

//////////////////// 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。



01	Microsoft Edgeをご利用の場合	3
1.	クライアント認証サービス用のファイルの準備	3
2.	CA証明書 (cacert.pem) のインストール	3
3.	クライアント証明書ファイル (*.pfx) のインストール	10
02	Google Chromeをご利用の場合	16
1.	クライアント認証サービス用のファイルの準備	16
2.	CA証明書 (cacert.pem) のインストール	16
3.	クライアント証明書ファイル (*.pfx) のインストール	24
03	Mozilla Firefoxをご利用の場合	30
1.	クライアント認証サービス用のファイルの準備	30
2.	CA証明書 (cacert.pem) のインストール	30
3.	クライアント証明書ファイル (*.pfx) のインストール	34
04	iPhone(iOS)をご利用の場合	37
1.	クライアント認証サービス用のファイルの準備	37
2.	CA証明書 (cacert.pem) のインストール	37
3.	クライアント証明書ファイル (*.pfx) のインストール	42

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。

The screenshot shows the Microsoft Edge browser interface. The address bar displays the URL `https://[redacted]dn-cloud.com/cgi-bin/dneo/dneo.cgi`. The main content area shows the desknet's NEO login page with a form for organization selection, name, and password. A red dashed box highlights the 'Settings' option in the browser's menu, which is accessed via the '...' button in the top right corner.

01 Microsoft Edgeをご利用の場合

- 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」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。

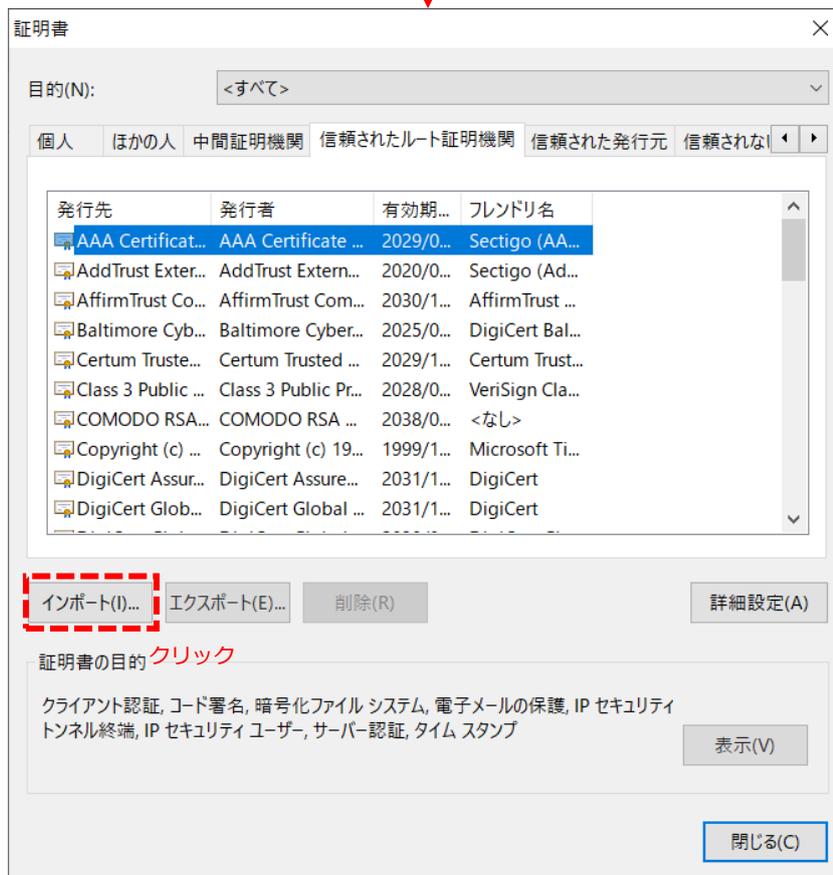
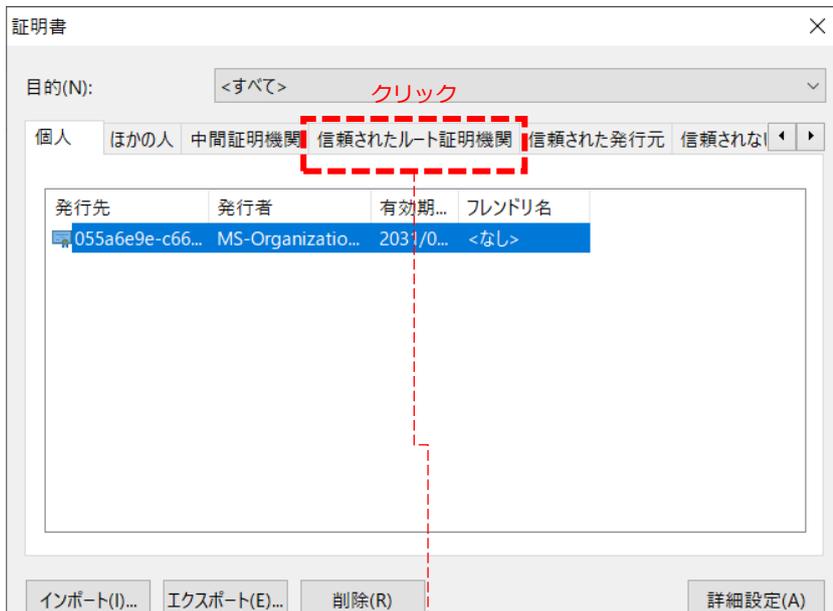
The screenshot shows the Microsoft Edge settings page at `edge://settings/privacy`. The left sidebar has '設定' (Settings) at the top, with a search box and a list of categories. 'プライバシー、検索、サービス' (Privacy, Search, Services) is highlighted with a red dashed box and labeled 'クリック' (Click). The main content area is titled 'セキュリティ' (Security) and contains several security-related settings. '証明書の管理' (Certificate Management) is highlighted with a red dashed box and labeled 'クリック' (Click). A vertical red dashed arrow on the right side of the page is labeled 'スクロール' (Scroll). Below the main settings, a '証明書' (Certificates) dialog box is open, showing a table of certificates. The table has columns for '発行先' (Issued to), '発行者' (Issued by), '有効期...' (Expiration date), and 'フレンドリ名' (Friendly name). One certificate is listed with the following details:

発行先	発行者	有効期...	フレンドリ名
055a6e9e-c66...	MS-Organizatio...	2031/0...	<なし>

At the bottom of the dialog, there are buttons for 'インポート(I)...', 'エクスポート(E)...', '削除(R)', and '詳細設定(A)'. Below the table, there is a section for '証明書の目的' (Certificate purposes) with 'クライアント認証' (Client authentication) selected and a '表示(V)' (View) button. At the very bottom of the dialog is a '閉じる(C)' (Close) button.

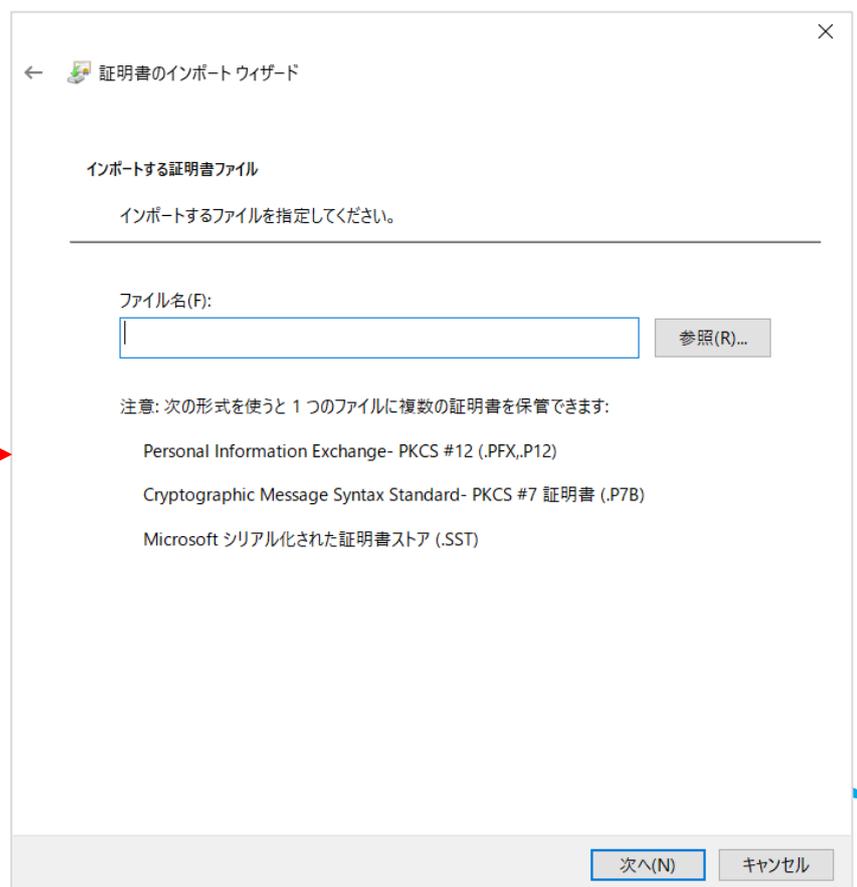
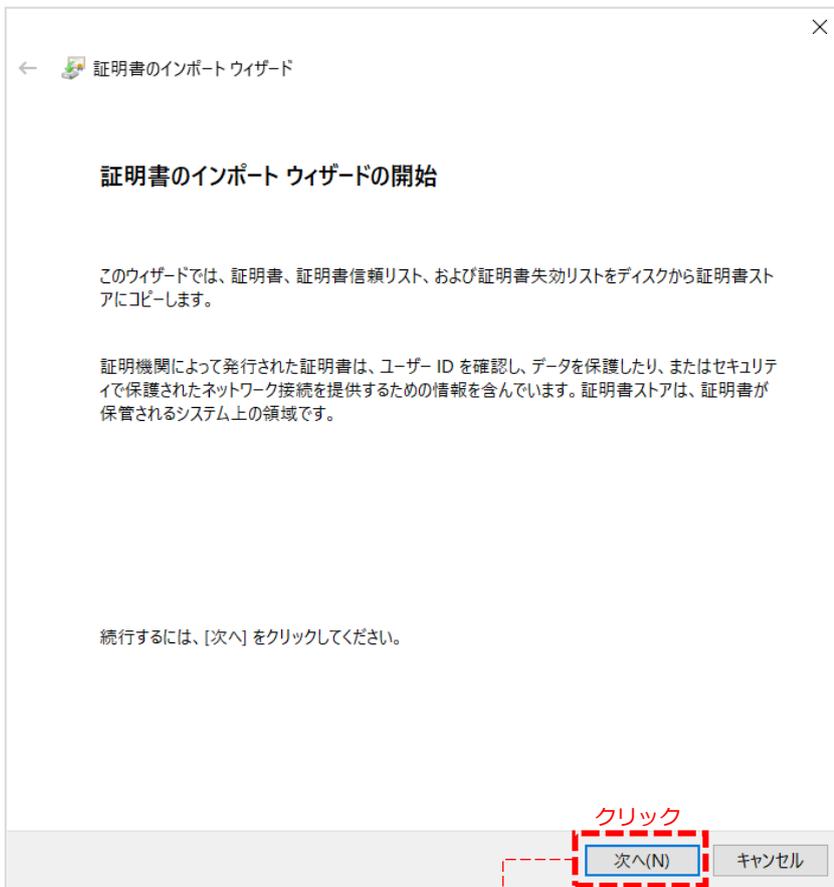
01 Microsoft Edgeをご利用の場合

