコンフィギュレーション配布には、ブートストラップコードを予め送付しておくという追加の操作が必要になります。下に示すものは、ThirdEye Zero-Touch のためのブートストラップ例です。〈IP〉の部分を実際の ThirdEye サーバの IP アドレスに読み替えてください。

```
cns id hardware-serial
!
cns connect cns-profile ping-interval 10 retries 3 sleep 5 discover interface FastEthernet template cns-
profile
!
cns template connect cns-profile
cli description Basic CNS Initial Template
cli ip address dhcp
cli ip route 0.0.0.0 0.0.0.0 ${interface}
cli no shutdown
exit
!
cns config initial <IP> status http://<IP>/cns/config.asp
!
end
```

第8章 システムバックアップ／復元

システムバックアップとは、ThirdEye 全体をバックアップするものです。各種設定やモニターデータ（ポーリング、SNMPトラップなど）をバックアップ／復元することができます。システムバックアップは、[設定]→[システムバックアップ]から実行します。

8.1 自動でシステムバックアップを実行する

自動でシステムバックアップを実行する設定は、デフォルトで有効になっています。無効にする場合は、自動でシステムバックアップを実行する時間を変更する場合には、以下の赤枠の内容を変更します。

サーバ設定

日次システムバックアップを有効にする

日次システムバックアップを次の時間に実行する: 7 : 0

保持するバックアップの数: 7

システムバックアップを実行

最新のシステムバックアップ: 2021/03/24 09:06 (ダウンロード)

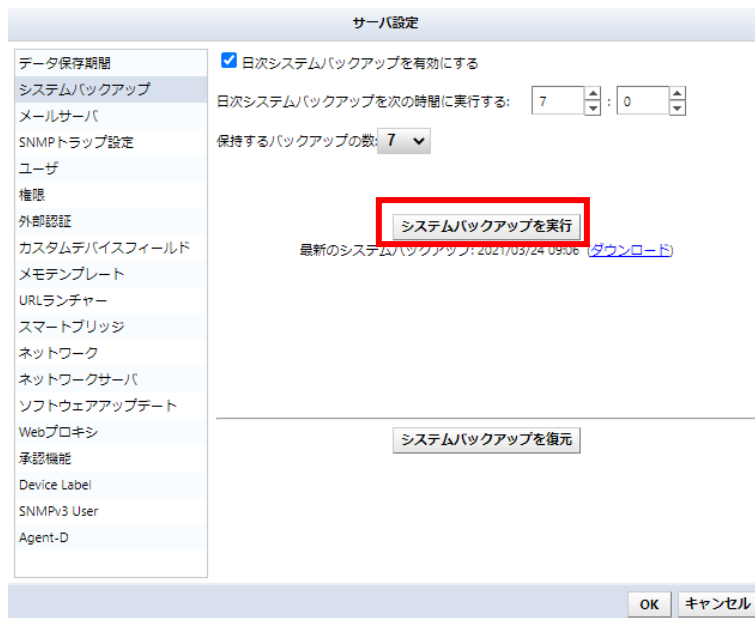
システムバックアップを復元

OK キャンセル

項目	説明
日次システムバックアップを有効にする	日次システムバックアップを有効に設定します。この設定が有効になっている場合、指定された時間にシステムバックアップが実行されます。(初期値: 有効)
日次システムバックアップを次の時間に実行する	日次システムバックアップの実行時間を指定します。(初期値: 7:00)

