LogicVein

ThirdEye

ユーザーズマニュアル

目次

1. 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 12
1.4 使用ポート一覧 13
2. インストール 14
2.1 インストールする 14
2.1.1 VMware ESXiへのデプロイ 14
2.1.2 Windows Hyper-Vへのデプロイ 16
2.1.3 Linux KVMへのデプロイ 22
2.1.4 Nutanix AHVへのデプロイ 25
2.1.5 Microsoft Azureへのデプロイ 27
2.1.6 AWSへのデプロイ 34
2.1.7 Podmanへのデプロイ 35
2.2 ネットワークを設定する 37
2.3 ライセンスを適用する 40
2.4 初期設定（詳細設定） 41
3. ログイン／ログアウト 42
3.1 ログインする 42
3.2 ログアウトする 42
4. 画面構成 43
4.1 画面の構成と各部の役割 43
4.1.1 メインタブ構成 43
4.1.2 グローバルメニュー構成 44
4.1.3 マップ画面構成 44
5. 基本設定 45
5.1 クレデンシャルを設定する 45
5.1.1 共通のクレデンシャルを設定する 45
5.1.2 機器ごとにクレデンシャルを設定する 48
5.1.3 クラウドアカウントのクレデンシャルを設定する 51
5.1.4 SSH秘密鍵認証 54
5.2 デバイスを追加する 55
5.2.1 1台ずつ登録する 56
5.2.2 ネットワーク上のデバイスを登録する 57
5.2.3 Excelファイルからインポート登録する 60
5.2.4 クラウドアカウントのディスカバリ 62
5.3 監視設定をする 62

Copyright (C) 2026 LogicVein, Inc.

5.3.1 障害を検知した時のアクションを設定する 62
5.3.2 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 73
5.3.3 Ping監視を設定する 76
5.3.4 SNMP情報を収集する 79
5.3.5 しきい値を設定して監視する 81
5.3.6 SNMPトラップを監視する（OID指定） 83
5.3.7 SNMPトラップを監視する（すべて） 86
5.3.8 モニターステータスレポート 88
5.4 マップを設定する 89
5.4.1 マップを作成する 89
5.4.2 マップにデバイスを挿入する 91
5.4.3 トポロジーマップを作成する 94
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 96
5.4.5 オブジェクトのアイコンを設定する 98
5.4.6 2つのオブジェクトの間を線で結ぶ 100
5.4.7 リンク線にインタフェースを紐付ける 102
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 105
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 107
5.4.10 マップの背景画像を設定する 108
5.4.11 マップの階層構造を設定する 110
5.5 ダッシュボードを作成する 112
5.5.1 ダッシュボードを追加する 112
5.5.2 ダッシュボードを切り替える 114
5.5.3 ウィジェットを追加する 115
5.5.4 ダッシュボードを削除する 117
5.5.5 ダッシュボードの編集メニュー 118
5.5.6 ウィジェットの編集メニュー 119
6. 運用操作 120
6.1 障害対応 120
6.1.1 障害が発生しているデバイスを確認する 120
6.1.2 障害内容を確認する 122
6.1.3 障害対応後、インシデントを「解決済み」にする 123
6.2 SNMP で収集したデータを確認する 124
6.2.1 コンソールからグラフを表示する 124
6.2.2 CSVファイルへエクスポートする 126
6.2.3 ダッシュボードレポートを発行する 127
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 127
6.3 デバイスのコンフィギュレーション取得 129

Copyright (C) 2026 LogicVein, Inc.

6.3.1 コンフィグバックアップ前の確認事項 129
6.3.2 バックアップを実行する 130
6.3.3 バックアップ後のステータスについて 131
6.3.4 取得したコンフィグを確認する 132
6.3.5 コンフィグの比較 133
6.3.6 コンフィグへのメモ 133
6.3.7 コンフィグバックアップを無効にする 134
6.4 デバイスに SSH/Telnet 接続をする 136
6.4.1 使用する前の準備 136
6.4.2 ターミナルプロキシを起動する 138
6.4.3 操作ログを確認する 140
6.5 リアルタイムで Ping を実行する 141
6.6 デバイスのインタフェースの Up/Down 状態を確認する 142
6.7 登録されている機器からの SNMP トラップを確認する 144
6.8 受信した Syslog を確認する 145
6.9 監視を一時的に停止する（非監視設定） 147
6.9.1 手動で非監視にする 147
6.9.2 スケジュールで非監視にする 149
6.9.3 非監視のデバイスを検索する 151
6.10 ジョブ管理 152
6.10.1 ジョブの作成 153
6.10.2 ジョブ履歴 156
6.10.3 ジョブ承認機能 156
6.10.4 過去のジョブ履歴を確認する 161
6.11 監視設定を解除する 162
6.11.1 モニターを削除する 162
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 163
6.11.3 マップを削除する 165
6.11.4 デバイスを削除する 166
6.11.5 ジョブを削除する 167
7. 詳細設定 168
7.1 いろいろな監視設定をする 168
7.1.1 Webサイトを監視する 168
7.1.2 TCPポートを監視する 170
7.1.3 計算式を使用した監視をする 172
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 175
7.1.5 トラップに含まれる値でアクションを変える 176
7.1.6 Agent-Dを使用したサーバ監視をする 180

Copyright (C) 2026 LogicVein, Inc.

7.1.7 WMIを使用したサーバ監視をする 226
7.1.8 ワイヤレスLANコントローラの監視 236
7.1.9 Aruba Access Pointの監視 240
7.1.10 MIBをコンパイルする 241
7.2 デバイスの EOS/EOL 管理 242
7.2.1 手動設定 242
7.2.2 自動設定 Suite 244
7.2.3 レポートによる通知 247
7.2.4 コンプライアンスの概要 Suite 250
7.3 ドラフトコンフィギュレーション Suite 275
7.3.1 ドラフトコンフィギュレーションの作成 275
7.3.2 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 277
7.3.3 ドラフトをエクスポートする 277
7.3.4 ドラフトを削除する 277
7.3.5 ドラフト同士の比較 278
7.3.6 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 278
7.4 チェンジアドバイザ Suite 279
7.4.1 チェンジアドバイザを用いてコマンドを実行する 280
7.5 閲覧ツール 281
7.5.1 DNSルックアップ 281
7.5.2 IOS Showコマンド 282
7.5.3 IP ルーティングテーブル 282
7.5.4 Ping 282
7.5.5 SNMPシステム情報 283
7.5.6 インタフェース概要 283
7.5.7 トレースルート 283
7.5.8 ポートマップ 283
7.5.9 ライブのARPテーブル 283
7.6 変更ツール Suite 284
7.6.1 MOTDバナーの設定 284
7.6.2 NTPサーバ 285
7.6.3 SNMPコミュニティストリング 285
7.6.4 SNMPトラップホスト 285
7.6.5 Syslogホスト 285
7.6.6 VLANのポート割当て 286
7.6.7 インタフェース設定 286
7.6.8 コマンドランナー 287
7.6.9 Allied Telesis OSソフトウェア配布 288

Copyright (C) 2026 LogicVein, Inc.

7.6.10 ASA OSソフトウェア配布 288
7.6.11 IOSソフトウェア配布 289
7.6.12 JUNOS OSソフトウェア配布 290
7.6.13 NEC WAソフトウェア配布 290
7.6.14 OSイメージ 291
7.6.15 OSイメージファイルの取得 291
7.6.16 Yamaha RT ファームウェアの配布 292
7.6.17 スタティックルートの追加 293
7.6.18 スタティックルートの削除 293
7.6.19 Enable Passwordの変更 293
7.6.20 VTY Passwordの変更 294
7.6.21 ユーザアカウントの削除 294
7.6.22 ユーザアカウントの追加 294
7.6.23 ローカルユーザパスワードの変更 294
7.7 Playbook Suite 295
7.7.1 Playbookの概要 295
7.7.2 Playbookノード 295
7.7.3 Playbookの管理 302
7.7.4 Playbookの実行 312
7.7.5 バルクチェンジの概要 Suite 321
7.8 ユーザを登録する 327
7.8.1 権限を追加する 327
7.8.2 ユーザを追加する 332
7.8.3 ユーザ情報を変更する 334
7.8.4 ログイン中のユーザのパスワードを変更する 335
7.9 二要素認証（2FA）を設定する 336
7.9.1 二要素認証を有効にする 336
7.9.2 二要素認証を解除する 337
7.9.3 外部認証を構成する 338
7.9.4 ユーザのセッションタイムアウトを設定する 350
7.9.5 データ保存期間を変更する 353
7.9.6 メールサーバを設定する 354
7.9.7 SNMPトラップ送信を設定する 356
7.9.8 カスタムデバイスフィールドのカラム名変更/カラム追加 364
7.9.9 ホスト名にsysNameを使用する 366
7.9.10 Syslogファイルの詳細設定 367
7.9.11 メモテンプレートを編集する 373
7.9.12 右クリックメニューに特定のURLを追加する 374

Copyright (C) 2026 LogicVein, Inc.

7.9.13 デバイスグループを使用する 376
7.9.14 ライセンスを更新する 378
7.9.15 オンラインでアップデートをする 379
7.9.16 リビジョンを確認する 380
7.9.17 プロキシサーバを使用する 381
7.9.18 Zero-Touch (オプション) 382
8. 冗長機能 394
8.1 概要 394
8.1.1 利用条件 394
8.1.2 制限される機能 394
8.2 設定 395
8.2.1 手順 395
8.2.2 ステータスの確認 398
8.2.3 再設定が必要ケース 398
8.3 フェイルオーバー 399
8.3.1 手動フェイルオーバー 399
8.3.2 自動フェイルオーバー 400
9. システムバックアップ／復元 401
9.1 自動でシステムバックアップを実行する 401
9.2 手動でシステムバックアップを実行する 402
9.3 システムバックアップの保有数を変更する 403
9.4 外部ストレージに保存する 404
9.5 システムバックアップを ZIP ファイルにする 406
9.6 システムバックアップを復元する 406
10. 再起動／シャットダウン 409
11. アンインストール 410
11.1 アンインストールする 410
12. お問い合わせ 411
13. 巻末資料 412
13.1 ICMP ポーリングについて 412
13.2 スマートブリッジ（オプション) 415
13.2.1 スマートブリッジのインストール 415
13.2.2 スマートブリッジをコアサーバに登録する 416
13.2.3 スマートブリッジ側の設定 416
13.2.4 スマートブリッジ経由でのデバイス管理 417
13.3 マルチテナント環境における管理ネットワーク制限 418

Copyright (C) 2026 LogicVein, Inc.

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 2 版	2023 年 8 月 30 日	機能追加による変更
第 3 版	2024 年 2 月 29 日	Basic の記載を削除、システムバックアップの仕様を変更
第 4 版	2024 年 3 月 15 日	機能追加による変更（クレデンシャル項目）、メールの宛先に関する記載を変更
第 5 版	2024 年 4 月 8 日	デプロイ方法に、Linux KVM / Nutanix AHV / AWS / Microsoft Azure を追加
第 6 版	2024 年 11 月 27 日	新機能を追加し、操作手順を追記
第 7 版	2024 年 12 月 25 日	新機能を追加（Allied Telesis/JUNOS OS 配布）
第 8 版	2025 年 1 月 30 日	新機能を追加（冗長機能、Playbook）
第 9 版	2025 年 3 月 28 日	新機能を追加（WLC モニター）
第 10 版	2025 年 4 月 18 日	新機能を追加（SAML 認証に keycloak の手順を追加）
第 11 版	2025 年 5 月 27 日	新機能を追加（LINE WORKS、Playbook ノード）
第 12 版	2025 年 7 月 24 日	新機能を追加（クラウドアカウント、WMI プロセス監視）
第 13 版	2025 年 8 月 27 日	新機能を追加（WMI サービス監視、Playbook ノード、ウェブフックのテンプレートに PagerDuty を追加）
第 14 版	2025 年 10 月 1 日	デプロイ手順に Podman を追加、新機能追加に伴い画像の変更（Playbook）
第 15 版	2025 年 10 月 7 日	機能追加による変更（SNMP トラップのディスカバリ）
第 16 版	2025 年 11 月 4 日	機能追加による変更（クラウドアカウント、SNMP トラップのディスカバリ、モニターステータスレポート）
第 17 版	2025 年 12 月 5 日	Playbook の承認機能追加、履歴表示画面の構成変更に伴い説明を更新
第 18 版	2026 年 4 月 24 日	新機能を追加（SSH 秘密鍵認証、Playbook ノード（フィールド編集)）
第 19 版	2026 年 5 月 27 日	新機能を追加（Google Chat）
第 20 版	2026 年 6 月 25 日	Playbook のノード構成変更に伴い説明を更新
第 21 版	2026 年 9 月 1 日	新機能を追加（Playbook ノード（Python スクリプト実行)）

Copyright (C) 2026 LogicVein, Inc.

1. 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

Copyright (C) 2026 LogicVein, Inc.

1.2　ThirdEye のエディションについて

ThirdEye には、「Suite」と「Enterprise」の 2 つのエディションがあります。使用できる機能はエディションによって異なります。エディションごとの機能の違いについては、下記の【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、本書で説明するすべての機能は、最上位エディションである「Suite」に基づいており、一部の機能は「Enterprise」では使用できない場合があります。特定のエディションでのみ使用できる機能には、各説明項目のタイトルに Enterprise / Suite のようなアイコンが表示されています。

【アイコンの種類】

- 2 エディション共通で使用可能 … 共 通 または アイコンなし
- Enterprise で使用可能 … Enterprise
- Suite で使用可能 … Suite

【エディションによる主な機能比較表】

機能		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	○	○
	PostgreSQL	○	○
	MySQL/MariaDB	○	○
	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	○	○
	ウェブフック(Mattermost / Slack / Teams/LINE WORKS/PagerDuty/Google Chat)	○	○
	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	○	○

Copyright (C) 2026 LogicVein, Inc.

機能		Enterprise	Suite
	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	○	○
	共有	○	○
	ウィジェット	○	○
	レポート	○	○
インシデント		○	○
EoL/EoS 管理	自動収集	×	○
	手動	○	○
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）		×	○

Copyright (C) 2026 LogicVein, Inc.

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
- Nutanix AHV
- Linux KVM
- Microsoft Azure

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: 2.5 GB HDD2: 50 GB 以上	HDD1: 2.5 GB HDD2: 50 GB	HDD1: 2.5 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。

■ブラウザ

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

Copyright (C) 2026 LogicVein, Inc.

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、必要なポートを解放してください。また、一部のプロトコルにおいて監視画面やプロトコル設定で使用するポート番号をユーザが変更することができます。変更した場合は、そのポートを開け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
データベース監視	PostgreSQL	5432	TCP	ThirdEye（→）送信先
	MySQL	3306	TCP	ThirdEye（→）送信先
WMI 監視	HTTP HTTPS	5985、 5986	TCP	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

Copyright (C) 2026 LogicVein, Inc.

2. インストール

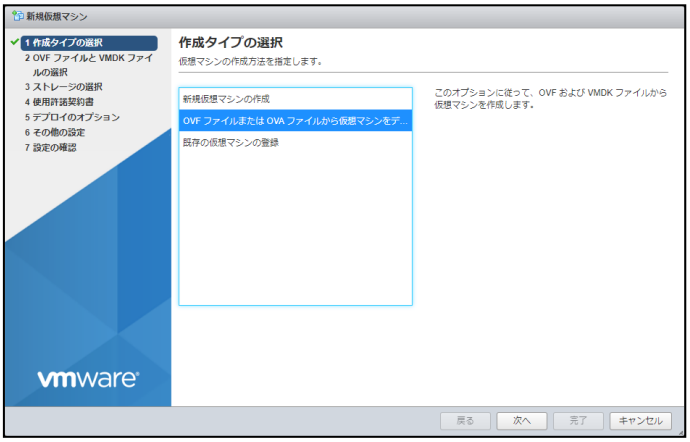
2.1 インストールする

2.1.1 VMware ESXi へのデプロイ

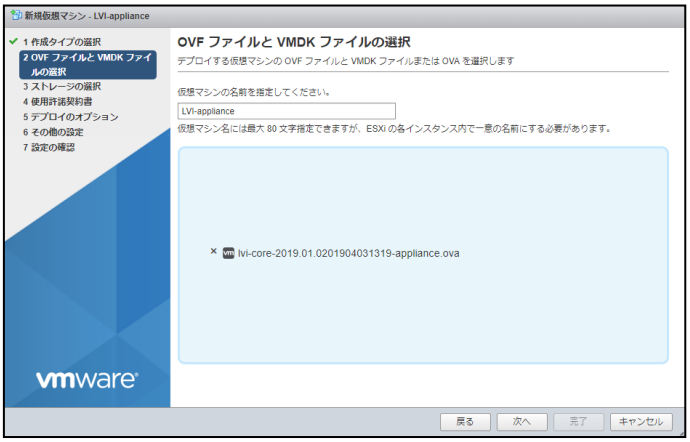
VMware ESXi へのデプロイ手順について説明します。ここでは ESXi 6.5 を使用した場合を例に説明します。

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。

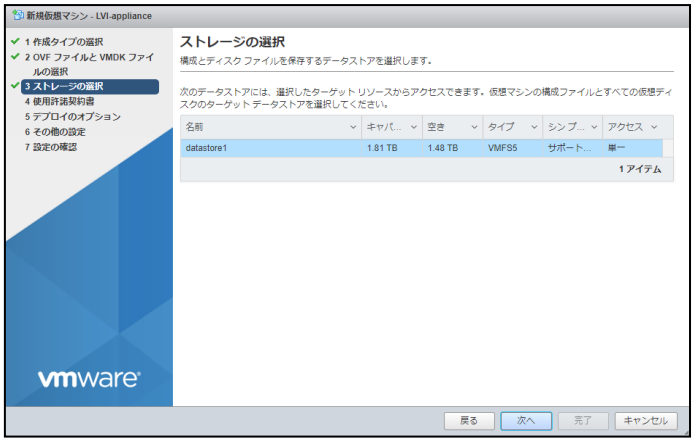


3. 任意の仮想マシン名を入力後、OVA ファイルをドラッグ・アンド・ドロップし、「次へ」をクリックします。

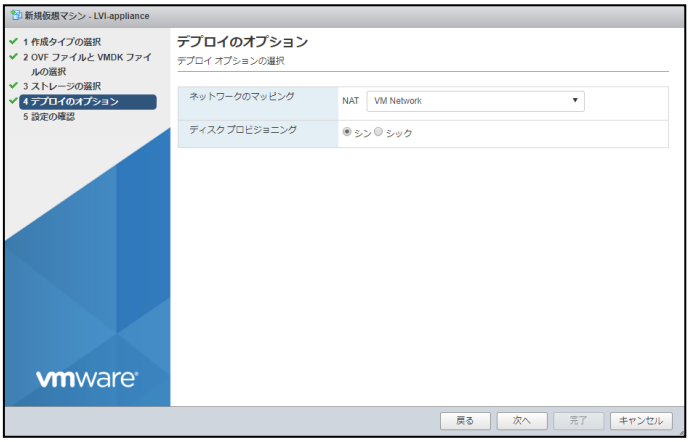


Copyright (C) 2026 LogicVein, Inc.

4. ストレージを選択し「次へ」をクリックします。



5. デプロイ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。



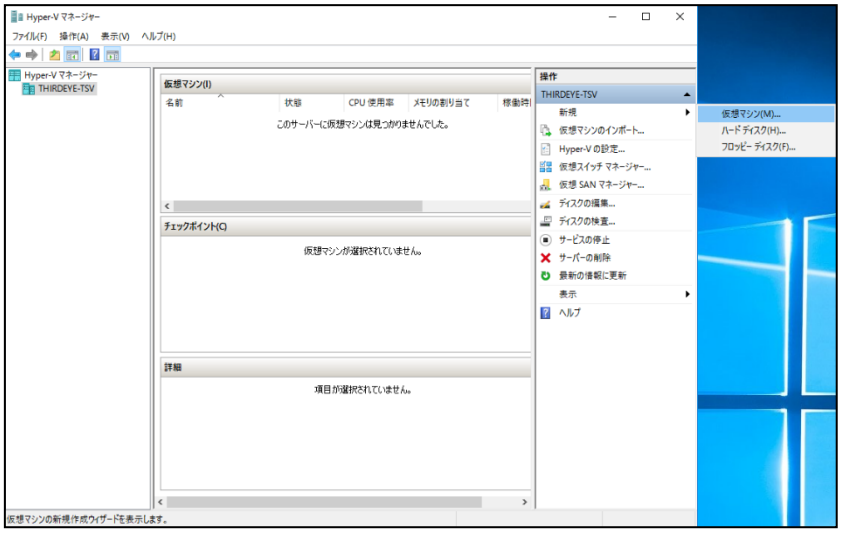
6. 「完了」をクリックします。

Copyright (C) 2026 LogicVein, Inc.

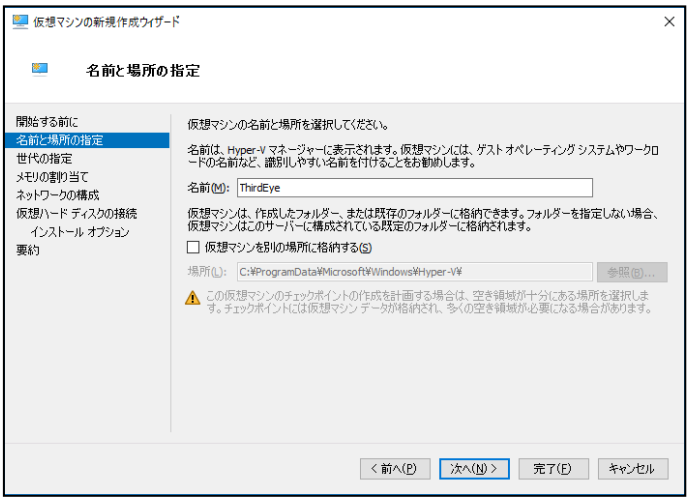
2.1.2　Windows Hyper-V へのデプロイ

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。

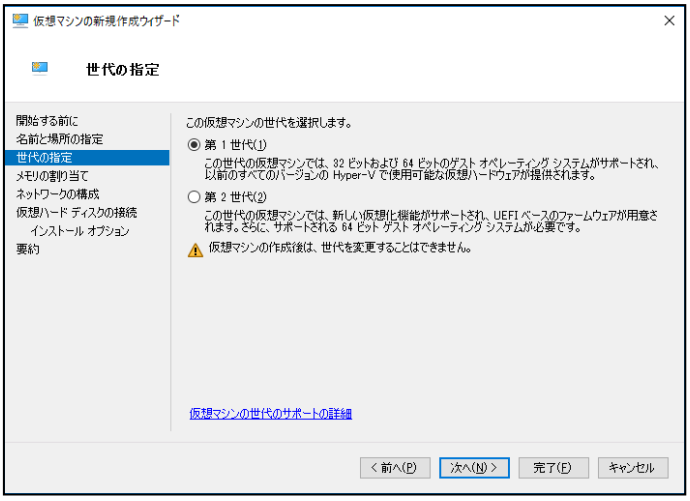


2. 仮想マシンの名前を入力し、「次へ」をクリックします。

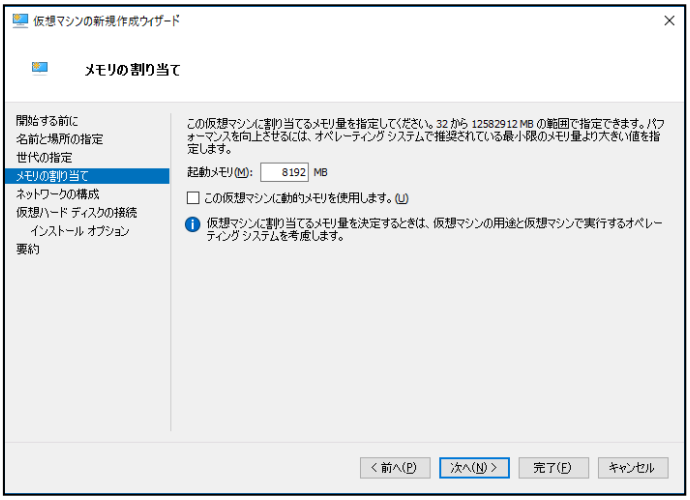


Copyright (C) 2026 LogicVein, Inc.

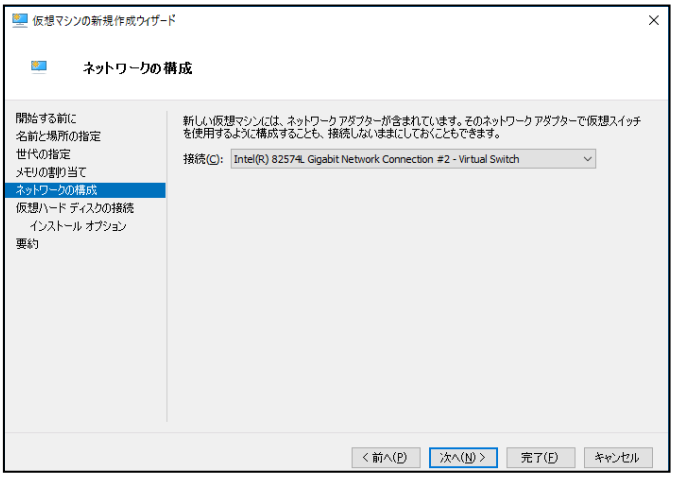
3. 「第 1 世代」を選択し、「次へ」をクリックします。



4. 起動メモリを設定し、「次へ」をクリックします。



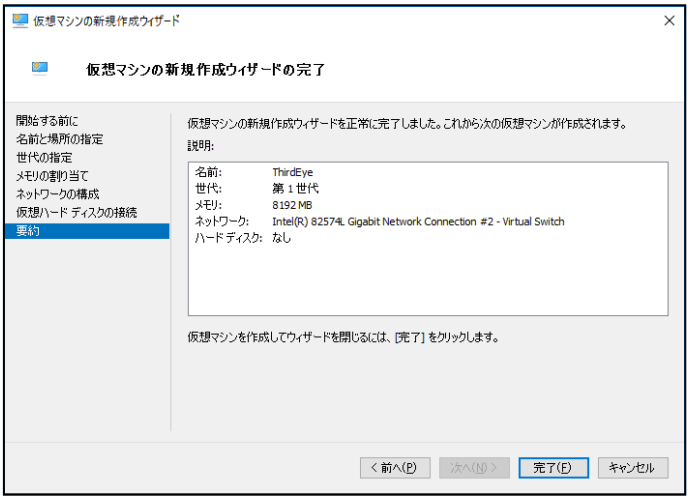
5. 接続先に使用する仮想スイッチを選択し、「次へ」をクリックします。



Copyright (C) 2026 LogicVein, Inc.

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。

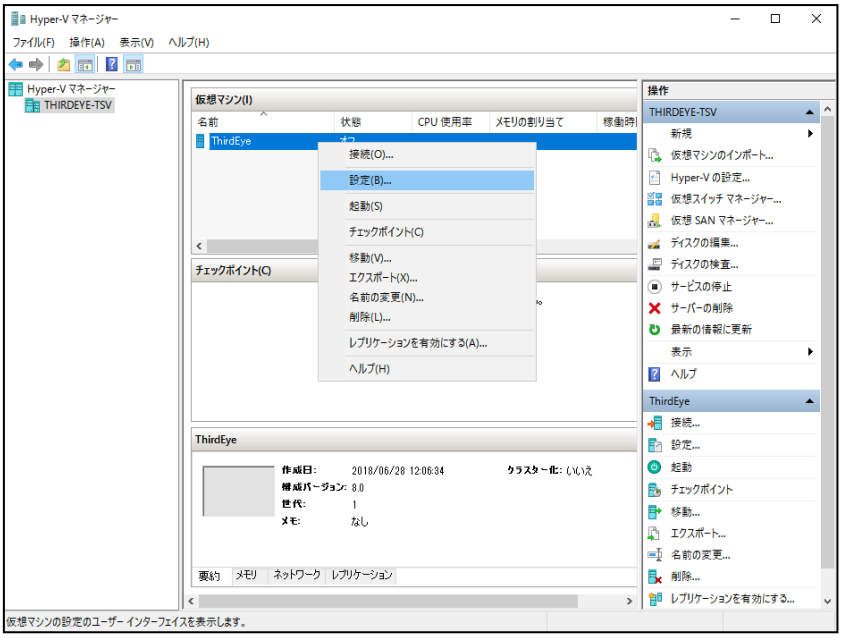
7. 「完了」をクリックします。



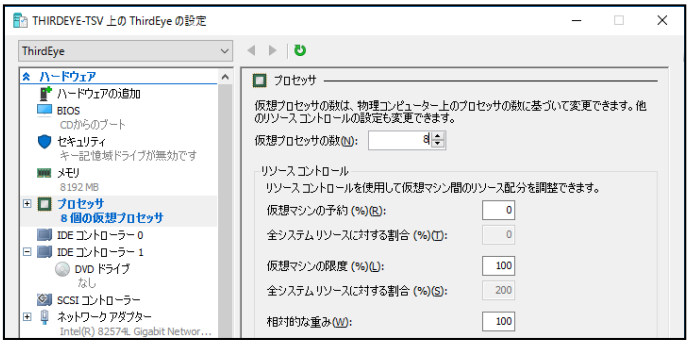
8. 以上で仮想マシンが作成されます。
9. 続いて、2 つの VHDX ファイルを作成した仮想マシンに割り当てます。

Copyright (C) 2026 LogicVein, Inc.

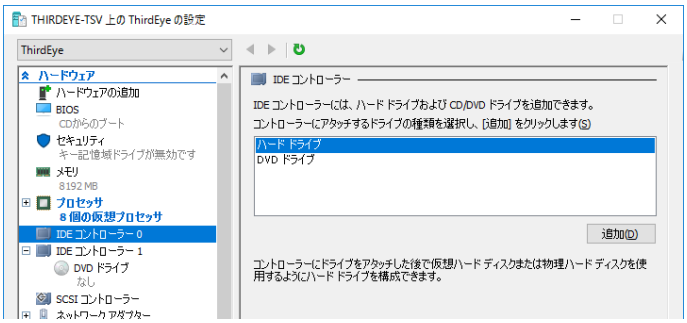
10. 作成した仮想マシンを右クリックし、「設定」をクリックします。



11. 「プロセッサ」を選択し、「仮想プロセッサ数」を変更します。

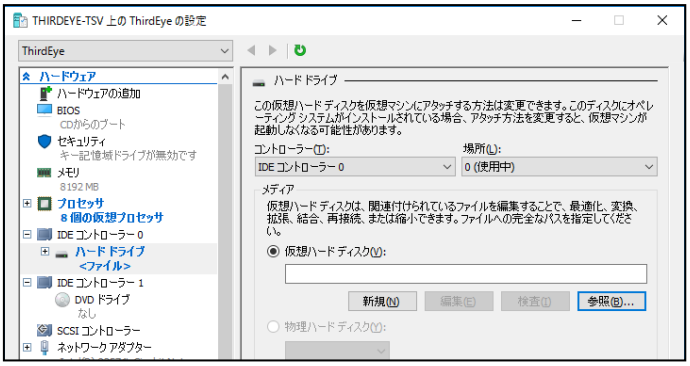


12. 「IDE コントローラー 0」を選択し、「追加」をクリックします。

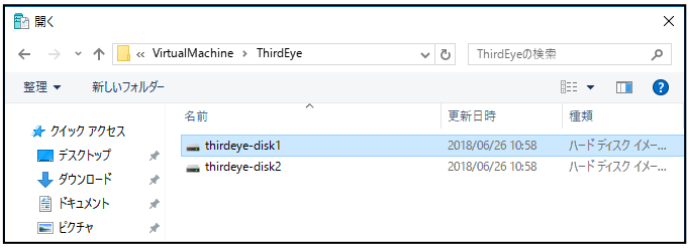


Copyright (C) 2026 LogicVein, Inc.

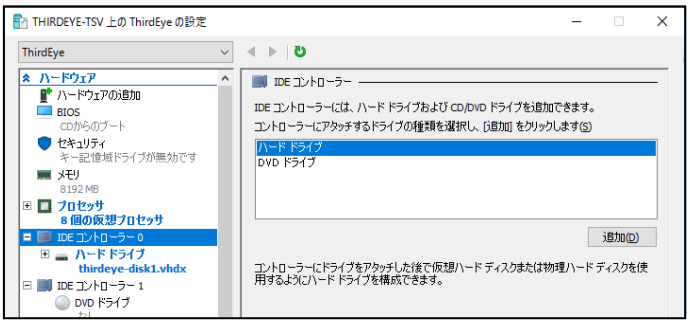
13. 「参照」をクリックします。



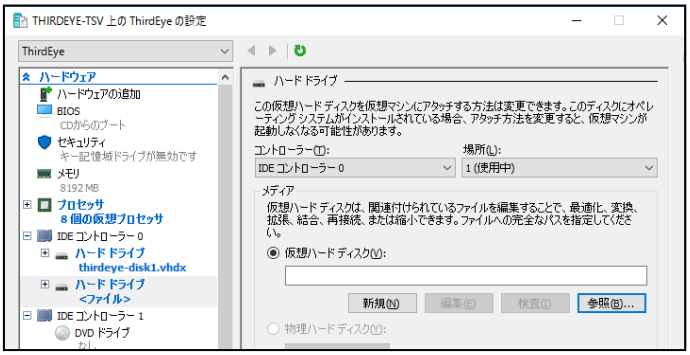
14. 「disk1」を追加し、「OK」をクリックします。



15. 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。

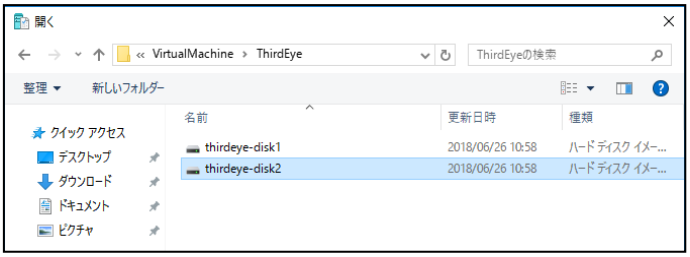


16. 「参照」をクリックします。

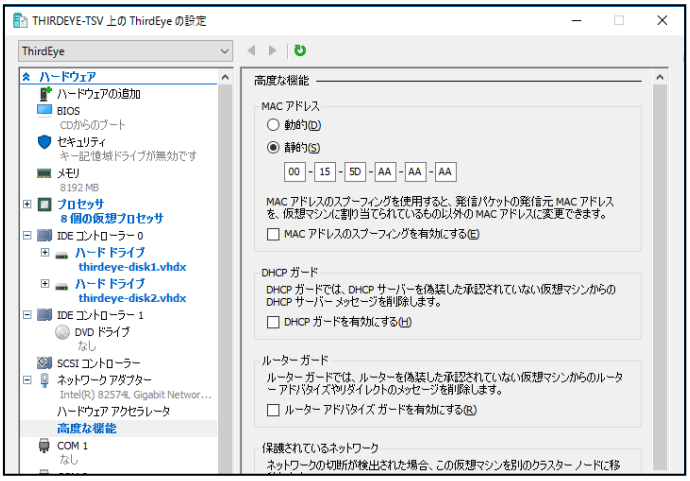


Copyright (C) 2026 LogicVein, Inc.

17. 「disk2」を追加し、「OK」をクリックします。



18. 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。



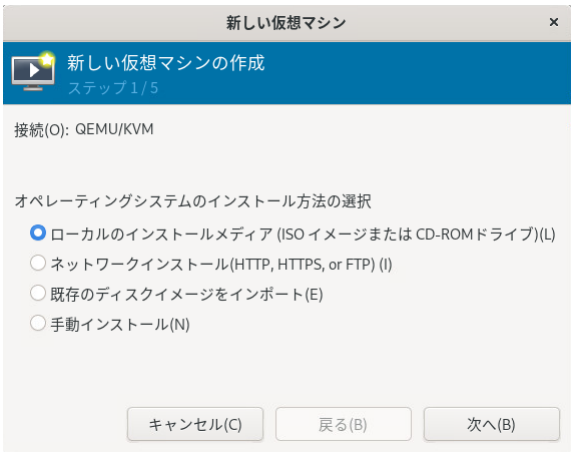
補足	本製品のライセンスは MAC アドレスで管理されています。仮想マシンに割り当てられた MAC アドレスが変更されないように、MAC アドレスを「静的」に設定することをおすすめします。

Copyright (C) 2026 LogicVein, Inc.

2.1.3 Linux KVM へのデプロイ

Linux KVM へのデプロイ手順について説明します。KVM にデプロイする場合は「qcow2」ファイルを使用します。KVM へのデプロイは CLI を使用して行うこともできますが、ThirdEye の IP アドレスなどの設定は GUI から行う必要があります。ここでは、GUI を使用してデプロイする方法について説明します。

1. 任意のディレクトリに qcow2 ファイルを保存します。（例：/var/lib/libvirt/images）
2. 「仮想マシンマネージャー」を起動します。
3. ファイルメニューから「新しい仮想マシン」をクリックします。
4. 「既存のディスクイメージをインポート」を選択し、「次へ」をクリックします。

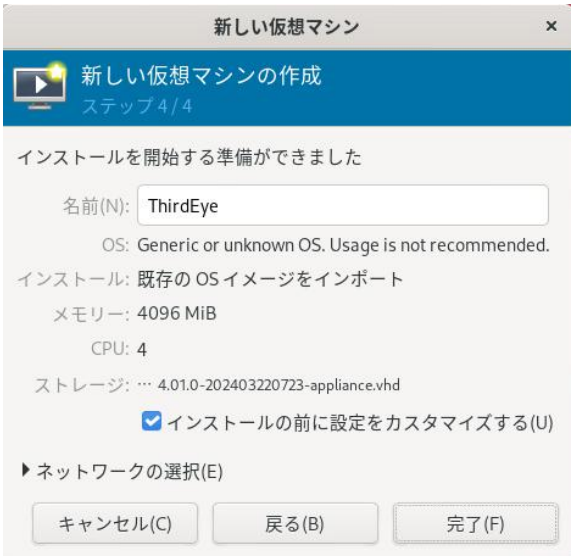


5. 「既存のストレージのパスを指定してください」にアップロードしたファイルを指定します。

6. 「インストールするオペレーティングシステムの選択」で「Generic or unknown OS」を選択し、「次へ」をクリックします。
7. 割り当てるリソースを入力し、「次へ」をクリックします。

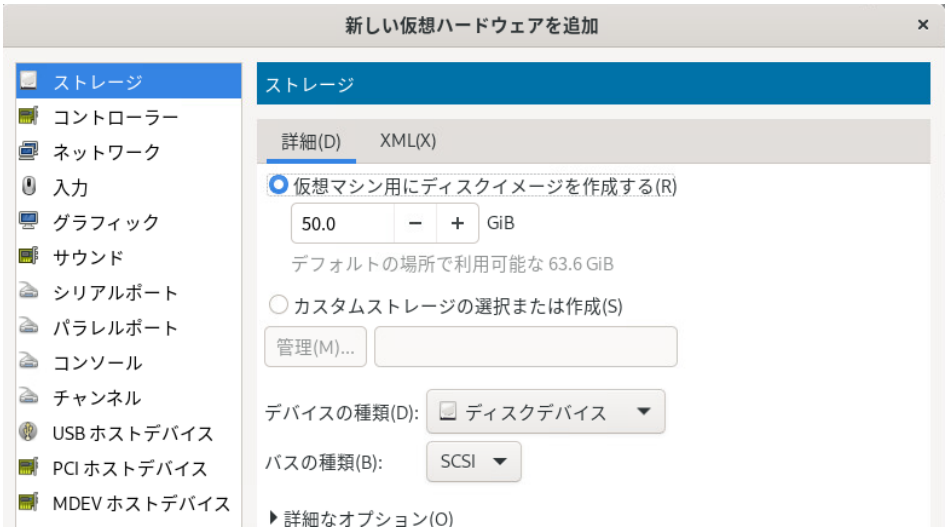
Copyright (C) 2026 LogicVein, Inc.

8. 仮想マシンの名前を入力し、「インストールの前に設定をカスタマイズする」にチェック入れます。



9. ネットワークの選択を開き、ネットワーク環境に合わせたデバイスを選択し、「完了」をクリックします。
10. 「IDE ディスク 1」をクリックし、ディスクバスを「SCSI」に変更します。

11. 「ハードウェアの追加」をクリックし、50GB 以上のストレージを追加します。



Copyright (C) 2026 LogicVein, Inc.

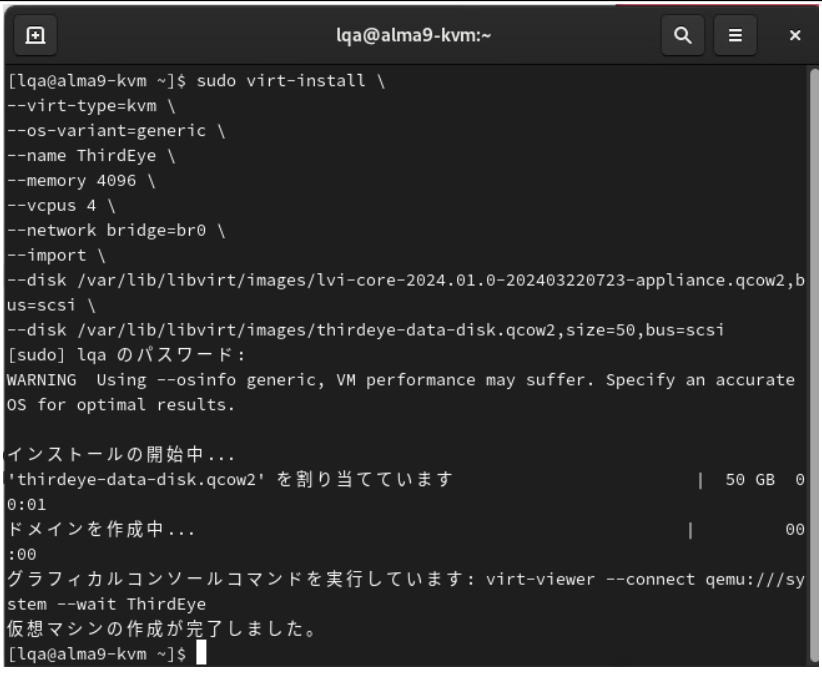
12. 「インストールの開始」をクリックします。

以上で、KVM へのデプロイは完了です。

2.1.3.1 CLI でデプロイするときのコマンド例

以下は、CLI を使用してデプロイする時のコマンドの例です。以下のコマンドは、AlmaLinux 9.3 および Virtual Machine Manager4.1.0 を使用しています。バージョンによって、オプションの指定方法が異なる可能性があります。

```
sudo virt-install --virt-type=kvm --os-variant=generic ¥
--name ThirdEye --memory 4096 --vcpus 4 --network bridge=br0 ¥
--import ¥
--disk /var/lib/libvirt/images/lvi-core-2024.01.0-202403220723-appliance.qcow2,bus=scsi ¥
--disk /var/lib/libvirt/images/thirdeye-data-disk.qcow2,size=50,bus=scsi
```



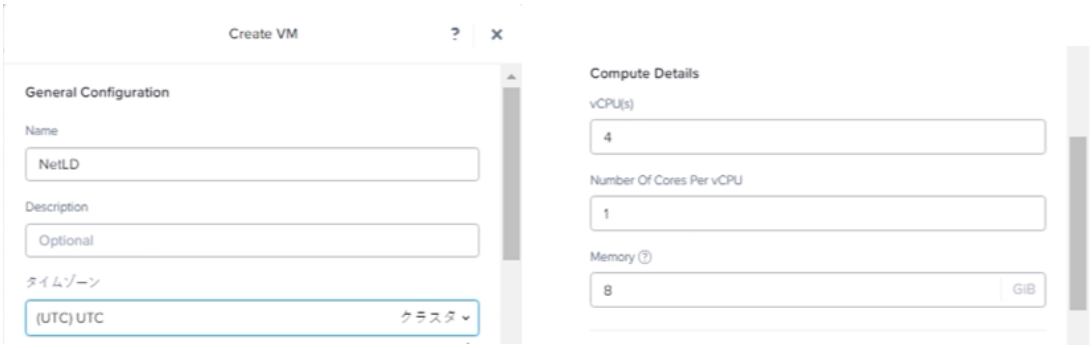
Copyright (C) 2026 LogicVein, Inc.

2.1.4 Nutanix AHV へのデプロイ

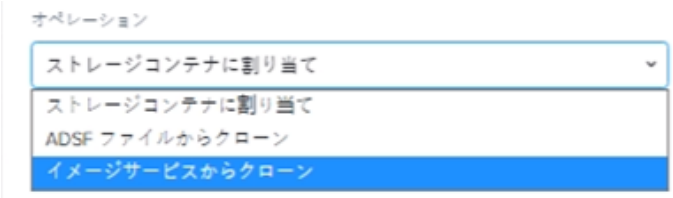
Nutanix AHV へのデプロイ手順について説明します。Nutanix AHV へのデプロイは「qcow2」ファイルを使用します。　ここではバージョン 6.5.3.6LTS を使用した場合を例に説明します。

1. Nutanix Prism にログインし、画面上部のプルダウンメニューから「設定」に移動します。
2. 左のメニューから「イメージ設定」をクリックします。
3. 「イメージをアップロード」をクリックします。

4. 「Name」と「Storage Container」を入力します。
5. 「Upload a file」に qcow2 ファイルを指定し、「Save」をクリックします。
6. アップロード完了後、画面上部のプルダウンメニューから「仮想マシン」に移動します。
7. 「仮想マシンを作成」をクリックします。
8. 任意の VM 名と割り当てるリソースを入力します。



9. 「Add New Disk」をクリックします。
10. Operation プルダウンから「イメージサービスからクローン」を選択します。

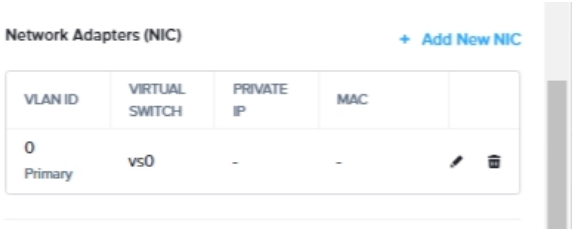


Copyright (C) 2026 LogicVein, Inc.

11. Image プルダウンから作成したイメージを選択し、追加します。

12. 再度「Add New Disk」をクリックします。
13. サイズを 50GB 以上に設定し、追加します。

14. 「Add New NIC」から、NIC を追加します。



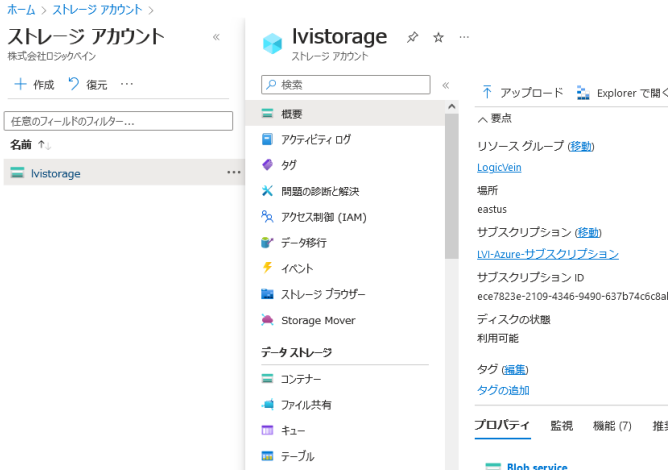
15. 「Save」をクリックします。
16. 仮想マシンが作成された後、パワーオンします。

Copyright (C) 2026 LogicVein, Inc.

2.1.5 Microsoft Azure へのデプロイ

Microsoft Azure へのデプロイ手順について説明します。Azure へのデプロイには、「VHD」ファイルを使用します。

1. Azure にログインし、「ストレージアカウント」サービスに移動します。
2. 既存のストレージアカウントをクリック、または「作成」からストレージアカウントを作成します。
3. ストレージアカウントメニュー内の、「データストレージ」->「コンテナー」をクリックします。



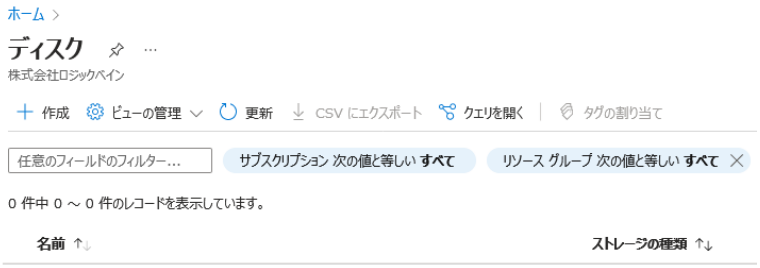
4. 既存のコンテナーをクリック、または「コンテナー」からコンテナーを作成します。
5. 「アップロード」をクリックします。

6. ダウンロードした VHD ファイルを選択します。
7. 「詳細設定」を開き、BLOB の種類を「ページ BLOB」に変更します。

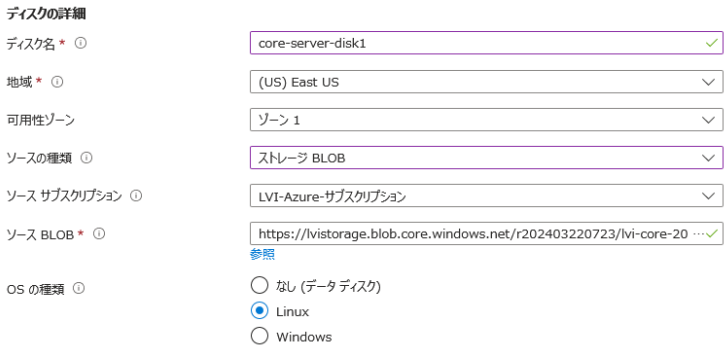
8. 「アップロード」をクリックします。
9. アップロード完了後、「ディスク」サービスに移動します。

Copyright (C) 2026 LogicVein, Inc.

10. 「作成」をクリックします。



11. サブスクリプション、リソースグループ、地域を選択します。
12. ディスク名を入力します。
13. ソースの種類を「ストレージ BLOB」に変更し、ソース BLOB をアップロードしたファイルを選択します。

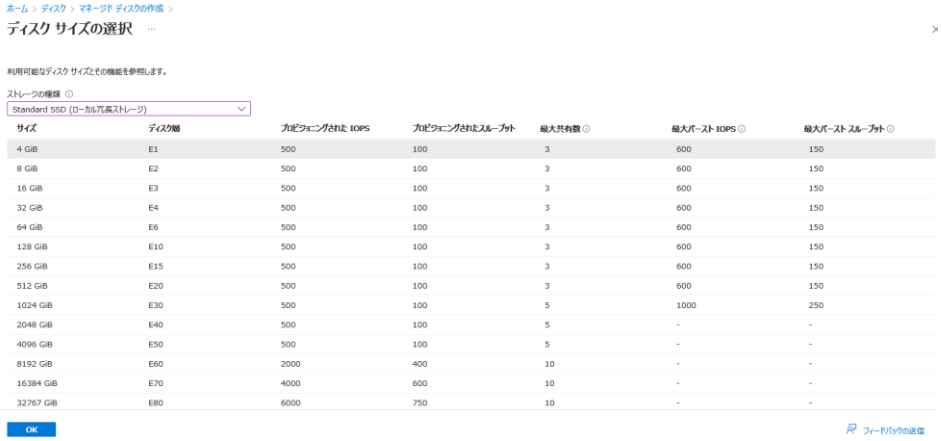


14. OS の種類を「Linux」に変更します。
15. サイズ項目で、サイズの変更をクリックします。

16. 環境にあった「ストレージの種類」を選択します。（SSD を推奨）

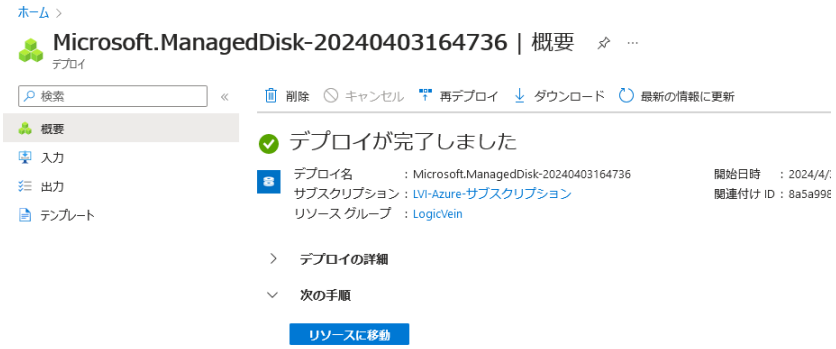
Copyright (C) 2026 LogicVein, Inc.

17. 一番上の 4GB を選択し、「OK」をクリックします。



18. 「確認および作成」をクリックします。
19. 内容を確認し、「作成」をクリックします。

20. 作成完了後、「リソースに移動」をクリックします。



21. 「VM の作成」をクリックします。

Copyright (C) 2026 LogicVein, Inc.

22. 仮想マシン名を入力します。
23. サイズで仮想マシンに割り当てるリソースを選択します。

24. 「ディスク」タブに移動します。
25. データディスク項目で「新しいディスクを作成し接続する」をクリックします。
26. サイズ項目で、サイズの変更をクリックします。
27. 環境にあった「ストレージの種類」を選択します。（SSD を推奨）

Copyright (C) 2026 LogicVein, Inc.

28. 64GB 以上のディスクを選択し、データディスクを追加します。

29. ホストキャッシュが「読み取り/書き込み」になっていることを確認します。

30. 「ネットワーク」タブに移動し、Azure 環境に合わせてネットワークを設定します。

31. 「確認および作成」をクリックします。

Copyright (C) 2026 LogicVein, Inc.

32. 内容を確認し、「作成」をクリックします。

以上で、Azure 上へのデプロイは完了です。

※既存の ThirdEye 環境を Azure 環境に移行する場合、既存の ThirdEye 環境でシステムバックアップを取得し、AWS 環境へ復元する事を推奨します。

Copyright (C) 2026 LogicVein, Inc.

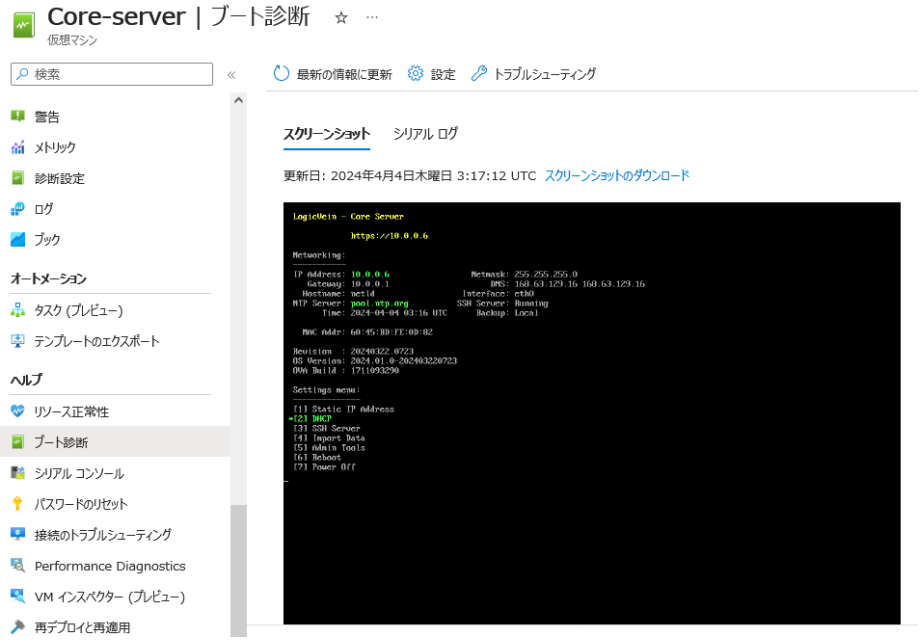
2.1.5.1　受信ポートルールの作成

Azure 上に作成された仮想マシンはデフォルトで外部からのアクセスが制限されています。そのため、画面にアクセスするためのポート（443）や監視/管理に必要なポートなどを別途設定する必要があります。ルールの作成は、ネットワーク設定メニュー内のルールセクションで作成します。

使用するポートについては、「1.4 使用ポート一覧」を参照し、必要なポートを設定してください。

2.1.5.2　MAC アドレスの確認方法

MAC アドレスの確認等は[ヘルプ]→[ブート診断]のスクリーンショットから可能です。



Copyright (C) 2026 LogicVein, Inc.

2.1.6 AWS へのデプロイ

AWS へのデプロイ手順について説明します。AWS へのデプロイは、AWS 上のコミュニティ AMI から AMI を選択し、インスタンスを作成します。

1. AWS EC2 にログインし、「インスタンスを起動」をクリックします。
2. 名前を設定し、必要に応じてタグを設定します。
3. アプリケーションおよび OS イメージで、「その他の AMI を閲覧する」をクリックします。
4. コミュニティ AMI を選択し、検索欄に「lvi-core」を入力し検索を実行します。

5. インスタンスタイプでサイジングガイドラインに従いタイプを選択します。

※メモリが 4GB 以下の場合、正常に動作しません。システム要件については、以下を参照してください。

- netLD: https://www.lvi.co.jp/NetLD/
- ThirdEye: https://www.lvi.co.jp/ThirdEye_system/

6. キーペア（ログイン）でキーペアを作成後、キーペアのダウンロードをクリックして下さい。
7. ネットワーク設定でグループを割り当てます。ここでは既存のセキュリティグループを選択、もしくは新しいセキュリティグループを追加する事が出来ます。

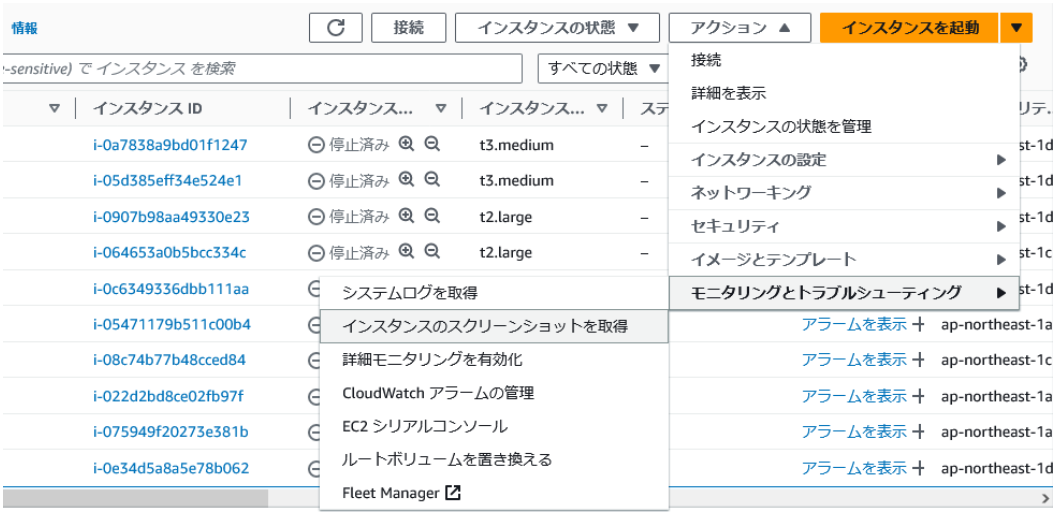
※セキュリティ設定については、「1.4 使用ポート一覧」を参照し使用するポートを設定してください。

8. ストレージを設定で新しいボリュームの追加をクリックし、50GB 以上にサイズを設定します。
9. 設定後、「インスタンスを起動」をクリックします。

Copyright (C) 2026 LogicVein, Inc.

2.1.6.1 MAC アドレスの確認方法

MAC アドレスなどは、［アクション］→［モニタリングとトラブルシューティング］→［インスタンスのスクリーンショットを取得］から確認できます。



※既存の ThirdEye 環境を AWS 環境に移行する場合、既存の ThirdEye 環境でシステムバックアップを取得し、AWS 環境へ復元する事を推奨します。

2.1.7 Podman へのデプロイ

Podman は、コンテナー化されたアプリケーションのデプロイと管理を目的として設計されたコンテナー化ツールであり、Docker の代替手段として機能します。ThirdEye は Podman コンテナーインフラストラクチャ上にデプロイできます。

2.1.7.1 Podman の機能

- セキュリティ機能: daemon を必要とせず、隔離された環境でコンテナーを実行する事が可能です。
- rootless 機能: root 権限なしでコンテナーの実行をサポートします。（ただし、低ポートバインディングなどの一部の操作には sudo が必要となる場合があります。）
- Docker 互換性: Docker と同様のコマンド構造を使用します。例えば docker run の変わりに podman run を使用します。

  例: docker を podman に置き換えた場合:

  docker pull harbor.logicvein.com/lvi/lvi-netld-core:2025.07.0-202508260025

2.1.7.2 Podman デプロイ

Podman/Docker ビルドは、LogicVein の Harbor インスタンスに公開されます。バックグラウンドで Docker コンテナ実行するには、オプション「--detach」を追加します。

Copyright (C) 2026 LogicVein, Inc.

実行例:

```
Podman run ¥
  --detach ¥
  --name thirdeyetest ¥
  --env LICENSE_SERIAL=<SERIALNUM> ¥
  --env JAVA_OPTIONS="-DNAT_RETURN_ADDRESS=<HOST-IPADDR>" ¥
  --ulimit nofile=8192:8192 ¥
  --ulimit nproc=128294:128294 ¥
  --pids-limit=-1 ¥
  --memory=8g ¥
  --cpus=4.0 ¥
  --sysctl net.ipv4.ping_group_range="0 9999" ¥
  --volume <DATA-DIR> ¥
  --publish 20:20 ¥
  --publish 21:21 ¥
  --publish 67:67/udp ¥
  --publish 69:69/udp ¥
  --publish 162:162/udp ¥
  --publish 162:162/tcp ¥
  --publish 443:443 ¥
  --publish 2222:2222 ¥
  --publish 50000-50031:50000-50031 ¥
  --cap-add=NET_RAW ¥
  --cap-add=NET_ADMIN ¥
  harbor.logicvein.com/lvi/lvi-netld-core: 2025.07.0-202508260025
```

SELinux が有効なシステム（例：RedHat）では、Docker / Podman を”sudo podman run”で実行できます。これにより、このコンテナー専用のディレクトリに対して SELinux コンテキストが設定されます。または、次のコマンドを使用して手動で SELinux コンテキストを設定することもできます。

例：

sudo semanage fcontext -a -t container_file_t "/home/lvi/data2(/.)?"*

sudo restorecon -Rv /home/lvi/data2/

これにより、このディレクトリの SELinux コンテキストが設定され、あらゆるコンテナーがこのフォルダにアクセスできるようになります。

例：

drwxr-xr-x. 2 lvi lvi unconfined_u:object_r:container_file_t:s0 6 Mar 26 19:37 /home/lvi/data2/

補足	上記のコマンドには、ユーザーが入力する必要がある値が 3 つあります。 ・<SERIALNUM>: ライセンスのシリアル番号で、適用されるシリアル番号と必ず

Copyright (C) 2026 LogicVein, Inc.

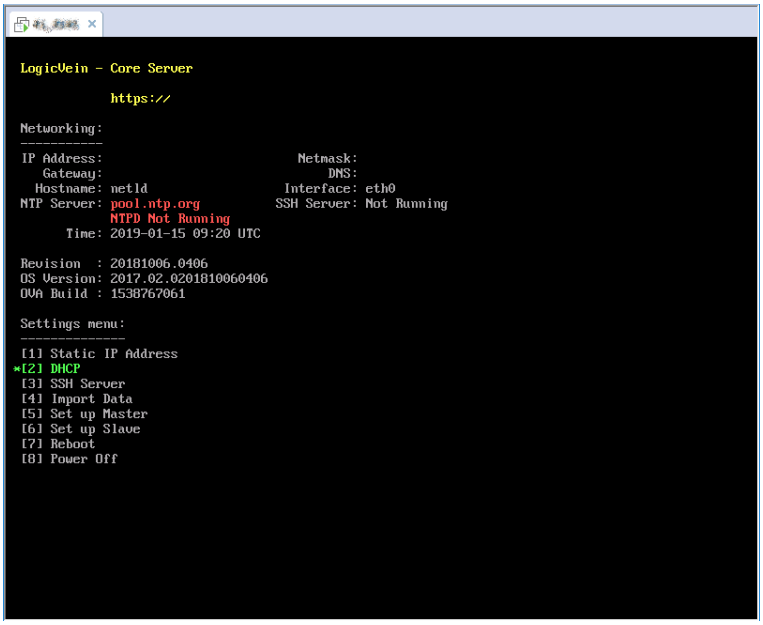
	一致させる必要があります。 ・<DATA-DIR>: データが保存されるローカルディレクトリです。通常、OVA 形式のアプライアンスに接続されるデータディスクに相当します。 このディレクトリは存在する必要があります。自動的に作成されません。 ・<HOST-IPADDR>:　FTP/TFTP/Agent-D のリターンアドレスを指定します。

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。

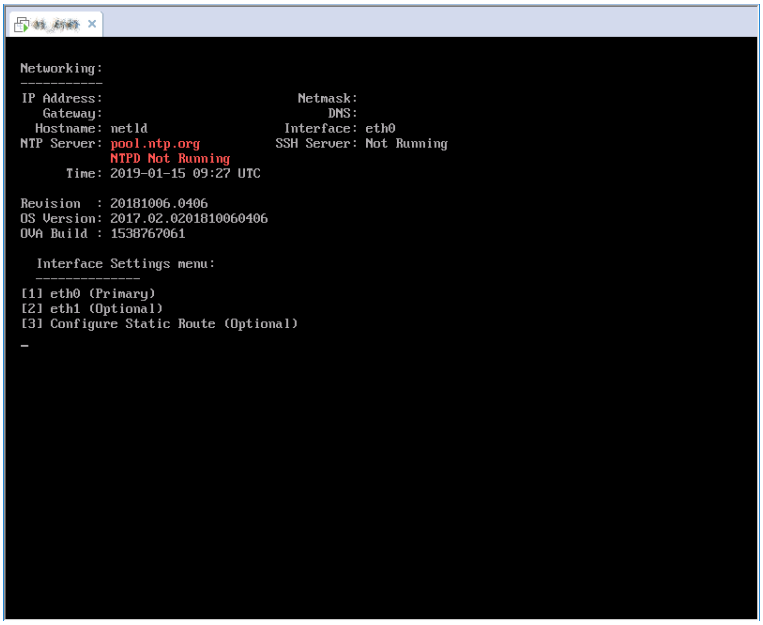
※ネットワーク設定は、仮想マシンコンソール上でキーボードを使って操作します。

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



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

Copyright (C) 2026 LogicVein, Inc.



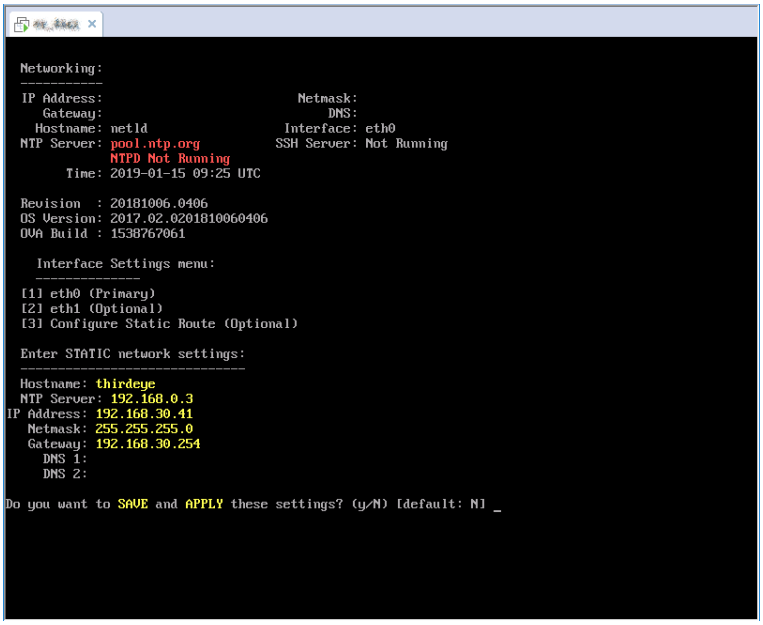
Copyright (C) 2026 LogicVein, Inc.

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。



設定が完了すると、サービスは自動的に再起動します。

Copyright (C) 2026 LogicVein, Inc.

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。

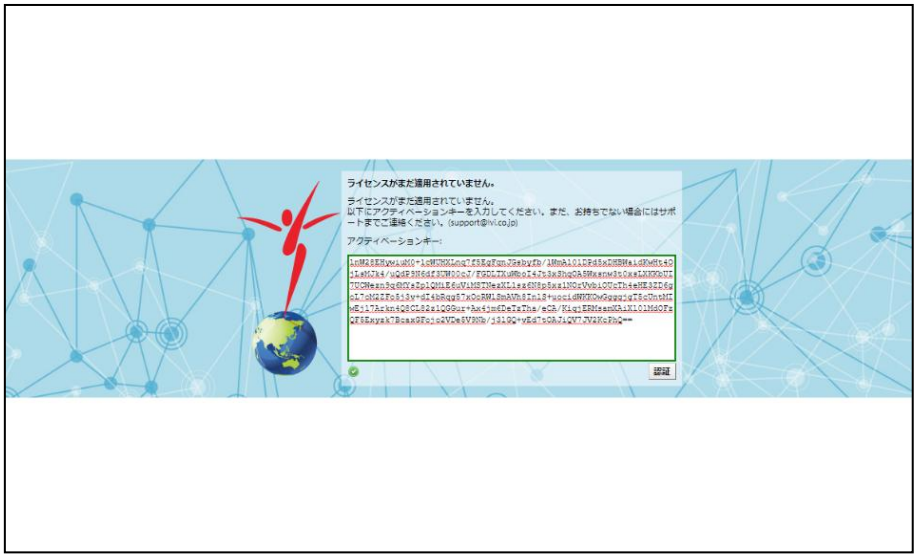
1. Web ブラウザで、ThirdEye のアドレスを入力し、アクセスします。

   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。

Copyright (C) 2026 LogicVein, Inc.

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。

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	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

設定後、［保存］をクリックし、ログイン画面に進みます。

Copyright (C) 2026 LogicVein, Inc.

3. 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。

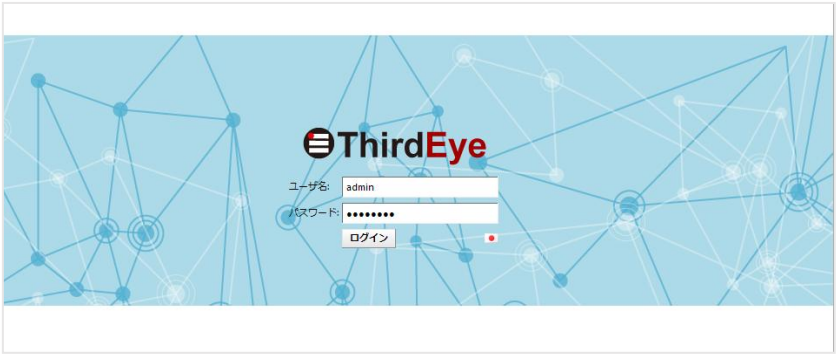
3.1 ログインする

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（admin）・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。

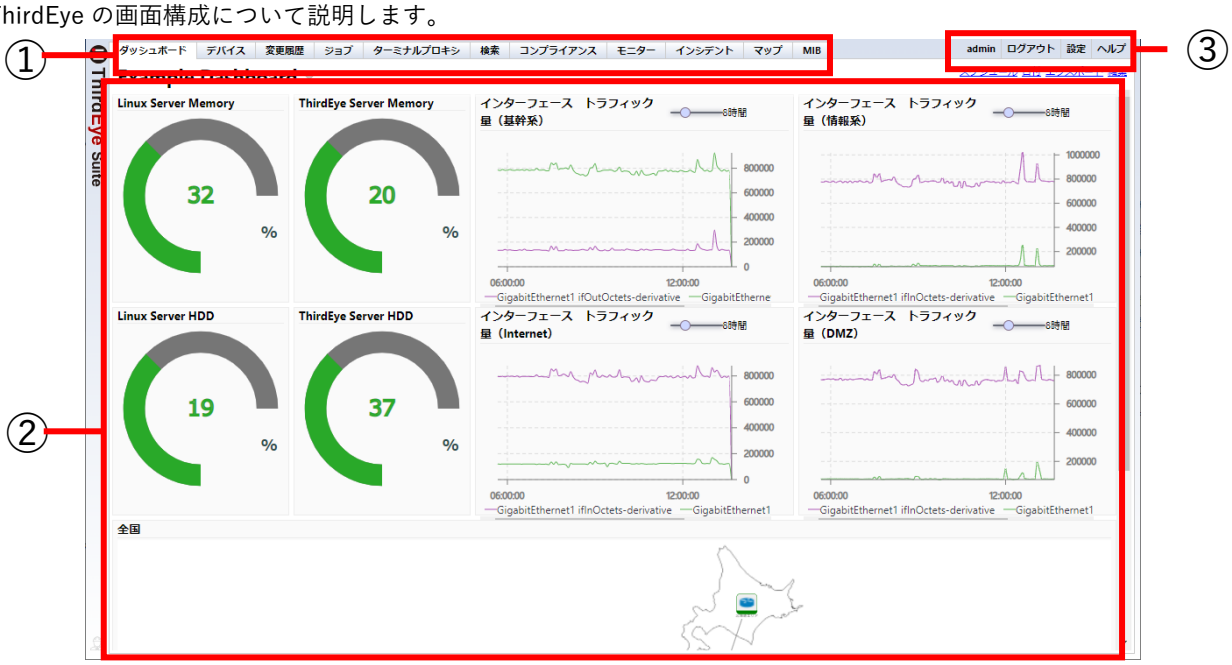
ログアウトすると、ThirdEye のログイン画面が表示されます。

Copyright (C) 2026 LogicVein, Inc.

4. 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

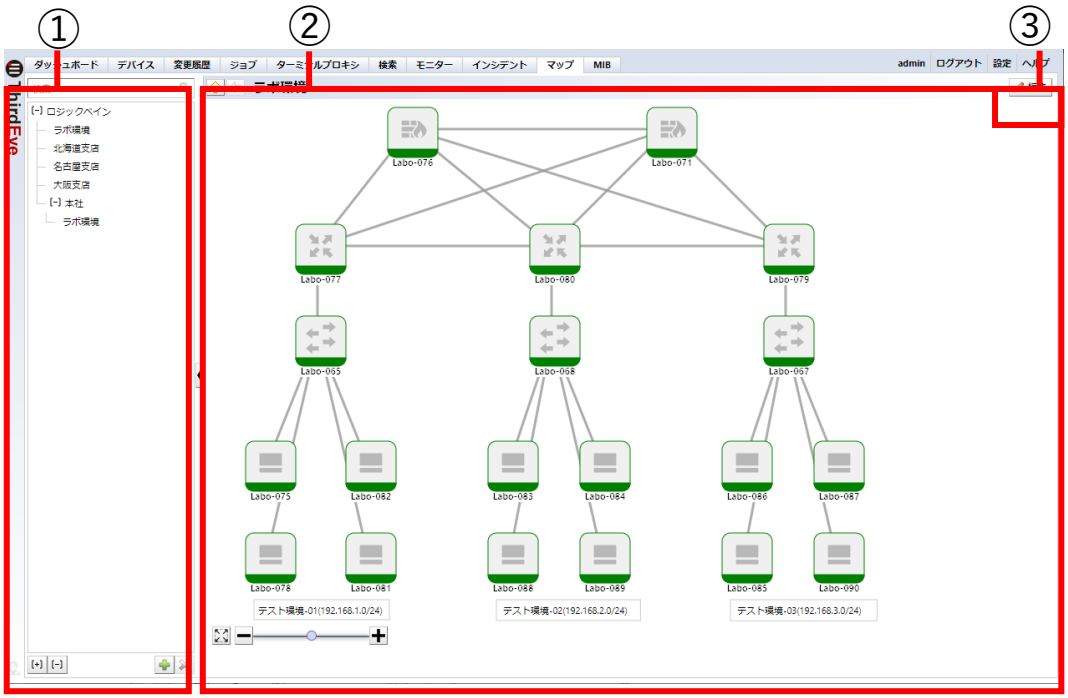
タブ	エディション	説明
ダッシュボード	共 通	ダッシュボードを表示します。詳しくは、「5.5 ダッシュボードを作成する」を参照してください。
デバイス	共 通	登録されているデバイスをインベントリ（一覧表）として表示します。
変更履歴	共 通	コンフィギュレーションの変更履歴を表示します。
ジョブ	共 通	ジョブの一覧を表示します。
ターミナルプロキシ	共 通	デバイスにターミナルで接続したときの記録の一覧を表示します。
検索	共 通	スイッチポート検索と ARP 検索、インタフェース検索を行うことができます。
コンプライアンス	Suite	デバイスのコンフィグがポリシーに従っているかを確認するための設定を行います。
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。

Copyright (C) 2026 LogicVein, Inc.

4.1.2 グローバルメニュー構成

項目	説明
ネットワーク	現在選択されている管理ネットワークが表示されます。 ※このオプションは、ログインユーザが 1 つの管理ネットワークにのみアクセスできる場合、または管理ネットワークが設定されていない場合は表示されません。
ユーザ名	現在ログイン中の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	各種設定画面（[サーバ設定]）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。

Copyright (C) 2026 LogicVein, Inc.

5. 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。

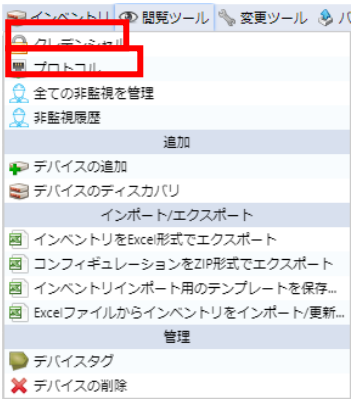
クレデンシャルの設定方法は、「ダイナミック」と「スタティック」と「クラウド」の 3 通りあります。

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。
クラウド	クラウドアカウントの認証情報を設定します。

5.1.1 共通のクレデンシャルを設定する

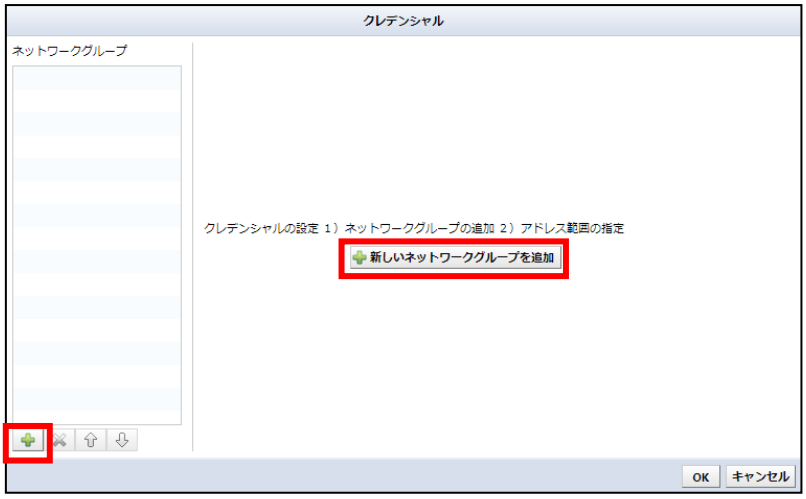
監視対象機器に共通のクレデンシャルを設定している場合は、「ダイナミック」を使用して設定します。

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。



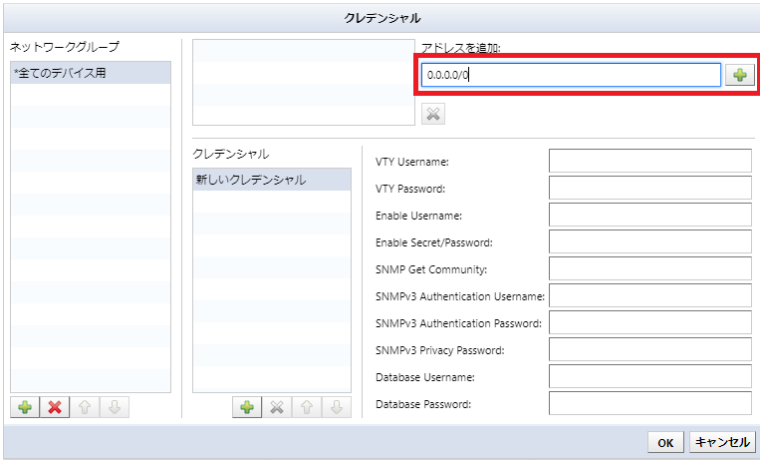
Copyright (C) 2026 LogicVein, Inc.

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。



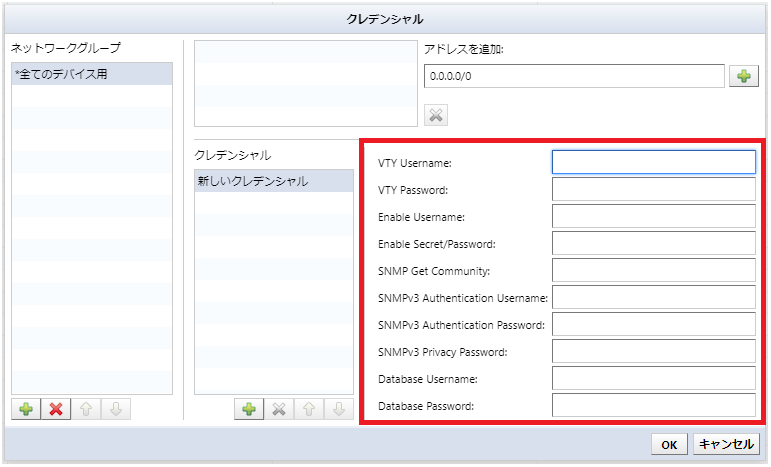
3. ネットワークグループ名を入力し、［ダイナミック］を選択して［OK］をクリックします。

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。



Copyright (C) 2026 LogicVein, Inc.

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
Database Username/Password	データベースのユーザ名/パスワードを入力します。

※設定が不要な項目は、空欄のままにできます。

※リビジョン 20240131.0729 から Postgres/MySQL/MariaDB のデータベース監視に対応しました。

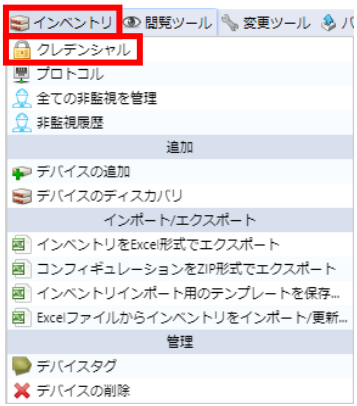
6. ［OK］をクリックし、設定を保存します。

Copyright (C) 2026 LogicVein, Inc.

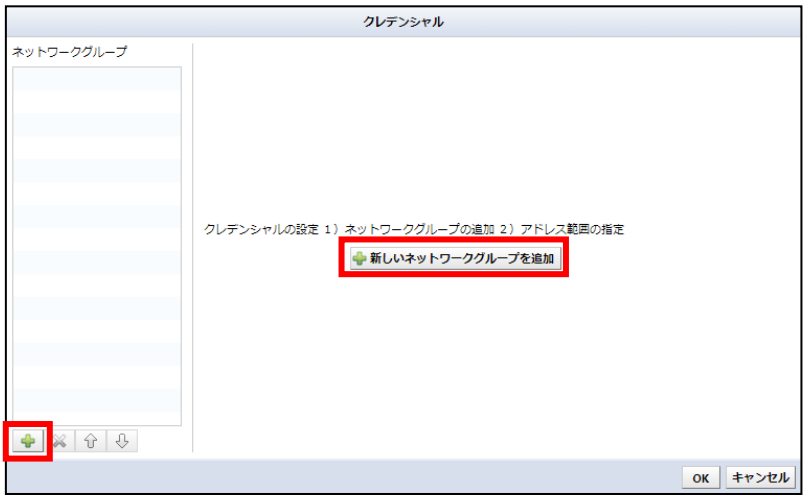
5.1.2 機器ごとにクレデンシャルを設定する

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。



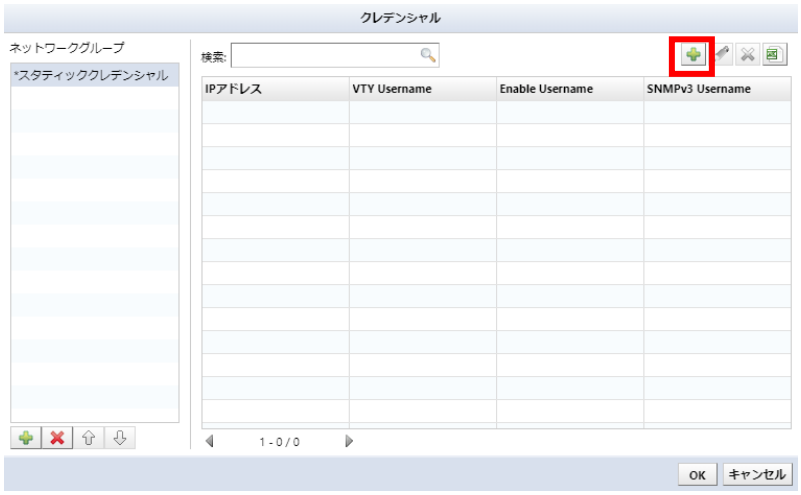
2. ［+(追加)］または［新しいネットワークグループを追加］をクリックします。



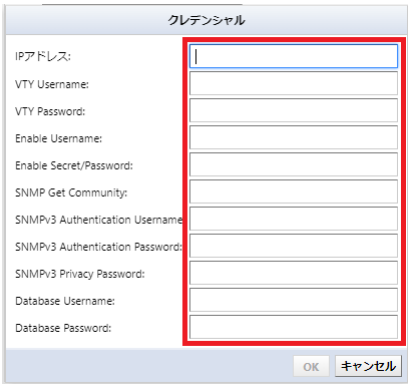
Copyright (C) 2026 LogicVein, Inc.

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。

Copyright (C) 2026 LogicVein, Inc.

項目	説明
SNMP Get Community	SNMP Get Request を実行する際に使用する 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。
Database Username/Password	データベースのユーザ名/パスワードを入力します。

※設定が不要な項目は、空欄のままにできます。

※リビジョン 20240131.0729 から Postgres/MySQL/MariaDB のデータベース監視に対応しました。

6. ［OK］をクリックします。

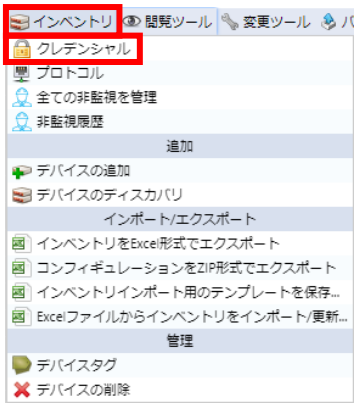
7. ［OK］をクリックし、設定を保存します。

Copyright (C) 2026 LogicVein, Inc.

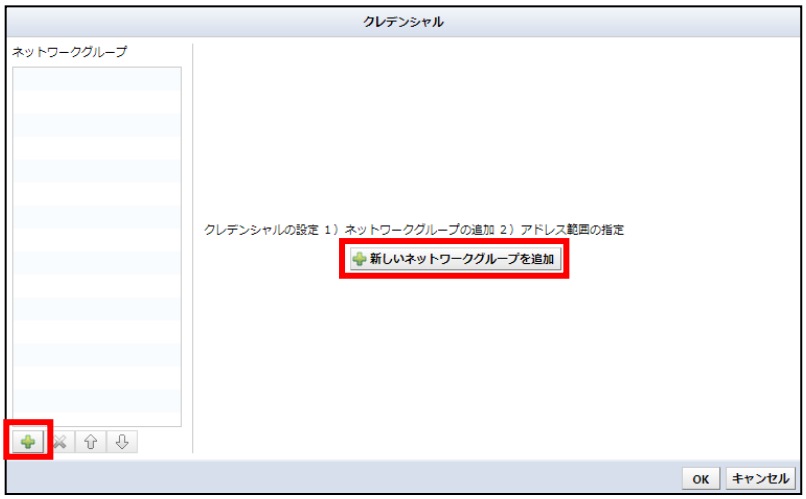
5.1.3 クラウドアカウントのクレデンシャルを設定する

リビジョン r20250627.0503 より、ThirdEye はクラウドデバイス管理に対応しました。ここではクレデンシャル設定について説明します。

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、［クラウド］を選択して［OK］をクリックします。

4. 作成されたクレデンシャルがネットワークグループに表示されます。

Copyright (C) 2026 LogicVein, Inc.

5.1.3.2　クラウドクレデンシャル設定

クラウドデバイスは主にクラウドアカウントを使用してデバイスにアクセスします。クレデンシャル/API アクセストークンがクラウドアカウントにアクセスできるように、以下の項目を設定する必要があります。表示される項目はクラウドサービスによって異なります。他のクレデンシャルとは異なり、アドレスを設定する必要はありません。アドレスフィルタを設定しない事で、ディスカバリ可能な全てのクラウドデバイスを検出します。

(1)　Cisco Meraki

クラウドデバイスは主にクラウドアカウントを使用してデバイスにアクセスするため、既存のダイナミックおよびスタティッククレデンシャルに加え、新しいクラウドクレデンシャルタイプを追加しました。Cisco Meraki ではクレデンシャル/アクセストークンがクラウドアカウントにアクセスできるよう、以下の項目を設定する必要があります。

項目	必須項目	説明
クレデンシャル表示名	必須	表示される名前を設定します。
クラウドサービス	必須	クラウドサービスプロバイダを設定します。
API キー	必須	パスワードもしくはアクセストークンを設定します。
アドレスフィルタ	—	IP もしくは CIDR を設定します。

(2)　Aruba EdgeConnect

ThirdEye は、HPE Aruba EdgeConnect（EC）デバイス（旧称 SilverPeak）向けのクラウドデバイスサポートを提供します。EdgeConnect デバイスは、導入済みの Orchestrator または Aruba Central クラウドポータルを介してローカルで管理できます。EdgeConnect デバイスでは、Orchestrator またはクラウド ポータルにアクセスするために、API キーと API URL を設定する必要があります。

項目	必須項目	説明
クレデンシャル表示名	必須	表示される名前を設定します。
クラウドサービス	必須	クラウドサービスプロバイダを設定します。
API Base URL	必須	API プロバイダ URL を設定します。
API キー	必須	パスワードもしくはアクセストークンを設定します。

Copyright (C) 2026 LogicVein, Inc.

アドレスフィルタ	—	IP もしくは CIDR を設定します。

API URL を設定する際は、IP（ドメイン）とプロキシマッピング（ある場合）のみ設定してください。
ThirdEye が API のベース URL を生成します。URL に https://10.0.99.8/を設定すると、システムは Base URL https://10.0.99.8/gms/rest を生成します。

(3) Aruba Central

ThirdEye は、Aruba Central 経由で Aruba アクセスポイント（AP）をクラウドデバイスとして管理するサポートを提供します。開始前に、API アクセスに必要な権限を持つ有効な Aruba Central アカウントが存在することを確認してください。Aruba アクセスポイントを監視するには、Aruba Central 用のクラウドアカウントクレデンシャルを設定し、その情報をディスカバリしてアクセスポイントを検索する必要があります。

Aruba Central 用のクラウドアカウントクレデンシャルを設定する際は、まず Aruba Central ポータルからアクセストークンを生成してください。アクセストークンの詳細が利用可能になったら、認証情報ページに移動し、新しいクラウドアカウント認証情報を作成します。Aruba Central API プロバイダはアクセストークンと更新トークンの両方に有効期限を設けています。そのため、ThirdEye はトークンを定期的に更新します。クレデンシャルの初期設定時からこの処理が開始されます。クレデンシャルを設定する際は、Aruba Central ポータルで生成したアクセストークンの情報を使用してください。クレデンシャルが設定されると、ThirdEye はアクセストークンの詳細を取得するために初期トークン更新を実行します。その後、トークンの有効期限の 90%が経過した時点で、トークンは定期的に更新されます。

項目	必須項目	説明
クレデンシャル表示名	必須	表示される名前を設定します。
クラウドサービス	必須	クラウドサービスプロバイダを設定します。
API Region	必須	API Gateway のリージョンを設定します。（アカウントが登録されている地理的クラスタに基づく）
Client ID	必須	新規で Refresh Token を要求する為の Client ID を設定します。
Client Secret	必須	Refresh Token の為の Client Secret を設定します。
Refresh Token	必須	Refresh Token を設定します。
アドレスフィルタ	—	IP もしくは CIDR を設定します。

Copyright (C) 2026 LogicVein, Inc.

5.1.4　SSH 秘密鍵認証

SSH 秘密鍵認証により、デバイスのバックアップ、コンフィグ管理、およびターミナルセッションでパスワード認証の代わりに鍵認証を使用することができます。クレデンシャルセットで SSH 秘密鍵認証が設定されている場合、以下の状況において、その秘密鍵を使用してデバイスとの認証を行います。

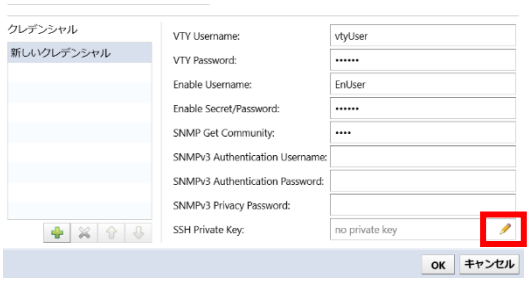
- バックアップ、復元
- ターミナルプロキシ
- ツール実行

秘密鍵とパスワードの両方が設定されている場合、まず鍵ベースの認証を試み、鍵が拒否された場合はパスワード認証に切り替えます。

備考	SSH 鍵認証を使用する際は、認証を正常に行うために、対象デバイス上で対応する公開鍵が適切に設定されていることを確認してください（authorized_keys ファイル）。 デバイス上で公開鍵が正しく設定されていない場合、鍵認証は失敗し、パスワードが設定されている場合はパスワード認証に切り替わります。

5.1.4.1　SSH 秘密鍵の設定

クレデンシャルでユーザ名を設定後、SSH Private Key フィールドを選択してください。これは読み取り専用フィールドで、鍵が存在する場合、検出された鍵の種類が表示されます。SSH 秘密鍵を追加または変更するには、フィールドの右側にある鉛筆アイコンをクリックします。

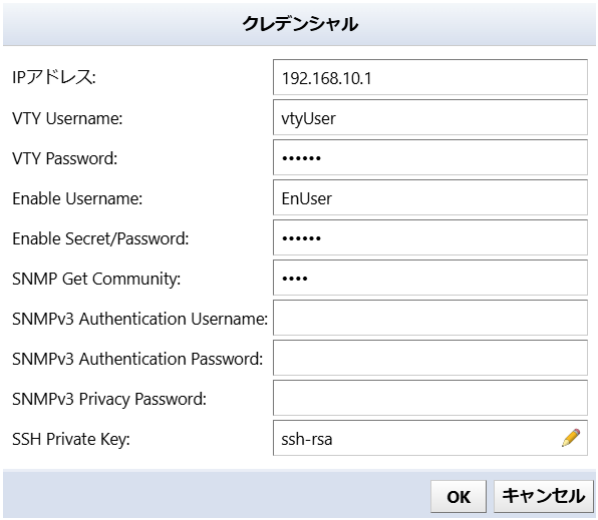


これにより、SSH キーエディタダイアログが開きます。SSH 秘密鍵を設定する際は、必ずヘッダー行とフッター行を含めてください。パスフレーズを設定する際、秘密鍵がパスフレーズで暗号化されている場合は、パスフレーズ欄に入力してください。鍵がパスフレーズで保護されていない場合は、その欄を空欄のままにしてください。

Copyright (C) 2026 LogicVein, Inc.

項目	説明
SSH 秘密鍵	秘密鍵ファイルの内容を全てテキストエリアに貼り付けます。
Passphrase	秘密鍵のパスフレーズを設定します。

「OK」をクリックして保存するか、「キャンセル」をクリックして変更を破棄します。鍵が設定されている場合、「SSH 秘密鍵」フィールドには、鍵の内容そのものではなく、検出された鍵の種類が表示されます。



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。
クラウドアカウントからのインポート	クレデンシャルで追加したクラウドアカウントのデバイスを自動的に検出、追加します。

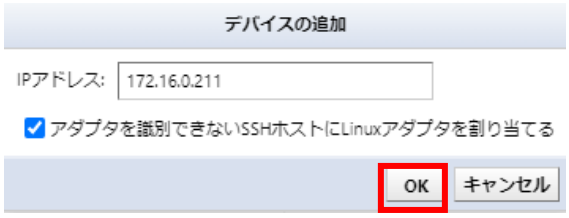
Copyright (C) 2026 LogicVein, Inc.

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。



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。

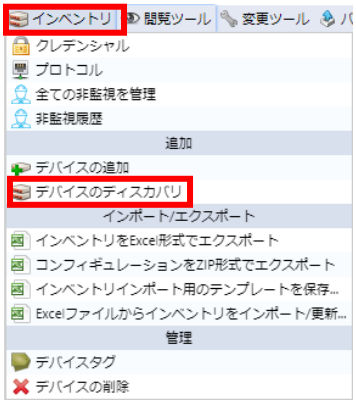
Copyright (C) 2026 LogicVein, Inc.

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。

※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、［インベントリ］→［デバイスのディスカバリ］の順にクリックします。



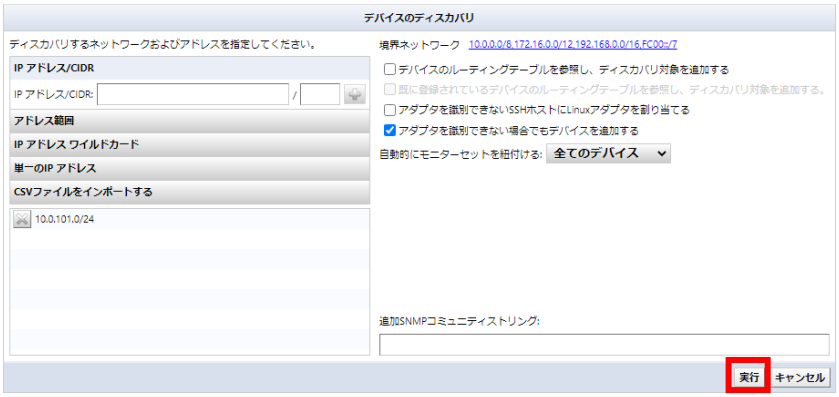
2. ディスカバリする IP アドレス範囲を指定し、［+(追加)］をクリックします。

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。

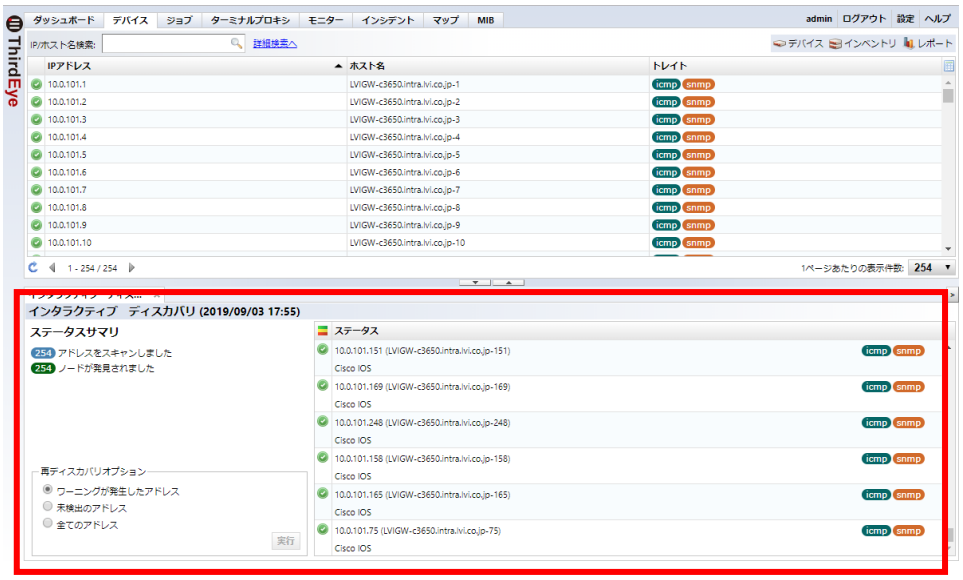
Copyright (C) 2026 LogicVein, Inc.

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。
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。

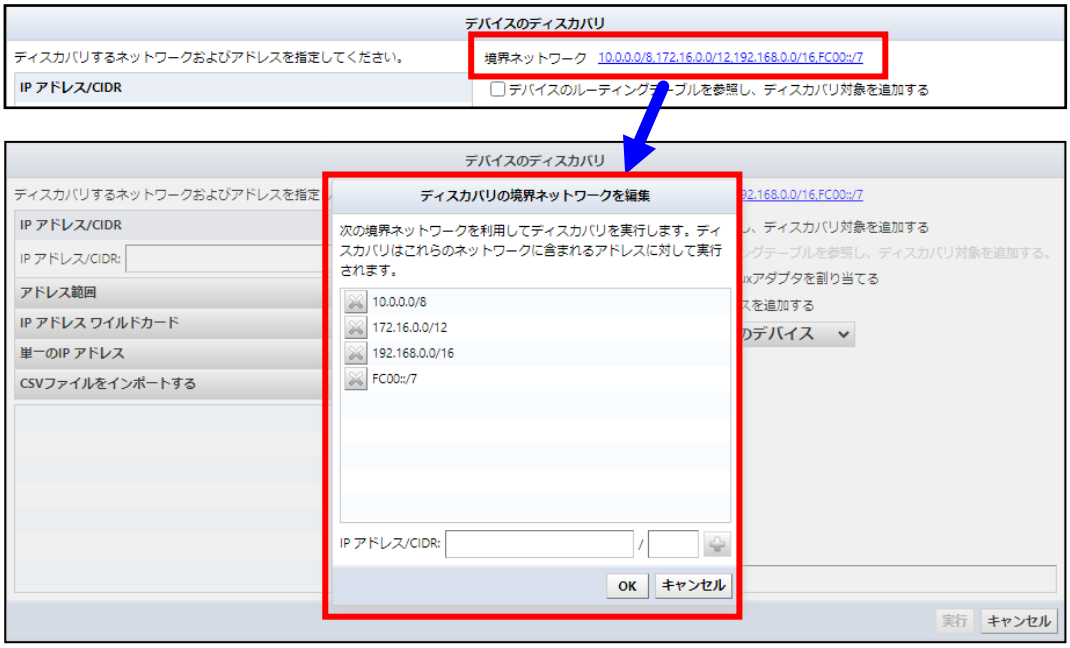


4. ディスカバリが開始され、画面下にディスカバリの結果が表示されます。



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。

Copyright (C) 2026 LogicVein, Inc.

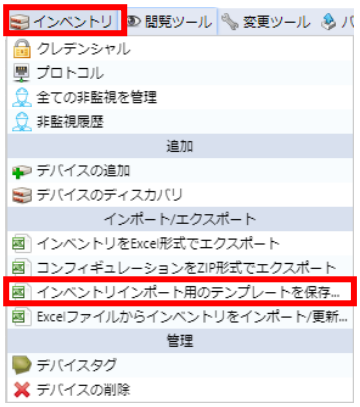
補足	ディスカバリには「境界ネットワーク」という設定があり、ディスカバリの対象範囲を「境界ネットワーク」に指定された範囲に制限することができます。「境界ネットワーク」には、デフォルトでいくつかの範囲が指定されていますので、必要に応じて「境界ネットワーク」を編集してください。 

Copyright (C) 2026 LogicVein, Inc.

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。

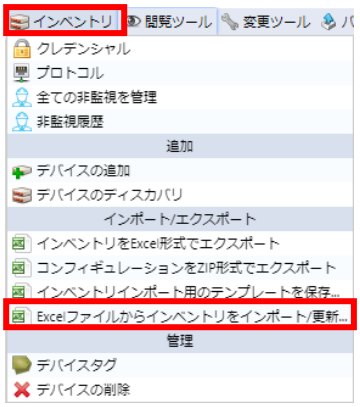
3. 保存したファイルを編集し、以下の項目に情報を入力し、上書き保存します。

	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																	

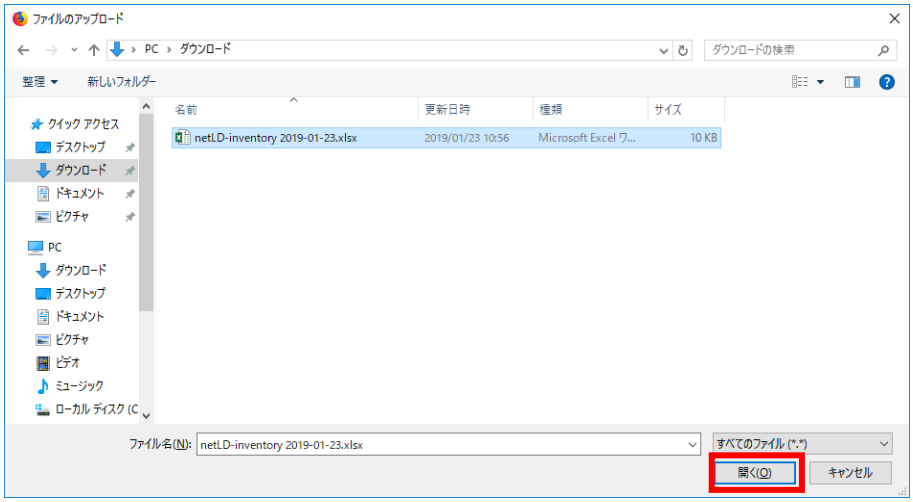
項目	説明	必須項目	入力例
IP Address	デバイスの IP アドレスを入力します。	必須	192.168.1.10
Network	機器を追加したいネットワーク名を選択します。	必須	Default
Adapter ID	デバイスのアダプタを選択します。 ※現在のバージョンでは、この項目を指定する必要はありません。	—	Cisco IOS
Hostname	デバイスのホスト名を入力します。	—	
End Of Sale	販売終了日を「yyyy/mm/dd」の形式で入力します。	—	2022/1/1
End Of Life	サポート終了日を「yyyy/mm/dd」の形式で入力します。	—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

Copyright (C) 2026 LogicVein, Inc.

