

Kompira AlertHub 基本マニュアル

もくじ

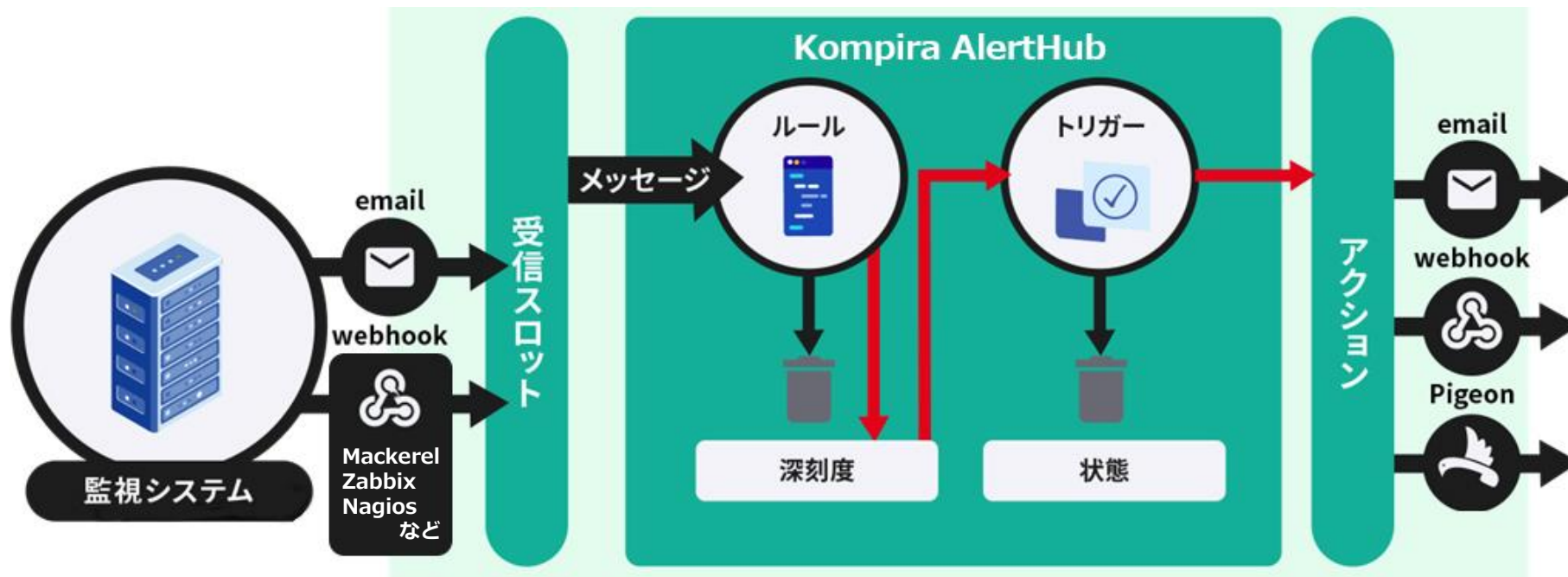
□ Kompira AlertHubとは	・・・	P.2	□ 作成の流れ：アクションの作成	・・・	P.20
□ 用語	・・・	P.4	□ 作成の流れ：トリガーの作成	・・・	P.21
□ 機能とはたらき	・・・	P.5	□ 事例の紹介	・・・	P.24
□ 機能とはたらき：受信スロット	・・・	P.6	□ 事例①：30分以内に10件以上のアラートが発生したらSlackに通知させたい	・・・	P.25
□ 機能とはたらき：スコープ	・・・	P.7	□ 事例②：ログ監視メールの復旧通知を不要にしたい	・・・	P.37
□ 機能とはたらき：静観スケジュール	・・・	P.8	□ Kompira AlertHubコミュニティ	・・・	P.49
□ 機能とはたらき：トリガー	・・・	P.9			
□ 機能とはたらき：ルール	・・・	P.10			
□ 機能とはたらき：イベント	・・・	P.11			
□ 機能とはたらき：アクション	・・・	P.12			
□ 作成の流れ：管理画面について	・・・	P.13			
□ 作成の流れ：受信スロットの作成	・・・	P.14			
□ 作成の流れ：スコープの作成	・・・	P.15			
□ 作成の流れ：ルールの作成	・・・	P.16			

Kompira AlertHubとは

監視アラートの判断業務を、簡単に自動化

一日の間に大量にアラートを受信しているけど、実際に確認が必要なのは、ほんの数件だけ…
メールのフィルターだと限界があるし、他のシステムでも通知が欲しいんだけどな…
そのようなことでお悩みではありませんか？

Kompira AlertHubは、Mackerel・Zabbix・Nagiosといった監視システムの結果を複合して判断する、アラートのフィルターのよう機能をするサービスです。



Kompira AlertHubとは

Kompira AlertHubで実現可能な集約例



夜間に自動で再起動しているため、0:00から01:00についてはアラート発生時のメール送信が不要



日中帯と夜間帯で、アラート発生をメール送信と電話と切替えて通知したい



30分以内に10件以上アラートが発生したらメール送信してほしい



アラート発生の初報のみメール送信してほしい



同種のアラート発生は、初報から1時間は通知が必要ない



異常が1分以内に回復したらアラート発生の通知が必要ない



アラートメッセージの中に「error」の文字列があったらメール送信が必要だが、「error.html」であれば送信は必要ない



複数のサーバから同時にアラートを受信した場合、システム単位で異常を通知したい

用語

Kompira AlertHub（以下、AlertHub）および本マニュアルで登場する用語について説明します。

用語	説明
アクション	メールやWebhookの送信、Pigeonで架電する動作
アラート	サーバ監視システムが異常状態や障害を検知した際に発する通知
トリガー	作成したアクションの実行条件、きっかけ
オペレータ	指定フィールドの値と数値の大小比較をどう行うかを選択できるセレクトボックス
フィールド	どの項目でアラートのフィルタリングを行うか指定する場所
ルール	監視システムから通知されるアラートのフィルタリング設定
ステータス	設定したフィルタリングの状態を、数値ごとに「正常」「警戒」「障害」といった項目で表したもの
スコープ	ルールやアクションの紐づけに必要な機能であり、ステータスの管理もおこなう
イベント	スコープの深刻度（障害の重要度を数値化したもの）が変化すること、またそのための機能
閾値(しきいち/いきち)	条件分岐の境目となる数値の区切り
受信(じゅしん)スロット	AlertHub内で設定する、アラートやメールの受け口
深刻度(しんこくど)	AlertHub内で任意に設定できる、障害の重要度を数値化したもの
静観(せいかん)スケジュール	アクションを実行させない時間（タイムテーブル）を定めることができる機能
正規表現（せいきひょうげん）	文字列内で文字の組み合わせを照合するために用いられるパターン
API	「Application Programming Interface」の略で、異なるプログラム同士が情報のやりとりを行う仕組み
JSON	「JavaScript Object Notation」の略で、JavaScriptの中でデータを簡単に表現するための書式 文字列・数値・配列・オブジェクトなどを表現できる
JSONパース	JSON形式を扱えるように分析し変換する処理のこと
Mackerel	サーバ監視システム（株式会社はてな運営）
Pigeon	電話自動化サービス、正式名称「Kompira Pigeon」（株式会社フィックスポイント（自社）運営）
Slack	ビジネスチャットツール（Slack Technology社運営）
Webhook	Webアプリケーションでイベントが実行された際、外部サービスにHTTPで通知する仕組み JSON形式を利用する
Zabbix	サーバ監視ソフトウェア（Zabbix社運営）