8.2 手動でシステムバックアップを実行する

設定変更などで、システムバックアップを実行する場合には、[システムバックアップを実行]をクリックします。



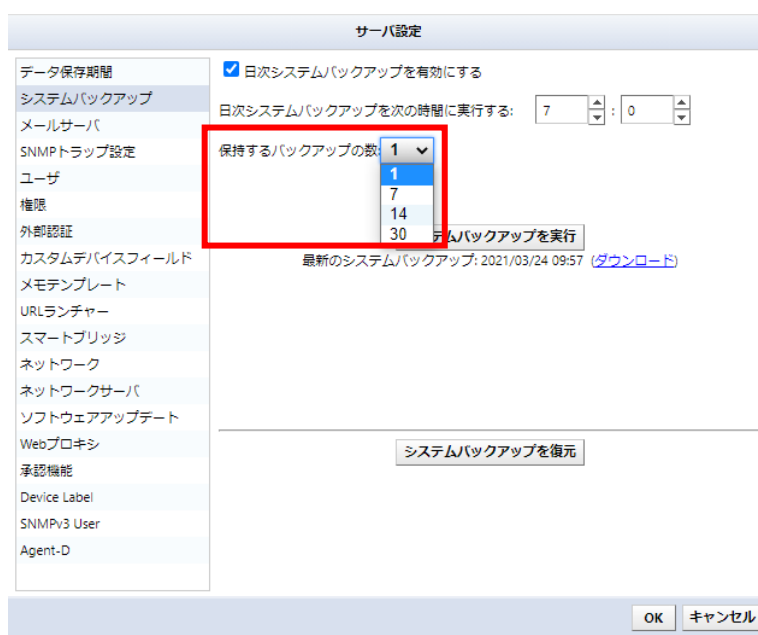
バックアップ実行中は、ボタンがグレーアウトされます。グレーアウトが解除され、最新のシステムバックアップ日時が更新されれば完了です。



8.3 システムバックアップの保有数を変更する

システムバックアップを保持する世代数をリストから選択します。[保持するシステムバックアップの数]のデフォルト値は「7」です。この場合、「7世代」分のシステムバックアップがファイルとして保持され、世代数を超えた古いデータは削除されます。

動作環境にもよりますが、運用期間が長くなるにつれて蓄積されるデータが増加し、システムバックアップ自体のファイルサイズが大きくなる傾向にあります。そのため、保持するシステムバックアップの数が多い場合、システムバックアップがディスク容量を圧迫する可能性があります。保持するシステムバックアップの世代数を減らすことで、ディスク使用量を抑えることができます。



8.4 外部ストレージに保存する

デフォルトでは、システムバックアップファイルは仮想アプライアンス内部に保存されますが、外部ストレージを設定することで仮想アプライアンスの外部に自動的に保存することができます。対応プロトコルは NFS/SMB です。

外部ストレージを設定するには、次の操作を行います。

1. キーボードの「5」キーを押し、「Admin Tools」を選択します。

```
LogicVein - Core Server
https://192.168.40.122

Networking:
-----
IP Address: 192.168.40.122      Netmask: 255.255.255.0
Gateway: 192.168.40.254      DNS: 192.168.0.3 192.168.0.3
Hostname: net1d              Interface: eth0
NTP Server: pool.ntp.org     SSH Server: Running
Time: 2021-03-23 07:54 UTC   Backup: Local
IPv6 Addr: fd14:5839:664d:40:20c:29ff:feb6:baf9
MAC Addr: 00:0C:29:B6:BA:F9

Revision : 20210316.0604
OS Version: 2019.24.0-202103160604
OVA Build : 1615874999

Settings menu:
-----
[1] Static IP Address
*[2] DHCP
[3] SSH Server
[4] Import Data
[5] Admin Tools
[6] Reboot
[7] Power Off
```

2. キーボードの「4」キーを押し、「Configure a remote filesystem for backups」を選択します。

```
Admin Tools menu:
-----
[1] Run Config Diff Cleanup
[2] Vacuum Database
[3] Reset Admin Password
[4] Configure a remote filesystem for backups
[5] Reset Admin Dashboard API Token
[6] Configure Built-in Agent-D
```

3. サーバの種類を選択します。

```
Configure an NFS/SMB backup share folder:
-----
[1] Configure an NFS server
[2] Configure an SMB server
-
```

4. 必要な情報を入力し、「Enter」キーを押します。

```

Configure an NFS/SMB backup share folder:
-----
[1] Configure an NFS server
[2] Configure an SMB server

Remote NFS path: _

```

項目	説明
Remote NFS/SMB path	ネットワークパス/IP アドレス
Username	サーバに設定しているユーザ名 ※SMB の場合のみ
Password	サーバに設定しているパスワード ※SMB の場合のみ

5. 以下を選択します。

```

Configure an NFS/SMB backup share folder:
-----
[1] Configure an NFS server
[2] Configure an SMB server

Remote NFS path: 10.0.111.1:/datastore
Validating configuration...
Saving configurations...
Configurations verified successfully. Do you want to?

[1] Copy existing backups to the NFS/SMB and delete
[2] Delete existing backups

