

//////////////////// 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。



<b>01</b>	<b>Microsoft Edgeをご利用の場合</b>	<b>3</b>
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
<b>02</b>	<b>Google Chromeをご利用の場合</b>	<b>16</b>
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
<b>03</b>	<b>Mozilla Firefoxをご利用の場合</b>	<b>30</b>
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
<b>04</b>	<b>iPhone(iOS)をご利用の場合</b>	<b>37</b>
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。

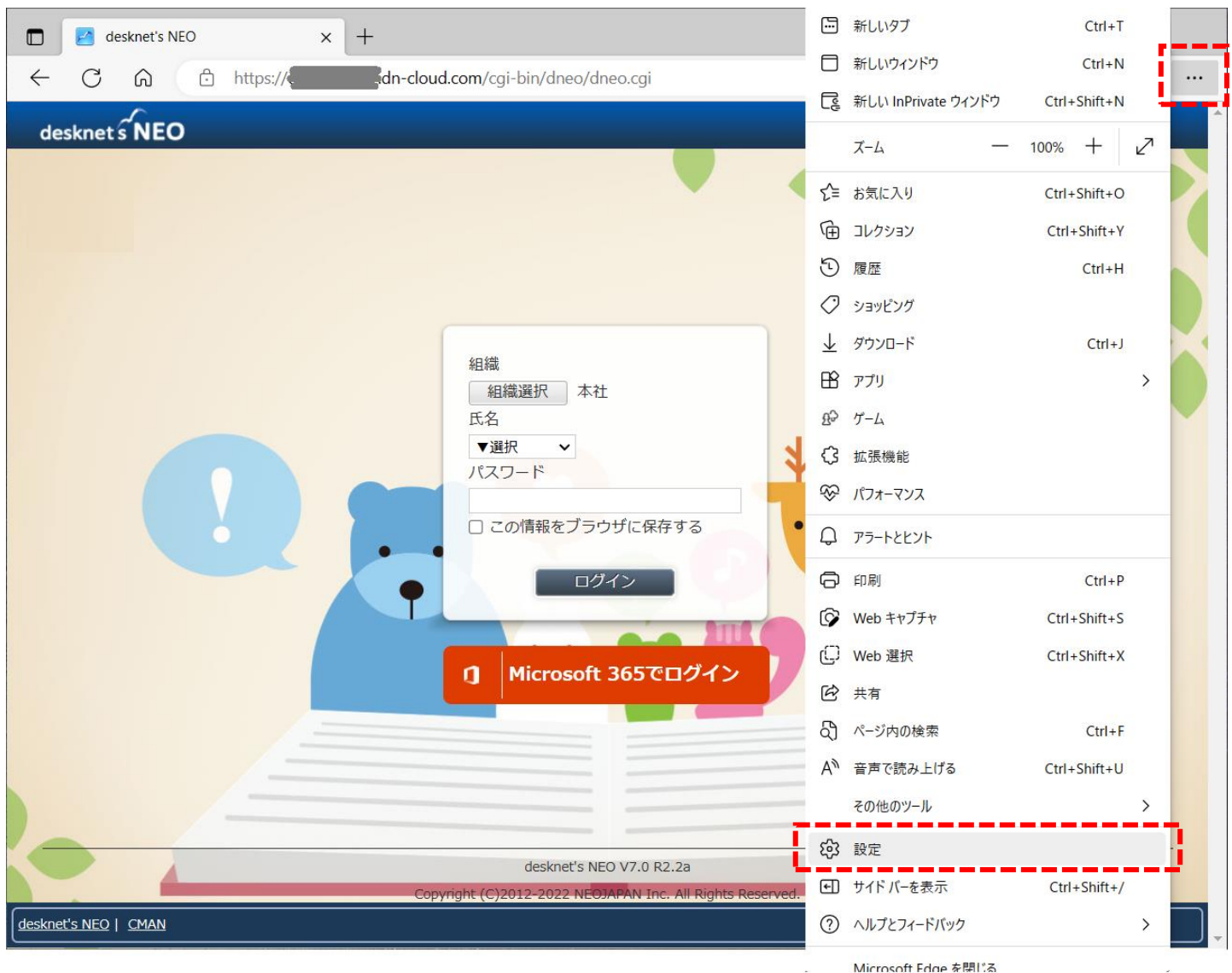
## 1. クライアント認証サービス用のファイルの準備

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。



# 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。

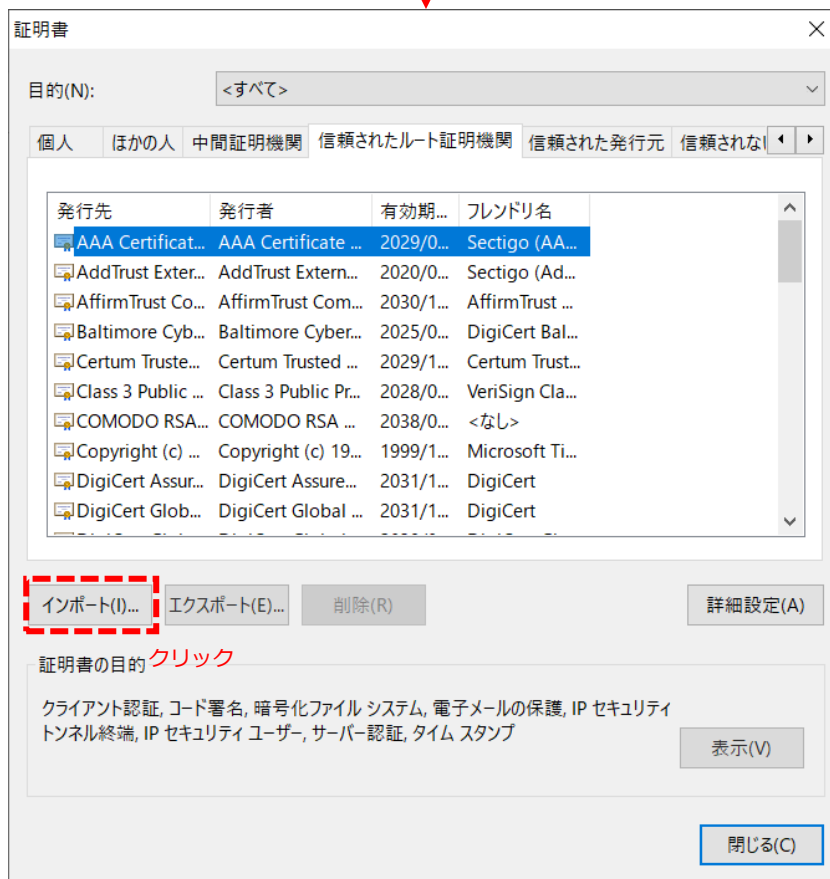
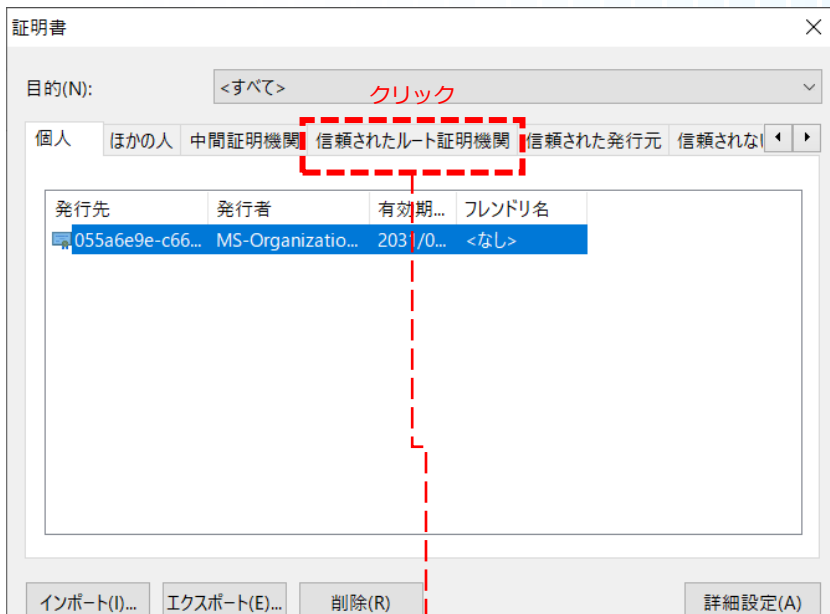
The screenshot shows the Microsoft Edge settings page at `edge://settings/privacy`. The left sidebar has '設定' (Settings) at the top, with a search box and a list of categories. 'プライバシー、検索、サービス' (Privacy, Search, Services) is selected and highlighted with a red dashed box and the label 'クリック' (Click). 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 the label 'クリック' (Click). A '証明書' (Certificate) dialog box is open, showing a list of certificates. The first entry is highlighted in blue. The dialog box has a close button (X) at the top right. Below the list 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 '表示(V)' and '閉じる(C)'. A vertical red dashed arrow on the right side of the main window is labeled 'スクロール' (Scroll).

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



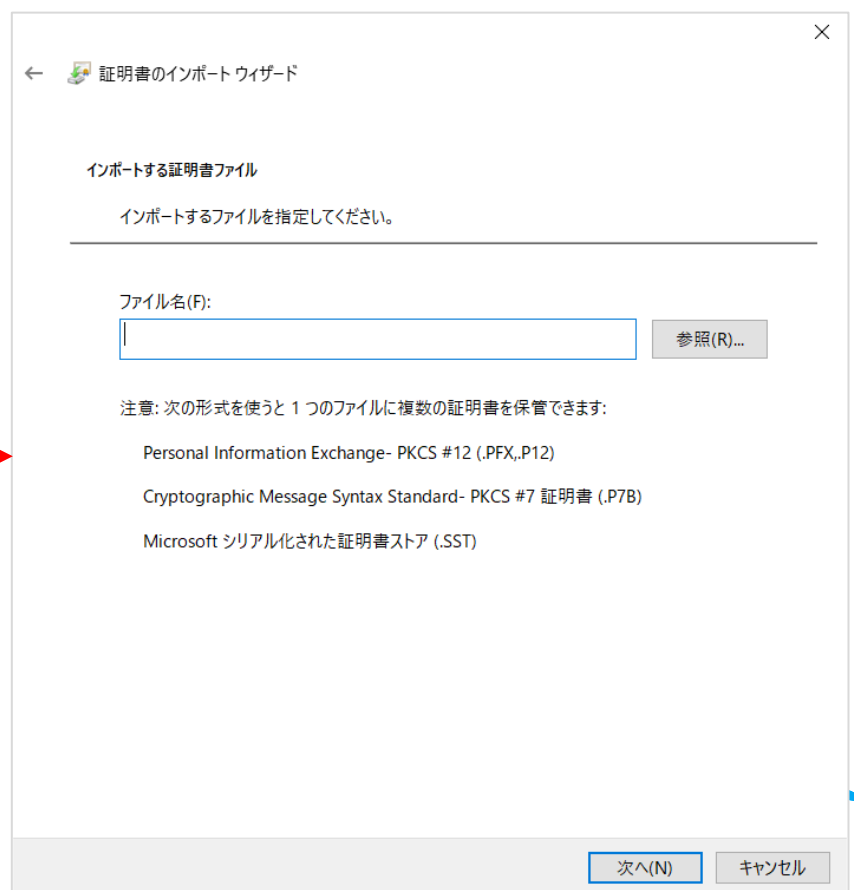
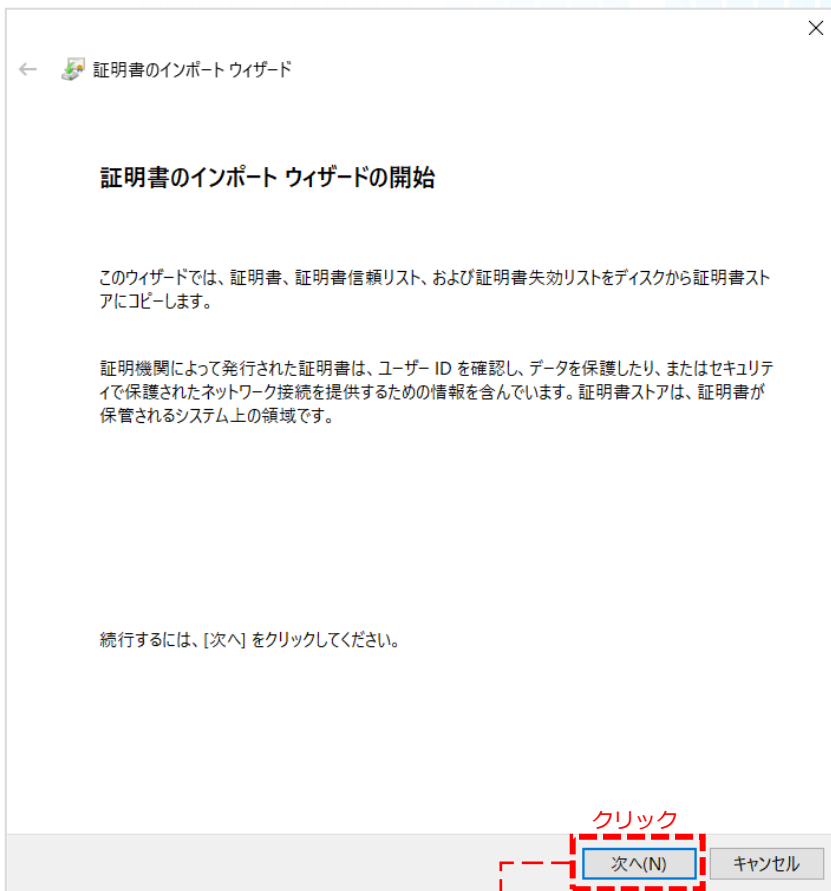
## 01 Microsoft Edgeをご利用の場合

