

Apache モジュール mod_authz_host

説明:	ホスト (名前もしくは IP アドレス) に基づいたグループ承認
ステータス:	Base
モジュール識別子:	authz_host_module
ソースファイル:	mod_authz_host.c
互換性:	Apache 2.1 以降

概要

`mod_authz_host` により提供されるディレクティブは サーバの特定の部分への アクセスを制御するために `<Directory>`, `<Files>`, `<Location>` と `.htaccess`¹ ファイルで使用されます。クライアントのホスト名、IP アドレスや 環境変数²として取得された、その他のリクエストの特徴に基づいて アクセス制御を行なうことができます。 `Allow` と `Deny` ディレクティブは どのようなクライアントにアクセスを 許可する、しないかを指定するために使用されます。一方、 `Order` ディレクティブは デフォルトのアクセス状態と、 `Allow` ディレクティブと `Deny` ディレクティブとのお互いへの影響の仕方を設定します。

ホストによるアクセス制限とパスワードによる認証を同時に 行なうことが可能です。その場合、その二つの制限の関係を指定するために `Satisfy` ディレクティブを使用します。

一般的には、アクセス制限ディレクティブはすべてのアクセスメソッド (GET, PUT, POST など) に適用されます。そして、ほとんどの場合これが望ましい動作です。しかし、`<Limit>` セクションの中にディレクティブを書くことで、一部のメソッドにのみ制限をかけることもできます。

トピック

URI References..... 4

ディレクティブ

`Allow`..... 1
`Deny`..... 3
`Order`..... 3

参照

- `Satisfy`
- `Require`

Allow ディレクティブ

説明:	サーバのある領域にアクセスできるホストを制御する
構文:	<code>Allow from all host env=env-variable [host env=env-variable] ...</code>
コンテキスト:	ディレクトリ, <code>.htaccess</code>
上書き:	<code>Limit</code>
ステータス:	Base
モジュール:	<code>mod_authz_host</code>

Allow ディレクティブはどのホストが サーバのある領域をアクセスできるかに影響を与えます。アクセスはホスト名、IP アドレス、IP アドレスの範囲や、環境変数として取得された、その他のクライアントのリクエストの 特徴によって制御することができます。

このディレクティブの最初の引数は常に `from` です。それに続く引数は三つの違った形式があります。Allow from all が指定されていれば、すべてのホストにアクセスを許可し、アクセス制限は下で説明されているように、**Deny** ディレクティブと **Order** ディレクティブの設定で決まります。特定のホストやホスト群にのみサーバへのアクセスを許可するためには、以下のどれかの形式で `host` を指定することができます:

ドメイン名 (の一部)

例: Allow from apache.org

この文字列に合うか、これで終わる名前のホストのアクセスが許可されます。各部分が完全に合うものだけに適用されますので、上の例は `foo.apache.org` にはマッチしませんが、`fooapache.org` にはマッチしません。この設定をすると、サーバは **HostnameLookups** の設定に関わらず、クライアントの IP アドレスに対して DNS の逆引きを行ないません。

完全な IP アドレス

例: Allow from 10.1.2.3

アクセスを許可する IP アドレスです。

IP アドレスの一部

例: Allow from 10.1

サブネットの制限用の、IP アドレスの最初の一つから三つまでのバイトです。

ネットワーク/ネットマスク の対

例: Allow from 10.1.0.0/255.255.0.0

ネットワーク `a.b.c.d` とネットマスク `w.x.y.z` です。より細粒度のサブネット制限用です。

ネットワーク/nnn CIDR 指定

例: Allow from 10.1.0.0/16

ネットマスクが `nnn` の上位ビットが 1 となっているものからなること以外は前のものと同じです。

注: 最後の三つの例はまったく同じホストに合います。

IPv6 アドレスと IPv6 のサブネットは以下のように指定できます:

```
Allow from fe80::a00:20ff:fea7:ccea
Allow from fe80::a00:20ff:fea7:ccea/10
```

Allow ディレクティブの引数の三つ目の形式は、環境変数² の存在によりアクセスの制御を行なえるようにするものです。Allow from env=variablename が指定されていると、環境変数 `variablename` が存在した場合にリクエストはアクセスを許可されます。サーバは **mod_setenvif** のディレクティブにより、クライアントのリクエストの特徴に基づいて柔軟に環境変数を設定する機能を提供します。ですから、このディレクティブはクライアントの User-Agent (ブラウザの種類)、Referer や他の HTTP リクエストのヘッダフィールドなどに基づいて アクセス許可をするために使うことができます。