機能とはたらき

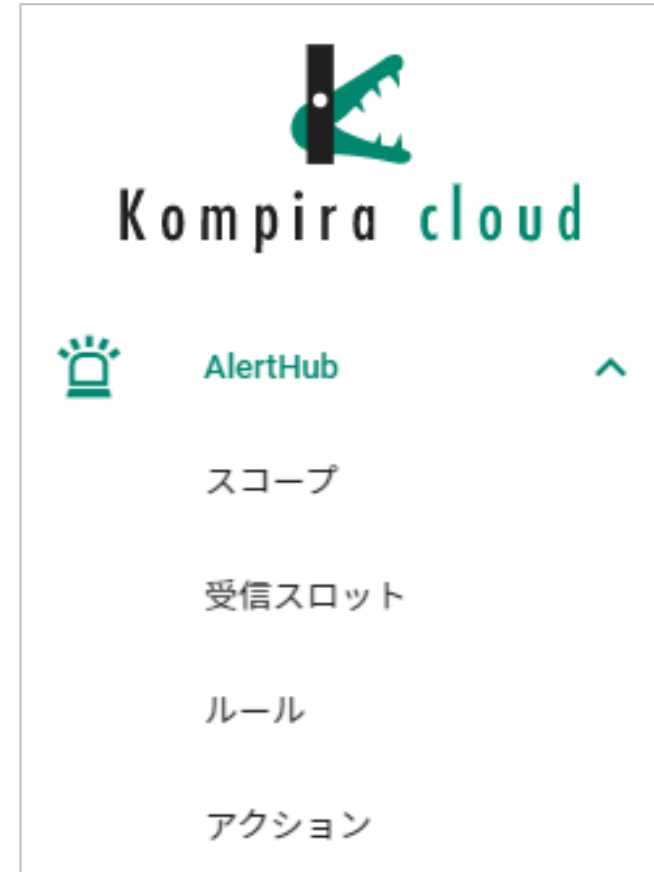
AlertHubの機能は設定順に、

- ・受信スロット
- ・スコープ
- ・ルール
- ・アクション
- ・トリガー

に分かれています。

これらが1セットとなっており、すべて作成することで
はじめてAlertHubが機能します。

それでは、はじめにそれぞれの機能について説明していきます。



※具体的な作成手順については、P.13からの「作成の流れ」の項目で説明します。



機能とはたらき

・受信スロットとは

メール・Webhookで送られてくるアラートの受け口となる場所です。

メールで例えると、受信ボックスのような存在です。

WebhookのURLやメールを受け取るメールアドレスを複数作成することができるため、システム別やサービス別に使い分けることが可能です。

受信スロット			+
表示名	種別	最終受信日	⚙️
test-Webhook	 Webhook		⋮
test-mail	 メール		⋮

機能とはたらき

・スコープとは

深刻度（障害の重要度を数値化したもの）を管理する機能です。

深刻度の変化によって「正常」「警戒」「障害」といったステータスを変化させたり、アラートの発生回数を捉えたりすることができます。

このスコープによって、ルールとアクションの紐づけを行います。

スコープ			+
12 正常	0 警戒	0 障害	
ステータス	表示名	深刻度	⚙️

機能とはたらき

・ 静観スケジュールとは

スコープ内の「設定」の項目から設定することができる機能です。

設定した時間にアクションを実行させたくないときに使用します。

静観スケジュールで設定した時間内においても、スコープの深刻度の変化は有効です。

The screenshot shows the 'Alerts - Trouble Test' interface. The top bar displays the alert ID '25F32304-F27D-451E-9CE5-30D077D06534' and the status '0 正常' (Normal) as of '2020/11/20 14:02'. The bottom navigation bar includes '概要' (Overview), 'ルール' (Rules), 'トリガー' (Triggers), and '設定' (Settings), with '設定' highlighted. Below the navigation bar, the '静観スケジュール' (Quiet Schedule) section is visible, with a '新規追加 +' (New Addition) button highlighted in a red box. An arrow points from this button to a modal dialog for adding a new quiet schedule. The dialog title is '業務時間内静観設定' (Business Hours Quiet Schedule). It includes fields for '開始' (Start) at '2020/11/25 08:00' and '終了' (End) at '2020/11/25 18:30'. A '繰り返し設定' (Repeat Setting) section is checked, with days '月' (Monday), '火' (Tuesday), '水' (Wednesday), '木' (Thursday), and '金' (Friday) selected. The dialog also features 'キャンセル' (Cancel) and '保存' (Save) buttons.

アラート_障害テスト

25F32304-F27D-451E-9CE5-30D077D06534

0
正常

2020/11/20 14:02
最終更新日

概要 ルール トリガー 設定

静観スケジュール

以下の静観スケジュールの期間内は、いかなるアクションも実行されません。

種別	表示名	開始	終了	繰り返し設定	
----	-----	----	----	--------	--

新規追加 +

毎週、月曜から金曜の8:00~18:30の間はアクションの実行を停止したい場合

表示名
業務時間内静観設定

開始
2020/11/25 08:00

終了
2020/11/25 18:30

繰り返し設定

月 火 水 木 金 土 日

キャンセル 保存

機能とはたらき

・トリガーとは

スコープ内の「トリガー」の項目から設定することのできる機能です。

スコープの深刻度やステータスの変化などによって、アクションを実行するかどうか判断します。アクションだけを設定しても、このトリガーがないと実行されないので注意が必要です。



状態	表示名	アクション	
✔ 有効	トリガー条件	障害発生_メール送信	⋮

1ページあたりの行数: 10 1-1 件目 / 1件 < >

機能とはたらき

・ルールとは

送られてくるアラートに対して、スコープの深刻度を変化させるかどうかの条件を指定する機能です。「受信スロット」「処理フロー」「イベント」の作成を行うことで設定が可能です。

アラート内の単語を条件に指定したり、様々な条件で柔軟に設定することができます。

ルール			
状態	表示名	受信スロット	
			<input type="radio"/> フィールド (F1) が数値 (N1) とオペレータ (O1) で一致したメッセージを許可する
			<input type="radio"/> フィールド (F1) が正規表現 (P1) とマッチした/マッチしなかったメッセージを許可する
			<input type="radio"/> フィールド (F1) が文字列 (S1) とオペレータ (O1) で一致したメッセージを許可する
			<input type="radio"/> フィールド (F1) が文字列 (S1) を含む/含まないメッセージを許可する
			<input type="radio"/> フィールド (F1) をJSONパースしてフィールド (F2) に保存する

機能とはたらき

・イベントとは

スコープの深刻度の変化を設定するために、スコープを選択した上で深刻度の変化量を設定する機能です。ルールで設定した条件に合うと、イベントが発生します。

🔗 イベント

[メール_障害テスト](#)

深刻度を

スコープの画面では、イベントの発生履歴が一覧表示されます。

イベント				
変化前の深刻度	深刻度	タイムスタンプ	eventId	⚙
2	0	2020/10/26 14:06	1ced7368-a879-49bd-ae77- 129e7ac5b698	
2	2	2020/10/26 14:01	18fdb624-8189-449a-9596- 447292641c64	
2	2	2020/10/26 13:55	6a6829b7-13a8-4614-a979- bd972548ed9e	
0	2	2020/10/26 13:52	18ab6a11-268e-4133-8ef3- 76c780a40d28	

1ページあたりの行数: 1-4 件目 / 4件 < >

機能とはたらき

・アクションとは

監視結果を通知する機能です。

- ・メール送信
- ・Pigeonを利用した電話発信
- ・Webhookを利用した外部APIの呼び出し

の3つの機能があります。

受信スロットに受信したアラート内容の本文・差出人等を変数で指定して記載し、送信することも可能です。

アクション			✉ メール	🐦 PIGEON	🔗 WEBHOOK
表示名	種別	最終実行日時	⚙️		

作成の流れ



管理画面にログイン後、

下記の流れの通り作成します。

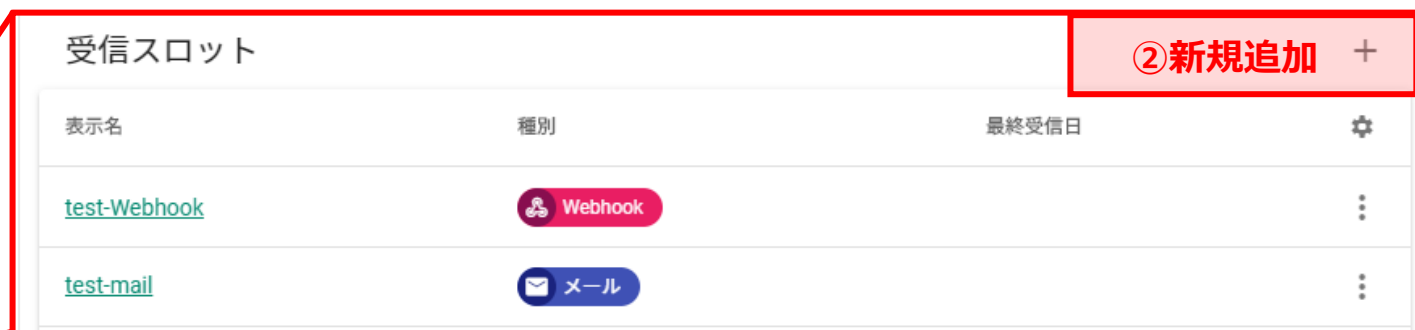
1. 受信スロットの作成
2. スコープの作成
3. ルールの作成
4. アクション作成
5. トリガー作成

作成の流れ

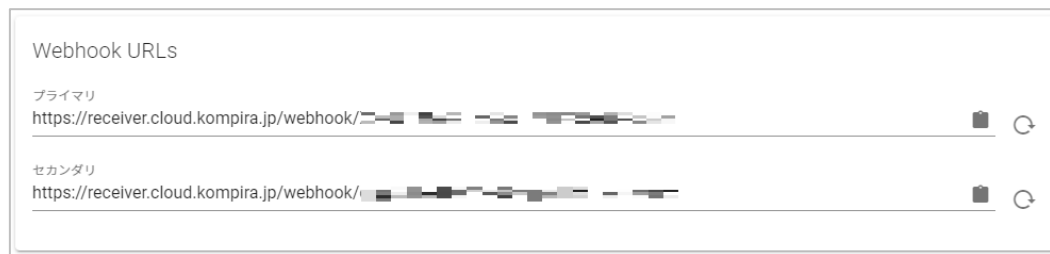
1.受信スロットの作成



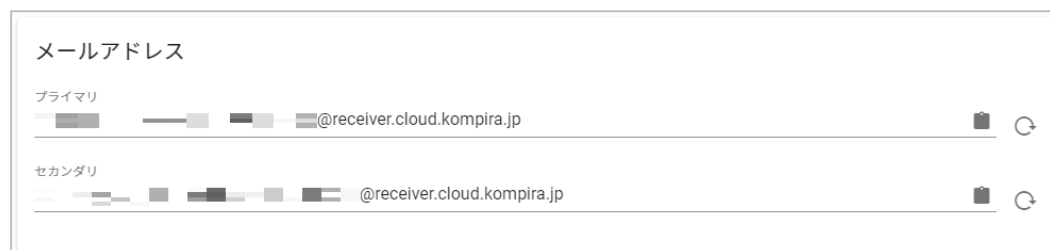
Webhook連携用のWebhook URLや、メールを受けるためのアドレスを発行します。
はじめにアラートやメールの受け口となる受信スロットを作成します。
「Webhook」ではURLが、「メール」はメールアドレスが作成されます。



