

# 日々是Oracle APEX

Oracle APEXを使った作業をしていて、気の付いたところを忘れないようにメモをとります。

2022年11月22日 火曜日

## Oracle APEXの環境作成(10) - 自己署名証明書によるHTTPS化

自己署名証明書を生成し、ORDSへの接続をHTTPSに変更します。

### ORDSのインストール時に構成する

Oracle REST Data Servicesのインストール時にHTTPSを選択することにより、自己署名証明書を生成した上でHTTPSによる接続を受け付けるようになります。

ORDS 24.1.1での作業例です。データベースの接続先や接続ユーザーの設定はHTTPのときと同じです。

**Protocol:** HTTPが設定されている番号（以下の作業例では7）を入力し、設定をHTTPからHTTPSへ切り替えます（2を入力します）。

**Enter the HTTPS port**と質問されるので、デフォルトの8443を選択します。

**Enter a number to select the certificate type**と質問されるので、デフォルトの1 - Use self-signed certificate (generates automatically)を選択します。

**Enter the SSL hostname**と聞かれるので、**ブラウザで接続先として指定するホスト名**を入力します。今回の例ではlocalhostを指定しています。**ブラウザに入力するホスト名と、ここで指定したホスト名が異なると、ORDSにHTTPSで接続できません**（TCPレベルでは接続するがTLSでの接続が確立しません）。

以上の設定で、ORDS（およびAPEX）にHTTPSで接続できるようになります。

```
[oracle@localhost config]$ cd /etc/ords/config
[oracle@localhost config]$ ords install
2024-06-20T03:29:10Z INFO      ORDS has not detected the option '--config' and
this will be set up to the default directory.

ORDS: Release 24.1 Production on Thu Jun 20 03:29:12 2024

Copyright (c) 2010, 2024, Oracle.

Configuration:
  /etc/ords/config

The configuration folder /etc/ords/config does not contain any configuration files.

Oracle REST Data Services - Interactive Install

Enter a number to select the database connection type to use
```

- [1] Basic (host name, port, service name)
- [2] TNS (TNS alias, TNS directory)
- [3] Custom database URL

Choose [1]:

Enter the database host name [localhost]:

Enter the database listen port [1521]:

Enter the database service name [orcl]: freepdb1

Provide database user name with administrator privileges.

Enter the administrator username: sys

Enter the database password for SYS AS SYSDBA: \*\*\*\*\*

Retrieving information.

ORDS is not installed in the database. ORDS installation is required.

Enter a number to update the value or select option A to Accept and Continue

- [1] Connection Type: Basic
- [2] Basic Connection: HOST=localhost PORT=1521 SERVICE\_NAME=freepdb1  
Administrator User: SYS AS SYSDBA
- [3] Database password for ORDS runtime user (ORDS\_PUBLIC\_USER): <generate>
- [4] ORDS runtime user and schema tablespaces: Default: SYSAUX Temporary TEMP
- [5] Additional Feature: Database Actions
- [6] Configure and start ORDS in Standalone Mode: Yes
- [7] Protocol: HTTP
- [8] HTTP Port: 8080
- [9] APEX static resources location:
- [A] Accept and Continue - Create configuration and Install ORDS in the database
- [Q] Quit - Do not proceed. No changes

Choose [A]: 7

Enter a number to select the protocol

- [1] HTTP
- [2] HTTPS

Choose [1]: 2

Enter the HTTPS port [8443]:

Enter a number to select the certificate type

- [1] Use self-signed certificate (generates automatically)
- [2] Use my SSL certificate (requires SSL certificate and SSL certificate

private key)

Choose [1]:

Enter the SSL hostname: localhost

Enter a number to update the value or select option A to Accept and Continue

- [1] Connection Type: Basic
- [2] Basic Connection: HOST=localhost PORT=1521 SERVICE\_NAME=freepdb1  
Administrator User: SYS AS SYSDBA
- [3] Database password for ORDS runtime user (ORDS\_PUBLIC\_USER): <generate>
- [4] ORDS runtime user and schema tablespaces: Default: SYSAUX Temporary TEMP
- [5] Additional Feature: Database Actions
- [6] Configure and start ORDS in Standalone Mode: Yes
- [7] Protocol: HTTPS
- [8] HTTPS Port: 8443
- [9] Certificate Type: Use Self-Signed Certificate
- [10] SSL Hostname: localhost
- [11] APEX static resources location:
- [A] Accept and Continue - Create configuration and Install ORDS in the database
- [Q] Quit - Do not proceed. No changes

