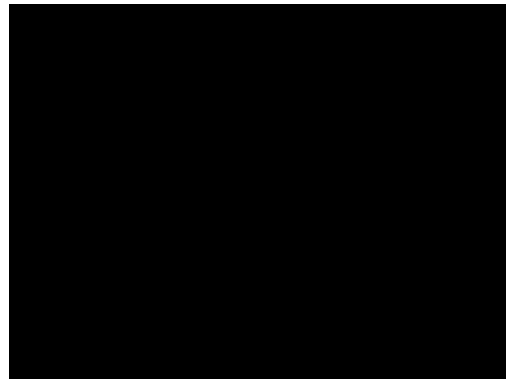


NRU 304 「AIOps とアラート設計の基本」

August 24, 2022

15:00より開始致します。しばらくお待ちください。
音声聞こえづらい場合は退出、再入室をお試ください。



Safe Harbor

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

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

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

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

ウェビナー 各種ご連絡

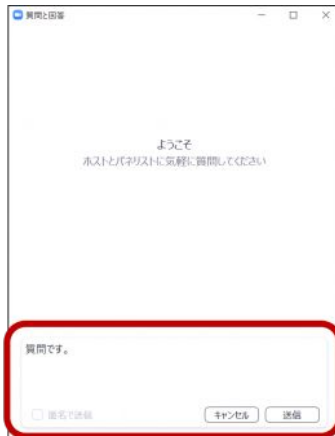
1. ご質問がある場合は、「Q & A」からご入力ください。



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。

原 健一郎

New Relic K.K.

Solutions Consultant

ネットワーク/パフォーマンス/サーバの運用監視にて
エンジニアとしてのキャリアを開始。

得意な技術は、

- **Content Delivery Network**
- **暗号化技術**
- **ID管理**
- **Cloud Security**



本日のゴール

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

本セッションの想定対象者と前提条件

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

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

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

Agenda

時間(目安)	内容	
15:00-15:15	座学(1)	ユーザー視点のアラート
15:15-15:30	座学(2)	New Relicのアラート機能
15:30-15:40	ハンズオン(0)	環境を確認する
15:40-16:00	ハンズオン(1)	アラートを作成する
16:00-16:15	座学(3)	New RelicのAIOps機能
16:15-16:30	ハンズオン(2)	AIOpsを使った異常検知と原因分析
16:30-16:45	座学(4)	AIOpsの意義
16:45-16:55	ハンズオン(3)	AIOpsを使った異常検知と原因分析 (応用編)
16:55-17:00		まとめ、アンケートご記入

座学(1)

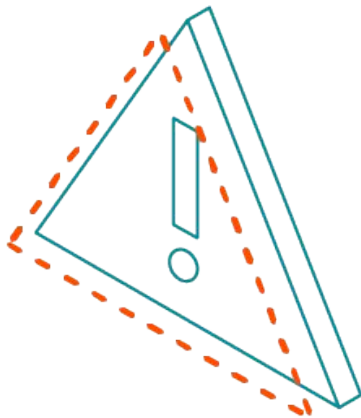
ユーザー視点のアラート

15:00 - 15:15 (15min)



突然ですが

- どんなアラートを設定していますか？



アラートを設定する目的

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

1. システムの停止、またはパフォーマンスの悪化が発生し、ユーザーへのサービス提供に支障が出ている
2. 1のような事象が近いうちに発生する可能性がある兆候が出ている

“受け取った結果、何かしらのアクションを起こせるようなアラート”を設定する

アラートのアンチパターンとデザインパターン

アンチパターン: OSのメトリクスのアラート

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

“OSのメトリクスは診断やパフォーマンス分析にとっては重要です。

しかし99%の場合、これらのメトリクスは誰かを叩き起こすには値しません。”

出典: 入門監視 (Oreilly, 2019)



アラートのアンチパターンとデザインパターン

デザインパターン: ユーザー視点の監視

“ユーザーが気にするのは、アプリケーションが動いているかどうかです。”

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

出典: 入門監視 (Oreilly, 2019)

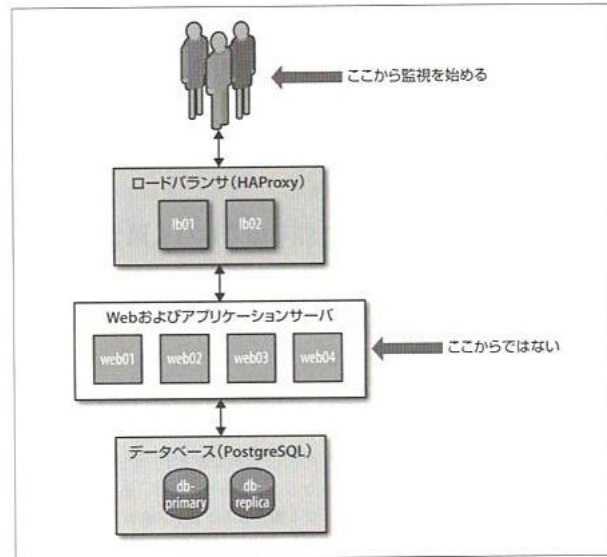
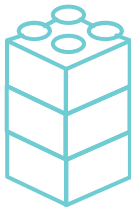


図2-1 できるだけユーザーに近いところから監視を始める

なぜアンチパターンが生み出されたのか

過去のシステム

アプリ



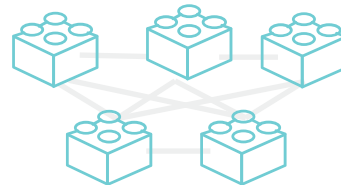
基盤



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

近年のシステム

アプリ



リソース抽象化
(仮想化、コンテナ等)

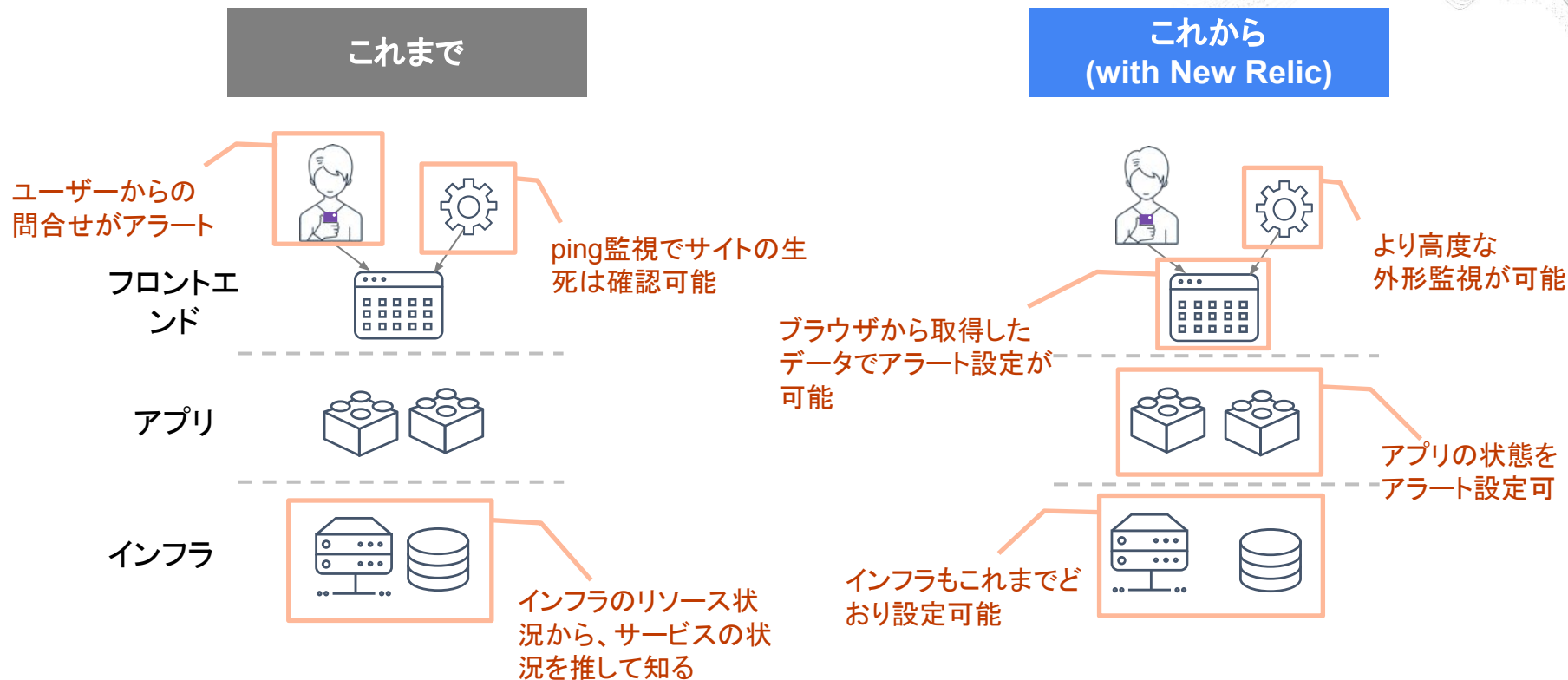


基盤



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

アラートのこれまでと、New Relicを使ったこれから



目的別、アラート設定例(Webアプリの一例)

カテゴリ	現在起こっているサービス影響		将来のリスクの兆候	
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 - 15:30 (15min)

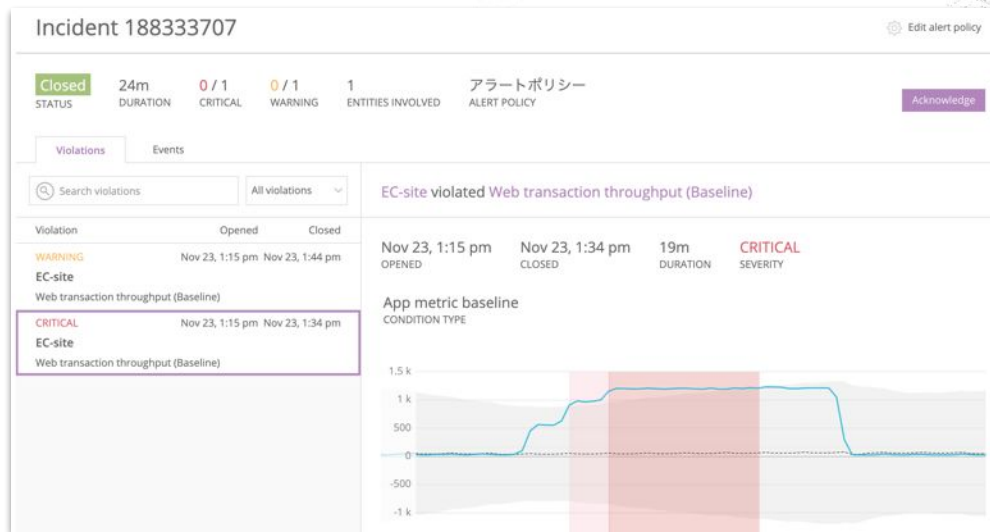


New Relicのアラート機能

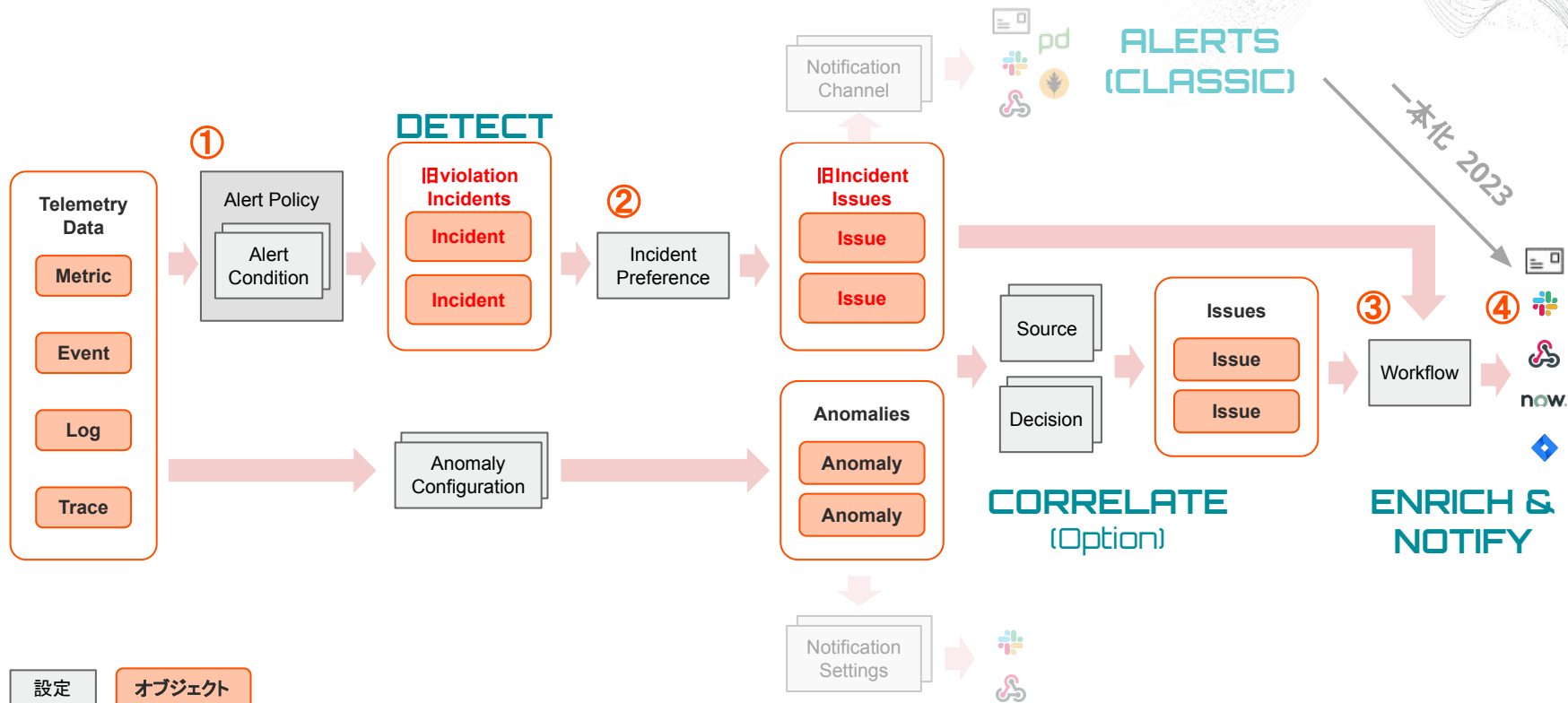
New Relicが**収集しているデータ**を使って、アラートを設定することが可能

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

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



New Relicのアラート構造全体像



アラート機能の全体UIと重要メニュー

The image displays the New Relic Alerts & AI interface. The top navigation bar includes the New Relic logo, a search bar, and a menu with items: Explorer, Browse data, Dashboards, Alerts & AI (highlighted), Errors inbox, APM, Browser, Infrastructure, Logs, Mobile, Synthetics, and More. A large arrow points from the 'Alerts & AI' menu item to a detailed view of the interface.

The detailed view shows the 'Alerts & AI' dashboard. The left sidebar contains the following menu items:

- ANALYZE
 - Overview
 - Issues & activity
- DETECT
 - Alert conditions (Policies)
 - Anomaly detection
 - Detection gaps [Beta](#)
- CORRELATE
 - Sources
 - Decisions
- ENRICH & NOTIFY
 - Muting rules
 - Workflows [New](#)
 - Destinations
- SETTINGS
 - General
- ALERTS (CLASSIC)
 - Events
 - Incidents
 - Channels

The main content area displays several charts and tables:

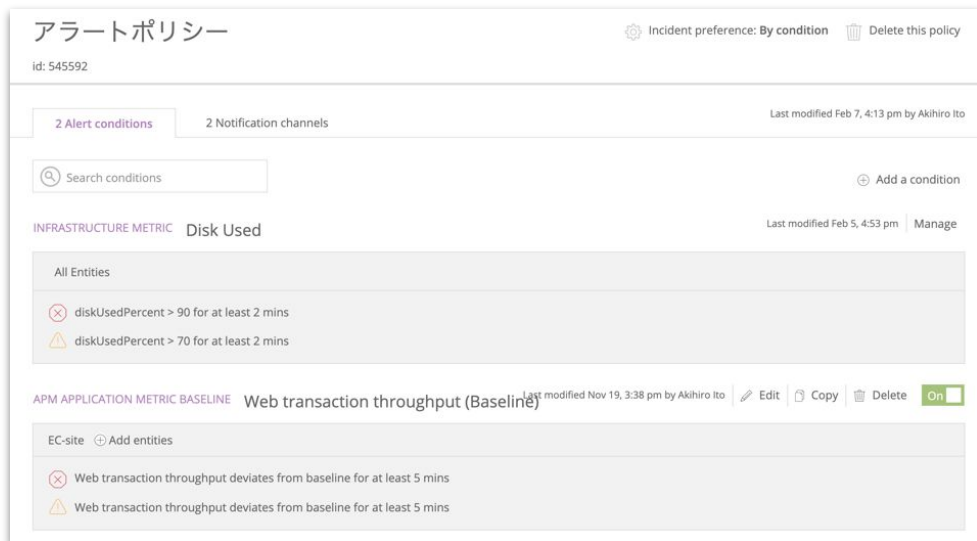
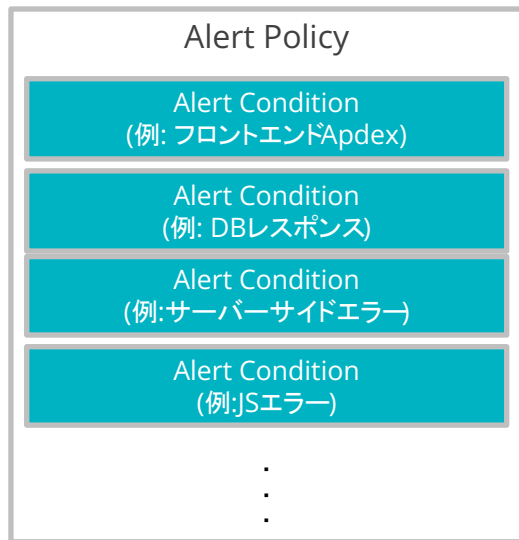
- Opened violations by priority:** A line chart showing violations over time (Aug 15 to Aug 23). The y-axis ranges from 0 to 4. A green area chart shows the number of violations, with a peak around Aug 18.
- Opened violations by priority (Summary):** A donut chart showing 17 violations, with 17 critical (100%).
- Closed violation durations:** A bar chart showing durations in minutes (0 to 350). The y-axis ranges from 0 to 12. A blue bar chart shows the number of violations, with a peak around 150 minutes.
- Muted violations:** A donut chart showing 34 violations, with 34 not muted (100%).
- Top policies creating violations:** A table showing the top policies creating violations. The first policy is 'ダッシュボードハンズオン用アラートポリシー' with 17 violations.
- Top conditions creating violations:** A table showing the top conditions creating violations. The first condition is 'NRU302_alert_lab' with 17 violations.
- Top sources of violations:** A table showing the top sources of violations. The first source is 'PageView query' with 17 violations.

