



NRU 304 「AIOps とアラート設計の基本」

February 15, 2023

15:00より開始致します。しばらくお待ちください。

音声が聞こえづらい場合は退出、再入室をお試しください。



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。



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 コンサルティング部

中島 良樹

Slerにて、さまざまなお客様のシステム開発やプロジェクトマネージャに従事。品質課題の改善を目的として主にWebシステムの負荷テストや機能テストの自動化を取り入れる。

外資テストツールベンダーに転職し、より多くのエンジニアにテスト自動化を取り入れてもらうべくプリセールスやコンサルティング業務を担当。

その後、データマネジメントベンダーにてデータ連携やデータ活用におけるプリセールスを担当。

開発や運用フェーズにおける自動化や効率化向上提案の経験を経て2022年より現職。



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エクスペリエンス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

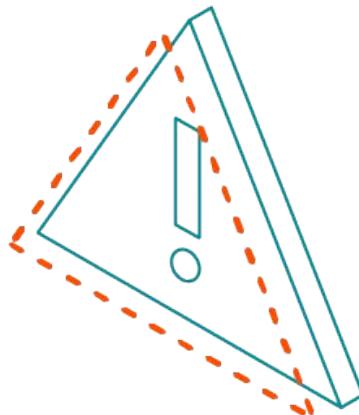
時間(目安)	内容	
15:00-15:15	座学(1)	ユーザー視点のアラート
15:15-15:35	座学(2)	New Relicのアラート機能
15:35-15:45	ハンズオン(0)	環境を確認する
15:45-16:05	ハンズオン(1)	アラートを作成する
16:05-16:15	座学(3)	New RelicのAIOps機能
16:15-16:30	ハンズオン(2)	AIOpsを使った異常検知と原因分析
16:30-16:45	座学(4)	AIOpsの意義
16:45-16:55	ハンズオン(3)	AIOpsを使った異常検知と原因分析 (応用編)
16:55-17:00		まと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

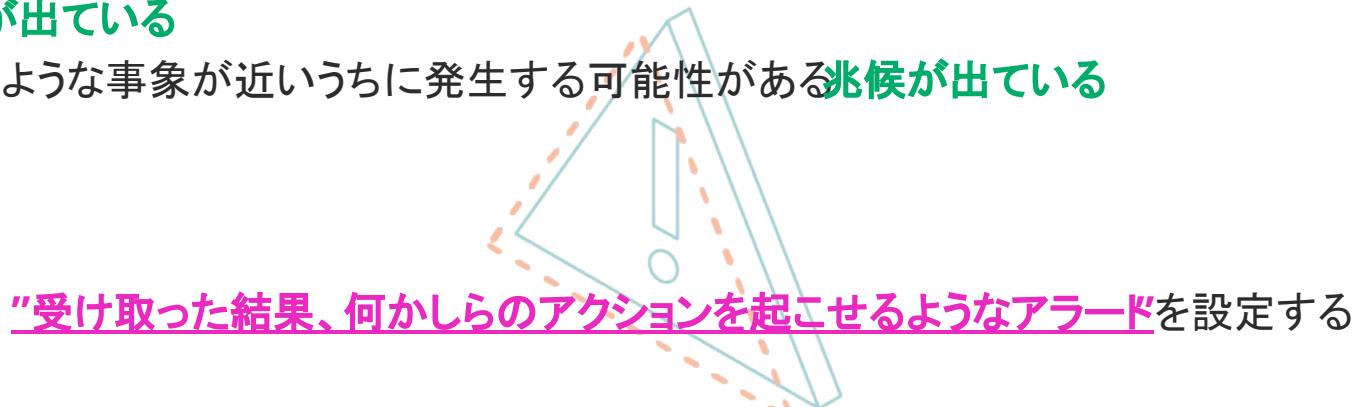
- ・ どんなアラートを設定していますか？



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**



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る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)

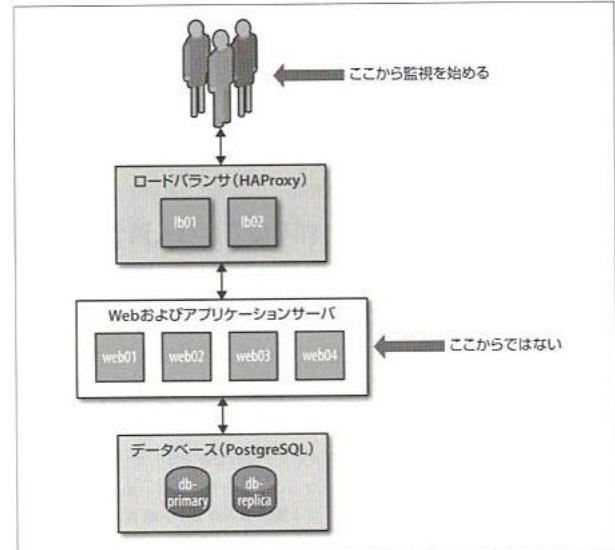


図2-1 できるだけユーザに近いところから監視を始める

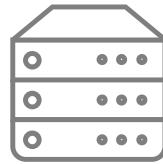
なぜアンチパターンが生み出されたのか

過去のシステム

アプリ



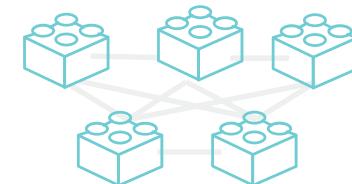
基盤



アプリがモノリシックかつ基盤が密結合だつたため、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)

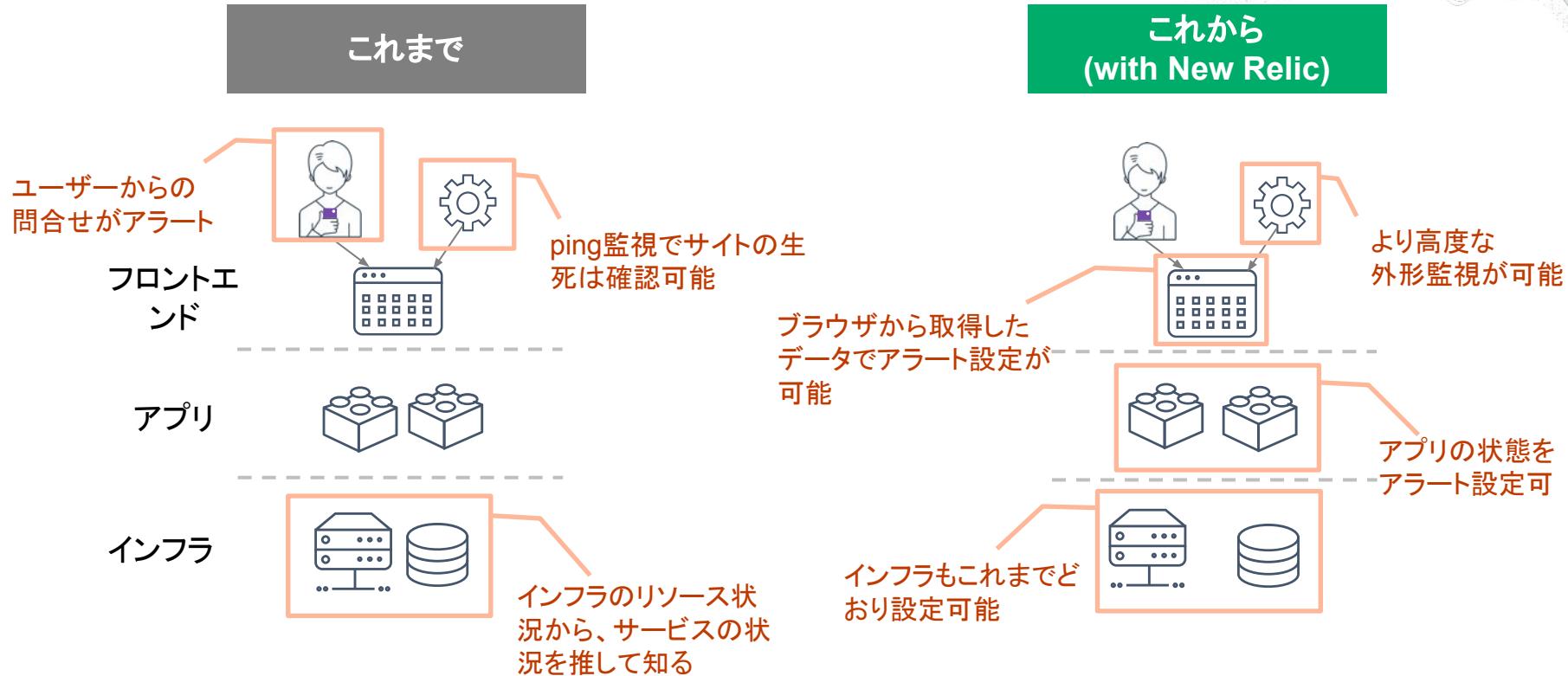


基盤



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	
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

座学(2) New Relicのアラート機能

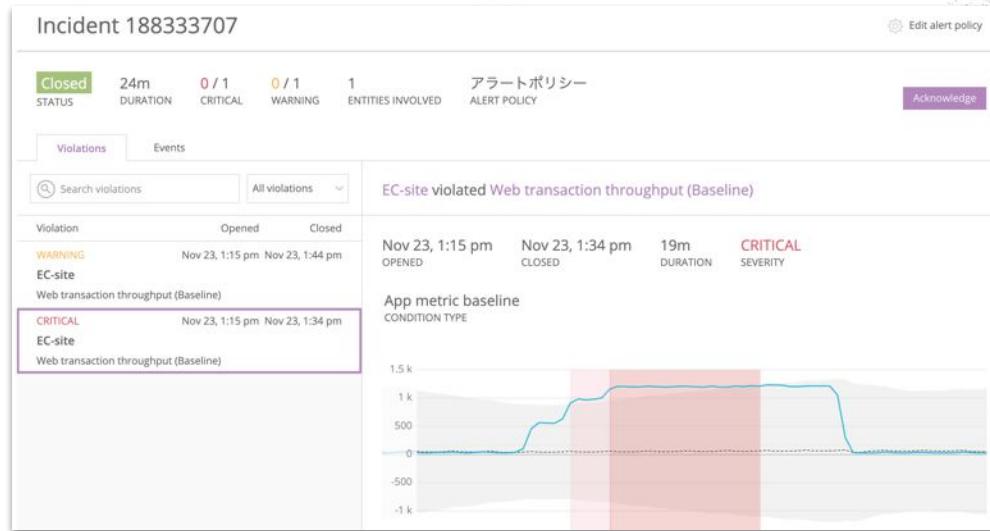
15:15 - 15:35 (20min)

New Relicのアラート機能

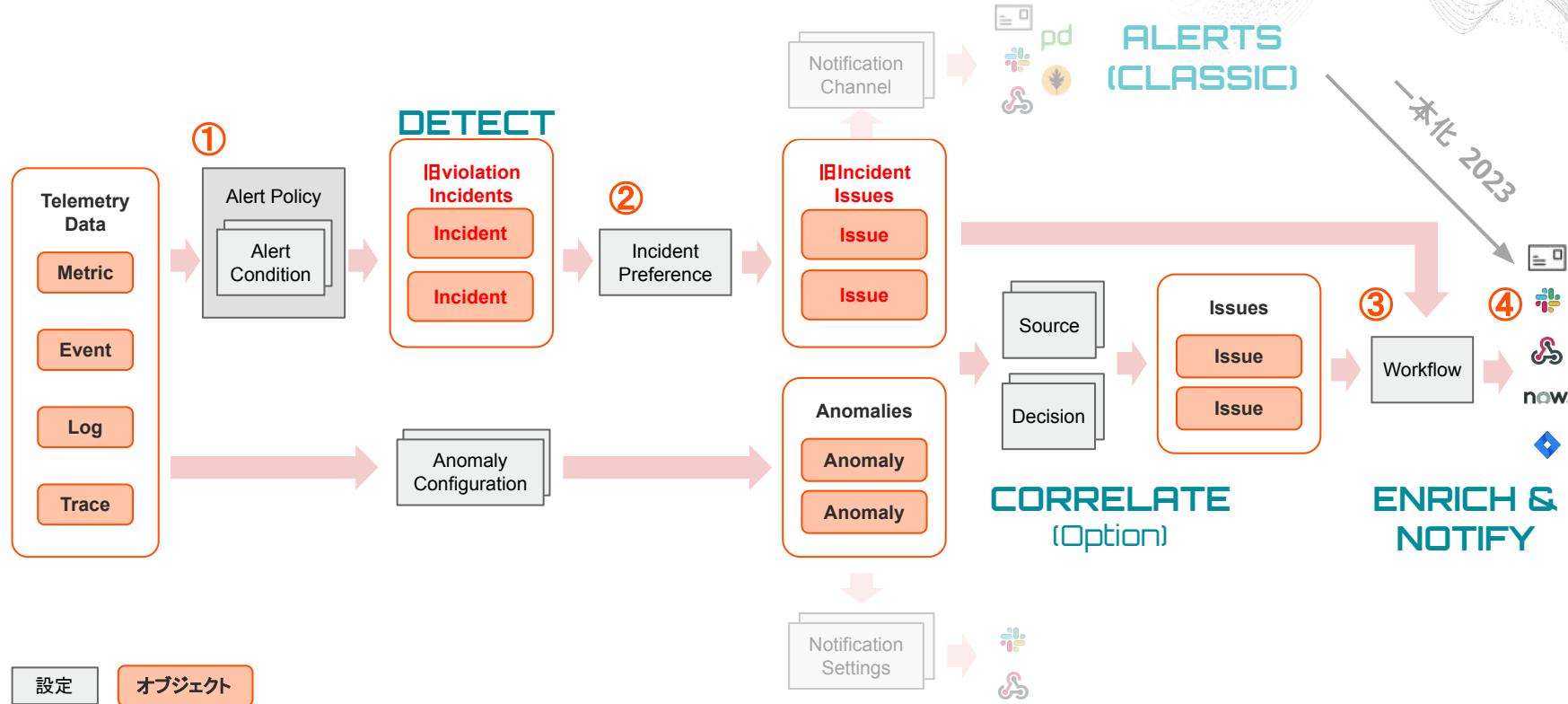
New Relicが収集しているデータを使って、アラートを設定することが可能

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

The screenshot displays the New Relic interface, highlighting the 'Alerts & AI' section.

Main Navigation:

- Search
- Add data
- All capabilities
- All entities
- Alerts & AI** (selected)
- APM & services
- Apps
- Browser
- Dashboards
- Errors inbox

Alerts & AI Dashboard:

DETECT

- Alert conditions (policy...)
- Anomaly detection
- Alert coverage ... **Beta**

ENRICH & NOTIFY

- Muting rules
- Workflows **New**
- Destinations

Alerts & AI Overview (Detailed View):

- ANALYZE** (highlighted with an orange box)
 - Overview
 - Issues & activity
 - DETECT
 - Alert conditions (policy...)
 - Anomaly detection
 - CORRELATE
 - Sources
 - Decisions
 - ENRICH & NOTIFY
 - Muting rules
 - Workflows
 - Destinations
 - SETTINGS
 - General

Metrics and Visualizations:

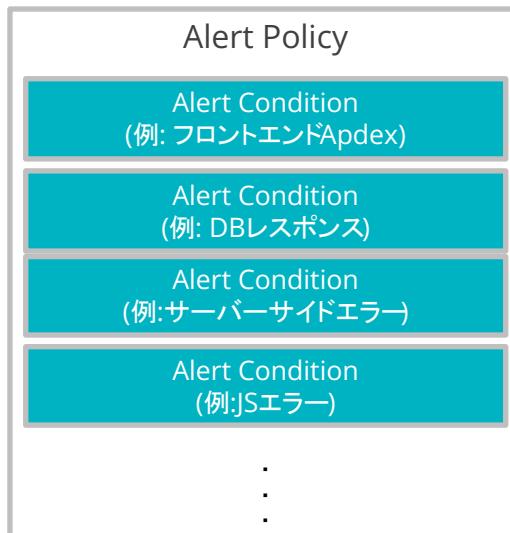
- Activated issues by priority Since 3 days ago
- Opened issues by priority Since 3 days ago
- Closed issues durations Since 3 days ago
- Muted issues Since 3 days ago

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



アラートポリシー

id: 545592

2 Alert conditions 2 Notification channels

Last modified Feb 7, 4:13 pm by Akihiro Ito

Search conditions Add a condition

INFRASTRUCTURE METRIC Disk Used

Last modified Feb 5, 4:53 pm | Manage

All Entities

diskUsedPercent > 90 for at least 2 mins

diskUsedPercent > 70 for at least 2 mins

APM APPLICATION METRIC BASELINE Web transaction throughput (Baseline)

Last modified Nov 19, 3:38 pm by Akihiro Ito | Edit | Copy | Delete | On

EC-site Add entities

Web transaction throughput deviates from baseline for at least 5 mins

Web transaction throughput deviates from baseline for at least 5 mins

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

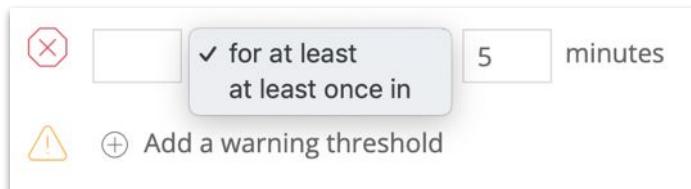
しきい値を超過した場合のアラート発報タイミング

- **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



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 the alert policy configuration. It includes fields for closing open violations after a specified number of days and adding a custom violation description. A 'Runbook URL' field is also present, containing a placeholder URL. The 'Add custom violation description' and 'Runbook URL' fields are highlighted with a yellow border.

