AX-Collector ユーザーズガイド

SOFT-AM-2382

■対象製品

このマニュアルは，AX-Collector Version1.15 以降の操作・インストール方法について記載しています。

■輸出時の注意

本製品を輸出される場合には，外国為替及び外国貿易法の規制ならびに米国の輸出管理規則など外国の輸出関連法規をご確認のうえ，必要な手続きをお取りください。
なお，不明な場合は，弊社担当営業にお問い合わせください。

■商標一覧

Linux は，Linus Torvalds 氏の日本およびその他の国における登録商標または商標です。
Red Hat，Red Hat Enterprise Linux は米国およびその他の国において Red Hat, Inc.の登録商標または商標です。
MIRACLE LINUX の名称およびロゴは，ミラクル・リナックス株式会社が使用権許諾を受けている登録商標です。
Docker は，Docker, Inc.の米国およびその他の国における商標または登録商標です。
NetFlow は米国およびその他の国における米国 Cisco Systems, Inc.の登録商標です。
Firefox は，Mozilla Foundation の登録商標です。
Google Chrome は，Google Inc.の登録商標です。
Impulse は，ブレインズテクノロジー株式会社の登録商標です。
Office 365，Outlook，Microsoft teams は，Microsoft Corporation の米国及びその他の国における商標または登録商標です。
Zoom は，Zoom Video Communications, Inc.の商標または登録商標です。
FortiGate は，フォーティネット社の登録商標です。
MaxMind，MMDB，GeoIP は MaxMind, Inc.の登録商標です。
そのほかの記載の会社名，製品名は，それぞれの会社の商標あるいは登録商標です。

■マニュアルはよく読み，保管してください。

製品を使用する前に，安全上の説明をよく読み，十分理解してください。
このマニュアルは，いつでも参照できるよう，手近な所に保管してください。

■ご注意

このマニュアルの内容については，改良のため，予告なく変更する場合があります。

■発行

２０２５年１２月　（第 17 版）　SOFT-AM-2382

変更内容

表　第 17 版改訂版の変更内容

章・節・項・タイトル	追加・変更内容
2.2.1 実行環境	・「表 2-2 ソフトウェア環境」についての記載を変更しました。
2.2.2 AX-Collector で使用可能なウェブブラウザ	・「表 2-3 使用可能なウェブブラウザ」を更新しました。
2.3 収容条件	・「2.3.5 Email 通知」を追加しました。
2.4 使用上の注意	・「2.4.1 使用文字について」を追加しました。
3.2.2 本製品のインストール	・「表 3-4 AX-Collector インストール時の設定項目一覧」を更新しました。
3.4.3 アップデートの準備	・「(2) 設定ファイルの更新」に Syslog 受信機能利用時の設定を追記しました。
4.1.6 コレクタ接続環境の設定	・「(4) Email 通知（任意）」を追加しました。
4.1.8 データ管理の設定	・ロギング情報を追記しました。
4.2.3 IP フロー複合ビューによる可視化	・「表 4-3 IP フロー複合ビューで表示可能な集計対象」に TCP パケットロス回数割合等を追加しました。 ・「表 4-5 IP フロー複合ビューのフィールドフィルタ」に ICMP タイプ等を追加しました。
4.2.4 フローデータ拡張の設定	・GEOIP 連携機能を追記しました。
4.3 SNMP 監視機能（閾値監視,Impulse 連携）の設定	・「4.3.2 監視設定」に Email 通知を追記しました。
4.4 フロー監視機能（閾値監視,Impulse 連携）の設定	・「4.4.2 監視設定」に Email 通知を追記しました。 ・「表 4-6 フロー監視 指定可能なユニーク数」に ICMP タイプ等を追加しました。 ・「表 4-7 フロー監視 指定可能な集計対象と集計奉納の組み合わせ」に TCP パケットロス回数割合等を追加しました。
4.5 フローランキング監視機能（閾値監視）の設定	・「4.5.2 監視設定」に Email 通知を追加しました。 ・「表 4-8 フローランキング監視 指定可能な集計対象と集計方法の組み合わせ」に TCP パケットロス回数割合等を追加しました。
4.6 外部データ監視機能（閾値監視,Impulse 連携）の設定	・「4.6.2 監視設定」に Email 通知を追記しました。
4.9 Syslog 受信機能の設定	・本節を追加しました。
4.10 GeoIP 連携機能の設定	・本節を追加しました。
4.9 AX-Collector の保守コマンド	・「(19) GEOIP 連携設定」を追加しました。 ・「(20) Syslog 受信機能設定」を追加しました。
5.2 AX-Collector の Web インタフェース機能一覧	・「表 5-2 AX-Collector の機能一覧」を更新しました。

章・節・項・タイトル	追加・変更内容
5.4.1 ダッシュボード	・「表 5-10 ダッシュボード 監視状況俯瞰ビューの概要」を更新しました。 ・「(9) 監視状況俯瞰ビュー一括エクスポート」を追加しました。 ・「(10) MAP ビュー」を追加しました。
5.4.5 フローランキング監視	・「表 5-29 フローランキング監視収集データの概要」にデータ数分析を追記しました。
5.4.7 Syslog	・本節を追加しました。
5.5 データ監視設定	・以下に Email 通知を追加しました。 「表 5-41 SNMP 監視項目の概要」 「表 5-43 環境設定の概要」 「表 5-46 フロー監視項目の概要」 「表 5-48 環境設定の概要」 「表 5-52 フローランキング監視項目の概要」 「表 5-54 環境設定の概要」 「表 5-58 外部データ監視項目の概要」 「表 5-60 環境設定の概要」
5.6.1 可視化エイリアス情報	・「表 5-66 管理・設定 可視化エイリアス情報の概要」に拡張設定を追記しました。
5.6.3 コレクタ接続環境	・「(3) Email 通知先」を追加しました。 ・「(6) Syslog 受信設定」を追加しました。
5.6.5 管理	・「(2)データ管理」にロギング情報を追加しました。 ・「(7)フローデータ拡張」に GEOIP 連携機能を追加しました。
5.6.6 保守	・「(4)保守情報」「表 5-103 コレクタ統計情報の概要」を更新しました。
5.9 検索	・「表 5-118 検索ウィンドウの概要（GEOIP 情報）」を追加しました。
7.3 IP フロー情報検索 API	・フィルタ条件に ICMP タイプ等,集計対象に TCP パケットロス回数割合等を追加しました。
8.1 トラブル発生時の対応	・「表 8-1 現象と対応」に，「12. AX-Collector の画面で，記号文字（¥，“等）が検索できない。」を追記しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

表　第 16 版改訂版の変更内容

章・節・項・タイトル	追加・変更内容
2.1 ハードウェア構成	・「表 2-1 動作スペック」を更新しました。
2.2.2 AX-Collector で使用可能なウェブブラウザ	・「表 2-3 使用可能なウェブブラウザ」を更新しました。
3.2.1 前提ソフトウェアのインストール	・「表 3-3 前提ソフトウェア」を更新しました。
3.2.2 本製品のインストール	・「表 3-4 AX-Collector インストール時の設定項目一覧」を更新しました。

章・節・項・タイトル	追加・変更内容
4.5.3 フローランキング監視の集計対象	・「表 4-8 フローランキング監視 指定可能な集計対象と集計方法の組み合わせ」の TCP 再送割合の注釈を削除しました。
5.4.2 フローランキングリスト	・「表 5-14 フローランキングリスト IP フローおよび MAC フローの概要」の TCP 再送割合の注釈を削除しました。
5.6.6 保守	・「(4)保守情報」にコレクタ統計情報の記載を追記しました。
5.8.1 検知状況	・「表 5-105 Impulse 連携 検知情報の概要」を更新しました。 ・「(3) 検知一覧」並び順保存の記載を更新しました。
5.9 検索	・「表 5-107」検索ウィンドウの概要（フロー情報）」注釈を更新しました。
8.1 トラブル発生時の対応	・「表 8-1 現象と対応」に，原因「データベースのストレージ容量不足」を追記しました。
付録	・謝辞を更新しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

表　第 15 版改訂版の変更内容

章・節・項・タイトル	追加・変更内容
1.1.3 主な特徴機能	・「(2)異常検知機能」に記載を追加しました。
2.2.1 実行環境	・「表 2-2 ソフトウェア環境」についての記載を変更しました。
2.3 収容条件	・「2.3.8 検知情報」を追加しました。
3. インストール	・コマンド実行例を更新しました。
4.2.3 IP フロー複合ビューによる可視化	・「表 4.5 IP フロー複合ビューのフィールドフィルタ」を更新しました。
4.4.3 フロー監視の集計対象	・「表 4.6 フロー監視 指定可能なユニーク数」を更新しました。
4.9 AX-Collector の保守コマンド	・コマンド実行例を更新しました。 ・「検知データの一括削除」を削除しました。
5.2 AX-Collector の Web インタフェース機能一覧	・「表 5-2 AX-Collector の機能一覧」を更新しました。
5.5.1 SNMP 監視	・「表 5-35 MIB オブジェクトグループの概要」を更新しました。 ・「表 5-38 環境設定」を更新しました。

章・節・項・タイトル	追加・変更内容
5.5.2 フロー監視	・「表 5-40 フロー条件グループの概要」を更新しました。 ・「表 5-43 環境設定」を更新しました。 ・「(6)過去データ／閾値生成・削除」に見出しを変更しました。 ・「表 5-44 過去データ／閾値生成・削除の概要」の見出しを変更し，内容を更新しました。 ・「表 5-45 閾値生成パラメータの概要」を追加しました。 ・「表 5-46 閾値詳細の概要」を追加しました。
5.5.3 フローランキング監視	・「表 5-47 フローランキング監視項目の概要」を更新しました。
5.5.4 外部データ監視	・「表 5-52 外部監視データの概要」を更新しました。 ・「表 5-55 環境設定の概要」を更新しました。
5.6.5 管理	・「(10)検知情報管理」を追加しました。
5.8.1 検知状況	・「(3)検知一覧」を更新しました。
7.3 IP フロー情報検索 API	・「表 7-10 IP フローバイト数ランキング取得 API」を更新しました。 ・「表 7-11 IP フローパケット数ランキング取得 API」を更新しました。 ・「表 7-12 IP フローバイト数時系列取得 API」を更新しました。 ・「表 7-12 IP フローパケット数時系列取得 API」を更新しました。
付録	・謝辞を更新しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

表　第 14 版改訂版の変更内容

章・節・項・タイトル	追加・変更内容
1.1 概要	・フォーティネット社 FortiGate の NAT ログ情報可視化の記載を追加しました。
2.2 AX-Collector で使用可能なウェブブラウザ	・「表 2-3 使用可能なウェブブラウザ」の Firefox に関する記述を変更しました。
4.2.3 IP フロー複合ビューによる可視化	・「表 4-3 IP フロー複合ビューで表示可能な集計対象」に NAT 関連情報等を追加しました。 ・「表 4-5 IP フロー複合ビューのフィールドフィルタ」に NAT 関連情報等を追加しました。
4.4.3 フロー監視の集計対象	・「表 4-6 フロー監視 指定可能なユニーク数」に NAT 関連情報等を追加しました。 ・「表 4-7 フロー監視 指定可能な集計対象と集計方法の組み合わせ」に NAT 関連情報等を追加しました。
4.5.3 フローランキング監視の集計対象	・「表 4-8 フローランキング監視 指定可能な集計対象と集計方法の組み合わせ」に NAT 関連情報等を追加しました。

章・節・項・タイトル	追加・変更内容
5.2 AX-Collector の Web インタフェース機能一覧	・「表 5-2 AX-Collector の機能一覧」を更新しました。
5.4.1 ダッシュボード	・「表 5-5 ダッシュボード カスタマイズダッシュボードの概要」を更新しました。
5.4.2 フローランキングリスト	・「表 5-14 フローランキングリスト IP フローおよび MAC フローの概要」を更新しました。 ・「表 5-15 IP フロー複合ビューの概要」を更新しました。
5.5.4 外部データ監視	・「表 5-53 環境設定の概要」を更新しました。
5.6.5 管理	・「表 5-72　管理 ユーザ管理の概要」に REST API の記載を追加しました。
5.8.2 検知通知一覧（機能別）	・見出し名を変更しました。
5.9 検索	・フロー情報の検索機能の記載を追加しました。
7 REST API	・「7.1 認証」を追加しました。 ・各 API の説明にトークン認証に関する記載を追加しました。 ・「7.2.2 外部データ監視 外部収集データ設定 API」の記載を追加しました。 ・「7.3 IP フロー情報検索 API」に NAT 関連情報等のパラメータを追加しました。 ・「7.4 MAC フロー情報検索 API」に，タイムスタンプ，送信ポート ifIndex のパラメータを追加しました。

表　第 13 版改訂版の変更内容

章・節・項・タイトル	追加・変更内容
2.2.1 実行環境	・「表 2-2 ソフトウェア環境」についての記載を変更しました。
2.2.2 AX-Collector で使用可能なウェブブラウザ	・「表 2-3 使用可能なウェブブラウザ」の Firefox に関する記述を変更しました。
2.3. 収容条件	・「2.3.1 フローランキングリスト」，「2.3.2 フローランキング監視機能」を追加しました。
3.1.4 本製品に含まれるファイル	・「表 3-2 AX-Collector のプログラムに含まれるファイル」の記載を変更しました。
3.2.2 本製品のインストール	・実行コマンド画面例を更新しました。
3.3 本製品のアンインストール	・実行コマンド画面例を更新しました。
4.2.3 IP フロー複合ビューによる可視化	・「表 4-3 IP フロー複合ビューで表示可能な集計対象」に UDP 情報を追加しました。 ・「表 4-4 IP フロー複合ビューの集約条件指定方法」に UDP 情報を追加しました。TCP フラグ情報を統合しました。

章・節・項・タイトル	追加・変更内容
4.4.3 フロー監視の集計対象	・「表 4-6 フロー監視 指定可能なユニーク数」にフローセット ID，UDP 情報を追加しました。 ・「表 4-7 フロー監視 指定可能な集計対象と集計方法の組み合わせ」に UDP 情報を追加しました。
4.5 フローランキング監視機能（閾値監視）の設定	・本節を追加しました。
4.8 冗長化機能の設定	・フローランキング機能の記載を追記しました。
4.9.1 ユーティリティコマンド	・「(13)フローランキング監視機能の開始・停止」を追加しました。 ・「(16)検知データの一括削除」にフローランキング監視機能を追記しました。
5 AX-Collector の Web インタフェース	・節番号を変更しました。「変更前」：5.5 検知，5.6 データ監視設定，5.7 ブックマーク，5.8 管理・設定，「変更後」：5.5 データ監視設定，5.6 管理・設定，5.7 ブックマーク，5.8 検知
5.1 AX-Collector の画面構成	・「図 5-1 画面構成」を更新しました。 ・「表 5-1 構成要素」を更新しました。
5.2 AX-Collector の Web インタフェース機能一覧	・「表 5-2 AX-Collector の機能一覧」を更新しました。
5.4.1 ダッシュボード	・「表 5-5 ダッシュボード カスタマイズダッシュボードの概要」を更新しました。 ・「表 5-6 ダッシュボード カスタマイズダッシュボード 画面編集モード 追加の概要」を更新しました。 ・「表 5-8 ダッシュボード 個別ビューの概要」を更新しました。 ・「表 5-10 ダッシュボード 監視状況俯瞰ビューの概要」を更新しました。
5.4.2 フローランキングリスト	・「表 5-14 フローランキングリスト IP フローおよび MAC フローの概要」を更新しました。 ・「表 5-15 IP フロー複合ビューの概要」を更新しました。
5.4.5 フローランキング監視	・本節を追加しました。
5.5.1 SNMP 監視	・「表 5-32 ネットワーク機器の概要」，「表 5-33 MIB オブジェクトの概要」，「表 5-34 MIB オブジェクトグループの概要」，「表 5-35 SNMP 監視項目の概要」を更新しました。 ・「表 5-37 環境設定の概要」を更新しました。
5.5.2 フロー監視	・「表 5-38 フロー条件の概要」，「表 5-39 フロー条件グループの概要」，「表 5-40 フロー監視項目の概要」を更新しました。 ・「表 5-41 一括登録・更新の概要」を更新しました。 ・「表 5-42 環境設定の概要」を更新しました。
5.5.3 フローランキング監視	・本節を追加しました。

章・節・項・タイトル	追加・変更内容
5.5.4 外部データ監視	・「表 5-48 外部収集データの概要」，「表 5-49 外部監視データの概要」，「表 5-50 外部データ監視項目の概要」を更新しました。 ・「表 5-52 環境設定の概要」を更新しました。
5.6.3 コレクタ接続環境	・「表 5-61 コレクタ接続環境 コレクタの概要」を更新しました。 ・「表 5-64 コレクタ接続環境 AX-NM 連携環境設定の概要」を更新しました。
5.6.5 管理	・「表 5-68 管理 データ管理の概要」を更新しました。 ・「表 5-69 データ種別とインデックスの一覧」を更新しました。
5.6.6 保守	・「表 5-83 保守 運用ログの概要」を更新しました。
5.7 ブックマーク	・「表 5-90 画面名称指定 URL 対象画面一覧」を更新しました。
5.8.1 検知状況	・「表 5-91 検知数カレンダーの概要」，「表 5-92 検知数ランキングの概要」，「表 5-93 検知一覧」を更新しました。 ・「表 5-96 フローランキング監視 閾値監視通知の概要」を追加しました。
5.8.2 検知一覧	・閾値監視通知（フローランキング）を追加しました。
7.1.2 SNMP 監視 CSV データ取得 API	・「表 7-2 SNMP 監視 CSV データ取得 API」に時刻指定パラメータを追加しました。
7.1.3 フロー監視 CSV データ取得 API	・「表 7-3 フロー監視 CSV データ取得 API」に時刻指定パラメータを追加しました。
7.1.4 外部データ監視 CSV データ取得 API	・「表 7-4 外部データ監視 CSV データ取得 API」に時刻指定パラメータを追加しました。
7.2 IP フロー情報検索 API	フローセット ID，UDP 情報のパラメータを追加しました。 ・「表 7-5 IP フロー バイト数ランキング取得 API」 ・「表 7.6 IP フロー パケット数ランキング取得 API」 ・「表 7-7 IP フロー バイト数時系列データ取得 API」 ・「表 7-8 IP フロー パケット数時系列データ取得 API」
7.3 MAC フロー情報検索 API	フローセット ID のパラメータを追加しました。 ・「表 7-9 MAC フロー バイト数ランキング取得 API」 ・「表 7-10 MAC フロー パケット数ランキング取得 API」 ・「表 7-11 MAC フロー バイト数時系列データ取得 API」 ・「表 7-12 MAC フロー パケット数時系列データ取得 API」
8.1 トラブル発生時の対応	・「表 8-1 現象と対応」8 を更新しました。

表　第 12 版改訂版の変更内容

章・節・項・タイトル	追加・変更内容
2.3.5 可視化エイリアス情報	・「表 2-8 可視化エイリアス情報に関する収容条件」に IPv6 の項目を追加しました。
3.2.2 本製品のインストール	・「表 3-4 AX-Collector インストール時の設定項目一覧」に画像管理の設定項目を追加しました。
3.2.3 インストール時の注意事項	・「表 3-6 除外ディレクトリ」に除外ディレクトリを追加しました。
4.2.1 カスタマイズダッシュボードの作成	・画像，テキスト情報の記載を追加しました。
4.2.3 IP フロー複合ビューによる可視化	・「表 4-4 IP フロー複合ビューで表示可能な集計対象」に TCP 再送割合を追加しました。 ・「表 4-6 IP フロー複合ビューのフィールドフィルタ」に IPv6 アドレス等を追記しました。
4.4.3 フロー監視の集計対象	・「表 4.7 フロー監視 指定可能なユニーク数」に IPv6 アドレス等を追加しました。 ・「表 4.8 フロー監視 指定可能な集計対象と集計方法の組み合わせ」に TCP 再送割合を追加しました。
4.8.1 ユーティリティコマンド	・「（10）リストア」の記載を変更しました。
5.1 AX-Collector の画面構成	・⑩ページリンクの記載を変更しました。
5.2 AX-Collector の Web インタフェース機能一覧	次の記載を追加，変更しました。 ・ブックマーク ブックマーク管理 ・管理・設定 可視化エイリアス情報 ・管理・設定 画像管理 ・保守 アクセスカウンタ ・保守 コンフィグ DB 管理
5.4.1 ダッシュボード	次の記載を追加，変更しました。 ・プリセットダッシュボード ・ダッシュボード ・監視状況俯瞰ビュー
5.4.2 フローランキングリスト	・「表 5-14 フローランキングリスト IP フローおよび MAC フローの概要」の記載を変更しました。
5.7 ブックマーク	・「（3）ブックマーク登録」を追加しました。
5.8.1 可視化エイリアス情報	・IPv6 アドレス等を追記しました。
5.8.3 コレクタ接続環境	・「（1）コレクタ」に検知通知および運用ログ保存上限を追加しました。
5.8.5 管理	・「（5）ユーザ管理」の記載を変更しました ・「（7）フローデータ拡張」の記載を変更しました。 ・「（9）画像管理」を追加しました。
5.8.6 保守	・「（1）運用ログ」に付加情報を追記しました。 ・「（2）アクセスカウンタ」を追加しました。 ・「（3）コンフィグ DB 管理」を追加しました。

章・節・項・タイトル	追加・変更内容
7 REST API	API 毎に節を分割しました。 ・7.1 データ監視関連 API ・7.2 IP フロー情報検索 API ・7.3 MAC フロー情報検索 API
7.1 データ監視関連 API	次の API を追加しました。 ・7.1.2 SNMP 監視 CSV データ取得 API ・7.1.3 フロー監視 CSV データ取得 API ・7.1.4 外部データ監視 CSV データ取得 API
7.2 IP フロー情報検索 API	・URI を追加しました ・API 名称を IPv4⇒IP に変更しました。 ・IPv6 および TCP 再送割合パラメータを追加しました。

表　第 11 版改訂版の変更内容

章・節・項・タイトル	追加・変更内容
1.2.2 使用期間	・ライセンスについての記述を変更しました。
2.2.1 実行環境	・「表 2-2 ソフトウェア環境」についての記載を変更しました。
3.1.2 インストールに関する注意事項	・「(1)インストール実施ユーザの権限」を変更しました。
3.2.2 本製品のインストール	・以下についての記述を変更しました。 「(1) プログラムの展開」 「表 3-5 AX-Collector インストール時の設定項目一覧」
3.4.2 アップデートに関する注意事項	「（2）AX-Sensor を同時にアップデートする場合の注意事項」の記述を追加しました。
4.2.3 IP フロー複合ビューによる可視化	・以下についての記述を変更しました。 「表 4-4 IP フロー複合ビューで表示可能な集計対象」 「表 4-5 IP フロー複合ビューの集約条件指定方法」 ・以下の記述を追加しました。 「表 4-6 IP フロー複合ビューのフィールドフィルタ」
4.2.4 フローデータ拡張の設定	・本節を追加しました。
4.4.3 フロー監視の集計対象	・以下についての記述を変更しました。 「表 4-7 フロー監視 指定可能なユニーク数」 「表 4-8 フロー監視 指定可能な集計対象と集計方法の組み合わせ」
5.1 AX-Collector の画面構成	・「表 5-1 構成要素」の記述を変更しました。
5.2 AX-Collector の Web インタフェース機能一覧	・「表 5-2 AX-Collector の機能一覧」の記述を変更しました。
5.4.1 ダッシュボード	・「表 5-9 ダッシュボード 監視状況俯瞰ビューの概要」の記述を変更しました。

章・節・項・タイトル	追加・変更内容
5.4.2 フローランキングリスト	・「(3) IP フロー複合ビュー」の記述を変更しました。
5.5.1 検知状況	・「(4) 通知詳細」の記述を追加しました。
5.7 ブックマーク	・「表 5-59　ブックマーク管理の概要」の記述を変更しました。
5.8.5 管理	・以下についての記述を変更しました。 「表 5-71 管理 データ管理の概要」 「表 5 74　管理 ユーザ管理の概要」 ・以下の記述を追加しました。 「表 5-72 データ種別とインデックスの一覧」 「(7) フローデータ拡張」 「(8) ページリンク管理」
7.2 IPv4 フロー バイト数ランキング API	・「表 7-2 IPv4 フロー バイト数ランキング取得 API」についての記述を変更しました。
7.3 IPv4 フロー パケット数ランキング API	・「表 7-3 IPv4 フロー パケット数ランキング取得 API」についての記述を変更しました。
7.4 IPv4 フロー バイト数時系列データ API	・「表 7-4　IPv4 フロー バイト数時系列データ取得 API」についての記述を変更しました。
7.5 IPv4 フロー パケット数時系列データ API	・「表 7-5 IPv4 フロー パケット数時系列データ取得 API」についての記述を変更しました。
7.6 MAC フロー バイト数ランキング API	・「表 7-6 MAC フロー バイト数ランキング取得 API」についての記述を変更しました。
7.7 MAC フロー パケット数ランキング API	・「表 7-7 MAC フロー パケット数ランキング取得 API」についての記述を変更しました。
7.8 MAC フロー バイト数時系列データ API	・「表 7-8 MAC フロー バイト数時系列データ取得 API」についての記述を変更しました。
7.9 MAC フロー パケット数時系列データ API	・「表 7-9 MAC フロー パケット数時系列データ取得 API」についての記述を変更しました。

表　第 10 版改訂版の変更内容

章・節・項・タイトル	追加・変更内容
2.2.2 AX-Collector で使用可能なウェブブラウザ	・「表 2-3 使用可能なウェブブラウザ」の Firefox に関する記述を変更しました。
2.3.4 ブックマーク	・「表 2-7 ブックマークに関する収容条件」の記述を変更しました。
4.1.7 Impulse 連携の設定	・Impulse 連携についての記述を変更しました。
4.2.3 遅延情報の可視化	・「表 4-4 フロー複合ビューで表示可能な項目」の表示項目名を変更しました。
4.3 SNMP 監視機能（閾値監視，Impulse 連携）の設定	・SNMP 監視機能についての記述を変更しました。
4.4 フロー監視機能（閾値監視，Impulse 連携）の設定	・フロー監視機能についての記述を変更しました。

章・節・項・タイトル	追加・変更内容
4.4.3 フロー監視の集計対象	・本項を追加しました。
4.5 外部データ監視機能（閾値監視, Impulse 連携）の設定	・外部データ監視機能についての記述を変更しました。
4.8.1 ユーティリティコマンド	・以下の項目についての記述を追加しました。 (14) 冗長化機能の開始・停止 (17) SNMP 監視 送信元ポート番号設定 (18) 監視停止設定
5.2 AX-Collector の Web インタフェース機能一覧	・「表 5-2 AX-Collector の機能一覧」の記述を変更しました。
5.3 TOP	・TOP ページについての記述を変更しました。
5.4.1 ダッシュボード	・以下についての記述を変更しました。 「表 5-4 ダッシュボード 登録一覧の概要」 「表 5-6 ダッシュボード カスタマイズダッシュボードの概要」 「表 5-8 ダッシュボード 個別ビューの概要」 「表 5-9 ダッシュボード 個別ビュー 一括登録・更新の概要」
5.4.2 フローランキングリスト	・以下についての記述を変更しました。 「表 5-13 フローランキングリスト 登録一覧の概要」 「表 5-14 フローランキングリスト IP フローおよび MAC フローの概要」 「表 5-15 IP フロー複合ビューの概要」
5.4.3 SNMP 監視	・以下についての記述を変更しました。 「表 5-16 ネットワーク機器毎 MIB 収集データ詳細の概要」 「表 5-17 MIB オブジェクト詳細の概要」 「表 5-18 SNMP 監視項目毎 監視データ詳細の概要」 「表 5-19 MIB オブジェクトグループ監視データ詳細の概要」
5.4.4 フロー監視	・以下についての記述を変更しました。 「表 5-22 フロー監視項目毎 監視データ詳細の概要」 「表 5-23 フロー条件グループ監視データ詳細の概要」
5.4.5 外部データ監視	・以下についての記述を変更しました。 「表 5-26 外部収集データの概要」 「表 5-27 外部監視項目毎 監視データ詳細の概要」 「表 5-28 外部監視データ詳細の概要」 「表 5-19 MIB オブジェクトグループ監視データ詳細の概要」
5.4.6 Impulse 連携	・本項を削除し 5.6.4 Impulse 連携へ移動しました。

章・節・項・タイトル	追加・変更内容
5.6.1 SNMP 監視	・以下についての記述を変更しました。 「表 5-36 ネットワーク機器の概要」 「表 5-37 MIB オブジェクトの概要」 「表 5-38 MIB オブジェクトグループの概要」 「表 5-38 SNMP 監視項目の概要」 「表 5-40 一括登録・更新の概要」 「表 5-41 環境設定の概要」
5.6.2 フロー監視	・以下についての記述を変更しました。 「表 5-42 フロー条件の概要」 「表 5-43 フロー条件グループの概要」 「表 5-44 フロー監視項目の概要」 「表 5-45 一括登録・更新の概要」 「表 5-46 環境設定の概要」 「表 5-47 過去データ生成・削除の概要」
5.6.3 外部データ監視	・以下についての記述を変更しました。 「表 5-49 外部監視データの概要」 「表 5-52 環境設定の概要」 「表 5-53 過去データ生成・削除の概要」
5.6.4 Impulse 連携	・5.4.6 Impulse 連携から移動した以下の項目を追加しました。 (2) syslog/trap 送信制御状態一覧 (4) Impulse
5.7 ブックマーク	・以下の項目を追加しました (1) ブックマーク管理 (2) ブックマーク一覧
5.8.3 コレクタ接続環境	・以下についての記述を変更しました。 「表 5-64 コレクタ接続環境 コレクタの概要」 「表 5-65 コレクタ接続環境 syslog 通知先の概要」
5.8.5 管理	・(1) コレクタ稼働状況 を追加しました。 ・以下についての記述を変更しました。 「表 5-71 管理 データ管理の概要」 「表 5-73 ユーザ管理の概要」
7.2 IPv4 フロー バイト数ランキング API	・「表 7-2 IPv4 フロー バイト数ランキング取得 API」の記述を変更しました。
7.3 IPv4 フロー パケット数ランキング API	・「表 7-3 IPv4 フロー パケット数ランキング取得 API」の記述を変更しました。
7.4 IPv4 フロー バイト数時系列データ API	・「表 7-4 IPv4 フロー バイト数時系列データ取得 API」の記述を変更しました。
7.5 IPv4 フロー パケット数時系列データ API	・「表 7-5 IPv4 フロー パケット数時系列データ取得 API」の記述を変更しました。
7.6 MAC フロー バイト数ランキング API	・「表 7-6 MAC フロー バイト数ランキング取得 API」の記述を変更しました。

章・節・項・タイトル	追加・変更内容
7.7 MAC フロー パケット数ランキング API	・「表 7-7 MAC フロー パケット数ランキング取得 API」の記述を変更しました。
7.8 MAC フロー バイト数時系列データ API	・「表 7-8 MAC フロー バイト数時系列データ取得 API」の記述を変更しました。
7.9 MAC フロー パケット数時系列データ API	・「表 7-9 MAC フロー パケット数時系列データ取得 API」の記述を変更しました。
8.1 トラブル発生時の対応	・トラブル発生時の対応についての記載を変更しました。

表　第 9 版改訂版の変更内容

章・節・項・タイトル	追加・変更内容
1.1.1 可視化・異常検知ソリューション	・可視化・異常検知ソリューションの概要図を変更しました。
1.1.3 主な特徴機能	・可視化機能についての記述を変更しました。
2.2.1 実行環境	・実行環境についての記述を変更しました。
2.2.2 AX-Collector で使用可能なウェブブラウザ	・「表 2-3 使用可能なウェブブラウザ」の Firefox に関する記述を変更しました。
3.2.2 本製品のインストール	・「表 3-5　AX-Collector インストール時の設定項目一覧」の設定項目を変更しました。
4.2.3 遅延情報の可視化	・本項を追加しました。
4.4.3 遅延情報の監視	・本項を追加しました。
5.1 AX-Collector の画面構成	・画面構成の図を変更しました。 ・構成要素についての記載を変更しました。
5.2 AX-Collector の Web インタフェース機能一覧	・AXCollector の機能一覧を変更しました。
5.4.1 ダッシュボード	・カスタマイズダッシュボードについての記載を変更しました。 ・カスタマイズダッシュボード 一括登録・設定についての記載を追加しました。 ・個別ビューについての記載を変更しました。 ・個別ビュー 一括登録・設定についての記載を追加しました。 ・監視状況俯瞰ビューについての記載を変更しました。 ・監視状況俯瞰ビュー 一括登録・設定についての記載を追加しました。
5.4.2 フローランキングリスト	・IP フロー・MAC フローについての記載を変更しました。 ・IP フロー複合ビューについての記載を追加しました。
5.4.3 SNMP 監視	・SNMP 監視データについての記載を変更しました。

章・節・項・タイトル	追加・変更内容
5.6.1 SNMP 監視	・ネットワーク機器についての記載を変更しました。 ・MIB オブジェクトについての記載を変更しました。 ・MIB オブジェクトグループについての記載を変更しました。 ・SNMP 監視項目についての記載を変更しました。 ・環境設定についての記載を変更しました。
5.6.2 フロー監視	・フロー監視についての記載を変更しました。 ・フロー条件グループについての記載を変更しました。 ・フロー監視項目についての記載を変更しました。 ・環境設定についての記載を変更しました。
5.6.3 外部データ監視	・外部収集データについての記載を変更しました。 ・外部監視データについての記載を変更しました。 ・外部データ監視項目についての記載を変更しました。 ・一括登録・更新についての記載を変更しました。 ・環境設定についての記載を変更しました。
5.8.5 管理	・データ管理についての記載を変更しました。
5.9 検索	・本項を追加しました。
7.2 IPv4 フロー バイト数ランキング API	・本項を追加しました。
7.3 IPv4 フロー パケット数ランキング API	・本項を追加しました。
7.4 IPv4 フローバイト数時系列データ API	・本項を追加しました。
7.5 IPv4 フロー パケット数時系列データ API	・本項を追加しました。
7.6 MAC フロー バイト数ランキング API	・本項を追加しました。
7.7 MAC フロー パケット数ランキング API	・本項を追加しました。
7.8 MAC フロー バイト数時系列データ API	・本項を追加しました。
7.9 MAC フロー パケット数時系列データ API	・本項を追加しました。
8.1 トラブル発生時の対応	・トラブル発生時の対応についての記載を変更しました。

表　第 8 版改訂版の変更内容

章・節・項・タイトル	追加・変更内容
1.2.1 ライセンスの構成	・外部データ監視について記述を追加しました。
2.2.2 AX-Collector で使用可能なウェブブラウザ	・「表 2-3 使用可能なウェブブラウザ」の Firefox に関する記述を変更しました。

章・節・項・タイトル	追加・変更内容
3.2.1 前提ソフトウェアのインストール	・Docker のインストール手順に関する記述を変更しました。
3.2.2 本製品のインストール	・「表 3-5　AX-Collector インストール時の設定項目一覧」の設定項目を追加しました。 ・Firewall 設定 Firewall 設定について記述を追加しました。
4.1.8 データ管理の設定	・外部データ監視について記述を追加しました。
4.2.1 カスタマイズダッシュボードの作成	・外部データ監視について記述を追加しました。
4.5 外部データ監視機能（閾値監視，Impulse 連携）の設定	・本節を追加しました。
4.6 Impulse syslog/trap 送信制御機能の設定	・機能概要の記述を変更しました。
4.7 冗長化機能の設定	・外部データ監視について記述を追加しました。
4.8.1 ユーティリティコマンド	・外部データ監視について記述を追加しました。
5.2 AX-Collector の Web インタフェース機能一覧	・「表 5-2 AX-Collector の機能一覧」に外部データ監視，レポート，カスタム権限に関する記述を追加しました。 ・SNMP 監視，フロー監視に関する記述を変更しました。
5.3 TOP	・TOP 画面に関する記述を変更しました。
5.4.3 SNMP 監視	・SNMP 監視に関する記述を変更しました。
5.4.4 フロー監視	・フロー監視に関する記述を変更しました。
5.4.5 外部データ監視	・本項を追加しました。
5.4.6 Impulse 連携	・「表 5-32 Impulse syslog/trap 送信制御機能状態一覧の詳細」に関する記述を変更しました。
5.5 検知	・外部データ監視について記述を追加しました。
5.6.1 SNMP 監視	・詳細画面に関する記述を変更しました。 ・Syslog/trap 通知 設定変更について記述を追加しました。
5.6.2 フロー監視	・詳細画面に関する記述を変更しました。 ・収集周囲，および Syslog/trap 通知 設定変更について記述を追加しました。
5.6.3 外部データ監視・収集設定	・本項を追加しました。
5.6.4 Impulse 連携設定	・Impulse syslog/trap 送信制御設定に関する記述を変更しました。
5.8.2 レポート	・本項を追加しました。
5.8.5 管理	・外部データ監視について記述を追加しました。 ・カスタム権限について記述を追加しました。
6 MIB リファレンス	・外部データ監視について記述を追加しました。
7 REST API	・本章を追加しました。

表　第 7 版改訂版の変更内容

章・節・項・タイトル	追加・変更内容
2.3.5 機械学習エンジン Impulse	・機械学習エンジン Impulse の収容条件に関する記述を追加しました。
2.3.5 可視化エイリアス情報	・可視化エイリアス情報の収容条件に関する記述を追加しました。
3.4.6 冗長構成時のアップデート	・本項を追加しました。
4.1.4 ユーザ登録とデフォルトユーザの削除	・ユーザ権限について記載を追加しました。 ・変更についての記載を追加しました。
4.2.2 エイリアス情報の設定	・イーサタイプ／プロトコル番号／L4 ポート番号のエイリアス情報に関する記述を追加しました。
4.7.1 ユーティリティコマンド	・ユーザ追加についての説明を追加しました。 ・リストア時のバックアップファイルについての説明を追加しました。
5.1 AX-Collector の画面構成	図 5-1 画面構成を更新
5.2 AX-Collector の Web インタフェース機能一覧	・「表 5-2 AX-Collector の機能一覧」に「可視化エイリアス情報」の「イーサタイプ」，「プロトコル番号」，「L4 ポート番号」および「検知」の記述を追加しました。
5.4.1 ダッシュボード	・「(4)個別ビュー」の「表 5-7 ダッシュボード 個別ビューの概要」の記述を変更しました。 ・「(5)監視状況俯瞰ビュー」の「表 5-8 ダッシュボード 監視状況俯瞰ビューの概要」の記述を変更しました。
5.4.3 SNMP 監視	・閾値監視通知を 5.5 検知へ移動
5.4.4 フロー監視	・閾値監視通知を 5.5 検知へ移動
5.4.5 Impulse 連携	・Impulse 連携通知を 5.5 検知へ移動
5.5 検知	・本章を追加しました。
5.6.2 フロー監視・収集設定	・「(6) 過去データ生成」の記述を追加しました。
5.7.1 可視化エイリアス情報	・イーサタイプ／プロトコル番号／L4 ポート番号のエイリアス情報に関する記述を追加しました。 ・「表 5-37 管理・設定 可視化エイリアス情報の概要」のエクスポート(CSV)のファイル名に関する記述を変更しました。
5.8.4 管理	・設定変更，およびユーザ権限について記載を追加しました。

表　第 6 版改訂版の変更内容

章・節・項・タイトル	追加・変更内容
1. AX-Collector の概要	・機械学習エンジン Impulse に関する記述を追加しました。

章・節・項・タイトル	追加・変更内容
3. インストール	・設定ファイルのファイル名を修正しました。 ・インストール，アンインストール，アップデートの実行例を修正しました。
4. オペレーション	・Impulse 連携機能に関する記述を追加しました。
4.2.1 カスタマイズダッシュボードの作成	・カスタマイズダッシュボードに組み込み可能なビューの記述を追加しました。
4.6 冗長化機能の設定	・本項を追加しました
5. AX-Collector の Web インタフェース	・Impulse 連携機能に関する記述を追加しました。
5.2 AX-Collector の Web インタフェース機能一覧	・「表 5-2 AX-Collector の機能一覧」に「監視状況俯瞰ビュー」，「SNMP 監視」の「一括エクスポート」，「フロー監視」の「一括エクスポート」，「syslog/trap 送信制御状態一覧」，「syslog/trap 送信制御設定」，「冗長」の記述を追加しました。
5.4.1 ダッシュボード	・「(2)プリセットダッシュボード」の「表 5-5 ダッシュボード プリセットダッシュボードの概要」の「レイアウト保存」の記述を変更しました。 ・「(3)カスタマイズダッシュボード」の「表 5-6　ダッシュボード カスタマイズダッシュボードの概要」の「新規登録」「表示対象変更」「操作」「レイアウト保存」の記述を変更しました。 ・「(5)監視状況俯瞰ビュー」を追加しました。
5.4.3 SNMP 監視	・「表 5-14 SNMP 監視 閾値監視通知の概要」の記述を追加しました。 ・「(5)一括エクスポート」を追加しました。
5.4.4 フロー監視	・「表 5-18 フロー監視 閾値監視通知の概要」の記述を追加しました。 ・「(5)一括エクスポート」を追加しました。
5.4.5 Impulse 連携	・「表 5-20 Impulse 連携通知の概要」の記述を追加しました。 ・「(3) syslog/trap 送信制御状態一覧」を追加しました。
5.5.3 Impulse 連携設定	・「表 5-33 Impulse 連携設定 Impulse 接続の概要」の記述を追加しました。 ・「(2) syslog/trap 送信制御設定」を追加しました。
5.7.2 コレクタ接続環境	・「表 5-38 コレクタ接続環境 コレクタの概要」の記述を追加しました。
5.7.3 冗長	・本項を追加しました
5.7.5 保守	「(1) 運用ログ」を追加しました。

表　第 5 版改訂版の変更内容

章・節・項・タイトル	追加・変更内容
2.2.2 AX-Collector で使用可能なウェブブラウザ	・「表 2-3 使用可能なウェブブラウザ」の Firefox に関する記述を変更しました。
2.3.3 ブックマーク	・本項を追加しました。

章・節・項・タイトル	追加・変更内容
3.1.4 本製品に含まれるファイル	・「表 3-3 AX-Collector のプログラムファイルに含まれるファイル」の記述を変更しました。
3. インストール	・保守コマンドの実行例の記述を変更しました。
4.1.1 初期設定の流れ	・「図 4-1 初期設定フロー」に「データ管理の設定」の記述を追加しました。
4.1.7 データ管理の設定	・本項を追加しました。
4.2.1 カスタマイズダッシュボードの作成	・本項を追加しました。
4.2.2 エイリアス情報の設定	・「表 4-2 エイリアス情報を使用する可視化画面」の記述を変更しました。
4.4 フロー監視機能（閾値監視）の設定	・本節を追加しました。
4.5.1 ユーティリティコマンド	・以下のコマンドの「入力形式」および「実行例」の記述を変更しました。 (1)AX-Collector インストール (2)AX-Collector コンテナイメージ作成 (3) AX-Collector コンテナ作成および起動 ・以下のコマンドの「実行例」の記述を変更しました。 (6)コンテナ停止 (7)コンテナ削除 (8)コンテナイメージ削除 (11)SNMP 監視機能の開始・停止 ・「(5)コンテナ開始」の記述を変更しました。 ・「(12)フロー監視機能の開始・停止」を追加しました。 ・「(13)検知データの一括削除」に「フロー閾値監視機能」の記述を追加しました。
5.1 AX-Collector の画面構成	・「図 5-1 画面構成」および「表 5-1 構成要素」に「画面表示自動更新情報，画面表示時刻」の記述を追加しました。

章・節・項・タイトル	追加・変更内容
5.2 AX-Collector の Web インタフェース機能一覧	・「表 5-2 AX-Collector の機能一覧」に「カスタマイズダッシュボード」，「収集データ表示」および「データ監視設定」の「フロー監視」，「ブックマーク」の記述を追加しました。また，「TOP」および「SNMP 監視」の「概況」の説明の記述を変更しました。
5.3 TOP 画面	・「表 5-3 TOP 画面の概要」の記述を変更しました。
5.4.1 ダッシュボード	・「(2)プリセットダッシュボード」の記述を変更しました。 ・「(3)カスタマイズダッシュボード」を追加しました。 ・「表 5-7 ダッシュボード 個別ビューの概要」の「新規登録」に，「正規化」「エイリアス表示」の記述を追加しました。また，「CSV 出力」「表示期間設定」の記述を追加しました。
5.4.2 フローランキングリスト	・「表 5-9 フローランキングリスト IP フローおよび MAC フローの概要」の「表示条件設定・表示対象変更」に，「フロー数」「宛先アドレス種別」「フィールドフィルタ」の記述を追加しました。また，「表示」の記述を追加しました。
5.4.3 SNMP 監視	・「表 5-10 SNMP 監視 概況の概要」の記述を変更しました。
5.4.4 フロー監視	・本項を追加しました。
5.5.1 SNMP 監視・収集設定	・「表 5-17 SNMP 監視・収集設定 MIB オブジェクトの概要」の「新規登録」に，「正規化」の記述を追加しました。 ・「表 5-19 SNMP 監視・収集設定 SNMP 監視項目の概要」に「CSV 出力」「raw」「表示期間設定」の記述を追加しました。 ・「表 5-21 SNMP 監視・収集設定 収集・監視動作設定の概要」に，「データ収集」「閾値監視」「Trap 通知」「Syslog 通知」の記述を追加しました。
5.5.2 フロー監視・収集設定	・本項を追加しました。
5.6 ブックマーク	・本節を追加しました。
5.7.2 コレクタ接続環境	・「表 5-29 コレクタ接続環境 コレクタの概要」に「アラート表示時間（分）」の記述を追加しました。
5.7.3 管理	・「表 5-32 管理 データ管理の概要」の「データストア情報」に，「全ディスクサイズ」「ディスク使用率」の記述を追加しました。また，「データストア設定」に「期間監視」「容量監視」の記述を追加しました。 ・「表 5-34 管理 ユーザ管理の概要」の「新規登録」の記述を変更しました。 ・「表 5-35 管理 ライセンス管理の概要」の「登録ライセンス一覧」の記述を変更しました。
6.3.1 axCollFlwMonitorTable	・本項を追加しました。
6.3.2 axCollFlwThreshold	・本項を追加しました。

章・節・項・タイトル	追加・変更内容
6.4.1 SNMP 通知の種類と発行契機	・「表 6.4-1 SNMP 通知の種類と発行契機」に「axCollFlwThresholdDetectTrap」「axCollFlwThresholdRecoverTrap」の記述を追加しました。
6.4.2 PDU 内パラメータ	・「表 6.4-2 Trap-PDU 内パラメータ一覧」に「axCollFlwThresholdDetectTrap」「axCollFlwThresholdRecoverTrap」の記述を追加しました。

表　第 4 版改訂版の変更内容

章・節・項・タイトル	追加・変更内容
2.3 収容条件	・本節を追加しました。
3.1.4 本製品に含まれるファイル	・本項を追加しました。
4.1.1 初期設定の流れ	・「図 4-1 初期設定フロー」の環境設定の項目に「Trap 通知」の記述を追加しました。
4.1.6 環境設定	・「(3) SNMP Trap 通知（任意）」を追加しました。
4.3.2 監視・収集設定	・「(4) SNMP 監視項目の登録」に「SNMP Trap 通知」の記述を追加しました。
5.2 AX-Collector の Web インタフェース機能一覧	・「表 5-2 AX-Collector 機能一覧」の接続環境に「Trap 通知」の記述を追加しました。
5.4.2 フローリスト	・「表 5-7 可視化 フローリスト IP フロー・MAC フローの概要」に，「フロー数」「合計パケット数」「合計バイト数」の記述を追加しました。
5.5.2 監視・収集設定	・「表 5-15 SNMP 監視・収集設定 SNMP 監視項目一覧・登録の概要」の「新規登録」に，「Trap 通知」の記述を追加しました。
5.6.2 接続環境	・「(3) Trap 通知」を追加しました。
6. MIB リファレンス	・本章を追加しました。

表　第 3 版改訂版の変更内容

章・節・項・タイトル	追加・変更内容
3.2.2 本製品のインストール	・「(2) 設定ファイルの編集」の項目を追加しました。 ・「表 3-4 AX-Collector インストール時の設定項目一覧」に，「AX-Collector 公開ポート番号」および「SSL で有効化するプロトコル」の記述を追加しました。 ・「(2) 設定ファイルの編集」に，「(2-1) AX-Collector を複数ポートで公開」および「(2-2) SSL(https)の有効化」の記述を追加しました。
4.3.1 環境設定	・「(1) SNMP 監視の環境設定」に「送信元 IP アドレス」「送信元ポート番号」の記述を追加しました。
4.4.1 インストールコマンド	・本項を追加しました。
5.1 AX-Collector の画面構成	・「図 5-1 画面構成」および「表 5-1 構成要素」に「ホスト名」の記述を追加しました。

章・節・項・タイトル	追加・変更内容
5.2 AX-Collector の Web インタフェース機能一覧	・「表 5-2 AX-Collector 機能一覧」のダッシュボード機能に「登録一覧（IP/MAC フロー）」，「フローリスト（ランキング）」に「登録一覧」の記述を追加しました。
5.4.1 ダッシュボード	・「(1) 登録一覧（IP/MAC フロー）」を追加しました。 ・「(2) IP フロー・MAC フロー」の「表示対象変更」の「対象期間」に，「データの集計粒度」の記述を追加しました。 ・「(2) IP フロー・MAC フロー」の「表示対象変更」に「対象宛先 MAC アドレス」「対象宛先 IP アドレス」の記述を追加しました。 ・「(2) IP フロー・MAC フロー」に「表示対象登録」の記述を追加しました。 ・「(2) IP フロー・MAC フロー」の「関連フローリスト」に「表示するフィールド情報の指定」に関する記述を追加しました。 ・「(2) IP フロー・MAC フロー」の「時系列トラフィック量」に「時系列グラフの再描画」に関する記述を追加しました。
5.4.2 フローリスト	・「(1) 登録一覧」を追加しました。 ・「(2) IP フロー・MAC フロー」の「表示対象変更」に「対象宛先 MAC アドレス」「対象宛先 IP アドレス」の記述を追加しました。 ・「(2) IP フロー・MAC フロー」に「表示対象登録」の記述を追加しました。
5.5.1 監視・通知一覧	・「(4) 閾値監視通知一覧」に「選択通知の削除」「検索」の記述を追加しました。
5.5.2 監視・収集設定	・「(4) SNMP 監視項目一覧・登録」の「新規登録」に「データ収集」の記述を追加しました。 ・「(4) SNMP 監視項目一覧・登録」の「詳細」にて，bps/pps 単位での表示サポートに伴い，記述を変更しました。
5.6.1 機能	・「(1) SNMP 監視」に「タイムアウト時間（秒）」「リトライ回数」「送信元 IP アドレス」「送信元ポート番号」の記述を追加しました。
5.6.2 接続環境	・「(1) Collector」に「ホスト名」の記述を追加しました。
5.7 管理	・「(3) ユーザ管理」に「パスワード変更」の記述を追加しました。
6.1 トラブル発生時の対応	・「AX-Collector のバージョンアップ後，AX-Collector の画面が正常に表示されない。」に関する記述を追加しました。

表　第 2 版の変更内容

章・節・項・タイトル	追加・変更内容
5.2 AX-Collector の Web インタフェース機能一覧	・「MIB 収集状況」および「監視・収集設定(一括)」の記述を追加しました。
5.5.1 監視・通知一覧	・「(2) MIB 収集状況」を追加しました。
5.5.3 監視・収集設定(一括)	・本項を追加しました。
5.8 管理	・「(1) データ管理」に「データストア設定」の記述を追加しました。

はじめに

■対象製品・対象ソフトウェアおよびソフトウェアバージョン

このマニュアルは，AX-Collector を対象に記載しています。操作を行う前にこのマニュアルをよく読み，書かれている指示や注意を十分に理解してください。また，このマニュアルは必要なときにすぐ参照できるよう使いやすい場所に保管してください。

■対象読者

本製品を使用したネットワークシステムを構築し，運用するシステム管理者の方を対象としています。また，サーバ管理，ネットワークシステム管理の基礎的な知識を理解していることを前提としています。

■このマニュアルでの表記

ARP	Address Resolution Protocol
CEF	Common Event Format
CSS	Cascading Style Sheets
CSV	Comma-Separated Values
DB	database
DHCP	Dynamic Host Configuration Protocol
ESR	Extended Support Release
FW	FireWall
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEEE	The Institute of Electrical and Electronics Engineers, Inc.
IP	Internet Protocol
LAN	Local Area Network
MAC	Media Access Control
MIB	Management Information Base
MMDB	MaxMind DataBase
NAT	Network Address Translation
OID	Object IDentifier
RTP	Real-time Transport Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VLAN	Virtual LAN
VM	Virtual Machine
VRF	Virtual Routing and Forwarding/Virtual Routing and Forwarding Instance
VRRP	Virtual Router Redundancy Protocol
WAN	Wide Area Network

目次

1. AX-Collector の概要

この章では，AX-Collector の概要について説明します。

1.1　概要

1.1.1　可視化・異常検知ソリューション

今日のネットワークシステムは社会インフラとして重要性がますます増しています。一方で，予期せぬ障害やサイレント故障，高度化されたサイバー攻撃などにより，サービス停止などの影響を受けるリスクを常に抱えています。

ネットワークの可視化・異常検知ソリューションは，上記の課題に対応するため，ネットワークの障害や問題が表面化する前に，予兆を捉えて対処を行うプロアクティブな運用管理を実現するものです。

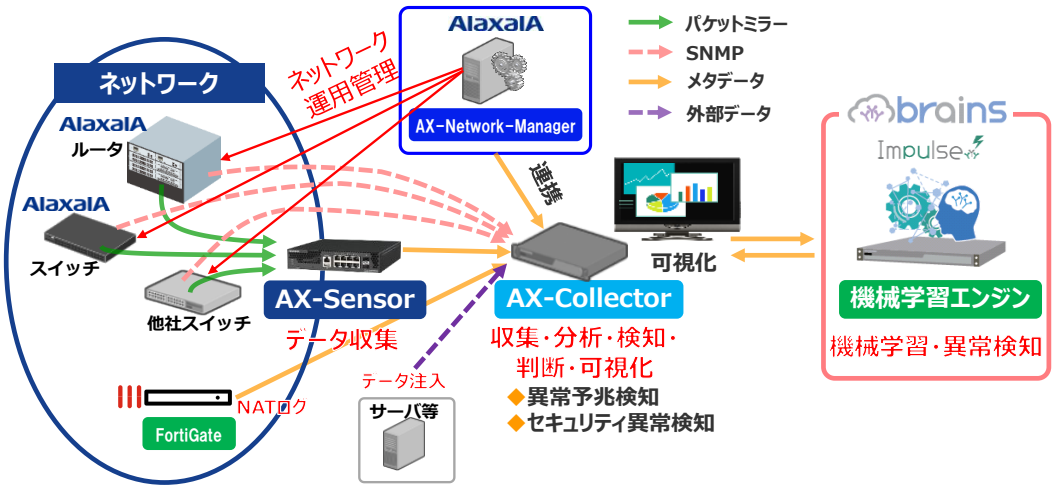

図 1-1　可視化・異常検知ソリューション

1.1.2　AX-Collector の位置付け

可視化・異常検知ソリューションは，下記の要素から構成されます。

AX-Collector は，可視化・異常検知ソリューションを構成する製品の 1 つで，ネットワークトラフィック情報を収集し，可視化や異常検知，ネットワークレイヤセキュリティ機能を提供します。

表 1-1　可視化・異常検知ソリューションの構成

構成要素	説明
AX-Collector	サーバ上で動作するアプリケーションソフトウェアです。AX-Sensor から送られるネットワークトラフィック情報，FortiGate から送られる NAT ログ情報，ルータやスイッチなどのネットワーク機器の MIB 情報，および REST-API により登録された任意の外部データ情報を収集・蓄積し，Web ブラウザを介して可視化を行います。 また，収集した情報を基に，閾値による異常検知，あるいは機械学習エンジン Impulse との連携による異常検知を実施します。
AX-Sensor（センサ）	ルータやスイッチのパケットミラーから各種ネットワークトラフィック情報を収集する装置です。収集した情報を加工（メタデータ化）し，AX-Collector に送信します。
FortiGate	フォーティネット社の次世代 Firewall 製品。NAT 機能のログ情報を netflow v9 形式，または CEF 形式の Syslog で送信すると，AX-Collector による可視化が可能です。
機械学習エンジン Impulse	ブレインズテクノロジー社製の機械学習エンジンです。AX-Collector と連携し，AX-Collector から送られるネットワークトラフィック情報を基に，機械学習による高度な分析機能で異常検知，および通知を行います。
ネットワーク機器	アラクサラの AX シリーズ ルータやスイッチ，または他社のルータやスイッチで，ネットワークトラフィックをパケットミラーにより，AX-Sensor へ送ります。
AX-Network-Manager	AX-Collector にて，ネットワークの異常を検知した場合，その通知を元に，不正な通信を行っている端末の通信を遮断するなどのネットワークの制御を行います。

1.1.3　主な特徴機能

AX-Collector の主な特徴機能を次に示します。

(1)　可視化機能

- ネットワークの全体概況を可視化（ダッシュボード表示機能）
- リアルタイムにユーザ環境に応じたトラフィック情報の可視化（フローリスト表示機能）
- 端末やサーバ毎，VLAN 毎，VM 毎，サービス毎，TCP フラグ等のパケット情報から識別できる情報から，目的に応じて可視化の内容を柔軟にカスタマイズ（個別ビュー表示機能，ダッシュボードカスタマイズ機能）
- 特定時刻における NAT 変換前後のトラフィック情報の可視化（FortiGate の NAT ログ情報収集）
- エイリアスによる容易な可視化とキーワード検索
- 通信障害のトラブルシュートやセキュリティインシデントの解析に有効なトラフィック情報（通信来歴）の長期間蓄積

(2)　異常検知機能

・アラクサラ独自のエンジンによる閾値（上限値／下限値）を用いた異常の検知および通知

・時系列グラフを用いた監視対象の異常状態表示

・異常検知情報一覧のカスタマイズ表示

・実績あるブレインズテクノロジー社の機械学習エンジン Impulse と連携し，機械学習技術をネットワークに適用

・機械学習技術を活用して，通常時のネットワークトラフィック情報の学習，周期性や相関性および状態変化の解析により，通常と異なる傾向を抽出し，従来の閾値監視では見つけられなかったサイレント故障や障害の予兆を検知

1.2 ライセンス

1.2.1 ライセンスの構成

AX-Collector は，サブスクリプション形式のソフトウェアです。

本ソフトウェアは，下記のライセンスからなります。

表 1-2 ライセンスの内訳

項目	説明
基本機能ライセンス	AX-Collector を使用するためのライセンス（必須）
Impulse 連携機能ライセンス※1※2	Impulse 連携機能を使用するためのライセンス （オプション）

注※1

SNMP 監視機能（Impulse 連携），フロー監視機能（Impulse 連携），および外部データ監視機能（Impulse 連携）による監視項目数は，1 ライセンスあたり 500 項目となります。500 項目より多い項目数を監視する場合，その項目数に応じて，複数の当該ライセンスが必要となります。例えば，2,000 項目を監視する場合，当該ライセンスは 4 ライセンス必要となります。仮に，監視したい項目数に対して必要な数のライセンスが登録されていない場合，AX-Collector に監視したい項目数分の情報を登録しても，登録したライセンス数に応じた項目数分のみの監視となります。

注※2

機械学習エンジン Impulse と連携するためには，AX-Collector の当該オプションライセンスの他に，機械学習エンジン Impulse 本体のライセンスも必要となります。

1.2.2 使用期間

ライセンスは，有効期間のある初年度ライセンス（納入日翌月から 15 か月後の月末まで有効）と 1 年延長ライセンス（12 か月有効），および有効期間のない永続ライセンスの 3 つに分類されます。

初年度ライセンスをご購入いただき，2 年目以降 継続利用する場合は，1 年延長ライセンスの購入が必要です。

表 1-3　ライセンスの使用期間例

1 年目	2 年目以降
基本機能ライセンス （初年度ライセンス）	基本機能ライセンス （1 年延長ライセンス）
基本機能ライセンス （永続ライセンス）	-
Impulse 連携機能ライセンス （初年度ライセンス）	Impulse 連携機能ライセンス （1 年延長ライセンス）

2. 動作条件

この章では，AX-Collector の動作条件について説明します。

2.1 ハードウェア構成

AX-Collector をインストールするために必要なハードウェアのスペックを次の表に示します。

フロー情報の収集を行う場合，フローの受信処理に複数の CPU コアを割り当てることで受信性能が向上します。次の動作スペック表に，ネットワーク規模（受信フロー数）毎の推奨構成（目安）を記載しています。ご利用のネットワークに適したハードウェアをご準備ください。

表 2-1 動作スペック

項目	小規模	中規模	大規模
受信フロー数／s	8K 未満	16K 未満	16K 以上
マルチコア CPU	8 コア以上	16 コア以上	32 コア以上
メモリ	32GB 以上	48GB 以上	64GB 以上
ストレージの空き容量※1※2※3	1TB 以上	2TB 以上	4TB 以上
イーサネットインタフェース	2 ポート以上 （データ受信用＋管理用）		

注※1

ストレージ容量が不足すると，AX-Collector が安定して動作することができなくなりますので，ディスク容量の確保は必ず行ってください。

注※2

ストレージ容量は，ネットワークフロー情報を保存できる期間に影響します。

ストレージの接続は，DAS(直接接続)を推奨します。NAS は非推奨です。

注※3

10K/s を超えるフロー受信環境では，ハードディスク読み書き性能を超過したデータ量となる場合があるため SSD を推奨します。

2.2 ソフトウェア構成

2.2.1 実行環境

AX-Collector をインストールするためには，次のいずれかのオペレーティングシステムが稼動している必要があります。

インストール手順に関しては，「3 インストール」を参照ください。

表 2-2 ソフトウェア環境

項番	オペレーティングシステム名
1	Red Hat Enterprise Linux 8, 9
2	MIRACLE LINUX 8, 9
3	Rocky Linux8, 9

※動作確認済み OS

2.2.2 AX-Collector で使用可能なウェブブラウザ

AX-Collector で使用可能な動作確認済みウェブブラウザを次に示します。

表 2-3 使用可能なウェブブラウザ

項番	ウェブブラウザ
1	Firefox 140 ESR
2	Google Chrome 最新版

2.3 収容条件

2.3.1 フローランキングリスト

フローランキングリストに関する収容条件を次に示します。

表 2-4 フローランキングリスト環境設定に関する収容条件

#	項目	収容条件
1	検索タイムアウト時間	最大 3,600 秒
2	最大 DB 検索数	最大 1,000,000
3	最大表示数 / 最大出力数	最大 1,000,000

2.3.2 フローランキング監視

フローランキング監視機能に関する収容条件を次に示します。

表 2-5 フローランキング監視 データ検索設定に関する収容条件

#	項目	収容条件
1	検索タイムアウト時間	最大 3,600 秒
2	最大検索数	最大 1,000,000

2.3.3 Syslog 通知

Syslog 通知に関する収容条件を次に示します。

表 2-6 Syslog 通知に関する収容条件

#	項目	収容条件
1	Syslog 通知の通知先数	最大 10

2.3.4 SNMP Trap 通知

SNMP Trap 通知に関する収容条件を次に示します。

表 2-7 SNMP Trap 通知に関する収容条件

#	項目	収容条件
1	SNMP Trap 通知の通知先数	最大 10

2.3.5 Email 通知

Email 通知に関する収容条件を次に示します。

表 2-8 Email 通知に関する収容条件

#	項目	収容条件
1	通知先接続 SMTP サーバ数	最大 10
2	通知先あたりのアドレス数（To）	最大 5
3	通知先あたりのアドレス数（Cc）	最大 5
4	通知先あたりのアドレス数（Bcc）	最大 5

2.3.6 機械学習エンジン Impulse

機械学習エンジン Impulse に関する収容条件を次に示します。

表 2-9 機械学習エンジン Impulse に関する収容条件

#	項目	収容条件
1	Impulse 同時接続数	最大 4

2.3.7 ブックマーク

ブックマークに関する収容条件を次に示します。

表 2-10 ブックマークに関する収容条件

#	項目	収容条件
1	コレクタあたりのトップカテゴリ数	最大 10
2	トップカテゴリあたりのカテゴリ数	最大 10
3	カテゴリあたりの登録可能 URL 数	最大 50
4	コレクタあたりの登録可能 URL 数	最大 5,000

2.3.8 可視化エイリアス情報

可視化エイリアス情報に関する収容条件を次に示します。

表 2-11 可視化エイリアス情報に関する収容条件

#	項目	収容条件
1	VLAN-ID のエイリアス登録数	4,096
2	VLAN(QinQ)のエイリアス登録数	10,000
3	MAC アドレスのエイリアス登録数	10,000
4	IPv4 アドレスのエイリアス登録数	10,000

#	項目	収容条件
5	IPv4 ネットワークのエイリアス登録数	10,000
6	IPv6 アドレスのエイリアス登録数	10,000
7	IPv6 ネットワークのエイリアス登録数	10,000
8	センサ・ポートのエイリアス登録数	10,000
9	イーサタイプのエイリアス登録数	10,000
10	プロトコル番号のエイリアス登録数	256
11	L4 ポート番号のエイリアス登録数	10,000

2.3.9 検知情報

検知情報に関する収容条件を次に示します。

表 2-12 検知付加情報１～３に関する収容条件

#	項目	収容条件
1	付加情報１登録数	最大 1,000
2	付加情報２登録数	最大 1,000
3	付加情報３登録数	最大 1,000

2.4　使用上の注意

2.4.1　使用文字について

本製品では，各機能の設定に記号文字（& < > " ' ¥ = - ; ` / : * ? |）を指定可能な対象がありますが，該当文字を画面あるいはフィルタ等で検索する機能はサポートしておりません。このため，記号文字についての使用は非推奨です。

3. インストール

この章では，本製品のインストール・アンインストールの手順について記載します。

3.1 インストール概要

この章では，本製品のインストールを行う手順について説明します。

3.1.1 インストールの流れ

本製品の新規インストールは大きく 3 つの手順に分かれます。新規インストール手順を次の表に示します。本手順をすべて実行し，インストールが正常に完了すると，本製品の使用が可能となります。

表 3-1 新規インストールの流れ

順番	手順	対象
1	インストール環境の準備	・ハードウェア環境 ・ソフトウェア環境
2	前提ソフトウェアのインストール	・Docker
3	本製品のインストール	・AX-Collector

3.1.2 インストールに関する注意事項

（1） インストール実施ユーザの権限

インストールは root 権限のあるユーザで行ってください。

（2） インストール先フォルダのアクセス権限

インストール先フォルダのアクセス権限を確認してください。書き込み権限のアクセス権がない場合，インストール前にあらかじめ付与しておいてください。

（3） ストレージ容量

フロー情報の格納には，大きな容量のパーティションが必要です。あらかじめ空き容量を確認してください。また，運用中も定期的にストレージ容量の空き容量を監視してください。

3.1.3 インストール環境の確認

AX-Collector をインストールするために必要なハードウェア・ソフトウェア環境のスペックを確認してください。

必要なスペックは，「2 動作条件」を参照してください。

3.1.4 本製品に含まれるファイル

本製品のプログラムファイルには以下のファイルが含まれます。

表 3-2 AX-Collector のプログラムファイルに含まれるファイル

項番	ファイル/ディレクトリ	説明
1	Dockerfile	Docker 環境の構築に使用するファイル
2	files	AX-Collector 内で使用するプログラム等のファイルを格納しているディレクトリ
3	ax-collector.conf	AX-Collector の設定ファイル
4	container.conf	AX-Collector の設定ファイル(コンテナ設定)
5	ax-collector-utility.sh	AX-Collector のインストール時や運用時に使用するスクリプト
6	AX-COLLECTOR-MIB.my	AX-Collector でサポートする MIB の定義ファイル

3.2　新規インストール

この章では，本製品の新規インストール手順について説明します。

3.2.1　前提ソフトウェアのインストール

インストール環境の確認後，次の表に示す AX-Collector の動作前提となるソフトウェアをインストールします。

表 3-3　前提ソフトウェア

インストールする必要のある前提ソフトウェア
[Docker] ・Docker-CE 19.03 以降

以降，前提ソフトウェアのインストール手順を説明します。

なお，インストールには，動作するオペレーティングシステムがインターネットに接続できる環境である必要があります。プロキシを経由してインターネットに接続し，かつ直接インターネットに接続できない場合には，環境変数 https_proxy および http_proxy にご利用中のプロキシを設定する必要がありますのでご注意ください。

① Proxy 環境変数確認例 （ご利用環境により設定は異なります）

```
# printenv http_proxy

http://user:password@proxyserver.co.jp:8080

# printenv https_proxy

http://user:password@proxyserver.co.jp:8080
```

（1）　Docker

本項では，docker-ce をインストールする際の例を示しますが，あくまで一例であるため環境によっては異なる部分があります。適宜該当部分についてはご利用の環境に合わせて読み替えてください。

なお，正式なインストール手順は次のサイトに記載されていますので，合わせてご確認いただいた上でインストール作業を実施ください。

https://docs.docker.com/engine/install/centos/

② yum-util のインストール

```
# yum install -y yum-utils
```

③ yum リポジトリの追加

```
# yum-config-manager --add-repo https://download.docker.com/linux/centos/docker-ce.repo
```

④ docker-ce のインストール

```
# yum install -y docker-ce docker-ce-cli containerd.io
```

⑤ システム起動時の docker 自動起動設定

```
# systemctl enable docker
```

⑥ ユーザを docker グループに追加（任意）

root 以外で docker を使用する場合，該当ユーザを docker グループに追加します。該当ユーザでログイン後，次のコマンドを実行ください。

```
$ sudo usermod -aG docker $USER
```

⑦ Docker を起動します。

```
# systemctl start docker
```

⑧ バージョンおよび起動確認

バージョン情報が表示され，プロセス表示画面が出力されれば，インストールは完了です。

インターネット接続にプロキシが必要な場合，次の手順を実行ください。

```
# docker -v
Docker version 19.03.15, build 99e3ed8919
# docker ps
CONTAINER ID        IMAGE               COMMAND
CREATED             STATUS              PORTS               NAMES
```

⑨　Docker のプロキシ設定

プロキシ設定ファイルを作成し，デーモンを再起動します。

```
# mkdir -p /etc/systemd/system/docker.service.d
# vi /etc/systemd/system/docker.service.d/http-proxy.conf
～～（編集）～～
# cat /etc/systemd/system/docker.service.d/http-proxy.conf
[Service]
Environment="HTTP_PROXY=http://user:password@proxyserver.co.jp:8080"
Environment="HTTPS_PROXY=http://user:password@proxyserver.co.jp:8080"
# systemctl daemon-reload
# systemctl restart docker
```

3.2.2　本製品のインストール

本製品をご利用いただくには，プログラムを展開後，インストールする必要があります。

（1）　プログラムの展開

AX-Collector のプログラムは， GZIP 形式のアーカイブ，および各アーカイブの MD5 ファイルにより提供します。

- AXCOLL<バージョン>-<ビルド番号>.tar.gz

MD5 ファイルは，上記ファイル名の後ろに”.md5”を付与したファイルとなります。

本項では，あらかじめ GZIP 形式アーカイブ，および MD5 ファイルが「/home/alaxala/」ディレクトリに転送してある前提で実行例を記載します。

あくまで一例であるため，環境によっては異なる部分があります。適宜該当部分についてはご利用の環境に合わせて読み替えてください。

① MD5 を確認します。ハッシュ値が同じであればアーカイブの転送が正常に終了しています。

```
# cd /home/alaxala

# ls -l AXCOLL*

-rw-r--r--. 1 root root 20920495  6 月  5 14:03 AXCOLL0113-258-g75de9d4b.tar.gz

-rw-r--r--. 1 root root       66  6 月  5 14:03 AXCOLL0113-258-g75de9d4b.tar.gz.md5

# md5sum AXCOLL0113-258-g75de9d4b.tar.gz

41ad111b1053dc4b9b7c6bcc0934f1b7  AXCOLL0113-258-g75de9d4b.tar.gz

# cat AXCOLL0113-258-g75de9d4b.tar.gz.md5

41ad111b1053dc4b9b7c6bcc0934f1b7  AXCOLL0113-258-g75de9d4b.tar.gz
```

② tar コマンドを使用してアーカイブを作業ディレクトリ「/home/alaxala/」に展開します。

```
# cd /home/alaxala

# tar xfvz AXCOLL0113-258-g75de9d4b.tar.gz

AXCOLL0113-258-g75de9d4b/

AXCOLL0113-258-g75de9d4b/Dockerfile

AXCOLL0113-258-g75de9d4b/ax-collector.conf

AXCOLL0113-258-g75de9d4b/container.conf

AXCOLL0113-258-g75de9d4b/ax-collector-utility.sh

～～中略～～

AXCOLL0113-258-g75de9d4b/files/mod/

#
```

③　次のファイル群が展開されていることを確認してください。

```
# cd AXCOLL0113-258-g75de9d4b

# ls -l

合計 80

-rw-rw-r--. 1 root root 16784  6 月  3 10:20 AX-COLLECTOR-MIB.my

-rw-rw-r--. 1 root root   418  6 月  3 10:20 Dockerfile

-rwxrwxr-x. 1 root root 48579  6 月  3 10:20 ax-collector-utility.sh

-rw-rw-r--. 1 root root  2821  6 月  3 10:20 ax-collector.conf

-rw-rw-r--. 1 root root   107  6 月  3 10:20 container.conf

drwxrwxr-x. 7 root root   135  6 月  3 10:20 files

#
```

（2）　設定ファイルの編集

ご利用環境に合わせて，各種設定を行う必要があります。各種設定は，ax-collector.conf ファイルに記載します。

① 設定ファイルを編集します。

```
# vi ax-collector.conf

～～（編集）～～

#
```

以下に設定項目の一覧を示します。

なお，先頭にシャープ(#)を記載した設定項目は，無効（未設定）として扱います。

表 3-4 AX-Collector インストール時の設定項目一覧

#	設定項目	設定名称	デフォルト値	備考
1	インターネット接続プロキシ※1	HTTP_PROXY	$http_proxy	デフォルトでは環境変数を参照します。
2		HTTPS_PROXY	$https_proxy	デフォルトでは環境変数を参照します。
3	JVM ヒープメモリサイズ(GB) ※1	JVM_HEAP_SIZE	8	搭載メモリの半分のサイズが推奨値です。
4	AX-Collector 公開ポート番号※1	AX_COLL_PORT1	80	AX-Collector のユーザインタフェース(HTTP/HTTPS)の接続ポート番号です
5		AX_COLL_PORT2	-	

#	設定項目	設定名称	デフォルト値	備考
6	フロー受信ポート番号※1	FLOWRCV_PORT	9996	フロー情報（IPフロー，MACフロー）の受信ポート番号です。AX-Sensorのフロー情報送信先ポート番号と同じ番号を指定ください。
7	負荷分散用の内部使用ポート1～8※1	BALANCING_PORT01	59991	AX-Collector内部でフロー情報の処理用に使用するポート番号です。 値を設定して有効化したポート数に応じて，負荷分散を行います。
8		BALANCING_PORT02	-	
9		BALANCING_PORT03	-	
10		BALANCING_PORT04	-	
11		BALANCING_PORT05	-	
12		BALANCING_PORT06	-	
13		BALANCING_PORT07	-	
14		BALANCING_PORT08	-	
15	フローDB格納処理のフラッシュ間隔（秒）※1	FLUSH_INTERVAL	10	受信したフロー情報をDBに格納する処理間隔を指定します。
16	SSLで有効化するプロトコル※1※4	SSL_PROTOCOLS	TLSv1.3	SSLで有効にするプロトコルを指定できます。
17	SSLで有効化する暗号スイート※1	SSL_CIPHERS	HIGH:!aNULL:!MD5	SSLで有効にする暗号スイートを指定できます。
18	AX-Collector設定情報格納ディレクトリ※2※3	DB_CL_DIR	/var/lib/ax-collector/db	

#	設定項目	設定名称	デフォルト値	備考
19	収集／監視情報格納ディレクトリ※2※3	DB_ES_DIR	/var/lib/ax-collector/db	収集／監視情報を格納するディレクトリのため，十分に大きいサイズのパーティションを割り当ててください。
20	レポート格納ディレクトリ※2※3	REPORT_DIR	/var/lib/ax-collector/report	
21	画像格納ディレクトリ※2※3	IMAGE_DIR	/var/lib/ax-collector/image	
22	ログ格納ディレクトリ※2※3	LOG_DIR	/var/log/ax-collector	
23	更新用ファイル格納ディレクトリ※2※3	SET_DIR	/var/lib/ax-collector/conf	
24	ガベッジコレクション方式※1※5※6	GC_METHOD	-	“CMSGC”または”G1”を指定します。
25	New 領域比率※1※6※7	GC_NEWRATIO	2	New 領域=1 に対する Old 領域の比率を指定します。
26	Old 領域の GC を開始する占有率※1※6※8	GC_INITIATING_OCCUPANCY	-	“1”～”99”の何れかの数値を指定します。