・ Webhookで発行されたURL



・ メールで発行されたアドレス



他サービスとのWebhook連携については、各公式ページを参照ください。

Slack

<https://slack.com/intl/ja-jp/help/articles/115005265063-Slack-%E3%81%A7%E3%81%AE-Incoming-Webhook-%E3%81%AE%E5%88%A9%E7%94%A8>

Mackerel

<https://mackerel.io/ja/docs/entry/howto/alerts/webhook>

Zabbix

<https://www.zabbix.com/documentation/current/manual/config/notifications/media/webhook>

作成の流れ

2. スコープの作成

ルールやアクションの紐づけを行うスコープを作成します。

ルールとアクションの紐づけ以外に「正常」「警戒」「障害」の状態判定の設定も行えます。

Kompira cloud

AlertHub

① スコープ

受信スロット

ルール

アクション

Pigeon

Sonar

スコープ

② 新規追加 +

12 正常

0 警戒

0 障害

ステータス 表示名 深刻度

表示名 ③任意の名前を設定

障害判定閾値 5 ④警戒・障害判定閾値は1000まで指定することができます。

警戒判定閾値 3

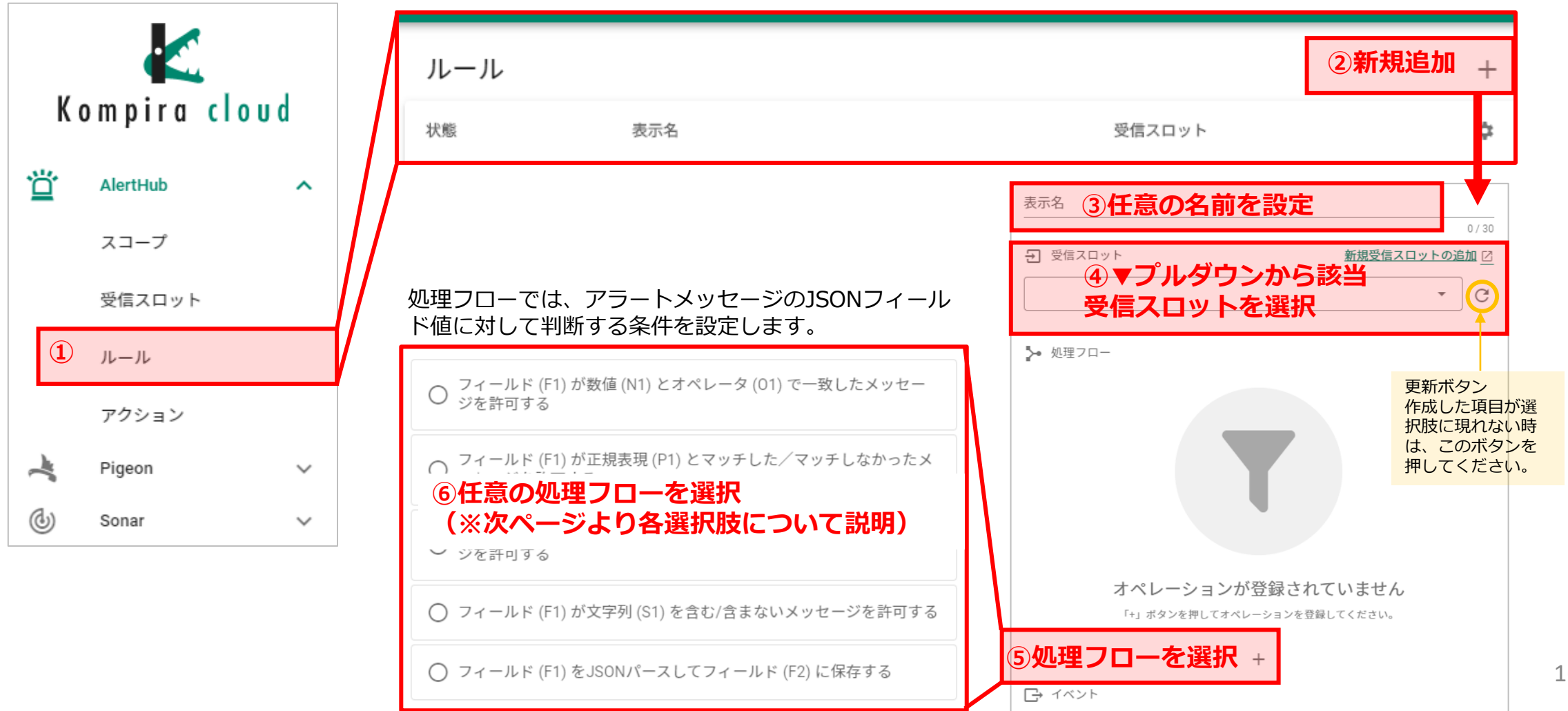
深刻度自動復旧の有効化 ⑤深刻度自動復旧を有効化すると、最後のイベント発生時から指定した時間が経過した後、深刻度を自動で0にします。(5分～24時間まで指定可能)

深刻度復旧時間 0 時間 5 分

作成の流れ

3. ルールの作成 (1/4)

アラートを判断するルールを設定を行います。



① ルール

② 新規追加 +

表示名 ③ 任意の名前を設定 0 / 30

受信スロット ④ ▼プルダウンから該当受信スロットを選択 新規受信スロットの追加

更新ボタン
作成した項目が選択肢に現れない時は、このボタンを押してください。

⑤ 処理フローを選択 +

⑥ 任意の処理フローを選択
(※次ページより各選択肢について説明)

オペレーションが登録されていません
「+」ボタンを押してオペレーションを登録してください。

処理フローでは、アラートメッセージのJSONフィールド値に対して判断する条件を設定します。

- フィールド (F1) が数値 (N1) とオペレータ (O1) で一致したメッセージを許可する
- フィールド (F1) が正規表現 (P1) とマッチした/マッチしなかったメッセージを許可する
- フィールド (F1) が文字列 (S1) を含む/含まないメッセージを許可する
- フィールド (F1) をJSONパースしてフィールド (F2) に保存する

作成の流れ

3. ルールの作成 (2/4) 各処理フローの説明です。先にこの項目を取り扱います。

- フィールド (F1) が数値 (N1) とオペレータ (O1) で一致したメッセージを許可する
- フィールド (F1) が正規表現 (P1) とマッチした/マッチしなかったメッセージを許可する
- フィールド (F1) が文字列 (S1) とオペレータ (O1) で一致したメッセージを許可する
- フィールド (F1) **この処理フローを選択した場合**
- フィールド (F1) をJSONパースしてフィールド (F2) に保存する

処理フロー

もし **F1** が **S1** を包含 **選択してください** 場合

1 どの項目の判定をしたいかで入力する値を決定

・メールの場合

項目	入力内容
件名	message.content.subject
本文 (テキスト形式)	message.content.text
本文 (HTML形式)	message.content.html
差出人の名前	message.metadata.from.name
差出人のメールアドレス	message.metadata.from.email

・Webhookの場合

※参照：P.42「事例②> ルールの作成 (2/3)」

2 キーにする単語などを指定

例) メール本文に「error」と表示があることをフィルタリングの条件とした場合は「error」を指定。

3 包含「した」か「しなかった」を選択

2 の条件の例)

▼「error」という表記がある場合のアラートした を選択。

▼「error」という表記がない場合のアラートしなかった を選択。

選択してください 場合

選択してください

した

しなかった

作成の流れ

3. ルールの作成 (3/4) 各処理フローの説明です。場合により使い分けます。

数値で一致させている場合

- フィールド (F1) が数値 (N1) とオペレータ (O1) で一致したメッセージを許可する
- フィールド (F1) が正規表現 (P1) とマッチした/マッチしなかったメッセージを許可する
- フィールド (F1) が文字列 (S1) とオペレータ (O1) で一致したメッセージを許可する
- フィールド (F1) が文字列 (S1) を含む/含まないメッセージを許可する
- フィールド (F1) をJSONパースしてフィールド (F2) に保存する

もし **1** F1 が **2** N1 **3** 選択してください 場合

コメント

1 入力項目 (メールの場合)

項目	入力内容
件名	message.content.subject
本文 (テキスト形式)	message.content.text
本文 (HTML形式)	message.content.html
差出人の名前	message.metadata.from.name
差出人のメールアドレス	message.metadata.from.email

2 任意の数値を設定

3 ▼プルダウンから比較を選択

2で指定した数値との大小比較をどう行うか選択する。

「ALL OK」等の文字列が一致しない場合

- フィールド (F1) が数値 (N1) とオペレータ (O1) で一致したメッセージを許可する
- フィールド (F1) が正規表現 (P1) とマッチした/マッチしなかったメッセージを許可する
- フィールド (F1) が文字列 (S1) とオペレータ (O1) で一致したメッセージを許可する
- フィールド (F1) が文字列 (S1) を含む/含まないメッセージを許可する
- フィールド (F1) をJSONパースしてフィールド (F2) に保存する

もし **1** F1 が **2** S1 **3** 選択してください 場合

コメント

1 入力項目 (メールの場合)

項目	入力内容
件名	message.content.subject
本文 (テキスト形式)	message.content.text
本文 (HTML形式)	message.content.html
差出人の名前	message.metadata.from.name
差出人のメールアドレス	message.metadata.from.email

