DoMobile ASP サービス 証明書置き換え手順

この手順書は、リモート端末（アクセスする側の端末）にインポートされた証明書（CA 証明書、および、クライアントデジタル証明書）を置き換えるための手順を示しています。

⚠ ご注意!!

① 証明書の置き換えは、1 カ月以内に行ってください。
※現行の証明書を使い続けると認証エラーが発生してリモートアクセスができなくなる場合があります。
② 証明書の置き換えは、リモートアクセス時には行わないでください。
③ リモート端末が Windows の場合、証明書の置き換えは Windows の管理者権限で行ってください。
④ 1 台の自席 PC に対して複数のリモート端末をご利用されている場合、すべてのリモート端末の証明書は同じタイミングで置き換えてください。
※証明書の置き換えを行ったリモート端末からリモートアクセスを行うと、その後、証明書の置き換えを行っていないリモート端末からは認証エラーが発生してリモートアクセスができなくなります。

目次

1. 事前準備

管理者から以下のものを入手してください。

① ca.cer ファイル ： CA 証明書

ca.cer ファイルをお持ちでない場合は以下の URL よりダウンロードしてください。

URL については、サポートサービスセンタから展開されるアカウント発行メールに記載されている「組織コード」に従い、以下の一覧表の URL をご使用ください。
アカウント発行メールに組織コードの記載がない場合は、「[0]または[S]で始まる場合」の URL をご使用ください。

#	組織コード	URL
1	[0]または[S]で始まる場合	https://dm0001.b-sol.jp/ca.crt
2	[W1]で始まる場合	https://dm0101.b-sol.jp/ca.crt
3	[W2]で始まる場合	https://dm0201.b-sol.jp/ca.crt
4	[W3]で始まる場合	https://dm0301.b-sol.jp/ca.crt
5	[W4]で始まる場合	https://dm0401.b-sol.jp/ca.crt
6	[W5]で始まる場合	https://dm0501.b-sol.jp/ca.crt

② 証明書のパスワード（アクティブ化コード）

③ Your Certificate.pfx ファイル ： リモート PC 用証明書

④ Your Certificate.01f ファイル ： DoMobile Go アプリ用証明書

（iOS 端末、Windows タブレット PC、Android 端末を使用しない場合は不要です。）

⑤ Your Certificate.01f ファイル設定用 PC（自席 PC やリモート PC でも可）

（iOS 端末、Android 端末を使用しない場合は不要です。）

2. 証明書と自席 PC のアクティブ化コードの確認（自席 PC 側作業）

管理者から入手したリモート PC 用証明書が格納されているフォルダ名（数字 8 桁）と、自席 PC のアクティブ化コード（数字 8 桁）とが一致していることを確認します。

① 管理者から入手したリモート PC 用証明書が格納されているフォルダ名（数字 8 桁）が証明書のアクティブ化コードです。この数字をメモ帳などに控えてください。

② 自席 PC のタスクトレイ内にある DoMobile アイコンをダブルクリックして、ステータスウィンドウを表示します。

よくあるお問合せ

（a）DoMobile アイコンが表示していない場合

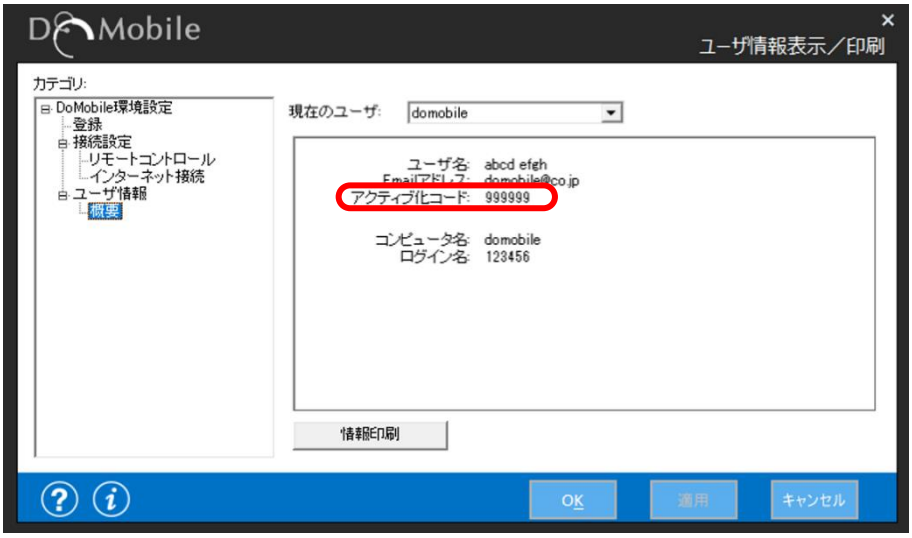
- DoMobile を再起動する
  - ① 「タスク マネージャー」起動－「プロセス」－「IIT.exe」選択－「タスクの終了」
  - ② DoMobile を起動する

（b）ステータスウィンドウが表示しない場合

- DoMobile をインストールした Windows ユーザで再ログインする
- DoMobile を再起動し、UAC（ユーザー アカウント制御）が表示されたら「はい」や「OK」をクリックする

③ 「カテゴリ」–「概要」の「アクティブ化コード」の数字 8 桁が①で控えた数字と一致していることを確認してください。

※一致していない場合リモートアクセスが行えません。管理者に連絡して確認を依頼してください。



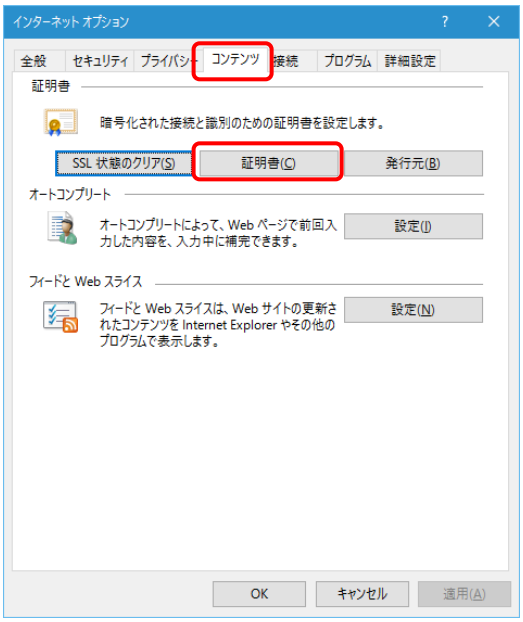
3. 証明書の置き換え（リモート PC）（リモート PC 側作業）

3.1 旧デジタル証明書の削除

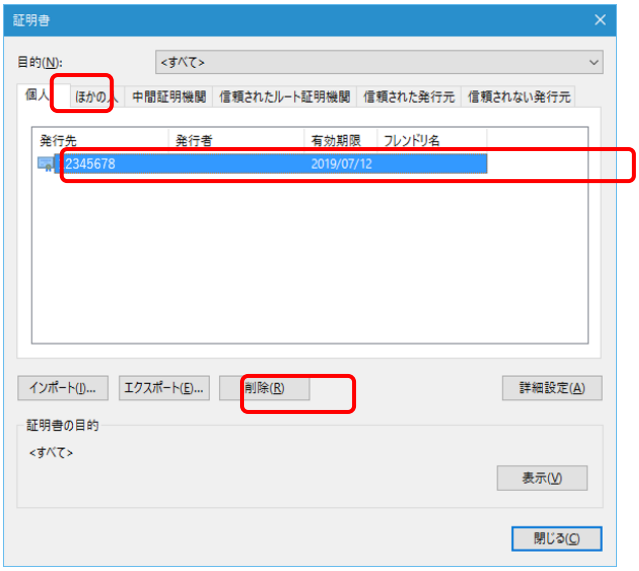
3.1.1 Microsoft Edge/Google Chrome/ Internet Explorer の場合

