ＣＴＣ教育サービス　News&Topics　　2011年7月号

発行元：ＣＴＣ教育サービス

目次

ニュース

◆◇　CISCO認定　CCNP関連コースにバウチャー付きコース新設　◇◆

この度、ＣＴＣ教育サービス（ＣＴＣテクノロジー）では
シスコ認定CCNP関連３コース（ROUTE、SWITCH、Tshoot）において、
バウチャーチケット付きコースの提供を開始させていただきます。
http://www.school.ctc-g.co.jp/news/20110701.html

N525V：『ROUTE(Implementing Cisco IP Routing)(試験バウチャー付)』
　期間：5日間
　金額：¥262,500（税込）
　開催日程：8/1-5　　9/5-9　　10/17-21　　11/14-18

N526V：『SWITCH(Implementing Cisco IP Switched Networks)
　　(試験バウチャー付)』
　期間：5日間
　金額：¥262,500（税込）
　開催日程：8/8-12　　9/12-16　　10/24-28　　11/28-12/2

N527V：『Tshoot(Troubleshooting and Maintaining Cisco IP Networks)
　　(試験バウチャー付)』
　期間：5日間
　金額：¥262,500（税込）
　開催日程：8/29-9/2　　9/26-30　　11/21-25　　12/19-22

Cisco関連技術のスキルアップはもちろん、認定試験のサポートも実施いたします。
この機会に是非ともご活用ください。

◆◇Ruby技術者認定試験合格者の声　◇◆
◆◇　＆まつもとゆきひろ氏からのメッセージ掲載◇◆

Ruby Association Certified Ruby Programmer 認定資格を取得された方に、
試験を受けるきっかけをはじめ、Ruby技術者認定試験に合格し、職場や趣味に
活用されているご経験や技術者として大事にしていることなどをお聞きしました。
さらに、Ruby開発者であるまつもとゆきひろ氏から、 受験をお考えの方に
メッセージをいただきました。

Ruby技術者認定試験の受験を検討されている方やRubyにご興味のある方は、
是非ご一読ください。
http://www.school.ctc-g.co.jp/voice_ruby/index.html

Ruby認定資格の受験をご検討の皆様には、資格対策コースもご用意しています！

http://www.school.ctc-g.co.jp/ruby/index.html

R020： Ruby技術者認定試験Silver（RYO-100）対策
　期間：1日間
　金額：¥39,900（税込）
　開催日程：11/18

R021： Ruby技術者認定試験Gold（RYO-200）対策
　期間：1日間
　金額：¥39,900（税込）
　開催日程：9/12　　12/19

トピック

◆◇『 Inst. Tech View～第4回“Ruby on Rails セキュリティ対策”～ 』◇◆

今回の Inst. Tech View は、生産性の高いWebアプリケーションフレームワーク
であるRuby on Railsのセキュリティ機能についての話題です。

Ruby on Railsはプログラミング言語Rubyで開発されたWebアプリケーション
フレームワークです。Webアプリケーションフレームワークとは、
Webアプリケーションを開発する際に頻繁に必要とされる機能を提供する
ソフトウェアです。Ruby on Railsを使用することで本来実現したい機能に集中し、
アプリケーションをスピーディに開発することができます。

Ruby on Railsは様々な機能を備えたフレームワークですが、その中でも
セキュリティ対策における機能をご紹介します。

Webアプリケーションにおける代表的な脆弱性としては以下のようなものが
挙げられます。
◇ SQLインジェクション
◆ クロスサイトスクリプティング(XSS)
◇ クロスサイトリクエストフォージェリ(CSRF)
◆ OSコマンド／スクリプトインジェクション
◇ セッション固定攻撃
◆ パラメータマニピュレーション

今回は、上記の脆弱性の中でもXSS、CSRFの対策方法に注目します。

XSSはWebページの入力フォームから入力した内容を適切にエスケープしないまま
HTML中に出力することで、入力中に存在するタグ等の文字がそのままHTMLとして
解釈されることを悪用した攻撃です。
これによりJavascript等のスクリプトが実行されてセッションハイジャック
などの悪意のある行為が行われてしまう可能性があります。

