

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。



Index

01	ご利用まで流れ	3
02	Microsoft Edgeをご利用の場合	4
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
03	Google Chromeをご利用の場合	17
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
04	Mozilla Firefoxをご利用の場合	31
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。

02

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。

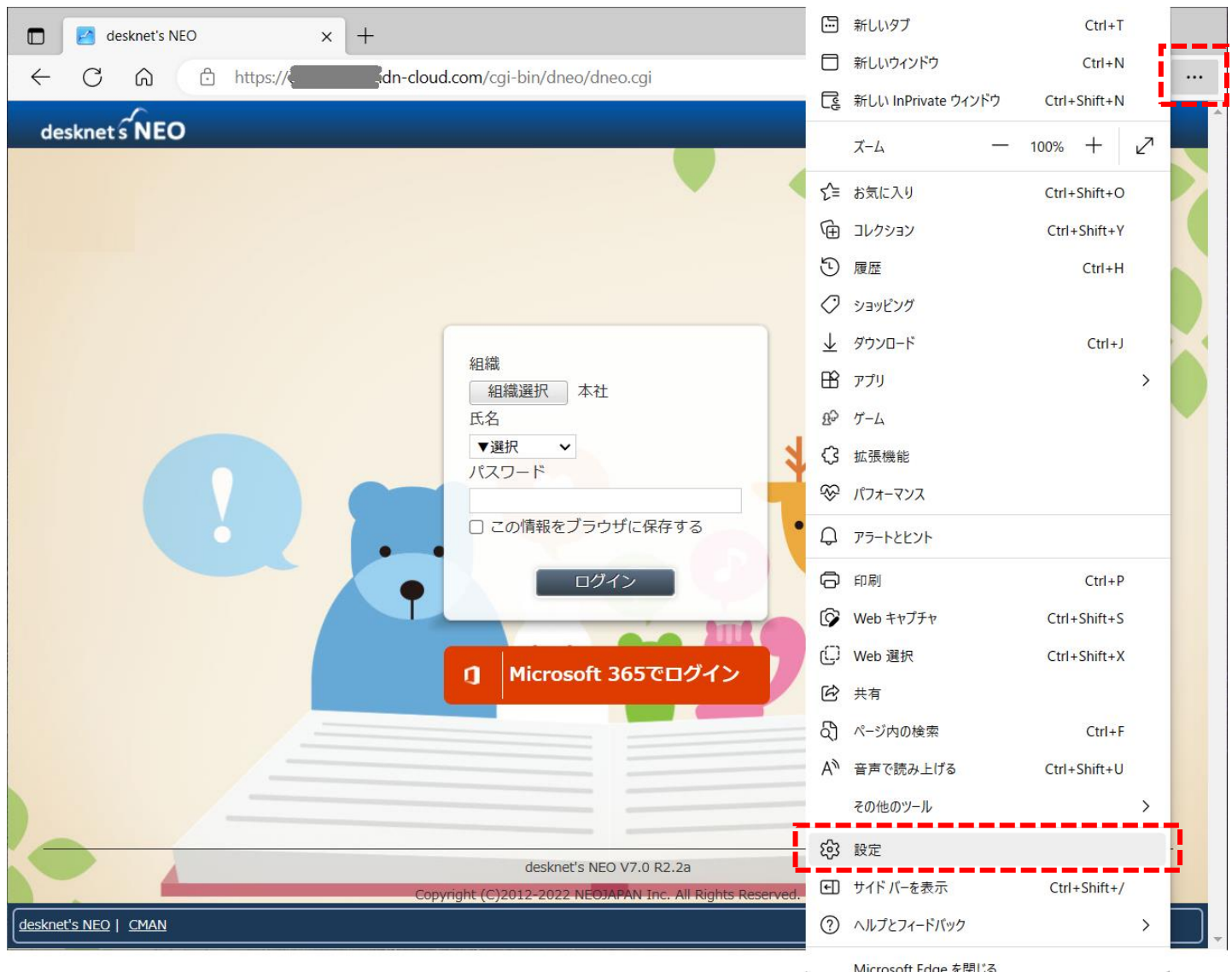
1. クライアント証明書発行サイト用のファイルの準備

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。



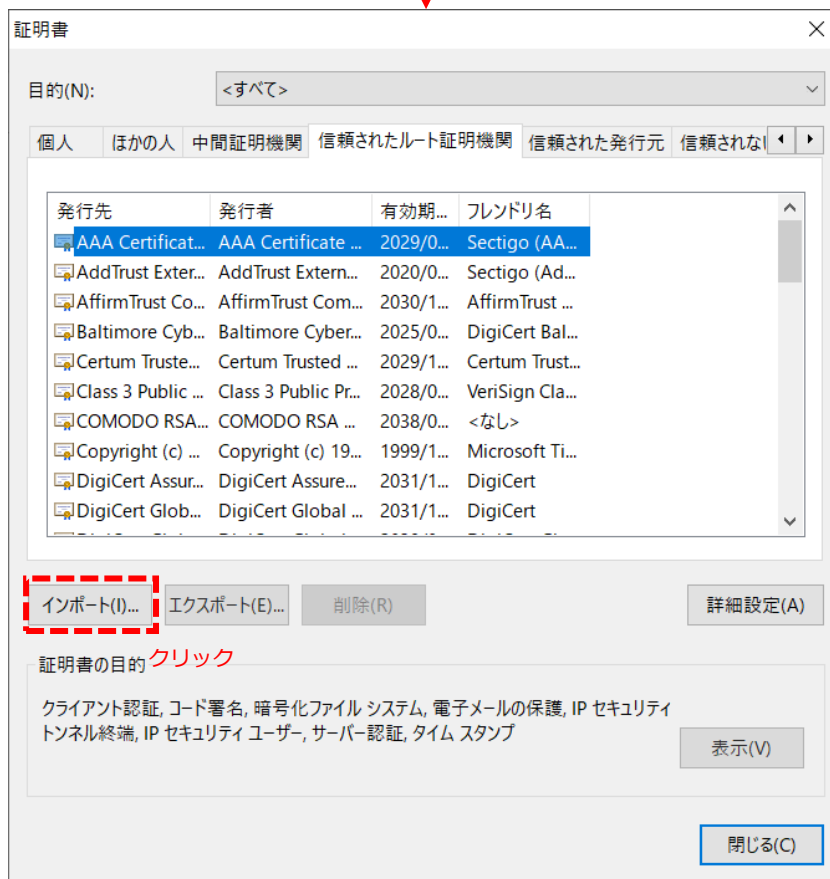
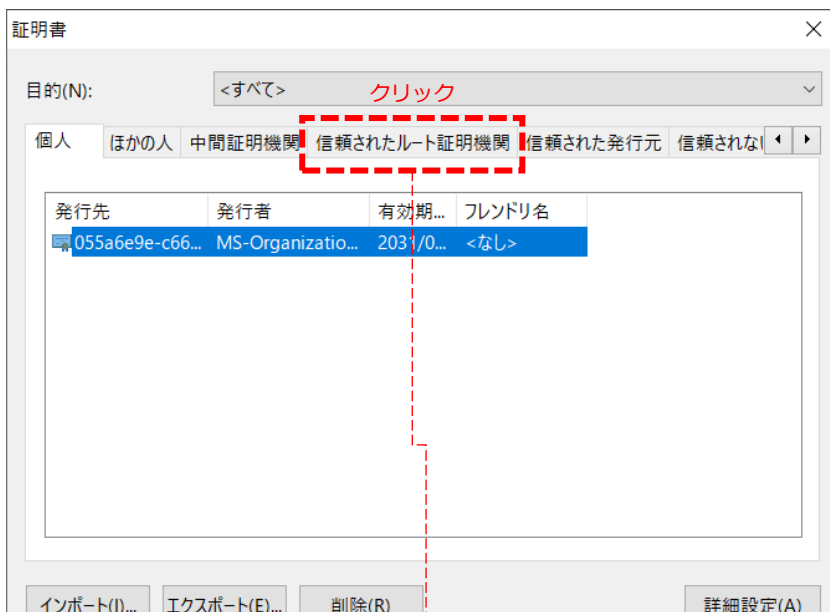
02 Microsoft Edgeをご利用の場合

- 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 interface. On the left, the '設定' (Settings) sidebar is visible, with 'プライバシー、検索、サービス' (Privacy, Search, Services) selected. A red dashed box highlights this option, with a red arrow pointing to it labeled 'クリック' (Click). The main content area shows the 'セキュリティ' (Security) section, with '証明書の管理' (Manage certificates) highlighted by a red dashed box and a red arrow pointing to it labeled 'クリック' (Click). A red dashed arrow on the right side of the screen indicates a 'スクロール' (Scroll) action. In the foreground, the '証明書' (Certificates) management window is open, showing a table of certificates. The table has columns for '発行先' (Issued to), '発行者' (Issuer), '有効期...' (Expiration date), and 'フレンドリ名' (Friendly name). One certificate is listed with the issuer '055a6e9e-c66...' and 'MS-Organizatio...'. Below the table 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)'.