2 設定したい文字列を設定「ALL OK」

3 「等しい」か「等しくない」かを選択 例の場合は「等しくない」を選択。

「Error」「ERROR」等、どちらかがマッチしたらという場合

- フィールド (F1) が数値 (N1) とオペレータ (O1) で一致したメッセージを許可する
- フィールド (F1) が正規表現 (P1) とマッチした/マッチしなかったメッセージを許可する
- フィールド (F1) が文字列 (S1) とオペレータ (O1) で一致したメッセージを許可する
- フィールド (F1) が文字列 (S1) を含む/含まないメッセージを許可する
- フィールド (F1) をJSONパースしてフィールド (F2) に保存する

もし **1** F1 が **2** P1 **3** とマッチ 選択してください 場合

コメント

1 入力項目 (メールの場合)

項目	入力内容
件名	message.content.subject
本文 (テキスト形式)	message.content.text
本文 (HTML形式)	message.content.html
差出人の名前	message.metadata.from.name
差出人のメールアドレス	message.metadata.from.email

2 設定したい文字列を、正規表現で設定「E (rror|RROR)」

3 マッチ「した」か「しなかった」を選択 例の場合はマッチ「した」を選択する。

メール受信でも構造化データを取り扱う場合

- フィールド (F1) が数値 (N1) とオペレータ (O1) で一致したメッセージを許可する
- フィールド (F1) が正規表現 (P1) とマッチした/マッチしなかったメッセージを許可する
- フィールド (F1) が文字列 (S1) とオペレータ (O1) で一致したメッセージを許可する
- フィールド (F1) が文字列 (S1) を含む/含まないメッセージを許可する
- フィールド (F1) をJSONパースしてフィールド (F2) に保存する

1 F1 をJSONパースして **2** F2 に保存する

コメント

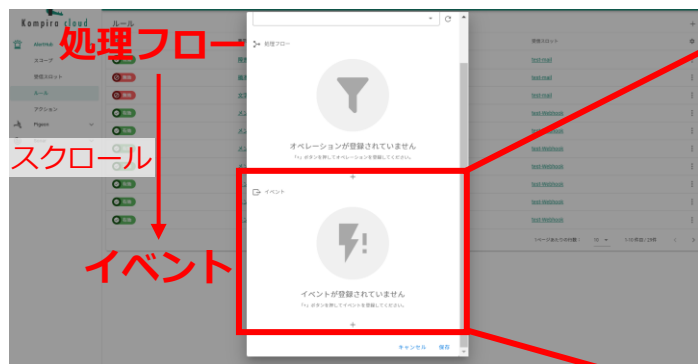
1 2 入力項目 (メールの場合)

項目	入力内容
件名	message.content.subject
本文 (テキスト形式)	message.content.text
本文 (HTML形式)	message.content.html
差出人の名前	message.metadata.from.name
差出人のメールアドレス	message.metadata.from.email

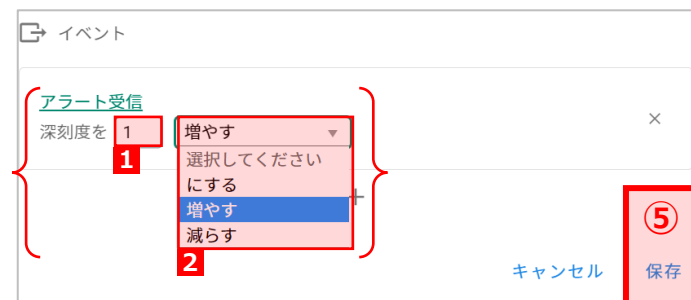
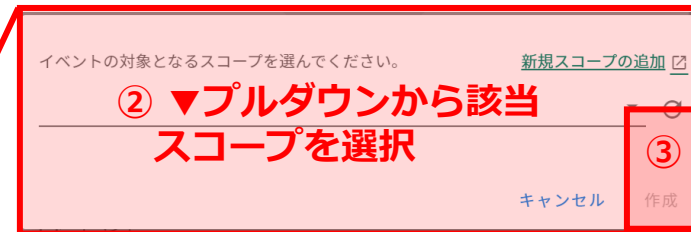
JSONパースに関しては主にメール本文に使用します。メール受信の場合はそういったJSONデータを扱う手段がありませんが、システムによってはWebhook送信に対応しておらずメールのみを送れる、というケースがあるので、本文をJSON形式で送りJSONパースする形を取ることで、メールでも構造化データを取り扱えます。

作成の流れ

3. ルールの作成 (4/4)



イベントでは、スコープの深刻度の変化を設定するために、スコープを選択した上で深刻度の変化量を指定します。



1 深刻度の設定

スコープの作成 (P.15) の「障害判定閾値」「警戒判定閾値」に合わせて、任意の数値を設定してください。

例) メール件数をカウントアップ/ダウンしたい場合は「1」に設定。

2 深刻度の数値の増減を選択

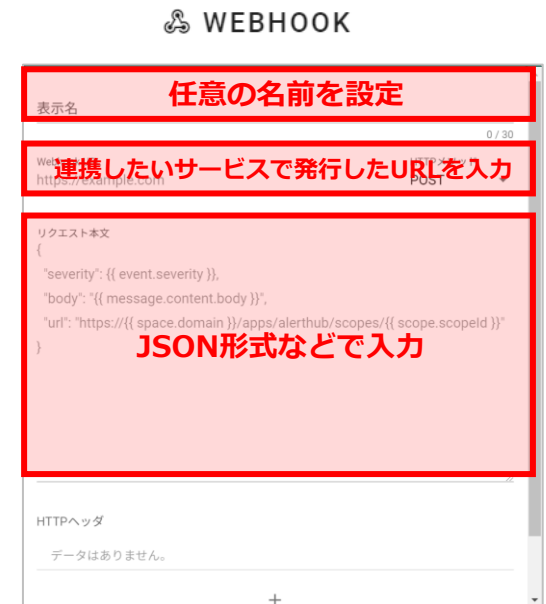
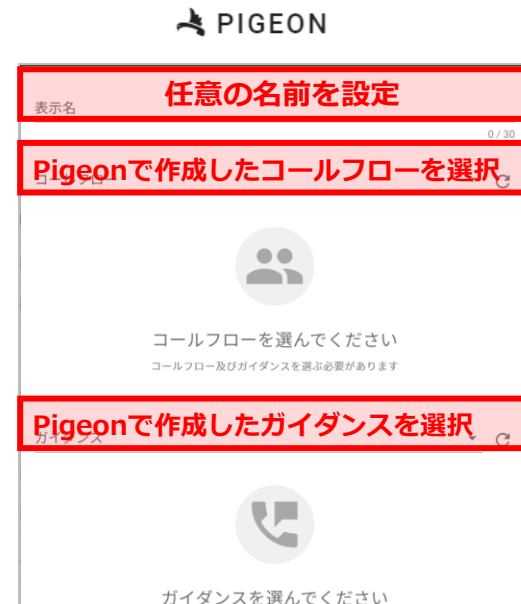
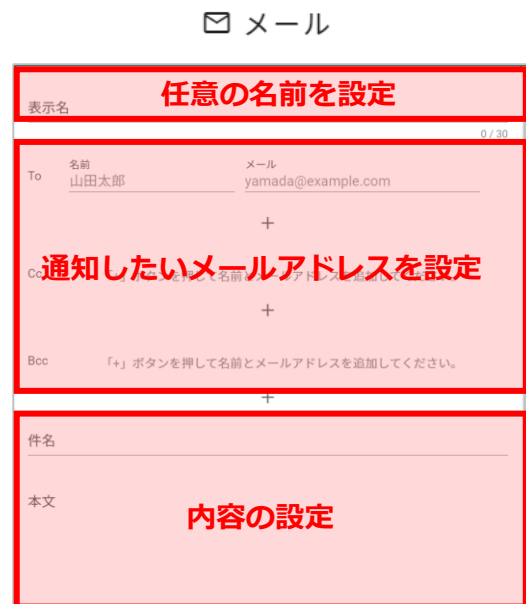
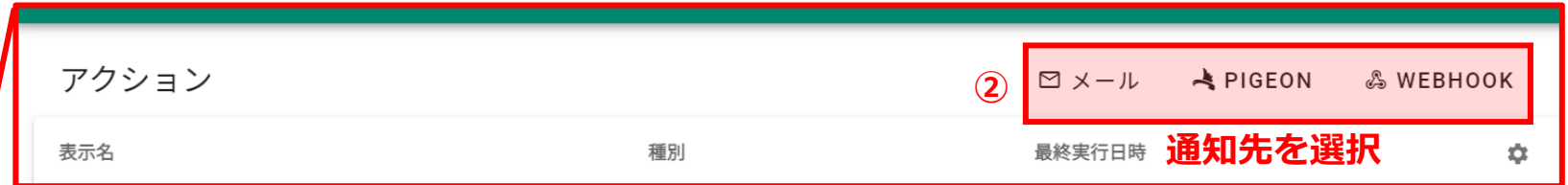
1 の例) の場合

- ・メール件数によって「正常」→「警戒」→「障害」にスコープステータスを変更させる場合 増やす を選択。
- ・メール件数によって「障害」→「警戒」→「正常」にスコープステータスを変更させる場合 減らす を選択。
- ・メール件数に関わらず「正常」として認識させる場合 にする を選択。

作成の流れ

4.アクションの作成

アラート通知の集約後に実行する設定を行います。



※別途、Pigeon側の設定が必要です。

作成の流れ

5.トリガーの作成 (1/3)

アクションの実行条件を設定します。

ステータス	表示名	深刻度
正常	メール_障害テスト	0
正常	スコープ	0
正常	マニュアル用テスト	0

トリガー

② トリガー

③ 新規追加 +

○ 過去 (T1) 秒間にアクションが発火した回数が数値 (N1) とオペレータ (O1) で一致することを必要とする

○ 過去 (T1) 秒間にイベントのフィールド (Y1) が数値 (N1) とオペレータ (O1) で一致するイベントの回数が数値 (N2) とオペレータ (O2) で一致することを必要とする