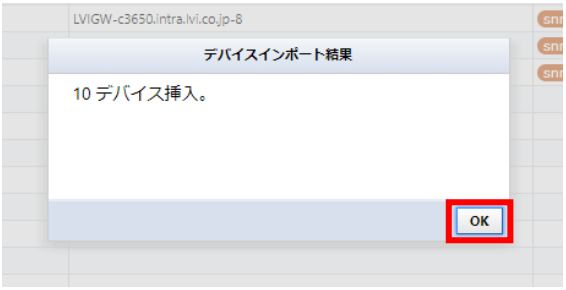
4. ［インベントリ］→［Excel ファイルからインベントリをインポート/更新］の順にクリックします。



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。



Copyright (C) 2026 LogicVein, Inc.

5.2.4　クラウドアカウントのディスカバリ

クラウドクレデンシャルの追加に伴い、デバイスのディスカバリにおいて複数のクラウドアカウントを選択できるようになりました。インベントリからデバイスディスカバリを実行するのと同様に、ディスカバリジョブでクラウドアカウントを設定し、ディスカバリを実行する事ができます。

実行をクリックすると、設定されたクレデンシャルセットを使用して、指定されたディスカバリ境界内にあるデバイスを検出します。

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）

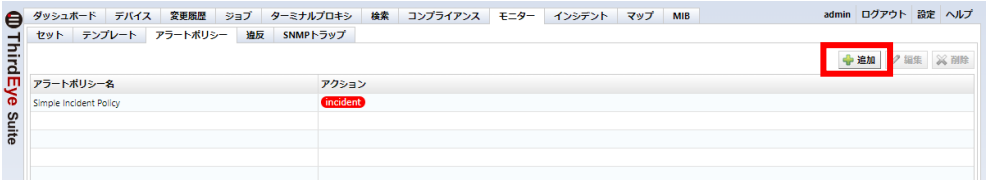
③　しきい値などトリガー設定（トリガー機能）

5.3.1　障害を検知した時のアクションを設定する

障害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。

※　障害を検知した後に、アラートポリシーを変更した場合には、その障害で発生した違反を一度クリアすることで、変更したアラートポリシーが適用されます。

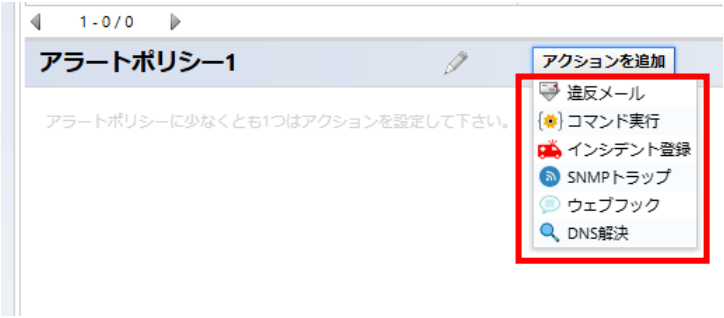
1. ［モニター］→［アラートポリシー］を選択し、［追加］をクリックします。



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。

Copyright (C) 2026 LogicVein, Inc.



【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。
違反メール	共 通	障害検知時にメール送信を実行します。
ウェブフック	共 通	障害検知時に Mattermost / Slack / Teams / Webex / LINE WORKS/PagerDuty/Google Chat に通知します。

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。

5.3.1.1 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。

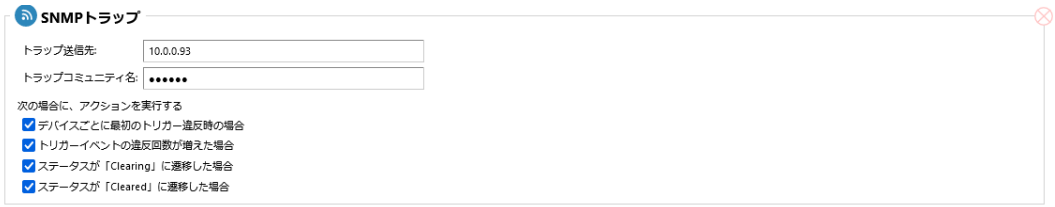
Copyright (C) 2026 LogicVein, Inc.

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。複数宛先にメールを送信したい場合には、カンマで区切ってください。 ※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 分に 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。
ユーザが違反をクリアした場合	違反が手動で更新された場合にメールを送信します。
ユーザがインシデントを更新した場合	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。
ユーザアクションに応じた操作が行われた場合、通知制限を無視してすぐに送信する	違反/インシデントに関わらず、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、「7.8.3.6 メールサーバを設定する」を参照してください。

5.3.1.2 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。

Copyright (C) 2026 LogicVein, Inc.

項目	説明
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

5.3.1.3　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。

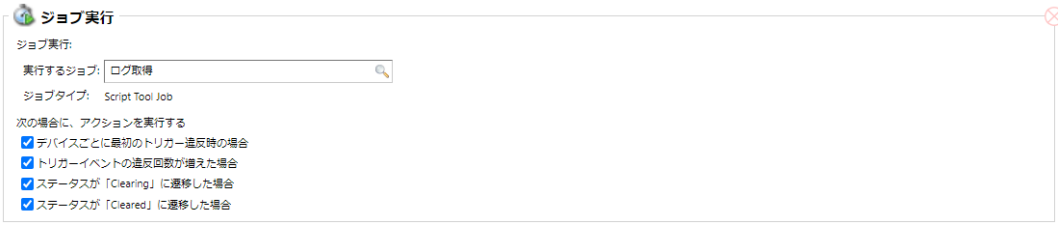
Copyright (C) 2026 LogicVein, Inc.

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にのみ実行	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。

Copyright (C) 2026 LogicVein, Inc.

5.3.1.4　ジョブ実行 Suite

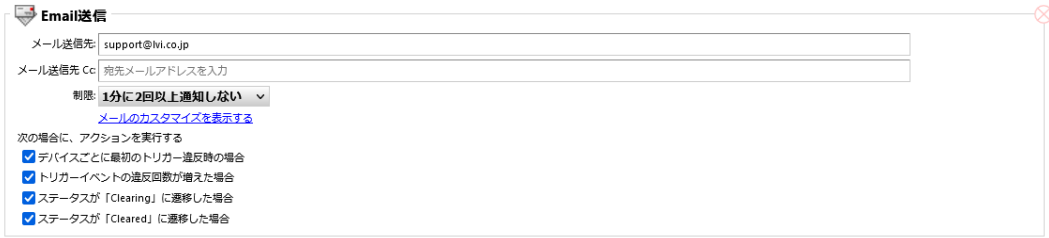
リモートホストからプログラムを実行できます。指定したリモートホストに SSH ログインし、リモートホストから指定したコマンドを実行します。



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にのみ実行	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。

5.3.1.5　メール送信

メール送信では、異常発生時にメールを送信します。インシデント登録アクションのメールは、インシデント機能によって異常がまとめられてメール送信されるケースがありますが、メール送信では、異常毎にメールを送信することが可能です。



項目	説明
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。複数宛先にメールを送信したい場合には、カンマで区切ってください。 ※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。複数宛先にメールを送信したい場合には、カンマで区切ってください。 ※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 分に 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。

Copyright (C) 2026 LogicVein, Inc.

項目	説明
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。

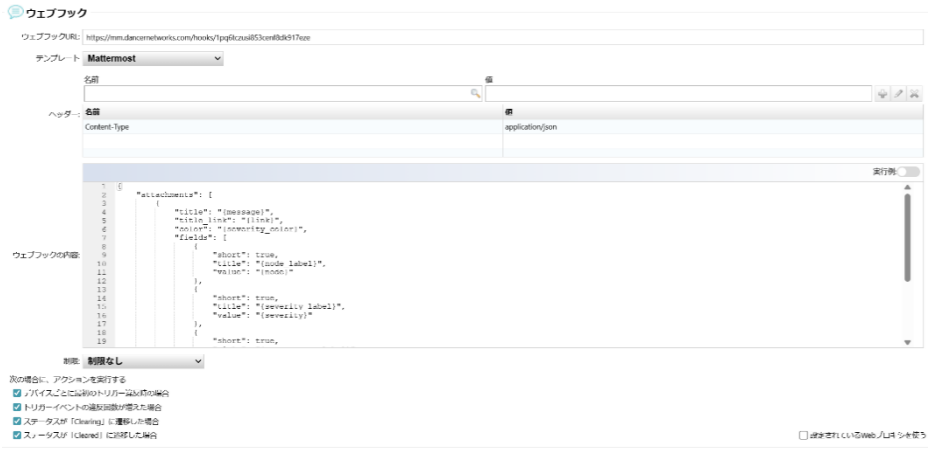
※メール送信をするには、あらかじめメールサーバを設定する必要があります。メールサーバの設定については、「7.8.3.6 メールサーバを設定する」を参照してください。

Copyright (C) 2026 LogicVein, Inc.

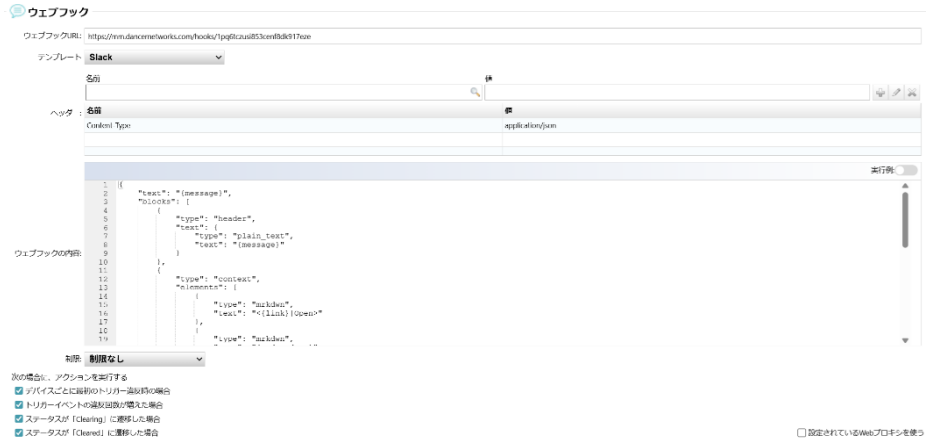
5.3.1.6　ウェブフック

Mattermost / Slack / Teams / Webex / LINE WORKS/ PagerDuty/Google Chat では、異常発生時にウェブフックを通じてそれぞれに通知します。この機能を使用するためには、予めそれぞれのツール上でウェブフックの設定やアプリの追加などが必要です。

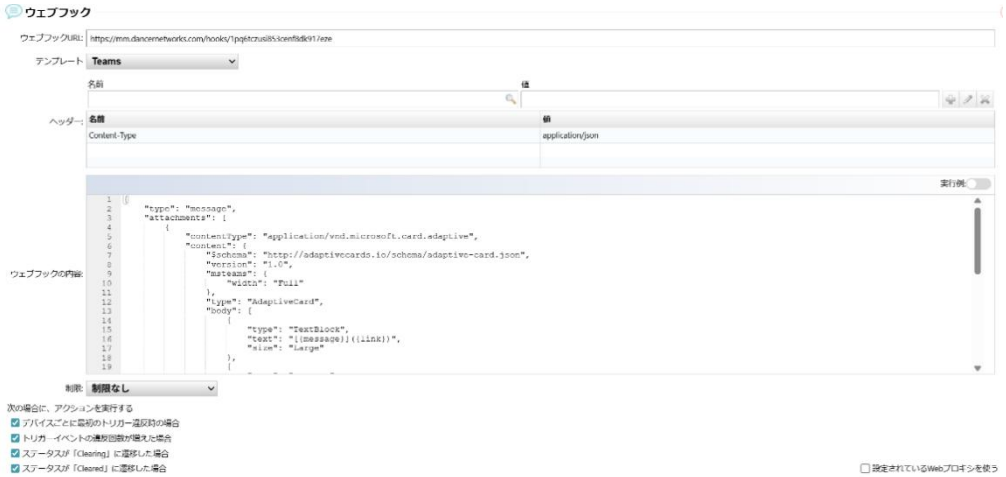
<Mattermost>



<Slack>

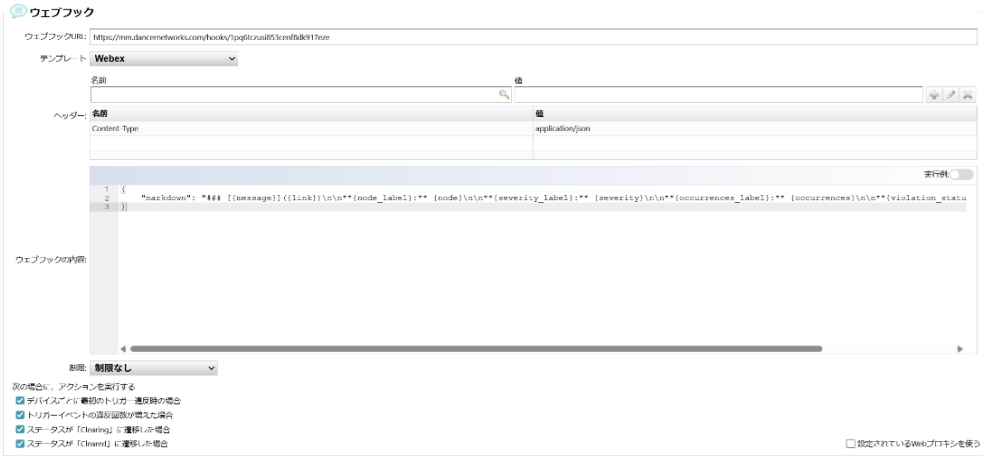


<Teams>

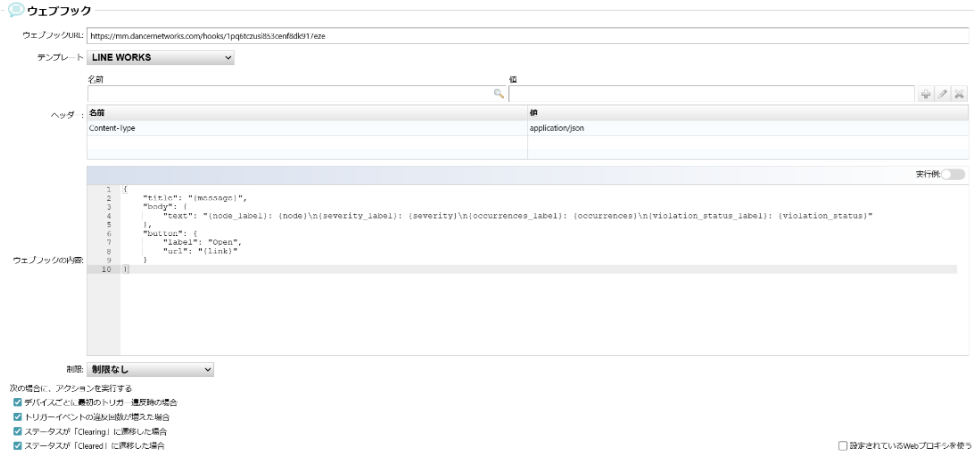


<Webex>

Copyright (C) 2026 LogicVein, Inc.

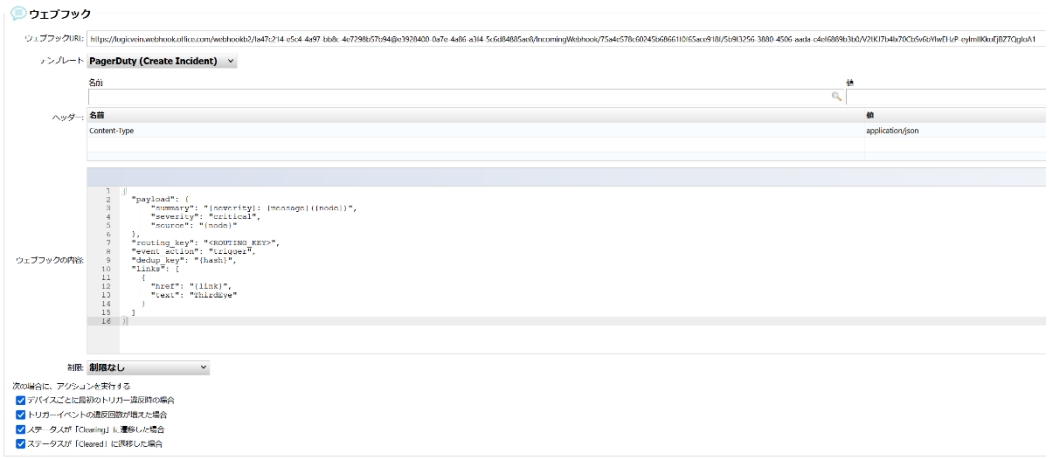


<LINE WORKS>



<PagerDuty>

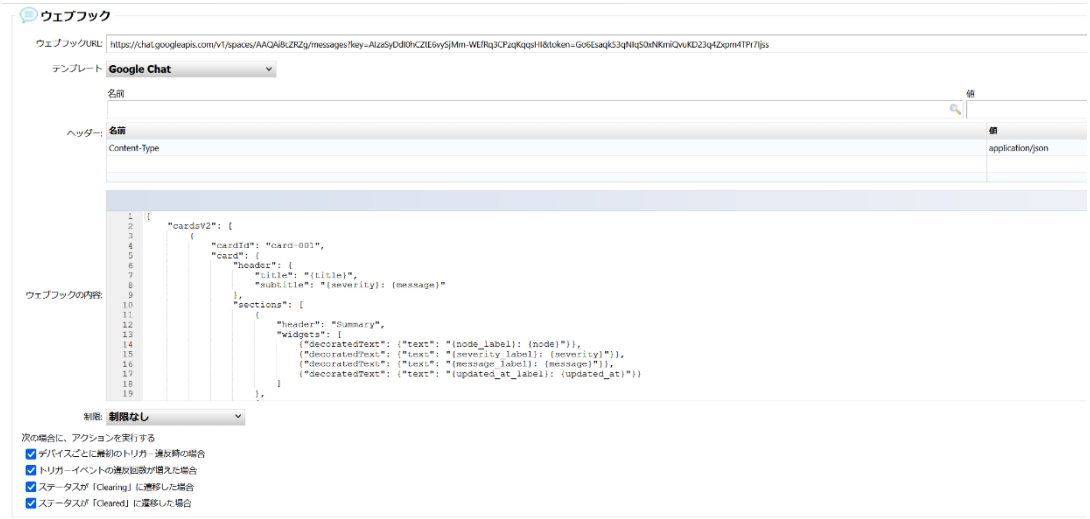
Create/Resolve Incident



※<ROUTING_KEY>に Integration Key を設定する必要があります。

<Google Chat>

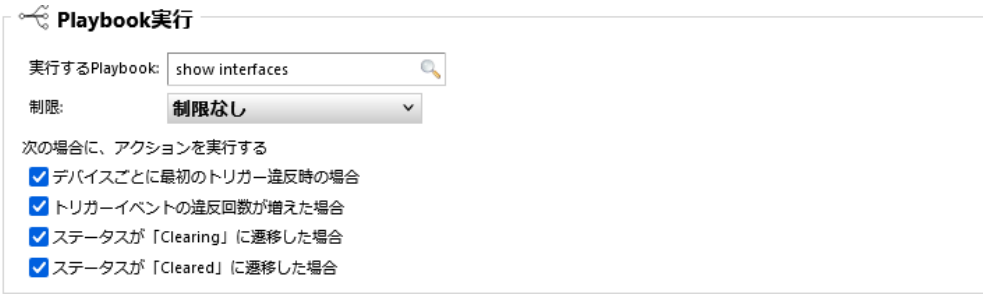
Copyright (C) 2026 LogicVein, Inc.



項目	説明
ウェブフック URL	Mattermost / Slack / Teams / Webex / LINE WORKS / PagerDuty/Google Chat 上で生成された URL を入力します。
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、初回違反時に通知します。
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通知します。
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」に遷移した場合に通知します。
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」に遷移した場合に通知します。
設定されている Web プロキシを使う	グローバルメニューの［設定］- [Web プロキシ]の設定を使用して通知します。

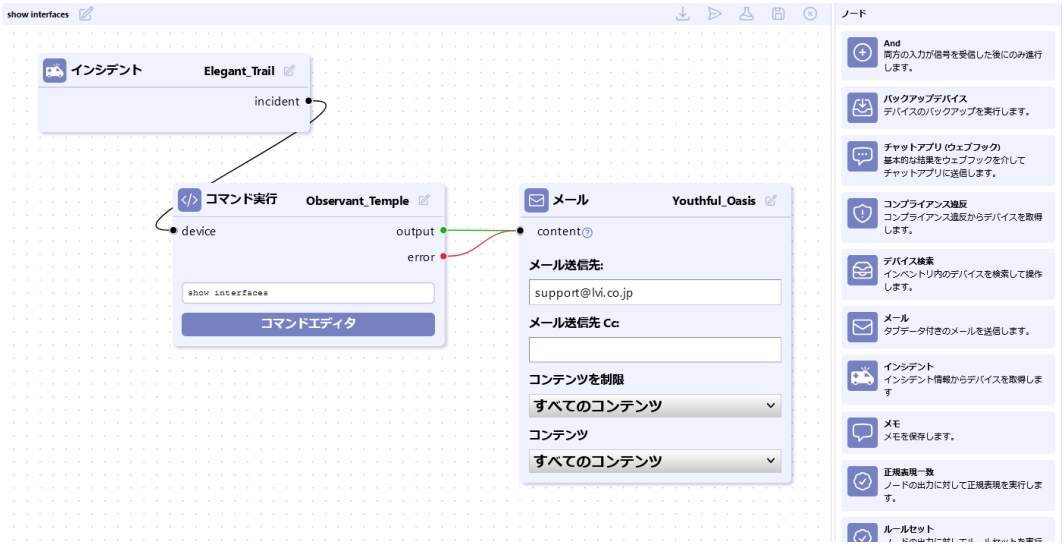
5.3.1.7 Playbook 実行 Suite

指定した Playbook を違反発生時に実行します。



違反発生時に実行できる Playbook の条件として、インシデントノードが Playbook に含まれている必要があります。

Copyright (C) 2026 LogicVein, Inc.



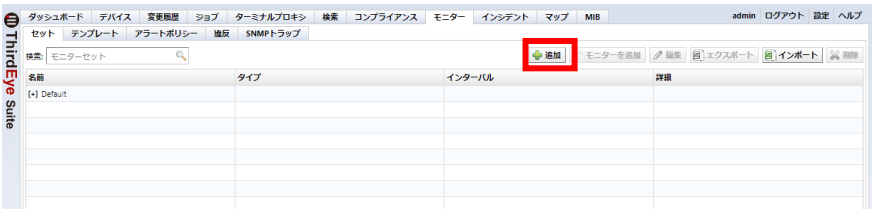
インシデントノードを持たない Playbook を実行する Playbook に指定した場合には、以下のようなメッセージが表示されます。

Copyright (C) 2026 LogicVein, Inc.

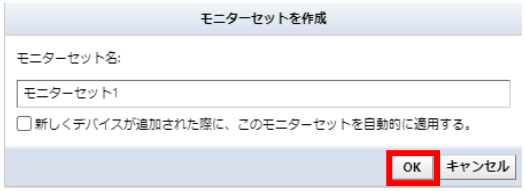
5.3.2 モニターセットを使用して多数の機器に対して監視設定をする

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。

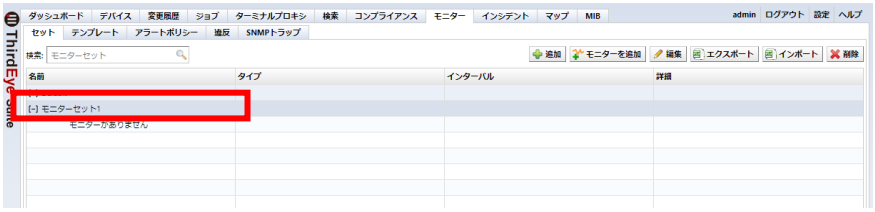


2. モニターセット名を入力し、［OK］をクリックします。



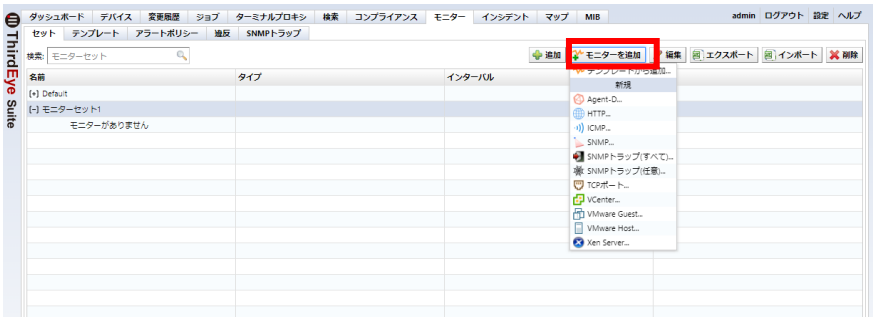
項目	説明
新しくデバイスが追加された際に、このモニターセットを自動的に適用する。	このモニターセットに含まれるモニターを、デバイスを追加した時に、デバイスとの通信ができる状態であれば、自動的に割り当てます。

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。

※ モニターは、個別のモニター設定と同様の手順で追加できます。

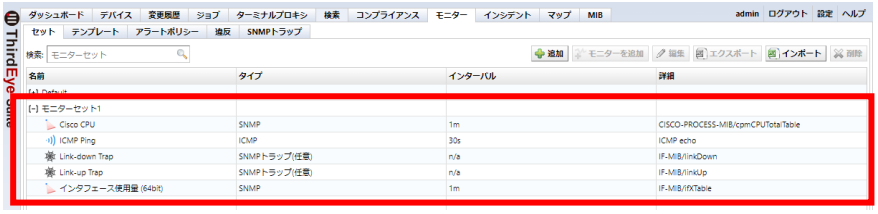


項目	説明
テンプレートから追加	［テンプレート］に、作成されているモニターテンプレートの中からモニターを追加します。

Copyright (C) 2026 LogicVein, Inc.

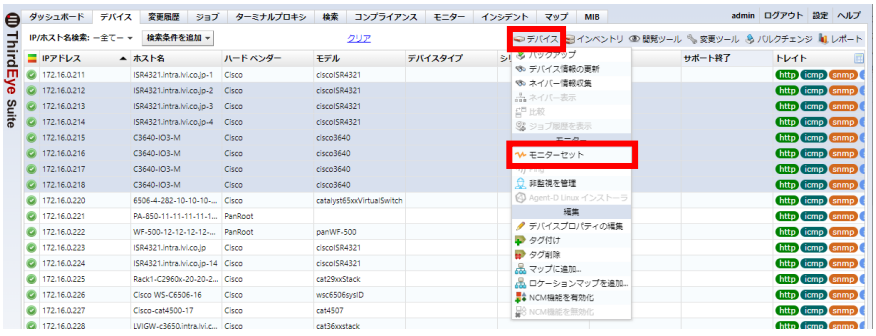
項目	説明
Agent-D	Agent-D のモニターを追加します。
HTTP	http または https に対する監視するモニターを追加します。
ICMP	ICMP Ping によるモニターを追加します。
SNMP	MIB テーブルから監視する MIB オブジェクトを指定し監視するモニターを追加します。
SNMP トラップ(すべて)	すべての SNMP トラップを監視するモニターを追加します。
SNMP トラップ(任意)	指定された SNMP トラップを監視するモニターを追加します。
TCP ポート	指定された TCP ポートに対する監視するモニターを追加します。
VCenter	vCenter 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】



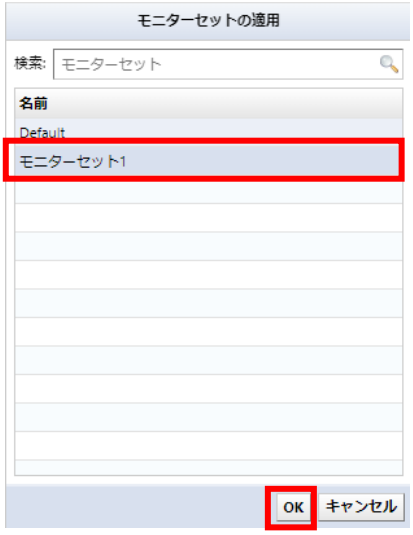
5. ［デバイス］タブを選択し、モニターセットを割り当てるデバイスを選択します。

6. ［デバイス］→［モニターセット］の順にクリックします。



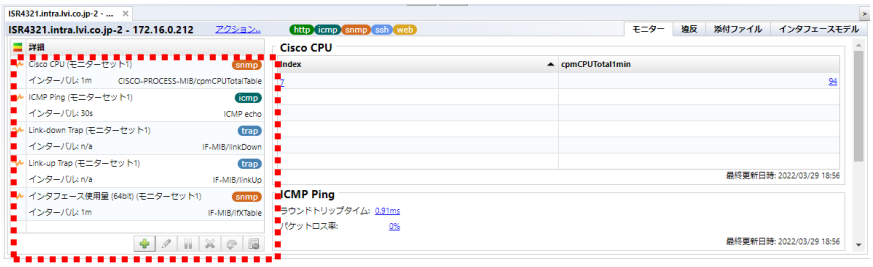
Copyright (C) 2026 LogicVein, Inc.

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。



Copyright (C) 2026 LogicVein, Inc.

5.3.3 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。

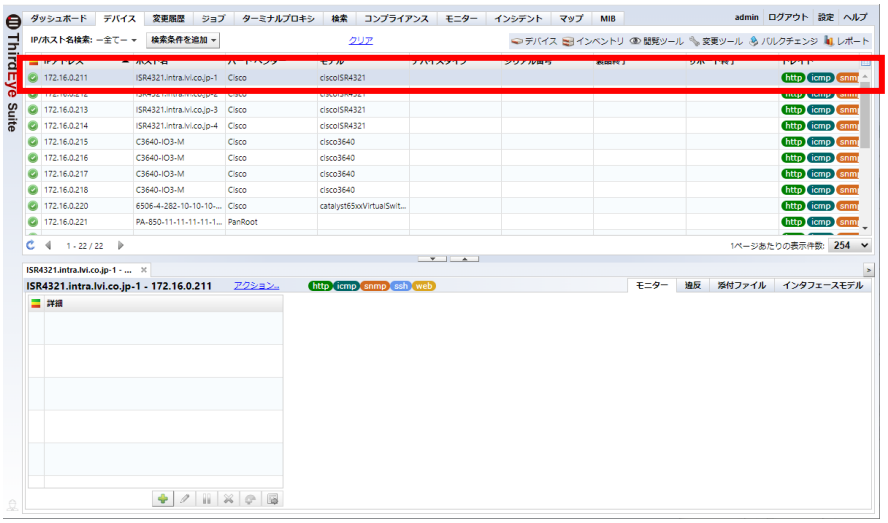
【条件】

監視間隔：5 分

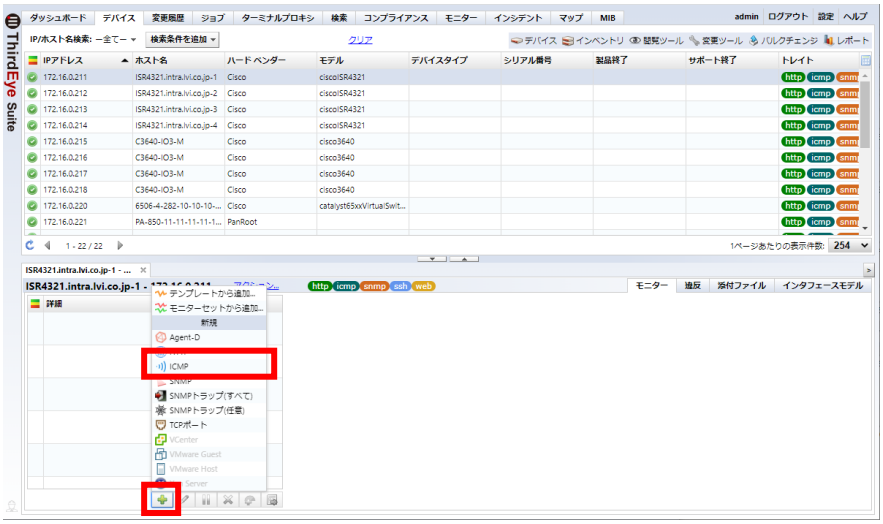
アラート条件：10 分間に 2 回、応答が無い場合

※ThirdEye の ICMP ポーリングの詳細は「13.1 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。



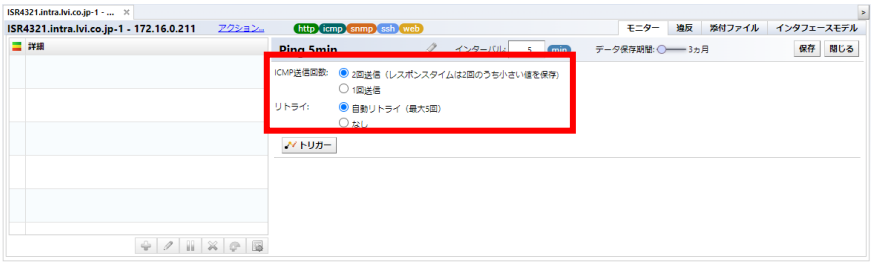
Copyright (C) 2026 LogicVein, Inc.

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。

Copyright (C) 2026 LogicVein, Inc.

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。

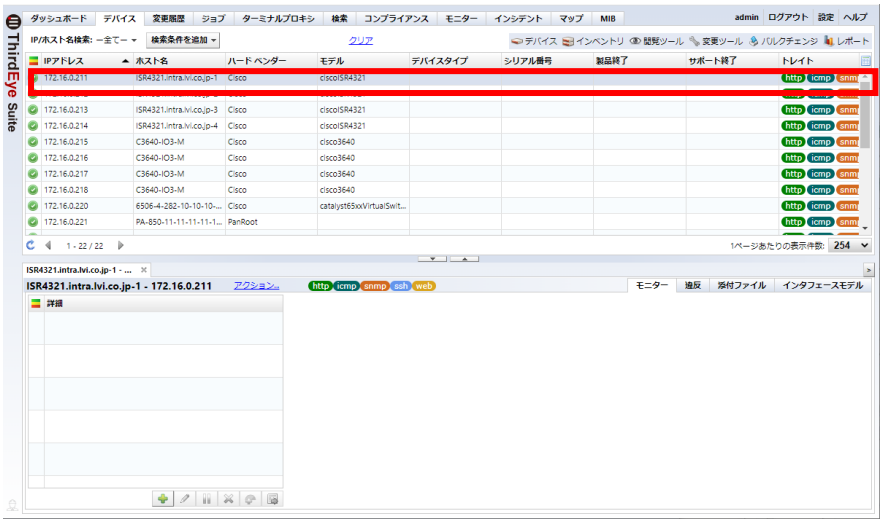
9. ［保存］をクリックします。

Copyright (C) 2026 LogicVein, Inc.

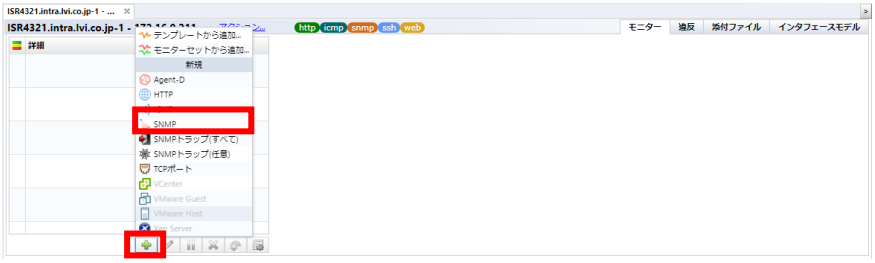
5.3.4 SNMP 情報を収集する

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。

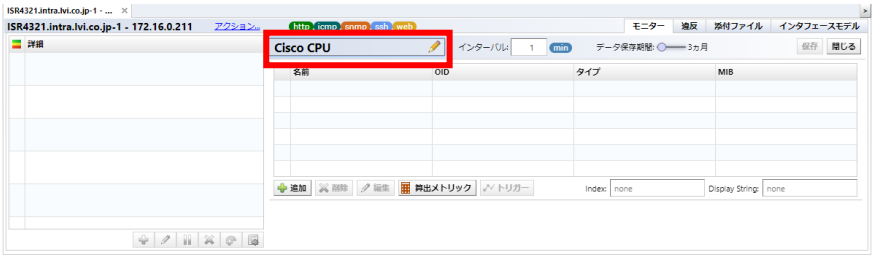
1. ［デバイス］タブの監視対象機器一覧から、モニターを設定する機器をダブルクリックします。



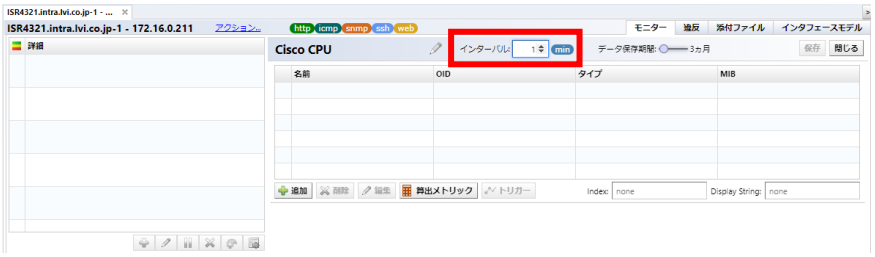
2. 左下の［+(追加)］をクリックし、「SNMP」をクリックします。



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。

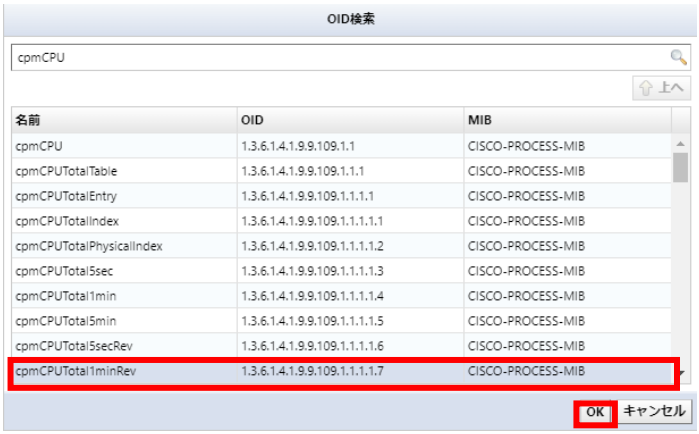


Copyright (C) 2026 LogicVein, Inc.

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。

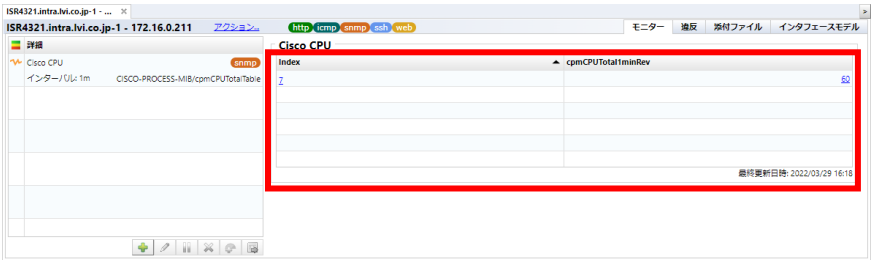
6. ［+(追加)］をクリックし、［MIB ライブラリ］をクリックします。

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ます。取得に成功するとデバイス詳細画面にデータが表示されます。

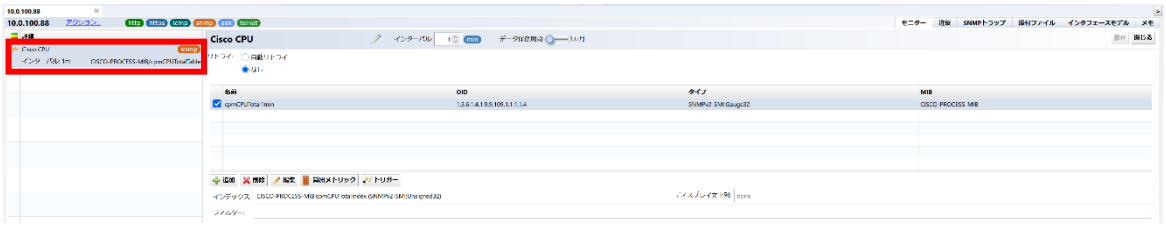


Copyright (C) 2026 LogicVein, Inc.

5.3.5 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、「5.3.4 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。

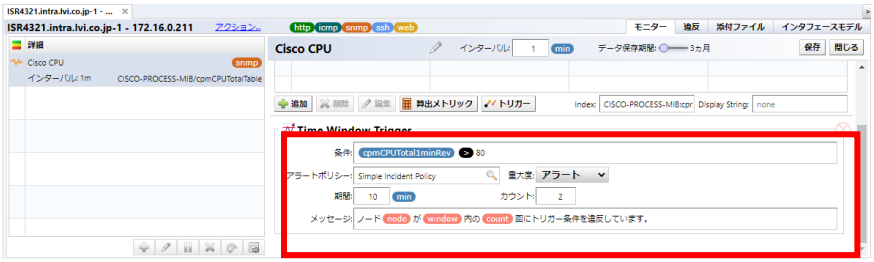
1. 詳細テーブルから、しきい値を設定するモニターをダブルクリックまたは［編集］をクリックします。



2. ［トリガー］をクリックし、［しきい値判定］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した例を示しています。

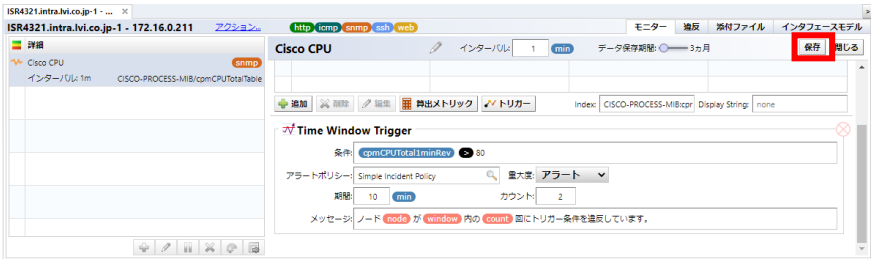


項目	説明
条件	以下の項目を使って、条件を指定することができます。 ● is （等しい） ● is not （等しくない） ● ＞ （より小さい、右の値のほうが小さい） ● ＜ （より大きい、右の値のほうが大きい） ● contains （含む） ● not contains （含まない）
アラートポリシー	アラートポリシーを指定します。
重大度	重大度を次の中から選択します。（初期値：ワーニング） 「エマージェンシー」、「アラート」、「クリティカル」、「エラー」、「ワーニング」、「通知」、「情報」、「デバッグ」 重大度とアイコンの枠線/ステータスアイコンの対応表は、こちらを参照してください。
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）

Copyright (C) 2026 LogicVein, Inc.

項目	説明
	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。



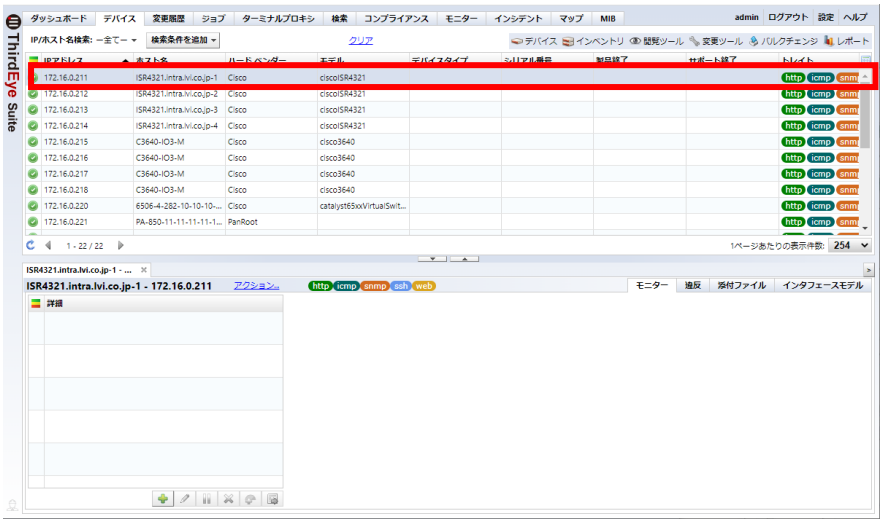
Copyright (C) 2026 LogicVein, Inc.

5.3.6 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。

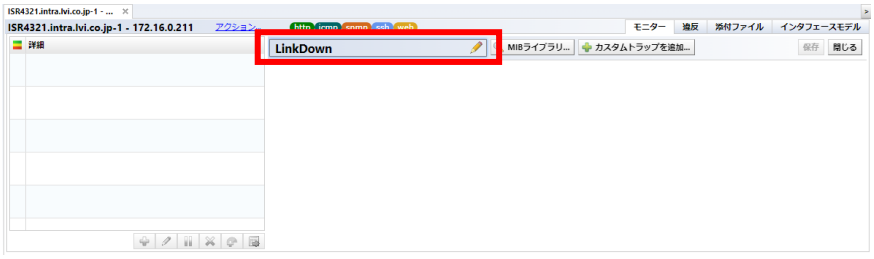
※すべての SNMP トラップを対象として監視を行う方法もあります。詳しくは、「5.3.7 SNMP トラップを監視する（すべて）」を参照してください。

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。

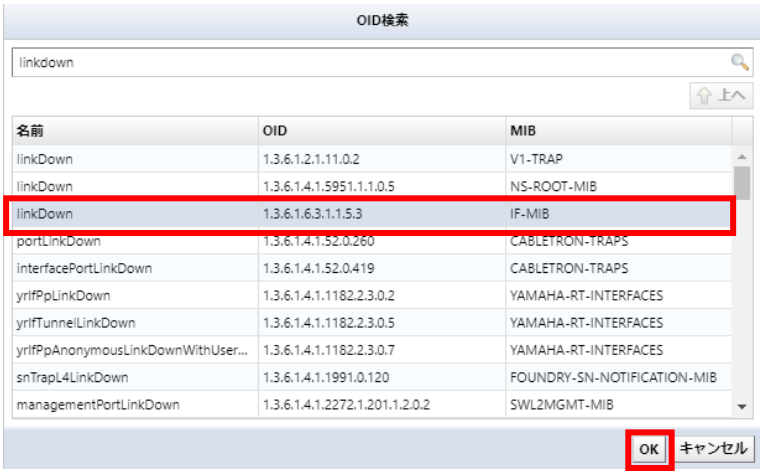
3. 任意のモニター名を入力します。



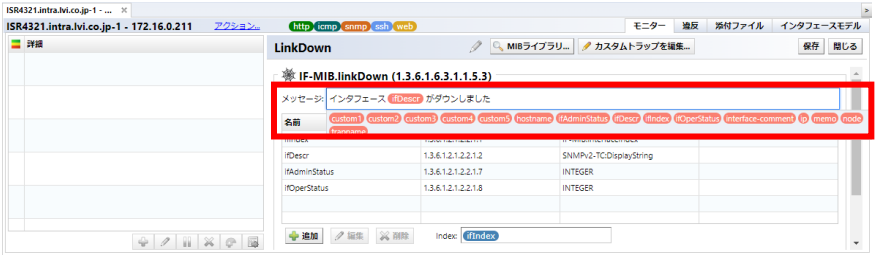
Copyright (C) 2026 LogicVein, Inc.

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。

Copyright (C) 2026 LogicVein, Inc.

8. 以下の項目を入力します。

項目	説明
条件	［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。 ● 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。

9. ［保存］をクリックします。

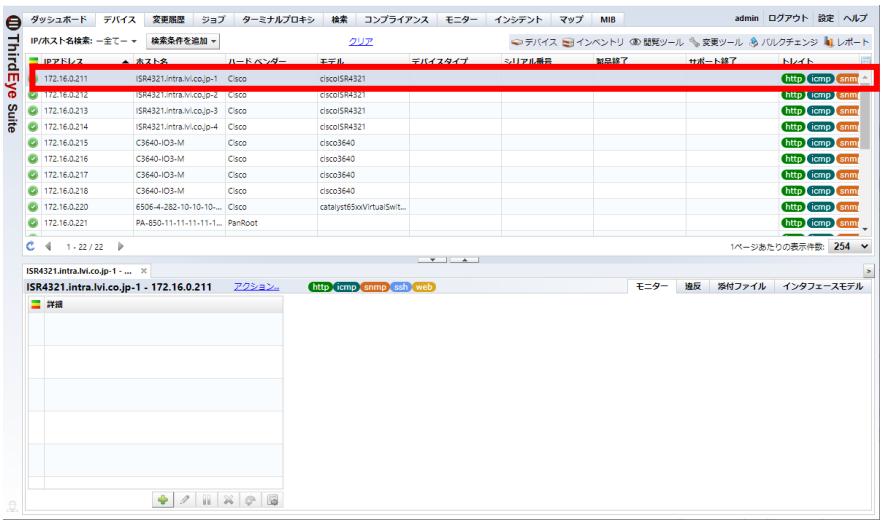
Copyright (C) 2026 LogicVein, Inc.

5.3.7 SNMP トラップを監視する（すべて）

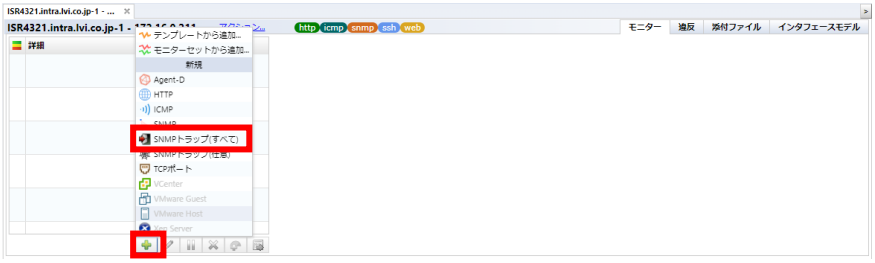
すべての SNMP トラップを対象として監視を行います。「SNMP トラップ(すべて)」をあらかじめ設定しておくことで、SNMP トラップを受信した時に、設定に基づいた共通のアクションを実行できます。監視対象のトラップがはっきりと決まっていない場合、または、すべての SNMP トラップを監視してインシデント登録したい場合に使用すると便利です。

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。



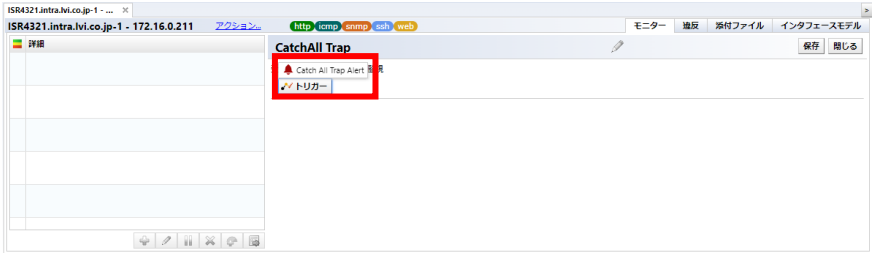
2. 左下の［+(追加)］をクリックし、「SNMP トラップ(すべて)」をクリックします。



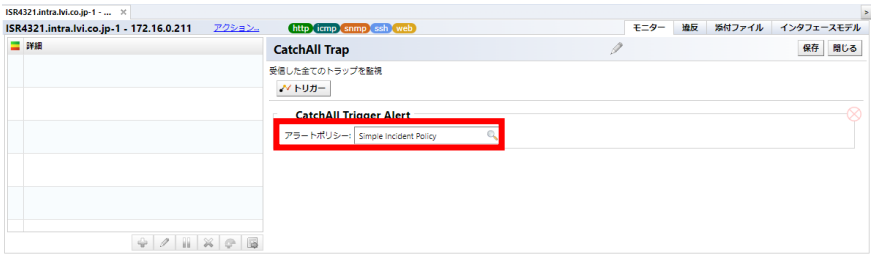
3. 任意のモニター名を入力します。

Copyright (C) 2026 LogicVein, Inc.

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。

Copyright (C) 2026 LogicVein, Inc.

5.3.8 モニターステータスレポート

モニターステータスレポートより、ThirdEye 監視システムが正常に機能していることを簡単に確認する事ができます。レポートではデバイスを選択すると、各デバイスに関連付けられたモニターごとに単一のステータス行が表示されます。「ポーリング」方式のモニターのみが含まれ、Agent-D や SNMP トラップモニターは含まれません。レポートの形式は Excel と CSV です。

	A	B	C	D	E	F	G	H	I
1	ステータス	IPアドレス	ホスト名	管理ネット	モニター	モニターセット	インターバル	遅延秒	最終更新日時
2	正常	10.0.0.249	Test20250704rev	Default	Cisco CPU使用率	Cisco	60		2025-10-27 10:03:21.217
3	正常	10.0.0.249	Test20250704rev	Default	Cisco IOS - メモリ使用率	Cisco	300		2025-10-27 09:59:07.241
4	正常	10.0.0.249	Test20250704rev	Default	Cisco CPU使用率	<無し>	60		2025-10-27 10:03:46.212
5	正常	10.0.0.249	Test20250704rev	Default	ifInErrors(1.3.6.1.2.1.2.2.1.14)	<無し>	60		2025-10-27 10:03:14.193

このレポートは、デバイスの直近のポーリング期間内に保存されたデータがあるかどうかを確認することで機能します。例えば、ポーリング間隔が 30 秒の ICMP モニターでは、少なくとも 30 秒ごとに何らかのデータが保存されていることが想定されます。本レポートでは、「応答なし」のデータポイントも正常と判断するのに十分なものとみなします。レポートの目的は、デバイス自体の健全性を判断することではなく、ThirdEye 監視サブシステムが適切に動作していることを確認することにあります。

SNMP トラップや Agent-D syslog などのプッシュ型モニターのデータは含まれません。これらのモニターは定期的なスケジュールで実行されないため、本レポートがモニターの健全性を判断する際に使用するロジックが適用されない為です。検索条件に基づいてデバイスが見つからない場合、または選択したデバイスに該当するモニターが存在しない場合、レポートは空になります。レポートが空の場合、メールは送信されません。

モニターのステータス

項目	説明
一時停止	デバイスに関連付けられたモニターは一時停止状(手動)になっています。
非監視	非監視が有効になっているため、データは収集されていません。
未取得	これまでに一度もデータが取得されたことがありません。
遅延	遅延が発生しているか、監視が正常に動作していません。
正常	監視は正常に動作しています。

	A	B	C	D	E	F	G	H	I
1	ステータス	IPアドレス	ホスト名	管理ネット	モニター	モニターセット	インターバル	遅延秒	最終更新日時
251	正常	10.0.100.7	qa-autotest-device	Default	Cisco IOS - メモリ使用率	Cisco	300		2025-10-24 13:54:38.125
252	正常	10.0.100.7	qa-autotest-device	Default	Cisco CPU使用率	Cisco	60		2025-10-24 13:56:45.161
253	遅延	10.10.45.254	LVI-L3-GW.intra.lvi.co.jp	Default	Cisco CPU使用率	Cisco	60	10179	2025-10-24 11:08:06.168
254	一時停止	10.10.45.254	LVI-L3-GW.intra.lvi.co.jp	Default	ICMP Ping	Cisco	30	10163	2025-10-24 11:08:22.131
255	遅延	10.10.45.254	LVI-L3-GW.intra.lvi.co.jp	Default	Cisco IOS - メモリ使用率	Cisco	300	10426	2025-10-24 11:03:59.129

モニターが正常でない場合、遅延秒数には前回の収集試行からの経過秒数が表示されます。また、最終更新日時には成功した収集試行日時と失敗した収集試行日時の両方が含まれています。

Copyright (C) 2026 LogicVein, Inc.

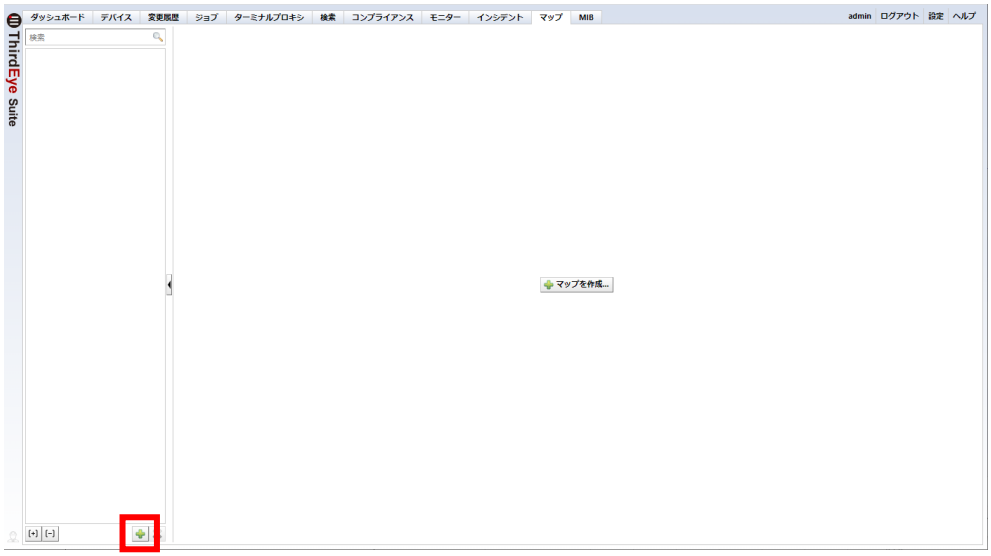
5.4　マップを設定する

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すことができます。

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. マップ名を入力し、［OK］をクリックします。

※ 現在のユーザが複数の管理ネットワークにアクセスできる場合、この画面には、マップに関連付ける管理ネットワークを明示的に選択するオプションが表示されます。

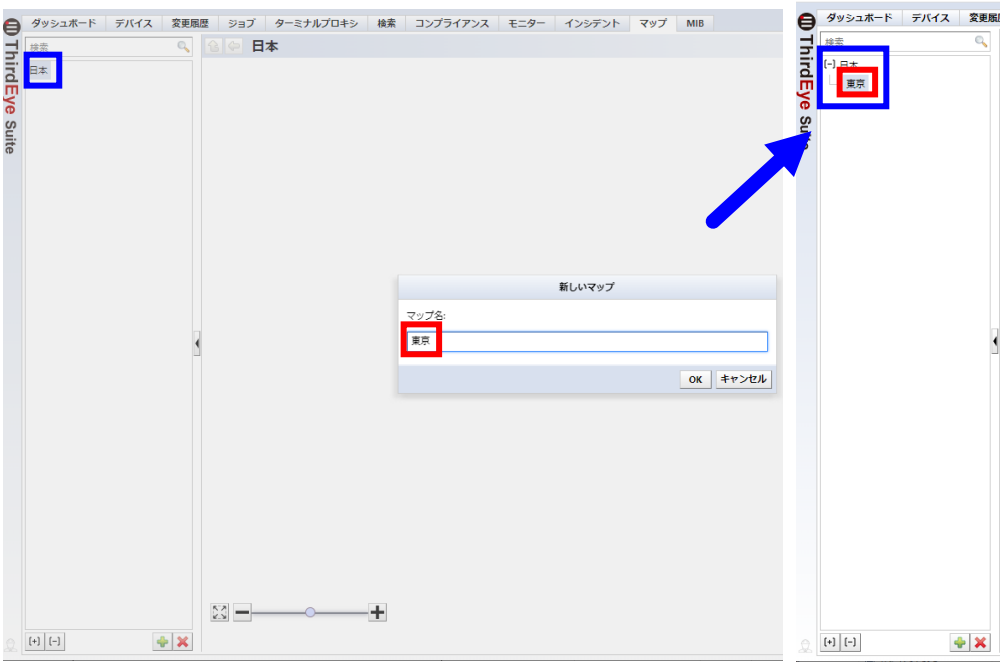
選択された管理ネットワークは、他のユーザがそのマップを表示できるかどうかに影響します。ユーザがマップにアクセスするには、そのマップに関連付けられたすべての管理ネットワークに対するアクセス権が必要です。
マップが他のマップのサブマップとして作成された場合、新しいマップには、上位マップで設定された範囲を超える管理ネットワークを関連付けることはできません。
また、上位マップに含まれていない管理ネットワークが追加された場合は、上位マップが自動的に更新され、必要なネットワークが追加されます。

Copyright (C) 2026 LogicVein, Inc.

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。

補足

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。

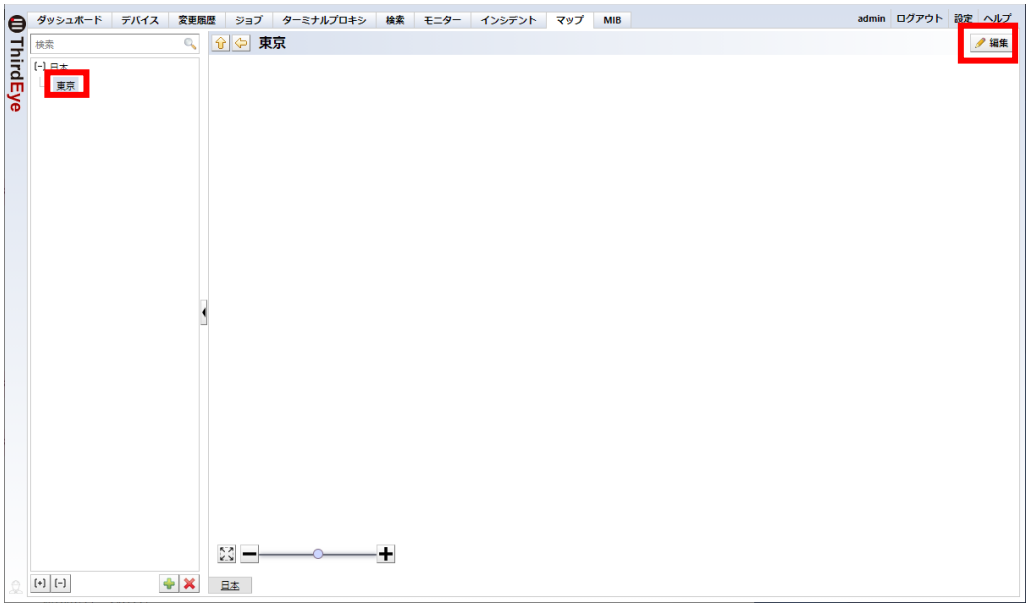


Copyright (C) 2026 LogicVein, Inc.

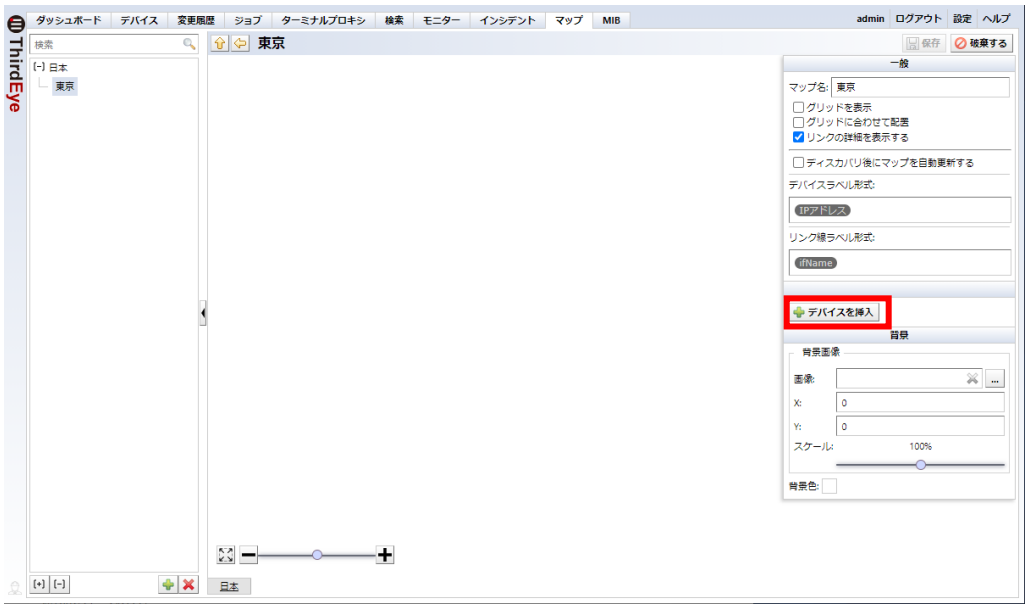
5.4.2 マップにデバイスを挿入する

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。

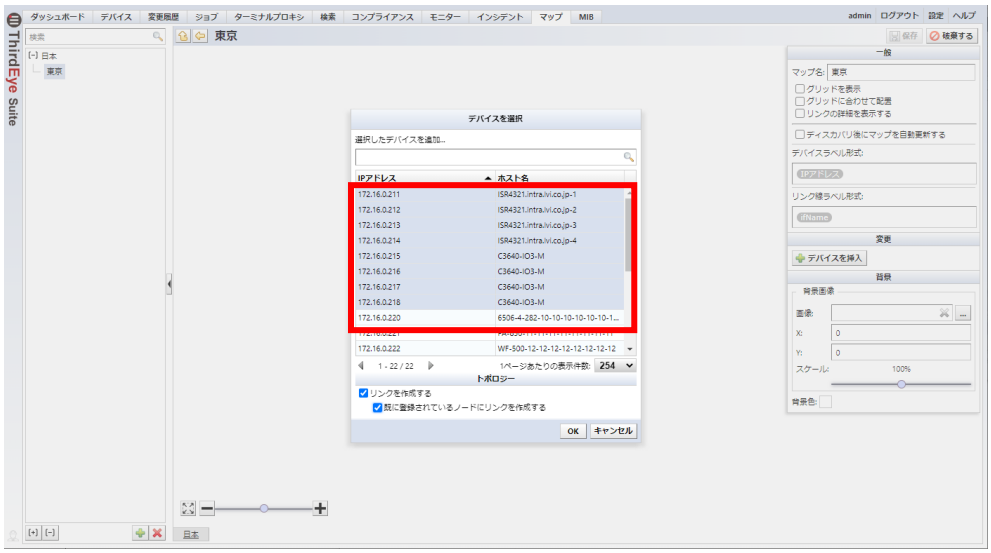


2. ［デバイスを挿入］をクリックします。



Copyright (C) 2026 LogicVein, Inc.

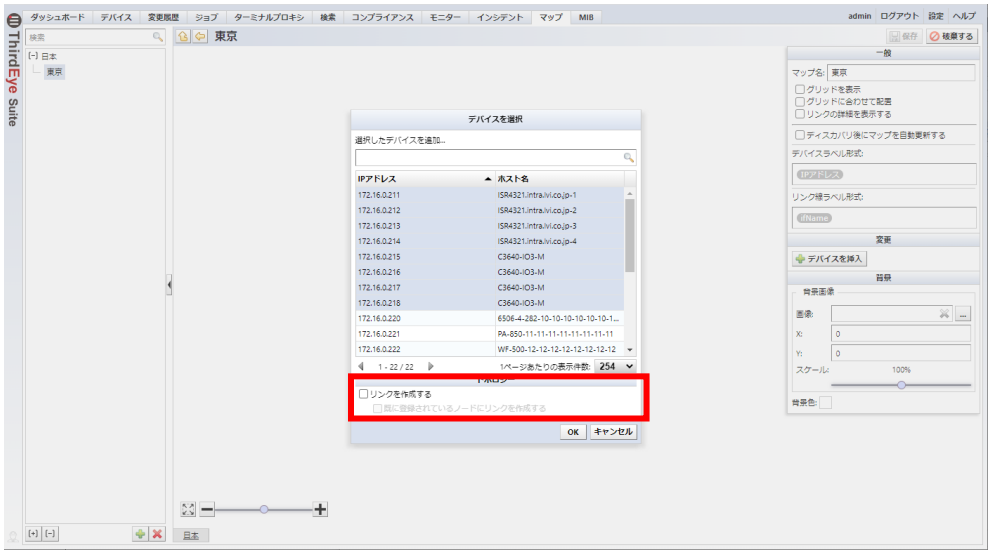
3. マップに挿入するデバイスを選択します。



※ 現在のユーザが複数の管理ネットワークにアクセスできる場合、現在のマップで設定されているネットワークに関わらず、［デバイスを選択］ダイアログには、グローバルメニューで選択されているネットワーク内のデバイスのみが表示されます。まだマップに関連付けられていないネットワークからデバイスを挿入しようした場合は、そのマップに該当のネットワークを追加する必要があります。

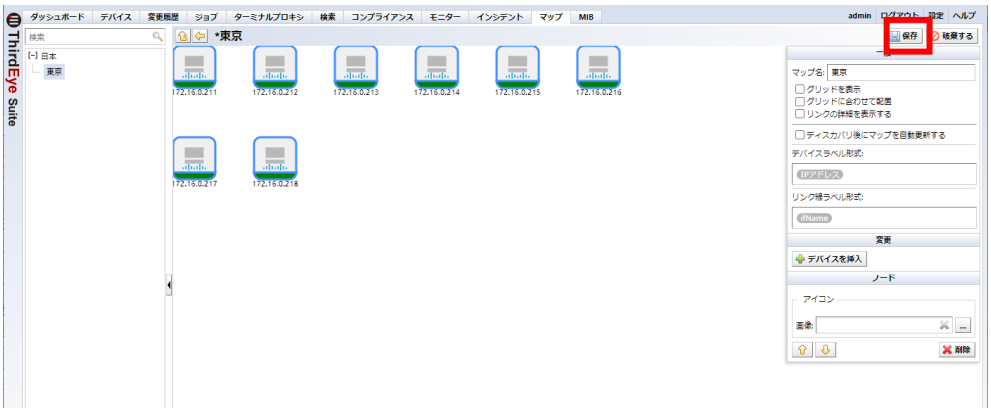
4. ［リンクを作成する］のチェックを外し、［OK］をクリックします。

※［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 マップを自動的に生成する機能です。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。



Copyright (C) 2026 LogicVein, Inc.

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。



Copyright (C) 2026 LogicVein, Inc.

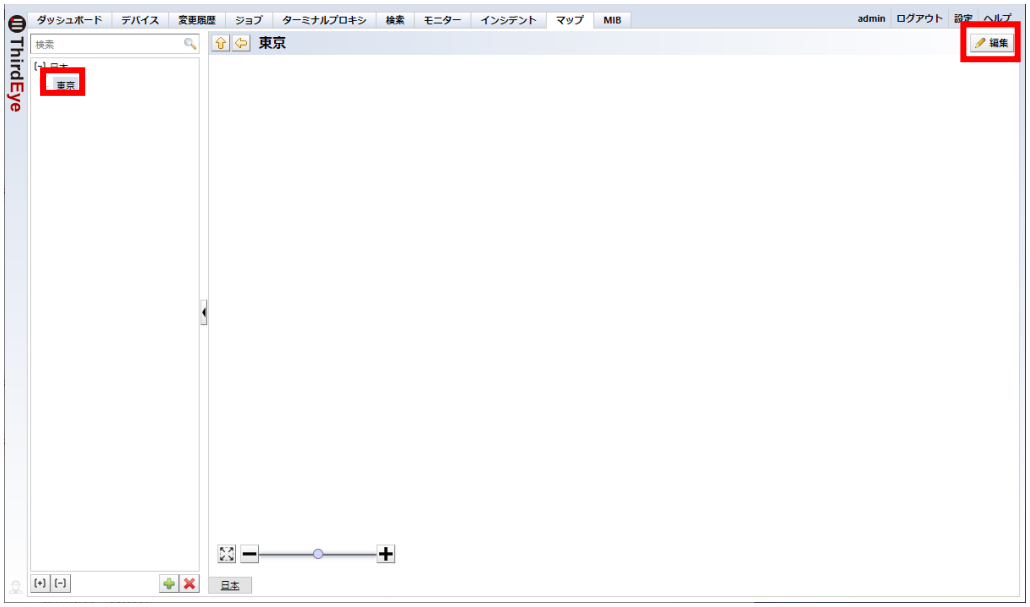
5.4.3 トポロジーマップを作成する

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。

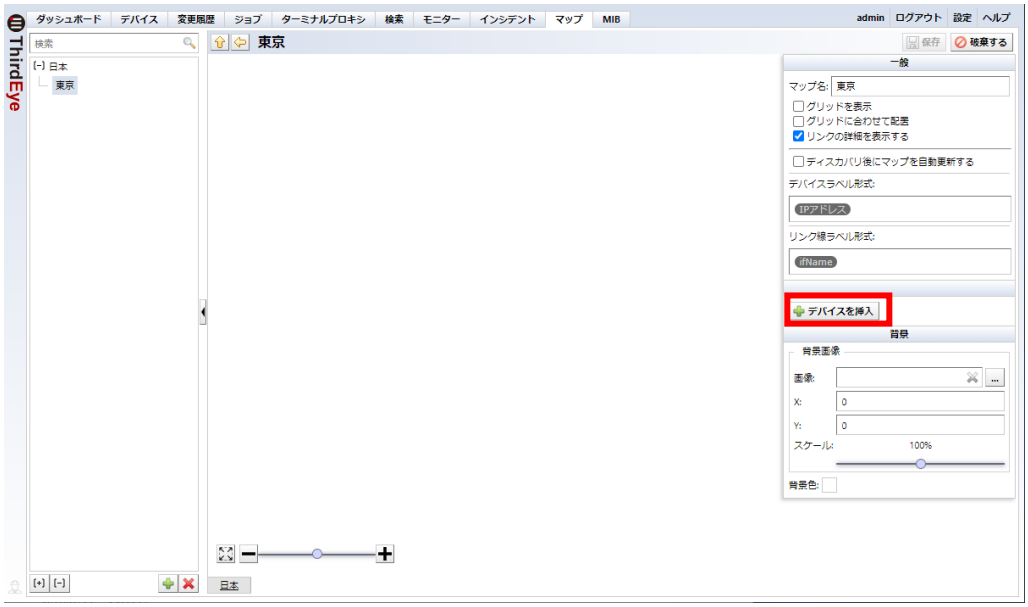
トポロジー機能を利用する場合の注意事項：

- SNMP ポーリングを使用してデバイスから情報を取得できる必要があります。
- 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。

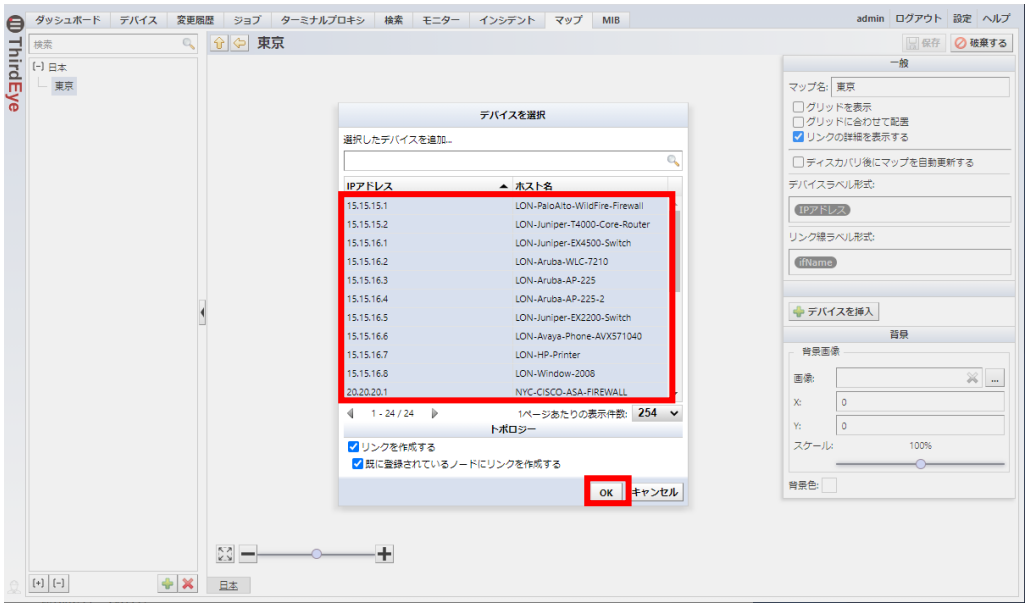


2. ［デバイスを挿入］をクリックします。

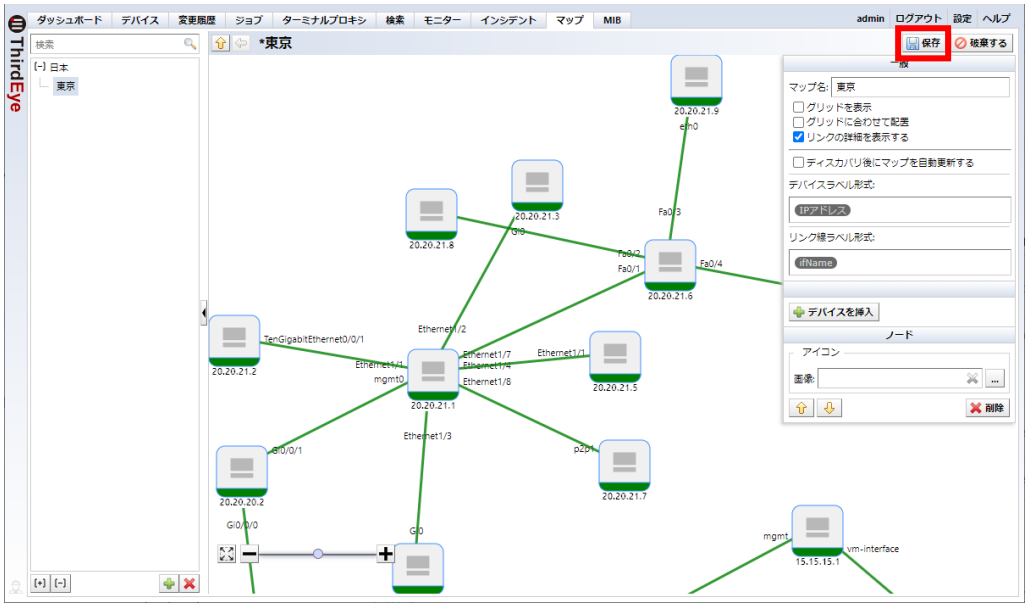


Copyright (C) 2026 LogicVein, Inc.

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。



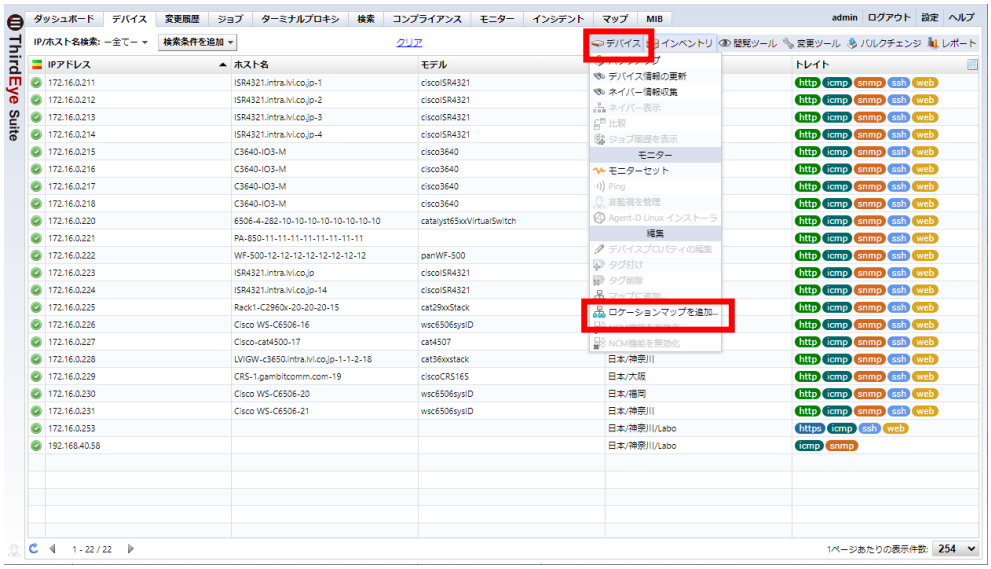
Copyright (C) 2026 LogicVein, Inc.

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】

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。

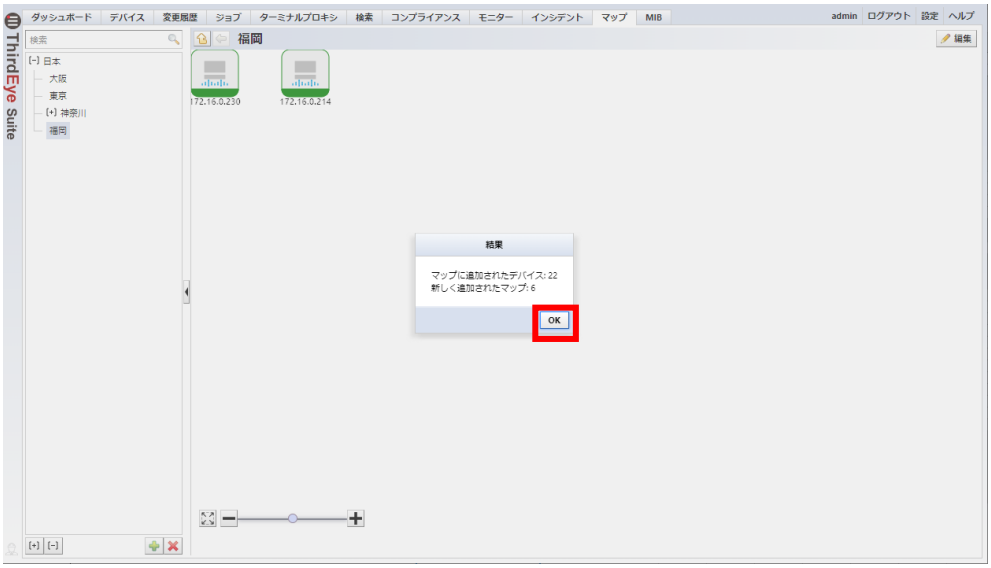


補足	デバイスを選択することで、選択したデバイスを対象にロケーションマップを作成することができます。

Copyright (C) 2026 LogicVein, Inc.

2. カスタムフィールドを選択し、［作成］をクリックします。

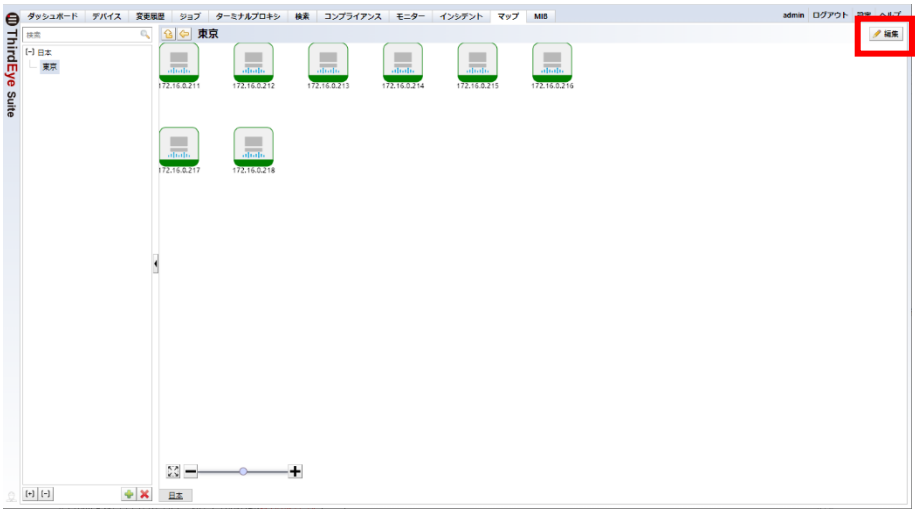
3. ［OK］をクリックします。



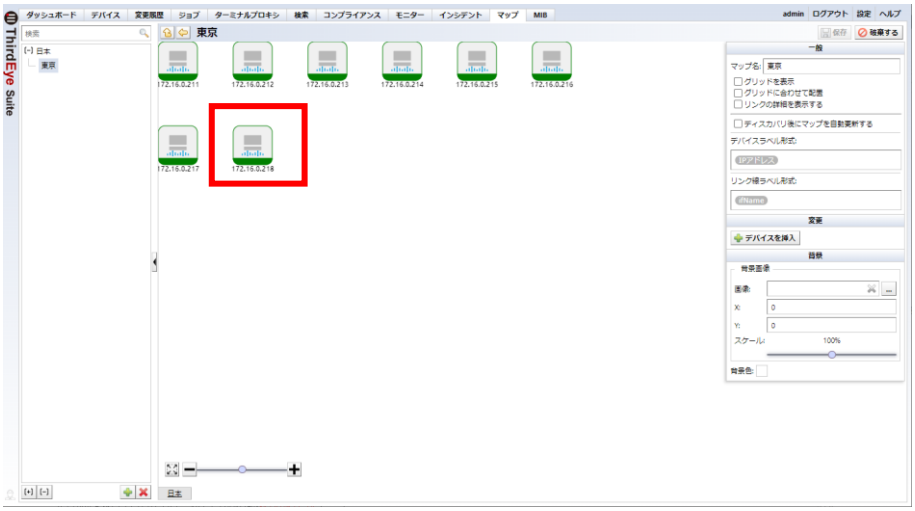
Copyright (C) 2026 LogicVein, Inc.

5.4.5 オブジェクトのアイコンを設定する

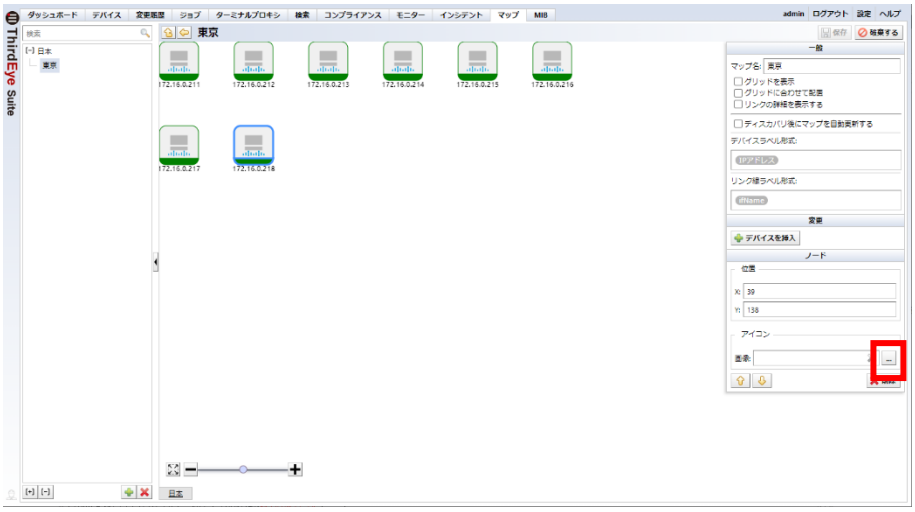
1. マップをダブルクリックで開き、［編集］をクリックします。



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。

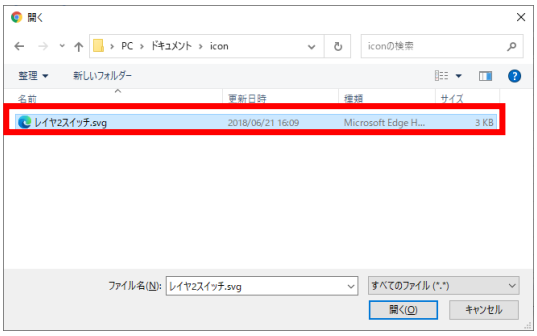


3. 編集メニューの中から、ノードセクションの［画像］欄の右にある［…］をクリックします。

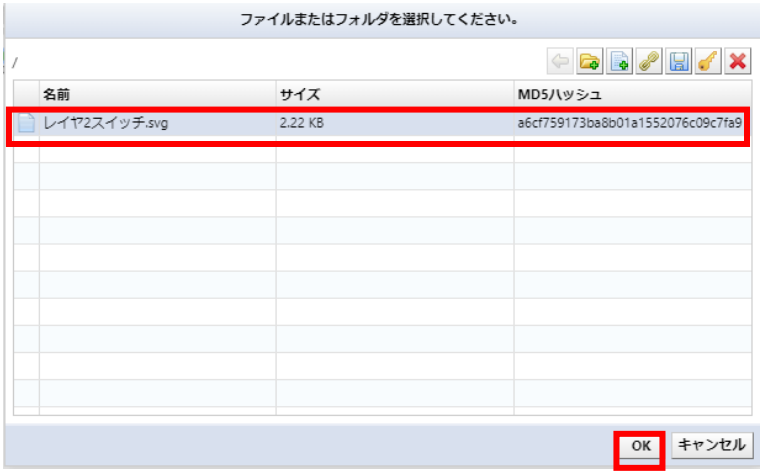


Copyright (C) 2026 LogicVein, Inc.

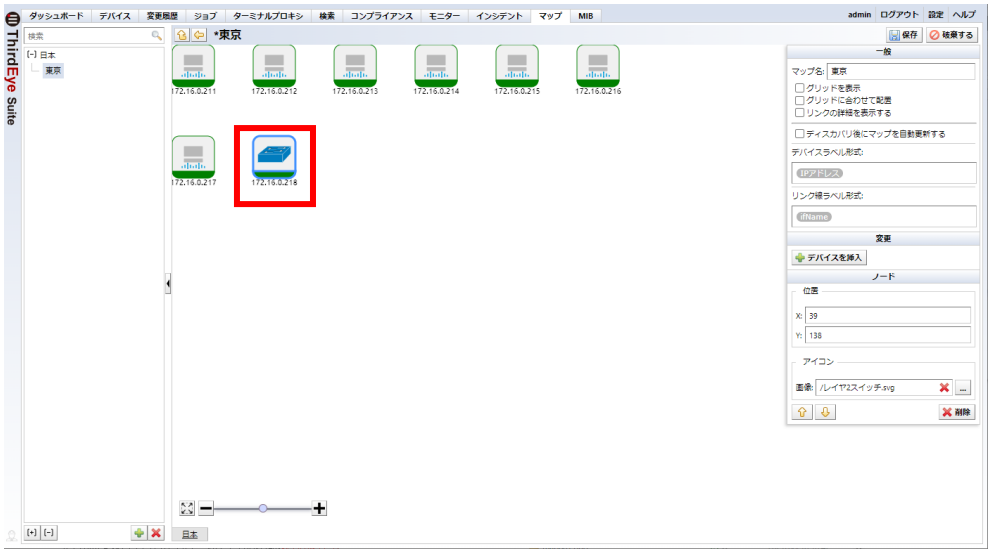
4. ファイルの選択画面が表示されます。［ ］をクリックし、ファイルをアップロードします。



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。



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。



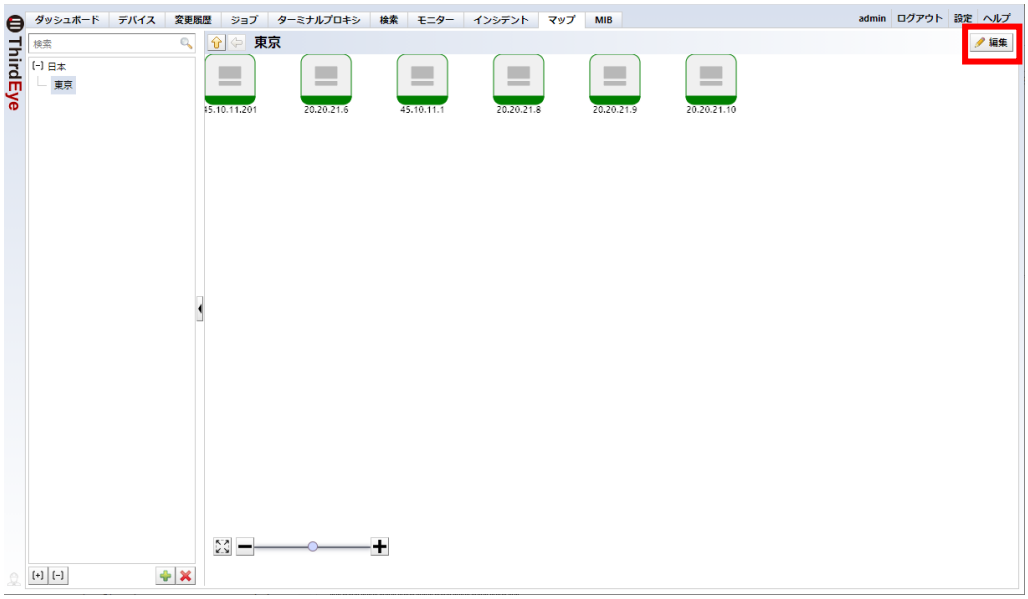
Copyright (C) 2026 LogicVein, Inc.

5.4.6 2 つのオブジェクトの間を線で結ぶ

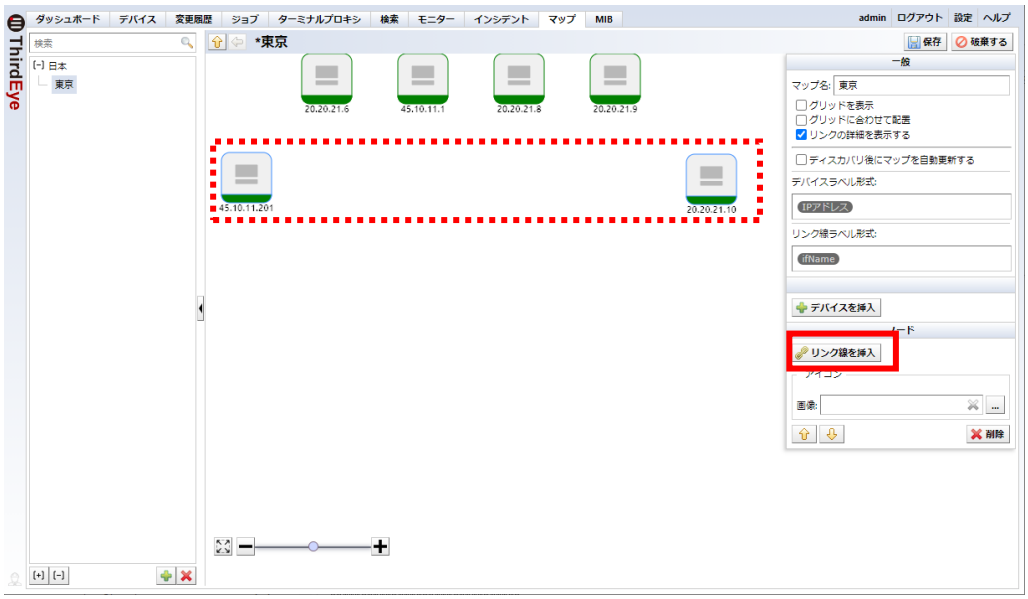
マップやデバイスなどのオブジェクト同士をリンク線でつなぐことができます。

※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。



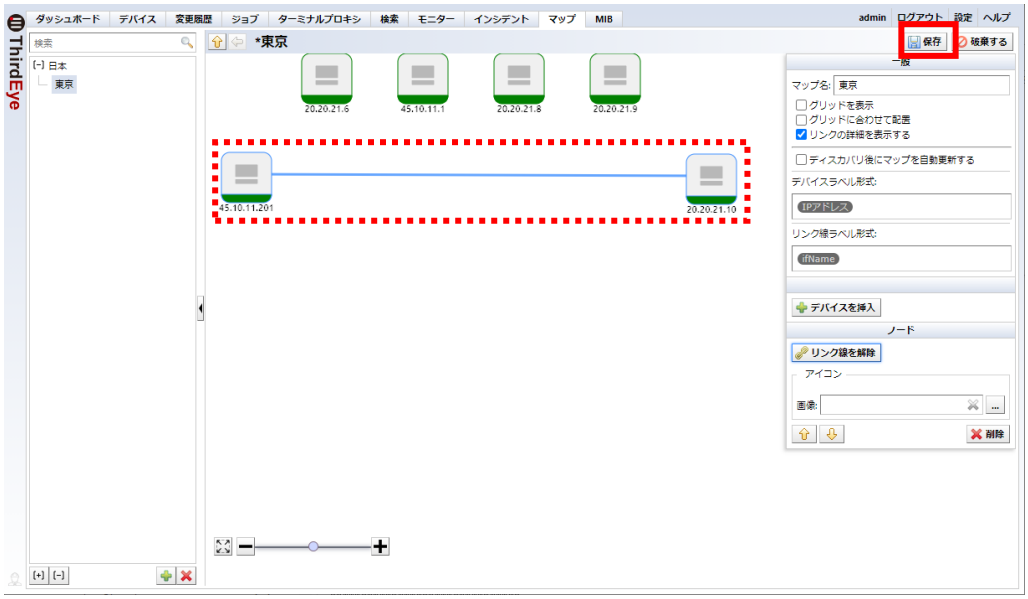
2. キーボードの「Ctrl」キーを押しながら、リンク線でつなぐ 2 つのデバイスをクリックし選択します。デバイスが選択された状態で［リンク線を挿入］をクリックします。



Copyright (C) 2026 LogicVein, Inc.

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。

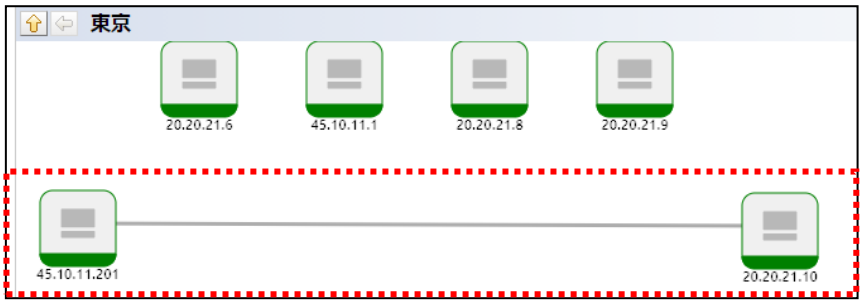


Copyright (C) 2026 LogicVein, Inc.

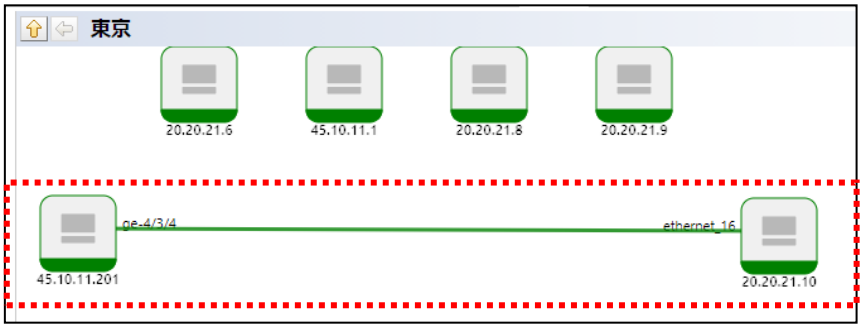
5.4.7 リンク線にインタフェースを紐付ける

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るようになりました。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、障害イベントの重大度に応じて、デバイスオブジェクトだけでなくリンク線の色が変化するようになります。

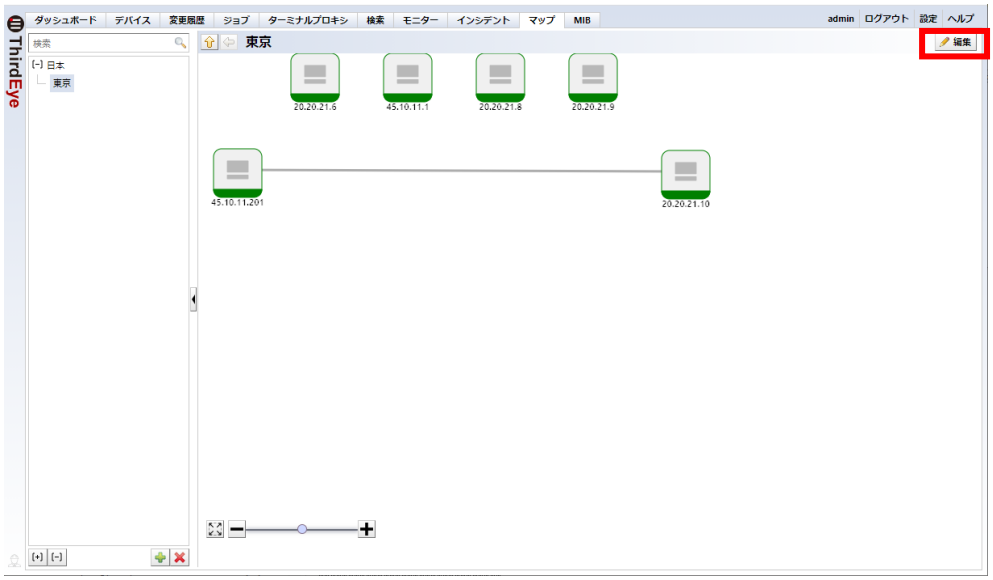
【リンク線にデバイスのインタフェースを紐付けていない状態】



【リンク線にデバイスのインタフェースを紐付けた状態】

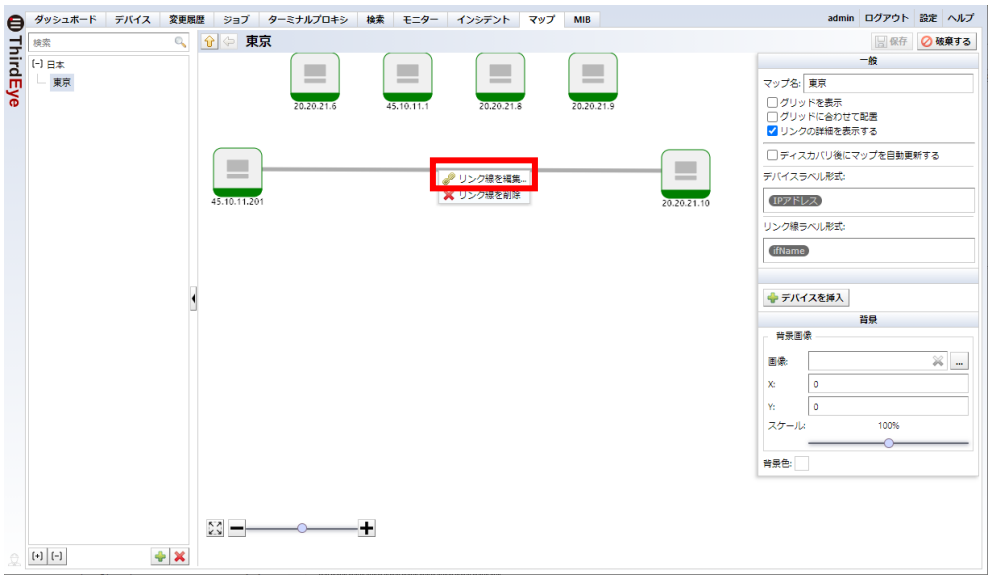


1. マップをダブルクリックで開き、［編集］をクリックします。

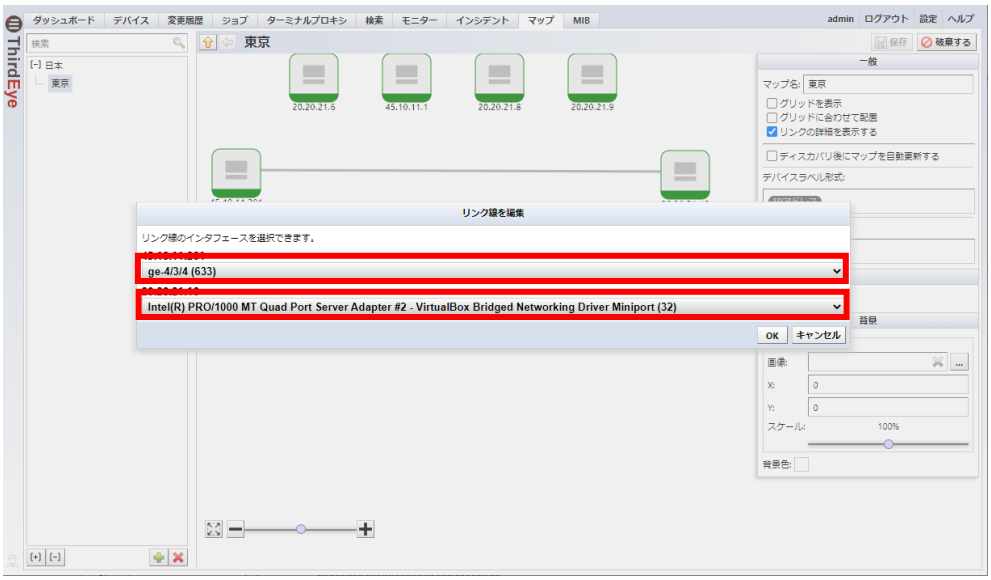


Copyright (C) 2026 LogicVein, Inc.

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。

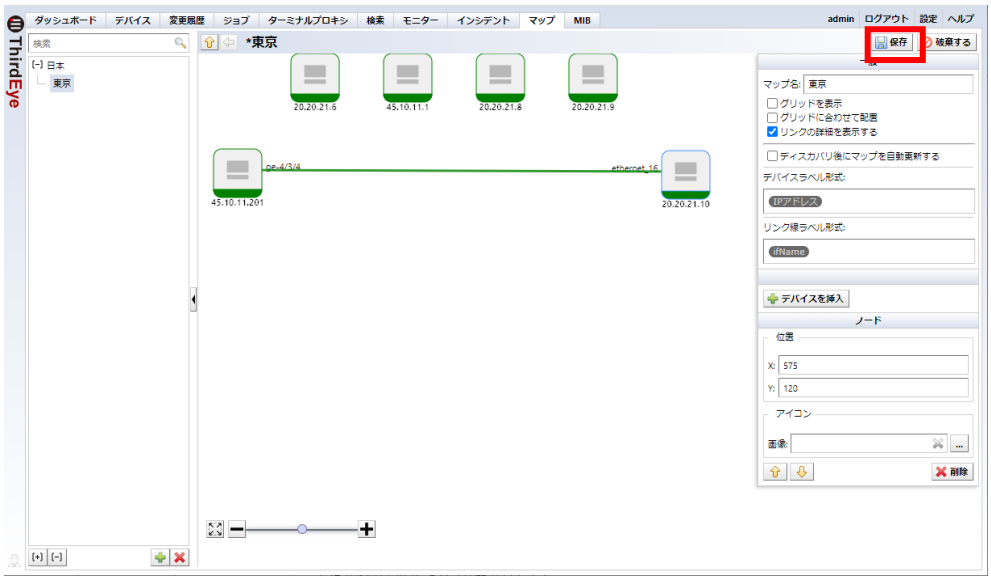


3. 各デバイスのプルダウンメニューからインタフェースを選択し、［OK］をクリックします。



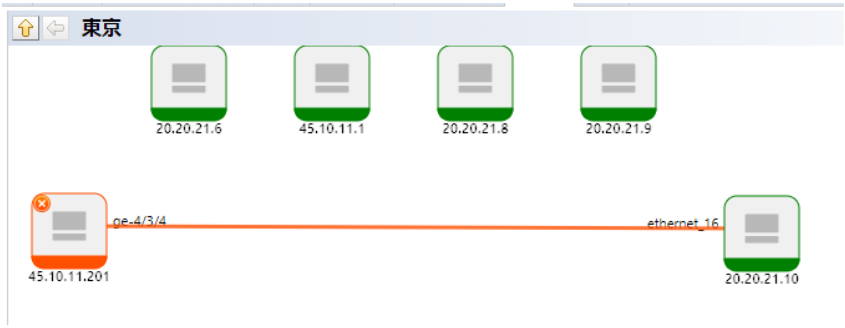
Copyright (C) 2026 LogicVein, Inc.

