# Rolieサーバーマニュアル

* (株)レピダム 菊池正史
* 2015/09/09

## セットアップ

* 通常のRailsと同様

$ ruby --version  
ruby 2.2.1p85 (2015-02-26 revision 49769) [i686-linux]

$ cd rolie-server  
$ bundle install  
Using rake 10.4.2  
略  
Bundle complete! 13 Gemfile dependencies, 54 gems now installed.  
Use `bundle show [gemname]` to see where a bundled gem is installed.

$ rake db:setup

* サーバーの起動

$ rails s  
=> Booting WEBrick  
=> Rails 4.2.3 application starting in development on http://localhost:3000  
=> Run `rails server -h` for more startup options  
=> Ctrl-C to shutdown server  
Unimplemented block at relaxng.c:3822  
[2015-09-01 20:43:48] INFO WEBrick 1.3.1  
[2015-09-01 20:43:48] INFO ruby 2.2.1 (2015-02-26) [i686-linux]  
[2015-09-01 20:43:48] INFO WEBrick::HTTPServer#start: pid=17872 port=3000

## 実行例

### トップページにアクセス

$ curl http://localhost:3000  
<!DOCTYPE html>  
<html>  
<head>  
 <title>RolieServer</title>  
 <link rel="stylesheet" media="all" href="/assets/application.self-e80e8f2318043e8af94dddc2adad5a4f09739a8ebb323b3ab31cd71d45fd9113.css?body=1" data-turbolinks-track="true" />  
 <script src="/assets/jquery.self-d03a5518f45df77341bdbe6201ba3bfa547ebba8ed64f0ea56bfa5f96ea7c074.js?body=1" data-turbolinks-track="true"></script>  
<script src="/assets/jquery\_ujs.self-ca5248a2fad13d6bd58ea121318d642f195f0b2dd818b30615f785ff365e8d1f.js?body=1" data-turbolinks-track="true"></script>  
<script src="/assets/turbolinks.self-c37727e9bd6b2735da5c311aa83fead54ed0be6cc8bd9a65309e9c5abe2cbfff.js?body=1" data-turbolinks-track="true"></script>  
<script src="/assets/application.self-3b8dabdc891efe46b9a144b400ad69e37d7e5876bdc39dee783419a69d7ca819.js?body=1" data-turbolinks-track="true"></script>  
 <meta name="csrf-param" content="authenticity\_token" />  
<meta name="csrf-token" content="uf0UK0gXmwRp0GDzKxaxIWuGT5PBGXk/gc/L6s+yxiRSw6vM6bIfv3991u2lRc96Rr2/msItoZu2aVg+/RRYXg==" />  
 <link rel="introspection" type="application/atomsvc+xml" title="Atom Publishing Protocol Service Document" href="http://localhost:3000/csirt/svcdoc.xml" />  
</head>  
<body>  
  
<h1>Service#index</h1>  
<p>Find me in app/views/service/index.html.erb</p>  
  
  
</body>  
</html>

head内のリンク をたどる

### サービス定義ファイルを取得

$ curl http://localhost:3000/csirt/svcdoc.xml  
<?xml version="1.0"?>  
<service xmlns="http://www.w3.org/2007/app" xmlns:atom="http://www.w3.org/2005/Atom">  
 <workspace>  
 <atom:title type="text">public</atom:title>  
 <collection href="http://localhost:3000/csirt/public/incidents">  
 <atom:title type="text">public incidents</atom:title>  
 <accept>application/atom+xml; type=entry</accept>  
 </collection>  
 </workspace>  
 <workspace>  
 <atom:title type="text">private</atom:title>  
 <collection href="http://localhost:3000/csirt/private/incidents">  
 <atom:title type="text">private incidents</atom:title>  
 <accept>application/atom+xml; type=entry</accept>  
 </collection>  
 </workspace>  
</service>

