NEOJAPAN

desknet's NEO

利用者向け

desknet's NEO

クライアント認証サービス用
証明書のインストール・設定

当社検証端末での画面遷移となります。
表示される画面に多少差異がある場合も
ございますので、予めご了承ください。

Index

01 Microsoft Edgeをご利用の場合

※ここでは、Microsoft Edge バージョン109を例に説明します。

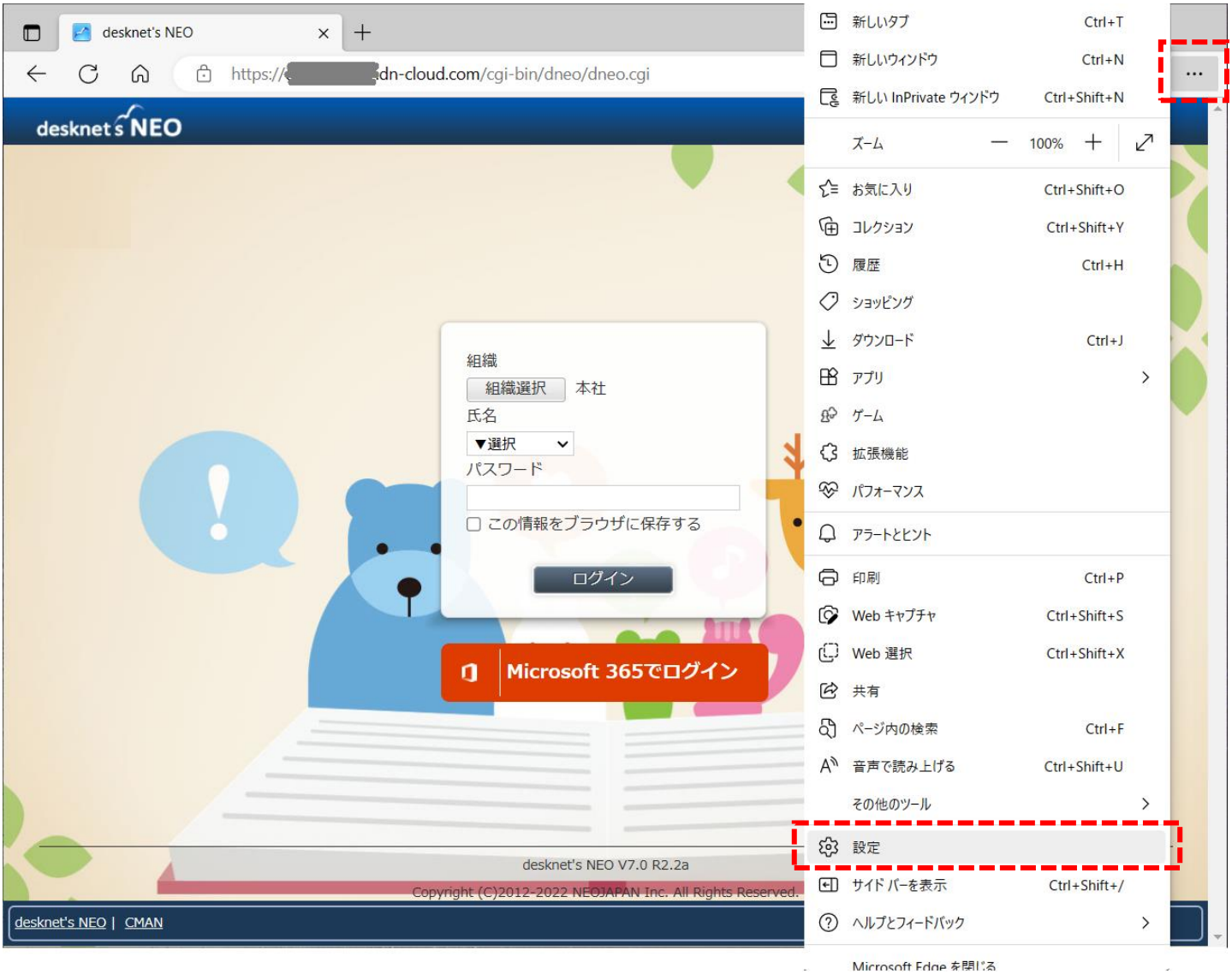
1. クライアント認証サービス用のファイルの準備

発行管理担当者から配布された、下記ファイルをご利用端末の任意の場所に保存します。

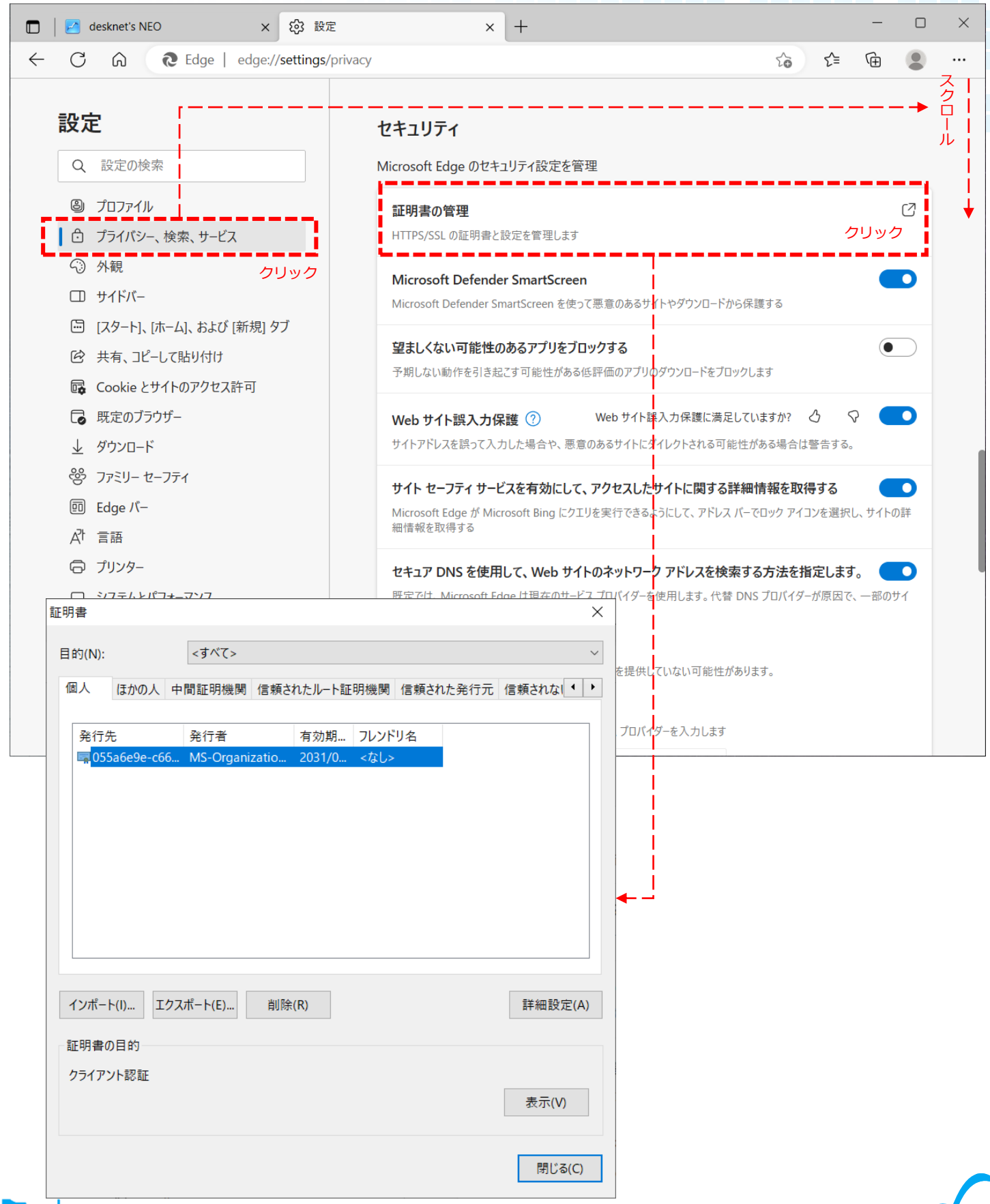
- CA証明書ファイル（cacert.pem）
- クライアント証明書ファイル（***.pfx）
- 配布されたクライアント証明書ファイルのパスワード

2. CA証明書（cacert.pem）のインストール

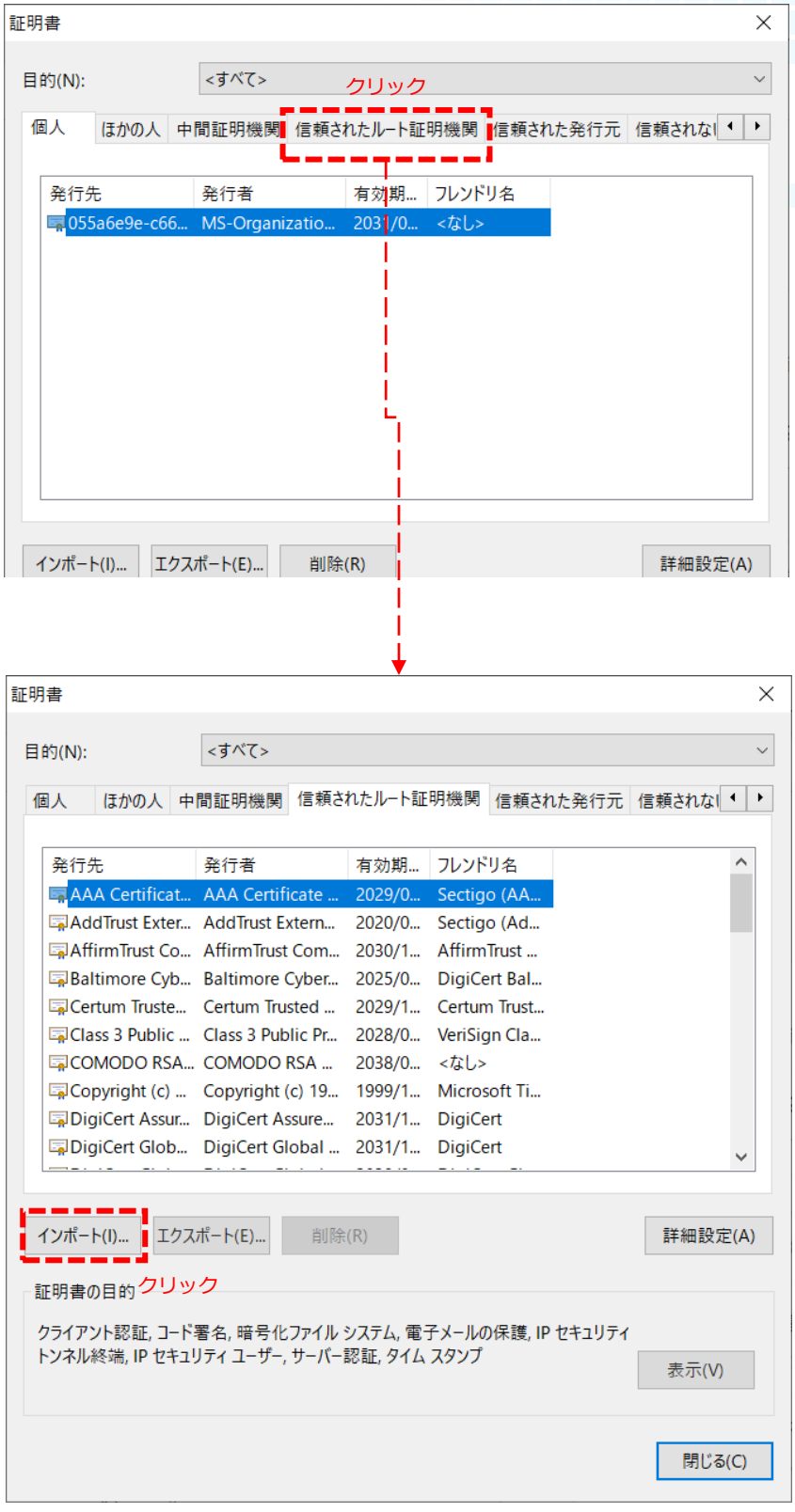
① Microsoft Edgeを立ち上げ、…（設定など）→「設定」の順にクリックします。



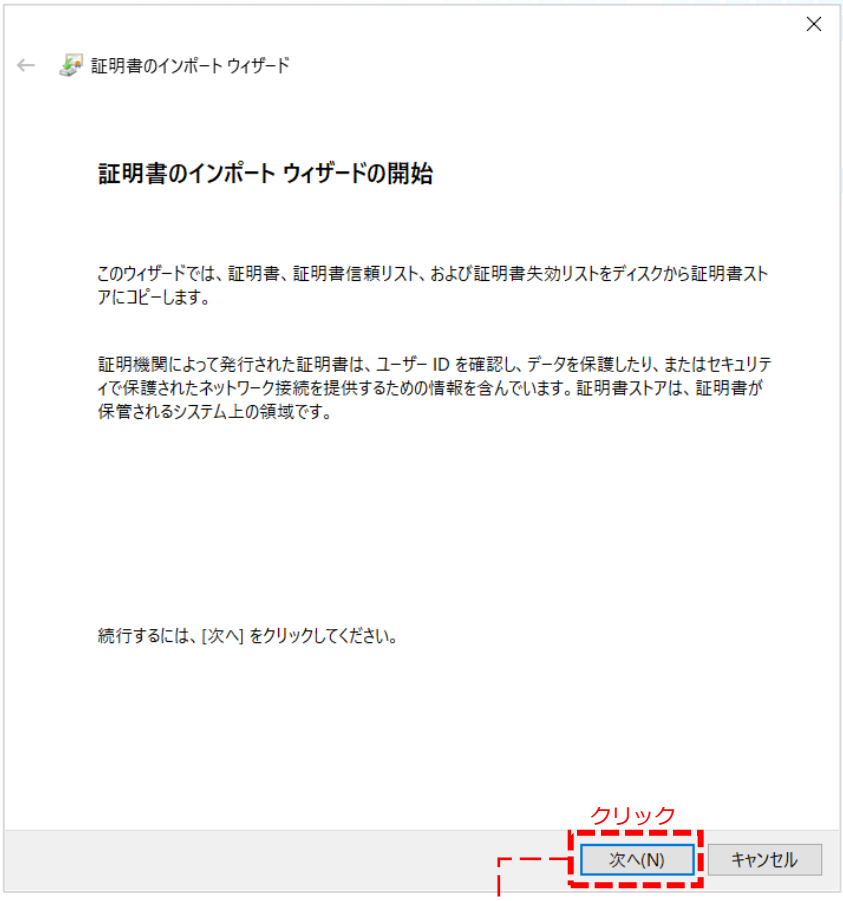
② 設定画面のタブが開きますので、メニューより「プライバシー、検索、サービス」を選択。
画面を項目「セキュリティー」までスクロールし「証明書の管理」をクリックしてください。