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。

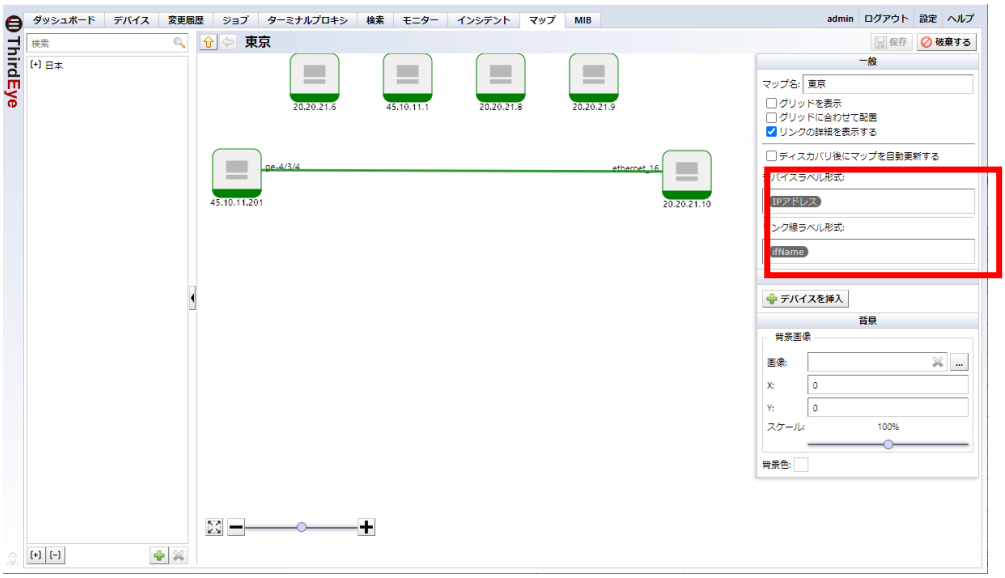


Copyright (C) 2026 LogicVein, Inc.

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】

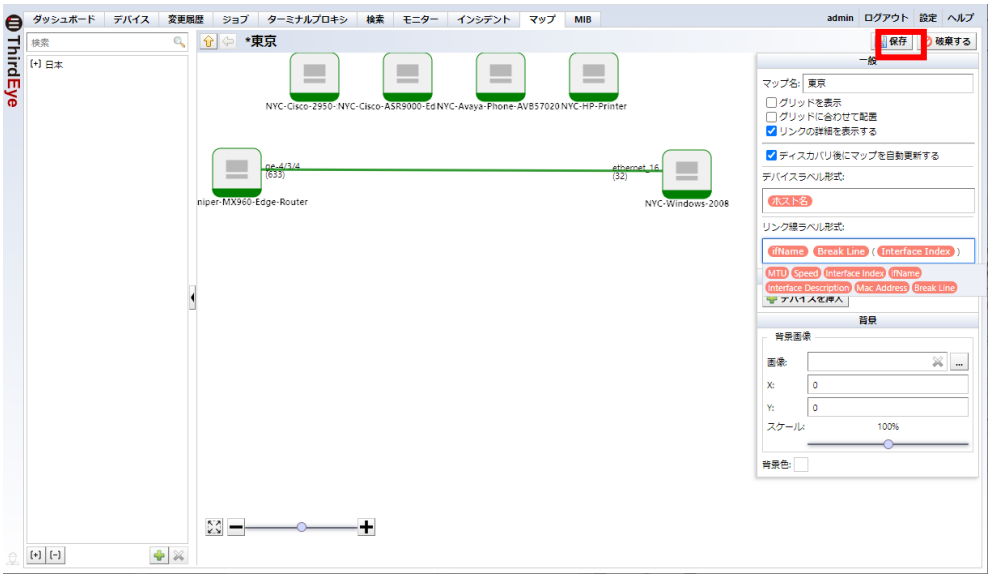
項目	説明
IP アドレス	デバイスの IP アドレスを表示する。（初期値）
ホスト名	デバイスのホスト名を表示する。
ネットワーク	デバイスのネットワークを表示する。
アダプタ	デバイスのアダプタを表示する。
デバイスタイプ	デバイスのデバイスタイプを表示する。
ハードベンダー	デバイスのハードベンダーを表示する。
ソフトベンダー	デバイスのソフトベンダーを表示する。
OS バージョン	デバイスの OS バージョンを表示する。
シリアル番号	デバイスのシリアル番号を表示する。
カスタム 1	デバイスの カスタム 1 の情報を表示する。
カスタム 2	デバイスの カスタム 2 の情報を表示する。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

Copyright (C) 2026 LogicVein, Inc.

【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	ifDesrc 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。



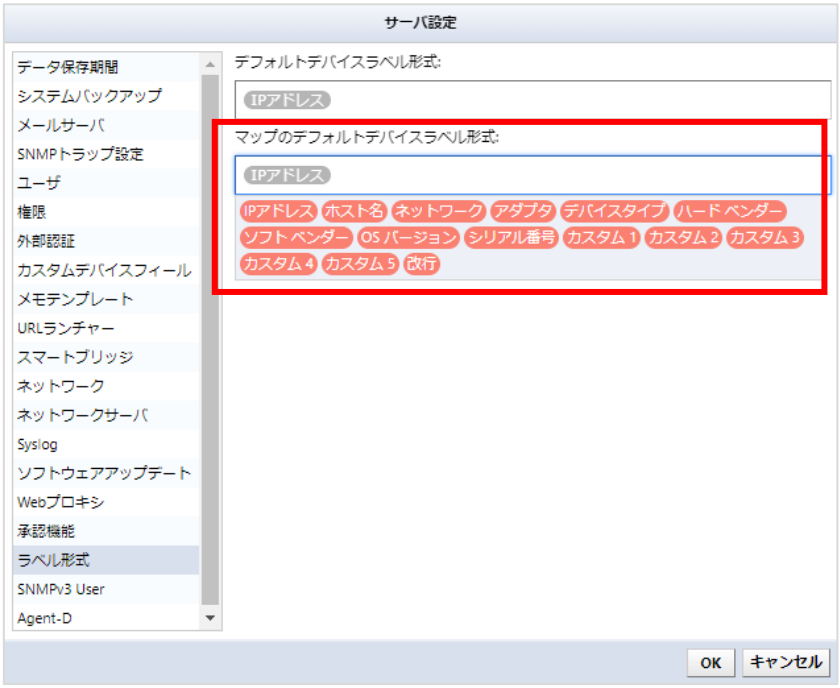
Copyright (C) 2026 LogicVein, Inc.

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

新しいマップを作成する時の、デフォルトのデバイス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スラベル形式」にラベル形式を設定します。



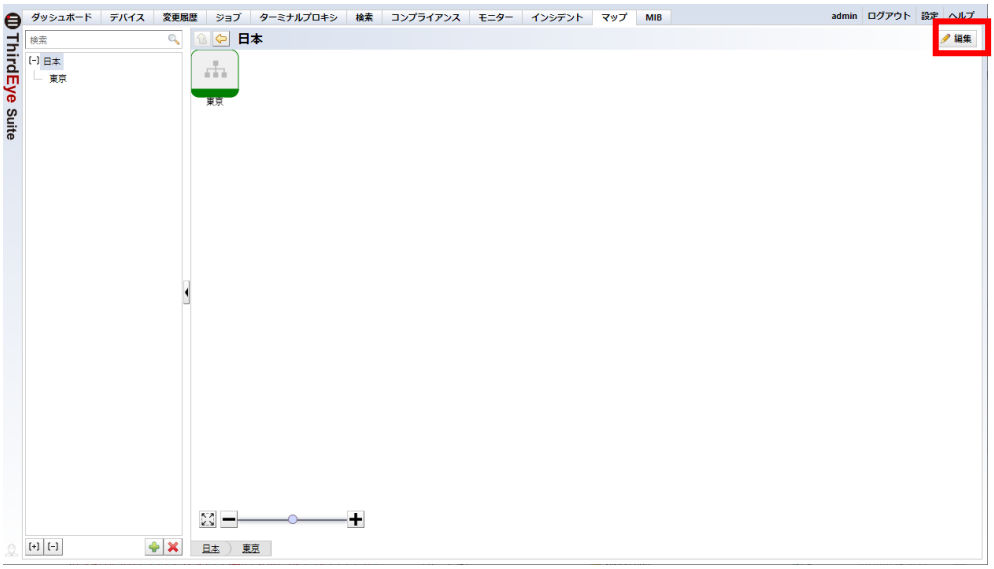
補足	グレーで表示される「IP アドレス」は、初期値であることを意味します。 「デフォルトデバイスラベル形式」は、マップに加えて、Live Ping 機能のラベル形式に使用されます。

Copyright (C) 2026 LogicVein, Inc.

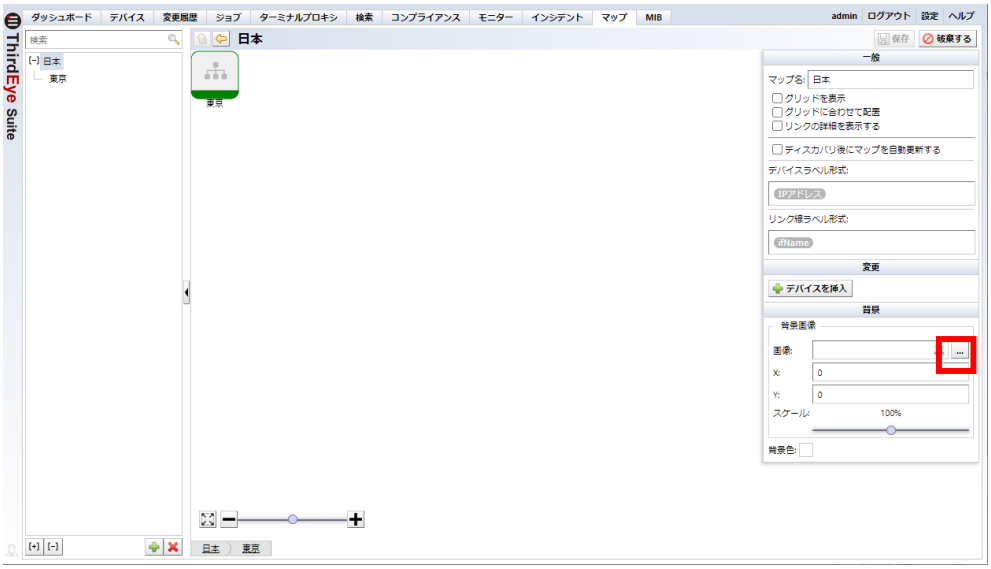
5.4.10 マップの背景画像を設定する

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。

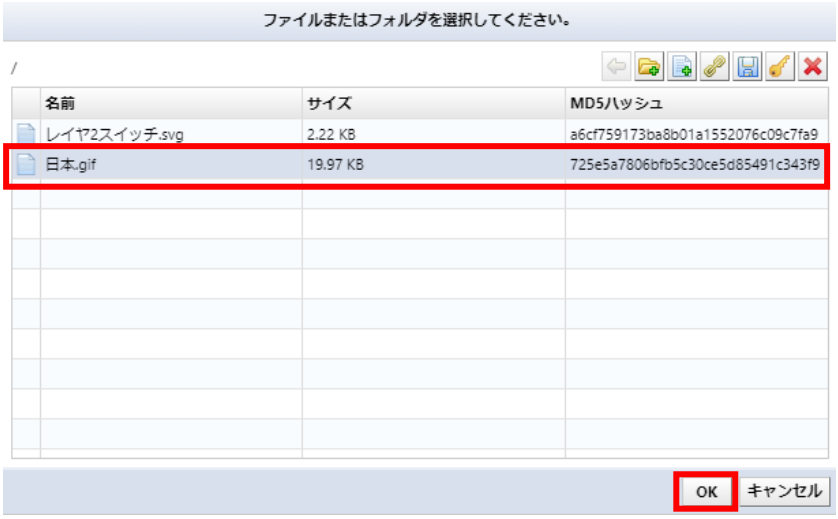


2. 画面右側の設定メニューの中から、背景セクションの［画像］欄の右にある［…］をクリックします。



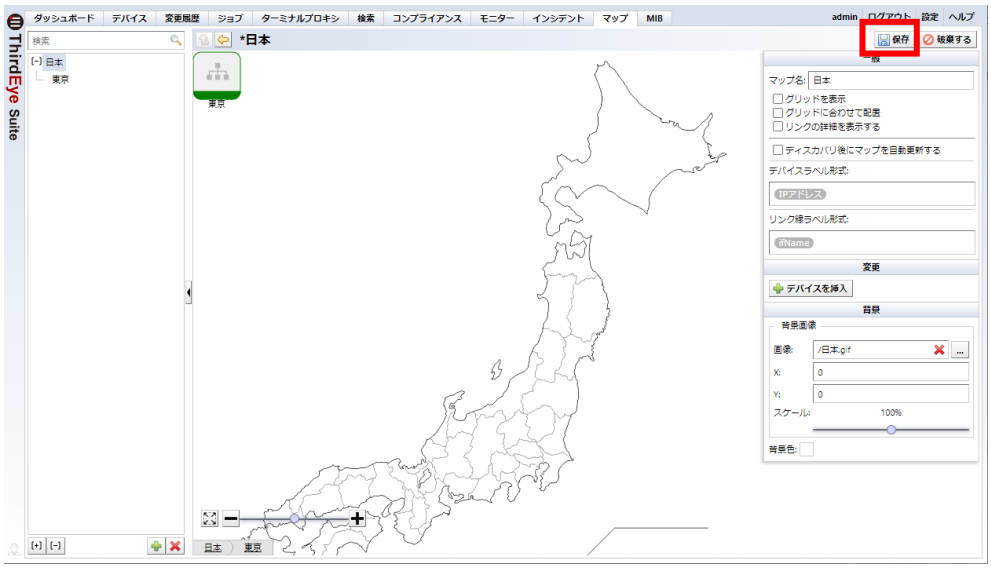
Copyright (C) 2026 LogicVein, Inc.

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。

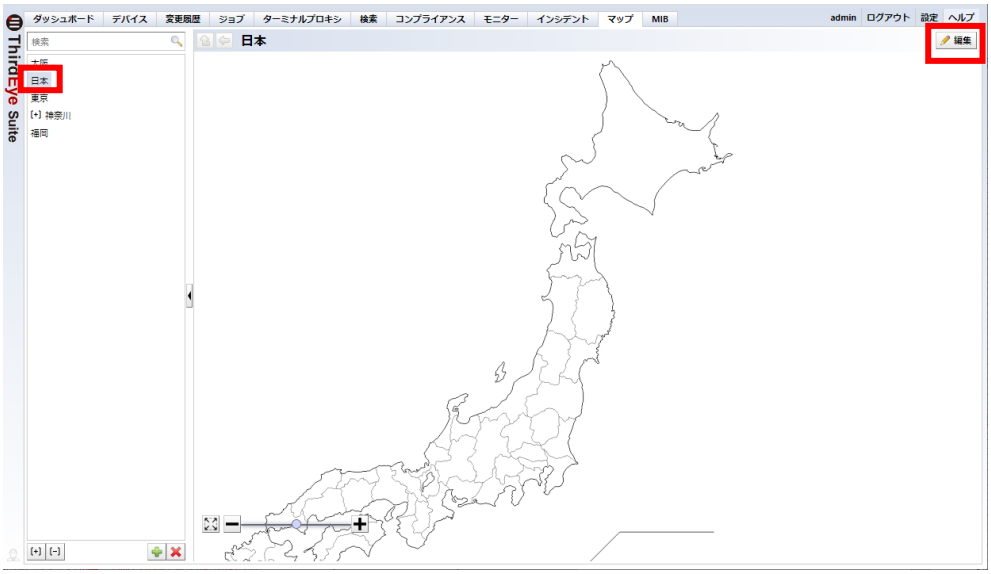


Copyright (C) 2026 LogicVein, Inc.

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には、上位階層となるマップに下位階層の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、上位階層とするマップをダブルクリックして開き、［編集］をクリックします。



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

Copyright (C) 2026 LogicVein, Inc.

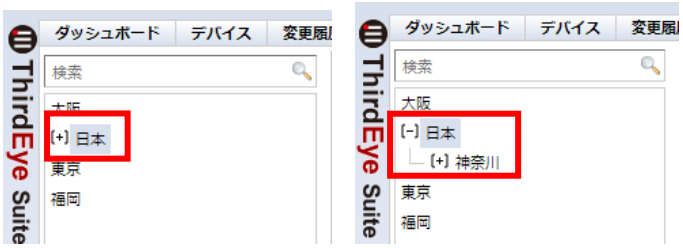
3. 下位階層として挿入するマップを選択し、［OK］をクリックします。

※ 選択したマップが、現在のマップにまだ設定されていない管理ネットワークに関連付けられている場合は、該当のネットワークを現在のマップとその上位マップに追加する必要があります。

4. 下位階層のマップがオブジェクトとして挿入されます。［保存］をクリックして編集を完了します。

階層構造が作成されると、画面左側のマップ一覧は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。



Copyright (C) 2026 LogicVein, Inc.

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。

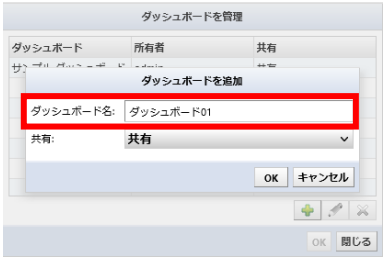
5.5.1 ダッシュボードを追加する

1. ［ダッシュボード］タブの下にある ”ダッシュボード名”（下図では、”サンプル ダッシュボード”）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。

Copyright (C) 2026 LogicVein, Inc.

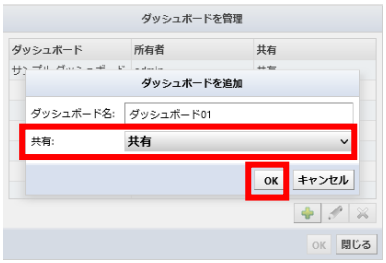
3. ダッシュボード名を入力します。



※ 現在のユーザが複数の管理ネットワークにアクセスできる場合、この画面には、ダッシュボードに関連付ける管理ネットワークを明示的に選択するオプションが表示されます。

選択された管理ネットワークは、他のユーザがそのダッシュボードを閲覧できるかどうかに影響します。ユーザがダッシュボードにアクセスするには、そのダッシュボードに関連付けられたすべての管理ネットワークに対するアクセス権が必要です。

4. 共有でダッシュボードの種類を選択し、［OK］をクリックします。



共有	説明
共有	他のユーザと共有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。

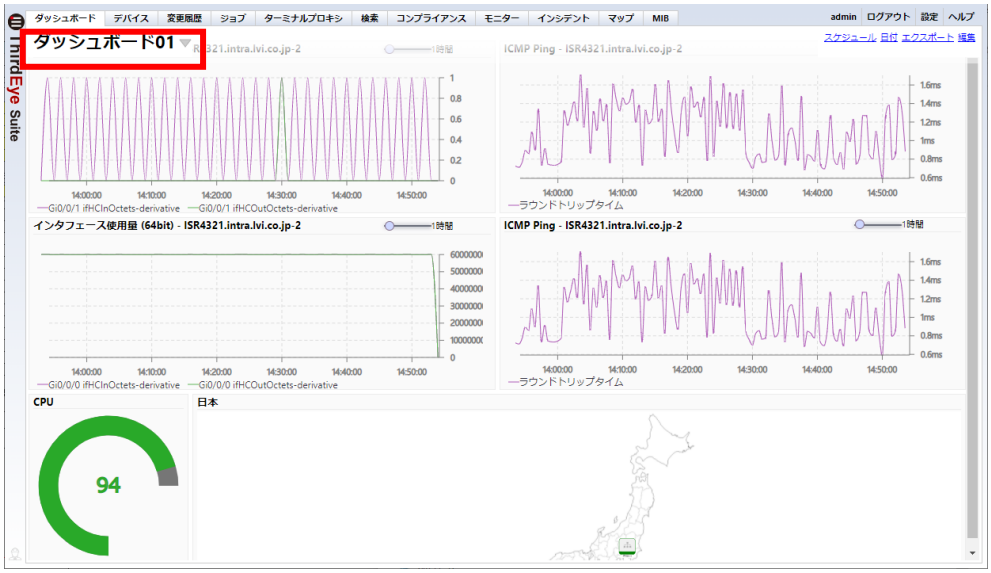
Copyright (C) 2026 LogicVein, Inc.

5.5.2　ダッシュボードを切り替える

1. ［ダッシュボード］タブの下にある ”ダッシュボード名”（下図では、”サンプル ダッシュボード”）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。



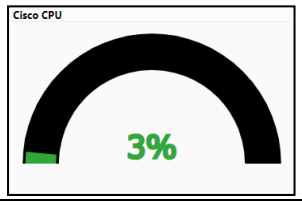
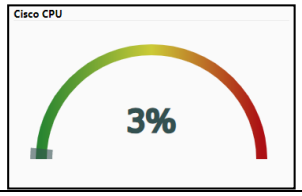
Copyright (C) 2026 LogicVein, Inc.

5.5.3 ウィジェットを追加する

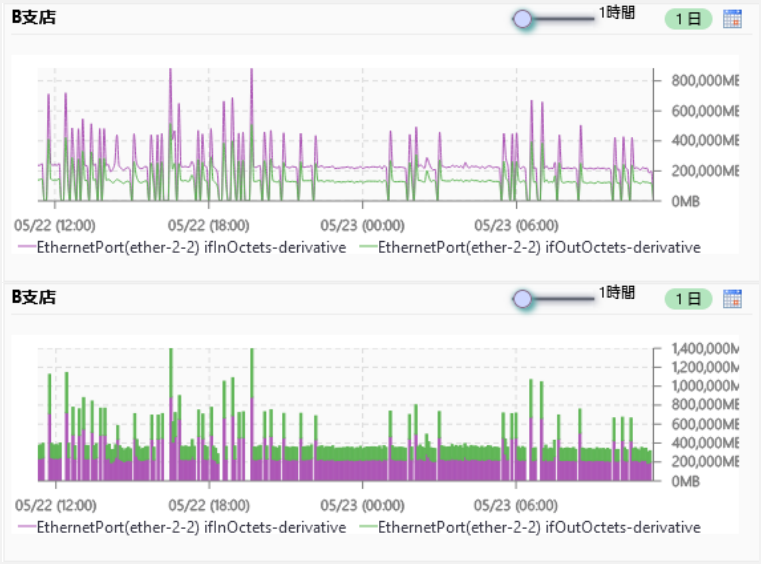
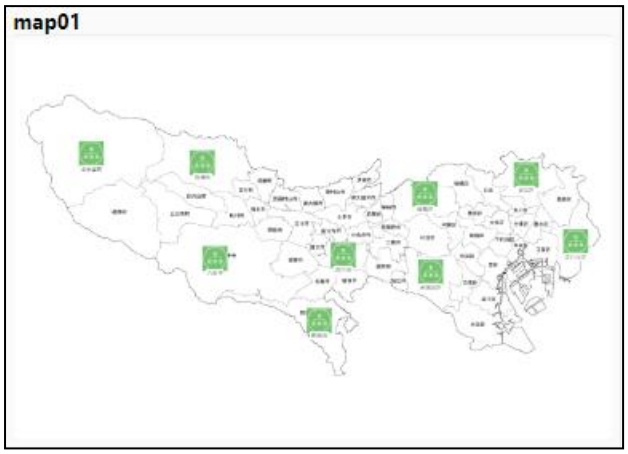
ウィジェットは、ダッシュボードにコンテンツを表示させる構成要素です。ウィジェットをダッシュボードに追加しておくと、見たい情報にすぐにアクセスすることができます。

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。

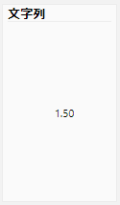
追加できるウィジェットの種類は、以下のとおりです。

ウィジェットの種類	説明
インベントリ	インベントリを表示する。
メーター	メーターグラフを表示する。 【デフォルト】  【温熱性】 

Copyright (C) 2026 LogicVein, Inc.

ウィジェットの種類	説明
グラフ	折れ線グラフ、または積み上げ棒グラフを選択し表示する。 
マップ	マップを表示する。 
違反	違反を表示する。 違反 S. 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 5 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 6 21/12/13 11:44.00 2 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 2 21/12/13 11:41.18 3 21/12/13 11:04.49 21/12/13 11:41.18
テーブル	テーブルを表示する。 テーブル 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

Copyright (C) 2026 LogicVein, Inc.

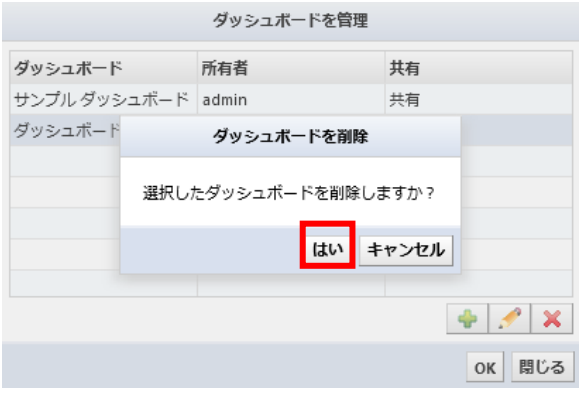
ウィジェットの種類	説明
文字列	文字列を表示する。 
画像	画像を表示する。

5.5.4 ダッシュボードを削除する

1. ［ダッシュボード］タブの下にある ”ダッシュボード名”（下図では、”サンプル ダッシュボード”）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。



Copyright (C) 2026 LogicVein, Inc.

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	表示されているダッシュボードを PDF 形式でエクスポートします。 ※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。

Copyright (C) 2026 LogicVein, Inc.

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。

Copyright (C) 2026 LogicVein, Inc.

6. 運用操作

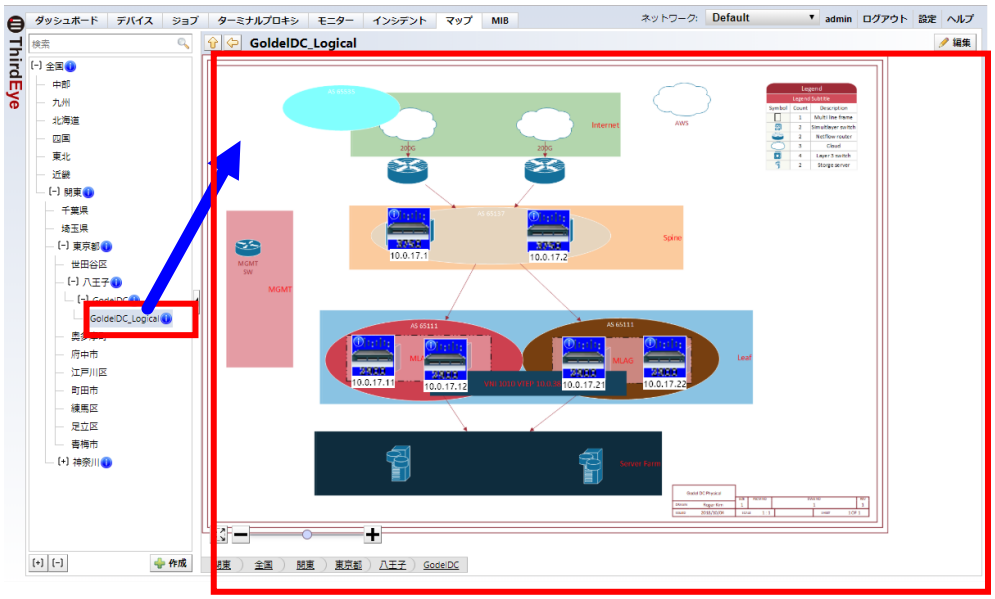
ここでは、日々の運用で使用する操作を記載しています。

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化すると、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。



Copyright (C) 2026 LogicVein, Inc.

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。

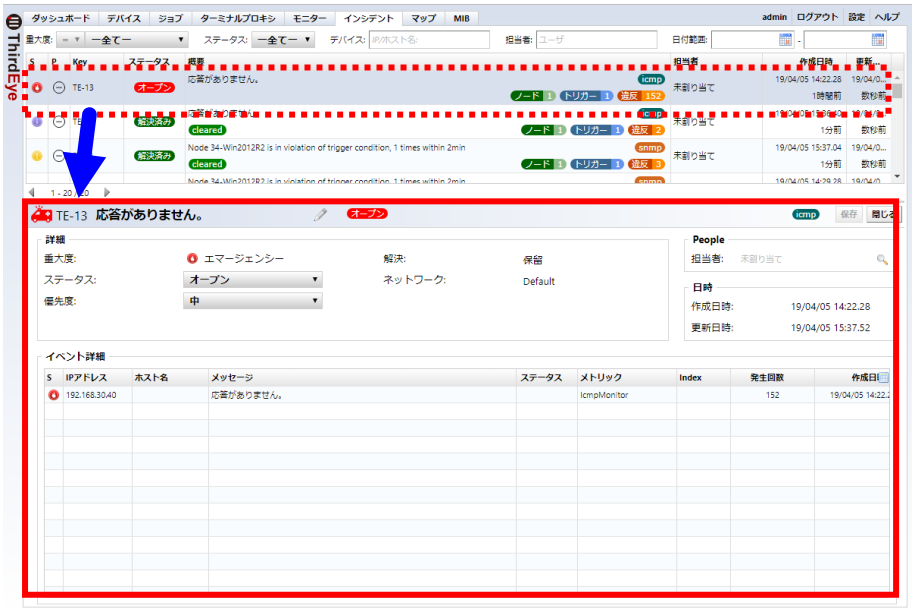
Copyright (C) 2026 LogicVein, Inc.

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。

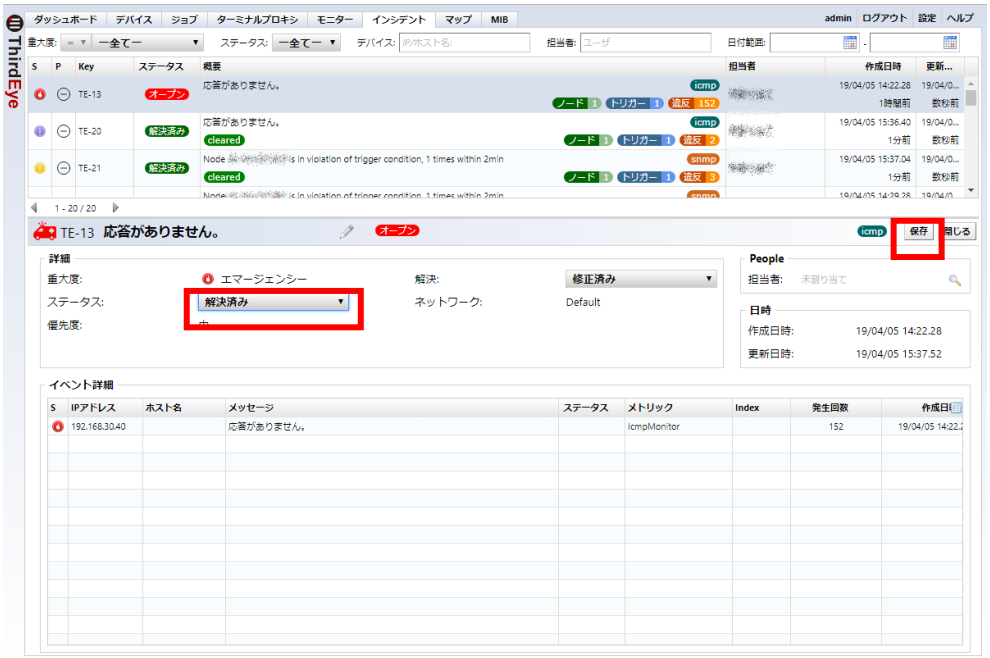
1. 確認したいインシデント行をダブルクリックします。
2. 画面下側にインシデント詳細画面が表示されます。イベント詳細でイベント内容を確認します。



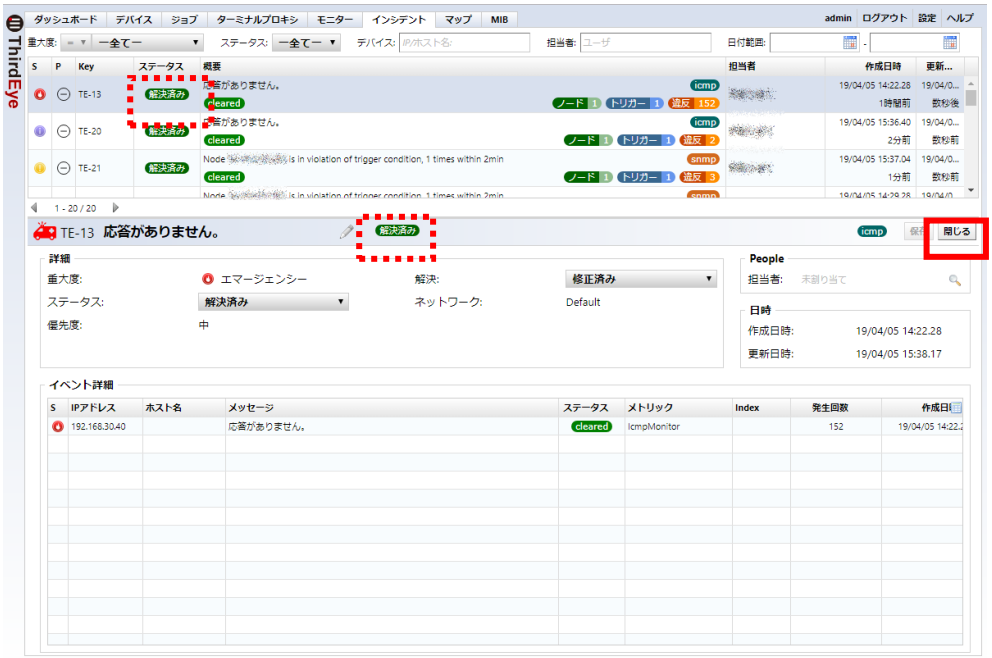
Copyright (C) 2026 LogicVein, Inc.

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。



Copyright (C) 2026 LogicVein, Inc.

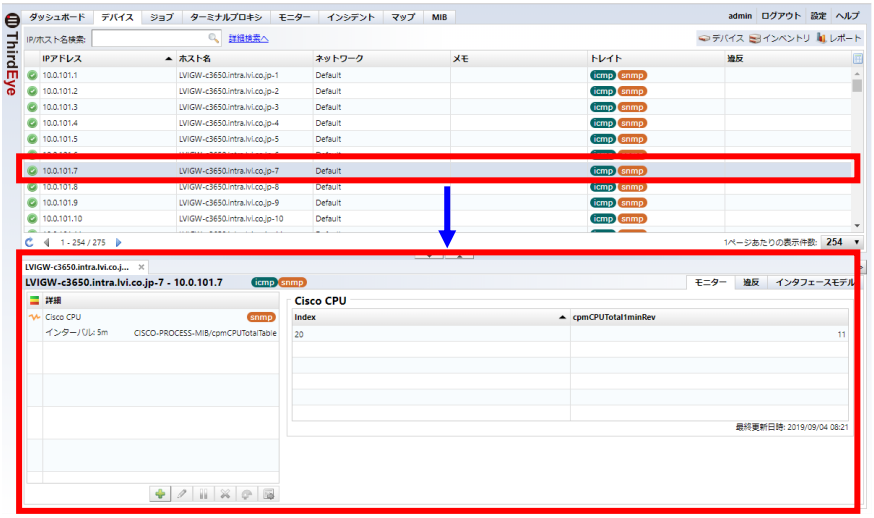
6.2　SNMP で収集したデータを確認する

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したりすることができます。

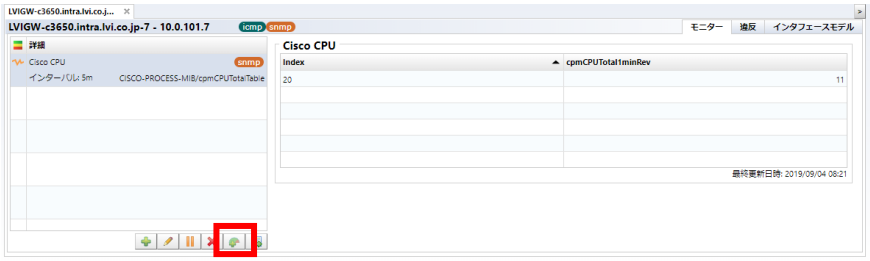
6.2.1 コンソールからグラフを表示する

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。

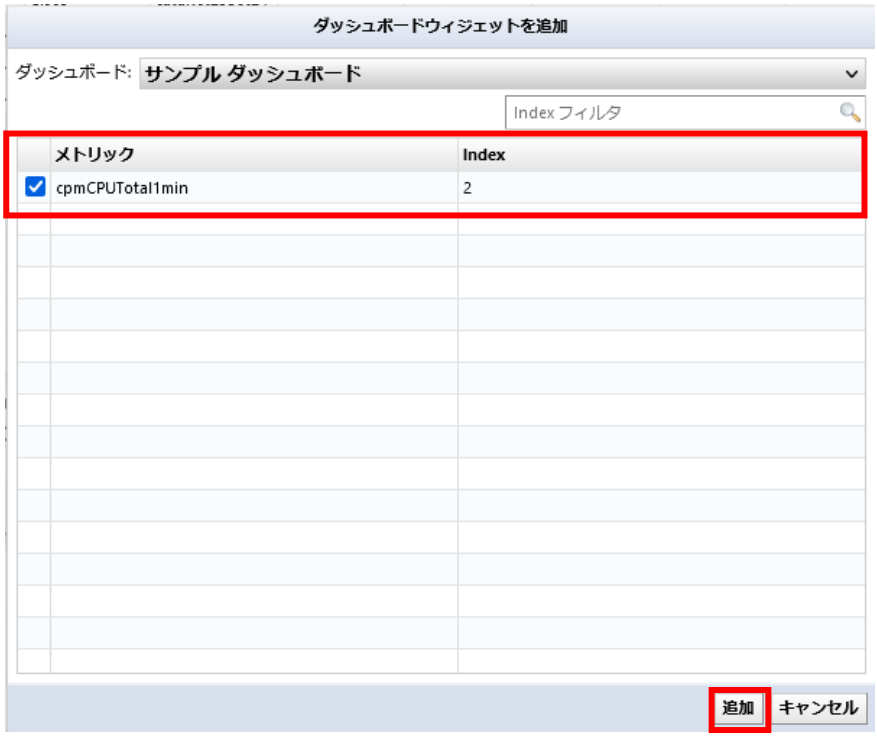


Copyright (C) 2026 LogicVein, Inc.

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。

4. グラフに追加するメトリックを選択し、［追加］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。

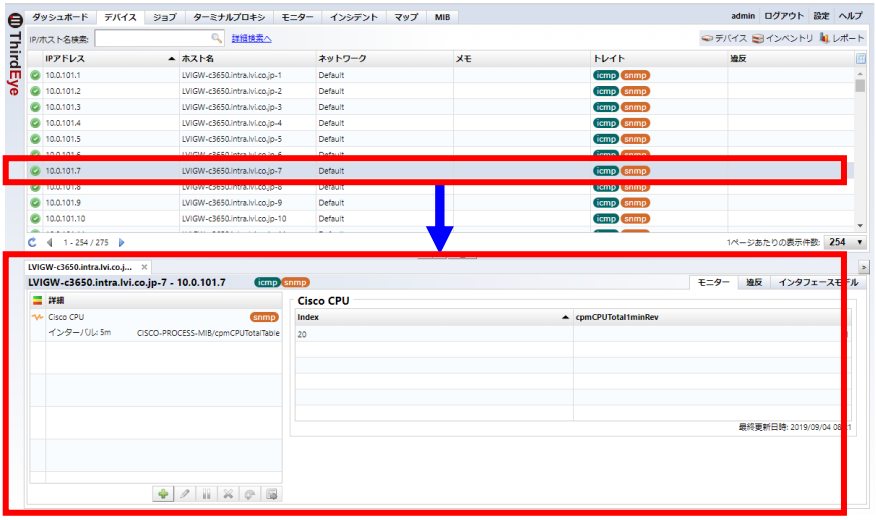


Copyright (C) 2026 LogicVein, Inc.

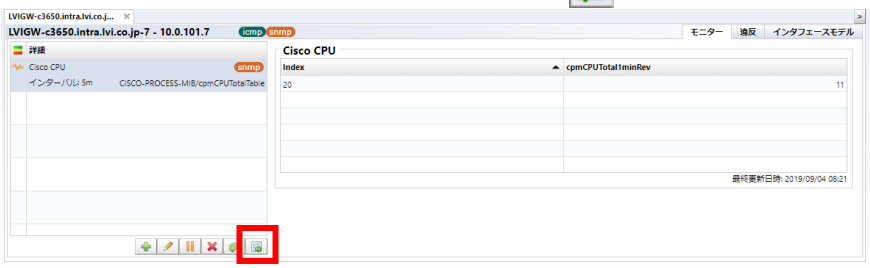
6.2.2 CSV ファイルへエクスポートする

SNMP で収集したデータは、CSV 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。

保存をクリック後、Excel ファイルがダウンロードされます。

Copyright (C) 2026 LogicVein, Inc.

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。

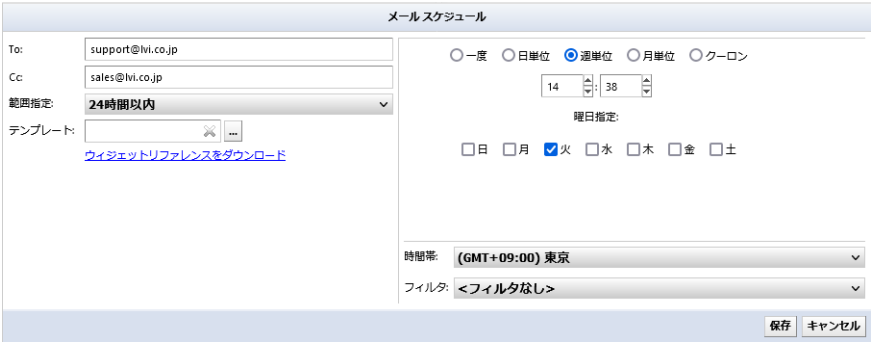
※メールを送信するには、まずメールサーバを設定する必要があります。メールサーバの設定については、「7.8.3.6 メールサーバを設定する」を参照してください。

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。

Copyright (C) 2026 LogicVein, Inc.

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。 • 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）
テンプレート	ダッシュボードグラフを、ワードファイルに貼り付けてレポート送信することができます。
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。

Copyright (C) 2026 LogicVein, Inc.

6.3　デバイスのコンフィギュレーション取得

ThirdEye は、Net LineDancer（コンフィグ管理ツール）の機能を使用してデバイスのコンフィギュレーションを取得できます。この処理は「コンフィグバックアップ」と呼ばれます。コンフィグバックアップ時、ThirdEye は SSH または Telnet でデバイスに接続し、show コマンドや tftp コマンドを実行してコンフィグを取得します。

6.3.1 コンフィグバックアップ前の確認事項

コンフィグをバックアップする前に、以下の要件を満たしていることを確認してください。

- コンフィグバックアップ対応機種であること
  - 対象デバイスがコンフィグバックアップ機能に対応していることを確認してください。対応機種の詳細は、以下の資料を参照してください。
    https://www.lvi.co.jp/NetLD/pdf/adapter_list.pdf
- アダプタの指定
  - 適切なアダプタが指定されていることを確認してください。通常、アダプタはディスカバリ機能により自動的に識別されますが、場合によっては手動で変更する必要があります。アダプタの設定は、[デバイス] > [デバイスプロパティの編集] で変更できます。
- NCM トレイトの表示
  - 対象デバイスのトレイトカラムに「ncm」が表示されていることを確認してください。これにより、NCM 機能が利用可能となります。「ncm」が表示されていない場合は、手動で設定を変更してください。設定の変更は、[デバイス] > [デバイスプロパティの編集] > [NCM 機能を切り替え] から行えます。

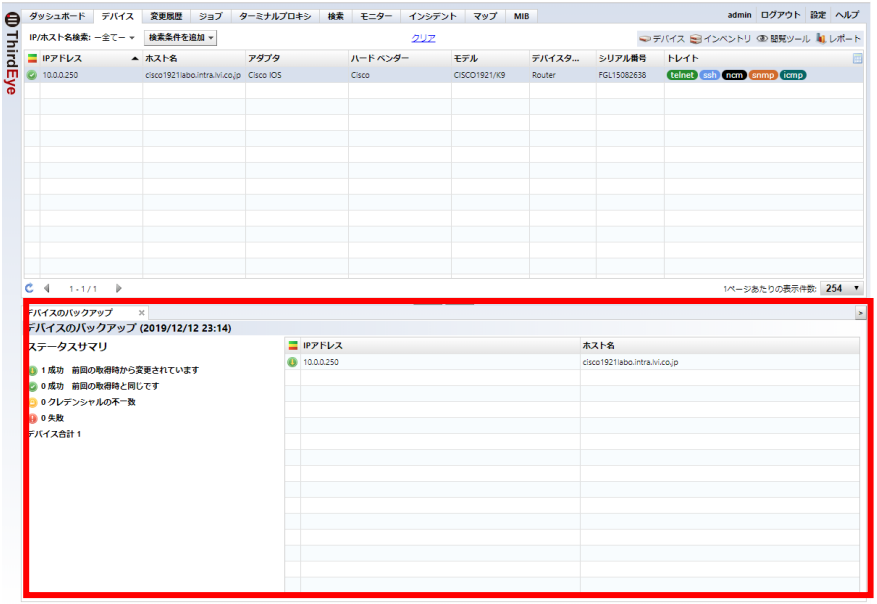
- クレデンシャルの設定
  - デバイスにログインするためのユーザ名およびパスワードが正しく設定されていることを確認してください。設定方法については「5.1 クレデンシャルを設定する」を参照してください。

Copyright (C) 2026 LogicVein, Inc.

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］をクリックしてください。デバイスが選択されていない場合は、NCM 機能が利用可能なデバイスを対象にバックアップが実行されます。

バックアップの実行後、画面下部に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

アイコン	説明
	バックアップ成功、変更あり。 前回のバックアップデータと比較し、デバイス上のコンフィギュレーションに差分が検知された場合に表示されます。初回のバックアップ時もこのステータスとなります。
	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一致する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る場合に表示されます。右側の結果をクリックすると、バックアップ時に使用したクレデンシャルを確認できます。［インベントリ］＞［クレデンシャル］で正しい情報が設定されていること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の取得に失敗した場合に表示されます。アイコンをダブルクリックすると、詳細情報を確認できます。

Copyright (C) 2026 LogicVein, Inc.

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使用されるアイコンとその説明は以下のとおりです。

アイコン	ステータス	状態説明
	バックアップ完了	デバイスのコンフィギュレーションが正常に取得され、バックアップが完了した状態です。
	コンフィギュレーション不一致	running-config と startup-config に差分が検出された状態です。アイコンをダブルクリックすると、比較結果を確認できます。
	クレデンシャルの不一致	登録されたクレデンシャルでログインできず、バックアップに失敗した状態です。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	バックアップの実行に失敗した状態です。アイコンをダブルクリックすると、詳細情報を確認できます。
	バックアップ未実行	バックアップが一度も実行されていない状態です。
	ワーニング	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る状態です。
	エラー	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る状態です。

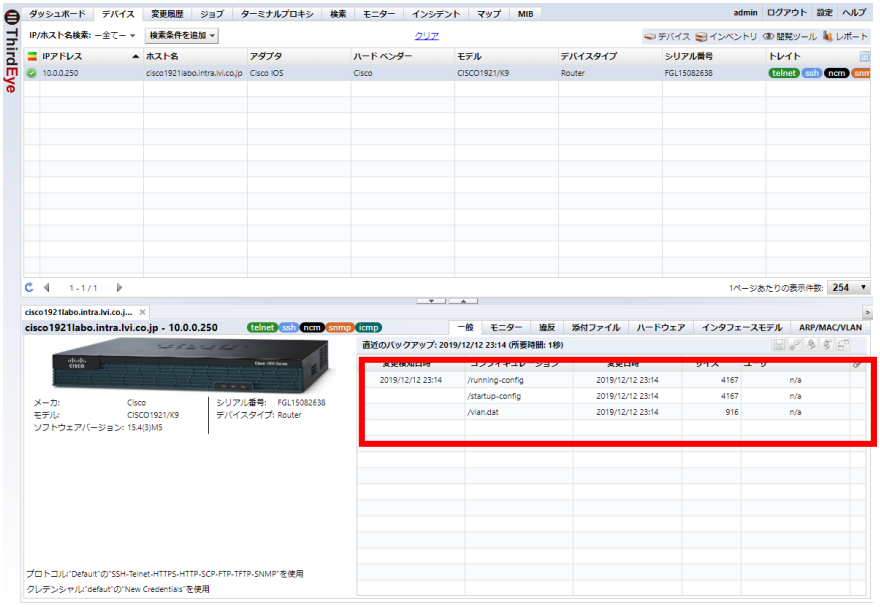
ステータスカラムには、モニター設定のトリガーで指定された重大度とバックアップステータスの中で、優先度が高いアイコンが表示されます。

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

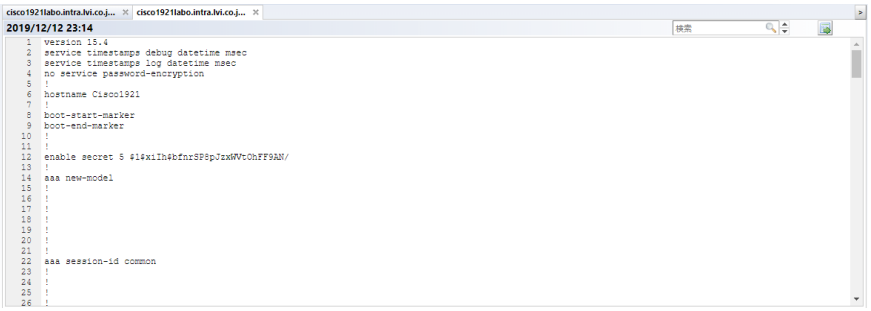
Copyright (C) 2026 LogicVein, Inc.

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。



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。



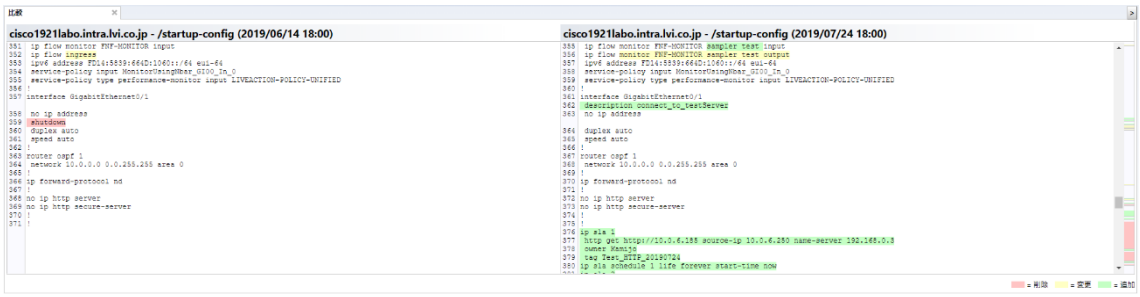
Copyright (C) 2026 LogicVein, Inc.

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。

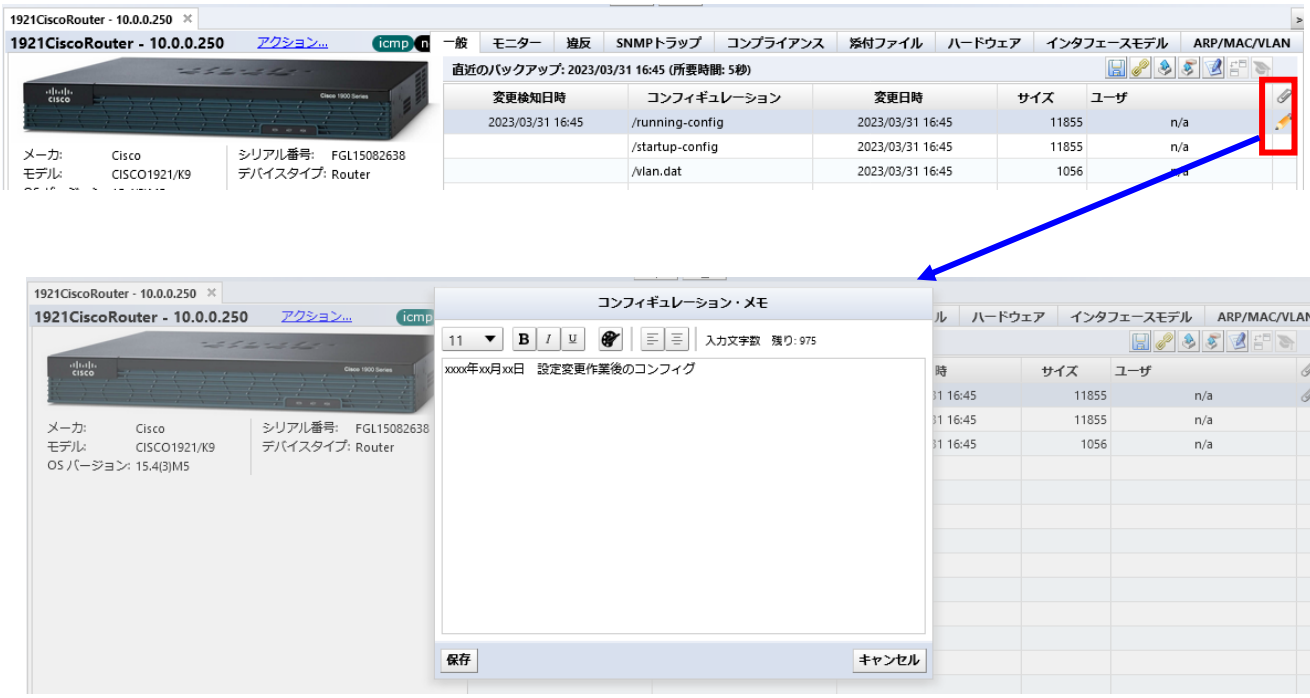
※「Ctrl」キーを押しながら選択すると、複数選択ができます。

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 コンフィグへのメモ

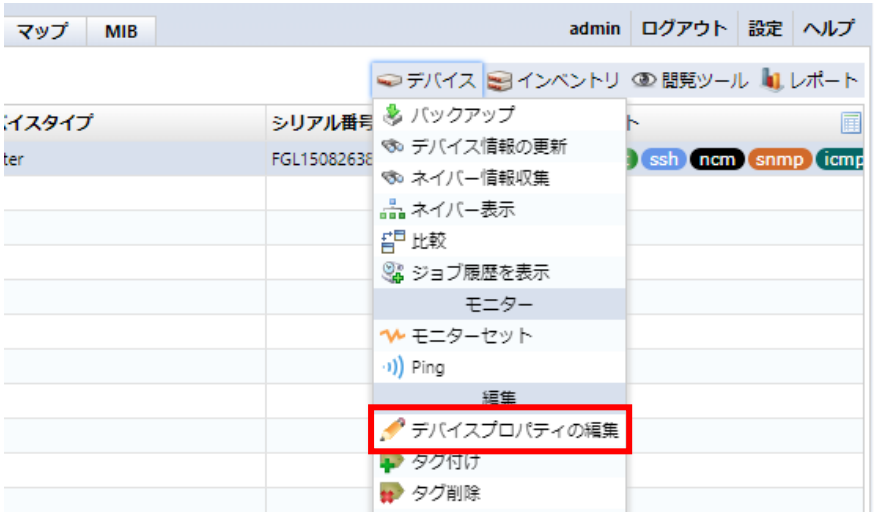
取得したコンフィグにメモを追加できます。各コンフィグのクリップアイコン列にマウスを合わせると編集アイコンが表示されます。ダブルクリックすると編集ウィンドウが表示され、コメントを入力できます。



Copyright (C) 2026 LogicVein, Inc.

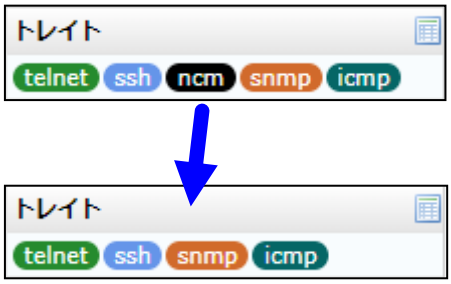
6.3.7　コンフィグバックアップを無効にする

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、[デバイスプロパティの編集]から無効化します。



「NCM 機能は無効」が表示されるまで、[NCM 機能を切り替え]をクリックし、保存します。

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。



Copyright (C) 2026 LogicVein, Inc.

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[デバイスプロパティの編集]から有効化します。

Copyright (C) 2026 LogicVein, Inc.

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。

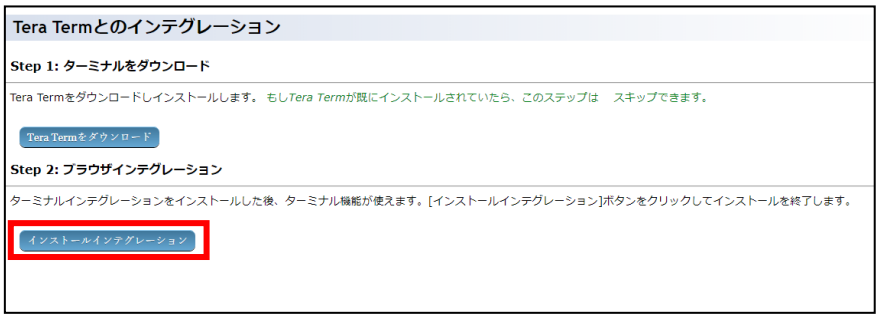
6.4.1 使用する前の準備

ターミナルプロキシには、Web ブラウザを使用する方法と Tera Term を使用する方法があります。Tera Term を使用する場合には、以下の準備が必要です。

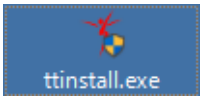
- 操作する端末に Tera Term をインストール
  ターミナルプロキシは、操作している PC の Tera Term を呼び出します。
- ブラウザインテグレーションのインストール
  ThirdEye に接続しているブラウザと Tera Term を紐付ける必要があります。

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。

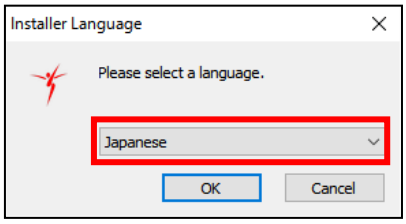
1. ［インストールインテグレーション］をクリックし、 ttinstall.exe をダウンロードします。



2. ダウンロードした ttinstall.exe を実行します。

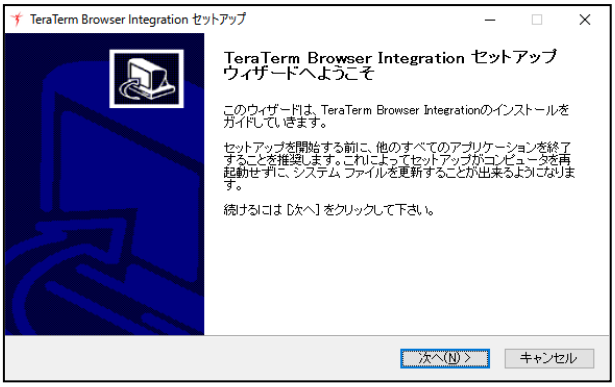


3. 表示言語を選択し、［OK］をクリックします。

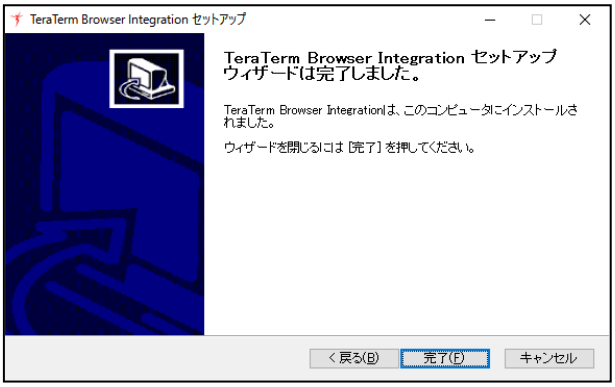


Copyright (C) 2026 LogicVein, Inc.

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。

Copyright (C) 2026 LogicVein, Inc.

6.4.2 ターミナルプロキシを起動する

ターミナルプロキシの起動時にデバイスのコンフィグバックアップを取得している場合は、ターミナルプロキシの起動後にプロトコルの選択やユーザ名/パスワードの入力を省略できます。

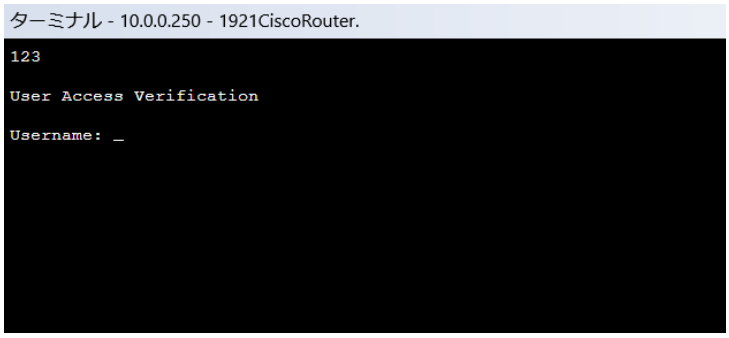
6.4.2.1 Web ブラウザを使用

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、［Web 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. ブラウザの新しいタブにターミナルが表示され、デバイスのログイン画面が表示されます。ユーザ名とパスワードを入力してデバイスにログインします。



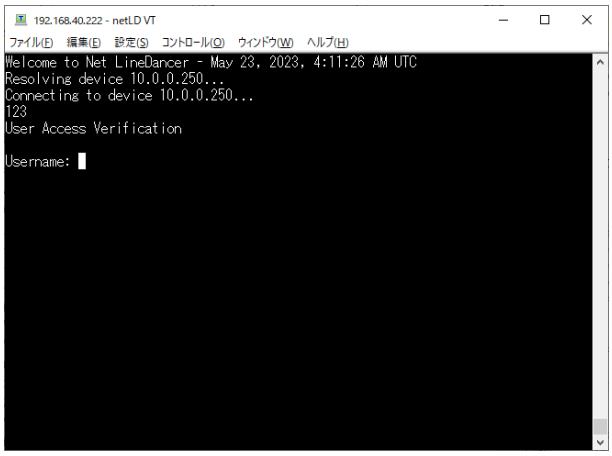
Copyright (C) 2026 LogicVein, Inc.

6.4.2.2　Tera Term を使用

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、［ターミナルソフトを起動］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。

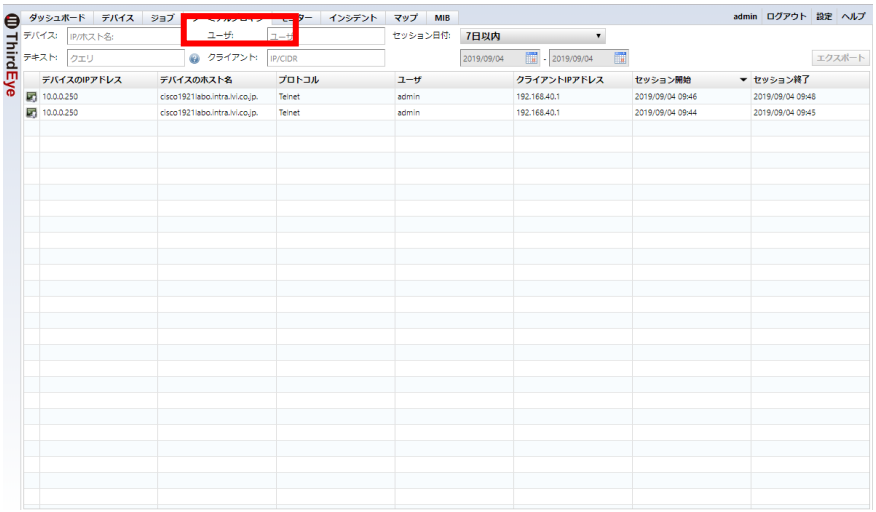
4. Tera Term が起動し、デバイスのログイン画面が表示されます。ユーザ名とパスワードを入力しデバイスにログインします。



Copyright (C) 2026 LogicVein, Inc.

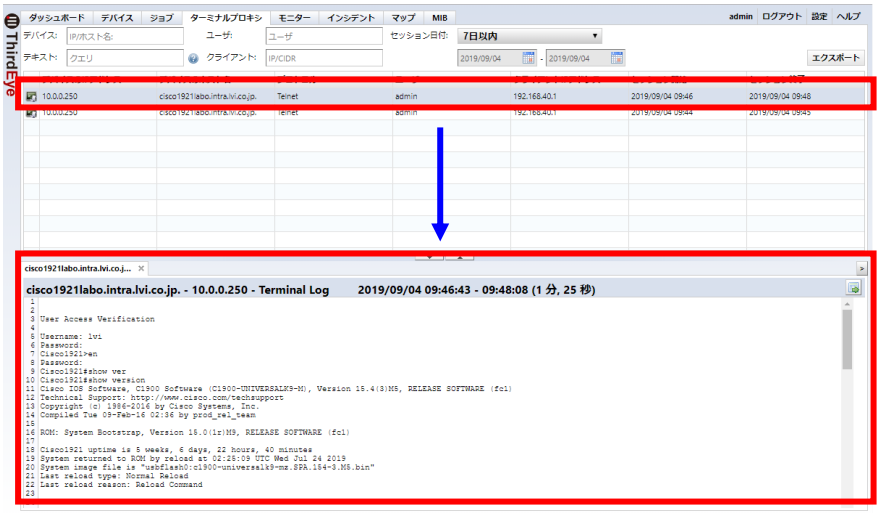
6.4.3 操作ログを確認する

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。



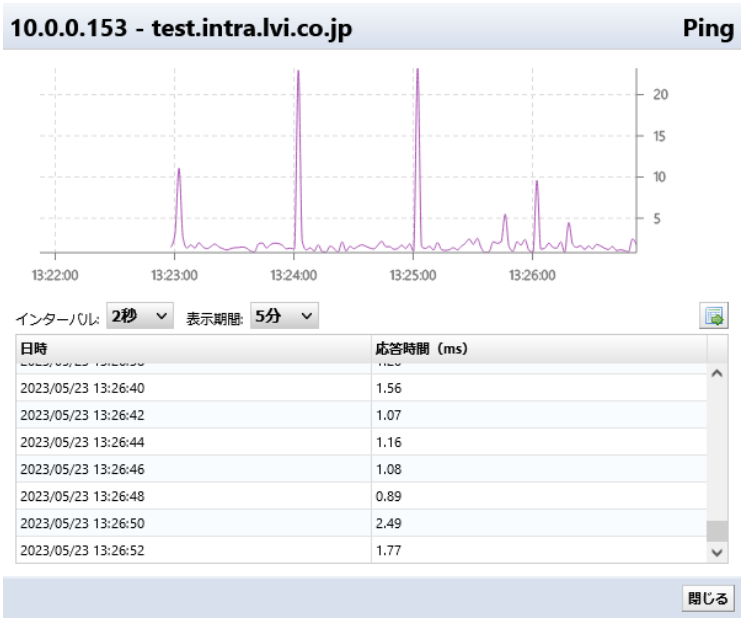
ログ画面右上にある［ (エクスポート)］をクリックすると、セッションデータをテキストファイルとして保存できます。なお、ファイル名は「termlogs *YYYY-MM-DD*.zip」となり、ZIP ファイル形式でまとめられます。「*YYYY-MM-DD*」は保存した年月日を表します。

Copyright (C) 2026 LogicVein, Inc.

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。



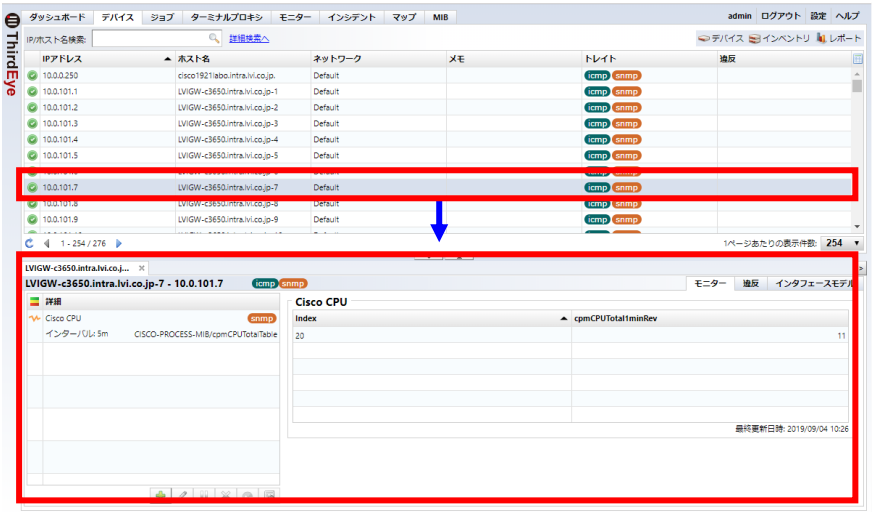
画面右にある［ (エクスポート)］をクリックすると、Ping の結果を CSV ファイルにエクスポートできます。

Copyright (C) 2026 LogicVein, Inc.

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。

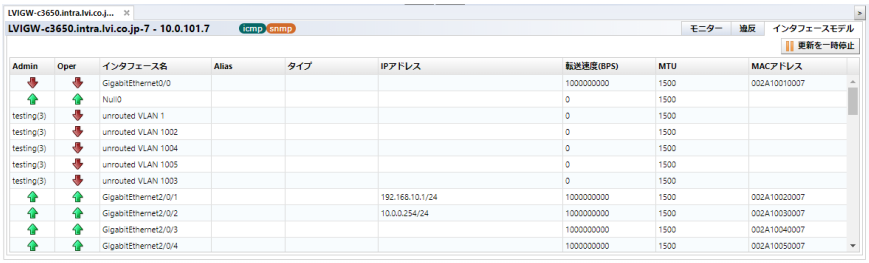


2. デバイス詳細画面内の［インタフェースモデル］タブをクリックします。

3. ［自動更新］をクリックします。

Copyright (C) 2026 LogicVein, Inc.

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。

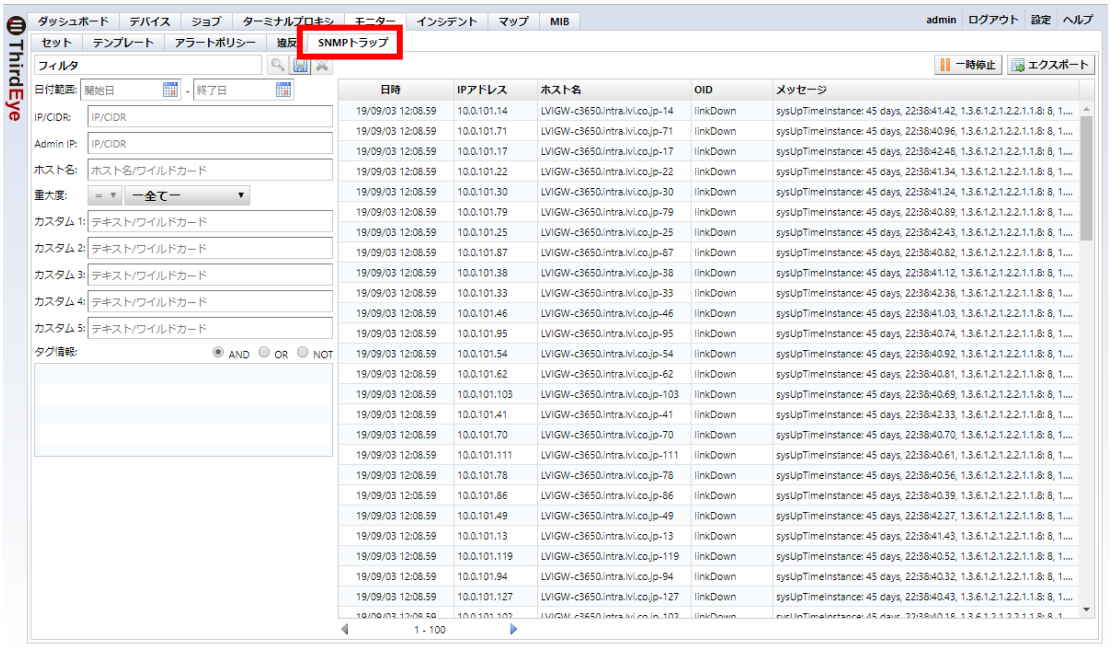


停止するには、デバイス詳細画面を閉じるか、[更新を一時停止]をクリックします。

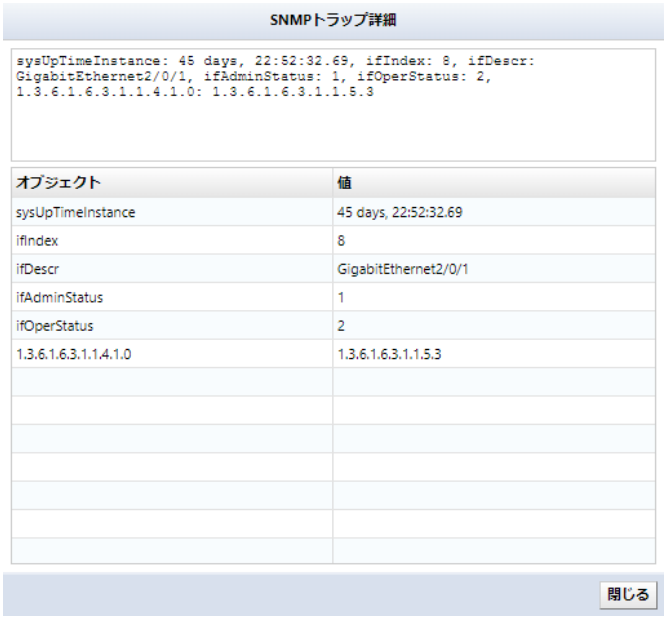
Copyright (C) 2026 LogicVein, Inc.

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。



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。



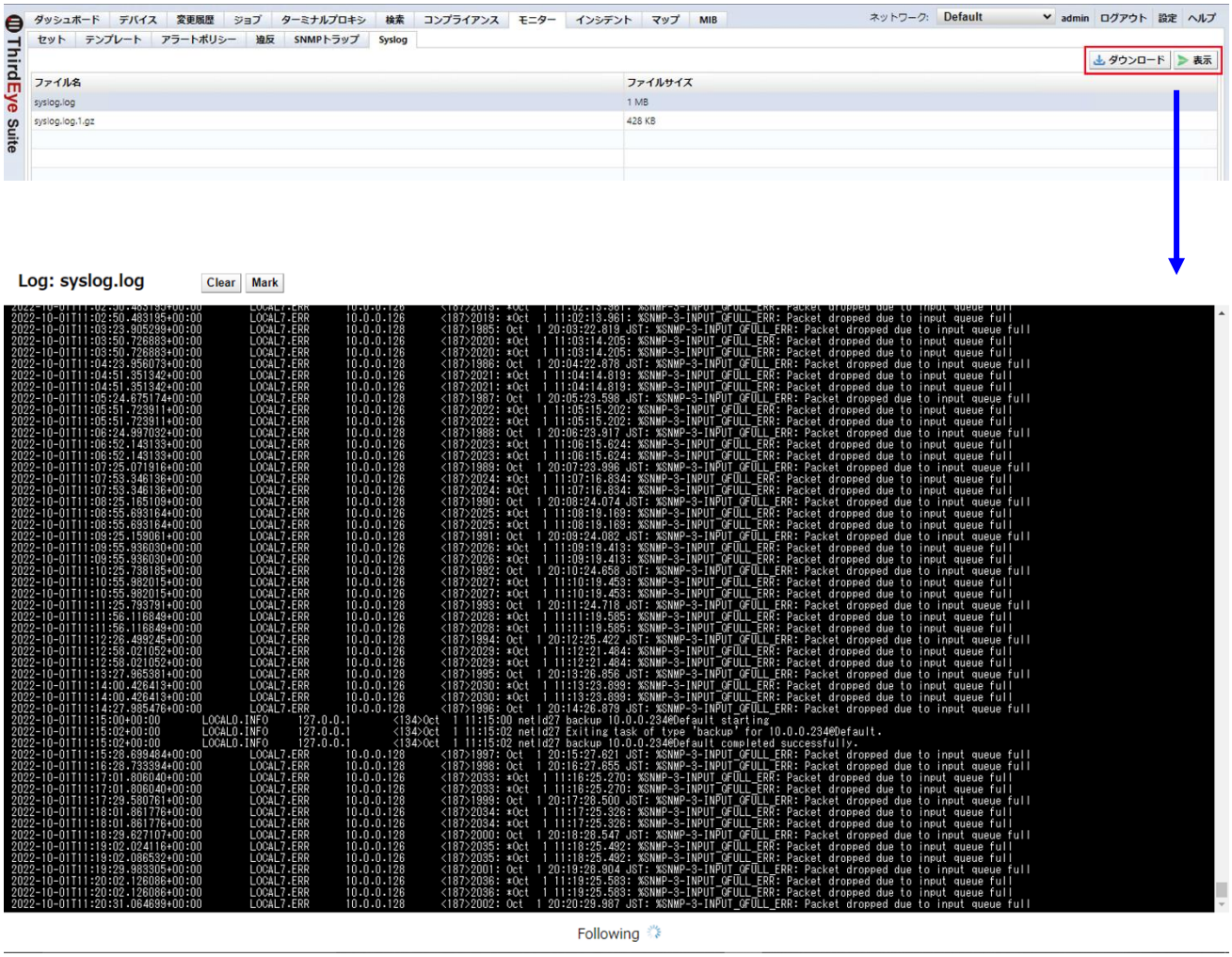
Copyright (C) 2026 LogicVein, Inc.

6.8　受信した Syslog を確認する

リビジョン 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。

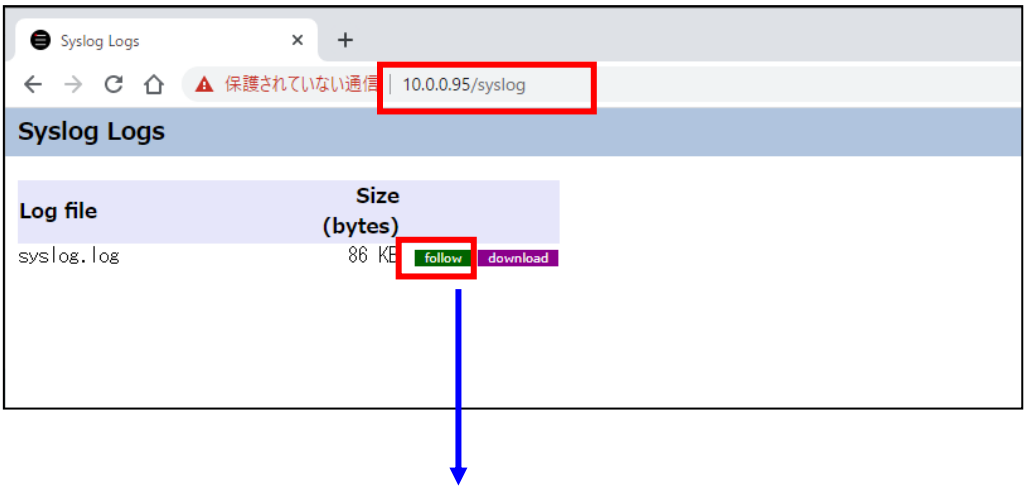


Copyright (C) 2026 LogicVein, Inc.

リビジョン 20221026.0600 以前のリビジョンにおいて、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。



Copyright (C) 2026 LogicVein, Inc.

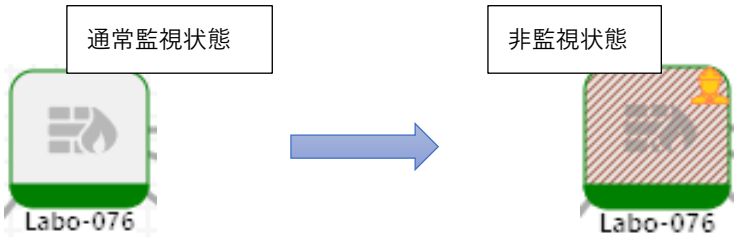
6.9　監視を一時的に停止する（非監視設定）

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。

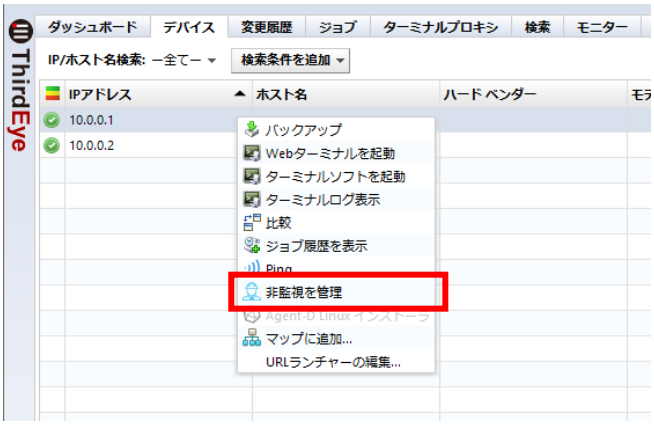
注意	リビジョン 20201203.0810 以降、［ジョブ］タブにあった非監視機能は、［デバイス］タブから操作するように変更されました。

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。



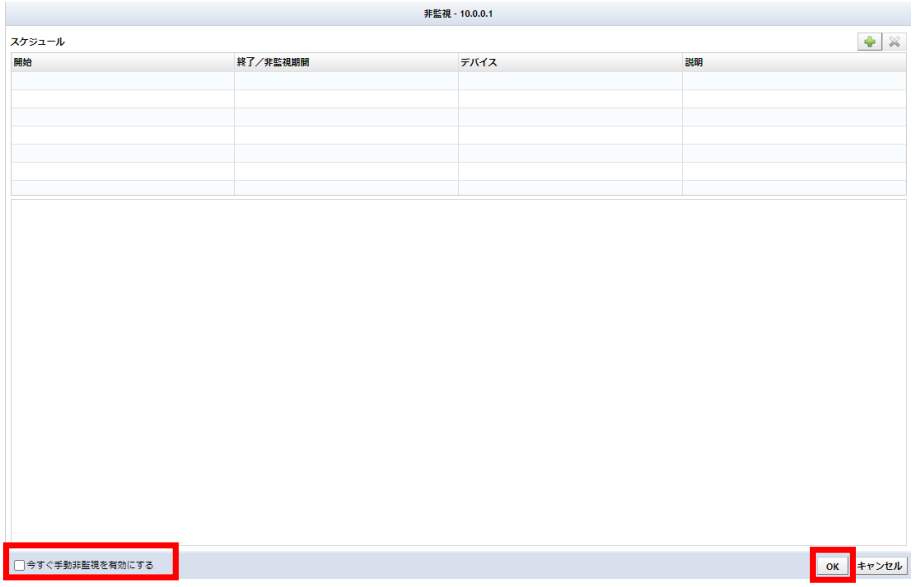
6.9.1 手動で非監視にする

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。



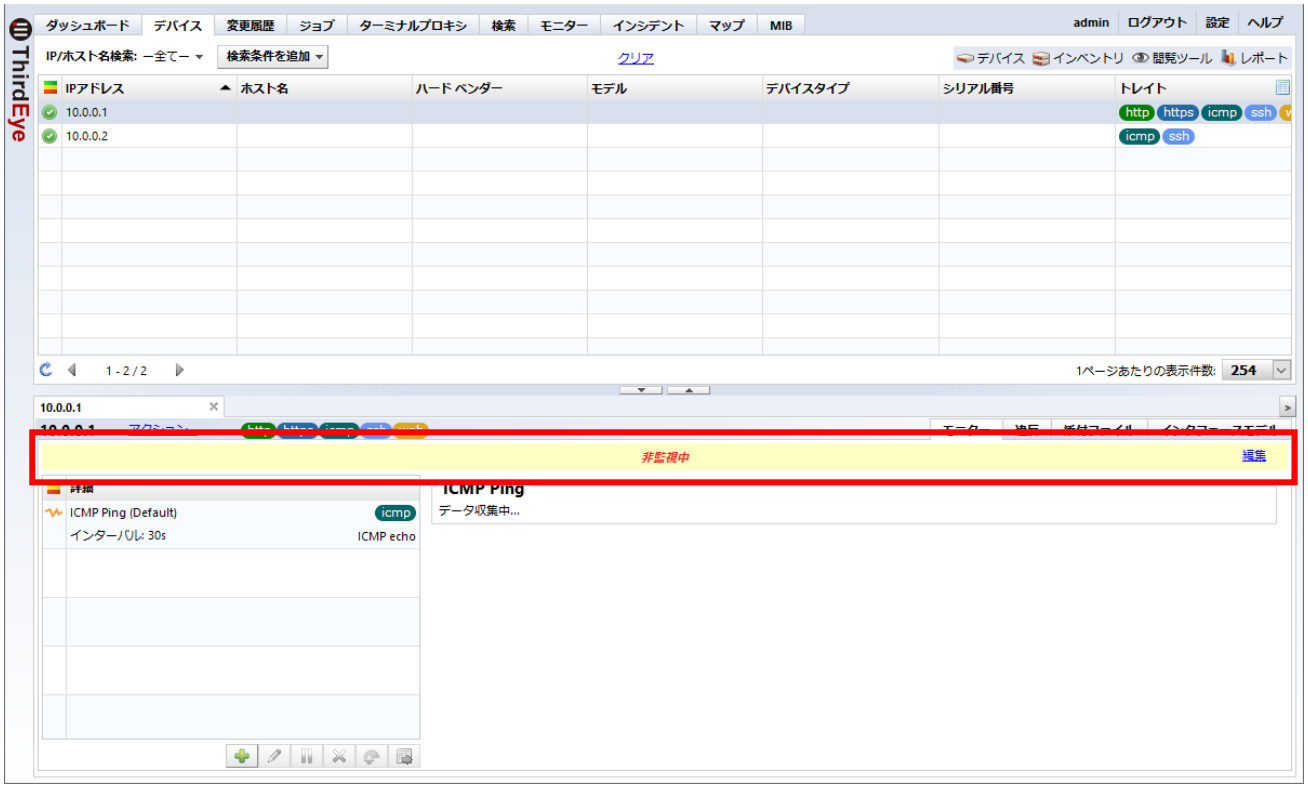
Copyright (C) 2026 LogicVein, Inc.

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。

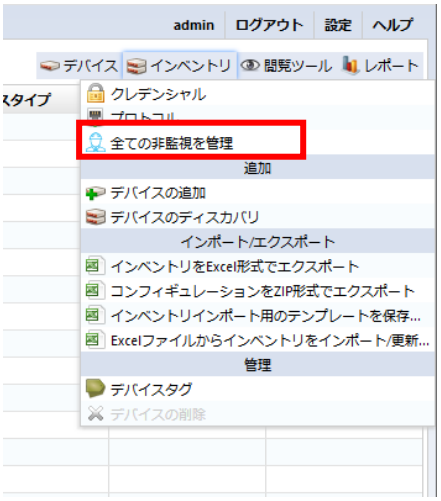


非監視状態を解除する場合は、上記［手順 3］で「今すぐ手動非監視を有効にする」のチェックをはずし、［OK］をクリックしてください。

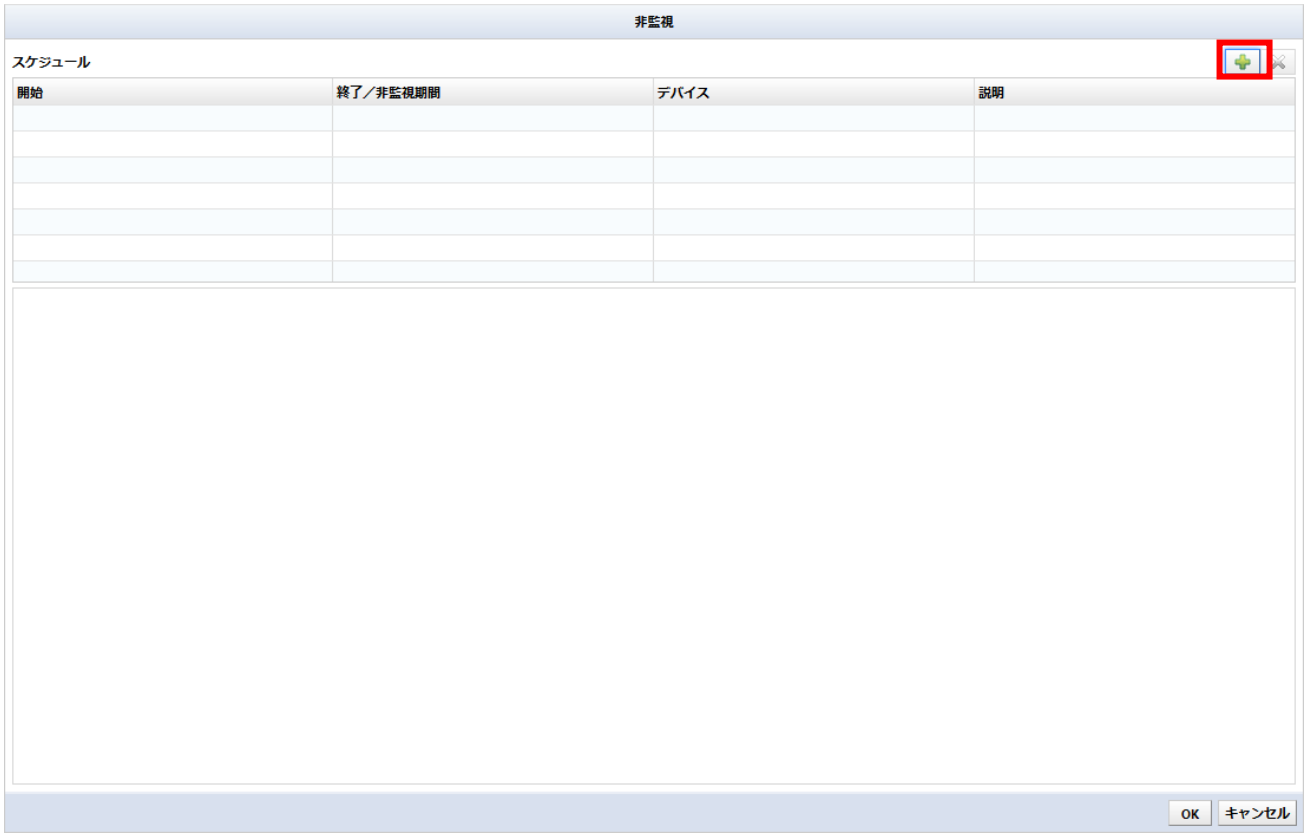
Copyright (C) 2026 LogicVein, Inc.

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。



Copyright (C) 2026 LogicVein, Inc.

3. 非監視のスケジュールと対象デバイスを設定します。

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。 • 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
	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。 ※終了の日時は、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。 • 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。

Copyright (C) 2026 LogicVein, Inc.

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。

Copyright (C) 2026 LogicVein, Inc.

6.10 ジョブ管理

ジョブタブは、ジョブ履歴タブとジョブ管理タブで構成されています。ジョブ履歴では、過去のジョブ実行の結果を見ることが出来ます。ジョブ管理タブでは、ジョブを作成、編集、管理そして実行が出来ます。また、作成したジョブを定期的に自動実行するように設定することができます。

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。

ジョブ管理サブタブでは、以下のボタンがあります。

項目	説明
監査ログ	ジョブの
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。
コピー	
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。EOL/EOS、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	クーロン形式のフィルタを登録します。

Copyright (C) 2026 LogicVein, Inc.

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。

【ジョブ作成手順の流れ】

1. 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ます。

6.10.1.1 ジョブ名を決め、機能を選ぶ

まずは、任意の名前でジョブ名を入力します。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 Enable Password の変更を選択しています。

6.10.1.2 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。Enable Password の変更では、パスワード欄に変更するパスワードの文字列を入力します。

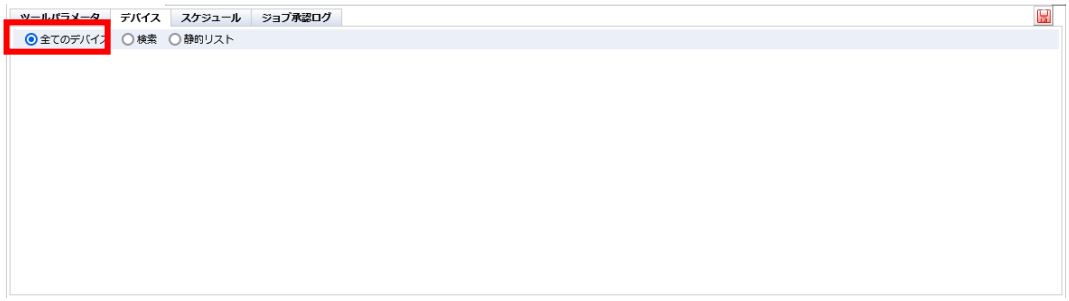
Copyright (C) 2026 LogicVein, Inc.

6.10.1.3　対象デバイスを選ぶ

デバイスサブタブでこのジョブを実行する対象デバイスを選択します。選択方法としては、「全てのデバイス」、「検索」、「静的リスト」の３つがあります。

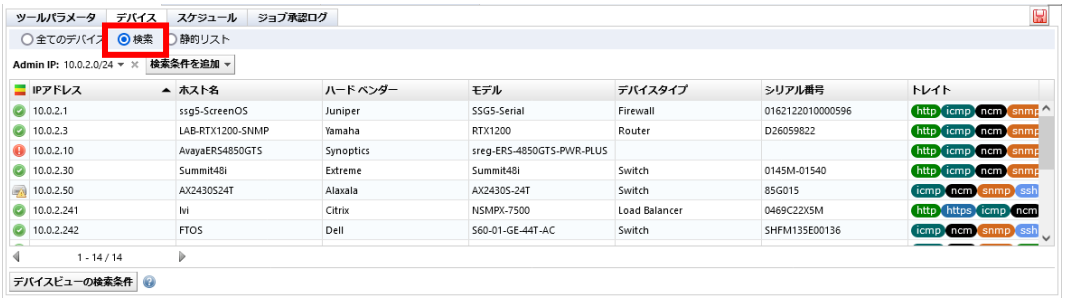
【全てのデバイス】

登録されているデバイス全てが対象となります。



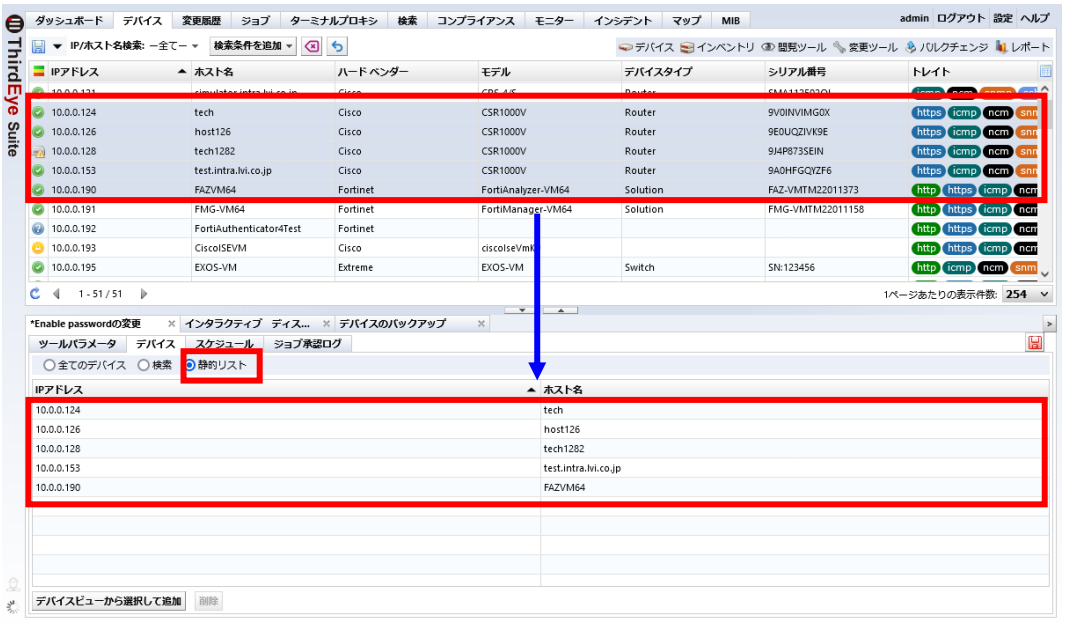
【検索】

検索条件に一致するデバイスが対象となります。ただし、検索はジョブ実行時に行われるため、ジョブ作成時に検索結果一覧に表示されているデバイスのみが対象ではありません。ジョブ作成後に検索条件に一致するデバイスが追加されれば、そのデバイスも対象となります。



【静的リスト】

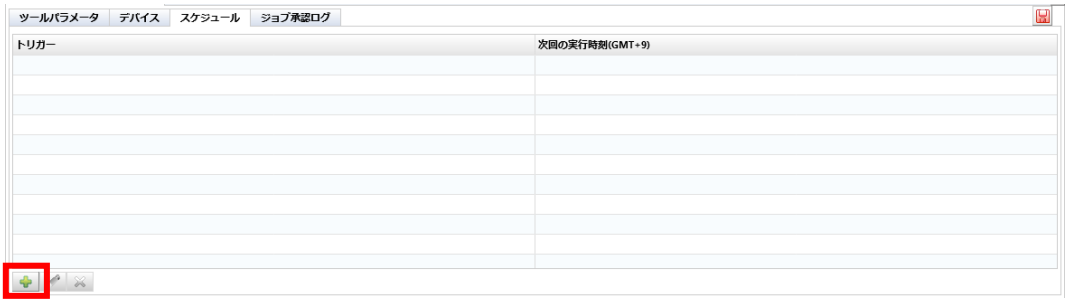
静的リストでは、デバイスタブで選択したデバイスを追加でき、追加されたデバイスが対象となります。



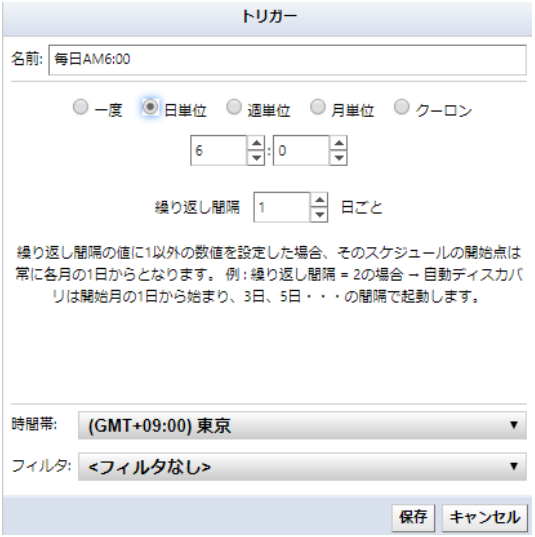
Copyright (C) 2026 LogicVein, Inc.

6.10.1.4　トリガーを追加する

最後に、トリガーを追加します。スケジュールサブタブをクリックします。下部、左の［+(追加)］ボタンから、新しいトリガーを追加することが出来ます。

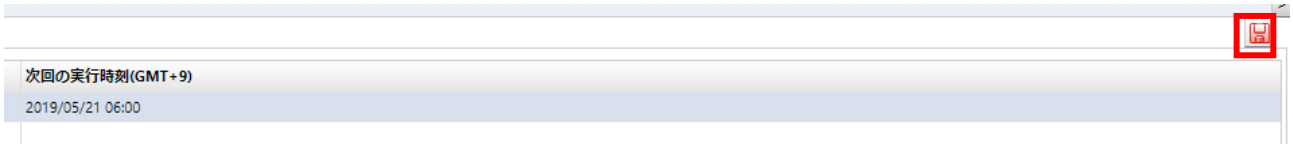


日付や繰り返し頻度を設定し、トリガーを作ります。すべての入力が終わったら、保存ボタンを押してください。



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。



Copyright (C) 2026 LogicVein, Inc.

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、「7.8.3.5 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。

Copyright (C) 2026 LogicVein, Inc.

6.10.3.1　承認機能の権限を設定する

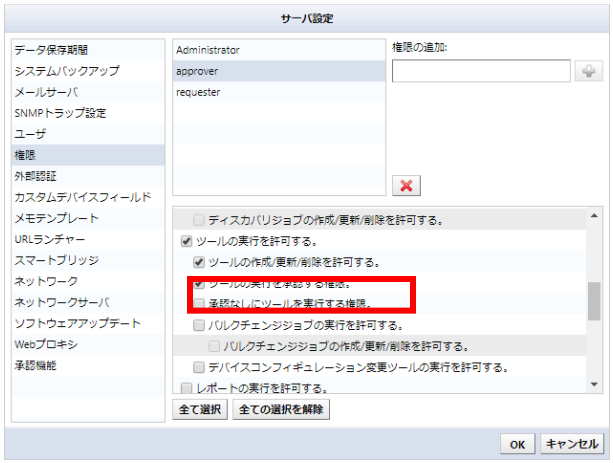
登録済みの権限に対して、承認者の設定をします。設定された権限を割り当てられたユーザが、ジョブの承認を行うことができます。

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。

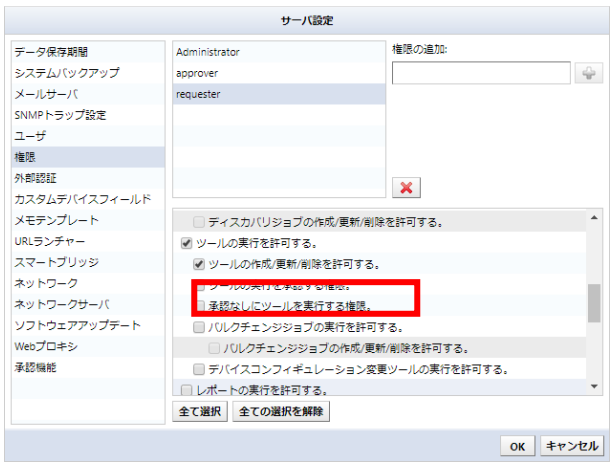
➢ 承認機能に関する権限は、以下の 2 つの権限内容です。

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。



■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。

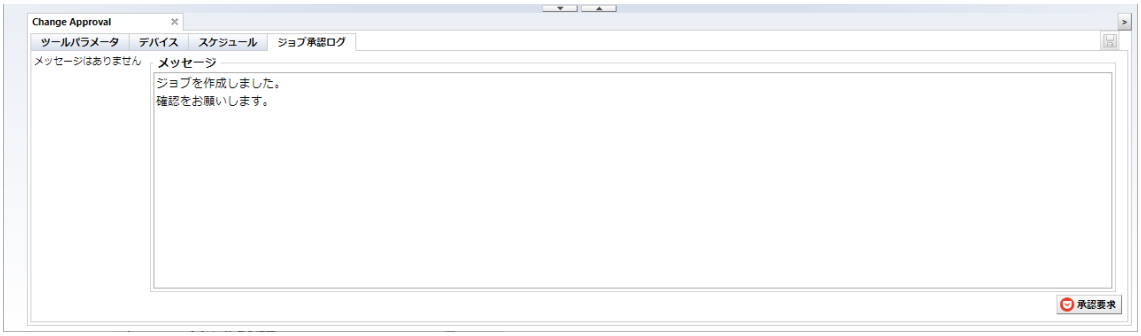


Copyright (C) 2026 LogicVein, Inc.

6.10.3.2　承認要求を申請する（ジョブを申請する）

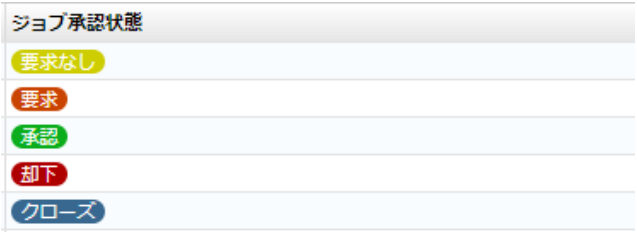
申請者はジョブを作成・編集する際に、承認要求を申請することができます。

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。 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。

Copyright (C) 2026 LogicVein, Inc.

6.10.3.3　承認要求を承認する（ジョブを承認する）

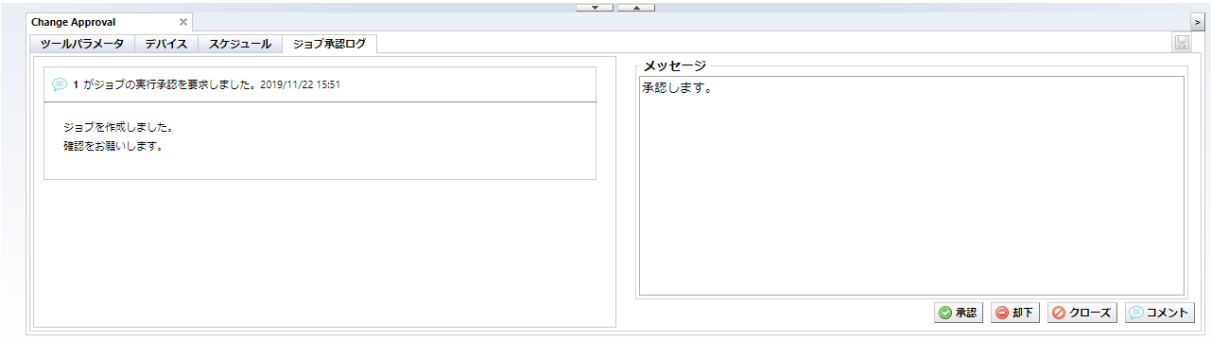
承認者は、申請者から申請されたジョブ（承認要求）を承認することができます。

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。

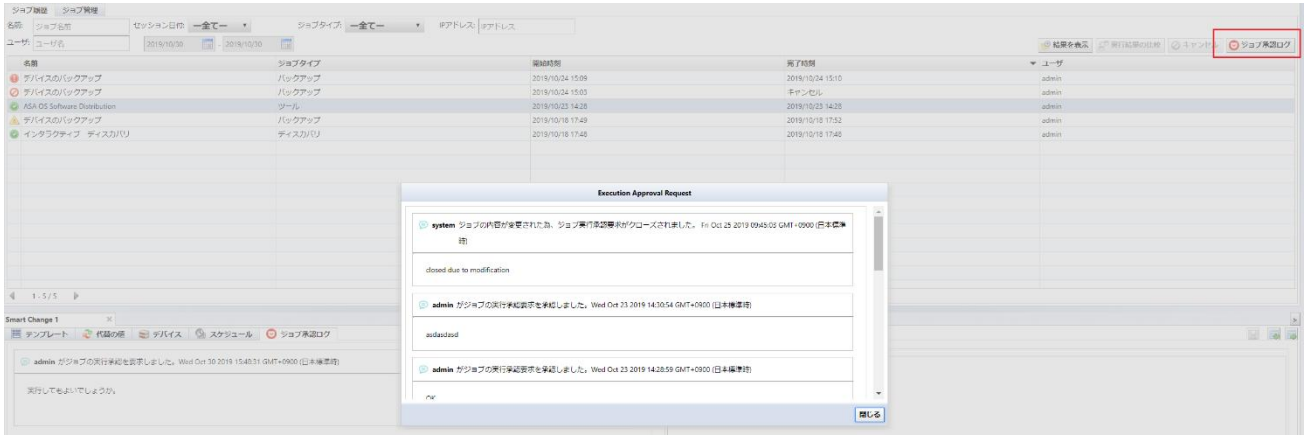
※　問題があれば、メッセージ欄にメッセージを入力し、［却下］または［コメント］をクリックします。



6.10.3.4　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。



Copyright (C) 2026 LogicVein, Inc.

