



NRU 304 「AIOps とアラート設計の基本」

November 22, 2023



ウェビナー 各種ご連絡

1. ご質問がある場合は、「Q&A」からご入力ください。



① 画面下
「Q&A」をクリック！

こちらにご質問をご記入し、
「送信」をクリックしてください！

②

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

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**



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.

本セッションのゴール

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

本セッションの想定対象者と前提条件

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

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

- [New Relicの基礎](#)
- [ダッシュボードワークショップ](#)（NRQL入門編に相当）
- [NRQL reference](#)（公式ドキュメント）

Agenda

時間(目安)	内容	
15:00-15:15	座学(1)	ユーザー視点のアラート
15:15-15:30	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)	アラートポリシー・ワークフローを作成する
16:00-16:15	座学(3)	アラートコンディションの作成
16:15-16:30	ハンズオン(2)	アラートコンディションを作る
16:30-16:40	ハンズオン(3)	発生したアラートの確認
16:40-16:55	座学(4)	New Relicのアラート分析支援機能とAIOpsを使った異常検知

16:55-17:00

© 2023New Relic, Inc. All rights reserved

まとめ、アンケートご記入

座学(1)

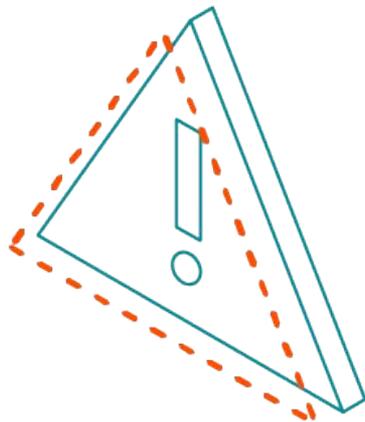
ユーザー視点のアラート

15:00 - 15:15 (15min)



突然ですが

- どんなアラートを設定していますか？



アラートを設定する目的

対象システムが、**何らかの対応が必要な状態**であることの通知を受け取るため

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

”受け取った結果、何かしらのアクションを起こせるようなアラート”を設定する

アラートのアンチパターンとデザインパターン

アンチパターン: OSのメトリクスのアラート

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

“OSのメトリクスは診断やパフォーマンス分析にとっては重要です。しかし99%の場合、これらのメトリクスは誰かを叩き起こすには値しません。”

出典: 入門監視 (Oreilly, 2019)



アラートのアンチパターンとデザインパターン

デザインパターン: ユーザー視点の監視

“ユーザーが気にするのは、アプリケーションが動いているかどうかです。”

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

出典: 入門監視 (Oreilly, 2019)

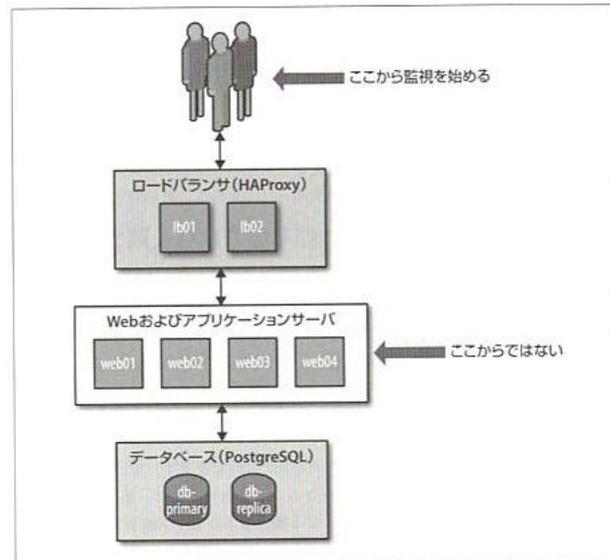
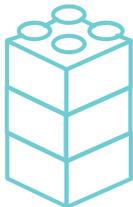


図2-1 できるだけユーザーに近いところから監視を始める

なぜアンチパターンが生み出されたのか

過去のシステム

アプリ



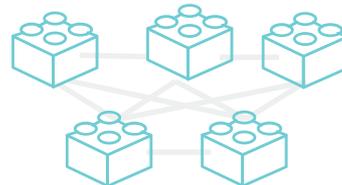
基盤



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

近年のシステム

アプリ



リソース抽象化
(仮想化、コンテナ等)

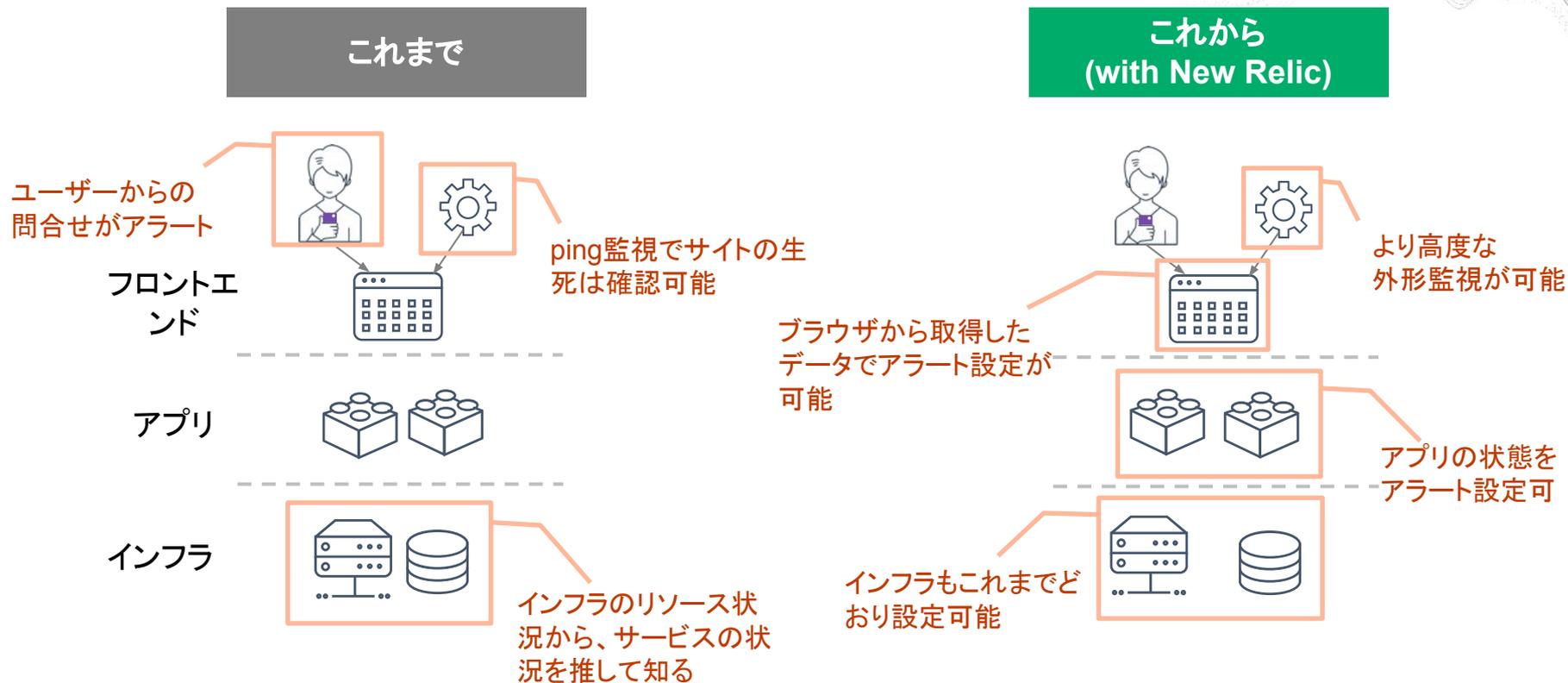


基盤



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

アラートのこれまでと、New Relicを使ったこれから



目的別、アラート設定例(Webアプリの一例)

カテゴリ	現在起こっているサービス影響		将来のリスクの兆候	
	サイトが遅い	エラーを返す	キャパシティを超える	リソースが枯渇する
外形監視	チェック応答時間	チェックエラー		
フロントエンド	CWV	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

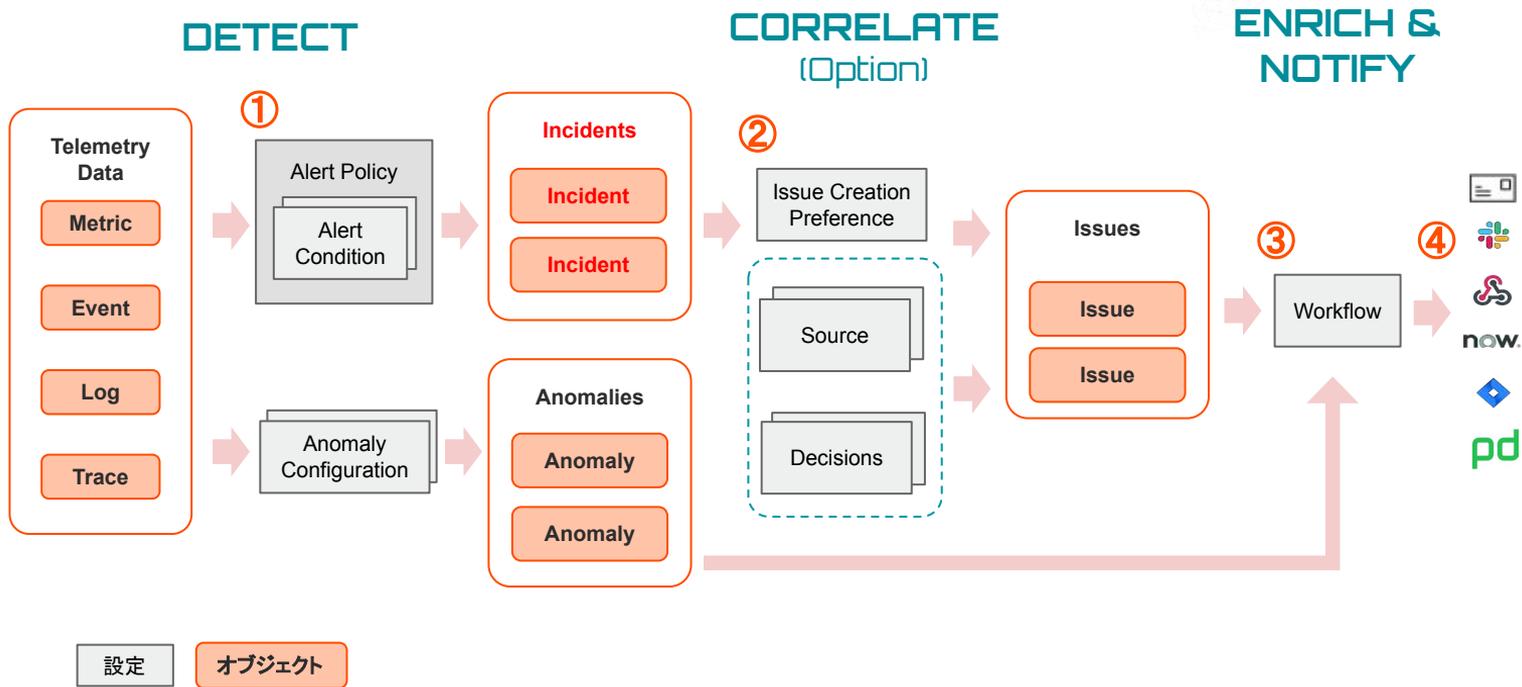
New Relicがリアルタイムに収集しているデータを使って、アラートを設定することが可能

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

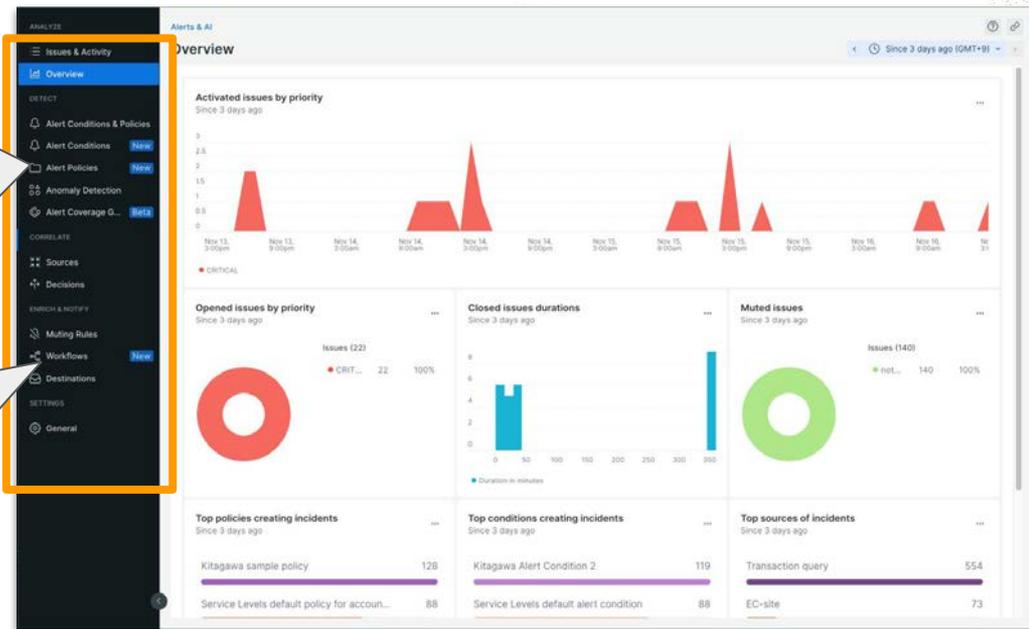
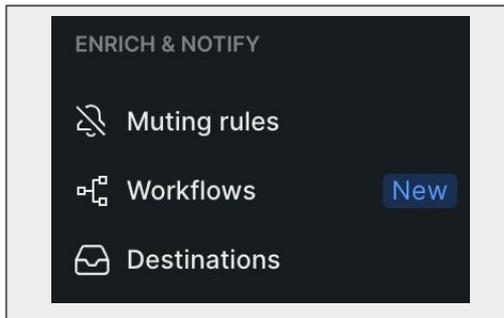
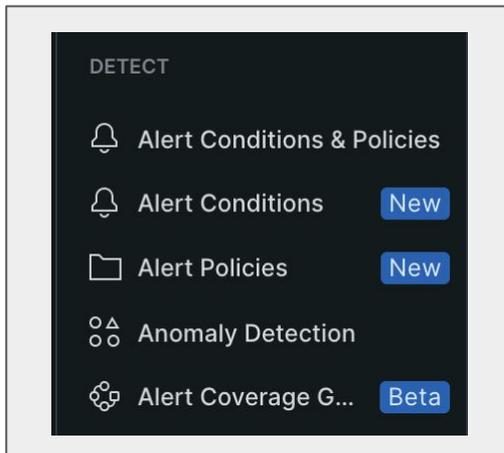
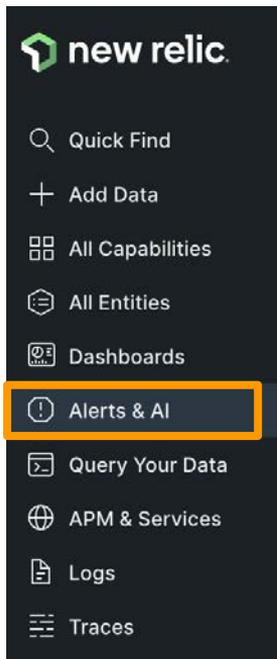
※アラートを上げる条件や頻度、通知先の設定など、様々な設定が可能なので、次ページ以降で解説していきます



New Relicのアラート構造全体像



アラート機能の全体UIと重要メニュー



New Relic アラートの構成要素1: Alert Policy

Alert Policy

Alert Conditionのグループ

Alert Condition

アラート対象や閾値、集計方法の定義

Incident

Alert Conditionで検出した個々の違反

Issue

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

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.

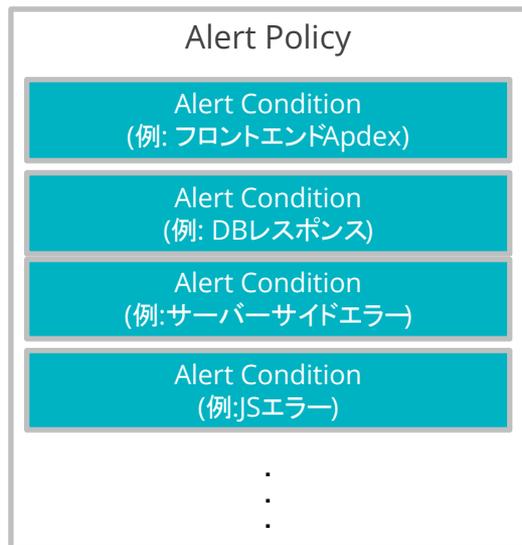
One issue per condition and signal 
Group incidents sharing the same condition and signal into an issue.
 This may create a large number of notifications.

[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1: Alert Policy

New Relic のアラートは、Alert Policyという器にAlert Conditionを内包した構造となっている
Alert Policyごとにアラートをグループ化したり、通知先の制御ができる
通常、送信先やアラートの目的別にポリシーを分けることが多い



アラートポリシー

id: 545592

Incident preference: By condition Delete this policy

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

Issue Creation Preference

IncidentをIssueにグループ化して、通知をまとめる設定

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

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

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

New Relic アラートの構成要素2: Alert Condition

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

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

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

How would you like to do this?

Use guided mode Recommended
Choose from options and we'll build your query

Write your own query
Use NRQL to define your alert

※詳細はこの後の章でご説明します

Tell us where to look ⓘ

<input checked="" type="checkbox"/> AWS (4 types)	<input type="checkbox"/> Browser applications
<input type="checkbox"/> On host integrations (2 types)	<input type="checkbox"/> Service Levels
<input type="checkbox"/> Synthetic monitors	<input type="checkbox"/> VPC Networks

New Relic アラートの構成要素3: Workflow

発生したIssueと、通知先・通知内容の関連付け

Filter data

どのようなIssueで、このWorkflowを起動するか

Enrich (Additional settings内)

通知に、Issueに関する付加情報を付与する

Mute issues (Additional settings内)

Muting Rulesが設定されていた場合の挙動の設定

Notify (Destinations: 後述)

通知先の定義と、通知内容のカスタマイズ

Test workflow

過去の該当データを元に、Workflowの通知テストを実行

The screenshot shows the 'Configure your workflow' interface in New Relic. It includes a text input field for a name, a 'Filter data' section with dropdowns for Tag, Policy, and Priority, and an 'Additional settings' section with a 'Notify' subsection. The 'Notify' section contains a grid of destination options: ServiceNow incidents, Webhook, Jira, Slack, Email, AWS EventBridge, Mobile push, and PagerDuty. At the bottom, there is a 'Test this workflow' section with a 'Test workflow' button.

Configure your workflow

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

Filter data

Select the kinds of issues you want to send.
Use the basic filter for the most common attributes or the advanced filter for all attributes. Basic Advanced

Tag Policy Priority

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

Additional settings

Notify

Choose one or more destinations and add an optional message.

