

# NRU 304 「AIOps とアラート設計の基本」

June 7, 2023



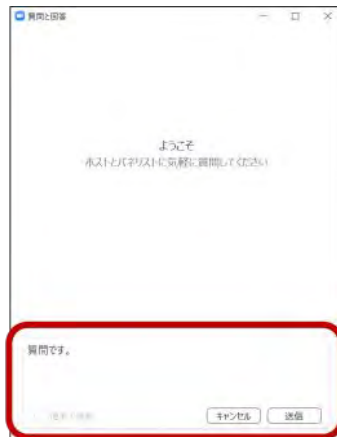
# ウェビナー 各種ご連絡

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。



New Relic 株式会社

技術統括 テクニカルサポート部

# 三井 翔太 / Shota Mitsui

## Senior Technical Support Engineer

→ HAクラスター製品のQAエンジニア

→ 国内Sler AWSインフラエンジニア(構築・運用設計)

→ 国内Sler AWS再販顧客向けのテクニカルサポート

→ 2022年8月～ New Relic テクニカルサポート

得意カテゴリ Infrastructure, Alerts & AI

# 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](http://ir.newrelic.com) or the SEC’s website at [www.sec.gov](http://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.

# 本セッションのゴール

- New Relicの収集データを活用した、**ユーザー体験に近い指標**に基づいたアラート設定を体験する
- New Relicの**AI Ops機能**を活用して、アラート対応の効率化を実現する方法を知る

# 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）
- [NRQL reference](#)（公式ドキュメント）

# 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
15:15-15:40	座学(2)	New Relicのアラート機能
15:40-15:50	ハンズオン(0)	環境を確認する
15:50-16:10	ハンズオン(1)	アラートを作成する
16:10-16:20	座学(3)	New Relicのアラート分析支援機能
16:20-16:30	ハンズオン(2)	New Relicのアラート分析支援ウォークスルー
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
16:55-17:00		まとめ、アンケートご記入

# 座学(1)

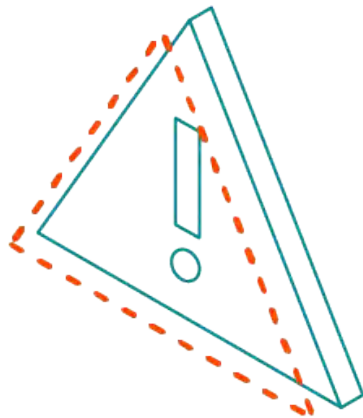
## ユーザー視点のアラート

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、**何らかの対応が必要な状態**であることの通知を受け取るため

1. システムの停止、またはパフォーマンスの悪化が発生  
→ **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**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)

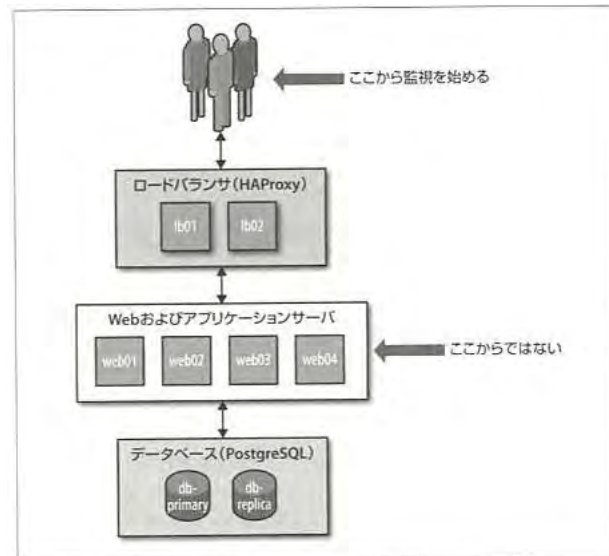
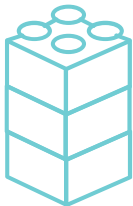


図2-1 できるだけユーザーに近いところから監視を始める

# 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



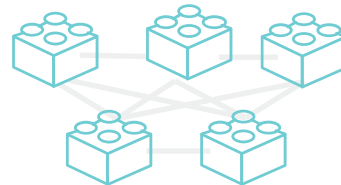
基盤



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)

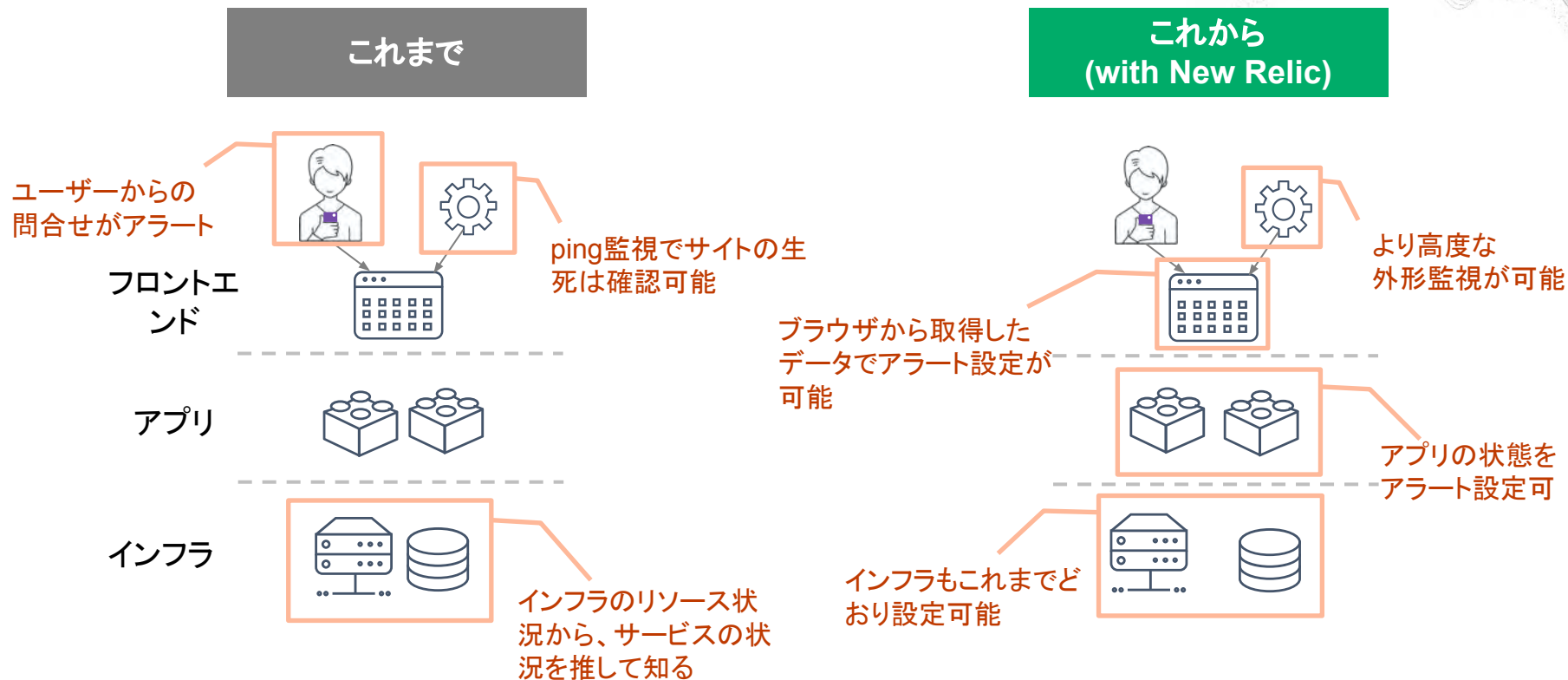


基盤



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 - 15:40 (25min)

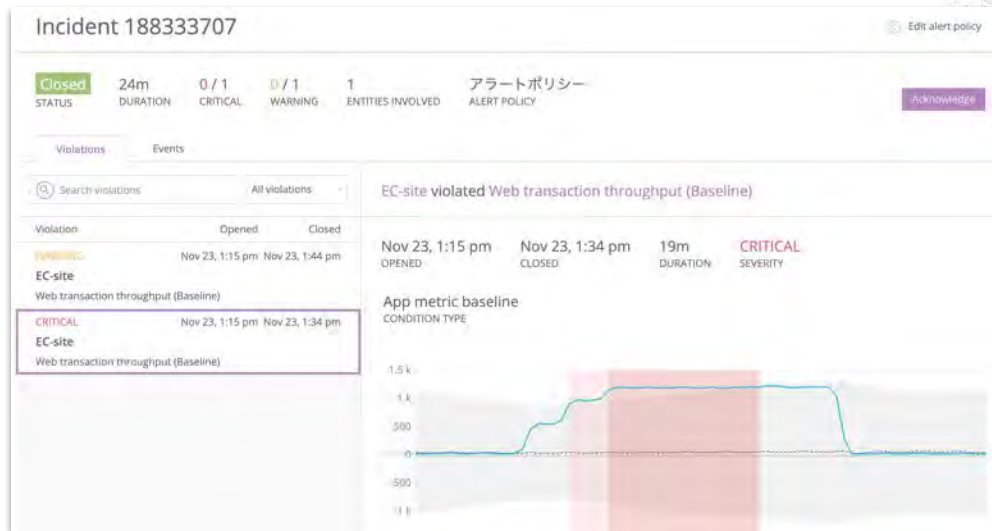


# New Relicのアラート機能

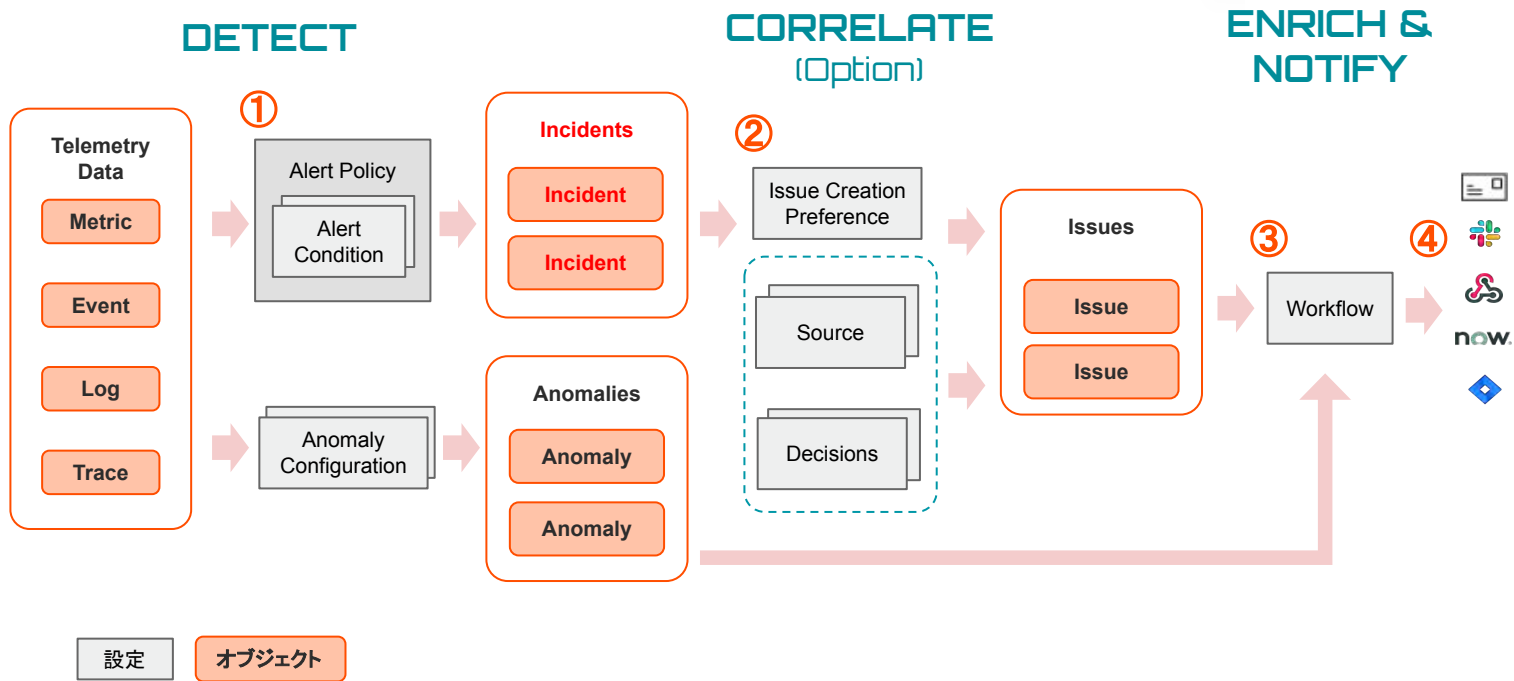
New Relicがリアルタイムに収集しているデータを使って、アラートを設定することが可能

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

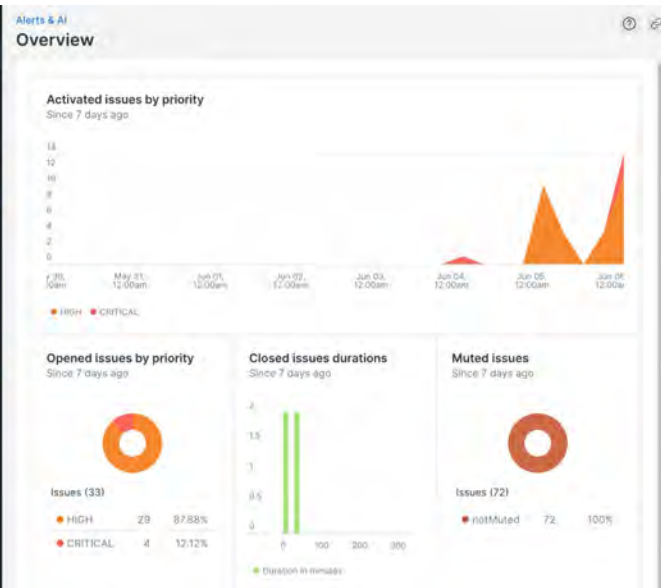
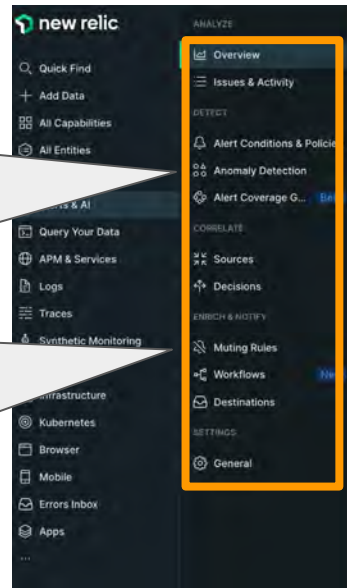
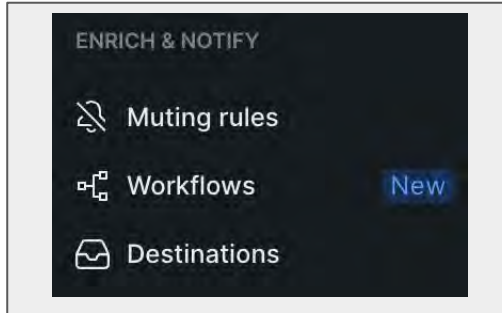
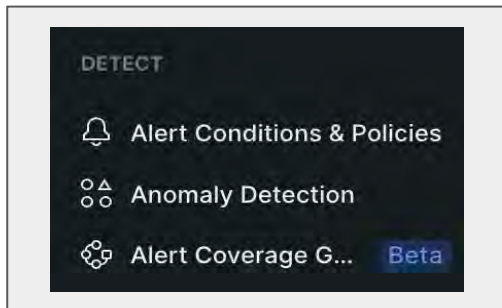
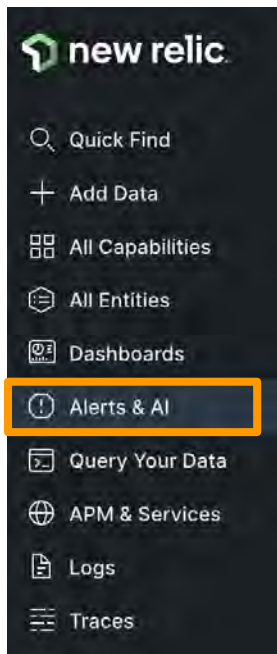
※アラートを上げる条件や頻度、通知先の設定など、様々な設定が可能なので、次ページ以降で解説していきます



# 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

## Alert Policy

Alert Conditionのグループ

## Alert Condition

アラート対象や閾値、集計方法の定義

## Incident

Alert Conditionで検出した個々の違反

## Issue

一つ以上のIncidentが示す、発生中の問題  
実際の通知はIssueに対して行われる

The screenshot shows the 'ISSUE CREATION PREFERENCE' configuration page. It includes a title, a descriptive paragraph, a link to a terminology update, three radio button options for grouping incidents, a 'See our docs' link, and a checkbox for 'Correlate and suppress noise' with a note about data processing in the U.S.

**ISSUE CREATION PREFERENCE** Specify how we create issues and group incidents into them. (You get notifications when an issue 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.

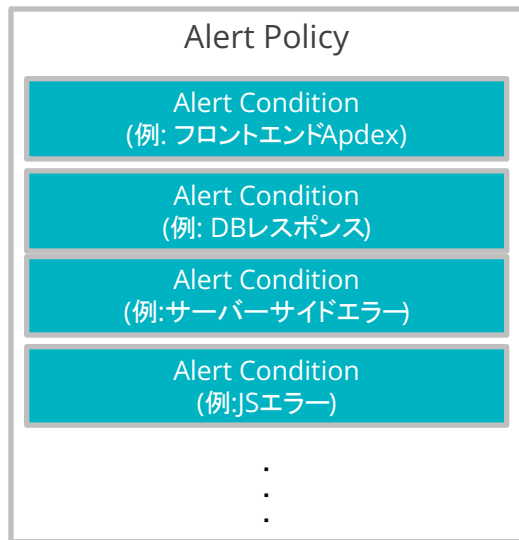
[See our docs](#)

**Correlate and suppress noise** Automatically correlate related incidents and issues to suppress noise, so you only get notified when you have a new issue.  
\* Data is sent to the U.S. for processing.