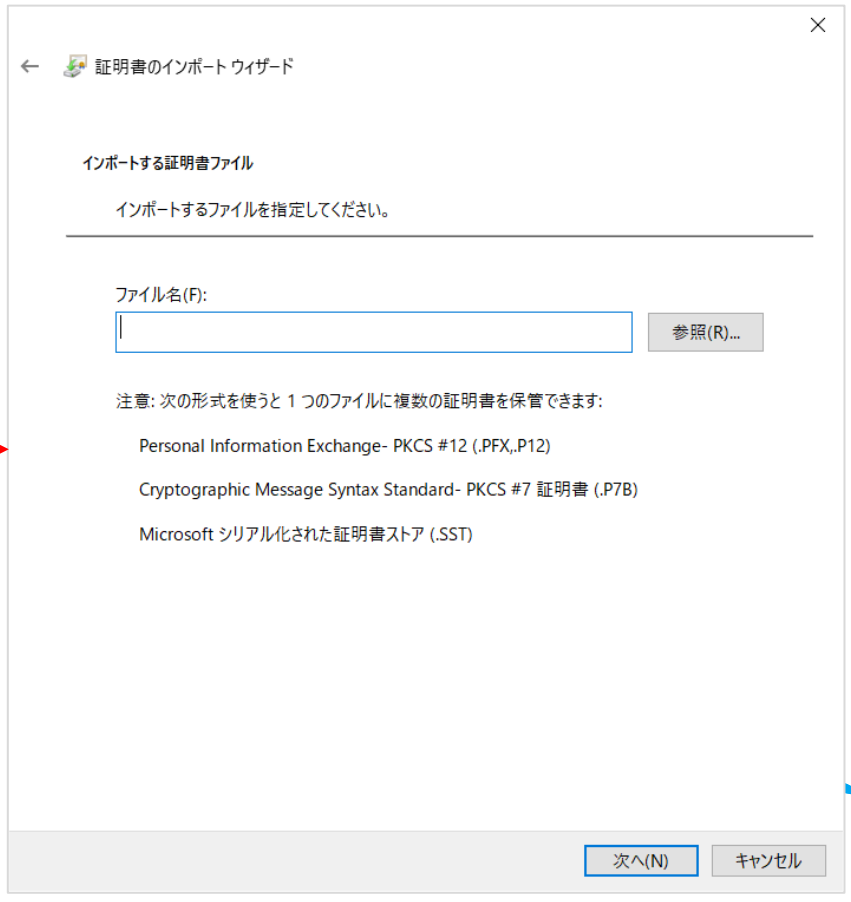


③ 「信頼された証明書」タブをクリックし、［インポート］ボタンをクリックしてください。

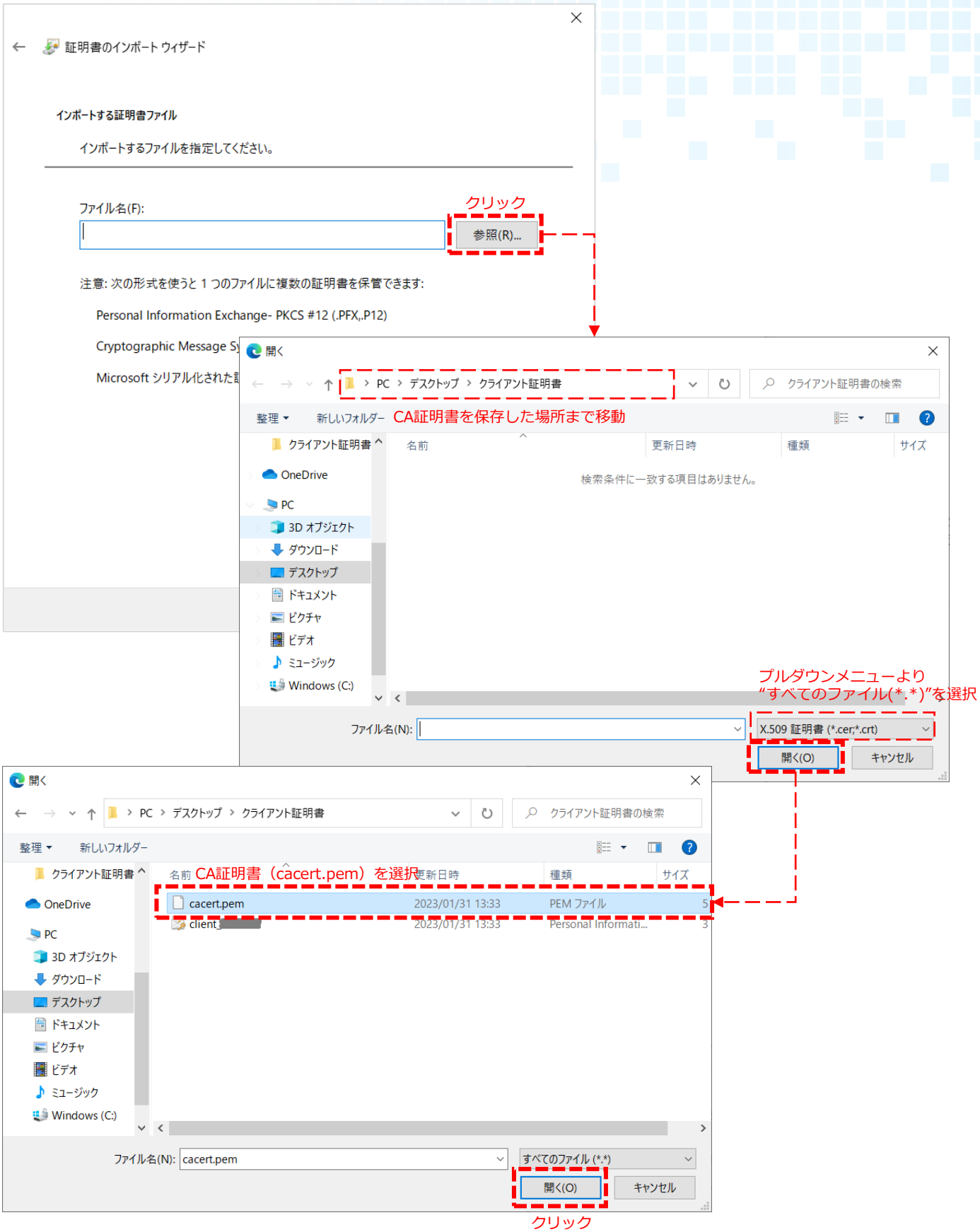


④ 「証明書のインポートウィザード」が表示されますので、［次へ］ボタンをクリックしてください。

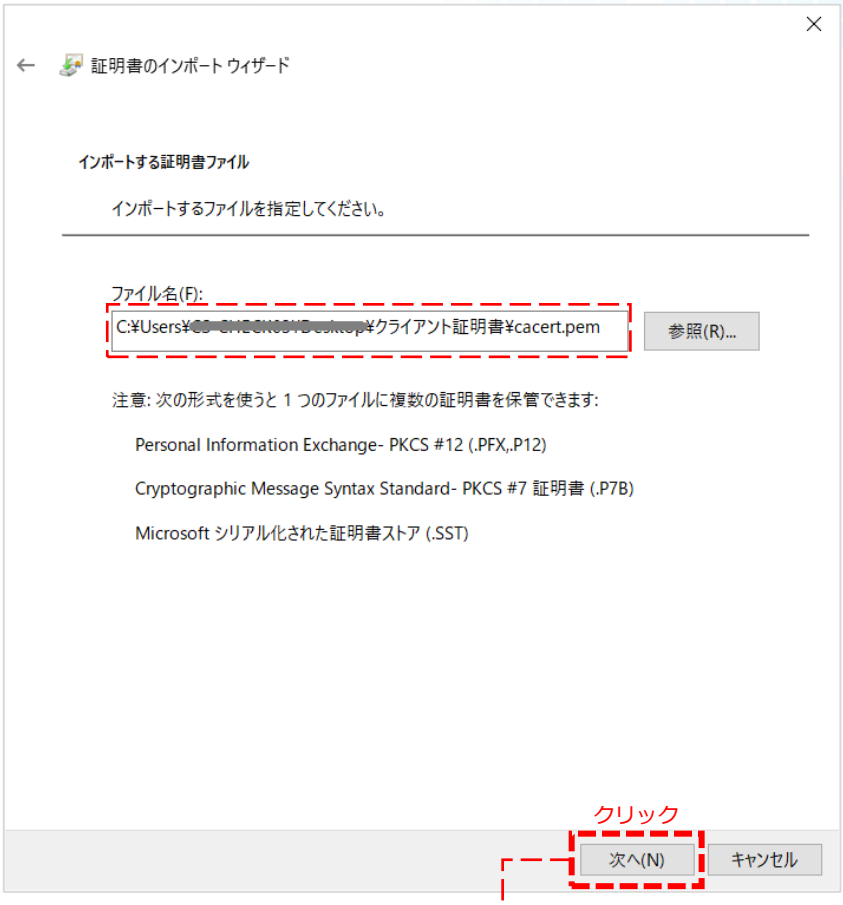


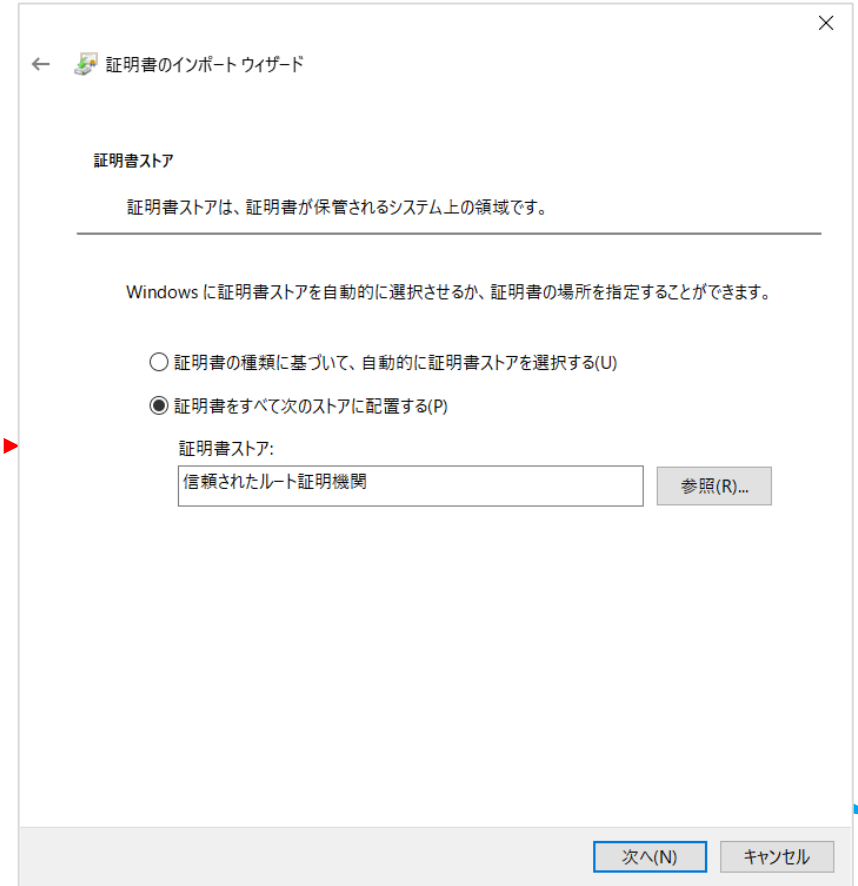


⑤ ［参照］ボタンをクリックし、インポートするCA証明書（cacert.pem）を選択します。

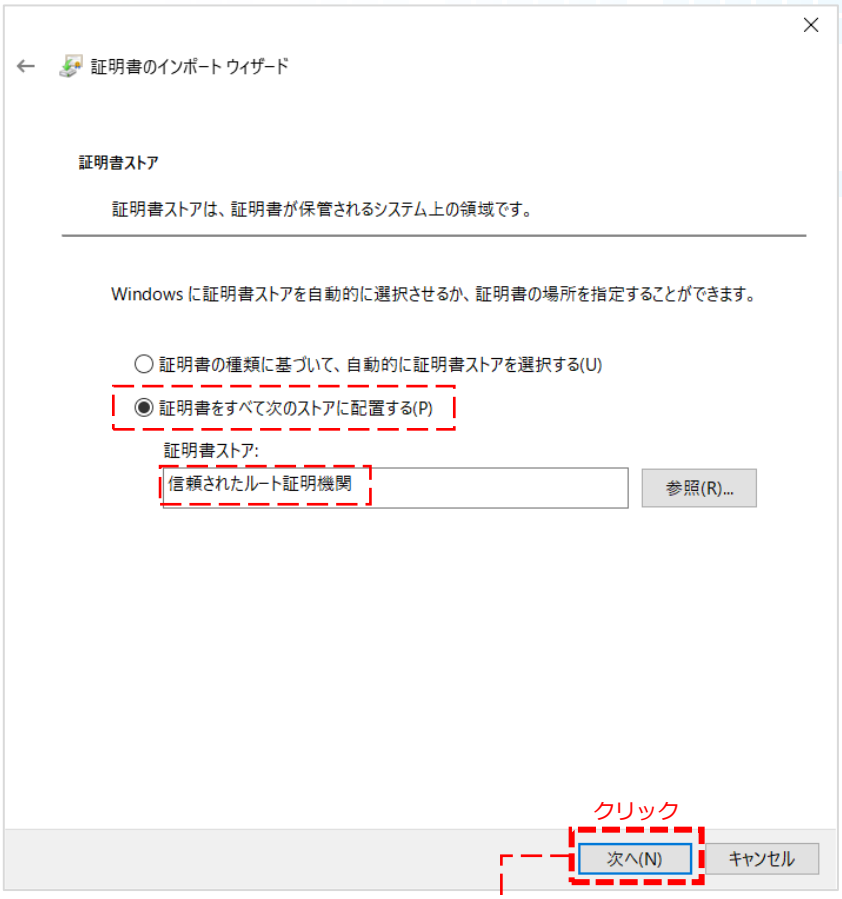


⑥ CA証明書（cacert.pem）が選択されていることを確認し、［次へ］ボタンをクリックしてください。

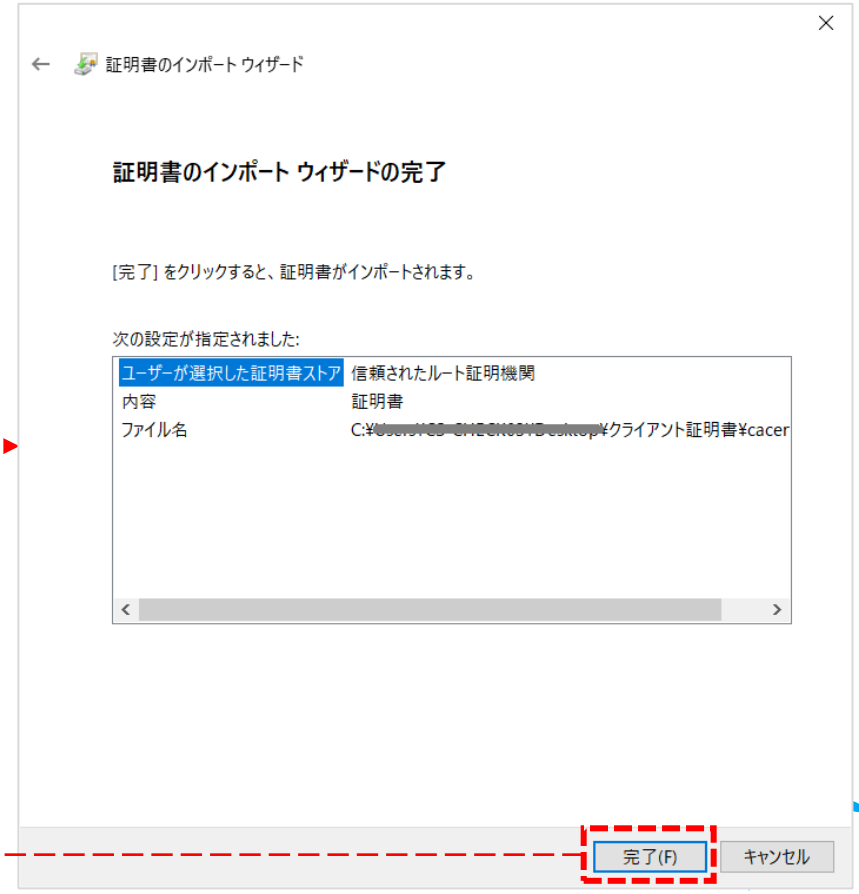




⑦ 「証明書をすべて次のストアに配置する(P)」のラジオボタンを選択、「証明書ストア：」に「信頼されたルート証明機関」を選択し、［次へ］ボタンをクリックします。

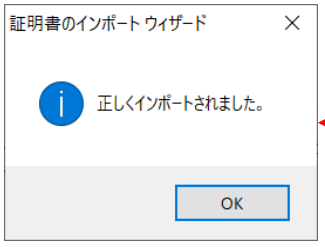


クリック



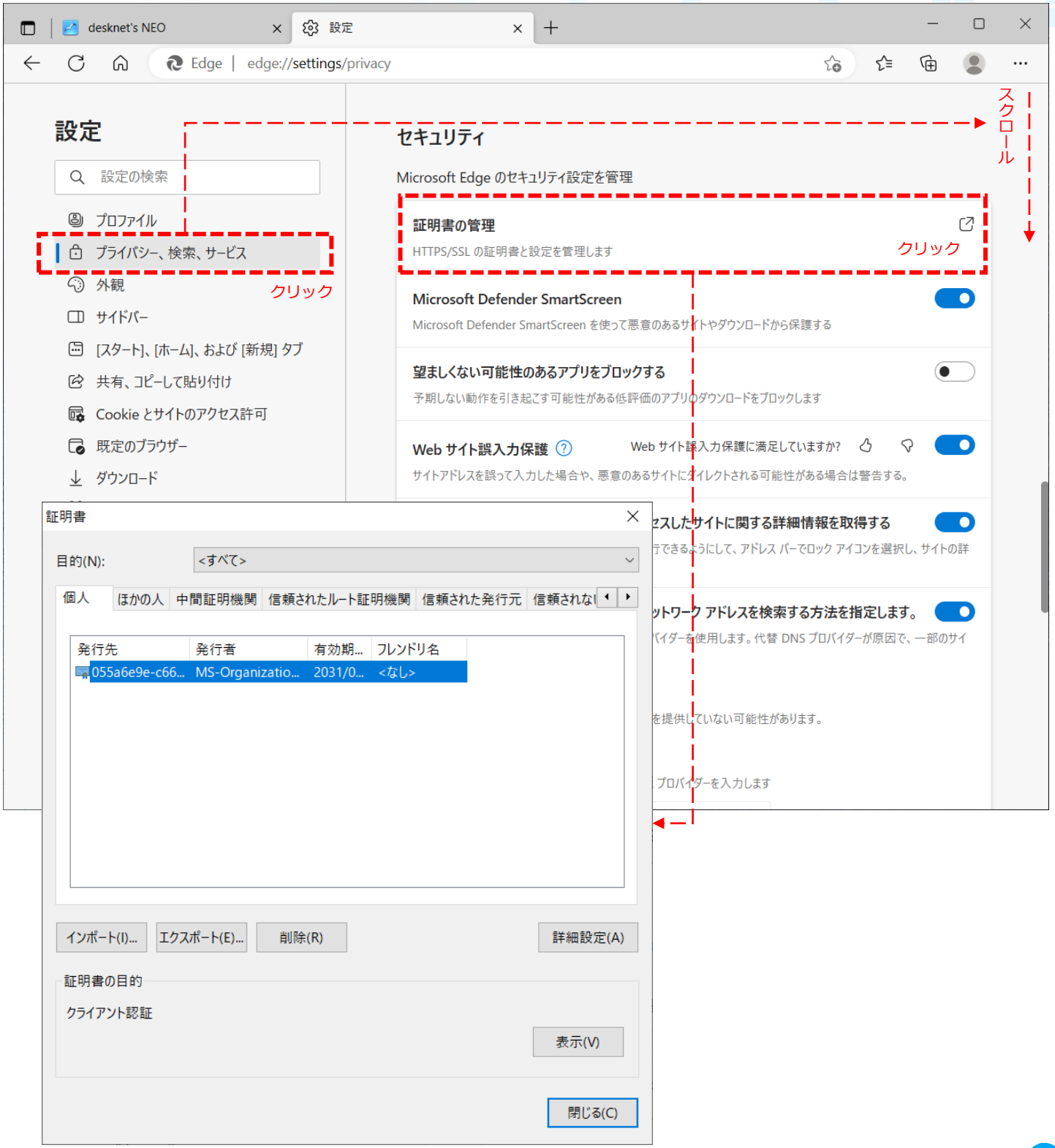
完了

「証明書のインポートウィザードの完了」画面で、「完了」をクリックすると、CA証明書（cacert.pem）が登録されます。

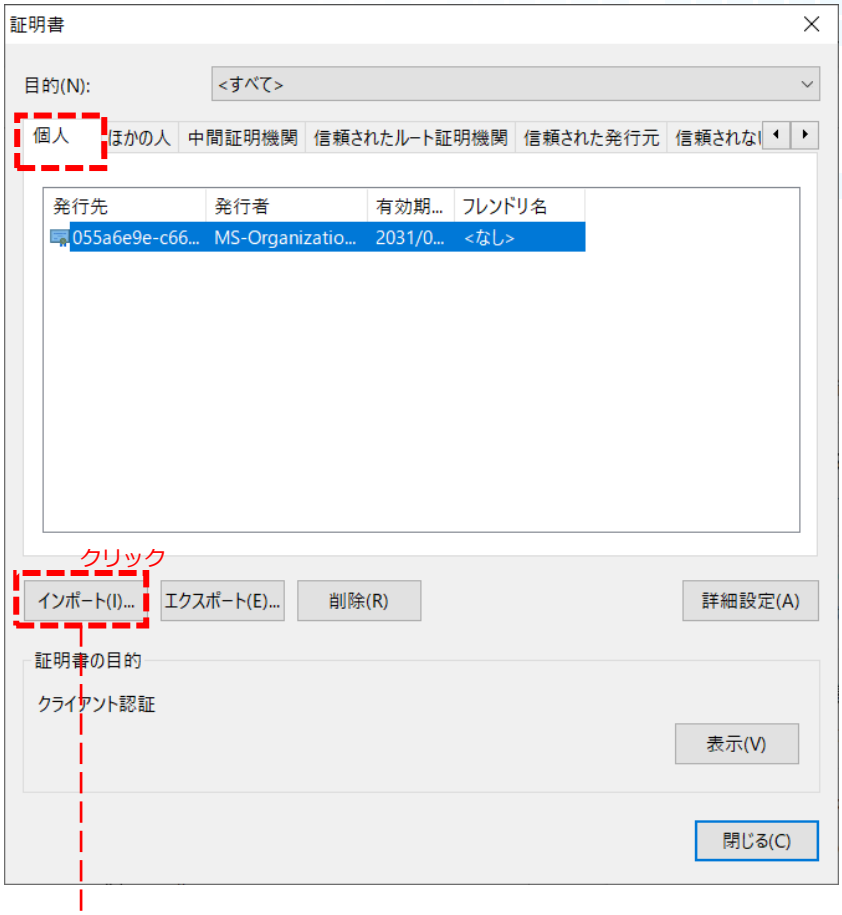


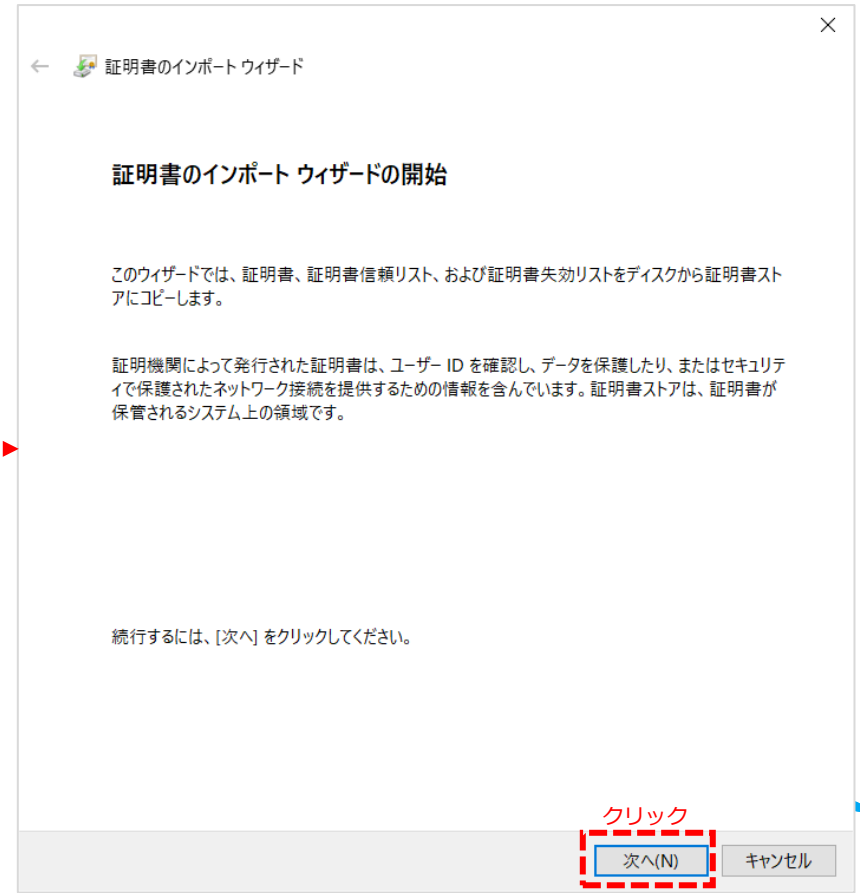
3. クライアント証明書ファイル（*.pfx）のインストール

① ･･･（設定など）→「設定」→設定画面タブのメニューより「プライバシー、検索、サービス」を選択。
画面を項目「セキュリティー」までスクロールし「証明書の管理」をクリックしてください。

