

//////////////////////////////////// 管理者向け //////////////////////////////////////

## desknet's NEO

# クライアント証明書発行サイト用 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>ご利用まで流れ</b> .....	<b>3</b>
<b>02</b>	<b>Microsoft Edgeをご利用の場合</b> .....	<b>4</b>
	1. クライアント証明書発行サイト用のファイルの準備 .....	4
	2. CA証明書 (cacert.pem) のインストール .....	4
	3. クライアント証明書ファイル (*.pfx) のインストール .....	11
<b>03</b>	<b>Google Chromeをご利用の場合</b> .....	<b>17</b>
	1. クライアント証明書発行サイト用のファイルの準備 .....	17
	2. CA証明書 (cacert.pem) のインストール .....	17
	3. クライアント証明書ファイル (*.pfx) のインストール .....	25
<b>04</b>	<b>Mozilla Firefoxをご利用の場合</b> .....	<b>31</b>
	1. クライアント証明書発行サイト用のファイルの準備 .....	31
	2. CA証明書 (cacert.pem) のインストール .....	31
	3. クライアント証明書ファイル (*.pfx) のインストール .....	35



## 01

## サービスご利用まで流れ

各ユーザーにご利用いただくクライアント証明書は、「クライアント認証書発行サイト」より、お客様自身で発行し配布いただくことで、配布可能となります。

また「クライアント認証書発行サイト」にアクセスするには、弊社より送付されたメール「件名：【重要】desknet's クラウドクライアント認証オプション証明書のご送付」に添付されている証明書類（圧縮ファイル）を発行管理を担当されるユーザー様ご利用端末へインストールが必要です。

### 下準備

案内メールに添付されている圧縮ファイルをダウンロードし、管理用端末に解凍してください。解凍すると、下記ファイルが表示されます。

- CA証明書ファイル (cacert.pem)
- クライアント証明書ファイル (\*\*\*.pfx)

### クライアント認証書発行サイト用クライアント証明書のインストール

【本書】発行サイト用のCA証明書および、クライアント証明書をインストールします。

### クライアント認証書発行サイトへのアクセスおよび、サイト操作

前段の証明書インストールが完了している端末で (<https://cltcert.dn-cloud.com/ncp/>) へアクセスするとログイン画面が表示されます。

- ログイン情報は、「件名：【重要】desknet's クラウドクライアント認証オプション証明書のご送付」内の[クライアント認証書発行サイトログイン情報]をご確認ください。

※操作方法は、マニュアル「クライアント証明書発行サイト 基本操作」を参照ください。

### 発行・配布されたクライアント証明書のインストール

※マニュアル「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」をご参照ください。

# 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。

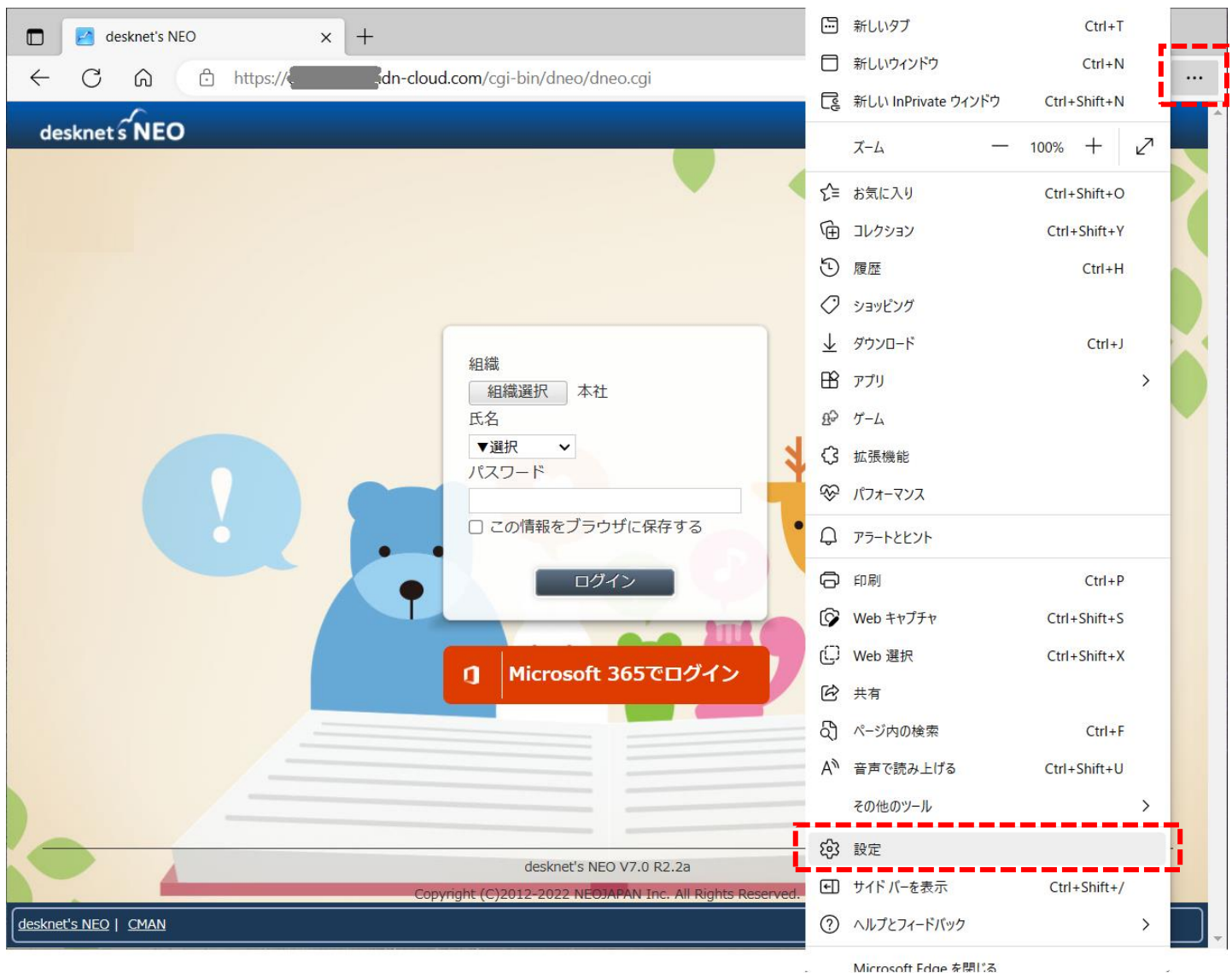
## 1. クライアント証明書発行サイト用のファイルの準備

案内メールに添付されている圧縮ファイルをダウンロードし、管理用端末に解凍してください。解凍すると、下記ファイルが表示されます。

- CA証明書ファイル (cacert.pem)
- クライアント証明書ファイル (\*\*\*.pfx)

## 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。



## 02 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。

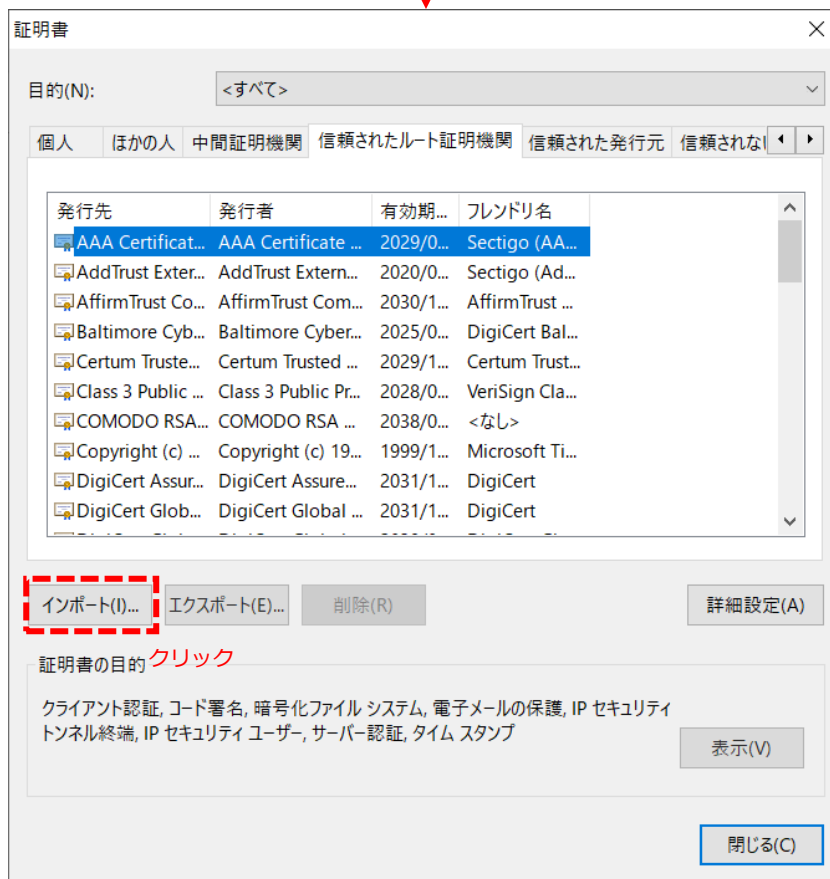
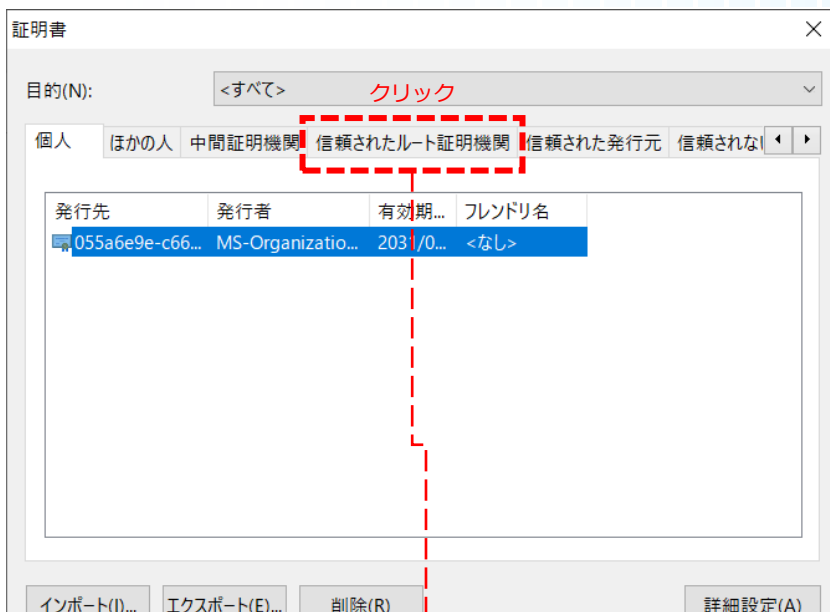
The screenshot shows the Microsoft Edge settings page at `edge://settings/privacy`. The left sidebar has '設定' (Settings) and a search bar. The 'プライバシー、検索、サービス' (Privacy, Search, Services) option is highlighted with a red dashed box and labeled 'クリック' (Click). The main content area is 'セキュリティ' (Security), with '証明書の管理' (Certificate Management) highlighted and labeled 'クリック' (Click). A red dashed arrow on the right indicates scrolling down. A '証明書' (Certificate) dialog box is open, showing a table of certificates:

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

Buttons at the bottom of the dialog include '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)'.

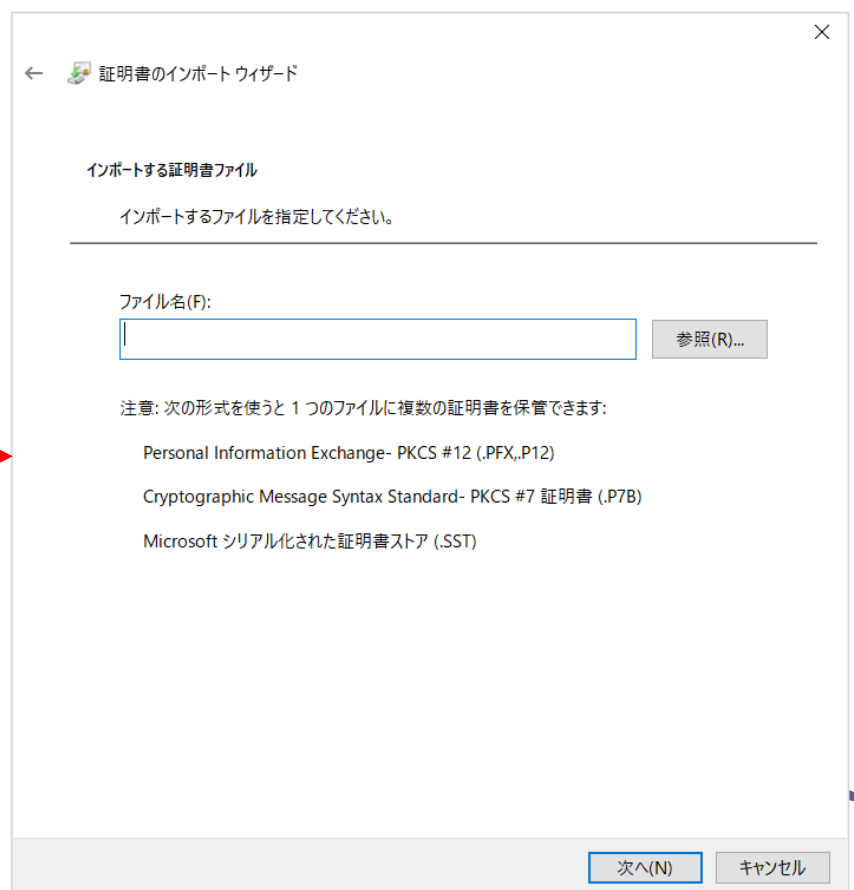
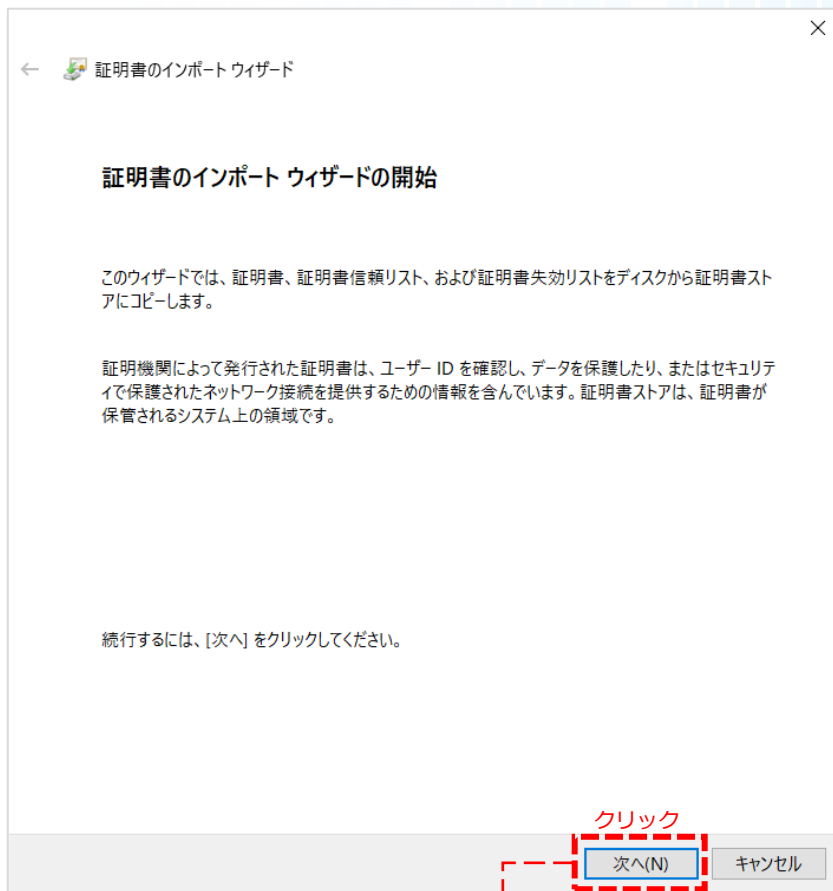
## 02 Microsoft Edgeをご利用の場合

