Kompira AlertHub　基本マニュアル

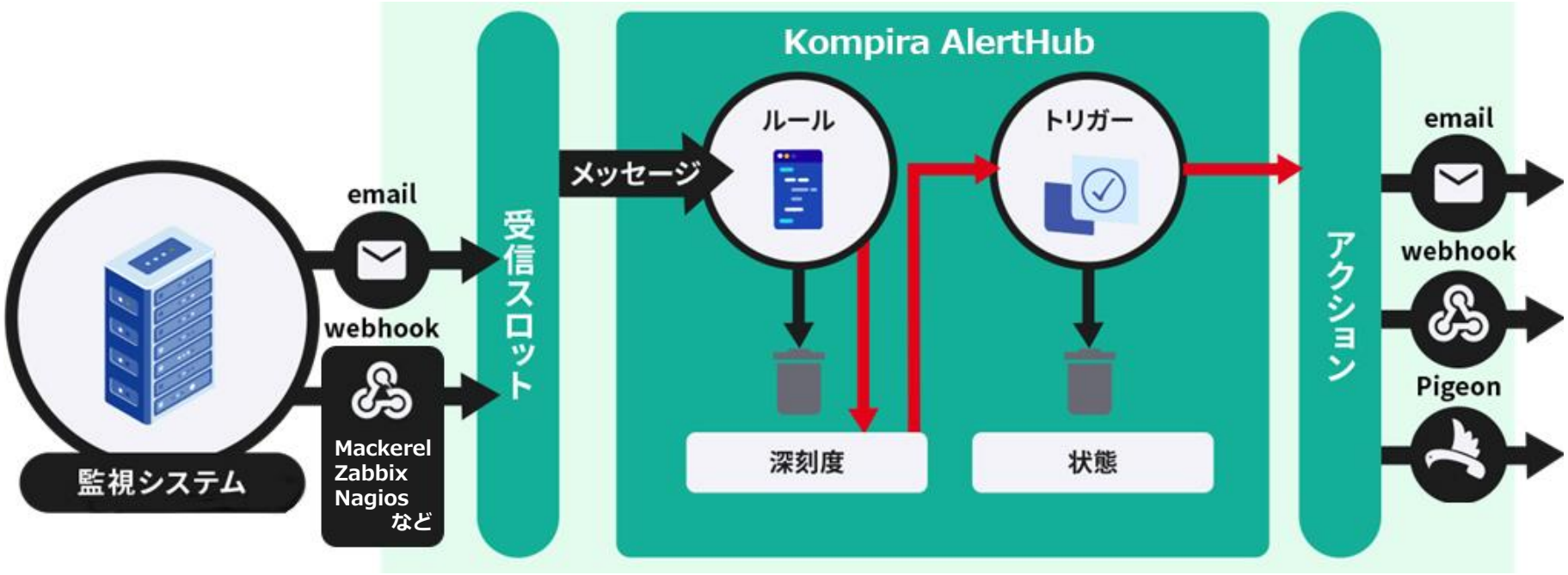
もくじ

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な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ので、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。

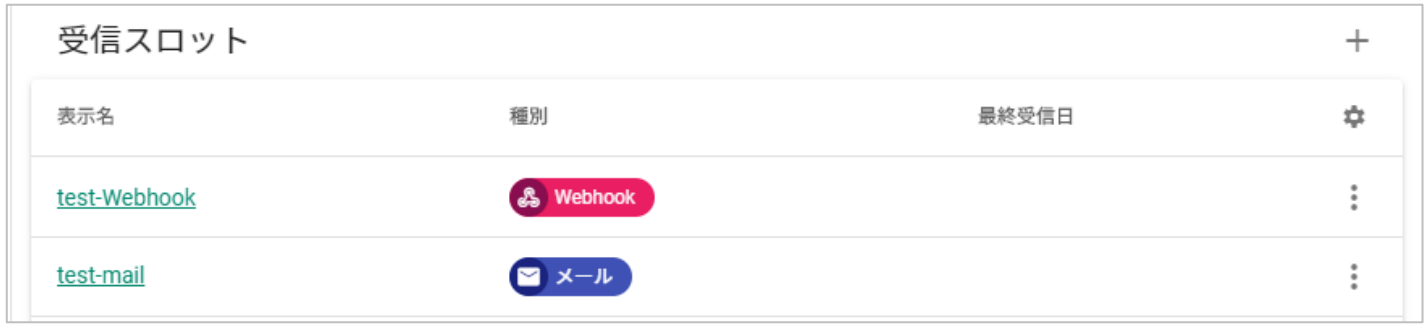
それでは、はじめにそれぞれの機能について説明していきます。

※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。



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。

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。

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

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。

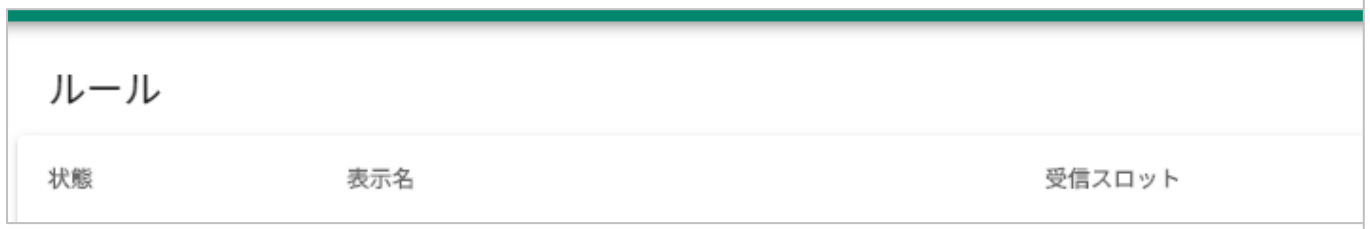
スコープの深刻度やステータスの変化などによって、アクションを実行するかどうか判断します。
アクションだけを設定しても、このトリガーがないと実行されないので注意が必要です。

