

1 認証局の電子証明書をダウンロードする

電子証明書の取得

電子証明書をダウンロードサイトよりダウンロードします。
お手元に電子証明書発行通知書の「電子証明書取得に関する情報」をご用意願います。
電子証明書のダウンロード可能期間は、発行後180日以内ですので、ご注意願います。

電子証明書発行通知書の「電子証明書取得に関する情報」（サンプル）

発行者	Online Billing NW Common Root CA - G1
発行先	※医療機関コード
端末名称等	※申請時に登録した端末名称等
リクエストID	20210121xxxxxx
リファレンスID	XXXXXXXXXX
電子証明書有効期間	YYYY/MM/DD ~ YYYY/MM/DD
ダウンロードサイト有効期限	YYYY/MM/DD

- 1 オンライン請求端末よりダウンロードサイトにアクセスします。
「オンライン請求システムのログイン画面」または「オンライン請求システム専用認証局電子証明書ダウンロードサイト」の下部にある「**電子証明書ダウンロードサイト（専用のID、パスワードが必要です。）**」をクリックします。

- 2 電子証明書発行通知書の「電子証明書取得に関する情報」に記載のリクエストIDとリファレンスID及び任意のパスワード（半角数字4桁）を入力し、「**ダウンロード**」をクリックします。

注意

入力した証明書パスワードは、「2 認証局の電子証明書をインストールする」の④で使用します。
設定したパスワードを忘れないようにしてください。

- 3 【▼】をクリックし、「名前をつけて保存」をクリックし、任意の場所に保存します。

- 4 電子証明書がダウンロードできていることを確認します。

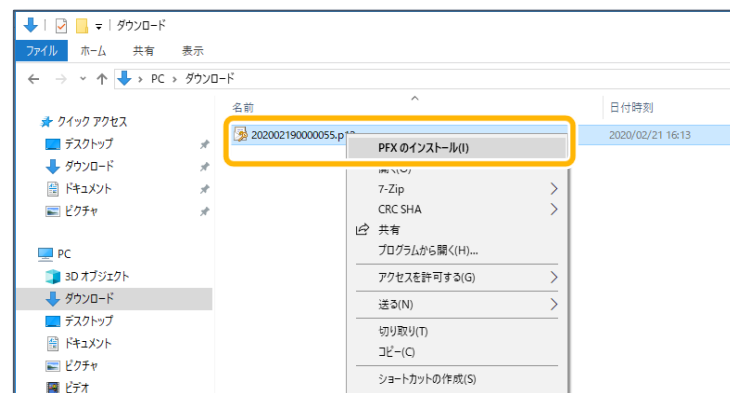
2 認証局の電子証明書をインストールする

01 セットアップ

電子証明書をオンライン請求端末または資格確認端末にセットアップします。

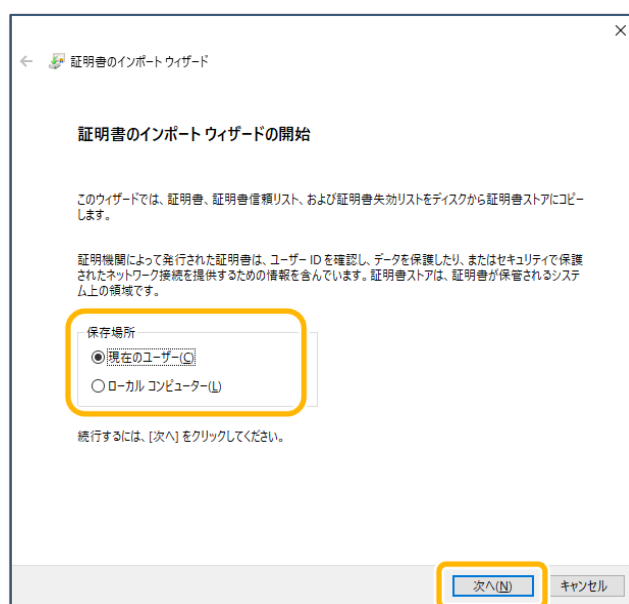
- 1 電子証明書ダウンロードサイトより取得した電子証明書ファイルが保存されているフォルダを開きます。

