

第7次 NACCS 用デジタル証明書 新規取得／更新手順書
〈NACCS デジタル証明書取得 Web ブラウザ編〉

Ver-202506

輸出入・港湾関連情報処理センター株式会社

目次

1. 留意事項	1
1.1. デジタル証明書登録時のアカウントについて.....	1
1.2. デジタル証明書の有効期間について.....	1
1.3. ユーザ利用環境について.....	1
2. 事前準備	2
2.1 社内システムへの通信許可設定	2
2.2. ルート証明書について.....	2
3. 証明書の新規取得手順.....	3
3.1. 証明書の新規取得手順.....	3
4. 証明書の登録手順	8
5. 証明書の確認方法	12
6. 証明書の更新手順	14
6.1. 証明書の更新手順.....	14
7. サポート情報	21
7.1. ルート証明書の取得方法について.....	21
7.2. ご利用にあたっての注意事項.....	27
7.3. サービスメンテナンス.....	27

1. 留意事項

本書では、第7次 NACCS 用デジタル証明書を Web ブラウザで新規取得／更新する方法について説明しています。

1.1. デジタル証明書登録時のアカウントについて

デジタル証明書を登録される際は、ご自身が業務をする際のログオンアカウントで登録してください。例えば「Administrator」でログオンしデジタル証明書を登録されますと、その証明書は「Administrator」でログオンしたときにしか使用できませんので、ご注意ください。

1.2. デジタル証明書の有効期間について

デジタル証明書の有効期間は、発行日から **5年1か月**となります。証明書の有効期間終了日の28日前から更新可能となり、有効期限までに更新をしてください。更新作業を怠りますと、有効期限を過ぎたデジタル証明書では、「netNACCS ソフトでの送受信」および「WebNACCS へのアクセス」、「netAPI での送受信」ができなくなり、デジタル証明書の再発行手続きが必要となりますので、ご自身のデジタル証明書の有効期限をご確認の上、更新作業は確実に行っていただきますようお願いいたします。

※ 再発行が必要となった場合の手続きにつきましては、NACCS 掲示板「申込手続 (NSS)」コンテンツに掲載の「デジタル証明書再発行の入力例」をご参照ください。

1.3. ユーザ利用環境について

(1) 対応 OS およびブラウザ

OS	対応ブラウザ		
	Microsoft Internet Explorer	Microsoft Edge	Google Chrome
Windows11 Pro	×	○	○

(2) 表示言語

日本語

2. 事前準備

本章は、第 7 次 NACCS 用デジタル証明書を Web ブラウザでの新規取得／更新する際の事前準備について説明します。

2.1 社内システムへの通信許可設定

「netNACCS ソフトでの送受信」および「WebNACCS へのアクセス」、「デジタル証明書の取得」等にあたり、貴社のセキュリティシステムで通信が制限されないよう、事前に以下 URL を通信許可設定するようお願いします。なお、通信ポートは TCP443(https)となります。

【netNACCS ソフトでの送受信】

(本番) uac21j0vvasdpv9j7.nac.nacacs.jp

(試験) acjh4icrfmdu4utg7.nac.nacacs.jp

【WebNACCS へのアクセス】

web-prod.nac.nacacs.jp

【デジタル証明書の取得】

cert.nac.nacacs.jp

2.2. ルート証明書について

第 7 次 NACCS では、TLS 暗号化通信に必要なルート証明書は、パブリック認証局（発行者：Security Communication RootCA2）で発行したものを利用します。

通常、WindowsOS では「ルート証明書更新プログラム」にて自動的に登録されるため、手動でのルート証明書の取得／登録作業は、不要となります。

もし、この「ルート証明書更新プログラム」を無効にしている場合などは、手動でルート証明書を取得／登録するようお願いします。（「7.1. ルート証明書の取得方法について」参照）

特に、netAPI 利用者様などサーバ OS でご使用されるお客様は、当該ルート証明書が登録されていない場合がありますので、ご注意ください。

3. 証明書の新規取得手順

本章は、下記の「第7次 NACCS 用デジタル証明書」を新規取得する手順となります。

- ・第7次 NACCS 用デジタル証明書（クライアント証明書）
- ・第7次 NACCS 用デジタル証明書（ルート証明書）

<注>

以下の手順は、画面が実際と一部異なる場合があります。

3.1. 証明書の新規取得手順

- (1) ブラウザを起動し、以下のユーザ認証画面 URL にアクセスします。

ユーザ認証画面 URL

<https://cert.nac.nacccs.jp/NACCSClientCA/pages/ee/index.jsp?s=Site1&p=CA1/NACCS&lan=ja>

- (2) 「認証コード1」、「認証コード2」にそれぞれ入力して「Login」をクリックします。

※ 認証コード1～2は、NSS（NACCS サポートシステム）の「契約内容の確認 | netNACCS | 論理端末名 / デジタル証明書」より、ご参照ください。