○ (T1) 秒経過後、イベントのフィールド (Y1) が数値 (N1) とオペレータ (O1) で一致することを必要とする

**次ページにて
各実行条件の詳細説明**

○ (T1) 秒経過後、スコープステータスが文字列 (S1) と等しい/等しくない (O1) ことを必要とする

○ スコープステータスが文字列 (S1) と等しい/等しくない (O1) ことを必要とする

表示名 ④ 任意の名前を設定

実行条件

オペレーションが登録されていません

「+」ボタンを押してオペレーションを登録してください。

⑤ 実行条件を選択 +

⑥ ▼プルダウンから該当アクションを選択

作成の流れ

5. トリガーの作成 (2/3) 各実行条件の説明です。先にこの2つをご紹介します。

過去 (T1) 秒間にアクションが発火した回数が数値 (N1) とオペレータ (O1) で一致することを必要とする

この実行条件を選択した場合

(T1) 秒経過後、イベントのフィールド (Y1) が数値 (N1) とオペレータ (O1) で一致することを必要とする

イベントのフィールド (Y1) が数値 (N1) とオペレータ (O1) で一致することを必要とする

(T1) 秒経過後、スコープステータスが文字列 (S1) と等しい/等しくない (O1) ことを必要とする

スコープステータスが文字列 (S1) と等しい/等しくない (O1) ことを必要とする

過去 T1 秒間に **1** 選択してください **2** が N1 **3** **4** 発生した イベントが N2 **5** **6** 選択してください

コメント

こんなときに使用します)

過去30分の間に10件以上のアラートを受信したときに通知させたい場合に使用。

1 任意の数値 (秒) を設定

2 深刻度の基準を▼プルダウンから選択

選択してください ▼

- 選択してください
- 深刻度
- 変化前の深刻度
- 深刻度の変化量

3 任意の数値を設定

4 ▼プルダウンから選択

選択してください ▼

- 選択してください
- と等しい
- と等しくない
- より大きい
- 以上の
- 以下の
- より小さい

5 任意の数値を設定

6 ▼プルダウンから選択

選択してください ▼

- 選択してください
- と等しい
- と等しくない
- より大きい
- 以上の
- 以下の
- より小さい

過去 (T1) 秒間にアクションが発火した回数が数値 (N1) とオペレータ (O1) で一致することを必要とする

過去 (T1) 秒間にイベントのフィールド (Y1) が数値 (N1) とオペレータ (O1) で一致するイベントの回数が数値 (N2) とオペレータ (O2) で一致することを必要とする

(T1) 秒経過後、イベントのフィールド (Y1) が数値 (N1) とオペレータ (O1) で一致することを必要とする

イベントのフィールド (Y1) が数値 (N1) とオペレータ (O1) で一致することを必要とする

(T1) 秒経過後、スコープステータスが文字列 (S1) と等しい/等しくない (O1) ことを必要とする

この実行条件を選択した場合

1 スコープステータスが **2** 選択してください

コメント

こんなときに使用します)

スコープステータスが警戒になったら通知させたい場合に使用。

1 ステータスを▼プルダウンから選択

選択してください ▼

- 選択してください
- 正常
- 警戒
- 障害

2 ▼プルダウンから選択

選択してください ▼

- 選択してください
- と等しい
- と等しくない

作成の流れ

5. トリガーの作成 (3/3) 各実行条件の説明です。各実行条件に応じてSlack等に通知させます。

過去n秒以内にm回アクションが発生したら通知させたい場合

- 過去 (T1) 秒間にアクションが発火した回数が数値 (N1) とオペレータ (O1) で一致することを必要とする
- 過去 (T1) 秒間にイベントのフィールド (Y1) が数値 (N1) とオペレータ (O1) で一致するイベントの回数が数値 (N2) とオペレータ (O2) で一致することを必要とする
- (T1) 秒経過後、イベントのフィールド (Y1) が数値 (N1) とオペレータ (O1) で一致することを必要とする
- イベントのフィールド (Y1) が数値 (N1) とオペレータ (O1) で一致することを必要とする
- (T1) 秒経過後、スコープステータスが文字列 (S1) と等しい/等しくない (O1) ことを必要とする
- スコープステータスが文字列 (S1) と等しい/等しくない (O1) ことを必要とする

過去 (T1) 秒間に、アクションが N1 回発生しました。選択してください

- 1 任意の数値を設定
時間 (秒) を設定。
- 2 任意の数値を設定
- 3 ▼プルダウンから比較を選択
2 で指定した数値との大小比較を
どう行うかを選択する。

イベント発生n秒経過後に深刻度の変化量によって通知させたい場合

- 過去 (T1) 秒間にアクションが発火した回数が数値 (N1) とオペレータ (O1) で一致することを必要とする
- (T1) 秒経過後、イベントのフィールド (Y1) が数値 (N1) とオペレータ (O1) で一致することを必要とする
- イベントのフィールド (Y1) が数値 (N1) とオペレータ (O1) で一致することを必要とする
- (T1) 秒経過後、スコープステータスが文字列 (S1) と等しい/等しくない (O1) ことを必要とする
- スコープステータスが文字列 (S1) と等しい/等しくない (O1) ことを必要とする

T1 秒経過後、選択してください が N1 値である

- 1 任意の数値を設定
- 2 ▼プルダウンから比較を選択
- 3 任意の数値を設定
- 4 ▼プルダウンから比較を選択

時間経過に関係なく深刻度によって通知させたい場合

- 過去 (T1) 秒間にアクションが発火した回数が数値 (N1) とオペレータ (O1) で一致することを必要とする
- 過去 (T1) 秒間にイベントのフィールド (Y1) が数値 (N1) とオペレータ (O1) で一致するイベントの回数が数値 (N2) とオペレータ (O2) で一致することを必要とする
- (T1) 秒経過後、イベントのフィールド (Y1) が数値 (N1) とオペレータ (O1) で一致することを必要とする
- イベントのフィールド (Y1) が数値 (N1) とオペレータ (O1) で一致することを必要とする
- (T1) 秒経過後、スコープステータスが文字列 (S1) と等しい/等しくない (O1) ことを必要とする
- スコープステータスが文字列 (S1) と等しい/等しくない (O1) ことを必要とする

選択してください が N1 選択してください 値である

- 1 ▼プルダウンから比較を選択
- 2 任意の数値を設定
- 3 ▼プルダウンから比較を選択

n秒経過後にスコープステータスが [正常/警戒/障害] だったら通知させたい場合

- 過去 (T1) 秒間にアクションが発火した回数が数値 (N1) とオペレータ (O1) で一致することを必要とする
- 過去 (T1) 秒間にイベントのフィールド (Y1) が数値 (N1) とオペレータ (O1) で一致するイベントの回数が数値 (N2) とオペレータ (O2) で一致することを必要とする
- (T1) 秒経過後、イベントのフィールド (Y1) が数値 (N1) とオペレータ (O1) で一致することを必要とする
- (T1) 秒経過後、スコープステータスが文字列 (S1) と等しい/等しくない (O1) ことを必要とする
- スコープステータスが文字列 (S1) と等しい/等しくない (O1) ことを必要とする

T1 秒経過後、スコープステータスが 選択してください

- 1 任意の数値を設定
- 2 ▼プルダウンから比較を選択
- 3 ▼プルダウンから比較を選択

事例の紹介

以上が基本的な流れです。

続いて、事例に沿った設定方法をご紹介します。

事例①

30分以内に10件以上のアラートが発生したらSlackに通知する

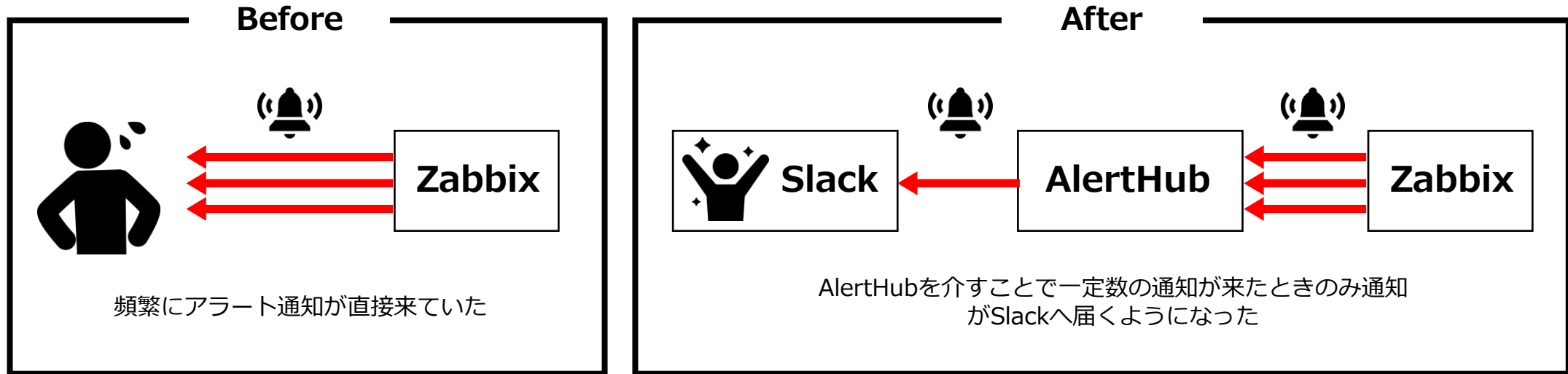
事例②

ログ監視の不要な復旧通知を送信しない

事例①

30分以内に10件以上のアラートが発生したらSlackに通知する

事例① 30分以内に10件以上のアラートが発生したらSlackに通知する



事例① 30分以内に10件以上のアラートが発生したらSlackに通知する

解決したいこと：

一日の間にZabbixから大量にアラートメッセージを受信しているため、確認作業に多く時間を取られてしまっている。

⇒一定数メッセージを受信したときのみSlackに通知させたい。

受信スロットの作成 (1/2)

