

サーバ設定: SSH のアタックが膨大にあるのですが、何らかの防止は無いでしょうか？

E-server では、デフォルトにて RSA 認証のみログインが可能な状態となっており、万が一パスワードが合致しましても、サーバに設置された公開鍵と合致する秘密鍵がございませんと、ログインすることは出来ません。

初期状態より変更されていない場合には、パスワードアタックがございまして、ログインは不可能なため特に対応なども不要となりますが、SSH 接続を拒否するというような設定も可能となりますが、必須ではございませんが、TCP Wrapper にて許可も可能でございます。

SSH のアクセス制限

アクセス制限を行う方法は、TCP wrapper 機能を使用しまして

/etc/hosts.allow (許可を記述するファイル)
/etc/hosts.deny (拒否を記述するファイル)

ファイルへの記述で行います。

例えば、/etc/hosts.allow に

```
sshd:210.143.96.72
```

と 1行記述を追加し、/etc/hosts.deny に

```
sshd:ALL
```

と 1行記述を追加しますと、210.143.96.72 からのみ ssh アクセスが可能となります。

また、/etc/hosts.allow に

```
sshd:ALL
```

と 1行記述を追加しまして、/etc/hosts.deny に

```
sshd:210.143.96.72
```

と 1行記述を追加しますと、210.143.96.72 以外からの ssh アクセスを許可いたします。

一意的回答 ID: #1237

サーバ設定: SSH のアタックが膨大にあるのですが、何らかの防止は無いでしょうか？

作成者: IXENT テクニカルサポート
最終更新: 2009-05-25 15:24