# New Relic アラートの構成要素1: Alert Policy

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ごとにアラートをグループ化したり、通知先の制御ができる

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 interface. The title is "アラートポリシー" (Alert Policy) with an ID of "id: 545592". It features tabs for "2 Alert conditions" and "2 Notification channels". The "Alert conditions" tab is active, showing a search bar and a list of conditions. The first section is "INFRASTRUCTURE METRIC Disk Used", which includes two conditions: "diskUsedPercent > 90 for at least 2 mins" and "diskUsedPercent > 70 for at least 2 mins". The second section is "APM APPLICATION METRIC BASELINE Web transaction throughput (Baseline)", which includes two conditions: "Web transaction throughput deviates from baseline for at least 5 mins". The interface also shows "Last modified" dates and "Manage" options for each condition.

# New Relic アラートの構成要素1: Alert Policy

## Issue Creation Preference

IncidentをIssueにグループ化して、通知をまとめる設定

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

- Condition1: フロントエンドのJSエラー率 (対象サイトは1つ)
- Condition2: サーバーサイドのエラー率 (ホスト別に集計、対象ホストは3台)

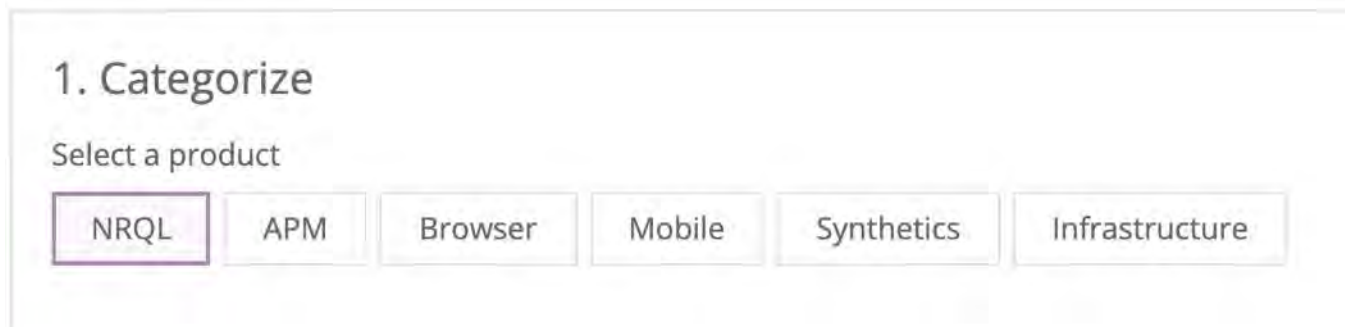
設定名	Incident発生時の挙動	この例で起票されるIssue(通知件数)
One issue per policy	同じAlert Policyから発生したIncidentを、一つのIssueにまとめる	1件
One issue per condition	同じAlert Conditionから発生したIncidentを、一つのIssueにまとめる	2件(JSエラーで1件、サーバーサイドエラー全体で1件)
One issue per condition and signal	同じConditionであっても、アラート対象ごとに個別にIssueを作成する	4件(JSエラーで1件, ホスト毎のサーバーサイドエラーで3件)

# New Relic アラートの構成要素2: Alert Condition

New Relicが収集しているリアルタイムなデータを、集計・評価する仕組み

- どのような方法で集計を行うか(平均値・最大値・データ件数カウントなど)
- どのような状況をアラートとして通知するか

機能(例. APM, Browser等)ごとに用意されたプリセットから簡単にアラートを作れるほか、自分で**NRQLクエリ**を記述して、独自の Alert Conditionを作成することも可能



1. Categorize

Select a product

NRQL APM Browser Mobile Synthetics Infrastructure

The screenshot shows a web interface for configuring an alert. The first step is '1. Categorize', which involves selecting a product. Below the heading, there is a row of six buttons: 'NRQL', 'APM', 'Browser', 'Mobile', 'Synthetics', and 'Infrastructure'. The 'NRQL' button is highlighted with a purple border, indicating it is the selected option.

# New Relic アラートの構成要素2: 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 <a href="https://docs.newrelic.com/docs/alerts-applied-intelligence/new-relic-alerts/alert-conditions/create-baseline-alert-conditions">https://docs.newrelic.com/docs/alerts-applied-intelligence/new-relic-alerts/alert-conditions/create-baseline-alert-conditions</a>	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2: Alert Condition

静的(Static) しきい値の超過を評価する方法

- **For at least xx minutes**

xx分間、しきい値を超過する状態が続いた場合に、Incidentが起票される

- **at least once in xx minutes**

xx分間で、しきい値を1回でも超過した場合に、Incidentが起票される

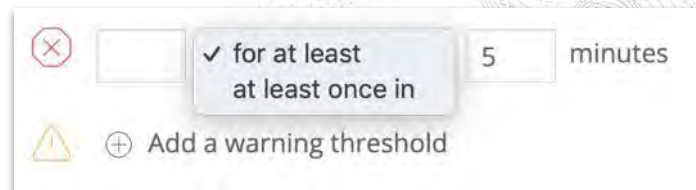
一つのAlert Conditionには、CriticalとWarning(オプション)の閾値を設定可能

その他、アラート設定に関する詳細は以下もご参照ください:

[ストリーミング・アラートの概念 | New Relic](https://newrelic.com/jp/blog/how-to-relic/streaming-alert-concept) (https://newrelic.com/jp/blog/how-to-relic/streaming-alert-concept)

[アラート条件を正しく設定するための詳細ガイド | New Relic](https://newrelic.com/jp/blog/how-to-relic/understand-nrql-alert-condition) (https://newrelic.com/jp/blog/how-to-relic/understand-nrql-alert-condition)

[アラート定義のガイダンス | New Relic](https://newrelic.com/jp/blog/how-to-relic/alert-configuration-guidance) (https://newrelic.com/jp/blog/how-to-relic/alert-configuration-guidance)



# New Relic アラートの構成要素2: Alert Condition

効果的な通知を送るためのプラクティス

- Additional settings > custom violation description  
発報されるアラートに任意の情報を付加することが可能 ([参考情報](#))
- Additional settings > Runbook URL  
アラート対応手順書や、情報を集約したダッシュボードにすぐにアクセスすることが可能

▼ **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3: Workflow

発生したIssueと、通知先・通知内容の関連付け

## Filter data

どのようなIssueで、このWorkflowを起動するか

## Enrich (Additional settings内)

通知に、Issueに関する付加情報を付与する

## Mute issues (Additional settings内)

Muting Rulesが設定されていた場合の挙動の設定

## Notify (Destinations: 後述)

通知先の定義と、通知内容のカスタマイズ

## Test workflow

過去の該当データを元に、Workflowの通知テストを実行

The screenshot shows the 'Configure your workflow' interface in New Relic. At the top, there is a text input field for naming the workflow, with a placeholder 'Enter a name you'll recognize' and a subtext 'Give it a unique, descriptive name you'll recognize later'. Below this is the 'Filter data' section, which includes a 'Select the kinds of issues you want to send' instruction and a 'Use the basic filter for the most common attributes or the advanced filter for all attributes.' note. There are 'Basic' and 'Advanced' filter options. Underneath are three dropdown menus for 'Tag', 'Policy', and 'Priority'. A yellow warning box states 'Please select at least one value' and 'At least one value must be selected in one of the attributes in order to build a valid filter'. The 'Additional settings' section is partially visible. The 'Notify' section has the instruction 'Choose one or more destinations and add an optional message.' and a grid of destination options: ServiceNow incidents, Webhook, Jira, Slack, Email, AWS EventBridge, Mobile push, and PagerDuty. At the bottom, the 'Test this workflow' section includes the text 'We'll use existing data from your account to test what you've configured and send a sample notification.' and a 'Test workflow' button.

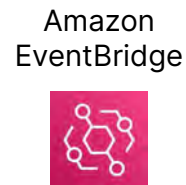
# New Relic アラートの構成要素4: Destinations

Issueのライフサイクル変化(オープン・クローズ)の通知を受け取ることができる

## シンプルな通知



## 連携サービスへの通知



# New Relic アラートの構成要素4: Destinations

The screenshot shows the 'Email' configuration window. At the top left is an envelope icon and the word 'Email'. Below this is a section for selecting recipients: 'Select users and emails you want to send notifications to. See our docs'. A search bar with a magnifying glass icon and the text 'Search by name or email' is provided. The 'Email subject' field contains the placeholder text '{{ issueTitle }}'. Under 'Custom Details (optional)', there is a text area with the instruction 'This payload uses Handlebars syntax. Type "{{" to select from a list of variables.' At the bottom left is a 'Send test notification' button, and at the bottom right are 'Cancel' and 'Save' buttons.

- [Workflows変数](#)を用いて、柔軟にタイトルや内容のカスタムができます
  - 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。

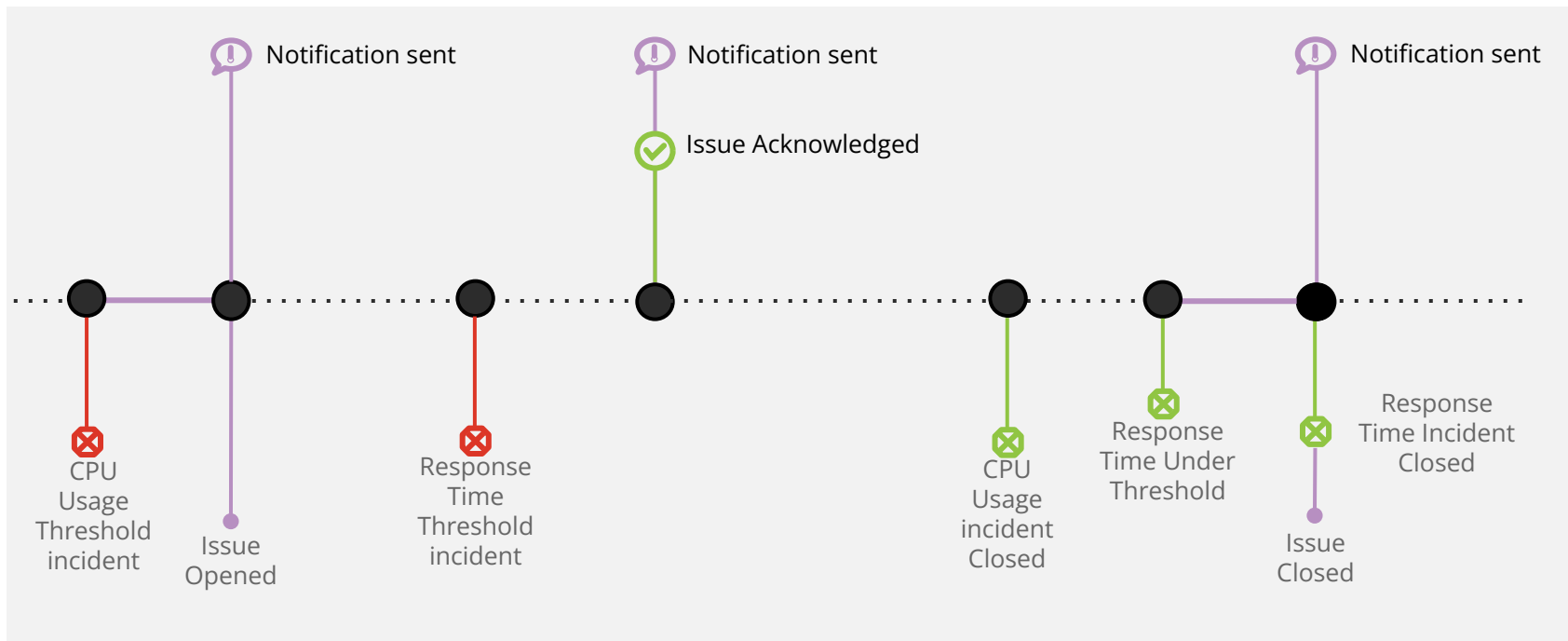
The screenshot shows the 'Slack' configuration window. At the top left is the Slack logo and the word 'Slack'. Below this is a section for selecting a destination: 'Slack destination' with a dropdown menu showing 'New Relic'. To the right of this is the text 'Select where you want to receive notifications. Pick an existing destination or create a new one. See our docs'. Under 'Channel', there is a dropdown menu showing 'Select Channel...' and a warning icon with the text 'Your user is not authenticated'. Under 'Custom Details (optional)', there is a text area with the instruction 'This payload uses Handlebars syntax. Type "{{" to select from a list of variables.' To the right of this is the text 'Custom Details (optional). Add a custom message at the bottom of every Slack notification. 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 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

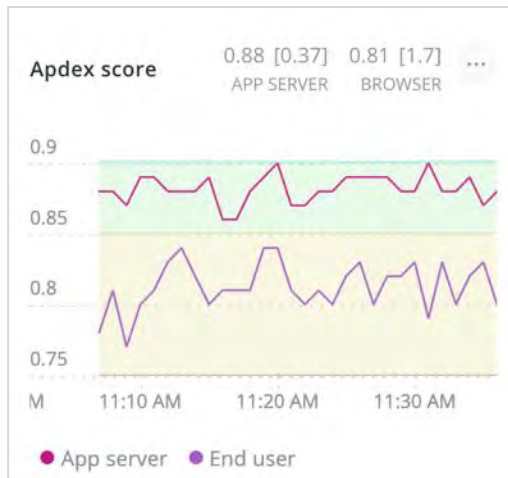
Issueの起票、Acknowledgeがされたタイミング、およびクローズの際に通知が届く



# 補足: 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 ?

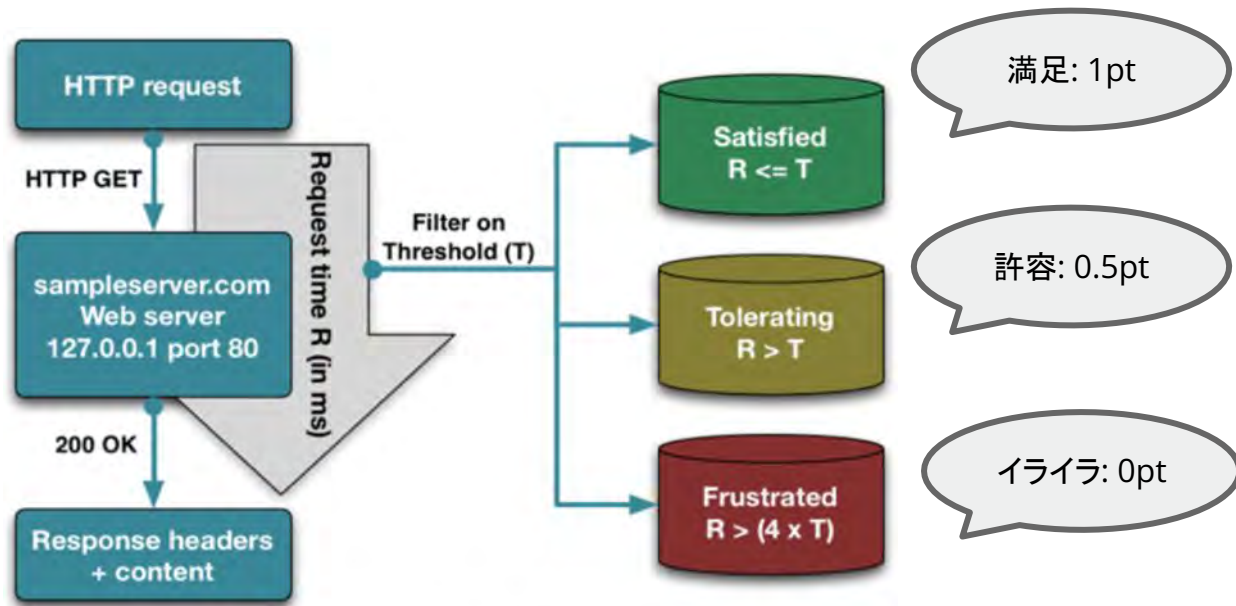
seconds

Please input a decimal or whole number only.