① Windows の検索ボックスで「インターネットオプション」を検索し、開きます。

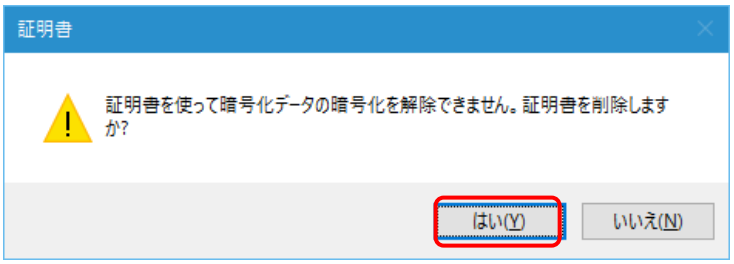
② 「インターネット オプション」が表示されましたら、「コンテンツ」タブの「証明書」ボタンをクリックします。



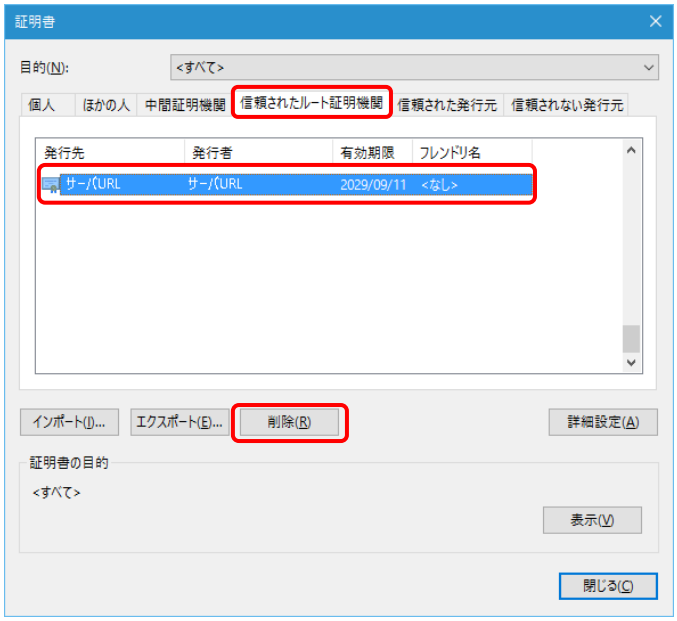
③ 「証明書」が表示されましたら、「個人」タブの該当するクライアントデジタル証明書（発行先にアクティブ化コードが表示）を選択し、「削除」ボタンをクリックします。



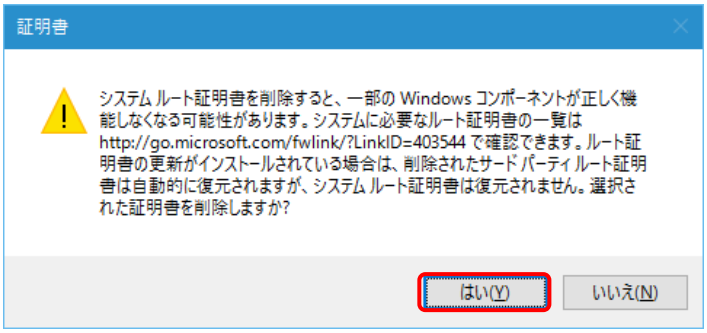
④ 確認ダイアログが表示されますので、「はい」ボタンをクリックします。



⑤ 「証明書」ダイアログの「信頼されたルート証明機関」タブの CA 証明書（発行先に **DoMobile サーバの FQDN** が表示）を選択し、「削除」ボタンをクリックします。



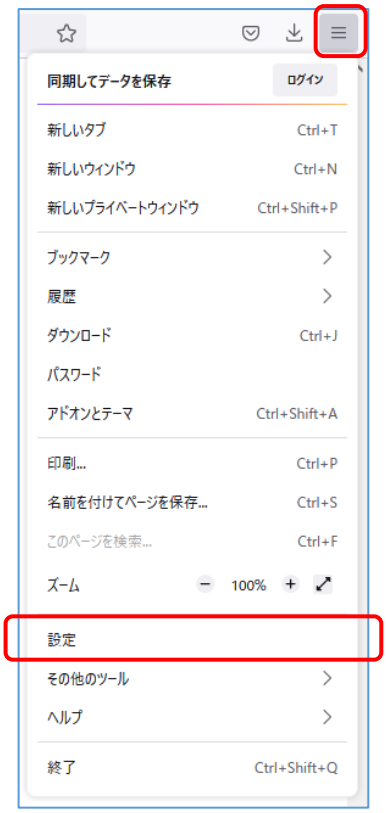
⑥ 確認のための「証明書」ダイアログが表示されますので、「はい」ボタンをクリックします。



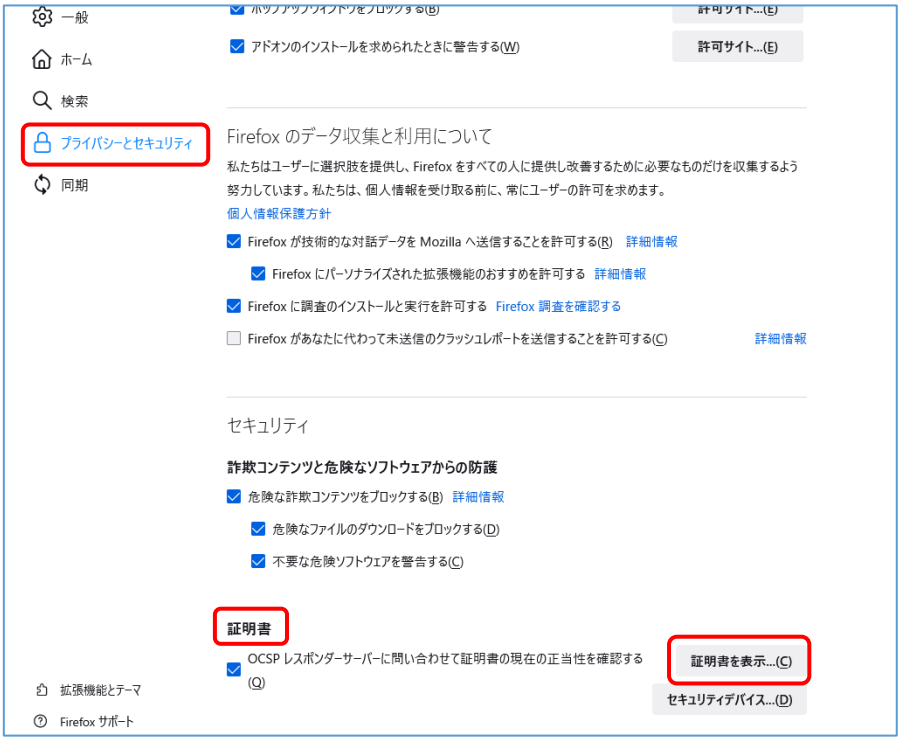
⑦ さらに、確認のための「ルート証明書ストア」ダイアログが表示されますので、「はい」ボタンをクリックします。