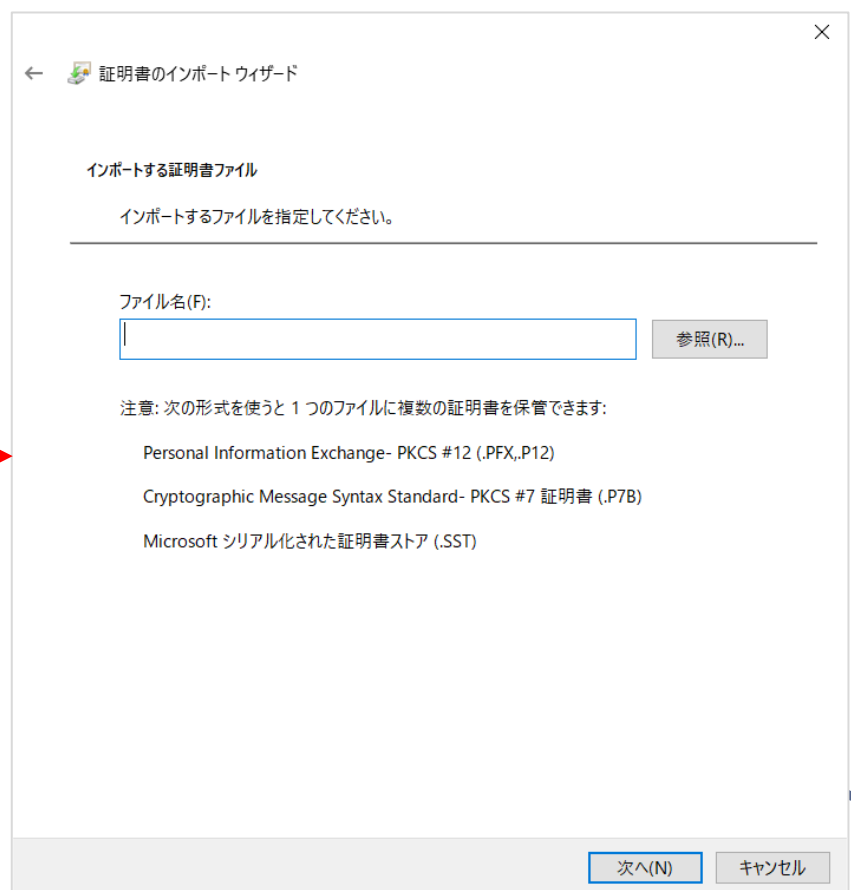
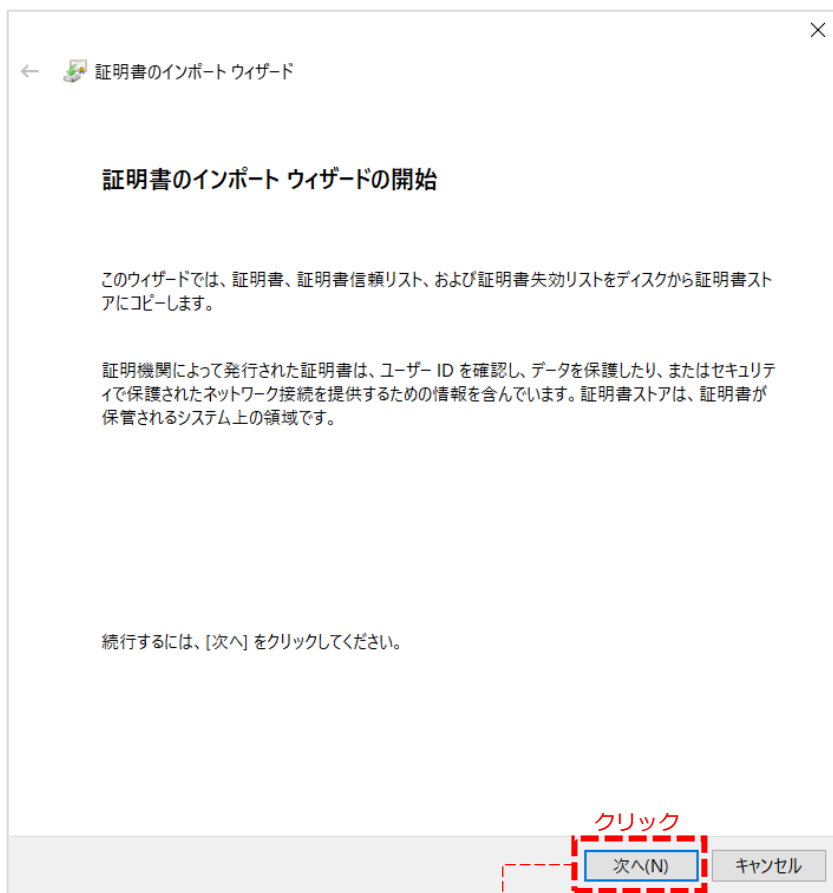
02 Microsoft Edgeをご利用の場合

- 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。



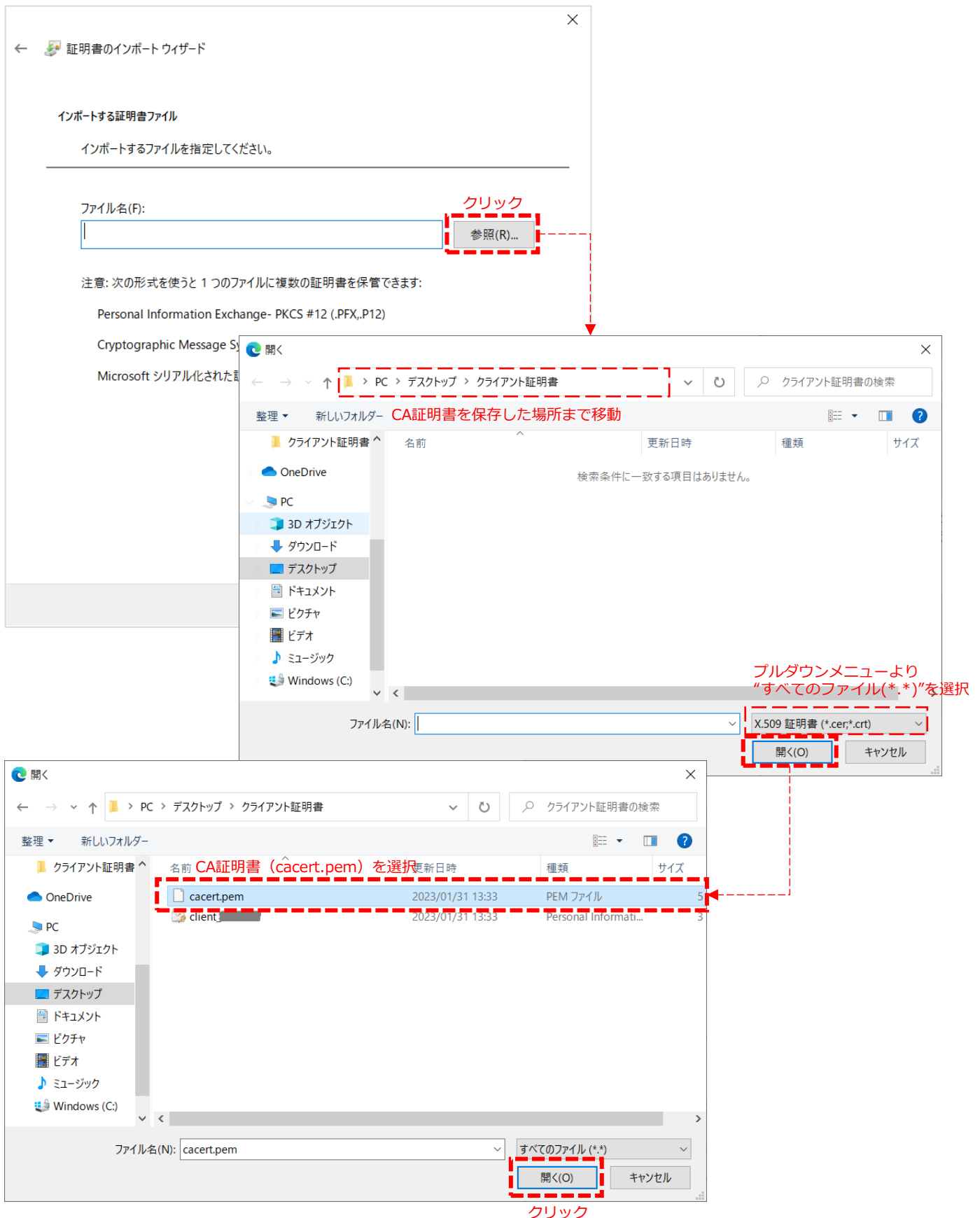
02 Microsoft Edgeをご利用の場合

- 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。

← 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-8\OneDrive\Desktop\クライアント証明書\cacert.pem

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

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:
信頼されたルート証明機関

参照(R)...

次へ(N) キャンセル

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。

← 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:
信頼されたルート証明機関

参照(R)...

クリック

次へ(N) キャンセル

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。

証明書のインポートウィザード

正しくインポートされました。

OK

← 証明書のインポートウィザード

証明書のインポート ウィザードの完了

[完了] をクリックすると、証明書がインポートされます。

次の設定が指定されました:

ユーザーが選択した証明書ストア	信頼されたルート証明機関
内容	証明書
ファイル名	C:\Users\NCS-CHEN\OneDrive\Desktop\クライアント証明書\cacert

完了(F) キャンセル

02 Microsoft Edgeをご利用の場合

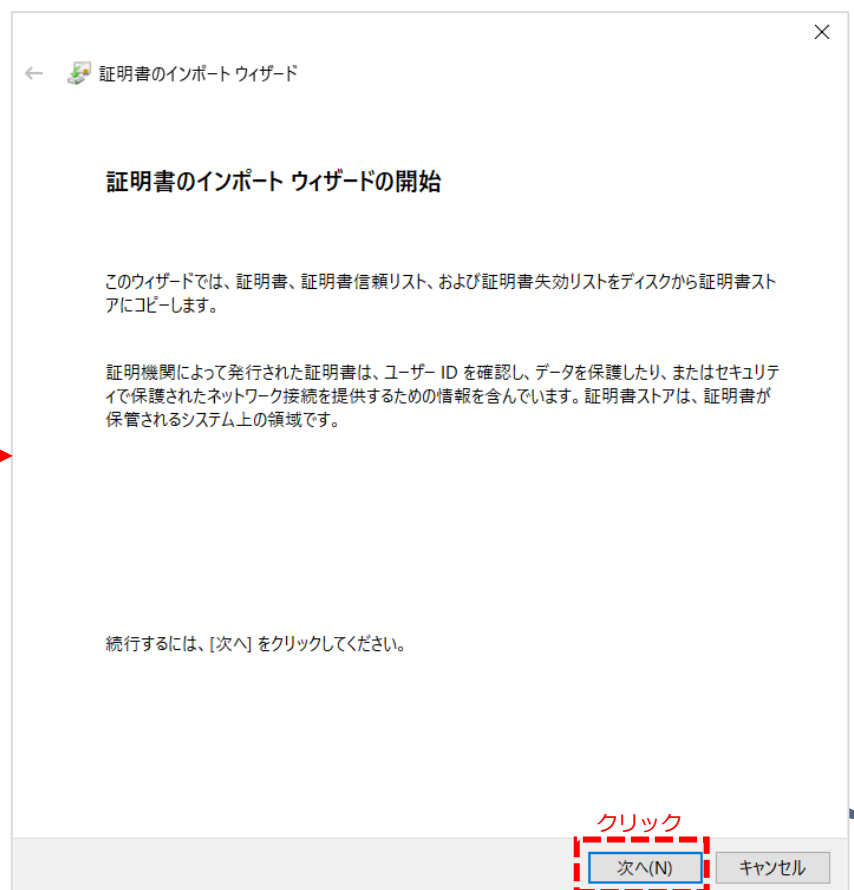
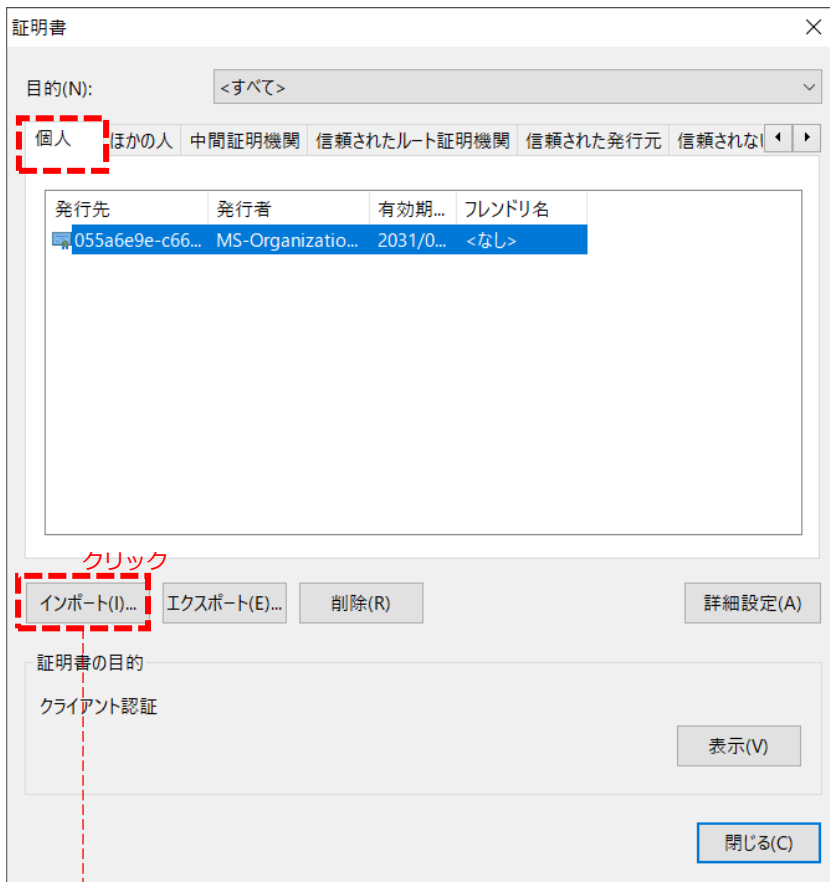
3. クライアント証明書ファイル (*.pfx) のインストール