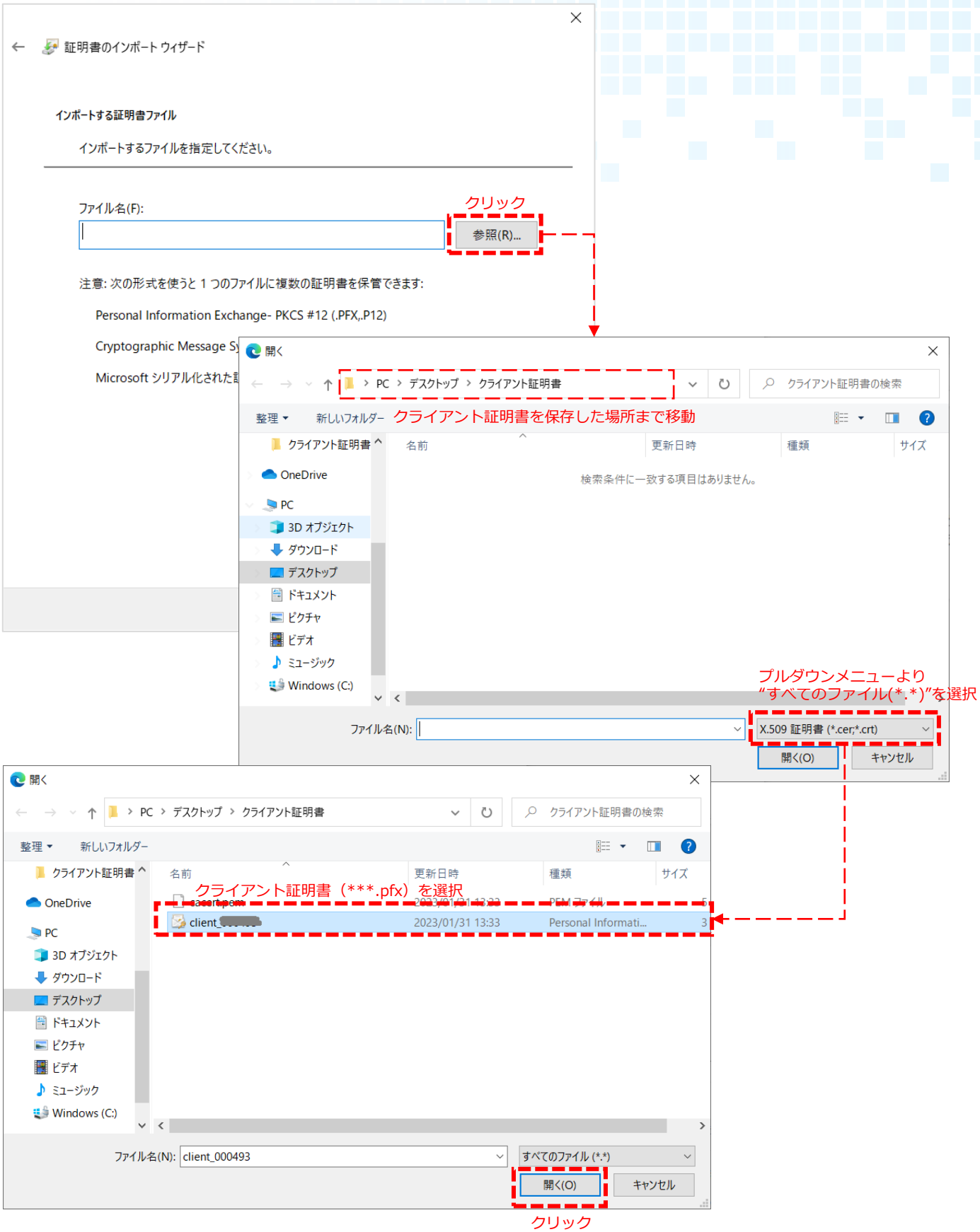


② 「個人」タブをクリックし、［インポート］ボタンをクリックすると、「証明書のインポート ウィザード」が表示されますので、［次へ］ボタンをクリックしてください。

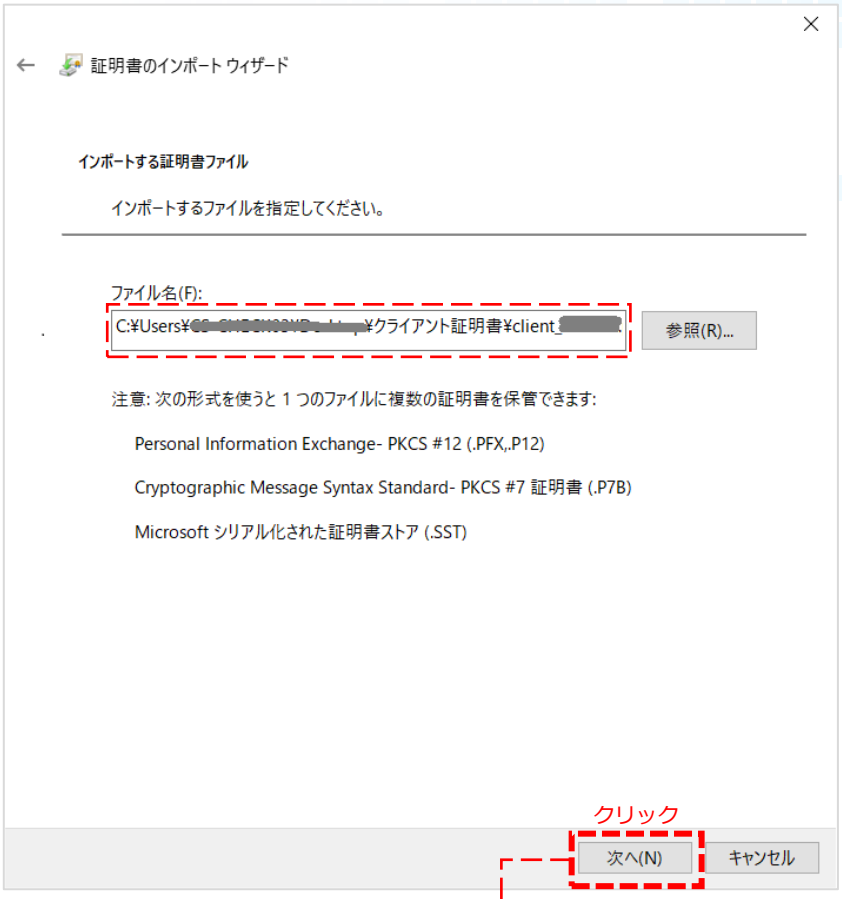


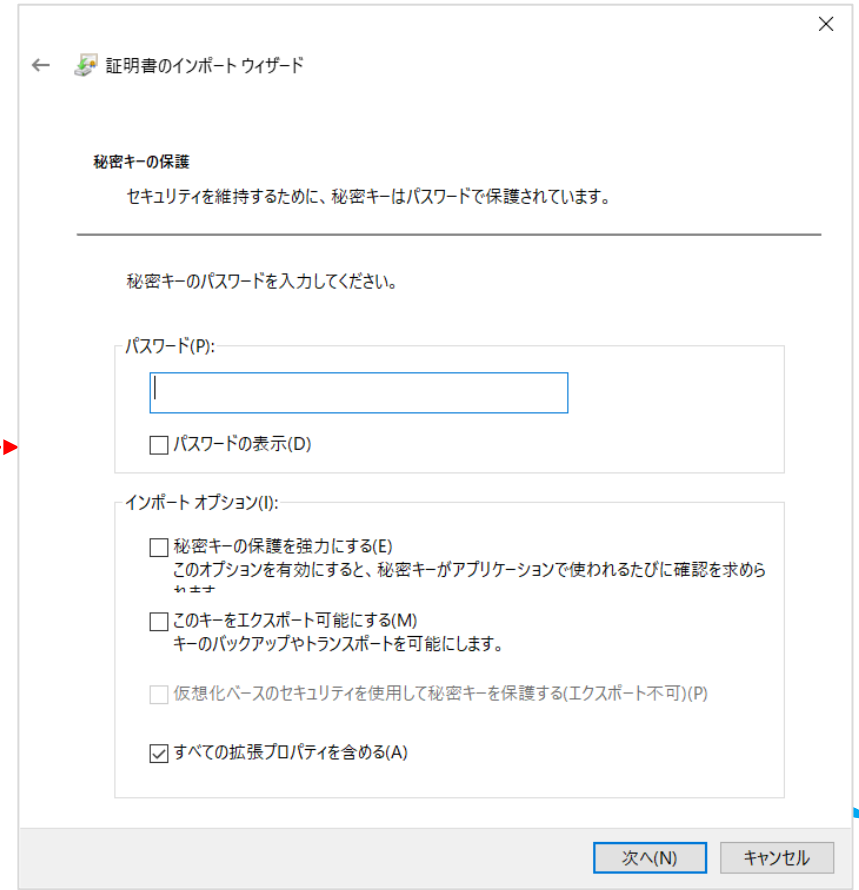


③ ［参照］ボタンをクリックし、インポートするクライアント証明書（***.pfx）を選択します。



④ クライアント証明書（***.pfx）が選択されていることを確認し、［次へ］ボタンをクリックしてください。

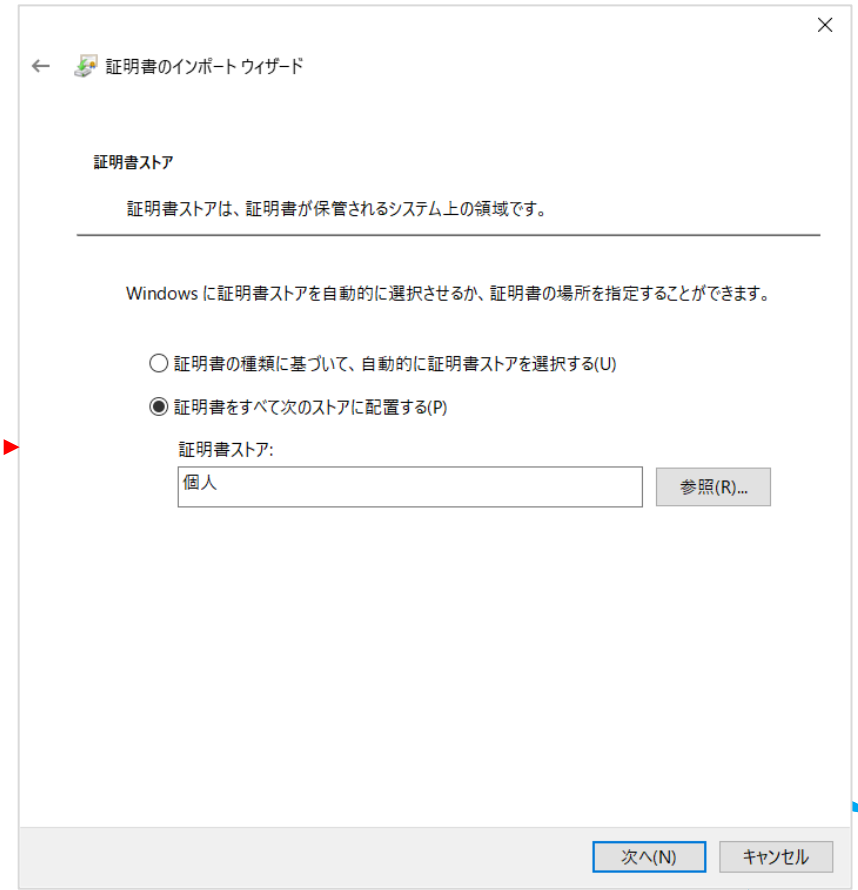




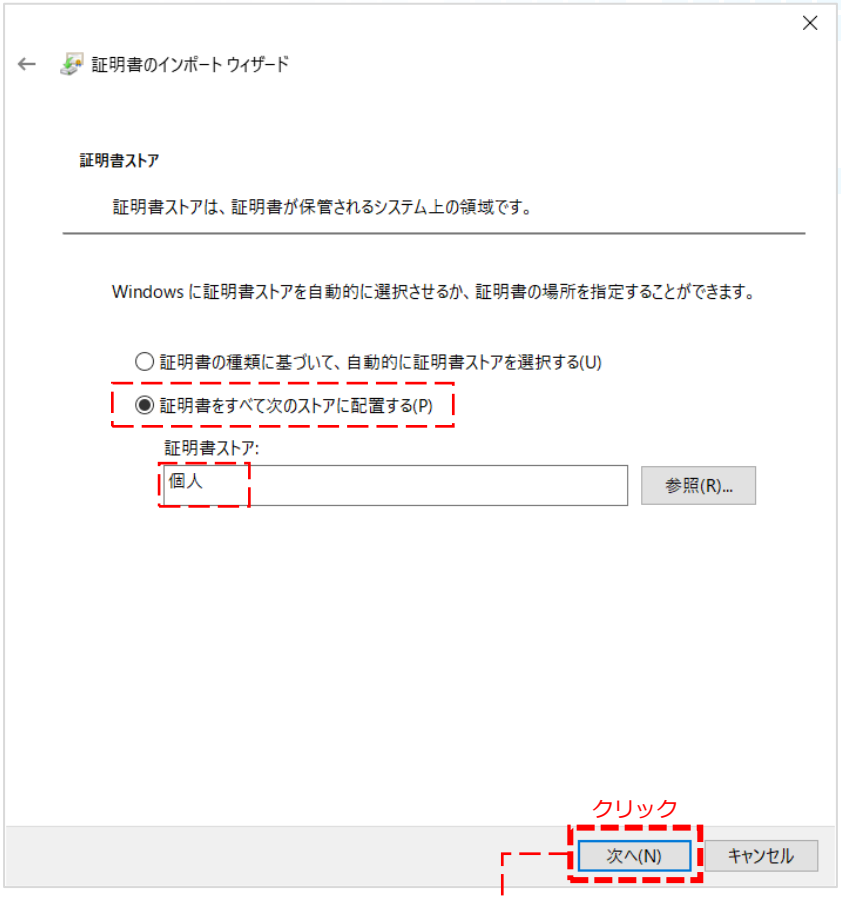
⑤ 配布された「クライアント証明書のパスワード」を「パスワード」欄に入力し、［次へ］ボタンをクリックしてください。

発行管理担当者から配布されたクライアント証明書ファイルのパスワードを入力してください。

クリック

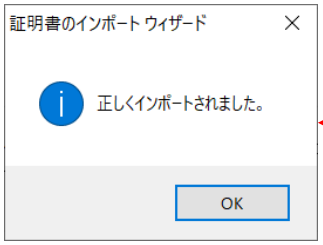


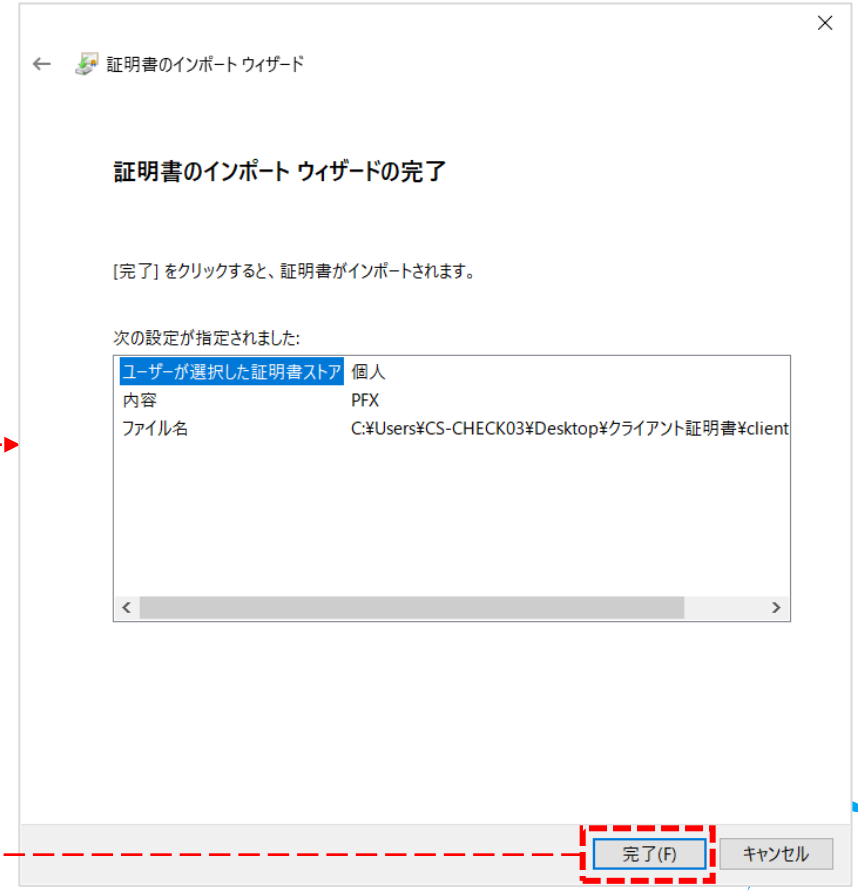
⑥　「証明書をすべて次のストアに配置する(P)」ラジオボタンを選択、「証明書ストア：」に「個人」を選択し、［次へ］ボタンをクリックします。