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。

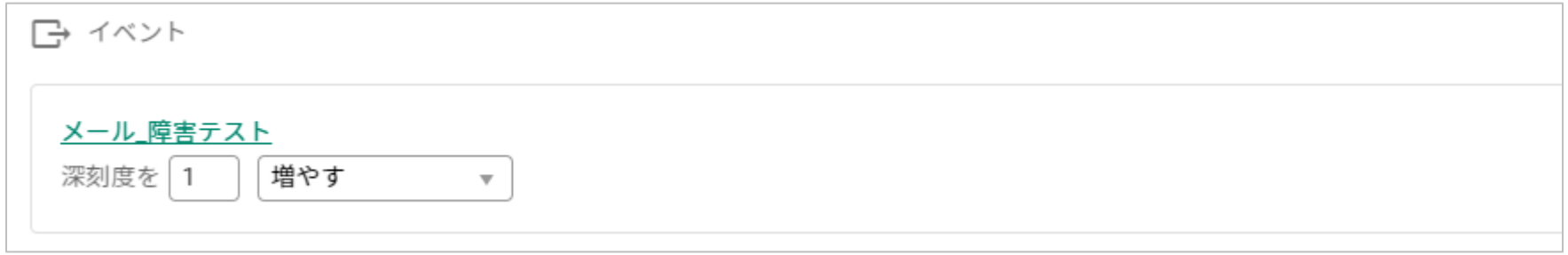
アラート内の単語を条件に指定したり、様々な条件で柔軟に設定することができます。



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。



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。

機能とはたらき

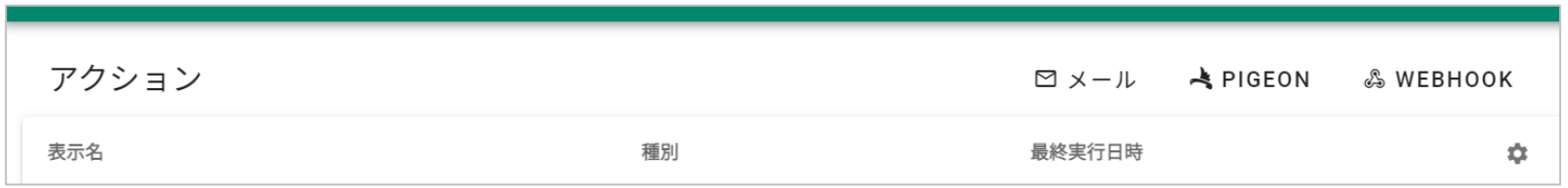
・アクションとは

監視結果を通知する機能です。

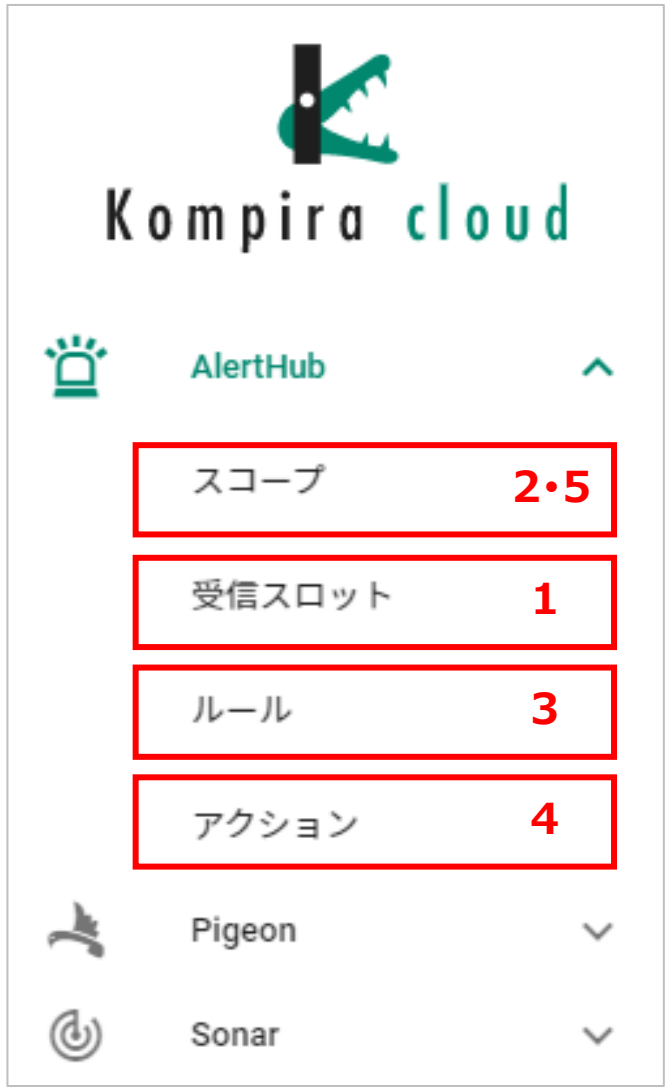
・メール送信
・Pigeonを利用した電話発信
・Webhookを利用した外部APIの呼び出し

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。



作成の流れ



管理画面にログイン後、

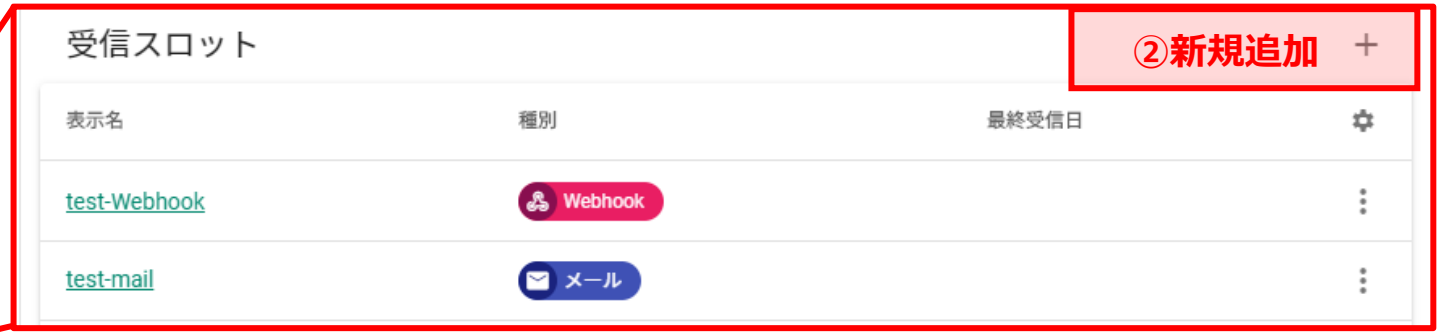
下記の流れの通り作成します。

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

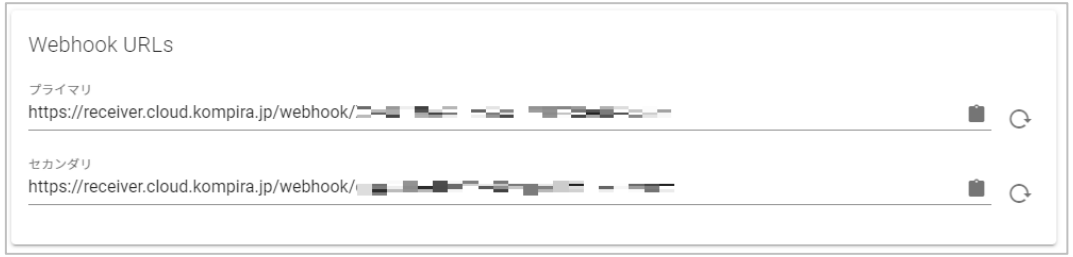
作成の流れ

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

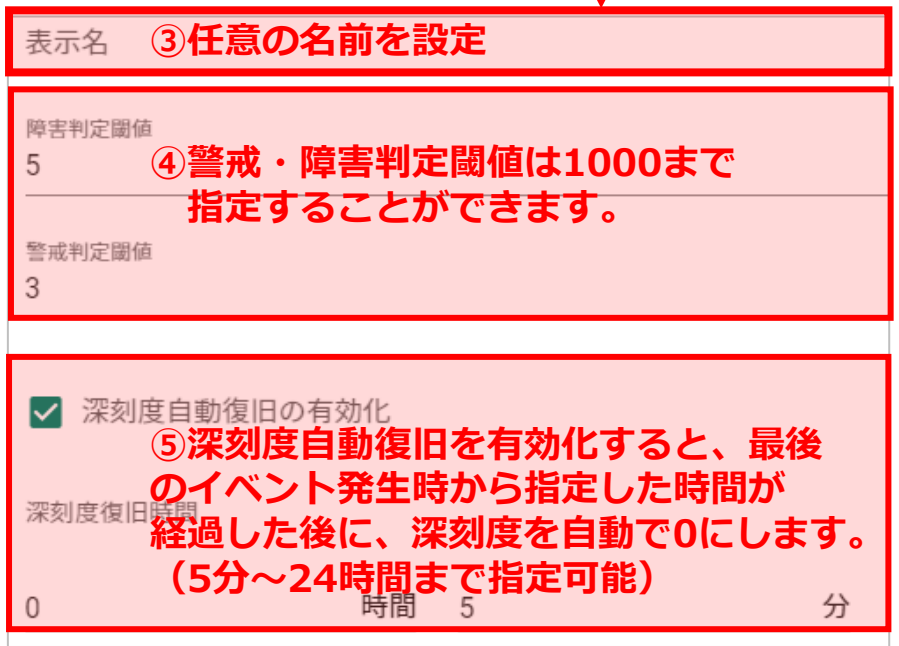
Mackerel
https://mackerel.io/ja/docs/entry/howto/alerts/webhook