3.1.2 Mozilla Firefox の場合

① Firefox を起動し、右上のアイコンから「設定」をクリックします。

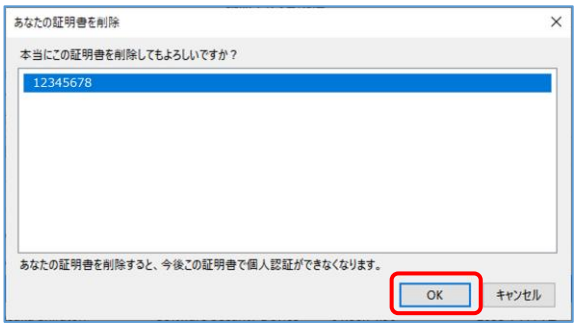


② 「プライバシーとセキュリティ」の「証明書」から「証明書を表示」をクリックします。

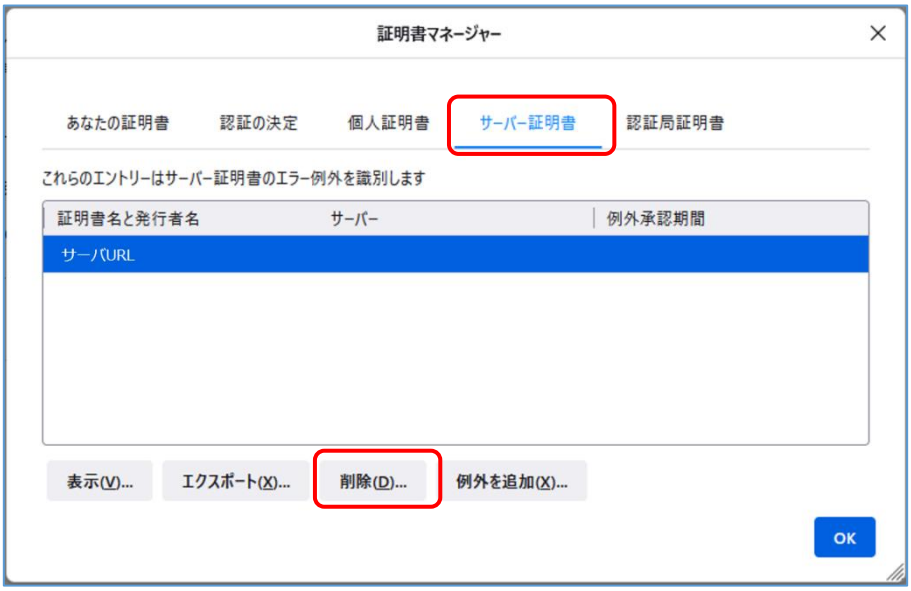


③　「あなたの証明書」タブの該当するクライアント証明書を選択し、「削除」ボタンをクリックします。

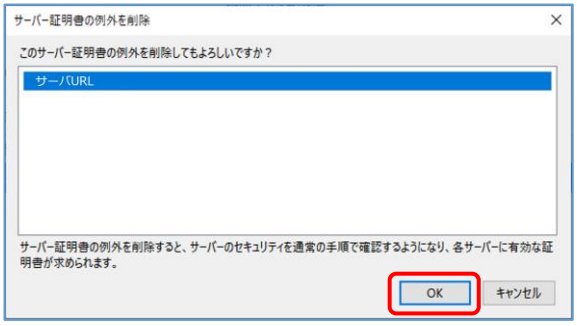
④　表示されたウインドウの「OK」ボタンをクリックします。



⑤　「サーバー証明書」の CA 証明書（発行先に **DoMobile サーバの FQDN** が表示）を選択し「削除」ボタンをクリックします。



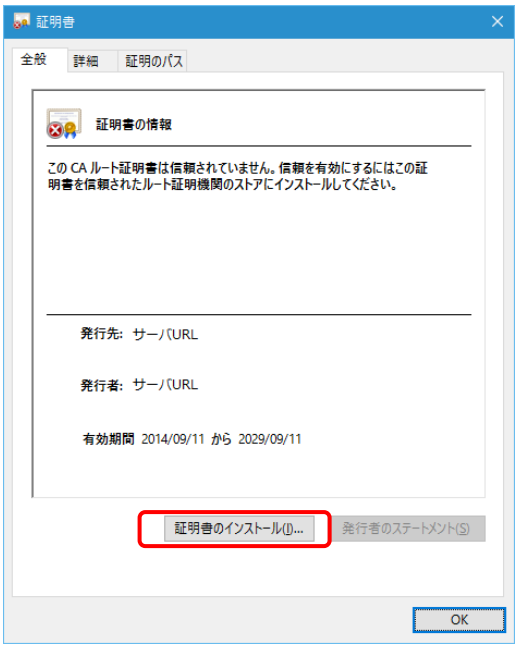
⑥　表示されたウインドウの「OK」ボタンをクリックします。



3.2　新 CA 証明書のインポート

3.2.1　Microsoft Edge/Google Chrome/ Internet Explorer の場合

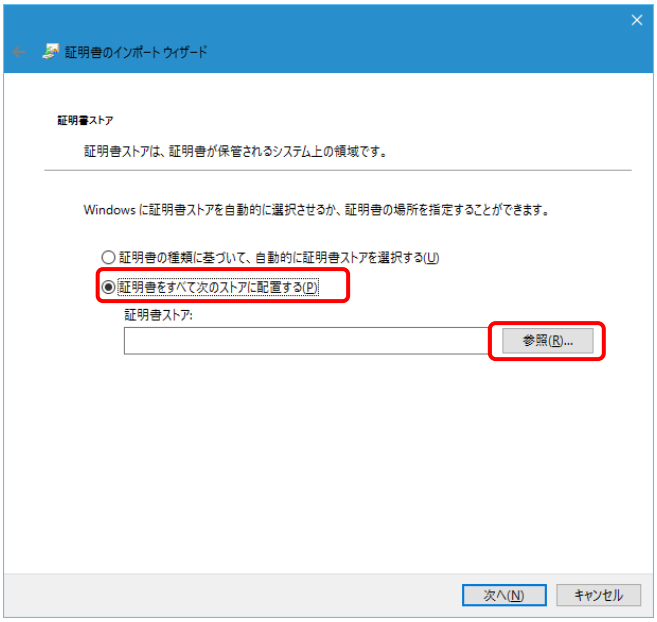
①　CA 証明書（ca.cer）を、ダブルクリックします。
ダブルクリック後、「開いているファイル - セキュリティの警告」というダイアログが表示された場合、「開く」ボタンをクリックしてください。
右の様な画面が表示されましたら「証明書のインストール」ボタンをクリックします。