- 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。



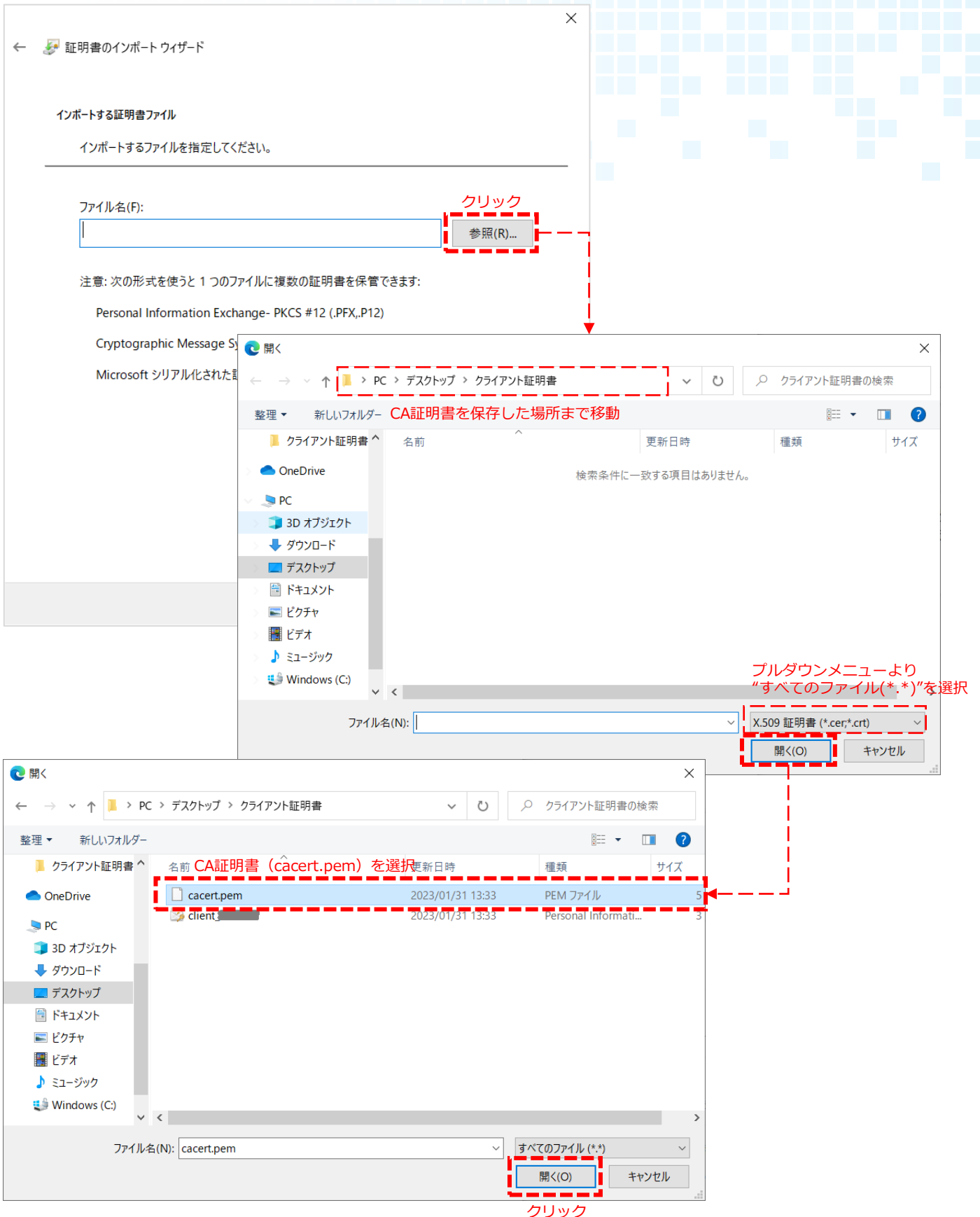
## 02 Microsoft Edgeをご利用の場合

- 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。



## 02 Microsoft Edgeをご利用の場合

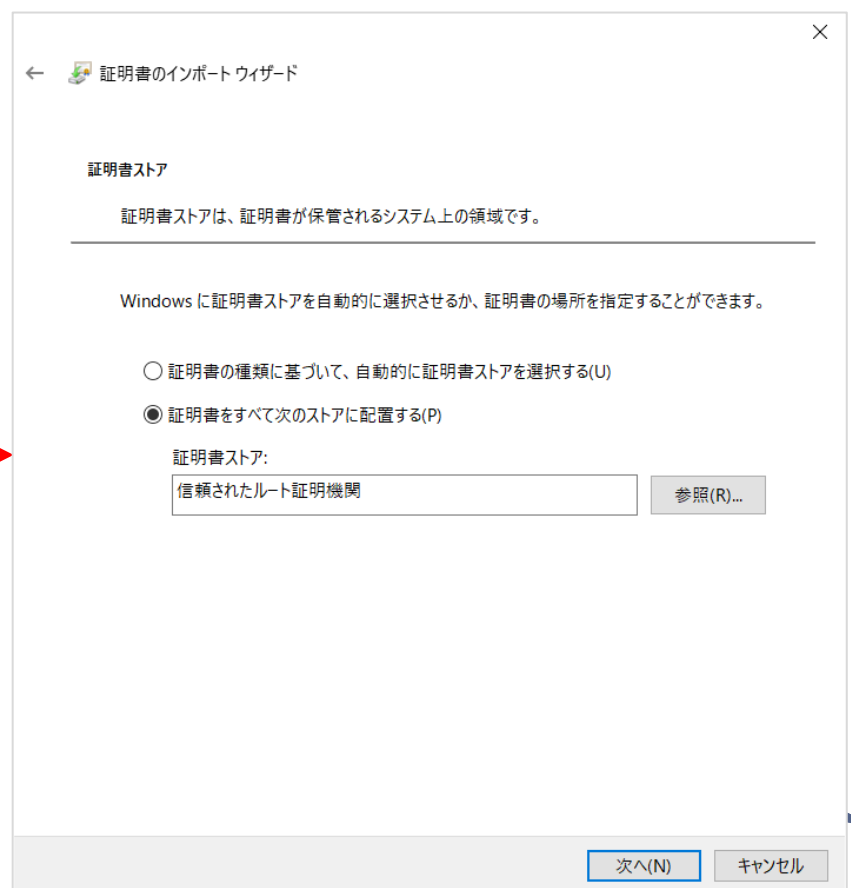
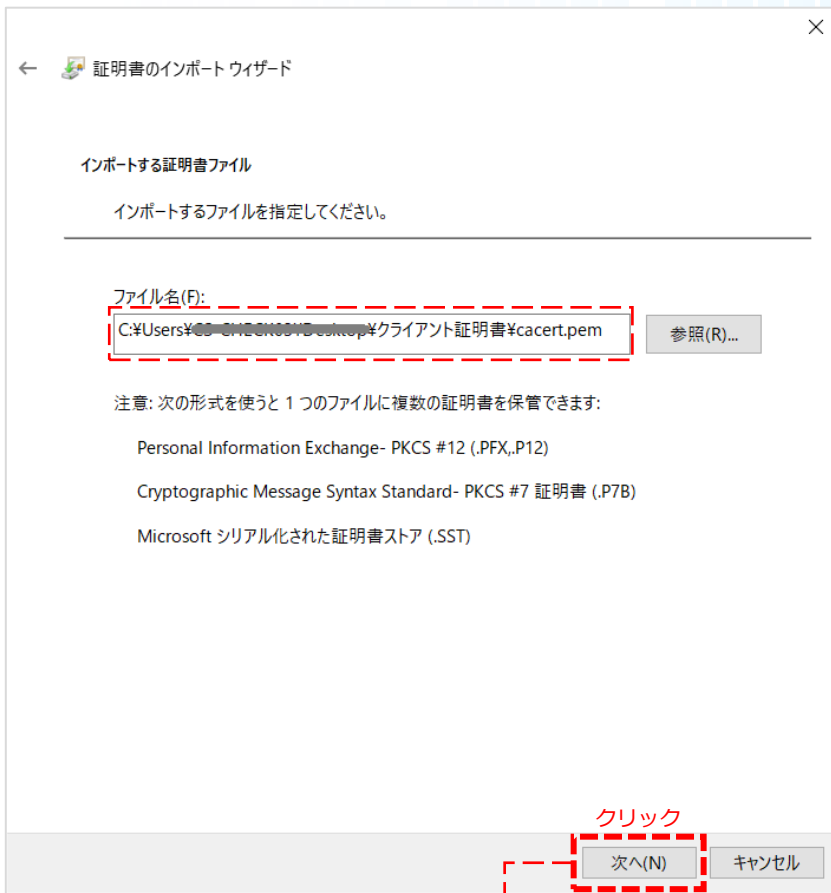
- ⑤ [参照] ボタンをクリックし、インポートするCA証明書（cacert.pem）を選択します。





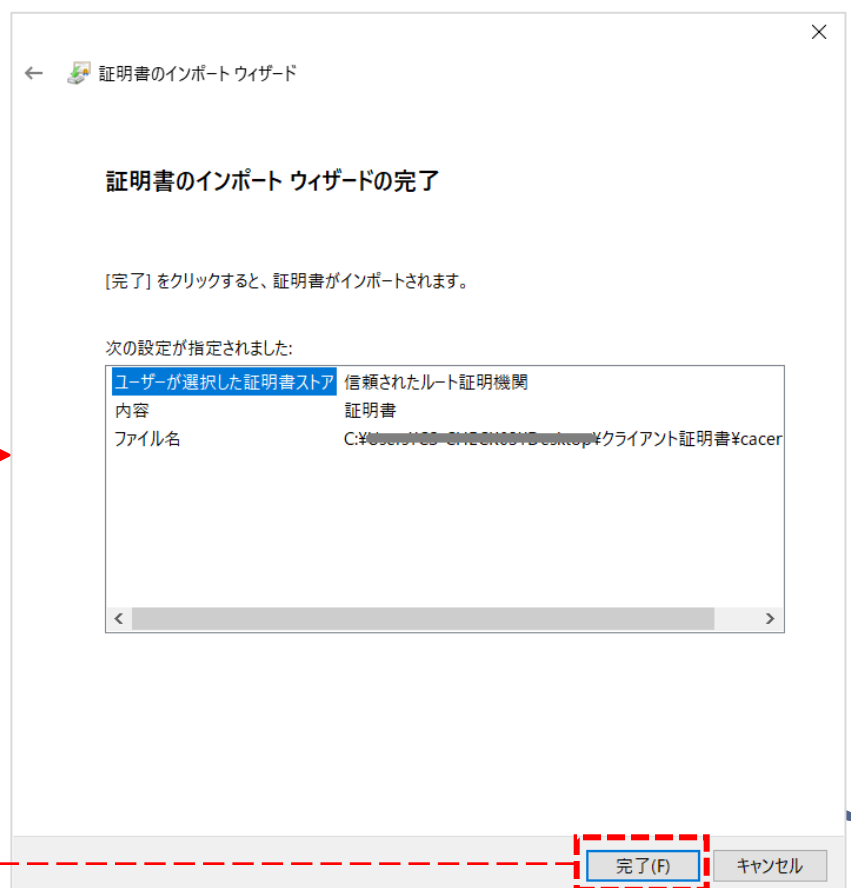
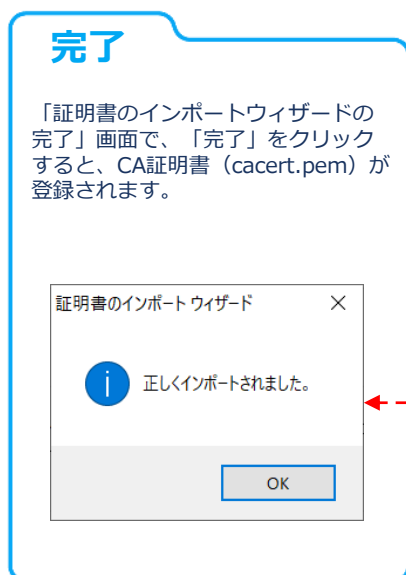
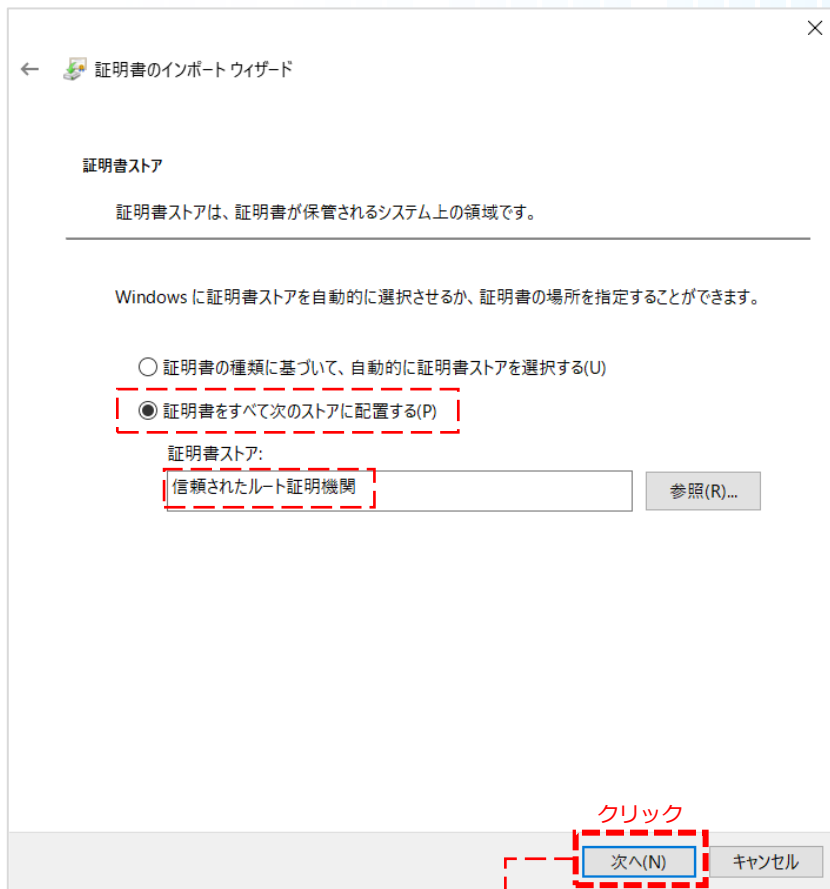
## 02 Microsoft Edgeをご利用の場合