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.)

ⓘ 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

The screenshot shows the 'Configure your workflow' page. At the top, there are input fields for 'Name' and 'Description'. Below that is a 'Filter data' section with three dropdown menus: 'Tag', 'Policy', and 'Priority'. A yellow warning box states: 'Please select at least one value. At least one value must be selected in one of the attributes in order to build a valid filter'. Under 'Additional settings', there's a 'Notify' section where users can choose destinations like ServiceNow, Webhook, Jira, Slack, Email, AWS EventBridge, Mobile push, and PagerDuty. At the bottom, there's a 'Test this workflow' section with 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



Webhooks



JIRA



Slack



Email



Amazon EventBridge



Pager Duty



Mobile push



重要: Email / Slack 内容の設定画面

The screenshot shows the 'Email' configuration page. It includes fields for selecting users and emails, an 'Email subject' field containing '{{ issueTitle }}', and a 'Custom Details (optional)' section with a placeholder for Handlebars syntax. A 'Send test notification' button is at the bottom.

Workflows variables:

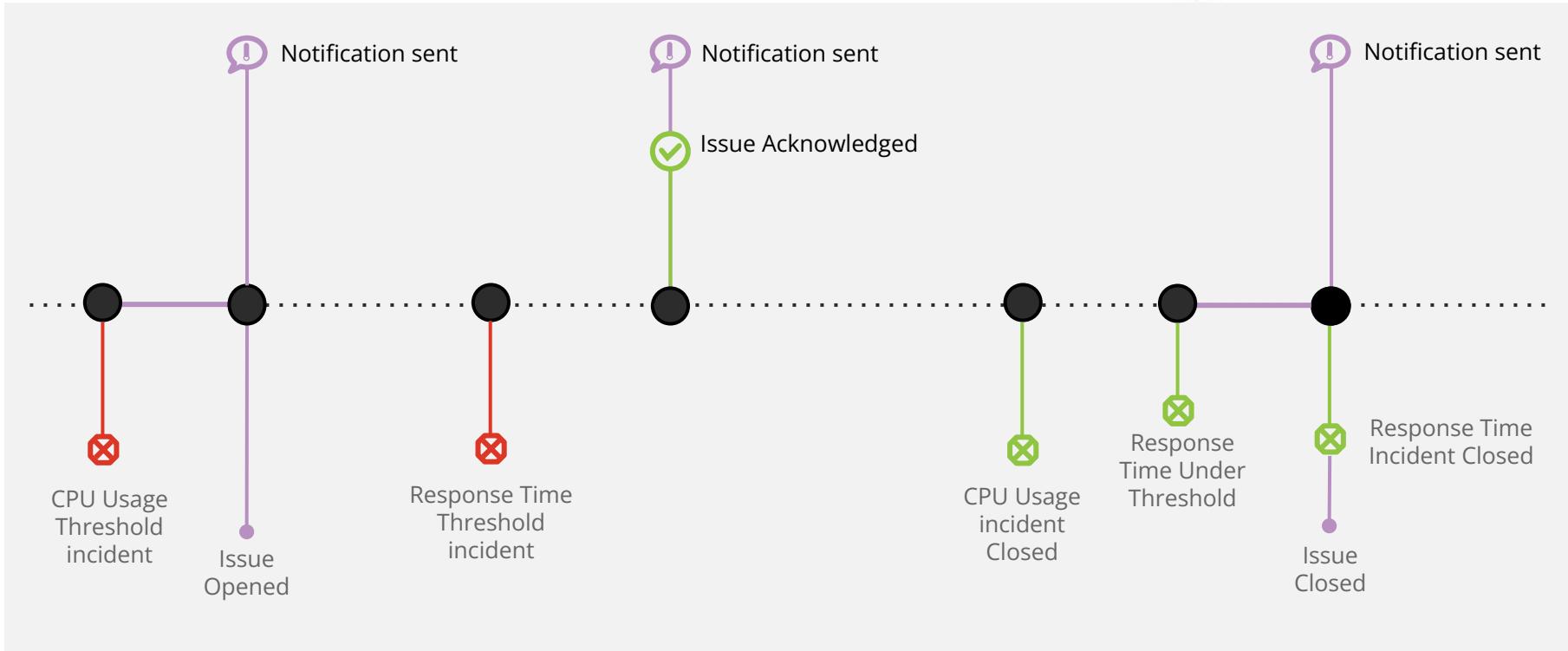
<https://docs.newrelic.com/docs/alerts-applied-intelligence/applied-intelligence/incident-workflows/custom-variables-incident-workflows/>

- 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 page. It includes a 'Slack destination' dropdown set to 'New Relic', a 'Channel' dropdown with a note about user authentication, and a 'Custom Details (optional)' section with a Handlebars syntax placeholder. A 'Send test notification' button is at the bottom.

補足: Issueのライフサイクルと通知タイミング

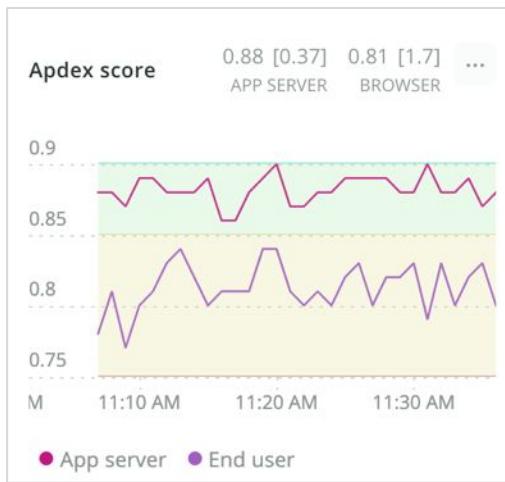
Issueの起票、Acknowledgeがされたタイミング、およびクローズの際に通知が届く



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



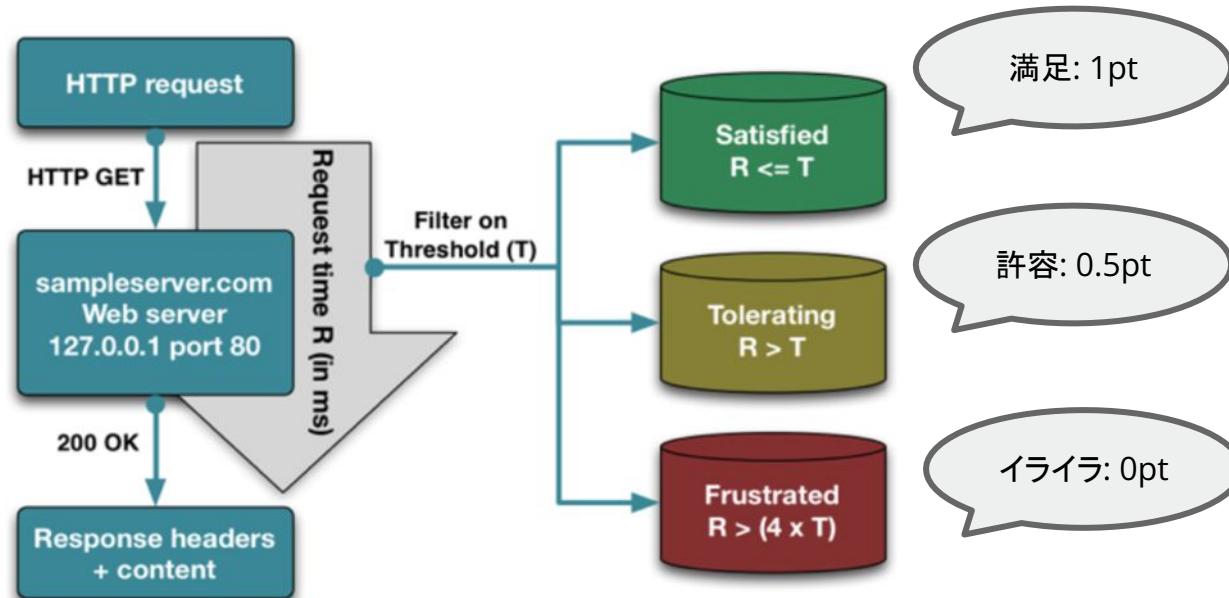
0.37 seconds

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
japan-handson+2021@newrelic.com [Full platform user](#)

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 organization

You have been signed out.

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+2021@newrelic.com [Original New Relic account](#)

japan-handson+2021@newrelic.com [Organization: NewRelic.kk](#) [Authentication Domain: 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

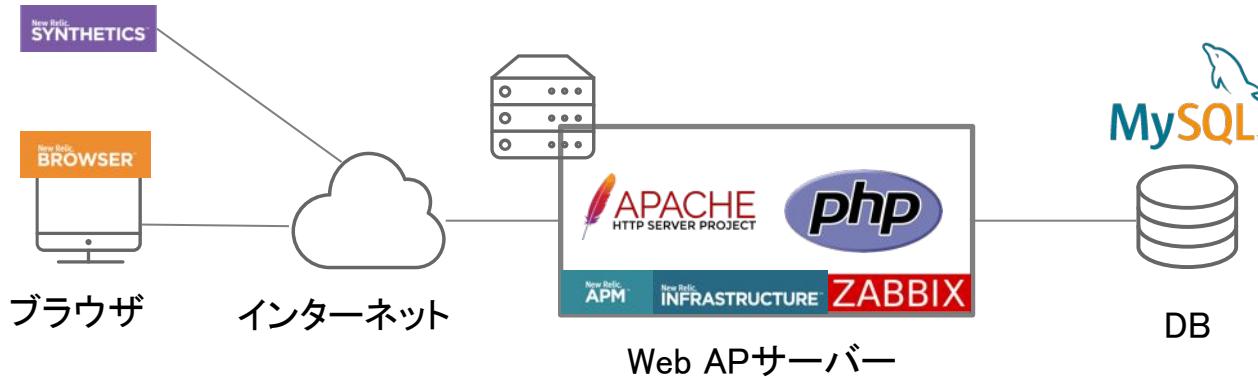
[NRUジェラートショップ](ECサイト)

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



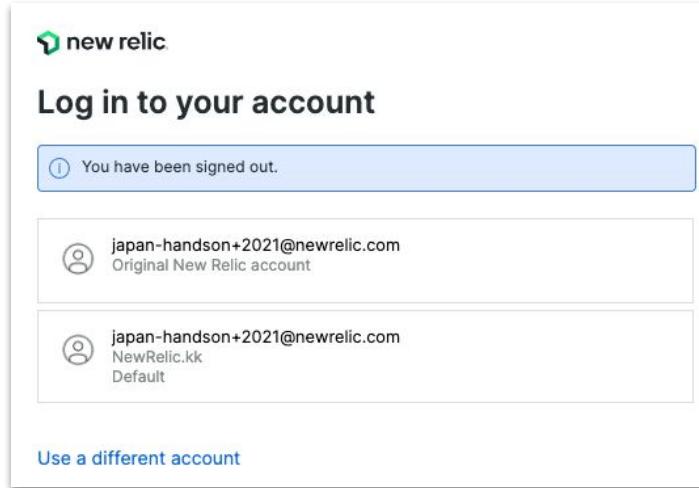
今回の環境の監視構成

- 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

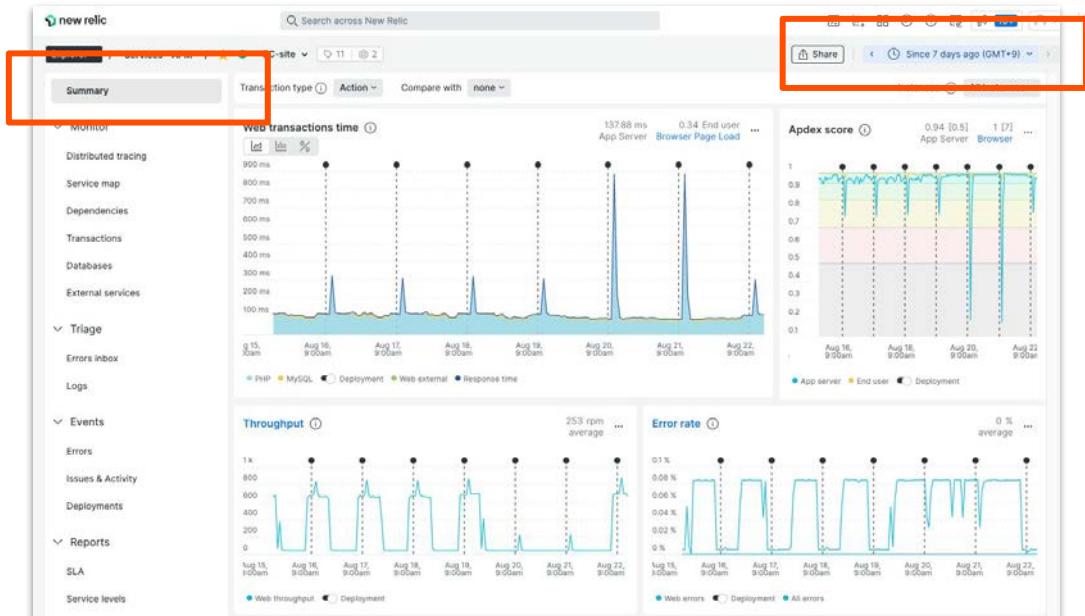
- ログイン先のアカウントを切り替えて確認頂くハンズオンが後半に予定されています。
- こちらの手順に従って、事前作業を行ないます。



ハンズオン(0) FSO UIの確認

- New Relicポータルの左ペインの”APM & 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

Apdex 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](#)

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

Add an alert

EC-site

Add recommended conditions

Our power users add these conditions to similar entities.

- Critical EC-site - Error Percentage
- 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).

Highly recommended

- Critical EC-site - Apex
- 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.

変更は行わない!!!

Create an alert condition

Account: 2518671 - NewRelicUniversity-Japan

Enter condition name
EC-site - Apex

Define your signal:

Enter NRQL Query ↗

```
SELECT apdex(apm.service.apdex) FROM Metric WHERE entity.guid = 'MJuMTY3QxXUE1BQVNGTE1QYRJTB5NDQ3MDAmdK3' FACET entity .guid
```

For help with null values, loss of signal, or other query options, see our docs ↗.

Showing 1/1 time series ↗

2 critical violations for displayed 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, filled data gaps). See our docs ↗.