Kompira cloud

受信スロット

表示名	種別
アラート受信スロット	Webhook
受信スロット	メール

種別 Webhook

表示名 任意の表示名を設定

0 / 30

①メニューから受信スロットを選択

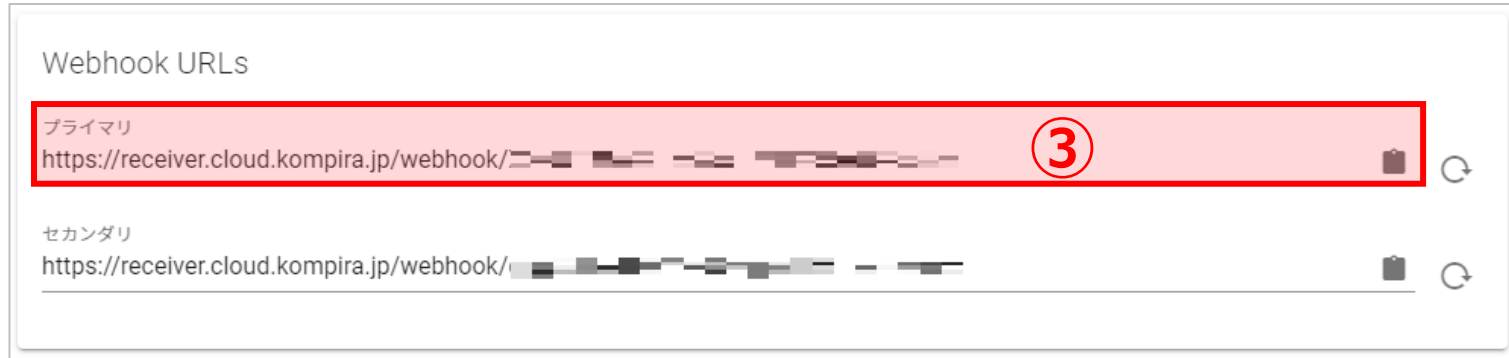
②受信スロットの新規作成

受信スロットの新規作成画面から種別「Webhook」を選択。

表示名はわかりやすい任意の表示名を設定してください。
今回は「アラート受信スロット」にしています。

事例① 30分以内に10件以上のアラートが発生したらSlackに通知する

受信スロットの作成 (2/2)



③ Webhook用URLの発行

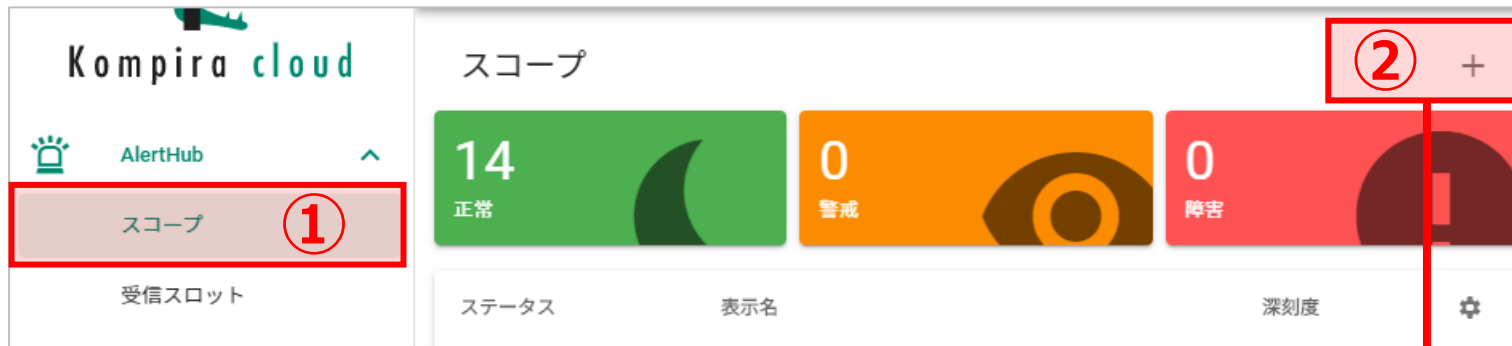
Zabbixと連携するためのURLを発行します。
下記を参考に設定してください。

※ Zabbix連携方法

<https://www.zabbix.com/documentation/current/manual/config/notifications/media/webhook>

事例① 30分以内に10件以上のアラートが発生したらSlackに通知する

スコープの作成



任意の表示名を設定

表示名
アラート_障害テスト

障害判定閾値 (3)
10

警戒判定閾値 (4)
5

深刻度自動復旧の有効化 (5)
深刻度復旧時間
0 時間 5 分

①メニューからスコープを選択

②スコープの新規作成

③障害判定閾値の設定

障害判定の数値によってスコープの警戒が1表示（赤い部分）されます。任意の数値に設定してください。

④警戒判定閾値の設定

警戒判定の数値によってスコープの警戒が1表示（黄色い部分）されます。任意の数値に設定してください。

⑤深刻度自動復旧の有効化

深刻度自動復旧の有効化にチェックを入れると、指定した時間が経過後に警戒・障害の表示を0に戻します。こちらも任意の時間を設定してください。

事例① 30分以内に10件以上のアラートが発生したらSlackに通知する

ルールの作成 (1/2)

The screenshot shows the Kompira cloud AlertHub interface. On the left, a sidebar menu has 'ルール' (Rules) highlighted with a red box and a circled '1'. The main area shows a table of rules. A red box with a circled '2' and a '+' sign is positioned above the table. A red arrow points from this box to a new rule entry. This entry has a red box around its '表示名' (Display Name) field containing 'アラートルール' (Alert Rule), with a red box and circled '3' around it. A red text box with the text '任意の表示名を設定' (Set an arbitrary display name) is overlaid on this field. Below the table, a dropdown menu for '受信スロット' (Receiving Slot) is shown with 'アラート受信スロット' (Alert Receiving Slot) selected, also with a red box and circled '3' around it. The '処理フロー' (Processing Flow) section below is empty, showing a message: 'オペレーションが登録されていません' (No operations are registered) and a '+ ' button.

状態	表示名	受信スロット	
有効	アラート受信ルール	アラート受信スロット	⋮
有効	マニュアル用テスト	test-Webhook	⋮
有効	アラートルール	アラート受信スロット	⋮

①メニューからルールを選択

②ルールの新規作成

③作成した(該当の)受信スロットを選択

処理フローの設定は不要です。

事例① 30分以内に10件以上のアラートが発生したらSlackに通知する

ルールの作成 (2/2)

The screenshot shows a configuration window for an event named 'アラート_障害テスト' (Alert Test). Below the event name, there is a field for '深刻度を' (Severity) with the value '1' and a dropdown menu currently set to '増やす' (Increase). A red box highlights the dropdown menu, and a red circle with the number '4' is placed next to it. A callout box points to the dropdown menu, showing a list of options: '増やす' (Increase), '選択してください' (Please select), 'にする' (Set to), '増やす' (Increase), and '減らす' (Decrease). The '増やす' option is highlighted in blue.

④ イベントを追加

▼プルダウンから作成したスコープを選択します。
今回は「アラート_障害テスト」を選択。

深刻度について

今回は深刻度を利用してメール件数のカウントを行いたいので、1件の受信につき深刻度を1増やす、というルールを設定します。

※参照：

PP.16-19 「作成の流れ>ルールの作成」

事例① 30分以内に10件以上のアラートが発生したらSlackに通知する

アクションの作成

アクション

表示名	種別	最終実行日時
slack宛	Webhook	2020/11/19 17:48

表示名
slack宛

任意の表示名を設定

Webhook URL
https://hooks.slack.com/services/...

