

NRU 304 「AIOps とアラート設計の基本」

December 7, 2022



ウェビナー 各種ご連絡

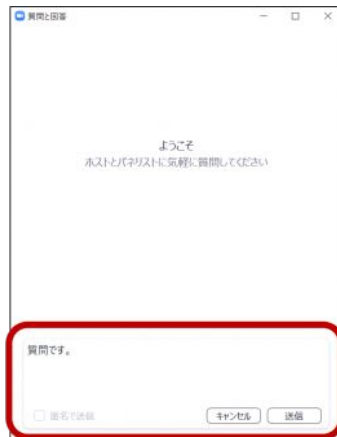
1. ご質問がある場合は、「Q&A」からご入力ください。



① 画面下
「Q&A」をクリック！

こちらにご質問をご記入し、
「送信」をクリックしてください！

②



2. 本日の資料はこの後「チャット」でURLを共有します。アクセスできない場合は、「Q&A」よりお名前とメールアドレスをご連絡ください。

Safe Harbor

This presentation and the information herein (including any information that may be incorporated by reference) is provided for informational purposes only and should not be construed as an offer, commitment, promise or obligation on behalf of New Relic, Inc. (“New Relic”) to sell securities or deliver any product, material, code, functionality, or other feature. Any information provided hereby is proprietary to New Relic and may not be replicated or disclosed without New Relic’s express written permission.

Such information may contain forward-looking statements within the meaning of federal securities laws. Any statement that is not a historical fact or refers to expectations, projections, future plans, objectives, estimates, goals, or other characterizations of future events is a forward-looking statement. These forward-looking statements can often be identified as such because the context of the statement will include words such as “believes,” “anticipates,” “expects” or words of similar import.

Actual results may differ materially from those expressed in these forward-looking statements, which speak only as of the date hereof, and are subject to change at any time without notice. Existing and prospective investors, customers and other third parties transacting business with New Relic are cautioned not to place undue reliance on this forward-looking information. The achievement or success of the matters covered by such forward-looking statements are based on New Relic’s current assumptions, expectations, and beliefs and are subject to substantial risks, uncertainties, assumptions, and changes in circumstances that may cause the actual results, performance, or achievements to differ materially from those expressed or implied in any forward-looking statement. Further information on factors that could affect such forward-looking statements is included in the filings New Relic makes with the SEC from time to time. Copies of these documents may be obtained by visiting New Relic’s Investor Relations website at ir.newrelic.com or the SEC’s website at www.sec.gov.

New Relic assumes no obligation and does not intend to update these forward-looking statements, except as required by law. New Relic makes no warranties, expressed or implied, in this presentation or otherwise, with respect to the information provided.

本日のゴール

- New Relicを使ってより**ユーザー体験に近い指標**でアラートを設定する手法を学ぶ
- New Relicを使って**AIOpsを実現する手法**を学ぶ

本セッションの想定対象者と前提条件

- これまでのインフラ監視から脱却し、ユーザー体験の悪化を迅速に知りたいと思っている
- 大量のアラートに悩んでいる、逆にアラートでは気づけない障害に悩んでいる
- アラートから素早く根本原因にたどり着きたい
- New Relicの基本的な知識をお持ちであること
- 簡単なNRQLを知っている

New Relicの知識に不安のある方はこちらを受講ください！(オンデマンド視聴可)

- [New Relicの基礎](#)
- [ダッシュボードワークショップ](#) (NRQL入門編に相当)

Agenda

時間(目安)	内容	
15:00-15:15	座学(1)	ユーザー視点のアラート
15:15-15:35	座学(2)	New Relicのアラート機能
15:35-15:45	ハンズオン(0)	環境を確認する
15:45-16:05	ハンズオン(1)	アラートを作成する
16:05-16:15	座学(3)	New RelicのAIOps機能
16:15-16:30	ハンズオン(2)	AIOpsを使った異常検知と原因分析
16:30-16:45	座学(4)	AIOpsの意義
16:45-16:55	ハンズオン(3)	AIOpsを使った異常検知と原因分析 (応用編)
16:55-17:00		まとめ、アンケートご記入

座学(1)

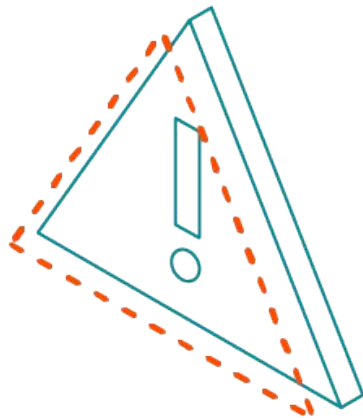
ユーザー視点のアラート

15:00 - 15:15 (15min)



突然ですが

- どんなアラートを設定していますか？



アラートを設定する目的

対象システムが以下のような観点で対応が必要であることを知るための**通知を得るため**に行う

1. システムの停止、またはパフォーマンスの悪化が発生し、**ユーザーへのサービス提供に支障が出ている**
2. 1のような事象が近いうちに発生する可能性がある**兆候が出ている**

"受け取った結果、何かしらのアクションを起こせるようなアラート"を設定する

アラートのアンチパターンとデザインパターン

アンチパターン: OSのメトリクスのアラート

“ MySQLが継続的にCPU全部を使っていたとしても、レスポンスタイムが許容範囲に収まっていれば何も問題ありません。 ”

“ OSのメトリクスは診断やパフォーマンス分析にとっては重要です。

しかし99%の場合、これらのメトリクスは誰かを叩き起こすには値しません。 ”

出典: 入門監視 (Oreilly, 2019)



アラートのアンチパターンとデザインパターン

デザインパターン: ユーザー視点の監視

”ユーザーが気にするのは、アプリケーションが動いているかどうかです。”

”ユーザー視点優先の監視によって、個別のノードを気にすることから解放されます。”

出典: 入門監視 (Oreilly, 2019)

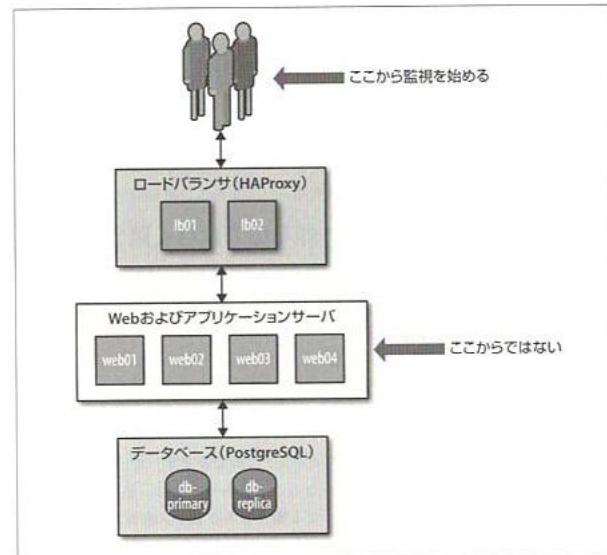
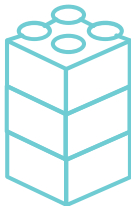


図2-1 できるだけユーザーに近いところから監視を始める

なぜアンチパターンが生み出されたのか

過去のシステム

アプリ



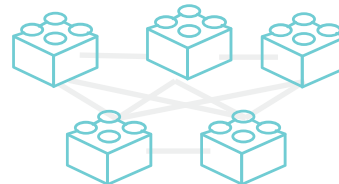
基盤



アプリがモノリシックかつ基盤が密結合だったため、リソースが枯渇しなければ大きな問題が発生しなかった

近年のシステム

アプリ



リソース抽象化
(仮想化、コンテナ等)

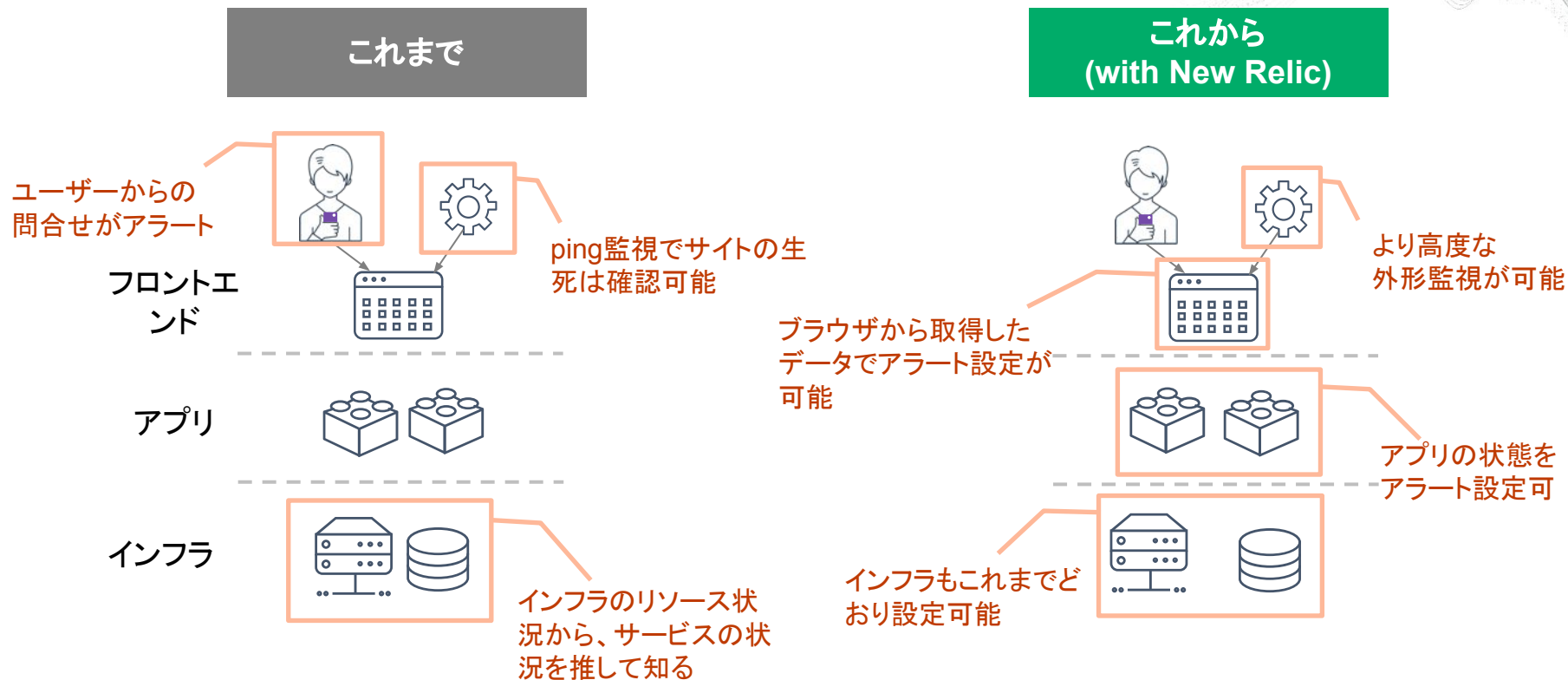


基盤



アプリがマイクロサービス化かつ基盤が疎結合なため、基盤リソースと関係なく問題が発生しうる

アラートのこれまでと、New Relicを使ったこれから



目的別、アラート設定例(Webアプリの一例)

カテゴリ	現在起こっているサービス影響		将来のリスクの兆候	
	サイトが遅い	エラーを返す	キャパシティを超える	リソースが枯渇する
外形監視	チェック応答時間	チェックエラー		
フロントエンド	Apdex	JSエラー		
アプリケーション	Apdex 応答時間	4xx, 5xxエラー	スループット バッチ遅延	
インフラ				各種インフラ リソース

座学(2)

New Relicのアラート機能

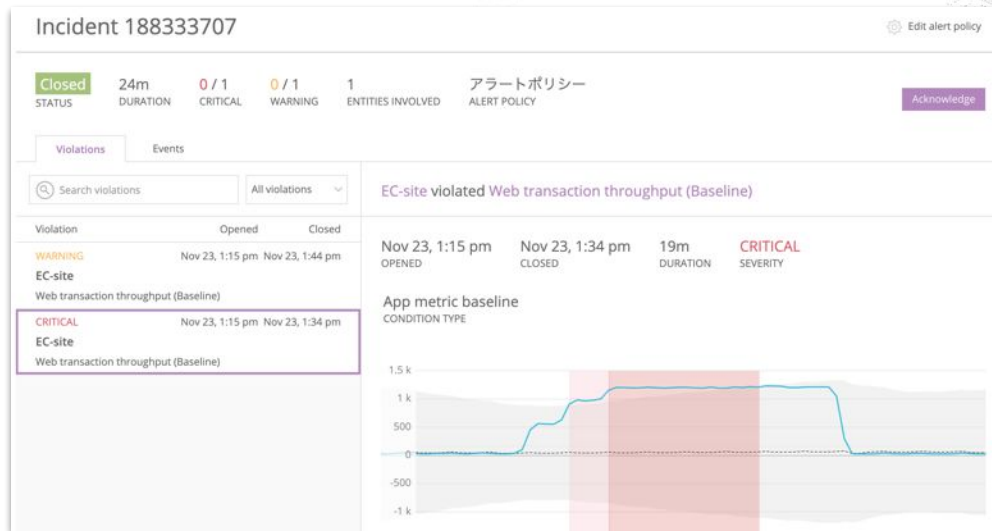
15:15 - 15:35 (20min)

New Relicのアラート機能

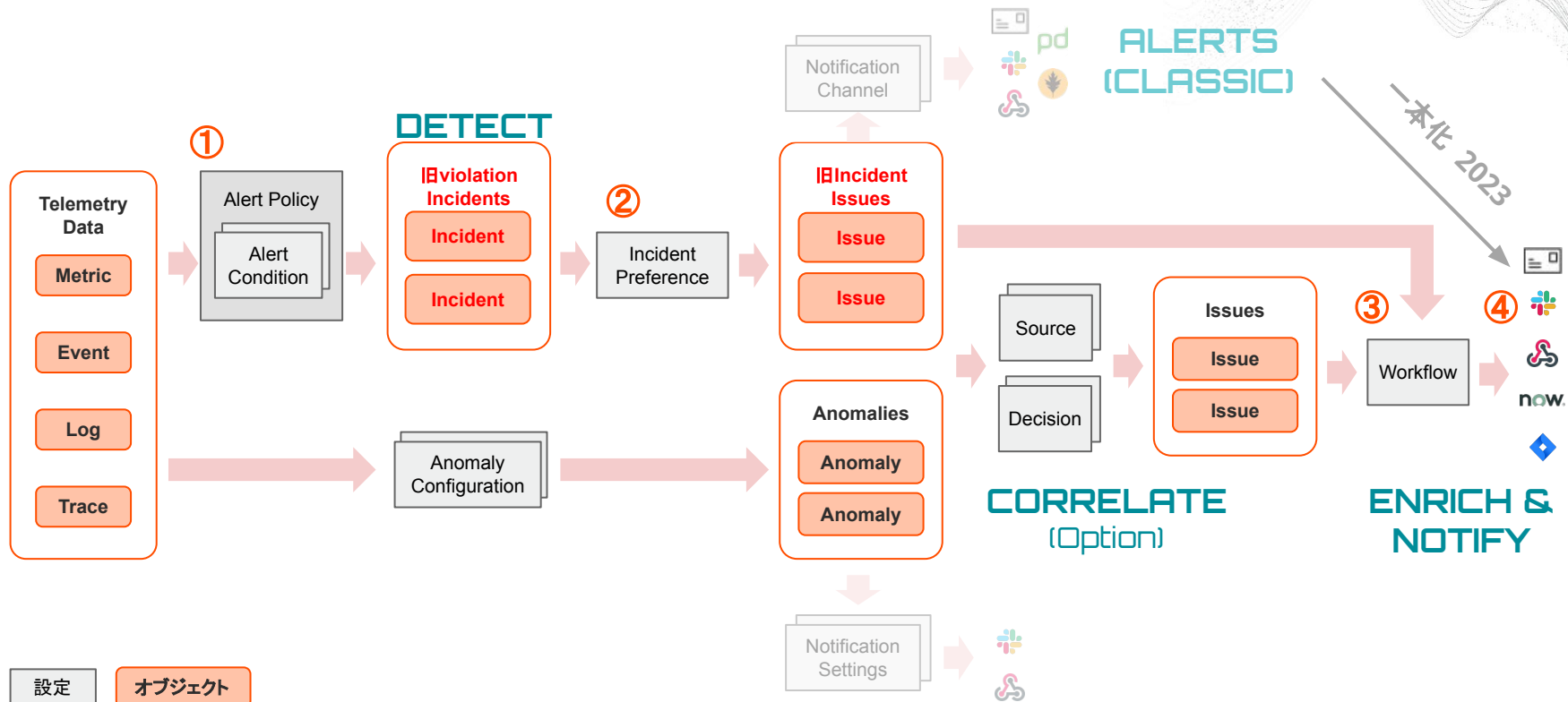
New Relicが収集しているデータを使って、アラートを設定することが可能

アラートを設定すると、アラート条件に従ってインシデントが起票され、通知を受けることができる

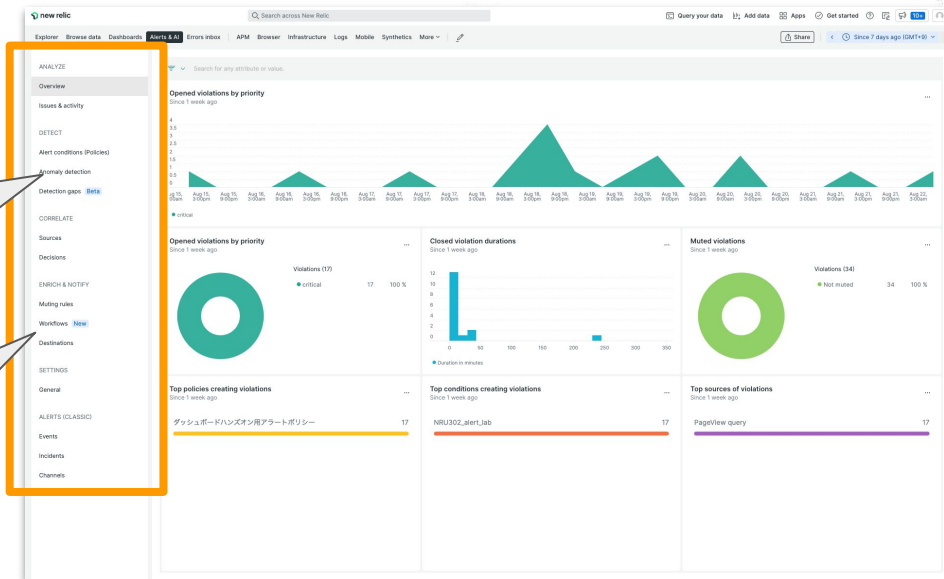
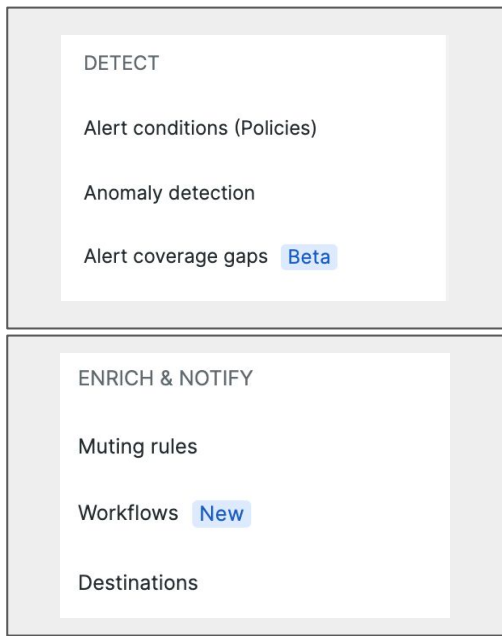
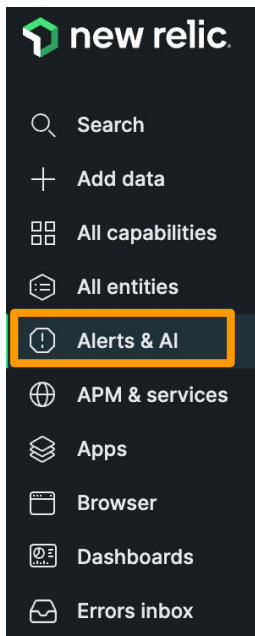
※アラートを上げる条件や頻度、通知先の設定など、様々な設定が可能なので、次ページ以降で解説していきます



New Relicのアラート構造全体像

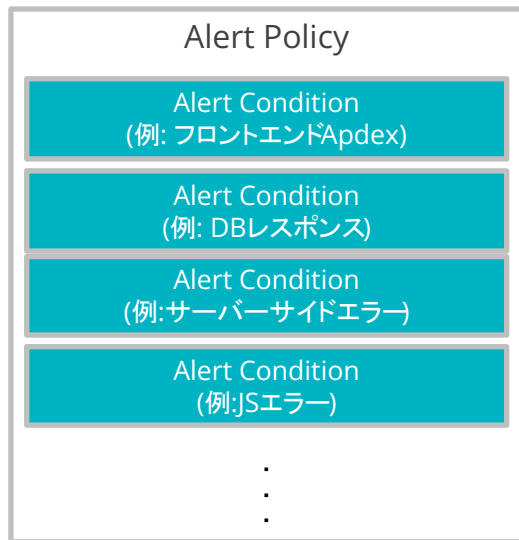


アラート機能の全体UIと重要メニュー



New Relic アラートの構成要素1: Alert PolicyとAlert Condition

New Relic のアラートは、Alert Policyという器にAlert Conditionを内包した構造となっている
Alert Policyは複数のAlert Conditionを内包し、送信先を制御できる
通常、送信先やアラートの目的別にポリシーを分けることが多い



The screenshot shows the New Relic Alert Policy configuration page. The title is "アラートポリシー" (Alert Policy) with an ID of "545592". It features a search bar for conditions and tabs for "2 Alert conditions" and "2 Notification channels". The page lists two alert conditions:

- INFRASTRUCTURE METRIC Disk Used**: Last modified Feb 5, 4:53 pm. Includes conditions like "diskUsedPercent > 90 for at least 2 mins" (critical) and "diskUsedPercent > 70 for at least 2 mins" (warning).
- APM APPLICATION METRIC BASELINE Web transaction throughput (Baseline)**: Last modified Nov 19, 3:38 pm. Includes conditions like "Web transaction throughput deviates from baseline for at least 5 mins" (critical) and "Web transaction throughput deviates from baseline for at least 5 mins" (warning).