- 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。



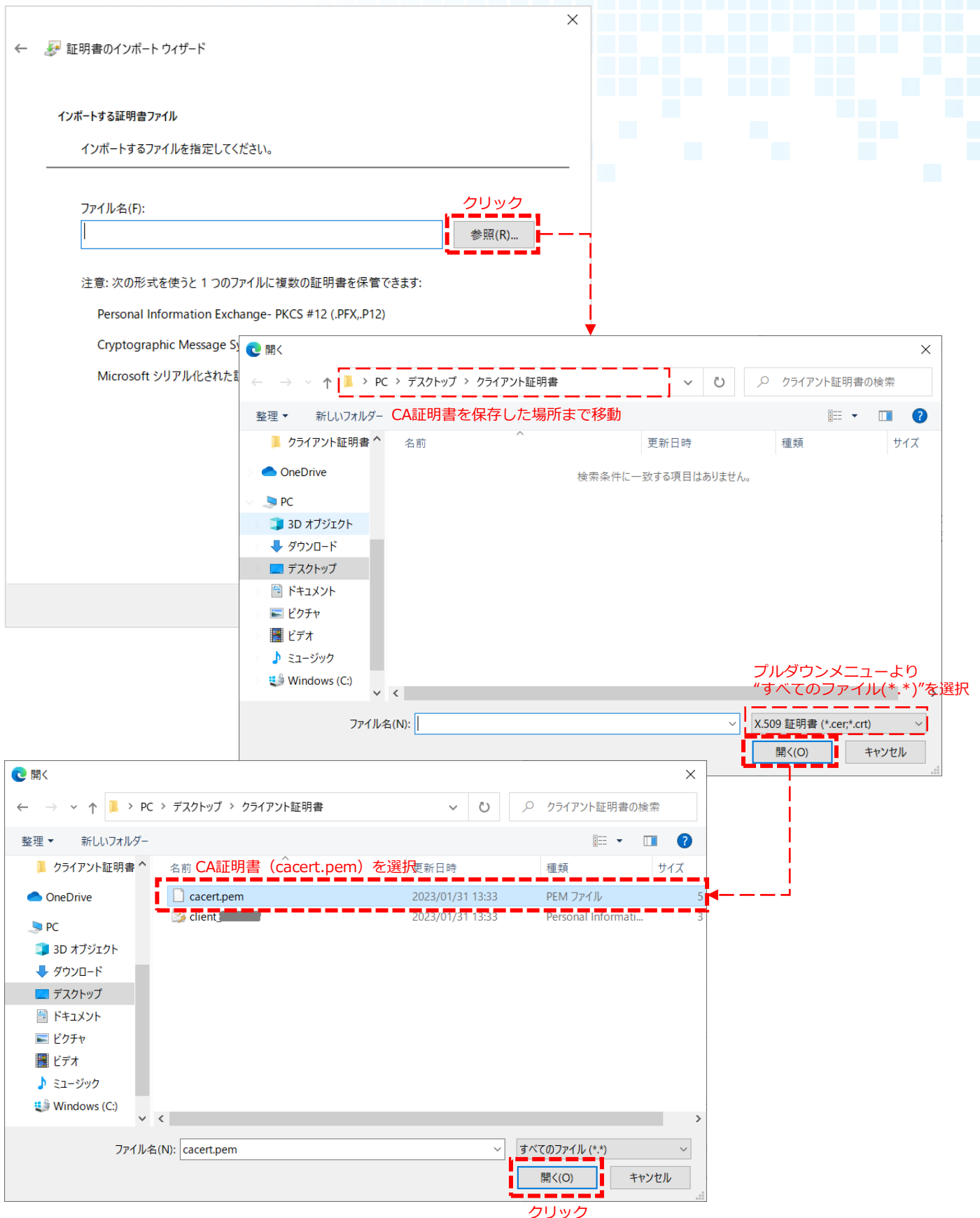
## 01 Microsoft Edgeをご利用の場合

- 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。



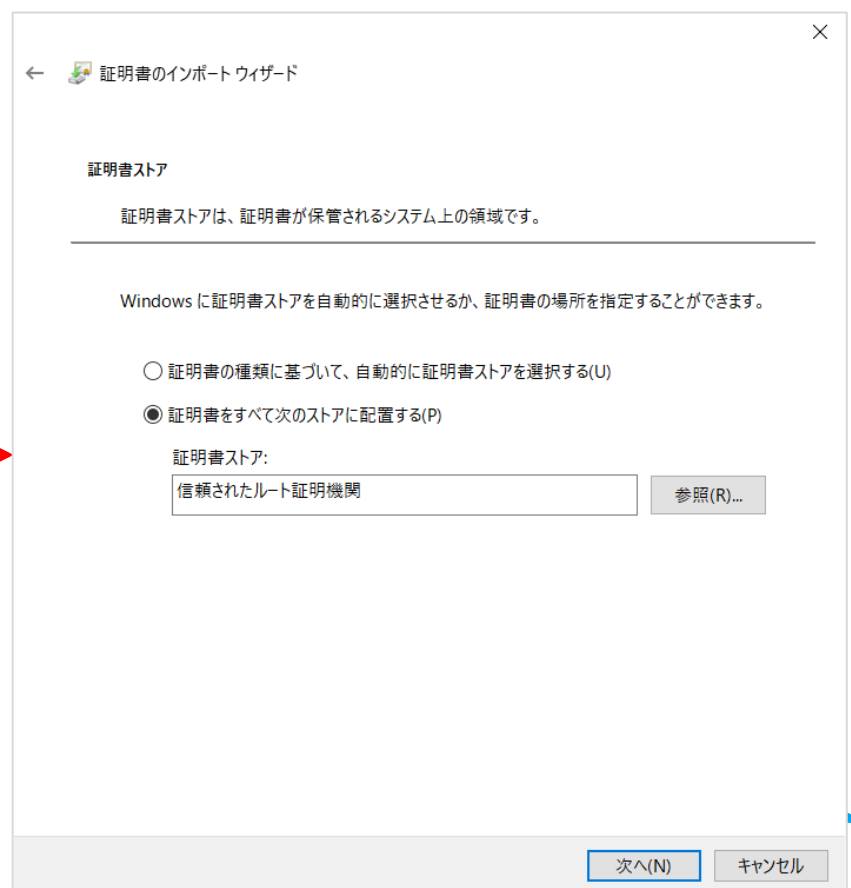
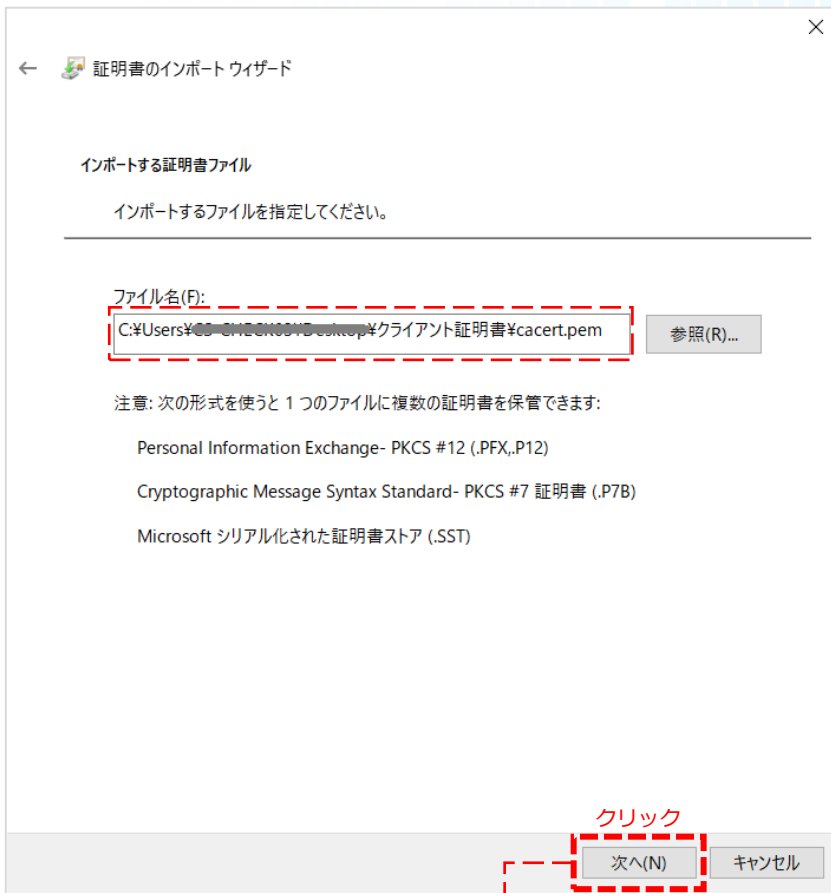
## 01 Microsoft Edgeをご利用の場合

- 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。



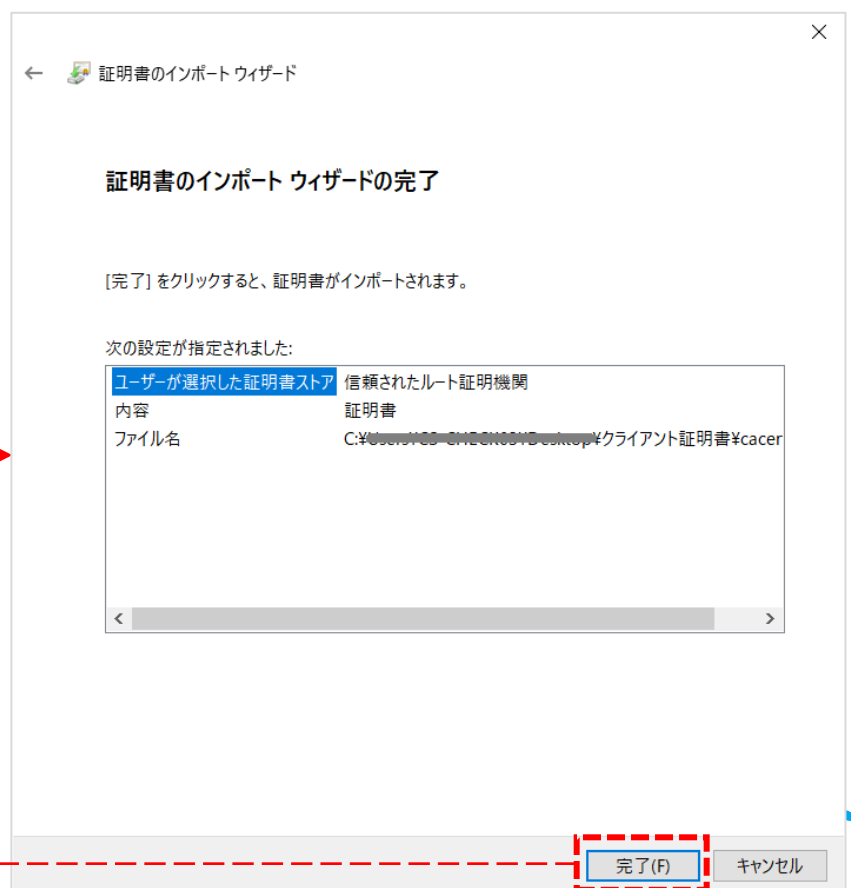
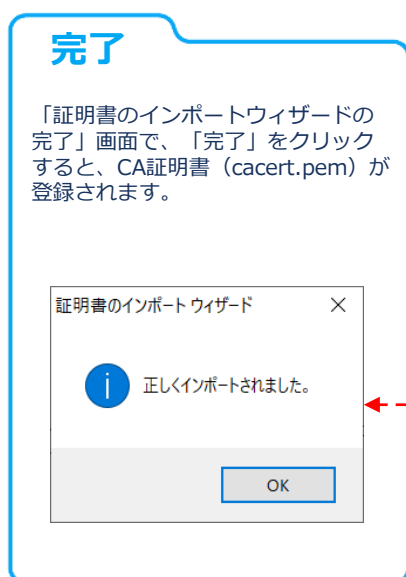
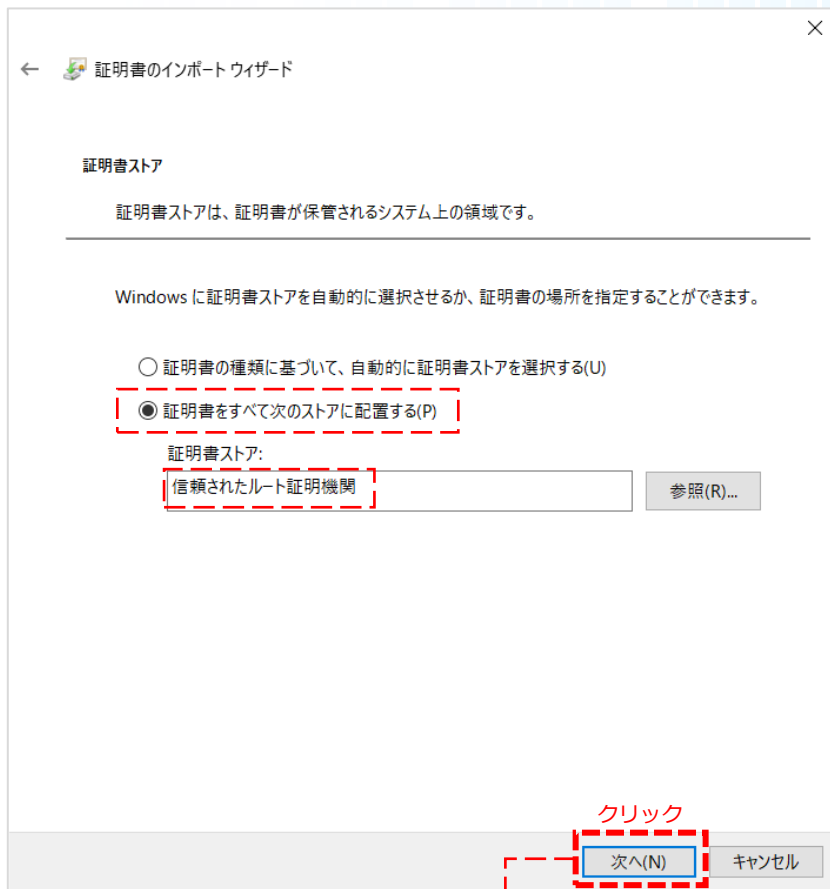
## 01 Microsoft Edgeをご利用の場合

- 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。

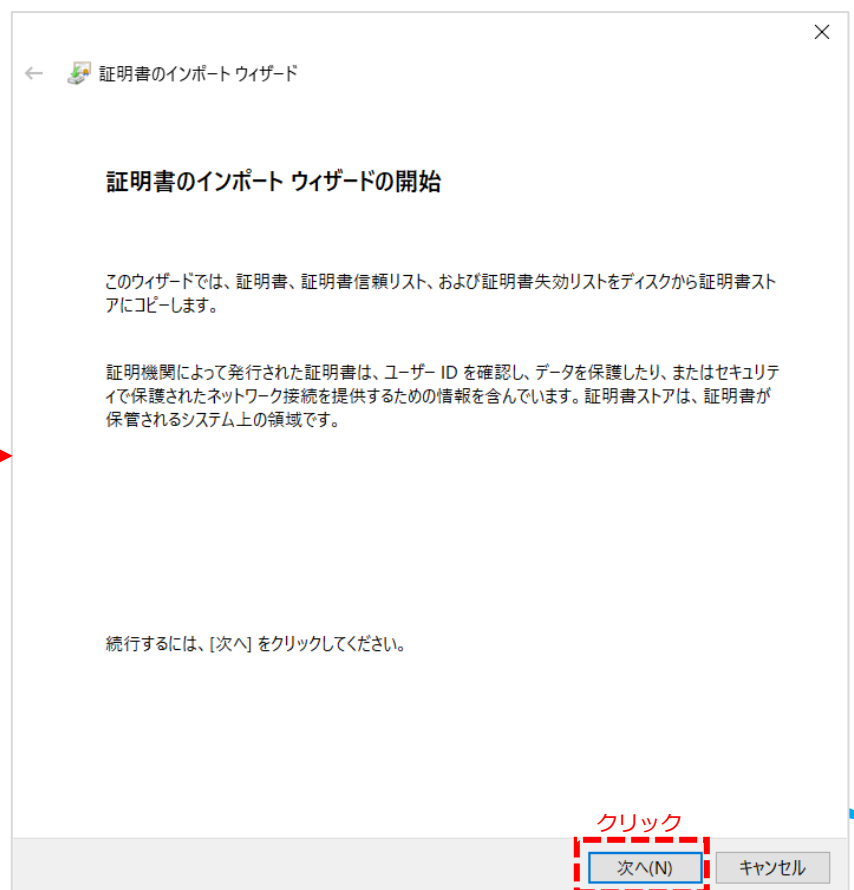
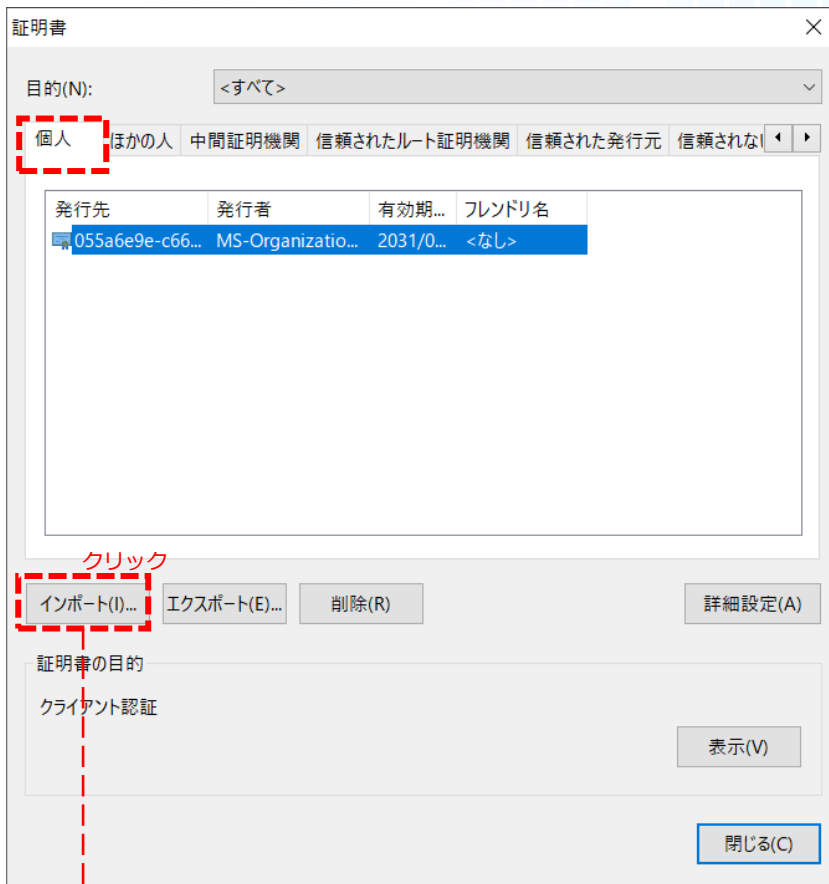
The screenshot shows the Microsoft Edge settings page at `edge://settings/privacy`. The left sidebar has '設定' (Settings) expanded, and 'プライバシー、検索、サービス' (Privacy, Search, Services) is selected. The main content area shows the 'セキュリティ' (Security) section. A red dashed box highlights the '証明書の管理' (Certificate Management) option, with a red arrow pointing to it and the word 'クリック' (Click). A vertical red dashed arrow on the right indicates scrolling down. Below the main settings, 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 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)', '詳細設定(A)', '表示(V)', and '閉じる(C)'.