Callouts from the left sidebar point to the corresponding sections in the main content area:

- DETECT** points to the 'DETECT' section of the sidebar.
- Alert conditions (Policies)** points to 'Alert conditions (Policies)' in the sidebar.
- Anomaly detection** points to 'Anomaly detection' in the sidebar.
- Detection gaps [Beta](#)** points to 'Detection gaps [Beta](#)' in the sidebar.
- ENRICH & NOTIFY** points to the 'ENRICH & NOTIFY' section of the sidebar.
- Muting rules** points to 'Muting rules' in the sidebar.
- Workflows [New](#)** points to 'Workflows [New](#)' in the sidebar.
- Destinations** points to 'Destinations' in the sidebar.

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



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

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

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

1. Categorize

Select a product

NRQL

APM

Browser

Mobile

Synthetics

Infrastructure

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

アラートのしきい値設定は2種類から選択可能

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

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

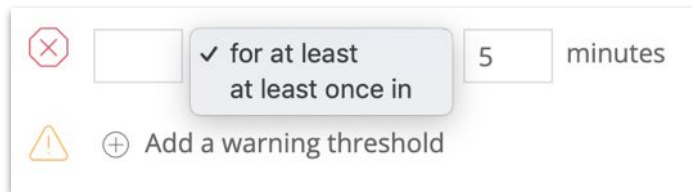
しきい値を超過した場合のアラート発報タイミング

- **For at least xx minutes**

しきい値をxx分継続して超過した場合のみ Incidentが起票される

- **at least once in xx minutes**

しきい値を1回でも超過した場合に Incidentが起票される



The screenshot shows a configuration panel for an alert condition. It features a red 'X' icon in a hexagon, a text input field, a dropdown menu with the selected option 'for at least at least once in', a numeric input field containing '5', and the unit 'minutes'. Below these elements is a yellow warning triangle icon and a button with a plus sign and the text 'Add a warning threshold'.

Alert ConditionはCriticalとWarning(オプション)2種類を作成できるが、
通知が飛ぶのはCriticalの場合のみ(WarningはUI上で確認できる)

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

▼ Additional settings

Close open violations after: Why is this required? 

 Add custom violation description

Runbook URL

 Remove

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

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

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

※アラートポリシーを作成する際に設定(後で編集可)

ISSUE CREATION PREFERENCE

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

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

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

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

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

[See our docs](#)

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

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

Issueの起票粒度について

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

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

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

New Relic アラートの構成要素3: Workflows

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

Select Issues

- 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 New Relic Workflow configuration interface. At the top, there is a 'Name' field with the placeholder 'Enter a name you'll recognize'. Below this is the 'Select issues' section, which includes two radio buttons: 'Build a query' (selected) and 'Send all issues'. Underneath is a 'Select or enter attribute' button with a help icon. A '+ AND' button is also present. The 'Enrich (optional)' section has a '+ Build a query' button. The 'Mute issues' section has three radio buttons: 'Do not send notifications for fully muted issues' (selected), 'Do not send notifications for fully or partially muted issues', and 'Always send notifications'. At the bottom, there are several destination tiles: 'ServiceNow incidents', 'Webhook', 'Jira', 'Slack', 'Email', 'AWS EventBridge', and 'PagerDuty'. A 'Test workflow' button is located at the very bottom.

New Relic アラートの構成要素4: Destinations

Issueのライフサイクルに応じた通知を受けることができる

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

Workflowsと関連づけると、以下の形式で通知される

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

その他、追加で利用可能な通知先一覧は以下のとおりとなります

servicenow
now™

Webhooks


JIRA


Slack

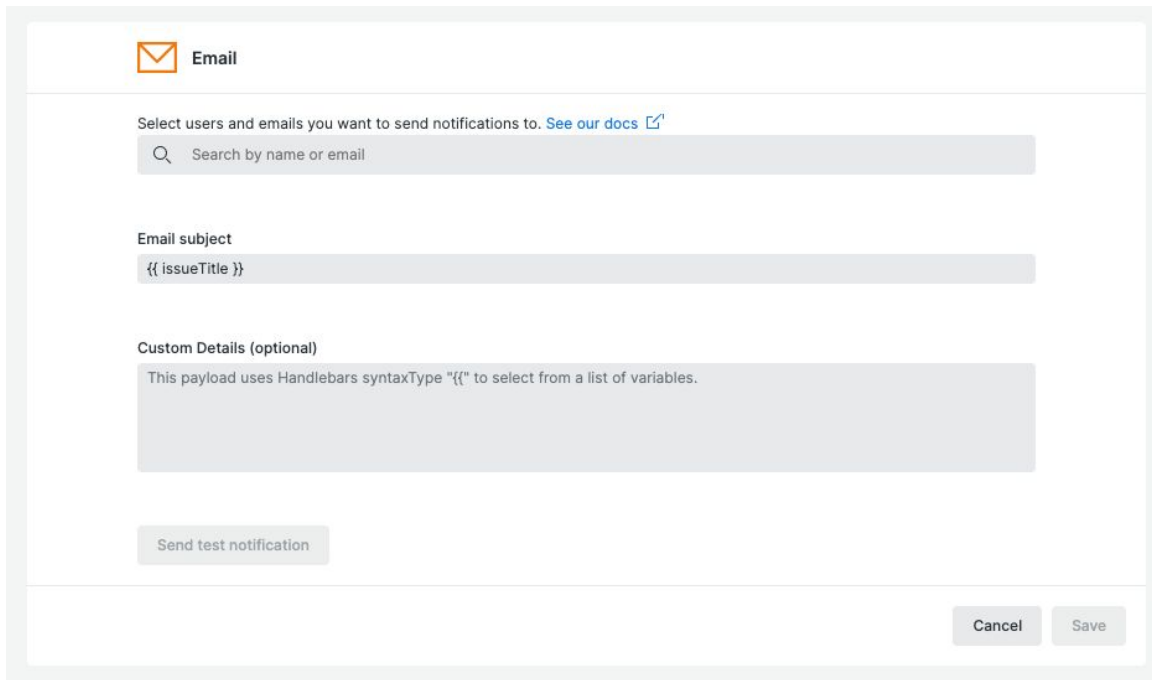

Email


Amazon
EventBridge


Pager Duty
pd

Mobile push


重要: Email内容の設定画面



 Email

Select users and emails you want to send notifications to. [See our docs](#) 

 Search by name or email

Email subject

{{ issueTitle }}

Custom Details (optional)

This payload uses Handlebars syntaxType "{{" to select from a list of variables.

Send test notification

Cancel Save

- [Workflows変数](#)を用いた柔軟なメールタイトル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。

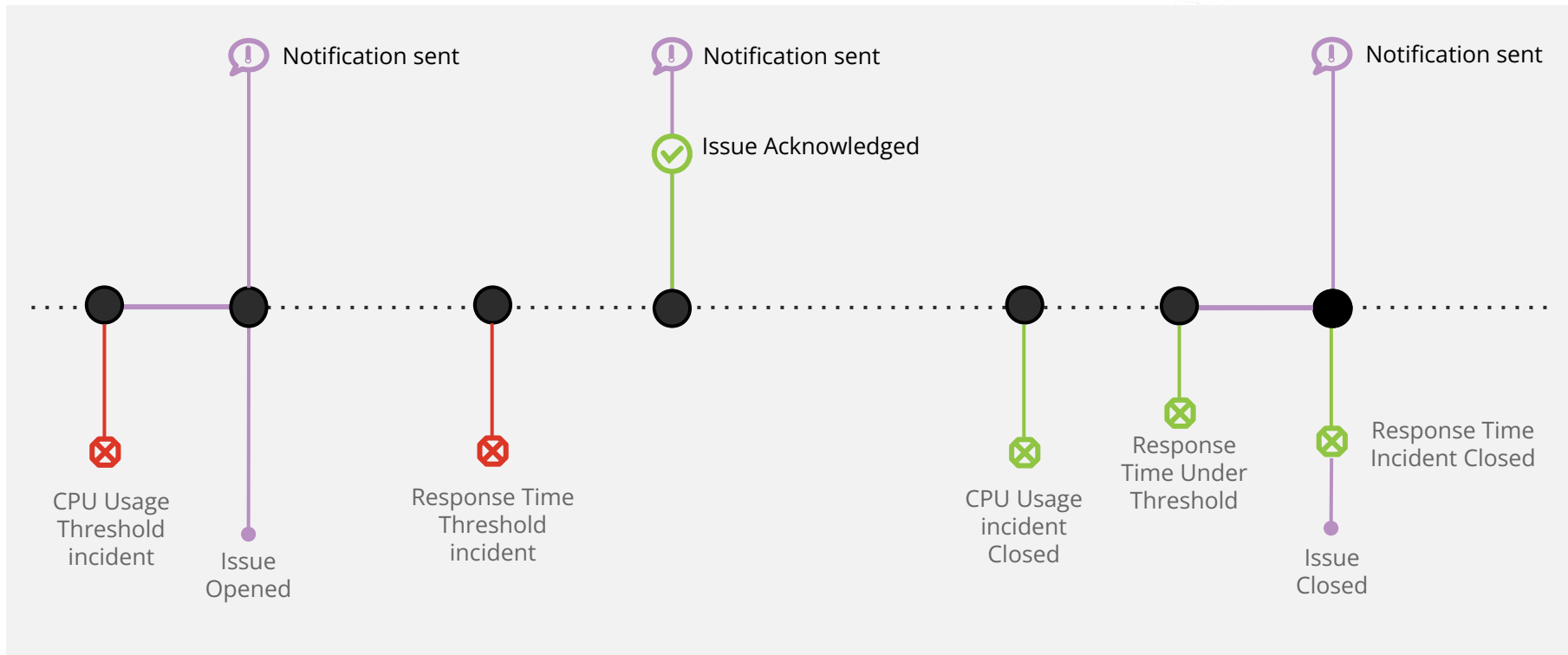
Workflows variables:

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

© 2022 New Relic, Inc. All rights reserved

補足: Issueのライフサイクルと通知タイミング

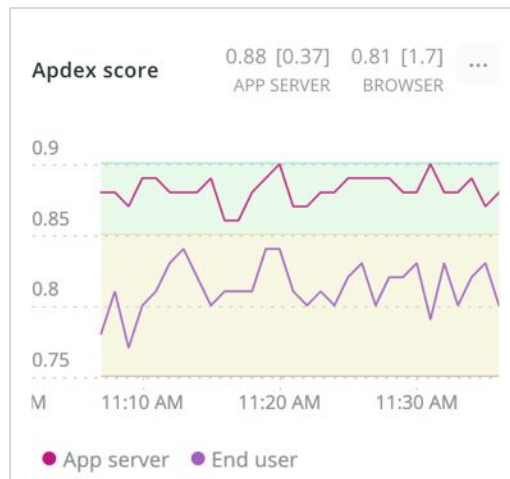
Issueの起票、Acknowledgeがされたタイミング、およびクローズの際に通知が届く



アラートを設定する前にやること

Apdex Tの値を適切に設定する

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



Application server

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

Apdex T

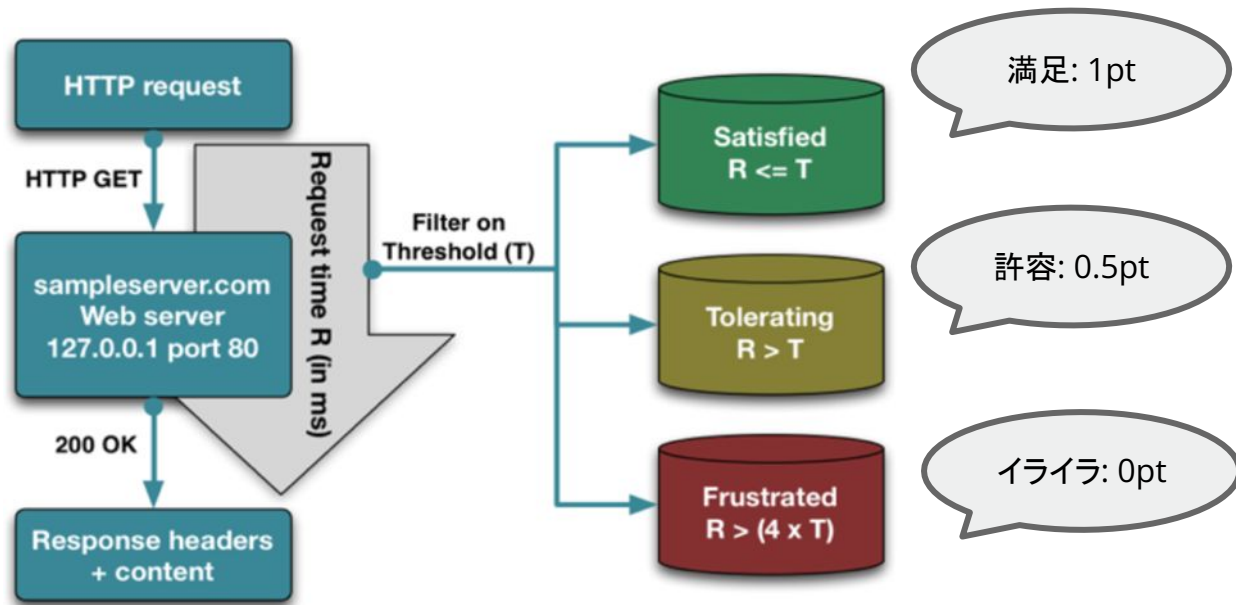
seconds

Please input a decimal or whole number only.

Apdex T値について

それを満たせばユーザーが満足すると想定される、最大応答速度

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



ハンズオン(0) 環境を確認する

15:30 - 15:40 (10min)

Presenter Name

Title



**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

The login page shows the email 'japan-handson+2021@newrelic.com' and a password field. The 'Remember my email' checkbox is checked and highlighted with a red box. A green 'Log in' button is at the bottom.

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](#)

The user profile page for 'NRU-User' (japan-handson+2021@newrelic.com) is shown. The 'Log out' button at the bottom is highlighted with a red box.

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

User preferences
API keys
Manage your plan

Administration

View settings
Theme New Light Dark Auto
NRQL console Show Hide

Add more data
Manage your data

Support >

Log out

The account selection page shows two accounts for the email 'japan-handson+2021@newrelic.com'. The first is 'Original New Relic account' and the second is 'NewRelic.kk Default'. A blue arrow points from the 'Log out' button in the previous screen to this page.

new relic

Log in to your account

You have been signed out.

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

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

[Use a different account](#)

ハンズオン環境へのログイン方法

[準備]

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

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

※本ハンズオンセミナーでは 2つのNew Relicアカウントにログインします。
スムーズに切り替えを行うためにログイン時に [Remember my email]にチェックをつけてください
ログイン切り替えは次項参照

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

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

今回監視対象のサイト

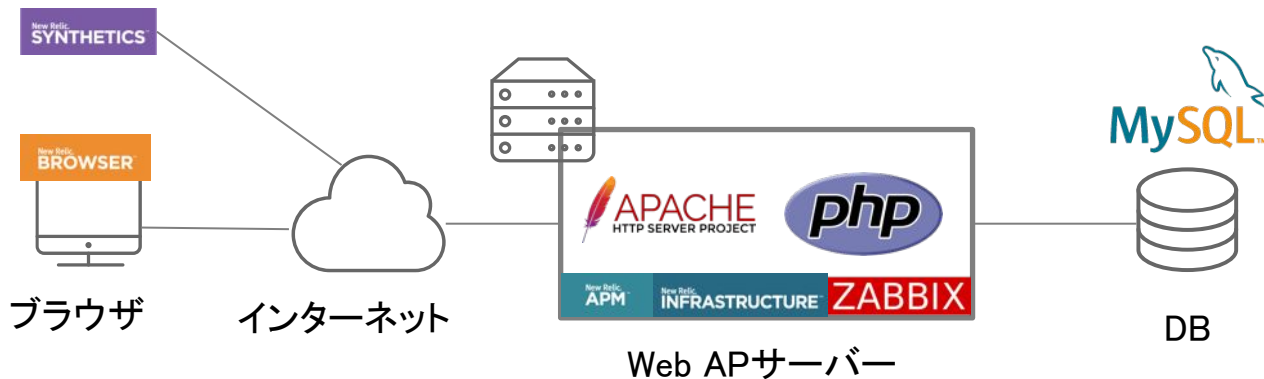
[NRUジェラートショップ](ECサイト)

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



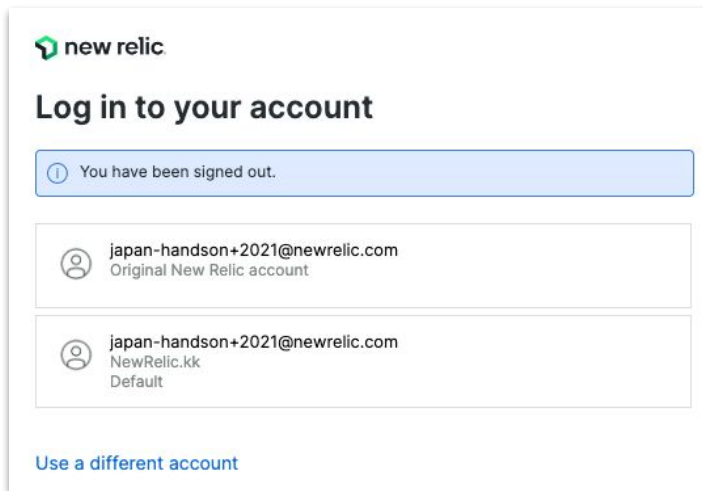
今回の環境の監視構成

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



ハンズオン(0) 2つのアカウントにログインする

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

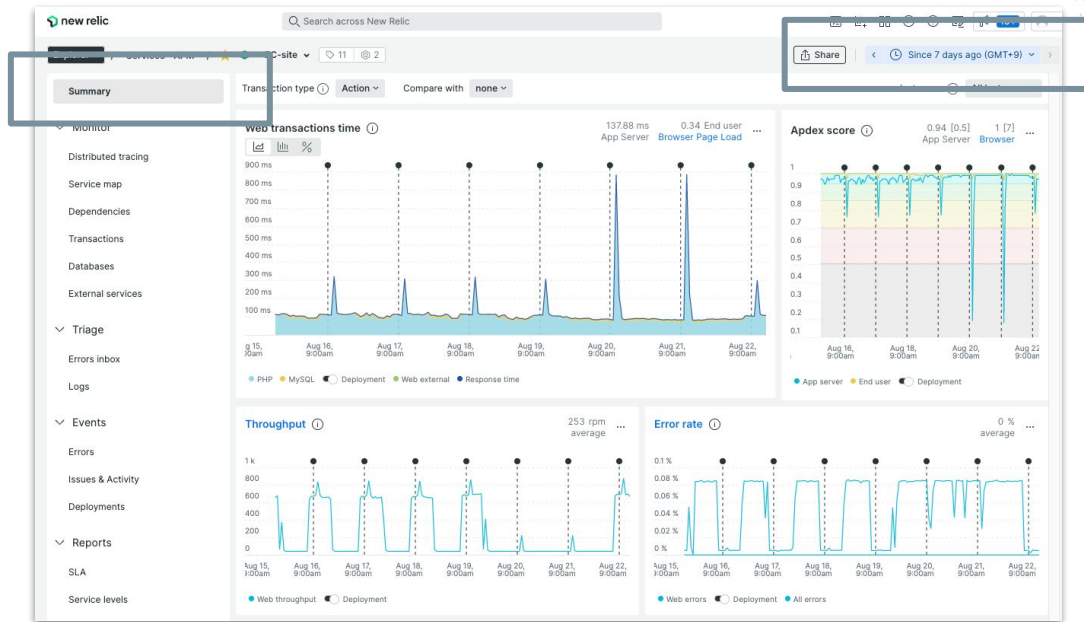


The screenshot shows the New Relic login interface. At the top is the New Relic logo and the text "Log in to your account". Below this is a blue notification bar that says "① You have been signed out." There are two account selection boxes. The first box shows a user icon, the email "japan-handson+2021@newrelic.com", and the label "Original New Relic account". The second box shows a user icon, the same email "japan-handson+2021@newrelic.com", and the label "NewRelic.kk Default". At the bottom of the login area is a link that says "Use a different account".