Add channel

ServiceNow incidents	Webhook	Jira	Slack
Email	AWS EventBridge	Mobile push	PagerDuty

Test this workflow

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

New Relic アラートの構成要素4: Destinations

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

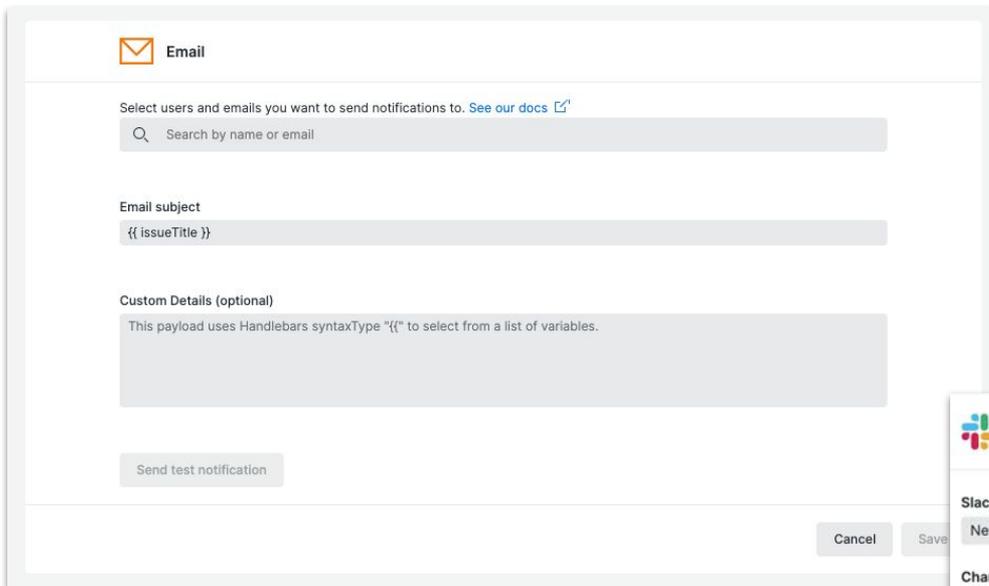
シンプルな通知



連携サービスへの通知



New Relic アラートの構成要素4: Destinations



Email

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

Search by name or email

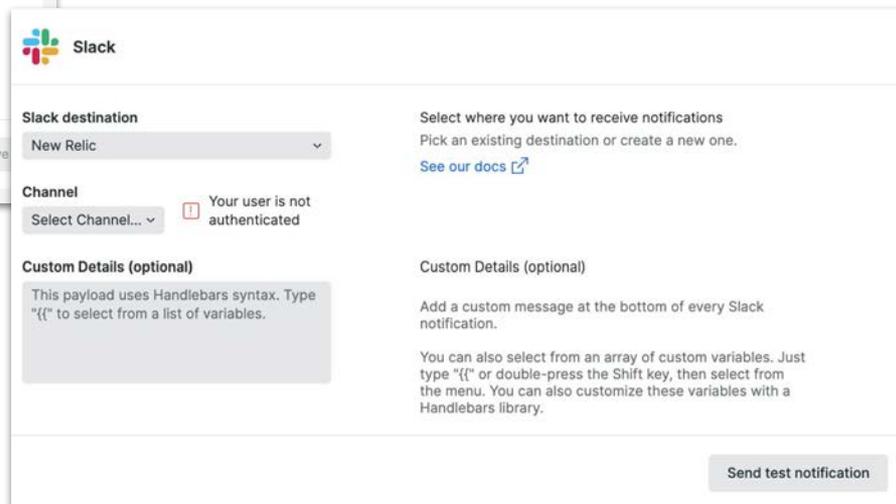
Email subject
{{ issueTitle }}

Custom Details (optional)
This payload uses Handlebars syntaxType "{{" to select from a list of variables.

Send test notification

Cancel Save

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



Slack

Slack destination
New Relic

Select where you want to receive notifications
Pick an existing destination or create a new one.
[See our docs](#)

Channel
Select Channel... Your user is not authenticated

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

Custom Details (optional)
Add a custom message at the bottom of every Slack notification.
You can also select from an array of custom variables. Just type "{{" or double-press the Shift key, then select from the menu. You can also customize these variables with a Handlebars library.

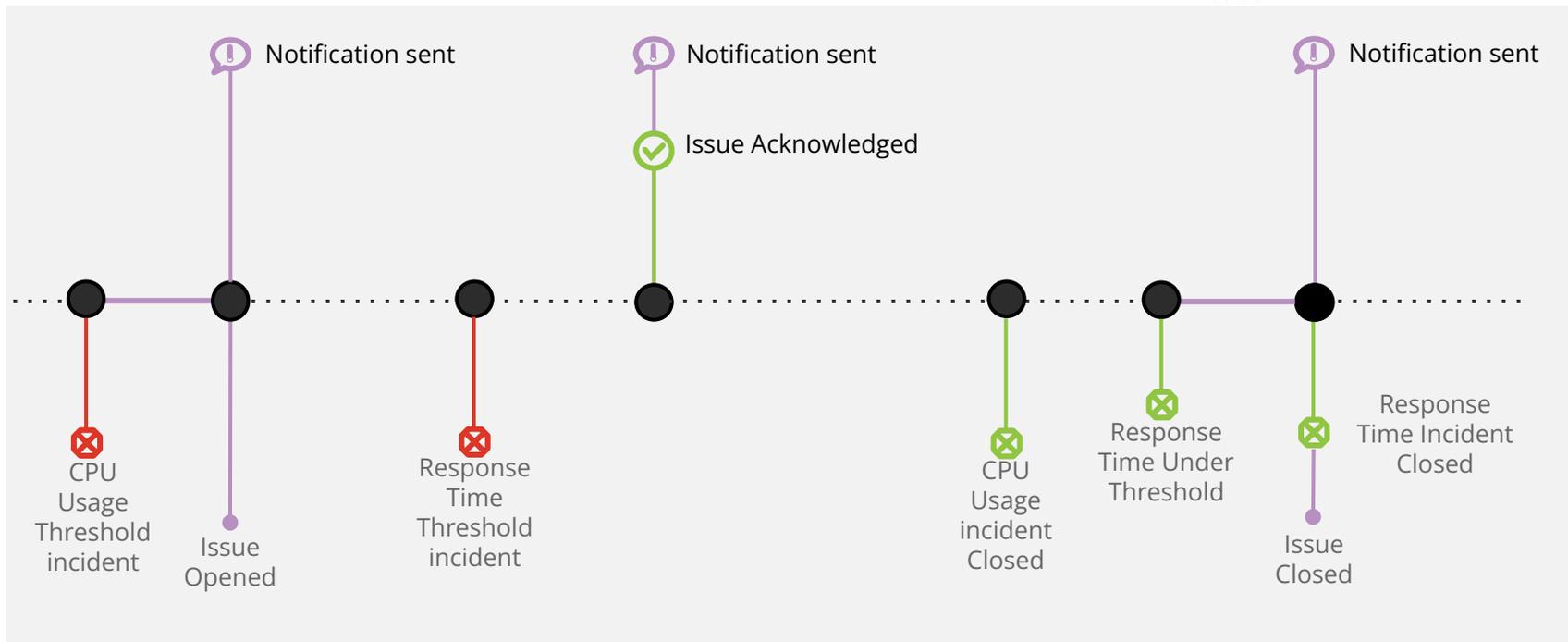
Send test notification

Workflows variables:

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

補足: Issueのライフサイクルと通知タイミング

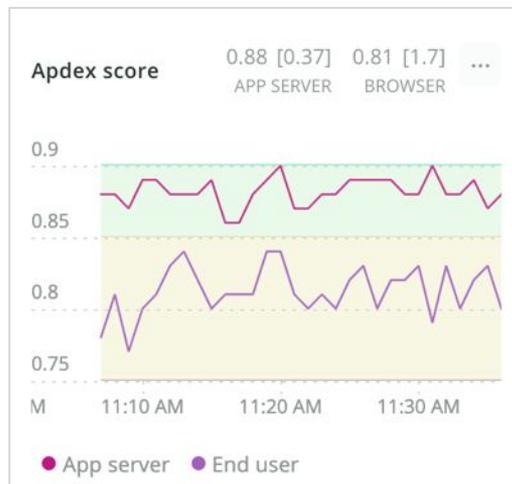
Issueの起票、Acknowledgeがされたタイミング、およびクローズの際に通知が届く



補足: アラートを設定する前にやること

Apdex Tの値を適切に設定する

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



Application server

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

Apdex T ?

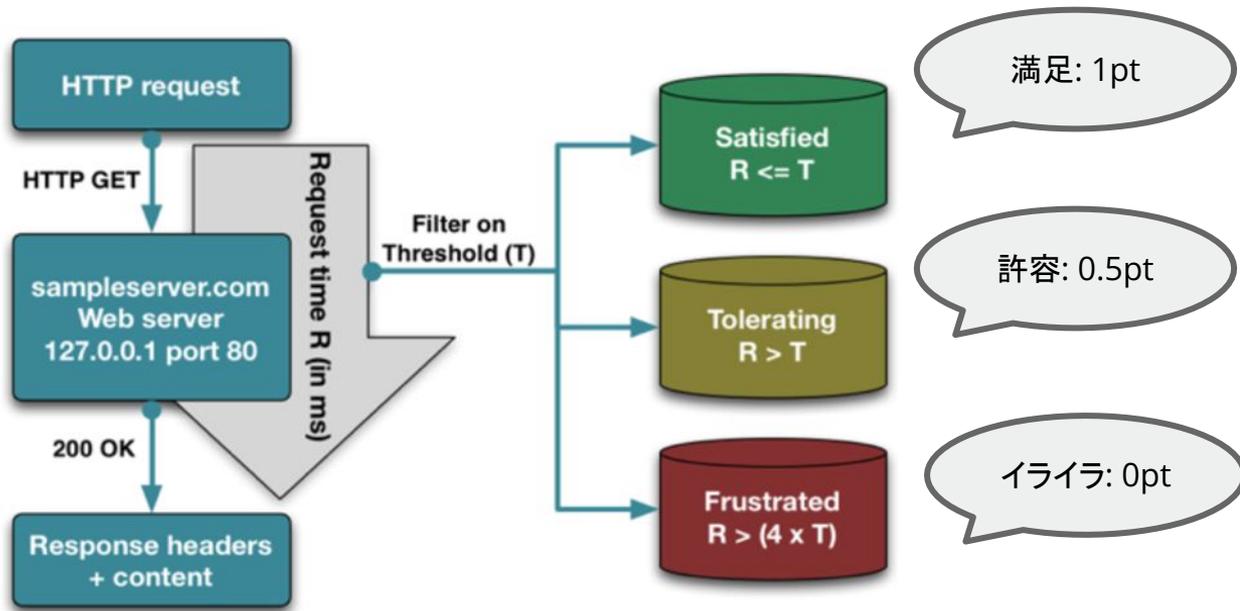
seconds

Please input a decimal or whole number only.

補足: Apdex T値について

それを満たせばユーザーが満足すると想定される、最大応答速度

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



今回監視対象のサイト

[NRUジェラートショップ](ECサイト)

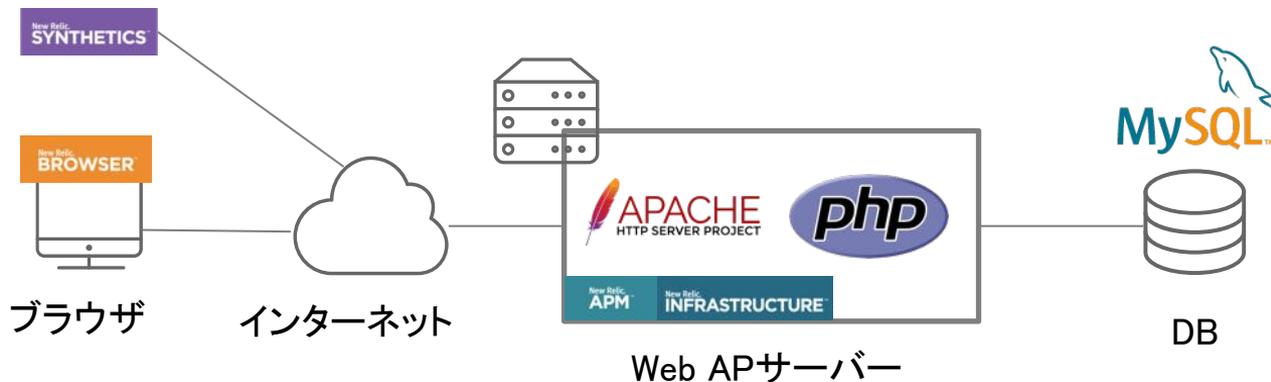
このハンズオンでは、PHPおよびMySQLにより構築されたジェラート屋さんの ECサイトをモニタリング対象にしています。

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



今回の環境の監視構成

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



ハンズオン(0) 環境を確認する

15:30 - 15:40 (10min)



ハンズオン環境について

New Relic にログインしてください。

New Relic : <https://one.newrelic.com>

- ユーザー: japan-handson+nru@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)

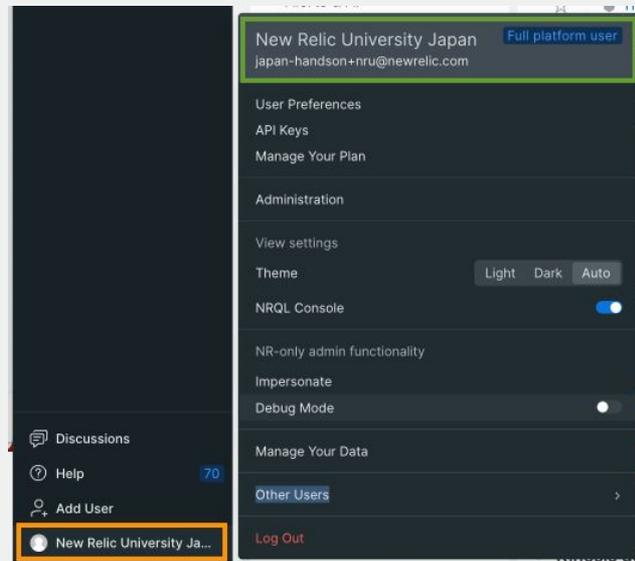
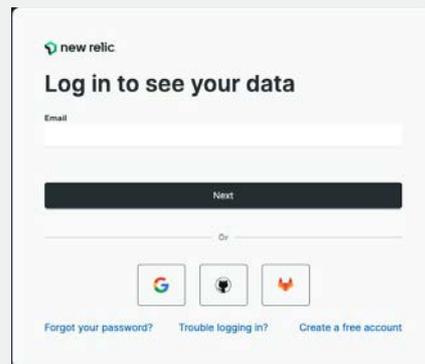
ユーザー名が “New Relic University Japan” であることをご確認ください

[ご注意ください]

普段 New Relic 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。
プライベートブラウジングをお使いください。

また、ブラウザは下記のいずれかをご利用ください。

- 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



ログイン後のアカウントの切り替え



“Japan NRU(Original NR Account)” の場合は

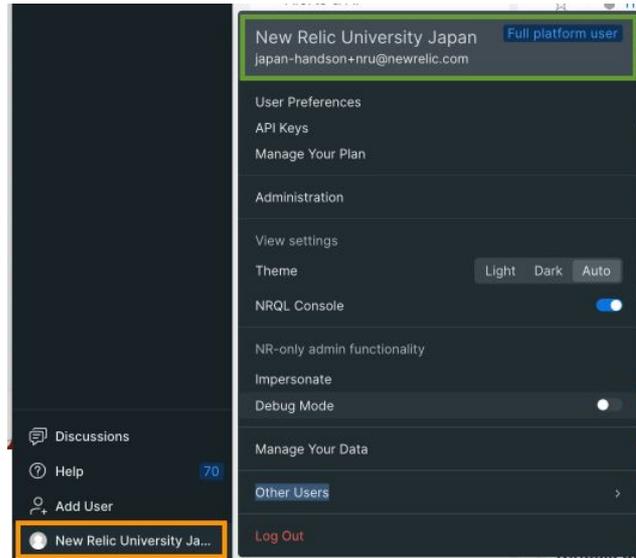
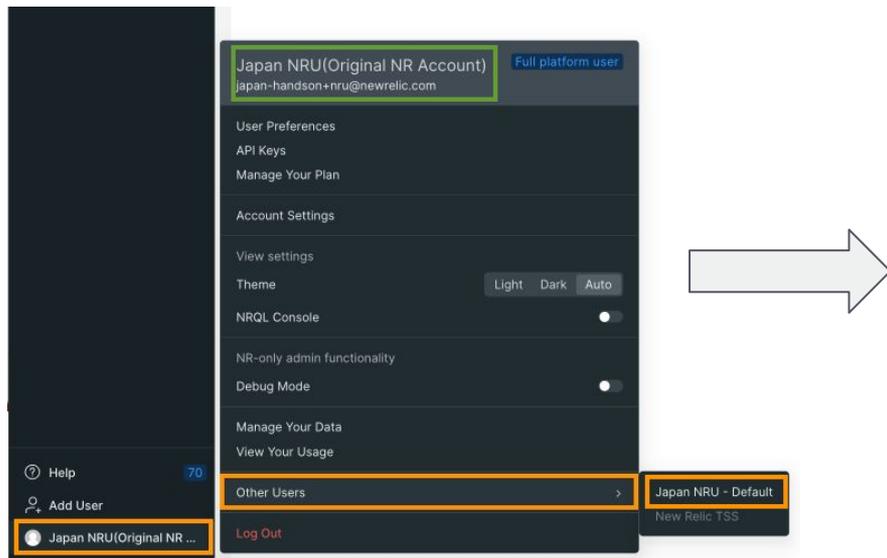
以下の操作にて、ユーザーの切り替えをお願いします

ユーザー名 > Other Users > “Japan NRU”

再度パスワードを入力し、ユーザーの切り替えを実施ください。

“Japan NRU (Original NR Account)” ではなく

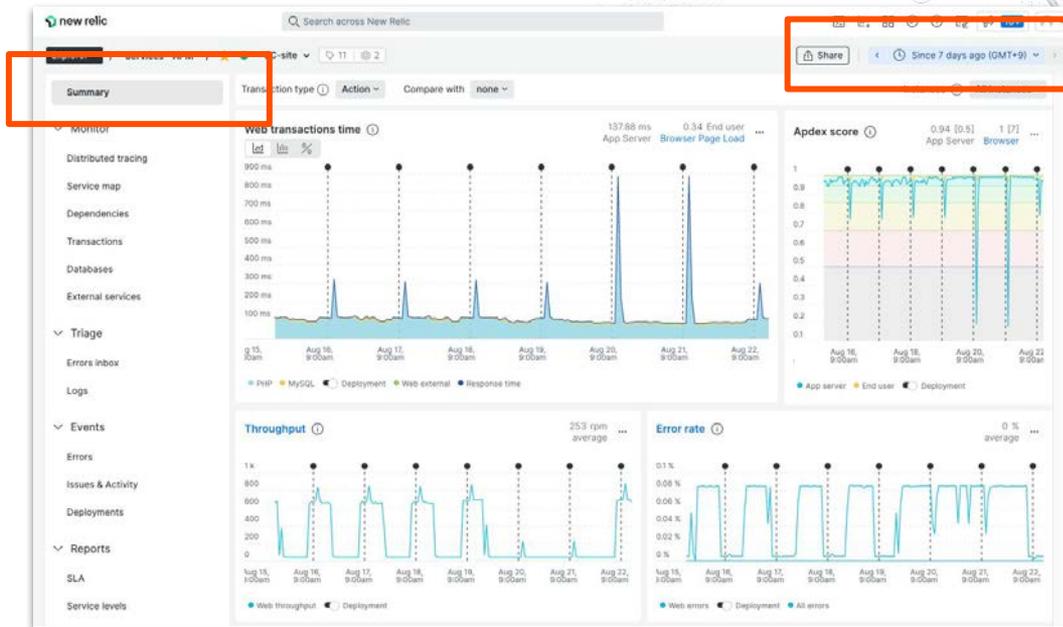
ユーザー “New Relic University Japan” を利用します



ハンズオン(0) UIの確認

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

同様に、BrowserやInfrastructureを参照してください。



ハンズオン(0) Apdex Tの設定箇所の確認



変更は行わない!!!