- ① ... (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 interface. On the left, the 'Settings' (設定) menu is open, and 'Privacy, Search, Services' (プライバシー、検索、サービス) is selected. A red dashed box highlights this menu item with the label 'クリック' (Click). A red arrow points from this menu item to the 'Security' (セキュリティ) section on the right. In the 'Security' section, 'Certificate Management' (証明書の管理) is highlighted with a red dashed box and the label 'クリック' (Click). A red arrow points from 'Certificate Management' to a 'Certificate' (証明書) dialog box that is open in the foreground. The dialog box shows a list of certificates with columns for 'Issued To' (発行先), 'Issued By' (発行者), 'Expiration Date' (有効期), and 'Friendly Name' (フレンドリ名). The first entry is highlighted: '055a6e9e-c66...' issued by 'MS-Organizatio...' with an expiration date of '2031/0...'. Below the list are buttons for 'Import' (インポート), 'Export' (エクスポート), 'Remove' (削除), and 'Details' (詳細設定). At the bottom, there are buttons for 'Import' (インポート), 'Export' (エクスポート), 'Remove' (削除), and 'Details' (詳細設定). The 'Certificate' dialog box also has a 'Close' (閉じる) button at the bottom right.

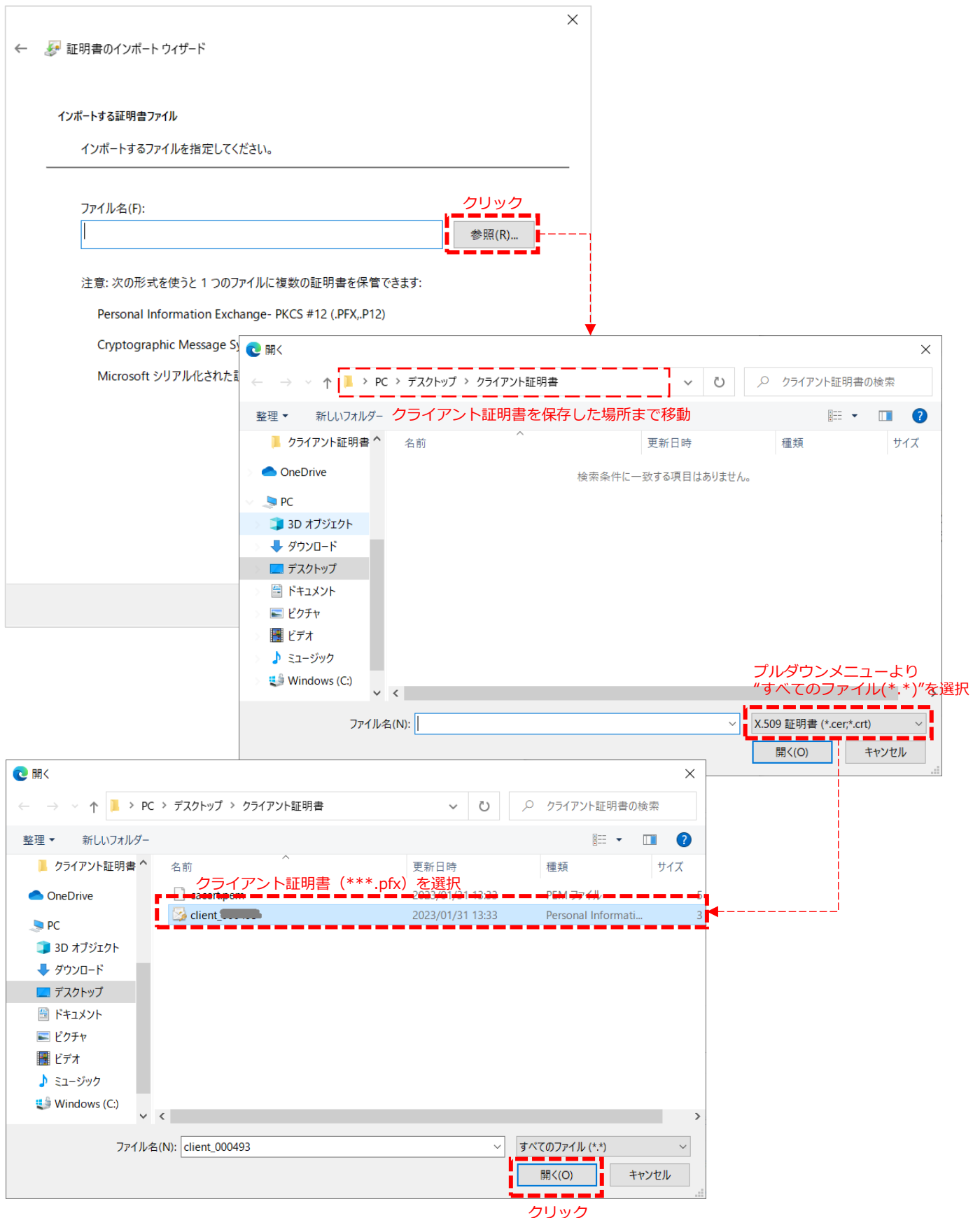
02 Microsoft Edgeをご利用の場合

- 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\%OS-ENVIRONMENT%\AppData\Local\Microsoft\Edge\%ClientID%\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

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。

← 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)...

クリック

次へ(N) キャンセル

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。

証明書のインポート ウィザード

正しくインポートされました。

OK

← 証明書のインポート ウィザード

証明書のインポート ウィザードの完了

[完了] をクリックすると、証明書がインポートされます。

次の設定が指定されました:

ユーザーが選択した証明書ストア	個人
内容	PFX
ファイル名	C:\Users\%CS-CHECK03\Desktop\クライアント証明書\client

完了(F) キャンセル

03

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。

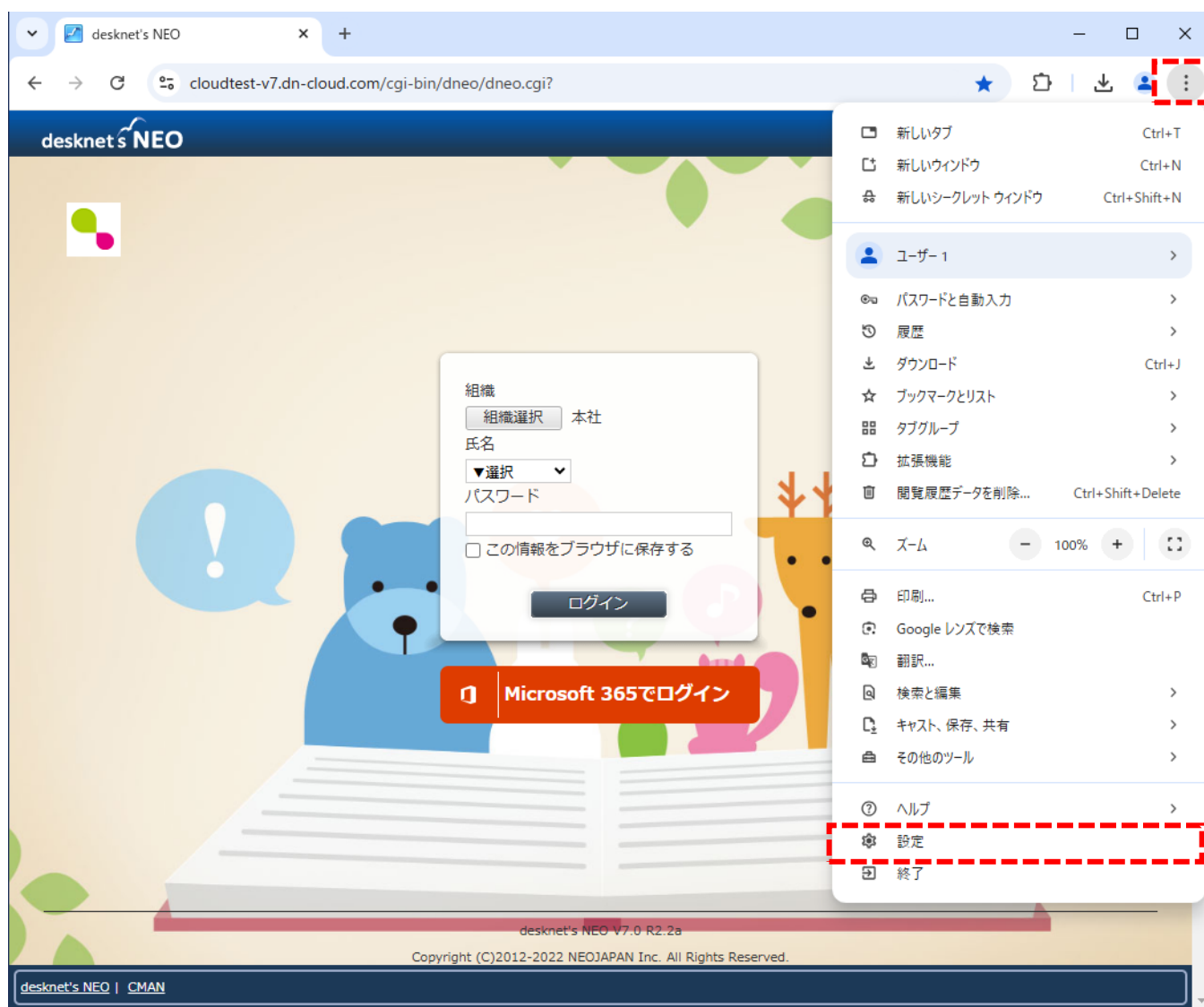
1. クライアント証明書発行サイト用のファイルの準備

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)