# 補足: 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)



# 今回監視対象のサイト

[NRUジェラートショップ](ECサイト)

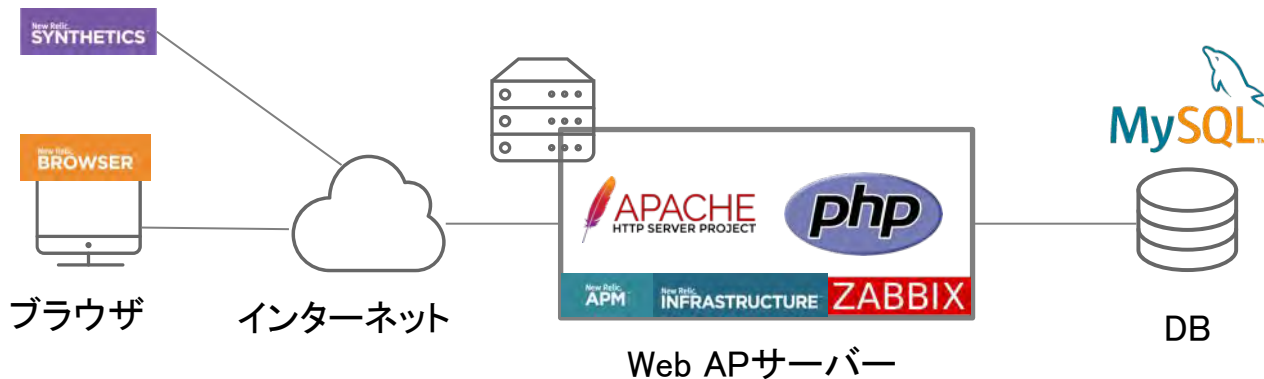
このハンズオンでは、PHPおよびMySQLにより構築されたジェラート屋さんの ECサイトを  
モニタリング対象にしています。

<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) 環境を確認する

15:40 - 15:50 (10min)



# 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+nrn@newrelic.com](mailto:japan-handson+nrn@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。

ユーザー名とパスワードは共通です。

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。



**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。

new relic

## Log in to see your data

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

Email  
japan-handson+nr@newrelic.com

Password  
|

Remember my email ⓘ

Log in

Or

Sign in with Google

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

Japan NRU Full platform user  
japan-handson+nr@newrelic.com

User Preferences  
API Keys  
Manage Your Plan

Account Settings

View settings  
Theme Light Dark Auto

NRQL Console ●

NR-only admin functionality  
Debug Mode ●

Manage Your Data  
View Your Usage

Other Users >

Log Out

new relic

## Log in to see your data

We found multiple logins for your email. This happens when you belong to more than one organization or authentication domain. [See the docs](#) for more info.

japan-handson+nr@newrelic.com  
Organization: Japan NRU  
Authentication Domain: Default

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

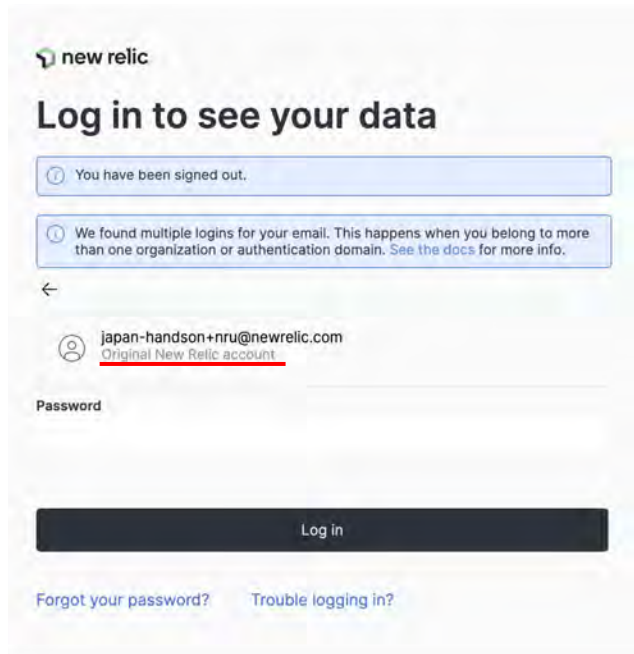
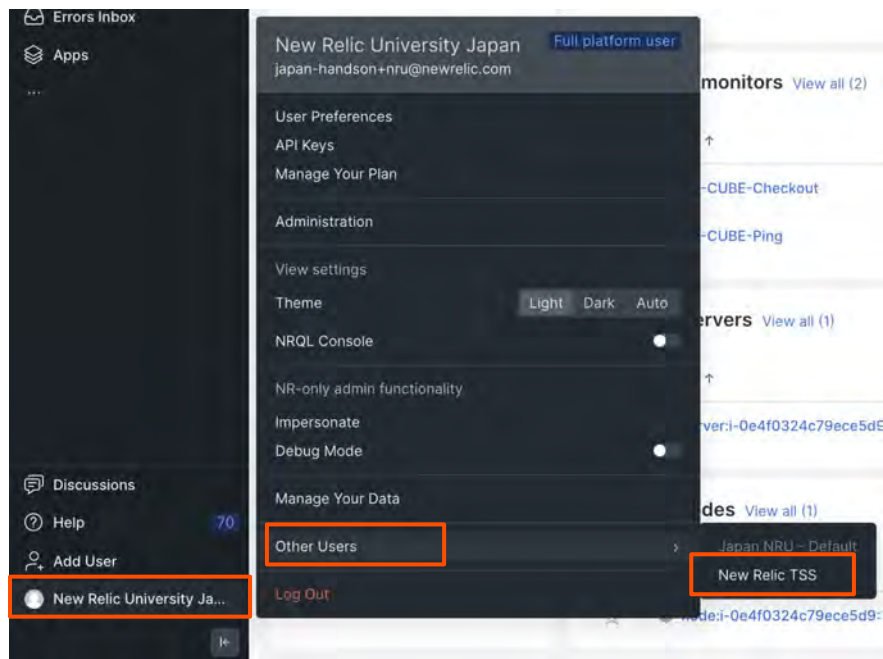
[Use a different account](#)



**IMPORTANT**

# ログインするNew Relicアカウントを切り替える

同じメールアドレスでログインしているアカウント間には、直接切り替えも可能です。  
(画面遷移が異なるだけで、結果は一回ログアウトする場合と同じです。)



# ハンズオン(0) 2つのアカウントにログインする

ログアウトすると、アカウントが選択できる  
パスワードは共通: oSz6nrupas

## Organization: Japan NRU


- 設定変更を伴うハンズオンはこちらのアカウントで実施します。

## Original New Relic account

- いくつかのサンプルデータが入っています。UI上でデータを確認する一部ハンズオンで、こちらのアカウントを使用します。
- Other Users の切替先に New Relic TSS と表示されているのも本アカウントです。

 new relic

## Log in to see your data

 We found multiple logins for your email. This happens when you belong to more than one organization or authentication domain. [See the docs](#) for more info.



japan-handson+nruc@newrelic.com  
Organization: Japan NRU  
Authentication Domain: Default



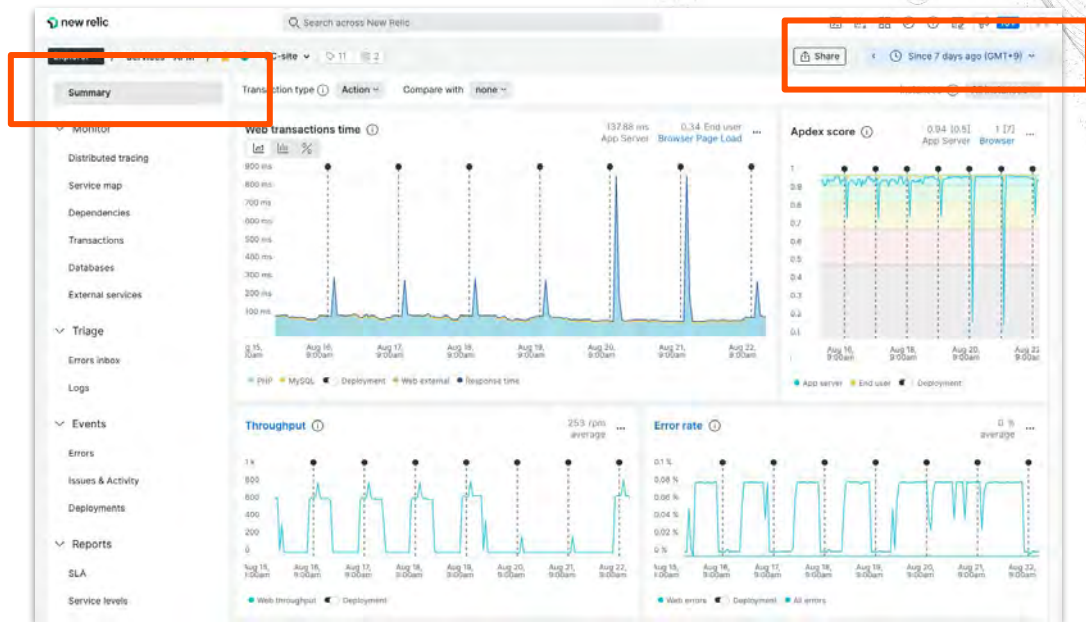
japan-handson+nruc@newrelic.com  
Original New Relic account

[Use a different account](#)

# ハンズオン(0) UIの確認

- New Relicポータルの左ペインの”APM & 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ポータルの左ペインの"APM & Services"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(1) アラートを作成する

15:50 - 16:10 (20min)



# 今回の環境の監視構成

## [前提]

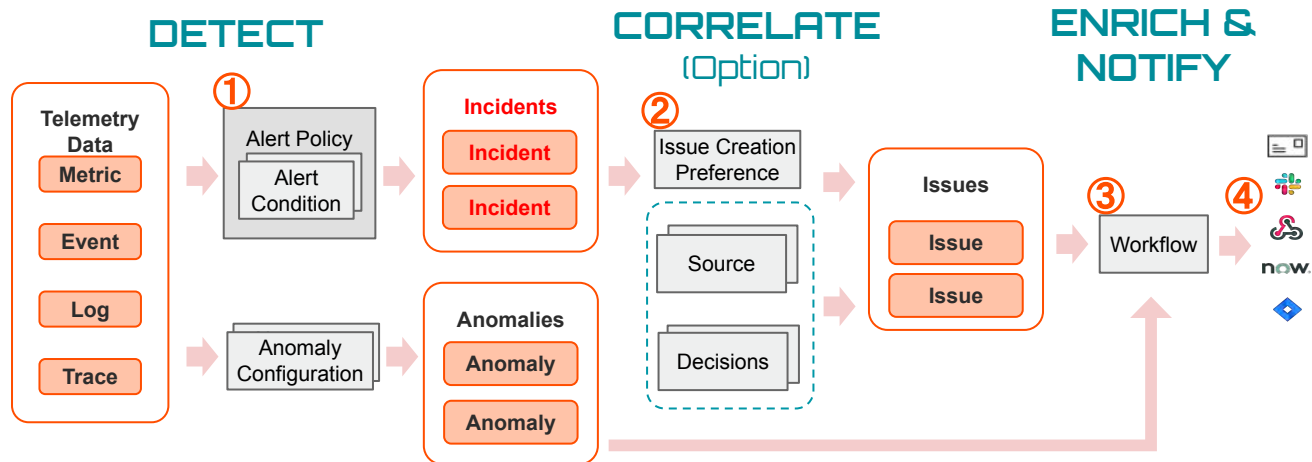
今回は**赤字**のアラートを設定してみます。

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	<b>チェックエラー</b>		
フロントエンド	<b>Apdex</b>	JSエラー		
アプリケーション	Apdex <b>応答時間</b>	<b>4xx, 5xxエラー</b>	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. Workflowを作成する



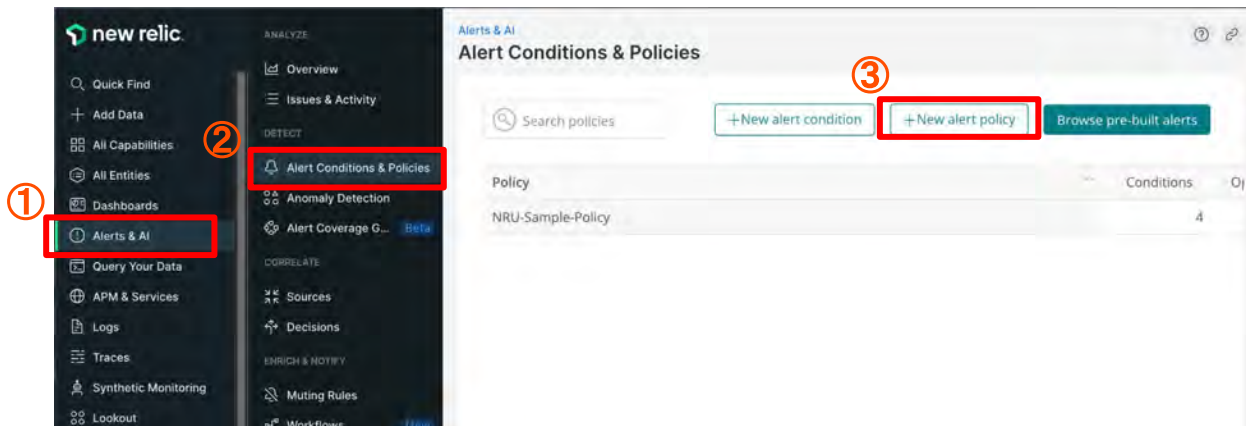


# 手順・解説

使用アカウント: Japan-NRU  
(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 1/2

1. Alerts&AI メニューを開きます。
2. Alert Conditions & Policies を開きます。
3. [+New alert policy] を選択して、新しいAlert Policyを作成します。



# ハンズオン(1-1) Alert policyを作成する 2/2

1. Alert Policy名には、ご自身が作成したとわかる名前をつけてください
2. [こちらのスライド](#) を参考に、好みの「Issue Creation Preference」を選択してください
3. [Correlate and suppress noise]をチェック
4. [Create policy without notifications] をクリックします

ウィザードでの一括作成もできますが、今回は各コンポーネントを手動で作成したいため、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-Sample-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.)

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 condition and signal

Group incidents sharing the same condition and signal into an issue.

This may create a large number of notifications.

③

#### 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.

④

Cancel

Create policy without notifications

Set up notifications

8

# ハンズオン(1-2) Alert Conditionを作成する 1/20

## [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	<b>チェックエラー</b>		
フロントエンド	<b>Apdex</b>	JSエラー		
アプリケーション	Apdex <b>応答時間</b>	<b>4xx, 5xxエラー</b>	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 2/20

- 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 3/20

- 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 interface for managing alert conditions. The left sidebar contains a navigation menu with categories like ANALYZE, DETECT, CORRELATE, ENRICH & NOTIFY, and SETTINGS. The 'Alerts & AI' section is highlighted. The main content area shows the 'Alert Conditions & Policies' page for a specific policy named 'NRU-Sample-Policy' with ID '4406018'. It includes options to 'Correlate and suppress noise', 'Issue Creation Preference: One issue per condition', and 'Delete this policy'. Below this, there are tabs for 'Alert conditions' and 'Notification settings'. The 'Alert conditions' tab is active, displaying a large gear icon and the message 'This policy doesn't have any conditions'. Below the message, it states 'Alert conditions are the criteria for creating incidents. Notifications are sent when an issue opens, is acknowledged, and closes.' A red box highlights the 'Create a condition' button at the bottom of the page.

# ハンズオン(1-2) Alert Conditionを作成する 4/20

- 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

Condition名は適切なものを各自設定してください

(例: NRU304-yourname-Synthetics-Failure)

# ハンズオン(1-2) Alert Conditionを作成する 5/20

- 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 6/20

- 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 7/20

- 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	
<input type="text" value="わかりやすい通知名"/>	
⊕ Add runbook URL	
<a href="#">← Back to Select entity</a>	<a href="#">Create condition</a>

# ハンズオン(1-2) Alert Conditionを作成する 8/20

- 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 9/20

- 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

(例: NRU304-yourname-End User Apdex)

# ハンズオン(1-2) Alert Conditionを作成する 10/20

- 「+ 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](#)

EC-CUBE-Checkout

Monitor check failure

[+ Add a condition](#)

# ハンズオン(1-2) Alert Conditionを作成する 11/20

- 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 12/20

- 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)

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

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

# ハンズオン(1-2) Alert Conditionを作成する 13/20

- 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 below

0.7 at least once in 5 minutes

⚠️ Add a warning threshold

Condition name

名前を追記 | End User Apdex (Low)

⊕ Add runbook URL

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

Create condition

# ハンズオン(1-2) Alert Conditionを作成する 14/20

- 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 15/20

- **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

(例: NRU304-yourname-transaction-time-baseline)

# ハンズオン(1-2) Alert Conditionを作成する 16/20

- 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。

The screenshot displays the '3. Define thresholds' configuration step for an alert condition. The 'Baseline Direction' is set to 'Upper only'. The target application is 'Web transaction time'. The condition is triggered when the 'average' deviates from the baseline 'at least once in' 5 minutes. A slider below this setting allows adjusting sensitivity, with a red callout box pointing to the left side labeled 'より敏感に' (More sensitive) and another pointing to the right side labeled 'より鈍感に' (Less sensitive).

The right side of the interface shows a performance chart for 'EC-site' over the last 2 days. The chart displays two data series: 'Web transaction time' (blue line) and 'Average web transaction time' (black line). Two vertical red lines indicate critical violations where the transaction time spikes significantly above the baseline. A legend at the bottom identifies the series, and a note suggests zooming in to see values not visible in larger time windows.

Buttons at the bottom include '< Back to Select entities' and 'Create condition'.

# ハンズオン(1-2) Alert Conditionを作成する 17/20

- **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. **Define your signal > Query the data you want to monitor**

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

3. **Set your condition thresholds**

- a. Threshold type: 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

(例: NRU304-yourname-NRQL-ErrorResponse)

# ハンズオン(1-2) Alert Conditionを作成する 18/20

- カテゴリにNRQL を選択すると右の画面に遷移します。
- クエリ入力欄に次の NRQL クエリをコピー&ペーストして、Nextをクリックします。

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

- クエリを入力すると、直近の状態を示す参考チャートが表示されます。

Define your signal

Tell this alert condition which signal to watch and tune it to match the signal.

Select your signals

[Build a query](#) Use NRQL to identify a signal

Golden signal or metric  
Entities: 7

Query the data you want to monitor \*

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

For help with [null values](#), [loss of signal](#), or other query options, see our [docs](#).

Showing 1/1 time series

100%  
95%  
90%  
85%  
80%  
75%  
70%  
65%  
60%  
55%  
50%  
45%  
40%  
35%  
30%  
25%  
20%  
15%  
10%  
5%  
0%

Critical threshold

2:00am 3:00am 4:00am 5:00am 6:00am 7:00am

# ハンズオン(1-2) Alert Conditionを作成する 19/20

- Adjust to signal behaviorはすべて初期値のままNextをクリックします。
- 閾値設定は任意ですが、以下を参考に設定してみてください。

**Set static thresholds** Looking for different setting? [Try anomaly thresholds](#)

Set thresholds for a query that returns a static value.

Open incidents:

Severity level **Critical** ▾

When a query returns a value **above or equal to** ▾ **1** **at least once in** ▾ **5** ▾ **minutes** ▾

[+ Add threshold](#)

[+ Add lost signal threshold](#)

Cancel [Back](#) [Next](#)

# ハンズオン(1-2) Alert Conditionを作成する 20/20

- 任意のAlert Condition名を設定します。
- Custom incident descriptionとRunbook URLはオプションです。何か思いついた内容を記載してみてください。
- Enable on saveが図の状態になっていることを確認し、Save conditionをクリックします。
- 設定確認画面が表示されるので、Closeをクリックして閉じます。

**Add alert condition details**

Make this alert condition easy to find and use.

