デジタル証明書

1. 概要

デジタル証明書は公開鍵基盤（Public Key Infrastructure：PKI）の構成要素の一つで、デジタル証明書を発行する認証局（Certificate Authority：CA）と公開鍵暗号技術を組み合わせてインターネットにおける通信の盗聴、改ざん、なりすまし、否認を防ぐ仕組みを提供します。この仕組みによってユーザは、インターネットでの安全なネットワーク通信を利用できます。

NTT ドコモが提供する「SECURITY for Biz」対応スマートフォン（タブレットも含み、以下同様とします）は、デジタル証明書（X.509 v3 証明書）をサポートしており、このデジタル証明書を利用した法人ユーザ向けのサービスや機能を利用することが可能です。

2. サポートする形式・規格

X.509 v3 証明書の DER エンコード方式のデータをサポートし、スマートフォンへインポートすることができます。ご利用の際は、ファイルの拡張子は「.crt」又は「.cer」と指定してください。

※PEM エンコード方式（DER のバイナリコードを Base64 でエンコードした形式）は、ご利用できませんので、別途変換作業が必要となります。

また、秘密鍵や公開鍵証明書等、複数のオブジェクトを単一ファイル内に格納できる PKCS#12 フォーマットもサポートしております。ご利用の際は、ファイルの拡張子は「.p12」または「.pfx」と指定してください。

3. デジタル証明書をサポートしている機能について

「SECURITY for Biz」対応スマートフォンにて動作確認を行っているデジタル証明書を利用可能な機能は下記となります。

- VPN：

  L2TP/IPSec や IPSec Xauth にてデジタル証明書（RSA）を利用した接続においてデジタル証明書を利用できます。

- 無線 LAN（Wi-Fi）:

  802.1X 仕様にある EAP（Extensible Authentication Protocol）を利用した認証（EAP-TLS）においてデジタル証明書を利用できます。

- Microsoft® Exchange:

  Microsoft 社の Exchange ActiveSync®（EAS）にて、HTTPS 通信を利用する場合、デジタル証明書を利用したクライアント証明書認証を行うことができます。

- ブラウザ（プリインストール）:

  HTTPS 通信を利用する場合、デジタル証明書を利用したクライアント証明書認証を行うことができます。

  ※Chrome ブラウザに関しては、本ドキュメントの対象外といたします。

4. デジタル証明書のインストール・削除・無効化について

<<インストール>>

・デジタル証明書をインストールする主な方法は、次の通りとなっています。

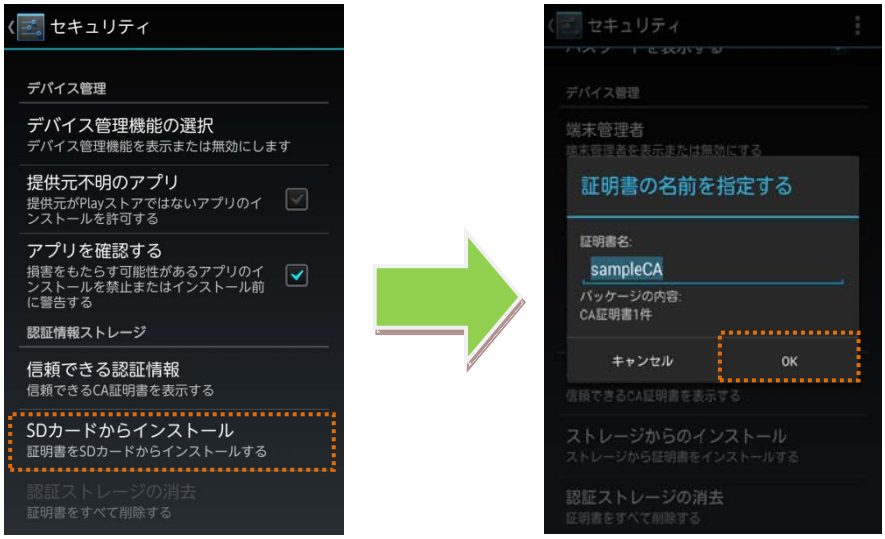
① SD カードディレクトリパス直下へ配置した証明書ファイルのインストール

② 内部ストレージディレクトリパス直下へ配置した証明書ファイルのインストール

③ Web ブラウザアプリを用いることで、URI によって指定した場所より、証明書ファイルを HTTP 通信プロトコル経由でダウンロードしてインストール

・方法①、②の場合は、予めデジタル証明書を Android™スマートフォン内の各所定ディレクトリに配置して、「本体設定」メニューから「セキュリティ」項目にある「SD カードからのインストール」よりインストールができます。