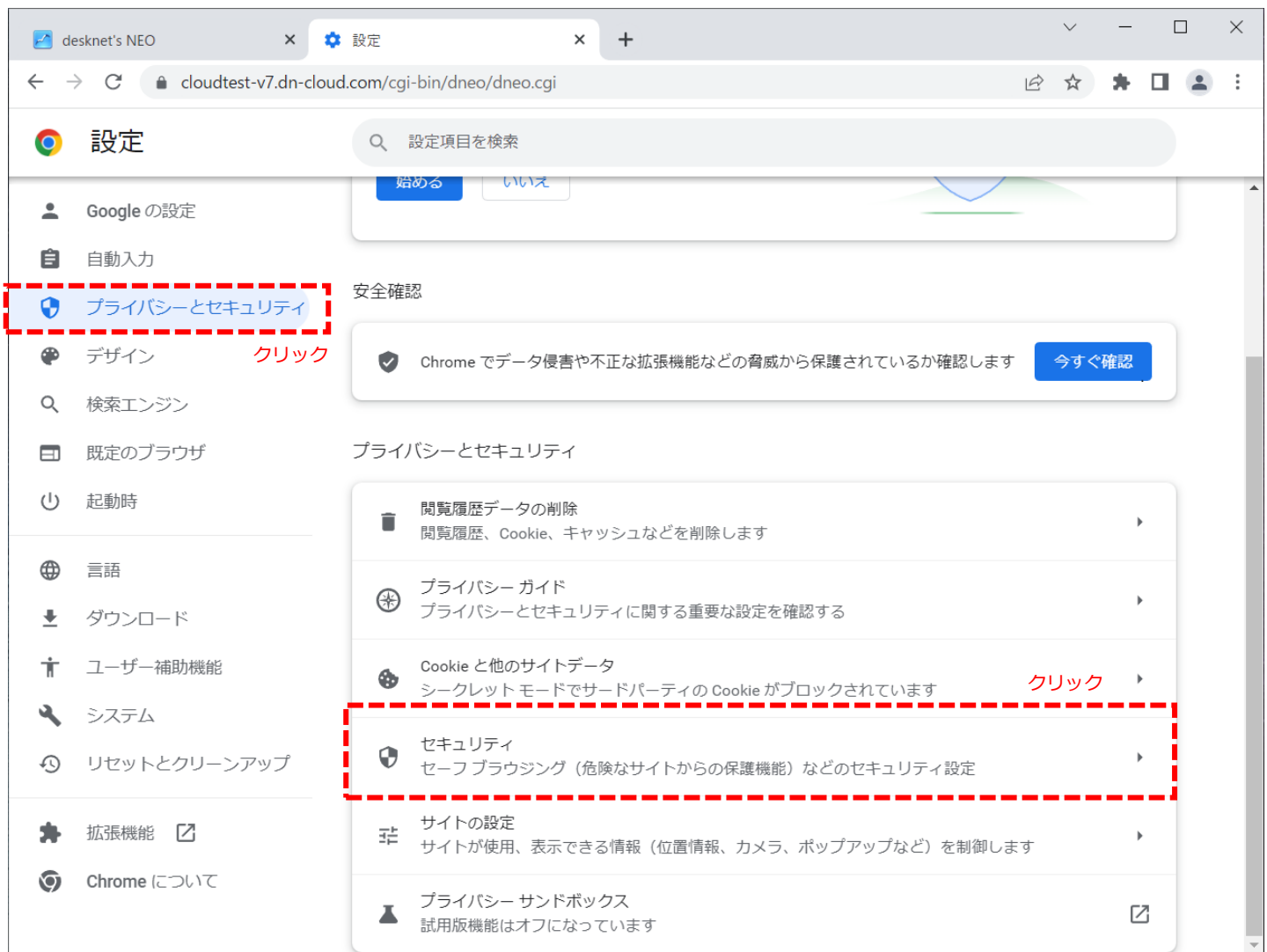
2. CA証明書 (cacert.pem) のインストール

- 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。



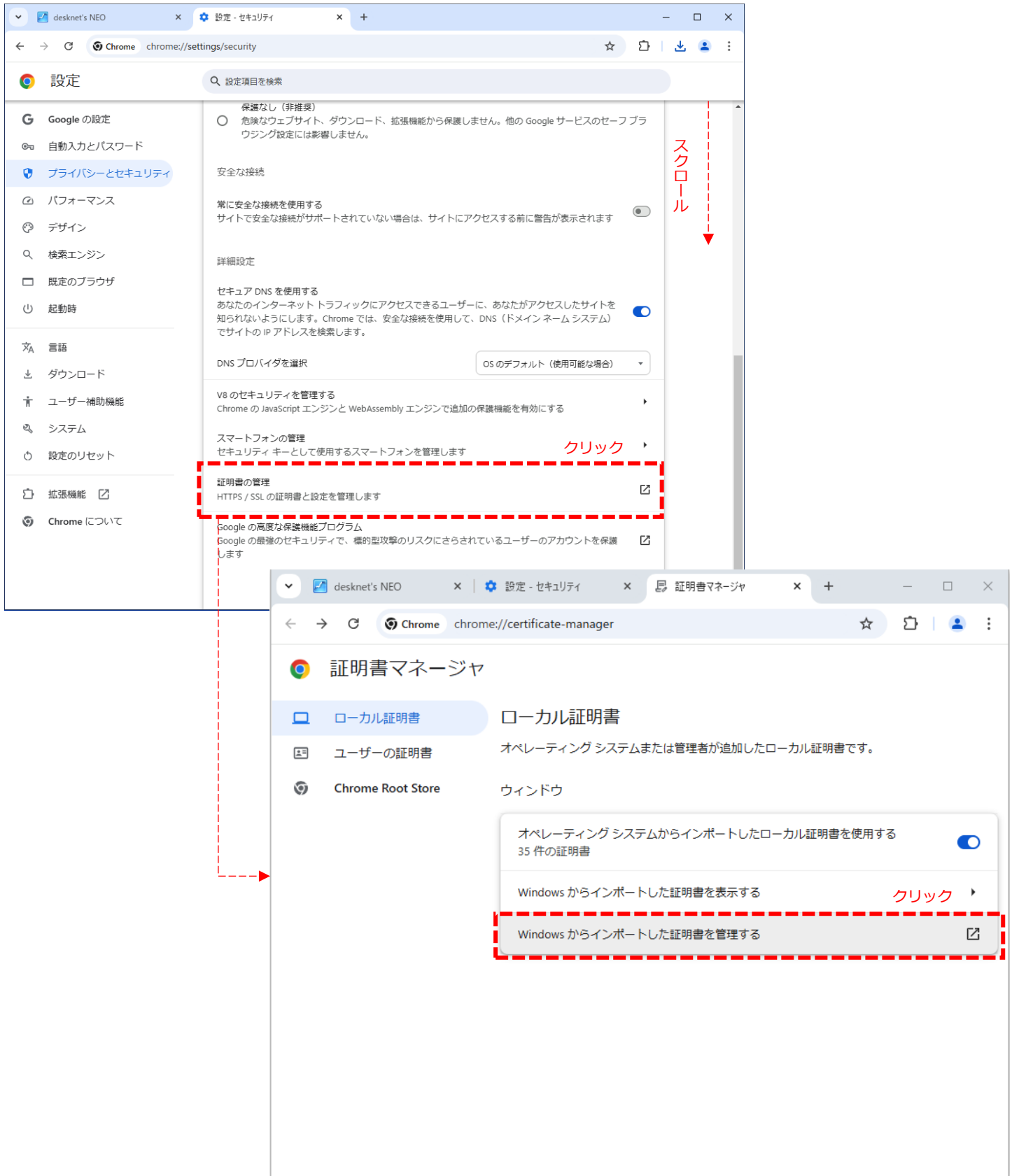
03 Google Chromeをご利用の場合

- 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」をクリックしてください。



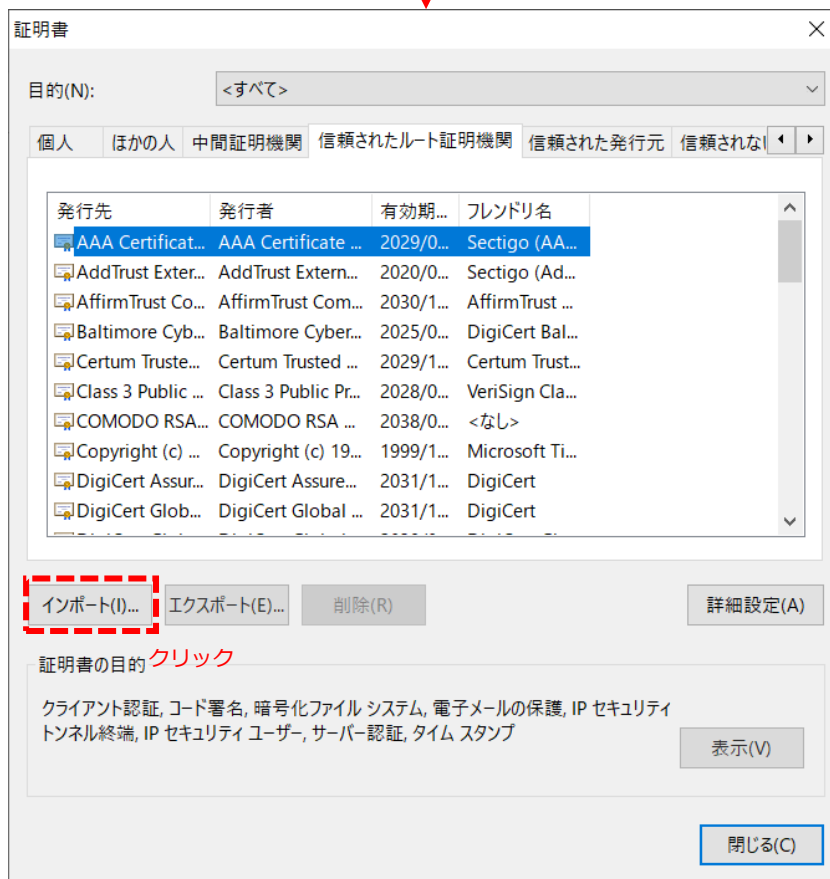
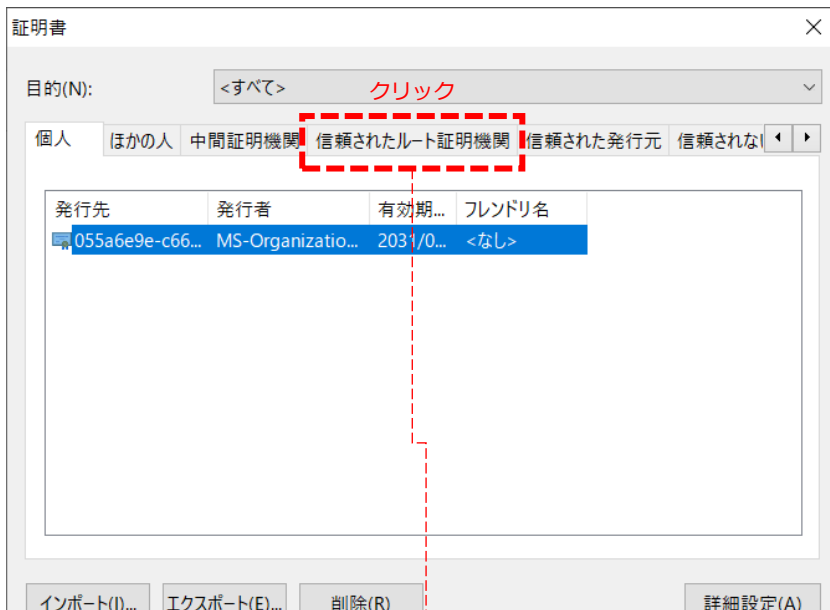
03 Google Chromeをご利用の場合