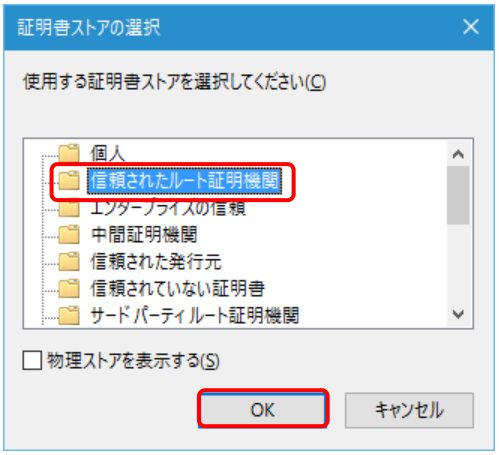
②　「次へ」ボタンをクリックします。

※　保存場所が表示されない場合があります。
※　他の Windows ユーザでもリモートアクセスを行う場合は「ローカル コンピュータ」をクリックしてください。この場合、「ユーザーアカウント制御」ダイアログが表示されます。

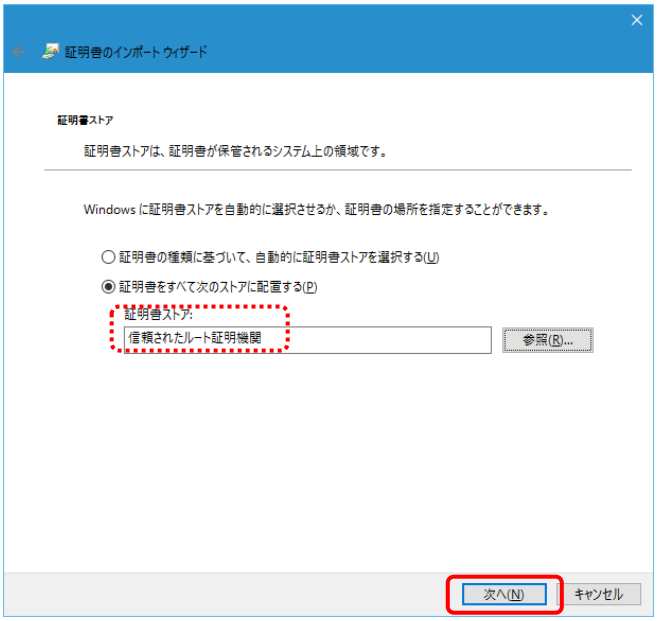
③ “証明書をすべて次のストアに配置する”を選択し、「参照」ボタンをクリックします。



