

URL Monitoring

release date. 2026. 09. 11.

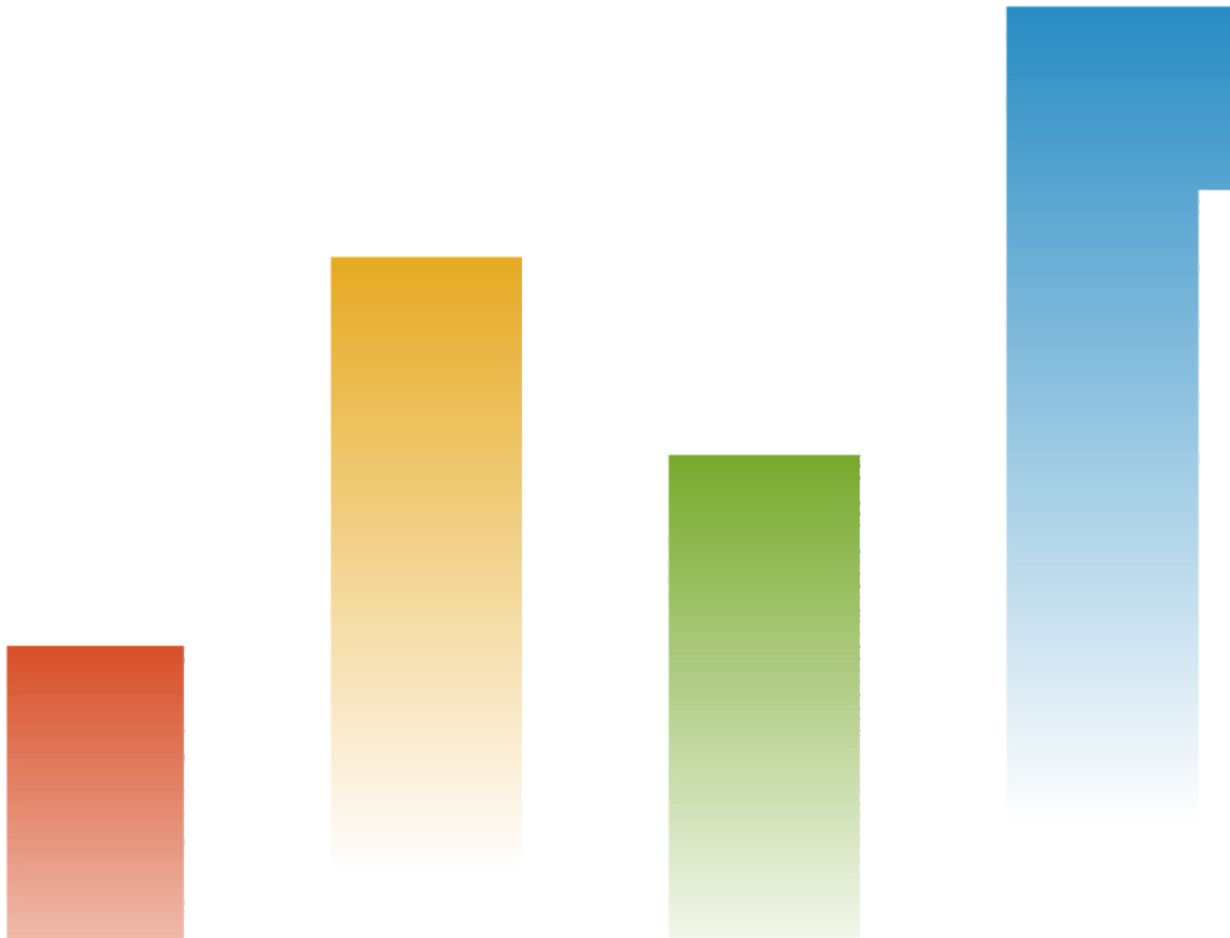


Table of Contents

• URLモニタリング	3
◦ はじめに	5
◦ URL一覧	8
◦ アラート通知	13
▪ イベント設定	0
▪ 通知設定	15
▪ イベント通知フォーマット	37
▪ イベント履歴	45
▪ リアルタイムアラート	53
▪ システムイベント	56
◦ HTTPステータスのコードタイプ	58
◦ エラータイプ	66

URLモニタリング

WhaTapのURLモニタリングは、ウェブサイトやサービスが正常に開くかどうかを定期的に確認するサービスです。

モニタリングするアドレス(URL)と確認周期を設定すると、WhaTapが該当アドレスに自動的に接続して、ウェブサイトが正しく開くかどうかを確認します。ウェブサイトが開かない、レスポンスが遅くなるなどの問題が発生した場合は通知を受け取れるため、障害状況を素早く把握して対応できます。



主な機能

- グローバルサービス向けのURLチェック

北米、ヨーロッパ、アジア、韓国等のサービス拠点を選択してモニタリングを行うことができます。

- フリーサービス

WhaTapのURLモニタリングサービスのすべての機能を無制限に無料で提供します。

- **サイトアベイラビリティチェック**

エンドユーザーのサイト接続の異常有無をHTTPステータスコードを通じてリアルタイムで確認します。

- **サイト性能モニタリング**

北米、ヨーロッパ、アジア、韓国等に位置するサーバーから、サイトにアクセスするまでにかかる時間を確認します。

- **URL毎のアラート設定**

Email、モバイルプッシュ、サードパーティープラグインを使用したアラート通知が設定できます。

❗ URLモニタリングサービスは、SMS通知を提供していません。

- **WhaTap サービス統合ダッシュボードの構成**

サーバー、アプリケーション、データベースなど、WhaTapの他のサービスとともにダッシュボードを構成できます。

はじめに

WhaTapモニタリングサービスを使用するには、[会員登録](#)後にプロジェクトを作成して、対応するURLを追加する必要があります。会員登録に関する詳細については、[次の文書](#)を参照してください。

プロジェクト生成

URLを追加する前に、まずプロジェクトを作成してください。

1. [WhaTapモニタリングサービス](#)に移動し、ログインします。
2. プロジェクトを作成するには、画面左のサイドメニューから**プロジェクト全体** > **+ Project**ボタンをクリックします。
3. **商品選択画面**で **URL** [作成する >] ボタンをクリックしてください。

❗ URLモニタリング製品を選択すると、プロジェクト作成画面で3ステップのオンボーディングが始まります。画面上部の進行バーとステップ表示で現在の位置を確認できます。各ステップで必須項目を入力すると **続行** ボタンが有効になり、**戻る** ボタンで前のステップに戻ることができます。最初のステップで **戻る** ボタンをクリックすると、製品選択画面に移動します。

4. **プロジェクト名を決めてください** ステップで **プロジェクト名** フィールドに名前を入力し、**続行** ボタンをクリックしてください。名前は必須項目です。
5. **プロジェクト設定** ステップで **プロジェクトタイムゾーン**、**通知言語の設定**、**プロジェクトグループ**、**プロジェクト説明** の項目を設定した後、**続行** ボタンをクリックしてください。

項目	必須の有無	説明
プロジェクトタイムゾーン	必須	通知とレポートを生成する基準時間 - 既定値: (GMT +9:00) Seoul, Tokyo, Yakutsk - 選択できるタイムゾーンは 次のリスト を参照してください。
通知言	必須	通知を送信する言語で、韓国語または英語を選択

項目	必須の有無	説明
語の設定		
プロジェクトグループ	組織アカウントは必須、その他は任意	複数のプロジェクトをまとめるグループ - プロジェクトが属するグループを選択してください。 - 選択するグループがない場合は、 グループ追加 ボタンをクリックして、先にグループを作成してください。入力した値はそのまま保持されますが、グループ作成画面から戻ると、最初のステップから再開されます。
プロジェクト説明	任意	プロジェクトを説明する内容を入力します。

① 選択できるタイムゾーン

- ①
- (GMT -12:00) Eniwetok, Kwajalein
 - (GMT -11:00) Midway Island, Samoa
 - (GMT -10:00) Hawaii
 - (GMT -9:00) Alaska
 - (GMT -8:00) Pacific Time (US & Canada)
 - (GMT -7:00) Mountain Time (US & Canada)
 - (GMT -6:00) Central Time (US & Canada), Mexico City
 - (GMT -5:00) Eastern Time (US & Canada), Bogota, Lima
 - (GMT -4:00) Atlantic Time (Canada), Caracas, La Paz
 - (GMT -3:00) Brazil, Buenos Aires, Georgetown
 - (GMT -2:00) Mid-Atlantic
 - (GMT -1:00) Azores, Cape Verde Islands
 - (GMT) Western Europe Time, London, Lisbon, Casablanca
 - (GMT +1:00) Brussels, Copenhagen, Madrid, Paris



- (GMT +2:00) Kaliningrad, South Africa
- (GMT +3:00) Baghdad, Riyadh, Moscow, St. Petersburg
- (GMT +4:00) Abu Dhabi, Muscat, Baku, Tbilisi
- (GMT +5:00) Ekaterinburg, Islamabad, Karachi, Tashkent
- (GMT +6:00) Almaty, Dhaka, Colombo
- (GMT +7:00) Bangkok, Hanoi, Jakarta
- (GMT +8:00) Beijing, Perth, Singapore, Hong Kong
- (GMT +9:00) Seoul, Tokyo, Yakutsk
- (GMT +10:00) Eastern Australia, Guam, Vladivostok
- (GMT +11:00) Magadan, Solomon Islands, New Caledonia
- (GMT +12:00) Auckland, Wellington, Fiji, Kamchatka

6. **チェック位置** ステップで使用するリージョンのボタンをクリックし、有効になった **プロジェクト作成** ボタンをクリックしてください。

- **チェック位置** ステップで選択する確認リージョンは、プロジェクトデータを保存するデータセンターの位置を意味します。

7. **プロジェクトリスト** でURL製品の新しいプロジェクトを確認できます。

❗ 複数のプロジェクトをグループでまとめて管理する **プロジェクトグループ** の詳細については、[次の文書](#)を参照してください。

✔ URLプロジェクトは最大10個まで作成できます。

URL一覧

URLリストでは、プロジェクトに登録されたURLの最新のチェック結果をリアルタイムで確認し、URLを追加または編集できます。

基本オプション

- 検索および整列

画面左上の検索入力ウィンドウから、URLまたはURL名を基準に一覧を検索できます。隣の整列ボタンをクリックすると、名前、ステータス、エージェント位置名を基準に一覧を整列できます。既定の設定は名前です。

- リアルタイムモード

画面右上の LIVE インジケーターで最後の更新時刻を確認できます。一時停止ボタンをクリックするとリアルタイムモードを停止し、更新ボタンをクリックすると最新データをすぐに参照します。

- プロジェクト要約カード

一覧の上部にある要約カードで、現在表示しているプロジェクトの名前と登録されたURLの数を確認できます。件数バッジはプロジェクトに登録された全URLを基準とするため、検索語や状態フィルターを適用しても値は減りません。まだチェック履歴がない場合は、データ収集の待機状態を知らせるメッセージが表示されます。

- 状態フィルター

要約カードの下部で、最終レスポンス状態ごとの件数を確認し、一覧をフィルタリングできます。全体を見る、成功、リダイレクト、クライアントエラー、サーバーエラー、不明などを基準に参照できます。既定の設定は全体を見るです。

- ☒ インポート / ☒ エクスポート

☒ インポート ボタンをクリックすると、ExcelファイルからURL一覧を読み込みます。☒ 抽出 ボタンをクリックすると、現在のURL一覧をExcelファイルとしてダウンロードします。

