



Webhook通知

Data Infrastructure Insights

NetApp
February 03, 2026

This PDF was generated from https://docs.netapp.com/ja-jp/data-infrastructure-insights/ws_notifications_using_webhooks.html on February 03, 2026. Always check docs.netapp.com for the latest.

目次

Webhook通知	1
Webhookを使用したワークロードセキュリティ通知	1
Webhookの作成	1
パラメーター: パラメーターとは何か、どのように使用するのか?	3
ワークロード セキュリティ Webhook リスト ページ	3
アラートポリシーでWebhook通知を構成する	4
Discord 向けワークロード セキュリティ Webhook の例	6
Discordの設定:	6
ワークロード セキュリティ Webhook を作成します。	6
Webhook経由の通知	8
PagerDuty のワークロード セキュリティ Webhook の例	9
PagerDutyのセットアップ:	10
Workload Security PagerDuty Webhook を作成します。	11
Webhook経由の通知	12
Slack 向けワークロード セキュリティ Webhook の例	14
Microsoft Teams のワークロード セキュリティ Webhook の例	18
Teams のセットアップ:	18
ワークロード セキュリティ チームの Webhook を作成します。	18
Webhook経由の通知	19

Webhook通知

Webhookを使用したワークロードセキュリティ通知

Webhook を使用すると、ユーザーはカスタマイズされた Webhook チャネルを使用して、さまざまなアプリケーションに重大なアラート通知や警告アラート通知を送信できます。

多くの商用アプリケーションは、Slack、PagerDuty、Teams、Discord など、標準の入力インターフェースとして Webhook をサポートしています。汎用的でカスタマイズ可能な Webhook チャネルをサポートすることで、Workload Security はこれらの配信チャネルの多くをサポートできます。Webhook の設定に関する情報は、それぞれのアプリケーションの Web サイトで確認できます。例えば、Slackは["この便利なガイド"](#)。

複数の Webhook チャネルを作成し、各チャネルを異なる目的、個別のアプリケーション、異なる受信者などを対象にすることができます。

Webhookチャネルインスタンスは次の要素で構成されています

Name	説明
URL	Webhook ターゲット URL (URL パラメータとともに http:// または https:// プレフィックスを含む)
方法	GET/POST - デフォルトはPOST
カスタムヘッダー	ここでカスタムヘッダーを指定します
メッセージ本文	メッセージの本文をここに入力してください
デフォルトのアラートパラメータ	Webhookのデフォルトパラメータを一覧表示します
カスタムパラメータとシークレット	カスタムパラメータとシークレットを使用すると、固有のパラメータやパスワードなどの安全な要素を追加できます。

Webhookの作成

Workload Security Webhook を作成するには、「管理」>「通知」に移動し、「Workload Security Webhooks」タブを選択します。次の画像は、Slack Webhook 作成画面のサンプルを示しています。

注意: Workload Security Webhook を作成および管理するには、ユーザーは Workload Security Admin である必要があります。

Add a Webhook

Name

Template Type

URL ?

 Validate SSL Certificate for secure communication

Method

Custom Header

```
Content-type: application/json  
Accept: application/json
```

Message Body

```
{  
  "blocks": [  
    {  
      "type": "section",  
      "text": {  
        "type": "mrkdwn",  
        "text": "*%severity%% Alert: %%synopsis%%*"  
      }  
    },  
    {  
      "type": "divider"  
    }  
  ]  
}
```

- 各フィールドに適切な情報を入力し、「保存」をクリックします。
- 「Webhook のテスト」ボタンをクリックして接続をテストすることもできます。これにより、選択したメソッドに従って、定義された URL に「メッセージ本文」（置換なし）が送信されることに注意してください。
- SWS Webhook は、いくつかのデフォルト パラメータで構成されています。さらに、独自のカスタム パラメータまたはシークレットを作成することもできます。

パラメーター: パラメーターとは何か、どのように使用するのか?