ハンズオン(0) FSO UIの確認

- New Relicポータルの大メニューのAPM、あるいは左ペインのServices - APMを選択し、EC-siteアプリを選択します。
- Summaryが選択されていることを確認します。
- 表示するデータの表示幅を 7 days に変更します。

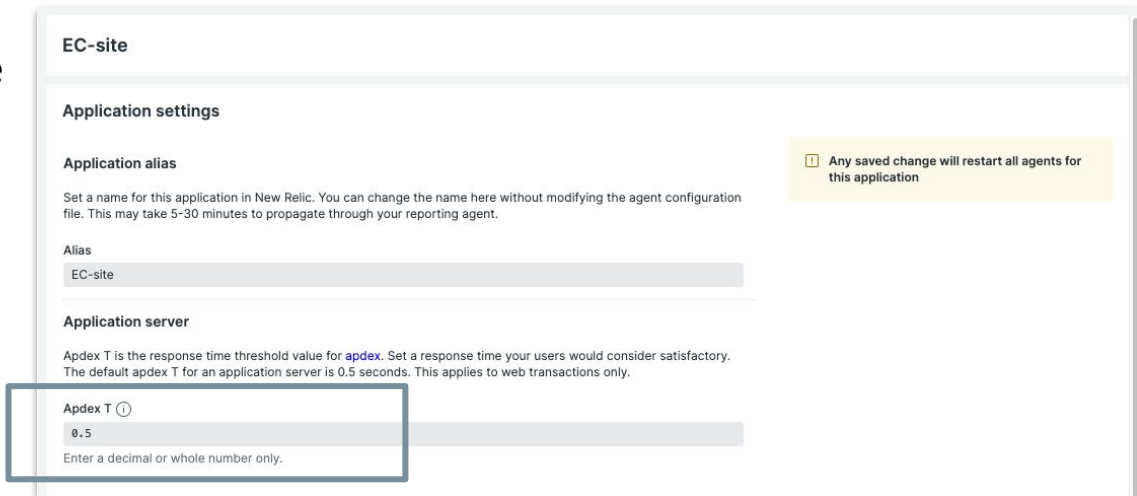
同様に、BrowserやInfrastructureを参照してください。



ハンズオン(0) Apdex Tの設定箇所の確認

変更は行わない!!!

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



The screenshot shows the 'EC-site' application settings page in New Relic. The page is divided into sections: 'Application settings', 'Application alias', and 'Application server'. The 'Application alias' section has a text input field with 'EC-site' and a warning message: 'Any saved change will restart all agents for this application'. The 'Application server' section has a text input field for 'Apdex T' with the value '0.5' and a warning message: 'Enter a decimal or whole number only.' The 'Apdex T' input field is highlighted with a blue box.

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 ①

0.5

Enter a decimal or whole number only.

① 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!!!

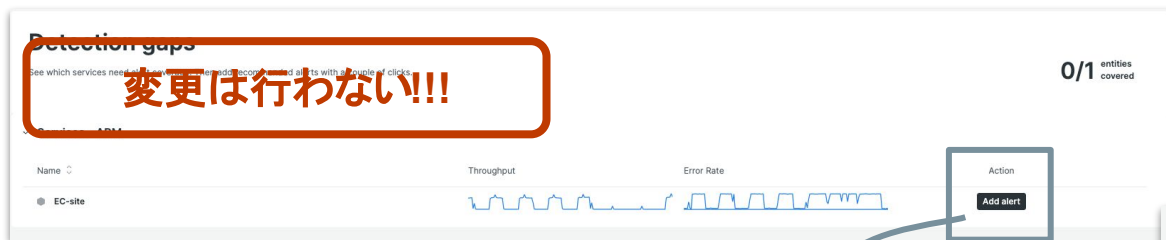
詳細については、後ほどご説明します。

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



- 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



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 - Apdex

Threshold type: Baseline

Alert when this signal deviates from its normal baseline, upper and lower, for at least 5 minutes by 3.00 standard deviation(s).

☐ **Critical** EC-site - Response Time (Web)

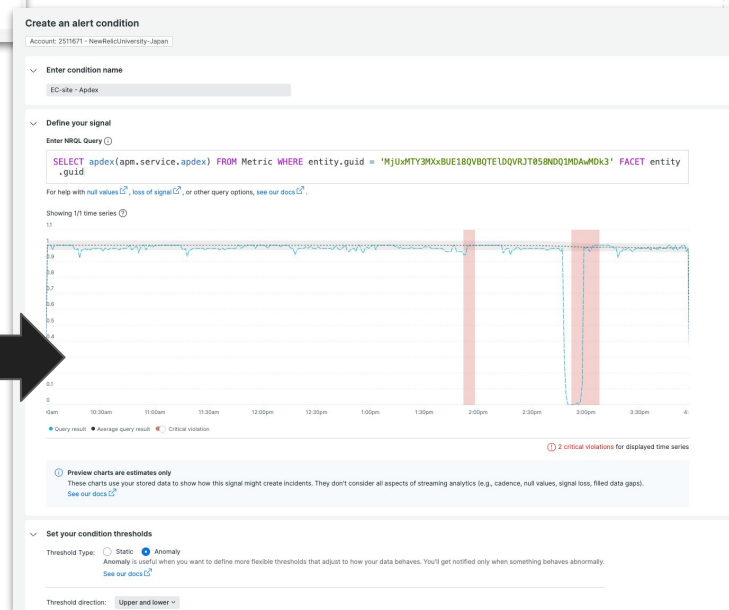
Threshold type: Baseline

Alert when this signal deviates from its normal baseline, upper and lower, for at least 5 minutes by 3.00 standard deviation(s).

Select policy to get notified

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

Next



ハンズオン(1) アラートを作成する

15:40 - 16:00 (20min)

Presenter Name

Title



今回の環境の監視構成

[前提]

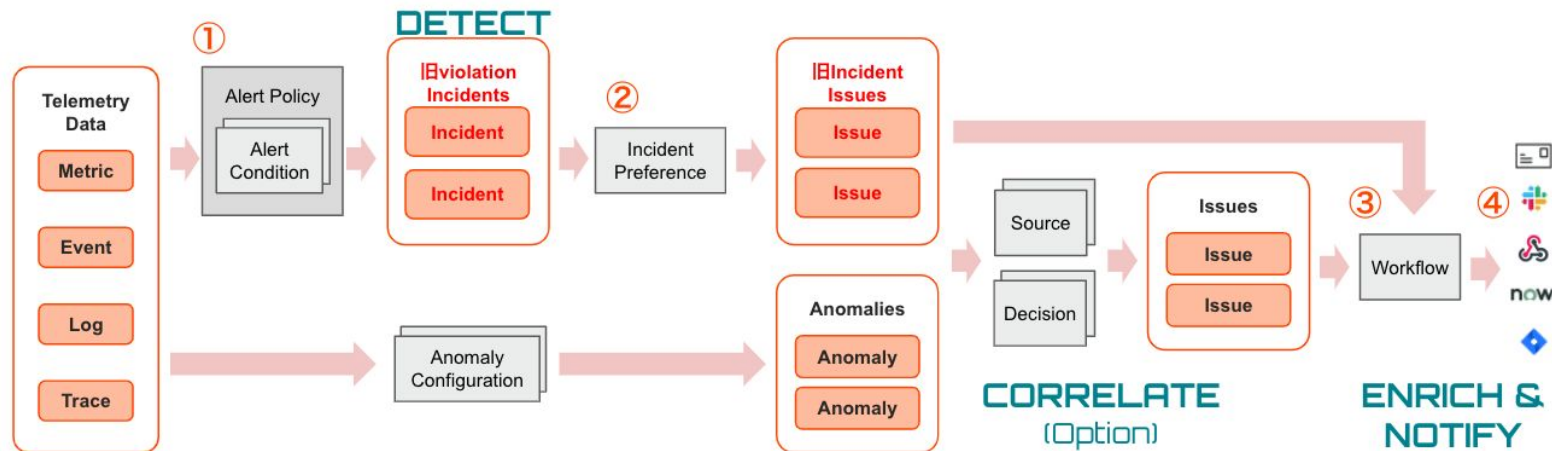
今回は赤字のアラートを設定してみます。

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

ハンズオン(1)アラートを作成する

作業内容

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





手順・解説

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

ハンズオン(1)-1 Alert policyを作成する 1/4

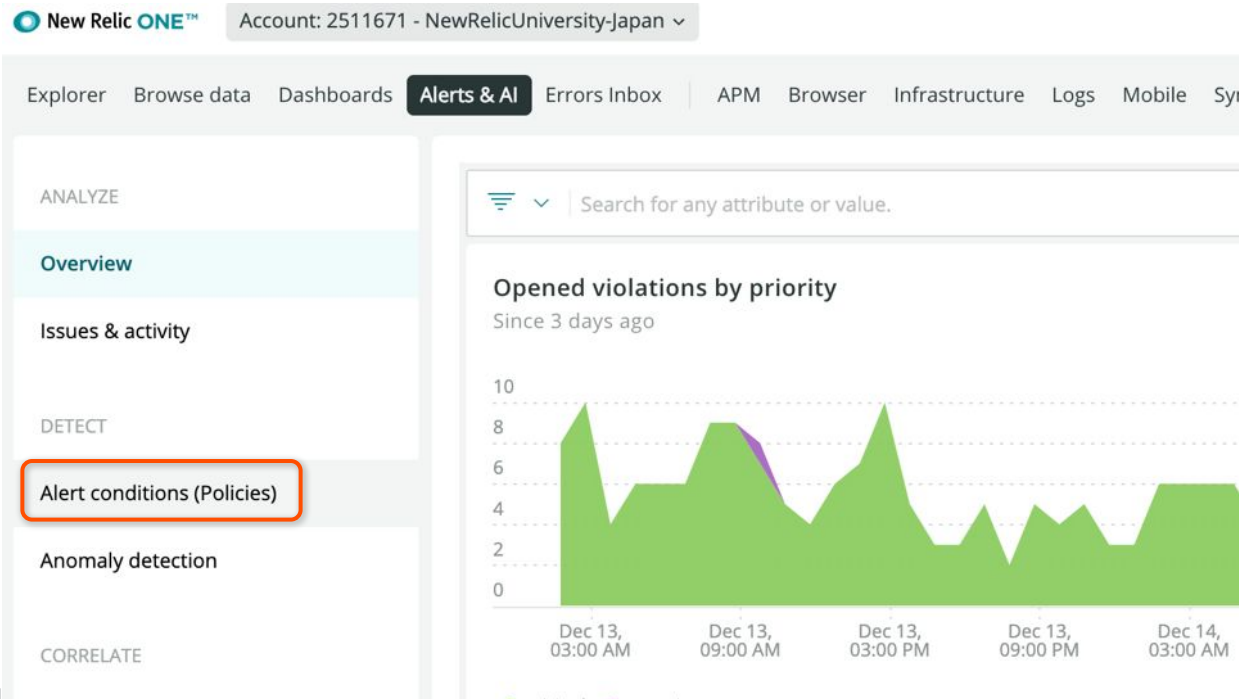
- Alert & AI メニューを開きます。

The screenshot shows the New Relic ONE web interface. The top navigation bar includes 'New Relic ONE™', 'All accounts', and links for 'Query your data', 'Apps', 'Quick start', and a progress indicator at 83%. Below this, a secondary navigation bar contains various tool categories: 'Home', 'Explorer', 'Browse data', 'Dashboards', 'Alerts & AI' (highlighted with a red box), 'APM', 'Browser', 'Infrastructure', 'Logs', 'Mobile', 'Synthetics', and 'More'. To the right of these are 'Share', 'Create a workload', and 'Add more data' buttons. A filter bar shows 'entityType = Service' and 'Add more filters'. On the left, a 'YOUR SYSTEM' sidebar lists entity counts: 'All entities (318)', 'APM/Services (5)' (highlighted), 'Hosts (2)', 'Containers (3)', 'Mobile applications (0)', 'Browser applications (3)', and 'Synthetic monitors (8)'. The main area displays a table of system entities with columns for Name, Account, End User, Page View, Response, Throughput, and Error Rate. The table lists five entities: EC-site, New Relic Pet Clinic, FoodMe, test-001, and ap-001. On the right, an 'Activity stream' panel shows two warning violations: 'Warning violation closed' at 10:31 am and 'Warning violation opened' at 10:29 am, both related to 'EC-site' and 'HttpDispatcher requests_per_minute'.

Name	Account	End User	Page Vi...	Respon...	Throug...	Error Ra...
☆ EC-site	NewRelic...	312.818 ms	11 page/s	79.409 ms	3 req/min	0 %
☆ New Relic Pet Clinic	New Relic ...	488.935 ms	1.74 page/s	17.314 ms	575 req/min	0 %
☆ FoodMe	New Relic ...	1083.486 ms	94 page/s	10.001 ms	851 req/min	0 %
☆ test-001	NewRelic...	-	-	0 s	0 req/min	0 %
☆ ap-001	NewRelic...	-	-	-	-	-

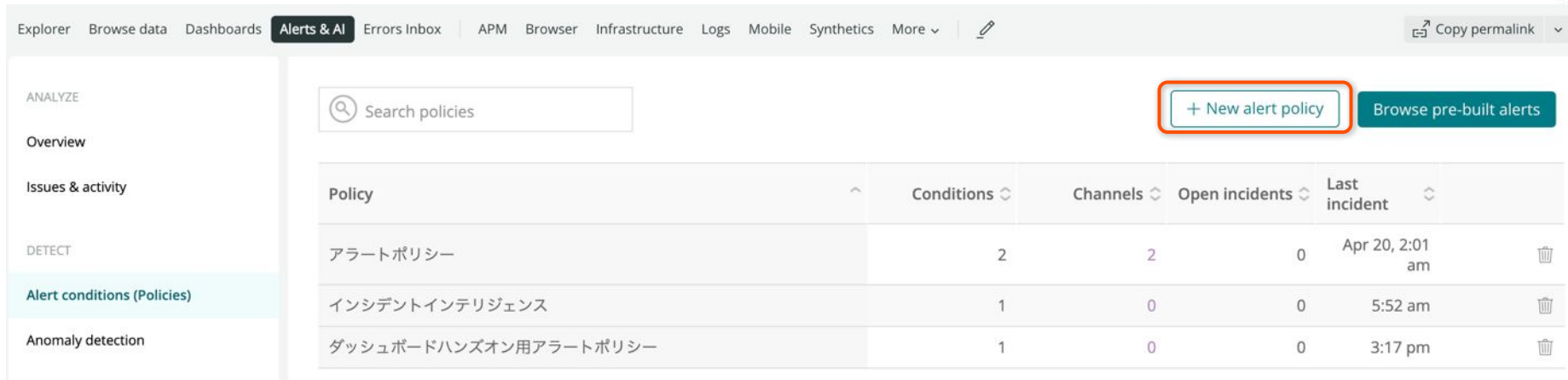
ハンズオン(1)-1 Alert policyを作成する 2/4

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



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 New Relic Alerts & AI interface. The top navigation bar includes 'Explorer', 'Browse data', 'Dashboards', 'Alerts & AI' (selected), 'Errors Inbox', 'APM', 'Browser', 'Infrastructure', 'Logs', 'Mobile', 'Synthetics', and 'More'. A 'Copy permalink' button is on the right. The left sidebar has sections for 'ANALYZE' (Overview, Issues & activity) and 'DETECT' (Alert conditions (Policies), Anomaly detection). The 'Alert conditions (Policies)' section is active, displaying a table of existing policies. A search bar 'Search policies' is at the top of the table. A '+ New alert policy' button is highlighted with a red box, and a 'Browse pre-built alerts' button is next to it.

Policy	Conditions	Channels	Open incidents	Last incident	
アラートポリシー	2	2	0	Apr 20, 2:01 am	
インシデントインテリジェンス	1	0	0	5:52 am	
ダッシュボードハンズオン用アラートポリシー	1	0	0	3:17 pm	

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 Create alert policy

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ため、ここではAlert policyのみを作成します

ALERT POLICY NAME

Give your policy a concise and descriptive name.