- (3) 「NACCS デジタル証明書取得画面」が表示されます。



＜セッションが無効になった場合の対応＞

ログインした状態で一定時間作業を行わない場合、自動的にログアウトします。自動的にログアウトするとメニュー項目をクリックしてもセッションが無効であることを示す画面が表示され操作を続けることができません。このような状態になった場合、ログインしなおしてください。

- (4) 「NACCS デジタル証明書取得画面」のメニューから「デジタル証明書の取得」をクリックします。



- (5) 事前に入手した「認証コード 3」及び「証明書パスワード」、「証明書パスワードの確認」を入力し、「Submit」をクリックします。

なお、「証明書パスワード」とは、証明書ファイル（PKCS#12 形式）を暗号化し、端末へ登録する際に一時的に使用するためのもので、任意の文字列を指定してください。この後、手順「4. 証明書の登録手順（3）」で証明書をインポートする際に使用します。忘れないようご注意ください。

※ 認証コード 3 は、NSS（NACCS サポートシステム）の「契約内容の確認 | netNACCS | 論理端末名 / デジタル証明書」より、ご参照ください。

※ 証明書パスワードには半角英数字または記号を指定できます。8 桁以上のパスワード設定を推奨します。証明書パスワードの設定条件は以下のとおりとなります。

- ・ 半角英字は、大文字、小文字を区別します。
- ・ 記号は以下の 32 種類となります。
 ‘ ` - ! “ # \$ % & () * , . / : ; ? @ [] ^ _ { | } ~ ¥ + < = > _)
- ・ 証明書パスワードを空白にすることはできません。
- ・ 文字数は、1 桁以上 16 桁以下となります。

※ 証明書パスワードを「4. 証明書の登録手順」までに忘れた場合は、再発行のお手続きが必要となり、新しい認証コード 3 にて再度「3. 1. 証明書の新規取得手順」から実施し直してください。

- (6) 「Download」をクリックします。

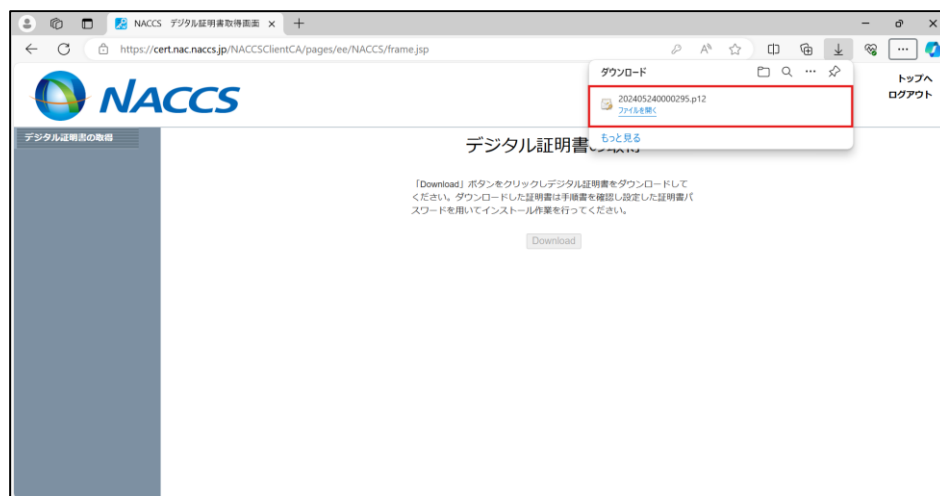


※ デジタル証明書の取得は、セキュリティ確保の目的から、最初に取得した日の翌日からロックされ、再取得できなくなります。ご注意ください。

- (7) 証明書ファイル（年月日から始まる数字 15 桁＋ファイル拡張子 p12）がダウンロードされます。（ファイル名例：202501011234567.p12）

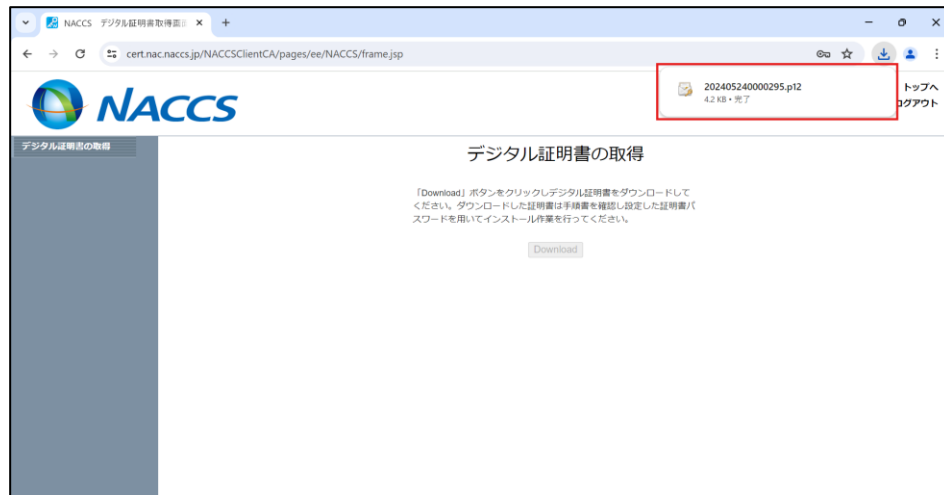
<Microsoft Edge の場合>

ウィンドウ右上部分に「ダウンロード」が表示されます。なお、一定時間経過後「ダウンロード」の表示は消えますが、メニューの設定「…」→「ダウンロード」から再度表示させることができます。