### コレクションのfeedを取得

最初なのでfeedは空

$ curl http://localhost:3000/csirt/public/incidents  
<?xml version="1.0" encoding="utf-8"?>  
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://www.w3.org/2005/Atom file:/C:/schemas/atom.xsd urn:ietf:params:xml:ns:iodef-1.0 file:/C:/schemas/iodef-1.0.xsd">  
 <generator>ROLIE prototype server</generator>  
 <id>http://localhost:3000/csirt/public/incidents</id>  
 <title type="text">public incidents</title>  
 <updated>2015-09-07T19:41:26+09:00</updated>  
 <author>  
 <email>csirt@example.org</email>  
 <name>EMC CSIRT</name>  
 </author>  
 <author>  
 <email>csirt2@example.org</email>  
 </author>  
 <link href="http://localhost:3000/csirt/public/incidents" rel="self"/>  
 <link href="http://localhost:3000/searchspec/public/incidents" rel="search" type="application/opensearchdescription+xml" title="CSIRT search facility"/>  
</feed>

### エントリーを追加

doc/example/minimum-entry.xml を追加する

$ curl -D - -X POST http://localhost:3000/csirt/public/incidents --data-binary @minimum-entry.xml   
HTTP/1.1 201 Created   
X-Frame-Options: SAMEORIGIN  
X-Xss-Protection: 1; mode=block  
X-Content-Type-Options: nosniff  
Location: http://localhost:3000/csirt/public/incidents/1  
Content-Type: application/xml; charset=utf-8  
Etag: W/"88f554162802ce81863855243b66a5be"  
Cache-Control: max-age=0, private, must-revalidate  
X-Request-Id: dae68a3e-4e44-40a7-b57b-4b74ca401173  
X-Runtime: 0.483025  
Server: WEBrick/1.3.1 (Ruby/2.2.1/2015-02-26)  
Date: Mon, 07 Sep 2015 12:03:43 GMT  
Content-Length: 878  
Connection: Keep-Alive  
Set-Cookie: request\_method=POST; path=/  
  
<?xml version="1.0" encoding="utf-8"?>  
<entry>  
 <id>http://localhost:3000/csirt/public/incidents/1</id>  
 <title>test</title>  
 <link href="http://localhost:3000/csirt/public/incidents/1" rel="self"/>  
 <link href="http://localhost:3000/csirt/public/incidents/1" rel="alternate"/>  
 <published>2001-09-13T23:19:24+00:00</published>  
 <updated>2015-09-07T12:03:43+00:00</updated>  
 <category/>  
 <content type="application/xml">  
 <IODEF-Document xmlns="urn:ietf:params:xml:ns:iodef-1.0" lang="en">  
 <Incident purpose="reporting">  
 <IncidentID name="http://localhost:3000/csirt/public/incidents">1</IncidentID>  
 <ReportTime>2001-09-13T23:19:24+00:00</ReportTime>  
 <Assessment>  
 <Impact completion="failed" type="admin"/>  
 </Assessment>  
 <Contact role="creator" type="organization">  
 </Contact>  
 </Incident>  
</IODEF-Document>  
 </content>  
</entry>

* 201 Created が返る
* Location ヘッダに新しい URL が返る
* 元のドキュメントの中で、id 要素と IncidentID 要素は新しいものに更新される

### 更新されたfeedを取得

$ curl http://localhost:3000/csirt/public/incidents  
<?xml version="1.0" encoding="utf-8"?>  
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://www.w3.org/2005/Atom file:/C:/schemas/atom.xsd urn:ietf:params:xml:ns:iodef-1.0 file:/C:/schemas/iodef-1.0.xsd">  
 <generator>ROLIE prototype server</generator>  
 <id>http://localhost:3000/csirt/public/incidents</id>  
 <title type="text">public incidents</title>  
 <updated>2015-09-07T21:16:43+09:00</updated>  
 <author>  
 <email>csirt@example.org</email>  
 <name>EMC CSIRT</name>  
 </author>  
 <author>  
 <email>csirt2@example.org</email>  
 </author>  
 <link href="http://localhost:3000/csirt/public/incidents" rel="self"/>  
 <link href="http://localhost:3000/searchspec/public/incidents" rel="search" type="application/opensearchdescription+xml" title="CSIRT search facility"/>  
 <entry>  
 <id>http://localhost:3000/csirt/public/incidents/1</id>  
 <title>test</title>  
 <link href="http://localhost:3000/csirt/public/incidents/1" rel="self"/>  
 <link href="http://localhost:3000/csirt/public/incidents/1" rel="alternate"/>  
 <published>2001-09-13T23:19:24+00:00</published>  
 <updated>2015-09-07T12:03:43+00:00</updated>  
 <category/>  
 </entry>  
</feed>