URL一覧を確認する

登録されたURL単位でモニタリングチェック結果を確認できます。各カラム項目は次のとおりです。

カラム	説明
現在ステータスコード	最終チェックレスポンスコード(HTTP Status Code)で、ステータスコードをクリックするとHTTPステータスコードの文書に移動します。
名前/ URL	URL登録時に入力した名前とチェック対象のURL
地域	URL登録時に選択した確認リージョン
経過時間	直近20分間のチェック結果(レスポンスコードおよびレスポンス時間)と最終レスポンス時間で、チャート領域をドラッグすると、その時間帯のレスポンスコードとレスポンス時間を参照できます。
	登録したURLの設定を変更するには、行の右側にある  アイコンをクリックすると URL編集 に移動します。
	既存のURLと同じ設定で新しいURLを登録するには、  アイコンをクリックすると URLコピー に移動します。確認リージョン、収集周期、イベント設定などの既存の値はそのまま保持され、名前とURLは重複して使用できないため、変更して保存します。
	登録したURLを削除するには、  アイコンをクリックした後、確認ポップアップウィンドウで 削除 ボタンをクリックします。

 URLを削除すると、そのURLで収集したデータはすべて削除され、復旧できません。

URLを追加および修正する

- 画面右上の **+ URL追加** ボタンをクリックしてください。画面の右側に **URL追加** パネルが開きます。
 - パネル右上の拡張アイコンをクリックすると、パネルを広く表示できます。
 - 追加を取り消すには、左上の閉じる(X)アイコンをクリックしてください。
 - ガイドへ** リンクをクリックすると、URL設定ガイドの文書に移動します。
- 基本情報を入力してください。アスタリスク(*)で表示された項目は必須項目です。

項目	必須の有無	説明
名前	必須	URL設定の固有の識別情報として使用されます。重複して使用することはできません。リセット時に同じ名前で登録すると、同じ名前の統計データを同じURLのデータとみなします。
URL	必須	チェック対象URLの完全パスを入力します。http/httpsプロトコルに対応します。
チェック位置	必須	チェックを実行するWhaTapエージェントのリージョンを選択します。 提供リージョン: California、Frankfurt、Jakarta、Mumbai、Seoul、Singapore、Tokyo
リージョンIP	-	選択したリージョンのエージェントのIPアドレスが表示されます。URL検査のために該当IPアドレスへ接続を試みるため、ファイアウォールルールを確認し、必要な場合はアクセスを許可してください。詳細は 確認リージョン選択 を参照してください。
収集周期	必須	モニタリングデータを収集する間隔です。 - 既定値は 1分 (60000 ms)で、最大5分まで1分単位で選択できます。

3. **アラート設定** 領域でURLごとの通知条件を設定してください。条件ごとにトグルで使用の有無を指定します。

- **通知メッセージ** を最大50文字まで入力できます。入力したメッセージは通知内容と一緒に伝達されます。

項目	説明
ステータス	チェック結果のレスポンス状態を基準に通知を発生させます。トグルをオンにした後、通知対象の状態を選択してください。 - クライアントエラー、サーバーエラー、不明 のうち複数を選択できます。
経過	チェックレスポンス時間を基準に通知を発生させます。トグルをオンにした後、しきい値を秒単位で

項目	説明
時間	入力してください。入力値を超えるレスポンス時間が発生すると通知を送信します。 最小5秒以上を指定でき、+、- ボタンで値を調整できます。

4. 設定を完了したら、**保存** ボタンをクリックしてください。

- 追加/修正/コピーしたURLが一覧に反映されるまで約1分の時間がかかります。

❗ 登録したURLは **イベント設定** 画面の **Classic** 領域にも通知対象として表示されます。詳細は[次の文書](#)を参照してください。

確認リージョン選択

今後の接続テストのための追加のリージョン(リージョン)を提供することができます。その他のリージョンについてはsupport@whatap.ioまでお問い合わせください。

★ チェック位置

Seoul
Mumbai
Tokyo
Singapore
Frankfurt
California
Jakarta

▼ リージョンIP

Tokyo 18.179.189.142

* URLチェックのために指定したIP アドレスへ接続しようとしています。
ファイアウォールのルールを確認し、必要に応じて許可してください。

閉域網サイトへの接続テストを遂行しようとしている場合、エージェントからの呼び出しが許可されるようにファイアウォールをオープンする必要がある場合があります。**リージョンIP**を選択すると、位置IPアドレスが表示されます。各エージェントのファイアウォールのオープン対象IP Addressは、次のとおりです。

ソウルリージョンプロジェクト使用時のエージェントリージョン別IP

- AWS-Seoul-Agent - 54.180.11.176
- AWS-Mumbai-Agent - 3.6.243.66
- AWS-Tokyo-Agent - 18.179.189.142

- AWS-Singapore-Agent - 54.169.168.45
- AWS-Frankfurt-Agent - 18.197.22.141
- AWS-California-Agent - 54.215.76.203
- AWS-Jakarta-Agent - 16.78.204.227

東京リージョンプロジェクト使用時のエージェントリージョン別IP

- Seoul - 54.180.11.176
- Mumbai - 3.6.243.66
- Tokyo - 52.193.204.10
- Singapore - 18.140.134.146
- Frankfurt - 18.158.138.224
- California - 13.52.131.66
- Jakarta - 16.78.204.227

cloudflareを使用する場合、cloudflare ファイアウォールのルールに対応するリージョンIPを許可する必要があります。

ⓘ WhaTap URL Monitoringサービスの使用

URLモニタリングは、ポリシー変更されるまで無料のサービスとして提供されます。ユーザーは、別のエージェントをインストールする必要はなく、WhaTapが提供するエージェントおよびサーバーリポジトリを使用します。

警告アラート

監視対象のシステムまたはアプリケーションで問題が発生した際に、あらかじめ設定した条件に基づいてユーザーへ通知を送信する機能です。通知は、メール、SMS、メッセージャー、アプリのプッシュ通知など、さまざまなチャネルを通じて配信されます。

たとえば、CPU 使用率、メモリ使用量、ディスク I/O、ネットワークトラフィック、トランザクション数、エラー発生、レスポンスタイムの遅延などの主要なパフォーマンス指標にアラート基準を設定しておく、その基準を超過した場合や異常な兆候が検出された際に通知が送信されます。

WhaTap の AI ベースのアラート機能を使用すると、複雑な条件を手動で設定する必要はありません。AI がアプリケーションの正常な動作パターンを学習し、異常パターンを自動的に検知して通知します。また、タグカウントアラート機能を活用することで、特定のタグを基準に集計された値に条件を設定でき、複雑な状況でも高精度な検知が可能です。

主な機能

- ・ **イベント設定:** 閾値ベースのアラート条件および通知チャネルの設定
- ・ **通知設定:** ユーザーごとの通知チャネルおよび時間帯設定
- ・ **イベント履歴:** アラート発生履歴の確認

権限

イベントを追加または設定するには、**アラート設定権限** が必要です。

- ・ **閲覧:** メトリクスイベント設定を確認するには、**閲覧・分析権限** が必要です。
- ・ **追加／編集／削除:** 設定を変更するには、**アラート設定権限** が必要です。
- ・ **通知受信:** 通知を受信するには、**通知受信権限** が必要です。

📌 参考資料

詳細については、[メンバー権限](#) を参照してください。

イベント設定 (Classic)

ホーム画面 > プロジェクト選択 >  アラート通知 > イベント設定

URLモニタリングプロジェクトでURLを登録すると、アラート設定の **Classic** 領域に該当URLの項目が自動的に表示されます。別途イベントを追加しなくても、登録したURL単位で通知対象が作成され、各URLの通知条件はURLの追加/編集画面で設定します。

URL通知一覧

登録されたURLは一覧で表示され、画面上部の **通知検索** 入力ウィンドウから名前を基準に検索できます。各カラム項目は次のとおりです。

- **名前:** URL登録時に指定した固有の識別情報
- **URL:** チェック対象URLの完全パス
- **リージョン:** URL登録時に選択した確認リージョンと、該当リージョンのIPアドレス
- **状態:** レスポンスコードベースの通知の設定状態で、通知を設定していない場合は **非活性** と表示されます。
- **経過時間:** レスポンス時間ベースの通知の設定状態で、通知を設定していない場合は **非活性** と表示されます。
- : URLのイベント設定の修正に移動し、状態、通知メッセージ(最大50文字)、経過時間を修正できます。

通知条件の設定

URL一覧 メニューで [+ URL追加] ボタンをクリックしてイベントを設定できます。詳細は **はじめに** の文書を参照してください。

通知設定

ホーム > プロジェクト選択 >  アラート通知 > 通知設定

ユーザー別アラート受信設定

 **ユーザー別アラート受信設定** における他メンバーの情報は、**メンバー管理** 権限を持つメンバーのみが確認できます。それ以外のメンバーには、必須情報がマスキングされて表示されます。

- イベント通知の一括受信設定およびアクセス設定のためのモバイル端末管理は、**アカウント情報** で行うことができます。
- メンバー権限の詳細については、[こちらのドキュメント](#) を参照してください。

通知手段の設定

メール、**SMS**、**WhatsApp**、**モバイル** による通知を提供します。

ユーザー別アラート受信設定 セクションで、受信したい通知手段のチェックボックスを選択すると警告アラートを受信できます。通知手段のチェックボックスを解除すると、その手段ではアラートは送信されません。

 プロジェクトの最高管理者を除き、すべてのユーザーは自分自身の受信設定のみ変更できます。

メール通知

メール通知は、会員登録時に入力したメールアドレス宛に送信されます。

SMS通知

SMSで通知を受信できます。

 SMS通知機能は、有料プロジェクトでのみ利用できます。

1. 画面右上の **プロフィールアイコン** をクリックし、**アカウント管理** に移動します。
2. **アカウント情報** の **ユーザー電話番号** セクションで、[一般携帯電話] ボタンをクリックします。
3. 認証番号を受信する **電話番号** を入力します。
 - SMS通知を受信できる電話番号は、**韓国の携帯電話番号のみ**対応しています。
4. [保存] ボタンをクリックします。

✔ 登録した電話番号の変更および削除

- 電話番号を変更する場合は、[変更] ボタンをクリックしてください。SMS認証が必要です。
- 電話番号を削除する場合は、[削除] ボタンをクリックしてください。削除後は、SMSによる通知を受信できなくなります。

WhatsApp通知

WhatsAppを通じて通知を受信できます。

ⓘ WhatsApp通知機能は、有料プロジェクトでのみ利用できます。

1. 画面右上の **プロフィールアイコン** をクリックし、**アカウント管理** に移動します。
2. **アカウント情報** の **ユーザー電話番号** セクションで、[WhatsApp] ボタンをクリックします。
3. 認証番号を受信する **電話番号** を入力します。
4. [認証番号送信] ボタンをクリックします。
5. WhatsAppアプリケーションに送信された6桁の認証番号を入力します。
 - 10分以内に認証番号を受信できなかった場合は、[認証番号再送信] ボタンをクリックしてください。
6. [認証] ボタンをクリックします。

モバイル通知

モバイル通知を受信するには、モバイル端末にWhaTapアプリケーションをインストールし、ログインする必要があります。

- WhaTapアプリケーションをダウンロード – [Android](#)
- WhaTapアプリケーションをダウンロード – [iOS](#)

繰り返し通知（エスカレーション）設定

アラート発生後も状況が解消されない場合、初回アラート発生時刻を基準に通知を繰り返す間隔を設定できます。この設定は **Critical** レベルのアラートにのみ適用されます。

例えば、初回アラート発生から即時（0分）、1時間後、1日後に通知を繰り返す場合は、**繰り返し通知（エスカレーション）** カラムに **0,1H,1D** と入力します。

1. **アラート通知 > 通知設定** に移動し、**ユーザー別アラート受信設定** セクションを開きます。
2. **繰り返し通知（エスカレーション）** 項目で設定します。
 - **M**: 分、**H**: 時間、**D**: 日。単位を省略した場合は分単位として扱われます。
 - 数値、または 数値+単位（**M, H, D**）の形式で入力してください。入力形式が正しくない場合はメッセージが表示されます。
3. [保存] ボタンをクリックしてください。保存しない場合、設定は反映されません。

