新しい中間認証局から発行したサーバ証明書への置き換えが完了しているか確認したい

問題

あるサーバについて、新中間認証局（2020年12月25日以降稼働）から発行したサーバ証明書への置き換えが完了しているか確認したい。

解決方法

当該サーバにインストールされている証明書の発行元(Issuer)が「**NII Open Domain CA - G7 RSA**」または「**NII Open Domain CA - G7 ECC**」となっていることを確認してください。

Google Chrome または Microsoft Edge(Chromium Base)の例

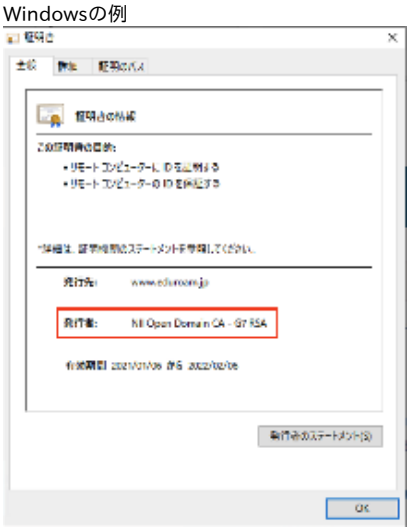
Google Chrome, Microsoft Edge(Chromium Base)

確認したいサーバにChromeでアクセスして、下記の手順で確認してください。

1. URL入力欄にある錠のマークをクリックしてください。

2. 開いたウィンドウから、「証明書」をクリックしてください。

3. 証明書の詳細が表示されるので、発行元が「**発行元: NII Open Domain CA - G7 RSA**」または「**発行元: NII Open Domain CA - G7 ECC**」となっていることを確認してください。
Windowsの例



macOSの例

Firefoxの例

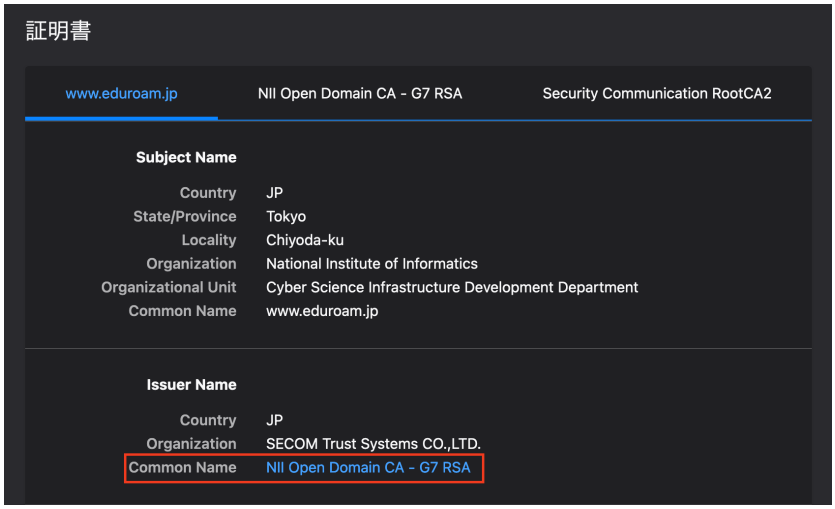
Firefox
確認したいサーバにFirefoxでアクセスして、下記の手順で確認してください。 1. URL入力欄にある錠のマークをクリックしてください。 

2. 開いたウィンドウ内「安全な接続」の右にある「>」をクリックしてください。

3. 表示されたウィンドウの「詳細を表示」をクリックしてください。

4. ページ情報のウィンドウが表示されるので、「証明書を表示...」ボタンをクリックしてください。

5. Firefoxで証明書の詳細のページが表示されるので、「Issuer Name」の「Common Name」が「**NII Open Domain CA - G7 RSA**」となっていることを確認してください。



OpenSSLの例

OpenSSL（Webサーバに対して確認したい場合）

確認したいサーバに対して、下記のコマンドを用いて確認してください。当該サーバにログインする必要はありません。

1. openssl s_client -connect hostname.ac.jp:443 -showcerts

   hostname.ac.jp の箇所は、対象のサーバのFQDNに置き換えてください。
   たとえばhttps://www.eduroam.jp について確認したい場合は、
   openssl s_client -connect www.eduroam.jp:443 -showcerts
   となります。
2. 実行結果の最初の7行程度に、下記の例の通り表示されます。

```
CONNECTED(00000005)
depth=2 C = JP, O = ”SECOM Trust Systems CO.,LTD.”, OU = Security Communication RootCA2
verify return:1
depth=1 C = JP, O = ”SECOM Trust Systems CO.,LTD.”, CN = NII Open Domain CA - G7 RSA
verify return:1
depth=0 C = JP, ST = Tokyo, L = Chiyoda-ku, O = National Institute of Informatics, OU = Cyber Science Infrastructure
Development Department, CN = www.eduroam.jp
verify return:1
--略--
```

3. UPKIの証明書の場合、depth=1となっている箇所が中間CA証明書です。
   「CN = NII Open Domain CA - G7 RSA」または「CN = NII Open Domain CA - G7 ECC」となっていることを確認してください。

OpenSSL（証明書単体で確認したい場合）

確認したい証明書に対して、下記のコマンドを用いて確認してください。

1. openssl x509 -noout -in <証明書ファイル名> -issuer

   <証明書ファイル名>の箇所は、対象の証明書ファイル名に置き換えてください。
   たとえば certs.nii.ac.jp.cer について確認したい場合は、
   openssl x509 -noout -in certs.nii.ac.jp.cer -issuer
   となります。
2. 実行結果に、下記の例の通り表示されます。

   ```
   issuer=C = JP, O = ”SECOM Trust Systems CO.,LTD.”, CN = NII Open Domain CA - G7 RSA
   ```

3. 発行者(issuer)が CN = NII Open Domain CA - G7 RSA または CN = NII Open Domain CA - G7 ECC となっていることを確認してください。

関連記事

- エラーコード212「主体者DN,指定したDNはすでに存在しています。」が表示される
- エラーコード371「主体者DN,主体者DNのOUが許可リストとして登録された値と一致しません。」が表示される
- 証明書更新発行申請時のCSRや鍵ペアの再利用について
- サーバ証明書のシリアル番号を確認したい
- 新しい中間認証局から発行したサーバ証明書への置き換えが完了しているか確認したい