**Name \***

NRU304-Sample-NRQL-ErrorResponse

**Additional Settings**

Close open incidents after 3 days

**Send a custom incident description (optional)**

ここに記述した情報が、Incidentの詳細情報としてアラート内に記載されます。

4,000 character limit

**Runbook URL (optional)**

https://one.newrelic.com/dashboards?account=3940716&duration=1800000&state=i

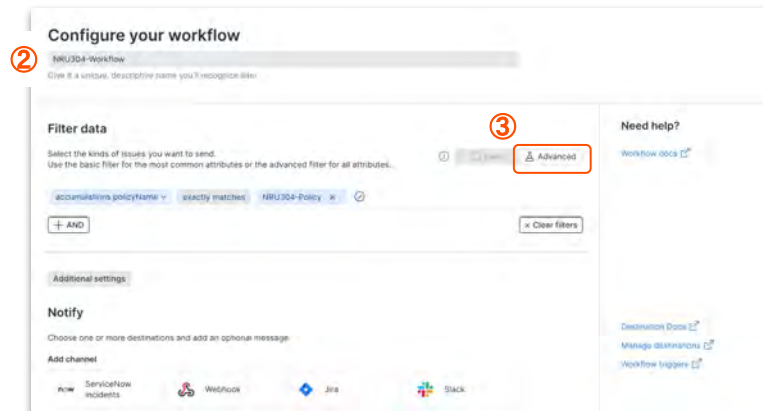
Enable on save

**Enable on save**

Cancel Back **Save condition**

# ハンズオン(1-3) Workflow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workflowであることがわかる名前を入力します
3. Filter dataで"Advanced"を選択し、次のフィルタを設定します
  - 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**



# ハンズオン(1-3) Workflowを作成する 2/6

4. Notify: **Email**を選択します
5. メール送信内容を設定します  
ご自身のメールアドレスを入力して下さい。
6. Send test notificationボタンをクリックし、テストメールを送信します。受信トレイを確認してみましょう。(次スライドで補足)
7. Saveボタンをクリックします

The screenshot displays the 'Notify' configuration screen in the New Relic workflow builder. At the top, it says 'Notify' and 'Choose one or more destinations and add an optional message.' Below this, there are several destination cards: ServiceNow incidents, Webhook, Jira, Slack, Email, AWS EventBridge, and PagerDuty. The 'Email' card is highlighted with a red circle 4. Below the destination cards, there is a 'Test this workflow' section with a 'Test workflow' button and a checkbox for 'We found a possible problem above.' A red circle 8 is next to the 'Test workflow' button. At the bottom right, there are 'Cancel' and 'Activate workflow' buttons, with a red circle 9 next to 'Activate workflow'. A red circle 5 is next to the 'Email' card in the second screenshot. The second screenshot shows the 'Email' configuration screen with fields for 'Select users and emails you want to send notifications to', 'Email subject', and 'Custom Details (optional)'. A red circle 6 is next to the 'Send test notification' button at the bottom. A red circle 7 is next to the 'Cancel' button at the bottom right.

# ハンズオン(1-3) Workflowを作成する 3/6

受信したテストメールを確認します。

- Policy名やCondition名は確認できますか？
- Runbook URLはどこに記載されていますか？
- Tagsというセクションには、どのような情報が含まれていますか？

余裕があれば、Email subjectやCustom Detailsを変更し、再度テストを行ってみてください。

- 例えばIssueが起票された時刻をCustom Detailsに含めるには、以下のように追記します。

```
Issue activated at : {{ issueActivatedAtUtc }}
```

- “`{{`”と入力すると、利用可能な環境変数の一覧が表示されます。

The screenshot shows a New Relic alert interface. At the top, it says "Critical priority issue is closed" and "Memory Used % is more than 90 for at least 2 minutes on 'Some-Entity'". Below this, it indicates "Issue duration: 5 minutes" and has a "Go to issue" button. The page lists "1 incidents" and "2 impacted entities", with one entity listed as "ip-172-31-26-144.ap-northeast-1.compute.internal". Under the "Alert Policy" section, it shows:
 

Policy Name	NRU-Sample-Policy
Condition	NRU-Sample-Web transaction time (Baseline)
Runbook	<a href="https://docs.newrelic.com/docs/alerts-applied-intelligence/new-relic-alerts/advanced-alerts/understand-technical-concepts/provide-runbook-instructions-alert-activity/">https://docs.newrelic.com/docs/alerts-applied-intelligence/new-relic-alerts/advanced-alerts/understand-technical-concepts/provide-runbook-instructions-alert-activity/</a>
NRQL	SELECT count(*) from Metric
Custom Violation Description	condition-1-a desc

 The "Tags" section at the bottom lists various metadata like account, assignmentGroup, language, type, and affectedService.

# ハンズオン(1-3) Workflowを作成する 4/6

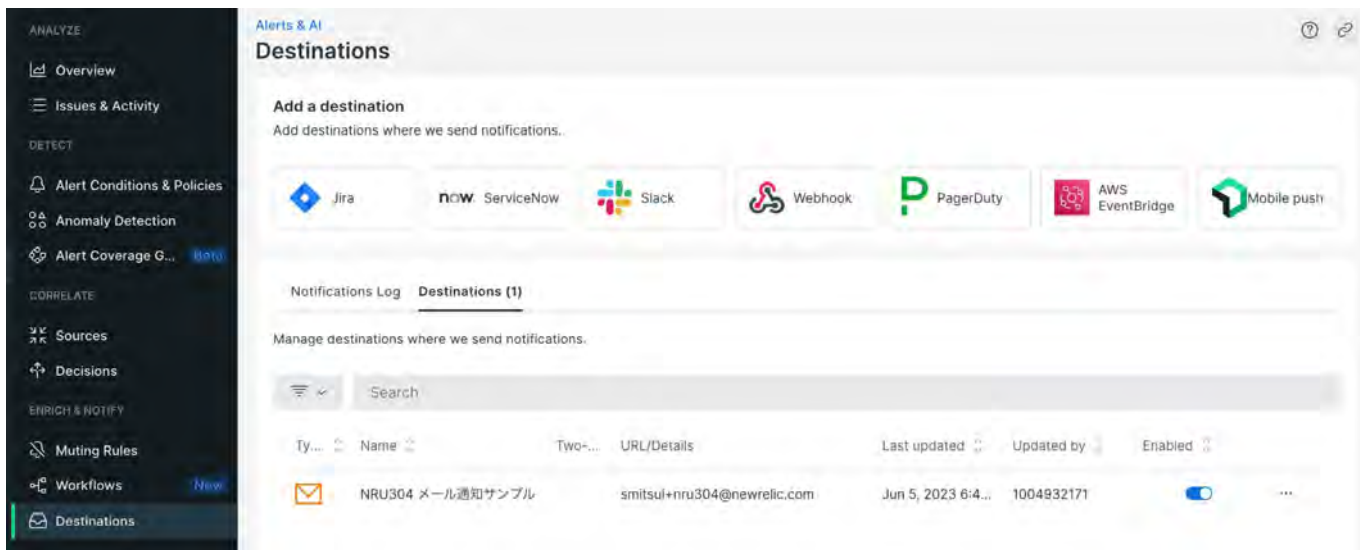
8. Test workflowボタンを押し、テスト用メール内容を確認してください。
  - b. 先程のテスト用メールとどのような違いがあるかを確認してください
9. Activate workflowボタンをクリックし、設定を保存します

The screenshot displays the New Relic workflow configuration interface. The top section is titled 'Notify' and includes a sub-instruction: 'Choose one or more destinations and add an optional message.' Below this, there are several destination selection cards: ServiceNow incidents, Webhook, Jira, Slack, Email, and AWS EventBridge. A red circle with the number '4' is placed over the 'Email' card. Below the destination cards, there is a 'Test this workflow' section with a 'Test workflow' button and a checkbox labeled 'We found a possible problem above.' A red circle with the number '8' is placed over the 'Test workflow' button. At the bottom right of the main configuration area, there are 'Cancel' and 'Activate workflow' buttons, with a red circle and the number '9' placed over the 'Activate workflow' button. An arrow points from the 'Email' card in the top section to the 'Email' configuration dialog shown below. This dialog has a search bar for selecting users and emails, an 'Email subject' field with a placeholder '({ issueTitle })', and a 'Custom Details (optional)' field. A red circle with the number '5' is placed over the 'Email subject' field. At the bottom of the dialog, there is a 'Send back notification' checkbox and a 'Done' button, with a red circle and the number '7' placed over the 'Done' button.

# ハンズオン(1-3) Workflow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 > Destinationsで、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。

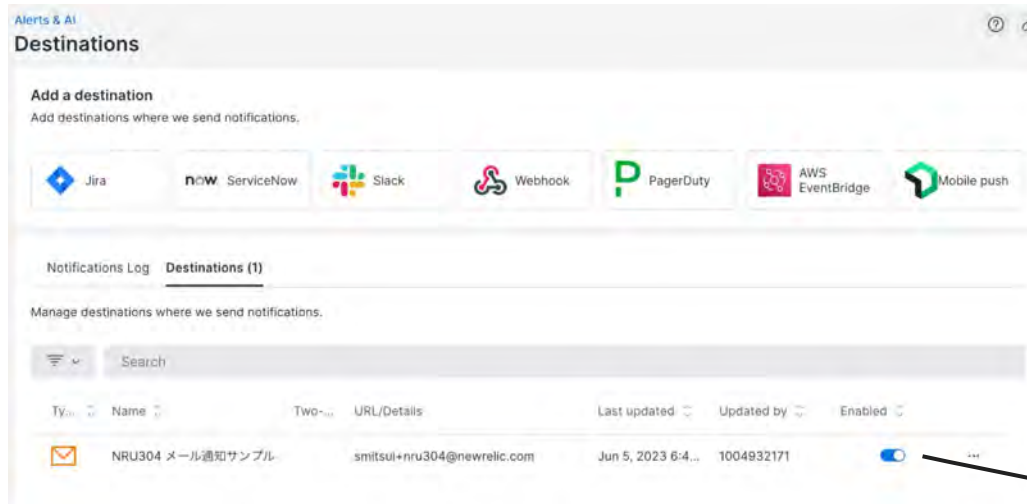


The screenshot displays the 'Alerts & AI' interface, specifically the 'Destinations' section. The left sidebar shows navigation options like 'Overview', 'Issues & Activity', 'Alert Conditions & Policies', 'Anomaly Detection', 'Alert Coverage G...', 'Sources', 'Decisions', 'Muting Rules', 'Workflows', and 'Destinations'. The main content area includes a search bar and a table of destinations. The table has columns for 'Name', 'URL/Details', 'Last updated', 'Updated by', and 'Enabled'. One destination is listed: 'NRU304 メール通知サンプル' with the URL 'smitsul+nru304@newrelic.com', last updated on 'Jun 5, 2023 6:4...', and updated by '1004932171'. The 'Enabled' toggle is turned on.

Type	Name	Two...	URL/Details	Last updated	Updated by	Enabled
✉	NRU304 メール通知サンプル		smitsul+nru304@newrelic.com	Jun 5, 2023 6:4...	1004932171	🔴

# ハンズオン(1-3) Workflow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。



Alerts & AI Destinations

Add a destination  
Add destinations where we send notifications.

Jira ServiceNow Slack Webhook PagerDuty AWS EventBridge Mobile push

Notifications Log Destinations (1)

Manage destinations where we send notifications.

Type	Name	Two...	URL/Details	Last updated	Updated by	Enabled
✉	NRU304 メール通知サンプル		smitsui+nru304@newrelic.com	Jun 5, 2023 6:4...	1004932171	🟢

有効



無効



Type	Name	Two...	URL/Details	Last updated	Updated by	Enabled
✉	NRU304 メール通知サンプル		smitsui+nru304@newrelic.com	Jun 5, 2023 6:4...	1004932171	🟢



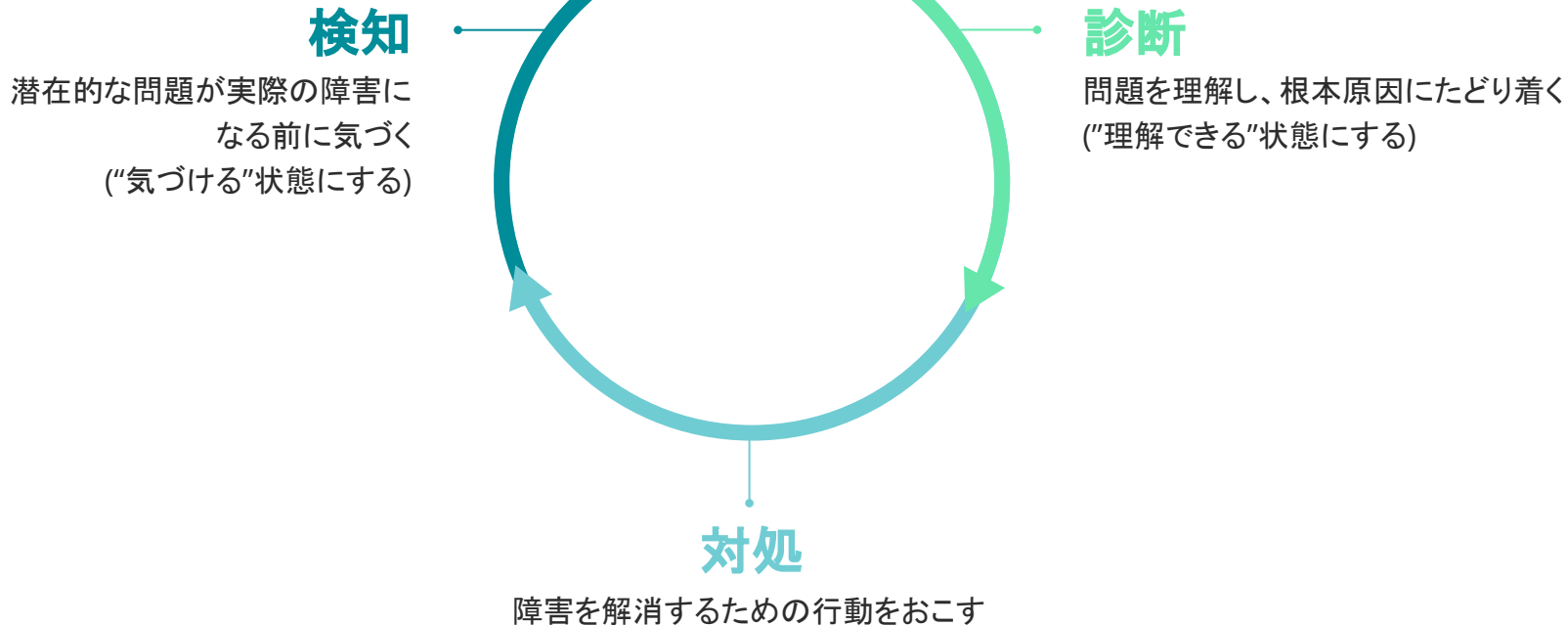
# 座学(3)

## New Relicのアラート分析支援機能

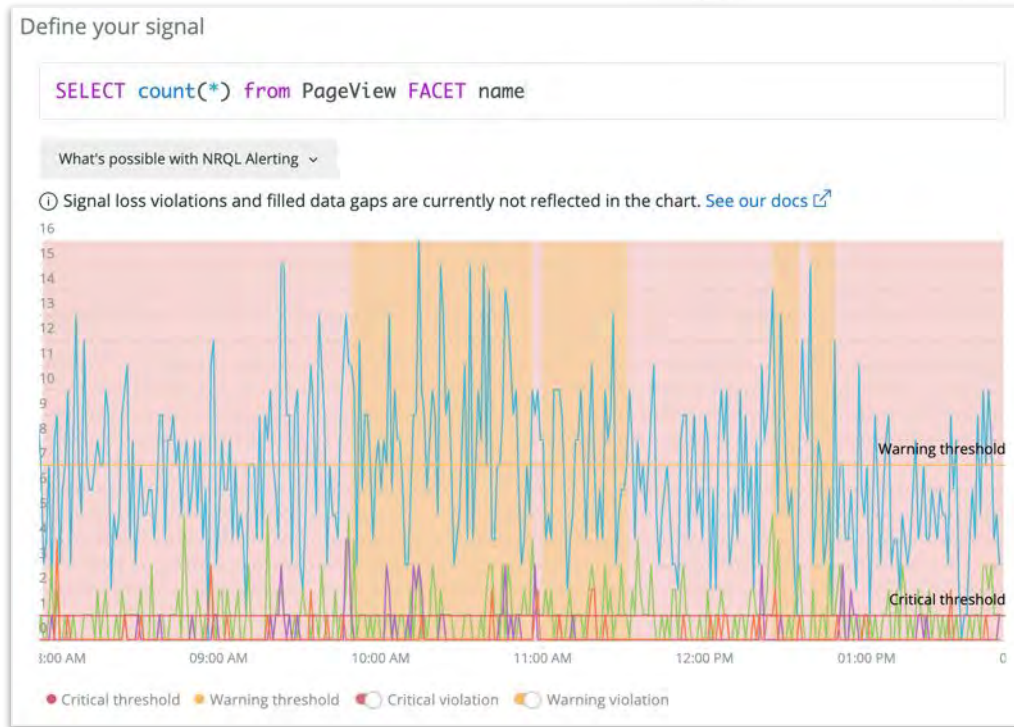
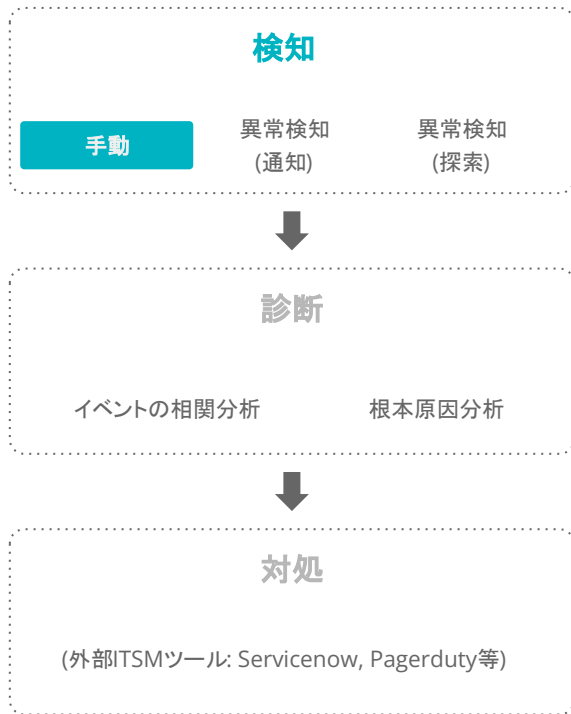
16:10 - 16:20 (10min)