## 01 Microsoft Edgeをご利用の場合

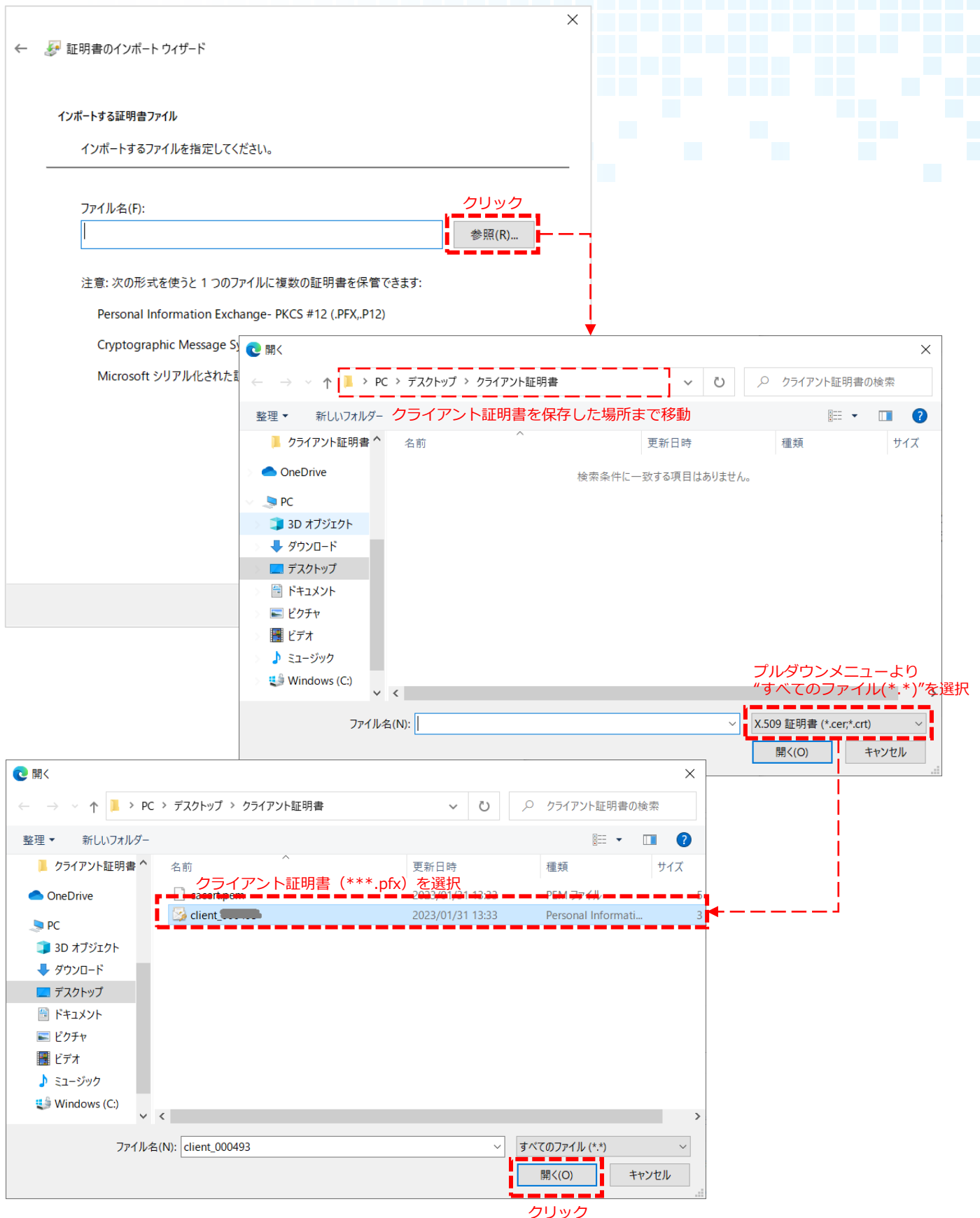
- ② 「個人」タブをクリックし、[インポート] ボタンをクリックすると、「証明書のインポートウィザード」が表示されますので、[次へ] ボタンをクリックしてください。





## 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\_\*.pfx

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(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)

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

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。

← 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:

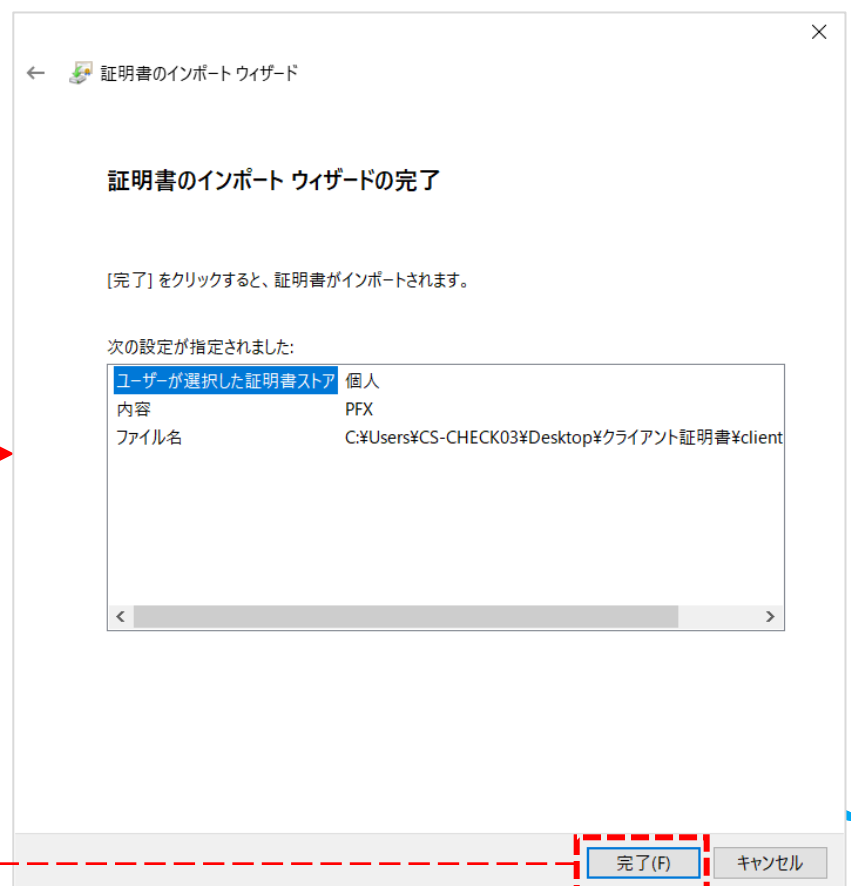
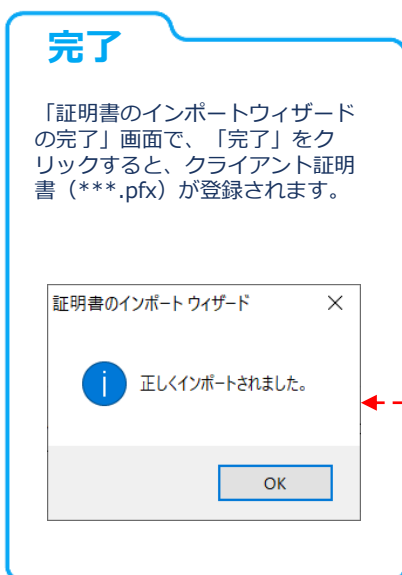
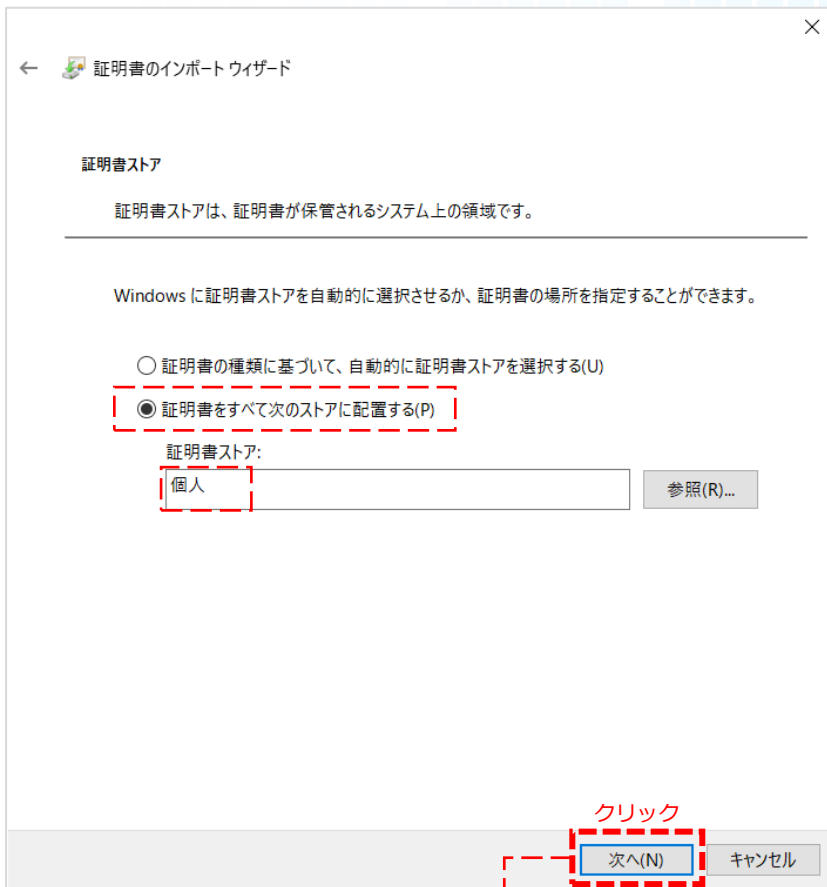
個人

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。



## 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。

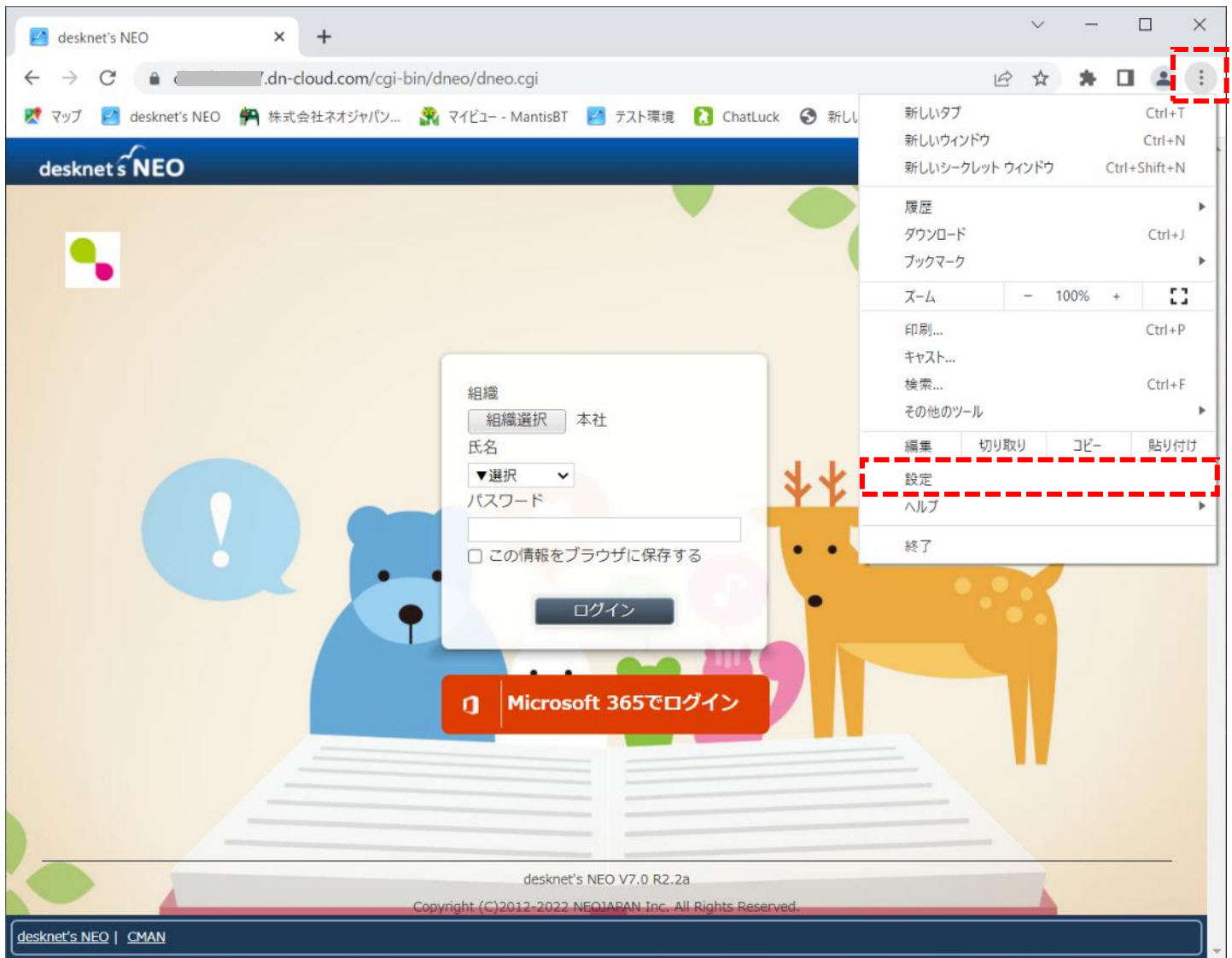
## 1. クライアント認証サービス用のファイルの準備

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

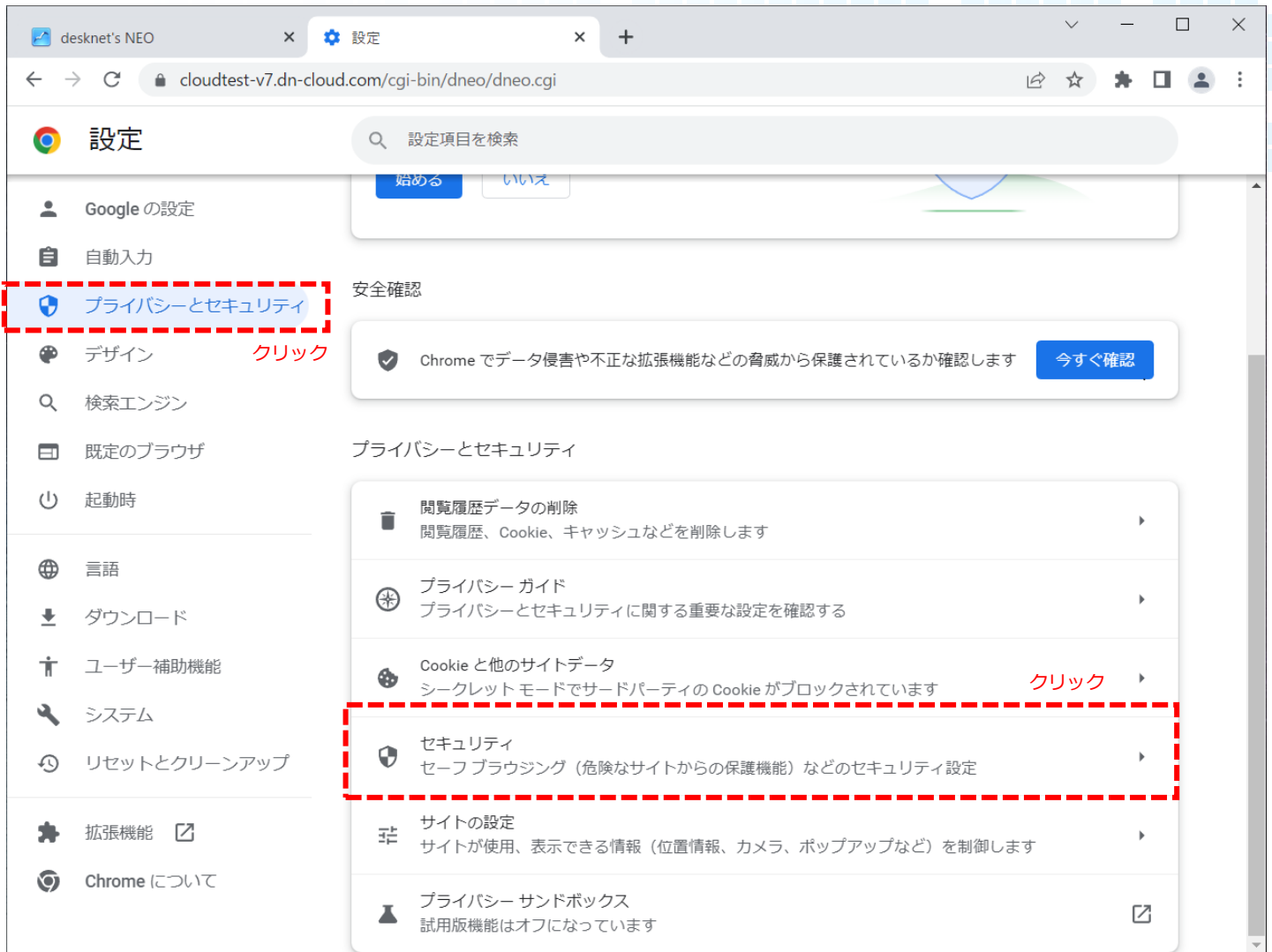
## 2. CA証明書 (cacert.pem) のインストール

- 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。



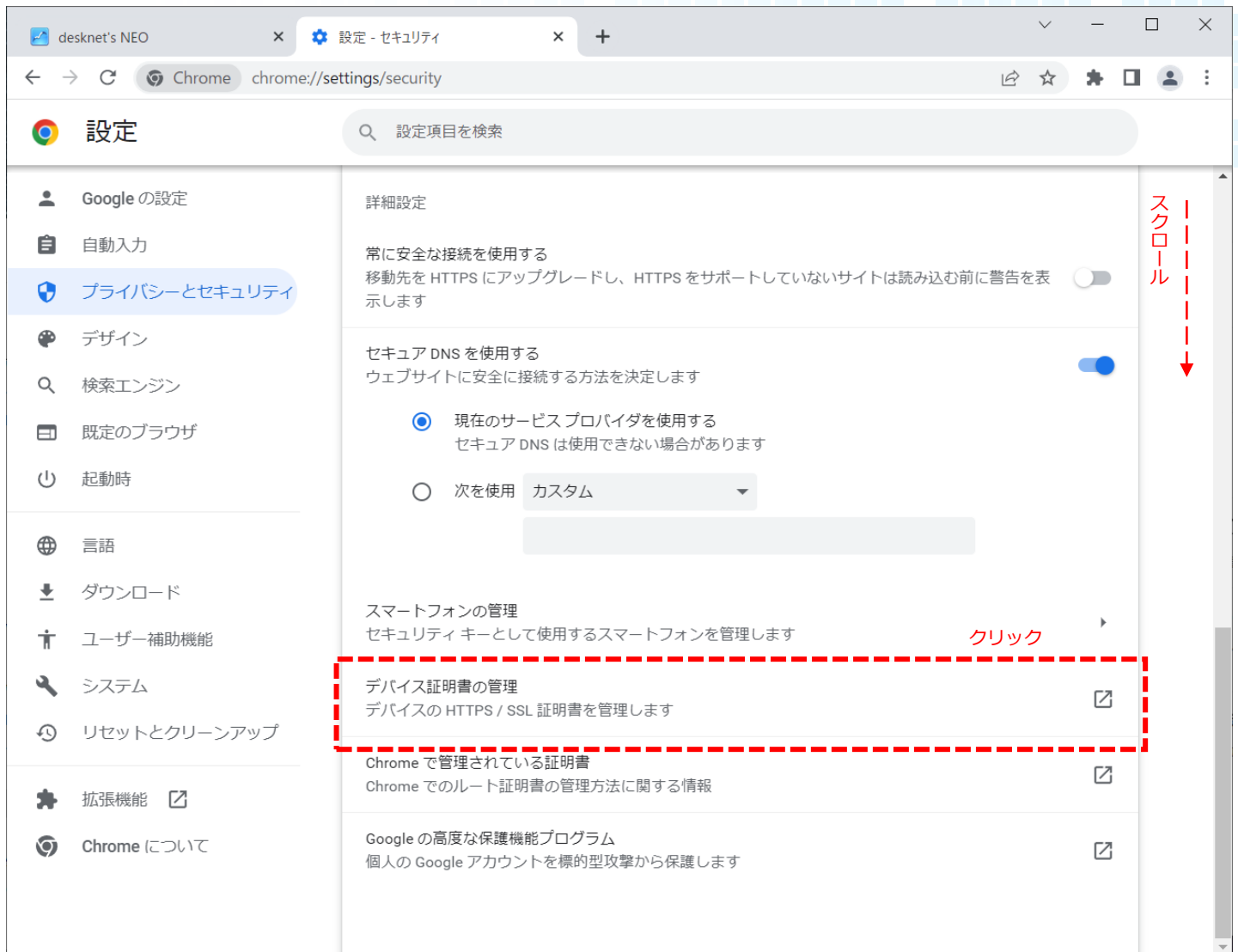
## 02 Google Chromeをご利用の場合

- 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「デバイス証明書の管理」をクリックしてください。



The screenshot shows the Google Chrome settings page for 'Security'. The left sidebar contains various settings categories, with 'Privacy and Security' selected. The main content area shows the 'Security' settings, including 'Secure DNS' and 'Smartphone Management'. The 'Device Certificate Management' option is highlighted with a red dashed box, and a red arrow points to it with the word 'クリック' (Click). A red arrow on the right side of the page indicates scrolling down.

