DoMobile ASP リモートアクセス手順

この説明書は、リモート端末（アクセスする側の PC）からアクセスされる側の DoMobile PC（以下、自席 PC）にアクセスするための手順を示しています。

- ✓ 既に自席 PC への DoMobile CSE プログラムのインストールは済んでおりますね？
- ✓ 自席 PC は電源が投入された状態ですね？
- ✓ リモート端末はインターネットに接続されていますね？
- ✓ 「ユーザーアカウント制御」が無効で一般/制限ユーザ権限の場合、本手順の実行ができない場合があります。

全ての操作は、リモート端末で実施していただきます。

＜事前準備＞

リモート端末につき、初回のみの作業となります。
リモート端末にリモートアクセス認証で用いられるデジタル証明書類をインポートします。
管理者より配布された以下のものを用意してください。

- ✓ Your Certificate.pfx ファイル
- ✓ Your Certificate.01f ファイル
  （iOS/Android 専用のクライアントデジタル証明書になります。
  これらの端末を使用しない場合には不要です。）
- ✓ クライアントデジタル証明書パスワード（アクティブ化コード）

DoMobile Go をご利用する場合：
■ リモートアクセス手順、リモートコントロールの使用方法、クライアントデジタル証明書のインポート方法については、ユーザーズガイドより「DoMobile Go について」をご参照ください。

DoMobile ASP 利用・試用期間終了後、全ての証明書(CA 証明書・クライアントデジタル証明書)は削除してください。

第11版　2025年5月

目次

1. CA 証明書のインポート

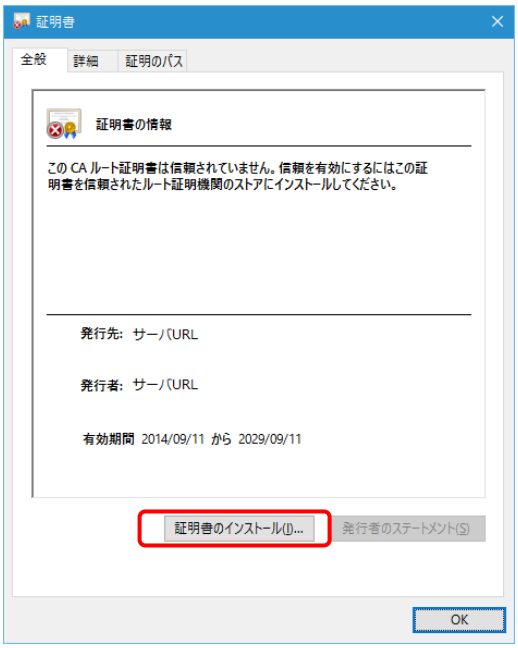
リモート端末にて以下の URL（注*1）へアクセスして、CA 証明書（ca.cer）をダウンロードし、デスクトップ上など任意の場所に保存します。

注）*1：
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

Microsoft Edge/Google Chrome の場合

① CA 証明書（ca.cer）をダブルクリックします。
（上記の URL へアクセスした際に、デジタル証明書の選択画面が表示された場合は、「OK」ボタンをクリックします。）
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。
右のよう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。

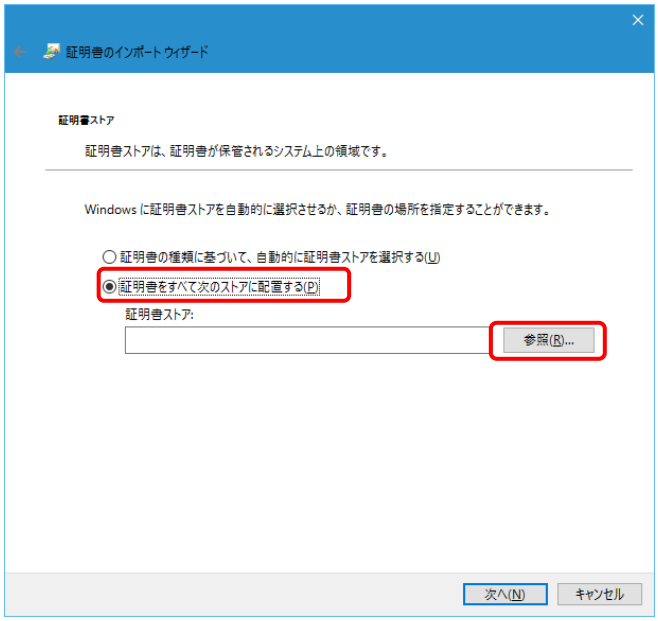


② 「次へ」ボタンをクリックします。

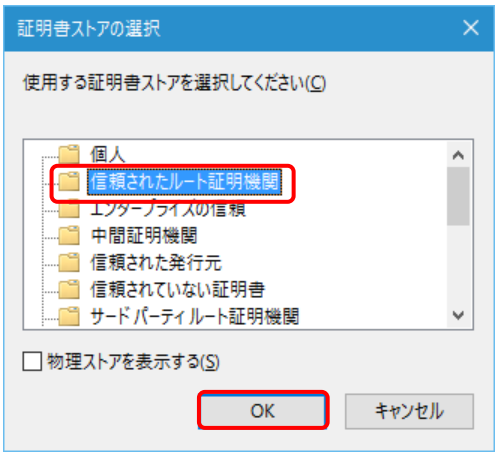
※ 保存場所が表示されない場合があります。

※ 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」を選択してください。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。

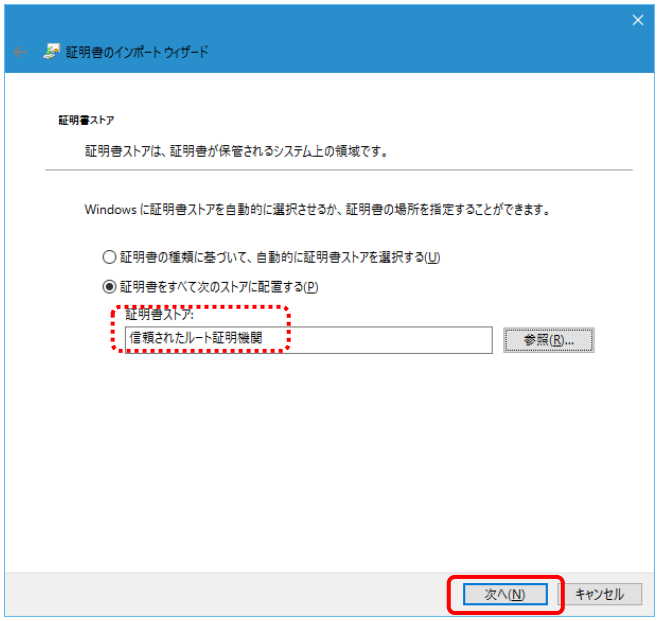
③ “証明書をすべて次のストアに配置する”を選択し、「参照」ボタンをクリックします。