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

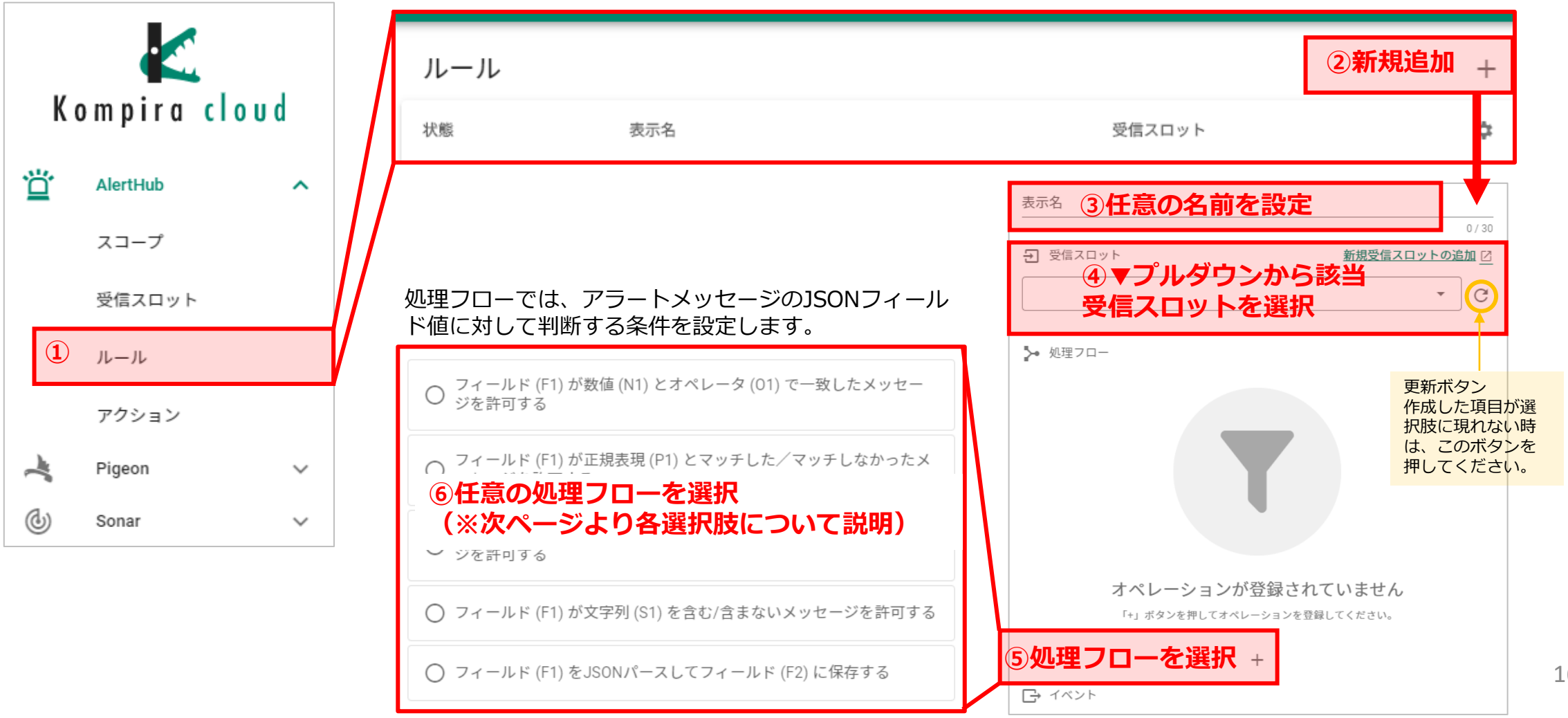
ルールやアクションの紐づけを行うスコープを作成します。
ルールとアクションの紐づけ以外に「正常」「警戒」「障害」の状態判定の設定も行えます。



作成の流れ

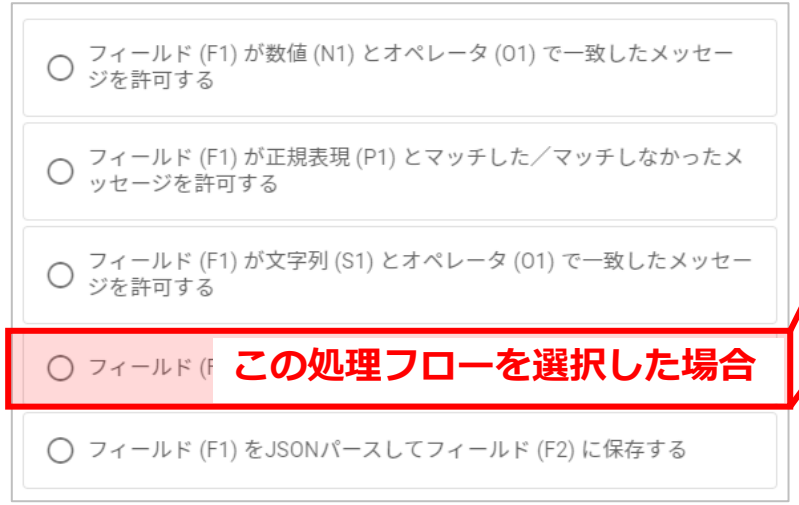
3.ルールの作成（1/4）

アラートを判断するルールの設定を行います。



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。



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

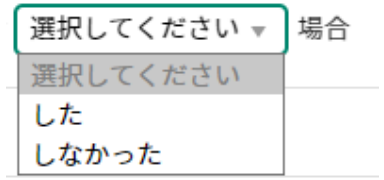
例）メール本文に「error」と表示があることをフィルタリングの条件とした場合は「error」を指定。