イベント受信タグ

イベント設定時に **イベント受信タグ** を選択すると、そのタグを持つプロジェクトメンバーや 3rd-party プラグインに通知を送信できます。イベント受信タグを設定しない場合、**すべてのプロジェクトメンバー** に警告アラートが送信されます。

イベント受信タグの追加・編集・削除

 イベントに **適用中のイベント受信タグ** は削除できません。

1. **アラート通知 > 通知設定** に移動します。
2. **ユーザー別アラート受信設定** セクションのユーザー一覧で、**+ タグ追加** または **+** をクリックします。
3. **イベント受信タグ** 画面で **+ 新しいタグ作成** をクリックします。
4. **タグ作成** 画面でタグ名を入力し、色を選択して [タグ作成] ボタンをクリックします。

5. 作成されたタグは、タグ一覧の  をクリックして編集または削除できます。
6. イベント受信タグ画面の **タグ一覧** から使用したいタグを選択すると適用されます。

イベント受信タグを解除する

1. アラート通知 > 通知設定 に移動し、**ユーザー別アラート受信設定** セクションを開きます。
2. イベント受信タグを解除したいユーザーの **イベント受信タグ** 項目にある + をクリックします。
3. イベント受信タグ画面で、解除したいタグの X をクリックすると、そのタグが解除されます。

受信タグ未設定のアラートを受信する

イベント設定時にイベント受信タグを選択すると、そのタグを持つプロジェクトメンバーや 3rd-party プラグインに通知を送信できます。

- イベント受信タグが設定されていないアラートを受信するには、**受信タグ未設定のアラートを受信** オプションを有効にしてください。
- イベント受信タグが設定されているアラートのみ受信したい場合は、このオプションを無効にしてください。

❗ すべての警告アラートを受信しない場合は、このオプションを無効にし、**イベント受信タグ** が一つも選択されていない状態にしてください。

イベント受信モードの選択

ユーザー別アラート受信設定 セクションで、メンバーまたはサードパーティチャネルごとにイベント通知の受信範囲を次の3つのモードから選択できます。受信モードは、各メンバーまたはチャネル行の**イベント受信タグ**列で選択します。

Mode	Description
すべての通知を受信	イベント受信タグに関係なく、すべての警告通知を受信
選択したタグのみ通知を受信	選択したイベント受信タグを持つ警告通知のみ受信。タグを最低1つ以上選択
すべての通知を受信しない	いかなるイベント通知も受信しない。選択したタグは削除されずそのまま保存

- 選択したタグのみ通知を受信モードでは、タグ選択領域で通知を受信するタグを1つ以上選択してください。
- イベント受信タグが指定されていない警告通知まで受信するには、タグ選択領域で未分類仮想タグを選択してください。未分類タグは通常のタグと同様に選択または解除でき、タグ自体を編集・削除することはできません。

❗ すべての通知を受信しないモードでは、該当メンバーまたはチャネルがイベント通知をまったく受信しません。このとき選択したタグは削除されず保存されるため、再び選択したタグのみ通知を受信モードに切り替えると、以前に選択したタグ設定をそのまま使用できます。

通知受信言語の選択

ユーザーが受信するアラート通知の言語を選択できます。

1. アラート通知 > 通知設定 に移動します。
2. ユーザー別アラート受信設定 セクションのユーザー一覧で、言語を設定したいユーザーの一番左にある ► ボタンをクリックします。
3. 通知受信言語 を選択します。

曜日・時間別通知設定

ユーザーごとに、曜日および時間帯別の通知受信可否を設定できます。

1. アラート通知 > 通知設定 に移動します。
2. ユーザー別アラート受信設定 セクションのユーザー一覧で、曜日・時間別通知を設定したいユーザーの一番左にある ► ボタンをクリックします。
3. 警告アラートを受信したい曜日を選択するか、時間帯を入力します。
 - 通知手段ごとに設定できます。

サードパーティプラグイン

外部アプリケーションを通じて警告アラートを受信できます。

- 対応アプリケーション: Slack、Telegram、Teams、Teams Workflows、Jandi、AlertNow、Webhook、Webhook

JSON、Opsgenie、PagerDuty、LINE、ilert

❗ WhaTap のサポート範囲に含まれない社内メッセンジャーは、標準の **Webhook** または **Webhook JSON** を使用して連携できます。

表 | サードパーティプラグイン一覧

項目	説明
プラグイン名	プラグインの名称
認証キー	認証キー
認証値	認証値
受信レベル	警告、全体、危険のいずれか
繰り返し通知（エスカレーション）	問題が解消されない場合、初回通知時刻から再通知する間隔 - Critical レベルのアラートにのみ適用
Smart メッセージ（AI）	Telegram プラグイン追加時に AI 通知機能を提供 - 対応言語：韓国語、英語、日本語
イベント受信タグ	プロジェクト内の特定メンバーまたはチームに対する通知受信設定
削除	サードパーティプラグインの削除

サードパーティプラグインの追加

1. アラート通知 > 通知設定 に移動します。
2. サードパーティプラグイン セクションで **追加** ボタンをクリックします。
3. サードパーティプラグイン追加 画面で、使用するサービスのタブを選択します。
4. 選択したサービスの案内（[サードパーティプラグイン通知の追加方法](#)）に従って設定します。
5. 受信テスト ボタンをクリックして設定を確認します。

6. すべて完了したら **追加** または **登録** ボタンをクリックします。

サードパーティプラグイン通知の追加方法

Slack

- ① サードパーティプラグイン追加 画面の **Slack** タブで、[**Slackに登録**] ボタンをクリックすると、Slack のチームおよびチャンネルに **WhaTapNotiBot** を登録できます。

Telegram

- ①
1. **Telegram**で **@WhaTapApmNotiBot** を検索してください。
 2. ボットを選択し、[**開始**] ボタンをクリックします。
 3. チャット画面に **/license** コマンドと、通知を受信したいプロジェクトのアクセスキーを入力してください。

Telegram

② 使用可能なコマンド一覧

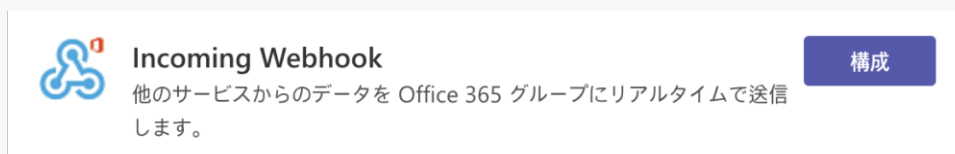
- **/help** : コマンド一覧を表示
- **/license** : 通知を受信するプロジェクトのアクセスキーを入力
- **/remove** : 通知を受信しないプロジェクトコードを入力
- **/list** : 現在通知を受信しているプロジェクトコードを表示

Teams

- ①
1. 通知を受信したいチャンネルの **コネクタ** に移動します。



2. Webhook を追加し、[構成] ボタンをクリックします。



3. Webhook 名を入力し、[作成] ボタンをクリックします。



Incoming Webhook

フィードバックの送信

Incoming Webhook コネクタを利用すると、トラッキング対象の活動についての通知を外部サービスから受け取ることができます。このコネクタを使うには、別サービスで設定を作成する必要があります。そのサービスが、Office 365 コネクタ形式 対応の Web フックをサポートしている必要があります。

* が付いているフィールドは必須です

着信 Web フック (Incoming Webhook) をセットアップするには、名前を入力して [作成] を選んでください。*

この着信 Web フック (Incoming Webhook) からのデータに関連付ける画像をカスタマイズします。

イメージをアップロードします。



既定のイメージ

作成

キャンセル

4. 生成された Webhook URL をコピーします。

以下の URL をコピーしてクリップボードに保存してから、[保存] を選んでください。この URL は、グループへのデータ送信元となるサービスの画面で必要になります。

`https://whatap.webhook.office.com/webf`



URL は最新です。

完了

削除

5. WhaTap モニタリングサービスの サードパーティプラグインの追加 画面に戻り、Teams タブ下部の Channel Name と Webhook URL に値を入力します。

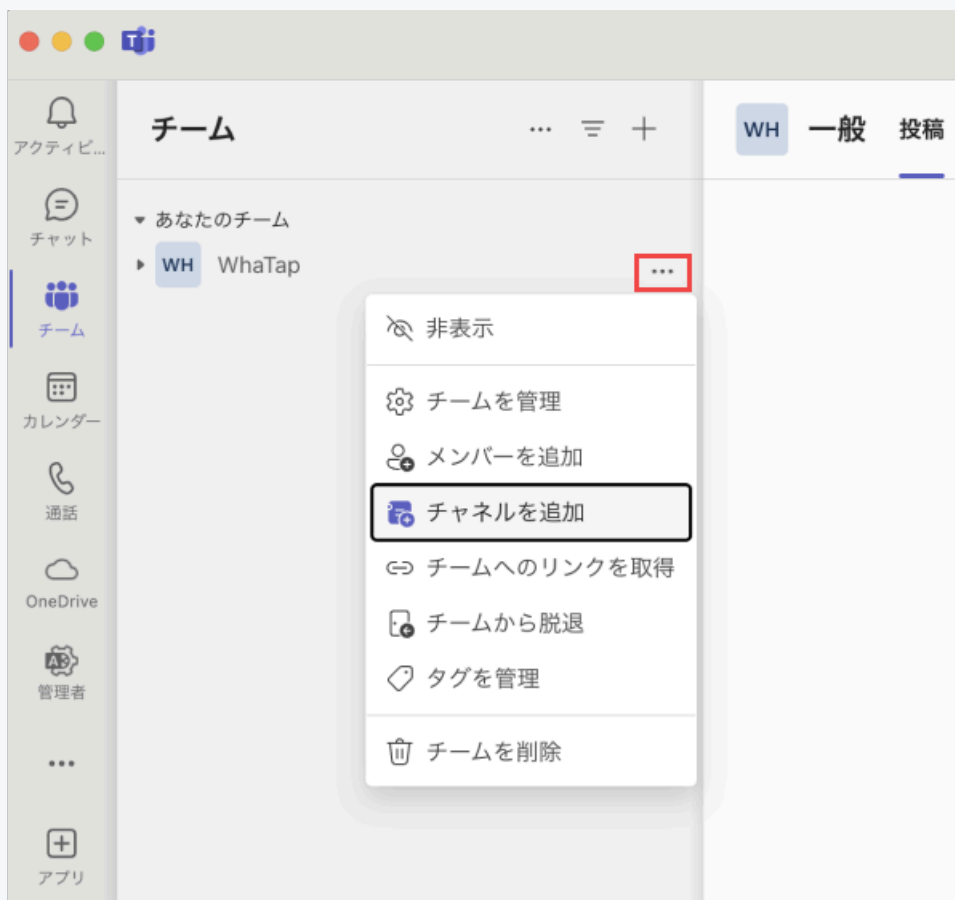
6. [登録] ボタンをクリックします。

Teams Workflows



- ① ワークフローを使用するには、**Microsoft Teams** にアクセス可能なアカウントと **ビジネスプランのサブスクリプション**が必要です。

1. チーム メニューの **その他の操作 (...)** > **チャンネルを追加** をクリックします。



2. チャンネルの作成画面で **チャンネル名** と **説明** を入力します。チャンネルの種類は **標準** を選択し、[作成] ボタンをクリックします。