New Relic アラートの構成要素1: Alert PolicyとAlert Condition

New Relicが収集しているデータを使って、Alert Conditionを作成できる

機能(例. APM, Browser等)ごとに簡単にアラートを作れる機能を持つ他、**汎用的なNRQL**を使い、自分でクエリを書いて細かなAlert Conditionを作成することも可能

1. Categorize

Select a product

NRQL

APM

Browser

Mobile

Synthetics

Infrastructure

New Relic アラートの構成要素1: Alert PolicyとAlert Condition

アラートのしきい値設定は2種類から選択可能

種類	説明	アラートトリガー例
静的(Static)	ある特定の数値を上回った、または下回った場合にアラートをトリガー	エラー発生割合が5%を超過した
動的(Dynamic) * baseline	いつもと異なる振る舞いをした場合にアラートをトリガー、どの程度の変動を許容するかを設定できる https://docs.newrelic.com/docs/alerts-applied-intelligence/new-relic-alerts/alert-conditions/create-baseline-alert-conditions	エラー発生割合がいつもよりも増加した

New Relic アラートの構成要素1: Alert PolicyとAlert Condition

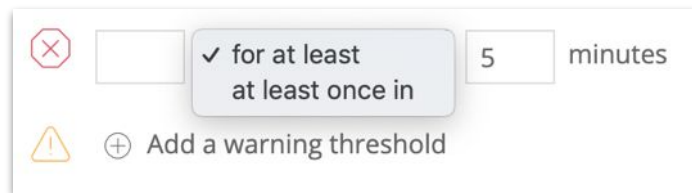
しきい値を超過した場合のアラート発報タイミング

- **For at least xx minutes**

しきい値をxx分継続して超過した場合のみ Incidentが起票される

- **at least once in xx minutes**

しきい値を1回でも超過した場合に Incidentが起票される



The screenshot shows a configuration interface for an alert condition. It features a dropdown menu with the selected option "for at least at least once in". To the right of the dropdown is a text input field containing the number "5", followed by the label "minutes". Below the dropdown is a button with a plus sign icon and the text "Add a warning threshold".

Alert ConditionはCriticalとWarning(オプション)2種類を作成可能

その他条件の設定に関する詳細は以下参照:

<https://newrelic.com/jp/blog/how-to-relic/alert-configuration-guidance>

New Relic アラートの構成要素1: Alert PolicyとAlert Condition

効果的な通知を送るためのプラクティス

- Additional settingsのcustom violation descriptionから発報されるアラートに詳細な情報を付加する様に設定することが可能 ([参考情報](#))
- Additional settingsのRunbook URLを設定することにより、アラート発報時に対応手順へのリンクにすぐにアクセスすることが可能

The screenshot shows the 'Additional settings' section of a New Relic alert policy configuration. It includes a dropdown menu for 'Close open violations after' set to '3 days', a link for 'Why is this required?', and two highlighted input fields: 'Add custom violation description' and 'Runbook URL' (containing 'http://').

Additional settings

Close open violations after: 3 days Why is this required? [↗](#)

+ Add custom violation description

Runbook URL

http:// [✕ Remove](#)


New Relic アラートの構成要素2: Incident Preference 1/2


New RelicはAlert Conditionの閾値を超過した場合は Incidentを起票する


Incident Preferenceの設定によって、Issueを起票する(Incidentをまとめる)粒度を設定できる


※アラートポリシーを作成する際に設定(後で編集可)

ISSUE CREATION PREFERENCE Specify how we create issues and group incidents into them. (You get notifications when an issue opens, is acknowledged, and closes.)

[① We streamlined our terminology. See what's changed](#) 

One issue per policy 
Group all incidents for this policy into one open issue at a time.

One issue per condition 
Group incidents from each condition into a separate issue.

One issue per incident 
No grouping. Create a separate issue for every incident.

[See our docs](#)

Correlate and suppress noise
Automatically correlate related incidents and issues to suppress noise, so you only get notified when you need to take action.
* Data is sent to the U.S. for processing.

New Relic アラートの構成要素2: Incident Preference 2/2

Issueの起票粒度について

例. 1つのAlert Policyに2つのAlert Conditionを設定し、その全てがCriticalになった

- フロントエンドのJSエラー率上昇(対象サイトは1つ)
- サーバーサイドのエラー率上昇(対象アプリケーションは3つ)

設定名	Issueの起票粒度	この例で起票される Issue
By Policy	ポリシーごと	1つ (ポリシー全体で1つ)
By condition	アラート条件ごと	2つ (JSエラーで1つ, サーバーサイドエラーで1つ)
By condition and signal	アラート条件と、その条件の対象となるエンティティ(構成要素)ごと	4つ (JSエラーで1つ, サーバーサイドエラーで3つ)

New Relic アラートの構成要素3: Workflows

Issueが起票された際に所定のデータを付与したり、通知先 (Destination) と関連づけて対象 Issue をどこに通知するのかをマッピングする機能

Filter data

- どのIssueとマッピングするかを定義する
- **Enrich**
 - Issue対象のEntityに関する付加情報を付与する
- **Mute issues**
 - Muting Rulesが設定されていた場合の挙動について定義する
- **Notify**
 - 通知先のDestinationを選択
- **Test workflow** (重要)
 - このworkflowの通知テストを実行

Configure your workflow

Enter a name you'll recognize
Give it a unique, descriptive name you'll recognize later

Filter data
Select the kinds of issues you want to send.
Select or enter attribute
+ AND

Additional settings ×
Enrich your data
Add more context to the issues by building NRQL queries to gather related data from across the New Relic platform

Mute issues
 Do not send notifications for fully muted issues
 Do not send notifications for fully or partially muted issues
 Always send notifications

Notify
Choose one or more destinations and add an optional message.
Add channel

ServiceNow incidents Webhook Jira Slack
 Email AWS EventBridge Mobile push PagerDuty

Test this workflow
We'll use existing data from your account to test what you've configured and send a sample notification.
Test workflow

New Relic アラートの構成要素4: Destinations

Issueのライフサイクルに応じた通知を受けることができる

デフォルトで各New Relic ユーザーは利用できる通知先として登録されている

Workflowsと関連づけると、以下の形式で通知される

- 登録メールアドレスに対する通知
- New Relicモバイルアプリ経由での通知

その他、追加で利用可能な通知先一覧は以下のとおりとなります

servicenow
now™

Webhooks


JIRA


Slack


Email 

Amazon
EventBridge


Pager Duty
pd 

Mobile push


重要: Email / Slack 内容の設定画面

The screenshot shows the 'Email' configuration screen. At the top, there is an 'Email' header with an envelope icon. Below it, a text field prompts the user to 'Select users and emails you want to send notifications to.' with a search icon and the text 'Search by name or email'. The 'Email subject' field contains the placeholder text '{{ issueTitle }}'. Under the 'Custom Details (optional)' section, a text area contains the instruction 'This payload uses Handlebars syntaxType "{{" to select from a list of variables.' At the bottom, there is a 'Send test notification' button and 'Cancel' and 'Save' buttons.

- [Workflows変数](#)を用いて柔軟に標題や内容のカスタムができるようになりました。
 - 補足: [custom violation description](#)とは別の情報付加機能となります。
- "{{"と入力することで、Workflows変数の補完機能を活用できます。

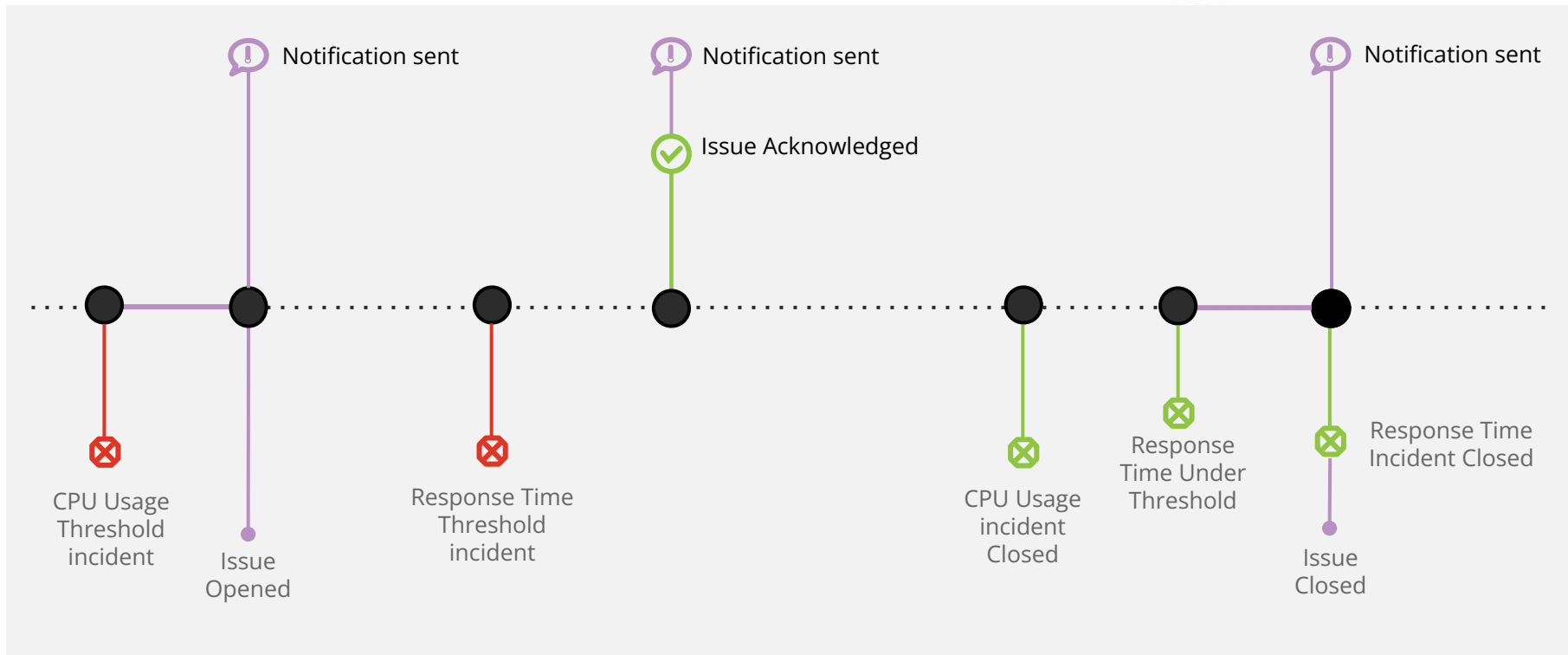
The screenshot shows the 'Slack' configuration screen. It features the Slack logo and the title 'Slack'. The 'Slack destination' section has a dropdown menu currently set to 'New Relic'. Below it, the 'Channel' section has a dropdown menu set to 'Select Channel...' and a warning icon with the text 'Your user is not authenticated'. The 'Custom Details (optional)' section has a text area with the instruction 'This payload uses Handlebars syntax. Type "{{" to select from a list of variables.' To the right of the form, there is explanatory text: 'Select where you want to receive notifications Pick an existing destination or create a new one. See our docs', 'Custom Details (optional) Add a custom message at the bottom of every Slack notification.', and 'You can also select from an array of custom variables. Just type "{{" or double-press the Shift key, then select from the menu. You can also customize these variables with a Handlebars library.' At the bottom right, there is a 'Send test notification' button.

Workflows variables:

<https://docs.newrelic.com/docs/alerts-applied-intelligence/applied-intelligence/incident-workflows/custom-variables-incident-workflows/>

補足: Issueのライフサイクルと通知タイミング

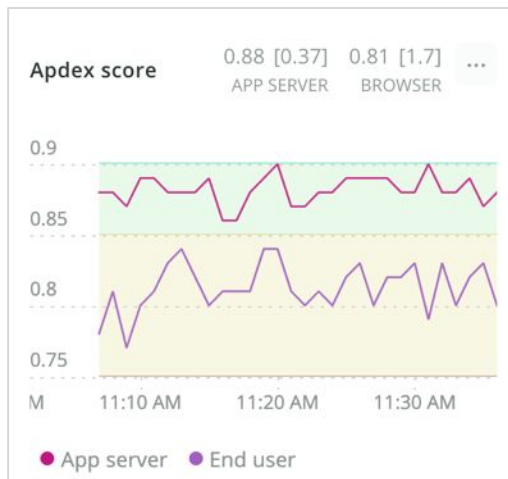
Issueの起票、Acknowledgeがされたタイミング、およびクローズの際に通知が届く



アラートを設定する前にやること

Apdex Tの値を適切に設定する

- Apdexはパフォーマンスに対するユーザーの満足度を示す指標
- 特にフロントエンドはエンドユーザー側のノイズに影響されやすいため、単純な応答時間の平均よりも有用な場合が多い



Application server

Apdex T is the response time threshold value for Apdex. Apdex T is the response time below which a user is satisfied with the experience. The default Apdex T threshold for an application server is 0.5 seconds. Apdex T applies to web transactions only.

Apdex T ?

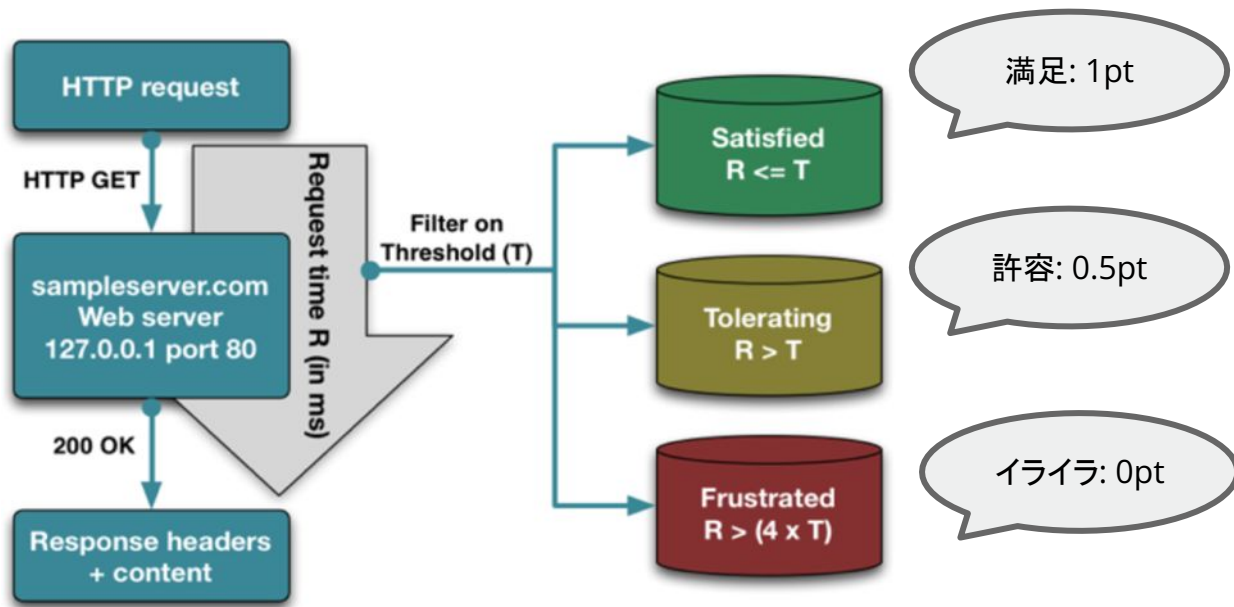
seconds

Please input a decimal or whole number only.

Apdex T値について

それを満たせばユーザーが満足すると想定される、最大応答速度

APMおよびBrowserのアプリケーションごとに設定可能 (Application Settingsメニュー)



ハンズオン(0) 環境を確認する

15:35 - 15:45 (10min)



**IMPORTANT**

ログインするNew Relicアカウントを切り替える

ログイン時に[Remember my email]にチェックをつけておくと、
Log outした際に次にどこのアカウントにログインするか選択する画面が表示されるようになります。
詳細は[ブログ](#)を参照

new relic

Log in to your account

Multiple accounts found. Verify your email to view all your accounts.

Email
japan-handson+2021@newrelic.com

Password

Remember my email ?

Log in

[Forgot your password?](#) [Trouble logging in?](#) [Create a free account](#)

NRU-User Full platform user
japan-handson+2021@newrelic.com

User preferences
API keys
Manage your plan

Administration

View settings
Theme **New** Light Dark Auto
NRQL console Show Hide

Add more data
Manage your data

Support >

Log out

new relic

Log in to your account

You have been signed out.

japan-handson+2021@newrelic.com
Original New Relic account

japan-handson+2021@newrelic.com
NewRelic.kk Default

[Use a different account](#)

ハンズオン環境へのログイン方法

[準備]

New Relicにログインしてください。 <https://login.newrelic.com/login>

- ユーザー: japan-handson+2021@newrelic.com
- パスワード: oSz6nrupas
(オー、エス、ゼット、ロク、エヌ、アール、ユー、ピー、エー、エス)

※本ハンズオンセミナーでは2つのNew Relicアカウントにログインします。

スムーズに切り替えを行うためにログイン時に [Remember my email]にチェックをつけてください
ログイン切り替えは次項参照

※普段NewRelicをお使いの方はセッションが残っている場合がありますのでプライベートブラウジングをお使いください。

- Chrome: シークレットウィンドウ
- Firefox: プライベートウィンドウ
- Edge: InPrivate ウィンドウ
- IE: New Relicの一部機能はIEをサポートしていません。上記のいずれかのブラウザをご利用ください。

今回監視対象のサイト

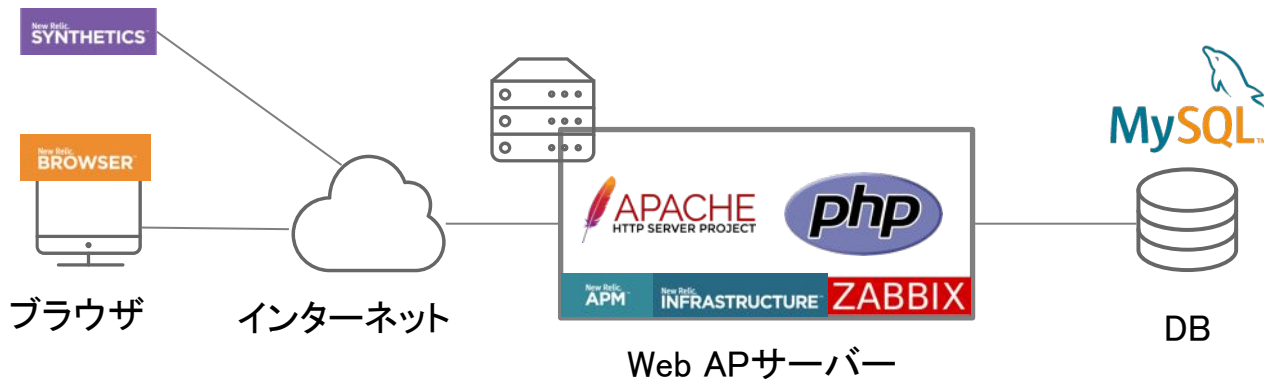
[NRUジェラートショップ](ECサイト)

<http://ec2-3-113-215-132.ap-northeast-1.compute.amazonaws.com/ec-cube/index.php>



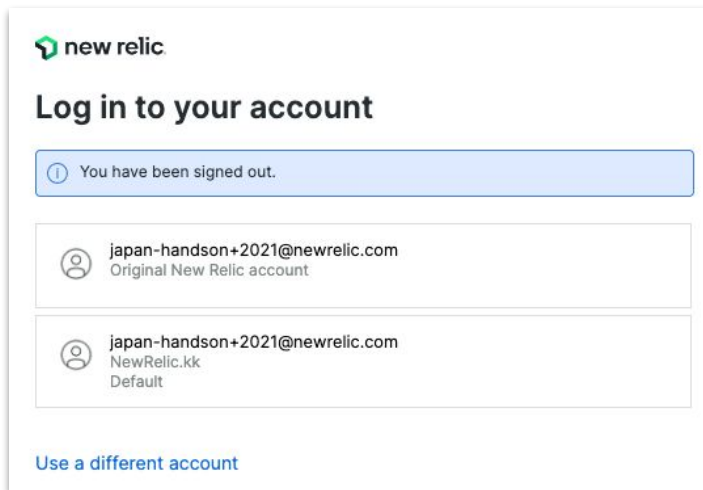
今回の環境の監視構成

- New Relic:
 - 外形監視, フロントエンド(ブラウザ), アプリケーション、インフラ
- Zabbix:
 - インフラ



ハンズオン(0) 2つのアカウントにログインする

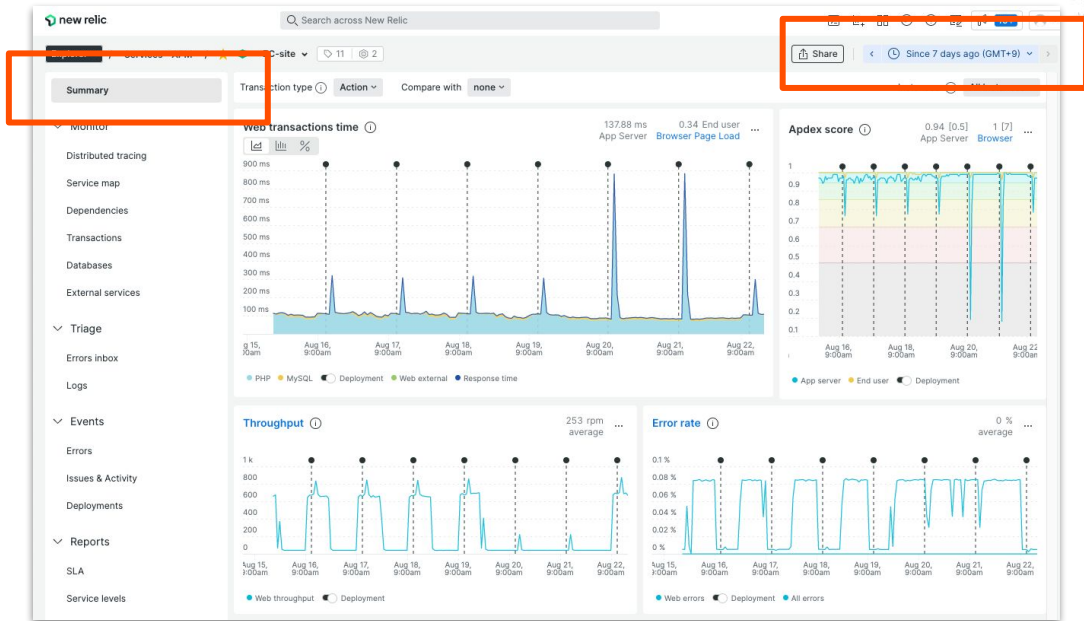
- ログイン先のアカウントを切り替えて確認頂くハンズオンが後半に予定されています。
- [こちら](#)の手順に従って、事前作業を行ないます。



ハンズオン(0) FSO UIの確認

- New Relicポータルの左ペインの”APM and services”を選択し、EC-siteアプリを選択します。
- Summaryが選択されていることを確認します。
- 表示するデータの表示幅を7 daysに変更します。

同様に、BrowserやInfrastructureを参照してください。



ハンズオン(0) Apdex Tの設定箇所の確認

変更は行わない!!!

