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 Android™ スマートフォン/タブレットは、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

Android スマートフォン/タブレット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:

  IPSec IKEv2 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 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。

-プリインストールの Web ブラウザ

  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。

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

・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、端末設定内のセキュリティ項目にある「証明書のインストール」から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。

・SD カードや内部ストレージへの証明書ファイル配置については、メール添付や Web ブラウザからのファイルダウンロード、他機器とのケーブル接続によるデータ移行など様々な方法があります。

●証明書のインストール方法について

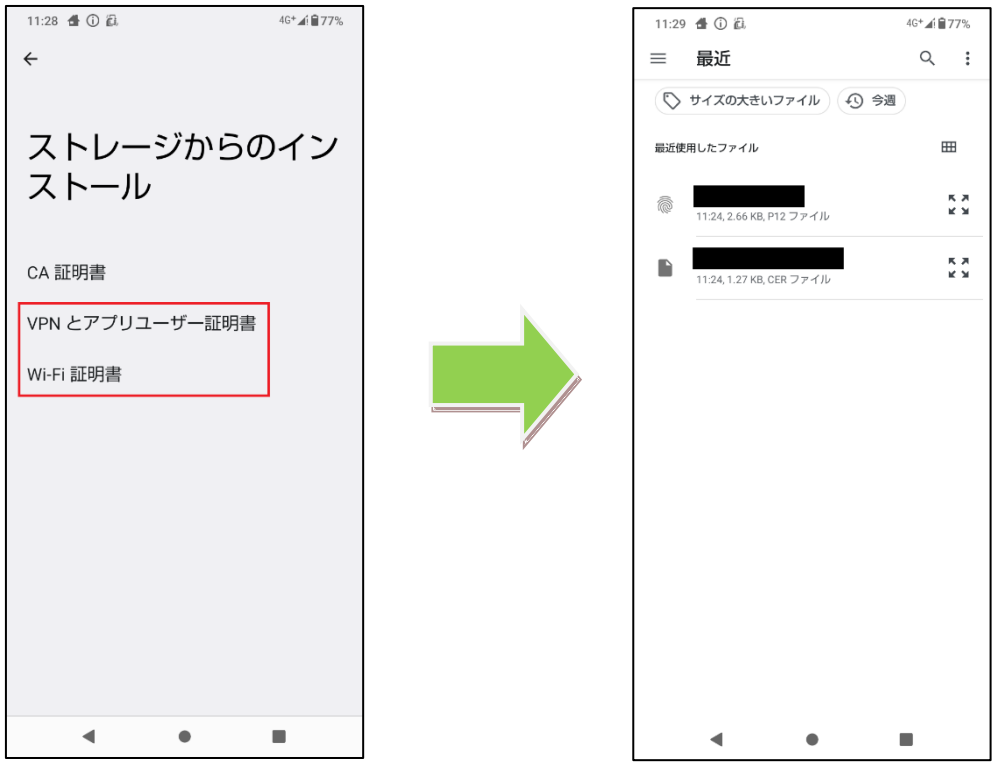
1. 端末設定内のセキュリティ設定で「暗号化と認証情報」→「ストレージからのインストール」と進みます。

※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 AQUOS wish2 SH-51C を使用しております。

2. CA 証明書をインストールする場合は、「CA 証明書」を選択し、「インストールする」を押下します。

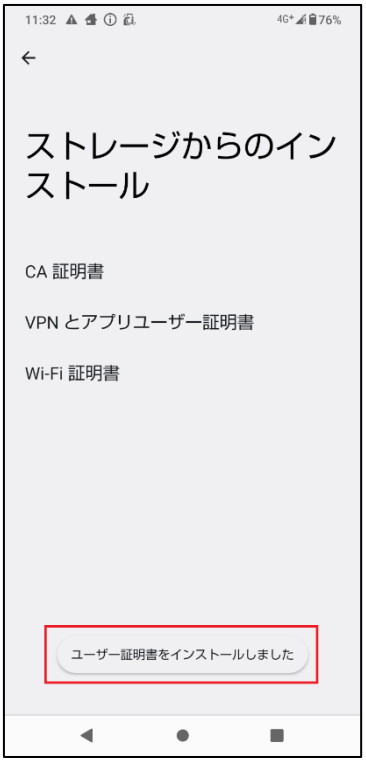
3. ストレージからインストールしたい CA 証明書を選択します。
   証明書が正常にインストールできた場合、インストールが完了した旨の通知が表示されます。

4. ユーザー証明書をインストールする場合は、用途に応じて「VPN とアプリユーザー証明書」または「Wi-Fi 証明書」を選択します。
   ストレージからインストールしたいユーザー証明書を選択します。



5. 証明書抽出用パスワードを入力し、証明書の名前を設定します。

6. 証明書が正常にインストールできた場合、インストールが完了した旨の通知が表示されます。



<<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。

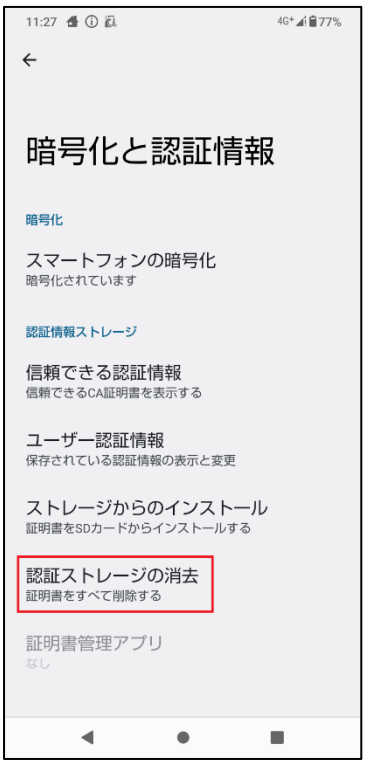
・端末設定内のセキュリティ項目にある「信頼できる認証情報」から証明書一覧を確認することができ、「システム」タブ内のプリインストールされている CA 証明書リストから CA 証明書を無効化することができます。また、「ユーザ」タブ内のアドインストール CA 証明書については、「認証ストレージの消去」を実行することで削除することが可能となります。

※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。

●プリインストールされている証明書一覧画面と証明書詳細画面

●アドインストールされている証明書一覧画面と証明書詳細画面

●「認証ストレージの消去」を押下することで、全てのアドインストール証明書を削除可能



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】
https://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。
- Web ブラウザの動作に関しては、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。
- 「Android」 は、Google LLC の商標または登録商標です。
- 「Wi-Fi」は、Wi-Fi Alliance の商標または登録商標です。
- 「Microsoft Exchange ActiveSync」 は、米国 Microsoft Corporation の米国およびその他の国における商標または登録商標です。
- 「AQUOS」、「AQUOS wish」 は、シャープ株式会社の商標または登録商標です。
- その他、本資料に記載されている会社名、製品名、サービス名は、一般に各開発メーカーおよびサービス提供元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

- 機種毎の対応状況、操作方法、動作確認状況、及びその他のご不明な点につきましては下記お客様サポートまでお問い合わせください。
  【NTTCom お客様サポート(ドコモ法人契約向け)】
  https://support.ntt.com/purpose?subContentsType=2106&businessPersonalFlg=business