- New Relicポータルの左ペインの"APM & Services"を選択し、EC-siteアプリを選択します。
- Settings → Applicationを選択します。

EC-site

Application settings

Application alias

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

Alias

EC-site

Application server

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

Apdex T ⓘ

0.5

Enter a decimal or whole number only.

ⓘ Any saved change will restart all agents for this application

ハンズオン(1) アラートポリシー・ワー クフローを作成する

15:40 - 16:00 (20min)

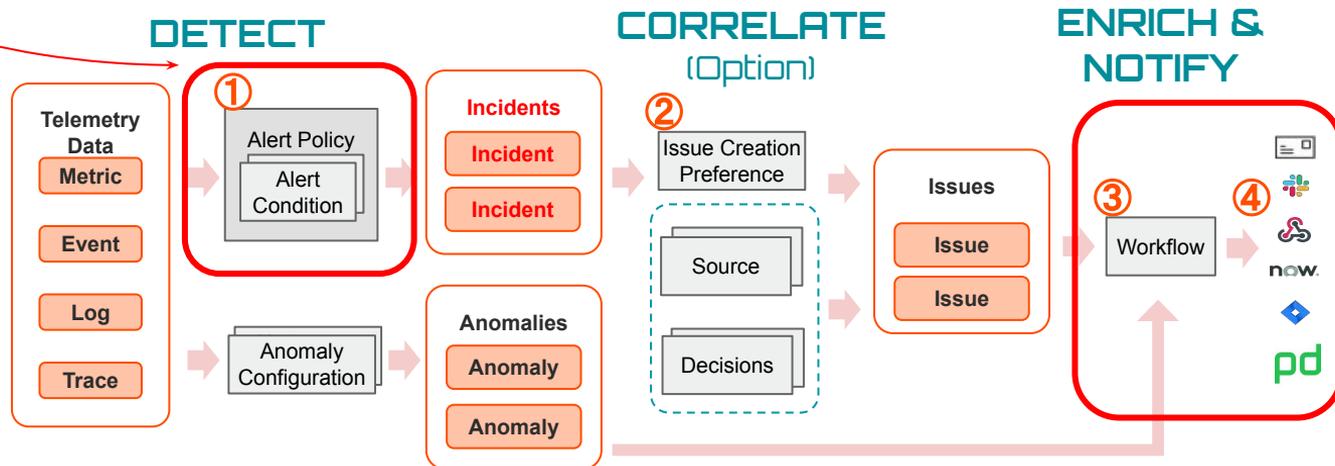




ハンズオン(1)アラートを作成する

作業内容

1. Alert Policyを作成する
2. Workflowを作成する





手順・解説

ハンズオン(1-1) Alert policyを作成する 1/2

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

The screenshot displays the New Relic Alerts & AI interface. On the left sidebar, the 'Alerts & AI' menu item is highlighted with a red box and a circled '1'. Below it, the 'Alert Policies' sub-menu item is also highlighted with a red box and a circled '2'. In the main content area, the 'Alert Policies' page is shown. At the top right of this page, the '+ New alert policy' button is highlighted with a red box and a circled '3'. Below the button, there is a table listing existing alert policies.

Name	Open issues	# of conditions	
NRU-Sample-Policy	0	4	...
Service Levels default policy for account 3940716	1	1	...
これがあなたのポリシーです。	0	0	...
ダッシュボードハンズオン用アラートポリシー	1	44	...



ハンズオン(1-1) Alert policyを作成する 2/2

1. 右側から設定画面がスライドされてくるので、Policy nameには、ご自身が作成したとわかる名前をつけてください
2. [こちらのスライド](#) を参考に、好みの「Incident Grouping」を選択してください
3. [Suppress noise...]をチェック
4. [Create & close] をクリックします

ウィザードでの一括作成もできますが、今回は各コンポーネントを手動で作成したいため、ここでは **Alert policyのみ**を作成します

Create an alert policy
Policies help you organize your alert conditions.

Policy name *
①

Incident Grouping

Group incidents within this policy
Tell us how you want to group incidents from this policy into issues. You get notified based on issues, not incidents.

② One issue per policy
 One issue per condition
 One issue per condition & signal
This may create a large number of notifications.

Group with other incidents from other sources

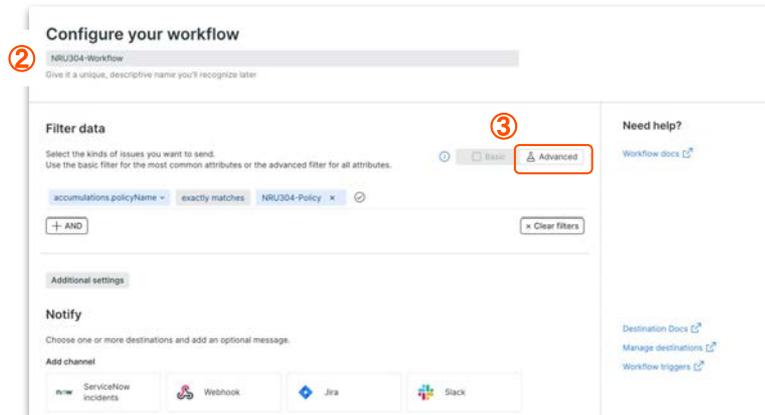
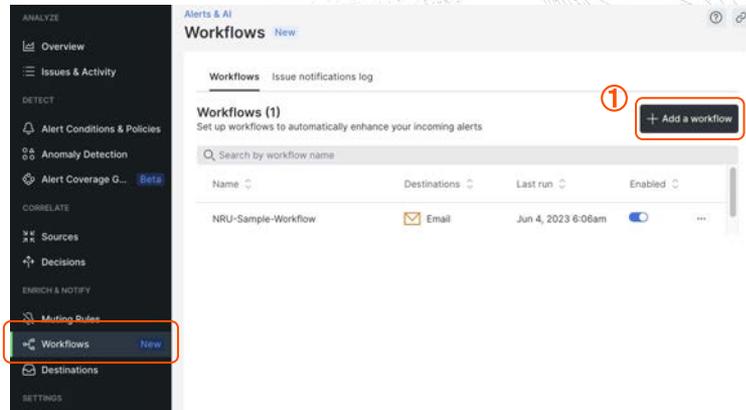
③ Suppress noise with machine learning correlation
We'll analyze incidents from all policies and sources and group related incidents into issues. [See our docs](#)

④

ハンズオン(1-2) Workflowを作成する 1/6

1. Alerts & AIメニューのWorkflowsをクリックし、[+ Add a workflow]をクリックします
2. ご自身のworkflowであることがわかる名前を入力します
3. Filter dataで"Advanced"を選択し、次のフィルタを設定します
 - a. Select or enter attribute: **policyName**
 - b. Select operator: **exactly matches**
 - c. Select or enter value: **作成したポリシーを選択**

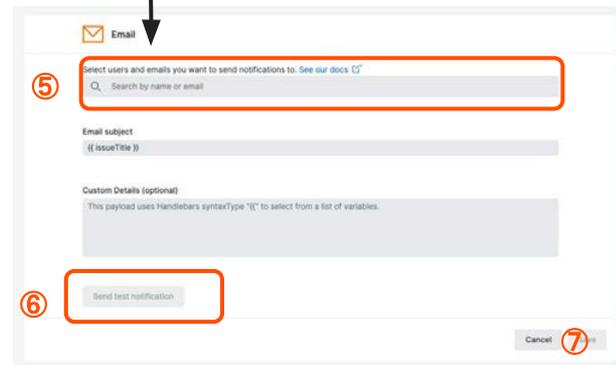
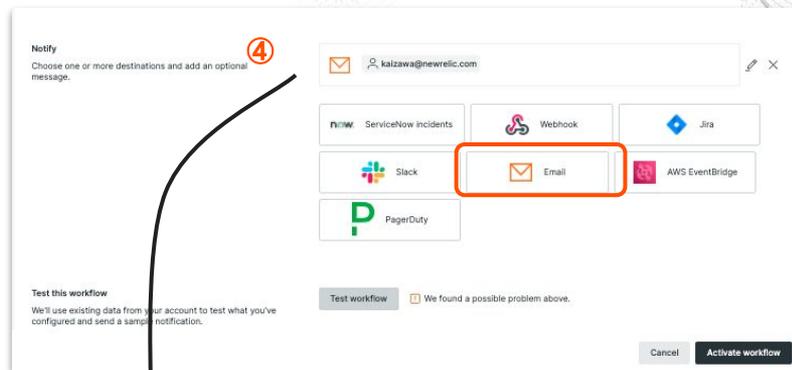
補足: 上記3番の設定はBasicでも可能ですが、より柔軟な設定を行う場合にはAdvancedを活用します。





ハンズオン(1-2) Workflowを作成する 2/6

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





ハンズオン(1-2) Workflowを作成する 3/6

受信したテストメールを確認します。

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

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

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

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

- “`{{`”と入力すると、利用可能な環境変数の一覧が表示されます。

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

Tags

```
account: Account 3940716  assignmentGroup: Team1  assignmentGroup: Team2
instrumentation.name: apm  language: php  type: APM Baseline  enabled: true
agentVersion: 10.10.0.1  id: 32666626  accountId: 3940716  affectedService: service1
affectedService: service2  causeService: Service1  causeService: Service2
instrumentation.provider: newRelic  nr.tracing: standard  policyId: 4406018
trustedAccountId: 3940716
```



ハンズオン(1-2) Workflowを作成する 4/6

8. 実際のルールでテストする際は、Test workflowボタンを押します

※Alert Conditionをまだ設定していないためTest workflow ボタンを押しても、今回メール送信はされません
(Warningが出ますが異常ではありません)

9. Activate workflowボタンをクリックし、設定を保存します

The screenshot displays the New Relic workflow configuration interface. The top section, titled 'Notify', allows selecting notification destinations. A red circle (4) highlights the email address field. Below this, a grid of destination icons is shown, including ServiceNow incidents, Webhook, Jira, Slack, Email, AWS EventBridge, and PagerDuty. The 'Test workflow' button (8) is highlighted with a red box. Below the 'Test workflow' button, a message states: '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.' The bottom section, titled 'Email', shows the configuration for email notifications. It includes a search field for recipients, an 'Email subject' field with a placeholder '({ issueTitle })' (5), and a 'Custom Details (optional)' field. A 'Send test notification' button (6) is at the bottom left. The 'Activate workflow' button (9) is at the bottom right. Arrows indicate the flow from the 'Test workflow' button to the configuration panel and back to the 'Activate workflow' button.



ハンズオン(1-2) Workflowを作成する 5/6

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

Alerts & AI > Destinationsで、ご自身のメールアドレスが追加されていることを確認します。

The screenshot displays the 'Alerts & AI Destinations' page in the New Relic console. The left sidebar contains navigation links for 'ANALYZE', 'DETECT', 'CORRELATE', and 'ENRICH & NOTIFY'. The 'Destinations' link is highlighted. The main content area shows a list of available destinations to add, including Jira, ServiceNow, Slack, Webhook, PagerDuty, AWS EventBridge, and Mobile push. Below this, there is a 'Notifications Log Destinations (1)' section with a search bar and a table listing the existing destination.

Ty...	Name	Two...	URL/Details	Last updated	Updated by	Enabled	
	NRU304 メール通知サンプル		smitsui+nr304@newrelic.com	Jun 5, 2023 6:4...	1004932171	<input checked="" type="checkbox"/>	...



ハンズオン(1-2) Workflowを作成する 6/6

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

Alerts & AI Destinations

Add a destination
Add destinations where we send notifications.

Jira ServiceNow Slack Webhook PagerDuty AWS EventBridge Mobile push

Notifications Log Destinations (1)

Manage destinations where we send notifications.

Search

Type	Name	Two...	URL/Details	Last updated	Updated by	Enabled	
✉	NRU304 メール通知サンプル		smitsui+nru304@newrelic.com	Jun 5, 2023 6:4...	1004932171	<input checked="" type="checkbox"/>	⋮



Type	Name	Two...	URL/Details	Last updated	Updated by	Enabled	
✉	NRU304 メール通知サンプル		smitsui+nru304@newrelic.com	Jun 5, 2023 6:4...	1004932171	<input checked="" type="checkbox"/>	⋮

座学(3)

アラートコンディションの作成

16:00 - 16:15 (15min)

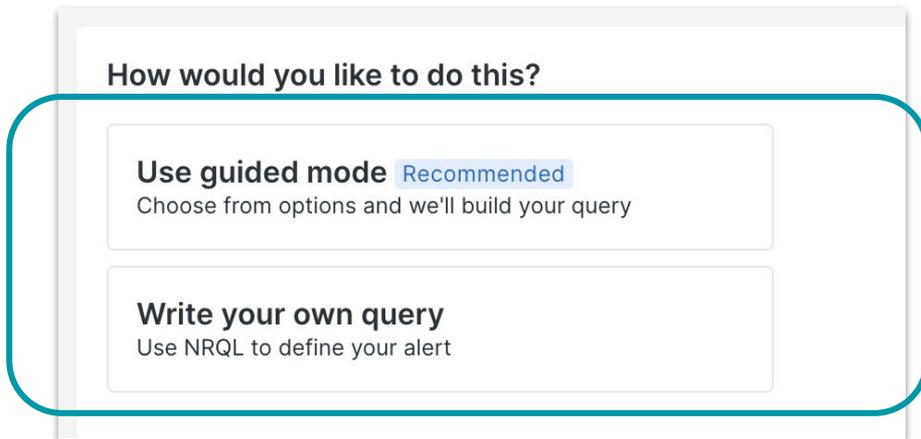


New Relic アラートの構成要素2: Alert Condition

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

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

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



How would you like to do this?

Use guided mode Recommended
Choose from options and we'll build your query

Write your own query
Use NRQL to define your alert

New Relic アラートの構成要素2: Golden signal or Metric

Golden Signalをベースにそれぞれの機能に合わせて、ガイド付きで簡単にアラート条件を作成

Tell us where to look ⓘ

<input type="checkbox"/> AWS (4 types)	<input type="checkbox"/> Browser applications	<input type="checkbox"/> Hosts
<input type="checkbox"/> On host integrations (2 types)	<input type="checkbox"/> Service Levels	<input checked="" type="checkbox"/> Services - APM
<input type="checkbox"/> Synthetic monitors	<input type="checkbox"/> VPC Networks	

▼ Select a metric to monitor

Golden metrics Other metrics

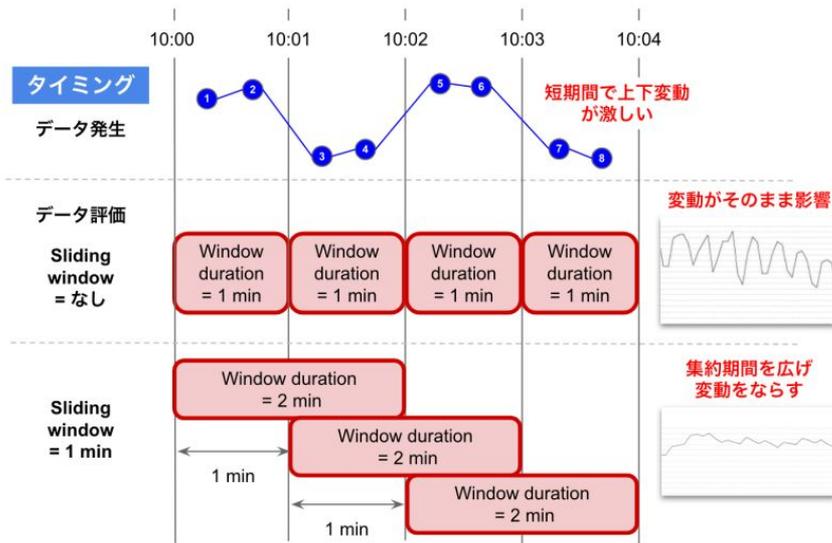
<input type="checkbox"/> Response time (ms)	<input type="checkbox"/> Throughput	<input type="checkbox"/> Error rate
---	-------------------------------------	-------------------------------------

機能毎に重要な監視項目を簡単に選択可能

Sliding Window(オプション)

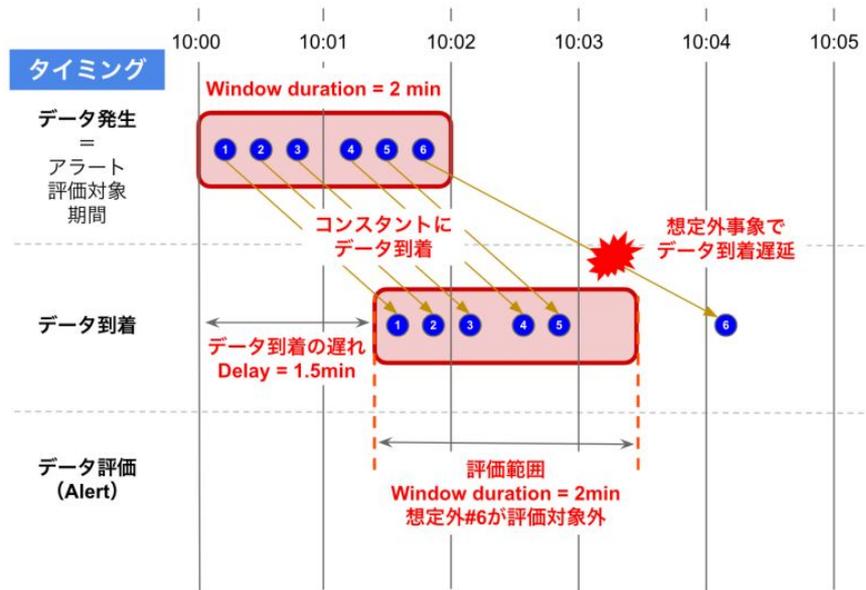
通常、集計ウィンドウの期間は互いに重なりません。

Sliding Windowオプションを有効にすると、指定した時間分スライドさせた複数の集計ウィンドウが並行して開かれるため、よりきめ細かい集計結果を得ることができます。



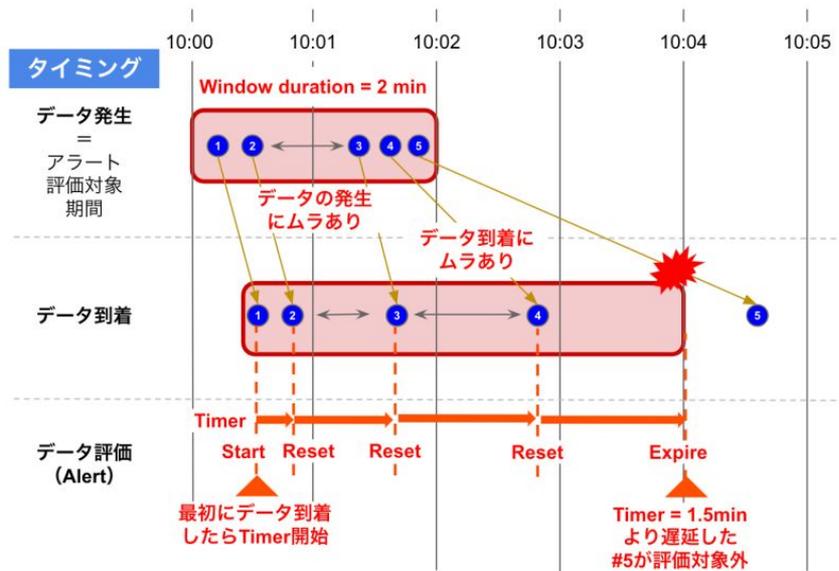
New Relic アラートの構成要素2: Streaming method

- Event Flow
頻繁かつ一定間隔で発生するデータに対するアラート設定に最適な方式です。
許容される遅延時間 (Delay) よりも後に続くデータが到着すると、集計ウィンドウが閉じられます。