アラート パラメータは、アラートごとに設定される動的な値です。たとえば、`%%severity%%` パラメータは、アラートの重大度タイプに置き換えられます。

「Test Webhook」ボタンをクリックしたときには置換は実行されないことに注意してください。テストでは、パラメータのプレースホルダー (`%%<param-name>%%`) を表示するペイロードが送信されますが、データに置き換えられることはできません。

カスタムパラメータとシークレット

このセクションでは、必要なカスタム パラメータやシークレットを追加できます。カスタム パラメータまたはシークレットは、URL またはメッセージ本文に含めることができます。シークレットを使用すると、ユーザーはパスワード、apiKey などの安全なカスタム パラメータを設定できます。

次のサンプル画像は、Webhook の作成時にカスタム パラメータがどのように使用されるかを示しています。

The screenshot shows the 'Add Webhook' configuration page. On the left, there are fields for 'Template Type' (Slack), 'URL' (https://hooks.slack.com/services/%%slack-id%%), 'Method' (POST), 'Custom Header' (Content-type: application/json, Accept: application/json), and 'Message Body' (JSON payload). The 'Message Body' field contains a red box around the '%%webhookConfiguredBy%%' placeholder. On the right, a table lists various alert details with their corresponding %%placeholder%% values. Below the table is a 'Custom Parameters and Secrets' section with a table containing two entries: '%%webhookConfiguredBy%%' with value 'system_admin_1' and '%%slack-id%%' with a redacted value. A '+ Parameter' button is at the bottom.

Name	Value	Description
%%webhookConfiguredBy%%	system_admin_1	...
%%slack-id%%	*****	...

ワークフロー セキュリティ Webhook リスト ページ

Webhook リスト ページには、名前、作成者、作成日、ステータス、セキュリティ、最終報告のフィールドが表示されます。注: 「ステータス」列の値は、最後の Webhook トリガーの結果に基づいて変化し続けます。以下はステータス結果の例です。

ステータス	説明
OK	通知を正常に送信しました。
403	禁止されています。

404	URLが見つかりません。
400	<p>要求の形式が正しくありません。メッセージ本文にエラーがある場合、このステータスが表示されることがあります。例:</p> <ul style="list-style-type: none"> 形式が不適切な json。 予約済みのキーに無効な値を指定しています。たとえば、PagerDuty は「重大度」として、critical/warning/error/info のみを受け入れます。その他の結果の場合は、400 ステータスが返される可能性があります。 アプリケーション固有の検証エラー。たとえば、Slack ではセクション内に最大 10 個のフィールドが許可されます。10 個を超えると、400 ステータスになる可能性があります。
410	リソースは利用できなくなりました

「最終報告」列には、Webhook が最後にトリガーされた時刻が示されます。

ウェブフック一覧ページから、ユーザーはウェブフックを編集/複製/削除することもできます。

アラートポリシーで**Webhook**通知を構成する

アラート ポリシーに Webhook 通知を追加するには、「ワーカロード セキュリティ」>「ポリシー」に移動し、既存のポリシーを選択するか、新しいポリシーを追加します。アクション セクション > Webhook 通知 ドロップダウンで、必要な Webhook を選択します。

Edit Attack Policy



Policy Name*

For Attack Type(s) *

- Ransomware Attack
- Data Destruction - File Deletion

On Device

[+ Another Device](#)

Actions

- Take Snapshot [?](#)
- Block User File Access [?](#)

Time Period

Webhooks Notifications

Test-Webhook-1

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

Webhook 通知はポリシーに関連付けられています。攻撃 (RW/DD/WARN) が発生すると、設定されたアクション (スナップショットの取得/ユーザーのブロック) が実行され、関連する Webhook 通知がトリガーされます。

注: 電子メール通知はポリシーとは無関係であり、通常どおりトリガーされます。

- ・ポリシーが一時停止されている場合、Webhook 通知はトリガーされません。
- ・複数の Webhook を 1 つのポリシーにアタッチできますが、ポリシーにアタッチする Webhook は 5 つ以下にすることをお勧めします。

ワークロードセキュリティ Webhook の例

Webhooks の "スラック"

Webhooks の "ページャーデューティ" Webhooks の "チーム" Webhooks の "不和"

Discord 向けワークロード セキュリティ Webhook の例

Webhook を使用すると、ユーザーはカスタマイズされた Webhook チャネルを使用してさまざまなアプリケーションにアラート通知を送信できます。このページでは、Discord 用の Webhook を設定する例を示します。



このページはサードパーティの指示を参照しており、変更される可能性があります。参照 "[Discord ドキュメント](#)" 最新情報についてはこちらをご覧ください。

Discord の設定:

- ・Discord でサーバーを選択し、テキストチャンネルの下にあるチャンネル編集（歯車アイコン）を選択します。
- ・*統合 > Webhook の表示*を選択し、*新しい Webhook*をクリックします。
- ・Webhook URL をコピーします。これを Workload Security Webhook 設定に貼り付ける必要があります。

ワークロード セキュリティ Webhook を作成します。

1. 「管理」>「通知」に移動し、「Workload Security Webhooks」タブを選択します。新しい Webhook を作成するには、「+ Webhook」をクリックします。
2. Webhook に意味のある名前を付けます。
3. テンプレート タイプ ドロップダウンで、Discord を選択します。
4. 上記の Discord URL を URL フィールドに貼り付けます。

Add a Webhook

Name

Template Type

URL ?