#	設定項目	設定名称	デフォルト値	備考
27	パケット受信バッファ（バイト）	RCV_BUF_SIZE	2097152	ホスト OS のパケット受信バッファです。kernel の net.core.rmem_default および net.core.rmem_max パラメータに反映されます。
28	フローインデックス単位設定	DB_FLOWDATA_INDEX_UNIT	-（1 日）	フロー情報を格納するデータベース Index の単位を指定します。本パラメータはデフォルト未設定であり，Index を 1 日毎に作成します。 1 日未満に変更する場合に,”H”,”2H”,”4H”,”6H”,”12H”の値が指定可能で，それぞれ 1,2,4,6,12 時間毎の Index を作成します。
29	メモリスワップ頻度	SWAPPINESS	-（10）	システムのメモリスワップ頻度を指定します。kernel の vm.swappiness パラメータに反映されます。0～200 の指定が可能です。

#	設定項目	設定名称	デフォルト値	備考
30	WSGI プロセス数	WSGI_PROCESSES	4	WEB アクセス時のアプリケーションプロセス数を指定します。1 以上の値を指定可能です。
32	WSGI スレッド数	WSGI_THREADS	8	WEB アクセス時のアプリケーションスレッド数を指定します。1 以上値を指定可能です。
33	CITY MMDB ファイル名	CITY_MMDB	GeoLite2-City.mmdb	GEOIP 連携機能に使用する CITY MMDB ファイル名です。
34	ASN MMDB ファイル名	ASN_MMDB	GeoLite2-ASN.mmdb	GEOIP 連携機能に使用する ASN MMDB ファイル名です。
35	Syslog 受信有効化設定	SYSLOG_RECEIVE_FUNCTION	DISABLE	Syslog 受信機能の有効化設定です。”ENABLE” 指定で有効化します。
36	Syslog 受信 IP アドレス	SYSLOG_RECEIVE_HOST	0.0.0.0 (すべて)	Syslog を受信するホスト IPv4 アドレスを指定します。
37	Syslog 受信ポート番号	SYSLOG_RECEIVE_PORT	514	Syslog 受信ポート番号を指定します。

#	設定項目	設定名称	デフォルト値	備考
38	Syslog 受信機能プロセス数	SYSLOG_WORKER_PROCESSES	1	Syslog 受信プロセス数を指定します。1～32 が指定可能です。
39	Syslog 受信バッファ	SYSLOG_RECEIVE_BUFFER_SIZE	2097152	Syslog 受信バッファです。#27 RCV_BUF_SIZE より大きい値を指定すると RCV_BUF_SIZE となります。
40	Syslog DB 格納処理のフラッシュ間隔（秒） ※1	SYSLOG_FLUSH_INTERVAL	10	受信した Syslog 情報を DB に格納する処理間隔を指定します。
41	Syslog インデックス単位設定	SYSLOG_DB_LOGGING_INDEX_UNIT	-（1 日）	Syslog 情報を格納するデータベース Index の単位を指定します。設定値は, #28 DB_FLOWDATA_INDEX_UNIT を参照。
42	Syslog ネットワークトラフィック連携フローセット ID	SYSLOG_FLOWDATA_FLOWSET_ID	262	Syslog ネットワークトラフィック可視化機能でフロー保存する際に付与するフローセット ID です。
43	Syslog ユーザ定義フィールド表示名称 1～10	SYSLOG_USER_DEFINED_LABEL_LOGEXT01	*ユーザ定義 1	Syslog ユーザ定義フィールドの表示名称です。
		SYSLOG_USER_DEFINED_LABEL_LOGEXT02	*ユーザ定義 2	

#	設定項目	設定名称	デフォルト値	備考
		SYSLOG_USER_DEFINED_LABEL_LOGEXT03	*ユーザ定義 3	
		SYSLOG_USER_DEFINED_LABEL_LOGEXT04	*ユーザ定義 4	
		SYSLOG_USER_DEFINED_LABEL_LOGEXT05	*ユーザ定義 5	
		SYSLOG_USER_DEFINED_LABEL_LOGEXT06	*ユーザ定義 6	
		SYSLOG_USER_DEFINED_LABEL_LOGEXT07	*ユーザ定義 7	
		SYSLOG_USER_DEFINED_LABEL_LOGEXT08	*ユーザ定義 8	
		SYSLOG_USER_DEFINED_LABEL_LOGEXT09	*ユーザ定義 9	
		SYSLOG_USER_DEFINED_LABEL_LOGEXT10	*ユーザ定義 10	

※1. インストール後に本設定を変更する場合は，設定の変更後に AX-Collector を再起動してください。

※2. インストール後に本設定を変更する場合は，AX-Collector を一度アンインストールして，再度インストールする必要があります。

※3. ディレクトリが存在しない場合は，インストール手順を実行することにより，自動的に作成されます。

※4. 暗号スイートは，鍵長が 128 bit 以上の暗号スイートを使用し，認証のない暗号スイート及び MD5 を用いる暗号スイートを使用しない設定となっています。

※5. 設定無効時は CMSGC で動作します。

※6. ax-collector.conf に無い GC 設定を指定する場合は，files/jvm.options.org を直接編集してインストールまたは再起動することで，コレクタ動作に反映することが出来ます。

※7. 設定無効時は NewRatio 未指定として動作し，New 領域と Old 領域の比率は自動で割り振られます。

※8. 設定無効時は，GC 方式が CMSGC の場合は 75%で動作します。GC 方式が G1GC の場合は 30%で動作します。

(2-1) AX-Collector を複数ポートで公開

AX_COLL_PORT1 および AX_COLL_PORT2 を有効にすることで，それぞれに指定したポート番号で http/https の待ち受けを行います。

また，ポート番号の前に IP アドレスを指定することで，待ち受けを行うサーバアドレスを指定することが出来ます。

例) ポート 80 はアドレスに関わらず待ち受け，ポート 10080 はアドレス 10.1.1.1 のみ待ち受ける場合の設定

AX_COLL_PORT1="80"

AX_COLL_PORT2="10.1.1.1:10080"

(2-2) SSL(https)の有効化

SSL(https)を使用して AX-Collector へアクセスする場合，以下の設定を行ってください。

① 設定ファイルで SSL を有効化

AX_COLL_PORT1，AX_COLL_PORT2 の設定で，ポート番号の後ろに”ssl”を指定することにより，ポート単位に SSL を有効化します。ポート番号と”ssl”の間にはスペースが必要です。

例) ポート 80 は http で，ポート 443 は https で接続可能とする場合の設定

AX_COLL_PORT1="80"

AX_COLL_PORT2="443 ssl"

② サーバ証明書ファイル及び秘密鍵ファイルの格納

SSL(https)を有効にした場合，サーバ証明書ファイル及び秘密鍵ファイルを指定のディレクトリに指定のファイル名で格納してください。

表 3-5 SSL 有効時に格納するファイル

#	ファイル	格納先ディレクトリ	ファイル名
1	サーバ証明書ファイル	SET_DIR で指定したディレクトリ（デフォルトでは/var/lib/ax-collector/conf）	ssl_server.crt

#	ファイル	格納先ディレクトリ	ファイル名
2	秘密鍵ファイル	SET_DIR で指定したディレクトリ （デフォルトでは/var/lib/ax-collector/conf）	ssl_server.key

運用開始後にサーバ証明書ファイル，秘密鍵ファイルを更新する場合，上記ファイルを置き換えた上で，AX-Collector を再起動してください。

再起動方法は「4.11 AX-Collector の保守コマンド」を参照してください。

③　有効化する SSL プロトコルの設定（任意）

デフォルトで TLS1.3 が有効となります。本設定を変更する場合，設定ファイルにて SSL_PROTOCOLS の設定を有効化し，設定内容を変更してください。

（3）　プログラムのインストール

プログラムをインストールします。

①　インストーラーを実行します。

インターネットから必要なソフトウェアをダウンロードするため，インストール完了までに時間がかかります。

```
# ./ax-collector-utility.sh --install

Do you want to install?

(y/n):y

2024 年  6 月  5 日 水曜日 14:28:56 JST

ax-collector:0113-258 build start ...

#0 building with "default" instance using docker driver

#1 [internal] load build definition from Dockerfile

#1 transferring dockerfile:

#1 transferring dockerfile: 516B 0.0s done

#1 DONE 0.3s

～～ 中略 ～～

#
```

② インストール終了後，Docker イメージとプロセスを確認します。

ax-collector イメージを使用したプロセスが確認できたら，正常にインストールができています。

```
# docker image ls

REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE

ax-collector            0113-258        df5df6a07200    2 minutes ago       1.48GB

# docker container ls

CONTAINER ID        IMAGE                    COMMAND             CREATED             STATUS
PORTS               NAMES

de674e8c0657   ax-collector:0113-258   "/sbin/init"   3 minutes ago   Up 3 minutes
ax-collector

#
```

③ AX-Collector で使用するアプリケーションの OS Firewall 設定を行います。

次の実行例は，AX-Collector の公開ポート番号を 80 番，フロー受信ポート番号を 9996 番に設定した場合の，Firewall の受信許可設定です。ご利用の環境に合わせて設定してください。

```
# firewall-cmd --add-service=http --permanent
success
# firewall-cmd --add-port=9996/udp --permanent
success
# firewall-cmd --reload
success
#
```

④ ご利用のブラウザにて，AX-Collector 公開用ポート番号を指定してアクセスし，ログイン画面が表示されることを確認してください。

3.2.3 インストール時の注意事項

（1） エンドポイントセキュリティ利用時の注意事項

各ディレクトリのファイルへのアクセスを監視するようなエンドポイントセキュリティ等のソフトウェアを利用する場合，下記ディレクトリは対象外とするよう設定してください。

表 3-6 除外ディレクトリ

#	除外ディレクトリ	備考
1	/var/lib/ax-collector/db	DB_CL_DIR で指定したディレクトリ
2	/var/lib/ax-collector/db	DB_ES_DIR で指定したディレクトリ
3	/var/lib/ax-collector/report	REPORT_DIR で指定したディレクトリ
4	/var/lib/ax-collector/image	IMAGE_DIR で指定したディレクトリ
5	/var/log/ax-collector	LOG_DIR で指定したディレクトリ
6	/var/lib/ax-collector/conf	SET_DIR で指定したディレクトリ
7	/var/lib/docker	Docker のイメージ，コンテナ，ボリュームの格納先ディレクトリ

3.3 アンインストール

この章では，本製品のアンインストール手順について説明します。

3.3.1 アンインストールの流れ

本製品のアンインストールを行う手順を説明します。

表 3-7 アンインストールの流れ

順番	手順	対象
1	アンインストールの準備	・本製品の実行終了
2	本製品のアンインストール	・AX-Collector

3.3.2 アンインストールに関する注意事項

（1） アンインストール実施ユーザの権限

アンインストールは root 権限のあるユーザで行ってください。

3.3.3 アンインストールの準備

アンインストール実施前の準備について説明します。

アンインストールを実施するためには，本製品の実行を終了し，かつ製品のファイルをすべて閉じた状態にしてから行ってください。

① 「3.2.2 本製品のインストール」で展開したディレクトリに移動し，プログラムを停止します。

```
# cd /home/alaxala/AXCOLL0113-258-g75de9d4b

# ./ax-collector-utility.sh --stop

Do you want to stop ax-collector?

(y/n): y

OK: ax-collector stopped.

#
```

3.3.4　本製品のアンインストール

アンインストールの手順について説明します。

① 本製品のコンテナを削除します。

```
# cd /home/alaxala/AXCOLL0113-258-g75de9d4b

# /ax-collector-utility.sh --remove-container

Do you want to remove ax-collector?

(y/n): y

OK: ax-collector container removed.

#
```

② 本製品のコンテナイメージを削除します。

```
# ./ax-collector-utility.sh --remove-image

Do you want to remove ax-collector?

(y/n): y

OK: ax-collector image removed.

#
```

③ 「3.2.2 本製品のインストール」で展開したプログラムを削除します。

```
# cd /home/alaxala

# rm -rf AXCOLL*
```

④ 「（2）設定ファイルの編集」で指定したディレクトリ配下のファイルを削除します。（任意）

ファイルを削除しない場合，AX-Collector の設定情報や収集したフロー情報，MIB 情報は残ります。

```
# rm -rf /var/lib/ax-collector/db

# rm -rf /var/log/ax-collector
```

3.4 アップデート

この章では，本製品のアップデート手順について説明します。

3.4.1 アップデートの流れ

本製品のアップデートを行う手順を説明します。

表 3-8 アップデートの流れ

順番	手順	対象
1	アップデートの準備	・新バージョンのプログラム展開 ・設定ファイルの更新
2	旧バージョンのアンインストール	・旧バージョンの実行終了 ・コンテナの削除
3	新バージョンのインストール	

3.4.2 アップデートに関する注意事項

（1） アップデート実施ユーザの権限

アップデートは，root 権限のあるユーザ，もしくはインストール時に使用したユーザで行ってください。

（2） AX-Sensor を同時にアップデートする場合の注意事項

新しいバージョンの AX-Sensor でサポートした機能を使用する場合は，該当機能をサポートするバージョンへ AX-Collector をアップデートしてから，AX-Sensor の該当機能を有効にしてください。

3.4.3 アップデートの準備

アップデートを実施するために，新しいバージョンのプログラムの展開，および ax-collector.conf ファイルを修正して各種設定を行います。

（1） プログラムの展開

新しいバージョンの AX-Collector のプログラムを展開します。

詳細な手順は本マニュアルの「（1） プログラムの展開」を参照してください。

（2） 設定ファイルの更新

新しいバージョンの AX-Collector の各種設定を行います。

「（1） プログラムの展開」で展開したディレクトリ配下の ax-collector.conf ファイルを，ご利用環境に合わせて修正してください。設定項目の詳細は「（2） 設定ファイルの編集」を参照してください。

ここで，「AX-Collector 設定情報格納ディレクトリ」や「フローDB 格納ディレクトリ」に旧バージョンと同様の設定を行うことで，アップデート後も旧バージョンのコンフィグレーションや収集情報を引き継いで動作します。

また，Syslog 受信機能の CEF 拡張文字列抽出設定を行っている場合は，アップデート前と同様の設定が必要です。設定方法は，「4.9.4CEF 形式フィールド情報**エラー! 参照元が見つかりません。エラー! 参照元が見つかりません。**」を参照してください。

3.4.4 旧バージョンのアンインストール

新バージョンの AX-Collector をインストールする前に，旧バージョンの AX-Collector をアンインストールします。本製品の実行を終了し，かつ製品のファイルをすべて閉じた状態にしてから行ってください。

① 旧バージョンのインストール時にプログラムを展開したディレクトリに移動し，旧バージョンのプログラムを停止します。

```
# cd /home/alaxala/AXCOLL0113-258-g75de9d4b

# ./ax-collector-utility.sh --stop

Do you want to stop ax-collector?

(y/n): y

OK: ax-collector stopped.

#
```

② 旧バージョンのコンテナを削除します。

```
# cd /home/alaxala/AXCOLL0113-258-g75de9d4b

# ./ax-collector-utility.sh --remove-container

Do you want to remove ax-collector?

(y/n): y

OK: ax-collector container removed.

#
```

3.4.5 新バージョンのインストール

新しいバージョンの AX-Collector をインストールします。

① 「3.4.3 アップデートの準備」でプログラムを展開したディテクトリに移動し，インストーラーを実行します。

インターネットから必要なソフトウェアをダウンロードするため，インストール完了までに時間がかかります。

```
# ./ax-collector-utility.sh --install

Do you want to install?

(y/n):y

ax-collector build start ...

～～ 中略 ～～

#
```

② インストール終了後，Docker イメージとプロセスを確認します。

ax-collector イメージを使用したプロセスが確認できたら，正常にインストールができています。

```
# docker image ls
REPOSITORY          TAG                 IMAGE ID            CREATED             SIZE
ax-collector            0113-260        6b508aa0ca1b    2 minutes ago    1.48GB
# docker container ls
CONTAINER ID        IMAGE                    COMMAND             CREATED             STATUS
PORTS               NAMES
be0cc65efbc1   ax-collector:0113-260   "/sbin/init"   5 minutess ago   Up 1 minutes
ax-collector
#
```

③ ご利用のブラウザにて，AX-Collector 公開用ポート番号を指定してアクセスし，ログイン画面が表示されることを確認してください。

バージョンアップ後に画面が正常に表示されない場合，ブラウザのキャッシュをクリアした上で再度読み込みを行ってください。

3.4.6 冗長構成時のアップデート

冗長構成での運用時には，次の手順でアップデートを行います。

① 待機系コレクタのアップデート

待機系コレクタを 3.4.3～3.4.5 の手順でアップデートします。

② 冗長構成の二重化組み込み確認

①でアップデートした待機系コレクタが起動後，運用系コレクタおよび，待機系コレクタにおいて，冗長状態が「二重化運用」となることを確認します。冗長状態は，メニュー→ナビゲーションバーより，「管理・設定」を選択し，「冗長」の表示項目から「概況」を選択し確認します。

③ 系切り替え

運用系コレクタの系切り替えを行います。系切り替えは，メニュー→ナビゲーションバーより，「管理・設定」を選択し，「冗長」の表示項目から「系切り替え」を選択し，「系切り替え」ボタンの押下で実行します。系切り替え実行後，②の手順で冗長状態が再度「二重化運用」となることを確認してください。

④　新待機系コレクタのアップデート

③で，新たに待機系となったコレクタを 3.4.3～3.4.5 の手順でアップデートします。アップデートした新待機系コレクタが起動後，運用系コレクタおよび，待機系コレクタにおいて，冗長状態が「二重化運用」となることを確認します。

4. オペレーション

この章では，AX-Collector の操作方法について説明します。

4.1 初期設定

AX-Collector を新規に起動した際におこなう初期設定について説明します。

各項目の設定方法や設定内容については，「5. AX-Collector の Web インタフェース」も参照してください。

4.1.1 初期設定の流れ

初期設定は，以下の流れでおこなってください。

図 4-1 初期設定フロー

4.1.2 サーバ環境確認

運用開始前に，AX-Collector が動作するサーバの時刻情報が AX-Sensor 等の周辺機器と一致していることを確認してください。

また，運用開始後の時刻ずれを防ぐために，NTP の使用を推奨します。

4.1.3 初回ログイン

初回起動時，次に示すユーザ名およびパスワードを使用して，AX-Collector にログインできます。

表 4-1 デフォルトユーザおよびパスワード

ユーザ名	ax-collector
パスワード	ax-collector

4.1.4 ユーザ登録とデフォルトユーザの削除

AX-Collector にログインする際に使用するユーザを登録します。

ナビゲーションバーより，「管理・設定」を選択し，「管理」の表示項目から「ユーザ管理」を選択します。

（1） 新規ユーザ登録

「新規登録」ボタンを押下し，任意のユーザ名とパスワードを入力し，ユーザ権限を選択します。AX-Collector の管理を行うユーザの場合は，ユーザ権限に”管理者”を選択してください。

「登録」ボタンを押下し，表示されたユーザ一覧に登録したユーザ名が表示されていることを確認します。

（2） 新規ユーザで再ログイン

ナビゲーションバーの「ログアウト」ボタンで，一旦，AX-Collector からログアウトし，新規に登録したユーザで再度ログインします。

初回ログイン時にユーザ自身でパスワードの変更を行ってください。

（3） デフォルトユーザの削除

セキュリティの観点から，デフォルトユーザの削除を推奨します。

ユーザ一覧から，ユーザ名 ax-collector の欄にある「ユーザ削除」ボタンを押下し，デフォルトユーザを削除します。

4.1.5 ライセンスの登録

AX-Collector の動作に必要なライセンスを登録します。

（1） ライセンスの登録

ナビゲーションバーより，「管理・設定」を選択し，「管理」の表示項目から「ライセンス管理」を選択します。

「機能ライセンス登録」ボタンを押下し，機能ライセンス追加画面で購入したライセンスキーを入力し，「登録」ボタンを押下してください。

表示されたライセンス一覧画面に，入力したライセンスキーが登録されていることを確認してください。

4.1.6 コレクタ接続環境の設定

AX-Collector の動作環境に関する設定を行います。

（1） コレクタ設定

ナビゲーションバーより，「管理・設定」を選択し，「コレクタ接続環境」の表示項目から「コレクタ」を選択します。

「変更」ボタンを押下し，IP アドレス欄に AX-Collector が動作するサーバの IP アドレスを入力してください。また，参照先ポート番号欄にインストール時に AX-Collector 公開ポート番号に設定したポート番号を入力し，「更新」ボタンを押下してください。

表示されたコレクタ設定情報に，入力した設定内容が反映されていることを確認してください。

（2） Syslog 通知 (任意)

ナビゲーションバーより，「管理・設定」を選択し，「コレクタ接続環境」の表示項目から「Syslog 通知先」を選択します。

「新規登録」ボタンを押下し，syslog の通知先として，IP アドレスおよびポート番号を入力してください。また，環境に合わせてファシリティを選択し，「登録」ボタンを押下してください。

表示された Syslog 通知先一覧に，入力した設定内容が反映されていることを確認してください。

（3） SNMP Trap 通知 (任意)

ナビゲーションバーより，「管理・設定」を選択し，「コレクタ接続環境」の表示項目から「Trap 通知先」を選択します。

「新規登録」ボタンを押下し，SNMP Trap の通知先として，IP アドレスおよびポート番号，コミュニティを入力し，「登録」ボタンを押下してください。

表示された Trap 通知先一覧に，入力した設定内容が反映されていることを確認してください。

（4） Email 通知 (任意)

ナビゲーションバーより，「管理・設定」を選択し，「コレクタ接続環境」の表示項目から「Email 通知先」を選択します。

「新規登録」ボタンを押下し，Email の通知先として，SMTP サーバの IP アドレス，暗号化種別やポート番号，認証情報，宛先および差出人メールアドレスを入力し，「登録」ボタンを押下してください。

表示された Email 通知先一覧に，入力した設定内容が反映されていることを確認してください。

4.1.7 Impulse 連携の設定

Impulse 連携に関する設定を行います。

ナビゲーションバーより，「データ監視設定」を選択し，「Impulse 連携」の表示項目から「Impulse 接続」を選択してください。

「新規登録」ボタンを押下し，Impulse 環境設定登録の画面を表示してください。

IP アドレスおよび設定先ポート番号，参照先ポート番号を入力し，「更新」ボタンを押下してください。

同じ条件で連続して異常を検知した場合に，最初の 1 回だけ通知を行いたい場合は，通知集約のチェックを有効にしてください。

4.1.8 データ管理の設定

AX-Collector のデータ管理に関する設定を行います。

AX-Collector を運用するにあたり，SNMP MIB 情報やフロー情報，外部データ情報等を格納するストレージの空き容量を定期的に監視し，空き容量が不足してきた場合には，過去のフロー情報を削除するなどして，空き容量を確保する必要があります。

AX-Collector では，収集した SNMP MIB 情報やフロー情報，外部データ情報，ロギング情報の保存期間，あるいはこれら保存情報のディスク使用率を監視し，定期的に保存情報を削除する機能を提供します。

ナビゲーションバーより，「管理・設定」を選択し，「管理」の表示項目から「データ管理」を選択します。

データストア情報の「データストア設定」ボタンを押下し，データストア設定の情報表示画面を表示してください。更に，「変更」ボタンを押下し，データストア設定の更新画面を表示してください。

定期削除のチェック，期間監視や容量監視等の設定情報を入力し，「更新」ボタンを押下してください。

4.2 可視化機能の設定

4.2.1 カスタマイズダッシュボードの作成

AX-Collector では，目的や用途に応じて，運用者が独自にカスタマイズしたダッシュボードを作成する機能を提供します。また，作成したダッシュボードに名称を付与して登録することにより，運用者はいつでも当該ダッシュボードを用いてトラフィック情報を表示することが可能になります。

カスタマイズダッシュボードは，以下の手順で作成します。

各項目の設定方法や設定内容については，「5. AX-Collector の Web インタフェース」も参照してください。

（1） ビューの作成

カスタマイズダッシュボードには，以下の機能で作成したビューを組み込むことができます。

表 4-2 組み込み対象の機能（ビュー）

機能(ビュー)
個別ビュー
SNMP 監視（時系列グラフ）
フロー監視（時系列グラフ）
外部データ監視（時系列グラフ）
監視状況俯瞰ビュー
画像

また，これらに加え，任意のテキスト・リンク情報も組み込むこともできます。

・個別ビューの作成

ナビゲーションバーより，「収集データ表示」を選択し，「ダッシュボード」の表示項目から「個別ビュー」を選択してください。

「新規登録」ボタンを押下し，個別ビューの登録画面を表示してください。

名前，可視化対象のフロー種別や絞り込み条件等を入力し，「登録」ボタンを押下してください。

・SNMP 監視（時系列グラフ）の作成

「4.3. SNMP 監視機能（閾値監視，Impulse 連携）の設定」を参照してください。

・フロー監視（時系列グラフ）の作成

「4.4. フロー監視機能（閾値監視，Impulse 連携）の設定」を参照してください。

・外部データ監視（時系列グラフ）の作成

「4.6. 外部データ監視機能（閾値監視，Impulse 連携）の設定」を参照してください。

・監視状況俯瞰ビューの作成

「4.3. SNMP 監視機能（閾値監視，Impulse 連携）の設定」，「4.4. フロー監視機能（閾値監視，Impulse 連携）の設定」もしくは「4.6. 外部データ監視機能（閾値監視，Impulse 連携）の設定」を行った後，ナビゲーションバーより，「収集データ表示」を選択し，「ダッシュボード」の表示項目から「監視状況俯瞰ビュー」を選択してください。

「新規登録」ボタンを押下し，監視状況俯瞰ビューの登録画面を表示してください。

名前，監視種別や表示データ等を入力し，「登録」ボタンを押下してください。

・画像の登録

ナビゲーションバーより，「管理・設定」を選択し，「管理」の表示項目から「画像ファイル」を選択してください。

「新規登録」ボタンを押下し，画像の登録画面を表示してください。

名前，画像ファイルを入力し，「登録」ボタンを押下してください。

（2） カスタマイズダッシュボードの作成

ナビゲーションバーより，「収集データ表示」を選択し，「ダッシュボード」の表示項目から「カスタマイズダッシュボード」を選択してください。

「新規登録」ボタンを押下し，カスタマイズダッシュボードの登録画面を表示してください。

名前，（1）で作成したビューを選択し，「登録」ボタンを押下してください。

また，ダッシュボードに組み込んだビューのレイアウトを変更する場合，作成したダッシュボードを表示し，画面編集モードに移行後，ビューの表示位置を変更して，レイアウト保存してください。

テキスト・リンク情報を追加する場合は，画面編集モードに移行後，「追加」ボタンを押下し，テキスト・リンクを選択後に表示するテキストメッセージ，リンク先URL 情報を入力してください。

4.2.2 エイリアス情報の設定

ダッシュボードおよびフローリストでは，エイリアス情報を設定することにより，可視化対象のネットワークや装置，端末情報等の把握・識別がより容易になります。

各項目の設定方法や設定内容については，「5. AX-Collector の Web インタフェース」も参照してください。

ナビゲーションバーより，「管理・設定」を選択し，「可視化エイリアス情報」の表示項目から設定対象項目のメニューを選択します。

エイリアス情報の登録は，「追加」ボタンの押下で表示される入力フォームから行います。※1

入力したエイリアス情報は，「エクスポート(CSV)」ボタンで CSV 形式のファイルとして保存することができます。また，CSV 形式の当該ファイルを「インポート(CSV)」ボタンにより，一括でインポートすることもできます※2。

エイリアスの各項目に使用できる文字は，半角の「&」「>」「<」を除く UTF-8 対応の文字で，各項目の最大文字数は 256 文字です。

4.2.3 IP フロー複合ビューによる可視化

IP フロー複合ビューを使用することにより，パケット数やバイト数に加えて，サーバ／クライアント間の遅延情報や TCP の再送情報をグラフ，およびリスト形式で可視化することができます。各項目の設定方法や設定内容については，「5. AX-Collector の Web インタフェース」も参照してください。

ナビゲーションバーより，「収集データ表示」を選択し，「フローランキングリスト」の表示項目から「IP フロー複合ビュー」を選択します。

IP フロー複合ビューでは，次に示す項目から２つを選択して，同時に可視化することが出来ます。

表 4-3 IP フロー複合ビューで表示可能な集計対象

表示項目	説明
パケット数	パケット数の合計値を表示します。
pps	パケット数の 1 秒毎の平均値を表示します。
バイト数	バイト数の合計値を表示します。
bps	ビット数の 1 秒毎の平均値を表示します。
送信パケット数	送信パケット数の合計値を表示します。
送信 pps	送信パケット数の 1 秒毎の平均値を表示します。
送信バイト数	送信バイト数の合計値を表示します。
送信 bps	送信ビット数の 1 秒毎の平均値を表示します。
フローレコード数	フローレコード数の合計値を表示します。
フローレコード数/s	フローレコード数の 1 秒毎の平均値を表示します。
TCP RTT(ms) ※1	TCP 接続時間の平均値を表示します。時系列グラフの場合はオプションで最大値，最小値を表示できます。
TCP SRT(ms) ※1	サーバ応答時間の平均値を表示します。時系列グラフの場合はオプションで最大値，最小値を表示できます。
TCP DELAY(ms) ※1	サーバ遅延時間の平均値を表示します。時系列グラフの場合はオプションで最大値，最小値を表示できます。
TCP 再送パケット数	TCP 再送パケット数の合計値を表示します。
TCP 再送パケット数割合（%）	TCP 再送パケット数／TCP パケット数の割合を%で表示します。
TCP 再送 pps	TCP 再送パケット数の 1 秒毎の平均値を表示します。
TCP 再送バイト数	TCP 再送バイト数の合計値を表示します。
TCP 再送バイト数割合（%）	TCP 再送バイト数／TCP バイト数の割合を%で表示します。
TCP 再送 bps	TCP 再送ビット数の 1 秒毎の平均値を表示します。
TCP パケットロス回数	TCP パケットロス回数の合計値を表示します。
TCP パケットロス回数/s	TCP パケットロス回数の 1 秒毎の平均値を表示します。
TCP パケットロス回数割合（%）	TCP 再送パケットロス回数／TCP パケット数の割合を%で表示します。
TCP 重複 ACK パケット数	TCP 重複パケット数の合計値を表示します。
TCP 重複 ACKpps	TCP 重複パケット数の 1 秒毎の平均値を表示します。
UDP DELAY(ms)	UDP 遅延時間の平均値を表示します。時系列グラフの場合はオプションで最大値，最小値を表示できます。
UDP JITTER(ms)	UDP JITTER の平均値を表示します。時系列グラフの場合はオプションで最大値，最小値を表示できます。
UDP RTP RTT(ms)	UDP RTP RTT の平均値を表示します。時系列グラフの場合はオプションで最大値，最小値を表示できます。

表示項目	説明
UDP RTP DELAY(ms)	UDP RTP 遅延時間の平均値を表示します。時系列グラフの場合はオプションで最大値，最小値を表示できます。
UDP RTP JITTER(ms)	UDP RTP JITTER の平均値を表示します。時系列グラフの場合はオプションで最大値，最小値を表示できます。
UDP RTP 順序違反回数	UDP RTP 順序違反回数の合計値を表示します。
UDP RTP 順序違反回数/s	UDP RTP 順序違反パケットロス回数の 1 秒毎の平均値を表示します。
UDP RTP ロストパケット数	UDP RTP ロストパケット数の合計値を表示します。
UDP RTP ロスト pps	UDP RTP ロストパケット数の 1 秒毎の平均値を表示します。
UDP RTP ロストパケット数割合（%）	UDP RTP ロストパケット数／UDP RTP パケット数の割合を%で表示します。
NAT 継続時間（s）	NAT セッションの継続時間（秒）を表示します。

※1. 特定のサーバ／クライアント間の TCP 遅延情報を監視する場合は，フィールドフィルタの宛先 IPv4／IPv6 アドレスにサーバのアドレスを指定し，送信元 IPv4／IPv6 アドレスにクライアントのアドレスを指定してください。

IP フロー複合ビューではグラフの表示形式として，時系列グラフとヒストグラム（分布図）の何れかを選択出来ます。ヒストグラムは集計対象に TCP RTT，TCP SRT，TCP DELAY，UDP DELAY，UDP JITTER，UDP RTP RTT，UDP RTP DELAY，UDP RTP JITTER を選択した場合のみ，遅延時間毎のフローレコード数をグラフ表示します。

また，集約条件として次の２パターンの何れかを選択することが出来ます。

表 4-4 IP フロー複合ビューの集約条件指定方法

集約条件	説明
表示フィールド	リストでは指定した表示・集約条件毎のランキングリストを表示数上限まで表示します。 時系列グラフでは，合計値または正規化した値を表示します。TCP 情報（RTT，SRT，DELAY），UDP 情報（JITTER，DLEAY，RTT）では全体の平均値を表示し，オプションにより最小値，最大値を表示します。 ヒストグラムでは遅延時間毎に全体のフローレコード数を表示します。
フィールドフィルタ	フィールドフィルタをフィルタとしてではなく，表示・集約条件として使用します。この場合，フィールドフィルタのシート毎にリストや時系列グラフ，ヒストグラムの値を表示します。

フィールドフィルタで指定が可能なフィールドを次に示します。

表 4-5 IP フロー複合ビューのフィールドフィルタ

フィールド	説明
有効	有効のチェックを外した場合，該当行は無効となり，指定内容を無視します。
除外	除外をチェックした場合は，該当行を AND NOT 条件として判定します。除外をチェックしていない場合は OR 条件として判定します。
フローセット ID	フローセット ID を指定します。
センサ IP アドレス	センサ IPv4 アドレスを指定します。
モニタポート ifIndex	モニタポートの ifIndex を指定します。
送信ポート ifIndex	送信ポートの ifIndex を指定します。
VLAN-ID（S-TAG）	VLAN-ID を指定します。 QinQ（IEEE802.1q トンネリング）を使用している場合は S-TAG（サービスタグ）を指定します。
VLAN-ID（C-TAG）	QinQ（IEEE802.1q トンネリング）を使用している場合に C-TAG（カスタマータグ）を指定します。
送信元 MAC アドレス	送信元 MAC アドレスを指定します。 完全一致での指定と，ワイルドカードを使用した指定が可能です。※1
宛先 MAC アドレス	宛先 MAC アドレスを指定します。 完全一致での指定と，ワイルドカードを使用した指定が可能です。※1
送信元 IPv4 アドレス	送信元 IPv4 アドレスを指定します。
宛先 IPv4 アドレス	宛先 IPv4 アドレスを指定します。
送信元 IPv6 アドレス	送信元 IPv6 アドレスを指定します。
宛先 IPv6 アドレス	宛先 IPv6 アドレスを指定します。
IP バージョン	IP バージョンを指定します。
プロトコル番号	プロトコル番号を 10 進数で指定します。
ICMP タイプ	ICMP タイプを 10 進数で指定します。
ICMP コード	ICMP コードを 10 進数で指定します。
送信元 L4 ポート番号	送信元 L4 ポート番号を指定します。
宛先 L4 ポート番号	宛先 L4 ポート番号を指定します。
TCP フラグ	TCP フラグの組み合わせを次の名称で指定します。 fin syn rst psh ack urg ece cwr 半角スペースで区切って複数のフラグを指定可能で，立っていないフラグを指定する場合は上記文字列の前に"!"を付加します。 または 10 進数での指定も可能です。 （例）syn のみセットの場合 文字列：!fin syn !rst !psh !ack !urg !ece !cwr 10 進数：2
HTTP サーバ名	HTTP サーバ名を指定します。 完全一致での指定と，ワイルドカードを使用した指定が可能です。※2
UDP RTP SSRC	UDP RTP パケットの SSRC（Synchronization Source）を 10 進数で指定します。
UDP RTP Clock Rate	UDP RTP パケットの Clock Rate を 10 進数で指定します。

フィールド	説明
UDP RTP Payload Type	UDP RTP パケットの Payload Type を 10 進数で指定します。
NAT 送信元 IPv4 アドレス	NAT 送信元 IPv4 アドレスを指定します。
NAT 宛先 IPv4 アドレス	NAT 宛先 IPv4 アドレスを指定します。
NAT 送信元 IPv6 アドレス	NAT 送信元 IPv6 アドレスを指定します。
NAT 宛先 IPv6 アドレス	NAT 宛先 IPv6 アドレスを指定します。
NAT 送信元 L4 ポート番号	NAT 送信元 L4 ポート番号を指定します。
NAT 宛先 L4 ポート番号	NAT 宛先 L4 ポート番号を指定します。
NAT L4 ポート番号範囲 Start	NAT 送信元 L4 ポート範囲の開始番号を指定します。
NAT L4 ポート番号範囲 End	NAT 宛先 L4 ポート範囲の終了番号を指定します。
NAT イベント	NAT イベント種別を 10 進数で指定します。
NAT タイプ	NAT タイプを 10 進数で指定します。
バーチャルドメイン名	バーチャルドメイン名を指定します。 後方完全一致での指定と，ワイルドカードを使用した指定が可能です。※3
*フロー拡張データ 01～10	フローデータ拡張で追加した拡張文字列を指定します。
*フロー拡張データ 11～16	GEOIP 連携機能で送信元 IP アドレスから検索した国名等の文字列を指定します。
*フロー拡張データ 21～26	GEOIP 連携機能で宛先 IP アドレスから検索した国名等の文字列を指定します。

※1. MAC アドレスでは，以下のワイルドカードが使用できます。

*：先頭か最後のどちらか片方のみ，”:”に隣接して指定可能で，0 文字以上の任意の文字列に一致します。

?：”:”以外の任意の場所に指定可能で，任意の 1 文字に一致します。

※2. HTTP サーバ名では，以下のワイルドカードが使用できます。

*：任意の場所に指定可能で，0 文字以上の任意の文字列に一致します。

?：任意の場所に指定可能で，任意の 1 文字に一致します。

※3. バーチャルドメイン名では，後方文字列に完全一致したレコードがフィルタされます。また，以下のワイルドカードが使用できます。

*：任意の場所に指定可能で，0 文字以上の任意の文字列に一致します。

?：任意の場所に指定可能で，任意の 1 文字に一致します。

4.2.4 フローデータ拡張の設定

フローデータ拡張は，AX-Collector が受信したフロー情報をデータベースに保存する際に，任意の文字列情報を追加して保存，および GEOIP 連携機能により検索した国情報との文字列情報を追加保存する機能です。

GEOIP 連携機能に関しては，「4.10 GEOIP 連携機能の設定」に記載しています。

文字列情報はひとつのフロー情報に最大 10 個まで追加することが出来，IP アドレス等のフロー情報の各項目と同様に，可視化や監視においてフィルタや集約に使用することが出来ます。

（1） フローデータ拡張の機能概要

フロー情報を受信した際に，フロー情報上の，検索フィールドに指定した項目の内容と，予め登録したマッチング文字列とを比較します。そして一致した場合は，一致した条件に紐付けた文字列情報を該当のフロー情報に追加して保存します。

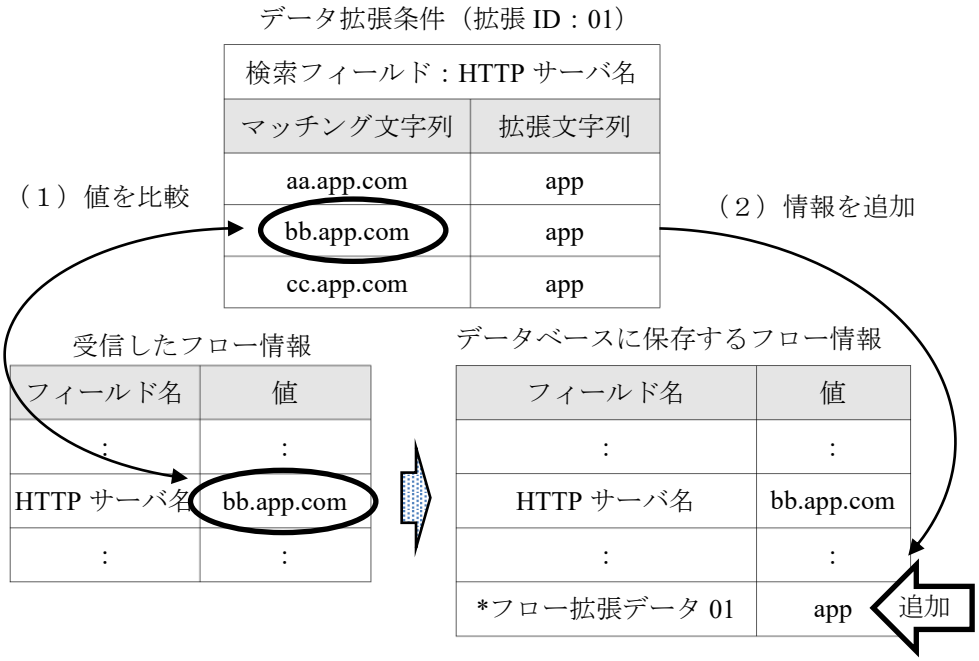

図 4-2 フローデータ拡張の動作概要

フローデータ拡張の設定は，データ拡張条件の設定，拡張データの設定，AX-Collector への設定内容の反映の順で行います。

各項目の設定方法や設定内容については，「5. AX-Collector の Web インタフェース」も参照してください。

（2） データ拡張条件の設定

ナビゲーションバーより，「管理・設定」を選択し，「管理」の表示項目から「フ

ローデータ拡張」を選択して，データ拡張一覧の画面を表示します。

「登録」ボタンを押下してデータ拡張条件の登録画面を表示し，コレクタ表示名，検索フィールド，一致種別を入力し，「登録」ボタンを押下してください。

（3） 拡張データの設定

前項で登録を行ったデータ拡張条件の「拡張データ一覧」ボタンを押下し，拡張データ一覧画面を表示します。「新規登録」ボタンを押下し，マッチング文字列と拡張条件を入力して「登録」ボタンを押下してください。この手順を繰り返し，必要な拡張データを登録してください。

（4） 設定の反映

ナビゲーションバーより，「管理・設定」を選択し，「管理」の表示項目から「フローデータ拡張」を選択して，データ拡張一覧の画面を表示します。

一覧の下にある「反映」ボタンを押下し，登録したフローデータ拡張の設定を AX-Collector の動作に反映させます。この反映処理は数分程度かかる場合があります。

4.3 SNMP 監視機能（閾値監視，Impulse 連携）の設定

SNMP 監視機能（閾値監視，Impulse 連携）の設定をおこないます。

各項目の設定方法や設定内容については，「5. AX-Collector の Web インタフェース」も参照してください。

4.3.1 環境設定

（1） SNMP 監視の環境設定

ナビゲーションバーより，「データ監視設定」を選択し，「SNMP 監視」の表示項目から「環境設定」を選択してください。

「変更」ボタンを押下し，SNMP 監視環境設定の更新画面を表示してください。

収集周期およびプロセス数，送信元 IP アドレスや送信元ポート番号等を入力し，「更新」ボタンを押下してください。

4.3.2 監視設定

本項で記載する各項目の登録方法として，次の 2 つの方法があります。いずれかの方法で登録を行ってください。

・Web インタフェースの各設定項目から登録する

・設定項目毎に設定内容を入力した CSV ファイルを作成し，Web インタフェースの「データ監視設定」－「SNMP 監視」の「一括登録・更新」の項目から，作成した CSV ファイルを取り込み，一括で登録する。

（1） ネットワーク機器の登録

ナビゲーションバーより，「データ監視設定」を選択し，「SNMP 監視」の表示項目から「ネットワーク機器」を選択してください。

「新規登録」ボタンを押下し，ネットワーク機器の登録画面を表示してください。

名前および IP アドレス，コミュニティ名を入力し，「登録」ボタンを押下してください。

登録したネットワーク機器にアクセス可能な環境で，登録後に表示されるネットワーク機器 設定詳細画面で「ステータス情報更新」ボタンを押下することで，対象のネットワーク機器のシステムやインタフェースに関するステータス情報を取得し表示

することが出来ます。

（2） MIB オブジェクトの登録

ナビゲーションバーより，「データ監視設定」を選択し，「SNMP 監視」の表示項目から「MIB オブジェクト」を選択してください。

「新規登録」ボタンを押下し，MIB オブジェクトの登録画面を表示してください。

名前およびネットワーク機器，オブジェクト識別子を入力し，「登録」ボタンを押下してください。

ネットワーク機器 設定詳細画面でステータス情報を取得していた場合は，インタフェースに関するオブジェクト識別子をプルダウンから選択して入力することが出来ます。

（3） MIB オブジェクトグループの登録

ナビゲーションバーより，「データ監視設定」を選択し，「SNMP 監視」の表示項目から「MIB オブジェクトグループ」を選択してください。

「新規登録」ボタンを押下し，MIB オブジェクトグループの登録画面を表示してください。

名前およびタグ名，MIB オブジェクト，上限閾値監視，下限閾値監視，syslog 補足説明を入力し，「登録」ボタンを押下してください。

上限閾値監視および下限閾値監視には，検知閾値，検知乗数，復旧閾値，復旧乗数のそれぞれについて適切な値を入力してください。

（4） SNMP 監視項目の登録

ナビゲーションバーより，「データ監視設定」を選択し，「SNMP 監視」の表示項目から「SNMP 監視項目」を選択してください。

「新規登録」ボタンを押下し，SNMP 監視項目の登録画面を表示してください。

名前およびインデックス名，MIB オブジェクトグループを入力し，データ収集のチェックボックスを有効にしてください。

監視機能として，閾値監視および Impulse 連携による監視を動作させる場合には，各機能のチェックボックスを有効化して「登録」ボタンを押下してください。

また，必要に応じて，次の通知機能の設定を行って下さい。

・Syslog 通知を使用する場合，チェックボックスの有効化および重要度，参照先 URL の入力を行ってください。

・SNMP Trap 通知／Email 通知を使用する場合，チェックボックスの有効化を行ってください。

4.4 フロー監視機能（閾値監視，Impulse 連携）の設定

フロー監視機能（閾値監視，Impulse 連携）の設定をおこないます。

各項目の設定方法や設定内容については，「5. AX-Collector の Web インタフェース」も参照してください。

4.4.1 環境設定

（1） フロー監視の環境設定

ナビゲーションバーより，「データ監視設定」を選択し，「フロー監視」の表示項目から「環境設定」を選択してください。

「変更」ボタンを押下し，フロー監視環境設定の更新画面を表示してください。

収集周期およびプロセス数，タイムアウト時間等を入力し，「更新」ボタンを押下してください。

4.4.2 監視設定

本項で記載する各項目の登録方法として，次の 2 つの方法があります。いずれかの方法で登録を行ってください。

・Web インタフェースの各設定項目から登録する

・設定項目毎に設定内容を入力した CSV ファイルを作成し，Web インタフェースの「データ監視設定」－「フロー監視・収集設定」の「一括登録・更新」の項目から，作成した CSV ファイルを取り込み，一括で登録する。

（1） フロー条件の登録

ナビゲーションバーより，「データ監視設定」を選択し，「フロー監視」の表示項目から「フロー条件」を選択してください。

「新規登録」ボタンを押下し，フロー条件の登録画面を表示してください。

名前およびデータ名，フロー種別，絞り込み条件，集計対象等を入力し，「登録」ボタンを押下してください。

絞り込み条件は複数行設定することができ，同一行内は AND 条件で判定します。各行間は，除外をチェックした場合は AND NOT，それ以外は OR 条件で判定します。

集計の対象は，ユニーク数，又は集計対象と集計方法の組み合わせを指定します。

ユニーク数を指定した場合はこれが優先され，集計対象，集計方法の設定は無視されます。

（2） フロー条件グループの登録

ナビゲーションバーより，「データ監視設定」を選択し，「フロー監視」の表示項目から「フロー条件グループ」を選択してください。

「新規登録」ボタンを押下し，フロー条件グループの登録画面を表示してください。

名前およびタグ名，フロー条件，上限閾値監視，下限閾値監視，syslog 補足説明を入力し，「登録」ボタンを押下してください。

上限閾値監視および下限閾値監視には，検知閾値，検知乗数，復旧閾値，復旧乗数のそれぞれについて適切な値を入力してください。

（3） フロー監視項目の登録

ナビゲーションバーより，「データ監視設定」を選択し，「フロー監視」の表示項目から「フロー監視項目」を選択してください。

「新規登録」ボタンを押下し，フロー監視項目の登録画面を表示してください。

名前およびインデックス名，フロー条件グループを入力し，データ収集のチェックボックスを有効にしてください。

監視機能として，閾値監視および Impulse 連携による監視を動作させる場合には，各機能のチェックボックスを有効化して「登録」ボタンを押下してください。

また，必要に応じて，次の通知機能の設定を行って下さい。

・Syslog 通知を使用する場合，チェックボックスの有効化および重要度，参照先 URL の入力を行ってください。

・SNMP Trap 通知／Email 通知を使用する場合，チェックボックスの有効化を行ってください。

4.4.3 フロー監視の集計対象

フロー条件の登録において，フロー監視の集計の対象としてユニーク数，又は集計対象と集計方法の組み合わせを指定します。ユニーク数を指定した場合はこれが優先さ

れ，集計対象，集計方法の設定は無視されます。

指定可能なユニーク数，および集計対象と集計方法の組み合わせの詳細を次に示します。

表 4-6 フロー監視 指定可能なユニーク数

ユニーク数	説明
フローセット ID	フローセット ID のユニーク数
センサ IP アドレス	センサ IP アドレスのユニーク数
モニタポート ifIndex	モニタポート ifindex のユニーク数
送信ポート ifindex	送信ポート ifindex のユニーク数
VLAN ID（S-Tag)	VLAN ID（S-Tag)のユニーク数
VLAN ID（C-Tag）	VLAN ID（C-Tag）のユニーク数
送信元 MAC アドレス	送信元 MAC アドレスのユニーク数
宛先 MAC アドレス	宛先 MAC アドレスのユニーク数
イーサタイプ	イーサタイプのユニーク数
送信元 IPv4 アドレス	送信元 IPv4 アドレスのユニーク数
宛先 IPv4 アドレス	宛先 IPv4 アドレスのユニーク数
送信元 IPv6 アドレス	送信元 IPv6 アドレスのユニーク数
宛先 IPv6 アドレス	宛先 IPv6 アドレスのユニーク数
IP バージョン	IP バージョンのユニーク数
プロトコル番号	プロトコル番号のユニーク数
ICMP タイプ	ICMP タイプのユニーク数
ICMP コード	ICMP コードのユニーク数
送信元ポート番号	送信元ポート番号のユニーク数
宛先ポート番号	宛先ポート番号のユニーク数
TCP フラグ	TCP フラグのユニーク数
HTTP サーバ名	HTTP サーバ名のユニーク数
NAT 送信元 IPv4 アドレス	NAT 送信元 IPv4 アドレスのユニーク数
NAT 宛先 IPv4 アドレス	NAT 宛先 IPv4 アドレスのユニーク数
NAT 送信元 IPv6 アドレス	NAT 送信元 IPv6 アドレスのユニーク数
NAT 宛先 IPv6 アドレス	NAT 宛先 IPv6 アドレスのユニーク数
NAT 送信元 L4 ポート番号	NAT 送信元 L4 ポート番号のユニーク数
NAT 宛先 L4 ポート番号	NAT 宛先 L4 ポート番号のユニーク数
NAT L4 ポート番号範囲 Start	NAT 送信元 L4 ポート範囲の開始番号のユニーク数
NAT L4 ポート番号範囲 End	NAT 宛先 L4 ポート範囲の終了番号のユニーク数
NAT イベント	NAT イベント種別のユニーク数
NAT タイプ	NAT タイプのユニーク数
バーチャルドメイン名	バーチャルドメイン名のユニーク数
UDP RTP SSRC	UDP RTP パケット SSRC（Synchronization Source）のユニーク数
UDP RTP Clock Rate	UDP RTP パケット Clock Rate のユニーク数

ユニーク数	説明
UDP RTP Payload Type	UDP RTP パケット Payload Type のユニーク数
フロー拡張データ 01～10	フローデータ拡張機能により追加した拡張文字列のユニーク数
*フロー拡張データ 11～16	GEOIP 連携機能で送信元 IP アドレスから検索した国名等のユニーク数
*フロー拡張データ 21～26	GEOIP 連携機能で宛先 IP アドレスから検索した国名等のユニーク数

＊ユニーク数の集計値は，集計アルゴリズムに起因する誤差が生じる場合があります。

表 4-7 フロー監視 指定可能な集計対象と集計方法の組み合わせ

集計対象	集計方法	説明
フローレコード数	合計	フローレコード数の合計値
	平均/s	1 秒毎のフローレコード数の平均値
	最大/s	1 秒毎のフローレコード数の最大値※1
	最小/s	1 秒毎のフローレコード数の最小値※1
バイト数	合計	バイト数の合計値
パケット数	合計	パケット数の合計値
bps	平均/s	bps の平均値
	最大/s	bps の最大値※1
	最小/s	bps の最小値※1
pps	平均/s	pps の平均値
	最大/s	pps の最大値※1
	最小/s	pps の最小値※1
送信バイト数	合計	送信バイト数の合計値
送信パケット数	合計	送信パケット数の合計値
送信 bps	平均/s	送信 bps の平均値
	最大/s	送信 bps の最大値※1
	最小/s	送信 bps の最小値※1
送信 pps	平均/s	送信 pps の平均値
	最大/s	送信 pps の最大値※1
	最小/s	送信 pps の最小値※1
TCP RTT(ms) ※2※3※4	平均	平均 TCP 接続時間（Round-Trip Time）（ミリ秒）
	最大	最大 TCP 接続時間（Round-Trip Time）（ミリ秒）
	最小	最小 TCP 接続時間（Round-Trip Time）（ミリ秒）
TCP SRT(ms) ※2※3※5	平均	平均 TCP サーバ応答時間（Server Response Time）（ミリ秒）
	最大	最大 TCP サーバ応答時間（Server Response Time）（ミリ秒）
	最小	最小 TCP サーバ応答時間（Server Response Time）（ミリ秒）

集計対象	集計方法	説明
TCP DELAY(ms) ※2※3※6	平均	平均 TCP サーバ遅延時間（Server Delay Time）（ミリ秒）
	最大	最大 TCP サーバ遅延時間（Server Delay Time）（ミリ秒）
	最小	最小 TCP サーバ遅延時間（Server Delay Time）（ミリ秒）
TCP RTT サンプル数 ※2※3※7	合計	TCP RTT を含むフロー数の合計値
	平均/s	1 秒毎の TCP RTT を含むフロー数の平均値
TCP SRT サンプル数 ※2※3※7	合計	TCP SRT の測定回数の合計値
	平均/s	1 秒毎の TCP SRT の測定回数の平均値
TCP DELAY サンプル数 ※2※3※7	合計	TCP DELAY の測定回数の合計値
	平均/s	1 秒毎の TCP DELAY の測定回数の平均値
TCP 再送パケット数 ※8	合計	TCP 再送パケットのパケット数の合計値
	割合	TCP パケット中の TCP 再送パケット数の割合（%）
TCP 再送 pps※8	平均/s	TCP 再送パケットの pps の平均値
	最大/s	TCP 再送パケットの pps の最大値※1
	最小/s	TCP 再送パケットの pps の最小値※1
TCP 再送バイト数 ※8	合計	TCP 再送パケットのバイト数の合計値
	割合	TCP バイト中の TCP 再送バイト数の割合（%）
TCP 再送 bps※8	平均/s	TCP 再送パケットの bps の平均値
	最大/s	TCP 再送パケットの bps の最大値※1
	最小/s	TCP 再送パケットの bps の最小値※1
TCP パケットロス回数※8	合計	TCP パケットロス回数の合計値
	平均/s	1 秒毎の TCP パケットロス回数の平均値
	最大/s	1 秒毎の TCP パケットロス回数の最大値※1
	最小/s	1 秒毎の TCP パケットロス回数の最小値※1
	割合	TCP パケット中の TCP 再送パケットロス回数の割合（%）
TCP 重複 ACK パケット数※8	合計	TCP 重複 ACK パケットのパケット数の合計値
TCP 重複 ACKpps ※8	平均/s	1 秒毎の TCP 重複 ACK パケットのパケット数の平均値
	最大/s	1 秒毎の TCP 重複 ACK パケットのパケット数の最大値※1
	最小/s	1 秒毎の TCP 重複 ACK パケットのパケット数の最小値※1
UDP DELAY(ms) ※2	平均	平均 UDP 遅延時間（Delay Time）（ミリ秒）
	最大	最大 UDP 遅延時間（Delay Time）（ミリ秒）
	最小	最小 UDP 遅延時間（Delay Time）（ミリ秒）
UDP JITTER(ms) ※2	平均	UDP ジッタの平均値（ミリ秒）
	最大	UDP ジッタの最大値（ミリ秒）
	最小	UDP ジッタの最小値（ミリ秒）
UDP RTP RTT(ms) ※2	平均	平均 UDP RTP 応答時間（Round-Trip Time）（ミリ秒）
	最大	最大 UDP RTP 応答時間（Round-Trip Time）（ミリ秒）

集計対象	集計方法	説明
	最小	最小 UDP RTP 応答時間（Round-Trip Time）（ミリ秒）
UDP RTP DELAY(ms) ※2	平均	平均 UDP RTP 遅延時間（Delay Time）（ミリ秒）
	最大	最大 UDP RTP 遅延時間（Delay Time）（ミリ秒）
	最小	最小 UDP RTP 遅延時間（Delay Time）（ミリ秒）
UDP RTP JITTER(ms) ※2	平均	UDP RTP ジッタの平均値（ミリ秒）
	最大	UDP RTP ジッタの最大値（ミリ秒）
	最小	UDP RTP ジッタの最小値（ミリ秒）
UDP DELAY(サンプル数) ※2※7	合計	UDP DELAY の測定回数の合計値
	平均/s	1 秒毎の UDP DELAY の測定回数の平均値
UDP JITTER(サンプル数) ※2※7	合計	UDP JITTER を含むフロー数の合計値
	平均/s	1 秒毎の UDP JITTER を含むフロー数の平均値
UDP RTP RTT(サンプル数) ※2※7	合計	UDP RTP RTT を含むフロー数の合計値
	平均/s	1 秒毎の UDP RTP RTT を含むフロー数の平均値
UDP RTP DELAY(サンプル数) ※2	合計	UDP RTP DELAY の測定回数の合計値
	平均/s	1 秒毎の UDP RTP DELAY の測定回数の平均値
UDP RTP JITTER(サンプル数) ※2※7	合計	UDP RTP JITTER を含むフロー数の合計値
	平均/s	1 秒毎の UDP RTP JITTER を含むフロー数の平均値
UDP RTP 順序違反回数 ※2	合計	UDP RTP 順序違反回数の合計値
	平均/s	1 秒毎の UDP RTP 順序違反回数の平均値
	最大/s	1 秒毎の UDP RTP 順序違反回数の最大値※1
	最小/s	1 秒毎の UDP RTP 順序違反回数の最小値※1
UDP RTP ロストパケット数 ※2	合計	UDP RTP ロストパケット数の合計値
	割合	UDP RTP パケット数に対する UDP RTP ロストパケット数の割合(%)
UDP RTP ロスト pps ※2	平均/s	1 秒毎の UDP RTP ロストパケット数の平均値
	最大/s	1 秒毎の UDP RTP ロストパケット数の最大値※1
	最小/s	1 秒毎の UDP RTP ロストパケット数の最小値※1
NAT 継続時間(s)	合計	NAT 継続時間の合計値（秒）
	平均	NAT 継続時間の平均値（秒）
	最大	NAT 継続時間の最大値（秒）
	最小	NAT 継続時間の最小値（秒）

※1. AX-Collector において 1 秒毎の最大値，最小値を監視する場合は，AX-Sensor の設定においても，フローを集計した際のエントリ有効期限を 1 秒に設定してください。

※2. 遅延情報の監視を行う場合は，AX-Sensor の設定においても，TCP 遅延測定機能，UDP 情報測定機能を有効にしてください。

※3. 特定のサーバ／クライアント間の TCP 遅延情報を監視する場合は，絞り込み条件の宛先 IPv4／IPv6 アドレスにサーバのアドレスを指定し，送信元 IPv4／IPv6 アドレスにクライアントのアドレスを指定してください。

※4. 監視期間に TCP RTT を含むフローが無い場合，TCP RTT 補完時間に指定した値を採用します。

※5. 監視期間に TCP SRT を含むフローが無い場合，データ無しとして扱います。

※6. 監視期間に TCP DELAY を含むフローが無い場合，データ無しとして扱います。

※7. 監視期間に各遅延情報を含むフローが無い場合，値 0 として扱います。

※8. TCP 再送カウンタ数の監視を行う場合は，AX-Sensor の設定においても TCP 再送情報の測定を有効にしてください。

4.5 フローランキング監視機能（閾値監視）の設定

フローランキング監視機能（閾値監視）の設定をおこないます。

各項目の設定方法や設定内容については，「5. AX-Collector の Web インタフェース」も参照してください。

4.5.1 環境設定

（1） フローランキング監視の環境設定

ナビゲーションバーより，「データ監視設定」を選択し，「フローランキング監視」の表示項目から「環境設定」を選択してください。

「変更」ボタンを押下し，フローランキング監視環境設定の更新画面を表示してください。

収集周期等を入力し，「更新」ボタンを押下してください。

4.5.2 監視設定

本項で記載する各項目の登録方法として，次の 2 つの方法があります。いずれかの方法で登録を行ってください。

・Web インタフェースの各設定項目から登録する

・設定項目毎に設定内容を入力した CSV ファイルを作成し，Web インタフェースの「データ監視設定」－「フローランキング監視」の「一括登録・更新」の項目から，作成した CSV ファイルを取り込み，一括で登録する。

（1） フローランキング監視項目の登録

ナビゲーションバーより，「データ監視設定」を選択し，「フローランキング監視」の表示項目から「フローランキング監視項目」を選択してください。

「新規登録」ボタンを押下し，フローランキング監視項目の登録画面を表示してください。

名前およびデータ名，絞り込み条件，集約条件，集計対象等を入力し，「登録」ボタンを押下してください。

絞り込み条件は複数行設定することができ，同一行内は AND 条件で判定します。各行間は，除外をチェックした場合は AND NOT，それ以外は OR 条件で判定します。

集約条件は，集計対象のランキング集計時に抽出するフィールドを指定します。最大５つの組み合わせを指定可能です。

集計対象は，集計対象と集計方法の組み合わせを指定します。最大１０個の集計値を指定可能です。また，集計値の閾値監視を行う場合は，集計値（あるいは集計値の割合）に対する上限閾値，下限閾値にも適切な値を指定してください。閾値は集約条件に指定したフィールド毎のランク別集計値と，集約条件に分類しない場合の全体に対するトータル集計値のそれぞれに指定可能です。

また，必要に応じて，次の通知機能の設定を行ってください。

・Syslog 通知を使用する場合，syslog(ランク別)／syslog(トータル)のチェックボックスの有効化および重要度，参照先 URL の入力を行ってください。

・Email 通知を使用する場合，チェックボックスの有効化を行ってください。

監視周期も選択してください。

4.5.3 フローランキング監視の集計対象

フローランキング監視項目の登録において，集計対象と集計方法の組み合わせを指定します。

指定可能な集計対象と集計方法の組み合わせの詳細を次に示します。

表 4-8 フローランキング監視 指定可能な集計対象と集計方法の組み合わせ

集計対象	集計方法	説明
表 4-6 フロー監視 指定可能なユニーク数 参照	ユニーク数	ユニークな値の組み合わせ数 ※2
フローレコード数	合計	フローレコード数の合計値
	平均/s	1 秒毎のフローレコード数の平均値
バイト数	合計	バイト数の合計値
パケット数	合計	パケット数の合計値
bps	平均/s	bps の平均値
pps	平均/s	pps の平均値
送信バイト数	合計	送信バイト数の合計値
送信パケット数	合計	送信パケット数の合計値
送信 bps	平均/s	送信 bps の平均値
送信 pps	平均/s	送信 pps の平均値
TCP 再送パケット数 ※1	合計	TCP 再送パケットのパケット数の合計値
	割合	TCP パケット中の TCP 再送パケット数の割合（%）

集計対象	集計方法	説明
TCP 再送 pps ※1	平均/s	TCP 再送パケットの pps の平均値
TCP 再送バイト数 ※1	合計	TCP 再送パケットのバイト数の合計値
	割合	TCP バイト中の TCP 再送バイト数の割合（%）
TCP 再送 bps ※1	平均/s	TCP 再送パケットの bps の平均値
TCP パケットロス回数 ※1	合計	TCP パケットロス回数の合計値
	平均/s	1 秒毎の TCP パケットロス回数の平均値
	割合	TCP パケット中の TCP パケットロス回数の割合（%）
TCP 重複 ACK パケット数 ※1	合計	TCP 重複 ACK パケットのパケット数の合計値
TCP 重複 ACKpps ※1	平均/s	1 秒毎の TCP 重複 ACK パケットのパケット数の平均値
UDP RTP 順序違反回数 ※1	合計	UDP RTP 順序違反回数の合計値
	平均/s	1 秒毎の UDP RTP 順序違反回数の平均値
UDP RTP ロストパケット数 ※1	合計	UDP RTP ロストパケット数の合計値
	割合	UDP RTP パケット数中の RTP ロストパケット数の割合（%）
URP RTP ロスト pps ※1	平均/s	1 秒毎の UDP RTP ロストパケット数の平均値
NAT 継続時間(s)	合計	NAT 継続時間の合計値（秒）
	平均	NAT 継続時間の平均値（秒）

※1.対象データの監視を行う場合は，AX-Sensor の設定においても，TCP 遅延測定機能，UDP 情報測定機能等を有効にしてください。

※2.ユニーク数の集計値は，集計アルゴリズムに起因する誤差が生じる場合があります。

4.6 外部データ監視機能（閾値監視，Impulse 連携）の設定

外部データ監視機能（閾値監視，Impulse 連携）の設定をおこないます。

外部データとは，外部サーバ等から REST-API により登録する任意の外部データ情報です。

各項目の設定方法や設定内容については，「5. AX-Collector の Web インタフェース」も参照してください。

4.6.1 環境設定

（1） 外部データ監視の環境設定

ナビゲーションバーより，「データ監視設定」を選択し，「外部データ監視」の表示項目から「環境設定」を選択してください。

「変更」ボタンを押下し，収集・監視動作設定の更新画面を表示してください。

収集周期およびプロセス数，タイムアウト時間等を入力し，「更新」ボタンを押下してください。

4.6.2 監視設定

本項で記載する各項目の登録方法として，次の 2 つの方法があります。いずれかの方法で登録を行ってください。

・Web インタフェースの各設定項目から登録する

・設定項目毎に設定内容を入力した CSV ファイルを作成し，Web インタフェースの「データ監視設定」－「外部データ監視」の「一括登録・更新」の項目から，作成した CSV ファイルを取り込み，一括で登録する。

（1） 外部収集データの登録

ナビゲーションバーより，「データ監視設定」を選択し，「外部データ監視」の表示項目から「外部収集データ」を選択してください。

「新規登録」ボタンを押下し，外部収集データの登録画面を表示してください。

外部データカテゴリ名や外部データ名等を入力し，「登録」ボタンを押下してください。

（2）　外部監視データの登録

ナビゲーションバーより，「データ監視設定」を選択し，「外部データ監視」の表示項目から「外部監視データ」を選択してください。

「新規登録」ボタンを押下し，外部監視データの登録画面を表示してください。

監視データカテゴリ名や監視データ名，メトリクス名，外部データ，演算種別，上限閾値監視，下限閾値監視等を入力し，「登録」ボタンを押下してください。

（3）　外部データ監視項目の登録

ナビゲーションバーより，「データ監視設定」を選択し，「外部データ監視」の表示項目から「外部監視項目」を選択してください。

「新規登録」ボタンを押下し，外部データ監視項目の登録画面を表示してください。

監視項目カテゴリ名や監視項目データ名，データセット名，監視データを入力し，監視データ集計のチェックボックスを有効にしてください。

監視機能として，閾値監視および Impulse 連携による監視を動作させる場合には，各機能のチェックボックスを有効化して「登録」ボタンを押下してください。

また，必要に応じて，次の通知機能の設定を行って下さい。

・Syslog 通知を使用する場合，チェックボックスの有効化および重要度，参照先 URL の入力を行ってください。

・SNMP Trap 通知／Email 通知を使用する場合，チェックボックスの有効化を行ってください。

監視周期を選択してください。

4.7 Impulse syslog/trap 送信制御機能の設定

Impulse syslog/trap 送信制御機能の設定をおこないます。

各項目の設定方法や設定内容については，「5. AX-Collector の Web インタフェース」も参照してください。

4.7.1 機能概要

本機能は，Impulse 異常検知/復旧検知が発生した際に出力する syslog/trap の送信頻度を軽減する機能です。

Impulse 異常検知または復旧検知の syslog/trap を送信する最大回数を設定し，最大回数に達した場合，それ以降の Impulse 異常検知/復旧検知による syslog/trap 送信を抑止します。本機能が有効の場合，通知集約機能の有効/無効に関わらず，連続した Impulse 異常検知は最初の 1 回のみ送信します。

本機能が継続動作する期間を制御期間と呼びます。制御期間は異常検知を契機に開始し，第 1 制御単位時間(分)に設定した時間分継続します。

制御期間終了時の検知状態と，制御期間内で最後に送信した syslog/trap の通知種別が不一致の場合，制御期間が終了した契機で現在の通知状態に合わせた syslog/trap を送信します。なお，手動で制御期間を終了した場合は，制御期間終了時の syslog/trap を送信しません。

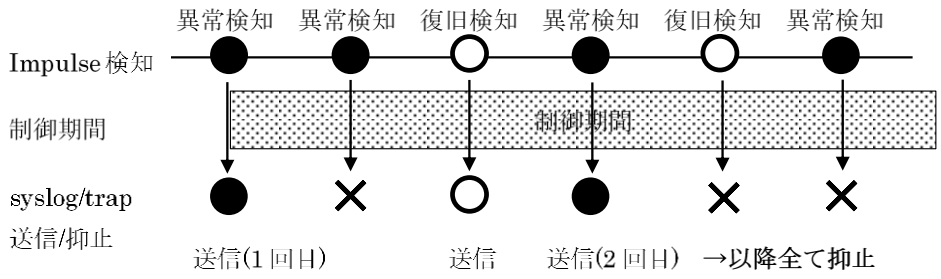

図 4-3 動作概要（異常検知最大送信回数が 2 回の場合の動作例）

4.7.2 基本設定

ナビゲーションバーより，「データ監視設定」を選択し，「Impulse 連携」の表示項目から「syslog/trap 送信制御設定」を選択してください。

「登録」ボタンを押下し，Impulse syslog/trap 送信制御 設定登録画面を表示してください。

送信制御機能のチェックボックスの有効化，異常検知最大送信回数，および第 1 制御単位時間(分)を入力し，「登録」ボタンを押下してください。

4.7.3 制御期間延長オプションの設定

延長オプションを設定することで，制御期間を延長することができます。

（1） Impulse 連携通知受信

制御期間内に Impulse 異常検知が発生すると，その時点から制御期間を単位時間延長します。本オプションを使用する場合は，Impulse syslog/trap 送信制御 設定登録画面で Impulse 連携通知受信のチェックボックスを有効化してください。

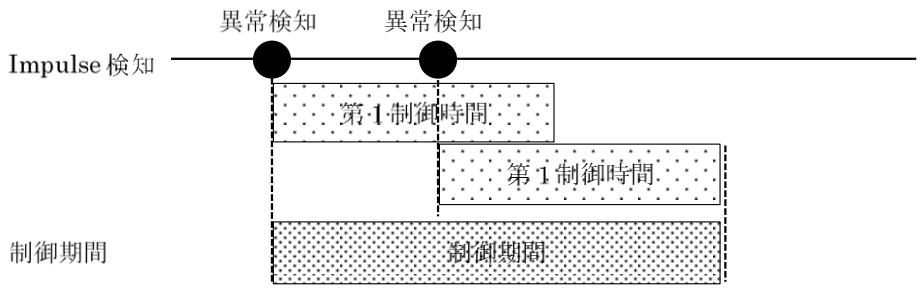

図 4-4 Imulse 連携通知受信による延長動作例

（2） 閾値連携

制御期間の終了のタイミングで監視対象の値と閾値監視機能で設定した閾値とを比較し，閾値外の場合はその時点から制御期間を単位時間延長します。本オプションを使用する場合は，Impulse syslog/trap 送信制御 設定登録画面で閾値連携のチェックボックスを有効化してください。

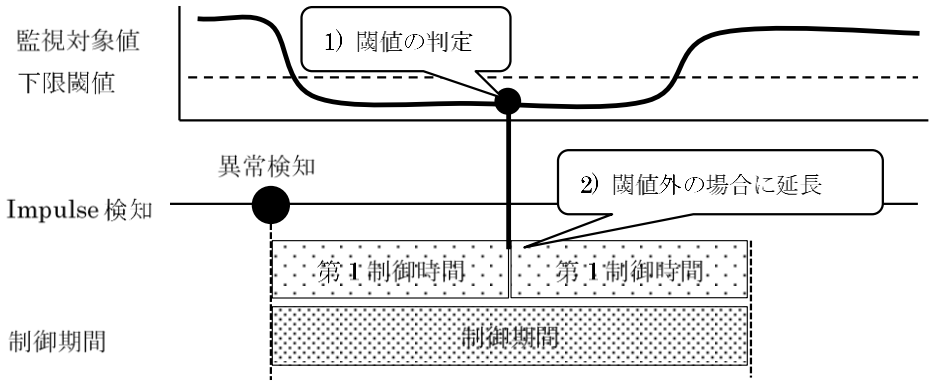

図 4-5　閾値連携による延長動作例

（3）　第 2 制御移行時間および第 2 制御単位時間

第 2 制御移行時間および第 2 制御単位時間に 0 分以外の時間を設定し，制御期間が第 2 制御移行時間に設定した時間を超えると，第 2 制御単位時間による制御に切り替わり，その時点から第 2 制御単位時間を延長した時間が制御期間となります。

第 2 制御移行時間に 0 を登録した場合，第 2 制御単位時間への切り替えを行いません。また，第 2 制御移行時間に 1 以上を登録し，第 2 制御単位時間に 0 を登録した場合，第 2 制御単位時間は無期限となり，手動で削除しない限り，制御期間を継続します。

本オプションを使用する場合は，Impulse syslog/trap 送信制御 設定登録画面で第 2 制御移行時間(分)，および第 2 制御単位時間(分)を登録してください。

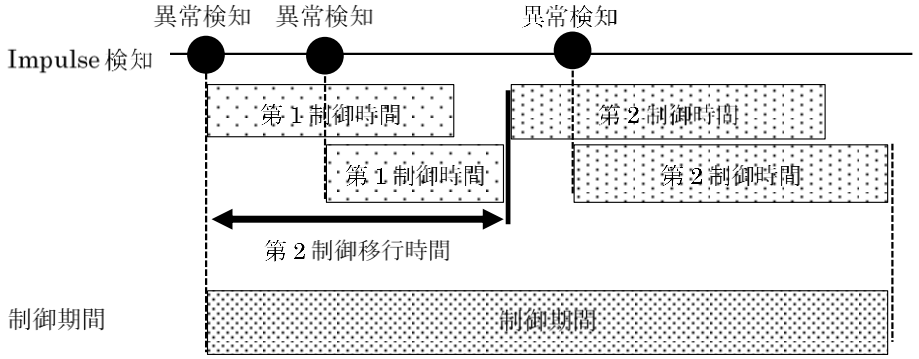

図 4-6　第 2 制御移行時間による動作例

4.8 冗長化機能の設定

本製品を冗長構成で運用する場合の設定をおこないます。

各項目の設定方法や設定内容については，「5. AX-Collector の Web インタフェース」も参照してください。

4.8.1 機能概要

冗長化機能は，本製品の実行環境を２つ準備することで，それぞれ運用系コレクタ，待機系コレクタとして動作する冗長構成で運用する機能です。

本機能を使用することで，運用系コレクタや連携する Impulse に対する死活監視を実施し，異常検出時に，待機系コレクタが新たな運用系コレクタに切り替わり，動作を継続するシステムを構築することが可能です。

冗長化機能有効化時，運用系コレクタと待機系コレクタではいくつかの動作が異なります。運用系コレクタは，非冗長構成時のコレクタと同じ動作を行い，待機系コレクタは監視動作および Syslog/Trap 通知動作を抑止します。次表に動作差分を示します。