### エントリーを取得

$ curl http://localhost:3000/csirt/public/incidents/1  
<?xml version="1.0" encoding="utf-8"?>  
<entry>  
 <id>http://localhost:3000/csirt/public/incidents/1</id>  
 <title>test</title>  
 <link href="http://localhost:3000/csirt/public/incidents/1" rel="self"/>  
 <link href="http://localhost:3000/csirt/public/incidents/1" rel="alternate"/>  
 <published>2001-09-13T23:19:24+00:00</published>  
 <updated>2015-09-07T12:03:43+00:00</updated>  
 <category/>  
 <content type="application/xml">  
 <IODEF-Document xmlns="urn:ietf:params:xml:ns:iodef-1.0" lang="en">  
 <Incident purpose="reporting">  
 <IncidentID name="http://localhost:3000/csirt/public/incidents">1</IncidentID>  
 <ReportTime>2001-09-13T23:19:24+00:00</ReportTime>  
 <Assessment>  
 <Impact completion="failed" type="admin"/>  
 </Assessment>  
 <Contact role="creator" type="organization">  
 </Contact>  
 </Incident>  
</IODEF-Document>  
 </content>  
</entry>

### 既存エントリーに上書き

$ curl -X PUT http://localhost:3000/csirt/public/incidents/1 --data-binary @codered-entry.xml   
<?xml version="1.0" encoding="utf-8"?>  
<entry>  
 <id>http://localhost:3000/csirt/public/incidents/1</id>  
 <title>Code Red</title>  
 <link href="http://localhost:3000/csirt/public/incidents/1" rel="self"/>  
 <link href="http://localhost:3000/csirt/public/incidents/1" rel="alternate"/>  
 <link href="http://www.example.org/csirt/private/incidents/123456/relationships/indicators" rel="indicators"/>  
 <link href="http://www.example.org/csirt/private/incidents/1234456/relationships/history" rel="history"/>  
 <link href="http://www.example.org/csirt/private/incidents/1234456/relationships/campaign" rel="campaign"/>  
 <published>2001-09-13T23:19:24+00:00</published>  
 <updated>2015-09-07T12:50:05+00:00</updated>  
 <category/>  
 <summary>Host sending out Code Red probes</summary>  
 <content type="application/xml">  
 <IODEF-Document xmlns="urn:ietf:params:xml:ns:iodef-1.0" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" version="1.00" lang="en" xsi:schemaLocation="urn:ietf:params:xml:schema:iodef-1.0">  
 <Incident purpose="reporting">  
 <IncidentID name="http://localhost:3000/csirt/public/incidents">1</IncidentID>  
 <ReportTime>2001-09-13T23:19:24+00:00</ReportTime>  
 <Description>Host sending out Code Red probes</Description>  
 <!-- An administrative privilege was attempted, but failed -->  
 <Assessment>  
 <Impact completion="failed" type="admin"/>  
 </Assessment>  
 <Contact role="creator" type="organization">  
 <ContactName>Example.com CSIRT</ContactName>  
 <RegistryHandle registry="arin">example-com</RegistryHandle>  
 <Email>contact@csirt.example.com</Email>  
 </Contact>  
 <EventData>  
 <Flow>  
 <System category="source">  
 <Node>  
 <Address category="ipv4-addr">192.0.2.200</Address>  
 <Counter type="event">57</Counter>  
 </Node>  
 </System>  
 <System category="target">  
 <Node>  
 <Address category="ipv4-net">192.0.2.16/28</Address>  
 </Node>  
 <Service ip\_protocol="6">  
 <Port>80</Port>  
 </Service>  
 </System>  
 </Flow>  
 <Expectation action="block-host"/>  
 <!-- <RecordItem> has an excerpt from a log -->  
 <Record>  
 <RecordData>  
 <DateTime>2001-09-13T18:11:21+02:00</DateTime>  
 <Description>Web-server logs</Description>  
 <RecordItem dtype="string">  
 192.0.2.1 - - [13/Sep/2001:18:11:21 +0200] "GET /default.ida?  
 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
 XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
 </RecordItem>  
 <!-- Additional logs -->  
 <RecordItem dtype="url">  
 http://mylogs.example.com/logs/httpd\_access</RecordItem>  
 </RecordData>  
 </Record>  
 </EventData>  
 <History>  
 <!-- Contact was previously made with the source network owner -->  
 <HistoryItem action="contact-source-site">  
 <DateTime>2001-09-14T08:19:01+00:00</DateTime>  
 <Description>Notification sent to  
 constituency-contact@192.0.2.200</Description>  
 </HistoryItem>  
 </History>  
 </Incident>  
</IODEF-Document>  
 </content>  
</entry>