Set your condition thresholds

Threshold Type: Static Anomaly

Anomaly is selected 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

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]

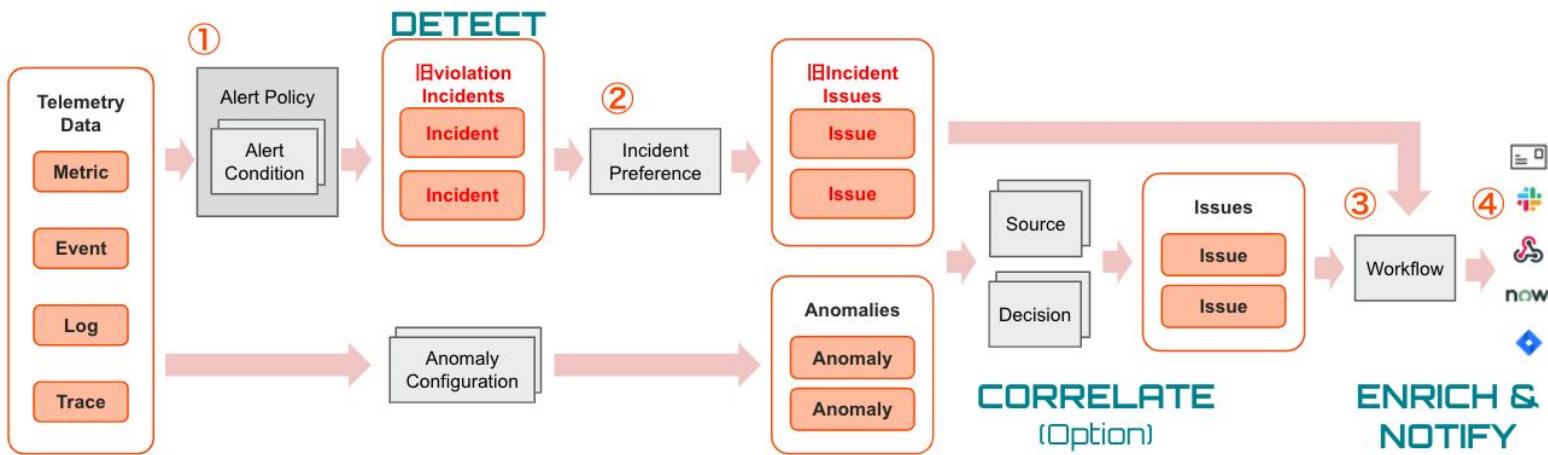
今回は赤字のアラートを設定してみます。

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ч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 shows the New Relic interface with the 'Alerts & AI' menu selected (highlighted with a red box). The main view displays a timeline from November 26 to December 3, showing alert coverage gaps. Three orange bars indicate High priority issues on December 2, 3, and 4. Below this is a table of active incidents:

State	Priority	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 New Relic interface for 'Alerts & AI'. On the left, there's a sidebar with categories: ANALYZE (Overview, Issues & activity), DETECT (Alert conditions (Policies) - highlighted with a red box, Anomaly detection, Alert coverage gaps [Beta]), and CORRELATE (Sources, Decisions). The main area has a search bar 'Search policies' and three buttons: '+New alert condition', '+New alert policy', and 'Browse pre-built alerts'. A table lists two policies: 'NRU インスタンス メンテナンス' (1 condition, 0 open issues) and 'ダッシュボードハンズオン用アラートポリシー' (2 conditions, 0 open issues).

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' section of the New Relic interface. On the left, there's a sidebar with categories: ANALYZE (Overview, Issues & activity), DETECT (Alert conditions (Policies) - highlighted in grey, Anomaly detection, Alert coverage gaps [Beta]), and CORRELATE (Sources, Decisions). The main area has a search bar labeled 'Search policies' and three buttons: '+New alert condition', '+New alert policy' (which is highlighted with a red box), and 'Browse pre-built alerts'. Below these buttons is a table with two rows:

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いめ、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

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

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

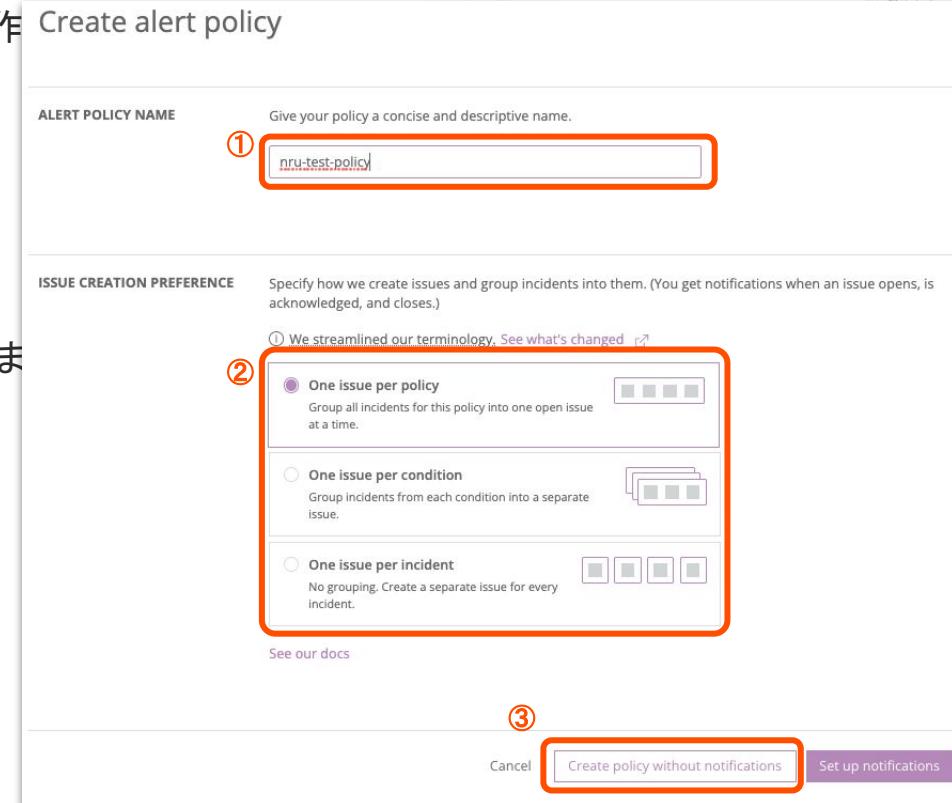
One issue per condition
Group incidents from each condition into a separate issue.

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

③

Cancel

See our docs



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ч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

- 外形監視:チェックエラー
- フロントエンド: Apdex(静的)
- アプリケーション: 応答時間(動的)
- 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 interface for creating alert conditions. On the left, the navigation bar is visible with various monitoring categories like APM & services, Apps, and Infrastructure. The 'Alerts & AI' section is selected. In the main content area, a policy titled '参加者名 アラートポリシー' (id: 3759739) is displayed. The 'DETECT' tab is selected, showing '0 Alert conditions'. A red box highlights this text. Below it, there's a large gear icon and the message 'This policy doesn't have any conditions'. Further down, it says 'Alert conditions are the criteria for creating incidents.' and 'Notifications are sent when an issue opens, is acknowledged, and closes.' A prominent red box highlights the 'Create a condition' button at the bottom.

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



Select a type of condition



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。

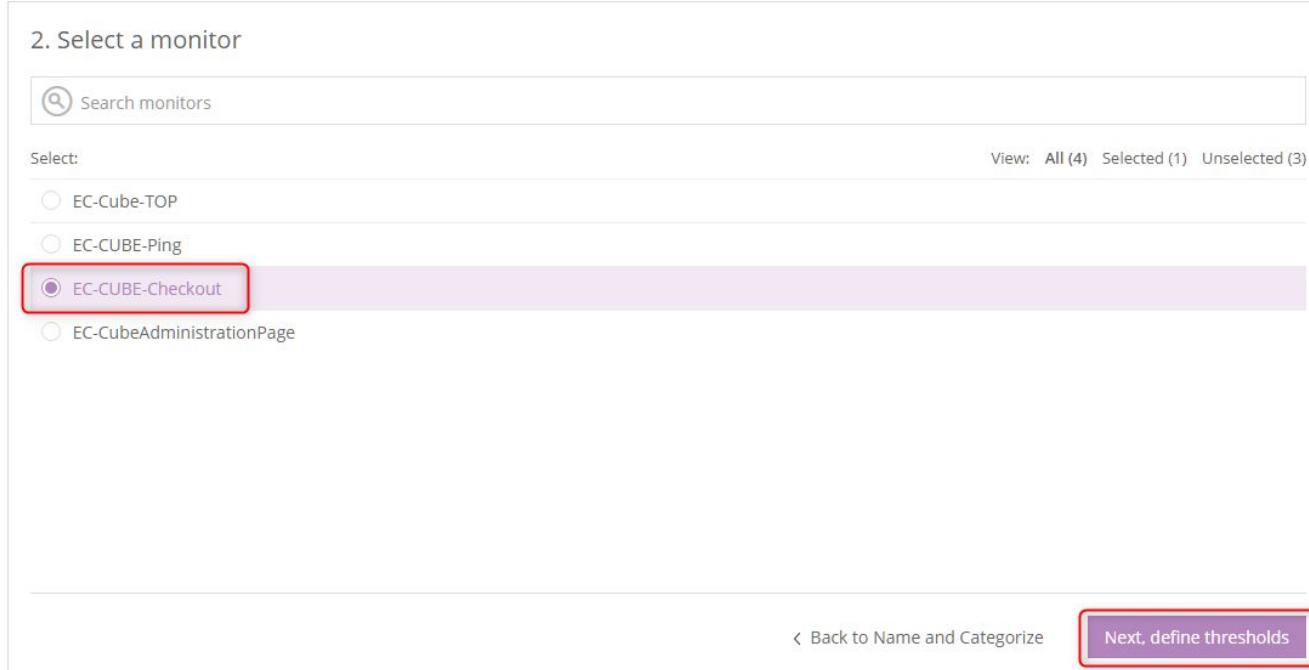
2. Select a monitor

Search monitors

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

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

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

わかりやすい通知名

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

id: 1314626

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

Connect to Incident Intelligence Incident preference: By policy Delete this policy

Search conditions 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 Add a condition

Monitor check failure

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

id: 1314626

Connect to Incident Intelligence Incident preference: By policy Delete this policy

1 Alert condition 0 Notification channels [Add a notification channel to receive alerts](#)

Last modified 7:37 am by NRU-User

Search conditions Add a condition

SYNTETICS 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

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

Select a type of condition

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

Search browser applications

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 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 14/18

- 2つめのconditionが作成されました。

The screenshot shows the New Relic Alert Conditions interface with two alert conditions listed:

- APM BROWSER APPLICATION METRIC** (Name: End User Apdex (Low))
 - Last modified 8:28 am by NRU-User
 - Action buttons: Edit, Copy, Delete, On/Off switch
 - Entity: EC-site
 - Condition: End User Apdex < 0.7 at least once in 5 mins (Status: Failed)
 - Warning threshold: Add a warning threshold
- SYNTHETICS MONITOR FAILURE** (Name: わかりやすい通知名)
 - Last modified 8:05 am by NRU-User
 - Action buttons: Edit, Copy, Delete, On/Off switch
 - Entity: EC-CUBE-Checkout
 - Condition: Monitor check failure (Status: Failed)

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ドバーで感度が変化します。

3. Define thresholds

Baseline Direction: New **Upper only**

When any target application **Web transaction time**

average deviates from the baseline **at least once in** **5 minutes**

more violations fewer violations

より敏感に **より鈍感に**

Add a warning threshold

Condition Name: Web transaction time (Baseline)

Add runbook URL

EC-site

2 critical violations

Last 2 days

Apr 24, 12:00 PM Apr 25, 12:00 AM Apr 25, 12:00 PM Apr 26, 12:00 AM

Web transaction time Average web transaction time

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

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 NRQL query

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

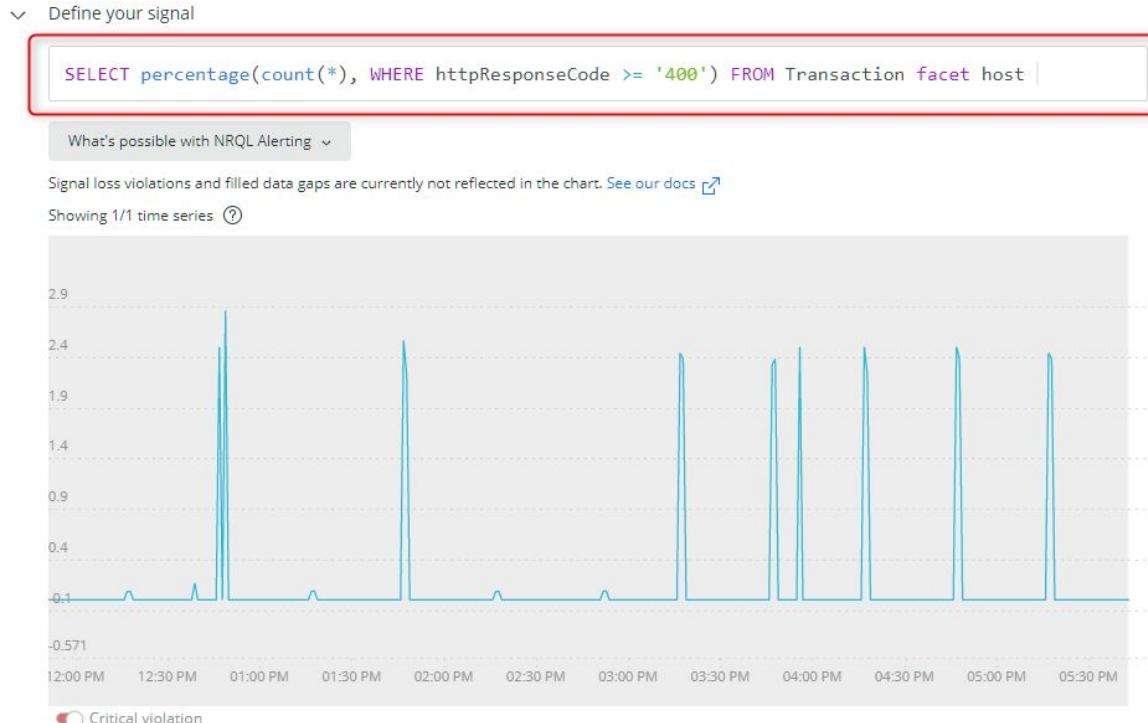
3. Set your condition thresholds

- 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

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。



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"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**

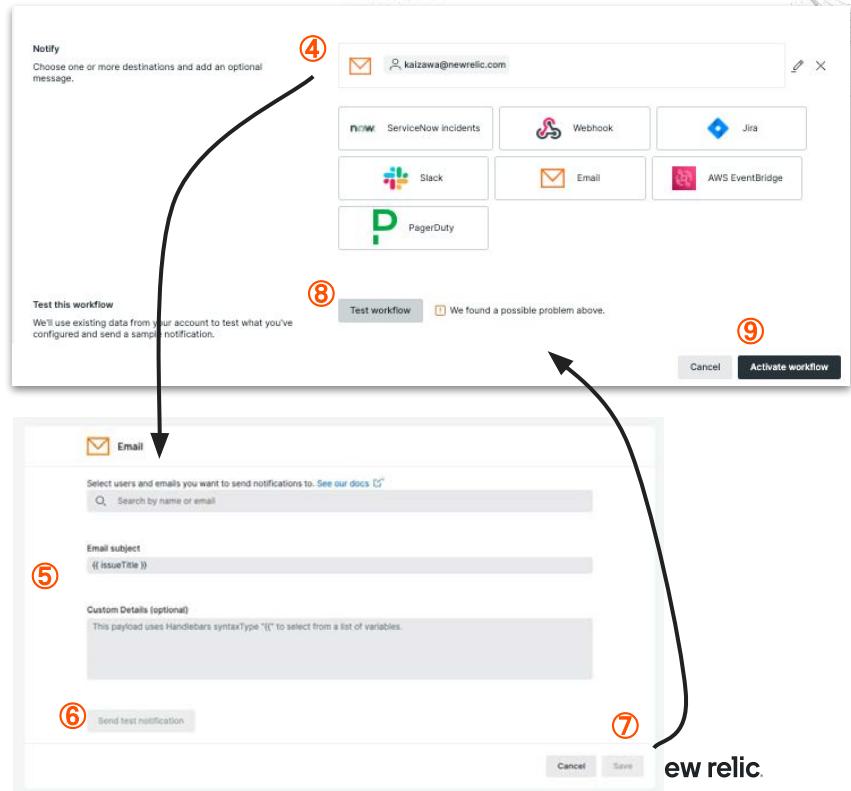
The screenshot shows the 'Configure your workflow' page. At the top, there's a search bar with 'NRU304-Workflow' and a note to 'Give it a unique, descriptive name you'll recognize later'. Below that is a 'Filter data' section with a dropdown set to 'accumulations.policyName' and an operator 'exactly matches' followed by 'NRU304-Policy'. A red circle labeled '③' highlights the 'Advanced' button next to 'Basic'. To the right of the filter section is a 'Need help?' sidebar with links to 'Workflow docs' and 'Destination Docs'. At the bottom right of the main area are buttons for 'Manage destinations' and 'Workflow triggers'.