- 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。



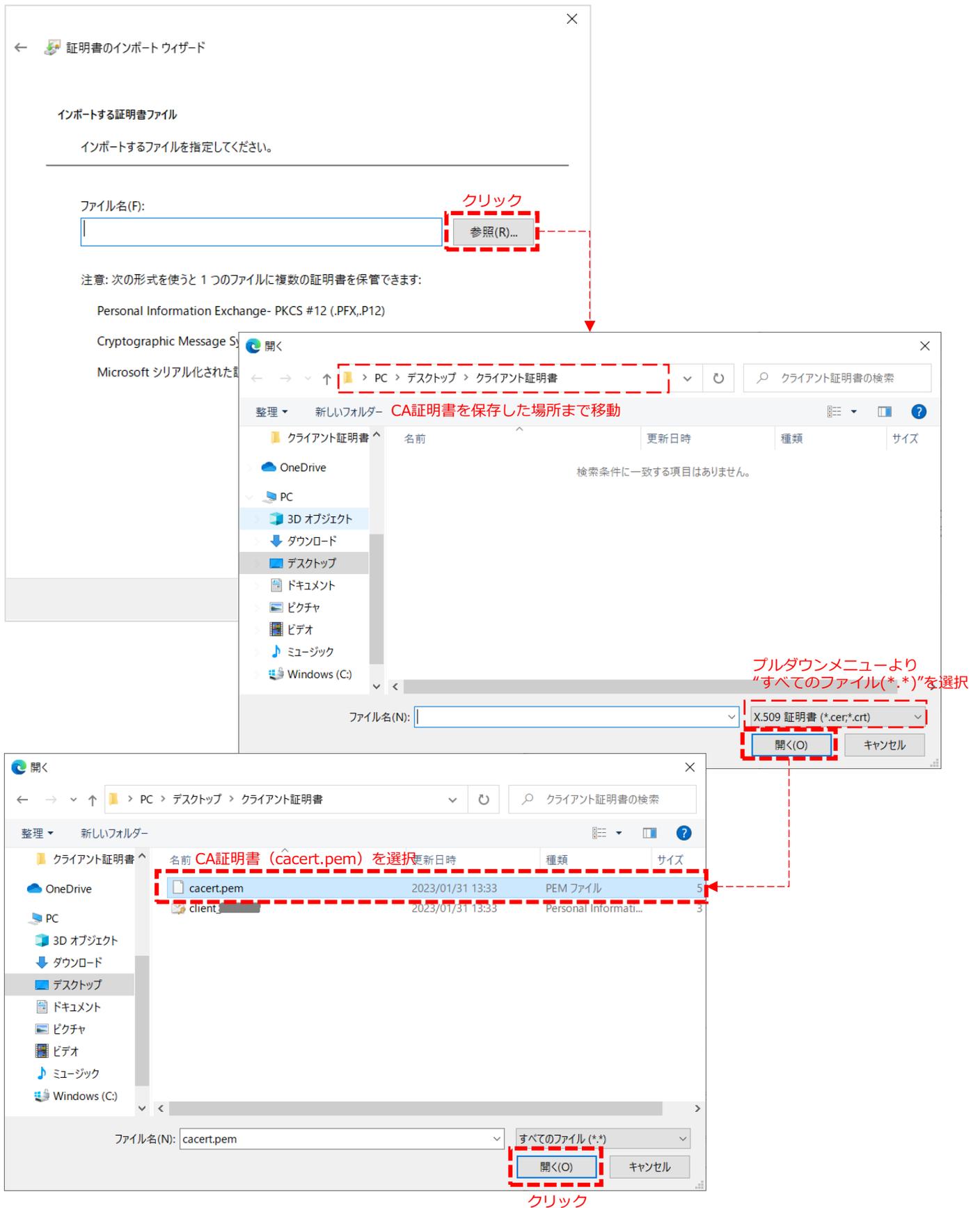
01 Microsoft Edgeをご利用の場合

- 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。



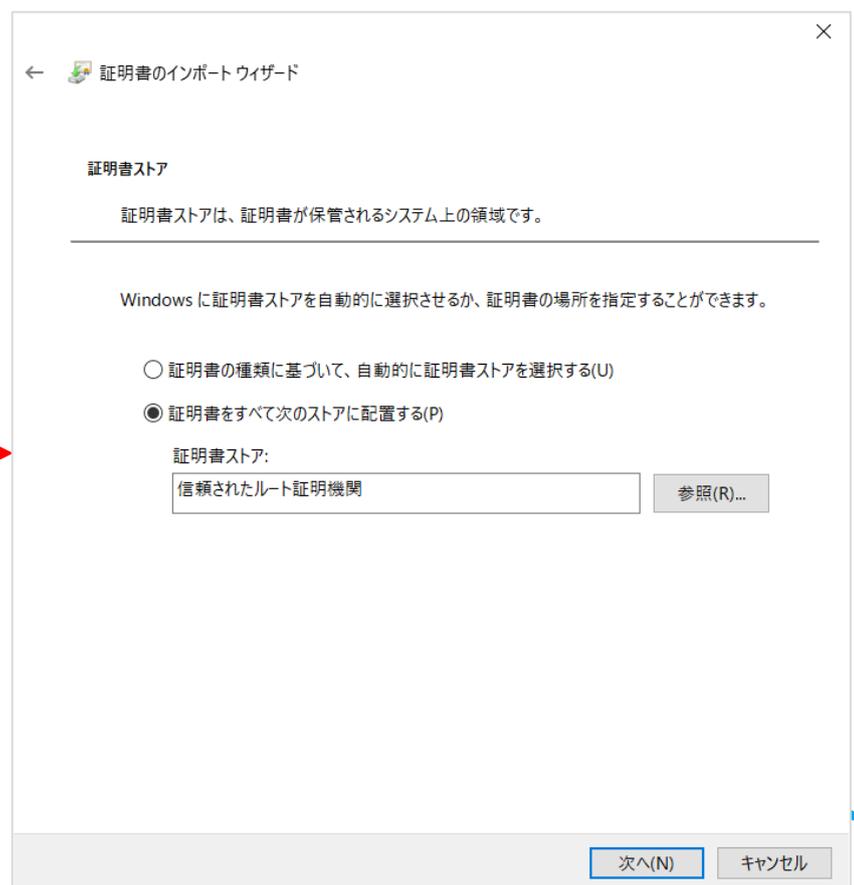
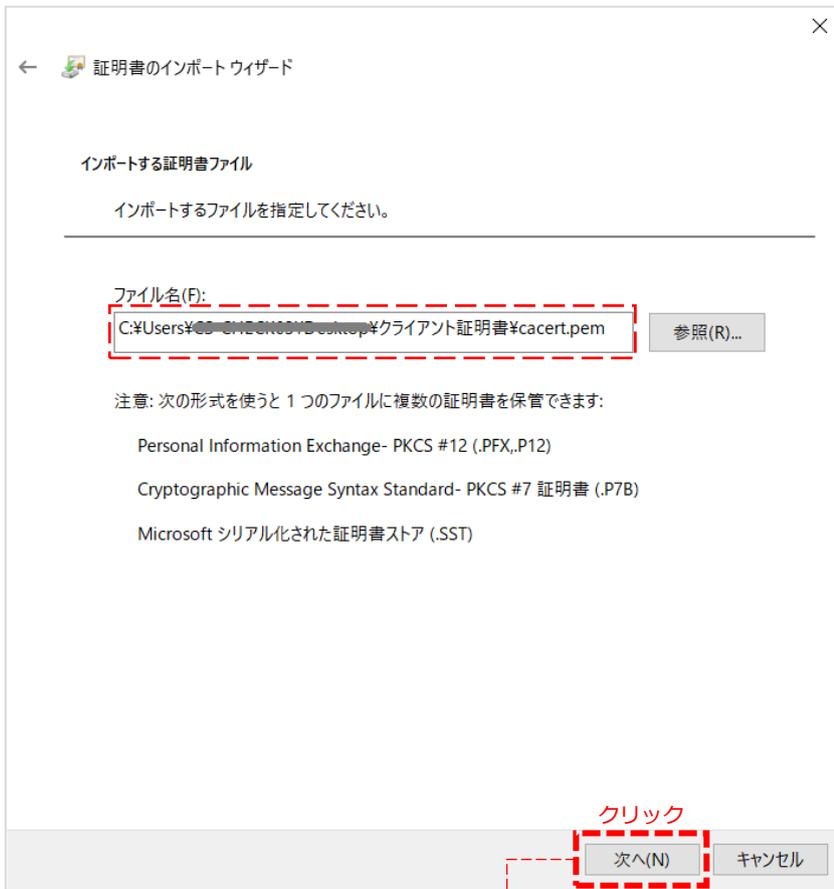
01 Microsoft Edgeをご利用の場合

- 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。



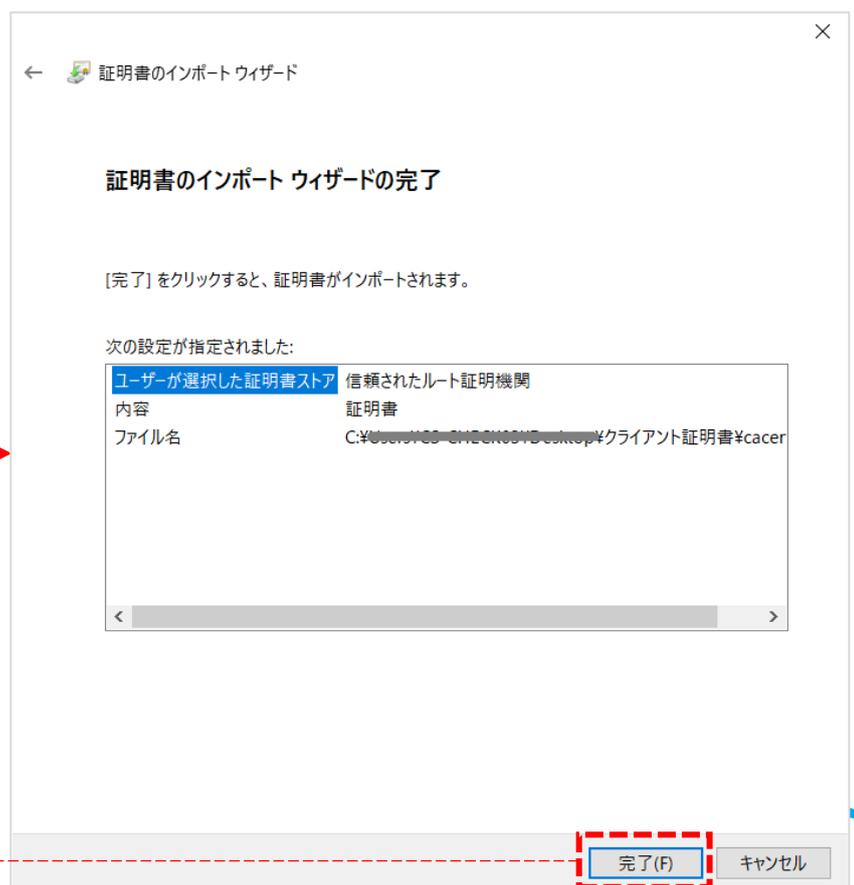
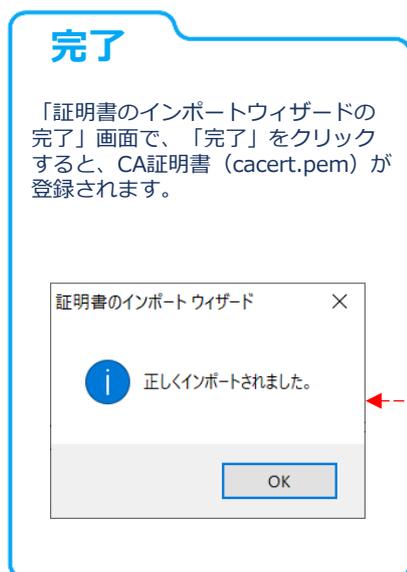
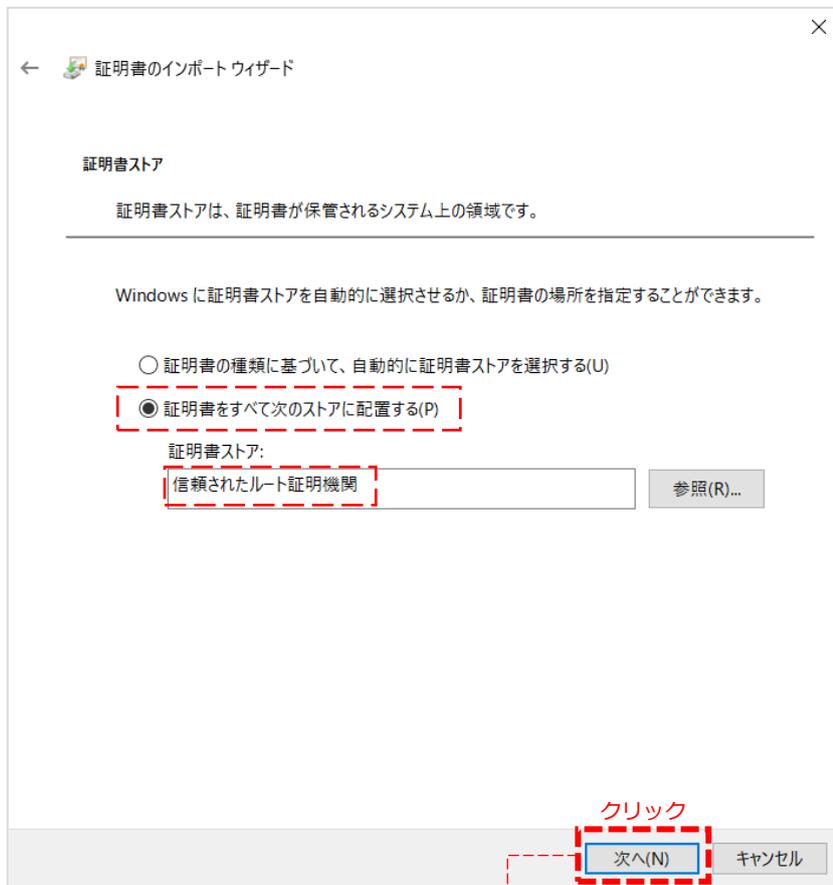
01 Microsoft Edgeをご利用の場合

- 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。



01 Microsoft Edgeをご利用の場合

- 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。



3. クライアント証明書ファイル (*.pfx) のインストール

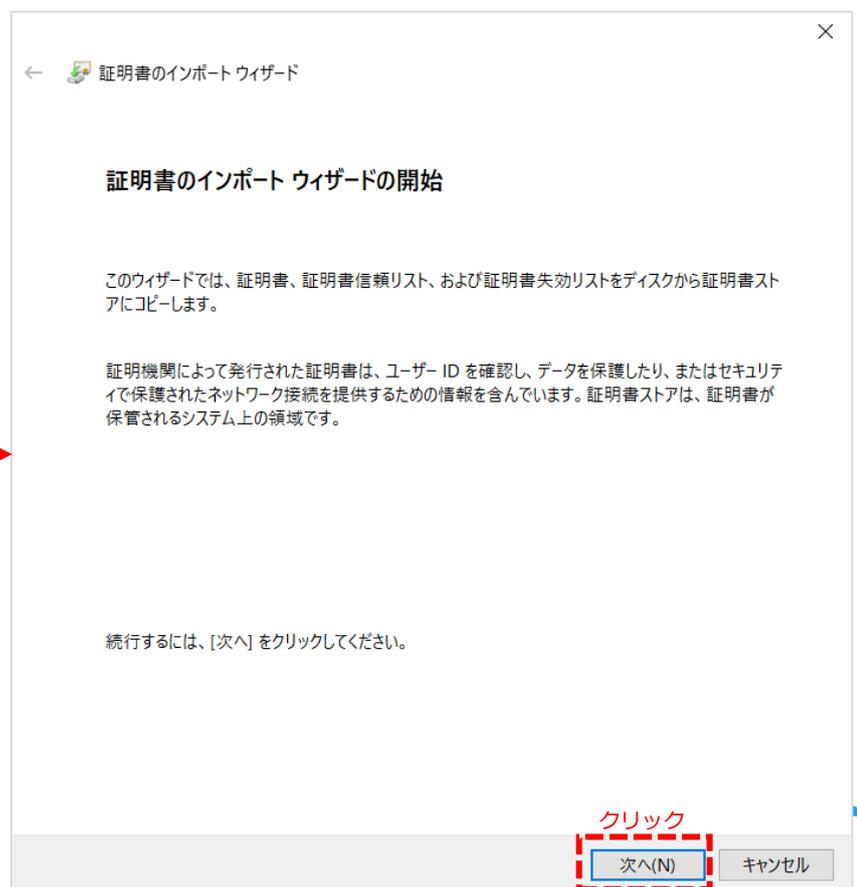
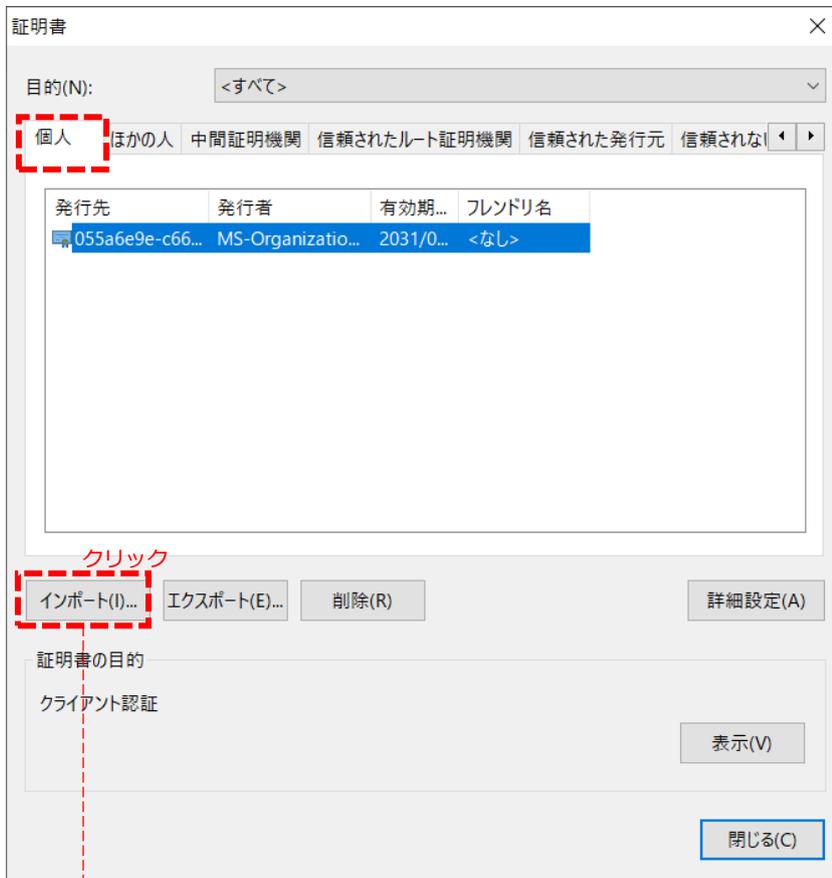
- ① … (設定など) → 「設定」 → 設定画面タブのメニューより「プライバシー、検索、サービス」を選択。
画面を項目「セキュリティ」までスクロールし「証明書の管理」をクリックしてください。

The screenshot shows the Microsoft Edge settings page in Japanese. The left sidebar has '設定' (Settings) at the top, with a search box and a list of categories. 'プライバシー、検索、サービス' (Privacy, Search, Services) is highlighted with a red dashed box and labeled 'クリック' (Click). The main content area is 'セキュリティ' (Security), with '証明書の管理' (Certificate Management) highlighted by a red dashed box and labeled 'クリック' (Click). A vertical red dashed arrow on the right side is labeled 'スクロール' (Scroll). Below the main content, a '証明書' (Certificate) dialog box is open, showing a table of certificates. The table has columns for '発行先' (Issued to), '発行者' (Issued by), '有効期...' (Valid until), and 'フレンドリ名' (Friendly name). One certificate is listed with '発行先' '055a6e9e-c66...' and '発行者' 'MS-Organizatio...'. Below the table are buttons for 'インポート(I)...', 'エクスポート(E)...', '削除(R)', and '詳細設定(A)'. At the bottom, there are buttons for '閉じる(C)' (Close) and '表示(V)' (View).

