NRA

Good Bye Password

NRA-PKI ご利用ガイド

利用法人管理者マニュアル

2022 年 8 月 18 日

Ver. 1.40

改訂履歴

版	日　付	内　容	備　考
Ver. 1.00	--	初版作成	
Ver. 1.06	2017/01/20	・サポート情報追記 ・利用者の削除機能追記	
Ver. 1.07	2018/06/01	定期システムメンテナンス日変更に伴い、サポート情報を削除	
Ver. 1.08	2019/04/12	一部図を変更	
Ver. 1.09	2019/07/12	ダウンロードサイトからクライアント証明書を配付する機能の説明を追加	
Ver. 1.10	2020/4/28	CSV 一括登録時の mobileconfig ファイルについて説明を追加	
Ver. 1.11	2020/5/21	CSV 一括登録時の注意点追記	
Ver. 1.12	2020/7/28	誤植修正	
Ver. 1.13	2020/7/30	管理者用証明書のインストールについて補足を追記	
Ver. 1.14	2021/9/21	期間指定と期間+時間指定の発行方法についての説明を追加	
Ver. 1.20	2022/1/21	Microsoft Edge 仕様に変更	
Ver. 1.21	2022/3/16	使用可能な記号についての備考を追記	
Ver. 1.30	2022/4/13	・O,OU 指定、インストール制限機能について証明書の発行方法を追記 ・CSV 一括登録時の注意点の補足追加	
Ver. 1.40	2022/8/18	証明書発行時の入力項目の変更	

目次

1. 管理者の役割

利用法人の管理者は、「NRA-PKI システム管理画面」より、クライアント証明書に関する以下の操作を行うことができます。

電子証明書の新規発行が許可されていない場合は、管理画面から電子証明書の新規発行はできません。

- **クライアント証明書の新規発行**
  利用者を新規登録して、クライアント証明書を発行します。
- **クライアント証明書の失効**
  利用者がクライアント証明書をインストールした端末を紛失したような場合に、クライアント証明書を失効して、端末を使えなくします。
- **クライアント証明書の再発行**
  端末を紛失した利用者が、新しい端末で業務を再開するような場合に、クライアント証明書を再発行します。

2. 管理者用証明書をインストールする

利用者へのクライアント証明書の操作（新規発行/失効/再発行）は「NRA-PKI システム管理画面」から行います。「NRA-PKI システム管理画面」にログインするには、管理者用証明書が必要です。以下の手順で、管理者用証明書をお使いの PC にインストールしてください。

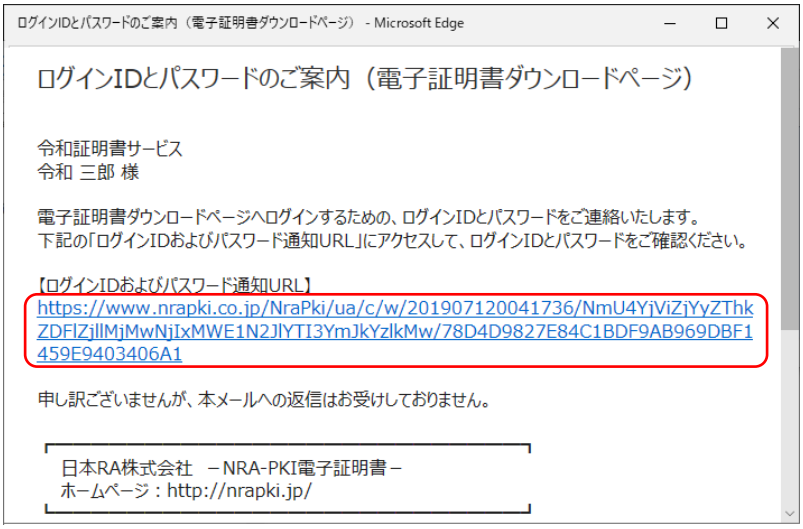
2-1 管理者用証明書をダウンロードする

1. 弊社クライアント証明書をご購入いただきますと、NRA-PKI 申請書にご記入いただいたご担当者様宛に以下のタイトルのメールが届きます。メールの指示にしたがって、管理者用証明書をダウンロードして PC にインポートしてください。

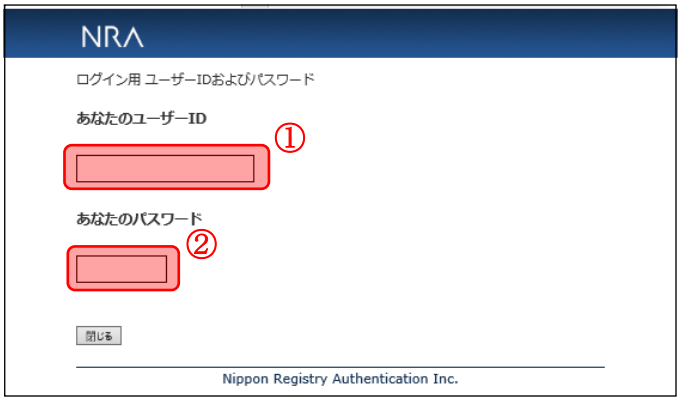
   - **メール１：「管理者用電子証明書をダウンロードしてください」**
     「NRA-PKI システム管理画面」にログインするために必要な管理者用証明書のダウンロード URL が記載されています。
   - **メール２：「ログイン ID とパスワードのご案内**