- 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。



## 02 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。

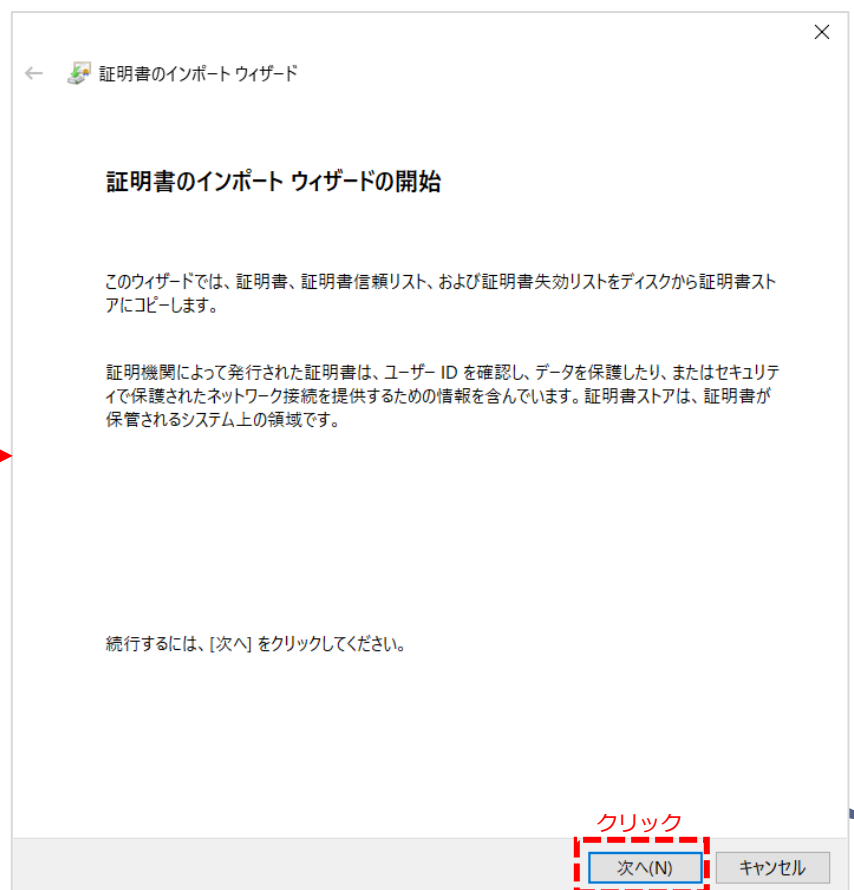
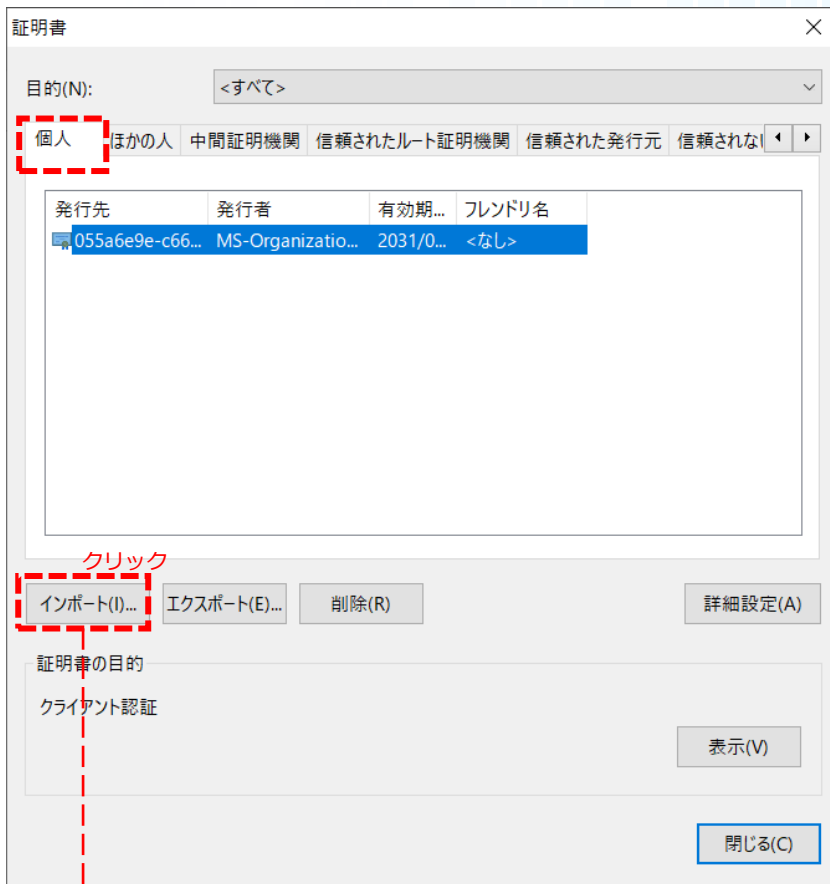
The screenshot shows the Microsoft Edge settings page at `edge://settings/privacy`. The left sidebar shows the '設定' (Settings) menu with 'プライバシー、検索、サービス' (Privacy, Search, Services) selected. The main content area shows the 'セキュリティ' (Security) section, where '証明書の管理' (Certificate Management) is highlighted with a red dashed box and labeled 'クリック' (Click). A vertical red dashed arrow on the right indicates scrolling down to this section. Below the main settings, a '証明書' (Certificate) dialog box is open, showing a table of certificates:

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

The dialog box also includes 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)'.

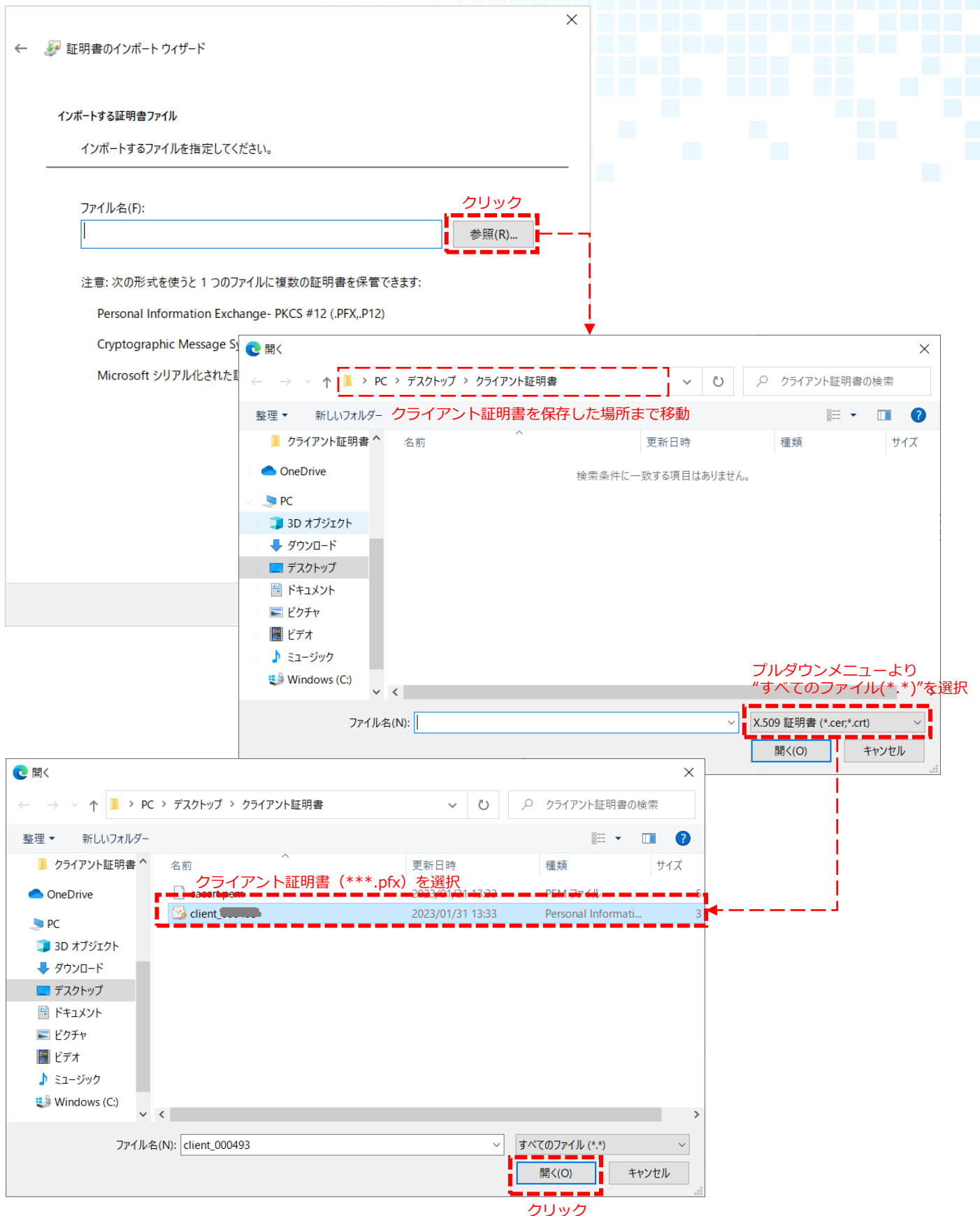
## 02 Microsoft Edgeをご利用の場合

- 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。



## 02 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。



## 02 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\%CS-0140103ND...%\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 Microsoft Edgeをご利用の場合

- ⑤ 案内メールに記載されている「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

「件名：【重要】desknet's クラウドクライアント認証オプション証明書のご送付」内の【ステップ2】に記載されているパスワードを入力ください。

← 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)

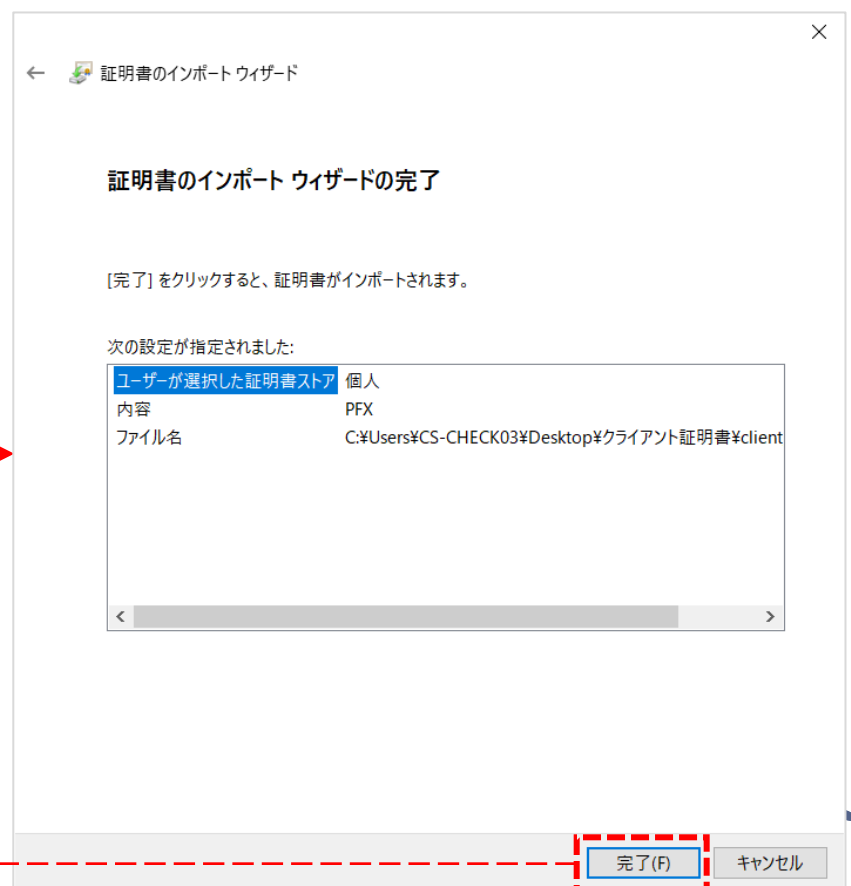
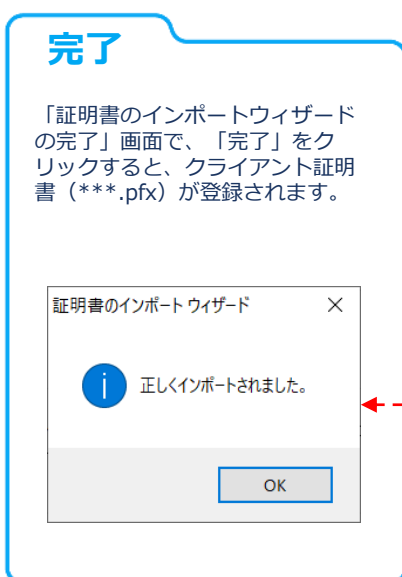
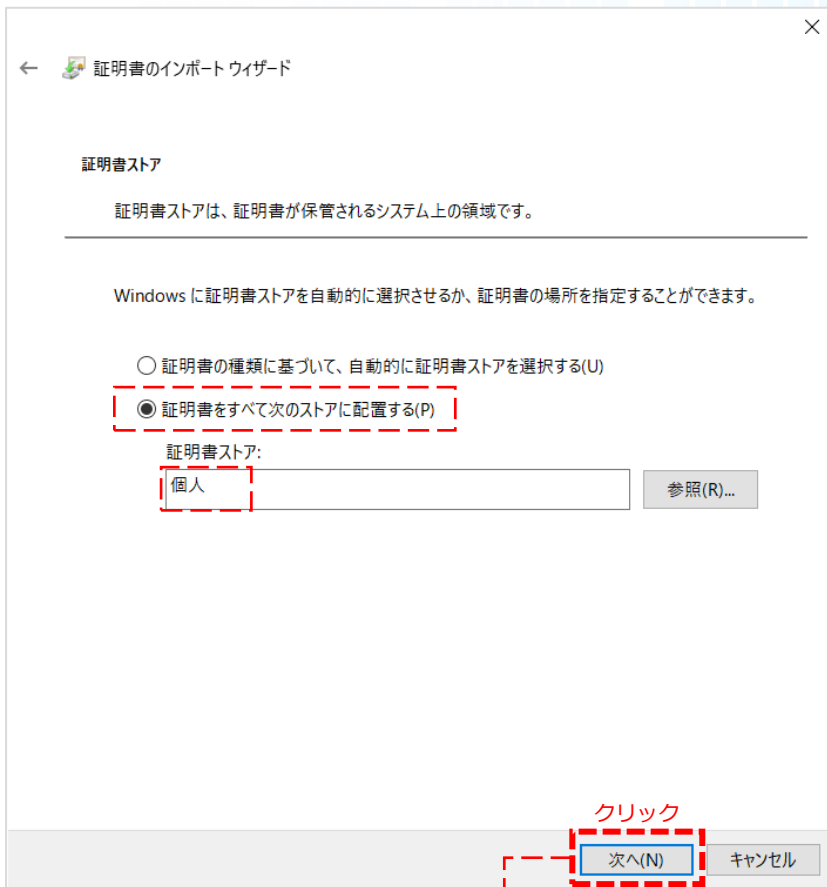
証明書ストア:

個人 参照(R)...