<Chrome の場合>

ウィンドウ右上部分にダウンロードした証明書ファイル名が表示されます。なお、一定時間経過後この表示は消えますが、メニューの「ダウンロード」アイコンをクリックすれば最近のダウンロード履歴を表示させることができます。



※ ダウンロードしたファイル名の「ファイルを開く」をクリックします（ブラウザが Chrome の場合は、ファイル名のところでクリックします）。

※ 証明書ファイル（PKCS#12 形式）の中に、第 7 次 NACCS 用クライアント証明書および秘密鍵、ルート証明書が入っています。ダウンロードしたファイルは「4. 証明書の登録手順」が終了するまで紛失しないようご注意ください。

- (8) 「証明書のインポートウィザードの開始」画面が表示されます。以降の手順は、「4. 証明書の登録手順」に進んでください。

なお、ダウンロードの表示が消えている場合であっても、エクスプローラでダウンロードフォルダを開き、該当のファイル名をダブルクリックすることでも「証明書のインポートウィザードの開始」画面が表示されます。

4. 証明書の登録手順

本章は、「第7次 NACCS 用デジタル証明書」を登録する手順となります。

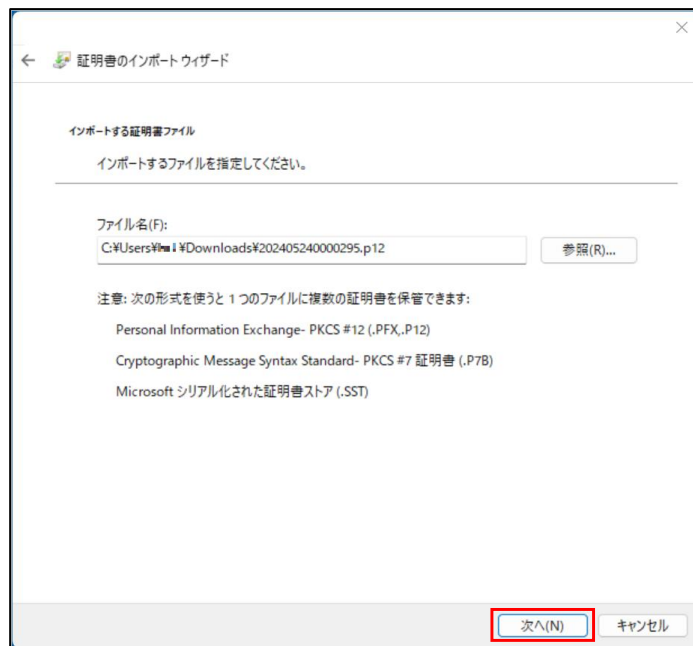
<注>

以下の手順は、画面が実際と一部異なる場合があります。

- (1) 登録したい証明書に該当する証明書ファイル（拡張子: p12）をダブルクリックします。「証明書のインポートウィザード」画面が表示されますので、保存場所が「現在のユーザー」になっていることを確認し、「次へ」をクリックします。



- (2) 「次へ」をクリックします。



- (3) 本手順「3. 1. 証明書の新規取得手順 (5)」、「6. 1. 証明書の更新手順 (7)」で指定した「証明書パスワード」を入力して「次へ」をクリックします。