```

項目	説明
[1] Copy existing backups to the NFS/SMB and delete	既存のバックアップを NFS/SMB にコピーしてから 削除する
[2] Delete existing backups	既存のバックアップを削除 する

以上でコンソール画面の設定は完了です。ThirdEye の自動再起動後、コンソール画面で設定内容を確認できます。


```
LogicVein - Core Server
https://192.168.40.122

Networking:
-----
IP Address: 192.168.40.122      Netmask: 255.255.255.0
Gateway: 192.168.40.254      DNS: 192.168.0.3 192.168.0.3
Hostname: net1d              Interface: eth0
NTP Server: pool.ntp.org      SSH Server: Running
Time: 2021-03-24 02:46 UTC    Backup: 10.0.111.1:/datastore
IPv6 Addr: fd14:5839:664d:40:20c:29ff:f0b6:baf9
MAC Addr: 00:0C:29:B6:BA:F9

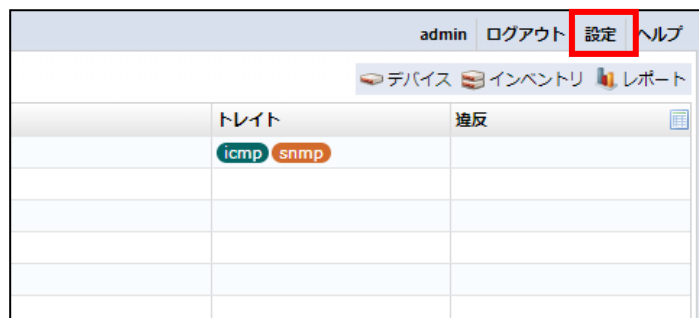
Revision : 20210316.0604
OS Version: 2019.24.0-202103160604
OVA Build : 1615874999

Settings menu:
-----
[1] Static IP Address
*[2] DHCP
[3] SSH Server
[4] Import Data
[5] Admin Tools
[6] Reboot
[7] Power Off
```

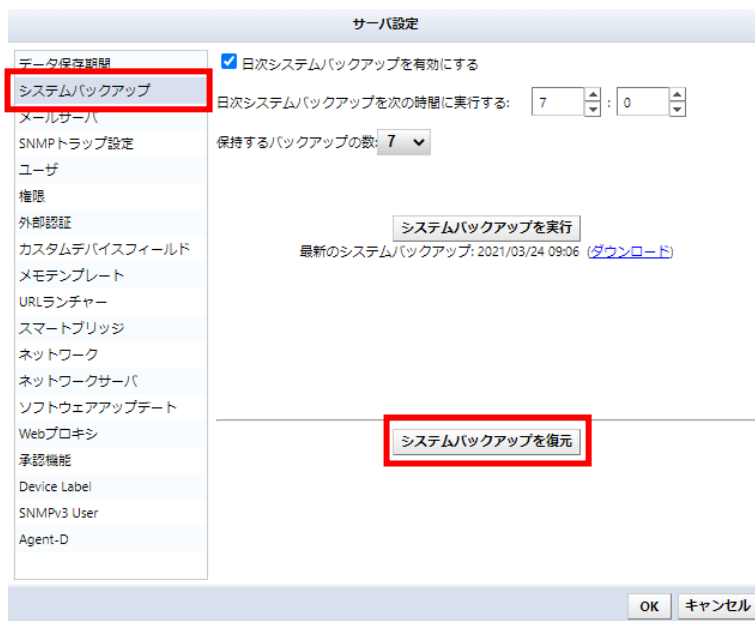
8.5 システムバックアップを復元する

復元するには、バックアップ元とリストア先のバージョン(リビジョン)が同じである必要があります。
バージョンの確認方法については、「[7.22 バージョン\(リビジョン\)を確認する](#)」を参照してください。

