報道各位

2019年2月26日
株式会社インプレスR&D
https://nextpublishing.jp/

ログ分析ツール Splunk を使ってあらゆるデータを可視化する！

『Splunk App のつくりかた』発行

技術書典シリーズ、3 月の新刊

インプレスグループで電子出版事業を手がける株式会社インプレス R&D は、『Splunk App のつくりかた』(著者：江口 佳記)を発行いたします。

『技術書典シリーズ』とは、今もっとも注目すべき、エンジニアによるアウトプットの場である技術同人誌イベント「技術書典」で、頒布された同人誌を底本として、商業書籍として刊行する書籍シリーズです。

『Splunk Appのつくりかた』
https://nextpublishing.jp/isbn/9784844398868

著者：江口 佳記
小売希望価格：電子書籍版 1600 円(税別)／印刷書籍版 1800 円(税別)
電子書籍版フォーマット:EPUB3／Kindle Format8
印刷書籍版仕様：B5 判／カラー／本文 76 ページ
ISBN：978-4-8443-9886-8
発行：インプレス R&D

＜＜発行主旨・内容紹介＞＞

本書は、あらゆるマシンのログを収集し、検索・分析・可視化する Splunk で動くアプリケーションを作るために、その環境整備からデータの抽出、さらにはアプリを配布するための方法までを紹介した解説書です。

〈本書の対象読者〉

・Splunk のダッシュボードで何ができるか興味がある
・Splunk を利用しているがダッシュボードの使い方がわからない
・Splunk でパネルを並べるぐらいはできるが、それ以上の使い方が知りたい

〈本書で得られる知識〉

・Splunk ダッシュボードの概要

・必要なデータの抽出方法

・パネルの作り方

・フォームやドリルダウンなどトークンを利用したダッシュボードの高度な使い方

（本書は、次世代出版メソッド「NextPublishing」を使用し、出版されています。）

ダッシュボードの作成やパネルの基礎知識など、Splank の基本的な使い方を紹介

第5章　ダッシュボードの作成

5.1　ダッシュボードの作成方法

ダッシュボードは、作成したAppの「Dashboards」→「Create New Dashboard」から作成できます。この際、Permissonsは「Shared in App」にします。

5.2　Dashboard editor

Splunkにはダッシュボードの情報をWeb UI上で編集できるDashboard editorがあります。ダッシュボード上で「Edit」をクリックすることでエディター画面に遷移できます。

Dashboard editorは、次の機能を持ちます。

・UIエディター
　―パネルやフォームなどをUIで確認しながらレイアウト
・ソースエディター
　―ソースコードであるSimple XMLを直接編集

両者はDashboard editor画面上部のボタン（「UI」「Source」）により切り替えが可能です。まずはレイアウトを行い、必要に応じてXMLを編集するというフローで作業することになるでしょう。

5.3　ダッシュボードに配置可能なコンポーネント

ダッシュボードに配置可能な代表的なコンポーネントは次の2種類です。

・パネル
・入力フォーム

5.3.1　パネル

パネルは、グラフや表、イベント情報などデータの可視化情報を表示するコンポーネントで、ひとつのダッシュボードにいくつも配置することができます。表示される情報のソースは、基本的にはクエリーによるサーチ結果です。ただし、HTMLパネルのように自由な情報を表示するパネルも作成できます。

5.3.1.1　パネルのレイアウト

パネルの配置は、UIエディターを用いてドラッグ＆ドロップで自由に変更することができます。ダッシュボードには「列」（Simple XML上で<row>タグで表現される）の概念があり、1列にパネルを複数枚横並びに配置可能です。ただしパネルを同じ列にいくつも並べすぎるとグラフなどが読みにくくなってしまうので、1列に並べるパネルは2~3個程度にしておいたほうがよいでしょう。

5.3.2　入力フォーム

入力フォームは、パネルに表示される情報を動的に変更するために利用されるUIの部品です。よく利用されるのはShared time pickerで、各パネルで共通の検索期間を設定できるようにすることができます。

入力フォームによる動的なパネル情報の更新は、**トークン**によって実現します。トークンの説明も含めたフォームの利用方法の詳細は後述します。

5.4　ナビゲーションメニュー

Appの上部には、常にナビゲーションメニューが表示されています。このナビゲーションメニューは編集可能で、作成したダッシュボードをメニューに並べることができます。また、Appを開いたときのデフォルトで表示される画面も設定できます。ユーザーが利用しやすいよう、主要なダッシュボードがデフォルトで表示されるようにしておくとよいでしょう。

5.4.1　ナビゲーションメニューの編集

Appのナビゲーションメニューの編集は、Appにアクセスした状態で「Settings」→「User interface」→「Navigation menu」→「default」へ移動して行います。