電子証明書ファイルを右クリックし、表示されたメニューから**PFXのインストール**をクリックします。



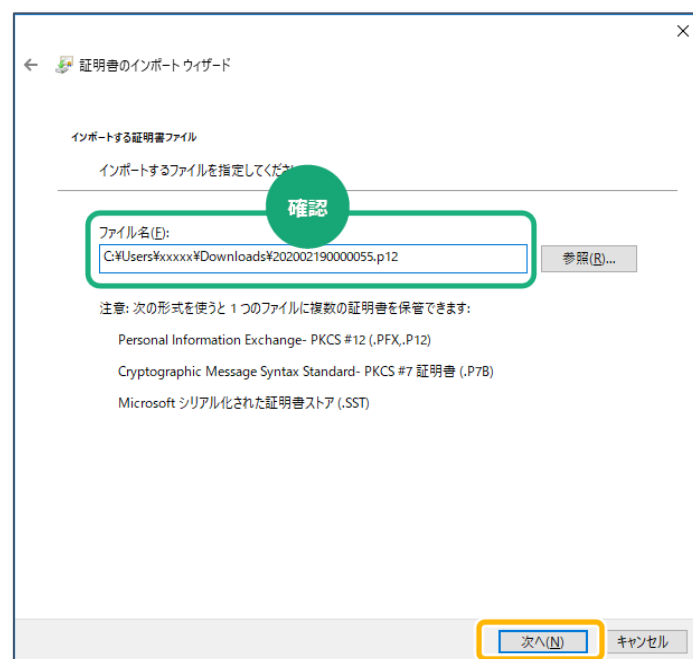
- 2 「証明書のインポートウィザード」が表示されます。

保存場所は**現在のユーザー**を選択し、**次へ**をクリックします。



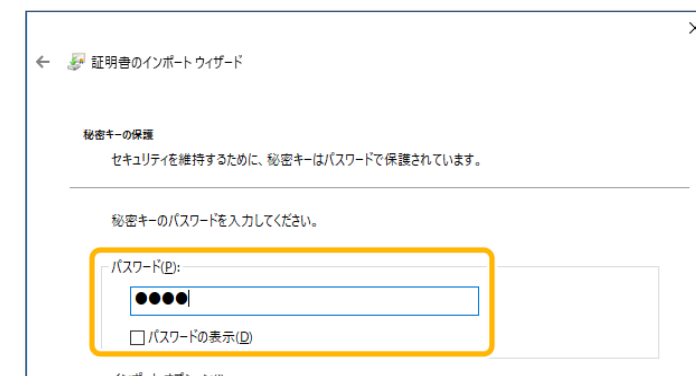
- 3 「インポートする証明書ファイル」が表示されます。

ファイル名に電子証明書のファイル名が表示されていることを確認し、**次へ**をクリックします。



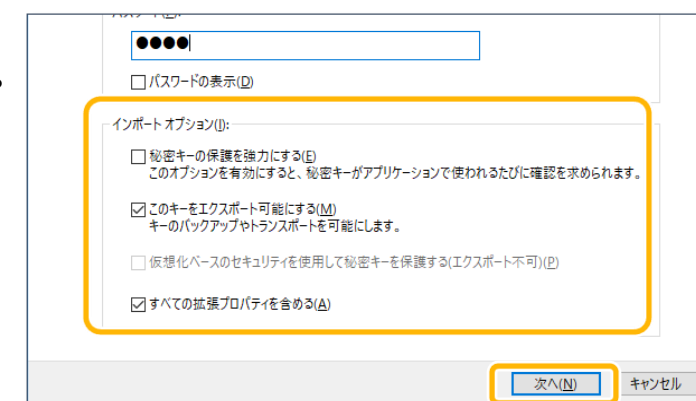
- 4 「秘密キーの保護」が表示されます。

パスワードに電子証明書ダウンロード時に設定した証明書パスワードを入力します。



- 5 **インポートオプション**について、以下の内容を設定します。設定後、**次へ**をクリックします。