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。

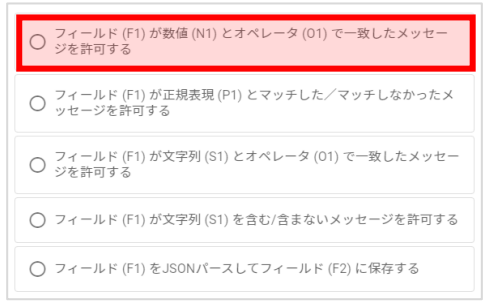
▼「error」という表記がない場合のアラート　しなかった　を選択。



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



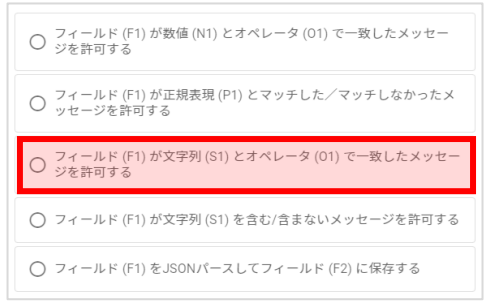
1 入力項目（メールの場合）

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



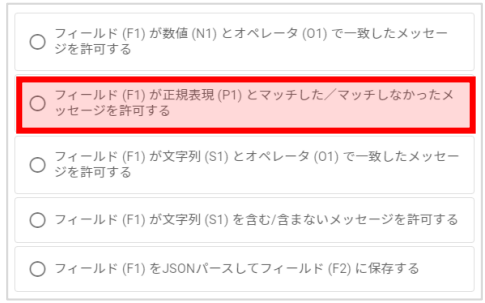
1 入力項目（メールの場合）

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



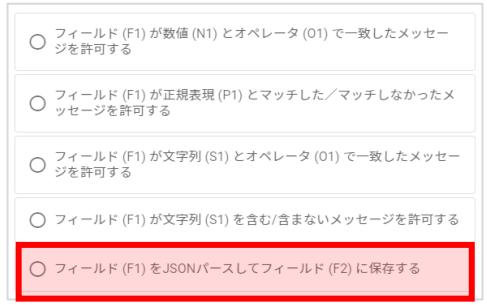
1 入力項目（メールの場合）

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



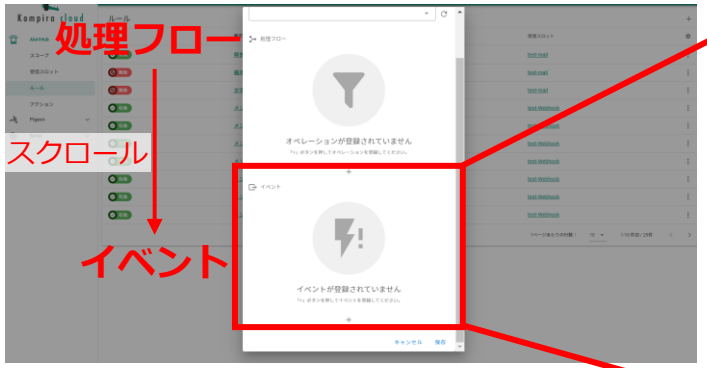
1 2 入力項目（メールの場合）

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

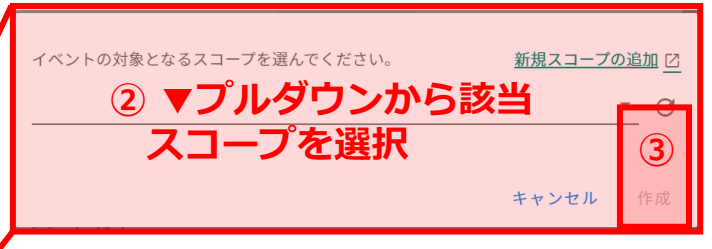
JSONパースに関しては主にメール本文に使用します。メール受信の場合はそういったJSONデータを扱う手段がありませんが、システムによってはWebhook送信に対応しておらずメールのみを送れる、というケースがあるので、本文をJSON形式で送りJSONパースする形を取ることで、メールでも構造化データを取り扱えます。