- New Relicポータルの大メニューのAPM、あるいは左ペインのServices - APMを選択し、EC-siteアプリを選択します。
- Settings → Applicationを選択します。

EC-site

Application settings

Application alias

Set a name for this application in New Relic. You can change the name here without modifying the agent configuration file. This may take 5-30 minutes to propagate through your reporting agent.

Alias

EC-site

Application server

Apdex T is the response time threshold value for [apdex](#). Set a response time your users would consider satisfactory. The default apdex T for an application server is 0.5 seconds. This applies to web transactions only.

Apdex T ⓘ

0.5

Enter a decimal or whole number only.

ⓘ Any saved change will restart all agents for this application

ハンズオン(0) Alerts & AIの確認

変更は行わない!!!

詳細については、後ほどご説明します。

- Alert coverage gaps (Beta)にアクセスします。Alerts & AI → Alert coverage gaps
- EC-siteのAdd alertボタンを押します。

Alert coverage gaps
Some of your services don't have alerts set up. Our machine learning engine recommends adding these alerts. [See our docs](#)

0% covered 1 entities

Services - APM

Name	Throughput	Error Rate	Action
EC-site	39.35 req/min	0 %	Add alert

- 表示される一覧の中の任意の1つを選び、鉛筆アイコンをクリックします。
- (後ほど説明します。)アラートに関する設定 (condition)のUIが表示されます。
 - **表示を確認したら、保存などは一切行わずに、設定の UIを閉じてください。**

ハンズオン(0) Alerts & AIの確認

Alert coverage gaps

Some of your services don't have alerts set up. Our machine learning engine recommends adding these alerts. [See our docs](#)

0% covered 1 entities

Services - APM

Name	Throughput	Error Rate	Action
EC-site	39.35 req/min	0%	Add alert

変更は行わない!!!

Add an alert

EC-site

Add recommended conditions

Our power users add these conditions to similar entities.

- Critical EC-site - Error Percentage** Highly recommended
Threshold type: Baseline
Alert when this signal deviates from its normal baseline, upper and lower, for at least 5 minutes by 3.00 standard deviation(s).
- Critical EC-site - Apdex**
Threshold type: Baseline
Alert when this signal deviates from its normal baseline, upper and lower, for at least 5 minutes by 3.00 standard deviation(s).
- Critical EC-site - Response Time (Web)**
Threshold type: Baseline
Alert when this signal deviates from its normal baseline, upper and lower, for at least 5 minutes by 3.00 standard deviation(s).

Select policy to get notified

Looking for more options? [Set up an alert from scratch.](#)

Create an alert condition

Account: 251671 - NewRelicUniversity-Japan

Enter condition name
EC-site - Apdex

Define your signal
Enter NRQL Query
`SELECT apdex(apm.service,apdex) FROM Metric WHERE entity.guid = 'HjUwMTY3Mx8UE18QV80TE1DQVJRT85NDQJMDAwMDk3' FACET entity -guid`

Showing 1/1 time series

Preview charts are estimates only
These charts use your stored data to show how this signal might create incidents. They don't consider all aspects of streaming analytics (e.g., cadence, null values, signal loss, filed data gaps).

Set your condition thresholds
Threshold Type: Static Anomaly
Threshold direction: Upper and lower

ハンズオン(1) アラートを作成する

15:45 - 16:05 (20min)



今回の環境の監視構成

[前提]

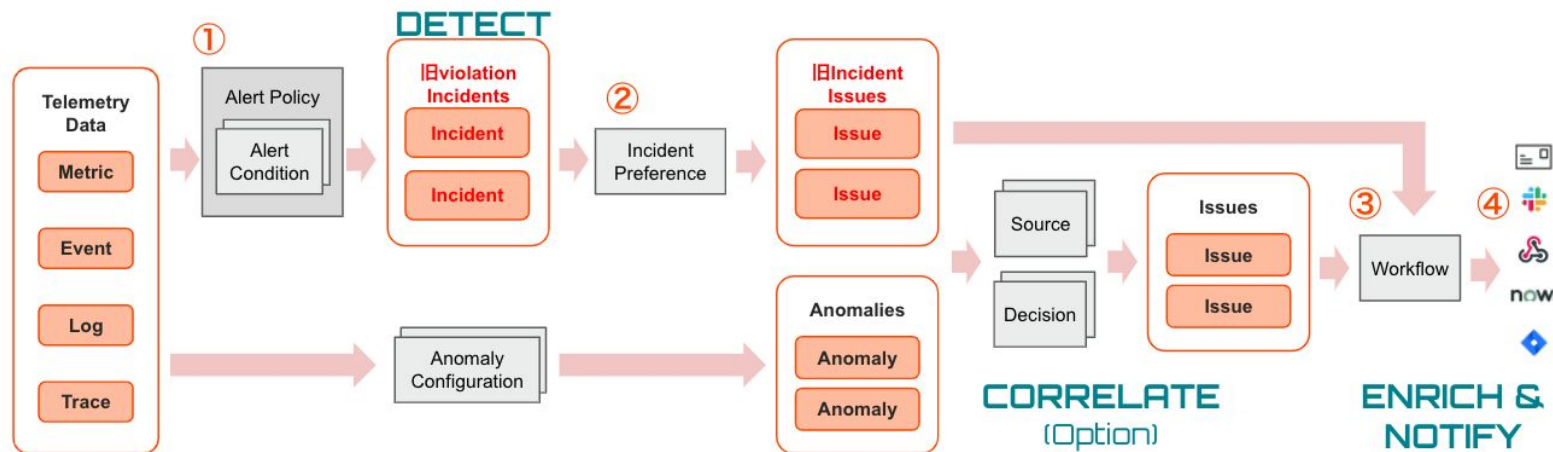
今回は**赤字**のアラートを設定してみます。

カテゴリ	現在起こっているサービス影響		将来のリスクの兆候	
具体例	サイトが遅い	エラーを返す	キャパシティを超える	リソースが枯渇する
外形監視	チェック応答時間	チェックエラー		
フロントエンド	Apdex	JSエラー		
アプリケーション	Apdex 応答時間	4xx, 5xxエラー	スループット バッチ遅延	
インフラ				各種インフラ リソース

ハンズオン(1)アラートを作成する

作業内容

1. Alert Policyを作成する
2. Alert Condition(4つ)を作成する
3. Workflowsを作成する





手順・解説

使用アカウント: NewRelic.kk
(ログイン先選択は[こちら](#)参照)

ハンズオン(1)-1 Alert policyを作成する 1/4

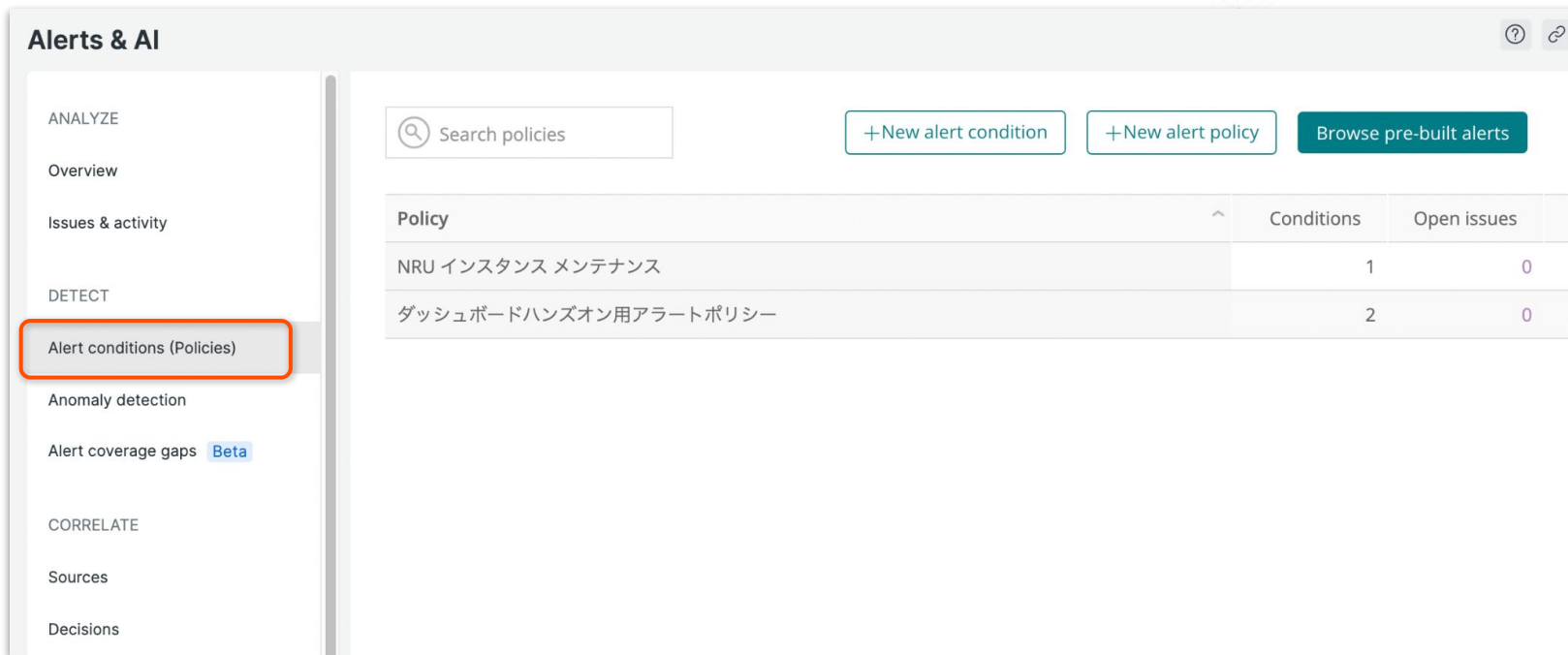
- Alerts & AI メニューを開きます。

The screenshot displays the New Relic Alerts & AI interface. The left sidebar contains a navigation menu with 'Alerts & AI' highlighted. The main content area shows a search bar with the text 'state = 'Active'' and a bar chart showing incident counts over time. Below the chart is a table of active incidents.

Sta...	Pri...	Created	Issue name	Entity name	Notified	Contains
Active	High	3h 52m ago	Problem started at 05:53:0...		1 incident	...
Active	High	6h 40m ago	Problem started at 03:04:3...		1 incident	...
Active	High	Dec 2, 202...	Problem started at 10:18:07...		1 incident	...

ハンズオン(1)-1 Alert policyを作成する 2/4

- 「Alert conditions (Policies)」をクリックします。

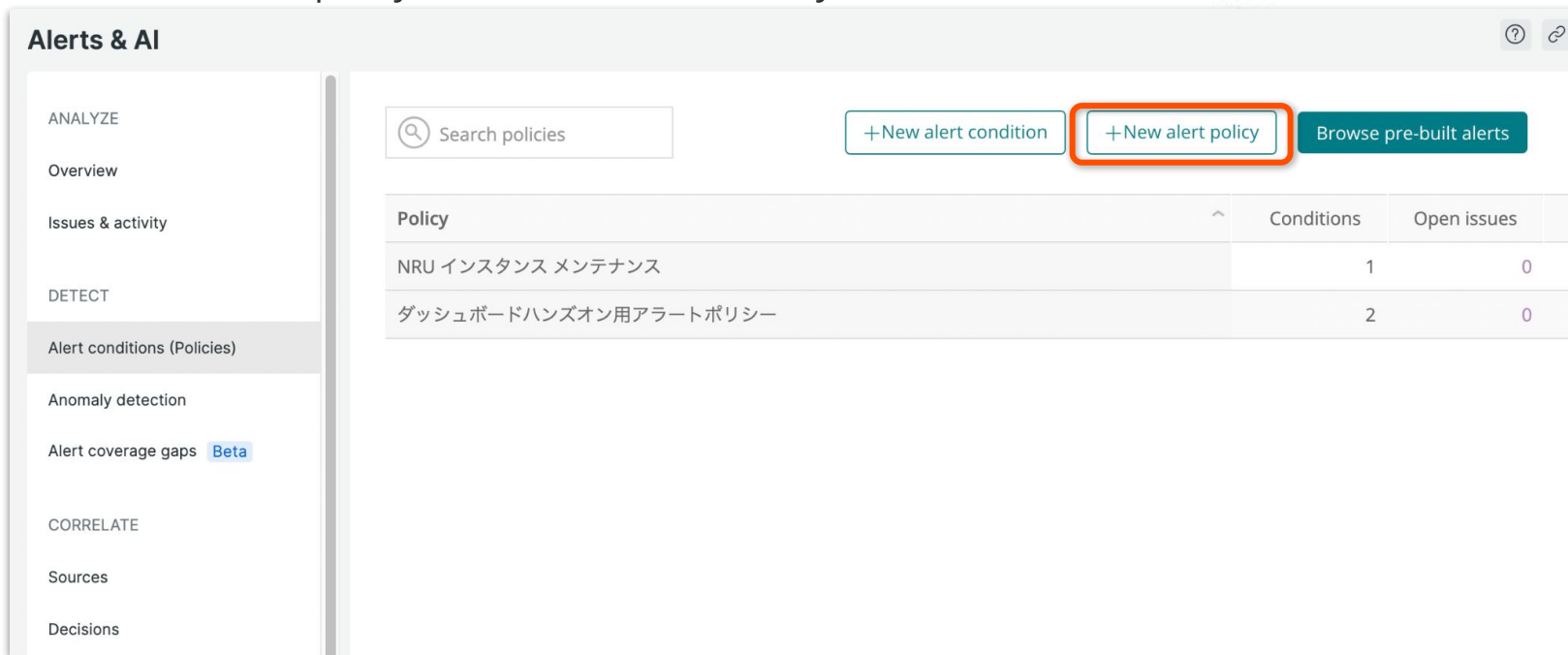


The screenshot shows the 'Alerts & AI' dashboard. On the left sidebar, the 'Alert conditions (Policies)' menu item is highlighted with a red box. The main content area displays a search bar, three buttons ('+New alert condition', '+New alert policy', 'Browse pre-built alerts'), and a table of existing policies.

Policy	Conditions	Open issues
NRU インスタンス メンテナンス	1	0
ダッシュボードハンズオン用アラートポリシー	2	0

ハンズオン(1)-1 Alert policyを作成する 3/4

- 「+ New alert policy」をクリックして新しい Policy を作成します。



The screenshot shows the 'Alerts & AI' interface. On the left is a navigation sidebar with categories: ANALYZE, Overview, Issues & activity, DETECT, Alert conditions (Policies), Anomaly detection, Alert coverage gaps (Beta), CORRELATE, Sources, and Decisions. The main area contains a search bar for policies, three buttons: '+New alert condition', '+New alert policy' (highlighted with a red box), and 'Browse pre-built alerts'. Below the buttons is a table of existing policies.

Policy	Conditions	Open issues
NRU インスタンス メンテナンス	1	0
ダッシュボードハンズオン用アラートポリシー	2	0

ハンズオン(1)-1 Alert policyを作成する 4/4

1. 自分用と判断できる名前を付けて AlertPolicyを作成します
2. [New Relic アラートの構成要素② Incident Preference 1/2](#) を参考に、好みの「INCIDENT PREFERENCE」を選択してください
3. [Create policy without notifications]をクリックします
 - a. あえてすべてのコンポーネントを手動で作成したため、ここではAlert policyのみを作成します

Create alert policy

ALERT POLICY NAME Give your policy a concise and descriptive name.

① nru-test-policy

ISSUE CREATION PREFERENCE Specify how we create issues and group incidents into them. (You get notifications when an issue opens, is acknowledged, and closes.)

① We streamlined our terminology. See what's changed [?](#)

② One issue per policy
Group all incidents for this policy into one open issue at a time.

One issue per condition
Group incidents from each condition into a separate issue.

One issue per incident
No grouping. Create a separate issue for every incident.

See our docs

Cancel

ハンズオン(1)-2 Alert Conditionを作成する 1/18

[前提]

今回は**赤字**のアラートを設定してみます。

カテゴリ	現在起こっているサービス影響		将来のリスクの兆候	
具体例	サイトが遅い	エラーを返す	キャパシティを超える	リソースが枯渇する
外形監視	チェック応答時間	チェックエラー		
フロントエンド	Apdex	JSエラー		
アプリケーション	Apdex 応答時間	4xx, 5xxエラー	スループット バッチ遅延	
インフラ				各種インフラ リソース

ハンズオン(1)-2 Alert Conditionを作成する 2/18

- 新規Alert Conditionの追加

4つのアラートを順番に設定していきます

1. 外形監視:チェックエラー
2. フロントエンド: Apdex(静的)
3. アプリケーション: 応答時間(動的)
4. アプリケーション: 4xx,5xxエラー(ホストごと発生数を設定する)

ハンズオン(1)-2 Alert Conditionを作成する 3/18

- Policyを作成したら「Create a condition」からconditionを作成します。

The screenshot shows the New Relic Alerts & AI interface. On the left is a dark sidebar with the New Relic logo and a navigation menu including Search, Add data, All capabilities, All entities, Alerts & AI (highlighted), APM & services, Apps, Browser, Dashboards, Errors inbox, Metrics & events, Hosts, Infrastructure, Logs, Mobile, Synthetic monitoring, Query your data, Serverless, Service levels, Help, and NRU-User. The main content area is titled 'Alerts & AI' and shows a policy named '参加者名 アラートポリシー' (id: 3759739). The policy has options for 'Correlate and suppress noise', 'Issue Creation Preference: One issue per policy', and 'Delete this policy'. Below these are '0 Alert conditions' (highlighted with a red box), 'Notification settings', and a link to 'Create a workflow to receive notifications'. The 'Alert conditions (Policies)' section is active, showing a gear icon and the message: 'This policy doesn't have any conditions. Alert conditions are the criteria for creating incidents. Notifications are sent when an issue opens, is acknowledged, and closes.' A 'Create a condition' button (highlighted with a red box) is visible at the bottom of this section.