- 秘密キーの保護を強力にする
：チェックをしない
- このキーをエクスポート可能にする
：チェックをする
- すべての拡張プロパティを含める
：チェックをする



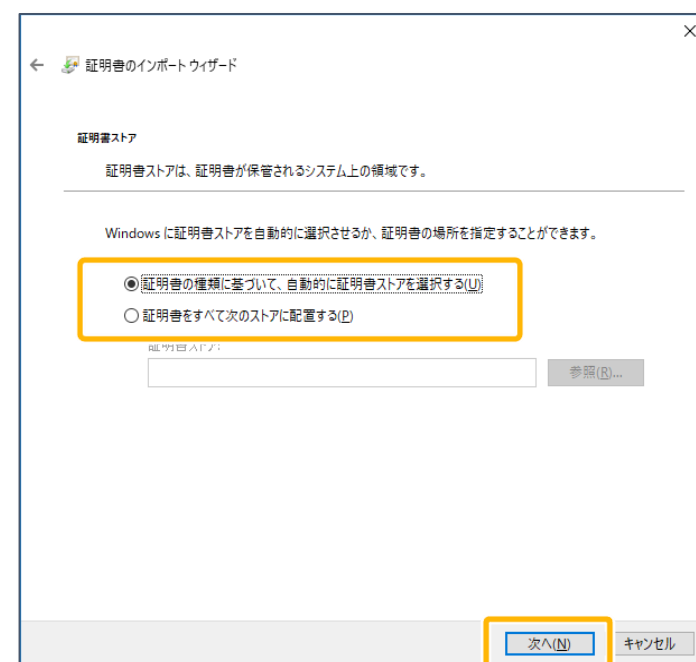
💡 こんなときは！

秘密キーの保護を強力にするのチェックが外せない場合

セキュリティを強化する設定がされているため、**オンライン請求ネットワーク関連システム共通認証局ユーザーマニュアル(オンライン請求ネットワーク関連システム Windows IE)1.1.0版のPage 10 「1.2.1 こんなときは！」**を参照し、パスワードを設定します。

- 6 証明書ストアが表示されます。

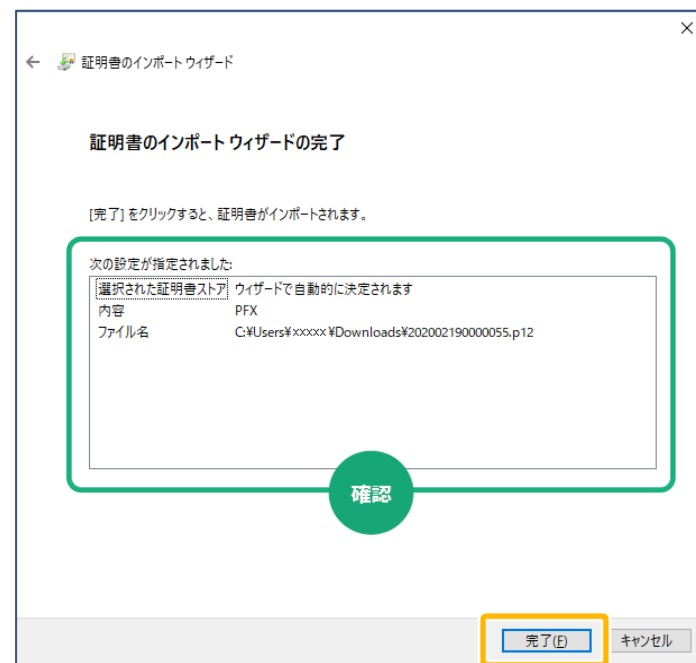
証明書の種類に基づいて、自動的に証明書ストアを選択するを選択し、**次へ**をクリックします。