完了

「証明書のインポートウィザードの完了」画面で、「完了」をクリックすると、クライアント証明書（***.pfx）が登録されます。





02 Google Chromeをご利用の場合

※ここでは、Google Chrome バージョン109を例に説明します。

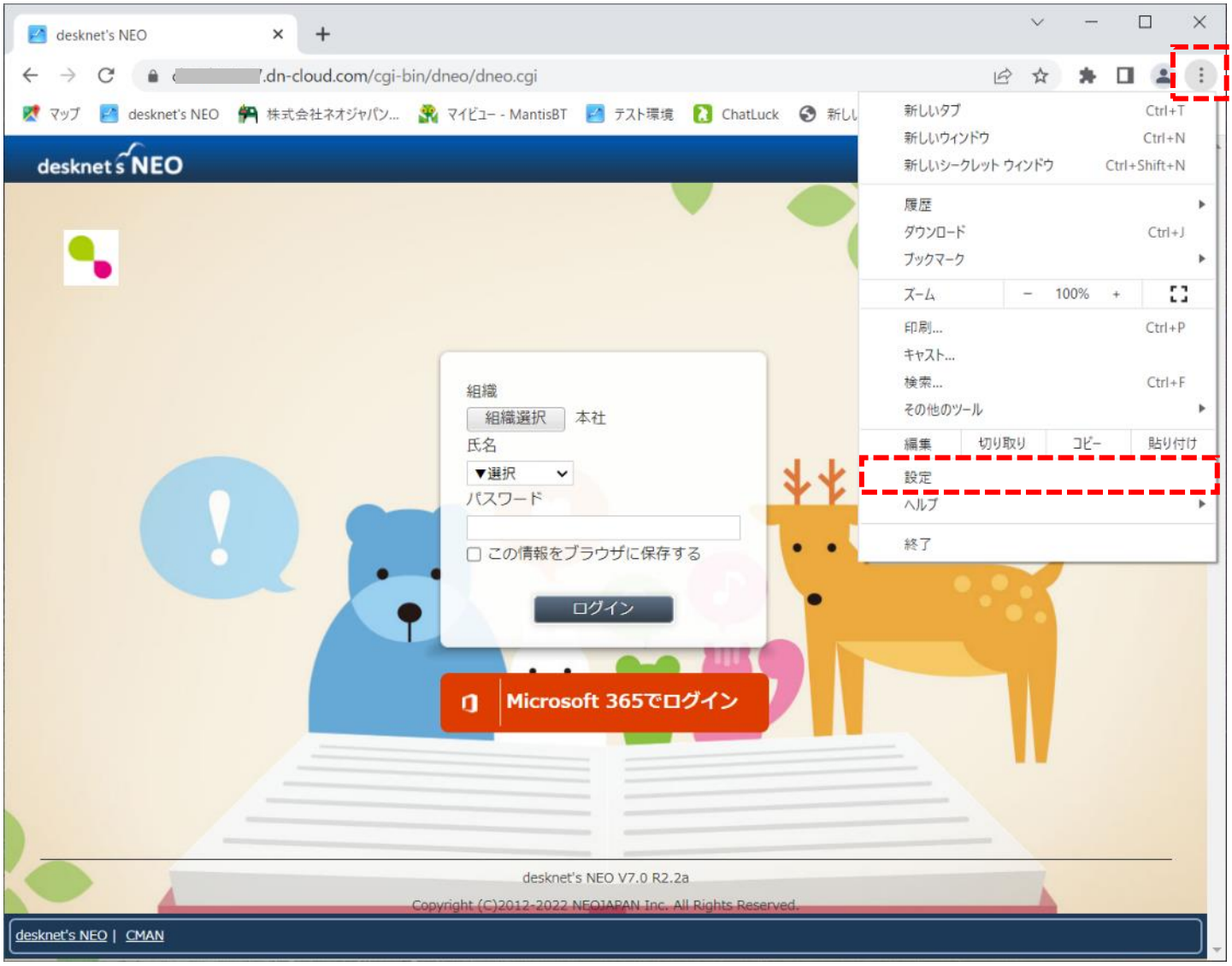
1. クライアント認証サービス用のファイルの準備

発行管理担当者から配布された、下記ファイルをご利用端末の任意の場所に保存します。

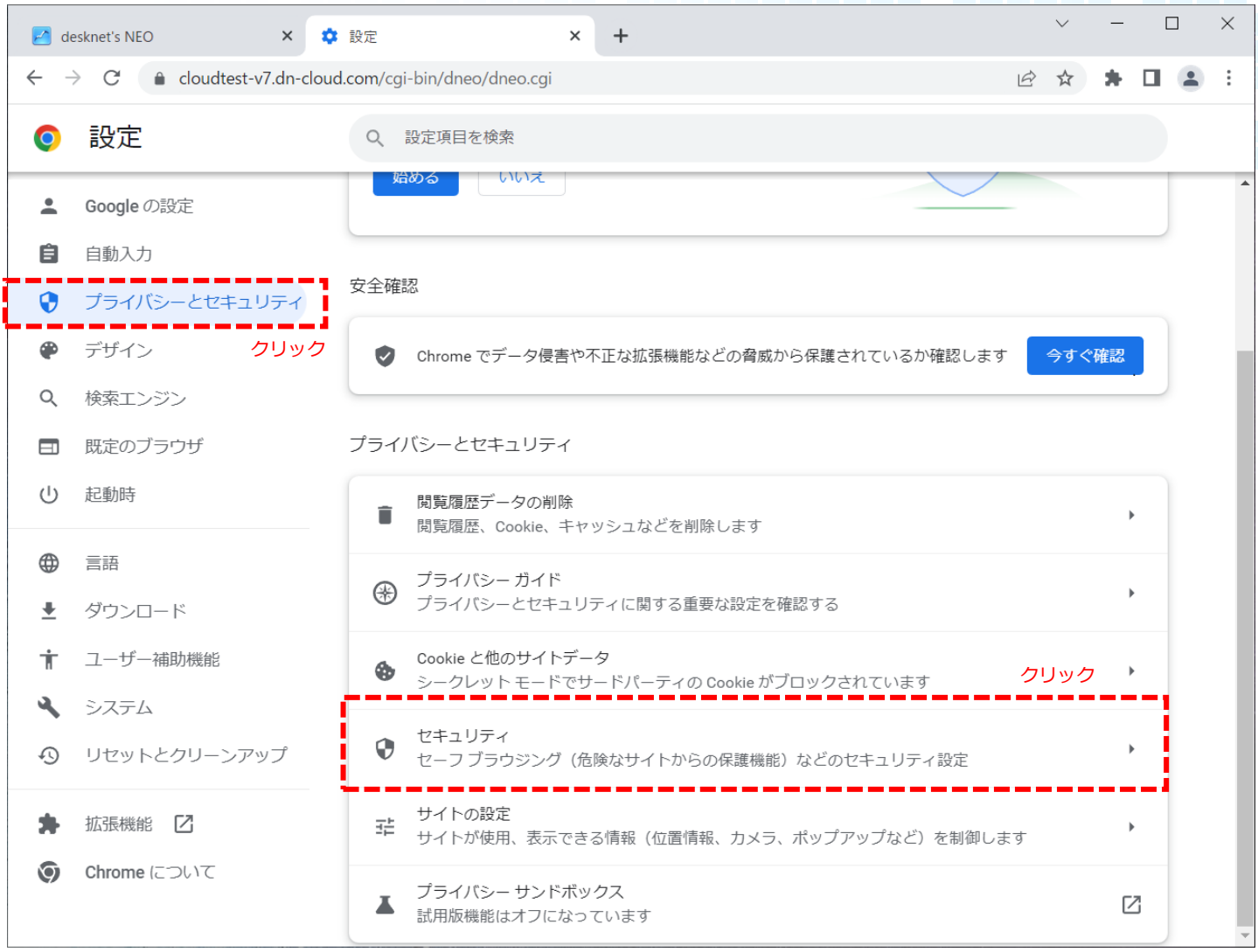
- CA証明書ファイル（cacert.pem）
- クライアント証明書ファイル（***.pfx）
- 配布されたクライアント証明書ファイルのパスワード

2. CA証明書（cacert.pem）のインストール

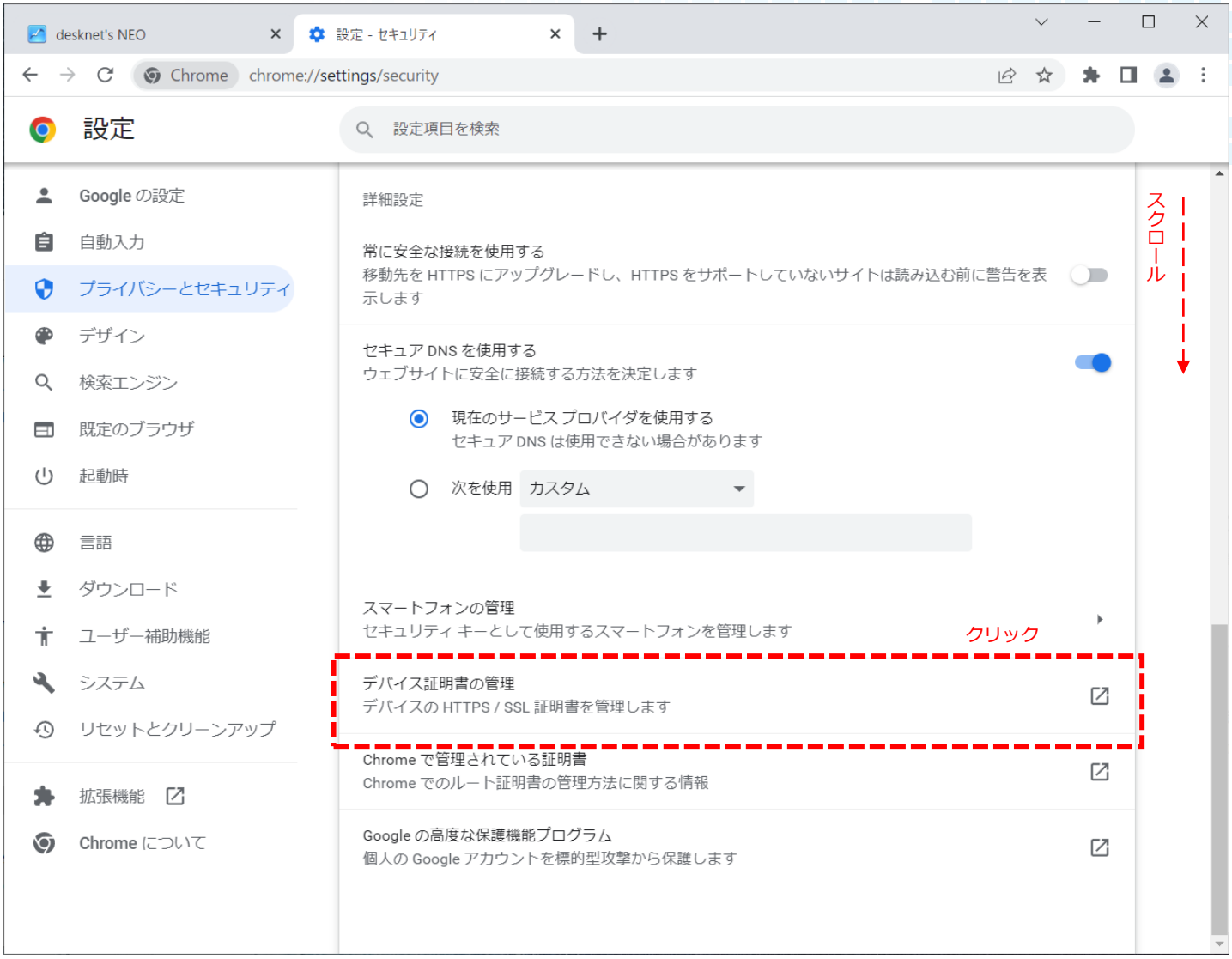
① Google Chromeを立ち上げ、⋮（Google Chromeの設定）→「設定」の順にクリックします。



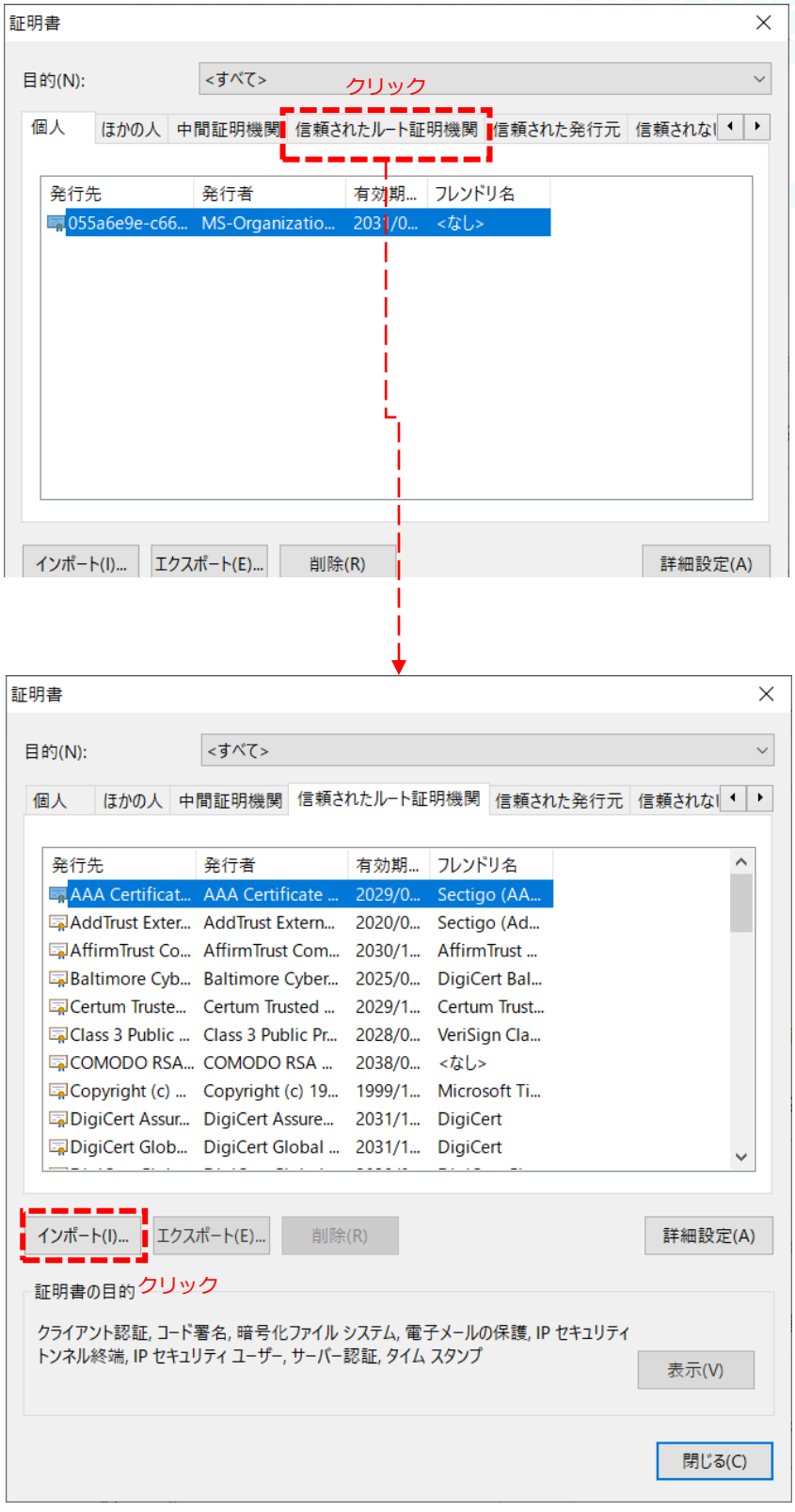
② 設定画面のタブが開きますので、メニューより「プライバシーとセキュリティ」を選択。
項目「セキュリティー」をクリックしてください。



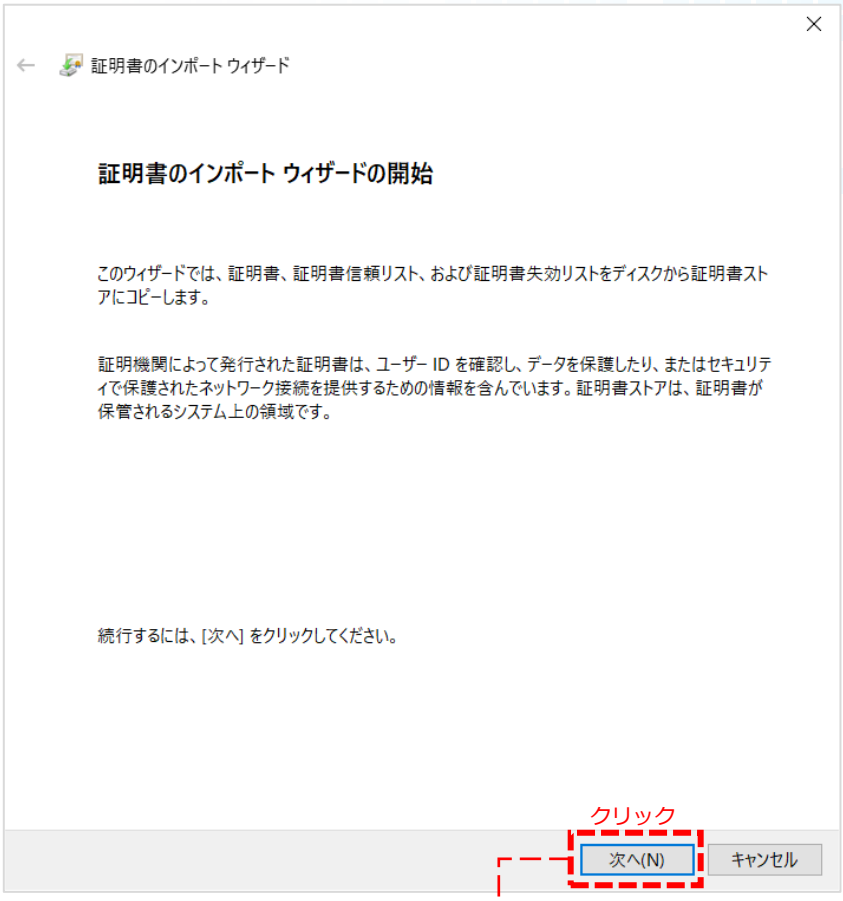
③ 「設定 – セキュリティ」画面に遷移しますので、スクロールして「デバイス証明書の管理」をクリックしてください。