Choose [A]: 11

Enter the APEX static resources location: /home/oracle/i

Enter a number to update the value or select option A to Accept and Continue

- [1] Connection Type: Basic
- [2] Basic Connection: HOST=localhost PORT=1521 SERVICE\_NAME=freepdb1  
Administrator User: SYS AS SYSDBA
- [3] Database password for ORDS runtime user (ORDS\_PUBLIC\_USER): <generate>
- [4] ORDS runtime user and schema tablespaces: Default: SYSAUX Temporary TEMP
- [5] Additional Feature: Database Actions
- [6] Configure and start ORDS in Standalone Mode: Yes
- [7] Protocol: HTTPS

```

[8]      HTTPS Port: 8443
[9]      Certificate Type: Use Self-Signed Certificate
[10]     SSL Hostname: localhost
[11]     APEX static resources location: /home/oracle/i
[A] Accept and Continue - Create configuration and Install ORDS in the database
[Q] Quit - Do not proceed. No changes
Choose [A]:
The setting named: db.connectionType was set to: basic in configuration: default
The setting named: db.hostname was set to: localhost in configuration: default
The setting named: db.port was set to: 1521 in configuration: default
The setting named: db.servicename was set to: freepdb1 in configuration: default
The setting named: plsql.gateway.mode was set to: proxied in configuration: default
The setting named: db.username was set to: ORDS_PUBLIC_USER in configuration:
default
The setting named: db.password was set to: ***** in configuration: default
The setting named: feature.sdw was set to: true in configuration: default
The global setting named: database.api.enabled was set to: true
The setting named: restEnabledSql.active was set to: true in configuration: default
The global setting named: standalone.https.port was set to: 8443
The global setting named: standalone.https.host was set to: localhost
The global setting named: standalone.static.path was set to: /home/oracle/i
The global setting named: standalone.static.context.path was set to: /i
The global setting named: standalone.doc.root was set to:
/etc/ords/config/global/doc_root
The setting named: security.requestValidationFunction was set to:
ords_util.authorize_plsql_gateway in configuration: default
2024-06-20T03:29:50.113Z INFO      Created folder /etc/ords/config/logs
2024-06-20T03:29:50.115Z INFO      The log file is defaulted to the current
working directory located at /etc/ords/config/logs
2024-06-20T03:29:50.215Z INFO      Installing Oracle REST Data Services version
24.1.1.r1201228 in FREEPDB1
2024-06-20T03:29:51.389Z INFO      ... Verified database prerequisites
2024-06-20T03:29:51.880Z INFO      ... Created Oracle REST Data Services proxy
user
2024-06-20T03:29:52.406Z INFO      ... Created Oracle REST Data Services schema
2024-06-20T03:29:53.079Z INFO      ... Granted privileges to Oracle REST Data
Services
2024-06-20T03:29:56.586Z INFO      ... Created Oracle REST Data Services database
objects
2024-06-20T03:30:09.166Z INFO      Completed installation for Oracle REST Data
Services version 24.1.1.r1201228. Elapsed time: 00:00:18.888

2024-06-20T03:30:09.237Z INFO      Completed configuring PL/SQL gateway user for
Oracle REST Data Services version 24.1.1.r1201228. Elapsed time: 00:00:00.70

2024-06-20T03:30:09.240Z INFO      Log file written to
/etc/ords/config/logs/ords_install_2024-06-20_032950_11604.log
2024-06-20T03:30:10.020Z INFO      HTTP and HTTP/2 cleartext listening on host:
0.0.0.0 port: 8080
2024-06-20T03:30:10.022Z INFO      HTTPS and HTTPS/2 listening on host: 0.0.0.0
port: 8443
2024-06-20T03:30:10.058Z INFO      Disabling document root because the specified
folder does not exist: /etc/ords/config/global/doc_root
2024-06-20T03:30:10.059Z INFO      Default forwarding from / to contextRoot
configured.
2024-06-20T03:30:13.441Z INFO      Configuration properties for: |default|lo|
db.servicename=freepdb1
db.hostname=localhost
db.password=*****
standalone.https.host=localhost
conf.use.wallet=true
security.requestValidationFunction=ords_util.authorize_plsql_gateway
standalone.static.context.path=/i
database.api.enabled=true
db.username=ORDS_PUBLIC_USER