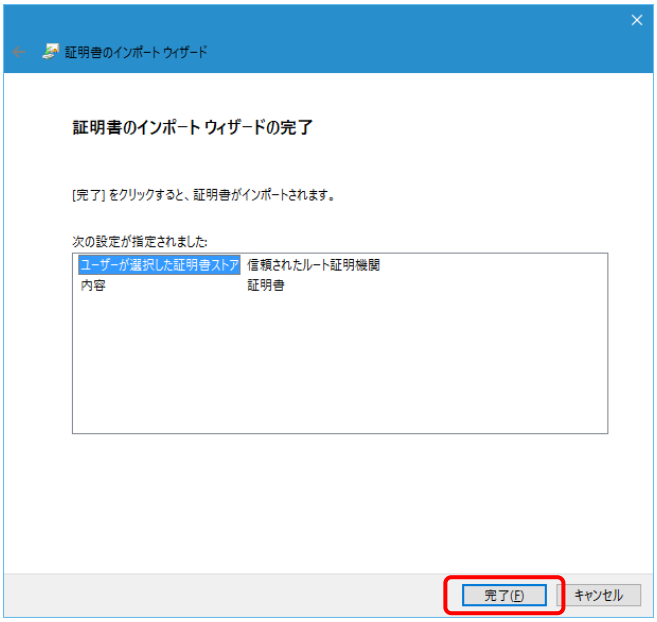
④ “信頼されたルート証明機関”を選択し、「OK」ボタンをクリックします。



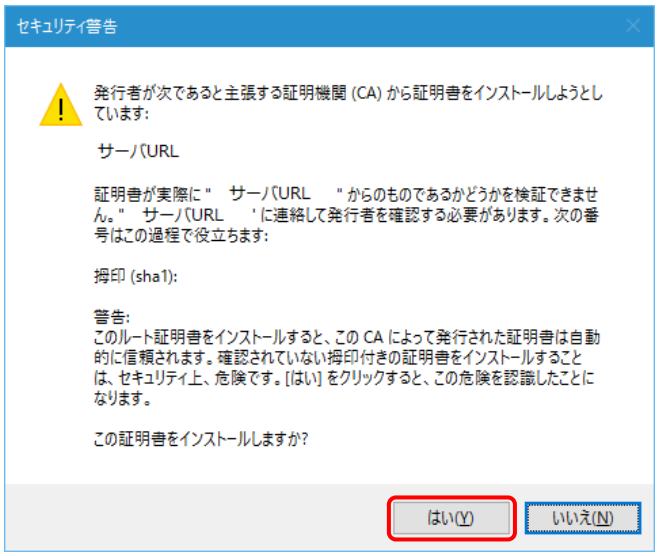
⑤ 「次へ」ボタンをクリックします。



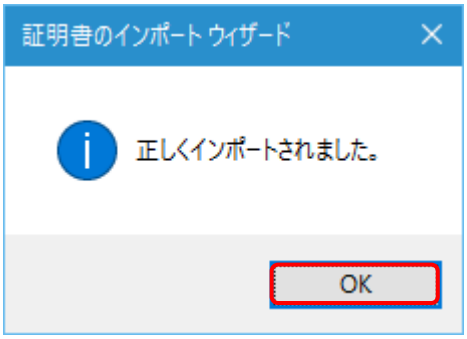
⑥　「完了」ボタンをクリックします。



⑦　「はい」ボタンをクリックします。

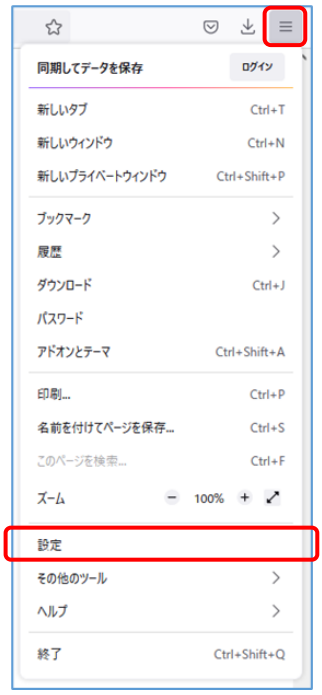


⑧　「OK」ボタンをクリックします。また、「証明書」ダイアログも「OK」ボタンをクリックして閉じてください。

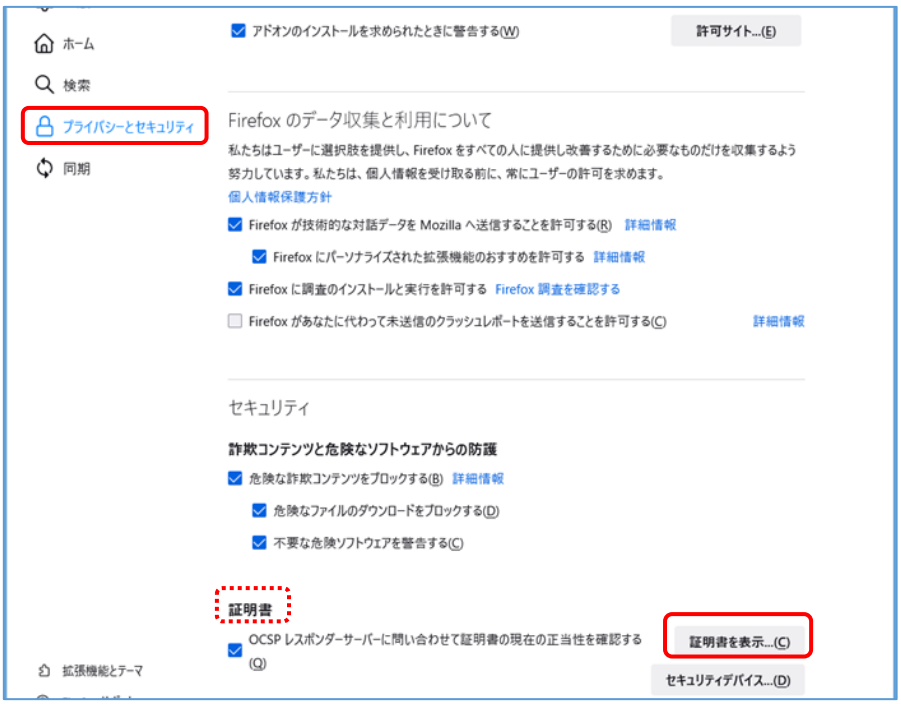


3.2.2 Mozilla Firefox の場合

① Mozilla Firefox を起動してメニューを開いて「設定」を選択します。

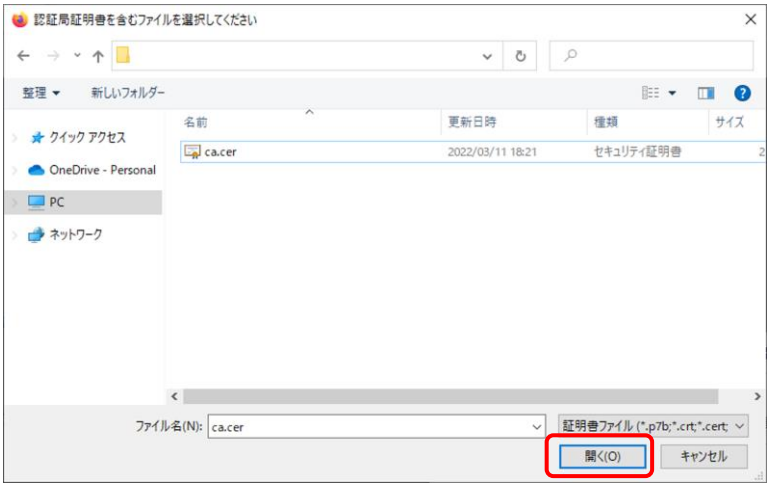


② 「プライバシーとセキュリティ」を選択し、「セキュリティ」から「証明書を表示」をクリックしてください。

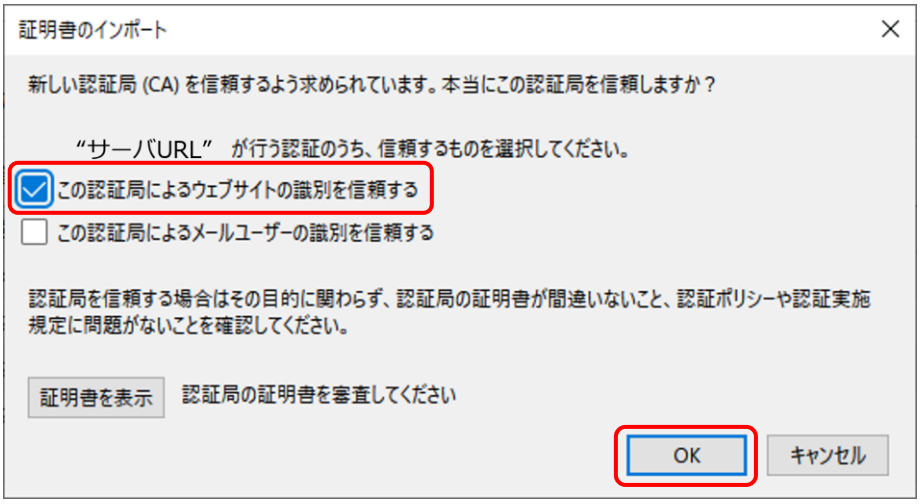


③　証明書マネージャーのウィンドウが表示され、認証局証明書が選択されていることを確認し、「インポート」をクリックします。

④　ダウンロードした ca.cer を選択し「開く」をクリックします。



⑤　証明書のインポートダイアログが表示されますので、「この認証局によるウェブサイトの識別を信頼する」をチェックオンして「OK」をクリックします。また、証明書マネージャーも「OK」ボタンをクリックして閉じてください。

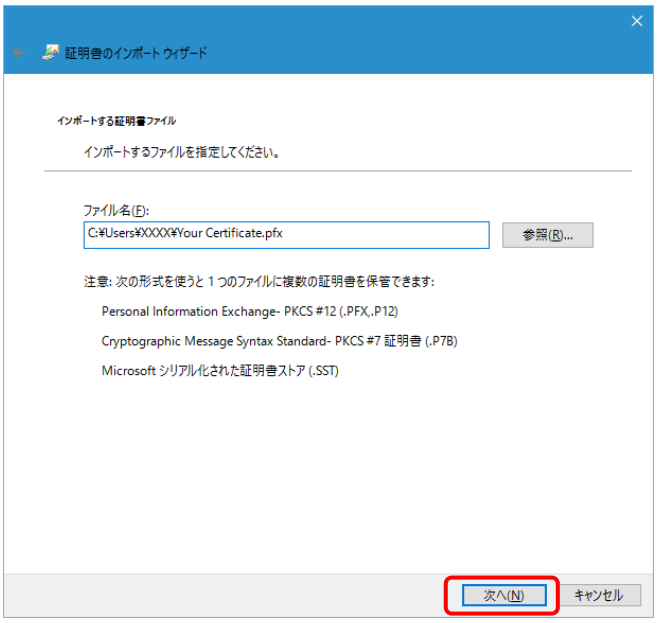


3.3 新クライアント証明書のインポート

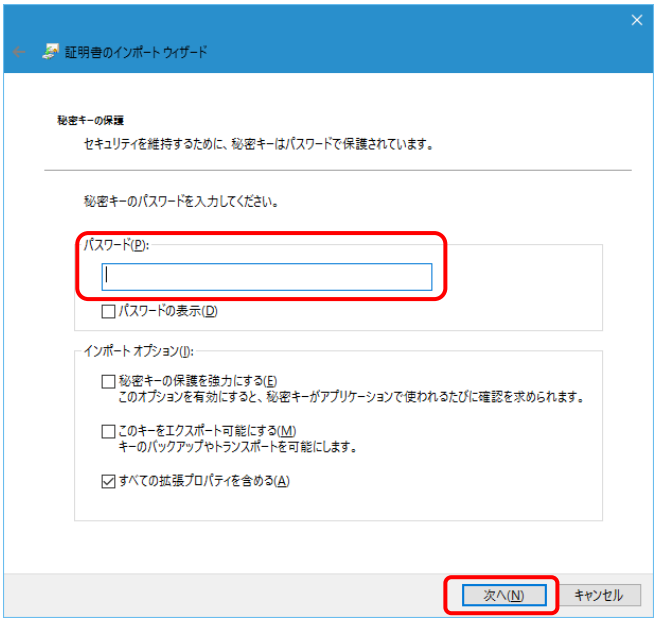
3.3.1 Microsoft Edge/Google Chrome/ Internet Explorer の場合