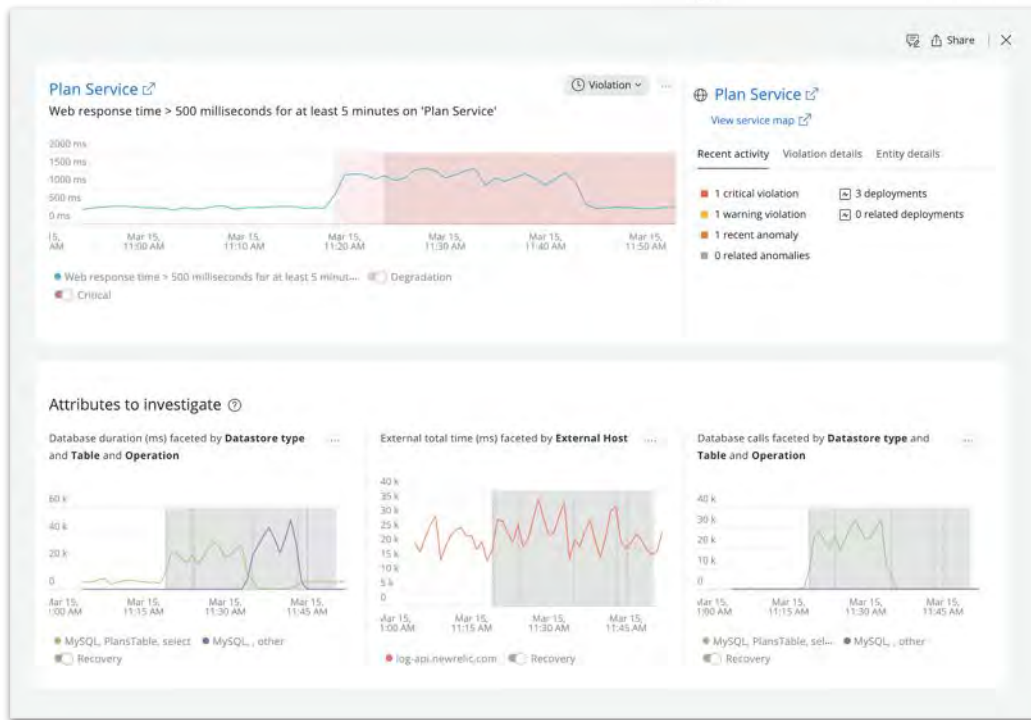
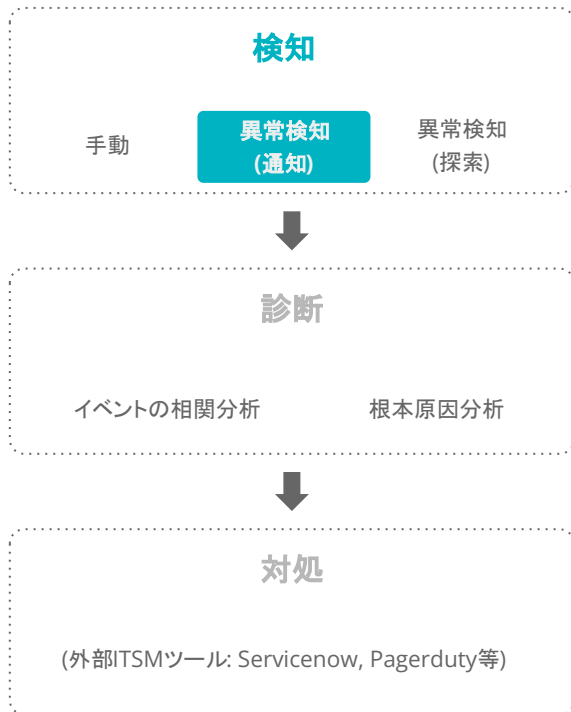
# New Relic AIOpsによるインシデント対応フロー



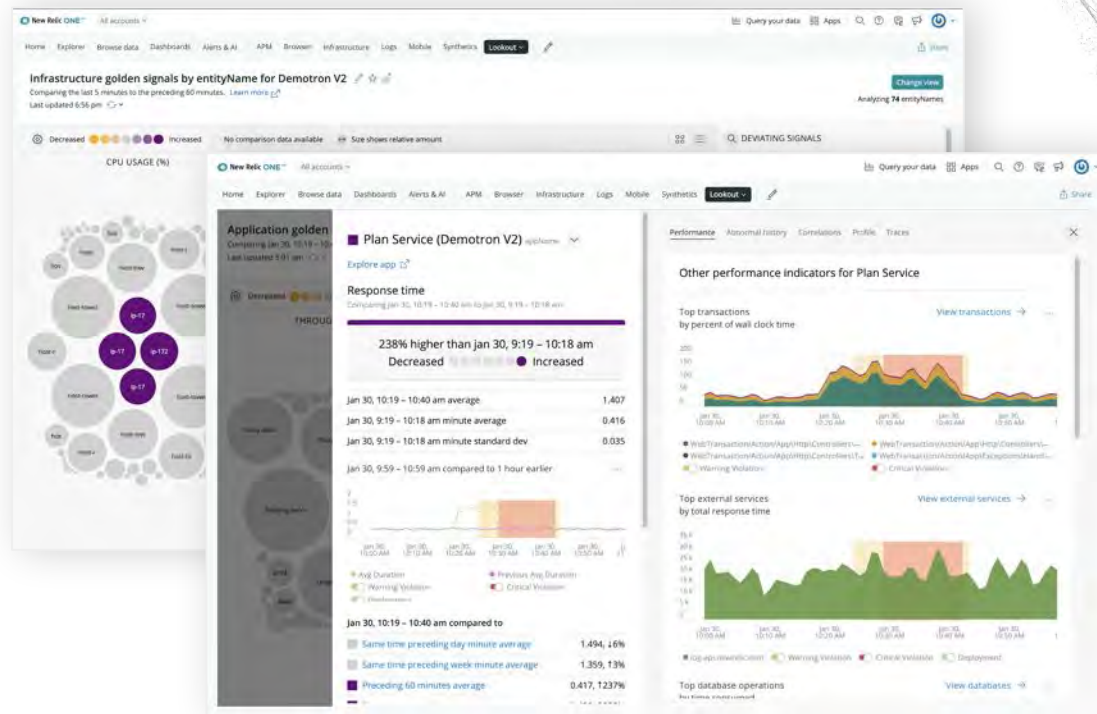
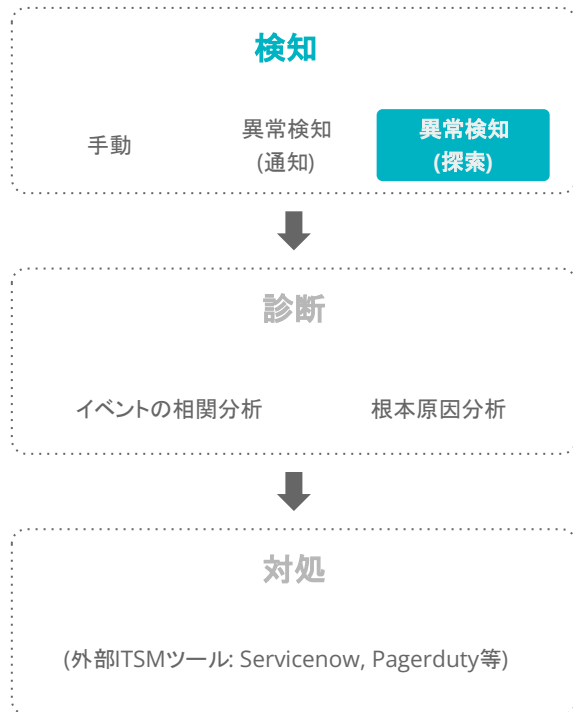
# 検知1: 重要な指標に対する手動アラートによる気づき



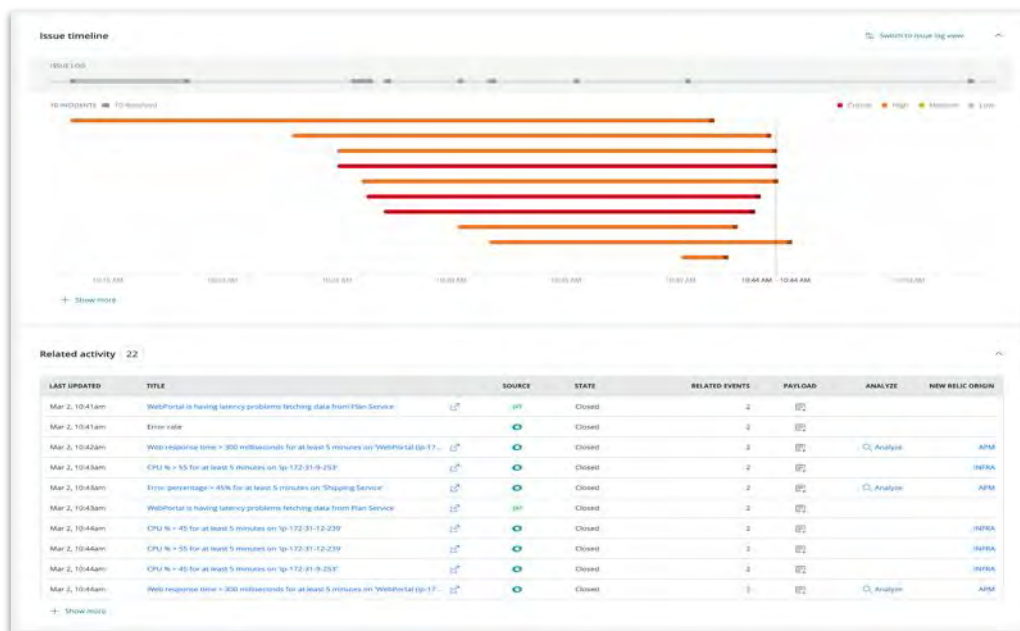
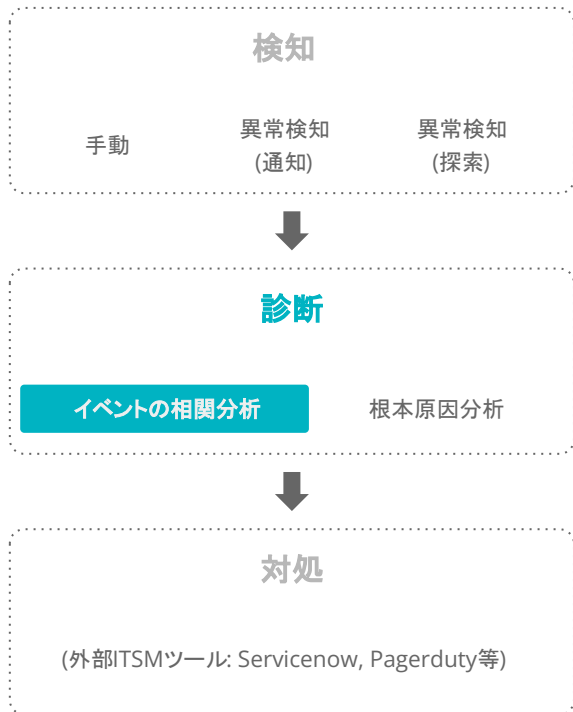
# 検知2: Anomaly Detectionによる異常の通知



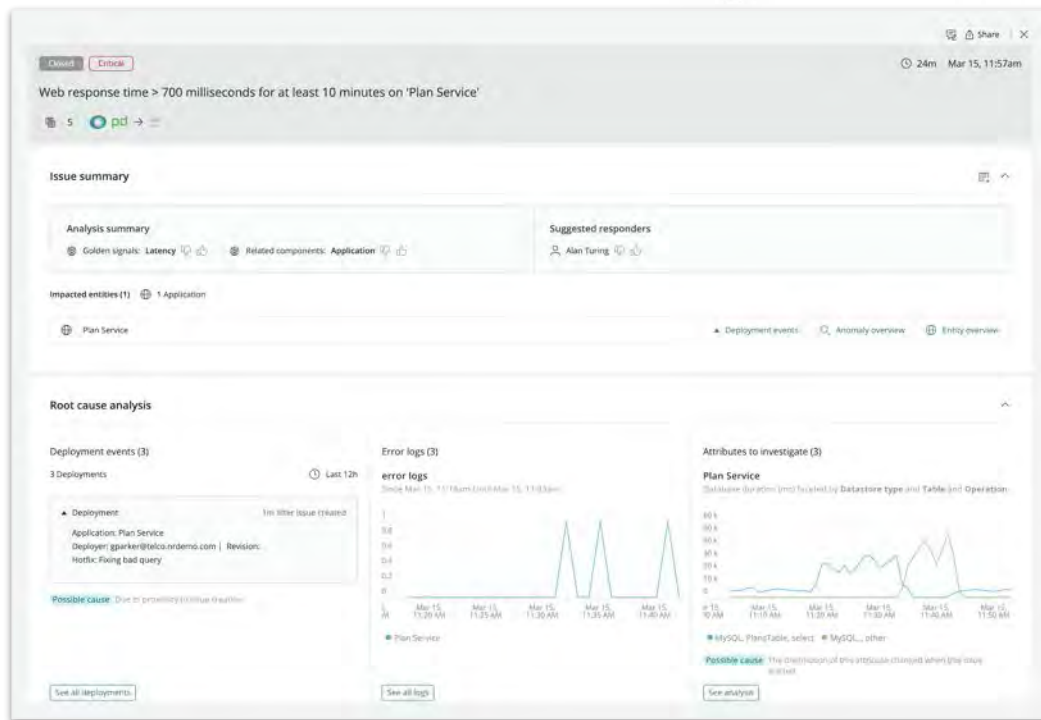
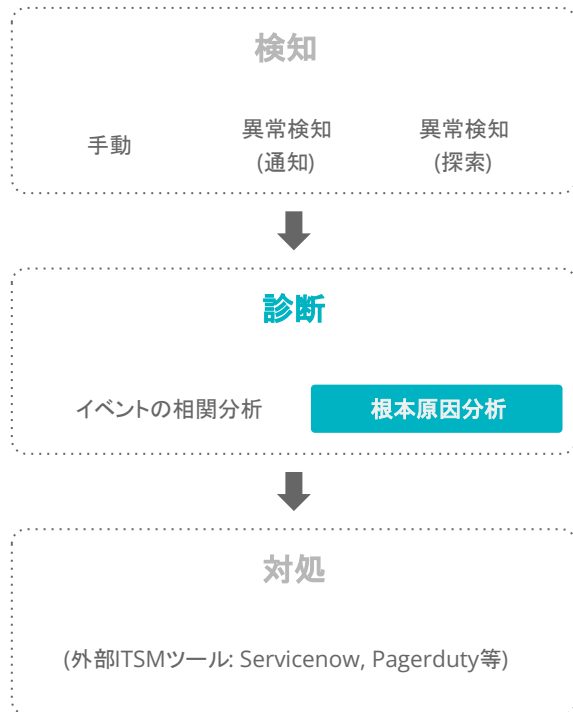
# 検知3: Lookoutによる異常の可視化と探索



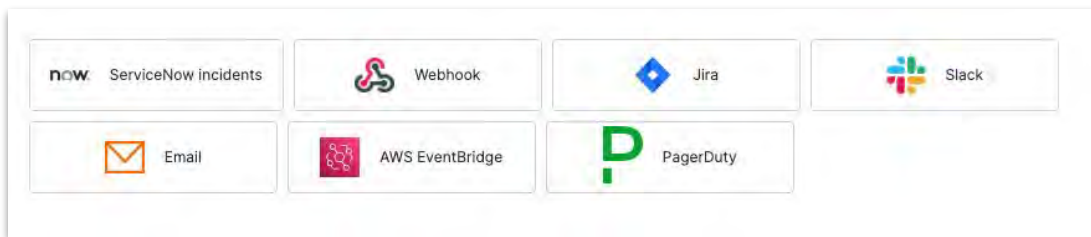
# 診断1: Correlationによるアラート統合とノイズの削減



# 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) アラート分析支援機能 ウォークスルー

16:20 - 16:30 (10min)



# ハンズオン(2-1) 異常を可視化する

## [目的]

New Relic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、「Original New Relic 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]

**New RelicのAlerts & AI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、個々のIncidentの詳細を確認する
  - 画面上部のフィルター設定で、Open中以外のものも表示してみましょう
  - 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]

ハンズオン(2-2)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、個々のIssueを確認する
  - Root cause analysisや、Impacted entitiesにはどのような項目が書かれているでしょうか