発行先	発行者	有効期...	フレンドリ名
055a6e9e-c66...	MS-Organizatio...	2031/0...	<なし>

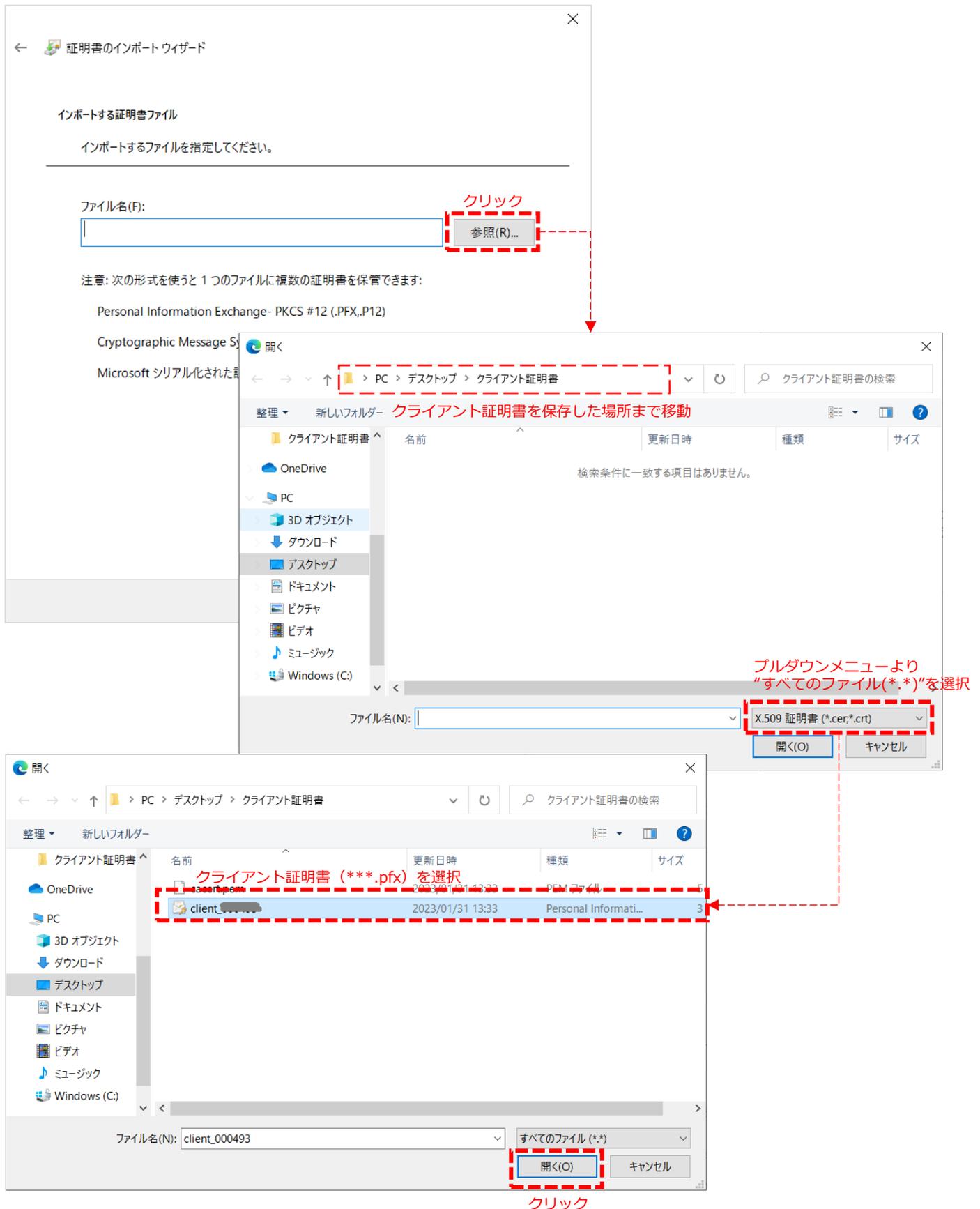
01 Microsoft Edgeをご利用の場合

- 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。



01 Microsoft Edgeをご利用の場合

- 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。



01 Microsoft Edgeをご利用の場合

- 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。

← 証明書のインポートウィザード

インポートする証明書ファイル

インポートするファイルを指定してください。

ファイル名(F):
C:\Users\%OS-USER%\AppData\Local\Microsoft\Edge\%クライアント証明書%client_...

参照(R)...

注意: 次の形式を使うと 1 つのファイルに複数の証明書を保管できます:

- Personal Information Exchange- PKCS #12 (.PFX,.P12)
- Cryptographic Message Syntax Standard- PKCS #7 証明書 (.P7B)
- Microsoft シリアル化された証明書ストア (.SST)

クリック

次へ(N) キャンセル

← 証明書のインポートウィザード

秘密キーの保護

セキュリティを維持するために、秘密キーはパスワードで保護されています。

秘密キーのパスワードを入力してください。

パスワード(P):

パスワードの表示(D)

インポート オプション(O):

- 秘密キーの保護を強力にする(E)
このオプションを有効にすると、秘密キーがアプリケーションで使われるたびに確認を求めら
れます。
- このキーをエクスポート可能にする(M)
キーのバックアップやトランスポートを可能にします。
- 仮想化ベースのセキュリティを使用して秘密キーを保護する(エクスポート不可)(P)
- すべての拡張プロパティを含める(A)

次へ(N) キャンセル

01 Microsoft Edgeをご利用の場合

- 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。

← 証明書のインポートウィザード

秘密キーの保護

セキュリティを維持するために、秘密キーはパスワードで保護されています。

秘密キーのパスワードを入力してください。

パスワード(P):

パスワードの表示(D)

インポート オプション(I):

- 秘密キーの保護を強力にする(E)
このオプションを有効にすると、秘密キーがアプリケーションで使われるたびに確認を求められます。
- このキーをエクスポート可能にする(M)
キーのバックアップやトランスポートを可能にします。
- 仮想化ベースのセキュリティを使用して秘密キーを保護する(エクスポート不可)(P)
- すべての拡張プロパティを含める(A)

クリック

次へ(N) キャンセル

← 証明書のインポートウィザード

証明書ストア

証明書ストアは、証明書が保管されるシステム上の領域です。

Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。

- 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(U)
- 証明書をすべて次のストアに配置する(P)

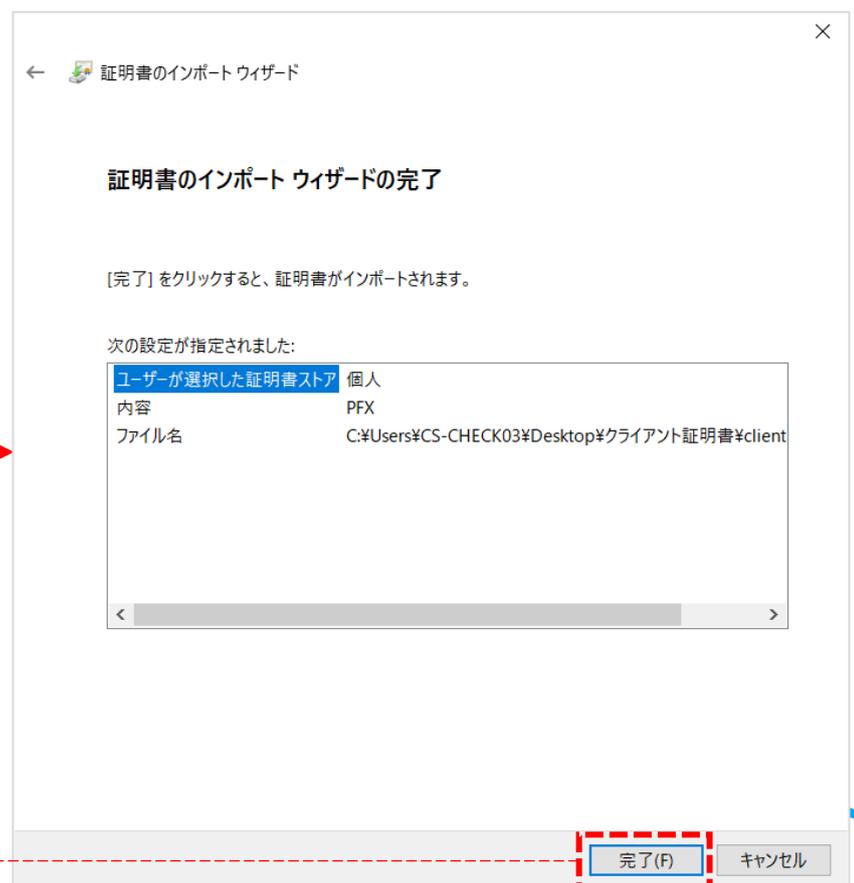
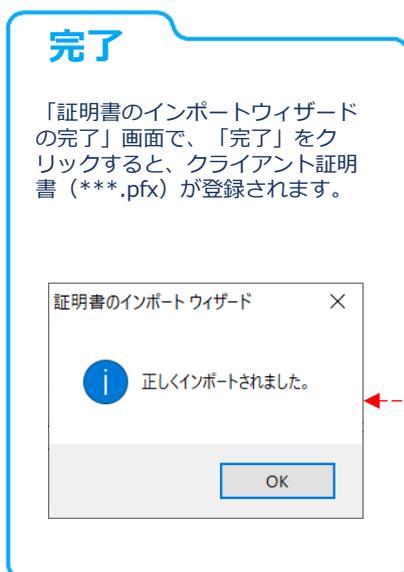
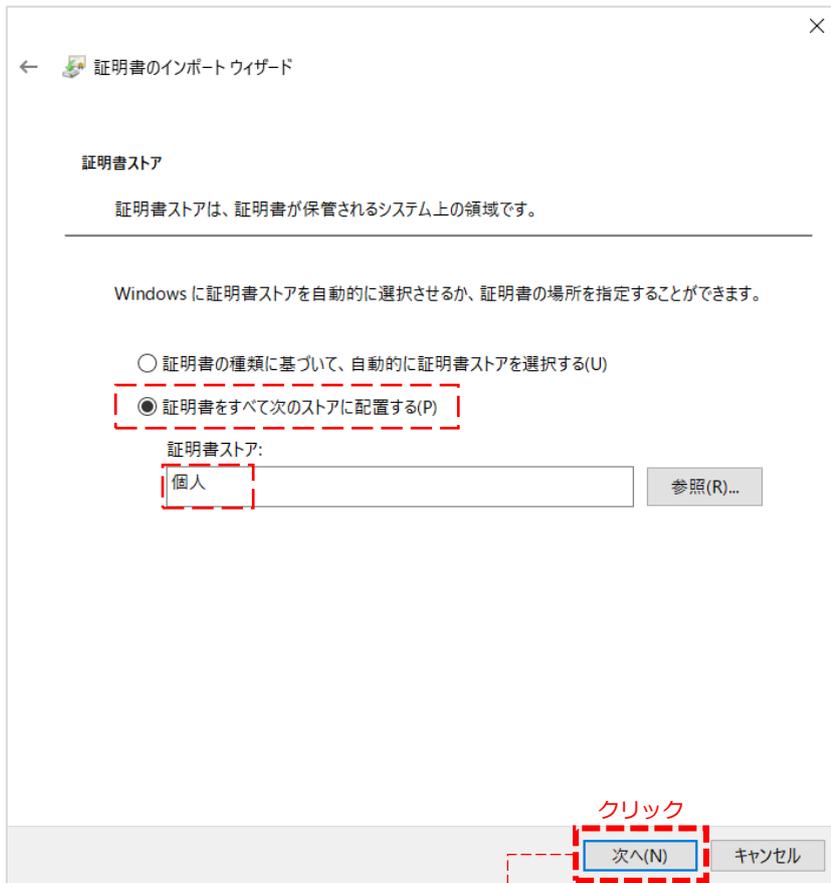
証明書ストア:

個人 参照(R)...