次のスライドに進みます

ハンズオン(1)-3 Workflowsを作成する 2/6

4. Notify: Emailを選択します **(重要)**
5. 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。
6. 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？

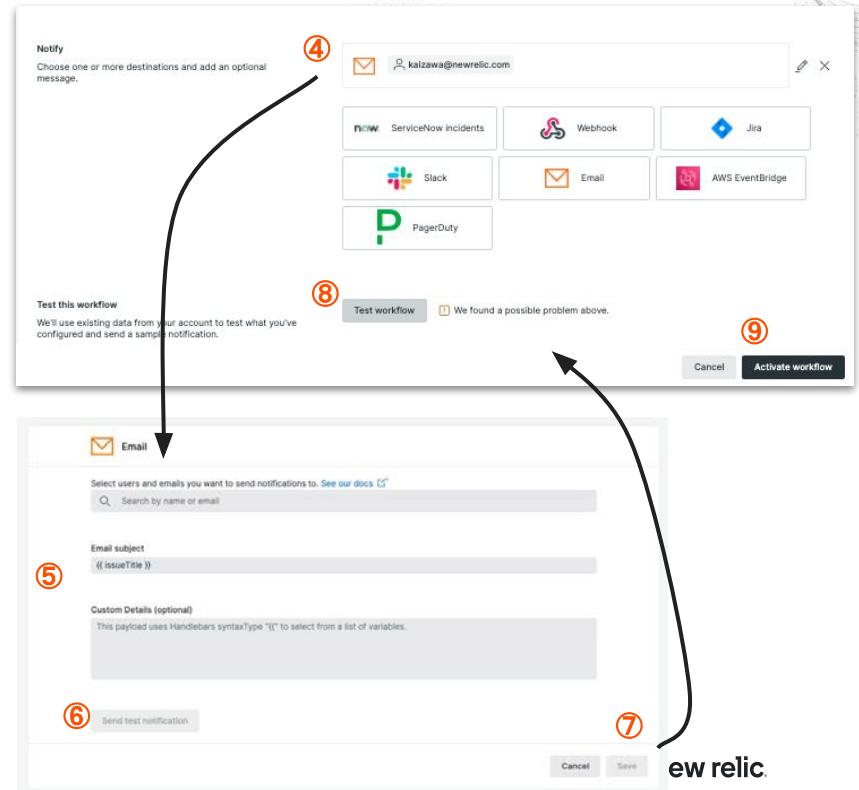
次のスライドに進みます



ハンズオン(1)-3 Workflowsを作成する 3/6

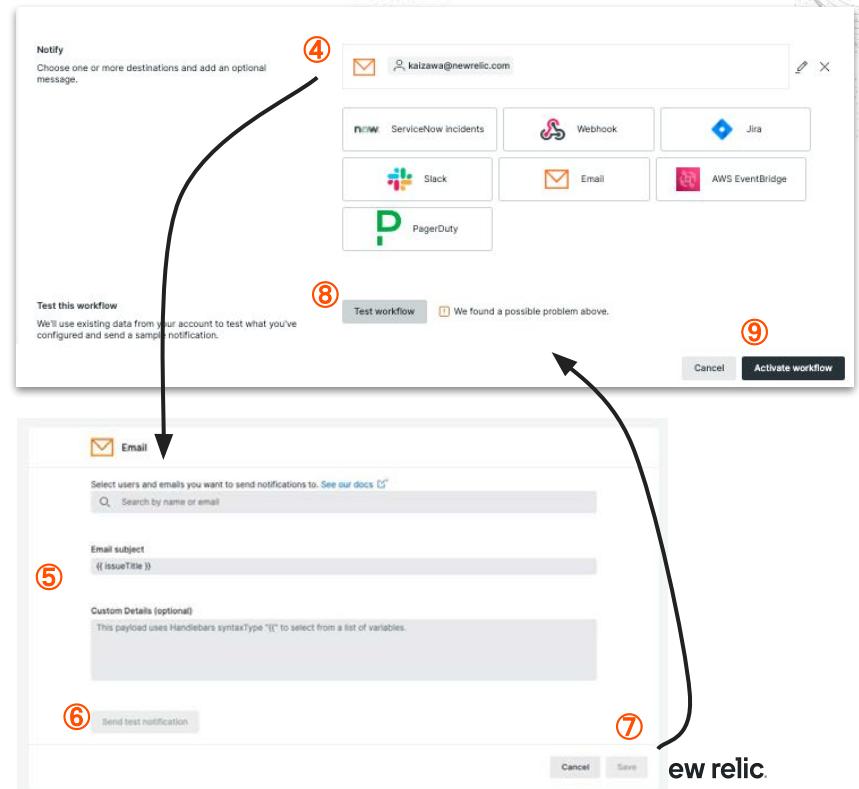
6. Send test notificationボタンをクリックし、指定したメールアドレスに通知メールが届くかを確認します
 - b. 無事に手元に届いたことを確認の後に、⑤に戻り、Email subjectやCustom Detailsを変更します。再度Send test notificationをクリックし、どのようにメールの中身が変わるかを確認します。(色々試してみて下さい。)
 - i. 補足: 環境変数を利用する際は、 "{{"と入力して開始して下さい。
7. Saveボタンを押します

次のスライドに進みます



ハンズオン(1)-3 Workflows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。
 - a. 先程のテスト用メールとどの様な違いがあるかを確認してください
9. Active workflowボタンをクリックし、設定を保存します



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.

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 ServiceNow Slack Webhook PagerDuty AWS EventBridge Mobile push

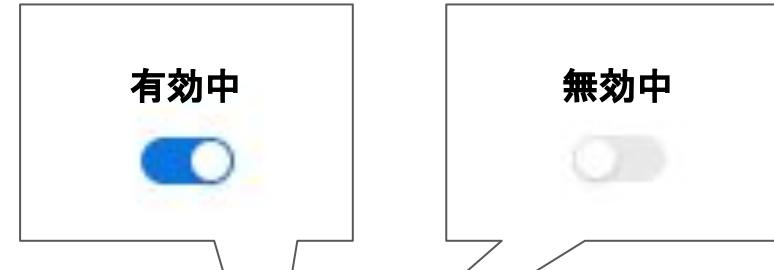
Notifications Log Destinations (3)

Manage destinations where we send notifications.

Search

Name	Two... URL/Details	Last updat...	Updated by	Enabled	Status	...
External address	m_ogawa@atlas.jp	Aug 10, 2022...	1001038720	<input type="checkbox"/>	DEFAULT	...
NRU-User	japan-hands-on+2021@newrelic...	Aug 22, 2022...	1001038720	<input checked="" type="checkbox"/>	DEFAULT	...
External address	kaojiri@gmail.com	Jun 6, 2022 7...	1001038720	<input type="checkbox"/>	DEFAULT	...

NRU-User japan-hands-on+2021@newrelic... Aug 22, 2022... 1001038720 DEFAULT ...

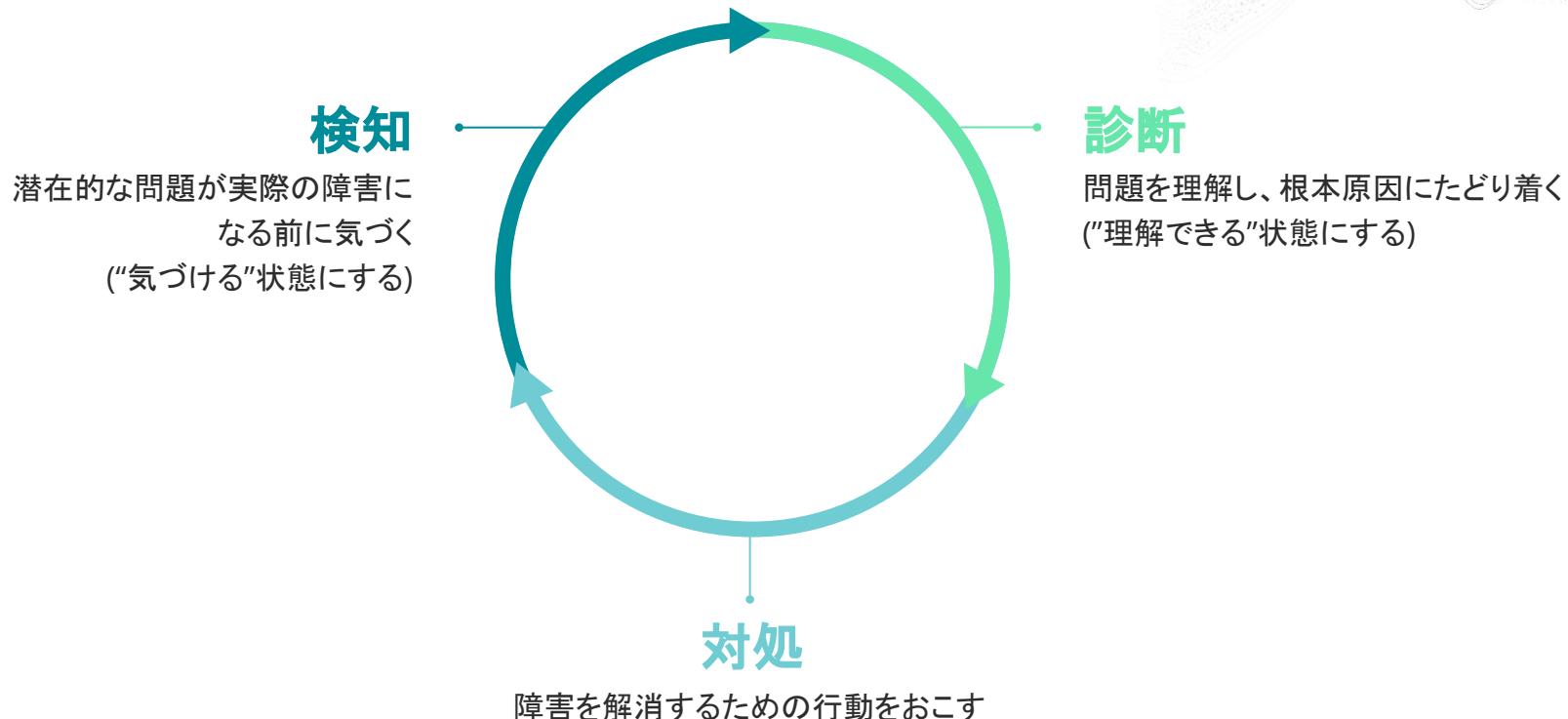




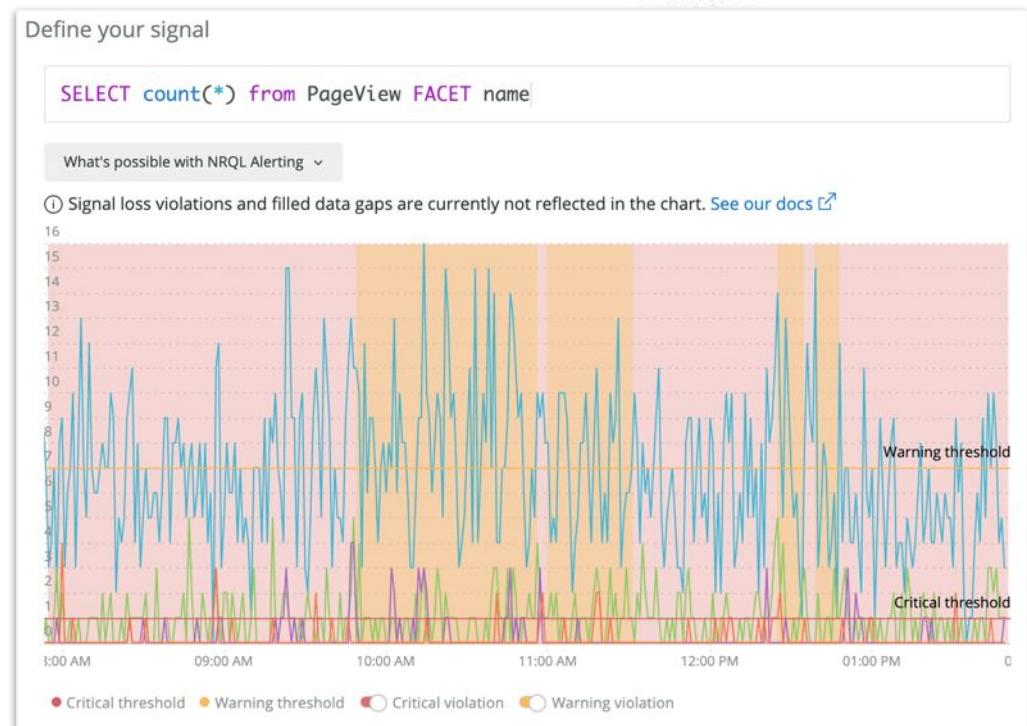
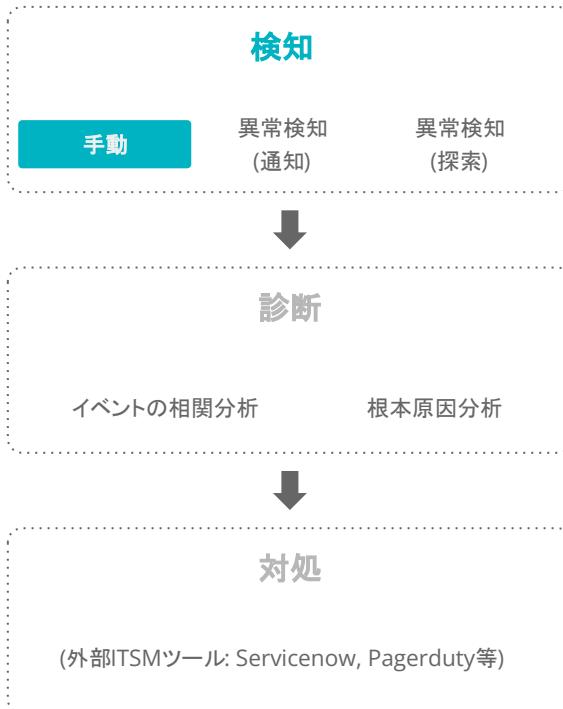
座学(3) New RelicのAIOps機能

16:05 - 16:15 (10min)

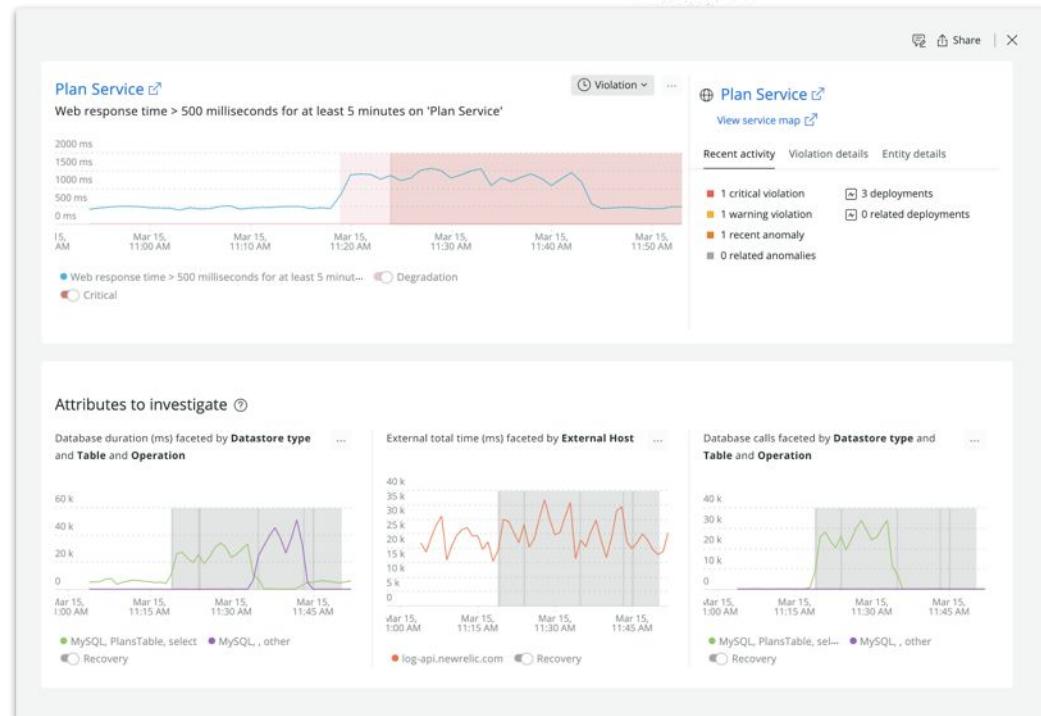
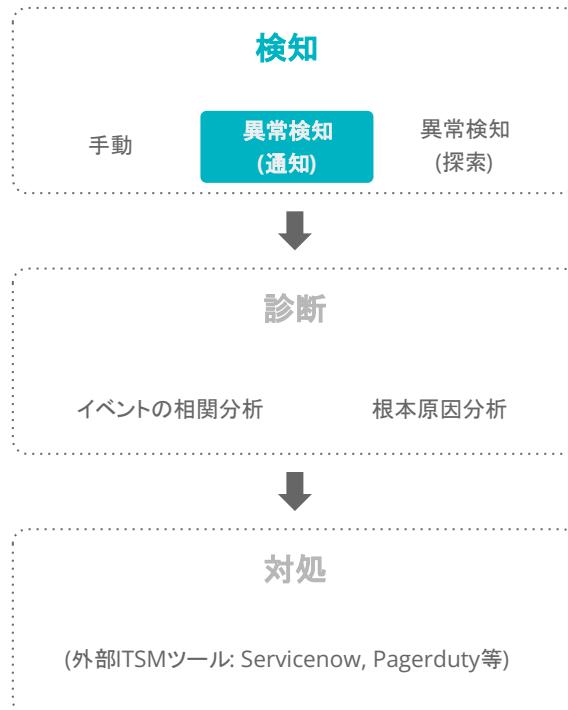
New Relic AIOpsによるインシデント対応フロー