※ナビゲーションメニューの名前は固定で「default」となっています。

ナビゲーションメニューも、ダッシュボード同様XMLで記述されています。初期状態では次のようになっています。

リスト5.1: ナビゲーションメニュー ソースコード

```
1: <nav search_view="search" color="#65A637">
2:   <view name="search" default='true' />
3:   <view name="datasets" />
4:   <view name="reports" />
5:   <view name="alerts" />
6:   <view name="dashboards" />
7: </nav>
```

ソースコード上に書かれたview要素が、左から順に並べられます。ダッシュボードをメニューに追加するには、<view name="ダッシュボード名" />を追加します。また`default="true"`を指定したview要素のメニューが、Appアクセス時にデフォルトで表示される画面となります。その他、`nav`要素の`color`の値を変更することで、メニューバーの色を変えることができます。

動的なダッシュボードを作成するためのドリルダウン機能も詳しく解説

第9章　ドリルダウンを使う

ドリルダウン機能を利用すると、あるパネルの情報を別のパネルのクエリーに利用するなど、フォーム同様に動的なダッシュボードが作成できます。またダッシュボード間で値を渡せるので、使いこなすことで高度なAppを作成することができます。本章ではその利用方法を紹介します。

9.1　ドリルダウンとは

ドリルダウンは一般的に「あるデータをさらに深掘りする機能」を指します。Splunkでは、あるパネルをクリックした際のアクションの定義で、他のコンポーネントに遷移したり、さらに値を渡したり、といったことを実現します。

9.1.1　ドリルダウンの設定

ドリルダウンは各パネルの「More actions」→「Edit Drilldown」から設定します。

9.1.2　ドリルダウンの種類

Splunkのドリルダウンでは、次のような機能が実現できます。

・Link to search
　―サーチ画面へリンク
・Link to dashboard
　―別のダッシュボードへリンク
・Link to report
　―レポートへリンク
・Link to custom URL
　―外部URLへリンク
・Manage tokens on this dashboard
　―このダッシュボードのトークンに値を設定

「Manage tokens on this dashboard」は、パネル内の情報をトークンに格納し、別のパネルでそのトークンを利用したクエリーを設定してパネル間の連携を行う機能です。この際、パネルに表示されるグラフ内のクリックした箇所のデータをトークンに格納する、といったことが行えるため、「気になるデータの情報を別のパネルで深掘りする」ということが実現できます。

また「Link to dashboard」では別のダッシュボードにトークンを渡すことができるほか、「Link to search」、「Link to custom URL」でもリンク先にパネル内の情報を渡すことができます。

この「値渡し」がドリルダウンの非常に重要な機能になります。

9.1.3　パネルから取得できる情報

パネル内からどのような情報を取得するかは、両端を$で囲んだトークンを参照する際の書式で指定します（パネル内の情報をトークンとして参照する、という理解でよいと思います）。

たとえば、あるグラフをクリックした場合のX軸の情報は、`"$click.value$"`で取得できます。表9.1は、参照可能な情報の代表的なものの一覧です。

表9.1: パネルから取得できる情報一覧

名前	取得される情報
$click.name$	X軸のフィールド名
$click.value$	クリックした箇所のX軸のデータの値
$click.name2$	Y軸のフィールド名（系列名）
$click.value2$	クリックした箇所のY軸のデータの値
$row.<fieldname>	クリックした箇所の指定したフィールドの情報

`$row.<fieldname>`は、実際にはフィールド名を指定します。例えば`$row.status`と指定した場合、テーブルであれば、クリックした行の`status`フィールドが取得されます。

9.1.4　ダッシュボード内ドリルダウンの設定

「Manage tokens on this dashboard」による、ダッシュボード内ドリルダウンの設定手順を紹介します。例として、次のようなシナリオを想定します。

1．Apacheアクセスログのステータスコードの出現頻度を示す円グラフから、任意のステータスコードをクリックする
2．そのステータスコードを返したURIとエージェントの情報を、別パネルに表示する