次へ(N) キャンセル

01 Microsoft Edgeをご利用の場合

- 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。



Google Chromeをご利用の場合

※ここでは、Google Chrome バージョン131を例に説明します。

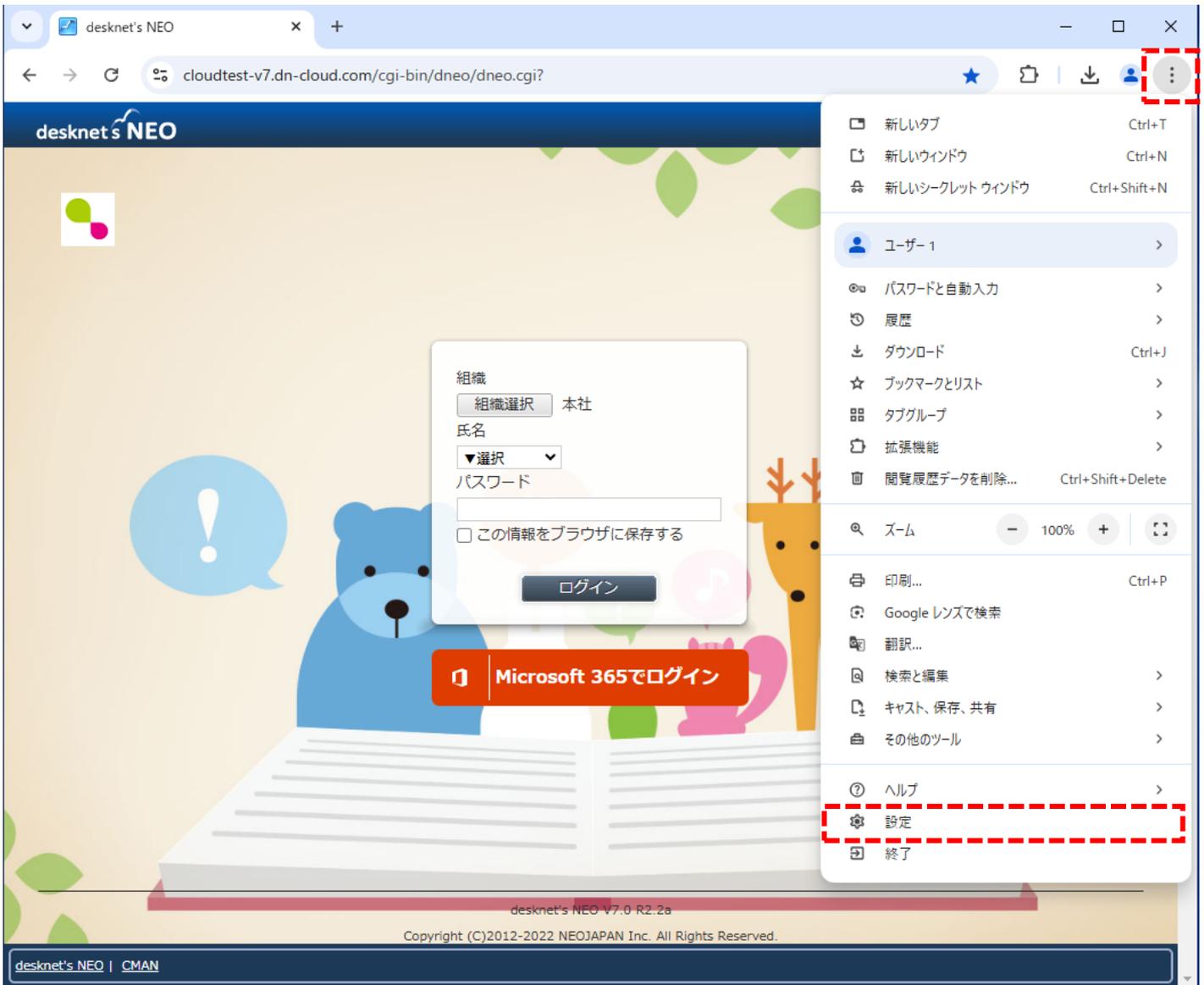
1. クライアント認証サービス用のファイルの準備

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

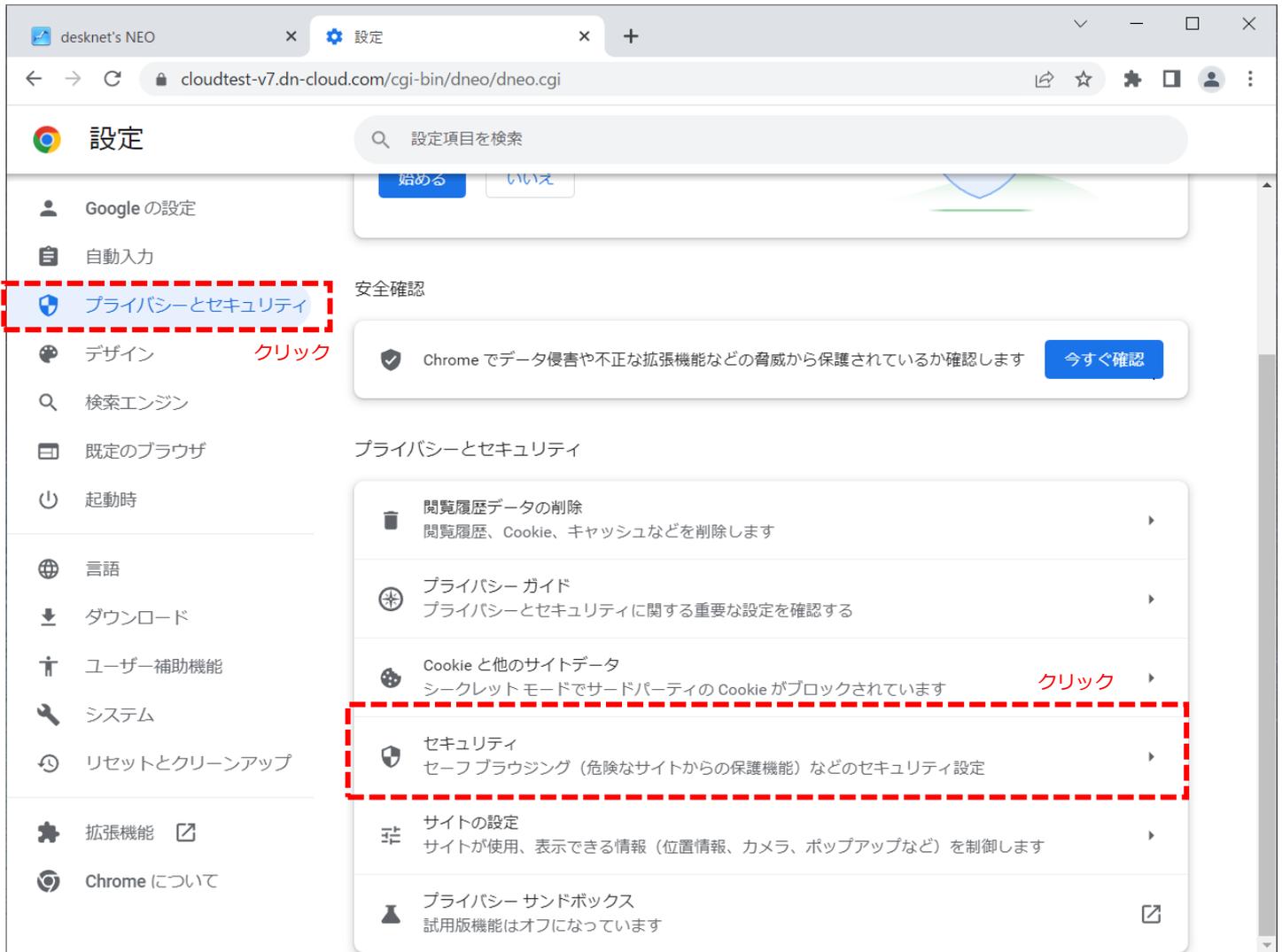
2. CA証明書 (cacert.pem) のインストール

- 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。



02 Google Chromeをご利用の場合

- 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。



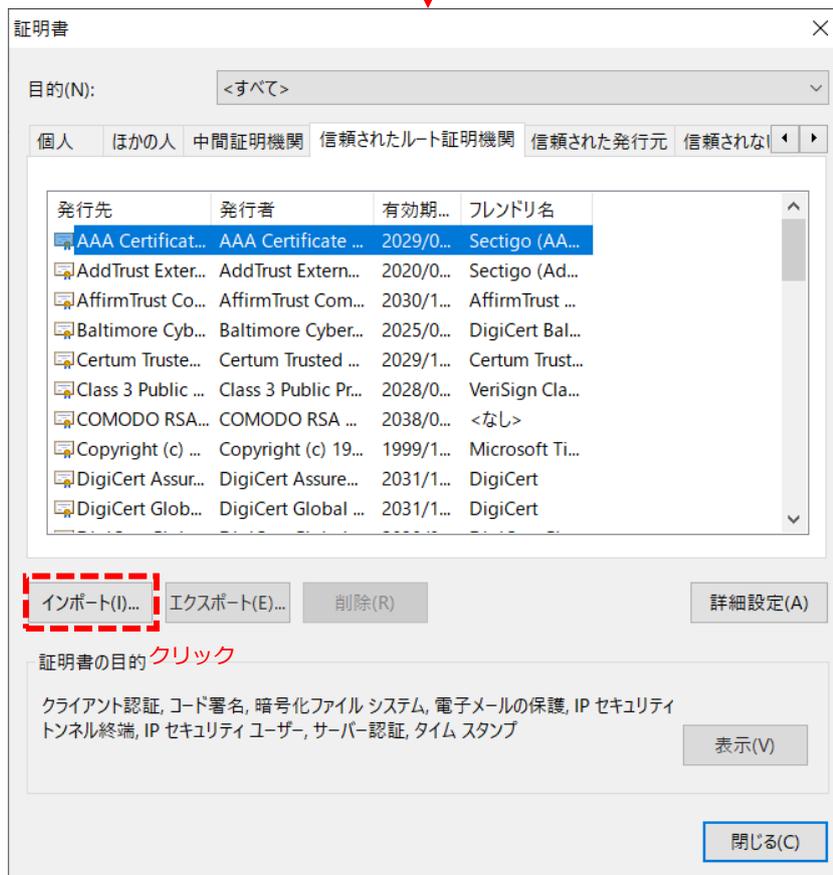
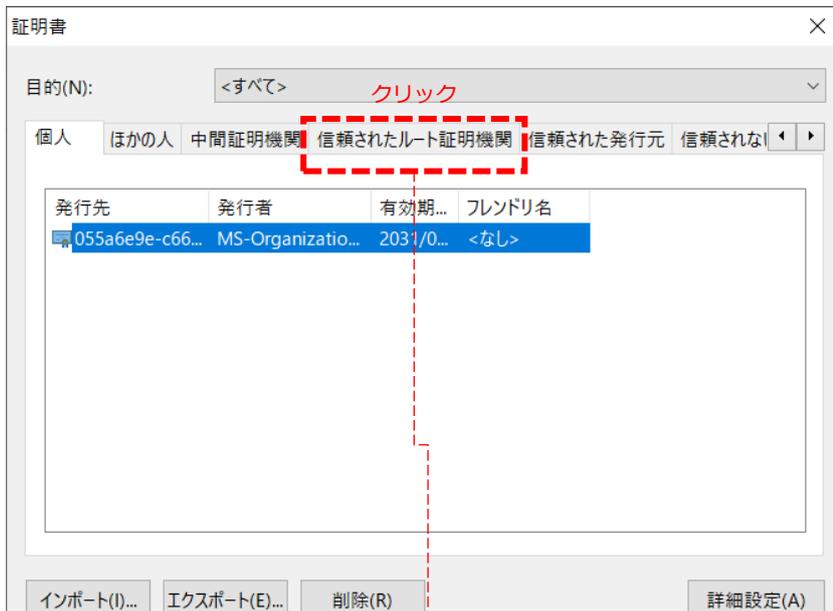
02 Google Chromeをご利用の場合

- 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「証明書の管理」をクリックしてください。次に「証明書マネージャ」の画面に遷移しますので、「Windows からインポートした証明書を管理する」をクリックしてください。

The image shows two screenshots from a Google Chrome browser window. The top screenshot is the 'Settings - Security' page (chrome://settings/security). The left sidebar shows 'Privacy and Security' selected. The main content area is scrolled down, with a red dashed box highlighting the 'Certificates' option. A red arrow labeled 'スクロール' (Scroll) points downwards. A red arrow labeled 'クリック' (Click) points to the 'Certificates' option. The bottom screenshot is the 'Certificate Manager' page (chrome://certificate-manager). The left sidebar shows 'Local Certificates' selected. The main content area shows 'Local Certificates' with a toggle for 'Use local certificates imported from the operating system' turned on. A red dashed box highlights the 'Windows certificates imported from Windows' section, and a red arrow labeled 'クリック' (Click) points to the 'Manage Windows certificates imported from Windows' option.

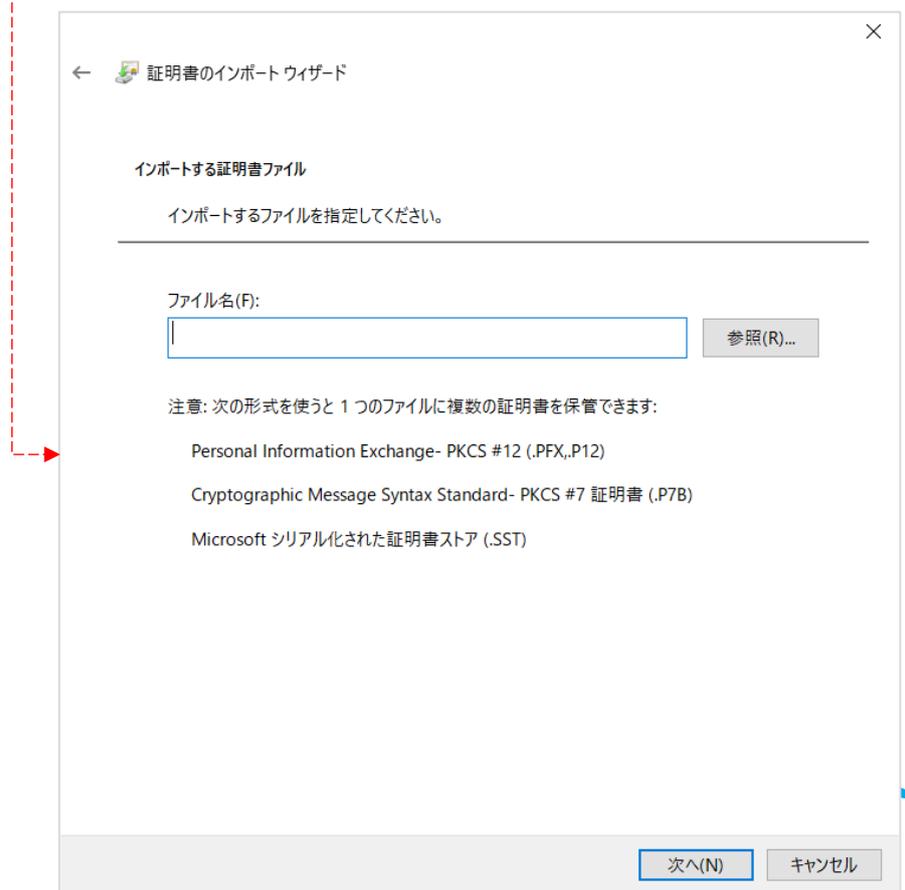
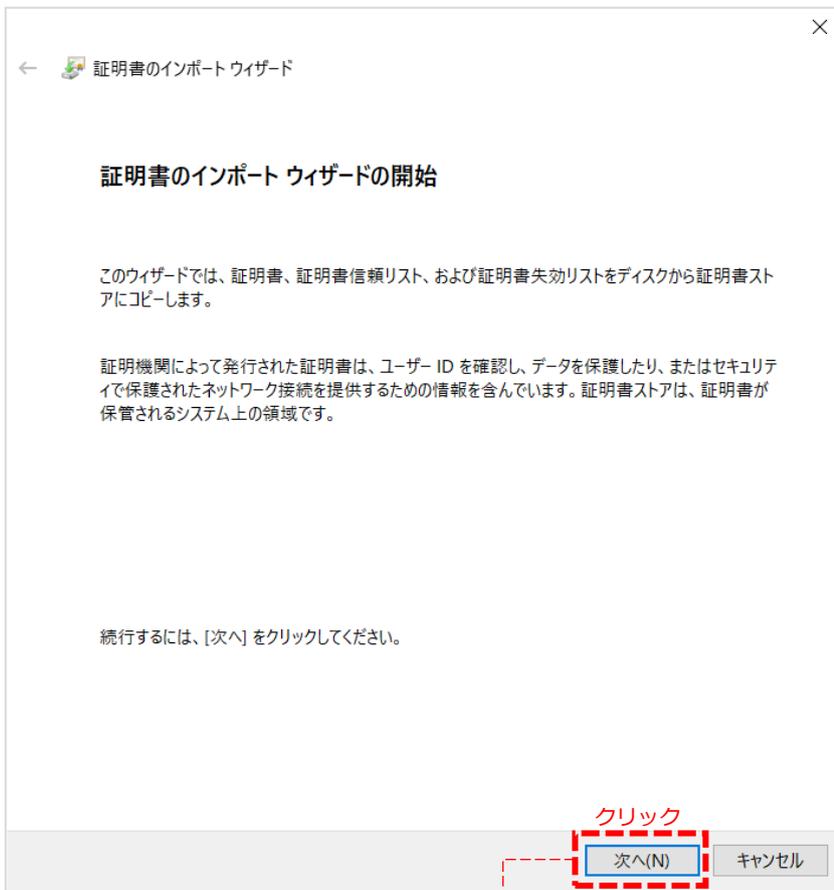
02 Google Chromeをご利用の場合

- 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。



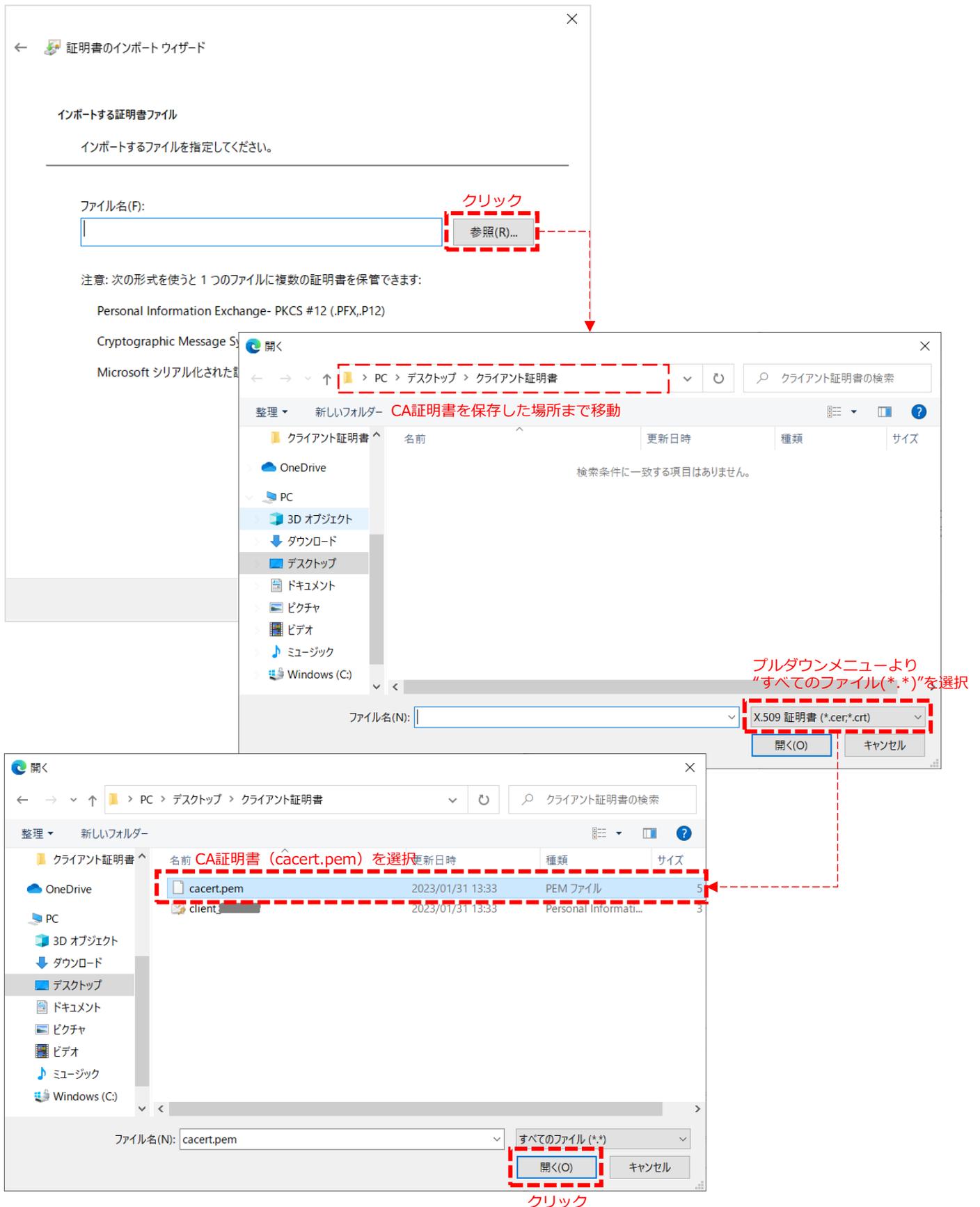
02 Google Chromeをご利用の場合

- 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。



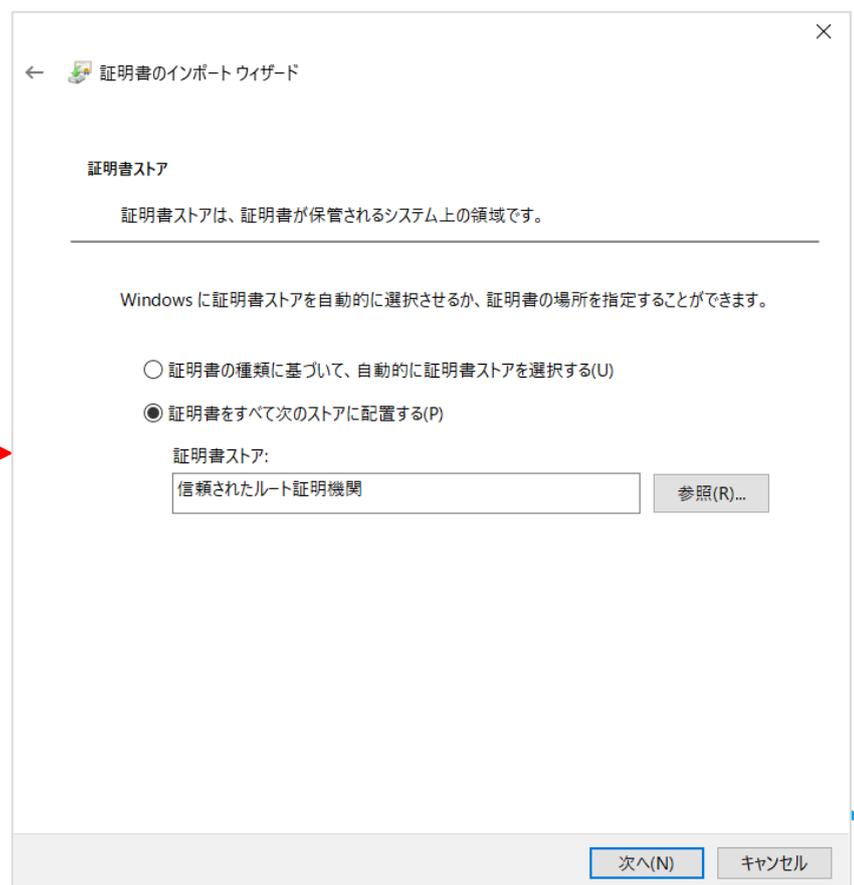
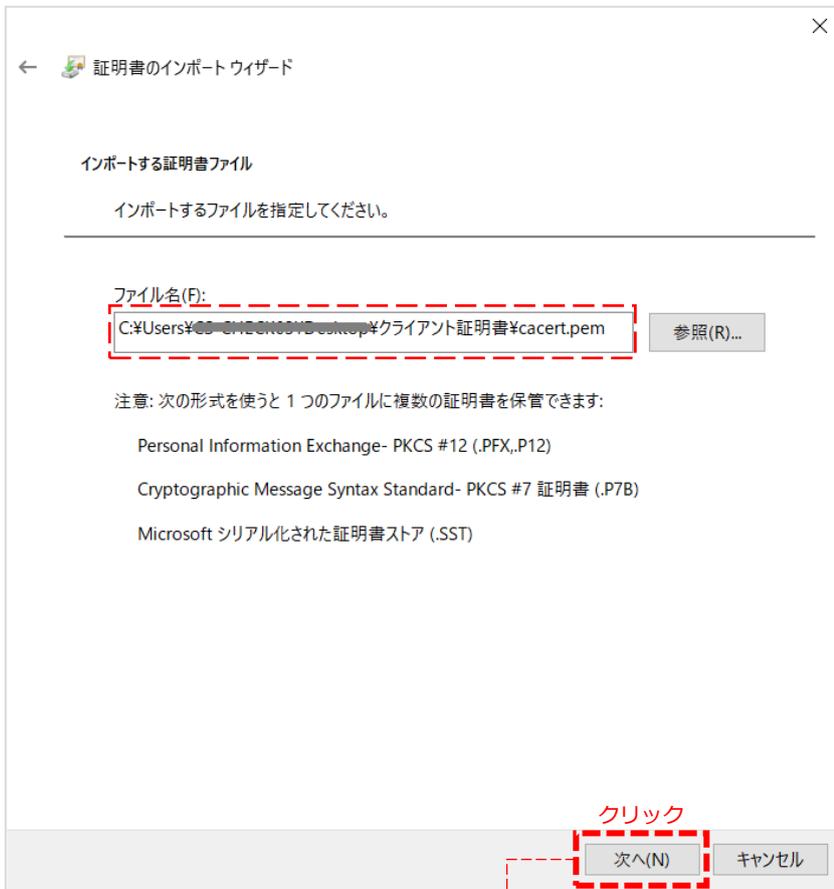
02 Google Chromeをご利用の場合