設定 - セキュリティ

設定項目を検索

Google の設定

自動入力

プライバシーとセキュリティ

デザイン

検索エンジン

既定のブラウザ

起動時

言語

ダウンロード

ユーザー補助機能

システム

リセットとクリーンアップ

拡張機能

Chrome について

詳細設定

常に安全な接続を使用する  
移動先を HTTPS にアップグレードし、HTTPS をサポートしていないサイトは読み込む前に警告を表示します

セキュア DNS を使用する  
ウェブサイトに安全に接続する方法を決定します

現在のサービスプロバイダを使用する  
セキュア DNS は使用できない場合があります

次に使用 **カスタム**

スマートフォンの管理  
セキュリティキーとして使用するスマートフォンを管理します **クリック**

**デバイス証明書の管理**  
デバイスの HTTPS / SSL 証明書を管理します

Chrome で管理されている証明書  
Chrome でのルート証明書の管理方法に関する情報

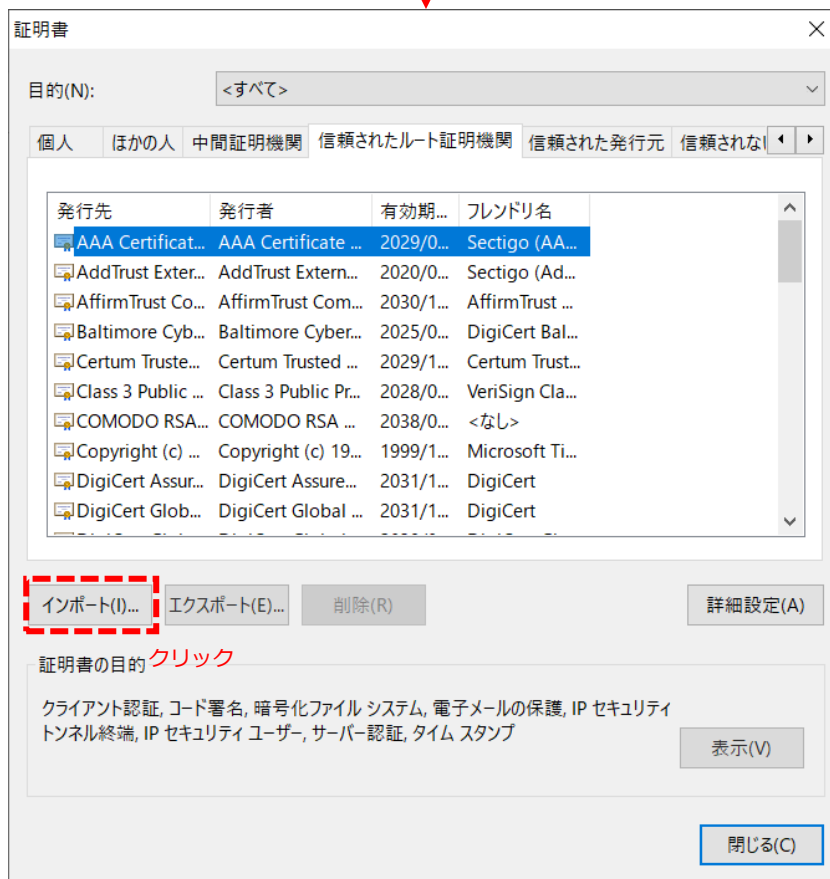
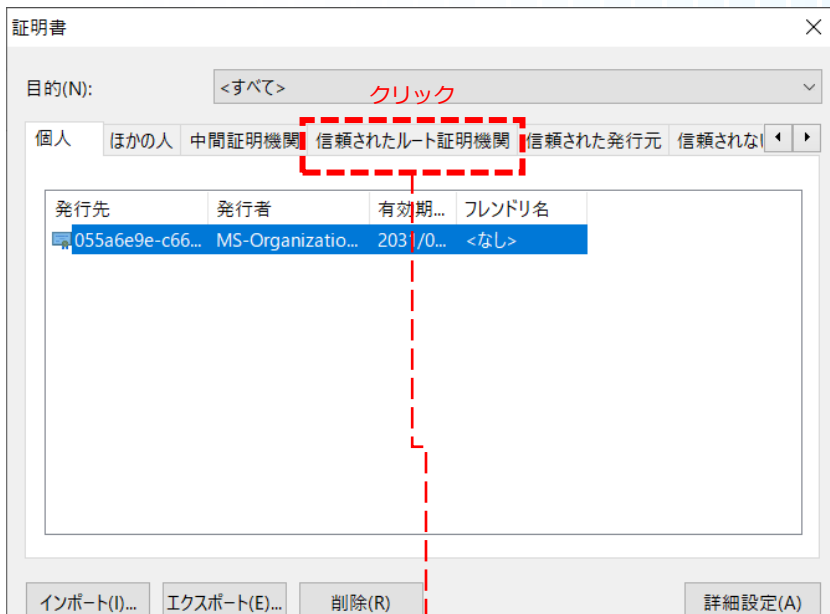
Google の高度な保護機能プログラム  
個人の Google アカウントを標的型攻撃から保護します

スクロール



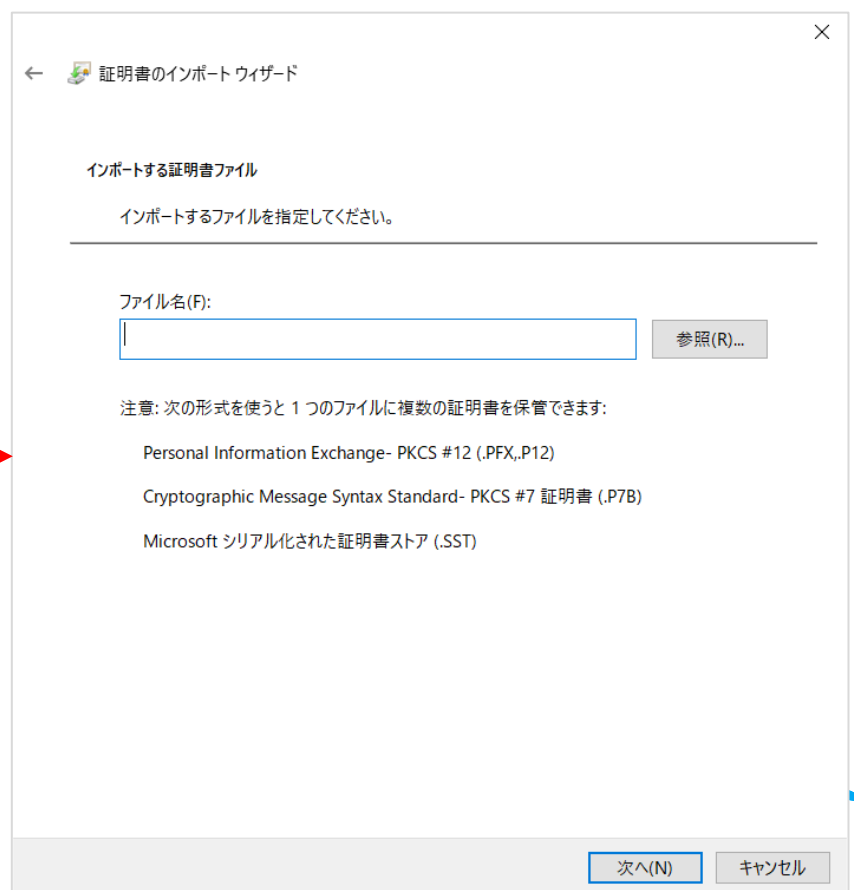
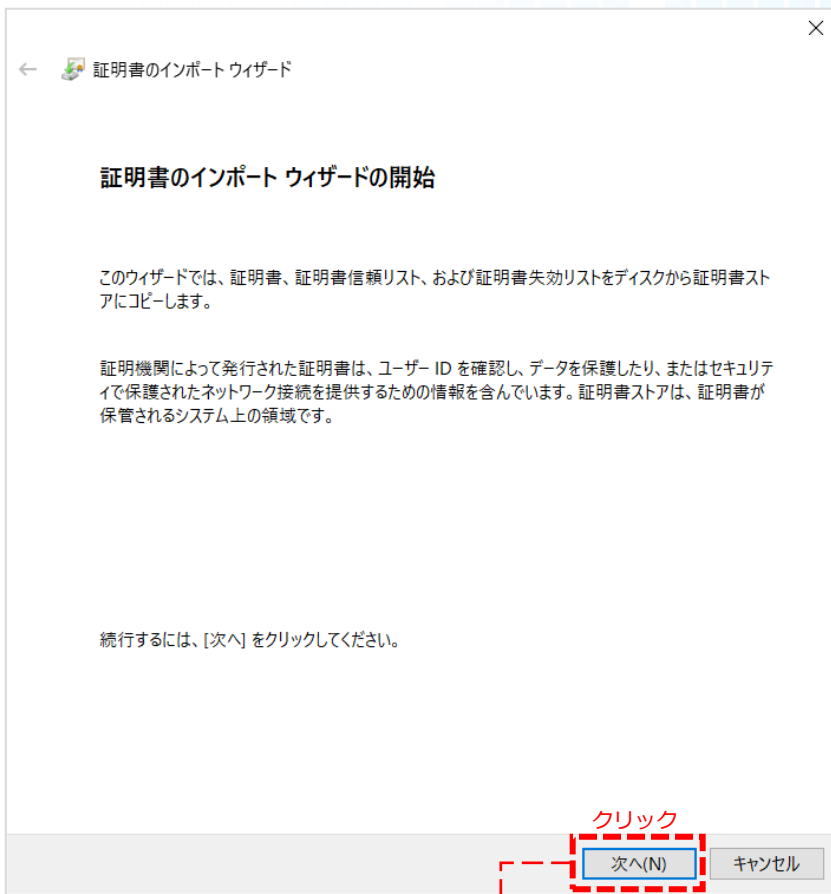
## 02 Google Chromeをご利用の場合

- 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。



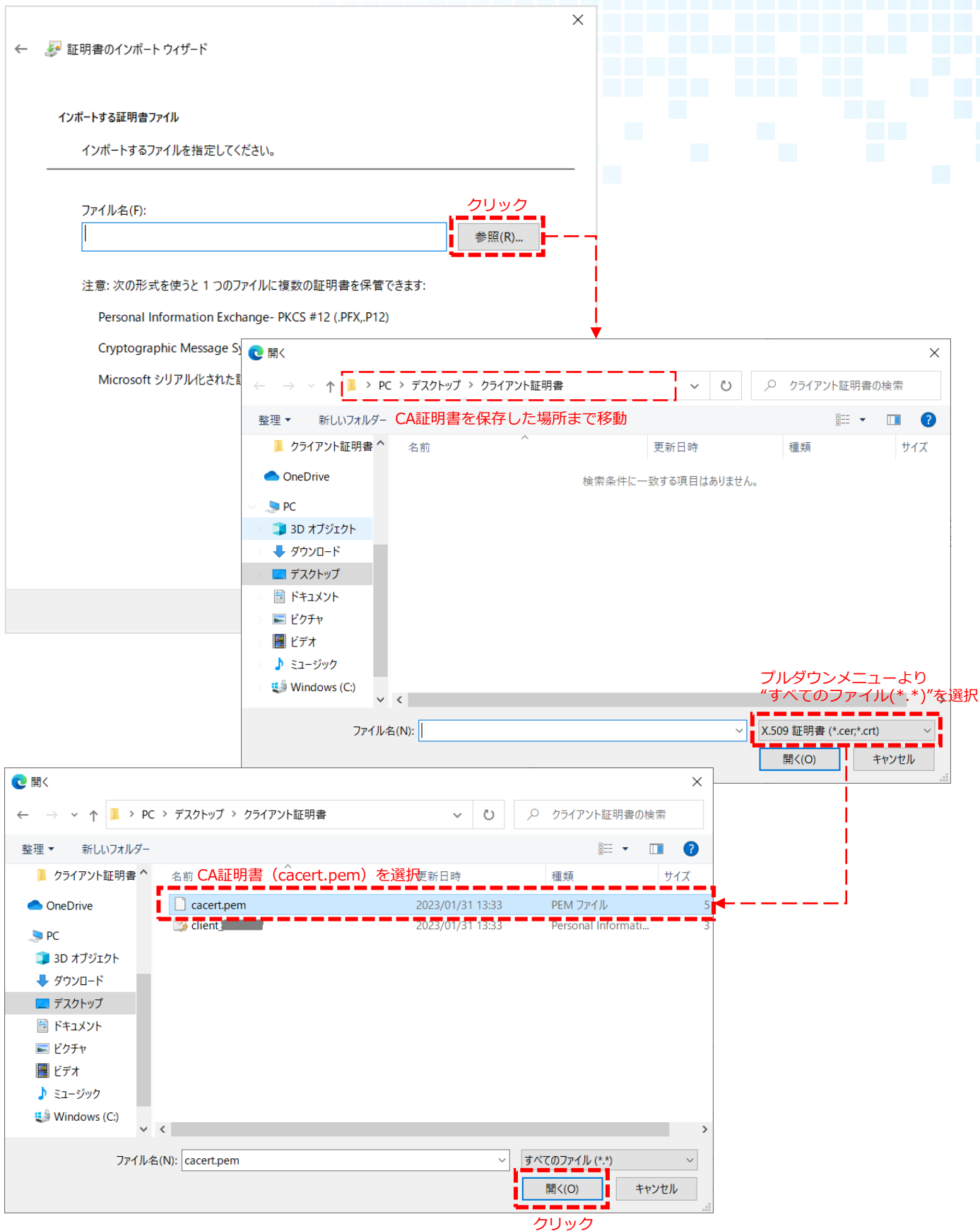
## 02 Google Chromeをご利用の場合

- 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。



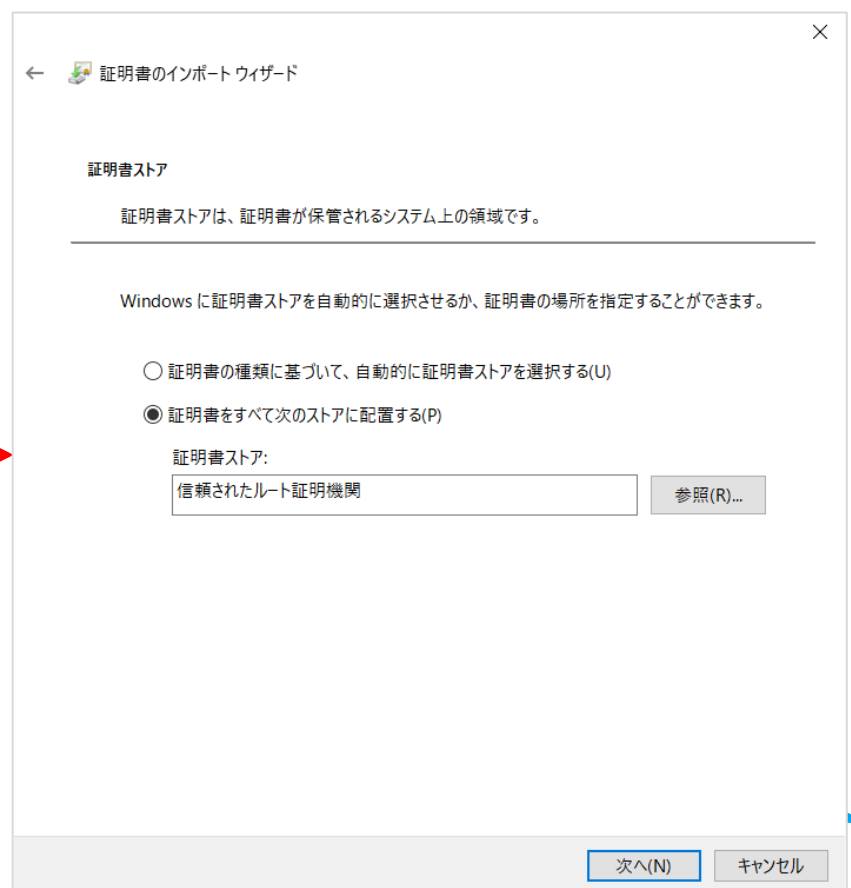
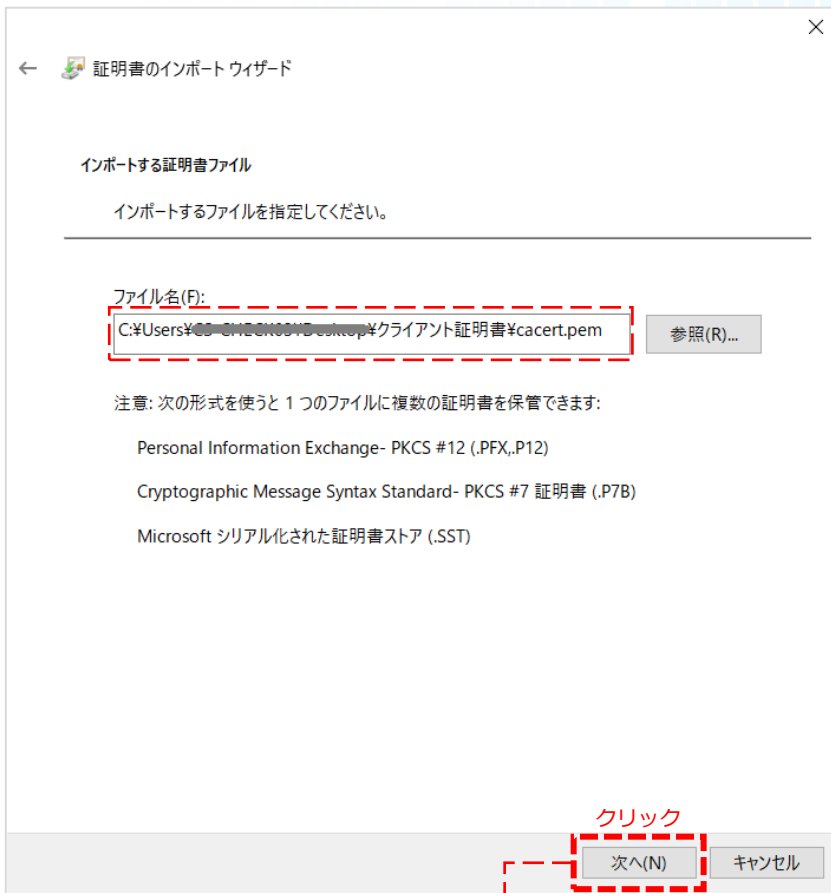
## 02 Google Chromeをご利用の場合

