2019年10月11日

真正なeduroamアクセスポイントを確認する方法について(注意喚起)

愛知教育大学 ICT教育基盤センター

eduroam JP事務局から，偽物のeduroam アクセスポイントに接続してIDとパスワードが盗まれることないよう，エンドユーザに真正なeduroamアクセスポイントであることを確認する方法を周知するよう依頼がありましたので，お伝えします．

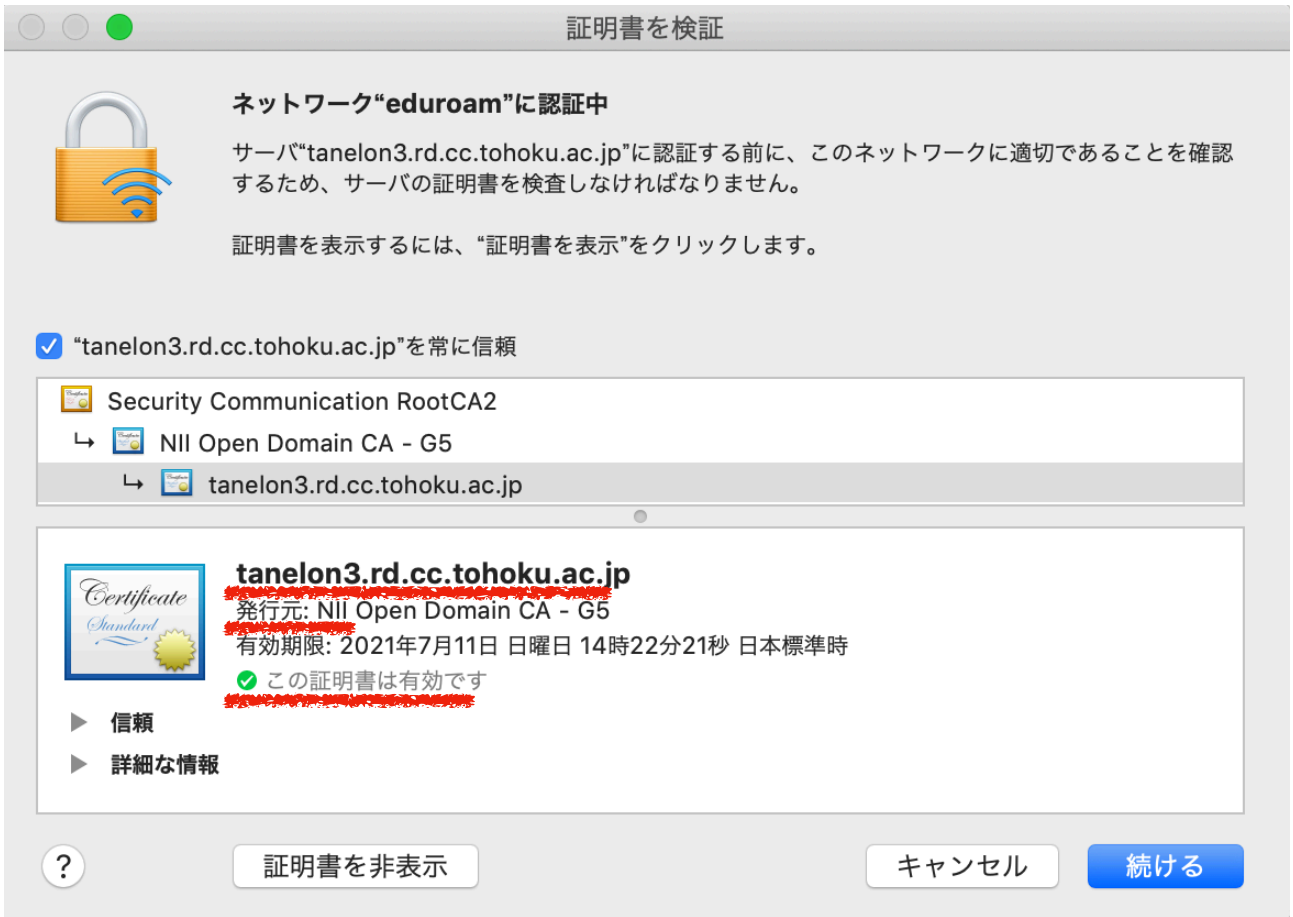
真正なeduroamアクセスポイントでは，認証時に，次ページ以降の方法で確認できる電子証明書が使われます．この確認は，各ノートパソコンやタブレットごとに初めて(1回目)eduroamを使うときに行うことができます．macOS，Windows10，タブレット(iOS，iPadOS，Android)の順に説明します．

真正なeduroamアクセスポイントの情報は，初めて(1回目)eduroamを利用する際，各ノートパソコンやタブレット毎に記憶されます．したがって，初めてeduroamを利用する時は，真正なeduroamアクセスポイントを使うことが極めて重要です．ですから，出張など学外で初めてeduroamを使うのではなく，本学内の真正なeduroamアクセスポイントへの接続が，各ノートパソコンなどにおいて初めてのeduroam利用となることを強く推奨します．学外に偽物のeduroamアクセスポイントがある可能性を否定できないからです．

これからの説明において，tanelon3.rd.cc.tohoku.ac.jpという東北大学のサーバコンピュータがでてきますが，本学ICT教育基盤センターが発行しているeduroamのIDとパスワードの認証は，東北大学が開発しているeduroam代理認証システムを利用しているからです．都合上，macOSの場合から説明が始まりますが，Windowsやタブレットの場合の理解に必要なことが書いてありますので，Windowsやタブレットの利用者もmacOSの場合の説明も含めて読んでくださるよう，お願いします．

macOSの場合(初めて，1回目)