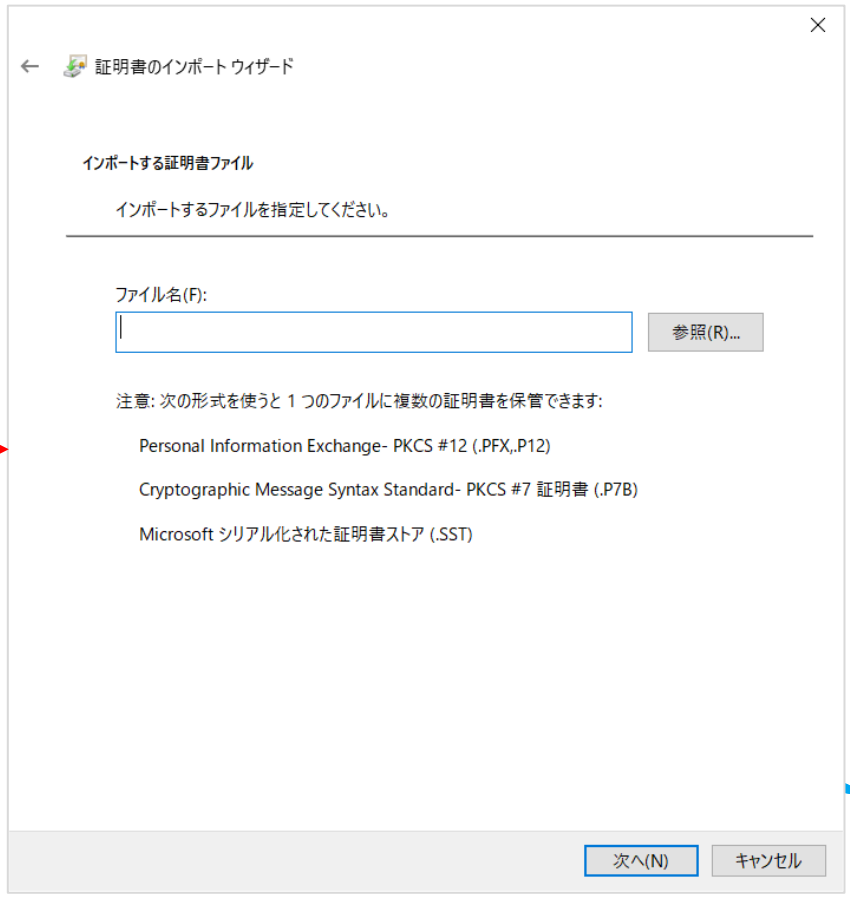
④ 「信頼された証明書」タブをクリックし、［インポート］ボタンをクリックしてください。



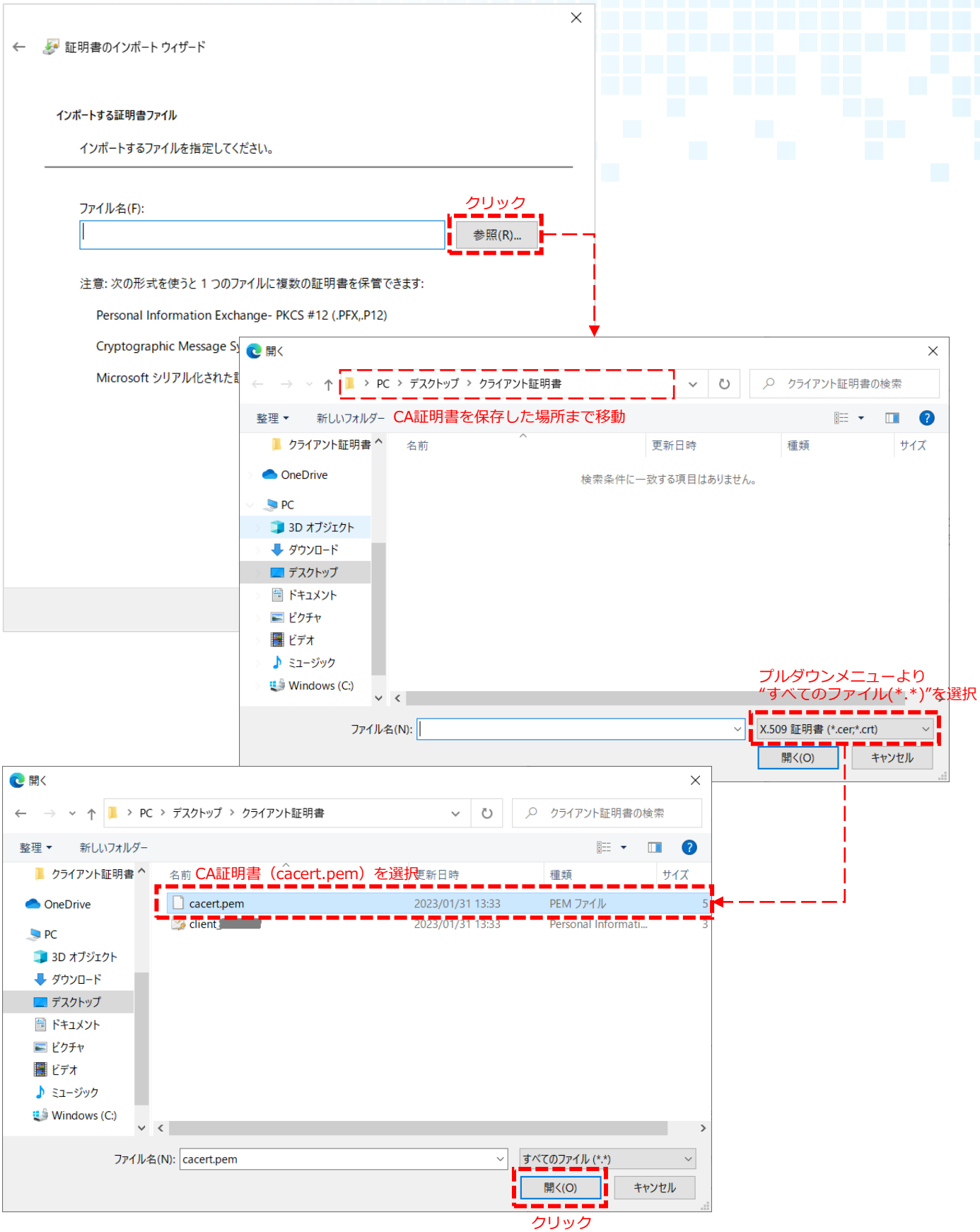
⑤ 「証明書のインポートウィザード」が表示されますので、［次へ］ボタンをクリックしてください。



