

IP アドレスによるデータベースへのアクセス拒否設定

ORA-12547 TNS : 接続を失いました

Oracle データベースのサーバーの SQL*Net の設定により、特定の IP アドレスからのクライアントしか接続できないような許可設定を行います

設定ファイル名

\$ORACLE_HOME/network/admin/sqlnet.ora

※ 過去の Oracle ではこの設定は、protocol. ora ファイルで行っていたが、Oracle10g より sqlnet.ora に変更された

設定内容 (sqlnet.ora)

IP によるアクセス制限を有効にする

tcp.validnode_checking = yes

以下の IP からの接続を許可

tcp.invited_nodes = (192.168.1.1, 192.168.1.2)

以下の IP からの接続を拒否

tcp.excluded_nodes = (192.168.1.10, 192.168.1.12)

※ 許可／拒否リストは、どちらか一方のみしか指定できない

複数 IP 指定の場合は、カンマ区切りで記述します

『*』のワイルドカードも使用できます 例) 192.168.100.*

【注意事項】

サーバー側の sqlnet.ora ファイルの設定変更を行った場合、Oracle リスナーの再起動が必要となる

lsnrctl stop

lsnrctl start

lsnrctl status

このコマンドは、コマンドプロンプト画面を『管理者権限で実行する』必要がある

また、リスナー・サービスが起動してから、しばらくの間はリスナーが機能しないので待つ（2分くらい）

この間に接続を行った場合は、

```
SQL> conn system/OraTest@oraconn
```

ERROR:

ORA-12514: TNS: リスナーは接続記述子でリクエストされたサービスを現在認識していません

と表示される

IP アドレス許可設定で拒否されたときの、クライアント側メッセージ

ERROR:

ORA-12537: TNS: 接続がクローズされました。

~~ORA-12547: TNS: 接続を失いました~~

このメッセージは、サーバー側でのクライアント接続 IP アドレス制限を行っているために、拒否された時に表示されるメッセージです

対応方法は、拒否 IP アドレスから外すことです

拒否された時の Lister.log ファイルへの出力内容

Incoming connection from 192.168.1.19 rejected

10-8月-2014 03:19:01 * 12546

TNS-12546 : TNS : 許可が拒否されました。

TNS-12560 : TNS : プロトコル・アダプタ・エラー

TNS-00516 : 許可されません。

【Linux における OS での通信拒否設定】

Linux サーバーに対して、IP アドレス許可および、拒否ファイルを使用して、通信クライアントの IP アドレス制限を行う

許可ファイルの設定が優先される

- ・ 拒否ファイル /etc/hosts.deny
- ・ 許可ファイル /etc/hosts.allow

通常の使用例)

まず、全てのアクセスを拒否させる

```
# vi /etc/hosts.deny
ALL: ALL
```

つぎに、許可する IP アドレスとポートを指定する

```
# vi /etc/hosts.deny
ALL: 192.168.0.100
vsftpd: 192.168.0.
sshd: 192.168.0.
```

この例では、192.168.0.100 がすべてのポートでの接続を許可
192.168.0.***で、ftp と ssh が許可されています