チャンネルの作成

チャンネル名 *

WhaTapのイベントチャンネル

説明

他のユーザーが、適切なチャンネルを見つけられるように説明を入力します

チャンネルの種類を選択する * ⓘ

選択

標準
チームの全員がアクセスできます。

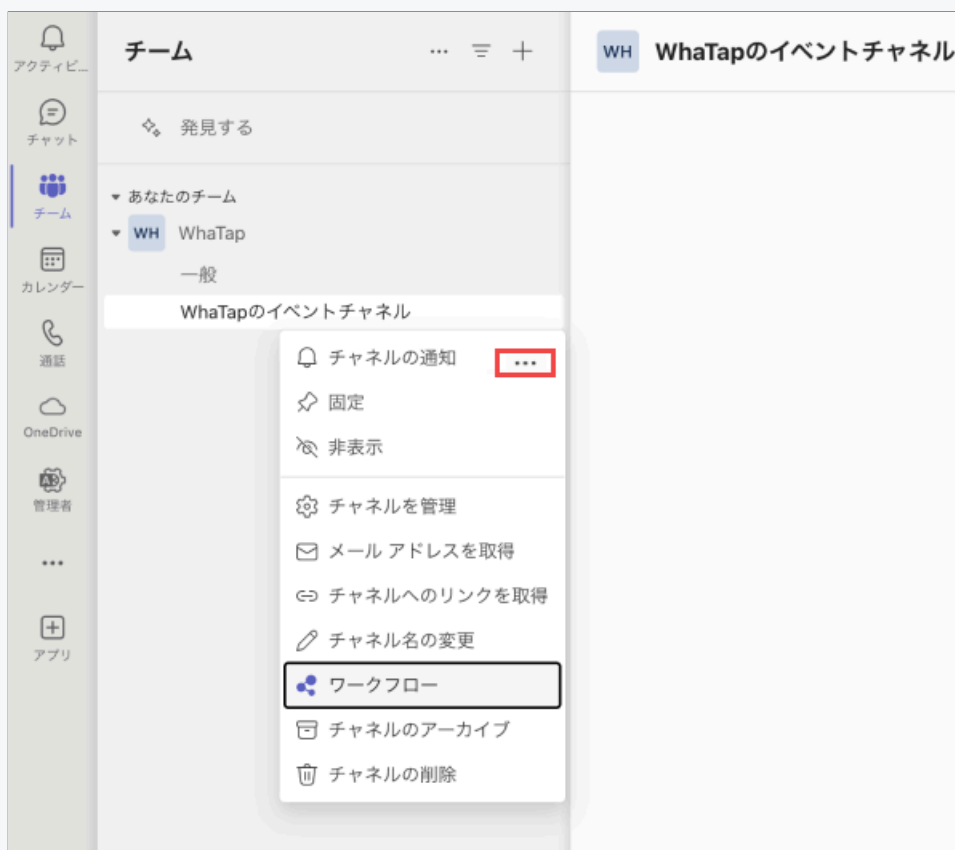
共有
組織内または組織外の人またはチームがアクセスできます。

プライベート
チームの特定のユーザーがアクセスできます。

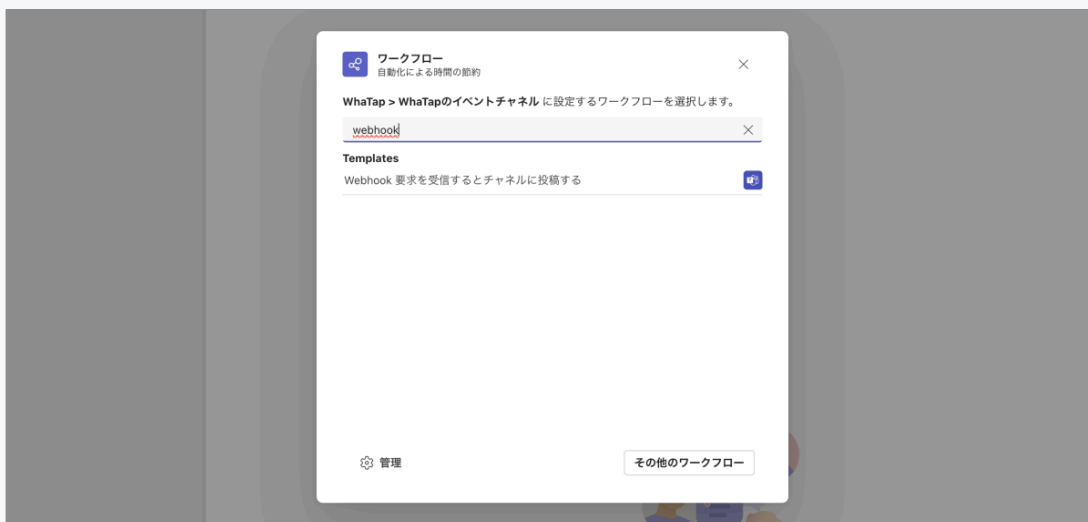
キャンセル 作成

❗ チャンネルの種類を **共有** にするとワークフローは使用できません。**プライベート** を選択した場合、ワークフローは追加できますが通知は受信できません。

- 作成したチャンネルの **その他の操作 (...)** > **ワークフロー** をクリックします。



4. ワークフロー ダイアログの一覧から Webhook 要求を受信したらチャンネルに投稿 を選択し、[ワークフローを追加] ボタンをクリックします。



5. 名前と接続の状態を確認し、[次へ] ボタンをクリックします。
6. 詳細を確認後、[ワークフローを追加] ボタンをクリックします。
7. ワークフローが追加されました。生成された URL をコピーします。



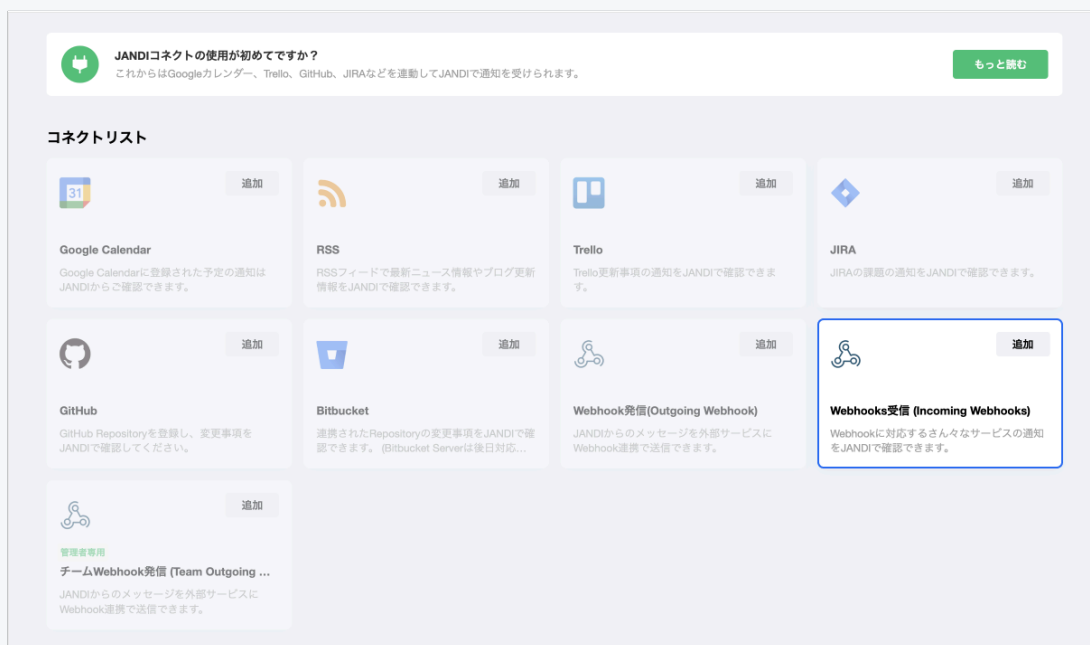
8. WhaTap モニタリングサービスの **サードパーティプラグインの追加** 画面に戻り、Teams **Workflows** タブ下部の **Channel Name** と **Webhook URL** に値を入力します。
9. [登録] ボタンをクリックします。

Jandi





1. 通知を受信するトピックまたはチャットで、**Jandi Connect 設定** に移動します。
2. **コネクト一覧** から **Webhook 受信 (Incoming Webhook)** を選択し、[連携する] ボタンをクリックします。



3. [**Webhook 受信を追加**] ボタンをクリックします。
4. **Webhook URL 登録** 項目に表示される Webhook URL をコピーします。



5. WhaTap モニタリングサービスの **サードパーティプラグインの追加** 画面に戻り、**Jandi** タブ下部の **Channel Name** と **Webhook URL** に値を入力します。
6. [**登録**] ボタンをクリックします。



1. AlertNow サービスにアクセスし、設定 > Integration メニューに移動します。



2. Integration 画面で [Integration 作成] ボタンをクリックします。
3. Integration タイプの中から **WhaTap** を選択します。
4. Integration 作成 画面で、名前 および 命名規則 を設定します。

5. [確認] ボタンをクリックすると、Integration が作成されます。
6. 作成された Integration の一覧を確認し、該当する Integration を選択します。



インテグレーション

インテグレーションの作成 検索語を入力 最後のアップデート: 2024-02-21 11:25:10

統合名	統合タイプ	統合キー	サービス名
ワットテスト	ワタップ		ワットテスト

7. 詳細画面で、URL 右側のコピーアイコンをクリックして URL をコピーします。

← インテグレーション

ワットテスト

基本情報

統合タイプ	ワタップ
統合キー	fda527a5140
URL	https://alertnowitgr.opsnow.com/integration/whatap/v1/
コンストラクタ	リサ

クリップボードにコピーする

8. Whatap モニタリングサービスの **サードパーティプラグインの追加** 画面に戻り、AlertNow タブ下部の **Channel Name** と **Webhook URL** に値を入力します。
9. [登録] ボタンをクリックします。

Webhook



1. 通知を受信する Webhook を登録します。登録した URL に対して、通知の **title** と **text** が POST メソッドで送信されます。

```
{
  "title": "Alert Title",
  "text": "Sample warning message"
}
```

2. **Webhook Name** と **Webhook URL** の項目を入力します。
3. [登録] ボタンをクリックします。

Webhook JSON



1. 通知を受信する Webhook を登録します。登録した URL に対して、通知データが **JSON 形式で POST** メソッドにより送信されます。JSON に含めることができる置換変数については、**使用可能な変数**を参照してください。

- `${something}` は WhaTap が提供する置換値を表します。対応する全一覧と意味については、**使用可能な変数**を参照してください。
- イベント状態（`status`）は、**イベント発生**（`on`）と**イベント解消**（`off`）に区別されます。
- `level` は `None`、`Info`、`Warning`、`Critical` に区別されます。

```
{
  "pcode": "${pcode}",
  "projectName": "${projectName}",
  "time": "${time}",
  "oid": "${oid}",
  "oname": "${oname}",
  "title": "${title}",
  "message": "${message}",
  "level": "${level}",
  "status": "${status}",
  "metricName": "${metricName}",
  "metricValue": "${metricValue}",
  "metricThreshold": "${metricThreshold}",
  "uuid": "${uuid}",
  "okind": "${okind}",
  "onode": "${onode}"
}
```

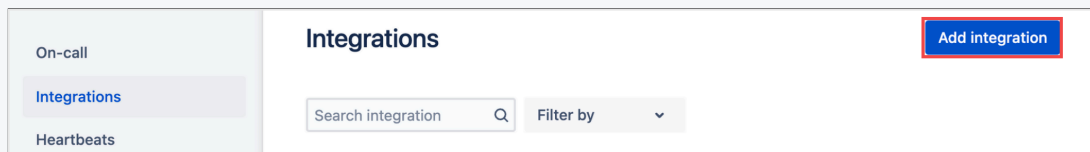
2. **Webhook Name** と **Webhook URL** の項目を入力してください。
3. ヘッダー値を追加するには、**ユーザーヘッダー値の追加** の + 追加 をクリックし、key と value を入力してください。
4. [登録] ボタンをクリックしてください。