 Validate SSL Certificate for secure communication

Method

Custom Header

```
Content-Type: application/json  
Accept: application/json
```

Message Body

```
{  
  "content": null,  
  "embeds": [  
    {  
      "title": "%%severity%% | %%id%%",  
      "description": "%%synopsis%%",  
      "url": "https://%%cloudInsightsHostname%%/%%alertDetailsPageUrl%% ",  
      "color": 3244733,  
      "fields": [  
        {  
          "name": "%%",  
          "value": "%%"  
        }  
      ]  
    }  
  ]  
}
```

Webhook をテストするには、メッセージ本文の URL 値を有効な URL (<https://netapp.com> など) に一時的に置き換えて、[Test Webhook] ボタンをクリックします。Discord では、テスト Webhook 機能が動作するために有効な URL を指定する必要があります。

テストが完了したら、必ずメッセージ本文を元に戻してください。

Webhook経由の通知

Webhook 経由でイベントを通知するには、[Workload Security] > [ポリシー] に移動します。 +攻撃ポリシー_ または+警告ポリシー_ をクリックします。

- 意味のあるポリシー名を入力します。
- 必要な攻撃タイプ、ポリシーを適用するデバイス、および必要なアクションを選択します。
- [Webhooks Notifications] ドロップダウンで、必要な Discord Webhook を選択して保存します。

注: Webhook は、編集することで既存のポリシーに添付することもできます。

Add Attack Policy

Policy Name*

For Attack Type(s) *

Ransomware Attack

Data Destruction - File Deletion

On Device

All Devices

+ Another Device

Actions

Take Snapshot ?

Block User File Access ?

Time Period

12 hours

Webhooks Notifications

Please Select

Test-Webhook-1

Cancel Save

This screenshot shows the configuration interface for a new attack policy. The policy is named "Test policy 1". It is set to respond to "Ransomware Attack" and "Data Destruction - File Deletion". The policy will be applied to "All Devices". Under "Actions", both "Take Snapshot" and "Block User File Access" are selected. The "Time Period" is set to "12 hours". In the "Webhooks Notifications" section, "Please Select" is chosen, and a specific webhook channel named "Test-Webhook-1" is listed. At the bottom, there are "Cancel" and "Save" buttons.

PagerDuty のワークフロー セキュリティ Webhook の例

Webhook を使用すると、ユーザーはカスタマイズされた Webhook チャネルを使用して

さまざまなアプリケーションにアラート通知を送信できます。このページでは、PagerDuty の Webhook を設定する例を示します。



このページはサードパーティの指示を参照しており、変更される可能性があります。参照["PagerDutyのドキュメント"](#)最新情報についてはこちらをご覧ください。

PagerDutyのセットアップ:

1. PagerDuty で、サービス > サービス ディレクトリ に移動し、+ 新しいサービス ボタンをクリックします。
2. _名前_ を入力し、_API を直接使用_ を選択します。_サービスの追加_ を選択します。

Add a Service

A service may represent an application, component or team you wish to open incidents against.

General Settings

Name

Description Add a description for this service (optional)

Integration Settings

Connect with one of PagerDuty's supported integrations, or create a custom integration through email or API. Alerts from a service from a supported integration or through the Events V2 API.

You can add more than one integration to a service, for example, one for monitoring alerts and one for change events.

Integration Type Select a tool

PagerDuty integrates with hundreds of tools, including monitoring tools, ticketing systems, code repositories, and deploy pipelines. This may involve configuration steps in the tool you are integrating with PagerDuty.

Integrate via email
If your monitoring tool can send email, it can integrate with PagerDuty using a custom email address.

Use our API directly
If you're writing your own integration, use our Events API. More information is in our developer documentation.

Events API v2

Don't use an integration
If you only want incidents to be manually created. You can always add additional integrations later.