```

```
standalone.static.path=/home/oracle/i
restEnabledSql.active=true
resource.templates.enabled=false
plsql.gateway.mode=proxied
db.port=1521
feature.sdw=true
standalone.https.port=8443
config.required=true
db.connectionType=basic
standalone.doc.root=/etc/ords/config/global/doc_root
```

```
2024-06-20T03:30:13.442Z WARNING      *** jdbc.MaxLimit in configuration
|default|lo| is using a value of 10, this setting may not be sized adequately for a
production environment ***
2024-06-20T03:30:13.442Z WARNING      *** jdbc.InitialLimit in configuration
|default|lo| is using a value of 10, this setting may not be sized adequately for a
production environment ***
2024-06-20T03:30:15.823Z INFO
```

```
Mapped local pools from /etc/ords/config/databases:
/ords/                                => default                                => VALID
```

```
2024-06-20T03:30:15.936Z INFO          Oracle REST Data Services initialized
Oracle REST Data Services version : 24.1.1.r1201228
Oracle REST Data Services server info: jetty/10.0.20
Oracle REST Data Services java info: OpenJDK 64-Bit Server VM 17.0.11+9-LTS
```

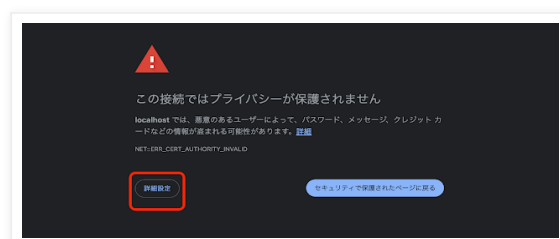
APEXを実行している仮想マシンのネットワークのポートフォワーディングの設定に、ホストポートが8443、ゲストポートが443の設定を追加します。VirtualBoxの外からの接続要求は、ポート8443で受け付け、仮想マシンのポート443へ転送し、仮想マシン（Linux）のfirewalldによりポート8443で待ち受けしているORDSへ転送されます。



ホストマシンのブラウザより、以下のURLよりAPEXにアクセスします。ブラウザはChromeで確認しています。

<https://localhost:8443/ords/>

証明書が無効とのエラーが発生します。詳細設定を開きます。



localhostにアクセスする（安全ではありません）をクリックします。



ORDSのランディング・ページが開きます。HTTPSで接続しています。



## HTTPからHTTPSに構成変更する

ORDSを停止した状態で、以下のコマンドを実行してORDSのプロパティを変更します。ORDSをインストールしたユーザーoracleで実行します。

```
ords config set standalone.https.port 8443
ords config set standalone.https.host localhost
ords config delete standalone.http.port
```

VirtualBoxの仮想マシンで作業を行うことを想定しているため、**standalone.https.host**に**localhost**を指定しています。OCIのコンピュート・インスタンスでの作業例は後述します。

コマンドは、ORDSの構成ディレクトリ**/etc/ords/config**上で実行しています。

```
[oracle@localhost config]$ cd /etc/ords/config
[oracle@localhost config]$ ords config set standalone.https.port 8443
2024-06-20T04:04:58Z INFO      ORDS has not detected the option '--config' and
this will be set up to the default directory.
```

```
ORDS: Release 24.1 Production on Thu Jun 20 04:05:00 2024
```

```
Copyright (c) 2010, 2024, Oracle.
```

```
Configuration:
/etc/ords/config
```

```
The global setting named: standalone.https.port was set to: 8443
[oracle@localhost config]$ ords config set standalone.https.host localhost
2024-06-20T04:05:03Z INFO          ORDS has not detected the option '--config' and
this will be set up to the default directory.
```

ORDS: Release 24.1 Production on Thu Jun 20 04:05:05 2024

Copyright (c) 2010, 2024, Oracle.