- 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。



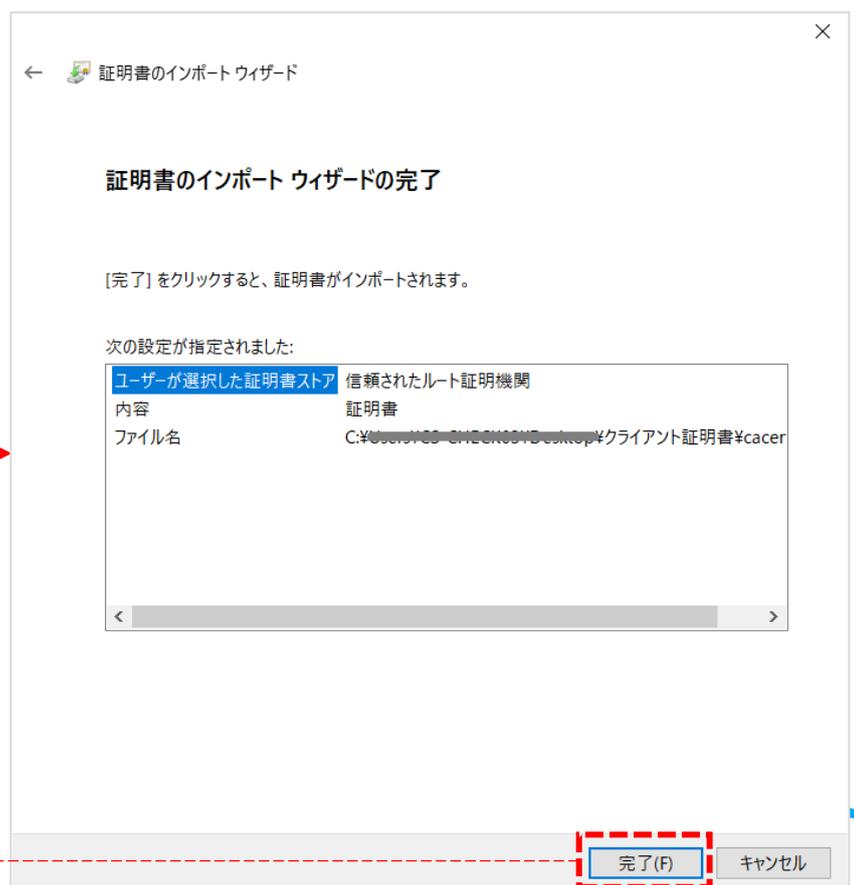
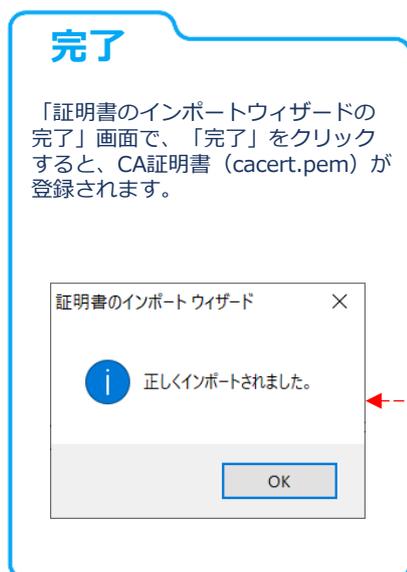
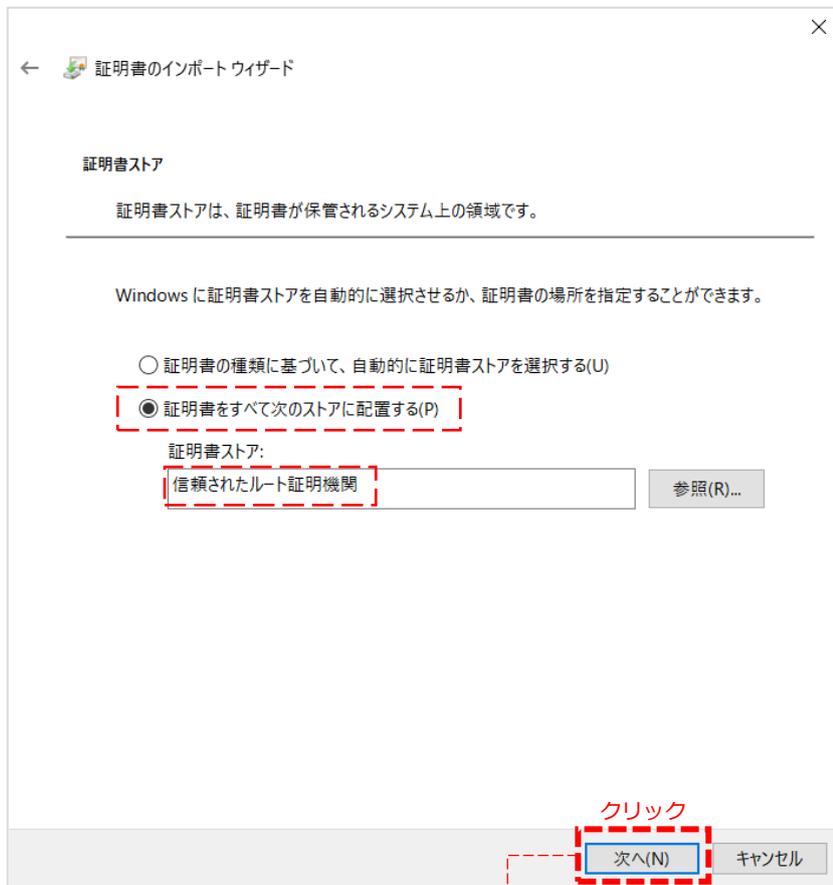
02 Google Chromeをご利用の場合

- 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。



02 Google Chromeをご利用の場合

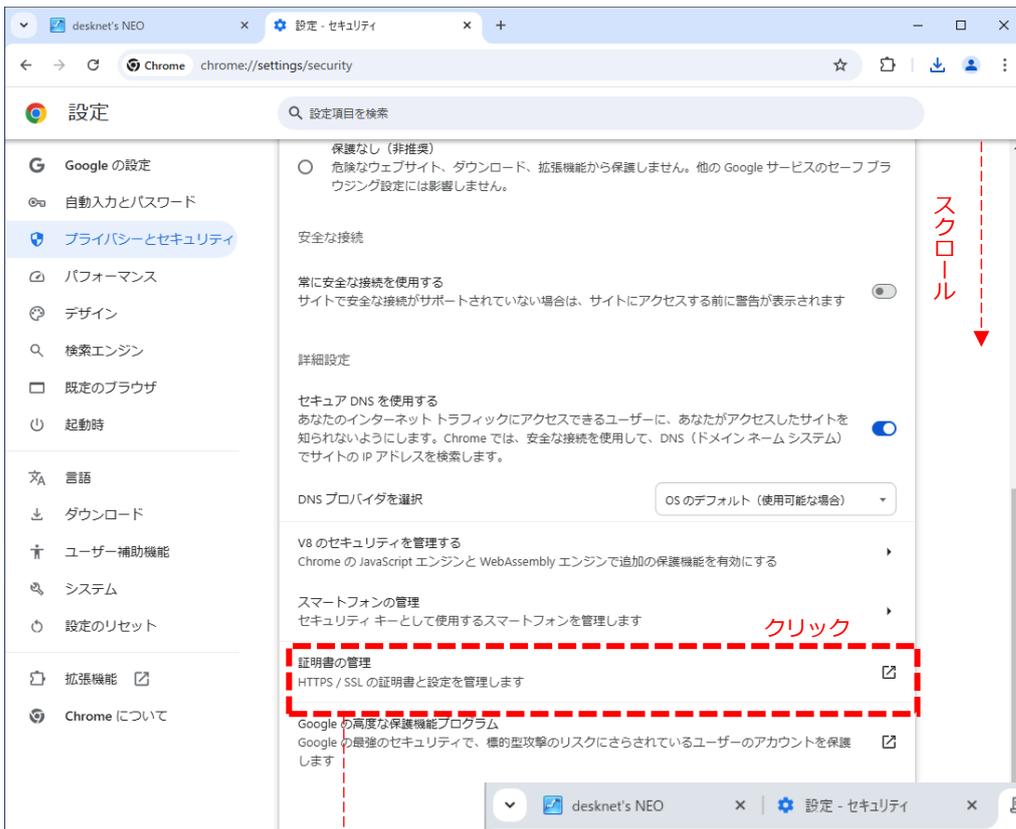
- ⑧ 「証明書をすべて次のストアに配置する(P)」のラジオボタンを選択、「証明書ストア：」に「信頼されたルート証明機関」を選択し、「次へ」ボタンをクリックします。



02 Google Chromeをご利用の場合

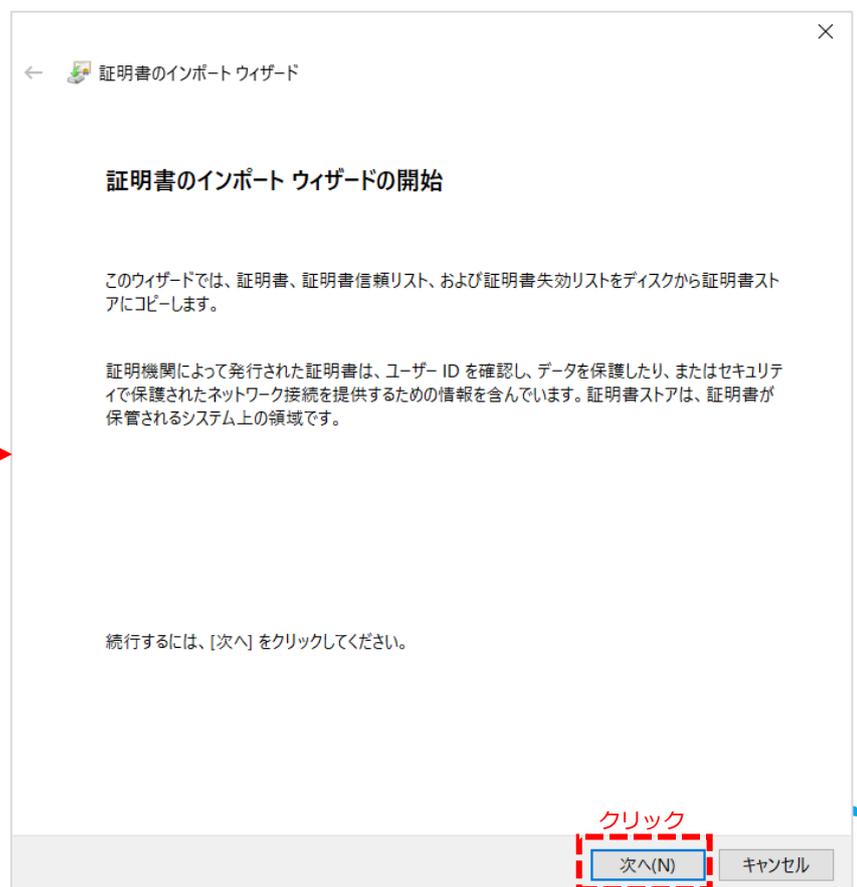
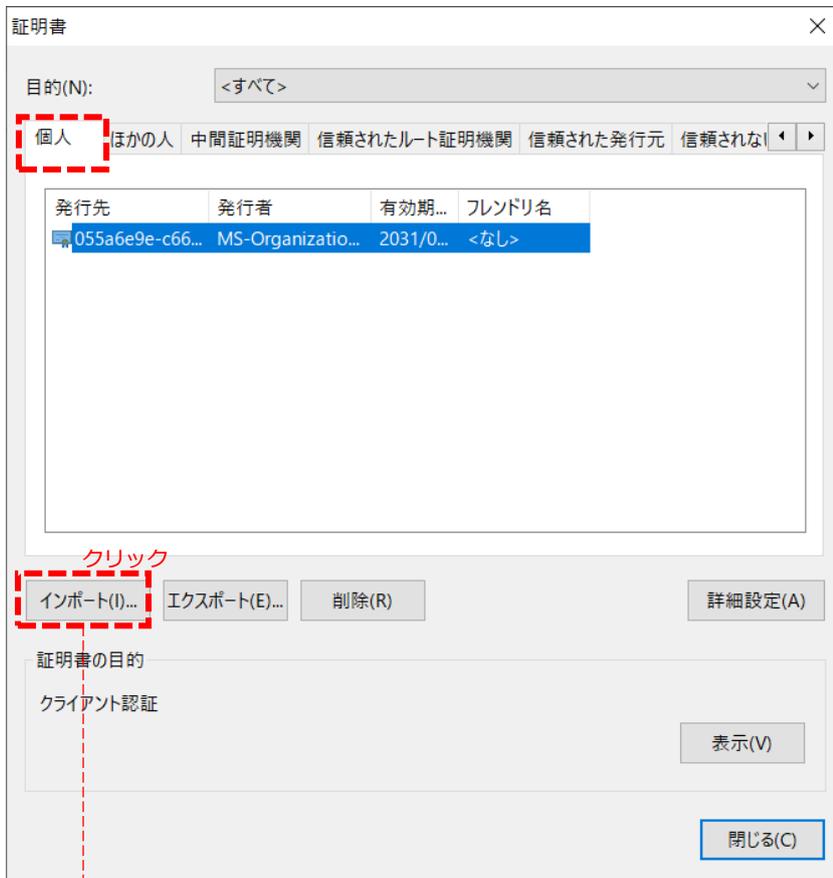
3. クライアント証明書ファイル (*.pfx) のインストール

- 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」で画面遷移し、スクロールして「証明書の管理」をクリックしてください。次に「証明書マネージャ」の画面に遷移しますので、「Windows からインポートした証明書を管理する」をクリックしてください。