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。

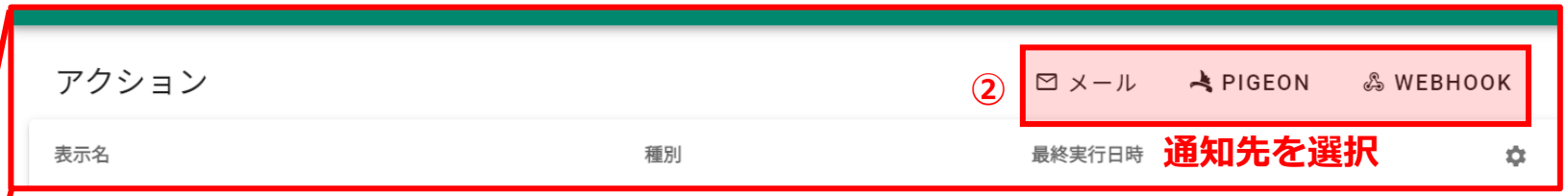
2 深刻度の数値の増減を選択

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。

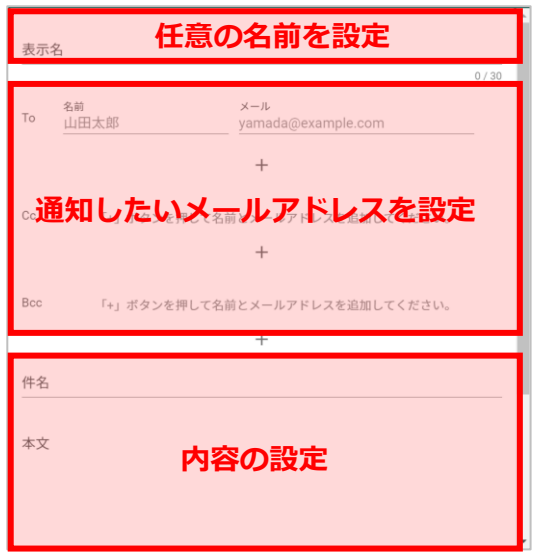
作成の流れ

4.アクションの作成

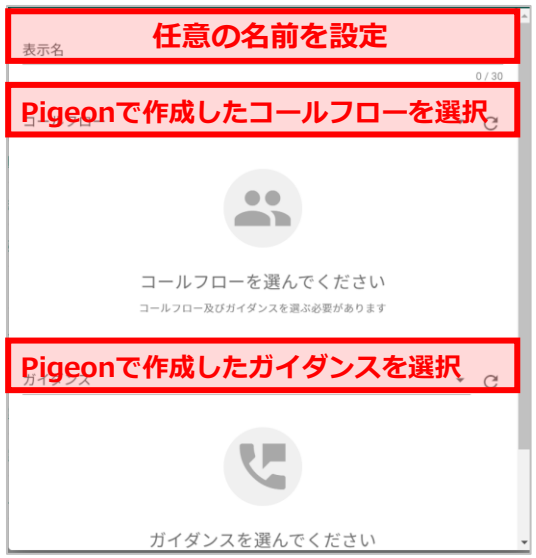
アラート通知の集約後に実行する設定を行います。



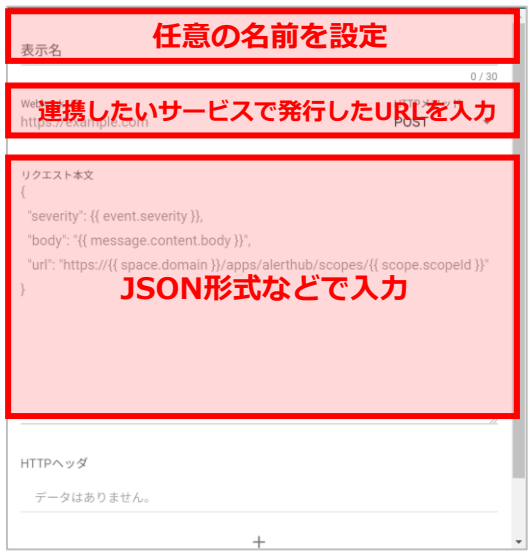
メール



PIGEON



WEBHOOK

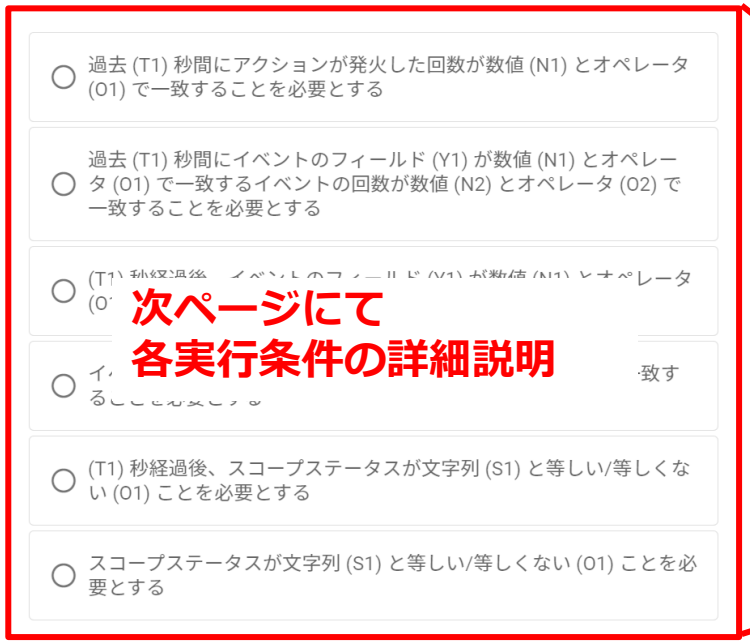


※別途、Pigeon側の設定が必要です。

作成の流れ

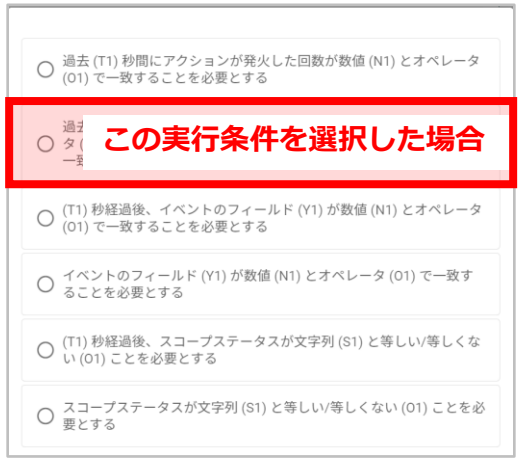
5.トリガーの作成（1/3）

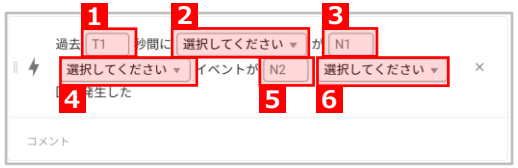
アクションの実行条件を設定します。



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。



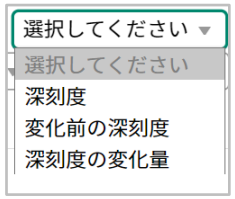


こんなときに使用します）

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。

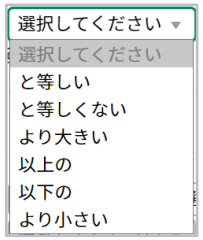
1 任意の数値（秒）を設定

2 深刻度の基準を▼プルダウンから選択



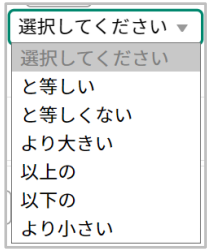
3 任意の数値を設定

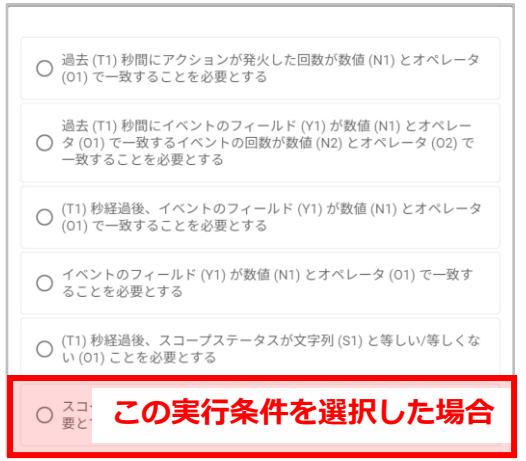
4 ▼プルダウンから選択