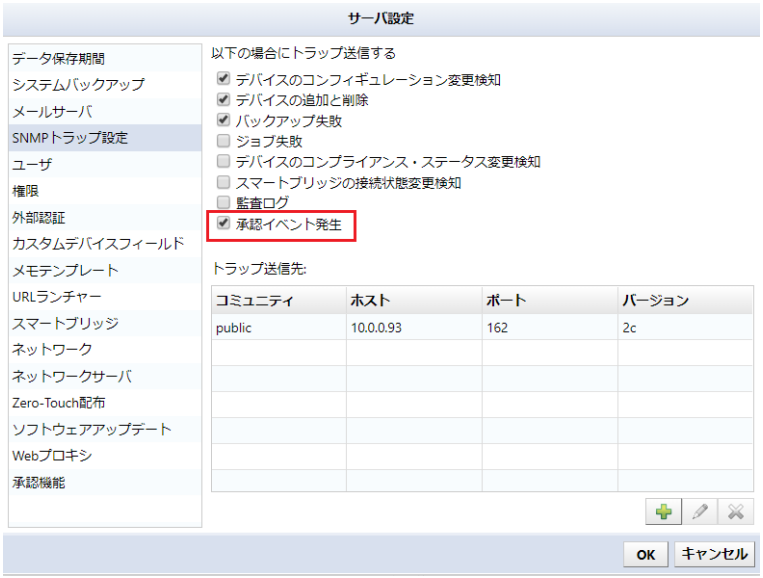
6.10.3.5　承認機能の通知

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。

（1）　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。

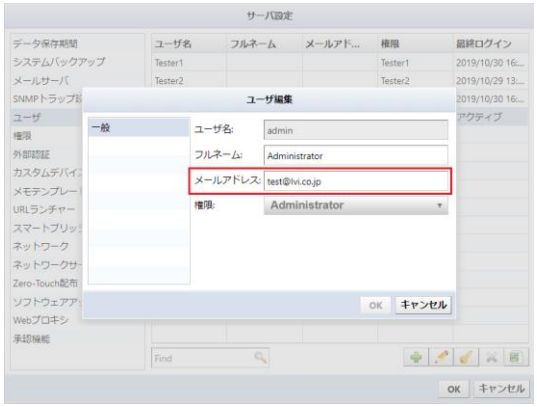
ジョブの要求/実行/承認/却下/クローズ時にトラップが送信されます。



（2）　メール送信

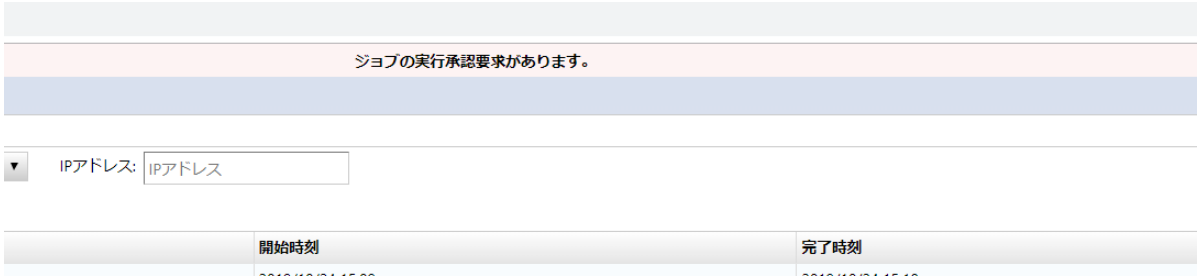
サーバ設定画面のユーザ編集でメールアドレスを設定することで、承認イベント発生時にメールを送信することができます。ジョブの要求/実行/承認/却下/クローズ時にメールが送信されます。

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。



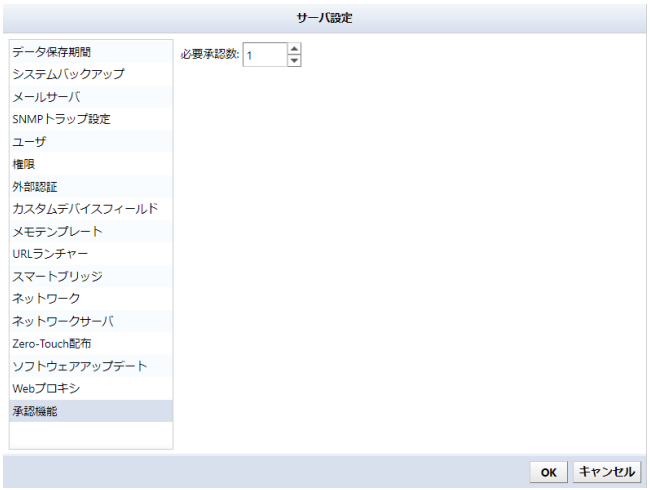
また、ジョブの承認要求がある場合、画面上部に以下のようなバナーが表示されます。

Copyright (C) 2026 LogicVein, Inc.



6.10.3.6　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】

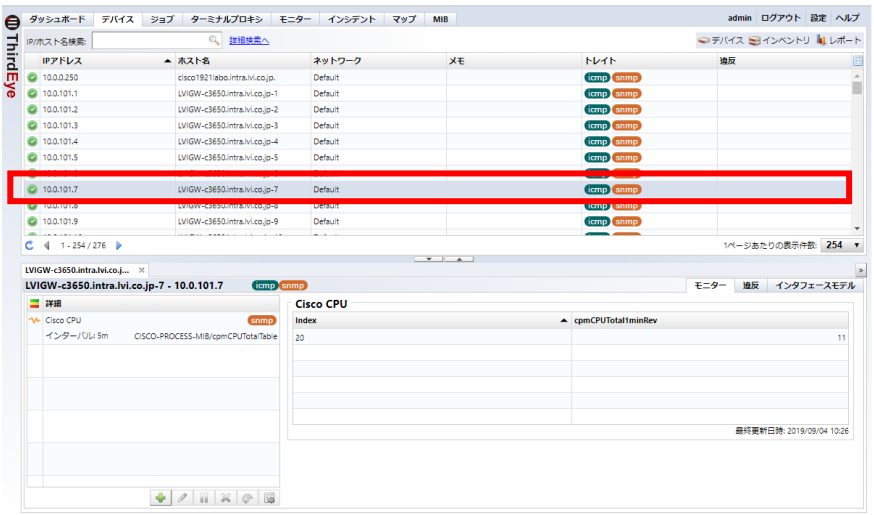
項目	説明
名前	ジョブの名前が表示されます。
ジョブタイプ	ジョブの種類が表示されます。
開始日時	ジョブを実行した開始日時が表示されます。
完了日時	ジョブを完了した完了日時が表示されます。
ユーザ	ジョブを実行したユーザ名が表示されます。

Copyright (C) 2026 LogicVein, Inc.

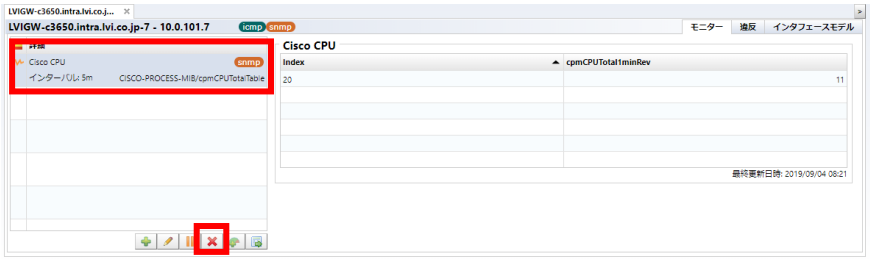
6.11 監視設定を解除する

6.11.1 モニターを削除する

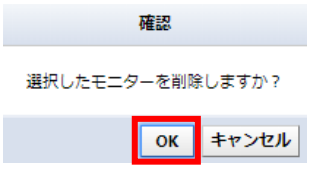
1. ［デバイス］タブの監視対象機器一覧から、モニターを設定する機器をダブルクリックします。



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。

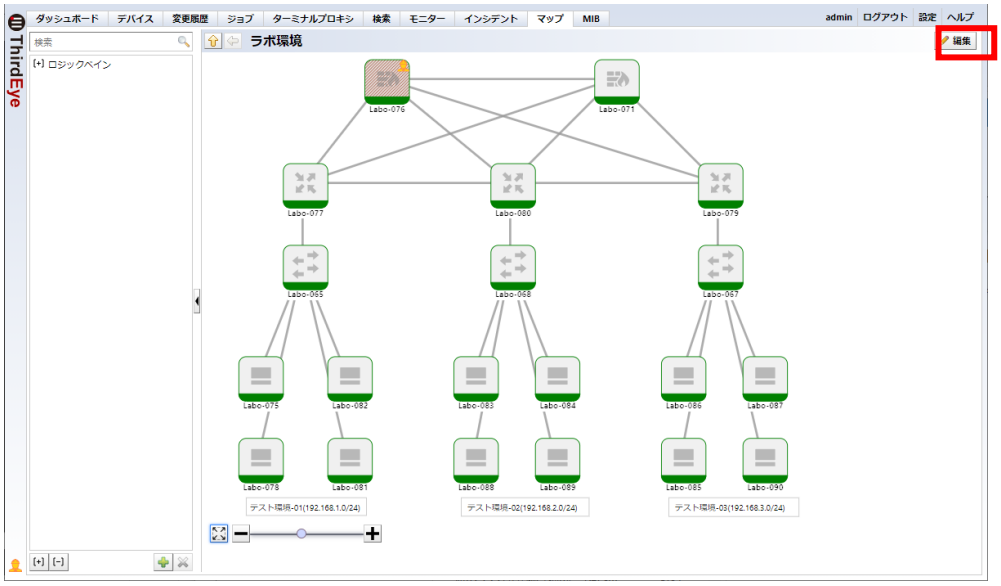


モニター詳細からモニターが削除され、データ収集が中止されます。

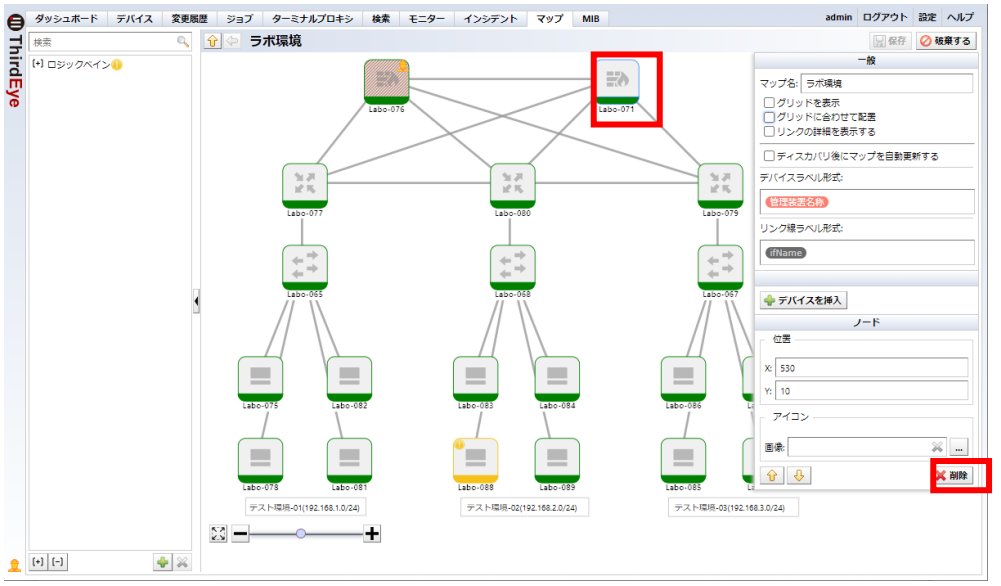
Copyright (C) 2026 LogicVein, Inc.

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。



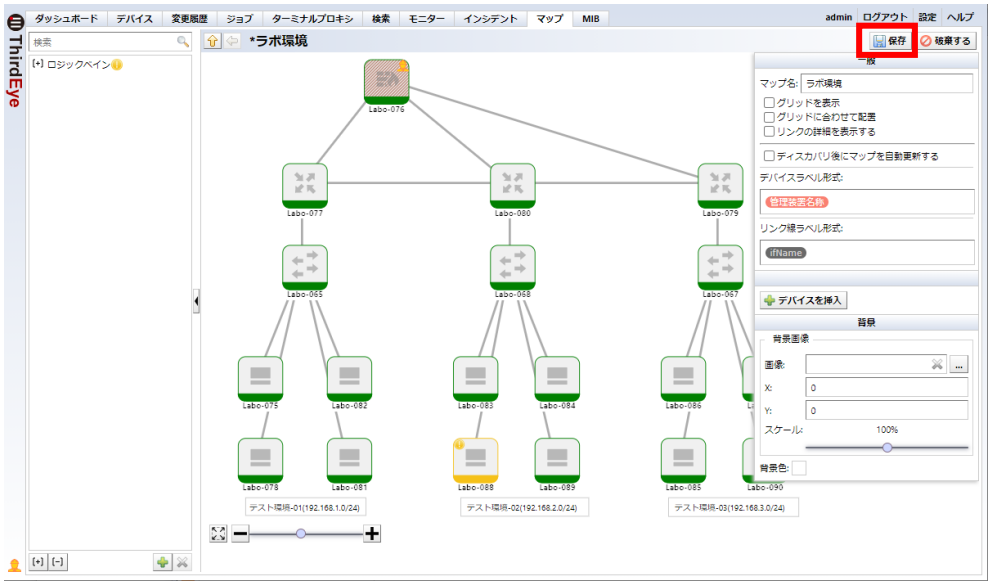
2. 削除したいオブジェクトを選択し、［削除］をクリックします。



Copyright (C) 2026 LogicVein, Inc.

3. 確認メッセージが表示されます。［OK］をクリックします。

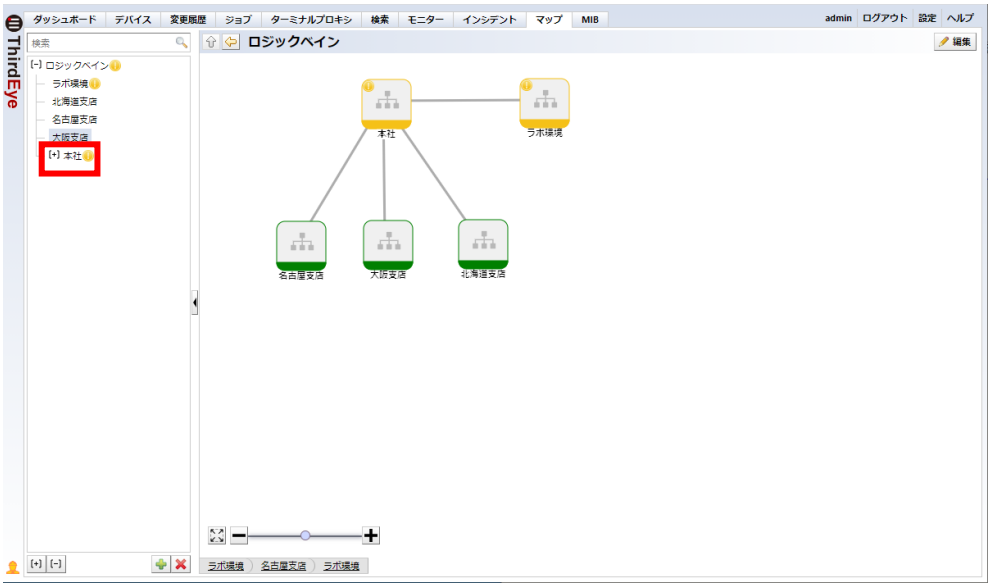
4. デバイスが削除されます。［保存］をクリックし、編集を完了します。



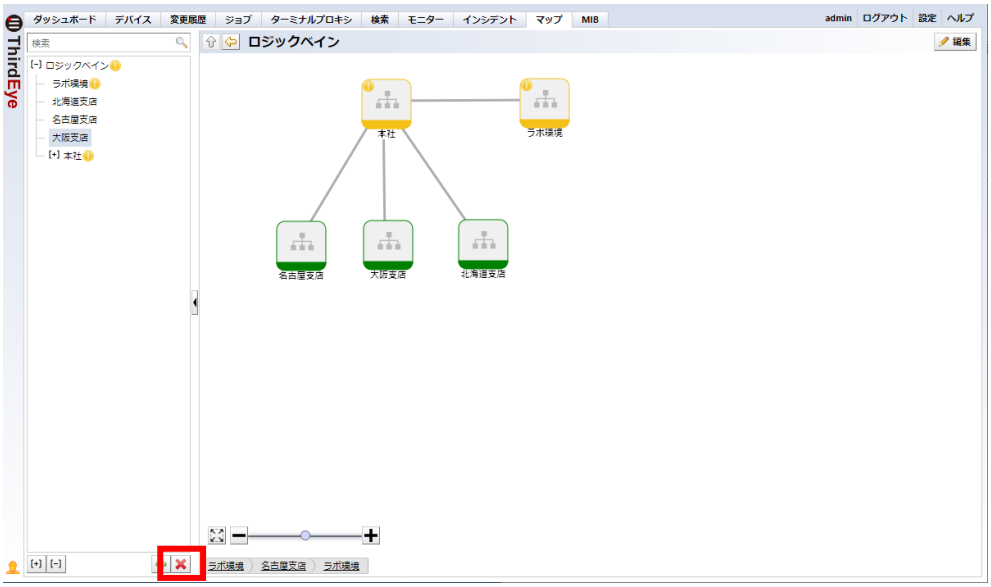
Copyright (C) 2026 LogicVein, Inc.

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。

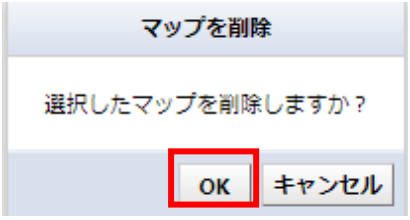


2. 左下の［×(削除)］をクリックします。



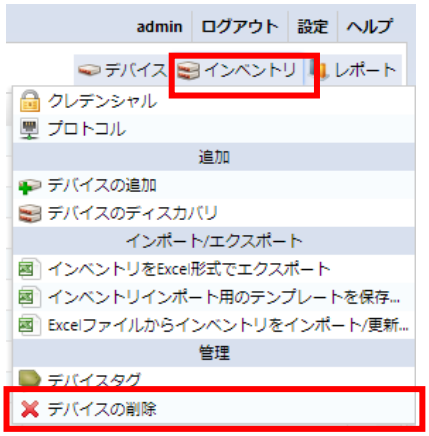
Copyright (C) 2026 LogicVein, Inc.

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。

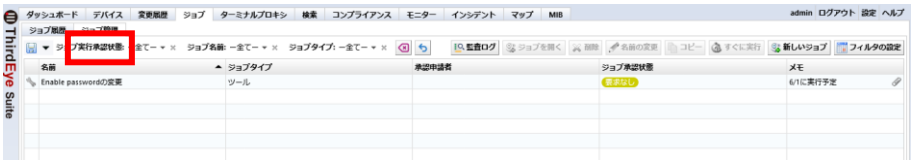


3. 確認メッセージが表示されます。［はい］をクリックします。

Copyright (C) 2026 LogicVein, Inc.

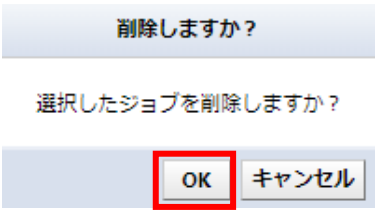
6.11.5 ジョブを削除する

1. ［ジョブ］タブ→［ジョブ管理］をクリックします。

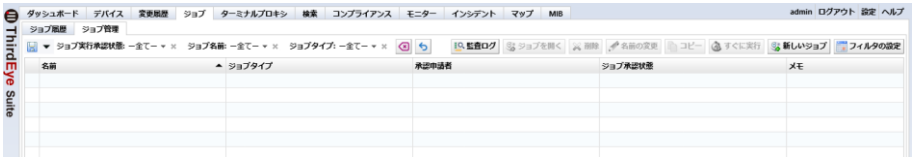


2. 削除するジョブを選択し、［削除］をクリックします。

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。



Copyright (C) 2026 LogicVein, Inc.

7. 詳細設定

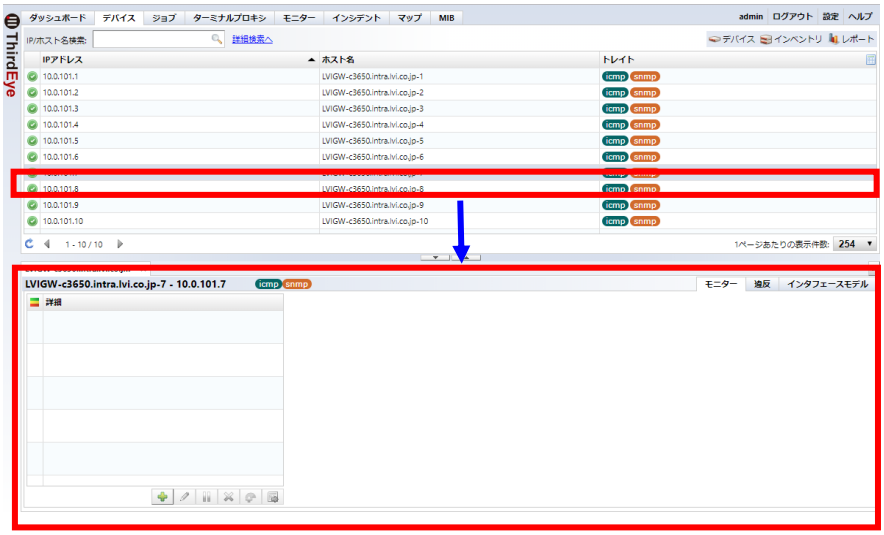
ここでは、ThirdEye のバックアップやグローバル設定、基本設定より詳細な監視設定を紹介します。

7.1 いろいろな監視設定をする

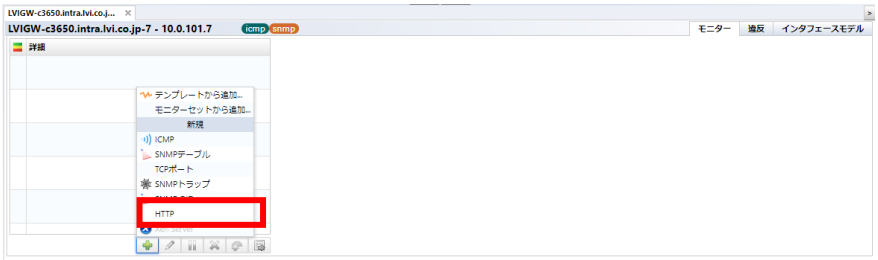
7.1.1 Web サイトを監視する

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。

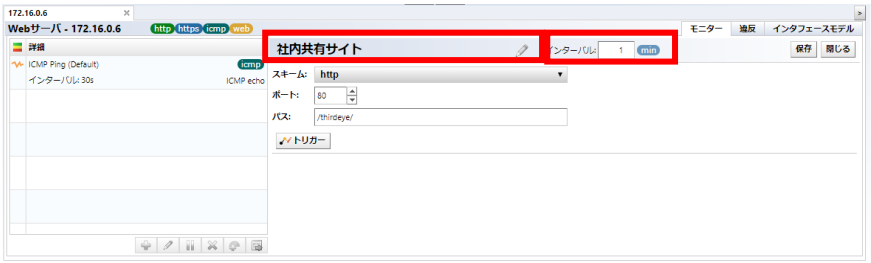
1. ［デバイス］タブの監視対象機器一覧から、モニターを設定する機器をダブルクリックします。



2. 左下の［+(追加)］をクリックし、「HTTP」をクリックします。

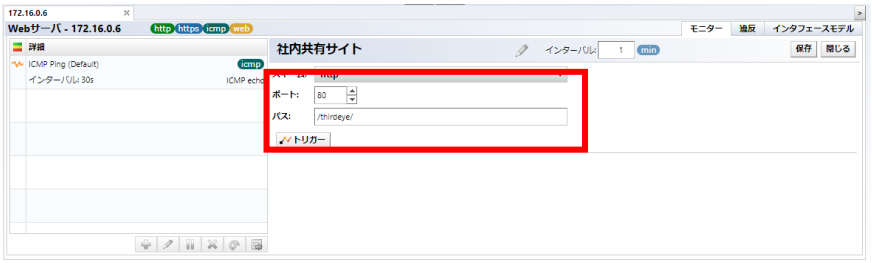


3. 任意のモニター名とインターバルを設定します。



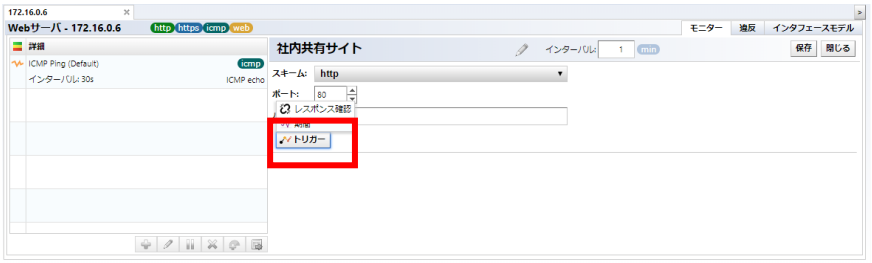
Copyright (C) 2026 LogicVein, Inc.

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。

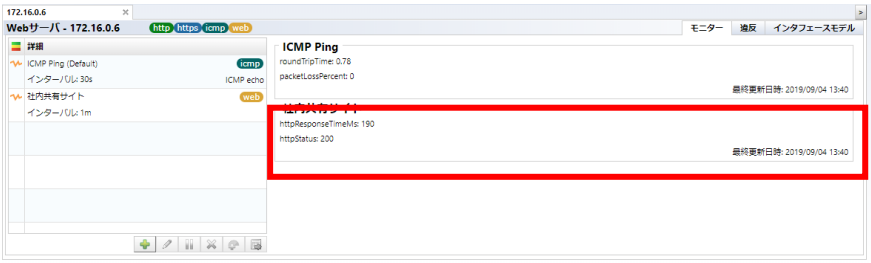
以下の画面の条件では、ステータスコードが「200」以外の場合がアラート対象になります。

※各項目の詳細については、「5.3.5 しきい値を設定して監視する」を参照してください。

7. ［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。

Copyright (C) 2026 LogicVein, Inc.

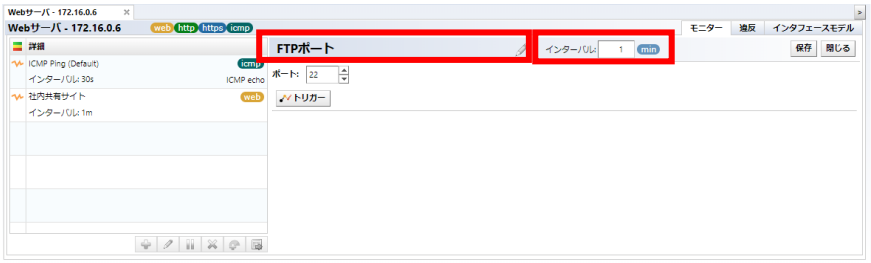


7.1.2 TCP ポートを監視する

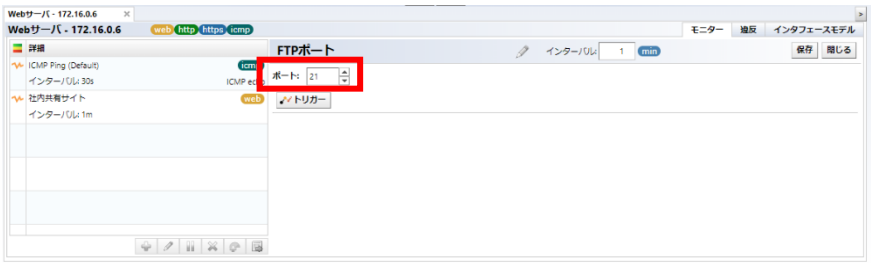
TCP ポートに syn メッセージを送信し、応答があるかを確認することができます。

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。

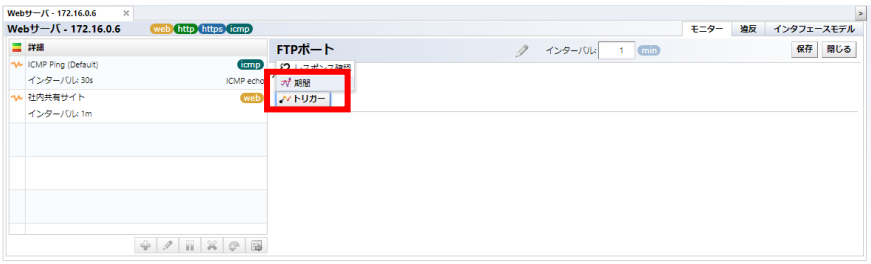


3. 監視するポート番号を設定します。



Copyright (C) 2026 LogicVein, Inc.

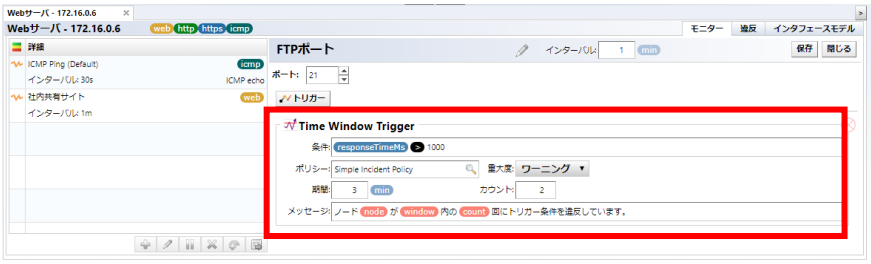
4. ［トリガー］をクリックし、［期間］をクリックします。



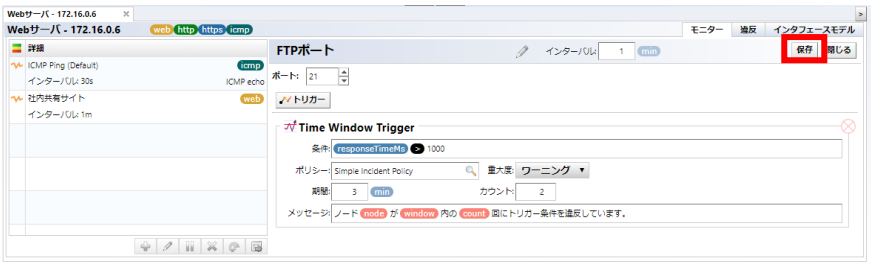
5. 各項目を設定します。

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、「5.3.5 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。



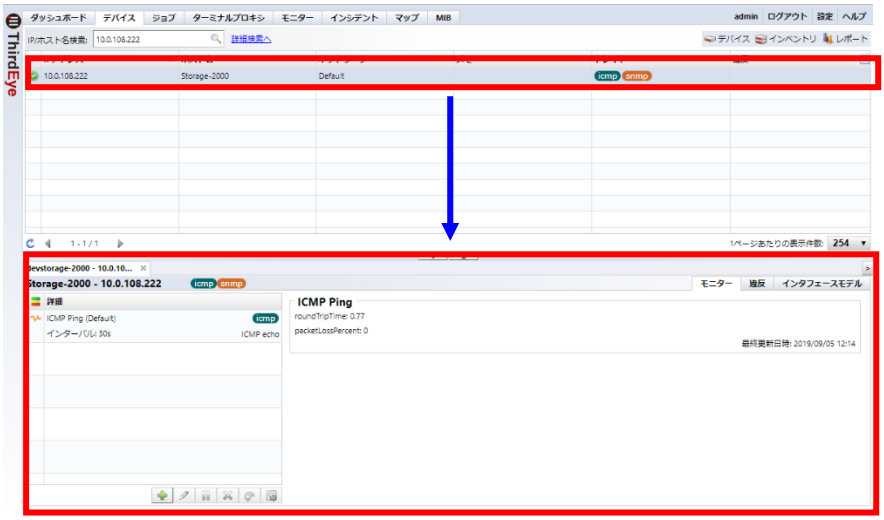
保存後、リクエストが開始され正常に取得できればデバイス詳細画面にデータが表示されます。

Copyright (C) 2026 LogicVein, Inc.

7.1.3 計算式を使用した監視をする

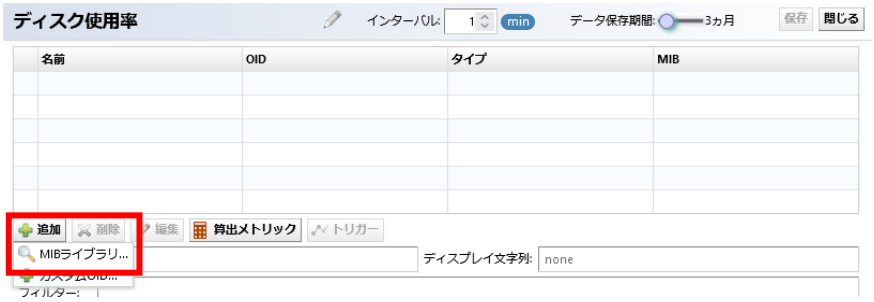
ThirdEye では、カスタム計算式を使用して取得したデータを自動で計算することができます。例えば、標準 MIB である HOST-RESOURCE-MIB にはサーバのディスクのサイズと使用量の MIB はありますが、使用率(%)の MIB はありません。カスタム計算式を使用することで、ディスクのサイズと使用量を計算して使用率を出すことができます。ここでは、HOST-RESOURCE-MIB を例に手順を記載します。

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。



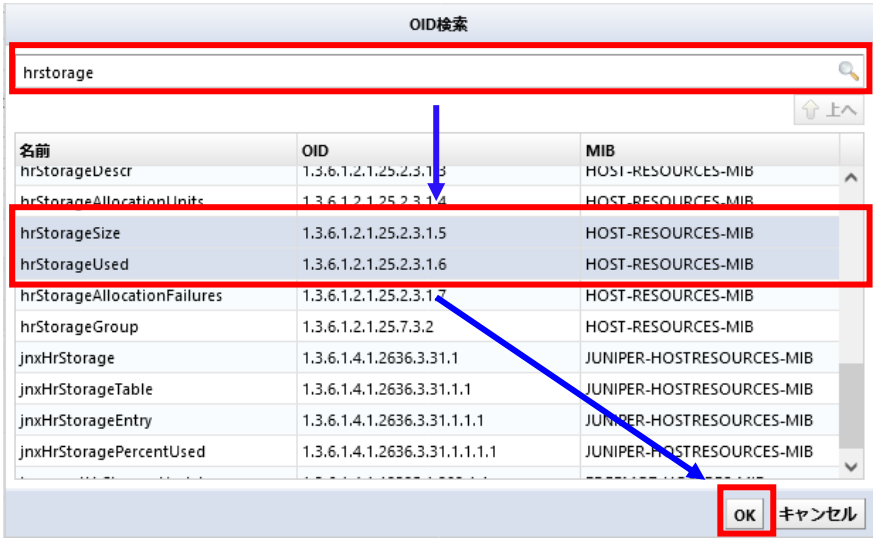
2. 左下の［+(追加)］をクリックし、「SNMP」をクリックします。
3. 任意のモニター名とインターバルを設定します。

4. ［追加］->[MIB ライブラリ]をクリックします。

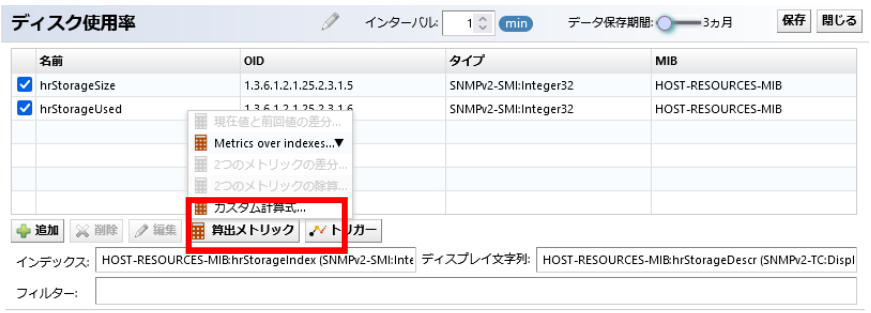


Copyright (C) 2026 LogicVein, Inc.

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

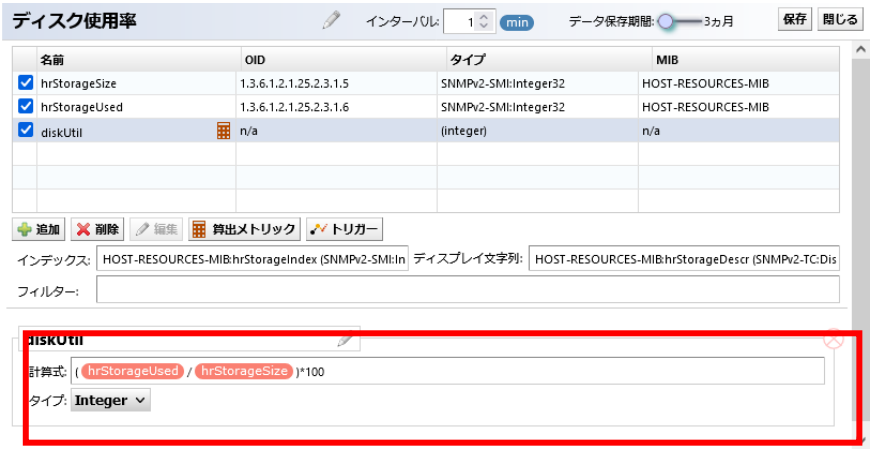


6. ［算出メトリック］→［カスタム計算式］をクリックします。



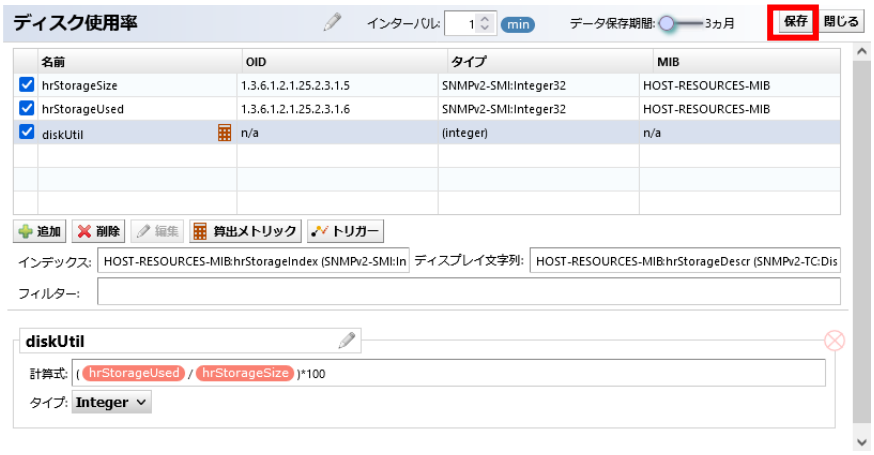
7. 名前と計算式を入力し、タイプを選択します。

タイプは、Integer または Float を選択できます。Integer では整数を使用し、Float では小数点第二位まで使用します。

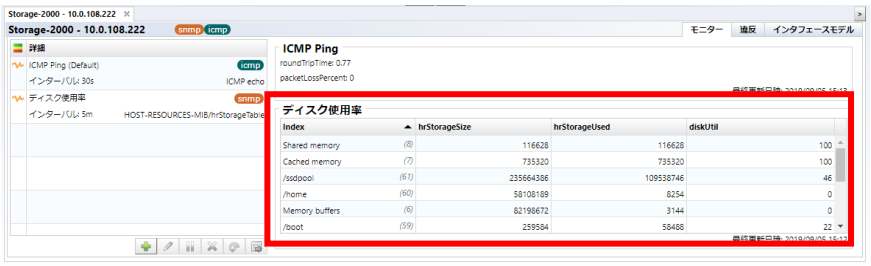


Copyright (C) 2026 LogicVein, Inc.

8. ［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。



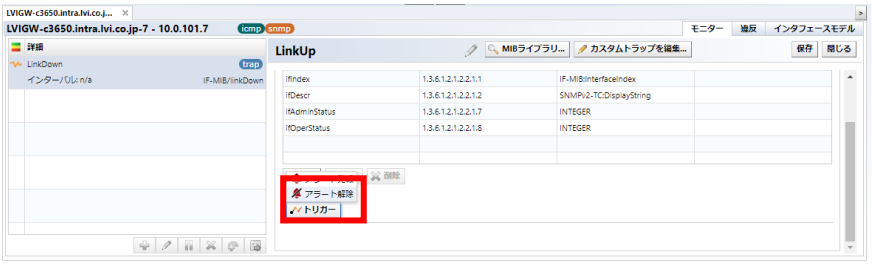
カスタム計算式を使用しても、計算後の値に対して、しきい値を設定することができます。しきい値設定については、「5.3.5 しきい値を設定して監視する」を参照してください。

Copyright (C) 2026 LogicVein, Inc.

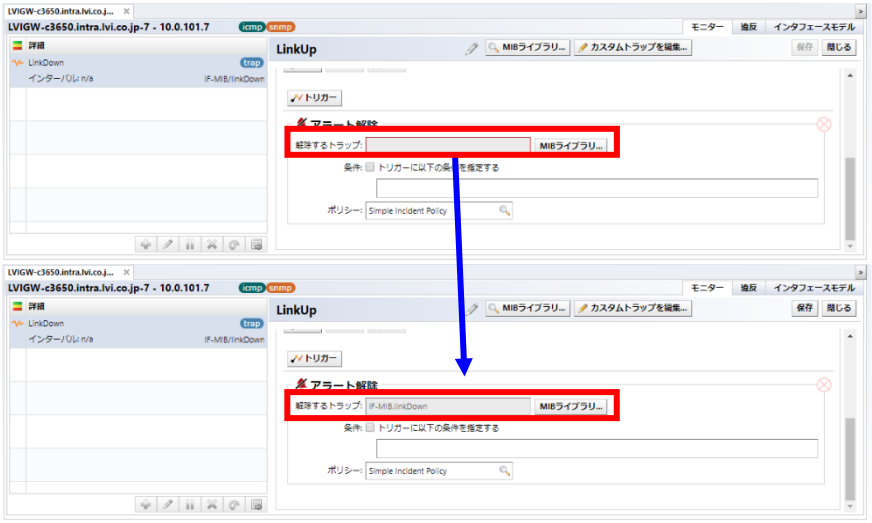
7.1.4 トラップ受信時に特定のトラップインシデントを自動でクリアする

相関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な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、［アラート解除］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。



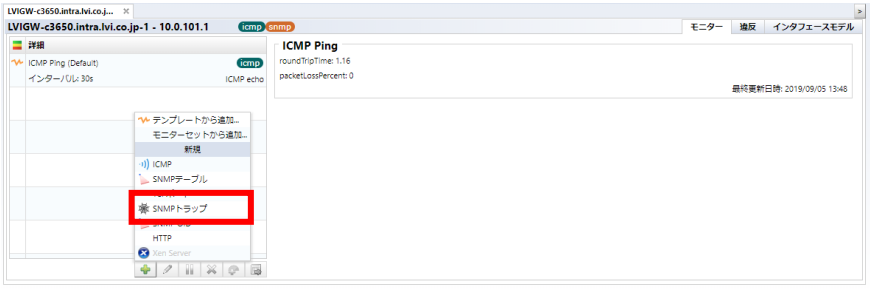
5. ［保存］をクリックします。

Copyright (C) 2026 LogicVein, Inc.

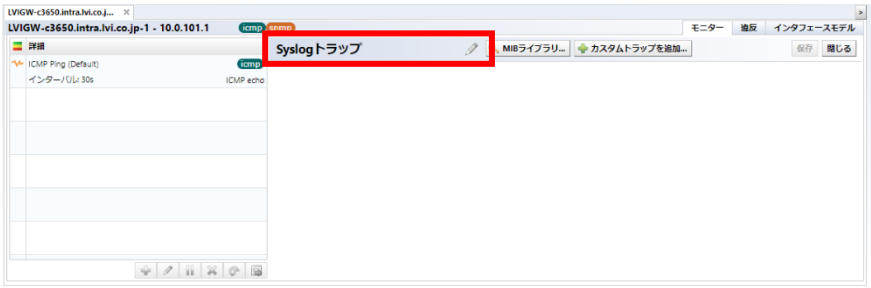
7.1.5 トラップに含まれる値でアクションを変える

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。



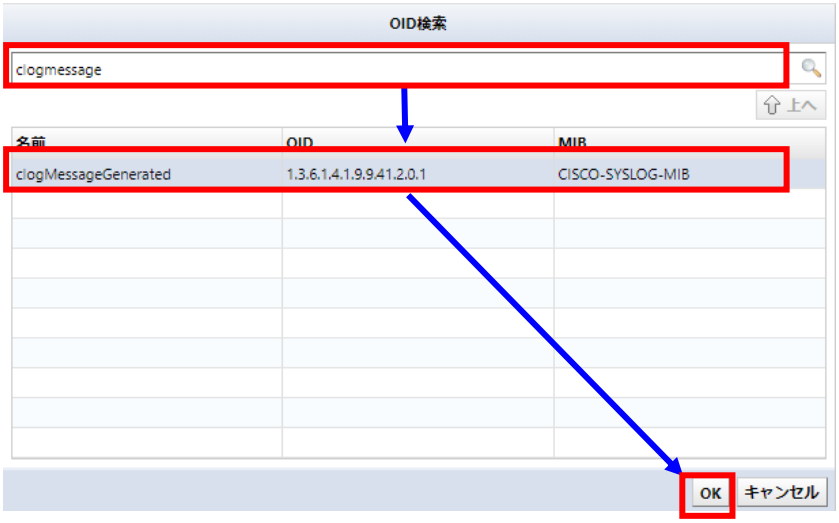
2. 任意のモニター名を表示します。



3. ［MIB ライブラリ］をクリックします。

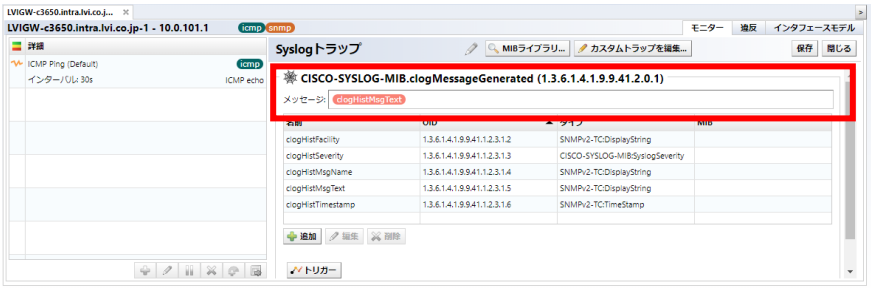
Copyright (C) 2026 LogicVein, Inc.

4. 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。

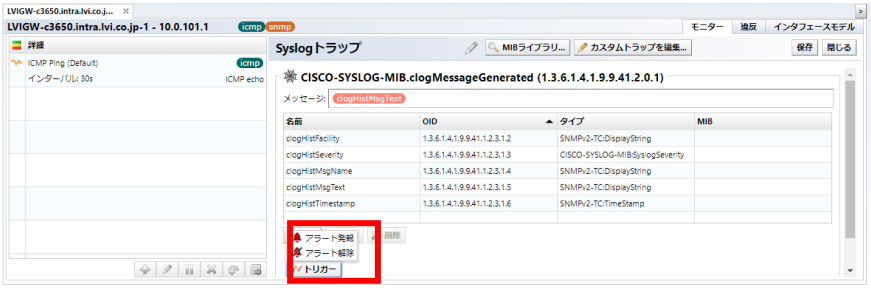


5. 障害発生時のメッセージを入力します。

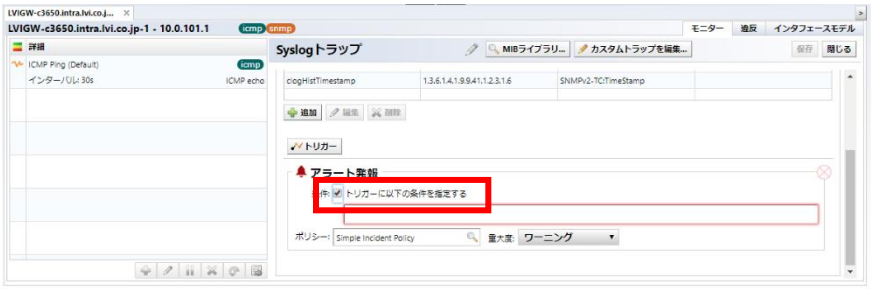
※ 以下では、トラップに含まれる clogHitMsgText(メッセージ内容)を表示します。



6. ［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。



Copyright (C) 2026 LogicVein, Inc.

8. 赤枠に「条件」を入力します。

上図の例では、clogHistSeverity が error 以上（emergency、alert、critical）であり、かつ clogHistMsgText の値に「LogicVein」が含まれない場合がアラートの対象となります。

メモ： clogHistSeverity の条件式について

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

機器から送信される `clogHistSeverity` の情報は、数値として送信されます。ThirdEye では、この数値を MIB 定義に基づいて文字列に変換して表示します。

MIB ファイルでは、`clogHistSeverity` の値は以下のように定義されています。

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

この定義に基づき、条件式「`clogHistSeverity < error (4)`」の場合、`error (4)` より小さい値である `emergency (1)`、`alert (2)`、`critical (3)` がアラート対象となります。

Copyright (C) 2026 LogicVein, Inc.

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。

Copyright (C) 2026 LogicVein, Inc.

7.1.6 Agent-D を使用したサーバ監視をする

Agent-D は、サーバ監視用のエージェントです。Windows または Linux サーバにインストールすることで、CPU 使用率やメモリ使用量、ログなどの情報を取得できます。

エージェントによる監視では、監視対象デバイスごとにエージェントをインストールする必要があります。そのため、監視対象デバイスが多い場合は、インストール作業に時間がかかることがあります。ThirdEye では、この作業負担を軽減するために、複数の監視対象デバイスに対して Agent-D を一括で配布してインストールできます。

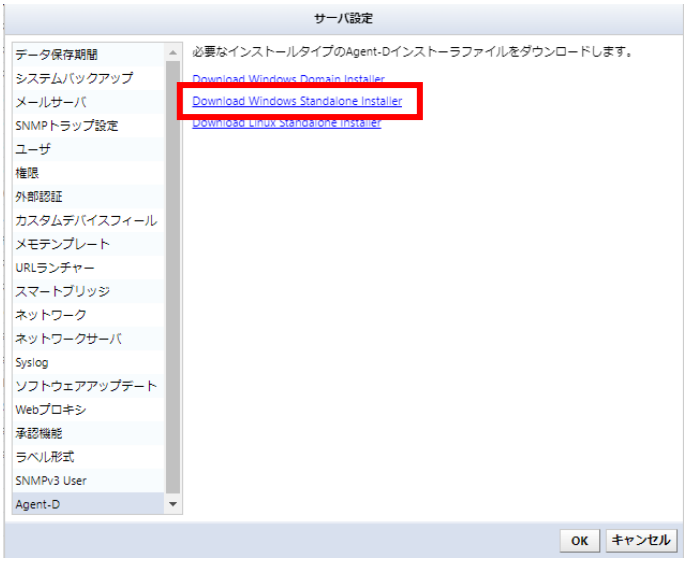
7.1.6.1 Windows にインストールする

(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 2016/2019/2022 です。

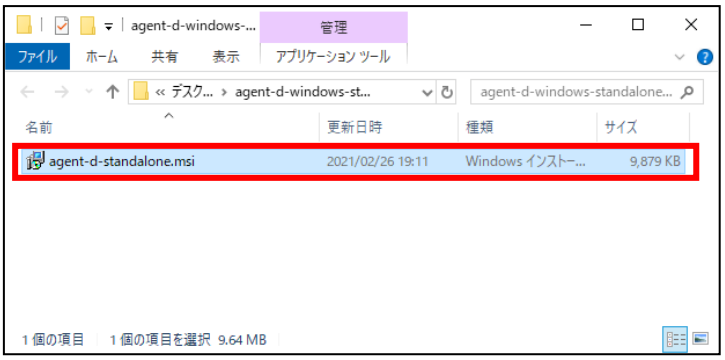
1. グローバルメニューの［設定］をクリックします。

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

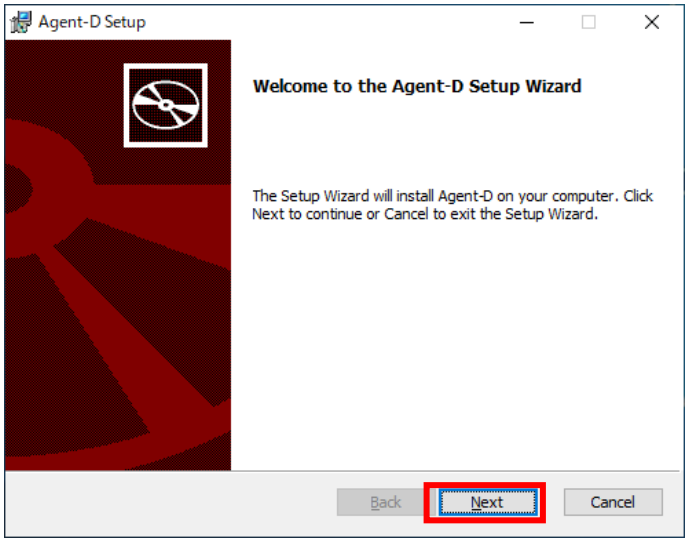


Copyright (C) 2026 LogicVein, Inc.

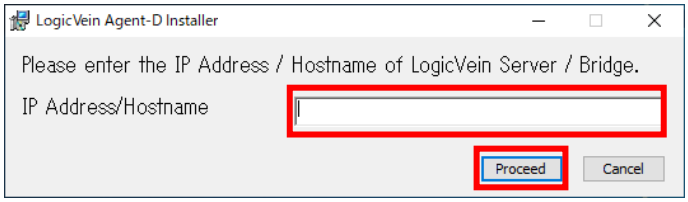
3. ダウンロードしたファイルをインストールする Windows サーバにコピーします。
4. ダウンロードしたファイルを解凍し、「agent-d-standalone.msi」をダブルクリックして実行します。



5. ［Next］をクリックします。

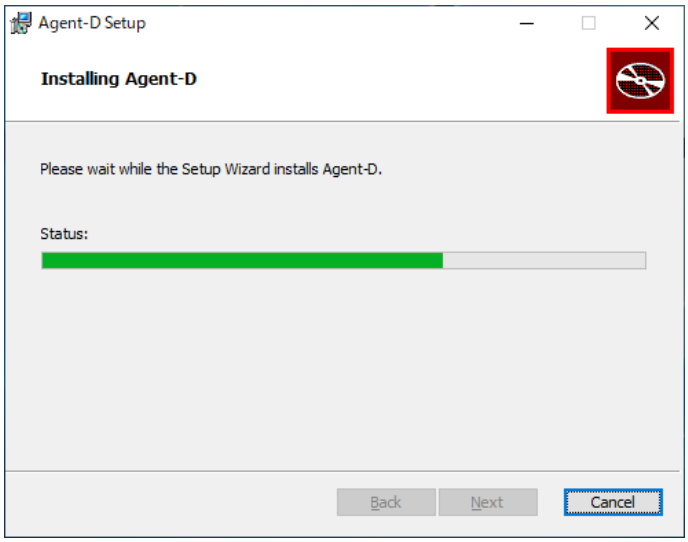


6. ThirdEye の IP アドレスまたはホスト名を入力し、［Proceed］をクリックします。

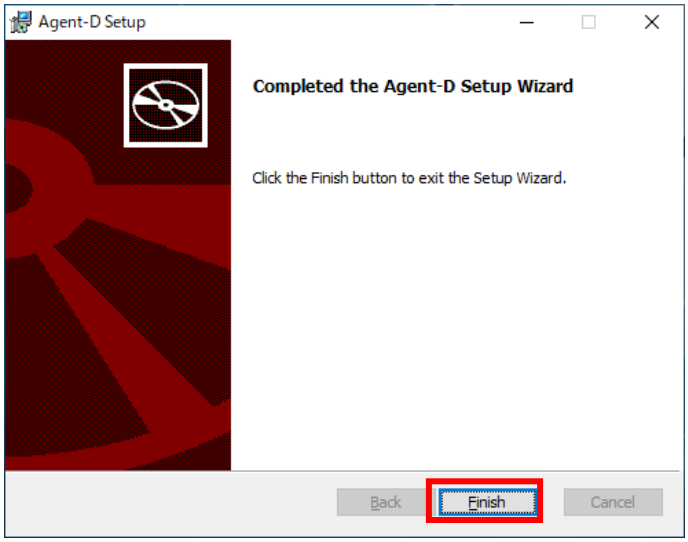


Copyright (C) 2026 LogicVein, Inc.

7. インストールが開始されます。



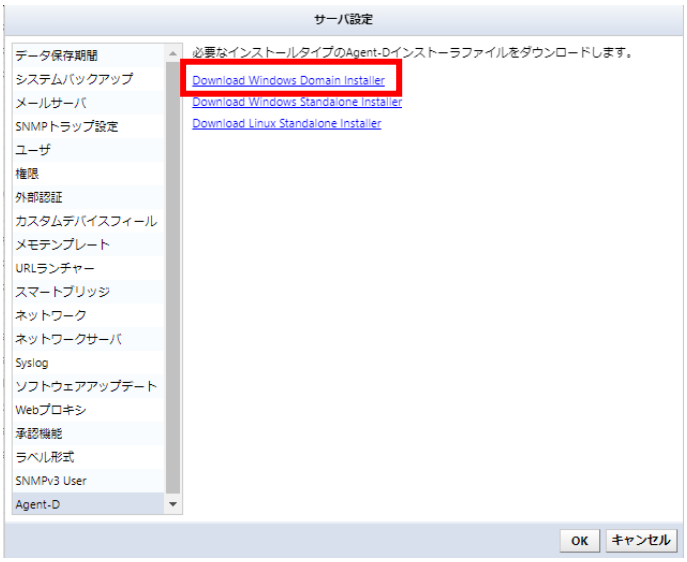
8. ［Finish］をクリックします。



Copyright (C) 2026 LogicVein, Inc.

（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

Copyright (C) 2026 LogicVein, Inc.

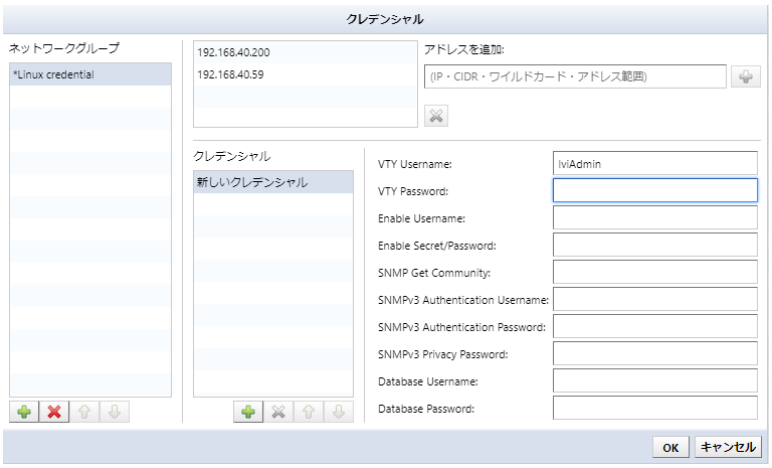
7.1.6.2 Linux にインストールする

7.1.6.3 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。コンフィグバックアップなどと同様にデバイスを一括選択することで、多数のデバイスに一括配布することができます。

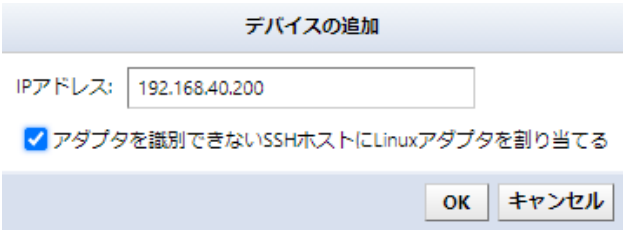
1. SSH 接続するための認証情報（ユーザ名/パスワード）を設定します。

   ※ 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。



2. 監視対象の Linux デバイスを追加します。

   以下の画像は、1 台ずつ登録する場合の一例です。

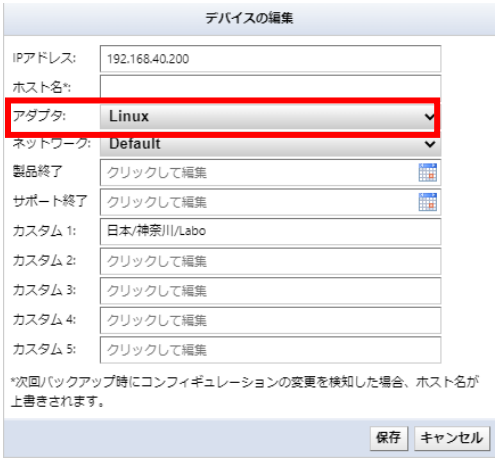


Copyright (C) 2026 LogicVein, Inc.

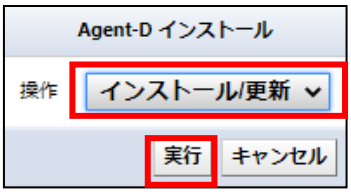
3. 監視対象の Linux デバイスが選択された状態で、デバイスメニューの［Agent-D Linux インストーラ］をクリックします。

補足

［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。

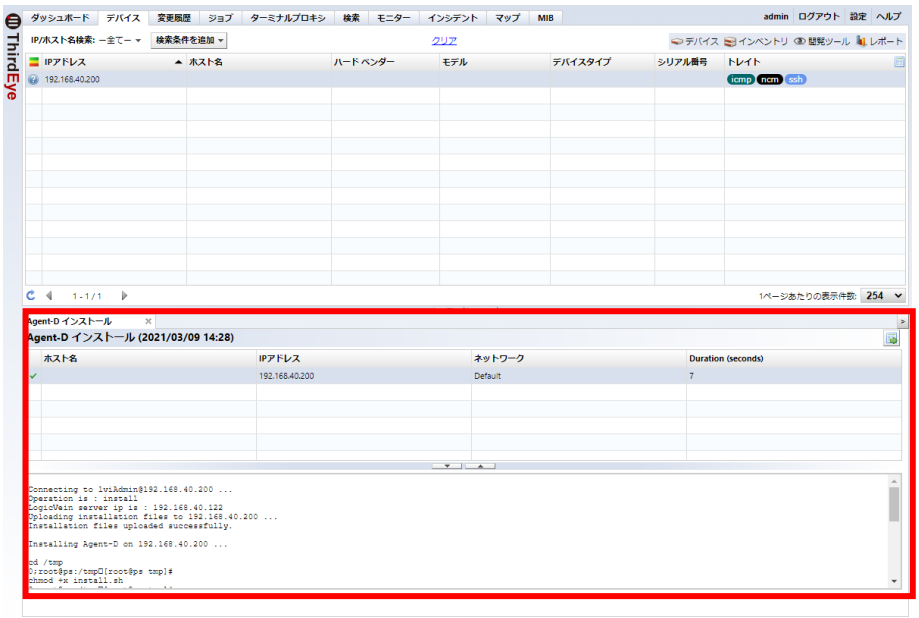


4. ［インストール/更新］を選択し、［実行］をクリックします。



Copyright (C) 2026 LogicVein, Inc.

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。



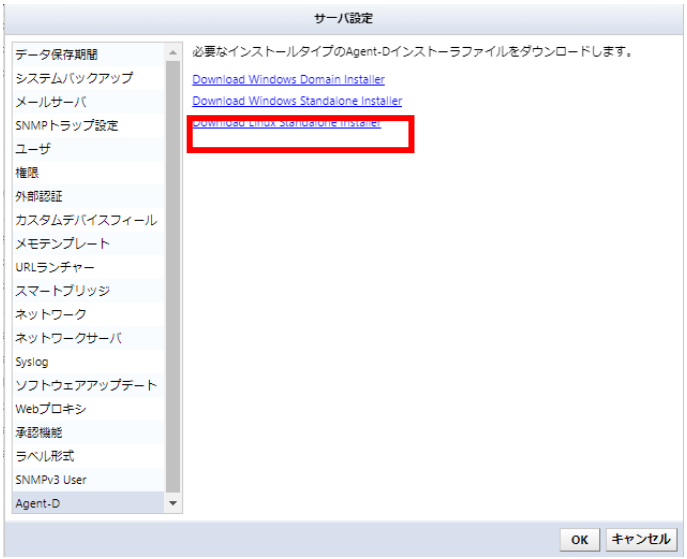
7.1.6.4 Agent-D を手動でインストールする

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。

Copyright (C) 2026 LogicVein, Inc.

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。

Copyright (C) 2026 LogicVein, Inc.

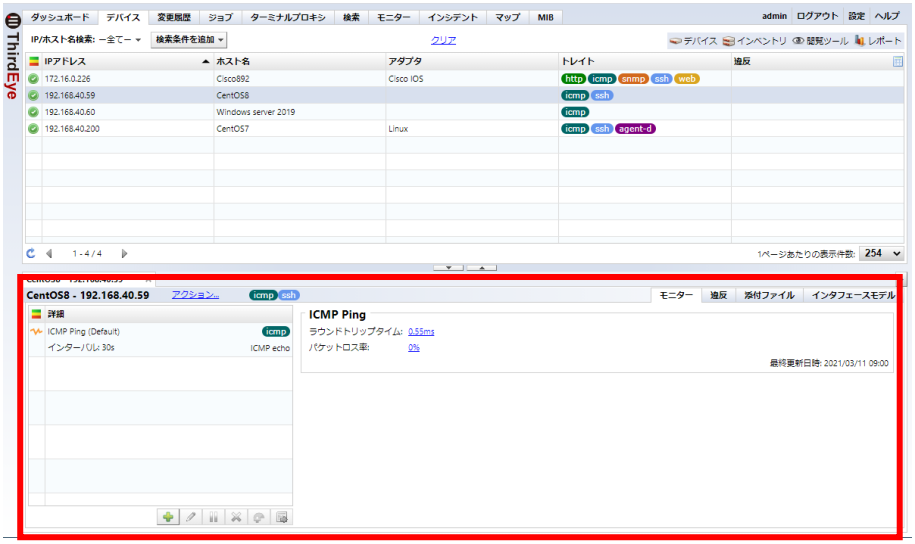
7.1.6.5　CPU 監視

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、「5.3.2 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。

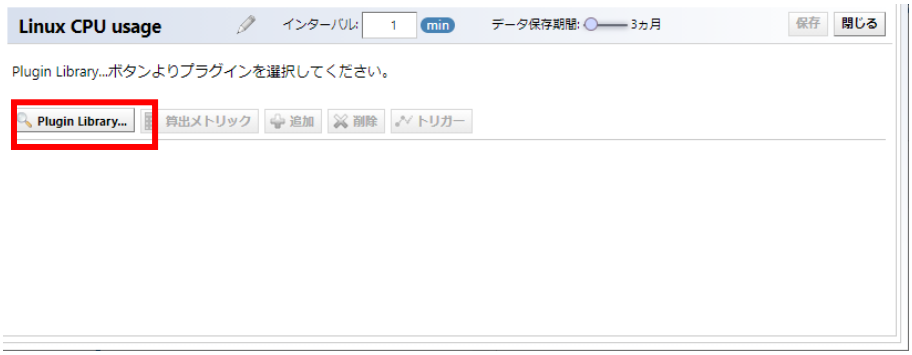


2. ［+(追加)］をクリックし、［Agent-D］をクリックします。

Copyright (C) 2026 LogicVein, Inc.

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。



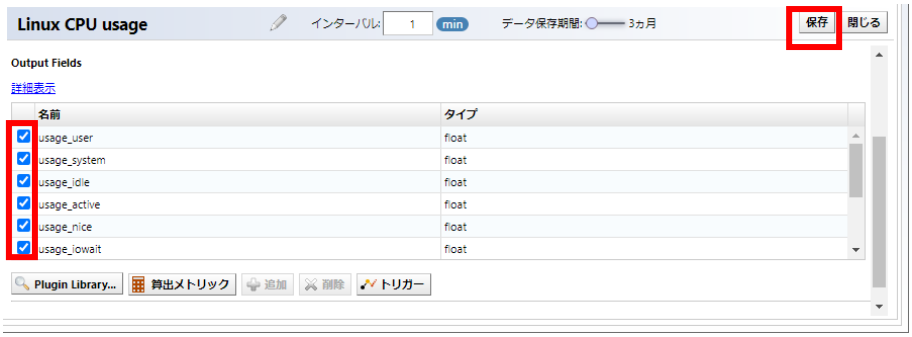
5. ［Linux CPU］を選択し、［OK］をクリックします。

6. Plugin Config で取得する項目にチェックを入れます。

Copyright (C) 2026 LogicVein, Inc.

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。

Copyright (C) 2026 LogicVein, Inc.

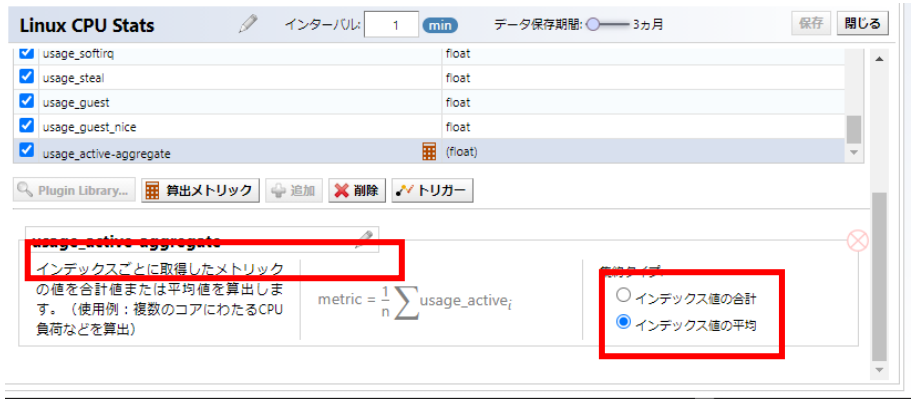
（1） CPU 全体の使用率を取得する

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。

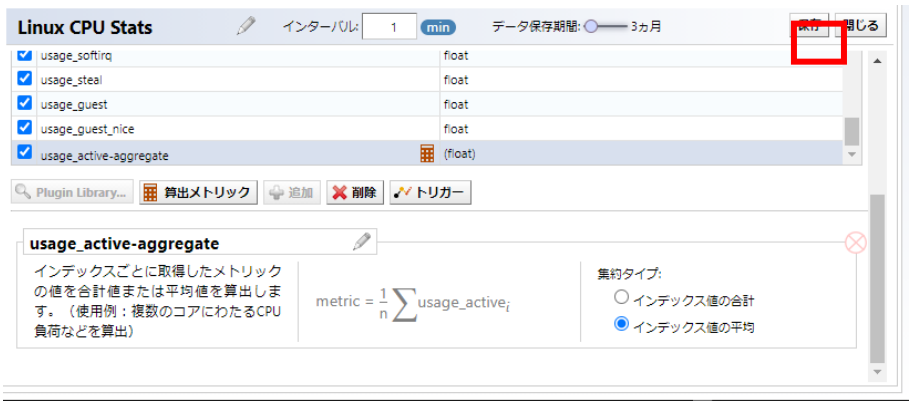
3. ［算出メトリック］→［Metrics over indexes］→［複数インデックスの集約］をクリックします。

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。

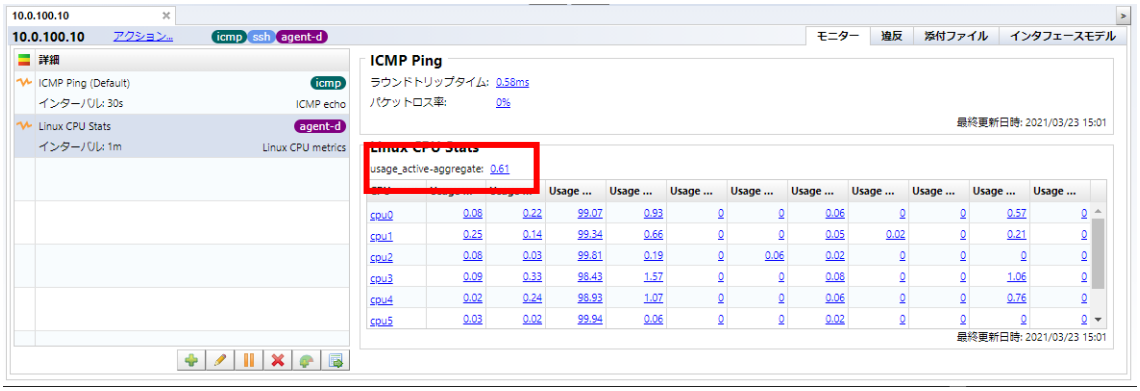


Copyright (C) 2026 LogicVein, Inc.

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_acticve 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。



Copyright (C) 2026 LogicVein, Inc.

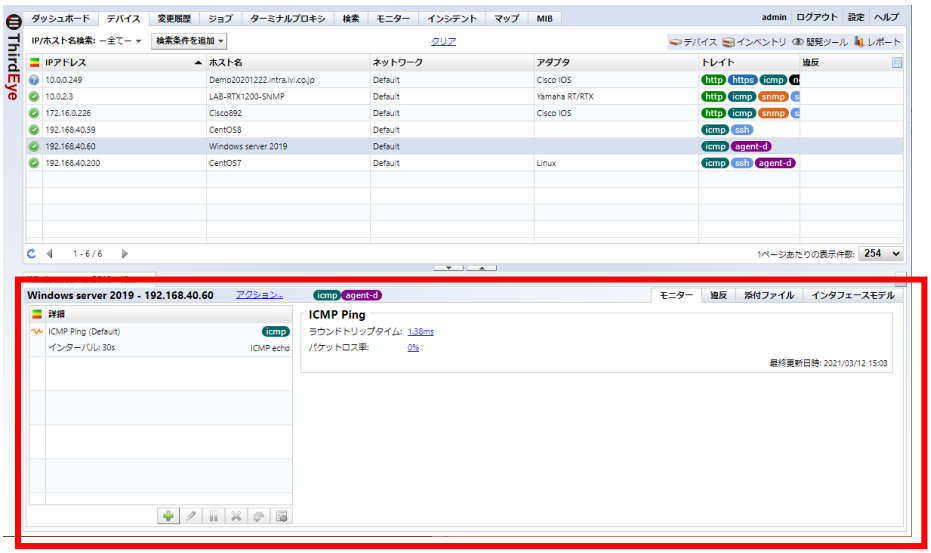
7.1.6.6　メモリ監視

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、「5.3.2 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。

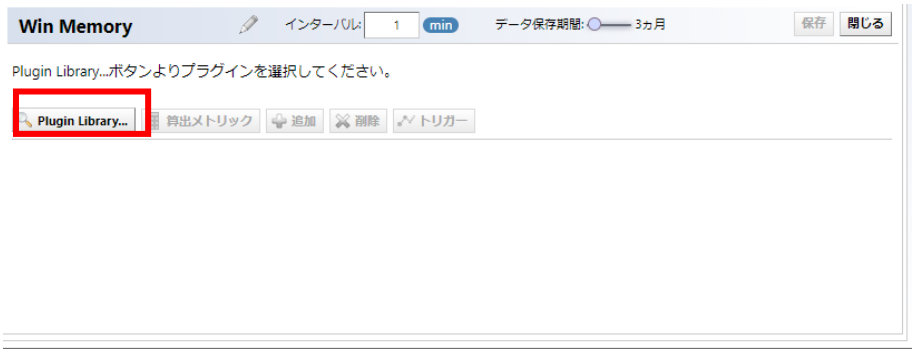


2. ［+(追加)］をクリックし、［Agent-D］をクリックします。

Copyright (C) 2026 LogicVein, Inc.

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。

Copyright (C) 2026 LogicVein, Inc.

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。

Copyright (C) 2026 LogicVein, Inc.

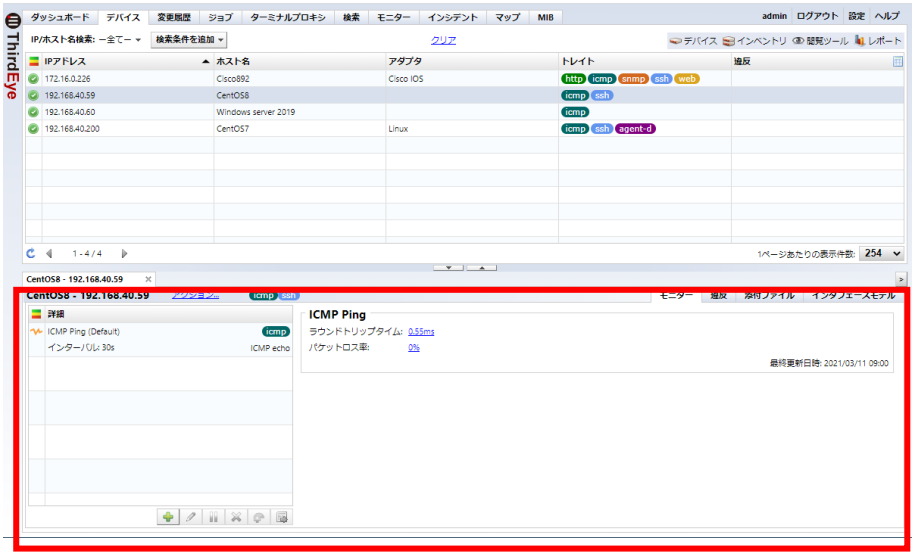
7.1.6.7　HDD 監視

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、「5.3.2 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。

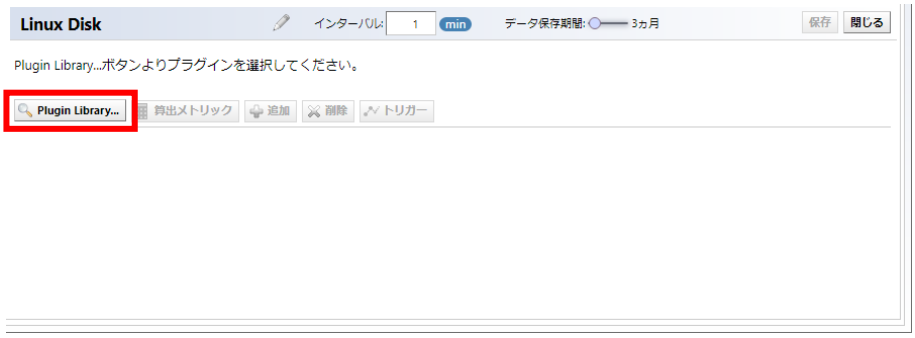


2. ［+(追加)］をクリックし、［Agent-D］をクリックします。

Copyright (C) 2026 LogicVein, Inc.

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。



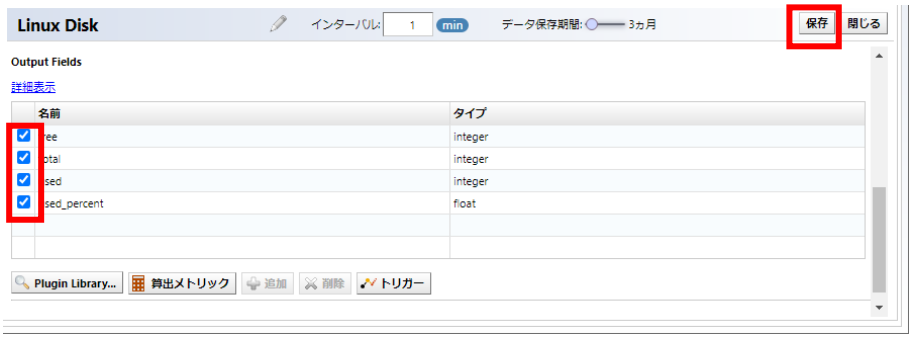
5. ［Linux Disk］を選択し、［OK］をクリックします。

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。

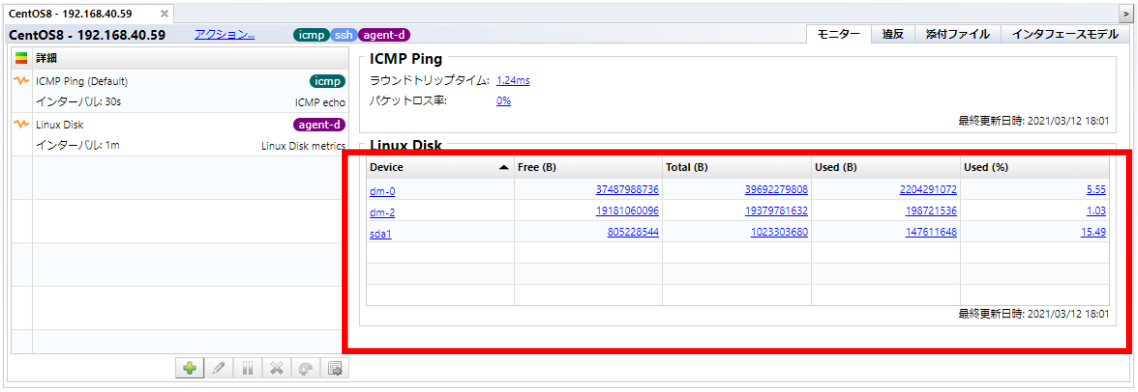
Copyright (C) 2026 LogicVein, Inc.

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。



Copyright (C) 2026 LogicVein, Inc.

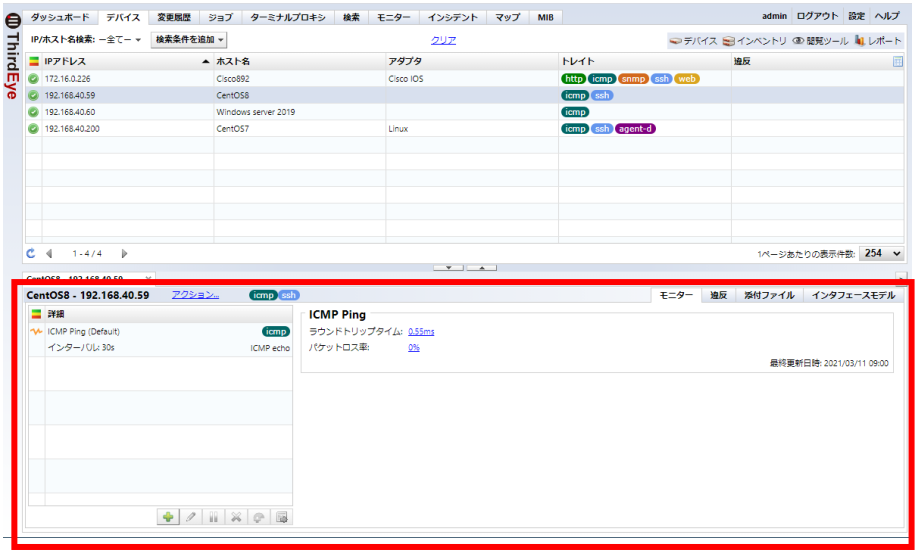
7.1.6.8　プロセス監視

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、「5.3.2 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。

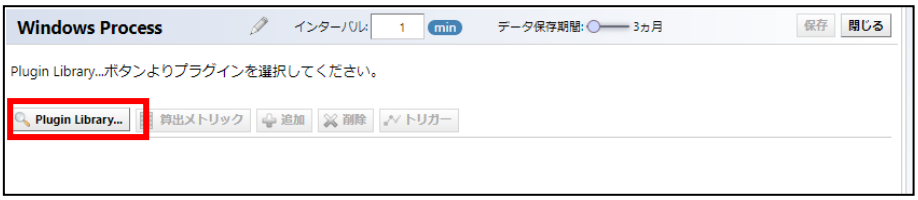


2. 追加をクリックし、［Agent-D］をクリックします。

Copyright (C) 2026 LogicVein, Inc.

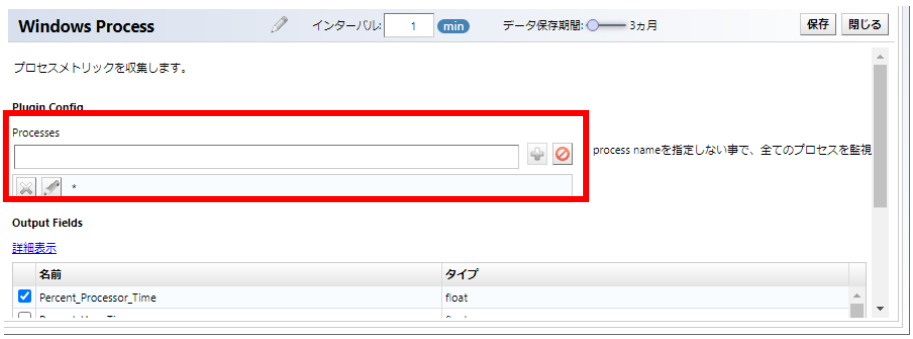
3. 任意のモニター名を入力し、［インターバル］および［データ保存期間］を設定します。

4. ［Plugin Library…］をクリックします。



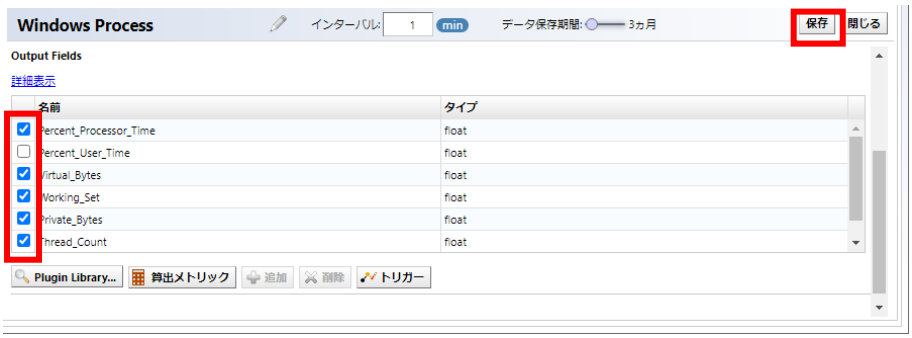
5. ［Windows Process］を選択し、［OK］をクリックします。

6. 監視するプロセス名を［Processes］欄に入力して追加します。



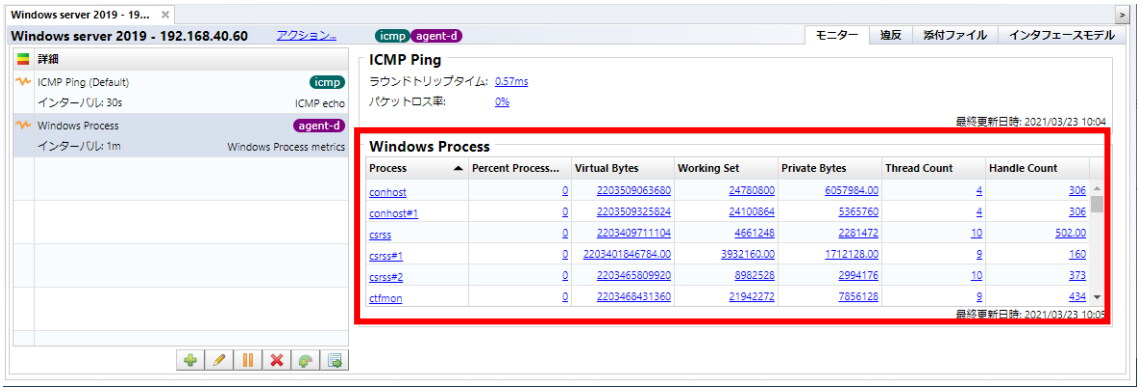
Copyright (C) 2026 LogicVein, Inc.

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。

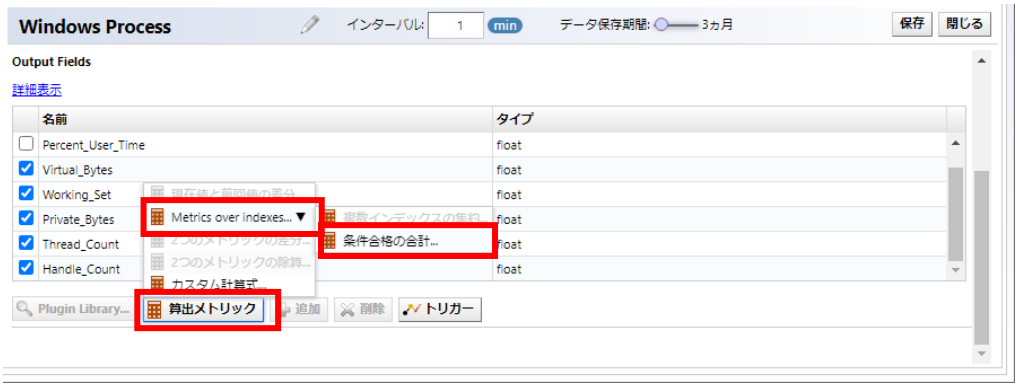


Copyright (C) 2026 LogicVein, Inc.

(1)　プロセス数を監視する

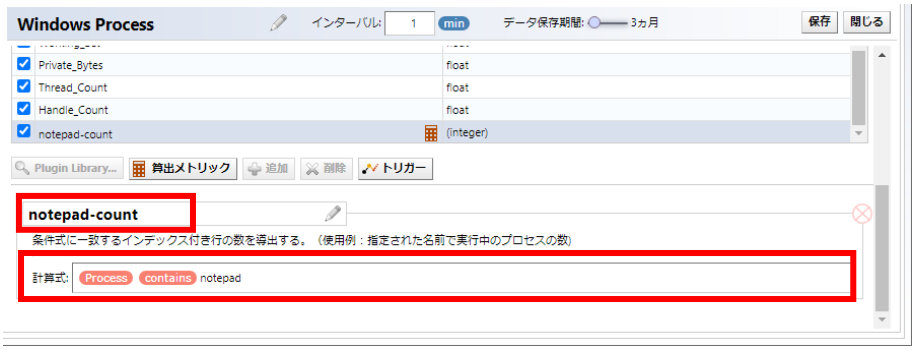
実行中のプロセス数を監視する場合、プロセス数をカウントするためのメトリックを追加する必要があります。

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}

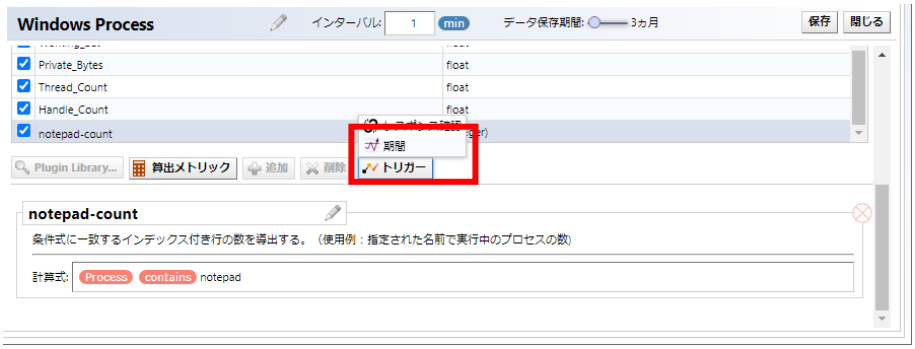
■　Linux の場合、プロセス名は「process_name」に対して設定します。

（設定例）

計算式: process_name　contains　{プロセス名}

Copyright (C) 2026 LogicVein, Inc.

4. ［トリガー］→［期間］をクリックします。

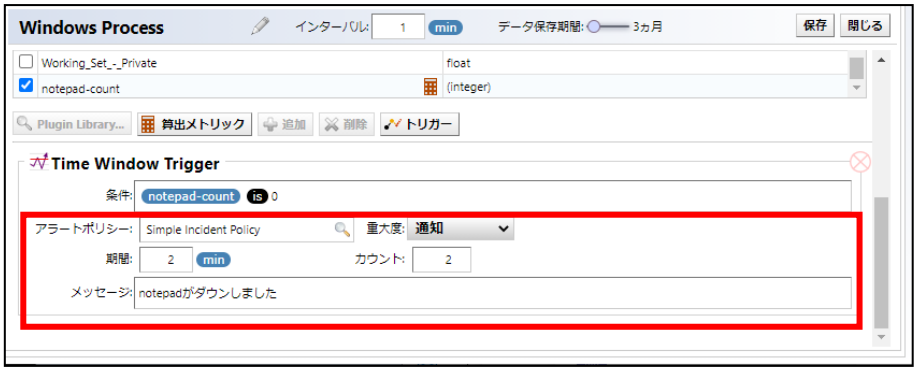


5. 作成した *count* メトリックを使用して条件を設定します。

項目	説明
条件	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）

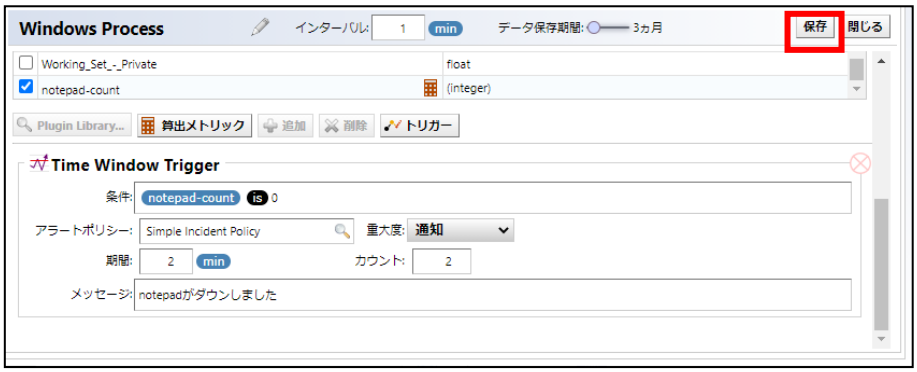
Copyright (C) 2026 LogicVein, Inc.

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。



Copyright (C) 2026 LogicVein, Inc.

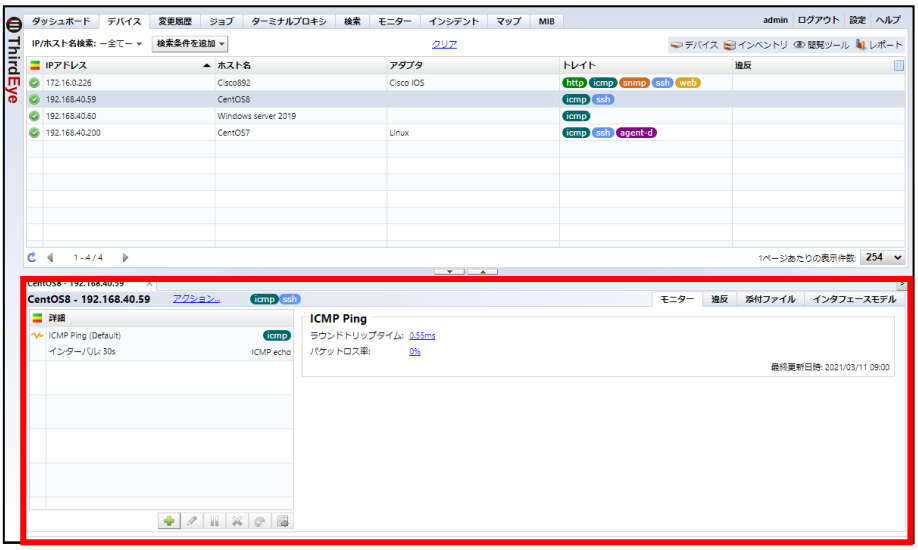
7.1.6.9 Windows サービス監視

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。

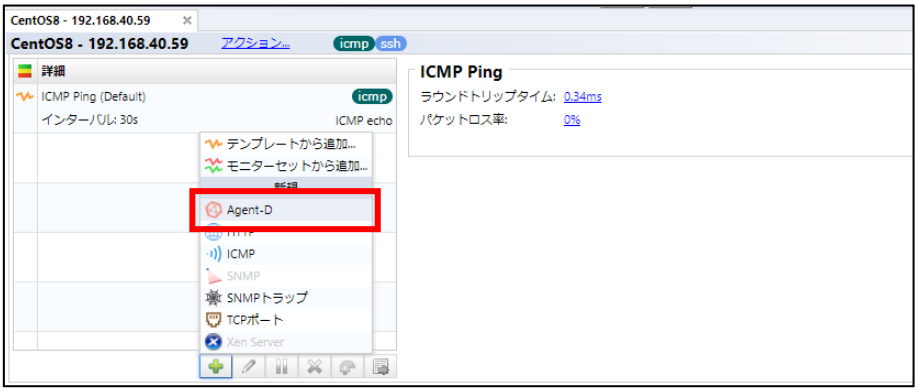
- Windows Service Status

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、「5.3.2 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。



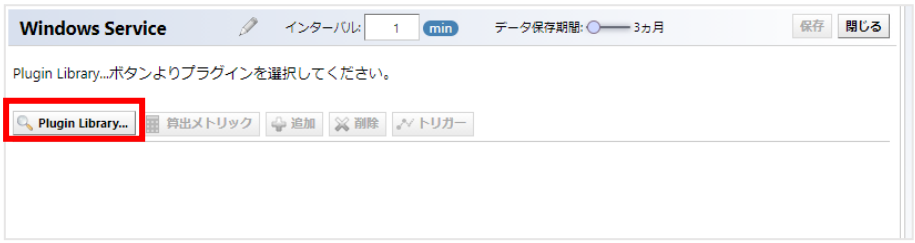
2. ［+(追加)］をクリックし、［Agent-D］をクリックします。



Copyright (C) 2026 LogicVein, Inc.

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。

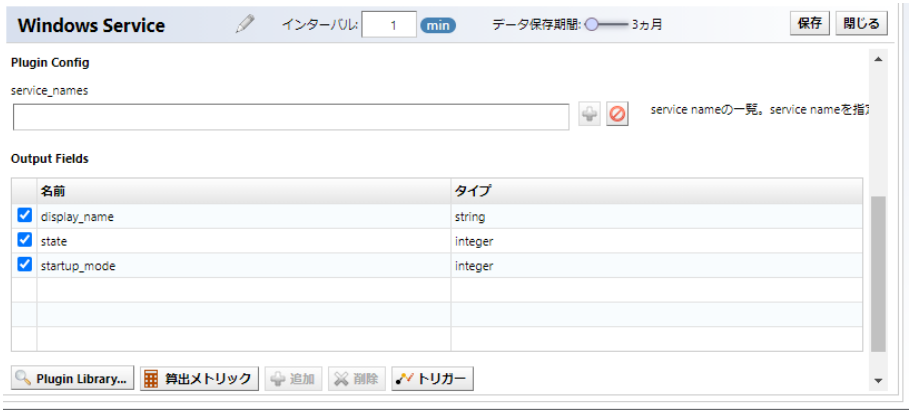
4. ［Plugin Library…］をクリックします。



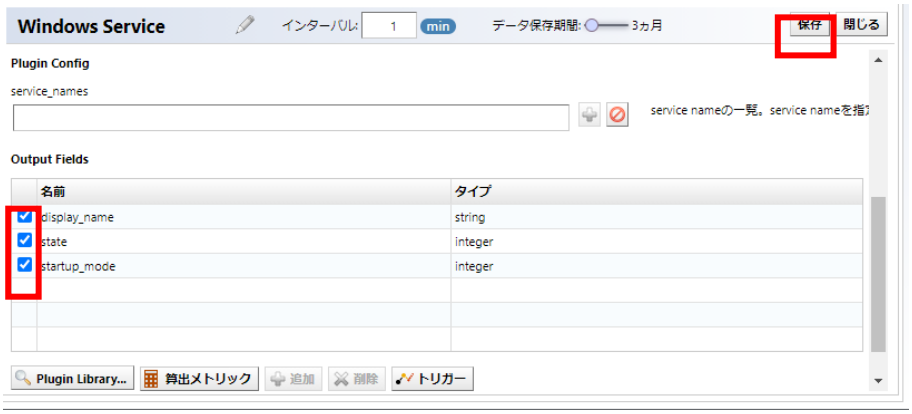
5. ［Windows Services］を選択し、［OK］をクリックします。

Copyright (C) 2026 LogicVein, Inc.

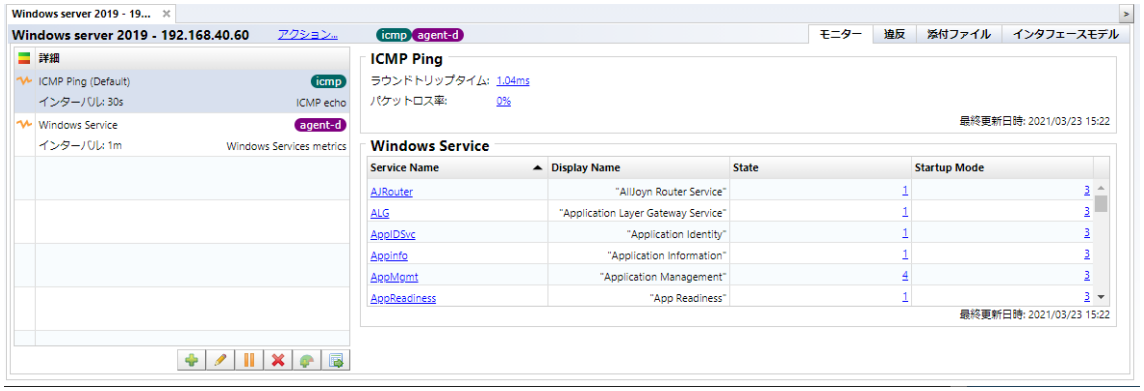
6. 監視するサービス名を［service_names］欄に入力して追加します。サービス名は完全一致です。（大文字小文字の区別はありません）



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。



Copyright (C) 2026 LogicVein, Inc.

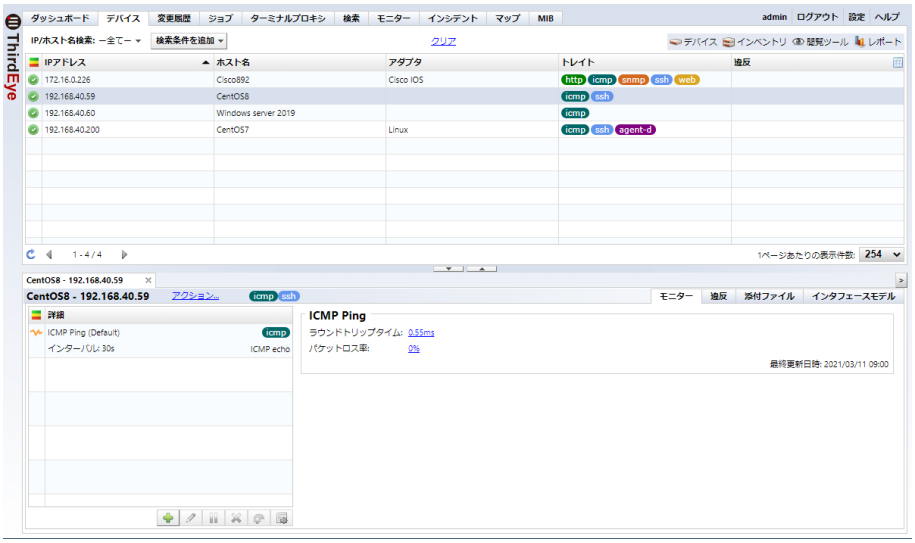
7.1.6.10　テキストログ監視

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 Fie 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。

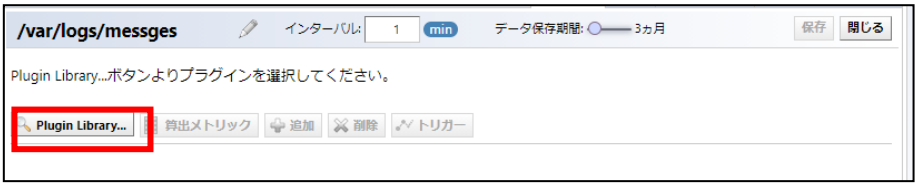


2. ［+(追加)］をクリックし、［Agent-D］をクリックします。

Copyright (C) 2026 LogicVein, Inc.

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。

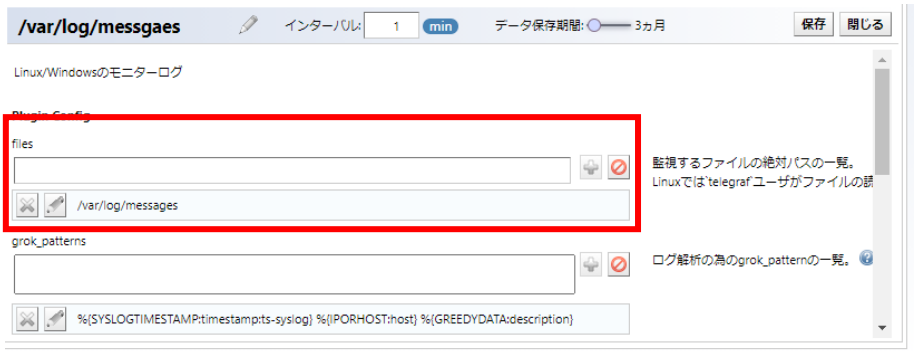
4. ［Plugin Library...］をクリックします。



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

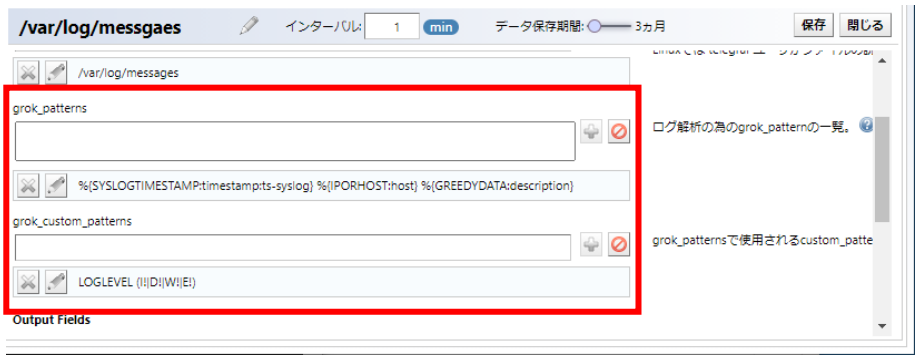
6. ［files］欄に監視するログファイルを絶対パスで追加します。

※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。



Copyright (C) 2026 LogicVein, Inc.