① リモート端末に管理者から配布された Your Certificate.pfx ファイルをコピーし、ダブルクリックします。右の様な画面が表示されますので、「次へ」ボタンをクリックします。

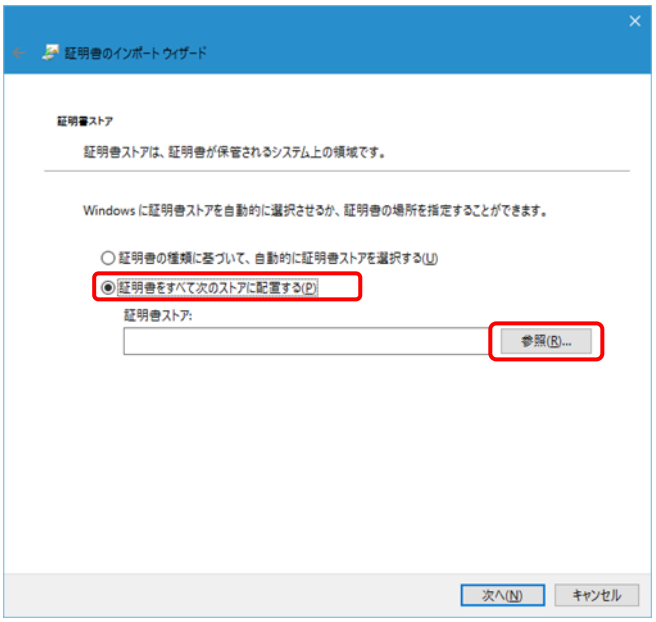
② 「次へ」ボタンをクリックします。



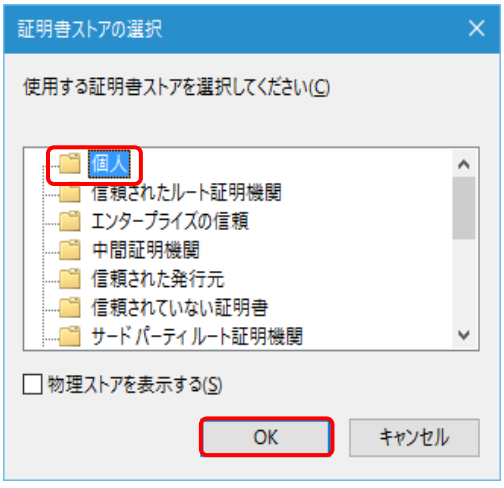
③ 管理者より配布された「クライアントデジタル証明書パスワード」をパスワード入力欄に入力して、「次へ」ボタンをクリックします。



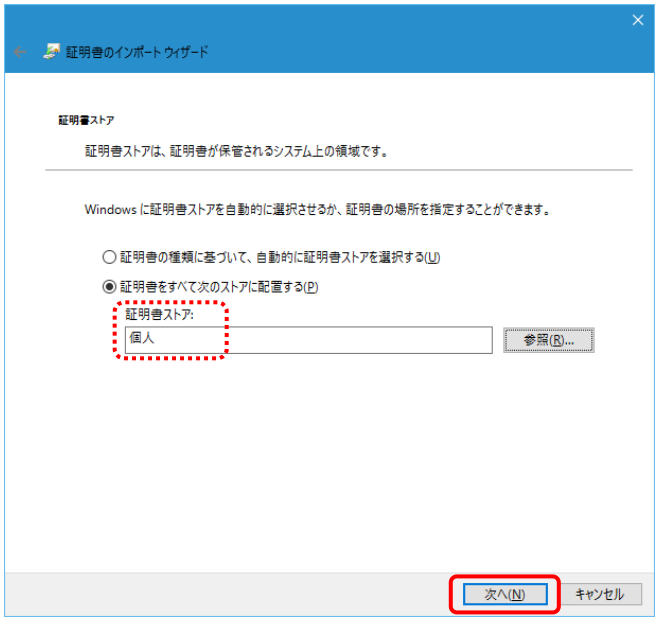
④ “証明書をすべて次のストアに配置する”を選択し、「参照」ボタンをクリックします。



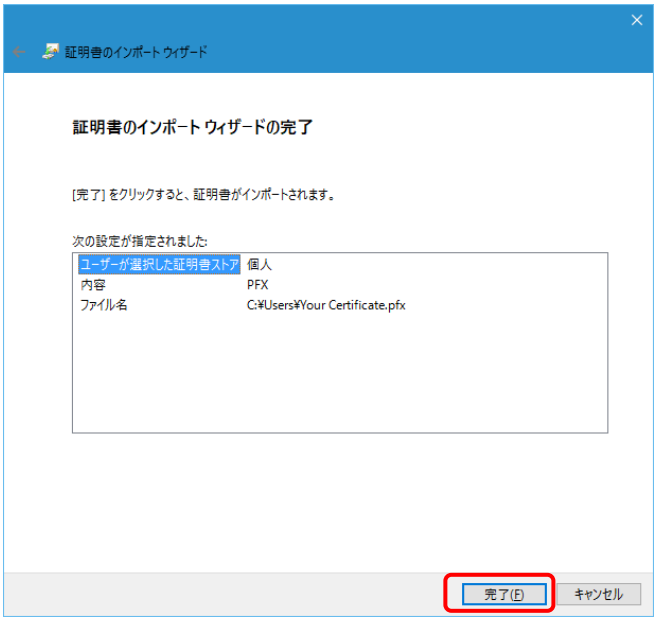
⑤ “個人”を選択し、「OK」ボタンをクリックします。



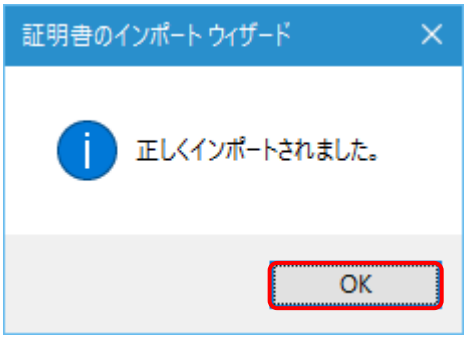
⑥　「次へ」ボタンをクリックします。



⑦　「完了」ボタンをクリックします。



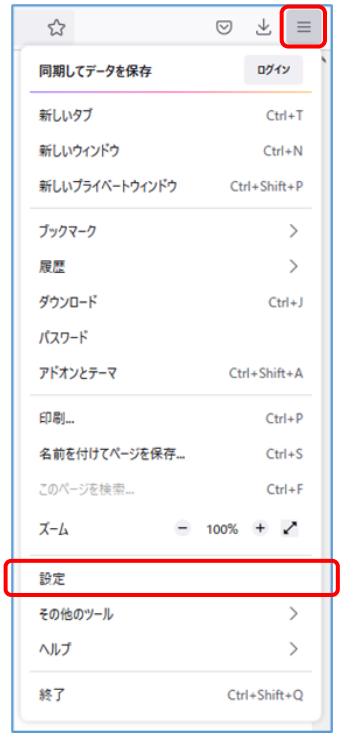
⑧　「OK」ボタンをクリックします。また、「証明書」ダイアログも「OK」ボタンをクリックして閉じてください。