　証明書を表示 ボタンが表示されたらクリックして，tanelon3.rd.cc.tohoku.ac.jpの表示において，この証明書は有効です，と表示されていたら，真正なアクセスポイントです．この証明書は有効です，と表示されていても，tanelon3.rd.cc.tohoku.ac.jpでなければ偽物です．

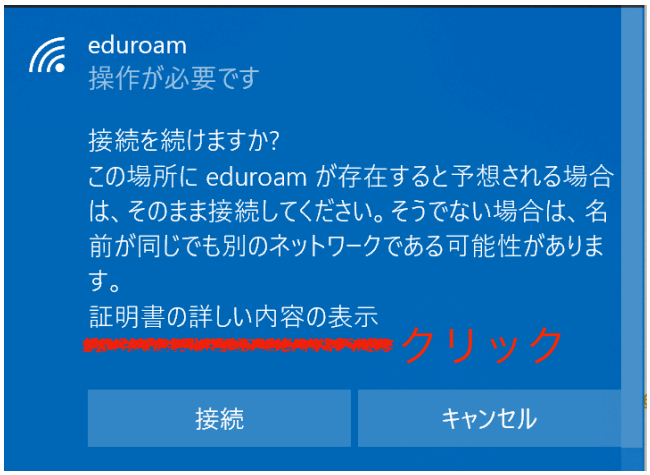


上記のようであれば，続けるをクリックしてOK(先に進んで構わない)．さもなければ，キャンセル．``詳細な情報''をクリックして以下の指紋まで一致すれば，なお安心(ただし2021年7月頃までの話)．

指紋	
SHA-256	E5 2A 21 59 8F E2 28 A6 29 7B BE 53 4B A6 EA 42 FF 8E 77 04 B5 C0 23 92 1E 81 15 FA 34 7B 22 44
SHA-1	36 D3 22 DB ED C6 4E 3F F1 77 6B 78 97 1F A5 D9 59 05 3D 37

Windows 10の場合(初めて，1回目)

左のような表示がでたときに，``証明書の詳しい内容の表示''をクリックして，右のようなサーバの拇印(16進数の数値が同じ)が表示されれば，真正なアクセスポイントです．サーバの拇印とは，電子証明書のデータを特別な計算によって要約したものです．



下記のどちらかなら，真正なアクセスポイントなので，接続をクリックしてOK(先に進んで構わない)．さもなければ，キャンセル．

サーバーの拇印: E5 2A 21 59 8F E2 28 A6 29 7B BE 53 4B A6 EA 42 FF 8E 77 04 B5 C0 23 92 1E 81 15 FA 34 7B 22 44

サーバーの拇印: 36 D3 22 DB ED C6 4E 3F F1 77 6B 78 97 1F A5 D9 59 05 3D 37

サーバの拇印は，2021年の6月から7月にかけて，変わると推測されます．現行のtanelon3.rd.cc.tohoku.ac.jpの電子証明書の有効期限が切れ，更新されるから．
WindowsではmacOSのように証明書の詳細を見ることはできません．拇印のみ見ることができます．

タブレットの場合(初めて，1回目)

iOS(iPadOS)の場合も，macOSと同様に，証明書を確認する画面が出ます．macOSと同様に対処してください．Androidの場合は，証明書を確認する画面が出ないことが多いようなので[1]，出ないならばそのバージョンのAndroidでeduroamを利用することは推奨されません．

[1] eduroam JP事務局からの情報による．近年のAndroid機種では，eduroamの接続設定において，CA証明書の項目で「システム証明書を使用」の選択で，証明書の確認ができる場合がある．

macOS，Windows，タブレットとともに，証明書の確認はIDとパスワードを入力してから行われますが，続ける(あるいは接続，信頼)をクリックしない限りはIDとパスワードはアクセスポイントに送信されません．証明書が正しくない(偽物のアクセスポイント)と判定して，キャンセルをクリックした場合はIDとパスワードは送信されませんので，ご安心下さい．

macOS，Windows，タブレットとともに，初めて(1回目)の接続時において，証明書の確認の表示がでる場合は，IDとパスワードの暗号化が十分安全な方式です．証明書の確認の表示がでない場合は，IDとパスワードの暗号化が不十分な方式なので，好ましくありません．

2回目以降のeduroamへの接続においては，1回目のような証明書の確認の画面は出ませんが，1回目と暗号化の方式が異なっていたり，1回目と電子証明書が異なっていたら，なんらかの警告が出ることになっています．macOS，Windows，タブレットが1回目のときの暗号化の方式と参照した電子証明書の情報を覚えているからです．なんらかの警告がでた場合は，IDとパスワードの暗号化の方式が不十分なアクセスポイントに遭遇，偽物のeduroamアクセスポイントに遭遇，あるいは電子証明書が(期限切れでなどの理由で)更新されたことを疑う必要があります．東北大学のサーバコンピュータの電子証明書が更新された場合，本学のeduroam利用者(Windows使用者)に，本学ICT教育基盤センターが何らかの方法で対処方法を含めて，お知らせすることになるでしょう．

以上のことから，各ノートパソコンなどにおいて1回目のeduroamへの接続において，暗号化方式が十分安全な真正なアクセスポイントに接続することが大切です．そのためには，各ノートパソコンなどにおいて，edruroam接続可否の確認も兼ねて，1回目は(学外ではなく)本学のeduroamアクセスポイントに接続することを強く勧めます．