- 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「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。



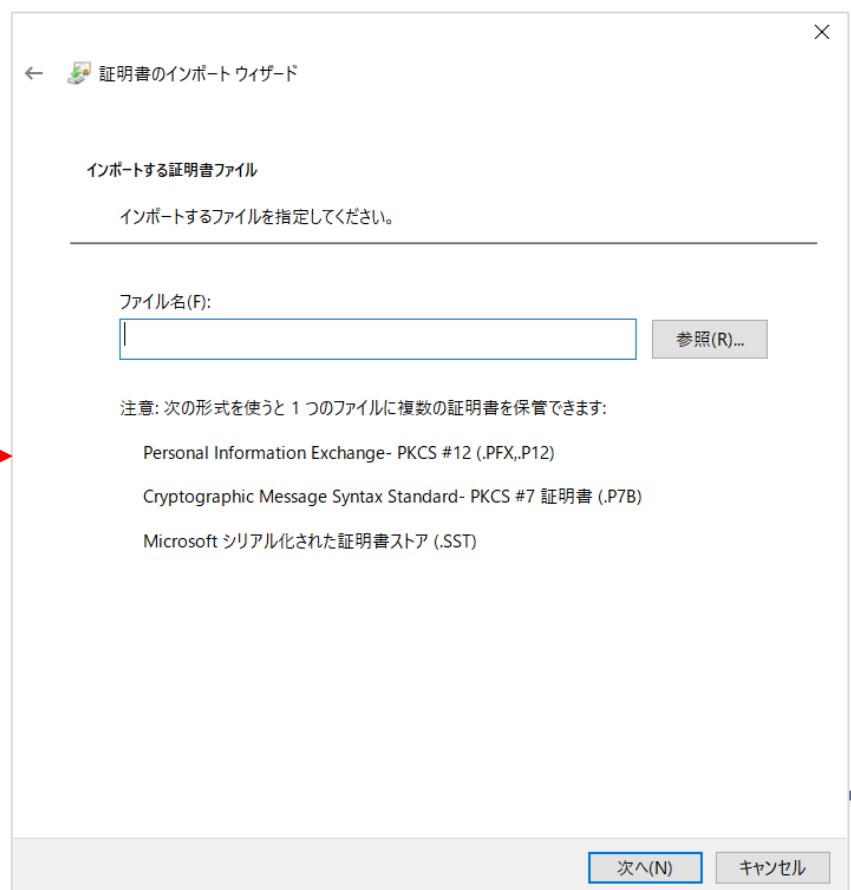
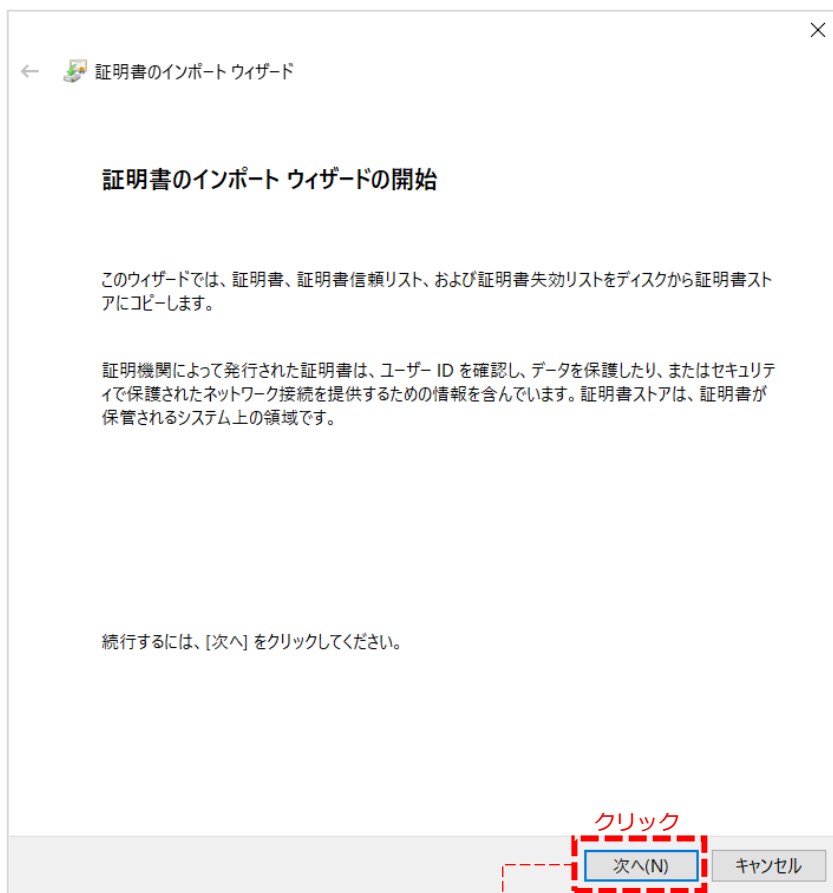
03 Google Chromeをご利用の場合

- 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。



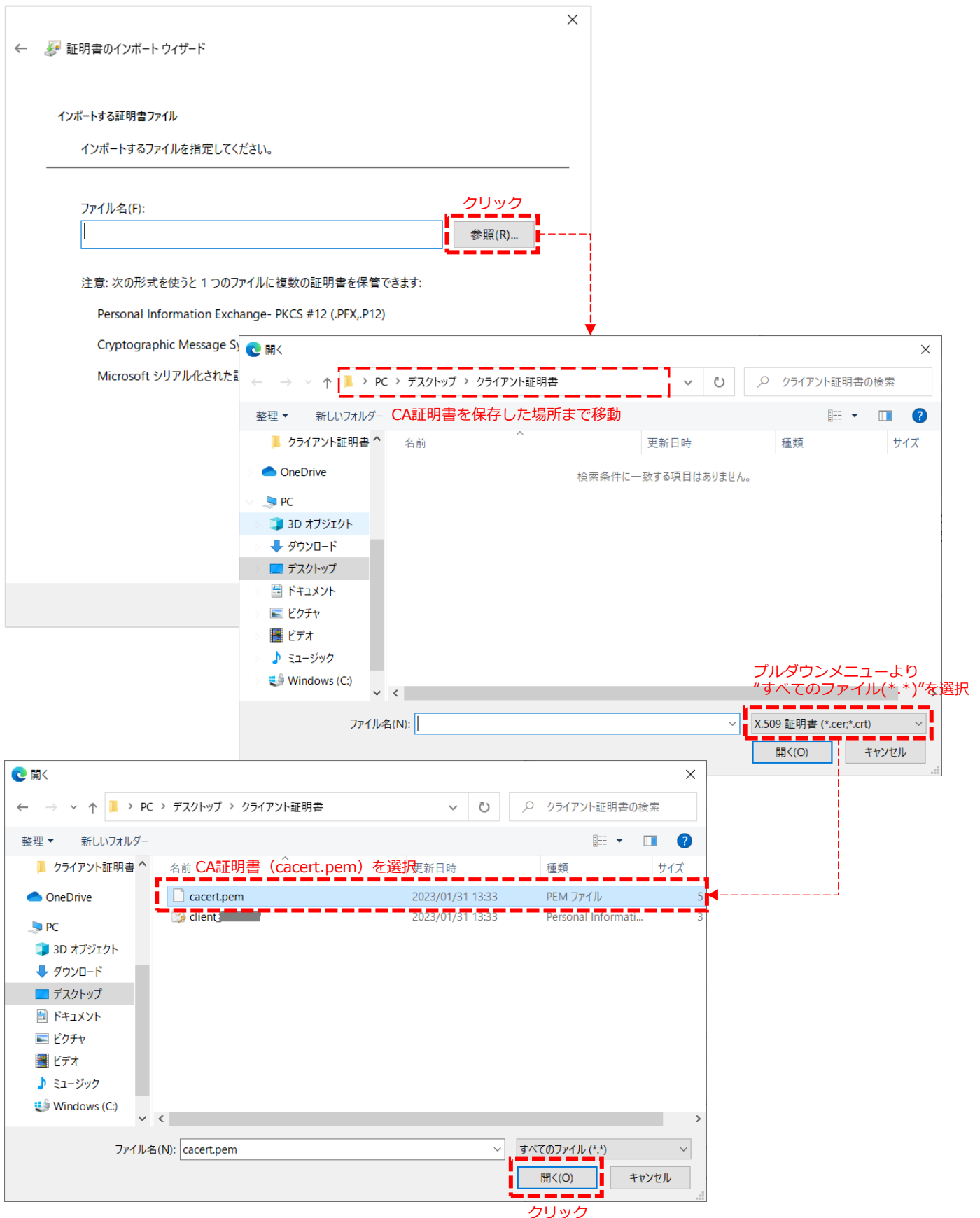
03 Google Chromeをご利用の場合

- 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。

← 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-8\OneDrive\Desktop\クライアント証明書\cacert.pem 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

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:
信頼されたルート証明機関 参照(R)...

次へ(N) キャンセル

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。

← 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:
信頼されたルート証明機関

参照(R)...

クリック

次へ(N) キャンセル

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。

証明書のインポートウィザード

正しくインポートされました。

OK

← 証明書のインポートウィザード

証明書のインポート ウィザードの完了

[完了] をクリックすると、証明書がインポートされます。

次の設定が指定されました:

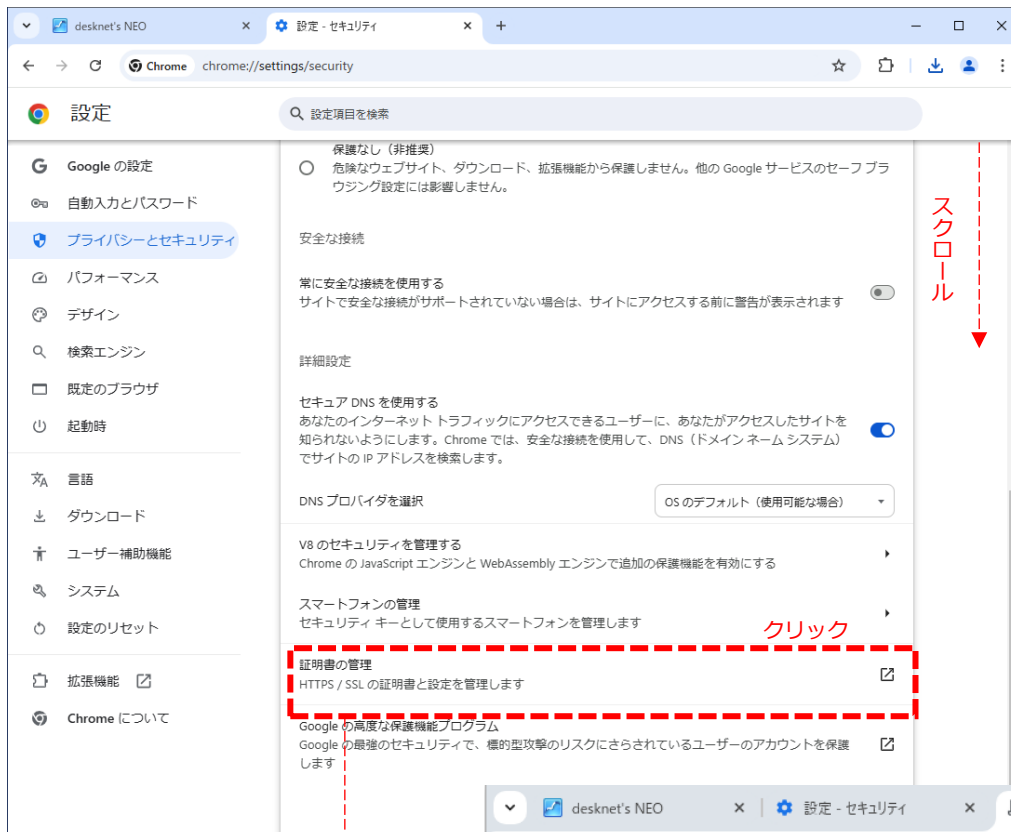
ユーザーが選択した証明書ストア	信頼されたルート証明機関
内容	証明書
ファイル名	C:\Users\NCS-CHEN\OneDrive\Desktop\クライアント証明書\cacert