① nru-test-policy

ISSUE CREATION PREFERENCE

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

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

②

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

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

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

See our docs

③

Cancel Create policy without notifications Set up notifications

ハンズオン(1)-2 Alert Conditionを作成する 1/18

[前提]

今回は赤字のアラートを設定してみます。

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

ハンズオン(1)-2 Alert Conditionを作成する 2/18

- 新規Alert Conditionの追加

4つのアラートを順番に設定していきます

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

ハンズオン(1)-2 Alert Conditionを作成する 3/18

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

The screenshot shows the New Relic ONE interface for the 'Alerts & AI' section. The left sidebar contains a navigation menu with items like Overview, ALERTS, Incidents, Events, Policies (highlighted), Notification channels, Muting rules, PROACTIVE DETECTION, Settings, INCIDENT INTELLIGENCE, Decisions, and Sources. The main content area displays the details for a policy named '参加者名 アラートポリシー' (Participant Name Alert Policy) with ID 1314626. It shows '0 Alert conditions' (highlighted with a red box), '0 Notification channels', and a link to 'Add a notification channel to receive alerts'. A large gear icon is centered below the text 'This policy doesn't have any conditions'. Below this, it explains that alert conditions are criteria for creating incidents and that notifications are sent when incidents are created. A 'Create a condition' button (highlighted with a red box) is at the bottom right of the main content area.

New Relic ONE Account: 2511671 - NewRelicUniversity-Japan

Home Explorer Browse data Dashboards **Alerts & AI** APM Browser Infrastructure Logs Mobile Synthetics More

Overview

ALERTS

Incidents

Events

Policies

Notification channels

Muting rules

PROACTIVE DETECTION

Settings

INCIDENT INTELLIGENCE

Decisions

Sources

参加者名 アラートポリシー

id: 1314626

0 Alert conditions

0 Notification channels

Add a notification channel to receive alerts

This policy doesn't have any conditions

Alert conditions are the criteria for creating incidents.

Notifications are sent when incidents are created.

Create a condition

ハンズオン(1)-2 Alert Conditionを作成する 4/18

- 外形監視:チェックエラー
- 監視設定は次のようにしてください。

1. Categories

- a. Synthetics -> Single failure

2. Select a monitor

- a. EC-CUBE-Checkout

ハンズオン(1)-2 Alert Conditionを作成する 5/18

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

New condition

ⓧ Cancel

1. Categorize

Select a product

NRQL

APM

Browser

Mobile

Plugins

Synthetics

Infrastructure

Select a type of condition

Single failure

Multiple location failures

Next, select entities

ハンズオン(1)-2 Alert Conditionを作成する 6/18

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

2. Select a monitor

Search monitors

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

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

< Back to Name and Categorize

Next, define thresholds

ハンズオン(1)-2 Alert Conditionを作成する 7/18

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

New condition

ⓧ Cancel

1. Categorize

Synthetics - Single failure

2. Select monitor

1 monitor

3. Define thresholds

A violation occurs whenever a monitor fails a check

Name this condition

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

☐ 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

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

Monitor check failure

Add a condition

ハンズオン(1)-2 Alert Conditionを作成する 9/18

- 新規Alert Conditionの追加

②フロントエンド: Apdex(静的)

1. **Categories:**

- a. Browser -> Metric

2. **Select entities:**

- a. EC-site

3. **Define thresholds**

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

Condition名は適切なものを各自設定してください

ハンズオン(1)-2 Alert Conditionを作成する 10/18

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

参加者名 アラートポリシー

☐ Connect to Incident Intelligence

Incident preference: By policy

Delete this policy

id: 1314626

1 Alert condition

0 Notification channels

① Add a notification channel to receive alerts

Last modified 7:37 am by NRU-User

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

Monitor check failure

+ Add a condition

ハンズオン(1)-2 Alert Conditionを作成する 11/18

- Categories を設定します。

New condition

⊗ Cancel

1. Categorize

Select a product

NRQL APM **Browser** Mobile Plugins Synthetics Infrastructure

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

Select a type of condition

Metric Metric baseline

Next, select entities

ハンズオン(1)-2 Alert Conditionを作成する 12/18

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

2. 1 entity selected

 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 Apex 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 Apex (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。

2 Alert conditions

0 Notification channels

Add a notification channel to receive alerts

Last modified 7:37 am by NRU-User

Search conditions

Add a condition

APM BROWSER APPLICATION METRIC 名前を追記 End User Apdex (Low)

Last modified 8:28 am by NRU-User

Edit

Copy

Delete

On

EC-site Add entities

End User Apdex < 0.7 at least once in 5 mins

Add a warning threshold

SYNTHETICS MONITOR FAILURE わかりやすい通知名

Last modified 8:05 am by NRU-User

Edit

Copy

Delete

On

EC-CUBE-Checkout

Monitor check failure

ハンズオン(1)-2 Alert Conditionを作成する 15/18

- **新規Alert Conditionの追加**

- ③アプリケーション: 応答時間(動的)

1. **Categories**

- a. APM -> Application metric baseline

2. **Select entities**

- a. EC-site

3. **Define thresholds**

- a. 次ページ参照

Condition名は適切なものを各自設定してください

ハンズオン(1)-2 Alert Conditionを作成する 16/18

- ベースラインアラートではスライダーで感度が変わります。

3. Define thresholds

Baseline Direction: New Upper only

When any target application Web transaction time

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

more violations

fewer violations

⚠ + Add a warning threshold

Condition Name

Web transaction time (Baseline)

+ Add runbook URL

EC-site

× 2 critical violations

Last 2 days

2.5 k
2 k
1.5 k
1 k
500
0
-500
-1 k

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

より敏感に

より鈍感に

< Back to Select entities

Create condition

ハンズオン(1)-2 Alert Conditionを作成する 17/18

- 新規Alert Conditionの追加

④アプリケーション: 4xx,5xxエラー(ホストごとに評価)

1. **Categories**

- a. NRQL

2. **Enter a NRQL query and thresholds**

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

3. **Define thresholds**

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

Condition名は適切なものを各自設定してください

ハンズオン(1)-2 Alert Conditionを作成する 18/18

- NRQLを入力すると自動的に参考となる Chartが表示されます。

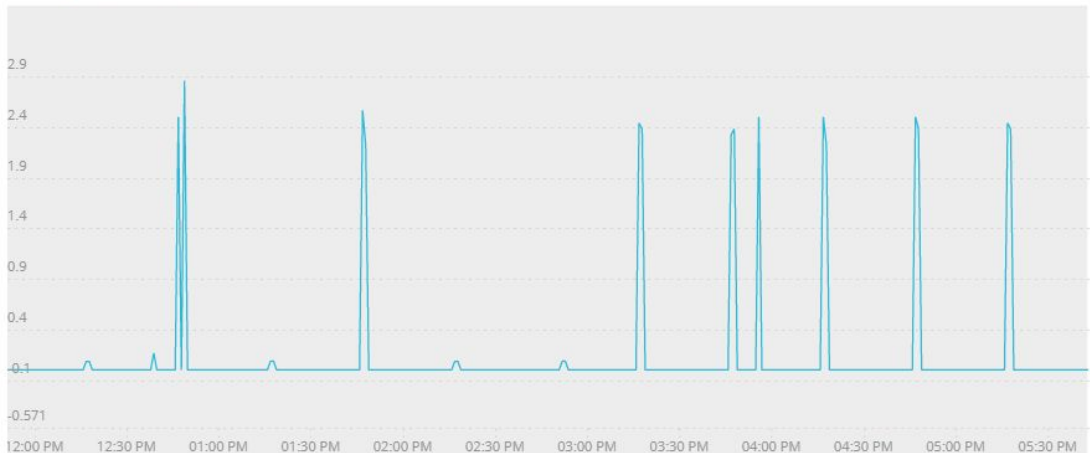
▼ Define your signal

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

What's possible with NRQL Alerting ▼

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

Showing 1/1 time series (?)



 Critical violation

ハンズオン(1)-3 Workflowsを作成する 1/6

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

次のスライドに進みます

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

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

2 Name
kaizawa-test-workflows

3 Select issues
☒ Build a query ☐ Send all issues

policyName exactly matches nru-test-policy x

+ AND

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

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

Enrich (optional)
+ Build a query

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

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

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

☒ kaizawa@newrelic.com

☐ ServiceNow incidents

☐ Webhook

☐ Jira

☐ Slack

☐ Email

☐ AWS EventBridge

☐ PagerDuty

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

☐ We found a possible problem above.

ハンズオン(1)-3 Workflowsを作成する 2/6

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

次のスライドに進みます

The screenshot shows the 'Notify' configuration screen in the New Relic workflow editor. At the top, there's a section 'Choose one or more destinations and add an optional message.' with a search bar containing 'katzawa@newrelic.com'. Below this are several destination tiles: 'ServiceNow incidents', 'Webhook', 'Jira', 'Slack', 'Email' (highlighted with a red circle 5), and 'AWS EventBridge'. Further down, there's a 'Test this workflow' section with a 'Test workflow' button (circled in red 9) and a message 'We found a possible problem above.' At the bottom right are 'Cancel' and 'Activate workflow' buttons (circled in red 10). An arrow points from the 'Email' tile to a detailed configuration panel below. This panel has a title 'Email' and a search bar 'Select users and emails you want to send notifications to. See our docs'. Below the search bar is a text field for 'Email subject' containing '{{ issueTitle }}' (circled in red 6). There's also a 'Custom Details (optional)' section. At the bottom of this panel is a 'Send test notification' button (circled in red 7). Another arrow points from the 'Test workflow' button in the top panel to the 'Send test notification' button in the bottom panel. At the very bottom right of the slide, the 'new relic.' logo is visible, with a red circle 8 near it.

ハンズオン(1)-3 Workflowsを作成する 3/6

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

8. Saveボタンを押します

次のスライドに進みます

The screenshot displays the New Relic workflow configuration interface. At the top, the 'Notify' section is active, showing a list of notification channels: ServiceNow incidents, Webhook, Jira, Slack, Email, AWS EventBridge, and PagerDuty. The 'Email' channel is selected. Below this, the 'Test this workflow' section is visible, with a 'Test workflow' button and a message: 'We'll use existing data from your account to test what you've configured and send a sample notification.' A 'Send test notification' button is located at the bottom left of the configuration area. A 'Save' button is at the bottom right. The interface includes various numbered callouts: ⑤ points to the email address field, ⑥ points to the 'Email' channel selection, ⑦ points to the 'Send test notification' button, ⑧ points to the 'Save' button, ⑨ points to the 'Test workflow' button, and ⑩ points to the 'Activate workflow' button. The 'Email' channel configuration details are shown in a separate panel below, including fields for 'Email subject' and 'Custom Details (optional)'.

ハンズオン(1)-3 Workflowsを作成する 4/6

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

The screenshot displays the New Relic workflow configuration interface. At the top, the 'Notify' step is configured with the email address 'katzawa@newrelic.com'. Below this, a grid of integration options is shown, including ServiceNow incidents, Webhook, Jira, Slack, Email, AWS EventBridge, and PagerDuty. The 'Email' option is selected. A red circle with the number 5 is placed over the 'Email' option. Below the grid, the 'Test this workflow' section is visible, with a red circle 9 over the 'Test workflow' button. A red circle 10 is over the 'Activate workflow' button. A red circle 6 is over the 'Email' step in the workflow list. A red circle 7 is over the 'Send test notification' button. A red circle 8 is over the 'Save' button. Arrows indicate the flow from the 'Test workflow' button to the 'Email' step and from the 'Activate workflow' button to the 'Save' button.

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

✉ katzawa@newrelic.com

ServiceNow incidents Webhook Jira
Slack Email AWS EventBridge
PagerDuty

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

Test workflow ⓘ We found a possible problem above.

Cancel Activate workflow

Email

Select users and emails you want to send notifications to. [See our docs](#)

Search by name or email

Email subject
{{ issueTitle }}

Custom Details (optional)
This payload uses Handlebars syntax "{{\$ }}" to select from a list of variables.

Send test notification

Cancel Save

ew relic.

ハンズオン(1)-3 Workflowsを作成する 5/6

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

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

Add a destination

Add destinations where we send notifications.



Jira

ServiceNow



Slack



Webhook



PagerDuty



AWS EventBridge



Mobile push

Notifications Log **Destinations (3)**

Manage destinations where we send notifications.



Search

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

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



NRU-User

japan-handson+2021@newrelic...

Aug 22, 2022...

1001038720



DEFAULT





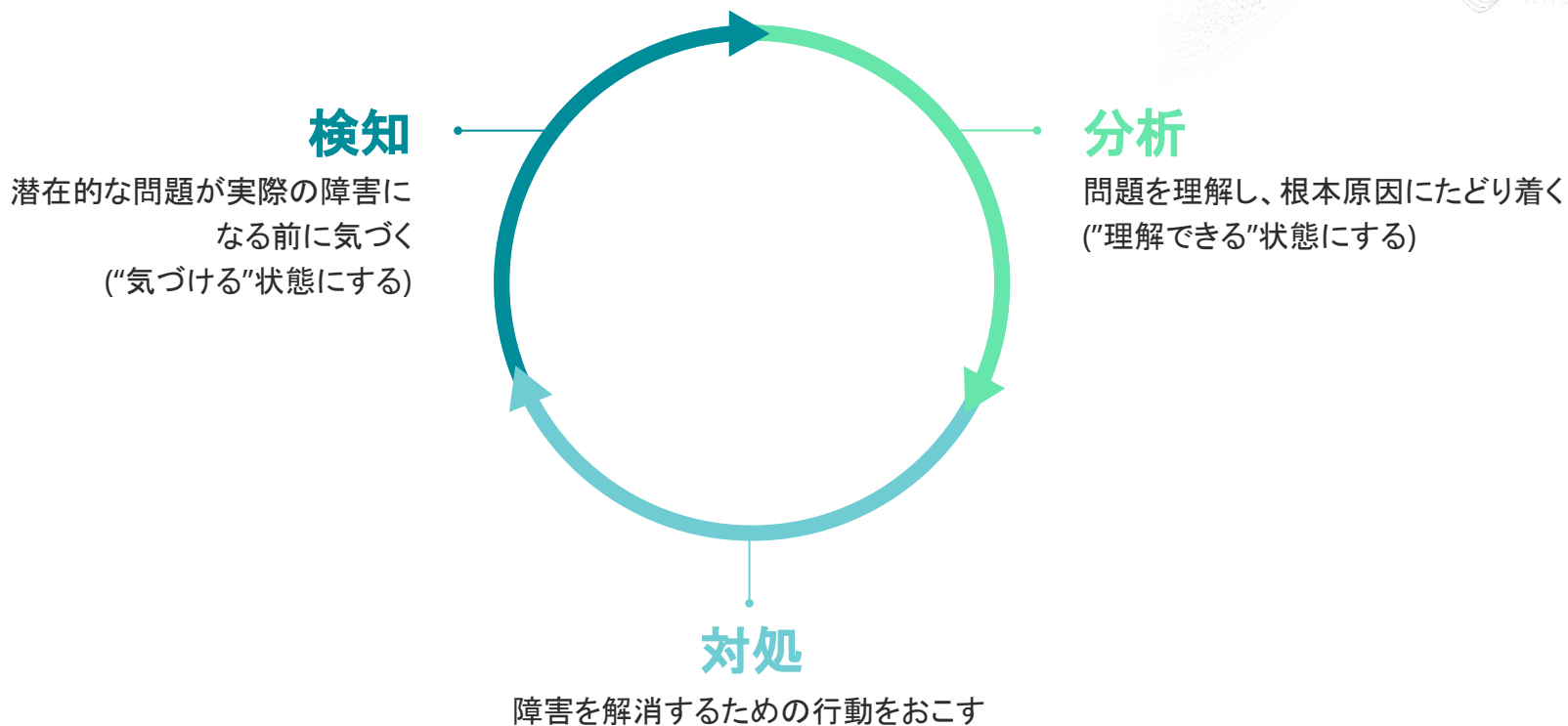
座学(3)

New RelicのAIOps機能

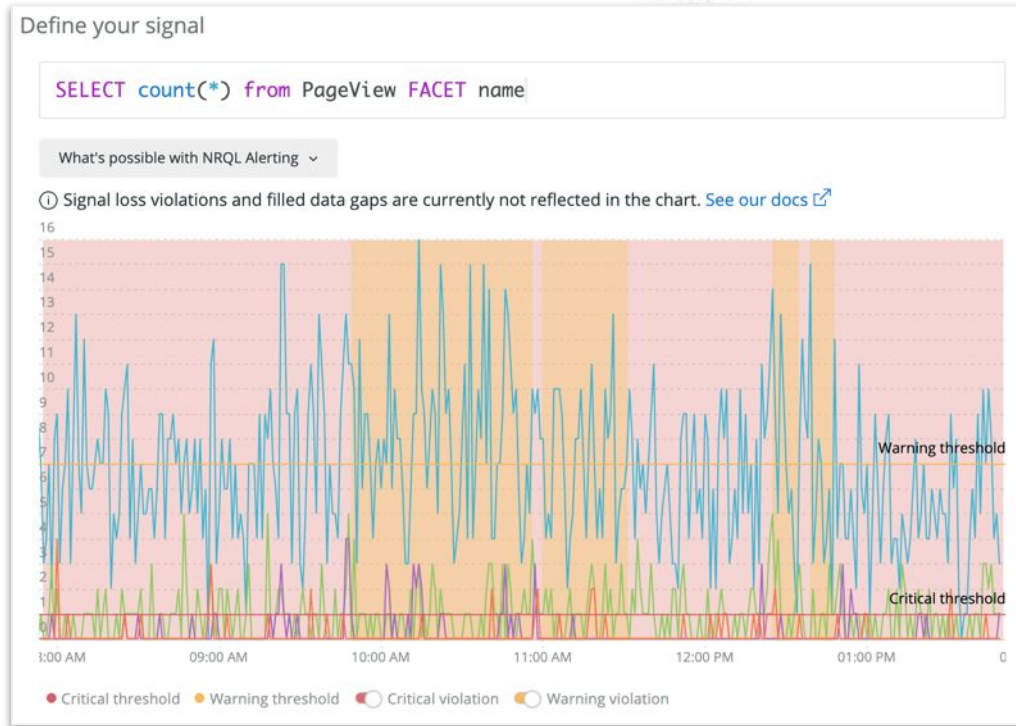
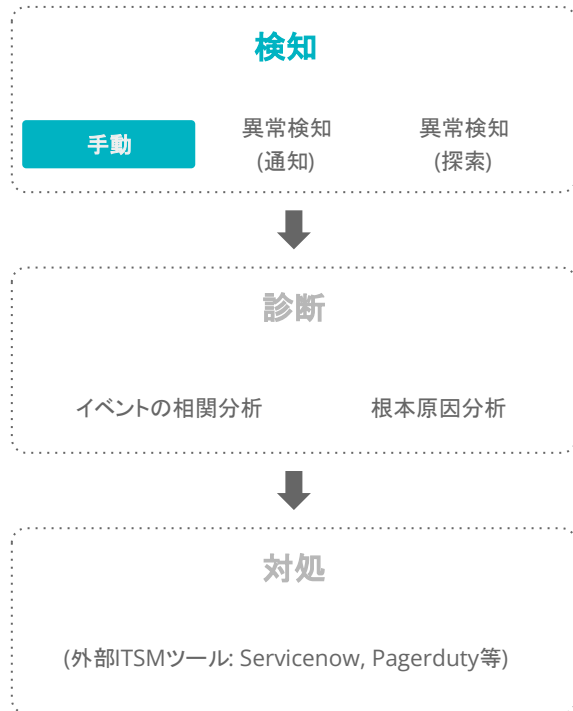
16:00 - 16:15 (15min)