ハンズオン(1)-2 Alert Conditionを作成する 4/18

- 外形監視:チェックエラー
- 監視設定は次のようにしてください。

1. Categories

- a. Synthetics -> Single failure

2. Select a monitor

- a. EC-CUBE-Checkout

ハンズオン(1)-2 Alert Conditionを作成する 5/18

- Categories を選択し、「Next, select entities」をクリックします。

New condition

⊗ Cancel

1. Categorize

Select a product

NRQL

APM

Browser

Mobile

Plugins

Synthetics

Infrastructure

Select a type of condition

Single failure

Multiple location failures

Next, select entities

ハンズオン(1)-2 Alert Conditionを作成する 6/18

- Select a monitor で「EC-CUBE-Checkout」を選択し「Next, define thresholds」をクリックします。

2. Select a monitor

Search monitors

Select: View: All (4) Selected (1) Unselected (3)

- EC-Cube-TOP
- EC-CUBE-Ping
- EC-CUBE-Checkout
- EC-CubeAdministrationPage

[← Back to Name and Categorize](#) [Next, define thresholds](#)

ハンズオン(1)-2 Alert Conditionを作成する 7/18

- コンディション名にわかりやすい名前を入力して「Create condition」をクリックします。

New condition

⊗ Cancel

1. Categorize

Synthetics - Single failure

2. Select monitor

1 monitor

3. Define thresholds

A violation occurs whenever a monitor fails a check

Name this condition

⊕ Add runbook URL

< Back to Select entity

Create condition

ハンズオン(1)-2 Alert Conditionを作成する 8/18

- コンディションが作成されました。名前やcategoryをクリックすれば設定を編集できます。

参加者名 アラートポリシー Connect to Incident Intelligence Incident preference: By policy Delete this policy

id: 1314626

1 Alert condition 0 Notification channels [Add a notification channel to receive alerts](#) Last modified 7:37 am by NRU-User

[Add a condition](#)

SYNTHETICS MONITOR FAILURE **わかりやすい通知名** Last modified 8:05 am by NRU-User [Edit](#) [Copy](#) [Delete](#) On

EC-CUBE-Checkout

Monitor check failure

[Add a condition](#)

ハンズオン(1)-2 Alert Conditionを作成する 9/18

- 新規Alert Conditionの追加

②フロントエンド: Apdex(静的)

1. **Categories:**

- a. Browser -> Metric

2. **Select entities:**

- a. EC-site



3. **Define thresholds**

- a. Critical: End User Apdexが5分間に1度でも(at least once)0.7を下回ったら(below)

Condition名は適切なものを各自設定してください

ハンズオン(1)-2 Alert Conditionを作成する 10/18

- 「+ Add a condition」をクリックすればPolicyにconditionを追加できます。

参加者名 アラートポリシー Connect to Incident Intelligence  Incident preference: By policy  Delete this policy

id: 1314626

1 Alert condition 0 Notification channels ① Add a notification channel to receive alerts Last modified 7:37 am by NRU-User

+ Add a condition

SYNTHETICS MONITOR FAILURE わかりやすい通知名 Last modified 8:05 am by NRU-User Edit Copy Delete On

EC-CUBE-Checkout

Monitor check failure

+ Add a condition

ハンズオン(1)-2 Alert Conditionを作成する 11/18

- Categories を設定します。

New condition

⊗ Cancel

1. Categorize

Select a product

NRQL APM **Browser** Mobile Plugins Synthetics Infrastructure

→ Browser Alerts can now be created using NRQL conditions. [Learn more](#)

Select a type of condition

Metric Metric baseline

Next, select entities

ハンズオン(1)-2 Alert Conditionを作成する 12/18

- Select entities で対象にするアプリケーションを選択します。

2. 1 entity selected

Select: All (1) None

View: All (1) Selected (1) Unselected (0)

EC-site

[← Back to Name and Categorize](#)

[Next, define thresholds](#)

ハンズオン(1)-2 Alert Conditionを作成する 13/18

- Thresholds を設定しわかりやすい名前を設定します。

3. Define thresholds

When target browser application

End User Apdex has an apdex score

Condition name

名前を追記 | End User Apdex (Low)

EC-site

03:00 AM 04:00 AM 05:00 AM 06:00 AM 07:00 AM 08:00 AM

● Apdex ● Critical threshold ● Critical violation

[← Back to Select entities](#)

ハンズオン(1)-2 Alert Conditionを作成する 14/18

- 2つめのconditionが作成されました。

2 Alert conditions 0 Notification channels ⓘ Add a notification channel to receive alerts Last modified 7:37 am by NRU-User

🔍 Search conditions ⊕ Add a condition

APM BROWSER APPLICATION METRIC 名前を追記 End User Apdex (Low) Last modified 8:28 am by NRU-User ✎ Edit 📄 Copy 🗑 Delete On

EC-site ⊕ Add entities

⊗ End User Apdex < 0.7 at least once in 5 mins

⚠ ⊕ Add a warning threshold

SYNTHETICS MONITOR FAILURE わかりやすい通知名 Last modified 8:05 am by NRU-User ✎ Edit 📄 Copy 🗑 Delete On

EC-CUBE-Checkout

⊗ Monitor check failure

ハンズオン(1)-2 Alert Conditionを作成する 15/18

- **新規Alert Conditionの追加**
 - ③アプリケーション: 応答時間(動的)
 1. **Categories**
 - a. APM -> Application metric baseline
 2. **Select entities**
 - a. EC-site
 3. **Define thresholds**
 - a. 次ページ参照

Condition名は適切なものを各自設定してください

ハンズオン(1)-2 Alert Conditionを作成する 16/18

- ベースラインアラートではスライダーで感度が変わります。

3. Define thresholds

Baseline Direction: New

When any target application

average deviates from the baseline minutes

Add a warning threshold

Condition Name

Add runbook URL

EC-site

2 critical violations Last 2 days

● Web transaction time ● Average web transaction time

To see values not visible in larger time windows, click and drag to zoom the chart

より敏感に

より鈍感に

[Back to Select entities](#) [Create condition](#)

ハンズオン(1)-2 Alert Conditionを作成する 17/18

- **新規Alert Conditionの追加**

④アプリケーション: 4xx,5xxエラー(ホストごとに評価)

- 1. Categories**

- a. NRQL

- 2. Enter a NRQL query and thresholds**

```
SELECT percentage(count(*), WHERE httpResponseCode >= '400') FROM Transaction facet host
```

- 3. Define thresholds**

- a. Critical: Staticで適宜好きな値(%)を設定してください

Condition名は適切なものを各自設定してください

ハンズオン(1)-2 Alert Conditionを作成する 18/18

- NRQLを入力すると自動的に参考となる Chartが表示されます。

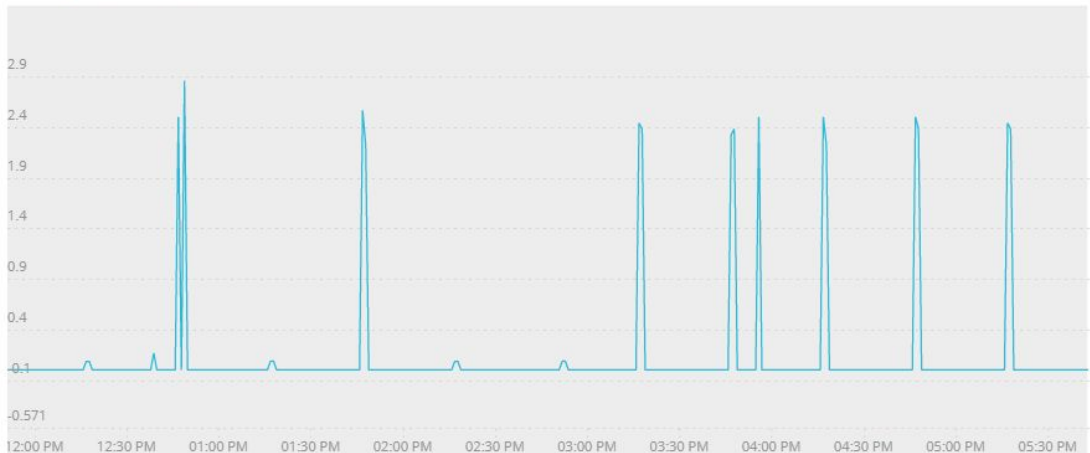
Define your signal

```
SELECT percentage(count(*), WHERE httpResponseCode >= '400') FROM Transaction facet host
```

What's possible with NRQL Alerting

Signal loss violations and filled data gaps are currently not reflected in the chart. [See our docs](#)

Showing 1/1 time series



ハンズオン(1)-3 Workflowsを作成する 1/6

1. Alerts & AIメニューのWorkflowsをクリックし、[+ Add a workflow]をクリックします
2. ご自身のworkflowsであることがわかる名前を入力します
3. Select Issuesで以下を選択します
 - a. Select or enter attribute: **policyName**
 - b. Select operator: **exactly matches**
 - c. Select or enter value: **作成したポリシーを選択**
4. Mute issues: デフォルトのまま

次のスライドに進みます

Configure your workflow
Use this flexible system to filter, enrich and send your alert data to the right destinations.
[See our docs](#)

Filter your data
Select the kinds of issues you want to send.

2 Name
kaizawa-test-workflows

3 Select issues
 Build a query Send all issues

policyName exactly matches nru-test-policy x

+ AND

We don't see any issues matching your filter. This doesn't mean it won't work.

Enrich your data
Build up to 5 NRQL queries to add more context to your issues.

Enrich (optional)
+ Build a query

Mute issues
You have rules in place that mute issues. Choose what to mute or ignore muting.
[See our docs](#)

4 Do not send notifications for fully muted issues
 Do not send notifications for fully or partially muted issues
 Always send notifications

Notify
Choose one or more destinations and add an optional message.

kaizawa@newrelic.com

ServiceNow incidents Webhook Jira Slack Email AWS EventBridge PagerDuty

Test this workflow
We'll use existing data from your account to test what you've configured and send a sample notification.

Test workflow We found a possible problem above.

Cancel **Activate workflow**

ハンズオン(1)-3 Workflowsを作成する 1/6

1. Alerts & AIメニューのWorkflowsをクリックし、[+ Add a workflow]をクリックします
2. ご自身のworkflowsであることがわかる名前を入力します
3. Filter dataで以下を選択します
 - a. Select or enter attribute: **policyName**
 - b. Select operator: **exactly matches**
 - c. Select or enter value: **作成したポリシーを選択**
4. Mute issues: デフォルトのまま

次のスライドに進みます

② **Configure your workflow**
NRU-Test-Workflow
Give it a unique, descriptive name you'll recognize later

③ **Filter data**
Select the kinds of issues you want to send.
accumulations.policyName v exactly matches 参加者名 アラートポリシー x

+ AND

Additional settings x
Enrich your data
Add more context to the issues by building NRQL queries to gather related data from across the New Relic platform

Mute issues
 Do not send notifications for fully muted issues
 Do not send notifications for fully or partially muted issues
 Always send notifications

Notify
Choose one or more destinations and add an optional message.
Add channel

ServiceNow incidents	Webhook	Jira	Slack
Email	AWS EventBridge	Mobile push	PagerDuty

Test this workflow
We'll use existing data from your account to test what you've configured and send a sample notification.
Test workflow

ハンズオン(1)-3 Workflowsを作成する 2/6

5. Notify: **Email**を選択します **(重要)**
6. メール送信内容を設定します
 - a. **ご自身のメールアドレスを入力して下さい。**
7. Send test notificationボタンをクリックし、指定したメールアドレスに通知メールが届くかを確認します
 - a. メール内容を確認します
 - i. Policy名やCondition名は確認できますか？
 - ii. Runbook情報URLはどこに記載されていますか？
 - iii. Tagsというセクションはありますか？

次のスライドに進みます

The screenshot shows the 'Notify' configuration screen in the New Relic workflow editor. At the top, there's a text input field for an email address, currently containing 'kalzawa@newrelic.com', with a red circled '5' next to it. Below this are several notification channel options: ServiceNow incidents, Webhook, Jira, Slack, Email (selected), AWS EventBridge, and PagerDuty. At the bottom, there's a 'Test this workflow' section with a 'Test workflow' button (circled in red '9') and a message 'We found a possible problem above.' (circled in red '10'). A 'Send test notification' button (circled in red '7') is located at the bottom left of the configuration area. A red circled '6' points to the 'Email subject' field, which contains the handlebars syntax '{{ issueTitle }}'. A red circled '8' points to the 'Send test notification' button. The 'ew relic' logo is visible in the bottom right corner.

ハンズオン(1)-3 Workflowsを作成する 3/6

7. Send test notificationボタンをクリックし、指定したメールアドレスに通知メールが届くかを確認します
 - b. 無事に手元に届いたことを確認の後に、⑥に戻り、Email subjectやCustom Detailsを変更します。再度Send test notificationをクリックし、どのようにメールの中身が変わるかを確認します。(色々試してみてください。)
 - i. 補足: 環境変数を利用する際は、"`{{`"と入力して開始して下さい。

8. Saveボタンを押します

次のスライドに進みます

The screenshot displays the New Relic workflow configuration interface. The top section is titled 'Notify' and includes a text input field for an email address (kalzawa@newrelic.com) and a grid of notification channel options: ServiceNow incidents, Webhook, Jira, Slack, Email, AWS EventBridge, and PagerDuty. Below this is the 'Test this workflow' section, which contains a 'Test workflow' button and a status message: 'We found a possible problem above.' At the bottom right of this section are 'Cancel' and 'Activate workflow' buttons. A second screenshot below shows the configuration for the 'Email' notification channel. It includes a search field for users and emails, an 'Email subject' field containing the variable `{{ issueTitle }}`, and a 'Custom Details (optional)' field with a note about Handlebars syntax. At the bottom of this section are 'Send test notification' and 'Save' buttons. Red circled numbers 5 through 8 are overlaid on the screenshots to indicate the sequence of steps described in the text.

ハンズオン(1)-3 Workflowsを作成する 4/6

9. Test workflowボタンを押し、テスト用メール内容を確認してください。
 - b. 先程のテスト用メールとどのような違いがあるかを確認してください
10. Active workflowボタンをクリックし、設定を保存します

The screenshot displays the New Relic workflow configuration interface. The top section is titled "Notify" and includes a text input field for an optional message, currently containing "katzawa@newrelic.com". Below this are several notification channel options: ServiceNow incidents, Webhook, Jira, Slack, Email, and AWS EventBridge. The "Email" option is selected. A red circled number 5 points to the email address field. Below the notification options, there is a "Test this workflow" section with a "Test workflow" button and a warning message: "We found a possible problem above." A red circled number 9 points to the "Test workflow" button. At the bottom right of this section are "Cancel" and "Activate workflow" buttons, with a red circled number 10 pointing to the "Activate workflow" button. The bottom section of the screenshot shows the "Email" configuration dialog. It has a search bar for selecting users and emails, an "Email subject" field with the placeholder "{ issueTitle }", and a "Custom Details (optional)" section. A red circled number 6 points to the "Email subject" field. At the bottom left of this dialog is a "Send test notification" button, with a red circled number 7 pointing to it. At the bottom right are "Cancel" and "Save" buttons, with a red circled number 8 pointing to the "Save" button. The New Relic logo is visible in the bottom right corner of the interface.

ハンズオン(1)-3 Workflowsを作成する 5/6

Workflows内でEmailを追加すると、Destinationも自動的に作成されます。

Alerts & AIメニューのDestinationsをクリックし、External addressとしてご自身のメールアドレスが追加されていることを確認します

Add a destination

Add destinations where we send notifications.

Jira ServiceNow Slack Webhook PagerDuty AWS EventBridge Mobile push

Notifications Log **Destinations (3)**

Manage destinations where we send notifications.

☰ Search

Type	Name	Two-way	URL/Details	Last updated	Updated by	Enabled	Status	
	External address		m_ogawa@atlas.jp	Aug 10, 2022 2:41pm	1001038720	<input type="checkbox"/>	DEFAULT	...
	NRU-User		japan-handson+2021@newrelic.com	Aug 10, 2022 2:41pm	1001038720	<input type="checkbox"/>	DEFAULT	...
	External address		kaojiri@gmail.com	Jun 6, 2022 7:49pm	1001038720	<input type="checkbox"/>	DEFAULT	...

ハンズオン(1)-3 Workflowsを作成する 6/6

メール通知をこのセッション中に無効にしたい場合、Enabledトグルボタンを無効化して下さい。

Add a destination
Add destinations where we send notifications.

Jira now. ServiceNow Slack Webhook PagerDuty AWS EventBridge Mobile push

Notifications Log Destinations (3)

Manage destinations where we send notifications.

Search

T...	Name	Two...	URL/Details	Last updat...	Updated by	Enabled	Status	
✉	External address	m_ogawa@atlas.jp		Aug 10, 2022...	1001038720	🔴	DEFAULT	...
✉	NRU-User	japan-handson+2021@newrelic...		Aug 22, 2022...	1001038720	🟢	DEFAULT	...
✉	External address	kaojiri@gmail.com		Jun 6, 2022 7...	1001038720	🔴	DEFAULT	...



✉	NRU-User	japan-handson+2021@newrelic...	Aug 22, 2022...	1001038720	🟢	DEFAULT	...
---	----------	--------------------------------	-----------------	------------	---	---------	-----

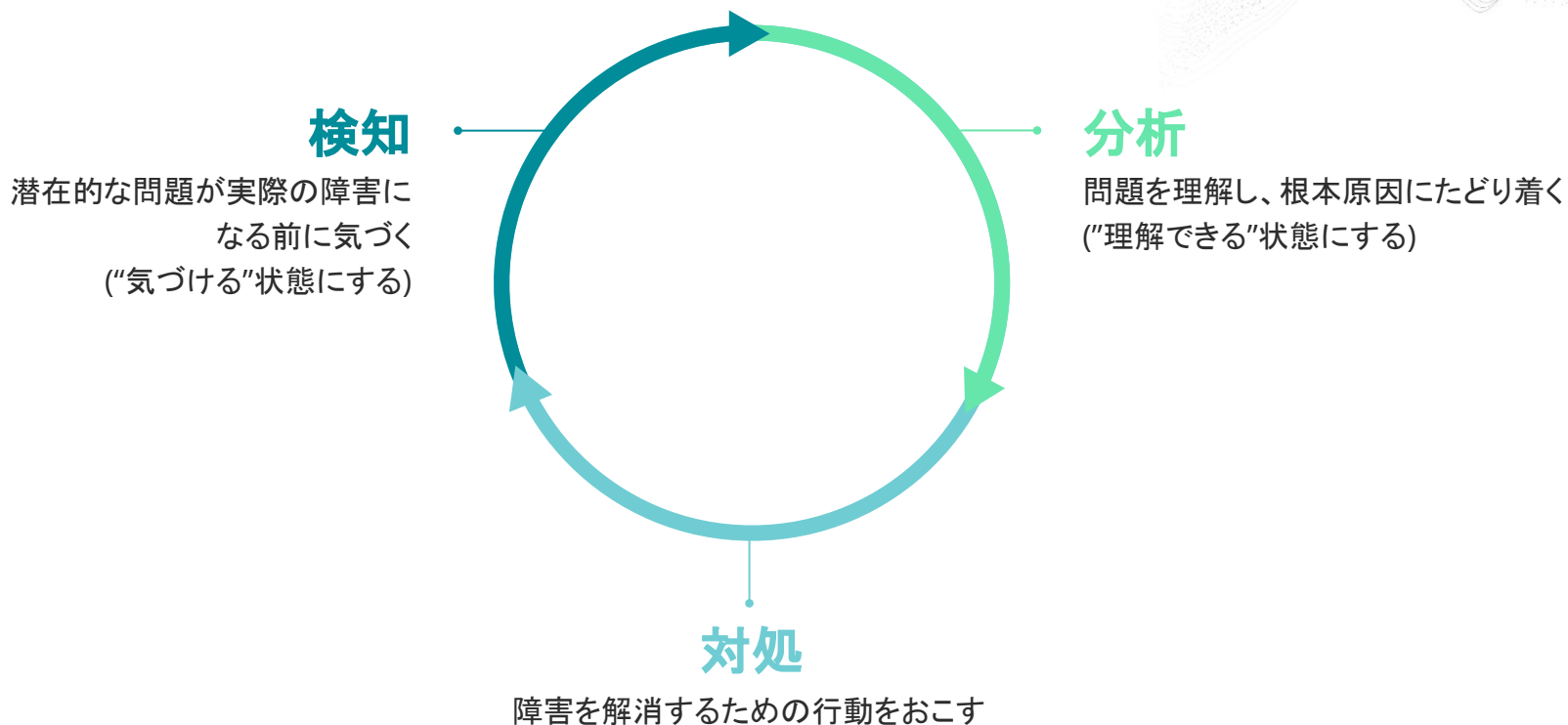


座学(3) New RelicのAIOps機能

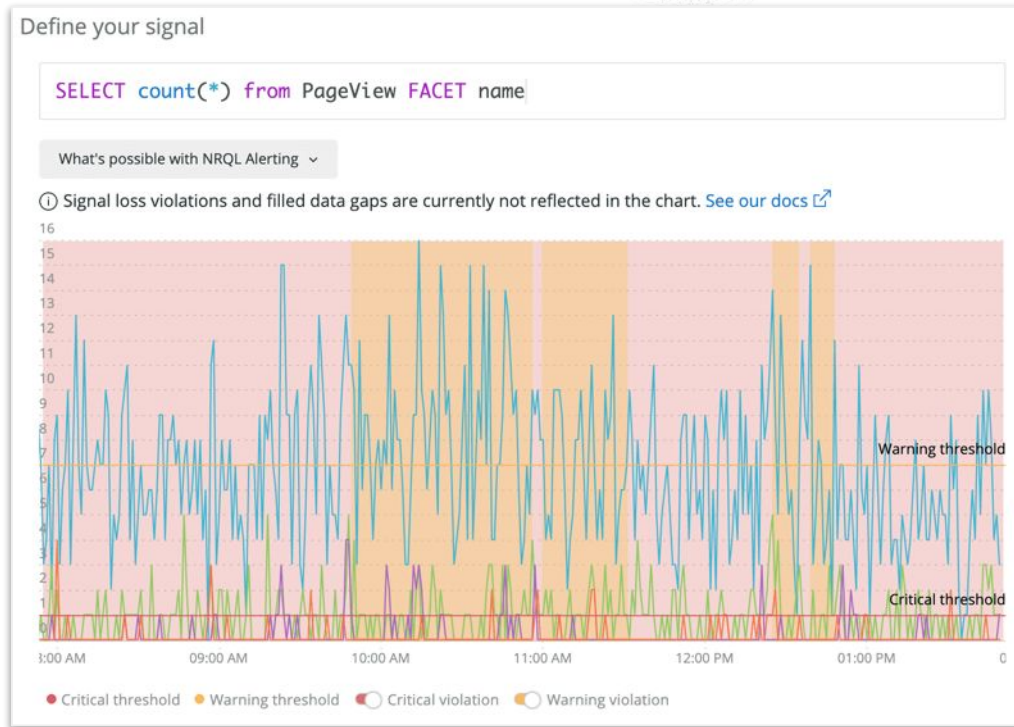
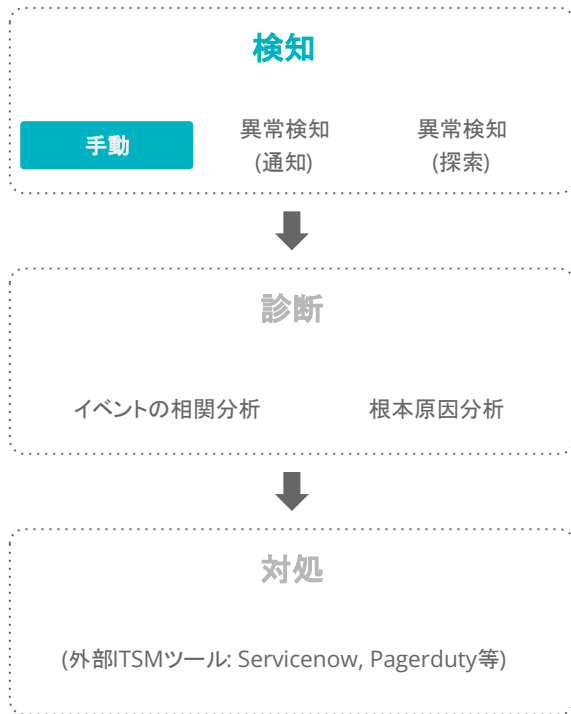
16:05 - 16:15 (10min)