次へ(N) キャンセル

## 02 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。





## 03

## 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。

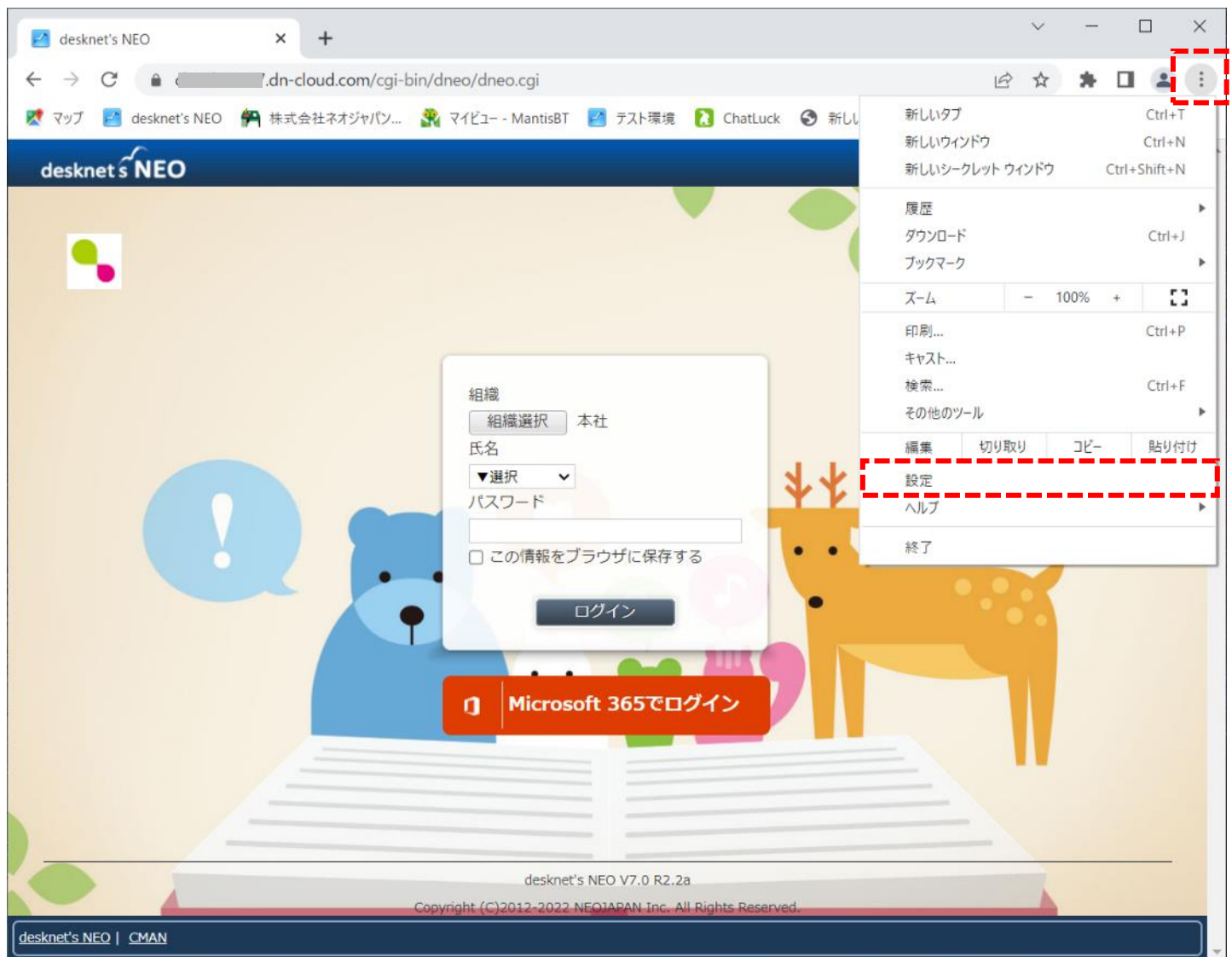
## 1. クライアント証明書発行サイト用のファイルの準備

案内メールに添付されている圧縮ファイルをダウンロードし、管理用端末に解凍してください。解凍すると、下記ファイルが表示されます。

- CA証明書ファイル (cacert.pem)
- クライアント証明書ファイル (\*\*\*.pfx)

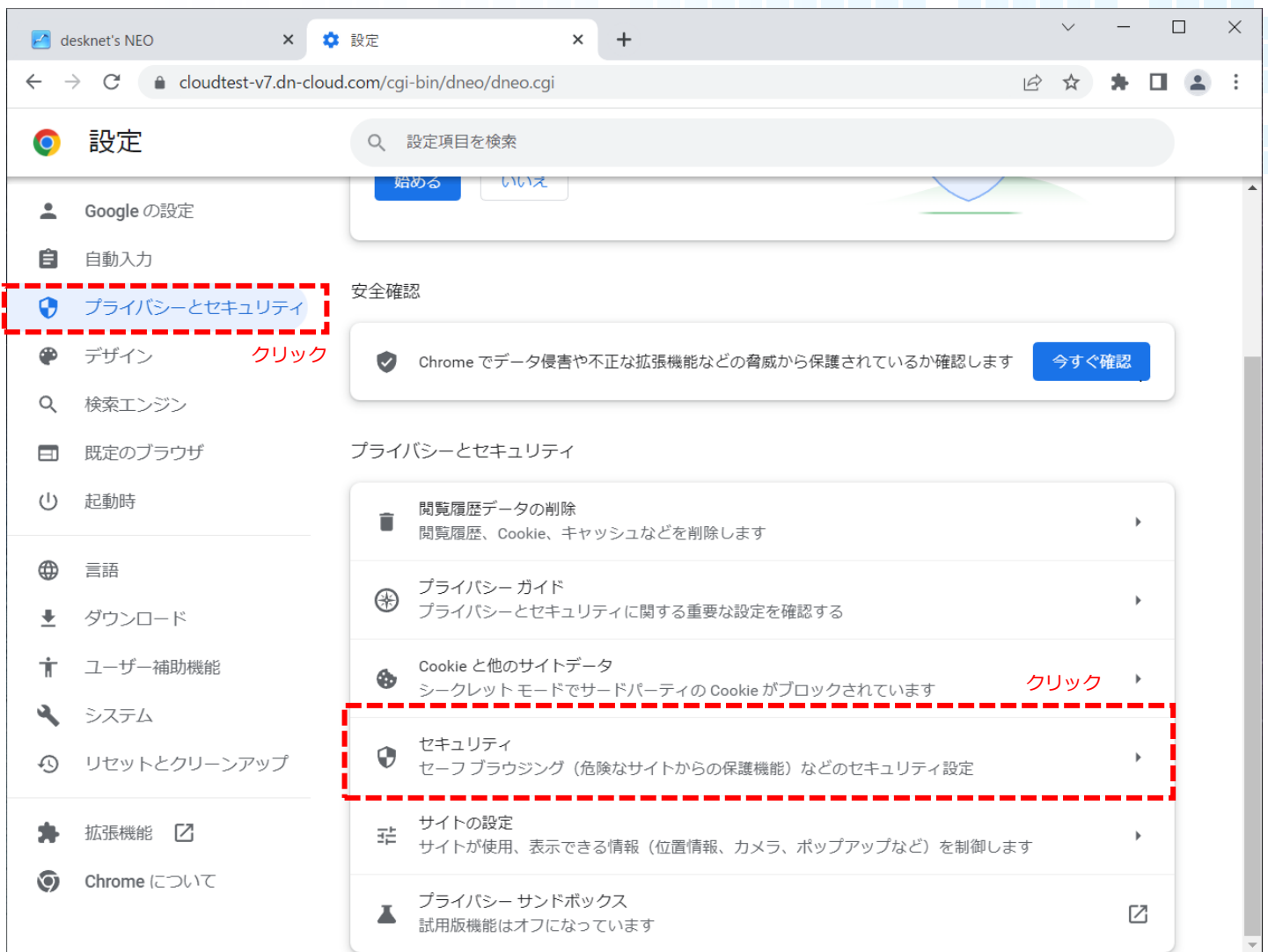
## 2. CA証明書 (cacert.pem) のインストール

- 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。



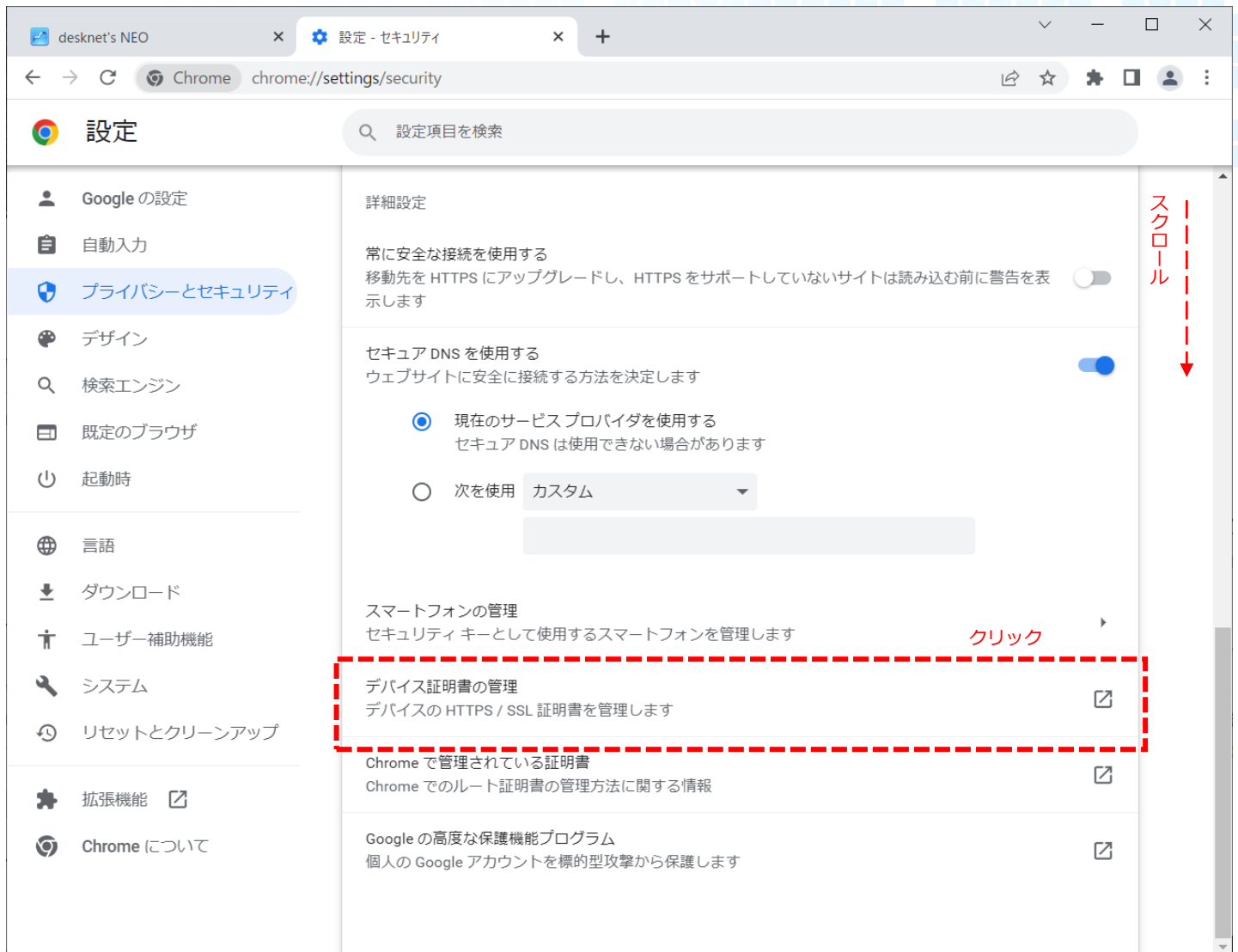
## 03 Google Chromeをご利用の場合

- 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。



## 03 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 lists 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.

Chrome 設定 chrome://settings/security

設定 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

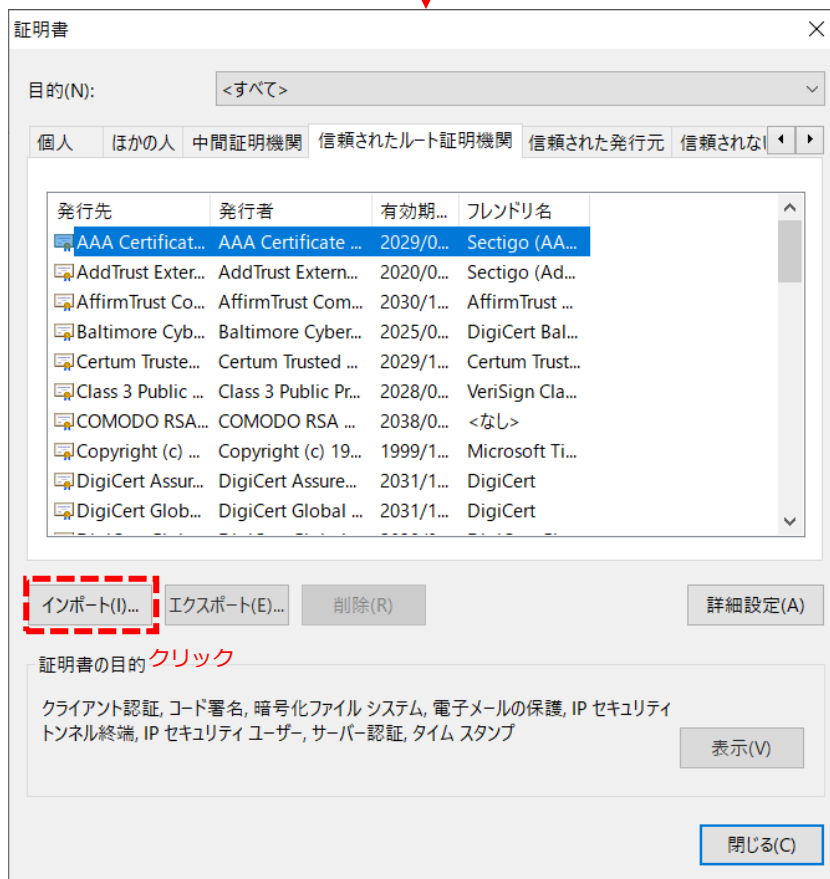
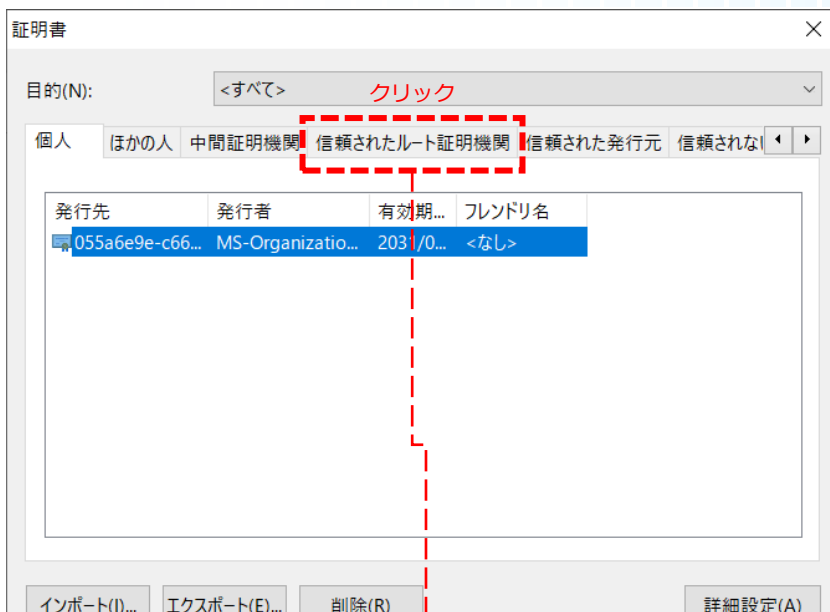
Chrome で管理されている証明書  
Chrome でのルート証明書の管理方法に関する情報