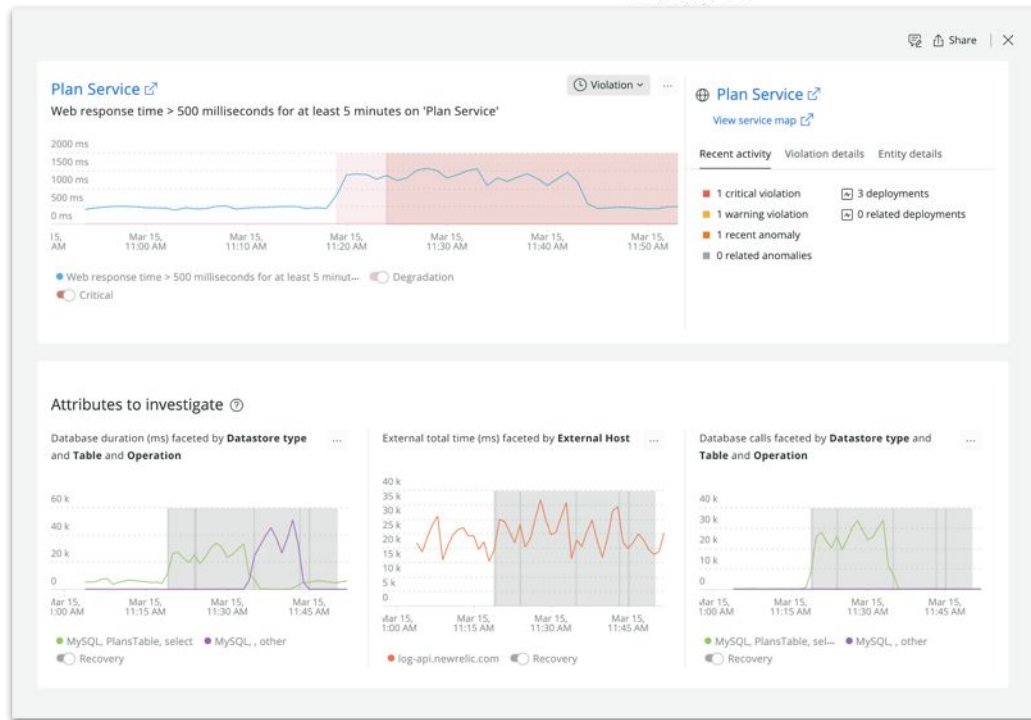
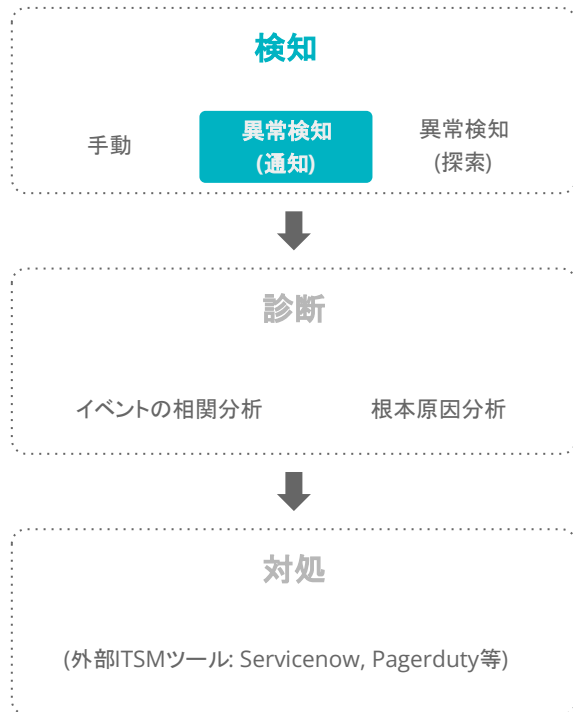
New Relic AIOpsによるインシデント対応フロー



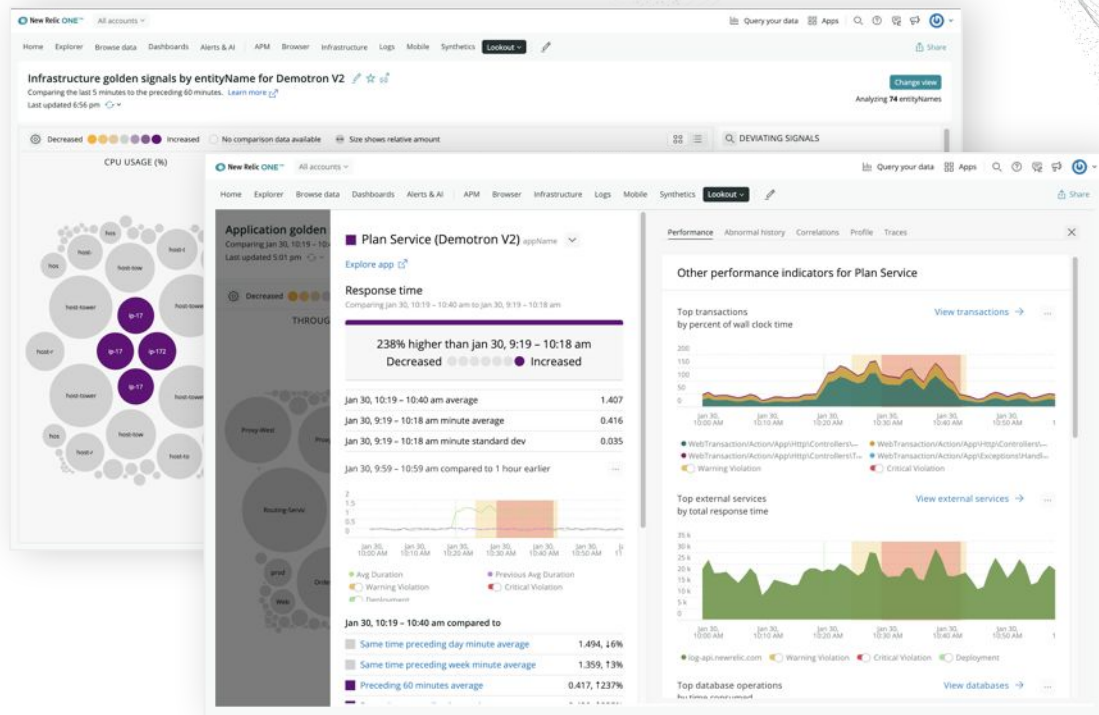
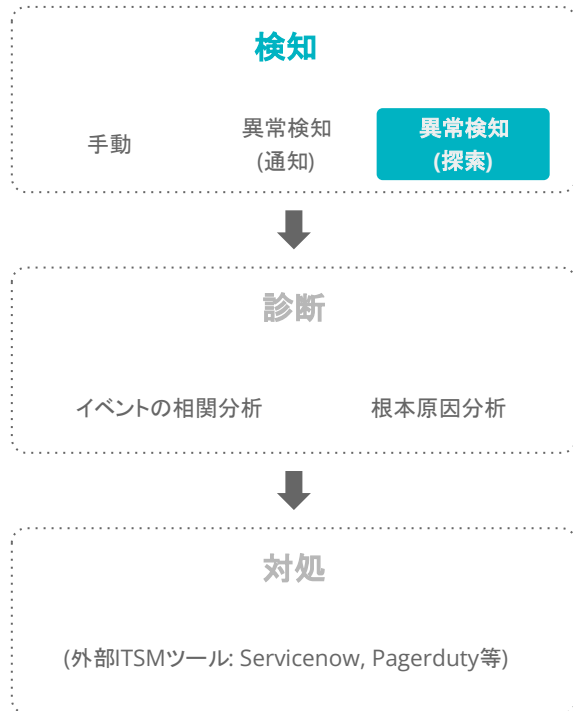
検知1: 重要な指標に対する手動アラートによる気づき



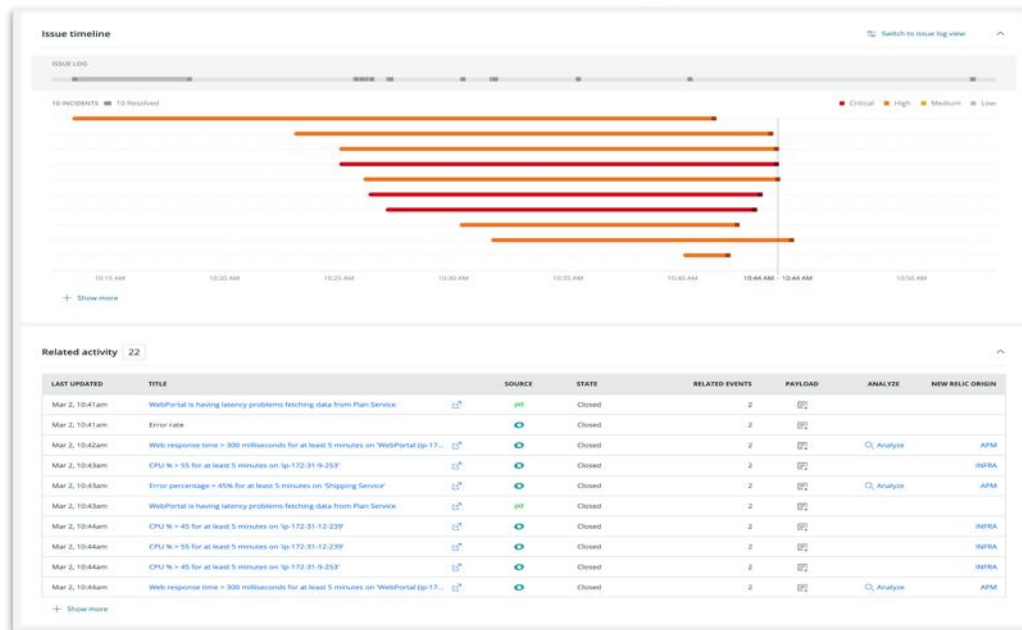
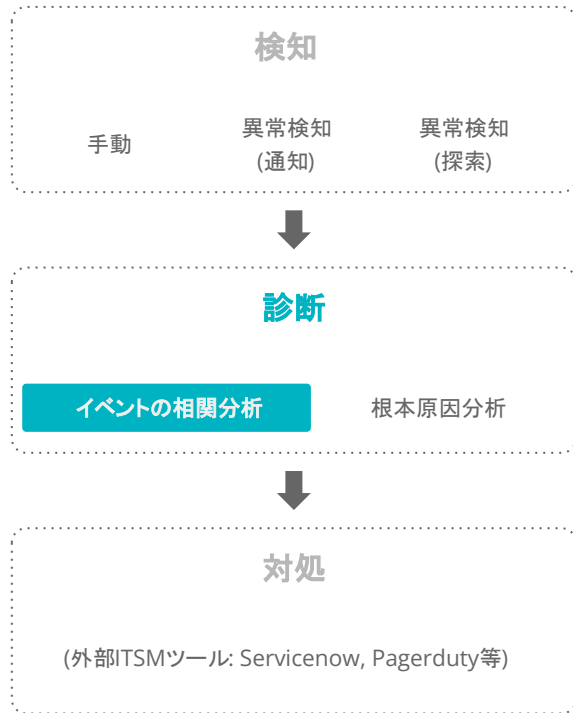
検知2: Proactive Detectionによる異常の通知



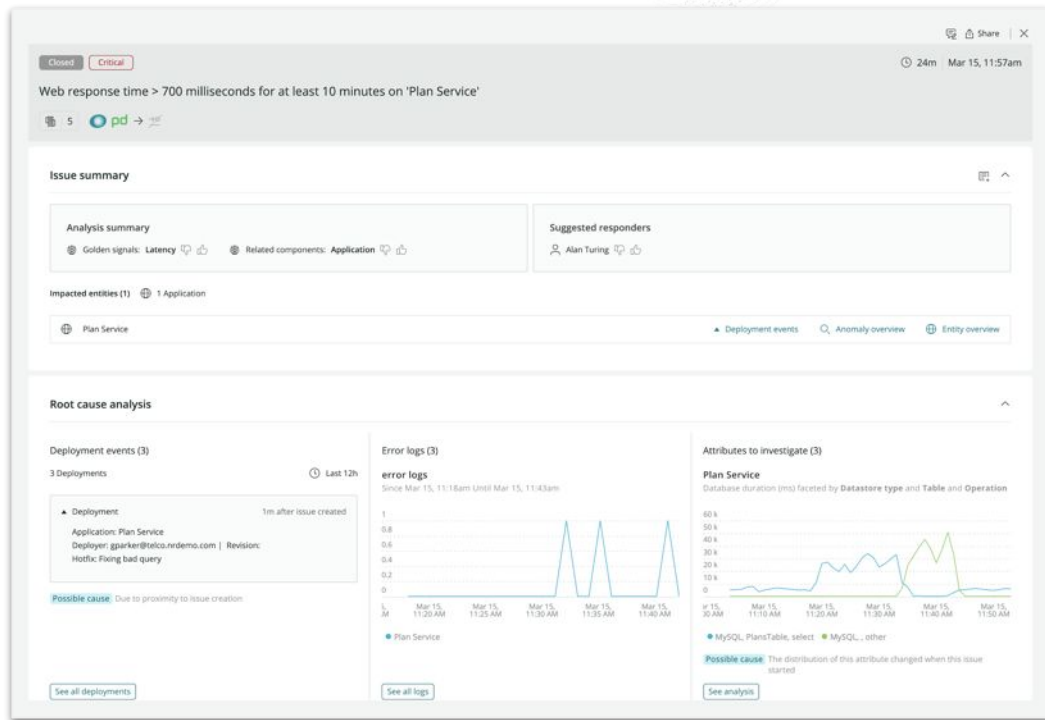
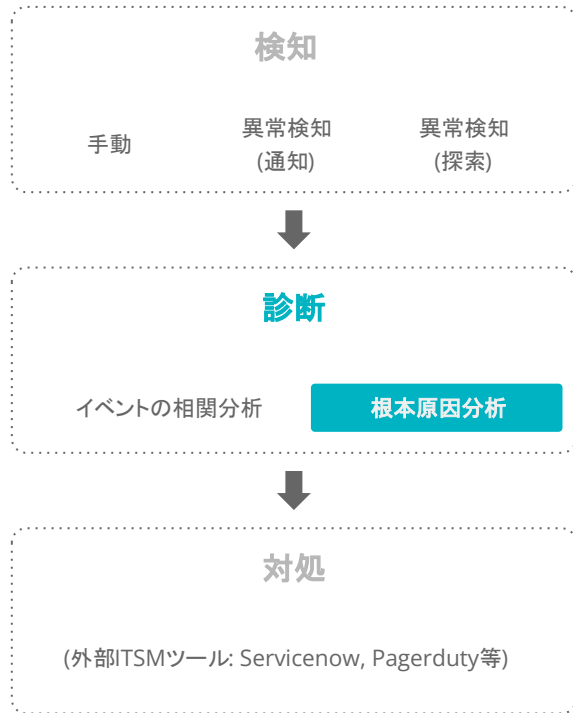
検知3: Lookoutによる異常の可視化と探索



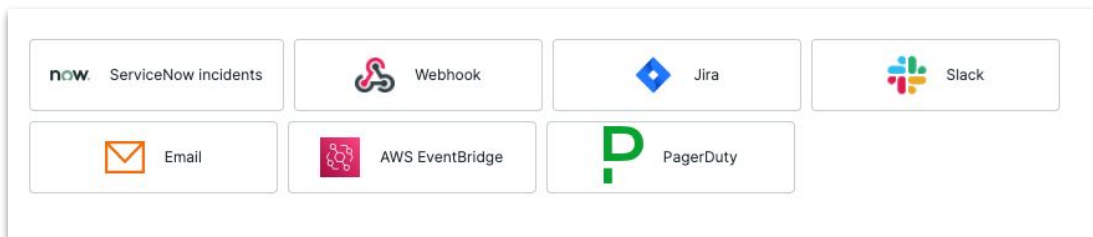
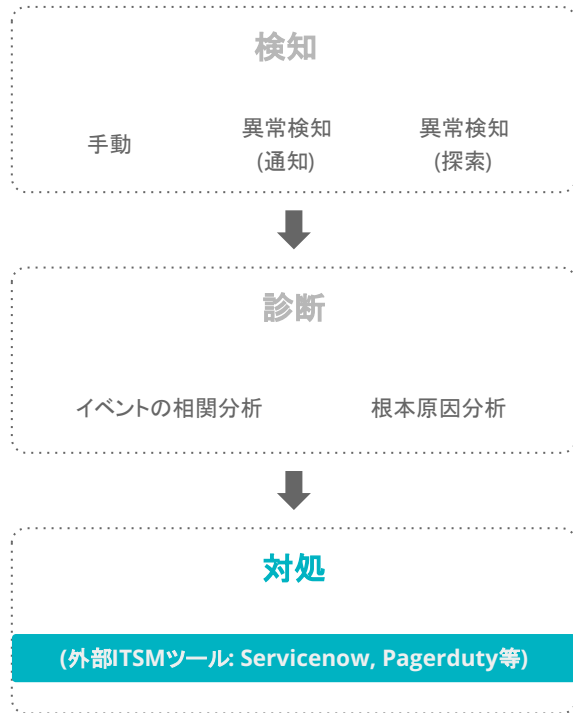
診断1: Correlationによるアラート統合とノイズの削減



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

Presenter Name

16:15 - 16:30 (15min)