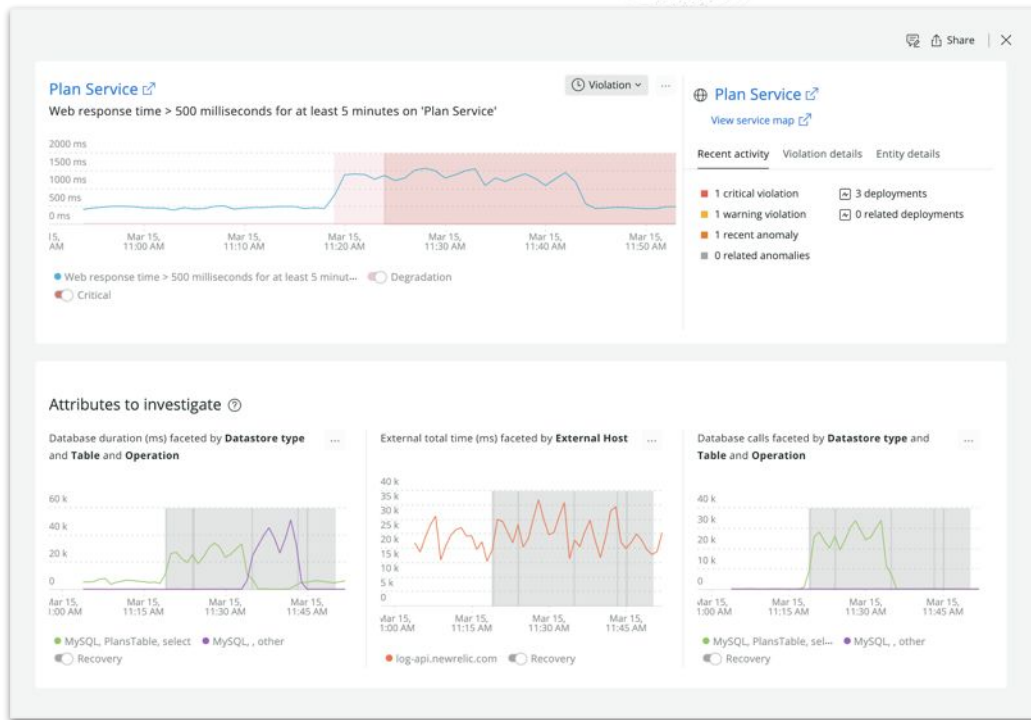
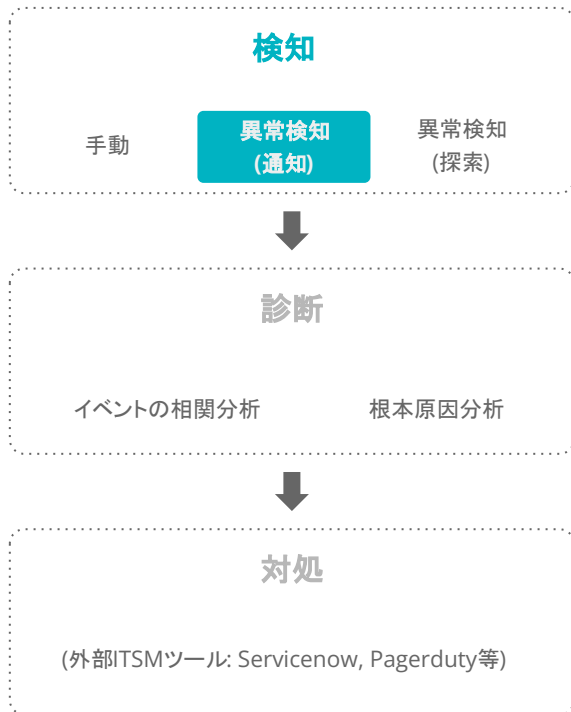
New Relic AIOpsによるインシデント対応フロー



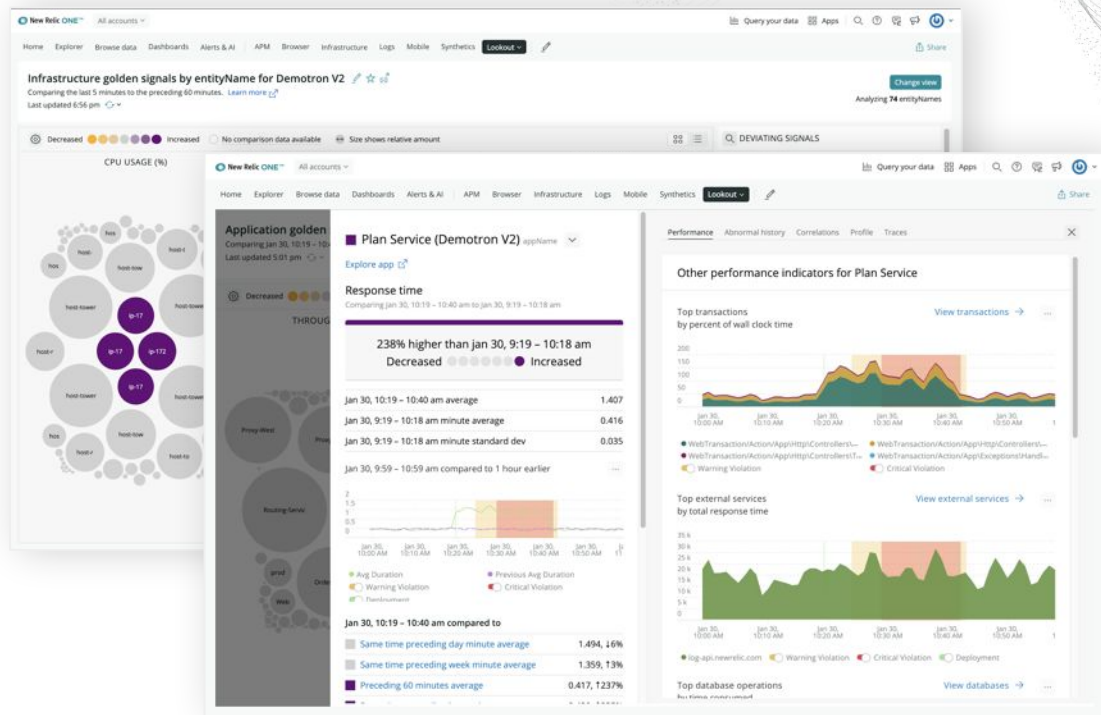
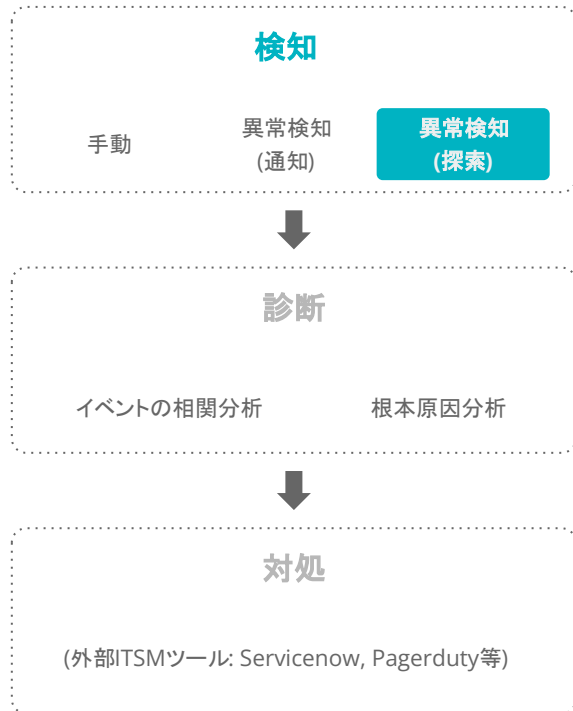
検知1: 重要な指標に対する手動アラートによる気づき



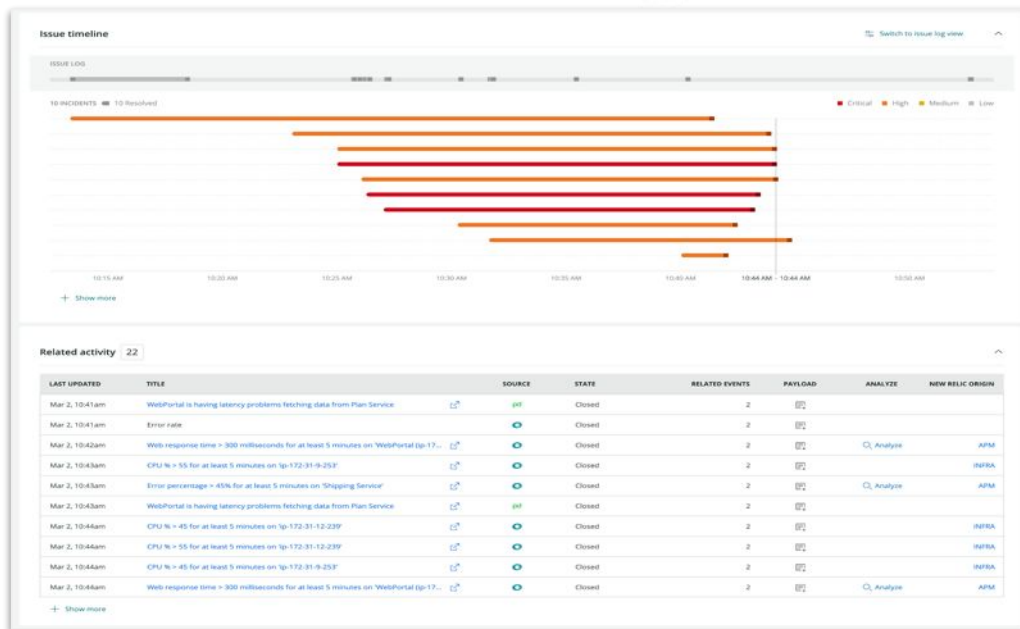
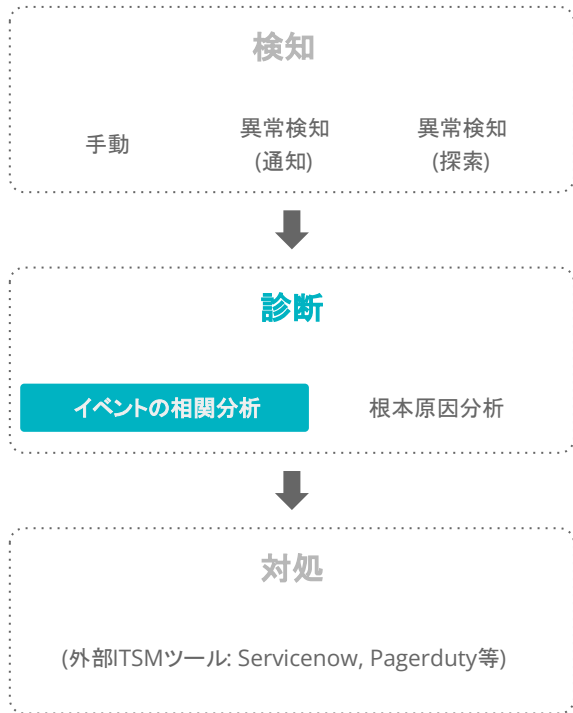
検知2: Anomaly Detectionによる異常の通知



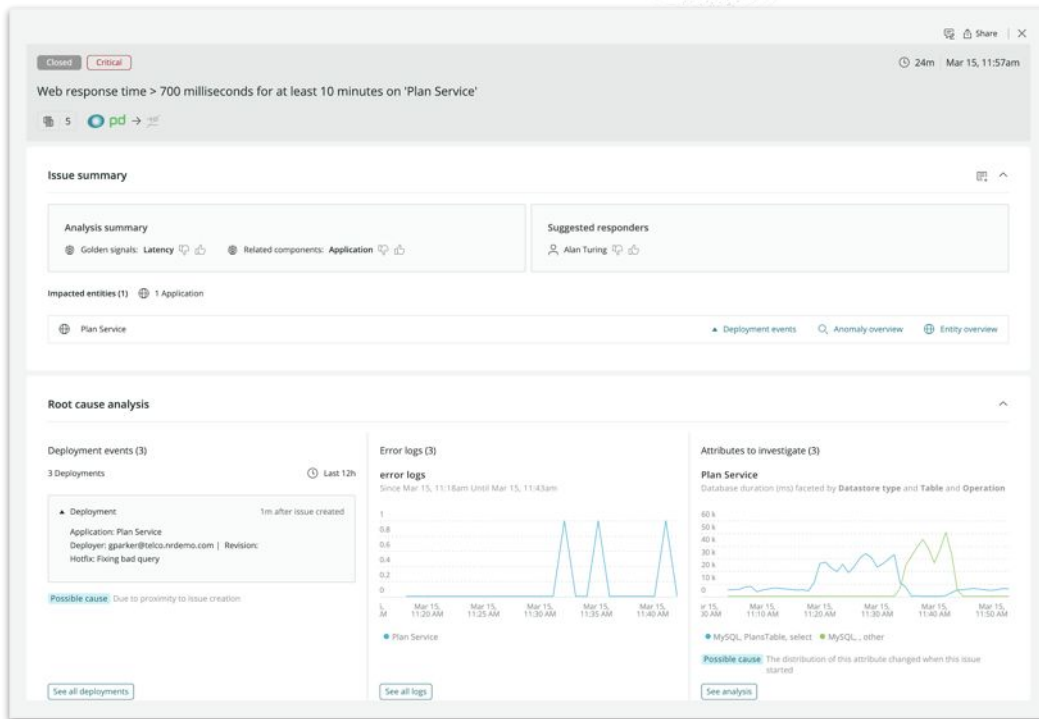
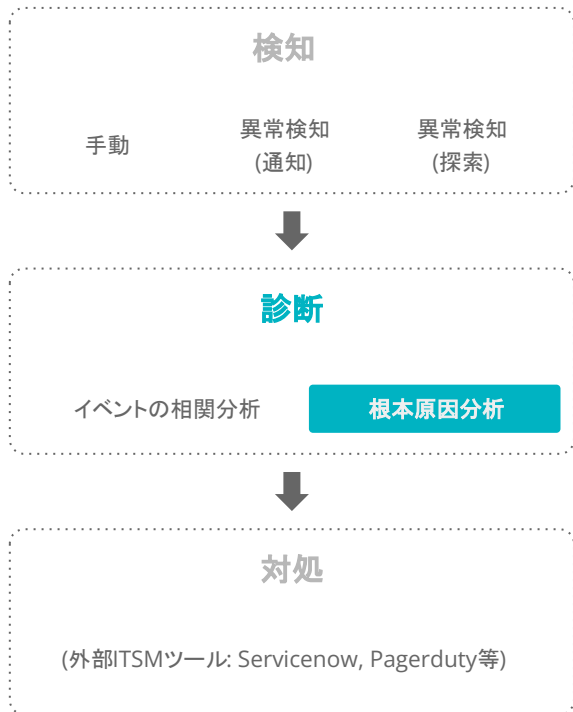
検知3: Lookoutによる異常の可視化と探索



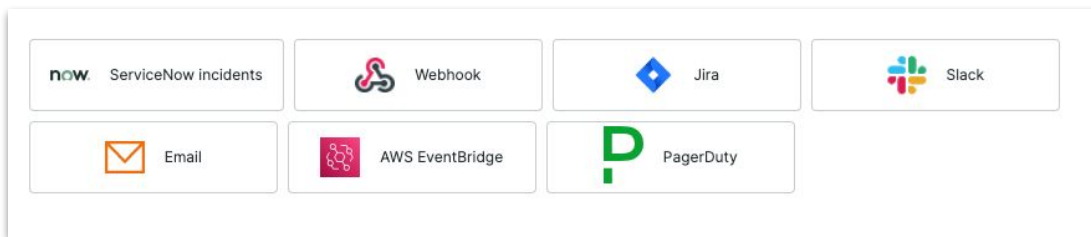
診断1: Correlationによるアラート統合とノイズの削減



診断2: Correlationによる根本原因の示唆



対処: ITSMツールと連携しアクションを実行



ハンズオン(2) AIOpsを使った異常検知 と原因分析

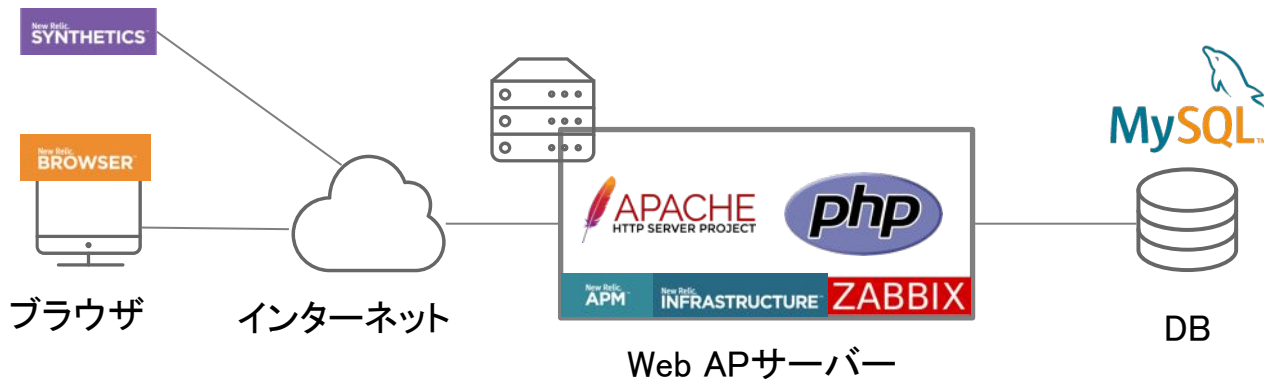
16:15 - 16:30 (15min)

※使用アカウント: NewRelic.kkとOriginal newrelic account
(ログイン先選択は[こちら](#)参照)



今回の環境の監視構成(再掲)

- New Relic:
 - 外形監視, フロントエンド(ブラウザ), アプリケーション、インフラ
- Zabbix:
 - インフラ



ハンズオン(2)

1. 異常を可視化する

[目的]

AIOpsの異常検知の仕組みを使い、異常を可視化する機能を学びましょう

- Topメニューの"More"から"Lookout"を選択
 - 何が表示されているか確認しましょう
 - 目的に応じたカスタムのビューを作ってみましょう

注: Lookoutを見るときだけ、New Relic Original Accountにログインしてください
(詳細は[こちら](#))

ハンズオン(2)

2. 個々のアラートを確認する

[目的]

AIOpsに送られたアラートを把握します (後続の演習の事前確認)

- Alerts&AI -> Overview -> Incidentsで、Open中のアラートを確認する
 - それぞれ、Originがなにかを確認しましょう
 - メッセージから、どのようなアラートかを推測してみましょう

ハンズオン(2)

3. 複数のアラートを紐付け、トラブルシューティングに役立てる

[目的]

2で確認した個々のアラートがどのように紐付けられ、分析されているかを確認しましょう

- Alerts&AI -> Overview -> Issueで、Active中のIssueを確認する
 - それぞれ、どのようなアラートが紐付いているかを確認しましょう
 - Root cause analysisにどのような項目が書かれているでしょうか

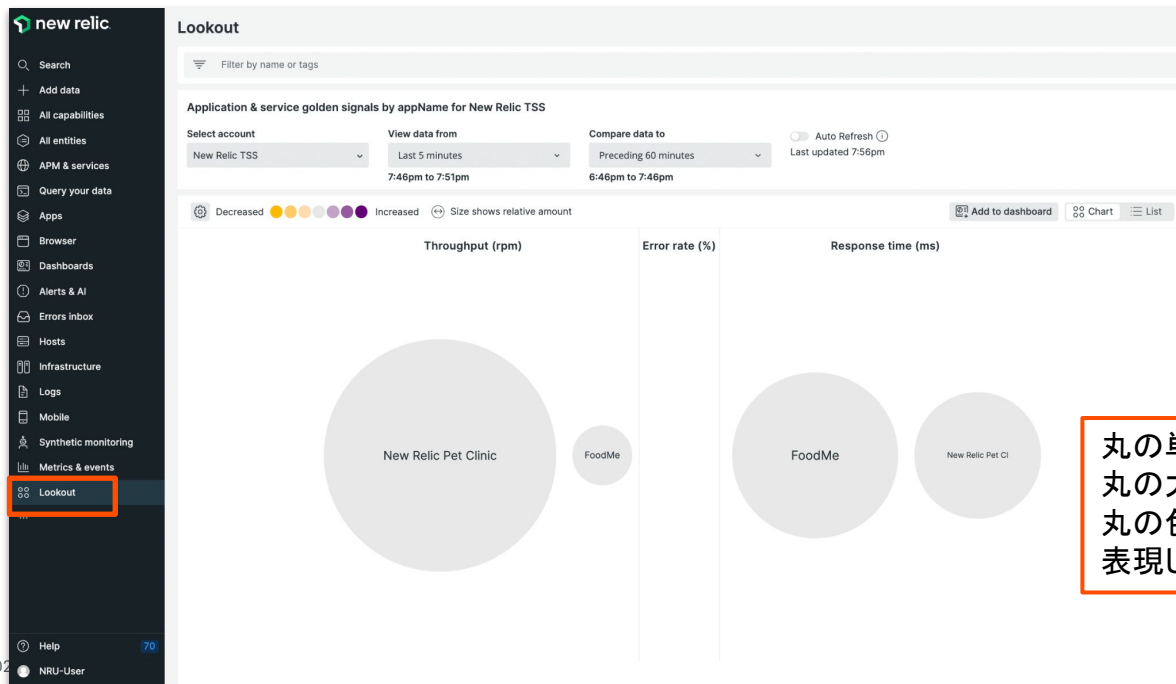


手順・解説

使用アカウント: NewRelic.kkとOriginal New Relic Account
(ログイン先選択は[こちら](#)参照)

ハンズオン(2)異常を可視化する

- Original New Relic Account側にログインします(詳細手順は [こちら](#))
- メニューから「Lookout」をクリックし、現れた画面上でサービスの現状を読み解きましょう



丸の単位はアプリケーション単位です
丸の大きさは値の大きさを、
丸の色は異常が発生しているかどうかを
表現しています

ハンズオン(2)異常を可視化する

- 気になる○(丸)を選択し、どのような変化が生じているか、詳細を確認します

The screenshot displays the New Relic Lookout interface for the 'New Relic Pet Clinic' application. The main section shows a 'Throughput' metric that is '1% lower than the preceding 60 minutes', with a 'Decreased' status indicator. A table provides comparison windows: Last 5 minutes average (552.8), Preceding 60 minutes minute average (557.3), and Preceding 60 minutes minute standard dev (72.6). Below this is a bar chart comparing the last 5 minutes to the preceding 60 minutes. The right sidebar shows the 'Performance' tab selected, with a close button (X) highlighted. Below the tab menu, there are sections for 'Other performance indicators for New Relic Pet Clinic', 'Top transactions by percent of wall clock time' (with a chart showing various transaction types), and 'Top errors by error class'.