※ 「3. 1. 証明書の新規取得手順」、「6. 1. 証明書の更新手順」で設定した「証明書パスワード」を入力してください。

- (4) 「次へ」をクリックします。



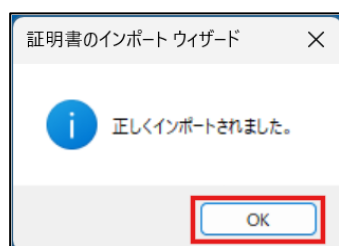
- (5) 「完了」をクリックします。



- (6) 初めてユーザ証明書の新規登録をした場合などで以下の画面が表示されることがあります。この画面が表示された場合は、「はい」をクリックしてください。



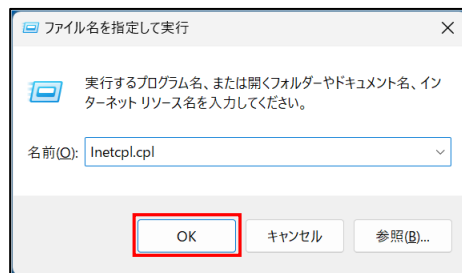
- (7) 下記のダイアログが表示されれば完了です。「OK」をクリックします。



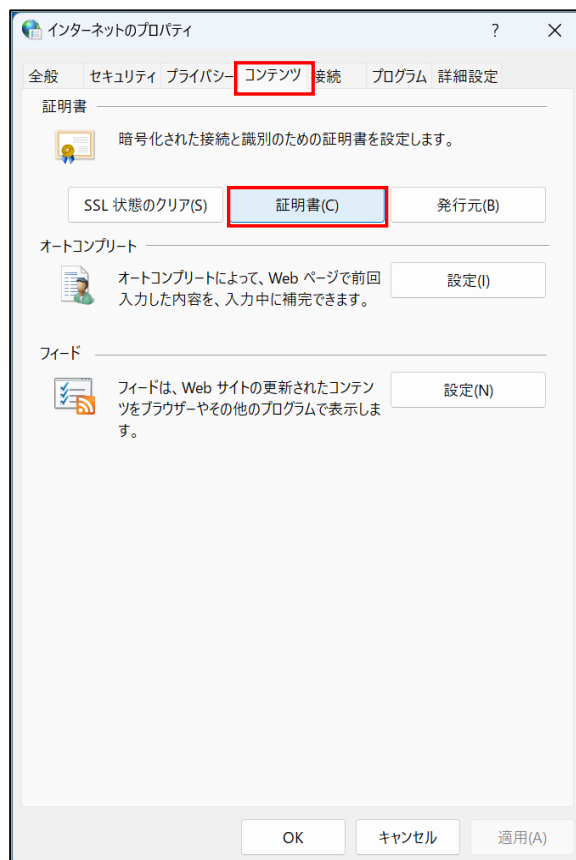
5. 証明書の確認方法

本章では、登録されている証明書を確認する方法を記載します。本手順で証明書が正しく登録されているか確認することができます。

- (1) Windows キーを押しながら R を押します。
- (2) ファイル名を指定して実行が起動します。名前の欄に「Inetcp1.cpl」と入力して「OK」をクリックします。



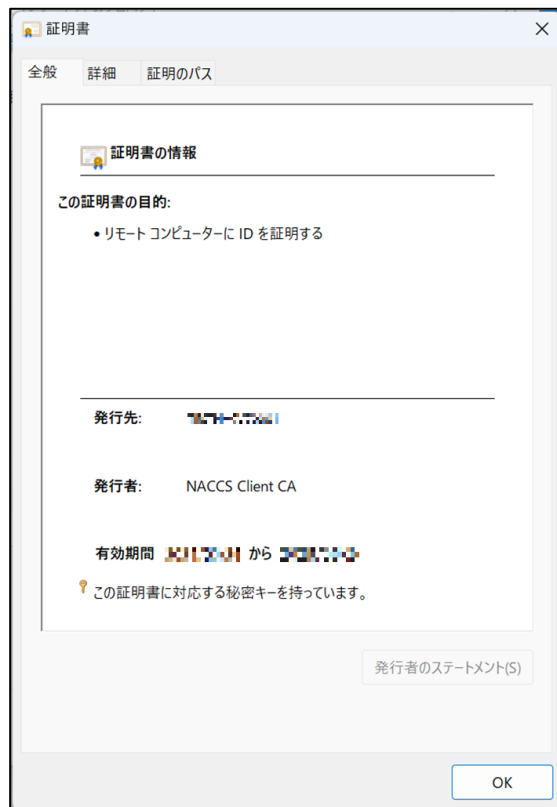
- (3) [コンテンツ] タブを開き、[証明書] をクリックします。



- (4) 以下の画面に、登録されている証明書が一覧で表示されます。本書に従いインストールした証明書は「個人」タブの証明書一覧の中の発行者が「NACCS Client CA」のものです。確認したい証明書を選択し、「表示」をクリックします（証明書をダブルクリックするでも可）。