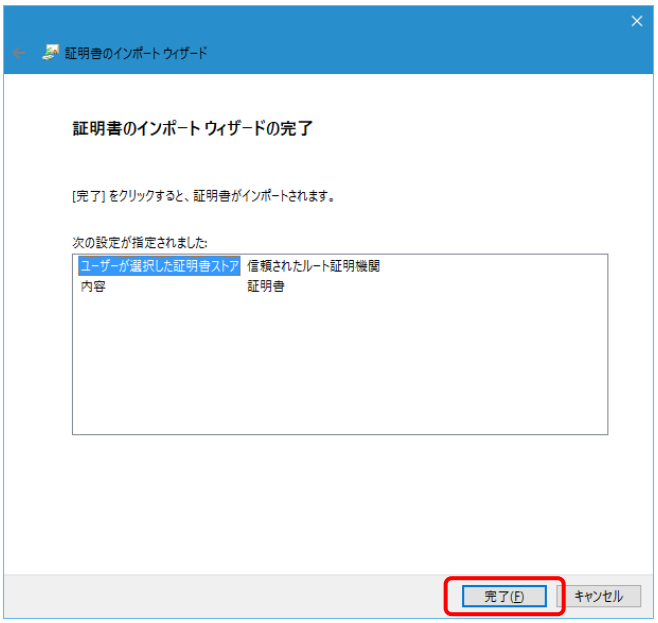
④ “信頼されたルート証明機関”を選択し、「OK」ボタンをクリックします。



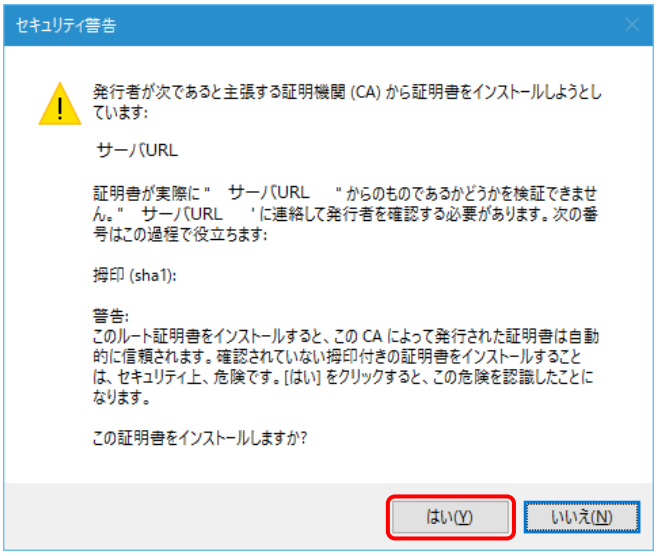
⑤　「次へ」ボタンをクリックします。



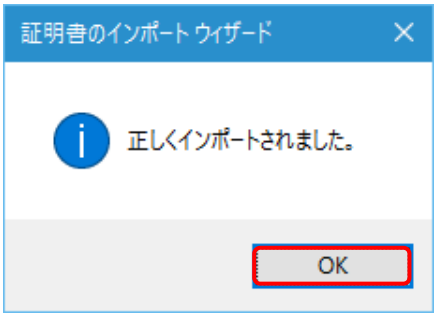
⑥　「完了」ボタンをクリックします。



⑦　「はい」ボタンをクリックします。

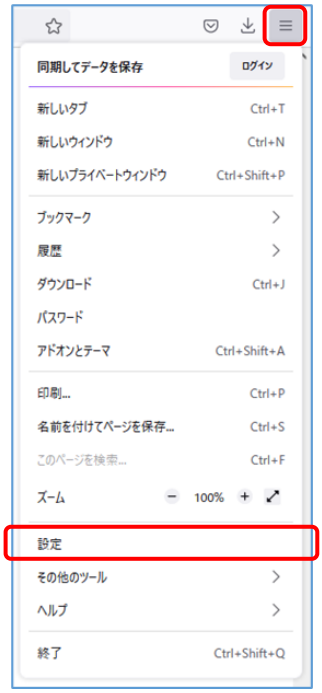


⑧　「OK」ボタンをクリックします。また、「証明書」ダイアログも「OK」ボタンをクリックして閉じてください。

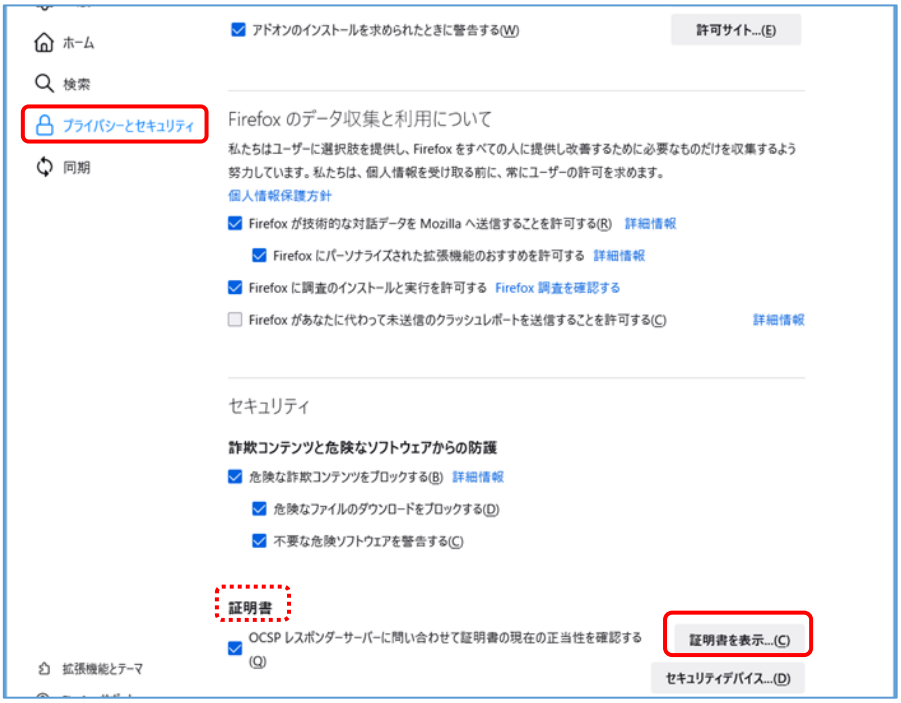


Mozilla Firefox の場合

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

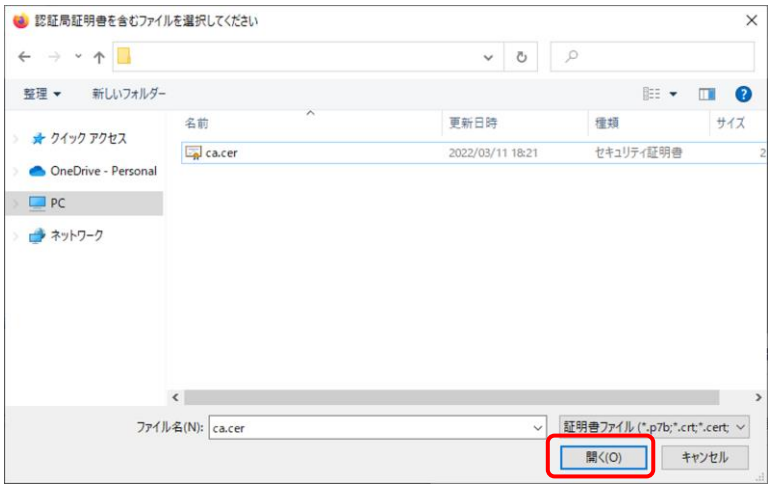


②　「プライバシーとセキュリティ」を選択し、「セキュリティ」から「証明書を表示」をクリックしてください。

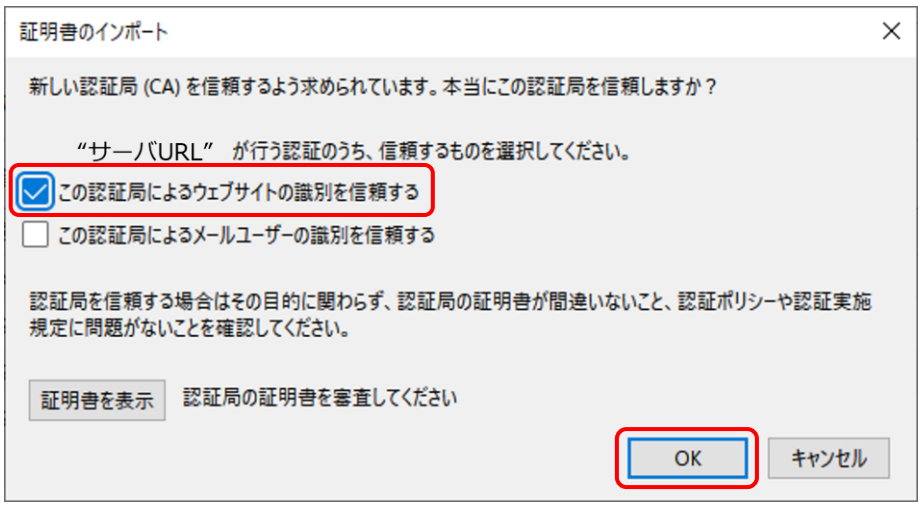


③ 証明書マネージャーのウィンドウが表示され、認証局証明書が選択されていることを確認し、「インポート」をクリックします。

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。

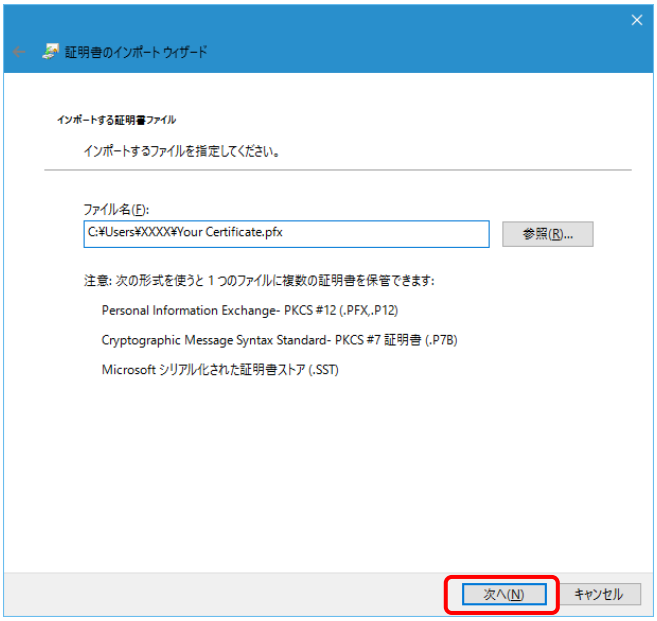


2. クライアント証明書のインポート

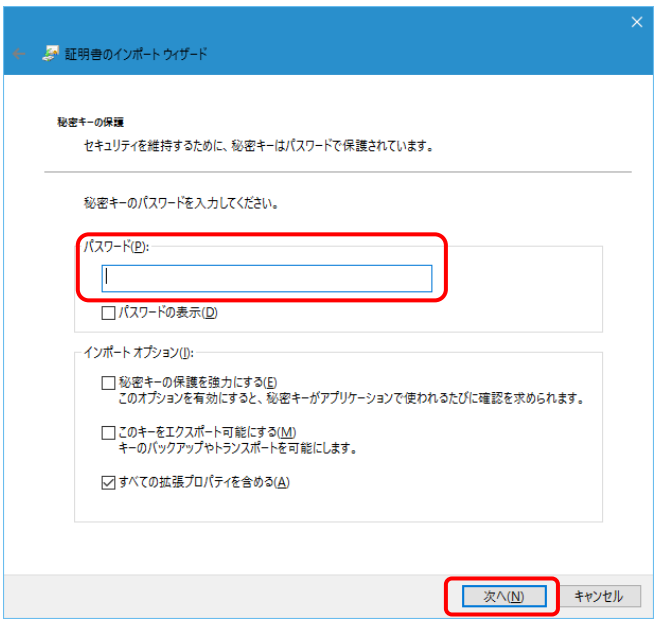
Microsoft Edge/Google Chrome の場合

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。
右のよう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。