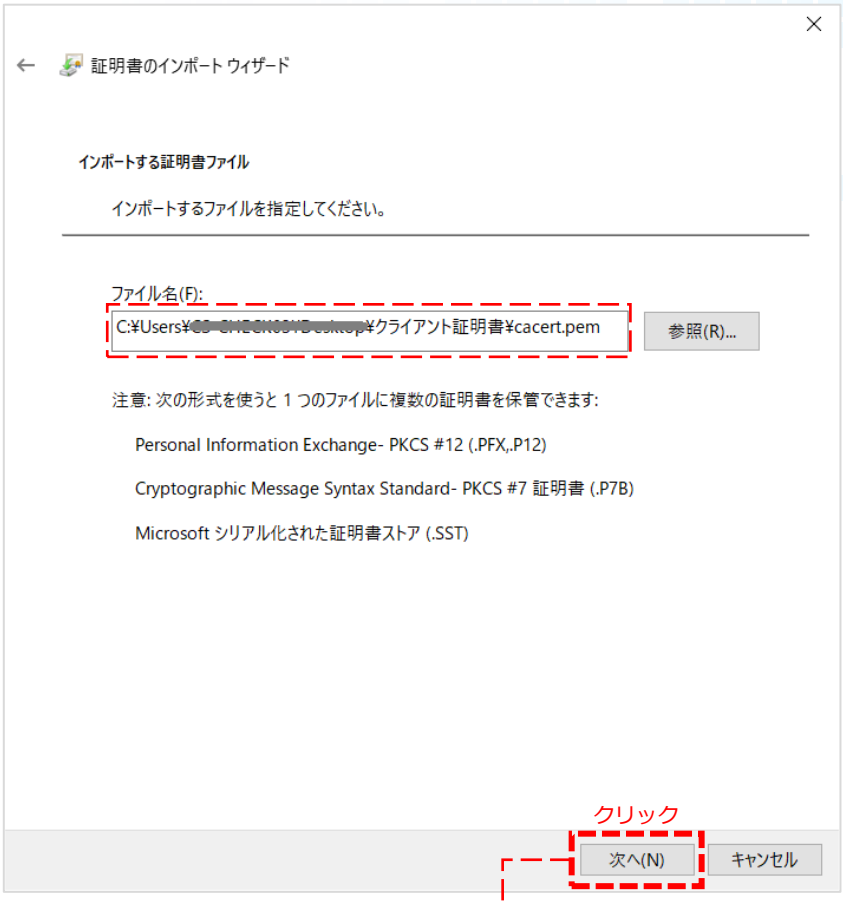
クリック

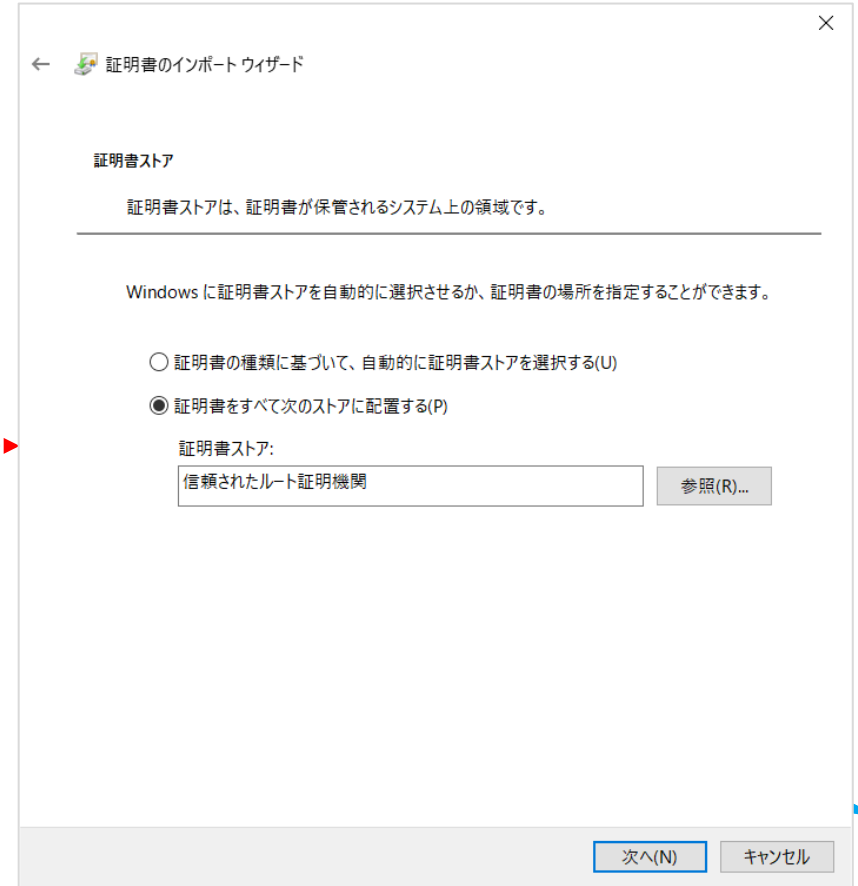


⑥ ［参照］ボタンをクリックし、インポートするCA証明書（cacert.pem）を選択します。

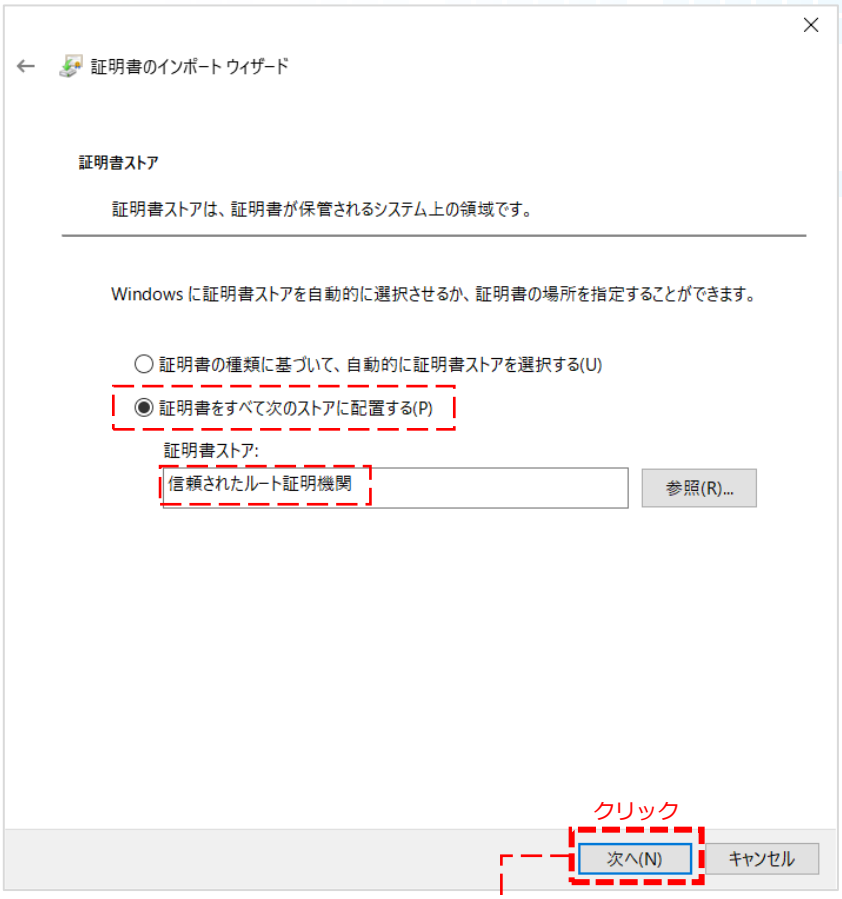


⑦ CA証明書（cacert.pem）が選択されていることを確認し、［次へ］ボタンをクリックしてください。

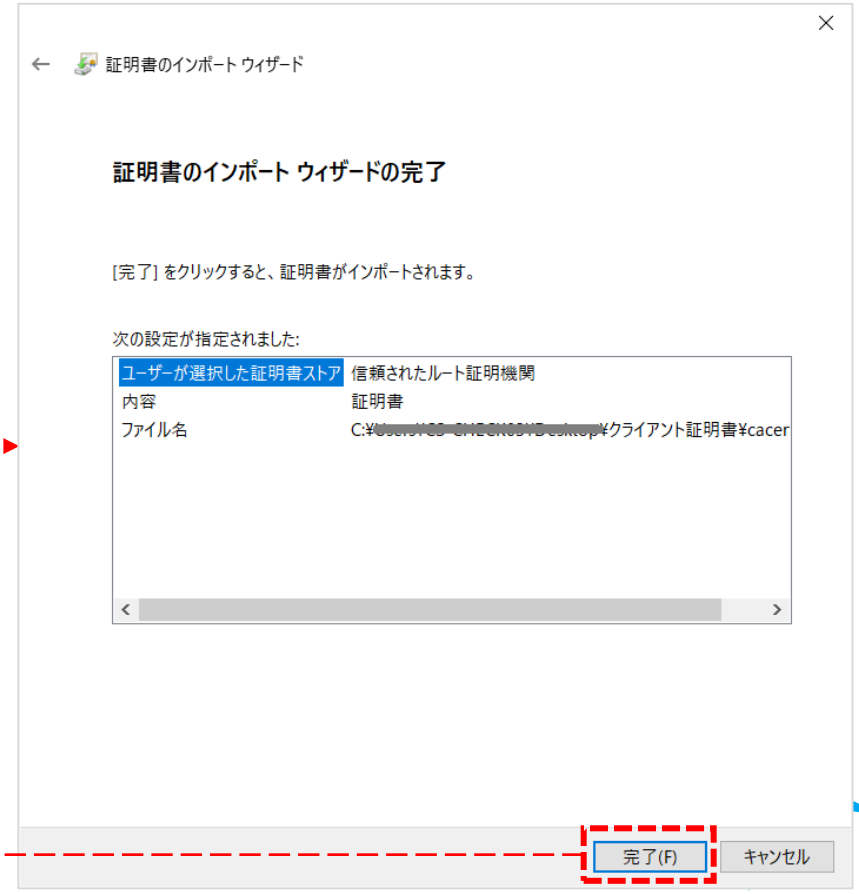




⑧ 「証明書をすべて次のストアに配置する(P)」のラジオボタンを選択、「証明書ストア：」に「信頼されたルート証明機関」を選択し、［次へ］ボタンをクリックします。

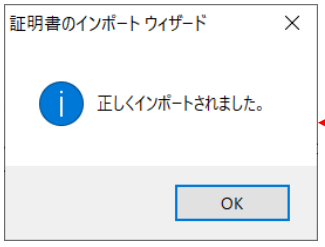


クリック



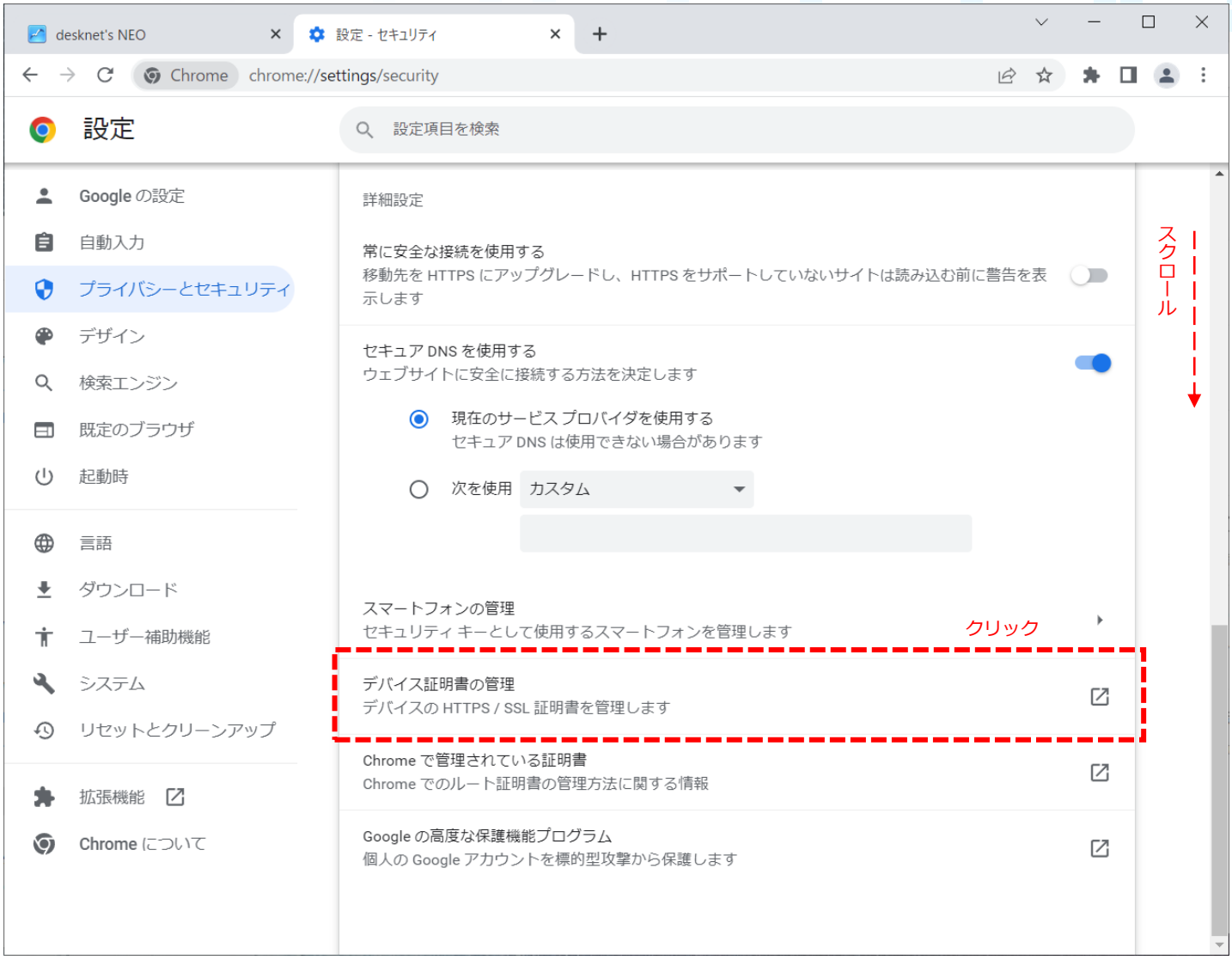
完了

「証明書のインポートウィザードの完了」画面で、「完了」をクリックすると、CA証明書（cacert.pem）が登録されます。

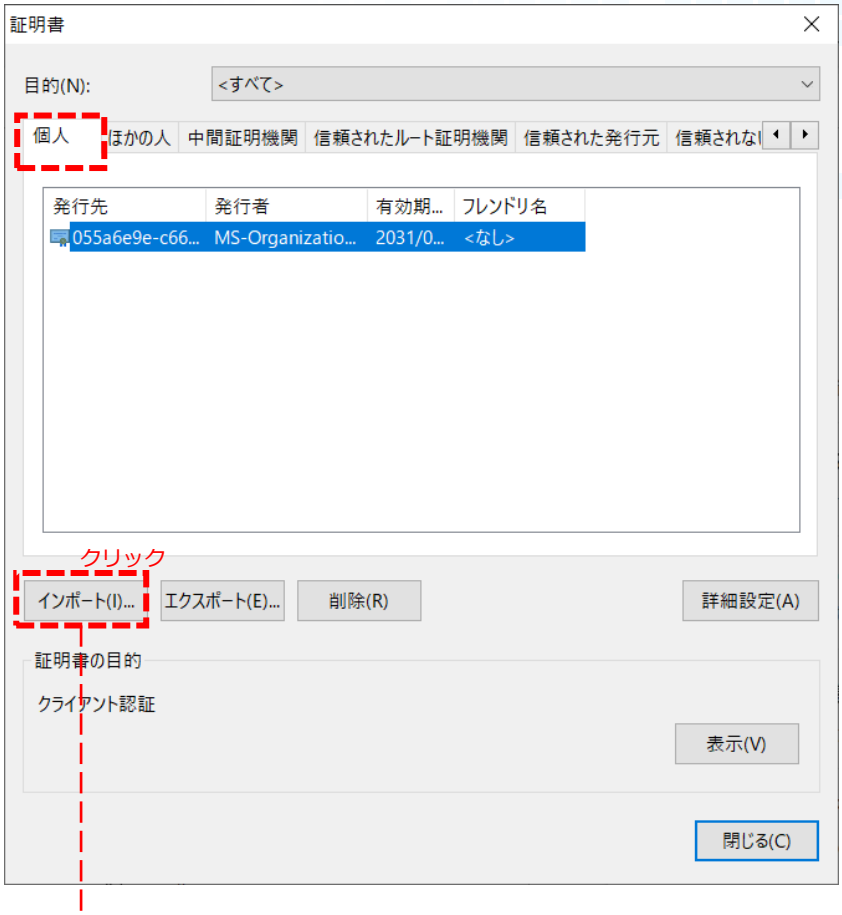


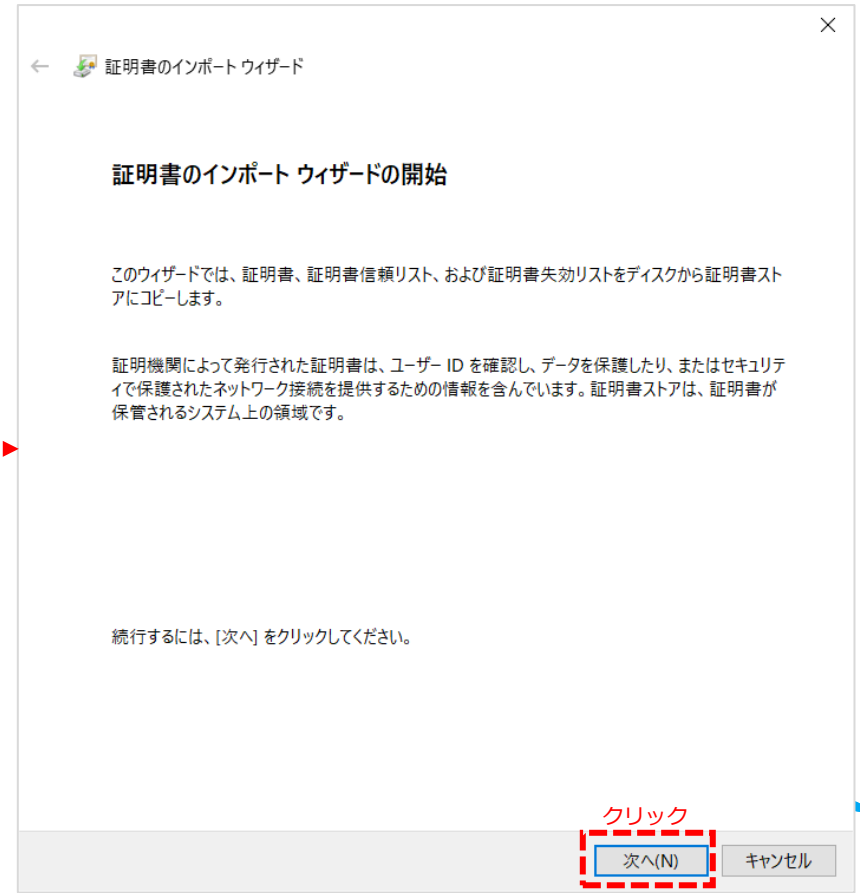
3. クライアント証明書ファイル（*.pfx）のインストール

① ⋮（Google Chromeの設定）→「設定」→設定画面タブのメニューより「プライバシーとセキュリティ」→項目「セキュリティー」で画面遷移し、スクロールして「デバイス証明書の管理」をクリックしてください。