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。



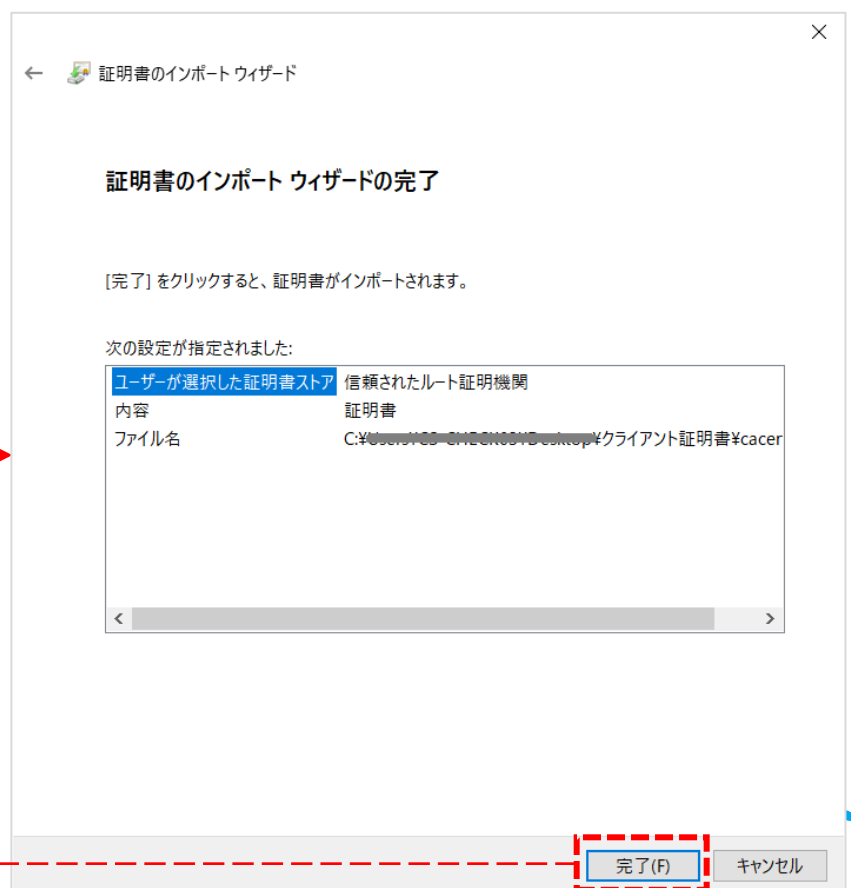
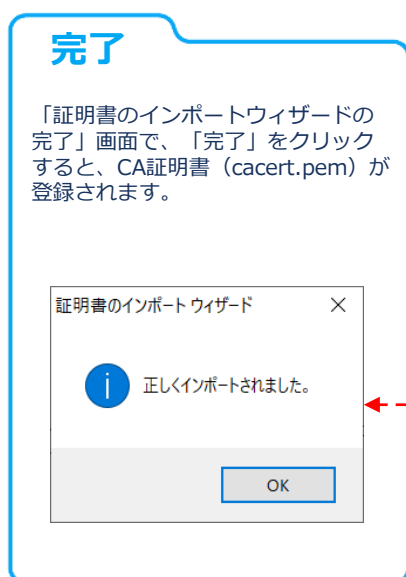
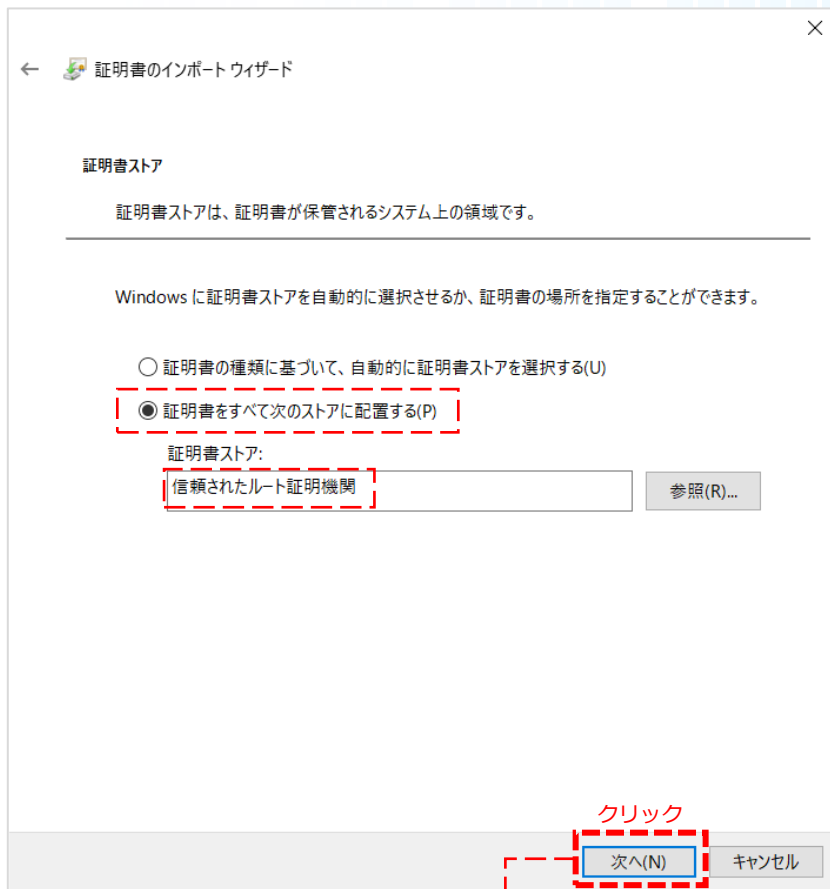
## 02 Google Chromeをご利用の場合

- 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

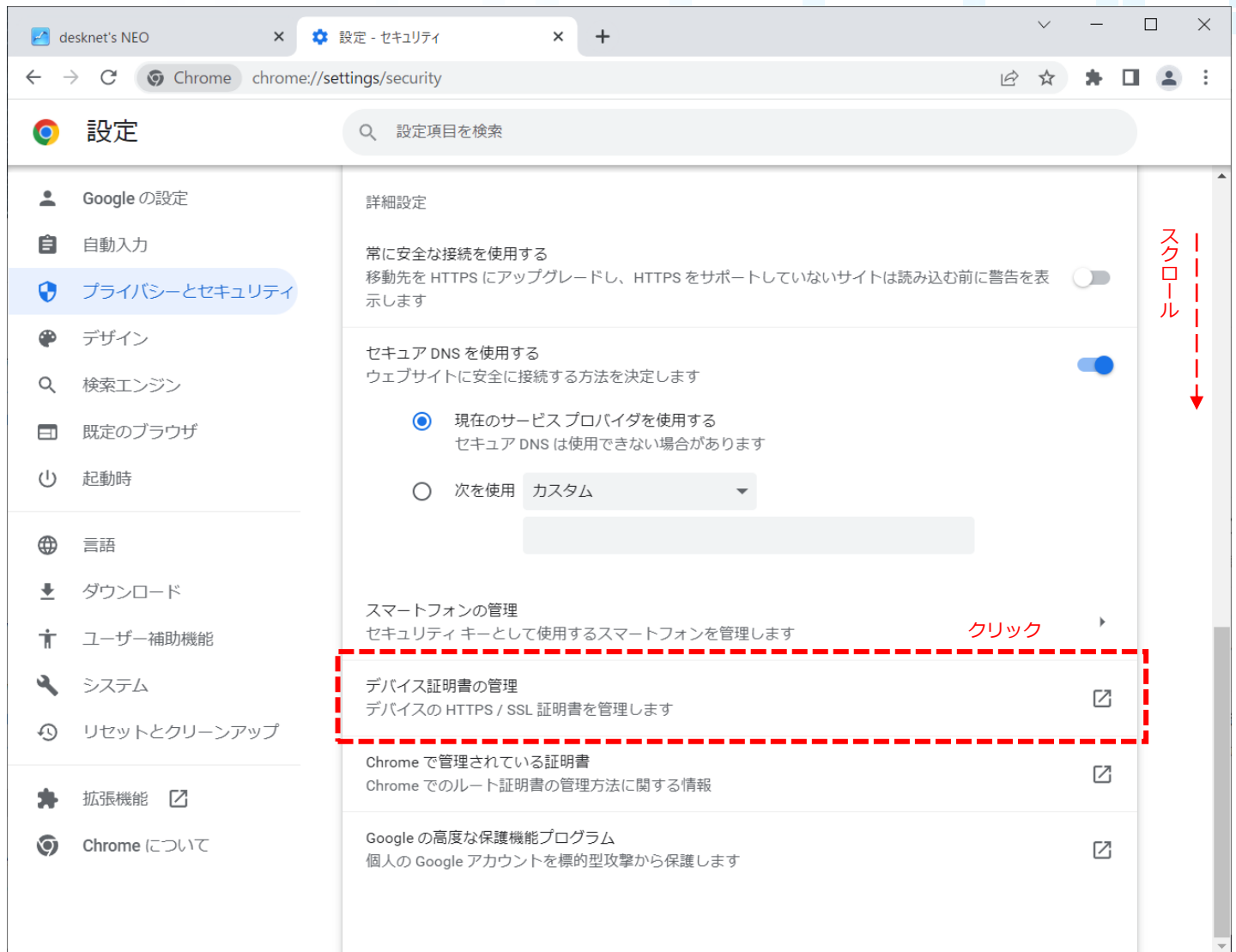
- ⑧ 「証明書をすべて次のストアに配置する(P)」のラジオボタンを選択、「証明書ストア：」に「信頼されたルート証明機関」を選択し、「次へ」ボタンをクリックします。



## 02 Google Chromeをご利用の場合

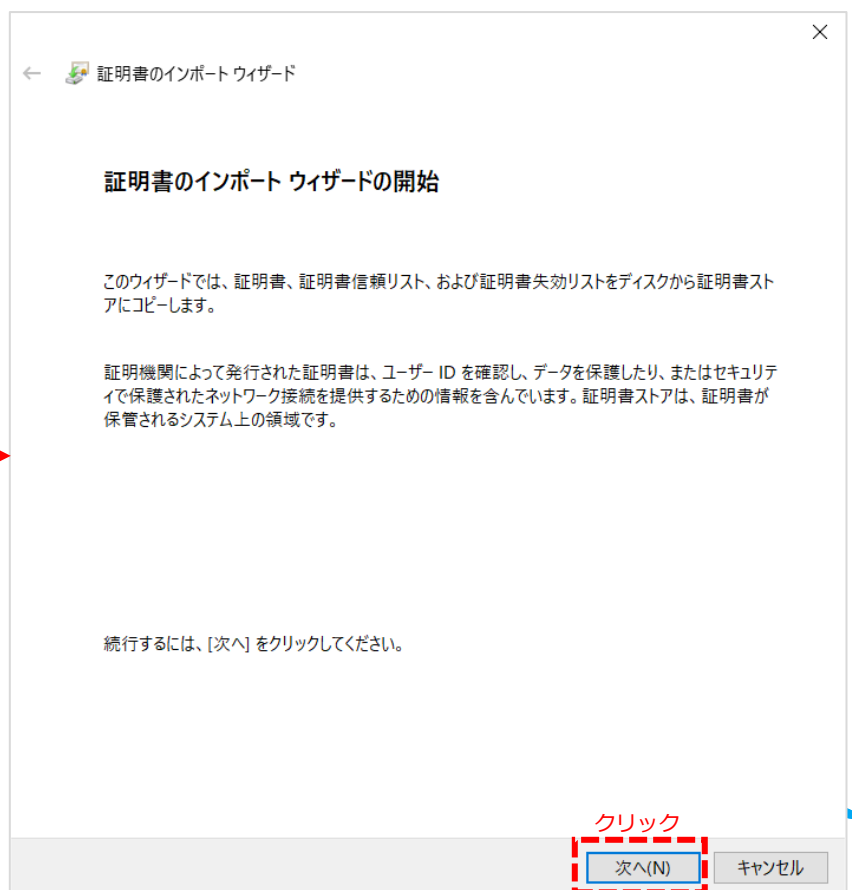
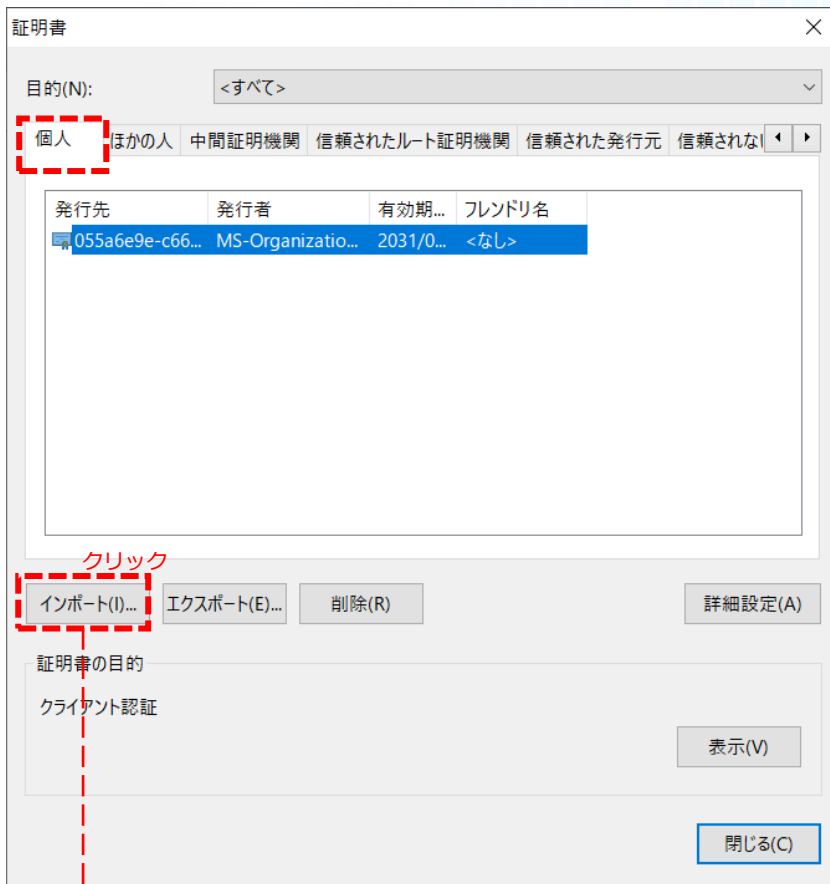
## 3. クライアント証明書ファイル (\*.pfx) のインストール