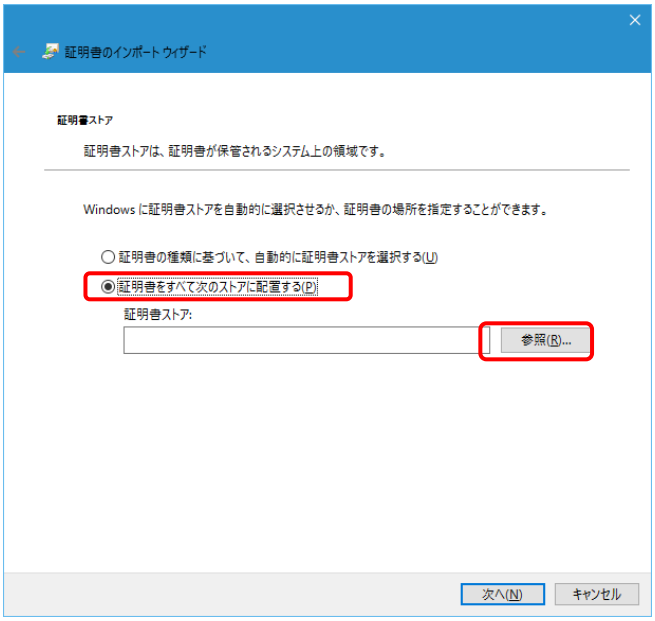
② 「次へ」ボタンをクリックします。



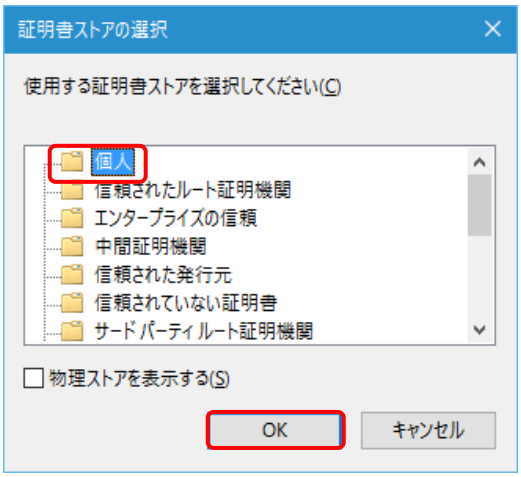
③ 管理者より配布された「クライアントデジタル証明書パスワード」をパスワード入力欄に入力して、「次へ」ボタンをクリックします。



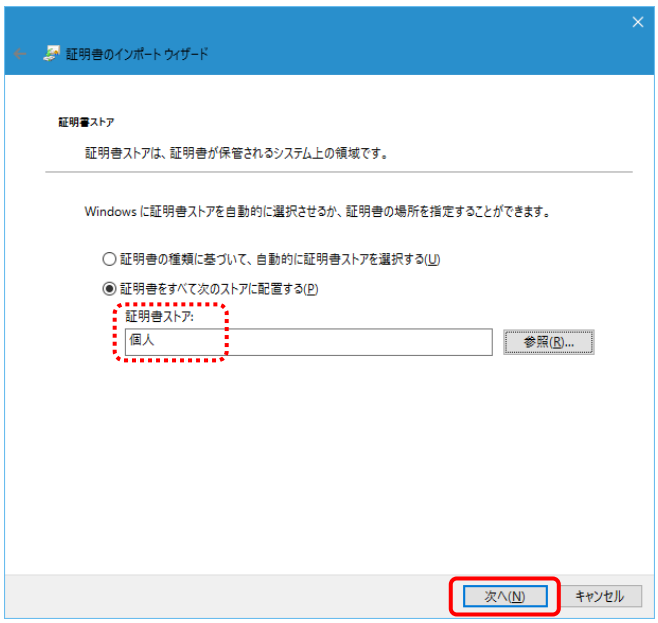
④ “証明書をすべて次のストアに配置する”を選択し、「参照」ボタンをクリックします。



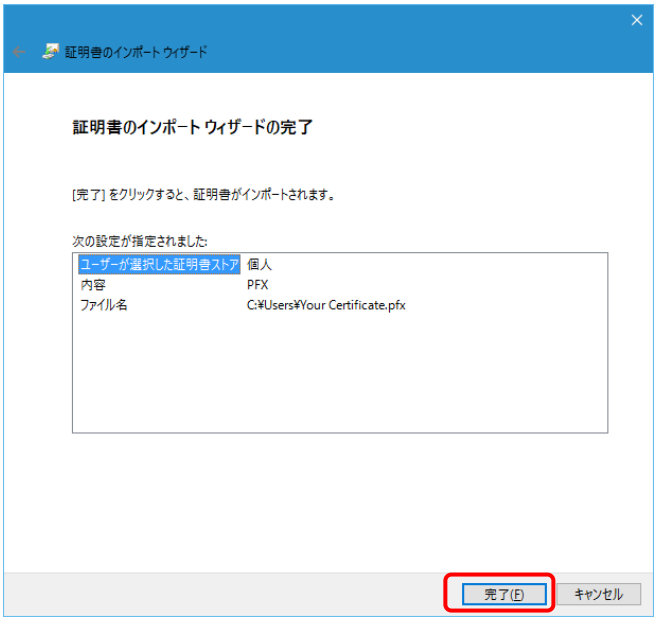
⑤ “個人”を選択し、「OK」ボタンをクリックします。



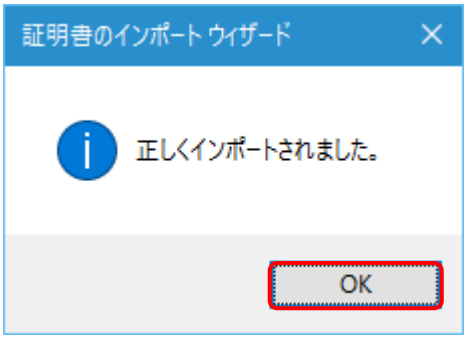
⑥　「次へ」ボタンをクリックします。



⑦　「完了」ボタンをクリックします。



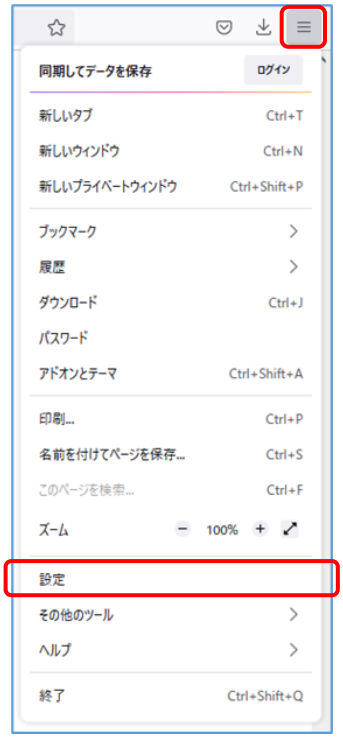
⑧　「OK」ボタンをクリックします。また、「証明書」ダイアログも「OK」ボタンをクリックして閉じてください。



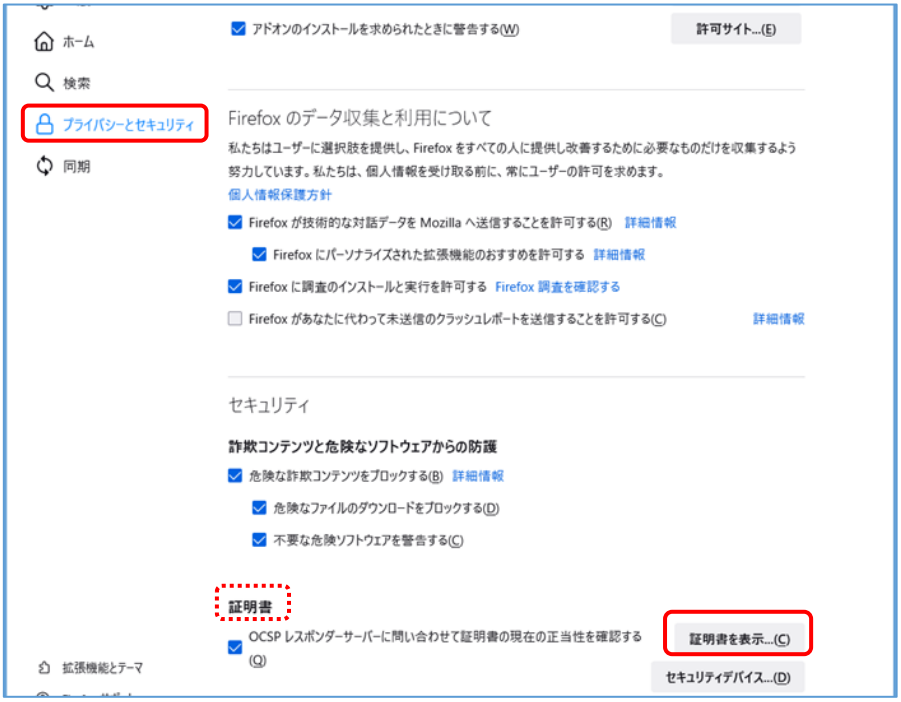
Mozilla Firefox の場合

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。

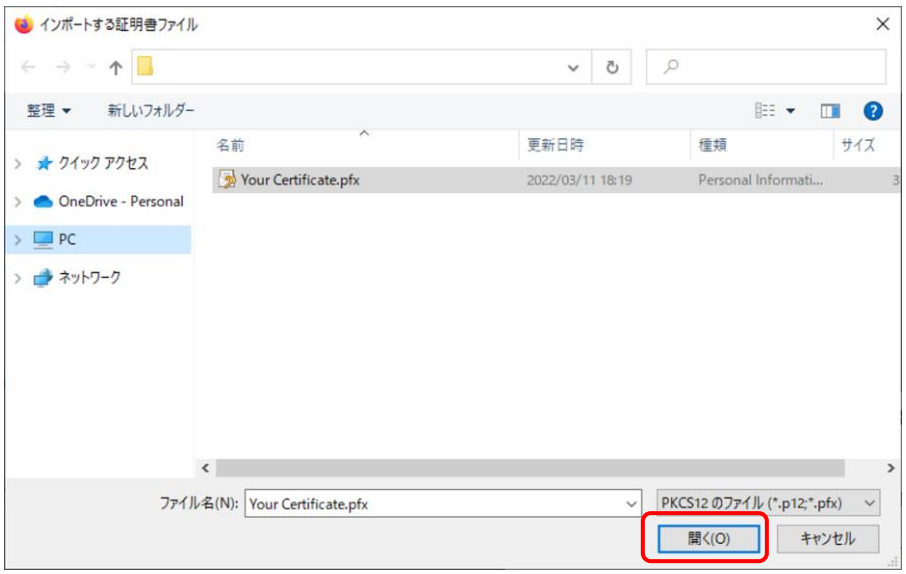


③ 「プライバシーとセキュリティ」を選択し、「セキュリティ」から「証明書を表示」をクリックしてください。



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. リモートコントロール開始

ブラウザ（Microsoft Edge/Google Chrome/Mozilla Firefox が使用できます）を起動して、アドレスバーに DoMobile サーバの URL（ポータルサイト）（注*1）を入力しアクセスします。