5 任意の数値を設定

6 ▼プルダウンから選択

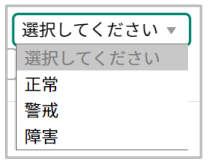




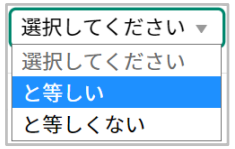
こんなときに使用します）

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



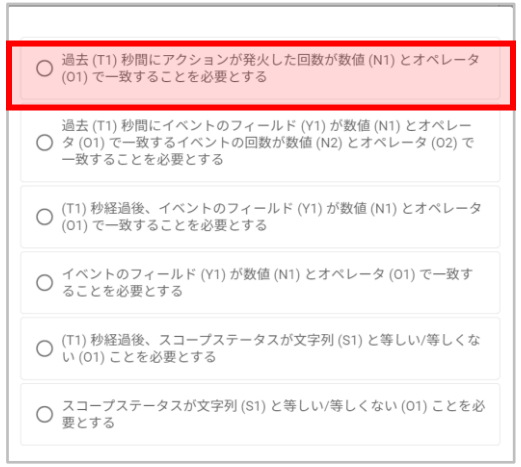
2 ▼プルダウンから選択



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

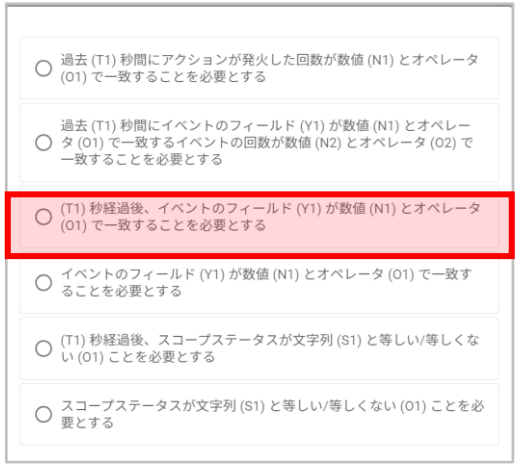


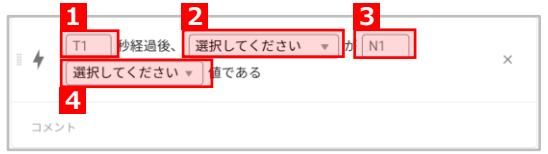
1 任意の数値を設定
時間（秒）を設定。

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





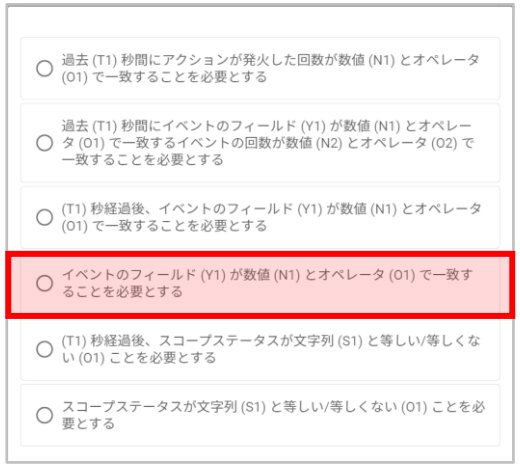
1 任意の数値を設定

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

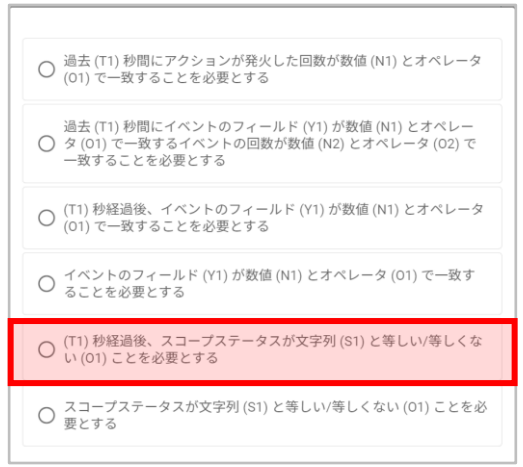


1 ▼プルダウンから比較を選択

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



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。

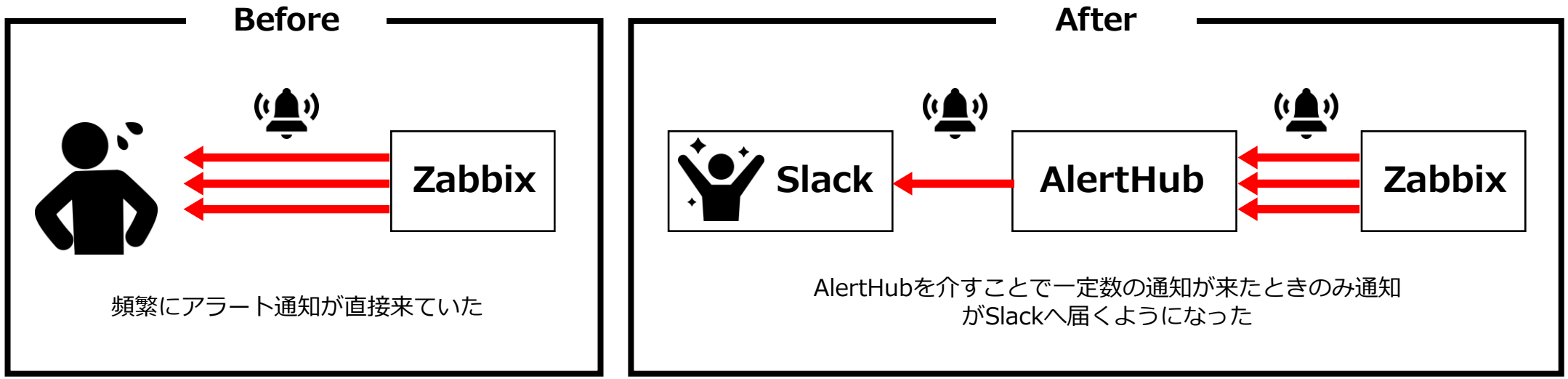
事例①
30分以内に10件以上のアラートが発生したらSlackに通知する

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）

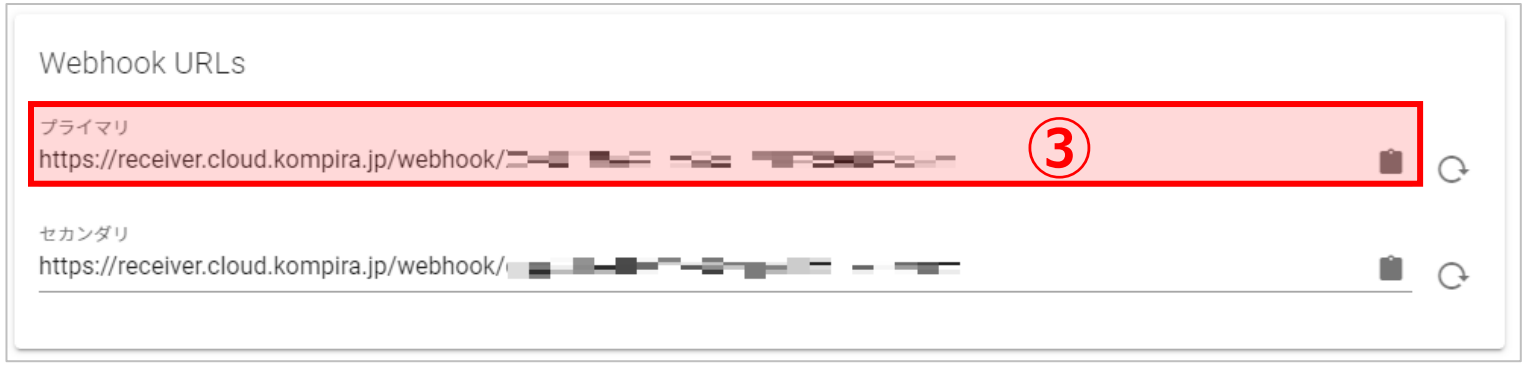