表 4-9 運用系／待機系の動作差分

機能		運用系	待機系	備考
可視化		○	○	
SNMP 監視	MIB 収集	○	－	
	監視データ生成	○	△	
	閾値監視	○	△	
フロー監視	フロー受信	○	○	いずれもフロー受信可能です。同期機能はありません。
	監視データ生成	○	△	
	閾値監視	○	△	
Impulse 連携	監視データ送信	○	－	運用系から複数の Impulse にデータ送信可能です。
	検知データ受信	○	△	Impulse から検知データ受信時，待機系コレクタは廃棄します。
冗長化機能監視対象	対向コレクタ	○	○	対向コレクタ死活監視を相互に行います。
	仮想 IP アドレス	○	○	自ノードに仮想 IP アドレスが付与されているかを監視します。
	Impulse	○	○	Impulse の死活監視を行います。

機能		運用系	待機系	備考
運用	Syslog 送信	○	－	
	SNMP Trap 送信	○	－	

（凡例）○：動作，　△：停止，ただし運用系からデータ同期，－：停止

運用系コレクタは，生成した監視データと，その監視結果の検知通知情報を，待機系コレクタへデータ同期を行います。

待機系コレクタは，MIB 収集や SNMP 監視，フロー監視，syslog/trap 送信の動作を行いませんが，同期される監視データと検知通知情報を共有します。

外部データ監視・フローランキング監視については，冗長化機能をサポートしていません。外部データ監視を使用する場合は，冗長化機能を使用しないでください。

次に，運用系コレクタと待機系コレクタ間で同期する情報を示します。コレクタの設定情報に関しては，同期対象外であるため，設定変更はそれぞれのコレクタで行う必要があります。

表 4-10 運用系／待機系の同期情報

情報	同期	説明
SNMP 監視データ	○	運用系から待機系に同期します。
SNMP 閾値監視通知	○	運用系から待機系に同期します。
フロー監視データ	○	運用系から待機系に同期します。
フロー閾値監視通知	○	運用系から待機系に同期します。
フロー情報	－	運用系と待機系のそれぞれで，同じフロー情報を受信する必要があります。
Impulse 検知通知	○	運用系から待機系に同期します。
コレクタ設定情報	－	運用系と待機系のそれぞれで，設定を行う必要があります。SNMP 監視，フロー監視は，同一の設定を行います。

4.8.2　構成

冗長化機能のシステム構成を示します。

（1）　前提条件

冗長構成を構築するには，コレクタおよび連携する Impulse で，次の条件を満たす必要があります。

表 4-11 冗長化機能の前提条件（コレクタ）

項目	内容
コレクタ実行環境	それぞれのコレクタ実行環境が次を満たすこと。 ・CPU やメモリなどのスペックが一致していること。 ・時刻が同期されていること。 ・運用系コレクタ／待機系コレクタ間で相互に IP 通信の到達性があること。※
コレクタ設定	それぞれのコレクタ設定が次を満たすこと。 ・ラインセンス設定 ライセンス種別，有効期間，項目数が一致していること。 ・冗長化機能設定 ヘルスチェック周期が一致していること，IP アドレス構成の設定情報がそれぞれ正しく設定されていること。 ・SNMP 監視 監視項目などの設定情報が一致していること。 ・フロー監視 監視項目などの設定情報が一致していること。 ・Impulse 連携 連携する Impuse が正しく設定されていること。
フロー情報	それぞれのコレクタで，同じフロー情報を受信すること。

※冗長化機能では，運用系コレクタと待機系コレクタ間で，IP 通信による系間通信（ヘルスチェックおよびデータ同期）を行います。この区間で通信障害が発生すると，運用系／待機系の判断が正常に行えなくなります。このため，複数の系間通信パスを用意し，系間通信障害への耐性を高めていただくことをお勧めします。本製品では最大５つのパス（IP アドレス）を用いた系間通信が可能です。

表 4-12 冗長化機能の前提条件（Impulse）

項目	内容
Impulse	異常検知通知先として，連携するコレクタのいずれかが正しく設定されていること。 （２）冗長構成を参照。

（2） 冗長構成

コレクタおよび Impulse の冗長構成を示します。

冗長構成は，コレクタと Impulse の組を２セット用意し，コレクタ＋Impulse を１システムとして扱い，システム冗長をとる構成となります。次の図に接続および動作の概要を示します。

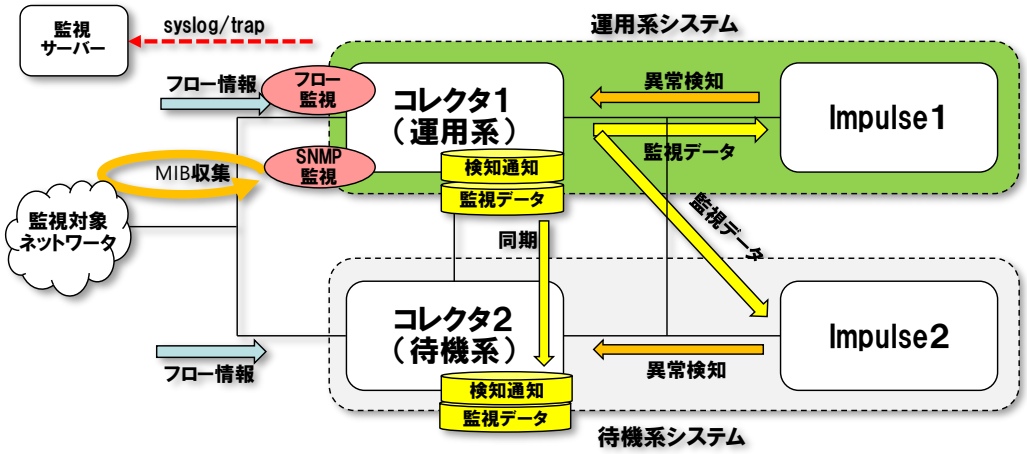

図 4-7　冗長構成図

上図のように，SNMP 監視機能／フロー監視機能における外部とのインタフェース（MIB 収集，および監視サーバへの syslog/trap 通知）は，運用系コレクタのみが実行します。また，Impulse への監視データ送信を運用系コレクタのみが実行することで，どちらの Impulse でも同一データからの学習モデル生成が可能となります。

本構成で運用時，運用系システムのコレクタまたは Impulse に障害が発生した場合，待機系コレクタがフェイルオーバし，新運用系コレクタとして監視動作を継続します。

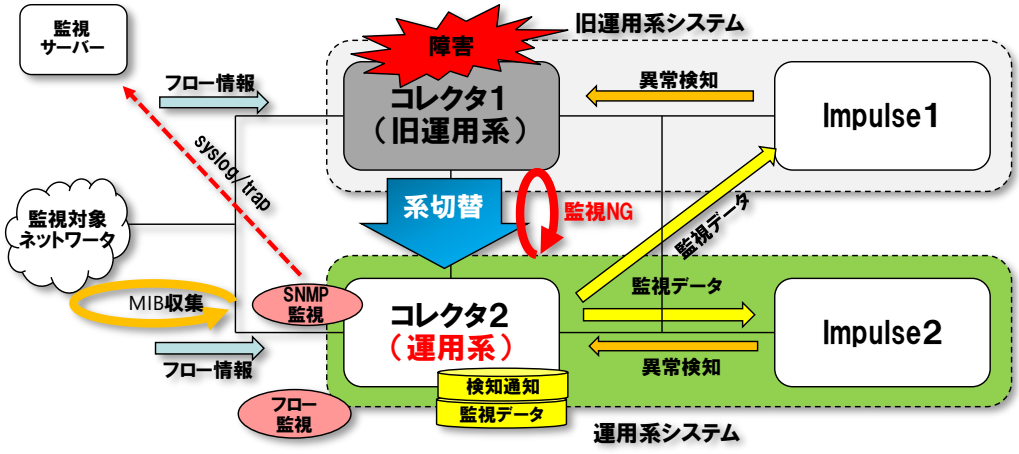

図 4-8　フェイルオーバ動作（運用系システムのコレクタ障害）

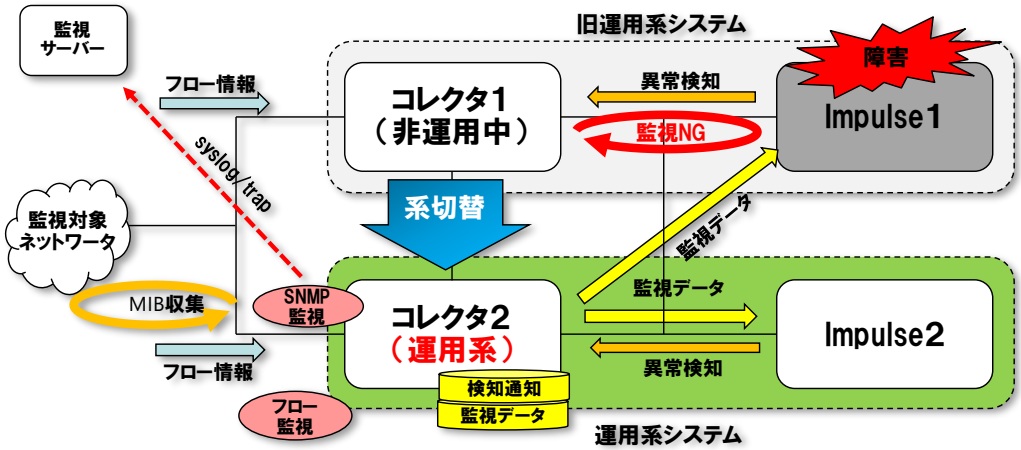

図 4-9　フェイルオーバ動作（運用系システムの Impulse 障害）

（3）　仮想 IP アドレス連携

冗長化機能では，コレクタに設定する特定 IP アドレス（本節では仮想 IP アドレスと表現）と連携するオプション動作が選択可能です。連携する動作は，仮想 IP アドレスを監視し冗長切り替えの条件とする動作，および仮想 IP アドレスを syslog/trap の送信元 IP アドレスとして使用する動作の２つです。

この動作は，ナビゲーションバーより，「管理・設定」を選択し，「冗長」の表示項目から「動作設定」を選択，変更ボタンを押した際の，IP アドレス構成と仮想 IP アドレスで選択可能です。設定可能な，IP アドレス構成と，連携動作を次の表に記載します。

表 4-13IP アドレス構成設定

IP アドレス構成設定	連携動作	
	仮想 IP アドレス監視	Syslog/Trap 送信元 IP アドレス
実 IP アドレス	監視しません。	OS による自動選択（自ノードの送信元インタフェースに付与されている IP アドレス）を使用します。
仮想 IP アドレス	監視します。※１	設定された仮想 IP アドレスを使用します。※２
仮想 IP アドレス（通知のみ）	監視しません。	設定された仮想 IP アドレスを使用します。※２

※１：自ノードのいずれかのインタフェースに，仮想 IP アドレスが存在するかどうかを監視し，運用系コレクタで該当アドレスが存在しなくなった契機で，系切り替え動作が可能です。

※２：送信時，自ノードのいずれかのインタフェースに，仮想 IP アドレスが存在している必

要があります。

この連携機能を利用し，IP アドレス構成が「仮想 IP アドレス」または「仮想 IP アドレス（通知のみ）」の場合，双方のコレクタに同じ仮想 IP アドレスを指定することで，どちらのコレクタが運用系になった場合でも，送信する syslog/trap パケットの送信元 IP アドレスが同じとなります。これにより syslog/trap を受信する監視サーバは，冗長構成のコレクタを同じ管理対象と認識することができます。

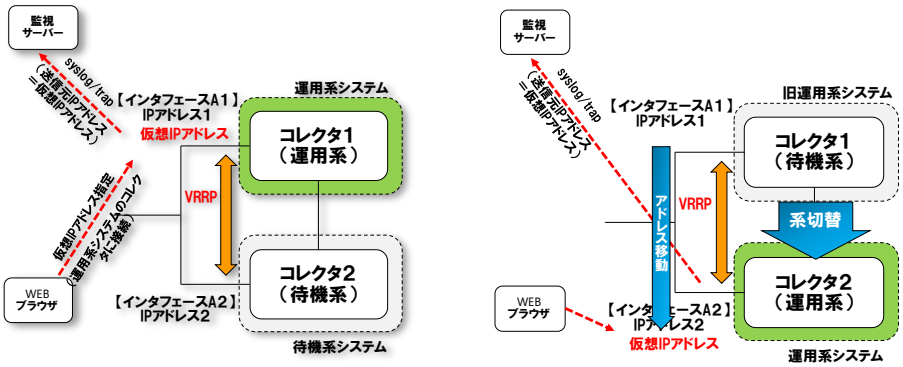

図 4-10　仮想 IP アドレス連携構成例（左図：通常時，右図：切り替え後）

また，IP アドレス構成が「仮想 IP アドレス」の場合，syslog/trap 連携動作に加え，コレクタは設定された仮想 IP アドレスを監視し，その IP アドレスが自ノードに存在しなくなったことを契機に，系切り替えを行うことが可能です。この監視機能を利用し，仮想 IP アドレスを WEB クライアントからアクセス可能であり，VRRP によって制御する仮想 IP アドレスに設定すると，WEB クライアントからのコレクタへのアクセス先を該当アドレスに一元化できます。このとき，仮想 IP アドレスへアクセスすると，運用系コレクタに接続します。（※）

なお，本製品には VRRP 機能は含まれておりません。別途ソフトウェアをご用意，設定いただく必要があります。（参考）動作確認ソフトウェア：keepalived（Copyright (C) 2000-2020 Alexandre Cassen. All rights reserved）

（※）VRRP と連携する構成では，コレクタの系切り替え時に，仮想 IP アドレスも待機系コレクタに移動させる必要があります。このため，VRRP ソフトウェア側で，仮想 IP アドレスの監視条件に自ノードのコレクタが運用系であることを加えてください。自ノードのコレクタが運用系であるかどうかの判定は，次のコマンドと，その応答結果の文字列で，判断可能です。

コマンド： docker container exec ax-collector curl -s -f http://{自ノードコレクタ IP アドレス}/redundancy/v1/healthcheck/

応答結果（運用系コレクタ）： {"system_status_self":"active"}

（参考）keepalived およびコレクタ監視スクリプト設定ファイル例

```
# cat /etc/keepalived/keepalived.conf
! Configuration File for keepalived
global_defs {
}
vrrp_script track_status {
    script "/etc/keepalived/collector_track_status.sh"
    interval 30
    timeout 10
    rise 1
    fall 1
    init_fail
}
vrrp_instance VI_1 {
    state MASTER
    interface <interface name>
    virtual_router_id <VRID>
    priority 100
    advert_int 1
    virtual_ipaddress {
        <仮想 IP アドレス>/24
    }
    track_script {
        track_status
    }
}

# cat /etc/keepalived/collector_track_status.sh
#!/bin/bash
status=`docker container exec ax-collector curl -s -f
http://127.0.0.1/redundancy/v1/healthcheck/`
if [ $? -ne 0 ]; then
    exit 1
elif [ $status != '{"system_status_self":"active"}' ]; then
    exit 2
else
    exit 0
fi
```

4.8.3 基本設定

本節では，**図 4-11 冗長構成設定例**における IP アドレス構成別の設定例を記載します。コレクタ１（運用系），コレクタ２（待機系）でそれぞれ設定を行います。

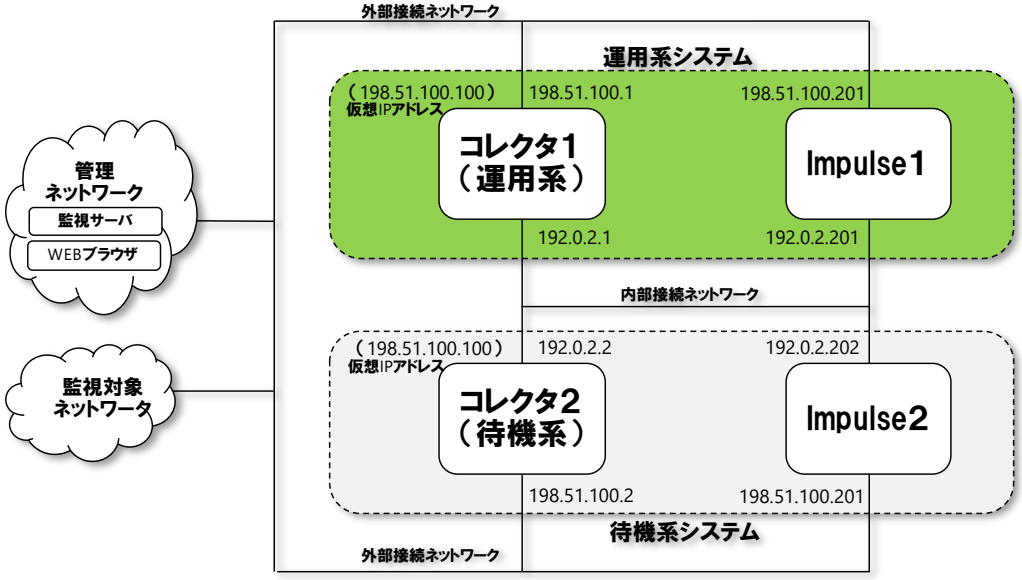

図 4-11 冗長構成設定例

設定は，冗長化機能の設定，および Impulse 連携の設定となります。

冗長化機能の設定は，ナビゲーションバーより，「管理・設定」を選択し，「冗長」の表示項目から「動作設定」を選択してください。変更ボタンを押下し設定します。

Impulse 連携の設定は，ナビゲーションバーより，「データ監視設定」を選択し，「Impulse 連携設定」の表示項目から「Impulse 接続」を選択してください。「新規」ボタンを押下し設定します。

（1） IP アドレス構成「実 IP アドレス」の設定例

コレクタ冗長設定項目の IP アドレス構成が「実 IP アドレス」の設定例を記載します。

表 4-14 コレクタ冗長設定例「IP アドレス構成：実 IP アドレス」

設定項目			コレクタ１（運用系）	コレクタ２（待機系）
冗長動作設定	冗長		有効	有効
	自系優先		有効	無効
	ヘルスチェック周期		30 秒間	30 秒間
	IP アドレス構成		実 IP アドレス	実 IP アドレス
	仮想 IP アドレス		－	－
	他系スキーム名		http	http
	他系 IP アドレス 1～5		192.0.2.2	192.0.2.1
	他系ポート番号		80	80
Impulse 接続※	上段表示	設定参照先 IP アドレス	192.0.2.201	192.0.2.202
		設定先ポート番号	5000	5000
		参照先 IP アドレス	198.51.2.201	198.51.2.202
		参照先ポート番号	3000	3000
		通知集約	有効	有効
	下段表示	設定参照先 IP アドレス	192.0.2.202	192.0.2.201
		設定先ポート番号	5000	5000
		参照先 IP アドレス	-	-
		参照先ポート番号	-	-
		通知集約	-	-

※冗長化機能では，Impulse 設定画面上で，一番上に表示される Impulse を監視対象とします。運用系システムのコレクタでは，最上位に Impulse（運用系）の接続先が表示されていることを確認ください。最上位に表示されていない場合は，設定を変更してください。

（2） IP アドレス構成「仮想 IP アドレス（通知のみ）」の設定例

コレクタ冗長設定項目の IP アドレス構成が「仮想 IP アドレス（通知のみ）」の設定例を記載します。Impulse 接続設定は，（1）IP アドレス構成「実 IP アドレス」の設定例と同じです。

表 4-15 コレクタ冗長設定例「IP アドレス構成：仮想 IP アドレス（通知のみ）」

設定項目		コレクタ１ （運用系）	コレクタ２ （待機系）
冗長 動作 設定	冗長	有効	有効
	自系優先	有効	無効
	ヘルスチェック周期	30 秒間	30 秒間
	IP アドレス構成	仮想 IP アドレス （通知のみ）	仮想 IP アドレス （通知のみ）
	仮想 IP アドレス ※	198.51.100.100	198.51.100.100
	他系スキーム名	http	http
	他系 IP アドレス 1～5	192.0.2.2	192.0.2.1
	他系ポート番号	80	80

※コレクタのネットワークインタフェースのいずれかに，この IP アドレスをつけておく必要があります。

（3） IP アドレス構成「仮想 IP アドレス」の設定例

コレクタ冗長設定項目の IP アドレス構成が「仮想 IP アドレス」の設定例を記載します。Impulse 接続設定は，（1）IP アドレス構成「実 IP アドレス」の設定例と同じです。

表 4-16 コレクタ冗長設定例「IP アドレス構成：仮想 IP アドレス」

設定項目		コレクタ１ （運用系）	コレクタ２ （待機系）
冗長 動作 設定	冗長	有効	有効
	自系優先	有効	無効
	ヘルスチェック周期	30 秒間	30 秒間
	IP アドレス構成	仮想 IP アドレス	仮想 IP アドレス
	仮想 IP アドレス ※	198.51.100.100	198.51.100.100
	他系スキーム名	http	http
	他系 IP アドレス 1～5	192.0.2.2	192.0.2.1
	他系ポート番号	80	80

※連携する VRRP ソフトウェアで制御する IP アドレスと同じアドレスを設定してください。

（4） Impulse 設定例

冗長構成時，コレクタと同様に，Impulse 側の設定も必要となります。それぞれの Impulse で，自システム側のコレクタを異常検知通知先に設定してください。

表 4-17 コレクタ冗長時の Impulse 側設定例

設定項目	Impulse1 （運用系システム）	Impulse2 （待機系システム）
異常検知通知先コレクタ	192.0.2.1	192.0.2.2

4.9 Syslog 受信機能の設定

Syslog 受信機能の設定をおこないます。

4.9.1 機能概要

ネットワークを構成する機器から Syslog 形式のロギング情報を受信・可視化する機能です。本製品では，次の２つの機能を有しています。

（1） Syslog 可視化機能

Syslog メッセージを受信し，蓄積・表示する機能です。IPv4／UDP の Syslog メッセージの受信のみに対応しています。

受信した Syslog メッセージは，ロギング情報データベース（index 名=ax-collector-logging.yyyy.mm.dd）に蓄積し，WEB インタフェースを通じて一覧表示可能です。重要度や，送信元などのフィルタ条件を指定して表示対象を絞り込み表示できます。

（2） ネットワークトラフィックログ可視化機能

ForiGate 等の外部機器からネットワークトラフィック情報に関する Syslog メッセージを受信時に，メッセージ中のトラフィック情報を抽出し，フロー情報のデータベース（index 名=ax-collector-flowdata.yyyy.mm.dd）に蓄積する機能です。IPv4／UDP かつ CEF 形式の Syslog メッセージのみ対応しています。

本機能の利用で，Syslog 形式で受信する NAT ログ情報をフロー情報として扱うことができます。フロー情報の可視化・監視動作や NAT ログ検索機能も利用できます。

CEF 形式の Syslog メッセージから抽出するトラフィック情報については，「4.9.4 CEF 形式フィールド情報」を参照してください。

4.9.2 構成

Syslog 受信機能の構成イメージを以下に示す。受信した Syslog メッセージはロギング情報 DB に格納されます。さらに,メッセージが CEF 形式のネットワークトラフィックログ情報であった場合には,フロー情報 DB にも抽出データが格納されま

す。

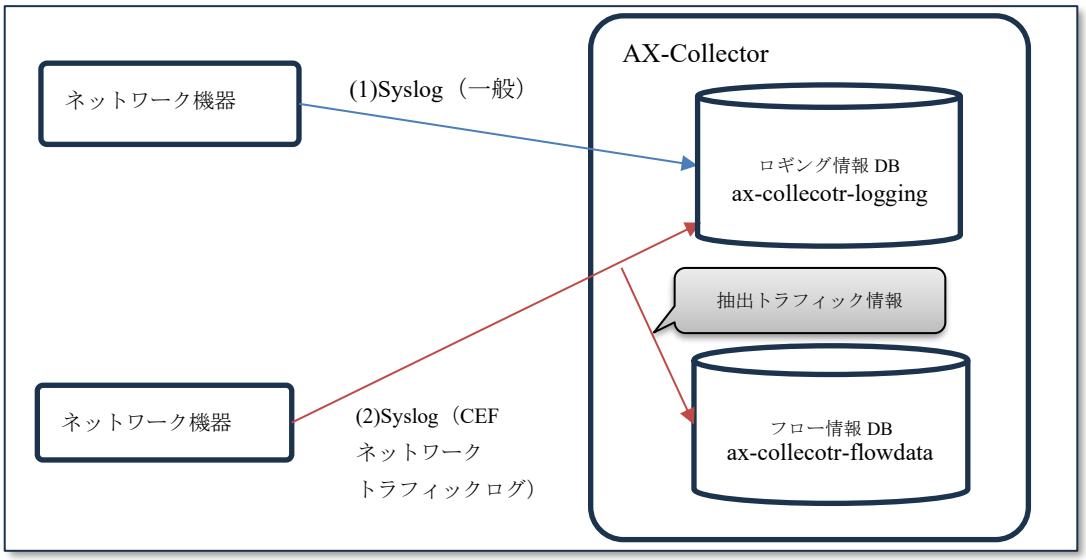

図 4-12　Syslog 受信機能構成イメージ

4.9.3　基本設定

Syslog 受信設定は，AX-Collector インストール時に使用する設定ファイル ax-collector.conf で指定します。Syslog 受信は，設定ファイルに次を記載し，コレクタを起動することで可能となります。初期値は無効となっています。

SYSLOG_RECEIVE_FUNCTION=”ENABLE”

その他の Syslog 受信設定の項目は，「**表 3-4　AX-Collector インストール時の設定項目一覧**」を参照してください。また，WEB インタフェースで Syslog 受信設定を確認可能です。「5.6.3 コレクタ接続環境」も参照してください。

4.9.4　CEF 形式フィールド情報

Syslog メッセージが CEF 形式である場合に，記録する情報を記載します。

表 4-18 Syslog メッセージ CEF 形式抽出情報

項目	説明	備考
CEF DeviceProduct	デバイス名	

項目	説明	備考
CEF DeviceVendor	デバイスベンダ名	
CEF DeviceVersion	デバイスバージョン	
CEF SignatureID	イベント識別子	
CEF Name	イベント文字列	
CEF Severity	イベント重要度（0-10）	10:最重要
CEF Extention	拡張文字列。 Key=Value 形式で空白区切りの文字列。 抽出情報は次の（1）（2）項を参照。	

（1） CEF 拡張文字列（トラフィックログ可視化）

CEF 拡張文字列中に，次表に示すフィールドキーがあった場合には，ネットワークトラフィックログ可視化機能により自動的にフロー情報 DB にフローデータが格納されます。

なお，下表以外にも Syslog 送信元機器の IP アドレスがフローフィールド送信元センサ IP アドレスに記録されます。

表 4-19 CEF Extention フィールドキー情報とフローフィールド情報対応

Extention フィールドキー	フローフィールド	備考
in	バイト数	
out	送信バイト数	
dmac	宛先 MAC アドレス	
smac	送信元 MAC アドレス	
dst	宛先 IPv4 アドレス または 宛先 IPv6 アドレス	v4/v6 は自動判定
src	送信元 IPv4 アドレス または 送信元 IPv6 アドレス	v4/v6 は自動判定
dpt	宛先 L4 ポート番号	
spt	送信元 L4 ポート番号	
proto	プロトコル番号	
destinationTranslatedAddress	NAT 宛先 IPv4 アドレス または NAT 宛先 IPv6 アドレス	v4/v6 は自動判定

Extention フィールドキー	フローフィールド	備考
sourceTranslatedAddress	NAT 送信元 IPv4 アドレス または NAT 送信元 IPv6 アドレス	v4/v6 は自動判定
destinationTranslatedPort	NAT 宛先 L4 ポート番号	
sourceTranslatedPort	NAT 送信元 L4 ポート番号	
FTNTFGTrcvdpkt	パケット数	
FTNTFGTsentpkt	送信パケット数	
FTNTFGTvd	バーチャルドメイン名	
FTNTFGTeventtime または rt	NAT 観測時刻（開始 or 終了）	
FTNTFGTduration または cn3	NAT 継続時間	

（2） CEF 拡張文字列（任意）

CEF 拡張文字列内の任意のフィールド情報を抽出し，ロギング DB に保存することが可能です。抽出したフィールド情報は，Syslog 受信データ表示時にユーザ定義フィールドとして表示やフィルタが可能となります。

抽出可能なユーザ定義の任意フィールド数は 10 個となります。

この任意情報の抽出設定は，コマンドライン上で設定ファイルの編集することで行います。以下は CEF 拡張フィールドの”cat”フィールド値を抽出しユーザ定義フィールド 1（logext01）へ，”tac”フィールド値を抽出しユーザ定義フィールド 2（logext02）へ代入する場合（太枠内が追記内容）の設定例です。

```
# cd インストール(ax-collector-uthility.sh がある)ディレクトリ
# vi ./files/org/ax-telegraf-syslog-user.conf.org
[[processors.ax_copyrename]]
  order = 101                                          ・・・①処理順序
  [[processors.ax_copyrename.replace.field]]
    source = "cat"                                     ・・・②拡張フィールドキー
    dest = "logext01"                                  ・・・③ユーザ定義フィールド
[[processors.ax_copyrename]]
  order = 102                                          ・・・①処理順序
  [[processors.ax_copyrename.replace.field]]
    source = "tac"                                     ・・・②拡張フィールドキー
    dest = "logext02"                                  ・・・③ユーザ定義フィールド
```

図 4-13　Syslog CEF ユーザ定義フィールド抽出設定例

① 処理順序は,101～110 までの値を指定ください。

② 拡張フィールドキーは抽出する CEF 拡張メッセージ内のキー文字列を指定してください。

③ ユーザ定義フィールドは”logext01”～”logext10” のいずれかを指定ください。

また，ユーザ定義フィールドの WEB インタフェース上での表示名称は，ax-collector.conf の設定で変更することも可能です。

変更した設定を動作へ反映するためには，コレクタの再起動，もしくは次のコマンドを実行ください。

```
# ax-collector-utility.sh --syslog-receiver restart
```

4.10 GEOIP 連携機能の設定

フローデータ拡張機能 GEOIP 連携機能の設定をおこないます。

4.10.1 機能概要

センサより受信するフロー情報に含まれる IP アドレスをキーに，位置情報を検索し，可視化する機能です。通信先の国や AS 情報等を取得することが可能です。

本製品では，検索データベースとして MaxMind 社の MMDB※を利用します。

※MaxMind 社　https://www.maxmind.com/

※MMDB フォーマット https://maxmind.github.io/MaxMind-DB/

※本製品には含まれておりません。

本製品で利用可能な MMDB は，City および ASN データベースです。City データベース使用すると国情報等が，ASN データベースを使用すると AS 情報が検索できます。検索可能な情報は次の通りです。ただし，データベース上に情報が格納されていない場合，結果は取得されません。

表 4-20 MMDB と検索対象

データベース	検索対象	説明
City	国コード	国コード（2 文字）ISO3166-1
	国	国名
	地域	地域名（州,県等）
	都市	都市名
	緯度・経度	緯度・経度情報
ASN	AS 番号	AS 番号
	AS 組織名	AS 組織名

これら情報の検索キーとなる IP アドレスは，フロー情報に含まれる IP アドレスフィールドとなります。IP アドレスフィールドは，送信元・宛先毎に次表に示す組み合わせを指定可能です。複数の組み合わせがある項目を指定した場合，後者のキー情報の検索結果を採用します。

4-21 MMDB と検索 IP アドレスフィールド(送信元/宛先)

#	IPv4 アドレス	IPv6 アドレス	NAT IPv4 アドレス	NAT IPv6 アドレス	検索順 左→右列
1	○	-	-	-	IPv4 のみ
2	-	○	-	-	IPv6 のみ
3	-	-	○	-	NAT 後 IPv4 のみ
4	-	-	-	○	NAT 後 IPv6 のみ
5	○	○	-	-	IPv4/IPv6
6	○	-	○	-	IPv4/NAT IPv4
7	○	-	-	○	IPv4/NAT IPv6
8	-	○	○	-	IPv6/NAT IPv4
9	-	○	-	○	IPv6/NAT IPv6
10	○	○	○	-	IPv4/IPv6/NAT IPv4
11	○	○	-	○	IPv4/IPv6/NAT IPv6

○：検索キーとして使用する，－：使用しない

（動作例）上表の#6 を国（宛先）の検索フィールドとして使用した場合

宛先 IPv4 アドレスと NAT 宛先 IPv4 アドレスが含まれているフロー情報を受信すると，宛先 IPv4 アドレスで MMDB を検索し，その後 NAT 宛先 IPv4 アドレスでも検索する動作となります。後者の検索結果が取得できた場合には後者が採用されます。

本動作は,次のように NAT 使用・未使用があるネットワークにおいて，外部ネットワークに抜けるフロー情報の宛先に対する GEOIP 情報取得時に有効です。

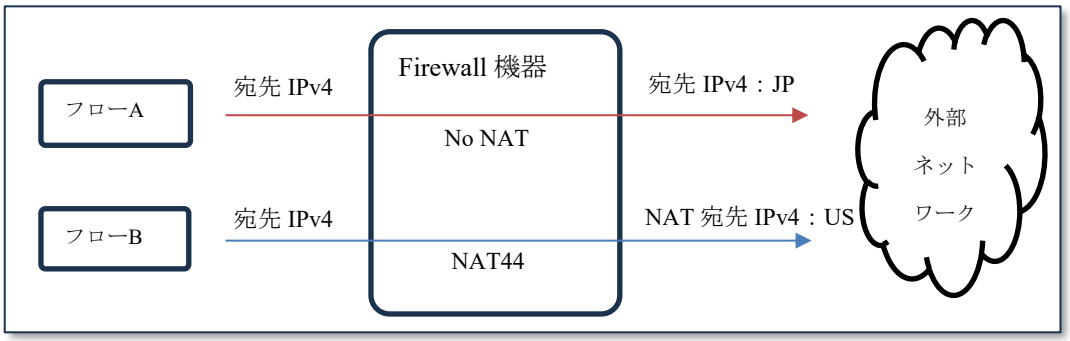

図 4-14　GEOIP 複数フィールド検索時の動作例

4.10.2 基本設定

GEOIP 連携機能を利用するには，次のステップが必要です。

① MMDB の準備

MaxMind 社から City および ASN の MMDB ファイルをダウンロードします。

なお，本製品では独自のプライベート MMDB を作成し，利用することも可能です。このプライベート MMDB のみ使用の場合は，次の手順②は不要です。詳しくは「4.10.3 プライベート MMDB 設定」を参照してください。

② MMDB ファイルのコピー

ダウンロードした MMDB ファイルを，ax-collector.conf の SET_DIR で指定したディレクトリにコピーします。以下は，デフォルトファイル名のコマンド例です。コピー先のファイル名を変更する場合は ax-collector.conf で指定します。

[City MMDB ファイルのコピー]

```
# cp GeoLite2-City.mmdb (SET_DIR 指定ディレクトリ)
```

[ASN MMDB ファイルのコピー]

```
# cp GeoLite2-ASN.mmdb (SET_DIR 指定ディレクトリ)
```

コピーした MMDB ファイルは，③の検索フィールド・格納情報設定を実施する，もしくは次のコマンドの実行で動作に反映されます。MMDB ファイルを更新した場合，この反映手順を実施ください。

[MMDB 再読み込みコマンドの実行]

```
# ./ax-collector-utility.sh --geoip
```

③ 検索フィールド・格納情報設定

WEB インタフェースのナビゲーションバーから,「管理・設定」を選択し，表示メニュー「管理」の「フローデータ拡張」を選択してください。その後，GEOIP データ拡張条件一覧表で，検索フィールド情報と検索情報の設定を行います。

（例）国コード（送信元）を検索，検索フィールドが送信元 IP アドレスの設定

1) GEOIP データ拡張条件一覧から国コード（送信元）に対応する拡張 ID11

の変更ボタンを押下します。

2) 検索フィールドで送信元 IP アドレスを選択し，有効のチェックボックスをチェックした上で更新ボタンを押下します。

以降，フロー情報を受信する際に送信元 IP アドレスから国コードが検索され有効な情報がある場合，フローデータベースに格納されます。この国コード情報は，各種可視化画面やフロー監視機能で参照可能となります。

4.10.3 プライベート MMDB 設定

本機能は IPv4 および IPv6 ネットワークエイリアス設定を元にした City MMDB と ASN MMDB を作成し使用する機能です。本機能を使うと，プライベート IP アドレス情報をキーとした組織情報や位置情報を検索可能な独自のプライベート MMDB を作成し，利用することが可能となります。

プライベート MMDB の作成は，次の手順で行います。作成後は，自動的にフロー受信時の検索動作に適用されます。

1. ナビゲーションバーより，「管理・設定」を選択し，「管理」の表示項目から「フローデータ拡張」を選択してください。
2. GEOIP データ拡張条件一覧表示右側にある「プライベート DB 設定」ボタンを押下し，プライベート DB 作成画面を表示してください。
3. 作成元データ（IPv4／IPv6 ネットワークエイリアス）および MMDB フィールドを指定し，作成ボタンを押下すると作成され動作に反映されます。

作成される MMDB フィールドと IPv4／IPv6 ネットワークエイリアスフィールドとの対応を次の表に示します。例えば City MMDB の国コード情報には，ネットワークエイリアスのコメント 1 フィールドの設定値が格納されます。

表 4-22 プライベート MMDB と IP ネットワークエイリアス対応表

MMDB	MMDB フィールド	IPv4/IPv6 ネットワークエイリアスフィールド	補足
City	国コード	コメント 1	
	国	エイリアス	
	地域	コメント 2	

MMDB	MMDB フィールド	IPv4/IPv6 ネットワーク エイリアスフィールド	補足
	都市	コメント３	
	緯度・経度	コメント４・コメント５	［緯度］ -90 より大きく 90 より小さい数値 ［経度］ -180 より大きく 180 より小さい数値 (*)緯度・経度は，少なくともどちらかが 0 以外の値を指定ください。
ASN	AS 番号	管理番号	0 から 4294967295 の整数値 (*)0 は，「5.9 検索」機能の GEOIP 検索のみ対応しています。
	AS 組織名	管理組織	

以下に本機能使用時の注意事項を記載します。ご理解の上，ご利用ください。

- ✓ ネットワークエイリアス情報を更新した場合には，変更した情報はプライベート MMDB に自動的に反映はされません。反映が必要な場合，再作成を行ってください。
- ✓ プレフィックス長が 0 のネットワークエイリアス情報は，プライベート MMDB に格納されません。
- ✓ IPv6 ネットワークエイリアスで IPv4 互換アドレスを登録した場合，対応する IPv4 アドレスも検索にヒットします。IPv4 ネットワークエイリアスで登録した IPv4 ネットワークアドレスは，対応する IPv4 互換アドレスを持つ IPv6 アドレスも検索にヒットします。
- ✓ 緯度・経度および AS 番号以外のフィールドにおいて，記号文字（”+ - = || ! ( ) { } [ ] ^ " ~ * ? : ¥ /）の利用は非推奨です。記号文字の検索はサポートしていません。
- ✓ 緯度・経度および AS 番号は数値である必要があります。エイリアス情報に数値

以外を設定していた場合，該当情報はプライベート MMDB に格納されません。

- ✓ 作成したプライベート MMDB は，直接バックアップすることができません。バックアップが必要な場合，作成元情報であるネットワークエイリアス情報を保存してください。
- ✓ MaxMind 社の MMDB との併用時，プライベート MMDB に該当するデータがある場合，プライベート MMDB にヒットした情報が記録されます。

4.11 AX-Collector の保守コマンド

この章では，AX-Collector が動作するサーバ上で実行することで，AX-Collector に対して各種操作を行う保守コマンドについて説明します。

保守コマンドを使用する際は，「3.2.2 本製品のインストール」でプログラムを展開したディレクトリに移動して実行してください。

「/home/alaxala/」ディレクトリでプログラムを展開した場合のディレクトリ移動のコマンド実行例を次に示します。

```
# cd /home/alaxala/AXCOLL0113-258-g75de9d4b
```

4.11.1 ユーティリティコマンド

（1） AX-Collector インストール

AX-Collector コンテナイメージの作成，コンテナの作成および起動を行います。

詳細な手順は「3.2.2 本製品のインストール」を参照してください。

［入力形式］

```
./ax-collector-utility.sh --install
```

［実行例］

```
# ./ax-collector-utility.sh --install
Do you want to install?
(y/n):y
ax-collector build start ...
        :
OK: ax-collector container running.
#
```

（2） AX-Collector コンテナイメージ作成

AX-Collector コンテナイメージの作成を行います。

本コマンド実行後，コンテナの作成および起動を行うことで AX-Collector を起動することが出来ます。

［入力形式］

```
./ax-collector-utility.sh --build-only
```

［実行例］

```
# ./ax-collector-utility.sh --build-only
Do you want to build this container image?
(y/n):y
ax-collector build start ...
        :
OK: ax-collector image built.
#
```

（3） AX-Collector コンテナ作成および起動

AX-Collector コンテナの作成および起動を行います。

［入力形式］

```
./ax-collector-utility.sh --run-only
```

［実行例］

```
# ./ax-collector-utility.sh --run-only
ax-collector run start ...
        :
OK: ax-collector container running.
#
```

（4） ユーザ追加

AX-Collector にログインするためのユーザを登録します。

本コマンドは，AX-Collector のインストール時と同じユーザ権限で実行してください。

また，本コマンドによるユーザ追加ではパスワードの脆弱性等のチェックを行いませんので，通常運用時は Web インタフェースのユーザ管理機能からユーザの追加登録を行ってください。

本コマンドで作成したユーザのユーザ権限は管理者になります。

［入力形式］

```
./ax-collector-utility.sh --useradd
```

［実行例］

```
# ./ax-collector-utility.sh --useradd
Username: test_user
Password:
Password (again):
OK: User test_user added.
#
```

（5） コンテナ開始

停止状態にある AX-Collector のコンテナの動作を開始します。

動作開始時に ax-collector.conf ファイルに記載の設定を反映します。ただし，各種情報の格納ディレクトリの設定は，本コマンドでは反映されません。

本コマンドは，root 権限で実行してください。

［入力形式］

```
./ax-collector-utility.sh --start
```

［実行例］

```
# ./ax-collector-utility.sh --start
OK: ax-collector started.
#
```

（6） コンテナ停止

AX-Collector のコンテナの動作を停止します。

本コマンドは，AX-Collector のインストール時と同じユーザ権限で実行してください。

［入力形式］

```
./ax-collector-utility.sh --stop
```

［実行例］

```
# ./ax-collector-utility.sh --stop
Do you want to stop ax-collector?
(y/n): y
OK: ax-collector stopped.
#
```

（7） コンテナ削除

AX-Collector のコンテナを削除します。

本コマンド実行時，パラメータに force を指定することで，実行中のコンテナでも強制的に停止して，コンテナの削除を行います。

本コマンドは，AX-Collector のインストール時と同じユーザ権限で実行してください。

本コマンドは AX-Collector のコンテナが停止している状態で実行してください。

［入力形式］

```
./ax-collector-utility.sh --remove-container [force]
```

［パラメータ］

force
　強制的にコンテナを削除します。

［実行例］

```
# ./ax-collector-utility.sh --remove-container
Do you want to remove ax-collector?
(y/n): y
OK: ax-collector container removed.
#
```

（8） コンテナイメージ削除

AX-Collector のコンテナイメージを削除します。

本コマンドは，AX-Collector のインストール時と同じユーザ権限で実行してください。

本コマンドは，AX-Collector のコンテナを削除した状態で実行してください。

［入力形式］

```
./ax-collector-utility.sh --remove-image
```

［実行例］

```
# ./ax-collector-utility.sh --remove-image
Do you want to remove ax-collector?
(y/n): y
```

```
OK: ax-collector image removed.
#
```

（9） バックアップ

AX-Collector のコンフィグレーション設定情報，および検知ログ情報，運用ログ情報のバックアップを取得します。フロー情報，MIB 情報，外部データ等の監視・可視化データは含まれませんので，ご注意下さい。

［入力形式］

```
./ax-collector-utility.sh --backup <file name>
```

［パラメータ］

<file name>
　バックアップファイルを指定します。

［実行例］

```
# ./ax-collector-utility.sh --backup backup.db
OK: DB file backup succeeded.
#
```

（10） リストア

バックアップした AX-Collector のコンフィグレーション設定情報，および検知ログ情報，運用ログ情報を AX-Collector にリストアします。リストア前の AX-Collector の情報は失われるため，リストア実施前にバックアップを取得することをお勧めします。「5.6.6 保守（3）コンフィグ DB 管理」機能で，作成した定期バックアップファイルも指定可能です。

本コマンドは，root 権限で実行してください。

本コマンドは，AX-Collector のコンテナが停止している状態で実行してください。

バックアップファイルは同じバージョンで作成したものを使用してください。

［入力形式］

```
./ax-collector-utility.sh --restore <file name>
```

［パラメータ］

<file name>
　バックアップファイルを指定します。

［実行例］

```
# ./ax-collector-utility.sh --restore backup.db
Do you want to overwrite the DB file?
(y/n) : y
OK: DB file restoration succeeded.
Please start ax-collector.
#
```

（11） SNMP 監視機能の開始・停止

SNMP 監視機能を開始，または停止します。

SNMP 監視機能が停止している状態では，MIB の取得，MIB 値に対する閾値監視，MIB 値に対する Impulse 連携による監視は動作しません。AX-Collector が起動した際，SNMP 監視機能は自動的に開始します。

本コマンドは，AX-Collector のインストール時と同じユーザ権限で実行してください。

［入力形式］

```
./ax-collector-utility.sh --snmpmonitor { start | stop | status }
```

［パラメータ］

start
　SNMP 監視機能を開始します。

stop
　SNMP 監視機能を停止します。

status
　SNMP 監視機能の動作状態を表示します。

［実行例］

動作開始：

```
# ./ax-collector-utility.sh --snmpmonitor start
OK: Snmpmonitor started.
#
```

動作停止：

```
# ./ax-collector-utility.sh --snmpmonitor stop
Do you want to stop snmpmonitor?
(y/n): y
```

OK: Snmpmonitor stopped.
#
動作状態表示（動作時）：
./ax-collector-utility.sh --snmpmonitor status
Status: active (running) since Mon 2018-11-13 20:18:11 JST; 13min ago
#
動作状態表示 （停止時）：
./ax-collector-utility.sh --snmpmonitor status
Status: inactive (dead) since Mon 2018-11-13 20:18:11 JST; 13min ago
#

（12） フロー監視機能の開始・停止

フロー監視機能を開始，または停止します。

フロー監視機能が停止している状態では，フローに対する閾値監視，フローに対するImpulse 連携による監視は動作しません。AX-Collector が起動した際，フロー監視機能は自動的に開始します。

本コマンドは，AX-Collector のインストール時と同じユーザ権限で実行してください。

［入力形式］

./ax-collector-utility.sh --flowmonitor { start | stop | status }

［パラメータ］

start
　フロー監視機能を開始します。
stop
　フロー監視機能を停止します。
status
　フロー監視機能の動作状態を表示します。

［実行例］

動作開始：
./ax-collector-utility.sh --flowmonitor start
OK: Flowmonitor started.
#
動作停止：

```
# ./ax-collector-utility.sh --flowmonitor stop
Do you want to stop flowmonitor?
(y/n): y
OK: Flowmonitor stopped.
#
動作状態表示 （動作時） :
# ./ax-collector-utility.sh --flowmonitor status
Status: active (running) since Fri 2019-06-28 10:00:37 JST; 39min ago
 :
#
動作状態表示 （停止時） :
# ./ax-collector-utility.sh --flowmonitor status
Status: inactive (dead) since Mon 2018-11-13 20:18:11 JST; 13min ago
 :
#
```

（13） フローランキング監視機能の開始・停止

フローランキング監視機能を開始，または停止します。

フローランキング監視機能が停止している状態では，フローに対する閾値監視は動作しません。AX-Collector が起動した際，フローランキング監視機能は自動的に開始します。

本コマンドは，AX-Collector のインストール時と同じユーザ権限で実行してください。

［入力形式］

```
./ax-collector-utility.sh --flowagg { start | stop | status }
```

［パラメータ］

start
　フローランキング監視機能を開始します。

stop
　フローランキング監視機能を停止します。

status
　フローランキング監視機能の動作状態を表示します。

［実行例］

動作開始：

```
# ./ax-collector-utility.sh --flowagg start
OK: FlowAgg started.
#
```

動作停止：

```
# ./ax-collector-utility.sh --flowagg stop
Do you want to stop FlowAgg?
(y/n): y
OK: FlowAgg stopped.
#
```

動作状態表示 （動作時）：

```
# ./ax-collector-utility.sh --flowagg status
Status: active (running) since Sun 2023-05-28 10:00:37 JST; 39min ago
 :
#
```

動作状態表示 （停止時）：

```
# ./ax-collector-utility.sh --flowagg status
Status: inactive (dead) since Mon 2023-05-29 20:18:11 JST; 13min ago
 :
#
```

（14） 外部データ監視機能の開始・停止

外部データ監視機能を開始，または停止します。

外部データ監視機能が停止している状態では，外部データに対する監視データ集計，閾値監視，および Impulse 連携による監視は動作しません。ただし，外部データ収集は動作します。AX-Collector が起動した際，外部データ監視機能は自動的に開始します。

本コマンドは，AX-Collector のインストール時と同じユーザ権限で実行してください。

［入力形式］

```
./ax-collector-utility.sh --extmonitor { start | stop | status }
```

［パラメータ］

start
　外部データ監視機能を開始します。

stop

外部データ監視機能を停止します。

status

外部データ監視機能の動作状態を表示します。

［実行例］

動作開始：

./ax-collector-utility.sh --extmonitor start

OK: Extmonitor started.

#

動作停止：

./ax-collector-utility.sh -- extmonitor stop

Do you want to stop extmonitor?

(y/n): y

OK: Extmonitor stopped.

#

動作状態表示 （動作時）：

./ax-collector-utility.sh --extmonitor status

Status: active (running) since Fri 2019-06-28 10:00:37 JST; 39min ago

：

#

動作状態表示 （停止時）：

./ax-collector-utility.sh --extmonitor status

Status: inactive (dead) since Mon 2018-11-13 20:18:11 JST; 13min ago

：

#

（15） 冗長化機能の開始・停止

冗長化機能を開始，または停止します。

冗長化機能が停止している状態では，冗長構成に関連する機能は動作しません。AX-Collector が起動した際，冗長化機能は自動的に開始します。

本コマンドは，AX-Collector のインストール時と同じユーザ権限で実行してください。

［入力形式］

./ax-collector-utility.sh --redundancymanagement { start | stop | status }

［パラメータ］

start

冗長化機能を開始します。

stop

冗長化機能を停止します。

status

冗長化機能の動作状態を表示します。

［実行例］

動作開始：

./ax-collector-utility.sh --redundancymanagement start

OK: Redundancymanagement started.

#

動作停止：

./ax-collector-utility.sh --redundancymanagement stop

Do you want to stop redundancymanagement?

(y/n): y

OK: Redundancymanagement stopped.

#

動作状態表示 （動作時）：

./ax-collector-utility.sh --redundancymanagement status

Status: active (running) since Mon 2018-11-13 20:18:11 JST; 13min ago

：

#

動作状態表示 （停止時）：

./ax-collector-utility.sh --redundancymanagement status

Status: inactive (dead) since Mon 2018-11-13 20:18:11 JST; 13min ago

：

#

（16） スナップショット作成

AX-Collector 上に保存されている MIB 情報，フロー情報，外部データ等の監視・可視化データのスナップショットを作成します。

［入力形式］

./ax-collector-utility.sh --snapshot create <index name> <snapshot name>

［パラメータ］

<index name>
スナップショットを作成する対象のインデックス名を指定します。

<snapshot name>
作成するスナップショットの名称を指定します。

［実行例］

```
# ./ax-collector-utility.sh --snapshot create “ax-collector-snmp-2018.11.13”
“snapshot-snmp-2018.11.13”
OK: ax-collector-snmp-2018.11.13 created.
#
```

（17） SNMP 監視 送信元ポート番号設定

SNMP 監視環境設定の送信元ポート番号の変更を，コレクタが停止した状態で登録します。設定変更はコレクタ起動直後に DB に反映されます。

SNMP 監視はコレクタ起動直後から動作するため，SNMP 監視が動作開始する前に予め送信元ポート番号を変更したい場合に本コマンドを使用します。

コレクタ起動中に本コマンドを実行した場合は，即座には設定変更が反映されず，次回コレクタ起動時に反映されます。

本コマンドは root 権限で実行してください。

［入力形式］

```
./ax-collector-utility.sh --set-snmp-source-port <port number>
```

［パラメータ］

<port number>
SNMP 監視の送信元ポート番号です。
設定可能なポート番号の範囲は 1～65535 です。

［実行例］

```
# ./ax-collector-utility.sh --set-snmp-source-port 16000
OK: Configuration completed.
#
```

（18） 監視停止設定

SNMP 監視環境設定のデータ収集，フロー監視環境設定のデータ収集，外部データ監

視環境設定の監視データ集計を無効にする設定を，コレクタが停止した状態で登録します。設定変更はコレクタ起動直後に DB に反映されます。

各監視機能はコレクタ起動直後から動作するため，コレクタ起動直後から監視機能を動作させたくない場合に本コマンドを使用します。

コレクタ起動中に本コマンドを実行した場合は，即座には設定変更が反映されず，次回コレクタ起動時に反映されます。

本コマンドは root 権限で実行してください。

［入力形式］

```
./ax-collector-utility.sh --set-monitor-disable
```

［実行例］

```
# ./ax-collector-utility.sh --set-monitor-disable
OK: Configuration completed.
#
```

（19） GEOIP 連携設定

GEOIP 連携機能で使用している MMDB を再読み込みします。MMDB ファイル更新後に実行します。プライベート MMDB 作成時には実行不要です。

なお，MMDB ファイル名を変更する場合，コレクタの停止・起動が必要です。

本コマンドは root 権限で実行してください。

［入力形式］

```
./ax-collector-utility.sh --geoip
```

［実行例］

```
# ./ax-collector-utility.sh --geoip
OK: GeoIP configuration successfully applied.
#
```

（20） Syslog 受信機能設定

Syslog 受信機能の動作を表示または変更します。

本コマンドは root 権限で実行してください。

［入力形式］

./ax-collector-utility.sh --syslog-receiver { start | restart | stop | status }

［パラメータ］

start

Syslog 受信機能を開始します。

restart

Syslog 受信機能を再起動します。

stop

Syslog 受信機能を停止します。

status

Syslog 受信機能の動作状態を表示します。

［実行例］

動作開始：

./ax-collector-utility.sh --syslog-receiver start
Successfully copied 1.54kB to ax-collector:/var/tmp/ax-collector/conf/
Successfully copied 2.05kB to ax-collector:/opt/ax-loadbalancer/
Successfully copied 20.5kB to ax-collector:/etc/telegraf
Successfully copied 20.5kB to ax-collector:/etc/telegraf
Successfully copied 20.5kB to ax-collector:/etc/telegraf
Successfully copied 20.5kB to ax-collector:/etc/telegraf
Successfully copied 9.22kB to ax-collector:/etc/telegraf
Successfully copied 1.54kB to ax-collector:/etc/telegraf
Successfully copied 3.07kB to ax-collector:/usr/local/share/ax-collector/logmonitor/
OK: The syslog receiver started.

動作再起動：

./ax-collector-utility.sh --syslog-receiver restart
Successfully copied 1.54kB to ax-collector:/var/tmp/ax-collector/conf/
Successfully copied 2.05kB to ax-collector:/opt/ax-loadbalancer/
Successfully copied 20.5kB to ax-collector:/etc/telegraf
Successfully copied 20.5kB to ax-collector:/etc/telegraf
Successfully copied 20.5kB to ax-collector:/etc/telegraf
Successfully copied 20.5kB to ax-collector:/etc/telegraf
Successfully copied 9.22kB to ax-collector:/etc/telegraf
Successfully copied 1.54kB to ax-collector:/etc/telegraf

Successfully copied 3.07kB to ax-collector:/usr/local/share/ax-collector/logmonitor/
Do you want to restart the syslog receiver?
(y/n): y
OK: The syslog receiving function restared.

動作停止：

./ax-collector-utility.sh --syslog-receiver stop
Do you want to stop the syslog receiver?
(y/n): y
OK: The syslog receiver stopped.

動作状態表示（動作時）：

./ax-collector-utility.sh --syslog-receiver status
● ax-telegraf-syslog-bsd@01.service - Telegraf
Active: active (running) since Wed 2025-10-29 16:47:25 JST; 1 weeks 6 days ago
● ax-telegraf-syslog-bsd@02.service - Telegraf
Active: active (running) since Wed 2025-10-29 16:47:27 JST; 1 weeks 6 days ago
● ax-telegraf-syslog-ietf@01.service - Telegraf
Active: active (running) since Wed 2025-10-29 16:47:26 JST; 1 weeks 6 days ago
● ax-telegraf-syslog-ietf@02.service - Telegraf
Active: active (running) since Wed 2025-10-29 16:47:27 JST; 1 weeks 6 days ago
● ax-loadbalancer-syslog.service - ax-loadbalancer-syslog
Active: active (running) since Wed 2025-10-29 16:47:25 JST; 1 weeks 6 days ago
#

5. AX-Collector の Web インタフェース

この章では，インストールした AX-Collector の Web インタフェースへのアクセス方法，および画面構成について説明します。

5.1 AX-Collector の画面構成

AX-Collector の画面構成を以下に示します。

図 5-1 画面構成

表 5-1 構成要素

項番	内容	説明
①	トップ画面へのリンク	AX-Collector トップ画面へのリンクです。 各機能画面で操作中，トップ画面へのリンクを選択することで，トップ画面へと移動します。
②	ナビゲーションバー	提供する各機能への移動を管理するメニュー機能です。メニュー内の機能を選択することで，各機能画面へと移動します。 コレクタ設定でメニュー位置を左サイド設定すると本メニューは画面左に表示されます。
③	ブックマーク，異常検知情報	ブックマーク機能と，異常検知情報の表示メニューです。 コレクタ設定のメニュー位置設定に依存せず，画面上部に表示されます。
④	冗長状態	冗長化機能有効時，冗長状態および自系状態を表示します。ログイン中に選択することで，冗長化機能の動作状況表示画面へと移動します。
⑤	ホスト名	コレクタ設定で設定したホスト名を表示します。
	ログインユーザ名	ログイン中のユーザ名を表示します。 クリックでパスワード変更またはログアウトの実行が可能です。
⑥	画面表示自動更新情報	画面表示の自動更新機能の有効・無効，および有効時の更新間隔を表示します。
⑦	検索	検索ウィンドウを表示します。

項番	内容	説明
⑧	画面表示時刻	現在のページを表示した時刻を表示します。
⑨	階層リンク	現在のページ位置をツリー構造で表示します。上位の階層にリンクをたどって戻ることができます。
⑩	ページリンク	任意に設定した別ページへのリンクを表示します。 また，プラスボタンからページリンクを追加することができます。また，歯車ボタンからページリンクの一覧画面を表示することができます。 コピーボタンでは，現在表示中の画面に対尾する URL が，クリップボートにコピーされます。コピーされる URL は，ホスト部以降でパラメータを含みます。特定ページでは，画面名称指定 URL が設定されます（表 5 63　画面名称指定 URL 対象画面一覧参照）。
⑪	機能画面	各機能の画面です。

5.2 AX-Collector の Web インタフェース機能一覧

AX-Collector の機能一覧，および各機能の概要を次に示します。

表 5-2 AX-Collector の機能一覧

項目	機能	サブ機能	説明
TOP	-	-	設定された TOP ページを表示します。初期設定ではコレクタ稼働状況を表示します。
収集データ表示	ダッシュボード	登録一覧	登録しているダッシュボードの表示対象情報の一覧を表示します。
		プリセットダッシュボード	AX-Collector にて，予め用意しているダッシュボードになります。 IP フロー，あるいは MAC フローに関する複数の情報を可視化するダッシュボードを表示します。
		カスタマイズダッシュボード	運用者が独自にカスタマイズしたダッシュボードを作成し，表示します。
		個別ビュー	IP フロー，あるいは MAC フローを詳細な条件を指定して可視化します。
		監視状況俯瞰ビュー	SNMP 監視，フロー監視および外部データ監視で収集した集計値・検知状況をサマリ表示します。
		MAP ビュー	GEOIP 連携機能利用時，送信元と宛先の位置情報を地図上に表示します。
	フローランキングリスト	登録一覧	登録しているフローリストの表示対象情報の一覧を表示します。
		IP フロー	IP フローをリスト形式で表示します。
		IP フロー複合ビュー	IP フローをグラフおよびリスト形式で表示します。
		MAC フロー	MAC フローをリスト形式で表示します。
		環境設定	フロー検索動作に関する設定を行います。
	SNMP 監視	MIB 収集データ	SNMP 監視において収集した MIB 値をグラフ表示します。
		SNMP 監視データ	SNMP 監視において生成した SNMP 監視データ（MIB オブジェクトグループ）をグラフ表示します。
		SNMP 監視状況	SNMP 監視設定の状況と，SNMP 監視データ（MIB オブジェクトグループ）の生成状況，MIB の収集状況を表示します。
		一括エクスポート	生成した SNMP 監視データ（MIB オブジェクトグループ）を CSV ファイルに出力します。
	フロー監視	フロー監視データ	フロー監視において生成したフロー監視データ（フロー条件グループ）をグラフ表示します。

項目	機能	サブ機能	説明
		フロー監視状況	フロー監視設定の状況と，フロー監視データ（フロー条件グループ）の生成状況を表示します。
		一括エクスポート	生成したフロー監視データ（フロー条件グループ）を CSV ファイルに出力します。
	フローランキング監視	フローランキング監視データ	フローランキング監視において生成した監視データをグラフおよびテーブル表示します。
	外部データ監視	外部収集データ	外部データ監視において収集した外部収集データの値をグラフ表示します。
		外部監視データ	外部データ監視において生成した外部監視データの値をグラフ表示します。
		外部データ監視状況	外部データ監視設定の状況と，外部監視データの生成状況，外部データの収集状況を表示します。
		一括エクスポート	生成した外部監視データを CSV ファイルに出力します。
	Syslog	Syslog 収集データ	受信した Syslog 情報をグラフおよびテーブル表示します。
データ監視設定	SNMP 監視	ネットワーク機器	MIB 情報を取得する対象の装置を登録します。
		MIB オブジェクト	取得対象の MIB の OID を登録します。
		MIB オブジェクトグループ	一つまたは複数の MIB オブジェクトをグループ化して，監視対象となる値を登録します。
		SNMP 監視項目	一つまたは複数の MIB オブジェクトグループに対して監視方法等を登録します。
		一括登録・更新	監視・収集設定に関する情報を一括で登録・更新します。
		環境設定	SNMP 監視動作に関する設定を行います。
	フロー監視	フロー条件	監視対象のフロー条件を登録します。
		フロー条件グループ	一つまたは複数のフロー条件をグループ化して，監視対象となる値を登録します。
		フロー監視項目	一つまたは複数のフロー条件グループに対して監視方法等を登録します。
		一括登録・更新	監視・収集設定に関する情報を一括で登録・更新します。
		環境設定	フロー監視動作に関する設定を行います。
		過去データ／閾値生成・削除	過去の期間を指定して，フロー監視データ／閾値の生成または削除を行います。
	フローランキング監視	フローランキング監視項目	監視対象のフロー条件，集計対象データ，監視方法等を登録します。

項目	機能	サブ機能	説明
		一括登録・更新	監視・収集設定に関する情報を一括で登録・更新します。
		環境設定	フローランキング監視動作に関する設定を行います。
		過去データ生成・削除	過去の期間を指定して，フローランキング監視データの生成または削除を行います。
	外部データ監視	外部収集データ	注入を行う外部データを登録します。
		外部監視データ	一つまたは複数の外部データから生成する，監視対象となる値を登録します。
		外部監視項目	一つまたは複数の外部監視データに対して監視方法等を登録します。
		一括登録・更新	監視・収集設定に関する情報を一括で登録・更新します。
		環境設定	外部データ監視動作に関する設定を行います。
		過去データ生成・削除	過去の期間を指定して，外部監視データの生成または削除を行います。
	Impulse 連携	Impulse 接続	Impulse との接続に関する設定を行います。
		syslog/trap 送信制御状態一覧	Impulse syslog/trap 送信制御機能の制御状態一覧を表示します。
		syslog/trap 送信制御設定	Impulse syslog/trap 送信制御機能の設定を行います。
		Impulse	Impulse の管理ページへの外部リンクです。
管理・設定	可視化エイリアス情報	VLAN-ID	VLAN-ID に関するエイリアスを登録します。
		VLAN(QinQ)	VLAN(QinQ)に関するエイリアスを登録します。
		MAC アドレス	MAC アドレスに関するエイリアスを登録します。
		IPv4 アドレス	IPv4 アドレスに関するエイリアスを登録します。
		IPv4 ネットワーク	IPv4 ネットワークに関するエイリアスを登録します。
		IPv6 アドレス	IPv6 アドレスに関するエイリアスを登録します。
		IPv6 ネットワーク	IPv6 ネットワークアドレスに関するエイリアスを登録します。
		センサ・ポート	IP フロー・MAC フローを生成する AX-Sensor に関するエイリアスを登録します。
		イーサタイプ	イーサタイプに関するエイリアスを登録します。
		プロトコル番号	プロトコル番号に関するエイリアスを登録します。

項目	機能	サブ機能	説明
		L4 ポート番号	L4 ポート番号に関するエイリアスを登録します。
	レポート	レポート一覧	収集したレポートの一覧を表示します。
		レポート設定	レポートを収集するための条件を登録します。
	コレクタ接続環境	コレクタ	コレクタに関する設定を行います。
		Syslog 通知先	Syslog 通知先に関する設定を行います。
		Email 通知先	Email 通知先に関する設定を行います。
		Trap 通知先	SNMP Trap 通知先に関する設定を行います。
		AX-NM 連携環境設定	検索ウィンドウにおいて AX-NM から端末接続履歴を取得するための設定を行います。
		Syslog 受信設定	Syslog 受信機能設定を表示します。
	冗長	概況	冗長状態を表示します。
		系切り替え	冗長構成時，系切り替えを行います。
		動作設定	冗長化機能の設定を行います。
	管理	コレクタ稼働状況	AX-Collector の稼働状況として，フロー受信状況，SNMP 監視状況，フロー監視状況，外部データ監視状況を表示します。
		データ管理	受信したフロー情報や取得した MIB 情報，外部データ情報を管理するデータベースの一覧を表示します。また，蓄積したデータの削除やスナップショットの作成を行います。
		スナップショット管理	データ管理で生成したスナップショットの一覧を表示します。また，スナップショットの削除やデータベースへの復元を行います。
		ユーザ管理	AX-Collector へログインするためのユーザを登録します。
		カスタム権限	ユーザのアクセス範囲を登録します。
		ライセンス管理	ライセンスを登録します。
		フローデータ拡張	フローデータ拡張機能，およびフィールドフィルタ表示に関する設定を行います。
		ページリンク管理	ページリンクに関する設定を行います。
		画像管理	ダッシュボードで表示可能な画像登録を行います。
		検知情報管理	検知一覧画面の表示設定や監視データに紐づける付加情報のリスト登録を行います。
	保守	運用ログ	コレクタの運用ログを表示します。

項目	機能	サブ機能	説明
		アクセスカウンタ	運用ログを分析し，各画面や API アクセスの統計値を表示します。
		コンフィグ DB 管理	コレクタ設定ファイルの定期バックアップ等の設定を行います。
		保守情報	保守情報のダウンロードを行います。
ブックマーク	ブックマーク管理	ブックマーク管理	Web サイト等の URL を登録します。
		ブックマーク一覧	登録したブックマーク一覧を表示します。
		ブックマーク登録	現在表示している画面をブックマークに登録します。
検知	検知状況	検知数カレンダー（今月）	検知通知の 1 日毎の検知数をカレンダー形式で表示します。
		検知数ランキング（今日）	検知数をランキング形式で表示します。
		検知通知一覧（今日）	検知通知を一覧表形式で表示します。
	検知一覧（機能別）	閾値監視通知（SNMP）	SNMP の閾値監視で検知した項目の一覧を表示します。
		閾値監視通知（フロー）	フロー情報の閾値監視で検知した項目の一覧を表示します。
		閾値監視通知（フローランキング）	フローランキングの閾値監視で検知した項目の一覧を表示します。
		閾値監視通知（外部データ）	外部データの閾値監視で検知した項目の一覧を表示します。
		Impulse 連携通知	Impulse で検知した項目の一覧を表示します。
検索	－	－	条件に一致する端末情報の検索を行います。

5.3 TOP

コレクタ設定およびユーザ管理で設定した TOP ページを表示します。

デフォルトではコレクタ稼働状況を表示します。

5.4 収集データ表示

AX-Collector が収集・監視している SNMP MIB 情報やフロー情報，外部データ情報，受信 Syslog 情報を可視化します。

5.4.1 ダッシュボード

AX-Collector が収集しているフロー情報や監視情報等をダッシュボード形式で表示します。

(1) 登録一覧

ダッシュボード 登録一覧の概要を次に示します。

表 5-3 ダッシュボード 登録一覧の概要

項目	説明
プリセット	プリセットダッシュボード一覧を表示します。
カスタマイズ	カスタマイズダッシュボード一覧を表示します。
登録一覧	登録した情報の一覧を表示します。
表示	登録した表示対象とするデータの条件でダッシュボードを表示します。
削除	登録内容を削除します。
検索	表示した一覧情報を対象に検索し，一致したものを表示します。

(2) プリセットダッシュボード

ダッシュボード プリセットダッシュボードの概要を次に示します。

表 5-4 ダッシュボード プリセットダッシュボードの概要

項目	説明
プリセットダッシュボード一覧	プリセットダッシュボードの一覧を表示します。
表示	ダッシュボードを表示します。
個別データ一覧	ダッシュボードを構成している個別データの一覧を表示します。
詳細	ダッシュボードを構成している個別データを表示します。
検索	表示した一覧情報を対象に検索し，一致したものを表示します。
表示対象変更	ダッシュボートの表示対象とするデータの範囲を設定します。 指定可能な条件を次に示します。 ・期間 ：可視化対象のデータの期間およびデータの集計粒度を指定します。 ・センサ・ポート：可視化対象のセンサ，モニタポート，送信ポートを指定します。

項目	説明
表示対象登録	表示対象変更で指定した条件に名称を付与して登録します。 最大 256 文字登録可能です。 登録した情報は登録一覧で表示されます。
画面編集モード	表示しているダッシュボードの編集モードに移行します。 編集モードに移行すると，次の操作が可能となります。 ・表示項目のレイアウト（位置，大きさ）変更 位置変更：対象ビューの上部タイトルをドラッグします。 大きさ変更：対象ビューにマウスをホバーし，左下，右下に表示される矢印アイコンをドラッグします。 ・レイアウト保存 ダッシュボードの各表示項目のレイアウトをサーバもしくはブラウザに保存します。サーバ保存はダッシュボード毎に AX-Collector あたり 1 つ保存できます。
画面編集モード終了	画面編集モードを終了します。 終了時，画面レイアウト保存の実行有無を選択します。

（3） カスタマイズダッシュボード

ダッシュボード カスタマイズダッシュボードの概要を次に示します。

表 5-5 ダッシュボード カスタマイズダッシュボードの概要

項目	説明
新規登録	カスタマイズダッシュボードを作成し，登録します。指定可能な条件を次に示します。 ・名前 ：任意の名前を登録します。最大 256 文字登録可能です。カンマ「,」を除く文字を使用できます。 ・表示対象 ：ダッシュボードに組み込むビューを指定します。以下の機能で作成したビューを指定できます。 個別ビュー SNMP 監視（時系列グラフ） フロー監視（時系列グラフ） 外部データ監視（時系列グラフ） 監視状況俯瞰ビュー 画像 1 つのダッシュボードに最大 20 のビューを指定できます。なお，新規登録後，カスタマイズダッシュボード表示画面の画面編集モードで，テキスト・リンク情報のビューも追加できます。
一覧ダウンロード（CSV）	登録しているカスタマイズダッシュボードの全情報を CSV 形式のファイルとしてダウンロードします。ファイル名は「D1_DashboardMain_<*日付*>.csv」，「D2_DashboardLayout_<*日付*>.csv」，「D3_DashboardCondition_<*日付*>.csv」「D4_DashboardTextArea_<*日付*>.csv」となります。
一括登録・更新	カスタマイズダッシュボード 一括登録・更新を表示します。

項目	説明
一覧表示項目の設定一括変更	カスタマイズダッシュボード一覧の変更可能なフィールドを一括更新します。表形式で編集可能です。 ・更新　：チェックした複数の設定を更新します。同時に変更可能な設定数は最大 20 です。 ・キャンセル　：更新操作をキャンセルします。変更途中の設定は破棄されます。
カスタマイズダッシュボード一覧	登録したカスタマイズダッシュボードの一覧を表示します。
選択設定の削除	一覧でチェックした複数の設定を一括で削除します。
選択設定の複製	一覧でチェックした 1 つの設定を複製します。
表示	ダッシュボードを表示します。
個別データ一覧	ダッシュボードを構成しているビューの一覧を表示します。
データ変更	登録内容を変更します。
表示順登録	ダッシュボードを構成するビューの表示順を変更します。
表示対象変更	ダッシュボートの表示対象とするデータの範囲を設定します。 指定可能な条件を次に示します。 ・期間　：可視化対象のデータの期間を指定します。 ・センサ・ポート：可視化対象のセンサ，モニタポート，送信ポートを指定します。 ただし，個別ビューのみが変更対象となります。
表示対象登録	表示対象変更で指定した条件に名称を付与して登録します。 最大 256 文字登録可能です。 登録した情報は登録一覧で表示されます。
操作	表示しているダッシュボードに対して，次の操作を行います。 ・一覧：ダッシュボードを構成しているビューの一覧を表示します。 ・変更：ダッシュボードを構成しているビューを変更します。 ・登録：ビューの表示順を登録します。 ・削除：ダッシュボードを削除します。
画面編集モード	表示しているダッシュボードの編集モードに移行します。 編集モードに移行すると，次の操作が可能となります。 ・表示項目のレイアウト（位置，大きさ）変更 位置変更：対象ビューの上部タイトルをドラッグします。 大きさ変更：対象ビューにマウスをホバーし，左下，右下に表示される矢印アイコンをドラッグします。 ・レイアウト保存 ダッシュボードの各表示項目のレイアウトをサーバもしくはブラウザに保存します。サーバ保存はダッシュボード毎に AX-Collector あたり 1 つ保存できます。 ・表示項目の追加 ダッシュボードにビューを追加します。追加後は，ダッシュボード画面全体が再描画されます。テキスト・リンク情報は，表示内容の設定をここで行います。 ・表示項目の削除 各ビューの右上に×アイコンが表示されます。押下すると，該当のビューが削除され，ダッシュボード全体が再描画されます。 ・表示項目内容の変更

項目	説明
	テキスト・リンク情報のビューの右上に編集アイコンが表示されます。押下すると，該当のビューの設定変更が可能です。変更後は，ダッシュボード画面全体が再描画されます。
画面編集モード終了	画面編集モードを終了します。 終了時，画面レイアウト保存の実行有無を選択します。

表 5-6　ダッシュボード カスタマイズダッシュボード 画面編集モード 追加の概要

項目	説明
対象データ	ダッシュボードに追加する表示対象を選択します。 次が選択可能な表示対象です。 ・個別ビュー ・監視状況俯瞰ビュー ・SNMP 監視 ・フロー監視 ・外部データ監視 ・画像 ・テキスト・リンク情報
データ	対象データにテキスト・リンク情報以外を選択した場合に，表示されます。 各表示対象の設定済みデータ名称を選択します。
テキスト	対象データにテキスト・リンク情報を選択した場合に表示されます。 ・テキスト： 表示するテキストメッセージです。 最大 256 文字。 ・リンク先 URL： テキストメッセージに埋め込むリンク先の URL です。 ・リンク先 URL インライン表示： リンク先 URL を埋め込み（インラインフレーム）表示するオプションです。リンク先 URL は閲覧が許可されている必要があります。 コレクタ自身（ダッシュボードを設定する同じサーバ）の任意画面の URL も登録可能です。他コレクタの画面は表示できません。 この時，テキストはビューのタイトルとなります。 ・表示サイズ： インライン表示の縦・横サイズを指定します。 設定範囲は，次のいずれかです。 1～9999：ピクセル値 1%～100%：データ表示部（ビュー）内の割合 初期設定は，縦，横共に 100%です。リンク先 URL インライン表示がチェックされている場合に表示されます。