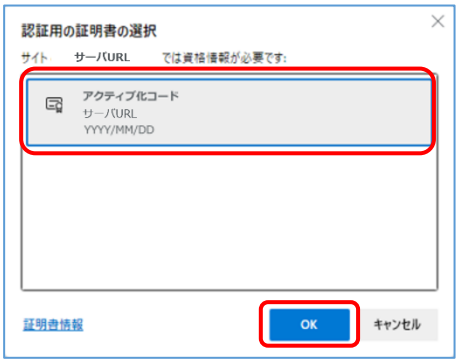
注）*1：
URL については、サポートサービスセンタから展開されるアカウント発行メールに記載されている「組織コード」に従い、以下の一覧表の URL をご使用ください。
アカウント発行メールに組織コードの記載がない場合は、「[0]または[S]で始まる場合」の URL をご使用ください。

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

Microsoft Edge の場合

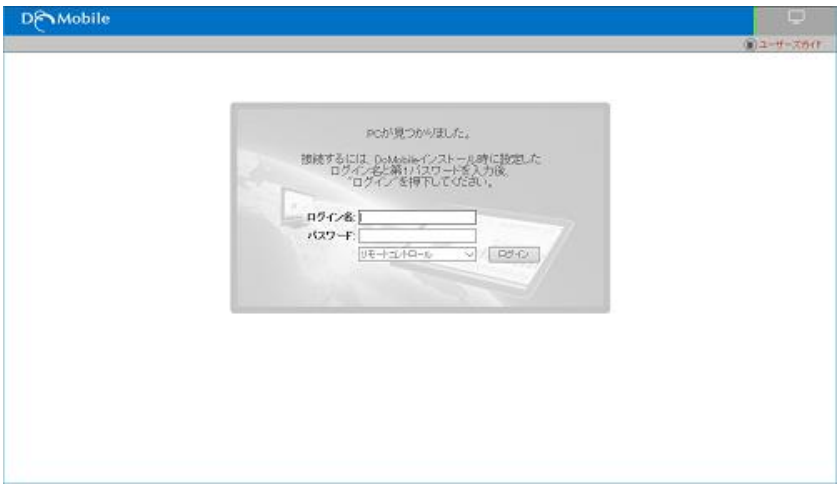
① Microsoft Edge を起動しリモート端末にてポータルサイトの URL を入力して「ENTER」キーを押します。

Microsoft Edge の設定によっては、クライアントデジタル証明書の確認のために証明書の選択画面が表示されます。表示されている証明書から使用する証明書をクリックして選択し、「OK」ボタンをクリックしてください。



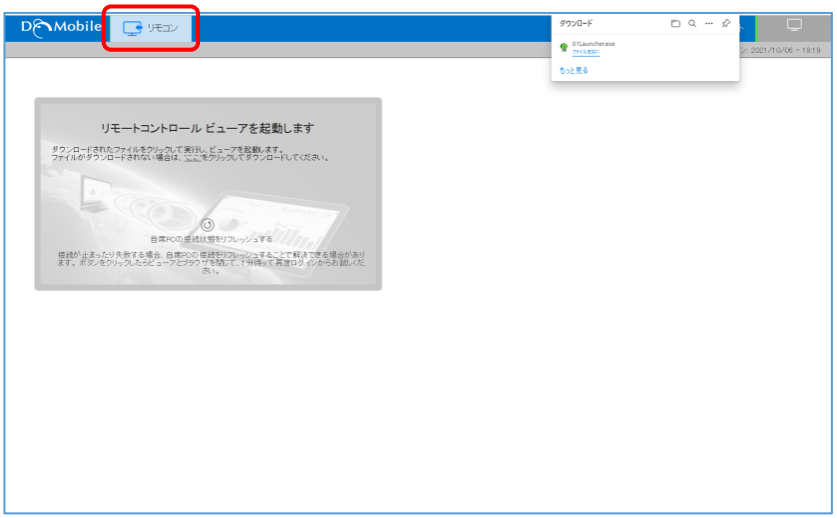
② DoMobile CSE サービスのポータル画面が表示されます。ポータル画面のコンピュータ名入力欄に（DoMobile CSE プログラムインストール時に指定した）コンピュータ名を入力し、「接続」ボタンをクリックします。

③ ログイン情報の入力が要求されますので、ログイン名、第１パスワードを入力して「ログイン」ボタンをクリックします。

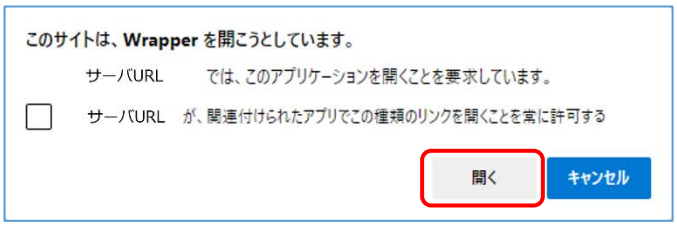


④ ログイン後、「01Launcher.exe」がダウンロードされますので、ダウンロード完了後に画面左上の「リモコン」をクリックします。

ブラウザを閉じずに再度ログインした場合は、⑤のメッセージが表示されます。



⑤ 右のようなメッセージが表示されますので「開く」ボタンをクリックします。

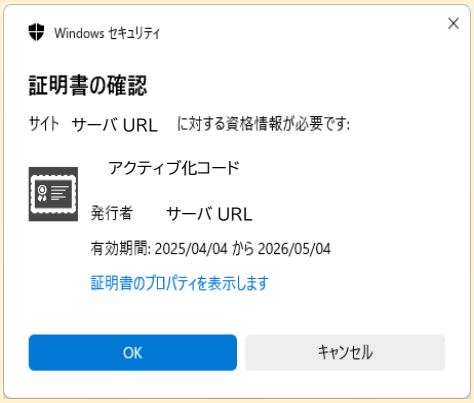


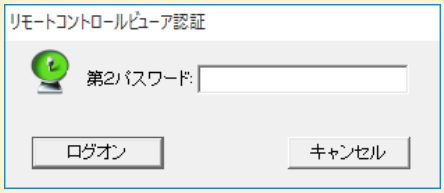
⑥ 「ユーザーアカウント制御」ダイアログが表示されます。リモート PC にログインしている Windows のユーザーアカウントが管理者ユーザか、標準ユーザかによって以下の操作を行います。

・管理者ユーザ … 「はい」ボタンをクリック
・標準ユーザ …… 「いいえ」ボタンをクリック

※ 警告が表示される場合があります。その場合は「はい」または「許可」ボタンをクリックしてください。

⑦ リモートコントロールの第 2 パスワード入力画面が表示される際、再度、証明書の選択画面が表示されます。接続に使用する証明書を選択し、「OK」ボタンをクリックしてください。





上記リモートコントロール時の証明書認証につきましては、証明書選択画面が表示されますが、自席プログラムの過去バージョンとの互換性を保つため、認証機能は一時的に無効化されております。
そのため、証明書選択の操作にかかわらず、従来通り第 2 パスワードによる認証のみ実行されます。
（セキュリティレベルは現行通りとなります）

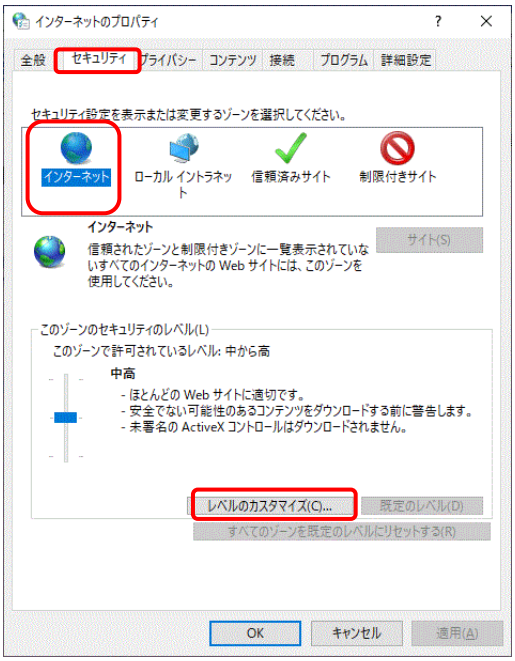
なお、リモートコントロール時の証明書認証の有効化につきましては、2025 年 10 月の Windows 10 サポート終了までに実施の予定です

⑧ 第 2 パスワードを入力してリモートコントロールを開始してください。

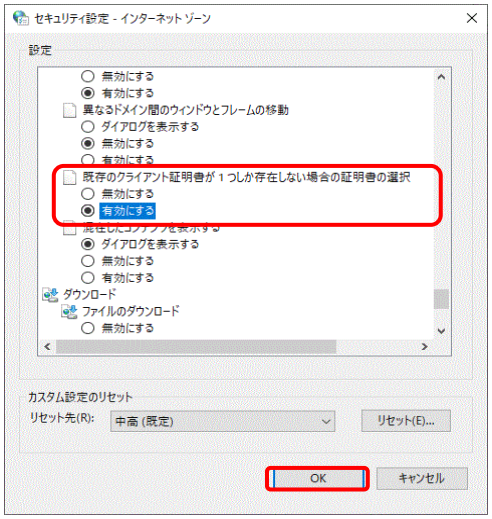
※　⑦の手順を省略したい場合は、以下の設定を行ってください。

以下の設定で、上記の⑥の画面を表示せずにリモートコントロールが行えます。
（クライアント証明書が 1 つのみインポートされている場合に適用されます。）

1. リモート PC の 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. 「セキュリティ」タブの「インターネット」「レベルのカスタマイズ」を開きます。