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

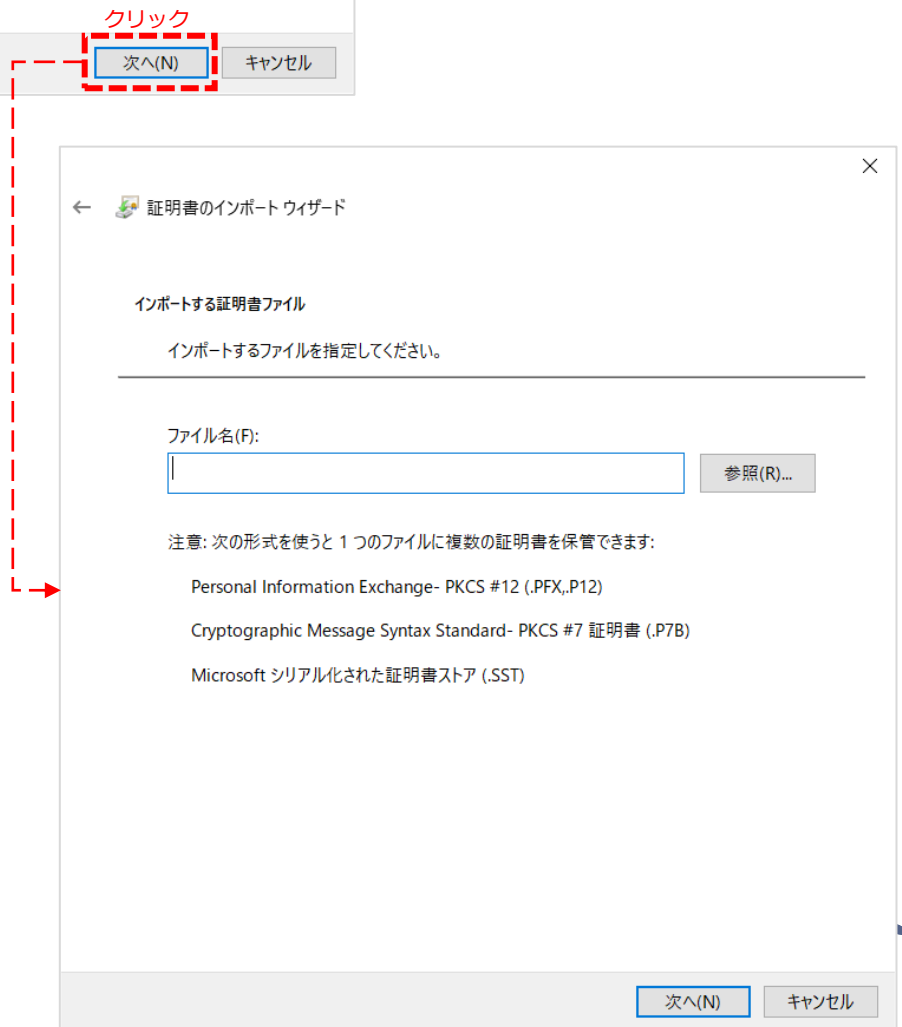
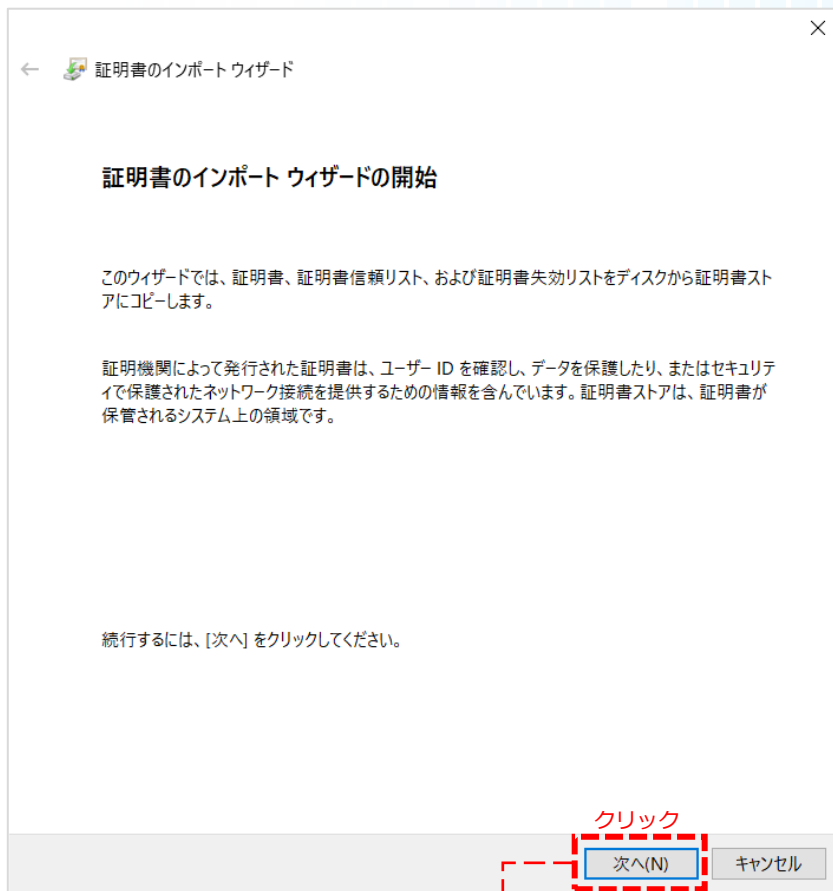
## 03 Google Chromeをご利用の場合

- 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。



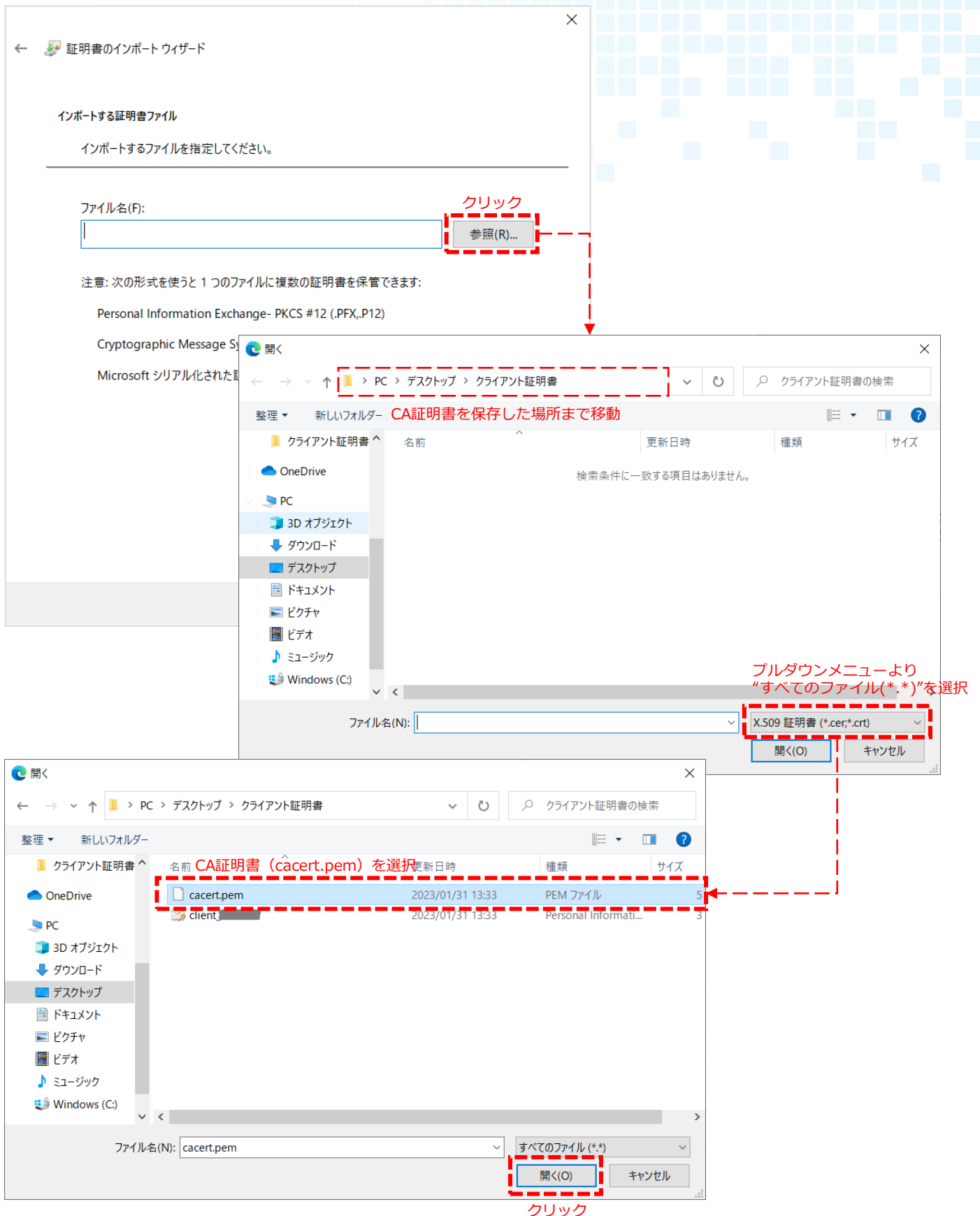
## 03 Google Chromeをご利用の場合

- 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。



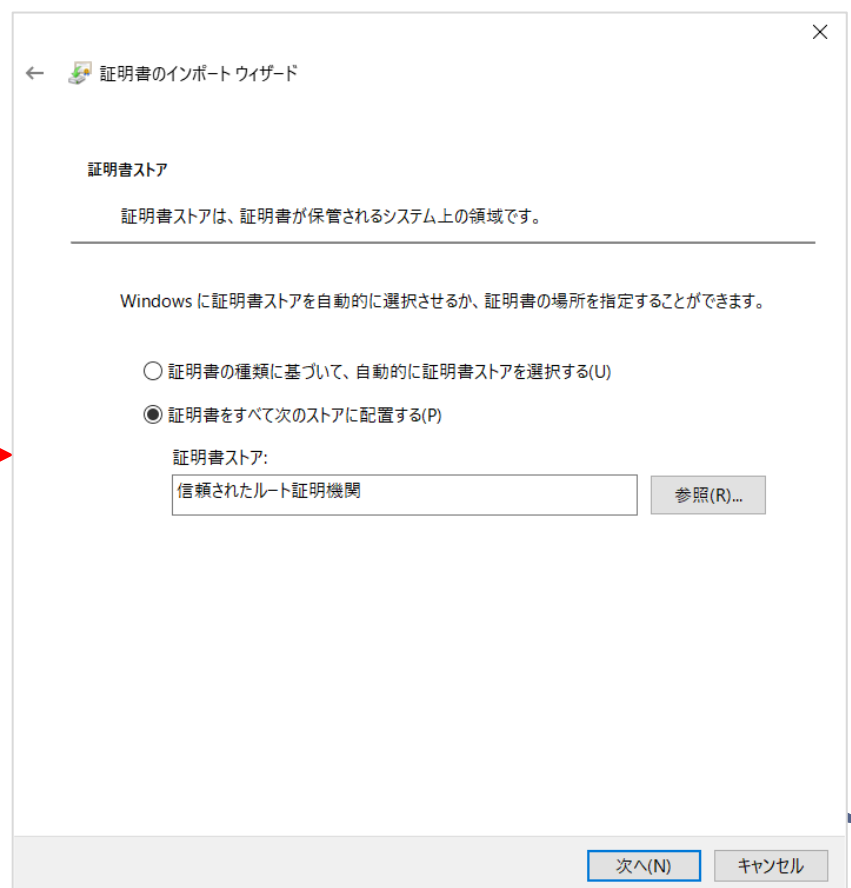
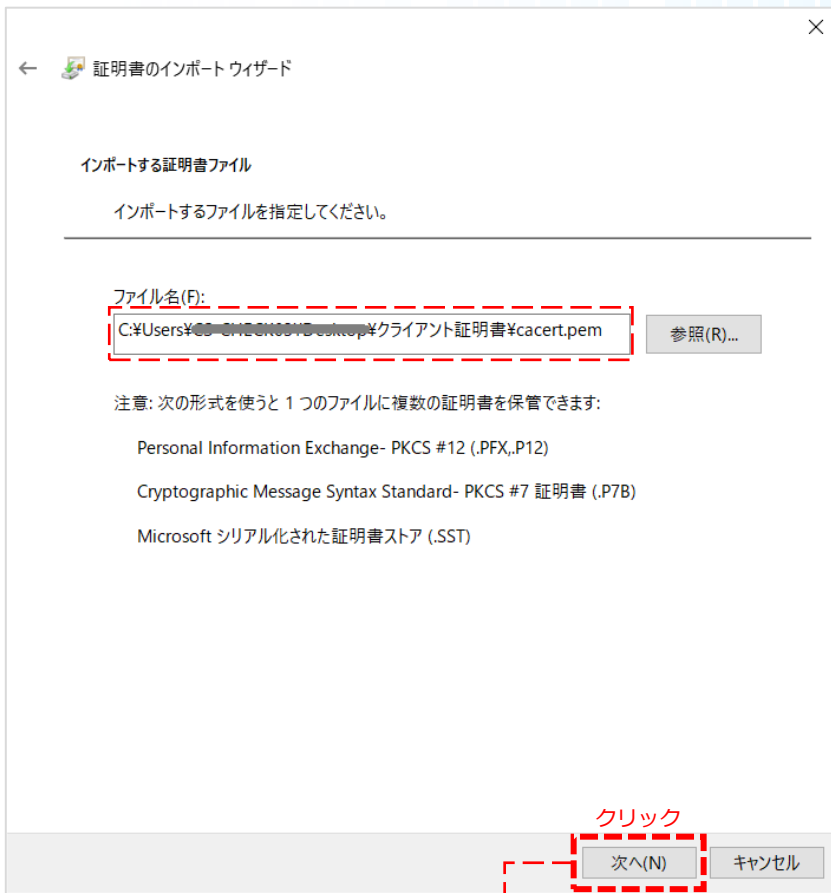
## 03 Google Chromeをご利用の場合

- 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。



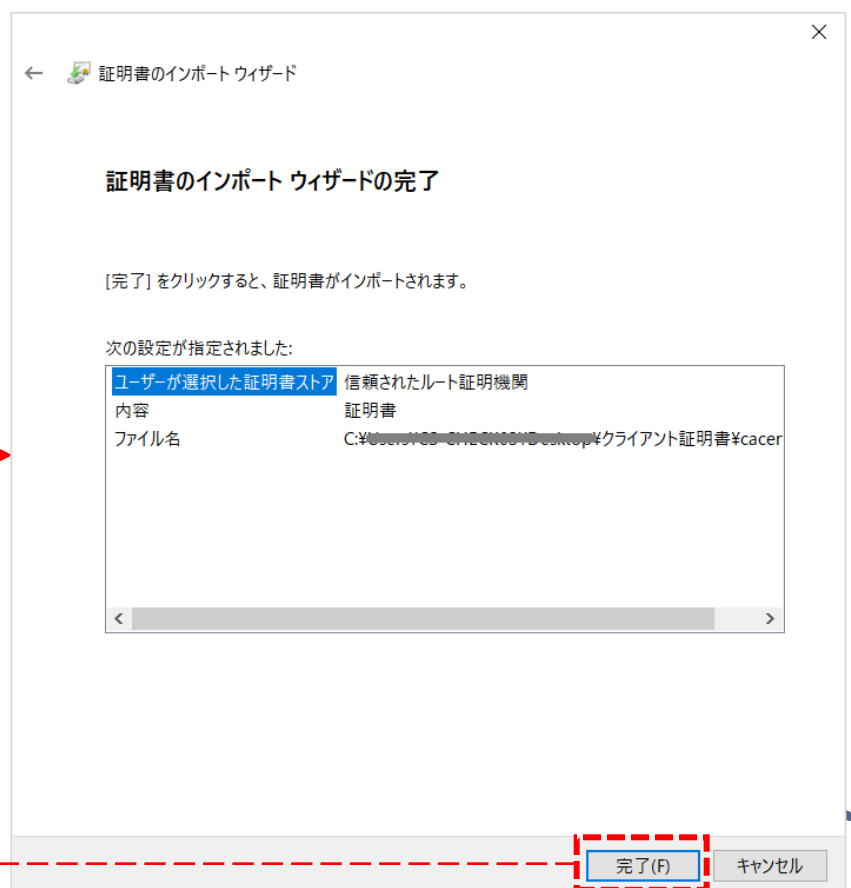
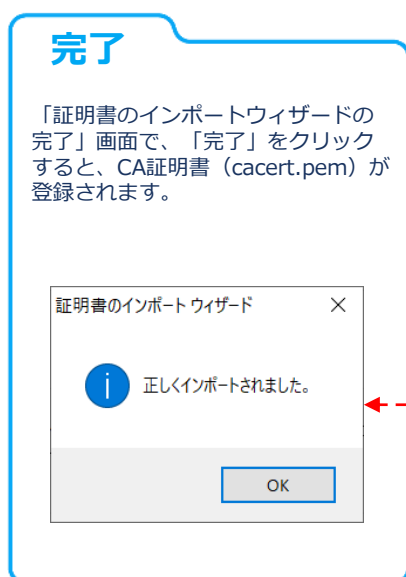
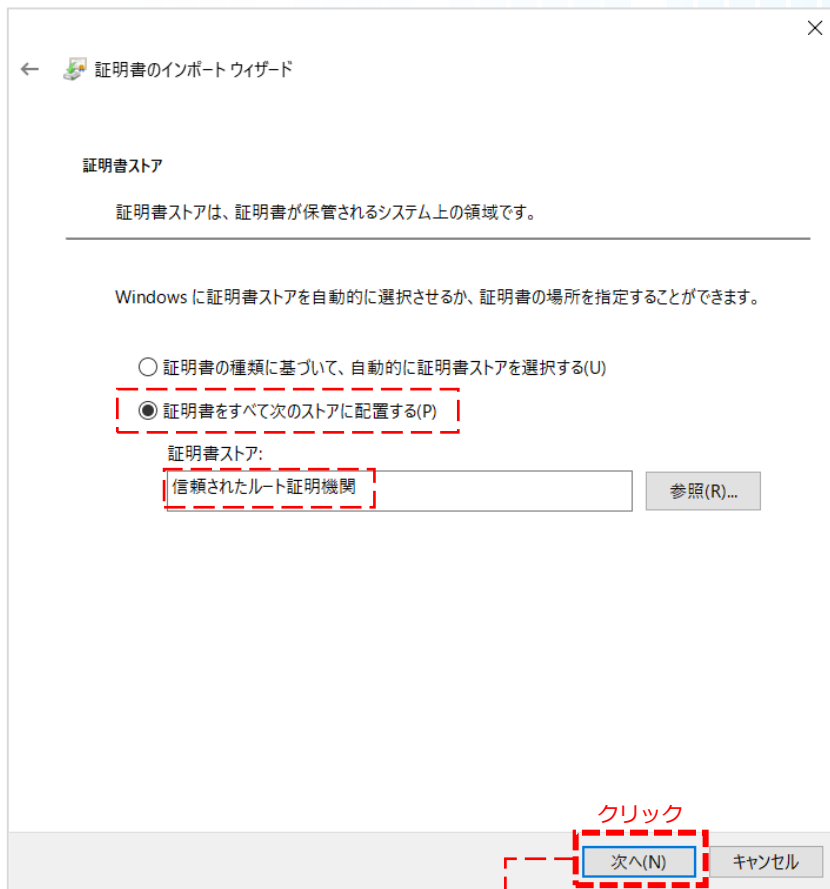
## 03 Google Chromeをご利用の場合