（4） カスタマイズダッシュボード 一括登録・設定

ダッシュボード カスタマイズダッシュボード 一括登録・更新の概要を次に示します。

表 5-7 ダッシュボード カスタマイズダッシュボード 一括登録・更新の概要

項目	説明
一括登録・更新	カスタマイズダッシュボードにおける各登録情報を一括で登録します。一部，または全ての登録項目に，登録情報を入力した CSV ファイルを指定します。 登録項目を次に示します。 ・カスタマイズダッシュボード表示データ： カスタマイズダッシュボードの表示項目に関する情報を入力した CSV ファイルを指定します。 ・カスタマイズダッシュボードレイアウト： カスタマイズダッシュボードの表示順，およびサーバに保存するレイアウトに関する情報を入力した CSV ファイルを指定します。 ・カスタマイズダッシュボード表示条件： 表示対象登録で保存した登録に関する情報を入力した CSV ファイルを指定します。 ・CSV ファイル未記載データ削除： CSV ファイルに入力されていない情報が AX-Collector に既に登録されている場合に削除するか，削除しないかを指定します。

（5） 個別ビュー

ダッシュボード 個別ビューの概要を次に示します。

表 5-8 ダッシュボード 個別ビューの概要

項目	説明
新規登録	IP フロー・MAC フローの可視化を行う詳細な条件を登録します。指定可能な条件を次に示します。 ・名前 ：任意の名前を登録します。最大 256 文字登録可能です。カンマ「,」を除く文字を使用できます。 ・フロー種別 ：可視化対象のデータを選択します。 ・絞り込み条件：可視化対象とするデータの範囲を絞り込む場合，その条件を指定します。 条件は最大 100 行指定することが出来，同一行内は AND 条件，各行間は除外をチェックした場合は AND NOT 条件，それ以外は OR 条件で絞り込みを行います。 ・集約条件 ：可視化対象の値を集約する場合，その条件を指定します。

項目	説明
	・集計対象　　：集計する対象の情報（値）を選択します。 ・対象期間　　：可視化対象のデータの期間を指定します。表示形式が時系列グラフの場合，データ集計間隔を指定します。 ・表示形式　　：可視化の形式を選択します。 ・グラフ表示設定：以下を設定／選択します。 [表示数] 集約条件指定の時系列グラフ，テーブル，および円グラフにおいて，ランキングの上位何件を表示対象とするかを指定します。 [その他集計表示（初期表示）] 集約条件指定の時系列グラフにおいて，表示対象でないランキング下位の総和を「その他」として初期表示するかどうかを指定します。 [積み上げグラフ（初期表示）] 集約条件指定の時系列グラフにおいて，各折れ線グラフを積み上げ表示とするかどうかを指定します。 [正規化] パケット数やバイト数などを単位時間あたりの変化量に換算して表示する場合，指定します。集計対象がユニーク数の場合は，本設定は無視され，正規化は実施されません。 [エイリアス表示] エイリアス機能により設定された名称を表示する場合，指定します。
一覧ダウンロード（CSV）	登録している個別ビューの全情報を CSV 形式のファイルとしてダウンロードします。ファイル名は「V1_SimplexViews_<*日付*>.csv」，「V2_FilterSheet_<*日付*>.csv」となります。
一括登録・更新	個別ビュー 一括登録・更新を表示します。
一覧表示項目の設定一括変更	個別ビュー一覧の変更可能なフィールドを一括更新します。表形式で編集可能です。 ・更新　　：チェックした複数の設定を更新します。同時に変更可能な設定数は最大 20 です。 ・キャンセル　　：更新操作をキャンセルします。変更途中の設定は破棄されます。
個別ビュー一覧	登録した個別ビューの一覧を表示します。
選択設定の削除	一覧でチェックした複数の設定を一括で削除します。
選択設定の複製	一覧でチェックした 1 つの設定を複製します。
詳細	登録内容の詳細を表示します。
変更	登録内容を変更します。
再描画	時系列グラフの表示形式にて，ズームアップしたグラフが表示している期間で，グラフ情報をコレクタから再取得し，再描画します。
表示切替（双方向矢印ボタン）	集約条件指定の時系列グラフにおいて，各折れ線グラフを積み上げ表示とするかどうかを切り替えます。
ズームリセット（undo ボタン）	時系列グラフの表示形式にて，ズームアップした表示を元に戻します。

項目	説明
CSV	時系列グラフ，および円グラフの表示形式にて，グラフ表示時に収集した情報を CSV 形式のファイルとしてダウンロードします。ファイル名は「個別ビュー”名前”.csv」となります。
フローランキングリスト	時系列グラフ，および円グラフの表示形式にて，個別ビューの表示と同様のフィルタ条件を指定したフローランキングリスト画面を表示します。
期間	可視化対象のデータの期間を指定します。

＊ユニーク数の集計値は，集計アルゴリズムに起因する誤差が生じる場合があります。

（6） 個別ビュー一括登録・設定

ダッシュボード 個別ビュー 一括登録・更新の概要を次に示します。

表 5-9 ダッシュボード 個別ビュー 一括登録・更新の概要

項目	説明
一括登録・更新	個別ビューにおける各登録情報を一括で登録します。 登録項目を次に示します。 ・個別ビュー：個別ビューの表示内容に関する情報を入力した CSV ファイルを指定します。 ・フローフィルタシート： 個別ビューの絞り込み条件に関する情報を入力した CSV ファイルを指定します。 ・CSV ファイル未記載データ削除： CSV ファイルに入力されていない情報が AX-Collector に既に登録されている場合に削除するか，削除しないかを指定します。

（7） 監視状況俯瞰ビュー

SNMP 監視，フロー監視および外部データ監視で登録／収集した監視項目／収集データを基に，複数の監視項目の集計値／検知状況を表形式で表示します。

ダッシュボード 監視状況俯瞰ビューの概要を次に示します。

表 5-10　ダッシュボード 監視状況俯瞰ビューの概要

項目	説明
新規登録	表示の詳細な条件を登録します。指定可能な条件を次に示します。 ・名前　　：任意の名前を登録します。最大 256 文字登録可能です。カンマ「,」を除く文字を使用できます。 ・監視種別　：俯瞰表示の対象となる監視種別（SNMP 監視／フロー監視／外部データ監視）を選択します。 ・表示データ：表形式で表示する監視項目，MIB オブジェクトグループ／フロー条件グループ／外部監視データを設定します。※1 また，表項目名を入力・カスタマイズします。最大 256 文字登録可能です。 （以降，本設定によって表示される表を俯瞰テーブルと呼びます。） ・セル内表示：以下を選択します。 [表示形式] 監視状況をアイコン・数値の両方，またはそのいずれかで表示することを選択します。 [集計対象] 表示する集計対象を「閾値監視値」「閾値検知通知回数」「Impulse 連携通知回数」から選択します。 [表示単位指定] 表示単位（キロ(k),メガ(M)等）を選択します。 [表示桁数] 小数点何位までを表示するかを選択します。 ・表示データ選択：表示する数値を平均値，最大値，最小値および最新値，設定閾値，スコアから一つ，または複数選択します。スコアを選択する場合，スコア計算に使用する警告閾値割合(%)も指定可能です。なお，スコアについては，本表下部の説明も参照ください。 ・状態表示　：検知状況を表すアイコンの色／形状を選択します。 ・トップサマリ表示：上記表示データで選択したデータの統計サマリ（表）の表示有無を選択します。統計サマリの集計方法については，上記表示データの表の行数を集計総数とするか，セル数を集計総数とするかを選択できます。他に，表示項目の検知率%（検知数／集計対象数）の表示を，スコア（検知率の逆数）に変更も可能です。 また，本表の項目名をカスタマイズできます。最大 256 文字登録可能です。 ・対象期間　：表示対象とする期間を指定します。 ・簡易表示　：俯瞰テーブルの MIB オブジェクトグループ／フロー条件グループ／外部監視データについて，監視状況の表示有無を選択します。

項目	説明
	・最小表示（検知率・スコアのみ）：トップサマリ表示の検知率またはスコアのみの表示設定です。 ・行番号表示：俯瞰テーブル行番号の表示有無を選択します。
一覧ダウンロード（CSV）	登録している監視状況俯瞰ビューの全情報を CSV 形式のファイルとしてダウンロードします。ファイル名は「B1_BirdsEyeViewMain_<*日付*>.csv」，「B2_BirdsEyeViewTable_<*日付*>.csv」となります。
一括登録・更新	監視状況俯瞰ビュー 一括登録・更新を表示します。
一括エクスポート	俯瞰ビューで表示する各画面の表示データを CSV ファイルで出力する画面を表示します。「（9）監視状況俯瞰ビュー一括エクスポート」を参照ください。
一覧表示項目の設定一括変更	監視状況俯瞰ビュー一覧の変更可能なフィールドを一括更新します。表形式で編集可能です。 ・更新　：チェックした複数の設定を更新します。同時に変更可能な設定数は最大 20 です。 ・キャンセル　：更新操作をキャンセルします。変更途中の設定は破棄されます。
監視状況俯瞰ビュー一覧・登録	登録した監視状況俯瞰ビューの一覧を表示します。
選択設定の削除	一覧でチェックした複数の設定を一括で削除します。
選択設定の複製	一覧でチェックした 1 つの設定を複製します。
詳細	登録内容の詳細を表示します。
変更	登録内容を変更します。
簡易表示 OFF・簡易表示 ON	俯瞰テーブルの MIB オブジェクトグループ／フロー条件グループ／外部監視データについて，監視状況の表示有無を切り替えます。
最小表示	トップサマリの検知率・スコアのみへ表示を切り替えます。
CSV	監視状況俯瞰ビューの表示情報を CSV 形式のファイルとしてダウンロードします。 一つのセルに複数の値（平均値，最大値，最小値，最新値，設定閾値，スコア）を表示している場合は，それぞれの値を別の列として出力します。 ファイル名は「<名前>.csv」となります。
表示期間設定	表示対象とする期間を指定します。
俯瞰テーブルの監視項目セル	SNMP 監視，フロー監視，または外部データ監視の監視項目毎監視データ詳細へのリンクです。
俯瞰テーブルの MIB オブジェクトグループ／フロー条件グループ／外部監視データセル	MIB オブジェクトグループ，フロー条件グループ，または外部監視データの監視データ詳細ページへのリンクです。

※１：設定数は次に示す収容条件以下としてください。

表 5-11　俯瞰テーブルの収容条件

項目	収容条件
監視項目数（行数）	24

項目	収容条件
1 監視項目あたりの MIB オブジェクトグループ／フロー条件グループ／外部監視データ数（列数）	16

【表示データ　スコア設定時の動作について】

セル内表示データとして「スコア」を選択した場合の動作について補足します。選択時のスコア値と，その表示色は，次のように決定されます。

・各セルのスコア値

異常データ数＝上限・下限閾値越えデータの数

警告データ数＝｛上限閾値～上限閾値×警告閾値割合(%)｝のデータ数

＋｛下限閾値～下限閾値×警告閾値割合(%)｝のデータ数

スコア値：100－{(異常データ数＋警告データ数×0.5)÷(全データ数)｝×100

数値・アイコン色：異常・警告データ数によって，次の色となります。

データ分布	数値色	アイコン色
異常データ有	赤	検知有の設定色（上限閾値以上、下限閾値以下、Impulse）
異常データ無 警告データ有	黄	検知無の設定色
正常 （異常・警告データなし）	緑	検知無の設定色

（注）スコア値の計算時，次の補正が入ります。

上限スコア値＝90（異常データ有）

上限スコア値＝95（警告データ有）

（例）異常データ，警告データが無い場合：スコア＝100（数値色：緑）

すべて警告データの場合　　：スコア＝ 50（数値色：黄）

・行・列サマリのスコア値

スコア値：各行・各列のセルスコア値の平均値

数値・アイコン色：スコア値によって次の色となります。変更はできません。

スコア値	数値色	アイコン色
40 未満	赤	赤
40 以上 80 未満	黄	黄
80 以上	黒	緑

・トップサマリのスコア値

スコア値：各セルのスコア値の平均値

数値・アイコン色：スコア値によって次の色となります。変更はできません。

スコア値	数値色	アイコン色
40 未満	赤	赤
40 以上 80 未満	黄	黄
80 以上	黒	緑

（8） 監視状況俯瞰ビュー 一括登録・設定

ダッシュボード 監視状況俯瞰ビュー 一括登録・更新の概要を次に示します。

表 5-12 ダッシュボード 監視状況俯瞰ビュー 一括登録・更新の概要

項目	説明
一括登録・更新	監視状況俯瞰ビューにおける各登録情報を一括で登録します。全ての登録項目に登録情報を入力した CSV ファイルを指定します。 登録項目を次に示します。 ・俯瞰ビュー　：監視状況俯瞰ビューの表示内容に関する情報を入力した CSV ファイルを指定します。 ・リレーション：監視状況俯瞰ビューの表示データに関する情報を入力した CSV ファイルを指定します。 ・CSV ファイル未記載データ削除：

項目	説明
	CSV ファイルに入力されていない情報が AX-Collector に既に登録されている場合に削除するか，削除しないかを指定します。

（9） 監視状況俯瞰ビュー一括エクスポート

ダッシュボード 監視状況俯瞰ビュー 一括エクスポートの概要を次に示します。

本画面では，各俯瞰ビューを表示画面の CSV ボタン押下時のファイルを一括してダウンロード可能です。

5-13 ダッシュボード 監視状況俯瞰ビュー 一括エクスポートの概要

項目	説明
俯瞰ビュー	エクスポートの対象とする俯瞰ビューを選択します。
期間	エクスポートの対象期間を指定します。
CSV 出力	選択した俯瞰ビュー毎にエクスポートした CSV ファイルを ZIP 形式で 1 ファイルに圧縮して出力します。 ファイル名は，以下となります。 ZIP ファイル（圧縮時）： ax-collector-birdseyeview_<*開始時刻*>-<*終了時刻*>.zip CSV ファイル（解凍後）： <*俯瞰ビュー名*>.csv

（10） MAP ビュー

MAP ビューの概要を次に示します。本画面は，地図上にネットワークの送信および宛先位置情報をプロットする画面です。GEOIP 連携機能を有効化し，緯度・経度情報がデータベースに格納されている場合に使用できます。

表 5-14 MAP ビューの概要

項目	説明
MAP ビュー	・地図(*)　：世界地図上に集計対象で指定した送信元地点を○，宛先地点を△のマーカでプロットします。送信元・宛先共に緯度・経度情報が存在する場合，該当パスを線で結びます。 ・集計データ一覧　：集計対象で指定した送信元・宛先毎のバイト数，パケット数，フローレコード数を一覧表示します。最大 10,000 件を表示します。 ・拡大／縮小　：表示中の地図描画領域をを拡大，縮小します。 ・CSV　：集計データ一覧表のデータを CSV 形式でダウンロードします。 ファイル名「map_data.csv」 （*）　表示地点は，集計対象毎の中心点となります。
集計対象	地図・集計データ一覧に表示する集計対象を指定します。 ・送信元　：国コード，国，地域，都市，AS 番号，AS 組織名から複数を選択します。 ・宛先　：国コード，国，地域，都市，AS 番号，AS 組織名から複数を選択します。 ・ソート　：バイト数，パケット数，フローレコード数から，集計データの降順ソートキーを指定します。
フィルタ条件	集計時のフィルタ条件を指定します。入力後，更新ボタンで反映されます。 複数の入力フィールドに記載した場合アンド条件となります。 指定可能な条件は次の通りです。 ・送信元 or 宛先　：送信元 or 宛先に入力情報を含む対象フィールド（A）（B） ・送信元　：送信元に入力情報を含む対象フィールド（A） ・宛先　：宛先に入力情報を含む対象フィールド（A） フィルタ可能なフィールド情報 （A）国コード，国，地域，都市，AS 番号，AS 組織名 IPv4 ネットワーク，IPv6 ネットワーク L4 ポート番号 NAT IPv4 ネットワーク，NAT IPv6 ネットワーク NAT L4 ポート番号 （B）HTTP サーバ名 ・クリア　：入力情報をクリアします。 ・更新　：入力情報に従って再集計します。

項目	説明
地図表示	地図の描画形式を指定します。 ・地図スタイル　：地図投影方法を選択 デフォルト：equirectangular ・緯度　：地図中心の緯度を指定 デフォルト：0 範囲：-90～90 ・経度　：地図中心の経度を指定 デフォルト：0 範囲：-180～180 ・スケール　：地図の拡大スケールを指定 デフォルト：1 範囲：1（縮小）～100（拡大） ・回転角度　：反時計回りの角度 デフォルト：0 範囲：-180～180 （注）地図はマウス操作でもズーム，回転可能ですが本地図表示のパラメータには反映されません。画面が乱れた場合，画面全体の再読み込みを実施ください。

5.4.2　フローランキングリスト

AX-Collector が収集しているフロー情報をランキングリスト形式で表示します。

（1）　登録一覧

フローランキングリスト 登録一覧の概要を次に示します。

表 5-15　フローランキングリスト 登録一覧の概要

項目	説明
IP フロー	IP フロー 表示条件設定を表示します。
IP フロー複合ビュー	IP フロー複合ビュー 表示条件設定を表示します。
MAC フロー	MAC フロー 表示条件設定を表示します。
登録一覧	登録した情報の一覧を表示します。
表示	登録した表示対象とするデータの条件でフローリストを表示します。
削除	登録内容を削除します。
検索	表示した一覧情報を対象に検索し，一致したものを表示します。

（2）　IP フロー・MAC フロー

フローランキングリスト IP フロー，および MAC フローの概要を次に示します。

表 5-16　フローランキングリスト IP フローおよび MAC フローの概要

項目	説明
表示条件設定・表示対象変更	フローリストの表示対象とするデータの範囲を設定します。指定可能な条件を次に示します。 ・期間　：可視化対象のデータの期間を指定します。 ・表示フィールド：可視化対象のフィールド情報を選択します。※1 ・フロー数　：可視化対象のフロー数を指定します。 ・センサ・ポート　：可視化対象のセンサ，モニタポート，送信ポートを指定します。 フィールドフィルタの設定とは AND 条件で判定します。 ・宛先アドレス種別　：可視化対象の宛先 MAC アドレス，あるいは宛先 IP アドレスの種別を指定します。宛先アドレス種別（MAC，IPv4，IPv6）間は AND 条件で判定します。また，フィールドフィルタの設定とも AND 条件で判定します。 ・フィールドフィルタ：可視化対象とするフロー情報の各フィールドのフィルタ条件を指定します。 条件は各シートの合計で最大 100 行指定することが出来，同一行内は AND 条件，各行間は除外をチェックした場合は AND NOT 条件，それ以外は OR 条件でフィルタします。 TCP フラグは TCP ヘッダに含まれるフラグを 10 進数に変換した値，あるいは名称指定で各フラグのオン・オフを指定します。
表示	設定した表示対象とするデータの条件でフローリストを表示します。
表示対象登録	表示対象変更で指定した条件に名称を付与して登録します。 最大 256 文字登録可能です。 登録した情報は登録一覧で表示されます。
フローリスト	表示対象に該当するフロー情報をリスト形式で表示します。
検索フィールド	表示したフローリストの全フィールド，または特定のフィールドを対象に検索し，一致したものを表示します。 全フィールドを対象に検索する場合，文字列は前方一致，数値は完全一致で検索します。
エイリアス詳細	選択したフロー情報に関するエイリアス情報が設定されている場合，そのエイリアス設定情報を表示します。
CSV 出力	表示対象に該当するフロー情報を CSV 形式のファイルとしてダウンロードします。ファイル名は「flow_list_ip.csv」，または「flow_list_mac.csv」となります。 なお，CSV 出力ボタンを押下したタイミングで取得したデータを出力するため，画面に表示している内容と差分が発生することがあります。
コピー	選択したフロー情報の任意の項目をクリップボードにコピーします。

項目	説明
フロー数	表示対象に該当するフローの数を表示します。
合計パケット数	表示対象に該当するフローの総パケット数を表示します。
合計バイト数	表示対象に該当するフローの総バイト数を表示します。

※1：指定した表示フィールドのデータが存在しない場合，’-‘や’-1’等で該当情報の集計結果を表示します。

（3） IP フロー複合ビュー

IP フロー複合ビューの概要を次に示します。IP フロー複合ビューでは，時系列グラフまたはヒストグラムの何れかとランキングリストを同時に表示することが出来ます。また，センサにおいて TCP 遅延測定機能や UDP 情報測定機能を有効にすることで，IP フローの遅延情報や再送数などを可視化表示することが出来ます。TCP 遅延測定機能や再送数などの有効，無効が異なるセンサが混在する環境で IP フロー複合ビューを使用する場合は，可視化対象のセンサ・ポートを指定してください。

表 5-17 IP フロー複合ビューの概要

項目	説明
表示条件設定・表示対象変更	IP フロー複合ビューの表示対象とするデータの範囲を設定します。指定可能な条件を次に示します。 ・期間 ：可視化対象のデータの期間を指定します。 ・表示形式・集計対象：可視化対象の表示形式を指定します。 - 表示形式 ：可視化表示するグラフ種別を指定します。時系列グラフまたはヒストグラムから選択可能です。ヒストグラムは集計対象に TCP RTT，TCP SRT，TCP DELAY，UDP DELAY，UDP JITTER，UDP RTP RTT，UDP RTP DELAY，UDP RTP JITTER の何れかを選択した場合のみグラフを表示します。 - 集計対象 ：IP フロー複合ビューでは１種類または２種類のデータを表示可能です。表示対象のデータを指定します。 - 集約条件 ：IP フロー複合ビューでは，指定した表示フィールド毎のランキング表示と，フィールドフィルタの条件シート毎の表示の，２種類の集約条件を選択できます。※1 表示フィールドを選択した場合は，表示対象のフィールドと表示フロー数を指定します。 フィールドフィルタを選択した場合は，後述のフィールドフィルタを設定します。 - 時系列集計データ表示オプション：時系列グラフのデータ集計間隔，および最小値，最大値のグラフ表示の有無を指定します。 - ヒストグラム集計データ表示オプション：ヒストグラムの

項目	説明
	データ集計間隔，および集計範囲を指定します。集計範囲は，フロー情報に含まれる集計情報が全て範囲内に収まっているフローのみを表示対象とします。 ・センサ・ポート：可視化対象のセンサ，モニタポート，送信ポートを指定します。 フィールドフィルタの設定とは AND 条件で判定します。 ・宛先アドレス種別：可視化対象の宛先 MAC アドレス，あるいは宛先 IP アドレスの種別を指定します。 宛先アドレス種別（MAC，IPv4，IPv6）間は AND 条件で判定します。また，フィールドフィルタの設定とも AND 条件で判定します。 ・フィールドフィルタ：集約条件に表示フィールドを選択した場合は，可視化対象とするフロー情報の各フィールドのフィルタ条件を指定します。 条件は各シートの合計で最大 100 行指定することが出来，同一行内は AND 条件，各行間は除外をチェックした場合は AND NOT 条件，それ以外は OR 条件でフィルタします。 集約条件にフィールドフィルタを選択した場合は，条件シート毎にフィールドフィルタ名および集約条件を指定します。
表示	設定した条件で IP フロー複合ビューを表示します。
表示対象登録	表示対象変更で指定した条件に名称を付与して登録します。 最大 256 文字登録可能です。 登録した情報は登録一覧で表示されます。
再描画	時系列グラフの表示形式にて，ズームアップしたグラフが表示している期間で，グラフ情報をコレクタから再取得し，再描画します。
ズームリセット（undo ボタン）	時系列グラフの表示形式にて，ズームアップした表示を元に戻します。
CSV	時系列グラフ表示時に収集した情報を CSV 形式のファイルとしてダウンロードします。 ファイル名は「flow_list_graph_ip.csv」となります。
検索フィールド	表示したフローリストの全フィールド，または特定のフィールドを対象に検索し，一致したものを表示します。 全フィールドを対象に検索する場合，文字列は前方一致，数値は完全一致で検索します。
エイリアス詳細	選択したフロー情報に関するエイリアス情報が設定されている場合，そのエイリアス設定情報を表示します。
CSV 出力	表示対象に該当するフロー情報を CSV 形式のファイルとしてダウンロードします。ファイル名は「flow_list_table_ip.csv」となります。 なお，CSV 出力ボタンを押下したタイミングで取得したデータを出力するため，画面に表示している内容と差分が発生することがあります。
コピー	選択したフロー情報の任意の項目をクリップボードにコピーします。

項目	説明
フロー数	フローランキングリストに表示したフローの合計数を表示します。
合計パケット数	フィルタ条件に該当するフローの総パケット数を表示します。 表示対象のデータとしてパケット数，パケット数(pps)を選択した場合に表示します。
合計バイト数	フィルタ条件に該当するフローの総バイト数を表示します。 表示対象のデータとしてバイト数，バイト数(bps)を選択した場合に表示します。

※1：指定した表示フィールドのデータが存在しない場合，’-‘や’-1’等で該当情報の集計結果を表示します。

(4) 環境設定

フローランキングリスト 環境設定の概要を次に示します。

環境設定では，フロー情報検索時のデータベース検索最大数および，検索結果のデータ取得数を設定します。

表 5-18 環境設定の概要

項目	説明
登録	フローランキングリスト環境設定を登録します。
変更	フローランキングリスト環境設定の登録内容を変更します。
削除	登録内容を初期化します。
フローランキングリスト 環境設定	・検索タイムアウト時間： フロー情報検索時のタイムアウト時間（秒）を指定します。 ・【最大 DB 検索数】画面表示： フローランキングリストおよび個別ビューでのフロー情報データベース最大検索数を指定します。 ・【最大表示数】画面表示： フローランキングリストおよび個別ビューでのフロー情報検索結果データの最大表示数を指定します。 ・【最大 DB 検索数】CSV 出力： フローランキングリストでの CSV ファイル出力時のフロー情報データベース最大検索数を指定します。 ・【最大出力数】CSV 出力： フローランキングリストでの CSV ファイル出力時のフロー情報検索結果データの CSV ファイル最大出力数を指定します。 ・【最大 DB 検索数】REST API： IP フロー情報検索 API，MAC フロー情報検索 API 実行時のフロー情報データベース最大検索数を指定します。 ・【最大出力数】REST API： IP フロー情報検索 API，MAC フロー情報検索 API 実行時のフロー情報検索結果データの API 応答最大出力数を指定します。

項目	説明
更新	登録内容を更新します。
キャンセル	登録・更新をキャンセルします。

5.4.3 SNMP 監視

SNMP 監視機能に関する各種情報を表示します。

（1） MIB 収集データ

SNMP 監視において収集した MIB 値をグラフ表示します。

ネットワーク機器毎 MIB 収集データ詳細では，ネットワーク機器毎に収集した MIB 値をグラフ表示します。また，MIB オブジェクト詳細では MIB オブジェクト毎に MIB 値をグラフ表示します。

表 5-19 ネットワーク機器毎 MIB 収集データ詳細の概要

項目	説明
設定画面	対象のネットワーク機器の設定詳細を表示します。
ネットワーク機器毎 MIB 収集データ詳細	対象のネットワーク機器の設定内容，およびネットワーク機器から収集したシステムおよびインタフェースに関する MIB 値を表示します。
収集データ	対象のネットワーク機器から収集した MIB 値をグラフ表示します。 ・表示単位 ：表示する MIB 値の単位を選択します。 - 取得値 ：収集した MIB そのものの値。（デフォルト） - 差分 ：前周期との差分値。 - 正規化差分(/秒)：差分を収集周期(秒)で割った値。 - 正規化差分(bps)：正規化差分(/秒)を 8 倍した値。カウンタ型でバイト数を応答する MIB の場合，bps 換算した値となります。 ・表示切替 ：グラフの表示形式として，集合（重ねて表示）又は積み上げに切り替えます。 ・ズームリセット：ズームアップした表示を元に戻します。 ・CSV ：グラフ表示時に使用した情報を CSV 形式のファイルとしてダウンロードします。 ・期間 ：任意の表示期間を指定します。 ・←→ ：表示期間を同じ間隔で未来又は過去に変更します。
MIB オブジェクト一覧	対象のネットワーク機器に関連する MIB オブジェクトの一覧を表示します。 ・詳細：MIB オブジェクト詳細を表示します。

表 5-20 MIB オブジェクト詳細の概要

項目	説明
設定画面	対象の MIB オブジェクトの設定詳細を表示します。
MIB オブジェクト詳細	対象の MIB オブジェクトの設定内容を表示します。
収集データ	対象のネットワーク機器から収集した MIB 値をグラフ表示します。 ・表示単位 ：表示する MIB 値の単位を選択します。 - 取得値 ：収集した MIB そのものの値。（デフォルト） - 差分 ：前周期との差分値。 - 正規化差分(/秒)：差分を収集周期(秒)で割った値。 - 正規化差分(bps)：正規化差分(/秒)を 8 倍した値。カウンタ型でバイト数を応答する MIB の場合，bps 換算した値となります。 ・表示切替 ：グラフの表示形式として，集合（重ねて表示）又は積み上げに切り替えます。 ・ズームリセット：ズームアップした表示を元に戻します。 ・CSV ：グラフ表示時に使用した情報を CSV 形式のファイルとしてダウンロードします。 ・期間 ：任意の表示期間を指定します。 ・←→ ：表示期間を同じ間隔で未来又は過去に変更します。
関連ネットワーク機器一覧	対象の MIB オブジェクトに関連するネットワーク機器の一覧を表示します。 ・詳細：ネットワーク機器毎 MIB 収集データ詳細を表示します。

（2） SNMP 監視データ

SNMP 監視において生成した SNMP 監視データ（MIB オブジェクトグループ）をグラフ表示します。

SNMP 監視項目毎 監視データ詳細では，各 SNMP 監視項目毎に生成した SNMP 監視データをグラフ表示します。また，MIB オブジェクトグループ監視データ詳細では MIB オブジェクトグループ毎に SNMP 監視データをグラフ表示します。

表 5-21 SNMP 監視項目毎 監視データ詳細の概要

項目	説明
設定画面	対象の SNMP 監視項目の設定詳細を表示します。
SNMP 監視項目毎 監視データ詳細	対象の SNMP 監視項目の設定内容を表示します。
収集データ	対象の SNMP 監視項目にて生成した SNMP 監視データをグラフ表示します。また，閾値監視，Impulse 連携による検知点を表示します。 ・検知点 ：表示する検知点を指定します。

項目	説明
	- Impulse ：Impulse 連携による検知点を表示します。 - 閾値 ：閾値監視による検知点を表示します。 - 発生検知：閾値超え又は異常検知による検知点を表示します。 - 復旧検知：閾値復旧又は復旧検知による検知点を表示します。 - 通知なし：syslog 又は trap による通知を行わなかった検知点も表示します。 ・表示切替 ：グラフの表示形式として，集合（重ねて表示）又は積み上げに切り替えます。 ・ズームリセット：ズームアップした表示を元に戻します。 ・CSV ：SNMP 監視データを CSV 形式のファイルとしてダウンロードします。 表示単位変更ボタンで変更した表示単位に応じた値を出力します。 ・bps ：表示単位変更ボタンを表示します。 ・期間 ：任意の表示期間を指定します。 ・←→ ：表示期間を同じ間隔で未来又は過去に変更します。
関連 MIB オブジェクトグループ一覧	対象の SNMP 監視項目に関連する MIB オブジェクトグループの一覧を表示します。 ・詳細：MIB オブジェクトグループ 監視データ詳細を表示します。
関連閾値監視通知一覧	対象の SNMP 監視項目に関連する閾値監視通知のうち，収集データで指定した表示期間内に検知した通知一覧を表示します。 ・詳細：閾値監視通知詳細を表示します。
関連 Impulse 連携通知一覧	対象の SNMP 監視項目に関連する Impulse 連携通知のうち，収集データで指定した表示期間内に検知した通知一覧を表示します。 ・詳細：Impulse 連携通知詳細を表示します。

表 5-22 MIB オブジェクトグループ監視データ詳細の概要

項目	説明
設定画面	対象の MIB オブジェクトグループの設定詳細を表示します。
MIB オブジェクトグループ監視データ詳細	対象の MIB オブジェクトグループの設定内容を表示します。
収集データ	対象の MIB オブジェクトグループにて生成した SNMP 監視データをグラフ表示します。また，閾値監視，Impulse 連携による検知点を表示します。 ・検知点 ：表示する検知点を指定します。 - Impulse ：Impulse 連携による検知点を表示します。 - 閾値 ：閾値監視による検知点を表示します。 - 発生検知：閾値超え又は異常検知による検知点を表示します。 - 復旧検知：閾値復旧又は復旧検知による検知点を表示します。

項目	説明
	- 通知なし：syslog 又は trap による通知を行わなかった検知点も表示します。 ・ズームリセット：ズームアップした表示を元に戻します。 ・CSV　：グラフ表示時に使用した情報を CSV 形式のファイルとしてダウンロードします。表示単位変更ボタンで変更した表示単位に応じた値を出力します。 ・bps　：表示単位変更ボタンを表示します。 ・期間　：任意の表示期間を指定します。 ・←→　：表示期間を同じ間隔で未来又は過去に変更します。
関連 MIB オブジェクト一覧	対象の MIB オブジェクトグループに関連する MIB オブジェクトの一覧を表示します。
関連 SNMP 情報監視項目一覧	対象の MIB オブジェクトグループに関連する SNMP 監視項目の一覧を表示します。 ・詳細：SNMP 監視項目毎 監視データ詳細を表示します。
関連閾値監視通知一覧	対象の MIB オブジェクトグループに関連する閾値監視通知のうち，収集データで指定した表示期間内に検知した通知一覧を表示します。 ・詳細：閾値監視通知詳細を表示します。
関連 Impulse 連携通知一覧	対象の MIB オブジェクトグループに関連する Impulse 連携通知のうち，収集データで指定した表示期間内に検知した通知一覧を表示します。 ・詳細：Impulse 連携通知詳細を表示します。

（3）　SNMP 監視状況

SNMP 監視設定の状況と，SNMP 監視データの生成状況，MIB の収集状況を表示します。

表 5-23　SNMP 監視状況の概要

項目	説明
SNMP 監視設定	SNMP 監視における，監視周期毎の設定数，および収集有効設定数を表示します。
SNMP 監視対象データ生成状況	SNMP 監視データの生成数をグラフ表示します。 また，SNMP 監視データ生成の失敗履歴を表示します。 ・ズームリセット：ズームアップした表示を元に戻します。 ・期間　：任意の表示期間を指定します。 ・←→　：表示期間を同じ間隔で未来又は過去に変更します。 ・詳細　：MIB オブジェクトグループ 生成失敗詳細を表示します。

項目	説明
MIB 収集状況	SNMP 監視における MIB 収集数をグラフ表示します。 また，MIB 収集の失敗履歴を表示します。 ・ズームリセット：ズームアップした表示を元に戻します。 ・期間　：任意の表示期間を指定します。 ・←→　：表示期間を同じ間隔で未来又は過去に変更します。 ・詳細　：MIB オブジェクト 収集失敗詳細を表示します。

(4)　一括エクスポート

SNMP 監視で収集した各監視項目のデータを CSV ファイルで出力します。

SNMP 監視 一括エクスポートの概要を次に示します。

表 5-24　SNMP 監視 一括エクスポートの概要

項目	説明
SNMP 監視項目	エクスポートの対象とする監視項目を選択します。
MIB オブジェクトグループ	選択した SNMP 監視項目に属する MIB オブジェクトグループからエクスポート対象を選択します。 ただし，複数の SNMP 監視項目を選択している場合は，属する全ての MIB オブジェクトグループがエクスポートの対象となります。
期間	エクスポートの対象期間を指定します。
CSV 出力	SNMP 監視項目ごとにエクスポートした CSV ファイルを ZIP 形式で 1 ファイルに圧縮して出力します。 「機械学習連携」を指定した場合，Impulse にインポート可能なフォーマットでエクスポートします。未指定の場合は，AX-Collector に蓄積している収集項目をエクスポートします。 ファイル名は，以下となります。 ・「機械学習連携」指定 ZIP ファイル（圧縮時）： ml_ax-collector-snmp_<*開始日*>-<*終了日*>.zip CSV ファイル（解凍後）： ax_cl_snmp_<*SNMP 監視項目のインデックス名*>.csv ・「機械学習連携」未指定 ZIP ファイル（圧縮時）： ax-collector-snmp_<*開始日*>-<*終了日*>.zip CSV ファイル（解凍後）： <*SNMP 監視項目のインデックス名*>.csv

5.4.4　フロー監視

フロー監視機能に関する各種情報を表示します。

（1） フロー監視データ

フロー監視において生成したフロー監視データ（フロー条件グループ）をグラフ表示します。

フロー監視項目毎 監視データ詳細では，フロー監視項目毎に生成したフロー監視データをグラフ表示します。また，フロー条件グループ監視データ詳細ではフロー条件グループ毎にフロー監視データをグラフ表示します。

表 5-25 フロー監視項目毎 監視データ詳細の概要

項目	説明
設定画面	対象のフロー監視項目の設定詳細を表示します。
フロー監視項目毎 監視データ詳細	対象のフロー監視項目の設定内容を表示します。
収集データ	対象のフロー監視項目にて生成したフロー監視データをグラフ表示します。また，閾値監視，Impulse 連携による検知点を表示します。 ・検知点 ：表示する検知点を指定します。 - Impulse ：Impulse 連携による検知点を表示します。 - 閾値 ：閾値監視による検知点を表示します。 - 発生検知：閾値超え又は異常検知による検知点を表示します。 - 復旧検知：閾値復旧又は復旧検知による検知点を表示します。 - 通知なし：syslog 又は trap による通知を行わなかった検知点も表示します。 ・表示切替 ：グラフの表示形式として，集合（重ねて表示）又は積み上げに切り替えます。 ・ズームリセット：ズームアップした表示を元に戻します。 ・CSV ：フロー監視データを CSV 形式のファイルとしてダウンロードします。 ・期間 ：任意の表示期間を指定します。 ・←→ ：表示期間を同じ間隔で未来又は過去に変更します。
関連フロー条件グループ一覧	対象のフロー監視項目に関連するフロー条件グループの一覧を表示します。 ・詳細：フロー条件グループ 監視データ詳細を表示します。
関連閾値監視通知一覧	対象のフロー監視項目に関連する閾値監視通知のうち，収集データで指定した表示期間内に検知した通知一覧を表示します。 ・詳細：閾値監視通知詳細を表示します。
関連 Impulse 連携通知一覧	対象のフロー監視項目に関連する Impulse 連携通知のうち，収集データで指定した表示期間内に検知した通知一覧を表示します。 ・詳細：Impulse 連携通知詳細を表示します。

表 5-26　フロー条件グループ監視データ詳細の概要

項目	説明
設定画面	対象のフロー条件グループの設定詳細画面を表示します。
フロー条件グループ 監視データ詳細	対象のフロー条件グループの設定内容を表示します。
収集データ	対象のフロー条件グループにて生成したフロー監視データをグラフ表示します。また，閾値監視，Impulse 連携による検知点を表示します。 ・検知点　：表示する検知点を指定します。 　- Impulse　：Impulse 連携による検知点を表示します。 　- 閾値　：閾値監視による検知点を表示します。 　- 発生検知：閾値超え又は異常検知による検知点を表示します。 　- 復旧検知：閾値復旧又は復旧検知による検知点を表示します。 　- 通知なし：syslog 又は trap による通知を行わなかった検知点も表示します。 ・ズームリセット：ズームアップした表示を元に戻します。 ・CSV　：フロー監視データを CSV 形式のファイルとしてダウンロードします。 ・期間　：任意の表示期間を指定します。 ・←→　：表示期間を同じ間隔で未来又は過去に変更します。
細分化収集データ	対象のフロー条件グループにて生成したフロー監視の細分化収集データをグラフ表示します。 ・ズームリセット：ズームアップした表示を元に戻します。 ・CSV　：フロー監視細分化収集データを CSV 形式のファイルとしてダウンロードします。 ・期間　：任意の表示期間を指定します。 ・←→　：表示期間を同じ間隔で未来又は過去に変更します。
関連フロー条件一覧	対象のフロー条件グループに関連するフロー条件の一覧を表示します。
関連フロー情報監視項目一覧	対象のフロー条件グループに関連するフロー監視項目の一覧を表示します。 ・詳細：フロー監視項目毎 監視データ詳細を表示します。
関連閾値監視通知一覧	対象のフロー条件グループに関連する閾値監視通知のうち，収集データで指定した表示期間内に検知した通知一覧を表示します。 ・詳細：閾値監視通知詳細を表示します。
関連 Impulse 連携通知一覧	対象のフロー条件グループに関連する Impulse 連携通知のうち，収集データで指定した表示期間内に検知した通知一覧を表示します。 ・詳細：Impulse 連携通知詳細を表示します。

（2）　フロー監視状況

フロー監視設定の状況と，フロー監視データの生成状況を表示します。

表 5-27　フロー監視状況の概要

項目	説明
フロー監視設定	フロー監視における，各監視周期毎の設定数，および収集有効設定数を表示します。
フロー監視対象データ生成状況	フロー監視データの生成数をグラフ表示します。 また，フロー監視データ生成の失敗履歴を表示します。 ・ズームリセット：ズームアップした表示を元に戻します。 ・期間　：任意の表示期間を指定します。 ・←→　：表示期間を同じ間隔で未来又は過去に変更します。 ・詳細　：MIB オブジェクトグループ 生成失敗詳細を表示します。

（3）　一括エクスポート

フロー監視で収集した各監視項目のデータを CSV ファイルで出力します。

フロー監視 一括エクスポートの概要を次に示します。

表 5-28　フロー監視 一括エクスポートの概要

項目	説明
フロー監視項目	エクスポートの対象とする監視項目を選択します。
フロー条件グループ	選択したフロー監視項目に属するフロー条件グループからエクスポート対象を選択します。 ただし，複数のフロー監視項目を選択している場合は，属する全てのフロー条件グループがエクスポートの対象となります。
期間	エクスポートの対象期間を指定します。
CSV 出力	フロー監視項目ごとにエクスポートした CSV ファイルを ZIP 形式で 1 ファイルに圧縮して出力します。 「機械学習連携」を指定した場合，Impulse にインポート可能なフォーマットでエクスポートします。未指定の場合は，AX-Collector に蓄積している収集項目をエクスポートします。 ファイル名は，以下となります。 ・「機械学習連携」指定 ZIP ファイル（圧縮時）： ml_ax-collector-flow_<*開始日*>-<*終了日*>.zip CSV ファイル（解凍後）： ax_cl_flow_<*フロー監視項目のインデックス名*>.csv ・「機械学習連携」未指定 ZIP ファイル（圧縮時）： ax-collector-flow_<*開始日*>-<*終了日*>.zip CSV ファイル（解凍後）： <*フロー監視項目のインデックス名*>.csv

5.4.5 フローランキング監視

フローランキング監視機能に関する各種情報を表示します。

(1) フローランキング監視収集データ

フローランキング監視において生成したフローランキング監視データをグラフ，テーブル表示します。

フローランキング監視項目毎監視データの詳細では，フローランキング監視項目毎に生成したフローランキング監視データをグラフ，テーブル表示します。

また，収集したデータから出現した集約条件の数を分析する画面も表示可能です。

表 5-29 フローランキング監視収集データの概要

項目	説明
フローランキング監視項目毎 監視データ詳細	対象のフローランキング監視項目の設定内容を表示します。
収集データ表示	対象のフローランキング監視項目にて収集したフローランキング監視データを時系列の棒グラフ，各時間のランキング表で表示します。 ・グラフ表示 ：時系列グラフ表示を ON・OFF します。 ・グラフ切替 ：時系列グラフの表示形式として，集合（並べて表示）又は積み上げに切り替えます。 ・テーブル表示 ：表示期間すべてのランキング表を表示します。特定行のランク番号をクリックでグラフ表示を該当データに絞り込みます。 ・ズームリセット：ズームアップした表示，また選択グラフを元に戻します。 ・CSV ：フローランキング監視データを CSV 形式のファイルとしてダウンロードします。 ・フローランキングリスト：フローランキングリスト画面を表示します。 ・期間 ：任意の表示期間を指定します。 ・集計 ：集計対象および設定閾値を表示します。集計対象をクリックすると，対象のデータの時系列グラフに切り替わります。
データ数分析	対象のフローランキング監視の収集データを分析し，出現した集約条件毎のデータ数を棒グラフや円グラフで表示します。 ・時系列グラフ表示：時系列グラフ表示を ON・OFF します。 ・円グラフ表示 ：円グラフ表示を ON・OFF します。 ・テーブル表示 ：テーブル表示を ON・OFF します。 ・検知データ ：検知データのみの集計を行います。 ・CSV ：分析データを CSV 形式のファイルと

項目	説明
	してダウンロードします。 ・期間　：集計期間を月単位で指定します。

5.4.6　外部データ監視

外部データ監視機能に関する各種情報を表示します。

（1）　外部収集データ

外部データ監視において収集した外部データをグラフ表示します。

表 5-30　外部収集データの概要

項目	説明
設定画面	対象の外部収集データの設定詳細を表示します。
外部収集データ詳細	対象の外部収集データの設定内容を表示します。
収集データ	対象の外部収集データの時系列グラフを表示します。 ・検知点（失敗）：収集した外部データに失敗情報が含まれている場合，検知点として表示します。 ・表示切替　：グラフの表示形式として，集合(重ねて表示）又は積み上げに切り替えます。 ・ズームリセット：ズームアップした表示を元に戻します。 ・CSV　：監視データを CSV 形式のファイルとしてダウンロードします。 ・期間　：任意の表示期間を指定します。 ・←→　：表示期間を同じ間隔で未来又は過去に変更します。
収集データ	選択した外部収集データの時系列グラフを表示します。
失敗履歴一覧	失敗情報を設定した外部データを注入した場合，対象時刻と失敗要因を表示します。
関連監視データ一覧	対象の外部データと関連する監視データを表示します。

（2）　外部監視データ

外部データ監視において生成した監視データをグラフ表示します。

外部監視項目毎 監視データ詳細では，外部監視項目毎に生成した外部監視データをグラフ表示します。また，外部監視データ詳細では外部監視データ毎にグラフを表示します。

表 5-31　外部監視項目毎 監視データ詳細の概要

項目	説明
設定画面	対象の外部データ監視項目の設定詳細を表示します。
外部監視項目 監視データ詳細	対象の外部データ監視項目の設定内容を表示します。
収集データ	対象の外部データ監視項目にて生成した監視データをグラフ表示します。また，閾値監視，Impulse 連携による検知点を表示します。 ・検知点　　：表示する検知点を指定します。 　- Impulse　：Impulse 連携による検知点を表示します。 　- 閾値　　：閾値監視による検知点を表示します。 　- 発生検知：閾値超え又は異常検知による検知点を表示します。 　- 復旧検知：閾値復旧又は復旧検知による検知点を表示します。 　- 通知なし：syslog 又は trap による通知を行わなかった検知点も表示します。 ・表示切替　　：グラフの表示形式として，集合(重ねて表示）又は積み上げに切り替えます。 ・ズームリセット：ズームアップした表示を元に戻します。 ・CSV　　：監視データを CSV 形式のファイルとしてダウンロードします。 ・期間　　：任意の表示期間を指定します。 ・←→　　：表示期間を同じ間隔で未来又は過去に変更します。
関連監視データ一覧	対象の外部データ監視項目に関連する監視データの一覧を表示します。 ・詳細：外部監視データ詳細を表示します。
関連閾値監視通知一覧	対象の外部データ監視項目に関連する閾値監視通知のうち，収集データで指定した表示期間内に検知した通知一覧を表示します。 ・詳細：閾値監視通知詳細を表示します。
関連 Impulse 連携通知一覧	対象の外部データ監視項目に関連する Impulse 連携通知のうち，収集データで指定した表示期間内に検知した通知一覧を表示します。 ・詳細：Impulse 連携通知詳細を表示します。

表 5-32　外部監視データ詳細の概要

項目	説明
設定画面	対象の外部監視データの設定詳細を表示します。
外部監視データ詳細	対象の外部監視データの設定内容を表示します。

項目	説明
収集データ	対象の外部監視データをグラフ表示します。また，閾値監視，Impulse 連携による検知点を表示します。 ・検知点　　：表示する検知点を指定します。 　- Impulse　：Impulse 連携による検知点を表示します。 　- 閾値　　：閾値監視による検知点を表示します。 　- 発生検知：閾値超え又は異常検知による検知点を表示します。 　- 復旧検知：閾値復旧又は復旧検知による検知点を表示します。 　- 通知なし：syslog 又は trap による通知を行わなかった検知点も表示します。 ・ズームリセット：ズームアップした表示を元に戻します。 ・CSV　　：監視データを CSV 形式のファイルとしてダウンロードします。 ・期間　　：任意の表示期間を指定します。 ・←→　　：表示期間を同じ間隔で未来又は過去に変更します。
細分化収集データ	対象の外部データ毎に細分化してグラフを表示します。 ・表示切替　　：グラフの表示形式として，集合(を重ねて表示）又は積み上げに切り替えます。 ・ズームリセット：ズームアップした表示を元に戻します。 ・CSV　　：監視データを CSV 形式のファイルとしてダウンロードします。 ・期間　　：任意の表示期間を指定します。 ・←→　　：表示期間を同じ間隔で未来又は過去に変更します。
関連外部データ一覧	対象の監視データに関連する外部データの一覧を表示します。 ・詳細：外部収集データ詳細を表示します。
関連外部データ監視項目一覧	対象の外部データに関連する監視項目の一覧を表示します。 ・詳細：外部監視項目毎 監視データ詳細を表示します。
関連閾値監視通知一覧	対象の外部監視データに関連する閾値監視通知のうち，収集データで指定した表示期間内に検知した通知一覧を表示します。 ・詳細：閾値監視通知詳細を表示します。
関連 Impulse 連携通知一覧	対象の外部監視データに関連する Impulse 連携通知のうち，収集データで指定した表示期間内に検知した通知一覧を表示します。 ・詳細：Impulse 連携通知詳細を表示します。

（3）　外部データ監視状況

外部データ監視設定の状況と，外部監視データの生成状況，外部データの収集状況を表示します。

表 5-33　外部データ監視状況の概要

項目	説明
外部データ監視設定	外部データ監視における，監視周期毎の設定数，および監視・収集有効設定数を表示します。

項目	説明
外部データ監視対象 データ生成状況	外部監視データの生成数をグラフ表示します。 また，外部監視データ生成の失敗履歴を表示します。 ・ズームリセット：ズームアップした表示を元に戻します。 ・期間　：任意の表示期間を指定します。 ・←→　：表示期間を同じ間隔で未来又は過去に変更します。 ・詳細　：外部監視データ 生成失敗詳細を表示します。
外部データ収集状況	外部データ監視における外部データ収集数をグラフ表示します。 また，外部データ収集の失敗履歴を表示します。 ・ズームリセット：ズームアップした表示を元に戻します。 ・期間　：任意の表示期間を指定します。 ・←→　：表示期間を同じ間隔で未来又は過去に変更します。 ・詳細　：外部データ 収集失敗詳細を表示します。

（4）　一括エクスポート

外部データ監視で生成した各監視項目のデータを CSV ファイルで出力します。

外部データ監視 一括エクスポートの概要を次に示します。

表 5-34　外部データ監視 一括エクスポートの概要

項目	説明
外部データ 監視項目	エクスポートの対象とする監視項目を選択します。
監視データ	選択した外部データ監視項目に属する監視データからエクスポート対象を選択します。 ただし，複数の外部データ監視項目を選択している場合は，属する全ての監視データがエクスポートの対象となります。
期間	エクスポートの対象期間を指定します。

項目	説明
CSV 出力	外部データ監視項目ごとにエクスポートした CSV ファイルを ZIP 形式で 1 ファイルに圧縮して出力します。 「機械学習連携」を指定した場合，Impulse にインポート可能なフォーマットでエクスポートします。未指定の場合は，AX-Collector に蓄積している収集項目をエクスポートします。 ファイル名は，以下となります。 ・「機械学習連携」指定 ZIP ファイル（圧縮時）： ml_ax-collector-external_<*開始日*>-<*終了日*>.zip CSV ファイル（解凍後）： ax_cl_external_<*外部データ監視項目のデータセット名*>.csv ・「機械学習連携」未指定 ZIP ファイル（圧縮時）： ax-collector-external_<*開始日*>-<*終了日*>.zip CSV ファイル（解凍後）： <*外部データ監視項目のデータセット名*>.csv

5.4.7 Syslog

受信した Syslog 情報を表示します。

（1） Syslog 収集データ

Syslog 収集データの概要と，表示項目を次に示します。

表 5-35　Syslog 収集データの概要

項目	説明
Syslog 収集データ	収集した Syslog 情報を表示します。 ・時系列グラフ　：期間内の Syslog 数を重要度別に積み上げ棒グラフで表示します。 ・ログ一覧　：期間内の Syslog 情報一覧表です。表示項目は「**表 5-36　Syslog 収集データ　表示項目一覧**」を参照。マウス操作により，表示列の入れ替えが可能です。最大 10,000 件表示します。 ・期間　：任意の表示期間を指定します。 ・CSV　：表示情報を CSV 形式でダウロードします。ファイル名は，「ax-collector-logging_[操作日時].csv」です。 ・時系列グラフ　：時系列グラフの表示・非表示を切り替えます。 ・列の表示／非表示：ログ一覧表示 列の表示非表示を選択します。 ・初期設定に戻す　：列の表示／非表示設定と表示順序を初期設定に戻します。 ・選択ログの削除　：ログ一覧で選択した Syslog 情報を削除します。
フィルタ条件追加	表示データのフィルタ条件を追加設定します。 フィールド・入力値・条件を指定し，設定ボタンを押下すると該当条件で絞り込まれた Syslog 情報を表示します。 設定されたフィルタ条件は,本ボタン横にタグで表示されます。タグ内の×ボタンでフィルタ条件を削除します。 フィールド毎の設定条件は,「**表 5-37　Syslog 収集データ　フィルタ条件一覧**」を参照ください。 ・フィールド　：絞り込みフィールドを指定します。 ・条件　：含む，除外　を指定します。 ・入力値　：フィールドに応じた値を指定します。 ・タグの表示名を変更する：フィルタ条件を追加した際に表示される表示名称を指定します。 ・設定　：フィルタ条件を有効化します。 ・キャンセル　：オペレーションをキャンセルします。

表 5-36　Syslog 収集データ　表示項目一覧

項目	説明	初期表示 ○：表示 －：非表示
チェックボックス	削除対象のデータを選択	○(*1)
重要度	Syslog ヘッダの重要度（Severity）	○

項目	説明	初期表示 ○：表示 －：非表示
受信時刻	Syslog パケットを受信しデータベースに登録した時刻 YYYY-MM-DD hh:mm:ss 形式	○
機器 IP アドレス	Syslog パケットの送信元 IPv4 アドレス	○
機器エイリアス	Syslog パケットの送信元 IPv4 アドレスに紐づくエイリアス（センサ・ポートエイリアス）情報	○
ホスト名	Syslog ヘッダのホスト名フィールド	○
ファシリティ	Syslog ヘッダのファシリティ(Facility)	○
タイムスタンプ	Syslog ヘッダのタイムスタンプ YYYY-MM-DD hh:mm:ss 形式	○
メッセージ	Syslog メッセージ部	○
アプリ名(*2)	Syslog ヘッダのアプリケーション名	－
プロセス ID(*2)	Syslog ヘッダのアプリケーション名に紐づくプロセス ID	－
MSG-ID (*2)	Syslog ヘッダのメッセージ ID	－
CEF DeviceProduct (*3)	CEF ヘッダの Device Product	－
CEF DeviceVendor (*3)	CEF ヘッダの Device Vendor	－
CEF DeviceVersion (*3)	CEF ヘッダの Device Version	－
CEF SigNatureID (*3)	CEF ヘッダの SignatureID	－
CEF Name (*3)	CEF ヘッダの Name	－
CEF Severity (*3)	CEF ヘッダの Severity	－
*ユーザ定義 1～10 (*4)	ユーザ定義したフィールド	－

(*1) 標準ユーザ,管理者のみ表示。
(*2) 受信した Syslog が RFC5424(IETF)フォーマットの場合のみ当該データが存在します。
(*3) 受信した Syslog のメッセージフォーマットが CEF の場合のみ当該データが存在します。
(*4) ユーザが表示名および表示内容を自由に定義出来ます。設定方法については「4.9Syslog 受信機能の設定」を参照してください。

表 5-37 Syslog 収集データ フィルタ条件一覧

#	フィールド名	入力値	入力値に設定可能な最大件数	入力フォーマット
1	タイムスタンプ	文字列（開始時刻）	1	YYYY-MM-DD hh:mm:ss (*1)
2		文字列（終了時刻）	1	YYYY-MM-DD hh:mm:ss (*1)
3	メッセージ	文字列（正規表現なし）	1	32 字以内の文字列(*2)
4		文字列（正規表現あり）	1	32 字以内の文字列(*3)

<table>
<tr><th>#</th><th>フィールド名</th><th>入力値</th><th>入力値に設定可能な最大件数</th><th>入力フォーマット</th></tr>
<tr><td>5</td><td>重要度
(Severity)</td><td>文字列</td><td>8</td><td>＜重要度（Severity）に指定可能な値(*3)＞
<table><tr><th>文字列</th><th>Code: Severity</th></tr><tr><td>Emergency</td><td>0: Emergency</td></tr><tr><td>Alert</td><td>1: Alert</td></tr><tr><td>Critical</td><td>2: Critical</td></tr><tr><td>Error</td><td>3: Error</td></tr><tr><td>Warning</td><td>4: Warning</td></tr><tr><td>Notice</td><td>5: Notice</td></tr><tr><td>Info</td><td>6: Informational</td></tr><tr><td>Debug</td><td>7: Debug</td></tr></table></td></tr>
<tr><td>6</td><td>ファシリティ</td><td>文字列</td><td>16</td><td>＜重要度（Severity）に指定可能な値(*4)＞
<table><tr><th>文字列</th><th>Code: Facility</th></tr><tr><td>kern</td><td>0: kernel messages</td></tr><tr><td>user</td><td>1: user-level messages</td></tr><tr><td>mail</td><td>2: mail system</td></tr><tr><td>daemon</td><td>3: system daemons</td></tr><tr><td>auth</td><td>4: security/authorization messages</td></tr><tr><td>syslog</td><td>5: messages generated internally by syslogd</td></tr><tr><td>lpr</td><td>6: line printer subsystem</td></tr><tr><td>news</td><td>7: network news subsystem</td></tr><tr><td>uucp</td><td>8: UUCP subsystem</td></tr><tr><td>cron</td><td>9: clock daemon</td></tr><tr><td>authpriv</td><td>10: security/authorization messages</td></tr><tr><td>ftp</td><td>11: FTP daemon</td></tr><tr><td>ntp</td><td>12: NTP subsystem</td></tr><tr><td>security</td><td>13: log audit</td></tr><tr><td>console</td><td>14: log alert</td></tr><tr><td>cron2</td><td>15: clock daemon (note 2)</td></tr><tr><td>local0</td><td>16: local use 0 (local0)</td></tr><tr><td>local1</td><td>17: local use 1 (local1)</td></tr><tr><td>local2</td><td>18: local use 2 (local2)</td></tr><tr><td>local3</td><td>19: local use 3 (local3)</td></tr><tr><td>local4</td><td>20: local use 4 (local4)</td></tr><tr><td>local5</td><td>21: local use 5 (local5)</td></tr><tr><td>local6</td><td>22: local use 6 (local6)</td></tr><tr><td>local7</td><td>23: local use 7 (local7)</td></tr></table></td></tr>
<tr><td>7</td><td>機器 IP アドレス</td><td>文字列（複数指定可能）</td><td>16</td><td>IPv4 アドレス（XXX.XXX.XXX.XXX）</td></tr>
<tr><td>8</td><td>その他</td><td>文字列（複数指定可能）</td><td>16(*5)</td><td>32 字以内の文字列</td></tr>
</table>

(*1) カレンダーから選択またはキーボード入力します。
(*2) 正規表現無効の場合，メッセージ中の文字列トークンに一致したものが表示対象となります。
(*3) 入力した正規表現がメッセージ中の文字列にマッチしたデータが表示対象となります。
(*4) ドロップダウンリストから選択またはキーボード入力します。リストに存在しない文字列は設定できません。
(*5) 「””」または「’’」を指定した場合，空文字または対象フィールドが存在しないデータが表示対象となります。

5.5 データ監視設定

AX-Collector が提供する監視機能に関する設定を行います。

5.5.1 SNMP 監視

SNMP 監視機能に関する設定を行います。

(1) ネットワーク機器

ネットワーク機器の概要を次に示します。

表 5-38 ネットワーク機器の概要

項目	説明
新規登録	MIB の収集対象となるネットワーク機器を登録します。 登録項目を次に示します。 ・名前 :任意の名前を登録します。最大 256 文字登録可能です。カンマ「,」および半角コロン「:」を除く文字を使用できます。 ・IP アドレス :収集対象となるネットワーク機器の IP アドレスを登録します。 ・コミュニティ名 :MIB を収集する際に指定するコミュニティ名を登録します。
一覧ダウンロード(CSV)	登録しているネットワーク機器の全情報を CSV 形式のファイルとしてダウンロードします。ファイル名は「S1_NetworkDevice_<*日付*>.csv」となります。
一覧表示項目の設定一括変更	ネットワーク機器一覧の変更可能なフィールドを一括更新します。表形式で編集可能です。 ・更新 :チェックした複数の設定を更新します。同時に変更可能な設定数は最大 20 です。 ・キャンセル :更新操作をキャンセルします。変更途中の設定は破棄されます。
ネットワーク機器一覧	登録したネットワーク機器の一覧を表示します。 参照ユーザでアクセスした場合，コミュニティ名を伏字で表示します。
選択設定の削除	一覧でチェックした複数の設定を一括で削除します。
選択設定の複製	一覧でチェックした 1 つの設定を複製します。

項目	説明
詳細	登録内容の詳細を表示します。また，該当のネットワーク機器のシステムおよびインタフェースに関する MIB 値を取得し表示することが出来ます。 ・収集データ表示　：SNMP 監視で該当のネットワーク機器から収集した MIB 値の時系列グラフを表示します。 ・ステータス情報更新：該当のネットワーク機器のシステムおよびインタフェースに関する MIB 値を取得し表示します。ここで MIB を取得することで，SNMP 監視の MIB オブジェクト設定において ifIndex の設定候補を表示することができます。
変更	登録内容を変更します。
検索	表示した一覧情報を対象に検索し，一致したものを表示します。

（2）　MIB オブジェクト

MIB オブジェクトの概要を次に示します。

表 5-39 MIB オブジェクトの概要

項目	説明
新規登録	収集対象となる MIB の OID を登録します。 登録項目を次に示します。 ・名前　：任意の名前を登録します。最大 256 文字登録可能です。カンマ「,」および半角コロン「:」を除く文字を使用できます。 ・ネットワーク機器　：ネットワーク機器一覧・登録で設定した，収集対象となるネットワーク機器を選択します。 ・オブジェクト識別子：収集対象となる MIB の OID を登録します。ニーモニックでの指定は出来ませんので，数字とピリオド(.)の組合せで指定して下さい。 ・反映　：インタフェース統計に関する代表的な OID をプルダウンから選択してオブジェクト識別子として入力することができます。また，ネットワーク機器詳細でステータス情報更新ボタンにより収集した ifIndex の一覧から任意の ifIndex を選択して入力することが出来ます。 ・正規化　：パケット数やバイト数などを単位時間あたりの変化量に換算した値を対象とする場合，指定します。

項目	説明
一覧ダウンロード(CSV)	登録している MIB オブジェクトの全情報を CSV 形式のファイルとしてダウンロードします。ファイル名は「S2_MibObject_<*日付*>.csv」となります。
一覧表示項目の設定一括変更	MIB オブジェクト一覧の変更可能なフィールドを一括更新します。表形式で編集可能です。 ・更新　：チェックした複数の設定を更新します。同時に変更可能な設定数は最大 20 です。 ・キャンセル　：更新操作をキャンセルします。変更途中の設定は破棄されます。
MIB オブジェクト一覧	登録した MIB オブジェクトの一覧を表示します。
選択設定の削除	一覧でチェックした複数の設定を一括で削除します。
選択設定の複製	一覧でチェックした 1 つの設定を複製します。
詳細	登録内容の詳細を表示します。
変更	登録内容を変更します。
検索	表示した一覧情報を対象に検索し，一致したものを表示します。

（3）　MIB オブジェクトグループ

MIB オブジェクトグループの概要を次に示します。

表 5-40 MIB オブジェクトグループの概要

項目	説明
新規登録	SNMP 監視の対象となる MIB オブジェクトと，閾値監視を行う際の閾値を登録します。 MIB オブジェクトグループには 1 つまたは複数の MIB オブジェクトを指定できます。1 つの MIB オブジェクトグループに複数の MIB オブジェクトを指定した場合， MIB 値の合計を監視対象とします。 登録項目を次に示します。 ・名前　：任意の名前を登録します。最大 256 文字登録可能です。カンマ「,」および半角コロン「:」を除く文字を使用できます。 ・タグ名　：MIB オブジェクトグループを一意に識別する名称を登録します。最大 32 文字登録可能です。使用できる文字は英数字とアンダーバー(_)です。なお，「time」で始まる名称はタグ名として使用できません。 ・MIB オブジェクト：SNMP 監視の対象となる MIB オブジェクトを選択します。 ・上限閾値監視：指定した値以上になった場合に異常として検知する閾値を登録します。 ・下限閾値監視：指定した値以下になった場合に異常として検知する閾値を登録します。 ・検知閾値　：正常な状態から異常な状態になったと判断する閾値を登録します。 ・検知乗数　：本項目で登録した回数分，連続して検知閾値以上または以下が発生した場合に，異常と判断して検知します。 ・復旧閾値　：異常を検知した状態から，正常な状態に復旧したと判断する閾値を登録します。 ・復旧乗数　：本項目で登録した回数分，連続して復旧閾値以上または以下が発生した場合に，正常な状態に復旧したと判断して検知します。 ・説明：該当の MIB オブジェクトグループについての説明を登録します。最大 256 文字登録可能です。 ・アクション　：該当の MIB オブジェクトグループに関する異常検知の際に必要なアクションを文字列として登録します。最大 256 文字登録可能です。 ・優先度　：該当の MIB オブジェクトグループに関する異常検知の優先度を登録します。優先度は，メニュー「管理」→「検知情報管理」で設定する優先度（１～５）およびラベルから選択します。 ・付加情報 1～3：該当の MIB オブジェクトグループに関する付加情報を登録します。付加情報は，メニュー「管理」→「検知情報管理」で設定する付加情報のリストから選択します。

項目	説明
一覧ダウンロード(CSV)	登録している MIB オブジェクトグループの全情報を CSV 形式のファイルとしてダウンロードします。ファイル名は「S3_MibObjectGroup_<*日付*>.csv」となります。
一覧表示項目の設定一括変更	MIB オブジェクトグループ一覧の変更可能なフィールドを一括更新します。表形式で編集可能です。 ・更新　：チェックした複数の設定を更新します。同時に変更可能な設定数は最大 20 です。 ・キャンセル　：更新操作をキャンセルします。変更途中の設定は破棄されます。
MIB オブジェクトグループ一覧	登録した MIB オブジェクトグループの一覧を表示します。
選択設定の削除	一覧でチェックした複数の設定を一括で削除します。
選択設定の複製	一覧でチェックした 1 つの設定を複製します。
詳細	登録内容の詳細を表示します。
変更	登録内容を変更します。
検索	表示した一覧情報を対象に検索し，一致したものを表示します。

（4）　SNMP 監視項目

SNMP 監視項目の概要を次に示します。

表 5-41 SNMP 監視項目の概要

項目	説明
新規登録	SNMP 監視の対象となる MIB オブジェクトグループと，監視方法，および検知・復旧時の Syslog 通知や SNMP Trap 通知を登録します。 SNMP 監視項目には 1 つまたは複数の MIB オブジェクトグループを指定できます。 登録項目を次に示します。 ・名前：任意の名前を登録します。最大 256 文字登録可能です。カンマ「,」および半角コロン「:」を除く文字を使用できます。 ・インデックス名：SNMP 監視項目を一意に識別する名称を登録します。最大 32 文字登録可能です。使用できる文字は英小文字，数字，アンダーバー(_)です。 ・MIB オブジェクトグループ：SNMP 監視の対象となる MIB オブジェクトグループを選択します。 ・データ収集：該当の SNMP 監視項目で MIB 情報の収集を行う場合はチェックします。 ・閾値監視：該当の SNMP 監視項目で閾値監視を行う場合はチェックします。 ・Impulse 連携：該当の SNMP 監視項目で Impulse 連携による監視を行う場合はチェックします。 ・Email 通知：該当の SNMP 監視項目の閾値監視または Impulse 連携で異常，または復旧検知の場合に，Email 通知を行う場合はチェックします。 ・Trap 通知：該当の SNMP 監視項目の閾値監視または Impulse 連携で異常，または復旧の検知時に，SNMP Trap 通知の送信を行う場合はチェックします。 ・Syslog 通知：該当の SNMP 監視項目の閾値監視または Impulse 連携で異常，または復旧の検知時に，Syslog の送信を行う場合はチェックします。 ・重要度：Syslog 通知する際の重要度(priority)を選択します。 ・参照先 URL：該当の SNMP 監視項目に関連する任意の URL を登録します。本項目で登録した URL は検知通知の詳細画面に表示されます。
一覧ダウンロード(CSV)	登録している監視項目の全情報を CSV 形式のファイルとしてダウンロードします。ファイル名は「S4_SnmpMonitoringItem_<*日付*>.csv」となります。

項目	説明
一覧表示項目の設定一括変更	SNMP 監視項目一覧の変更可能なフィールドを一括更新します。表形式で編集可能です。 ・更新　：チェックした複数の設定を更新します。同時に変更可能な設定数は最大 20 です。 ・キャンセル　：更新操作をキャンセルします。変更途中の設定は破棄されます。
SNMP 監視項目一覧	登録した SNMP 監視項目の一覧を表示します。
選択設定の削除	一覧でチェックした複数の設定を一括で削除します。
選択設定の複製	一覧でチェックした 1 つの設定を複製します。
詳細	登録内容の詳細を表示します。
変更	登録内容を変更します。
検索	表示した一覧情報を対象に検索し，一致したものを表示します。
Syslog/trap 通知 設定変更	Syslog 通知および Trap 通知の有効，無効のみを変更可能な画面を表示します。

また，SNMP 監視機能（Impulse 連携）では，登録したインデックス名と固定文字列”ax_cl_snmp_”を組み合わせた文字列を，データセット名として使用します。

（5）　一括登録・更新

一括登録・更新の概要を次に示します。

表 5-42 一括登録・更新の概要

項目	説明
一括登録・更新	SNMP 監視・収集設定における各登録情報を一括で登録します。一括登録には，全ての登録項目に関して，登録情報を入力した CSV ファイルを作成し，指定する必要があります。 登録項目を次に示します。 ・ネットワーク機器：ネットワーク機器に関する情報を入力した CSV ファイルを指定します。 ・MIB オブジェクト：MIB オブジェクトに関する情報を入力した CSV ファイルを指定します。 ・MIB オブジェクトグループ：MIB オブジェクトグループに関する情報を入力した CSV ファイルを指定します。 ・SNMP 監視項目　：SNMP 監視項目に関する情報を入力して CSV ファイルを指定します。 ・CSV ファイル未記載データ削除：CSV ファイルに入力されていない情報が AX-Collector に既に登録されている場合に削除するか，削除しないかを指定します。

（6）　環境設定

環境設定の概要を次に示します。

表 5-43 環境設定の概要

項目	説明
変更	SNMP 監視環境設定の登録内容を変更します。
初期化	登録内容を初期化します。
SNMP 監視環境設定	SNMP 監視環境設定の登録内容を表示します。
通知集約	SNMP 閾値監視において，異常検知中に，同じ監視項目で再度異常検知と判断した場合に通知を行うかどうかを設定します。 検知中に同じ監視項目で再度通知する必要が無い場合は，本項目をチェックしてください。同じ監視項目で検知中に関わらず毎回通知を行いたい場合はチェックを外してください。
収集周期	SNMP 監視を行う周期を選択します。 監視対象とする項目数により，収集周期を調整してください。
プロセス数	SNMP 監視に使用するプロセスの数を設定します。 監視対象とする項目数が多い場合，プロセス数を調整することで性能を改善できる場合があります。 システムのリソース（CPU，メモリ）に余裕がある場合にのみ変更ください。
タイムアウト時間（秒）	MIB 情報の取得要求にて，応答受信するまでのタイムアウト時間を設定します。
リトライ回数	MIB 情報の取得要求にて，取得失敗時のリトライ回数を設定します。
GenError 時リトライ	MIB 情報の取得要求が GenError によりエラーとなった場合にリトライを行います。
強制タイムアウト	MIB 情報の取得要求が，強制タイムアウト回数で指定した回数分タイムアウトした場合，その周期における，同じネットワーク機器からの MIB 情報の取得を行わず，タイムアウトとして扱います。
強制タイムアウト回数	監視項目毎に，強制タイムアウトを実行するまでのタイムアウト回数を設定します。
送信元 IP アドレス	SNMP 監視において，MIB 情報の取得要求を行う際に使用する送信元 IP アドレスを設定します。本設定は，SNMP 監視を行う全プロセスに適用されます。 送信元 IP アドレスとして，0.0.0.0 を設定した場合，MIB 取得に使用する送信元インタフェースから自動的に IP アドレスを選択し，使用します。
送信元ポート番号	SNMP 監視において，MIB 情報の取得要求を行う際に使用する送信元ポート番号を設定します。本項目で設定したポート番号からプロセス数分の連続したポート番号を，SNMP 監視を行うプロセスに当該ポート番号を適用します。
データ収集	SNMP 監視項目で MIB 情報の収集を行う場合はチェックします。

項目	説明
差分値補正	MIB 情報の取得がエラーまたはスキップとなった場合に，その次の監視タイミングで生成する MIB 収集データの差分値，および Counter 型 MIB の場合の監視データの生成方法を指定します。 今回収集した MIB 値と，その前の最後に収集成功した MIB 値との差分を，1 周期分相当の差分値に補正する場合はチェックします。 チェックが無い場合，今回収集した MIB 値と，その前の最後に収集成功した MIB 値との差分をそのまま使用します。
収集エラー時 0 補完	MIB オブジェクトグループに含まれる MIB 情報の取得が全てエラーとなった場合の，閾値監視の扱いを指定します。 該当の MIB オブジェクトグループの監視データを 0 として扱い，閾値監視の対象とする場合はチェックします。 チェックが無い場合，該当の MIB オブジェクトグループの監視データをデータ無しとして扱い，閾値監視の対象外とします。
閾値監視	SNMP 監視項目で閾値監視を行う場合はチェックします。
Impulse 連携	SNMP 監視項目で Impulse 連携を行う場合はチェックします。
Email 通知	SNMP 監視項目の閾値監視または Impulse 連携で異常，または復旧検知の場合に，Email 通知を行う場合はチェックします。
Trap 通知	SNMP 監視項目の閾値監視または Impulse 連携で異常，または復旧の検知時に，SNMP Trap 通知の送信を行う場合はチェックします。
Syslog 通知	SNMP 監視項目の閾値監視または Impulse 連携で異常，または復旧の検知時に，Syslog の送信を行う場合はチェックします。

項目	説明
Syslog メッセージ	以下に示すイベント発生時に送信する syslog のメッセージフォーマットを登録します。最大 1024 文字登録できます。 ・閾値監視 異常検知 ・閾値監視 復旧検知 ・Impulse 連携 異常検知 ・Impulse 連携 復旧検知 Syslog メッセージには，任意の文字，および予約語を指定します。予約語は syslog 送信時に適切な値に変換して送信されます。予約語はプルダウンから選択することで，入力欄の最後尾に追加されます。また，プルダウンから CEF フォーマットのヘッダ部分を入力することができます。 プルダウンから入力可能な予約語およびフォーマットを次に示します。 ・監視対象 {$MONITORING.TYPE} ・監視種別 {$MONITORING.OBJECT} ・異常検知時刻 {$DETECTED.DATETIME} ・復旧検知時刻 {$RECOVERED.DATETIME} ・監視項目名称 {$ITEM.NAME} ・インデックス名 {$ITEM.DATASET} ・グループ名 {$DATA.NAME} ・タグ名 {$DATA.METRICS} ・閾値種別 {$THRESHOLD.TYPE} ・閾値 {$THRESHOLD.VALUE} ・監視値 {$MONITORING.VALUE} ・機械学習の特性 {$IMPULSE.CHARACTERISTIC} ・機械学習の検知要件 {$IMPULSE.REQUIREMENT} ・通知詳細の URL {$URL} ・説明 {$DESCRIPTION} ・アクション {$ACTION} ・優先度 {$PRIORITY} ・優先度ラベル {$PRIORITY.LABEL} ・付加情報 1 {$ADDITIONAL1} ・付加情報 2 {$ADDITIONAL2} ・付加情報 3 {$ADDITIONAL3} ・CEF フォーマットヘッダー