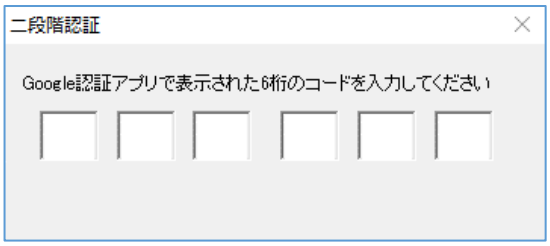
3. 「設定」の項目にある「既存のクライアント証明書が 1 つしか存在しない場合の選択を「有効にする」にチェックオンして「OK」



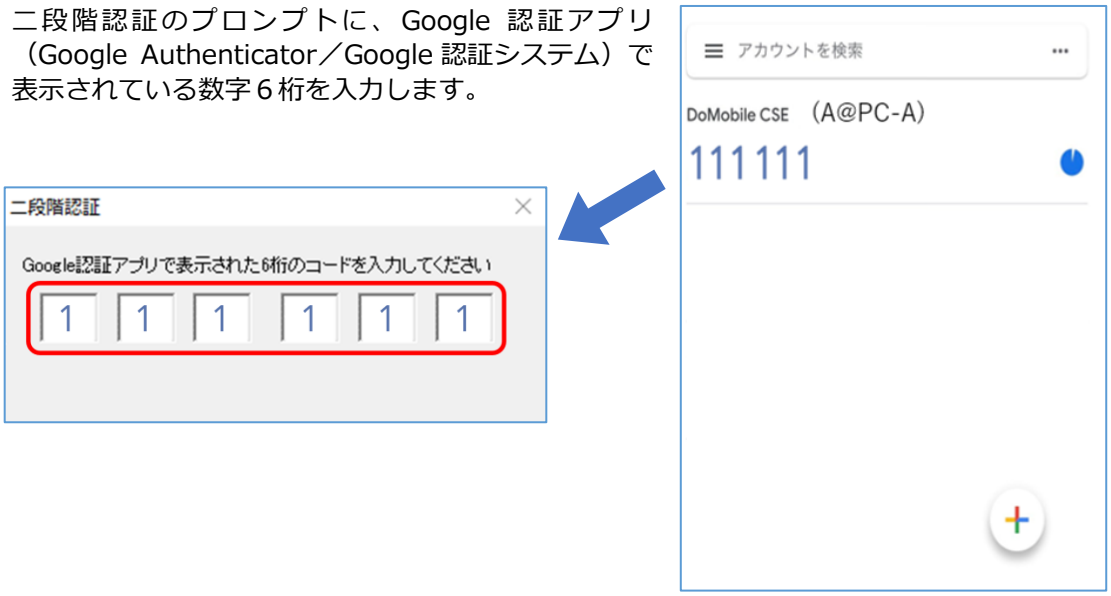
※　「二段階認証」を有効にしている場合

「第２パスワード」入力画面表示後に二段階認証のプロンプトが表示されます。

①　二段階認証のプロンプトが表示されます。



②　二段階認証のプロンプトに、Google 認証アプリ（Google Authenticator／Google 認証システム）で表示されている数字６桁を入力します。



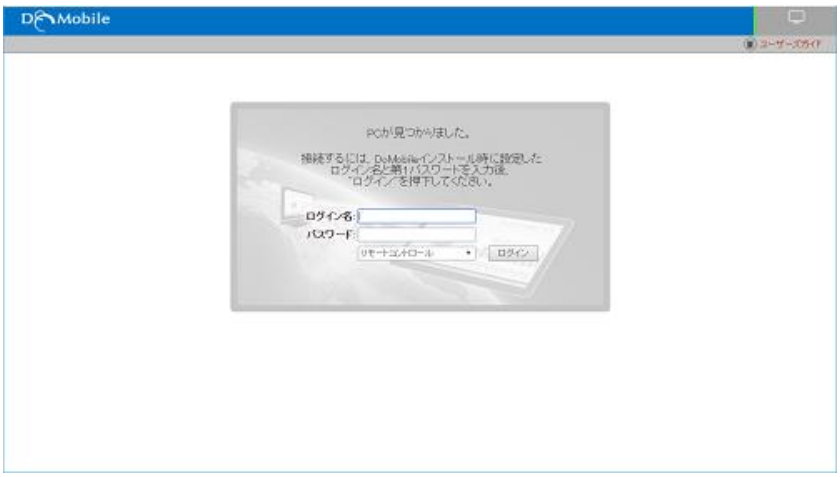
以上の操作で、自席 PC の画面がリモート端末に表示され、リモートコントロールができるようになります。
リモートコントロールの使用方法については、②ポータル画面（コンピュータ名入力画面）の「ユーザーズガイド」リンクより参照ください。

Google Chrome の場合

① Google Chrome を起動しリモート端末にてポータルサイトの URL を入力して「ENTER」キーを押します。
Google Chrome の設定によっては、クライアントデジタル証明書の確認のために「証明書の選択」画面が表示されますので「OK」ボタンをクリックしてください。

② DoMobile CSE サービスのポータル画面が表示されます。ポータル画面のコンピュータ名入力欄に（DoMobile CSE プログラムインストール時に指定した）コンピュータ名を入力し、「接続」ボタンをクリックします。

③ ログイン情報の入力が要求されますので、ログイン名、第１パスワードを入力して「ログイン」ボタンをクリックします。



④ ログイン後、「01Launcher.exe」がダウンロードされますので、ダウンロード完了後に画面左上の「リモコン」をクリックします。

ブラウザを閉じずに再度ログインした場合は、⑤のメッセージが表示されます。

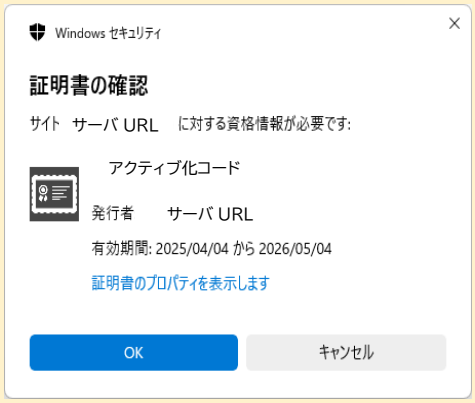
⑤ 右のようなメッセージが表示されますので「Wrapper を開く」ボタンをクリックします。

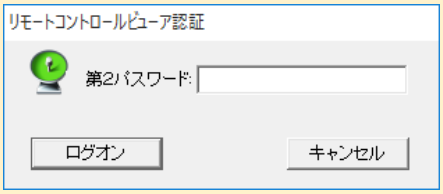
⑥ 「ユーザーアカウント制御」ダイアログが表示されます。リモート PC にログインしている Windows のユーザーアカウントが管理者ユーザか、標準ユーザかによって以下の操作を行います。

・管理者ユーザ … 「はい」ボタンをクリック
・標準ユーザ …… 「いいえ」ボタンをクリック

※ 警告が表示される場合があります。その場合は「はい」または「許可」ボタンをクリックしてください。

⑦ リモートコントロールの第 2 パスワード入力画面が表示される際、再度、証明書の選択画面が表示されます。接続に使用する証明書を選択し、「OK」ボタンをクリックしてください。





上記リモートコントロール時の証明書認証につきましては、証明書選択画面が表示されますが、自席プログラムの過去バージョンとの互換性を保つため、認証機能は一時的に無効化されております。
そのため、証明書選択の操作にかかわらず、従来通り第 2 パスワードによる認証のみ実行されます。
（セキュリティレベルは現行通りとなります）

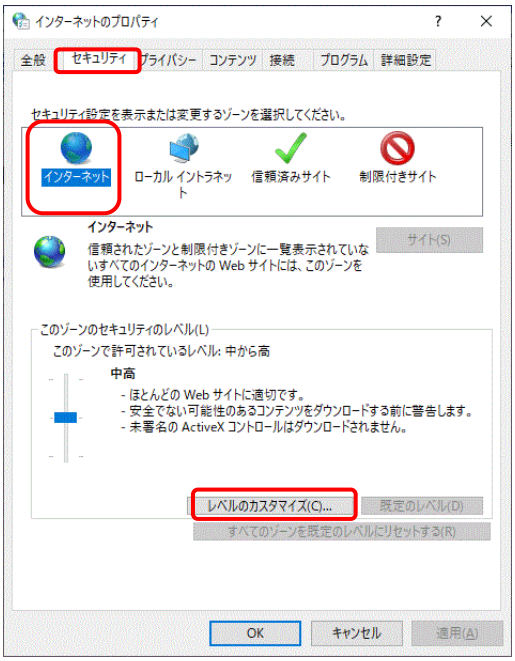
なお、リモートコントロール時の証明書認証の有効化につきましては、2025 年 10 月の Windows 10 サポート終了までに実施の予定です

⑧ 第 2 パスワードを入力してリモートコントロールを開始してください。

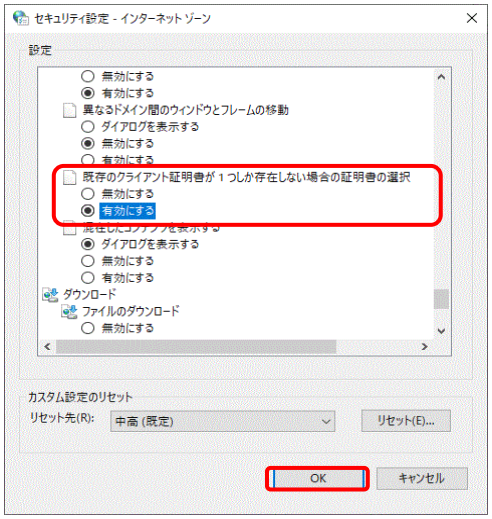
※　⑦の手順を省略したい場合は、以下の設定を行ってください。

以下の設定で、上記の⑥の画面を表示せずにリモートコントロールが行えます。
（クライアント証明書が 1 つのみインポートされている場合に適用されます。）

1. リモート PC の 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. 「セキュリティ」タブの「インターネット」「レベルのカスタマイズ」を開きます。