Configuration:  
/etc/ords/config

```
The global setting named: standalone.https.host was set to: localhost
[oracle@localhost config]$ ords config delete standalone.http.port
2024-06-20T04:05:13Z INFO          ORDS has not detected the option '--config' and
this will be set up to the default directory.
```

ORDS: Release 24.1 Production on Thu Jun 20 04:05:14 2024

Copyright (c) 2010, 2024, Oracle.

Configuration:  
/etc/ords/config

```
The global setting named: standalone.http.port was removed from the configuration
[oracle@localhost config]$
```

構成変更を行った後、ORDSを起動します。スーパーユーザー**root**で実行します。

## systemctl start ords

```
[root@localhost ~]# systemctl start ords
[root@localhost ~]#
```

ORDSが起動される際に、自己署名証明書と署名に必要な秘密キーが**/etc/ords/config/global/standalone**以下に生成されます。

```
[oracle@localhost config]$ ls /etc/ords/config/global/standalone/
self-signed.key  self-signed.pem
[oracle@localhost config]$
```

以上でHTTPからHTTPSへの切り替えが完了しました。

OCIのコンピュート・インスタンスで構成した場合の切り替えでは、**standalone.https.host**として**localhost以外**を指定します。以下では**oci-apex**としています。

```
ords config set standalone.https.port 8443
ords config set standalone.https.host oci-apex
ords config delete standalone.http.port
```

ユーザー**opc**でコンピュート・インスタンスに接続し、上記のコマンドを実行します。

```
[opc@apex-310089 ~]$ sudo -s
[root@apex-310089 opc]# su - oracle
Last login: Thu Jun 20 14:54:09 JST 2024 on pts/0
[oracle@apex-310089 ~]$ cd /etc/ords/config
[oracle@apex-310089 config]$ ords config set standalone.https.port 8443
```

```
2024-06-20T05:55:29Z INFO      ORDS has not detected the option '--config' and
this will be set up to the default directory.
```

```
ORDS: Release 24.1 Production on Thu Jun 20 05:55:31 2024
```

```
Copyright (c) 2010, 2024, Oracle.
```

```
Configuration:
/etc/ords/config
```

```
The global setting named: standalone.https.port was set to: 8443
```

```
[oracle@apex-310089 config]$ ords config set standalone.https.host oci-apex
```

```
2024-06-20T05:55:39Z INFO      ORDS has not detected the option '--config' and
this will be set up to the default directory.
```

```
ORDS: Release 24.1 Production on Thu Jun 20 05:55:41 2024
```

```
Copyright (c) 2010, 2024, Oracle.
```

```
Configuration:
/etc/ords/config
```

```
The global setting named: standalone.https.host was set to: oci-apex
```

```
[oracle@apex-310089 config]$ ords config delete standalone.http.port
```

```
2024-06-20T05:55:45Z INFO      ORDS has not detected the option '--config' and
this will be set up to the default directory.
```

```
ORDS: Release 24.1 Production on Thu Jun 20 05:55:46 2024
```

```
Copyright (c) 2010, 2024, Oracle.
```

```
Configuration:
/etc/ords/config
```

```
The global setting named: standalone.http.port was removed from the configuration
```

```
[oracle@apex-310089 config]$ exit
```

```
logout
```

```
[root@apex-310089 opc]# systemctl start ords
```

```
[root@apex-310089 opc]#
```

ブラウザを実行するPCの/etc/hostsなどに、コンピュータ・インスタンスのパブリックIPとホスト名（上記の例ではoci-apex）を追加します。

ブラウザから接続は、以下のURLから行います。HTTPSの標準ポートに接続します。

<https://oci-apex/ords/>

自己署名証明書なので接続を許可する必要があります。許可すると、今までの作業と同様にORDSのランディング・ページが表示されます。

## OpenSSLを使って自己署名証明書を作成する

ORDSが生成する自己署名証明書でHTTPSを構成できなかった頃の手順です。参考として残していますが、現在はこの手順に沿って作業を行うことはありません。

手元のPCにホスト名からIPアドレスが解決できるように、/etc/hostsファイル（または同等のファイル）にエントリを追加しておきます。IPアドレスはコンピュータ・インスタンスのパブリックIP



