

web アプリケーションでの IP 制限

■ 設定ファイル

- CATALINA_HOME/conf/{EngineName}/{hostname}/{WebAppName}.xml
- CATALINA_HOME/webapps/{WebAppName}/WEB-INF/context.xml
- WAR ファイル内の WEB-INF/context.xml

■ 設定内容

- Context 要素に Valve 要素を作成

```
<Context>
  <Valve className="org.apache.catalina.valves.RemoteAddrValve" allow="127.0.0.1,192.168.*.*" />
</Context>
```

Host での IP 制限

- 調査中
- Host 要素に上記 Valve を作る ? (未確認)

参考サイト

■ [JBoss 3.2.7 + Tomcat] ホスト /IP によるクライアントのアクセス制限 / CannGuLoo.do

- <http://cannguloo.seesaa.net/article/7836000.html>

Jakarta Tomcat + AJP + JBoss 使用時、IP やホスト名で接続先を制限したい場合は Tomcat の バルブ を使うとかなり幸せ。

```
<Valve className="org.apache.catalina.valves.RemoteAddrValve" allow="192.168.1.10, 192.168.20.10, 192.168.30.*" deny="" />
```

■ LimitAccessToCertainClients / JBoss.org

- <http://wiki.jboss.org/wiki/Wiki.jsp?page=LimitAccessToCertainClients>

```
<Context debug="1" privileged="true" >
  <Valve className="org.apache.catalina.valves.RemoteAddrValve?" allow="10.254.*.*" deny="" />
</Context>
```

No editing of the Tomcat server.xml is required unless you're applying valves to Hosts.

- Tomcat の server.xml を編集する必要はない。Hosts 要素で制限する場合でなければ。

■ The Valve Component / apache-tomcat

- <http://tomcat.apache.org/tomcat-5.5-doc/config/valve.html>
- クライアント IP での接続制御
- className: org.apache.catalina.valves.RemoteAddrValve.

A comma-separated list of regular expression patterns that the remote client's IP address is compared to. If this attribute is specified, the remote address **MUST** match for this request to be accepted. If this attribute is not specified, all requests will be accepted **UNLESS** the remote address matches a deny pattern.

- allow: コンマ区切りの正規表現で IP アドレスを記述する。
- allow が指定された場合は、接続が許可されるにはクライアント IP が合致しなければならない。合致しない場合には接続が拒否される。
- allow が指定されず、deny で指定したパターンに合致しない場合は許可される。

A comma-separated list of regular expression patterns that the remote client's IP address is compared to. If this attribute is specified, the remote address **MUST NOT** match for this request to be accepted. If this attribute is not specified, request acceptance is governed solely by the accept attribute.

- deny: コンマ区切りの正規表現で IP アドレスを記述する。
- deny が指定された場合は、パターンが合致してはならない
- deny が指定されていない場合は、accept でのみ接続が制御される。