Opsgenie

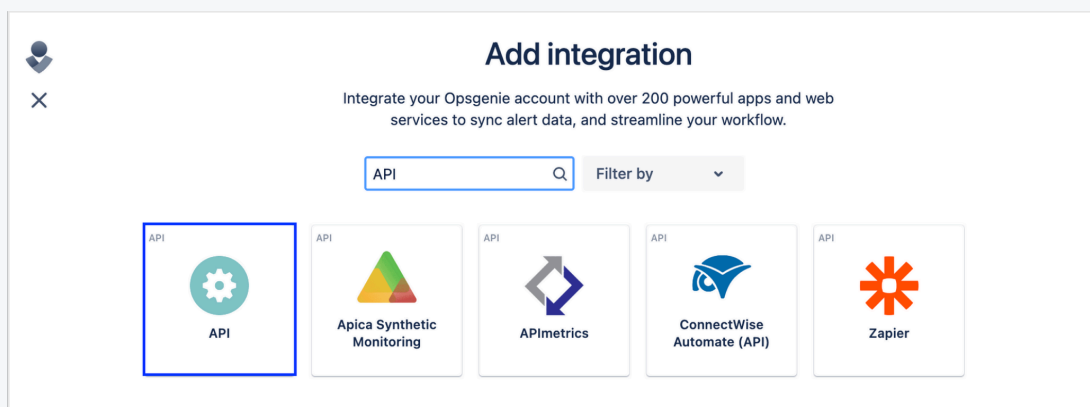




1. **Teams** メニューで、アラートを受信するチームを選択してください。
2. **Integration** メニューに移動し、[Add Integration] ボタンをクリックしてください。



3. インテグレーション一覧で **API** を検索し、選択してください。



4. API 名を設定し、チームを割り当て、各権限を設定した後、[Save Integration] ボタンをクリックしてください。



Forwarding rules
Your on-call schedule

ON-CALL
Global policies
All schedules
All escalations

CONNECTED APPS
Atlassian products

INTEGRATIONS
Integrations
Heartbeats
Slack
GitLab

Settings

Name:

Assigned to Team:

API Key:  

Read Access: ☒

Create and Update Access: ☒

Delete Access: ☒

Restrict Configuration Access: ☐

Enabled: ☒

Suppress Notifications: ☐

[Save Integration](#) [Cancel](#)

5. Whatap モニタリングサービスの **サードパーティプラグインの追加** 画面に戻り、Opsgenie タブ下部の **Name** と **API Key** を入力してください。
6. [登録] ボタンをクリックしてください。



PagerDuty



1. [PagerDuty](#) アカウントを登録し、ログインしてください。
2. PagerDuty で **Services > Service Directory** メニューに移動し、[+ New Service] ボタンをクリックしてください。
3. サービス情報 (Name) を入力し、[Next] ボタンをクリックしてください。
4. **Escalation Policy** を設定し、[Next] ボタンをクリックしてください。



PagerDuty

5. **Alert Grouping** と **Transient Alerts** を設定し、[Next] ボタンをクリックしてください。

PagerDuty

6. **Integrations** で **Event API V2** を選択し、[Create Service] ボタンをクリックしてください。

PagerDuty

7. 作成されたサービス画面で **Integration Name** と **Integration Key** の値をコピーしてください。

PagerDuty

8. WhaTap モニタリングサービスの **サードパーティプラグインの追加** 画面に戻り、**Integration Name** と **Integration Key** を入力してください。
9. [登録] ボタンをクリックしてください。

❗ メッセージを受信できない、またはプラグインが登録されない場合は、**Integration Name** または **Integration Key** の値が正しいか確認してください。

LINE



1. LINE アプリをインストールしてください。
2. 以下の QR コードをスキャンして、**WhaTapLabs** 公式チャンネルを友だち追加してください。

LINE 3rd パーティプラグイン追加

3. 次のコマンドを使用して、プロジェクトを LINE と連携し、通知を設定してください。

コマンド

```
/help # 使用可能なコマンド一覧を表示
/list # 連携されているプロジェクト一覧を表示
/license [アクセスキー] # 新しいプロジェクト連携を追加
```



```
/remove [プロジェクトコード] # プロジェクト連携を解除
/language [ko|ja|en] # 通知言語を設定（韓国語／日本語／英語）
```

- プロジェクトのアクセスキーは **管理 > プロジェクト管理** で確認できます。
- LINE 内で `/language` コマンドを使用した場合、その設定は **該当する LINE チャットルーム内のみ** に適用されます。他の 3rd パーティプラグインやプロジェクトの通知言語は変更されません。

使用例

```
/license XXXXXXXXXX # プロジェクトを連携
/language ko # 言語を韓国語に設定
/list # 連携済みプロジェクトを確認
```



- **プロジェクトアクセスキー**: WhaTap プロジェクト内の **管理 > プロジェクト管理** で確認できます。
- **言語設定**: `/language` コマンドは LINE チャットルーム内でのみ有効で、他の通知チャンネルの言語は変更されません。

ilert



1. ilert コンソールの **Alert sources** 画面右上にある **[+ Create alert source]** をクリックします。
2. **Integration type** ステップ下部の **Filter integrations** 検索欄に **WhaTap** を入力して検索します。
3. 検索結果から **WhaTap** タイルを選択し、**[Next]** ボタンをクリックします。
4. アラートソース名を入力し、チームを指定した後、**[Next]** ボタンをクリックします。
 - エスカレーションポリシーは、新規作成または既存のものを選択できます。
5. アラートのグループ化方式を選択し、**[Continue setup]** ボタンをクリックします。
 - 最初に選択した **Do not group alerts** は後から変更可能です。
6. 次の画面で **アラートテンプレートや優先度などの追加設定** を行うことができます。ここでは [



Finish setup] ボタンをクリックして設定を完了します。

7. 設定が完了すると、完了画面で **API キー** または **Webhook URL** が生成されます。
8. **Webhook JSON** タブで生成された **Webhook URL** をコピーし、下部の **Webhook URL** 入力欄に貼り付けます。
9. [登録] ボタンをクリックします。

大量アラート発生の防止

短時間に大量のアラートが発生した場合、指定した時間だけアラート通知を一時的に停止します。たとえば、5 分間に 20 件のイベントが発生すると、その後 5 分間は警告アラートが送信されません。設定した **停止時間** が経過すると、大量アラート防止機能は自動的に解除されます。

1. 次の画面に移動してください。 **アラート通知** > **通知設定** > **大量アラート通知発生防止** セクション
2. トグルボタンをクリックして **有効化** または **無効化** します。
 -  **有効**: 大量アラートを検知した場合、一時的に通知を停止
 -  **無効**: アラート通知を再開
3. **検知時間**, **検知回数**, **停止時間** を設定してください。
 - **検知時間** 内に **検知回数** 以上のイベントが発生すると、**停止時間** の間、警告アラートが停止されます。



大量アラートによってブロックされた場合、ブロック案内ボックスが表示されます。大量アラート防止機能をすぐに解除するには、ボックス内の **大量アラート発生中止** ボタンをクリックしてください。

イベント通知フォーマット

共通アラートテンプレート

共通テンプレートは、ほとんどのケースで適用できます。さまざまな環境において、同一のフォーマットでアラートを受信できます。

- プロダクトタイプ: アプリケーション、データベース、Kubernetes
- イベントタイプ: アプリケーションアラート、データベースアラート、メトリクスアラート
- イベントチャンネル: SMS、Mobile、3rd-party プラグイン、プラグイン

イベントタイトル

Event title format

```
[Level][Platform][ProjectName][ApplicationName][EventTitle]
```

Event title example

```
[Info][JAVA][アプリケーションプロジェクト][TC-0-1-8081][CRITICAL_HIGH_MEMORY]
```

❗ ApplicationName が設定されていない場合、イベントタイトルから省略されます。

- Platform は以下のいずれかで表示されます。
 - JAVA
 - NODEJS
 - PYTHON
 - PHP
 - DOTNET
 - GO
 - POSTGRESQL



- ORACLE
- MYSQL
- MSSQL
- BSM_JAVA
- CLOUDWATCH
- TIBERO
- KUBERNETES
- KUBE_NS
- URLCHECK
- URLCHECK_ADMIN
- CUBRID
- ALTIBASE
- CLUSTER
- REDIS
- MONGODB
- VR
- RUM

イベントメッセージ

イベントメッセージに含めることができる情報です。 `optional` が `false` の場合、常にメッセージに含まれます。
`optional` が `true` の場合、該当データが確認できるときのみ表示されます。

イベントメッセージ例

```
Project Name : アプリケーションプロジェクト  
Project Code : 3  
Agent Name : TC-0-1-8081  
Message : RECOVERED: Memory is too high. less than 10%  
Event Time : 2022-04-12 18:53:24 +0900
```

Event OFF Time : 2022-04-12 18:53:24 +0900
 Alert Type : APPLICATION_MEMORY
 Metric Name : memory
 Metric Value : 20
 Metric Threshold : 10
 Stateful : true

表 | イベントメッセージ構成要素

En	Ko	対応するアラートタイプ	説明
Project Name	プロジェクト名	全て	-
Project Code	プロジェクトコード	全て	-
Agent Name	エージェント名	全て (optional)	oname
Message	イベントメッセージ	全て	-
Alert Type	イベント種別	全て	下記の AlertType 表を参照
Event Time	イベント発生時間	全て	2022-04-13 10:40:49 +0900 の +0900 は GMT オフセット
Event Off Time	イベント解除時間	全て (optional)	2022-04-13 10:40:49 +0900 の +0900 は GMT オフセット
Metric Name	メトリクス名	全て (optional)	イベント条件判定に使用されるメトリクス名
Metric Value	メトリクス値	全て (optional)	メトリクス値が閾値を超えた場合に含まれる
Metric Threshold	メトリクス閾値	全て (optional)	メトリクス条件の閾値

En	Ko	対応するアラートタイプ	説明
Stateful	復旧イベント通知	全て (optional)	復旧通知が有効な場合 <code>true</code> 、それ以外は <code>false</code>
Event Rule	イベント発生条件	メトリクスアラート	-
Target Filter	イベント対象選択	メトリクスアラート	特定対象から収集されたメトリクスのみ評価
Repeat Count	イベント繰り返し回数	メトリクスアラート	繰り返し時間内に指定回数条件を満たすと発生
Repeat Duration	イベント繰り返し時間	メトリクスアラート	繰り返し回数を評価する時間
Receiver	受信者	メトリクスアラート	-
Query	MXQL クエリ	複合メトリクスアラート	-
Rule	イベント発生条件	複合メトリクスアラート	-
Query Period	クエリ期間	複合メトリクスアラート	-
Query Interval	クエリ間隔	複合メトリクスアラート	-
Silent Time	サイレント時間	複合メトリクスアラート	-
Query	URL	Exception アラート	例外を発生させたリクエストの URL
TXID	トランザクション ID	Exception アラート	-

En	Ko	対応するアラートタイプ	説明
Class	エラークラス名	Exception アラート	-
Log Message	ログメッセージ	サーバーファイル ログアラート	-
Log File	ログファイルパス	サーバーファイル ログアラート	-
IP	IP	サーバーアラート全 体	-
CPU	CPU	サーバーアラート全 体	イベント発生時のスナップショット
CPU_load1	CPU_load1	サーバーアラート全 体	イベント発生時のスナップショット
CPU_loadPerCore	CPU_loadPerCore	サーバーアラート全 体	イベント発生時のスナップショット
Memory	メモリ	サーバーアラート全 体	イベント発生時のスナップショット
Swap	スワップ	サーバーアラート全 体	イベント発生時のスナップショット
Disk Name Used Percent Free Size IO Percent	ディスクパフォー マンス	サーバーアラート全 体	イベント発生時のスナップショット
Name Bps Pps	トラフィックパフ ォーマンス	サーバーアラート全 体	イベント発生時のスナップショット
Message Time Name	処理履歴メッセー ジ	サーバーアラート全 体	-