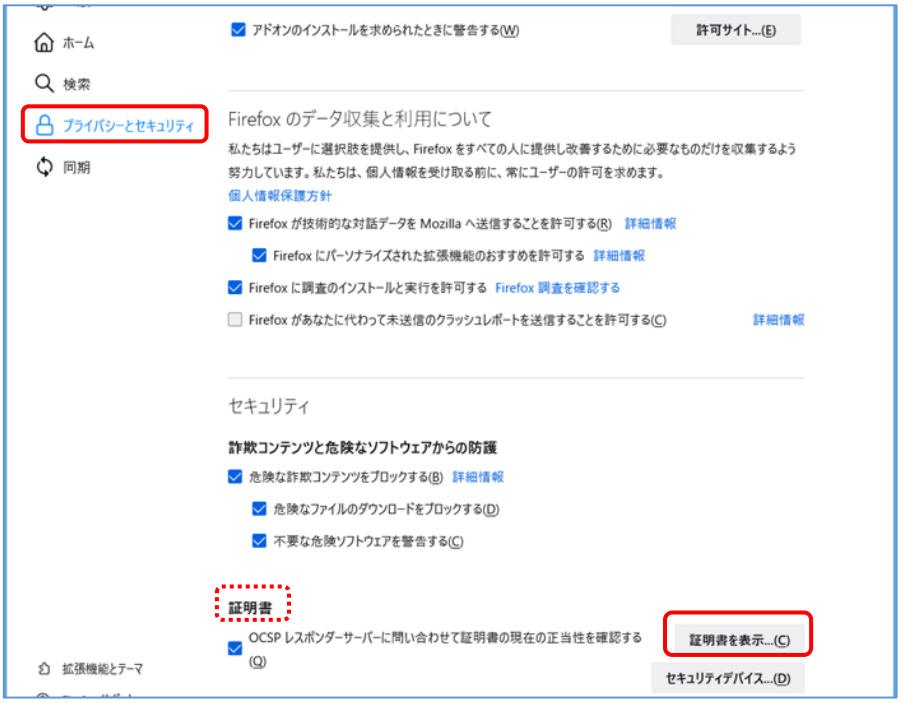
3.3.2 Mozilla Firefox の場合

① リモート端末に管理者から配布された Your Certificate.pfx ファイルをデスクトップ上など任意の場所に保存します。

② Mozilla Firefox を起動してメニューを開いて「設定」を選択します。

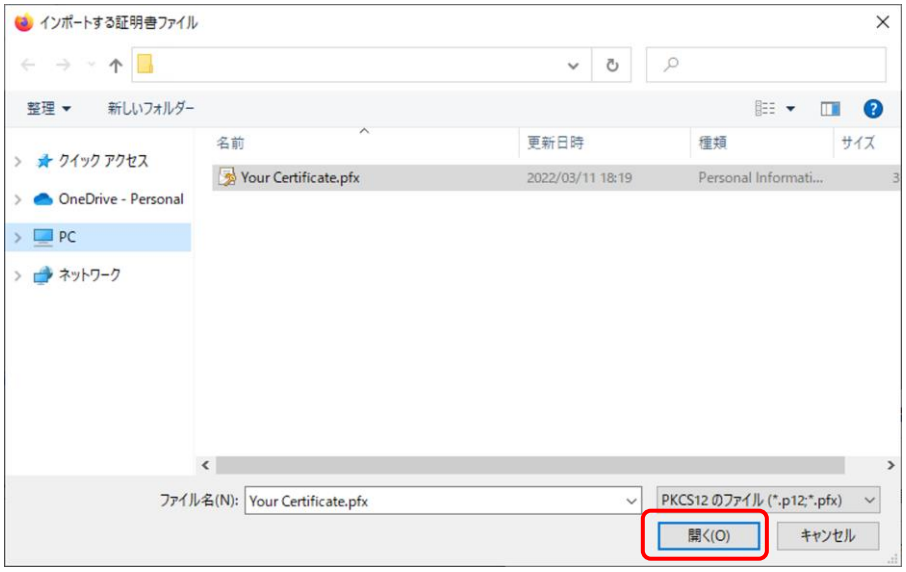


③ 「プライバシーとセキュリティ」を選択し、「セキュリティ」から「証明書を表示」をクリックしてください。



④ 証明書マネージャーのウィンドウが表示され、あなたの証明書が選択されていることを確認し、「インポート」をクリックします。

⑤ ダウンロードした"Your Certificate.pfx"を選択し「開く」をクリックします。



⑥ 管理者から通知された証明書のパスワードを入力し、「ログイン」ボタンをクリックします。また、証明書マネージャーも「OK」ボタンをクリックして閉じてください。

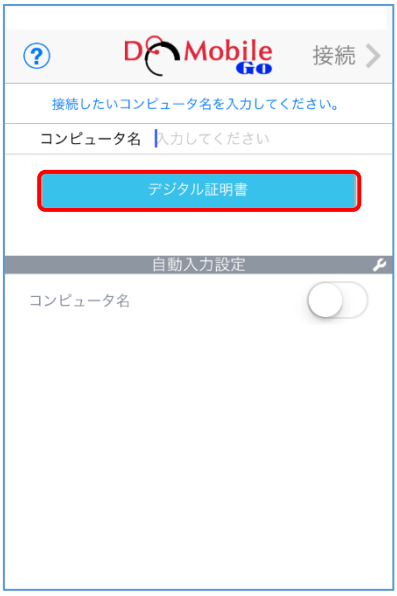
3.4 リモートコントロールの確認

※一台の自席 PC に対して複数のリモート端末を利用されている場合は、すべてのリモート端末の証明書を置き換えてから確認してください。

4. 証明書の置き換え（iOS 端末）（iPad / iPhone 側作業）

旧デジタル証明書の削除

① DoMobile Go アプリを起動し、「デジタル証明書」をタップします。



② 「デジタル証明書」が表示されましたら、アクティブ化コードが表示された証明書をタップして、「削除」をタップします。

③ DoMobile Go アプリを終了します。

新デジタル証明書のインポート

メールで端末に送る:

① リモート端末で読み込めるメールアカウントで、メールに添付したデジタル証明書（Your Certificate.01f）を受信します。

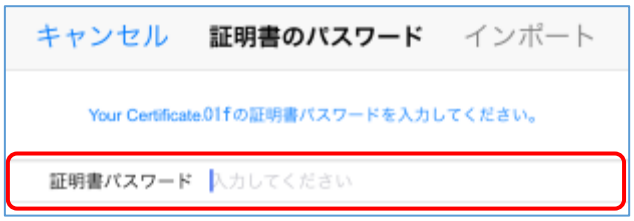
② メールに添付したデジタル証明書をタップします。

③ 「サポートされていないファイル形式です」と表示された画面に遷移します。

④ 右上のアイコンをタップします。

⑤　表示されたメニューの中から  を選択します。

⑥　タップすると DoMobile Go が起動し、デジタル証明書のパスワード画面が表示します。パスワードの入力画面が表示されたら、「証明書パスワード」を入力し、「インポート」ボタンをタップします。



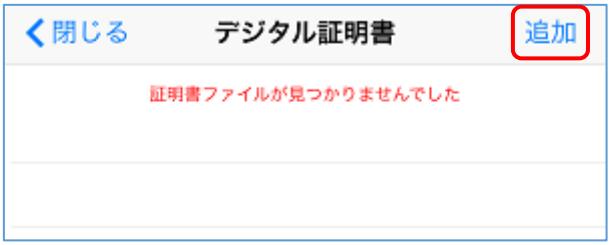
⑦　デジタル証明書がインストールされたことを確認して、「閉じる」ボタンをタップします。