New Relic アラートの構成要素2: Streaming method

- Event Timer
到着順序や発生間隔に一貫性のないデータを評価するのに最適な方式です。
集計ウィンドウ内のデータが最後に到着してからの時間経過によって、集計ウィンドウが閉じられます。



New Relic アラートの構成要素2: Streaming method

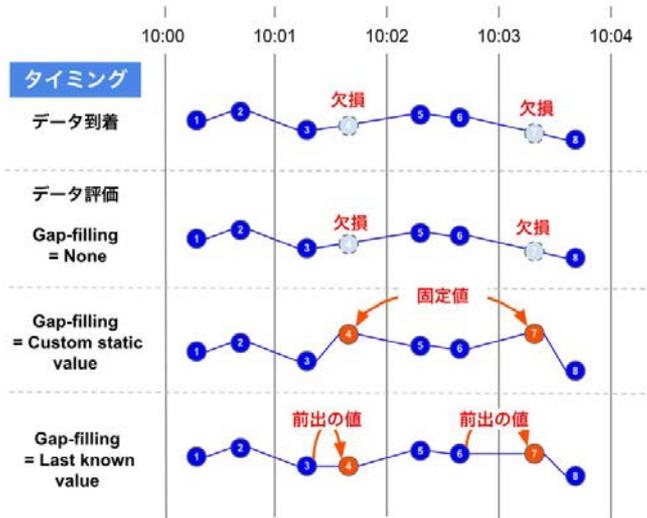
- Cadence
Cadenceは、データのタイムスタンプではなく、New Relic内部のシステムクロックに基づいて、一定の間隔で集計を行う方法です。多くのケースでは Event FlowまたはEvent Timerが適していますが、モバイル端末やブラウザから送信されるイベントのように、ユーザー端末の時刻設定に影響されて、タイムスタンプに一貫性がないデータを対象にする場合には、Cadenceが有効です。

補足: Gap-filling strategy

- Gap-filling strategy

集計結果が存在しない集計ウィンドウ(ギャップ)を検出した場合に0、任意の値、直前の集計結果のいずれかで、その期間の集計結果を埋めることができます。

ただし、集計結果が存在しないことを検出してギャップを埋めることができるのはNRQLクエリのWHERE句に該当する集計対象データが新たに到着したタイミングであり、集計対象データが存在しない状況をリアルタイムで検出して置換するものではない点に留意してください。



New Relic アラートの構成要素2: Alert Condition

アラートのしきい値設定は2種類から選択可能

種類	説明	アラートトリガー例
静的(Static)	ある特定の数値を上回った、または下回った場合にアラートをトリガー	エラー発生割合が5%を超過した
動的(Anomaly)	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2: Alert Condition

静的(Static) しきい値の超過を評価する方法

- **For at least xx minutes**

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

- **at least once in xx minutes**

xx分間で、しきい値を1回でも超過した場合に、Incidentが起票される

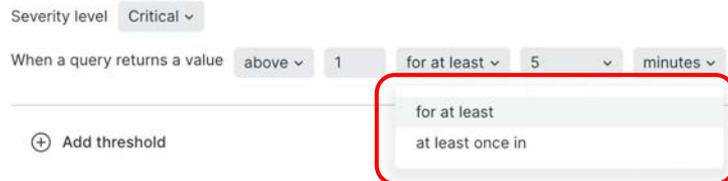
一つのAlert Conditionには、CriticalとWarning(オプション)の閾値を設定可能

その他、アラート設定に関する詳細は以下もご参照ください:

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

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

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



New Relic アラートの構成要素2: Alert Condition

効果的な通知を送るためのプラクティス

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

Send a custom incident description (optional) ⓘ

4,000 character limit

Runbook URL (optional)

Enable on save

ハンズオン(2) アラートコンディションを 作成

16:15 - 16:30 (15min)





ハンズオン(2-1) Alert Conditionを作成する 1/21

- 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. フロントエンド: ページロード時間
2. 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)
3. アプリケーション: 応答時間(動的)
4. 外形監視:チェックエラー



ハンズオン(2-1) Alert Conditionを作成する 2/21

画面遷移(一部スキップあり)のヒント

- **新規Alert Conditionの追加**

- ① **フロントエンド: ページロード時間**

- 1. Add alerts**

- a. Use guided mode

- 2. Tell us what where to look**

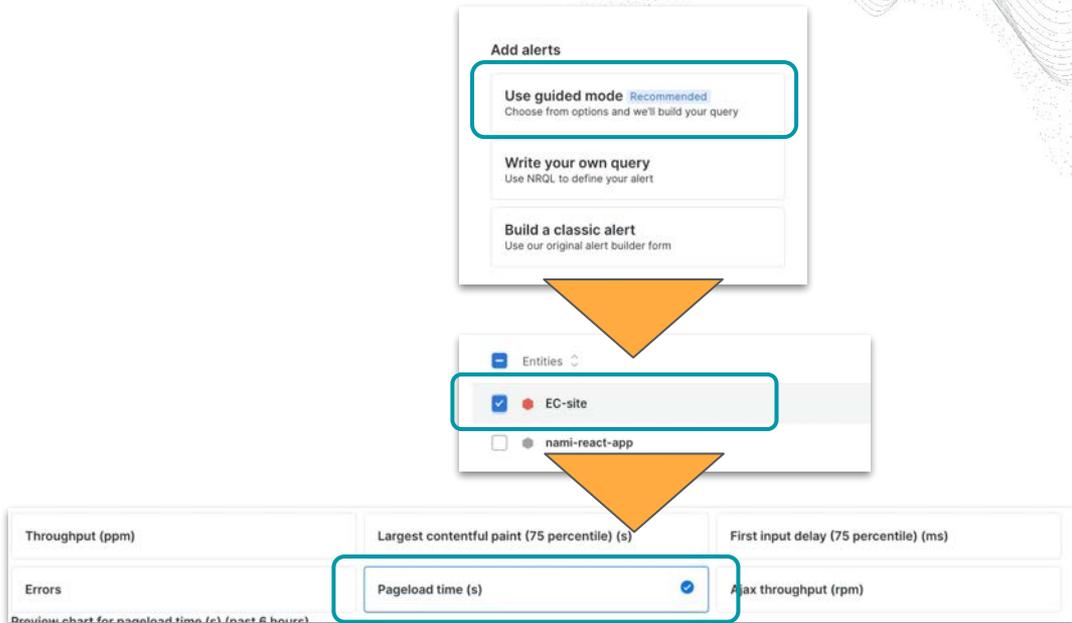
- a. Browser applications

- 3. Tell us what to watch**

- a. EC-site

- 4. Select a metric to monitor**

- a. Pageload time(s)



Condition名は適切なものを各自設定してください

(例:NRU304-yourname-NRQL-pageloadtime)



ハンズオン(2-1) Alert Conditionを作成する 3/21

1. Alerts&AI メニューを開きます。
2. Alert Policies を開きます。
3. 前のハンズオンセクションで作成したポリシーを選択します。
4. 画面右側にある [+New alert condition] を選択して、新しい Alert Condition を作成します。

The screenshot shows the New Relic Alerts & AI interface. The left sidebar has 'Alerts & AI' highlighted (1). The main area shows 'Alert Policies' (2) with a table of policies. One policy is selected (3). A callout box (4) highlights the '+ New alert condition' button.

Name	Open issues	# of conditions	
NRU-Sample-Policy	0	4	...
Service Levels default policy for account 3940716	1	1	...
これがあなたのポリシーです。	0		
ダッシュボードハンズオン用アラートポリシー	1		



ハンズオン(2-1) Alert Conditionを作成する 4/21

- 「Browser applications」を選択し、設定画面を進みます。

Tell us where to look ⓘ

AWS (4 types)	Browser applications	Hosts
On host integrations (2 types)	Service Levels	Services - APM
Synthetic monitors	VPC Networks	



ハンズオン(2-1) Alert Conditionを作成する 5/21

- 「EC-site」、「Pageload time(s)」を選択し「Next」をクリックします。

Tell us what to watch

Select the entities to watch (max 20)

Search entities by name or attributes. If you create new entities with these attributes, we'll watch those as well.

All Selected 1

Filter by name or tags

Entities

- EC-site
- nami-react-app

Select a metric to monitor

Golden metrics Other metrics

Throughput (ppm)	Largest contentful paint (75 percentile) (s)	First input delay (75 percentile) (ms)
Errors	Pageload time (s) <input checked="" type="checkbox"/>	Ajax throughput (rpm)

Preview chart for pageload time (s) (past 6 hours)

Cancel **Next**



ハンズオン(2-1) Alert Conditionを作成する 6/21

- 監視設定は次のようにしてください。
 - 1. Window Duration**
 - a. 1 minutes
 - 2. Streaming method**
 - a. Event flow
 - 3. Delay**
 - a. 2minutes
 - 4. Severity level**
 - a. Critical
 - 5. When a query returns a value**
 - a. above 1 for at least 5 minutes



ハンズオン(2-1) Alert Conditionを作成する 7/21

- それぞれ 設定を確認し「Next」をクリック。

The screenshot shows the configuration interface for an alert condition, divided into two main sections: "Fine-tune your signal" and "Set condition thresholds".

Fine-tune your signal

- Data aggregation**
 - Window duration: 1 minutes (callout 1)
 - Use sliding window aggregation:
 - Streaming method: Event flow, Event timer, Cadence (callout 2)
 - Delay: 2 minutes (callout 3)
- Gap filling strategy**
 - Fill data gaps with: None
- Evaluation delay**
 - Use evaluation delay:

Set condition thresholds

- Static / Anomaly
- Open incidents with a: Severity level: Critical (callout 4)
- When a query returns a value: above 1 for at least 5 minutes (callout 5)
- + Add threshold
- + Add lost signal threshold

At the bottom right, there are "Cancel" and "Next" buttons, with the "Next" button highlighted by a red box (callout 5).



ハンズオン(2-1) Alert Conditionを作成する 8/21

- コンディション名にわかりやすい名前を入力し、「 Save condition」をクリックする。

Add details

Name your alert condition *

Use a clear name that indicates what's wrong

Close open incidents after 3 days

Send a custom incident description (optional)

4,000 character limit

Runbook URL (optional)

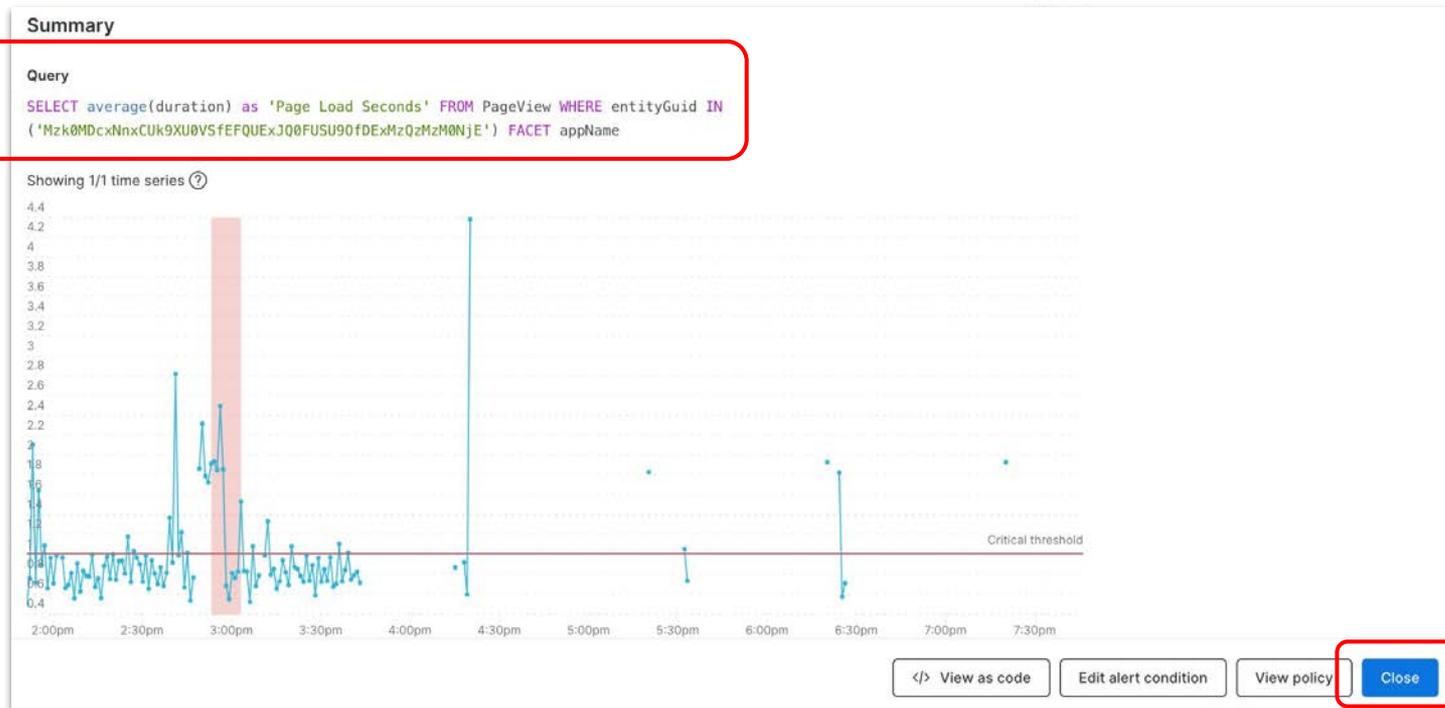
https://

Enable on save

Cancel </> View as code **Save condition**

ハンズオン(2-1) Alert Conditionを作成する 9/21

- Summaryページが開き、Queryの内容やチャートが表示されます。「Close」をクリックします。





ハンズオン(2-1) Alert Conditionを作成する 10/21

- 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。

The screenshot shows the New Relic Alert Policies interface. The top navigation bar includes "Alerts & AI / Alert Policies" and a search bar. Below the navigation, there are tabs for "Alert conditions", "Notifications", and "Settings". A search bar is present with the text "Search by condition name or id" and a filter dropdown set to "Condition Name = All". Below the search bar, it says "Showing 1 condition". A table displays the details of the alert condition:

Alert condition	Query	Thresholds	Type	Open issues	Enabled
とってもわかりやすいコンディション名	SELECT average(duration) as 'P...	Critical: above 1 for 5 minutes Create a warning threshold	NRQL Query	...	On



ハンズオン(2-1) Alert Conditionを作成する 11/21

- **新規Alert Conditionの追加**

②アプリケーション: 4xx,5xxエラー(ホストごとに評価)

1. **Categories**

- a. NRQL

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

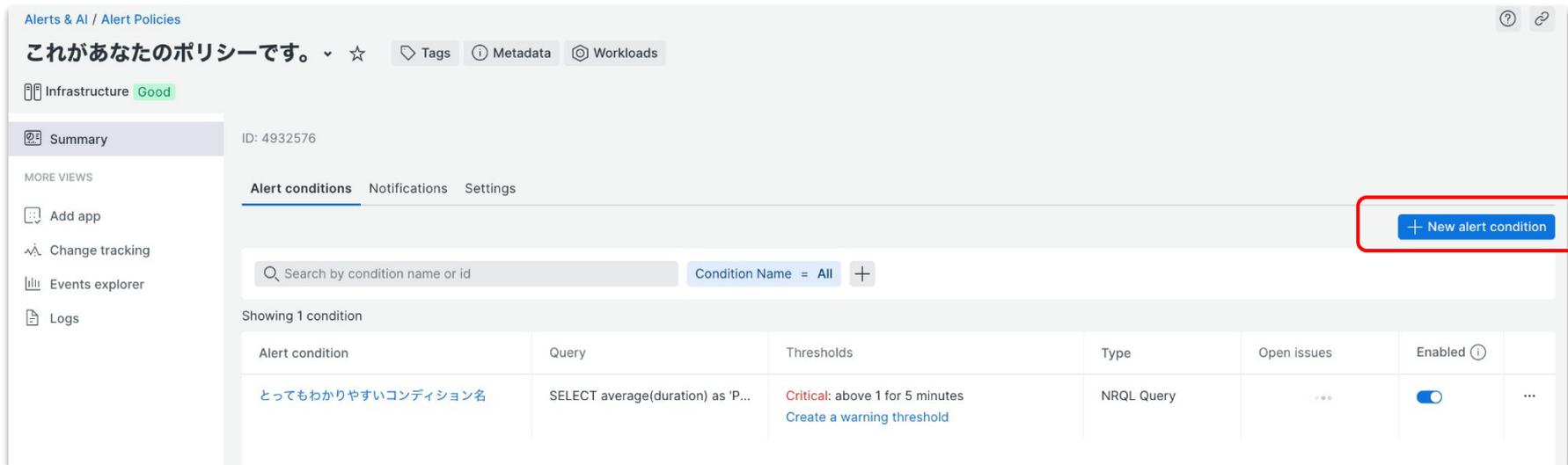
```
SELECT percentage(count(*), WHERE httpResponseCode >= '400') FROM Transaction FACET host
```

Condition名は適切なものを各自設定してください

(例:NRU304-yourname-NRQL-ErrorResponse)

ハンズオン(2-1) Alert Conditionを作成する 12/22

- 作成したポリシー内にて「+ New alert condition」をクリックする。



The screenshot displays the New Relic Alert Policies management interface. At the top, it shows the breadcrumb 'Alerts & AI / Alert Policies' and a header 'これがあなたのポリシーです。' (This is your policy). Below this, there are tabs for 'Tags', 'Metadata', and 'Workloads'. The main content area is titled 'Alert conditions' and includes a search bar and a filter 'Condition Name = All'. A table lists one alert condition with the following details:

Alert condition	Query	Thresholds	Type	Open issues	Enabled
とってわかりやすいコンディション名	SELECT average(duration) as 'P...	Critical: above 1 for 5 minutes Create a warning threshold	NRQL Query	...	<input checked="" type="checkbox"/>



ハンズオン(2-1) Alert Conditionを作成する 13/21

- 右側からスライドして表示される Add alerts画面から「Write your own query」を選択する。
- クエリ入力欄に次のNRQLクエリをコピー&ペーストして、Runをクリックします。

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

- クエリ実行後、直近の状態を示す参考チャートが表示されることを確認し、Nextをクリックする。

Query the data you want to monitor

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

Clear Run

See our docs for help with null values, loss of signal, or other query options.