- 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。



## 02 Google Chromeをご利用の場合

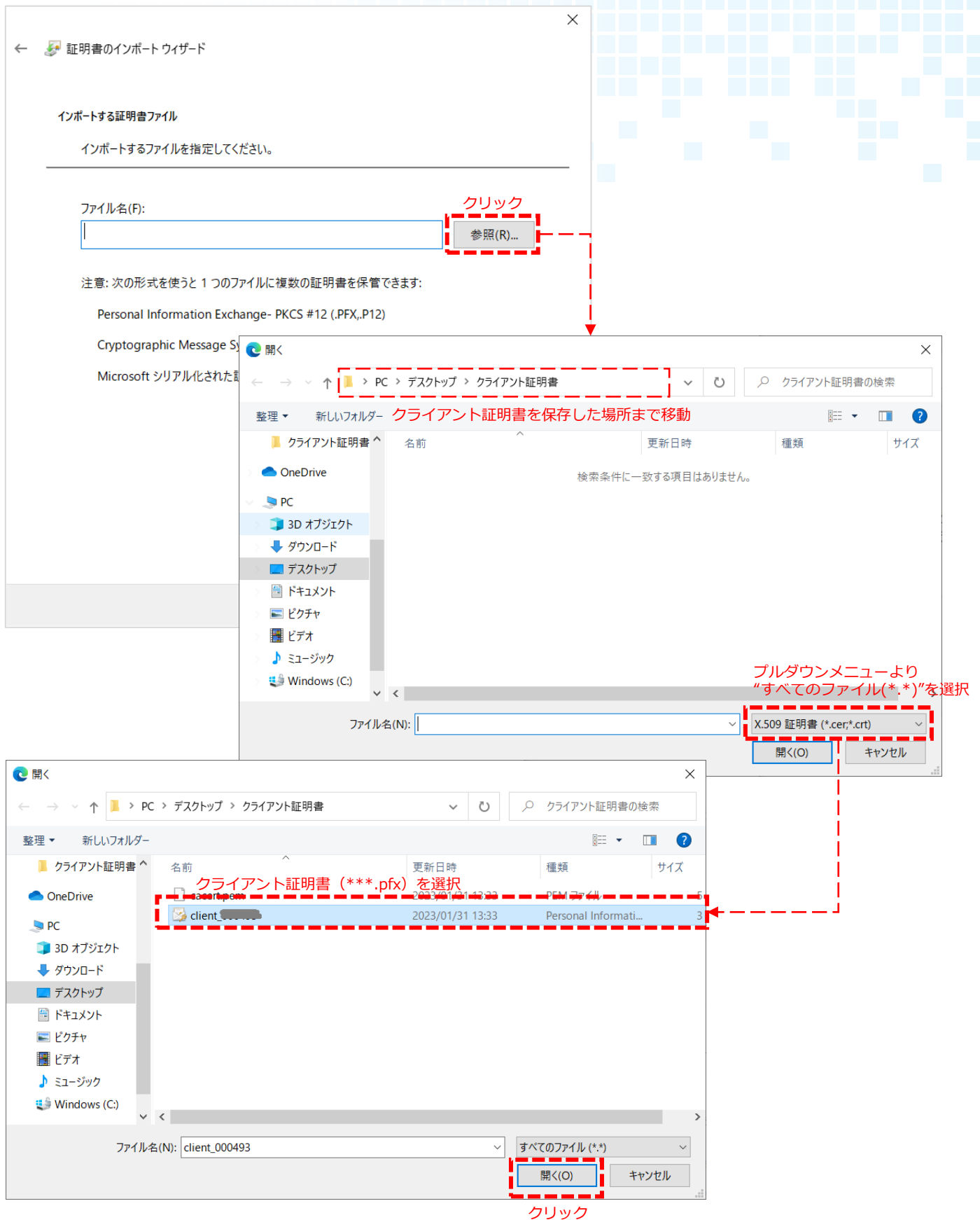
- ② 「個人」タブをクリックし、[インポート] ボタンをクリックすると、「証明書のインポートウィザード」が表示されますので、[次へ] ボタンをクリックしてください。





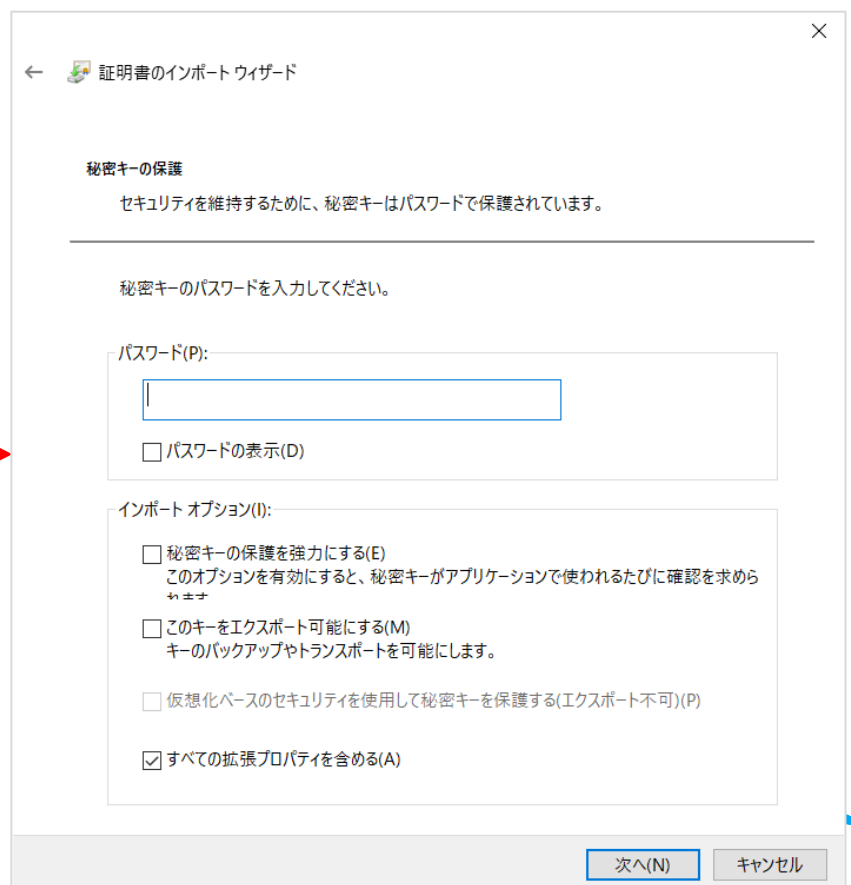
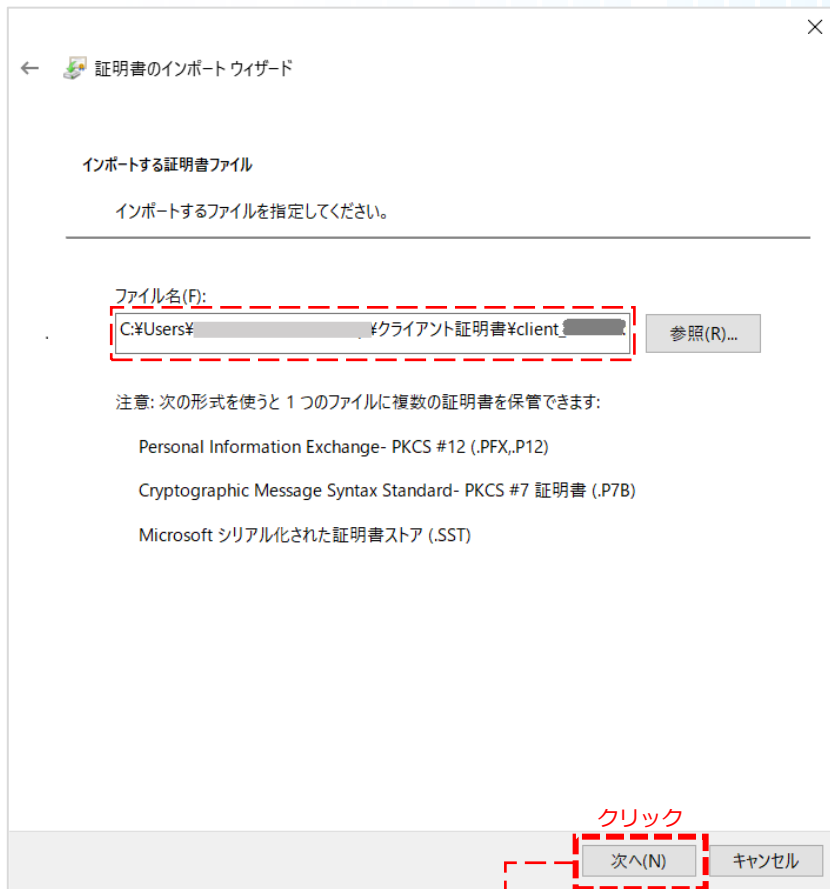
## 02 Google Chromeをご利用の場合

- 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。



## 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

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。

← 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:

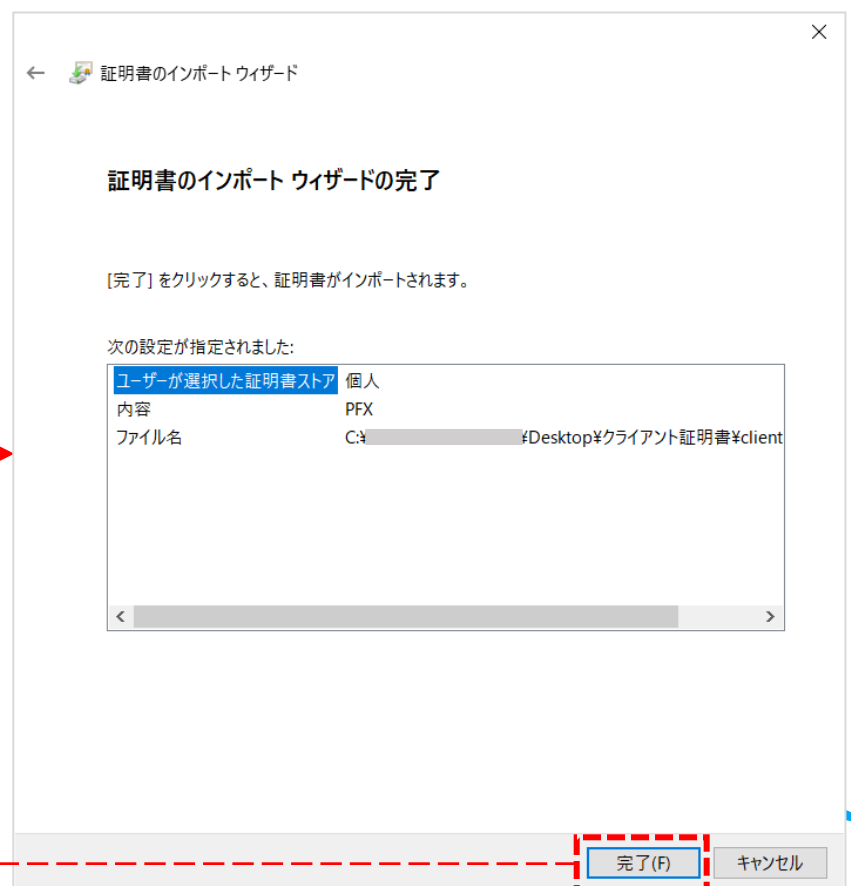
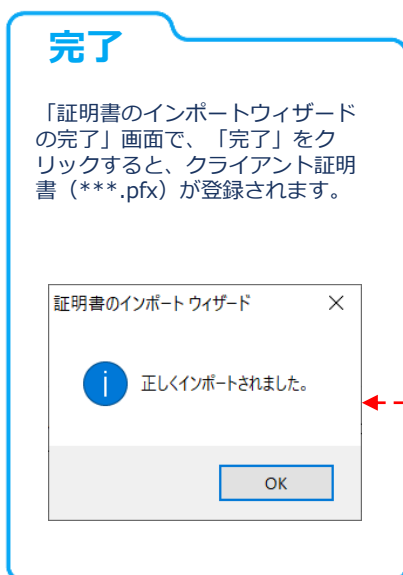
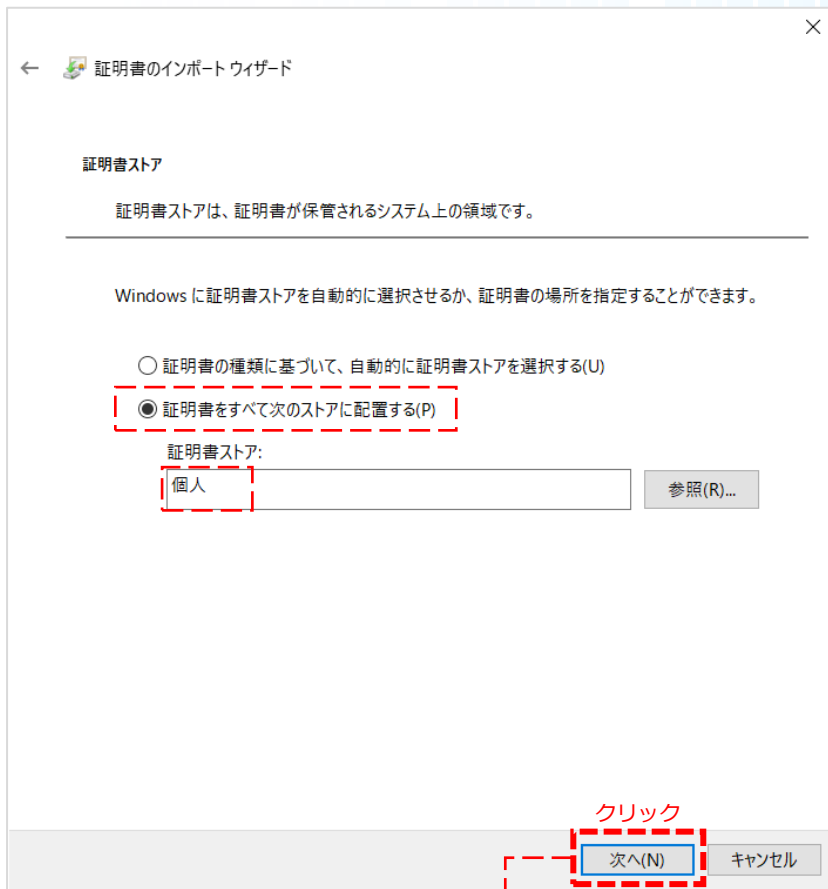
個人

