

「TDB 電子認証サービス Class2」よくある質問

2025 年 4 月 (v 11.0.0)

株式会社帝国データバンク

目次

1. Q&A : Class2 のサービス終了に関して.....	3
① サービス終了の理由を教えてください.....	3
② サービス終了のスケジュールを教えてください.....	3
③ 現在利用中の電子証明書への影響はありますか？.....	3
④ 2025 年 3 月 30 日までに証明書をダウンロードしなかった場合、どうなりますか？.....	3
⑤ 2025 年 3 月 31 日以降に再発行が必要になった場合はどのような対応になりますか？.....	3
⑥ バックアップの方法が知りたい.....	4
⑦ 後継サービスは用意されますか？.....	4
⑧ Class2 の有効期限後も電子証明書を利用したい.....	4
2. Q&A : Class2 について.....	5
① TDB Digicert 電子認証サービス Class2 の仕様を教えてください.....	5
② どのような用途に利用できますか？.....	5
③ どのような情報が証明書に格納されていますか？.....	5
④ 電子メールへの署名(S/MIME)に利用できますか？.....	6
⑤ プログラムへの電子署名に利用できますか？.....	6
⑥ VBA マクロへの電子署名に利用できますか？.....	6
⑦ 電子入札/電子申告(e-Tax/eLTAX)/電子申請(e-gov)に利用できますか？.....	6
3. Q&A : 証明書を取得 (ダウンロード) した後.....	7
① 証明書をダウンロードした後は何をすればいいですか？.....	7
② 「秘密キーのパスワードを入力してください」のパスワードは何を入力すればいいですか？.....	7
③ 電子証明書が正しく設定 (インポート) 出来ているか、確認する方法はありますか？.....	7
④ ダウンロードした証明書ファイルは削除しても構わないですか？.....	7
⑤ 名義人や組織名 (会社名) を変更できますか？.....	7
⑥ メールアドレスを変更できますか？.....	7
⑦ 本店所在地、申込担当者、電話番号、勤務先住所などを変更できますか？.....	7
⑧ 電子証明書ファイルをバックアップも含めて紛失しました.....	7
⑨ パソコンを変更する際の設定はどうすればいいですか？.....	8
⑩ 電子証明書を失効したい。利用を休止したい.....	8
⑪ 更新はどのように行いますか？.....	9
⑫ 名義人が退職したためファイルを紛失しました.....	9
⑬ 証明書ファイルのバックアップはどのようにしたらいいですか？.....	9
4. Q&A : 利用中.....	10
① 【ゲートウェイシステム】企業管理者登録申請で証明書を登録するとエラーになります.....	10

②	【ゲートウェイシステム】ログイン時のユーザーID、パスワードがわかりません.....	10
③	【ゲートウェイシステム】証明書の再発行後、ログインができなくなった	10
④	【ゲートウェイシステム】証明書の更新をしたあとはどうすればいいですか？	10
⑤	【Adobe Acrobat】取り込んでしまった証明書を削除したい.....	10
⑥	【Adobe Acrobat】署名検証で「完全性が不明です」というエラーになる	11
⑦	【Adobe Acrobat】電子署名の手順が知りたい.....	11
⑧	【e-Success】タイムスタンプ処理設定画面の電子証明書パスワードは何を入力しますか？	11
⑨	CRL（失効リスト）はどこで入手できますか？	11
5.	手順：電子証明書のインポート（Windows10/11）	12
6.	手順：電子証明書が正しく設定されているかの確認	15
7.	手順：証明書（秘密鍵）のエクスポート.....	17
8.	手順：公開鍵のエクスポート	22
9.	手順：不要な証明書の削除	26

改訂履歴

Rev	内容
1.0.0	初稿
7.0.0	全面リニューアル
8.0.0	エクスポート手順修正
9.0.0	インポート、インポート後確認の手順を追加、質問追加
9.1.0	質問追加
9.1.1	URL のリンク切れを修正
9.2.0	ダウンロード手順、質問を追加、URL のリンク切れを修正
9.2.1	誤字を修正
9.2.2	URL 修正
9.2.3	URL 修正
10.0.0	サービス終了についての項目を追加
10.1.0	申込み受付終了に伴う修正
11.0.0	ダウンロードや再発行の終了につき内容を修正

商標について

Windows および Microsoft Edge は Microsoft の商標または登録商標です。

Google chrome は Google の商標または登録商標です。

Adobe Acrobat はアドビ株式会社の商標または登録商標です。

e-Success はアンテナハウス株式会社の商標または登録商品です。

その他の社名、製品名は各社の商標または登録商標です。

1. Q&A : Class2 のサービス終了に関して

① サービス終了の理由を教えてください

電子証明書 Class2 の発行元であるデジサート・ジャパン合同会社、及び米国デジサート社の意向によります。詳しくは以下、デジサート社のお知らせをご確認ください。

<https://www.digicert.com/jp/pki/pki-class2-end-of-life-notification>

② サービス終了のスケジュールを教えてください

以下のスケジュールにてサービスを終了いたします。

なお、発行済の電子証明書は全て有効期限までご利用いただけますが、紛失された場合は再発行ができなくなります。

サービス終了前に必ず[バックアップ](#)のご用意をお願いいたします。

2025 年 2 月 28 日	お申込受付終了
2025 年 3 月 30 日	電子証明書のダウンロード、 および再発行申請受付の終了

③ 現在利用中の電子証明書への影響はありますか？

影響ありません。有効期間までご利用いただけます。またサポートも継続いたします。

ただし、2025 年 3 月 31 日以降は再発行が不可能となりますので、紛失等にはくれぐれもご注意ください。

④ 2025 年 3 月 30 日までに証明書をダウンロードしなかった場合、どうなりますか？

システムが停止するため、証明書のダウンロードが行えなくなります。

それまでにダウンロード操作を行って頂くよう、お願いいたします。

⑤ 2025 年 3 月 31 日以降に再発行が必要になった場合はどのような対応になりますか？

原則再発行不可となりますが、**以下 3 つの条件を満たせる**場合は代替証明書を提供できる場合がございますので電子認証局ヘルプデスクまでご連絡ください。条件を満たせない場合はご提供不可となります。

条件① メールアドレスのドメインが自社ドメインである

条件② メールアドレスがグループアドレス個人のものである

条件③ 法人である

⑥ バックアップの方法が知りたい

以下に手順書をご用意いたしましたのでご確認ください。

https://www.tdb.co.jp/typeA/support/pdf/class2_bkup.pdf

⑦ 後継サービスは用意されますか？

デジサート社にてリリースを予定しております。詳しくは以下をご参照ください。

<https://www.digicert.com/jp/pki/pki-class2-introducing-successor>

なお、弊社帝国データバンクでの取り扱いはございません。

⑧ Class2 の有効期限後も電子証明書を利用したい

他社電子証明書や代替サービスへの移行をご検討ください。

利用用途	移行先候補
電子契約	弊社 IC カード TypeA、デジサート社後継証明書、 他社電子証明書、電子契約サービスへの移行
WEB サイトへのアクセスコントロール (クライアント認証)	・デジサート社や他社製 Private 証明書への移行
厚生労働省ゲートウェイシステム	厚生労働省が推奨する他社電子証明書
設計図書の電子保存	他社電子証明書への移行
不動産鑑定評価書への電子署名	日本不動産鑑定士協会連合会様が 推奨する電子証明書への移行
アンテナハウス株式会社	アンテナハウス株式会社が推奨する
電子文書管理システム「e-Success」	電子証明書への移行
日鉄ソリューションズ株式会社	日鉄ソリューションズ株式会社が推奨する
電子契約サービス「CONTRACTHUB」	電子証明書への移行
クーポンを利用して申請されているお客さま	クーポンをご購入されている代理店様へご相談ください。