2 認証局の電子証明書をインストールする（つづき）

- 7 「証明書のインポートウィザードの完了」が表示されます。

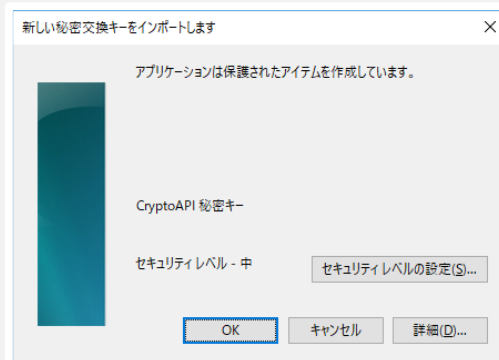
電子証明書のファイル名等を確認し、完了をクリックします。



💡 こんなときは！

「新しい秘密交換キーをインポートします」が表示された場合

既存のオン請求端末などをセットアップした場合、右図の画面が表示されることがあります。
この場合は、**オンライン請求ネットワーク関連システム共通認証局ユーザーマニュアル(オンライン請求ネットワーク関連システムWindows IE)1.1.0版のPage 10「1.2.1 こんなときは！」**を参照してください。



- 8 セキュリティ警告が表示されます。

※本画面が表示されず正しくインポートされました画面が表示された場合は、次に進んでください。

Windowsの信頼されたルート証明機関に証明書発行者（認証局）の証明書を登録するため、**はい** をクリックします。

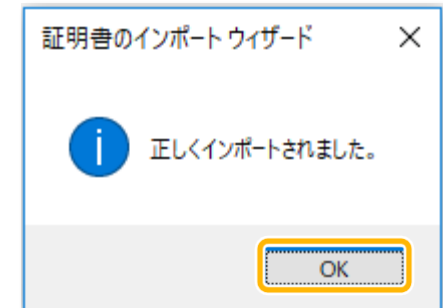


注意

いいえ をクリックした場合は、インストール中止となり、電子証明書がセットアップされません。電子証明書のインストールを再度実施する必要があります（P.2の ①に戻り、再セットアップしてください。）。

- 9 「正しくインポートされました」が表示されます。

OKをクリックします。

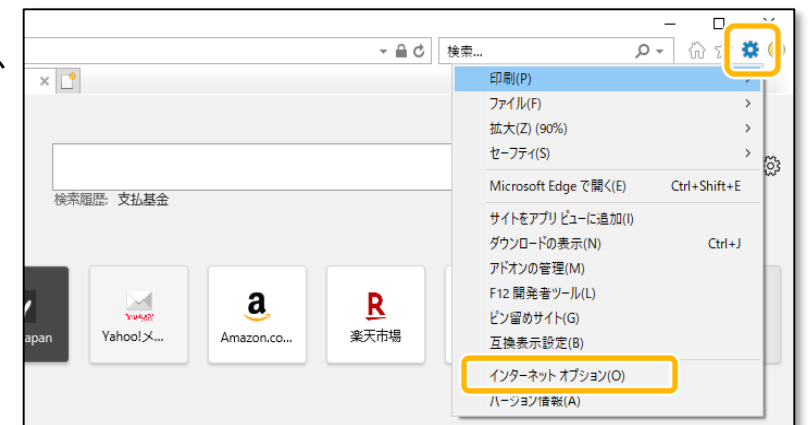


02 セットアップ結果の確認

電子証明書が、ブラウザに正しく登録されたかを確認します。

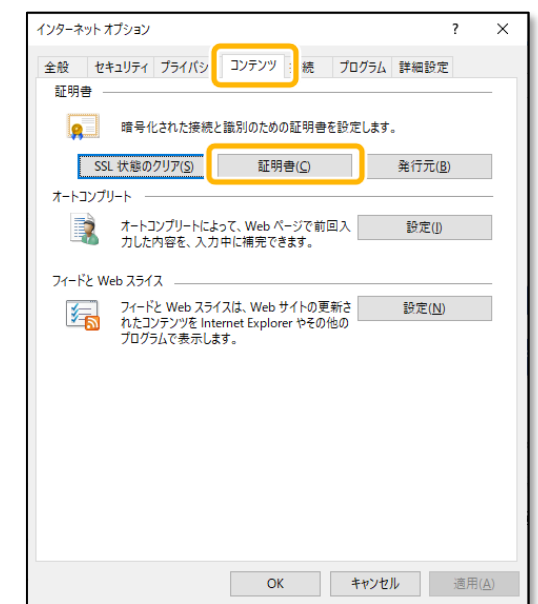
- 1 Internet Explorerを起動し、（ツール）をクリックします。