⑧　リモート端末で「マルチタスク」を起動し、アプリを終了させてください。

itunes 経由でコピーする:

① PC に itunes をインストールします。
② PC とデバイスをケーブルで接続し、itunes 上でデバイスを選択します。
③ 左側の「設定」カテゴリに表示される「ファイル共有」メニューをクリックします。
④ 「App」欄に DoMobile Go が表示されますので、クリックします。
⑤ 右側に「DoMobile Go の書類」が表示されますので、「ファイルを追加」でデジタル証明書（YourCertificate.01f）を選択して追加します。
⑥ DoMobile Go を起動します。
⑦ デジタル証明書をタップします。

⑧ 「追加」をタップします。



⑨ Your Certificate.01f を選択して「インポート」をタップします。

⑩ デジタル証明書のパスワード画面が表示されます。パスワードの入力画面が表示されたら、「証明書パスワード」を入力し、「インポート」ボタンをタップします。

⑪ デジタル証明書がインストールされたことを確認して、「閉じる」ボタンをタップします。

⑫ リモート端末のホーム画面で「ホーム」ボタンを 2 回押し「マルチタスク」を起動し、アプリを終了させてください。

リモートコントロールの確認

iOS 端末からリモートコントロールが開始されることを確認します。

5. 証明書の置き換え（Windows タブレット PC）（Windows タブレット PC 側作業）

旧デジタル証明書の削除

① DoMobile Go アプリをアンインストールします。
② DoMobile Go アプリをインストールします。

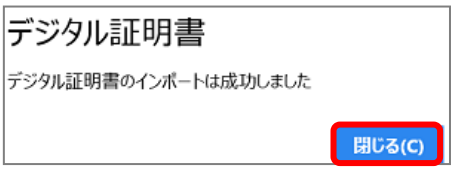
新デジタル証明書のインポート

① リモート端末のデスクトップなど任意の場所に Your Certificate.01f ファイルをコピーして、ダブルクリックします。

② 「プログラムから開く」-「すべての.01f ファイルでこのアプリを使う」がチェックオンされていることを確認後、「今後も DoMobile Go を使う」をタップします。

③ 「証明書パスワード」が表示されましたら、「パスワード」にアクティブ化コードを入力して、「インポート」をタップします。

④ 「デジタル証明書」が表示されましたら、「閉じる」をタップします。



⑤ DoMobile Go アプリを終了します。

リモートコントロールの確認

Windows タブレット PC からリモートコントロールが開始されることを確認します。

6. 証明書の置き換え（Android 端末）（Android 端末側作業）

旧デジタル証明書の削除

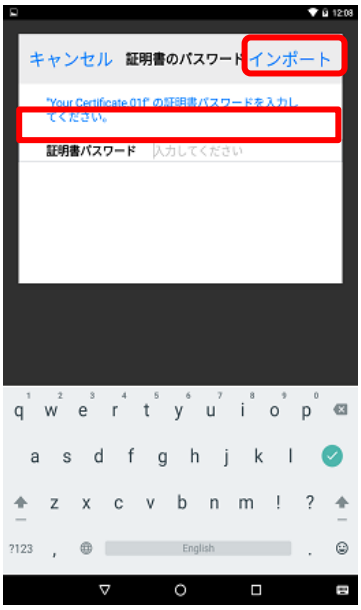
① DoMobile Go アプリを起動し、「デジタル証明書」をタップします。

② アクティブ化コードが表示された証明書をタップして、「削除」をタップします

新クライアントデジタル証明書のインポート

メールで端末に送る：

① リモート端末で読み込めるメールアカウントで、(Your Certificate.01f)を受信します。
② メールに添付したデジタル証明書をタップします。
③ 「DoMobile Go で開く」(またはそれに類するボタン)をタップします。
④ タップすると DoMobile Go が起動し、デジタル証明書のパスワード画面が表示されます。
パスワードの入力画面が表示されたら、「証明書パスワード」を入力し「インポート」ボタンをタップします。

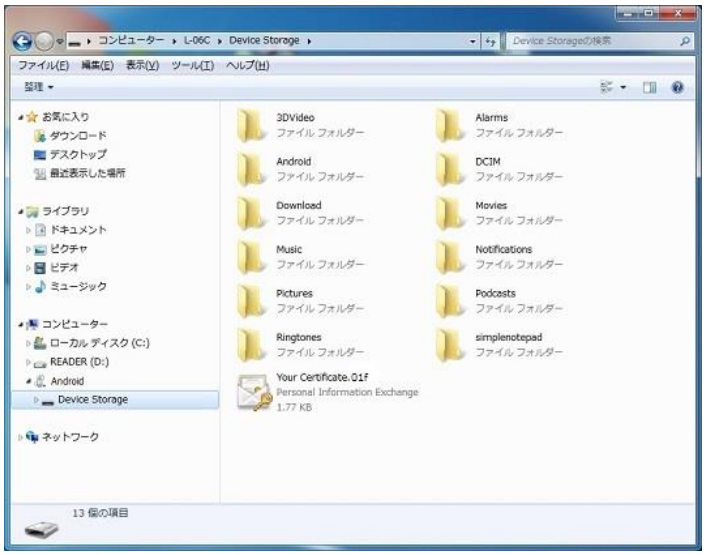


⑤　デジタル証明書がインストールされたことを確認して、「閉じる」ボタンをタップします。

⑥　デジタル証明書がインポートされたら、DoMobile Go を一度終了します。

メールが使用できない場合：

①　Your Certificate.01f ファイル設定用 PC（以降、設定用 PC と表記）にリモート端末を接続します。
②　設定用 PC がリモート端末を認識されたら、マイコンピュータからリモート端末を選択します。
③　Your Certificate.01f ファイルを設定用 PC からリモート端末にコピーします。



④　リモート端末を設定用 PC から切断します。
⑤　DoMobile Go を起動して、「デジタル証明書」をタップします。

⑥　「デジタル証明書」が表示されましたら、「追加」をタップします。

⑦ 「証明書のインポート」が表示されましたら、設定用 PC からコピーした Your Certificate.01f ファイルを選択して、「インポート」をタップします。

⑧ 「証明書のパスワード」が表示されましたら、「証明書パスワード」にアクティブ化コードを入力して、「インポート」をタップします。

⑨ 「デジタル証明書」が表示されましたら、アクティブ化コードが表示された証明書がインポートされていることを確認して、「閉じる」をタップします。

リモートコントロールの確認

Android 端末からリモートコントロールが開始されることを確認します。

以上で証明書の置き換え作業は終了です。

お困りの場合は・・・

◆◇ユーザーズガイド◇◆

https://support.hitachi-solutions-create.co.jp/asp/domobile/webhelp/asp1/jp/getting_start.htm

◆◇よくある質問・FAQ◇◆

https://www.hitachi-solutions-create.co.jp/solution/domobile_asp/faq/index.html

◆◇その他お問合せ◇◆

日立ソリューションズ・クリエイト　サービスサポートセンター

hsc-asp_support@mlc.hitachi-solutions.com

-以上-