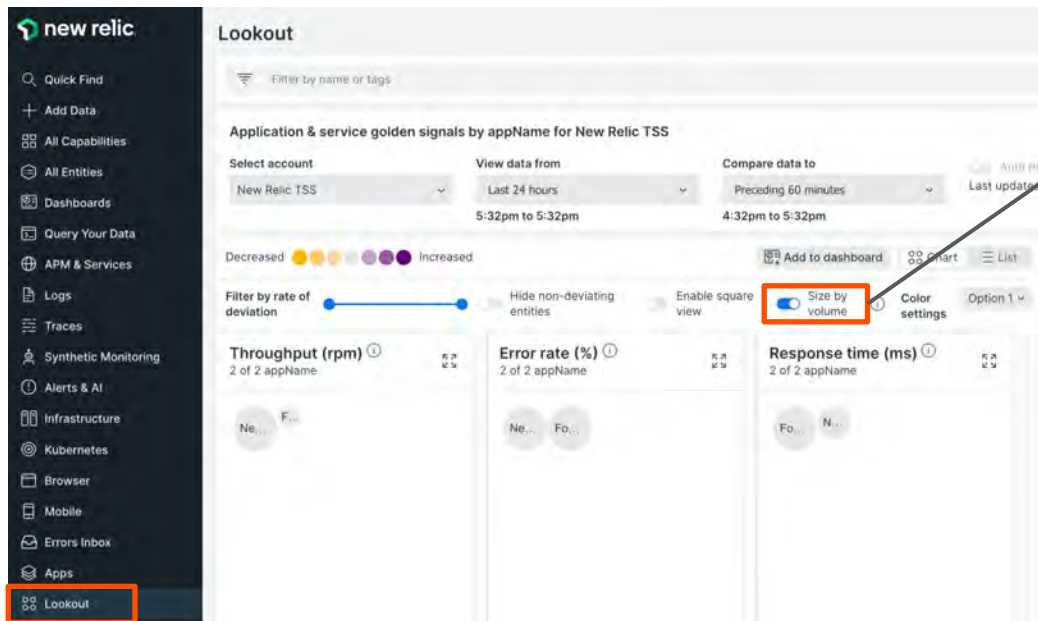


# 手順・解説

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

# ハンズオン(2-1) 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

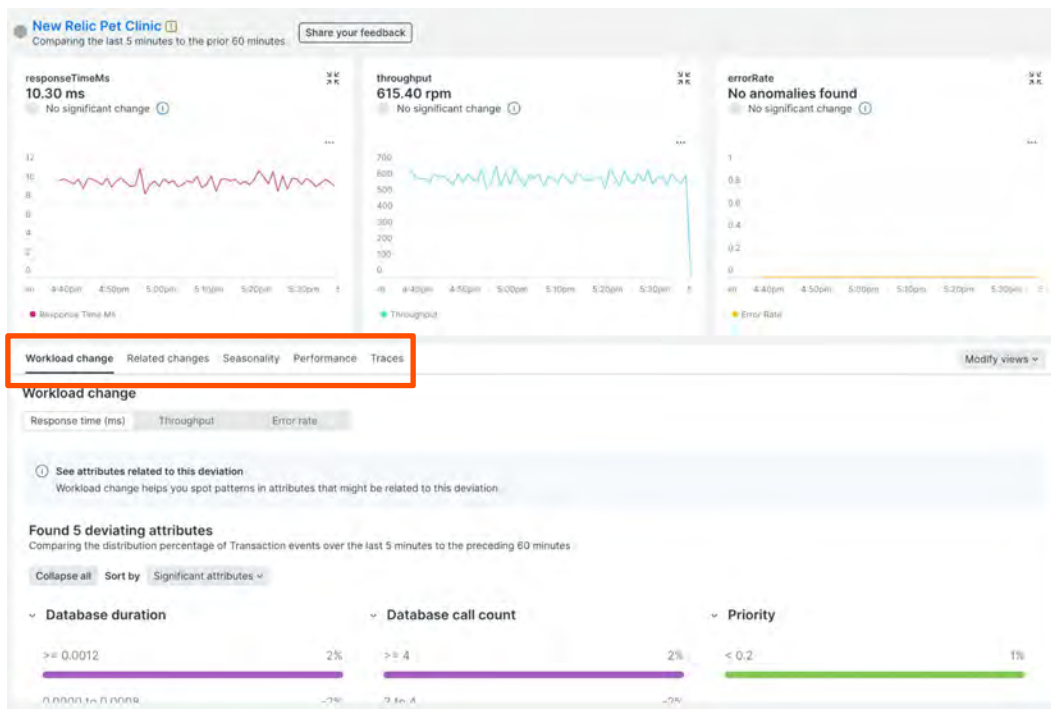
ハンズオン環境では大きな変化率を確認できない可能性があるため、その場合は後ほどデモ環境をお見せします

# ハンズオン(2-1) 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

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

見終わったら右上のxをクリックします



# ハンズオン(2-1) 異常を可視化する

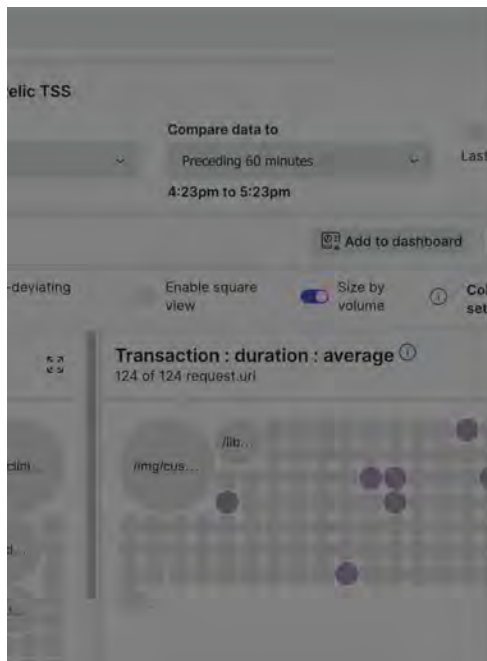
- カスタムのビューを作成します

Manage Views → Create a new queryを選択

The screenshot shows the New Relic Lookout interface. At the top, the title 'Lookout' is visible. Below it, there's a search bar 'Filter by name or tags'. The main section is titled 'Application & service golden signals by appName for New Relic TSS'. It includes controls for 'Select account' (New Relic TSS), 'View data from' (Last 5 minutes, 7:46pm to 7:51pm), and 'Compare data to' (Preceding 60 minutes, 6:46pm to 7:46pm). There's also an 'Auto Refresh' toggle and a 'Last updated' timestamp of 7:56pm. A legend indicates 'Decreased' (yellow to red) and 'Increased' (purple to blue) with a note 'Size shows relative amount'. Three charts are visible: 'Throughput (rpm)', 'Error rate (%)', and 'Response time (ms)'. The 'Throughput (rpm)' chart shows data for 'New Relic Pet Clinic' and 'FoodM'. The 'Response time (ms)' chart shows data for 'FoodMe' and 'New Relic Pet'. On the right, 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' (highlighted with a red box), 'Save view', and 'Save view as...'. The page number '90' is in the bottom right corner.

# ハンズオン(2-1) 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

New Relic TSS

### Select data type

Metrics

Events

①Eventsを選択

Or write a NRQL query

### View a chart with

Transaction : count

Transaction : average : duration

+ Add row

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

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

### Facet by

request.uri

④request.uriを選択

### View data from

Last 5 minutes

### Compare data to

Preceding 60 minutes

### Name your view (optional)

NRU304-Sample-CustomView

⑤ご自身の名前を入力

Cancel

Create New View

⑥Create New Viewをクリック

# ハンズオン(2-2) 個々のアラートを確認する

- 「Organization: Japan-NRU」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 shows the New Relic Alerts & AI interface. The left sidebar is dark-themed and contains a navigation menu. The 'Alerts & AI' section is highlighted, and the 'Overview' option is circled in red. The main content area is titled 'Alerts & AI Issues & Activity'. It features a tabbed interface with 'Issues' selected. Below the tabs is a search bar and a 'Show issues chart' toggle. The chart is a bar chart showing the number of issues over time. The x-axis represents time intervals from Jun 03 11:59am to Jun 05 11:59pm. The y-axis represents the number of issues, ranging from 0 to 4. The chart shows a single red bar (Critical) at Jun 04 5:59am and several orange bars (High) on Jun 05. A legend below the chart identifies the severity levels: Low (grey), Medium (yellow), High (orange), and Critical (red). A note at the bottom of the chart area states: 'Anomalies are included by default in the "source" filter above. If you want to hide anomalies in this view, remove them from the filter. Filter out anomalies'.

# ハンズオン(2-2) 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 interface. On the left is a dark sidebar with a navigation menu. The 'Issues & Activity' option is highlighted with a red box. The main content area is titled 'Alerts & AI Issues & Activity'. Below the title, the 'Incidents' tab is selected and highlighted with a red box. A bar chart shows incident counts over time, with a legend for Low, Medium, High, and Critical priorities. Below the chart, a notification states: 'Anomalies are included by default in the "source" filter above. If you want to hide anomalies in this view, remove them from the filter. Filter out anomalies.' At the bottom, a table lists incidents with columns for State, Priority, Created, Duration, Incident name, Entity name, Source, Events, and Muted.

State	Priority	Created ↓	Duration	Incident name	Entity name	Source	Events	Muted
<input type="checkbox"/>	Closed	Critical	54m ago	24m	Web respons...	EC-s...	2	
<input type="checkbox"/>	Open	High	56m ago	56m	Problem start...	API	1	

# ハンズオン(2-2) 個々のアラートを確認する

- Incidentをクリックします。



	State	Priority	Created ↓	Duration	Incident name	Entity na...	Source	Events	Muted
<input type="checkbox"/>	Closed	Critical	54m ago	24m	Web respons...	EC-s...		2	
<input type="checkbox"/>	Open	High	56m ago	56m	Problem start...		API	1	
<input type="checkbox"/>	Closed	Critical	1h 55m ...	31m	Web respons...	EC-s...		2	

# ハンズオン(2-2) 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。



Incident accumulation [Copy payload](#)

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(2-3) 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

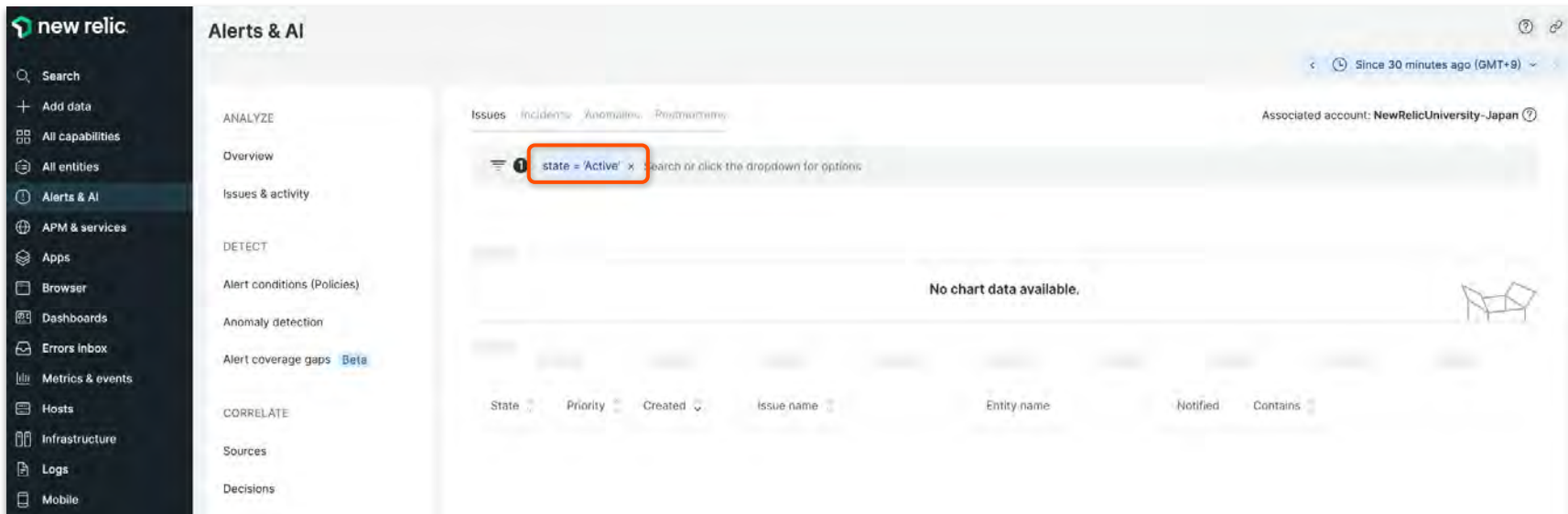
- 「Issues」タブをクリックします。

The screenshot shows the New Relic Alerts & AI interface. The left sidebar contains navigation options like Search, Add data, All capabilities, All entities, Alerts & AI, APM & services, Apps, Browser, Dashboards, Errors inbox, Metrics & events, Hosts, Infrastructure, Logs, and Mobile. The main content area is titled 'Alerts & AI' and includes sections for ANALYZE, Overview, Issues & activity, DETECT, Alert conditions (Policies), Anomaly detection, Alert coverage gaps (Beta), CORRELATE, Sources, and Decisions. The 'Issues' tab is highlighted with a red box. Below the tabs, there is a search bar with the filter 'state = 'Active'' and a bar chart showing two orange bars representing active issues. 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(2-3) 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

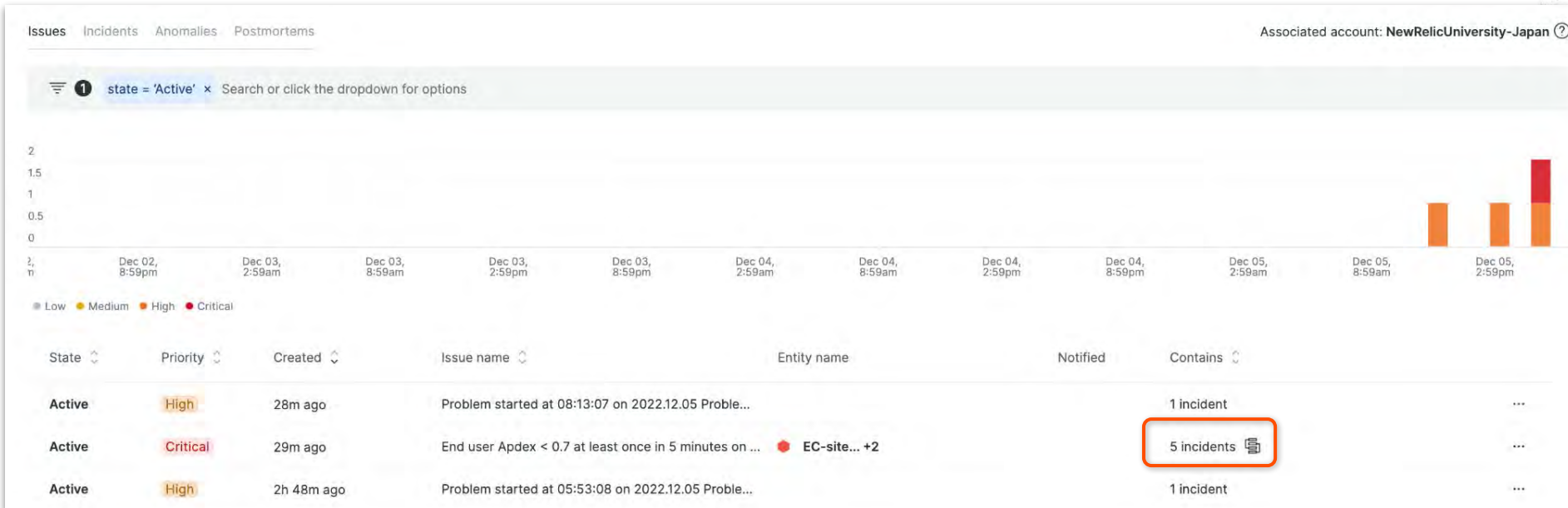
- オープン中のIssueが存在しない場合は「Active」フィルタを削除します。



The screenshot shows the New Relic Alerts & AI interface. The left sidebar contains navigation options such as Search, Add data, All capabilities, All entities, Alerts & AI (selected), 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 the filter 'state = Active' highlighted by a red box. Below the search bar, there is a section for 'ANALYZE' with options like Overview, Issues & activity, DETECT, Alert conditions (Policies), Anomaly detection, and Alert coverage gaps (Beta). The 'CORRELATE' section includes Sources and Decisions. A table at the bottom shows columns for State, Priority, Created, Issue name, Entity name, Notified, and Contains. The interface also displays 'Since 30 minutes ago (GMT+9)' and 'Associated account: NewRelicUniversity-Japan'.