5.5.2 フロー監視

フロー監視機能に関する設定を行います。

(1) フロー条件

フロー条件の概要を次に示します。

表 5-44 フロー条件の概要

項目	説明
新規登録	監視対象となるフロー条件を登録します。 登録項目を次に示します。 ・名前　：任意の名前を登録します。最大 256 文字登録可能です。カンマ「,」および半角コロン「:」を除く文字を使用できます。 ・データ名　：フロー条件を一意に識別する名称を登録します。最大 32 文字登録可能です。使用できる文字は英数字とアンダーバー(_)です。 ・フロー種別　：監視対象のデータを選択します。 ・絞り込み条件：可視化対象とするデータの範囲を絞り込む場合，その条件を指定します。 条件は最大 100 行指定することが出来，同一行内は AND 条件，各行間は除外をチェックした場合は AND NOT 条件，それ以外は OR 条件でフィルタします。 ・ユニーク数　：集計対象として，各パラメータのユニーク数を指定します。ユニーク数を指定した場合はこれが優先され，集計対象，集計方法の設定は無視されます。 ・集計対象　：集計する対象の情報（値）を指定します。 ・集計方法　：集計対象の集計方法を指定します。 ・TCP RTT 補完時間(ms)：集約条件に RTT を選択して，監視周期内に RTT を含むフローが無い場合に採用する値を指定します。
一覧ダウンロード(CSV)	登録しているフロー条件の全情報を CSV 形式のファイルとしてダウンロードします。ファイル名は「F1_FlowObject_<*日付*>.csv」，「F2_FilterSheet_<*日付*>.csv」となります。
一覧表示項目の設定一括変更	フロー条件一覧の変更可能なフィールドを一括更新します。表形式で編集可能です。 ・更新　：チェックした複数の設定を更新します。同時に変更可能な設定数は最大 20 です。 ・キャンセル　：更新操作をキャンセルします。変更途中の設定は破棄されます。
フロー条件一覧	登録したフロー条件の一覧を表示します。
選択設定の削除	一覧でチェックした複数の設定を一括で削除します。
選択設定の複製	一覧でチェックした 1 つの設定を複製します。
詳細	登録内容の詳細を表示します。
変更	登録内容を変更します。
検索	表示した一覧情報を対象に検索し，一致したものを表示します。

(2)　フロー条件グループ

フロー条件グループの概要を次に示します。

表 5-45 フロー条件グループの概要

項目	説明
新規登録	フロー監視の対象となるフロー条件と，閾値監視を行う際の閾値を登録します。 フロー条件グループには 1 つまたは複数のフロー条件を指定できます。1 つのフロー条件グループに複数のフロー条件を指定した場合， 対象となるフロー情報の合計を監視対象とします。 登録項目を次に示します。 ・名前 ：任意の名前を登録します。最大 256 文字登録可能です。カンマ「,」および半角コロン「:」を除く文字を使用できます。 ・タグ名 ：フロー条件グループを一意に識別する名称を登録します。最大 32 文字登録可能です。使用できる文字は英数字とアンダーバー(_)です。なお，「time」で始まる名称はタグ名として使用できません。 ・フロー条件 ：フロー監視の対象となるフロー条件を選択します。 ・上限閾値監視：指定した値以上になった場合に異常として検知する閾値を登録します。 ・下限閾値監視：指定した値以下になった場合に異常として検知する閾値を登録します。 ・検知閾値 ：正常な状態から異常な状態になったと判断する閾値を登録します。 ・検知乗数 ：本項目で登録した回数分，連続して検知閾値以上または以下が発生した場合に，異常と判断して検知します。 ・復旧閾値 ：異常を検知した状態から，正常な状態に復旧したと判断する閾値を登録します。 ・復旧乗数 ：本項目で登録した回数分，連続して復旧閾値以上または以下が発生した場合に，正常な状態に復旧したと判断して検知します。 ・説明 ：該当のフロー条件グループについての説明を登録します。最大 256 文字登録可能です。 ・アクション ：該当のフロー条件グループに関する異常検知の際に必要なアクションを文字列として登録します。最大 256 文字登録可能です。 ・優先度 ：該当のフロー条件グループに関する異常検知の優先度を登録します。優先度は，メニュー「管理」→「検知情報管理」で設定する優先度（１～５）およびラベルから選択します。 ・付加情報 1～3：該当のフロー条件グループに関する付加情報を登録します。付加情報は，メニュー「管理」→「検知情報管理」で設定する付加情報のリストから選択します。

項目	説明
一覧ダウンロード(CSV)	登録しているフロー条件グループの全情報を CSV 形式のファイルとしてダウンロードします。ファイル名は「F3_FlowObjectGroup_<*日付*>.csv」となります。
一覧表示項目の設定一括変更	フロー条件グループ一覧の変更可能なフィールドを一括更新します。表形式で編集可能です。 ・更新　：チェックした複数の設定を更新します。同時に変更可能な設定数は最大 20 です。 ・キャンセル　：更新操作をキャンセルします。変更途中の設定は破棄されます。
フロー条件グループ一覧	登録したフロー条件グループの一覧を表示します。
選択設定の削除	一覧でチェックした複数の設定を一括で削除します。
選択設定の複製	一覧でチェックした 1 つの設定を複製します。
詳細	登録内容の詳細を表示します。
変更	登録内容を変更します。
検索	表示した一覧情報を対象に検索し，一致したものを表示します。

（3）　フロー監視項目

フロー監視項目の概要を次に示します。

表 5-46 フロー監視項目の概要

項目	説明
新規登録	フロー監視の対象となるフロー条件グループと，監視方法，および検知・復旧時の Syslog 通知や SNMP Trap 通知を登録します。 フロー監視項目には 1 つまたは複数のフロー条件グループを指定できます。 登録項目を次に示します。 ・名前　：任意の名前を登録します。最大 256 文字登録可能です。カンマ「,」および半角コロン「:」を除く文字を使用できます。 ・インデックス名：フロー監視項目を一意に識別する名称を登録します。最大 32 文字登録可能です。使用できる文字は英小文字，数字，アンダーバー(_)です。 ・フロー条件グループ：フロー監視の対象となるフロー条件グループを選択します。 ・データ収集　：該当のフロー監視項目でフロー情報の収集を行う場合はチェックします。 ・閾値監視　：該当のフロー監視項目で閾値監視を行う場合はチェックします。 ・Impulse 連携　：該当のフロー監視項目で Impulse 連携による監視を行う場合はチェックします。 ・Email 通知　：該当のフロー監視項目の閾値監視または

項目	説明
	Impulse 連携で異常，または復旧検知の場合に Email 通知を行う場合はチェックします。 ・Trap 通知 ：該当のフロー監視項目の閾値監視または Impulse 連携で異常，または復旧の検知時に，SNMP Trap 通知の送信を行う場合はチェックします。 ・Syslog 通知 ：該当のフロー監視項目の閾値監視または Impulse 連携で異常，または復旧の検知時に，Syslog の送信を行う場合はチェックします。 ・重要度 ：Syslog 通知する際の重要度(priority)を選択します。 ・細分化 ：フロー条件グループで合算する前のフロー条件毎のデータを保存する場合はチェックします。 ・参照先 URL ：該当のフロー監視項目に関連する任意の URL を登録します。本項目で登録した URL は検知通知の詳細画面に表示されます。 ・監視周期 ：フロー監視を行う周期を環境設定で設定した周期から選択します。
一覧ダウンロード(CSV)	登録している監視項目の全情報を CSV 形式のファイルとしてダウンロードします。ファイル名は「F4_FlowMonitoringItem_<*日付*>.csv」となります。
一覧表示項目の設定一括変更	フロー監視項目一覧の変更可能なフィールドを一括更新します。表形式で編集可能です。 ・更新 ：チェックした複数の設定を更新します。同時に変更可能な設定数は最大 20 です。 ・キャンセル ：更新操作をキャンセルします。変更途中の設定は破棄されます。
フロー監視項目一覧	登録したフロー監視項目の一覧を表示します。
選択設定の削除	一覧でチェックした複数の設定を一括で削除します。
選択設定の複製	一覧でチェックした 1 つの設定を複製します。
詳細	登録内容の詳細を表示します。
変更	登録内容を変更します。
検索	表示した一覧情報を対象に検索し，一致したものを表示します。
Syslog/trap 通知 設定変更	Syslog 通知および Trap 通知の有効，無効のみを変更可能な画面を表示します。

また，フロー監視機能（Impulse 連携）では，登録したインデックス名と固定文字列”ax_cl_flow_”を組み合わせた文字列を，データセット名として使用します。

（4） 一括登録・更新

一括登録・更新の概要を次に示します。

表 5-47 一括登録・更新の概要

項目	説明
一括登録・更新	フロー監視・収集設定における各登録情報を一括で登録します。一括登録には，全ての登録項目に関して，登録情報を入力した CSV ファイルを作成し，指定する必要があります。 登録項目を次に示します。 ・フロー条件：フロー条件に関する情報を入力した CSV ファイルを指定します。 ・フローフィルタシート：フロー条件の絞り込み条件に関する情報を入力した CSV ファイルを指定します。 フロー条件毎に，絞り込み条件の最大行数 100 行です。 ・フロー条件グループ：フロー条件グループに関する情報を入力した CSV ファイルを指定します。 ・フロー監視項目：フロー監視項目に関する情報を入力して CSV ファイルを指定します。 ・CSV ファイル未記載データ削除：CSV ファイルに入力されていない情報が AX-Collector に既に　登録されている場合に削除するか，削除しないかを指定します。

(5)　環境設定

環境設定の概要を次に示します。

表 5-48 環境設定の概要

項目	説明
変更	フロー監視環境設定の登録内容を変更します。
初期化	登録内容を初期化します。
フロー監視環境設定	フロー監視環境設定の登録内容を表示します。
通知集約	フロー閾値監視において，異常検知中に，同じ監視項目で再度異常検知と判断した場合に通知を行うかどうかを設定します。 検知中に同じ監視項目で再度通知する必要が無い場合は，本項目をチェックしてください。同じ監視項目で検知中に関わらず毎回通知を行いたい場合はチェックを外してください。
プロセス数	フロー監視に使用するプロセスの数を設定します。 監視対象とする項目数が多い場合，プロセス数を調整することで性能を改善できる場合があります。 システムのリソース（CPU，メモリ）に余裕がある場合にのみ変更ください。
タイムアウト時間（秒）	フロー情報の収集要求にて，応答受信するまでのタイムアウト時間を設定します。

項目	説明
オフセット時間（秒）	監視開始タイミングのオフセット時間を設定します。 本オフセット時間を設定することにより，AX-Sensor から送信される当該周期の Netflow パケットをすべて受信してから対象フロー情報の収集が可能になります。
データ収集	フロー監視項目でフロー情報の収集を行う場合はチェックします。
閾値監視	フロー監視項目で閾値監視を行う場合はチェックします。
Impulse 連携	フロー監視項目で Impulse 連携を行う場合はチェックします。
Email 通知	フロー監視項目の閾値監視または Impulse 連携で異常，または復旧検知の場合に Email 通知を行う場合はチェックします。
Trap 通知	フロー監視項目の閾値監視または Impulse 連携で異常，または復旧の検知時に，SNMP Trap 通知の送信を行う場合はチェックします。
Syslog 通知	フロー監視項目の閾値監視または Impulse 連携で異常，または復旧の検知時に，Syslog の送信を行う場合はチェックします。

項目	説明
Syslog メッセージ	以下に示すイベント発生時に送信する syslog のメッセージフォーマットを登録します。最大 1024 文字登録できます。 ・閾値監視 異常検知 ・閾値監視 復旧検知 ・Impulse 連携 異常検知 ・Impulse 連携 復旧検知 Syslog メッセージには，任意の文字，および予約語を指定します。予約語は syslog 送信時に適切な値に変換して送信されます。予約語はプルダウンから選択することで，入力欄の最後尾に追加されます。また，プルダウンから CEF フォーマットのヘッダ部分を入力することができます。 プルダウンから入力可能な予約語およびフォーマットを次に示します。 ・監視対象 {$MONITORING.TYPE} ・監視種別 {$MONITORING.OBJECT} ・異常検知時刻 {$DETECTED.DATETIME} ・復旧検知時刻 {$RECOVERED.DATETIME} ・監視項目名称 {$ITEM.NAME} ・インデックス名 {$ITEM.DATASET} ・グループ名 {$DATA.NAME} ・タグ名 {$DATA.METRICS} ・閾値種別 {$THRESHOLD.TYPE} ・閾値 {$THRESHOLD.VALUE} ・監視値 {$MONITORING.VALUE} ・機械学習の特性 {$IMPULSE.CHARACTERISTIC} ・機械学習の検知要件 {$IMPULSE.REQUIREMENT} ・通知詳細の URL {$URL} ・説明 {$DESCRIPTION} ・アクション {$ACTION} ・優先度 {$PRIORITY} ・優先度ラベル {$PRIORITY.LABEL} ・付加情報１ {$ADDITIONAL1} ・付加情報２ {$ADDITIONAL2} ・付加情報３ {$ADDITIONAL3} ・CEF フォーマットヘッダー
収集周期	フロー監視を行う周期を３つ設定します。 監視項目単位に何れかの周期を適用することが出来ます。 監視対象とする項目数により，収集周期を調整してください。
タイムスタンプ	収集周期毎に監視データに紐付ける監視時刻として，周期の先頭時刻か周期の最終時刻かを選択します。 REST-API によるデータ取得や個別ビュー等の可視化と同じ動作にする場合は，周期の先頭時刻を選択してください。

（6） 過去データ／閾値生成・削除

過去データ生成・削除の概要を次に示します。

表 5-49 過去データ／閾値生成・削除の概要

項目	説明
監視データ生成	監視データ生成の条件を登録します。 登録項目を次に示します。 ・フロー監視項目：設定済のフロー監視項目から，監視データ生成の対象を選択します。 ・期間：開始日と終了日で，監視データ生成の対象期間を指定します。 ・監視データ生成：指定した条件の監視データ生成を登録します。待機中，生成中または停止中の監視データ生成で，監視項目が同じ，かつ期間が重複するものが他にある場合は，登録できません。
監視データ削除	監視データ削除の条件を登録します。 登録項目を次に示します。 ・フロー監視項目：設定済のフロー監視項目から，監視データ削除の対象を選択します。 ・期間：開始日と終了日で，監視データ削除の対象期間を指定します。 ・監視データ削除：指定した条件の監視データ削除を登録します。
閾値生成	監視閾値生成の条件を登録します。指定期間の収集済み監視データを参照し，閾値を生成します。 登録項目を次に示します。 ・フロー監視項目：設定済のフロー監視項目から，監視閾値生成の対象を選択します。 ・期間：開始日と終了日で，監視データ閾値生成の対象期間を指定します。 ・閾値生成パラメータ：生成する閾値の算出条件を指定します。詳細は，「**表 5-50 閾値生成パラメータの概要**」を参照。 ・閾値生成：指定した条件の監視閾値生成を登録します。待機中，生成中または停止中の監視閾値生成で，監視項目が同じ，かつ期間が重複するものが他にある場合は，登録できません。
閾値削除	監視閾値削除の条件を登録します。指定した監視データの閾値を削除します。 登録項目を次に示します。 ・フロー監視項目：設定済のフロー監視項目から，監視閾値削除の対象を選択します。 ・削除対象閾値：削除対象の閾値を選択します。 ・閾値削除：指定した条件の監視閾値を削除します。
選択履歴の削除	選択した履歴を削除します。 状態が待機中，生成完了，削除完了，異常終了および生成停止の場合のみ削除できます。
監視項目名	生成／削除対象の監視項目名を表示します。
生成・削除対象	生成／削除対象（収集データ／閾値）を表示します。
開始期間	生成／削除対象期間の開始日時を表示します。
終了期間	生成／削除対象期間の終了日時を表示します。

項目	説明
処理開始時間	生成／削除処理を開始した日時を表示します。
処理終了時間	生成／削除処理を終了した日時を表示します。
状態	状態（待機中／生成中／生成完了／削除完了／異常終了／停止中／生成停止）を表示します。
詳細	監視データ生成／削除対象のフロー監視項目毎 監視データ詳細画面を表示します。
閾値詳細	閾値生成／削除の実施結果詳細画面を表示します。 詳細画面は**表 5-51 閾値詳細の概要**を参照。
停止	監視データ／閾値生成を途中停止します。 なお，監視データ／閾値生成は即座には停止せず，停止中を経由して，最終的に生成停止となります。 状態が生成中の場合のみ停止できます。
再開	停止中の監視データ／閾値生成を再開します。 状態が停止中の場合のみ再開できます。

表 5-50 閾値生成パラメータの概要

項目	説明
閾値生成方式	指定した監視項目の収集済みデータを指定期間で集計した値を元に閾値を生成する計算方式を指定します。 ・上限閾値＝最大値，下限閾値＝最小値 上限閾値を集計データの最大値，下限閾隊を集計データの最小値とする方式です。
閾値生成オプション	閾値生成方式別の生成オプションパラメータを指定します。 【閾値生成方式＝上限閾値＝最大値，下限閾値＝最小値】 集計した最大値または最小値を，閾値毎に指定した割合で調整し，閾値に設定します。閾値は次の計算式で算出されます。 ・上限検知閾値 生成閾値＝最大値 ＋｜最大値｜*【割合 a%】 ・上限復旧閾値 生成閾値＝最大値 ＋｜最大値｜*【割合 b%】 ・下限検知閾値 生成閾値＝最小値 ＋｜最小値｜*【割合 c%】 ・下限復旧閾値 生成閾値＝最小値 ＋｜最小値｜*【割合 d%】 割合 a～d に指定可能な数値：-100,000～100,000 未指定時，0 として計算します。 ・自動適用 各生成閾値の監視設定への自動適用を指定します。 有効：生成した閾値を監視設定に自動適用します。 無効：閾値の生成のみを行います。

表 5-51 閾値詳細の概要

項目	説明
監視項目収集データ	閾値生成に指定した期間のフロー監視項目のフロー監視データをグラフ表示します。 過去の監視による検知点も表示されます。
閾値生成パラメータ	指定した閾値の生成条件と状態，および処理時刻を表示します。
算出閾値	フロー監視項目内のフロー条件グループ毎に，集計値および生成した閾値を表示します。 ・ID　：フロー条件グループの ID ・名前　：フロー条件グループ名 ・集計値　：指定期間内の該当フロー条件グループの集計データ値（平均値，最大値，最小値）を表示します。 ・旧閾値　：閾値生成処理時点で該当フロー条件グループの設定閾値を表示します。 ・生成閾値：収集データから閾値生成パラメータを用いて，生成した閾値を表示します。 ・適用時刻：生成閾値を監視設定に適用した時刻を表示します。なお，閾値生成パラメータで，自動適用オプションが無効である場合には，適用ボタンが表示されます。押下すると適用され，その時刻が表示されます。 ・操作　：詳細ボタンを押下すると，該当フロー条件グループのデータ収集画面が表示されます。

5.5.3 フローランキング監視

フローランキング監視機能に関する設定を行います。

(1) フローランキング監視項目

フローランキング監視項目の概要を次に示します。

表 5-52 フローランキング監視項目の概要

項目	説明
新規登録	監視対象となるフロー条件，集計対象と閾値を登録します。 登録項目を次に示します。 ・名前　：最大 128 文字登録可能です。半角の「&＜＞"'¥=-;`/:*?|,」を除く文字を使用できます。 ・データ名　：フローランキング監視設定を一意に識別す

項目	説明
	る名称を登録します。最大 64 文字登録可能です。使用できる文字は英数字とアンダーバー(_)です。 ・説明　：該当のフローランキング監視項目についての説明を登録します。最大 256 文字登録可能です。 ・絞り込み条件：収集対象とするデータの範囲を絞り込む場合，その条件を指定します。 条件は最大 100 行指定することが出来，同一行内は AND 条件，各行間は除外をチェックした場合は AND NOT 条件，それ以外は OR 条件でフィルタします。 ・集約条件　：集計ランキング数 集計フィールド組み合わせ毎の集計対象のランキング集計数を指定します。最大数は 100 です。 集計フィールド ランキング集計時に抽出するフィールド名を指定します。最大５つの組み合わせを指定可能です。 ・集計対象　：集約条件毎に集計する値および閾値を設定します。最大 10 の組み合わせを指定可能です。 集計値 集約条件毎の集計対象と集計方法を設定します。値のソート順（降順／昇順）も指定します。 閾値（ランク別集計値） 集約条件毎に集計した集計値に対する監視閾値（上限値／下限値）を設定します。集計した値または，割合（トータル集計値に対する割合，もしくは指定値に対する割合）を閾値として指定可能です。 閾値（トータル集計値） 集約条件毎ではなくトータルの集計値に対する監視閾値（上限値／下限値）を設定します。集計した値または，割合（トータル集計値に対する割合，もしくは指定値に対する割合）を閾値として指定可能です。 ・監視動作設定：データ収集 該当のフローランキング監視項目でフロー情報の収集を行う場合はチェックします。 監視周期 フローランキング監視を行う周期を環境設定で設定した周期から選択します。 ・検知通知設定：通知集約時間（分） 該当のフローランキング監視項目の検知

項目	説明
	を集約する時間（分）を指定します。指定時間内に複数回の検知イベントが発生した場合，検知通知・syslog は抑止されます。 Email 通知 該当フローランキング監視項目の閾値監視で検知の場合に Email 通知を行う場合はチェックします。 syslog 通知（ランク別閾値監視） 集約条件毎のランキング上位の集計値に対する閾値監視条件にヒットした場合の syslog 送信を行う場合はチェックします。 syslog 通知（トータル閾値監視） トータルの集計値に対する閾値監視条件にヒットした場合の syslog 送信を行う場合はチェックします。 syslog 通知（CEF 形式） ランク別閾値監視，トータル閾値監視に対する syslog の形式を CEF 形式にする場合はチェックします。 重要度 Syslog 通知する際の重要度(priority)を選択します。 参照先 URL 該当のフローランキング監視項目に関連する任意の URL を登録します。本項目で登録した URL は検知通知の詳細画面に表示され，syslog にも含まれます。 アクション 該当のフローランキング監視項目に関する異常検知の際に必要なアクションを文字列として登録します。最大 256 文字登録可能です。 優先度 該当のフローランキング監視項目に関する異常検知の優先度を登録します。優先度は，メニュー「管理」→「検知情報管理」で設定する優先度（１～５）およびラベルから選択します。 付加情報 1～3 該当のフローランキング監視項目に関する付加情報を登録します。付加情報は，メニュー「管理」→「検知情報管理」で設定する付加情報のリストから選択します。 ・データ検索設定： フロー種別 監視対象のデータを選択します。 最大検索数

項目	説明
	データベース検索時の最大検索数を指定します。 検索タイムアウト時間（秒） データベース検索時の検索タイムアウト時間を指定します。
一覧ダウンロード(CSV)	登録しているフローランキング監視項目の全情報を CSV 形式のファイルとしてダウンロードします。ファイル名は「FR1_FlowRanking_<*日付*>.csv」，「FR2_FilterSheet_<*日付*>.csv」，「FR3_FlowRankingAggs_<*日付*>.csv」，「FR4_FlowRankingMetrics_<*日付*>.csv」となります。
一覧表示項目の設定一括変更	フローランキング監視設定一覧の変更可能なフィールドを一括更新します。表形式で編集可能です。 ・更新　：チェックした複数の設定を更新します。同時に変更可能な監視項目数は最大 20 です。 ・キャンセル　：更新操作をキャンセルします。変更途中の設定は破棄されます。
フローランキング監視項目一覧	登録したフローランキング監視項目の一覧を表示します。
選択設定の削除	チェックした複数の設定を一括で削除します。
選択設定の複製	チェックした 1 つの設定を複製します。
詳細	登録内容の詳細を表示します。
変更	登録内容を変更します。
検索	表示した一覧情報を対象に検索し，一致したものを表示します。

（2）　一括登録・更新

一括登録・更新の概要を次に示します。

表 5-53　一括登録・更新の概要

項目	説明
一括登録・更新	フローランキング監視における各登録情報を一括で登録します。 一部，または全ての登録項目に，登録情報を入力した CSV ファイルを指定します。 登録項目を次に示します。 ・フローランキング監視： フローランキング監視項目に関する情報を入力した CSV ファイルを指定します。 ・フローフィルタシート： フローランキング監視項目の絞り込み条件に関する情報を入力した CSV ファイルを指定します。 フローランキング監視項目毎に，絞り込み条件の最大行数 100 行です。 ・フローランキング集約条件： フローランキング監視項目の集約条件に関する情報を

項目	説明
	入力した CSV ファイルを指定します。 ・フローランキング集計対象： フローランキング監視項目の集計対象に関する情報を入力して CSV ファイルを指定します。 ・CSV ファイル未記載データ削除： CSV ファイルに入力されていない情報が AX-Collector に既に 登録されている場合に削除するか，削除しないかを指定します。

（3） 環境設定

環境設定の概要を次に示します。

表 5-54 環境設定の概要

項目	説明
変更	環境設定の登録内容を変更します。
初期化	登録内容を初期化します。
フローランキング監視環境設定	フローランキング監視環境設定の登録内容を表示します。
プロセス数	フローランキング監視に使用するプロセスの数を設定します。監視対象とする項目数が多い場合，プロセス数を調整することで性能を改善できる場合があります。 システムのリソース（CPU，メモリ）に余裕がある場合にのみ変更ください。
データ収集	フローランキング監視項目で監視データの集計を行う場合はチェックします。
閾値監視	フローランキング監視項目で閾値監視を行う場合はチェックします。
Email 通知	フローランキング監視項目の閾値監視で検知の場合に Email 通知を行う場合はチェックします。
Syslog 通知	フローランキング監視項目の閾値監視で検知時に，Syslog の送信を行う場合はチェックします。
収集周期	フローランキングデータ監視を行う周期を選択します。
オフセット時間（秒）	各周期の監視開始タイミングのオフセット時間を設定します。本オフセット時間を設定することにより，AX-Sensor から送信される当該周期の Netflow パケットをすべて受信してから対象フロー情報の収集が可能になります。 またプロセス間での動作タイミングをずらすことで CPU リソース等の有効利用が可能です。
タイムスタンプ	収集周期毎に監視データに紐付ける監視時刻として，周期の先頭時刻か周期の最終時刻かを選択します。

（4） 過去データ生成

過去データ生成の概要を次に示します。

表 5-55　過去データ生成・削除の概要

項目	説明
監視データ生成	監視データ生成の条件を登録します。 登録項目を次に示します。 ・フローランキング監視項目：設定済のフローランキング監視項目から，監視データ生成の対象を選択します。 ・期間　：開始日と終了日で，監視データ生成の対象期間を指定します。 ・監視データ生成：指定した条件の監視データ生成を登録します。待機中，生成中または停止中の監視データ生成で，監視項目が同じ，かつ期間が重複するものが他にある場合は，登録できません。
監視データ削除	監視データ削除の条件を登録します。 登録項目を次に示します。 ・フローランキング監視項目：設定済のフローランキング監視項目から，監視データ削除の対象を選択します。 ・期間　：開始日と終了日で，監視データ削除の対象期間を指定します。 ・監視データ削除：指定した条件の監視データ削除を登録します。
選択履歴の削除	選択した履歴を削除します。 状態が待機中，生成完了，削除完了，異常終了および生成停止の場合のみ削除できます。
フローランキング監視項目名	監視データ生成／削除対象の監視項目名を表示します。
開始期間	監視データ生成／削除対象期間の開始日時を表示します。
終了期間	監視データ生成／削除対象期間の終了日時を表示します。
処理開始時間	監視データ生成／削除処理を開始した日時を表示します。
処理終了時間	監視データ生成／削除処理を終了した日時を表示します。
状態	監視データ生成状態（待機中／生成中／生成完了／削除完了／異常終了／停止中／生成停止）を表示します。
詳細	対象の外部監視項目毎 監視データ詳細画面を表示します。
停止	監視データ生成を途中停止します。 なお，監視データ生成は即座には停止せず，停止中を経由して，最終的に生成停止となります。 状態が生成中の場合のみ停止できます。
再開	停止中の監視データ生成を再開します。 状態が停止中の場合のみ再開できます。

5.5.4　外部データ監視

外部データ監視機能に関する設定を行います。

（1） 外部収集データ

外部収集データの概要を次に示します。

表 5-56 外部収集データの概要

項目	説明
新規登録	監視対象となる外部収集データを登録します。 登録項目を次に示します。 ・外部データカテゴリ名： 任意のカテゴリ名を登録します。最大 128 文字登録可能です。半角の「& < > " ' ¥ = - ; ` / : * ? | ,」を除く文字を使用できます。 ・外部データ名： 任意のデータ名を登録します。最大 128 文字登録可能です。半角の「& < > " ' ¥ = - ; ` / : * ? | ,」を除く文字を使用できます。 ・カテゴリ（入力データ）： REST API に指定するカテゴリ名を登録します。最大 128 文字登録可能です。使用できる文字は英数字とアンダーバー(_)です。 ・データ名（入力データ）： REST API に指定するデータ名を登録します。最大 128 文字登録可能です。使用できる文字は英数字とアンダーバー(_)です。 ・補足説明： 外部収集データ一覧に表示する補足説明を登録します。最大 128 文字登録可能です。半角の「& < > " ' ¥ = - ; ` / : * ? | ,」を除く文字を使用できます。 ・外部データ収集： 該当の外部データの収集を行う場合はチェックします。
一覧ダウンロード(CSV)	登録している外部収集データの全情報を CSV 形式のファイルとしてダウンロードします。ファイル名は「E1_ExternalData_<*日付*>.csv」となります。
一覧表示項目の設定一括変更	外部収集データ一覧の変更可能なフィールドを一括更新します。表形式で編集可能です。 ・更新 ：チェックした複数の設定を更新します。同時に変更可能な監視項目数は最大 20 です。 ・キャンセル ：更新操作をキャンセルします。変更途中の設定は破棄されます。
外部収集データ設定一覧	登録した外部収集データの一覧を表示します。
選択設定の削除	チェックした複数の設定を一括で削除します。
選択設定の複製	チェックした 1 つの設定を複製します。
詳細	登録内容の詳細を表示します。
変更	登録内容を変更します。
検索	表示した一覧情報を対象に検索し，一致したものを表示します。

（2） 外部監視データ

外部監視データの概要を次に示します。

表 5-57 外部監視データの概要

項目	説明
新規登録	外部データ監視の対象となる外部データと，外部データから生成する監視データの演算方法，および閾値監視を行う際の閾値を登録します。 登録項目を次に示します。 ・監視データカテゴリ名： 任意のカテゴリ名を登録します。最大 128 文字登録可能です。半角の「& < > " ' ¥ = - ; ` / : * ? | ,」を除く文字を使用できます。 ・監視データ名： 任意のデータ名を登録します。最大 128 文字登録可能です。半角の「& < > " ' ¥ = - ; ` / : * ? | ,」を除く文字を使用できます。 ・メトリクス名： 監視データを一意に識別する名称を登録します。最大 32 文字登録可能です。使用できる文字は英数字とアンダーバー(_)です。なお，「time」で始まる名称はメトリクス名として使用できません。 ・外部データ（操作パネル）： ➢ 外部データ 外部データ監視の対象となる外部収集データもしくは SNMP／フロー／外部データ監視機能による収集済みデータを選択します。以降の記載で外部データはこれらデータの総称です。 [注意事項] 1 つの外部監視データ内に同一の外部データを複数選択しないでください。監視・表示が正しく行われない場合があります。 ➢ 演算種別 監視周期内において，同一の外部データを複数受信した場合の監視データの算出に使用する外部データの演算種別を以下から選択します。 ①合計：監視周期内で受信した外部データの値の合計を監視データの算出に使用します。 ②平均：監視周期内で受信した外部データの値の平均を監視データの算出に使用します。 ③最大：監視周期内で受信した外部データの値の中で最大の値を監視データの算出に使用します。 ④最小：監視周期内で受信した外部データの値の中で最小の値を監視データの算出に使用します。 ⑤最新：監視周期内で最後に受信した外部データの値を監視データの算出に使用します。 ➢ 移動[合計/平均]の期間(秒) 上記演算種別で合計もしくは平均を指定し，本設定（秒数）を指定した場合，移動合計もしくは移動平均の値を監視データの算出に使用します。

項目	説明
	例）監視周期を 1 分，本設定を 120 秒と設定した場合，12:00 の監視データは 11:58～12:00 の外部データから算出し，12:01 の監視データは 11:59～12:01 の外部データから算出します。 ➢ 未受信時の補完値 監視周期内において，外部データを受信しなかった場合に監視データの算出に使用する補完値を指定します。未指定の場合，データなし（補完しない）と扱います。 ・演算種別： 上記外部データ（操作パネル）の指定において，複数の外部データを指定した場合の監視データの演算方法を以下から選択します。 ①合計：外部データの値の合計を監視データとして使用します。 ②平均：外部データの値の平均を監視データとして使用します。 ③最大：指定した外部データの値の中で最大の値を監視データとして使用します。 ④最小：指定した外部データの値の中で最小の値を監視データとして使用します。 ⑤差分：外部データ（操作パネル）の「ID:1 の外部データ」－「ID:2 の外部データ」を監視データとして使用します。 ⑥割合：外部データ（操作パネル）の「ID:1 の外部データ」÷「ID:2 の外部データ」を監視データとして使用します。 「ID:2 の外部データ」が 0 の場合，監視データなしと扱います。 ・未受信設定： 上記外部データ（操作パネル）に設定した外部データが監視周期内において，データなし（未受信かつ補完なし）の場合の監視データの扱いを指定します。 ➢ 一部未受信時 一部の外部データがデータなしの場合の監視データの扱いを以下から選択します。 ①演算：データが存在する外部データで監視データを算出します。ただし，差分／割合については，設定できません。 ②データなし：監視データをデータなしと扱います。 ③指定値：下記指定値で設定した値を監視データとして使用します。 ➢ 全未受信時 全ての外部データがデータなしの場合の監視データの扱いを以下から選択します。 ①データなし：監視データをデータなしと扱います。 ②指定値：下記指定値で設定した値を監視データとして使用します。

項目	説明
	➢ 指定値 上記，一部未受信時および全未受信時で指定値を選択した場合に使用する監視データの値を設定します。 ・上限閾値監視：指定した値以上になった場合に異常として検知する閾値を登録します。 ・下限閾値監視：指定した値以下になった場合に異常として検知する閾値を登録します。 ・検知閾値　：正常な状態から異常な状態になったと判断する閾値を登録します。 ・検知乗数　：本項目で登録した回数分，連続して検知閾値以上または以下が発生した場合に，異常と判断して検知します。 ・復旧閾値　：異常を検知した状態から，正常な状態に復旧したと判断する閾値を登録します。 ・復旧乗数　：本項目で登録した回数分，連続して復旧閾値以上または以下が発生した場合に，正常な状態に復旧したと判断して検知します。 ・説明　：該当の外部監視データについての説明を登録します。最大 256 文字登録可能です。 ・アクション　：該当の外部監視データに関する異常検知の際に必要なアクションを文字列として登録します。最大 256 文字登録可能です。 ・優先度　：該当の外部監視データに関する異常検知の優先度を登録します。優先度は，メニュー「管理」→「検知情報管理」で設定する優先度（１～５）およびラベルから選択します。 ・付加情報 1～3　：該当の外部監視データに関する付加情報を登録します。付加情報は，メニュー「管理」→「検知情報管理」で設定する付加情報のリストから選択します。
一覧ダウンロード(CSV)	登録している外部監視データの全情報を CSV 形式のファイルとしてダウンロードします。ファイル名は「E2_Metrics_<*日付*>.csv」と「E3_ExternalDataMetricsRelation_<*日付*>.csv」となります。
一覧表示項目の設定一括変更	外部監視データ設定一覧の変更可能なフィールドを一括更新します。表形式で編集可能です。 ・更新　：チェックした複数の設定を更新します。同時に変更可能な監視項目数は最大 20 です。 ・キャンセル　：更新操作をキャンセルします。変更途中の設定は破棄されます。
外部監視データ設定一覧	登録した外部監視データの一覧を表示します。
選択設定の削除	チェックした複数の設定を一括で削除します。
選択設定の複製	チェックした１つの設定を複製します。
詳細	登録内容の詳細を表示します。
変更	登録内容を変更します。

項目	説明
検索	表示した一覧情報を対象に検索し，一致したものを表示します。

（3） 外部データ監視項目

外部データ監視項目の概要を次に示します。

表 5-58 外部データ監視項目の概要

項目	説明
新規登録	外部データ監視の対象となる外部監視データ，監視方法，検知・復旧時の Syslog 通知や SNMP Trap 通知，および監視周期を登録します。 外部データ監視項目には 1 つまたは複数の外部監視データを指定できます。 登録項目を次に示します。 ・監視項目カテゴリ名： 任意のカテゴリ名を登録します。最大 128 文字登録可能です。半角の「& < > " ' ¥ = - ; ` / : * ? | ,」を除く文字を使用できます。 ・監視項目データ名： 任意のデータ名を登録します。最大 128 文字登録可能です。半角の「& < > " ' ¥ = - ; ` / : * ? | ,」を除く文字を使用できます。 ・データセット名： 外部データ監視項目を一意に識別する名称を登録します。最大 32 文字登録可能です。使用できる文字は英小文字，数字，アンダーバー(_)です。 ・監視データ： 外部データ監視の対象となる監視データを選択します。 ・監視データ集計： 該当の外部データ監視項目で外部データの集計を行う場合はチェックします。 ・閾値監視： 該当の外部データ監視項目で閾値監視を行う場合はチェックします。 ・Impulse 連携： 該当の外部データ監視項目で Impulse 連携による監視を行う場合はチェックします。 ・Email 通知 該当の外部データ監視項目の閾値監視／Impulse 連携監視で異常，または復旧の検知時に，Email 通知の送信を行う場合はチェックします。 ・Trap 通知： 該当の外部データ監視項目の閾値監視／Impulse 連携監視で異常，または復旧の検知時に，SNMP Trap 通知の送信を行う場合はチェックします。 ・Syslog 通知：

項目	説明
	該当の外部データ監視項目の閾値監視／Impulse 連携監視で異常，または復旧の検知時に，Syslog の送信を行う場合はチェックします。 ・重要度： Syslog 通知する際の重要度(priority)を選択します。 ・参照先 URL： 該当の外部データ監視項目に関連する任意の URL を登録します。本項目で登録した URL は検知通知の詳細画面に表示されます。 ・監視周期： 該当の外部データ監視項目の監視周期を選択します。
一覧ダウンロード(CSV)	登録している監視項目の全情報を CSV 形式のファイルとしてダウンロードします。ファイル名は「E4_ExternalMonitoringItem_<*日付*>.csv」となります。
一覧表示項目の設定一括変更	外部データ監視項目一覧の変更可能なフィールドを一括更新します。表形式で編集可能です。 ・更新　：チェックした複数の設定を更新します。同時に変更可能な監視項目数は最大 20 です。 ・キャンセル　：更新操作をキャンセルします。変更途中の設定は破棄されます。
外部データ監視項目 設定一覧	登録した外部データ監視項目の一覧を表示します。
選択設定の削除	チェックした複数の設定を一括で削除します。
選択設定の複製	チェックした 1 つの設定を複製します。
詳細	選択した外部データ監視項目の設定詳細と関連監視データ一覧を表示します。
変更	登録内容を変更します。
検索	表示した一覧情報を対象に検索し，一致したものを表示します。
Syslog/Trap 通知設定変更	Syslog 通知および Trap 通知の有効，無効のみを変更可能な画面を表示します。

また，外部データ監視機能（Impulse 連携）では，登録したデータセット名と固定文字列”ax_cl_ext_”を組み合わせた文字列を，Impulse 送信用データセット名として使用します。

（4）　一括登録・更新

一括登録・更新の概要を次に示します。

表 5-59　一括登録・更新の概要

項目	説明
一括登録・更新	外部データ監視における各登録情報を一括で登録します。 一部，または全ての登録項目に，登録情報を入力した CSV ファイルを指定します。 登録項目を次に示します。 ・外部データ： 外部収集データに関する情報を入力した CSV ファイルを指定します。 ・監視データ： 外部監視データに関する情報を入力した CSV ファイルを指定します。 ・外部監視詳細データ： 外部監視データ（外部データと監視データの関連付け）に関する情報を入力した CSV ファイルを指定します。 ・外部データ監視項目： 外部データ監視項目に関する情報を入力して CSV ファイルを指定します。 ・CSV ファイル未記載データ削除： CSV ファイルに入力されていない情報が AX-Collector に既に　登録されている場合に削除するか，削除しないかを指定します。

（5）　環境設定

環境設定の概要を次に示します。

表 5-60　環境設定の概要

項目	説明
変更	環境設定の登録内容を変更します。
初期化	登録内容を初期化します。
収集・監視動作設定一覧	外部データ監視環境設定の登録内容を表示します。
通知集約	外部データ閾値監視において，異常検知中に，同じ監視項目で再度異常検知と判断した場合に通知を行うかどうかを設定します。 検知中に同じ監視項目で再度通知する必要が無い場合は，本項目をチェックしてください。同じ監視項目で検知中に関わらず毎回通知を行いたい場合はチェックを外してください。
プロセス数	外部データ監視に使用するプロセスの数を設定します。 監視対象とする項目数が多い場合，プロセス数を調整することで性能を改善できる場合があります。 システムのリソース（CPU，メモリ）に余裕がある場合にのみ変更ください。
タイムアウト時間（秒）	外部データ情報のデータ集計において，応答受信するまでのタイムアウト時間を設定します。
外部データ収集	外部データの収集を行う場合はチェックします。

項目	説明
外部データ抽入 API 設定登録	外部データ抽入 API で，未登録の外部データ受信時に，外部データ設定を登録する場合はチェックします。
監視データ集計	外部データ監視項目で監視データの集計を行う場合はチェックします。
閾値監視	外部データ監視項目で閾値監視を行う場合はチェックします。
Impulse 連携	外部データ監視項目で Impulse 連携を行う場合はチェックします。
Email 通知	外部データ監視項目の閾値監視／Impulse 連携監視で異常，または復旧の検知時に，Email 通知の送信を行う場合はチェックします。
Trap 通知	外部データ監視項目の閾値監視／Impulse 連携監視で異常，または復旧の検知時に，SNMP Trap 通知の送信を行う場合はチェックします。
Syslog 通知	外部データ監視項目の閾値監視／Impulse 連携監視で異常，または復旧の検知時に，Syslog の送信を行う場合はチェックします。

項目	説明
Syslog メッセージ	以下に示すイベント発生時に送信する syslog のメッセージフォーマットを登録します。最大 1024 文字登録できます。 ・閾値監視 異常検知 ・閾値監視 復旧検知 ・Impulse 連携 異常検知 ・Impulse 連携 復旧検知 Syslog メッセージには，任意の文字，および予約語を指定します。予約語は syslog 送信時に適切な値に変換して送信されます。予約語はプルダウンから選択することで，入力欄の最後尾に追加されます。また，プルダウンから CEF フォーマットのヘッダ部分を入力することができます。 プルダウンから入力可能な予約語およびフォーマットを次に示します。 ・監視対象 {$MONITORING.TYPE} ・監視種別 {$MONITORING.OBJECT} ・異常検知時刻 {$DETECTED.DATETIME} ・復旧検知時刻 {$RECOVERED.DATETIME} ・監視項目名称 {$ITEM.NAME} ・データセット名 {$ITEM.DATASET} ・監視データ名 {$DATA.NAME} ・メトリクス名 {$DATA.METRICS} ・閾値種別 {$THRESHOLD.TYPE} ・閾値 {$THRESHOLD.VALUE} ・監視値 {$MONITORING.VALUE} ・機械学習の特性 {$IMPULSE.CHARACTERISTIC} ・機械学習の検知要件 {$IMPULSE.REQUIREMENT} ・通知詳細の URL {$URL} ・説明 {$DESCRIPTION} ・アクション {$ACTION} ・優先度 {$PRIORITY} ・優先度ラベル {$PRIORITY.LABEL} ・付加情報１ {$ADDITIONAL1} ・付加情報２ {$ADDITIONAL2} ・付加情報３ {$ADDITIONAL3} ・CEF フォーマットヘッダー
収集周期	外部データ監視を行う周期を選択します。
オフセット時間（秒）	各周期の監視開始タイミングのオフセット時間を設定します。 本オフセット時間を設定することにより，外部サーバなどから送信される当該周期の外部データをすべて受信してから対象外部データの監視が可能になります。
タイムスタンプ	収集周期毎に監視データに紐付ける監視時刻として，周期の先頭時刻か周期の最終時刻かを選択します。

（6） 過去データ生成

過去データ生成の概要を次に示します。

表 5-61　過去データ生成・削除の概要

項目	説明
監視データ生成	監視データ生成の条件を登録します。 登録項目を次に示します。 ・外部データ監視項目：設定済の外部データ監視項目から，監視データ生成の対象を選択します。 ・期間：開始日と終了日で，監視データ生成の対象期間を指定します。 ・監視データ生成：指定した条件の監視データ生成を登録します。待機中，生成中または停止中の監視データ生成で，監視項目が同じ，かつ期間が重複するものが他にある場合は，登録できません。
監視データ削除	監視データ削除の条件を登録します。 登録項目を次に示します。 ・外部データ監視項目：設定済の外部データ監視項目から，監視データ削除の対象を選択します。 ・期間：開始日と終了日で，監視データ削除の対象期間を指定します。 ・監視データ削除：指定した条件の監視データ削除を登録します。
選択履歴の削除	選択した履歴を削除します。 状態が待機中，生成完了，削除完了，異常終了および生成停止の場合のみ削除できます。
監視項目カテゴリ名	監視データ生成／削除対象の監視項目カテゴリ名を表示します。
監視項目データ名	監視データ生成／削除対象の監視項目データ名を表示します。
開始期間	監視データ生成／削除対象期間の開始日時を表示します。
終了期間	監視データ生成／削除対象期間の終了日時を表示します。
処理開始時間	監視データ生成／削除処理を開始した日時を表示します。
処理終了時間	監視データ生成／削除処理を終了した日時を表示します。
状態	監視データ生成状態（待機中／生成中／生成完了／削除完了／異常終了／停止中／生成停止）を表示します。
詳細	対象の外部監視項目毎 監視データ詳細画面を表示します。
停止	監視データ生成を途中停止します。 なお，監視データ生成は即座には停止せず，停止中を経由して，最終的に生成停止となります。 状態が生成中の場合のみ停止できます。
再開	停止中の監視データ生成を再開します。 状態が停止中の場合のみ再開できます。

5.5.5　Impulse 連携

Impulse 連携に関する各種情報を表示します。

（1） Impulse 接続

Impulse 連携設定 Impulse 接続の概要を次に示します。

表 5-62 Impulse 連携設定 Impulse 接続の概要

項目	説明
新規登録	Impulse 連携の設定を最大 4 つまで登録します。 設定先 IP アドレス，設定先ポート番号は全ての設定が同時に有効となります。参照先 IP アドレス，参照先ポート番号，通知集約は最上位に表示される設定のみ有効となります。
変更	Impulse 設定の登録内容を変更します。
削除	登録内容を削除します。
Impulse 設定	Impulse 設定の登録内容を表示します。
設定/参照先 IP アドレス	Impulse が動作しているサーバの IP アドレスを登録してください。 本項目で登録した IP アドレスは，Impulse への学習情報の注入で使用します。また，参照先 IP アドレスが未設定の場合は，Impulse への外部リンク等でも使用します。
設定先ポート番号	Impulse への学習情報の注入に使用する，Impulse の公開ポートを登録します。
参照先 IP アドレス	Impulse が動作しているサーバの IP アドレスを登録してください。本項目で登録した IP アドレスは， Impulse への外部リンク等で使用します。 本項目は省略可能です。省略した場合は，設定/参照先 IP アドレスに登録した IP アドレスを使用します。
参照先ポート番号	Impulse の Web インタフェースにアクセスする際に使用する Impulse の公開ポートを登録します。
通知集約	Impulse 連携において，異常検知中に，同じ条件で再度異常検知と判断した場合に，AX-Collector で通知を行うかどうかを設定します。 検知中に同じ条件で再度通知する必要が無い場合は，本項目をチェックしてください。同じ条件で検知中に関わらず毎回通知を行いたい場合はチェックを外してください。

（2） syslog/trap 送信制御状態一覧

Impulse syslog/trap 送信制御状態一覧の概要および詳細を次に示します。

表 5-63 Impulse syslog/trap 送信制御機能状態一覧の概要

項目	説明
Impulse syslog/trap 送信制御状態一覧	Impulse syslog/trap 送信制御機能の制御状態の一覧を表示します。
削除	Impulse syslog/trap 送信制御機能の制御状態を削除し，制御を終了します。
選択状態の削除	選択した Impulse syslog/trap 送信制御機能の制御状態を削除し，制御を終了します。

項目	説明
検索	表示した制御状態一覧を対象に検索し，一致したものを表示します。

表 5-64　Impulse syslog/trap 送信制御機能状態一覧の詳細

項目	説明
ID	制御状態毎に付与される ID を表示します。
監視項目カテゴリ	Impulse 連携により異常を検知した監視項目のカテゴリ名を表示します。
監視項目名	Impulse 連携により異常を検知した監視項目名を表示します。
監視データ	Impulse 連携により異常を検知した監視項目内の MIB オブジェクトグループ名，フロー条件グループ名，または外部監視データのカテゴリ名およびデータ名を表示します。
特性	異常を検知した特性分析を表示します。
検知要件	異常を検知した検知要件を表示します。
状態	最後に検知した検知状況，および syslog/trap の通知状況を表示します。 ・検知中　　：異常を検知済みの状態です。 ・復旧済み　：異常復旧を検知済みで，異常復旧検知の syslog/trap を送信済みの状態です。(※1) ・復旧保留中：異常復旧を検知済みで，異常復旧検知の syslog/trap を送信抑止中の状態です。
異常検知回数	制御を開始してから異常を検知した回数を表示します。
送信回数	異常検知の syslog/trap 送信を実施した回数を表示します。(※1)
復旧検知回数	制御を開始してから復旧を検知した回数を表示します。
送信回数	復旧検知の syslog/trap 送信を実施した回数を表示します。(※1)
初回検知日時	制御開始の契機となった異常を検知した日時を表示します。
経過時間	初回検知からの経過時間を表示します。
最終検知日時	制御期間内に最後に異常を検知した日時を表示します。
経過時間	最終検知からの経過時間を表示します。
制御	使用している制御単位時間を表示します。 ・第 1：第 1 制御単位時間を使用する場合に表示します。 ・第 2：第 2 制御単位時間を使用する場合に表示します。
延長理由	最後に制御期間を延長した際の延長理由を表示します。 ・-(ハイフン)：延長していない場合に表示します。 ・移行　　：第 2 制御移行時間が経過したことによる延長，又は制御期間が無期限の場合に表示します。 ・検知　　：Impulse 連携通知受信による延長の場合に表示します。 ・閾値　　：閾値連携による延長の場合に表示します。
期間延長日時	Impulse 連携通知受信，閾値連携または第 2 制御移行時間が経過したことによって制御期間を延長した日時を表示します。 延長していない場合は，-(ハイフン)を表示します。
終了予定日時	今後延長が発生しない場合の，制御期間の終了予定日時を表示します。 制御期間が無期限の場合は”無期限”を表示します。

※1. データ監視設定や syslog 通知先，trap 通知先等の設定により，実際には syslog/trap を送信しなかった場合でも，Impulse syslog/trap 送信制御機能により抑止を行わなかった場合は送信を実施した回数としてカウントします。

（3） syslog/trap 送信制御設定

Impulse syslog/trap 送信制御設定の概要を次に示します。

表 5-65 Impulse syslog/trap 送信制御設定の概要

項目	説明
登録	Impulse syslog/trap 送信制御機能の動作設定を登録します。
変更	Impulse syslog/trap 送信制御設定の登録内容を変更します。
削除	登録内容を削除します。
Impulse syslog/trap 送信制御設定	Impulse syslog/trap 送信制御設定の登録内容を表示します。
送信制御機能	Impulse syslog/trap 送信制御機能を有効にする場合はチェックします。
最大送信回数判定通知	制御期間内で syslog/trap 送信を行う最大回数を判定する通知の種別を指定します。 異常検知，または復旧検知を指定します。
最大送信回数	最大送信回数判定通知を制御期間内で syslog/trap 送信を行う最大回数を登録します。 設定できる値の範囲は 1～144 回です。
第 1 制御単位時間(分)	Impulse 異常検知後，Impulse syslog/trap 送信制御機能が動作する制御単位時間(分)を登録します。 設定できる値の範囲は 1～10080 分です。
制御期間延長オプション Impulse 連携通知受信	制御期間内に Impulse 異常検知が発生した場合，その時点から制御期間を単位時間延長する延長オプションを有効にする場合はチェックします。
制御期間延長オプション 閾値連携	制御期間終了時に監視対象の値が閾値外だと，その時点から制御期間を単位時間延長する延長オプションを有効にする場合はチェックします。
制御期間延長オプション 第 2 制御移行時間(分)	第 1 制御時間による制御期間が継続した場合に，第 2 制御単位時間による制御に切り替わる時間を登録します。 設定できる値の範囲は 0～10080 分です。 0 を設定した場合は，第 2 制御単位時間への切り替えを行いません。
制御期間延長オプション 第 2 制御単位時間(分)	第 2 制御に移行した後の，第 2 段階目の制御単位時間を登録します。 設定できる値の範囲は 0～10080 分です。 本設定に 0 を登録すると，第 2 制御移行時間を経過した後の制御期間は無期限となり，オペレーションにより制御状態を解除（削除）しない限り，Impulse syslog/trap 送信制御機能による制御を継続します。

（4） Impulse

Impulse 管理画面への外部リンクです。

Impulse 接続で正しい Impulse の IP アドレスと参照先ポート番号を登録した上で使用してください。

5.6 管理・設定

5.6.1 可視化エイリアス情報

可視化エイリアス情報では，VLAN-ID，VLAN(QinQ)，MAC アドレス，IPv4 アドレス，IPv4 ネットワーク，IPv6 アドレス，IPv6 ネットワーク，センサ・ポート，イーサタイプ，プロトコル番号，L4 ポート番号に関するエイリアス情報を登録します。

ここで登録したエイリアス情報はダッシュボードやフローランキングリストなどに反映されます。

また，イーサタイプ／プロトコル番号／L4 ポート番号については，本製品にデフォルトのエイリアスが組み込まれています。デフォルトのエイリアスは，ここで登録したエイリアス情報で書き換えることができます。

管理・設定 可視化エイリアス情報の概要を次に示します。

表 5-66 管理・設定 可視化エイリアス情報の概要

項目	説明
エイリアス情報	登録したエイリアス情報をリスト形式で表示します。
検索フィールド	表示したエイリアス情報の全フィールド，または特定のフィールドを対象に検索し，一致したものを表示します。
追加 ※1	エイリアス情報を新規に追加します。
削除 ※1	選択したエイリアス情報を削除します。
保存 ※1	登録済みのエイリアス情報の各項目を選択・ダブルクリックで編集した場合に，その編集内容を保存します。
インポート(CSV) ※1	エクスポート(CSV)で作成した CSV 形式のファイルをアップロードして，エイリアス情報を登録します。
エクスポート(CSV)	エイリアス情報を CSV 形式のファイルとしてダウンロードします。ファイル名は以下となります。 ・VLAN-ID : 「vlan_alias_list_＜*日付*>.csv」 ・VLAN(QinQ) : 「vlanqinq_alias_list_＜*日付*>.csv」 ・MAC アドレス : 「mac_alias_list_＜*日付*>.csv」 ・IPv4 アドレス : 「ipv4_alias_list_＜*日付*>.csv」 ・IPv4 ネットワーク : 「ipv4network_alias_list_＜*日付*>.csv」 ・IPv6 アドレス : 「ipv6_alias_list_＜日付>.csv」 ・IPv6 ネットワーク : 「ipv6network_alias_list_＜日付＞.csv」 ・センサ・ポート : 「sensorport_alias_list_＜*日付*>.csv」 ・イーサタイプ : 「＜*表示形式*＞_ethertype_alias_list_＜*日付*>.csv」 ・プロトコル番号 : 「＜*表示形式*＞*_protocol*_alias_list_＜*日付*>.csv」 ・L4 ポート番号 : 「＜*表示形式*＞*_l4port*_alias_list_＜*日付*＞.csv」

項目	説明
表示形式	イーサタイプ／プロトコル番号／L4 ポート番号のエイリアス情報について，以下の形式で表示を切り替えます。 ・デフォルト 本製品のデフォルトのエイリアス情報を表示します。 ・登録 運用者が登録したエイリアス情報を表示します。 ・マージ（デフォルト＋登録） 上記「デフォルト」と「登録」をマージしたエイリアス情報を表示します。
拡張設定※2	・IPv4/IPv6 エイリアス補完 IP ネットワークエイリアス情報のエイリアスを IP アドレスエイリアスとして補完使用する動作の有効化設定です。有効化した場合，IP アドレスエイリアスを表示する画面において，エイリアス情報が存在しない場合，IP ネットワークエイリアスを検索します。該当ネットワーク情報が存在する場合に，ネットワークエイリアス情報を IP アドレスエイリアス情報として表示します。 ・デフォルト：無効

注※1

イーサタイプ／プロトコル番号／L4 ポート番号のエイリアス情報については，表示形式が登録の場合のみ，ボタンが表示され，操作が可能となります。

注※2

IPv4 ネットワークエイリアス，IPv6 ネットワークエイリアス画面でのみ表示され，操作が可能となります。有効化時，IPv4 アドレスエイリアス，IPv6 アドレスエイリアスの画面に有効化設定情報が表示（！）されます。

5.6.2 レポート

レポート出力に関わる設定，および出力したレポートの参照を行います。

（1） レポート一覧

出力したレポートの参照を行います。レポート一覧の概要を次に示します。

表 5-67 レポート一覧の概要

項目	説明
レポート一覧	出力したレポートを終了時間順に表示します。
表示期間設定	表示するレポートの範囲を開始時間で指定します。
HTML1	生成したレポートをナビゲーションバーと共に表示します。

項目	説明
HTML2	生成したレポートのみを表示します。ナビゲーションバーは表示しません。
レポート設定詳細	レポート設定の詳細を表示します。
削除	レポートを削除します。
レポートの削除	選択したレポートを削除します。
検索	表示した一覧情報を対象に検索し，一致したものを表示します。

（2） レポート設定

レポートの出力設定を行います。レポート設定の概要を次に示します。

表 5-68 レポート設定の概要

項目	説明
新規登録	レポート出力を行う条件を登録します。指定可能な条件を次に示します。 ・名前 ：任意の名前を登録します。最大 256 文字登録可能です。 ・レポート期間：レポート生成する期間を指定します。日間，週間，月間の何れかを指定します。 ・カスタマイズダッシュボート：出力するレポートの内容を，設定済みのカスタマイズダッシュボードから選択します。ここで選択したカスタマイズダッシュボードの内容を，レポート期間で指定した周期毎に，レポートとして出力します。
レポート設定一覧	登録したレポート設定の一覧を表示します。
詳細	登録内容の詳細を表示します。
変更	登録内容を変更します。
削除	登録内容を削除します。
収集レポート一覧	出力したレポート一覧を表示します。

5.6.3 コレクタ接続環境

AX-Collector の接続環境に関する設定を行います。

（1） コレクタ

コレクタ接続環境 コレクタの概要を次に示します。

表 5-69　コレクタ接続環境 コレクタの概要

項目	説明
登録	コレクタ設定を登録します。
変更	コレクタ設定の登録内容を変更します。
削除	登録内容を削除します。
コレクタ設定	コレクタ設定の登録内容を表示します。
参照先スキーム名	AX-Collector にアクセスする際のスキーム名を登録してください。
参照先 IP アドレス	AX-Collector を動作させるサーバの IP アドレスを登録してください。 本項目で登録した IP アドレスは，syslog メッセージ内の AX-Collector 参照先への URL に使用します。
参照先ポート番号	AX-Collector のインストール時に設定した，AX-Collector の公開ポート番号を登録してください。
ホスト名	AX-Collector が動作しているホスト名を登録します。最大 63 文字登録可能です。登録したホスト名は，ナビゲーションバーに表示します。
アラート表示時間（分）	閾値監視通知および Impulse 連携通知の発生件数をナビゲーションバーにバッジ表示するにあたり，対象とする時間を登録します。画面表示時刻から，登録した時間分を過去に遡り，その間に発生した件数を表示します。 登録可能な値の範囲は 0～1440 分です。 当該時間に 0 分を指定すると，バッジ表示を行いません。
検知通知 保存上限	検知通知を保存する上限件数を指定します。 閾値検知(SNMP)，閾値検知(フロー)，閾値監視(外部データ)および Impulse 連携をそれぞれ別に件数カウントします。 上限を超えた検知通知は毎日 AM3:30 に検知日時の古いものから削除されます。 設定範囲　：0～65,535 件 　0 件　　：検知通知を削除しません。 　1～65,535 件：設定件数を超えた検知通知を削除します。 デフォルト：10,000 件
運用ログ 保存上限	運用ログを保存する上限件数を指定します。 上限を超えた運用ログは毎日 AM3:30 に日時の古いものから削除されます。 設定範囲　：0～65,535 件 　0 件　　：運用ログを削除しません。 　1～65,535 件：設定件数を超えた運用ログを削除します。 デフォルト：10,000 件
TOP ページ	ユーザ管理で TOP ページ設定が未指定のユーザがログインした場合に，TOP ページとして表示する画面を登録します。 設定対象はデフォルト，カスタマイズダッシュボード詳細，ブックマーク一覧，検知数カレンダーです。 デフォルトを選択した場合はコレクタ稼働状況を表示します。カスタマイズダッシュボード詳細を選択した場合は，設定済のカスタマイズダッシュボードから表示対象を登録します。

項目	説明
メニュー表示位置	メニュー位置を設定します。 トップ：画面上部のナビゲーションバーにプルダウンの機能メニューを表示します。 左サイド：画面左に階層化されたサイドメニューを表示します。設定時，左上に表示されるアイコン操作でメニュー表示・非表示を切り替えます。 デフォルト：トップ
フォントサイズ	画面描画に使用する基本フォントサイズを指定します。 設定値：最小，小，標準，大，最大 デフォルト：小

（2） Syslog 通知先

コレクタ接続環境 Syslog 通知先の概要を次に示します。

表 5-70 コレクタ接続環境 Syslog 通知先の概要

項目	説明
新規登録	syslog 通知先を新規に登録します。
テスト送信	登録した syslog 通知先に対して，テスト用の syslog を送信します。
IP アドレス	syslog 通知時の宛先 IP アドレスを登録します。
ポート番号	syslog 通知時の宛先ポート番号を登録します。
ファシリティ	syslog 通知時のファシリティを選択します。
Syslog 通知先一覧	登録した syslog 通知先の一覧を表示します。
変更	syslog 通知先の登録内容を変更します。
削除	登録内容を削除します。

（3） Email 通知先

コレクタ接続環境 Email 通知先の概要を次に示します。

表 5-71 コレクタ接続環境 Email 通知先の概要

項目	説明
新規登録	Email 通知先を新規に登録します。
送信間隔変更	Email の送信間隔を指定します。 前回の送信時からの更新された送信情報がある場合，登録された SMTP サーバに接続し E-mail を送信します。 ・設定間隔：1 分/5 分/10 分/1 時間/3 時間/12 時間/1 日 ・デフォルト：5 分
テスト送信	登録した Email 通知先に対して，テスト用の Email を送信します。
有効	該当通知先の Email 送信動作の有効化を行います。 ・デフォルト：有効
通知先名称	Email 通知先の名称を指定します。
メールサーバ情報	SMTP サーバの IPv4 または IPv6 アドレスを指定します。

項目	説明
暗号化種別	SMTP サーバの暗号化種別を以下から選択し指定します。 ・なし（SMTP） ・SMTP STARTTLS ・SSL（SMTPS）
通知先ポート番号	SMTP サーバのポート番号を指定します。 ・デフォルト値は暗号化種別によって異なります。 25　暗号化種別：なし（SMTP） 587 暗号化種別：SMTP STARTTLS 465 暗号化種別：SSL（SMTPS）
認証	SMTP サーバのユーザ認証を指定します。 有効化時，認証ユーザ名と認証パスワードを指定します。
宛先メールアドレス（to）	宛先メールアドレスを指定します。 to/cc/bcc でそれぞれ最大 5 件の宛先を指定可能です。 複数指定時は,メールアドレス間をダブルクオーテーションで区切って指定してください。
宛先メールアドレス（cc）	
宛先メールアドレス（bcc）	
差出人メールアドレス(from)	差出人メールアドレスを指定します。
定型文	メールアドレス本文先頭に記載する定型文を指定します。
Email 通知先一覧	登録した syslog 通知先の一覧を表示します。
詳細	Email 通知先の登録内容を表示します。
変更	Email 通知先の登録内容を変更します。
削除	登録内容を削除します。

Email 通知内容は次の通りです。送信間隔毎に，前回送信以降に変化のあった検知情報を本文に記載し通知します。

5-72　Email 通知内容

送信契機	送信内容	説明
通常 メール	Subject: AX-Collector 検知情報 <ユーザ定義の定型文> ・送信元コレクタ名称：<送信元コレクタ名称> ・通知先名称：<通知先名称> ・送信日時：<送信日時> ・検知/復旧通知件数 <検知/復旧通知件数> ・検知一覧	・送信元コレクタ名称 コレクタ名称設定時，コレクタ設定の参照先へリンクとして表示 ・検知/復旧通知件数 優先度(Critical 等)毎の検知数/復旧数 ・検知一覧 検知通知対象の監視項目の一覧。優先度の高い順に表示。”詳細”は該当検知通知画面へのリンク。最大 100 件。

テスト メール	Subject：AX-Collector 接続テスト 送信元コレクタ名称：<コレクタ名称> 通知先名称：<通知先名称> 送信日時：<送信日時>	

（4） Trap 通知先

コレクタ接続環境 Trap 通知先の概要を次に示します。

表 5-73 コレクタ接続環境 Trap 通知先の概要

項目	説明
新規登録	Trap 通知先を新規に登録します。
IP アドレス	Trap 通知時の宛先 IP アドレスを登録します。
ポート番号	Trap 通知時の宛先ポート番号を登録します。
コミュニティ	Trap 通知時のコミュニティ名称を登録します。 最大 255 文字登録可能です。
Trap 通知先一覧	登録した Trap 通知先の一覧を表示します。
変更	Trap 通知先の登録内容を変更します。
削除	登録内容を削除します。

（5） AX-NM 連携環境設定

コレクタ接続環境 AX-NM 連携環境設定の概要を次に示します。

表 5-74 コレクタ接続環境 AX-NM 連携環境設定の概要

項目	説明
変更	AX-NM 連携環境設定の登録内容を変更します。
AX-NM 連携機能	AX-NM 連携機能を有効にする場合はチェックします。 AX-NM 連携機能を有効にして，AX-NM トークンを設定することで，AX-NM から取得した端末接続履歴を表示することが可能となります。
URL スキーム	AX-NM にアクセスする際のスキームを登録してください。
IP アドレス	AX-NM にアクセスする際の IP アドレスを登録してください。
ポート番号	AX-NM にアクセスする際のポート番号を登録してください。
トークン登録	AX-NM で発行した認証トークンを登録します。 AX-NM 連携環境設定を正しく登録し，AX-NM との通信が可能な状態で登録を行うと，自動でトークン期限を取得します。
トークン更新	登録済の認証トークンを更新します。
トークン削除	登録済の認証トークンを更新します。
AX-NM トークン	AX-NM で発行した認証トークンの設定状態を表示します。

項目	説明
トークン期限	AX-NM 連携環境設定を正しく登録し，AX-NM との通信が可能な状態で認証トークンの登録，更新を行うと，自動的にトークンの有効期限を表示します。
検索タイムアウト時間(秒)	AX-NM から端末情報を取得する際の応答待ち最大時間（秒）を設定します。 設定範囲：1～600 デフォルト：30

（6） Syslog 受信設定

コレクタ接続環境 Syslog 受信設定の概要を次に示します。本画面は，Syslog 受信設定情報の表示のみとなります。設定はコマンドラインで実施します。「4.9Syslog 受信機能の設定」を参照してください。

表 5-75 コレクタ接続環境 Syslog 受信設定の概要

項目	説明
Syslog 受信設定	・状態 ：Syslog 受信動作の状態を表示します。 停止中/初期化中/稼働中/障害中 ・ポート番号 ：Syslog 受信ポート番号 ・プロトコル ：UDP ・プロセス数 ：受信プロセス数
ユーザ定義フィールド・コレクタ表示名	・データフィールド名 ：logext01～logext10 ・コレクタ表示名 ：*ユーザ定義 1～10

5.6.4 冗長

AX-Collector の冗長化機能に関する設定を行います。

（1） 概況

冗長状態の概要を表示します。

表 5-76 冗長概況の概要

項目	説明
冗長状態	冗長状態を表示します。 初期化中／二重化運用／一重化運用／非運用中
自系状態	自系コレクタの系状態を表示します。 初期化中／運用系／待機系／系切り替え中／非運用中

項目	説明
他系状態	他系コレクタの系状態を表示します。 初期化中／運用系／待機系／系切り替え中／非運用中
他系 IP アドレス	他系の監視に使用中の IP アドレスを表示します。
動作設定	（3）動作設定による設定内容を表示します。

（2） 系切り替え

手動でのコレクタ系切り替えを行います。切り替えは運用系コレクタから二重化運用状態時のみ実行可能です。

（3） 動作設定

表 5-77 冗長動作設定の概要

項目	説明
冗長	冗長化機能を有効化します。
自系優先	起動時優先的に運用系とするコレクタ側で有効に設定します。 起動時優先的に待機系とするコレクタ側で無効に設定します。
ヘルスチェック周期	冗長構成の対向コレクタ，Impulse，仮想 IP アドレスの監視周期です。
IP アドレス構成	冗長化機能で使用する IP アドレスの構成を設定します。 ・実 IP アドレス 仮想 IP アドレスを使用しません ・仮想 IP アドレス 仮想 IP アドレスが自ノードに割り当てられているか監視し，冗長切り替え条件に加えます。また，仮想 IP アドレスを syslog/trap の送信元 IP アドレスとします。 ・仮想 IP アドレス（通知のみ） 仮想 IP アドレスを syslog/trap の送信元 IP アドレスとしてのみ使用します。
仮想 IP アドレス	IP アドレス構成設定が“仮想 IP アドレス”または“仮想 IP アドレス（通知のみ）”の場合に使用する仮想 IP アドレスを設定します。
他系スキーム名	冗長構成の対向コレクタの監視およびデータ同期に使用する接続スキーム(HTTP/ HTTPS)を設定します。WEB インタフェースと同じスキーム設定にします。

項目	説明
他系 IP アドレス 1～5	冗長構成の対向コレクタの監視およびデータ同期に使用する対向コレクタの IPv4 アドレスを設定します。対向コレクタのノード上に付与された IP アドレスを最大 5 つ設定可能です。数字の若番での接続に失敗する場合に，順番に 2～5 のアドレスで接続を試みます。
他系ポート番号	冗長構成の対向コレクタの監視およびデータ同期に使用する接続スキーム(HTTP/ HTTPS)のポート番号を設定します。WEB インタフェースと同じポート番号にします。

5.6.5 管理

AX-Collector の管理機能に関する設定を行います。

（1） コレクタ稼働状況

AX-Collector の稼働状況に関する情報を表示します。

コレクタ稼働状況の概要を次に示します。

表 5-78 コレクタ稼働状況の概要

項目	説明
フロー受信状況	直近 5 分間の Netflow パケットの平均フローレコード受信数，および最新 1 週間の Netflow パケットの平均フローレコード受信数の時系列グラフを表示します。
データ監視状況	SNMP 監視，フロー監視，外部データ監視における，各監視周期毎の設定数，および収集有効設定数を表示します。

（2） データ管理

管理 データ管理の概要を次に示します。

表 5-79 管理 データ管理の概要

項目	説明
データストア情報	AX-Collector では受信したフロー情報，取得した MIB 情報および外部データ情報等を 1 日単位にインデックスを付けて管理します。本項目では，次の情報を表示します。 ・総インデックス数：保存しているインデックスの総数 ・総ドキュメント数：保存しているインデックスに含まれるすべてのドキュメント(受信したフロー情報，取得した MIB 情報および外部データ情報)の総数 ・全ディスクサイズ：データ(インデックス)の保存に使用可能なディスクサイズ

項目	説明
	・DB 使用ディスクサイズ：受信したフロー情報や各監視データの保存に使用しているディスクサイズの合計および，全ディスクサイズに対する割合 ・フロー情報　：受信したフロー情報の保存に使用しているディスクサイズの合計および，全ディスクサイズに対する割合 ・MIB 情報　：SNMP 監視において収集した MIB 収集データと，生成した SNMP 監視データの保存に使用しているディスクサイズの合計および，全ディスクサイズに対する割合 ・フロー監視　：フロー監視において生成したフロー監視データの保存に使用しているディスクサイズの合計および，全ディスクサイズに対する割合 ・フローランキング監視：フローランキング監視において生成したフローランキング監視データの保存に使用しているディスクサイズの合計および，全ディスクサイズに対する割合 ・外部データ監視　：外部データ監視において収集した外部収集データと，生成した外部監視データの保存に使用しているディスクサイズの合計および，全ディスクサイズに対する割合 ・ロギング情報　：受信した Syslog 情報の保存に使用しているディスクサイズの合計および，全ディスクサイズに対する割合 ・管理データ　：フロー情報および監視データ以外で DB に保存している管理データのディスクサイズの合計および，全ディスクサイズに対する割合 ・他使用ディスクサイズ：DB 以外で使用しているディスクサイズの合計および，全ディスクサイズに対する割合 ・空きディスクサイズ：未使用のディスクサイズおよび，全ディスクサイズに対する割合 ・容量監視閾値　：データストア設定の容量監視で設定した閾値

項目	説明
データストア設定	データ（インデックス）の蓄積・保存に関して，次の項目を設定します。 ・定期削除　：有効に設定した場合，期間監視および容量監視の設定情報に基づき，データを定期的に削除します。 ・期間監視　：保存期間経過データは削除します。データ種別毎にデータを保存する期間を指定します。指定可能な値の範囲は 1～3650 日です。※1 ・容量監視　：保存しているデータのディスク使用率が閾値を超えた場合，日付の古いデータを削除します。閾値，およびデータ種別毎に削除対象か否かを指定します。指定可能な値の範囲は 1～99%です。※2 ・削除タイミング：定期的に削除する時刻を指定します。 初期設定では，定期削除が有効で，180 日以上経過したインデックス，あるいはデータのディスク使用率が 75%超過時に日付の古いインデックスを，定期的に毎朝 5 時に削除します。削除したくないインデックスはスナップショットを作成してください。 ・アラートメッセージ表示：有効にした場合，1 日に蓄積する平均データ量から，あと何日分のデータが蓄積可能かを画面表示します。 ・平均データ量算出期間：アラートメッセージ表示で使用する，1 日の平均データ量を算出するための期間を開始日と終了日で指定します。
インデックス一覧	AX-Collector が管理しているインデックスの一覧を 1 日単位で表示します。
選択インデックスの削除	選択したインデックスを削除します。
選択インデックスのスナップショット作成	選択したインデックスのスナップショットを作成します。 スナップショットを作成することで，インデックスデータが削除された場合に，データを復元することができます。 作成したスナップショットは「スナップショット管理」で管理されます。
検索	表示した一覧情報を対象に検索し，一致したものを表示します。

※1. 各データ種別と，そこに含まれるインデックスを次に示します。

表 5-80　データ種別とインデックスの一覧

データ種別	インデックス	説明
フロー情報	ax-collector-flowdata-<日付>	受信したフロー情報
MIB 情報	ax-collector-orgdata-snmp-<日付>	SNMP 監視において収集した MIB 収集データ
	ax-collector-snmp-<日付>	SNMP 監視において生成した SNMP 監視データ

データ種別	インデックス	説明
フロー監視	ax-collector-flow-<日付>	フロー監視において生成したフロー監視データ
	ax-collector-subdivision-flow-<日付>	フロー監視において生成した細分化データ
フローランキング監視	ax-collector-flow-monitoring-<日付>	フローランキング監視において生成したフローランキング監視データ
外部データ監視	ax-collector-orgdata-external-<日付>	外部データ監視において収集した外部収集データ
	ax-collector-monitoring-<日付>	外部データ監視において生成した外部監視データ
	ax-collector-period-external-<日付>	外部データ監視において生成した細分化データ
ロギング情報	ax-collector-logging-<日付>	受信した Syslog 情報

※2. 容量監視において特定のデータ種別を指定した場合，全体の使用率が閾値を超えた場合に，削除対象のデータのみを削除します。なお，削除対象のデータであっても，全体の 1%は削除を行いません。

（3） スナップショット管理

管理 スナップショット管理の概要を次に示します。

表 5-81 管理 スナップショット管理の概要

項目	説明
スナップショット一覧	作成したスナップショットの一覧を表示します。
選択スナップショットの削除	選択したスナップショットを削除します。
選択スナップショットの復元	選択したスナップショットから，インデックスデータを復元します。
検索	表示した一覧情報を対象に検索し，一致したものを表示します。