を設定します。（VirtualBoxの仮想マシンでの作業であれば、127.0.0.1をIPアドレスとします）。ホスト名は**apex.mydomain.dev**とします。

```
***.***.***.*** apex.mydomain.dev
```

sshで接続し、ユーザーrootに切り替えます。

最初にORDSを停止します。

**systemctl stop ords**

```
[root@localhost ~]# systemctl stop ords
[root@localhost ~]#
```

ORDSの実行ユーザーである、oracleに切り替えて作業を進めます。作業ディレクトリである/etc/ords/configへ移動します。

**su - oracle**  
**cd /etc/ords/config**

```
[root@localhost ~]# su - oracle
Last login: Thu May 18 11:48:18 JST 2023 on pts/0
[oracle@localhost ~]$ cd /etc/ords/config
[oracle@localhost config]$
```

証明書と秘密鍵を配置するディレクトリglobal/standaloneを作成します。別の場所でも良いのですが、その場合は**settings.xml**のパラメータ**standalone.https.cert**、**standalone.https.cert.key**としてファイルを指定する必要があります。

ディレクトリ作成後、移動します。

**mkdir global/standalone**  
**cd global/standalone**

```
[oracle@localhost config]$ mkdir global/standalone
[oracle@localhost config]$ cd global/standalone
[oracle@localhost standalone]$
```

OpenSSLを使って、自己署名証明書を生成します。

RSA公開鍵暗号のキーペアを鍵長2048ビットで生成します。ファイルは**private.pem**になります。

**openssl genrsa -out private.pem 2048**

CSR（Certificate Signing Request - 証明書署名要求）として**test.csr**を生成します。

国名などの入力を求められますが、共通名（Common Name）としてサーバー名が設定されていれば十分です。共通名以外はピリオドを入力することで、空白を設定しています。（何も入力しないと、デフォルトのXXなどが設定されます。）

**openssl req -new -key private.pem -out test.csr**

SAN（Subject Alternative Name）の設定に使用するファイル**san.txt**を作成します。



```
echo "subjectAltName = DNS:apex.mydomain.dev" > san.txt
```

自己署名証明書self-signed.pemを作成します。

```
openssl x509 -req -days 3650 -signkey private.pem -in test.csr -out self-signed.pem -extfile san.txt
```

秘密鍵のファイルself-signed.keyを作成します。

```
openssl pkcs8 -topk8 -nocrypt -in private.pem -outform PEM -out self-signed.key
```

ORDSはself-signed.pemおよびself-signed.keyを使用します。これらのファイル名はstandalone.https.cert、standalone.https.cert.keyのデフォルト値であるため、settings.xmlへの設定を省略できます。

```
[oracle@localhost standalone]$ openssl genrsa -out private.pem 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
.....+++++
.....+++++
e is 65537 (0x010001)
[oracle@localhost standalone]$ openssl req -new -key private.pem -out test.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:.
State or Province Name (full name) []:.
Locality Name (eg, city) [Default City]:.
Organization Name (eg, company) [Default Company Ltd]:.
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:apex.mydomain.dev
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
[oracle@localhost standalone]$ echo "subjectAltName = DNS:apex.mydomain.dev" >
san.txt
[oracle@localhost standalone]$ openssl x509 -req -days 3650 -signkey private.pem -
in test.csr -out self-signed.pem -extfile san.txt
Signature ok
subject=C = JP, L = Tokyo, O = Oracle, CN = apex.jp.oracle.com
Getting Private key
[oracle@localhost standalone]$ openssl pkcs8 -topk8 -nocrypt -in private.pem -
outform PEM -out self-signed.key
[oracle@localhost standalone]$
```

設定ファイル/etc/ords/config/settings.xmlを開きます。

```
[oracle@localhost ~]$ vi /etc/ords/config/global/settings.xml
[oracle@localhost ~]$
```

HTTPSを有効にする設定であるstandalone.https.portを追加します。standalone.http.portは削除します。HTTPSの待ち受けをするポート番号は8443とします。firewalldによりポート443への接続