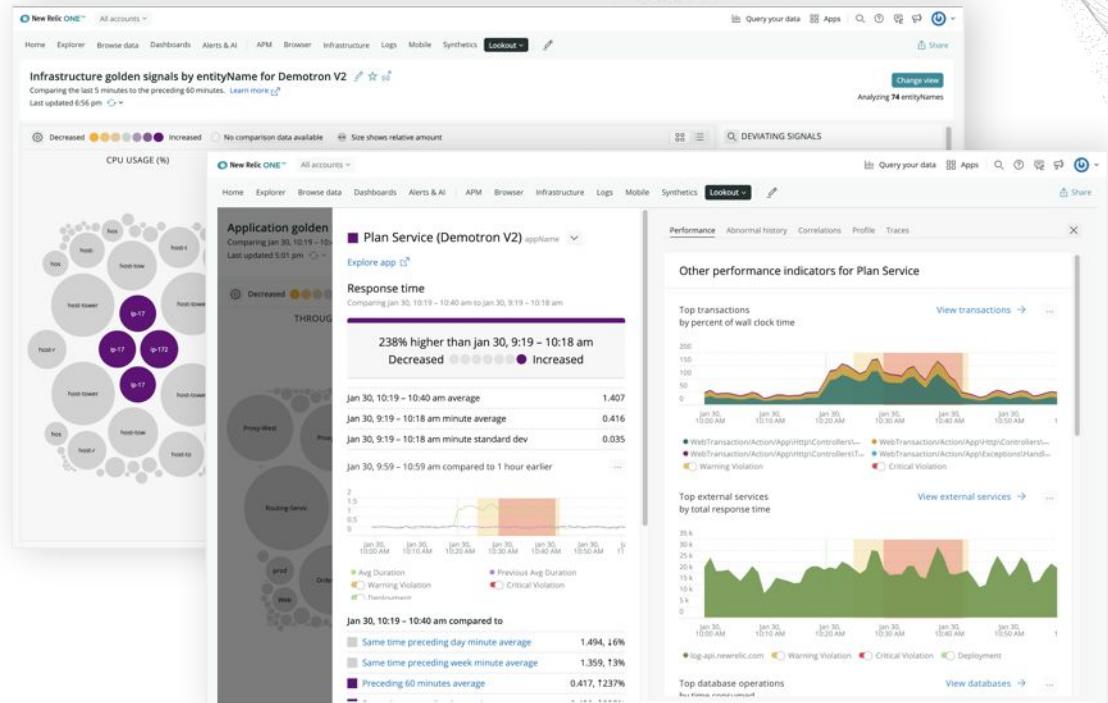
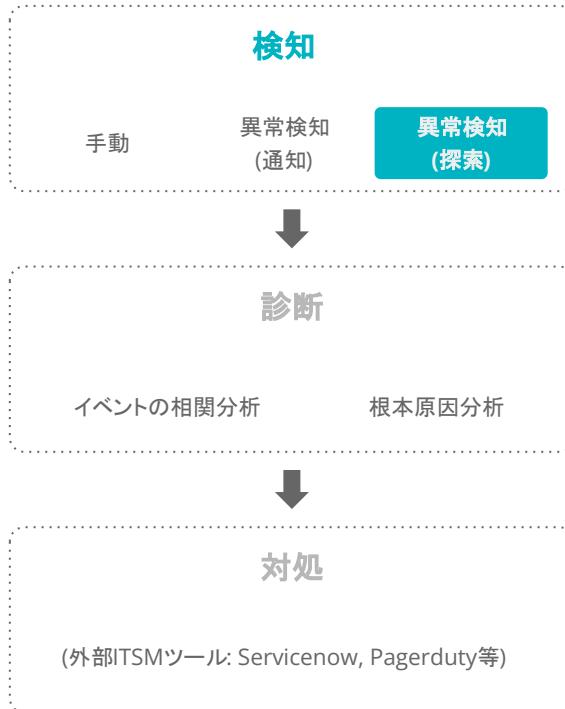
検知1: 重要な指標に対する手動アラートによる気づき



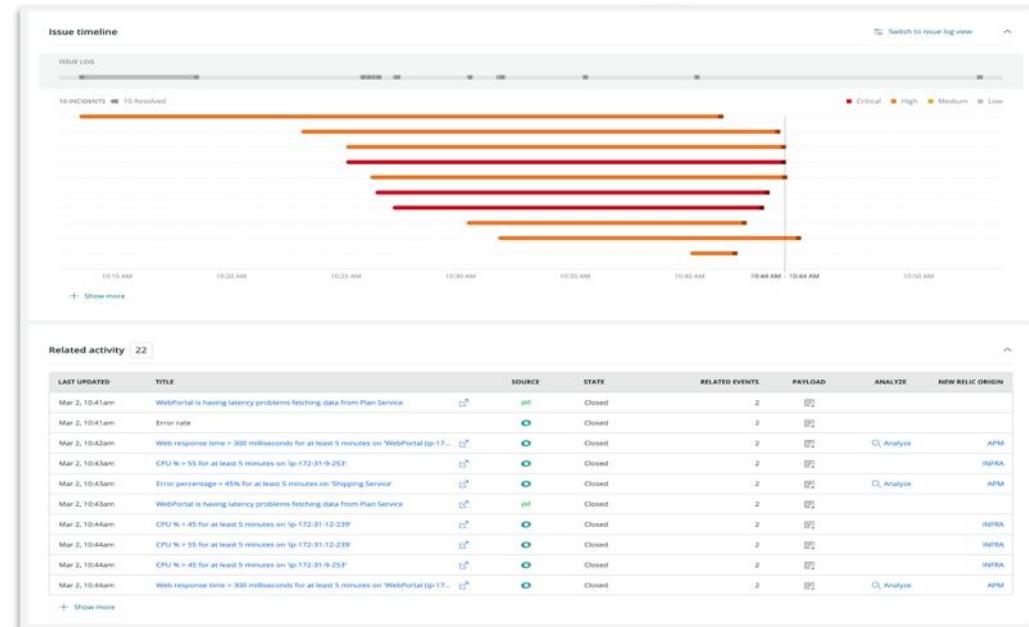
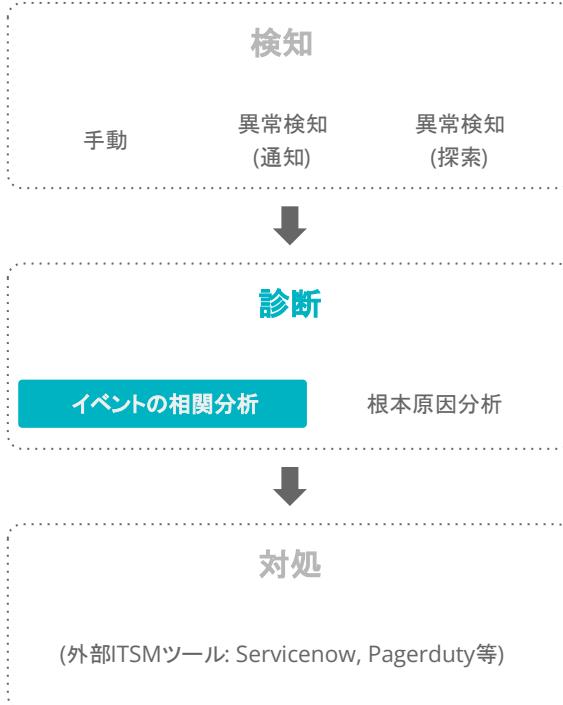
検知2: Anomaly Detectionによる異常の通知



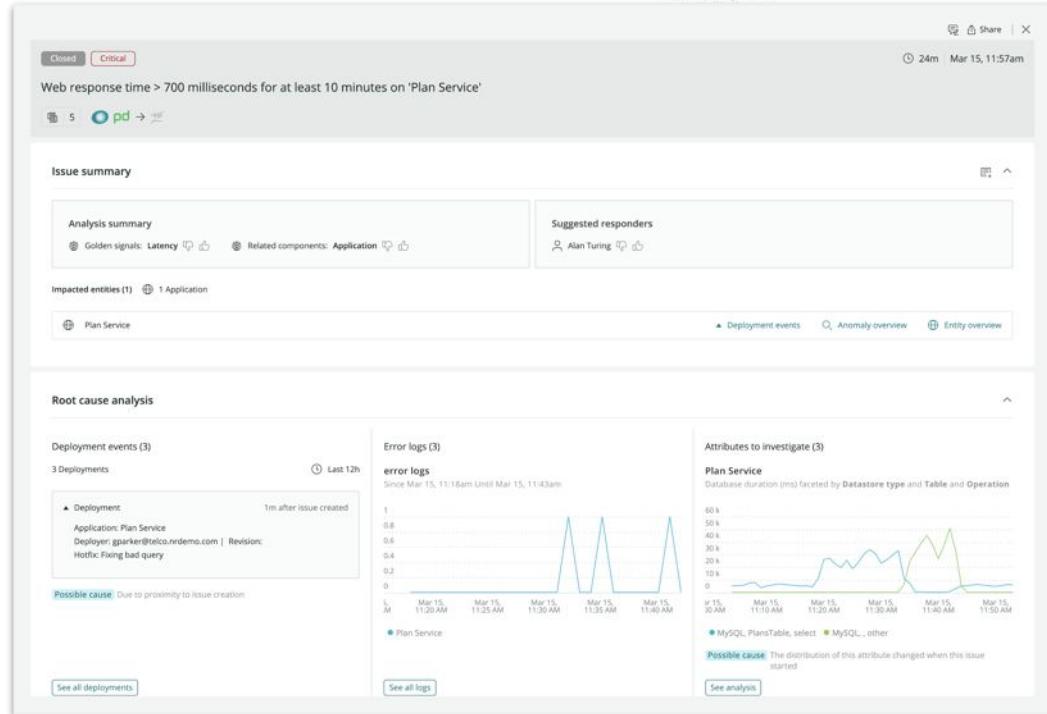
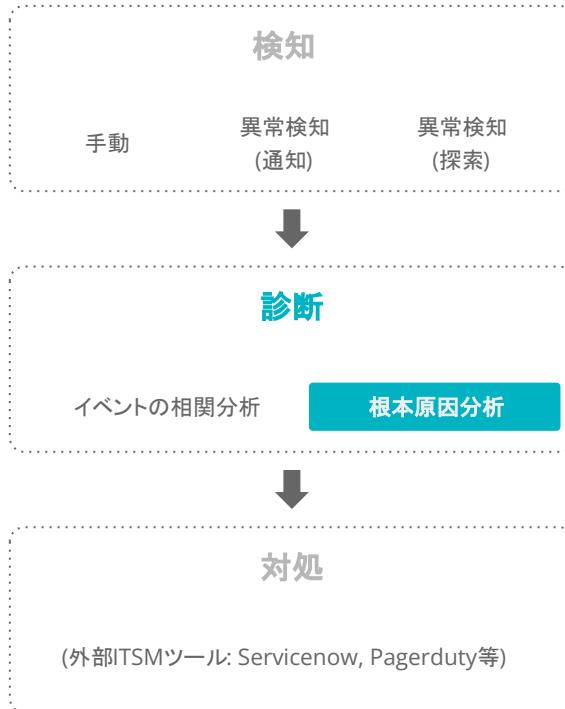
検知3: Lookoutによる異常の可視化と探索



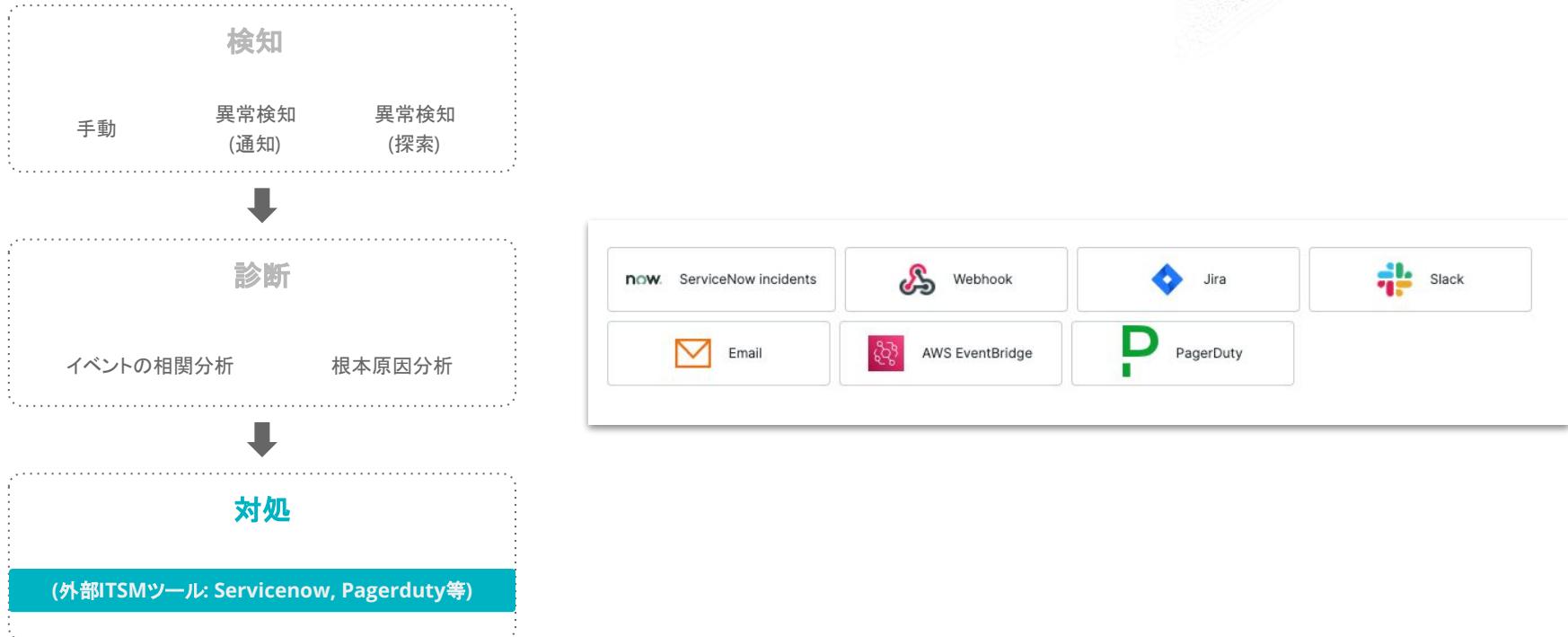
診断1: Correlationによるアラート統合とノイズの削減



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

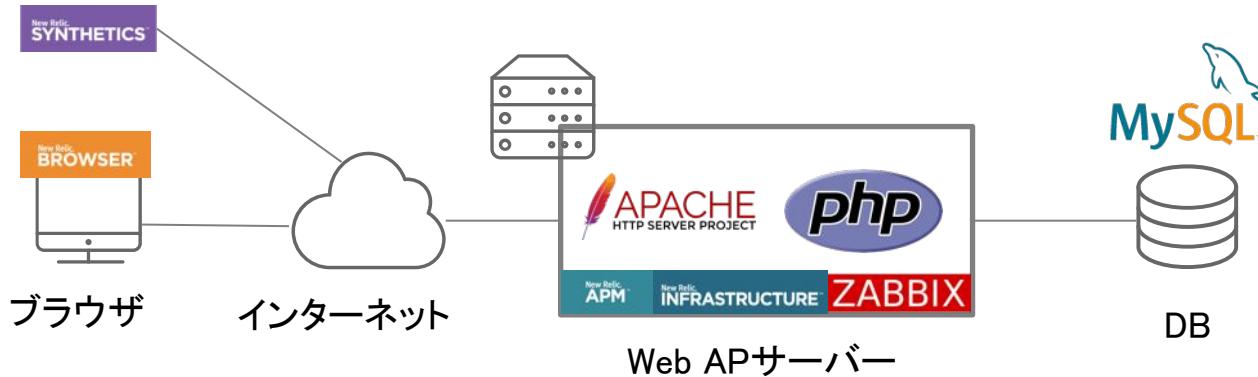
16:15 - 16:30 (15min)