3. *統合キー*を表示するには、[統合] タブを選択します。以下の Workload Security Webhook を作成するときに、このキーが必要になります。
4. アラートを表示するには、「インシデント」または「サービス」に移動します。

Open Incidents (5)

<input type="checkbox"/>	Status	Priority	Urgency	Alerts	Title	Assigned To	Created
<input type="checkbox"/>	Acknowledged		High	1	Critical Alert: Ransomware attack from user account #403982 + SHOW DETAILS (1 triggered alert)	Chandan SS	Today at 4:11 AM
<input type="checkbox"/>	Acknowledged		High	1	Critical Alert: Data Destruction - File Deletion attack from user account #403996 + SHOW DETAILS (1 triggered alert)	Chandan SS	Today at 5:41 AM

Workload Security PagerDuty Webhook を作成します。

- 「管理」>「通知」に移動し、「Workload Security Webhooks」タブを選択します。新しいWebhookを作成するには、「+ Webhook」を選択します。
- Webhookに意味のある名前を付けます。
- テンプレートタイプドロップダウンで、*PagerDuty* トリガーを選択します。
- routingKeyという名前のカスタムパラメータシークレットを作成し、その値を上記で作成した PagerDuty Integration Key に設定します。

Custom Parameters and Secrets i

Name	Value ↑	Description
%routingKey%	*****	⋮

+ Parameter

Name i	Value
routingKey	*****
Type	Description
Secret	

Cancel

Save Parameter

Add a Webhook

Name

Test PagerDuty

Template Type

PagerDuty Trigger

URL 

https://events.pagerduty.com/%%pagerDutyId%%

 Validate SSL Certificate for secure communication**Method**

POST

Custom Header

Content-Type: application/json
 Accept: application/json

Message Body

```
{
  "dedup_key": "%%id%%",
  "event_action": "trigger",
  "links": [
    {
      "href": "https://%%cloudInsightsHostname%%/%%alertDetailsPageUrl%%",
      "text": "%%severity%% | %%id%% | %%detected%%"
    }
  ],
  "payload": {
    "user": "00000000000000000000"
  }
}
```

Cancel**Test Webhook****Create Webhook**

Webhook経由の通知

- Webhook 経由でイベントを通知するには、[Workload Security] > [ポリシー] に移動します。 +攻撃ポリシー_または+警告ポリシー_を選択します。
- 意味のあるポリシー名を入力します。
- 必要な攻撃タイプ、ポリシーを適用するデバイス、および必要なアクションを選択します。
- [Webhooks Notifications] ドロップダウンで、必要な PagerDuty Webhook を選択します。ポリシーを保存します。

注: Webhook は、編集することで既存のポリシーに添付することもできます。

Add Attack Policy

Policy Name*
Test policy 1

For Attack Type(s) *

Ransomware Attack
 Data Destruction - File Deletion

On Device

All Devices ▾

+ Another Device

Actions

Take Snapshot ?
 Block User File Access ?