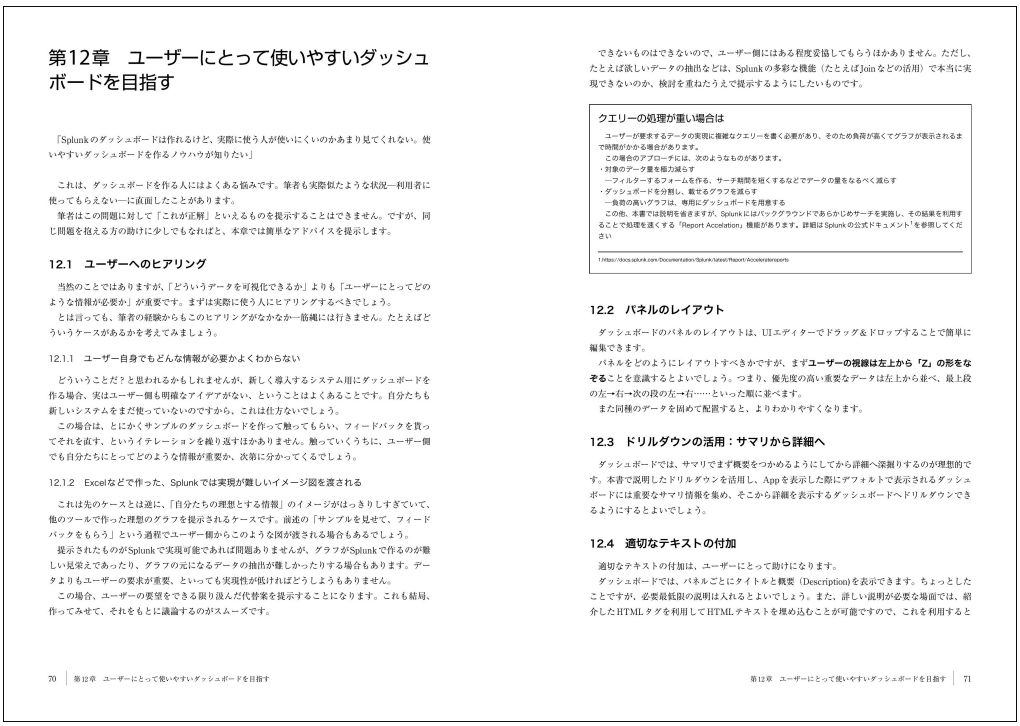
1.のクエリーはリスト9.1のようになります。

リスト9.1: ステータスコード円グラフ描画用クエリー

```
index=test sourcetype="access_combined" | stats count by status
```

このパネルでは、図9.1のようにドリルダウンを設定します。円グラフの場合、円に描画された各値の情報は`$click.value$`で取得できます。その値を、トークン「`status_drilldown`」に格納します。

実際にユーザーにダッシュボードを使ってもらうための注意点やノウハウを紹介



第12章　ユーザーにとって使いやすいダッシュボードを目指す

「Splunkのダッシュボードは作れるけど、実際に使う人が使いにくいのかあまり見てくれない。使いやすいダッシュボードを作るノウハウが知りたい」

これは、ダッシュボードを作る人にはよくある悩みです。筆者も実際似たような状況―利用者に使ってもらえない―に直面したことがあります。

筆者はこの問題に対して「これが正解」といえるものを提示することはできません。ですが、同じ問題を抱える方の助けに少しでもなればと、本章では簡単なアドバイスを提示します。

12.1　ユーザーへのヒアリング

当然のことではありますが、「どういうデータを可視化できるか」よりも「ユーザーにとってどのような情報が必要か」が重要です。まずは実際に使う人にヒアリングするべきでしょう。

とは言っても、筆者の経験からもこのヒアリングがなかなか一筋縄には行きません。たとえばどういうケースがあるかを考えてみましょう。

12.1.1　ユーザー自身でもどんな情報が必要かよくわからない

どういうことだ？と思われるかもしれませんが、新しく導入するシステム用にダッシュボードを作る場合、実はユーザー側も明確なアイデアがない、ということはよくあることです。自分たちも新しいシステムをまだ使っていないのですから、これは仕方ないでしょう。

この場合は、とにかくサンプルのダッシュボードを作って触ってもらい、フィードバックを貰ってそれを直す、というイテレーションを繰り返すほかありません。触っていくうちに、ユーザー側でも自分たちにとってどのような情報が重要か、次第に分かってくるでしょう。

12.1.2　Excelなどで作った、Splunkでは実現が難しいイメージ図を渡される

これは先のケースとは逆に、「自分たちの理想とする情報」のイメージがはっきりしすぎていて、他のツールで作った理想のグラフを提示されるケースです。前述の「サンプルを見せて、フィードバックをもらう」という過程でユーザー側からこのような図が渡される場合もあるでしょう。

提示されたものがSplunkで実現可能であれば問題ありませんが、グラフがSplunkで作るのが難しい見栄えであったり、グラフの元になるデータの抽出が難しかったりする場合もあります。データよりもユーザーの要求が重要、といっても実現性が低ければどうしようもありません。