※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、「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]

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

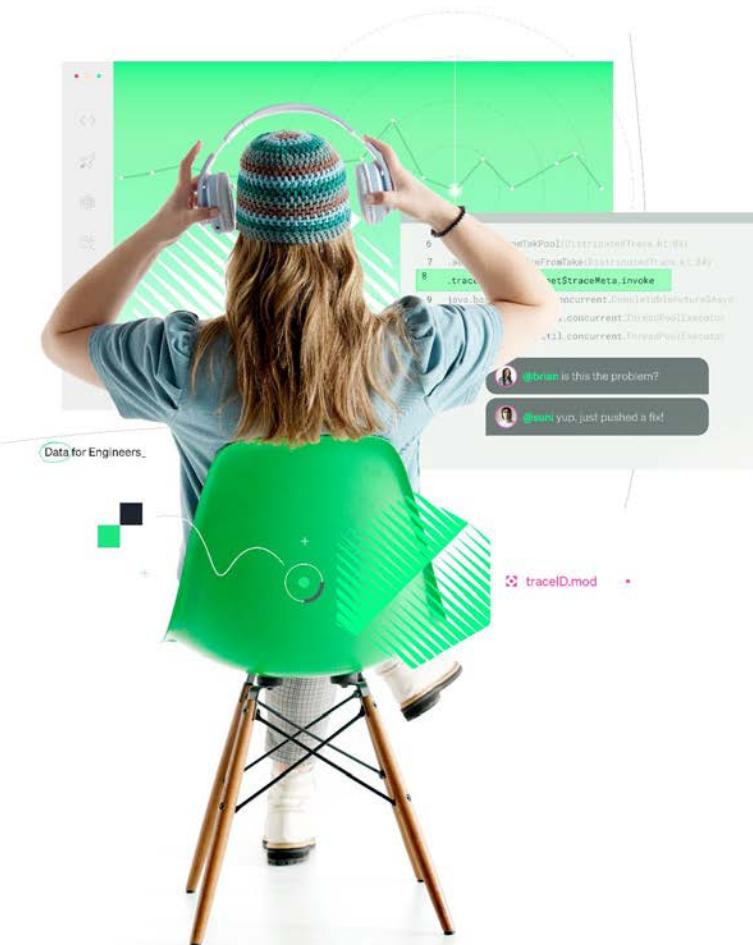
ハンズオン(2)

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

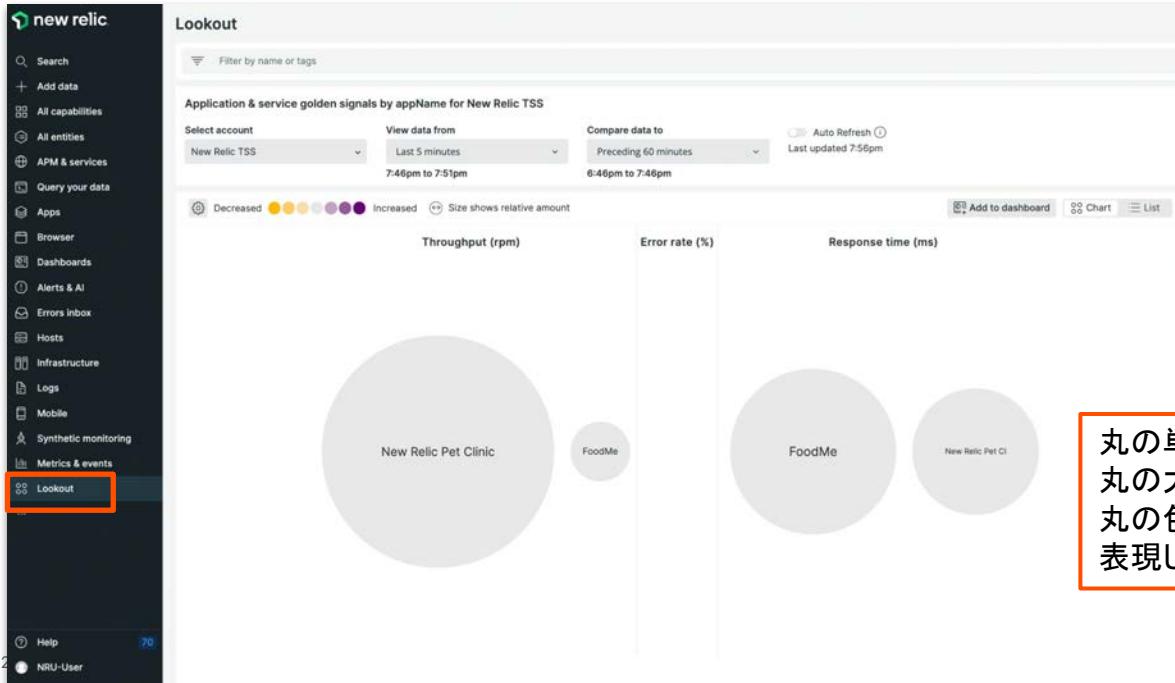


手順・解説

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 shows the New Relic Lookout interface. On the left, the navigation bar includes 'Search', 'Add data', 'All capabilities', 'All entities', 'APM & services', 'Query your data', 'Apps', 'Browser', 'Dashboards', 'Alerts & AI', 'Errors inbox', 'Hosts', 'Infrastructure', 'Logs', 'Mobile', 'Synthetic monitoring', 'Metrics & events', and 'Lookout' (which is selected). The main area displays 'New Relic Pet Clinic' with a 'Throughput' chart comparing the last 5 minutes to the preceding 60 minutes. A message indicates a '1% lower than the preceding 60 minutes' change, with 'Decreased' highlighted. Below this are comparison windows for average and standard deviation. At the bottom, there's a chart for 'Last 5 minutes compared to Preceding 60 minutes'. To the right, a modal window titled 'Other performance indicators for New Relic Pet Clinic' is open, showing tabs for 'Performance' (selected), 'Abnormal history', 'Correlations', 'Profile', and 'Traces'. The 'Performance' tab displays 'Top transactions by percent of wall clock time' (with a purple line graph) and 'Top errors by error class' (with a green line graph). Red boxes highlight the 'Performance' tab and the 'X' button in the top right of the modal. Orange text annotations provide instructions: '見終わったらxを押して閉じます' (Close when you're done) and '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' (Click each tab to see what kind of information it displays).

new relic

Lookout

Search

Add data

All capabilities

All entities

APM & services

Query your data

Apps

Browser

Dashboards

Alerts & AI

Errors inbox

Hosts

Infrastructure

Logs

Mobile

Synthetic monitoring

Metrics & events

Lookout

Help

70

NRU-User

new relic

Lookout

Filter by name or tags

New Relic Pet Clinic

Select account

New Relic TSS

Decreased

1% lower than the preceding 60 minutes

Decreased Increased

Comparison windows

Last 5 minutes average 552.8

Preceding 60 minutes minute average 557.3

Preceding 60 minutes minute standard dev 72.6

Last 5 minutes compared to Preceding 60 minutes

1.4k

1.2k

1k

800

600

400

200

0

3pm 6:50pm 7:00pm 7:10pm 7:20pm 7:30pm 7:40pm 7:50pm

● Newrelic.goldenmetrics.apm.application.throughputs

Alternative comparison windows

Performance Abnormal history Correlations Profile Traces

X

Other performance indicators for New Relic Pet Clinic

Top transactions by percent of wall clock time

View Transactions

WebTransaction/SpringController/owners/{ownerId} (GET)

WebTransaction/SpringController/owners/{ownerId}/edit (GET)

WebTransaction/SpringController/vets (GET)

Top errors by error class

View errors

TransactionError

See end of slide for footer content.

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

90

ハンズオン(2)異常を可視化する

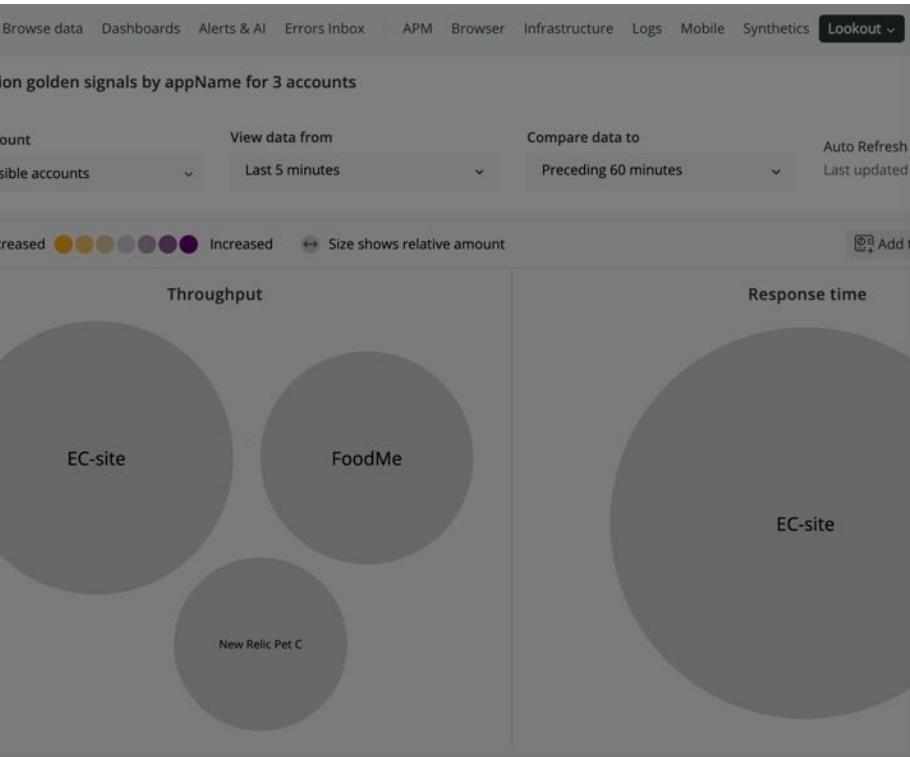
- カスタムのビューを作成します

Manage Views -> Create a new queryを選択

The screenshot shows the New Relic Lookout interface. At the top right, there is a dropdown menu labeled "Manage Views". This menu has several options: "Manage Views", "Open a saved view", "Edit current query", and "Create a new query". The "Create a new query" option is highlighted with a red box. On the left, there are filters for "Select account" (set to "New Relic TSS"), "View data from" (set to "Last 5 minutes" from "7:46pm to 7:51pm"), and "Compare data to" (set to "Preceding 60 minutes" from "6:46pm to 7:46pm"). There is also an "Auto Refresh" toggle. Below these filters, there is a legend for signal changes: "Decreased" (yellow circle), "Increased" (purple circle), and "Size shows relative amount" (grey circle). To the right, there is a section titled "Deviating services" with a search bar and buttons for "Add to dashboard", "Chart", and "List". A message in this section states: "We found no significant deviation in appearances from the prior time window." At the bottom, there are three large circular icons representing different services: "New Relic Pet Clinic", "FoodMe", and "New Relic Pet".

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** Or write a NRQL query

①Eventsを選択

View a chart with
Transaction : count
Transaction : average : duration

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

+ Add row

Facet by
request.uri

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

View data from Compare data to
Last 5 minutes Preceding 60 minutes

Name your view (optional)
csasaki

④request.uriを選択

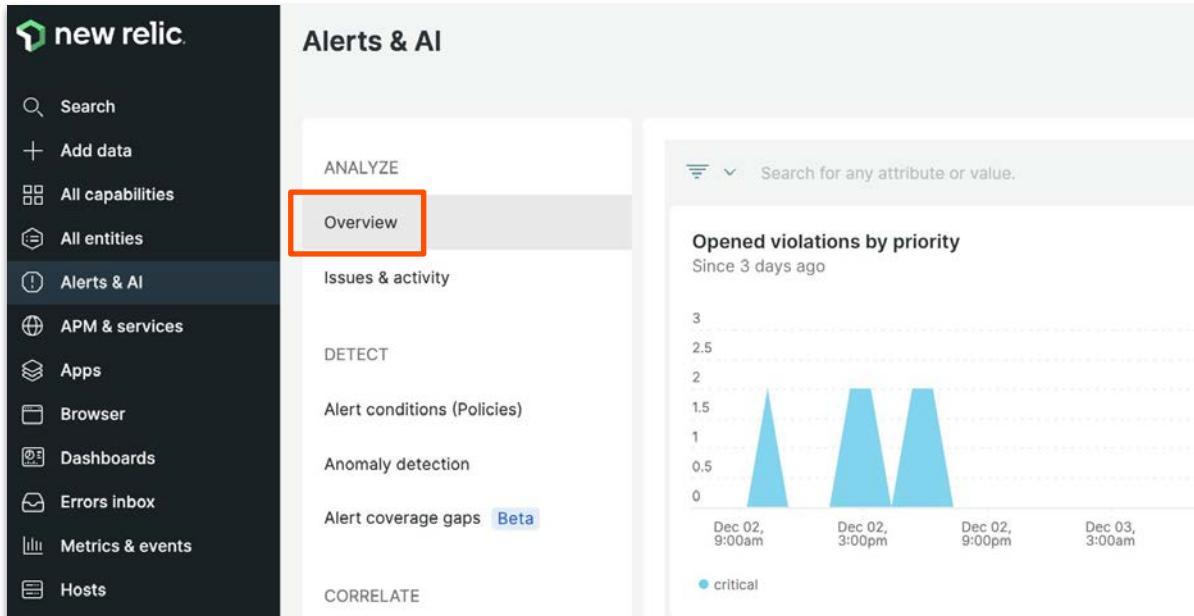
⑤ご自身の名前を入力

⑥Create New Viewを押す **Create New View**

new relic 92

ハンズオン(2)個々のアラートを確認する

- 「Organization: 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



ハンズオン(2)個々のアラートを確認する

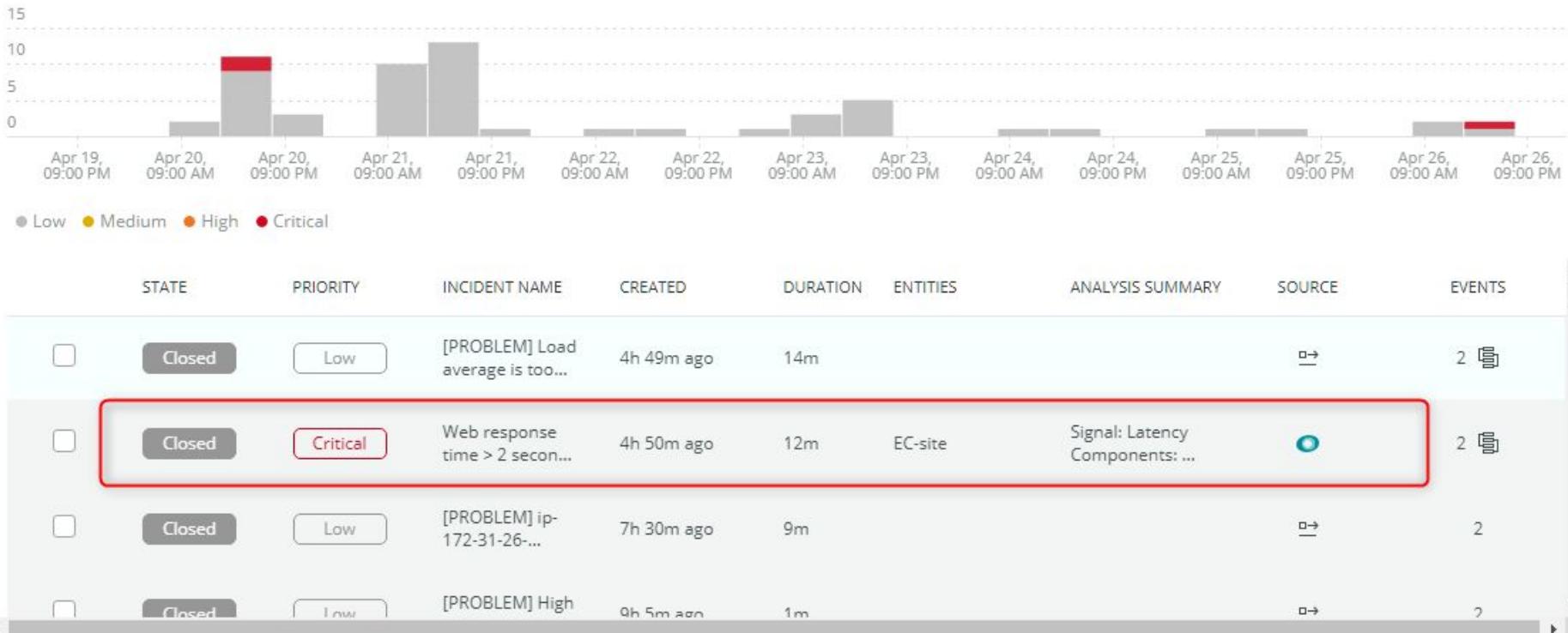
- 「Issues & activity」>「Incidents」タブをクリックします。