表示されたメニューから**インターネットオプション**をクリックします。



- 2 「インターネットオプション」が表示されます。

コンテンツタブを選択し、**証明書**をクリックします。



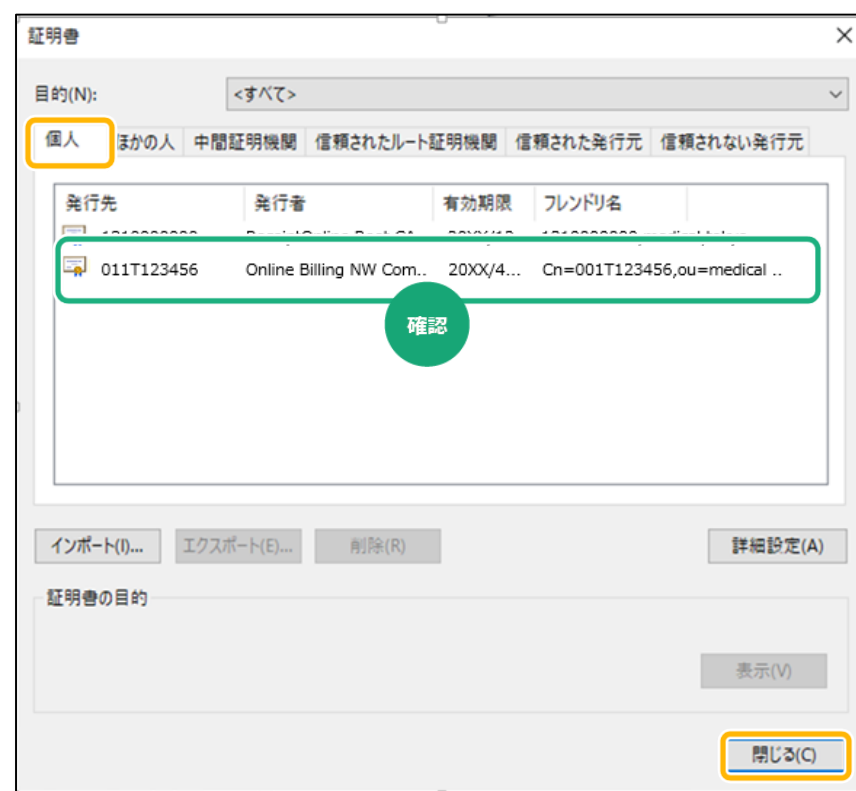
3へ進む

2 認証局の電子証明書をインストールする（つづき）

3 「証明書」が表示されます。

個人タブに、発行者が
**Online Billing NW
Common Root CA**と表示
されている証明書が登録され
ていることを確認します。

確認後、**閉じる** をクリック
します。

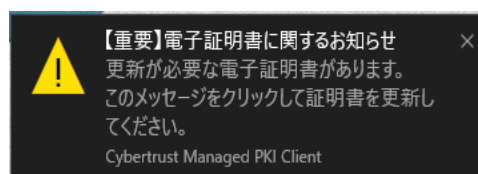


注意

MPKIクライアント（Cybertrust Managed PKI Client）のインストール

MPKIクライアントとは、電子証明書の有効期限が到来する前に更新通知を送信したり、電子証明書の更新時期が到来した際に、更新を簡単に行うことができる機能です。以下のマニュアルを参照し、インストールしてください。

（参照先）オンライン請求ネットワーク関連システム共通認証局ユーザーマニュアル(オンライン請求ネットワーク関連システムWindows IE)1.1.0版のPage 13