- 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。



## 03 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。

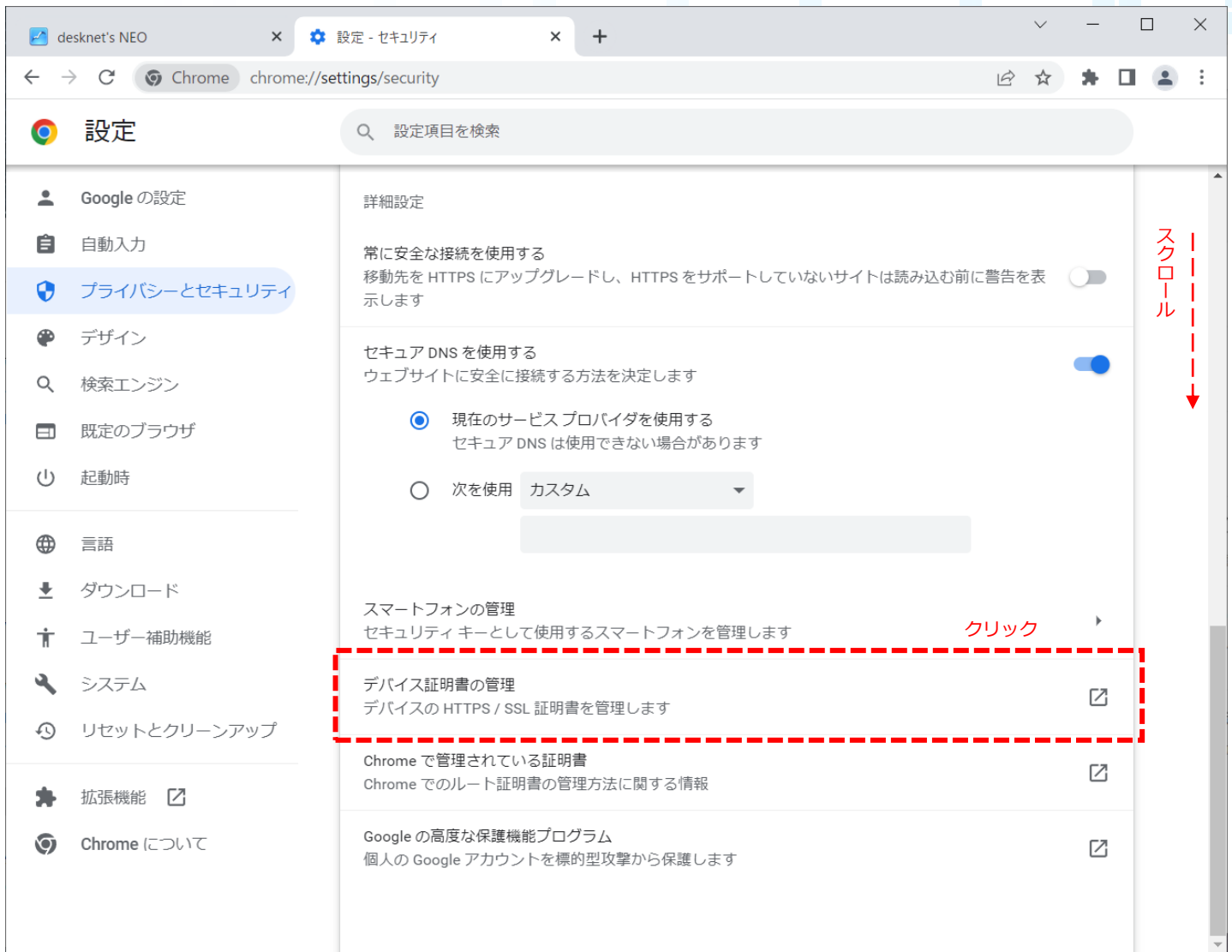




## 03 Google Chromeをご利用の場合

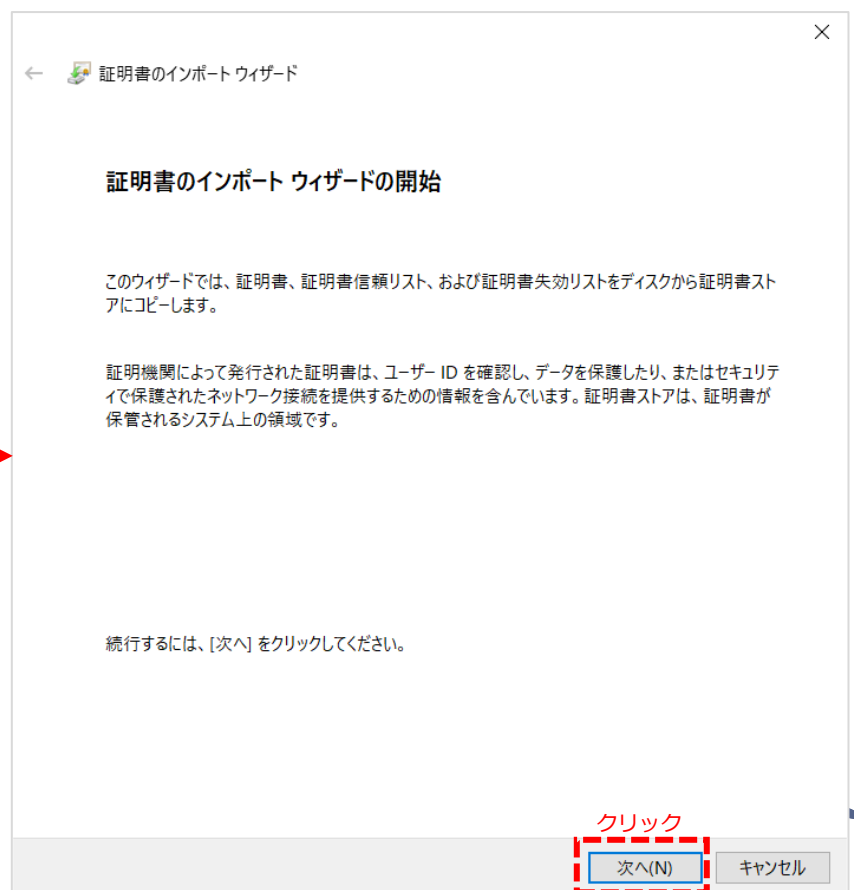
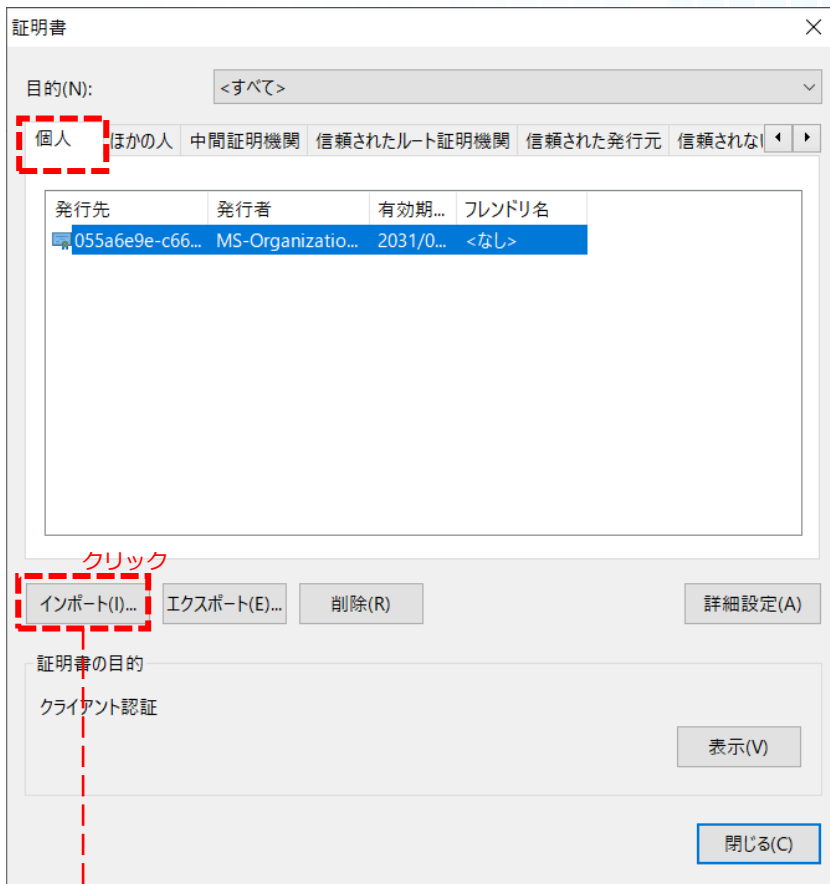
## 3. クライアント証明書ファイル (\*.pfx) のインストール