（4） ユーザ管理

管理 ユーザ管理の概要を次に示します。

表 5-82 管理 ユーザ管理の概要

項目	説明
ユーザ一覧	作成したユーザの一覧を表示します。
新規登録	AX-Collector にログインするためのユーザを新規に登録します。 ・ユーザ名： ユーザ名を入力します。 最大 128 文字登録可能です。使用できる文字は英数字，ハイフン(-)，アンダーバー(_)，ピリオド(.)，プラス(+)，アットマーク(@)です。 ・パスワード： パスワードを入力します。 最大 128 文字登録可能です。使用できる文字は英数字と記号です。パスワードには英大文字，英小文字，数字，記号を全て含む 10 文字以上の文字列を指定してください。 ・ユーザ権限： 管理者，標準ユーザ，参照ユーザの何れかを選択します。各ユーザ権限のアクセス範囲は，ユーザ権限毎のアクセス範囲を参照してください。 ・カスタム権限： カスタム権限で登録した権限を指定します。 ・TOP ページ： 該当のユーザがログインした場合に TOP ページとして表示する画面を登録します。設定対象はデフォルト，カスタマイズダッシュボード詳細，ブックマーク一覧，検知数カレンダー，未指定です。 デフォルトを選択した場合はコレクタ稼働状況を表示します。カスタマイズダッシュボード詳細を選択した場合は，設定済のカスタマイズダッシュボードから表示対象を登録します。未指定を選択した場合は，コレクタ設定の TOP ページ設定が適用されます。 ・REST API： REST API で使用する認証方式を指定します。 ・トークン認証 トークン認証の使用可否を指定します。 発行するトークンの最長有効期間を無期限，もしくは 1～12 カ月から選択します。 ・ベーシック認証 ベーシック認証の使用可否を指定します。 ※上記ユーザ名／パスワードを認証に使用します。
ユーザー設定変更	ユーザ権限，カスタム権限，TOP ページおよび REST API の設定変更を行います。
パスワード変更	AX-Collector にログインしているユーザのパスワードを変更します。
ユーザ削除	選択したユーザを削除します。
認証トークン発行	REST API で使用する認証トークンの有効期間を選択し，トークンを発行します。 ※HTTP ヘッダに以下のようにトークンを設定し，認証を行ってください。 「Authorization: Bearer <トークン>」
認証トークン削除	認証トークンを削除します。

ユーザ権限毎のアクセス範囲を次に示します。

表 5-83　ユーザ権限毎のアクセス範囲

ユーザ権限	アクセス可能な機能	制限される機能
管理者	・全て可能です。	・制限はありません。
標準ユーザ	・全ての機能の参照 ・可視化機能や監視機能の設定・参照 ・ユーザアカウント, ライセンス関係以外の管理・設定関連操作 ・自ユーザのパスワード変更 ・syslog テスト送信	・運用ログの付加情報の表示 ・ユーザアカウント, ライセンスの管理・設定関連操作
参照ユーザ	・全ての機能の参照 ・自ユーザのパスワード変更	・全ての機能の登録，変更，削除 ・syslog テスト送信

（5）　カスタム権限

カスタム権限は特定の機能に対する権限を任意に組み合わせて，ユーザに設定することができる機能です。カスタム権限はユーザ権限と同時に設定することができ，カスタム権限で指定した機能についてはユーザ権限より優先して適用されます。カスタム権限で設定していない機能では，ユーザ権限が適用されます。

カスタム権限の概要を次に示します。

表 5-84　管理 カスタム権限の概要

項目	説明
カスタム権限一覧	作成したカスタム権限の一覧を表示します。
新規登録	カスタム権限を新規に登録します。 ・カスタム権限名：カスタム権限名を登録します。最大 256 文字登録可能です。 ・設定可能機能　：該当のカスタム権限において，登録・変更・削除が可能となる機能を登録します。
変更	カスタム権限の変更を行います。
削除	カスタム権限を削除します。 ユーザに設定済のカスタム権限を削除した場合，該当のユーザはカスタム権限未設定となります。

カスタム権限において設定可能な機能を次に示します。

表 5-85　管理 カスタム権限で指定可能な機能

機能名称
SNMP 監視項目 設定一覧（Syslog/Trap 通知設定変更）
フロー監視項目 設定一覧（Syslog/Trap 通知設定変更）
外部データ監視項目 設定一覧（Syslog/Trap 通知設定変更）

(6) ライセンス管理

管理 ライセンス管理の概要を次に示します。

表 5-86 管理 ライセンス管理の概要

項目	説明
ライセンス情報	現在有効になっているライセンス機能を表示します。 項目数が規定されているライセンスが登録されている場合，現在有効となっている項目数を表示します。
登録ライセンス一覧	AX-Collector に登録されているライセンスの一覧を表示します。 登録されているライセンスの有効期限や初年度ライセンスの識別番号などを表示します。
機能ライセンス登録	AX-Collector の各種サポート機能を有効化する機能ライセンス（初年度ライセンス）を登録します。 購入したライセンスキーを入力する際は，ハイフン有り，無しのどちらでも入力が可能です。
延長ライセンス登録	対象の機能ライセンスの有効期限を延長する，延長ライセンスを登録します。 延長ライセンスを登録することで，対象の機能ライセンスの有効期限が更新されます。
機能ライセンス削除	登録された機能ライセンスを削除します。 該当の機能ライセンスに延長ライセンスが設定されている場合は，延長ライセンスも同時に削除します。
延長ライセンス削除	登録された延長ライセンスを削除します。 延長ライセンスを削除することで，対象の機能ライセンスの有効期限が更新されます。

(7) フローデータ拡張

管理 フローデータ拡張の概要を次に示します。

表 5-87 管理 フローデータ拡張 データ拡張条件一覧の概要

項目	説明
データ拡張条件一覧	作成したデータ拡張条件の一覧を表示します。 データ拡張条件は 10 件まで登録可能です。

項目	説明
登録	データ拡張条件を新規に登録します。指定可能な条件を次に示します。 ・有効： 各データ拡張条件の有効/無効を登録します。有効の場合，フロー情報へ拡張データの追加を行います。 ・コレクタ表示名： 該当の拡張データの項目名を登録します。最大 32 文字登録でき，ここで登録した文字列の先頭にアスタリスクを追加した名称が，フローフィルタ等で表示されます。 ・検索フィールド： 拡張データのマッチング文字列と比較するフロー情報のフィールドを指定します。 ・一致種別： 検索フィールドをマッチング文字列と比較する際の一致種別を”完全一致”と”部分一致”から選択します。一致種別に部分一致を選択した場合は，マッチング文字列の先頭と最後にアスタリスクを指定することが出来ます。
変更	データ拡張条件を変更します。
削除	データ拡張条件を削除します。
拡張データ一覧	拡張データ一覧を表示します。
反映	登録したデータ拡張条件，および拡張データをコレクタ動作に反映します。

表 5-88　管理 フローデータ拡張 拡張データ一覧の概要

項目	説明
拡張データ一覧	該当のデータ拡張条件における拡張データの一覧を表示します。
新規登録	拡張データを新規に登録します。指定可能な条件を次に示します。 ・マッチング文字列： フローデータ拡張の検索フィールドで指定したフィールドの値と比較する文字列を登録します。最大 256 文字登録できます。 一致種別に部分一致を選択した場合は，マッチング文字列の先頭と最後にアスタリスクを指定することが出来ます。アスタリスクは 0 文字以上の任意の文字列と一致します。 イーサタイプや TCP フラグなど，数値情報が格納されるフィールドは 10 進数で指定してください。 IPv6 アドレスは，省略形で指定してください。 複数のマッチング文字列に一致する場合は，その何れかに一致します。どの条件に一致するかは未保障となります。 ・拡張文字列： フローデータ拡張の検索フィールドで指定したフィールドの値とマッチング文字列が一致した場合に，該当

項目	説明
	のフロー情報に拡張データとして追加する文字列を登録します。 最大 256 文字登録でき，半角の「& < > " ' ¥ = - ; ` / : * ? | ,」を除く文字を使用できます。
一覧ダウンロード（CSV）	該当のデータ拡張条件における拡張データの全情報を CSV 形式のファイルとしてダウンロードします。 ファイル名は「FE1_FlowDataExtension_<*拡張 ID*> _<*日付*>.csv」となります。
一括登録・更新	一覧ダウンロード(CSV)で作成した CSV 形式のファイルをアップロードして，拡張データを登録します。
全削除	該当のデータ拡張条件における拡張データを全て削除します。
変更	拡張データを変更します。
削除	拡張データを削除します。

表 5-89　管理 フローデータ拡張 GEOIP データ拡張条件一覧の概要

項目	説明
GEOIP データ拡張条件一覧	GEOIP データ拡張条件の一覧を表示します。
変更	GEOIP データ拡張条件の設定を変更します。指定可能な条件を次に示します。 ・有効： 各 GEOIP データ拡張条件の有効/無効を登録します。有効の場合，フロー情報へ GEOIP 拡張データの追加を行います。 ・GEOIP 名 GEOIP データ名称を表示します。 ・コレクタ表示名： 該当の GEOIP 拡張データの表示項目名を登録します。最大 32 文字登録でき，ここで登録した文字列の先頭にアスタリスクを追加した名称が，フローフィルタ等で表示されます。 ・検索フィールド： GEOIP 検索を実行するフロー情報のフィールドを指定します。指定可能なフィールドは，「4.10.3 プライベート MMDB 設定」を参照ください。
プライベート DB 設定	IPv4 ネットワークエイリアス情報,IPv6 ネットワークエイリアス情報を元に，プライベート MMDB を作成します。

表 5-90　管理 フローデータ拡張 プライベート DB 作成の概要

項目	説明
DB 情報	作成したプライベート MMDB 情報を表示します。 ・作成日時　　：作成した日時 ・IPv4 ネットワークエイリアス：作成時のエントリ数 ・IPv6 ネットワークエイリアス：作成時のエントリ数 ・対象データ　　：作成時に選択した作成対象 ・削除　　：DB を削除します。
DB 作成	プライベート MMDB を作成，適用します。 本機能の動作は「4.10.3 プライベート MMDB 設定」も参照ください。 ・作成元　　：作成元のエイリアス情報を指定します。 IPv4 ネットワークエイリアス IPv6 ネットワークエイリアス ・作成対象　　：対象データフィールドを指定します。 カッコ内は作成元エイリアスのフィールド情報です。 国　　（エイリアス） 国コード（コメント 1） 地域　　（コメント 2） 都市　　（コメント 3） 緯度-経度（コメント 4－コメント 5） AS 番号　（管理番号） AS 組織名（管理組織） ・作成　　：指定した条件でプライベート MMDB を作成し動作に適用します。

表 5-91　管理 フィールドフィルタ表示設定の概要

項目	説明
変更	フィールドフィルタ表示設定を変更します。
フィールドフィルタ表示設定	個別ビュー，フローランキングリスト，フロー監視等でフィルタ条件を指定するフィールドフィルタの各項目の表示・非表示を表示します。 なお，各機能において個別の表示/非表示が設定されている場合は，そちらの設定が優先されます。

(8)　ページリンク管理

管理 ページリンク管理の概要を次に示します。

表 5-92　管理 ページリンク管理の概要

項目	説明
新規登録	ページリンクを新規に登録します。指定可能な条件を次に示します。 ・表示元 URL： 該当のページリンクを表示するコレクタ画面の URL を登録します。表示元 URL はスキームやホスト名を記載せず，パスのみを記載してください。 ・リンク名： ページリンクとして表示する文字列を指定します。最大 256 文字まで登録できます。 ・表示順： ページリンクの表示順を 1～100 の値で指定します。同じ画面内のページリンクは，左から表示順の値が小さい順に表示します。 ・リンク先 URL： ページリンクで遷移する先の画面の URL を登録します。先頭が”http://”，”https://”から始まる URL，および先頭が”/”から始まるパスを登録できます。 ・ナビゲーションバー リンク先の画面を AX-Collector のナビゲーションバー内に表示する場合にチェックします。
一覧ダウンロード（CSV）	登録しているページリンクの全情報を CSV 形式のファイルとしてダウンロードします。ファイル名は「PL1_PageLink_<日付>.csv」となります。
一括登録・更新	ページリンク　一括登録・更新を表示します。
ページリンク一覧	登録したページリンクの一覧を表示します。
選択リンクの削除	選択したページリンクを削除します。
変更	ページリンクを変更します。
削除	ページリンクを削除します。

表 5-93　管理 ページリンク 一括登録・更新の概要

項目	説明
一括登録・更新	ページリンクにおける各登録情報を一括で登録します。 登録項目を次に示します。 ・ページリンク： ページリンクに関する情報を入力した CSV ファイルを指定します。 ・CSV ファイル未記載データ削除： CSV ファイルに入力されていない情報が AX-Collector に既に登録されている場合に削除するか，削除しないかを指定します。

(9)　画像管理

管理 画像管理の概要を次に示します。

表 5-94　管理 画像管理の概要

項目	説明
新規登録	画像ファイルを新規に登録します。ここに登録した画像をカスタマイズダッシュボードで表示可能です。 登録可能な条件を次に示します。 ・名前： 画像の管理名称を指定します。最大 128 文字まで登録できます。 ・画像： 登録する画像ファイルを指定します。次が登録可能なファイルの条件です。 - フォーマット JPEG(JPG)，PNG，GIF ※1 - 画像ファイル名称 半角文字（英数字，ハイフン，ピリオド）のみ可 ※2 - 画像サイズ（縦×横） 制限なし - データサイズ 最大 5MB/ファイル - ファイル数 最大 100
一覧ダウンロード（CSV）	登録している画像全情報を CSV 形式（画像管理情報）のファイルおよび，ZIP 形式（画像ファイルアーカイブ）としてダウンロードします。 ファイル名は「IM1_DisplayImage_<日付>.csv」，「IM2_ImageFiles_<日付>.zip」となります。
一括登録・更新	画像管理 一括登録・更新を表示します。
名前変更	登録済みの画像管理名称を変更します。
画像変更	登録済みの画像を変更します。
削除	登録画像を削除します。

※1　透過 GIF ファイルは，未サポートです。

※2　コレクタに登録後は，アップロードした元ファイル名とは異なるファイル名称で保存・表示されます。

表 5-95　管理 画像管理 一括登録・更新の概要

項目	説明
一括登録・更新	画像管理における各登録情報を一括で登録します。 登録項目を次に示します。 ・画像管理設定（CSV）： 画像管理情報を入力した CSV ファイルを指定します。 ・画像ファイルアーカイブ（ZIP）： 画像ファイルをアーカイブした ZIP ファイルを指定します。ファイルサイズは，500MB 以下としてください。 パスワード付きの ZIP ファイルは登録できません。 ・CSV ファイル未記載データ削除： CSV ファイルに入力されていない情報が AX-Collector に既に登録されている場合に削除するか，削除しないかを指定します。

（10）　検知情報管理

管理 検知情報管理の概要を次に示します。

監視データに設定する優先度に対するラベル変更や，付加情報の文字列を登録します。また検知一覧画面の検知一覧表の列表示のカスタマイズも本設定で行います。

表 5-96　管理 検知情報管理 優先度ラベルの概要

項目	説明
変更	監視データに設定する優先度１～５に対応するラベルを変更します。各優先度の初期ラベルは次の値です。 優先度１：Critical 優先度２：Error 優先度３：Warning 優先度４：Info 優先度５：Debug 使用可能文字：半角の-&<>'"=`¥/:*?|,;を含まない文字 最大文字数：32 文字
優先度	優先度と設定されているラベルを表示します。

表 5-97　管理 検知情報管理 付加情報の概要

項目	説明
CSV	登録している付加情報１～３情報を CSV 形式のファイルとしてダウンロードします。 ファイル名は「AL_AdditinalInfo_<日付>.csv」となります。

項目	説明
一括登録・更新	付加情報１～３を CSV ファイルにより一括登録・更新します。
変更	変更ボタンにより，付加情報１～３の表示データを直接編集可能なモードとなります。
編集キャンセル	変更ボタンを押下後，編集をキャンセルします。
適用	変更ボタンを押下後，編集した付加情報を登録します。
ID	登録済みの付加情報の管理 ID を表示します。
付加情報１～３	登録済みの付加情報を表示します。 変更ボタンを押下した際には，表示データを直接編集可能です。編集後に変更の適用，もしくは編集キャンセルが可能です。 使用可能文字：半角の&<>"'=`¥/:*?|,;を含まない文字 最大文字数：32 文字

表 5-98　管理 検知情報管理 検知情報一覧表示設定の概要

項目	説明
変更	検知情報一覧表示設定を変更します。
検知情報一覧表示設定	検知情報一覧で表示するフィールドの選択および表示タイトルを設定します。 【一覧表示フィールド】 ＊：初期設定時の表示フィールド 【表示設定】 ○：変更可，－：変更不可 【表示タイトル】 ○：変更可，－：変更不可 使用可能文字：半角の-&<>"'=`¥/:*?| ,;を含まない文字 最大文字数：32 文字

一覧表示フィールド		表示設定	表示タイトル
監視種別		○	－
監視対象	＊	○	－
監視項目カテゴリ		○	－
監視項目	＊	－	－
監視データカテゴリ		○	－
監視データ	＊	○	－
検知種別	＊	○	－
特性		○	－
状態	＊	○	－
検知日時	＊	－	－
復旧日時	＊	○	－
検知継続時間	＊	○	－
優先度	＊	○	○
優先度ラベル	＊	○	○
説明		○	○
アクション		○	○
付加情報１		○	○
付加情報２		○	○

項目	説明		
	付加情報 3	○	○
更新	変更を反映します。		
キャンセル	変更をキャンセルします。		

5.6.6 保守

(1) 運用ログ

保守 運用ログの概要を次に示します。

表 5-99 保守 運用ログの概要

項目	説明
運用ログ	AX-Collector の運用ログを表示条件内で検知日時が新しい順に 10000 件まで表示します。 表示されていない運用ログを表示する場合は，表示期間，表示レベル，表示種別を変更してください。
表示期間設定	ログ一覧で表示する項目を，検知日時で指定します。
表示レベル設定	ログ一覧で表示する項目を，レベルで指定します。 指定可能なレベル： 重大エラー／エラー／警告／情報
表示種別設定	ログ一覧で表示する項目を，種別で指定します。 指定可能な種別： システム／アクセス／ライセンス／データ管理／SNMP 監視／フロー監視／フローランキング監視／外部データ監視／冗長／レポート
付加情報	ログ一覧で追加情報を表示する設定です。ユーザ権限が管理者の場合のみ指定可能です。 アクセス元の IP アドレスやユーザ情報が表示されます。
ログの削除	選択した運用ログを削除します。
検索	表示した運用ログを対象に検索し，一致したものを表示します。
CSV	表示中の運用ログを CSV 形式のファイルでダウンロードします。

(2) アクセスカウンタ

保守 アクセスカウンタの概要を次に示します。

表 5-100 保守 アクセスカウンタの概要

項目	説明
URL／アクセス回数	AX-Collector への画面アクセス，REST-API アクセスの運用ログを指定期間内で集計し，URL 毎のアクセス回数をランキング形式で表示します。
表示期間設定	アクセスカウンタを表示する期間を指定します。 デフォルトの期間は，直近 1 か月です。

項目	説明
ユーザ毎表示	ユーザ毎表示のオプションを指定することで，ユーザアカウント毎に集計したランキングを表示します。

（3） コンフィグ DB 管理

保守 コンフィグ DB 管理の概要を次に示します。

コンフィグ DB は，AX-Collector の設定や検知ログ，運用ログを保存しているデータベースです。本機能を使用すると，1 日に 1 回，コンフィグ DB のバックアップファイルを作成します。

バックアップファイルは，「3.2 新規インストール **表 3-4 AX-Collector インストール時の設定項目一覧**」で指定した”AX-Collector 設定情報格納ディレクトリ“配下の，ax-collector ディレクトリ内に作成されます。ファイル名称は，backup-ax-collector.db-<バックアップ日付>です。ユーティリティコマンドの「（10）リストア機能」で，本バックアップファイルを指定することで，バックアップ時点のコンフィグ DB にリストア可能です。

表 5-101 保守 コンフィグ DB 管理の概要

項目	説明
コンフィグ DB 管理設定	・コンフィグ DB の定期バックアップ： チェックをすると，コンフィグ DB の定期バックアップが有効となります。 初期設定：有効 ・コンフィグ DB の定期バキューム： チェックをすると，コンフィグ DB のバキューム（未使用領域の最適化）が有効となります。 初期設定：有効 ・バックアップ数上限： コンフィグ DB のバックアップファイル数の上限を指定します。設定範囲は，0～32 です。 0：バックアップを作成せず，作成済みのバックアップファイルがあれば削除します。 1～32：バックアップファイル数です。設定値を超過したバックアップファイルは古い順に削除します。 初期設定：10 ・実行タイミング： コンフィグ DB のバックアップおよびバキュームを実行する時刻を指定します。設定範囲は，0:00～23:59 です。 初期設定：3:00
コンフィグ DB ファイル一覧	コンフィグ DB ファイルおよび作成したバックアップファイルの一覧を表示します。
変更	コンフィグ DB 管理設定を変更します。

(4) 保守情報

保守 保守情報の概要を次に示します。

表 5-102 保守 保守情報の概要

項目	説明
コレクタ統計情報表示	コレクタの保守用統計情報を表示します。
保守情報	保守情報ファイルをダウンロードします。

コレクタ統計情報表示では，1 分間隔で収集したコレクタ内部統計情報の時系列グラフを主に表示します。

表 5-103 コレクタ統計情報の概要

項目	説明
稼働状況 統計情報	・コレクタ起動時刻 コレクタが起動した時刻 ・動作時間 コレクタが起動してからの経過時間 ・論理 CPU 数 ホストの論理 CPU 数 ・搭載メモリ ホストの実装メモリ量 ・統計情報 指定した統計情報を表示します。 - 収集データ数統計（常時表示） - 受信パケット数統計 - CPU メモリ統計 - データベース統計
収集データ統計	・フローレコード数/s データベースに保存したフローレコード数／秒を表示します。データ集計間隔毎の最大・平均・最小値を表示します。 ・Syslog 数/s データベースに保存した Syslog 数／秒を表示します。データ集計間隔毎の最大・平均・最小値を表示します。

項目	説明
受信パケット統計	・インタフェース毎 pps コレクタ稼働ホストのネットワークインタフェース毎の受信 PPS を表示します。 ・インタフェース毎 bps コレクタ稼働ホストのネットワークインタフェース毎の受信 BPS を表示します。 ・UDP pps，UDP errors コレクタ稼働ホスト全体の UDP 受信 PPS および，UDP 受信エラーパケット数を表示します。 UDP 受信エラーパケット数は，データ集計間隔毎の合計を表示します。 ・受信解析プロセス毎廃棄レコード数 コレクタアプリケーション内での受信データレコード廃棄数を表示します。本統計は廃棄が発生した場合のみ表示され，データ集計間隔毎の合計値を表示します。 ・UDP ポート番号毎廃棄数 コレクタで使用する UDP ポート番号別の受信パケット廃棄数を表示します。データ集計間隔毎の合計値を表示します。 ・インタフェース毎 drop 数 コレクタ稼働ホストのネットワークインタフェース毎の廃棄パケット数を表示します。データ集計間隔毎の合計値を表示します。 ・インタフェース毎 err 数 コレクタ稼働ホストのネットワークインタフェース毎のエラーパケット数を表示します。データ集計間隔毎の合計値を表示します。
CPU メモリ統計	・CPU 使用率（論理 CPU 毎） 論理 CPU 毎の平均 CPU 使用率を表示します。 ・メモリ使用率（システム） コレクタ稼働ホストのメモリ使用率と搭載メモリ量を表示します。 ・CPU 使用率（機能毎） コレクタの主な機能別平均 CPU 使用率を表示します。 ・メモリ使用率（機能毎） コレクタの主な機能別平均メモリ使用率を表示します。

項目	説明
データベース統計	・ファイルシステム データベースアプリケーションが読み出し・書き込みを行ったデータ量（バイト数）を，データ集計間隔毎の合計値で表示します。また，認識しているストレージ量と使用量も表示します。 ・使用メモリ量 データベースアプリケーション使用しているメモリ量（バイト数）をメモリ種別毎に表示します。メモリ量は集計間隔毎の平均値を表示します。 また，認識している合計メモリ量および使用量もあわせて表示します。 ・その他 データベースアプリケーションのメモリガベッジコレクションにかかった合計時間を表示します。 また，使用しているファイルディスクリプタ数も表示します。

5.7 ブックマーク

AX-Collector では，頻繁にアクセスする Web サイトの URL，あるいは頻繁に使用するサーバアプリおよび同アプリで作成した Web ページなどの URL を登録する機能を提供します。URL はトップカテゴリおよびカテゴリにより階層的に管理できます。ブックマークに登録した URL は，AX-Collector の全ユーザが共通的に使用可能となり，利便性の向上をはかれます。

(1) ブックマーク管理

ブックマーク管理の概要を次に示します。

表 5-104 ブックマーク管理の概要

項目	説明
一覧ダウンロード(CSV)	登録しているブックマークの全情報を CSV 形式のファイルとしてダウンロードします。ファイル名は「BM1_Bookmark_<*日付*>.csv」となります。
一括登録・更新	ブックマークにおける各登録情報を一括で登録します。 登録項目を次に示します。 ・ブックマーク：ブックマークの内容に関する情報を入力した CSV ファイルを指定します。 ・CSV ファイル未記載データ削除： CSV ファイルに入力されていない情報が AX-Collector に既に登録されている場合に削除するか，削除しないかを指定します。
ブックマーク設定一覧	ブックマークの設定をトップカテゴリ毎に一覧表示します。
変更	トップカテゴリ毎にブックマークを登録します。 登録項目を次に示します。 ・トップカテゴリ名：トップカテゴリの名前を登録します。 ・カテゴリ名：カテゴリの名前を登録します。 ・リンク名：リンクの名前を登録します。 ・URL：ブックマークのリンク先の URL を登録します。先頭が”http://”，”https://”から始まる URL，および先頭が”/”から始まるパスを登録できます。 ・ナビゲーションバー：リンク先の画面を AX-Collector のナビゲーションバー内に表示する場合にチェックします。 ・選択項目のクリア：選択したブックマークの入力内容を初期化します。

(2) ブックマーク一覧

ブックマーク一覧の概要を次に示します。

表 5-105　ブックマーク一覧の概要

項目	説明
トップカテゴリ	トップカテゴリ毎にブックマークの表示をフィルタします。
検索	任意の文字列を入力して，一致するブックマークのみを表示します。複数の文字列を半角スペースと and 又は or で接続して入力することができます。 検索対象はトップカテゴリ名，カテゴリ名，リンク名です。 トップカテゴリ名またはカテゴリ名に一致した場合は，その配下のリンクを全て表示します。
メニューを開く	ブックマークのトップカテゴリ配下またはカテゴリ配下を表示します。
メニューを閉じる	ブックマークのトップカテゴリ配下またはカテゴリ配下を非表示にします。
ブックマーク一覧	ブックマークを階層形式で表示します。 トップカテゴリまたはカテゴリを選択することで，その配下の表示・非表示を切り替えることができます。

(3)　ブックマーク登録

現在表示中の画面をブックマークに登録します。登録（＋）ボタンを押下すると，新規追加，あるいは既存ブックマークの上書き変更が可能です。なお，トップカテゴリ，カテゴリの設定は，(1)ブックマーク管理の変更オペレーションで行います。

ブックマーク追加の概要を次に示します。

表 5-106　ブックマーク登録の概要

項目	説明
トップカテゴリ名	設定済みのトップカテゴリ名称を選択します。 初期選択：未登録のリンク ID が存在するトップカテゴリ名称
カテゴリ名	設定済みのカテゴリ名称を選択します。 初期選択：未登録のリンク ID が存在するカテゴリ名称
リンク ID	トップカテゴリ，カテゴリ内のリンク ID を選択します。 初期選択：未登録のリンク ID
リンク名	リンク名文字列を設定します。 新規登録： 　未登録のリンク ID が選択されている場合，新規登録となり，入力が必須です。 登録変更： 　登録済みリンク ID を選択し，入力した場合，リンク名が上書き登録されます。
URL	リンク先の URL を設定します。 初期表示：現在表示中の画面に対応する URL。パラメータを含みます。特定ページでは，画面名称指定 URL が設定されます（**表 5-107　画面名称指定 URL 対象画面一覧**参照）。
ナビゲーションバー	リンク先の画面を AX-Collector のナビゲーションバー内に表示する場合にチェックします

特定の画面では，画面名称指定 URL でブックマーク登録可能です。画面名称指定 URL は，カスタマイズダッシュボードや個別ビュー等の画面を，各画面につけた名称をパラメータ指定して表示可能な URL です。

ブラウザに表示される URL は，画面の作成順序によって変わりますが，画面名称指定 URL を使うと，作成順序に異存ぜずに該当画面の表示が可能となります。対応する画面と URL を以下の表示に記載します。

表 5-107　画面名称指定 URL 対象画面一覧

画面種別	ブラウザ表示 URL	画面名称指定 URL ※1
プリセット ダッシュボード	/view /embedded-combination-views /<ID>/	/disp/ ?app=embedded-combination-views &name=<プリセットダッシュボード名>
カスタマイズ ダッシュボード	/view /combination-views /<ID>/	/disp/ ?app=combination-views &name=<カスタマイズダッシュボード名>
個別ビュー	/view /simplex-views /<ID>/	/disp/ ?app=simplex-views &name=<個別ビュー名>
監視状況俯瞰 ビュー	/statusoverview /birds-eye-views /<ID>/	/disp/ ?app=birds-eye-views &name=<監視状況俯瞰ビュー名>
SNMP 監視データ 表示画面	/snmp /monitoring-items /view /<ID>/	/disp/ ?app=snmp_monitoring-items_view &name=<SNMP 監視項目名>
フロー 監視データ 表示画面	/flow /monitoring-items /view /<ID>/	/disp/ ?app=flow_monitoring-items_view &name=<フロー監視項目名>
フローランキング監視データ 表示画面	/flowmonitor /monitoring-ranking /gather /<ID>/	/disp/ ?app=flowmonitor_monitoring-ranking_gather&name=＜フローランキング監視項目名＞
外部 監視データ 表示画面	/extmonitor /monitoring-items /view /<ID>/	/disp/ ?app=extmonitor_monitoring-items_view &name=<監視項目カテゴリ名>:<監視項目データ名>

※1　名称は URL エンコードされたものになります。

5.8 検知

AX-Collector が提供する監視機能における検知状況を可視化します。

5.8.1 検知状況

各監視機能における検知状況をカレンダー形式，およびランキング形式で表示します。

（1） 検知数カレンダー

SNMP 閾値監視，フロー閾値監視，外部データ閾値監視，および Impulse 連携監視における 1 日毎の検知数をカレンダー形式で表示します。

表 5-108 検知数カレンダーの概要

項目	説明
絞り込み条件	検知数カレンダーの表示対象とするデータの範囲を設定します。指定可能な条件を次に示します。 ・全体 ：監視種別および監視状態を指定します。 ・閾値監視 ：閾値監視が表示対象である場合，SNMP 監視における監視項目およびオブジェクトグループ，フロー監視における監視項目およびフロー条件グループ，フローランキング監視における監視項目，外部データ監視における監視項目および監視データを指定します。 ・Impulse 連携監視：Impulse 連携監視が表示対象である場合，監視対象として SNMP 監視，フロー監視，外部データ監視を指定します。SNMP 監視における監視項目およびオブジェクトグループ，フロー監視における監視項目およびフロー条件グループ，外部データ監視における監視項目および監視データを指定します。
前月	一か月前のカレンダーを表示します。
年月表示	現在表示しているカレンダーの年月を表示します。 クリックすることで，年月を指定してカレンダーを表示することができます。
次月	一か月先のカレンダーを表示します。

項目	説明
日付セル	該当の日付における，SNMP 閾値監視機能，フロー閾値監視機能，フローランキング閾値監視機能，外部データ閾値監視機能，Impulse 連携による監視機能の検知数を表示します。 表示した検知数情報をクリックすることにより，当該検知数情報を対象とした検知数ランキングを表示します。
総検知数	表示した月における，SNMP 閾値監視機能，フロー閾値監視機能，フローランキング閾値監視機能，外部データ閾値監視機能，Impulse 連携による監視機能の総検知数を表示します。 表示した総検知数情報をクリックすることにより，当該総検知数情報を対象とした検知数ランキングを表示します。

（2） 検知数ランキング

SNMP 閾値監視，フロー閾値監視，外部データ閾値監視，および Impulse 連携監視における検知数をランキング形式で表示します。

表 5-109 検知数ランキングの概要

項目	説明
絞り込み条件	検知数ランキングの表示対象とするデータの範囲を設定します。指定可能な条件を次に示します。 ・全体 ：監視種別および監視状態を指定します。 ・閾値監視 ：閾値監視が表示対象である場合，SNMP 監視における監視項目およびオブジェクトグループ，フロー監視における監視項目およびフロー条件グループ，フローランキング監視における監視項目，外部データ監視における監視項目および監視データを指定します。 ・Impulse 連携監視：Impulse 連携監視が表示対象である場合，監視対象として SNMP 監視，フロー監視，外部データ監視を指定します。SNMP 監視における監視項目およびオブジェクトグループ，フロー監視における監視項目およびフロー条件グループ，外部データ監視における監視項目および監視データを指定します。 ・期間 ：表示対象のデータの期間を指定します。
一覧(全項目)	検知数を表示している全項目の検知情報の一覧を表示します。表示内容は，(3) 検知一覧を参照。

項目	説明
CSV	検知数を表示している全項目の検知情報の一覧を CSV 形式でダウンロードします。 ファイル名は，以下となります。 絞り込み条件の期間で特定の日を指定： *ax-collector-alert(＜指定日＞).csv* 絞り込み条件の期間で複数日を指定： *ax-collector-alert(<開始日>-<終了日>).csv*
検知数ランキング情報	SNMP 閾値監視，フロー閾値監視，フローランキング閾値監視，外部データ閾値監視，および Impulse 連携監視において，絞り込み条件に該当する項目の検知数をランキング形式で表示します。
操作	表示している各項目の検知情報に対して，次の操作を行います。 ・一覧 ：各項目の検知一覧を表示します。 ・CSV：各項目の検知一覧を CSV 形式でダウンロードします。 ファイル名は，以下となります。 絞り込み条件の期間で特定の日を指定： *ax-collector-alert(＜指定日＞).csv* 絞り込み条件の期間で複数日を指定： *ax-collector-alert(<開始日>-<終了日>).csv*

（3） 検知一覧

SNMP 閾値監視，フロー閾値監視，フローランキング閾値監視，外部データ閾値監視，および Impulse 連携監視における検知一覧を表示します。

検知一覧表の表示内容は，設定によりカスタマイズすることが可能です。設定内容は，「5.6.5 管理」の「（10）検知情報管理」を参照してください。

また，検知一覧表の画面上の列見出しをドラッグし，横に移動することで列の位置を入替可能です。移動した位置と表示列毎の幅は，自動的にブラウザに保存され，再度表示した際には前回の位置で表示されます。

また，表示中の列並び順は，画面右上のレイアウト保存ボタンにより，コレクタに保存可能です。初めて利用するブラウザで検知一覧画面を開く場合や，ブラウザの保存データを削除した後に開く場合に，サーバに保存された並び順で表示されます。

なお，保存データの削除も，画面右上のレイアウト保存ボタンから可能です。

表 5-110　検知一覧の概要

項目	説明
絞り込み条件	検知一覧の表示対象とするデータの範囲を設定します。 指定可能な条件を次に示します。 ・全体　：監視種別および監視状態を指定します。 ・閾値監視　：閾値監視が表示対象である場合，SNMP 監視における監視項目およびオブジェクトグループ，フロー監視における監視項目およびフロー条件グループ，フローランキング監視における監視項目，外部データ監視における監視項目および監視データを指定します。 ・Impulse 連携監視：Impulse 連携監視が表示対象である場合，監視対象として SNMP 監視，フロー監視，外部データ監視を指定します。SNMP 監視における監視項目およびオブジェクトグループ，フロー監視における監視項目およびフロー条件グループ，外部データ監視における監視項目および監視データを指定します。 ・期間　：表示対象のデータの期間を指定します。
CSV	表示している全項目の検知情報の一覧を CSV 形式でダウンロードします。CSV ファイル内の列は，画面表示されている順番となります。また，検知設定で非表示としている項目も CSV ファイルには格納されます。 ファイル名は，以下となります。 絞り込み条件の期間で特定の日を指定： ax-collector-alert(＜指定日＞).csv 絞り込み条件の期間で複数日を指定： ax-collector-alert(<開始日>-<終了日>).csv
選択通知の削除	選択した検知通知を削除します。
検索	表示した一覧情報を対象に検索し，一致したものを表示します。 検知一覧の表示列毎に絞り込みが可能です。
検知一覧	検知数ランキングの一覧表示の対象となる SNMP 閾値監視，フロー閾値監視，フローランキング閾値監視，外部データ閾値監視，および Impulse 連携監視の検知情報を，表示期間内で検知日時が新しい順に 10000 件まで表示します。
操作	表示している各項目の検知情報に対して，次の操作を行います。 ・収集データ：検知対象の収集データを表示します。 ・詳細：当該検知通知の詳細情報を表示します。

(4) 通知詳細

SNMP 閾値監視，フロー閾値監視，外部データ閾値監視，および Impulse 連携監視における検知通知の詳細を表示します。

表 5-111 SNMP 監視 閾値監視通知の概要

項目	説明
ID	検知通知の ID を表示します。
状態	検知中または復旧済みを表示します。
検知日時	閾値超え検知が発生した日時を表示します。
復旧日時	閾値超えからの復旧が発生した日時を表示します。
SNMP 監視項目	検知が発生した SNMP 監視項目の名前を表示します。
MIB オブジェクトグループ	検知が発生した MIB オブジェクトグループの名前を表示します。
閾値種別	上限検知または下限検知を表示します。
検知閾値	検知が発生した閾値を表示します。
値	検知が発生した監視値を表示します。
説明	検知が発生した MIB オブジェクトグループに設定した説明を表示します。
アクション	検知が発生した MIB オブジェクトグループに設定したアクションを表示します。
優先度	検知が発生した MIB オブジェクトグループに設定した優先度を表示します。
優先度ラベル	優先度に対応するラベルを表示します。
付加情報 1	検知が発生した MIB オブジェクトグループに設定した付加情報 1 を表示します。
付加情報 2	検知が発生した MIB オブジェクトグループに設定した付加情報 2 を表示します。
付加情報 3	検知が発生した MIB オブジェクトグループに設定した付加情報 3 を表示します。
参照先 URL	検知が発生した SNMP 監視項目に設定した参照先 URL を表示します。

表 5-112 フロー監視 閾値監視通知の概要

項目	説明
ID	検知通知の ID を表示します。
状態	検知中または復旧済みを表示します。
検知日時	閾値超え検知が発生した日時を表示します。
復旧日時	閾値超えからの復旧が発生した日時を表示します。
フロー情報監視項目	検知が発生したフロー監視項目の名前を表示します。
フロー条件グループ	検知が発生したフロー条件グループの名前を表示します。
閾値種別	上限検知または下限検知を表示します。
検知閾値	検知が発生した閾値を表示します。

項目	説明
値	検知が発生した監視値を表示します。
説明	検知が発生したフロー条件グループに設定した説明を表示します。
優先度	検知が発生したフロー条件グループに設定した優先度を表示します。
優先度ラベル	優先度に対応するラベルを表示します。
付加情報 1	検知が発生したフロー条件グループに設定した付加情報 1 を表示します。
付加情報 2	検知が発生したフロー条件グループに設定した付加情報 2 を表示します。
付加情報 3	検知が発生したフロー条件グループに設定した付加情報 3 を表示します。
参照先 URL	検知が発生したフロー監視項目に設定した参照先 URL を表示します。

表 5-113　フローランキング監視 閾値監視通知の概要

項目	説明
ID	検知通知の ID を表示します。
状態	復旧済みを表示します。
検知日時	閾値超え検知が発生した日時を表示します。
復旧日時	検知日時と同じ日時を表示します。
フローランキング監視項目	検知が発生したフローランキング監視項目の名前を表示します。
説明	検知が発生したフローランキング監視項目に設定した説明を表示します。
優先度	検知が発生したフローランキング監視項目に設定した優先度を表示します。
優先度ラベル	優先度に対応するラベルを表示します。
付加情報 1	検知が発生したフローランキング監視項目に設定した付加情報 1 を表示します。
付加情報 2	検知が発生したフローランキング監視項目に設定した付加情報 2 を表示します。
付加情報 3	検知が発生したフローランキング監視項目に設定した付加情報 3 を表示します。
参照先 URL	検知が発生したフロー監視項目に設定した参照先 URL を表示します。
検知データ	検知した詳細データを表示します。

表 5-114　外部データ監視 閾値監視通知の概要

項目	説明
ID	検知通知の ID を表示します。
状態	検知中または復旧済みを表示します。
検知日時	閾値超え検知が発生した日時を表示します。

項目	説明
復旧日時	閾値超えからの復旧が発生した日時を表示します。
監視項目カテゴリ名	検知が発生した外部データ監視項目の監視項目カテゴリ名を表示します。
監視項目データ名	検知が発生した外部データ監視項目の監視項目データ名を表示します。
監視データカテゴリ名	検知が発生した外部監視データの監視データカテゴリ名を表示します。
監視データ名	検知が発生した外部監視データの監視データ名を表示します。
閾値種別	上限検知または下限検知を表示します。
検知閾値	検知が発生した閾値を表示します。
値	検知が発生した監視値を表示します。
説明	検知が発生した外部監視データに設定した説明を表示します。
優先度	検知が発生した外部監視データに設定した優先度を表示します。
優先度ラベル	優先度に対応するラベルを表示します。
付加情報 1	検知が発生した外部監視データに設定した付加情報 1 を表示します。
付加情報 2	検知が発生した外部監視データに設定した付加情報 2 を表示します。
付加情報 3	検知が発生した外部監視データに設定した付加情報 3 を表示します。
参照先 URL	検知が発生した外部データ監視項目に設定した参照先 URL を表示します。

表 5-115　Impulse 連携 検知通知の概要

項目	説明
ID	検知通知の ID を表示します。
状態	検知中または復旧済みを表示します。
検知日時	Impulse 連携で異常検知が発生した日時を表示します。
復旧日時	Impulse 連携で復旧検知が発生した日時を表示します。
監視項目 名前	検知が発生した SNMP 監視項目の名前，フロー監視項目の名前，または外部データ監視項目のデータ名を表示します。
監視項目 データセット名	検知が発生した SNMP 監視項目のインデックス名，フロー監視項目のインデックス名，または外部データ監視項目のデータセット名を表示します。
オブジェクトグループ 名前	検知が発生した MIB オブジェクトグループの名前，フロー条件グループの名前，または外部監視データの監視データ名を表示します。

項目	説明
オブジェクトグループ メトリクス名	検知が発生した MIB オブジェクトグループのタグ名，フロー条件グループのタグ名，または外部監視データのメトリクス名を表示します。
オブジェクトグループ 値	検知が発生した監視値を表示します。
特性	Impulse より通知された特性を表示します。
検知要件	Impulse より通知された検知要件を表示します。
説明	検知が発生した MIB オブジェクトグループ，フロー条件グループ，または外部監視データ（以降検知対象）に設定した説明を表示します。
優先度	検知対象に設定した優先度を表示します。
優先度ラベル	検知対象に設定した優先度に対応するラベルを表示します。
付加情報 1	検知対象に設定した付加情報 1 を表示します。
付加情報 2	検知対象に設定した付加情報 2 を表示します。
付加情報 3	検知対象に設定した付加情報 3 を表示します。
参照先 URL	検知対象に設定した参照先 URL を表示します。

5.8.2 検知通知一覧（機能別）

各監視機能における検知通知一覧を表示します。

（1） 閾値監視通知（SNMP）

SNMP 監視 閾値監視通知についての検知一覧を表示します。

（2） 閾値監視通知（フロー）

フロー監視 閾値監視通知についての検知一覧を表示します。

（3） 閾値監視通知（フローランキング）

フローランキング監視 閾値監視通知についての検知一覧を表示します。

（4） 閾値監視通知（外部データ）

外部データ監視 閾値監視通知についての検知一覧を表示します。

（5） Impulse 連携通知

Impulse 連携通知についての検知一覧を表示します

5.9 検索

ナビゲーションバーの検索ボタンから表示できる検索ウィンドウで， AX-NM の端末接続履歴情報，またはコレクタのフロー情報を検索し表示します。

検索結果の端末接続履歴情報は，同じ検索ウィンドウ下部に表示され，フロー情報は指定した表示画面が別ウィンドウに表示されます。

表 5-116 検索ウィンドウの概要（端末接続履歴）

項目	説明
開始日時	検索対象期間の開始日時を指定します。 終了日時と同時に指定して下さい。片方のみ指定した場合は，検索期間未指定として扱います。 例）2021-01-11 10:00:00
終了日時	検索対象期間の終了日時を指定します。 開始日時と同時に指定して下さい。片方のみ指定した場合は，検索期間未指定として扱います。 例）2021-01-11 10:00:00
MAC アドレス	検索対象の MAC アドレスを指定します。 例）00:00:5e:00:53:01
IP アドレス	検索対象の IPv4 アドレスを指定します。 例）192.168.192.73
検索実行	AX-NM から指定した条件に該当する端末接続履歴を取得して表示します。 本機能を使用するためには，AX-NM 連携環境設定を登録し，AX-Network-Manager との接続が可能である必要があります。

表 5-117 検索ウィンドウの概要（フロー情報）

項目	説明
開始日時	検索対象期間の開始日時を指定します。 終了日時と同時に指定して下さい。片方のみ指定した場合は，検索期間未指定として扱います。 例）2021-01-11 10:00:00
終了日時	検索対象期間の終了日時を指定します。 開始日時と同時に指定して下さい。片方のみ指定した場合は，検索期間未指定として扱います。 例）2021-01-11 10:00:00
MAC アドレス	検索対象の MAC アドレスを指定します。 例）00:00:5e:00:53:01
IP アドレス	検索対象の IPv4 アドレス，または IPv4 ネットワークアドレスを指定します。 IPv4 ネットワークアドレスはスラッシュでマスク長を指定します。 例）192.168.192.73，192.168.253.0/24

項目	説明
L4 ポート番号	検索対象の L4 ポート番号を指定します。 例）80
NAT IP アドレス	検索対象の NAT IPv4 アドレス，または NAT IPv4 ネットワークアドレスを指定します。 NAT IPv4 ネットワークアドレスはスラッシュでマスク長を指定します。 例）10.1.1.2，10.1.0.0/16
NAT L4 ポート番号	検索対象の NAT L4 ポート番号を指定します。 例）80
表示画面	指定した検索条件がセットされたフロー情報検索結果の表示画面をプルダウンで指定します。選択できる表示画面と，設定される検索条件は次の通りです。 ・IP フローランキングリスト 検索条件：開始日時，終了日時，MAC アドレス IP アドレス，L4 ポート番号 NAT IP アドレス，NAT L4 ポート番号 ・IP フロー複合ビュー 検索条件：開始日時，終了日時，MAC アドレス IP アドレス，L4 ポート番号 ・MAC フローランキングリスト 検索条件：開始日時，終了日時，MAC アドレス
表示フィールドオプション	表示画面 IP フローランキングリスト選択時の設定済み表示フィールドを選択するオプションです。 クリックして選択します。選択可能なオプションと設定済み表示フィールドを示します。 ・標準 標準の表示オプション ・OS NAT FortiGate OS NAT ログ表示オプションです。 表示フィールド：タイムスタンプ 送信元，宛先 IPv4 アドレス プロトコル番号 NAT 送信元，宛先 IPv4 アドレス NAT 送信元，宛先 L4 ポート番号 ・Hyperscale NAT ※1 FortiGate Hyperscale License 適用時の NAT ログ情報表示オプションです。 表示フィールド：タイムスタンプ 送信元，宛先 IPv4 アドレス プロトコル番号 NAT 送信元，宛先 IPv4 アドレス NAT 送信元，宛先 L4 ポート番号 NAT 観測時間（開始，終了） NAT 継続時間（s） 送信バイト数，送信パケット数

項目	説明
表示画面を開く	選択した表示画面を別ウィンドウに表示します。 表示画面は，指定した条件があらかじめセットされた検索条件画面です。指定条件を確認後，表示ボタンを押下することで検索を開始し結果が表示されます。

※1：FortiGate Hyperscale License 適用時の NAT ログ情報には，アクセス網から外部ネットワーク方向のフロー情報のみが記録されます。バイト数・パケット数には外部⇒アクセス方向，送信バイト数・送信パケット数は，アクセス⇒外部のトラフィックが格納されます。

表 5-118　検索ウィンドウの概要（GEOIP 情報）

項目	説明
IP アドレス	検索対象の IPv4 または IPv6 アドレスを指定します。 例）192.168.192.73
検索実行	GEOIP 連携機能で使用している MMDB を検索し，検索結果を表示します。 また,検索対象の IP アドレス種別（linklocal 等）も併せて表示します。

6. MIB リファレンス

この章では，AX-Collector で使用するプライベート MIB の実装仕様について説明します。Ax-Collector では，SNMPv2C に対応しています。

6.1 サポート MIB

6.1.1 MIB 体系図

AX-Collector がサポートする MIB の体系図を以下に示します。

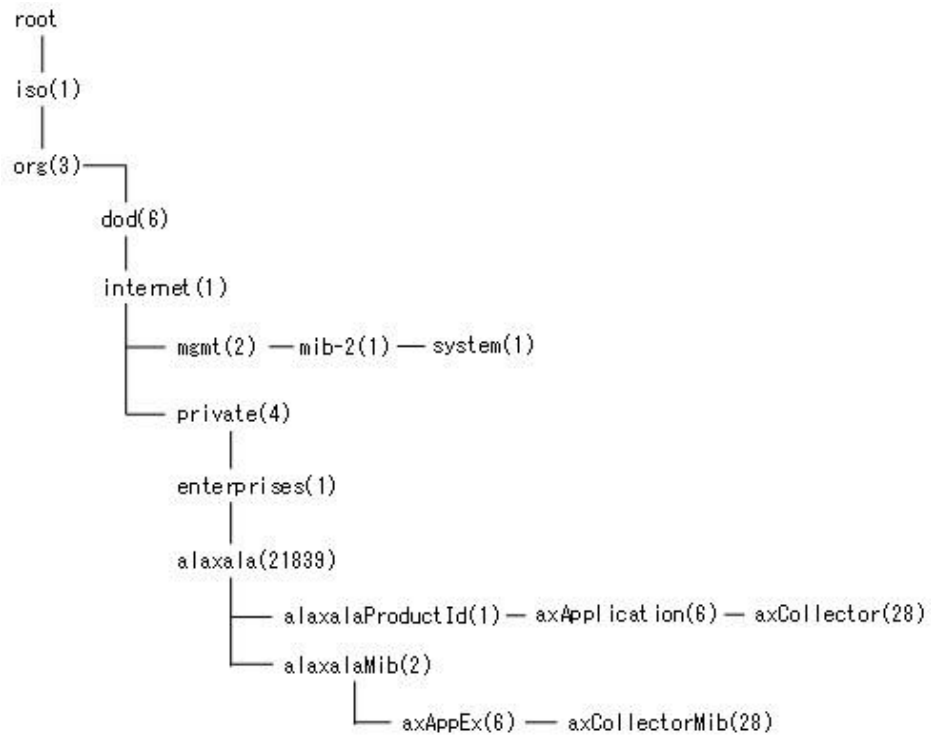

図 6-1 MIB 体系図

6.1.2 MIB の記述形式

このマニュアルで記述しているサポート MIB の記述形式について説明します。各 MIB はグループごとに識別子および実装仕様を記述しています。

- **識別子**

  オブジェクト識別子の公認された記述形式です。

  例として，プライベート MIB axCollMibMonitorTable グループの識別子の記述形式とオブジェクト ID 値を次に示します。

  識別子

```
axAppEx OBJECT IDENTIFIER ::= {alaxalaMib 6}
axCollectorMib OBJECT IDENTIFIER ::= {axAppEx 28}
axCollMibMonitor OBJECT IDENTIFIER ::= {axCollectorMib 3}
axCollMibMonitorTable OBJECT IDENTIFIER ::= {axCollMibMonitor 1}
```

  オブジェクト ID 値

1.3.6.1.4.1.21839.2.6.28.3.1

● 実装仕様

各 MIB の実装仕様を表で説明しています。

オブジェクト識別子

MIB のオブジェクト識別子の名称を示しています。

SYNTAX

AX-Collector のプライベート MIB で使用している SYNTAX の意味を次の表に示します。

表 6-1 プライベート MIB で使用している SYNTAX の意味

項番	SYNTAX	SYNTAX の説明
1	Counter64	0..18446744073709551615(2^{64}-1)まで増加し，また 0 に戻る整数値。
2	Integer32	-2147483648..2147483647(-2^{31}..2^{31}-1)の範囲の整数情報を表す。
3	OCTET STRING	0 個以上の文字列（8 ビット単位）。各バイトは，0..255。

アクセス

AX-Collector のプライベート MIB で使用しているアクセス種別を次に示します。

- AN：規格ドキュメント上の MIB アクセスが accessible-for-notify であることを示します。Object の取得および設定ができませんが，SNMP 通知の variable として読み取ることができます。
- NA：規格ドキュメント上の MIB アクセスが not-accessible であることを示します。

実装仕様

AX-Collector での実装仕様を記述しています。

実装有無

- Y：AX-Collector でサポート（応答）する MIB を示しています。ただし，アクセス欄が「NA」の場合，MIB の応答はしません。また使用する機能によって応答するものが変わりますので注意してください。
- N：AX-Collector でサポート（応答）しない MIB を示しています。

6.2 標準 MIB(RFC 準拠および IETF ドラフト MIB)

AX-Collector で使用する標準 MIB の実装仕様について説明します。

6.2.1 System グループ(MIB-II)

system グループの準拠規格を次に示します。

・RFC3418

(1) 識別子

system OBJECT IDENTIFIER ::= {mib-2 1}

オブジェクト ID 値　1.3.6.1.2.1.1

(2) 実装仕様

system グループの実装仕様を次の表に示します。

表 6.2-1 system グループ MIB の実装仕様

#	オブジェクト識別子	アクセス	実装仕様	実装有無
1	sysUpTime {system 3}	AN	［規格］システムが起動してからの累積時間（10 ミリ秒カウンタ）。 ［実装］AX-Collector 起動時からの累積時間。	Y

6.3 プライベート MIB

AX-Collector で使用するプライベート MIB の実装仕様について説明します。

6.3.1 axCollFlwMonitorTable

AX-Collector のフロー監視機能のフロー収集情報に関する MIB です。

（1） 識別子

axAppEx OBJECT IDENTIFIER ::= {alaxalaMib 6}

axCollectorMib OBJECT IDENTIFIER ::= {axAppEx 28}

axCollFlwMonitor OBJECT IDENTIFIER ::= {axCollectorMib 2}

axCollFlwMonitorTable OBJECT IDENTIFIER ::= {axCollFlwMonitor 1}

オブジェクト ID 値　1.3.6.1.4.1.21839.2.6.28.2.1

（2） 実装仕様

axCollFlwMonitorTable の実装仕様を次の表に示します。

表 6.3-1 axCollFlwMonitorTable の実装仕様

#	オブジェクト識別子	SYNTAX	アクセス	実装仕様	実装有無
1	axCollFlwMonitorTable {axCollFlwMonitor 1}	SEQUENCE OF axCollFlwMonitorEntry	NA	AX-Collector のフロー監視におけるフロー収集情報テーブル	Y
2	axCollFlwMonitorEntry {axCollFlwMonitorTable 1}	axCollFlwMonitorEntry	NA	フロー収集情報テーブルのエントリ INDEX { axCollFlwMonitorItemIndex, axCollFlwMonitorObjectGroupIndex }	Y
3	axCollFlwMonitorItemIndex {axCollFlwMonitorEntry 1}	Integer32	AN	フロー監視項目のインデックス	Y
4	axCollFlwMonitorObjectGroupIndex {axCollFlwMonitorEntry 2}	Integer32	AN	フロー監視対象のフロー条件グループのインデックス	Y
5	axCollFlwMonitorItemName {axCollFlwMonitorEntry 3}	OCTET STRING	AN	フロー監視項目に設定したインデックス名	Y
6	axCollFlwMonitorObjectGroupName {axCollFlwMonitorEntry 4}	OCTET STRING	AN	フロー監視対象のフロー条件グループに設定したタグ名	Y
7	axCollFlwMonitorValue {axCollFlwMonitorEntry 5}	Counter64	AN	フロー監視対象のフロー条件グループ毎に収集した値 1 未満（小数点以下）は切り捨て 負の値の場合は 0 を格納する	Y

6.3.2 axCollFlwThreshold

AX-Collector のフロー監視機能の閾値監視情報に関する MIB です。

(1) 識別子

axCollFlwThreshold OBJECT IDENTIFIER ::= {axCollFlwMonitor 2}

オブジェクト ID 値　1.3.6.1.4.1.21839.2.6.28.2.2

(2) 実装仕様

axCollFlwThreshold の実装仕様を次の表に示します。

表 6.3-2 axCollFlwThreshold の実装仕様

#	オブジェクト識別子	SYNTAX	アクセス	実装仕様	実装有無
1	axCollFlwThresholdDetectTime {axCollFlwThreshold 1}	OCTET STRING	AN	フロー監視で閾値超えを検知した日時。 "YYYY-MM-DDThh:mm:ss+ 09:00"で示します。 ・ YYYY：年 ・ MM：月 ・ DD：日 ・ hh：時 ・ mm：分 ・ ss：秒	Y
2	axCollFlwThresholdRecoverTime {axCollFlwThreshold 2}	OCTET STRING	AN	フロー監視で閾値超えからの復旧を検知した日時。 "YYYY-MM-DDThh:mm:ss+ 09:00"で示します。 ・ YYYY：年 ・ MM：月 ・ DD：日 ・ hh：時 ・ mm：分 ・ ss：秒	Y
3	axCollFlwThresholdType {axCollFlwThreshold 3}	OCTET STRING	AN	閾値の種別。以下の何れかの文字列。 “upper_threshold”：上限閾値 “lower_threshold”：下限閾値	Y
4	axCollFlwThresholdValue {axCollFlwThreshold 4}	Counter64	AN	閾値として設定された値。整数値。 負の値の場合は 0 を格納する。	Y

6.3.3 axCollMibMonitorTable

AX-Collector の SNMP 監視機能の MIB 収集情報に関する MIB です。

（1） 識別子

axAppEx OBJECT IDENTIFIER ::= {alaxalaMib 6}

axCollectorMib OBJECT IDENTIFIER ::= {axAppEx 28}

axCollMibMonitor OBJECT IDENTIFIER ::= {axCollectorMib 3}

axCollMibMonitorTable OBJECT IDENTIFIER ::= {axCollMibMonitor 1}

オブジェクト ID 値　1.3.6.1.4.1.21839.2.6.28.3.1

（2） 実装仕様

axCollMibMonitorTable の実装仕様を次の表に示します。

表 6.3-3 axCollMibMonitorTable の実装仕様

#	オブジェクト識別子	SYNTAX	アクセス	実装仕様	実装有無
1	axCollMibMonitorTable {axCollMibMonitor 1}	SEQUENCE OF AxCollMibMonitorEntry	NA	AX-Collector の SNMP 監視における MIB 収集情報テーブル	Y
2	axCollMibMonitorEntry {axCollMibMonitorTable 1}	AxCollMibMonitorEntry	NA	MIB 収集情報テーブルのエントリ INDEX { axCollMibMonitorItemIndex, axCollMibMonitorObjectGroupIndex }	Y
3	axCollMibMonitorItemIndex {axCollMibMonitorEntry 1}	Integer32	AN	SNMP 監視項目のインデックス	Y
4	axCollMibMonitorObjectGroupIndex {axCollMibMonitorEntry 2}	Integer32	AN	SNMP 監視対象の MIB オブジェクトグループのインデックス	Y
5	axCollMibMonitorItemName {axCollMibMonitorEntry 3}	OCTET STRING	AN	SNMP 監視項目に設定したインデックス名	Y
6	axCollMibMonitorObjectGroupName {axCollMibMonitorEntry 4}	OCTET STRING	AN	SNMP 監視対象の MIB オブジェクトグループに設定したタグ名	Y
7	axCollMibMonitorValue {axCollMibMonitorEntry 5}	Counter64	AN	SNMP 監視対象の MIB オブジェクトグループ毎に収集した MIB 値 1 未満（小数点以下）は切り捨て 負の値の場合は 0 を格納する	Y

6.3.4 axCollMibThreshold

AX-Collector の SNMP 監視機能の閾値監視情報に関する MIB です。

（1） 識別子

axCollMibThreshold OBJECT IDENTIFIER ::= {axCollMibMonitor 2}

オブジェクト ID 値　1.3.6.1.4.1.21839.2.6.28.3.2

（2） 実装仕様

axCollMibThreshold の実装仕様を次の表に示します。

表 6.3-4 axCollMibThreshold の実装仕様

#	オブジェクト識別子	SYNTAX	アクセス	実装仕様	実装有無
1	axCollMibThresholdDetectTime {axCollMibThreshold 1}	OCTET STRING	AN	SNMP 監視で閾値超えを検知した日時。 "YYYY-MM-DDThh:mm:ss+ 09:00"で示します。 ・ YYYY：年 ・ MM：月 ・ DD：日 ・ hh：時 ・ mm：分 ・ ss：秒	Y
2	axCollMibThresholdRecoverTime {axCollMibThreshold 2}	OCTET STRING	AN	SNMP 監視で閾値超えからの復旧を検知した日時。 "YYYY-MM-DDThh:mm:ss+ 09:00"で示します。 ・ YYYY：年 ・ MM：月 ・ DD：日 ・ hh：時 ・ mm：分 ・ ss：秒	Y
3	axCollMibThresholdType {axCollMibThreshold 3}	OCTET STRING	AN	閾値の種別。以下の何れかの文字列。 “upper_threshold”：上限閾値 “lower_threshold”：下限閾値	Y
4	axCollMibThresholdValue {axCollMibThreshold 4}	Counter64	AN	閾値として設定された値。整数値。 負の値の場合は 0 を格納する	Y

6.3.5 axCollExtMonitorTable

AX-Collector の外部データ監視機能の外部データ収集情報に関する MIB です。

（1） 識別子

axAppEx OBJECT IDENTIFIER ::= {alaxalaMib 6}

axCollectorMib OBJECT IDENTIFIER ::= {axAppEx 28}

axCollExtMonitor OBJECT IDENTIFIER ::= {axCollectorMib 4}

axCollExtMonitorTable OBJECT IDENTIFIER ::= {axCollExtMonitor 1}

オブジェクト ID 値　1.3.6.1.4.1.21839.2.6.28.4.1

（2） 実装仕様

axCollExtMonitorTable の実装仕様を次の表に示します。

表 6.3-5 axCollExtMonitorTable の実装仕様

#	オブジェクト識別子	SYNTAX	アクセス	実装仕様	実装有無
1	axCollExtMonitorTable {axCollExtMonitor 1}	SEQUENCE OF axCollExtMonitorEntry	NA	AX-Collector の外部データ監視における外部データ収集情報テーブル。	Y
2	axCollExtMonitorEntry {axCollExtMonitorTable 1}	axCollExtMonitorEntry	NA	外部データ収集情報テーブルのエントリ。 INDEX { axCollExtMonitorDatasetIndex, axCollExtMonitorMetricsIndex }	Y
3	axCollExtMonitorDatasetIndex {axCollExtMonitorEntry 1}	Integer32	AN	外部データ監視項目のインデックス。	Y
4	axCollExtMonitorMetricsIndex {axCollExtMonitorEntry 2}	Integer32	AN	外部データ監視対象の外部データ監視データのインデックス。	Y
5	axCollExtMonitorDatasetName {axCollExtMonitorEntry 3}	OCTET STRING	AN	外部データ監視項目に設定したデータセット名。	Y
6	axCollExtMonitorMetricsName {axCollExtMonitorEntry 4}	OCTET STRING	AN	外部データ監視対象の外部データ監視データフロー条件グループに設定したメトリクス名。	Y
7	axCollExtMonitorValue {axCollExtMonitorEntry 5}	Counter64	AN	フロー監視対象のフロー条件グループ毎に収集した値。 1 未満（小数点以下）は切り捨て 負の値の場合は 0 を格納する。 18,446,744,073,709,551,615 を超える値は 18,446,744,073,709,551,615 を格納する。	Y

6.3.6 axCollExtThreshold

AX-Collector の外部データ監視機能の閾値監視情報に関する MIB です。

(1) 識別子

axCollExtThreshold OBJECT IDENTIFIER ::= {axCollExtMonitor 2}

オブジェクト ID 値　1.3.6.1.4.1.21839.2.6.28.4.2

(2) 実装仕様

axCollExtThreshold の実装仕様を次の表に示します。

表 6.3-6 axCollExtThreshold の実装仕様

#	オブジェクト識別子	SYNTAX	アクセス	実装仕様	実装有無
1	axCollExtThresholdDetectTime {axCollExtThreshold 1}	OCTET STRING	AN	外部データ監視で閾値超えを検知した日時。 "YYYY-MM-DDThh:mm:ss+ 09:00"で示します。 ・ YYYY：年 ・ MM：月 ・ DD：日 ・ hh：時 ・ mm：分 ・ ss：秒	Y
2	axCollExtThresholdRecoverTime {axCollExtThreshold 2}	OCTET STRING	AN	外部データ監視で閾値超えからの復旧を検知した日時。 "YYYY-MM-DDThh:mm:ss+ 09:00"で示します。 ・ YYYY：年 ・ MM：月 ・ DD：日 ・ hh：時 ・ mm：分 ・ ss：秒	Y
3	axCollExtThresholdType {axCollExtThreshold 3}	OCTET STRING	AN	閾値の種別。以下の何れかの文字列。 “upper_threshold”：上限閾値 “lower_threshold”：下限閾値	Y
4	axCollExtThresholdValue {axCollExtThreshold 4}	Counter64	AN	閾値として設定された値。整数値。 負の値の場合は 0 を格納する。	Y

6.3.7 axCollImpulseNotice

AX-Collector の Impulse 連携通知情報に関する MIB です。

（1） 識別子

axAppEx OBJECT IDENTIFIER ::= {alaxalaMib 6}

axCollectorMib OBJECT IDENTIFIER ::= {axAppEx 28}

axCollImpulse OBJECT IDENTIFIER ::= {axCollectorMib 100}

axCollImpulseNotice OBJECT IDENTIFIER ::= {axCollMibMonitor 1}

オブジェクト ID 値　1.3.6.1.4.1.21839.2.6.28.100.1

（2） 実装仕様

axCollImpulseNotice の実装仕様を次の表に示します。

表 6.3-7 axCollImpulseNotice の実装仕様

#	オブジェクト識別子	SYNTAX	アクセス	実装仕様	実装有無
1	axCollImpulseNoticeDetectTime {axCollImpulseNotice 1}	OCTET STRING	AN	Impulse で異常を検知した日時。 "YYYY-MM-DDThh:mm:ss+ 09:00"で示します。 ・ YYYY：年 ・ MM：月 ・ DD：日 ・ hh：時 ・ mm：分 ・ ss：秒	Y
2	axCollImpulseNoticeRecoverTime {axCollImpulseNotice 2}	OCTET STRING	AN	Impulse で異常からの復旧を検知した日時。 "YYYY-MM-DDThh:mm:ss+ 09:00"で示します。 ・ YYYY：年 ・ MM：月 ・ DD：日 ・ hh：時 ・ mm：分 ・ ss：秒	Y
3	axCollImpulseNoticeChar {axCollImpulseNotice 3}	OCTET STRING	AN	Impulse で生成した学習モデルの特性。 “period”：周期性 “corr”：相関 “changepoint”：変化点 “gaussian”：正規性	Y
4	axCollImpulseNoticeRequirement {axCollImpulseNotice 4}	OCTET STRING	AN	Impulse で異常検知した際の検知要件。以下のいずれかの文字列。 “period”：周期崩れ検知 “pos”：急増検知 “neg”：急減検知	Y

				“outlierDetection”：相関崩れ検知 “changeDetection”：変化点検知 “gaussian”：外れ値検知	

6.4 SNMP 通知

AX-Collector でサポートする SNMP 通知について説明します。

6.4.1 SNMP 通知の種類と発行契機

AX-Collector がサポートする SNMP 通知の種類と発行契機を下表に示します。

表 6.4-1 SNMP 通知の種類と発行契機

#	種類	意味	送信契機
1	axCollFlwThresholdDetectTrap	フロー監視の閾値超え検知	フロー監視において，設定した上限検知閾値を上回った，もしくは下限検知閾値を下回ったとき
2	axCollFlwThresholdRecoverTrap	フロー監視の閾値超え復旧	フロー監視において，設定した上限復旧閾値を下回った，もしくは下限復旧閾値を上回ったとき
3	axCollMibThresholdDetectTrap	SNMP 監視の閾値超え検知	SNMP 監視において，設定した上限検知閾値を上回った，もしくは下限検知閾値を下回ったとき
4	axCollMibThresholdRecoverTrap	SNMP 監視の閾値超え復旧	SNMP 監視において，設定した上限復旧閾値を下回った，もしくは下限復旧閾値を上回ったとき
5	axCollExtThresholdDetectTrap	外部データ監視の閾値超え検知	外部データ監視において，設定した上限検知閾値を上回った，もしくは下限検知閾値を下回ったとき
6	axCollExtThresholdRecoverTrap	外部データ監視の閾値超え復旧	外部データ監視において，設定した上限復旧閾値を下回った，もしくは下限復旧閾値を上回ったとき
7	axCollImpulseFlwDetectTrap	Impulse 連携の異常検知	Impulse においてフロー監視情報の異常を検知したとき
8	axCollImpulseFlwRecoverTrap	Impulse 連携の復旧検知	Impulse においてフロー監視情報の異常からの復旧を検知したとき
9	axCollImpulseMibDetectTrap	Impulse 連携の異常検知	Impulse において SNMP 監視情報の異常を検知したとき
10	axCollImpulseMibRecoverTrap	Impulse 連携の復旧検知	Impulse において SNMP 監視情報の異常からの復旧を検知したとき
11	axCollImpulseExtDetectTrap	Impulse 連携の異常検知	Impulse において外部データ監視情報の異常を検知したとき
12	axCollImpulseExtRecoverTrap	Impulse 連携の復旧検知	Impulse において外部データ監視情報の異常からの復旧を検知したとき

6.4.2 PDU 内パラメータ

Trap-PDU パラメータを次の表に示します。

表 6.4-2 Trap-PDU 内パラメーター一覧

#	種類	Trap-PDU データ値		
		Variable-Binding [1](SysUpTime.0)	Variable-Binding [2] (SnmpTrapOID.0)	Variable-Binding [3～]

1	axCollFlwThresholdDetectTrap	sysUpTime の値	axCollFlwThresholdDetectTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.28.2.2.10.0.1)	axCollFlwMonitorItemName, axCollFlwMonitorObjectGroupName, axCollFlwMonitorValue, axCollFlwThresholdDetectTime, axCollFlwThresholdType, axCollFlwThresholdValue
2	axCollFlwThresholdRecoverTrap	sysUpTime の値	axCollFlwThresholdRecoverTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.28.2.2.10.0.2)	axCollFlwMonitorItemName, axCollFlwMonitorObjectGroupName, axCollFlwThresholdRecoverTime, axCollFlwThresholdType
3	axCollMibThresholdDetectTrap	sysUpTime の値	axCollMibThresholdDetectTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.28.3.2.10.0.1)	axCollMibMonitorItemName, axCollMibMonitorObjectGroupName, axCollMibMonitorValue, axCollMibThresholdDetectTime, axCollMibThresholdType, axCollMibThresholdValue
4	axCollMibThresholdRecoverTrap	sysUpTime の値	axCollMibThresholdRecoverTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.28.3.2.10.0.2)	axCollMibMonitorItemName, axCollMibMonitorObjectGroupName, axCollMibThresholdRecoverTime, axCollMibThresholdType
5	axCollExtThresholdDetectTrap	sysUpTime の値	axCollExtThresholdDetectTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.28.4.2.10.0.1)	axCollExtMonitorDatasetName, axCollExtMonitorMetricsName, axCollExtMonitorValue, axCollExtThresholdDetectTime, axCollExtThresholdType, axCollExtThresholdValue
6	axCollExtThresholdRecoverTrap	sysUpTime の値	axCollExtThresholdRecoverTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.28.4.2.10.0.2)	axCollExtMonitorDatasetName, axCollExtMonitorMetricsName, axCollExtThresholdRecoverTime, axCollExtThresholdType
7	axCollImpulseFlwDetectTrap	sysUpTime の値	axCollImpulseFlwDetectTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.28.100.1.10.0.1)	axCollFlwMonitorItemName, axCollFlwMonitorObjectGroupName, axCollFlwMonitorValue, axCollImpulseNoticeDetectTime, axCollImpulseNoticeChar, axCollImpulseNoticeRequirement
8	axCollImpulseFlwRecoverTrap	sysUpTime の値	axCollImpulseFlwRecoverTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.28.100.1.10.0.2)	axCollFlwMonitorItemName, axCollFlwMonitorObjectGroupName, axCollImpulseNoticeRecoverTime, axCollImpulseNoticeChar, axCollImpulseNoticeRequirement

9	axCollImpulseMibDetectTrap	sysUpTime の値	axCollImpulseMibDetectTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.28.100.1.10.0.3)	axCollMibMonitorItemName, axCollMibMonitorObjectGroupName, axCollMibMonitorValue, axCollImpulseNoticeDetectTime, axCollImpulseNoticeChar, axCollImpulseNoticeRequirement
10	axCollImpulseMibRecoverTrap	sysUpTime の値	axCollImpulseMibRecoverTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.28.100.1.10.0.4)	axCollMibMonitorItemName, axCollMibMonitorObjectGroupName, axCollImpulseNoticeRecoverTime, axCollImpulseNoticeChar, axCollImpulseNoticeRequirement
11	axCollImpulseExtDetectTrap	sysUpTime の値	axCollImpulseExtDetectTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.28.100.1.10.0.5)	axCollExtMonitorDatasetName, axCollExtMonitorMetricsName, axCollExtMonitorValue, axCollImpulseNoticeDetectTime, axCollImpulseNoticeChar, axCollImpulseNoticeRequirement
12	axCollImpulseExtRecoverTrap	sysUpTime の値	axCollImpulseExtRecoverTrap のオブジェクト ID (1.3.6.1.4.1.21839.2.6.28.100.1.10.0.6)	axCollExtMonitorDatasetName, axCollExtMonitorMetricsName, axCollImpulseNoticeRecoverTime, axCollImpulseNoticeChar, axCollImpulseNoticeRequirement

7. REST API

この章では，AX-Collector が提供する REST API のインタフェース仕様について説明します。

7.1 認証

REST API は認証方式として，ベーシック認証とトークン認証をサポートしています。認証に関する設定および利用方法は 5.6.5「（4）ユーザ管理」を参照してください。

7.1.1 認証トークン情報取得 API

本 API をコールしたユーザの認証トークン情報(発行日時／有効期限)を取得します。

表 7-1 認証トークン情報取得 API

<table>
<tr><td>#</td><td>項目</td><td>説明</td><td colspan="3"></td></tr>
<tr><td>1</td><td>メソッド</td><td colspan="4">GET</td></tr>
<tr><td>2</td><td>URI</td><td colspan="4">/api/v1/token/</td></tr>
<tr><td>3</td><td rowspan="3">リクエスト</td><td>認証</td><td colspan="3">ベーシック認証もしくはトークン認証。</td></tr>
<tr><td>4</td><td>クエリパラメータ</td><td colspan="3">なし</td></tr>
<tr><td>5</td><td>Content-Type</td><td colspan="3">application/json</td></tr>
<tr><td>6</td><td rowspan="4">レスポンス</td><td>レスポンス
ステータス</td><td colspan="3">以下のステータスコードを応答します。
コード：内容
200：成功
401：認証エラー
404：未検出
500：内部エラー</td></tr>
<tr><td>7</td><td>Content-Type</td><td colspan="3">application/json</td></tr>
<tr><td>8</td><td>レスポンス
ボディ：

ステータスコード=200 の場合</td><td colspan="3">・例
{
"register_date": "2023-11-20T17:39:43.869628+09:00",
"expired_date": "2023-12-20T17:39:43.869628+09:00"
}

・パラメータ説明
パラメータ名 ｜ 型 ｜ 説明
register_date ｜ String ｜ 発行日時。
expired_date ｜ String ｜ 有効期限。（無期限の場合は null を応答します。）</td></tr>
<tr><td>9</td><td>レスポンス
ボディ：