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。



## 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。

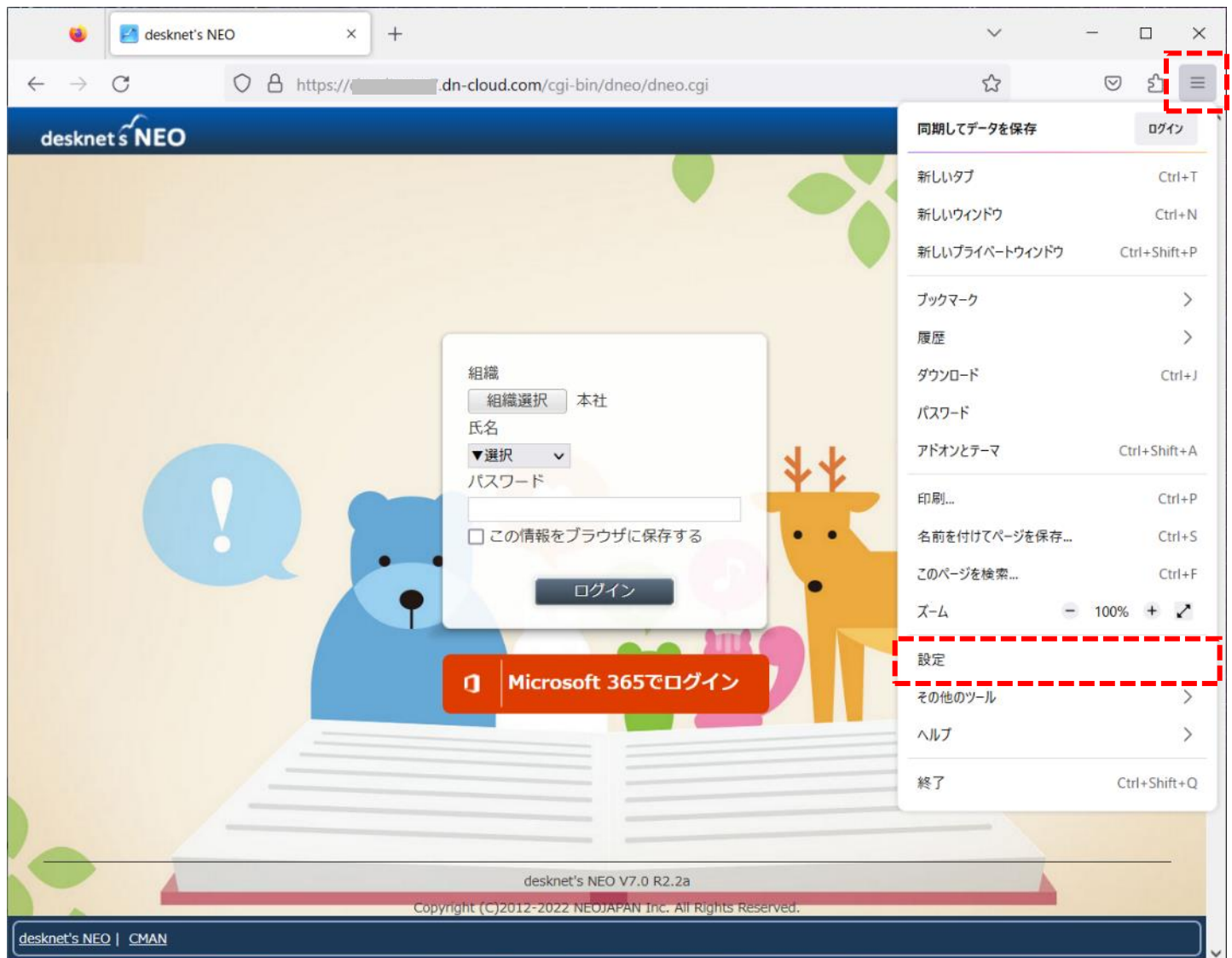
## 1. クライアント認証サービス用のファイルの準備

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

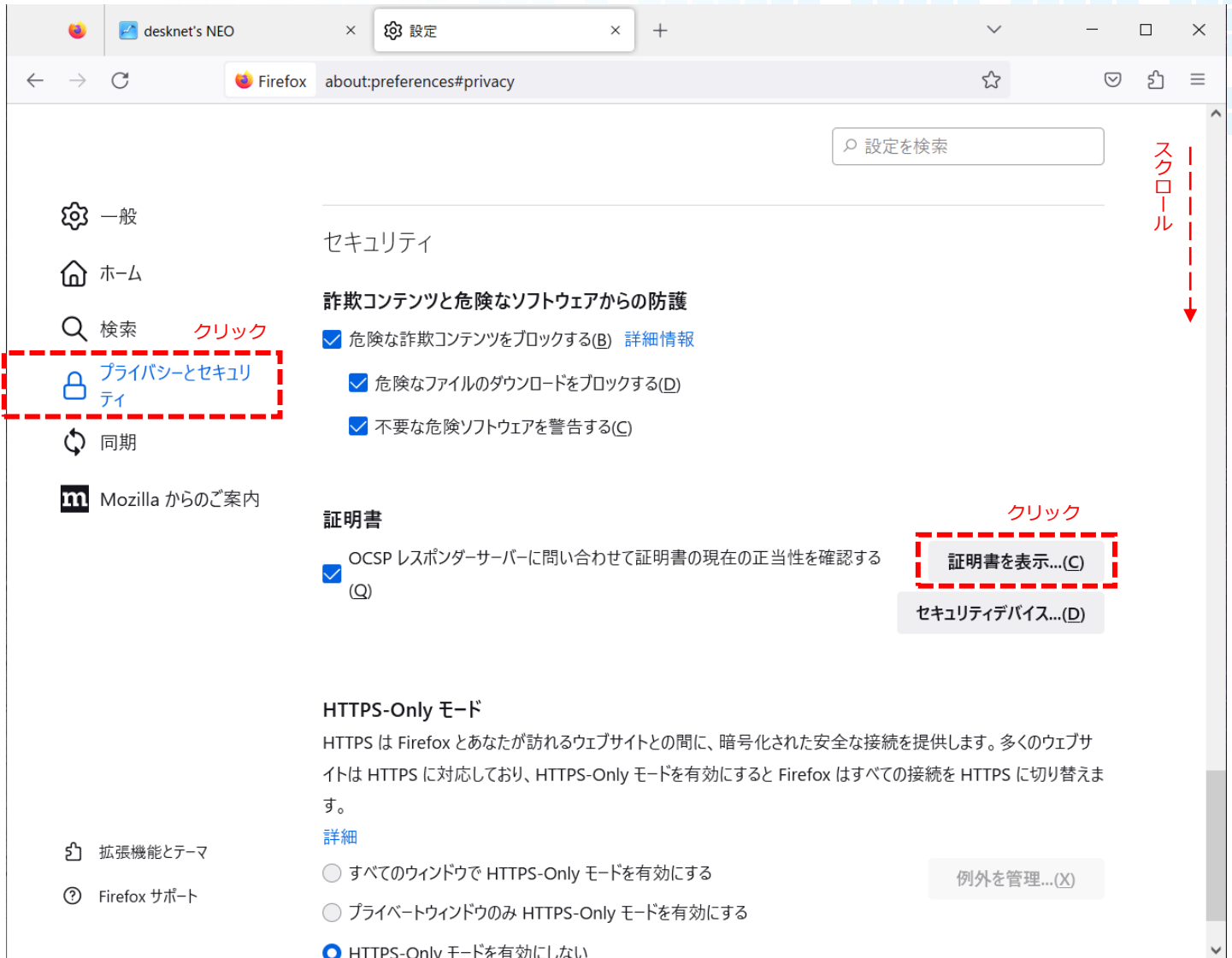
## 2. CA証明書 (cacert.pem) のインストール

- 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。



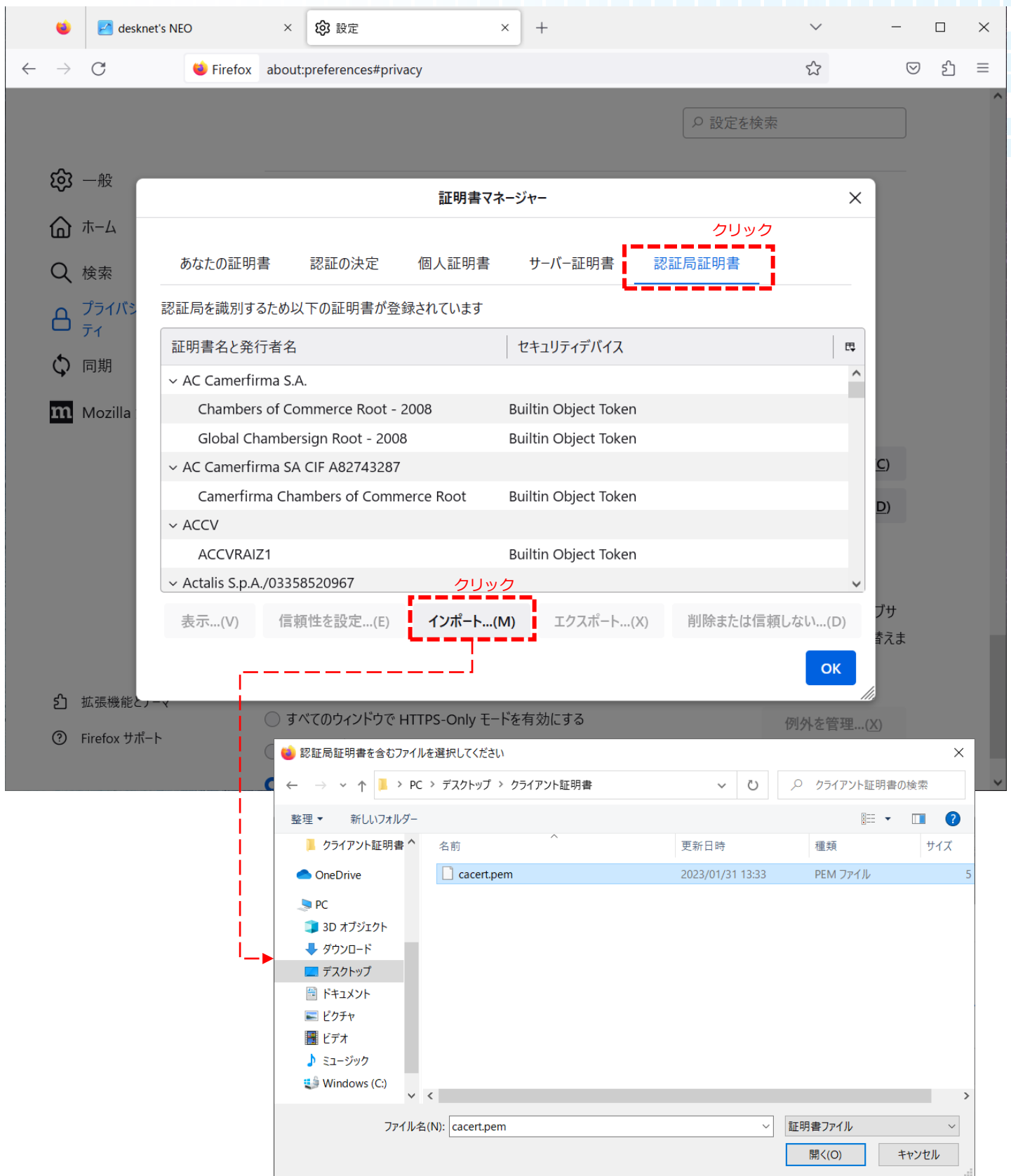
## 03 Mozilla Firefoxをご利用の場合

- 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

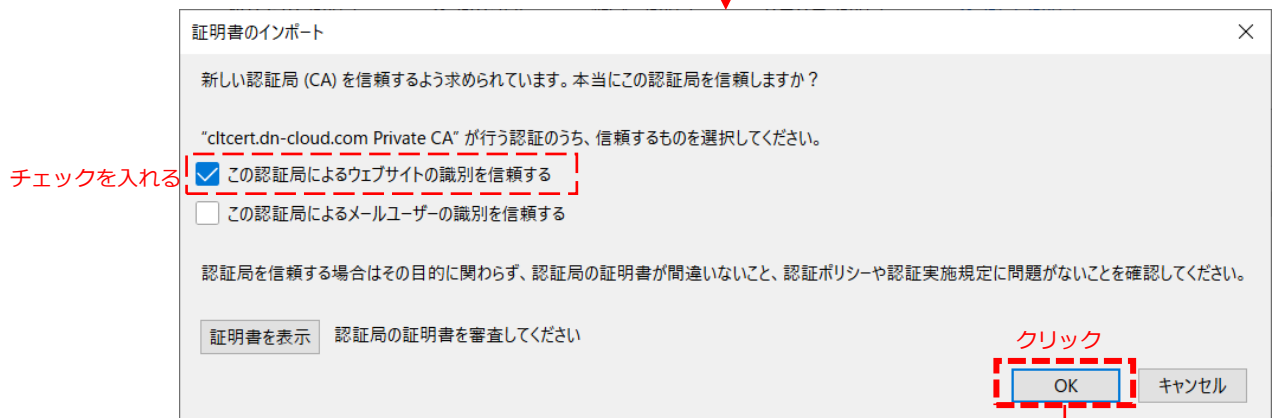
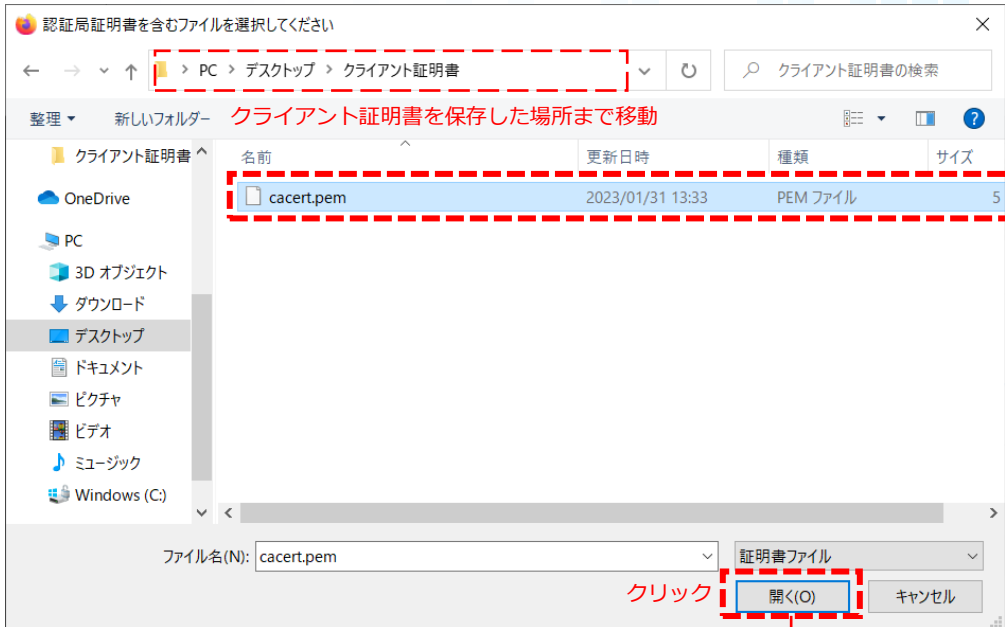
③ 「証明局証明書」タブを選択し、[インポート] ボタンをクリックしてください。





### 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。



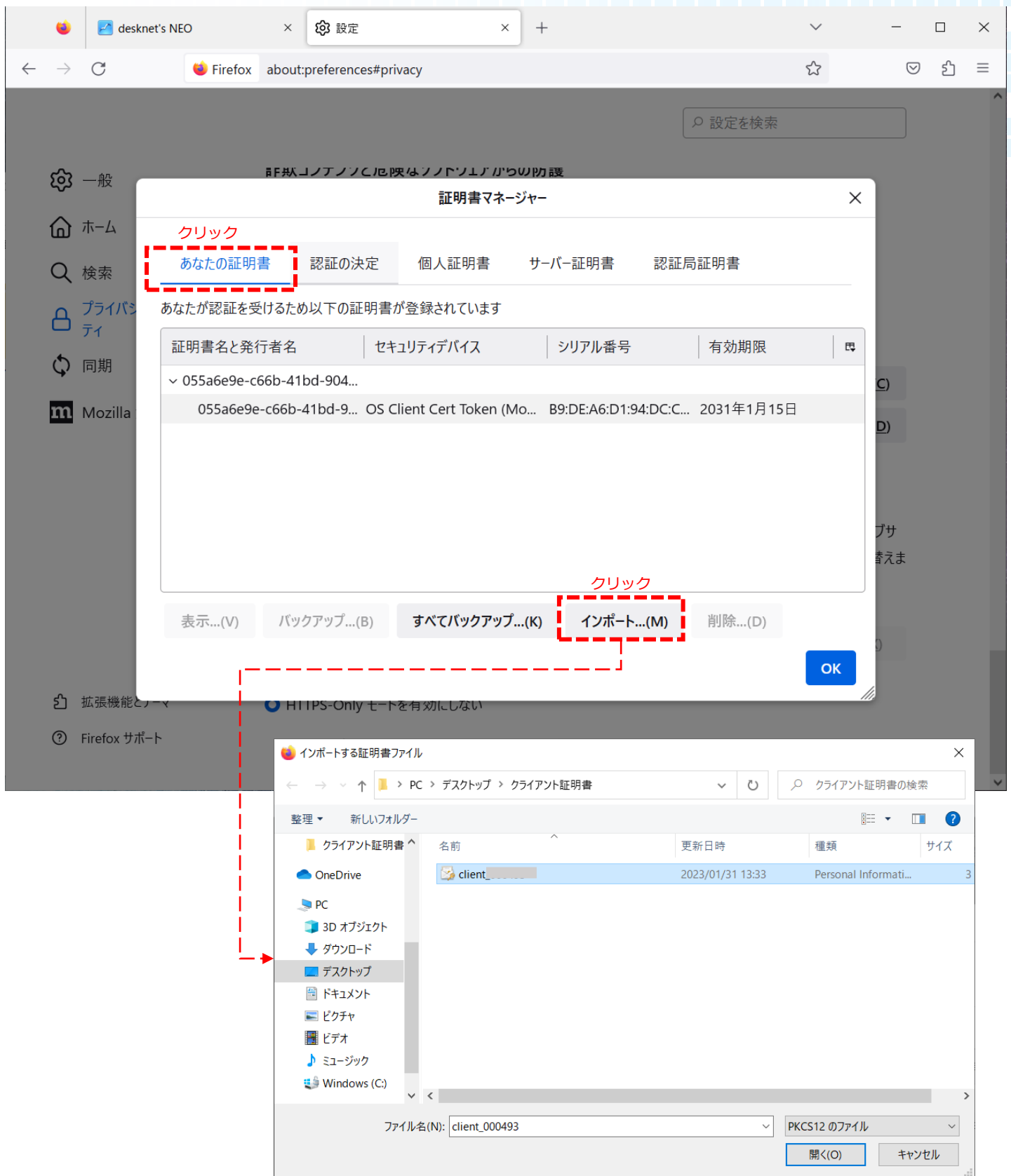
## 3. クライアント証明書ファイル (\*.pfx) のインストール

- 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。



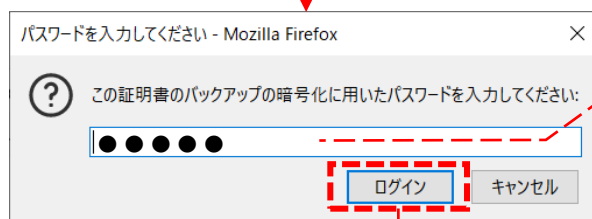
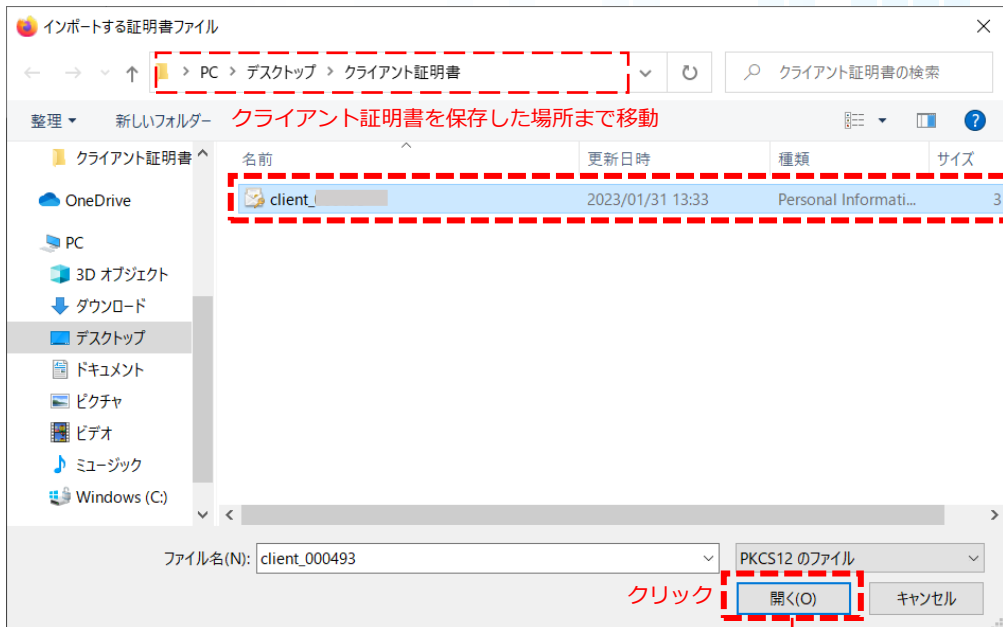
## 03 Mozilla Firefoxをご利用の場合