例:

Apache モジュール mod_authz_host

```
SetEnvIf User-Agent ^KnockKnock/2.0 let_me_in
<Directory /docroot>
  Order Deny,Allow
  Deny from all
  Allow from env=let_me_in
</Directory>
```

この場合、user-agent の文字列が KnockKnock/2.0 で始まるブラウザのみがアクセスを許可され、他のものはアクセスを拒否されます。

Deny ディレクティブ

説明:	サーバがアクセスを拒否するホストを制御する
構文:	Deny from all host env=env-variable [host env=env-variable] ...
コンテキスト:	ディレクトリ, .htaccess
上書き:	Limit
ステータス:	Base
モジュール:	mod_authz_host

このディレクティブはホスト名、IP アドレス、環境変数に基づいてサーバへのアクセスを制限します。Deny ディレクティブの引数は Allow ディレクティブとまったく同じです。

Order ディレクティブ

説明:	デフォルトのアクセス可能な状態と、Allow と Deny が評価される順番を制御する
構文:	Order ordering
デフォルト:	Order Deny,Allow
コンテキスト:	ディレクトリ, .htaccess
上書き:	Limit
ステータス:	Base
モジュール:	mod_authz_host

Order ディレクティブはデフォルトのアクセスの状態と Allow ディレクティブと Deny ディレクティブが評価される順番を制御します。Ordering は以下のどれかです。

Deny, Allow

Deny ディレクティブが Allow ディレクティブの前に評価されます。アクセスはデフォルトで許可されます。Deny ディレクティブに合わないか、Allow ディレクティブに合うクライアントはアクセスを許可されます。

Allow, Deny

Allow ディレクティブが Deny ディレクティブの前に評価されます。アクセスはデフォルトで拒否されます。Allow ディレクティブに合わないか、Deny ディレクティブに合うクライアントはアクセスを拒否されます。

Mutual-failure

Apache モジュール mod_authz_host

`Allow` のリストに現れて、`Deny` のリストに現れないホストのみがアクセスを許可されます。この順番付けは `Order Allow, Deny` と同じ効果を持ち、その設定の方が好ましいために非推奨となっています。

キーワードはコンマで分離することだけが可能です。間に空白があってははいけません。どの場合でも、`Allow` と `Deny` 文は 全て評価されるということに注意してください。

以下の例では、`apache.org` ドメインのすべてのホストはアクセスを許可されます。他のすべてのホストはアクセスを拒否されます。

```
Order Deny, Allow
Deny from all
Allow from apache.org
```

次の例では、`foo.apache.org` サブドメインにあるホスト以外の、`apache.org` ドメインのすべてのホストがアクセスを許可されます。`apache.org` ドメインでないホストは、デフォルトの状態がアクセス拒否のため、サーバへのアクセスを拒否されます。

```
Order Allow, Deny
Allow from apache.org
Deny from foo.apache.org
```

一方、上の例の `Order` が `Deny, Allow` に変わっていれば、すべてのホストにアクセスが許可されます。これは、設定ファイル中の実際の順番に関わらず、`Allow from apache.org` が最後に評価されて、`Deny from foo.apache.org` を上書きするからです。`apache.org` ドメインでないホストも、デフォルトの状態が `allow` に変化するために、アクセスを許可されます。

`Order` ディレクティブはデフォルトのアクセスの状態に影響を与えるので、`Allow` ディレクティブと `Deny` ディレクティブが無くても、サーバのアクセスに影響を与えることができます。たとえば、

```
<Directory /www>
  Order Allow, Deny
</Directory>
```

はデフォルトのアクセス状態が `deny` になるため、`/www` ディレクトリへのすべてのアクセスを拒否します。

`Order` ディレクティブはサーバの設定処理の各段階でだけ アクセスディレクティブの処理の順番を変更します。これは、たとえば、`Order` ディレクティブの設定に関わらず、`<Location>` セクションの `Allow` ディレクティブや `Deny` ディレクティブは、`Directory` セクションや `.htaccess` ファイルの `Allow` ディレクティブや `Deny` ディレクティブよりも常に後に評価されるということの意味します。設定セクションのマージの詳細については、`Directory, Location, Files` セクションの動作方法³を参照してください。

URI References

[1] <http://httpd.apache.org/docs-2.1/mod/core.html#accessfilename>

[2] <http://httpd.apache.org/docs-2.1/env.html>

[3] <http://httpd.apache.org/docs-2.1/sections.html>