ステータスコード=200 以外の場合</td><td colspan="3">・例
{
"detail": "不正なトークンです。"
}

・パラメータ説明
パラメータ名 ｜ 型 ｜ 説明
detail ｜ String ｜ エラー詳細を格納します。</td></tr>
</table>

7.2 データ監視関連 API

7.2.1 外部データ監視 外部データ抽入 API

外部サーバ等から AX-Collector へ外部監視機能の外部データを注入します。

データ抽入には，AX-Collector に外部収集データ設定が必要です。5.5.4 外部データ監視（5）環境設定で，外部データ抽入 API 設定登録を有効にしている場合は，本 API にて外部収集データの設定が実施されます。

表 7-2 外部データ監視 外部データ注入 API

#	項目	説明	
1	メソッド	POST	
2	URI	/api/v1/monitoring/external/data/	
3	リクエスト	認証	ベーシック認証もしくはトークン認証。 管理者および標準ユーザ権限のユーザで認証できます。
4		クエリパラメータ	なし
5		Content-Type	application/json

6		ボディパラメータ	・例
			{
			"ext_data": [
			{
			"category": "category_A",
			"dataname": "data_A",
			"timestamp": "2020-06-15T10:00:00+09:00",
			"value": 1234.5
			},
			{
			"category": "category_B",
			"dataname": "data_B",
			"timestamp": "2020-06-15T10:00:00+09:00",
			"failed": true,
			"failed_cause": "Error"
			}
			]
			}
			・パラメータ説明（*必須パラメータ）

パラメータ名	型	説明
ext_data*	List	外部データリスト。 最大数：100 リスト。
category	String	カテゴリ名。最大 128 文字。 英数字とアンダーバー(_)を使用可。省略時:_none_
dataname*	String	データ名。最大 128 文字。 英数字とアンダーバー(_)を使用可。
timestamp*	String	時刻。ISO8601 フォーマット。 （例)2019-03-04T11:16:47+09:00

<table>
<tr><th>#</th><th>項目</th><th>説明</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>failed</td><td>Boolean</td><td>注入データの取得に失敗した場合，true。デフォルトは false。</td></tr>
<tr><td>failed_cause</td><td>String</td><td>failed が true の場合，注入データの取得失敗要因を設定。
最大 128 文字。
アスキー文字のみ使用可。</td></tr>
<tr><td>value</td><td>Number</td><td>監視対象の値
(倍精度浮動小数点数)</td></tr>
</table>
</td></tr>
<tr><td>7</td><td>レスポンス</td><td>レスポンス
ステータス</td><td>以下のステータスコードを応答します。
<table>
<tr><td>コード</td><td>内容</td></tr>
<tr><td>200</td><td>成功</td></tr>
<tr><td>400</td><td>要求不正エラー</td></tr>
<tr><td>401</td><td>認証エラー</td></tr>
<tr><td>403</td><td>アクセス権限なし
（参照ユーザはアクセス不可）</td></tr>
<tr><td>408</td><td>タイムアウト</td></tr>
<tr><td>500</td><td>内部エラー</td></tr>
<tr><td>503</td><td>サービス利用不可</td></tr>
</table>
</td></tr>
<tr><td>8</td><td></td><td>Content-Type</td><td>application/json</td></tr>
<tr><td>9</td><td></td><td>レスポンス
ボディ：

ステータスコード
=200 の場合</td><td>・例
<pre>{
  "results": [
    {
      "category": "category_A",
      "dataname": "data_A",
      "timestamp": "2020-06-15T10:00:00+09:00",
      "result": true
    },
    {
      "category": "category_B",
      "datename": "data_B",
      "timestamp": "2020-06-15T10:00:00+09:00",
      "result": false,
      "cause": "Invalid category or dataname; ..."
    }
  ]
}</pre>
・パラメータ説明
<table>
<tr><td>パラメータ名</td><td>型</td><td>説明</td></tr>
<tr><td>results</td><td>List</td><td>応答リスト。</td></tr>
<tr><td>category</td><td>String</td><td>カテゴリ名。</td></tr>
<tr><td>dataname</td><td>String</td><td>データ名。</td></tr>
<tr><td>timestamp</td><td>String</td><td>時刻。</td></tr>
<tr><td>result</td><td>Boolean</td><td>登録成功時，true。
登録失敗時，false。</td></tr>
<tr><td>cause</td><td>String</td><td>result が false の場合，要因を設定。</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>#</th><th>項目</th><th>説明</th><th></th></tr>
<tr><td>10</td><td></td><td>レスポンス
ボディ：

ステータスコード
=200 以外の場合</td><td>・例
{
"detail": "データ収集設定が有効になっていません。"
}

・パラメータ説明
<table><tr><th>パラメータ名</th><th>型</th><th>説明</th></tr><tr><td>detail</td><td>String</td><td>エラー詳細を格納します。</td></tr></table></td></tr>
</table>

7.2.2 外部データ監視 外部収集データ設定 API

AX-Collector 外部データ監視機能の外部収集データ設定の操作を実施します。

取得（GET），新規登録（POST），更新（PUT），削除（DELETE）の操作が可能です。

表 7-3 外部データ監視 外部収集データ設定取得（GET）API

<table>
<tr><th>#</th><th>項目</th><th>説明</th><th></th></tr>
<tr><td>1</td><td>メソッド</td><td>GET</td><td></td></tr>
<tr><td>2</td><td>URI</td><td>/api/v1/monitoring/external/external-data/</td><td></td></tr>
<tr><td>3</td><td>リクエスト</td><td>認証</td><td>ベーシック認証もしくはトークン認証</td></tr>
<tr><td>4</td><td></td><td>クエリパラメータ</td><td>取得対象の設定を絞り込む条件を指定します。
・パラメータ説明（*必須パラメータ）
<table><tr><th>パラメータ名</th><th>型</th><th>説明</th></tr><tr><td>id</td><td>Integer</td><td>外部抽入データ設定 ID</td></tr><tr><td>display_category</td><td>String</td><td>カテゴリ名</td></tr><tr><td>display_dataname</td><td>String</td><td>外部データ名</td></tr><tr><td>category</td><td>String</td><td>カテゴリ名（入力データ）</td></tr><tr><td>dataname</td><td>String</td><td>データ名（入力データ）</td></tr><tr><td>collection</td><td>Boolean</td><td>外部データ収集</td></tr></table></td></tr>
<tr><td>5</td><td></td><td>Content-Type</td><td>application/json</td></tr>
<tr><td>6</td><td></td><td>ボディパラメータ</td><td>なし</td></tr>
<tr><td>7</td><td>レスポンス</td><td>レスポンス
ステータス</td><td>以下のステータスコードを応答します。
<table><tr><th>コード</th><th>内容</th></tr><tr><td>200</td><td>成功</td></tr><tr><td>400</td><td>要求不正エラー</td></tr><tr><td>401</td><td>認証エラー</td></tr><tr><td>403</td><td>アクセス権限なし</td></tr><tr><td>408</td><td>タイムアウト</td></tr><tr><td>500</td><td>内部エラー</td></tr><tr><td>503</td><td>サービス利用不可</td></tr></table></td></tr>
<tr><td>8</td><td></td><td>Content-Type</td><td>application/json</td></tr>
</table>

<table>
<tr><th>#</th><th>項目</th><th colspan="2">説明</th></tr>
<tr><td>9</td><td></td><td>レスポンス
ボディ：

ステータスコード
=200 の場合</td><td>・例
{
"results": [
{
"id": 1,
"display_category": "disp_category_A",
"display_dataname": "disp_data_A",
"category": "category_A",
"dataname": "data_A",
"description": "description_A",
"collection": true
},
{
"id": 2,
"display_category": "disp_category_B",
"display_dataname": "disp_data_B",
"category": "category_B",
"datename": "data_B",
"description": "description_B",
"collection": true
}
]
}

・パラメータ説明
<table><tr><th>パラメータ名</th><th>型</th><th>説明</th></tr><tr><td>results</td><td>List</td><td>応答リスト</td></tr><tr><td>id</td><td>Integer</td><td>ID</td></tr><tr><td>display_category</td><td>String</td><td>カテゴリ名</td></tr><tr><td>display_dataname</td><td>String</td><td>外部データ名</td></tr><tr><td>category</td><td>String</td><td>カテゴリ名（入力データ）</td></tr><tr><td>dataname</td><td>String</td><td>データ名（入力データ）</td></tr><tr><td>collection</td><td>Boolean</td><td>外部データ収集</td></tr></table></td></tr>
<tr><td>10</td><td></td><td>レスポンス
ボディ：

ステータスコード
=200 以外の場合</td><td>・例
{
"detail": "ユーザ名かパスワードが違います。"
}

・パラメータ説明
<table><tr><th>パラメータ名</th><th>型</th><th>説明</th></tr><tr><td>detail</td><td>String</td><td>エラー詳細を格納します。</td></tr></table></td></tr>
</table>

表 7-4　外部データ監視 外部収集データ設定新規登録（POST）API

#	項目	説明	
1	メソッド	POST	
2	URI	/api/v1/monitoring/external/external-data/	
3	リクエスト	認証	ベーシック認証もしくはトークン認証 管理者および標準ユーザ権限のユーザで認証できます。
4		クエリパラメータ	なし
5		Content-Type	application/json

<table>
<tr><th>#</th><th>項目</th><th>説明</th><th></th></tr>
<tr><td>6</td><td></td><td>ボディパラメータ</td><td>新規登録する外部収集データ設定を指定します。
最大 20 件を同時に登録指定可能です。

・例
{
"ext_data": [
{
"display_dataname": "disp_data_A",
"dataname": "data_A"
},
{
"display_category": "disp_category_B",
"display_dataname": "disp_data_B",
"category": "category_B",
"dataname": "data_B",
"description": "description_B",
"collection": true
}
]
}

・パラメータ説明（*必須パラメータ）
<table><tr><th>パラメータ名</th><th>型</th><th>説明</th></tr><tr><td>ext_data *</td><td>List</td><td>新規登録設定リスト
最大 20 件</td></tr><tr><td>display_category</td><td>String</td><td>カテゴリ名</td></tr><tr><td>display_dataname *</td><td>String</td><td>外部データ名</td></tr><tr><td>category</td><td>String</td><td>カテゴリ名（入力データ）</td></tr><tr><td>dataname *</td><td>String</td><td>データ名（入力データ）</td></tr><tr><td>description</td><td>String</td><td>補足説明</td></tr><tr><td>collection</td><td>Boolean</td><td>外部データ収集</td></tr></table></td></tr>
<tr><td>7</td><td>レスポンス</td><td>レスポンス
ステータス</td><td>以下のステータスコードを応答します。
<table><tr><th>コード</th><th>内容</th></tr><tr><td>200</td><td>成功</td></tr><tr><td>400</td><td>要求不正エラー</td></tr><tr><td>401</td><td>認証エラー</td></tr><tr><td>403</td><td>アクセス権限なし
（参照ユーザはアクセス不可）</td></tr><tr><td>408</td><td>タイムアウト</td></tr><tr><td>500</td><td>内部エラー</td></tr><tr><td>503</td><td>サービス利用不可</td></tr></table></td></tr>
<tr><td>8</td><td></td><td>Content-Type</td><td>application/json</td></tr>
</table>

<table>
<tr><th>#</th><th>項目</th><th>説明</th></tr>
<tr><td>9</td><td></td><td>レスポンス
ボディ：

ステータスコード
=200 の場合</td><td>新規登録処理結果が格納されます。

・例
{
"results": [
{
"id": 1,
"display_category": "（未設定）",
"display_dataname": "disp_data_A",
"category": "_none_",
"dataname": "data_A",
"description": "",
"collection": true,
"result": true,
"cause": ""
},
{
"id": 2,
"display_category": "disp_category_B",
"display_dataname": "disp_data_B",
"category": "category_B",
"datename": "data_B",
"description": "description_B",
"collection": true,
"result": true,
"cause": ""
}
]
}

・パラメータ説明
<table><tr><th>パラメータ名</th><th>型</th><th>説明</th></tr><tr><td>results</td><td>List</td><td>応答リスト</td></tr><tr><td>id</td><td>Integer</td><td>ID</td></tr><tr><td>display_category</td><td>String</td><td>カテゴリ名</td></tr><tr><td>display_dataname</td><td>String</td><td>外部データ名</td></tr><tr><td>category</td><td>String</td><td>カテゴリ名（入力データ）</td></tr><tr><td>dataname</td><td>String</td><td>データ名（入力データ）</td></tr><tr><td>description</td><td>String</td><td>補足説明</td></tr><tr><td>collection</td><td>Boolean</td><td>外部データ収集</td></tr><tr><td>result</td><td>Boolean</td><td>登録成功時，true。
登録失敗時，false。</td></tr><tr><td>cause</td><td>String</td><td>result が false の場合，要因を設定。</td></tr></table></td></tr>
<tr><td>10</td><td></td><td>レスポンス
ボディ：

ステータスコード
=200 以外の場合</td><td>・例
{
"detail": "ユーザ名かパスワードが違います。"
}

・パラメータ説明
<table><tr><th>パラメータ名</th><th>型</th><th>説明</th></tr><tr><td>detail</td><td>String</td><td>エラー詳細を格納します。</td></tr></table></td></tr>
</table>

表 7-5　外部データ監視 外部収集データ設定更新（PUT）API

#	項目	説明	
1	メソッド	PUT	
2	URI	/api/v1/monitoring/external/external-data/	
3	リクエスト	認証	ベーシック認証もしくはトークン認証 管理者および標準ユーザ権限のユーザで認証できます。
4		クエリパラメータ	なし
5		Content-Type	application/json

6		ボディパラメータ	更新する登録済みの外部収集データ設定を指定します。
			最大 20 件を同時に更新指定可能です。
			更新対象データを特定する ID は必須です。
			
			・例
			{
			"ext_data": [
			{
			"id": 1,
			"description": "updated description_A"
			},
			{
			"id": 2,
			"collection": false
			}
			]
			}
			
			・パラメータ説明（*必須パラメータ）

パラメータ名	型	説明
ext_data *	List	新規登録設定リスト 最大 20 件
id *	Integer	更新対象の ID
display_category	String	更新後のカテゴリ名
display_dataname	String	更新後の外部データ名
category	String	更新後のカテゴリ名（入力データ）
dataname	String	更新後のデータ名（入力データ）
description	String	更新後の補足説明
collection	Boolean	更新後の外部データ収集

<table>
<tr><th>#</th><th>項目</th><th>説明</th><th></th></tr>
<tr><td>7</td><td>レスポンス</td><td>レスポンス
ステータス</td><td>以下のステータスコードを応答します。<table><tr><th>コード</th><th>内容</th></tr><tr><td>200</td><td>成功</td></tr><tr><td>400</td><td>要求不正エラー</td></tr><tr><td>401</td><td>認証エラー</td></tr><tr><td>403</td><td>アクセス権限なし
（参照ユーザはアクセス不可）</td></tr><tr><td>408</td><td>タイムアウト</td></tr><tr><td>500</td><td>内部エラー</td></tr><tr><td>503</td><td>サービス利用不可</td></tr></table></td></tr>
<tr><td>8</td><td></td><td>Content-Type</td><td>application/json</td></tr>
</table>

<table>
<tr><th>#</th><th>項目</th><th>説明</th></tr>
<tr><td>9</td><td></td><td>レスポンス
ボディ：

ステータスコード
=200 の場合</td><td>更新処理結果が格納されます。

・例
{
"results": [
{
"id": 1,
"display_category": "disp_category_A",
"display_dataname": "disp_data_A",
"category": "category_A",
"dataname": "data_A",
"description": "updated description_A",
"collection": true,
"result": true,
"cause": ""
},
{
"id": 2,
"display_category": "disp_category_B",
"display_dataname": "disp_data_B",
"category": "category_B",
"datename": "data_B",
"description": "description_B",
"collection": false,
"result": true,
"cause": ""
}
]
}

・パラメータ説明
<table><tr><th>パラメータ名</th><th>型</th><th>説明</th></tr><tr><td>results</td><td>List</td><td>応答リスト</td></tr><tr><td>id</td><td>Integer</td><td>ID</td></tr><tr><td>display_category</td><td>String</td><td>カテゴリ名</td></tr><tr><td>display_dataname</td><td>String</td><td>外部データ名</td></tr><tr><td>category</td><td>String</td><td>カテゴリ名（入力データ）</td></tr><tr><td>dataname</td><td>String</td><td>データ名（入力データ）</td></tr><tr><td>description</td><td>String</td><td>補足説明</td></tr><tr><td>collection</td><td>Boolean</td><td>外部データ収集</td></tr><tr><td>result</td><td>Boolean</td><td>登録成功時，true。
登録失敗時，false。</td></tr><tr><td>cause</td><td>String</td><td>result が false の場合，要因を設定。</td></tr></table></td></tr>
<tr><td>10</td><td></td><td>レスポンス
ボディ：

ステータスコード
=200 以外の場合</td><td>・例
{
"detail": "ユーザ名かパスワードが違います。"
}

・パラメータ説明
<table><tr><th>パラメータ名</th><th>型</th><th>説明</th></tr><tr><td>detail</td><td>String</td><td>エラー詳細を格納します。</td></tr></table></td></tr>
</table>

表 7-6　外部データ監視 外部収集データ設定削除（DELETE）API

<table>
<tr><th>#</th><th>項目</th><th colspan="2">説明</th></tr>
<tr><td>1</td><td>メソッド</td><td colspan="2">DELETE</td></tr>
<tr><td>2</td><td>URI</td><td colspan="2">/api/v1/monitoring/external/external-data/</td></tr>
<tr><td>3</td><td rowspan="4">リクエスト</td><td>認証</td><td>ベーシック認証もしくはトークン認証
管理者および標準ユーザ権限のユーザで認証できます。</td></tr>
<tr><td>4</td><td>クエリパラメータ</td><td>なし</td></tr>
<tr><td>5</td><td>Content-Type</td><td>application/json</td></tr>
<tr><td>6</td><td>ボディパラメータ</td><td>削除する登録済みの外部収集データ設定を指定します。
最大 20 件を同時に削除指定可能です。
削除対象データを特定する ID または(category,dataname の組)または(display_category, display_dataname の組)のいずれかは必須です。

・例
{
"ext_data": [
{
"id": 1
},
{
"category": "category_B",
"dataname": "data_B"
}
]
}

・パラメータ説明（*必須パラメータ）
<table><tr><th>パラメータ名</th><th>型</th><th>説明</th></tr><tr><td>ext_data *</td><td>List</td><td>新規登録設定リスト
最大 20 件</td></tr><tr><td>id</td><td>Integer</td><td>ID</td></tr><tr><td>display_category</td><td>String</td><td>カテゴリ名</td></tr><tr><td>display_dataname</td><td>String</td><td>外部データ名</td></tr><tr><td>category</td><td>String</td><td>カテゴリ名（入力データ）</td></tr><tr><td>dataname</td><td>String</td><td>更新後のデータ名（入力データ）</td></tr></table></td></tr>
<tr><td>7</td><td>レスポンス</td><td>レスポンス
ステータス</td><td>以下のステータスコードを応答します。
<table><tr><th>コード</th><th>内容</th></tr><tr><td>200</td><td>成功</td></tr><tr><td>400</td><td>要求不正エラー</td></tr><tr><td>401</td><td>認証エラー</td></tr><tr><td>403</td><td>アクセス権限なし
（参照ユーザはアクセス不可）</td></tr><tr><td>408</td><td>タイムアウト</td></tr><tr><td>500</td><td>内部エラー</td></tr><tr><td>503</td><td>サービス利用不可</td></tr></table></td></tr>
</table>

<table>
<tr><td>#</td><td>項目</td><td>説明</td><td></td></tr>
<tr><td>8</td><td></td><td>Content-Type</td><td>application/json</td></tr>
<tr><td>9</td><td></td><td>レスポンス
ボディ：

ステータスコード
=200 の場合</td><td>削除処理結果が格納されます。
result, cause 以外のフィールドはリクエスト時のパラメータが格納されます。

・例
{
"ext_data": [
{
"id": 1,
"result": true,
"cause": ""
},
{
"category": "category_B",
"dataname": "data_B",
"result": true,
"cause": ""
}
]
}

・パラメータ説明
<table><tr><td>パラメータ名</td><td>型</td><td>説明</td></tr><tr><td>results</td><td>List</td><td>応答リスト</td></tr><tr><td>id</td><td>Integer</td><td>ID</td></tr><tr><td>display_category</td><td>String</td><td>カテゴリ名</td></tr><tr><td>display_dataname</td><td>String</td><td>外部データ名</td></tr><tr><td>category</td><td>String</td><td>カテゴリ名（入力データ）</td></tr><tr><td>dataname</td><td>String</td><td>データ名（入力データ）</td></tr><tr><td>description</td><td>String</td><td>補足説明</td></tr><tr><td>collection</td><td>Boolean</td><td>外部データ収集</td></tr><tr><td>result</td><td>Boolean</td><td>削除成功時，true。
削除失敗時，false。</td></tr><tr><td>cause</td><td>String</td><td>result が false の場合，要因を設定。</td></tr></table></td></tr>
<tr><td>10</td><td></td><td>レスポンス
ボディ：

ステータスコード
=200 以外の場合</td><td>・例
{
"detail": "ユーザ名かパスワードが違います。"
}

・パラメータ説明
<table><tr><td>パラメータ名</td><td>型</td><td>説明</td></tr><tr><td>detail</td><td>String</td><td>エラー詳細を格納します。</td></tr></table></td></tr>
</table>

7.2.3 SNMP 監視 CSV データ取得 API

SNMP 監視機能で収集した監視データを取得します。指定した監視項目毎 CSV 形式データファイル一式をアーカイブした zip ファイルをダウンロードします。

ダウンロードする監視データと形式は，WEB インタフェース（5.4.3SNMP 監視（4）参照）と同じです。

表 7-7 SNMP 監視 CSV データ取得 API

#	項目	説明	
1	メソッド	POST	
2	URI	/api/v1/snmp/export_csv/	
3	リクエスト	認証	ベーシック認証もしくはトークン認証。
4		クエリパラメータ	なし
5		Content-Type	application/json

6		ボディパラメータ	・例
			{
			"date_from": "2022-08-01",
			"date_to": "2022-08-07”,
			"monitoring_item": ["SNMP_A"],
			"csv_type": "impulse"
			}
			
			・パラメータ説明（*必須パラメータ）
			date_from/date_to または，time_from/time_to のいずれかの組み合わせで検索期間を指定します。

パラメータ名	型	説明
date_from*	String	検索期間の開始日。 (例) 2022-08-01
date_to*	String	検索期間の終了日。 (例) 2022-08-07
time_from *	String	検索期間の開始時刻。 (例) 2023-01-01T09:00:00+09:00
time_to *	String	検索期間の終了時刻。 (例) 2023-01-01T09:30:00+09:00
monitoring_item*	List	SNMP 監視項目名
	String	SNMP 監視項目名 (例)SNMP_A
object_group	List	SNMP 監視項目が 1 つの場合に，指定可能な MIB オブジェクトグループ名。 省略時：指定した SNMP 監視項目中の全 MIB オブジェクトグループ。
	String	MIB オブジェクトグループ名。 (例)data1

#	項目	説明			
			csv_type	Enum	出力 CSV ファイル形式。 impulse: impulse に取り込み可能な形式。 省略時：コレクタ形式。時系列に複数データが並びます。
7	レスポンス	レスポンス ステータス	以下のステータスコードを応答します。 コード：内容 200：成功 400：要求不正エラー 401：認証エラー 500：内部エラー		
8		Content-Type	application/json		
9		Content-Disposition	attachment; filename 保存に使用可能な zip ファイル名を記載しています。 (例) ml_ax-collector-snmp_20220801-20220808.zip		
10		レスポンス ボディ： ステータスコード=200 の場合	指定期間の各監視項目の CSV 形式データファイル一式をアーカイブした zip 形式ファイルデータ。		

11		レスポンス
		ボディ：
		
		ステータスコード=200 以外の場合
			・例
			{
			"detail": "ユーザ名かパスワードが違います。"
			}
			
			・パラメータ説明
			パラメータ名：型：説明
			detail：String：エラー詳細を格納します。		

7.2.4 フロー監視 CSV データ取得 API

フロー監視機能で収集した監視データを取得します。指定した監視項目毎 CSV 形式データファイル一式をアーカイブした zip ファイルをダウンロードします。

ダウンロードする監視データと形式は，WEB インタフェース（5.4.4 フロー監視（3）参照）と同じです。

表 7-8 フロー監視 CSV データ取得 API

#	項目	説明	
1	メソッド	POST	
2	URI	/api/v1/flow/export_csv/	
3	リクエスト	認証	ベーシック認証もしくはトークン認証。
4		クエリパラメータ	なし
5		Content-Type	application/json
6		ボディパラメータ	・例 {

<table>
<tr><th>#</th><th>項目</th><th>説明</th><th></th></tr>
<tr><td></td><td></td><td></td><td>
"date_from": "2022-08-01",
"date_to": "2022-08-07”,
"monitoring_item": ["FLOW_A"],
"csv_type": "impulse"
}

・パラメータ説明（*必須パラメータ）
date_from/date_to または，time_from/time_to のいずれかの組み合わせで検索期間を指定します。
<table>
<tr><th>パラメータ名</th><th>型</th><th>説明</th></tr>
<tr><td>date_from*</td><td>String</td><td>検索期間の開始日。
(例) 2022-08-01</td></tr>
<tr><td>date_to*</td><td>String</td><td>検索期間の終了日。
(例) 2022-08-07</td></tr>
<tr><td>time_from *</td><td>String</td><td>検索期間の開始時刻。
(例) 2023-01-01T09:00:00+09:00</td></tr>
<tr><td>time_to *</td><td>String</td><td>検索期間の終了時刻。
(例) 2023-01-01T09:30:00+09:00</td></tr>
<tr><td>monitoring_item*</td><td>List</td><td>フロー監視項目名</td></tr>
<tr><td>　</td><td>String</td><td>フロー監視項目名
(例)SNMP_A</td></tr>
<tr><td>object_group</td><td>List</td><td>フロー監視項目が１つの場合に，指定可能なフロー条件グループ名。
省略時：指定したフロー監視項目中の全フロー条件グループ。</td></tr>
<tr><td>　</td><td>String</td><td>フロー条件グループ名。
(例)data1</td></tr>
<tr><td>csv_type</td><td>Enum</td><td>出力 CSV ファイル形式。
impulse: impulse に取り込み可能な形式。
省略時：コレクタ形式。時系列に複数データが並びます。</td></tr>
</table>
</td></tr>
<tr><td>7</td><td>レスポンス</td><td>レスポンスステータス</td><td>以下のステータスコードを応答します。
<table>
<tr><th>コード</th><th>内容</th></tr>
<tr><td>200</td><td>成功</td></tr>
<tr><td>400</td><td>要求不正エラー</td></tr>
<tr><td>401</td><td>認証エラー</td></tr>
<tr><td>500</td><td>内部エラー</td></tr>
</table>
</td></tr>
<tr><td>8</td><td></td><td>Content-Type</td><td>application/json</td></tr>
<tr><td>9</td><td></td><td>Content-Disposition</td><td>attachment; filename
保存に使用可能な zip ファイル名を記載しています。
(例) ml_ax-collector-flow_20220801-20220808.zip</td></tr>
</table>

#	項目	説明	
10		レスポンス ボディ： ステータスコード =200 の場合	指定期間の各監視項目の CSV 形式データファイル一式を アーカイブした zip 形式ファイルデータ。

11		レスポンス
		ボディ：
		
		ステータスコード
		=200 以外の場合
			・例
			{
			"detail": "ユーザ名かパスワードが違います。"
			}
			
			・パラメータ説明

パラメータ名	型	説明
detail	String	エラー詳細を格納します。

7.2.5 外部データ監視 CSV データ取得 API

外部データ監視機能で収集した監視データを取得します。指定した監視項目毎 CSV 形式データファイル一式をアーカイブした zip ファイルをダウンロードします。

ダウンロードする監視データと形式は，WEB インタフェース（5.4.6 外部データ監視（4）参照）と同じです。

表 7-9 外部データ監視 CSV データ取得 API

#	項目	説明	
1	メソッド	POST	
2	URI	/api/v1/external/export_csv/	
3	リクエスト	認証	ベーシック認証もしくはトークン認証。
4		クエリパラメータ	なし
5		Content-Type	application/json

6		ボディパラメータ	・例
			{
			"date_from": "2022-08-01",
			"date_to": "2022-08-07”,
			"monitoring_item": [
			{
			"category":"CATEGORY_A",
			"name":"EXTERNAL_A"
			}
			],
			"csv_type": "impulse"
			}
			
			・パラメータ説明（*必須パラメータ）
			date_from/date_to または，time_from/time_to のいずれかの組み合わせで検索期間を指定します。

<table>
<tr><th>#</th><th>項目</th><th>説明</th></tr>
<tr><td></td><td></td><td></td></tr>
</table>

パラメータ名	型	説明
date_from*	String	検索期間の開始日。 (例) 2022-08-01
date_to*	String	検索期間の終了日。 (例) 2022-08-07
time_from *	String	検索期間の開始時刻。 (例) 2023-01-01T09:00:00+09:00
time_to *	String	検索期間の終了時刻。 (例) 2023-01-01T09:30:00+09:00
monitoring_item*	List	外部監視項目名
Category	String	外部監視項目カテゴリ名 (例)CATEGORY_A
name*	String	外部監視項目データ名 (例)EXTERNAL_A
object_group	List	外部監視項目が 1 つの場合に，指定可能な外部監視データ名。 省略時：指定した外部監視項目中の全外部監視データ。 (例)DATA_CATEGORY1
category	String	外部監視データのカテゴリ名。 (例) data1
name*	String	外部監視データのデータ名
csv_type	Enum	出力 CSV ファイル形式。 impulse: impulse に取り込み可能な形式。 省略時：コレクタ形式。時系列に複数データが並びます。

#	項目	説明	
7	レスポンス	レスポンスステータス	以下のステータスコードを応答します。
8		Content-Type	application/json
9		Content-Disposition	attachment; filename 保存に使用可能な zip ファイル名を記載しています。 (例) ml_ax-collector-external_20220801-20220808.zip
10		レスポンスボディ： ステータスコード=200 の場合	指定期間の各監視項目の CSV 形式データファイル一式をアーカイブした zip 形式ファイルデータ。

コード	内容
200	成功
400	要求不正エラー
401	認証エラー
500	内部エラー

<table>
<tr><th>#</th><th>項目</th><th>説明</th><th></th></tr>
<tr><td>11</td><td></td><td>レスポンス
ボディ：

ステータスコード
=200 以外の場合</td><td>・例
{
"detail": "ユーザ名かパスワードが違います。"
}

・パラメータ説明
<table><tr><th>パラメータ名</th><th>型</th><th>説明</th></tr><tr><td>detail</td><td>String</td><td>エラー詳細を格納します。</td></tr></table></td></tr>
</table>

7.3 IP フロー情報検索 API

7.3.1 IP フロー バイト数ランキング取得 API

IP フロー情報を検索し，バイト数ランキング上位のパケット情報を取得します。

表 7-10 IP フロー バイト数ランキング取得 API

<table>
<tr><th>#</th><th>項目</th><th colspan="2">説明</th></tr>
<tr><td>1</td><td>メソッド</td><td colspan="2">POST</td></tr>
<tr><td>2</td><td>URI</td><td colspan="2">/api/v1/flowdata/ip/ranking/bytes/
または
/api/v1/flowdata/ipv4/ranking/bytes/</td></tr>
<tr><td>3</td><td rowspan="4">リクエスト</td><td>認証</td><td>ベーシック認証もしくはトークン認証。</td></tr>
<tr><td>4</td><td>クエリパラメータ</td><td>なし</td></tr>
<tr><td>5</td><td>Content-Type</td><td>application/json</td></tr>
<tr><td>6</td><td>ボディパラメータ</td><td>・例
{
"time_from": "2021-01-11T10:00:00+09:00",
"time_to": "2021-01-11T12:00:00+09:00",
"numbers":10,
"search_filters":{
"packet_field" : [
[{"src_vlan":4000 }, {"src_vlan":3000}]
]
},
"aggregate_groups": {
"src_vlan":false,
"ipv4_src_addr":true
}
}

・パラメータ説明（*必須パラメータ）
<table>
<tr><th>パラメータ名</th><th>型</th><th>説明</th></tr>
<tr><td>time_from *</td><td>String</td><td>検索時刻 - 始まり。ISO8601 フォーマット。（例）2021-01-11T10:00:00+09:00</td></tr>
<tr><td>time_to *</td><td>String</td><td>検索時刻 - 終わり。ISO8601 フォーマット。（例）2021-01-11T12:00:00+09:00</td></tr>
<tr><td>numbers</td><td>integer</td><td>取得する検索結果数。指定範囲は，1～100000。省略時：10。</td></tr>
<tr><td>search_filters</td><td>Object</td><td>検索フィルタ条件</td></tr>
</table>
</td></tr>
</table>

#	項目	説明				
				sensor_addr	String	センサ IPv4 アドレス（ネットフローパケット送信元 IP アドレス）
				monitor_port_ifindex	Integer	センサモニタポート SNMP ifIndex
				output_port_ifindex	Integer	送信ポート SNMP ifIndex
				mac_kind	String	MAC アドレス種別（ユニキャスト，マルチキャスト，ブロードキャスト） unicast, broadcast, multicast, unicast_broadcast, unicast_multicast, broadcast_multicast, all
				ip_kind	String	IPv4 アドレス種別（ユニキャスト＋ブロードキャスト，マルチキャスト） unicast_broadcast, multicast, all
				ipv6_kind	String	IPv6 アドレス種別 all：すべて unicast：ユニキャスト multicast：マルチキャスト unicast_linklocal_or_multicast：ユニキャスト（リンクローカル）＋マルチキャスト unicast_exclude_linklocal：ユニキャスト（リンクローカル以外） unicast_execlude_linklocal_or_multicast：ユニキャスト（リンクローカル以外）＋マルチキャスト
				packet_field	List	パケットフィールドフィルタ。AND 条件リスト。最大指定数：10 リスト。
					List	OR 条件リスト。最大指定数："packet_field"（パケットフィールドフィルタ）の総計で 100 リスト。
				@exclude	Boolean	除外条件。未指定時は False。
				flowset_id	Integer	フローセット ID
				sensor_addr	String	センサ IPv4 アドレス（ネットフローパケット送信元 IP アドレス）
				monitor_port_ifindex	Integer	センサモニタポート SNMP ifIndex
				output_port_ifindex	Integer	送信ポート SNMP ifIndex
				src_vlan	Integer	VLAN-ID 値（QinQ の場合，S-TAG）
				dst_vlan	Integer	VLAN-ID 値（QinQ の C-TAG）
				in_src_mac	String	送信元 MAC アドレス値。（例）00:00:5e:00:53:01
				in_dst_mac	String	宛先 MAC アドレス値。（例）00:00:5e:00:53:01

#	項目	説明					
					ipv4_src_addr	String	送信元 IPv4 アドレス値
					ipv4_dst_addr	String	宛先 IPv4 アドレス値
					ipv6_src_addr	String	送信元 IPv6 アドレス値
					ipv6_dst_addr	String	宛先 IPv6 アドレス値
					protocol	Integer	プロトコル番号
					icmp_type	Integer	ICMP タイプ値
					icmp_code	Integer	ICMP コード値
					l4_src_port	Integer	送信元 L4 ポート番号
					l4_dst_port	Integer	宛先 L4 ポート番号
					tcp_flags	String	TCP フラグ。 fin, syn, rst, psh, ack, urg, ece, cwr 半角スペースでくぎることで複数フラグを指定可。上記文字列の先頭に! を指定することで，対象フラグが Off のフローを指定可。 （例）"syn !ack"
					udp_rtp_ssrc	Integer	UDP RTP SSRC
					udp_rtp_pt	Integer	UDP RTP Payload Type
					udp_rtp_clock_rate	Integer	UDP RTP Clock Rate
					http_servername	String	HTTP サーバ名
					nat_ipv4_src_addr	String	NAT 送信元 IPv4 アドレス値
					nat_ipv4_dst_addr	String	NAT 宛先 IPv4 アドレス値
					nat_ipv6_src_addr	String	NAT 送信元 IPv6 アドレス値
					nat_ipv6_dst_addr	String	NAT 宛先 IPv6 アドレス値
					nat_l4_src_port	Integer	NAT 送信元 L4 ポート番号
					nat_l4_dst_port	Integer	NAT 宛先 L4 ポート番号
					nat_l4port_start	Integer	NAT L4 ポート番号範囲 Start
					nat_l4port_end	Integer	NAT L4 ポート番号範囲 End
					nat_event	Integer	NAT イベント
					nat_type	Integer	NAT タイプ
					vdom_name	String	バーチャルドメイン名
					ext01	String	フロー拡張データ 01
					ext02	String	フロー拡張データ 02
					ext03	String	フロー拡張データ 03
					ext04	String	フロー拡張データ 04
					ext05	String	フロー拡張データ 05
					ext06	String	フロー拡張データ 06
					ext07	String	フロー拡張データ 07
					ext08	String	フロー拡張データ 08
					ext09	String	フロー拡張データ 09
					ext10	String	フロー拡張データ 10
					ext11	String	国コード（送信元）
					ext12	String	国（送信元）
					ext13	String	地域（送信元）
					ext14	String	都市（送信元）
					ext15	String	AS 番号（送信元）
					ext16	String	AS 組織名（宛先）
					ext21	String	国コード（宛先）

#	項目	説明			
			ext22	String	国（宛先）
			ext23	String	地域（宛先）
			ext24	String	都市（宛先）
			ext25	String	AS 番号（宛先）
			ext26	String	AS 組織名（宛先）
			aggregate_groups *	Object	検索集約条件
			timestamp	Boolean	タイムスタンプ毎の集計
			flowset_id	Boolean	フローセット ID 毎の集計
			sensor_addr	Boolean	センサ IPv4 アドレス毎の集計
			monitor_port_ifindex	Boolean	センサモニタポート SNMP ifIndex 毎の集計
			output_port_ifindex	Boolean	送信ポート SNMP ifIndex 毎の集計
			src_vlan	Boolean	VLAN-ID（QinQ の場合，S-TAG）毎の集計
			dst_vlan	Boolean	QinQ の C-TAG 毎の集計
			in_src_mac	Boolean	送信元 MAC アドレス毎の集計
			in_dst_mac	Boolean	宛先 MAC アドレス毎の集計
			ipv4_src_addr	Boolean	送信元 IPv4 アドレス毎の集計。 ipv4_src_netaddr が true の場合，無効。
			ipv4_src_netaddr	Boolean	送信元 IPv4 ネットワークアドレス毎の集計
			ipv4_dst_addr	Boolean	宛先 IPv4 アドレス毎の集計。 ipv4_dst_netaddr が true の場合，無効。
			ipv4_dst_netaddr	Boolean	宛先 IPv4 ネットワークアドレス毎の集計
			ipv6_src_addr	Boolean	送信元 IPv6 アドレス毎の集計。 ipv6_src_netaddr が true の場合，無効。
			ipv6_src_netaddr	Boolean	送信元 IPv6 ネットワークアドレス毎の集計
			ipv6_dst_addr	Boolean	宛先 IPv6 アドレス毎の集計。 ipv6_dst_netaddr が true の場合，無効。
			ipv6_dst_netaddr	Boolean	宛先 IPv6 ネットワークアドレス毎の集計
			protocol	Boolean	プロトコル番号毎の集計
			icmp_type	Boolean	ICMP タイプ毎の集計
			icmp_code	Boolean	ICMP コード毎の集計

#	項目	説明				
				l4_src_port	Boolean	送信元 L4 ポート番号毎の集計
				l4_dst_port	Boolean	宛先 L4 ポート番号毎の集計
				tcp_flags	Boolean	TCP フラグ毎の集計
				udp_rtp_ssrc	Boolean	UDP RTP SSRC
				udp_rtp_pt	Boolean	UDP RTP Payload Type
				udp_rtp_clock_rate	Boolean	UDP RTP Clock Rate
				http_servername	Boolean	HTTP サーバ名毎の集計
				nat_ipv4_src_addr	Boolean	NAT 送信元 IPv4 アドレス毎の集計。 nat_ipv4_src_netaddr が true の場合， 無効。
				nat_ipv4_src_netaddr	Boolean	NAT 送信元 IPv4 ネットワークアドレス毎の集計
				nat_ipv4_dst_addr	Boolean	NAT 宛先 IPv4 アドレス毎の集計。 nat_ipv4_dst_netaddr が true の場合， 無効。
				nat_ipv4_dst_netaddr	Boolean	NAT 宛先 IPv4 ネットワークアドレス毎の集計
				nat_ipv6_src_addr	Boolean	NAT 送信元 IPv6 アドレス毎の集計。 nat_ipv6_src_netaddr が true の場合， 無効。
				nat_ipv6_src_netaddr	Boolean	NAT 送信元 IPv6 ネットワークアドレス毎の集計
				nat_ipv6_dst_addr	Boolean	NAT 宛先 IPv6 アドレス毎の集計。 nat_ipv6_dst_netaddr が true の場合， 無効。
				nat_ipv6_dst_netaddr	Boolean	NAT 宛先 IPv6 ネットワークアドレス毎の集計
				nat_l4_src_port	Boolean	NAT 送信元 L4 ポート番号毎の集計
				nat_l4_dst_port	Boolean	NAT 宛先 L4 ポート番号毎の集計
				nat_l4port_start	Boolean	NAT L4 ポート番号範囲 Start 毎の集計
				nat_l4port_end	Boolean	NAT L4 ポート番号範囲 End 毎の集計
				nat_event	Boolean	NAT イベント毎の集計
				nat_type	Boolean	NAT タイプ毎の集計
				nat_observ_time	Boolean	NAT 観測時刻（開始，終了）毎の集計
				vdom_name	Boolean	バーチャルドメイン名毎の集計

#	項目	説明			
			ext01	Boolean	フロー拡張データ 01 毎の集計
			ext02	Boolean	フロー拡張データ 02 毎の集計
			ext03	Boolean	フロー拡張データ 03 毎の集計
			ext04	Boolean	フロー拡張データ 04 毎の集計
			ext05	Boolean	フロー拡張データ 05 毎の集計
			ext06	Boolean	フロー拡張データ 06 毎の集計
			ext07	Boolean	フロー拡張データ 07 毎の集計
			ext08	Boolean	フロー拡張データ 08 毎の集計
			ext09	Boolean	フロー拡張データ 09 毎の集計
			ext10	Boolean	フロー拡張データ 10 毎の集計
			ext11	Boolean	国コード（送信元）毎の集計
			ext12	Boolean	国（送信元）毎の集計
			ext13	Boolean	地域（送信元）毎の集計
			ext14	Boolean	都市（送信元）毎の集計
			ext15	Boolean	AS 番号（送信元）毎の集計
			ext16	Boolean	AS 組織名（宛先）毎の集計
			ext21	Boolean	国コード（宛先）毎の集計
			ext22	Boolean	国（宛先）毎の集計
			ext23	Boolean	地域（宛先）毎の集計
			ext24	Boolean	都市（宛先）毎の集計
			ext25	Boolean	AS 番号（宛先）毎の集計
			ext26	Boolean	AS 組織名（宛先）毎の集計
			aggregate_option	Object	集計オプション
			packets	Boolean	パケット数
			out_packets	Boolean	送信パケット数
			out_bytes	Boolean	送信バイト数
			tcp_retx_pkts	Boolean	TCP 再送パケット数

<table>
<tr><th>#</th><th>項目</th><th>説明</th><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td>tcp_retx_bytes</td><td>Boolean</td><td>TCP 再送バイト数</td></tr>
<tr><td></td><td></td><td></td><td></td><td>tcp_pkt_losses</td><td>Boolean</td><td>TCP パケットロス回数</td></tr>
<tr><td></td><td></td><td></td><td></td><td>tcp_dupack_pkts</td><td>Boolean</td><td>TCP 重複 ACK パケット数</td></tr>
<tr><td></td><td></td><td></td><td></td><td>tcp_retx_pkts_percent</td><td>Boolean</td><td>TCP 再送パケット数割合（%）</td></tr>
<tr><td></td><td></td><td></td><td></td><td>tcp_retx_bytes_percent</td><td>Boolean</td><td>TCP 再送バイト数割合（%）</td></tr>
<tr><td></td><td></td><td></td><td></td><td>tcp_pkt_losses_percent</td><td>Boolean</td><td>TCP パケットロス回数割合（%）</td></tr>
<tr><td></td><td></td><td></td><td></td><td>udp_rtp_out_of_order</td><td>Boolean</td><td>UDP RTP 順序違反回数</td></tr>
<tr><td></td><td></td><td></td><td></td><td>udp_rtp_lost_pkts</td><td>Boolean</td><td>UDP RTP ロストパケット数</td></tr>
<tr><td></td><td></td><td></td><td></td><td>udp_rtp_lost_pkts_percent</td><td>Boolean</td><td>UDP RTP ロストパケット数割合（%）</td></tr>
<tr><td></td><td></td><td></td><td></td><td>nat_duration</td><td>Boolean</td><td>NAT 継続時間（s）</td></tr>
<tr><td>7</td><td>レスポンス</td><td>レスポンスステータス</td><td colspan="4">以下のステータスコードを応答します。<table><tr><th>コード</th><th>内容</th></tr><tr><td>200</td><td>成功</td></tr><tr><td>400</td><td>要求不正エラー</td></tr><tr><td>401</td><td>認証エラー</td></tr><tr><td>403</td><td>アクセス禁止</td></tr><tr><td>408</td><td>タイムアウト</td></tr><tr><td>500</td><td>内部エラー</td></tr><tr><td>503</td><td>サービス利用不可</td></tr></table></td></tr>
<tr><td>8</td><td></td><td>Content-Type</td><td colspan="4">application/json</td></tr>
</table>

9 レスポンスボディ：

ステータスコード=200 の場合

・例

```
[
   {
      "rank": 1,
      "packets_info": {
         "ipv4_src_addr": "192.168.253.144",
         "ipv4_src_addr_alias": "-"
      },
      "bytes_counts": 37884564
   },
   :  ～省略～
   {
      "rank": 5,
      "packets_info": {
         "ipv4_src_addr": "192.168.192.73",
         "ipv4_src_addr_alias": "-"
      },
      "bytes_counts": 33339574
   }
]
```

・拡張データ ext のパラメータ名は,設定された表示名称となります。

・パラメータ説明

パラメータ名		型	説明
		List	応答リスト。
rank		Integer	集計ランキング
packets_info		Object	パケット情報 aggregate_groups で，指定された関連情報のみ格納
	timestamp	String	タイムスタンプ
	flowset_id	Integer	フローセット ID
	sensor_addr	String	センサ IPv4 アドレス（ネットフローパケット送信元 IP アドレス）
	sensor_addr_alias	String	センサ IPv4 アドレスエイリアス
	monitor_port_ifindex	Integer	センサモニタポート SNMP ifIndex
	monitor_port_alias	String	センサモニタポート SNMP ifIndex エイリアス
	output_port_ifindex	Integer	送信ポート SNMP ifIndex
	output_prot_alias	String	送信ポート SNMP ifIndex エイリアス
	src_vlan	Integer	VLAN-ID 値（QinQ の場合，S-TAG）
	src_vlan_alias	String	VLAN-ID エイリアス。dst_vlan 集約時は非表示。
	dst_vlan	Integer	VLAN-ID 値（QinQ の C-TAG）
	qinq_alias	String	VLAN(QinQ)エイリアス。 src_vlan/dst_vlan 集約時に表示。

			in_src_mac	String	送信元 MAC アドレス値
			in_src_mac_alias	String	送信元 MAC アドレスエイリアス
			in_src_mac_vendor	String	送信元 MAC アドレスベンダ名
			in_dst_mac	String	宛先 MAC アドレス値
			in_dst_mac_alias	String	宛先 MAC アドレスエイリアス
			in_dst_mac_vendor	String	宛先 MAC アドレスベンダ名
			ipv4_src_addr	String	送信元 IPv4 アドレス値
			ipv4_src_addr_alias	String	送信元 IPv4 アドレスエイリアス
			ipv4_src_netaddr	String	送信元 IPv4 ネットワークアドレス値
			ipv4_src_netaddr_alias	String	送信元 IPv4 ネットワークアドレスエイリアス
			ipv4_dst_addr	String	宛先 IPv4 アドレス値
			ipv4_dst_addr_alias	String	宛先 IPv4 アドレスエイリアス
			ipv4_dst_netaddr	String	宛先 IPv4 ネットワークアドレス値
			ipv4_dst_netaddr_alias	String	宛先 IPv4 ネットワークアドレスエイリアス
			ipv6_src_addr	String	送信元 IPv6 アドレス値
			ipv6_src_addr_alias	String	送信元 IPv6 アドレスエイリアス
			ipv6_src_netaddr	String	送信元 IPv6 ネットワークアドレス値
			ipv6_src_netaddr_alias	String	送信元 IPv6 ネットワークアドレスエイリアス
			ipv6_dst_addr	String	宛先 IPv6 アドレス値
			ipv6_dst_addr_alias	String	宛先 IPv6 アドレスエイリアス
			ipv6_dst_netaddr	String	宛先 IPv6 ネットワークアドレス値
			ipv6_dst_netaddr_alias	String	宛先 IPv6 ネットワークアドレスエイリアス
			protocol	Integer	プロトコル番号
			protocol_name	String	プロトコル名
			icmp_type	Integer	ICMP タイプ番号
			icmp_type_name	String	ICMP タイプ名称 集約条件に protocol 指定時のみ
			icmp_code	Integer	ICMP コード番号
			icmp_code_name	String	ICMP コード名称 集約条件に protocol 指定時のみ
			l4_src_port	Ingeter	送信元 L4 ポート番号
			l4_src_port_name	String	送信元 L4 ポート名
			l4_dst_port	Integer	宛先 L4 ポート番号
			l4_dst_port_name	String	宛先 L4 ポート名
			tcp_flags	Integer	TCP フラグ
			tcp_flags_name	String	TCP フラグ名
			udp_rtp_ssrc	Integer	UDP RTP SSRC
			udp_rtp_pt	Integer	UDP RTP Payload Type
			udp_rtp_clock_rate	Integer	UDP RTP Clock Rate

				http_servername	String	HTTP サーバ名
				nat_ipv4_src_addr	String	NAT 送信元 IPv4 アドレス値
				nat_ipv4_src_addr_alias	String	NAT 送信元 IPv4 アドレスエイリアス
				nat_ipv4_src_netaddr	String	NAT 送信元 IPv4 ネットワークアドレス値
				nat_ipv4_src_netaddr_alias	String	NAT 送信元 IPv4 ネットワークアドレスエイリアス
				nat_ipv4_dst_addr	String	NAT 宛先 IPv4 アドレス値
				nat_ipv4_dst_addr_alias	String	NAT 宛先 IPv4 アドレスエイリアス
				nat_ipv4_dst_netaddr	String	NAT 宛先 IPv4 ネットワークアドレス値
				nat_ipv4_dst_netaddr_alias	String	NAT 宛先 IPv4 ネットワークアドレスエイリアス
				nat_ipv6_src_addr	String	NAT 送信元 IPv6 アドレス値
				nat_ipv6_src_addr_alias	String	NAT 送信元 IPv6 アドレスエイリアス
				nat_ipv6_src_netaddr	String	NAT 送信元 IPv6 ネットワークアドレス値
				nat_ipv6_src_netaddr_alias	String	NAT 送信元 IPv6 ネットワークアドレスエイリアス
				nat_ipv6_dst_addr	String	NAT 宛先 IPv6 アドレス値
				nat_ipv6_dst_addr_alias	String	NAT 宛先 IPv6 アドレスエイリアス
				nat_ipv6_dst_netaddr	String	NAT 宛先 IPv6 ネットワークアドレス値
				nat_ipv6_dst_netaddr_alias	String	NAT 宛先 IPv6 ネットワークアドレスエイリアス
				nat_l4_src_port	Ingeter	NAT 送信元 L4 ポート番号
				nat_l4_src_port_name	String	NAT 送信元 L4 ポート名
				nat_l4_dst_port	Integer	NAT 宛先 L4 ポート番号
				nat_l4_dst_port_name	String	NAT 宛先 L4 ポート名
				nat_l4port_start	Ingeter	NAT L4 ポート番号範囲 Start
				nat_l4port_end	Integer	NAT L4 ポート番号範囲 End
				nat_event	String	NAT イベント
				nat_type	String	NAT タイプ
				nat_start_time	String	NAT 開始時刻
				nat_end_time	String	NAT 終了時刻
				vdom_name	String	バーチャルドメイン名
				ext01	String	フロー拡張データ 01
				ext02	String	フロー拡張データ 02
				ext03	String	フロー拡張データ 03
				ext04	String	フロー拡張データ 04
				ext05	String	フロー拡張データ 05
				ext06	String	フロー拡張データ 06
				ext07	String	フロー拡張データ 07
				ext08	String	フロー拡張データ 08
				ext09	String	フロー拡張データ 09
				ext10	String	フロー拡張データ 10

<table>
<tr><th>#</th><th>項目</th><th>説明</th><td colspan="4"></td></tr>
<tr><td></td><td></td><td></td><td></td><td>ext11</td><td>String</td><td>国コード（送信元）</td></tr>
<tr><td></td><td></td><td></td><td></td><td>ext12</td><td>String</td><td>国（送信元）</td></tr>
<tr><td></td><td></td><td></td><td></td><td>ext13</td><td>String</td><td>地域（送信元）</td></tr>
<tr><td></td><td></td><td></td><td></td><td>ext14</td><td>String</td><td>都市（送信元）</td></tr>
<tr><td></td><td></td><td></td><td></td><td>ext15</td><td>String</td><td>AS 番号（送信元）</td></tr>
<tr><td></td><td></td><td></td><td></td><td>ext16</td><td>String</td><td>AS 組織名（宛先）</td></tr>
<tr><td></td><td></td><td></td><td></td><td>ext21</td><td>String</td><td>国コード（宛先）</td></tr>
<tr><td></td><td></td><td></td><td></td><td>ext22</td><td>String</td><td>国（宛先）</td></tr>
<tr><td></td><td></td><td></td><td></td><td>ext23</td><td>String</td><td>地域（宛先）</td></tr>
<tr><td></td><td></td><td></td><td></td><td>ext24</td><td>String</td><td>都市（宛先）</td></tr>
<tr><td></td><td></td><td></td><td></td><td>ext25</td><td>String</td><td>AS 番号（宛先）</td></tr>
<tr><td></td><td></td><td></td><td></td><td>ext26</td><td>String</td><td>AS 組織名（宛先）</td></tr>
<tr><td></td><td></td><td></td><td>bytes_counts</td><td></td><td>Integer64</td><td>集計バイト数</td></tr>
<tr><td></td><td></td><td></td><td>packets_counts</td><td></td><td>Integer64</td><td>集計パケット数</td></tr>
<tr><td></td><td></td><td></td><td>out_bytes_counts</td><td></td><td>Integer64</td><td>集計送信バイト数</td></tr>
<tr><td></td><td></td><td></td><td>out_packets_counts</td><td></td><td>Integer64</td><td>集計送信パケット数</td></tr>
<tr><td></td><td></td><td></td><td>tcp_retx_pkts_counts</td><td></td><td>Integer64</td><td>集計 TCP 再送パケット数</td></tr>
<tr><td></td><td></td><td></td><td>tcp_retx_bytes_counts</td><td></td><td>Integer64</td><td>集計 TCP 再送バイト数</td></tr>
<tr><td></td><td></td><td></td><td>tcp_pkt_losses_counts</td><td></td><td>Integer64</td><td>集計 TCP パケットロス回数</td></tr>
<tr><td></td><td></td><td></td><td>tcp_dupack_pkts_counts</td><td></td><td>Integer64</td><td>集計 TCP 重複 ACK パケット数</td></tr>
<tr><td></td><td></td><td></td><td>tcp_retx_pkts_percent</td><td></td><td>float</td><td>集計 TCP 再送パケット数割合（%）</td></tr>
<tr><td></td><td></td><td></td><td>tcp_retx_bytes_percent</td><td></td><td>float</td><td>集計 TCP 再送バイト数割合（%）</td></tr>
<tr><td></td><td></td><td></td><td>tcp_pkt_losses_percent</td><td></td><td>float</td><td>集計 TCP パケットロス回数割合（%）</td></tr>
<tr><td></td><td></td><td></td><td>udp_rtp_out_of_order_counts</td><td></td><td>Integer64</td><td>UDP RTP 順序違反回数</td></tr>
<tr><td></td><td></td><td></td><td>udp_rtp_lost_pkts_counts</td><td></td><td>Integer64</td><td>UDP RTP ロストパケット数</td></tr>
<tr><td></td><td></td><td></td><td>udp_rtp_lost_pkts_percent</td><td></td><td>float</td><td>UDP RTP ロストパケット数割合（%）</td></tr>
<tr><td></td><td></td><td></td><td>nat_duration</td><td></td><td>Float</td><td>NAT 継続時間（s）</td></tr>
<tr><td>10</td><td></td><td>レスポンスボディ：

ステータスコード=200 以外の場合</td><td colspan="4">・例
{
"detail": "ユーザ名かパスワードが違います。"
}
・パラメータ説明
<table><tr><th>パラメータ名</th><th>型</th><th>説明</th></tr><tr><td>detail</td><td>String</td><td>エラー詳細を格納します。</td></tr></table></td></tr>
</table>

7.3.2 IP フロー パケット数ランキング取得 API

IP フロー情報を検索し，パケット数ランキング上位のパケット情報を取得します。

表 7-11 IP フロー パケット数ランキング取得 API

#	項目	説明	
1	メソッド	POST	
2	URI	/api/v1/flowdata/ip/ranking/packets/ または /api/v1/flowdata/ipv4/ranking/packets/	
3	リクエスト	認証	ベーシック認証もしくはトークン認証。
4		クエリパラメータ	なし
5		Content-Type	application/json

6		ボディパラメータ	・例
			{
			"time_from": "2021-01-11T10:00:00+09:00",
			"time_to": "2021-01-11T12:00:00+09:00",
			"numbers":10,
			"search_filters":{
			"packet_field" : [
			[{"src_vlan":4000 }, {"src_vlan":3000}]
			]
			},
			"aggregate_groups": {
			"src_vlan":false,
			"ipv4_src_addr":true
			}
			}
			・パラメータ説明（*必須パラメータ）

パラメータ名	型	説明
time_from *	String	検索時刻 - 始まり。ISO8601 フォーマット。（例）2021-01-11T10:00:00+09:00
time_to *	String	検索時刻 - 終わり。ISO8601 フォーマット。（例）2021-01-11T12:00:00+09:00
numbers	integer	取得する検索結果数。指定範囲は，1～100000。省略時：10。
search_filters	Object	検索フィルタ条件
sensor_addr	String	センサ IPv4 アドレス（ネットフローパケット送信元 IP アドレス）
monitor_port_ifindex	Integer	センサモニタポート SNMP ifIndex
output_port_ifindex	Integer	送信ポート SNMP ifIndex

#	項目	説明					
				mac_kind	String	MAC アドレス種別（ユニキャスト，マルチキャスト，ブロードキャスト） unicast, broadcast, multicast, unicast_broadcast, unicast_multicast, broadcast_multicast, all
				ip_kind	String	IPv4 アドレス種別（ユニキャスト＋ブロードキャスト，マルチキャスト） unicast_broadcast, multicast, all
				ipv6_kind	String	IPv6 アドレス種別 all：すべて unicast：ユニキャスト multicast：マルチキャスト unicast_linklocal_or_multicast：ユニキャスト（リンクローカル）＋マルチキャスト unicast_exclude_linklocal：ユニキャスト（リンクローカル以外） unicast_execlude_linklocal_or_multicast：ユニキャスト（リンクローカル以外）＋マルチキャスト
				packet_field	List	パケットフィールドフィルタ。AND 条件リスト。最大指定数：10 リスト。
					List	OR 条件リスト。最大指定数："packet_field"（パケットフィールドフィルタ）の総計で 100 リスト。
				@exclude	Boolean	除外条件。未指定時は False。
				flowset_id	Integer	フローセット ID
				sensor_addr	String	センサ IPv4 アドレス（ネットフローパケット送信元 IP アドレス）
				monitor_port_ifindex	Integer	センサモニタポート SNMP ifIndex
				output_port_ifindex	Integer	送信ポート SNMP ifIndex
				src_vlan	Integer	VLAN-ID 値（QinQ の場合，S-TAG）
				dst_vlan	Integer	VLAN-ID 値（QinQ の C-TAG）
				in_src_mac	String	送信元 MAC アドレス値。（例）00:00:5e:00:53:01
				in_dst_mac	String	宛先 MAC アドレス値。（例）00:00:5e:00:53:01
				ipv4_src_addr	String	送信元 IPv4 アドレス値
				ipv4_dst_addr	String	宛先 IPv4 アドレス値
				ipv6_src_addr	String	送信元 IPv6 アドレス値
				ipv6_dst_addr	String	宛先 IPv6 アドレス値

#	項目	説明					
					protocol	Integer	プロトコル番号
					icmp_type	Integer	ICMP タイプ値
					icmp_code	Integer	ICMP コード値
					l4_src_port	Integer	送信元 L4 ポート番号
					l4_dst_port	Integer	宛先 L4 ポート番号
					tcp_flags	String	TCP フラグ。 fin, syn, rst, psh, ack, urg, ece, cwr 半角スペースでくぎることで複数フラグを指定可。上記文字列の先頭に! を指定することで，対象フラグが Off のフローを指定可。 （例）"syn !ack"
					udp_rtp_ssrc	Integer	UDP RTP SSRC
					udp_rtp_pt	Integer	UDP RTP Payload Type
					udp_rtp_clock_rate	Integer	UDP RTP Clock Rate
					http_servername	String	HTTP サーバ名
					nat_ipv4_src_addr	String	NAT 送信元 IPv4 アドレス値
					nat_ipv4_dst_addr	String	NAT 宛先 IPv4 アドレス値
					nat_ipv6_src_addr	String	NAT 送信元 IPv6 アドレス値
					nat_ipv6_dst_addr	String	NAT 宛先 IPv6 アドレス値
					nat_l4_src_port	Integer	NAT 送信元 L4 ポート番号
					nat_l4_dst_port	Integer	NAT 宛先 L4 ポート番号
					nat_l4port_start	Integer	NAT L4 ポート番号範囲 Start
					nat_l4port_end	Integer	NAT L4 ポート番号範囲 End
					nat_event	Integer	NAT イベント
					nat_type	Integer	NAT タイプ
					vdom_name	String	バーチャルドメイン名
					ext01	String	フロー拡張データ 01
					ext02	String	フロー拡張データ 02
					ext03	String	フロー拡張データ 03
					ext04	String	フロー拡張データ 04
					ext05	String	フロー拡張データ 05
					ext06	String	フロー拡張データ 06
					ext07	String	フロー拡張データ 07
					ext08	String	フロー拡張データ 08
					ext09	String	フロー拡張データ 09
					ext10	String	フロー拡張データ 10
					ext11	String	国コード（送信元）
					ext12	String	国（送信元）
					ext13	String	地域（送信元）
					ext14	String	都市（送信元）
					ext15	String	AS 番号（送信元）
					ext16	String	AS 組織名（宛先）
					ext21	String	国コード（宛先）
					ext22	String	国（宛先）
					ext23	String	地域（宛先）
					ext24	String	都市（宛先）
					ext25	String	AS 番号（宛先）

#	項目	説明			
			ext26	String	AS 組織名（宛先）
			aggregate_groups *	Object	検索集約条件
			timestamp	Boolean	タイムスタンプ毎の集計
			flowset_id	Boolean	フローセット ID 毎の集計
			sensor_addr	Boolean	センサ IPv4 アドレス毎の集計
			monitor_port_ifindex	Boolean	センサモニタポート SNMP ifIndex 毎の集計
			output_port_ifindex	Boolean	送信ポート SNMP ifIndex 毎の集計
			src_vlan	Boolean	VLAN-ID（QinQ の場合，S-TAG）毎の集計
			dst_vlan	Boolean	QinQ の C-TAG 毎の集計
			in_src_mac	Boolean	送信元 MAC アドレス毎の集計
			in_dst_mac	Boolean	宛先 MAC アドレス毎の集計
			ipv4_src_addr	Boolean	送信元 IPv4 アドレス毎の集計。 ipv4_src_netaddr が true の場合，無効。
			ipv4_src_netaddr	Boolean	送信元 IPv4 ネットワークアドレス毎の集計
			ipv4_dst_addr	Boolean	宛先 IPv4 アドレス毎の集計。 ipv4_dst_netaddr が true の場合，無効。
			ipv4_dst_netaddr	Boolean	宛先 IPv4 ネットワークアドレス毎の集計
			ipv6_src_addr	Boolean	送信元 IPv6 アドレス毎の集計。 ipv6_src_netaddr が true の場合，無効。
			ipv6_src_netaddr	Boolean	送信元 IPv6 ネットワークアドレス毎の集計
			ipv6_dst_addr	Boolean	宛先 IPv6 アドレス毎の集計。 ipv6_dst_netaddr が true の場合，無効。
			ipv6_dst_netaddr	Boolean	宛先 IPv6 ネットワークアドレス毎の集計
			protocol	Boolean	プロトコル番号毎の集計
			icmp_type	Boolean	ICMP タイプ毎の集計
			icmp_code	Boolean	ICMP コード毎の集計
			l4_src_port	Boolean	送信元 L4 ポート番号毎の集計
			l4_dst_port	Boolean	宛先 L4 ポート番号毎の集計

#	項目	説明				
				tcp_flags	Boolean	TCP フラグ毎の集計
				udp_rtp_ssrc	Boolean	UDP RTP SSRC
				udp_rtp_pt	Boolean	UDP RTP Payload Type
				udp_rtp_clock_rate	Boolean	UDP RTP Clock Rate
				http_servername	Boolean	HTTP サーバ名毎の集計
				nat_ipv4_src_addr	Boolean	NAT 送信元 IPv4 アドレス毎の集計。 nat_ipv4_src_netaddr が true の場合， 無効。
				nat_ipv4_src_netaddr	Boolean	NAT 送信元 IPv4 ネットワークアドレス毎の集計
				nat_ipv4_dst_addr	Boolean	NAT 宛先 IPv4 アドレス毎の集計。 nat_ipv4_dst_netaddr が true の場合， 無効。
				nat_ipv4_dst_netaddr	Boolean	NAT 宛先 IPv4 ネットワークアドレス毎の集計
				nat_ipv6_src_addr	Boolean	NAT 送信元 IPv6 アドレス毎の集計。 nat_ipv6_src_netaddr が true の場合， 無効。
				nat_ipv6_src_netaddr	Boolean	NAT 送信元 IPv6 ネットワークアドレス毎の集計
				nat_ipv6_dst_addr	Boolean	NAT 宛先 IPv6 アドレス毎の集計。 nat_ipv6_dst_netaddr が true の場合， 無効。
				nat_ipv6_dst_netaddr	Boolean	NAT 宛先 IPv6 ネットワークアドレス毎の集計
				nat_l4_src_port	Boolean	NAT 送信元 L4 ポート番号毎の集計
				nat_l4_dst_port	Boolean	NAT 宛先 L4 ポート番号毎の集計
				nat_l4port_start	Boolean	NAT L4 ポート番号範囲 Start 毎の集計
				nat_l4port_end	Boolean	NAT L4 ポート番号範囲 End 毎の集計
				nat_event	Boolean	NAT イベント毎の集計
				nat_type	Boolean	NAT タイプ毎の集計
				nat_observ_time	Boolean	NAT 観測時刻（開始，終了）毎の集計
				vdom_name	Boolean	バーチャルドメイン名毎の集計
				ext01	Boolean	フロー拡張データ 01 毎の集計
				ext02	Boolean	フロー拡張データ 02 毎の集計

#	項目	説明				
				ext03	Boolean	フロー拡張データ 03 毎の集計
				ext04	Boolean	フロー拡張データ 04 毎の集計
				ext05	Boolean	フロー拡張データ 05 毎の集計
				ext06	Boolean	フロー拡張データ 06 毎の集計
				ext07	Boolean	フロー拡張データ 07 毎の集計
				ext08	Boolean	フロー拡張データ 08 毎の集計
				ext09	Boolean	フロー拡張データ 09 毎の集計
				ext10	Boolean	フロー拡張データ 10 毎の集計
				ext11	Boolean	国コード（送信元）毎の集計
				ext12	Boolean	国（送信元）毎の集計
				ext13	Boolean	地域（送信元）毎の集計
				ext14	Boolean	都市（送信元）毎の集計
				ext15	Boolean	AS 番号（送信元）毎の集計
				ext16	Boolean	AS 組織名（宛先）毎の集計
				ext21	Boolean	国コード（宛先）毎の集計
				ext22	Boolean	国（宛先）毎の集計
				ext23	Boolean	地域（宛先）毎の集計
				ext24	Boolean	都市（宛先）毎の集計
				ext25	Boolean	AS 番号（宛先）毎の集計
				ext26	Boolean	AS 組織名（宛先）毎の集計
			aggregate_option		Object	集計オプション
				bytes	Boolean	バイト数
				out_packets	Boolean	送信パケット数
				out_bytes	Boolean	送信バイト数
				tcp_retx_pkts	Boolean	TCP 再送パケット数
				tcp_retx_bytes	Boolean	TCP 再送バイト数
				tcp_pkt_losses	Boolean	TCP パケットロス回数

<table>
<tr><td>#</td><td>項目</td><td>説明</td><td>
<table>
<tr><td></td><td>tcp_dupack_pkts</td><td>Boolean</td><td>TCP 重複 ACK パケット数</td></tr>
<tr><td></td><td>tcp_retx_pkts_percent</td><td>Boolean</td><td>TCP 再送パケット数割合（%）</td></tr>
<tr><td></td><td>tcp_retx_bytes_percent</td><td>Boolean</td><td>TCP 再送バイト数割合（%）</td></tr>
<tr><td></td><td>tcp_pkt_losses_percent</td><td>Boolean</td><td>TCP パケットロス回数割合（%）</td></tr>
<tr><td></td><td>udp_rtp_out_of_order</td><td>Boolean</td><td>UDP RTP 順序違反回数</td></tr>
<tr><td></td><td>udp_rtp_lost_pkts</td><td>Boolean</td><td>UDP RTP ロストパケット数</td></tr>
<tr><td></td><td>udp_rtp_lost_pkts_percent</td><td>Boolean</td><td>UDP RTP ロストパケット数割合（%）</td></tr>
<tr><td></td><td>nat_duration</td><td>Boolean</td><td>NAT 継続時間（s）</td></tr>
</table>
</td></tr>
<tr><td>7</td><td rowspan="2">レスポンス</td><td>レスポンスステータス</td><td>以下のステータスコードを応答します。
<table>
<tr><td>コード</td><td>内容</td></tr>
<tr><td>200</td><td>成功</td></tr>
<tr><td>400</td><td>要求不正エラー</td></tr>
<tr><td>401</td><td>認証エラー</td></tr>
<tr><td>403</td><td>アクセス禁止</td></tr>
<tr><td>408</td><td>タイムアウト</td></tr>
<tr><td>500</td><td>内部エラー</td></tr>
<tr><td>503</td><td>サービス利用不可</td></tr>
</table>
</td></tr>
<tr><td>8</td><td>Content-Type</td><td>application/json</td></tr>
</table>

9 | | レスポンスボディ：

ステータスコード=200 の場合

・例

```
[
   {
      "rank": 1,
      "packets_info": {
         "ipv4_src_addr": "192.168.253.144",
         "ipv4_src_addr_alias": "-"
      },
      "packets_counts": 37884564
   },
   :  ～省略～
   {
      "rank": 5,
      "packets_info": {
         "ipv4_src_addr": "192.168.192.73",
         "ipv4_src_addr_alias": "-"
      },
      "packets_counts": 33339574
   }
]
```

・拡張データ ext のパラメータ名は,設定された表示名称となります。

・パラメータ説明

パラメータ名		型	説明
		List	応答リスト。
rank		Integer	集計ランキング
packets_info		Object	パケット情報 aggregate_groups で，指定された関連情報のみ格納
	timestamp	String	タイムスタンプ
	flowset_id	Integer	フローセット ID
	sensor_addr	String	センサ IPv4 アドレス（ネットフローパケット送信元 IP アドレス）
	sensor_addr_alias	String	センサ IPv4 アドレスエイリアス
	monitor_port_ifindex	Integer	センサモニタポート SNMP ifIndex
	monitor_port_alias	String	センサモニタポート SNMP ifIndex エイリアス
	output_port_ifindex	Integer	送信ポート SNMP ifIndex
	output_prot_alias	String	送信ポート SNMP ifIndex エイリアス
	src_vlan	Integer	VLAN-ID 値（QinQ の場合，S-TAG）
	src_vlan_alias	String	VLAN-ID エイリアス。dst_vlan 集約時は非表示。
	dst_vlan	Integer	VLAN-ID 値（QinQ の C-TAG）
	qinq_alias	String	VLAN(QinQ)エイリアス。 src_vlan/dst_vlan 集約時に表示。
	in_src_mac	String	送信元 MAC アドレス値
	in_src_mac_alias	String	送信元 MAC アドレスエイリアス

				in_src_mac_vendor	String	送信元 MAC アドレスベンダ名
				in_dst_mac	String	宛先 MAC アドレス値
				in_dst_mac_alias	String	宛先 MAC アドレスエイリアス
				in_dst_mac_vendor	String	宛先 MAC アドレスベンダ名
				ipv4_src_addr	String	送信元 IPv4 アドレス値
				ipv4_src_addr_alias	String	送信元 IPv4 アドレスエイリアス
				ipv4_src_netaddr	String	送信元 IPv4 ネットワークアドレス値
				ipv4_src_netaddr_alias	String	送信元 IPv4 ネットワークアドレスエイリアス
				ipv4_dst_addr	String	宛先 IPv4 アドレス値
				ipv4_dst_addr_alias	String	宛先 IPv4 アドレスエイリアス
				ipv4_dst_netaddr	String	宛先 IPv4 ネットワークアドレス値
				ipv4_dst_netaddr_alias	String	宛先 IPv4 ネットワークアドレスエイリアス
				ipv6_src_addr	String	送信元 IPv6 アドレス値
				ipv6_src_addr_alias	String	送信元 IPv6 アドレスエイリアス
				ipv6_src_netaddr	String	送信元 IPv6 ネットワークアドレス値
				ipv6_src_netaddr_alias	String	送信元 IPv6 ネットワークアドレスエイリアス
				ipv6_dst_addr	String	宛先 IPv6 アドレス値
				ipv6_dst_addr_alias	String	宛先 IPv6 アドレスエイリアス
				ipv6_dst_netaddr	String	宛先 IPv6 ネットワークアドレス値
				ipv6_dst_netaddr_alias	String	宛先 IPv6 ネットワークアドレスエイリアス
				protocol	Integer	プロトコル番号
				protocol_name	String	プロトコル名
				icmp_type	Integer	ICMP タイプ番号
				icmp_type_name	String	ICMP タイプ名称 集約条件に protocol 指定時のみ
				icmp_code	Integer	ICMP コード番号
				icmp_code_name	String	ICMP コード名称 集約条件に protocol 指定時のみ
				l4_src_port	Ingeter	送信元 L4 ポート番号
				l4_src_port_name	String	送信元 L4 ポート名
				l4_dst_port	Integer	宛先 L4 ポート番号
				l4_dst_port_name	String	宛先 L4 ポート名
				tcp_flags	Integer	TCP フラグ
				tcp_flags_name	String	TCP フラグ名
				udp_rtp_ssrc	Integer	UDP RTP SSRC
				udp_rtp_pt	Integer	UDP RTP Payload Type
				udp_rtp_clock_rate	Integer	UDP RTP Clock Rate
				http_servername	String	HTTP サーバ名
				nat_ipv4_src_addr	String	NAT 送信元 IPv4 アドレス値
				nat_ipv4_src_addr_alias	String	NAT 送信元 IPv4 アドレスエイリアス

				nat_ipv4_src_netaddr	String	NAT 送信元 IPv4 ネットワークアドレス値
				nat_ipv4_src_netaddr_alias	String	NAT 送信元 IPv4 ネットワークアドレスエイリアス
				nat_ipv4_dst_addr	String	NAT 宛先 IPv4 アドレス値
				nat_ipv4_dst_addr_alias	String	NAT 宛先 IPv4 アドレスエイリアス
				nat_ipv4_dst_netaddr	String	NAT 宛先 IPv4 ネットワークアドレス値
				nat_ipv4_dst_netaddr_alias	String	NAT 宛先 IPv4 ネットワークアドレスエイリアス
				nat_ipv6_src_addr	String	NAT 送信元 IPv6 アドレス値
				nat_ipv6_src_addr_alias	String	NAT 送信元 IPv6 アドレスエイリアス
				nat_ipv6_src_netaddr	String	NAT 送信元 IPv6 ネットワークアドレス値
				nat_ipv6_src_netaddr_alias	String	NAT 送信元 IPv6 ネットワークアドレスエイリアス
				nat_ipv6_dst_addr	String	NAT 宛先 IPv6 アドレス値
				nat_ipv6_dst_addr_alias	String	NAT 宛先 IPv6 アドレスエイリアス
				nat_ipv6_dst_netaddr	String	NAT 宛先 IPv6 ネットワークアドレス値
				nat_ipv6_dst_netaddr_alias	String	NAT 宛先 IPv6 ネットワークアドレスエイリアス
				nat_l4_src_port	Ingeter	NAT 送信元 L4 ポート番号
				nat_l4_src_port_name	String	NAT 送信元 L4 ポート名
				nat_l4_dst_port	Integer	NAT 宛先 L4 ポート番号
				nat_l4_dst_port_name	String	NAT 宛先 L4 ポート名
				nat_l4port_start	Ingeter	NAT L4 ポート番号範囲 Start
				nat_l4port_end	Integer	NAT L4 ポート番号範囲 End
				nat_event	String	NAT イベント
				nat_type	String	NAT タイプ
				nat_start_time	String	NAT 開始時刻
				nat_end_time	String	NAT 終了時刻
				vdom_name	String	バーチャルドメイン名
				ext01	String	フロー拡張データ 01
				ext02	String	フロー拡張データ 02
				ext03	String	フロー拡張データ 03
				ext04	String	フロー拡張データ 04
				ext05	String	フロー拡張データ 05
				ext06	String	フロー拡張データ 06
				ext07	String	フロー拡張データ 07
				ext08	String	フロー拡張データ 08
				ext09	String	フロー拡張データ 09
				ext10	String	フロー拡張データ 10
				ext11	String	国コード（送信元）
				ext12	String	国（送信元）
				ext13	String	地域（送信元）