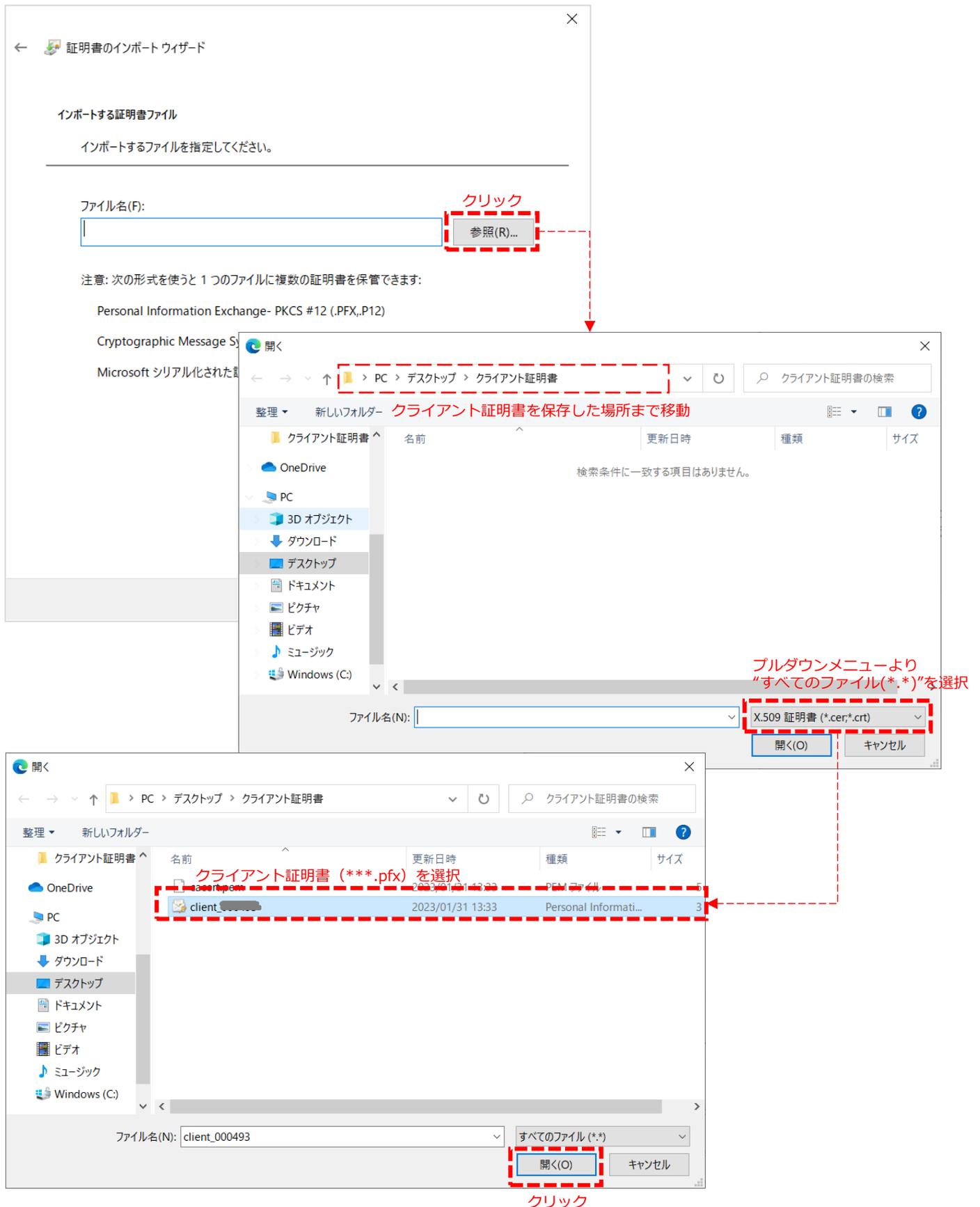
02 Google Chromeをご利用の場合

- 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。



02 Google Chromeをご利用の場合

- 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。



02 Google Chromeをご利用の場合

- 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。

← 証明書のインポートウィザード

インポートする証明書ファイル

インポートするファイルを指定してください。

ファイル名(F):
C:\Users\%...%\クライアント証明書\client... 参照(R)...

注意: 次の形式を使うと 1 つのファイルに複数の証明書を保管できます:

- Personal Information Exchange- PKCS #12 (.PFX,.P12)
- Cryptographic Message Syntax Standard- PKCS #7 証明書 (.P7B)
- Microsoft シリアル化された証明書ストア (.SST)

クリック

次へ(N) キャンセル

← 証明書のインポートウィザード

秘密キーの保護

セキュリティを維持するために、秘密キーはパスワードで保護されています。

秘密キーのパスワードを入力してください。

パスワード(P):
[]

パスワードの表示(D)

インポート オプション(O):

- 秘密キーの保護を強力にする(E)
このオプションを有効にすると、秘密キーがアプリケーションで使われるたびに確認を求めら
れます。
- このキーをエクスポート可能にする(M)
キーのバックアップやトランスポートを可能にします。
- 仮想化ベースのセキュリティを使用して秘密キーを保護する(エクスポート不可)(P)
- すべての拡張プロパティを含める(A)

次へ(N) キャンセル

02 Google Chromeをご利用の場合

- 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。

← 証明書のインポートウィザード

秘密キーの保護

セキュリティを維持するために、秘密キーはパスワードで保護されています。

秘密キーのパスワードを入力してください。

パスワード(P):

パスワードの表示(D)

インポート オプション(I):

- 秘密キーの保護を強力にする(E)
このオプションを有効にすると、秘密キーがアプリケーションで使われるたびに確認を求められます。
- このキーをエクスポート可能にする(M)
キーのバックアップやトランスポートを可能にします。
- 仮想化ベースのセキュリティを使用して秘密キーを保護する(エクスポート不可)(P)
- すべての拡張プロパティを含める(A)

クリック

次へ(N) キャンセル

← 証明書のインポートウィザード

証明書ストア

証明書ストアは、証明書が保管されるシステム上の領域です。

Windows に証明書ストアを自動的に選択させるか、証明書の場所を指定することができます。

- 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(U)
- 証明書をすべて次のストアに配置する(P)

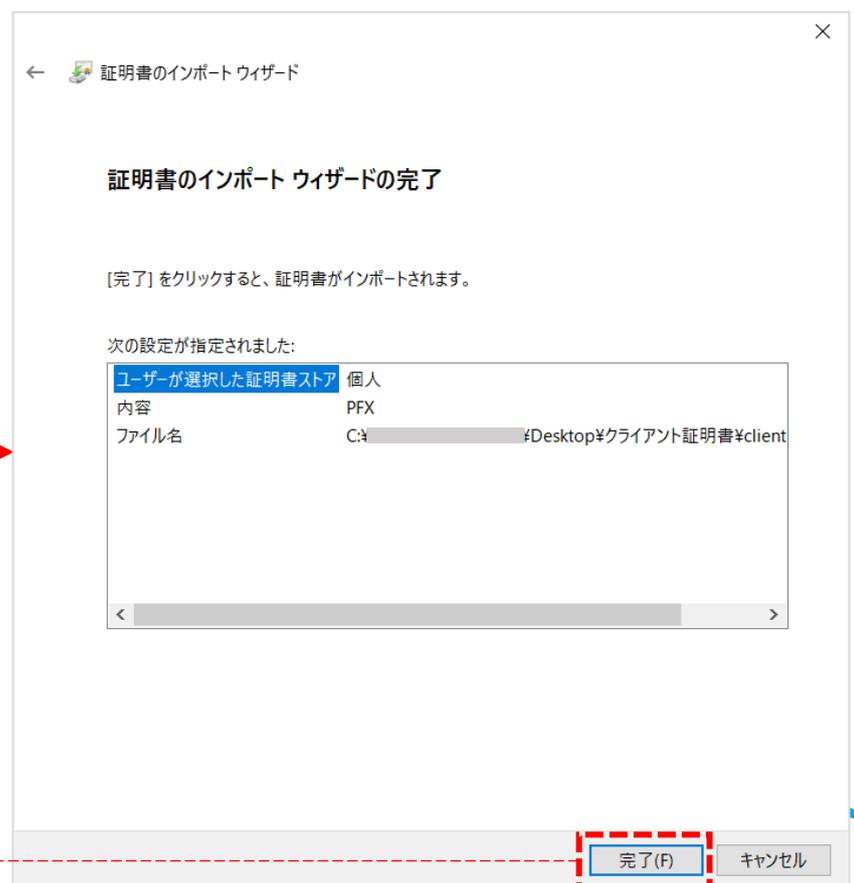
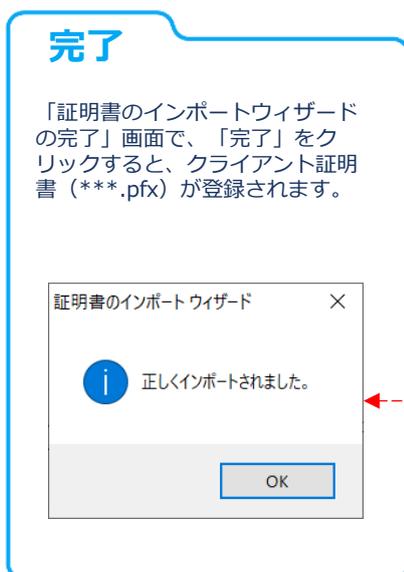
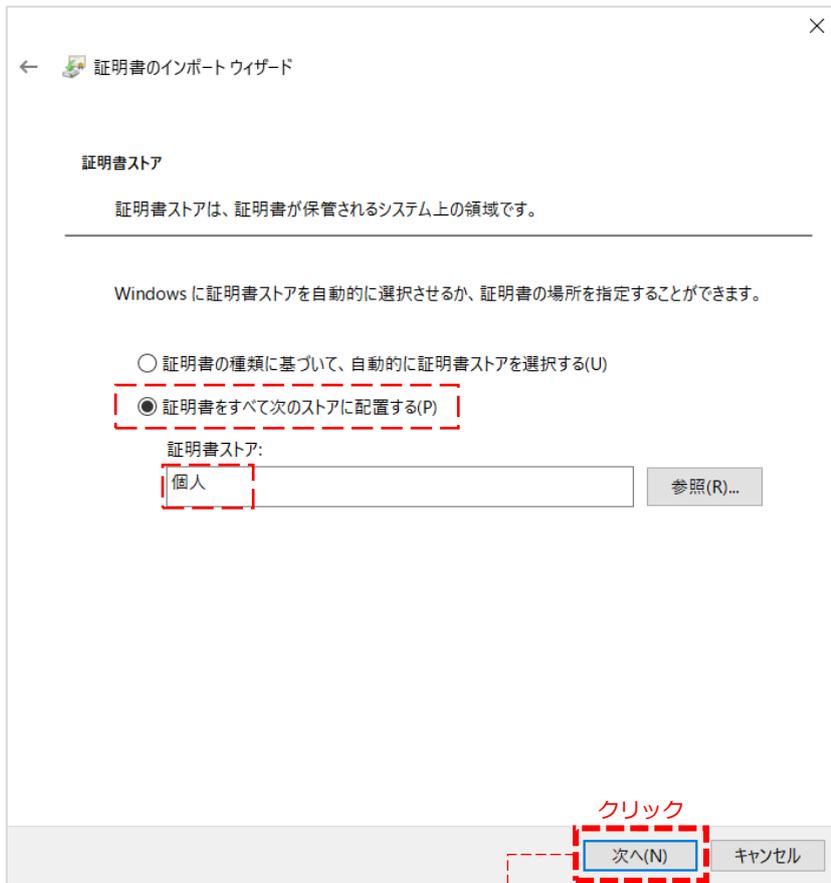
証明書ストア:

個人 参照(R)...