電子証明書をセットアップできました。

・証明書のダウンロード・インストールの詳細手順や更新、失効については以下をご参照ください。
オンライン請求ネットワーク関連システム共通認証局ユーザーマニュアル

インターネットから「オンライン資格確認・医療情報化支援基金関係医療機関等向けポータルサイト」を検索し、「各種資料ダウンロード」の「電子証明書インストール」から参照

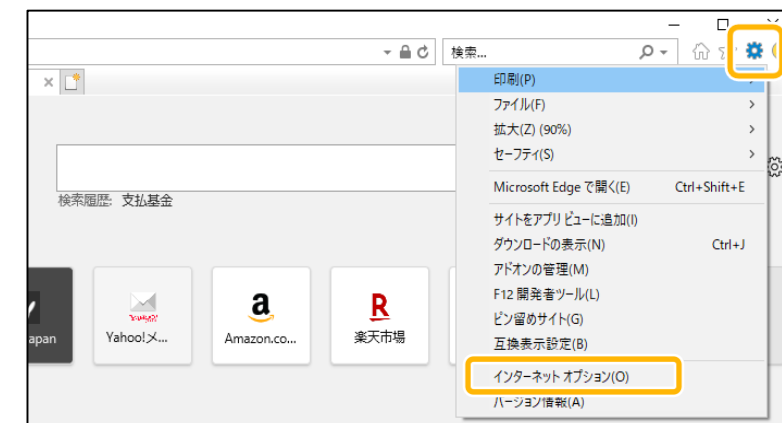
3 古い電子証明書の削除

電子証明書の削除

古い電子証明書を削除します。

1 Internet Explorerを起動し、 （ツール）をクリックします。

表示されたメニューから**インターネットオプション**を
クリックします。



2 インターネットオプションが 表示されます。

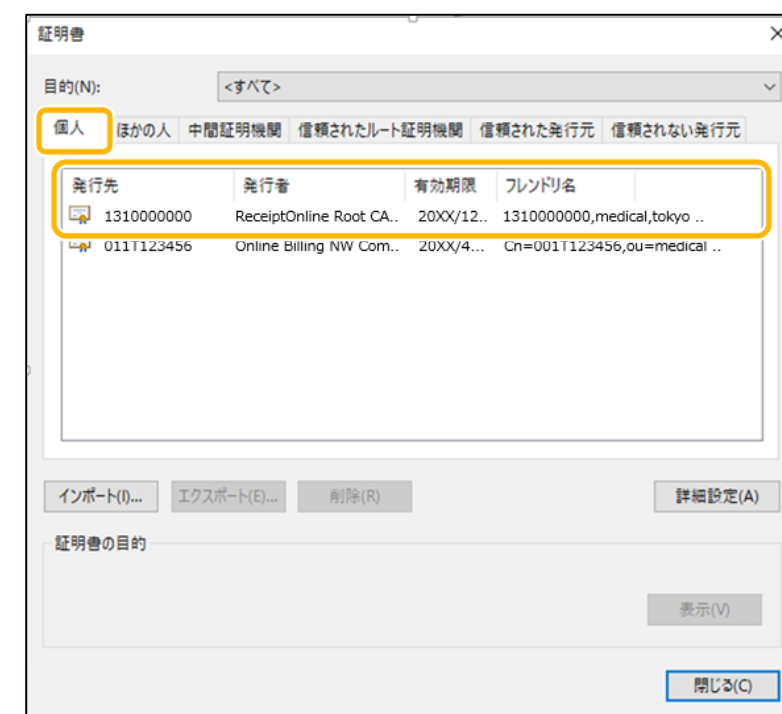
コンテンツタブを選択し、**証