Slackにて発行したURLを入力

リクエスト本文

```
{
  "text": "
【 】 \n
【ステータス】 {{message.content.data.alert.status}}\n
【モニターネーム】 {{message.content.data.alert.monitorName}}\n
【URL】 {{message.content.data.alert.url}}\n
【ホスト】 {{message.content.data.host.name}}
}
```

①メニューからアクションを選択

②アクションの新規作成

今回はSlackへ通知させたいのでWebhookを選択しアクションの新規作成を行います。

③Webhook用URLを入力

Slackと連携するためのURLを入力します。下記を参考に設定してください。

<https://slack.com/intl/ja-jp/help/articles/115005265063-Slack-%E3%81%A7%E3%81%AE-Incoming-Webhook-%E3%81%AE%E5%88%A9%E7%94%A8>

④設定内容

リクエスト本文はJSON形式で記載をします。

受信したアラート内容の差出人や件名等の項目を指定して送ることができます。

事例① 30分以内に10件以上のアラートが発生したらSlackに通知する

トリガーの作成 (1/3)

Kompira cloud

AlertHub

スコープ

受信スロット

ルール

スコープ

14 正常

0 警戒

ステータス

表示名

メール_障害テスト

正常

アラート_障害テスト

25F32304-F27D-451E-9CE5-30D077D06534

0 正常

2020/11/20 11:36 最終更新日

概要

ルール

トリガー

設定

トリガー

状態

表示名

アクション

①メニューからスコープを選択

②作成したスコープを選択

③トリガーを選択

④トリガーの新規作成

事例① 30分以内に10件以上のアラートが発生したらSlackに通知する

トリガーの作成 (2/3)

トリガー

状態	表示名	アクション
	トリガー条件	

任意の表示名を設定

実行条件

過去 1800 秒間に 深刻度の変化量 が 1
と等しい イベントが 10 以上の
回数発生した

コメント

↓ 今回の設定では下記を選択

- 過去 (T1) 秒間にアクションが発火した回数が数値 (N1) とオペレータ (O1) で一致することを必要とする
- 過去 (T1) 秒間にイベントのフィールド (Y1) が数値 (N1) とオペレータ (O1) で一致するイベントの回数が数値 (N2) とオペレータ (O2) で一致することを必要とする
- (T1) 秒経過後、イベントのフィールド (Y1) が数値 (N1) とオペレータ (O1) で一致することを必要とする
- イベントのフィールド (Y1) が数値 (N1) とオペレータ (O1) で一致することを必要とする
- (T1) 秒経過後、スコープステータスが文字列 (S1) と等しい/等しくない (O1) ことを必要とする
- スコープステータスが文字列 (S1) と等しい/等しくない (O1) ことを必要とする

⑤ 実行条件の設定内容

「過去 (T1) 秒間にイベントのフィールド (Y1) が数値 (N1) とオペレータ (O1) で一致するイベントの回数が数値 (N2) とオペレータ (O2) で一致することが必要とする」を選択。

30分以内に10件以上のアラートが発生したら通知が必要なので

T1 = 「1800」秒
30分を秒数で設定

Y1/N1/O1 = 深刻度の変化量が1と等しい
ルールの設定で行った深刻度

メール 障害テスト

深刻度を 1 増やす

N2/O2 = 10以上
10件以上のアラート

と設定します。

事例① 30分以内に10件以上のアラートが発生したらSlackに通知する

トリガーの作成 (3/3)

アクション [新規アクションの追加](#)

障害発生_メール送信 ⑥

⑥作成したアクションを選択
「障害発生_メール送信」を選択。

事例① 30分以内に10件以上のアラートが発生したらSlackに通知する

アラート受信後の画面

The screenshot shows the Kompira cloud AlertHub interface. A red banner at the top indicates a critical state: "10 障害 Zabbixからのアラート通知が10件以上発生している状態 = スコープステータスが障害". Below this, there are tabs for "正常" (Normal, < 5), "警戒" (Warning, 5 ~ 10), and "障害" (Incident, 10 <). The "障害" tab is active. Two tables are visible: "イベント" (Events) and "アクション" (Actions).

イベント	アクション
変化前の深刻度	アクション
深刻度	タイムスタンプ
タイムスタンプ	actionId
eventId	actionRecordId
9	slack宛
10	2020/10/19 16:40
2020/10/19 16:40	339c7218-a9f2-4723-bade-c80d6033c841
8	5d6a0fcd-2cfd-42f2-9fe3-c223924e643c
9	
2020/10/19 16:39	
8	
2020/10/19 16:38	
7	
2020/10/19 16:38	
5	
2020/10/19 16:38	
8101-76e0a892adf5	
2020/10/19 16:38	
4823980a-0a05-4b1a-	

Zabbixから受け取ったアラートがイベント欄に表示されます

実際にSlackへ送信された通知がアクション欄に表示されます

Slackで受け取った通知

The screenshot shows a Slack message received from an incoming webhook. The message content is as follows:

Incoming Webhook #279 14:04

【ステータス】

【モニターネーム】

【URL】

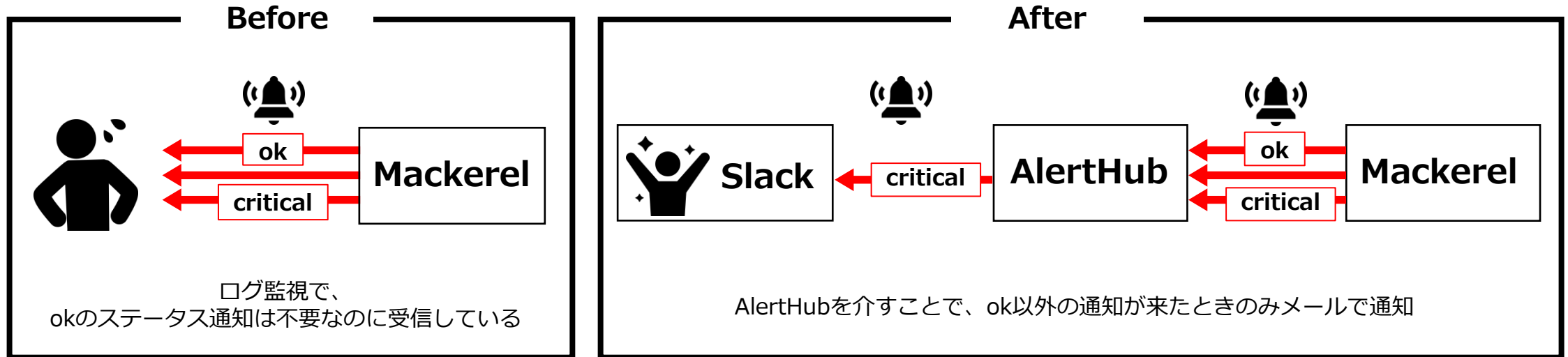
【ホスト】

【IPアドレス】

事例②

ログ監視の不要な復旧通知を送信しない

事例② ログ監視の不要な復旧通知を送信しない



事例② ログ監視の不要な復旧通知を送信しない

解決したいこと：

Mackerelからログ監視の通知メッセージを受信しているが、「OK」のステータスの通知メール（復旧通知）はいらない。

⇒ 「OK」以外の通知メールのみを受信したい。

受信スロットの作成 (1/2)

Kompira cloud

AlertHub

スコープ

受信スロット ①

受信スロット

表示名	種別	
アラート受信スロット	Webhook	⋮
受信スロット	メール	⋮

② +

種別 Webhook

表示名 任意の表示名を設定

0 / 30

メール

Webhook

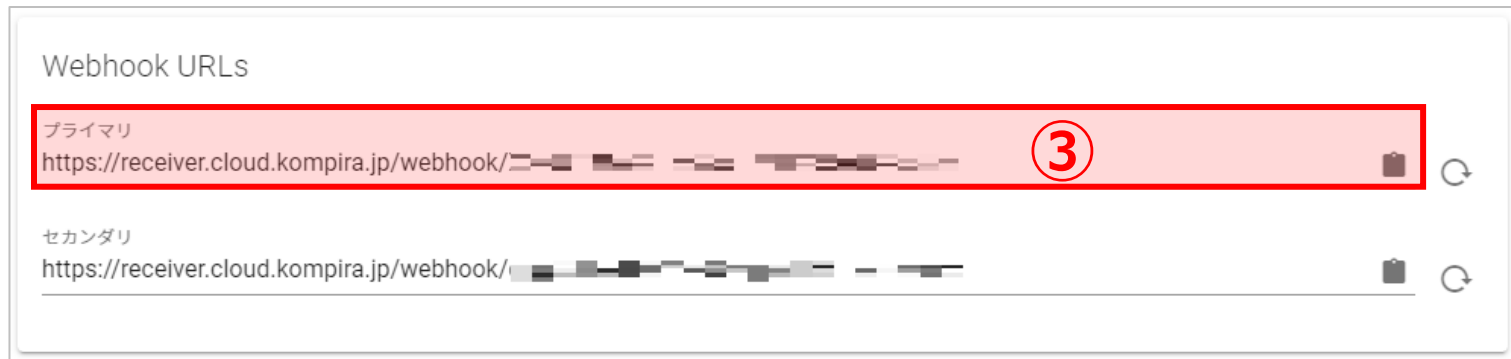
①メニューから受信スロットを選択

②受信スロットの新規作成
受信スロットの新規作成画面から種別「Webhook」を選択。

表示名はわかりやすい任意の表示名を設定してください。
今回は「アラート受信スロット」にしています。

事例② ログ監視の不要な復旧通知を送信しない

受信スロットの作成 (2/2)



③ Webhook用URLの発行

Mackerelと連携するためのURLを発行します。
下記を参考に設定してください。

※ Mackerel連携方法

<https://mackerel.io/ja/docs/entry/howto/alerts/webhook>

事例② ログ監視の不要な復旧通知を送信しない

スコープの作成

①メニューからスコープを選択

②スコープの新規作成

③障害判定閾値の設定
今回は障害判定閾値に設定できる最大値の「1000」と設定。

④警戒判定閾値の設定
警戒判定の数値によってスコープの警戒が1表示（黄色い部分）されます。「999」と設定。

⑤深刻度自動復旧の有効化
深刻度自動復旧の有効化にチェックを入れると、指定した時間が経過後に警戒・障害の表示を0に戻します。こちらは任意の時間を設定してください。

事例② ログ監視の不要な復旧通知を送信しない

ルールの作成 (1/3)