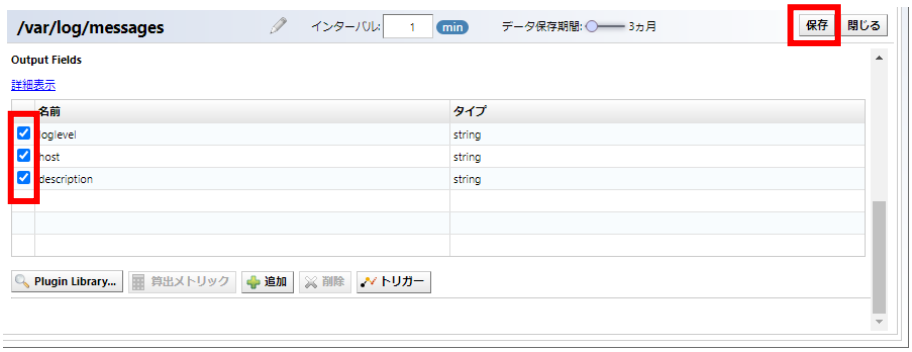
7. grok_patterns および grok_cusom_patterns を入力します。



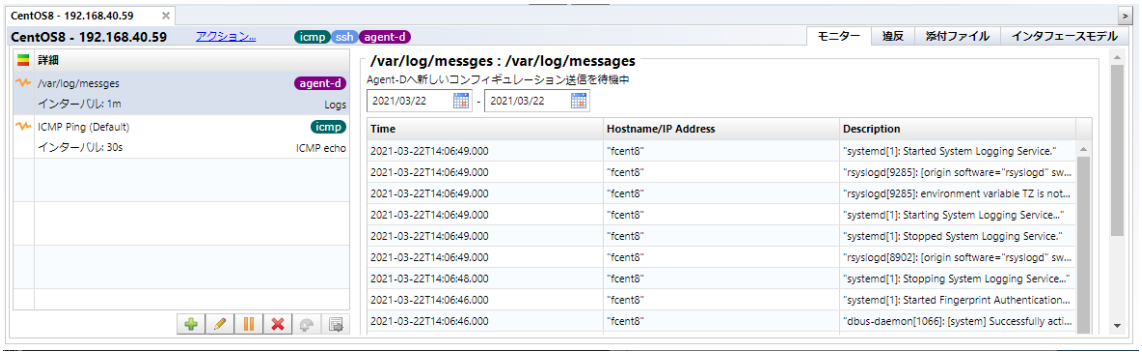
項目	説明
grok_patterns	grok_pattern を使用して、1 行のログを分割し、指定した field と一致した文字を入れるための式を入力します。 grok_pattern とは、 「%{PATTERN_NAME:FIELD_NAME:MODIFIER(optinon)}」で構成され、正規表現を定義した PATTERN_NAME にマッチした内容を FIELD_NAME に入れます。 例：ログメッセージ「Aug 20 11:15:40 192.168.0.1 ERROR systemd: Started Hostname Service.」 式: %{SYSLOGTIMESTAMP:timestamp}¥s%{IPORHOST:iporhost}¥s %{LOGLEVEL:level}¥s%{GREEDYDATA:message} • 「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: %{SYSLOGTIMESTAMP:timestamp} • 「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: %{IPORHOST:iporhost} • 「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: %{LOGLEVEL:level} • 「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	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。 PATTERN__NAME (正規表現)

Copyright (C) 2026 LogicVein, Inc.

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。



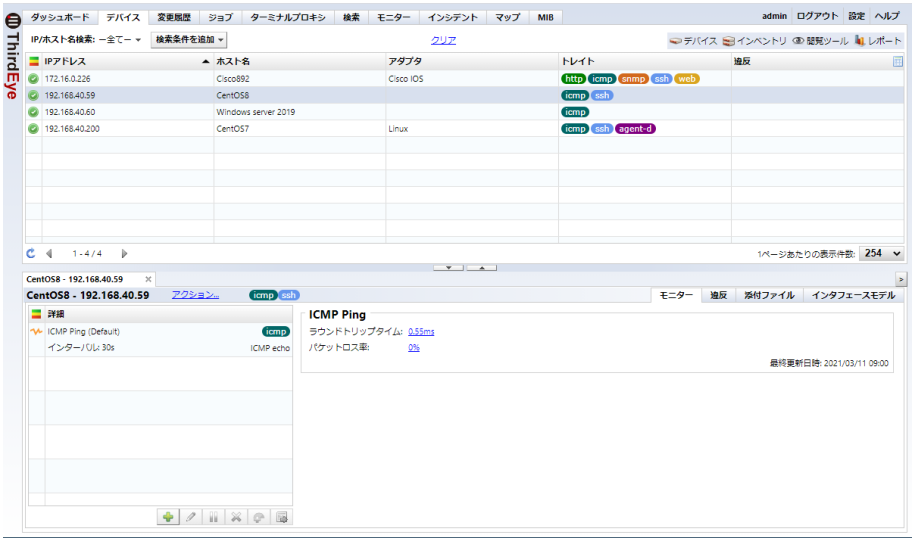
Copyright (C) 2026 LogicVein, Inc.

7.1.6.11　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。

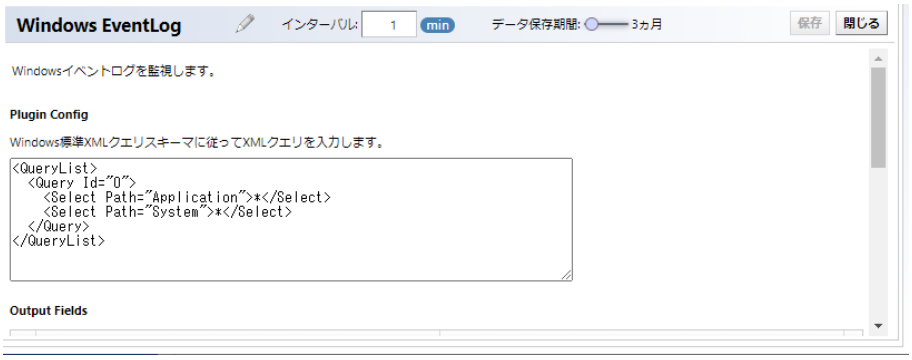
Copyright (C) 2026 LogicVein, Inc.

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。

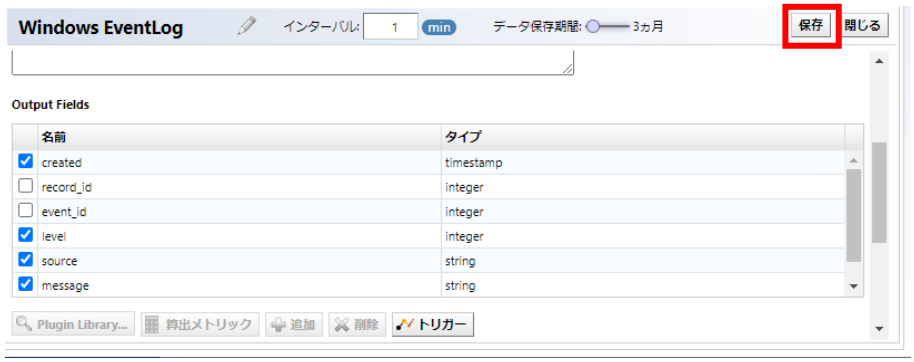
※ 「高度な設定を使用」をクリックすると XML 形式で指定することができます。



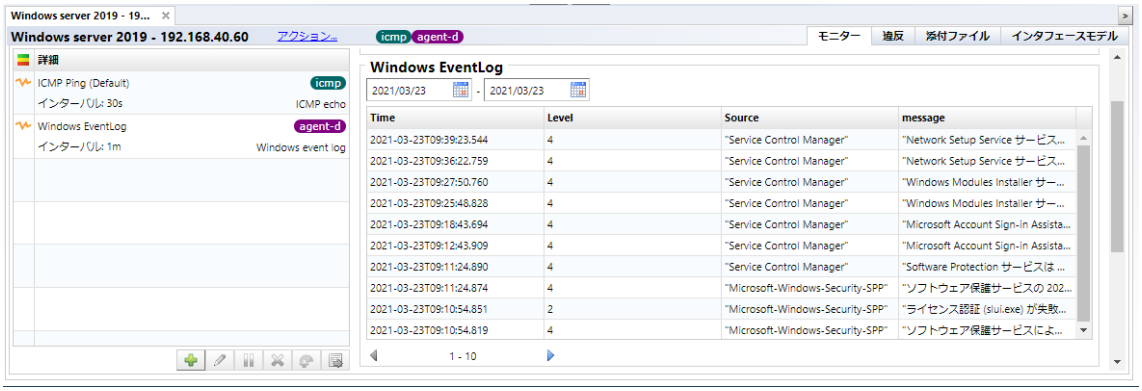
Copyright (C) 2026 LogicVein, Inc.

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。

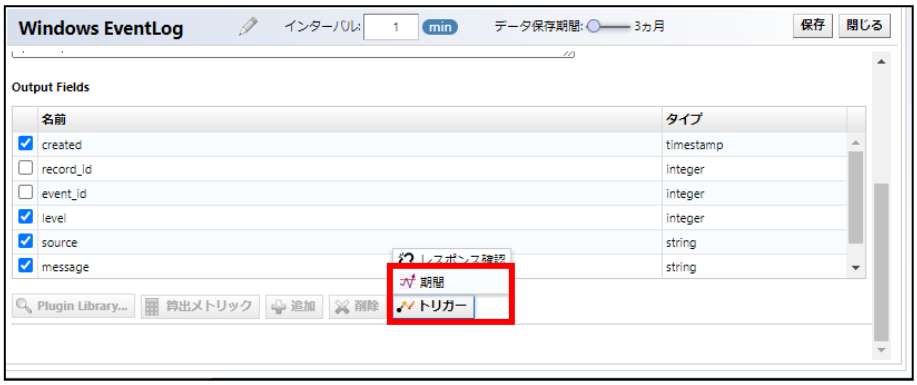


Copyright (C) 2026 LogicVein, Inc.

(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	以下の項目を使って、条件を指定することができます。 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。

Copyright (C) 2026 LogicVein, Inc.

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。

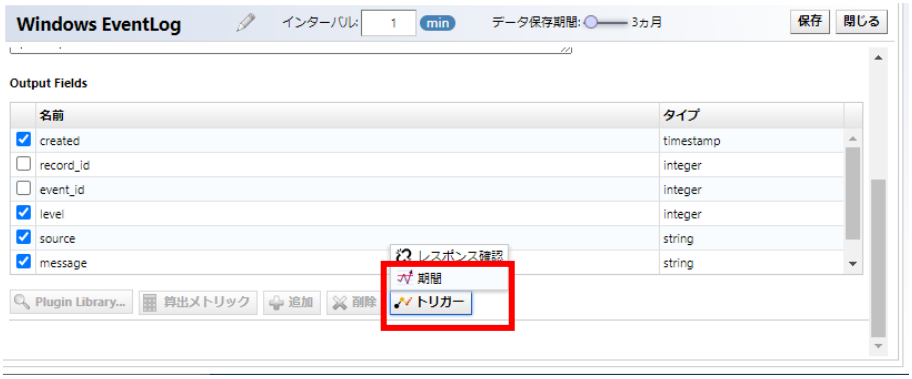
5. ［保存］をクリックします。

Copyright (C) 2026 LogicVein, Inc.

(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）

Copyright (C) 2026 LogicVein, Inc.

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。

Copyright (C) 2026 LogicVein, Inc.

7.1.6.12　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。

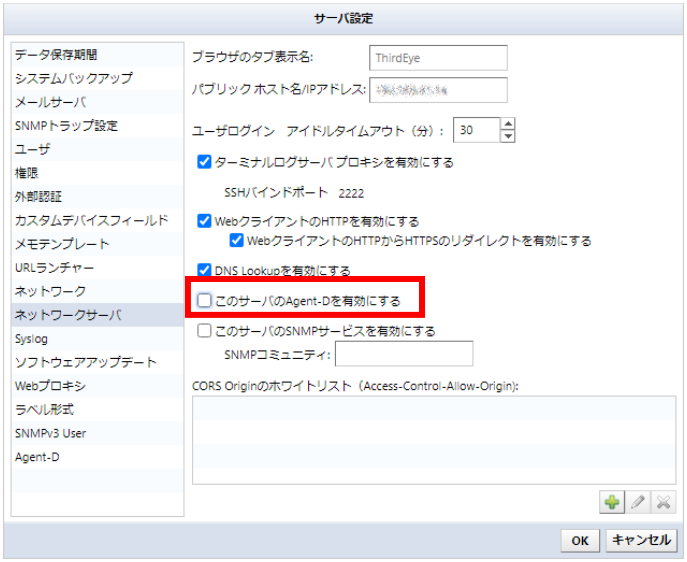
- ThirdEye Syslog Monitor

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。

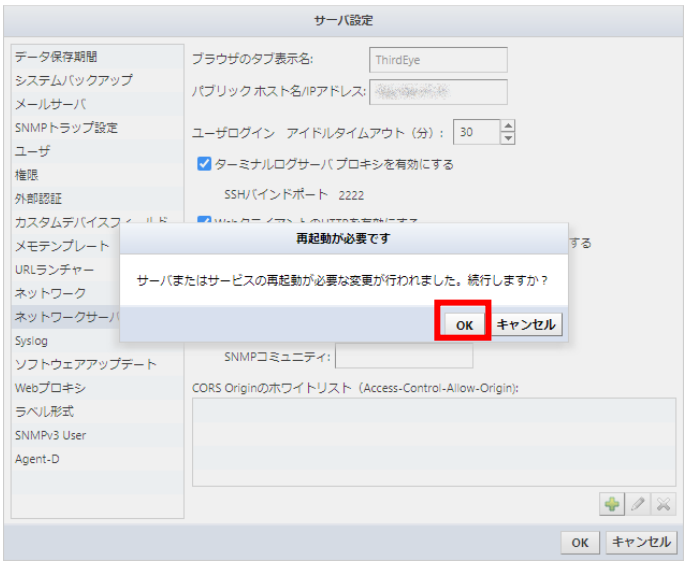


Copyright (C) 2026 LogicVein, Inc.

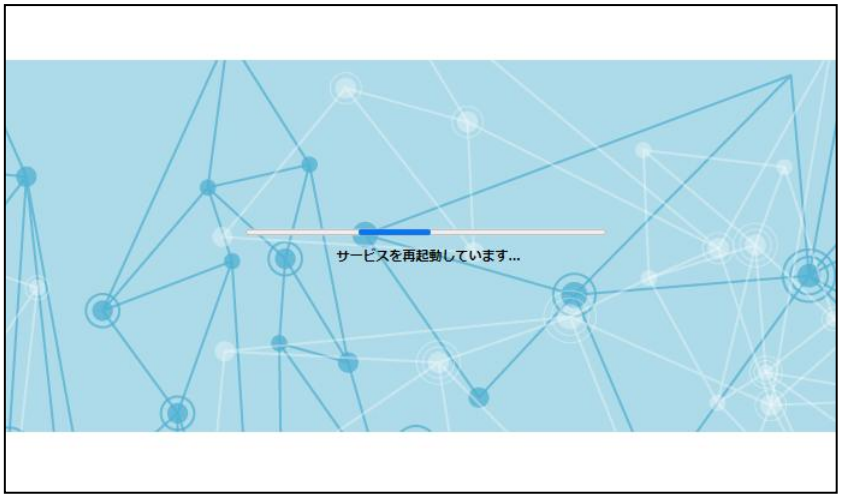
3. 再起動の確認画面で［OK］をクリックします。

［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。



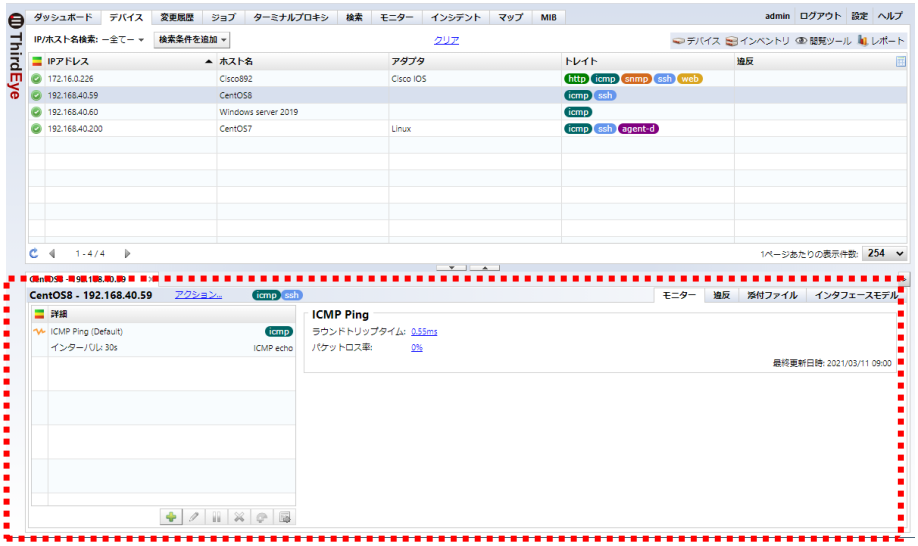
4. 「サービスを再起動しています...」のメッセージを確認し、数分待ちます。



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。

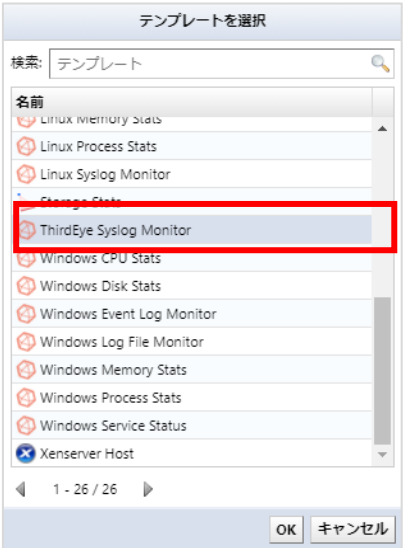
Copyright (C) 2026 LogicVein, Inc.

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。

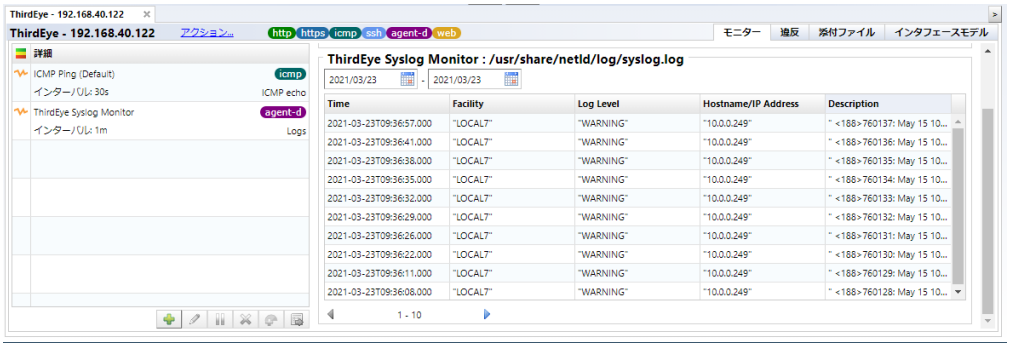


Copyright (C) 2026 LogicVein, Inc.

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。



Copyright (C) 2026 LogicVein, Inc.

(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。

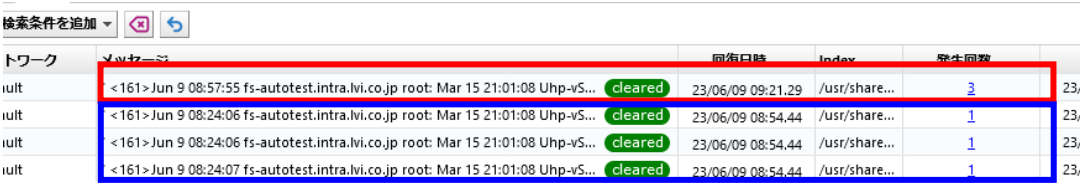
項目	説明
条件	以下の項目を使って、条件を指定することができます。 contains　（含む） そのほかの条件式（「is」，「is not」，「>」，「<」，「not contains」）を選択できますが、特定の文字列を含む条件を設定する場合は「contains」を使用してください。

Copyright (C) 2026 LogicVein, Inc.

4. 「違反の発生を自動的に 1 つの違反にまとめる」のチェックを外します。

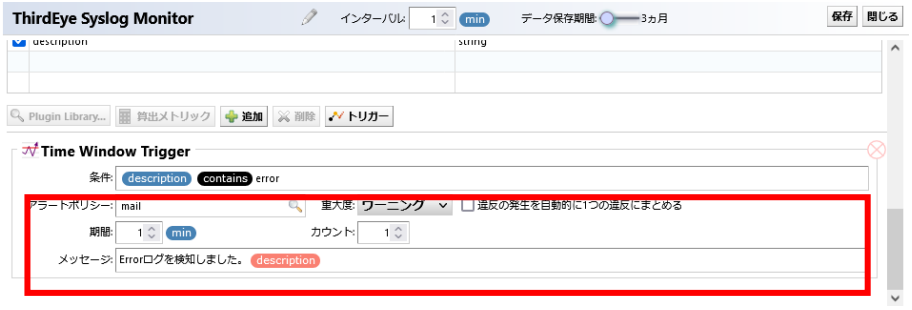
ThirdEye の特性上、同じトリガー、同じ Index で違反が発生した場合、同じ違反に集約されますが、このチェックボックスを無効にすると、条件にマッチしたログごとに違反が発生します。そのため、1 つの違反にまとめられた場合よりも多くの違反やメール送信が発生します。

ただし、ログ監視では Index が監視されるログファイル名が Index となるため何か違反発生後、別のメッセージを検知しても、最初の違反がクリアされていないと集約されてしまい、後から検知されたメッセージがわかりにくくなるため、チェックボックスをオフにすることをおすすめします。



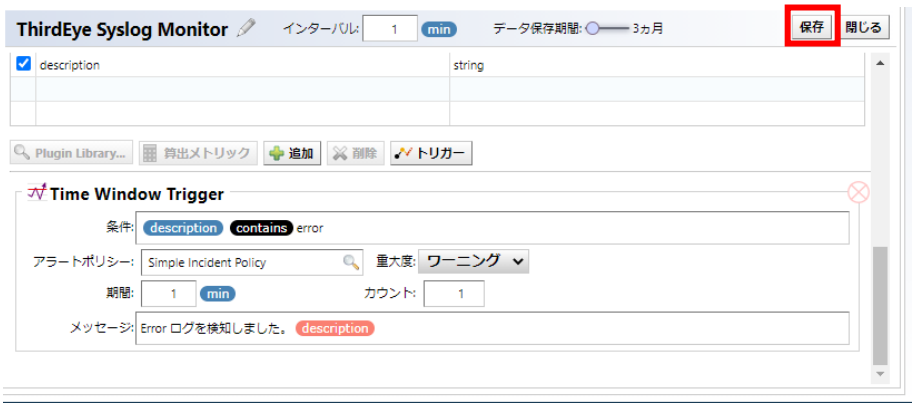
Copyright (C) 2026 LogicVein, Inc.

5. 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。

6. ［保存］をクリックします。



Copyright (C) 2026 LogicVein, Inc.

7.1.7 WMI を使用したサーバ監視をする

ThirdEye では、HTTP/SOAP ベースの WS-Management プロトコルを使用して WMI オブジェクトを取得します。現時点で取得できるオブジェクトは以下の通りです。

Win32_PerfFormattedData_PerfOS_Processor（CPU 監視）
Win32_PerfFormattedData_PerfDisk_LogicalDisk（ディスク監視）
Win32_PerfFormattedData_PerfOS_Memory（メモリ監視）
Win32_PerfFormattedData_PerfProc_Process（プロセス監視）

7.1.7.1 Windows 上での設定

Windows システムをリモートから管理するため、Windows リモート管理（WinRM）サービスが必要です。現在、Microsoft 社でサポートされているシステムにはあらかじめ WinRM がインストールされています。

はじめに、「winrm quickconfig」コマンドをコマンドプロンプトまたは Powershell から実行します。このコマンドは WinRM の規定の構成を設定します。コマンド実行後、「winrm get winrm/config/service」を実行することで現在の構成を確認できます。

```
PS C:¥Users¥Administrator> winrm get winrm/config/service
Service
    RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)(A;;GR;;;IU)S:P(AU;FA;GA;;;WD)(AU;SA;GXGW;;;WD)
    MaxConcurrentOperations = 4294967295
    MaxConcurrentOperationsPerUser = 1500
    EnumerationTimeoutms = 240000
    MaxConnections = 300
    MaxPacketRetrievalTimeSeconds = 120
    AllowUnencrypted = false
    Auth
        Basic = false
        Kerberos = true
        Negotiate = true
        Certificate = false
        CredSSP = false
        CbtHardeningLevel = Relaxed
    DefaultPorts
        HTTP = 5985
        HTTPS = 5986
    IPv4Filter = *
    IPv6Filter = *
    EnableCompatibilityHttpListener = false
    EnableCompatibilityHttpsListener = false
    CertificateThumbprint
    AllowRemoteAccess = true
```

また、「winrm enumerate winrm/config/listener」を実行することで、現在のリスナーの構成を取得できます。

Copyright (C) 2026 LogicVein, Inc.

```
PS C:¥Users¥Administrator> winrm enumerate winrm/config/listener
Listener
    Address = *
    Transport = HTTP
    Port = 5985
    Hostname
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint
    ListeningOn = 127.0.0.1, 192.168.40.66, ::1, 2001:0:348b:fb58:1077:394:3f57:d7bd,
fd14:5839:664d:40:58c0:c882:310d:3
```

7.1.7.2 非セキュア HTTP 接続設定

規定の設定では、暗号化されたトラフィックのみ許可されています。HTTP を使用して監視を行う場合には、「winrm set winrm/config/service '@{AllowUnencrypted="true"}'」を実行し、暗号化されていないトラフィックを許可します。

```
PS C:¥Users¥Administrator> winrm set winrm/config/service '@{AllowUnencrypted="true"}'
Service
    RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)(A;;GR;;;IU)S:P(AU;FA;GA;;;WD)(AU;SA;GXGW;;;WD)
    MaxConcurrentOperations = 4294967295
    MaxConcurrentOperationsPerUser = 1500
    EnumerationTimeoutms = 240000
    MaxConnections = 300
    MaxPacketRetrievalTimeSeconds = 120
    AllowUnencrypted = true
    Auth
        Basic = false
        Kerberos = true
```

7.1.7.3 認証設定

Basic 認証を使用する場合には、「winrm set winrm/config/service/auth '@{Basic="true"}'」を実行します。システムがドメインに参加していない場合（WORKGROUP）には、Basic 認証を有効にします。

```
PS C:¥Users¥Administrator> winrm set winrm/config/service/auth '@{Basic="true"}'
Auth
    Basic = true
    Kerberos = true
    Negotiate = true
    Certificate = false
    CredSSP = false
    CbtHardeningLevel = Relaxed
```


Copyright (C) 2026 LogicVein, Inc.

7.1.7.4　監視設定

（1）　クレデンシャル設定

認証に使用するユーザ名とパスワードをクレデンシャルに登録します。ユーザ名は VTY Username、パスワードは VTY Password に設定します。

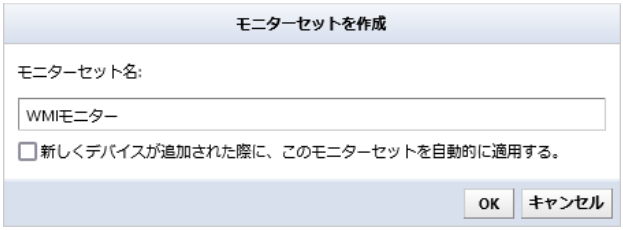
（2）　モニター設定

WMI を使用したモニターは、以下の監視をサポートしています。

- Windows Disk (ディスク使用率のメトリックを収集)
- Windows Memory (システムメモリのメトリックを収集)
- Windows Processor (CPU 使用率のメトリックを収集)
- Windows Process (プロセスのメトリックを収集)
- Windows Service (サービスのメトリックを収集)

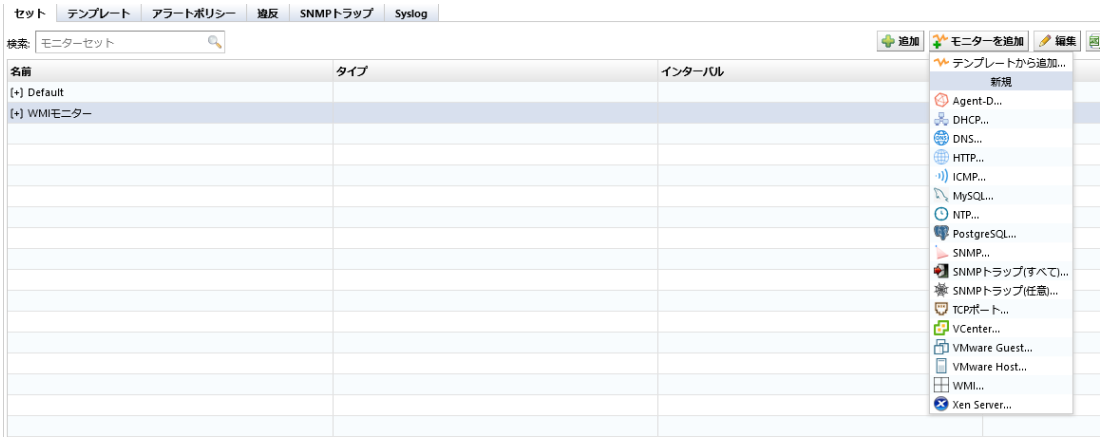
モニターは他のモニターと同様にデバイス詳細画面やモニターセットに追加することができます。以下では、モニターセットを使用して追加する手順を記載しています。

1. [モニター]->[セット]タブを開きます。
2. [追加]をクリック、モニターセットを追加します。

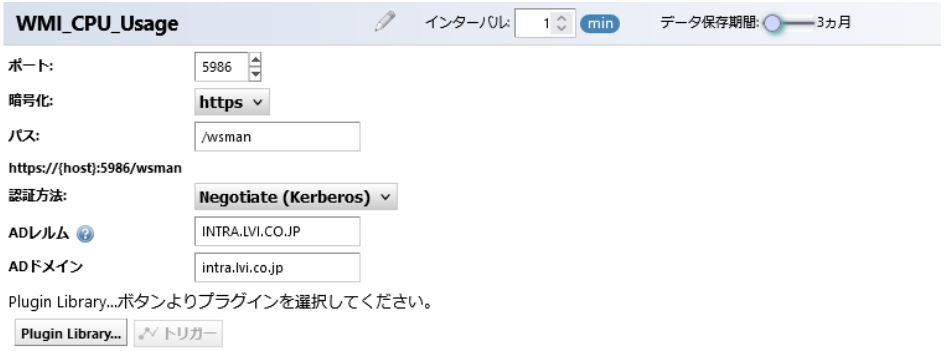


3. 追加されたモニターセットをクリックし、[モニターを追加]から[WMI]をクリックします。

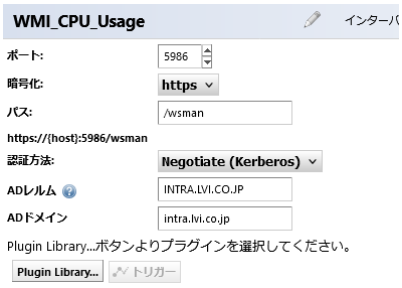
Copyright (C) 2026 LogicVein, Inc.



4. 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。



5. 各項目を設定します。



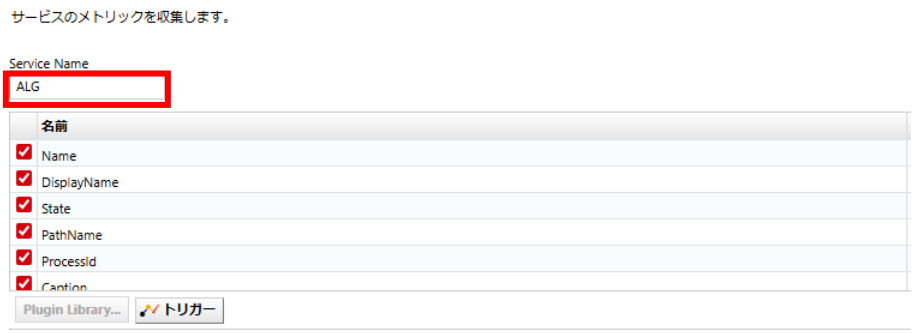
項目	説明
ポート	WMI のポートを指定します。デフォルトでは、暗号化に「https」が選択されている場合には”5986”、「なし」の場合には”5985”が指定されます。
暗号化	環境に合わせて、「https」または「なし」を選択します。
パス	サーバ側でパスを変更している場合には、パスを変更します。デフォルトでは、「/wsman」です。
認証方法	環境に合わせて、「Negotiate」または「Http Basic」を選択します。
AD レルム	レルムを入力します。（認証方法が「Negotiate」の場合のみ）
AD ドメイン	ドメインを入力します。（認証方法が「Negotiate」の場合のみ）

Copyright (C) 2026 LogicVein, Inc.

6. ［Plugin Library…］をクリックします。
7. プラグインを選択し、[OK]をクリックします。

8. 取得するメトリックを選択します。

9. プロセス監視やサービス監視を行う場合、Process Name/Service Name を指定する必要があります。



10. [保存]をクリックし、[閉じる]から設定画面を閉じます。

Copyright (C) 2026 LogicVein, Inc.

7.1.7.5　各プラグインで取得できるメトリック

モニターに設定できる各プラグインで取得できるメトリックは、以下のとおりです。

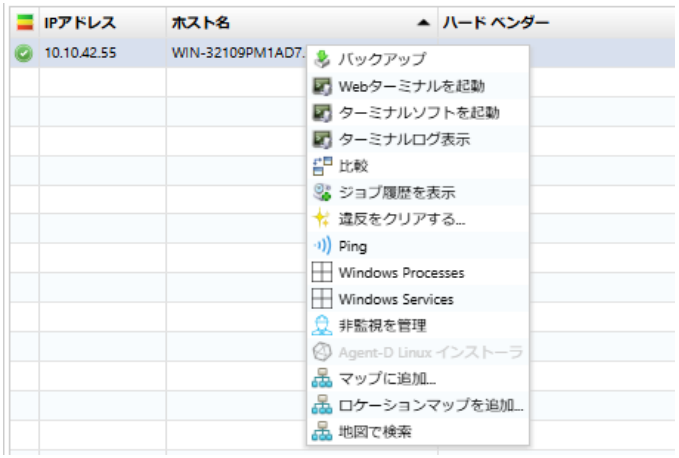
プラグイン	メトリック	説明
Windows Disk	Win32_PerfFormattedData_PerfDisk_LogicalDisk クラスを使用	
	Free Space (Megabytes)	「FreeMegabytes」を参照
	Free Space (%)	「PercentFreeSpace」を参照
	Idle Time (%)	「PercentIdleTime」を参照
	Read Time (%)	「PercentDiskReadTime」を参照
	Write Time (%)	「PercentDiskWriteTime」を参照
	Disk Time (%)	「PercentDiskTime」を参照
	Bytes Per Second	「DiskBytesPersec」を参照
	Bytes Read Per Second	「DiskReadBytesPersec」を参照
	Bytes Written Per Second	「DiskWriteBytesPersec」を参照
	Reads Per Second	「DiskReadsPersec」を参照
	Writes Per Second	「DiskWritesPersec」を参照
Windows Memory	Win32_PerfFormattedData_PerfOS_Memory クラスを使用	
	Bytes Available	「AvailableBytes」を参照
	Bytes Cached	「CacheBytes」を参照
	Bytes Committed	「CommittedBytes」を参照
	Page Faults	「PageFaultsPersec」を参照
Windows Processor	Win32_PerfRawData_PerfProc_Process クラスを使用	
	Idle Time (%)	「PercentIdleTime」を参照
	Interrupts Time (%)	「PercentInterruptTime」を参照
	Privileged Time (%)	「PercentPrivilegedTime」を参照
	Processor Time (%)	「PercentProcessorTime」を参照
	User Time (%)	「PercentUserTime」を参照
Windows Service	Service Name	「Service Name」を参照
	Description	「Description」を参照
	Status	「Status」を参照
	Startup Type	「Startup Type」を参照
	Assigned Application	「Assigned Application」を参照

7.1.7.6　プロセス監視

Windows サーバのホスト名を使用して、リアルタイムのプロセス情報を収集、該当プロセスを指定することで、プロセス監視のモニターを作成することができます。WinRM が Windows Server 上で有効になっている場合、ディスカバリを行う事でデバイスに対して wmi トレイトが追加されます。

Copyright (C) 2026 LogicVein, Inc.

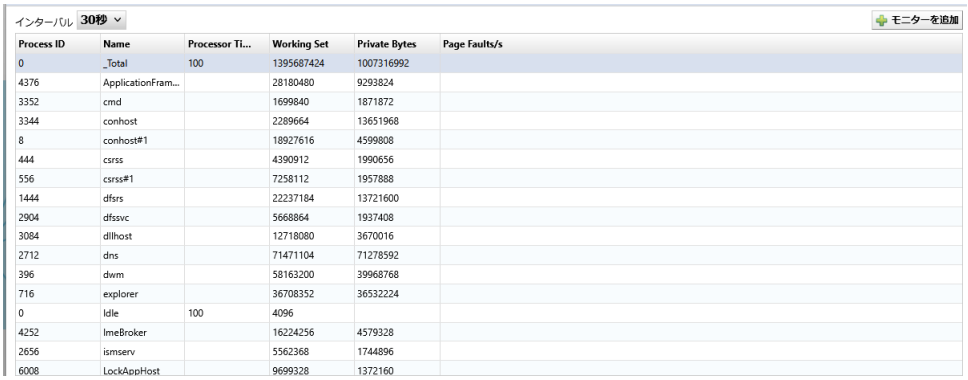
デバイスを右クリックした際に表示される"Windows Processes"は、デバイスに wmi トレイトがある場合のみ利用可能です。



1. ［Windows Processes］をクリックします。
2. WinRM LiveProcess Monitor Authentication を設定します。

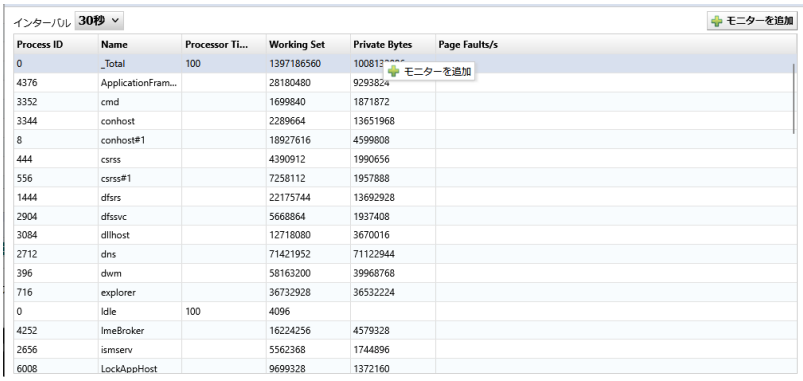
※WMI モニターを追加する認証設定と同様の設定となります。

3. [開始]をクリックすると、Ping モニターと同様のライブモニターページが開きます。



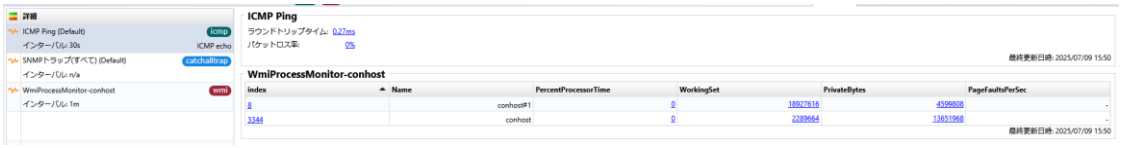
4. プロセスを右クリックし、[モニターの追加]をクリックします。

Copyright (C) 2026 LogicVein, Inc.



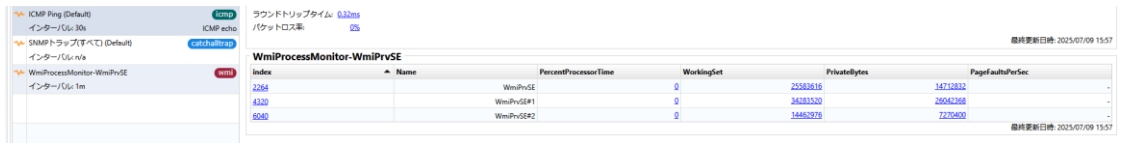
Process ID	Name	Processor Ti...	Working Set	Private Bytes	Page Faults/s
0	_Total	100	1397186560	100813	
4376	ApplicationFram...		28180480	929824	
3352	cmd		1699840	1871872	
3344	conhost		2289664	13651968	
8	conhost#1		18927616	4599808	
444	csrss		4390912	1990656	
556	csrss#1		7258112	1957888	
1444	dfsrs		22175744	13692928	
2904	dfssvc		5668864	1937408	
3084	dllhost		12718080	3670016	
2712	dns		71421952	71122944	
396	dwm		58163200	39968768	
716	explorer		36732928	36532224	
0	Idle	100	4096		
4252	ImeBroker		16224256	4579328	
2656	ismserv		5562368	1744896	
6008	LockAppHost		9699328	1372160	

モニターがデバイスに追加され、監視が開始されます。



index	Name	PercentProcessorTime	WorkingSet	PrivateBytes	PageFaultsPerSec
8	conhost#1	0	18927616	4599808	
3344	conhost	0	2289664	13651968	

選択されたプロセスに複数のインスタンスがある場合、追加されたモニターは自動的にプロセスのすべてのインスタンスを追加/監視します。インスタンスは「<プロセス名>」、「<プロセス名>#1」、「<プロセス名>#2」などで表示されます。以下の例では、プロセスモニター 「WmiPrvSE 」を選択することにより、『WmiPrvSE』、「WmiPrvSE#1」、「WmiPrvSE#2 」という名前で、同じプロセスの異なるインスタンスを持っており、全てを監視対象とします。



index	Name	PercentProcessorTime	WorkingSet	PrivateBytes	PageFaultsPerSec
2264	WmiPrvSE	0	25583616	14712832	
4320	WmiPrvSE#1	0	34281520	26042368	
6040	WmiPrvSE#2	0	14462976	7270400	

7.1.7.7 サービス監視

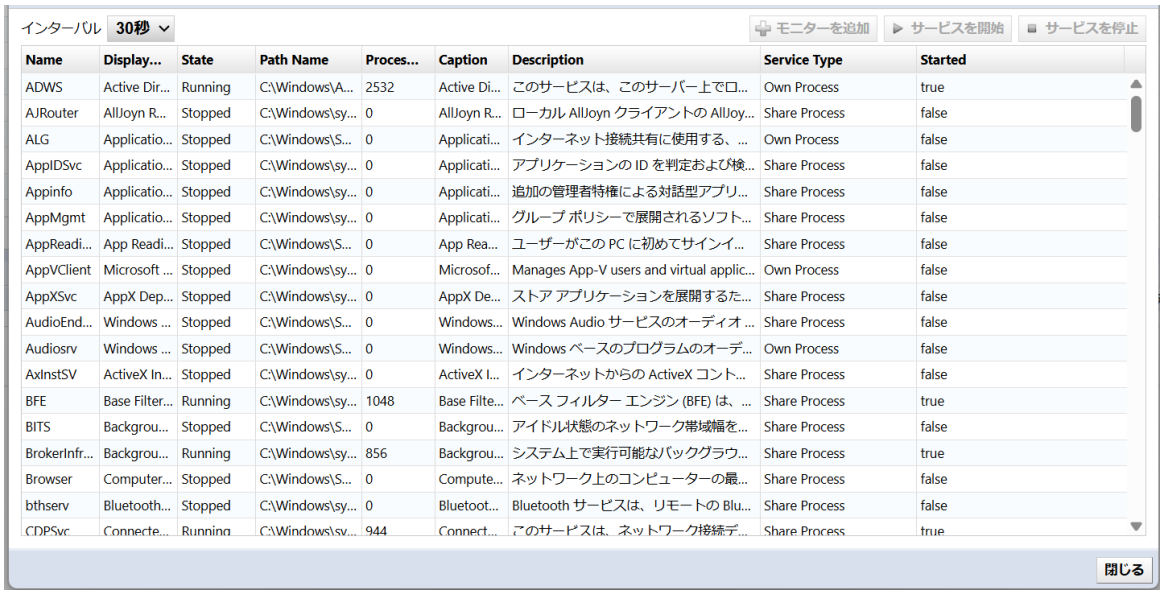
WMI（Windows Management Instrumentation）を通じて Windows サービスをリアルタイムで可視化します。サービス開始/終了イベント、リソース使用状況（CPU/メモリ）、および親子プロセス関係を監視します。このモニターは、不正なプロセスの検出、リソースのボトルネックの特定、詳細なプロセス監査によるコンプライアンス維持など、重要なセキュリティと運用ツールとして機能します。Thirdeye のアラートシステムと統合されているので、異常なプロセスパターンを検知して通知をトリガーし、他のシステムメトリクスとデータを相関分析して根本原因の特定を行います。
サービス監視は Windows サーバのホスト名を使用して行われます。WinRM が Windows Server 上で有効になっている場合、ディスカバリを行う事でデバイスに対して wmi トレイトが追加されます。

Copyright (C) 2026 LogicVein, Inc.

デバイスを右クリックした際に表示される"Windows Services"は、デバイスに wmi トレイトがある場合のみ利用可能です。

1. ［Windows Services］をクリックします。
2. WMI Live Service Monitor Authentication を設定します。

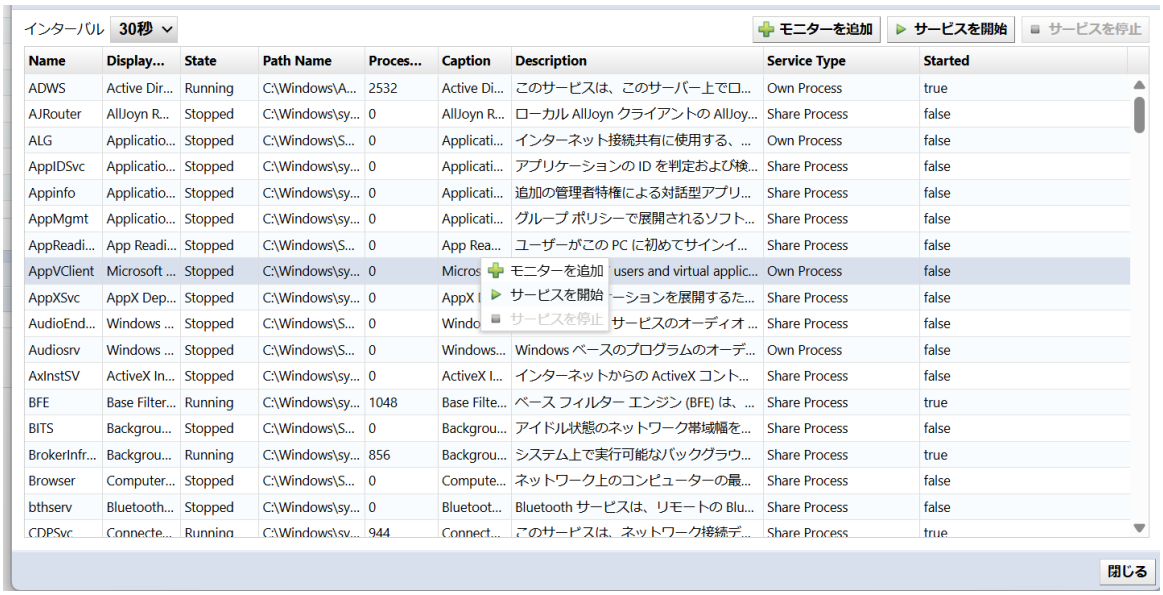
3. [開始]をクリックすると、Windows Services ページが開きます。

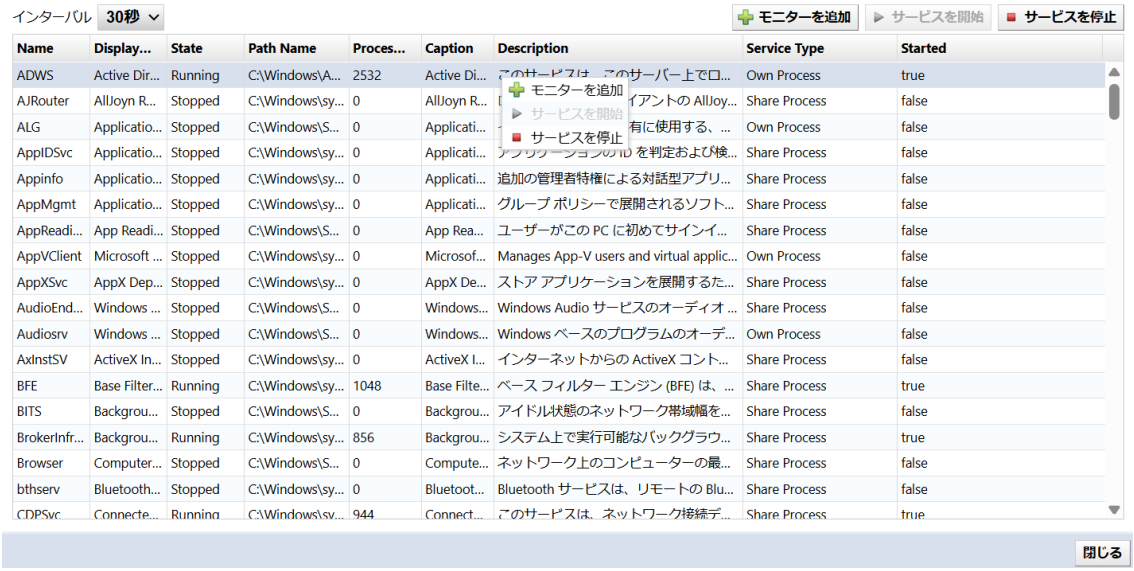


Name	Display...	State	Path Name	Proces...	Caption	Description	Service Type	Started
ADWS	Active Dir...	Running	C:\Windows\A...	2532	Active Di...	このサービスは、このサーバー上でロ...	Own Process	true
AJRouter	AllJoyn R...	Stopped	C:\Windows\sy...	0	AllJoyn R...	ローカル AllJoyn クライアントの AllJoy...	Share Process	false
ALG	Applicatio...	Stopped	C:\Windows\S...	0	Applicati...	インターネット接続共有に使用する、...	Own Process	false
AppIDSvc	Applicatio...	Stopped	C:\Windows\sy...	0	Applicati...	アプリケーションの ID を判定および検...	Share Process	false
Appinfo	Applicatio...	Stopped	C:\Windows\sy...	0	Applicati...	追加の管理者特権による対話型アプリ...	Share Process	false
AppMgmt	Applicatio...	Stopped	C:\Windows\sy...	0	Applicati...	グループ ポリシーで展開されるソフト...	Share Process	false
AppReadi...	App Readi...	Stopped	C:\Windows\S...	0	App Rea...	ユーザーがこの PC に初めてサインイ...	Share Process	false
AppVClient	Microsoft ...	Stopped	C:\Windows\sy...	0	Microsof...	Manages App-V users and virtual applic...	Own Process	false
AppXSvc	AppX Dep...	Stopped	C:\Windows\sy...	0	AppX De...	ストア アプリケーションを展開するた...	Share Process	false
AudioEnd...	Windows ...	Stopped	C:\Windows\S...	0	Windows...	Windows Audio サービスのオーディオ ...	Share Process	false
Audiosrv	Windows ...	Stopped	C:\Windows\S...	0	Windows...	Windows ベースのプログラムのオーデ...	Own Process	false
AxInstSV	ActiveX In...	Stopped	C:\Windows\sy...	0	ActiveX I...	インターネットからの ActiveX コント...	Share Process	false
BFE	Base Filter...	Running	C:\Windows\sy...	1048	Base Filte...	ベース フィルター エンジン (BFE) は、...	Share Process	true
BITS	Backgrou...	Stopped	C:\Windows\S...	0	Backgrou...	アイドル状態のネットワーク帯域幅を...	Share Process	false
BrokerInfr...	Backgrou...	Running	C:\Windows\sy...	856	Backgrou...	システム上で実行可能なバックグラウ...	Share Process	true
Browser	Computer...	Stopped	C:\Windows\S...	0	Compute...	ネットワーク上のコンピューターの最...	Share Process	false
bthserv	Bluetooth...	Stopped	C:\Windows\sy...	0	Bluetoot...	Bluetooth サービスは、リモートの Blu...	Share Process	false
CDPSvc	Connecte...	Running	C:\Windows\sy...	944	Connect...	このサービスは、ネットワーク接続デ...	Share Process	true

4. ウィンドウの右上にあるボタンをクリックするか、サービスを右クリックして、サービスの開始/停止を行うことができます。

Copyright (C) 2026 LogicVein, Inc.

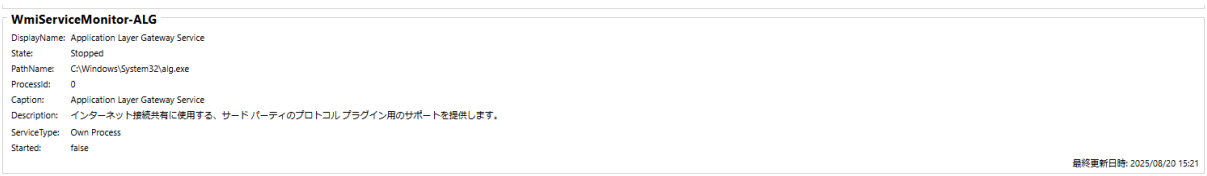




※ ［サービスを開始］と［サービスを停止］ボタンは、サービスの現在の状態に応じて有効になります。サービスを複数選択した状態での開始/停止には対応していません。

5. サービスを右クリックし、[モニターの追加]をクリックします。

サービスがデバイスに追加され、監視が開始されます。



Copyright (C) 2026 LogicVein, Inc.

7.1.8　ワイヤレス LAN コントローラの監視

Cisco IOS XE を実行しているワイヤレス LAN コントローラに、WLC モニターを追加できるようになりました。WLC モニターは、監視対象の WLC デバイスを HTTPS 経由で定期的にポーリングし、接続中のクライアント一覧や各クライアントが接続しているアクセスポイントなどの関連情報を取得します。これにより、MAC アドレスや IP アドレス、最終検出日時などのデータポイントに基づいて、アクセスポイントに関連付けられたクライアントを参照できます。さらに、マップ上では、各アクセスポイントに関連付けられたクライアントを表示することが可能です。監視を行う為に、WLC デバイス側で restconf を有効にする必要があります。

例:

configure terminal

ip http secure-server

restconf

exit

7.1.8.1　WLC モニターの設定

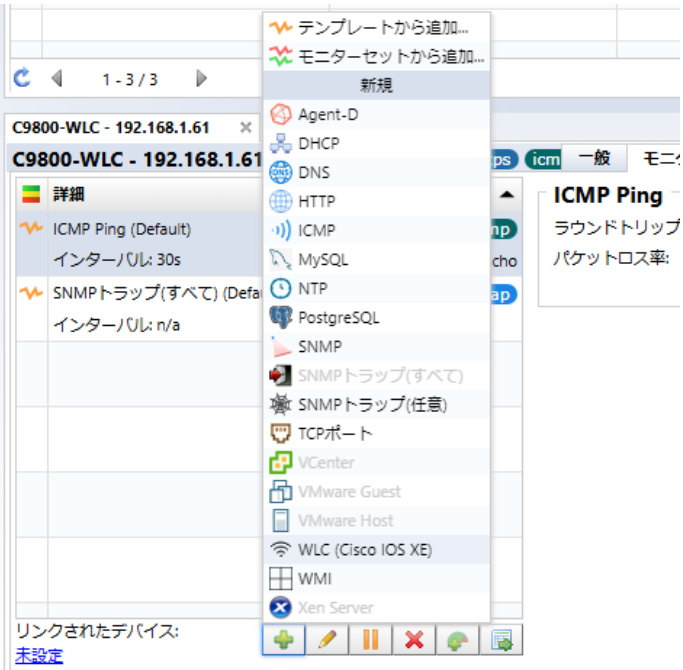
1. ワイヤレス LAN コントローラをインベントリに追加します。

   ※　ワイヤレス LAN コントローラのアダプタは「Cisco IOS」である必要があります。

2. ワイヤレス LAN コントローラへのログインに必要な認証情報をクレデンシャルに設定します。

   ※　認証には「VTY Username」と「VTY Password」が使用されます。

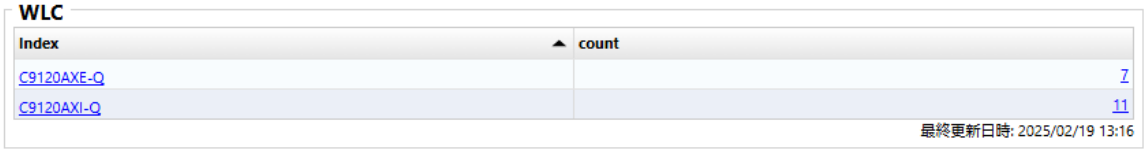
3. ワイヤレス LAN コントローラに「WLC (Cisco IOS XE)」モニターを追加します。



4. モニターの設定を行います。

Copyright (C) 2026 LogicVein, Inc.

モニター名、インターバル、データ保存期間、任意でオプションのトリガーを設定し、[保存]をクリックします。データ収集が完了すると、AP 名と現在接続されているクライアントの数を示すテーブルが表示されます。



7.1.8.2 クライアントの詳細を確認する

Wi-Fi クライアントタブでは、WLC モニターによって取得されたクライアントの詳細を確認できます。

項目	説明
ステータス	次の 2 種類のアイコンが表示されます。 ：過去に 1 回以上クライアントとして認識されたが、現在は接続されていないことを示す ：現在接続されていることを示す
アイコン	マップ上でクライアントを表すノードのアイコンとして使用される画像です。任意の画像をアップロードして設定できます。
SSID	クライアントが接続している SSID 名が表示されます。
アクセスポイント	クライアントが接続しているアクセスポイント名を表示されます。
名前	ユーザが任意で設定した名前が表示されます。名前はこのテーブルとマップで使用されます。
IP アドレス	クライアントが使用している IP アドレスが表示されます。
IPv6 アドレス	クライアントが使用している IPv6 アドレスが表示されます。
MAC	クライアントの MAC アドレスが表示されます。
最終確認日時	ThirdEye が最後に WLC でクライアント情報を確認した日時が表示されます。
最終接続日時	クライアントが最後に接続された日時が表示されます。

※ SSID/アクセスポイント/IP アドレス/IPv6 アドレス/MAC の情報は、WLC の Web 管理コンソールの「モニタリング->ワイヤレス->クライアント」で確認できる情報と同じです。

名前とアイコンは、右上の編集ボタンをクリックすることでカスタマイズできます。このカスタマイズはクライアント

Copyright (C) 2026 LogicVein, Inc.

の MAC アドレスに関連付けられているため、クライアントが新しい IP アドレスを取得しても、カスタマイズは引き続き適用されます。

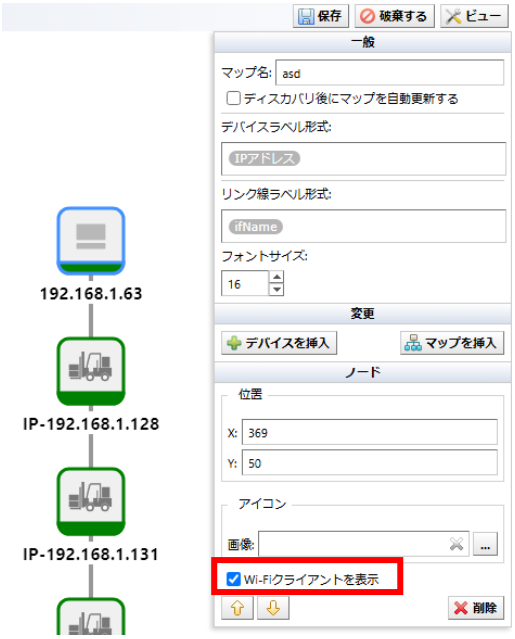
7.1.8.3　マップにクライアントを表示する

1. アクセスポイントをワイヤレス LAN コントローラと同じ管理ネットワークに追加します。
   ※　アクセスポイントのホスト名が正しく設定されていることを確認してください。

2. アクセスポイントに「ap」トレイトが付与されていることを確認します。

※　ワイヤレス LAN コントローラの「WLC (Cisco IOS XE)」モニターがデータ収集を完了すると、アクセスポイントに自動的に「ap」トレイトが付与されます。

3. 「ap」トレイトが付与されたアクセスポイントをマップに挿入します。
4. アクセスポイントを選択し、「Wi-Fi クライアントを表示」オプションを有効にします。



マップの編集中にアクセスポイントを選択すると、新しいオプション「Wi-Fi クライアントを表示」が利用可能になります。このオプションを有効にすると、アクセスポイントに接続されているすべてのクライアントが下方向に表示されます。

※クライアントの表示方向の変更や、表示されたクライアントの配置移動はできません。

5. マップを保存します。

マップに表示されるクライアントのラベルには、Wi-Fi クライアントタブで設定された名前が使用されます。名前が未

Copyright (C) 2026 LogicVein, Inc.

設定の場合は、クライアントの MAC アドレスが表示されます。名前やアイコンは、Wi-Fi クライアントタブで編集できるほか、マップ上のクライアントアイコンを右クリックして編集することも可能です。

　また、クライアントの接続が解除されたり、別のアクセスポイントへ移動したりすると、マップ上のクライアントアイコンも自動的に更新されます。

Copyright (C) 2026 LogicVein, Inc.

7.1.9　Aruba Access Point の監視

ThirdEye は Aruba アクセスポイント向けに Aruba AP と Aruba AP クライアントの 2 種類のモニターをサポートします。これらのモニターは、aruba-ap トレイトを有するデバイスに 1 回のみ追加可能です。Aruba Central API 経由でアクセスポイントを監視します。いずれのモニターも「期間」以外の設定項目は表示しませんが、利用可能なトリガーの設定は可能です。

7.1.9.1　Aruba AP モニター

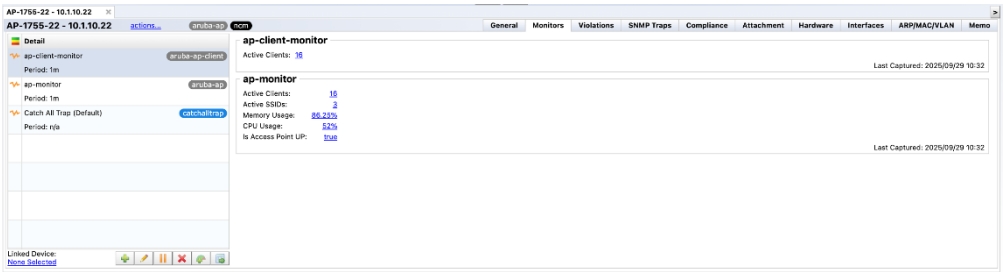
Aruba AP モニターは、以下のメトリックデータを使用してアクセスポイントを監視するために使用できます。

項目	説明
Active Client	AP に接続しているクライアントの数です。
Active SSIDs	AP の SSID の数です。
Memory Usage	AP のメモリ使用量です。
CPU Usage	AP の CPU 使用量です。
Access Point Operational Status	AP が起動中かを表示します。

7.1.9.2　Aruba AP クライアントモニター

Aruba AP クライアントモニターは、アクセスポイントに接続されたクライアントを監視するために使用できます。このモニターを Aruba アクセスポイントに追加すると、Wi-Fi クライアントが[Wi-Fi クライアント]タブで確認可能になります。Aruba AP クライアントモニターでは、以下のメトリックデータが利用可能です。

項目	説明
Active Clients	AP に接続しているクライアントの数です。

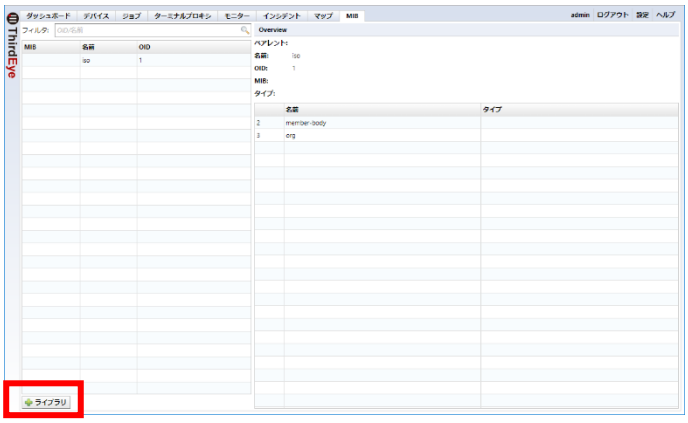


Copyright (C) 2026 LogicVein, Inc.

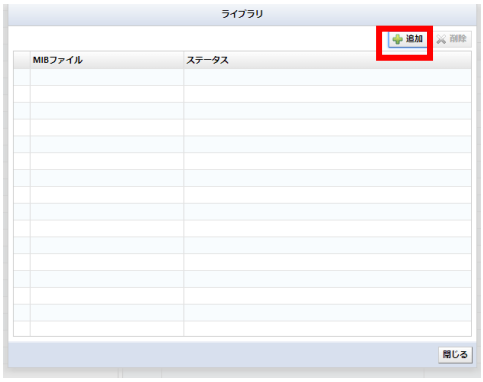
7.1.10　MIB をコンパイルする

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。

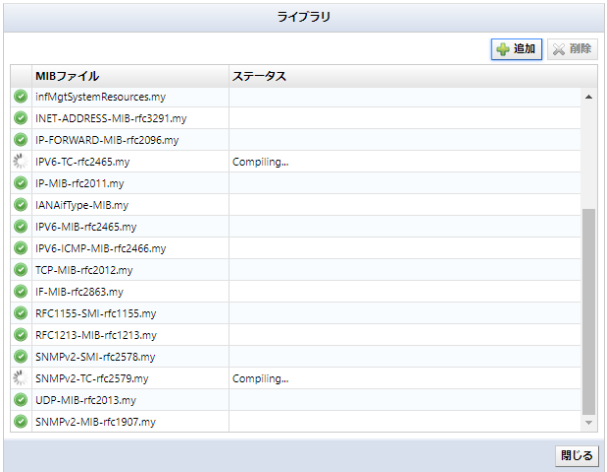


2. ライブラリ画面が表示されます。［追加］をクリックします。



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。



Copyright (C) 2026 LogicVein, Inc.

7.2　デバイスの EOS/EOL 管理

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)」のカラムが追加されました。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。

7.2.1　手動設定

7.2.1.1　手順

1. EOS/EOL を取得する機器を選択します。

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。

Copyright (C) 2026 LogicVein, Inc.

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。

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。

Copyright (C) 2026 LogicVein, Inc.

7.2.2　自動設定 Suite

7.2.2.1　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

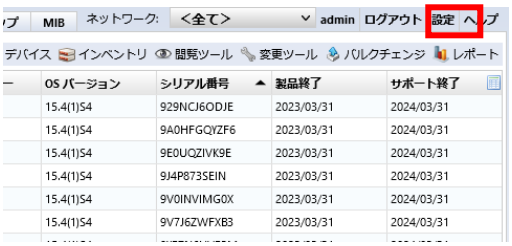
➢ ※有効な Cisco Smart Net Total Care (SNTC)が必要です。

➢ ※API の取得について、以下を参照してください。

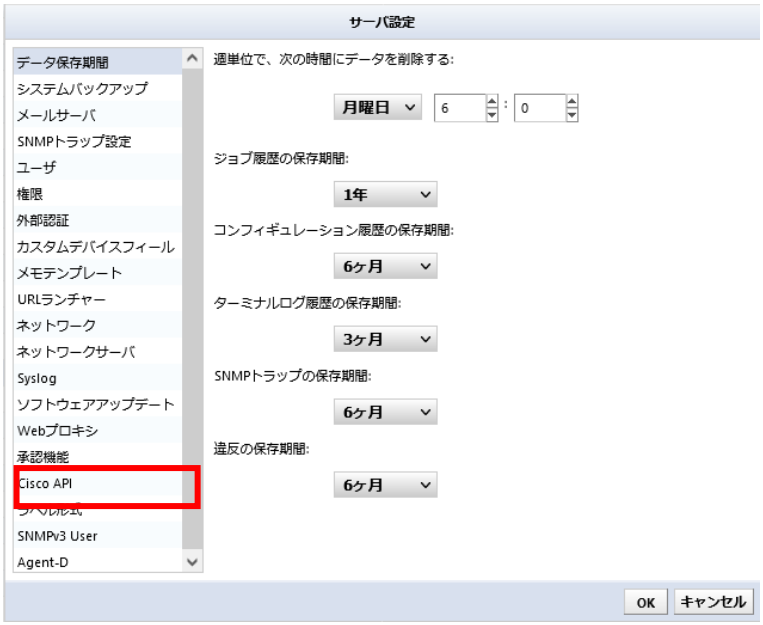
➢ (https://developer.cisco.com/docs/support-apis/#!user-onboarding-process)

7.2.2.2　手順（オンライン環境）

1. 設定をクリックします。

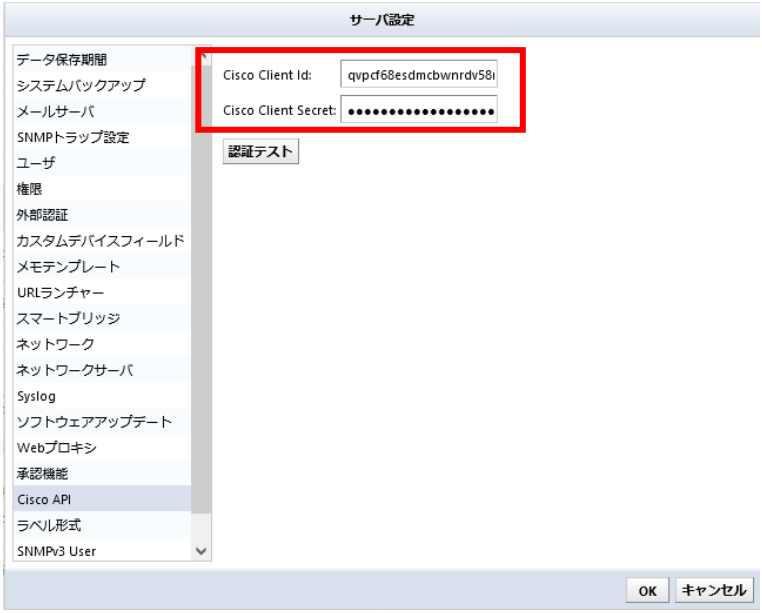


2. Cisco API をクリックします。



Copyright (C) 2026 LogicVein, Inc.

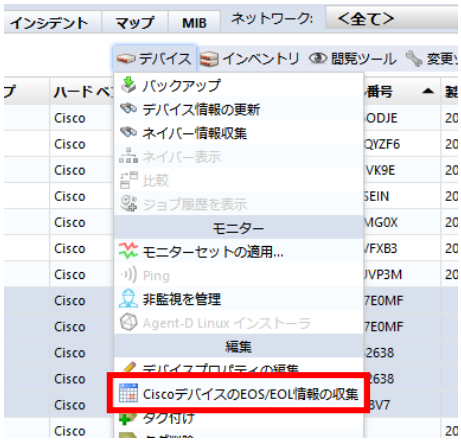
3. API キーとシークレットコードを入力し、OK をクリックします。



認証テストをクリックすることで、入力した ID と Secret コードが使用できるか確認できます。

4. EOS/EOL を取得する機器を選択します。

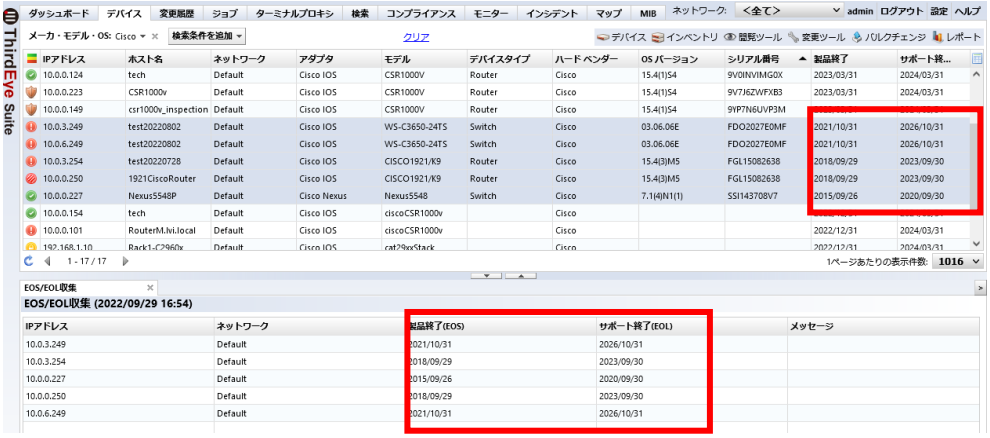
5. デバイスメニューから「Cisco デバイスの EOS/EOL 情報の収集」をクリックします。



Copyright (C) 2026 LogicVein, Inc.

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。



7.2.2.3 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、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。

Copyright (C) 2026 LogicVein, Inc.

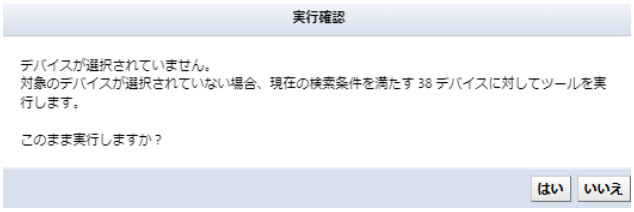
7.2.3　レポートによる通知

レポート機能を使用することで、レポート実行日から 1 年以内、または任意の期間内に EOS/EOL を迎える管理デバイスを確認できます。また、レポートをスケジュール設定することで、定期的に EOS/EOL 対象デバイスの情報をメールで自動通知することもできます。例えば、毎月 1 回、1 年以内に EOS/EOL を迎える管理デバイスを事前に把握するための通知を受け取るように設定することができます。

7.2.3.1　手動

1. デバイスタブに移動します。
2. レポートメニュー内の「製品/サポート終了」をクリックします。

3. 「はい」をクリックします。

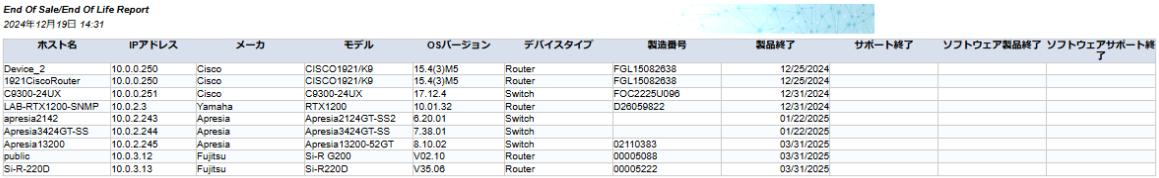


4. 対象および範囲指定をドロップダウンメニューから選択します。

Copyright (C) 2026 LogicVein, Inc.

5. フォーマットを選択し、「実行」をクリックします。

実行がクリックされると指定されたフォーマットでレポートが出力されます。

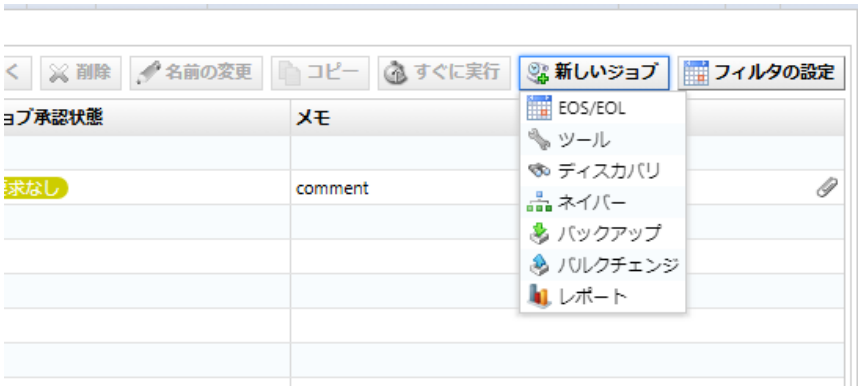


End Of Sale/End Of Life Report
2024年12月19日 14:31

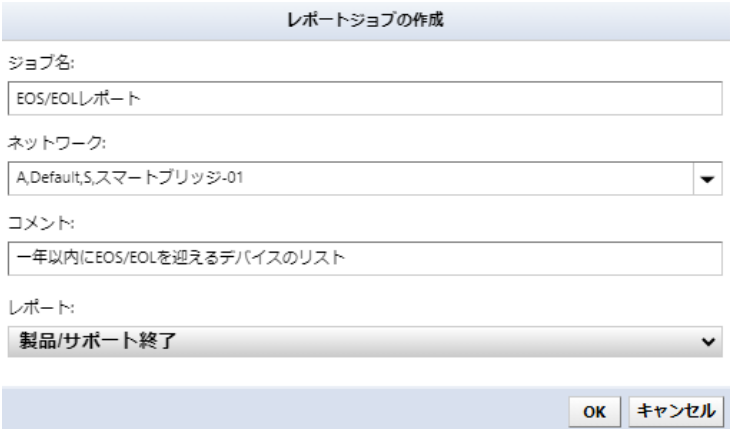
ホスト名	IPアドレス	メーカ	モデル	OSバージョン	デバイスタイプ	製造番号	製品終了	サポート終了	ソフトウェア製品終了	ソフトウェアサポート終了
Device_2	10.0.0.250	Cisco	CISCO1921/K9	15.4(3)M5	Router	FGL15082638	12/25/2024			
1921CiscoRouter	10.0.0.250	Cisco	CISCO1921/K9	15.4(3)M5	Router	FGL15082638	12/25/2024			
C9300-24UX	10.0.0.251	Cisco	C9300-24UX	17.12.4	Switch	FOC2225U096	12/31/2024			
LAB-RTX1200-SNMP	10.0.2.3	Yamaha	RTX1200	10.01.32	Router	D26059822	12/31/2024			
apresia2142	10.0.2.243	Apresia	Apresia2124GT-SS2	6.20.01	Switch		01/22/2025			
Apresia3424GT-SS	10.0.2.244	Apresia	Apresia3424GT-SS	7.38.01	Switch		01/22/2025			
Apresia13200	10.0.2.245	Apresia	Apresia13200-52GT	8.10.02	Switch	02110383	03/31/2025			
public	10.0.3.12	Fujitsu	Si-R G200	V02.10	Router	00005088	03/31/2025			
SI-R-220D	10.0.3.13	Fujitsu	Si-R220D	V35.06	Router	00005222	03/31/2025			

7.2.3.2 自動（スケジュール化）

1. [ジョブタブ]->[ジョブ管理]に移動します。
2. 新しいジョブから「レポート」をクリックします。

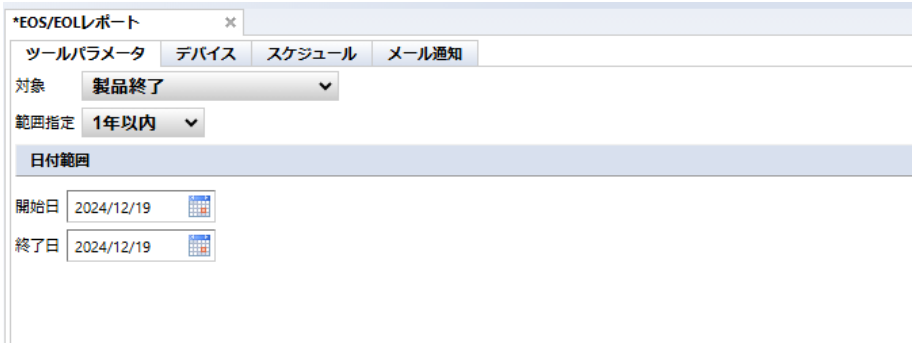


3. ジョブ名を入力し、レポートを「製品/サポート終了」を選択後、[OK]をクリックします。



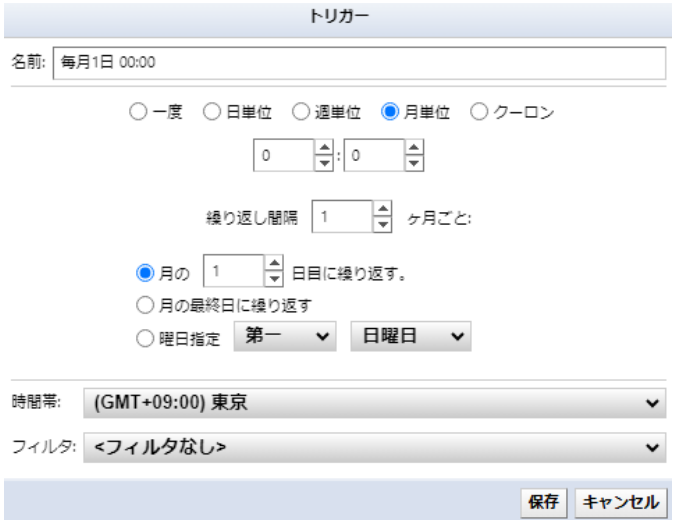
Copyright (C) 2026 LogicVein, Inc.

4. ツールパラメータタブに対象を選択し、範囲指定を「1 年以内」に設定します。

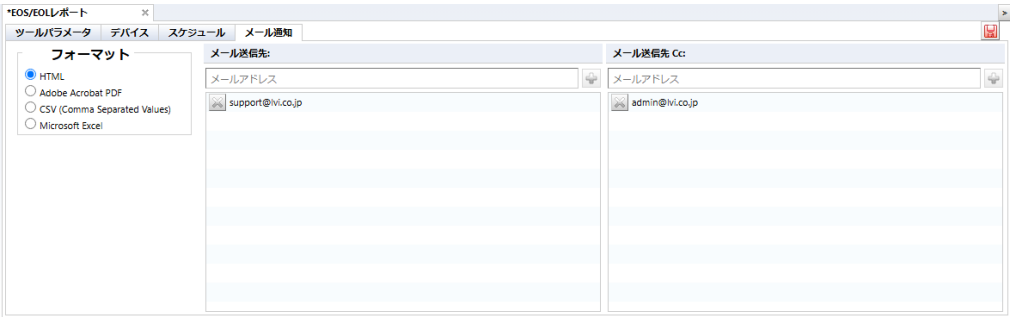


5. スケジュールタブに移動し、[+]ボタンからスケジュールを追加します。

※ 以下の例では、毎月 1 日の 00:00 にレポート発行されます。



6. メール通知タブに移動し、フォーマットを選択後、メール送信先を追加します。



7. 保存ボタンをクリックします

Copyright (C) 2026 LogicVein, Inc.

7.2.4　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て作られますが、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。

7.2.4.1　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。

Copyright (C) 2026 LogicVein, Inc.

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。

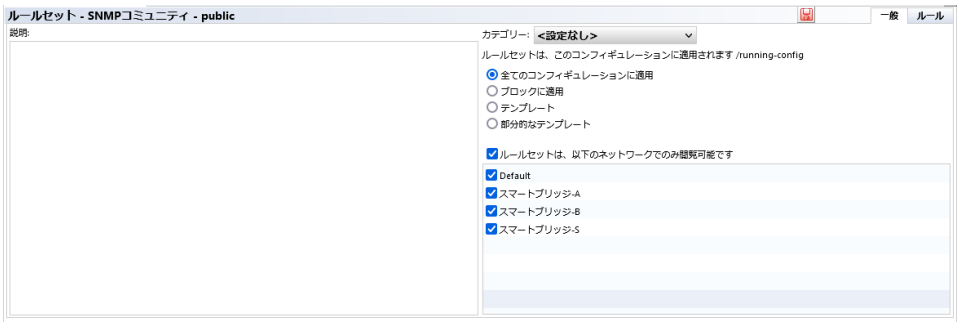
項目	説明
違反メッセージ	ルールに違反した場合に表示されるメッセージを入力します。
開始/終了	「一致」項目で指定された文字列を検索する範囲を指定します。この欄は、一般サブタブで「ブロックに適用」が選択された場合に表示されます。
一致	検索される文字列を指定します。文字列を「~（チルダ）」で挟むことで変数化することができます。 例： interface gigabitEthernet ~INT_NUM~
アクション	マッチングの条件を選択します。 一致しない場合、対象外 一致した場合、対象外 一致しなかった場合、違反 一致した場合、違反
変数	「一致」項目で指定する文字列に変数を使用した場合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

Copyright (C) 2026 LogicVein, Inc.

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が、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
カテゴリー	ルールの説明を入力します。
説明	ルールの説明を入力します。
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、ブロッグ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	チェックを有効にすると、ルールの適用対象となるネットワークが制限されます。

Copyright (C) 2026 LogicVein, Inc.

(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［作成］ボタンをクリックします。

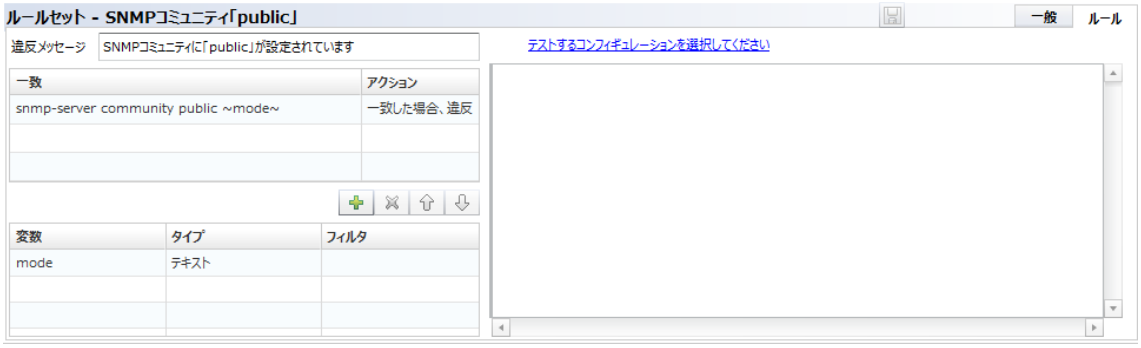
2. ルールの名前、対象アダプタ(機種の分類)、どちらのコンフィギュレーションに適用するルールであるか(running-config か startup-config か)を選び、OK ボタンをクリックします。

3. 違反メッセージ欄に、違反が検出されたときに表示されるメッセージを入力し、［+］ボタンをクリックします。

Copyright (C) 2026 LogicVein, Inc.

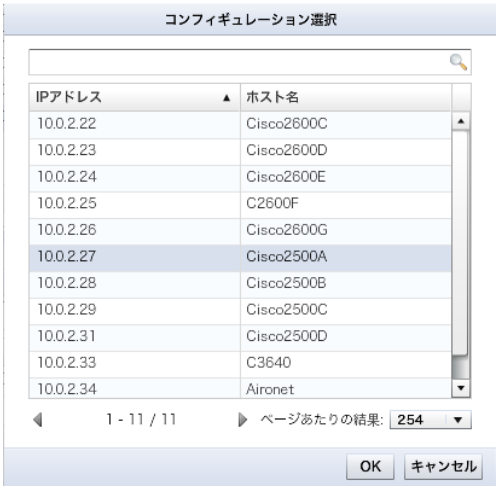
4. 一致に、違反となるテキストを入力し、アクションで「一致した場合、違反」を選択します。

5. 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。



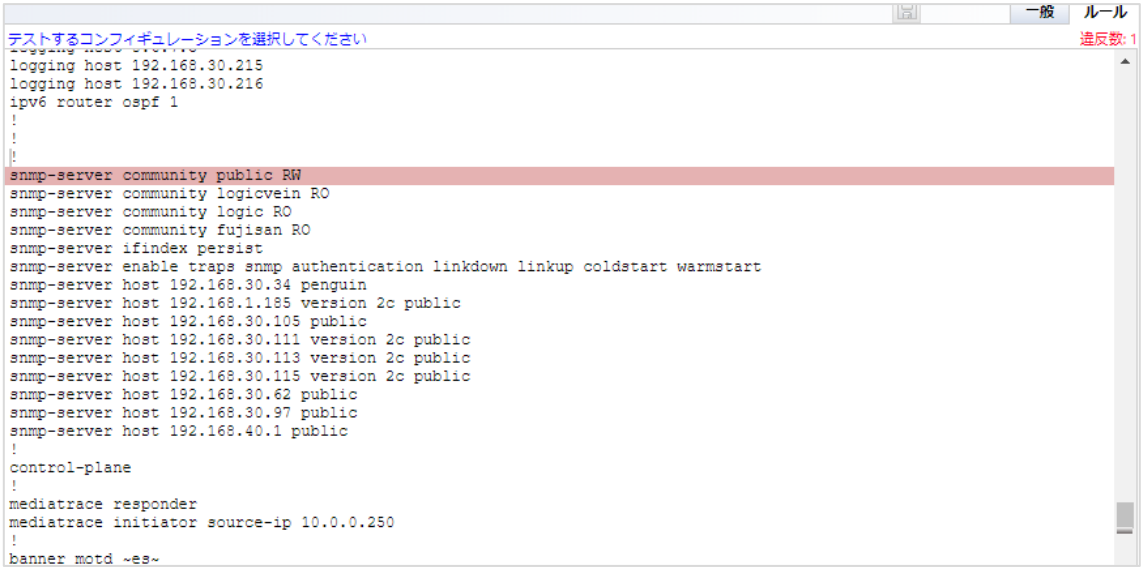
6. ルール作成時に選択したアダプタに当てはまるデバイスのリストがコンフィギュレーション選択ウィンドウに一覧表示されます。

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。



Copyright (C) 2026 LogicVein, Inc.

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か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。

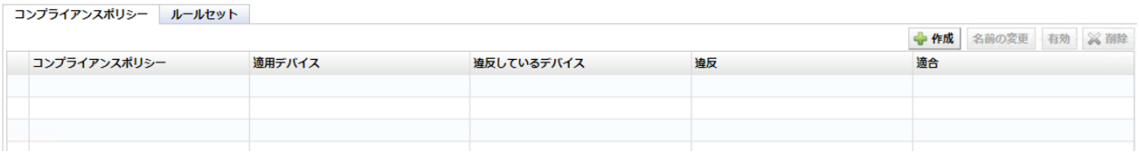


Copyright (C) 2026 LogicVein, Inc.

7.2.4.2　コンプライアンスポリシー

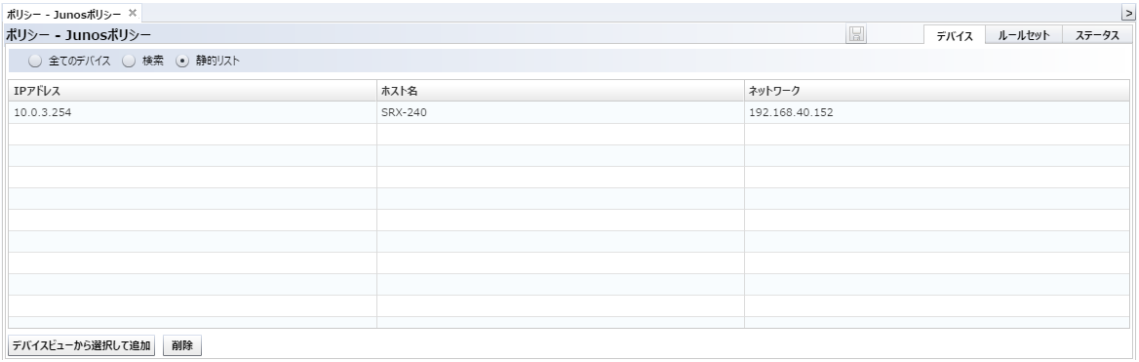
（1）　コンプライアンスポリシータブ

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。



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。

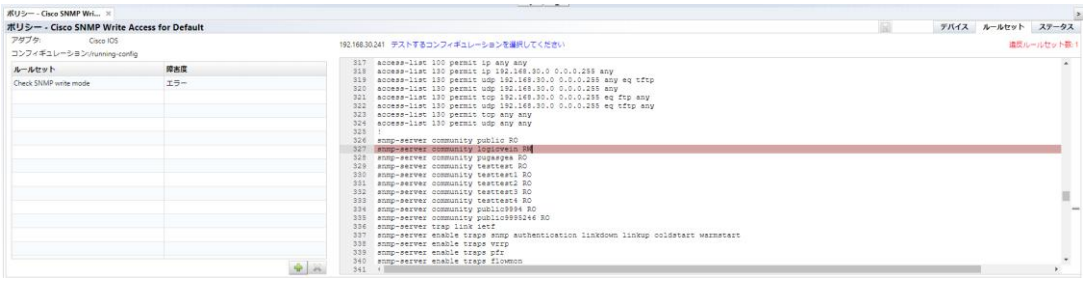


項目	説明
全てのデバイス	全てのデバイスにポリシーを適用します。
検索	検索条件に一致したデバイスにポリシーを適用します。
静的リスト	「デバイス」タブで選択して追加したデバイスにポリシーを適用します。

Copyright (C) 2026 LogicVein, Inc.

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。

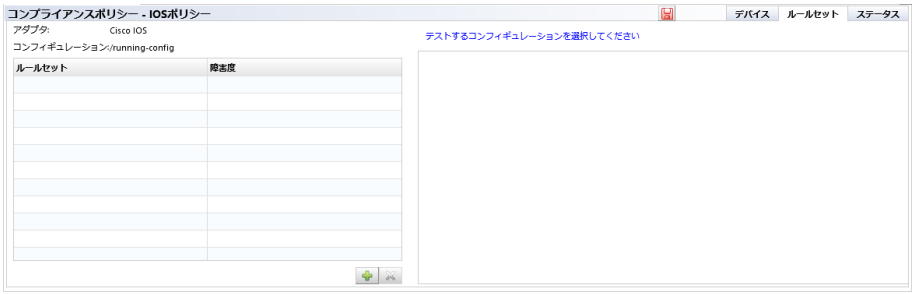
2. ポリシー名、対象アダプタ、コンフィギュレーションの種類を入力し、OK をクリックします。

Copyright (C) 2026 LogicVein, Inc.

3. デバイスサブタブにて、この例では検索を選択します。

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。

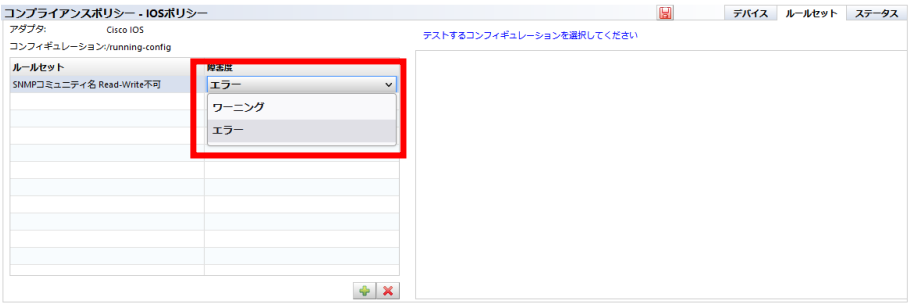


ルールセットを選択し［+］ボタンを押してください。この例では、SNMP コミュニティ「public」& IOS セキュア Enable Password ルールを選択しました。

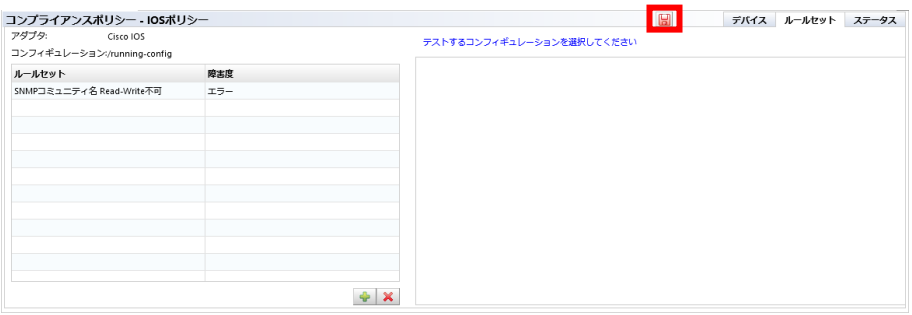
このウィンドウに現れるルールは、*そのアダプタタイプが現在のポリシーのアダプタタイプにマッチするもの*に限られます。 全くルールが表示されない場合には、ポリシーかルールのアダプタタイプを見直してください。

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。

Copyright (C) 2026 LogicVein, Inc.



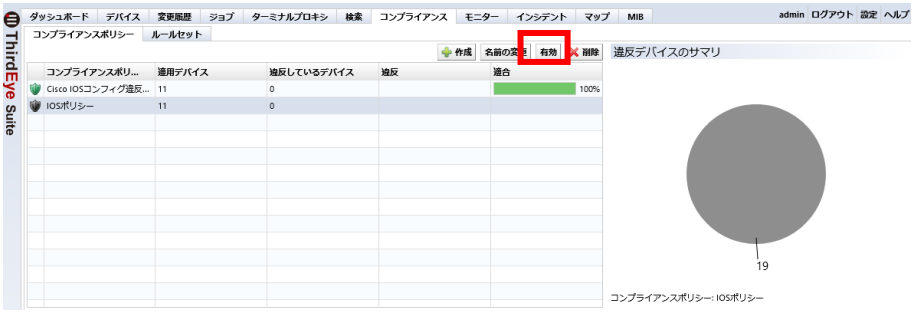
最後に保存します。保存後、次はポリシーを有効化しましょう。ポリシーを作成しただけでは、違反チェックは行われません。



（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。

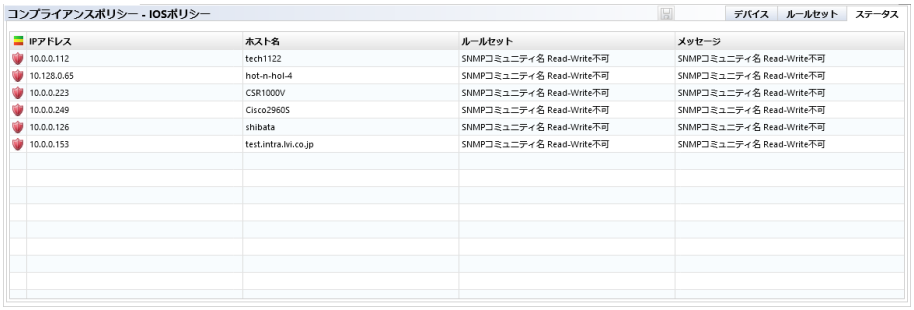
ポリシーを選択した状態で*有効*ボタンを押してください。右の*違反デバイスのサマリ*に円グラフが表示され、違反状況が一目でチェックできます。

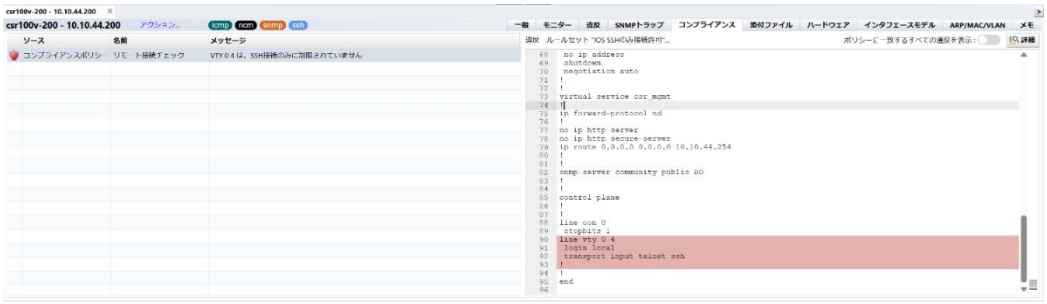


ポリシー違反のあるデバイスがあった場合には、ポリシーのアイコンが変化します。その障害度に応じて、オレンジのワーニング、 あるいは赤いエラーアイコンが表示されます。

Copyright (C) 2026 LogicVein, Inc.

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。

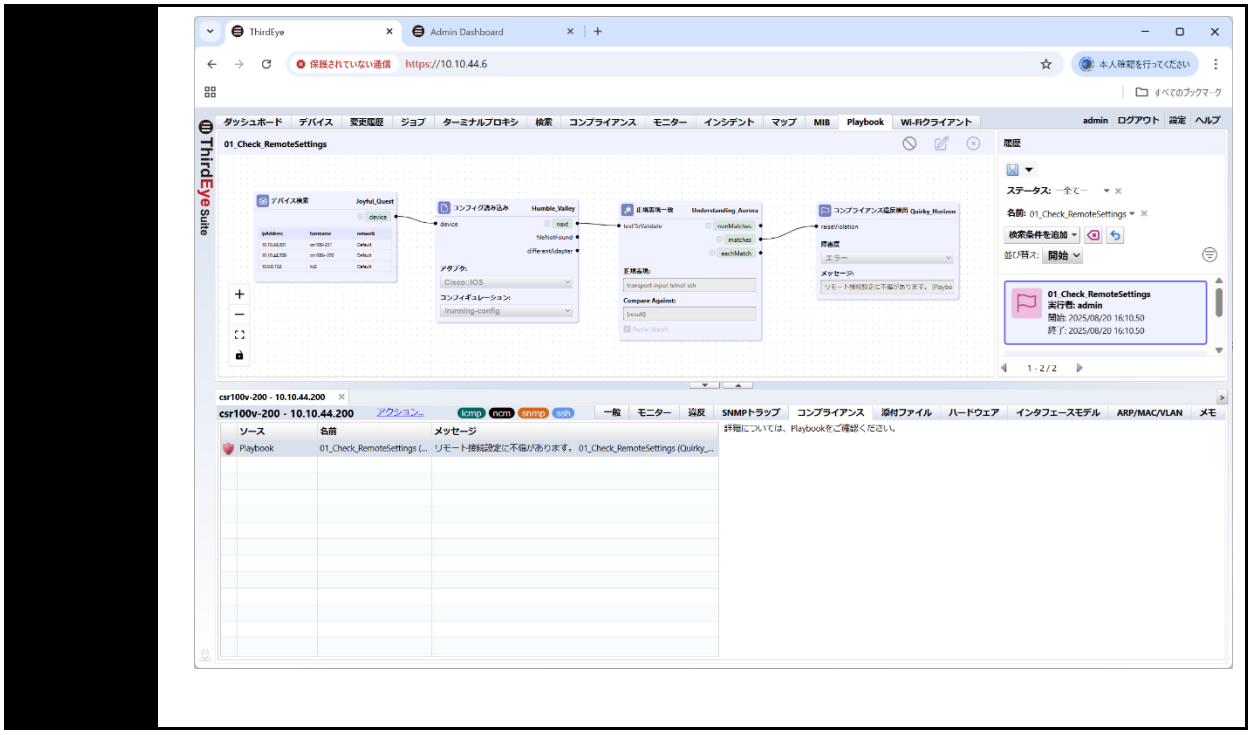




違反アイコンはデバイスビューにも表示されます。 アイコンをダブルクリックすれば、違反の詳細を知ることができます。

補足	Playbook の［コンプライアンス違反検知］ノードを使用すると、デバイスビューに違反が登録されます。登録された違反の詳細は、Playbook の履歴から確認できます。

Copyright (C) 2026 LogicVein, Inc.



7.2.4.3　自動修復機能

コンプライアンス機能とバルクチャ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。

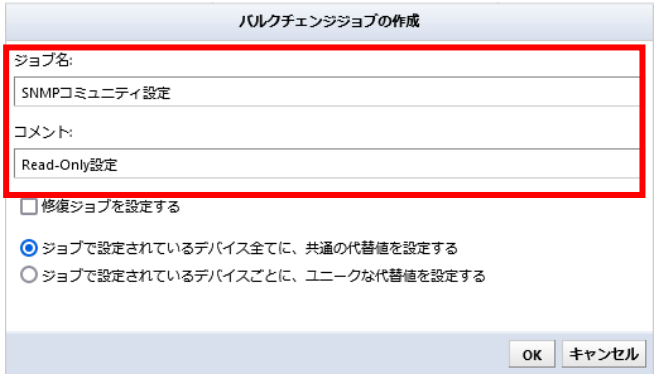
以下では、設定例を使用して設定方法を説明します。

(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。

Copyright (C) 2026 LogicVein, Inc.

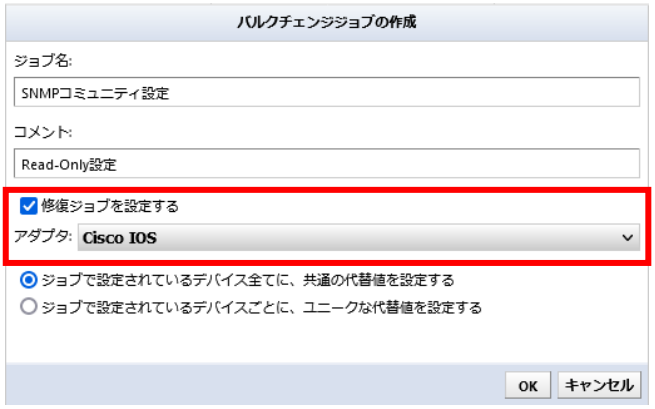
2. ジョブ名、コメント（オプション）を入力します。



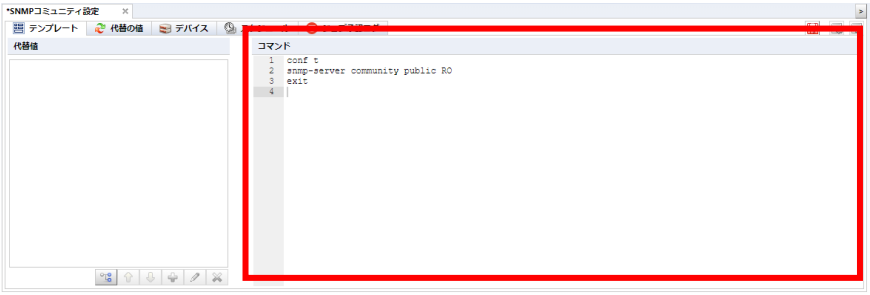
Copyright (C) 2026 LogicVein, Inc.