明書**をクリックします。



3 「証明書」が表示されます。

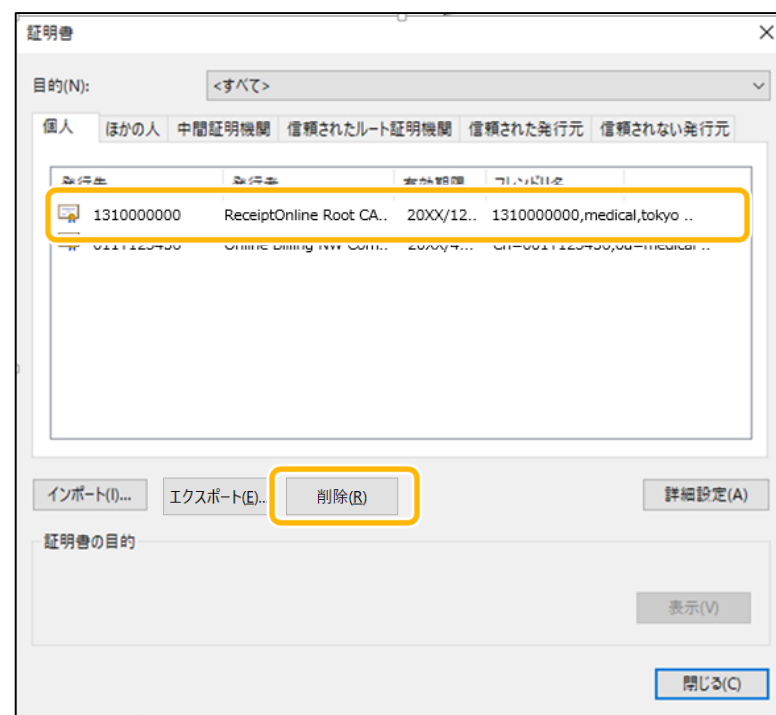
個人タブを開き、削除対象の
古い証明書（発行者が
ReceiptOnline Root CA
と表示されている証明書）
を確認します。

古い証明書（削除対象の証明
書）をクリックします。

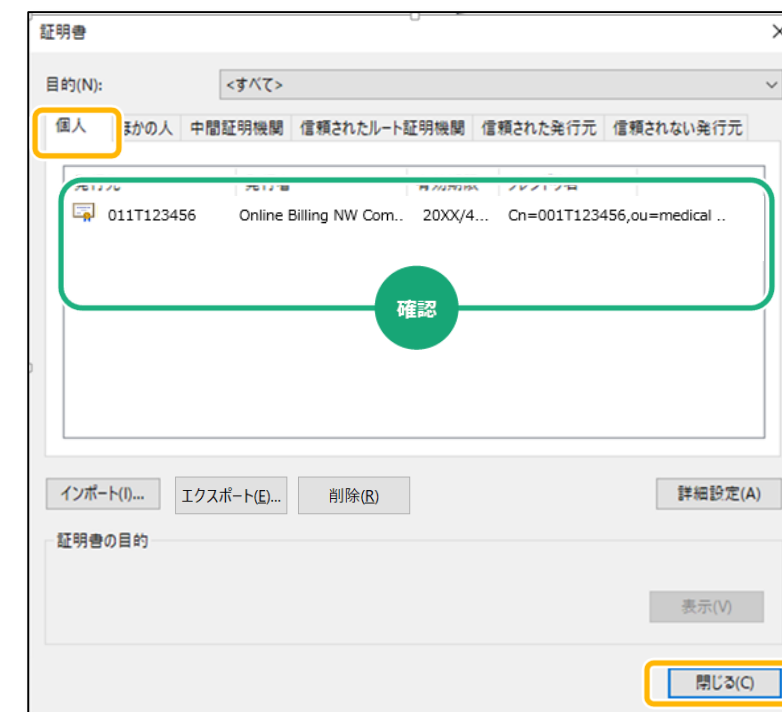


3 古い電子証明書の削除（つづき）

- 4 削除ボタンをクリックします。
「証明書を削除しますか？」
画面に遷移します。



- 6 「証明書」が表示されます。
個人タブを開き、削除を行った証明書が一覧から消えていることを確認します。
確認後、「閉じる」をクリックします。



- 5 確認画面が表示されます。
「はい」ボタンをクリックすると証明書の削除が行われます。
「証明書」画面に遷移します。