2. Q&A : Class2 について

① TDB Digicert 電子認証サービス Class2 の仕様を教えてください

以下になります。

ファイル形式	PKCS#12(p12)
X509 バージョン	V3
署名アルゴリズム	SHA256RSA
公開鍵アルゴリズム	RSA(2048bit)
有効期間	760 日(2 年+1 か月)
CRL 更新周期	24 時間毎

② どのような用途に利用できますか？

以下の用途にご利用いただけます。

- ・電子文書(PDF)への電子署名
- ・WEB サイトへのアクセスコントロール（クライアント認証）
- ・不動産鑑定評価書への電子署名
- ・以下を含めた厚生労働省ゲートウェイシステムの利用
 - ・厚生労働省「医薬品医療機器申請・審査システム」に関する届出等のオンライン提出(FD 申請)
 - ・独立行政法人医薬品医療機器総合機構（PMDA）に対する ICSR 受付サイト及び EDI ツールを介した医薬品等の治験及び市販後副作用等報告の提出

③ どのような情報が証明書に格納されていますか？

以下の情報が格納されています。格納情報を発行後に変更することはできません。

- ・組織名（日本語&ローマ字）
- ・名義人氏名（日本語&ローマ字）
- ・メールアドレス
- ・TDB 企業コード

以下は通常は格納されず、特別にご希望頂いた場合のみ格納されています。

- ・英文役職 *日本語役職は格納されません
- ・建築士資格番号

④ 電子メールへの署名(S/MIME)に利用できますか？

ご利用いただけません。

⑤ プログラムへの電子署名に利用できますか？

ご利用いただけません。

⑥ VBA マクロへの電子署名に利用できますか？

ご利用いただけません。

⑦ 電子入札/電子申告(e-Tax/eLTAX)/電子申請(e-gov)に利用できますか？

ご利用いただけません。

「TDB 電子認証サービス TypeA (<https://www.tdb.co.jp/typeA>) 」をご利用ください。

3. Q&A：証明書を取得（ダウンロード）した後

① 証明書をダウンロードした後は何をすればいいですか？

証明書のファイルを開き、**電子証明書のインポート**を行ってください。
インポート後の設定は各利用先にご確認ください。

② 「秘密キーのパスワードを入力してください」のパスワードは何を入力すればいいですか？

申込書に記載頂いた**申請パスワード（秘密キー）**をご入力ください。

③ 電子証明書が正しく設定（インポート）出来ているか、確認する方法はありますか？

Windows の証明書ストアにて確認が可能です。
詳しくは P15 の手順をご確認ください。
インポート後は利用先ごとの手順を実施ください。

④ ダウンロードした証明書ファイルは削除しても構わないですか？

パソコン変更や故障で再度インポートが必要になる場合がございます。
削除せずに、バックアップとして大切に保管してください。

⑤ 名義人や組織名（会社名）を変更できますか？

名義人と会社名は発行時に認証を行っている情報のため、変更することが出来かねます。
なお、名義人退職に伴う場合、または組織名変更の場合は失効申請が必要になります。

⑥ メールアドレスを変更できますか？

サービス終了に伴う電子証明書発行システムの停止により、2025 年 3 月 31 日以降は変更出来かねます。

⑦ 本店所在地、申込担当者、電話番号、勤務先住所などを変更できますか？

これらの情報は証明書に格納されていない情報のため、変更手続きは不要です。
変更のご連絡も必要ございません。

⑧ 電子証明書ファイルをバックアップも含めて紛失しました

原則再発行不可となりますが、**以下 3 つの条件を満たせる**場合は代替証明書を提供できる場合がございますので
電子認証局ヘルプデスクまでご連絡ください。条件を満たせない場合はご提供不可となります。

条件① メールアドレスのドメインが自社ドメインである

条件② メールアドレスがグループアドレス個人のものである

条件③ 法人である

⑨ パソコンを変更する際の設定はどうすればいいですか？

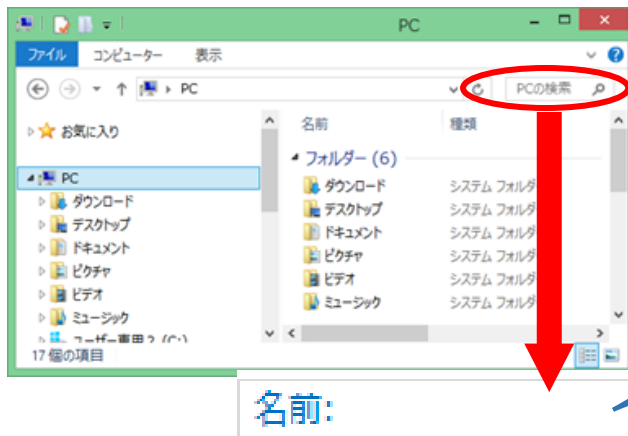
古いパソコンやバックアップから新しいパソコンへ電子証明書をコピーした後、インポートして利用用途別の設定に従ってください。

古いパソコンでのファイル検索手順は以下のとおりです。

から証明書ファイルクアップが見当たらない場合は以下の方法で検索を行い、見つからなければエクスポート(P17)を行ってください。

【検索手順】

1. キーボードの[Windows]キーを押しながら[E]キーを押します。
2. 右上の検索ボックスに「名前:.p12」と入力します。



⑩ 電子証明書を失効したい。利用を休止したい

電子認証局ヘルプデスク (certinfo@mail.tdb.co.jp) まで

以下 3 つの情報をご連絡頂く事で承っております。

なお、失効完了後の取り消しは出来かねますので、くれぐれもご注意ください。

- (1) 「名義人氏名」
- (2) 「登録メールアドレス」
- (3) 電子証明書の「シリアル番号」または 発行時のメールに記載されている「証明書コード」

【シリアル番号確認方法】

1. キーボードの[Windows]キーを押しながら[R]キーを押します。
「ファイル名を指定して実行」が立ち上がりますので「inetcppl.cpl」と入力し、OK を押します。
2. インターネットオプション」が立ち上がります。
[コンテンツ]の[証明書]を開きます。
3. 当該の証明書をWクリックし、[詳細]の[シリアル番号]をご確認ください。

⑪ **更新**はどのように行いますか？

Class2 は 2025 年 2 月 28 日をもって新規のお申込み受付を終了いたしました。
各利用先が推奨する別の証明書やサービスへの以降をお願いいたします。

⑫ **名義人が退職したためファイルを紛失**しました

名義人が退職された場合、該当の電子証明書を利用し続けることはご遠慮ください。
退職された方の電子証明書の失効申請をお願いいたします。⇒Q&A 項目 3-⑨

⑬ **証明書ファイルのバックアップ**はどのようにしたらいいですか？

以下、バックアップ手順書をご確認ください。
https://www.tdb.co.jp/typeA/support/pdf/class2_bkup.pdf

4. Q&A：利用中

① 【ゲートウェイシステム】企業管理者登録申請で証明書を登録するとエラーになります

ゲートウェイシステムに登録する証明書は秘密鍵(.p12)ではなく公開鍵(.cer)になります。

「10. 公開鍵のエクスポート手順」(P22)をご参考ください。

② 【ゲートウェイシステム】ログイン時のユーザーID、パスワードがわかりません

弊社で管理している情報ではないため、PMDA 様にご確認ください。

③ 【ゲートウェイシステム】証明書の再発行後、ログインができなくなった

再発行を行うと旧証明書が失効されるため、申請電子データシステムへのログインができなくなります。

申請電子データシステム（ゲートウェイシステム）の「企業管理者」、または「企業ユーザー管理者」に、当該ユーザーを削除し、再度新たなユーザーとして登録し直すことをご依頼ください。また、その際にご登録頂く公開鍵は再発行で取得した新しい電子証明書からエクスポートした公開鍵になります。