- (5) 「証明書」が表示されます。



6. 証明書の更新手順

本章は、下記の「第7次 NACCS 用デジタル証明書」を更新する手順となります。

- ・第7次 NACCS 用デジタル証明書（クライアント証明書）
- ・第7次 NACCS 用デジタル証明書（ルート証明書）

<注>

以下の手順は、画面が実際と一部異なる場合があります。

6.1. 証明書の更新手順

- (1) ブラウザを起動し、以下の更新画面 URL にアクセスします。

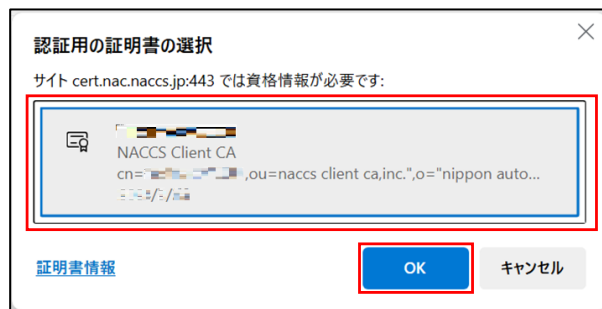
更新画面 URL

<https://cert.nac.naccs.jp/NACCSClientCA/pages/renew/index.jsp?s=Site1&lan=ja>

- (2) クライアント認証画面が表示されます。

<Microsoft Edge の場合>

「認証用の証明書の選択」画面から更新対象の証明書を選択し、「OK」をクリックします。

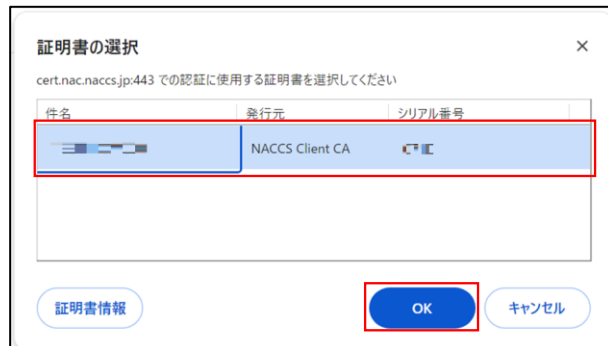


※ 更新対象の証明書を選択せずに「OK」ボタンをクリックしても認証は進みませんのでご注意ください。証明書が1つだけの場合であっても必ず対象をクリックし、証明書を選択した状態にしてから「OK」ボタンをクリックしてください。

※ 有効期限が切れている証明書は一覧の中には表示されません。

<Chrome の場合>

「認証用の選択」画面から更新対象の証明書を選択し、「OK」をクリックします。



※ 有効期限が切れている証明書は選択一覧の中に表示されません。

(3) 「NACCS デジタル証明書更新画面」が表示されます。



<セッションが無効になった場合の対応>

ログインした状態で一定時間作業を行わない場合、自動的にログアウトします。自動的にログアウトするとメニュー項目をクリックしてもセッションが無効であることを示す画面が表示され操作を続けることができません。このような状態になった場合、ログインしなおしてください。

※ 証明書の更新は、ユーザ証明書の有効期間終了日の 28 日前から可能です。これより前に証明書の更新を実施しようとしても更新できませんのでご注意ください。

- (4) 「NACCS デジタル証明書更新画面」のメニューから「デジタル証明書更新申請」をクリックします。



- (5) 「デジタル証明書更新申請情報の確認」が表示されます。申請の内容を確認し、「Submit」をクリックします。



- (6) 認証局での処理を待ちます。処理中は証明書ステータスが、鍵生成中→発行要求中→発行済みの順に遷移します。



- (7) 「デジタル証明書の取得」に自動的に遷移したら、「証明書パスワード」、「証明書パスワードの確認」を入力して「Submit」をクリックします。

なお、「証明書パスワード」とは、証明書ファイル（PKCS#12 形式）を暗号化し、端末へ登録する際に一時的に使用するためのもので、任意の文字列を指定してください。この後、手順「4. 証明書の登録手順（3）」で証明書をインポートする際に使用します。忘れないようご注意ください。

※ 証明書パスワードには半角英数字または記号を指定できます。8 桁以上のパスワード設定を推奨します。証明書パスワードの設定条件は以下のとおりとなります。

- ・ 半角英字は、大文字、小文字を区別します。
- ・ 記号は以下の 32 種類となります。
 ' ` - ! " # \$ % & () * , . / : ; ? @ [] ^ _ { | } ~ ¥ + < = > _)
- ・ 証明書パスワードを空白にすることはできません。
- ・ 文字数は、1 桁以上 16 桁以下となります。

※ 証明書パスワードを「4. 証明書の登録手順」までに忘れた場合は、再発行のお手続きが必要となり、新しい認証コード 3 にて再度「3. 1. 証明書の新規取得手順」から実施し直してください。

- (8) 「Download」をクリックします。

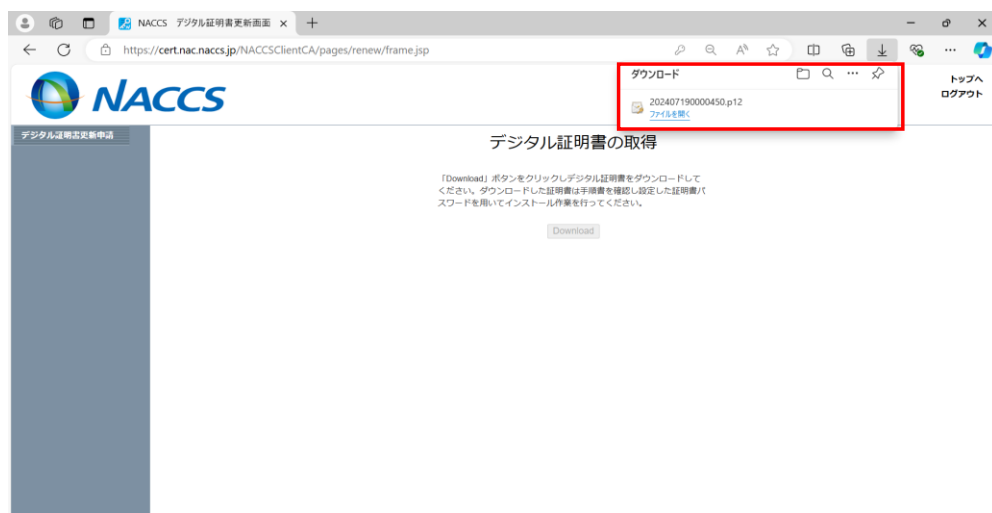


※ デジタル証明書の取得は、セキュリティ確保の目的から、最初取得した日の翌日からロックされ、再取得できなくなります。ご注意ください。

- (9) 証明書ファイル（年月日から始まる数字 15 桁＋ファイル拡張子 p12）がダウンロードされます。（ファイル名例：202501011234567.p12）