3. 「修復ジョブを設定する」にチェックを入れ、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。



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。

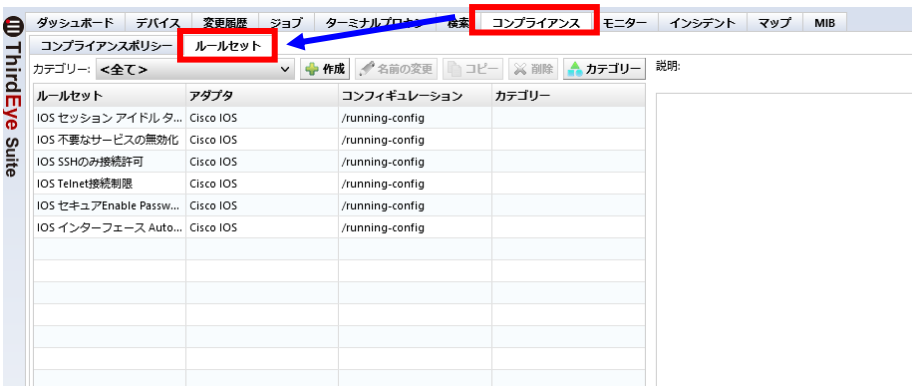
※今回のケースでは、コミュニティ名はコンフィグから取得する為、コミュニティ名の部分を変数化します。

Copyright (C) 2026 LogicVein, Inc.

6. 変数名を入力し、OK をクリックします。

7. 保存します。

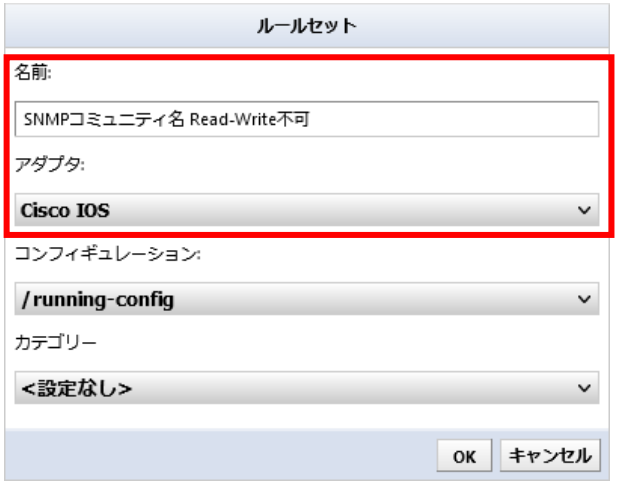
8. コンプライアンス->ルールセットに移動し、作成をクリックします。



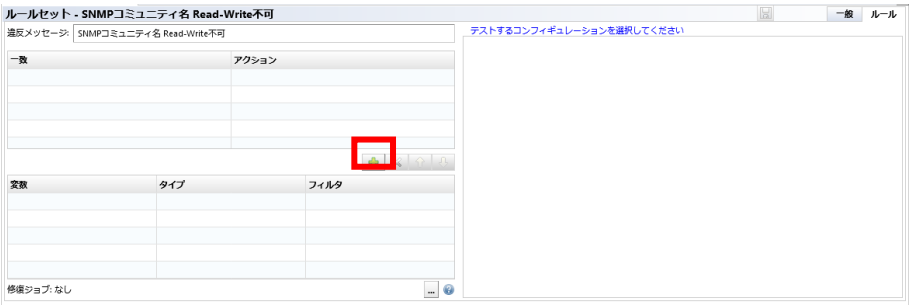
Copyright (C) 2026 LogicVein, Inc.

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。

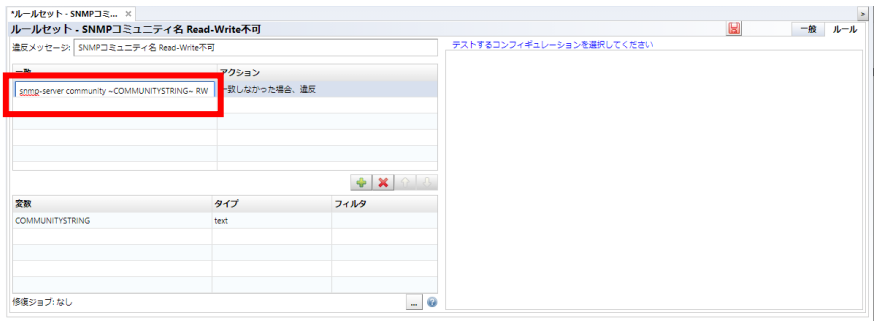
※アダプタはバルクチェンジ作成時に選択したアダプタを選択してください。



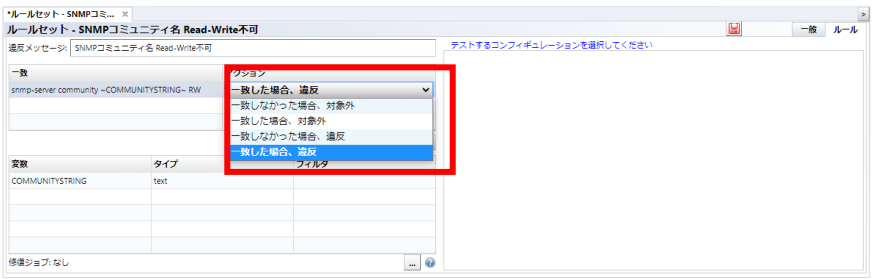
10. ＋をクリックし、一致条件を追加します。



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。



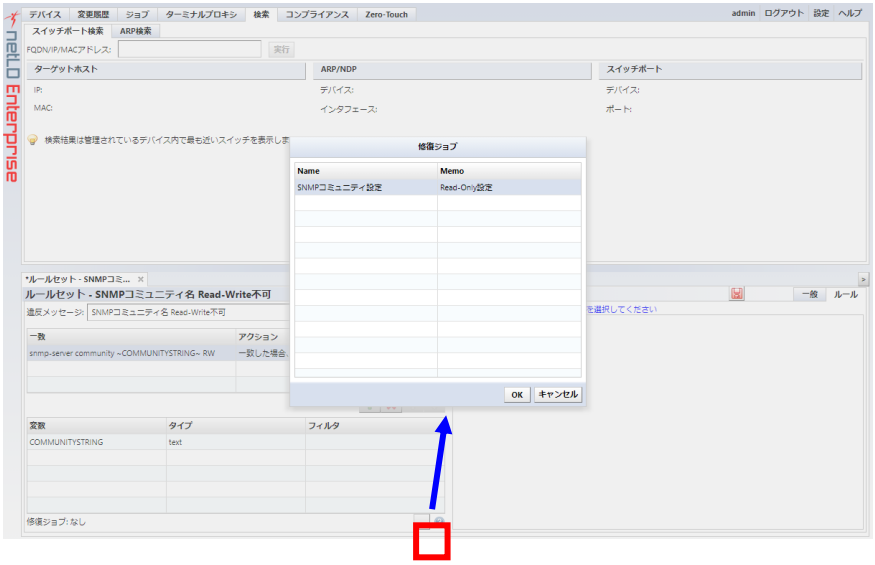
12. アクションを「一致した場合、違反」に設定します。



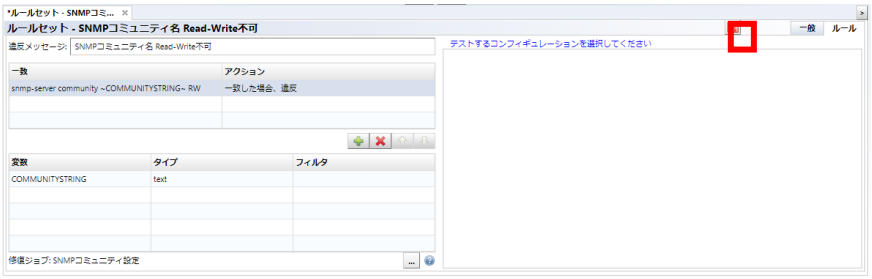
Copyright (C) 2026 LogicVein, Inc.

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。



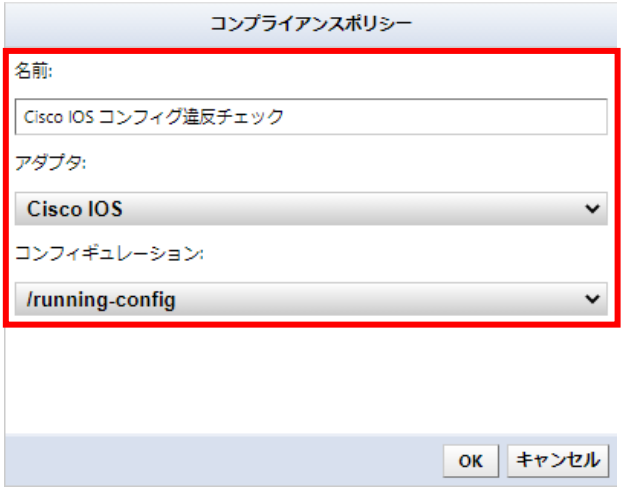
14. 設定を保存します。



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。

Copyright (C) 2026 LogicVein, Inc.

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。

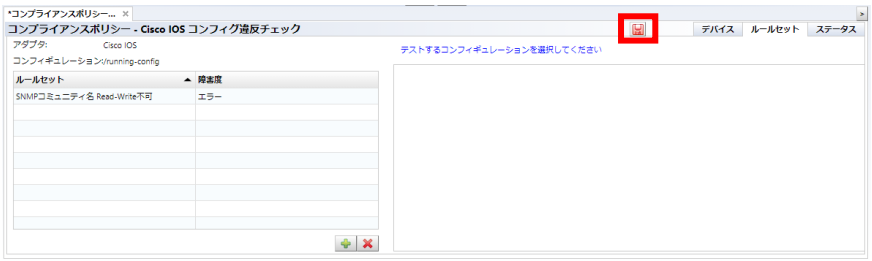


17. ＋をクリックします。

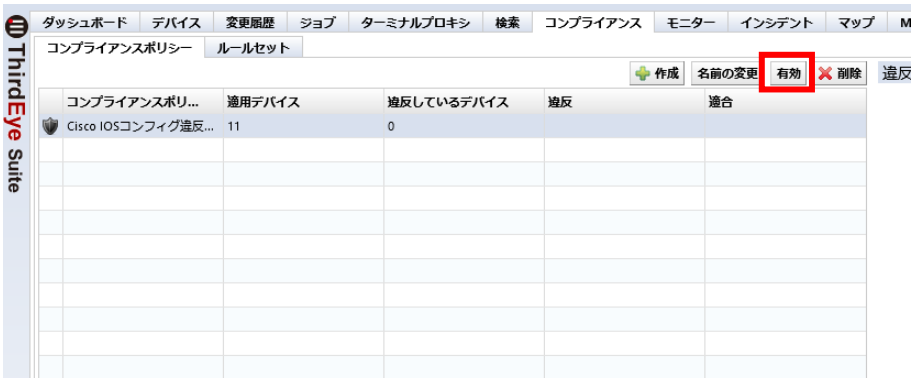
18. ルールセットを選択し、追加をクリックします。

Copyright (C) 2026 LogicVein, Inc.

19. 保存をクリックします。



20. 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。

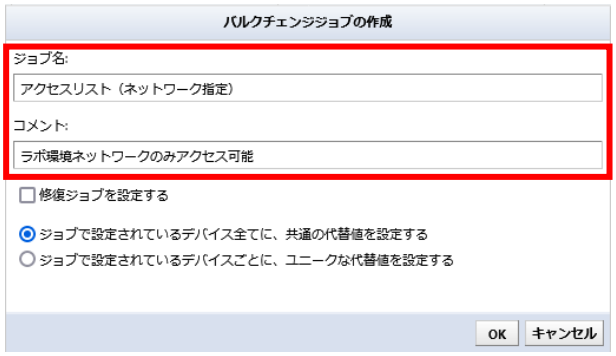


Copyright (C) 2026 LogicVein, Inc.

(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

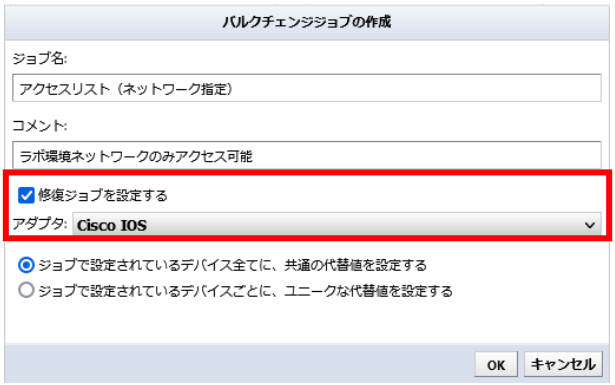
1. ジョブ->ジョブ管理に移動し、新しいジョブ->バルクチェンジを選択します。

2. ジョブ名、コメント（オプション）を入力します。

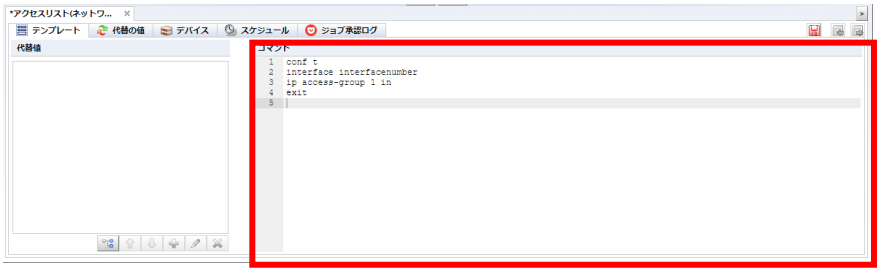


3. 「修復ジョブを設定する」にチェックを入れ、デバイスのアダプタを選択し OK をクリックします。

※　ルールセットとの紐付けに使用します。



4. テンプレートに実行するコマンドを入力します。

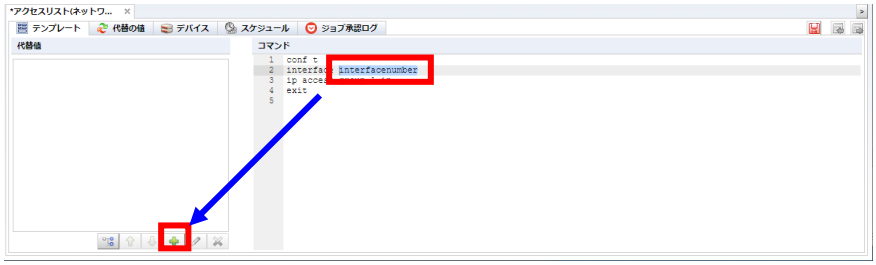


Copyright (C) 2026 LogicVein, Inc.

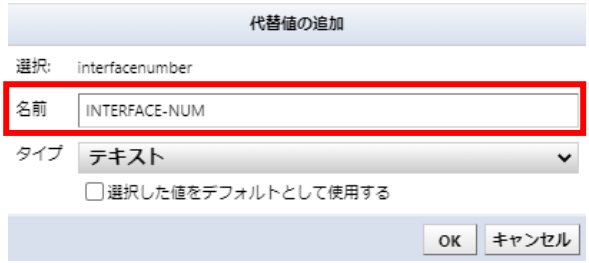
5. 変数化する箇所を選択し、+をクリックします。

※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。

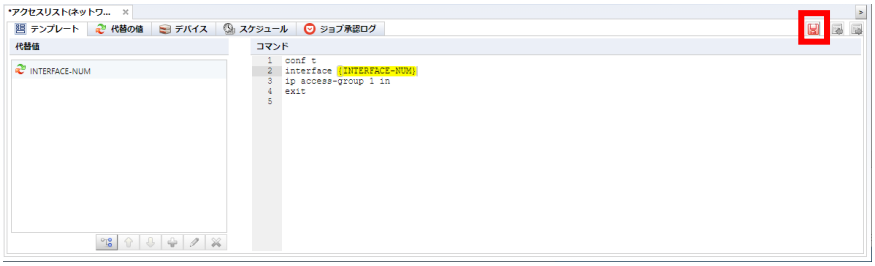
※今回のケースでは、コミュニティ名はコンフィグから取得する為、コミュニティ名の部分を変数化します。



6. 変数名を入力し、OK をクリックします。



7. 保存します。

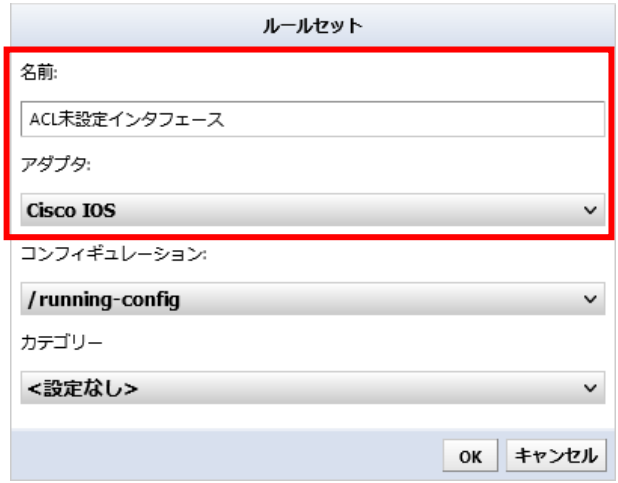


8. コンプライアンス->ルールセットに移動し、作成をクリックします。

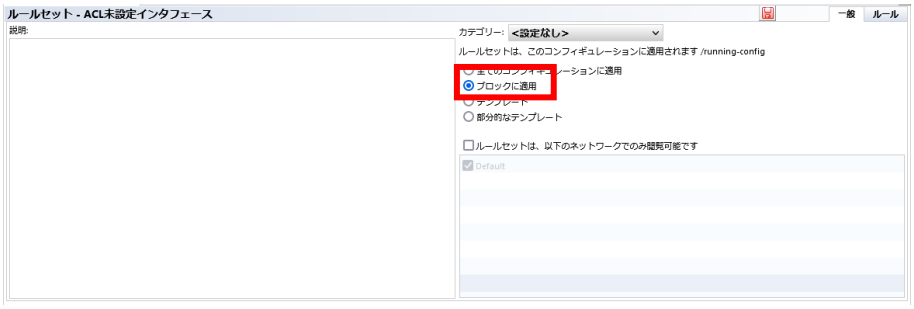
Copyright (C) 2026 LogicVein, Inc.

9. ルール名を入力後、アダプタを選択し、OK をクリックします。

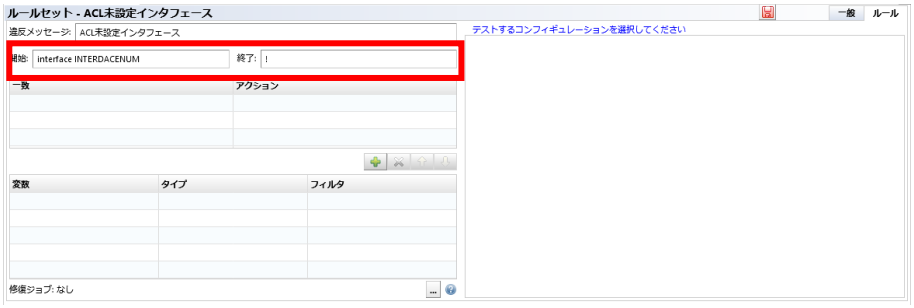
※アダプタはバルクチェンジ作成時に選択したアダプタを選択してください。



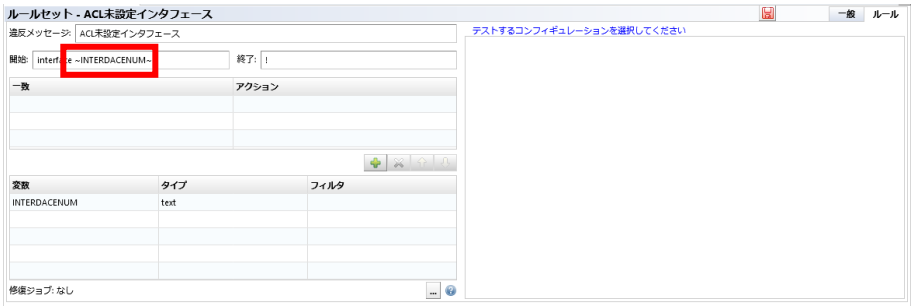
10. 一般タブに移動し、「ブロックに適用」を選択します。



11. ルールを適用するブロックを「開始/終了」で指定します。



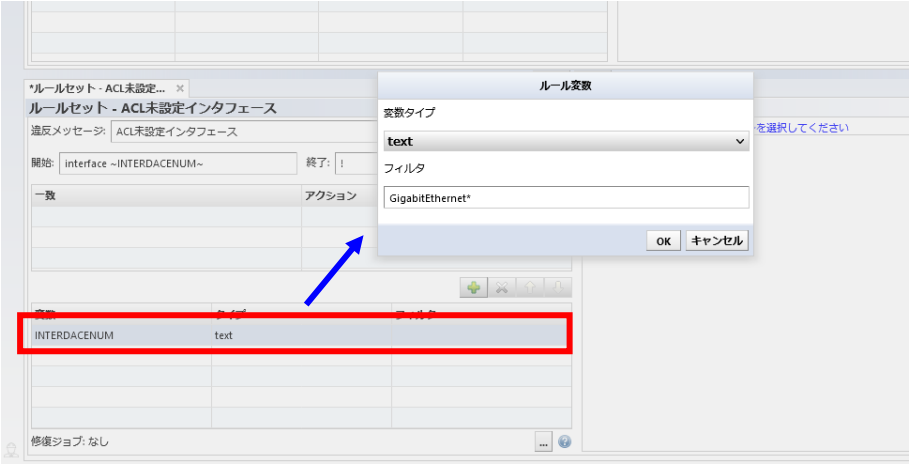
12. インタフェース番号の部分をバルクチェンジの変数名に指定し「~」で挟みます。



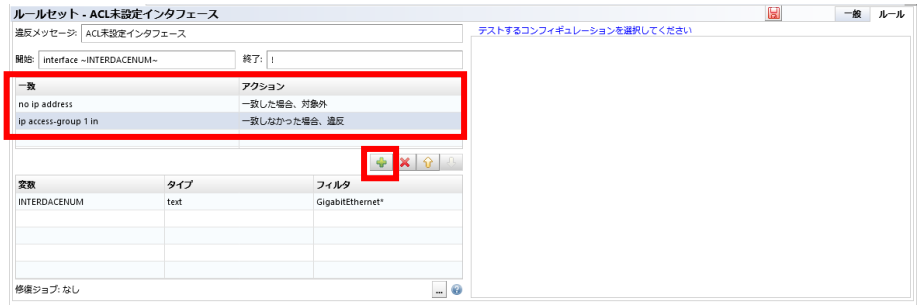
Copyright (C) 2026 LogicVein, Inc.

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。

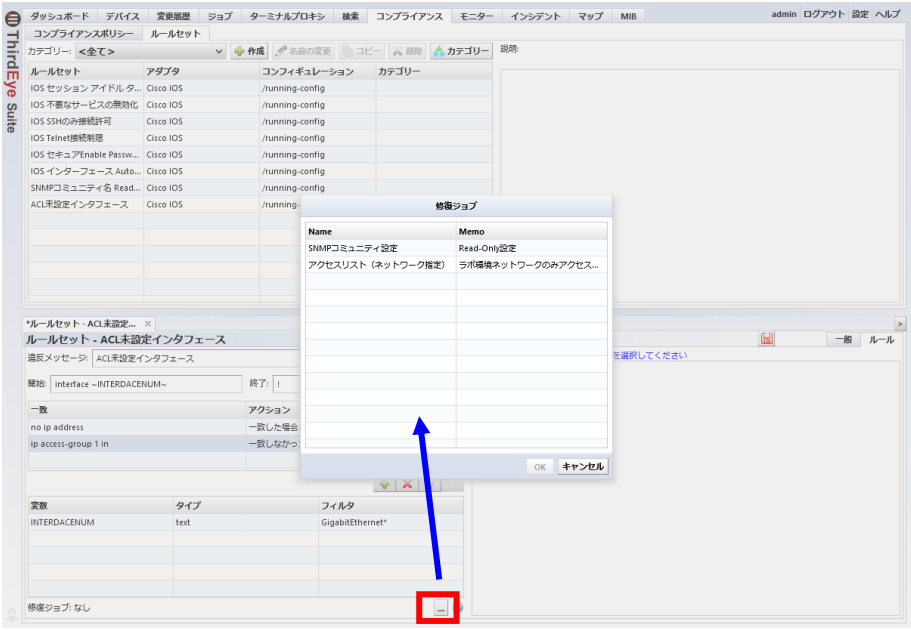


14. ＋をクリックし、一致条件を追加します。



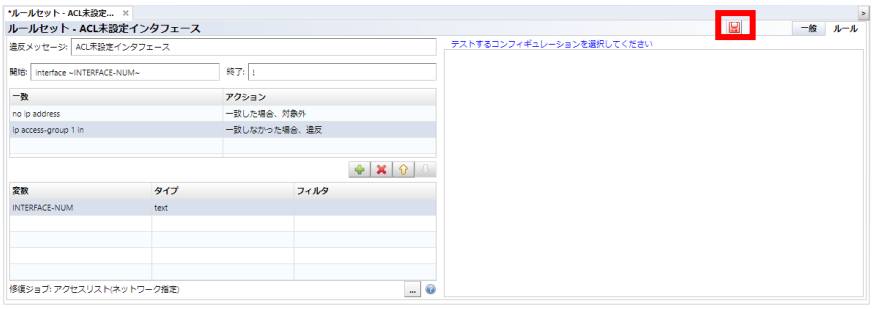
15. 修復ジョブの「…」をクリックし、違反時に実行するバルクチェンジジョブを指定します。

※指定できるジョブは１つです。



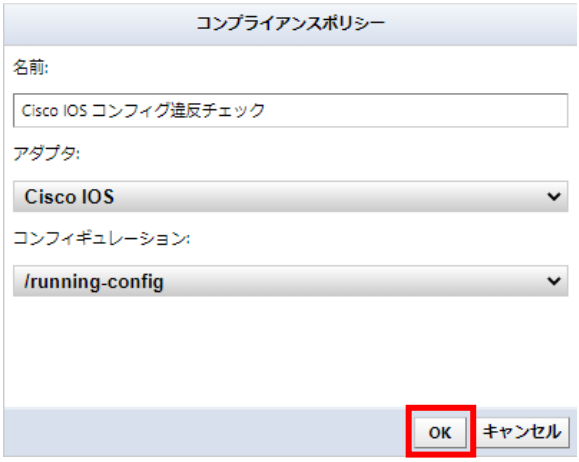
Copyright (C) 2026 LogicVein, Inc.

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。



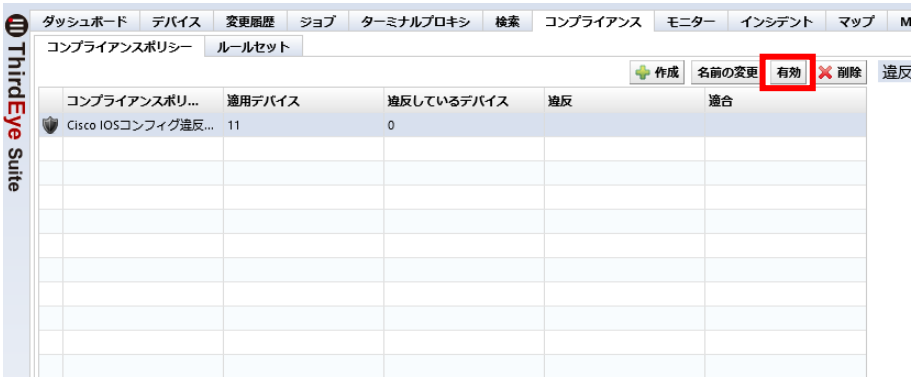
19. ＋をクリックします。

Copyright (C) 2026 LogicVein, Inc.

20. ルールセットを追加します。

21. 保存をクリックします。

22. 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。



Copyright (C) 2026 LogicVein, Inc.

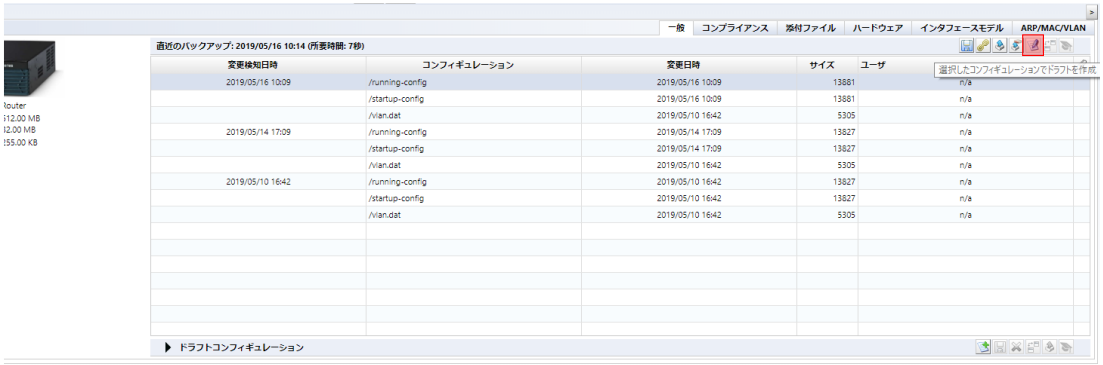
7.3　ドラフトコンフィギュレーション Suite

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。

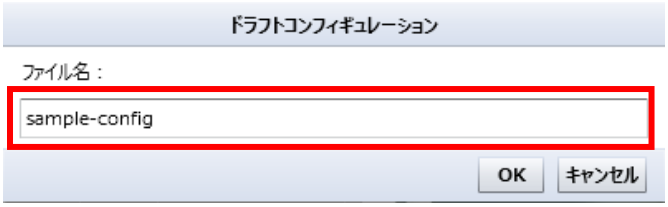
7.3.1　ドラフトコンフィギュレーションの作成

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。

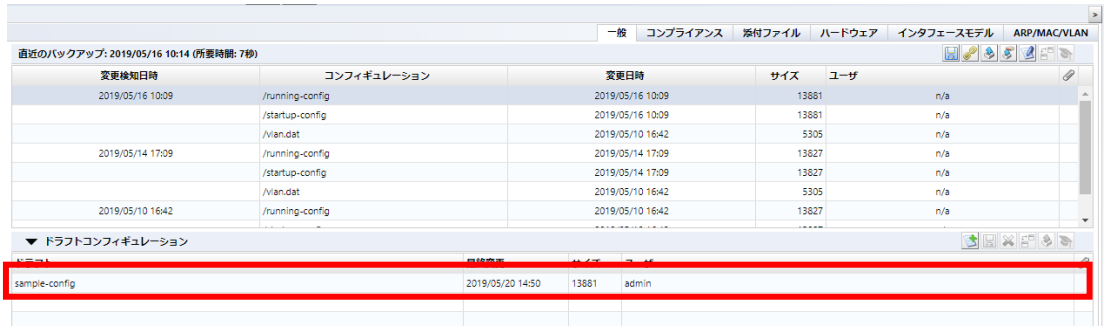
1. 対象デバイスをダブルクリックしてコンフィグ履歴を開いてください。
2. ドラフトコンフィギュレーションのベースとなるものを選択し ボタンをクリックします。



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。

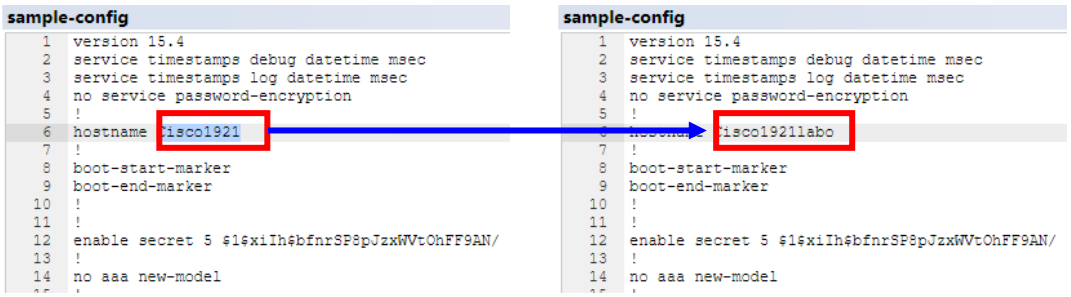


4. 作成されたドラフトコンフィギュレーションをダブルクリックします。



Copyright (C) 2026 LogicVein, Inc.

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。



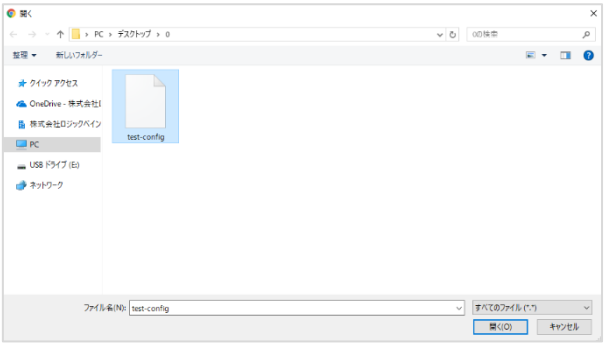
Copyright (C) 2026 LogicVein, Inc.

7.3.2　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

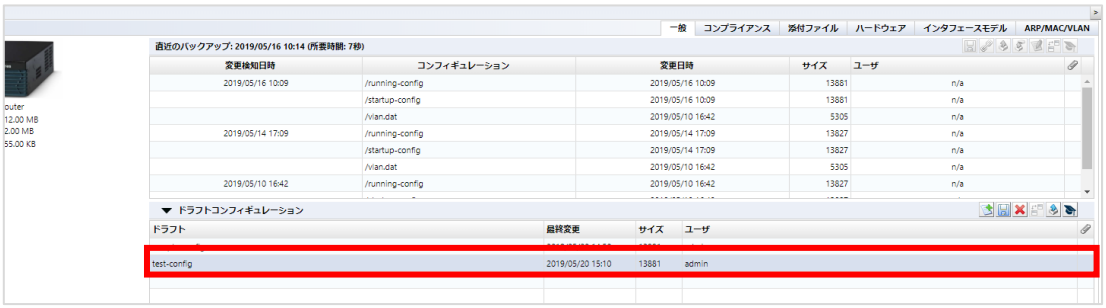
テキストエディタ等で編集したコンフィギュレーションをインポートすることで、ドラフトコンフィギュレーションを作成することができます。まず、デバイスビューで対象デバイスをダブルクリックし、 コンフィグ履歴を表示してください。

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。



7.3.3　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。

7.3.4　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。

Copyright (C) 2026 LogicVein, Inc.

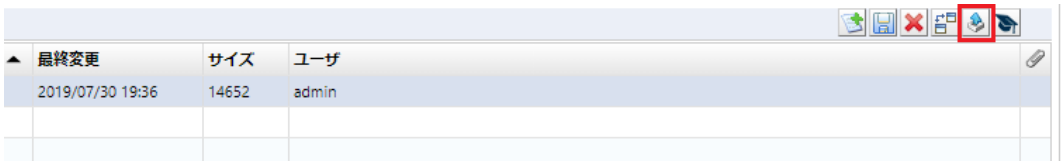
7.3.5　ドラフト同士の比較

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。

7.3.6　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出来ます。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。



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。)

OK を押してアップロードを開始してください。

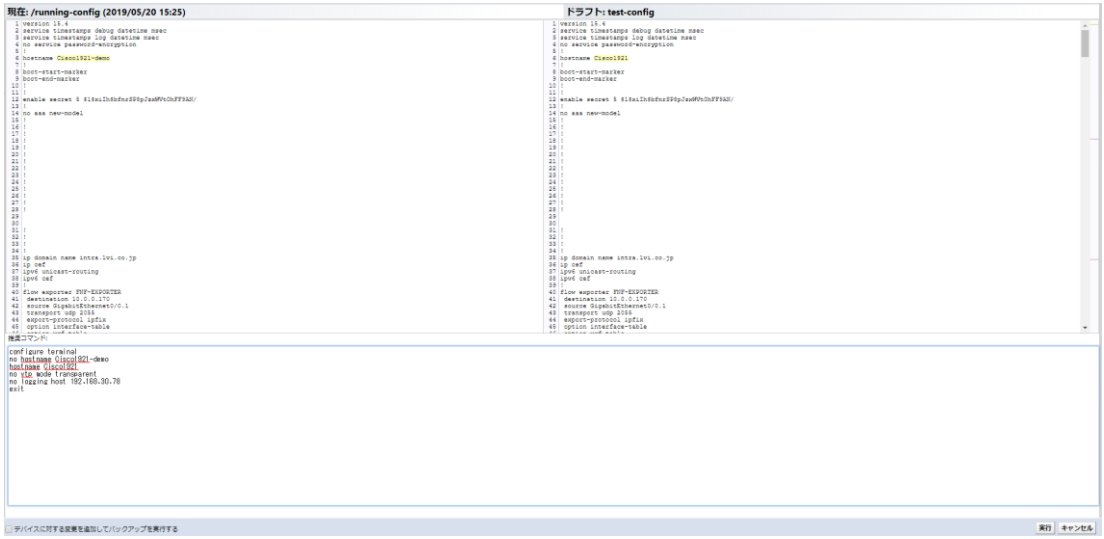
Copyright (C) 2026 LogicVein, Inc.

7.4　チェンジアドバイザ Suite

チェンジアドバイザは、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。

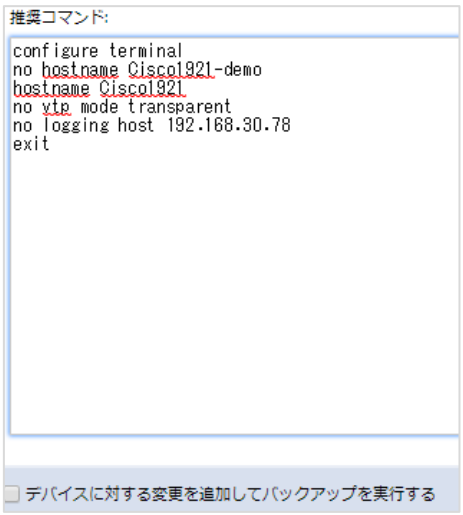
4. チェンジアドバイザが起動し、下側のペインでコマンドが提示されます。



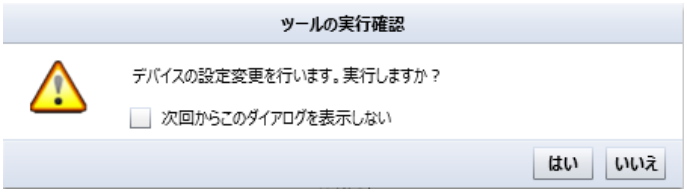
Copyright (C) 2026 LogicVein, Inc.

7.4.1　チェンジアドバイザを用いてコマンドを実行する

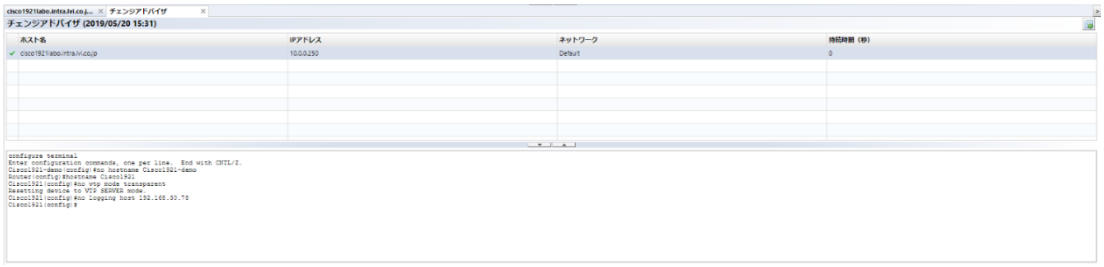
チェンジアドバイザの出力したコマンドをデバイスで実行することが出来ます。提示されたコマンドを実行する前に、実行するコマンドを一度確認してください。不適切なコマンドがあった場合には、出力されたコマンドを直接編集することが出来ます。



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の機能を用いて代用することが出来ます。

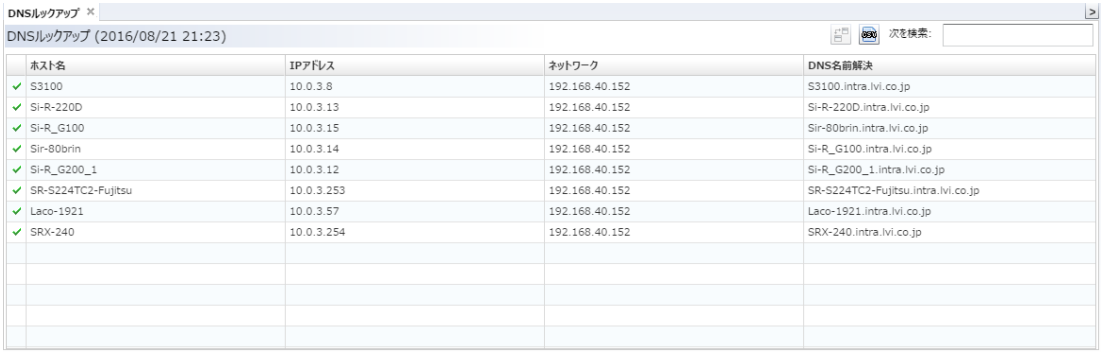
Copyright (C) 2026 LogicVein, Inc.

7.5　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、そこの常に右上にある ボタンから行うことが出来ます。

7.5.1　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。



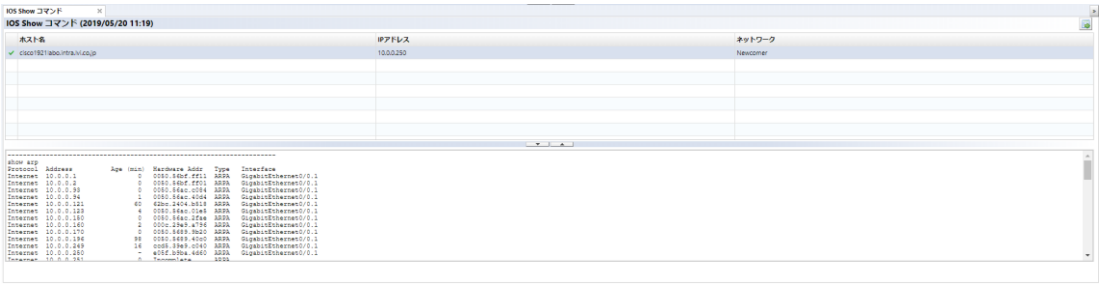
ホスト名	IPアドレス	ネットワーク	DNS名前解決
S3100	10.0.3.8	192.168.40.152	S3100.intra.lvi.co.jp
Si-R-220D	10.0.3.13	192.168.40.152	Si-R-220D.intra.lvi.co.jp
Si-R_G100	10.0.3.15	192.168.40.152	Sir-80brin.intra.lvi.co.jp
Sir-80brin	10.0.3.14	192.168.40.152	Si-R_G100.intra.lvi.co.jp
Si-R_G200_1	10.0.3.12	192.168.40.152	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

Copyright (C) 2026 LogicVein, Inc.

7.5.2 IOS Show コマンド

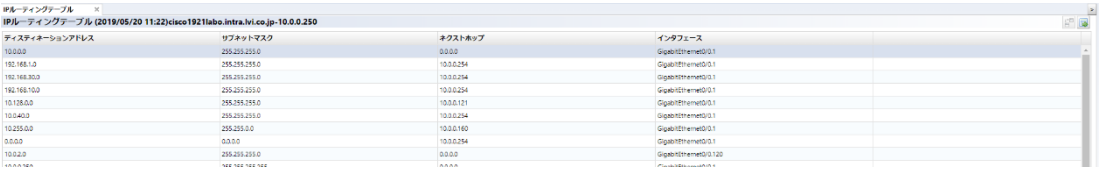
デバイスの IOS Show コマンドの結果を表示します。ただしこのコマンドは Cisco IOS と互換性のあるデバイス上でしか実行できません。はじめに実行する show コマンドをリストから選択し、*実行*を押すとコマンドが発行されます。

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。



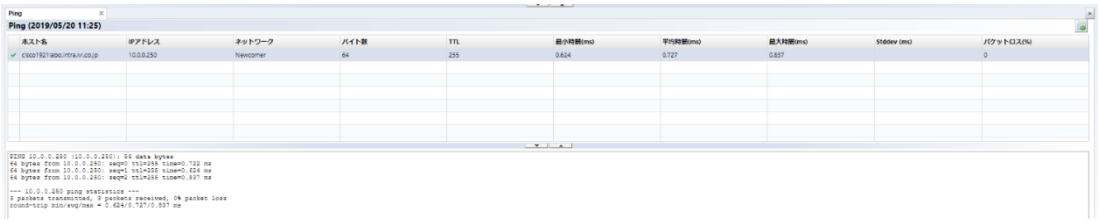
7.5.3 IP ルーティングテーブル

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。



7.5.4 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。



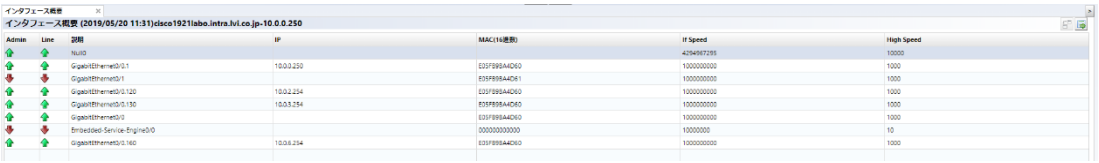
Copyright (C) 2026 LogicVein, Inc.

7.5.5 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。

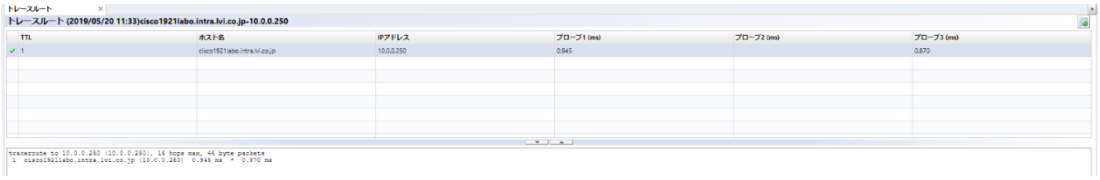
7.5.6 インタフェース概要

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。



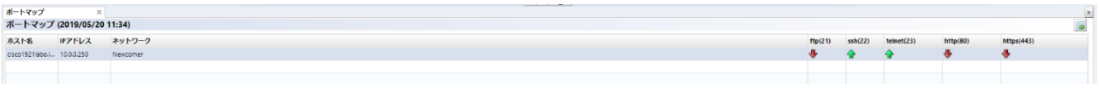
7.5.7 トレースルート

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。



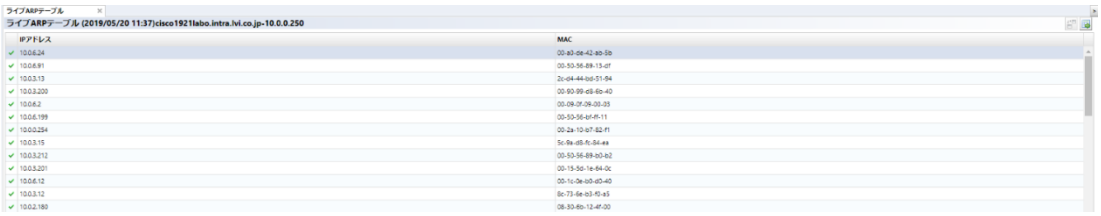
7.5.8 ポートマップ

デバイスのポート開閉情報を表示します。



7.5.9 ライブの ARP テーブル

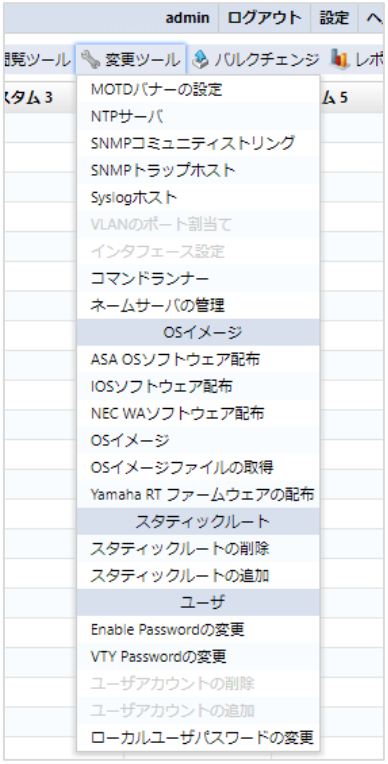
ARP テーブルのライブステータスを表示します。なお、この機能はデバイスを複数選択した状態では実行することができません。



Copyright (C) 2026 LogicVein, Inc.

7.6　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。



7.6.1 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。

Copyright (C) 2026 LogicVein, Inc.

7.6.2 NTP サーバ

NTP サーバをデバイスに追加/削除します。

7.6.3 SNMP コミュニティストリング

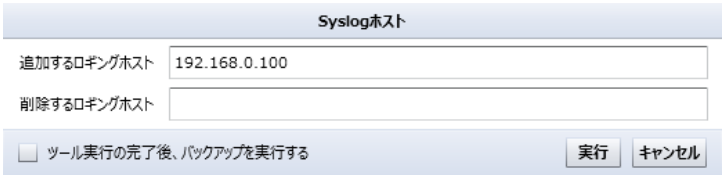
デバイスに対して、SNMP コミュニティを追加/削除します。

7.6.4 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。

7.6.5 Syslog ホスト

デバイスに対して、Syslog ホストを追加/削除します。



Copyright (C) 2026 LogicVein, Inc.

7.6.6 VLAN のポート割当て

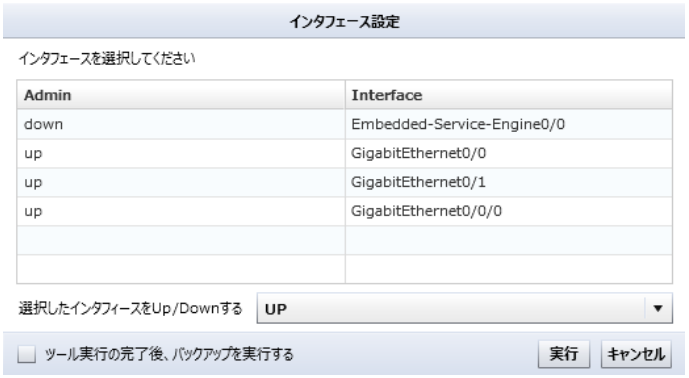
デバイスのアクセスポートに対して、VLAN ポートの設定を実行します。なお、この機能はデバイスを複数選択した状態では実行することができません。

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。

7.6.7 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。

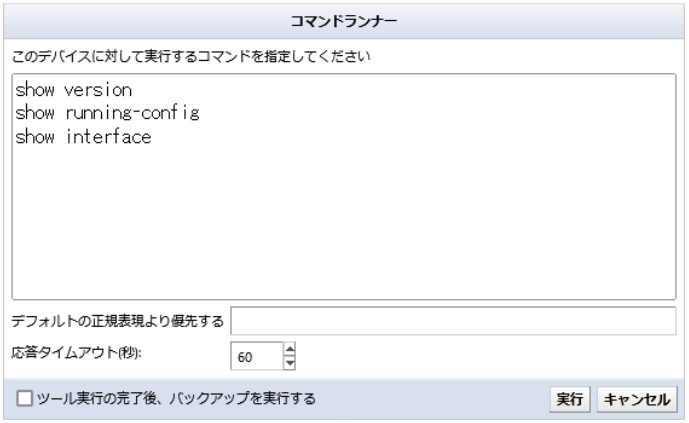
「インタフェースを選択してください」欄から、Admin Status を変更するインタフェースを選択(複数選択可)し、プルダウンメニューで Up/Down を選択して「実行」ボタンをクリックします。



Copyright (C) 2026 LogicVein, Inc.

7.6.8 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。

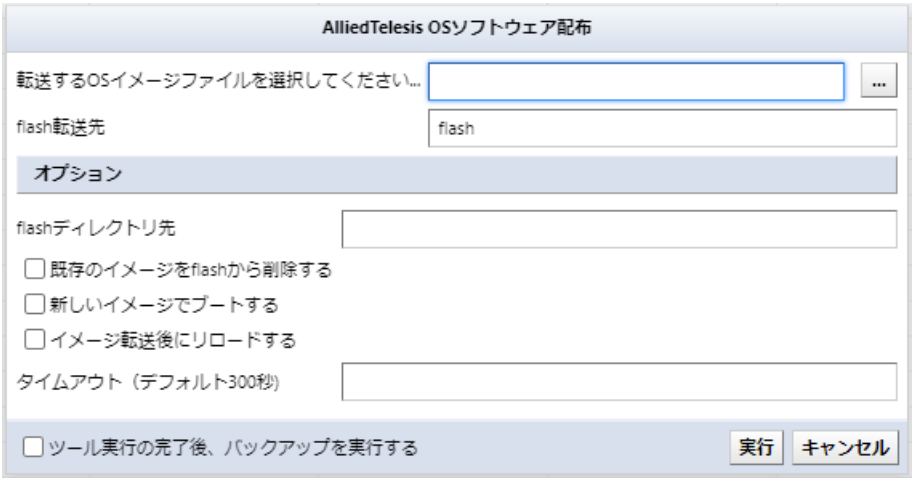


デフォルトの正規表現より優先するという欄は、特定のタイプのプロンプトにマッチする正規表現を指定します。マッチされるプロンプトは、シェルスクリプトで言えば PS1 変数のようなものです。この欄を指定する必要があるのは、あるコマンドが通常と異なるプロンプトを用いた返答をする場合です。たとえば、一部のインタラクティブなコマンドは通常『<username>#』で始まるプロンプトではなく、よりシンプルな『<』で始まるコマンドを用いて次の入力を促してくるかもしれません。その場合には、それを正規表現^< (行頭の<)で指定する必要があります。そうしなくては、コマンドの出力結果とプロンプトを区別することができ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

Copyright (C) 2026 LogicVein, Inc.

7.6.9　Allied Telesis OS ソフトウェア配布

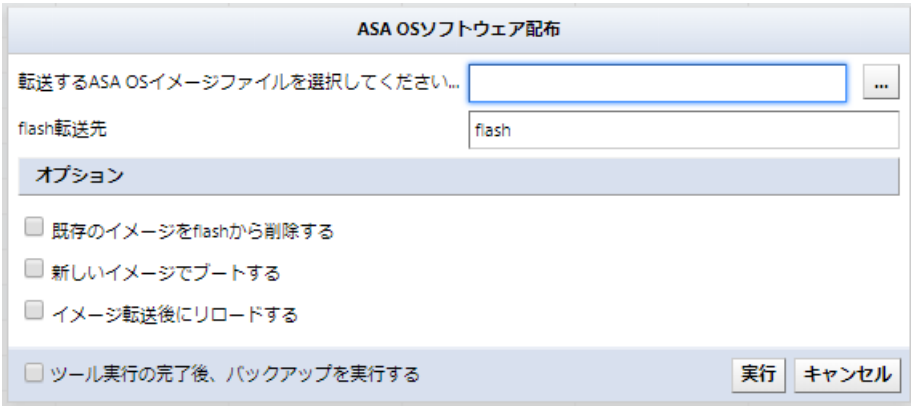
Allied Telesis のデバイスに対して OS をリモート配布することができます。本機能を使用するには、予め OS を保存しておく必要があります。保存方法の詳細については「7.6.14 OS イメージ」を参照してください。



項目	説明
転送する 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 イメージをブラウズ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。
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。
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。
タイムアウト（デフォルト 300 秒）	ネットワークの通信遅延が多い環境で待機時間を指定する。

7.6.10　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「7.6.14 OS イメージ」を参照してください。



Copyright (C) 2026 LogicVein, Inc.

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 イメージをブラウズ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。

7.6.11　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「7.6.14 OS イメージ」を参照してください。

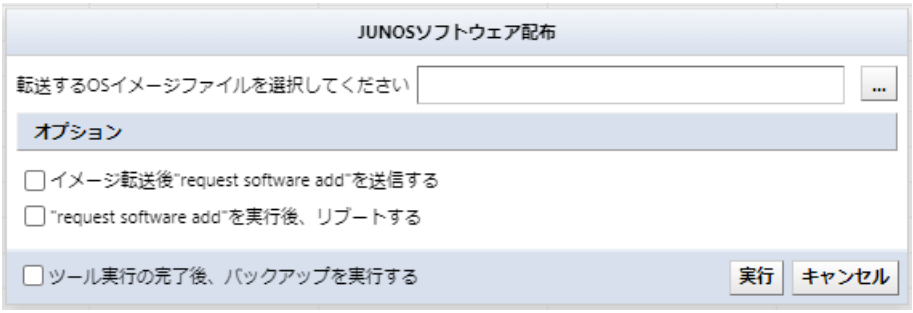
項目	説明
転送する IOS イメージファイルを選択してください	右側の［…］ボタンを押すと、登録してある OS イメージをブラウズするウィンドウが現れますので、アップロードするイメージを選択してください。
flash 転送先	デバイスの備える記憶ドライブを指定します。機種によって、flashusbflashOnvram など、指定できる内容が異なります。
flash ディレクトリ先	転送先ドライブ・パーティション内のディレクトリ。ディレクトリが存在しないときは、指定した名前のディレクトリが自動で生成されます。
flash パーティション先	転送先ドライブのパーティション。指定されたパーティシ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

Copyright (C) 2026 LogicVein, Inc.

項目	説明
ツールの完了後、バックアップを実行する	--

7.6.12 JUNOS OS ソフトウェア配布

JUNOS 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「7.6.14 OS イメージ」を参照してください。



項目	説明
転送する 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 イメージをブラウズ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。
イメージ転送後”request software add”を送信する	イメージ転送後、”request software add”を実行する。
”request software add”を実行後、リブートする	”request software add”を実行後、リブートする。

7.6.13 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「7.6.14 OS イメージ」を参照してください。

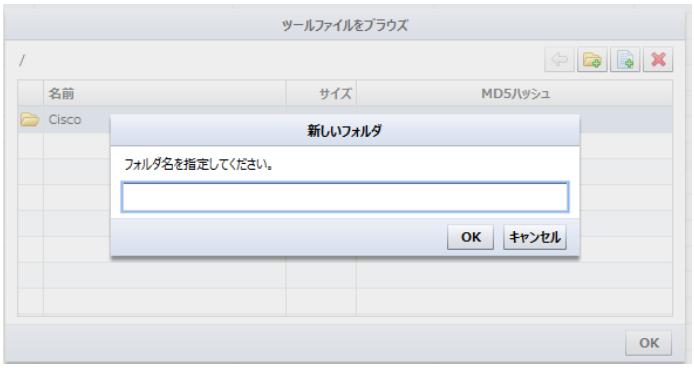
項目	説明
flash ディレクトリ先	転送先のディレクトリ
既存のイメージを flash から削除する	既存のイメージを flash から削除する。
新しいイメージでブートする	イメージ転送後、新しいイメージでブートする設定をする。
イメージ転送後にリロードする	イメージ転送後にリロードする。

Copyright (C) 2026 LogicVein, Inc.

7.6.14　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。

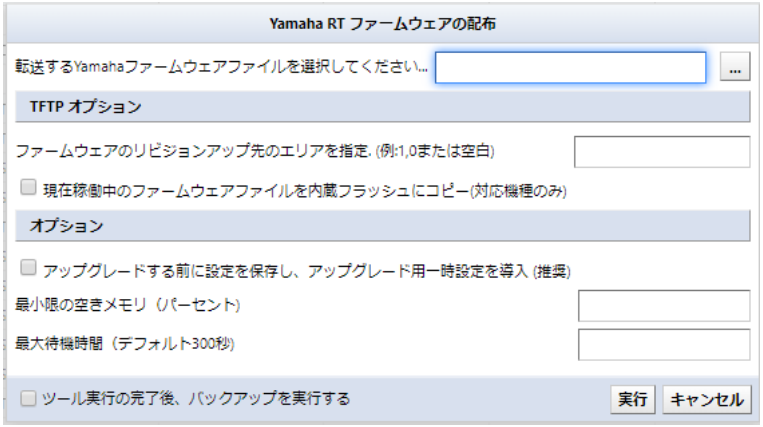
7.6.15　OS イメージファイルの取得

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。

Copyright (C) 2026 LogicVein, Inc.

7.6.16　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「7.6.14 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する。
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。

```
No.   Revision
------------------------------------
  0   Rev.14.01.11
* 1   Rev.14.01.14
------------------------------------
```

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トは中止されます。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”

Copyright (C) 2026 LogicVein, Inc.

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
```

7.6.17　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。

7.6.18　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。

7.6.19　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。

また、スタティッククレデンシャルが使用されている場合、「変更後、クレデンシャルを確認する」にチェックを入れることにより、自動でクレデンシャルが変更され、設定したパスワードでログインできるかを確認します。

Copyright (C) 2026 LogicVein, Inc.

7.6.20　VTY Password の変更

デバイスの VTY Password の設定を変更します。

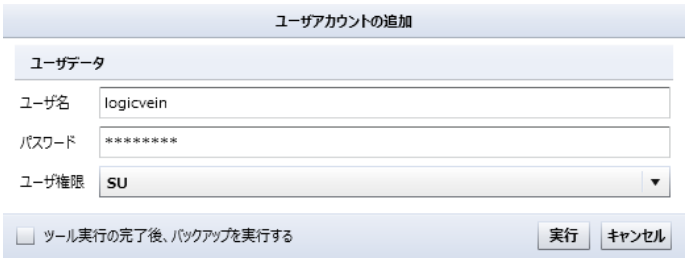
また、Enable Password の変更と同様に、「変更後、クレデンシャルを確認する」にチェックを入れることにより、自動でクレデンシャルが変更され、設定したパスワードでログインできるかを確認します。

7.6.21　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。

7.6.22　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。



7.6.23　ローカルユーザパスワードの変更

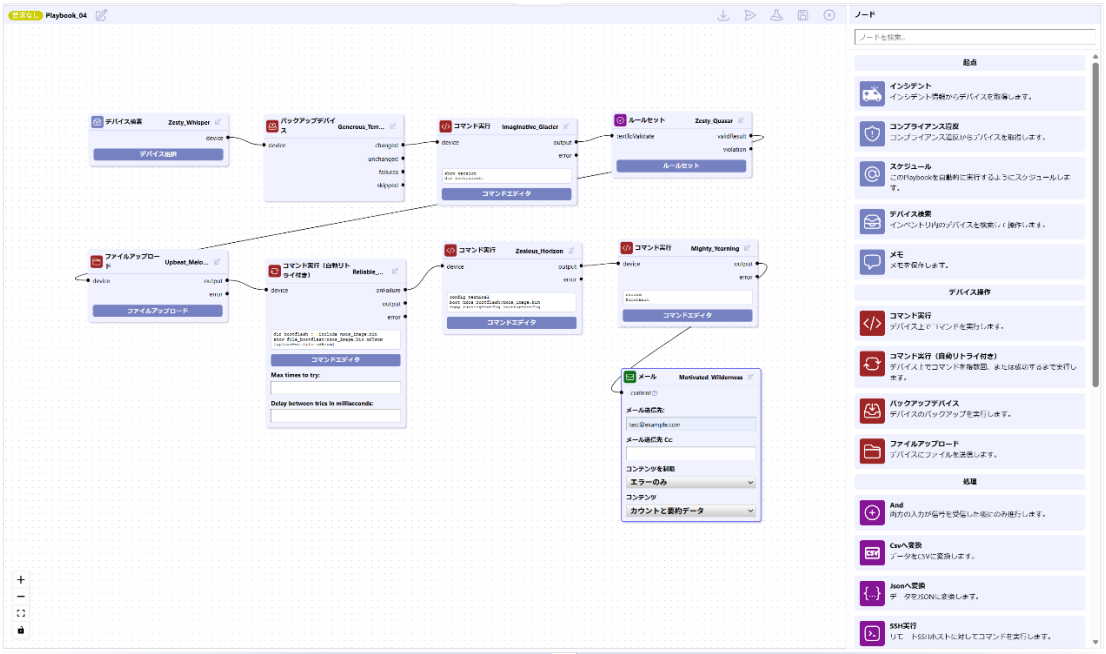
デバイスに設定されているユーザアカウントのパスワードを変更します。

Copyright (C) 2026 LogicVein, Inc.

7.7 Playbook Suite

7.7.1 Playbook の概要

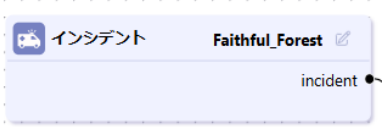
Playbook 機能は、複数のジョブやコマンドの実行結果を組み合わせて、一連のタスクを自動化できる機能です。従来のジョブ機能は、show コマンドの実行などの一方向の処理フローで完結していましたが、Playbook では、show コマンドの実行結果に基づいて条件分岐を行い、追加のコマンドを実行したり、メール通知を送信したりすることができます。これによって、より複雑な業務フローを自動化し、効率的な運用を実現できます。



7.7.2 Playbook ノード

Playbook では、アクションを表す「ノード」と呼ばれるボックスを線でつなげて、一連のタスクを構築します。ノードは機能別に 4 つのカテゴリに大別されます。カテゴリごとのノードの種類とその説明を、次の表に示します。

1.「起点」ノード：Playbook にデバイスを追加し、プロセスを開始するノードです。

ノードアイコン	ノードラベル	説明
	インシデント	インシデント情報からデバイスを取得します。 
	コンプライアンス違反	コンプライアンス違反が発生したデバイスに関する情報を次のノードに送信します。

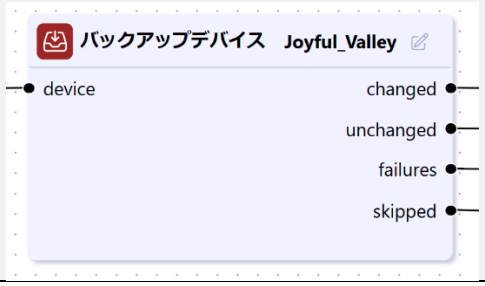
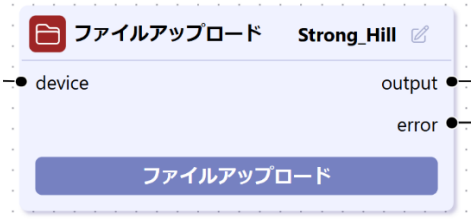
Copyright (C) 2026 LogicVein, Inc.

ノードアイコン	ノードラベル	説明
	スケジュール	Playbook を自動的に実行するようにスケジュールします。このノードは次のノードに接続されていなくても、有効に設定されていれば実行されます。
	デバイス検索	Playbook 開始時に、検索条件に一致したデバイスに関する情報を次のノードに送信します。検索方法には、「全てのデバイス」、「検索」、「静的リスト」の 3 つがあります。
	メモ	Playbook 画面にメモを保存します。一連のタスクにメモを追加し、その内容を次のノードに送信できます。また、このメモは Playbook の内容を把握する際にも役立ちます。

2. 「デバイス操作」ノード：CLI コマンドを送信し、デバイスを操作するノードです。

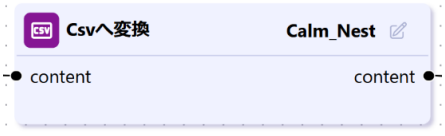
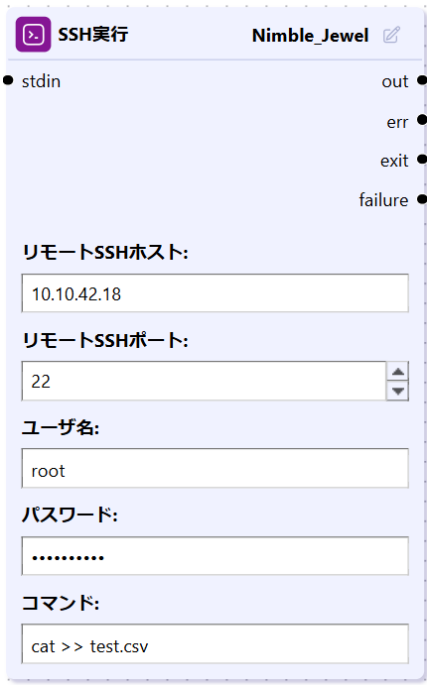
ノードアイコン	ノードラベル	説明
	コマンド実行	前のノードから受信した対象デバイスの情報をもとに、指定されたコマンドを実行し、その結果を次のノードに送信します。

Copyright (C) 2026 LogicVein, Inc.

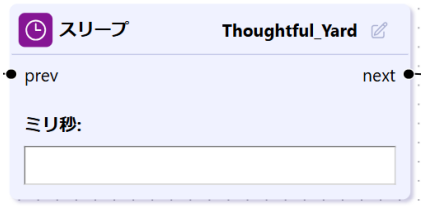
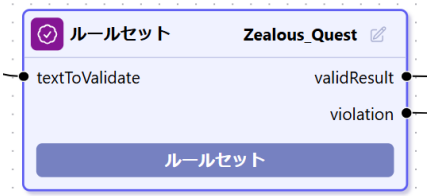
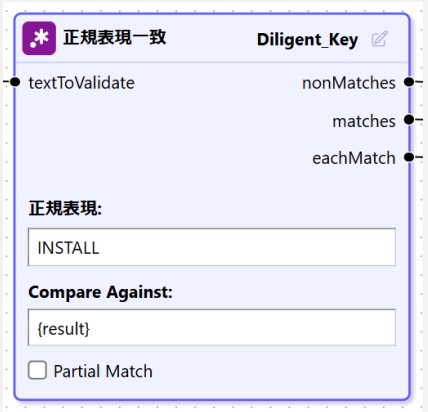
ノードアイコン	ノードラベル	説明
	コマンド実行 （自動リトライ付き）	前のノードから受信した対象デバイスの情報をもとに、指定されたコマンドを、指定回数実行します。リトライは、「Delay between tries in milliseconds:」で指定されたミリ秒間隔で、指定された回数行われます。
	バックアップデバイス	デバイスのバックアップを実行し、バックアップの結果（「変更あり」、「変更なし」、「失敗」、「スキップ」）に基づいて処理を分岐します。 
	ファイルアップロード	前のノードから受信した対象デバイスにファイルを送信します。サポートされているプロトコルは、FTP/TFTP/SCP です。 

Copyright (C) 2026 LogicVein, Inc.

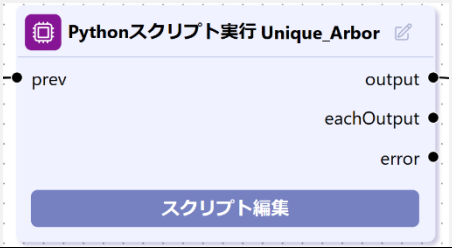
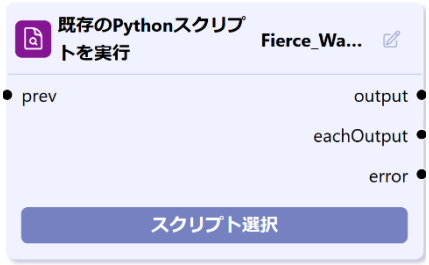
3. 「処理」ノード：データ処理や条件分岐・制御を行うノードです。

ノードアイコン	ノードラベル	説明
	And	a と b の両方の入力信号が受信された後、処理が進行します。各入力から受信した情報は、ノードの右側にある a と b それぞれから次のノードに送信されます。
	Csv へ変換	出力されたデータを Csv フォーマットへ変換します。 
	Json へ変換	出力されたデータを Json フォーマットへ変換します。
	SSH 実行	データを受信した後に SSH ホストに対してコマンドを実行し、結果を次のノードに送信します。 

Copyright (C) 2026 LogicVein, Inc.

ノードアイコン	ノードラベル	説明
	コンフィグ読み込み	最新のバックアップコンフィギュレーションを読み込みます。
	スリープ	指定されたミリ秒数だけ、入力の送信を遅延させます。 
	デバイス別マージ	デバイスごとに出力を一つにまとめます。
	ルールセット	前のノードから受信したコマンドの実行結果などのテキストデータを、指定されたルールセットに従って評価し、その結果を次のノードに送信します。 
	正規表現一致	前のノードから受信したコマンドの出力結果に対して、正規表現を用いた文字列検索を実行します。検索結果が正規表現にマッチしたかどうかに応じて、処理を分岐させることができます。また、「Partial Match」オプションを有効にすることで、部分一致の検索も可能です。 

Copyright (C) 2026 LogicVein, Inc.

ノードアイコン	ノードラベル	説明
	変数の設定	変数を設定し、次のノードへ指定した値を送信します。
	Python スクリプト実行	実行コンテナで Python スクリプトを実行します。 
	既存の Python スクリプトを実行	実行コンテナにアップロードされた Python スクリプトを実行します。 

4. 「出力」ノード：実行結果を外部、またはシステム内へ出力するノードです。

ノードアイコン	ノードラベル	説明
	コンプライアンス違反検出	コンプライアンス違反としてデバイスのステータスを更新します。このノードを使用するとデバイスプロパティのコンプライアンスタブにコンプライアンス違反として登録されます。

Copyright (C) 2026 LogicVein, Inc.

ノードアイコン	ノードラベル	説明
	チャットアプリ (ウェブフック)	前のノードから実行結果を受信後、その内容をウェブフック経由で指定されたチャットアプリに送信します。通知内容はコマンドの結果ではなく、実行結果の要約です。サポートされているチャットアプリは「Microsoft Teams / Slack / Mattermost / WebEx /LINE WORKS/Google Chat」です。
	フィールドを編集	デバイスのカスタムフィールドを更新します。{中括弧}で囲んだ変数名を記述することで変数を設定することができます。

Copyright (C) 2026 LogicVein, Inc.

ノードアイコン	ノードラベル	説明
	メール	Playbook の実行結果をメールで送信します。メールの内容は、コンテンツおよびコンテンツ制限のプルダウンで変更することができます。

7.7.3 Playbook の管理

Playbook を管理する方法について説明します。ここでは、新しい Playbook の作成から、既存の Playbook の編集、削除方法について説明します。

7.7.3.1 Playbook の追加

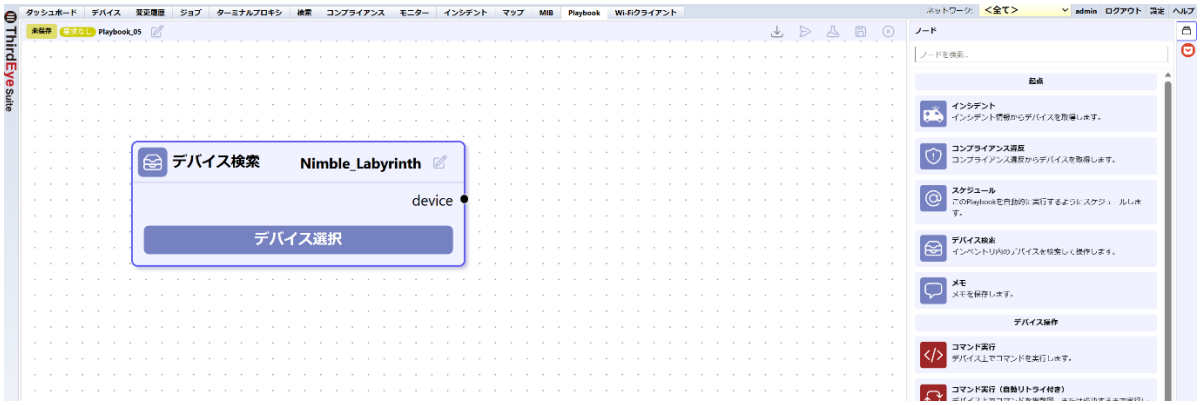
1. ［Playbook］タブを開きます。
2. ［追加］をクリックします。

Copyright (C) 2026 LogicVein, Inc.

3. 名前欄に作成する Playbook の名前を入力します。説明欄の入力は任意です。

Copyright (C) 2026 LogicVein, Inc.

4. ［OK］をクリックします。
5. 画面右側のリストから構成するノードを選択し、左側の表示領域にドラッグ・アンド・ドロップして追加します。

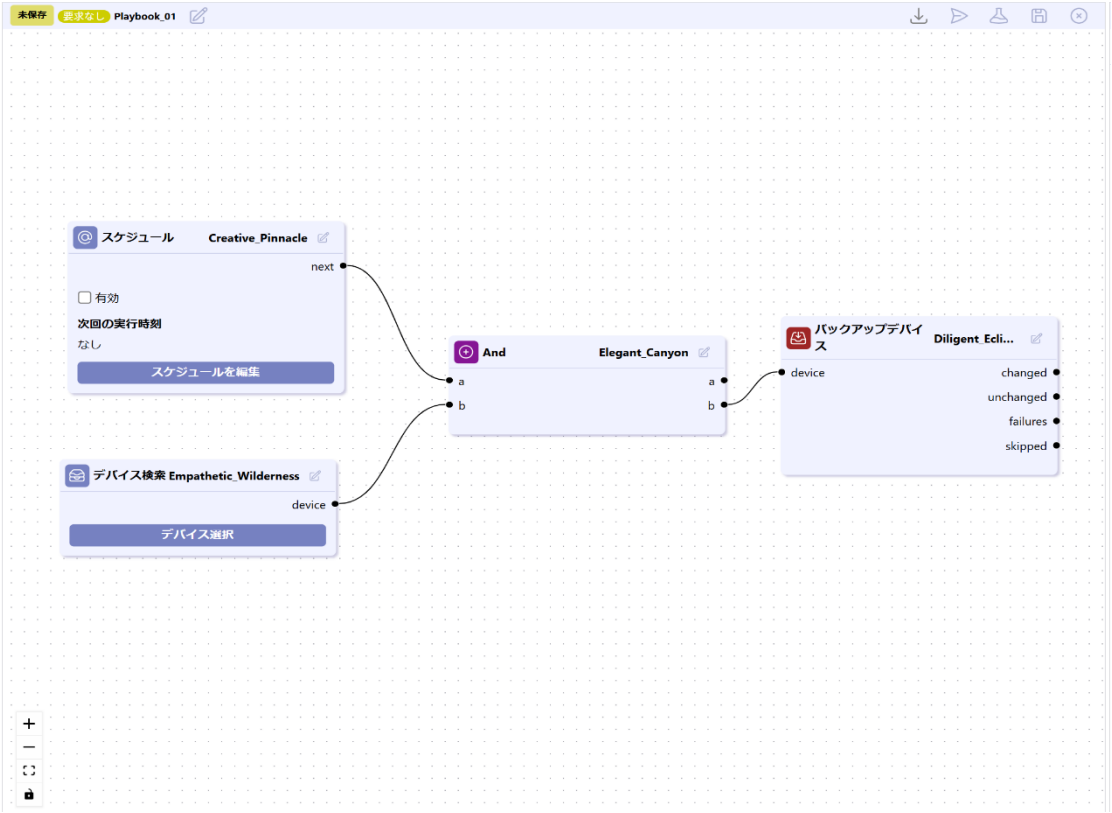


補足

検索ボックスを使用することで、ノード一覧に表示されるノードをノード名で絞り込むことが可能です。

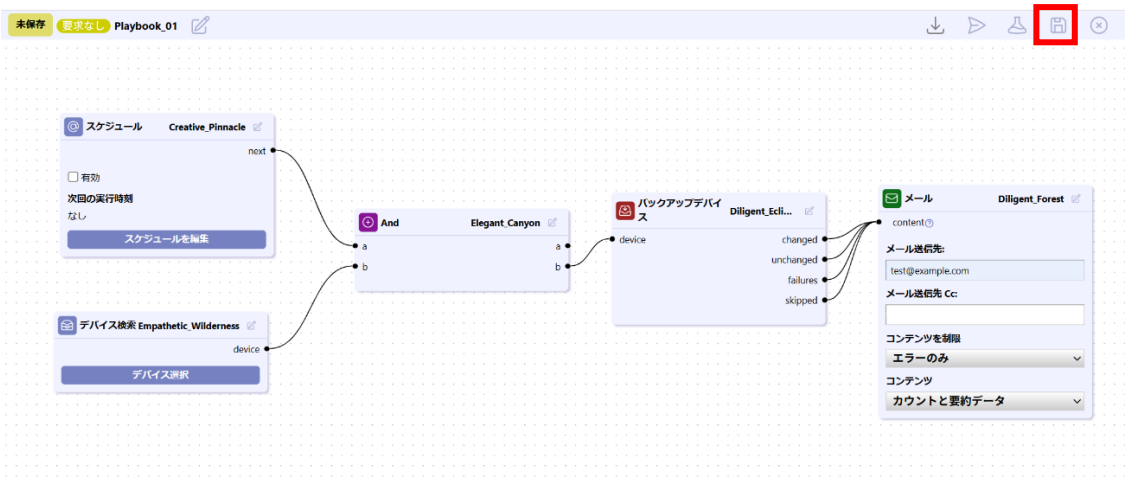
Copyright (C) 2026 LogicVein, Inc.

6. ドラッグ操作でノード間を接続します。



Copyright (C) 2026 LogicVein, Inc.

7. 編集が完了したら、［Playbook を保存する］ボタンをクリックします。

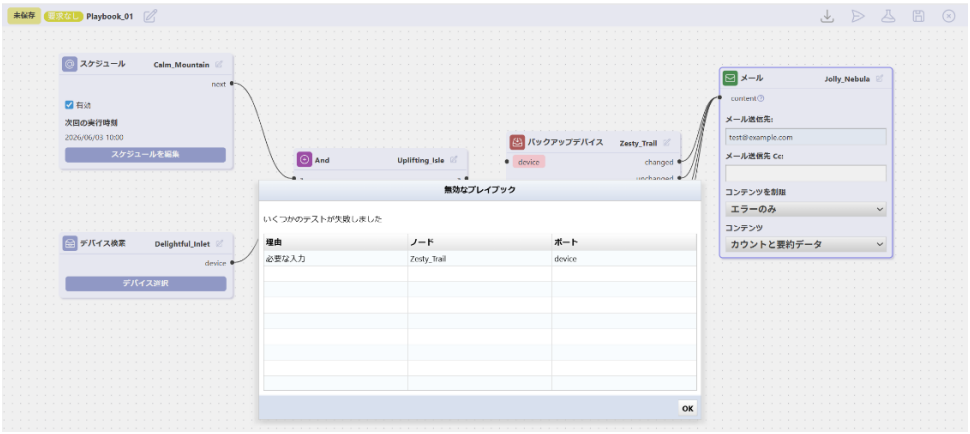


補足

Playbook の設定に無効な設定がないか、以下のアイコンをクリックして確認できます。

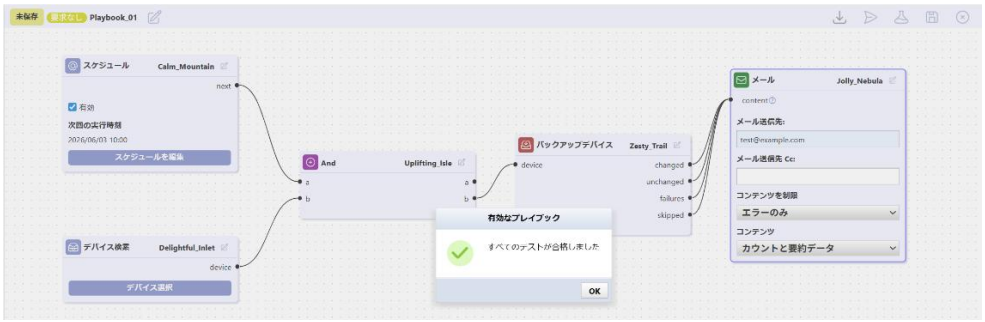
＜無効な設定がある場合＞

無効な設定がある箇所はテーブル形式で表示され、修正が必要な箇所は赤色でハイライトされます。



＜無効な設定がない場合＞

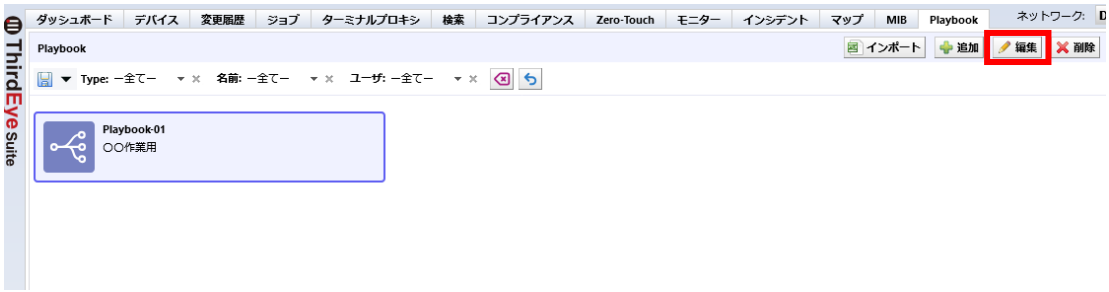
「すべてのテストが合格しました」というメッセージが表示されます。



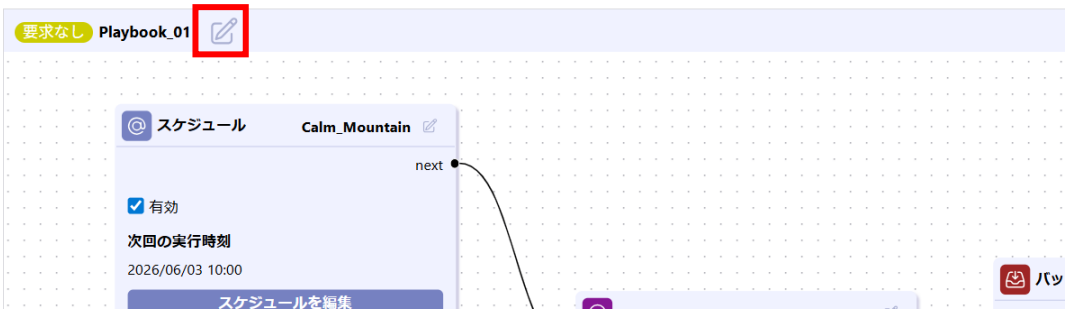
Copyright (C) 2026 LogicVein, Inc.

7.7.3.2　Playbook の編集

1. ［Playbook］タブを開きます。
2. 編集する Playbook を選択してダブルクリックするか、［編集］ボタンをクリックします。



※　［Playbook の詳細を編集する］をクリックすると、Playbook の名前や説明を編集できます。



3. 編集が完了したら、［Playbook を保存する］ボタンをクリックします。

7.7.3.3　Playbook の削除

1. ［Playbook］タブを開きます。
2. 削除する Playbook を選択し、［削除］ボタンをクリックします。

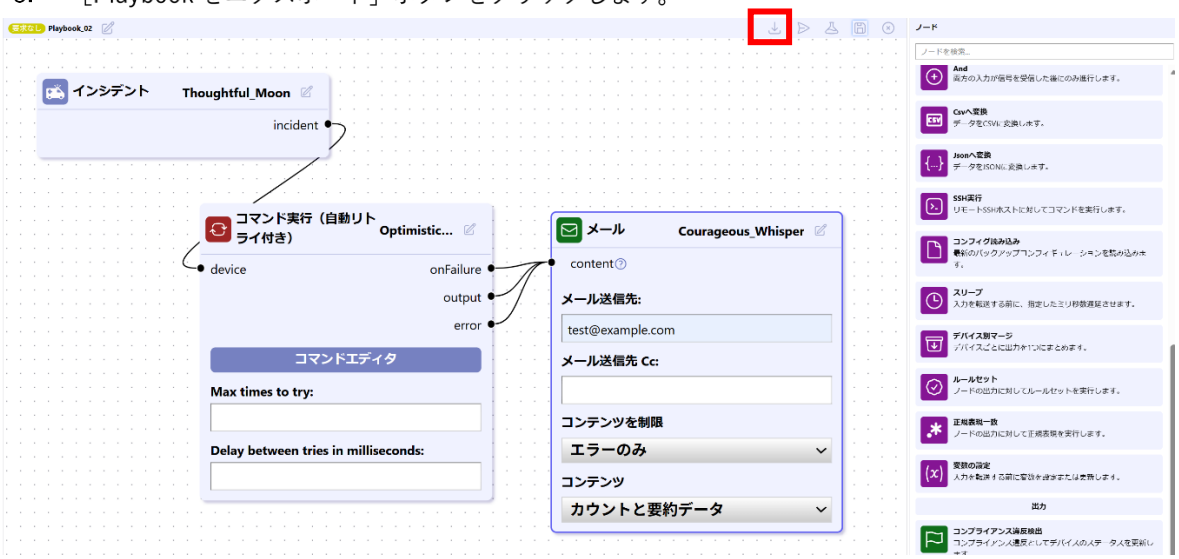
3. 確認メッセージが表示されたら、［OK］をクリックします。

4. 一覧から Playbook が削除されます。

Copyright (C) 2026 LogicVein, Inc.

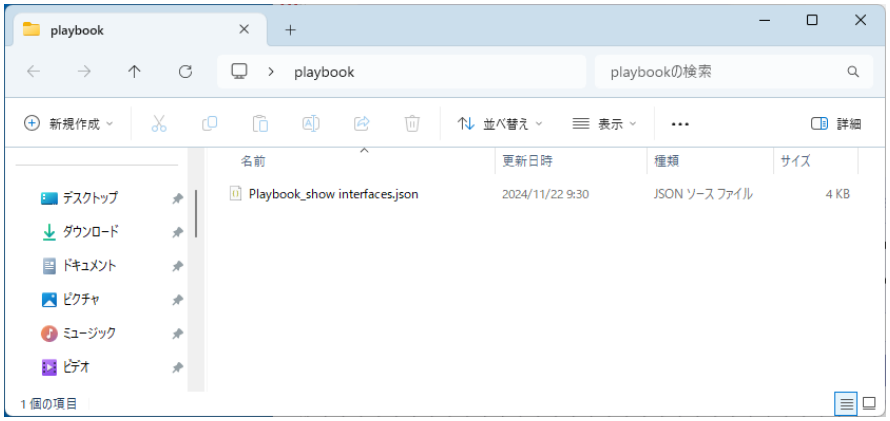
7.7.3.4　Playbook のエクスポート

1. ［Playbook］タブを開きます。
2. エクスポートする Playbook を選択してダブルクリックするか、［編集］ボタンをクリックします。
3. ［Playbook をエクスポート］ボタンをクリックします。



4. ファイルをダウンロードします。

※　ファイルは、JSON ファイル形式で出力されます。

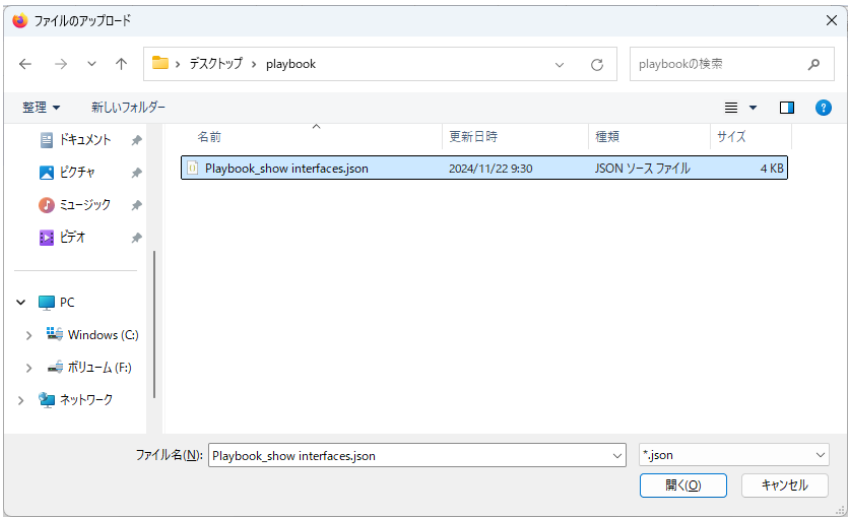


7.7.3.5　Playbook のインポート

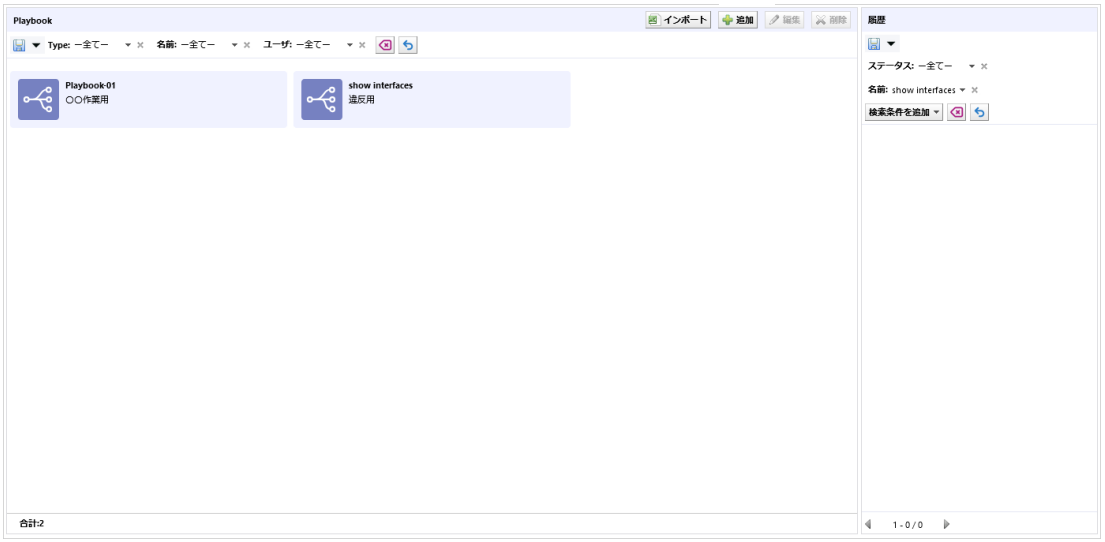
1. ［Playbook］タブを開きます。
2. ［インポート］ボタンをクリックします。

Copyright (C) 2026 LogicVein, Inc.

3. インポートするファイルを選択し、開きます。



4. インポートが完了すると、一覧に追加されます。



Copyright (C) 2026 LogicVein, Inc.

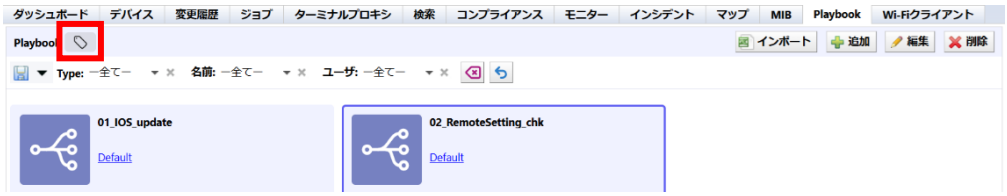
7.7.3.6　Playbook のカテゴリ

Playbook のカテゴリ機能は、Playbook を管理する際の利便性を向上させます。

- カスタムカテゴリの作成・編集
- Playbook 一覧でのカラータグによるラベル付け
- 1 つの Playbook 内での複数カテゴリ作成

(1)　Playbook カテゴリの作成

1. [Playbook] タブを開きます。
2. “Playbook”タイトルの横にある ボタンをクリックすると「カテゴリー覧」ウィンドウが開きます。



3. ボタンをクリックすると「カテゴリを追加」ウィンドウが開きます。

4. デフォルト画像 ボタンをクリックしてカテゴリ用の SVG 形式のアイコン画像を選択します。
5. カテゴリ名を入力します。
6. [OK]ボタンをクリックし、続けて[閉じる]ボタンをクリックします

(2)　Playbook カテゴリの編集

1. “Playbook”タイトルの横にある ボタンをクリックし「カテゴリー覧」ウィンドウを開きます。
2. 「カテゴリー覧」ウィンドウでカテゴリ名をクリックします。
3. ボタンをクリックし「カテゴリを編集」ウィンドウを開きます。

Copyright (C) 2026 LogicVein, Inc.

4. 編集が完了したら、[OK]をクリックします。

(3) Playbook カテゴリの削除

1. “Playbook”タイトルの横にある ボタンをクリックし「カテゴリー覧」ウィンドウを開きます。
2. 「カテゴリー覧」ウィンドウでカテゴリ名をクリックします。
3. ボタンをクリックすると「カテゴリを削除」ウィンドウが開きます。

4. [はい]をクリックします。

Copyright (C) 2026 LogicVein, Inc.

7.7.4　Playbook の実行

Playbook を実行する方法について説明します。手動での実行から、スケジュール実行やトリガー実行など、さまざまな実行方法について説明します。

Playbook は[承認機能]の対象となるため、ユーザの権限や Playbook の承認状態により[Playbook を実行する]ボタンが無効化されている場合があります。

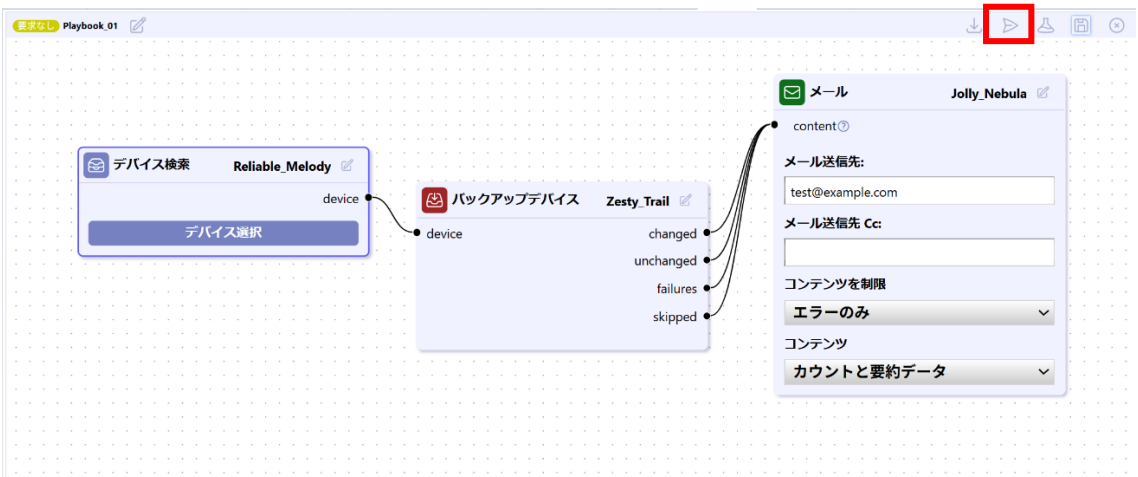
- 承認機能に関する権限は、以下の 2 つの権限内容です。

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。

7.7.4.1　手動で実行

Playbook を手動で実行する手順は以下のとおりです。

1. ［Playbook］タブを開きます。
2. 実行する Playbook を選択してダブルクリックするか、［編集］ボタンをクリックします。
3. ［Playbook を実行する］ボタンをクリックします。

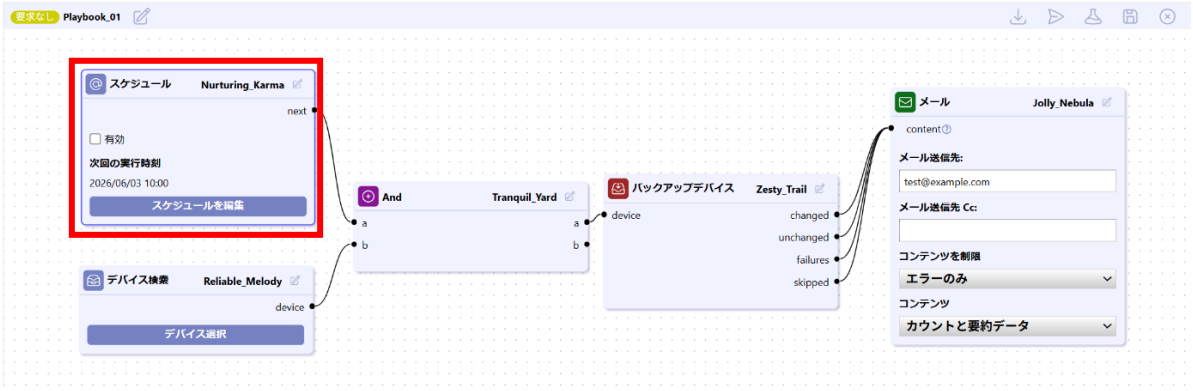


4. Playbook が実行されると、自動で実行画面に移動します。

Copyright (C) 2026 LogicVein, Inc.

7.7.4.2　スケジュール実行

スケジュールに従って Playbook を自動的に実行します。スケジュール実行を設定するには、スケジュールノードを使用します。

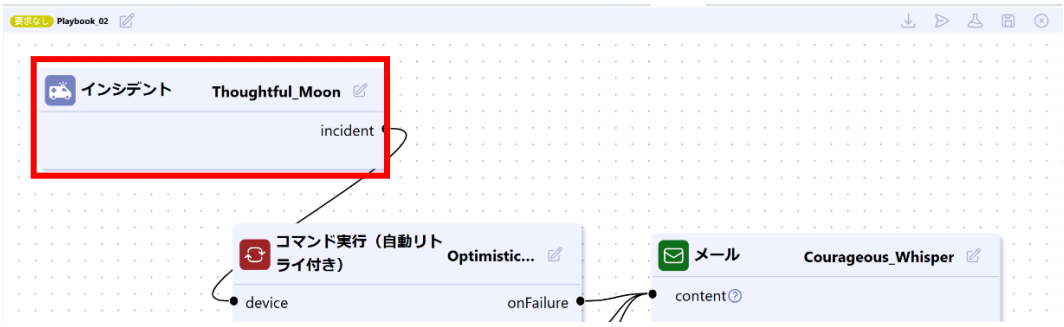


Copyright (C) 2026 LogicVein, Inc.

7.7.4.3　違反発生時に実行

違反が発生したときに Playbook を自動的に実行します。これを実行するには、インシデントノードを使用し、作成した Playbook をアラートポリシーで指定する必要があります。

1. Playbook にインシデントノードを追加します。



2. ［モニター］→［アラートポリシー］から任意のアラートポリシーに「Playbook 実行」アクションを追加します。

これにより、指定したアラートポリシーがトリガーされたときに Playbook が自動的に実行されます。

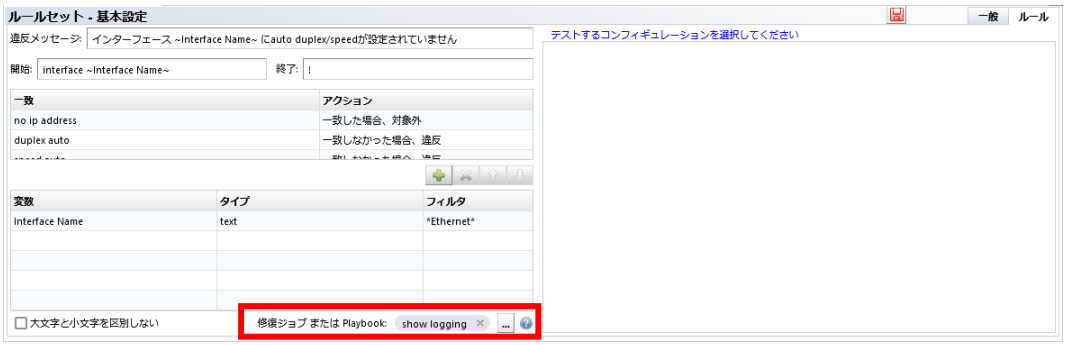
Copyright (C) 2026 LogicVein, Inc.

7.7.4.4　コンプライアンス違反検知時に実行

コンプライアンス違反を検知した際に Playbook を実行します。これを実行するには、コンプライアンスノードを使用し、作成した Playbook をコンプライアンスのルールセットに指定する必要があります。

1. Playbook にコンプライアンス違反ノードを追加します。

2. ［コンプライアンス］→［ルールセット］から任意のルールセットに「Playbook 実行」アクションを追加します。



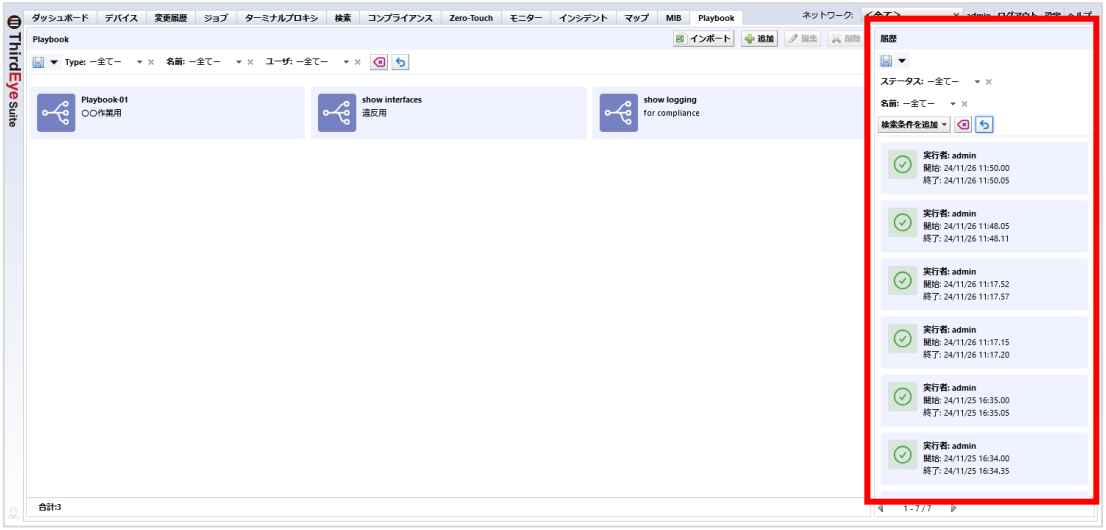
7.7.4.5　承認ログの表示

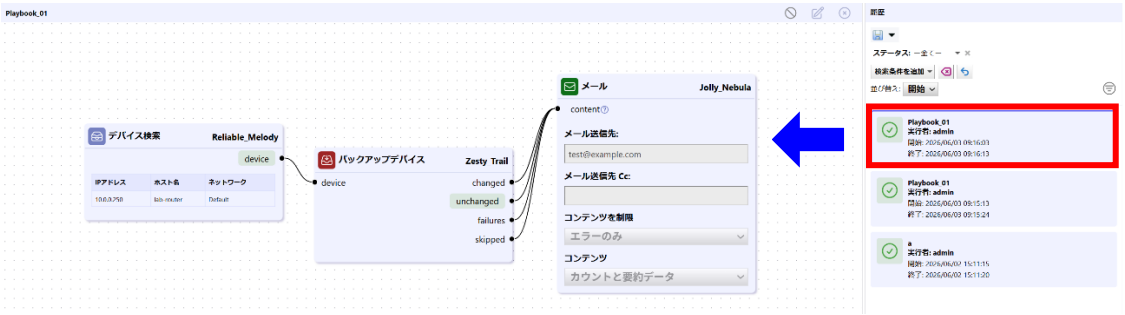
1. [Playbook]メインタブをクリックします。
2. 対象の Playbook をダブルクリックします。
3. ノードパネルの右側にある[ジョブ承認ログ] をクリックします。

Copyright (C) 2026 LogicVein, Inc.

7.7.4.6　実行履歴

Playbook の実行履歴は、画面右側に表示されます。履歴から任意の Playbook をクリックすると、詳細情報を確認できます。また、[ジョブ]メインタブの[ジョブ管理]タブからも確認することができます。



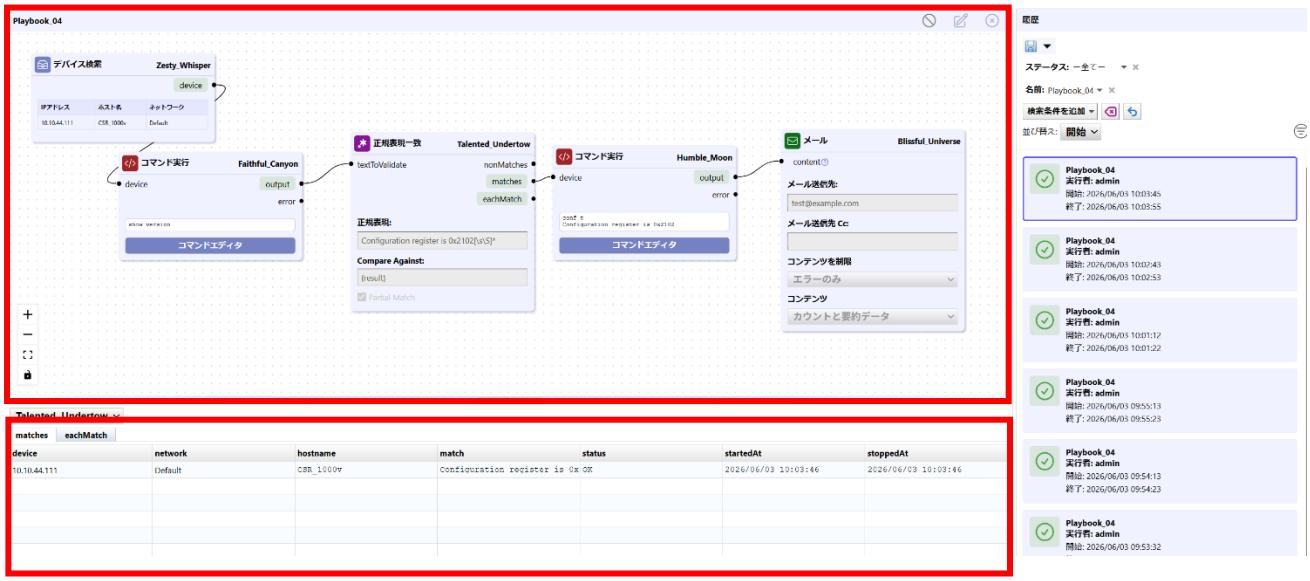


Copyright (C) 2026 LogicVein, Inc.

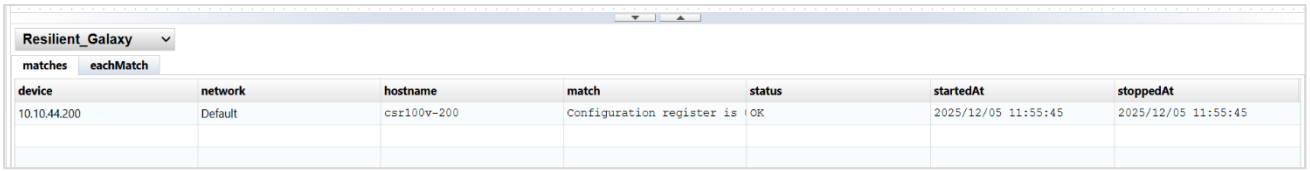
履歴確認画面は、大きく 2 つのセクションに分かれています。

画面上部では、実行時の Playbook が表示され、実行中に出力があったノードは緑色で強調表示されます。

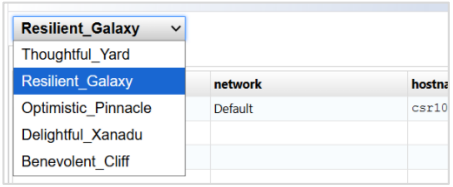
ノードをクリックすると画面下部のパネルがそのノードを出力結果に切り替わります。



画面下部のパネルでは各ノードの出力が表形式で表示されます。選択したノードに 1 つ以上の出力がある場合は、タブが複数表示され、それぞれのタブに表形式で表示されます。

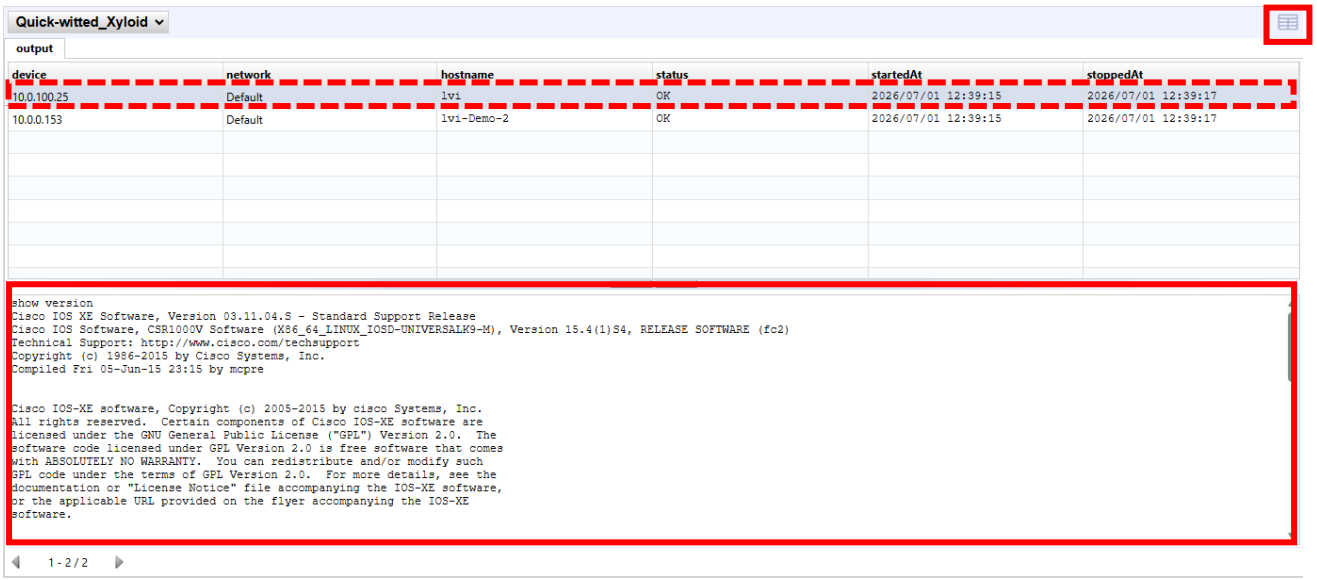


パネル上部で確認したいノードを選択表示することができます。ノードを選択すると画面上部の Playbook 画面で選択したノードが自動的にスクロールされます。

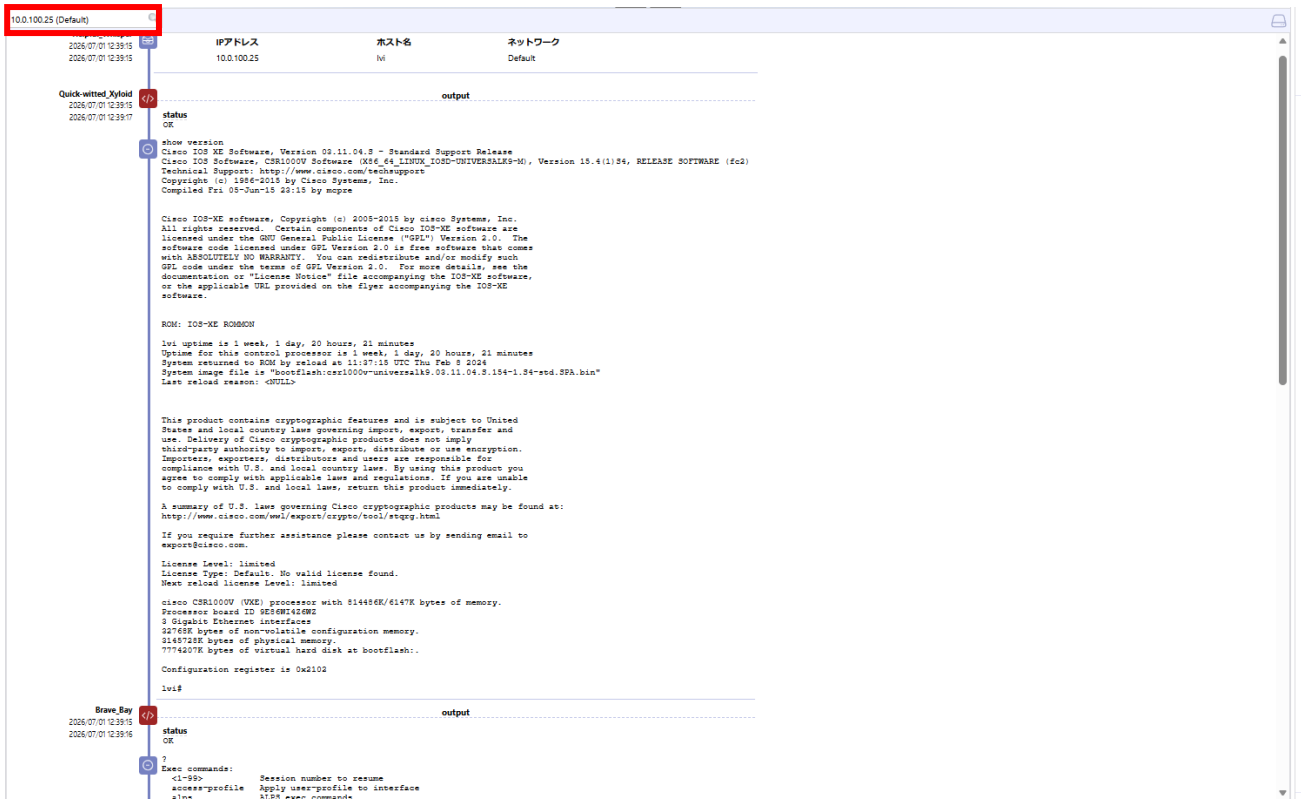


Copyright (C) 2026 LogicVein, Inc.

追加情報を持つ行を選択すると追加情報が表示するパネルが開きます。例えば、「コマンド実行」ノードの出力結果は行を選択するするとパネルが開き結果が表示されます。



をクリックする事で、出力詳細を一括で表示する事ができます。検索フィールドでデバイスの IP を設定する事で、デバイス毎に表示する事も可能です。



Copyright (C) 2026 LogicVein, Inc.

7.7.4.7　代替値の使用

多くのノードは主な結果とともにメタデータを出力します。「コマンド実行」ノードの場合、device や status などが含まれます。これらはすべて、Playbook の実行開始後にそのノードの出力テーブルで確認できます。フィールドが代替値に対応している場合、値を{中括弧}で囲むことでその値を参照できます。多くのノードでは、これらの値に対してテンプレート化された代替値をサポートしています。

ノード	設定可能フィールド
正規表現一致	正規表現と Compare Against で代替値を設定する事ができます。
コマンド実行	コマンドエディタで代替値を設定する事ができます。
コマンド実行(自動リトライつき)	コマンドエディタで代替値を設定する事ができます。
SSH 実行	コマンドで代替値を設定する事ができます。
変数の設定	値で代替値を設定する事ができます。
フィールド編集	カスタムフィールドで代替値を設定する事ができます。
ファイルアップロード	サーバからファイルを取得するコマンドで代替値を設定することができます。
コンプライアンス違反検出	メッセージで代替を設定する事ができます。

ある情報を独自のメタデータとして抽出し、ノードから列として出力したい場合、最も簡単な方法は「正規表現一致」ノードを使用することです。このノードは Java 形式の正規表現をサポートしており、名前付きマッチグループはその名前を持つ値として取り出されます。例えば Cisco デバイスの稼働時間を「uptime」という名前の値として抽出するには、`show version` コマンドの出力を、以下の正規表現を指定した正規表現一致ノードに渡します。

lab-router uptime is (?[¥w ,]+)

「Compare Against」がデフォルトの {result} に設定されている場合、この正規表現は「Compare Against」の値全体と一致するように設計されません。「Partial Match」を有効にして、正規表現の一部が少なくとも含まれていれば一致としてカウントするように指定しましょう。この設定を行うと、正規表現の一致結果には、一致した uptime が新しい「uptime」列に表示され、後続のノードで {uptime} として使用できます。

また、「Compare Against」を変更することで、これらを連鎖させてより具体的な情報を取得することも可能です。例えば、最近リセットされたスイッチを確認したい場合は、正規表現の一致条件に「day」を含めない稼働時間を確認することができます。「uptime」の正規表現マッチノードを新しい正規表現マッチノードに接続し、正規表現を day に設定します。「Compare Against」を{uptime}に設定し、「Partial Match」を有効にします。

Copyright (C) 2026 LogicVein, Inc.

その後、nonMatches の出力を確認するか、このノードを「Email」、「Webhook」、「コンプライアンス違反検出」、または「変数の設定」ノードに接続し、「デバイスが最近リセットされました：{uptime}」といったメッセージを設定することで、別の方法で結果を受け取ることができます。

Copyright (C) 2026 LogicVein, Inc.

7.7.4.8　スクリプト実行用コンテナ

Playbook のワークフローによっては、より一般的なプログラミング言語を使用した方が実装しやすい場合があります。こうしたワークフローを実現するために、以下の URL で docker イメージを提供しています。