### エントリーの削除

$ curl -D - -X DELETE http://localhost:3000/csirt/public/incidents/1  
HTTP/1.1 200 OK   
X-Frame-Options: SAMEORIGIN  
X-Xss-Protection: 1; mode=block  
X-Content-Type-Options: nosniff  
Content-Type: text/plain; charset=utf-8  
Cache-Control: no-cache  
X-Request-Id: f6c9ac31-fd30-4dcb-ba02-ba847998a814  
X-Runtime: 0.033875  
Server: WEBrick/1.3.1 (Ruby/2.2.1/2015-02-26)  
Date: Mon, 07 Sep 2015 13:11:07 GMT  
Content-Length: 0  
Connection: Keep-Alive  
Set-Cookie: request\_method=DELETE; path=/

### OpenSearch 検索フォーマットの取得

$ curl http://localhost:3000/searchspec/public/incidents  
<?xml version="1.0" encoding="utf-8"?>  
<OpenSearchDescription xmlns="http://a9.com/-/spec/opensearch/1.1/">  
 <ShortName>CSIRT search</ShortName>  
 <Description>Cyber security information sharing consortium search interface</Description>  
 <Tags>example csirt indicator search</Tags>  
 <Contact>admin@example.org</Contact>  
 <Url type="application/opensearchdescription+xml" rel="self" template="http://localhost:3000/searchspec/public/incidents"/>  
 <Url type="application/atom+xml" rel="results" template="http://localhost:3000/csirt/public/incidents?q={searchTerms}"/>  
 <LongName>www.example.org CSIRT search</LongName>  
 <Query role="example" searchTerms="incident"/>  
 <Language>en-us</Language>  
 <OutputEncoding>UTF-8</OutputEncoding>  
 <InputEncoding>UTF-8</InputEncoding>  
</OpenSearchDescription>

### 検索

$ curl http://localhost:3000/csirt/public/incidents?q=foo  
<?xml version="1.0" encoding="utf-8"?>  
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="http://www.w3.org/2005/Atom file:/C:/schemas/atom.xsd urn:ietf:params:xml:ns:iodef-1.0 file:/C:/schemas/iodef-1.0.xsd">  
 <generator>ROLIE prototype server</generator>  
 <id>http://localhost:3000/csirt/public/incidents</id>  
 <title type="text">public incidents</title>  
 <updated>2015-09-08T20:42:00+09:00</updated>  
 <author>  
 <email>csirt@example.org</email>  
 <name>EMC CSIRT</name>  
 </author>  
 <author>  
 <email>csirt2@example.org</email>  
 </author>  
 <link href="http://localhost:3000/csirt/public/incidents" rel="self"/>  
 <link href="http://localhost:3000/searchspec/public/incidents" rel="search" type="application/opensearchdescription+xml" title="CSIRT search facility"/>  
</feed>