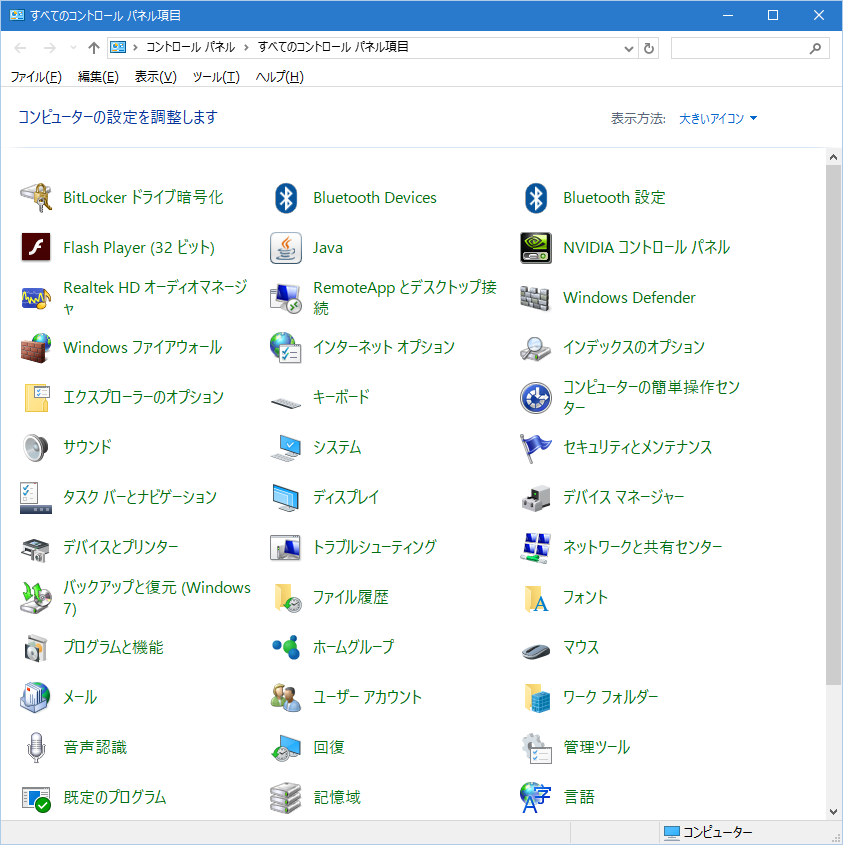
Chapter5　セキュリティ演習

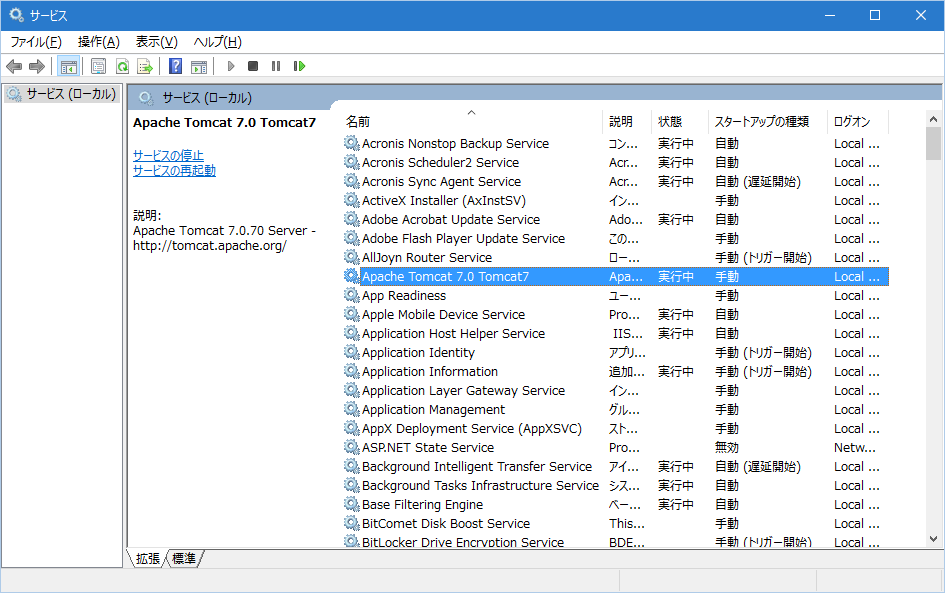
# 以下のアプリケーションを設定してください

Chapter5フォルダーのなかの、**ScriptInjectionSample**フォルダーを、**C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps**フォルダーにコピーします。

コントロールパネルを、右肩の設定で「大きなアイコン」に変更します。



「**管理ツール**」をダブルクリックして、開かれたウィンドウのなかから、「**サービス**」をダブルクリックして開きます。

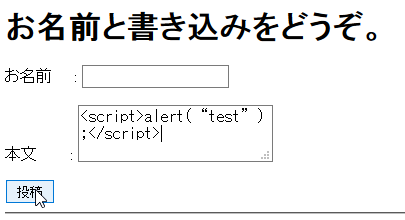


「**Apache Tomcat 7.0 Tomcat7**」を右クリックして、開始、または再起動を選択します。これでTomcatが再起動されます。

# Webブラウザを開き、以下の操作を実行してください

<http://localhost:8080/ScriptInjectionSample/crossSiteScriptingTest.jsp> を開きます。

掲示板が表示されるので、 <script>alert(“test”);</script> と入力してください。投稿ボタンをクリックすると、alertダイアログが表示されるのを確認してください。

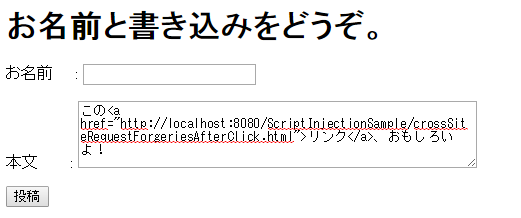


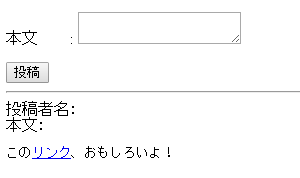
# Webブラウザを開き、以下の操作を実行してください

ブラウザを閉じ、Tomcatを再起動します。（可能なら別のブラウザで）<http://localhost:8080/ScriptInjectionSample/crossSiteScriptingTest.jsp> を開きます。

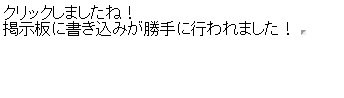
掲示板に以下の投稿を行ってください。コピペの場合、変なスペースが入ったり、 “ が全角になったりしているので注意！！！

「 この<a href=” http://localhost:8080/ScriptInjectionSample/crossSiteRequestForgeriesAfterClick.html”>リンク</a>、おもしろいよ！」



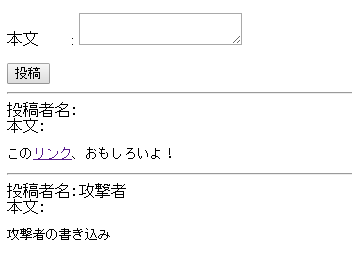


リンクをクリックします。すると、以下のように自動投稿がされます。



掲示板をもう一度開きます。

<http://localhost:8080/ScriptInjectionSample/crossSiteScriptingTest.jsp>



リンクをクリックしたことで、自動的に攻撃者の投稿がされています。