エクスポート手順につきましては、「7. 公開鍵のエクスポート手順」(P22)をご参考ください。

④ 【ゲートウェイシステム】証明書の更新をしたあとはどうすればいいですか？

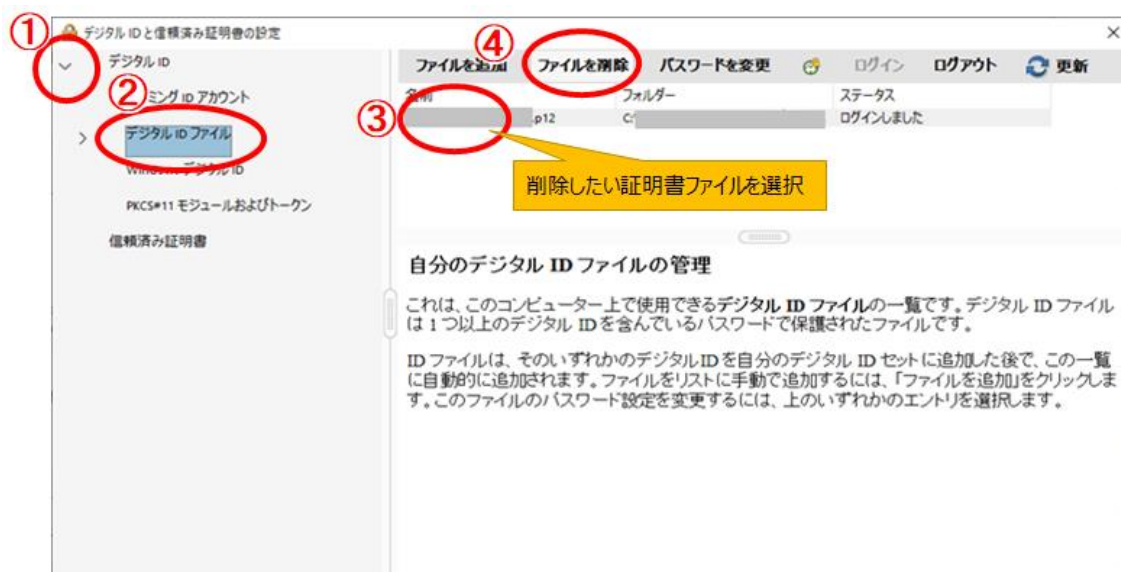
旧証明書の有効期限が切れる前に申請電子データシステム（ゲートウェイシステム）へログインし、「個人証明書変更」にて更新後の証明書からエクスポートした公開鍵をご登録ください。

エクスポート手順につきましては、「7. 公開鍵のエクスポート手順」(P22)をご参考ください。

⑤ 【Adobe Acrobat】取り込んでしまった証明書を削除したい

[編集]-[環境設定]-[署名]-[ID と信頼済み証明書]を開きます。

以降は下記画像通りに削除を行ってください。



⑥ 【Adobe Acrobat】署名検証で「完全性が不明です」というエラーになる

AdobeAcrobat で署名検証を成功させるには、以下 2 つの条件を満たす必要があります。

1. パソコンに Class2 自体か、Class2 の中間 CA がインポートされていること
2. Windows 統合設定を行うこと

【解決方法】

1. Class2 の中間 CA は以下リポジトリから入手可能です。
入手した CA ファイルを右クリックし、**証明書のインポート**を実行ください。
・**中間 CA 証明書(Individual Certificate Issuance Service CA)**
<https://knowledge.digicert.com/ja/jp/solution/SOT0048>
2. 以下手順で Windows 統合設定を行ってください。
 - ① AdobeAcrobatReader を起動し、[編集]-[環境設定]-[一般]を開きます。
 - ② [署名]を選択し、[検証]の[詳細]を開きます。
 - ③ ウィンドウ下部の **Windows 統合**欄の **以下 2 項目**にチェックをつけ、**OK** をクリックします。
 - ・「署名を検証」
 - ・「証明済み文書を検証」

なお、AdobeAcrobat の操作、仕様に関するご質問は、提供元へご相談ください。

⑦ 【Adobe Acrobat】電子署名の手順が知りたい

以下手順書をご用意しておりますのでご参照ください。

https://www.tdb.co.jp/typeA/support/pdf/adobeacrobat_manual.pdf

なお、当手順書の内容に関するサポートは承っておりません。予めご了承ください。

⑧ 【e-Success】タイムスタンプ処理設定画面の電子証明書パスワードは何を入力しますか？

申込書に記入頂いた「申請パスワード（秘密キー）」をご入力ください。

⑨ CRL（失効リスト）はどこで入手できますか？

CRL（失効リスト）の配布ポイント(CRL Distribution Point)は以下になります。

https でアクセスするとエラーになりますのでご注意ください。

http://pki-crl.symauth.com/ca_0ae7dba2f378c9db5b4e41a029c73d38/LatestCRL.crl

5. 手順：電子証明書のインポート（Windows10/11）

Windows10/11 で電子証明書をインポートする際の手順です。

Windows8.1 以下については以下（デジサート社ナレッジ）をご参照ください。

<https://knowledge.digicert.com/ja/jp/solution/SO23695.html>

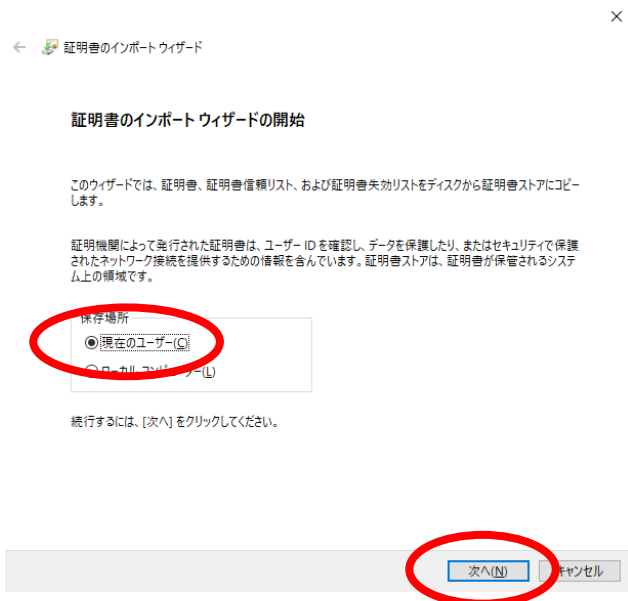
【手順】

- ① ダウンロードした電子証明書のファイル
(cert.p12) をダブルクリックします。
※拡張子 (.p12) はパソコンの設定により非表示の場合
もあります。



- ② 証明書のインポートウィザードが表示されます。

現在のユーザーにチェックをつけて次へをクリックしてください。



- ③ インポートするファイル名を指定する画面が表示されます。**次へ** をクリックします。

← 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(E):

C:\Users#\Downloads\cert.p12

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)

次へ(N)

キャンセル

- ④ 秘密キーのパスワードを入力する画面が表示されます。

申込書に記入頂いた申請パスワード(秘密キー)を入力し、

このキーをエクスポート可能にする

と

全ての拡張プロパティを含めるにチェックをつけ、

次へ をクリックします。

← 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)

こ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

- ⑤ 証明書ストアの画面が表示されます。

証明書の種類に基づいて、自動的に証明書ストア

を選択するが選択されていることを確認し、**次へ**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(M)

☐ 証明書をすべて次のストアに配置する(P)

証明書ストア:

参照(R)...