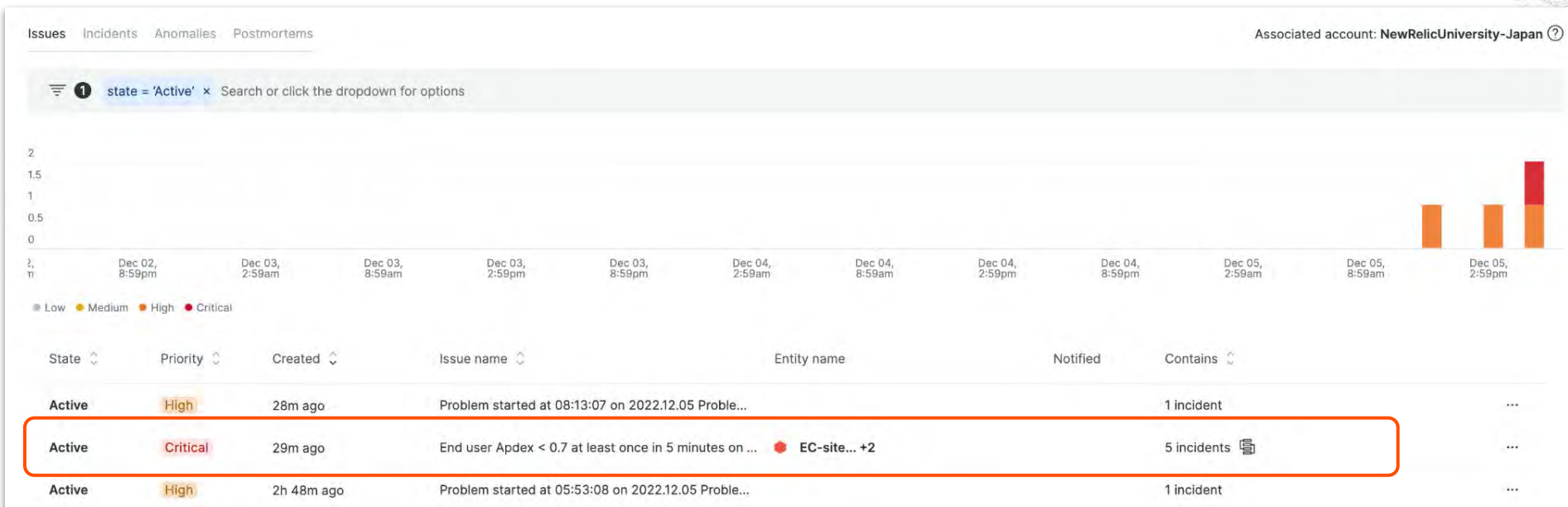
# ハンズオン(2-3) 複数のアラートを紐付け トラブルシューティングに役立てる

- 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(2-3) 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

- Issueをクリックすると詳細が表示されます。



# 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

- 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

The screenshot displays the New Relic incident management interface. At the top, a critical priority issue is activated at Dec 5, 2022 5:12pm. The main alert is 'End user Apdex < 0.7 at least once in 5 minutes on 'EC-site'', with 5 incidents and a source of 'Issue payload'. A list of 5 incidents is shown, with the first one highlighted in an orange box. The detailed view of the selected incident shows it was opened today at 5:16pm. The alert is 'EC-site query result is > 1.0 for 5 minutes on 'NRU302\_alert\_lab'', with a source of 'Alert Policy: ダッシュボードハンズオン用アラートポリ...' and a condition of 'NRU302\_alert\_lab'. A line graph shows the query result over time, with a red shaded area indicating the alert period from 5:10pm to 5:25pm. The graph shows a sharp increase in the query result starting at 5:10pm, peaking at approximately 25, and remaining high until 5:25pm. The incident is tagged with 'EC-site' and has 10 tags. The entity type is 'BROWSER' and the account is 'NewRelicUniversity-Japan'.

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

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

Incidents: 5 Source: Issue payload

Last updated Dec 5, 2022 5:17pm

Close Issue Acknowledge

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

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

See NRQL overview

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

EC-site

Tags: 10

account: NewRelicUniversit... accountId: 2511671 appName: EC-site clusterAgentId: 445000097 enabled: true

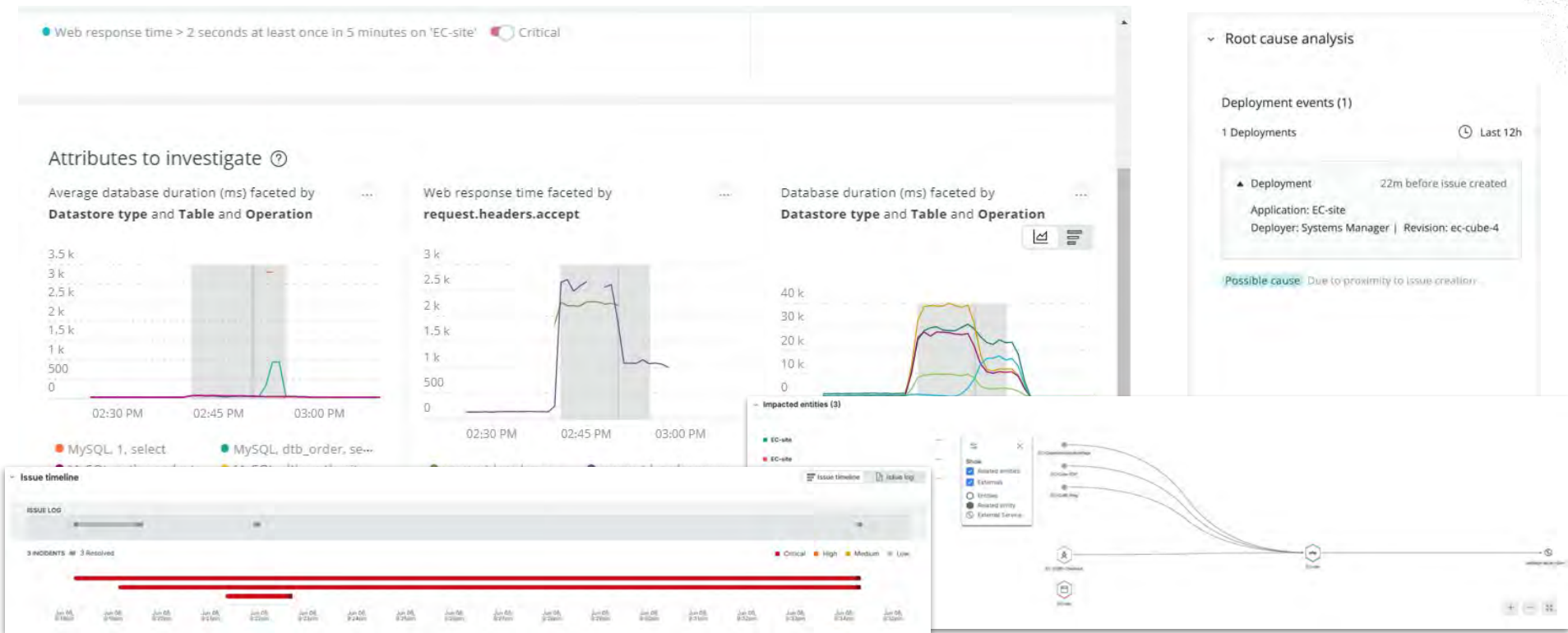
Entity type: BROWSER

Account: NewRelicUniversity-Japan id: 24752895 nr.has\_sliis: true policyId: 1065477 trustedAccountId: 2490334 type: NRQL Query

Incident payload

# 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

- 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



# 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)



## とりあえずの監視

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

努力と根性と属人性で  
Actionableな監視を増やす



Actionableな監視予備群

監視できていない未知  
の領域

気づける

頑張ってすべての  
障害ポイントを  
洗い出す



気づけない

# 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

New RelicのAlerts & “AI”

→ **Applied Intelligence**

応用知能:機械学習によって得たデータを元に運用をアシスト

# AI Ops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

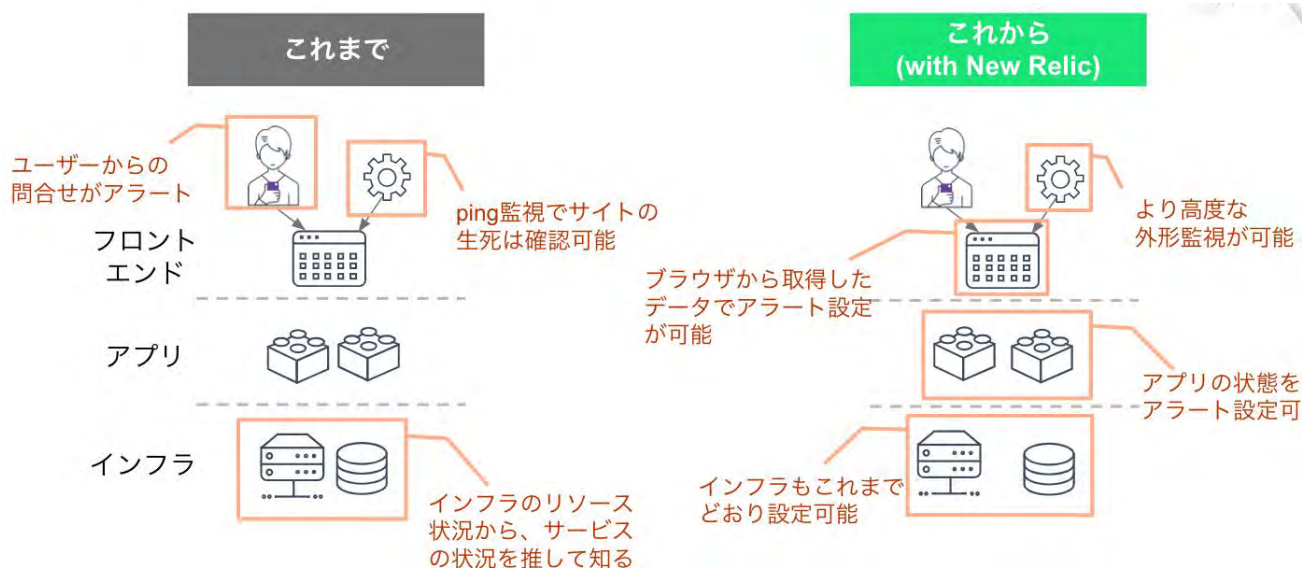


アプリがマイクロサービス化かつ基盤が疎結合なため、基盤リソースと関係なく問題が発生しうる

# 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

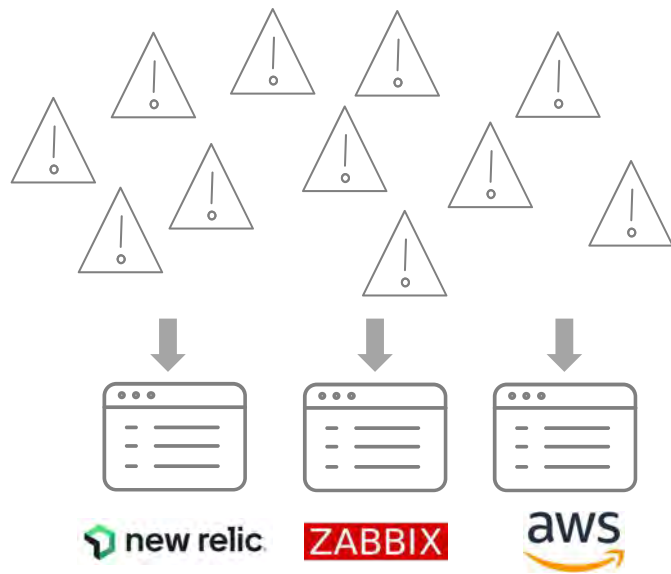


# 監視にまつわる新たな課題

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

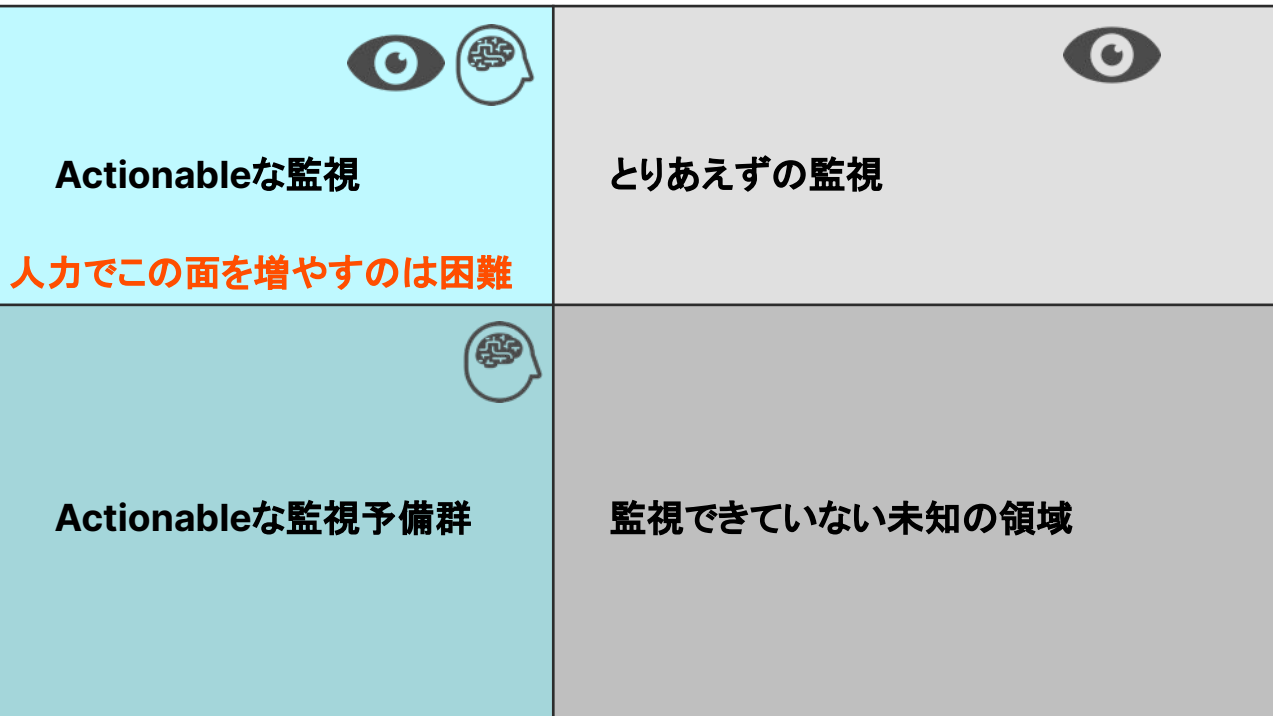


ITサービスに  
発生しうる障害

理解できる

理解できない

気づける



気づけない

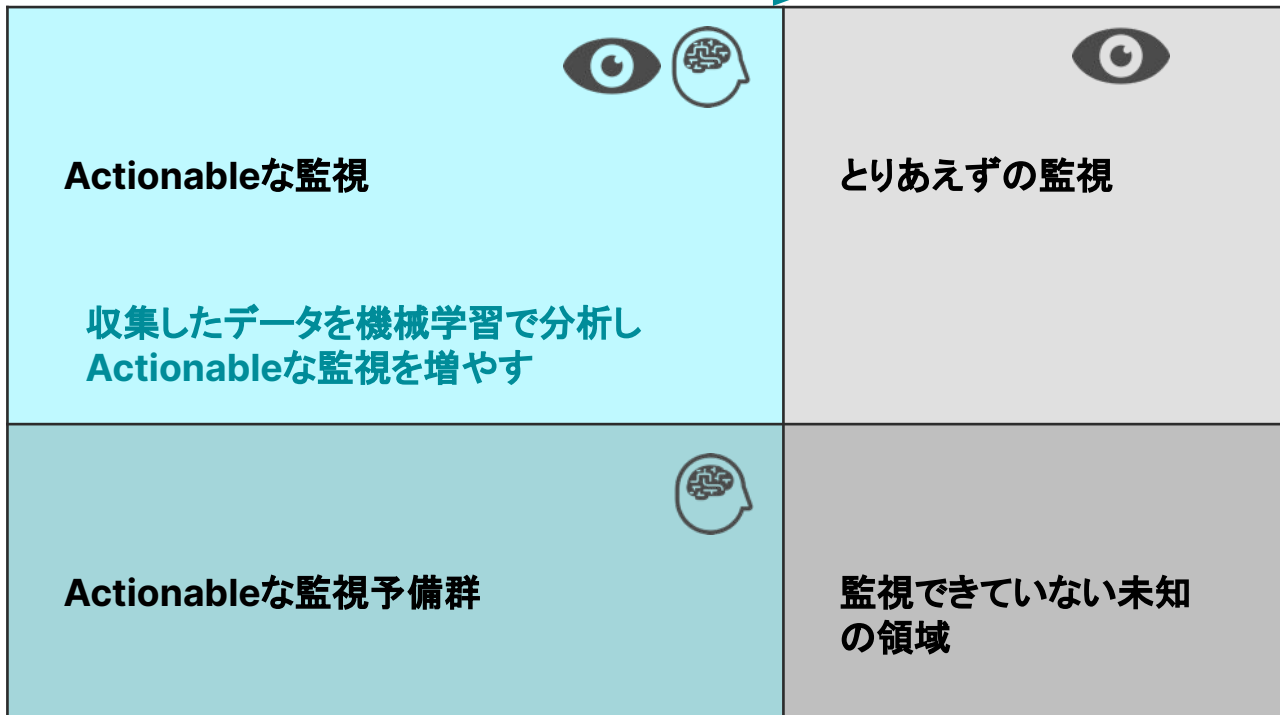
# AI Opsのアプローチ

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

アラートを一つ一つ網羅的に  
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

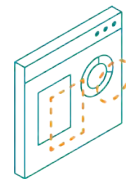
Anomaly Detection  
Alert coverage gaps

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

Correlation  
Root Cause Analysis

# 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

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

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).