Showing 1/1 time series

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

Critical threshold

2:30pm 3:00pm 3:30pm 4:00pm 4:30pm 5:00pm 5:30pm 6:00pm 6:30pm 7:00pm 7:30pm 8:00pm

Cancel Next



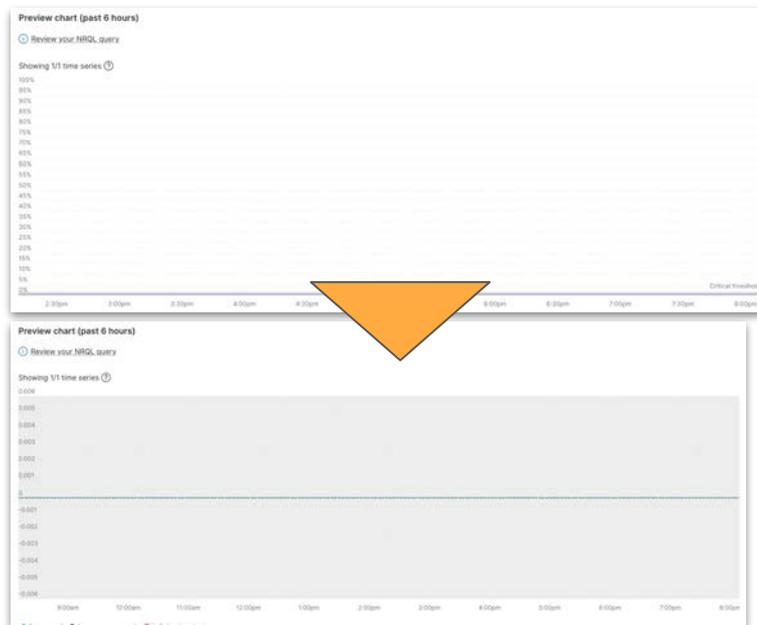
ハンズオン(2-1) Alert Conditionを作成する 14/21

- Fine-tune your signalはすべて初期値のままNextをクリックします。
- 補足: もし時間がある場合は、閾値条件の設定項目にある「Static」を「Anomaly」に変更した場合、チャートがどのように変更されるかを確認してください。

Set condition thresholds

Static ⓘ Anomaly ⓘ

Open incidents with a:





ハンズオン(2-1) Alert Conditionを作成する 15/21

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

Add details

Name your alert condition *

とってわかりやすいコンディション名

Close open incidents after 3 days

Send a custom incident description (optional)

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

4,000 character limit

Runbook URL (optional)

https://www.yahoo.co.jp

Enable on save

Cancel </> View as code Save condition

Enable on save



ハンズオン(2-1) Alert Conditionを作成する 16/21

- **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. NRQL

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

```
From Transaction SELECT average(duration) WHERE appName ='EC-site'
```

Condition名は適切なものを各自設定してください

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

ハンズオン(2-1) Alert Conditionを作成する 17/21

- 右側からスライドして表示される Add alerts画面から「Write your own query」を選択する。
- クエリ入力欄に次のNRQLクエリをコピー&ペーストして、Runをクリックします。

*From Transaction SELECT average(duration)
WHERE appName = 'EC-site'*

- クエリ実行後、直近の状態を示す参考チャートが表示されることを確認し、Nextをクリックする。

The screenshot displays the 'Add alerts' configuration page in New Relic. It features three main options: 'Use guided mode' (recommended), 'Write your own query', and 'Build a classic alert'. The 'Write your own query' option is selected and highlighted with a red box. Below this, the NRQL query `From Transaction SELECT average(duration) WHERE appName = 'EC-site'` is entered into a text field, also highlighted with a red box. To the right of the query field is a 'Run' button, also highlighted with a red box. Below the query field, there is a line chart showing the average duration of transactions over time. The chart has a y-axis from 0 to 1.2 and an x-axis from 10:00am to 3:30pm. A horizontal red line represents the 'Critical threshold' at approximately 1.1. A vertical red bar indicates a 'Critical incident' at 3:00pm. The legend at the bottom identifies the blue line as 'Avg Duration', the red line as 'Critical threshold', and the red bar as 'Critical incident'. At the bottom right of the chart area, there are 'Cancel' and 'Next' buttons, with the 'Next' button highlighted by a red box.

ハンズオン(2-1) Alert Conditionを作成する 18/21

- Set condition thresholdsの閾値のタイプをStaticからAnomalyに変更する。
 - Fine-tune your signalの値は初期値のままにする。
- これまでの手順同様「Save condition」で保存する。
 - もし時間の余裕がある場合、「XXX standard deviation(s)」のXXXの値を変えることで、上部のチャートがどのように表示を変えるかを確認してください。

Set condition thresholds

Static ⓘ Anomaly ⓘ

Threshold direction Upper and lower ▾

Open incidents with a:

Severity level Critical ▾

When a query returns a value outside the threshold

by 3 standard deviation(s) for at least 5 minutes ↻

More incidents Fewer incidents

+ Add threshold

+ Add lost signal threshold

Cancel **Next**



ハンズオン(2-1) Alert Conditionを作成する 19/21

- **新規Alert Conditionの追加**

- ④ 外形監視:チェックエラー

1. **Categories**

- a. NRQL

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

```
FROM SyntheticCheck SELECT filter(count(*), WHERE result = 'FAILED')  
WHERE monitorName ='NRU304-Synthetic Check'
```

Condition名は適切なものを各自設定してください

(例:NRU304-yourname-synthetics-check)

ハンズオン(2-1) Alert Conditionを作成する 20/21

- 右側からスライドして表示される Add alerts画面から「Write your own query」を選択する。
- クエリ入力欄に次の NRQLクエリをコピー&ペーストして、Runをクリックします。

```
FROM SyntheticCheck SELECT filter(count(*),  
WHERE result = 'FAILED') WHERE monitorName  
='NRU304-Synthetic Check'
```

- クエリ実行後、直近の状態を示す参考チャートが表示されることを確認し、Nextをクリックする。

Add alerts

Use guided mode **Recommended**
Choose from options and we'll build your query

Write your own query
Use NRQL to define your alert

Build a classic alert
Use our original alert builder form

FROM SyntheticCheck SELECT filter(count(*), WHERE result = 'FAILED') WHERE monitorName = 'NRU304-Synthetic Check'

Clear Run

See our docs for help with null values, loss of signal, or other query options.

2
1.8
1.6
1.4
1.2
1
0.8
0.6
0.4
0.2
0

10:30am 11:00am 11:30am 12:00pm 12:30pm 1:00pm 1:30pm 2:00pm 2:30pm 3:00pm 3:30pm 4:00pm

● result = 'FAILED' ● Critical threshold

Cancel Next



ハンズオン(2-1) Alert Conditionを作成する 21/21

- Set condition thresholdsの閾値条件を変更する。
 - Fine-tune your signalの値は初期値のままにする。
 - 右側のサンプルを参考にして変更する。
 - Above or equal toの適用
 - At least once inの適用
- これまでの手順同様「Save condition」で保存する。

Set condition thresholds

Static ⓘ Anomaly ⓘ

Open incidents with a:

Severity level **Critical** ▾

When a query returns a value

above or equal to ▾ 1 **at least once in** ▾ 5 ▾ minutes ▾

Next

参考：該当しない状態を「0」として扱いたい場合

アラート条件の評価が行われるのは、クエリのWhere句に該当する値が発生した場合です。

そのためWhere句で絞り込んだ結果が0件の場合はデータなし(NULL)扱いとなりアラート条件として評価されません。

例えば全てのresultが'SUCCESS'だった場合、以下のクエリでは「該当データなし」となります。アラートとして通知できませんが、復旧判定ができず状況によっては適切に通知できない場合があります。

```
FROM SyntheticCheck SELECT count(*)  
WHERE result = 'FAILED' AND monitorName = 'NRU304-Synthetic Check'
```

その場合filter関数の中で絞り込むことで評価対象にすることができます

```
FROM SyntheticCheck SELECT filter(count(*), WHERE result = 'FAILED')  
WHERE monitorName = 'NRU304-Synthetic Check'
```

参考：[Example: null value returned](#)

ハンズオン(3) 発生したアラートの確認

16:30 - 16:40 (10min)





手順・解説

ハンズオン(3-1) 個々のアラートを確認する 1/3

- [Alerts & AI] > [Issues & Activity] > [Incidents]タブをクリックします。

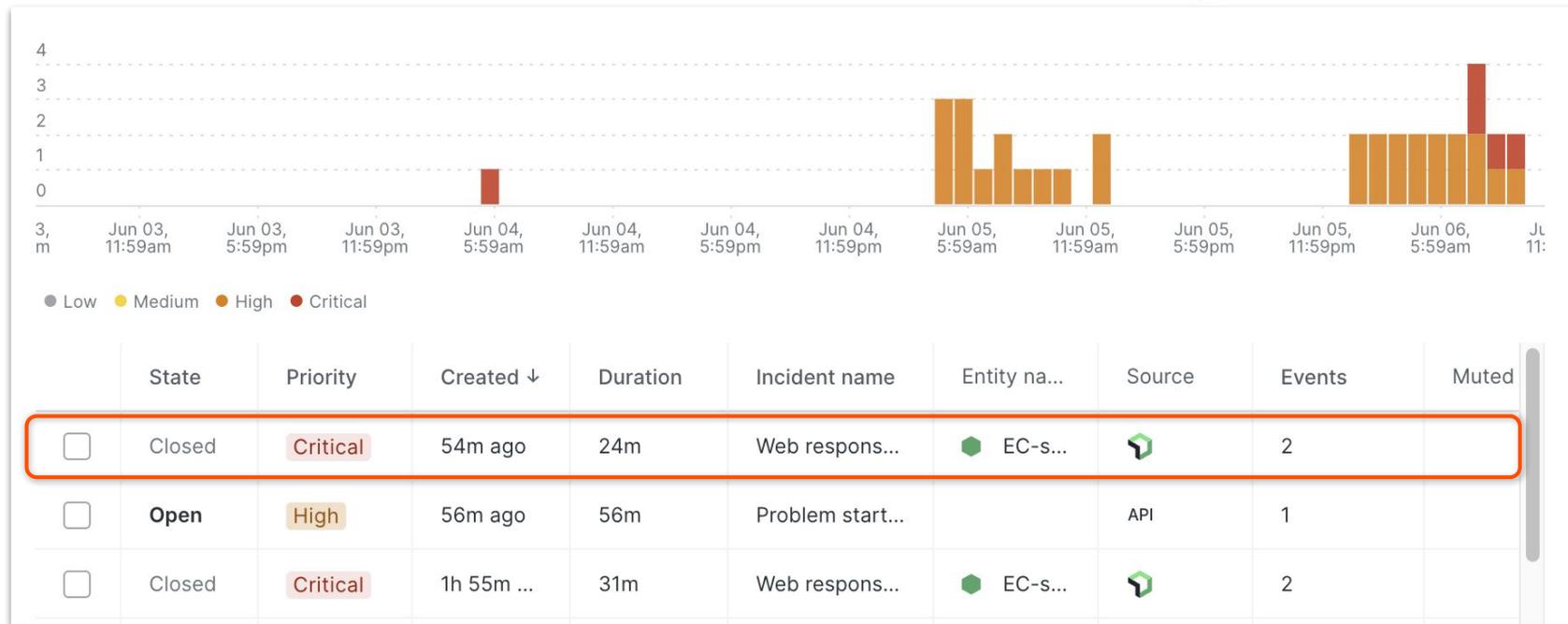
The screenshot displays the New Relic dashboard. On the left sidebar, the 'Alerts & AI' menu item is highlighted with an orange box. In the main content area, the 'Issues & Activity' section is active, and the 'Incidents' tab is also highlighted with an orange box. Below the navigation, a bar chart shows incident counts over time, with a peak at 4:29pm. A table below the chart lists incident details.

State	Priority	Created ↓	Duration
Open	Critical	16m ago	16m



ハンズオン(3-1) 個々のアラートを確認する 2/3

- Incidentをクリックします。





ハンズオン(3-1) 個々のアラートを確認する 3/3

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

The screenshot displays the New Relic alert interface. On the left, a line graph titled "Web response time deviated from the baseline at least once in 5 minutes on 'EC-site'" shows a spike in response time between 12:20 PM and 12:40 PM. The y-axis ranges from -1k to 2.5k. Below the graph is an "Analysis" section with "Attributes" and "Anomalies" subsections, both indicating no further details were found.

The central "Incident details" panel for "EC-site" includes the following information:

- Type: Account
- Application: NewRelicUniversity-Japan
- Incident details:
 - Condition: Web transaction time (Baseline)
 - Policy: test deleteeme
 - Issue: Policy: 'test deleteeme'. Condition: 'テスト太郎さんのEnd User Apex (Low)'
- View incident payload (highlighted with a red box)
- Tags (8):
 - accountid: 2511671 language: php
 - instrumentation.name: apm nr.has_slis: true
 - trustedAccountid: 2490334 slug: lixi-lvm1-ya6i8pf
 - account: NewRelicUniversity-Japan
 - instrumentation.provider: newRelic

An orange arrow points from the "View incident payload" link to a table on the right titled "Incident accumulation". This table lists various keys and their values:

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

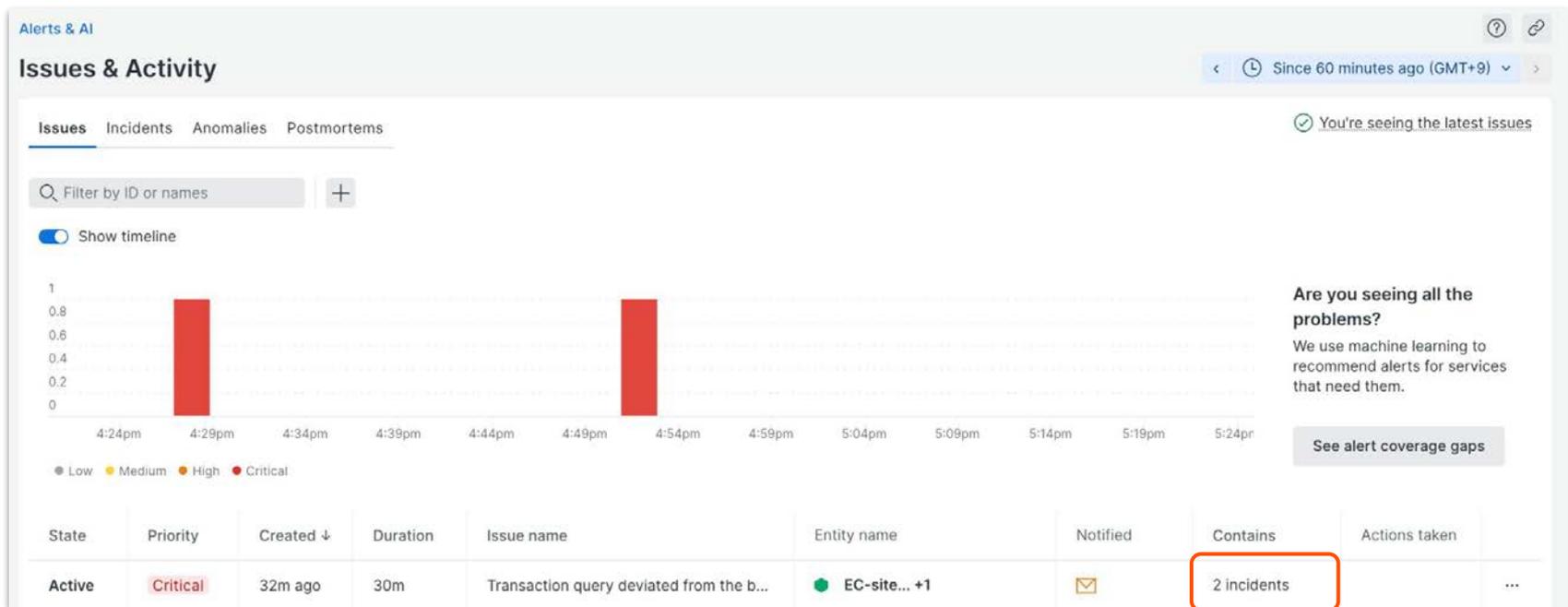
ハンズオン(3-2) 複数のアラートを紐付け トラブルシューティングに役立てる 1/5

- [Alerts & AI] > [Issues & Activity] > [Issues]タブをクリックします。

The screenshot displays the New Relic web interface. On the left is a dark sidebar with the 'new relic' logo at the top. Below the logo are various navigation items: 'Quick Find', 'Add Data', 'All Capabilities', 'All Entities', 'Query Your Data', 'APM & Services', 'Dashboards', 'Logs', 'Alerts & AI' (highlighted with an orange box), 'Metrics & Events', 'Infrastructure', 'Synthetic Monitoring', and 'Service Levels'. The main content area is divided into sections: 'ANALYZE' with 'Issues & Activity' (highlighted with an orange box) and 'Overview'; 'DETECT' with 'Alert Conditions & Policies', 'Alert Conditions' (marked 'New'), 'Alert Policies' (marked 'New'), 'Anomaly Detection', and 'Alert Coverage G...' (marked 'Beta'); and 'CORRELATE' with 'Sources' and 'Decisions'. Below these is an 'ENRICH & NOTIFY' section. The right-hand pane is titled 'Alerts & AI' and 'Issues & Activity'. It features tabs for 'Issues' (highlighted with an orange box), 'Incidents', 'Anomalies', and 'Postmortems'. Below the tabs is a search bar 'Filter by ID or names' and a 'Show timeline' toggle. A bar chart shows a single red bar representing a critical issue between 4:29pm and 4:31pm. A legend below the chart identifies priority levels: Low (grey), Medium (yellow), High (orange), and Critical (red). At the bottom, a table header is visible with columns for 'State', 'Priority', 'Created ↓', 'Duration', and 'Issue name'.

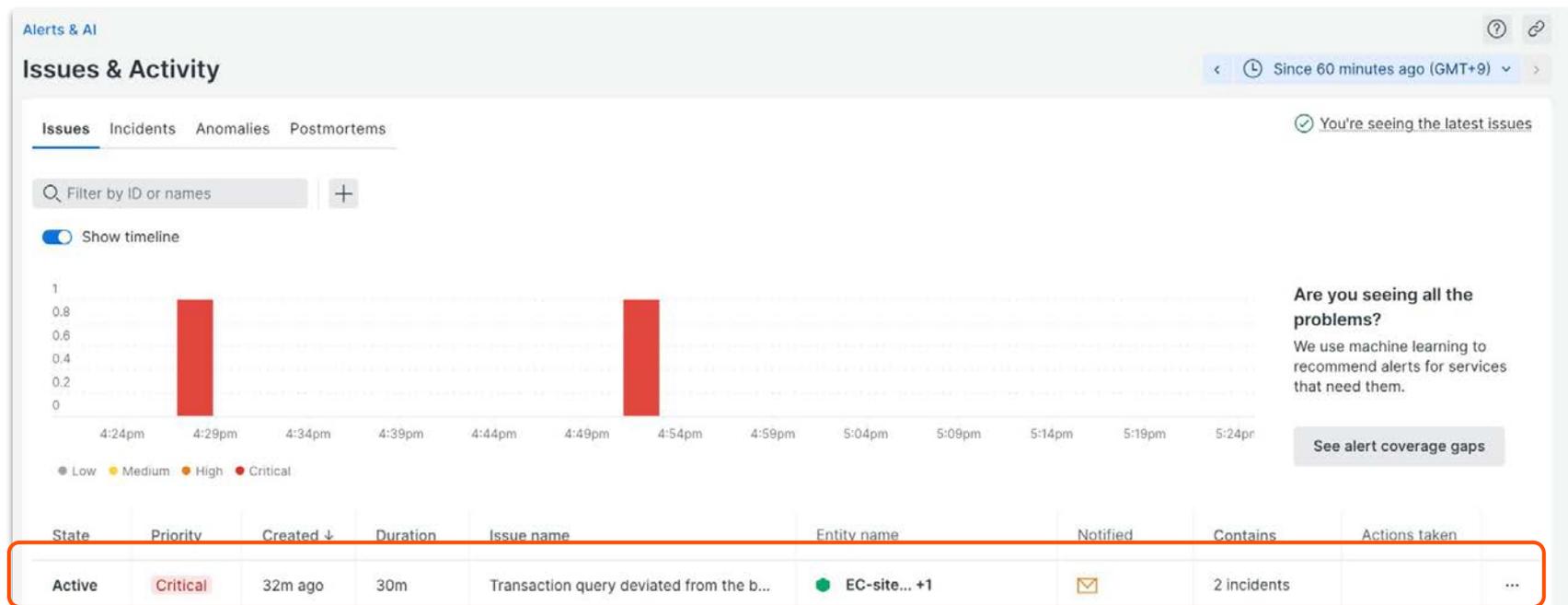
ハンズオン(3-2) 複数のアラートを紐付け トラブルシューティングに役立てる 2/5

- 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(3-2) 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 3/5

- Issueをクリックすると詳細が表示されます。





ハンズオン(3-2) 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 4/5

- どのIncidentがまとめられているのか確認することができます

The screenshot displays the New Relic incident management interface. At the top, a critical incident is shown with the title "Transaction query deviated from the baseline for at least 5 minutes on '非常にわかりやすいコンディション名を設定する'". Below this, a list of incidents is shown, with two incidents highlighted in a red box:

- Incident 1:** Critical, Open. Title: "NRU304-Synthetic Check query result is >= 1.0 on '少し複雑なコンディション名'". Opened: Today 5:01pm. Duration: 28m.
- Incident 2:** Critical, Closed. Title: "Transaction query deviated from the baseline for at least 5 minutes on '非常にわかりやすいコンディション名を設定する'". Opened: Today 4:53pm. Duration: 24m.