次へ(N)

キャンセル

- ⑥ インポートウィザードの完了画面が表示されます。

完了をクリックします。

← 証明書のインポートウィザード

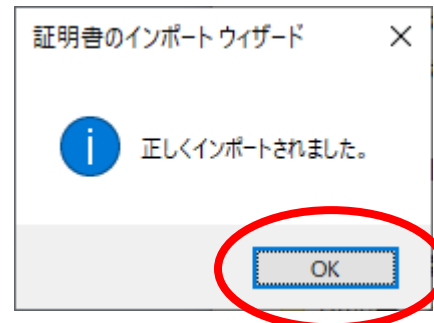
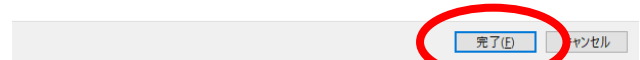
証明書のインポートウィザードの完了

[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

選択された証明書ストア	ウィザードで自動的に決定されます
内容	PFX
ファイル名	C:\Users\1200136\Desktop\デスクトップ整理\大鹿bu\Makoto Ohshika(20

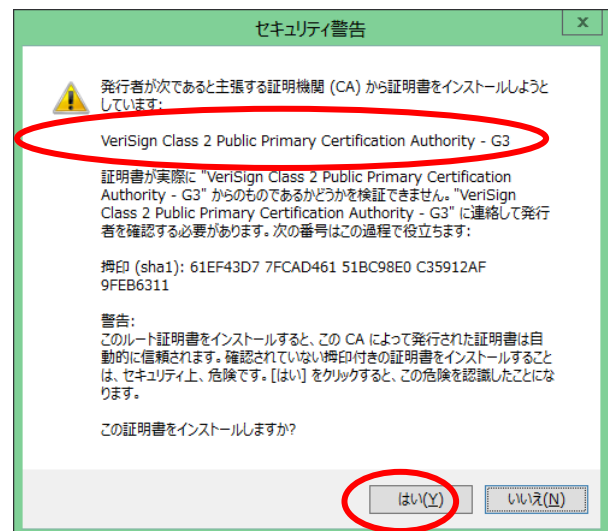
- ⑦ 正しくインポートされました。
と表示されましたら OK を押します。
これで完了です。



■ポイント■

Class2 を初めてインポートした端末では、
セキュリティ警告が表示されます。

証明機関の名称（画像赤枠部分）が
Individual Certificate Issuance Service CA
と記載されていることを確認して
はいをクリックしてください。



以上

6. 手順：電子証明書が正しく設定されているかの確認

電子証明書がパソコンに正しくインポートされているかを確認する場合の手順です。

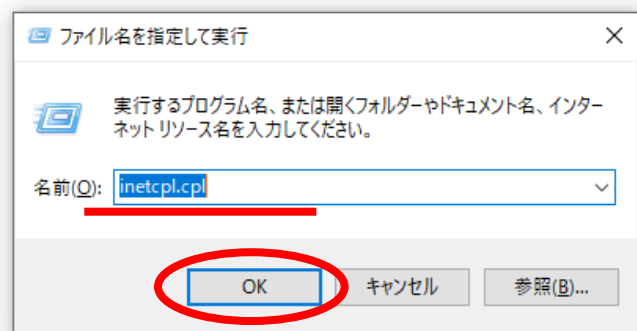
【手順】

- ① キーボードの[Windows]キーを押しながら[R]キーを押します。



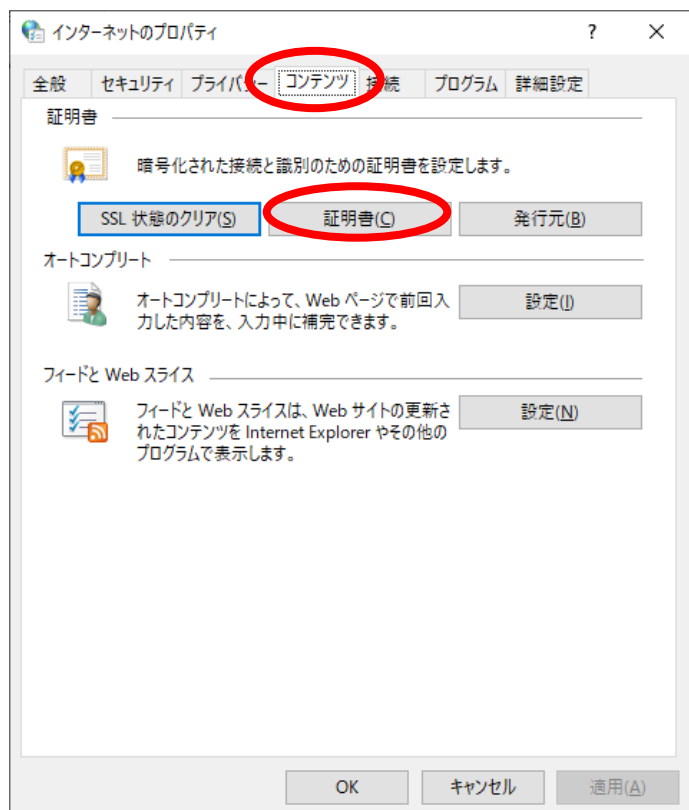
- ② ファイル名を指定して実行が立ち上がります。
名前に以下を入力し、OKを押します。