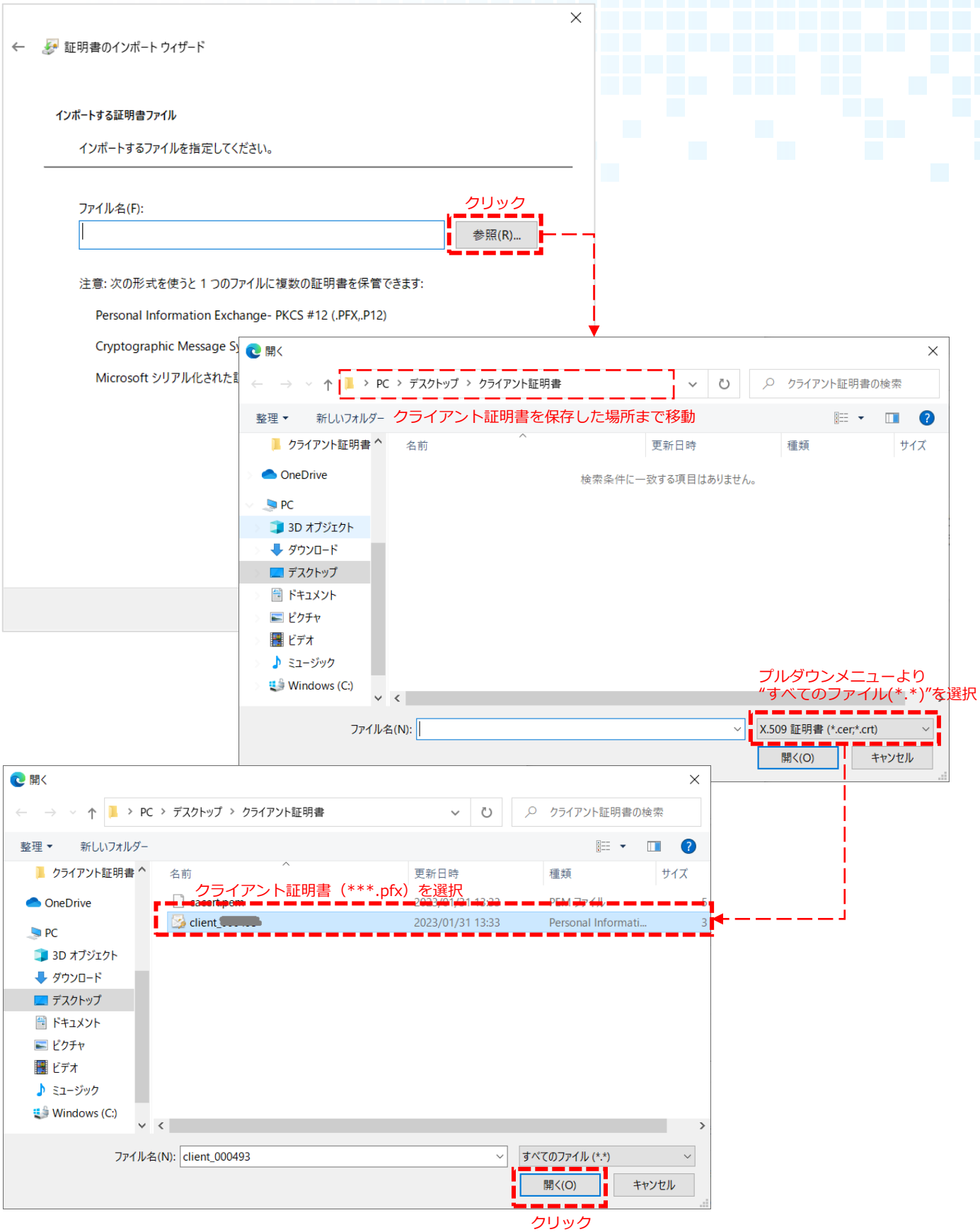


② 「個人」タブをクリックし、［インポート］ボタンをクリックすると、「証明書のインポート ウィザード」が表示されますので、［次へ］ボタンをクリックしてください。

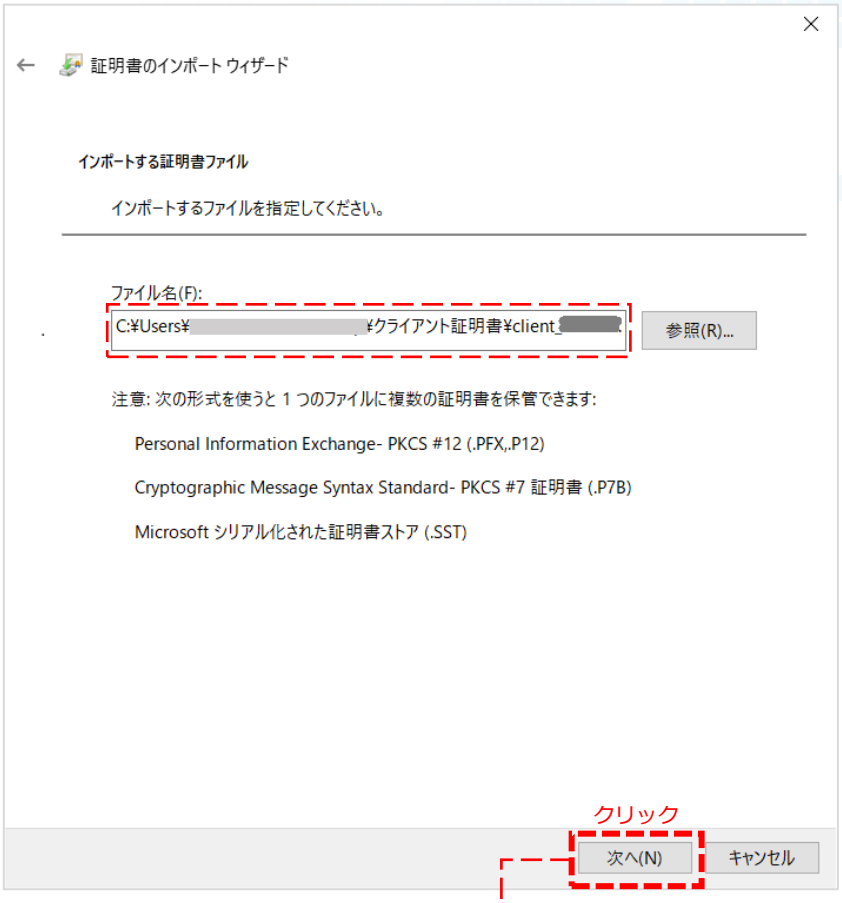


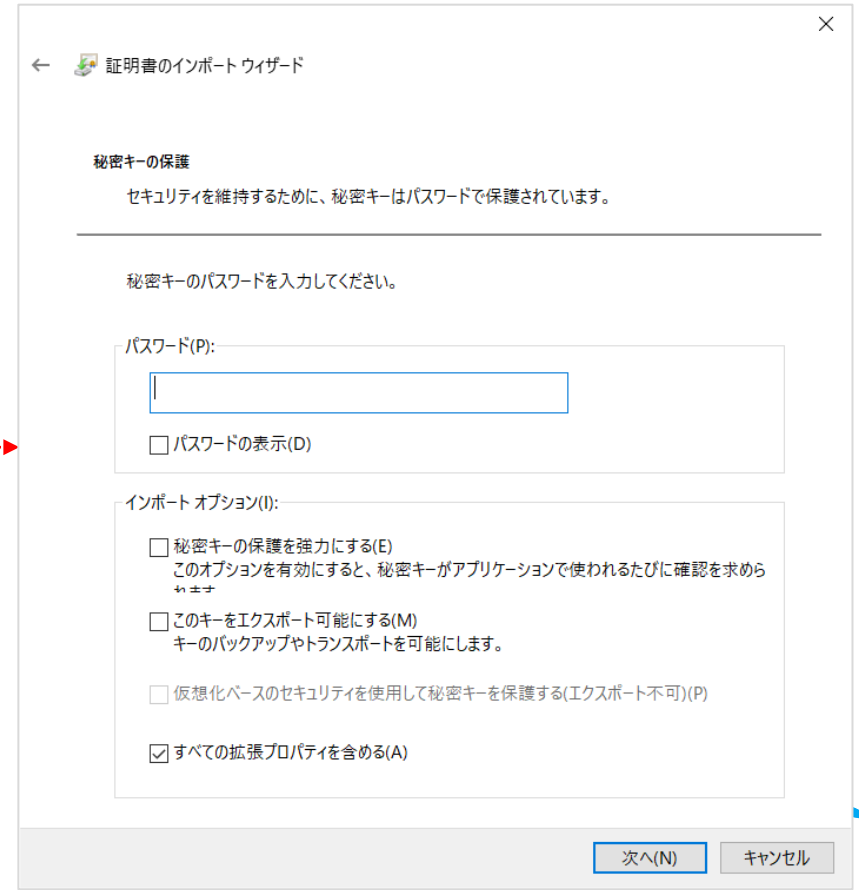


③ ［参照］ボタンをクリックし、インポートするクライアント証明書（***.pfx）を選択します。

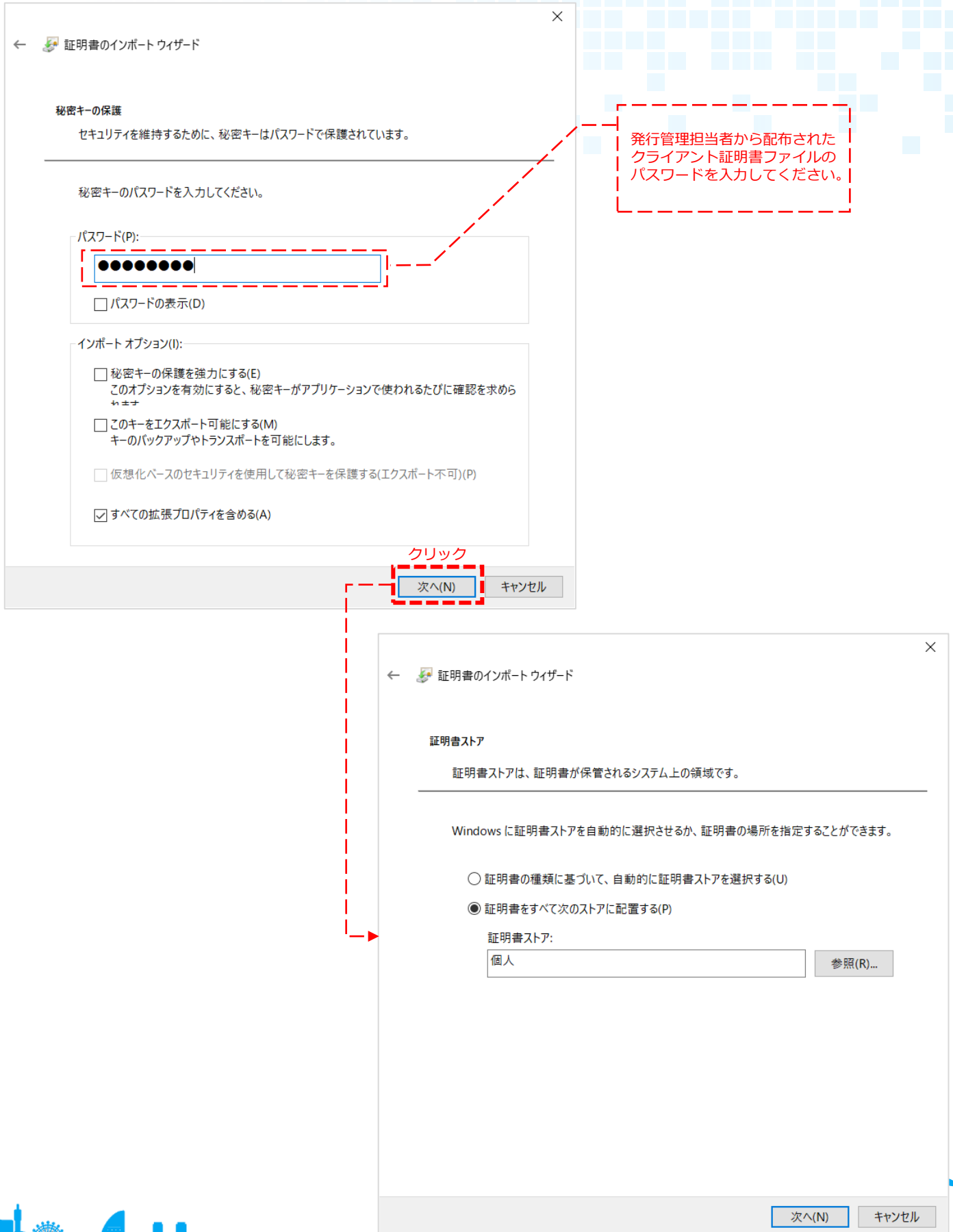


④ クライアント証明書（***.pfx）が選択されていることを確認し、［次へ］ボタンをクリックしてください。

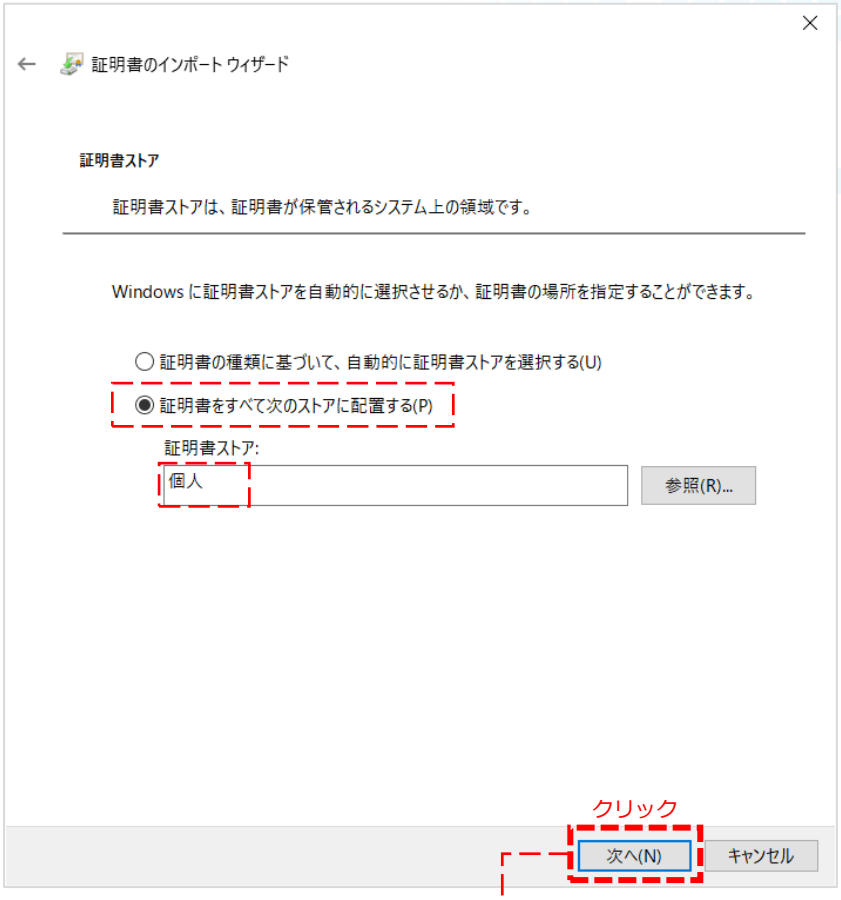




⑤ 配布された「クライアント証明書のパスワード」を「パスワード」欄に入力し、［次へ］ボタンをクリックしてください。

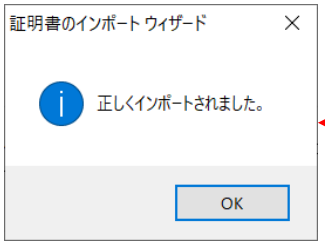


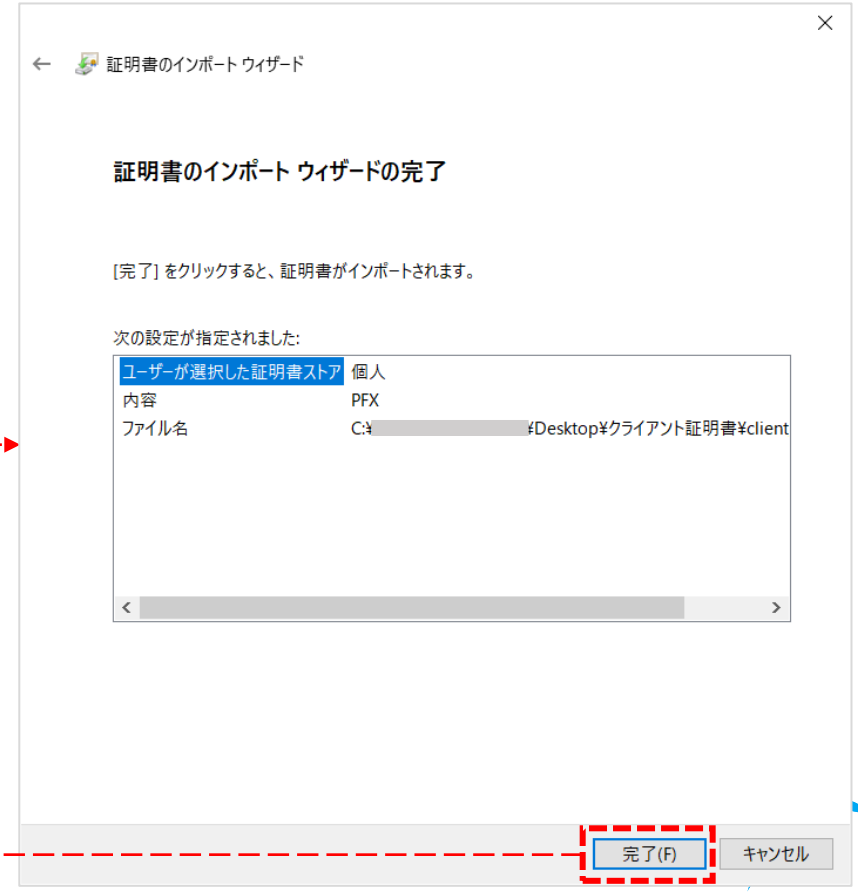
⑥ 「証明書をすべて次のストアに配置する(P)」ラジオボタンを選択、「証明書ストア：」に「個人」を選択し、［次へ］ボタンをクリックします。



完了

「証明書のインポートウィザードの完了」画面で、「完了」をクリックすると、クライアント証明書（***.pfx）が登録されます。





03 Mozilla Firefoxをご利用の場合

※ここでは、Mozilla Firefox バージョン109を例に説明します。

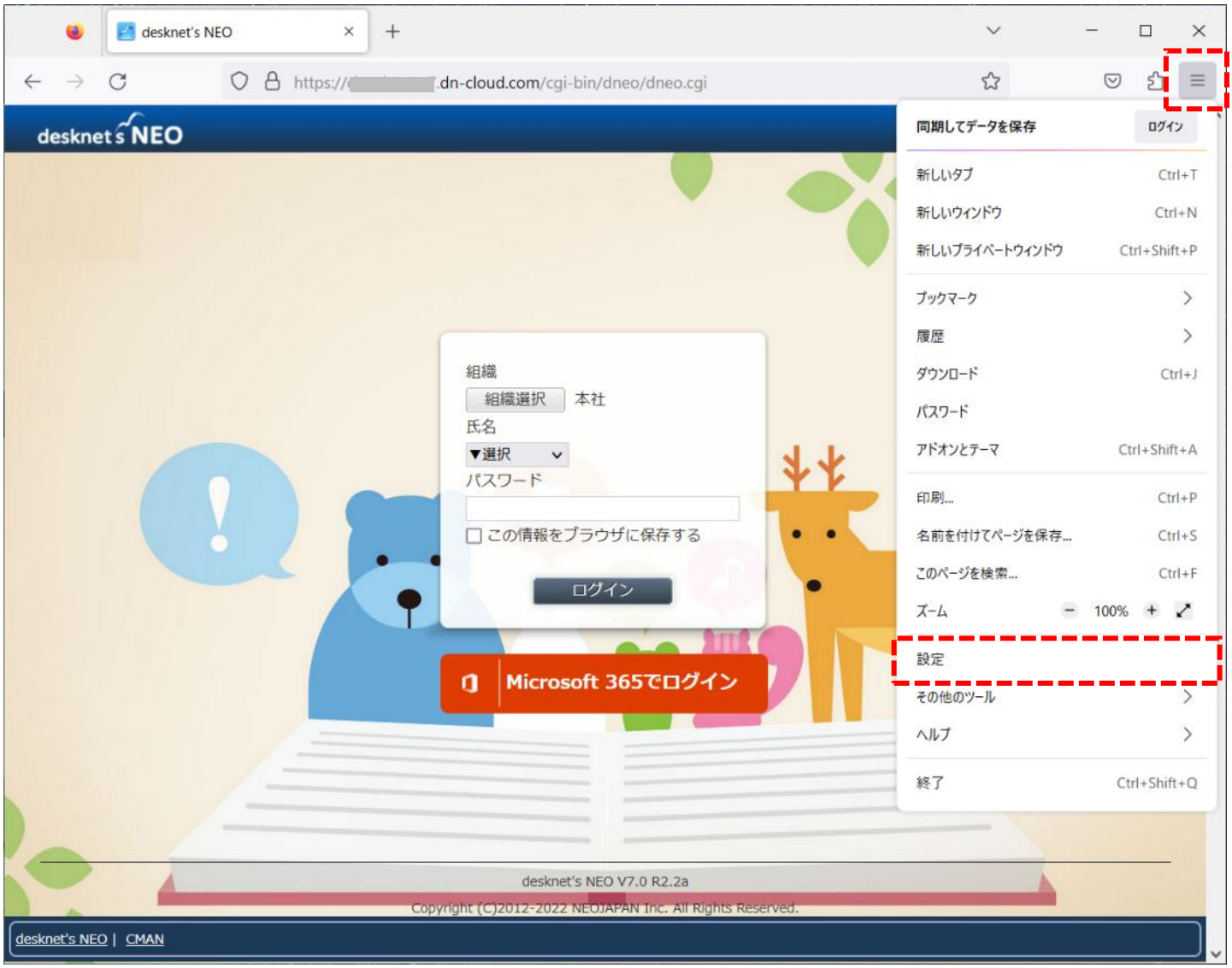
1. クライアント認証サービス用のファイルの準備

発行管理担当者から配布された、下記ファイルをご利用端末の任意の場所に保存します。

- CA証明書ファイル（cacert.pem）
- クライアント証明書ファイル（***.pfx）
- 配布されたクライアント証明書ファイルのパスワード

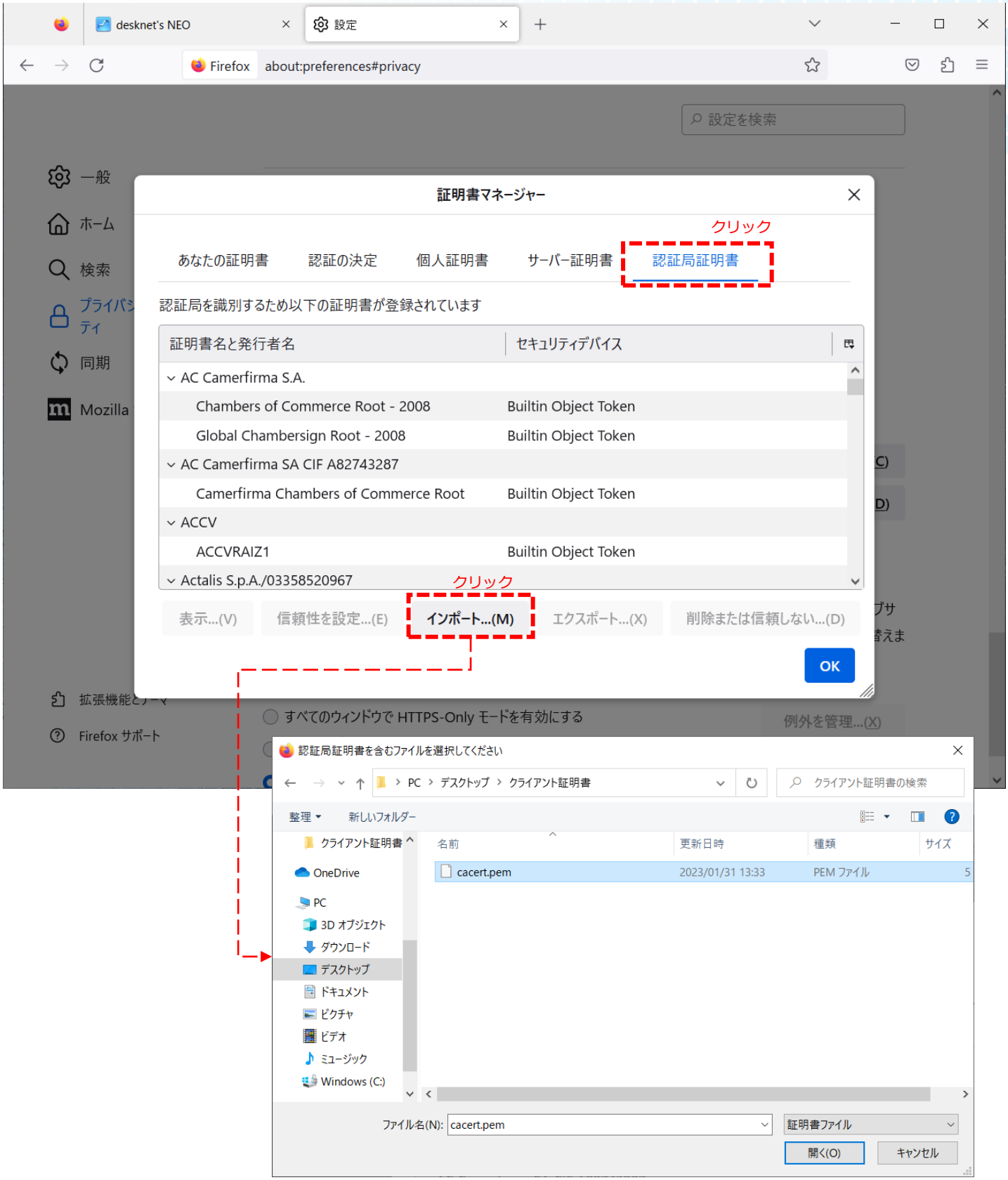
2. CA証明書（cacert.pem）のインストール

① Mozilla Firefoxを立ち上げ、≡（アプリケーションメニュー）→「設定」の順にクリックします。

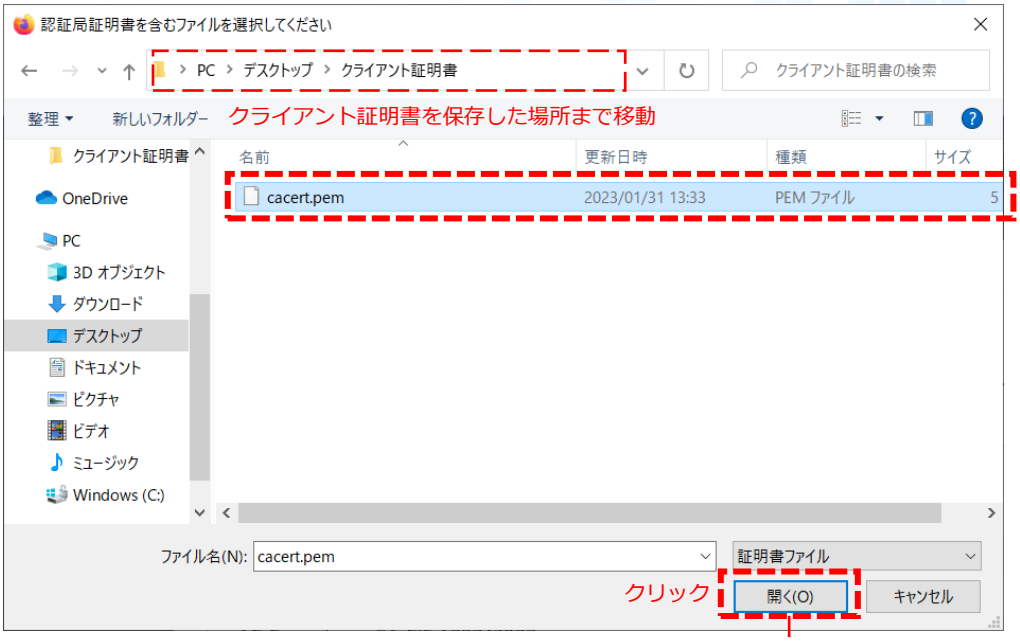


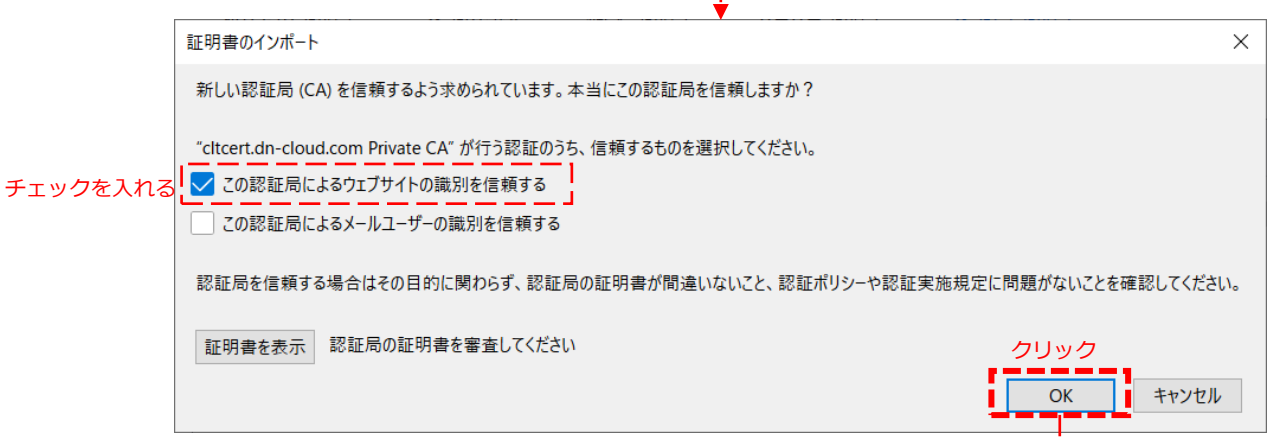
② 設定画面のタブが開きますので、メニューより「プライバシーとセキュリティ」を選択。
画面を項目「セキュリティー」までスクロールし［証明書の表示…］ボタンをクリックしてください。

③ 「証明局証明書」タブを選択し、［インポート］ボタンをクリックしてください。



④ インポートするCA証明書（cacert.pem）を選択し、［開く］ボタンをクリックすると、「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」にチェックを入れ、［OK］ボタンをクリックしてください。