The screenshot shows the New Relic interface with the 'Alerts & AI' section selected in the sidebar. The 'Issues & activity' tab is highlighted with a red box. The 'Incidents' tab is also highlighted with a red box. A message at the top says 'This page is going away soon' and 'To analyze incidents side-by-side with other related activity, check the issues page. See your issues'. Below this is a search bar and a chart showing incident counts by date. A table below the chart lists three incidents:

STA...	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	Compon...		2	
<input type="checkbox"/>	Closed	Critical	EC-site query res...	Dec 4, 2022 2:12m	EC-site	Compon...		2	
<input type="checkbox"/>	Open	High	Problem started at...	Dec 4, 2022 2:18h 35m			API	1	

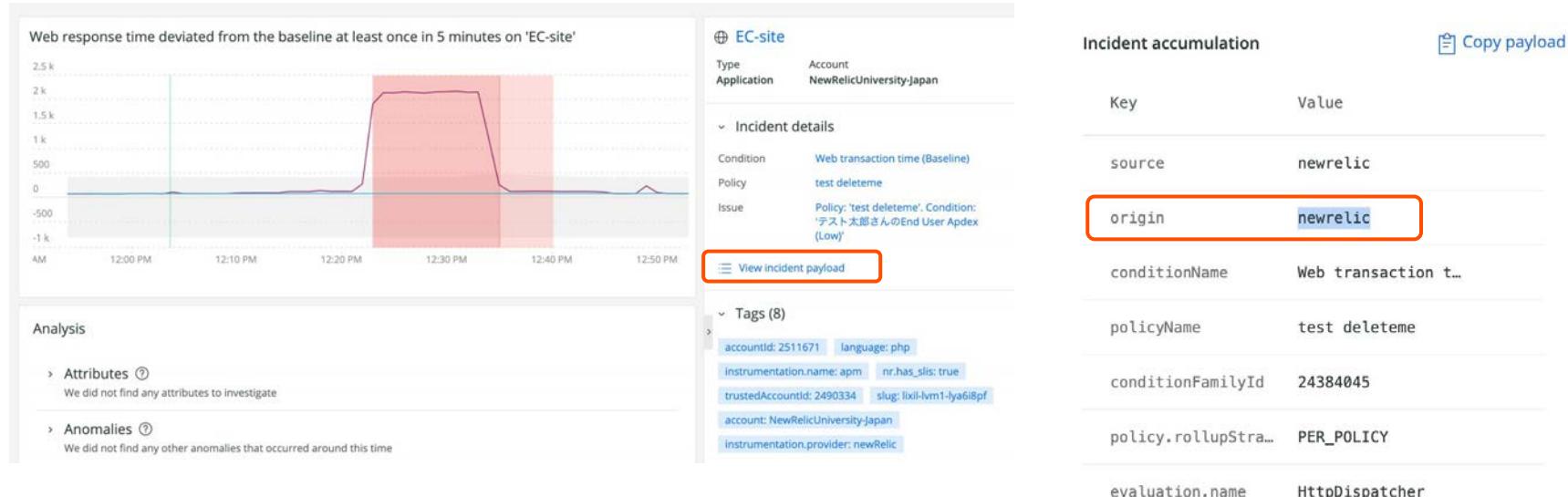
ハンズオン(2)個々のアラートを確認する

- 個々のIncidentをクリックします。



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。



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 shows the New Relic interface with the 'Alerts & AI' menu selected. The main area is titled 'Issues & AI' and displays the 'Issues' tab. A red box highlights the 'Issues' tab in the top navigation bar. Below it, there's a search bar with the query 'state = "Active"'. The main content area shows a chart of anomalies from December 2nd to 5th, with two orange bars indicating activity on December 4th. Below the chart is a table of 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	...

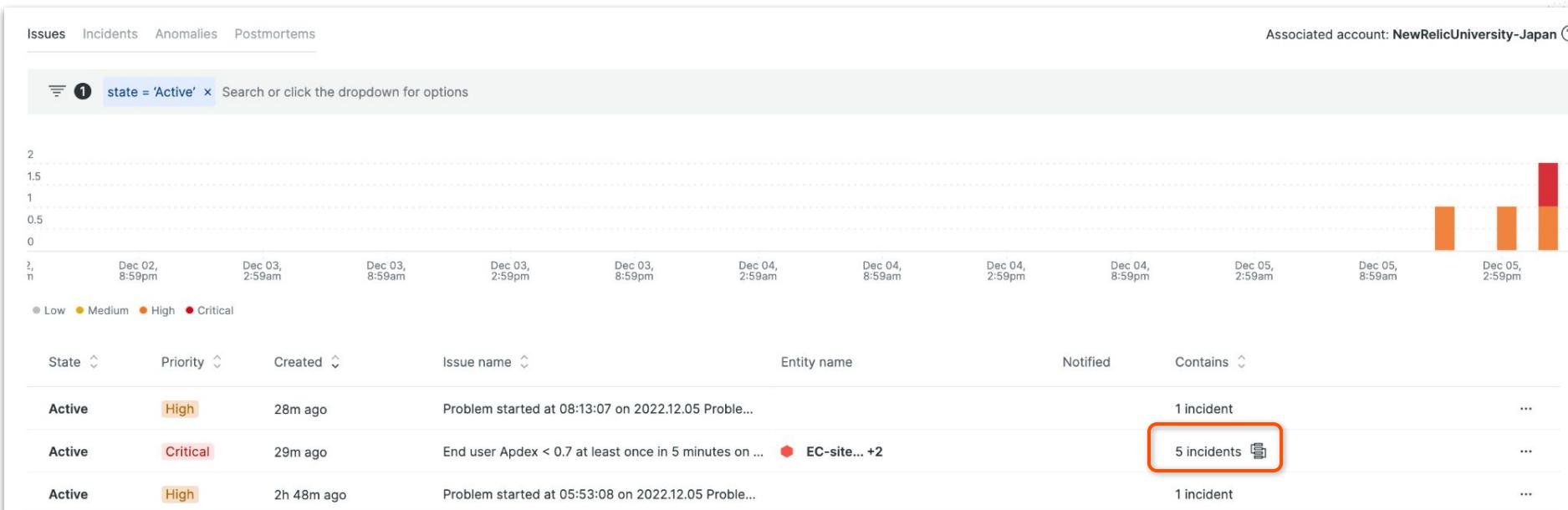
ハンズオン(2)複数のアラートを紐付け トラブルシューティングに役立てる

- ・ 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 shows the New Relic interface with the 'Alerts & AI' menu selected. On the right, the 'Issues & activity' section is displayed. At the top of this section, there is a search bar with the query 'state = 'Active''. This query is highlighted with a red rectangle. Below the search bar, it says 'No chart data available.' and there is a small line chart icon.

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。

Associated account: NewRelicUniversity-Japan (2)

Issues Incidents Anomalies Postmortems

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

A bar chart showing the count of issues over time. The y-axis ranges from 0 to 2. The x-axis shows dates from Dec 02 to Dec 05. There are three bars: one orange bar at 0.5 on Dec 05, 8:59am; one orange bar at 0.5 on Dec 05, 2:59pm; and one red bar at 1.5 on Dec 05, 8:59pm.

Date	Count
Dec 05, 8:59pm	1.5
Dec 05, 2:59pm	0.5
Dec 05, 8:59am	0.5

Legend: Low (grey), Medium (yellow), High (orange), Critical (red)

State	Priority	Created	Issue name	Entity name	Notified	Contains
Active	High	28m ago	Problem started at 08:13:07 on 2022.12.05 Problem...		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 Problem...		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'

Incidents: 5 Source: Issue payload 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 See NRQL overview

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

EC-site query result is > 1.0 for 5 minutes on 'NRU302_alert_lab'

Tags: 10

Entity type: BROWSER Account: NewRelicUniversity-Japan

account: NewRelicUniversit... accountId: 2511671 appName: EC-site clusterAgentId: 445000097 enabled: true id: 24752895 nr.has_slis: true policyId: 1065477 trustedAccountId: 2490334 type: NRQL Query

Incident payload

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

The screenshot displays a complex monitoring and troubleshooting interface, likely from AWS CloudWatch Insights or a similar service. It includes several panels:

- Attributes to investigate**: A section showing facets for Average database duration (ms) and Web response time.
- Web response time > 2 seconds at least once in 5 minutes on 'EC-site'**: A critical alert for EC-site.
- Deployment events (1)**: Shows one deployment event from 22m before issue creation.
- Root cause analysis**: A graph showing the relationship between various entities and the issue.
- Issue timeline**: A timeline showing the progression of the issue from June 06, 9:15pm to June 06, 9:42pm.
- ISSUE LOG**: A log showing 3 incidents, all resolved.
- Database duration (ms) facet**: Faceted by Datastore type and Table and Operation.
- Impact entities**: Three entities are impacted: EC-site, EC-Cube-4, and EC-Cube-1.
- 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

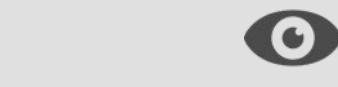
理解できない



気づける

頑張ってすべての
障害ポイントを
洗い出す

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

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. イベントの相關分析
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



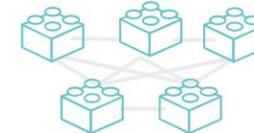
基盤



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

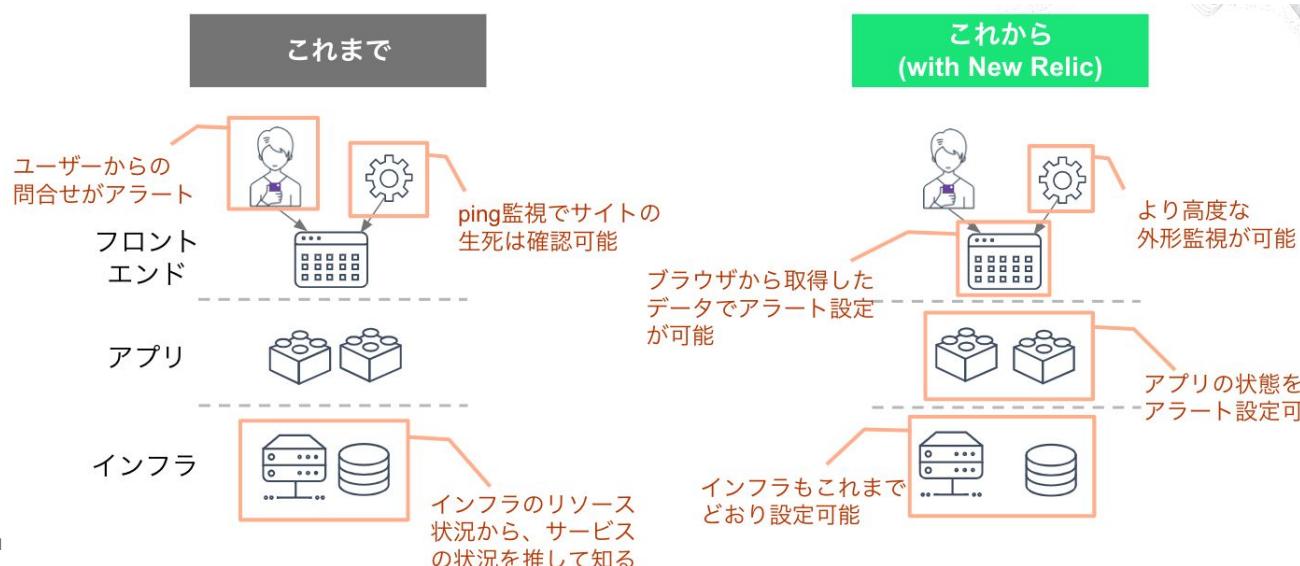


アプリがマイクロサービス化かつ基盤が疎結合なため、基盤リソースと関係なく問題が発生しうる

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

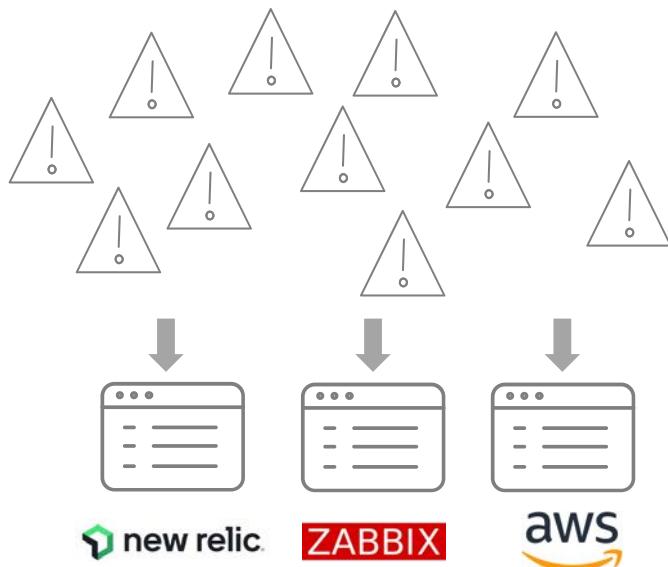


監視にまつわる新たな課題

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

Actionableな監視

とりあえずの監視

人力でこの面を増やすのは困難



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

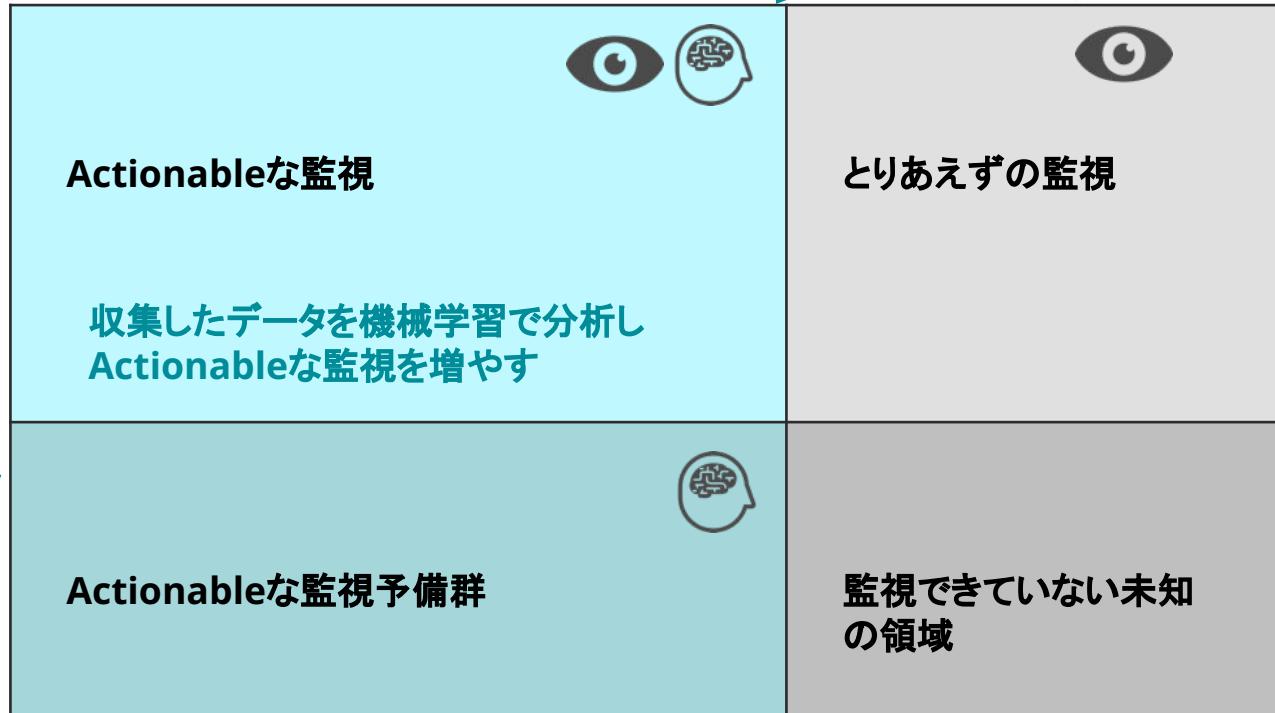
AIOpsのアプローチ

ITサービスに
発生しうる障害

複数の事象を自動で関連付け
根本原因を推察

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

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]
• 異常検知

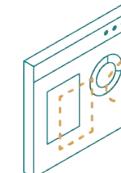


手動でアラート設定せずとも自動で検知

[Alert coverage gaps](#)
[\(BETA\)](#)



[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

Add an alert

EC-site

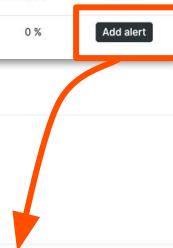
Add recommended conditions

Our power users add these conditions to similar entities.