❗ このセクションでは、該当するイベントで提供可能な情報を最大限に表示します。

- **AlertType** は以下のいずれかの値で表示されます。

AlertType	説明
APPLICATION_CPU	アプリケーション CPU アラート
APPLICATION_MEMORY	アプリケーション メモリアラート
APPLICATION_DISK	アプリケーション ディスクアラート
APPLICATION_ACTIVE_TRANSACTION	アプリケーション アクティブTXアラート
APPLICATION_ERROR_TRANSACTION	アプリケーション エラートランザクションアラート
APPLICATION_SLOW_TRANSACTION	アプリケーション トランザクション応答時間アラート
METRICS	メトリクスアラート
COMPOSITE_METRICS	複合メトリクスアラート
ANOMALY	異常値アラート
LOG_REALTIME	リアルタイムログアラート
COMPOSITE_LOG	複合ログアラート
SERVER_REBOOT	サーバー 再起動アラート
SERVER_NO_DATA	サーバー データ未受信アラート
SERVER_PORT	サーバー ポートアラート
SERVER_NETWORK_IOPS	サーバー ネットワーク IOPS アラート
SERVER_NETWORK_BPS	サーバー ネットワーク BPS アラート



AlertType	説明
SERVER_DISK_IO	サーバー ディスク I/O アラート
SERVER_DISK_QUOTA	サーバー ディスク使用量アラート
SERVER_DISK_INODE	サーバー inode アラート
SERVER_CPU	サーバー CPU アラート
SERVER_MEMORY	サーバー メモリアラート
SERVER_CPU_STEAL	サーバー CPU steal アラート
SERVER_MEMORY_SWAP	サーバー スワップメモリアラート
SERVER_LOG_FILE	サーバー ログファイルアラート
SERVER_WINDOW_EVENT	サーバー Windows イベントアラート
SERVER_OFF	サーバー アラート OFF 通知
SERVER_ACKNOWLEDGE	サーバー 処理確認通知
SERVER_PROCESS_COUNT	サーバー プロセス数アラート
SERVER_PROCESS_CPU	サーバー プロセス CPU アラート
SERVER_PROCESS_MEMORY	サーバー プロセス メモリアラート
SERVER_PROCESS_OFF	サーバー プロセスアラート OFF 通知
AGENT_ACTIVE	エージェント 有効化アラート
AGENT_INACTIVE	エージェント 無効化アラート



AlertType	説明
AGENT_REACTIVATED	エージェント 再有効化アラート
URL	URL アラート
TOO_MANY_EVENT	イベント多発アラート
CLOUD_WATCH	CloudWatch アラート
EXCEPTION	例外アラート

イベント履歴

ホーム > プロジェクト選択 > 🔍 アラート通知 > イベント履歴

イベント履歴では、プロジェクトで発生したさまざまなイベントを確認し、詳細情報を分析できます。Elasticsearch DSL クエリをサポートしており、指定した条件に一致するイベントを迅速かつ正確に検索できます。

イベント履歴の確認

検索結果でイベントタイトルをクリックすると、そのイベントが発生した時間帯の詳細データを分析できる画面に移動します。これにより、イベント発生前後の状況を総合的に把握できます。

1. アラート通知 > イベント履歴 に移動してください。
2. イベント履歴 画面の 時間選択 で、イベント履歴を確認する期間を設定してください。
3. フィルター入力欄にクエリを入力し、[虫眼鏡] ボタンをクリックしてください。
 - クエリを入力しない場合、すべてのイベントが表示されます。

🔧 カラム設定

表示するカラムや非表示にするカラムを設定できます。

1. イベント履歴 画面の左上にある [🔧 カラム設定] ボタンをクリックしてください。
2. カラム設定 画面で、表示または非表示にするカラムを選択してください。
 - 表示項目 でカラムの順序を変更できます。
 - カラム名検索 欄で目的のカラムを検索できます。

カラム項目	説明
イベント名	イベントのタイトル
メッセージ	イベントのメッセージまたはスナップショット情報

カラム項目	説明
イベント状態	イベントの現在の状態
エージェント名	イベントが発生した対象エージェントの名前 (Oname) - 特定のエージェントに紐づかないイベントの場合は空欄で表示されます
エージェントグループ	イベントが発生した対象エージェントの種類 (OkindName) - 特定のエージェントに紐づかないイベントの場合は空欄で表示されます
エージェントノード	イベントが発生した対象エージェントのサーバー (OnodeName) - 特定のエージェントに紐づかないイベントの場合は空欄で表示されます
イベント発生時刻	イベントが発生した時刻
イベント解消時刻	イベントが解消された時刻 - 解消状態を持たないイベントの場合は - と表示されます

3. 設定が完了したら、[確認] ボタンをクリックしてカラム設定を反映してください。

↓ CSV ダウンロード

検索結果を CSV ファイル形式でダウンロードできます。

1. アラート通知 > イベント履歴 で [CSV] ボタンをクリックしてください。
2. 現在のフィルター条件に一致するイベント一覧が CSV ファイルとして保存されます。

進行中のイベントのみ表示

現在進行中の状態のイベントのみを表示できます。

1. アラート通知 > イベント履歴 で [進行中のイベントのみ表示] ボタンをクリックしてください。
2. フィルタークエリに次の条件が自動的に追加され、検索が実行されます。

```
Stateful: true and Status : "ON"
```

イベント検索

- **正確な検索:** 必要なイベントだけを取得できるよう、条件を正確に指定
- **複合条件:** 複数のフィールドを同時に検索し、複雑な条件も一度に処理
- **柔軟なパターン:** ワイルドカードや部分一致など、さまざまな検索方式をサポート
- **高速パフォーマンス:** インデックス化されたデータを活用した高速検索

検索可能なフィールド

フィールド名および値は大文字と小文字を区別しません。

- **フィールド名タグ:** フィールドがサポートされるイベントタイプ
- **フィールドタイプ:** フィールドのデータ型
 -  #: Number
 -  T: String
 -  C: Boolean
 -  D: Date

イベント情報フィールド

フィールド名	タイプ	説明	例
Title	String	イベントタイトル	"Database Connection Error"
OffTitle	String	イベント解消タイトル	"RECOVERED: Database Connection Error"
Message	String	イベントメッセージ	"Connection timeout occurred"
OffMessage	String	イベント解消メッセージ	"RECOVERED: Connection timeout occurred"

フィールド名	タイプ	説明	例
Level	String	現在のイベントレベル	Critical, Warning, Info
OriginLevel	String	元のイベントレベル	Critical, Warning, Info
Status	String	イベント状態	ON, OFF, CANCEL, ACKNOWLEDGE, MAINTENANCE, DISABLED
ActCount	Number	発生回数	2
MetricName	String	指標名	"memory"
MetricValue	String	指標値	"85.5"
OffValue	String	解消時の値	"72.8"
MetricThreshold	String	閾値	"80"
alertType	String	イベント種別	"BASIC", "METRICS", "TRANSACTION" など
alertId	String	イベントルールの一意識別子	"zf3uoj0fv4v7"

イベントタイプ別対応フィールド

ⓘ 特定のイベントタイプでのみサポートされるフィールドです。該当しないイベントタイプの場合、値が存在しないことがあります。

フィールド名	タイプ	イベント種別	説明	例
eventRule	String	基本、メト	イベント発生	"memory ≥ 80"

フィールド名	タイプ	イベント種別	説明	例
		リクス	ルール	
field	String	リアルタイムログ	ログ検索キー	"content"
keyword	String	リアルタイムログ	ログ検索値	"Error"
logCategory	String	リアルタイムログ	ログカテゴリ	"AppLog"
logContent	String	リアルタイムログ	ログ内容	"00:00000:00009:2025/04/06 23:03:52.55 server Error: 1601, Severity: 17, State: 3\n00:00000:00009:2025/04/06 23:03:52.55 server There are not enough 'user connections' available to start a new process."

対象フィールド

フィールド名	タイプ	説明	例
Oid	Number	エージェントの一意識別子	-98765432
Oname	String	エージェント名	"web-server-01"
Okind	Number	エージェント種別の一意識別子	867318026

フィールド名	タイプ	説明	例
OkindName	String	エージェント種別名	"web-server"
Onode	Number	エージェントノードの一意識別子	334634079
OnodeName	String	エージェントノード名	"production-node-1"

イベント固有値フィールド

フィールド名	タイプ	説明	例
Id	Number	イベントの一意識別子	5768121
UUID	String	イベント固有識別子	"550e8400-e29b-41d4-a716"

状態／フラグフィールド

フィールド名	タイプ	説明	例
Stateful	Boolean	状態ベースイベントかどうか	true, false
Disabled	Boolean	無効化されたイベントかどうか	true, false
Escalation	Boolean	エスカレーション有無	true, false
SystemEvent	Boolean	システムイベントかどうか	true, false

検索タイプ別クエリ構文

❗ 検索の基本構文については、[WhaTap ログ検索クエリ構文](#) ドキュメントを参照してください。

1. キーワード検索

「Database Connection」という文字列を含むイベント

```
title: "Database Connection"
```

2. 複数値検索

指定した複数の値のうち、いずれかを含むイベントを検索します。

```
title: Database Connection
```

現在のイベントレベルが Info または Warning のイベント

```
level: info warning
```

3. パターン検索

ワイルドカードを使用してパターン検索ができます。

名前パターンで特定のエージェントで発生したイベントを検索

```
oname: web-*-prod
```

タイトルが Connection で終わるイベントを検索

```
title: *Connection
```

4. 複合条件検索

複数の条件を組み合わせて、より正確に検索できます。

レベルが Critical で、タイトルに Database を含むイベント

```
level: critical and title: Database
```

特定のエージェントにおける Warning または Critical のイベント

```
oname: web-server-01 and level: Warning Critical
```

5. OR 条件検索

複数の条件のうち、**いずれか一つでも満たす**イベントを検索します。

タイトルまたはメッセージに特定のキーワードを含むイベント

```
title: Connection or message: Connection
```

6. 除外条件

特定の条件を除外して検索できます。

Info レベルを除いたすべてのイベント

```
not level: info
```

リアルタイムアラート

リアルタイムアラート機能は、イベント設定で設定したイベントが発生した際に、ポップアップ形式で表示されます。イベント発生と同時に通知を受け取ることで、問題を迅速に把握し、対応することができます。また、すでに発生した通知や見逃した通知の履歴を確認することで、リアルタイム対応が難しかった状況を把握し、解決に役立てることができます。

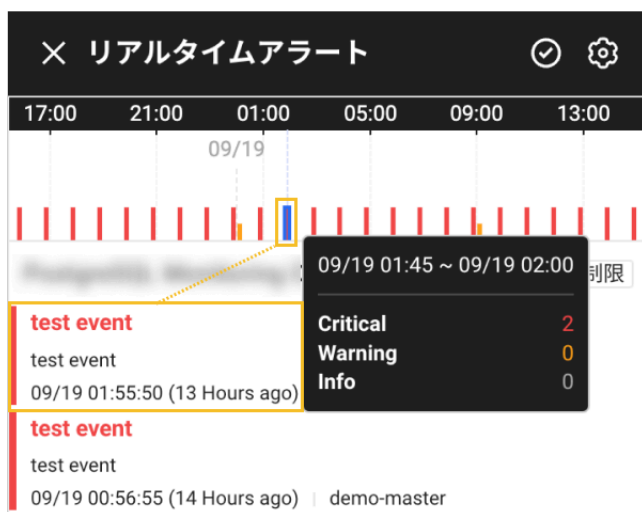
リアルタイムアラートを確認する

リアルタイムアラートは、画面右上にポップアップとして表示されます。通知が発生した時刻、タイトル、メッセージを確認できます。

- 個別の通知を閉じるには、メッセージ右上の ✕ ボタンをクリックしてください。
- 画面に表示されているすべてのポップアップ通知を閉じるには、**すべての通知を閉じる** をクリックしてください。