```
harbor.logicvein.com/lvi/lvi-script-sandbox:latest
```

このイメージには Python がプリインストールされており、SSH（ポート：2022）経由で API を提供することで、よりサンドボックス化された環境でスクリプトを実行できるようにしています。イメージを pull したら、次のように実行できます。

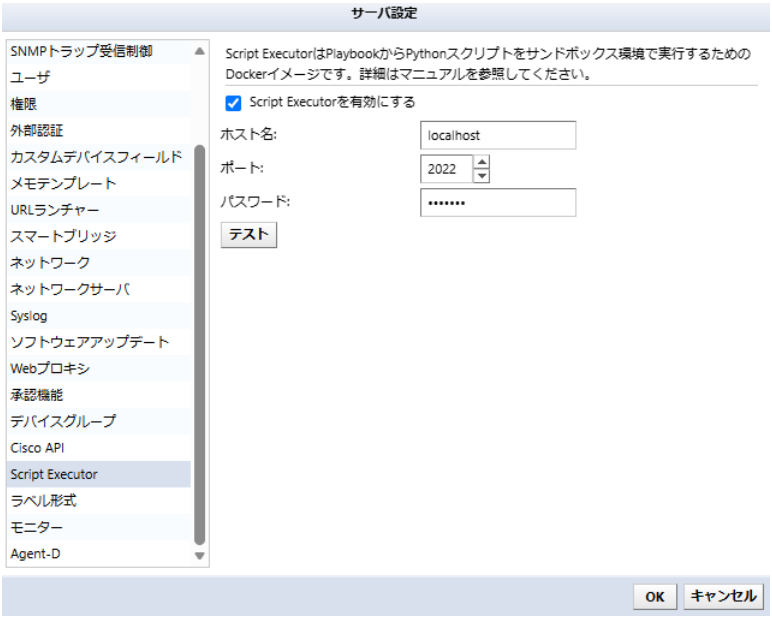
```
docker run -d ¥
  --name lvi-script-sandbox ¥
  --read-only ¥
  --tmpfs /tmp:size=1G ¥
  --cap-add=SYS_ADMIN ¥
  --security-opt no-new-privileges ¥
  -v ./scripts:/shared:ro ¥
  -v ./packages:/packages ¥
  lvi/lvi-script-sandbox:latest
```

サンドボックス環境にログインする為のデフォルトパスワードは’sandbox’です。サンドボックス環境内でログインし、いくつかのコマンドを実行する事ができます。/shared ボリュームは、ホストからファイルにアクセスできるようにするためのものです。たとえば、使用したいスクリプトのライブラリがある場合などが挙げられます。/packages ボリュームは、pip でインストールされたパッケージを保存するために使用されます。

(1)　スクリプト実行用コンテナを有効にする

サーバ設定には［Script Executor］オプションがあり、ここで実行モジュールを有効にし、ホスト名、ポート、および設定したパスワードを入力できます。実行モジュールを有効にすると、「Python スクリプトの実行」および「既存のスクリプトの実行」プレイブックノードにアクセスできるようになります。

Copyright (C) 2026 LogicVein, Inc.



(2)　スクリプト実行

「Python スクリプト実行」ノードへの各入力は、個別に Python を呼び出します。呼び出しは並行して実行され、順序やタイミングは保証されません。

Copyright (C) 2026 LogicVein, Inc.

7.8　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出来ます。

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。

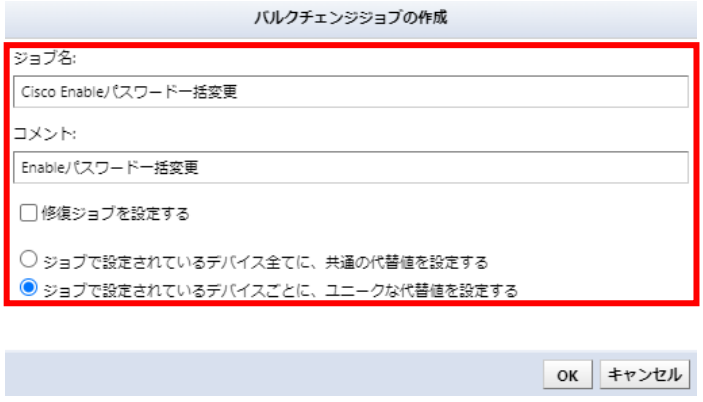
しかし、バルクチェンジを使用することで、パスワードを変数化し、それぞれのデバイスに別の値を割り振ることで、1 回のジョブで違ったパスワードで設定をすることができます。

7.8.1　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」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。

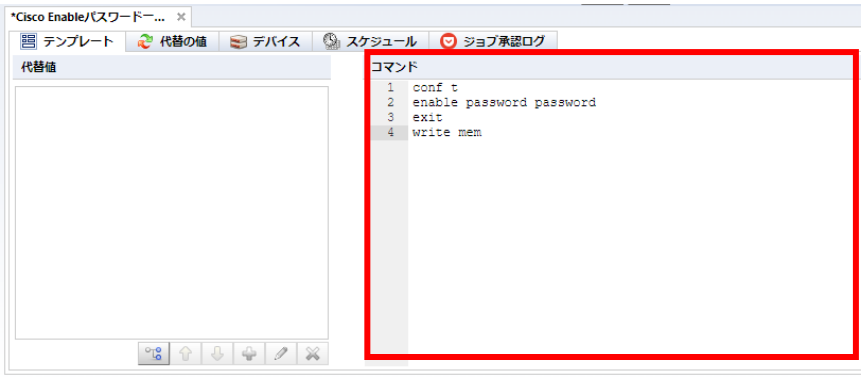


タイプ	説明
ジョブ名	バルクチェンジジョブの名前を入力します。
コメント	バルクチェンジジョブのコメント（説明）を入力します。
修復ジョブに設定する	バルクチェンジジョブを修復ジョブとして使用するかどうかを選択します。

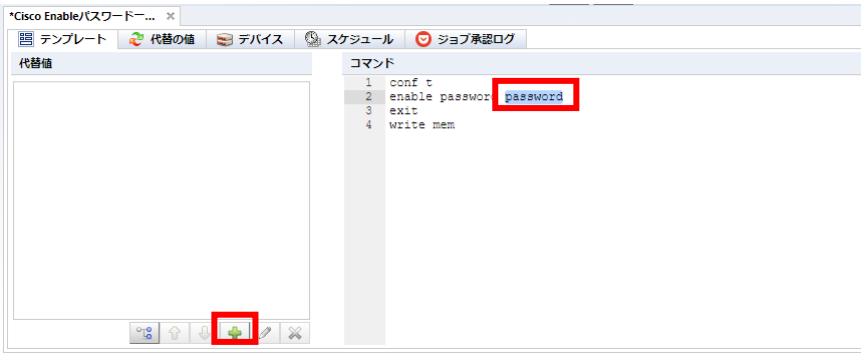
Copyright (C) 2026 LogicVein, Inc.

タイプ	説明
	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。



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。



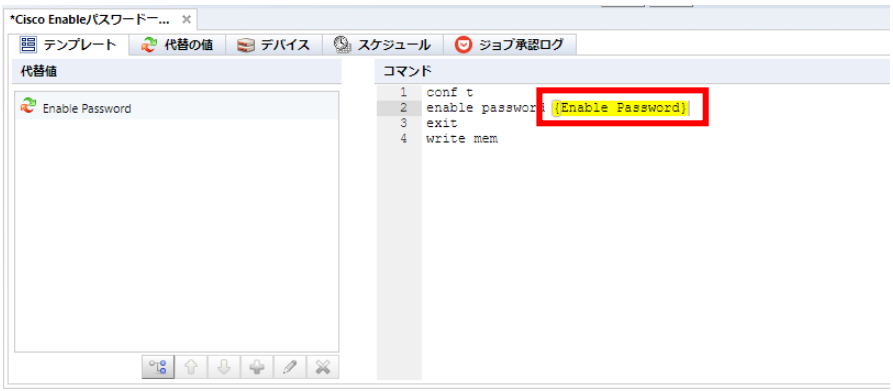
5. 代替値の名前を入力し、タイプを選択します。

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

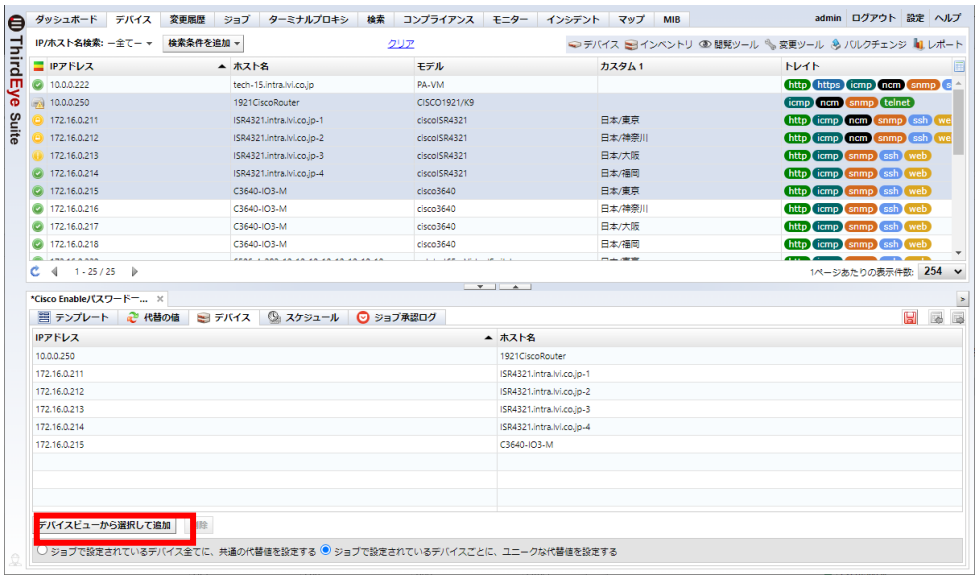
Copyright (C) 2026 LogicVein, Inc.

タイプ	説明
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で表示されます。

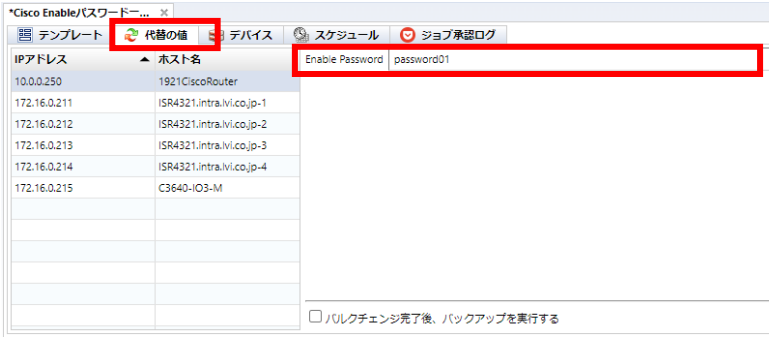


6. デバイスタブで実行するデバイスを追加します。



Copyright (C) 2026 LogicVein, Inc.

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」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。

Copyright (C) 2026 LogicVein, Inc.

7.8.2　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。

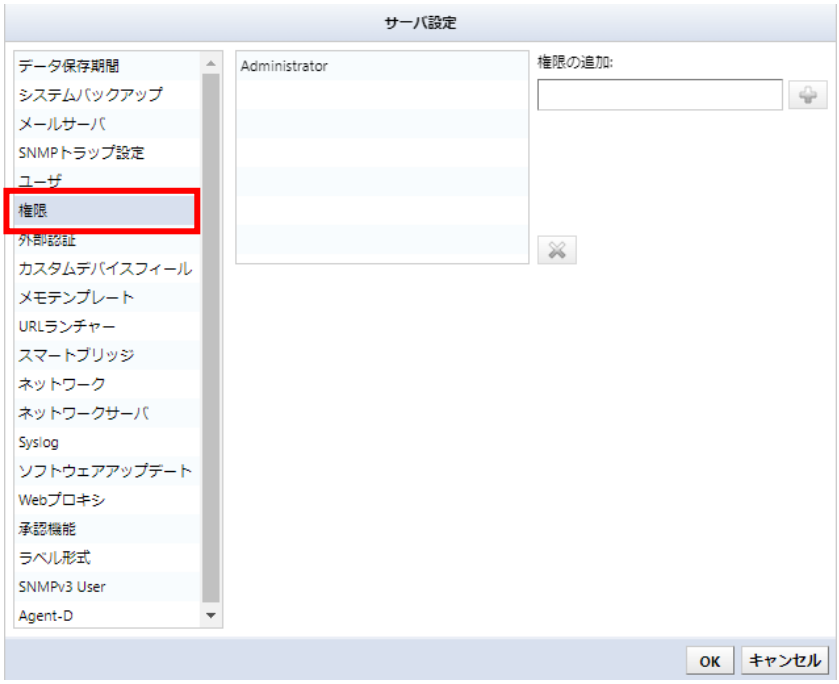
ユーザに権限を割り当てることで、実行可能な操作を制限できます。ThirdEye では、複数の権限を組み合わせて、柔軟に操作範囲を設定することが可能です。

ユーザと権限の設定は、グローバルメニューの［設定］から行えます。

7.8.2.1　権限を追加する

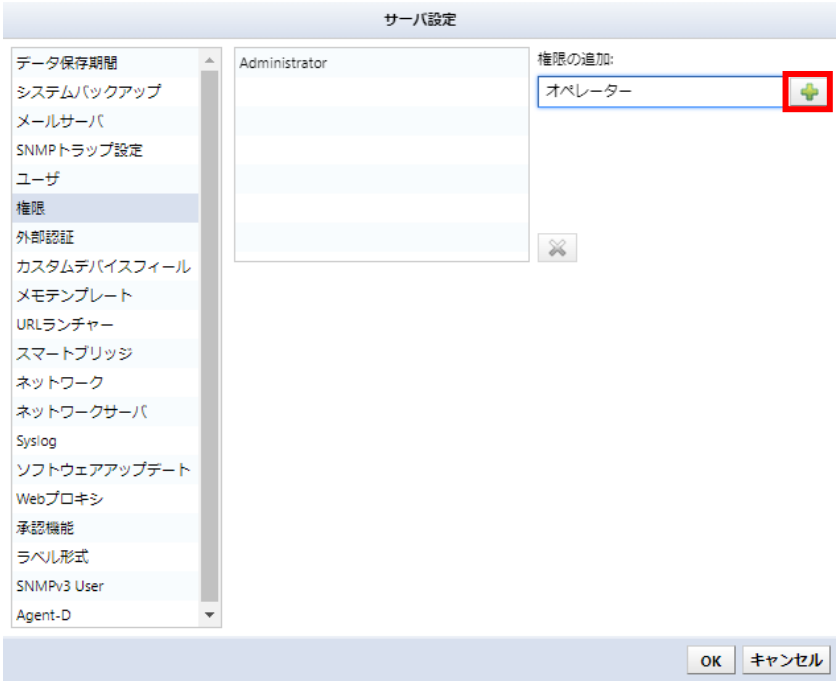
※すべての実行権限を持つ「Administrator」権限があらかじめ登録されています。「Administrator」権限は削除できません。

1. ［権限］をクリックします。

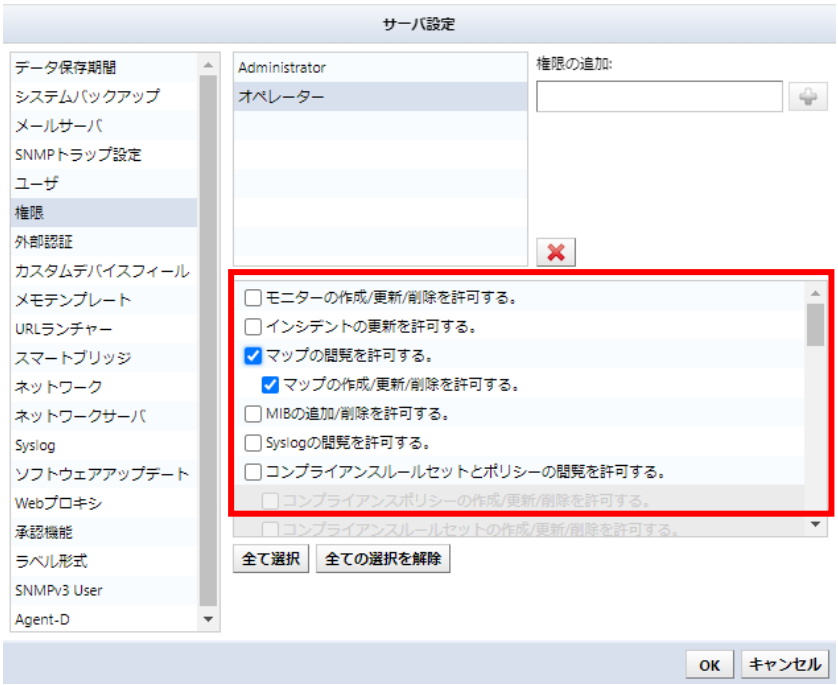


Copyright (C) 2026 LogicVein, Inc.

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、選択された状態になります。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。



Copyright (C) 2026 LogicVein, Inc.

【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。	共通	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。	共通	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。	共通	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。	共通	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。	共通	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。	共通	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。	共通	ツールを実行できます。

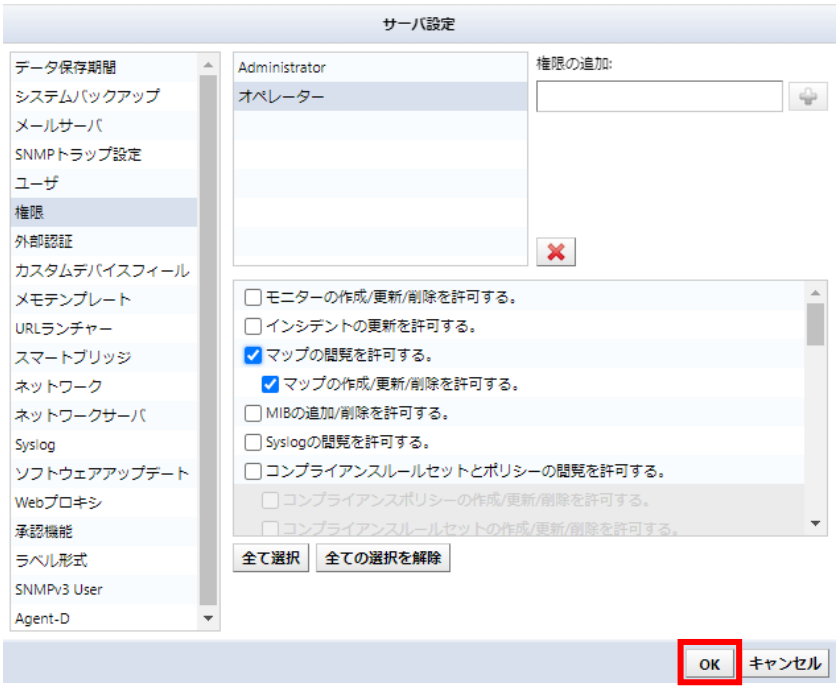
Copyright (C) 2026 LogicVein, Inc.

権限項目		説明
ツールの作成/更新/削除を許可する。	共 通	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)
ツールの実行を承認する権限。	共 通	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。	共 通	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。	共 通	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。	共 通	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。	共 通	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。	共 通	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。	共 通	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。	共 通	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。	共 通	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。
システムバックアップの実行を許可する。	共 通	システムバックアップを実行できます。
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。	共 通	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。	共 通	enable mode に直接自動ログインができます。

Copyright (C) 2026 LogicVein, Inc.

権限項目		説明
		(※「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。	共 通	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。	共 通	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。

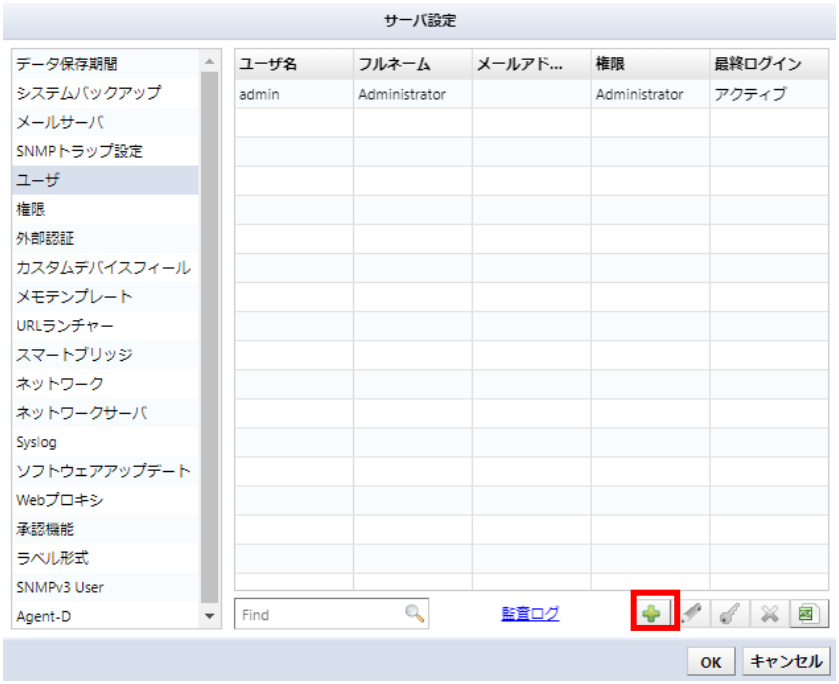


Copyright (C) 2026 LogicVein, Inc.

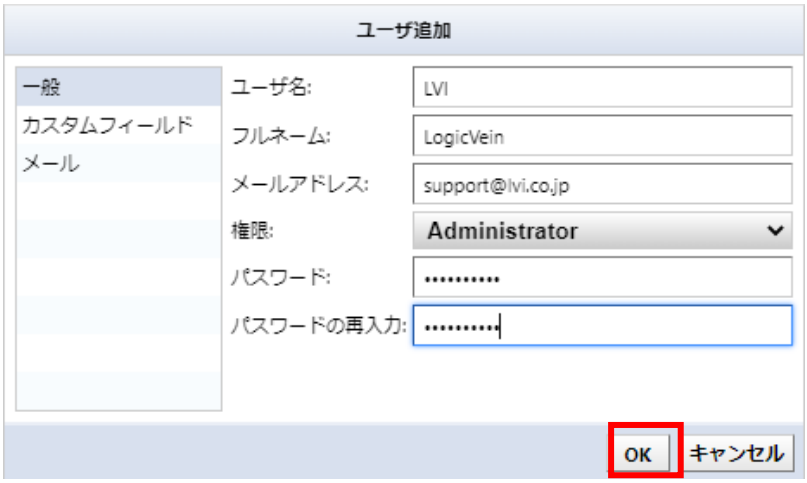
7.8.2.2　ユーザを追加する

※「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。

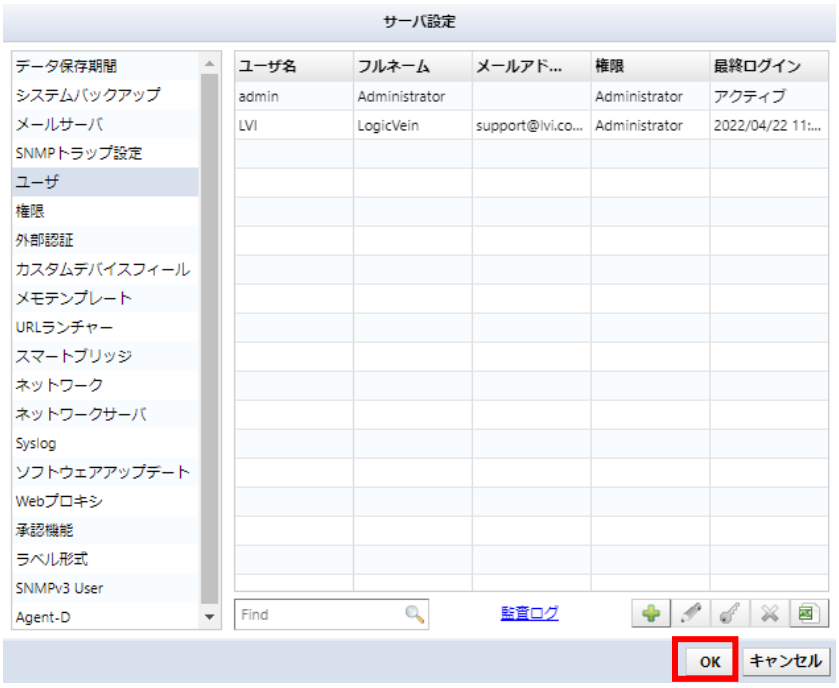


カテゴリー	項目	説明	必須
一般	ユーザ名	ユーザ名を入力します。	必須
	フルネーム	ユーザのフルネームを入力します。	—
	メールアドレス	ユーザのメールアドレスを入力します。	—
	権限	ユーザの権限を選択します。「7.8.2.1 権限を追加する」で設定した権限をプルダウンメニューから選択できます。	必須
	パスワード	ユーザのパスワードを設定します。	必須

Copyright (C) 2026 LogicVein, Inc.

カテゴリー	項目	説明	必須
		※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	
ネットワーク	ユーザのアクセスを制限します	ユーザが、システム内のすべての管理ネットワークにアクセスできるかどうかを設定します。	—
	ネットワーク	ユーザがアクセスできる管理ネットワークの一覧です。 ● 「ユーザのアクセスを以下のネットワークに制限します」にチェックが入っていない場合、この一覧は無効になり、ユーザはすべてのネットワークにアクセスできます。 ● 「ユーザのアクセスを以下のネットワークに制限します」にチェックが入っている場合、この一覧が有効になり、チェックされたネットワークのみがユーザのアクセス対象として設定されます。	—
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、「7.9.8 カスタムデバイスフィールドのカラム名変更/カラム追加」の設定に基づいて変化します。	—
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。	—

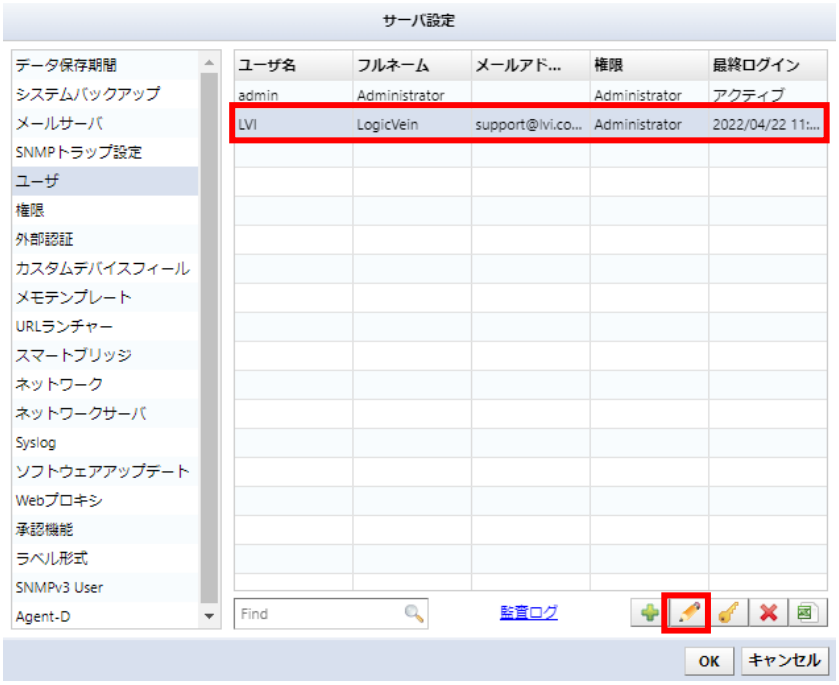
3. ［OK］をクリックします。



Copyright (C) 2026 LogicVein, Inc.

7.8.2.3　ユーザ情報を変更する

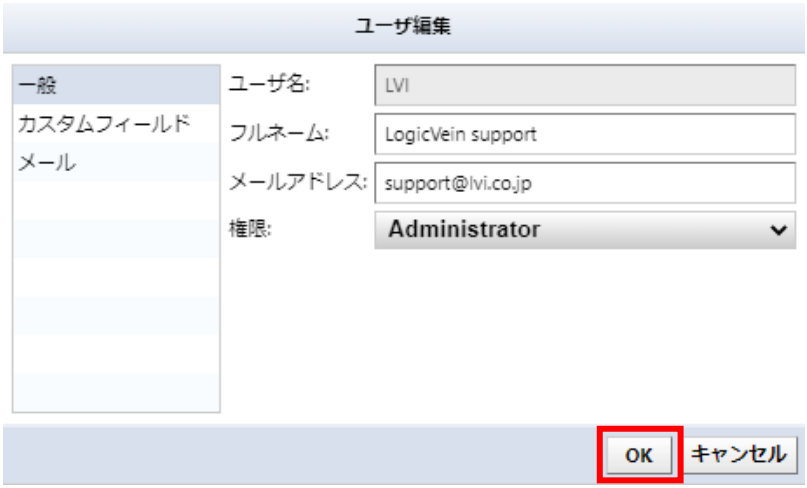
1. 編集したいユーザを選択し、［ (編集)］をクリックします。



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。

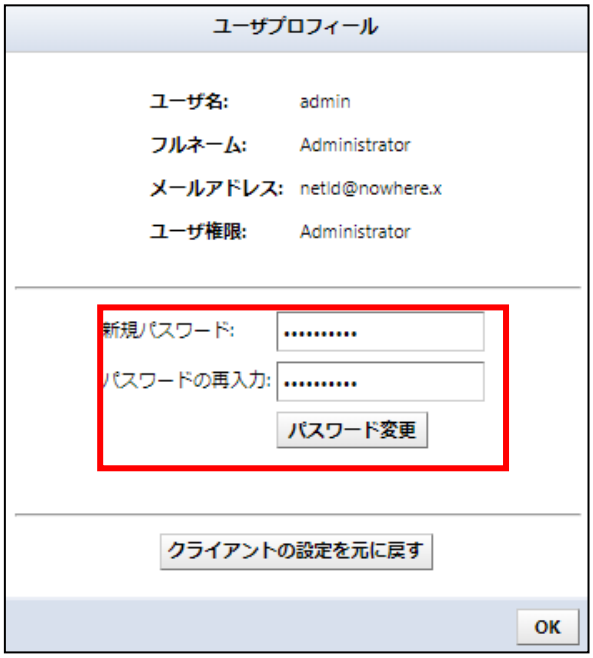


Copyright (C) 2026 LogicVein, Inc.

7.8.2.4　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。



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

Copyright (C) 2026 LogicVein, Inc.

7.8.3 二要素認証（2FA）を設定する

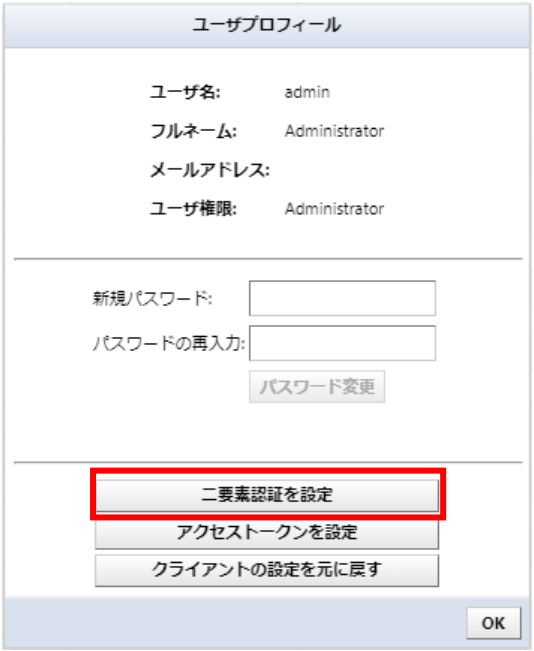
リビジョン 20240905.2154 から、二要素認証を設定できるようになりました。二要素認証は、パスワードに加えて認証アプリによる追加認証を行うことで、ユーザアカウントのセキュリティを強化する機能です。ユーザは任意で設定できるほか、管理者はすべてのユーザに対して必須に設定することもできます。

7.8.3.1 二要素認証を有効にする

ユーザがログインしている場合、［ユーザプロフィール］ダイアログから二要素認証を設定できます。

1. ユーザ名をクリックし、［ユーザプロフィール］ダイアログを開きます。

2. ［二要素認証を設定］をクリックします。



Copyright (C) 2026 LogicVein, Inc.

3. 画面上の指示に従って設定を行い、認証コードを入力します。

4. ［OK］をクリックします。

以上で設定は完了です。ログアウト後、再度ログインすると、認証コードの入力が求められるようになります。

7.8.3.2 二要素認証を解除する

二要素認証の設定を解除したい場合、ログイン中のユーザ自身で解除することができます。また、admin ユーザの場合は、すべてのユーザの二要素認証の設定を解除することができます。

1. ［設定］>［ユーザ］を開きます。
2. 対象のユーザを選択し、［鍵］ボタンをクリックします。
3. ［二要素認証を解除する］にチェックを入れ、［OK］をクリックします。
   ※ 二要素認証が設定されていない場合は、「このユーザには二要素認証が設定されていません」と表示され、このチェックボックスオプションは表示されません。
4. ［サーバ設定］ダイアログで［OK］をクリックします。

Copyright (C) 2026 LogicVein, Inc.

7.8.3.3　外部認証を構成する

外部認証を設定すると、認証サーバを使用してシステムにログインできるようになります。これにより、すべてのユーザアカウントを事前にシステム上で作成しておく必要がなくなります。また、認証サーバからグループ情報を取得することで、ユーザに権限や管理ネットワークの制限を自動的に割り当てることができます。

外部認証は、［サーバ設定］ダイアログ内の［外部認証］ページで設定します。このページでは、プロトコル固有の設定に加え、グループマッピングも設定できます。これにより、システムがユーザにどの権限を割り当て、どの管理ネットワークにアクセスを許可するかを指定できます。グループマッピングは、外部認証プロバイダ側の「グループ」と、システム側の権限や管理ネットワークに関連付けることで実現されます。

(i)　RADIUS 連携

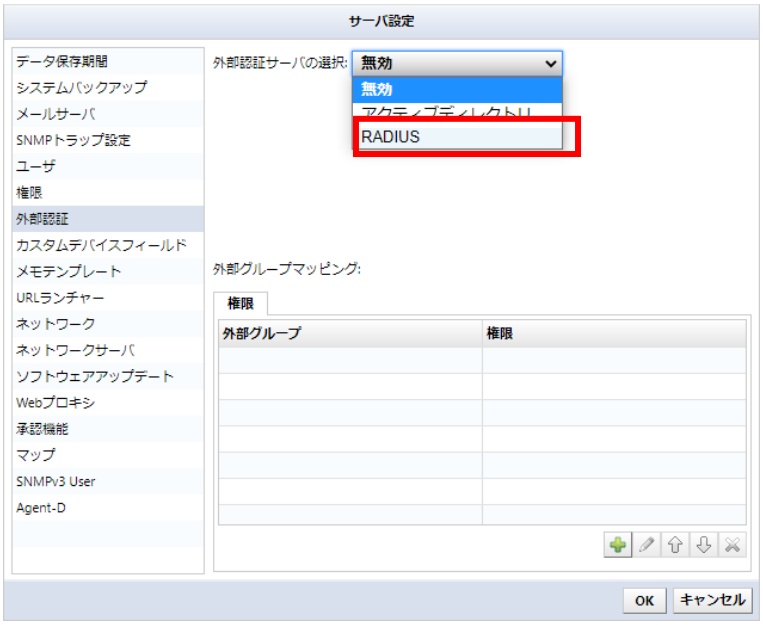
RADIUS 認証を利用する場合、RADIUS サーバに Access-Request を送信して認証を行います。RADIUS サーバと連携するには、Access-Accept 応答に Filter-Id を含めて返すように設定する必要があります。

以下は、FreeRADIUS でユーザにグループ情報（Filter-Id）を付与する設定のサンプルです。

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

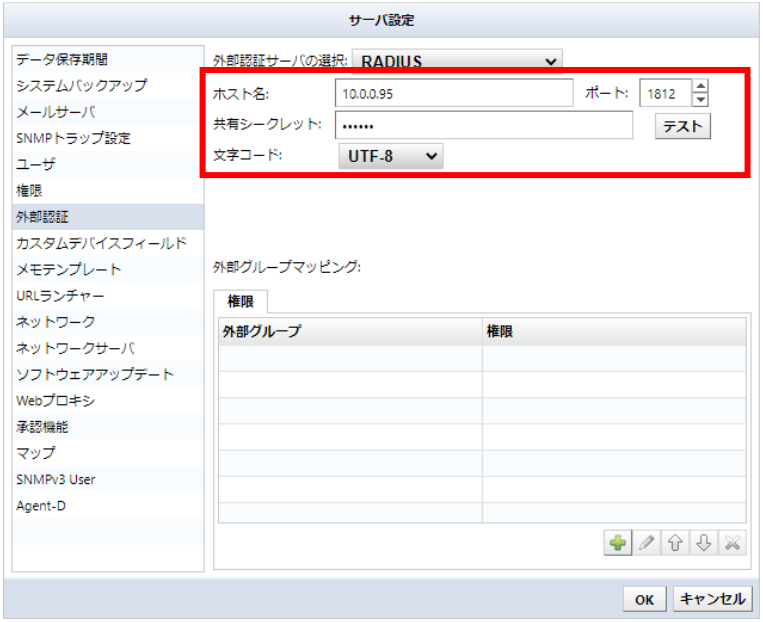
この設定では、「ユーザ名：LogicVein」「パスワード：password」で送信された Access-Request に対し、認証に成功すると Filter-Id 属性を含む Access-Accept 応答が返されます。
Filter-Id は、認証されたユーザが所属するグループを示す情報として扱われます。

1. ［外部認証サーバの選択］を「RADIUS」に変更します。



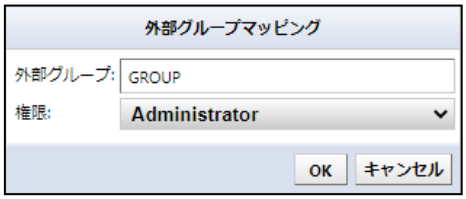
Copyright (C) 2026 LogicVein, Inc.

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。



3. 外部グループマッピングの権限を設定します。［+(追加)］をクリックします。

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。



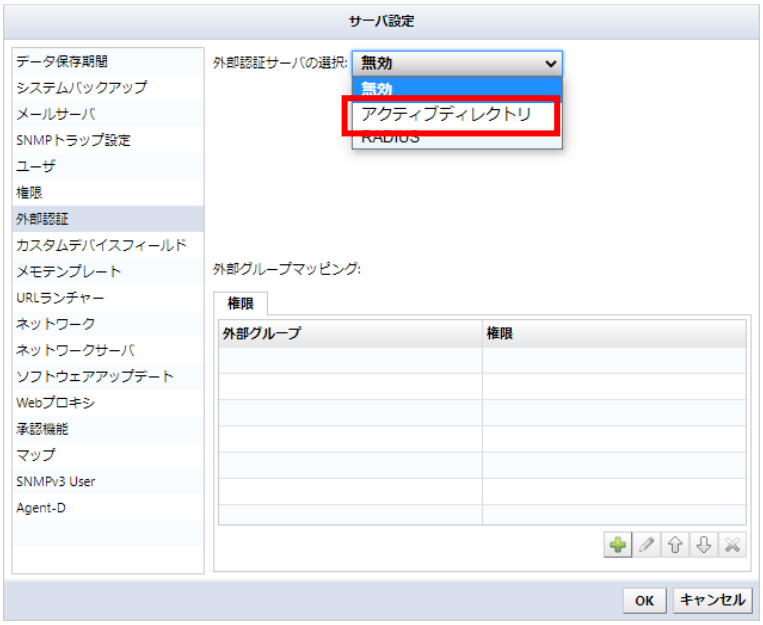
設定が完了したら、［OK］をクリックして保存し、RADIUS サーバに登録されたユーザでログインを確認します。

Copyright (C) 2026 LogicVein, Inc.

(ii)　Active Directory 連携

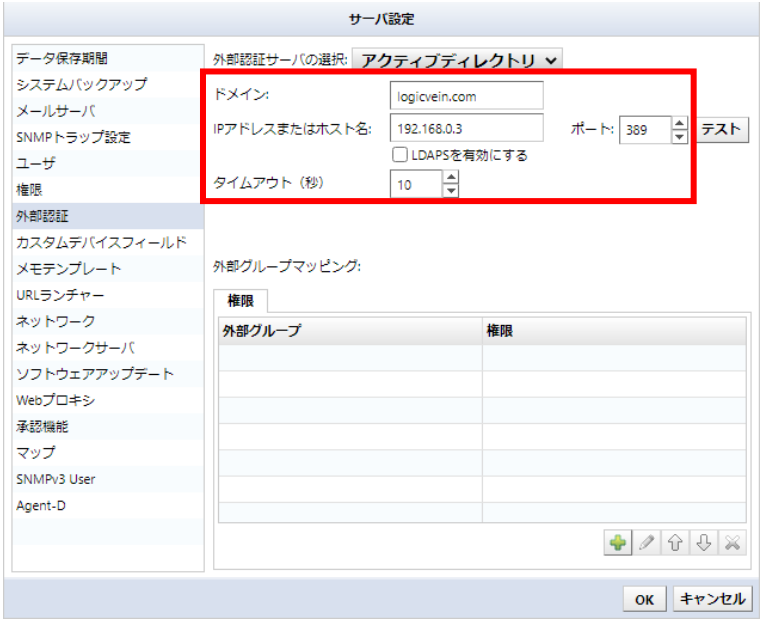
Active Directory と連携することで、ユーザが所属するグループ情報をもとに、システム上での権限およびアクセス可能なネットワークを自動的に割り当てることができます。

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。



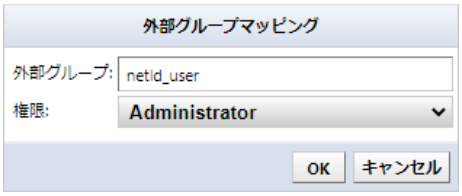
Copyright (C) 2026 LogicVein, Inc.

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。



3. 外部グループマッピングの権限を設定します。［+(追加)］をクリックします。

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。



設定が完了したら、［OK］をクリックして保存し、Active Directory に登録されているユーザでログインを確認します。

Copyright (C) 2026 LogicVein, Inc.

(iii) SAML 連携

外部認証サービス（IdP）と連携した SAML 認証を構成することで、シングルサインオン（SSO）を実現できます。これにより、ユーザは IdP 経由で ThirdEye にシームレスにログインできるようになります。

Microsoft Entra ID 連携

【前提条件】

シングルサインオンを構成する前に、以下の条件を満たしていることを確認してください。

- 管理者権限で Microsoft Entra ID にサインインできること
- Microsoft Entra ID に連携対象のユーザおよびグループが存在すること
- ThirdEye で設定を構成する権限(※)を持っていること
  - （※) Administrator 権限 または 「セキュリティの設定を許可する。」を有する権限

【手順】

ThirdEye で SAML を構成する

1. ThirdEye にログインします。
2. ［設定］>［外部認証］を開きます。
3. ［外部認証サーバの選択］から「SAML」を選択します。
4. ［コールバック URL］が ThirdEye サーバの正しい URL であることを確認します。
   ※ コールバック URL の形式： https://[IP アドレスまたはホスト名]/auth
   ※ デフォルトでは、［ネットワークサーバ］>［パブリック ホスト名/IP アドレス］の値を参照します。
5. ［SP メタデータ XML をダウンロード］リンクをクリックして、SP メタデータ XML ファイルをダウンロードします。
   ※ ファイル名: LogicVein-saml-sp-metadata.xml
   ※ ダウンロードしたファイルは、次の手順で利用します。

新しいアプリケーションを作成

1. 「Microsoft Entra 管理センター」にサインインします。
2. ［ID］>［アプリケーション］>［エンタープライズ アプリケーション］を開きます。
3. ［新しいアプリケーション］メニューをクリックします。
4. ［独自のアプリケーションの作成］メニューをクリックします。
5. アプリの名前を設定し、［ギャラリーに見つからないその他のアプリケーションを統合します（ギャラリー以外)］を選択し、［作成］をクリックします。
6. ［管理］>［シングル サインオン］を選択します。
7. ［シングル サインオン方式の選択］ページで、［SAML］を選択します。
8. ［SAML によるシングル サインオンのセットアップ］で、［メタデータ ファイルをアップロードする］をクリックし、先の手順でダウンロードした「LogicVein-saml-sp-metadata.xml」をアップロードし、［追加］をクリックします。
9. ［保存］をクリックします。

Copyright (C) 2026 LogicVein, Inc.

10. ［×］をクリックして編集画面を閉じます。
    ※　［シングル サインオンを Test］のポップアップメッセージが表示された場合、「いいえ、後で test します」をクリックします。
11. ［属性とクレーム］セクションで［編集］をクリックします。
12. ［属性とクレーム］ページで、［グループ要求を追加する］を選択します。
13. ［セキュリティグループ］オプションを選択し、［ソース属性］で「グループ ID」を選択します。
14. ［保存］をクリックします。
15. ［×］をクリックして［属性とクレーム］ページを閉じます。

IdP メタデータを取得

1. ［SAML 証明書］セクションで、［フェデレーション メタデータ XML］の［ダウンロード］をクリックします。
2. IdP メタデータ XML ファイルをダウンロードします。

ThirdEye にアプリケーションを登録

1. ThirdEye の［設定］>［外部認証］を開きます。
2. ［IdP メタデータ XML をアップロード］をクリックし、手順「0 IdP メタデータを取得」で作成した XML ファイルを選択します。
3. ［OK］をクリックし、［サーバ設定］を保存します。

オブジェクト ID をメモ

1. 「Microsoft Entra 管理センター」に戻り、［管理］>［ユーザーとグループ］をクリックします。
2. ［ユーザーまたはグループの追加］をクリックします。
3. ［ユーザー］セクションの［選択されていません］をクリックします。
4. 一覧から、ThirdEye へのログインを許可する必要があるユーザを選択します。
5. ［選択］をクリックします。
6. ［割り当て］をクリックして、ユーザーの割り当てを完了します。
7. 左側のペインで［ID］>［グループ］>［すべてのグループ］に移動します。
8. ThirdEye へのログインを許可するグループの［オブジェクト ID］をメモします。

外部グループマッピングを構成する

1. ［設定］>［外部認証］を開きます。
2. ［外部グループマッピング］で、［+］をクリックします。
3. ［外部グループ］フィールドに、先の手順でメモした「オブジェクト ID」を入力し、［権限］に割り当てる権限を指定して、［OK］をクリックします。
4. ［OK］をクリックし、［サーバ設定］を保存します。
5. ThirdEye のログアウトをクリックします。Microsoft のログインページに移動します。

Copyright (C) 2026 LogicVein, Inc.

Okta 連携

【前提条件】

シングルサインオンを構成する前に、以下の条件を満たしていることを確認してください。

- 管理者権限で Okta ダッシュボードにサインインできること
- Okta に連携対象のユーザおよびグループが存在すること
- ThirdEye で設定を構成する権限(※)を持っていること
  - (※) Administrator 権限 または 「セキュリティの設定を許可する。」を有する権限

【手順】

ThirdEye で SAML を構成する

1. ThirdEye にログインします。
2. ［設定］＞［外部認証］を開きます。
3. ［外部認証サーバの選択］から「SAML」を選択します。
4. ［コールバック URL］がサーバの正しい URL であることを確認します。
   ※ デフォルトでは、［ネットワークサーバ］＞［パブリック ホスト名/IP アドレス］の値を参照します。
5. ［SP 証明書をダウンロード］リンクをクリックして、SP 証明書ファイルをダウンロードします。
   ※ ファイル名: LogicVein-saml-sp-signing-certificate.crt
   ※ ダウンロードしたファイルは、次の手順で利用します。

Copyright (C) 2026 LogicVein, Inc.

新しいアプリケーションを作成

1. Okta Admin Console で、［Applications］＞［Applications］に移動します。
2. ［Create App Integration］をクリックします。
3. ［Sign-in method］として［SAML 2.0］を選択し、［Next］をクリックします。
4. ［App name］に任意の名前を入力し、［Next］をクリックします。
5. ［SAML Settings］の［General］セクションで、以下の項目を設定します。

項目	設定
Single sign-on URL	https://[IP アドレスまたはホスト名]/auth?client_name=SAML2Client
Audience URI (SP Entity ID)	https://[IP アドレスまたはホスト名]/auth
Application username	メール
Update application username on	作成・更新

6. ［Show Advanced Settings］をクリックします。
7. ［Signature Certificate］で［Browse files...］をクリックし、先の手順で ThirdEye からダウンロードした SP 証明書を選択します。

   ※　ファイル名: LogicVein-saml-sp-signing-certificate.crt
8. 以下の項目を設定します。

項目	設定
Enable Single Logout	有効 「Allow application to initiate Single Logout」オプションにチェックを入れる
Single Logout URL	https://[IP アドレスまたはホスト名]
SP Issuer	https://[IP アドレスまたはホスト名]/auth

9. ［Attribute Statements (optional)］セクションで、次の 2 つの項目を追加します。

   ※　1)

Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
Name format	URI 参照
Value	user.email

   ※　2)

Name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
Name format	URI 参照
Value	user.lastName

10. ［Group Attribute Statements (optional)］セクションで、次のように設定します。

Name	http://schemas.logicvein.com/ws/2024/05/identity/claims/groups
Name format	URI 参照
Filter	正規表現と一致
	.*

Copyright (C) 2026 LogicVein, Inc.

11. ［Next］をクリックします。
12. 「I'm an Okta customer adding an internal app」を選択します。
13. 「It's required to contact the vendor to enable SAML」を選択します。
14. ［Finish］をクリックします。

アプリケーションを利用するグループを割り当て

1. アプリケーションの［Assignments］タブを選択します。
2. ［Assign］>［Assign to Groups］を選択します。
3. 割り当てるグループを見つけて、［Assign］ボタンをクリックします。
4. ［Done］をクリックします。

IdP メタデータを取得

1. ［Sign On］タブを選択します。
2. ［Settings］で［Metadata URL］の URL をコピーします。
3. ブラウザの新しいタブを開き、アドレスバーに URL を貼り付けてアクセスします。
4. メタデータページを右クリックし、［名前を付けて保存...］を選択します。
   ※ メタデータを .xml ファイル として保存します。
   ※ ダウンロードしたファイルは、次の手順で利用します。

ThirdEye にアプリケーションを登録

1. ThirdEye の［設定］>［外部認証］を開きます。
2. ［IdP メタデータ XML をアップロード］をクリックし、手順「0 IdP メタデータを取得」で作成した XML ファイルを選択します。

外部グループマッピングを構成する

1. ［設定］>［外部認証］を開きます。
2. ［外部グループマッピング］で、［+］をクリックします。
3. ［外部グループ］フィールドに Okta グループ を入力し、［権限］に割り当てる権限を指定して［OK］をクリックします。
4. ［OK］をクリックします。

ThirdEye にログイン

Okta のユーザで ThirdEye にログインします。

「0 Okta 連携」に記載された設定が完了後、ThirdEye にアクセスすると Okta のサインオン画面が表示されます。

keycloak 連携

【前提条件】

シングルサインオンを構成する前に、以下の条件を満たしていることを確認してください。

Copyright (C) 2026 LogicVein, Inc.

- 管理者権限で keycloak ダッシュボードにサインインできること
- keycloak に連携対象のユーザおよびグループが存在すること
- ThirdEye で設定を構成する権限(※)を持っていること

・ (※) Administrator 権限 または 「セキュリティの設定を許可する。」を有する権限

【手順】

ThirdEye で SAML を構成する

1. ［設定］>［外部認証］を開きます。
2. ［外部認証サーバの選択］から「SAML」を選択します。
3. コールバック URL が正しいことを確認します。

※デフォルトでは、［ネットワークサーバ］>［パブリック ホスト名/IP アドレス］の値を参照します。

4. ［SP 証明書をダウンロード］リンクをクリックして、SP 証明書ファイルをダウンロードします。

※ファイル名: LogicVein-saml-sp-signing-certificate.crt

※ダウンロードしたファイルは、次の手順で利用します。

Docker で keycloak を設定する

1. Keycloak にログインする際には、KEYCLOAK_ADMIN と KEYCLOAK_ADMIN を使用します。
2. 以下のコマンドを使用して、Keycloak ログ取得とデバッグを行います。
   docker logs -f keycloak
3. https://localhost:8080 に接続します。
4. [Client] > ［Create Client］を選択します。
5. Client ID と Name を入力します。Client ID: https:// IP アドレスまたはホスト名/auth　Name:任意の名前
   [Next]をクリックし、コールバック URL を設定します。例. https:// IP アドレスまたはホスト名
   /auth?client_name=SAML2Client
6. [Save]をクリックします。
7. [Client Scope]タブをクリックします。
8. [https:// IP アドレスまたはホスト名/auth-dedicated]をクリックします。
9. [Add predefined mapper]をクリックします。
10. [X500 email]を選択し[Add]をクリックします。
11. X500 email をクリックします。
12. [SAML Attribute Name]に http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress を設定します。
13. [SAML Attribute NameFormat]を“URI Reference”に設定します。
14. [Save]をクリックします。
15. 左サイドバーにある[Client scopes]をクリックし、“Name”カラムにある[role list]をクリックします。
16. [Mappers]タブをクリックし“Name”カラムにある[role list]をクリックします。
17. “Role attribute name”に http://schemas.logicvein.com/ws/2024/05/identity/claims/groups を設定します。

Copyright (C) 2026 LogicVein, Inc.

18. “SAML Attribute NameFormat”を“URI Reference”に設定します。
19. [Save]をクリックします。
20. 左サイドバーにある[Users]をクリックします。
21. “Username”カラムにある[admin]をクリックし、メールアドレスを設定します。
22. [Save]をクリックします。
23. 左サイドバーにある[Clients]をクリックし、client list にある[https:// IP アドレスまたはホスト名/auth]をクリックします。
24. [Advanced]タブをクリックします。
25. Logout Service POST Binding URL を“https:// IP アドレスまたはホスト名/”に設定します。
26. [Keys]タブをクリックします。
27. “Client signature required”を OFF にし、再度 ON にします。
28. ポップアップウィンドウで[Import]を選択します。
29. “Archive format“を“Certificate PEM”に設定します。
30. LogicVein-saml-sp-signing-certificate.crt をアップロードします。(※)
31. [Confirm]をクリックします。
32. 左サイドバーにある[Realm Settings]をクリックし、“SAML 2.0 Identity Provider Metadata”をダウンロードします。

※新しい Keycloak のバージョン(keycloak: 26.2.0)では証明書のアップロードに失敗します。keycloak:25.0.6-0 では動作する事を確認しております。

ThirdEye にアプリケーションを登録

1. ThirdEye の［設定］>［外部認証］を開きます。
2. ［IdP メタデータ XML をアップロード］をクリックし、作成した XML ファイルを選択します。

外部グループマッピングを構成する

1. ThirdEye の［設定］>［外部認証］を開きます。
2. ［外部グループマッピング］で、［+］をクリックします。
3. ［外部グループ］フィールドに keycloak グループ を入力し、［権限］に割り当てる権限を指定して［OK］をクリックします。
4. ［OK］をクリックします。

ThirdEye にログイン

keycloak のユーザで ThirdEye にログインします。

ThirdEye にアクセスすると keycloak のサインオン画面が表示されます。

(iv) ローカル認証を使用する方法（SAML 認証設定後）

SAML 認証の設定完了後、ThirdEye の製品ページにアクセスすると、連携先のサインインページが表示されます。SAML 認証ではなく、ローカル認証を使用して製品にログインする場合は、URL の末尾に「/?forceLoginPage=true」を

Copyright (C) 2026 LogicVein, Inc.

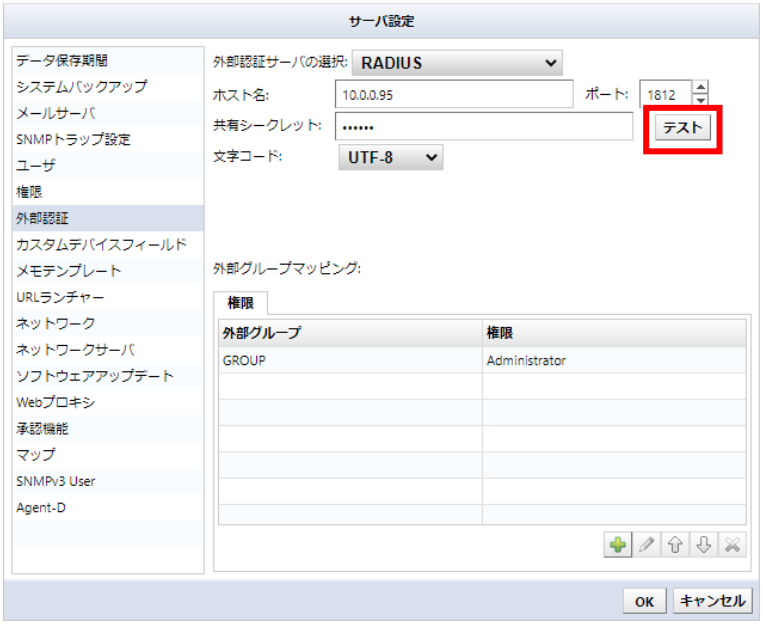
追加してアクセスしてください。