「 **inetcpl.cpl** 」



- ③ インターネットのプロパティが表示されます。

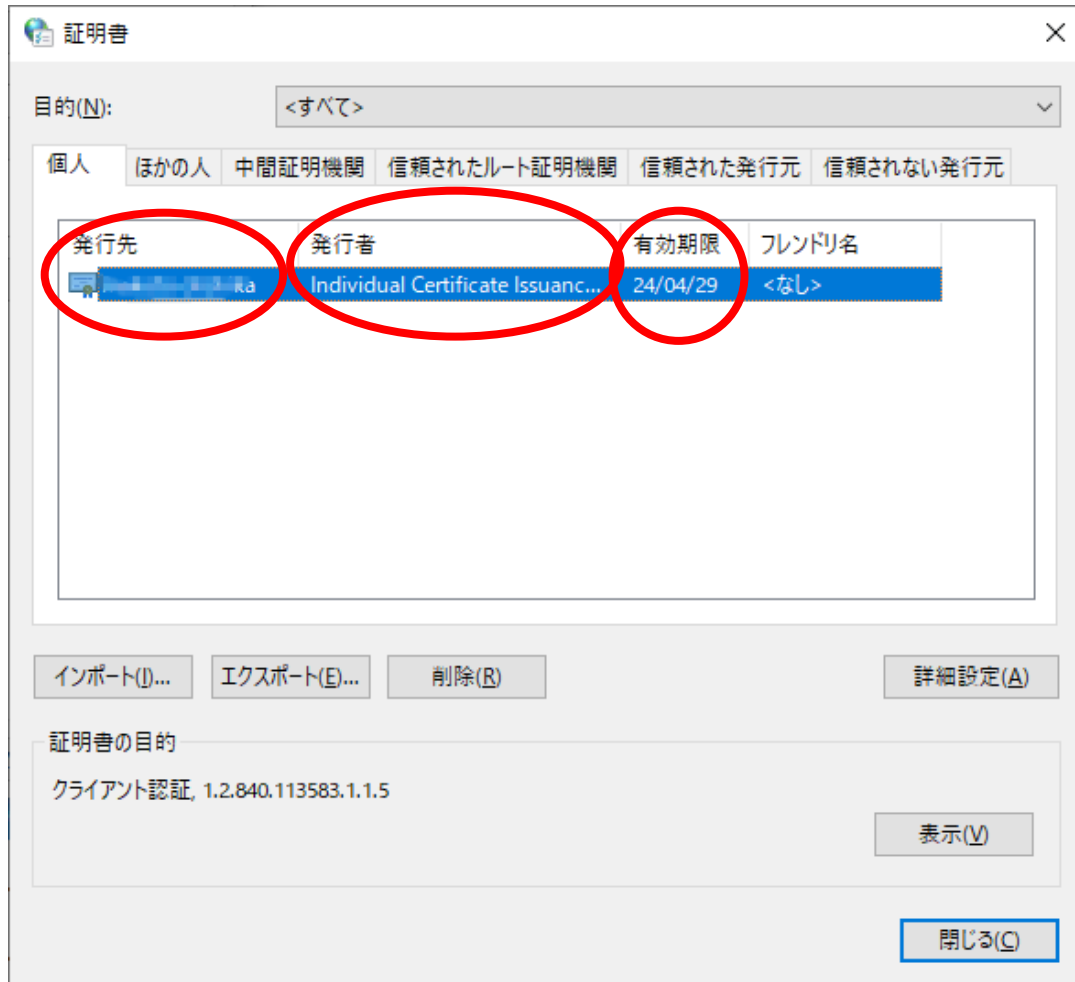
コンテンツタブの証明書をクリックします。



④ 証明書の一覧が表示されます。

このうち、発行者が「Individual Certificate Issuance Service CA」となっているものが電子証明書 Class2 です。

発行先（名義人の名前）や有効期限を確認し、間違いなければ正しくインポートが来ています。



以上

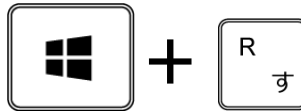
7. 手順：証明書（秘密鍵）のエクスポート

証明書をエクスポートする場合の手順です。

公開鍵(cer)をエクスポートする場合は「公開鍵のエクスポート手順」(P22)をご参考ください。

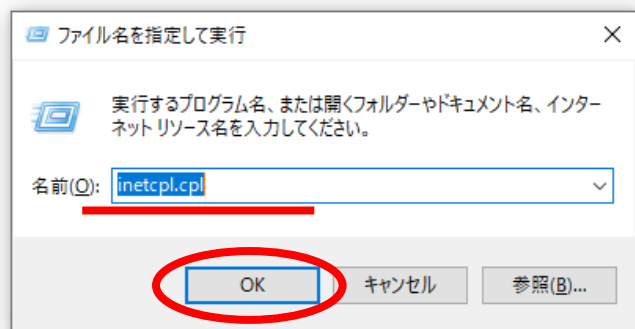
【手順】

- ① キーボードの[Windows]キーを押しながら[R]キーを押します。



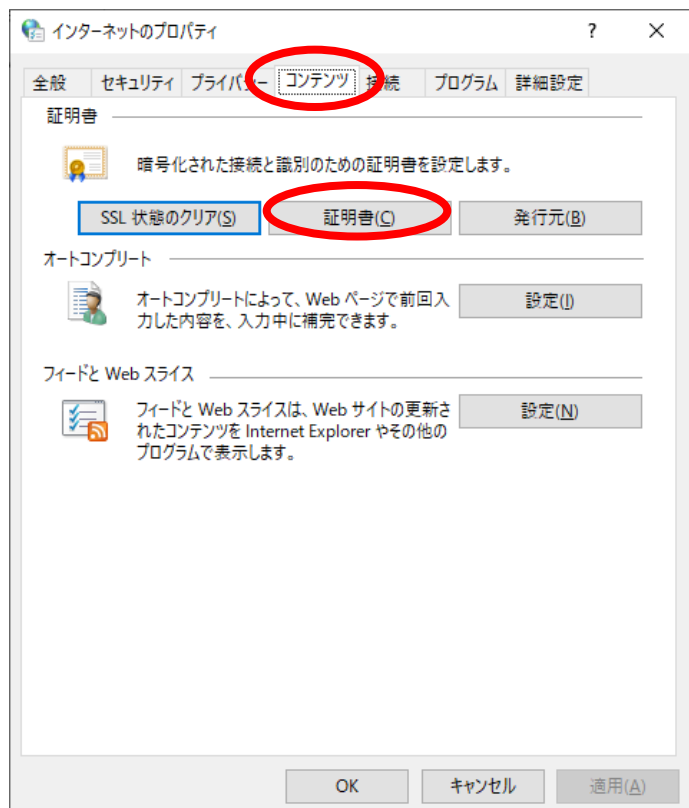
- ② ファイル名を指定して実行が立ち上がります。
名前に以下を入力し、OKを押します。

「 **inetcpl.cpl** 」



- ③ インターネットのプロパティが表示されます。

コンテンツタブの証明書をクリックします。



- ④ エクスポートしたい電子証明書をクリックし、エクスポートをクリックします。

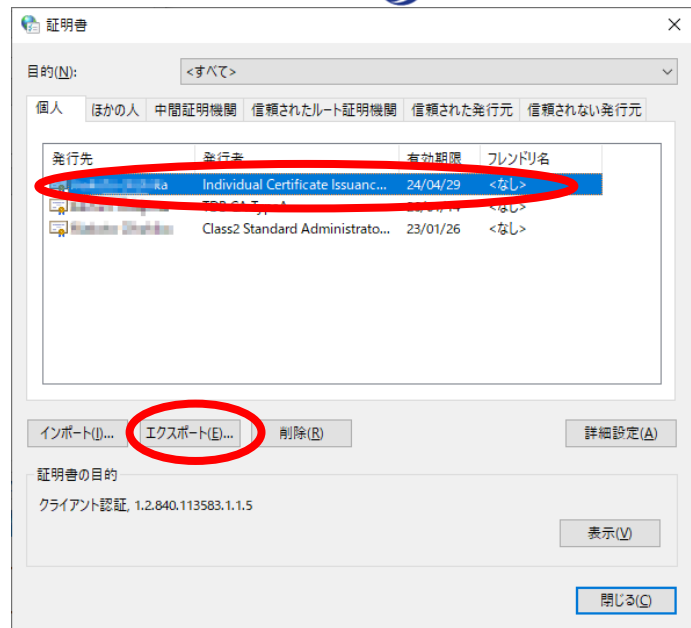
* 一覧に電子証明書が複数登録されている場合は、有効期限や発行者で正しいものを選びください。

* 電子証明書 Class2 は『発行者』が以下となっています。

「Individual Certificate Issuance Service CA」

(有効期限が 23/12/6 以前の場合は「Class2～」です。)

- ⑤ 次へをクリックします。



← 証明書のエクスポートウィザード

証明書のエクスポートウィザードの開始

このウィザードでは、証明書、証明書信頼リストおよび証明書失効リストを証明書ストアからディスクにコピーします。

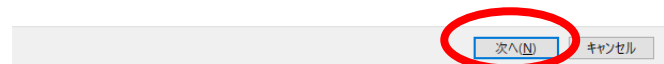
証明機関によって発行された証明書は、ユーザー ID を確認し、データを保護したり、またはセキュリティで保護されたネットワーク接続を提供するための情報を含んでいます。証明書ストアは、証明書が保管されるシステム上の領域です。

続行するには、[次へ] をクリックしてください。

- ⑥ はい、秘密キーをエクスポートしますにチェックをつけて、次へをクリックします。

■ここで「はい」が選べない場合

インポート時の設定によりエクスポートは不可となります。



← 証明書のエクスポートウィザード

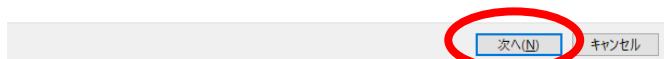
秘密キーのエクスポート

秘密キーを証明書と一緒にエクスポートすることができます。

秘密キーはパスワードで保護されています。秘密キーを証明書と一緒にエクスポートする場合は、パスワードを入力する必要があります。

証明書と一緒に秘密キーをエクスポートしますか?