#	項目	説明			
			ext14	String	都市（送信元）
			ext15	String	AS 番号（送信元）
			ext16	String	AS 組織名（宛先）
			ext21	String	国コード（宛先）
			ext22	String	国（宛先）
			ext23	String	地域（宛先）
			ext24	String	都市（宛先）
			ext25	String	AS 番号（宛先）
			ext26	String	AS 組織名（宛先）
			packets_counts	Integer64	集計パケット数
			bytes_counts	Integer64	集計バイト数
			out_bytes_counts	Integer64	集計送信バイト数
			out_packets_counts	Integer64	集計送信パケット数
			tcp_retx_pkts_counts	Integer64	集計 TCP 再送パケット数
			tcp_retx_bytes_counts	Integer64	集計 TCP 再送バイト数
			tcp_pkt_losses_counts	Integer64	集計 TCP パケットロス回数
			tcp_dupack_pkts_counts	Integer64	集計 TCP 重複 ACK パケット数
			tcp_retx_pkts_percent	Float	集計 TCP 再送パケット数割合（%）
			tcp_retx_bytes_percent	Float	集計 TCP 再送バイト数割合（%）
			tcp_pkt_losses_percent	float	集計 TCP パケットロス回数割合（%）
			udp_rtp_out_of_order_counts	Integer64	UDP RTP 順序違反回数
			udp_rtp_lost_pkts_counts	Integer64	UDP RTP ロストパケット数
			udp_rtp_lost_pkts_percent	float	UDP RTP ロストパケット数割合（%）
			nat_duration	Float	NAT 継続時間（s）

10		レスポンスボディ：
		
		ステータスコード=200 以外の場合
			・例
			{
			"detail": "ユーザ名かパスワードが違います。"
			}
			・パラメータ説明		

パラメータ名	型	説明
detail	String	エラー詳細を格納します。

7.3.3 IP フロー バイト数時系列データ取得 API

IP フロー情報を検索し，バイト数の時系列情報を取得します。

表 7-12 IP フロー バイト数時系列データ取得 API

#	項目	説明	
1	メソッド	POST	
2	URI	/api/v1/flowdata/ip/timeseries/bytes/ または /api/v1/flowdata/ipv4/timeseries/bytes/	
3	リクエスト	認証	ベーシック認証もしくはトークン認証。
4		クエリパラメータ	なし
5		Content-Type	application/json

6		ボディパラメータ	・例
			{
			"time_from": "2021-01-11T10:00:00+09:00",
			"time_to": "2021-01-11T12:00:00+09:00",
			"time_interval":"5m",
			"search_filters":{
			"packet_field" : [
			[{"src_vlan":4000 }, {"src_vlan":3000}]
			]
			}
			}

・パラメータ説明（*必須パラメータ）

パラメータ名	型	説明
time_from *	String	検索時刻 - 始まり。ISO8601 フォーマット。（例）2021-01-11T10:00:00+09:00
time_to *	String	検索時刻 - 終わり。ISO8601 フォーマット。（例）2021-01-11T12:00:00+09:00
time_interval *	String	取得間隔。 1s, 10s, 30s, 1m, 5m, 10m, 15m, 30m, 1h, 3h, 6h, 12h, 1d
search_filters	Object	検索フィルタ条件
sensor_addr	String	センサ IPv4 アドレス（ネットフローパケット送信元 IP アドレス）
monitor_port_ifindex	Integer	センサモニタポート SNMP ifIndex
output_port_ifindex	Integer	送信ポート SNMP ifIndex

#	項目	説明					
				mac_kind	String	MAC アドレス種別（ユニキャスト，マルチキャスト，ブロードキャスト） unicast, broadcast, multicast, unicast_broadcast, unicast_multicast, broadcast_multicast, all
				ip_kind	String	IPv4 アドレス種別（ユニキャスト＋ブロードキャスト，マルチキャスト） unicast_broadcast, multicast, all
				ipv6_kind	String	IPv6 アドレス種別 all：すべて unicast：ユニキャスト multicast：マルチキャスト unicast_linklocal_or_multicast：ユニキャスト（リンクローカル）＋マルチキャスト unicast_exclude_linklocal：ユニキャスト（リンクローカル以外） unicast_execlude_linklocal_or_multicast：ユニキャスト（リンクローカル以外）＋マルチキャスト
				packet_field	List	パケットフィールドフィルタ。AND 条件リスト。最大指定数：10 リスト。
					List	OR 条件リスト。最大指定数："packet_field"（パケットフィールドフィルタ）の総計で 100 リスト。
				@exclude	Boolean	除外条件。未指定時は False。
				flowset_id	Integer	フローセット ID
				sensor_addr	String	センサ IPv4 アドレス（ネットフローパケット送信元 IP アドレス）
				monitor_port_ifindex	Integer	センサモニタポート SNMP ifIndex
				output_port_ifindex	Integer	送信ポート SNMP ifIndex
				src_vlan	Integer	VLAN-ID 値（QinQ の場合，S-TAG）
				dst_vlan	Integer	VLAN-ID 値（QinQ の C-TAG）
				in_src_mac	String	送信元 MAC アドレス値。（例）00:00:5e:00:53:01
				in_dst_mac	String	宛先 MAC アドレス値。（例）00:00:5e:00:53:01
				ipv4_src_addr	String	送信元 IPv4 アドレス値
				ipv4_dst_addr	String	宛先 IPv4 アドレス値
				ipv6_src_addr	String	送信元 IPv6 アドレス値
				ipv6_dst_addr	String	宛先 IPv6 アドレス値

#	項目	説明					
					protocol	Integer	プロトコル番号
					icmp_type	Integer	ICMP タイプ値
					icmp_code	Integer	ICMP コード値
					l4_src_port	Integer	送信元 L4 ポート番号
					l4_dst_port	Integer	宛先 L4 ポート番号
					tcp_flags	String	TCP フラグ。 fin, syn, rst, psh, ack, urg, ece, cwr 半角スペースでくぎることで複数フラグを指定可。上記文字列の先頭に! を指定することで，対象フラグが Off のフローを指定可。 （例）"syn !ack"
					udp_rtp_ssrc	Integer	UDP RTP SSRC
					udp_rtp_pt	Integer	UDP RTP Payload Type
					udp_rtp_clock_rate	Integer	UDP RTP Clock Rate
					http_servername	String	HTTP サーバ名
					nat_ipv4_src_addr	String	NAT 送信元 IPv4 アドレス値
					nat_ipv4_dst_addr	String	NAT 宛先 IPv4 アドレス値
					nat_ipv6_src_addr	String	NAT 送信元 IPv6 アドレス値
					nat_ipv6_dst_addr	String	NAT 宛先 IPv6 アドレス値
					nat_l4_src_port	Integer	NAT 送信元 L4 ポート番号
					nat_l4_dst_port	Integer	NAT 宛先 L4 ポート番号
					nat_l4port_start	Integer	NAT L4 ポート番号範囲 Start
					nat_l4port_end	Integer	NAT L4 ポート番号範囲 End
					nat_event	Integer	NAT イベント
					nat_type	Integer	NAT タイプ
					vdom_name	String	バーチャルドメイン名
					ext01	String	フロー拡張データ 01
					ext02	String	フロー拡張データ 02
					ext03	String	フロー拡張データ 03
					ext04	String	フロー拡張データ 04
					ext05	String	フロー拡張データ 05
					ext06	String	フロー拡張データ 06
					ext07	String	フロー拡張データ 07
					ext08	String	フロー拡張データ 08
					ext09	String	フロー拡張データ 09
					ext10	String	フロー拡張データ 10
					ext11	String	国コード（送信元）
					ext12	String	国（送信元）
					ext13	String	地域（送信元）
					ext14	String	都市（送信元）
					ext15	String	AS 番号（送信元）
					ext16	String	AS 組織名（宛先）
					ext21	String	国コード（宛先）
					ext22	String	国（宛先）
					ext23	String	地域（宛先）
					ext24	String	都市（宛先）
					ext25	String	AS 番号（宛先）

#	項目	説明			
			ext26	String	AS 組織名（宛先）
			aggregate_option	Object	集計オプション
			packets	Boolean	パケット数
			out_packets	Boolean	送信パケット数
			out_bytes	Boolean	送信バイト数
			tcp_retx_pkts	Boolean	TCP 再送パケット数
			tcp_retx_bytes	Boolean	TCP 再送バイト数
			tcp_pkt_losses	Boolean	TCP パケットロス回数
			tcp_dupack_pkts	Boolean	TCP 重複 ACK パケット数
			tcp_retx_pkts_percent	Boolean	TCP 再送パケット数割合（%）
			tcp_retx_bytes_percent	Boolean	TCP 再送バイト数割合（%）
			tcp_pkt_losses_percent	Boolean	TCP パケットロス回数割合（%）
			udp_rtp_out_of_order	Boolean	UDP RTP 順序違反回数
			udp_rtp_lost_pkts	Boolean	UDP RTP ロストパケット数
			udp_rtp_lost_pkts_percent	Boolean	UDP RTP ロストパケット数割合（%）
			nat_duration	Boolean	NAT 継続時間（s）
7	レスポンス	レスポンスステータス	以下のステータスコードを応答します。		

コード	内容
200	成功
400	要求不正エラー
401	認証エラー
403	アクセス禁止
408	タイムアウト
500	内部エラー
503	サービス利用不可

#	項目	説明	
8		Content-Type	application/json

<table>
<tr><th>#</th><th>項目</th><th>説明</th><th></th></tr>
<tr><td>9</td><td></td><td>レスポンスボディ：

ステータスコード=200 の場合</td><td>・例
[
{
"datetime": "2021-01-11T10:00:00+09:00",
"bytes_counts": 37884564
},
： ～省略～
{
"datetime": "2021-01-11T11:55:00+09:00",
"bytes_counts": 33339574
}
]

・パラメータ説明
<table><tr><th>パラメータ名</th><th>型</th><th>説明</th></tr><tr><td></td><td>List</td><td>応答リスト。</td></tr><tr><td>datetime</td><td>String</td><td>対象時刻。</td></tr><tr><td>bytes_counts</td><td>Integer64</td><td>集計バイト数</td></tr><tr><td>packets_counts</td><td>Integer64</td><td>集計パケット数</td></tr><tr><td>out_bytes_counts</td><td>Integer64</td><td>集計送信バイト数</td></tr><tr><td>out_packets_counts</td><td>Integer64</td><td>集計送信パケット数</td></tr><tr><td>tcp_retx_pkts_counts</td><td>Integer64</td><td>集計 TCP 再送パケット数</td></tr><tr><td>tcp_retx_bytes_counts</td><td>Integer64</td><td>集計 TCP 再送バイト数</td></tr><tr><td>tcp_pkt_losses_counts</td><td>Integer64</td><td>集計 TCP パケットロス回数</td></tr><tr><td>tcp_dupack_pkts_counts</td><td>Integer64</td><td>集計 TCP 重複 ACK パケット数</td></tr><tr><td>tcp_retx_pkts_percent</td><td>Float</td><td>集計 TCP 再送パケット数割合（%）</td></tr><tr><td>tcp_retx_bytes_percent</td><td>Float</td><td>集計 TCP 再送バイト数割合（%）</td></tr><tr><td>tcp_pkt_losses_percent</td><td>float</td><td>集計 TCP パケットロス回数割合（%）</td></tr><tr><td>udp_rtp_out_of_order_counts</td><td>Integer64</td><td>UDP RTP 順序違反回数</td></tr><tr><td>udp_rtp_lost_pkts_counts</td><td>Integer64</td><td>UDP RTP ロストパケット数</td></tr><tr><td>udp_rtp_lost_pkts_percent</td><td>float</td><td>UDP RTP ロストパケット数割合（%）</td></tr><tr><td>nat_duration</td><td>Float</td><td>NAT 継続時間（s）</td></tr></table></td></tr>
</table>

<table>
<tr><th>#</th><th>項目</th><th>説明</th><th></th></tr>
<tr><td>10</td><td></td><td>レスポンスボディ：

ステータスコード=200 以外の場合</td><td>・例
{
"detail": "ユーザ名かパスワードが違います。"
}
・パラメータ説明
<table><tr><th>パラメータ名</th><th>型</th><th>説明</th></tr><tr><td>detail</td><td>String</td><td>エラー詳細を格納します。</td></tr></table></td></tr>
</table>

7.3.4 IP フロー パケット数時系列データ取得 API

IP フロー情報を検索し，パケット数の時系列情報を取得します。

表 7-13 IP フロー パケット数時系列データ取得 API

<table>
<tr><th>#</th><th>項目</th><th>説明</th><th></th></tr>
<tr><td>1</td><td>メソッド</td><td colspan="2">POST</td></tr>
<tr><td>2</td><td>URI</td><td colspan="2">/api/v1/flowdata/ip/timeseries/packets/
または
/api/v1/flowdata/ipv4/timeseries/packets/</td></tr>
<tr><td>3</td><td rowspan="4">リクエスト</td><td>認証</td><td>ベーシック認証もしくはトークン認証。</td></tr>
<tr><td>4</td><td>クエリパラメータ</td><td>なし</td></tr>
<tr><td>5</td><td>Content-Type</td><td>application/json</td></tr>
<tr><td>6</td><td>ボディパラメータ</td><td>・例
{
"time_from": "2021-01-11T10:00:00+09:00",
"time_to": "2021-01-11T12:00:00+09:00",
"time_interval":"5m",
"search_filters":{
"packet_field" : [
[{"src_vlan":4000 }, {"src_vlan":3000}]
]
}
}

・パラメータ説明（*必須パラメータ）</td></tr>
</table>

#	項目	説明

パラメータ名	型	説明
time_from *	String	検索時刻 - 始まり。ISO8601 フォーマット。（例）2021-01-11T10:00:00+09:00
time_to *	String	検索時刻 - 終わり。ISO8601 フォーマット。（例）2021-01-11T12:00:00+09:00
time_interval *	String	取得間隔。 1s, 10s, 30s, 1m, 5m, 10m, 15m, 30m, 1h, 3h, 6h, 12h, 1d
search_filters	Object	検索フィルタ条件
sensor_addr	String	センサ IPv4 アドレス（ネットフローパケット送信元 IP アドレス）
monitor_port_ifindex	Integer	センサモニタポート SNMP ifIndex
output_port_ifindex	Integer	送信ポート SNMP ifIndex
mac_kind	String	MAC アドレス種別（ユニキャスト，マルチキャスト，ブロードキャスト） unicast, broadcast, multicast, unicast_broadcast, unicast_multicast, broadcast_multicast, all
ip_kind	String	IPv4 アドレス種別（ユニキャスト＋ブロードキャスト，マルチキャスト） unicast_broadcast, multicast, all
ipv6_kind	String	IPv6 アドレス種別 all：すべて unicast：ユニキャスト multicast：マルチキャスト unicast_linklocal_or_multicast：ユニキャスト（リンクローカル）＋マルチキャスト unicast_exclude_linklocal：ユニキャスト（リンクローカル以外） unicast_execlude_linklocal_or_multicast：ユニキャスト（リンクローカル以外）＋マルチキャスト
packet_field	List	パケットフィールドフィルタ。AND 条件リスト。最大指定数：10 リスト。
	List	OR 条件リスト。最大指定数："packet_field"（パケットフィールドフィルタ）の総計で 100 リスト。
@exclude	Boolean	除外条件。未指定時は False。

#	項目	説明					
					flowset_id	Integer	フローセット ID
					sensor_addr	String	センサ IPv4 アドレス（ネットフローパケット送信元 IP アドレス）
					monitor_port_ifindex	Integer	センサモニタポート SNMP ifIndex
					output_port_ifindex	Integer	送信ポート SNMP ifIndex
					src_vlan	Integer	VLAN-ID 値（QinQ の場合，S-TAG）
					dst_vlan	Integer	VLAN-ID 値（QinQ の C-TAG）
					in_src_mac	String	送信元 MAC アドレス値。（例） 00:00:5e:00:53:01
					in_dst_mac	String	宛先 MAC アドレス値。（例） 00:00:5e:00:53:01
					ipv4_src_addr	String	送信元 IPv4 アドレス値
					ipv4_dst_addr	String	宛先 IPv4 アドレス値
					ipv6_src_addr	String	送信元 IPv6 アドレス値
					ipv6_dst_addr	String	宛先 IPv6 アドレス値
					protocol	Integer	プロトコル番号
					icmp_type	Integer	ICMP タイプ値
					icmp_code	Integer	ICMP コード値
					l4_src_port	Integer	送信元 L4 ポート番号
					l4_dst_port	Integer	宛先 L4 ポート番号
					tcp_flags	String	TCP フラグ。 fin, syn, rst, psh, ack, urg, ece, cwr 半角スペースでくぎることで複数フラグを指定可。上記文字列の先頭に! を指定することで，対象フラグが Off のフローを指定可。 （例）"syn !ack"
					udp_rtp_ssrc	Integer	UDP RTP SSRC
					udp_rtp_pt	Integer	UDP RTP Payload Type
					udp_rtp_clock_rate	Integer	UDP RTP Clock Rate
					http_servername	String	HTTP サーバ名
					ext01	String	フロー拡張データ 01
					nat_ipv4_src_addr	String	NAT 送信元 IPv4 アドレス値
					nat_ipv4_dst_addr	String	NAT 宛先 IPv4 アドレス値
					nat_ipv6_src_addr	String	NAT 送信元 IPv6 アドレス値
					nat_ipv6_dst_addr	String	NAT 宛先 IPv6 アドレス値
					nat_l4_src_port	Integer	NAT 送信元 L4 ポート番号
					nat_l4_dst_port	Integer	NAT 宛先 L4 ポート番号
					nat_l4port_start	Integer	NAT L4 ポート番号範囲 Start
					nat_l4port_end	Integer	NAT L4 ポート番号範囲 End
					nat_event	Integer	NAT イベント
					nat_type	Integer	NAT タイプ
					vdom_name	String	バーチャルドメイン名
					ext01	String	フロー拡張データ 01
					ext02	String	フロー拡張データ 02
					ext03	String	フロー拡張データ 03
					ext04	String	フロー拡張データ 04
					ext05	String	フロー拡張データ 05

#	項目	説明				
				ext06	String	フロー拡張データ 06
				ext07	String	フロー拡張データ 07
				ext08	String	フロー拡張データ 08
				ext09	String	フロー拡張データ 09
				ext10	String	フロー拡張データ 10
				ext11	String	国コード（送信元）
				ext12	String	国（送信元）
				ext13	String	地域（送信元）
				ext14	String	都市（送信元）
				ext15	String	AS 番号（送信元）
				ext16	String	AS 組織名（宛先）
				ext21	String	国コード（宛先）
				ext22	String	国（宛先）
				ext23	String	地域（宛先）
				ext24	String	都市（宛先）
				ext25	String	AS 番号（宛先）
				ext26	String	AS 組織名（宛先）
			aggregate_option		Object	集計オプション
			bytes		Boolean	バイト数
			out_packets		Boolean	送信パケット数
			out_bytes		Boolean	送信バイト数
			tcp_retx_pkts		Boolean	TCP 再送パケット数
			tcp_retx_bytes		Boolean	TCP 再送バイト数
			tcp_pkt_losses		Boolean	TCP パケットロス回数
			tcp_dupack_pkts		Boolean	TCP 重複 ACK パケット数
			tcp_retx_pkts_percent		Boolean	TCP 再送パケット数割合（%）
			tcp_retx_bytes_percent		Boolean	TCP 再送バイト数割合（%）
			tcp_pkt_losses_percent		Boolean	TCP パケットロス回数割合（%）
			udp_rtp_out_of_order		Boolean	UDP RTP 順序違反回数
			udp_rtp_lost_pkts		Boolean	UDP RTP ロストパケット数
			udp_rtp_lost_pkts_percent		Boolean	UDP RTP ロストパケット数割合（%）
			nat_duration		Boolean	NAT 継続時間（s）

<table>
<tr><th>#</th><th>項目</th><th>説明</th><th></th></tr>
<tr><td>7</td><td rowspan="2">レスポンス</td><td>レスポンスステータス</td><td>以下のステータスコードを応答します。<table><tr><th>コード</th><th>内容</th></tr><tr><td>200</td><td>成功</td></tr><tr><td>400</td><td>要求不正エラー</td></tr><tr><td>401</td><td>認証エラー</td></tr><tr><td>403</td><td>アクセス禁止</td></tr><tr><td>408</td><td>タイムアウト</td></tr><tr><td>500</td><td>内部エラー</td></tr><tr><td>503</td><td>サービス利用不可</td></tr></table></td></tr>
<tr><td>8</td><td>Content-Type</td><td>application/json</td></tr>
</table>

<table>
<tr><th>#</th><th>項目</th><th>説明</th><th></th></tr>
<tr><td>9</td><td></td><td>レスポンスボディ：

ステータスコード=200 の場合</td><td>・例
[
{
"datetime": "2021-01-11T10:00:00+09:00",
"packets_counts": 37884564
},
： ～省略～
{
"datetime": "2021-01-11T11:55:00+09:00",
"packets_counts": 33339574
}
]

・パラメータ説明
<table><tr><th>パラメータ名</th><th>型</th><th>説明</th></tr><tr><td></td><td>List</td><td>応答リスト。</td></tr><tr><td>datetime</td><td>String</td><td>対象時刻。</td></tr><tr><td>packets_counts</td><td>Integer64</td><td>集計パケット数</td></tr><tr><td>bytes_counts</td><td>Integer64</td><td>集計バイト数</td></tr><tr><td>out_bytes_counts</td><td>Integer64</td><td>集計送信バイト数</td></tr><tr><td>out_packets_counts</td><td>Integer64</td><td>集計送信パケット数</td></tr><tr><td>tcp_retx_pkts_counts</td><td>Integer64</td><td>集計 TCP 再送パケット数</td></tr><tr><td>tcp_retx_bytes_counts</td><td>Integer64</td><td>集計 TCP 再送バイト数</td></tr><tr><td>tcp_pkt_losses_counts</td><td>Integer64</td><td>集計 TCP パケットロス回数</td></tr><tr><td>tcp_dupack_pkts_counts</td><td>Integer64</td><td>集計 TCP 重複 ACK パケット数</td></tr><tr><td>tcp_retx_pkts_percent</td><td>Float</td><td>集計 TCP 再送パケット数割合（%）</td></tr><tr><td>tcp_retx_bytes_percent</td><td>Float</td><td>集計 TCP 再送バイト数割合（%）</td></tr><tr><td>tcp_pkt_losses_percent</td><td>float</td><td>集計 TCP パケットロス回数割合（%）</td></tr><tr><td>udp_rtp_out_of_order_counts</td><td>Integer64</td><td>UDP RTP 順序違反回数</td></tr><tr><td>udp_rtp_lost_pkts_counts</td><td>Integer64</td><td>UDP RTP ロストパケット数</td></tr><tr><td>udp_rtp_lost_pkts_percent</td><td>float</td><td>UDP RTP ロストパケット数割合（%）</td></tr><tr><td>nat_duration</td><td>Float</td><td>NAT 継続時間（s）</td></tr></table></td></tr>
</table>

<table>
<tr><th>#</th><th>項目</th><th>説明</th><th></th></tr>
<tr><td>10</td><td></td><td>レスポンスボディ：

ステータスコード=200 以外の場合</td><td>・例
{
"detail": "ユーザ名かパスワードが違います。"
}
・パラメータ説明
<table><tr><th>パラメータ名</th><th>型</th><th>説明</th></tr><tr><td>detail</td><td>String</td><td>エラー詳細を格納します。</td></tr></table></td></tr>
</table>

7.4 MAC フロー情報検索 API

7.4.1 MAC フロー バイト数ランキング取得 API

MAC フロー情報を検索し，バイト数ランキング上位のパケット情報を取得します。

表 7-14 MAC フロー バイト数ランキング取得 API

#	項目	説明	
1	メソッド	POST	
2	URI	/api/v1/flowdata/mac/ranking/bytes/	
3	リクエスト	認証	ベーシック認証もしくはトークン認証。
4		クエリパラメータ	なし
5		Content-Type	application/json

6		ボディパラメータ	・例
			{
			"time_from": "2021-01-11T10:00:00+09:00",
			"time_to": "2021-01-11T12:00:00+09:00",
			"numbers":10,
			"search_filters":{
			"packet_field" : [
			[{"src_vlan":4000 }, {"src_vlan":3000}]
			]
			},
			"aggregate_groups": {
			"in_src_mac":true
			}
			}
			
			・パラメータ説明（*必須パラメータ）

パラメータ名	型	説明
time_from *	String	検索時刻 - 始まり。ISO8601 フォーマット。（例）2021-01-11T10:00:00+09:00
time_to *	String	検索時刻 - 終わり。ISO8601 フォーマット。（例）2021-01-11T12:00:00+09:00
numbers	integer	取得する検索結果数。指定範囲は，1～100000。省略時：10。
search_filters	Object	検索フィルタ条件
sensor_addr	String	センサ IPv4 アドレス（ネットフローパケット送信元 IP アドレス）
monitor_port_ifindex	Integer	センサモニタポート SNMP ifIndex
output_port_ifindex	Integer	送信ポート SNMPifIndex

#	項目	説明				
				mac_kind	String	MAC アドレス種別（ユニキャスト，マルチキャスト，ブロードキャスト） unicast, broadcast, multicast, unicast_broadcast, unicast_multicast, broadcast_multicast, all
				packet_field	List	パケットフィールドフィルタ。AND 条件リスト。最大指定数：10 リスト。
					List	OR 条件リスト。最大指定数："packet_field"（パケットフィールドフィルタ）の総計で 100 リスト。
				@exclude	Boolean	除外条件。未指定時は False。
				flowset_id	Integer	フローセット ID
				sensor_addr	String	センサ IPv4 アドレス（ネットフローパケット送信元 IP アドレス）
				monitor_port_ifindex	Integer	センサモニタポート SNMP ifIndex
				output_port_ifindex	Integer	送信ポート SNMP ifIndex
				ether_type	Integer	イーサタイプ値
				src_vlan	Integer	VLAN-ID 値（QinQ の場合，S-TAG）
				dst_vlan	Integer	VLAN-ID 値（QinQ の C-TAG）
				in_src_mac	String	送信元 MAC アドレス値。（例） 00:00:5e:00:53:01
				in_dst_mac	String	宛先 MAC アドレス値。（例） 00:00:5e:00:53:01
				ext01	String	フロー拡張データ 01
				ext02	String	フロー拡張データ 02
				ext03	String	フロー拡張データ 03
				ext04	String	フロー拡張データ 04
				ext05	String	フロー拡張データ 05
				ext06	String	フロー拡張データ 06
				ext07	String	フロー拡張データ 07
				ext08	String	フロー拡張データ 08
				ext09	String	フロー拡張データ 09

#	項目	説明			
			ext10	String	フロー拡張データ 10
			aggregate_groups *	Object	検索集約条件
			timestamp	Boolean	タイムスタンプ毎の集計
			flowset_id	Boolean	フローセット ID 毎の集計
			sensor_addr	Boolean	センサ IPv4 アドレス毎の集計
			monitor_port_ifindex	Boolean	センサモニタポート SNMP ifIndex 毎の集計
			output_port_ifindex	Boolean	送信ポート SNMP ifIndex 毎の集計
			ether_type	Boolean	イーサタイプ毎の集計
			src_vlan	Boolean	VLAN-ID（QinQ の場合，S-TAG）毎の集計
			dst_vlan	Boolean	QinQ の C-TAG 毎の集計
			in_src_mac	Boolean	送信元 MAC アドレス毎の集計
			in_dst_mac	Boolean	宛先 MAC アドレス毎の集計
			ext01	Boolean	フロー拡張データ 01 毎の集計
			ext02	Boolean	フロー拡張データ 02 毎の集計
			ext03	Boolean	フロー拡張データ 03 毎の集計
			ext04	Boolean	フロー拡張データ 04 毎の集計
			ext05	Boolean	フロー拡張データ 05 毎の集計
			ext06	Boolean	フロー拡張データ 06 毎の集計
			ext07	Boolean	フロー拡張データ 07 毎の集計
			ext08	Boolean	フロー拡張データ 08 毎の集計
			ext09	Boolean	フロー拡張データ 09 毎の集計
			ext10	Boolean	フロー拡張データ 10 毎の集計
			aggregate_option	Object	集計オプション
			packets	Boolean	パケット数

<table>
<tr><th>#</th><th>項目</th><th>説明</th><th></th></tr>
<tr><td>7</td><td>レスポンス</td><td>レスポンスステータス</td><td>以下のステータスコードを応答します。<table><tr><th>コード</th><th>内容</th></tr><tr><td>200</td><td>成功</td></tr><tr><td>400</td><td>要求不正エラー</td></tr><tr><td>401</td><td>認証エラー</td></tr><tr><td>403</td><td>アクセス禁止</td></tr><tr><td>408</td><td>タイムアウト</td></tr><tr><td>500</td><td>内部エラー</td></tr><tr><td>503</td><td>サービス利用不可</td></tr></table></td></tr>
<tr><td>8</td><td></td><td>Content-Type</td><td>application/json</td></tr>
</table>

9

レスポンス
ボディ：

ステータスコード=200 の場合

・例

```
[
   {
      "rank": 1,
      "packets_info": {
         "in_src_mac": "00:00:5e:00:53:01",
         "in_src_mac_alias": "-",
         "in_src_mac_vendor": "XXX"
      },
      "bytes_counts": 37884564
   },
   :  ～省略～
   {
      "rank": 5,
      "packets_info": {
         "in_src_mac": "00:00:5e:00:53:02",
         "in_src_mac_alias": "-",
         "in_src_mac_vendor": "XXX"
      },
      "bytes_counts": 33339574
   }
]
```

・パラメータ説明

パラメータ名		型	説明
		List	応答リスト。
rank		Integer	集計ランキング
packets_info		Object	パケット情報 aggregate_groups で，指定された関連情報のみ格納
	timestamp	String	タイムスタンプ
	flowset_id	Integer	フローセット ID
	sensor_addr	String	センサ IPv4 アドレス（ネットフローパケット送信元 IP アドレス）
	sensor_addr_alias	String	センサ IPv4 アドレスエイリアス
	monitor_port_ifindex	Integer	センサモニタポート SNMP ifIndex
	monitor_port_alias	String	センサモニタポート SNMP ifIndex エイリアス
	output_port_ifindex	Integer	送信ポート SNMP ifIndex
	output_port_alias	String	送信ポート SNMP ifIndex エイリアス
	ether_type	Integer	イーサタイプ値
	ether_type_name	String	イーサタイプ名
	src_vlan	Integer	VLAN-ID 値（QinQ の場合，S-TAG）

<table>
<tr><th>#</th><th>項目</th><th>説明</th><td colspan="4">
<table>
<tr><td></td><td>src_vlan_alias</td><td>String</td><td>VLAN-ID エイリアス。dst_vlan 集約時は非表示。</td></tr>
<tr><td></td><td>dst_vlan</td><td>Integer</td><td>VLAN-ID 値（QinQ の C-TAG）</td></tr>
<tr><td></td><td>qinq_alias</td><td>String</td><td>VLAN(QinQ)エイリアス。src_vlan/dst_vlan 集約時に表示。</td></tr>
<tr><td></td><td>in_src_mac</td><td>String</td><td>送信元 MAC アドレス値</td></tr>
<tr><td></td><td>in_src_mac_alias</td><td>String</td><td>送信元 MAC アドレスエイリアス</td></tr>
<tr><td></td><td>in_src_mac_vendor</td><td>String</td><td>送信元 MAC アドレスベンダ名</td></tr>
<tr><td></td><td>in_dst_mac</td><td>String</td><td>宛先 MAC アドレス値</td></tr>
<tr><td></td><td>in_dst_mac_alias</td><td>String</td><td>宛先 MAC アドレスエイリアス</td></tr>
<tr><td></td><td>in_dst_mac_vendor</td><td>String</td><td>宛先 MAC アドレスベンダ名</td></tr>
<tr><td></td><td>ext01</td><td>String</td><td>フロー拡張データ 01</td></tr>
<tr><td></td><td>ext02</td><td>String</td><td>フロー拡張データ 02</td></tr>
<tr><td></td><td>ext03</td><td>String</td><td>フロー拡張データ 03</td></tr>
<tr><td></td><td>ext04</td><td>String</td><td>フロー拡張データ 04</td></tr>
<tr><td></td><td>ext05</td><td>String</td><td>フロー拡張データ 05</td></tr>
<tr><td></td><td>ext06</td><td>String</td><td>フロー拡張データ 06</td></tr>
<tr><td></td><td>ext07</td><td>String</td><td>フロー拡張データ 07</td></tr>
<tr><td></td><td>ext08</td><td>String</td><td>フロー拡張データ 08</td></tr>
<tr><td></td><td>ext09</td><td>String</td><td>フロー拡張データ 09</td></tr>
<tr><td></td><td>ext10</td><td>String</td><td>フロー拡張データ 10</td></tr>
<tr><td colspan="2">bytes_counts</td><td>Integer64</td><td>集計バイト数</td></tr>
<tr><td colspan="2">packets_counts</td><td>Integer64</td><td>集計パケット数</td></tr>
</table>
</td></tr>
<tr><td>10</td><td></td><td>レスポンスボディ：

ステータスコード=200 以外の場合</td><td colspan="4">・例
{
"detail": "ユーザ名かパスワードが違います。"
}
・パラメータ説明
<table>
<tr><th>パラメータ名</th><th>型</th><th>説明</th></tr>
<tr><td>detail</td><td>String</td><td>エラー詳細を格納します。</td></tr>
</table>
</td></tr>
</table>

7.4.2 MAC フロー パケット数ランキング取得 API

MAC フロー情報を検索し，パケット数ランキング上位のパケット情報を取得します。

表 7-15 MAC フロー パケット数ランキング取得 API

#	項目	説明	
1	メソッド	POST	
2	URI	/api/v1/flowdata/mac/ranking/packets/	
3	リクエスト	認証	ベーシック認証もしくはトークン認証。
4		クエリパラメータ	なし
5		Content-Type	application/json

6		ボディパラメータ	・例
			{
			"time_from": "2021-01-11T10:00:00+09:00",
			"time_to": "2021-01-11T12:00:00+09:00",
			"numbers":10,
			"search_filters":{
			"packet_field" : [
			[{"src_vlan":4000 }, {"src_vlan":3000}]
			]
			},
			"aggregate_groups": {
			"in_src_mac":true
			}
			}

・パラメータ説明（*必須パラメータ）

パラメータ名	型	説明
time_from *	String	検索時刻 - 始まり。ISO8601 フォーマット。（例）2021-01-11T10:00:00+09:00
time_to *	String	検索時刻 - 終わり。ISO8601 フォーマット。（例）2021-01-11T12:00:00+09:00
numbers	integer	取得する検索結果数。指定範囲は，1～100000。省略時：10。
search_filters	Object	検索フィルタ条件
sensor_addr	String	センサ IPv4 アドレス（ネットフローパケット送信元 IP アドレス）
monitor_port_ifindex	Integer	センサモニタポート SNMP ifIndex
output_port_ifindex	Integer	送信ポート SNMPifIndex

#	項目	説明				
				mac_kind	String	MAC アドレス種別（ユニキャスト，マルチキャスト，ブロードキャスト） unicast, broadcast, multicast, unicast_broadcast, unicast_multicast, broadcast_multicast, all
				packet_field	List	パケットフィールドフィルタ。AND 条件リスト。最大指定数：10 リスト。
					List	OR 条件リスト。最大指定数："packet_field"（パケットフィールドフィルタ）の総計で 100 リスト。
				@exclude	Boolean	除外条件。未指定時は False。
				flowset_id	Integer	フローセット ID
				sensor_addr	String	センサ IPv4 アドレス（ネットフローパケット送信元 IP アドレス）
				monitor_port_ifindex	Integer	センサモニタポート SNMP ifIndex
				output_port_ifindex	Integer	送信ポート SNMP ifIndex
				ether_type	Integer	イーサタイプ値
				src_vlan	Integer	VLAN-ID 値（QinQ の場合，S-TAG）
				dst_vlan	Integer	VLAN-ID 値（QinQ の C-TAG）
				in_src_mac	String	送信元 MAC アドレス値。（例） 00:00:5e:00:53:01
				in_dst_mac	String	宛先 MAC アドレス値。（例） 00:00:5e:00:53:01
				ext01	String	フロー拡張データ 01
				ext02	String	フロー拡張データ 02
				ext03	String	フロー拡張データ 03
				ext04	String	フロー拡張データ 04
				ext05	String	フロー拡張データ 05
				ext06	String	フロー拡張データ 06
				ext07	String	フロー拡張データ 07
				ext08	String	フロー拡張データ 08
				ext09	String	フロー拡張データ 09

#	項目	説明			
			ext10	String	フロー拡張データ 10
			aggregate_groups *	Object	検索集約条件
			timestamp	Boolean	タイムスタンプ毎の集計
			flowset_id	Boolean	フローセット ID 毎の集計
			sensor_addr	Boolean	センサ IPv4 アドレス毎の集計
			monitor_port_ifindex	Boolean	センサモニタポート SNMP ifIndex 毎の集計
			output_port_ifindex	Boolean	送信ポート SNMP ifIndex 毎の集計
			ether_type	Boolean	イーサタイプ毎の集計
			src_vlan	Boolean	VLAN-ID（QinQ の場合，S-TAG）毎の集計
			dst_vlan	Boolean	QinQ の C-TAG 毎の集計
			in_src_mac	Boolean	送信元 MAC アドレス毎の集計
			in_dst_mac	Boolean	宛先 MAC アドレス毎の集計
			ext01	Boolean	フロー拡張データ 01 毎の集計
			ext02	Boolean	フロー拡張データ 02 毎の集計
			ext03	Boolean	フロー拡張データ 03 毎の集計
			ext04	Boolean	フロー拡張データ 04 毎の集計
			ext05	Boolean	フロー拡張データ 05 毎の集計
			ext06	Boolean	フロー拡張データ 06 毎の集計
			ext07	Boolean	フロー拡張データ 07 毎の集計
			ext08	Boolean	フロー拡張データ 08 毎の集計
			ext09	Boolean	フロー拡張データ 09 毎の集計
			ext10	Boolean	フロー拡張データ 10 毎の集計
			aggregate_option	Object	集計オプション
			bytes	Boolean	バイト数

<table>
<tr><th>#</th><th>項目</th><th>説明</th><th></th></tr>
<tr><td>7</td><td>レスポンス</td><td>レスポンスステータス</td><td>以下のステータスコードを応答します。<table><tr><th>コード</th><th>内容</th></tr><tr><td>200</td><td>成功</td></tr><tr><td>400</td><td>要求不正エラー</td></tr><tr><td>401</td><td>認証エラー</td></tr><tr><td>403</td><td>アクセス禁止</td></tr><tr><td>408</td><td>タイムアウト</td></tr><tr><td>500</td><td>内部エラー</td></tr><tr><td>503</td><td>サービス利用不可</td></tr></table></td></tr>
<tr><td>8</td><td></td><td>Content-Type</td><td>application/json</td></tr>
</table>

9

レスポンス
ボディ：

ステータスコード=200 の場合

・例

```
[
  {
    "rank": 1,
    "packets_info": {
      "in_src_mac": "00:00:5e:00:53:01",
      "in_src_mac_alias": "-",
      "in_src_mac_vendor": "XXX"
    },
    "packets_counts": 37884564
  },
  :  ～省略～
  {
    "rank": 5,
    "packets_info": {
      "in_src_mac": "00:00:5e:00:53:02",
      "in_src_mac_alias": "-",
      "in_src_mac_vendor": "XXX"
    },
    "packets_counts": 33339574
  }
]
```

・パラメータ説明

パラメータ名		型	説明
		List	応答リスト。
rank		Integer	集計ランキング
packets_info		Object	パケット情報 aggregate_groups で，指定された関連情報のみ格納
	flowset_id	Integer	フローセット ID
	sensor_addr	String	センサ IPv4 アドレス（ネットフローパケット送信元 IP アドレス）
	sensor_addr_alias	String	センサ IPv4 アドレスエイリアス
	monitor_port_ifindex	Integer	センサモニタポート SNMP ifIndex
	monitor_port_alias	String	センサモニタポート SNMP ifIndex エイリアス
	output_port_ifindex	Integer	送信ポート SNMP ifIndex
	output_prot_alias	String	送信ポート SNMP ifIndex エイリアス
	ether_type	Integer	イーサタイプ値
	ether_type_name	String	イーサタイプ名
	src_vlan	Integer	VLAN-ID 値（QinQ の場合，S-TAG）

<table>
<tr><th>#</th><th>項目</th><th>説明</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td></td><td>src_vlan_alias</td><td>String</td><td>VLAN-ID エイリアス。dst_vlan 集約時は非表示。</td></tr>
<tr><td></td><td>dst_vlan</td><td>Integer</td><td>VLAN-ID 値（QinQ の C-TAG）</td></tr>
<tr><td></td><td>qinq_alias</td><td>String</td><td>VLAN(QinQ)エイリアス。src_vlan/dst_vlan 集約時に表示。</td></tr>
<tr><td></td><td>in_src_mac</td><td>String</td><td>送信元 MAC アドレス値</td></tr>
<tr><td></td><td>in_src_mac_alias</td><td>String</td><td>送信元 MAC アドレスエイリアス</td></tr>
<tr><td></td><td>in_src_mac_vendor</td><td>String</td><td>送信元 MAC アドレスベンダ名</td></tr>
<tr><td></td><td>in_dst_mac</td><td>String</td><td>宛先 MAC アドレス値</td></tr>
<tr><td></td><td>in_dst_mac_alias</td><td>String</td><td>宛先 MAC アドレスエイリアス</td></tr>
<tr><td></td><td>in_dst_mac_vendor</td><td>String</td><td>宛先 MAC アドレスベンダ名</td></tr>
<tr><td></td><td>ext01</td><td>String</td><td>フロー拡張データ 01</td></tr>
<tr><td></td><td>ext02</td><td>String</td><td>フロー拡張データ 02</td></tr>
<tr><td></td><td>ext03</td><td>String</td><td>フロー拡張データ 03</td></tr>
<tr><td></td><td>ext04</td><td>String</td><td>フロー拡張データ 04</td></tr>
<tr><td></td><td>ext05</td><td>String</td><td>フロー拡張データ 05</td></tr>
<tr><td></td><td>ext06</td><td>String</td><td>フロー拡張データ 06</td></tr>
<tr><td></td><td>ext07</td><td>String</td><td>フロー拡張データ 07</td></tr>
<tr><td></td><td>ext08</td><td>String</td><td>フロー拡張データ 08</td></tr>
<tr><td></td><td>ext09</td><td>String</td><td>フロー拡張データ 09</td></tr>
<tr><td></td><td>ext10</td><td>String</td><td>フロー拡張データ 10</td></tr>
<tr><td colspan="2">packets_counts</td><td>Integer64</td><td>集計パケット数</td></tr>
<tr><td colspan="2">bytes_counts</td><td>Integer64</td><td>集計バイト数</td></tr>
</table>
</td></tr>
<tr><td>10</td><td></td><td>レスポンスボディ：

ステータスコード=200 以外の場合</td><td>・例
{
"detail": "ユーザ名かパスワードが違います。"
}
・パラメータ説明
<table>
<tr><th>パラメータ名</th><th>型</th><th>説明</th></tr>
<tr><td>detail</td><td>String</td><td>エラー詳細を格納します。</td></tr>
</table>
</td></tr>
</table>

7.4.3 MAC フロー バイト数時系列データ取得 API

MAC フロー情報を検索し，バイト数の時系列情報を取得します。

表 7-16 MAC フロー バイト数時系列データ取得 API

#	項目	説明
1	メソッド	POST

<table>
<tr><td>#</td><td>項目</td><td colspan="2">説明</td></tr>
<tr><td>2</td><td>URI</td><td colspan="2">/api/v1/flowdata/mac/timeseries/bytes/</td></tr>
<tr><td>3</td><td rowspan="4">リクエスト</td><td>認証</td><td>ベーシック認証もしくはトークン認証。</td></tr>
<tr><td>4</td><td>クエリパラメータ</td><td>なし</td></tr>
<tr><td>5</td><td>Content-Type</td><td>application/json</td></tr>
<tr><td>6</td><td>ボディパラメータ</td><td>・例
{
"time_from": "2021-01-11T10:00:00+09:00",
"time_to": "2021-01-11T12:00:00+09:00",
"time_interval":"5m",
"search_filters":{
"packet_field" : [
[{"src_vlan":4000 }, {"src_vlan":3000}]
]
}
}

・パラメータ説明（*必須パラメータ）
<table>
<tr><td>パラメータ名</td><td>型</td><td>説明</td></tr>
<tr><td>time_from *</td><td>String</td><td>検索時刻 - 始まり。
ISO8601 フォーマット。（例）2021-01-11T10:00:00+09:00</td></tr>
<tr><td>time_to *</td><td>String</td><td>検索時刻 - 終わり。
ISO8601 フォーマット。（例）2021-01-11T12:00:00+09:00</td></tr>
<tr><td>time_interval *</td><td>String</td><td>取得間隔。
1s, 10s, 30s, 1m, 5m, 10m, 15m, 30m, 1h, 3h, 6h, 12h, 1d</td></tr>
<tr><td>search_filters</td><td>Object</td><td>検索フィルタ条件</td></tr>
<tr><td>sensor_addr</td><td>String</td><td>センサ IPv4 アドレス（ネットフローパケット送信元 IP アドレス）</td></tr>
<tr><td>monitor_port_ifindex</td><td>Integer</td><td>センサモニタポート SNMP ifIndex</td></tr>
<tr><td>output_port_ifindex</td><td>Integer</td><td>送信ポート SNMPifIndex</td></tr>
<tr><td>mac_kind</td><td>String</td><td>MAC アドレス種別（ユニキャスト，マルチキャスト，ブロードキャスト）
unicast,
broadcast,
multicast,
unicast_broadcast,
unicast_multicast,
broadcast_multicast,
all</td></tr>
</table>
</td></tr>
</table>

#	項目	説明				
				packet_field	List	パケットフィールドフィルタ。AND 条件リスト。最大指定数：10 リスト。
					List	OR 条件リスト。最大指定数："packet_field"（パケットフィールドフィルタ）の総計で 100 リスト。
				@exclude	Boolean	除外条件。未指定時は False。
				flowset_id	Integer	フローセット ID
				sensor_addr	String	センサ IPv4 アドレス（ネットフローパケット送信元 IP アドレス）
				monitor_port_ifindex	Integer	センサモニタポート SNMP ifIndex
				output_port_ifindex	Integer	送信ポート SNMPifIndex
				ether_type	Integer	イーサタイプ値
				src_vlan	Integer	VLAN-ID 値（QinQ の場合，S-TAG）
				dst_vlan	Integer	VLAN-ID 値（QinQ の C-TAG）
				in_src_mac	String	送信元 MAC アドレス値。（例）00:00:5e:00:53:01
				in_dst_mac	String	宛先 MAC アドレス値。（例）00:00:5e:00:53:01
				ext01	String	フロー拡張データ 01
				ext02	String	フロー拡張データ 02
				ext03	String	フロー拡張データ 03
				ext04	String	フロー拡張データ 04
				ext05	String	フロー拡張データ 05
				ext06	String	フロー拡張データ 06
				ext07	String	フロー拡張データ 07
				ext08	String	フロー拡張データ 08
				ext09	String	フロー拡張データ 09
				ext10	String	フロー拡張データ 10
			aggregate_option		Object	集計オプション
				packets	Boolean	パケット数

<table>
<tr><td>#</td><td>項目</td><td>説明</td><td colspan="3"></td></tr>
<tr><td>7</td><td>レスポンス</td><td>レスポンス
ステータス</td><td colspan="3">以下のステータスコードを応答します。
<table><tr><td>コード</td><td>内容</td></tr><tr><td>200</td><td>成功</td></tr><tr><td>400</td><td>要求不正エラー</td></tr><tr><td>401</td><td>認証エラー</td></tr><tr><td>403</td><td>アクセス禁止</td></tr><tr><td>408</td><td>タイムアウト</td></tr><tr><td>500</td><td>内部エラー</td></tr><tr><td>503</td><td>サービス利用不可</td></tr></table></td></tr>
<tr><td>8</td><td></td><td>Content-Type</td><td colspan="3">application/json</td></tr>
<tr><td>9</td><td></td><td>レスポンス
ボディ：

ステータスコード=200 の場合</td><td colspan="3">・例
[
{
"datetime": "2021-01-11T10:00:00+09:00",
"bytes_counts": 37884564
},
： ～省略～
{
"datetime": "2021-01-11T11:55:00+09:00",
"bytes_counts": 33339574
}
]

・パラメータ説明
<table><tr><td>パラメータ名</td><td>型</td><td>説明</td></tr><tr><td></td><td>List</td><td>応答リスト。</td></tr><tr><td>datetime</td><td>String</td><td>対象時刻。</td></tr><tr><td>bytes_counts</td><td>Integer64</td><td>集計バイト数</td></tr><tr><td>packets_counts</td><td>Integer64</td><td>集計パケット数</td></tr></table></td></tr>
<tr><td>10</td><td></td><td>レスポンス
ボディ：

ステータスコード=200 以外の場合</td><td colspan="3">・例
{
"detail": "ユーザ名かパスワードが違います。"
}
・パラメータ説明
<table><tr><td>パラメータ名</td><td>型</td><td>説明</td></tr><tr><td>detail</td><td>String</td><td>エラー詳細を格納します。</td></tr></table></td></tr>
</table>

7.4.4 MAC フロー パケット数時系列データ取得 API

MAC フロー情報を検索し，パケット数の時系列情報を取得します。

表 7-17 MAC フロー パケット数時系列データ取得 API

#	項目	説明	
1	メソッド	POST	
2	URI	/api/v1/flowdata/mac/timeseries/packets/	
3		認証	ベーシック認証もしくはトークン認証。

<table>
<tr><th>#</th><th>項目</th><th>説明</th><th colspan="3"></th></tr>
<tr><td>4</td><td>リクエスト</td><td>クエリパラメータ</td><td colspan="3">なし</td></tr>
<tr><td>5</td><td></td><td>Content-Type</td><td colspan="3">application/json</td></tr>
<tr><td>6</td><td></td><td>ボディパラメータ</td><td colspan="3">・例
{
"time_from": "2021-01-11T10:00:00+09:00",
"time_to": "2021-01-11T12:00:00+09:00",
"time_interval":"5m",
"search_filters":{
"packet_field" : [
[{"src_vlan":4000 }, {"src_vlan":3000}]
]
}
}

・パラメータ説明（*必須パラメータ）
<table>
<tr><th>パラメータ名</th><th>型</th><th>説明</th></tr>
<tr><td>time_from *</td><td>String</td><td>検索時刻 - 始まり。
ISO8601 フォーマット。（例）2021-01-11T10:00:00+09:00</td></tr>
<tr><td>time_to *</td><td>String</td><td>検索時刻 - 終わり。
ISO8601 フォーマット。（例）2021-01-11T12:00:00+09:00</td></tr>
<tr><td>time_interval *</td><td>String</td><td>取得間隔。
1s, 10s, 30s, 1m, 5m, 10m, 15m, 30m, 1h, 3h, 6h, 12h, 1d</td></tr>
<tr><td>search_filters</td><td>Object</td><td>検索フィルタ条件</td></tr>
<tr><td>　sensor_addr</td><td>String</td><td>センサ IPv4 アドレス（ネットフローパケット送信元 IP アドレス）</td></tr>
<tr><td>　monitor_port_ifindex</td><td>Integer</td><td>センサモニタポート SNMP ifIndex</td></tr>
<tr><td>　output_port_ifindex</td><td>Integer</td><td>送信ポート SNMPifIndex</td></tr>
<tr><td>　mac_kind</td><td>String</td><td>MAC アドレス種別（ユニキャスト，マルチキャスト，ブロードキャスト）
unicast,
broadcast,
multicast,
unicast_broadcast,
unicast_multicast,
broadcast_multicast,
all</td></tr>
<tr><td>　packet_field</td><td>List</td><td>パケットフィールドフィルタ。AND 条件リスト。最大指定数：10 リスト。</td></tr>
</table></td></tr>
</table>

#	項目	説明					
						List	OR 条件リスト。最大指定数："packet_field"（パケットフィールドフィルタ）の総計で 100 リスト。
					@exclude	Boolean	除外条件。未指定時は False。
					flowset_id	Integer	フローセット ID
					sensor_addr	String	センサ IPv4 アドレス（ネットフローパケット送信元 IP アドレス）
					monitor_port_ifindex	Integer	センサモニタポート SNMP ifIndex
					output_port_ifindex	Integer	送信ポート SNMPifIndex
					ether_type	Integer	イーサタイプ値
					src_vlan	Integer	VLAN-ID 値（QinQ の場合，S-TAG）
					dst_vlan	Integer	VLAN-ID 値（QinQ の C-TAG）
					in_src_mac	String	送信元 MAC アドレス値。（例）00:00:5e:00:53:01
					in_dst_mac	String	宛先 MAC アドレス値。（例）00:00:5e:00:53:01
					ext01	String	フロー拡張データ 01
					ext02	String	フロー拡張データ 02
					ext03	String	フロー拡張データ 03
					ext04	String	フロー拡張データ 04
					ext05	String	フロー拡張データ 05
					ext06	String	フロー拡張データ 06
					ext07	String	フロー拡張データ 07
					ext08	String	フロー拡張データ 08
					ext09	String	フロー拡張データ 09
					ext10	String	フロー拡張データ 10
				aggregate_option		Object	集計オプション
					bytes	Boolean	バイト数
7	レスポンス	レスポンスステータス	以下のステータスコードを応答します。				

コード	内容
200	成功
400	要求不正エラー
401	認証エラー
403	アクセス禁止
408	タイムアウト
500	内部エラー
503	サービス利用不可

8		Content-Type	application/json

<table>
<tr><th>#</th><th>項目</th><th>説明</th><th></th></tr>
<tr><td>9</td><td></td><td>レスポンス
ボディ：

ステータスコード=200 の場合</td><td>・例
[
{
"datetime": "2021-01-11T10:00:00+09:00",
"packets_counts": 37884564
},
： ～省略～
{
"datetime": "2021-01-11T11:55:00+09:00",
"packets_counts": 33339574
}
]

・パラメータ説明
<table><tr><th>パラメータ名</th><th>型</th><th>説明</th></tr><tr><td></td><td>List</td><td>応答リスト。</td></tr><tr><td>datetime</td><td>String</td><td>対象時刻。</td></tr><tr><td>packets_counts</td><td>Integer64</td><td>集計パケット数</td></tr><tr><td>bytes_counts</td><td>Integer64</td><td>集計バイト数</td></tr></table></td></tr>
<tr><td>10</td><td></td><td>レスポンス
ボディ：

ステータスコード=200 以外の場合</td><td>・例
{
"detail": "ユーザ名かパスワードが違います。"
}
・パラメータ説明
<table><tr><th>パラメータ名</th><th>型</th><th>説明</th></tr><tr><td>detail</td><td>String</td><td>エラー詳細を格納します。</td></tr></table></td></tr>
</table>

8. トラブルシューティング

この章では，発生する問題への対処方法について説明します。

8.1 トラブル発生時の対応

AX-Collector の運用中に発生するトラブルへの対処方法を解説します。

表 8-1 現象と対応

項番	現象	原因	対応
1	ユーザ名やパスワードを忘れてログインできない。	-	ユーティリティコマンドを使用して，新しいユーザを AX-Collector に追加してください。ユーティリティコマンドの詳細は「4.11.1 ユーティリティコマンド」を参照してください。
2	AX-Sensor からのフローや監視データ等が表示されない。	周辺ネットワーク機器やファイヤウォール等の設定ミス。 AX-Sensor と AX-Collector との設定不一致。	AX-Sensor と AX-Collector 間で通信が可能かを確認してください。 また，AX-Collector のインストール時に指定したフロー受信ポート番号と AX-Sensor のコンフィグレーションが一致しているか，ファイヤウォールの設定が正しいかを確認してください。
3		データベース上のデータ破損。	コレクタをインストールしたサーバ上で以下のコマンドを実行して，インデックスの状態が green であることを確認してください。 curl -X GET http://localhost:9200/_cat/indices 状態が red のインデックスがある場合は，コレクタをインストールしたサーバ上で以下のコマンドを実行して，該当のインデックスを削除してください。（※. 削除したインデックス上のデータは参照出来なくなります。） curl -X DELETE http://localhost:9200/<インデックス名> インデックスの削除後，コレクタを再起動してください。

項番	現象	原因	対応
4		データベースのストレージ容量不足。	メニューから「管理・設定」⇒「管理」⇒「データ管理」を選択し，空きディスクサイズを確認してください。 AX-Collector のインストール時に指定した収集／監視情報格納ディレクトリのストレージ空き容量が 5%を下回っている場合，システム保全のためデータの書き込みを停止した状態です。不要な Index や，該当ディレクトリのファイルを削除し，空き容量を増やしてください。
5	AX-Collector の画面が正常に表示されない。	バージョンアップを行った場合，ブラウザにバージョンアップ前のキャッシュが残っていることがあります。	ブラウザの来歴や一時ファイルを削除した上で，再度アクセスしてください。
6		ブラウザの戻るボタンや右クリックからの操作など，メニューやボタン押下以外の操作で画面表示した場合，画面が正常に表示されないことがあります。	メニューから画面を表示し直してください。
7	個別 VIEW，SNMP/フロー監視のグラフ表示画面で，CSV ダウンロードボタン押下によるファイルが保存できない。または，保存されたファイル名が，「個別 VIEW 名称」，「SNMP/フロー監視項目名称」より短い。	ファイル「個別 VIEW 名称.csv」，または「SNMP/フロー監視項目名称.csv」の保存先ディレクトリ含めた文字数が，クライアント OS のサポートしているものより長いことが原因です。	クライアント OS およびブラウザの仕様となるため，必要な対応はありません。 なお，「個別 VIEW 名称」，または「SNMP/フロー監視項目名称」を短く設定することで回避可能です。
8	サーバの時刻を変更後，AX-Sensor からのフローが表示されない，または SNMP 監視データが生成されない。	サーバの時刻を変更した場合，フローの受信や SNMP 監視が動作しなくなる場合があります。	時刻を変更した場合は，データ管理画面にて，時刻変更日を含む以降の日付のインデックス名称を削除してください。 その後，コレクタを再起動してください。 また，センサ等周辺機器と時刻が一致していることを確認してください。

項番	現象	原因	対応
9	ダッシュボードやデータ監視設定において，カンマ「,」を含む名前を登録できない。	Ver.1.7 より，カンマ「,」を含む名前は登録できません。	カンマ「,」を含まない名前を設定してください。 なお，Ver.1.7 より前の Ver.で設定したカンマ含む名前の設定は Ver.1.7 以降でも動作可能ですが，設定変更する場合はカンマを含まない名前に変更する必要があります。
10	データ監視設定において，コロン「:」を含む名前を登録できない。	Ver.1.11 より，コロン「:」を含む名前は登録できません。	コロン「:」を含まない名前を設定してください。 なお，Ver.1.11 より前の Ver.で設定したコロン含む名前の設定は Ver.1.11 以降でも動作可能ですが，設定変更する場合はコロンを含まない名前に変更する必要があります。
11	AX-Collector の画面で，「OK/キャンセル」を選択する確認メッセージが表示されない。	確認メッセージと共に表示された「確認ダイアログを繰り返し表示しない」オプション設定が有効となっている可能性があります。	一度，ブラウザを終了，または確認メッセージが表示されない画面のタブを閉じてください。新しいウィンドウで画面の表示を行うことで，確認メッセージは表示されます。
12	AX-Collector の画面で，記号文字が検索できない。	「2.4.1 使用文字について」に記載している記号文字を検索している可能性があります。	検索対象の記号文字を設定している場合，該当文字を使わないよう設定変更してください。

付録

謝辞（Acknowledgments）

本製品で導入しているオープンソースソフトウェアは，下記になります。

（1） Bootstrap

The MIT License (MIT)

Copyright (c) 2011-2022 Twitter, Inc.
Copyright (c) 2011-2022 The Bootstrap Authors

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

（2） bootstrap-duallistbox

Bootstrap Dual Listbox

Responsive dual multiple select with filtering. Designed to work on small touch devices.

https://github.com/istvan-meszaros/bootstrap-duallistbox
http://www.virtuosoft.eu/code/bootstrap-duallistbox/

Copyright 2013-2014 István Ujj-Mészáros

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

（3） bootstrap-waitingfor

The MIT License (MIT)

Copyright (c) 2014 Eugene Maslovich

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all
copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE
SOFTWARE.

(4) D3

Copyright 2010-2017 Mike Bostock
All rights reserved.

Redistribution and use in source and binary forms, with or without modification,
are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this
  list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice,
  this list of conditions and the following disclaimer in the documentation
  and/or other materials provided with the distribution.

* Neither the name of the author nor the names of contributors may be used to
  endorse or promote products derived from this software without specific prior
  written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE
DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR
ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES
(INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON
ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS
SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

(5) dataTables

MIT license

Copyright (C) 2008-2023, SpryMedia Ltd.

Permission is hereby granted, free of charge, to any person obtaining a copy of this
software and associated documentation files (the "Software"), to deal in the

Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

(6) Django

Copyright (c) Django Software Foundation and individual contributors.
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of Django nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

(7) Font Awesome

Font Awesome Free License

Font Awesome Free is free, open source, and GPL friendly. You can use it for commercial projects, open source projects, or really almost whatever you want.
Full Font Awesome Free license: https://fontawesome.com/license/free.

Icons: CC BY 4.0 License (https://creativecommons.org/licenses/by/4.0/)
In the Font Awesome Free download, the CC BY 4.0 license applies to all icons packaged as SVG and JS file types.

Fonts: SIL OFL 1.1 License (https://scripts.sil.org/OFL)
In the Font Awesome Free download, the SIL OLF license applies to all icons packaged as web and desktop font files.

Code: MIT License (https://opensource.org/licenses/MIT)
In the Font Awesome Free download, the MIT license applies to all non-font and non-icon files.

Attribution
Attribution is required by MIT, SIL OLF, and CC BY licenses. Downloaded Font Awesome Free files already contain embedded comments with sufficient attribution, so you shouldn't need to do anything additional when using these files normally.

We've kept attribution comments terse, so we ask that you do not actively work to remove them from files, especially code. They're a great way for folks to learn about Font Awesome.

Brand Icons
All brand icons are trademarks of their respective owners. The use of these trademarks does not indicate endorsement of the trademark holder by Font Awesome, nor vice versa. **Please do not use brand logos for any purpose except to represent the company, product, or service to which they refer.**

(8) gridstack.js

The MIT License (MIT)

Copyright (c) 2014-2017 Pavel Reznikov, Dylan Weiss

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

(9) jQuery

Copyright JS Foundation and other contributors, https://js.foundation/

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish,

distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE
LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION
WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

（10） jQueryUI

Copyright jQuery Foundation and other contributors, https://jquery.org/

This software consists of voluntary contributions made by many
individuals. For exact contribution history, see the revision history
available at https://github.com/jquery/jquery-ui

The following license applies to all parts of this software except as
documented below:

====

Permission is hereby granted, free of charge, to any person obtaining
a copy of this software and associated documentation files (the
"Software"), to deal in the Software without restriction, including
without limitation the rights to use, copy, modify, merge, publish,
distribute, sublicense, and/or sell copies of the Software, and to
permit persons to whom the Software is furnished to do so, subject to
the following conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF
MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE
LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION
OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION
WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

====

Copyright and related rights for sample code are waived via CC0. Sample
code is defined as all source code contained within the demos directory.

CC0: http://creativecommons.org/publicdomain/zero/1.0/

====

All files located in the node_modules and external directories are

externally maintained libraries used by this software which have their own licenses; we recommend you read them, as their terms may differ from the terms above.

（11） lodash

The MIT License

Copyright JS Foundation and other contributors <https://js.foundation/>

Based on Underscore.js, copyright Jeremy Ashkenas,
DocumentCloud and Investigative Reporters & Editors <http://underscorejs.org/>

This software consists of voluntary contributions made by many individuals. For exact contribution history, see the revision history available at https://github.com/lodash/lodash

The following license applies to all parts of this software except as documented below:

====

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

====

Copyright and related rights for sample code are waived via CC0. Sample code is defined as all source code displayed within the prose of the documentation.

CC0: http://creativecommons.org/publicdomain/zero/1.0/

====

Files located in the node_modules and vendor directories are externally maintained libraries used by this software which have their own licenses; we recommend you read them, as their terms may differ from the terms above.

（12） moment-with-locales.js

Copyright (c) JS Foundation and other contributors

Permission is hereby granted, free of charge, to any person
obtaining a copy of this software and associated documentation
files (the "Software"), to deal in the Software without
restriction, including without limitation the rights to use,
copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the
Software is furnished to do so, subject to the following
conditions:

The above copyright notice and this permission notice shall be
included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND,
EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES
OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND
NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY,
WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING
FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR
OTHER DEALINGS IN THE SOFTWARE.

（13） plotly

The MIT License (MIT)

Copyright (c) 2021 Plotly, Inc

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.

（14） popper.js

The MIT License (MIT)

Copyright © 2016 Federico Zivolo and contributors

Permission is hereby granted, free of charge, to any person obtaining a copy of this
software and associated documentation files (the “Software”), to deal in the
Software without restriction, including without limitation the rights to use, copy,

modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

（15） tempusdominus-bootstrap-4

MIT License

Copyright (c) 2016 Tempus Dominus

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

（16） Video.js

Copyright Brightcove, Inc.

Licensed under the Apache License, Version 2.0 (the "License");
you may not use this file except in compliance with the License.
You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.

（17） w2ui

MIT License

Copyright (C) 2014 (vitmalina@gmail.com)

Permission is hereby granted, free of charge, to any person obtaining a copy
of this software and associated documentation files (the "Software"), to deal
in the Software without restriction, including without limitation the rights
to use, copy, modify, merge, publish, distribute, sublicense, and/or sell
copies of the Software, and to permit persons to whom the Software is
furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in
all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR
IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,
FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,
OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN
THE SOFTWARE.

（18） tabulator.js

The MIT License (MIT)

Copyright (c) 2015-2024 Oli Folkerd

Permission is hereby granted, free of charge, to any person obtaining a copy of this
software and associated documentation files (the "Software"), to deal in the
Software without restriction, including without limitation the rights to use, copy,
modify, merge, publish, distribute, sublicense, and/or sell copies of the Software,
and to permit persons to whom the Software is furnished to do so, subject to the
following conditions:

The above copyright notice and this permission notice shall be included in all
copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED,
INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A
PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT
HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF
CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE
OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

（19） IPAex フォント

IPA フォントライセンス V1.0
許諾者は，この使用許諾（以下「本契約」といいます。）に定める条件の下で，許諾プログラム（1 条に定義するところによります。）を提供します。受領者（1 条に定義するところによります。）が，許諾プログラムを使用し，複製し，または頒布する行為，その他，本契約に定める権利の利用を行った場合，受領者は本契約に同意したものと見なします。

第 1 条　用語の定義
本契約において，次の各号に掲げる用語は，当該各号に定めるところによります。

1．「デジタル･フォント･プログラム」とは，フォントを含み，レンダリングしまたは表示するために用いられるコンピュータ・プログラムをいいます。

２．「許諾プログラム」とは，許諾者が本契約の下で許諾するデジタル･フォント･プログラムをいいます。
３．「派生プログラム」とは，許諾プログラムの一部または全部を，改変し，加除修正等し，入れ替え，その他翻案したデジタル･フォント･プログラムをいい，許諾プログラムの一部もしくは全部から文字情報を取り出し，またはデジタル･ドキュメント･ファイルからエンベッドされたフォントを取り出し，取り出された文字情報をそのまま，または改変をなして新たなデジタル・フォント・プログラムとして製作されたものを含みます。
４．「デジタル・コンテンツ」とは，デジタル・データ形式によってエンド・ユーザに提供される制作物のことをいい，動画・静止画等の映像コンテンツおよびテレビ番組等の放送コンテンツ，ならびに文字テキスト，画像，図形等を含んで構成された制作物を含みます。
５．「デジタル・ドキュメント・ファイル」とは，PDF ファイルその他，各種ソフトウェア･プログラムによって製作されたデジタル・コンテンツであって，その中にフォントを表示するために許諾プログラムの全部または一部が埋め込まれた（エンベッドされた）ものをいいます。フォントが「エンベッドされた」とは，当該フォントが埋め込まれた特定の「デジタル・ドキュメント・ファイル」においてのみ表示されるために使用されている状態を指し，その特定の「デジタル・ドキュメント・ファイル」以外でフォントを表示するために使用できるデジタル・フォント・プログラムに含まれている場合と区別されます。
６．「コンピュータ」とは，本契約においては，サーバを含みます。
７．「複製その他の利用」とは，複製，譲渡，頒布，貸与，公衆送信，上映，展示，翻案その他の利用をいいます。
８．「受領者」とは，許諾プログラムを本契約の下で受領した人をいい，受領者から許諾プログラムを受領した人を含みます。

第２条 使用許諾の付与
許諾者は受領者に対し，本契約の条項に従い，すべての国で，許諾プログラムを使用することを許諾します。ただし，許諾プログラムに存在する一切の権利はすべて許諾者が保有しています。本契約は，本契約で明示的に定められている場合を除き，いかなる意味においても，許諾者が保有する許諾プログラムに関する一切の権利および，いかなる商標，商号，もしくはサービス・マークに関する権利をも受領者に移転するものではありません。

１．受領者は本契約に定める条件に従い，許諾プログラムを任意の数のコンピュータにインストールし，当該コンピュータで使用することができます。
２．受領者はコンピュータにインストールされた許諾プログラムをそのまま，または改変を行ったうえで，印刷物およびデジタル・コンテンツにおいて，文字テキスト表現等として使用することができます。
３．受領者は前項の定めに従い作成した印刷物およびデジタル・コンテンツにつき，その商用・非商用の別，および放送，通信，各種記録メディアなどの媒体の形式を問わず，複製その他の利用をすることができます。
４．受領者がデジタル・ドキュメント・ファイルからエンベッドされたフォントを取り出して派生プログラムを作成した場合には，かかる派生プログラムは本契約に定める条件に従う必要があります。
５．許諾プログラムのエンベッドされたフォントがデジタル・ドキュメント・ファイル内のデジタル・コンテンツをレンダリングするためにのみ使用される場合において，受領者が当該デジタル・ドキュメント・ファイルを複製その他の利用をする場合には，受領者はかかる行為に関しては本契約の下ではいかなる義務をも負いません。
６．受領者は，3 条 2 項の定めに従い，商用・非商用を問わず，許諾プログラムをそのままの状態で改変することなく複製して第三者への譲渡し，公衆送信し，その他の方法で再配布することができます（以下，「再配布」といいます。）。
７．受領者は，上記の許諾プログラムについて定められた条件と同様の条件に従って，派生プログラムを作成し，使用し，複製し，再配布することができます。ただし，受領者が派生プログラムを再配布する場合には，3 条 1 項の定めに従うものとします。

第３条　制限
前条により付与された使用許諾は，以下の制限に服します。

１．派生プログラムが前条 4 項及び 7 項に基づき再配布される場合には，以下の全ての条件を満たさなければなりません。

(1) 派生プログラムを再配布する際には，下記もまた，当該派生プログラムと一緒に再配布され，オンラインで提供され，または，郵送費・媒体及び取扱手数料の合計を超えない実費と引き換えに媒体を郵送する方法により提供されなければなりません。
(a) 派生プログラムの写し；および
(b) 派生プログラムを作成する過程でフォント開発プログラムによって作成された追加のファイルであって派生プログラムをさらに加工するにあたって利用できるファイルが存在すれば，当該ファイル
(2) 派生プログラムの受領者が，派生プログラムを，このライセンスの下で最初にリリースされた許諾プログラム（以下，「オリジナル・プログラム」といいます。）に置き換えることができる方法を再配布するものとします。かかる方法は，オリジナル・ファイルからの差分ファイルの提供，または，派生プログラムをオリジナル・プログラムに置き換える方法を示す指示の提供などが考えられます。
(3) 派生プログラムを，本契約書に定められた条件の下でライセンスしなければなりません。
(4) 派生プログラムのプログラム名，フォント名またはファイル名として，許諾プログラムが用いているのと同一の名称，またはこれを含む名称を使用してはなりません。
(5) 本項の要件を満たすためにオンラインで提供し，または媒体を郵送する方法で提供されるものは，その提供を希望するいかなる者によっても提供が可能です。
２．受領者が前条 6 項に基づき許諾プログラムを再配布する場合には，以下の全ての条件を満たさなければなりません。
(1) 許諾プログラムの名称を変更してはなりません。
(2) 許諾プログラムに加工その他の改変を加えてはなりません。
(3) 本契約の写しを許諾プログラムに添付しなければなりません。
３．許諾プログラムは，現状有姿で提供されており，許諾プログラムまたは派生プログラムについて，許諾者は一切の明示または黙示の保証（権利の所在，非侵害，商品性，特定目的への適合性を含むがこれに限られません）を行いません。いかなる場合にも，その原因を問わず，契約上の責任か厳格責任か過失その他の不法行為責任かにかかわらず，また事前に通知されたか否かにかかわらず，許諾者は，許諾プログラムまたは派生プログラムのインストール，使用，複製その他の利用または本契約上の権利の行使によって生じた一切の損害（直接・間接・付随的・特別・拡大・懲罰的または結果的損害）（商品またはサービスの代替品の調達，システム障害から生じた損害，現存するデータまたはプログラムの紛失または破損，逸失利益を含むがこれに限られません）について責任を負いません。
４．許諾プログラムまたは派生プログラムのインストール，使用，複製その他の利用に関して，許諾者は技術的な質問や問い合わせ等に対する対応その他，いかなるユーザ・サポートをも行う義務を負いません。

第４条　契約の終了
１．本契約の有効期間は，受領者が許諾プログラムを受領した時に開始し，受領者が許諾プログラムを何らかの方法で保持する限り続くものとします。
２．前項の定めにかかわらず，受領者が本契約に定める各条項に違反したときは，本契約は，何らの催告を要することなく，自動的に終了し，当該受領者はそれ以後，許諾プログラムおよび派生プログラムを一切使用しまたは複製その他の利用をすることができないものとします。ただし，かかる契約の終了は，当該違反した受領者から許諾プログラムまたは派生プログラムの配布を受けた受領者の権利に影響を及ぼすものではありません。

第５条　準拠法
１．IPA は，本契約の変更バージョンまたは新しいバージョンを公表することができます。その場合には，受領者は，許諾プログラムまたは派生プログラムの使用，複製その他の利用または再配布にあたり，本契約または変更後の契約のいずれかを選択することができます。その他，上記に記載されていない条項に関しては日本の著作権法および関連法規に従うものとします。
２．本契約は，日本法に基づき解釈されます。

（20）　telegraf

The MIT License (MIT)
Copyright (c) 2015-2025 InfluxData Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

(21) geoip2-golang

ISC License

Copyright (c) 2015, Gregory J. Oschwald <oschwald@gmail.com>

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

(22) maxminddb-golang

ISC License

Copyright (c) 2015, Gregory J. Oschwald <oschwald@gmail.com>

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.