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。

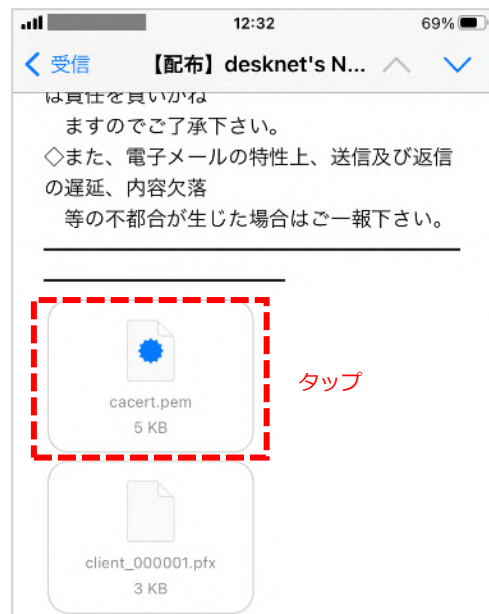
## 1. クライアント認証サービス用のファイルの準備

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。

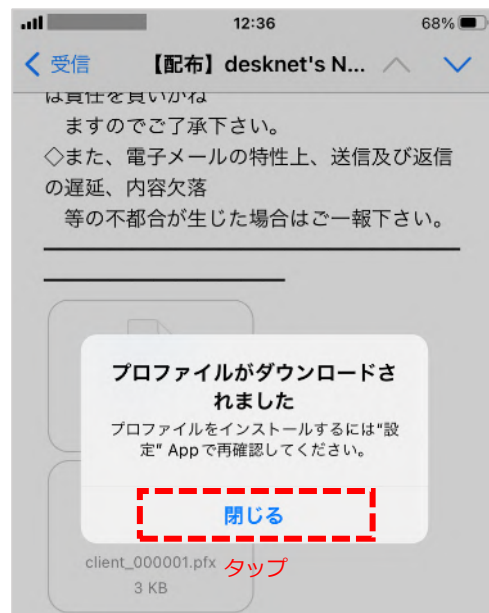
- CA証明書ファイル (cacert.pem)
- クライアント証明書ファイル (\*\*\*.pfx)
- 配布されたクライアント証明書ファイルのパスワード

## 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) をタップします。

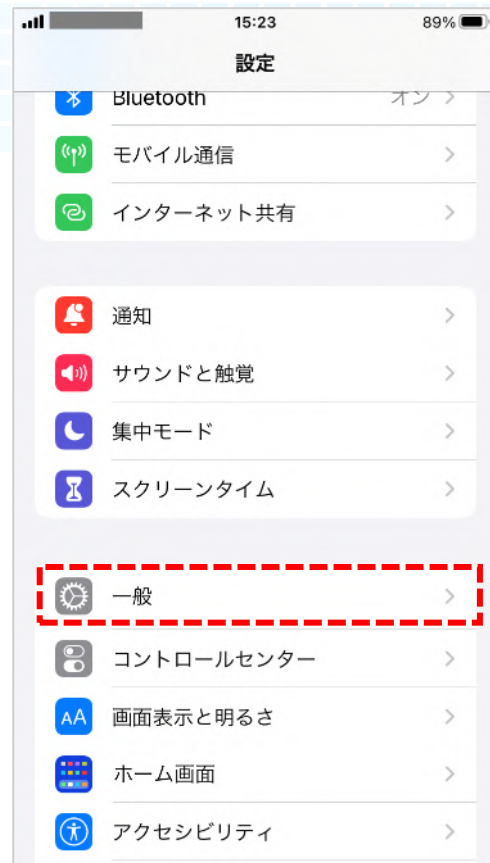


- ② ダウンロードが完了するとメッセージが表示されるので、「閉じる」をタップします。



## 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。



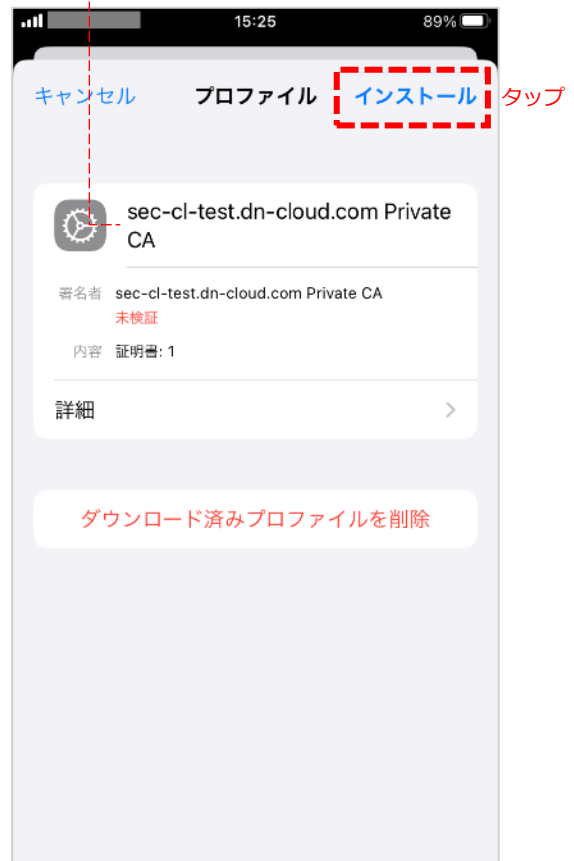
- iOS 13の場合  
「VPNとデバイス管理」はメニューにございません。  
「プロファイル」を選択ください。
- iOS 14の場合  
「VPNとデバイス管理」はメニューにございません。  
「プロファイルとデバイス管理」を選択ください。

## 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。

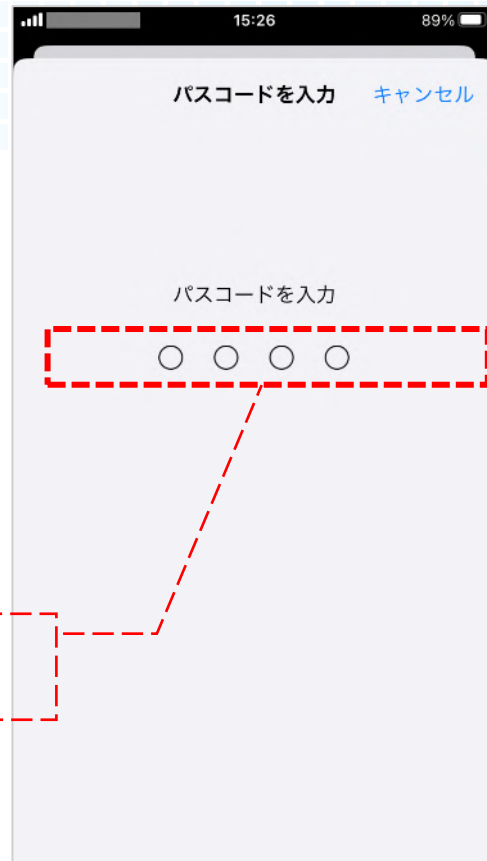


- ⑥ 「インストール」をタップします。



## 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。



パスコードは、ご利用のiPhoneの機種により、桁数が異なります。

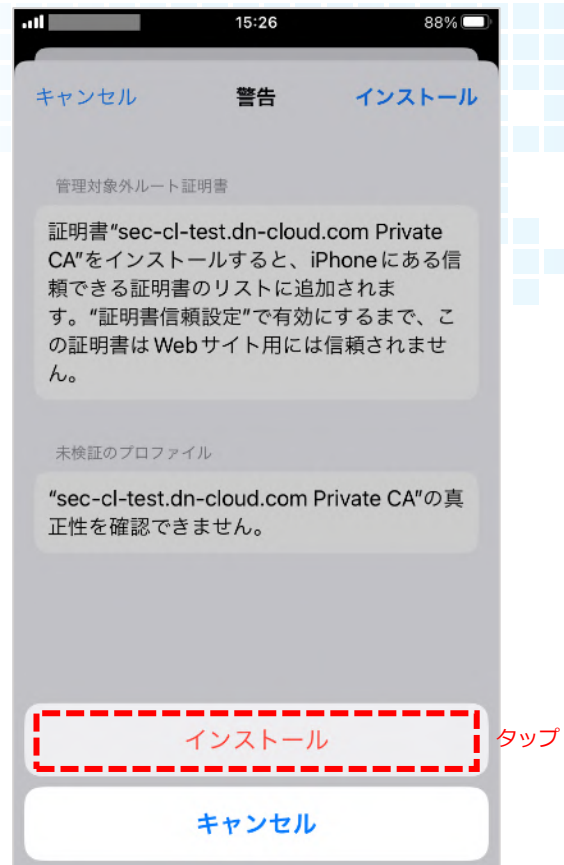
- ⑧ 警告メッセージが表示されますが、そのまま「インストール」をタップします。





## 04 iPhone(iOS)をご利用の場合

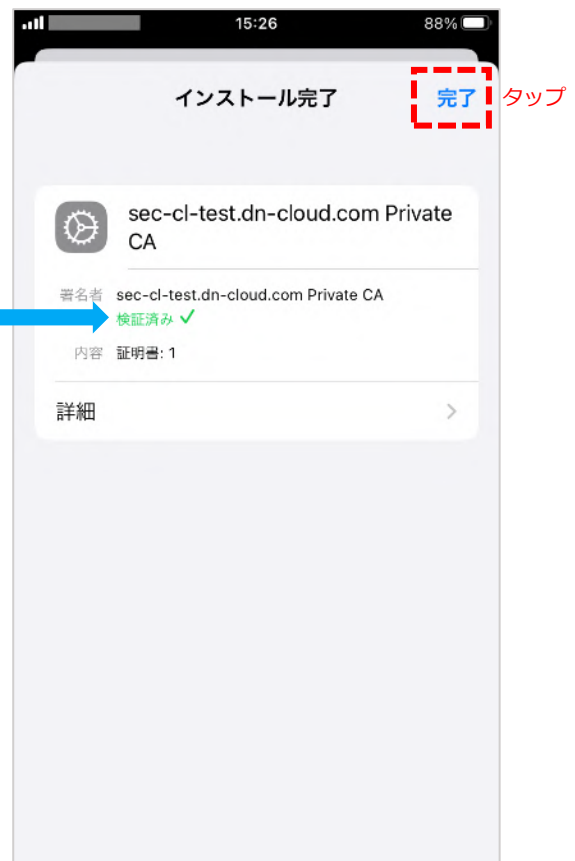
⑨ 再度「インストール」をタップします。



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。

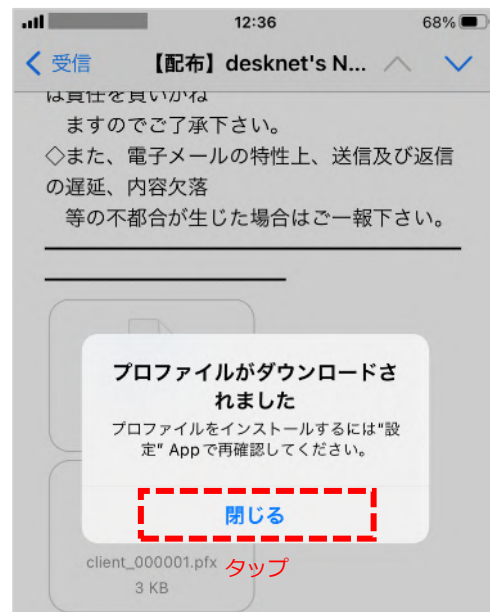


### 3. クライアント証明書ファイル (\*.pfx) のインストール

- 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) をタップします。

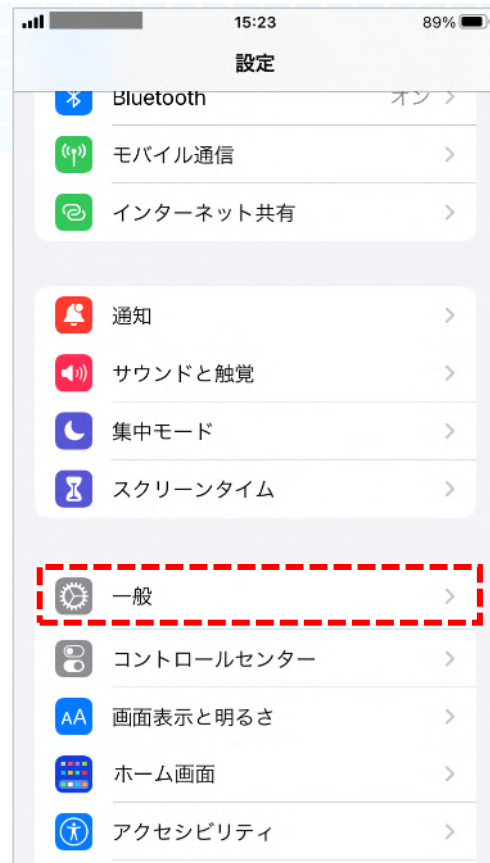


- ② ダウンロードが完了するとメッセージが表示されるので、「閉じる」をタップします。



## 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。

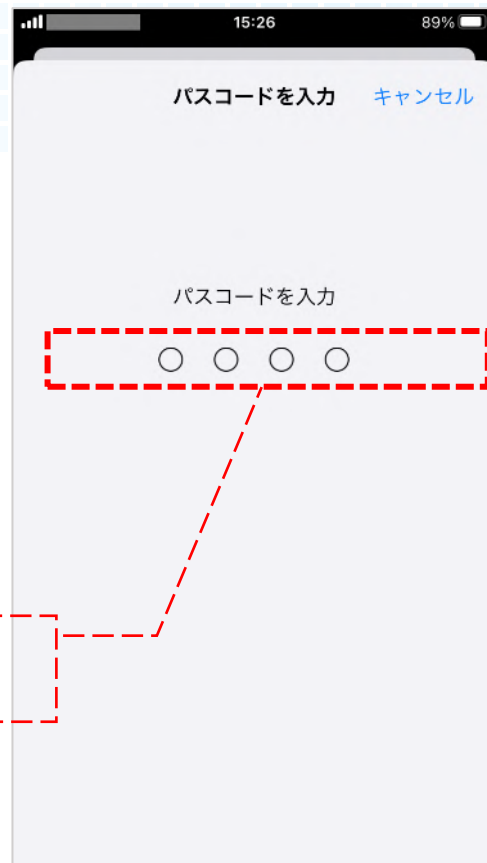


- ⑥ 「インストール」をタップします。



## 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。

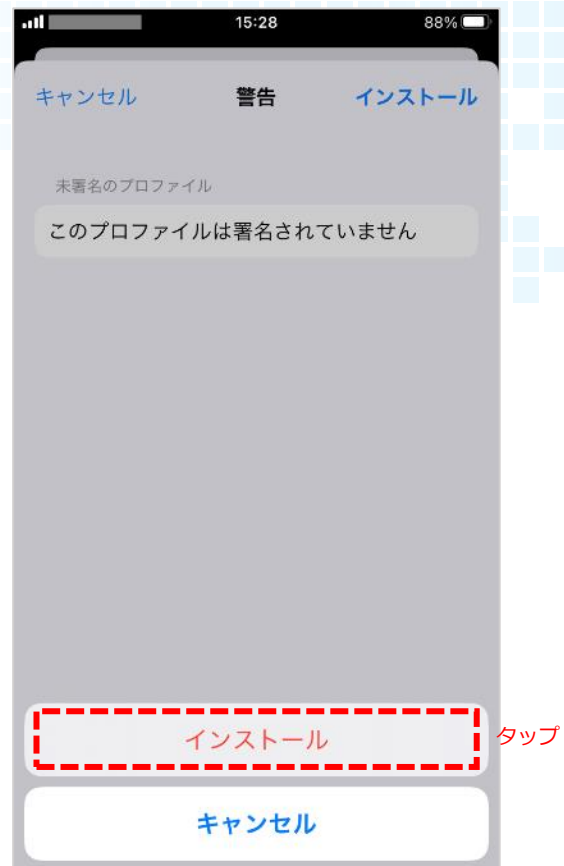


- ⑧ 警告メッセージが表示されますが、そのまま「インストール」をタップします。

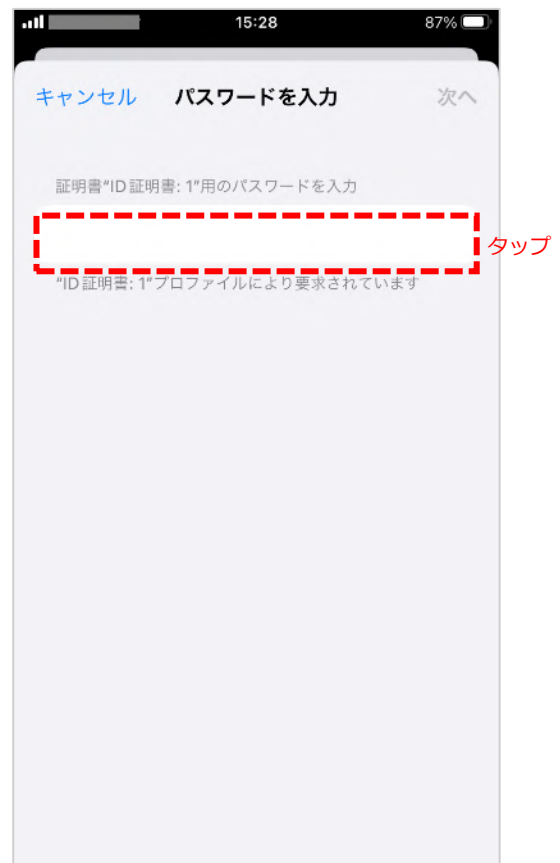


## 04 iPhone(iOS)をご利用の場合

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。

## 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)

**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**