①メニューから受信スロットを選択

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）



③Webhook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

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）

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）

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

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）

①メニューからスコープを選択

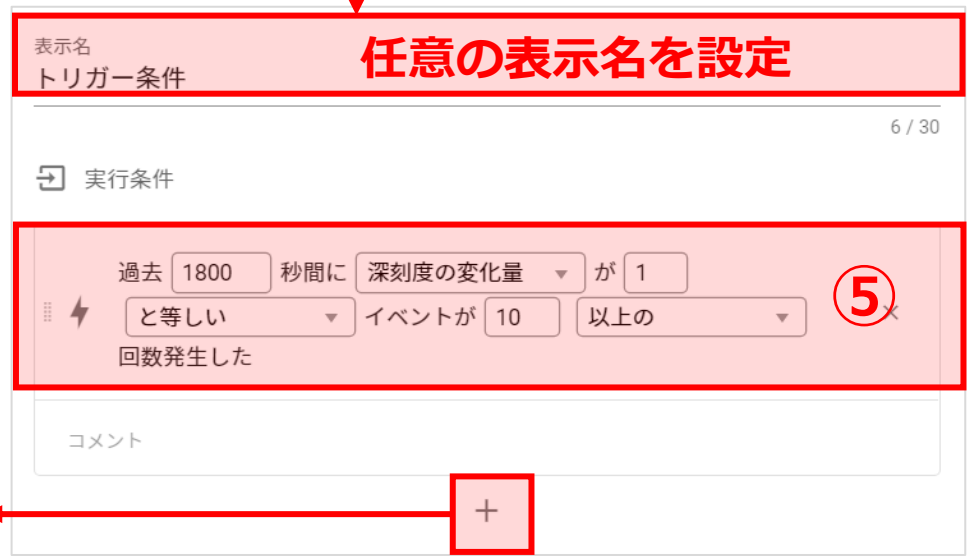
②作成したスコープを選択

③トリガーを選択

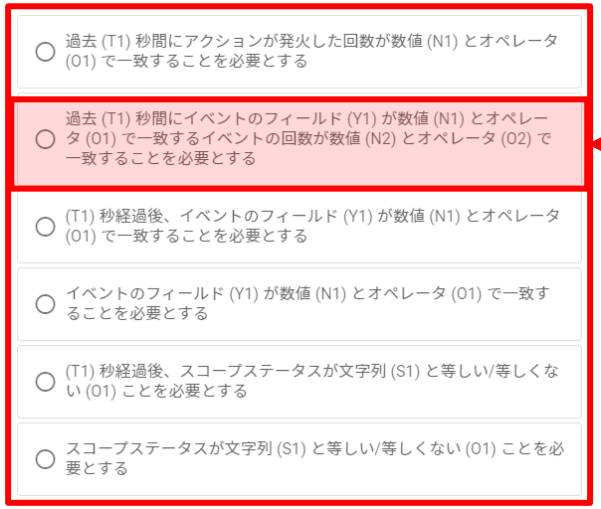
④トリガーの新規作成

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）



↓今回の設定では下記を選択



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

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

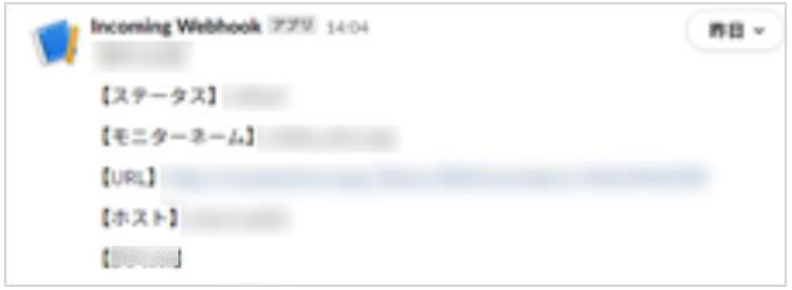
トリガーの作成（3/3）

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

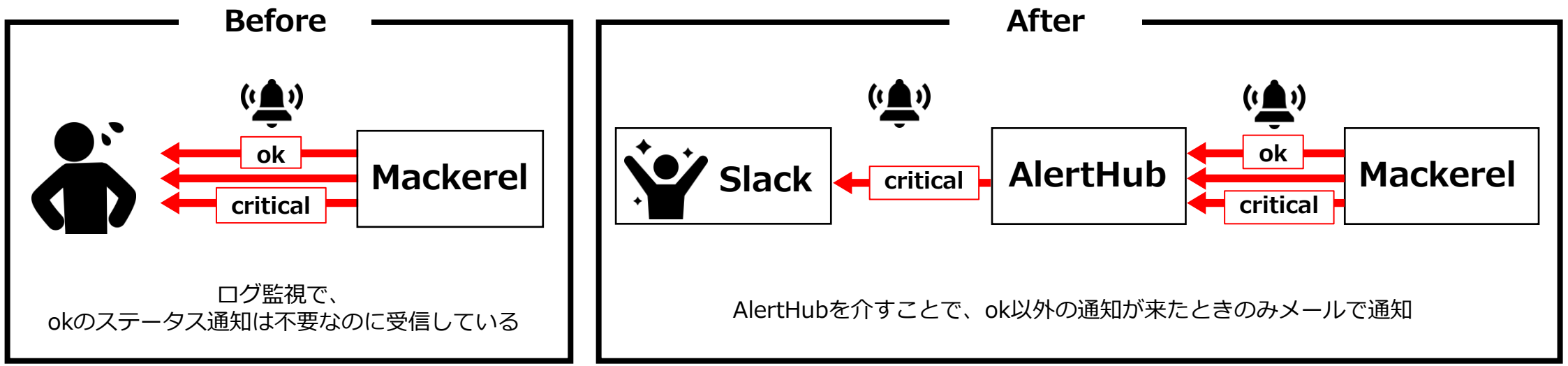
Slackで受け取った通知



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）

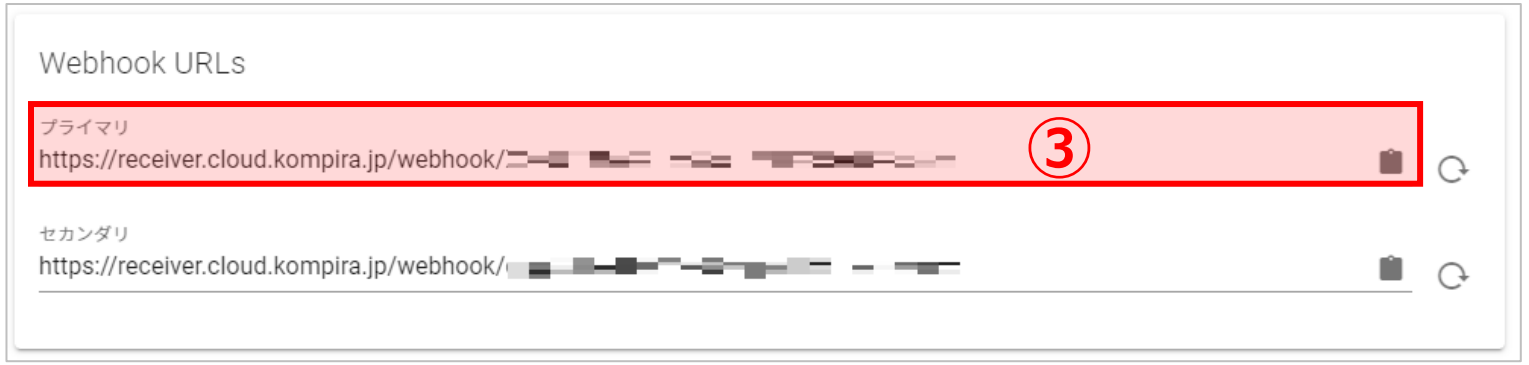