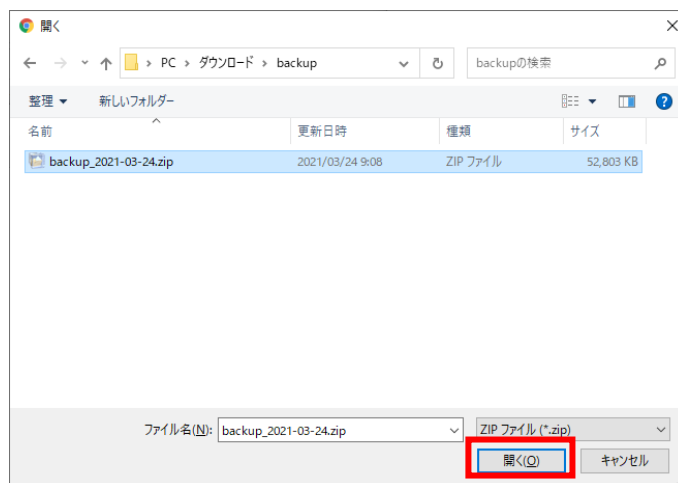
1. Administrator 権限を持つユーザでログインします。
2. [設定]をクリックします。



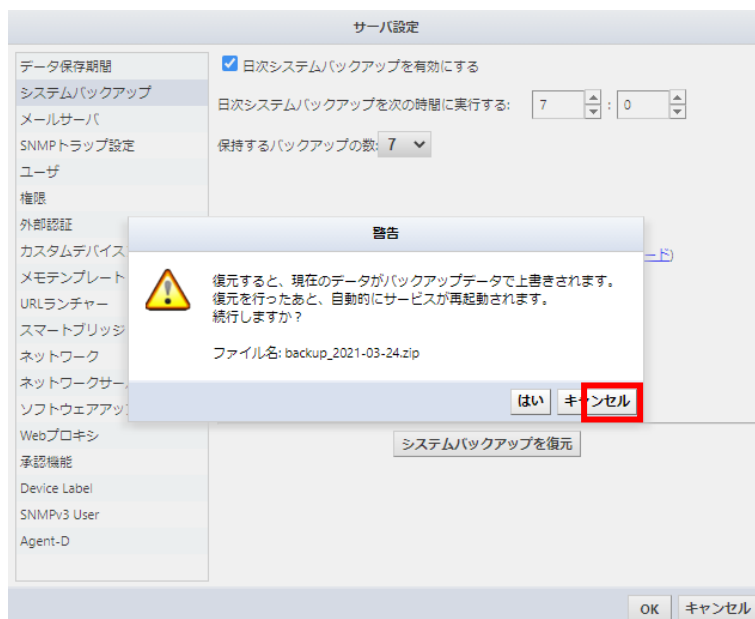
3. [システムバックアップ]から、[システムバックアップを復元]をクリックします。