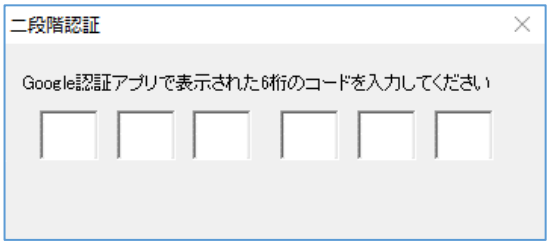
3. 「設定」の項目にある「既存のクライアント証明書が 1 つしか存在しない場合の選択を「有効にする」にチェックオンして「OK」



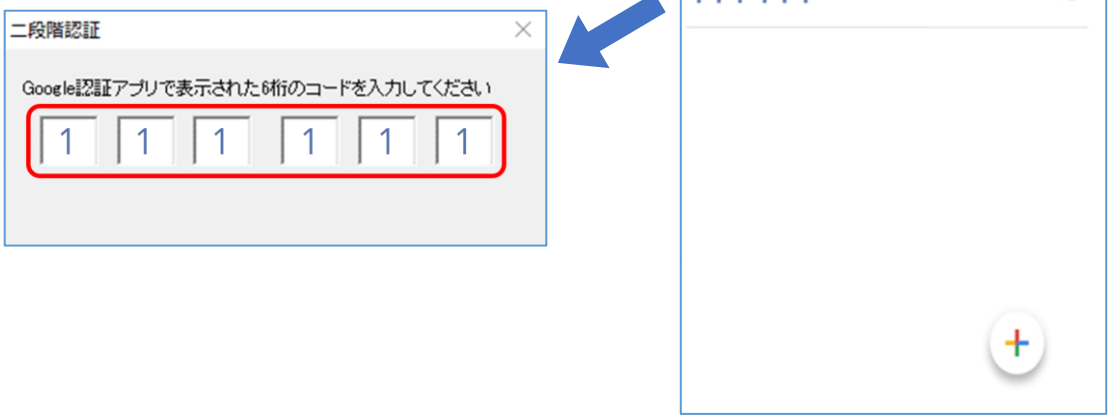
※ 「二段階認証」を有効にしている場合

「第２パスワード」入力画面表示後に二段階認証のプロンプトが表示されます。

① 二段階認証のプロンプトが表示されます。



② 二段階認証のプロンプトに、Google 認証アプリ（Google Authenticator／Google 認証システム）で表示されている数字６桁を入力します。



以上の操作で、自席 PC の画面がリモート端末に表示され、リモートコントロールができるようになります。
リモートコントロールの使用方法については、②ポータル画面（コンピュータ名入力画面）の「ユーザーズガイド」リンクより参照ください。

Mozilla Firefox の場合

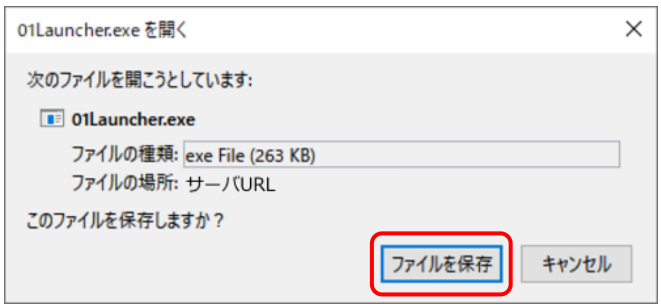
① Mozilla Firefox を起動しリモート端末にてポータルサイトの URL を入力して「ENTER」キーを押します。
Mozilla Firefox の設定によっては、クライアントデジタル証明書の確認のために「個人証明書の要求」画面が表示されますので「OK」ボタンをクリックしてください。

② DoMobile CSE サービスのポータル画面が表示されます。ポータル画面のコンピュータ名入力欄に（DoMobile CSE プログラムインストール時に指定した）コンピュータ名を入力し、「接続」ボタンをクリックします。

③ ログイン情報の入力が要求されますので、ログイン名、第１パスワードを入力して「ログイン」ボタンをクリックします。

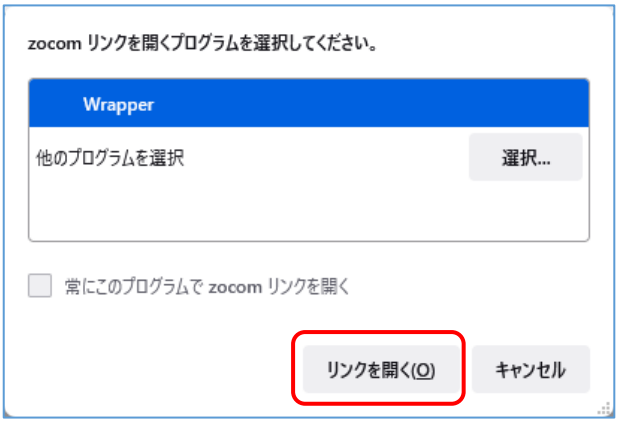
ブラウザを閉じずに再度ログインした場合は、ログイン後、⑥の画面に遷移します。

④ 画面に右のようなメッセージが表示されますので、「ファイルを保存」をクリックします。



⑤ 画面左上の「リモコン」をクリックします。

⑥ 右のようなメッセージが表示されますので「リンクを開く」ボタンをクリックします。

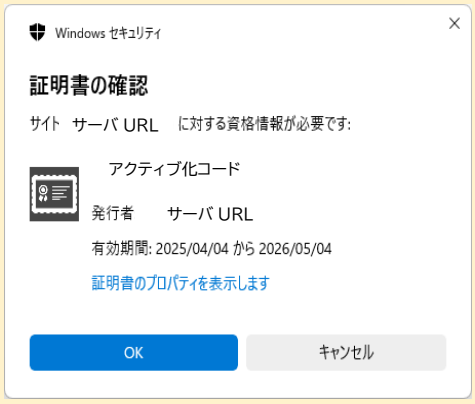


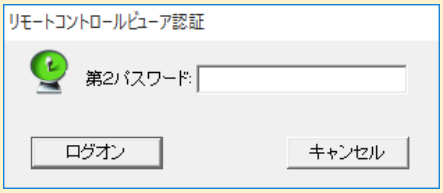
⑦ 「ユーザーアカウント制御」ダイアログが表示されます。リモート PC にログインしている Windows のユーザーアカウントが管理者ユーザか、標準ユーザかによって以下の操作を行います。

・管理者ユーザ … 「はい」ボタンをクリック
・標準ユーザ …… 「いいえ」ボタンをクリック

※ 警告が表示される場合があります。その場合は「はい」または「許可」ボタンをクリックしてください。

⑧ リモートコントロールの第 2 パスワード入力画面が表示される際、再度、証明書の選択画面が表示されます。接続に使用する証明書を選択し、「OK」ボタンをクリックしてください。





上記リモートコントロール時の証明書認証につきましては、証明書選択画面が表示されますが、自席プログラムの過去バージョンとの互換性を保つため、認証機能は一時的に無効化されております。
そのため、証明書選択の操作にかかわらず、従来通り第 2 パスワードによる認証のみ実行されます。
（セキュリティレベルは現行通りとなります）

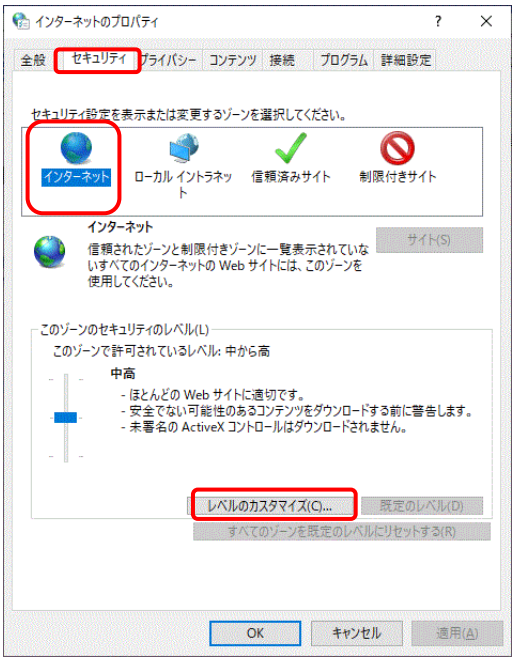
なお、リモートコントロール時の証明書認証の有効化につきましては、2025 年 10 月の Windows 10 サポート終了までに実施の予定です

⑨ 第 2 パスワードを入力してリモートコントロールを開始してください。

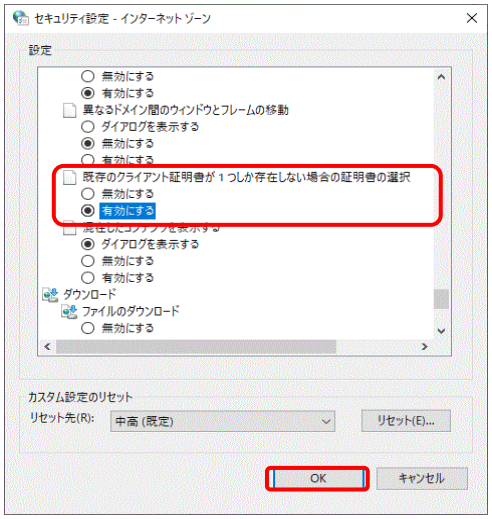
※　⑧の手順を省略したい場合は、以下の設定を行ってください。

以下の設定で、上記の⑥の画面を表示せずにリモートコントロールが行えます。
（クライアント証明書が 1 つのみインポートされている場合に適用されます。）

1. リモート PC の 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. 「セキュリティ」タブの「インターネット」「レベルのカスタマイズ」を開きます。