Time Period

12 hours ▾

Webhooks Notifications

Please Select ▾

Test-Webhook-1

Cancel Save

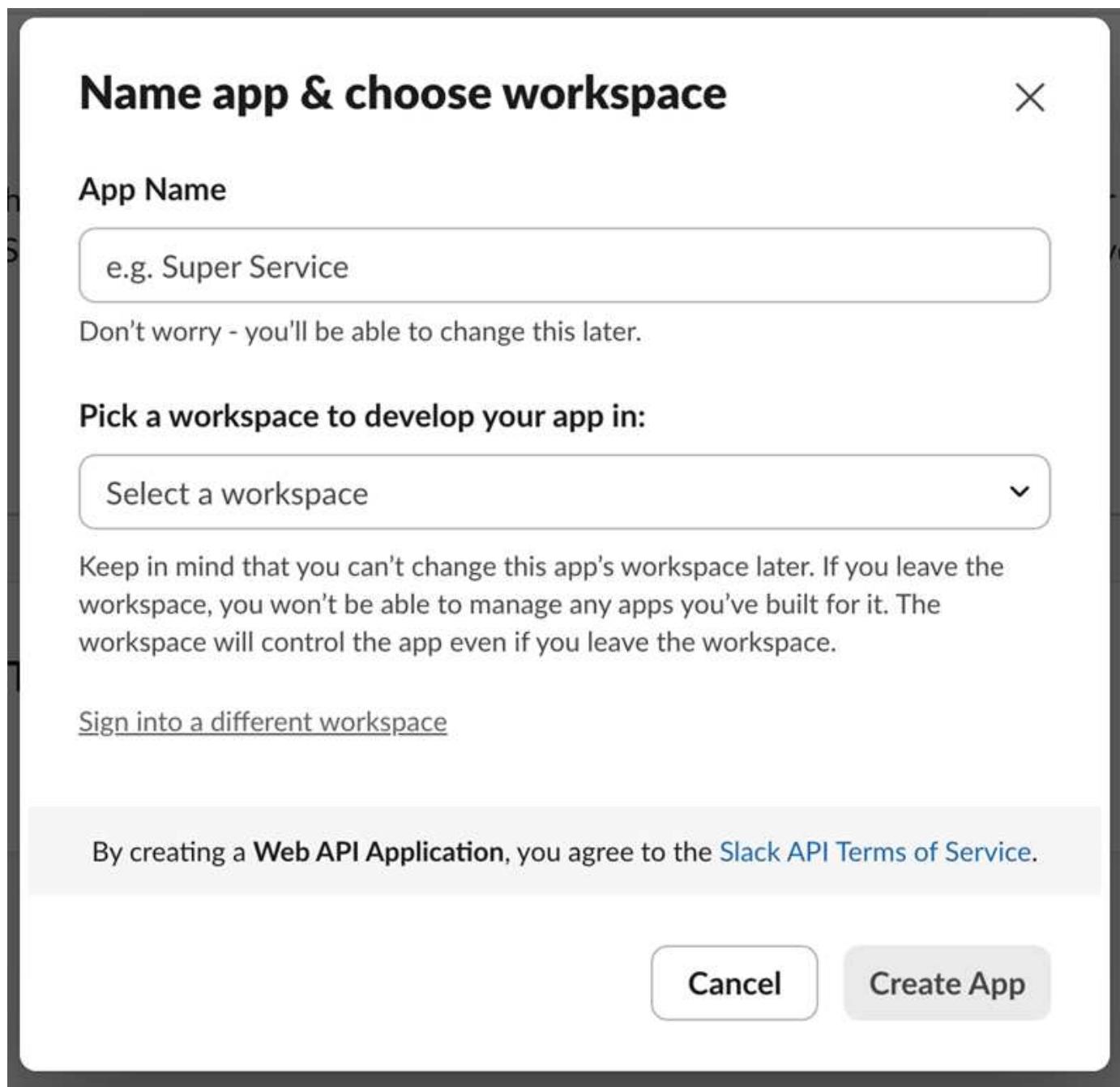
Slack 向けワークロード セキュリティ Webhook の例

Webhook を使用すると、ユーザーはカスタマイズされた Webhook チャネルを使用してさまざまなアプリケーションにアラート通知を送信できます。このページでは、Slack 用の Webhook を設定する例を示します。

このページはサードパーティの指示を参照しており、変更される可能性があります。最新情報については、Slack のドキュメントを参照してください。

Slackの例

- へ移動 <https://api.slack.com/apps>新しいアプリを作成します。意味のある名前を付けて、ワークスペースを選択します。



- ・「Incoming Webhooks」に移動し、「Activate Incoming Webhooks」をクリックし、「Add New Webhook」を選択して、投稿するチャネルを選択します。
- ・Webhook URL をコピーします。この URL は、Workload Security Webhook を作成するときに提供されます。

ワークロードセキュリティ **Slack Webhook** を作成する

1. 「管理」>「通知」に移動し、「Workload Security Webhooks」タブを選択します。新しい Webhook を作成するには、[+ Webhook] を選択します。
2. Webhook に意味のある名前を付けます。
3. テンプレート タイプ ドロップダウンで、*Slack* を選択します。
4. 上記からコピーしたURLを貼り付けます。

Add a Webhook

Name

Template Type



URL ?

 Validate SSL Certificate for secure communication

Method



Custom Header

```
Content-type: application/json  
Accept: application/json
```

Message Body

```
{  
  "blocks": [  
    {  
      "type": "section",  
      "text": {  
        "type": "mrkdwn",  
        "text": "*%severity%% Alert: %%synopsis%%*"  
      }  
    },  
    {  
      "type": "divider"  
    }  
  ]  
}
```

Webhook経由の通知

- Webhook 経由でイベントを通知するには、[Workload Security] > [ポリシー] に移動します。 +攻撃ポリシー_または+警告ポリシー_をクリックします。
- 意味のあるポリシー名を入力します。
- 必要な攻撃タイプ、ポリシーを適用するデバイス、および必要なアクションを選択します。

- [Webhooks Notifications] ドロップダウンで、必要な Webhook を選択します。ポリシーを保存します。

注: Webhook は、編集することで既存のポリシーに添付することもできます。

Add Attack Policy

Policy Name*
Test policy 1

For Attack Type(s) *

Ransomware Attack
 Data Destruction - File Deletion

On Device

All Devices

+ Another Device

Actions

Take Snapshot ?
 Block User File Access ?