Sched policy to get notified

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

### Create an alert condition

Account: 2514271 - NewRelicUniversity - Japan

Enter condition name  
EC-site - Apdex

Define your signal  
Enter NRQL Query  
`SELECT apdex(apm.service.apdex) FROM Metric WHERE entity.guid = 'HjuMTY3Kx8UE180V8TE1DQVJ7ES8NDQJGAu4dk3' FACET entity -guid`

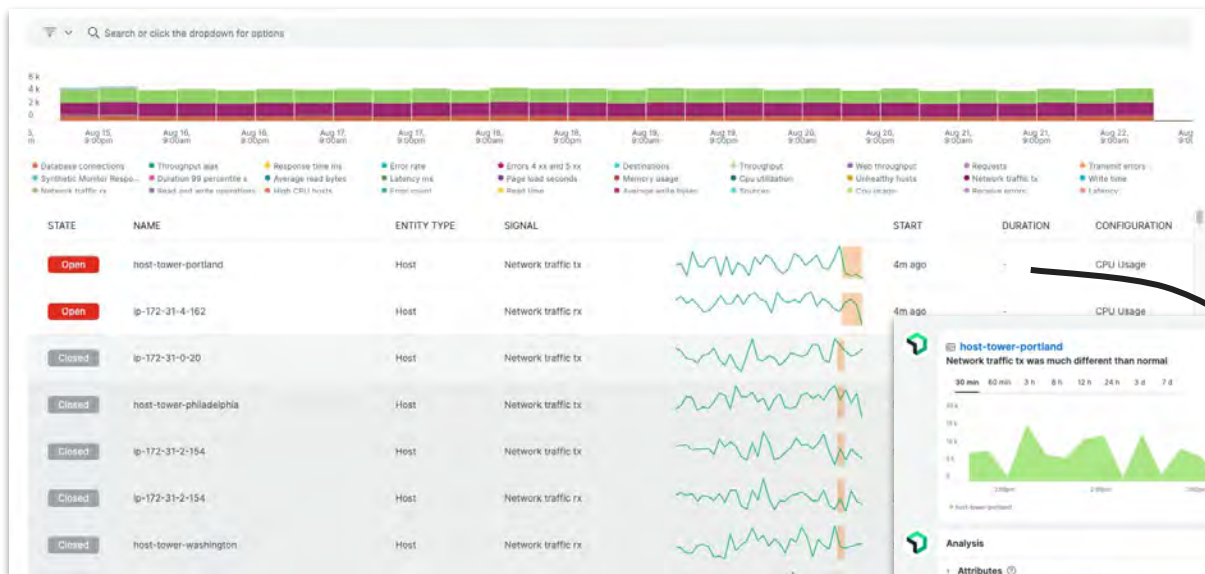
Showing 1/1 time series

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, filter data gaps). [See our docs](#)

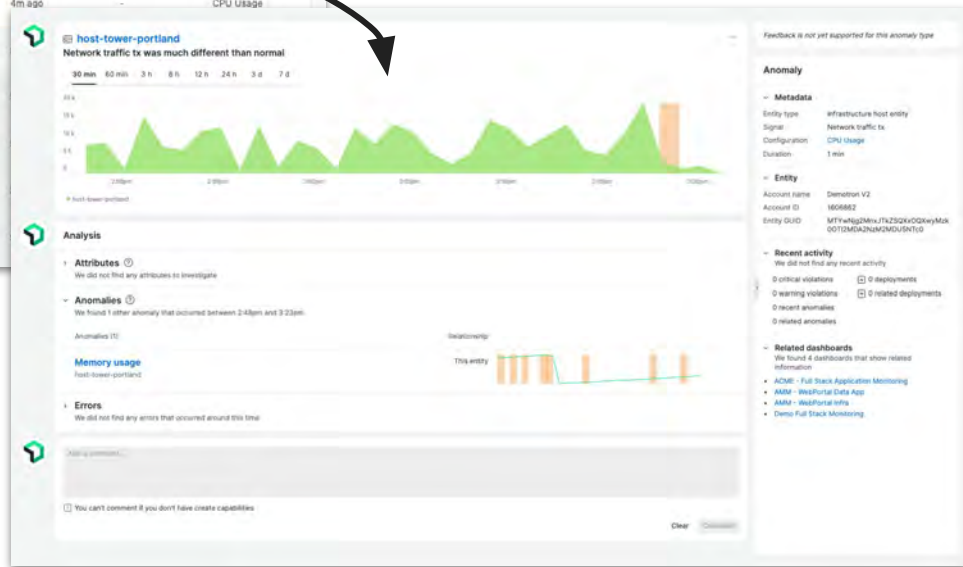
Set your condition thresholds  
Threshold type:  Static  Anomaly  
Anomaly is useful when you want to define more flexible thresholds that adjust to how your data behaves. You'll get notified only when something behaves abnormally. [See our docs](#)

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

# 機能紹介: Correlate (Decisions)

## Alerts & AI → Decisions

- Incidentの構造を分析して、関連性の高いものを一つのIssueにまとめる  
(対象エンティティ、Incidentデータ構造の一致度)
- 相関関係を持たせる基準はプリセットが用意されているほか、独自に設定可

Name and description	Correlations	Created by	Last edit	Enabled
Application Anomalies and Violations with 5... Correlation activated because the anomalie...	0	New Relic AI Global decision	Jan 6, 2023 4:45am	<input checked="" type="checkbox"/>
Same New Relic Condition and Title Correlation activated because New Relic co...	0	New Relic AI Global decision	Nov 18, 2022 11:20am	<input checked="" type="checkbox"/>

### Same Application Name, Policy and Id

Correlation activated because the application name, policy ID and id

New Relic AI - Global decision 0 likes 0 dislikes

### Decision logic

#### Correlate by attributes

```
tag.appName = tag.appName
```

```
tag.policyId = tag.policyId
```

```
tag.id = tag.id
```

### Advanced Setting

Time window: 20 min

Minimum incidents before activating: 2

# ハンズオン(3) AIOpsを使った異常検知 と原因分析

16:45 - 16:55 (10min)



# ハンズオン(3)

## 3-1 AIOpsの機能をセットアップする: 異常検知の設定

### [目的]

### 異常検知を有効化しましょう

- 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 New Relic University Japan(3940716)、アプリはEC-siteを選択
- Anomalies種別は全てチェック、通知は No notificationに設定して [Save configuration]

# ハンズオン(3)

## 3-2 AIOpsの機能をセットアップする: 相関分析の有効化

### [目的]

AIOpsの機能を活用するため、作成したアラートポリシーの相関分析を有効化しましょう

- 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)

## 3-3 AIOpsの機能をセットアップする: New Relic以外のイベントデータを取り込む

(実際に手を動かすものではなく、スライドに目を通して頂ければ OKです)

### [参考情報] Zabbixからのイベント取り込みの設定例

- 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。

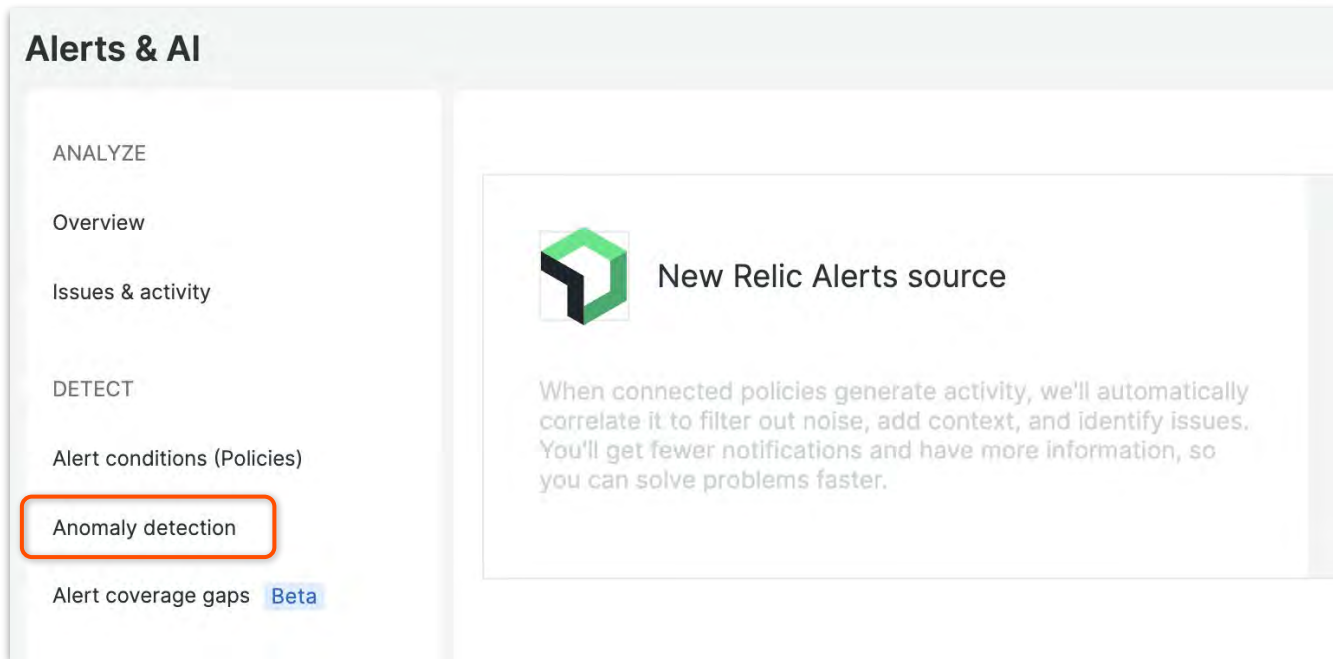


# 手順・解説

使用アカウント: Japan-NRU  
(ログイン先選択は[こちら](#)参照)

# ハンズオン(3-1) AIOpsの機能をセットアップする

- Alerts&AI > 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(3-1) AIOpsの機能をセットアップする

- [+ Add a Configuration] ボタンをクリックします。

Alerts & AI

## 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 feed](#). You can adjust your visibility preferences to change what you see. [Visibility preferences](#)

### Notifications

**① No need to set up a configuration. Set up anomaly notifications using workflows.**  
You can now use Workflows to send anomaly notifications to your Destination channels.  
[Go to workflows](#) [See our docs](#)

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 +
NRU304-Sample-Condi...	Account 3940716	1		Jun 4, 2023 3:00pm

# ハンズオン(3-1) AIOpsの機能をセットアップする

- 「設定名」には識別しやすい名前を設定します。
- Accountは「3940716 - New Relic University Japan」を選択します。
- 「EC-site」にチェックを入れます。

▼ Make this configuration easy to identify

NRU304-参加者名-Configuration

▼ What account do you want to use?

Account: 3940716 - New Relic University Japan ▼

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

Service - APM

APM

Entities: 1

Search in this table...

All (1) Selected (1/1) Unselected (0)

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

# ハンズオン(3-1) AIOpsの機能をセットアップする

- 5カテゴリ全てにチェックをつけ、「No notifications」を選択します。
- 「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"/>
-------	---------	--

Cancel

Save configuration

# ハンズオン(3-1) AIOpsの機能をセットアップする

- Anomaly設定の一覧に戻り、設定が追加されたことを確認します。

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 ↓	
NRU304-参加者名-Configuration	New Relic University Japan	1		Jun 5, 2023 5:55am	...
NRU304-Sample-Configuration	New Relic University Japan	1		Jun 4, 2023 3:00pm	...

# ハンズオン(3-2) AIOpsの機能をセットアップする

- 「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 active issues. Below the chart is a table of active issues.

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(3-2) AIOpsの機能をセットアップする


- 「Alerts」カードをクリックします。

The screenshot shows the New Relic Alerts & AI dashboard. The left sidebar contains navigation links: ANALYZE, Overview, Issues & activity, DETECT, Alert conditions (Policies), Anomaly detection, Alert coverage gaps [Beta](#), CORRELATE, Sources (highlighted), Decisions, ENRICH & NOTIFY, Muting rules, and Workflows [New](#). The main content area is titled 'Alerts & AI' and shows 'Associated account: NewRelicUniversity-Japan'. It displays '1 active source' and '1 policy connected'. Under 'Available sources', there are two cards: 'Alerts' (with 1 active policy and a description: 'Ingest your existing alert policies for correlations to gain actionable insights and cross-source visibility of your stack.') and 'REST API' (with a description: 'Use REST endpoint to easily ingest monitoring data for correlations from any other tool, including homegrown solutions.'). The 'Alerts' card is highlighted with a red border.

# ハンズオン(3-2) AIOpsの機能をセットアップする

- 「+ 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)

**+ Add a policy**

POLICY 

ACCOUNT 

[ダッシュボードハンズオン用アラートポリシー](#) 

NewRelicUniversity-Japan

# ハンズオン(3-2) AIOpsの機能をセットアップする

- ハンズオン(1)で作成した自分の Alert Policy 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 | Search policies

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


POLICY	ACCOUNT NAME
<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 インスタンス メンテナンス	NewRelicUniversity-Japan
<input checked="" type="checkbox"/> nru-test-policy	NewRelicUniversity-Japan

Cancel | Connect

# ハンズオン(3-2) AIOpsの機能をセットアップする

- 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.

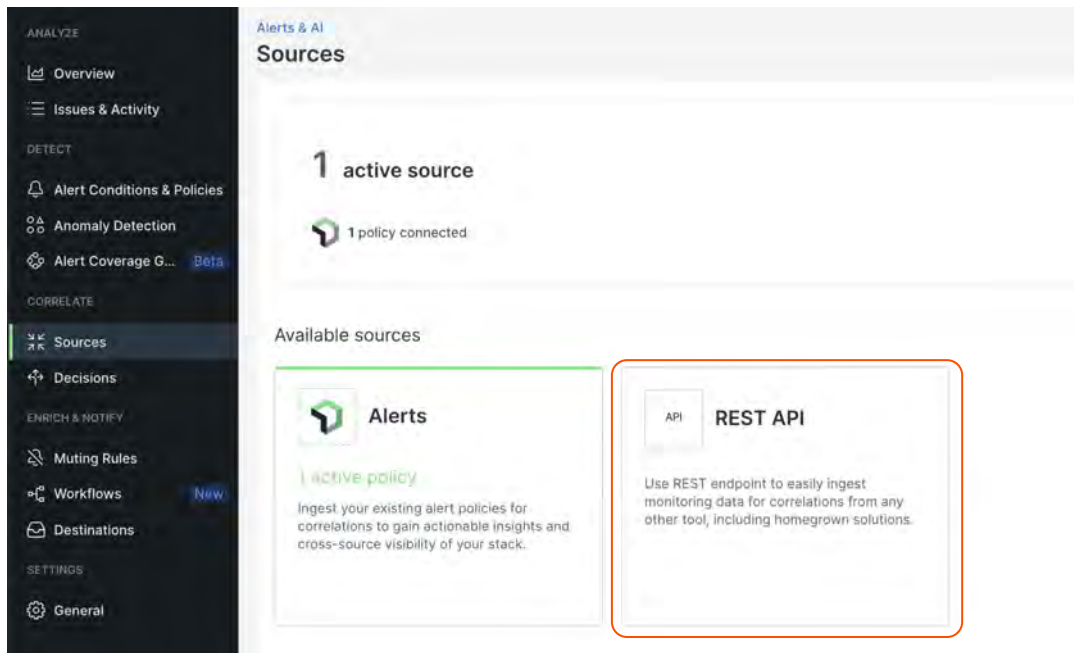
**NEW RELIC IS CONNECTED**

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(3-3) 参考 Zabbixの連携1

- ZabbixからNew Relicへのアラート連携には REST APIを利用しています。



Alerts & AI  
Sources

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.

# ハンズオン(3-3) 参考 Zabbixの連携2

- 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。

**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.



event_id	(EVENT.ID)	削除
event_severity	(EVENT.SEVERITY)	削除
event_recovery_status	(EVENT.RECOVERY.STATUS)	削除
event_recovery_value	(EVENT.RECOVERY.VALUE)	削除
event_source	(EVENT.SOURCE)	削除
event_tags	(EVENT.TAGS)	削除
event_time	(EVENT.TIME)	削除
event_update_status	(EVENT.UPDATE.STATUS)	削除
event_value	(EVENT.VALUE)	削除
host_name	(HOST.HOST)	削除
new_relic_bearer	Bearer eyJ0eXAI0LKV1Oj_CjhbGciOi...	削除
new_relic_proxy_url		削除
new_relic_url	https://collectors.signifai.io/v1/inciden	削除
urgency_for_average	2	削除
urgency_for_disaster	1	削除
urgency_for_high	2	削除

# ハンズオン(3-3) 参考 Zabbixの連携3

- Zabbixのトリガーアクションで、メディアタイプNew Relic Incident Intelligenceを呼び出します。

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	<a href="#">変更</a> <a href="#">削除</a>
	<a href="#">追加</a>			
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			<a href="#">変更</a> <a href="#">削除</a>
	<a href="#">追加</a>			
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			<a href="#">変更</a> <a href="#">削除</a>
	<a href="#">追加</a>			

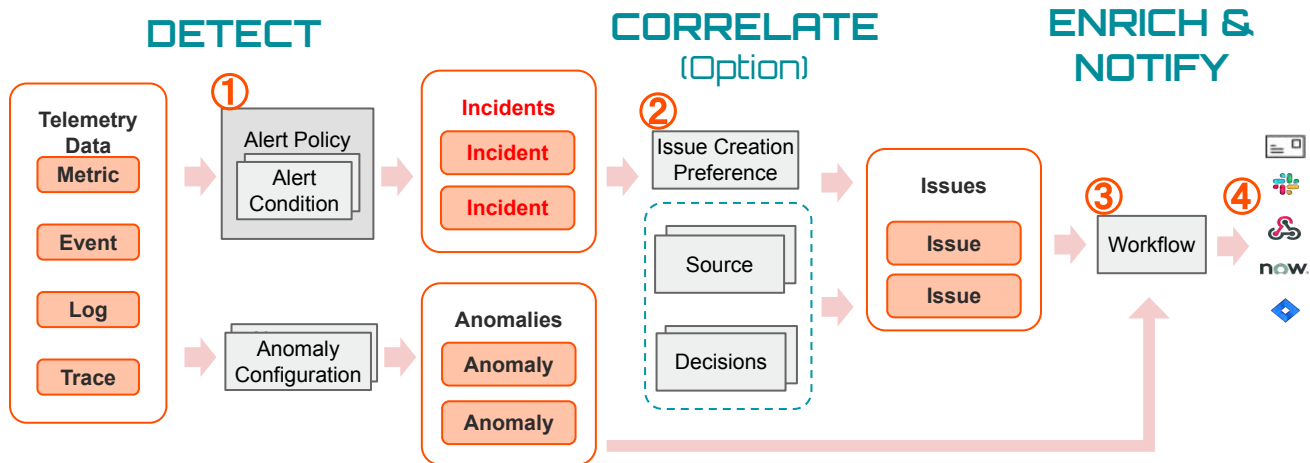
\* 少なくとも1つ以上の実行内容が設定されている必要があります。

[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
  - インフラ監視だけではサービスの異常に気付くには不十分
- New Relicのアラート構造と設定方法を理解しよう



- New RelicのAIOps機能を活用して、アラート分析を効率化しましょう



お疲れさまでした。

ご質問があればQ & A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.