見終わったらxを押して閉じます

各タブをクリックしてどのような情報が
見えるか見てみましょう

ハンズオン(2)異常を可視化する

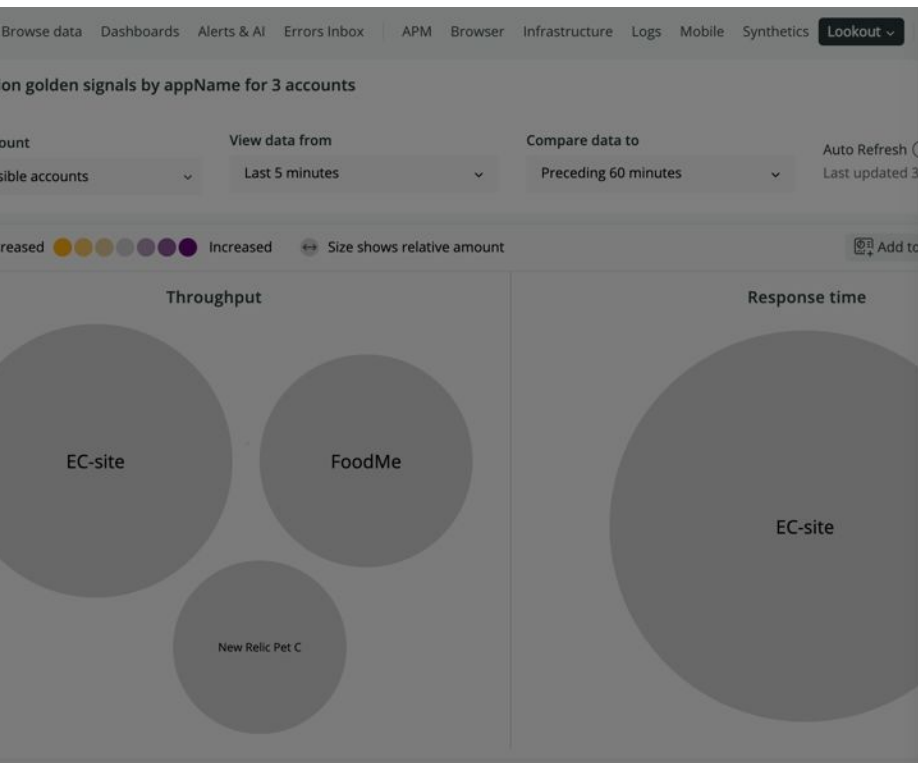
- カスタムのビューを作成します

Manage Views -> Create a new queryを選択

The screenshot displays the New Relic Lookout interface. At the top, the title 'Lookout' is visible. Below it is a search bar with the text 'Filter by name or tags'. The main content area is titled 'Application & service golden signals by appName for New Relic TSS'. It includes several configuration options: 'Select account' (New Relic TSS), 'View data from' (Last 5 minutes, 7:46pm to 7:51pm), 'Compare data to' (Preceding 60 minutes, 6:46pm to 7:46pm), and 'Auto Refresh' (Last updated 7:56pm). A legend indicates 'Decreased' (yellow) and 'Increased' (purple) with a note 'Size shows relative amount'. There are buttons for 'Add to dashboard', 'Chart', and 'List'. The dashboard contains three panels: 'Throughput (rpm)', 'Error rate (%)', and 'Response time (ms)'. The 'Throughput (rpm)' panel shows a large bubble for 'New Relic Pet Clinic' and a smaller one for 'FoodM'. The 'Response time (ms)' panel shows bubbles for 'FoodMe' and 'New Relic Pet'. On the right side, a 'Deviating services' panel shows a search icon and the text 'We found no significant deviation in appnames from the prior time window.' A 'Manage Views' dropdown menu is open, showing options: 'Open a saved view', 'Edit current query', 'Create a new query', 'Save view', and 'Save view as...'. The 'Create a new query' option is highlighted with a red box.

ハンズオン(2)異常を可視化する

- カスタムのビューを作成します(続き)。作成後の画面から詳細分析ができます。
この手順によりアクセス先URLごとのレスポンスの多さと速さの大きさ、変化率が可視化できます。



Create a new query

Select account

All accessible accounts

Select data type

Metrics

Events

①Eventsを選択

Or write a NRQL query

②Select your event ->
Build a custom queryから
Transaction->countを選択

View a chart with

Transaction : count

Transaction : average : duration

+ Add row

X

Filter

Refresh

Close

Copy

Facet by

request.uri

③Add rowし、同じ要領でTransaction
->average->durationを選択

④request.uriを選択

View data from

Last 5 minutes

Compare data to

Preceding 60 minutes

Name your view (optional)

csasaki

⑤ご自身の名前を入力

⑥Create New Viewを押す

Create New View

ハンズオン(2)個々のアラートを確認する

- NewRelic.kkアカウントにログインし直します
- Alerts&AI、[Overview]をクリックします

The screenshot displays the New Relic Alerts & AI dashboard. On the left, a dark sidebar contains navigation options, with 'Alerts & AI' selected. The 'Overview' tab in the main content area is highlighted with a red border. Below the navigation, the dashboard is organized into sections: 'ANALYZE' (containing 'Issues & activity'), 'DETECT' (containing 'Alert conditions (Policies)', 'Anomaly detection', and 'Alert coverage gaps Beta'), and 'CORRELATE'. On the right, a search bar is present above a chart titled 'Opened violations by priority' for the period 'Since 3 days ago'. The chart shows three blue bars representing critical violations at Dec 02, 9:00am, Dec 02, 3:00pm, and Dec 02, 9:00pm, each with a value of 1.5. A legend indicates that blue dots represent 'critical' violations.

Time	Priority	Count
Dec 02, 9:00am	critical	1.5
Dec 02, 3:00pm	critical	1.5
Dec 02, 9:00pm	critical	1.5

ハンズオン(2)個々のアラートを確認する

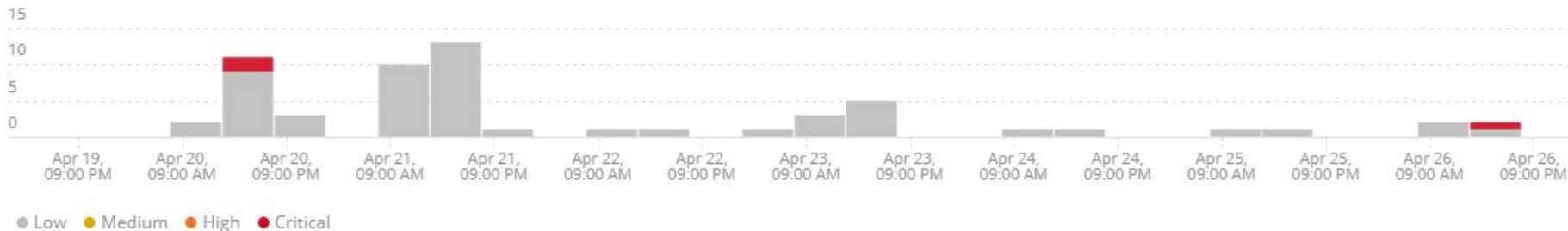
- 「Issues & Activity」>「Incidents」タブをクリックします。

The screenshot shows the New Relic Alerts & AI interface. The left sidebar contains navigation options, with 'Alerts & AI' selected. The main content area is titled 'Alerts & AI' and has a sub-tab 'Incidents' highlighted with a red box. A yellow warning banner at the top of the main content area reads: 'This page is going away soon. To analyze incidents side-by-side with other related activity, check the issues page. See your issues'. Below the banner is a search bar and a bar chart showing incident counts by severity (Low, Medium, High, Critical) over time. The chart shows several incidents, with the highest count being 4 incidents on Dec 04, 2:59pm. Below the chart is a table of incident details.

STAL...	PRI...	INCID...	CRE...	D.	ENTIT...	ANAL...	SOU...	EVEN...	MUTED
<input type="checkbox"/>	Closed	Critical	EC-site query res...	Dec 4, 2022 2	12m	EC-site	Compone...		2
<input type="checkbox"/>	Closed	Critical	EC-site query res...	Dec 4, 2022 2	12m	EC-site	Compone...		2
<input type="checkbox"/>	Open	High	Problem started at...	Dec 4, 2022 2	18h 35m		API		1

ハンズオン(2)個々のアラートを確認する

- 個々のIncidentをクリックします。



	STATE	PRIORITY	INCIDENT NAME	CREATED	DURATION	ENTITIES	ANALYSIS SUMMARY	SOURCE	EVENTS
<input type="checkbox"/>	Closed	Low	[PROBLEM] Load average is too...	4h 49m ago	14m			→	2
<input type="checkbox"/>	Closed	Critical	Web response time > 2 secon...	4h 50m ago	12m	EC-site	Signal: Latency Components: ...		2
<input type="checkbox"/>	Closed	Low	[PROBLEM] ip-172-31-26-...	7h 30m ago	9m			→	2
<input type="checkbox"/>	Closed	Low	[PROBLEM] High	9h 5m ago	1m			→	2

ハンズオン(2)個々のアラートを確認する

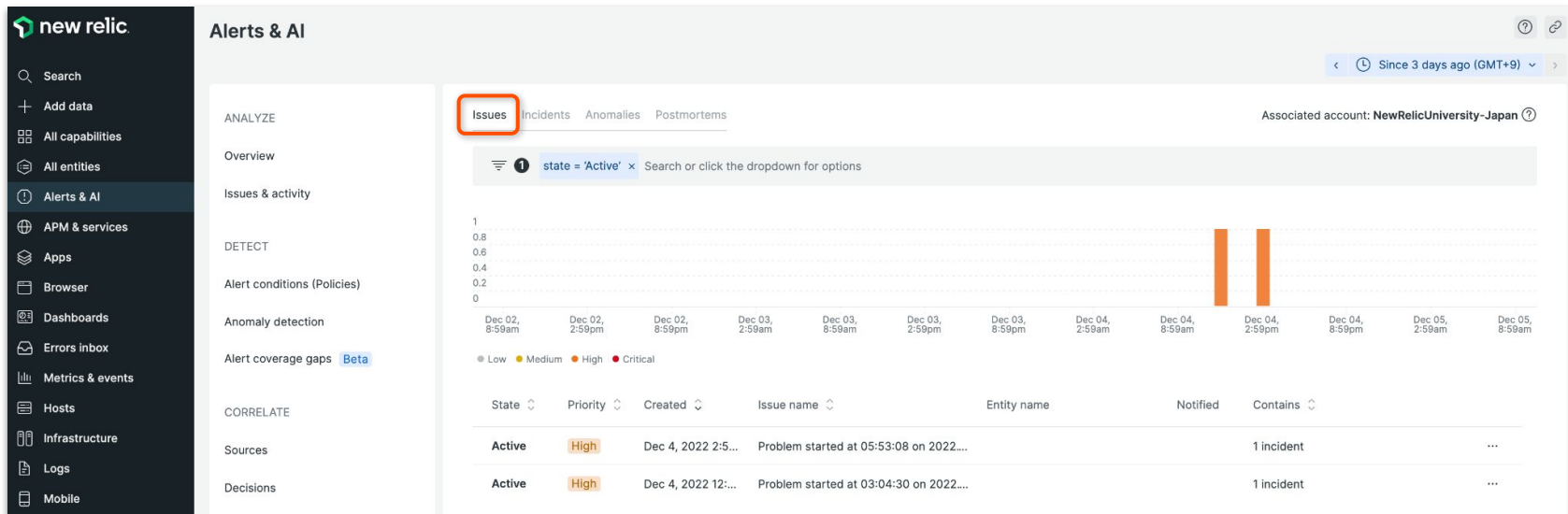
- Origin Key の値を確認することで、どのツールによって判定されたアラートかを確認することができます。

The screenshot displays the New Relic alert interface. On the left, a line graph shows the 'Web response time deviated from the baseline at least once in 5 minutes on 'EC-site'' with a red shaded area indicating the alert period between 12:20 PM and 12:40 PM. Below the graph is an 'Analysis' section with 'Attributes' and 'Anomalies' subsections, both indicating no findings. The right side shows incident details for 'EC-site', including the condition 'Web transaction time (Baseline)', policy 'test deleteme', and issue 'テスト太郎さんのEnd User Apex (Low)'. A 'View incident payload' button is highlighted with a red box. To the right of the incident details is a table titled 'Incident accumulation' with a 'Copy payload' link. The table lists various keys and values, with 'origin' and 'newrelic' highlighted by a red box.

Key	Value
source	newrelic
origin	newrelic
conditionName	Web transaction t...
policyName	test deleteme
conditionFamilyId	24384045
policy.rollupStra...	PER_POLICY
evaluation.name	HttpDispatcher

ハンズオン(2)複数のアラートを紐付け トラブルシューティングに役立てる

- 「Issues」タブをクリックします。



The screenshot displays the New Relic Alerts & AI dashboard. The left sidebar contains navigation options such as Search, Add data, All capabilities, All entities, Alerts & AI (highlighted), APM & services, Apps, Browser, Dashboards, Errors inbox, Metrics & events, Hosts, Infrastructure, Logs, and Mobile. The main content area is titled 'Alerts & AI' and includes tabs for ANALYZE, Overview, Issues & activity, DETECT, Alert conditions (Policies), Anomaly detection, Alert coverage gaps (Beta), CORRELATE, Sources, and Decisions. The 'Issues' tab is selected and highlighted with a red box. Below the tabs, there is a search bar with the filter 'state = 'Active'' and a search button. A bar chart shows the number of active issues over time, with two prominent orange bars on Dec 04. Below the chart is a table of active issues.

State	Priority	Created	Issue name	Entity name	Notified	Contains
Active	High	Dec 4, 2022 2:5...	Problem started at 05:53:08 on 2022...			1 incident
Active	High	Dec 4, 2022 12:...	Problem started at 03:04:30 on 2022...			1 incident

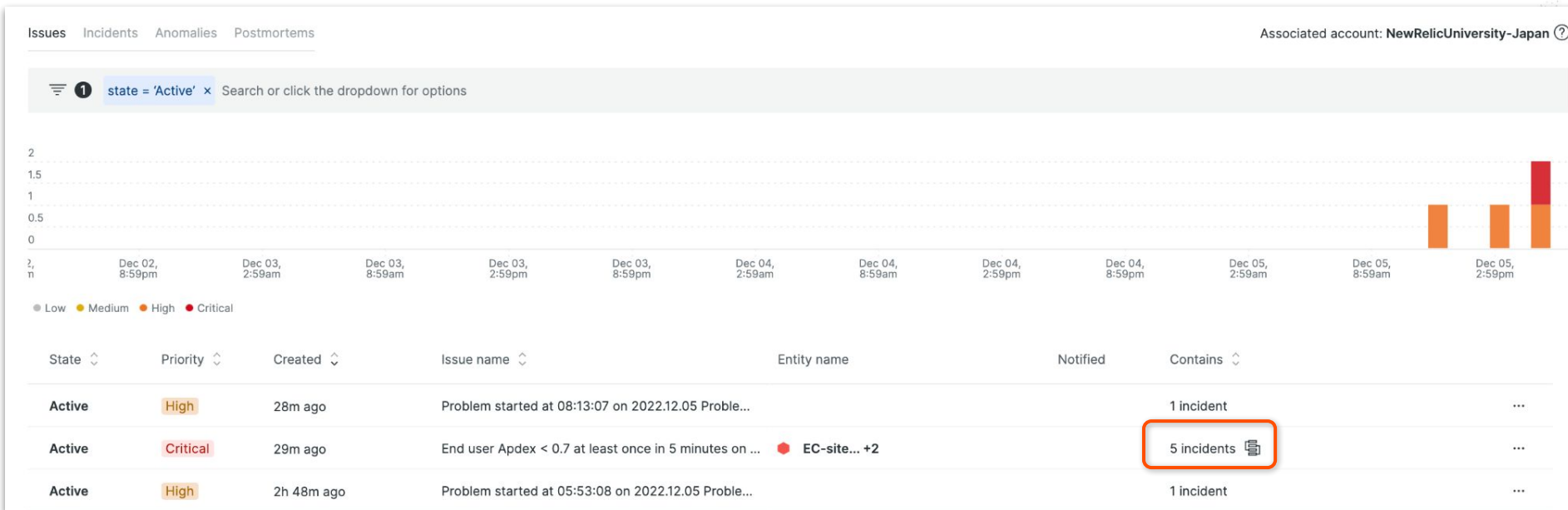
ハンズオン(2)複数のアラートを紐付け トラブルシューティングに役立てる

- オープン中のIssueが存在しない場合は「Active」フィルタを削除します。

The screenshot displays the New Relic Alerts & AI dashboard. On the left is a dark sidebar with the New Relic logo and a navigation menu including Search, Add data, All capabilities, All entities, Alerts & AI (highlighted), APM & services, Apps, Browser, Dashboards, Errors inbox, Metrics & events, Hosts, Infrastructure, Logs, and Mobile. The main content area is titled 'Alerts & AI' and includes a search bar with a filter 'state = Active' highlighted by a red box. Below the search bar, there are tabs for 'Issues', 'Incidents', 'Anomalies', and 'Postmortems'. The 'Issues' tab is active, showing a table with columns: State, Priority, Created, Issue name, Entity name, Notified, and Contains. The table is currently empty, with a message 'No chart data available.' displayed above it. The top right of the dashboard shows a time filter set to 'Since 30 minutes ago (GMT+9)' and the associated account 'NewRelicUniversity-Japan'.

ハンズオン(2)複数のアラートを紐付け トラブルシューティングに役立てる

- Issues ではユーザーが設定した Alert や Anomaly、API 連携などの複数のアラートの中で関連しそうなものをまとめて取り扱います。



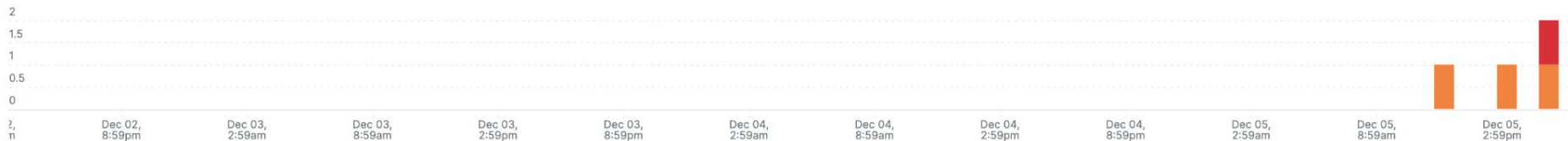
ハンズオン(2)複数のアラートを紐付け トラブルシューティングに役立てる

- Issueをクリックすると詳細が表示されます。

Issues Incidents Anomalies Postmortems

Associated account: NewRelicUniversity-Japan ?

state = 'Active' x Search or click the dropdown for options



● Low ● Medium ● High ● Critical

State	Priority	Created	Issue name	Entity name	Notified	Contains
Active	High	28m ago	Problem started at 08:13:07 on 2022.12.05 Proble...			1 incident
Active	Critical	29m ago	End user Apdex < 0.7 at least once in 5 minutes on ...	EC-site... +2		5 incidents
Active	High	2h 48m ago	Problem started at 05:53:08 on 2022.12.05 Proble...			1 incident

ハンズオン(2)複数のアラートを紐付け トラブルシューティングに役立てる

- どのIncidentがまとめられているのか確認することができます

Critical priority issue activated at Dec 5, 2022 5:12pm 32m Last updated Dec 5, 2022 5:17pm

End user Apdex < 0.7 at least once in 5 minutes on 'EC-site' Close Issue Acknowledge

Incidents: 5 Source: Issue payload

▼ Incidents: 5

Sort by Newest to oldest Show open only

Critical Open
EC-site query result is > 1.0 for 5 minutes on 'NRU302_alert_Lab'
Created: Today 5:16pm 27m

Critical Open
EC-site query result is > 1.0 for 5 minutes on 'サンプルアラート'
Created: Today 5:16pm 28m

Critical Open
Monitor failed for location Tokyo, JP on 'EC-CUBE-Checkout'
Created: Today 5:15pm 29m

Critical Open
Web response time deviated from the baseline at least once in 5 minutes on 'EC-site'
Created: Today 5:12pm 31m

Critical priority incident opened today 5:16pm 27m See NRQL overview

EC-site query result is > 1.0 for 5 minutes on 'NRU302_alert_Lab'

Source: Alert Policy: ダッシュボードハンズオン用アラートポリ... Condition: NRU302_alert_Lab Condition type: NRQL

4:55pm 5:00pm 5:05pm 5:10pm 5:15pm 5:20pm 5:25pm

● EC-site Tags: 10

Entity type: BROWSER account: NewRelicUniversit... accountid: 2511671 appName: EC-site clusterAgentid: 445000097 enabled: true Incident payload

Account: NewRelicUniversity-Japan id: 24752895 nr.has_slis: true policyid: 1065477 trustedAccountid: 2490334 type: NRQL Query

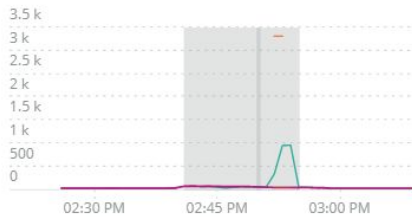
ハンズオン(2)複数のアラートを紐付け トラブルシューティングに役立てる

- Issue timelineや関連するEntity情報、デプロイ履歴など、原因分析に役立つ情報が表示されます

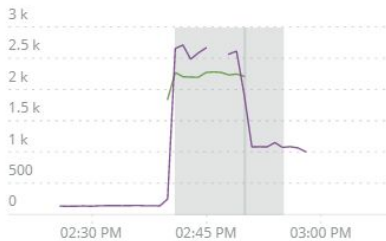
● Web response time > 2 seconds at least once in 5 minutes on 'EC-site' Critical

Attributes to investigate ?

