.....

作成:令和2年9月14日

## インターネットスポット接続手順【android】- CA 証明書インストール編-

Android 端末の機種やバージョンによっては、大学で使用している証明書を署名した機関の CA 証明書(Security Communication RootCA2)がご利用の端末にプリインストールされていない可能性があります。

CA 証明書選択欄にて「システム証明書を使用」が選択できない場合,下記手順にて CA 証明書 をインストールしていただきインターネットスポットに接続してください。

#### 1. はじめに(CA 証明書について)

証明書は,情報の暗号化に加え,その Web サイトやサーバが確かに信頼できるものと証明する ために使われる重要なものです。ここで説明している CA 証明書 についても同様で,安易にイン ストールするものではなく,本当に正しい証明書かどうかをしっかりと確認した上でインストー ルする必要があります。

#### 2. CA 証明書の取得

下記の URL から「Security Communication RootCA2 証明書」をダウンロードしてください。 (右の QR コードからもアクセスすることができます)

https://repository.secomtrust.net/SC-Root2/SCRoot2ca.cer



#### 3. CA 証明書のインストール

ここではAndroid10を例に説明しています。

証明書の名前	を指定する	<b>b</b>
英数字で証明書名を 証明書名:	入力してくださ	い。
SCRoot2ca		
認証情報の使用 Wi-Fi	•	•
パッケージの内容: CA証明書1件		
	キャンセル	ок

任意の証明書名を入力し、認証情報の使用を「Wi-Fi」にして「OK」をタップしてください。

Copyright(c) 2001-2020, Kyoto Sangyo University. All rights reserved.

■■ コンピュータ環境の使い方 ■■ 京都産業大学 情報センター ..... ※ 証明書をすでにダウンロードしている場合の証明書のインストール方法 (Android 端末の機種やバージョンによって設定項目に違いがある可能性があります。) 1) 「設定」を開き「セキュリティ」→「詳細設定」→「暗号化と認証情報」→「ストレージか らのインストール」と順にタップしてください。 プニ イバシー ← セキュリティ Q Q 設定を検索 2020年/月1日 暗号化 デバイスのセキュリティ 位置情報 スマートフォンの暗号化 ON - 43 個のアプリに位置情報へのアクセ 暗号化されています 画面ロック スを許可 ۲ ロックNo. (PIN) 認証情報ストレージ セキュリティ 指紋 ഫ് ストレージのタイプ 画面ロック、指紋 5個の指紋を登録済み ハードウェア式 Smart Lock ドコモのサービス/クラウド 信頼できる認証情報 • dアカウント設定、ドコモクラウド 信頼できるCA証明書を表示する デバイス管理アプリ 有効なアプリ:4個 ユーザー認証情報 アカウント 0 保存されている認証情報の表示と変更 Adobe, Google, Twitter SIM カードロック設定 ストレージからのインストール ユーザー補助 ストレージから証明書をインストールする 暗号化と認証情報 Ť スクリーン リーダー、表示、操作のコントロール

# 4. インターネットスポットへの接続

2)

以下の「1.インターネットスポットへの接続手順」と同じように設定していきます。

暗号化されています

ダウンロードした「SCRoot2ca.cer」を選択するとインストール画面が開きます。

認証 フトレージの 消井

インターネットスポット接続手順【Android】

http://www.kyoto-su.ac.jp/ccinfo/use network/internet spot/android.html

「手順 1-4.」で、「CA 証明書」欄にインストールした「SCRoot2ca.cer」を選択します。

### 5. 取得した CA 証明書が正しいかどうか確認する方法

パソコンにダウンロードすることで CA 証明書が本当に正しいものかどうかを確認できます。 以下, Windows パソコンでの作業です。

1) ダウンロードした CA 証明書をダブルクリックしてください。



2) 証明書情報ウィンドウが表示されますので,詳細タブ(下図①)をクリックし、フィールドに「拇 印アルゴリズム」「拇印」の項目が表示するまでスクロールし,「拇印」をクリック(下図②) します。

. IL	表示(S): 〈すべて〉	•	
	フィールド	值	
	□□ 公開キー	RSA (2048 Bits)	
- 11	前サブジェクト キー識別子	0a 85 a9 77 65 05 98 7c 40 8	
- 11	データーの おまま 4月2日	Certificate Signing, Off-line C	
- 11	※ 第一条の目的でしていた。	subject Type=CA, Path Lengt	
- 11	1000	5f 3b 8c f2 f8 10 b3 7d 78 b4	-
- 11	and the second s		

「拇印アルゴリズム」が「sha1」で,「拇印」が「5f 3b 8c f2 f8 10 b3 7d 78 b4 ce ec 19 19 c3 73 34 b9 c7 74」であることを確認してください。