完了(F) キャンセル

03 Google Chromeをご利用の場合

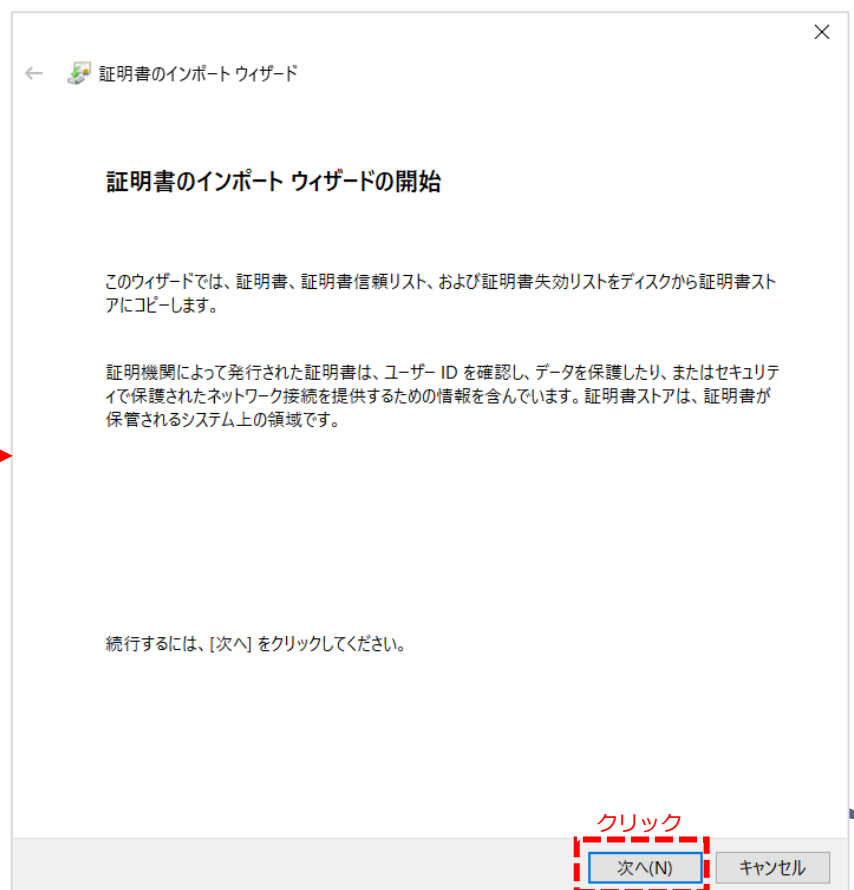
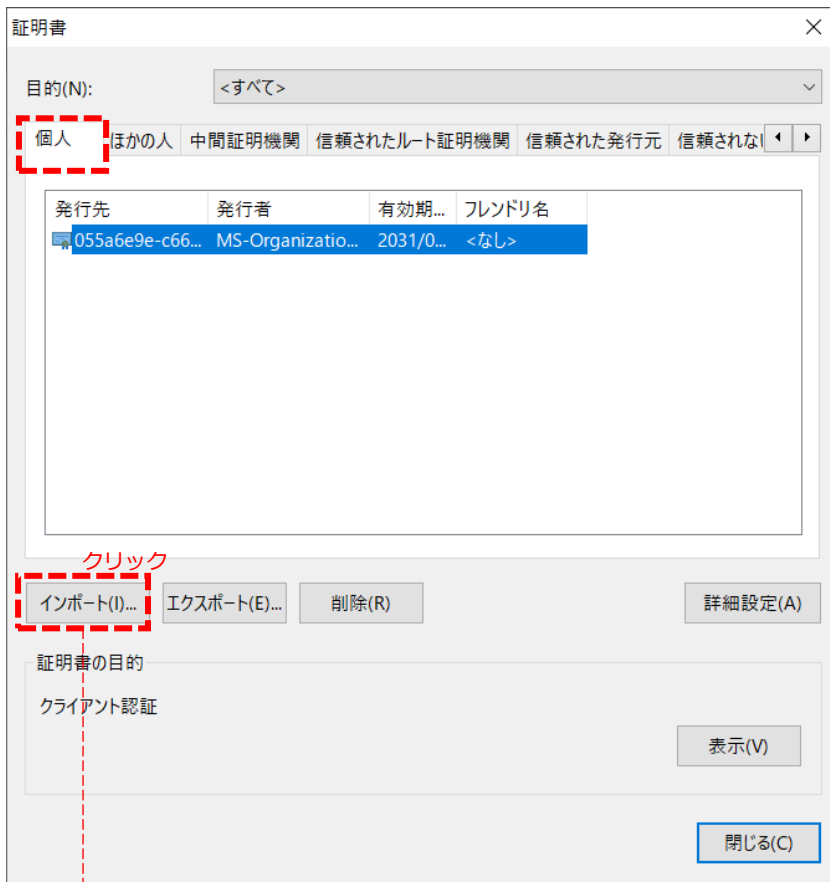
3. クライアント証明書ファイル (*.pfx) のインストール

- 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」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。



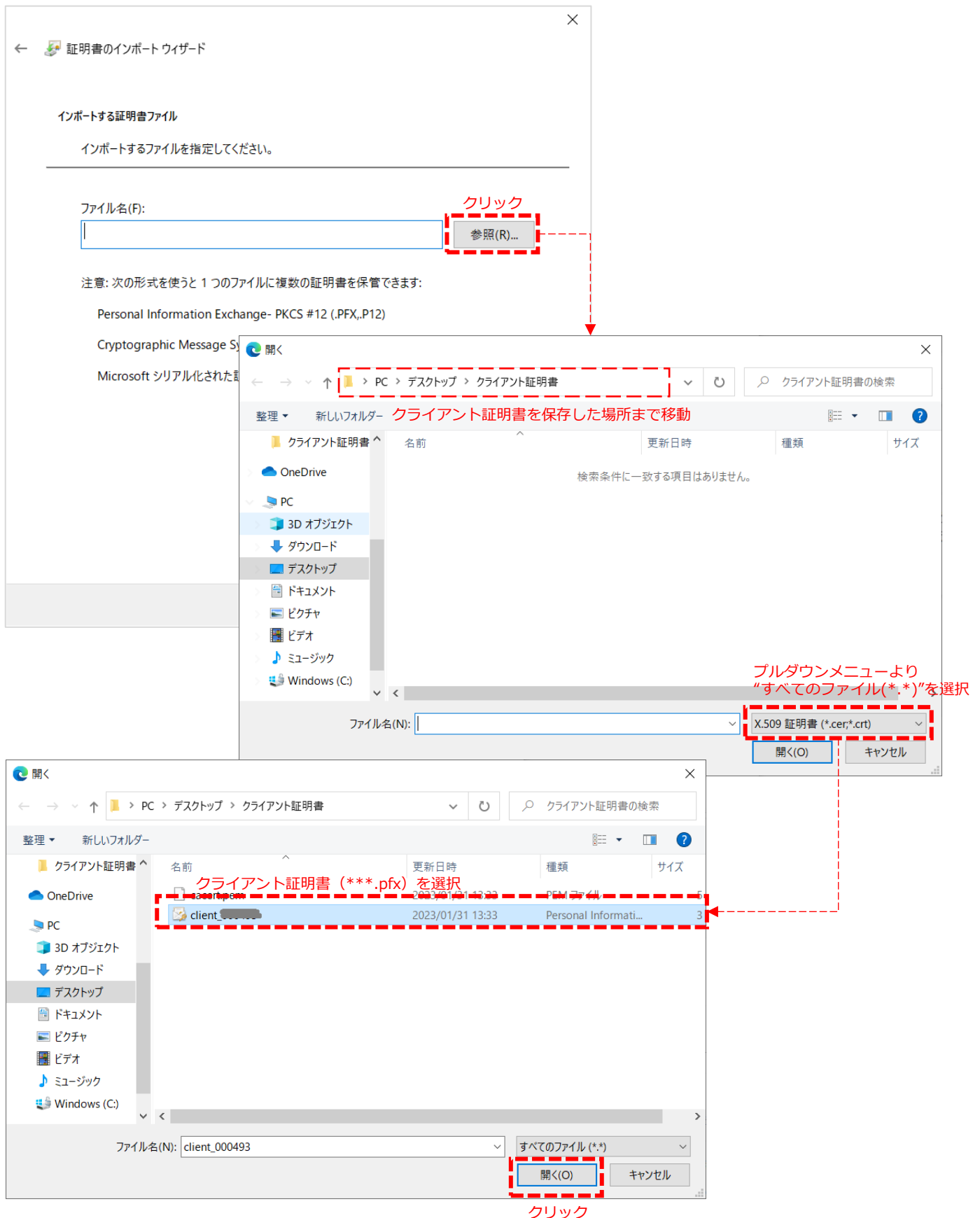
03 Google Chromeをご利用の場合

- 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。

The screenshot shows the "Certificate Import Wizard" window. At the top, it says "インポートする証明書ファイル" (Import certificate file) and "インポートするファイルを指定してください。" (Specify the file to import). Below this, there's a label "ファイル名(F):" followed by a text input field containing "C:\Users¥¥クライアント証明書¥client_". A red dashed rectangle highlights this input field. To the right of the input field is a button labeled "参照(R)..." (Browse...). Below the input field, there's a note: "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:" (Note: Using the following format, you can store multiple certificates in one file:). This is followed by three options: "Personal Information Exchange- PKCS #12 (.PFX,.P12)", "Cryptographic Message Syntax Standard- PKCS #7 証明書 (.P7B)", and "Microsoft シリアル化された証明書ストア (.SST)". At the bottom, there are two buttons: "次へ(N)" (Next) and "キャンセル" (Cancel). The "次へ(N)" button is highlighted with a red dashed rectangle, and a red arrow points to it from the word "クリック" (Click) written above it.