①

② +

状態	表示名	受信スロット	
有効	アラート受信ルール	アラート受信スロット	⋮
有効	マニュアル用テスト	test-Webhook	⋮
有効			⋮

任意の表示名を設定

③

アラート受信スロット

④

フィールド (F1) が文字列 (S1) を含む/含まないメッセージを許可する

操作が登録されていません
「+」ボタンを押してオペレーションを登録してください。

+

①メニューからルールを選択

②ルールの新規作成

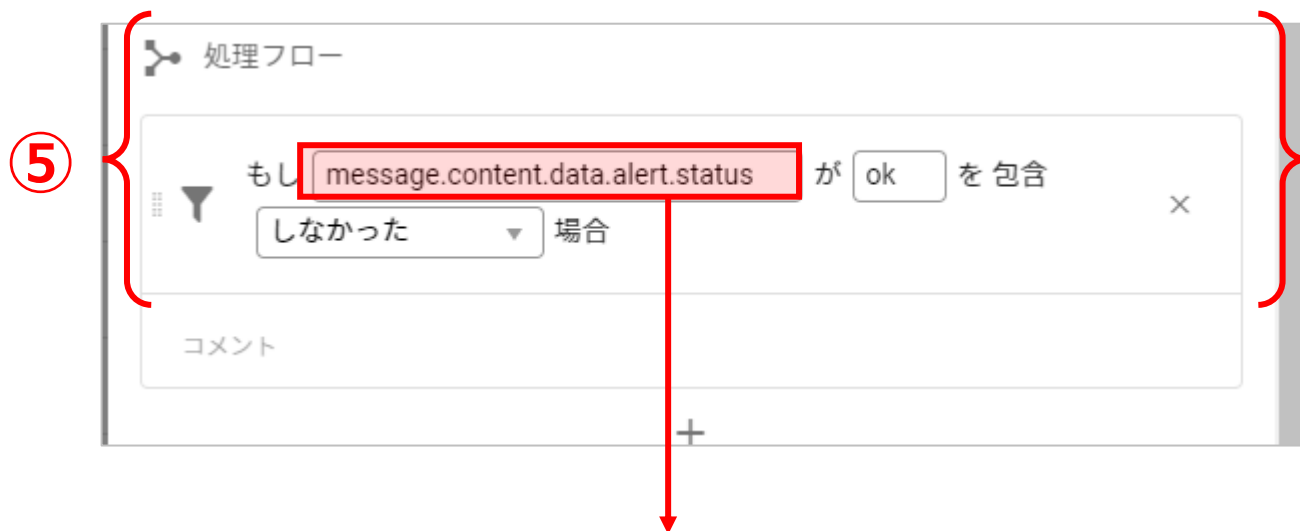
③作成した（該当の）受信スロットを選択

④処理フローを選択

「フィールド (F1) が文字列 (S1) を含む/含まないメッセージを許可する」を選択。

事例② ログ監視の不要な復旧通知を送信しない

ルールの作成 (2/3)



※ Mackerelから送信されてくるJSONの内容についての詳細は、公式の一覧表を参考にしてください。

今回は、JSONの各項目（アラート情報）を参考にしています。

<https://mackerel.io/ja/docs/entry/howto/alerts/webhook>

status	string	アラートのステータス(<code>ok</code> , <code>warning</code> , <code>critical</code> , <code>unknown</code>)
--------	--------	---

⑤処理フローを設定

今回はアラートのステータスが、「ok」以外の通知が必要なので

F1 = message.content.data.alert.status

S1 = ok

包含「しなかった」場合

と設定します。

事例② ログ監視の不要な復旧通知を送信しない

ルールの作成 (3/3)

イベント

アラート_障害テスト2

深刻度を 1 増やす

⑥

増やす

選択してください

にする

増やす

減らす

⑥ イベントを追加

▼プルダウンから作成したスコープを選択します。
今回は「アラート_障害テスト2」を選択。

深刻度について

今回は深刻度を利用して1件の受信につき1アクションを実行させたいので、1増やすというルールを設定します。

※参照：

PP.16-19 「作成の流れ> ルールの作成」

事例② ログ監視の不要な復旧通知を送信しない

アクションの作成

Kompira cloud

AlertHub

スコープ

受信スロット

ルール

アクション ①

アクション

② メール

PIGEON WEBHOOK

表示名	種別	最終実行日時	
メールテスト	メール	2020/11/24 13:09	

表示名
メールテスト 任意の表示名を設定

To

名前	メール
テスト太郎	test@testtarxxxx.net

+

Cc

「+」ボタンを押して名前とメールアドレスを追加してください。

+

Bcc

「+」ボタンを押して名前とメールアドレスを追加してください。

+

件名
テスト ④

本文
{{message.content.data}}

①メニューからアクションを選択

②アクションの新規作成

今回はメールへ通知させたいので、メールを選択しアクションの新規作成を行います。

③メールの宛先を設定

メールを送信したい人の名前・アドレス（TO）を入力します。必要に応じてCC・BCCも追加してください。

④メール内容

任意の件名を入力してください。

本文は、Mackerelから受信したJSON形式をメールで送信したいので、

`{{message.content.data}}`

と設定します。

事例② ログ監視の不要な復旧通知を送信しない

トリガーの作成 (1/2)

Kompira cloud

AlertHub

① スコープ

受信スロット

ルール

マナー

スコープ

15 正常

0 警戒

ステータス 表示名

正常

アラート_障害テスト2 ②

< アラート_障害テスト2

137347ED-E0CC-4543-BB5D-981DA47B2012

0 正常

2020/11/24 12:36 最終更新日

概要 ルール ③ トリガー 設定

トリガー ④ +

状態	表示名	アクション	
----	-----	-------	--

①メニューからスコープを選択

②作成したスコープを選択

③トリガーを選択

④トリガーの新規作成

事例② ログ監視の不要な復旧通知を送信しない

トリガーの作成 (2/2)

トリガー	+		
状態	表示名	アクション	+

↓ 今回の設定では下記を選択

- 過去 (T1) 秒間にアクションが発火した回数が数値 (N1) とオペレータ (O1) で一致することを必要とする
- 過去 (T1) 秒間にイベントのフィールド (Y1) が数値 (N1) とオペレータ (O1) で一致するイベントの回数が数値 (N2) とオペレータ (O2) で一致することを必要とする
- (T1) 秒経過後、イベントのフィールド (Y1) が数値 (N1) とオペレータ (O1) で一致することを必要とする
- イベントのフィールド (Y1) が数値 (N1) とオペレータ (O1) で一致することを必要とする
- (T1) 秒経過後、スコープステータスが文字列 (S1) と等しい/等しくない (O1) ことを必要とする
- スコープステータスが文字列 (S1) と等しい/等しくない (O1) ことを必要とする

表示名	任意の表示名を設定
メール通知条件	7 / 30
実行条件	
深刻度の変化量	が 1 と等しい 値である ⑤ ×
コメント	
アクション	新規アクションの追加
メールテスト	⑥
キャンセル	保存

⑤ 実行条件の設定内容

「イベントのフィールド (Y1) が数値 (N1) とオペレータ (O1) で一致することを必要とする」を選択。

ルールの設定時、1件の受信につき1アクションを実行させたいので深刻度を1ずつ増やすというルールを設定したので、

「深刻度の変化量」
N1 = 「1」
「と等しい」

と設定します。

⑥ 作成したアクションを選択

「メールテスト」を選択。

事例② ログ監視の不要な復旧通知を送信しない

アラート受信後の画面

The screenshot shows the Kompira cloud AlertHub interface. The top bar displays the alert name 'アラート_障害テスト2' and a status of '0 正常' (0 Normal) as of '2020/11/24 12:36'. Below this, there are summary statistics: '正常 ≤ 998', '警戒 999', and '障害 1000 ≤'. A section for '深刻度復旧時間' (Severity recovery time) is set to '5分' (5 minutes). Two tables are highlighted with red boxes:

イベント				
変化前の深刻度	深刻度	タイムスタンプ	eventId	
1	0	2020/11/24 14:10	f072be26-0c60-4187-8c86-d29edd741da2	
Mackerelから受け取ったアラートがイベント欄に表示されます				
4	5	2020/11/24 13:09	3be71e6d-b5ce-4fca-a7f0-e3dc46f2cc02	
3	4	2020/11/24 13:09	1c9ae325-346e-4173-91ed-399196823dc2	

アクション				
アクション	タイムスタンプ	actionId	actionRecordId	
アクション	2020/11/24 14:04	0f74e3a0-fc0f-4167-b704-4167-b704-4167-b704-4167-b704	0e7d8b8d-669a-4071-a2c8-4071-a2c8-4071-a2c8-4071-a2c8	
アクション	2020/11/24 13:09	0f74e3a0-fc0f-4167-b704-ab207674888f	48da-b3c5-8895c2af1be8	
アクション	2020/11/24 13:04	0f74e3a0-fc0f-4167-b704-4167-b704-4167-b704-4167-b704	7f561450-5a81-49a0-a186-49a0-a186-49a0-a186-49a0-a186	

メールで受け取った通知

The screenshot shows an email notification from Kompira cloud. A red box highlights the text 'status:critical' in the email body. Below it, a red text box says 'criticalのみ受信できています' (Only critical alerts are received).

Kompira AlertHubコミュニティ

本サービスについてご質問がございましたら、
株式会社フィックスポイントの公式コミュニティにお問い合わせください。

<https://kompira.zendesk.com/hc/ja/community/topics/900000101443-AlertHub%E9%96%A2%E9%80%A3>

また、Kompira cloud Blogでは「AlertHub ハンズオンガイド」や
「AlertHub 逆引き設定ガイド」を公開しております。ぜひこちらもご参照ください。

- ・AlertHub ハンズオンガイド

<https://blog.cloud.kompira.jp/entry/2020/09/30/203601>

- ・AlertHub 逆引き設定ガイド

<https://blog.cloud.kompira.jp/entry/2020/09/30/203341>