To the right of the incident list, a "Signal over time" chart is displayed. The chart shows a signal that remains at 0 until approximately 4:55pm, then spikes to 1.0 at 5:00pm and remains there until 5:10pm. The chart is titled "NRU304-Synthetic Check query result is >= 1.0 on '少し複雑なコンディション名'". Below the chart, the incident details for "NRU304-Synthetic Check" are shown, including tags and account information.

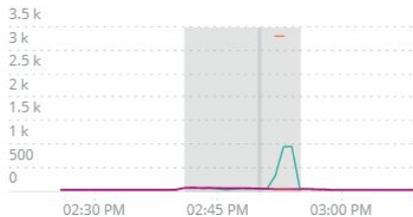
ハンズオン(3-2) 複数のアラートを紐付け トラブルシューティングに役立てる 5/5

- 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

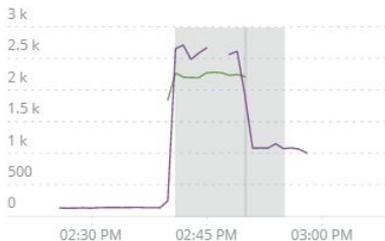
● Web response time > 2 seconds at least once in 5 minutes on 'EC-site' Critical

Attributes to investigate ?

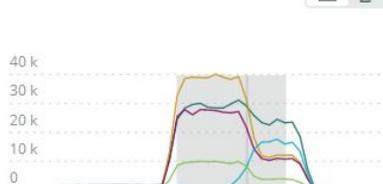
Average database duration (ms) faceted by
Datastore type and Table and Operation



Web response time faceted by
request.headers.accept



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



Root cause analysis

Deployment events (1)

1 Deployments

Last 12h

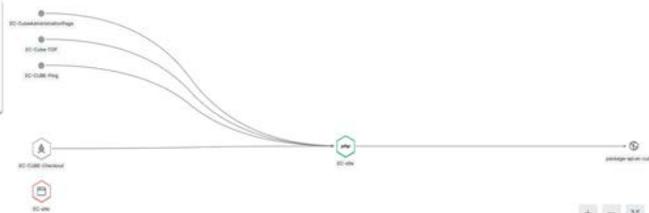
▲ Deployment 22m before issue created
Application: EC-site
Deployer: Systems Manager | Revision: ec-cube-4

Possible cause Due to proximity to issue creation

Impacted entities (3)

EC-site
EC-site

Show
Related entities
Externals
Entities
Related entity
External Service



Issue timeline

ISSUE LOG

3 INCIDENTS 3 Resolved





ハンズオン(3-3) 届いたメール通知を確認する

- 通知されたEmailからIssueの詳細など、確認に役立つ情報が表示されます

The screenshot shows an email notification from New Relic. At the top, it says "new relic". Below that, a red banner indicates "Critical priority issue is active". The main message is "NRU304-Synthetic Check query result is ≥ 1.0 on 'Synthetics'". There are three buttons: "Acknowledge", "Close issue", and "Go to issue". Below this, there is a section for "1 correlated issues" with a sub-header "We've used correlation to merge new issues into your active issue" and a bullet point: "Transaction query deviated from the baseline for at least 5 minutes on 'NRU304-baseline'". The next section is "3 incidents", with a bullet point: "NRU304-Synthetic Check query result is ≥ 1.0 on 'Synthetics'". Below this is a bar chart titled "Since 34 minutes ago until 4 minutes ago" showing a value of 1.0 from 4:37:00am to 4:38:00am. The x-axis has labels: 4:37:00am, 4:37:15am, 4:37:30am, 4:37:45am, 4:38:00am. The y-axis has labels: 0, 0.5, 1. Below the chart is another bullet point: "Transaction query deviated from the baseline for at least 5 minutes on 'NRU304-baseline'".



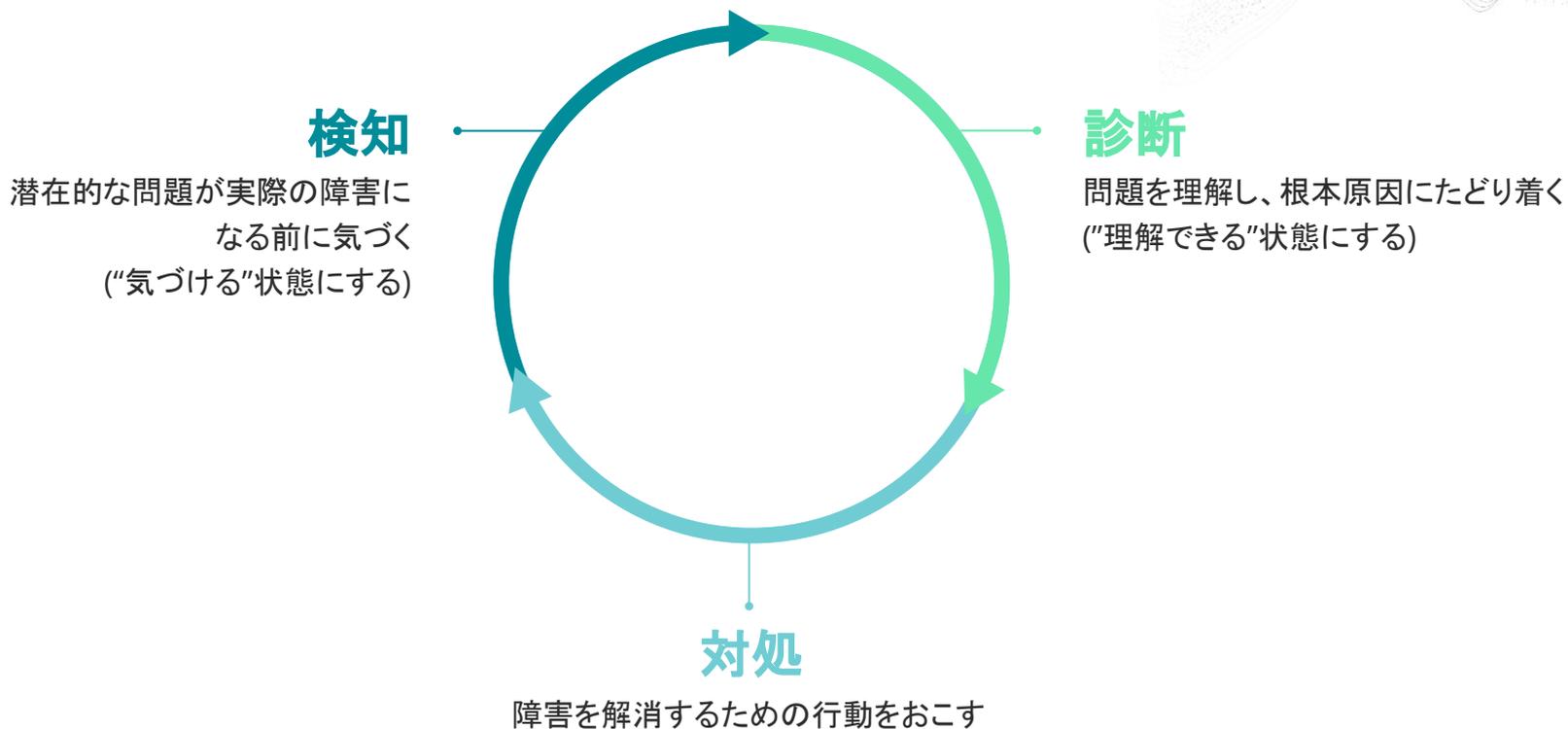
座学(4)

New Relicのアラート分析支援機能と AIOpsを使った異常検知

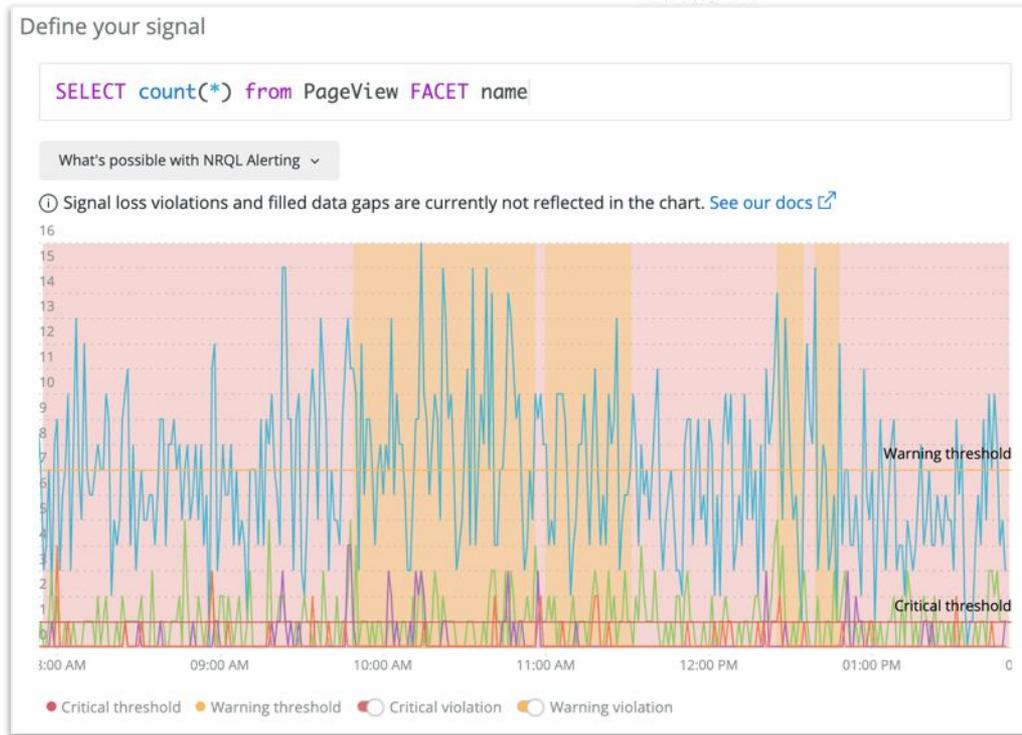
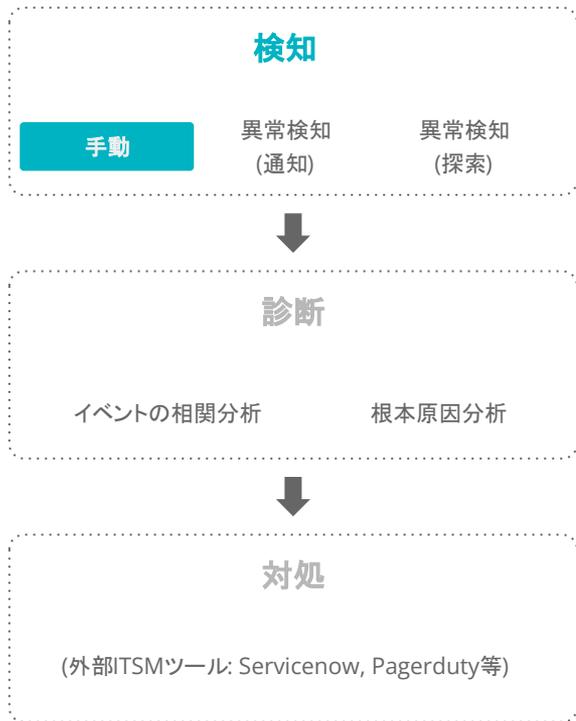
16:40 - 16:55 (15min)



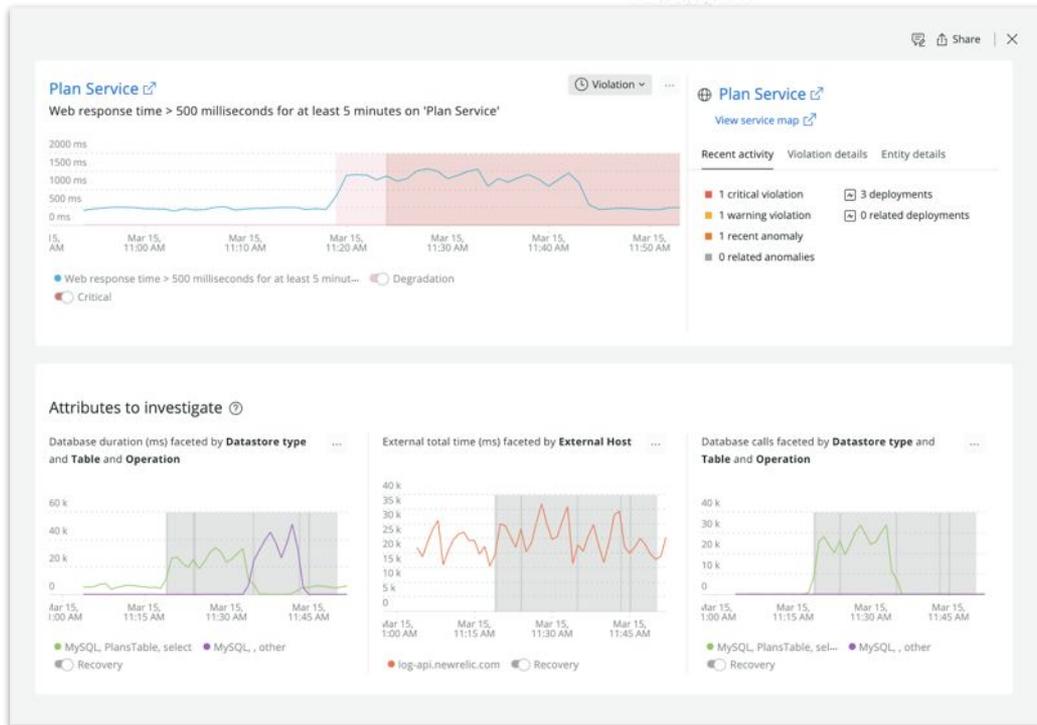
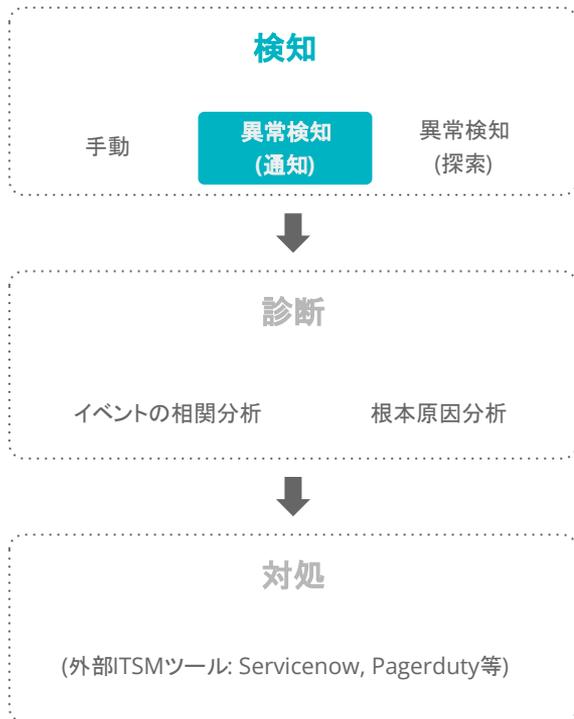
New Relic AIOpsによるインシデント対応フロー



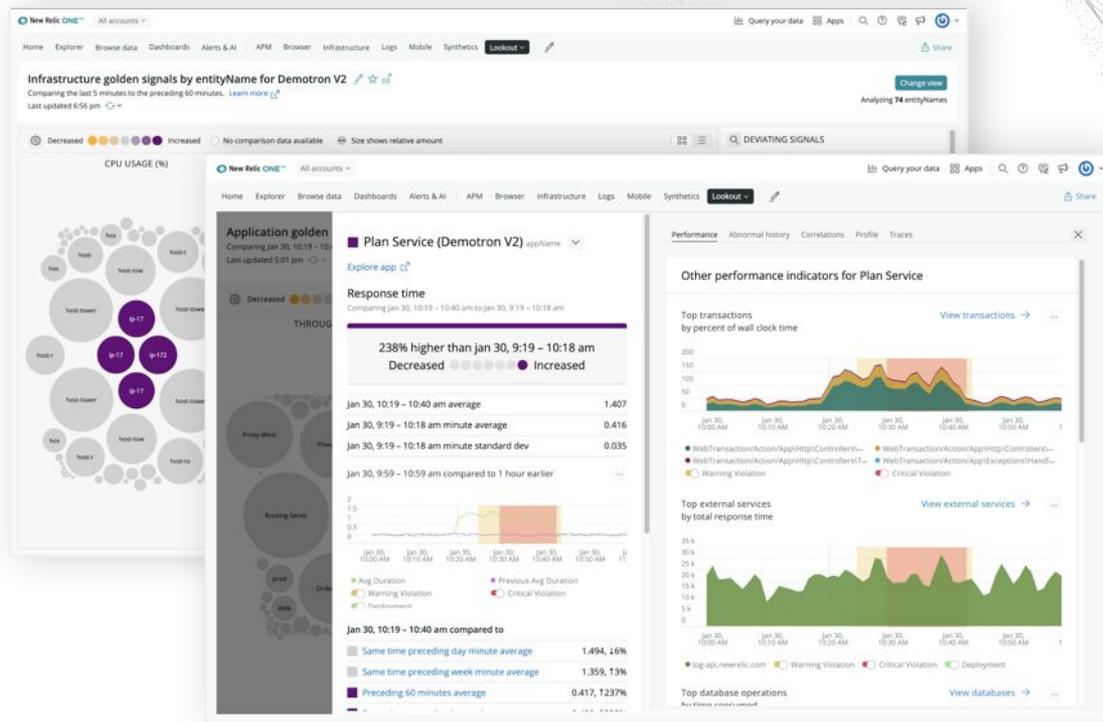
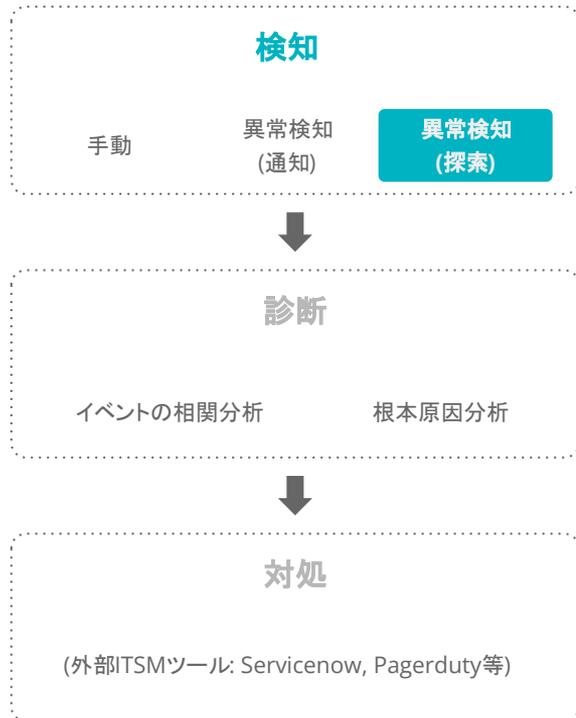
検知1: 重要な指標に対する手動アラートによる気づき