- 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。



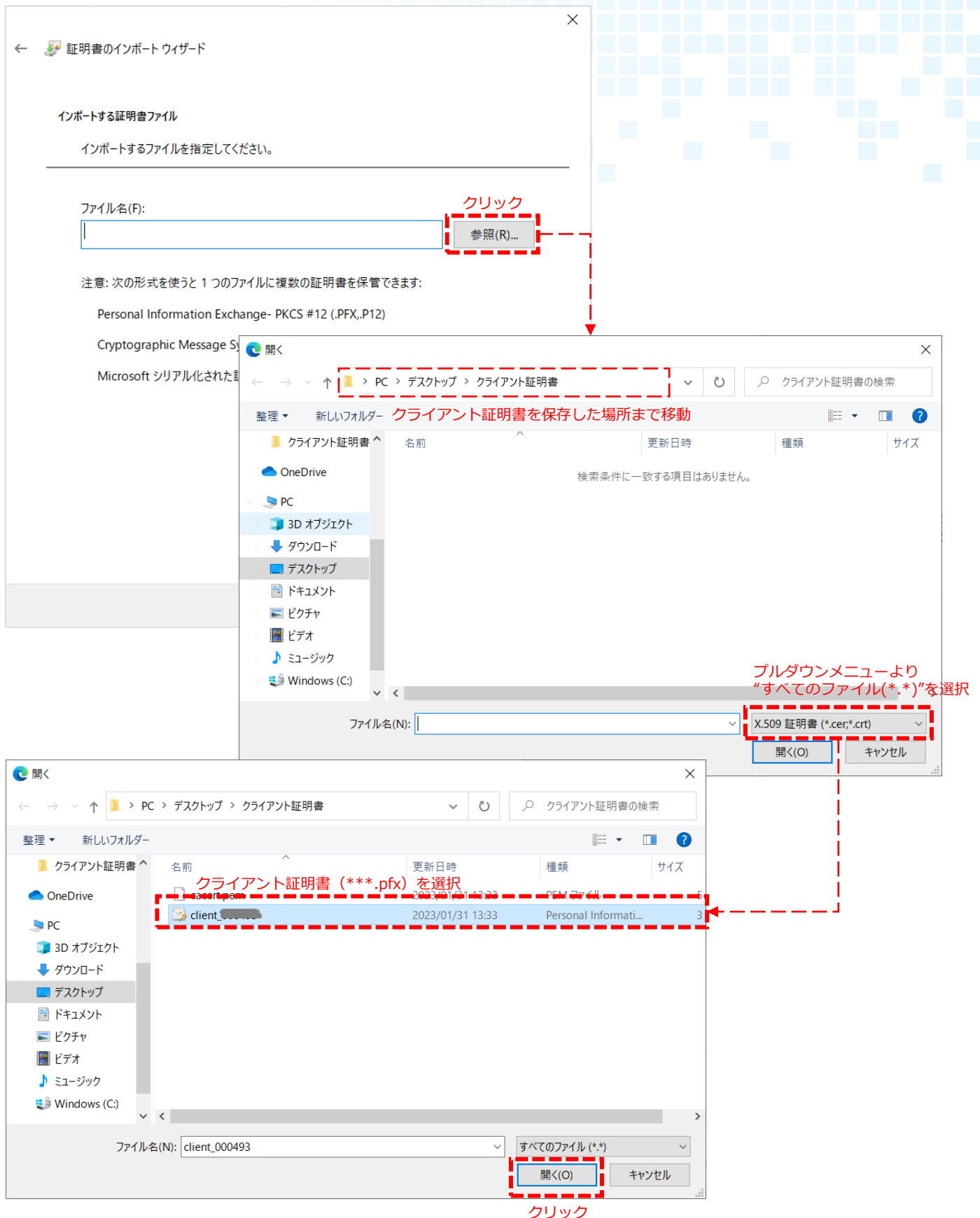
## 03 Google Chromeをご利用の場合

- 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。



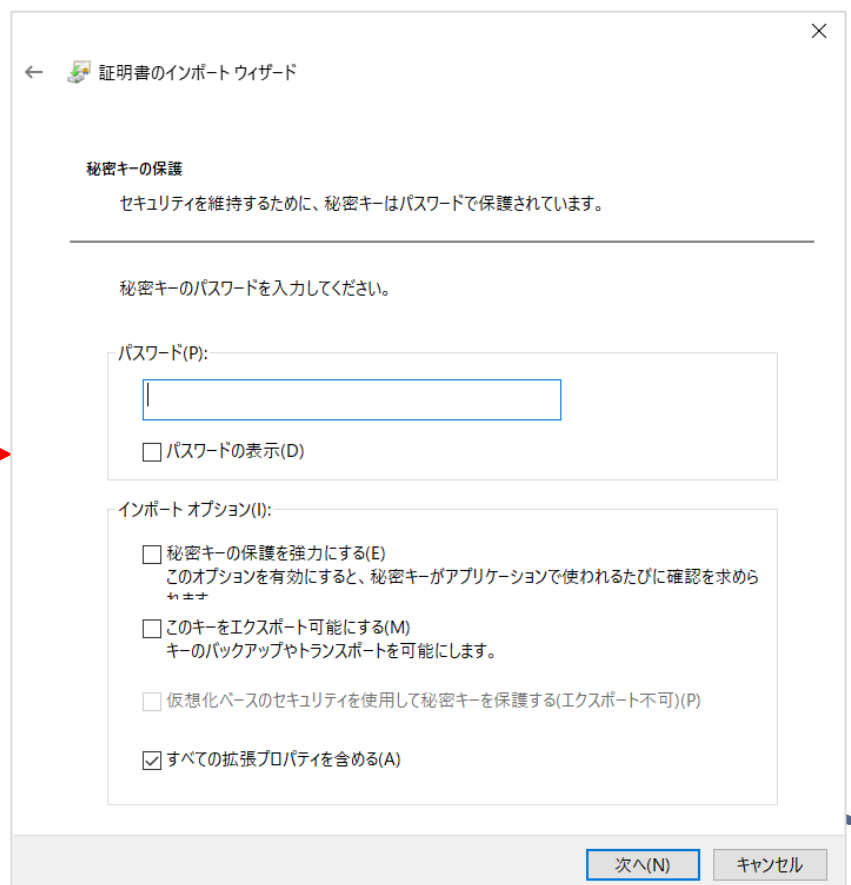
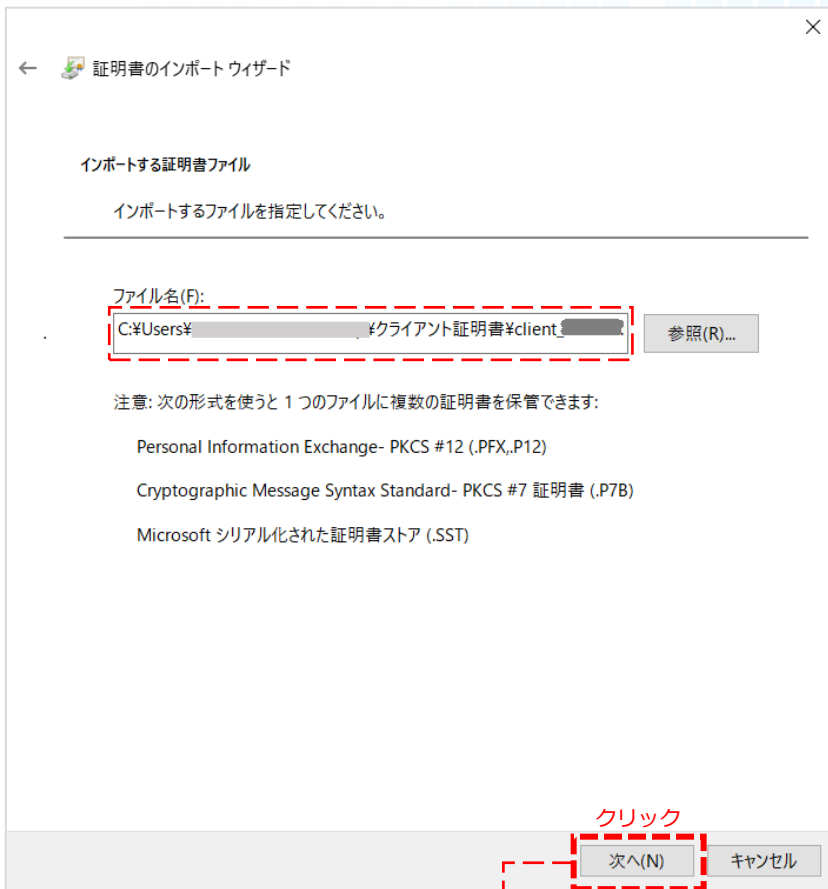
## 03 Google Chromeをご利用の場合

- 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。



## 03 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。



## 03 Google Chromeをご利用の場合

- ⑤ 案内メールに記載されている「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

「件名：【重要】desknet's クラウドクライアント認証オプション証明書のご送付」内の【ステップ2】に記載されているパスワードを入力ください。

← 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)

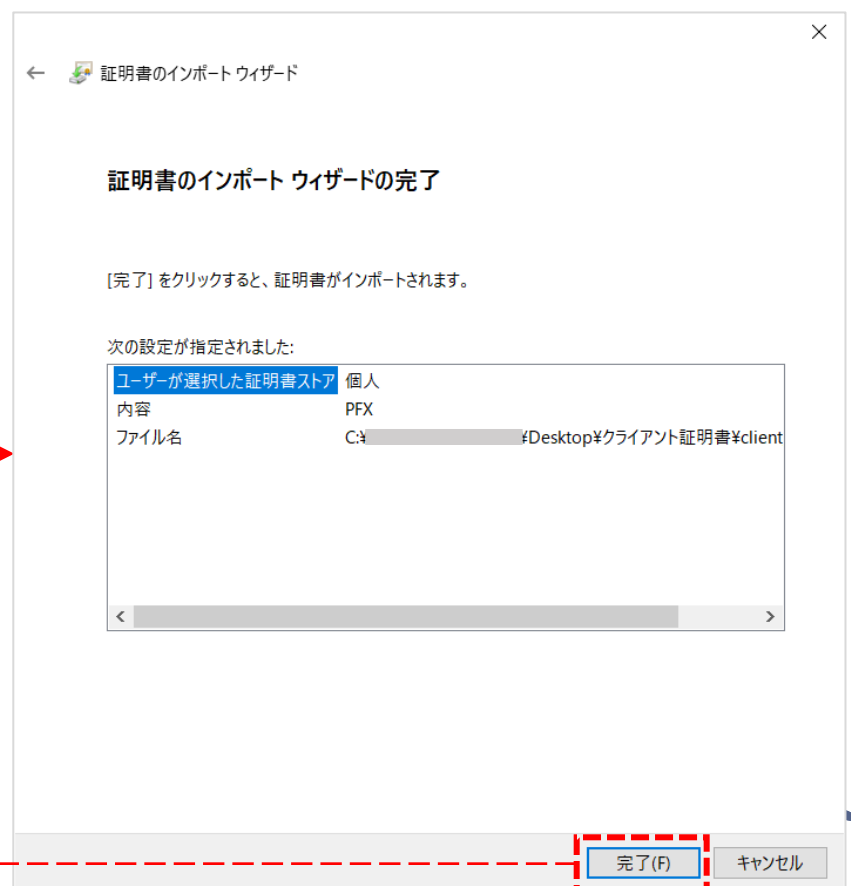
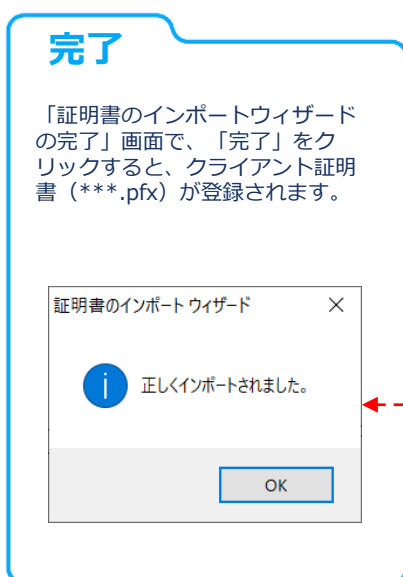
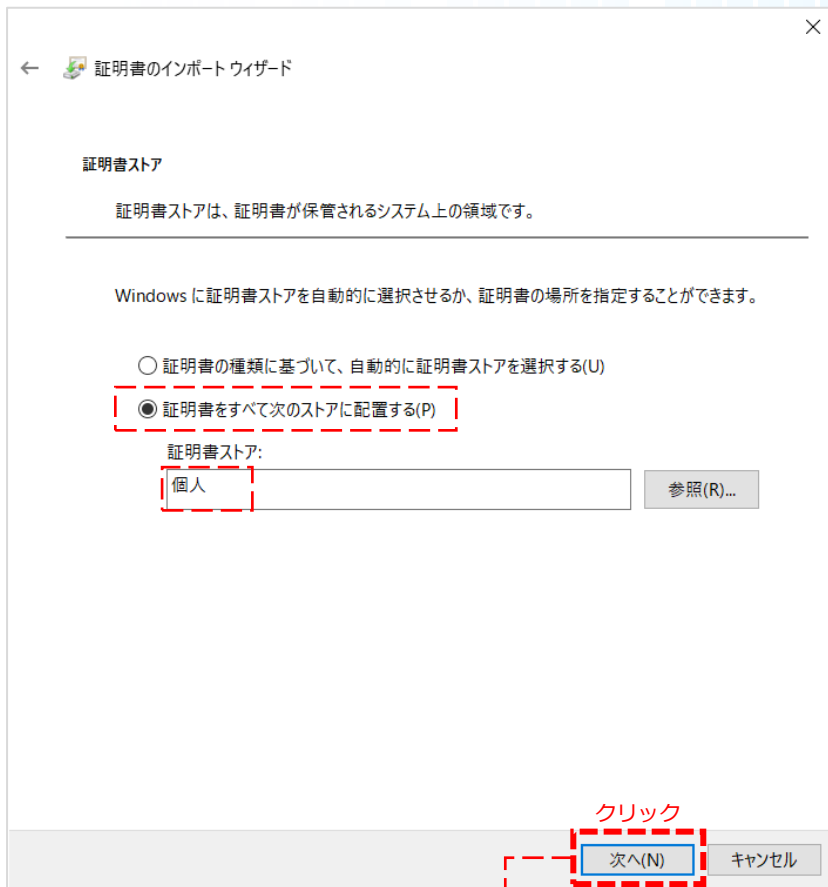
証明書ストア:

個人 参照(R)...

次へ(N) キャンセル

## 03 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。



## 04

## 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。

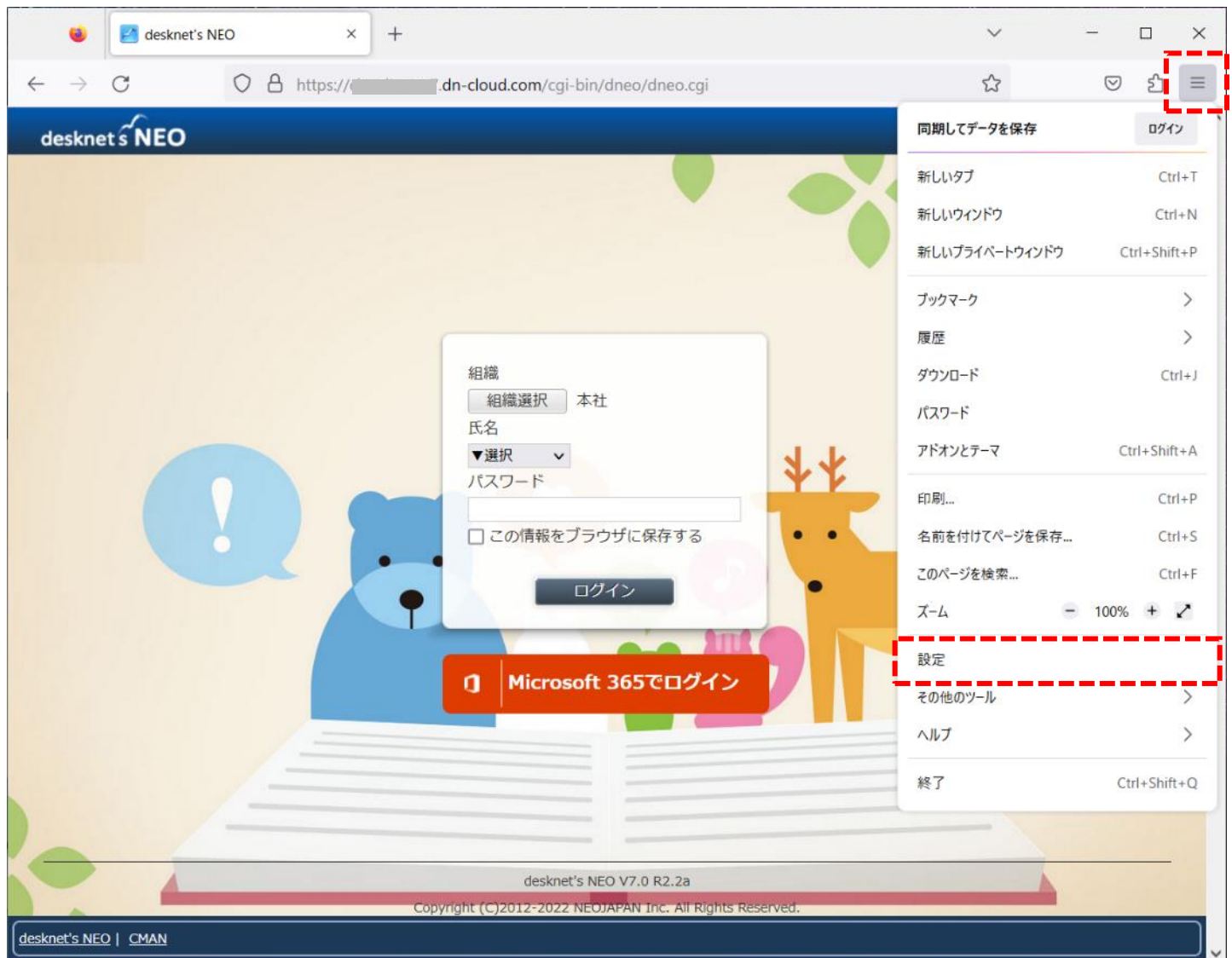
## 1. クライアント証明書発行サイト用のファイルの準備

案内メールに添付されている圧縮ファイルをダウンロードし、管理用端末に解凍してください。解凍すると、下記ファイルが表示されます。

- CA証明書ファイル (cacert.pem)
- クライアント証明書ファイル (\*\*\*.pfx)