※デジタル証明書のインストールメニュー表示は、機種毎にメニュー配置や名称が異なります。



※本ドキュメントに掲載している端末キャプチャ画像には説明のため ARROWS NX（F-06E）を使用しております。

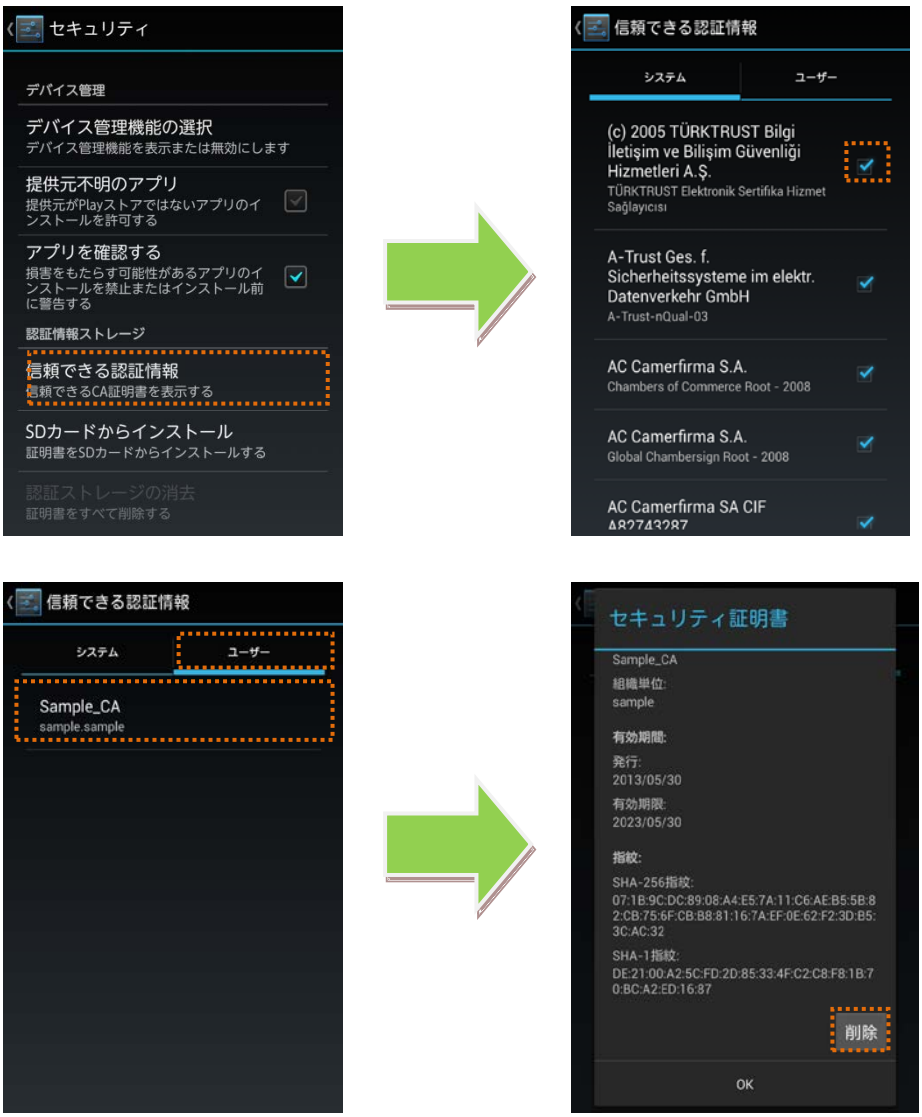
・方法③の場合は、デジタル証明書ファイルがあるアクセス先に Web ブラウザアプリでアクセスするだけで、証明書のインストールオペレーションが実行されます。

<<削除/無効化>>

・Android スマートフォンへインストールしたデジタル証明書の削除やプリインストールされている CA 証明書の無効化は、スマートフォン内で管理されているデータベースを操作することで可能です。

・「設定」メニューから「セキュリティ」項目にある「信頼できる認証情報」より証明書一覧を確認することができ、「システム」タブ内のプリインストールされている CA 証明書リストから CA 証明書を無効化することができます。また、「ユーザ」タブ内にある CA 証明書リストから自身の証明書そのものを削除することが可能です。

※デジタル証明書のインストールメニュー表示は、機種毎にメニュー配置や名称が異なります。



※本ドキュメントに掲載している端末キャプチャ画像には説明のため ARROWS NX（F-06E）を使用しております。

・クライアント証明書はスマートフォンから個別削除できません。消去するには、認証ストレージの消去をする必要があります。

5. プリインストールされているルート CA 証明書について

スマートフォンに初期状態（お買い上げ状態）からインストールされているルートCA 証明書は、メーカーや機種によって異なります。

スマートフォンごとのルート CA 証明書リストは、下記のドコモサイトに記載しております。

【NTT ドコモ 端末・ブラウザスペック】
http://spec.nttdocomo.co.jp/spmss/
各機種のリンク先にある、機能選択より「SSL」を選択いただくことでご確認頂けます。

6. 注意事項

- 機種により対応状況や操作方法が異なる場合があります。
- 本ドキュメントの掲載内容について、お客様環境での動作を完全に保証するものではございません。
- Chrome ブラウザの動作に関しては、Google 社のアップデートにより変更となる場合がございます。
- 本ドキュメント掲載のサービス内容、商品の仕様・性能などは、予告なしに変更する場合があります。
- 本ドキュメント掲載のアクセスフロー、URL などは、予告なしに変更する場合があります。
  掲載されている会社名、商品名は、各社の商標または登録商標です。
- 本ドキュメントから許可なく転記、複写することを固く禁じます。

7. お問い合せ先

※ご不明点については下記窓口にお問い合わせください。
【NTT ドコモお客様窓口】
http://www.docomo.biz/d/contact_wp2