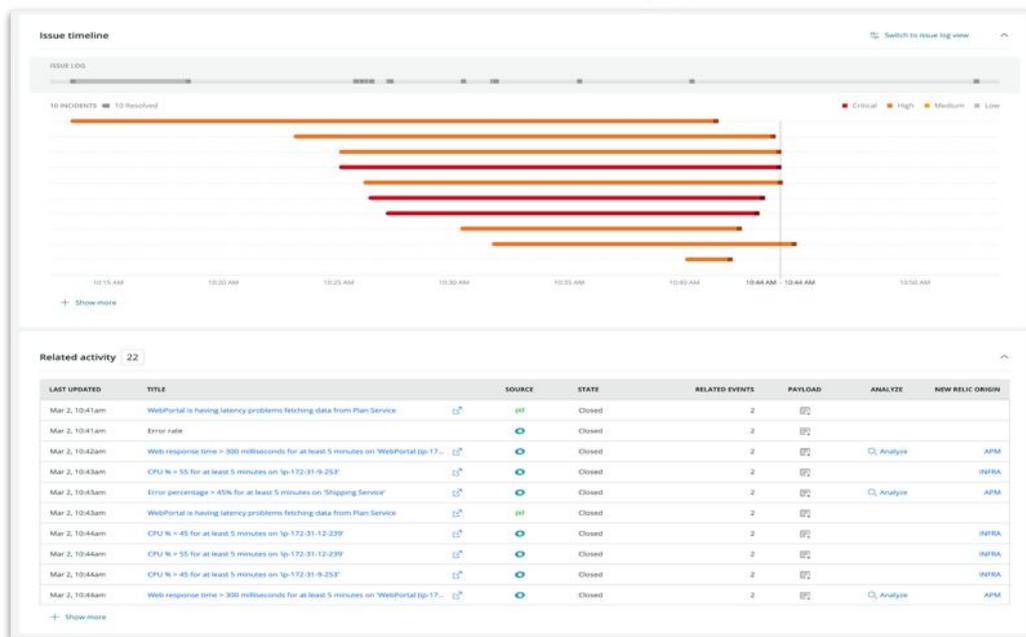
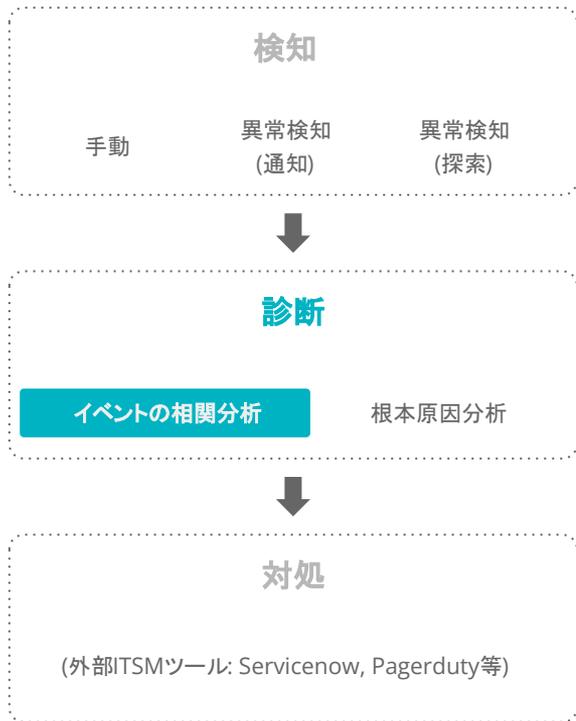
検知2: Anomaly Detectionによる異常の通知



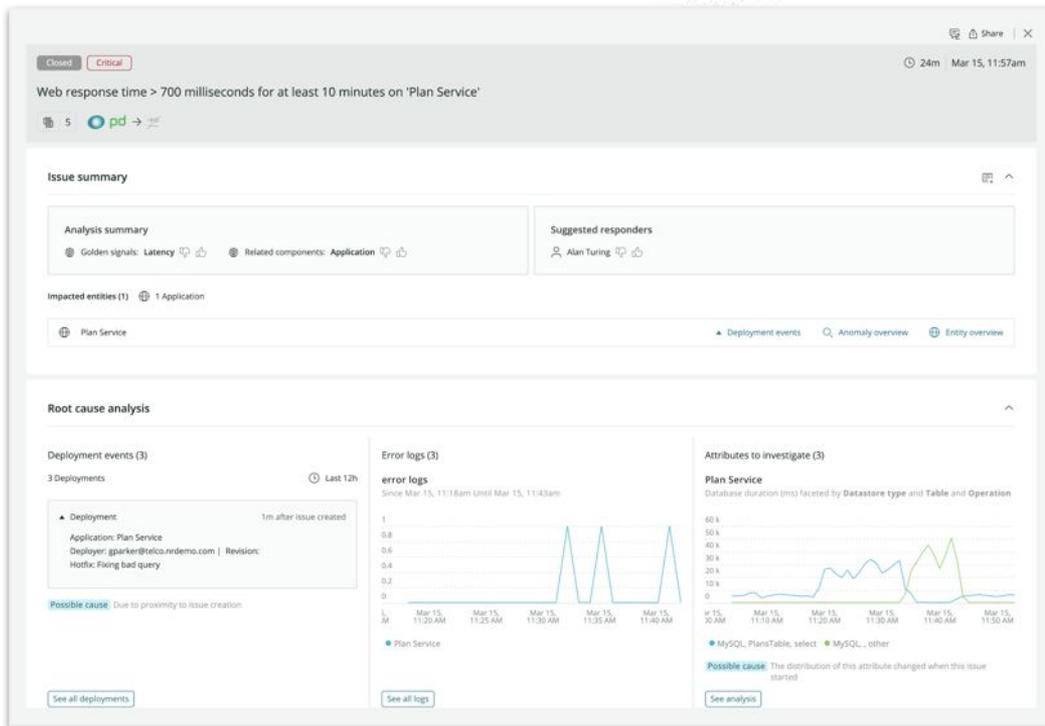
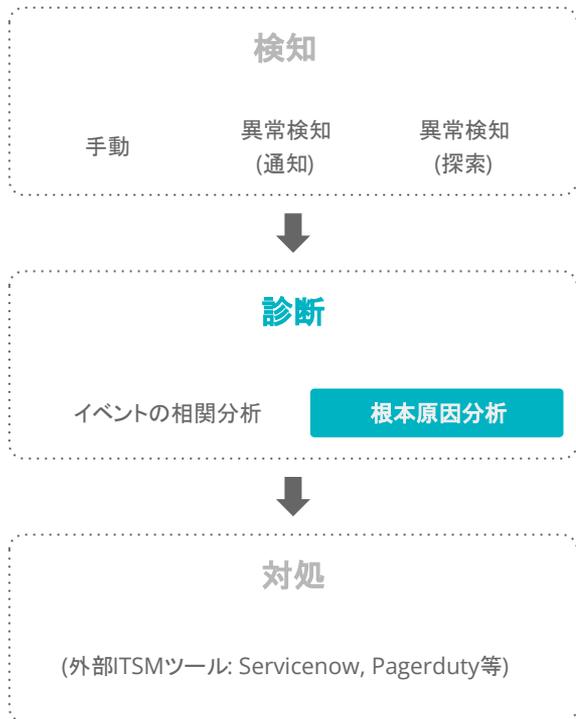
検知3: Lookoutによる異常の可視化と探索



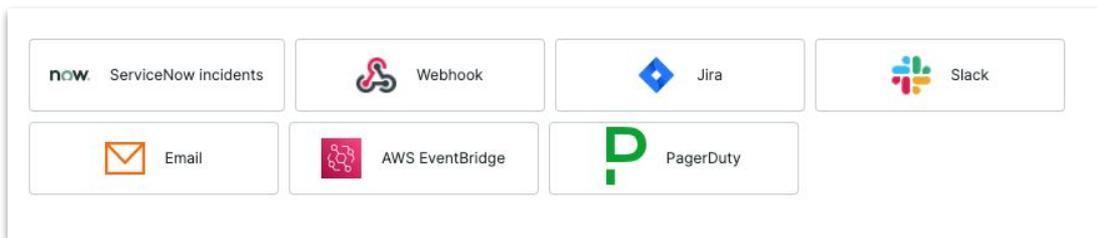
診断1: Correlationによるアラート統合とノイズの削減



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



ITサービスに発生しうる障害と監視の関連性

ITサービスに
発生しうる障害

理解できる

理解できない

気づける

Actionableな監視

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



とりあえずの監視

気づいても対処につなげられない
(例. インフラのリソース使用率上昇)



気づけない

Actionableな監視予備群

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



監視できていない未知の領域

障害発生したが原因がわからず監視
もできない

従来の監視のアプローチ

ITサービスに
発生しうる障害

運用スペシャリストがログから気合いで分析
のちのち手順化

理解できる

理解できない



Actionableな監視

とりあえずの監視

努力と根性と属人性で
Actionableな監視を増やす



Actionableな監視予備群

監視できていない未知
の領域

気づける

頑張っ
てすべての
障害ポイント
を洗い出す



気づけない

AIOpsとは

ガートナーによる定義

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

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

1. 異常検知
2. イベントの相関分析
3. 根本原因分析

New RelicのAlerts & “AI”

→ **Applied Intelligence**

応用知能:機械学習によって得たデータを元に運用をアシスト

AI Opsが必要とされる背景

1. モノリスからマイクロサービスへ

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

過去のシステム

アプリ



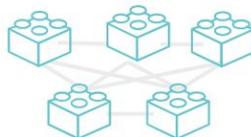
基盤



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

近年のシステム

アプリ



リソース抽象化
(仮想化、コンテナ等)



基盤

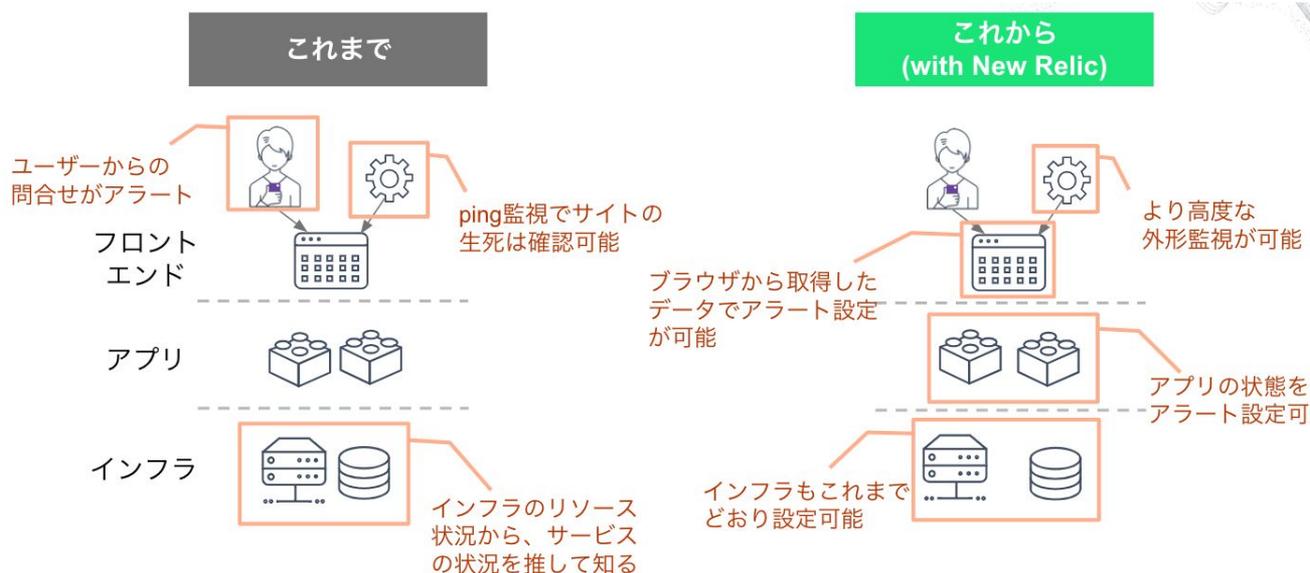


アプリがマイクロサービス化かつ基盤が疎結合なため、基盤リソースと関係なく問題が発生しうる

AIopsが必要とされる背景

2. 捕捉できるデータの増加と多様化

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

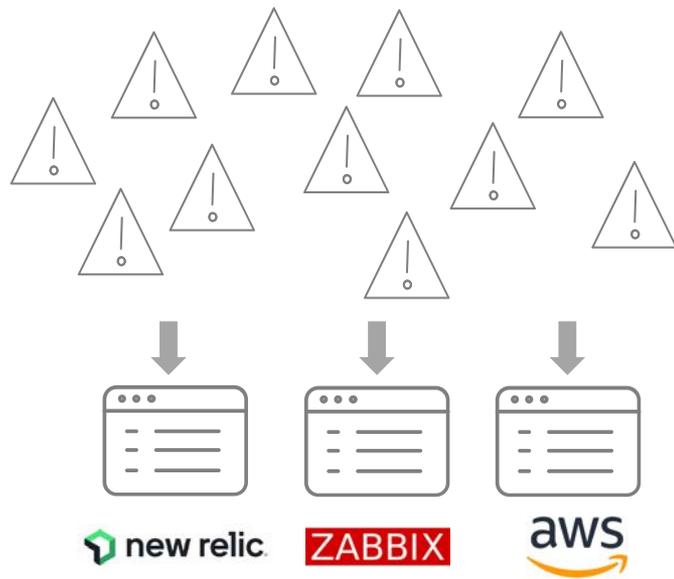


監視にまつわる新たな課題

アラートを1つ1つ網羅的に
設定するのか問題



大量のアラートをどう解釈してトラ
シューするのか問題



従来の監視の限界



ITサービスに
発生しうる障害

理解できる

理解できない

気づける

Actionableな監視

とっぴあえずの監視

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

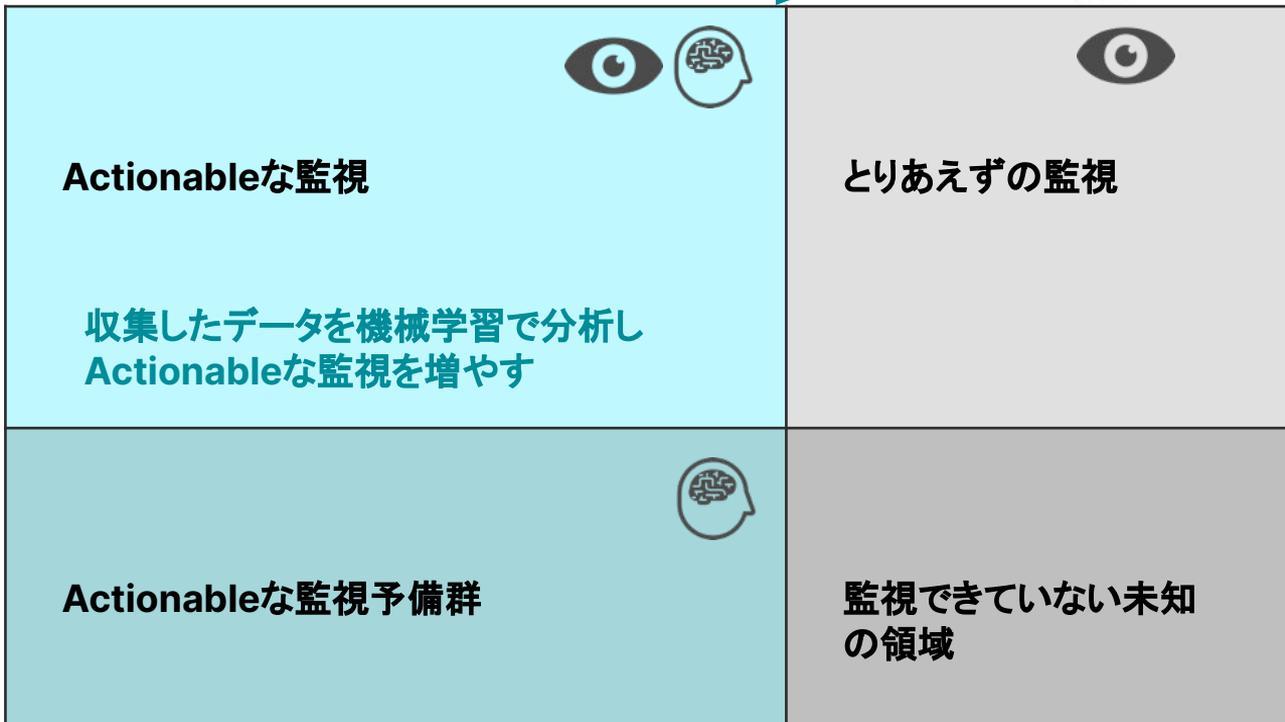
AI Opsのアプローチ

複数の事象を自動で関連付け
根本原因を推察

ITサービスに
発生しうる障害

理解できる

理解できない



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

アラートを一つ一つ網羅的に
設定するのか問題



[解決するAIOpsの機能]

- 異常検知



手動でアラート設定せずとも自動で検知

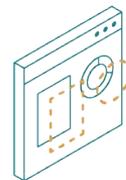
Anomaly Detection
Alert coverage gaps

大量のアラートをどう解釈してトラ
シューするのか問題



[解決するAIOpsの機能]

- イベントの相関分析
- 根本原因分析



複数の事象を自動で関連付け、根本原因を推察

Correlation
Root Cause Analysis

機能紹介: Alert coverage gaps

Alert coverage gaps

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

0% covered 1 entities

Services - APM

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

設定すべきアラートを通知します。

現行ではAPMのみを対象としています。

Add an alert

EC-site

Add recommended conditions

Our power users add these conditions to similar entities.