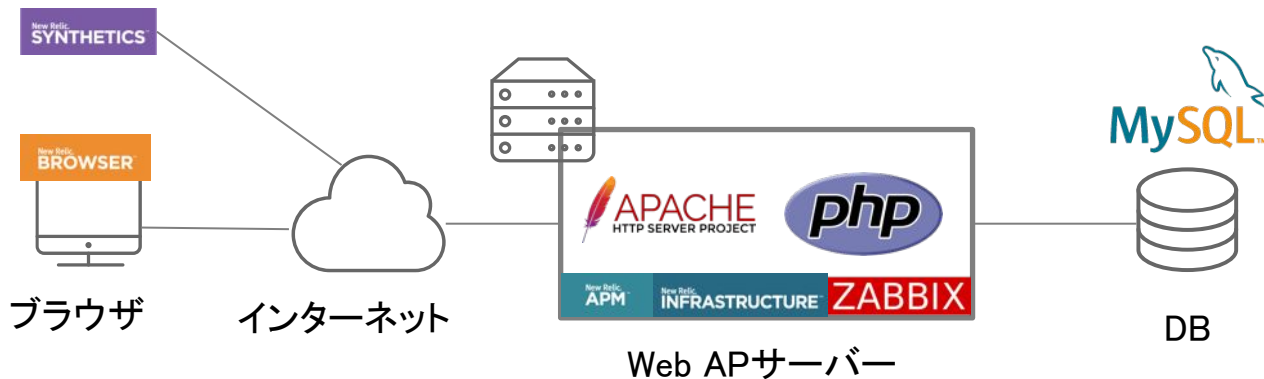
Title

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



今回の環境の監視構成(再掲)

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



ハンズオン(2)

1. 異常を可視化する

[目的]

AIOpsの異常検知の仕組みを使い、異常を可視化する機能を学びましょう

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

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

ハンズオン(2)

2. 個々のアラートを確認する

[目的]

AIOpsに送られたアラートを把握します(後続の演習の事前確認)

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

ハンズオン(2)

AIOps:イベントの相関分析

AIOps:根本原因分析

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

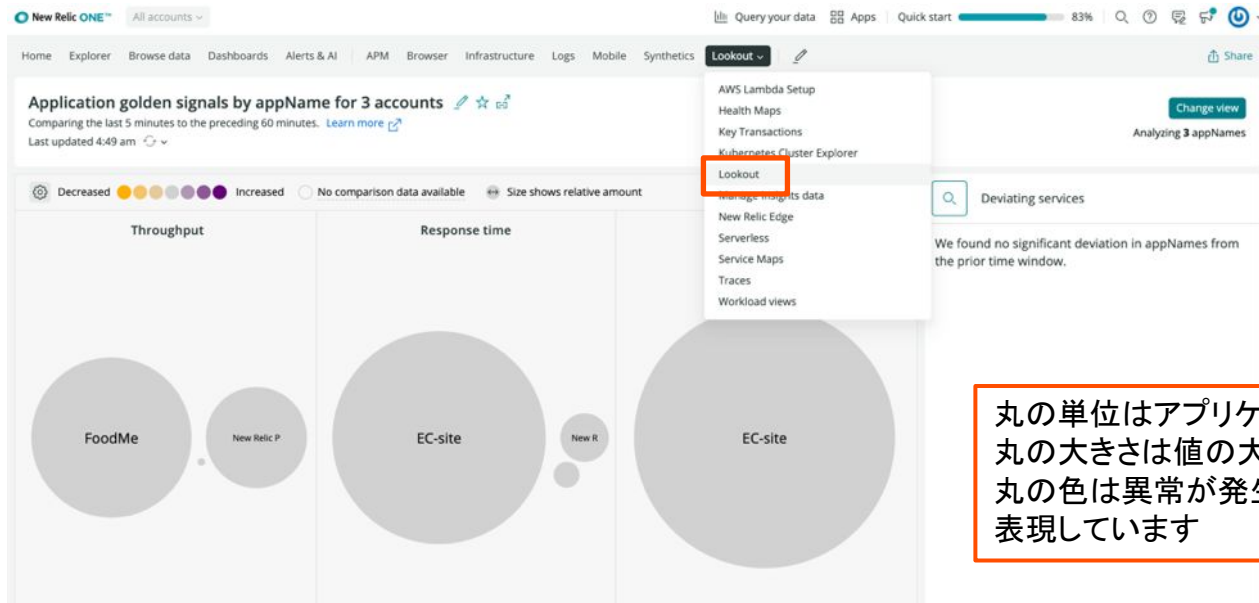


手順・解説

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

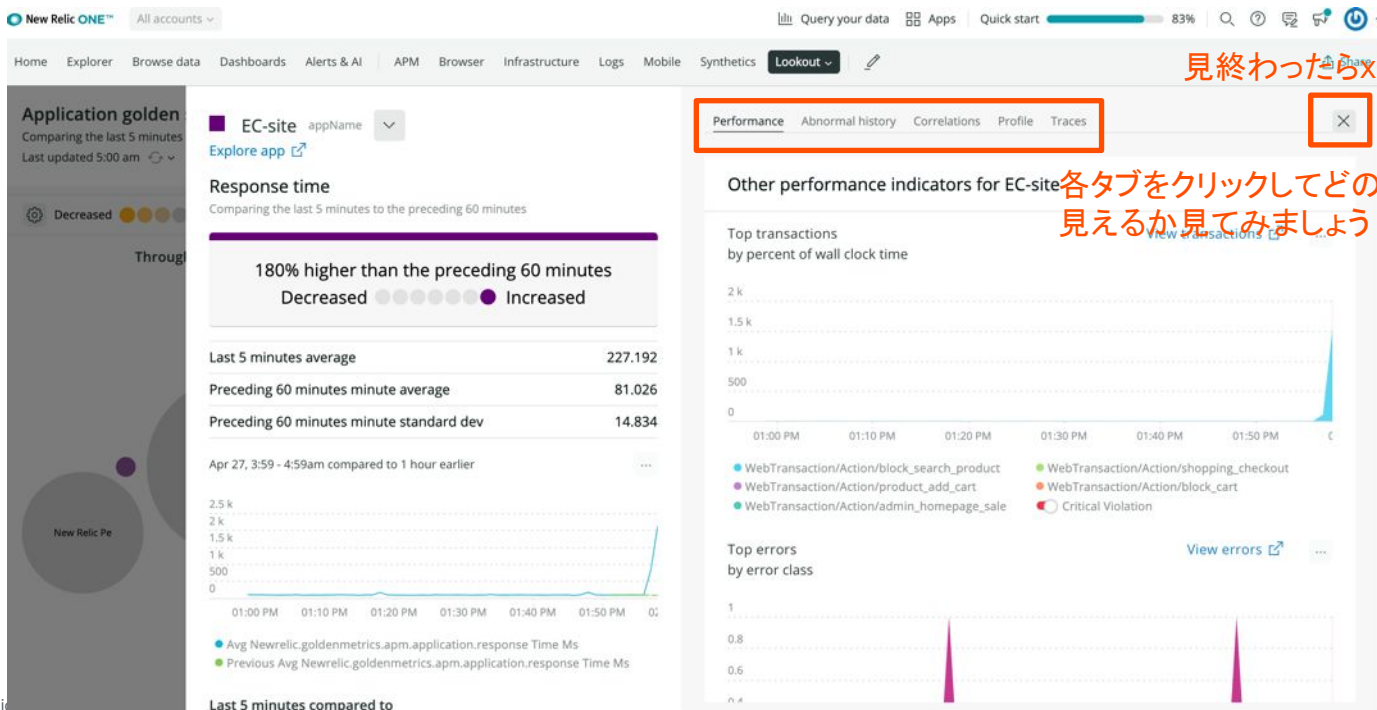
- Original New Relic Account側にログインします(詳細手順は [こちら](#))
- トップメニューの「More」->「Lookout」をクリックし、現れた画面上でサービスの現状を読み解きましょう



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



見終わったらxを押して閉じます

各タブをクリックしてどのような情報が見えるか見てみましょう

ハンズオン(2)異常を可視化する

- カスタムのビューを作成します

Manage Views -> Create a new queryを選択

The screenshot displays the New Relic ONE dashboard. The top navigation bar includes links for 'Query your data', 'Instant Observability', 'Apps', 'Get started', and a search icon. Below this, a secondary bar shows 'Explorer', 'Browse data', 'Dashboards', 'Alerts & AI', 'Errors Inbox', 'APM', 'Browser', 'Infrastructure', 'Logs', 'Mobile', 'Synthetics', and a 'Lookout' button. The main content area is titled 'Application golden signals by appName for 3 accounts'. It features filters for 'Select account' (All accessible accounts), 'View data from' (Last 5 minutes), and 'Compare data to' (Preceding 60 minutes). An 'Auto Refresh' toggle is set to 'Off'. The dashboard displays two charts: 'Throughput' and 'Response time'. The 'Throughput' chart shows data for 'EC-site' and 'FoodMe'. The 'Response time' chart shows data for 'EC-site'. A 'Deviating services' panel on the right indicates 'We found no significant deviation 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), 'Revert changes', 'Save view', and 'Save view as...'. The 'Create a new query' option is the target of the instruction in the text above.

New Relic ONE™

Query your data Instant Observability Apps Get started

Explorer Browse data Dashboards Alerts & AI Errors Inbox APM Browser Infrastructure Logs Mobile Synthetics Lookout

Copy permalink

Application golden signals by appName for 3 accounts

Select account View data from Compare data to Auto Refresh

All accessible accounts Last 5 minutes Preceding 60 minutes Last updated 3:18 am

Decreased Increased Size shows relative amount Add to dashboard

Throughput Response time

EC-site FoodMe EC-site

Deviating services

We found no significant deviation the prior time window.

Manage Views

Open a saved view

Edit current query

Create a new query

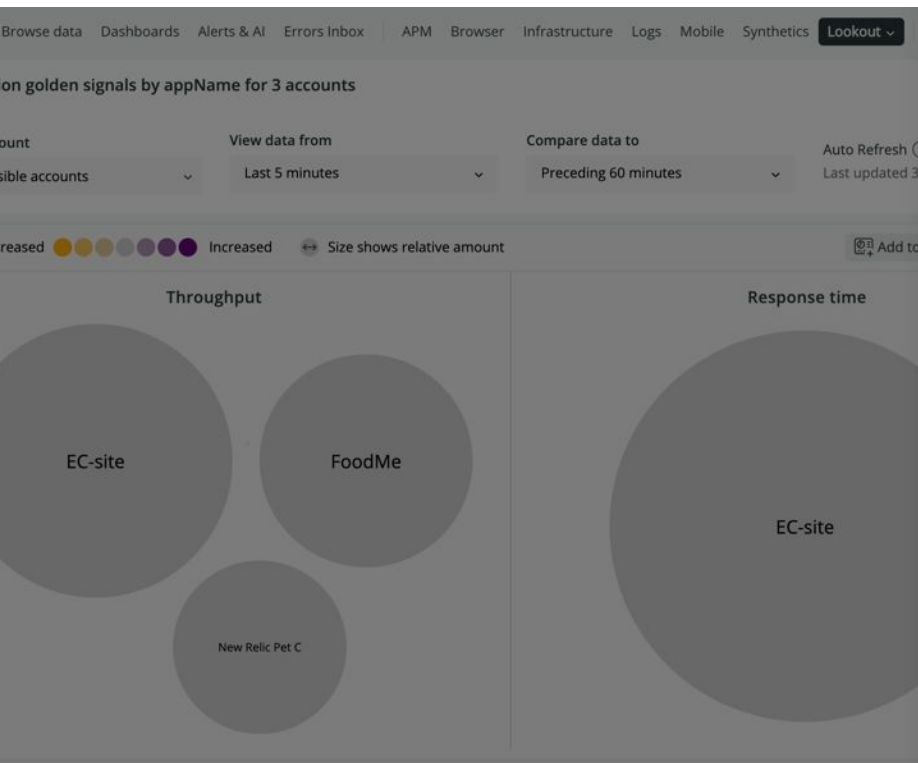
Revert changes

Save view

Save view as...

ハンズオン(2)異常を可視化する

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



Create a new query

Select account

All accessible accounts

Select data type

Metrics

Events

①Eventsを選択

Or write a NRQL query

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

View a chart with

Transaction : count

Transaction : average : duration

+ Add row

Facet by

request.uri

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

④request.uriを選択

View data from

Last 5 minutes

Compare data to

Preceding 60 minutes

Name your view (optional)

csasaki

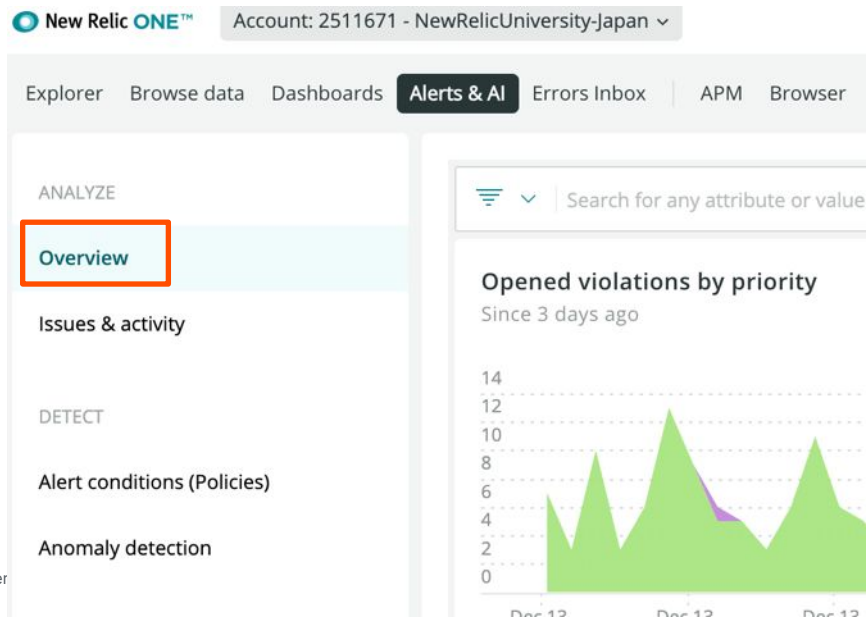
⑤ご自身の名前を入力

⑥Create New Viewを押す

Create New View

ハンズオン(2)個々のアラートを確認する

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



ハンズオン(2)個々のアラートを確認する

- 「Incidents」タブをクリックします。

The screenshot shows the New Relic ONE interface. The top navigation bar includes 'Query your data', 'Instant Observability', 'Apps', 'Get started', and search icons. The left sidebar has 'ANALYZE' as the main section, with 'Overview' and 'Issues & activity' (highlighted) as sub-sections. The main content area shows the 'Incidents' tab selected, with a bar chart and a table of incidents. The 'Incidents' tab is highlighted with a red box.

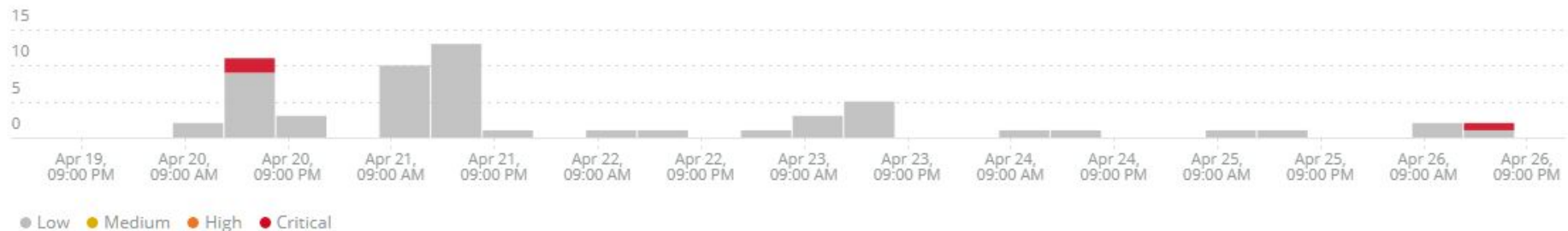
Associated account: NewRelicUniversity-Japan ?