Time Period

12 hours

Webhooks Notifications

Please Select

Test-Webhook-1

Cancel Save

Microsoft Teams のワークロード セキュリティ Webhook の例

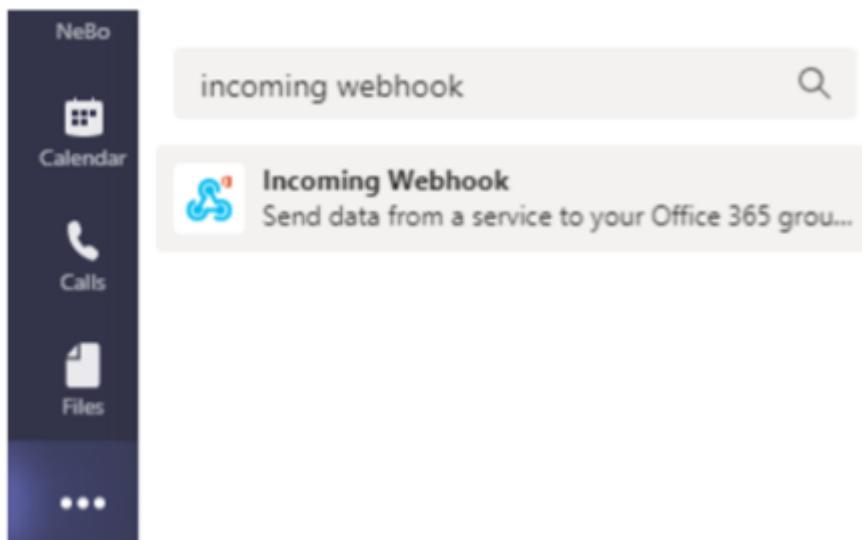
Webhook を使用すると、ユーザーはカスタマイズされた Webhook チャネルを使用してさまざまなアプリケーションにアラート通知を送信できます。このページでは、Teams の Webhook を設定する例を示します。



このページはサードパーティの指示を参照しており、変更される可能性があります。参照["Teams ドキュメント"](#)最新情報についてはこちらをご覧ください。

Teams のセットアップ:

1. Teams でケバブを選択し、Incoming Webhook を検索します。



2. *チームに追加 > チームを選択 > コネクタの設定*を選択します。
3. Webhook URL をコピーします。これを Workload Security Webhook 設定に貼り付ける必要があります。

ワークロード セキュリティ チームの Webhook を作成します。

1. 「管理」>「通知」に移動し、「Workload Security Webhooks」タブを選択します。新しい Webhook を作成するには、[+ Webhook] を選択します。
2. Webhook に意味のある名前を付けます。
3. [テンプレート タイプ] ドロップダウンで、[Teams] を選択します。

Add a Webhook

Name

Template Type

URL ?

 Validate SSL Certificate for secure communication

Method

Custom Header

```
Content-Type: application/json  
Accept: application/json
```

Message Body

```
{  
    "@type": "MessageCard",  
    "@context": "http://schema.org/extensions",  
    "themeColor": "0076D7",  
    "summary": "%%severity%% Alert: %%synopsis%%",  
    "sections": [  
        {  
            "activityTitle": "%%severity%% Alert: %%synopsis%%",  
            "activitySubtitle": "%%detected%%",  
            "markdown": false,  
            "facts": []  
        }  
    ]  
}
```

4. 上記の URL を URL フィールドに貼り付けます。

Webhook経由の通知

Webhook 経由でイベントを通知するには、[Workload Security] > [ポリシー] に移動します。 +攻撃ポリシー_または+警告ポリシー_を選択します。

- 意味のあるポリシー名を入力します。

- ・必要な攻撃タイプ、ポリシーを適用するデバイス、および必要なアクションを選択します。
- ・[Webhooks Notifications] ドロップダウンで、必要な Teams Webhook を選択します。ポリシーを保存します。

注: Webhook は、編集することで既存のポリシーに添付することもできます。

Add Attack Policy



Policy Name*

For Attack Type(s) *

- Ransomware Attack
- Data Destruction - File Deletion

On Device

[+ Another Device](#)

Actions

- Take Snapshot [?](#)
- Block User File Access [?](#)

Time Period

Webhooks Notifications

Test-Webhook-1

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

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を隨時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5225.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。