通知履歴を確認する

1. プロジェクトを選択して表示される画面の最上部にある 🔔 をクリックしてください。
2. リアルタイムアラート ウィンドウが表示されます。
 - 現在のプロジェクトについて、直近24時間以内の通知を最大100件まで確認できます。
 - 個別のイベント項目を選択すると、関連するメニューに移動します。
 - リアルタイムアラート ウィンドウ内の時間別チャートで任意の時間帯を選択すると、該当するイベント項目に移動します。



- すべての通知履歴を確認するには、**全体の通知履歴** ボタンをクリックしてください。**アラート通知 > イベント履歴** メニューに移動します。

❗ リアルタイムアラート の一覧が空の場合、**全体の通知履歴** ボタンが表示されます。受信タグ未設定の通知を受け取る オプションを無効にしてください。

イベントを一括で解消する

リアルタイムアラート の一覧から、進行中のすべてのイベントを一括で解消できます。

イベント解消が完了するまでに、約30秒～1分程度かかる場合があります。

- **イベント一括処理** 機能を使用すると、現在進行中のイベントに対する解消通知が大量に発生する可能性があります。
- **イベント一括処理** 機能を使用した後でも、イベントルールが有効であり、データが引き続きしきい値を超えている場合、イベントは再度発生することがあります。
- イベント解消通知は、**アラート通知 > イベント設定** メニューでイベントを編集し、**イベントが解消されたときに追加通知** または **解消通知** オプションを無効にすることで停止できます。

使用方法:

1. プロジェクトを選択して表示される画面上部の  をクリックします。
2. リアルタイムアラート ウィンドウが表示されたら、右上の  をクリックします。
3. リアルタイムアラートリストの進行中イベントを一括で解消します。 というメッセージが表示されたら、解消 ボタンをクリックします。

リアルタイムアラートを設定する

1. プロジェクトを選択して表示される画面上部の  をクリックします。
2. リアルタイムアラート ウィンドウが表示されたら、右上の  をクリックします。
3. リアルタイムアラート設定画面で各項目を設定します。
 - ポップアップ通知: リアルタイムアラート ウィンドウが閉じている状態でも、ポップアップ形式で通知を表示します。
 - 解消済みイベントを表示: リアルタイムアラート 一覧に解消済みイベントも含めて表示します。
 - 通知音の試聴: ブラウザで再生される通知音を事前に確認できます。Critical または Warning の横にある  をクリックしてください。音が再生されない場合は、ブラウザの設定をご確認ください。

システムイベント

WhaTap モニタリングは、プラットフォーム全体で自動的に検知・生成される共通イベントを提供します。本ドキュメントでは、システムによって発生するイベントの種類、発生条件、および対応方法について説明します。

EVENT_BLOCKED_BY_SYSTEM

プロジェクト内で短時間に過剰な数のイベントが発生した場合、WhaTap システムがこれを検知し、イベントの発生を一時的にブロックします。イベントがブロックされると、システムは次のメッセージをユーザーに通知します。このイベントが発生した場合は、イベント設定内容を確認し、必要に応じて調整してください。

 **Critical**



イベントメッセージ

Excessive events detected, event blocked for stability. name: server agent

プロジェクト番号	8
プロジェクト名	new server
対象	server agent
イベント名	EVENT_BLOCKED_BY_SYSTEM
イベント日時	(GMT+0900) 2024-11-18 18:03:18

WhaTapにログイン

new serverプロジェクトのserver agentから過度なイベントが検知されたため、イベント発生が遮断されます。server agentから一定期間の間にイベントが発生しなくなると、遮断が自動で解除されます。

ブロック基準

イベントは次の基準に基づいてブロックされます。

1. エージェント単位のブロック

1つのエージェントで **1分以内に10件** のイベントが発生した場合、そのエージェントから発生する以降のイベントはブロックされます。

2. 複数エージェントによる全体ブロック

条件 **1** によりイベントがブロックされたエージェントが **1分以内に3件以上** 発生した場合、プロジェクト全体のイベントがブロックされます。

3. プロジェクト単位のブロック

1つのプロジェクトで **1分以内に100件** のイベントが発生した場合、プロジェクト全体のイベントがブロックされます。

ブロック解除方法

システムによってイベントがブロックされた場合、対象のエージェントまたはプロジェクトで **1分間** イベントが発生しない状態を維持する必要があります。

- **アラート通知 > イベント設定** メニューから設定されているすべてのイベントを無効化してください。**イベント設定** を見直し、過剰なイベントが発生しないように閾値を調整する必要があります。
- イベントを設定する前に、**シミュレーション** 機能を活用してイベント発生回数を事前に予測できます。

HTTPステータスのコードタイプ

WhaTap URLモニタリングを通じてウェブサービスの障害有無を確認できます。ウェブサービスからのリターンされるステータスコードが4xx、5xxの場合、警告通知を送信します。このようなステータスコードは、**HTTPステータスコード(HTTP Status Code)**と呼びます。代表例として"404 Not Found"があります。

ステータスコードは3桁の数字で構成され、最初の桁は1から5までです。最初の桁が4または5の場合は、正常な状況ではないため、サイト管理者が直ちに認知する必要があります。

- **1xx(情報)**: リクエストを受けており、プロセスは継続中です。
- **2xx(成功)**: リクエストは正常に受付、認識、処理されました。
- **3xx(リダイレクション)**: リクエストを完了するには、追加の作業が必要です。
- **4xx(クライアントエラー)**: リクエストの文法が正しくないか、リクエストを処理できません。
- **5xx(サーバーエラー)**: サーバーは有効なリクエストの処理に失敗しました。

❗ HTTPステータスコードの詳細については、次のリンクを参照してください。

- [W3 RFC 2616ステータスコードのまとめ](#)
- [mozilla財団ステータスコードのまとめ](#)
- [IETFのRFC 2616](#)

1XX: Information responses

ステータスコードが'1'で始まる場合は、サーバーがリクエストを受けており、サーバーに接続されたクライアントが作業を続行する必要があることを意味します。このコードはHTTP 1.0には対応していません。

- **100 Continue**

進行中であることを意味するレスポンスコードです。現在までの進行状況に問題はなく、クライアントがリクエストを継続するか、すでにリクエストを完了した場合は無視してもよいことを通知します。

- **101 Switching Protocol**

101レスポンスコードは、クライアントが送信したアップグレードリクエストヘッダーへのレスポンスとして送信

されます。このコードは、サーバーがクライアントのUpgradeリクエストを受け入れ、プロトコルを変更することを通知します。主にWebSocketプロトコルの切り替えに使用されます。

- **102 Processing(WebDAV)**

このレスポンスコードは、サーバーがリクエストを受信し、処理中だが、まだ最終レスポンスを提供できないことを意味します。

2XX: Successful responses

- **200 OK**

リクエストが正常に処理されました。リクエストに対するレスポンスとして情報が返されます。

- **201 Created**

リクエストは正常に処理され、その結果で新しいリソースが作成されました。このレスポンスは、主にPOSTリクエストや一部のPUTリクエスト以降に使用されます。

- **202 Accepted**

リクエストは受信されましたが、まだ処理されていません。このレスポンスは、リクエスト処理が非同期的に行われ、その後HTTPレスポンスで結果がリターンされたことを明示しません。別のプロセスがリクエストを処理しているか、サーバーがリクエストをバッチプロセスとして処理しているときに使用されます。

- **203 Non-Authoritative Information**

返されたメタ情報はオリジンサーバーのものではなく、ローカルまたはサードパーティのコピーから収集されたことを意味します。この場合、**200 OK**のレスポンスが優先される必要があります。

- **204 No Content**

リクエストを正常に処理しましたが、返すコンテンツがありません。ただ、ヘッダーは有効である可能性があり、ユーザーエージェントはキャッシュされたヘッダーを最新情報に更新できます。

- **205 Reset Content**

リクエストが完了した後、ユーザーエージェントがリクエストを送信したドキュメントビューをリセットする必要があることを意味します。

- **206 Partial Content** クライアントがスコープヘッダーを介して部分コンテンツをリクエストしたときに使用されます。ウェブサーバーは'206 Partial Content'レスポンスコードとともに、Range ヘッダーに指定されたデータ部分

を送信します。

- **207 Multi-Status**

マルチステータスレスポンスは、複数のリソースの複数のステータスコードを含む状況で使用されます。WebDAV(Web Distributed Authoring and Versioning)で主に使われます。

- **208 Already Reported**

Prostat(PropertyとStatusの合成語) レスポンス属性として、同じコレクションにバインディングされた複数の内部メンバーを繰り返し並べることを避けるために使用されます。WebDAV(Web Distributed Authoring and Versioning)で使われます。

- **226 IM Used (HTTP Delta encoding)**

サーバーがGETリクエストを処理し、レスポンスが1つ以上のインスタンス操作が適用された現在のインスタンスを含んでいることを通知します。

3XX: Redirection messages

- **300 Multiple Choice**

リクエストに対して1つ以上のレスポンスが可能であることを意味します。ユーザーエージェントまたはユーザーは、それらのいずれかを選択する必要があります。標準化されたレスポンスの選択方法はありません。

- **301 Moved Permanently**

リクエストしたリソースのURIが永久に変更されたことを意味します。新しいURIがレスポンスに提供されることもあります。

- **302 Found**

リクエストしたリソースのURIが一時的に変更されたことを意味します。新しいURIは後で提供されることがあり、クライアントはその後のリクエストでも必ず同じURIを使用する必要があります。

- **303 See Other**

サーバーがクライアントにリクエストしたリソースを他のURIからGETリクエストを通じて取得するように指示します。

- **304 Not Modified**

キャッシュ目的で使用されます。クライアントにレスポンスが修正されていないことを通知し、クライアントはキ

キャッシュされたバージョンを引き続き使用できます。

- **305 Use Proxy**

以前のHTTP仕様で定義されており、リクエストされたレスポンスが必ずプロキシを通じて接続する必要があることを通知します。プロキシのin-band設定に対するセキュリティ上の懸念により、使用が徐々に減少しています。

- **306 Unused**

現在は使用されておらず、今後の使用のために予約された状態です。HTTP 1.1以前のバージョンで使用されました。

- **307 Temporary Redirect**

クライアントがリクエストしたリソースが他のURIにあり、以前のリクエストと同じメソッドを使用してリクエストする必要があることを意味します。**302 Found**と似ていますが、**307 Temporary Redirect**の場合、使用されたHTTPメソッドを変更してはなりません。最初のリクエストがPOSTなら、2番目のリクエストもPOSTにする必要があります。

- **308 Permanent Redirect**

リソースが永続に異なるURIに位置することを意味します。**301 Moved Permanently**と似ていますが、**308 Permanent Redirect**の場合、使用されたHTTPメソッドを変更してはなりません。最初のリクエストがPOSTなら、2番目のリクエストもPOSTにする必要があります。

4XX: Client error responses

- **400 Bad Request**

このレスポンスは、リクエストの文法が正しくないため、サーバーがリクエストを理解できないことを意味します。

- **401 Unauthorized**

HTTP標準では'未承認(unauthorized)'を明確にしているが、実際にこのレスポンスは'非認証(unauthenticated)'を意味します。要求されたレスポンスを受け取るために、クライアントは認証を行う必要があります。