Legend: ● Low ● Medium ● High ● Critical

STATE	PRIORITY	INCIDENT NAME	CREATED	DURATION	ENTITIES	ANALYSIS SUMMARY	SOURCE	EVENTS
☐	Closed	Critical	Monitor failed for location...	12m ago	5m	Signal: Error		2
☐	Open	Critical	Web response time deviated...	16m ago	16m	Signal: Latency Components: ...		1

ハンズオン(2)個々のアラートを確認する

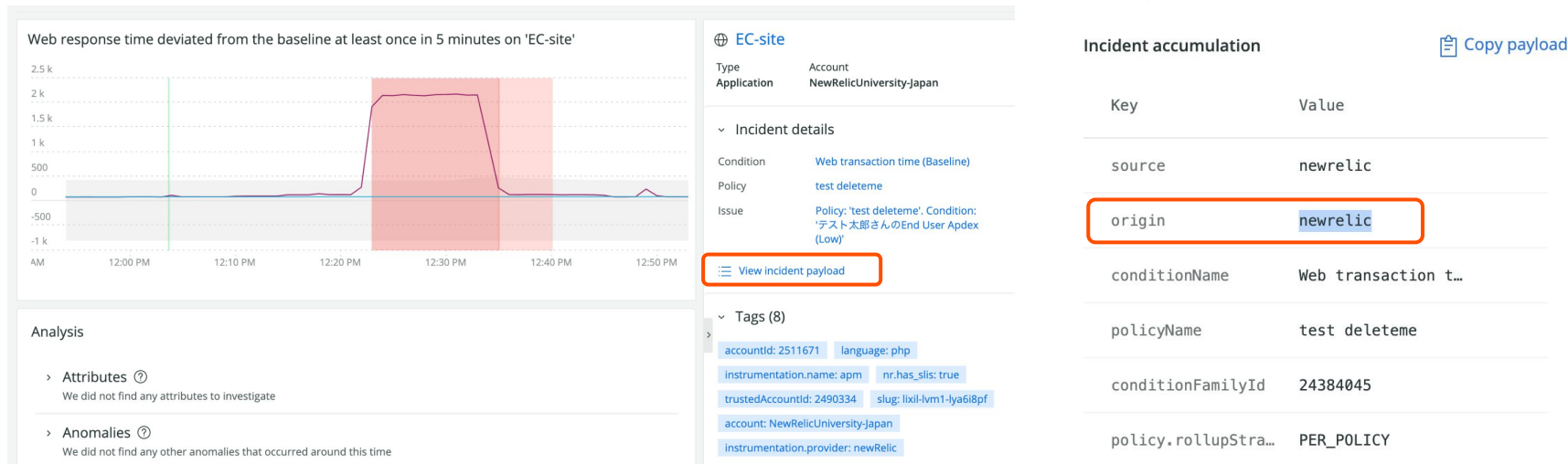
- 個々のIncidentをクリックします。



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

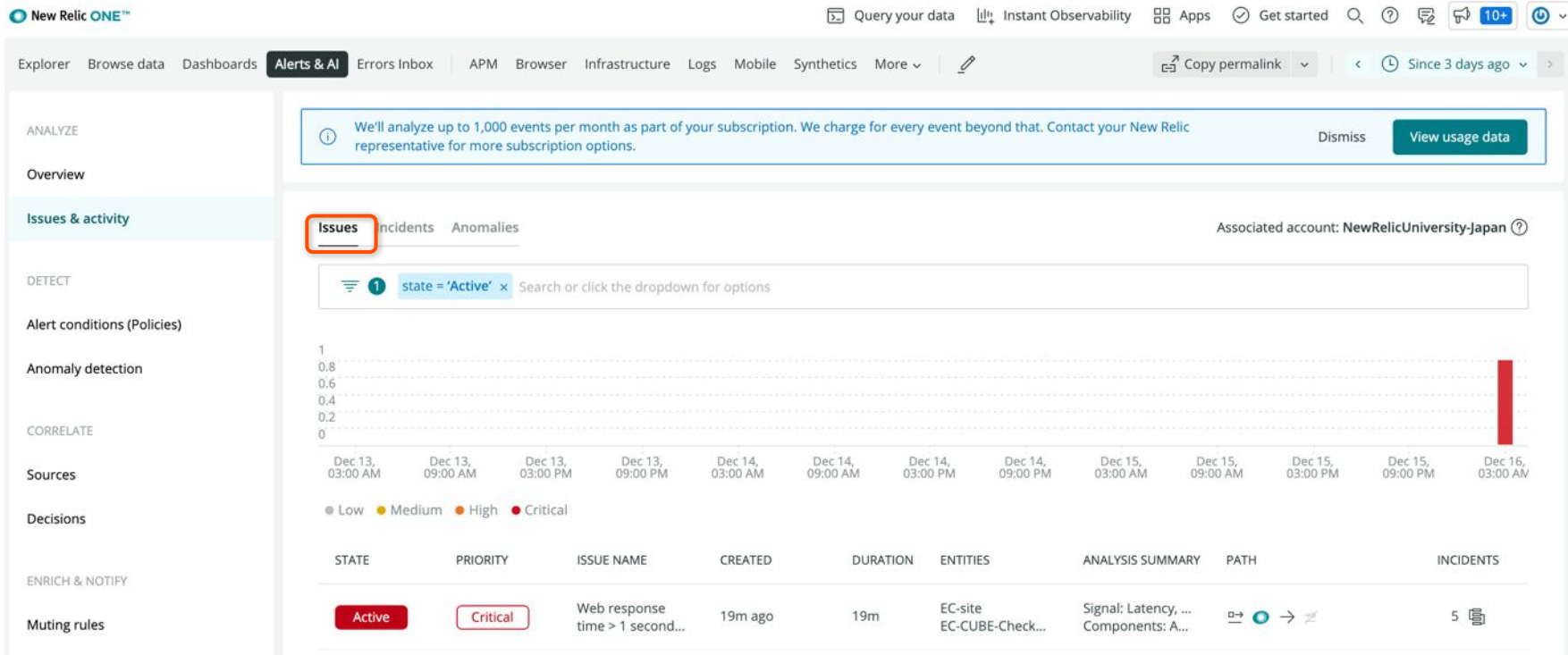
ハンズオン(2)個々のアラートを確認する

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



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。



New Relic ONE™

Query your data Instant Observability Apps Get started 10+

Explorer Browse data Dashboards Alerts & AI Errors Inbox APM Browser Infrastructure Logs Mobile Synthetics More

Copy permalink Since 3 days ago

ANALYZE

Overview

Issues & activity

DETECT

Alert conditions (Policies)

Anomaly detection

CORRELATE

Sources

Decisions

ENRICH & NOTIFY

Muting rules

We'll analyze up to 1,000 events per month as part of your subscription. We charge for every event beyond that. Contact your New Relic representative for more subscription options. Dismiss View usage data

Issues incidents Anomalies Associated account: NewRelicUniversity-Japan ?

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

1 0.8 0.6 0.4 0.2 0

Dec 13, 03:00 AM Dec 13, 09:00 AM Dec 13, 03:00 PM Dec 13, 09:00 PM Dec 14, 03:00 AM Dec 14, 09:00 AM Dec 14, 03:00 PM Dec 14, 09:00 PM Dec 15, 03:00 AM Dec 15, 09:00 AM Dec 15, 03:00 PM Dec 15, 09:00 PM Dec 16, 03:00 AM

Low Medium High Critical

STATE	PRIORITY	ISSUE NAME	CREATED	DURATION	ENTITIES	ANALYSIS SUMMARY	PATH	INCIDENTS
Active	Critical	Web response time > 1 second...	19m ago	19m	EC-site EC-CUBE-Check...	Signal: Latency, ... Components: A...	→ → →	5

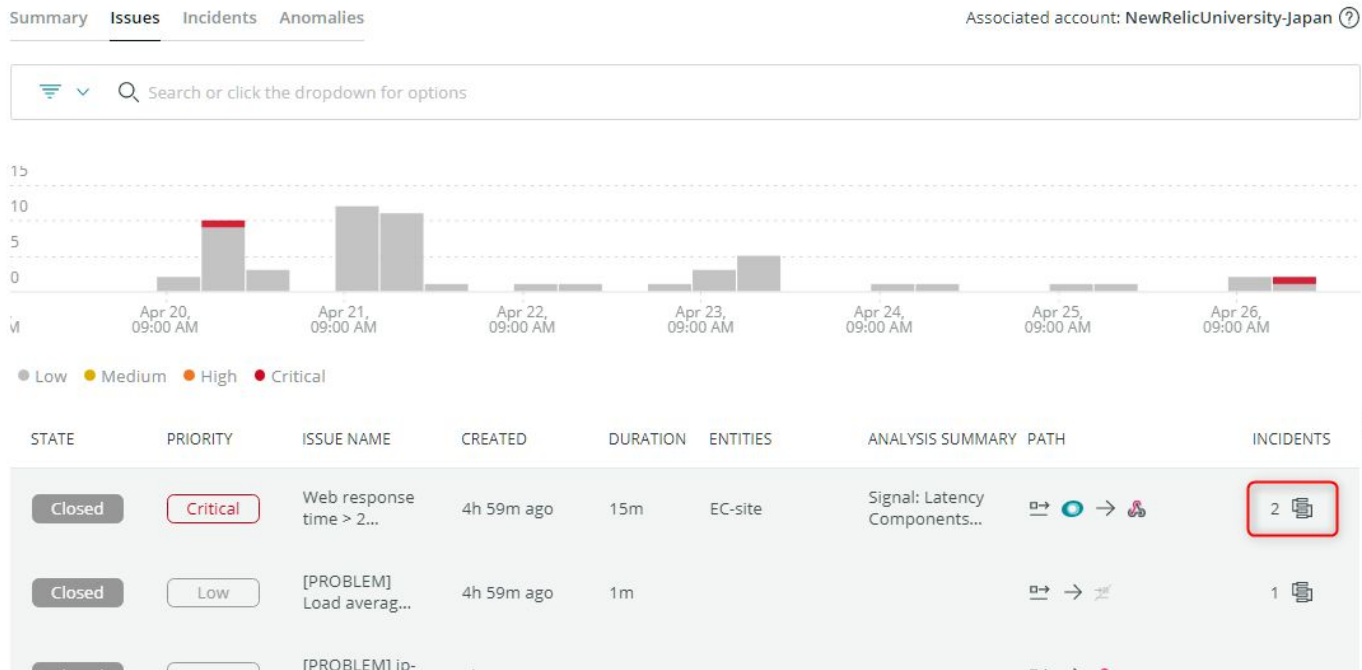
ハンズオン(2)複数のアラートを紐付け トラブルシューティングに役立てる

- 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 Alerts & AI interface. The top navigation bar includes 'Dashboards', 'Alerts & AI' (selected), 'APM', 'Browser', 'Infrastructure', 'Logs', 'Mobile', 'Synthetics', and 'More'. The right side of the bar shows a share icon, a time range selector set to 'Since 7 days ago', and a refresh icon. Below the navigation bar, the 'Issues' tab is selected, with other tabs being 'Summary', 'Incidents', and 'Anomalies'. The associated account is 'NewRelicUniversity-Japan'. A search bar contains the filter 'state = Active', which is highlighted by a red box and a red arrow. Below the search bar, a message states 'No chart data available.' with a line graph icon. At the bottom, a table header is visible with columns: STATE, PRIORITY, ISSUE NAME, CREATED, DURATION, ENTITIES, ANALYSIS SUMMARY, PATH, and INCIDENTS. Below the table, a message states 'No issues in sight' and 'We don't see any issues in the selected account or time window. When we do, you'll see a summary here.'

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。



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

The screenshot displays the New Relic incident management interface. At the top, a red banner indicates a "Critical priority issue was closed" with the text "End user Apdex < 0.7 at least once in 5 minutes on 'EC-site'". Below this, a summary bar shows "4 Incidents", "Source: [icon]", "Notified: [icon]", and "Issue payload". The main section is titled "Incidents (4)" and contains a table with the following data:

STATE	PRIORITY	INCIDENT NAME	CREATED	DU...	ENTITIES	ANALYSIS SUM...	SOURCE	EVENTS
Closed	Critical	Monitor failed for location Tokyo, JP on...	Mar 16, 3:28am	6m	EC-CUBE-Checkout		[icon]	2
Closed	Critical	Web response time deviated from the...	Mar 16, 3:26am	16m	EC-site	Components: Appl...	[icon]	2
Closed	Critical	Web response time > 1 seconds at least once...	Mar 16, 3:26am	6m	EC-site	Components: Appl...	[icon]	2

Below the incidents table, the "Root cause analysis" section is visible, containing three panels: "Deployment events (1)" showing "1 Deployments", "Error logs" showing "No logs detected", and "Attributes to investigate" showing "No outstanding attributes".

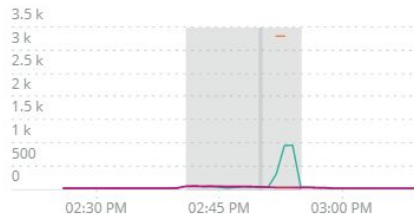
ハンズオン(2)複数のアラートを紐付け トラブルシューティングに役立てる

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

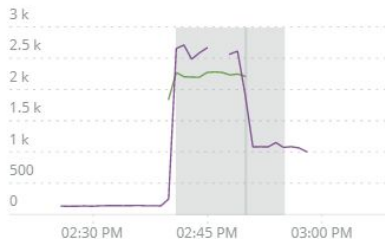
● Web response time > 2 seconds at least once in 5 minutes on 'EC-site' ● Critical

Attributes to investigate ?

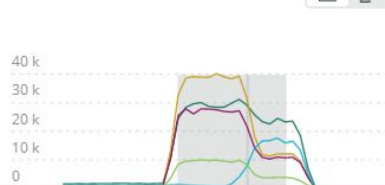
Average database duration (ms) faceted by
Datastore type and Table and Operation



Web response time faceted by
request.headers.accept



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

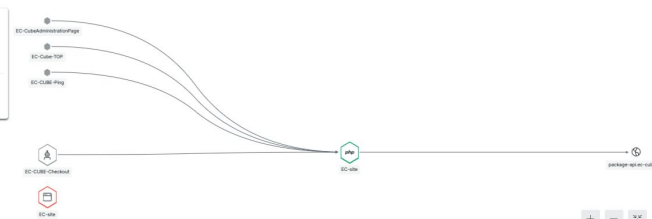


Impacted entities (3)

■ EC-site
■ EC-site

Issue timeline Issue log

Show
Related entities
Externals
Entities
Related entity
External Service



Root cause analysis

Deployment events (1)

1 Deployments

Last 12h

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

Possible cause Due to proximity to issue creation

座学(4)

AIOpsの意義

16:30 - 16:45 (15min)



ITサービスに発生しうる障害と監視の関連性

ITサービスに
発生しうる障害

理解できる

理解できない

気づける

Actionableな監視

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



とりあえずの監視

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

頑張るすべての
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

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



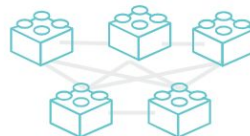
基盤



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

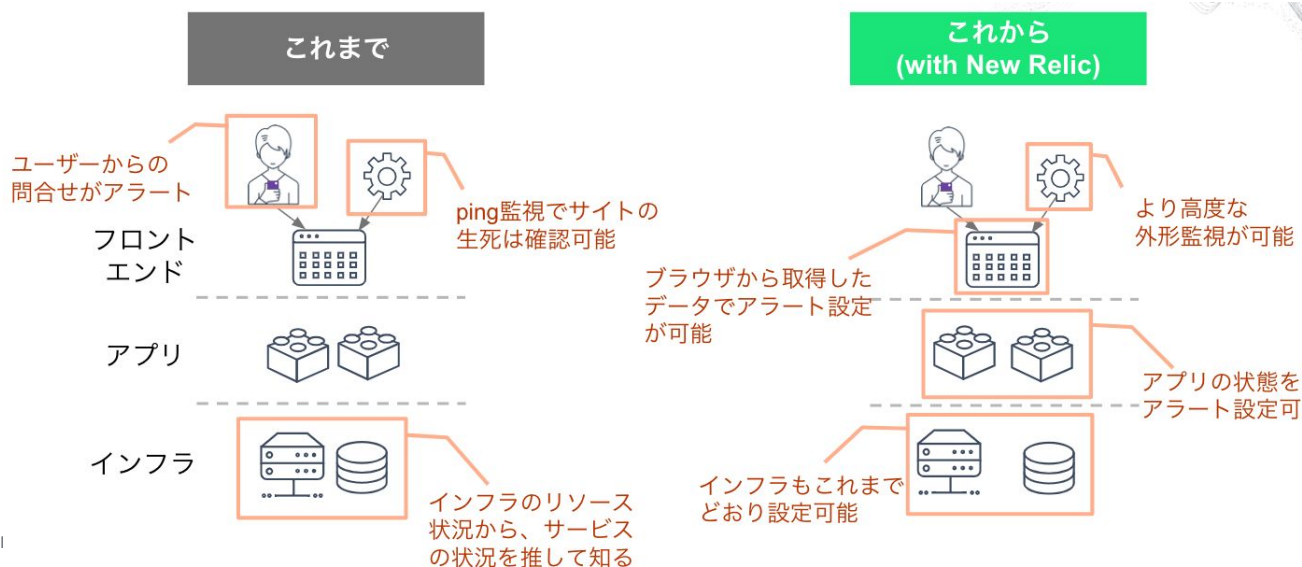


アプリがマイクロサービス化かつ基盤が疎結合なため、基盤リソースと関係なく問題が発生しうる

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

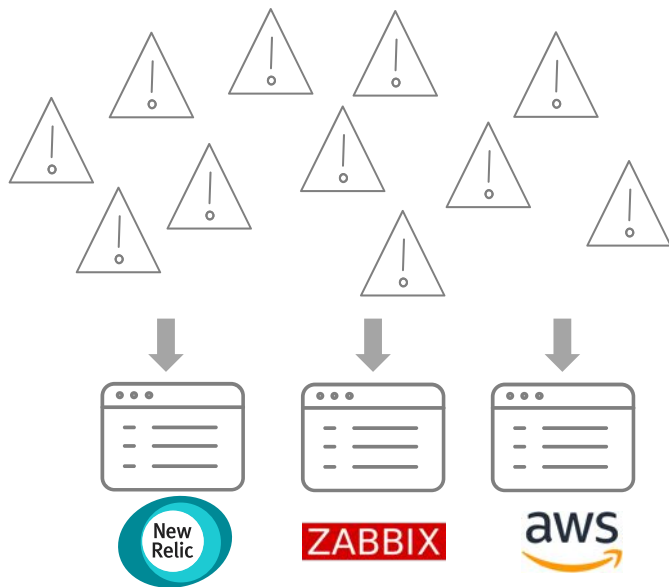


監視にまつわる新たな課題

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

人力でこの面を増やすのは困難

とっあえずの監視

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

理解できる

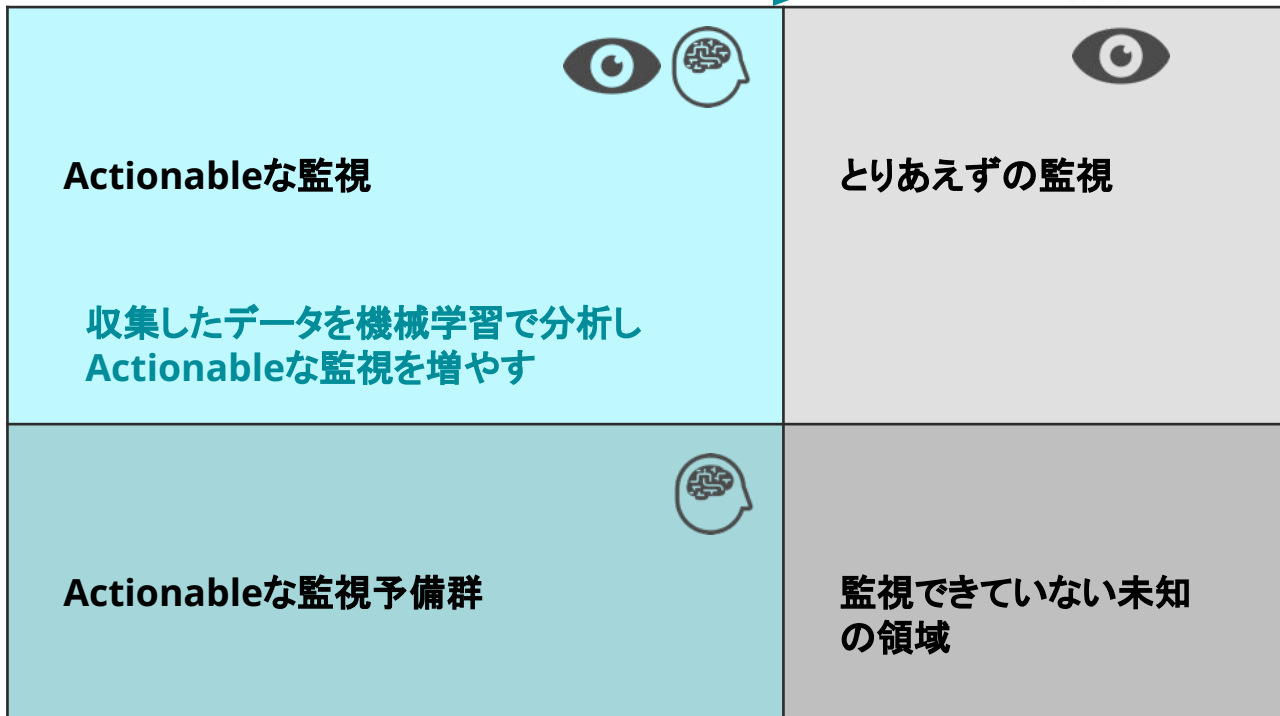
複数の事象を自動で関連付け
根本原因を推察

理解できない

気づける

手動でアラート
設定せずとも自動
で検知

気づけない



AIOpsによってサービスの信頼性を高める

アラートを1つ1つ網羅的に
設定するのか問題



[解決するAIOpsの機能]

- 異常検知



手動でアラート設定せずとも自動で検知

Detection gaps (BETA)

大量のアラートをどう解釈してトラ
シューするのか問題



[解決するAIOpsの機能]

- イベントの相関分析
- 根本原因分析



複数の事象を自動で関連付け、根本原因を推察

Anomaly Detection

機能紹介: Detection gaps

Detection gaps

See which services need alert coverage. Then add recommended alerts with a couple of clicks.