```
https://[IP アドレスまたはホスト名]/?forceLoginPage=true
```

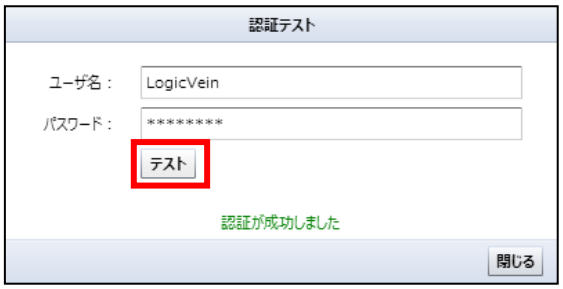
この URL を開くことで、製品のログインページが表示されます。admin などのローカルアカウントを使用してログインできます。

(v)　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。



［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。



Copyright (C) 2026 LogicVein, Inc.

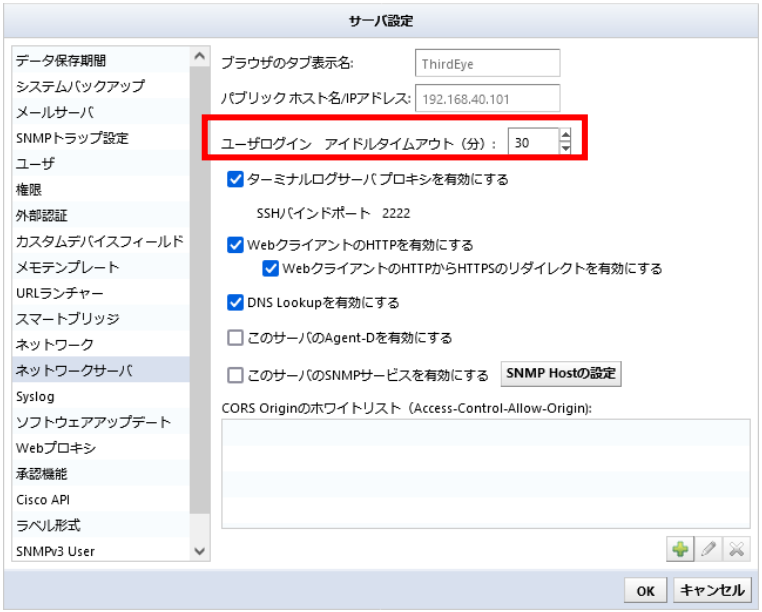
7.8.3.4　ユーザのセッションタイムアウトを設定する

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）



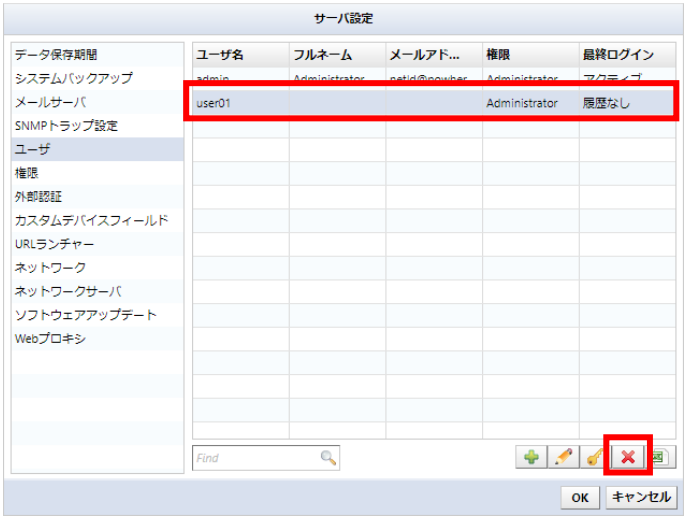
3. ［OK］をクリックします。
4. ログアウトして、再度ログインします。

※　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。

Copyright (C) 2026 LogicVein, Inc.

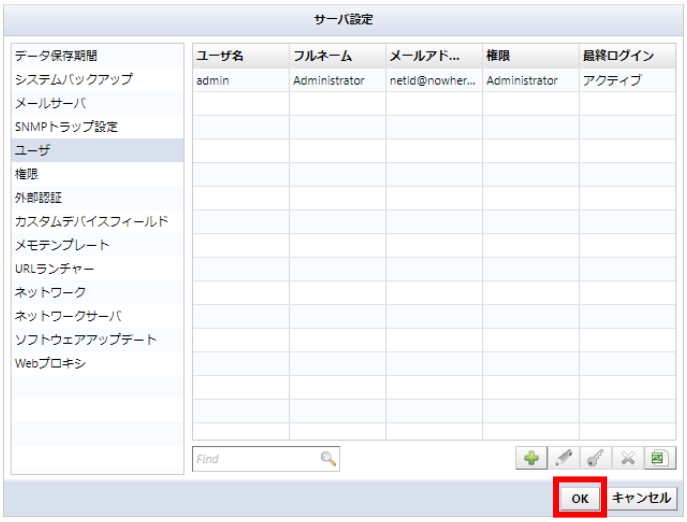
(1)　ユーザを削除する

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。

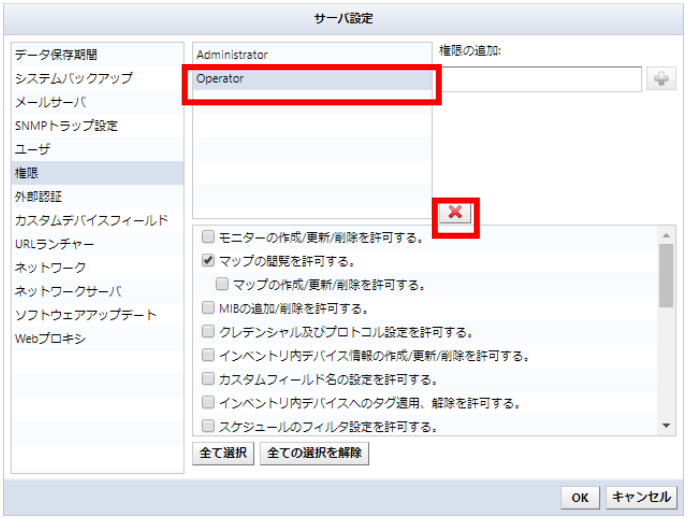
※　誤ってユーザを削除した場合は、［キャンセル］をクリックしてください。



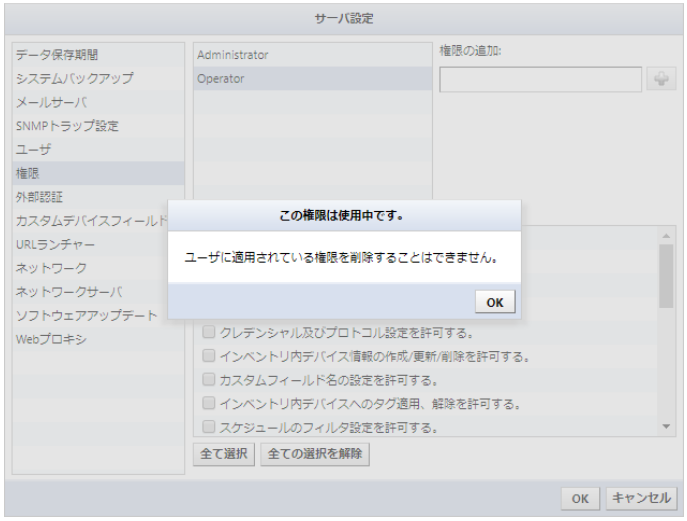
Copyright (C) 2026 LogicVein, Inc.

(2) 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。



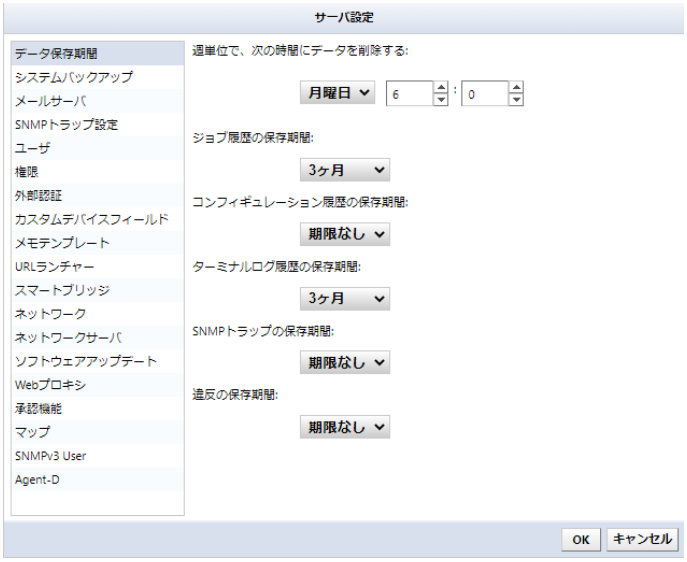
2. サーバ設定で［OK］をクリックします。

注意	使用中の権限を削除しようとすると、以下のエラーが発生します。  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。

Copyright (C) 2026 LogicVein, Inc.

7.8.3.5　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」

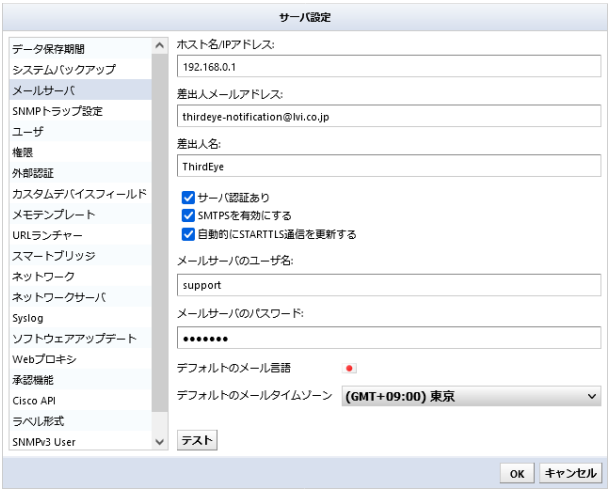
Copyright (C) 2026 LogicVein, Inc.

7.8.3.6　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。
自動的に STARTTLS 通信を更新する	自動で TLS または SSL を使用して安全な接続にアップグレードします。
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。
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。
ルート証明書	メールサーバが証明書を必要とする場合は、[選択]からルート証明書(*.pem)を選択します。

Copyright (C) 2026 LogicVein, Inc.

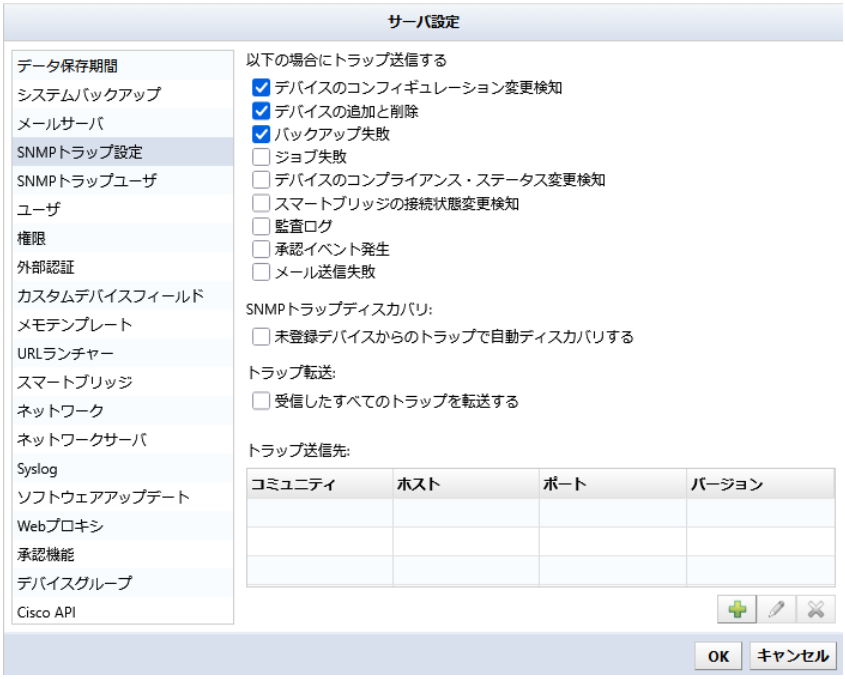
3. ［OK］をクリックします。

Copyright (C) 2026 LogicVein, Inc.

7.8.3.7　SNMP トラップ送信を設定する

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	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	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	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	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	コンプライアンスの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	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	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。
承認イベント発生	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	メール送信に失敗した場合、SNMP トラップを送信します。
未知デバイスからのトラップ発生時のデバイス検出	ThirdEye に登録されていないデバイスから SNMP トラップを受信した場合、その送信元 IP アドレスに対して自動的にディスカバリを実行します。

Copyright (C) 2026 LogicVein, Inc.

項目	説明
受信したすべてのトラップを転送する	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。

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「2c」または「３」から指定します。
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」

Copyright (C) 2026 LogicVein, Inc.

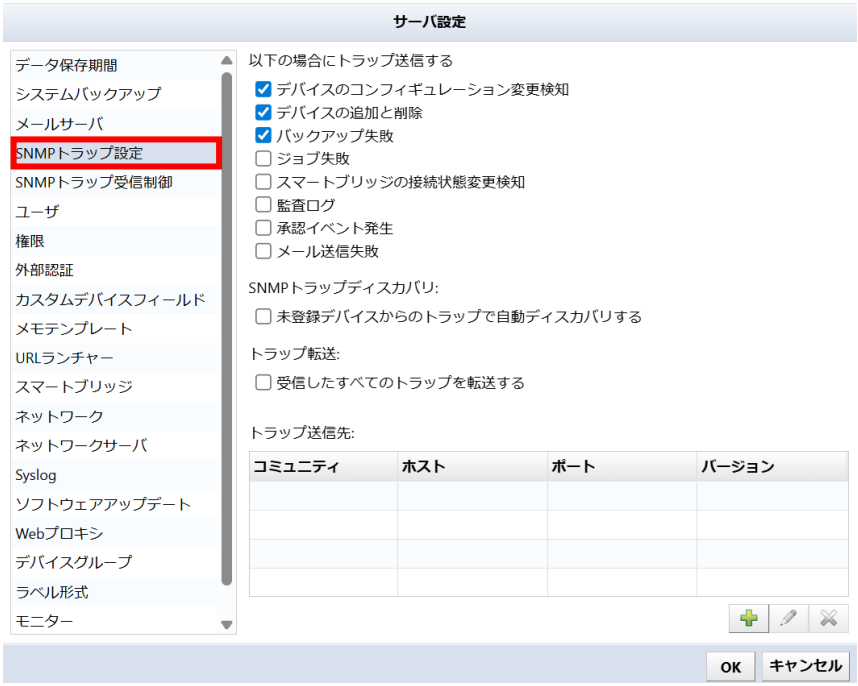
(1) SNMP トラップディスカバリ

r20251003.0827 より SNMP トラップディスカバリの機能に対応しました。この機能をオンにする事で、ThirdEye に登録されていないデバイスから SNMP トラップを受信した場合、その送信元 IP アドレスに対して自動的にディスカバリを実行します。製品に複数のネットワークが設定されている場合、サーバはトラップの送信元 IP アドレスをもとにヒューリスティック手法を用いて、そのデバイスが属するネットワークを判定します。

補足	*ヒューリスティック手法*とは、サブネットマスクの一致度や既知の管理 IP 情報などの推定ルールに基づき、送信元 IP アドレスから最も適合度の高いネットワークを自動的に判断する方式です。

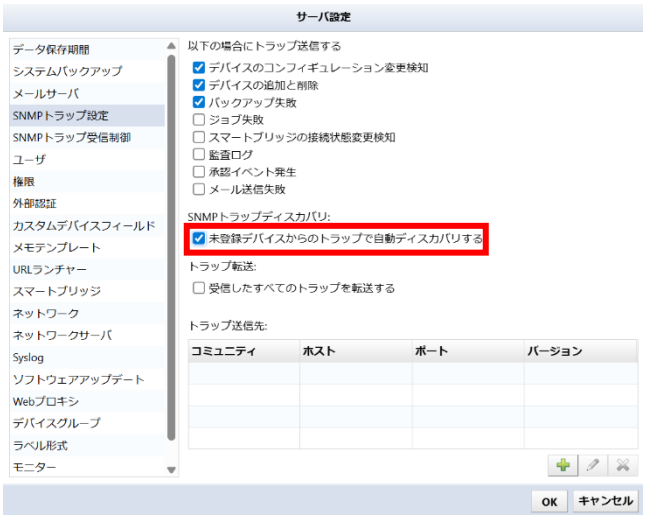
ディスカバリを成功させるには、あらかじめ該当ネットワークの SNMP クレデンシャルを設定しておく必要があります。また、過剰なディスカバリの試行を防ぎ、同一ネットワーク内の複数デバイスからのトラップをまとめて処理できるようにするため、ディスカバリの実行までに最大数分の遅延が発生する場合があります。ディスカバリに失敗したデバイスからの後続トラップは、5 分間は無視され、その後再びディスカバリが試行されます。一度ディスカバリされ登録された後に削除されたデバイスは、サーバが再起動されるまで再びディスカバリの対象にはなりません。また、デバイスを削除した後は SNMP トラップディスカバリを行ってもデバイス登録は行われません。

1. グローバルメニューの［設定］をクリックし、［SNMP トラップ設定］を選択します。

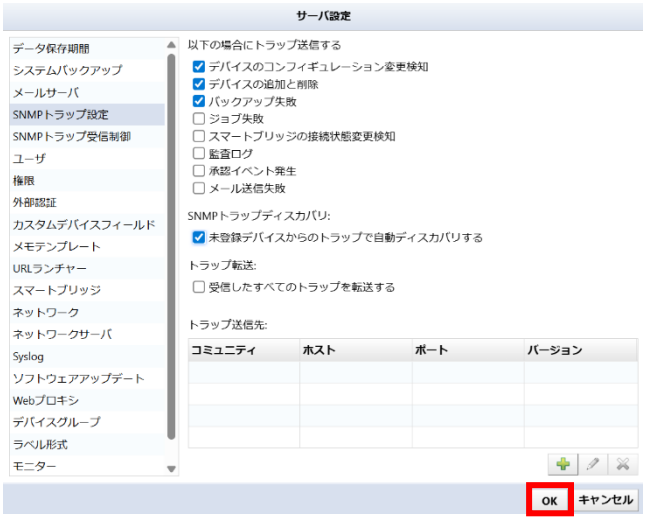


2. 未登録デバイスからのトラップで自動ディスカバリするにチェックをいれます。

Copyright (C) 2026 LogicVein, Inc.



3. 設定を有効にする為に、サーバ設定の下にある[OK]をクリックします。

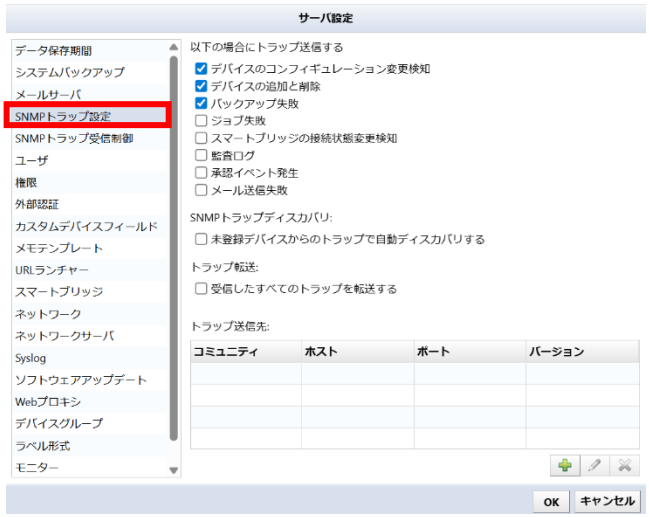


(i) SNMPv1/v2 でトラップを受信する

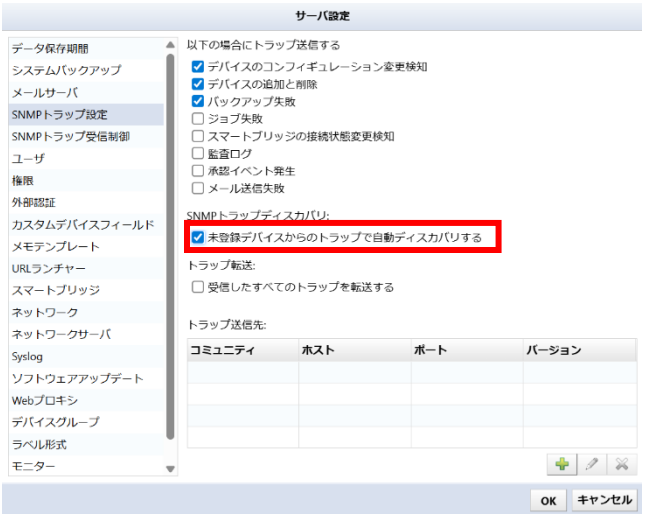
SNMP v1/v2 トラップで送信されるコミュニティ文字列を検証し、有効なもののみを受け付けるようにする場合は、[SNMP トラップ受信制御］であらかじめ許可するコミュニティ文字列を指定する必要があります。これらが定義されている場合、一致するコミュニティ文字列を持つトラップのみが受信され、それ以外は拒否されます。この機能を使用する為には、あらかじめ SNM P トラップ設定で SNMP トラップディスカバリの機能を有効にしておく必要があります。

1. グローバルメニューの［設定］をクリックし、［SNMP トラップ設定］を選択します。

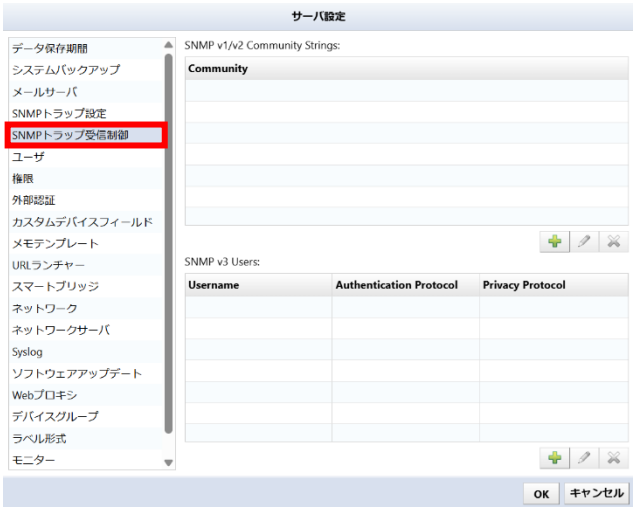
Copyright (C) 2026 LogicVein, Inc.



2. 未登録デバイスからのトラップで自動ディスカバリするにチェックをいれます。

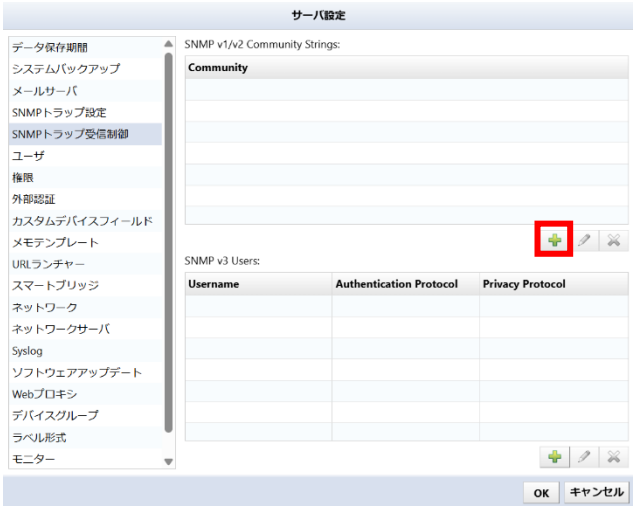


3. ［SNMP トラップユーザ受信制御］を選択します。

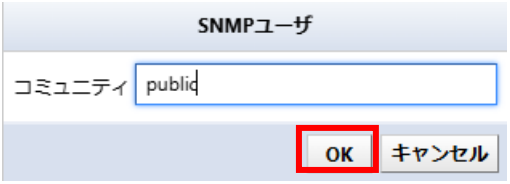


4. SNMP v1/v2 テーブルの下にある[ ]をクリックします。

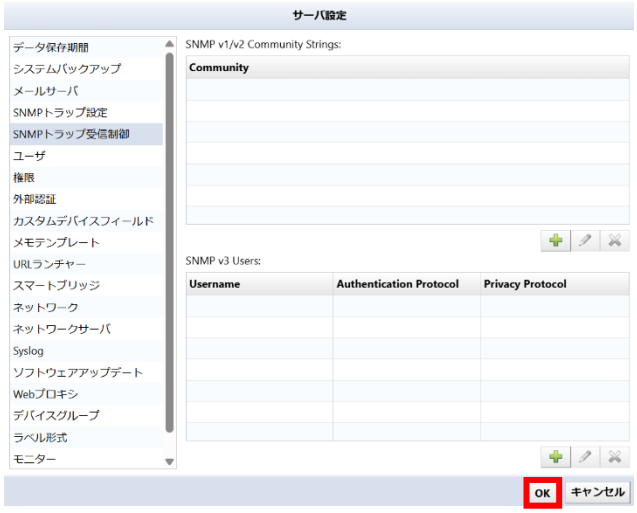
Copyright (C) 2026 LogicVein, Inc.



5. 受信する SNMP トラップの認証に使用されるコミュニティ文字列を入力します。
6. [OK]をクリックします。



7. 設定を有効にする為に、サーバ設定の下にある[OK]をクリックします。

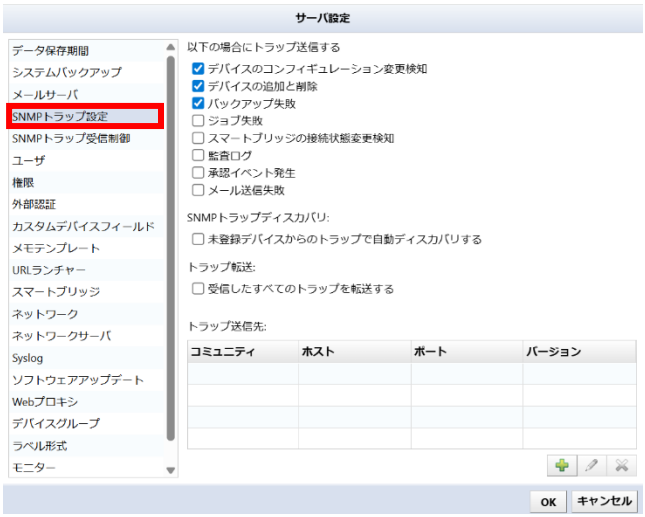


(ii)　SNMPv3 でトラップを受信する

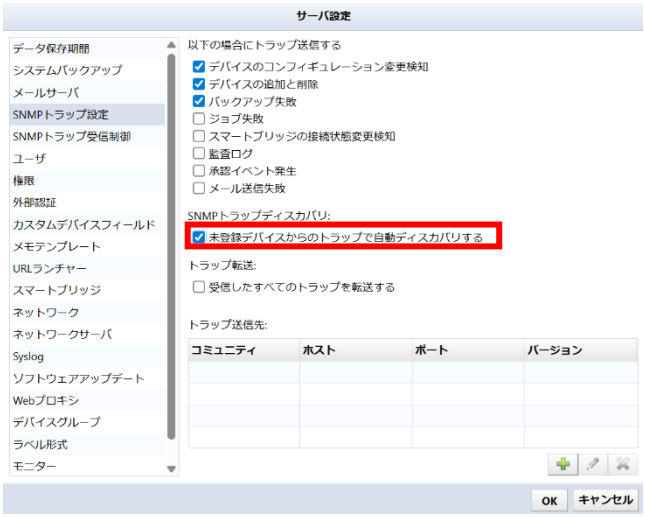
SNMPv3 トラップを有効なもののみを受け付けるようにする場合には、ThirdEye が受信した SNMP トラップを認証または復号化できるように事前に認証情報を設定する必要があります。この機能を使用する為には、あらかじめ SNMP トラップ設定で SNMP トラップディスカバリの機能を有効にしておく必要があります。

1. グローバルメニューの［設定］をクリックし、［SNMP トラップ設定］を選択します。

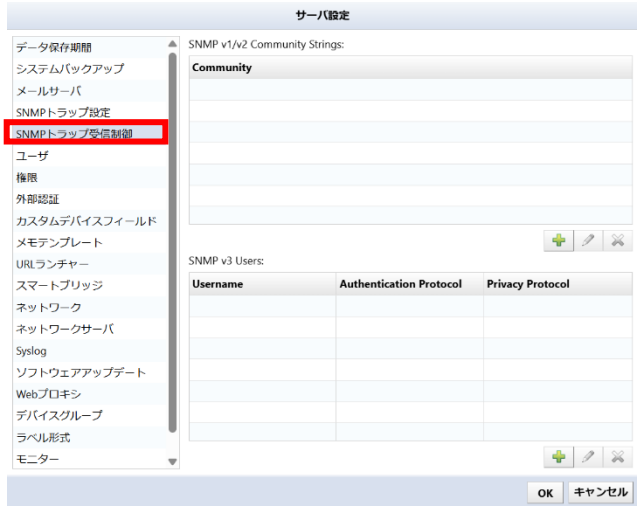
Copyright (C) 2026 LogicVein, Inc.



2. 未登録デバイスからのトラップで自動ディスカバリするにチェックをいれます。

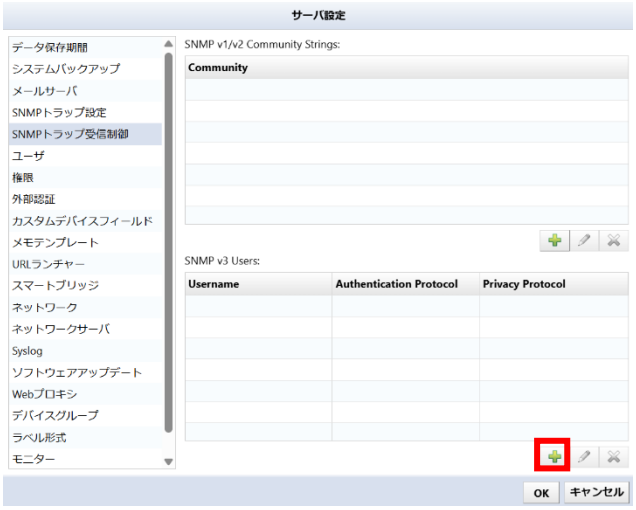


3. ［SNMP トラップ受信制御］を選択します。

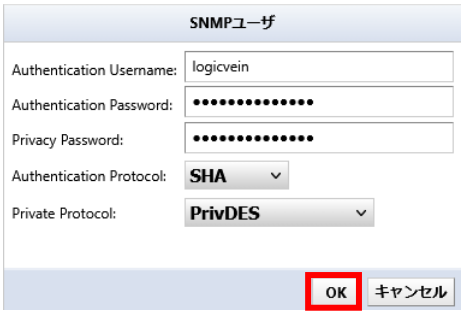


4. SNMP v3 テーブルの下にある[ ]をクリックします。

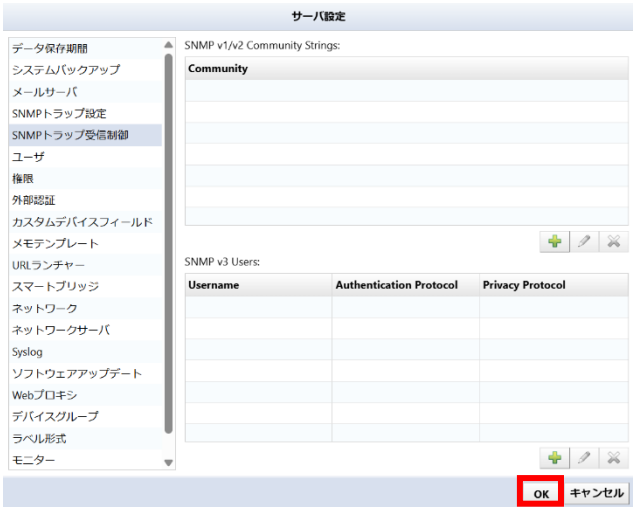
Copyright (C) 2026 LogicVein, Inc.



5. SNMPv3 ユーザ情報を設定します。これは、受信する SNMP トラップの認証または復号化に使用されます。
6. [OK]をクリックします。



7. 設定を有効にする為に、サーバ設定の下にある[OK]をクリックします。

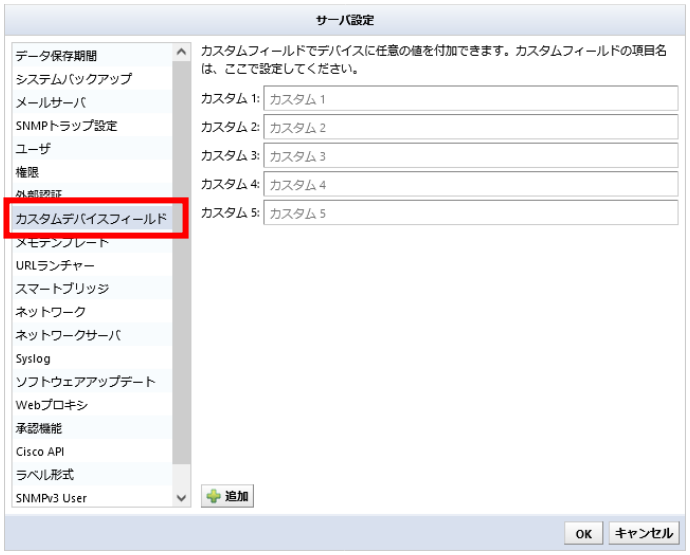


Copyright (C) 2026 LogicVein, Inc.

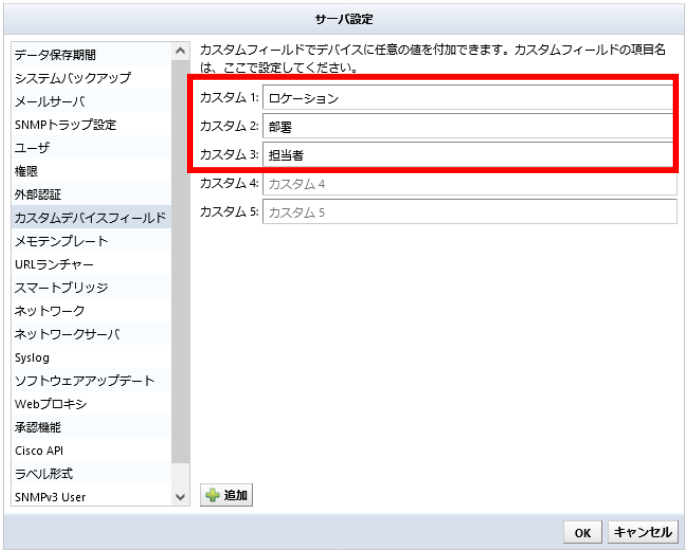
7.8.3.8　カスタムデバイスフィールドのカラム名変更/カラム追加

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変更や、新しいカスタムカラムの追加が可能です。

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。

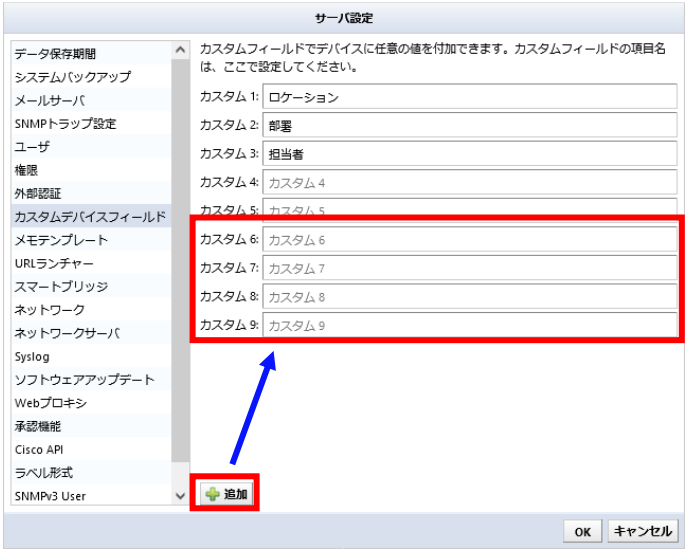


3. カラム名を変更する場合には、入力欄に任意の表示名を設定します。



Copyright (C) 2026 LogicVein, Inc.

4. カラムを追加する場合には、追加ボタンをクリックしカラムを追加します。



※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。

補足	SNMP トラップアクションの変数には、デフォルトのカスタム 1～5 が含まれます。あとから追加されたカスタムフィールドは、SNMP トラップアクションの変数に含まれません。

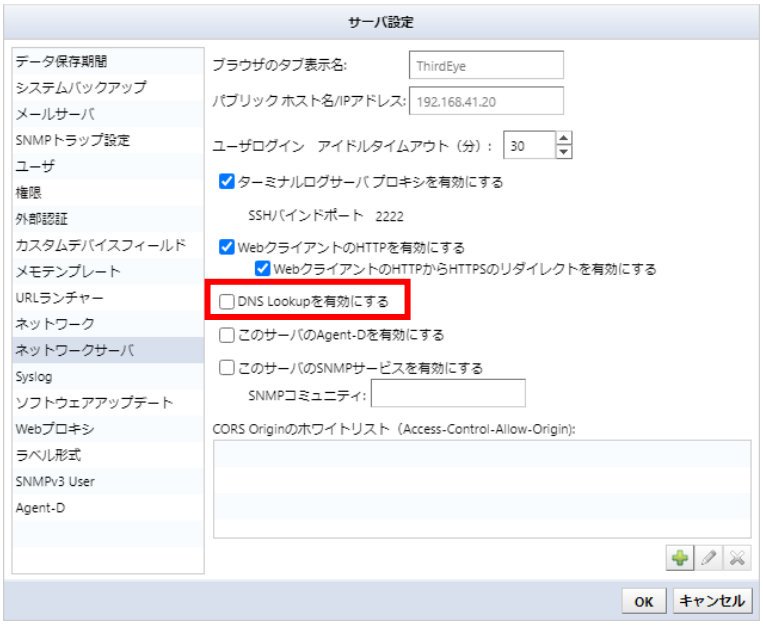
Copyright (C) 2026 LogicVein, Inc.

7.8.3.9 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］内の「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。

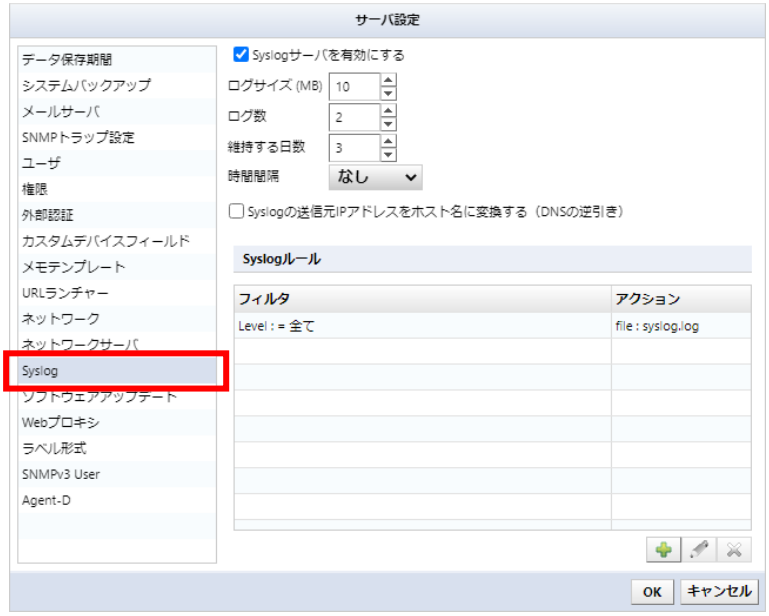
Copyright (C) 2026 LogicVein, Inc.

7.8.3.10 Syslog ファイルの詳細設定

（1） Syslog ファイルの保存期間/サイズを設定する

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。

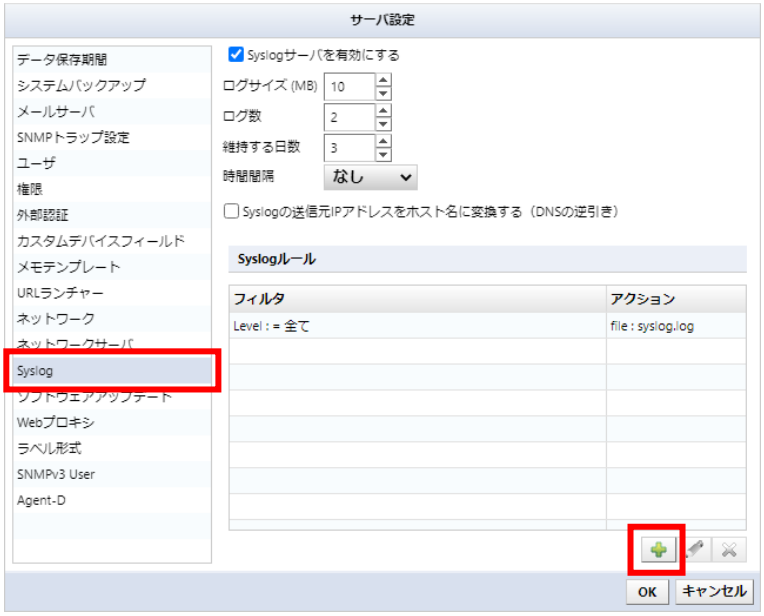
Copyright (C) 2026 LogicVein, Inc.

(2)　Syslog ルールを設定する

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。

Copyright (C) 2026 LogicVein, Inc.

- 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。

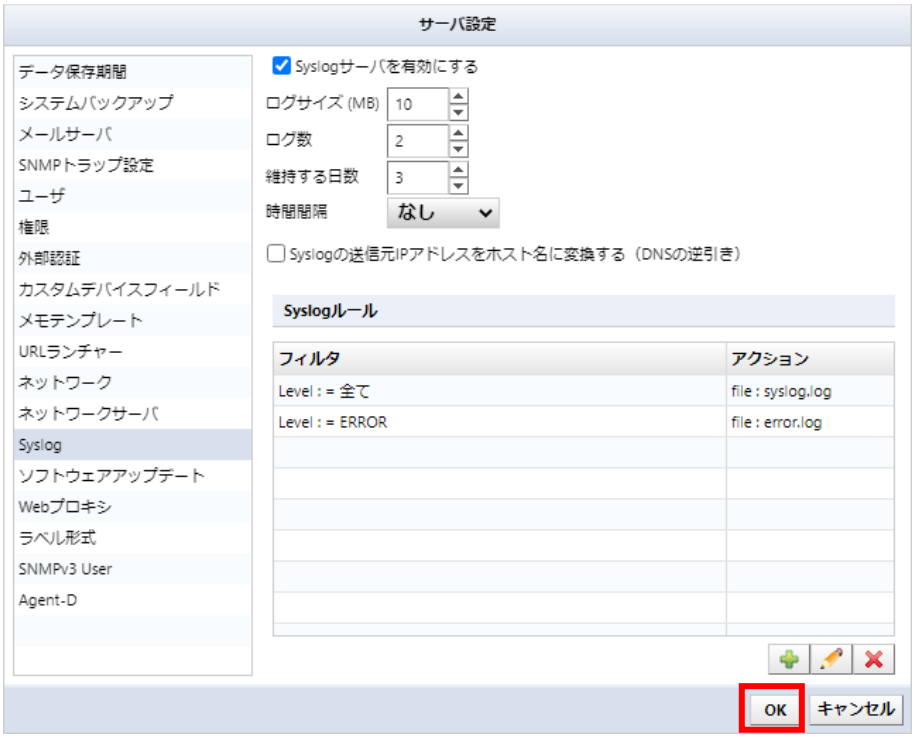
- Syslog アクション

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。 • 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。

Copyright (C) 2026 LogicVein, Inc.

4. 設定後、［OK］をクリックします。

5. サーバ設定画面で［OK］をクリックします。



Copyright (C) 2026 LogicVein, Inc.

（3） Syslog ファイルを外部ストレージに保存する

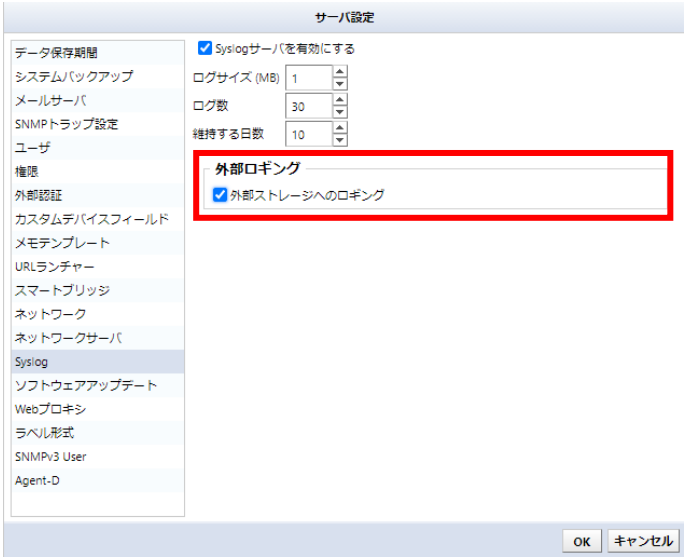
通常、受信した Syslog はローカルの syslog.log ファイルに保存されますが、NFS/SMB サーバと連携することで、外部ストレージに保存することができます。

※ 外部ストレージとの連携手順については、「9.4 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。

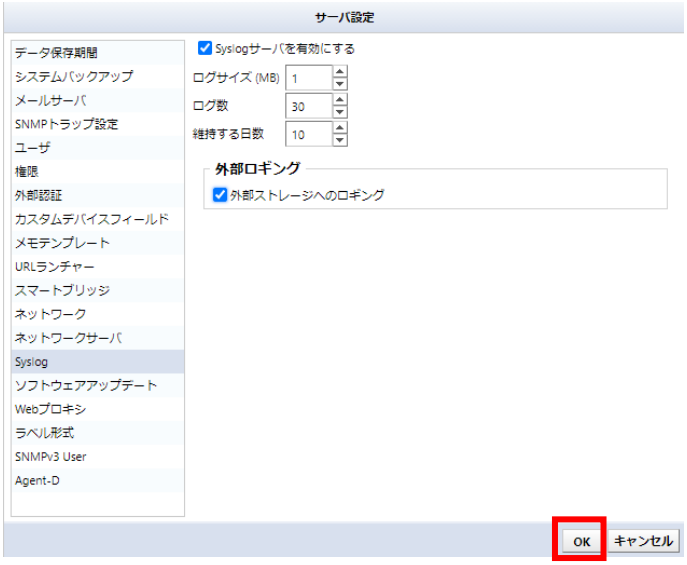
2. ［Syslog］をクリックし、「外部ストレージへのロギング」にチェックをいれます。



※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表示されます。

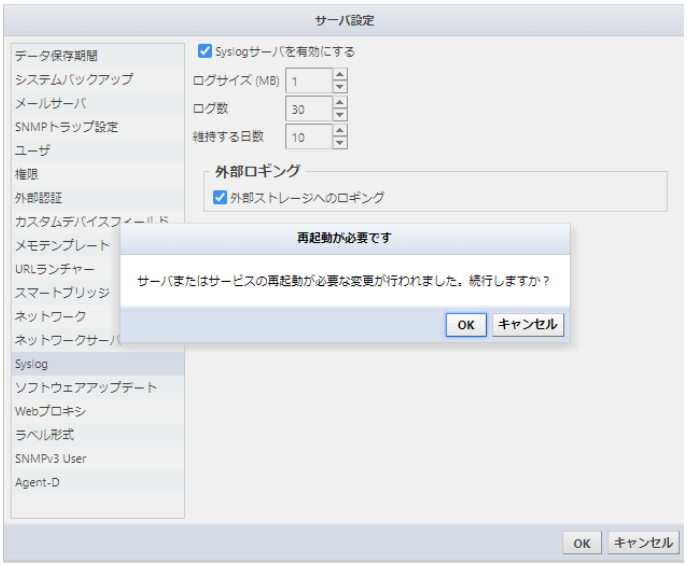
Copyright (C) 2026 LogicVein, Inc.

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。

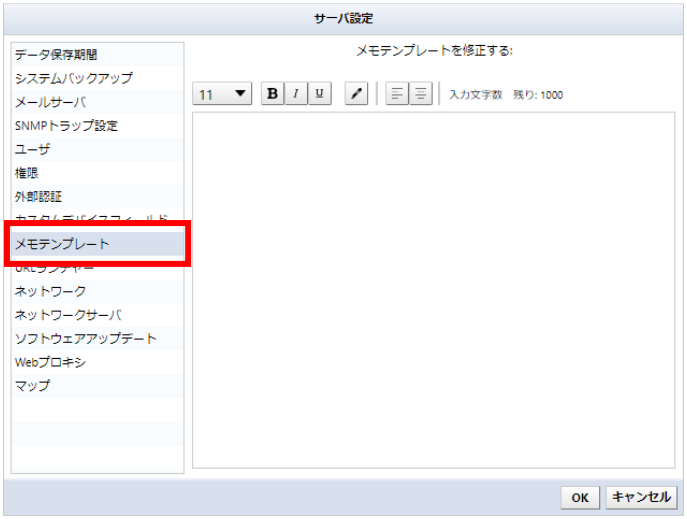
Copyright (C) 2026 LogicVein, Inc.

7.8.3.11 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。

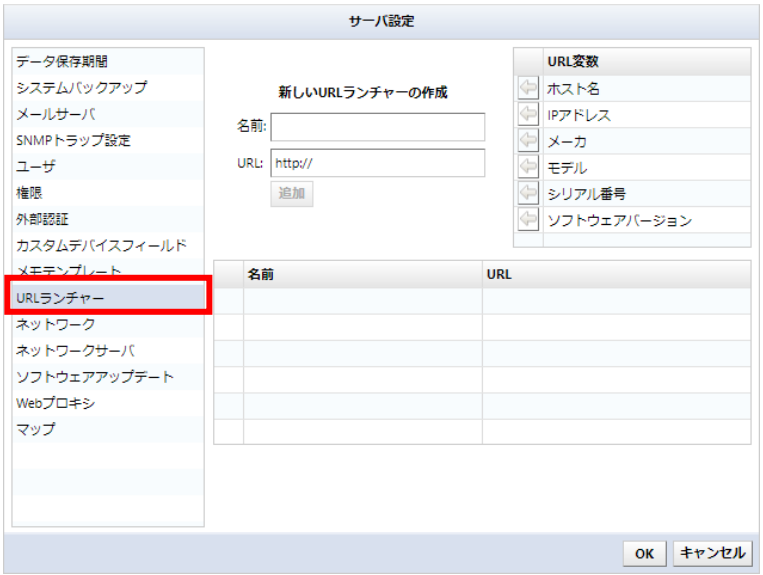
Copyright (C) 2026 LogicVein, Inc.

7.8.3.12 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



Copyright (C) 2026 LogicVein, Inc.

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	コンフィグバックアップで取得したメーカ名を引用する	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。

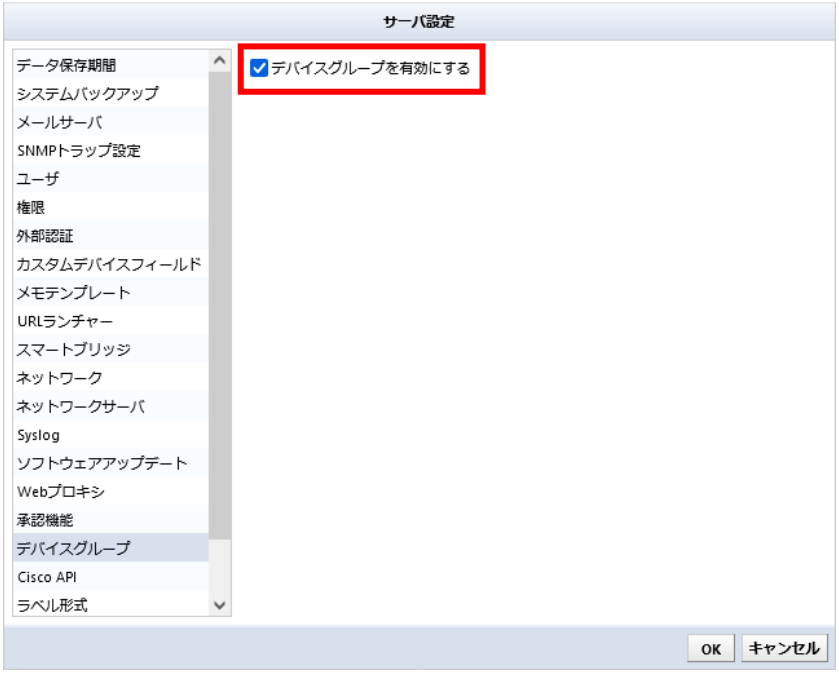
Copyright (C) 2026 LogicVein, Inc.

7.8.3.13 デバイスグループを使用する

リビジョン 20240905.2154 から、デバイスグループを使用した検索ができるようになりました。デバイスグループとは、任意の条件でデバイスを分類できる機能です。すべてのユーザが共通して使用する「共有」グループと、各ユーザが個別に使用する「プライベート」グループを設定できます。また、階層的なグルーピングにも対応しており、より柔軟な管理ができます。

(1) デバイスグループを有効にする

デバイスグループ機能は、デフォルトで無効になっています。デバイスグループを有効にするには、[サーバ設定]→[デバイスグループ]メニューで「デバイスグループを有効にする」にチェックを入れ、[OK]をクリックします。



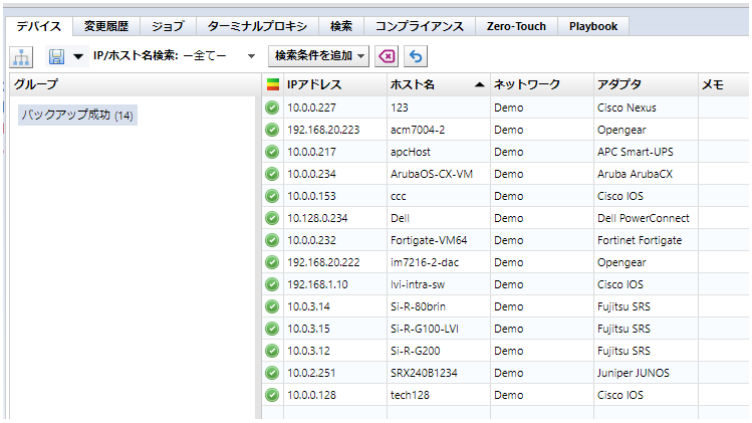
デバイスタブにデバイスグループのアイコンが追加されます。アイコンをクリックするとサイドバーが表示され、デバイスグループを構成することができます。

Copyright (C) 2026 LogicVein, Inc.

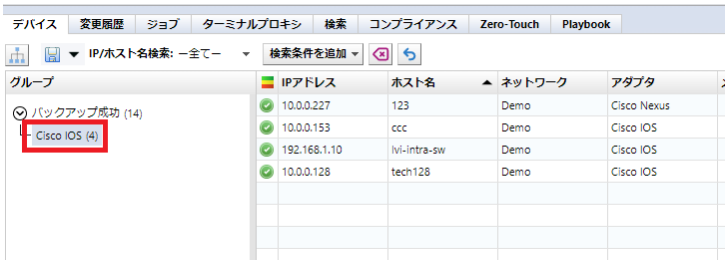
(2)　デバイスグループを追加する

デバイスグループを追加するには、グループサイドバーの左下にある［+］ボタンをクリックします。「名前」と「条件」を設定した後、［OK］ボタンをクリックします。なお、デバイスグループが最上位階層にある場合のみ、グループの「共有」または「プライベート」を選択できます。

デバイスグループを追加すると、作成したグループがサイドバーに表示されます。デバイスグループを選択すると、インベントリ内のデバイスがその分類条件に基づいてフィルタリングされます。



デバイスグループは階層構造にすることができます。上位階層のグループを選択した状態で［+］ボタンをクリックすると、下位階層にグループを追加できます。ただし、下位階層のグループでは「共有」または「プライベート」を選択できません。



Copyright (C) 2026 LogicVein, Inc.

7.8.3.14 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。

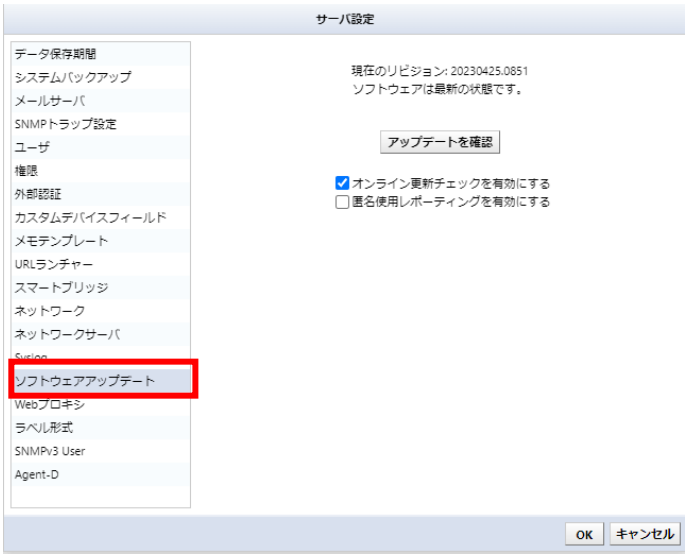
2. ［ライセンス更新］をクリックします。

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。

Copyright (C) 2026 LogicVein, Inc.

7.8.3.15 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。



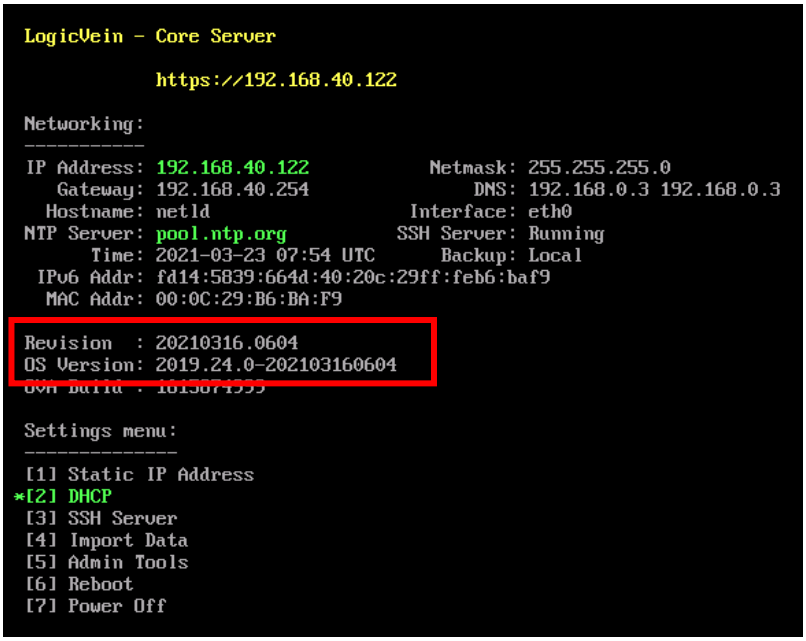
項目	説明
アップデートを確認	[アップデートを確認] をクリックすると、更新プログラムの配信をオンラインでチェックします。
オンライン更新チェックを有効にする	[オンライン更新チェックを有効にする] にチェックが入っていると、更新プログラムの配信があるかを定期的に確認します。(初期値：有効)
匿名使用レポーティングを有効にする	[匿名使用レポーティングを有効にする] にチェックが入っていると、匿名で利用状況データを送信します。 (初期値：無効)

Copyright (C) 2026 LogicVein, Inc.

7.8.3.16 リビジョンを確認する

現在使用している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。



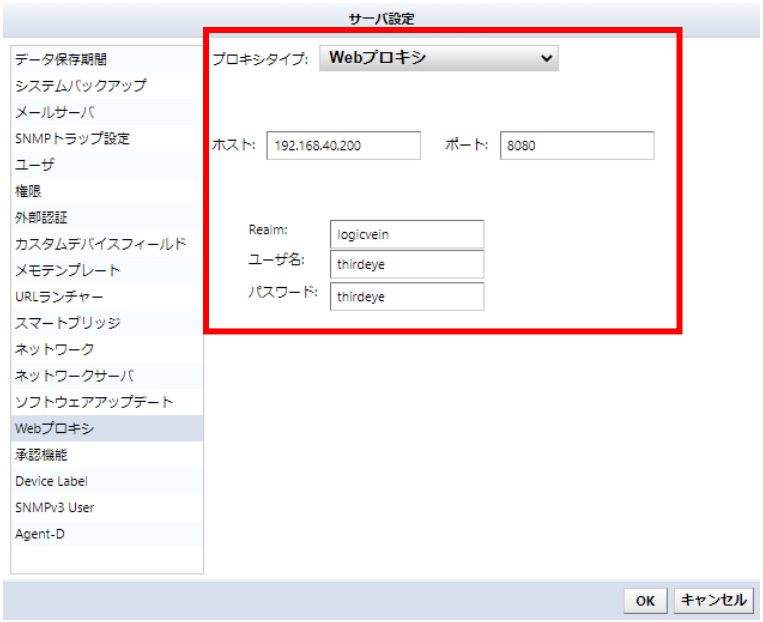
Copyright (C) 2026 LogicVein, Inc.

7.8.3.17　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。



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。

Copyright (C) 2026 LogicVein, Inc.

7.8.3.18 Zero-Touch (オプション)

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効率的に配布するための機能です。この機能は Cisco Plug and Play (PnP) や Cisco Networking Services (CNS) の技術を基盤としており、それに対応したデバイスでのみ使用できます。

Zero-Touch のコンフィグ配布形式

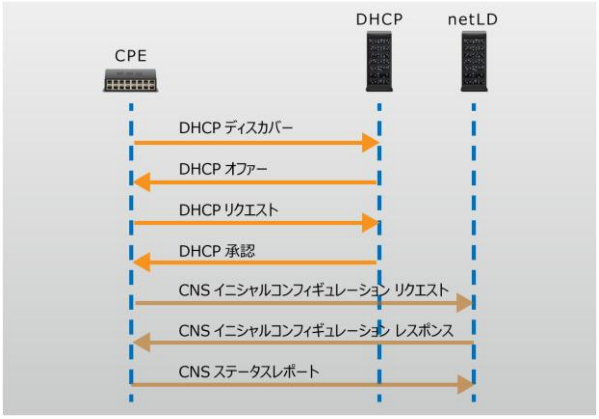
Zero-Touch は以下の 3 つの形式でコンフィグを配布できます。

形式	説明
テンプレート	テンプレートを基にコンフィグを配布します。主に、リモートオフィスに新規デバイスを導入する際に使用します。
セルフリカバリ	異常なコンフィグが適用され、動作しなくなったデバイスをリセットするのに利用します。
特定デバイスの復元	故障したデバイスを同じモデルの新しいデバイスに置き換える際に、既存の設定を転送します。

ThirdEye Zero-Touch は、以下のプロトコルを使用してコンフィギュレーションを配布します。そのため、ファイアウォール設定を適切に構成する必要があります。

PnP を使用する場合

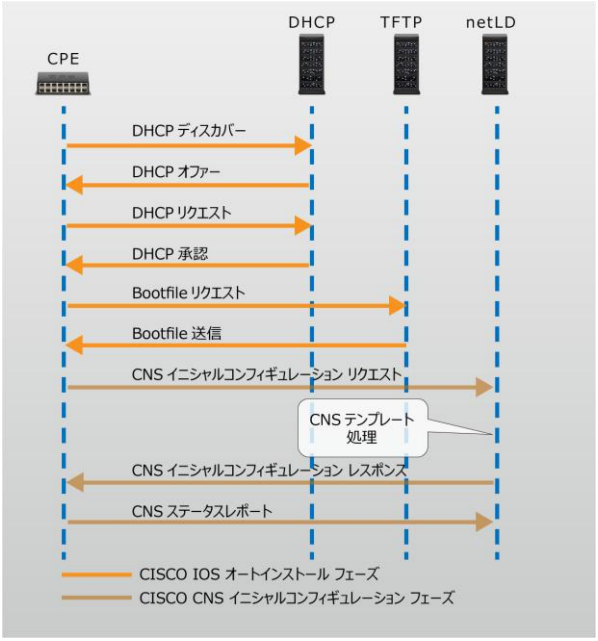
下図に示すように、DHCP を用いてデバイスに IP アドレスを割り当てた後、ThirdEye サーバが処理を実行します。図では説明を簡潔にするため、DHCP サーバと ThirdEye サーバが分かれているように示していますが、実際には 1 台のコンピュータ上で実行されます。



Copyright (C) 2026 LogicVein, Inc.

CNS を使用する場合

下図に示すように、DHCP で IP アドレスを取得した後、TFTP でブートファイルを取得して処理を進めます。



（1） Zero-Touch の利用条件

Zero-Touch を利用するには、以下の条件を満たし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 のバージョンが対応していること。
  - PnP: IOS 15.2(2)以降
  - CNS: IOS 12.2 以降
- デバイスに startup-config が存在しないこと。
- DHCP サーバで IP アドレスを割り当てた後、デバイスと ThirdEye サーバ間で通信が可能であること。

（2） Zero-Touch タイプの選択

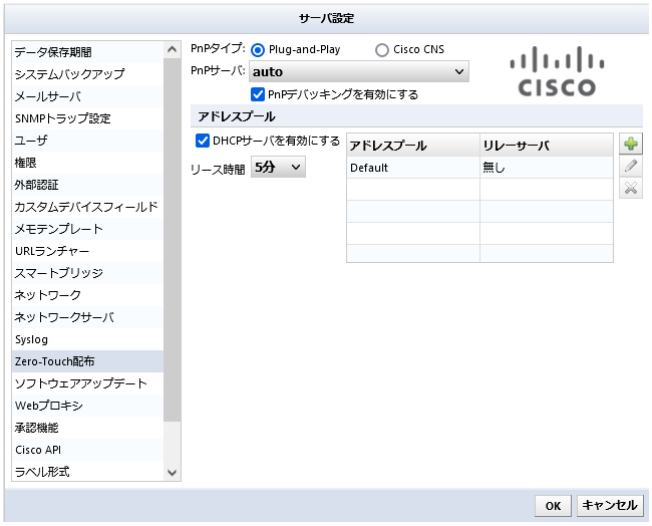
Zero-Touch のタイプには、「Plug and Play」と「Cisco CNS」の 2 種類があります。同時に使用することはできません。［設定］→［Zero-Touch 配布］から、PnP タイプを選択してください。

Copyright (C) 2026 LogicVein, Inc.

(3) DHCP サーバ

(i) ThirdEye の DHCP サーバを使用する

1. ［設定］→ [Zero-Touch 配布]を開き、「DHCP サーバを有効にする」にチェックを入れます。



2. ［+(追加)］をクリックまたは Default アドレスプールを編集します。
3. 必要な情報を入力し、OK ボタンをクリックします。

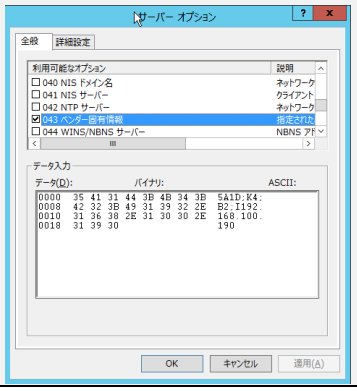
項目	説明
プール名	作成する DHCP プールの名前を入力
リレーサーバ CIDR	DHCP リレーサーバの存在する IP 範囲を入力
アドレス範囲	配布する IP アドレス範囲を入力（必須）
サブネットマスク	サブネットマスクを入力（必須）
デフォルトゲートウェイ	デバイスのデフォルトゲートウェイを指定
DNS サーバ(オプション)	デバイスからサーバの名前解決するための DNS サーバを指定

4. ［OK］をクリックします。

Copyright (C) 2026 LogicVein, Inc.

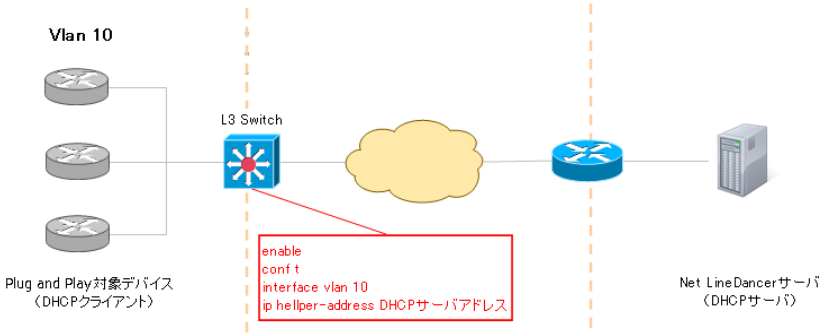
(ii)　外部の DHCP サーバを使用する

ThirdEye 以外の DHCP サーバを使用する場合、以下のオプションを設定する必要があります。PnP タイプに応じて設定内容が異なります。

PnP タイプ	オプション	説明
Plug and Play	43	43 では、ベンタ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。 
CNS	150 または 6 と 66	CNS では、TFTP を使用してブートファイルを送信します。そのため、DHCP で IP を付与する際に TFTP サーバの情報も渡す必要があります。150 では TFTP サーバの IP アドレスを渡します。66 では TFTP サーバの名前を、6 では DNS サーバの IP アドレスを渡します。

(iii)　同一ネットワーク外の DHCP サーバを使用する

DHCP サーバとデバイスが異なるネットワークにある場合は、DHCP リレーを設定し、デバイスからの DHCP リクエストがサーバに届くようにしてください。



Copyright (C) 2026 LogicVein, Inc.

(4)　コンフィギュレーションの配布

(i)　テンプレート

テンプレートの作成

大規模ネットワークでは、ほぼ同一の設定内容を持つデバイスが複数存在することがあります。IP アドレスやホスト名、DNS、syslog サーバのアドレスなど、一部の項目が異なるだけの場合が多いです。このような状況に対応するために、Zero-Touch では「テンプレート」機能を活用することで、設定作業の効率化と自動化が実現できます。テンプレートの基本的な概念については「7.7.4.7 代替値の使用

多くのノードは主な結果とともにメタデータを出力します。「コマンド実行」ノードの場合、device や status などが含まれます。これらはすべて、Playbook の実行開始後にそのノードの出力テーブルで確認できます。フィールドが代替値に対応している場合、値を{中括弧}で囲むことでその値を参照できます。多くのノードでは、これらの値に対してテンプレート化された代替値をサポートしています。

ノード	設定可能フィールド
正規表現一致	正規表現と Compare Against で代替値を設定する事ができます。
コマンド実行	コマンドエディタで代替値を設定する事ができます。
コマンド実行(自動リトライつき)	コマンドエディタで代替値を設定する事ができます。
SSH 実行	コマンドで代替値を設定する事ができます。
変数の設定	値で代替値を設定する事ができます。
フィールド編集	カスタムフィールドで代替値を設定する事ができます。
ファイルアップロード	サーバからファイルを取得するコマンドで代替値を設定することができます。
コンプライアンス違反検出	メッセージで代替を設定する事ができます。

ある情報を独自のメタデータとして抽出し、ノードから列として出力したい場合、最も簡単な方法は「正規表現一致」ノードを使用することです。このノードは Java 形式の正規表現をサポートしており、名前付きマッチグループはその名前を持つ値として取り出されます。例えば Cisco デバイスの稼働時間を「uptime」という名前の値として抽出するには、`show version` コマンドの出力を、以下の正規表現を指定した正規表現一致ノードに渡します。

lab-router uptime is (?[¥w ,]+)

「Compare Against」がデフォルトの {result} に設定されている場合、この正規表現は「Compare Against」の値全体と一致するように設計されません。「Partial Match」を有効にして、正規表現の一部が少なくとも含まれていれば一致としてカウントするように指定しましょう。この設定を行うと、正規表現の一致結果には、一致した uptime が新しい「uptime」列に表示され、後続のノードで {uptime} として使用できます。

また、「Compare Against」を変更することで、これらを連鎖させてより具体的な情報を取得することも可能です。例えば、最近リセットされたスイッチを確認したい場合は、正規表現の一致条件に「day」を含めない稼働時間を確認することができます。「uptime」の正規表現マッチノードを新しい正規表現マッチノードに接続し、正規表現を day に設定しま

Copyright (C) 2026 LogicVein, Inc.

す。「Compare Against」を{uptime}に設定し、「Partial Match」を有効にします。

その後、nonMatches の出力を確認するか、このノードを「Email」、「Webhook」、「コンプライアンス違反検出」、または「変数の設定」ノードに接続し、「デバイスが最近リセットされました：{uptime}」といったメッセージを設定することで、別の方法で結果を受け取ることができます。

Copyright (C) 2026 LogicVein, Inc.

7.8.3.19　スクリプト実行用コンテナ

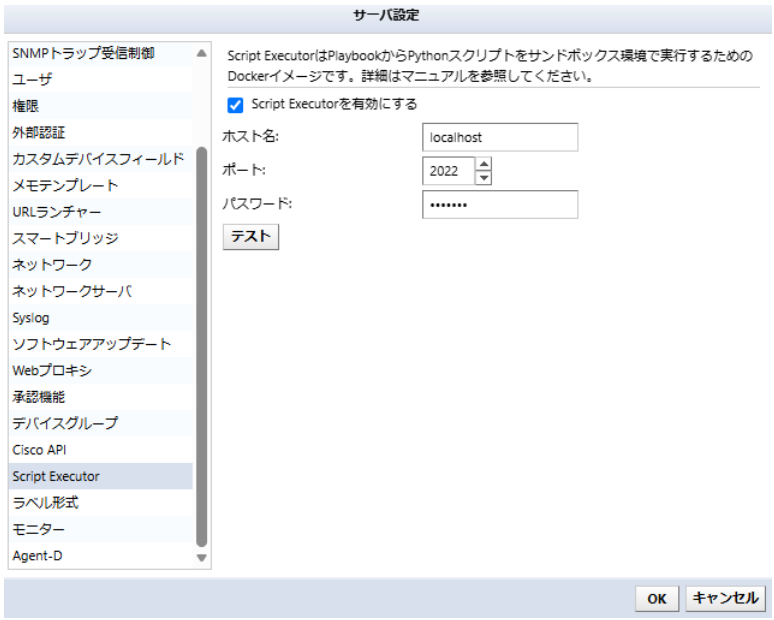
Playbook のワークフローによっては、より一般的なプログラミング言語を使用した方が実装しやすい場合があります。こうしたワークフローを実現するために、以下の URL で docker イメージを提供しています。

このイメージには Python がプリインストールされており、SSH（ポート：2022）経由で API を提供することで、よりサンドボックス化された環境でスクリプトを実行できるようにしています。イメージを pull したら、次のように実行できます。

サンドボックス環境にログインする為のデフォルトパスワードは'sandbox'です。サンドボックス環境内でログインし、いくつかのコマンドを実行する事ができます。/shared ボリュームは、ホストからファイルにアクセスできるようにするためのものです。たとえば、使用したいスクリプトのライブラリがある場合などが挙げられます。/packages ボリュームは、pip でインストールされたパッケージを保存するために使用されます。

(1)　スクリプト実行用コンテナを有効にする

サーバ設定には［Script Executor］オプションがあり、ここで実行モジュールを有効にし、ホスト名、ポート、および設定したパスワードを入力できます。実行モジュールを有効にすると、「Python スクリプトの実行」および「既存のスクリプトの実行」プレイブックノードにアクセスできるようになります。



(2)　スクリプト実行

「Python スクリプト実行」ノードへの各入力は、個別に Python を呼び出します。呼び出しは並行して実行され、順序やタイミングは保証されません。

Copyright (C) 2026 LogicVein, Inc.

7.9　バルクチェンジの概要 Suite

」で解説していますので、未読の場合は参照してください。

テンプレートを作成する手順は以下の通りです。

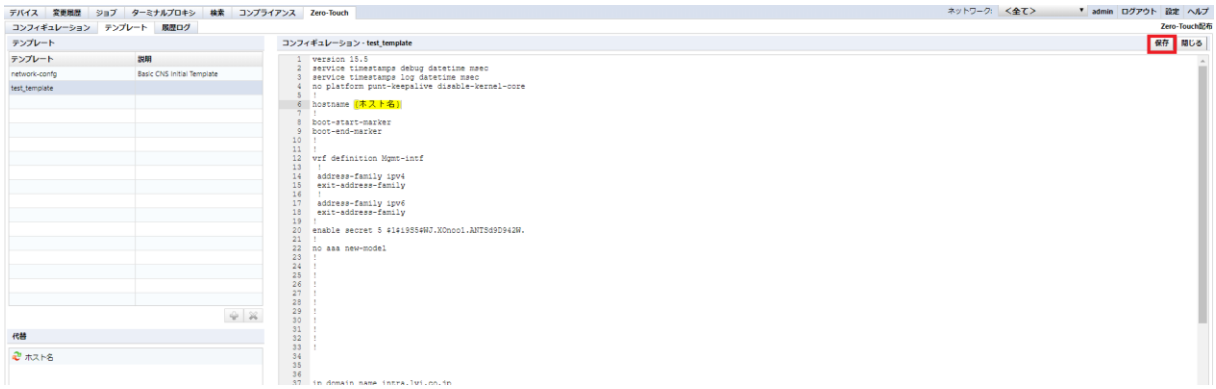
1. [Zero-Touch] → [テンプレート] に移動し、 をクリックします。

2. テンプレートタイプに「ダイナミックテンプレート」を選択します。
3. テンプレート名フィールドに名前を入力し、任意で説明を追加します。
4. OK ボタンをクリックします。

5. 画面右側に表示されるテキストエリアに、元となるコンフィギュレーションを入力します。
   ※　既存デバイスの設定（例: startup-config）をコピーして貼り付けると効率的です。
6. 必要に応じて、コンフィギュレーションの一部を変数に置き換えます。

Copyright (C) 2026 LogicVein, Inc.

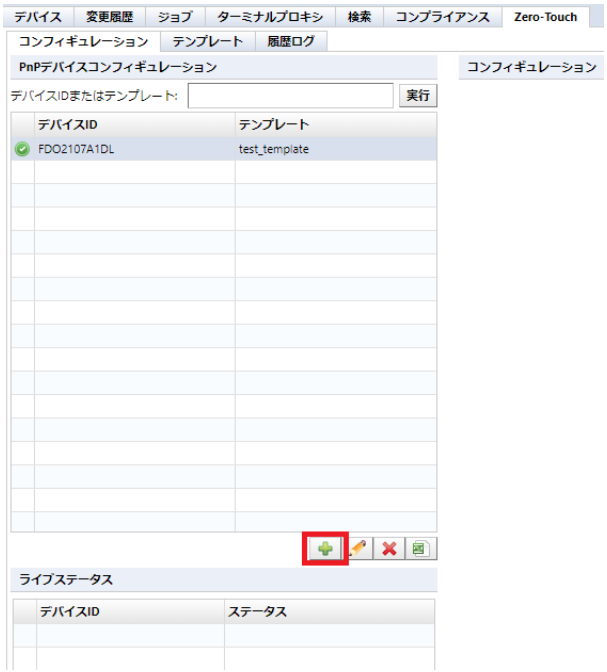
7. テキストエリア右上の［保存］ボタンをクリックして、テンプレートを保存します。



デバイスの登録

テンプレートの準備が完了したら、次にコンフィグを適用するデバイスを登録します。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。

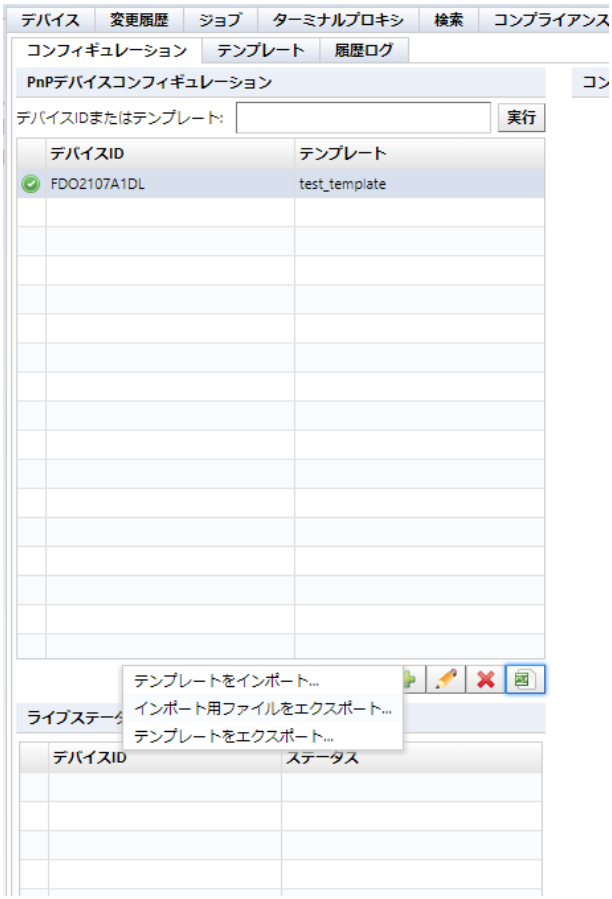


Copyright (C) 2026 LogicVein, Inc.

テンプレート変数の値を外部からインポート

テンプレート変数の値を、外部で作成した Excel ファイルからインポートすることができます。以下の手順に従ってください。

1. 代替値の入力画面で、［閉じる］ボタンをクリックします。
2. ボタンをクリックし、サブメニューを表示します。
3. メニューから「テンプレートをインポート」を選択します。



項目	説明
テンプレートをインポート	変数値を含む Excel 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	変数値を追記可能な空の Excel 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 Excel シートを出力します。

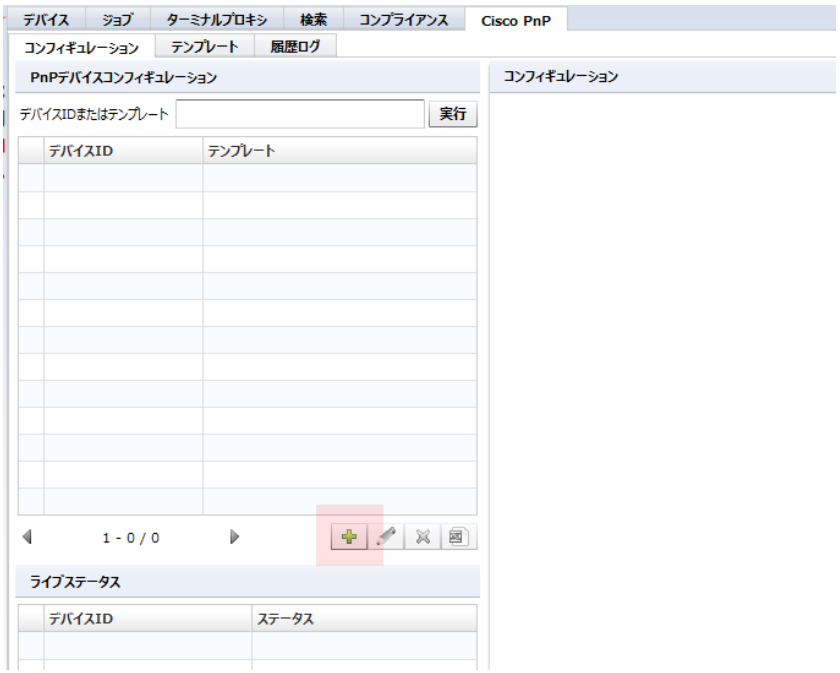
Copyright (C) 2026 LogicVein, Inc.

(i) Zero-Touch セルフリカバリ

Zero-Touch では、新しいコンフィギュレーションを送信する代わりに、ThirdEye 内部に保存されている過去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のコンフィギュレーションが誤って消去された場合に有効です。コンフィギュレーションが失われたデバイスは応答しなくなるため、Zero-Touch のような特別な機能を使わないと復旧できません。

この手順は、テンプレートを使用した Zero-Touch 操作と多くの点で共通しています。

1. メインペインの「コンフィギュレーション」サブタブに移動し、［+］をクリックします。



2. デバイスコンフィギュレーションダイアログで必要な情報を入力後、「配布タイプ」の項目で「セルフリカバリオプション」を選択し、［OK］ボタンをクリックします。

その後、ThirdEye 内に保存され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、テンプレート配信モードと異なる点はありません。

Copyright (C) 2026 LogicVein, Inc.

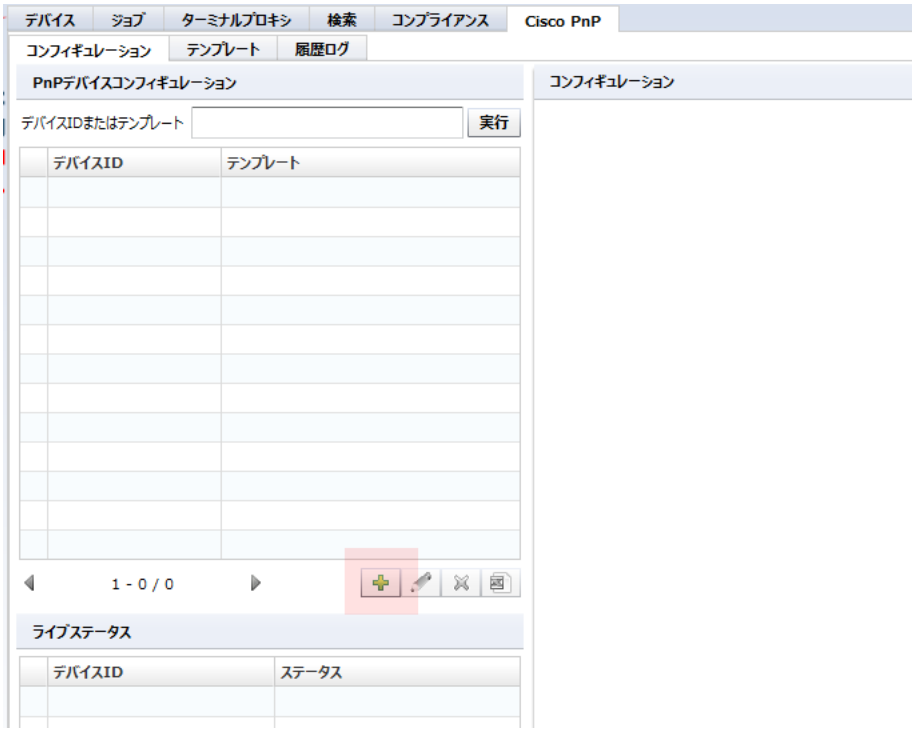
(ii)　Zero-Touch 特定デバイスの復元

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。

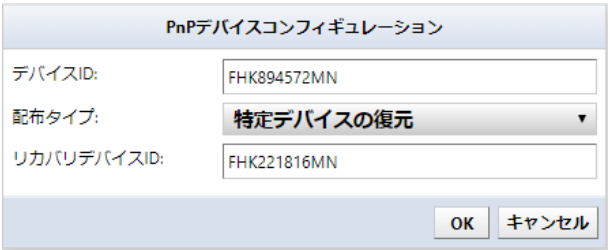
この機能は、デバイスが遠く離れた位置にあって(別のデータセンターなど)、かつ現地に操作を担当できるものがおらず、直接手で操作することができない時に極めて有効です。Zero-Touch を用いれば、現地のデータセンターの人間にケーブルを挿し込むよう電話で指示できればよく、現地の人間に特殊技能は求められません。その後のデバイス復元などの操作が、現地でではなくネットワーク経由で行われるからです。

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。



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。



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

Copyright (C) 2026 LogicVein, Inc.

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。

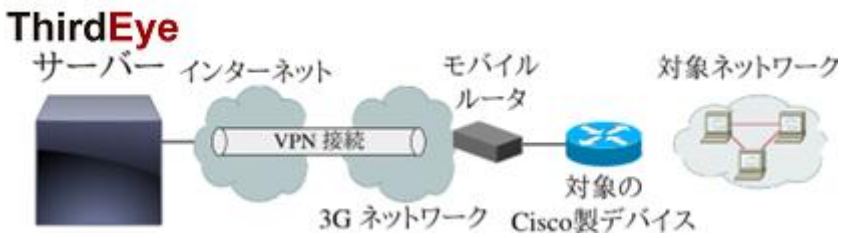
その後、ThirdEye にある、古いデバイス用のコンフィギュレーション情報が、ネットワーク経由で新しいデバイスにアップロードされます。その他の操作方法は Zero-Touch テンプレートの操作方法と同じです。

（2） 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。)

（3） 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動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を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。

Copyright (C) 2026 LogicVein, Inc.

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。

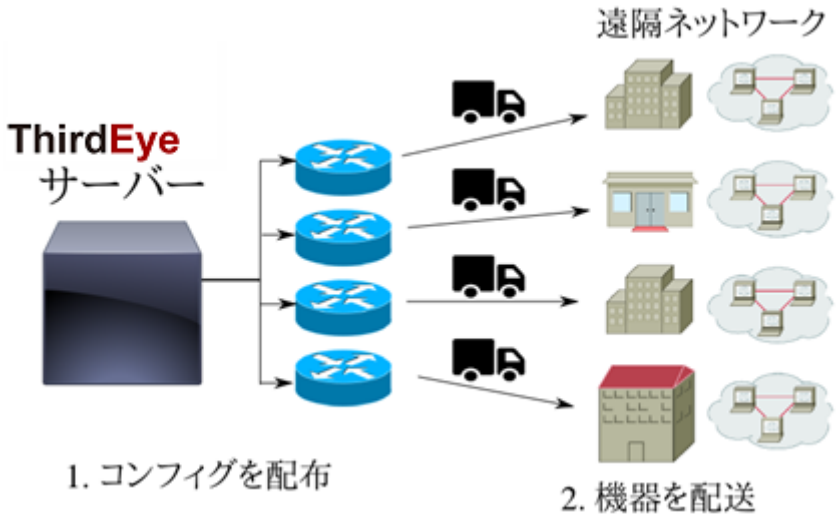
ThirdEye がデバイスからのリクエストを自動的に受け取り、コンフィギュレーションを 3G ネットワーク経由で送信します。

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。

Copyright (C) 2026 LogicVein, Inc.

(4)　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。

(5)　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必要があります。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。

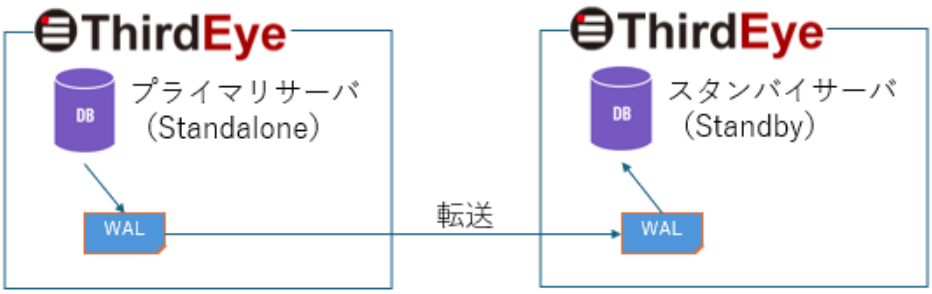
```
cns id hardware-serial
!
cns connect cns-profile ping-interval 10 retries 3 sleep 5 discover interface FastEthernet template cns-profile
!
cns template connect cns-profile
cli description Basic CNS Initial Template
cli ip address dhcp
cli ip route 0.0.0.0 0.0.0.0 ${interface}
cli no shutdown
exit
!
cns config initial <IP> status http://<IP>/cns/config。asp
!
end
```


Copyright (C) 2026 LogicVein, Inc.

8. 冗長機能

8.1 概要

リビジョン 20241218.0941 より、冗長機能がサポートされました。冗長機能では、「Standalone」と「Standby」という 2 つの役割を使用します。Standalone では、通常どおり監視や設定を行います。Standby は、Standalone からのトランザクションログ（以後、WAL）を受信し、それをリカバリすることで同期を行います。



※ Standalone は冗長構成において「プライマリサーバ」と呼ばれます。

※ OS イメージファイルや添付されたファイル、マップのアイコンなどのファイルは 120 秒間隔でスタンバイサーバに同期されます

8.1.1 利用条件

冗長機能は、eth1 を使用してデータを同期します。SSH を使用するため、プライマリサーバとスタンバイサーバ間にファイアウォールがある場合は、スタンバイサーバからプライマリサーバへの SSH 通信を許可してください。また、両サーバの CPU コア数、メモリ容量、ディスクサイズは同一である必要があります。

8.1.2 制限される機能

冗長機能には以下の制限があります。これらの機能はサポートされていませんので、ご注意ください。

- スマートブリッジとの同時使用
- AWS や Azure などのクラウド環境での使用
- プライマリサーバで受信した Syslog データの引き継ぎ
- プライマリサーバで取得したシステムバックアップファイルの引き継ぎ
- OVA コンソールで設定する内容の引き継ぎ

Copyright (C) 2026 LogicVein, Inc.

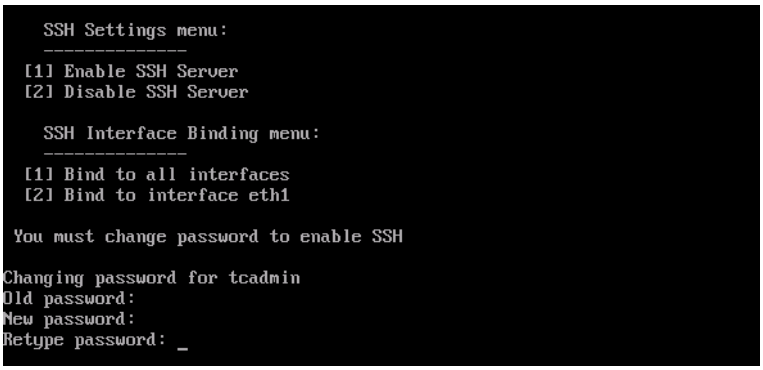
8.2　設定

冗長構成の設定は、OVA コンソールを使用して行います。この設定を実施するためには、VMware や Windows Hyper-V を操作できる権限を持つユーザが必要です。

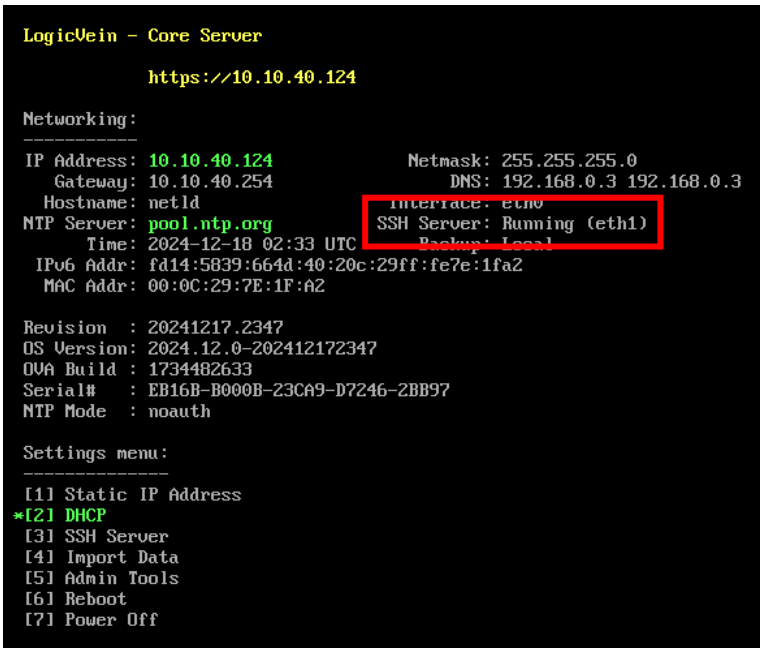
8.2.1　手順

設定を行う前に、プライマリサーバとスタンバイサーバの eth1 インタフェースに IP アドレスを設定し、eth1 間で通信可能な状態にしておいてください。

1. プライマリサーバの OVA コンソールに接続します。
2. キーボードの[3](SSH Server)->[1](Enable SSH Server)->[2](Bind to interface eth1)と押下し、eth1 に対して SSH を有効にします。

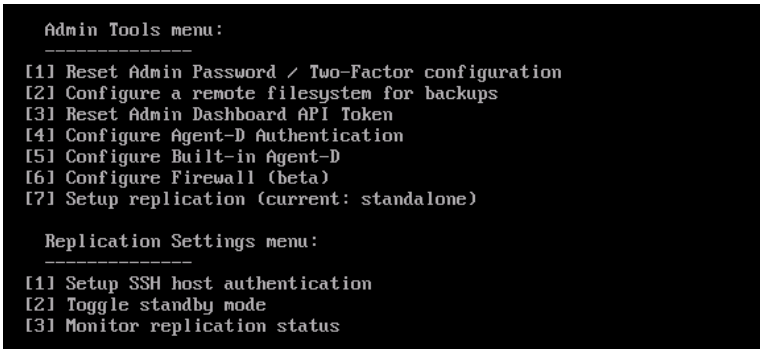


3. SSH Server が Running になっていることを確認します。

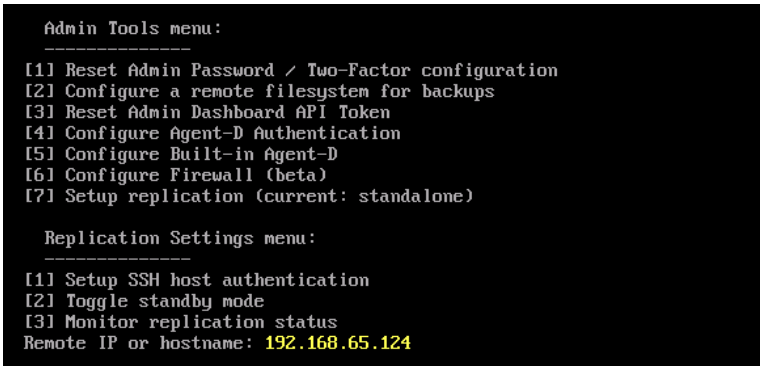


Copyright (C) 2026 LogicVein, Inc.

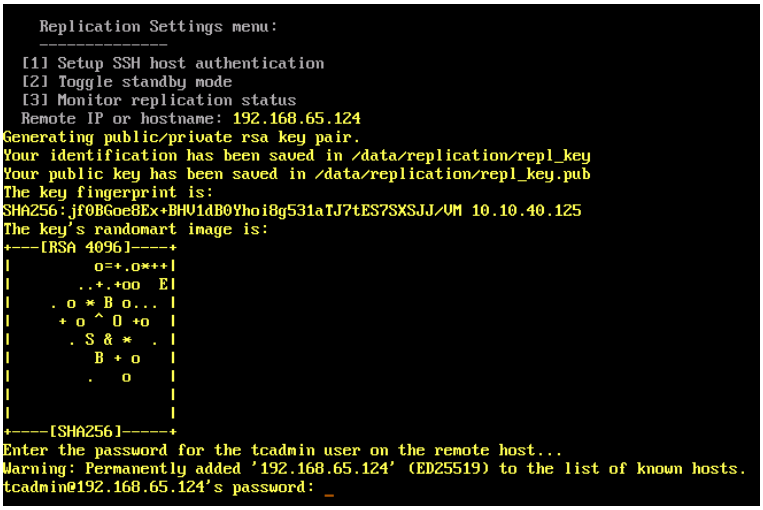
4. スタンバイサーバの OVA コンソールに接続します。
5. キーボードの[5](Admin Tools)->[7](Setup replication)->[1](Setup SSH host authentication)と押下し、プライマリサーバの SSH ホスト認証設定をします。



6. プライマリサーバの eth1 の IP アドレスを入力します。

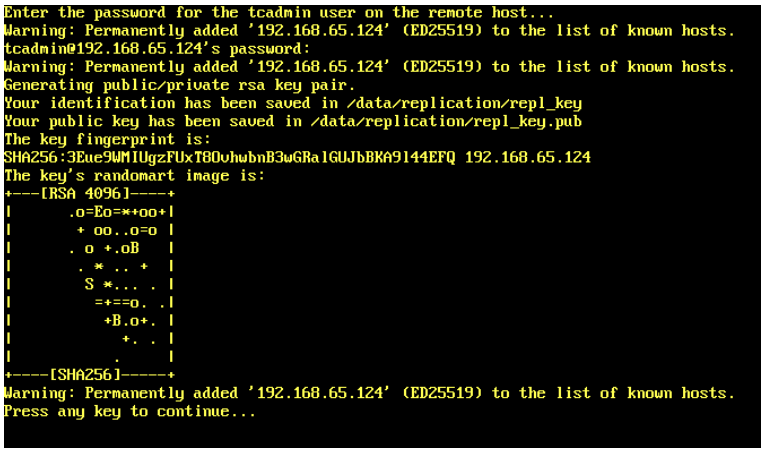


7. プライマリサーバへ SSH する時のパスワードを入力します。

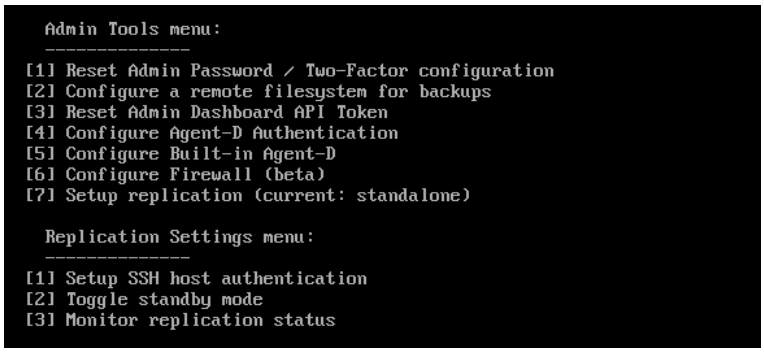


Copyright (C) 2026 LogicVein, Inc.

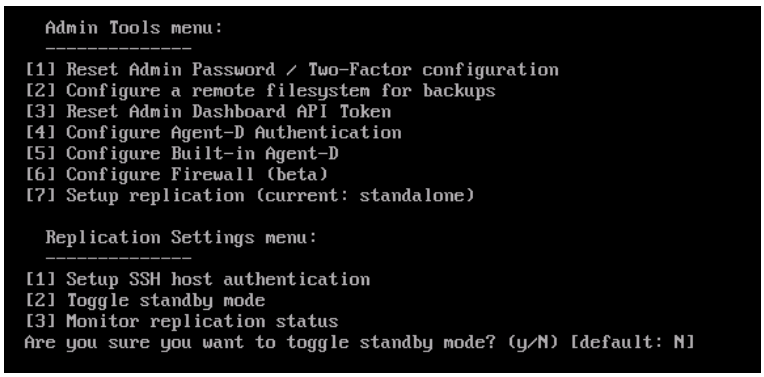
8. Enter キーなど何かキーを押下します。



9. キーボードの[5](Admin Tools)->[7](Setup replication)->[2](Toggle standby mode)と押下し、スタンバイサーバをサーバの役割を Standalone から Standby に変更します。



10. 「y」を押下します。



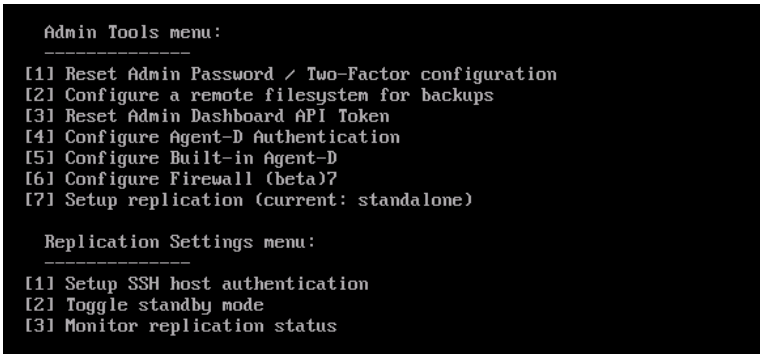
設定は以上です。「y」を押下すると、自動でスタンバイサーバが再起動されます。

Copyright (C) 2026 LogicVein, Inc.

8.2.2　ステータスの確認

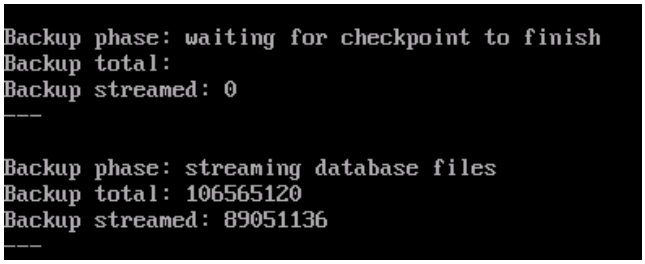
冗長機能のステータスは、OVA コンソールから確認することができます。

1. プライマリサーバの OVA コンソールに接続します。
2. キーボードの[5](Admin Tools)->[7](Setup replication)->[3](Monitor replication status)と押下し、ステータスを確認します。



※　ステータスが表示されると自動で更新されていきます。ステータス画面を閉じるには、ctrl+c を押してください。

冗長構成が設定されると、まずはバックアップフェーズが開始されます。バックアップフェーズでは、初期データがプライマリサーバからスタンバイサーバにコピーされます。



バックアップフェーズが完了すると、データストリーミングが開始されます。開始されると、以下のような画面が表示されます。設定後は、”Replication state: streaming”が表示されることを確認します。

8.2.3　再設定が必要ケース

以下のケースでは、再度冗長機能の設定が必要です。

- プライマリサーバでシステムバックアップを復元した場合
- フェイルオーバー後、元の状態に戻す場合

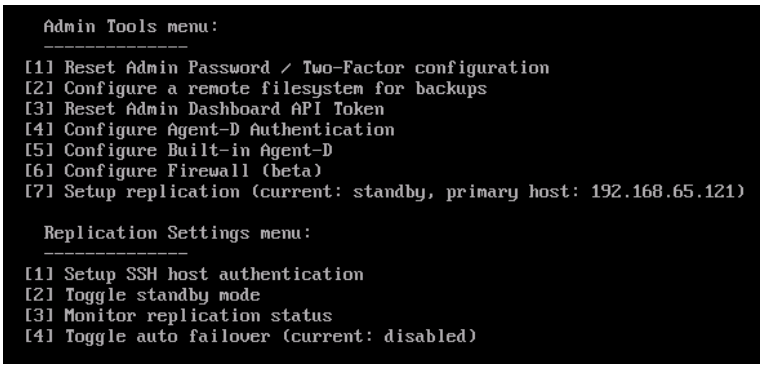
Copyright (C) 2026 LogicVein, Inc.

8.3　フェイルオーバー

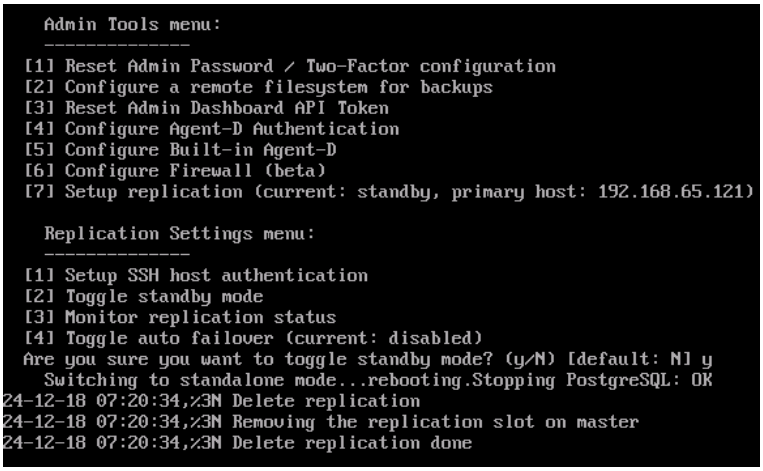
8.3.1　手動フェイルオーバー

スタンバイサーバで監視を行う場合には、役割を Standby から Standalone に変更します。変更手順は以下のとおりです。

1. スタンバイサーバの OVA コンソールに接続します。
2. キーボードの[5](Admin Tools)->[7](Setup replication)->[2](Toggle standby mode)と押下し、スタンバイサーバをサーバの役割を Standby から Standalone に変更します。



3. 「y」を押下します。



「y」を押下すると、自動でスタンバイサーバが再起動されます。再起動後、Web ブラウザからログインしてください。

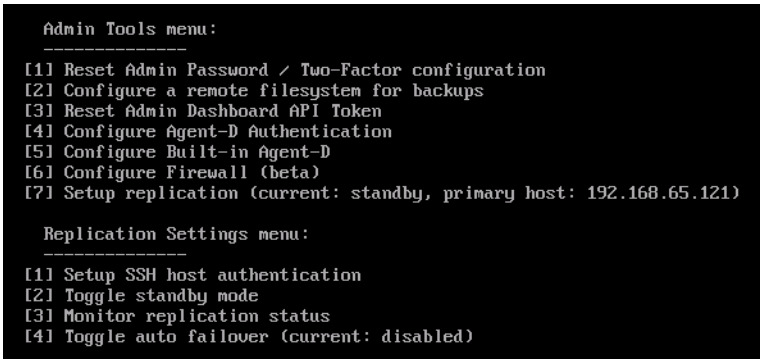
Copyright (C) 2026 LogicVein, Inc.

8.3.2　自動フェイルオーバー

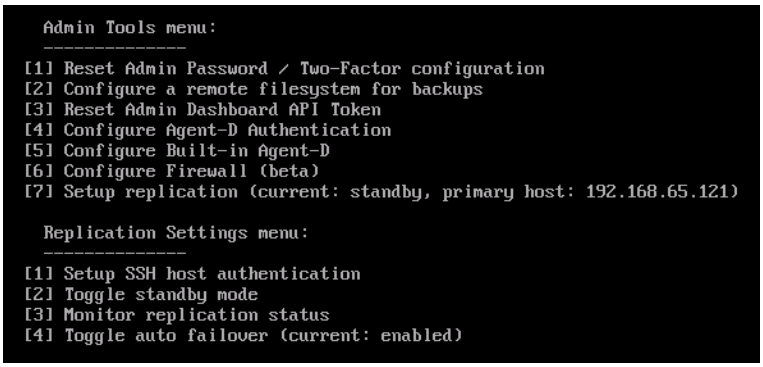
自動フェイルオーバーを有効に設定すると、プライマリサーバとスタンバイサーバ間で 60 秒以上の意図しない通信断が発生した場合、スタンバイサーバが自動で役割を Standby から Standalone に変更し、監視を引き継ぎます。ユーザがプライマリサーバを再起動/シャットダウンした場合、または 60 秒以内の再接続に成功した場合、切り替わりは行われません。

デフォルトでは、自動フェイルオーバーは無効に設定されています。プライマリサーバに障害が発生した場合に、スタンバイサーバが自動的に監視を引き継ぐようにするには、次の手順に従って自動フェイルオーバーを有効に設定します。

1. スタンバイサーバの OVA コンソールに接続します。
2. キーボードの[5](Admin Tools)->[7](Setup replication)->[4](Toggle auto failover)と押下し、自動フェイルオーバーを有効にします。



3. [4]を押下後、自動で最初の画面に戻ります。再度、[5](Admin Tools)->[7](Setup replication)と進み、Toggle auto failover の current が「enabled」になっていることを確認します。



Copyright (C) 2026 LogicVein, Inc.

9.　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。

9.1　自動でシステムバックアップを実行する

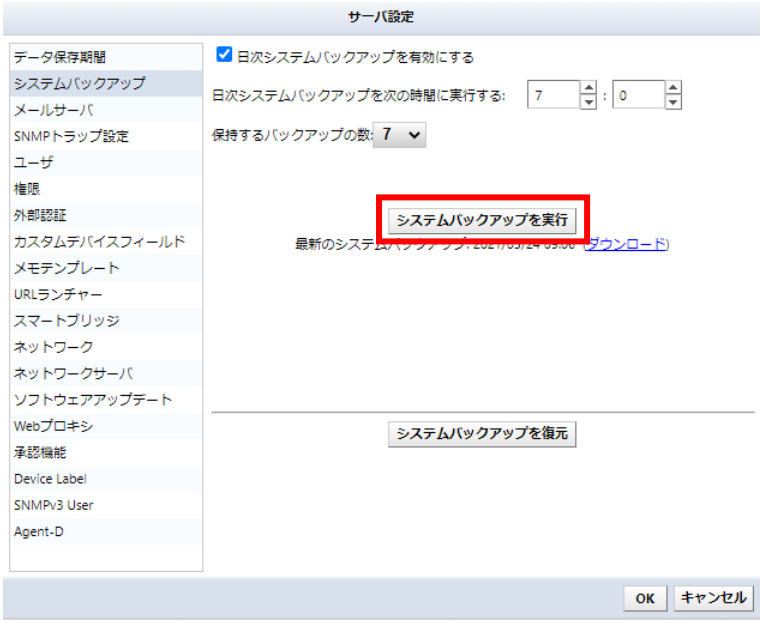
自動でシステムバックアップを実行する設定は、デフォルトで無効になっています。有効にする場合は、自動でシステムバックアップを実行する時間を変更する場合には、以下の赤枠の内容を変更します。

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）

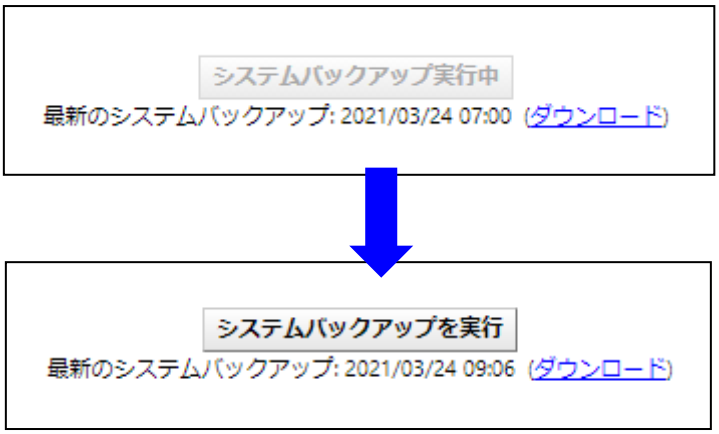
Copyright (C) 2026 LogicVein, Inc.

9.2　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。



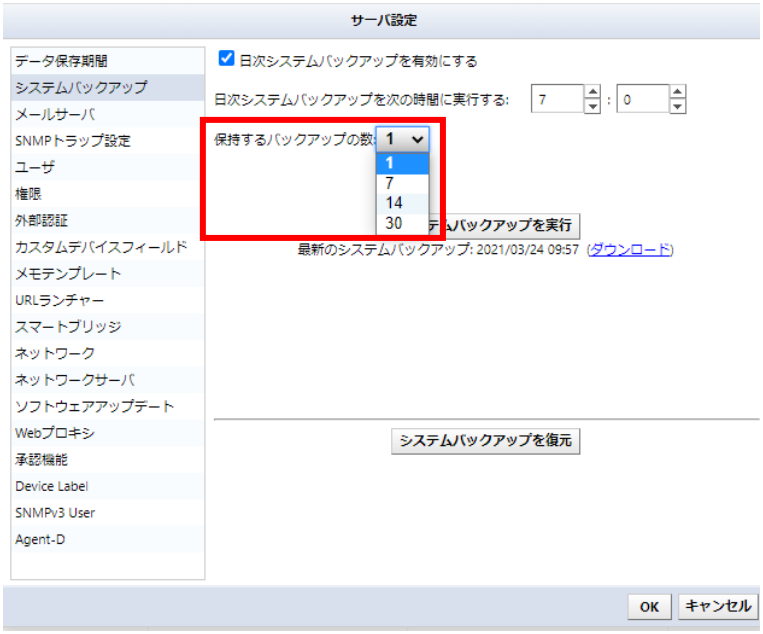
Copyright (C) 2026 LogicVein, Inc.

9.3　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。リビジョン 20240131.0749 以降では、ローカルに保存されるシステムバックアップの数は「1」に制限されます。

システムバックアップを外部サーバに保存する場合、[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、保持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。



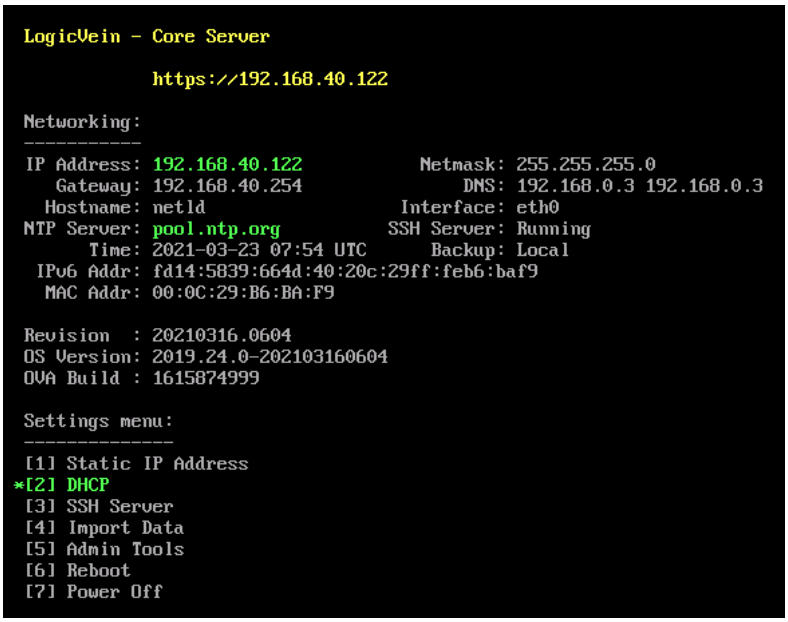
Copyright (C) 2026 LogicVein, Inc.

9.4　外部ストレージに保存する

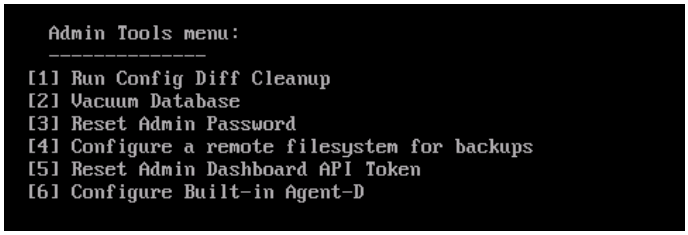
デフォルトでは、システムバックアップファイルは仮想アプライアンス内部に保存されますが、外部ストレージを設定することで仮想アプライアンスの外部に自動的に保存することができます。対応プロトコルは NFS/SMB です。

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。



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。



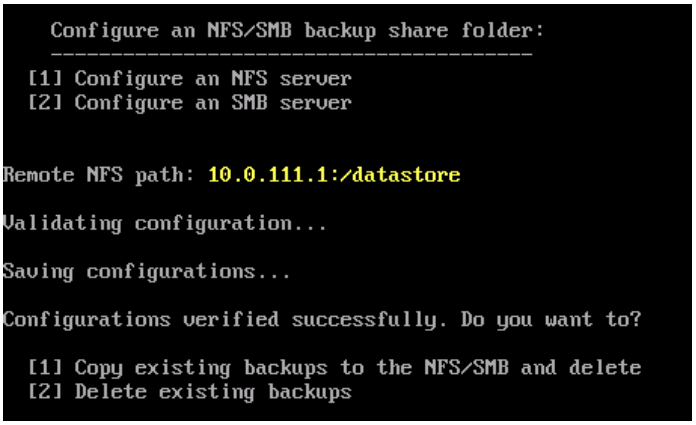
3. サーバの種類を選択します。

4. 必要な情報を入力し、「Enter」キーを押します。

Copyright (C) 2026 LogicVein, Inc.

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

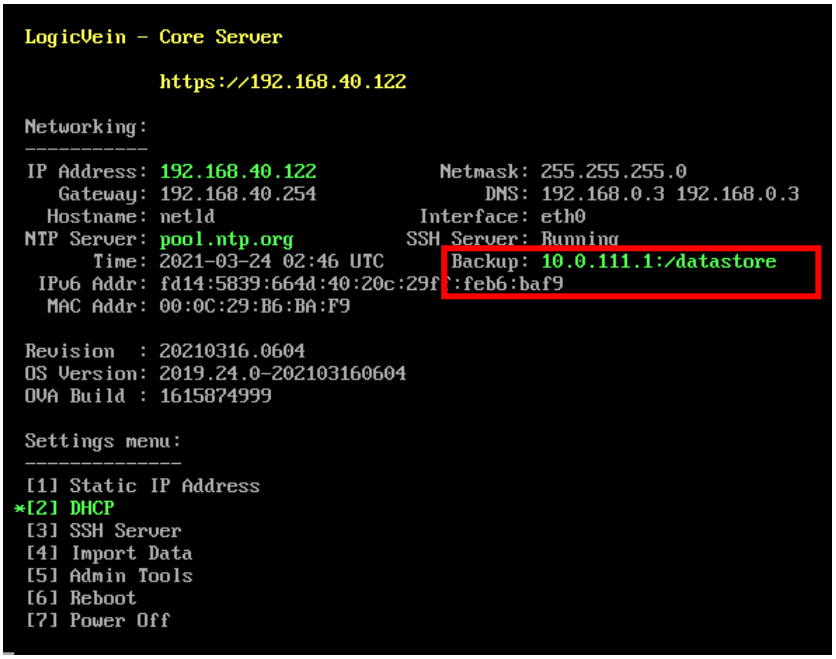
5. 以下を選択します。



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。



Copyright (C) 2026 LogicVein, Inc.

9.5　システムバックアップを ZIP ファイルにする

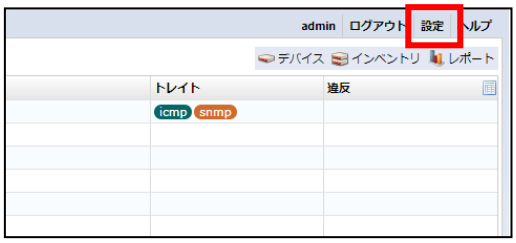
システムバックアップを外部ストレージに保存している場合は、手動で ZIP ファイルを作成する必要があります。

1. バックアップフォルダを開きます。フォルダ名は「backup_YYYY¥MM¥DD」の形式になっています。
2. 次の 3 つのファイル/フォルダを 1 つの ZIP ファイルにまとめます。
   - pgsql（フォルダ）
   - complete（ファイル）
   - version.txt（ファイル）

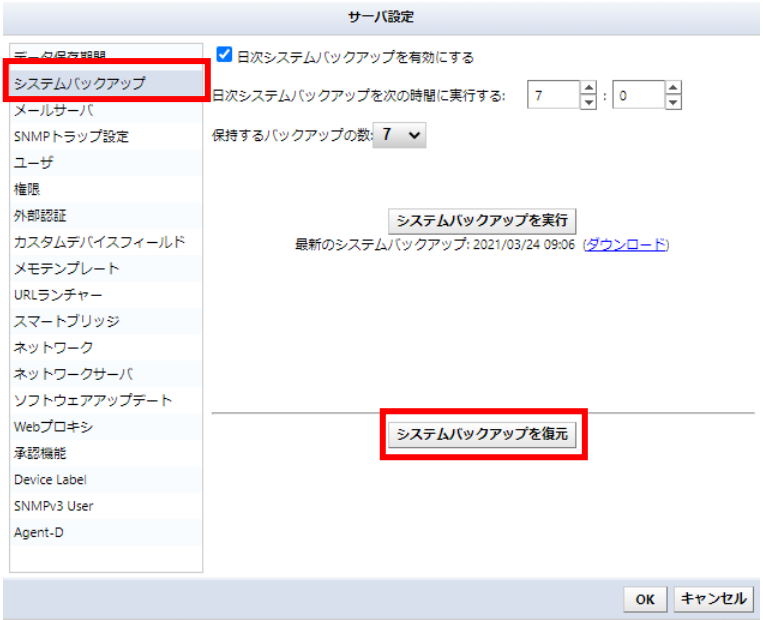
9.6　システムバックアップを復元する

復元を行うには、バックアップ元とリストア先のバージョン（リビジョン）が同一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、「7.8.3.16 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。

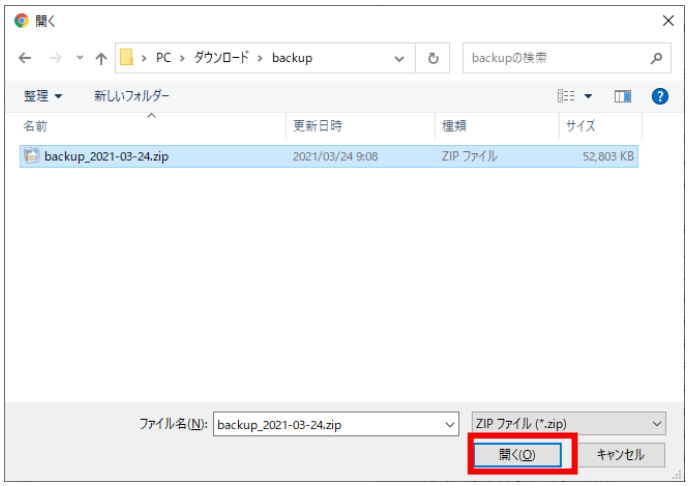


3. ［システムバックアップ］から［システムバックアップを復元］をクリックします。

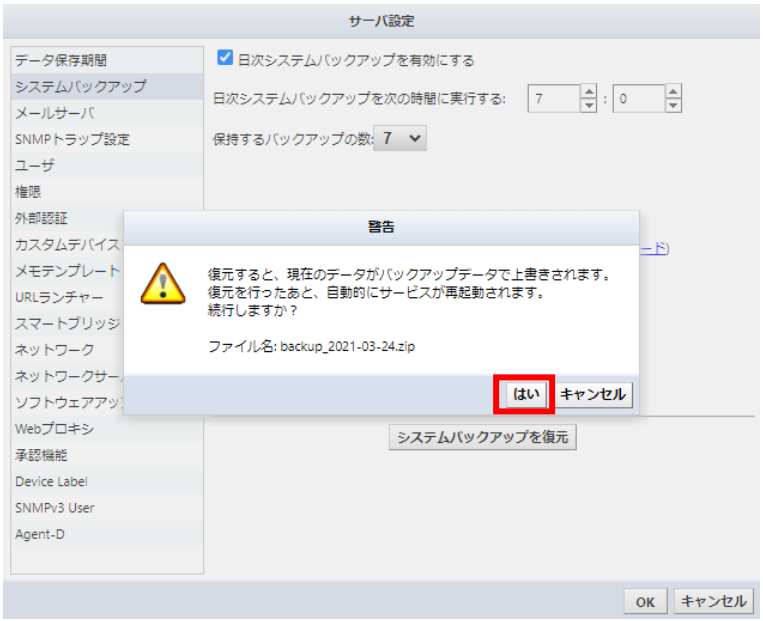


Copyright (C) 2026 LogicVein, Inc.

4. 復元するファイルを選択し、［開く］をクリックします。

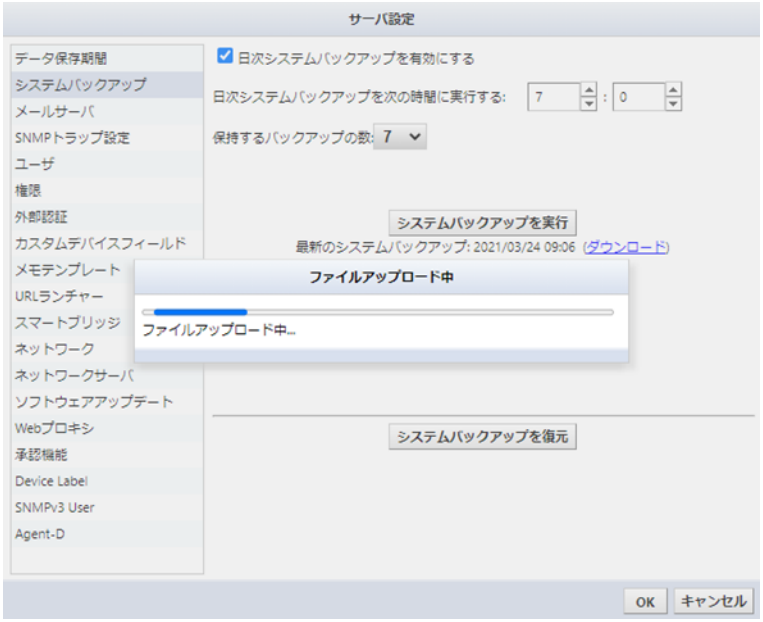


5. 警告メッセージが表示された場合は、内容を確認し、［はい］をクリックします。



Copyright (C) 2026 LogicVein, Inc.

6. ファイルがアップロードされ、復元処理が自動的に開始されます。



以上で操作は完了です。アップロード後、サービスが自動的に再起動し、ログイン画面が表示されます。

Copyright (C) 2026 LogicVein, Inc.

10. 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。

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】

【シャットダウン】

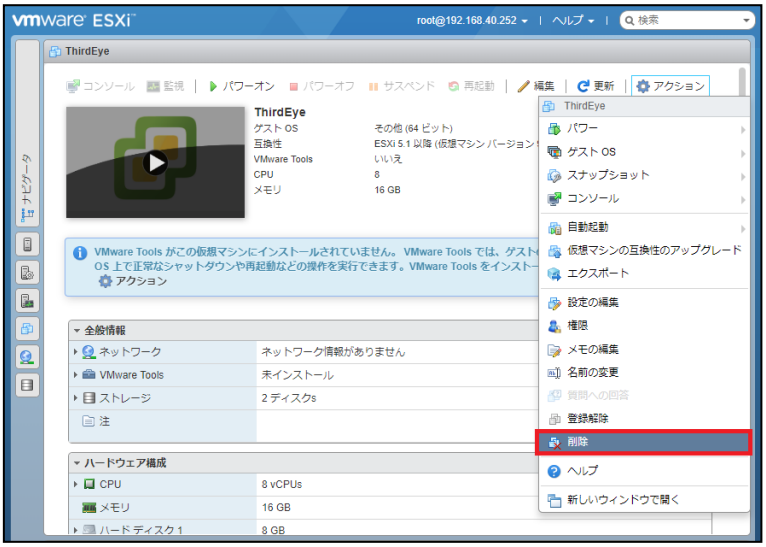
Copyright (C) 2026 LogicVein, Inc.

11. アンインストール

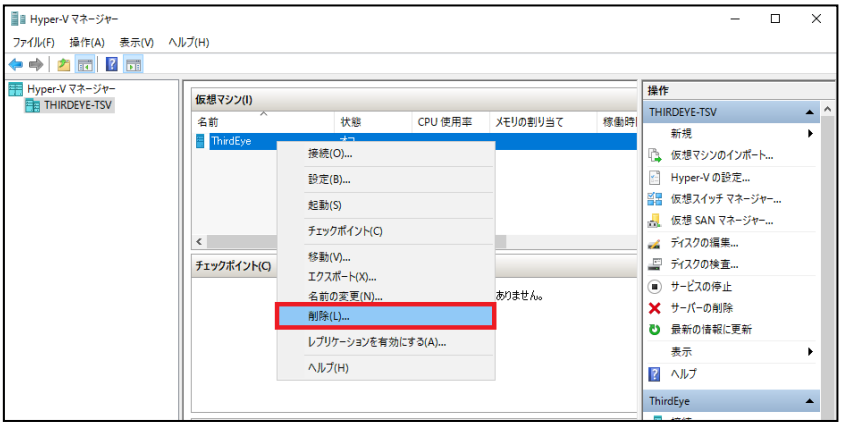
11.1 アンインストールする

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。

Copyright (C) 2026 LogicVein, Inc.

12. 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■

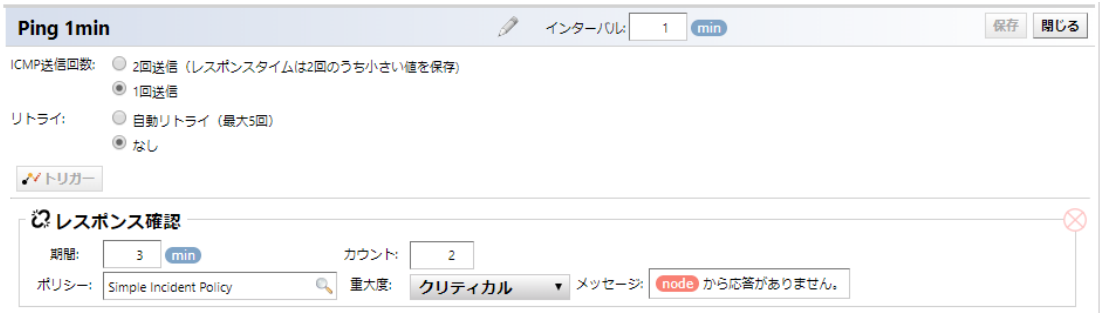
- 株式会社ロジックベイン　サポート窓口
- 電話　　：044-871-4010
- メール　：support@lvi.co.jp
- 受付時間：平日 9:00～12:00／13:00～17:00 （※土・日・祝日および弊社休業日を除く）

Copyright (C) 2026 LogicVein, Inc.

13. 巻末資料

13.1 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。



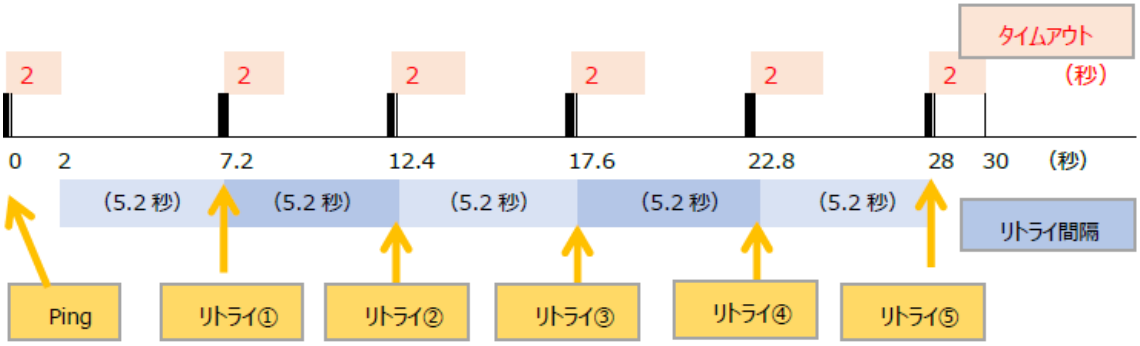
項目	説明	
インターバル	ICMP モニターのポーリング間隔	
ICMP 送信回数	ICMP パケットの送信回数を、次の中から選択する。	
	2 回送信	ICMP パケットを 2 回送信する。 ※ICMP モニターで監視可能な「roundTripTime」(レスポンスタイム)は、2 回のうち小さい値が保存される。
	1 回送信	ICMP パケットを 1 回送信する。
リトライ	ICMP 送信回数とは別に、リトライを実行するかを選択する。	
	自動リトライ	ICMP 送信回数に対して応答がない場合、自動リトライアルゴリズムが開始される。自動リトライは 5 回実施される。リトライ間隔は、モニター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。

Copyright (C) 2026 LogicVein, Inc.

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



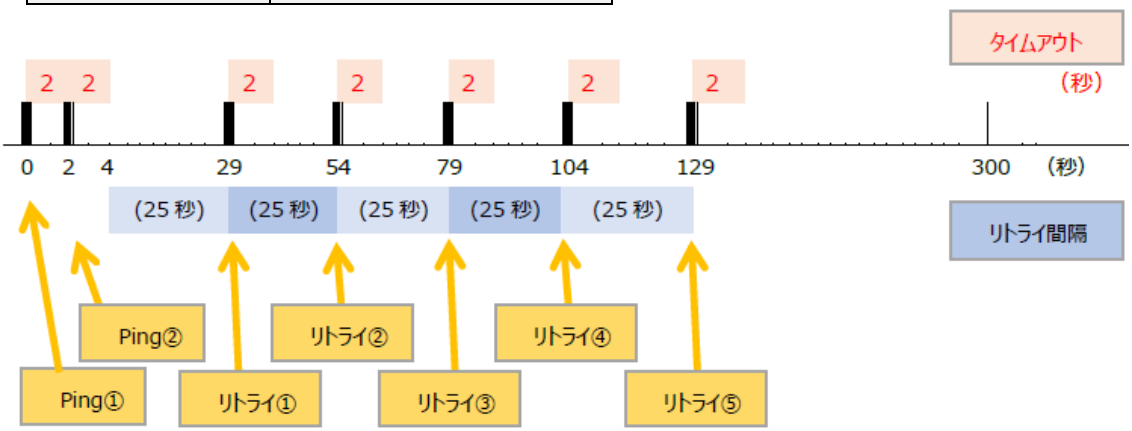
【説明①】

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）、リトライが 5 回実行されます。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



【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、リトライが 5 回実行されます。

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。

Copyright (C) 2026 LogicVein, Inc.

■アラート発生までの所要時間

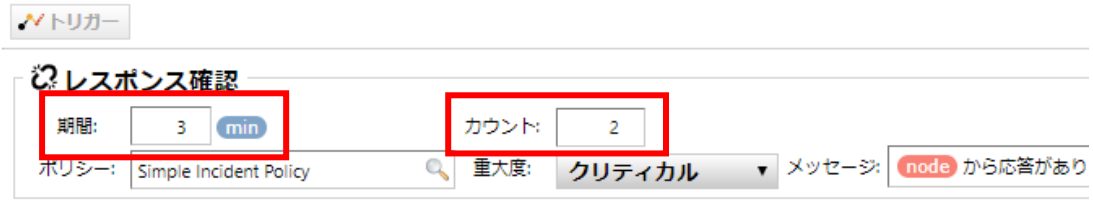
理論値：30 秒（2+5.2*5+2）

※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]



※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、パケットロスの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]

Copyright (C) 2026 LogicVein, Inc.

13.2 スマートブリッジ（オプション）

ThirdEye は、スマートブリッジとコアサーバ間の接続に、以下の 2 つのモードをサポートしています。

- ブリッジ→サーバ モード
- サーバ→ブリッジ モード

いずれのモードでも、通信は HTTPS を使用して行われるため、通信内容はすべて暗号化されます。

ブリッジ→サーバ モード（デフォルト）

このモードでは、スマートブリッジ側からコアサーバへ接続を開始します。コアサーバがスマートブリッジに対して接続を開始することはありません。

スマートブリッジは、社内ネットワークの外、あるいはパブリックネットワーク上に設置されることが多く、多くの場合ファイアウォールの内側にあります。セキュリティ上の理由から、外部からの着信接続を許可することに慎重な組織も多いため、このモードではスマートブリッジ側のファイアウォールに穴を開ける必要がありません（HTTPS のアウトバウンド通信が可能であれば動作します）。ファイアウォール管理者による設定変更は不要です。

サーバ→ブリッジ モード

このモードは、コアサーバがスマートブリッジに対して接続を開始する構成であり、主にファイアウォールのない社内ネットワーク（LAN/WAN）での利用に適しています。スマートブリッジはコアサーバに対して接続を開始しません。

なお、コアサーバとスマートブリッジの間にファイアウォールが存在する場合は、コアサーバからの着信接続（HTTPS）を許可する設定が必要です。

トークン

スマートブリッジをコアサーバに登録すると、ユニークなトークン（接続トークン）が自動的に生成されます。

ブリッジ→サーバ モードでは、スマートブリッジがこのトークンを提示しない限り、コアサーバは接続を受け付けません。これにより、不正な接続を防止できます。

サーバ→ブリッジ モードでも、トークンなしで接続することは可能ですが、セキュリティ上の観点から、トークンの使用を強く推奨します。

13.2.1 スマートブリッジのインストール

スマートブリッジのインストール手順は、コアサーバのインストール手順とほぼ同一です。異なるのは使用するファイル名のみです。

【例】:

- コアサーバ： lvi-core-2024.03.0-202406180814-appliance.ova
- スマートブリッジ： lvi-bridge-2024.03.0-202406180814-appliance.ova

インストール手順は「2 インストール」を、ネットワーク設定については「ネットワークを設定する」を参照してください。

Copyright (C) 2026 LogicVein, Inc.

13.2.2 スマートブリッジをコアサーバに登録する

スマートブリッジをコアサーバに登録すると、接続トークンが自動的に生成されます。

1. Administrator 権限でコアサーバにログインし、［設定］をクリックします。
2. 左側のメニューから［スマートブリッジ］を選択し、［+］をクリックします。
3. スマートブリッジの名前を入力します。
4. 接続モードを選択します。「サーバ→ブリッジ」を選択した場合は、スマートブリッジの IP アドレスとポート番号も入力します。
5. ［OK］をクリックします。
6. 登録後、スマートブリッジ一覧の下に表示される「トークン」をコピーします。
7. ［OK］をクリックします。

登録が完了したら、スマートブリッジ側にコアサーバ情報とトークンを設定します。

13.2.3 スマートブリッジ側の設定

スマートブリッジには Web コンソールがありません。OVA コンソールを使って設定を行います。

1. コンソール画面でキーボードの「4」を押し、「SmartBridge Direction」を選択します。

2. 以下の情報をキーボードで入力し、「Enter」で確定します。

項目	説明	入力例
Bridge initiated or server initiated	接続方向 B：Bridge→Server（トークン使用） S：Server→Bridge（トークン使用） A：Server→Bridge（トークン未使用）	 B S A
Hostname or IP address	コアサーバの IP アドレス	192.168.0.1
Port	コアサーバの HTTPS ポート	443
SmartBridge authentication token	スマートブリッジ登録時に生成された接続トークン	（貼り付け）

設定完了後、サービスは自動的に再起動し、初期画面に戻ります。

Copyright (C) 2026 LogicVein, Inc.

13.2.4 スマートブリッジ経由でのデバイス管理

スマートブリッジ経由でデバイスを管理するには、「ネットワーク」機能を使用します。対象のデバイスが含まれるネットワークにスマートブリッジを割り当てることで、そのスマートブリッジ経由での監視・管理が可能になります。

1. ［設定］をクリックします。
2. 左側メニューから［ネットワーク］を選択し、［+］をクリックします。
3. ネットワーク名を入力し、［ブリッジホスト］に割り当てるスマートブリッジを選択します。
4. ［OK］をクリックして設定を保存します。

保存後、グローバルメニューのネットワーク選択ドロップダウンに、新しく追加されたネットワークが表示されます。そのネットワークを選択すると、［デバイス］タブのインベントリがそのネットワークに対応する内容に切り替わります。このネットワークに登録されたデバイスは、選択したスマートブリッジを通じて監視・管理されます。

Copyright (C) 2026 LogicVein, Inc.

13.3 マルチテナント環境における管理ネットワーク制限

管理ネットワークは、IP アドレス範囲や拠点などの条件に基づいて、デバイスを論理的に分類するための機能です。この仕組みは、1 つのプラットフォームで複数の顧客を管理する MSP（マネージドサービスプロバイダ）に特に有効です。

マルチテナント環境では、MSP がすべての顧客ネットワークを一元的に可視化・管理しつつ、個々の顧客には自社ネットワークのみにアクセスを許可したいというケースがよくあります。

このような要件に対応するため、管理ネットワークへのアクセスをユーザ単位で制限することができます。ユーザにネットワーク制限を適用することで、他の顧客のネットワークやデバイスの閲覧・操作をできないようにし、データの分離とセキュリティを維持しながら、集中管理を実現できます。

この構成は、1 つのプラットフォーム上で複数の顧客を安全かつ効率的に管理する必要がある組織に最適です。

Copyright (C) 2026 LogicVein, Inc.