- **402 Payment Required**

このレスポンスコードは、後で使用されるために予約されています。デジタル決済システムに使用するもののですが、現在は使用されていません。

- **403 Forbidden**

クライアントは、コンテンツにアクセスする権限がありません。サーバーは、リクエストを拒否するための適切なレスポンスを送信します。 **401 Unauthorized**と異なる点は、サーバーがクライアントを認識していることです。

- **404 Not Found**

サーバーがリクエストしたリソースが見つかりません。ブラウザでは知られていないURLを意味します。APIでは、終点が適切ですが、リソースが存在しないことを示します。サーバーは、認証されていないクライアントからリソースを非表示にするために、このレスポンスを403の代わりに送信する場合があります。このレスポンスコードは、ウェブ上で最も広く知られています。

- **405 Method Not Allowed**

リクエストしたメソッドはサーバーで認識できますが、使用が禁止されています。例えば、特定のAPIでのリソースの削除が禁止されることがあります。必須メソッドであるGETとHEADは削除できず、このエラーコードを返すことはできません。

- **406 Not Acceptable**

サーバーからユーザーエージェントが指定した規格に適合するコンテンツを見つけられなかったときに、このレスポンスを送信します。

- **407 Proxy Authentication Required**

このレスポンスは、**401 Unauthorized**と似ていますが、プロキシ認証が必要であることを意味します。

- **408 Request Timeout**

サーバーがアイドル状態の接続を終了しようとしているときに、このレスポンスを送信します。Chrome、Firefox 27+、またはIE 9などのブラウザは、HTTP事前接続メカニズムを使用してこのレスポンスを受信できます。一部のサーバーは、このメッセージを送信せずに切断する場合があります。

- **409 Conflict**

リクエストが現在のサーバーのステータスと衝突したときにこのレスポンスを送信します。

- **410 Gone**

リクエストしたコンテンツがサーバーから永久に削除され、使用できなくなったときにこのレスポンスを送信します。クライアントは、キャッシュとリソースに対するリンクを削除する必要があります。

- **411 Length Required**

Content-Lengthヘッダーフィールドが定義されていないリクエストをサーバーが拒否します。

- **412 Precondition Failed**

クライアントのヘッダーにある前提条件がサーバーの前提条件と一致しない場合にこのレスポンスを送信します。

- **413 Payload Too Large**

リクエストエンティティがサーバーで定義した制限を超えています。サーバーは接続を切断するか、Retry-Afterヘッダーフィールドを含めてレスポンスできます。

- **414 URI Too Long**

クライアントがリクエストしたURIがサーバーで処理できる長さを超えています。

- **415 Unsupported Media Type**

リクエストしたメディア形式がサーバーで対応していないため、サーバーはそのリクエストを拒否します。

- **416 Requested Range Not Satisfiable**

Rangeヘッダーフィールドにリクエストした範囲を満たしません。リクエストした範囲が対象URIのデータサイズを超えている可能性があります。

- **417 Expectation Failed**

このレスポンスは、Expectリクエストヘッダフィールドの要件がサーバーで満たされていないときに送信されます。

- **418 I'm a teapot**

サーバーは、コーヒーをティーポットで沸騰させることを拒否します。HTCPCPプロトコルステータスコードの1つです。

- **421 Misdirected Request**

サーバーに誘導されたリクエストは、レスポンスを生成できません。これは、サーバがリクエストURIと接続されたスキームと権限を構成し、レスポンスを生成できないときに送信されます。

- **422 Unprocessable Entity (WebDAV)**

リクエストには異常はありませんが、文法上の誤りにより従うことはできません。

- **423 Locked (WebDAV)**

リクエストしたリソースがロックされているため、アクセスできません。

- **424 Failed Dependency (WebDAV)**

以前のリクエストが失敗したため、現在のリクエストも失敗しました。

- **426 Upgrade Required**

サーバーは現在プロトコルを使用してリクエストを処理しませんが、クライアントが他のプロトコルにアップグレードすると処理できます。サーバーは、必要なプロトコルをUpgrade ヘッダーに含めてレスポンスします。

- **428 Precondition Required**

サーバーはリクエストが条件的である必要があります。これは、クライアントがリソースをGETした後に修正し、PUTでサーバに戻す間、サードパーティによってサーバの状態が変更される'アップデート喪失'を防止するためです。

- **429 Too Many Requests**

ユーザーが指定された時間内にあまりにも多くのリクエストを送信したことを意味します。("rate limiting")

- **431 Request Header Fields Too Large**

リクエストしたヘッダーフィールドが大きすぎて、サーバーがリクエストを処理できません。リクエストを減らして再送信する必要があります。

- **451 Unavailable For Legal Reasons**

リクエストしたリソースが政府によって検閲されたウェブページなど、違法であることを示します。

5XX: Server error responses

- **500 Internal Server Error**

サーバーに問題がありますが、正確な問題を明確に説明できないことを意味します。

- **501 Not Implemented**

サーバーがリクエストを実行するために必要な機能に対応していないことを意味します。

- **502 Bad Gateway**

サーバーがゲートウェイからの誤ったレスポンスを受信したことを意味します。インターネット上のサーバーが他のサーバーから有効でないレスポンスを受けた場合に発生します。

- **503 Service Unavailable**

サーバーがリクエストを処理する準備ができていないことを意味します。これは、主にサーバーのメンテナンス中または過負荷がかかったときに発生します。このレスポンスとともにユーザーフレンドリーなページを提供する必要があり、可能な場合はRetry-Afterヘッダーにサービスの復旧予想時間を含める必要があります。

- **504 Gateway Timeout**

サーバーがゲートウェイとして機能し、適時にレスポンスを得られなかったことを意味します。これは主に、サーバー間のネットワークの問題が原因で発生します。

- **505 HTTP Version Not Supported**

これは、クライアントがサーバーで対応していないHTTPバージョンをリクエストしたことを意味します。ほとんどのウェブブラウザは、サーバーがHTTP 1.xバージョンに対応していると想定しています。最新バージョンのプロトコルを使用しないことは、セキュリティと性能上の理由で推奨されません。

- **506 Variant Also Negotiates**

サーバーに内部構成エラーが発生し、リクエストに対する透明なコンテンツ交渉が循環参照につながるときに発生します。

- **507 Insufficient Storage**

サーバーがリクエストを保存する十分なスペースを持っていない場合に発生します。これは主にWebDAVで発生します。

- **508 Loop Detected (WebDAV)**

サーバーがリクエストの処理中に無限ループを検出したときに発生します。

- **510 Not Extended**

サーバーがリクエストを実行するために追加の拡張が必要な場合に発生します。

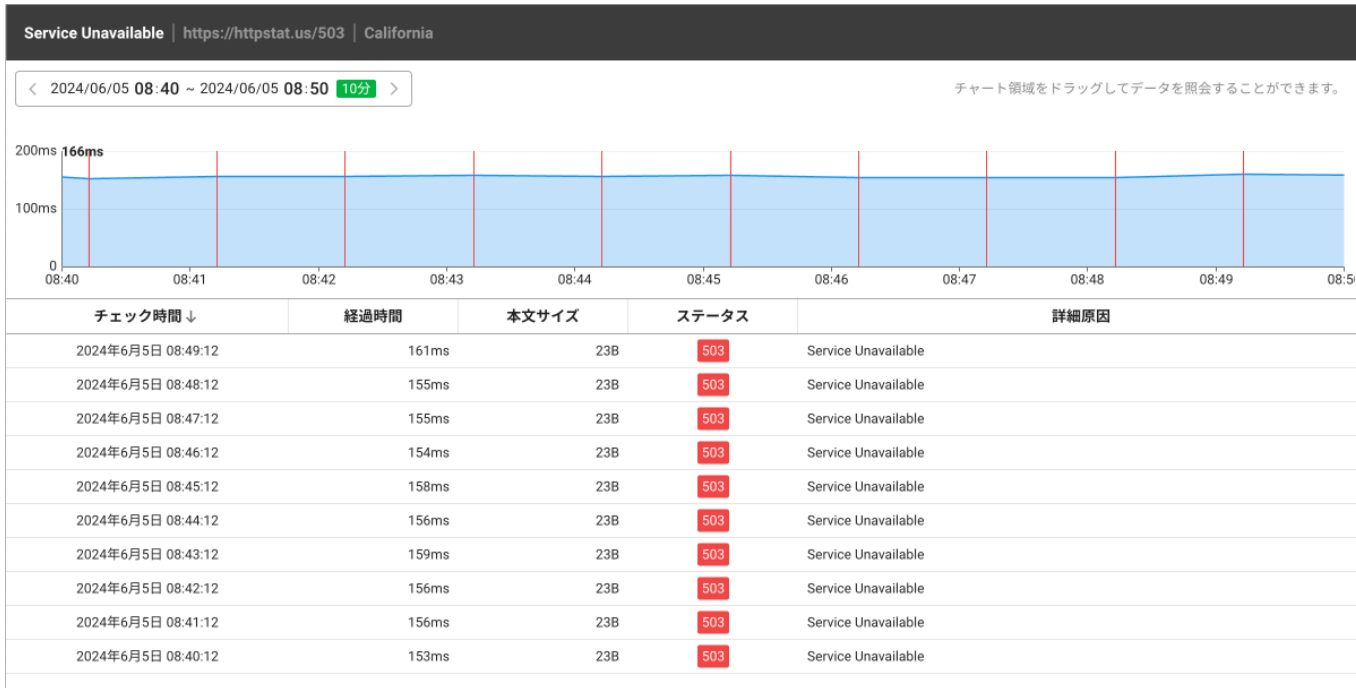
- **511 Network Authentication Required**

クライアントがネットワークにアクセスするために認証が必要であることを意味します。

エラータイプ

WhaTapのURLモニタリングを適用するときに発生する可能性のあるエラータイプとそのタイプによる設定方法について説明します。

URLモニタリング画面に表示されるチャート領域をドラッグすると、その時点でURLを呼び出したときに取得した結果データが画面下部に表示します。データの詳細原因に表示されたメッセージによる対処方法を案内します。



Invalid URL

誤ったURLを入力する場合に発生するメッセージです。

Unknown Host or URL

このホストまたはURLが見つからない場合に発生するメッセージです。プロトコルを正しく入力しているか、正しい

URL形式およびホストアドレスを入力しているかを確認してください。

Connect Time Out

誤ったURLに対する接続時間が超過して接続できないときに発生するメッセージです。サーバーへの接続の試行中に、最大所要時間の5秒以内に接続に失敗した場合に発生します。

Read Time Out

読み取り操作が指定された時間内に完了していないときに発生するメッセージです。サーバーからのデータ受信中に最大所要時間の10秒以内にレスポンスがない場合に発生します。

Unexpected end of file from server

エージェントとサーバーのエンコード値が異なる場合、またはパラメータに対するエンコード方法が異なる場合に発生するメッセージです。

Connection Refused

URL呼び出しのための接続自体がブロックされた場合に発生するメッセージです。エージェントから呼び出しが不可能な場合で、該当URL、またはサーバーのファイアウォールの確認が必要です。

- ウェブブラウザでURLを入力して接続に問題がないかチェックしてください。入力中にエラーが発生する場合があります。
- ファイアウォールおよび頻繁な呼び出しに対するIPのブロック履歴を確認し、モニタリングエージェントのIPに対するアクセスを許可してください。

No route to host

目的地に到達するためのパスが存在しない場合に発生するメッセージです。DNSから情報が見つからない場合と、その

URLに関する情報がない場合、またはアップデートされていない場合に発生します。次の項目を正確に入力したことを確認してください。

- ポート指定
- 入力URLのプロトコル

例、'htts://'と'https://'を間違えて入力した場合