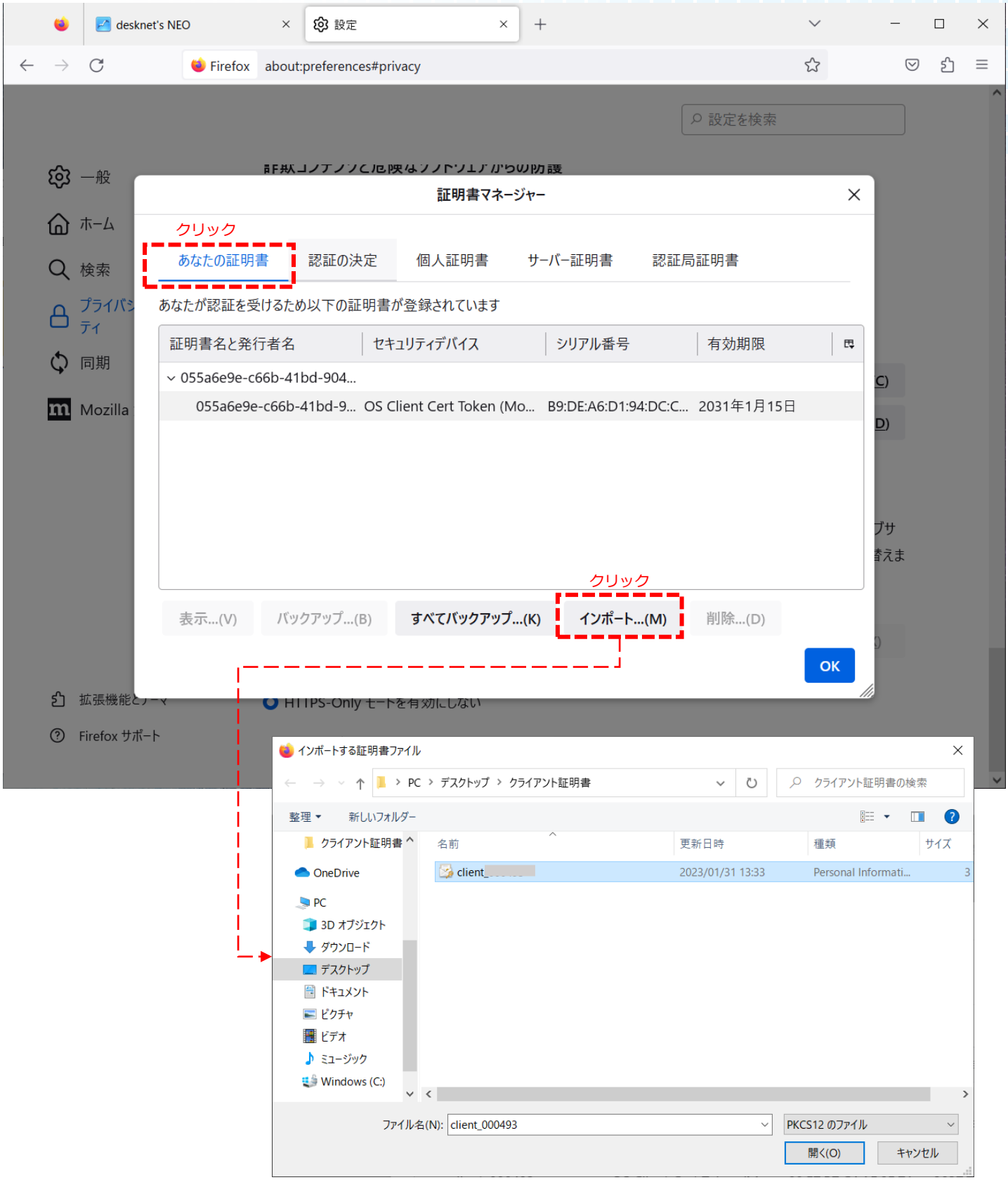
完了

「OK」をクリックしインポートが完了すると、③の画面（証明書マネージャー）一覧にCA証明書（cacert.pem）が登録されます。

3. クライアント証明書ファイル（*.pfx）のインストール

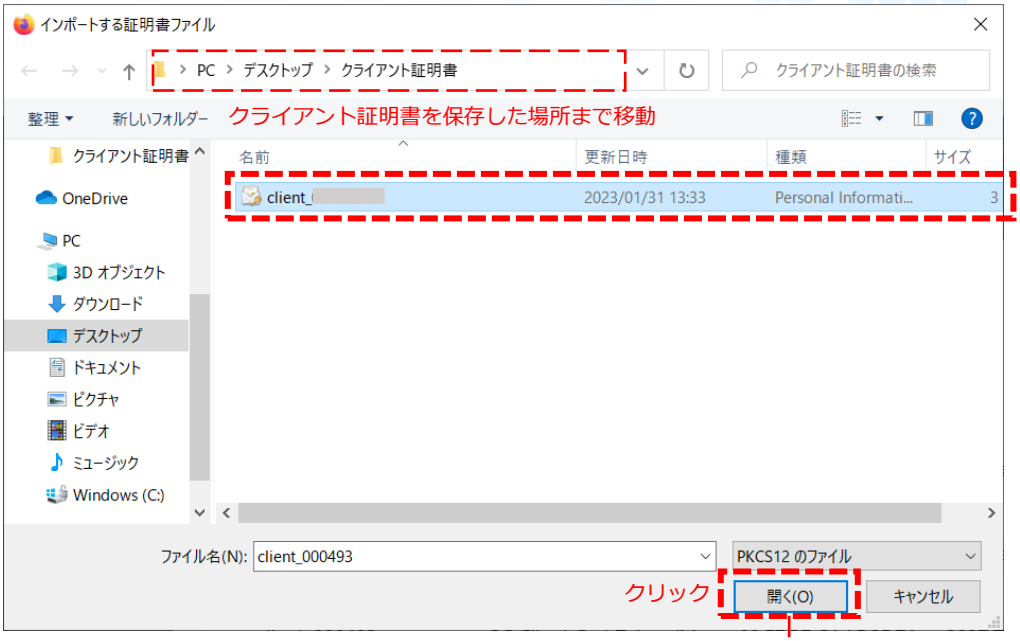
① ≡（アプリケーションメニュー）→「設定」→設定画面タブのメニューより「プライバシーとセキュリティ」→項目「セキュリティー」までスクロールし［証明書の表示…］ボタンをクリックしてください。

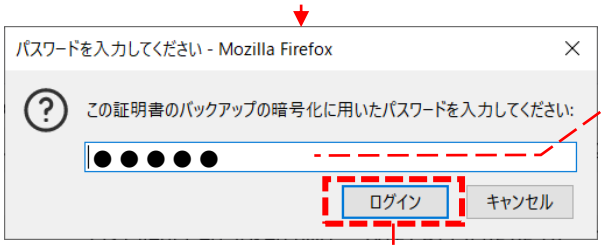
② 「あなたの証明書」タブを選択し、［インポート］ボタンをクリックしてください。



03　Mozilla Firefoxをご利用の場合

③ インポートするインポートするクライアント証明書（***.pfx）を選択し、［開く］ボタンをクリックするとパスワードの入力を求められますので、配布された「クライアント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てください。





発行管理担当者から配布されたクライアント証明書ファイルのパスワードを入力してください。

完了

「ログイン」をクリックしインポートが完了すると、②のクライアント証明書（***.pfx）が登録されます。

04 iPhone(iOS)をご利用の場合

※ここでは、iOS 15以降を例に説明します。

1. クライアント認証サービス用のファイルの準備

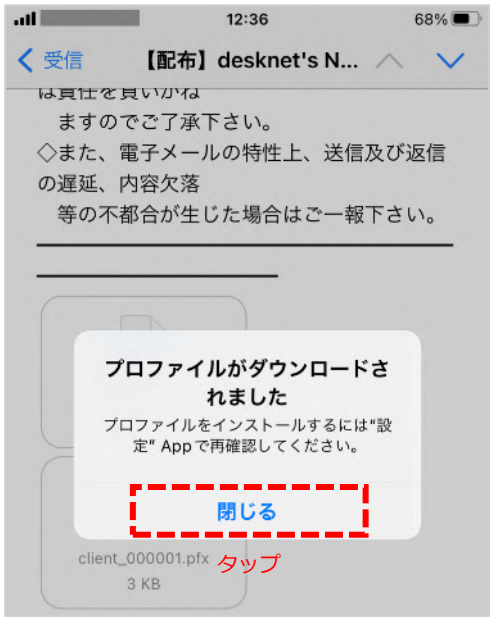
発行管理担当者から配布された、下記ファイルをご利用のiPhoneにメール等で送付します。

- CA証明書ファイル（cacert.pem）
- クライアント証明書ファイル（***.pfx）
- 配布されたクライアント証明書ファイルのパスワード

2. CA証明書（cacert.pem）のインストール

① ご利用のiPhoneに送付したメールを開き、添付されているCA証明書（cacert.pem）をタップします。

② ダウンロードが完了するとメッセージが表示されるので、「閉じる」をタップします。



③ iPhoneの「設定」アイコン開き、
「一般」をタップします。

④ 「一般」画面をスクロールし、
「VPNとデバイス管理」をタップします。

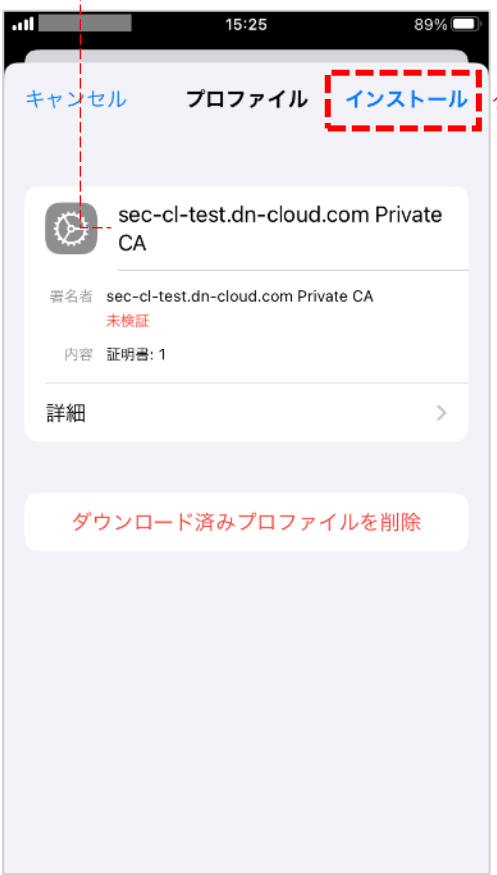
●iOS 13の場合
「VPNとデバイス管理」はメニューにございません。
「プロファイル」を選択ください。

●iOS 14の場合
「VPNとデバイス管理」はメニューにございません。
「プロファイルとデバイス管理」を選択ください。

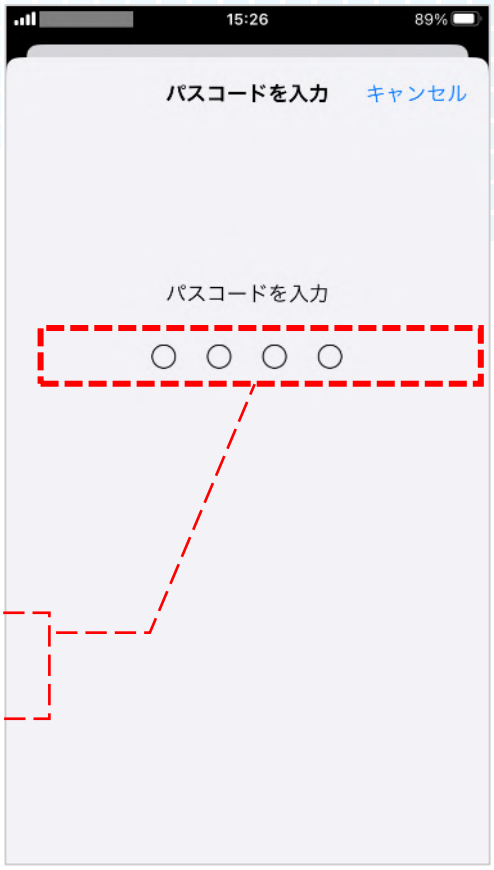
⑤ 項目「ダウンロード済みプロファイル」にダウンロードしたCA証明書（cacert.pem）が表示されているのでタップします。

sec-貴社環境のサブドメイン.dn-cloud.com Private CA
と表記されています。

⑥ 「インストール」をタップします。



⑦ 端末のセキュリティ設定によっては、
パスコードなどを求められますので、
ご利用iPhoneのパスコードを入力します。

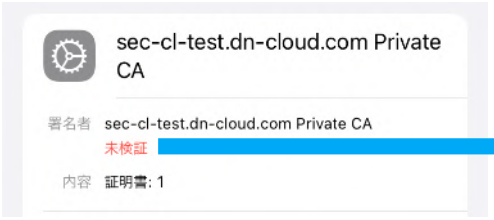


⑧ 警告メッセージが表示されますが、
そのまま「インストール」をタップします。

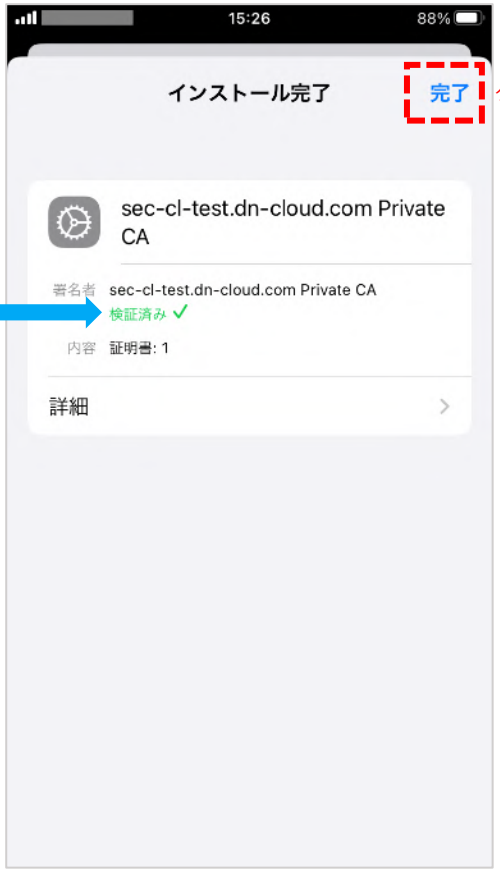
⑨ 再度「インストール」をタップします。

タップ

⑩ インストール完了画面が表示されますので、
「完了」をタップして終了です。



インストールが完了すると、
赤文字「未検証」から緑文字「検証済み」
に変わります。

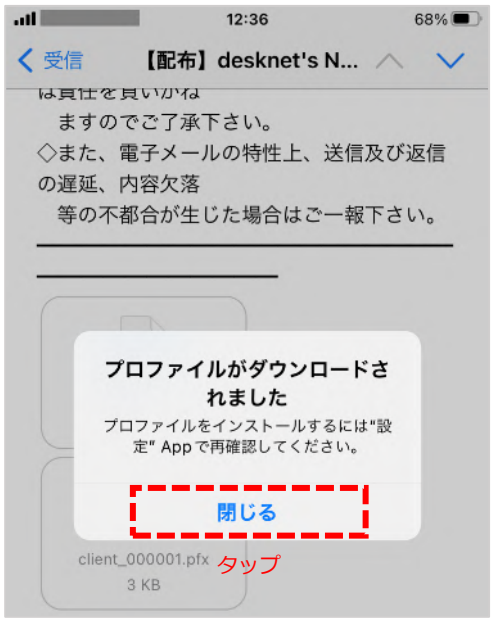


タップ

3. クライアント証明書ファイル（*.pfx）のインストール

① ご利用のiPhoneに送付したメールを開き、
添付されているクライアント証明書
（***.pfx）をタップします。

② ダウンロードが完了するとメッセージが
表示されるので、「閉じる」をタップします。



③ iPhoneの「設定」アイコン開き、
「一般」をタップします。

④ 「一般」画面をスクロールし、
「VPNとデバイス管理」をタップします。

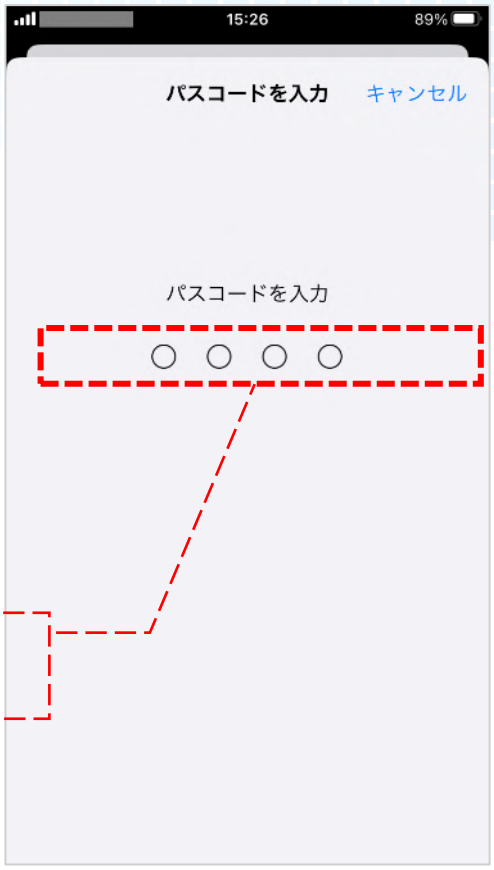
●iOS 13の場合
「VPNとデバイス管理」はメニューにございません。
「プロファイル」を選択ください。

●iOS 14の場合
「VPNとデバイス管理」はメニューにございません。
「プロファイルとデバイス管理」を選択ください。

⑤ 項目「ダウンロード済みプロファイル」にダウンロードしたクライアント証明書（***.pfx）が表示されているのでタップします。

⑥ 「インストール」をタップします。

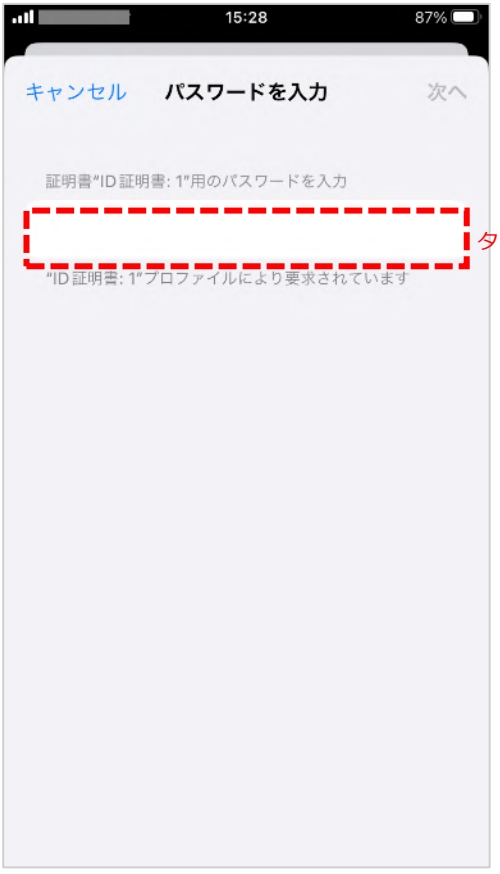
⑦ 端末のセキュリティ設定によっては、
パスコードなどを求められますので、
ご利用iPhoneのパスコードを入力します。



⑧ 警告メッセージが表示されますが、
そのまま「インストール」をタップします。

⑨ 再度「インストール」をタップします。

⑩ 証明書のパスワードを入力します。
配布された「クライアント証明書のパスワード」を入力してください。



⑪　「次へ」をタップします。

⑫　インストール完了画面が表示されるので、
「完了」をタップします。

基本的には、ここまでの手順でインストールが完了しています。

以降の手順で、著名社が赤文字「未著名」から緑文字「検証済み」に変わっているか確認してください。

⑬　「VPNデバイス管理」画面の「構成プロファイル」にインストールしたクライアント証明書（***.pfx）が表示されていますのでタップします。

⑭　「著名者」欄が「検証済み」になっていることを確認できたら完了です。

改版履歴

- 2018 年 9 月 27 日 初版
- 2023 年 2 月 03 日 2版（V2.0 R01）

株式会社ネオジャパン
〒220-8110 神奈川県横浜市西区みなとみらい 2-2-1 横浜ランドマークタワー10 階

クラウド版カスタマーセンター

0120-365-800

営業時間： 平日9:00～17:30（土日祝日、弊社指定休日を除く）

メールでのお問い合わせ

cloudsupport@desknets.com