- Critical EC-site - Error Percentage
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 - Apex
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.



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。

Create an alert condition

Account: 2518671 - NewRelicUniversity-Japan

Enter condition name: EC-site - Apex

Define your signal:

Enter NRQL Query ↗

```
SELECT apdex(apm.service.apdex) FROM Metric WHERE entity.guid = 'MjUxMTY3OXxUUE1BQVNGTE1QVRJTB5BNQ2MDAwMDk3' FACET entity .guid
```

For help with null values, loss of signal, or other query options, see our docs ↗.

Showing 1/1 time series ↗

2 critical violations for displayed time series

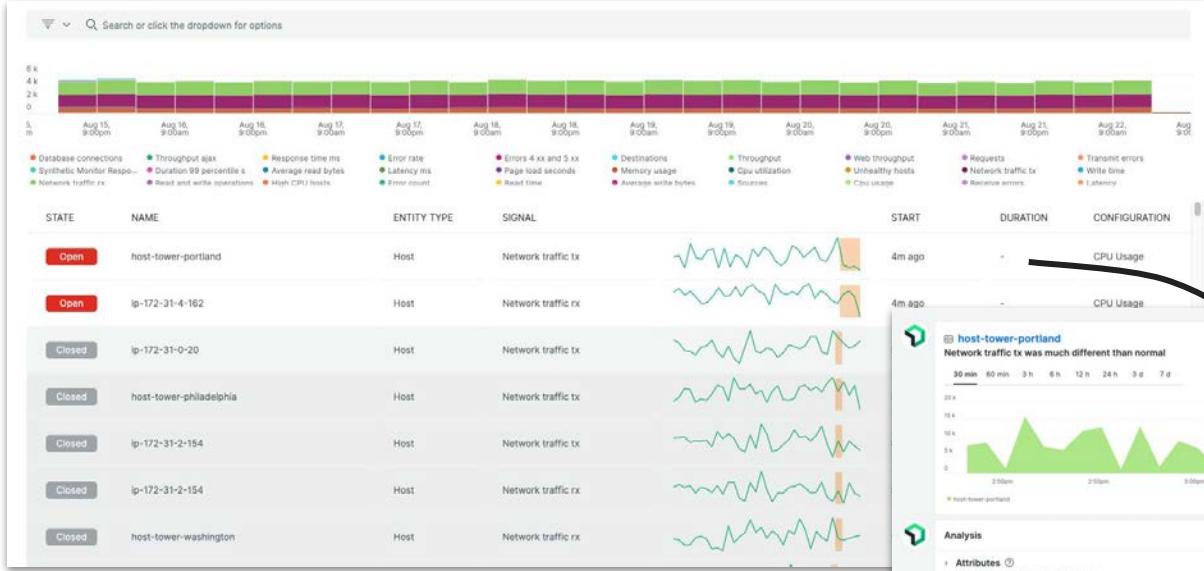
Preview results are estimates only
These charts use your stored data to show how this signal might create incidents. They don't consider all aspects of streaming analytics (e.g., cadence, null values, signal loss, filled data gaps). See our docs ↗

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 ↗

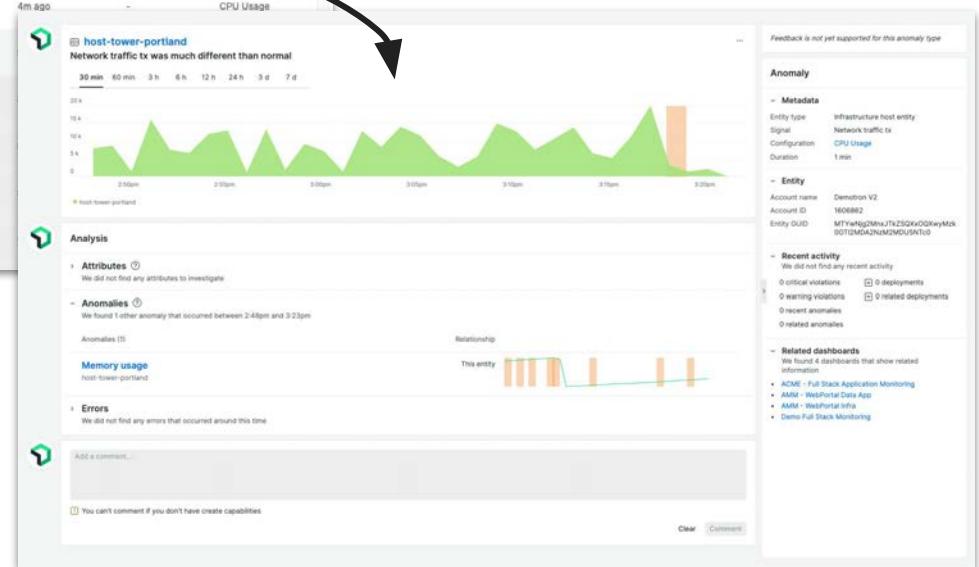
機能紹介: Anomaly Detection



Alerts & AI -> Issues & activity -> Anomalies

- 発生したAnomalyの1つを選択し、詳細を確認する

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。



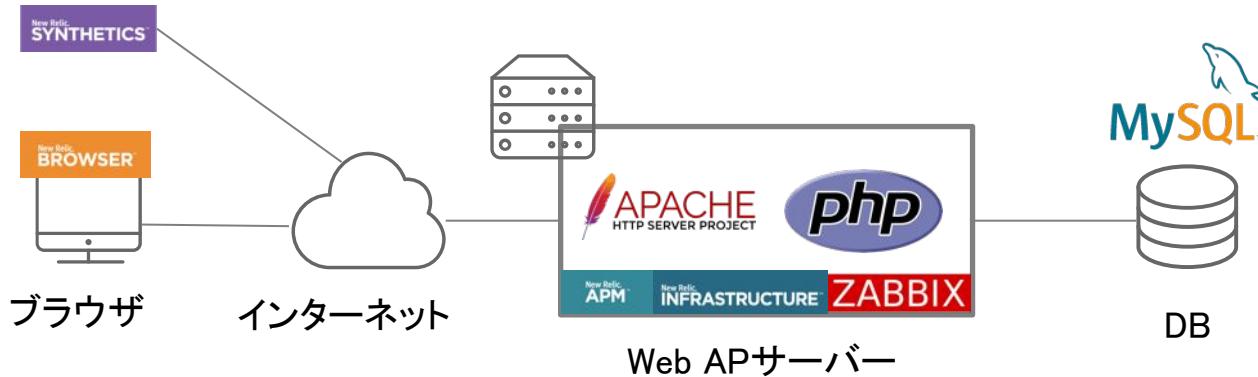
ハンズオン(3) AIOpsを使った異常検知 と原因分析(応用編)

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、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、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(1)

- 「Sources」をクリックします。

The screenshot shows the New Relic interface for 'Alerts & AI'. On the left, a sidebar lists various monitoring categories like 'Add data', 'All capabilities', and 'Metrics & events'. The 'Alerts & AI' category is selected. A red box highlights the 'Sources' link under the 'CORRELATE' section. The main area displays an 'Issues' dashboard with a bar chart showing alert volumes over time (Dec 2-5) and a table of active issues. The table includes columns for State, Priority, Created, Issue name, Entity name, Notified, and Contains.

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。

The screenshot shows the 'Alerts & AI' interface with the 'Sources' tab selected. On the left, there's a sidebar with 'ANALYZE' (Overview, Issues & activity), 'DETECT' (Alert conditions (Policies), Anomaly detection), 'CORRELATE' (Sources, Decisions), and 'ENRICH & NOTIFY' (Muting rules, Workflows). The main area displays '1 active source' connected to '1 policy'. Below this, the 'Available sources' section is shown, featuring two cards: 'Alerts' (selected, highlighted with a red box) and 'REST API'. The 'Alerts' card shows '1 active policy' and a brief description: 'Ingest your existing alert policies for correlations to gain actionable insights and cross-source visibility of your stack.' The 'REST API' card has a small icon and a brief description: 'Use REST endpoint to easily ingest monitoring data for correlations from any other tool, including homegrown solutions.'

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。

The screenshot shows the 'Associated account: NewRelicUniversity-Japan' header. On the left, there's a 'New Relic Alerts source' section with a green icon and a brief description about connecting policies to filter noise. On the right, a 'NEW RELIC IS CONNECTED' message is displayed. At the bottom, there's a 'POLICIES (1)' section showing a single policy named 'ダッシュボードハンズオン用アラートポリシー' and an 'ACCOUNT' section showing 'NewRelicUniversity-Japan'. A prominent orange-outlined button labeled '+ Add a policy' is located at the bottom right.

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 ↗

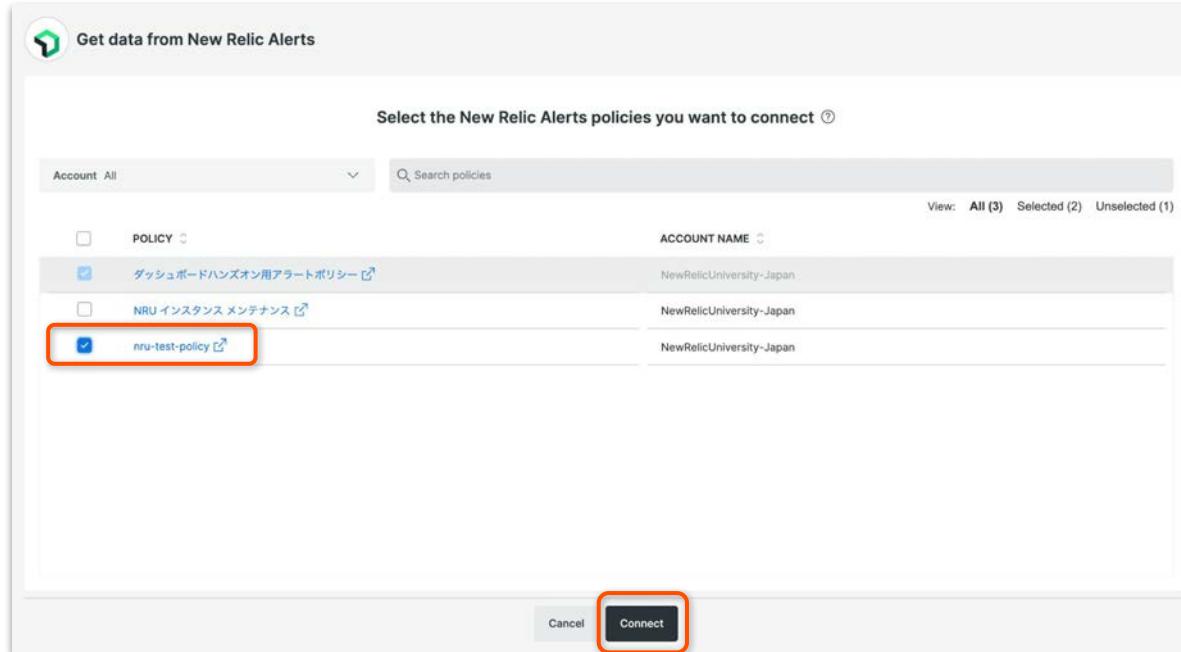
ACCOUNT ⓘ

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。



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 checked="" 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	Entities: 2
APM	<input checked="" type="checkbox"/>

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 Non-web throughput Error rate Web response time Non-web response time

▼ 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

▼ Do you want to correlate anomalies from this configuration? [?](#)

Correlate with other alerts

[Cancel](#) [Save configuration](#)

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](#)

Search configurations

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 shows the 'Alerts & AI' section of the New Relic platform. On the left, a sidebar lists various features: ANALYZE (Overview, Issues & activity), DETECT (Alert conditions (Policies), Anomaly detection), CORRELATE (Sources, Decisions), ENRICH & NOTIFY (Muting rules), and Workflows (New). The 'Sources' option under CORRELATE is selected. In the main area, there's a summary card showing '1 active source' and '1 policy connected'. Below this, two boxes are displayed: 'Available sources' (Alerts, REST API). The 'REST API' box is highlighted with an orange border. It contains a small icon of a computer monitor with the word 'API' and 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。

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

Create an insert key

1. Go to our [Insights insert key page](#).
2. 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

- Incident Intelligence 用メディアタイプは現在プロトタイプです。

The screenshot shows the Zabbix 5.0 interface with a red box highlighting the 'Media Types' option in the left-hand navigation menu. The main content area displays a configuration form for a 'Media Type' named 'ALERTS_SUBJECT'. The form contains several fields with placeholder values:

ALERTS_SUBJECT	(ALERTS SUBJECT)
event_id	{EVENT.ID}
event_nseverity	{EVENT.NSEVERITY}
event_recovery_status	{EVENT.RECOVERY.STATUS}
event_recovery_value	{EVENT.RECOVERY.VALUE}
event_source	{EVENT.SOURCE}
event_tags	{EVENT.TAGS}
event_time	{EVENT.TIME}
event_update_status	{EVENT.UPDATE STATUS}
event_value	{EVENT.VALUE}
host_name	{HOST.HOST}
new_relic_bearer	Bearer eyJ0eXAiOiJKV1QiLCJhbGki
new_relic_proxy_url	
new_relic_url	https://collectors.signalfx.io/v1/inciden
urgency_for_average	2
urgency_for_disaster	1
urgency_for_high	2

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](#)

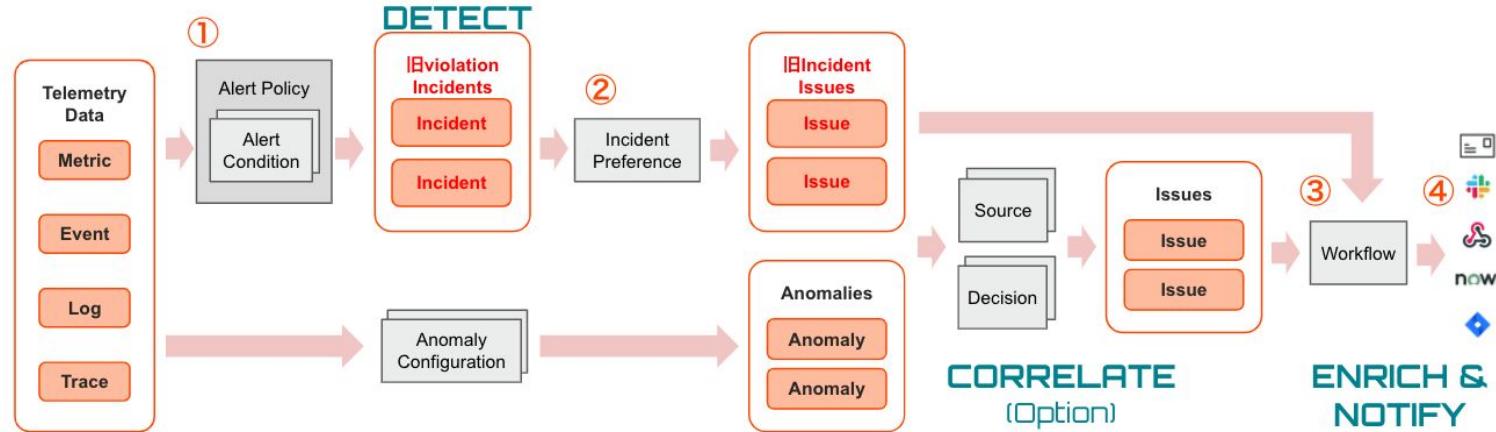
* 少なくとも1つ以上の実行内容が設定されている必要があります。

[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.