Ruby on Railsのバージョンによって対応方法は異なりますが、
バージョン3からは自動で特殊文字がエスケープされますので、
入力内容の表示部分では以下のように記述することができます。

以下はRuby on Railsで作成したWebアプリケーションの一部で、
ブログなどで入力されたタイトルを表示する例です。

```
# タイトルに「<script>alert("crack");</script>」が
  入力されていたとします。

| <h1><%= @title %></h1>
#=> <h1>&lt;script&gt;alert(&quot;crack&quot;);&lt;/script&gt;</h1>
```

テンプレートエンジンによって記号がエスケープされている事がわかります。

また、XSSの攻撃対象に成りかねないのであまり推奨されておりませんが、
敢えてエスケープ処理を行わせない場合rawメソッドを使用します。

```
  | <h1><%= raw @title %></h1>
  #=> <h1><script>alert("crack");</script></h1>
```

次に、CSRFの対策方法です。
CSRFは別のサイトに用意したコンテンツ上にある罠のリンクを踏ませること等を
きっかけとして不正なコードを実行させる攻撃です。
例えば正規アカウントのセッションを利用し、ショッピングの決済や
アカウント退会などの重要な処理が行われてしまう可能性があります。

これに対してRuby on RailsではデフォルトでCSRFの対策が行われております。
不正なアクセスであれば自動で例外処理を行う、protect_from_forgeryという
メソッドがすべてのコントローラに適用されるコントローラクラスに
記述されています。
これにより、form_for等のメソッドで生成するフォームに自動でトークンが
埋め込まれ、入力された値と合わせてトークンがサーバに送られます。
このトークンを用いて自動照合が行われ、正規の入力フォームからの入力かを
判断します。
これにより強制的に送りつけられたパラメータを除外することができ、
対策に繋がります。

Ruby on Railsは様々なWebアプリケーションの脆弱性に対してデフォルトで
対応しているなど、初心者でも入りやすいフレームワークです。
弊社トレーニングを参考にRuby on Railsを始めてみてはいかがでしょうか。

コースの詳細情報はこちら：
「Ruby on Rails」関連コース
http://www.school.ctc-g.co.jp/ruby/

コラム

◆◇　スーパーエンジニアの独り言　第1回　“Java SE 7 登場”　』　◇◆

今回から始まったスーパーエンジニアの独り言。
最初の話題は、7月28日にメジャーバージョンアップの正式リリースが
予定されている「Java SE 7 (JDK 7)」の話題です。

新機能として搭載が予定されている主要な機能は以下が挙げられます。
◇ もっと新 I/O ("NIO.2") (JSR 203)
◆ 細かな構文変更 (Project Coin) の一部 (JSR 334)
◇ JVMの動的型付け言語のサポート (JSR 292)
◆ G1ガベージコレクタの導入 (Garbage-First GC)
◇ クラスローダの拡張
◆ Unicode 6.0
◇ etc ...

ライブラリでの機能拡張の目玉として "NIO.2" で非同期入出力サポートである
java.nio.channels パッケージが用意されます。

これには "AsynchronousSocketChannel" など4つの非同期チャネルがあり、
バッファ(ByteBuffer)を取得し、それに対して読み取り/書き込みすることで、
処理が非同期で行われます。非同期チャネルによって下位のファイルやソケット
は、隠蔽され抽象化されます。また実行プラットフォームの対応次第では、
ネイティブな非同期機能が利用されることで、実行速度の向上も見込めます。

次に「言語仕様の細かな変更(Project Coin)」と題されている新機能では、
コーディングでの記述構文の一部が変更されて簡略表記が可能になりました。
（「細かい」ので、コインなんだそうです。）

例えば、Genericsでの例を挙げますと、従来では

```
Map<String, Collection<Integer>> map
    = new LinkedHashMap<String, Collection<Integer>>();
```

と書いていましたが、Java SE 7 では、

```
Map<String, Collection<Integer>> map
    = new LinkedHashMap<>();
```