- ☒ はい、秘密キーをエクスポートします(Y)
☐ いいえ、秘密キーをエクスポートしません(Q)



- ⑦
- ・証明のパスにある証明書を可能であればすべて含む
 - ・すべての拡張プロパティをエクスポートする
 - ・証明書のプライバシーを有効にする*

(*windows10 以降)

にチェックをつけ、次へをクリックします。

← 証明書のエクスポートウィザード ×

エクスポート ファイルの形式
さまざまなファイル形式で証明書をエクスポートできます。

使用する形式を選択してください

☐ DER encoded binary X.509 (.CER)(D)
☐ Base 64 encoded X.509 (.CER)(S)
☐ Cryptographic Message Syntax Standard - PKCS #7 証明書 (.P7B)(Q)
☐ 証明のパスにある証明書を可能であればすべて含む(I)
☒ Personal Information Exchange - PKCS #12 (.PFX)(P)
☒ 証明のパスにある証明書を可能であればすべて含む(U)
☐ 正しくエクスポートされたときは秘密キーを削除する(K)
☒ すべての拡張プロパティをエクスポートする(A)
☒ 証明書のプライバシーを有効にする(E)
☐ Microsoft シリアル化された証明書ストア (.SST)(I)

次へ(N) キャンセル

- ⑧
- パスワードにチェックをつけて、任意のパスワードを入力し、次へをクリックします。

← 証明書のエクスポートウィザード ×

セキュリティ
セキュリティを維持するために、セキュリティプリンスパルで秘密キーを保護する必要があります。

☐ グループまたはユーザー名 (推奨)(G)

パスワード(P):
●●●●●●

パスワードの確認(C):
●●●●●●

暗号化: TripleDES-SHA1

次へ(N) キャンセル

- ⑨
- 参照をクリックします。

← 証明書のエクスポートウィザード ×

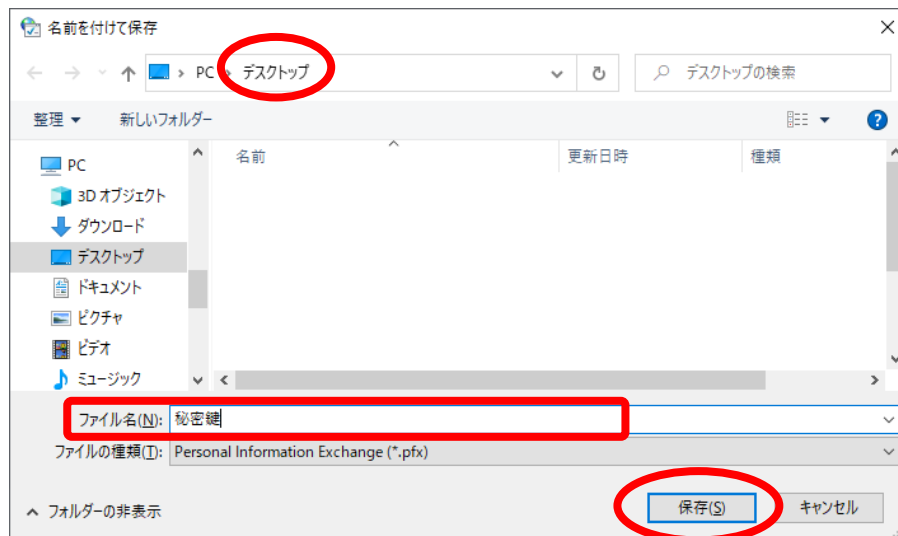
エクスポートするファイル
エクスポートするファイルの名前を入力してください

ファイル名(F):
|

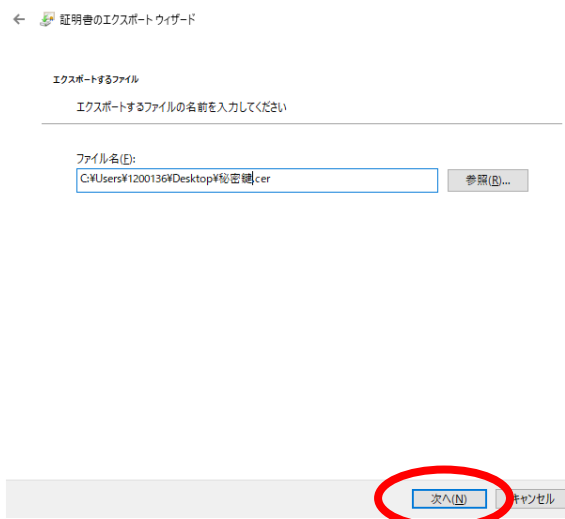
参照(R)...

次へ(N) キャンセル

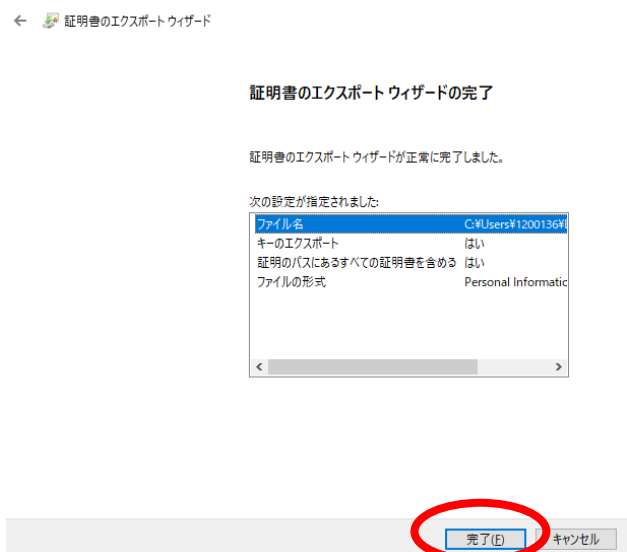
- ⑩ 保存場所がデスクトップになっている事を確認し、ファイル名を入力して保存をクリックします。
(画像では例としてファイル名を「秘密鍵」としています。)



- ⑪ 次へをクリックします。

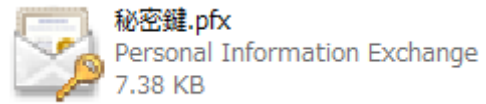
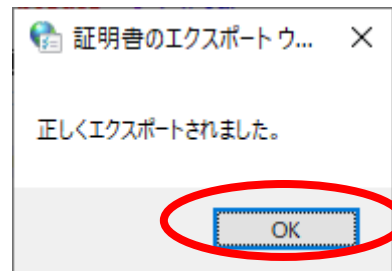


- ⑫ 完了をクリックします。



⑬ OK をクリックします。

デスクトップに⑩で設定したファイル名で証明書がエクスポートされています。



以上

8. 手順：公開鍵のエクスポート

公開鍵(cer)をエクスポートする際の手順です。

証明書自体(秘密鍵を含む、pfx)をエクスポートする場合は「秘密鍵のエクスポート手順」(P17)をご参考ください。

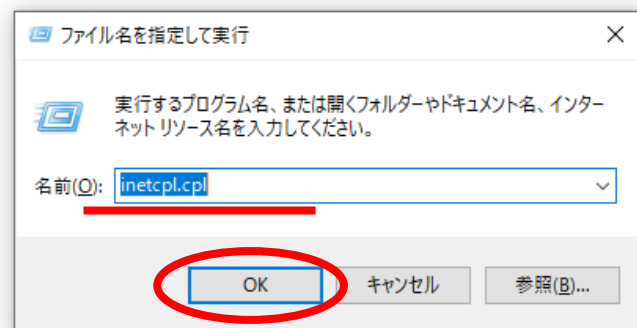
【手順】

- ① キーボードの[Windows]キーを押しながら[R]キーを押します。



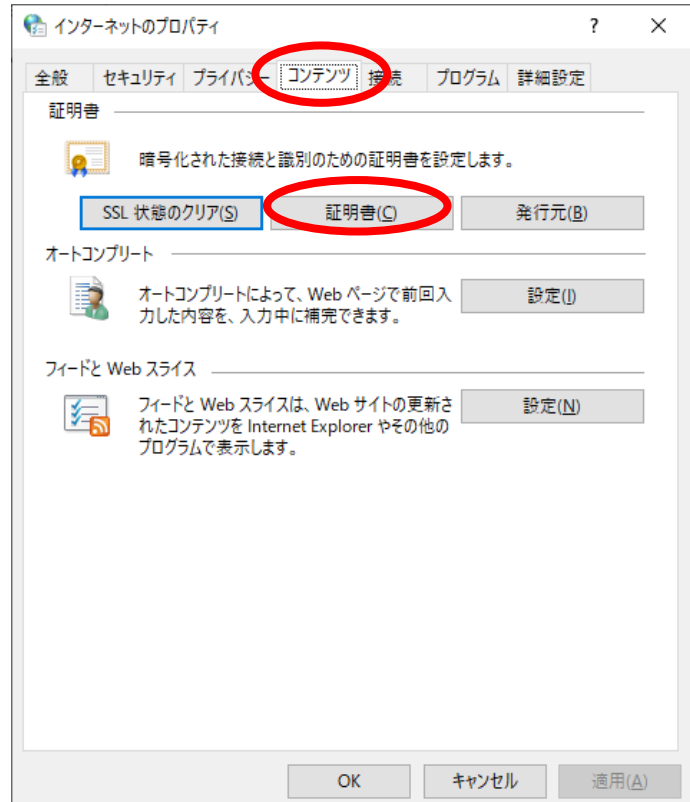
- ② ファイル名を指定して実行が立ち上がります。
名前に以下を入力し、OKを押します。