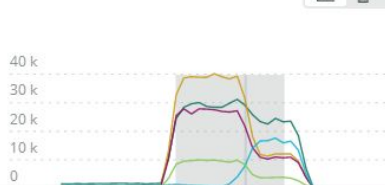
Average database duration (ms) faceted by
Datastore type and Table and Operation



Web response time faceted by
request.headers.accept



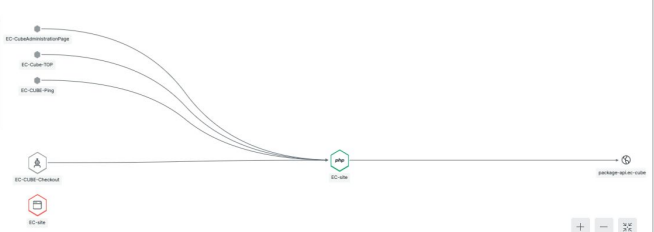
Database duration (ms) faceted by
Datastore type and Table and Operation



Impacted entities (3)

■ EC-site
■ EC-site

- Show
- Related entities
- Externals
- Entities
- Related entity
- External Service



Root cause analysis

Deployment events (1)

1 Deployments

Last 12h

▲ Deployment 22m before issue created
Application: EC-site
Deployer: Systems Manager | Revision: ec-cube-4

Possible cause: Due to proximity to issue creation



座学(4) AIOpsの意義

16:30 - 16:45 (15min)



ITサービスに発生しうる障害と監視の関連性

ITサービスに
発生しうる障害

理解できる

理解できない

気づける

Actionableな監視

気づいたあとに正しく対処が
できる
(例. ユーザーが特定の機能を使えない)



とりにあらずの監視

気づいても対処につなげられない
(例. インフラのリソース使用率上昇)



気づけない

Actionableな監視予備群

障害発生して後手対応になったが、
原因がわかったので次回から監視で
気づける



監視できていない未知の領域

障害発生したが原因がわからず監視
もできない

従来の監視のアプローチ

ITサービスに
発生しうる障害

運用スペシャリストがログから気合いで分析
のちのち手順化

理解できる

理解できない



Actionableな監視

とりあえずの監視

気づける
頑張ってすべての
障害ポイントを
洗い出す

努力と根性と属人性で
Actionableな監視を増やす



気づけない

Actionableな監視予備群



監視できていない未知
の領域

AIOpsとは

ガートナーによる定義

<https://www.gartner.com/en/information-technology/glossary/aiops-artificial-intelligence-operations>

AIOpsとは、IT運用プロセスを自動化するためにビッグデータと機械学習を紐付けたものであり、以下のような機能を含む:

1. 異常検知
2. イベントの相関分析
3. 根本原因分析

AIopsが必要とされる背景

1. モノリスからマイクロサービスへ

監視対象となるコンポーネントの絶対数が増えると同時に、コンポーネント同士の関連性がより複雑に

過去のシステム

アプリ



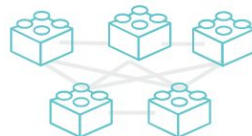
基盤



アプリがモノリシックかつ基盤が密結合だったため、リソースが枯渇しなければ大きな問題が発生しなかった

近年のシステム

アプリ



リソース抽象化
(仮想化、コンテナ等)



基盤

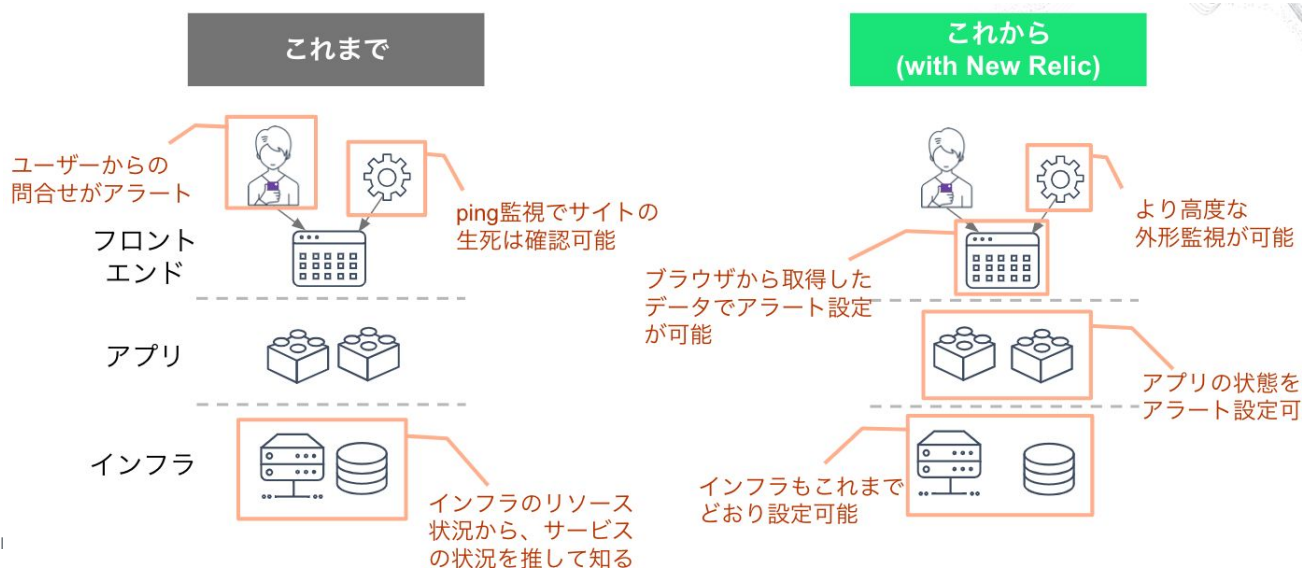


アプリがマイクロサービス化かつ基盤が疎結合なため、基盤リソースと関係なく問題が発生しうる

AIOpsが必要とされる背景

2. 捕捉できるデータの増加と多様化

New Relicのようなオブザーバビリティプラットフォームによって、サービスを構成する様々なコンポーネントから多種多様なデータを取得できるように

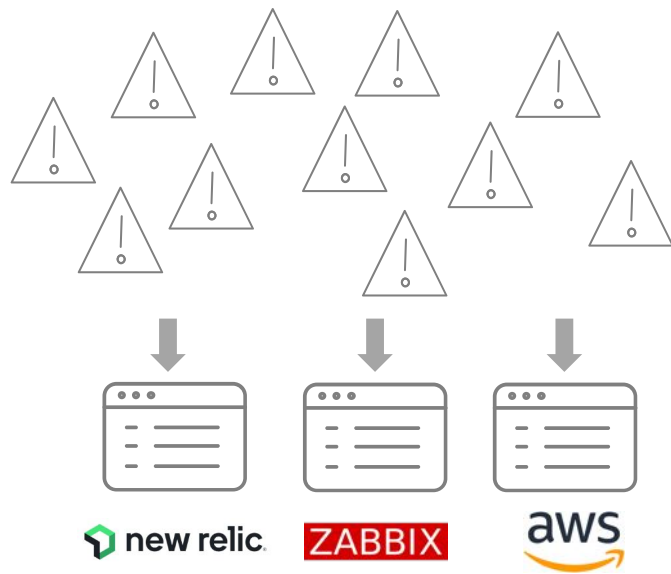


監視にまつわる新たな課題

アラートを1つ1つ網羅的に
設定するのか問題



大量のアラートをどう解釈してトラ
シューするのか問題



従来の監視の限界

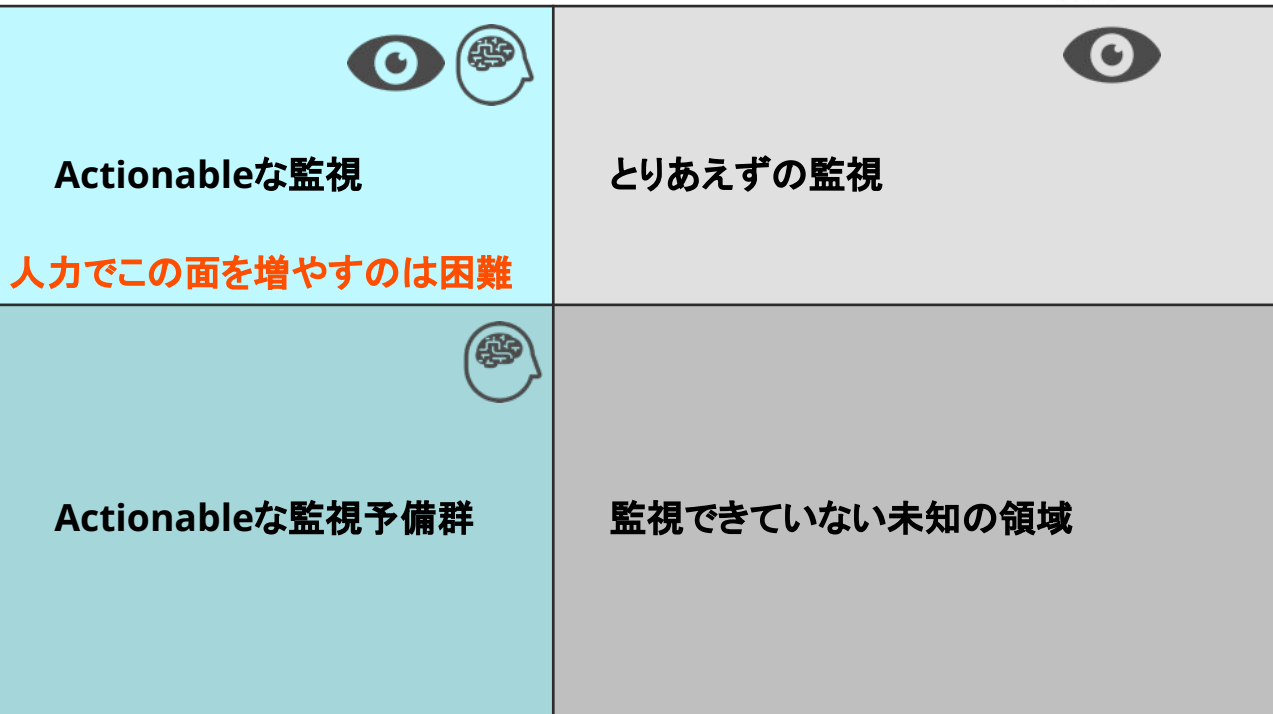


ITサービスに
発生しうる障害

理解できる

理解できない

気づける



気づけない

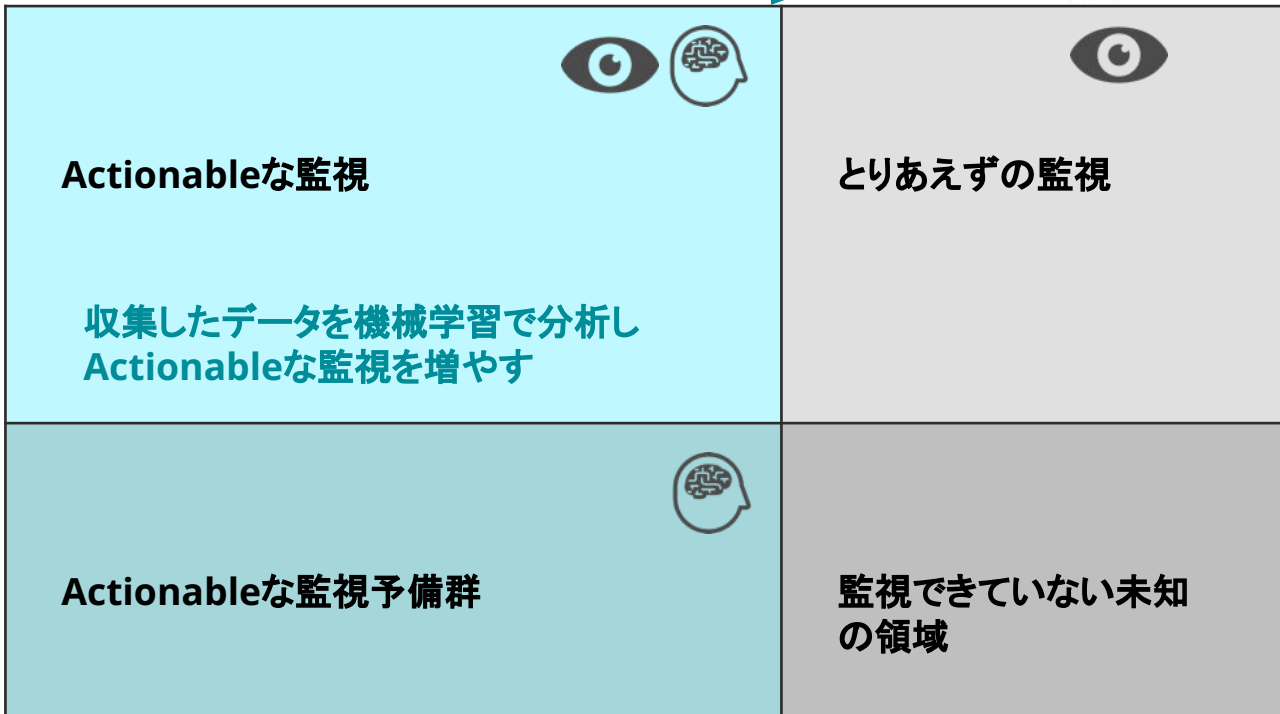
AI Opsのアプローチ

複数の事象を自動で関連付け
根本原因を推察

ITサービスに
発生しうる障害

理解できる

理解できない



AIOpsによってサービスの信頼性を高める

アラートを1つ1つ網羅的に
設定するのか問題



[解決するAIOpsの機能]

- 異常検知



手動でアラート設定せずとも自動で検知

Alert coverage gaps

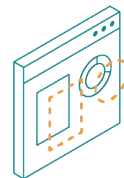
(BETA)

大量のアラートをどう解釈してトラ
シューするのか問題



[解決するAIOpsの機能]

- イベントの相関分析
- 根本原因分析



複数の事象を自動で関連付け、根本原因を推察

Anomaly Detection

機能紹介: Alert coverage gaps

Alert coverage gaps

Some of your services don't have alerts set up. Our machine learning engine recommends adding these alerts. [See our docs](#)

0% covered 1 entities

Services - APM

Name	Throughput	Error Rate	Action
EC-site	39.35 req/min	0%	Add alert

設定すべきアラートを通知します。

現行ではAPMのみを対象としています。

Add an alert

EC-site

Add recommended conditions

Our power users add these conditions to similar entities.

- Critical EC-site - Error Percentage** Highly recommended
Threshold type: Baseline
Alert when this signal deviates from its normal baseline, upper and lower, for at least 5 minutes by 3.00 standard deviation(s).
- Critical EC-site - Apdex**
Threshold type: Baseline
Alert when this signal deviates from its normal baseline, upper and lower, for at least 5 minutes by 3.00 standard deviation(s).
- Critical EC-site - Response Time (Web)**
Threshold type: Baseline
Alert when this signal deviates from its normal baseline, upper and lower, for at least 5 minutes by 3.00 standard deviation(s).

Select policy to get notified

Looking for more options? [Set up an alert from scratch.](#)

Create an alert condition

Account: 2511671 - NewRelicUniversity-Japan

Enter condition name
EC-site - Apdex

Define your signal
Enter NRQL Query

```
SELECT apdex(apm.service,apdex) FROM Metric WHERE entity.guid = 'HjuM7Y3Mx8UE18QV80TE1DQVJ3T85NDQJMDAwMDk3' FACET entity -guid
```

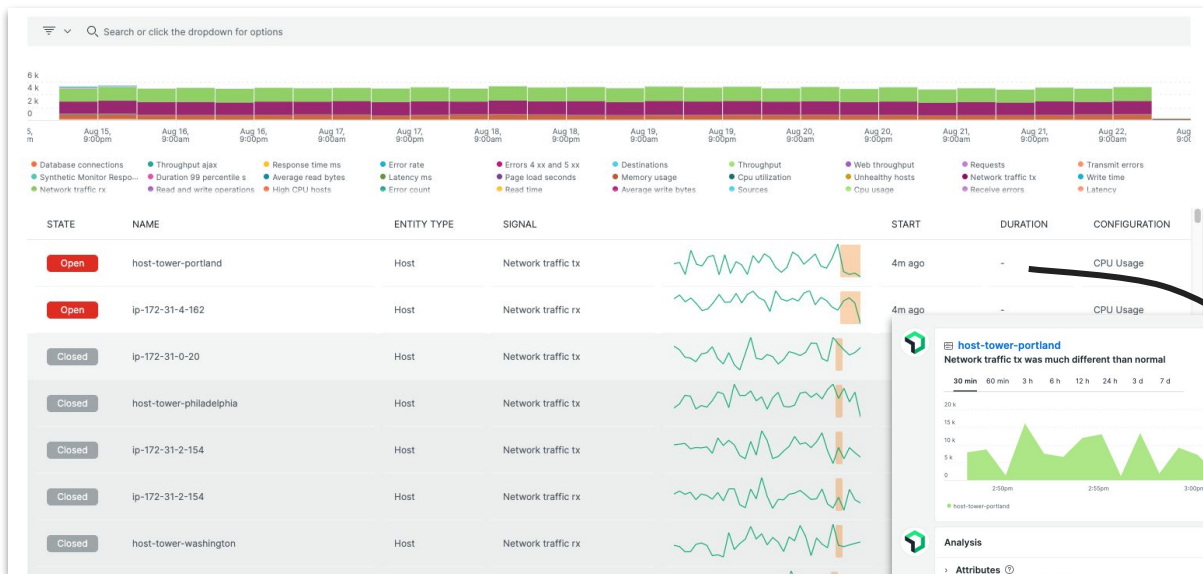
Showing 1/1 time series

Preview charts are estimates only
These charts use your stored data to show how this signal might create incidents. They don't consider all aspects of streaming analytics (e.g., cadence, null values, signal loss, filtered data gaps). [See our docs](#)

Set your condition thresholds
Threshold Type: Static Anomaly
Anomaly is useful when you want to define more flexible thresholds that adjust to how your data behaves. You'll get notified only when something behaves abnormally. [See our docs](#)

Threshold direction: Upper and lower

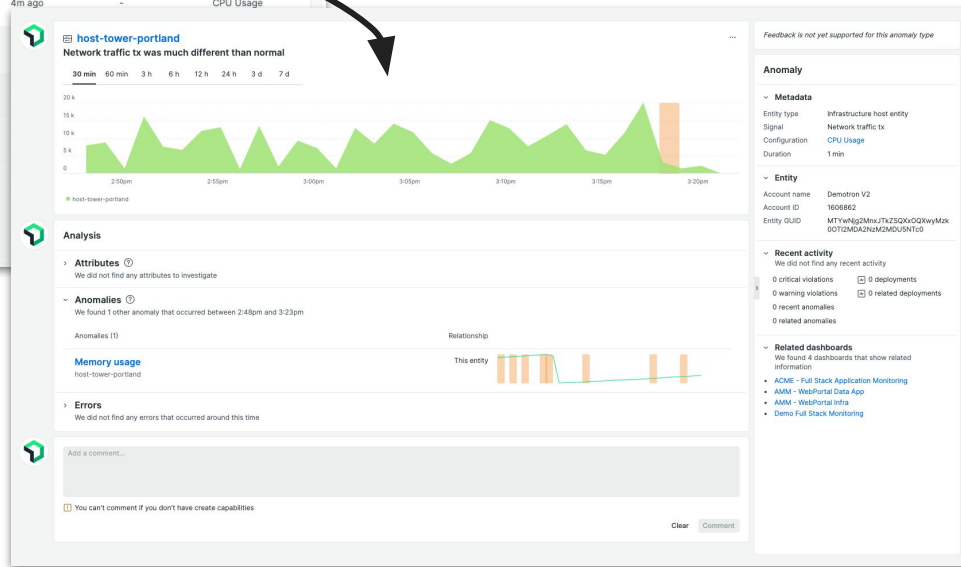
機能紹介: Anomaly Detection



現行では、APMのみの対応となっていますが、HOSTやBrowserなど、他の監視entityのサポートを今後計画しています。

Alerts & AI -> Issues & activity -> Anomalies

- 発生したAnomalyの1つを選択し、詳細を確認する



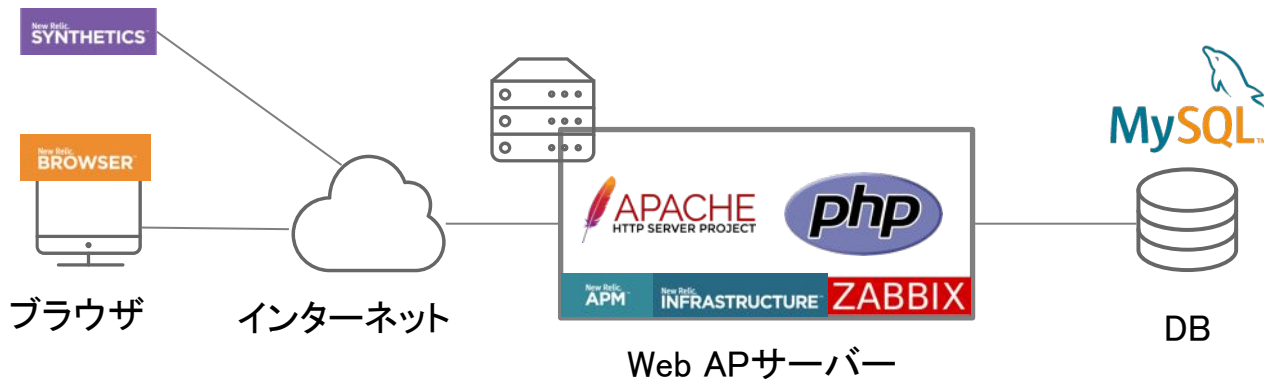
ハンズオン(3) AIOpsを使った異常検知 と原因分析(応用編)