と、右辺の型指定が省略できるように構文が改良されました。
（これを "Diamond Syntax" と呼ぶようです。省略された "<>" が、
ダイヤモンドに見えるからだそうです。）

他にも構文変更では、"switch" 構文での条件式に "String" オブジェクトを
使えるなどといった細かな変更が多数ある様子です。

プログラマにとってだけでなく、メインテナンスでの互換性の問題も含めて
シンタックスが変わるのは結構悩ましいことですが、簡略化できるという事で
可読性が落ちない様に、コーディングすることが重要になるでしょう。

他の新機能についてのご紹介は、機会があればまたいずれ。

今回の新機能で搭載が期待されており、大きな話題であったクロージャ
(Project Lambda) は、結局 Java SE 8 へと持ち越しになりました。

Java SE 6 で仕様確定の際に実現を見送った機能が、次期に盛り込まれる予定で
Java SE 7 では長期にわたり新機能への取り組みがなされてました。紆余曲折を
経た末に全てを盛り込む事が出来ず、再度 Java 8 へと申し送りされました。
今後は Java 自体の方向性として Java 8 を注視するのが肝要となるでしょう。

現在、最もポピュラーなプログラミング言語であり、アプリケーションの実行環境
としてもデファクトスタンダードの位置を確保しているのが "Java" です。
単なるプログラムではなく実行処理系としてJVMがシステムの重要な位置を占め
ているのは既知であり、将来を見越しても当面その座は揺るがないでしょう。
Java VMに於ける「動的型付け言語のサポート」こそが、JRubyを代表とする
処理系の誘致を示しているのであり、そこからも計り知れます。

まさにクラウドコンピューティングに於いても開発言語としてだけではなく
実行環境及びシステム／サービス間のインターフェースとして必須の知識です。

"Java 5" で文法自身に大きな変更が加えられたのは知っているものの、
いわゆる"Java 2" までの理解で完了していて現在進行している動向に
追従できていない方々が（筆者を含めて）大勢いることかと思います。
あらゆるシステムが、仮想化／クラウドサービス化されていくのを機会に、
Java 関連の棚卸しするために知識の習得／再確認されるのは如何でしょうか？
（トレーニングコースも順次、新バージョンにアップデートされる予定です。）

コースの詳細情報はこちら：

「Java」関連コース
http://www.school.ctc-g.co.jp/java/

「クラウド・仮想化」関連コース
http://www.school.ctc-g.co.jp/cldvir/

■お問合せ・ご意見・ご感想は◆ＣＴＣ教育サービス◆窓口まで――――――――
シーティーシー・テクノロジー株式会社　エデュケーションサービス部
E-Mail： kyouiku@ctc-g.co.jp / TEL： 03-5712-8701

――

●外部委託について
　　弊社はメールニュース配信業務をシーティーシー・ビジネスサービス
　　株式会社（ＣＴＣ100%出資子会社）に委託しております。
●本メールマガジン編集・配信責任者
　　ＣＴＣＴ　エデュケーションサービス部　部長　篠原　義一
　　所在地：東京都世田谷区駒沢1-16-7　ctc_edu_mail@ctc-g.co.jp
●個人情報保護方針
　　ＣＴＣグループの個人情報保護方針につきましては下記ＵＲＬをご参照
　　ください。
　　http://www.ctc-g.co.jp/guide/security_policy.html?top=b_security
●配信中止及びお問合せ対応について
・「ＣＴＣ教育サービス　News&Topics」の配信が不要な場合には、
　下記ＵＲＬから配信停止のお手続きを行ってください。
　　https://krs.bz/ctc-g/m/ctc-education
・当社では、複数種類のメールマガジンやメールニュースを発行しております。
　大変お手数ではございますが、ＣＴＣ教育サービス以外からのメール配信に
　ついての受信拒否および個人情報に関するご要求は、各メールに記載の個々
　の連絡先宛にそれぞれご連絡をお願いします。
・受信者ご本人様からの個人情報の開示・訂正・削除に関するご要求は、随時
　ctc_edu_mail@ctc-g.co.jpにてお受けいたします。
――