←

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

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

← 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。

← 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

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。

証明書のインポート ウィザード

正しくインポートされました。

OK

← 証明書のインポート ウィザード

証明書のインポート ウィザードの完了

[完了] をクリックすると、証明書がインポートされます。

次の設定が指定されました:

ユーザーが選択した証明書ストア	個人
内容	PFX
ファイル名	C:\Desktop\クライアント証明書\client

完了(F) キャンセル

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。

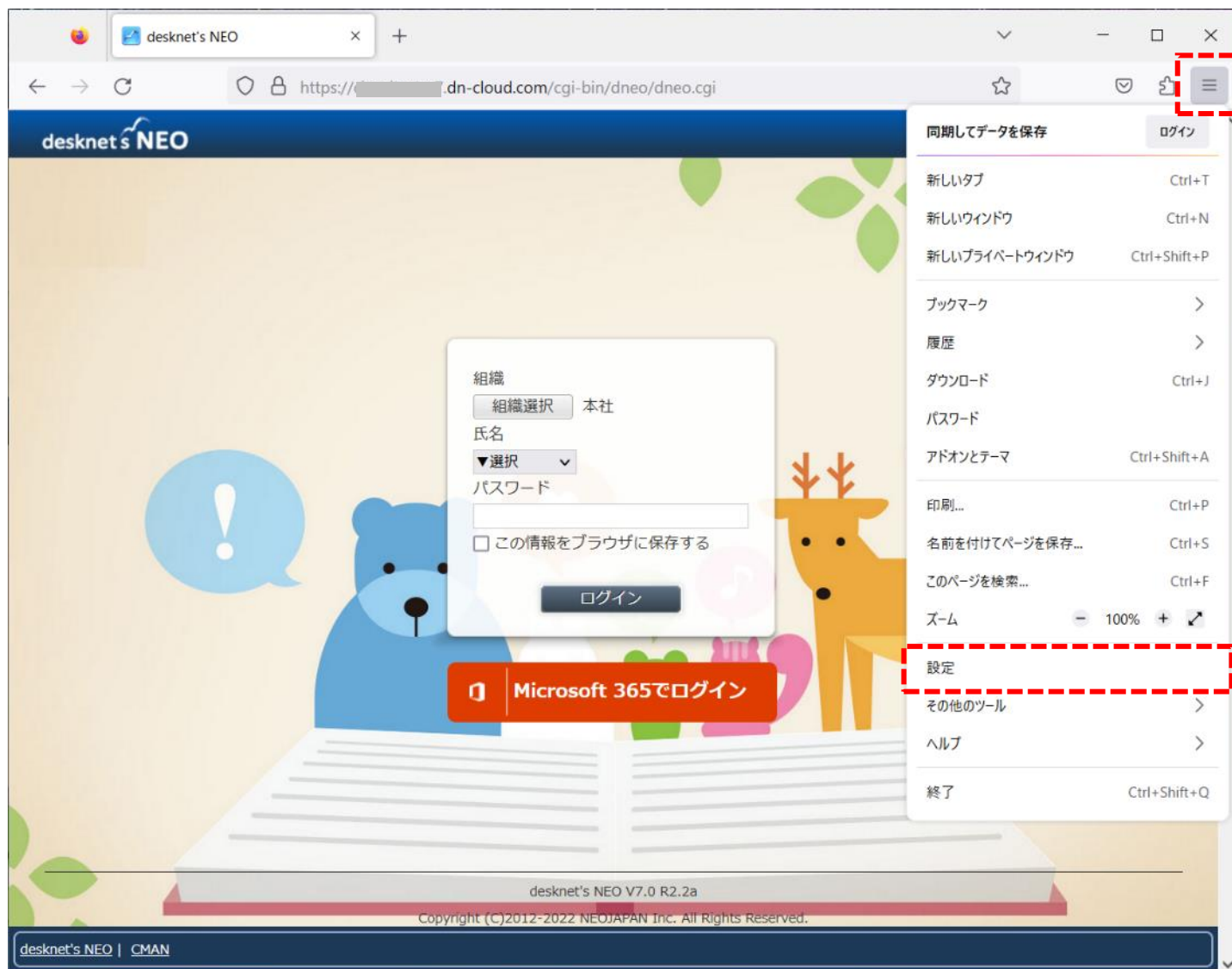
1. クライアント証明書発行サイト用のファイルの準備

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)