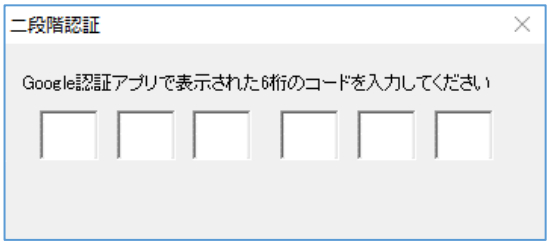
3. 「設定」の項目にある「既存のクライアント証明書が 1 つしか存在しない場合の選択を「有効にする」にチェックオンして「OK」



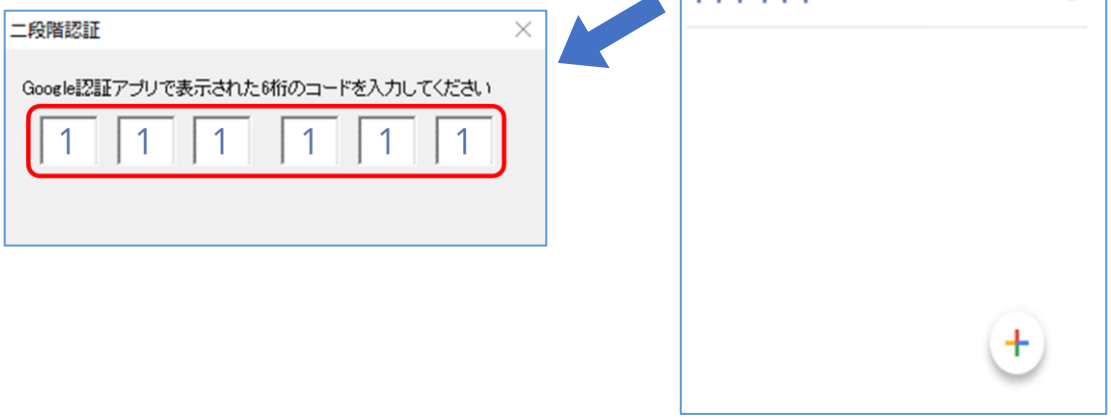
※ 「二段階認証」を有効にしている場合

「第２パスワード」入力画面表示後に二段階認証のプロンプトが表示されます。

① 二段階認証のプロンプトが表示されます。



② 二段階認証のプロンプトに、Google 認証アプリ（Google Authenticator／Google 認証システム）で表示されている数字６桁を入力します。



以上の操作で、自席 PC の画面がリモート端末に表示され、リモートコントロールができるようになります。
リモートコントロールの使用方法については、②ポータル画面（コンピュータ名入力画面）の「ユーザーズガイド」リンクより参照ください。

4. リモートコントロール終了

① リモートコントロールビューア上部のツールバーの「×」アイコンをクリックし、セッションを切断します。

② 「はい」ボタンをクリックします。

③ ブラウザの画面右上の「ログアウト」をクリックし、接続を終了します。

【注意】

リモートコントロールで自席 PC のシャットダウンを行う際は、以下の「リモートシャットダウン用ショートカットご利用方法」にてご案内しております、シャットダウン用ショートカットを利用してのシャットダウンを実行してください。

「リモートシャットダウン用ショートカットご利用方法」
https://www.hitachi-solutions-create.co.jp/solution/domobile_asp/pdf/hostpc_shut_man.pdf

※ リモートシャットダウン用ショートカットを利用せずにシャットダウンし、強制シャットダウンの確認画面でキャンセルを選択した場合、リモートコントロールビューアの操作が行えない状態となります。この場合、「接続状態リフレッシュ」機能をご利用ください。

※ 「接続状態リフレッシュ」機能について（リモート PC のみ）

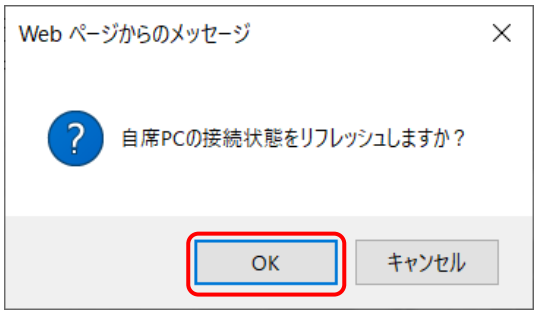
・リモートコントロール接続時、画面が真っ黒になり操作を行えない場合
・初期画面ロード中のまま先に進まない場合
・「他のユーザが使用中です」のメッセージが表示される場合

上記のような状況が繰り返し発生した場合に「接続状態リフレッシュ」機能が有効です。

① リモートコントロールビューアを起動している場合は、ビューア左上の×をクリックし、ビューアを閉じてください。

② ログイン情報入力後の画面から「自席 PC の接続状態をリフレッシュする」の上部にあるアイコンをクリックします。

③ 右のポップアップが表示されますので、[OK]ボタンをクリックします。

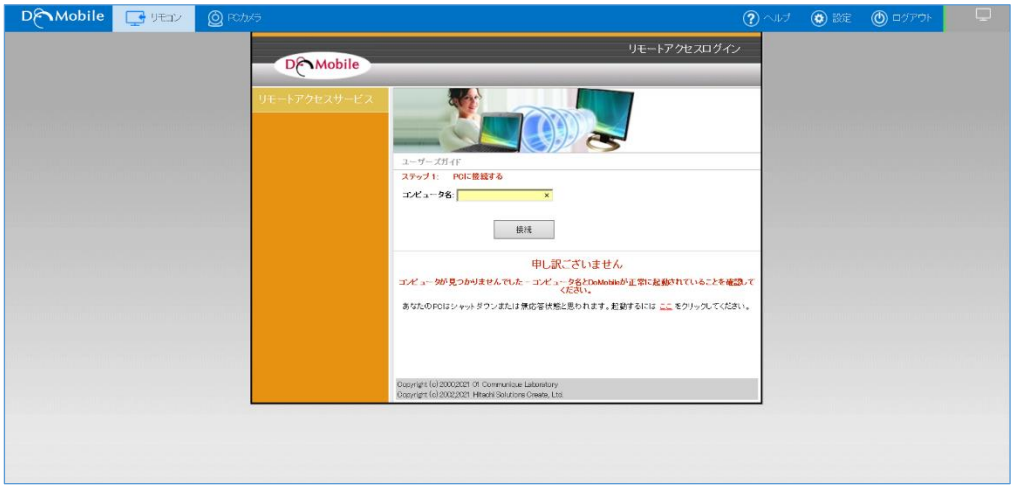


④ 一度、ブラウザを閉じて 1 分程待ちます。

⑤ 再度ブラウザを立ち上げ、ログイン画面にアクセス。以降は通常通りにリモートコントロールを行ってください。

【注意】

接続状態リフレッシュを実行後に以下のような画面になる場合ありますが、こちらの画面からログインは行わず、必ず一度ブラウザを立ち上げなおしてからログインを行ってください。



※ 接続状態リフレッシュはリモート端末が PC の時のみご利用可能な機能です。

※ 接続状態リフレッシュはリモートコントロール時に「DoMobile プログラム」を再起動する機能です。**これによって自席 PC のシャットダウン・再起動が行われることはございません。**

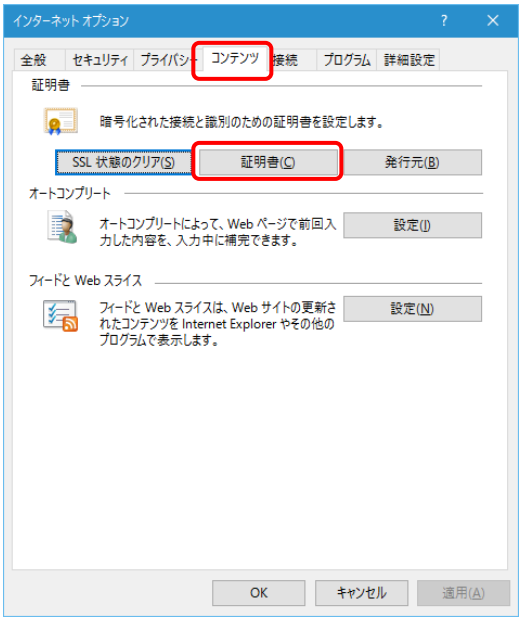
※ セッションファイルがロックして処理が続行できないような場合に、自動で DoMobile のサービスの再起動が行われます。再起動が実行された場合、リモートアクセスは切断されますので、ブラウザを閉じて、再度接続を実行しなおしてご利用ください。

5. 証明書の削除

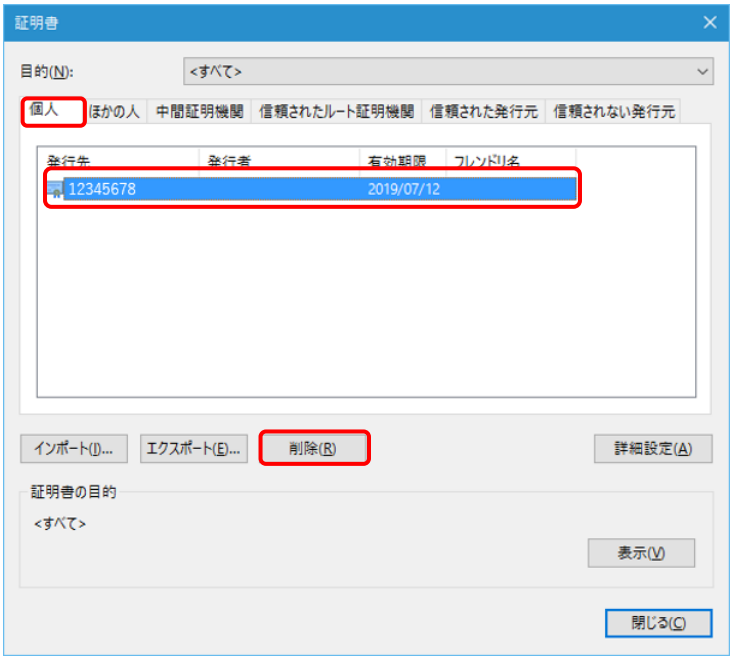
Microsoft Edge/Google Chrome の場合

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。

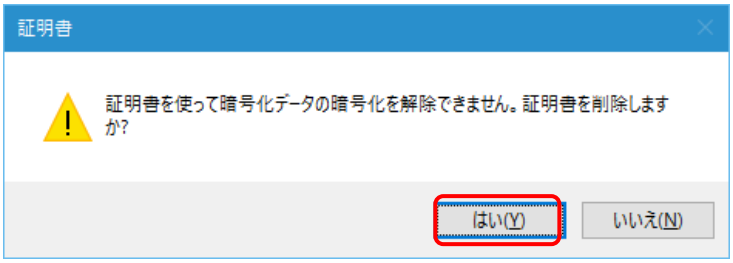
② 「インターネット オプション」が表示されましたら、「コンテンツ」タブの「証明書」ボタンをクリックします。