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

Select policy to get notified

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

Create an alert condition

Account: 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 = 'HjuMYT3Kx8UE18QV8TE1DQVRJTES8NDQDGAu4dk3' FACET entity -guid`

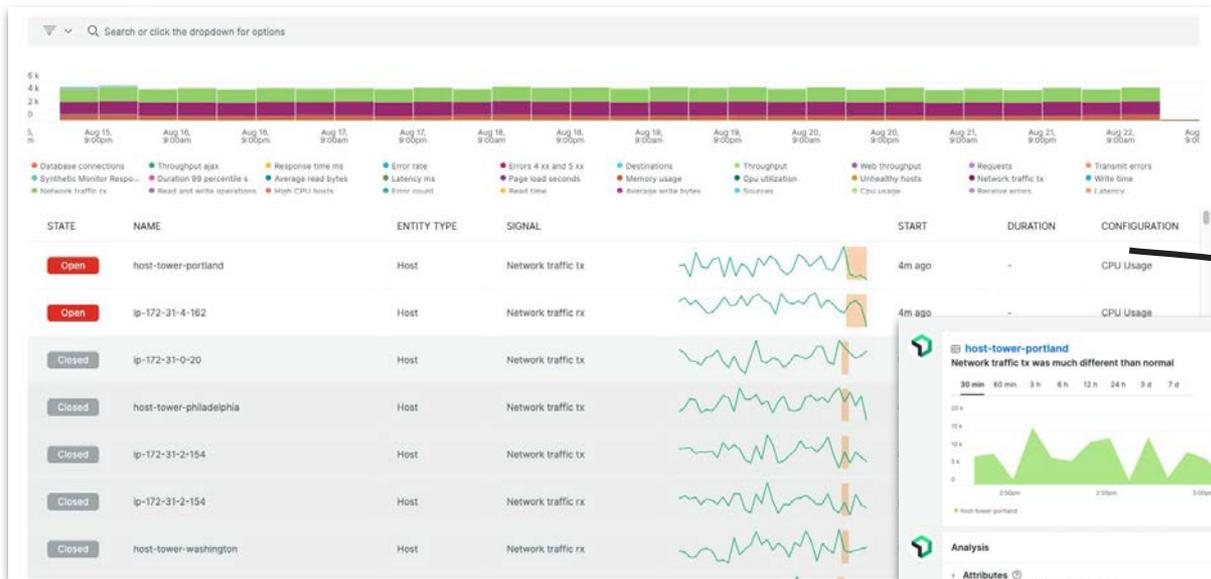
Showing 1/1 time series

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

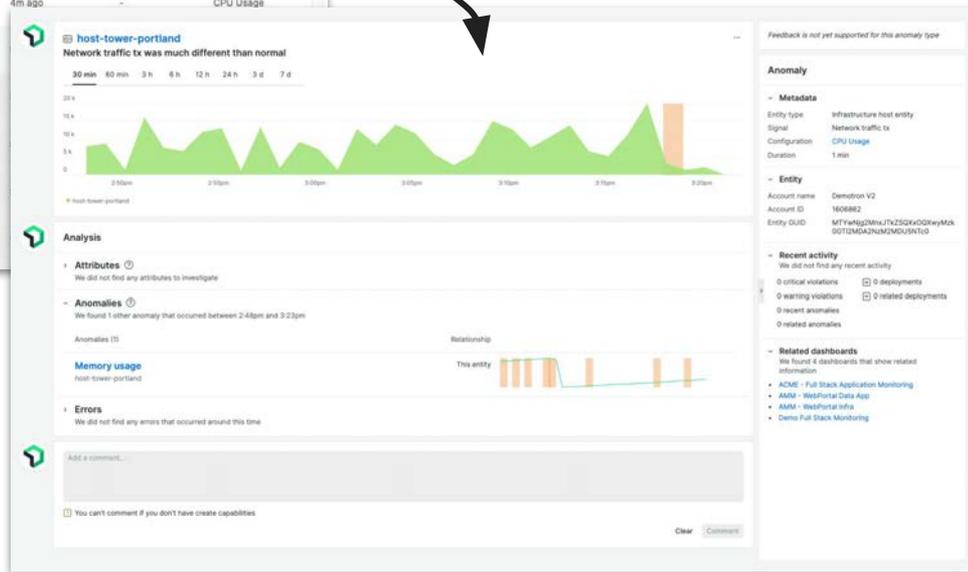
Threshold direction: Upper and lower

機能紹介: Anomaly Detection



Alerts & AI → Issues & activity → Anomalies

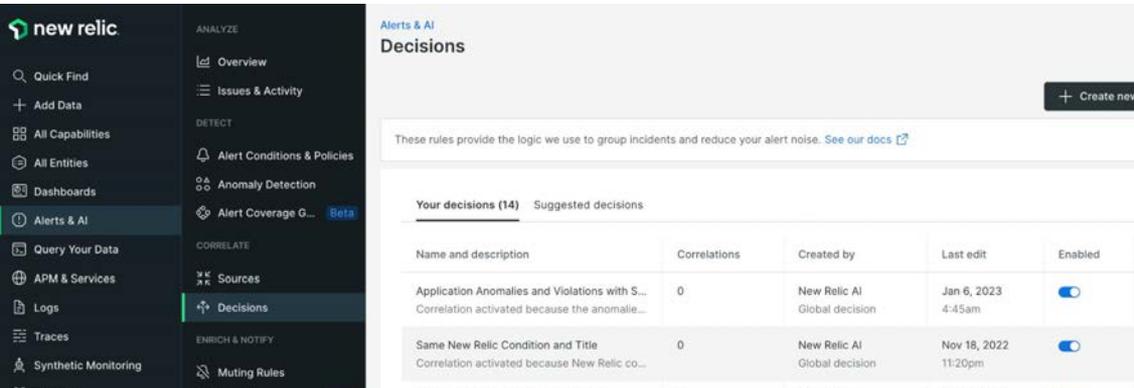
- 発生したAnomalyの1つを選択し、詳細を確認する



機能紹介: Correlate (Decisions)

Alerts & AI → Decisions

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



The screenshot shows the New Relic interface. On the left is a dark sidebar with the 'new relic' logo and a navigation menu. The 'Alerts & AI' option is highlighted. The main content area is titled 'Alerts & AI Decisions' and contains a table of decisions.

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

Same Application Name, Policy and Id

Correlation activated because the application name, policy ID and id

New Relic AI - Global decision 0 likes 0 dislikes

Decision logic

Correlate by attributes

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

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

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

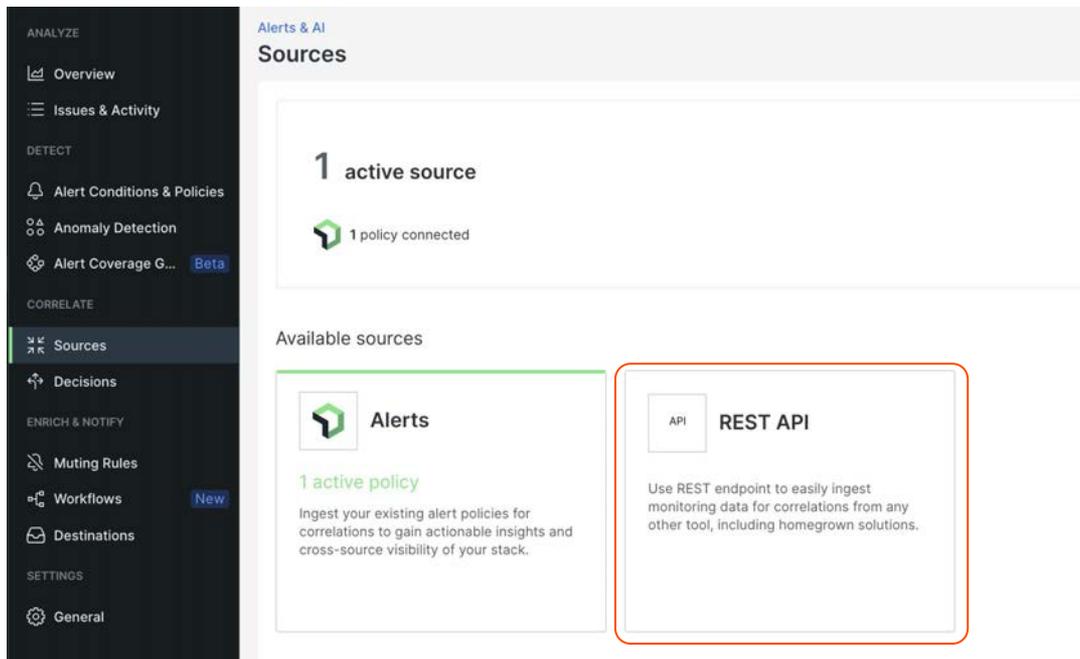
Advanced Setting

Time window: 20 min

Minimum incidents before activating: 2

参考：Zabbixの連携1

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



The screenshot displays the New Relic interface for Alerts & AI Sources. The left sidebar contains navigation options under categories: ANALYZE (Overview, Issues & Activity), DETECT (Alert Conditions & Policies, Anomaly Detection, Alert Coverage G... Beta), CORRELATE (Sources, Decisions), ENRICH & NOTIFY (Muting Rules, Workflows New, Destinations), and SETTINGS (General). The main content area shows 'Alerts & AI Sources' with a summary of '1 active source' and '1 policy connected'. Below this, the 'Available sources' section lists 'Alerts' (with 1 active policy) and 'REST API'. The 'REST API' option is highlighted with a red border and includes the text: 'Use REST endpoint to easily ingest monitoring data for correlations from any other tool, including homegrown solutions.'

参考：Zabbixの連携3

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

アクション

アクション 実行内容

* デフォルトのアクション実行ステップの間隔

メンテナンス中の場合に実行を保留

実行内容	ステップ 詳細	開始時刻	継続期間	アクション
	1 ユーザーグループにメッセージを送信: New Relic via New Relic Incident Intelligence	すぐに	標準	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			

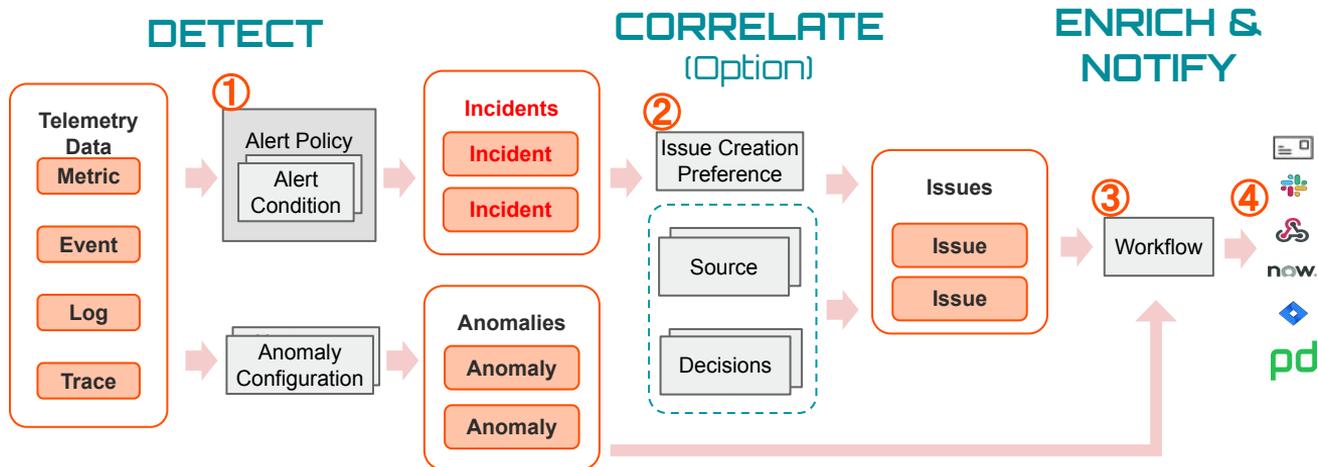
* 少なくとも1つ以上の実行内容が設定されている必要があります。

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



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

New Relicを個人で試してみよう。

無料サインアップは <https://newrelic.com/jp/sign-up-japan> より
手順は[こちら](#)。

- **100GB/月まで一生無料**
- **New Relic の オブザーバ
ビリティ機能を試せる**
- **FSOユーザー1名つき！**
- **クレジットカード不要**



The screenshot shows the New Relic sign-up page for Japan. The header includes the New Relic logo and navigation links for Platform, Pricing, Solutions, Partners, Resources, and Documentation. The main heading is "New Relic 無料サインアップ" (New Relic Free Sign-up). Below the heading, it states that all New Relic features are accessible for free without a credit card. A note indicates that this is a trial form, and users should enter their email and password. A section titled "無料アカウントでは以下の内容が含まれています:" (Included in the free account) lists: "無料ユーザーアカウント" (Free user account) with "100GB of data per month" and "Full access to all features for 1 user per platform" (free users are not included). Another section lists "メトリクス、ログ、イベント、トレースのすべてデータを統合可能なプラットフォーム" (Platform that integrates all metrics, logs, events, and traces) with "beta-scale data processing at high speed" and "data ingestion up to 1GB or 0.30 dollars per month". On the right, there is a "サインアップ" (Sign up) form with fields for "姓" (Last name) containing "山田", "名" (First name) containing "太郎", and "会社名" (Company name) containing "New Relic, Inc.". A "ログイン" (Login) link and a "デモをリクエストする" (Request demo) button are also visible.

New Relic University

<https://newrelic.com/jp/learn>

New Relicについて基本から応用まで学べるコンテンツです

New Relic University

New Relic One を学ぶ

自分のレベルに合わせて学びはじめよう

弊社では、New Relic Oneについて学べるコンテンツを New Relic University として無償で公開しています。これから使い始める方も、既に習熟されている方も、お客様のペースで、お好きなところから始めて頂けます。



インストール方法を学ぶ

New Relic One を実際にインストールしてあるための手順書や必要な情報について学びます。



New Relic One の全体概要を学ぶ (1月中旬公開予定)

New Relic One の全体像やライセンス形態をオンデマンドの動画視聴で学びます。



New Relic One の主要機能を学ぶ

New Relic One に含まれる TDP/PSO/NAI の3レイヤーにおける主要機能を動画で学びます。



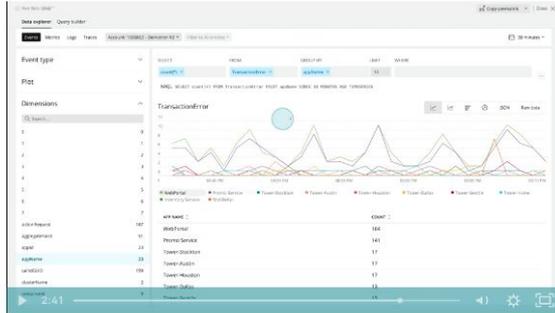
New Relic One の実践方法を学ぶ

New Relic のエンジニアが提供するハンズオントレーニングを通じて実践操作方法を学びます。

Event & Metrics

IN THIS ARTICLE

- ▶ Telemetry Data Platform >
- Event & Metrics >
- OSS Data Explorer >
- Dashboard >
- ▶ Full Stack Observability >
- Explorer >
- APM >
- APM for Serverless >
- Browser >
- Mobile >
- Synthetics >
- Infrastructure >
- Distributed Tracing >
- Workloads >
- Errors Inbox >
- Recommendations >



Data Explorer でデータを確認する

New Relic に送信されたデータを確認する方法の一つであるデータエクスプローラーをご紹介します。データエクスプローラーは New Relic One の画面上で、確認したいデータや条件を選択することで、New Relic にあるデータを簡単に表示することが出来る機能です。

New Relic University (詳細)

New Relicの基礎から応用までを学べ、認定資格も取得できるセルフラーニングコンテンツです

Install

New Relicを 使い始める

New Relic One へのサインアップやエージェントインストールの方法などのガイドを提供

[APM / Browser / Infrastructure / Logs / Mobile \(iOS/Android\) / AWS統合 / Azure統合 / GCP統合](#) インストール手順

- ▶ [サインアップ方法](#)
- ▶ [インストールガイド](#)

NRU 100

Observability/New Relicを知る

New Relic One やオブザーバビリティに関する基礎知識を座学にて学習

[NRU Practitioner](#) オブザーバビリティ入門

[NRU 101](#) New Relic One 入門

- ▶ [オンデマンドセミナー \(practitioner\), \(nru101\)](#)

NRU 200

New Relicの主要 機能を学ぶ

New Relic One に含まれる3つの主要機能に含まれる54の機能群を動画で説明

[NRU201](#) Telemetry Data Platform
[NRU202](#) Full Stack Observability
[NRU203](#) Applied Intelligence

- ▶ [主要機能解説動画](#)

NRU 300/400

New Relicの使い方を 体感する

New Relic One を実際に操作し、主要機能を利用できる状態にするためのトレーニング

[NRU 301](#) アプリケーションとインフラ性能観測の基本
[NRU 302](#) ダッシュボード開発とNRQLの基本
[NRU 303](#) SLI/SLO設計の基本
[NRU 304](#) AIOps とアラート設計の基本
[NRU 401](#) CodeStream によるDevOps を想定したエラー分析対応の基本

- ▶ [開催スケジュール](#)

Exam

資格を得る

New Relicの知識を有していることを証明するための試験、合格すると資格バッジを授与

[フルスタックオブザーバビリティ認定試験](#)

- ▶ [受験サイト](#)

ロール別 New Relic ラーニングパス

フロントエンド
開発エンジニア

サーバーサイド
開発エンジニア

インフラ運用
エンジニア

SRE

ネットワーク
エンジニア

セキュリティ
エンジニア

プロジェクト
マネージャー

プロダクト
マネージャー

Observability
/New Relicを知る

Observability入門

New Relic入門

New Relicを
使い始める

サインアップ(アカウント開設)

エージェント導入を体験

[Relicstraurant\(セルフハンズオンラボ\)](#)

[Java パッチの計測ハンズオン](#)

[ネットワークモニタリングハンズオン](#)

ご自身の環境へのエージェント導入

フロントエンド機能 ※サーバーサイドインフラ担当は特にSynthetics受講を推奨

(興味に応じて左記から受講)

New Relicの
主要機能を学
ぶ

バックエンド機能 ※フロントエンド担当は興味に応じて受講

分散トレーシング、Errors Inbox、
CodeStream

セキュリティ
機能(作成中)

データ分析(NRQL) / アラート / サービスレベルマネジメント

New Relicの
使い方を体感
する

ハンズオントレーニング：アプリケーションとインフラ性能観測の基本

ハンズオントレーニング：ダッシュボード開発とNRQLの基本

ハンズオントレーニング：SLI/SLO設計の基本

ハンズオントレーニング：AIOps とアラート設計の基本

ハンズオントレーニング：
CodeStream(エラー分析対応の基本)

資格を得る

フルスタックオペザビリティ認定試験 ※受験のためには上記コンテンツをできるだけ網羅的に学習することを推奨

NRUG

ぬるぐで学ぶ

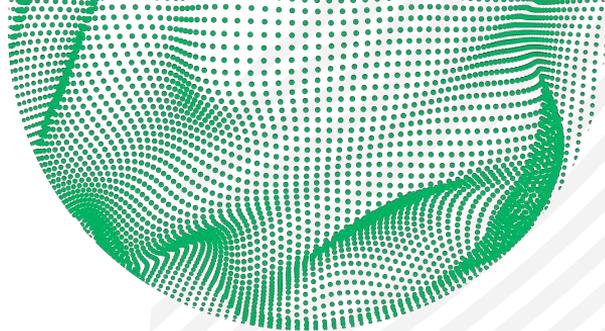
New Relic User Group

New Relic ユーザーが集い、実践事例や最新機能紹介などを実施。初心者支部や SRE 支部などが形成されており、エンジニア同士でのネットワーキングや信頼性の高い情報交換が可能。

ConnpassのNRUGページより
ご登録ください。

(<https://nrug.connpass.com/>)





本当にお疲れさまでした。



最後となりますが、
是非、アンケートへのご協力をお願いいたします。

また、もっと詳しい話を聞きたい方は、
その旨アンケートにご記載ください。



Thank you.