①メニューから受信スロットを選択

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）

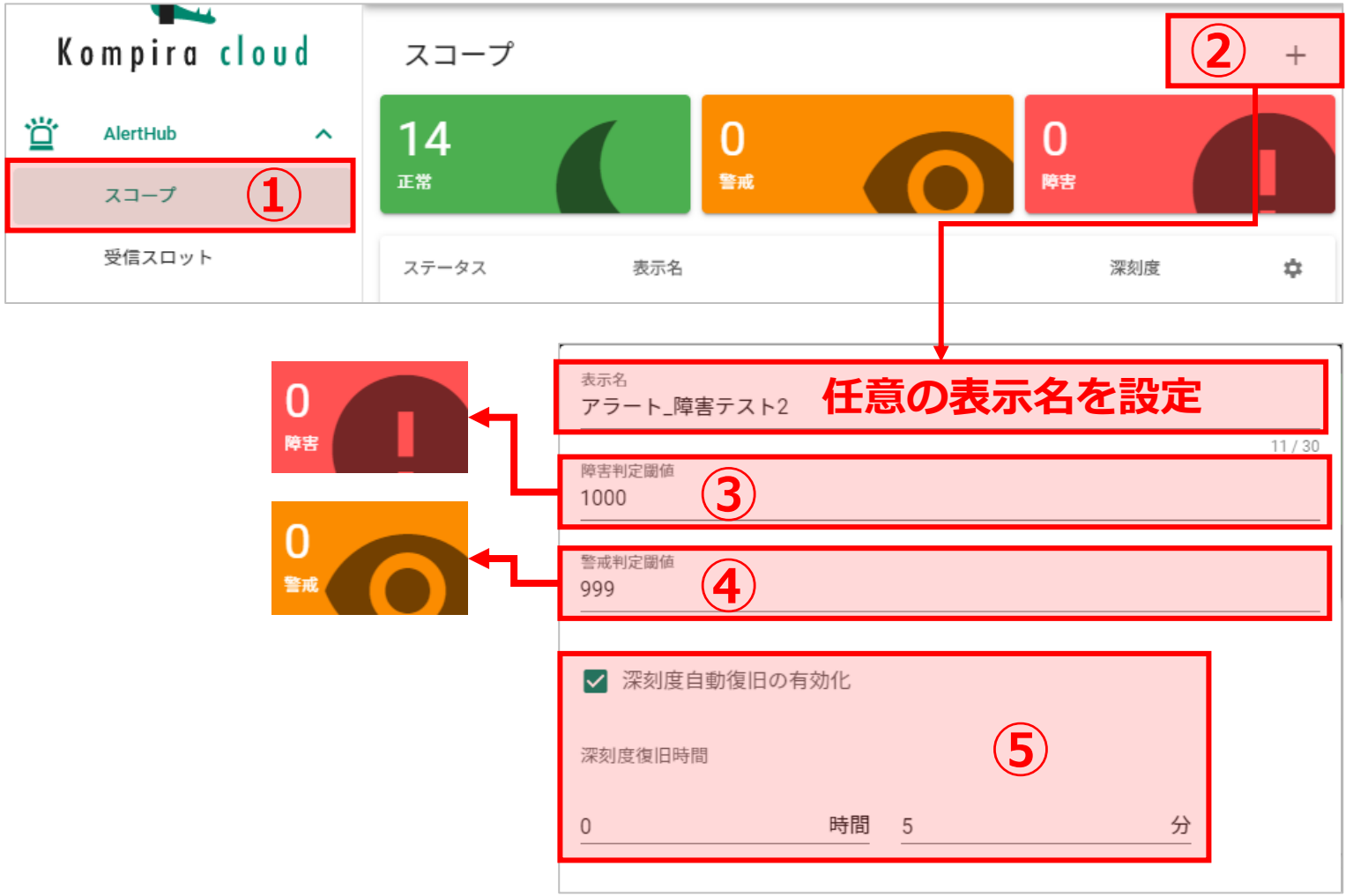


③Webhook用URLの発行
Mackerelと連携するためのURLを発行します。
下記を参考に設定してください。

※ 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

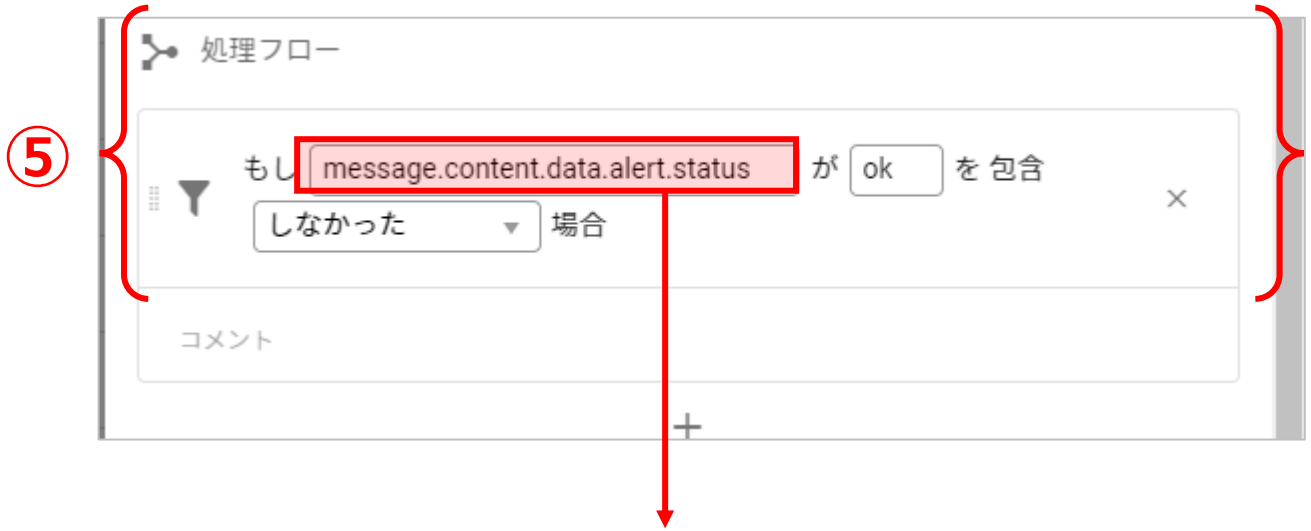
②ルールの新規作成

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(ok , warning , critical , unknown)

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）

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

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）

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）

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」

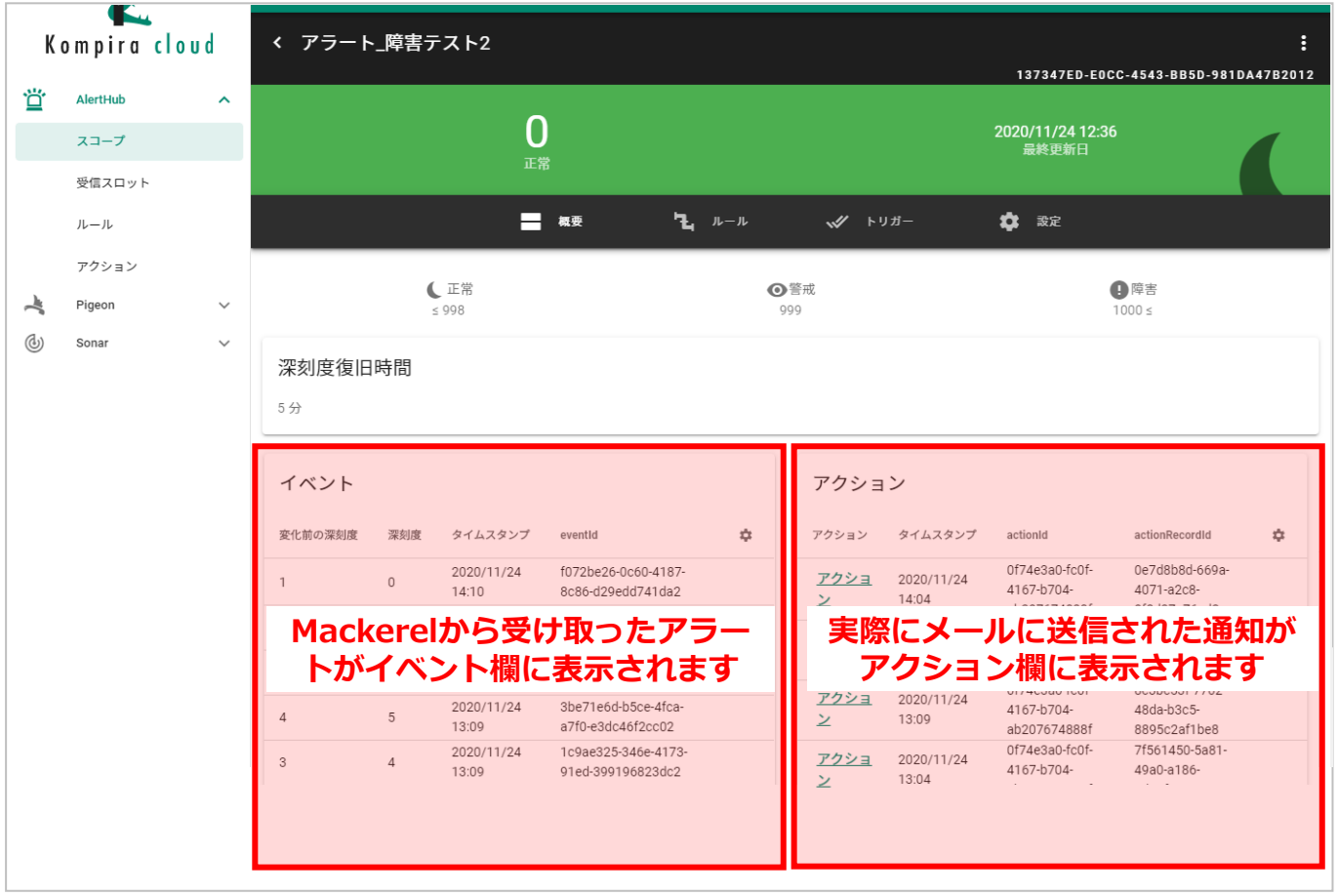
と設定します。

⑥作成したアクションを選択

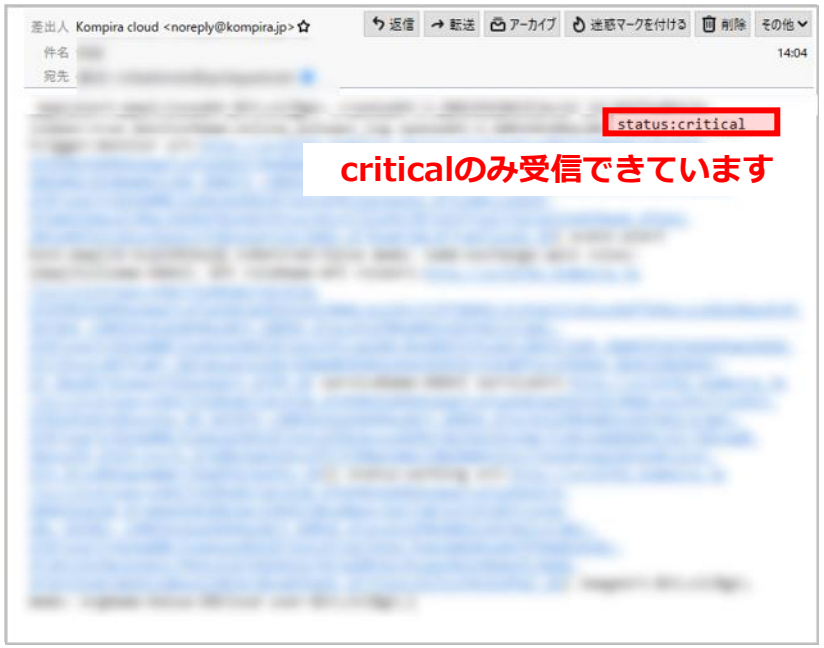
「メールテスト」を選択。

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



メールで受け取った通知



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