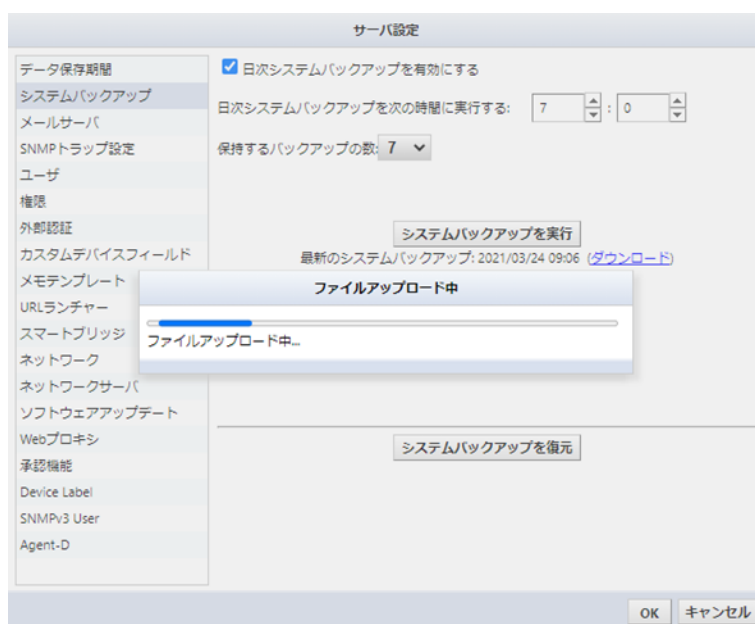
4. 復元するファイルを選択し、[開く]をクリックします。



5. 警告画面にて[はい]をクリックします。



6. ファイルがアップロードされ、復元が開始されます。



操作は以上です。アップロード後、サービスが自動で再起動されログイン画面に戻ります。

第9章 再起動／シャットダウン

再起動およびシャットダウンは、仮想マシンコンソール上でキーボードを使って操作します。

```
LogicVein - Core Server
https://192.168.40.122

Networking:
-----
IP Address: 192.168.40.122           Netmask: 255.255.255.0
Gateway: 192.168.40.254           DNS: 192.168.0.3 192.168.0.3
Hostname: netld                   Interface: eth0
NTP Server: pool.ntp.org          SSH Server: Running
Time: 2021-03-23 07:54 UTC       Backup: Local
IPv6 Addr: fd14:5839:664d:40:20c:29ff:feb6:baf9
MAC Addr: 00:0c:29:b6:ba:f9

Revision : 20210316.0604
OS Version: 2019.24.0-202103160604
OVA Build : 1615874999

Settings menu:
-----
[1] Static IP Address
*[2] DHCP
[3] SSH Server
[4] Import Data
[5] Admin Tools
[6] Reboot
[7] Power Off
```

再起動する場合は、キーボードの「6」キーを押し[Reboot]を選択します。

シャットダウンする場合は、キーボードの「7」キーを押し[Power Off]を選択します。

メニュー選択後、確認メッセージが表示されるので、キーボードの「Y」キーを押し実行します。

【再起動】

```
Settings menu:
-----
[1] Static IP Address
*[2] DHCP
[3] SSH Server
[4] Import Data
[5] Admin Tools
[6] Reboot
[7] Power Off
Are you sure you want to REBOOT ? (y/N) [default: N]
```

【シャットダウン】

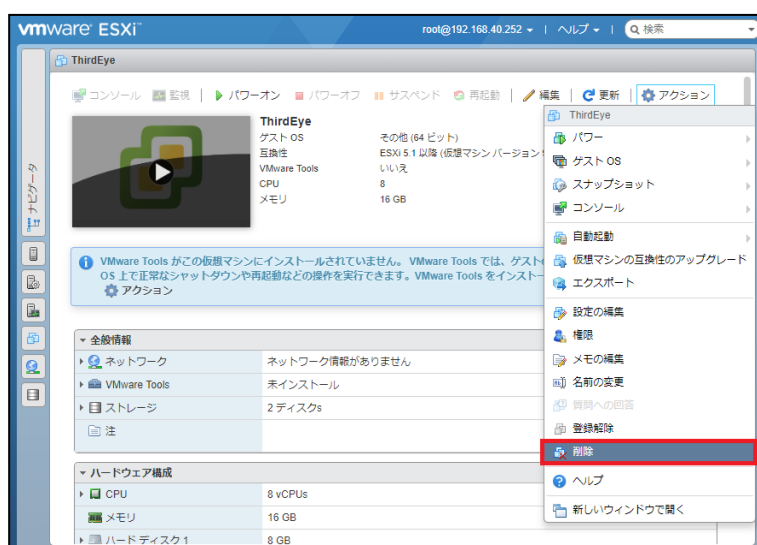
```
Settings menu:
-----
[1] Static IP Address
*[2] DHCP
[3] SSH Server
[4] Import Data
[5] Admin Tools
[6] Reboot
[7] Power Off
Are you sure you want to POWER OFF ? (y/N) [default: N] _
```