は8443へ転送されるように構成されているため、接続に使用するURLにポート番号を含む必要はありません。

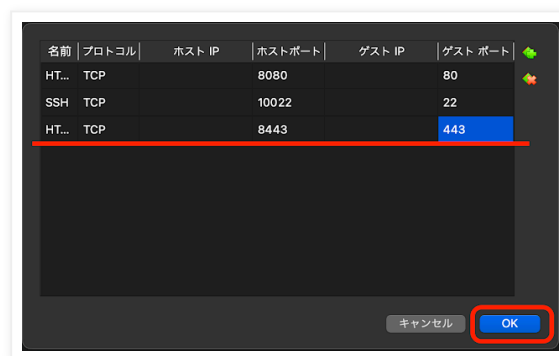
```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<comment>Saved on Thu May 18 02:07:03 UTC 2023</comment>
<entry key="database.api.enabled">true</entry>
<entry key="standalone.context.path">/ords</entry>
<entry key="standalone.doc.root">/etc/ords/config/global/doc_root</entry>
<entry key="standalone.https.port">8443</entry>
<entry key="standalone.static.context.path">/i</entry>
<entry key="standalone.static.path">/home/oracle/i/</entry>
</properties>
```

ユーザーrootに戻ってORDSを起動します。

```
[root@localhost ~]# systemctl start ords
[root@localhost ~]#
```

サーバー側の設定は以上で完了です。

VirtualBoxでの作業の場合、仮想マシンのネットワーク設定にポート・フォワーディングを追加します。



ブラウザより、Oracle APEXの環境に接続すると証明書が不正と報告されます。

[https://apex.mydomain.dev/ords/apex\\_admin](https://apex.mydomain.dev/ords/apex_admin)

または（VirtualBoxの場合）

[https://apex.mydomain.dev:8443/ords/apex\\_admin](https://apex.mydomain.dev:8443/ords/apex_admin)

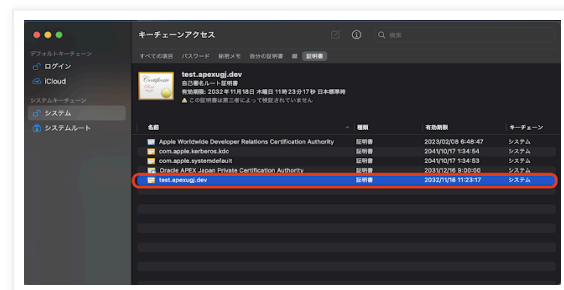
NET::ERR\_CERT\_AUTHORITY\_INVALIDをクリックするとPEM encoded chainとして自己署名証明書が表示されます。エラーを回避するには、この証明書を信頼させる必要があります。



## 信頼できる証明書の追加（macOSの例）

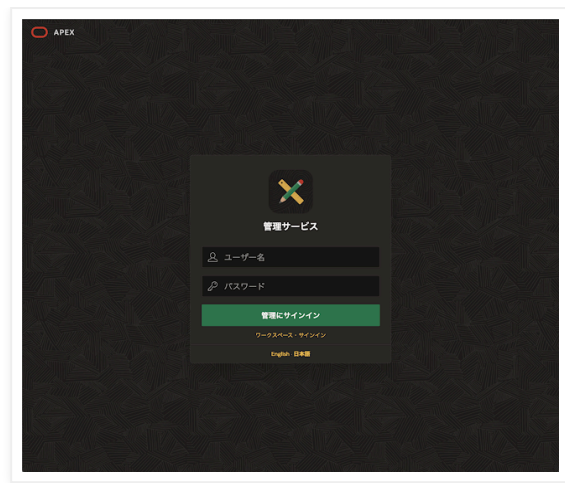
macOSの場合は、**キーチェーンアクセス**に証明書を登録します。

**PEM encoded chain**として表示されている証明書をファイルにコピー＆ペーストし、キーチェーンアクセスにドロップします。



登録した証明書の情報を表示させ（ダブルクリックまたはコンテキスト・メニューの情報を見る）、**信頼**のSSL(Secure Socket Layer)を常に**信頼**に変更します。

以上の変更で、Oracle APEXにHTTPSで接続できるようになります。



続く

Yuji N. 時刻: 15:24

共有

◀

ホーム

▶

[ウェブ バージョンを表示](#)

自己紹介

**Yuji N.**

日本オラクル株式会社に勤務していて、Oracle APEXのGroundbreaker Advocateを拝命しました。  
こちらの記事につきましては、免責事項の参照をお願いいたします。

[詳細プロフィールを表示](#)

Powered by Blogger.