<Microsoft Edge の場合>

ウィンドウ右上部分に「ダウンロード」が表示されます。なお、一定時間経過後「ダウンロード」の表示は消えますが、メニューの設定「…」→「ダウンロード」から再度表示させることができます。



<Chrome の場合>

ウィンドウ右上部分にダウンロードした鍵・証明書ファイル名が表示されます。なお、一定時間経過後この表示は消えますが、メニューの「ダウンロード」アイコンをクリックすれば最近のダウンロード履歴を表示させることができます。



※ ダウンロードした鍵・証明書ファイル名の「ファイルを開く」をクリックします(ブラウザが Chrome の場合は、鍵・証明書ファイル名のところでクリックします)。

※ 証明書ファイル (PKCS#12 形式) の中に、第 7 次 NACCS 用クライアント証明書および秘密鍵、ルート証明書が入っています。ダウンロードしたファイルは「4. 証明書の登録手順」が終了するまで紛失しないようご注意ください。

- (10) 「証明書のインポートウィザードの開始」画面が表示されます。以降の手順は、「4. 証明書の登録手順」に進んでください。

なお、ダウンロードの表示が消えている場合であっても、エクスプローラでダウンロードフォルダを開き、該当のファイル名をダブルクリックすることでも「証明書のインポートウィザードの開始」画面が表示されます。

7. サポート情報

本章では「ご利用に当たっての注意事項」、「サービスメンテナンス」等を記載します。

7.1. ルート証明書の取得方法について

TLS 暗号化通信に必要なルート証明書の取得方法を記載します。

- (1) ブラウザを起動し、以下のルート証明書のダウンロード画面 URL にアクセスします。

ルート証明書のダウンロード画面 URL

<https://www.cybertrust.ne.jp/ssl/download-ca/sureserver-ov.html>

- (2) ルート証明書（コモンネーム：Security Communication RootCA2）のダウンロード「テキスト形式」リンクをクリックします。



cybertrust

企業認証(OV)証明書用 ルート・中間 CA 証明書 ダウンロード

SureServer Home

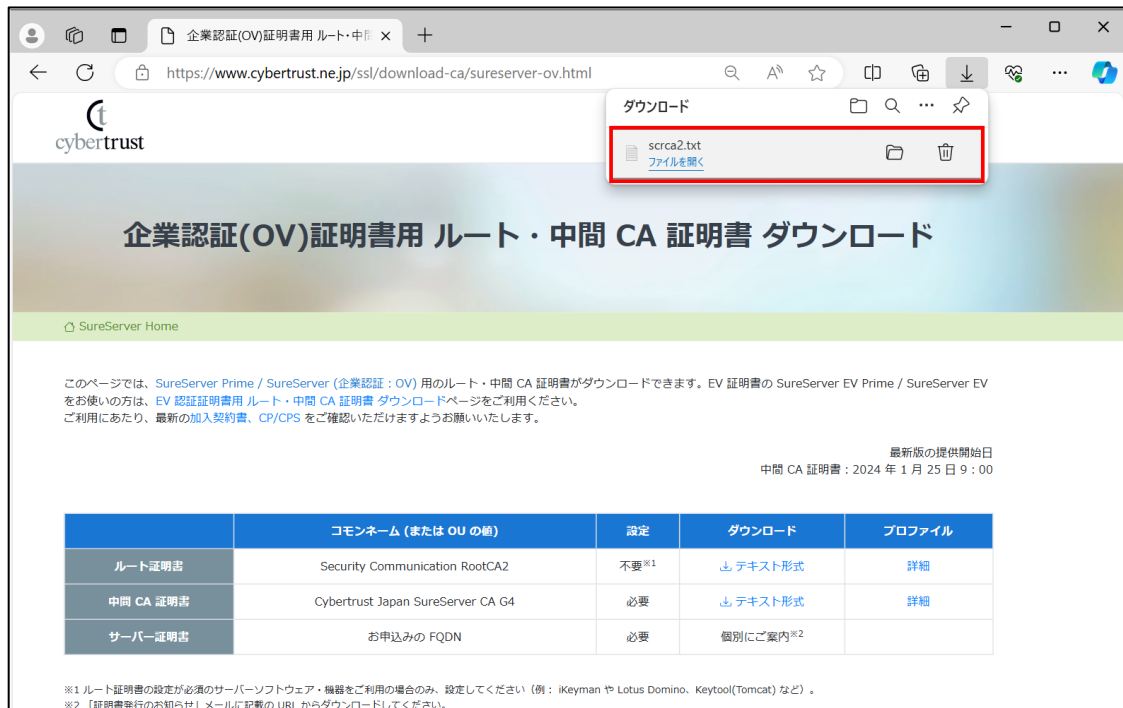
このページでは、SureServer Prime / SureServer (企業認証 : OV) 用のルート・中間 CA 証明書がダウンロードできます。EV 証明書の SureServer EV Prime / SureServer EV をお使いの方は、EV 認証証明書用 ルート・中間 CA 証明書 ダウンロードページをご利用ください。
ご利用にあたり、最新の加入契約書、CP/CPS をご確認くださいませようお願いします。