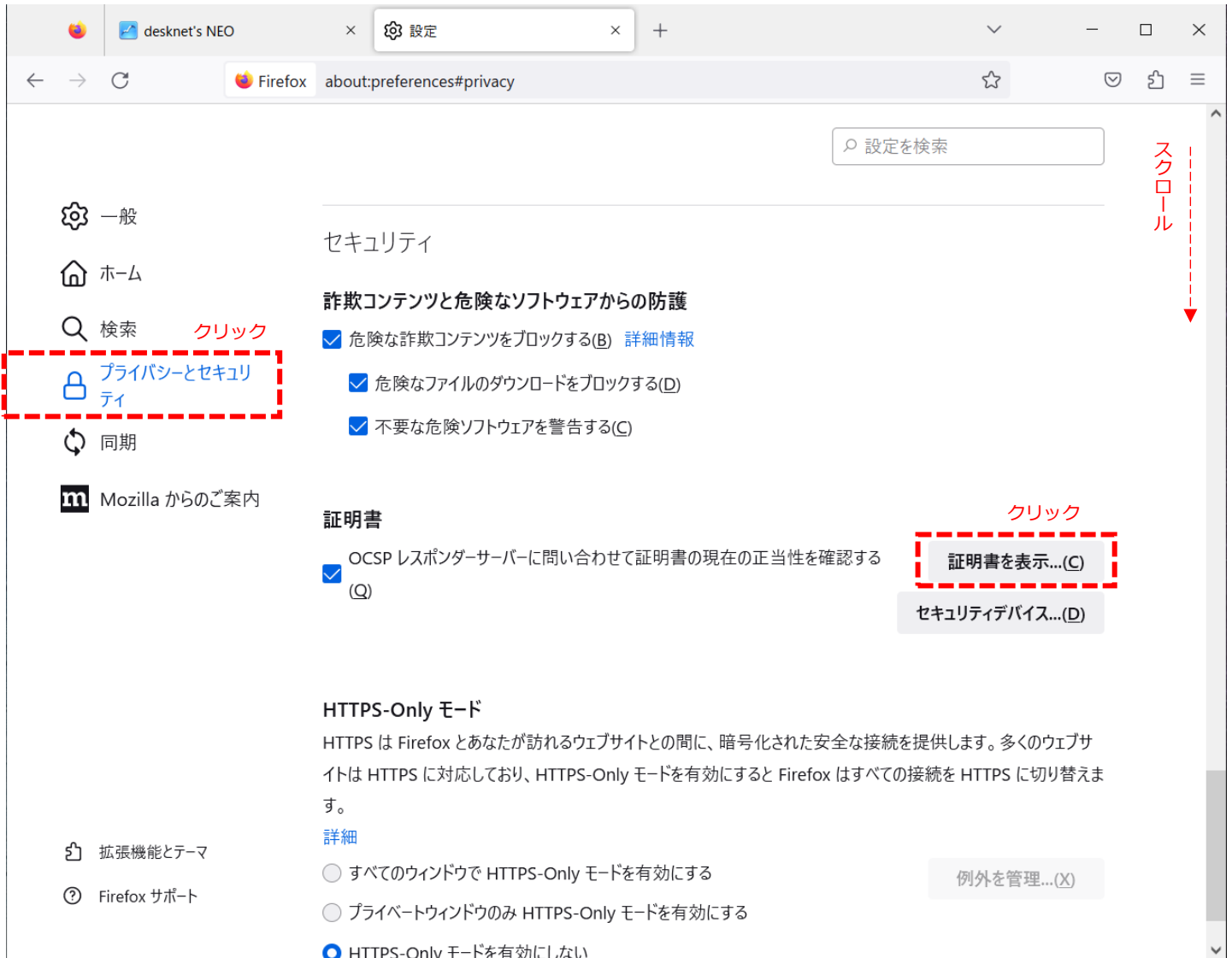
2. CA証明書 (cacert.pem) のインストール

- 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。



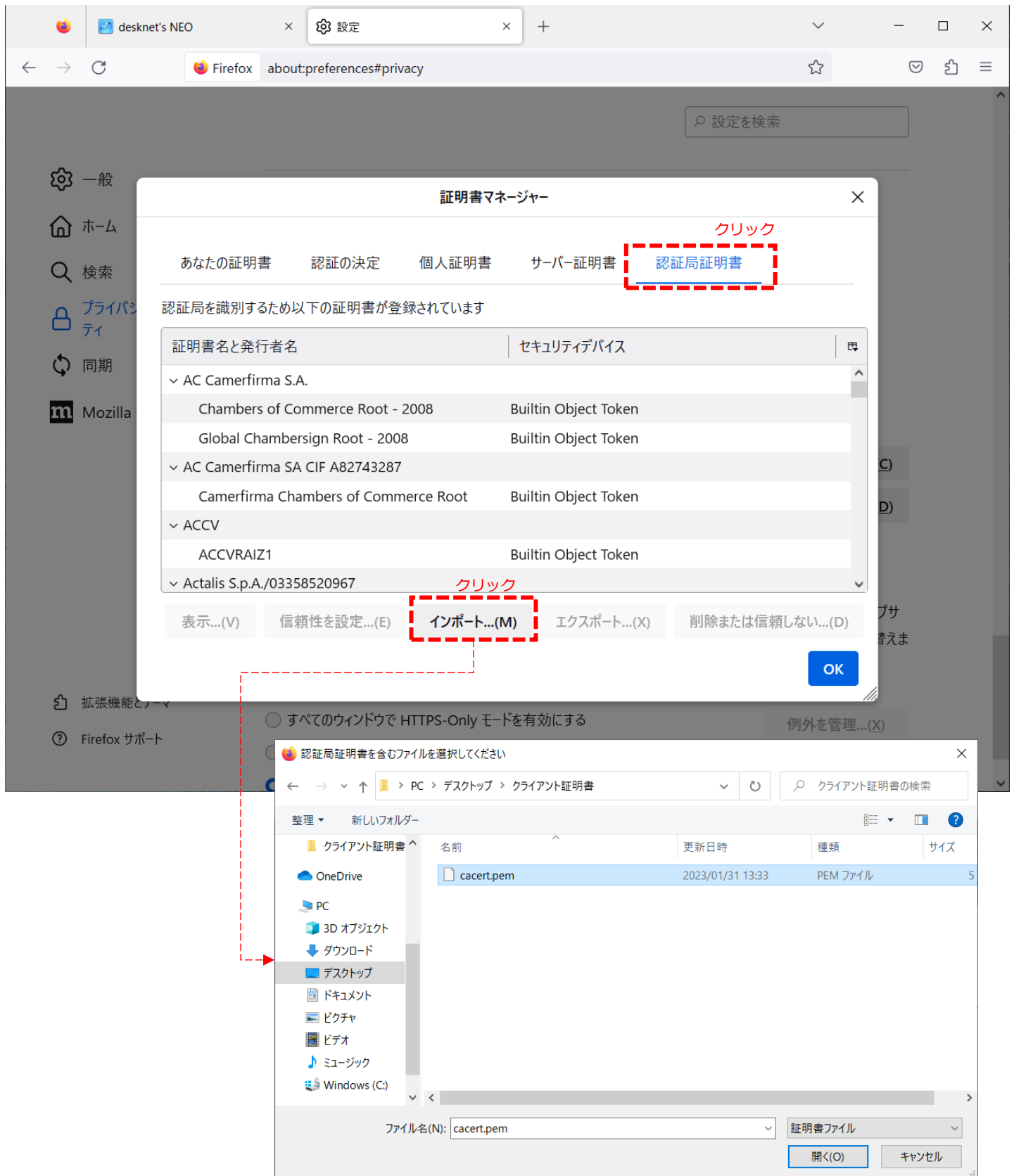
04 Mozilla Firefoxをご利用の場合

- 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。



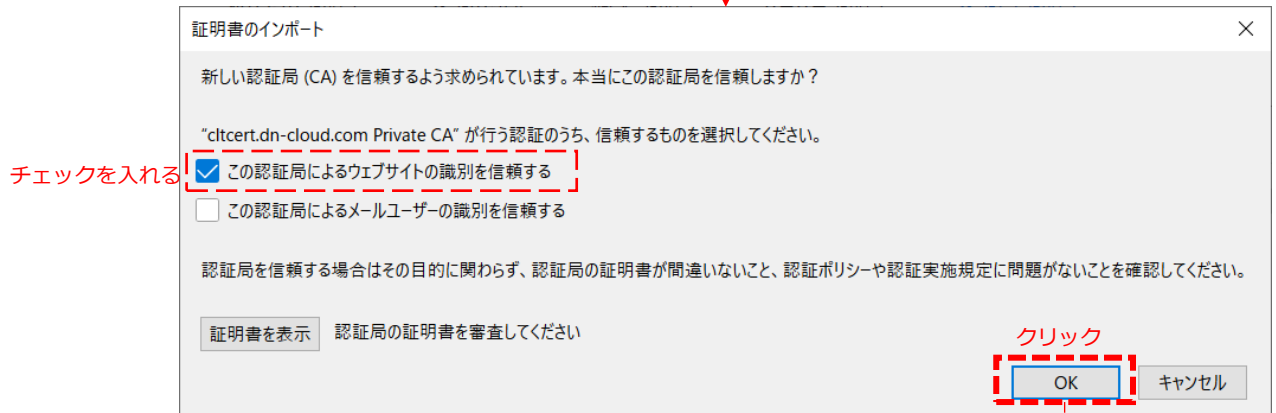
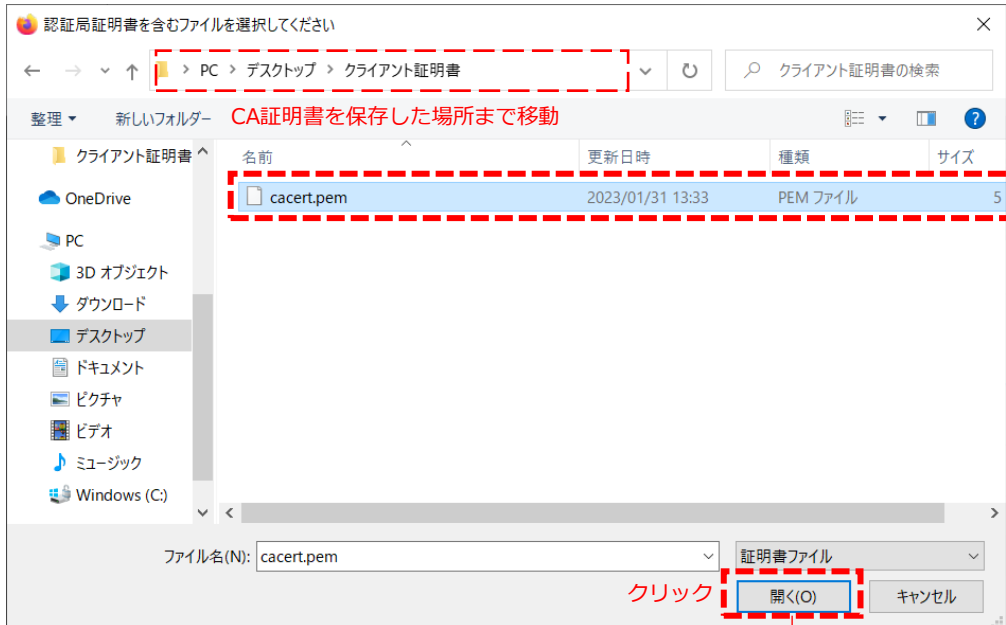
04 Mozilla Firefoxをご利用の場合

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。



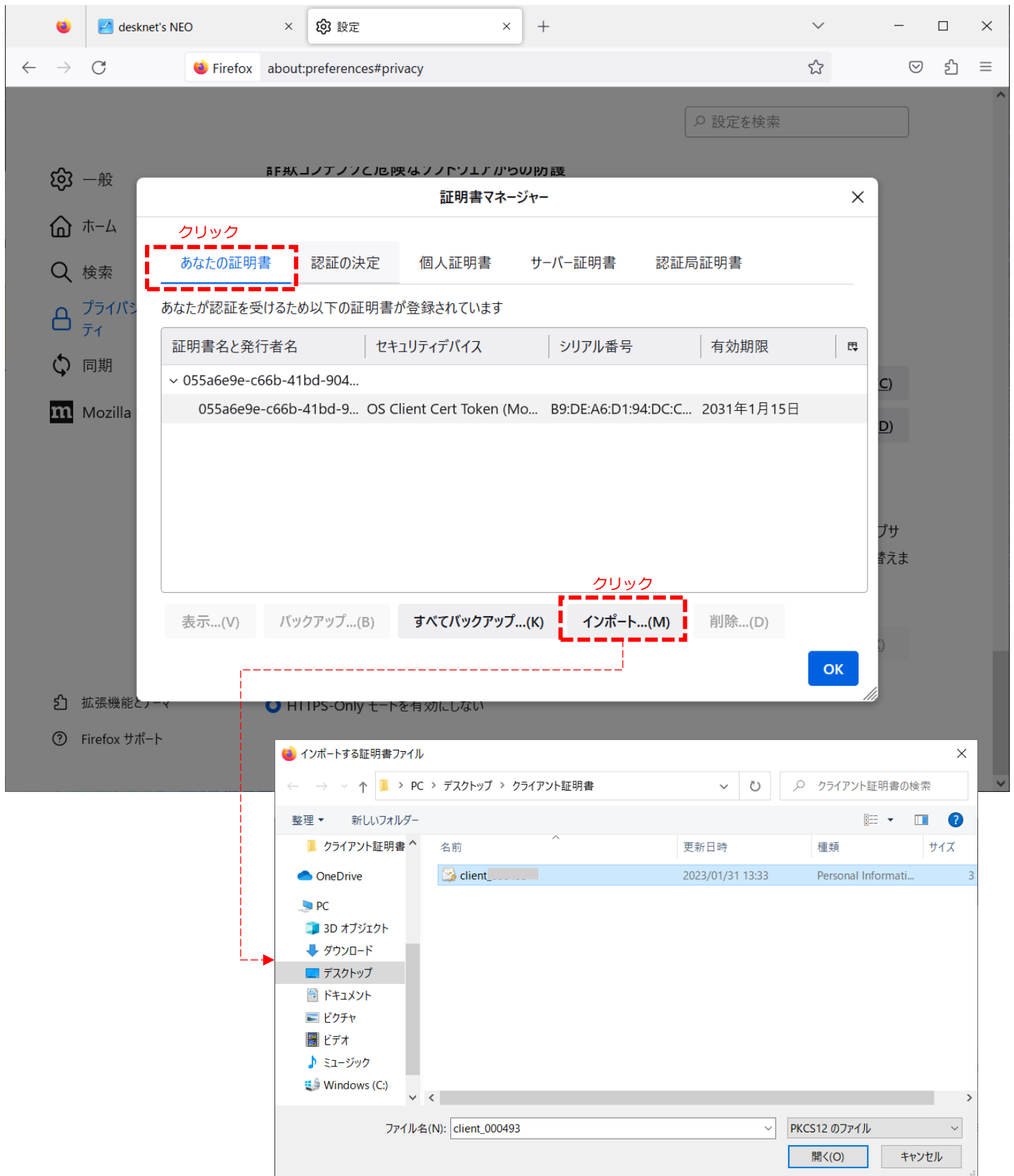
3. クライアント証明書ファイル (*.pfx) のインストール

- 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。



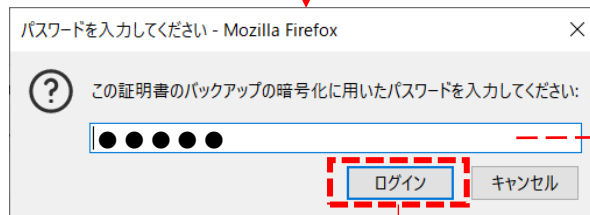
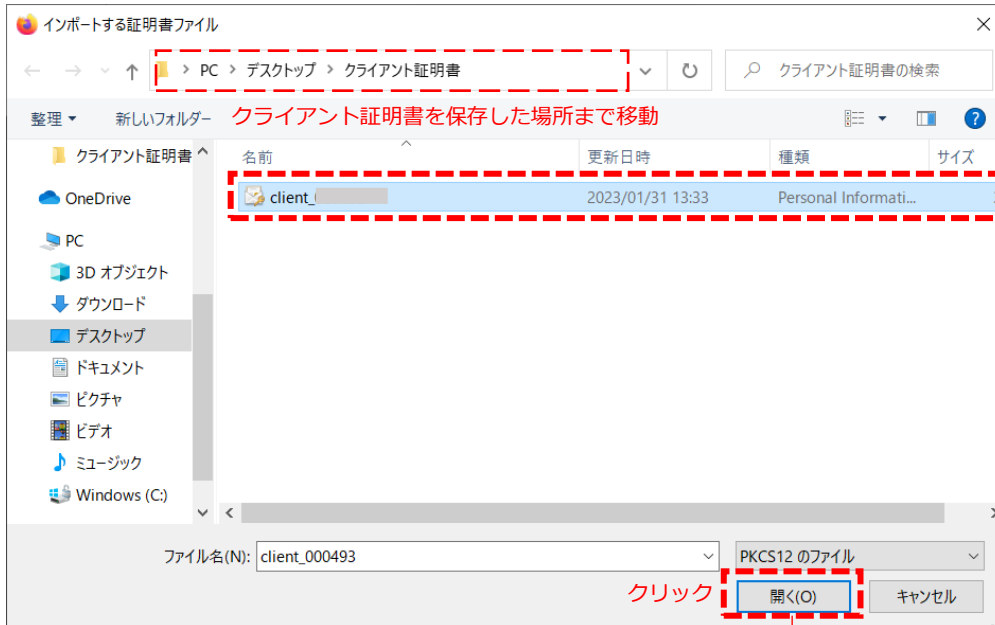
04 Mozilla Firefoxをご利用の場合

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)
- 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