この場合、ユーザーの要望をできる限り汲んだ代替案を提示することになります。これも結局、作ってみせて、それをもとに議論するのがスムーズです。

できないものはできないので、ユーザー側にはある程度妥協してもらうほかありません。ただし、たとえば欲しいデータの抽出などは、Splunkの多彩な機能（たとえばJoinなどの活用）で本当に実現できないのか、検討を重ねたうえで提示するようにしたいものです。

クエリーの処理が重い場合は

ユーザーが要求するデータの実現に複雑なクエリーを書く必要があり、そのため負荷が高くてグラフが表示されるまで時間がかかる場合があります。

この場合のアプローチには、次のようなものがあります。

・対象のデータ量を極力減らす
　―フィルターするフォームを作る、サーチ期間を短くするなどでデータの量をなるべく減らす
・ダッシュボードを分割し、載せるグラフを減らす
　―負荷の高いグラフは、専用にダッシュボードを用意する

この他、本書では説明を省きますが、Splunkにはバックグラウンドであらかじめサーチを実施し、その結果を利用することで処理を速くする「Report Accelation」機能があります。詳細はSplunkの公式ドキュメント[1]を参照してください

1 https://docs.splunk.com/Documentation/Splunk/latest/Report/Acceleratereports

12.2　パネルのレイアウト

ダッシュボードのパネルのレイアウトは、UIエディターでドラッグ＆ドロップすることで簡単に編集できます。

パネルをどのようにレイアウトすべきかですが、まず**ユーザーの視線は左上から「Z」の形をなぞる**ことを意識するとよいでしょう。つまり、優先度の高い重要なデータは左上から並べ、最上段の左→右→次の段の左→右……といった順に並べます。

また同種のデータを固めて配置すると、よりわかりやすくなります。

12.3　ドリルダウンの活用：サマリから詳細へ

ダッシュボードでは、サマリでまず概要をつかめるようにしてから詳細へ深掘りするのが理想的です。本書で説明したドリルダウンを活用し、Appを表示した際にデフォルトで表示されるダッシュボードには重要なサマリ情報を集め、そこから詳細を表示するダッシュボードへドリルダウンできるようにするとよいでしょう。

12.4　適切なテキストの付加

適切なテキストの付加は、ユーザーにとって助けになります。

ダッシュボードでは、パネルごとにタイトルと概要（Description）を表示できます。ちょっとしたことですが、必要最低限の説明は入れるとよいでしょう。また、詳しい説明が必要な場面では、紹介したHTMLタグを利用してHTMLテキストを埋め込むことが可能ですので、これを利用すると

＜＜目次＞＞

＜＜著者紹介＞＞

江口 佳記(えぐち よしき)
株式会社テリロジー所属のエンジニア(シニアスペシャリスト)。1978 年生。現在は主にセキュリティーソリューション事業に携わっている。
Twitter:@mochigumi07

＜＜販売ストア＞＞

電子書籍:
Amazon Kindle ストア、楽天 kobo イーブックストア、Apple Books、紀伊國屋書店 Kinoppy、Google Play Store、honto 電子書籍ストア、Sony Reader Store、BookLive!、BOOK☆WALKER
印刷書籍:
Amazon.co.jp、三省堂書店オンデマンド、honto ネットストア、楽天ブックス

※　各ストアでの販売は準備が整いしだい開始されます。
※　全国の一般書店からもご注文いただけます。

【株式会社インプレス R&D】 https://nextpublishing.jp/

株式会社インプレス R&D（本社：東京都千代田区、代表取締役社長：井芹昌信）は、デジタルファーストの次世代型電子出版プラットフォーム「NextPublishing」を運営する企業です。また自らも、NextPublishing を使った「インターネット白書」の出版など IT 関連メディア事業を展開しています。

※NextPublishing は、インプレス R&D が開発した電子出版プラットフォーム（またはメソッド）の名称です。電子書籍と印刷書籍の同時制作、プリント・オンデマンド（POD）による品切れ解消などの伝統的出版の課題を解決しています。これにより、伝統的出版では経済的に困難な多品種少部数の出版を可能にし、優秀な個人や組織が持つ多様な知の流通を目指しています。

【インプレスグループ】 https://www.impressholdings.com/

株式会社インプレスホールディングス（本社：東京都千代田区、代表取締役：唐島夏生、証券コード：東証 1 部 9479）を持株会社とするメディアグループ。「IT」「音楽」「デザイン」「山岳・自然」「旅・鉄道」「学術・理工学」を主要テーマに専門性の高いメデイア&サービスおよびソリューション事業を展開しています。さらに、コンテンツビジネスのプラットフォーム開発・運営も手がけています。

【お問い合わせ先】

株式会社インプレス R&D NextPublishing センター
TEL 03-6837-4820
電子メール: np-info@impress.co.jp