最新版の提供開始日
中間 CA 証明書 : 2024 年 1 月 25 日 9 : 00

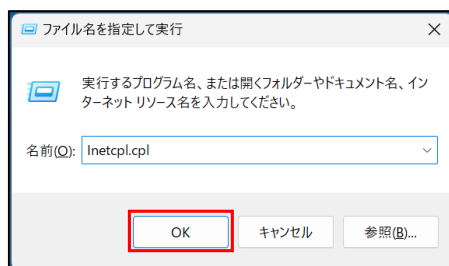
証明書の種類	コモンネーム (または OU の値)	設定	ダウンロード	プロフィール
ルート証明書	Security Communication RootCA2	不要※1	↓ テキスト形式	詳細
中間 CA 証明書	Cybertrust Japan SureServer CA G4	必要	↓ テキスト形式	詳細
サーバー証明書	お申込みの FQDN	必要	個別にご案内※2	

※1 ルート証明書の設定が必須のサーバーソフトウェア・機器をご利用の場合のみ、設定してください（例：iKeyman や Lotus Domino、Keytool(Tomcat) など）。
※2 「証明書発行のお知らせ」メールに記載の URL からダウンロードしてください。

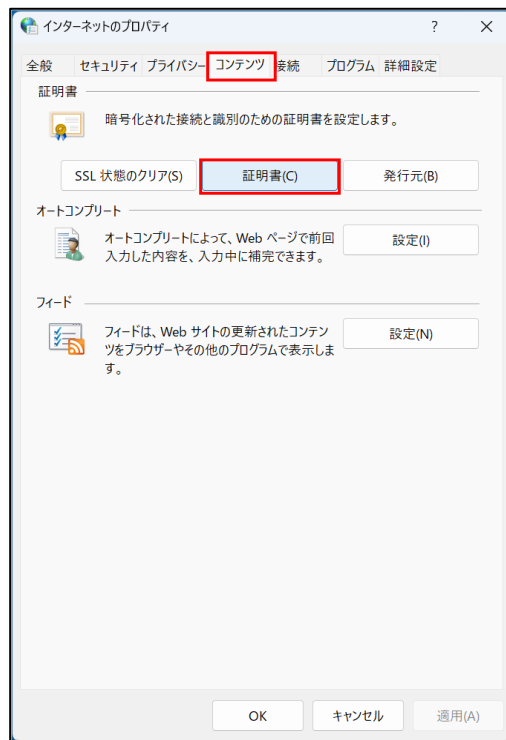
- (3) ルート証明書のテキストファイル(scrca2.txt) をダウンロードします。



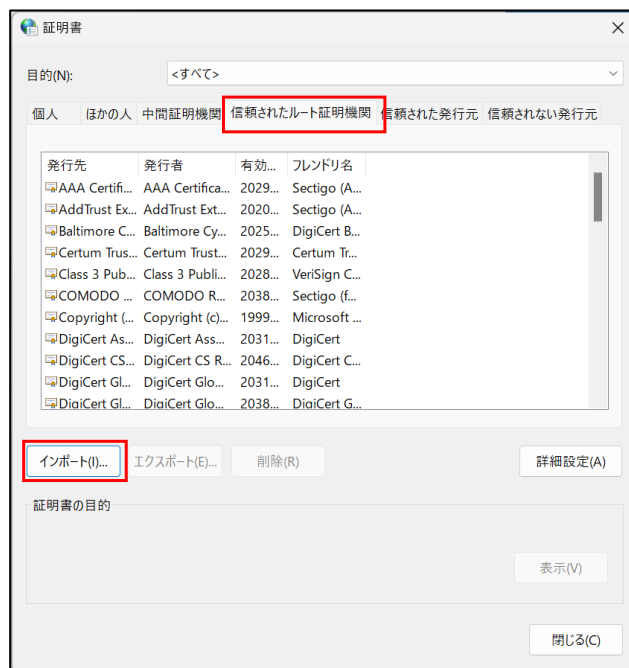
- (4) Windows キーを押しながら R を押します。
- (5) ファイル名を指定して実行が起動します。名前の欄に「Inetcp1.cpl」と入力して「OK」をクリックします。