次へ(N) キャンセル

02 Google Chromeをご利用の場合

- 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。



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。

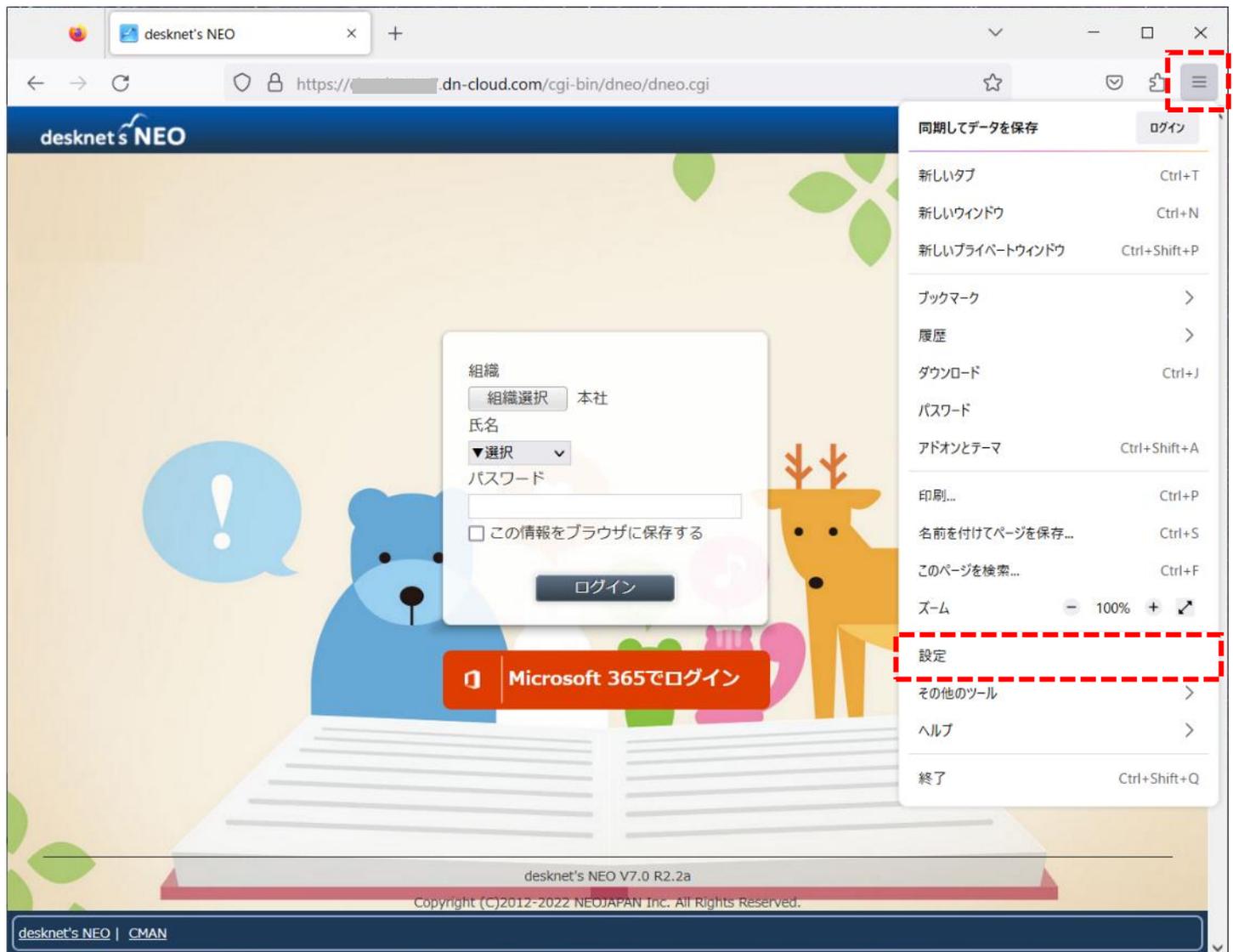
1. クライアント認証サービス用のファイルの準備

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

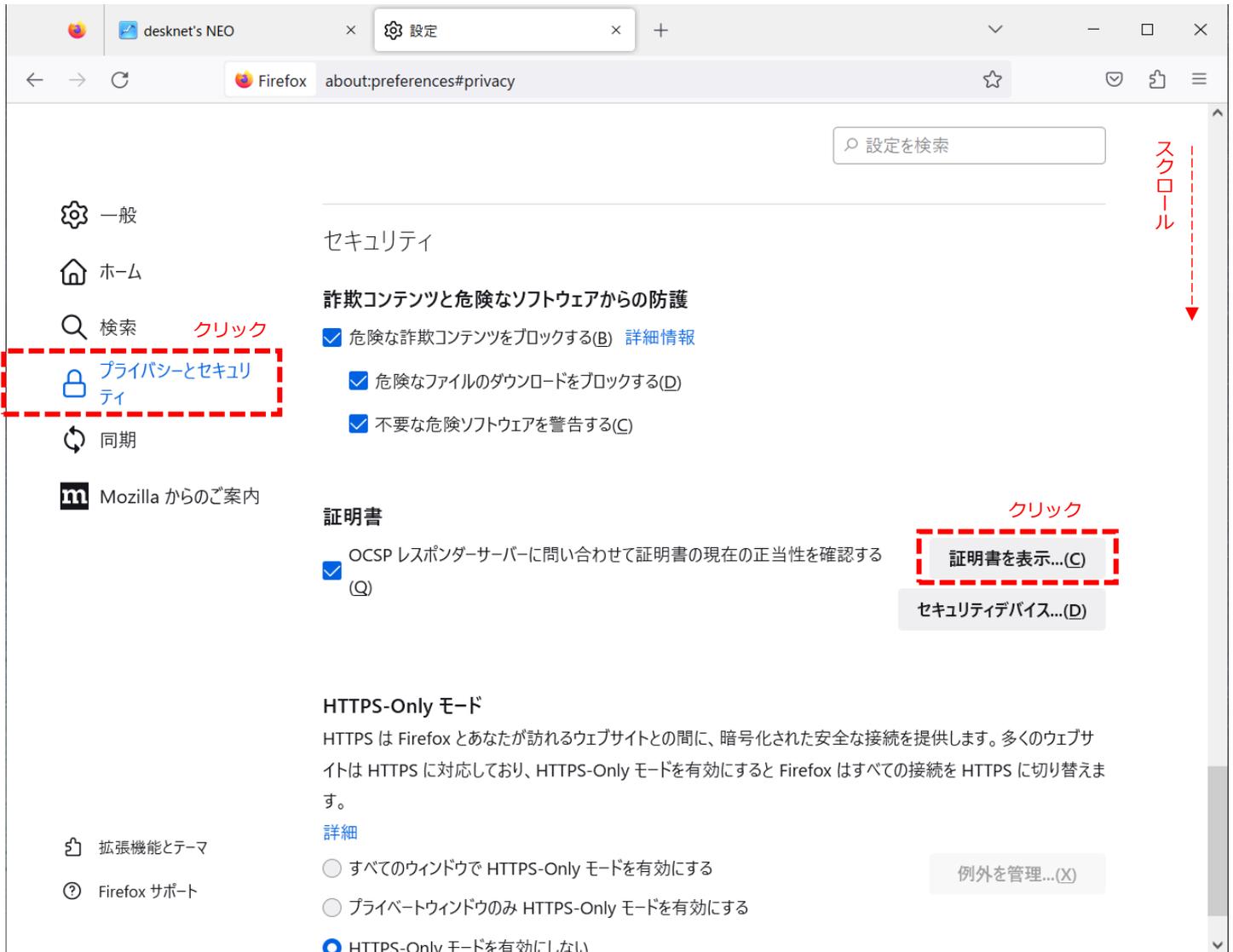
2. CA証明書 (cacert.pem) のインストール

- 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。



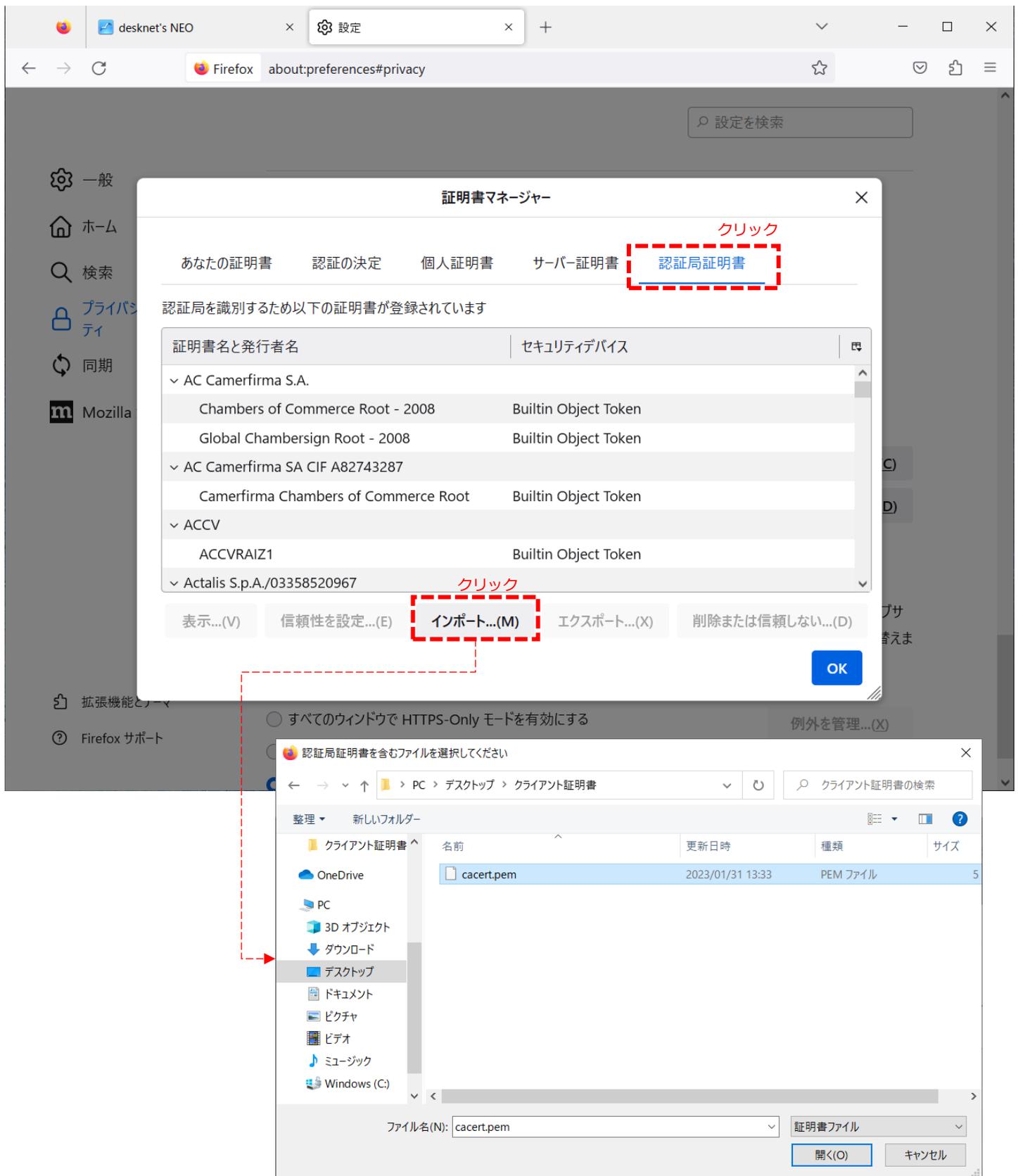
03 Mozilla Firefoxをご利用の場合

- 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」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。



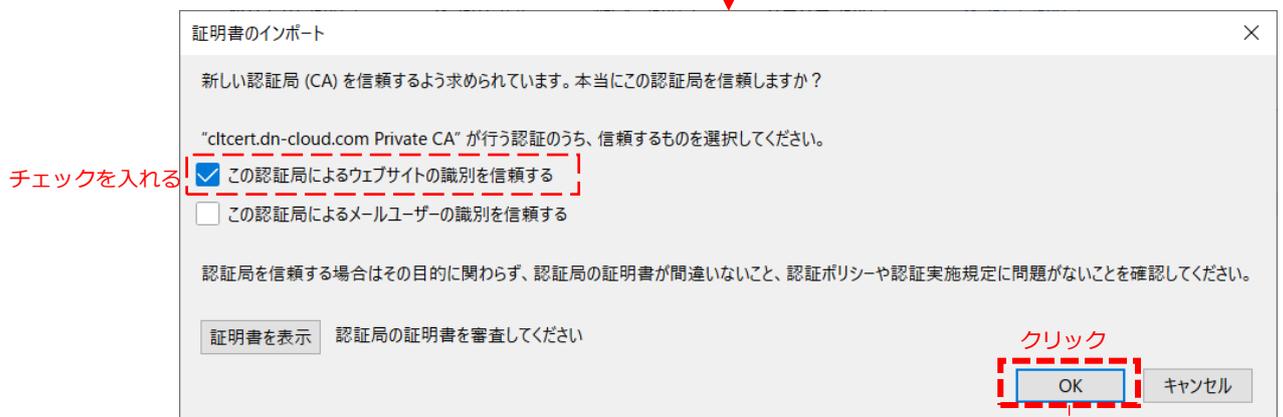
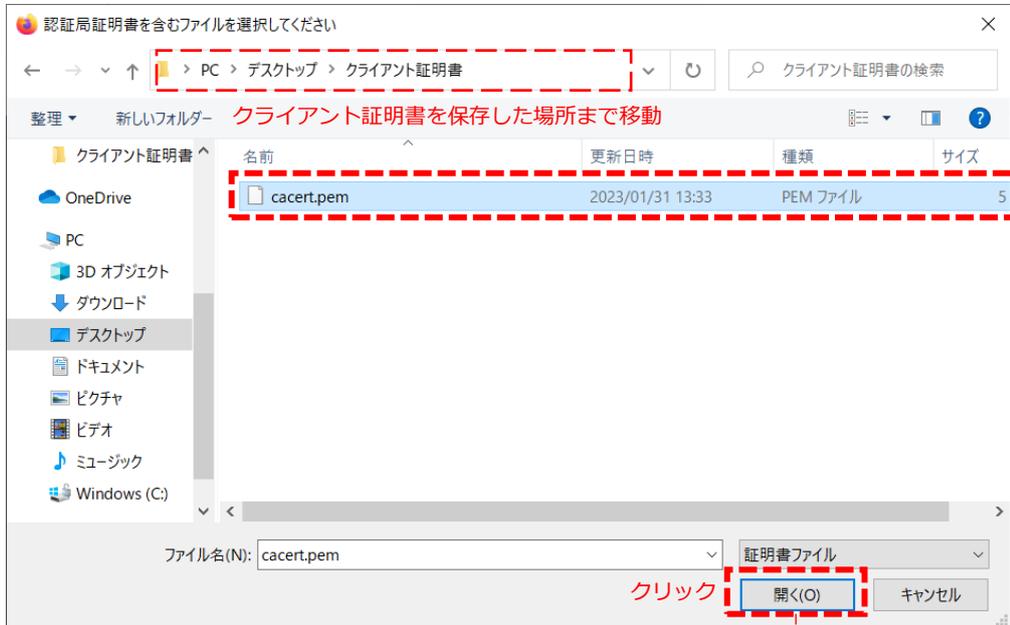
03 Mozilla Firefoxをご利用の場合

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。



03 Mozilla Firefoxをご利用の場合

- 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。



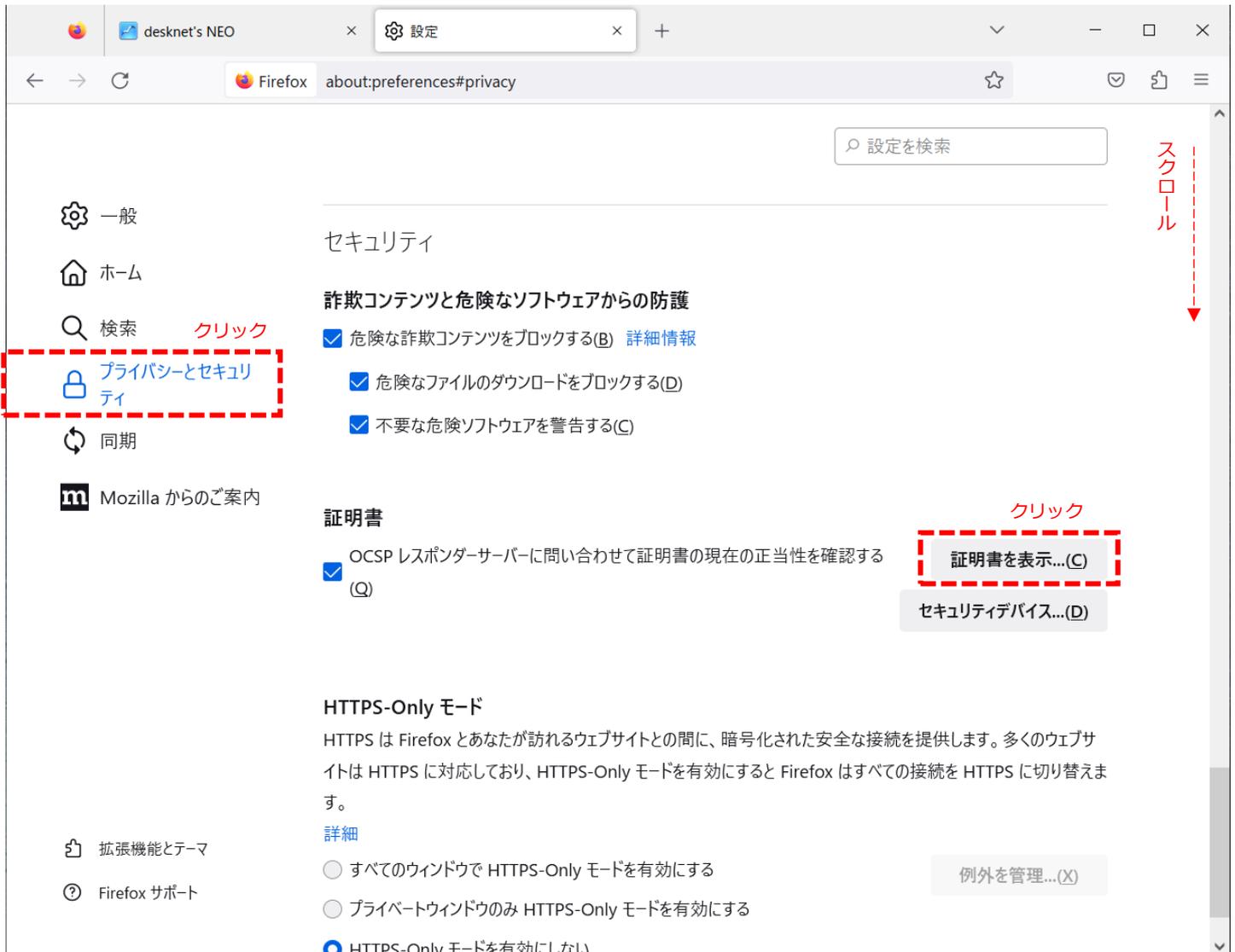
完了

「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。



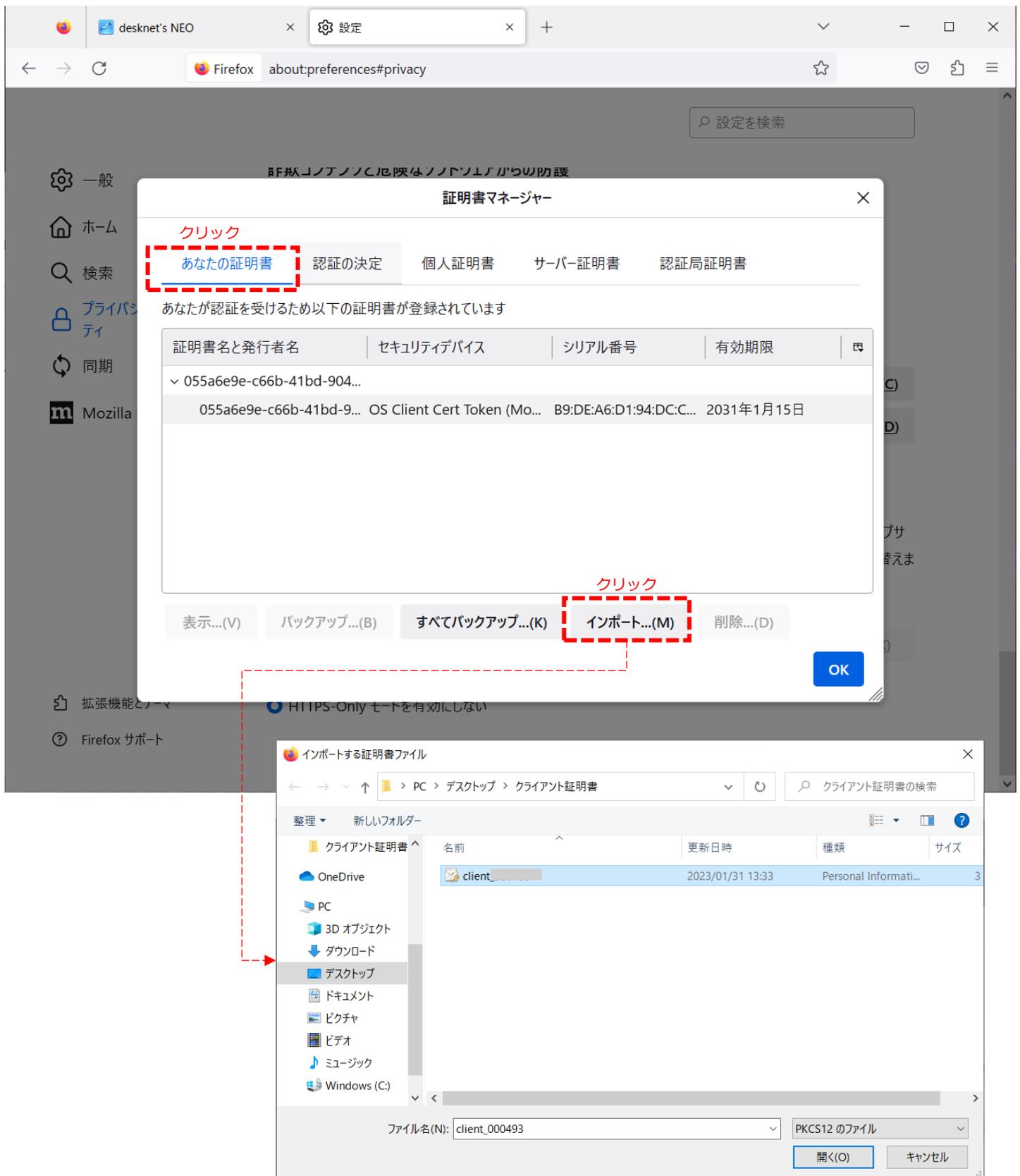
3. クライアント証明書ファイル (*.pfx) のインストール

- 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」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。