0/1 entities covered

Services - APM

Name

EC-site

Throughput

Error Rate

Action

Add alert

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).

Next

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: 251671 - NewRelicUniversity-Japan

Enter condition name

EC-site - Apdex

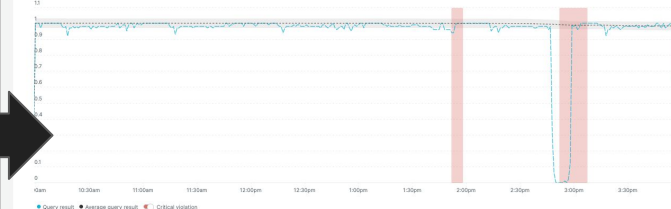
Define your signal

Enter NRQL Query

```
SELECT apdex(apm.service,apdex) FROM Metric WHERE entity.guid = 'HjUwMTY3Mx8UE18QV8QTE1DQVJ7T85NDQJMDA4MDk3' FACET entity .guid
```

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

Showing 1/1 time series



Preview charts are estimates only

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

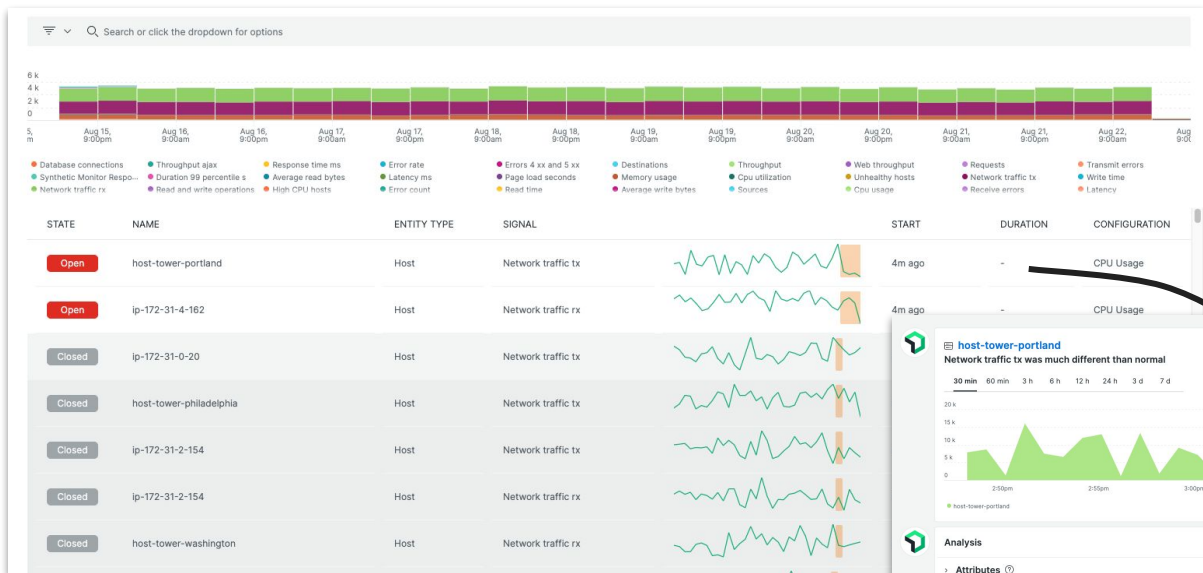
Set your condition thresholds

Threshold Type: ☐ Static ☒ Anomaly

Anomaly is useful when you want to define more flexible thresholds that adjust to how your data behaves. You'll get notified only when something behaves abnormally. See our docs.

Threshold direction: Upper and lower

機能紹介: Anomaly Detection



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

Alerts & AI -> Issues & activity -> Anomalies

- 発生したAnomalyの1つを選択し、詳細を確認する

ハンズオン(3) AIOpsを使った異常検知 と原因分析(応用編)

Presenter Name

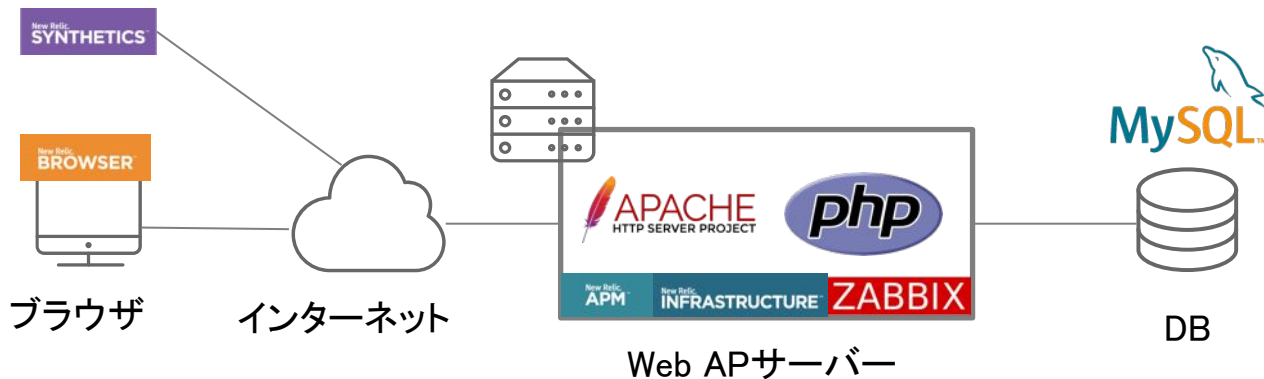
16:45 - 16:55 (10min)

Title



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。

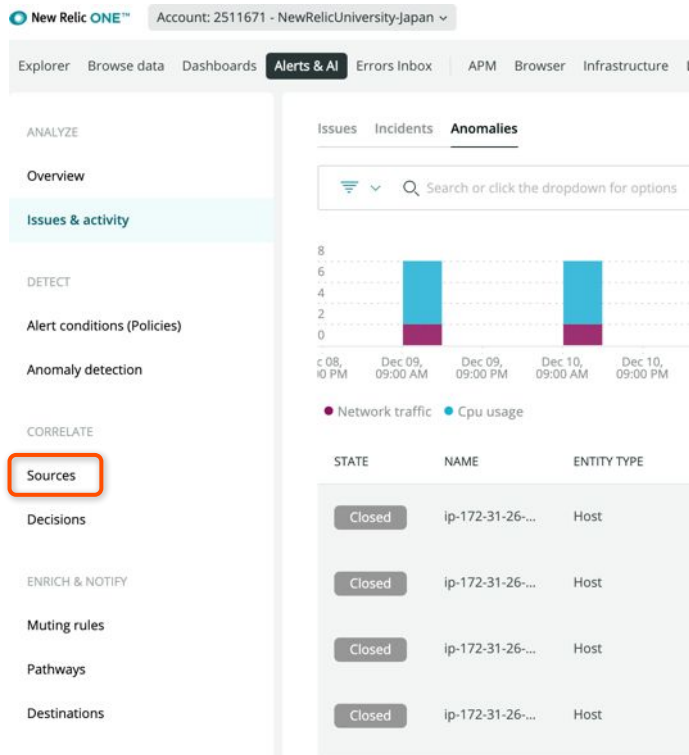


手順・解説

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る(1)

- 「Sources」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

- 「Alerts」カードをクリックします。

The screenshot shows the New Relic Alerts & AI interface. The top navigation bar includes links for Explorer, Browse data, Dashboards, Alerts & AI (selected), Errors inbox, APM, Browser, Infrastructure, Logs, Mobile, Synthetics, and More. The left sidebar contains a tree view with categories: ANALYZE (Overview, Issues & activity), DETECT (Alert conditions (Policies), Anomaly detection), CORRELATE (Sources, Decisions), ENRICH & NOTIFY (Muting rules), Workflows (marked as New), and Destinations. The main content area displays '2 active sources' with '1 policy connected' and '1 configuration connected'. Below this, the 'Available sources' section features two cards: 'Alerts' (with '1 active policy' and a description about ingesting alert policies) and 'REST API' (with a description about using the REST endpoint for data ingestion).

ハンズオン(3-1)様々なソースのアラートをまとめる

- 「+ Add a policy」ボタンをクリックします。

Associated account: NewRelicUniversity-Japan ?



New Relic Alerts source

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

NEW RELIC IS CONNECTED

POLICIES (1)

+ Add a policy

POLICY ↕	ACCOUNT ↕
インシデントインテリジェンス 	NewRelicUniversity-Japan

ハンズオン(3-1)様々なソースのアラートをまとめる

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

 Get data from New Relic Alerts

Select the New Relic Alerts policies you want to connect ?

Account All

Search policies

View: All (4) Selected (2) Unselected (2)

☐	POLICY	ACCOUNT NAME
☒	インシデントインテリジェンス	NewRelicUniversity-Japan
☐	アラートポリシー	NewRelicUniversity-Japan
☐	ダッシュボード/ハンズオン用アラートポリシー	NewRelicUniversity-Japan
☒	参加者名 アラートポリシー	NewRelicUniversity-Japan

Cancel

Connect

ハンズオン(3-1)様々なソースのアラートをまとめる

- 自分のPolicyが追加された事を確認します。



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

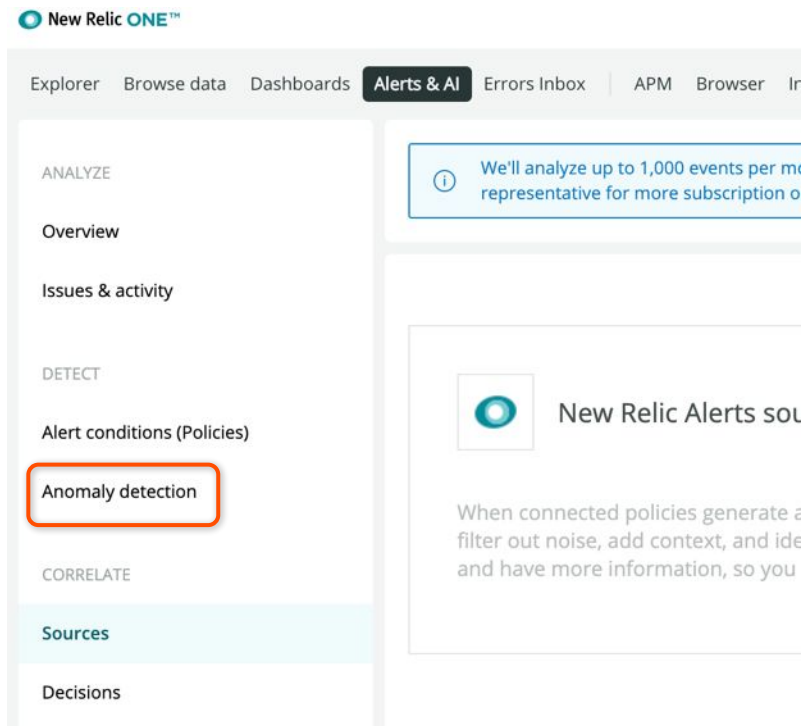
POLICIES (2)

+ Add a policy

POLICY ▾	ACCOUNT ▾
インシデントインテリジェンス 🔗	NewRelicUniversity-Japan
参加者名 アラートポリシー 🔗	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。



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 settings

We automatically detect anomalies that you can [query](#) and add to dashboards. Use this page to adjust which anomalies you see, where you see them, and whether you get notified. For more info or help with querying, [see our docs](#) 

Visibility

We display anomalies in the activity stream and AI overview. Use the button below to adjust what you see.

Anomaly 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 ⌵

Applications ⌵

Account ⌵

Last updated ⌵

Destination ⌵

ハンズオン(3-2)様々なソースのアラートをまとめる

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

Configure anomaly detection

▼ Make this configuration easy to identify

自分の名前

▼ What account do you want to use?

Account: 2511671 - NewRelicUniversity-Japan ▼

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

Service - APM

APM

Entities: 2

Search in this table...

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

Name

☒ ★ EC-site

☐ webapp

© 2022 New Relic, Inc. All rights reserved

 new relic 128

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 settings

We automatically detect anomalies that you can [query](#) and add to dashboards. Use this page to adjust which anomalies you see, where you see them, and whether you get notified. For more info or help with querying, [see our docs](#) ↗

Visibility

We display anomalies in the activity stream and AI overview. Use the button below to adjust what you see.

Anomaly visibility preferences

Notifications

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

+ Add a configuration

Q Search configurations

Configuration name ↕	Applications ↕	Account ↕	Last updated ↕	Destination ↕
自分名前	1	NewRelicUniversity-Japan	Apr 26, 2021 7:11pm	...
sasaki-test	1	NewRelicUniversity-Japan	Apr 22, 2021 7:16pm	...

参考 Zabbixの連携

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

The screenshot displays the New Relic Incident Intelligence web interface. The top navigation bar includes links for Explorer, Browse data, Dashboards, Alerts & AI (which is the active tab), Errors inbox, APM, Browser, Infrastructure, Logs, Mobile, Synthetics, and More. A left sidebar contains a hierarchical menu with sections: ANALYZE (Overview, Issues & activity), DETECT (Alert conditions (Policies), Anomaly detection), CORRELATE (Sources, Decisions), ENRICH & NOTIFY (Muting rules, Workflows, Destinations), and a 'New' badge next to Workflows. The main content area shows '2 active sources' with '1 policy connected' and '1 configuration connected'. Below this, the 'Available sources' section features two cards: 'Alerts' (with '1 active policy' and a description about ingesting alert policies) and 'REST API' (highlighted with an orange border, with a description about using the REST endpoint for data ingestion). The REST API card includes an icon of a server with a cloud and a plus sign.

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。



event_subject	{ALERT.SUBJECT}	削除
event_id	{EVENT.ID}	削除
event_nseverity	{EVENT.NSEVERITY}	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 eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiIsInR5cCI6IkpXZWx0eXkiLCJ1aWkiOiJhbm91dCJ9.eyJ1b29udCI6IjEiLCJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiIsInR5cCI6IkpXZWx0eXkiLCJ1aWkiOiJhbm91dCJ9	削除
new_relic_proxy_url		削除
new_relic_url	https://collectors.signifai.io/v1/incident	削除
urgency_for_average	2	削除
urgency_for_disaster	1	削除
urgency_for_high	2	削除

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

1h

メンテナンス中の場合に実行を保留



実行内容

ステップ 詳細

開始時刻 継続期間 アクション

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

[追加](#)

復旧時の実行内容

詳細

アクション

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

[変更](#) [削除](#)

[追加](#)

更新時の実行内容

詳細

アクション

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

[変更](#) [削除](#)

[追加](#)

* 少なくとも1つ以上の実行内容が設定されている必要があります。

更新

複製

削除

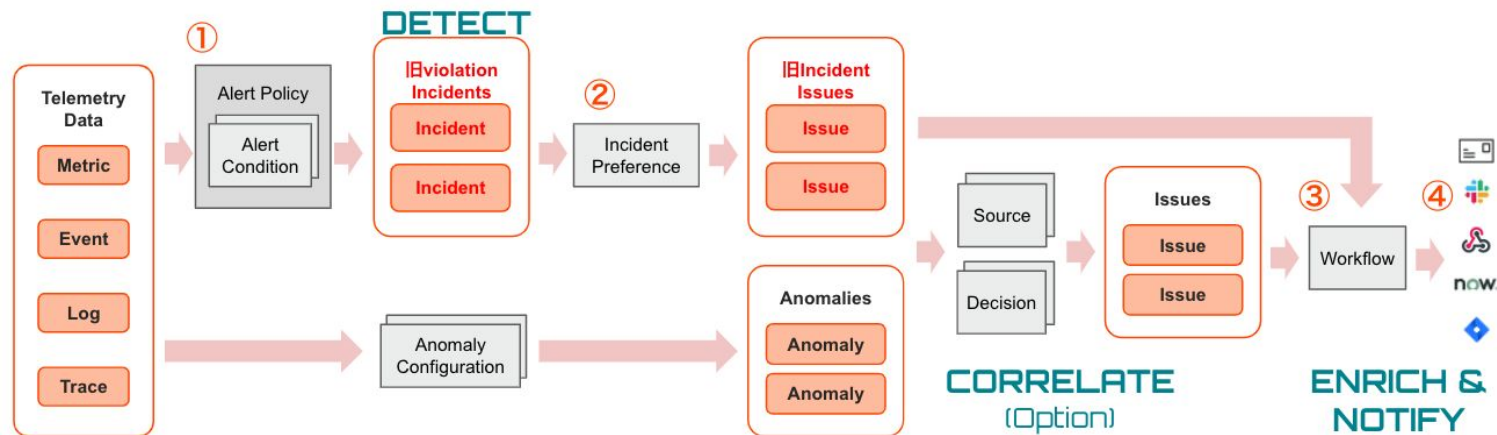
キャンセル

まとめ



まとめ

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



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



お疲れさまでした。

ご質問があればチャットにご記入ください
アンケートにご協力お願いいたします

Thank you.