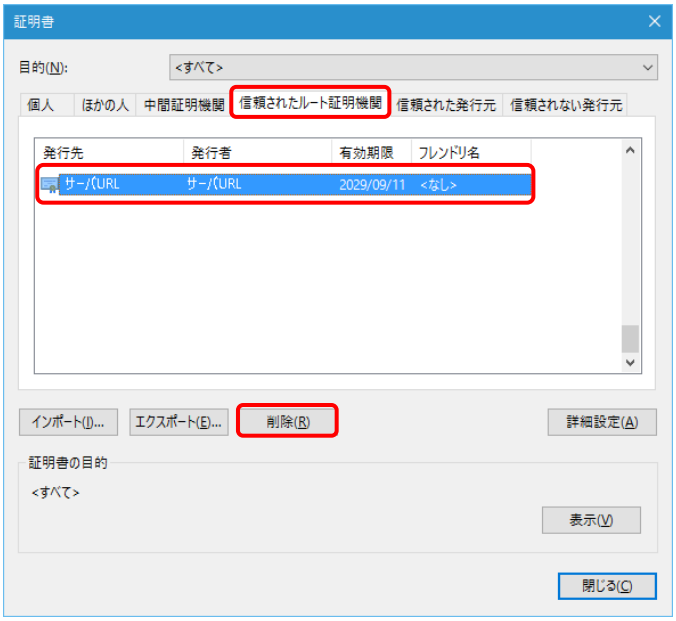
③ 「証明書」が表示されましたら、「個人」タブの該当するクライアントデジタル証明書（発行先にアクティブ化コードが表示）を選択し、「削除」ボタンをクリックします。



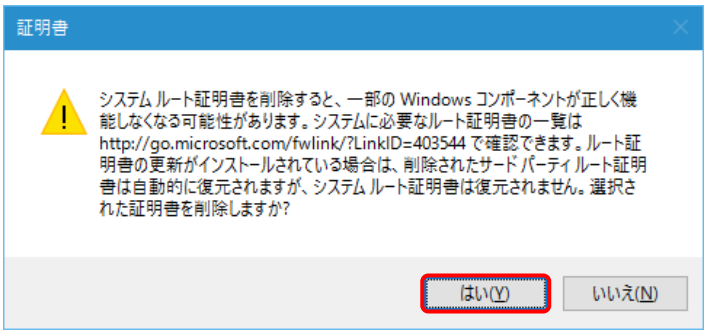
④ 確認ダイアログが表示されますので、「はい」ボタンをクリックします。



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。



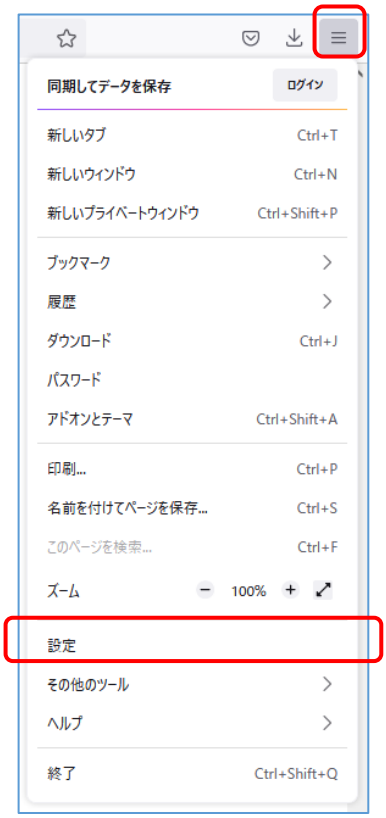
⑥ 確認のための「証明書」ダイアログが表示されますので、「はい」ボタンをクリックします。



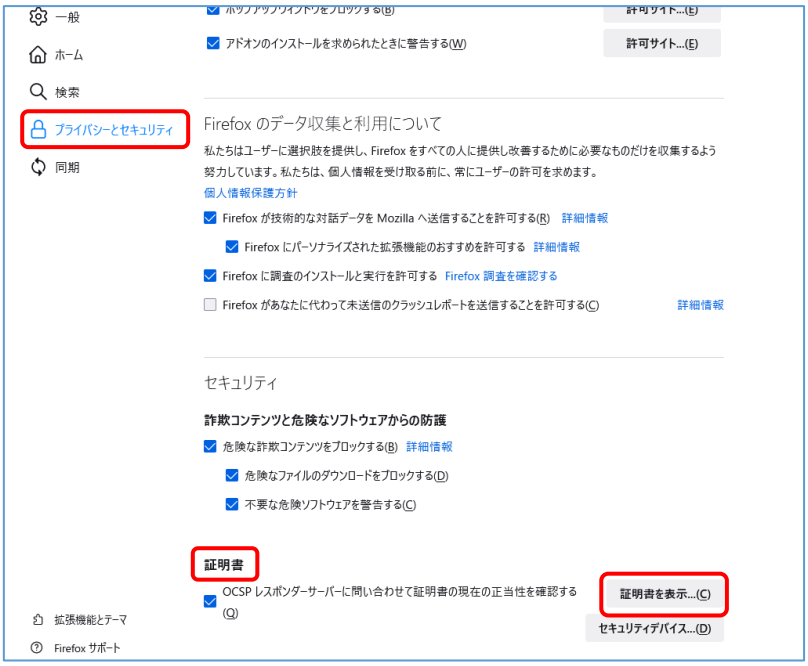
⑦ さらに、確認のための「ルート証明書ストア」ダイアログが表示されますので、「はい」ボタンをクリックします。

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。

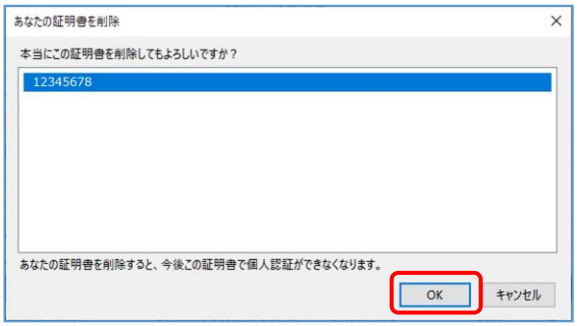


② 「プライバシーとセキュリティ」の「証明書」から「証明書を表示」をクリックします。

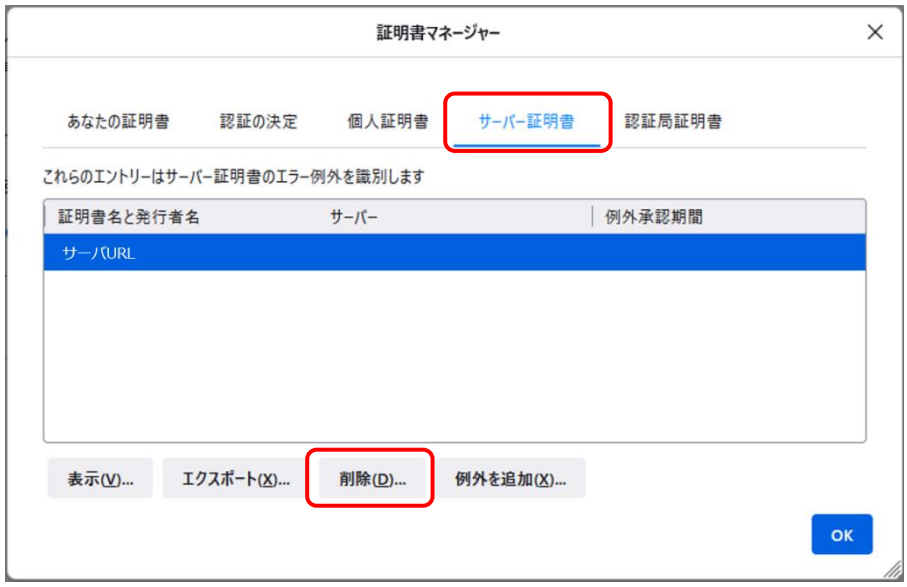


③　「あなたの証明書」タブの該当するクライアント証明書を選択し、「削除」ボタンをクリックします。

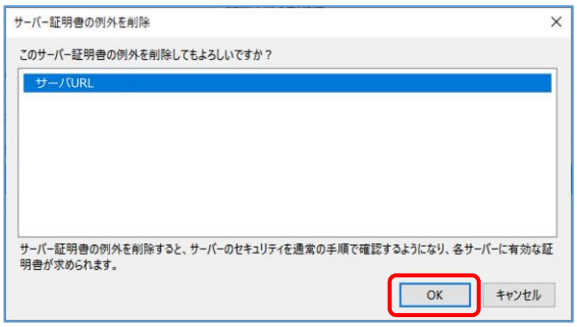
④　表示されたウィンドウの「OK」ボタンをクリックします。



⑤　「サーバー証明書」の CA 証明書を選択し「削除」ボタンをクリックします。



⑥　表示されたウィンドウの「OK」ボタンをクリックします。



■お問い合わせ

本件に関するお問い合わせは、メールにて承っております。
サポートサービスセンタ：hsc-asp_support@mlc.hitachi-solutions.com

◆◇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

以上