「 **inetcpl.cpl** 」



- ③ インターネットのプロパティが立ち上がります。

コンテンツタブの証明書をクリックします。



- ④ 公開鍵を作りたい電子証明書をクリックし、エクスポートをクリックします。

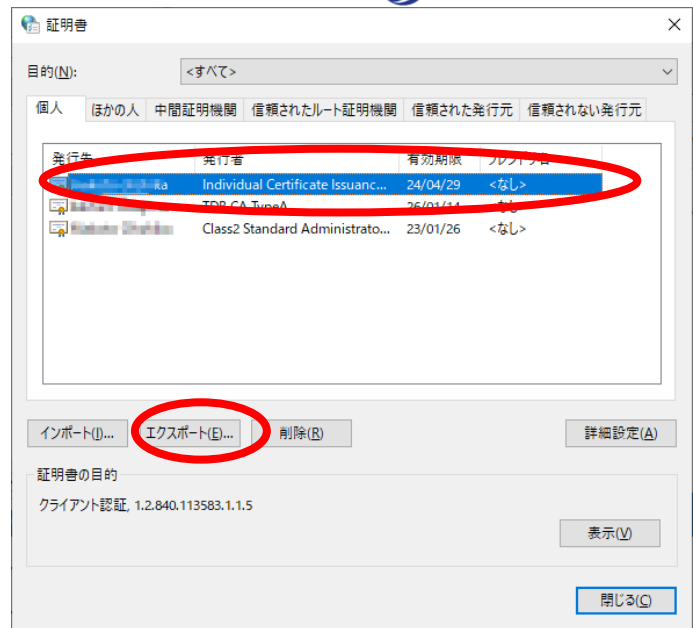
* 一覧に電子証明書が複数登録されている場合は、有効期限や発行者で正しいものを選びください。

* 電子証明書 Class2 は『発行者』が以下となっています。

「Individual Certificate Issuance Service CA」

(有効期限が 23/12/6 以前の場合は「Class2～」です。)

- ⑤ 次へをクリックします。



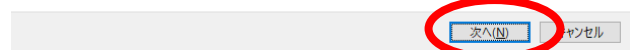
← 証明書のエクスポートウィザード

証明書のエクスポートウィザードの開始

このウィザードでは、証明書、証明書信頼リストおよび証明書失効リストを証明書ストアからディスクにコピーします。

証明機関によって発行された証明書は、ユーザー ID を確認し、データを保護したり、またはセキュリティで保護されたネットワーク接続を提供するための情報を含んでいます。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。

続けるには、[次へ] をクリックしてください。



- ⑥ いいえ、秘密キーをエクスポートしませんにチェックをつけて、次へをクリックします。

← 証明書のエクスポートウィザード

秘密キーのエクスポート

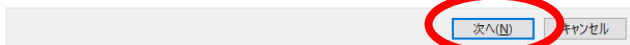
秘密キーを証明書と一緒にエクスポートすることができます。

秘密キーはパスワードで保護されています。秘密キーを証明書と一緒にエクスポートする場合は、パスワードを入力する必要があります。

証明書と一緒に秘密キーをエクスポートしますか？

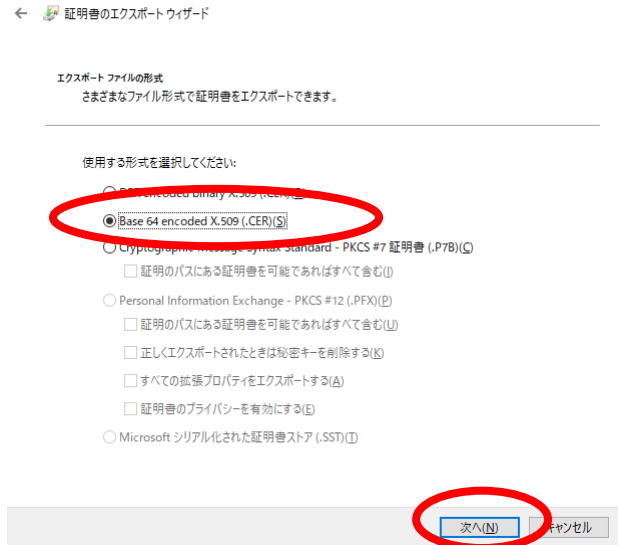
☐ はい、秘密キーをエクスポートします。

☒ いいえ、秘密キーをエクスポートしません(Q)



- ⑦ 形式を選択し、**次へ**をクリックします。

申請電子データシステム（ゲートウェイシステム）を利用される場合は2段目の「Base 64」を選択してください。



← 証明書のエクスポートウィザード

×

エクスポートファイルの形式
さまざまなファイル形式で証明書をエクスポートできます。

使用する形式を選択してください

☒ Base 64 encoded X.509 (.CER) (S)

☐ Cryptographic Message Syntax Standard - PKCS #7 証明書 (.P7B) (Q)

☐ 証明のパスにある証明書を可能であればすべて含む (I)

☐ Personal Information Exchange - PKCS #12 (.PFX) (P)

☐ 証明のパスにある証明書を可能であればすべて含む (I)

☐ 正しくエクスポートされたときは秘密キーを削除する (K)

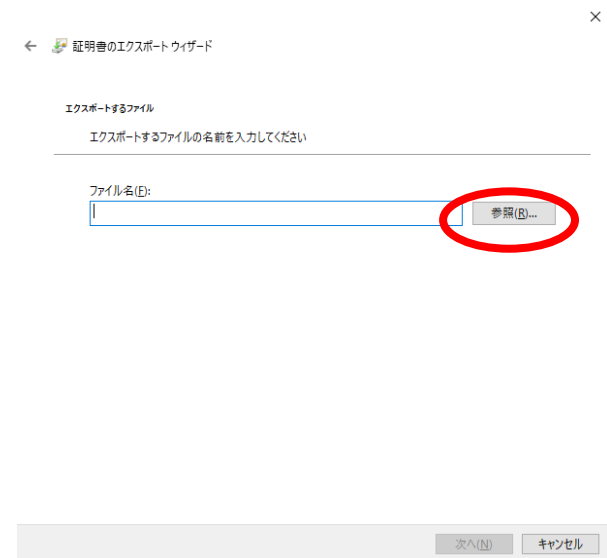
☐ すべての拡張プロパティをエクスポートする (A)

☐ 証明書のプライバシーを有効にする (E)

☐ Microsoft シリアル化された証明書ストア (.SST) (T)

次へ (N) キャンセル

- ⑧ **参照**をクリックします。



← 証明書のエクスポートウィザード

×

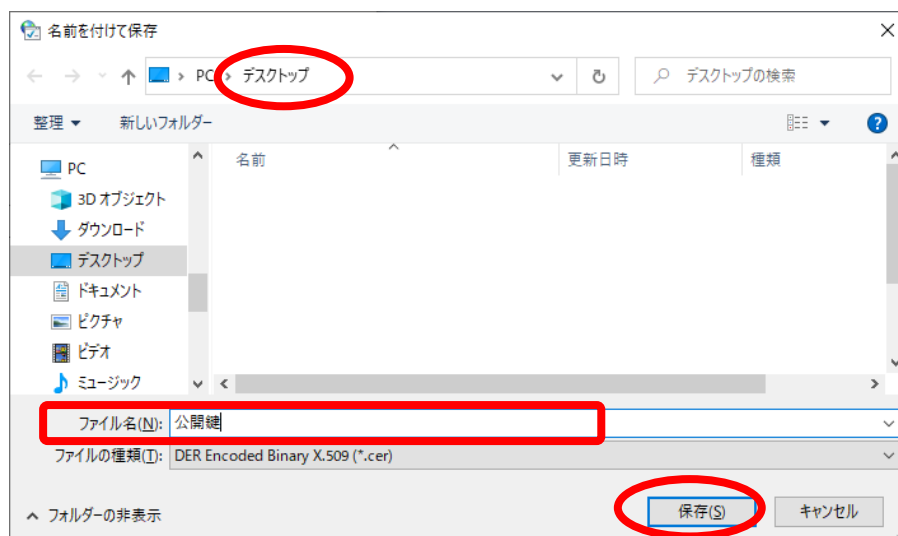
エクスポートするファイル
エクスポートするファイルの名前を入力してください

ファイル名 (F):

参照 (R)...