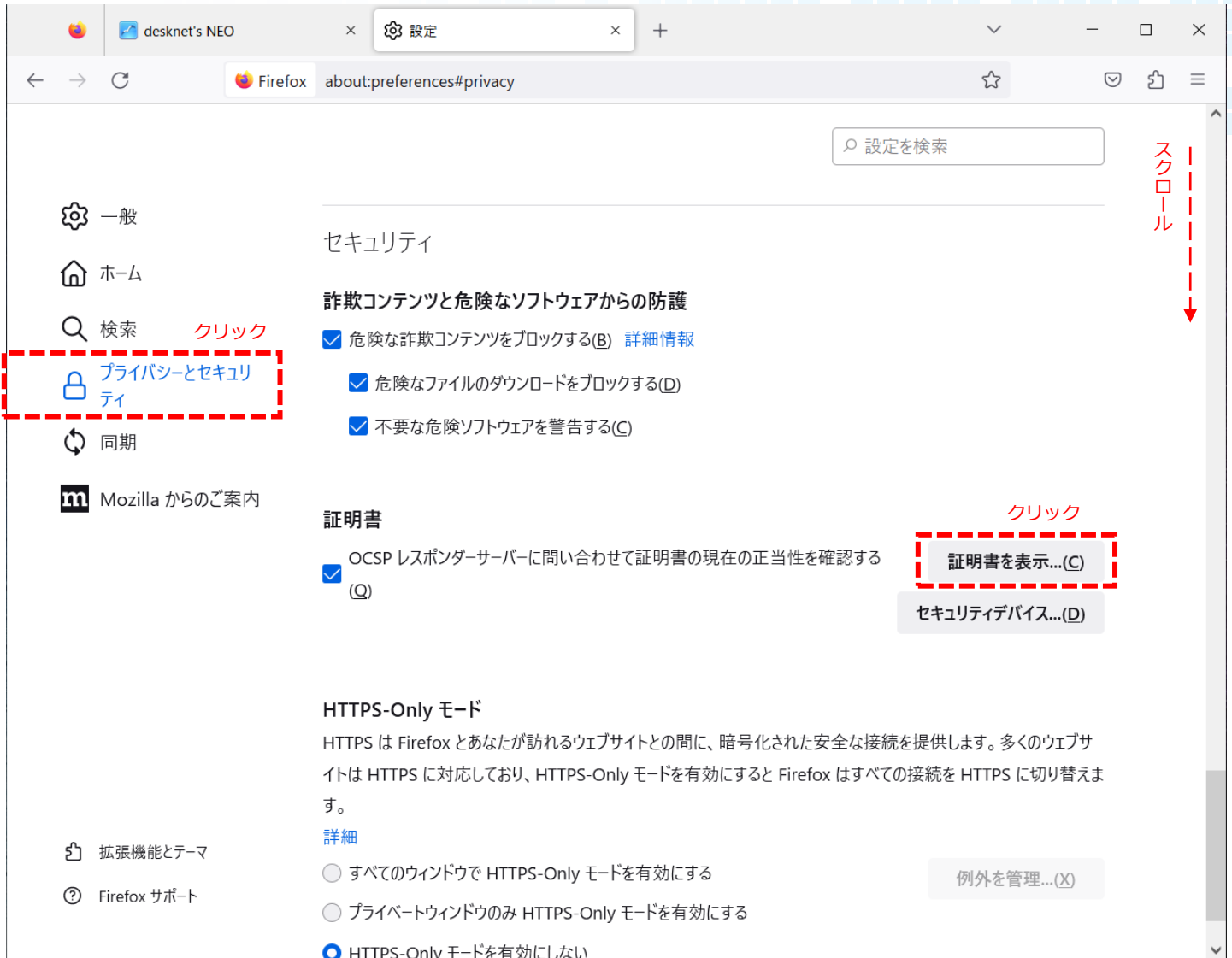
## 2. CA証明書 (cacert.pem) のインストール

- 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。



## 04 Mozilla Firefoxをご利用の場合

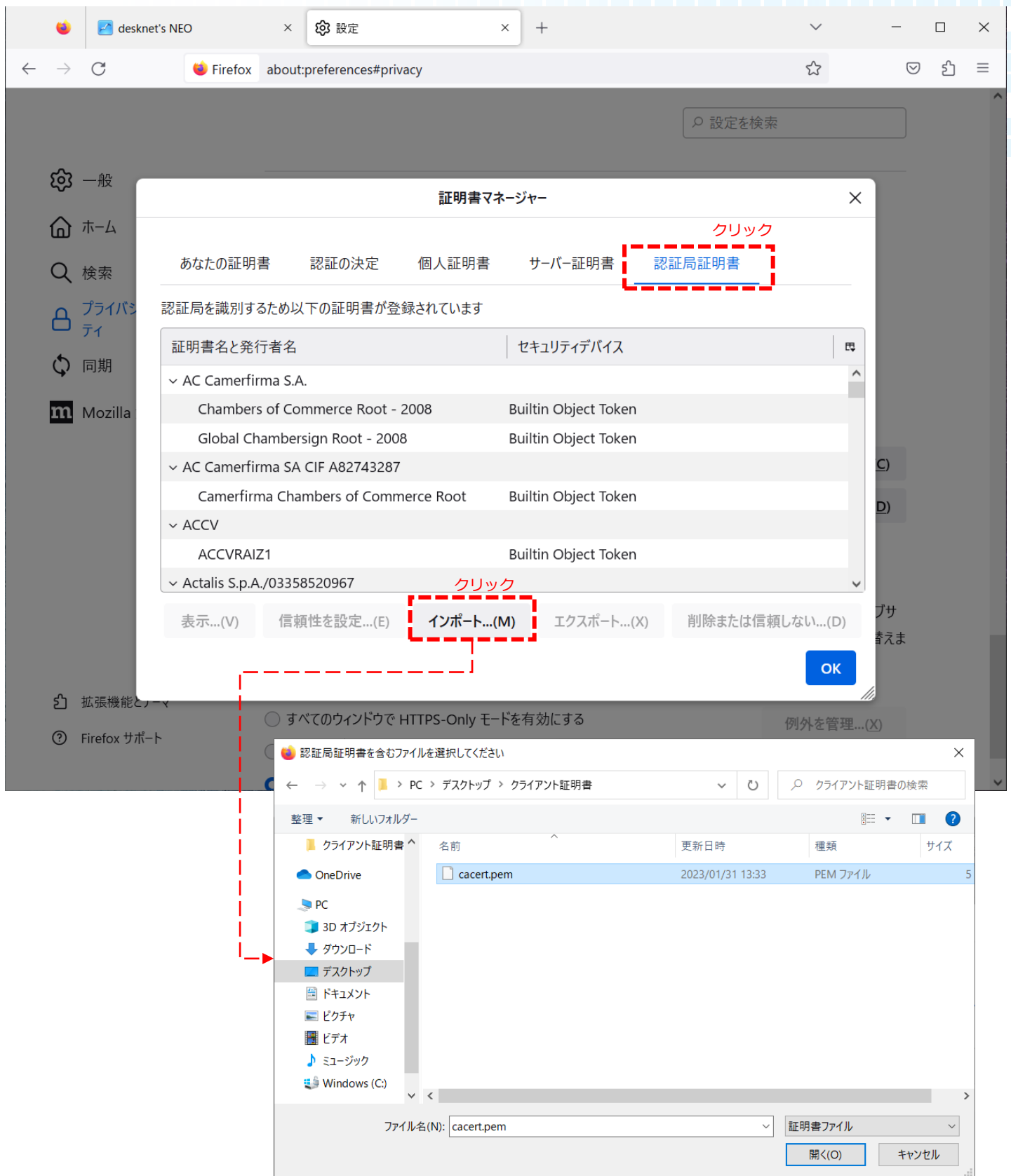
- ② 設定画面のタブが開きますので、メニューより「プライバシーとセキュリティ」を選択。画面を項目「セキュリティ」までスクロールし「証明書の表示…」ボタンをクリックしてください。





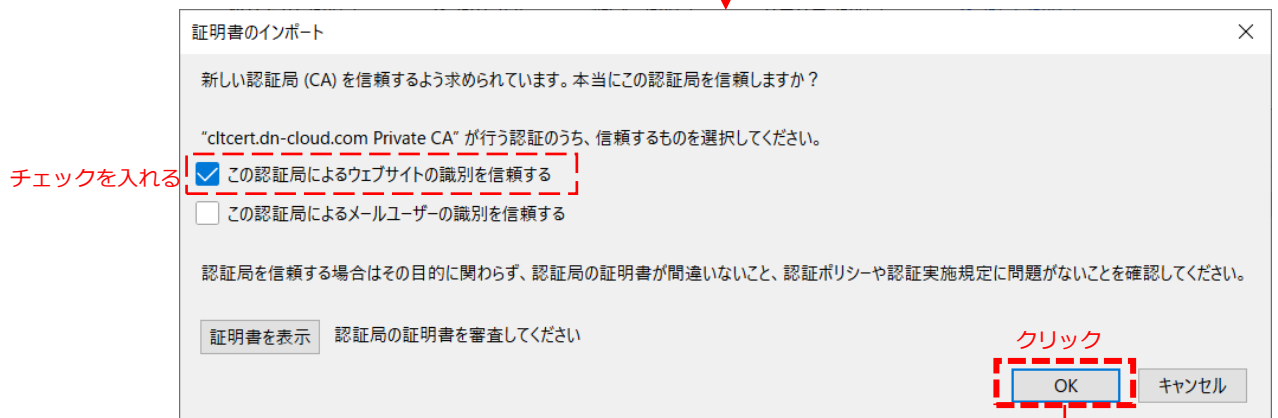
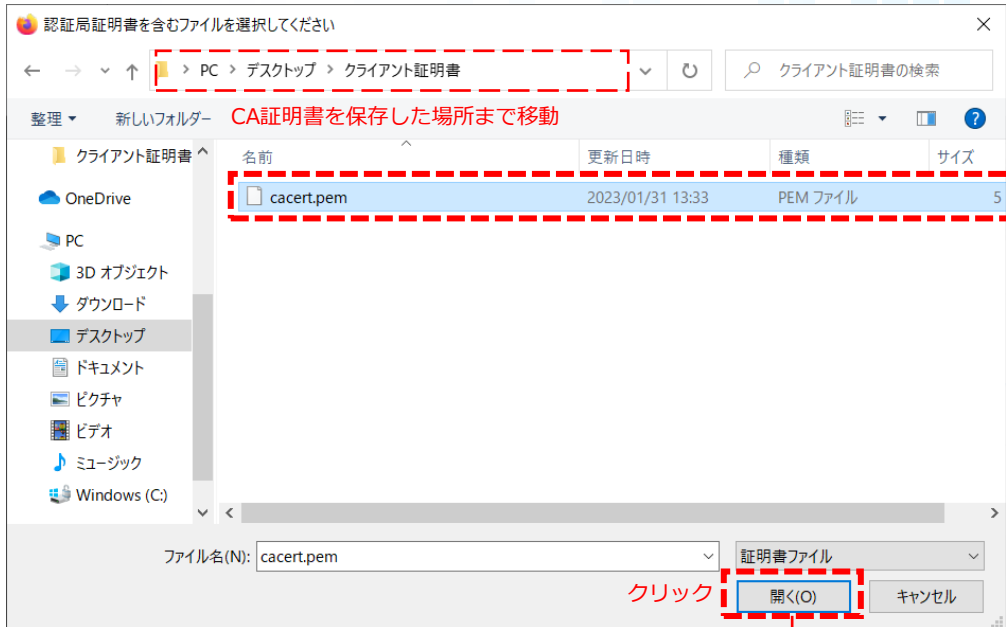
## 04 Mozilla Firefoxをご利用の場合

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。



## 04 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。



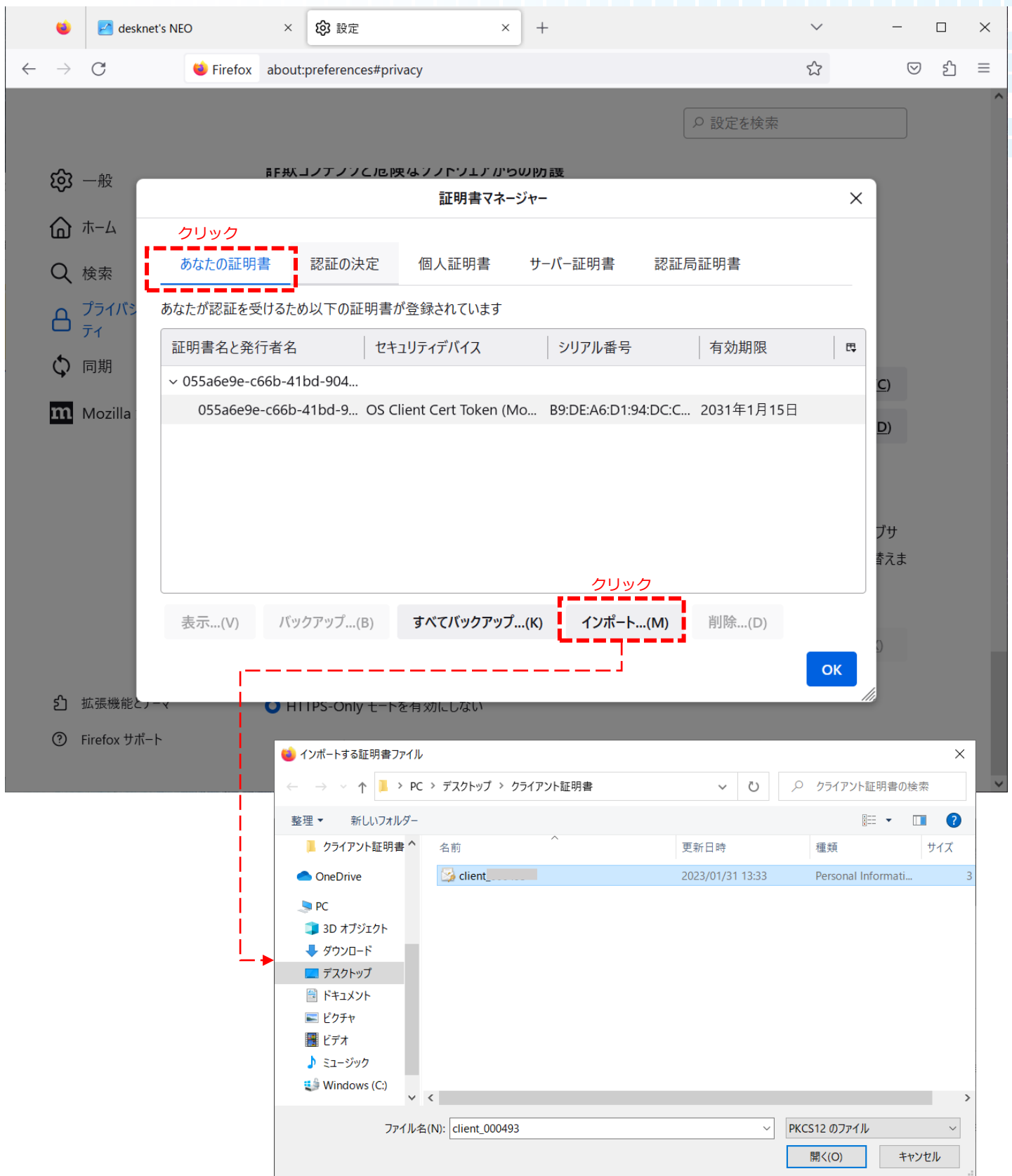
### 3. クライアント証明書ファイル (\*.pfx) のインストール

- 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。



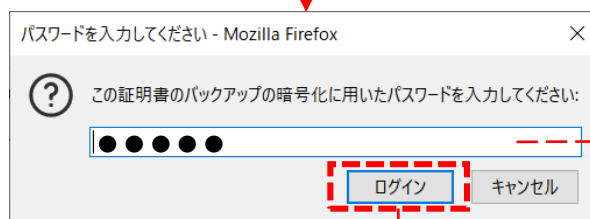
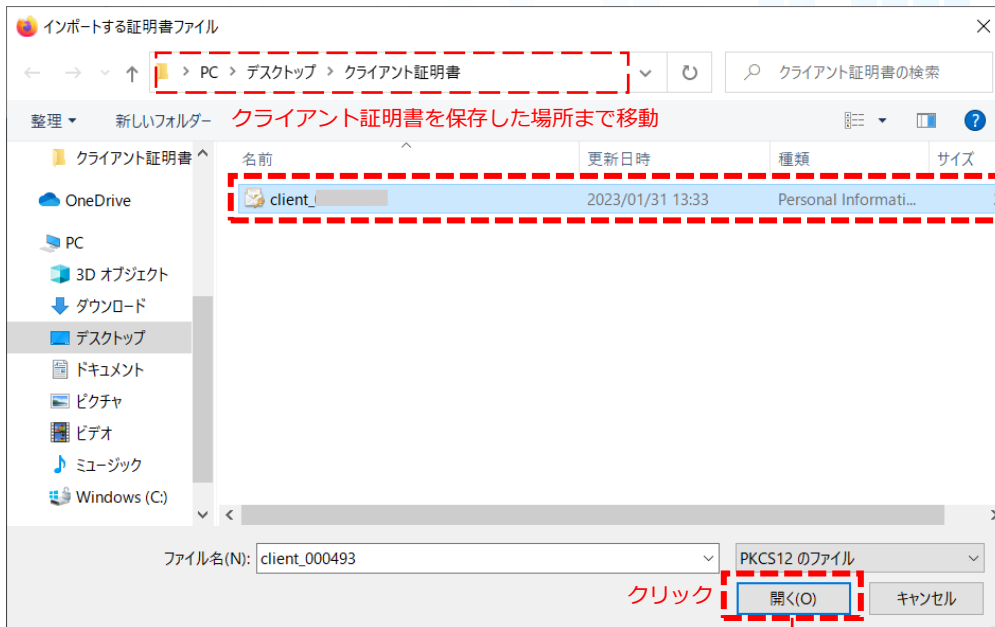
## 04 Mozilla Firefoxをご利用の場合

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。



## 04 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、案内メールに記載されている「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。



「件名：【重要】desknet's クラウドクライアント認証オプション証明書のご送付」内の【ステップ2】に記載されているパスワードを入力ください。

## 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。



### 改版履歴

- 2017年8月29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**