第10章 アンインストール

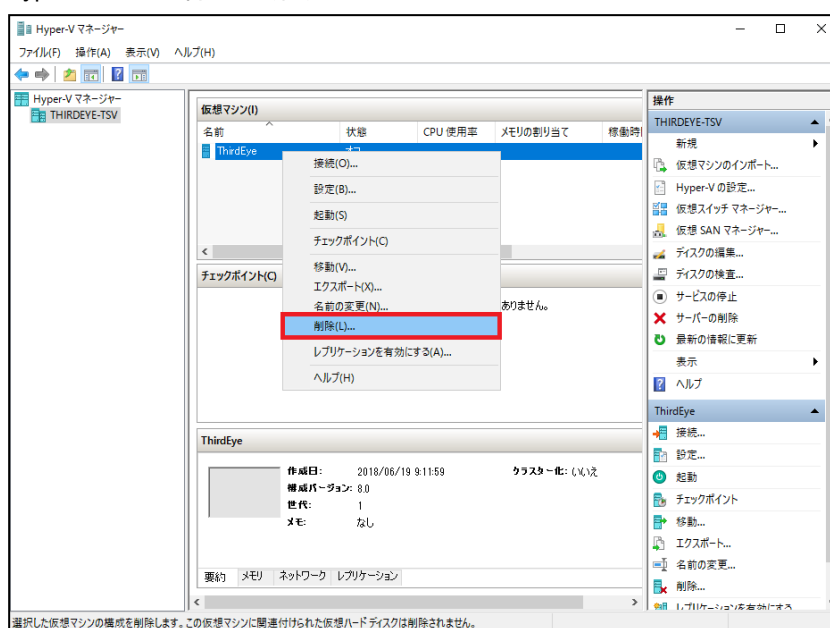
10.1 アンインストールする

1. ThirdEye をシャットダウンします。
2. シャットダウン完了後、仮想のホスト OS から ThirdEye の仮想マシンを削除します。

- VMware ESXi 6.5 での削除画面(例)



- Windows Hyper-V での削除画面(例)



以上で ThirdEye のアンインストールは完了です。

第11章 お問い合わせ

ThirdEye の操作中に問題や疑問が生じた場合は、下記の弊社サポートまでお問い合わせください。

お問い合わせの前に、あらかじめ下記の必要事項をご確認ください。

【必須事項】

1. 製品名
2. 製品のバージョン情報(リビジョンを含む)
3. 製品のシリアル番号(ThirdEye のライセンス情報)
4. 具体的な症状や疑問点(スクリーンショットをお送りいただけると、情報共有を円滑に行うことができ、問題の解決に役立つことがあります。)

■お問い合わせ先■

株式会社ロジックベイン サポート窓口

電話: 044-871-4010

メール: support@lvi.co.jp

受付時間: 平日 9:00～12:00 / 13:00～17:00 (※土・日・祝日および弊社休業日を除く)

第12章 巻末資料

12.1 ICMP ポーリングについて

ThirdEye の ICMP モニターは、「インターバル」、「ICMP 送信回数」、「リトライ」の設定で構成されています。各項目の説明を以下に示します。

Ping 1min ✎ インターバル: min 保存 閉じる

ICMP送信回数: 2回送信 (レスポンスタイムは2回のうち小さい値を保存)
 1回送信

リトライ: 自動リトライ (最大5回)
 なし

🚩 トリガー

レスポンス確認 ✕

期間: min カウント:

ポリシー: 重大度: メッセージ:

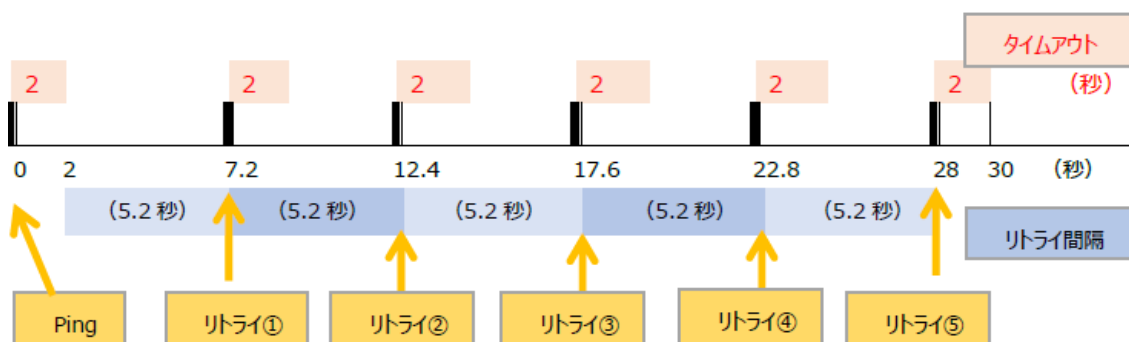
項目	説明	
インターバル	ICMP モニターのポーリング間隔	
ICMP 送信回数	ICMP パケットの送信回数を、次の中から選択する。	
	2 回送信	ICMP パケットを 2 回送信する。 ※ICMP モニターで監視可能な「roundTripTime」(レスポンスタイム)は、2 回のうち小さい値が保存される。
	1 回送信	ICMP パケットを 1 回送信する。
リトライ	ICMP 送信回数とは別に、リトライを実行するかを選択する。	
	自動リトライ (最大 5 回)	ICMP 送信回数に対して応答がない場合、自動リトライアルゴリズムが開始される。自動リトライは最大 5 回まで行われる。リトライ間隔は、モニターのインターバルに基づき、動的に平均化される。ただし、リトライ間隔は最大 25 秒である。 初回ポーリングと自動リトライに応答がない場合、2 回目以降のポーリングで自動リトライは実行されない。
	なし	リトライを行わない。