次へ (N) キャンセル

- ⑨ 保存場所が**デスクトップ**になっている事を確認し、**ファイル名**を入力して**保存**をクリックします。
（画像では例としてファイル名を「公開鍵」としています。）



名前を付けて保存

← → ↑ ↓ PC > デスクトップ

デスクトップの検索

整理 新しいフォルダー

名前	更新日時	種類
PC		
3D オブジェクト		
ダウンロード		
デスクトップ		
ドキュメント		
ピクチャ		
ビデオ		
ミュージック		

ファイル名 (N): 公開鍵

ファイルの種類 (T): DER Encoded Binary X.509 (*.cer)

保存 (S) キャンセル

⑩ 次へをクリックします。

← 証明書のエクスポートウィザード ×

エクスポートするファイル

エクスポートするファイルの名前を入力してください

ファイル名(E):

C:\Users¥1200136¥Desktop¥公開鍵.cer

参照(R)...

次へ(N)

キャンセル

⑪ 完了をクリックします。

デスクトップに⑨で設定したファイル名で公開鍵がエクスポートされています。



証明書のエクスポートウィザードの完了

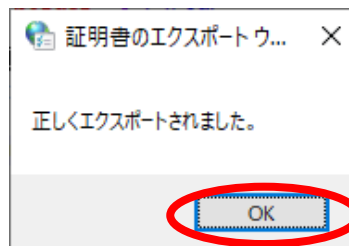
証明書のエクスポートウィザードが正常に完了しました。

次の設定が指定されました

ファイル名	C:\Users¥1200136¥
キーのエクスポート	いいえ
証明のパスにあるすべての証明書を含める	いいえ
ファイルの形式	DER Encoded Binary

完了(F)

キャンセル



以上

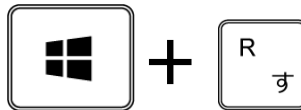
9. 手順：不要な証明書の削除

更新や再発行を行ったあとの古い証明書や使用しなくなった証明書を削除する手順です。

削除後の復旧は出来ませんので、必ず証明書ファイル(.p12)やエクスポートした秘密鍵証明書(.pfx)のバックアップを行ってから削除されることをご推奨いたします。

エクスポート手順は「本書【5.証明書（秘密鍵）のエクスポート手順】」（P12）をご参考ください。

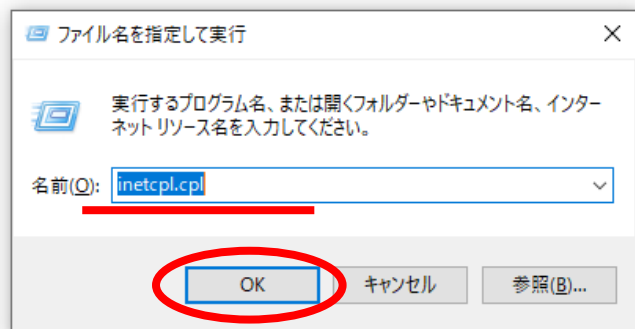
- ① キーボードの[Windows]キーを押しながら[R]キーを押します。



- ② ファイル名を指定して実行が立ち上がります。

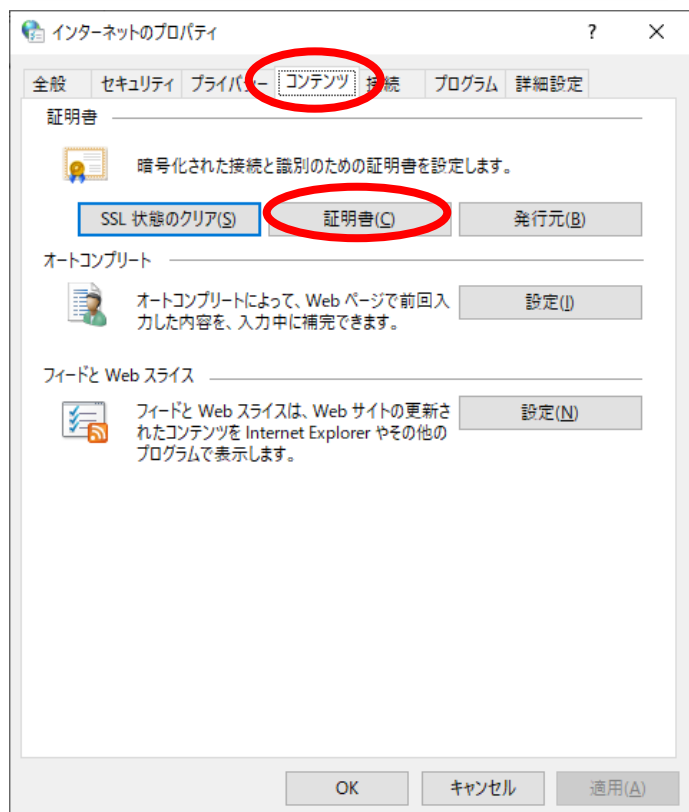
名前に以下を入力し、OKを押します。

「 **inetcpl.cpl** 」

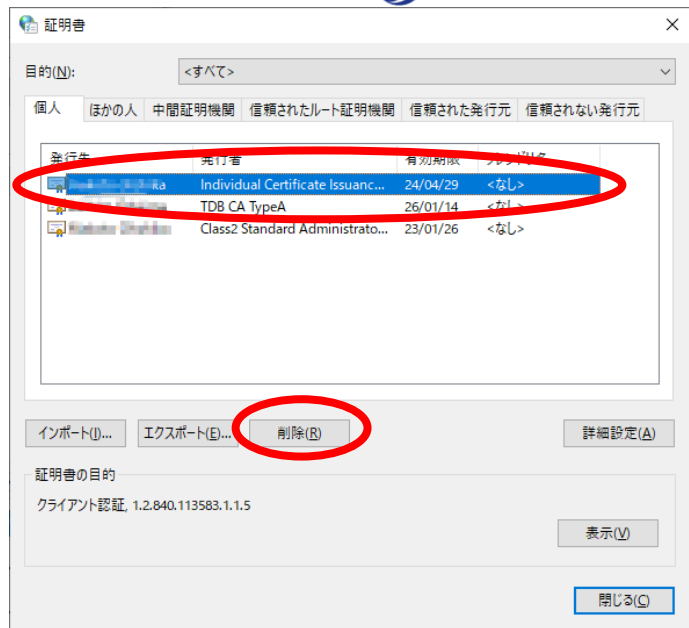


- ③ インターネットのプロパティが表示されます。

コンテンツタブの証明書をクリックします。



- ④ 削除したい電子証明書をクリックし、
削除をクリックします。



- ⑤ はいをクリックします。



■ ポイント ■

※削除後は元に戻すことが出来ません。

念の為、秘密鍵のエクスポート（P17）やバックアップを取ることを推奨いたします。

以上