- (6) 「コンテンツ」タブを開き、「証明書」をクリックします。



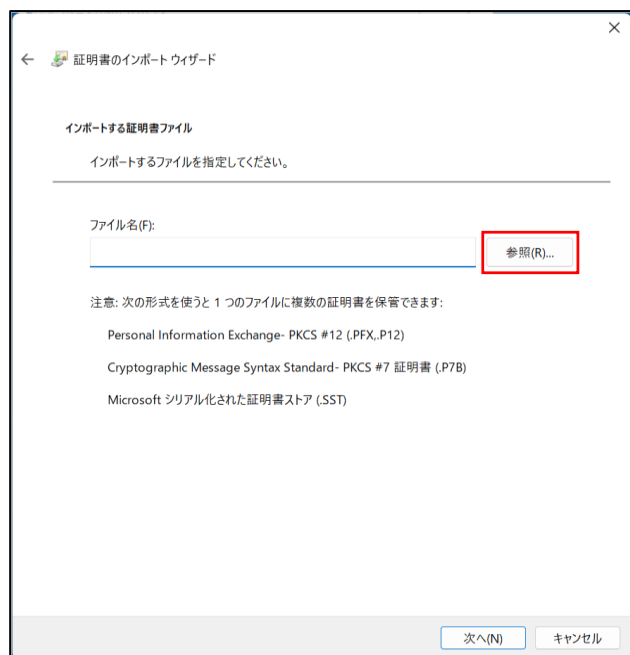
- (7) 「信頼されたルート証明書期間」タブを選択し、「インポート」をクリックします。



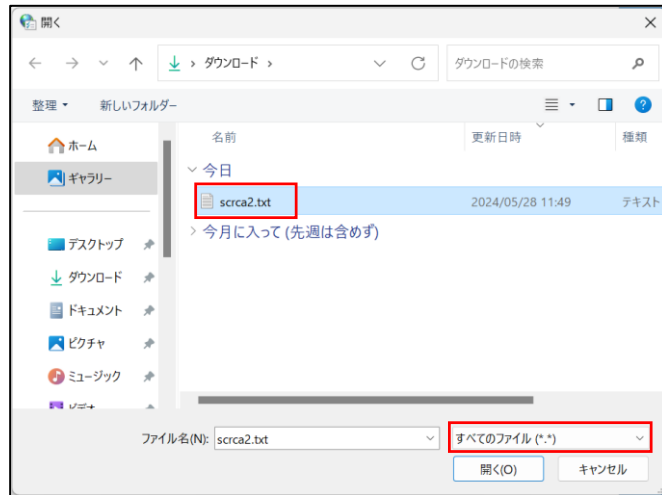
- (8) 「次へ」をクリックします。



- (9) 「参照」をクリックしてファイルを指定します。



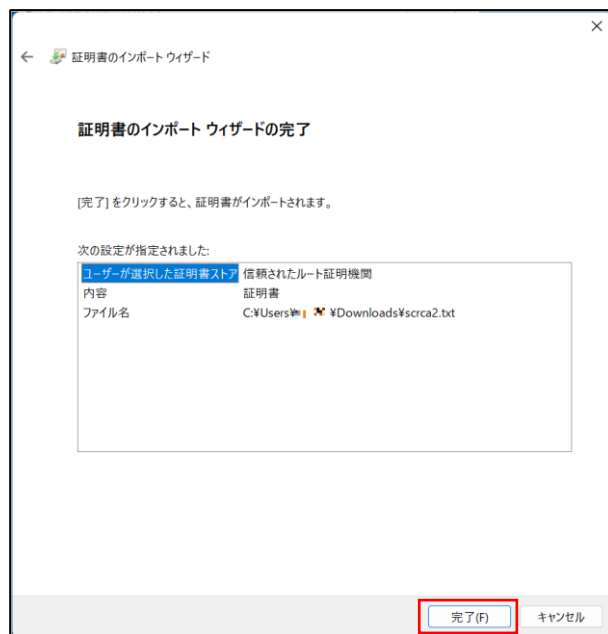
- (10) 指定する際には、ファイル拡張子を「すべてのファイル (*.*)」にして、手順 (3) でダウンロードしたテキストファイル(scrca2.txt)を選択ください。



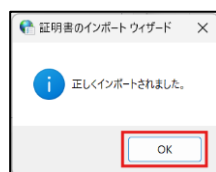
- (11) 「次へ」をクリックします。



(12) 「完了」をクリックします。



(13) 下記のダイアログが表示されれば完了です。「OK」をクリックします。



7.2. ご利用にあたっての注意事項

ご利用にあたりまして、以下のブラウザ操作は行わないでください。

- ・ ブラウザの「戻る」ボタン等を使ったページ遷移
- ・ 複数のウィンドウにまたがった作業

7.3. サービスメンテナンス

デジタル証明書発行／更新サービスの定期メンテナンスとして、月に1度定期停止日（原則、毎月第3火曜日(22:00～翌8:00)）があります。

メンテナンス時には、Web サイトへアクセスしたタイミングで以下の画面が表示されます。