※ICMP タイムアウトは常に 2 秒で、変更することはできません。

動作イメージ①

【設定例①】

項目	設定値
インターバル	30 秒
ICMP 送信回数	1 回送信
リトライ	自動リトライ(最大 5 回)



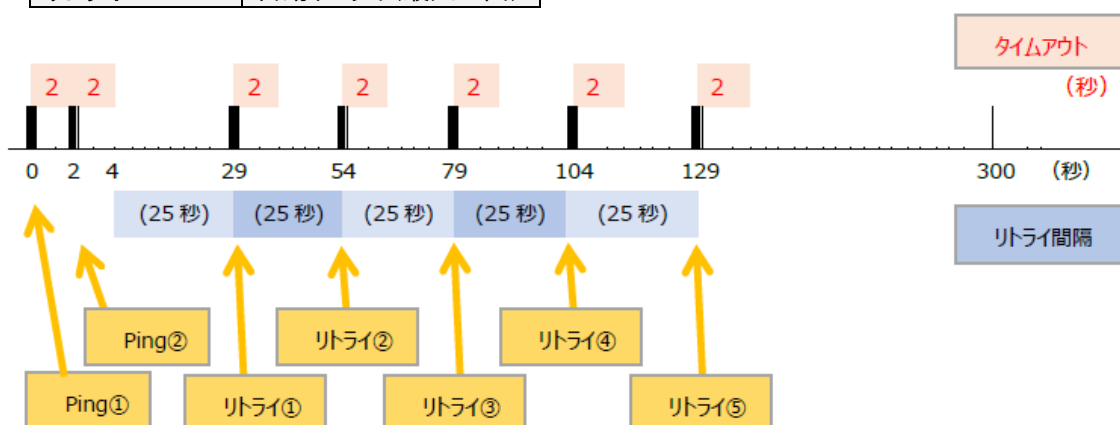
【説明①】

インターバルを 30 秒に設定すると、30 秒のあいだに Ping(ここでは 1 回)、リトライ最大 5 回が実行されます。リトライ間隔は、モニターのポーリング間隔に基づいて動的に平均化され、ここでは 5.2 秒となっています。

動作イメージ②

【設定内容②】

項目	設定値
インターバル	5 分(300 秒)
ICMP 送信回数	2 回送信
リトライ	自動リトライ(最大 5 回)



【説明②】

ICMP 送信回数が「2 回送信」の場合、Ping を 2 回送信した後、リトライ最大 5 回が実行されます。リトライ間隔は、モニターのポーリング間隔に基づいて動的に平均化されますが、最大 25 秒であるため、インターバルが長いと上図のように実行されます。

■アラート発生までの所要時間

理論値: 30 秒 (2+5.2*5+2)

※インターバルを 30 秒に設定した場合

また、ThirdEye には、アラートを発生させるトリガーとして、「レスポンス確認」と「期間」があります。レスポンス確認トリガーでは、「カウント」と「期間」を使用して、「一定期間内に、N回応答がない」場合にアラートを発生させることができます。

[サンプル画像]

トリガー

レスポンス確認

期間: 3 min カウント: 2

ポリシー: Simple Incident Policy 重大度: クリティカル メッセージ: node から応答がありません

※上記の場合は、3 分以内に 2 回応答がない場合にアラートを発生させます。

期間トリガーでは、レスポンス確認トリガーの「カウント」と「期間」に加え、「条件」を使用することができます。「条件」には Ping 応答のパケットのラウンドトリップタイム (RTT) と、パケットロスパーセントを使用することができます。この条件を併用することにより、例えば監視対象からの Ping 応答が返って来ても RTT がユーザの期待する水準に達していないので NG と判定しアラートを発生させるといった監視が可能となります。

[サンプル画像]

Time Window Trigger

条件: roundTripTime > 200 and packetLossPercent > 50

アラートポリシー: Simple Incident Policy 重大度: エラー

期間: 3 min カウント: 2

メッセージ: ノード node が window 内の count 回にトリガー条件を違反しています。