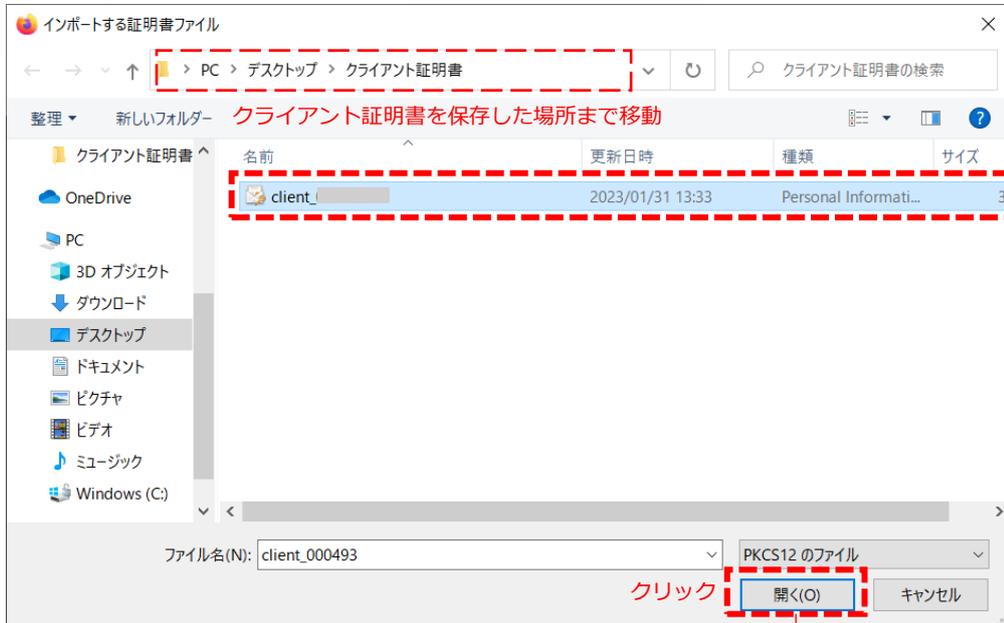
03 Mozilla Firefoxをご利用の場合

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。

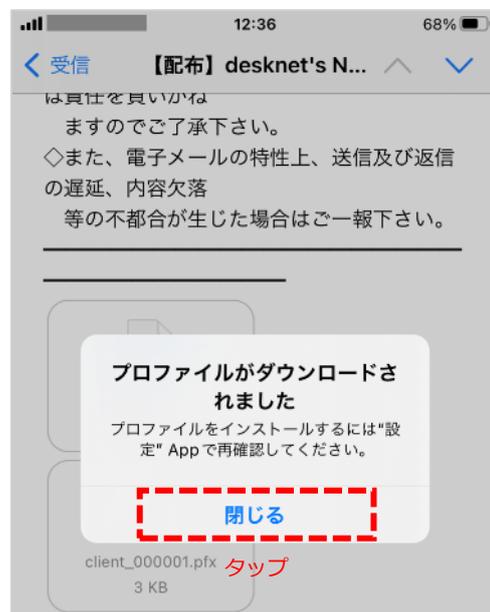
- CA証明書ファイル (cacert.pem)
- クライアント証明書ファイル (***.pfx)
- 配布されたクライアント証明書ファイルのパスワード

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) のダウンロードアイコンをタップします。

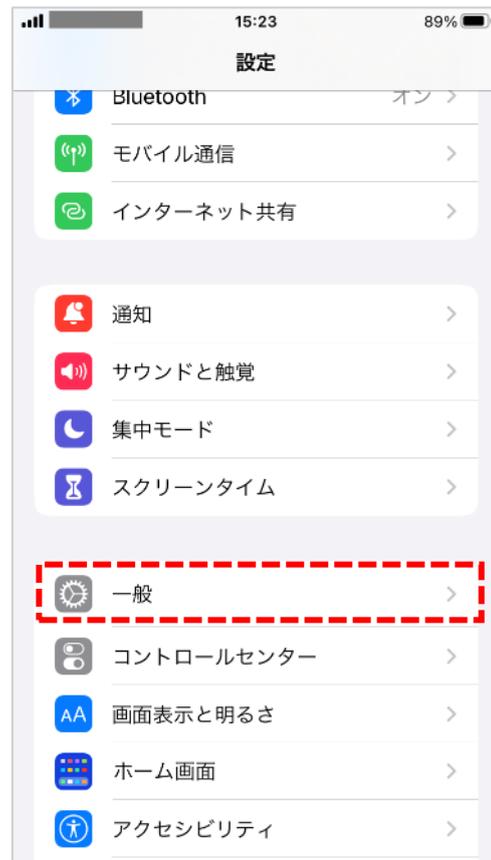


- ② ダウンロードが完了するとメッセージが表示されるので、「閉じる」をタップします。



04 iPhone(iOS)をご利用の場合

- 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。



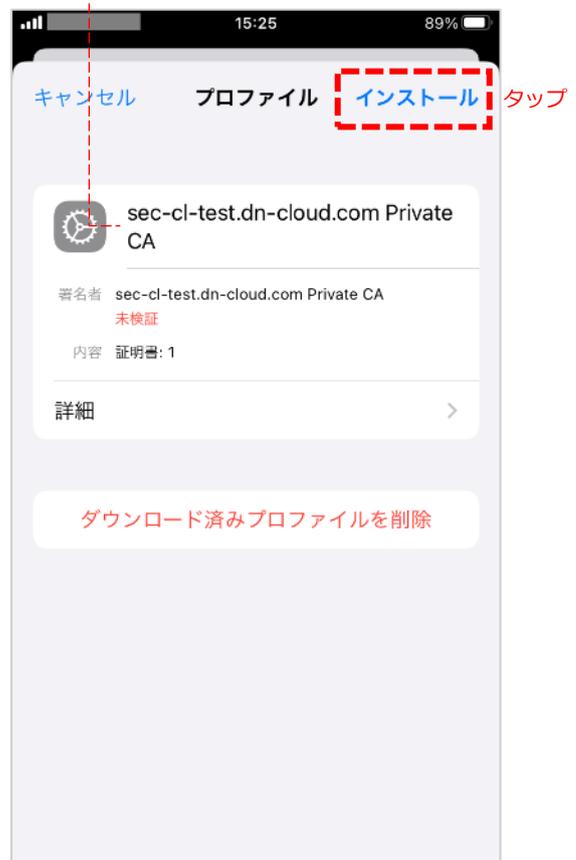
- iOS 13の場合
「VPNとデバイス管理」はメニューにございません。
「プロファイル」を選択ください。
- iOS 14の場合
「VPNとデバイス管理」はメニューにございません。
「プロファイルとデバイス管理」を選択ください。

04 iPhone(iOS)をご利用の場合

- 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。

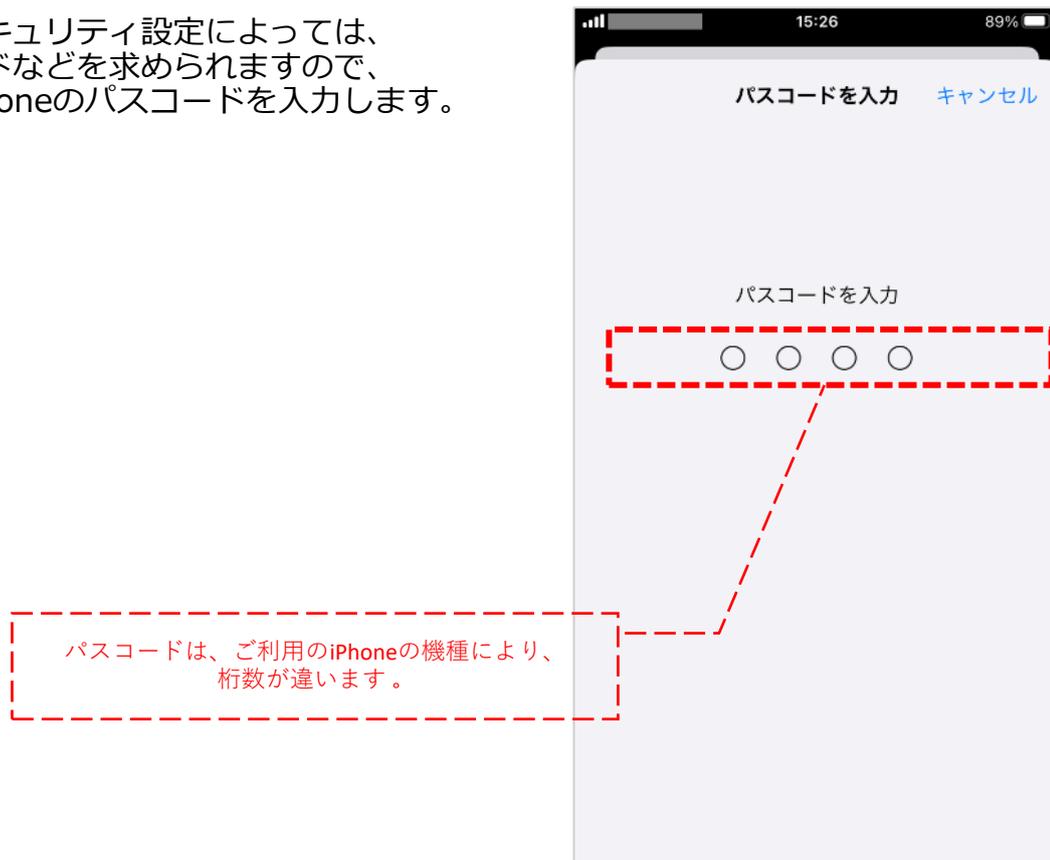


- ⑥ 「インストール」をタップします。



04 iPhone(iOS)をご利用の場合

- 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。



04 iPhone(iOS)をご利用の場合

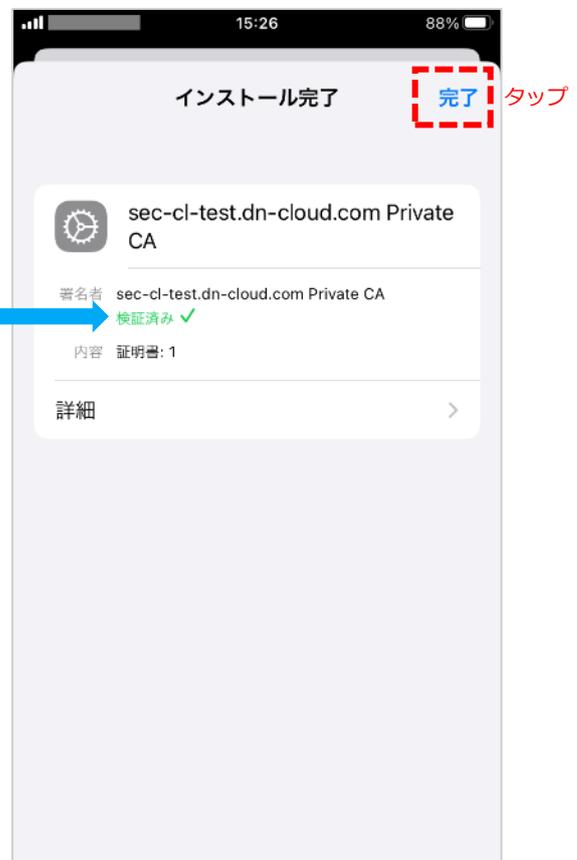
⑨ 再度「インストール」をタップします。



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。

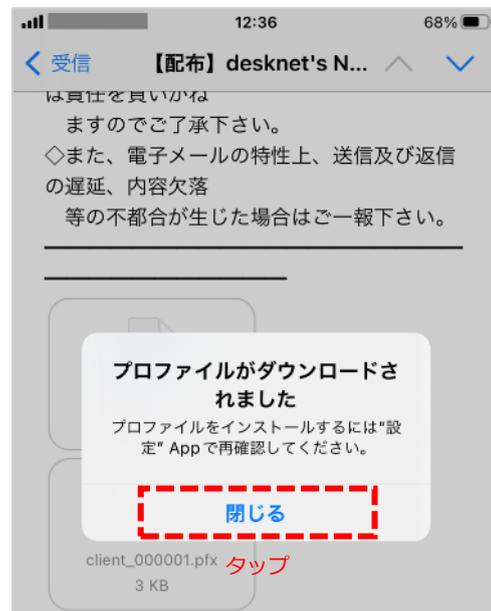


3. クライアント証明書ファイル (*.pfx) のインストール

- 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) のダウンロードアイコンをタップします。

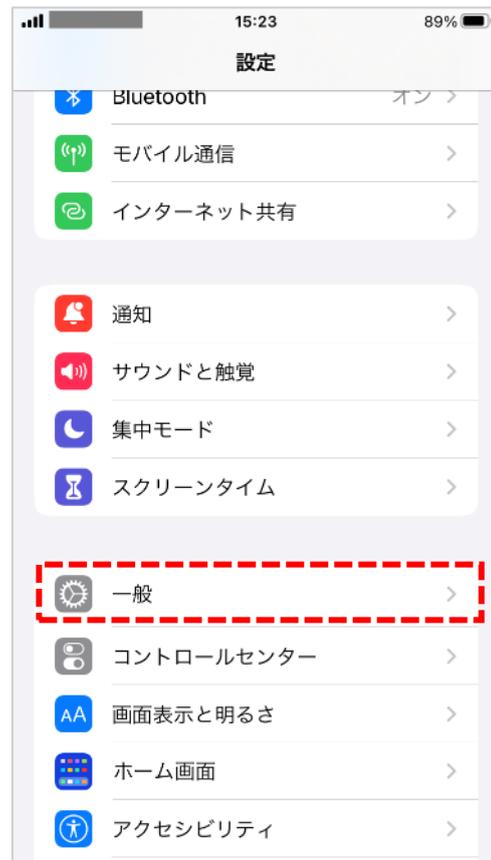


- ① ダウンロードが完了するとメッセージが表示されるので、「閉じる」をタップします。



04 iPhone(iOS)をご利用の場合

- 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。

04 iPhone(iOS)をご利用の場合

- 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。

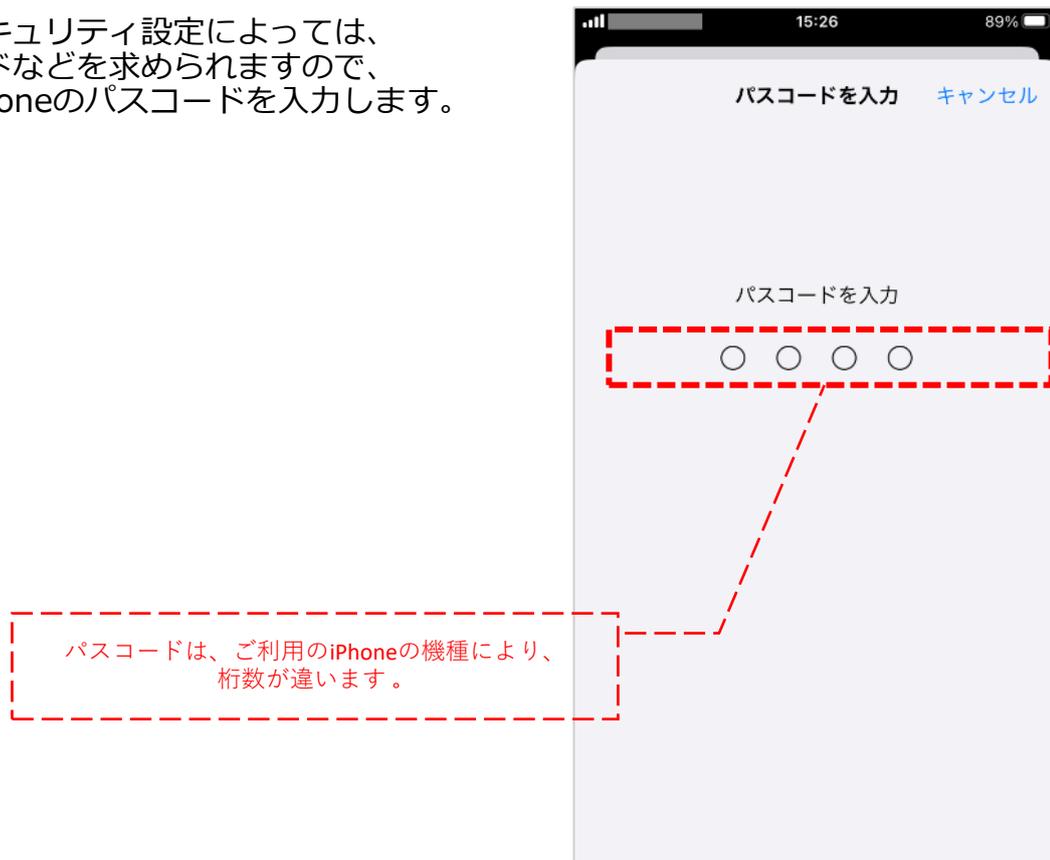


- ⑥ 「インストール」をタップします。



04 iPhone(iOS)をご利用の場合

- 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。



04 iPhone(iOS)をご利用の場合

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。



04 iPhone(iOS)をご利用の場合

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「未署名」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。

04 iPhone(iOS)をご利用の場合

- 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)
- 2025年1月29日 3版 (V3.0 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