16:45 - 16:55 (10min)



今回の環境の監視構成(再掲)

- New Relic:
 - 外形監視, フロントエンド(ブラウザ), アプリケーション、インフラ
- Zabbix:
 - インフラ



ハンズオン(3)

3-1 様々なソースのアラートをまとめる: 通常のアラート

[目的]

アラートを相関分析できるように、複数ソースのアラートを New RelicのAIOpsに取り込みましょう

- Alerts&AI -> Sourcesを選択
- Alertsカードを選択
- [+ Add a policy]をクリックして自分が作成した Alert Policyを追加する

ハンズオン(3)

3-2 様々なソースのアラートをまとめる : 異常検知情報の接続

[目的]

アラートを相関分析できるように、複数ソースのアラートを New RelicのAIOpsに取り込みましょう

- Alerts & AI -> Anomaly Detectionを選択
- Add a configurationを押す
- 設定名は自分の名前、アカウントは NRU(2511671)、アプリはEC-site、No notification、Correlate with other alerts をオンにして[Save configuration]

ハンズオン(3)

3-3 様々なソースのアラートをまとめる: **[参考情報]** Zabbixからのアラート

[目的]

アラートを相関分析できるよう、複数ソースのアラートを New RelicのAIOpsに取り込みましょう

- Zabbix 5.0 以降で追加されたwebhook メディアタイプによって、ZabbixのAlertをNew Relic Incident Intelligence APIに通知することができます。
- Zabbix のMacroから値を受け取り、New Relic APIエンドポイントURLとInsights Insert Keyを利用してJavaScript から送信することができます。



手順・解説

使用アカウント: NewRelic.kk
(ログイン先選択は[こちら](#)参照)

ハンズオン(3)様々なソースのアラートをまとめる(1)

- 「Sources」をクリックします。

The screenshot shows the New Relic Alerts & AI interface. The left sidebar contains a navigation menu with 'Sources' highlighted. The main panel shows a bar chart with two orange bars representing alerts, and a table of active alerts.

State	Priority	Created	Issue name	Entity name	Notified	Contains
Active	High	1h 3m ago	Problem started at 03:03:37 on 2022...			1 incident
Active	High	Dec 4, 2022 2:5...	Problem started at 05:53:08 on 2022...			1 incident


ハンズオン(3-1)様々なソースのアラートをまとめる

- 「Alerts」カードをクリックします。


Alerts & AI ? [↗](#)

Associated account: **NewRelicUniversity-Japan** ?

1 active source

 **1 policy connected**

Available sources

 **Alerts**

1 active policy

Ingest your existing alert policies for correlations to gain actionable insights and cross-source visibility of your stack.

API **REST API**

Use REST endpoint to easily ingest monitoring data for correlations from any other tool, including homegrown solutions.

ANALYZE

Overview

Issues & activity

DETECT

Alert conditions (Policies)

Anomaly detection

Alert coverage gaps **Beta**

CORRELATE

Sources

Decisions

ENRICH & NOTIFY


Muting rules

Workflows **New**

ハンズオン(3-1)様々なソースのアラートをまとめる

- 「+ Add a policy」ボタンをクリックします。

Associated account: **NewRelicUniversity-Japan** ?



New Relic Alerts source

When connected policies generate activity, we'll automatically correlate it to filter out noise, add context, and identify issues. You'll get fewer notifications and have more information, so you can solve problems faster.

NEW RELIC IS CONNECTED

POLICIES (1)

POLICY ⌵

[ダッシュボードハンズオン用アラートポリシー](#) 🔗

ACCOUNT ⌵

NewRelicUniversity-Japan

+ Add a policy

ハンズオン(3-1)様々なソースのアラートをまとめる

- ハンズオン(1)で作成した自分の AlertPolicy にチェックを付けて「Connect」ボタンをクリックします。

Get data from New Relic Alerts

Select the New Relic Alerts policies you want to connect ⓘ

Account All ▼

View: All (3) Selected (2) Unselected (1)


<input type="checkbox"/>	POLICY ↕	ACCOUNT NAME ↕
<input checked="" type="checkbox"/>	ダッシュボードハンズオン用アラートポリシー ↗	NewRelicUniversity-Japan
<input type="checkbox"/>	NRU インスタンス メンテナンス ↗	NewRelicUniversity-Japan
<input checked="" type="checkbox"/>	nrui-test-policy ↗	NewRelicUniversity-Japan

Cancel **Connect**

ハンズオン(3-1)様々なソースのアラートをまとめる

- 自分のPolicyが追加された事を確認します。

Associated account: **NewRelicUniversity-Japan** ?



New Relic Alerts source

When connected policies generate activity, we'll automatically correlate it to filter out noise, add context, and identify issues. You'll get fewer notifications and have more information, so you can solve problems faster.

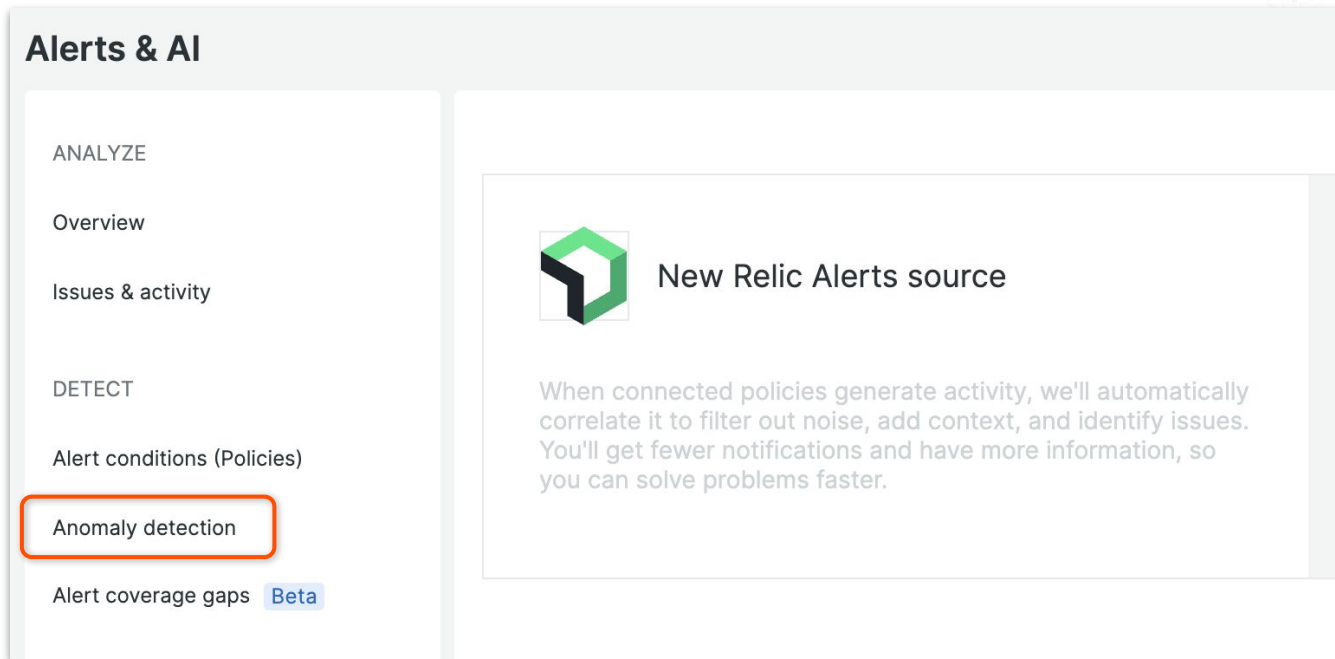
NEW RELIC IS CONNECTED

POLICIES (2) + Add a policy

POLICY	ACCOUNT
<input type="checkbox"/> ダッシュボードハンズオン用アラートポリシー ↗	NewRelicUniversity-Japan
<input type="checkbox"/> nru-test-policy ↗	NewRelicUniversity-Japan

ハンズオン(3-2)様々なソースのアラートをまとめる

- 「Anomaly detection」をクリックします。




Alerts & AI

ANALYZE

- Overview
- Issues & activity

DETECT

- Alert conditions (Policies)
- Anomaly detection**
- Alert coverage gaps Beta

 **New Relic Alerts source**

When connected policies generate activity, we'll automatically correlate it to filter out noise, add context, and identify issues. You'll get fewer notifications and have more information, so you can solve problems faster.

ハンズオン(3-2)様々なソースのアラートをまとめる

- 「+ Add a Configuration」ボタンをクリックします。

Anomaly detection

We automatically detect anomalies for your APM applications that you can [query](#) and add to dashboards. [See our docs](#) 

Visibility

We display anomalies in the activity stream and the [anomalies tab](#). You can adjust your visibility preferences to change what you see.


Visibility preferences

Notifications

Add configurations to get notifications (Slack or webhook) and customize what you see for specific applications.

+ Add a configuration

🔍 Search configurations

Configuration name 	Account 	Applications 	Destination 	Last updated 
NRU Proactive Detection Sample	NewRelicUniversity-Japan	1		Aug 10, 2022 5:00pm 

ハンズオン(3-2)様々なソースのアラートをまとめる

- 「設定名」に自分の名前を付け、Accountは「NewRelicUniversity-Japan」を選択します。
- 「EC-site」にチェックを入れます。

Configure anomaly detection

▼ Make this configuration easy to identify

自分の名前

▼ What account do you want to use?

Account: 2511671 - NewRelicUniversity-Japan ▼

▼ What applications and services do you want to include? (Select up to 1,000)

Service - APM

APM

Entities: 2

Search in this table...

All (2) Selected (1/2) Unselected (1)

Name
<input checked="" type="checkbox"/> ★ EC-site
<input type="checkbox"/> webapp

ハンズオン(3-2)様々なソースのアラートをまとめる

- 5カテゴリ全てにチェックをつけ、「No notifications」を選択します。
- 「Correlate with other alerts」を有効にして「Save configuration」をクリックします。

▼ What signals should we monitor for anomalies?

Web throughput <input checked="" type="checkbox"/>	Non-web throughput <input checked="" type="checkbox"/>	Error rate <input checked="" type="checkbox"/>	Web response time <input checked="" type="checkbox"/>	Non-web response time <input checked="" type="checkbox"/>
--	--	--	---	---

▼ Where do you want to receive notifications?

We'll write anomalies we detect to NRDB, which means you can query them and view them in the [anomalies tab](#).

Slack	Webhook	No notifications <input checked="" type="checkbox"/>
-------	---------	--


▼ Do you want to correlate anomalies from this configuration? ?

Correlate with other alerts

ハンズオン(3-2)様々なソースのアラートをまとめる

- 設定が追加されたことを確認します。

Anomaly detection

We automatically detect anomalies for your APM applications that you can [query](#) and add to dashboards. [See our docs](#) 

Visibility








We display anomalies in the activity stream and the [anomalies tab](#). You can adjust your visibility preferences to change what you see.

[Visibility preferences](#)

Notifications

Add configurations to get notifications (Slack or webhook) and customize what you see for specific applications.

[+ Add a configuration](#)

Configuration name 	Account 	Applications 	Destination 	Last updated 
自分の名前	NewRelicUniversity-Japan	1		Dec 5, 2022 1:37pm 
NRU Proactive Detection Sample	NewRelicUniversity-Japan	1		Aug 10, 2022 5:00pm 

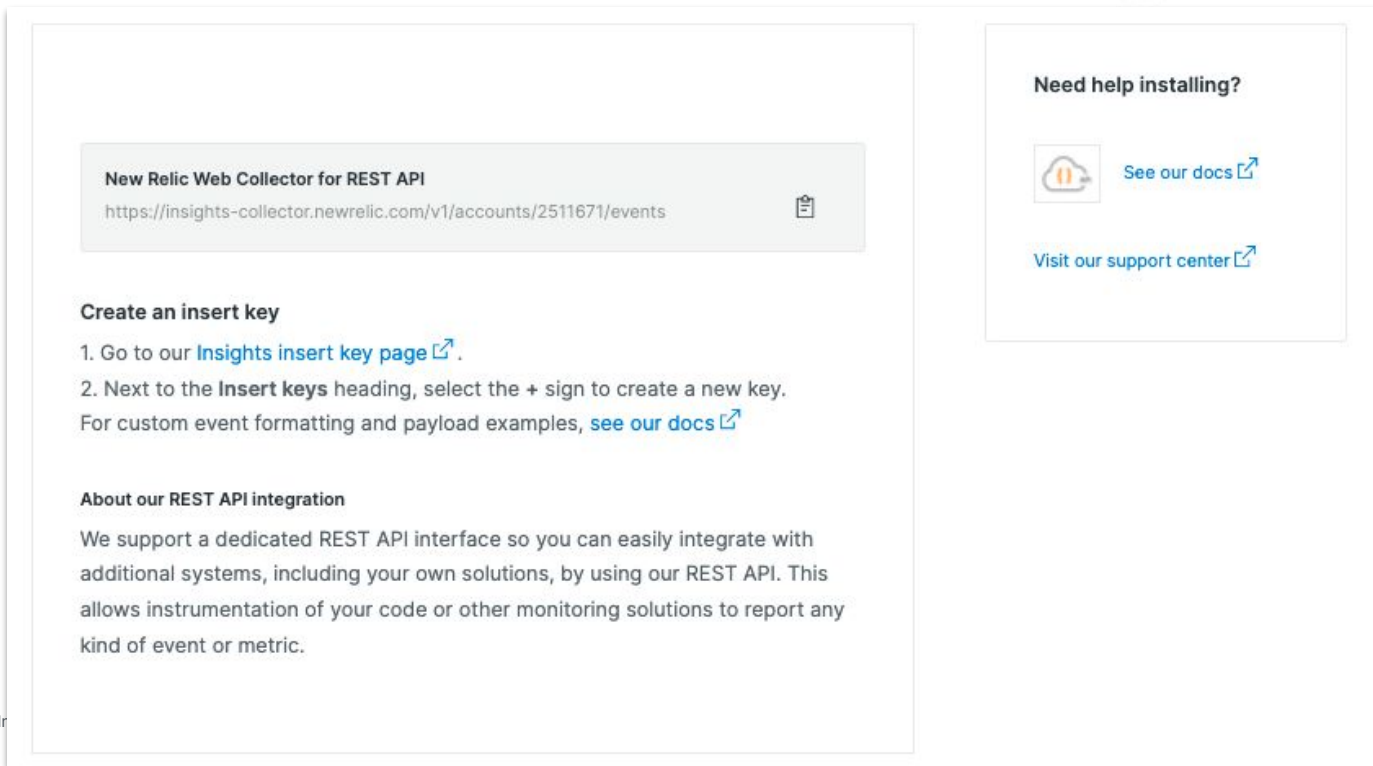
参考 Zabbixの連携

- ZabbixからIncident Intelligence への連携にはREST APIを利用しています。

The screenshot displays the 'Alerts & AI' dashboard. On the left is a navigation sidebar with categories: ANALYZE (Overview, Issues & activity), DETECT (Alert conditions (Policies), Anomaly detection, Alert coverage gaps **Beta**), CORRELATE (Sources, Decisions), and ENRICH & NOTIFY (Muting rules, Workflows **New**). The main content area shows 'Associated account: NewRelicUniversity-Japan' and '1 active source' with '1 policy connected'. Under 'Available sources', there are two cards: 'Alerts' (1 active policy) and 'REST API' (highlighted with an orange border). The REST API card includes the text: 'Use REST endpoint to easily ingest monitoring data for correlations from any other tool, including homegrown solutions.'

参考 Zabbixの連携

- API URLとInsights Insert keyを作成し、それをコピーしてZabbix側に登録します。



The screenshot displays the New Relic REST API documentation page. At the top, there is a code block for the API URL: `https://insights-collector.newrelic.com/v1/accounts/2511671/events`. Below this, the section "Create an insert key" provides a two-step guide: 1. Go to the "Insights insert key page" and 2. Select the "+" sign to create a new key. A link to "see our docs" is provided for custom event formatting and payload examples. The "About our REST API integration" section explains that a dedicated REST API interface is available for integration with other systems.

New Relic Web Collector for REST API
`https://insights-collector.newrelic.com/v1/accounts/2511671/events`

Create an insert key


- Go to our [Insights insert key page](#).
- Next to the **Insert keys** heading, select the + sign to create a new key.

For custom event formatting and payload examples, [see our docs](#)

About our REST API integration

We support a dedicated REST API interface so you can easily integrate with additional systems, including your own solutions, by using our REST API. This allows instrumentation of your code or other monitoring solutions to report any kind of event or metric.

Need help installing?

 [See our docs](#)

[Visit our support center](#)

参考 Zabbixの連携

- Zabbixのトリガーアクションによってメディアタイプを呼び出して利用しています。

アクション

アクション

実行内容

* デフォルトのアクション実行ステップの間隔

メンテナンス中の場合に実行を保留

実行内容

ステップ 詳細

開始時刻 継続期間 アクション

1 ユーザーグループにメッセージを送信: New Relic via New Relic Incident Intelligence すぐに 標準 [変更](#) [削除](#)

[追加](#)

復旧時の実行内容

詳細

アクション

ユーザーグループにメッセージを送信: New Relic via New Relic Incident Intelligence

[変更](#) [削除](#)

[追加](#)

更新時の実行内容

詳細

アクション

ユーザーグループにメッセージを送信: New Relic via New Relic Incident Intelligence

[変更](#) [削除](#)

[追加](#)

* 少なくとも1つ以上の実行内容が設定されている必要があります。

更新

複製

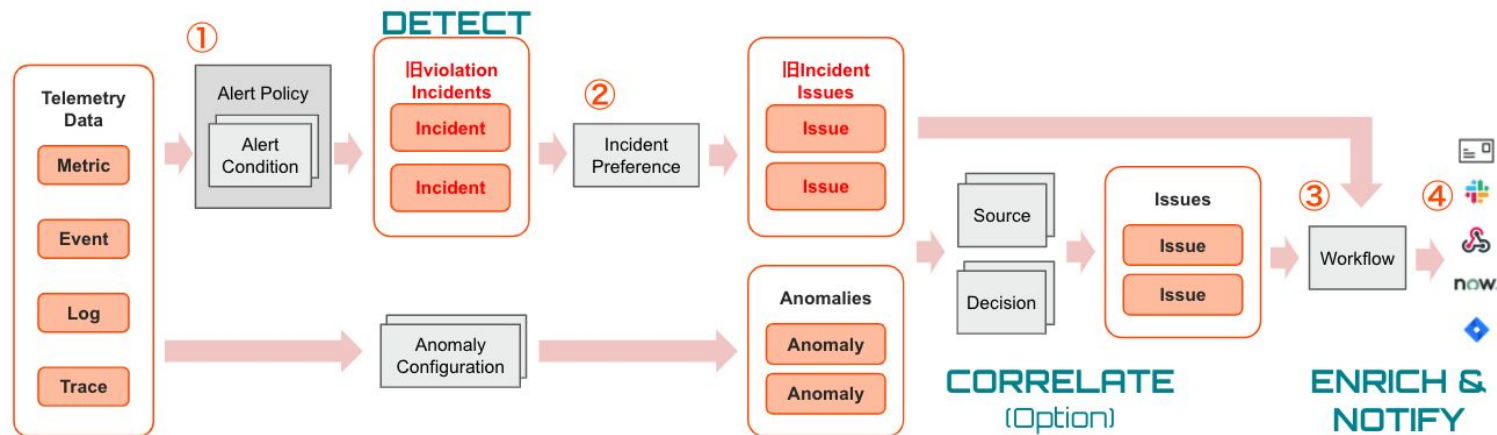
削除

キャンセル

まとめ

まとめ

- ユーザー体験に近い指標でアラートを設定しよう
 - インフラ監視はアンチパターン
- New Relicのアラート構造と設定方法を理解しよう



- New Relicを使ってAIOpsを実現しよう
 - Anomaly DetectionとCorrelation、Lookoutを使った異常検知



お疲れさまでした。
ご質問があればチャットにご記入ください
アンケートにご協力お願いいたします

Thank you.