DNS と Apache にまつわる注意事項

本文書の内容は次の一言に尽きます。「Apache が設定ファイルを読み込むときに DNS を使用する必要がないようにして下さい」。Apache が設定ファイルを 読み込むときに DNS を使用する必要がある場合、信頼性の問題（起動しないかもしれません）やサービス拒否や盗用アタック（他のユーザからヒットを盗むことを含みます）の問題に直面するかもしれません。

トピック

簡単な例

```
<VirtualHost www.abc.dom>
ServerAdmin webgirl@abc.dom
DocumentRoot /www/abc
</VirtualHost>
```

Apache が正常に機能するには、バーチャルホスト毎に必ず二つの 情報が必要になります。それは、 ServerName と、そのサーバが応答するための IP（最低一つ）です。 この例では IP アドレスを含んでいませんので、Apache は DNS を使用して www.abc.dom を見つけなければなりません。 何らかの理由で設定ファイルを読み込んでいるときに DNS が利用できなかった場合、 バーチャルホストは設定されません。 そして、そのバーチャルホストに対するヒットには応答がなされません（Apache 1.2 以前では起動すらしません）。

www.abc.dom のアドレスが 10.0.0.1 だとします。では、次の設定について考えてみましょう。

```
<VirtualHost 10.0.0.1>
ServerAdmin webgirl@abc.dom
DocumentRoot /www/abc
</VirtualHost>
```

現在のリリースでは Apache は DNS 逆引きを使用して このバーチャルホストの ServerName を見つけます。 その逆引きが失敗した場合は部分的にバーチャルホストを無効にします (Apache 1.2 より前では起動すらしません)。 バーチャルホストが名前ベースであれば完全に無効になりますが、 IP ベースであれば概ね動作します。しかしながら、サーバ名を 含む完全な URL を生成しなければならない場合は、正しい URL の生成ができません。

次の例は上記の問題を解決しています。

```
<VirtualHost 10.0.0.1>
ServerName www.abc.dom
ServerAdmin webgirl@abc.dom
DocumentRoot /www/abc
```

```
</VirtualHost>
```

サービス拒否

サービス拒否が起こる場合、(少なくとも) 二つのケースがあります。 Apache 1.2 より前を実行している場合、バーチャルホストのための 上記の二つの DNS 検索のうち一つ失敗すれば起動すらしません。 そしてこの DNS 検索が自分の制御下にすらない場合もありえます。 例えば、abc.dom が顧客のサーバの一つで、 DNS は顧客自身で管理している場合、単に www.abc.dom レコードを削除するだけで、 (1.2 より前の) サーバを起動不能にすることができます。

もう一つのケースは、より気付きにくいものです。 次の設定について考えてみましょう。

```
<VirtualHost www.abc.dom>
  ServerAdmin webgirl@abc.dom
  DocumentRoot /www/abc
</VirtualHost>

<VirtualHost www.def.dom>
  ServerAdmin webguy@def.dom
  DocumentRoot /www/def
</VirtualHost>
```

10.0.0.1 を www.abc.dom に、 10.0.0.2 を www.def.dom に割り当てているとします。 また、def.dom は顧客自身の DNS の制御下にあるとします。この設定で、abc.dom に向けられたトラフィック全てを奪うことができる位置に def.dom を設置できています。後は単に www.def.dom が 10.0.0.1 を参照するように 設定するだけです。DNS は顧客側の DNS でコントロールされているので、 www.def.dom レコードが好きな場所を指すように 設定できてしまうのを止めさせることができません。

10.0.0.1 に対するリクエスト (http://www.abc.dom/whatever 形式の URL を入力したユーザからのもの全てを含みます) は、def.dom バーチャルホストで応答されます。 このようなことが何故起こるかもっと良く知るためには、 応答の必要なバーチャルホストへのリクエストに対して、 Apache がどのように整合性を確保するかについて、 深い議論が必要になります。おおざっぱな説明はこちら [1]に記述されています。

「主サーバ」アドレス

Apache 1.1 での 名前ベースのバーチャルホストのサポート [2] 追加の際に、 Apache は httpd の実行されているホストの IP アドレスを知る必要が出てきました。このアドレスを得るために、 (もしあれば) グローバルな ServerName を使用するか、 C 言語の関数 gethostname (コマンドプロンプトで hostname とタイプしたときと同じものを返します) を呼び出すかをします。 その後、得られたアドレスで DNS 検索を行ないます。 現在のところ、この DNS 検索を回避する方法はありません。

DNS サーバがダウンして、この検索ができない事態が起こることを 恐れているのであれば、/etc/hosts にホスト名を記述しておくことができます (マシンが正常に起動するように既に設定されているかもしれません)。 その場合、DNS 参照が失敗した場合にマシンが /etc/hosts を使用するように設定していることを確認してください。 その方法は、どの OS

を使用しているかに依存しますが、 /etc/resolv.conf か /etc/nsswitch.conf を編集することで設定できます。

もし他の理由で DNS を利用する必要がない場合は、 HOSTRESORDER 環境変数を「 local 」に設定することでそのようにできます。以上これらの事柄は、どんな OS 、レゾルバライブラリを使用しているかに依存します。また、 mod_env を使用して環境変数を制御しない限り、CGI にも影響を与えます。man ページや使用している OS の FAQ で調べると良いでしょう。

以上の問題を解決する方法

- VirtualHost で IP アドレスを使用する。
- Listen で IP アドレスを使用する。
- 全てのバーチャルホストが明示的に ServerName を持つようにする。
- 何も応答しない <VirtualHost _default_:*> サーバを作る。

付録: 将来的な方向性

DNS に関して、現状は全く宜しくありません。Apache 1.2 で、 DNS のイベントが失敗しても少なくとも起動プロセスが続くようにしましたが、 これが最高の解決方法ではないでしょう。アドレスの再割り当てが必要不可避 となっている今日のインターネットにおいては、 設定ファイルの中で明示的な IP アドレスを要求する仕様は、 全く宜しくありません。

盗用のサービスアタックに関して行なうべき事は、 DNS 順引きを行なって得られたアドレスに対する DNS 逆引きを行なって、二つの名前を比較することです。 この二つが一致しなければバーチャルホストは無効になるようにします。 こうするためには逆引き DNS が適切に設定されている必要があります (FTP サーバや TCP ラッパーのおかげで「二重逆引き」DNS は一般的に なっていますので、管理者にはお馴染みものでしょう)。

IP アドレスが使用されていなくて DNS が失敗した場合は、 どうしてもバーチャルホストウェブサーバを信頼性を確保して 起動させることは不可能のようです。 設定の一部を無効にするというような部分的な解決では、 サーバが何をするようにするかにもよりますが、そのサーバが起動しないより確実に悪い状況になるでしょう。

HTTP/1.1 が開発され、ブラウザやプロキシが Host ヘッダを発行するようになったので、IP ベースのバーチャルホストを 全く使用しなくても済むようになるかもしれません。 この場合、ウェブサーバは設定中に DNS 参照をしなくても済みます。 しかし 1997 年 3 月時点の状況では、 商用レベルのウェブサーバで使用できるほどには、 これらの機能は広く開発が進んでいません。

URI References

[1] http://httpd.apache.org/docs-2.1/vhosts/details.html
[2] http://httpd.apache.org/docs-2.1/vhost/name-based.html