     （電子証明書ダウンロードページ）」
     管理者用証明書をダウンロード、インストールする際に必要な ID とパスワードが記載されています。

2. 「ログイン ID とパスワードのご案内（電子証明書ダウンロードページ）」メールを開き「ログイン ID およびパスワード通知 URL」をクリックします。

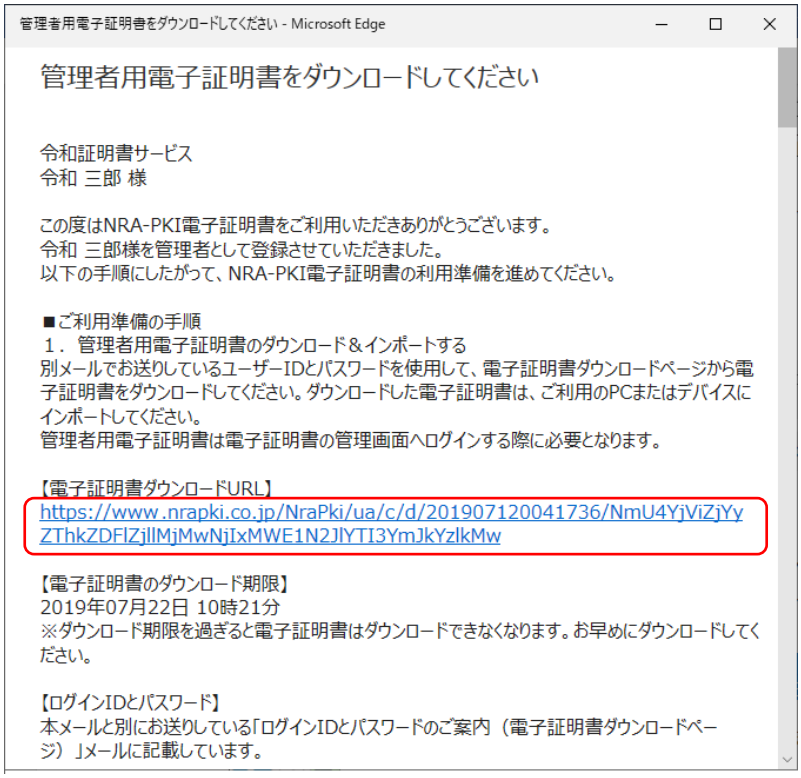


3. ブラウザが起動し、「ID およびパスワード通知」画面が表示されます。ID（下図赤枠①内）とパスワード（下図赤枠②内）を確認します。



パスワードは、証明書を PC にインストールするときにも必要ですので、忘れないようにしてください。

4. 「管理者用電子証明書をダウンロードしてください」のメールを開き「電子証明書ダウンロード URL」に記載されている URL をクリックします。



5. ブラウザが起動し、「証明書ダウンロード ログイン画面」が表示されます。「ID およびパスワード通知」画面で確認した ID とパスワードを入力して、［ログイン］ボタンをクリックします。

6. ［証明書ダウンロード画面］が表示されます。［証明書ダウンロード］ボタンをクリックします。
※管理者用証明書（拡張子が p12 のファイル）を任意のフォルダに保存してください。

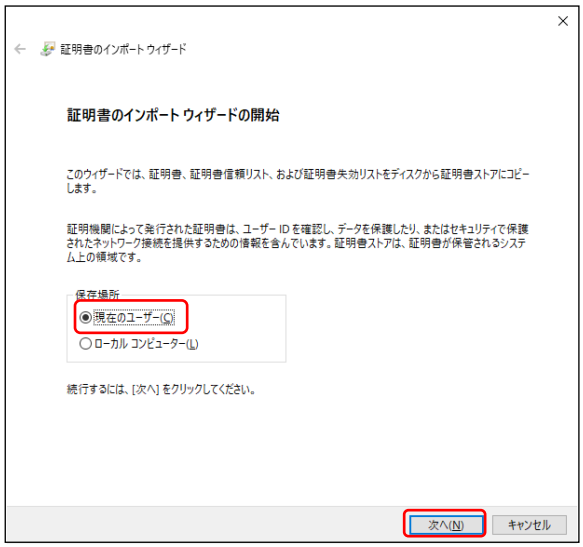
7. 証明書のダウンロードが完了しましたらブラウザを終了します。

8. 以上で管理者用証明書のダウンロードは終了になります。ダウンロードした証明書ファイルは厳重に保管してください。

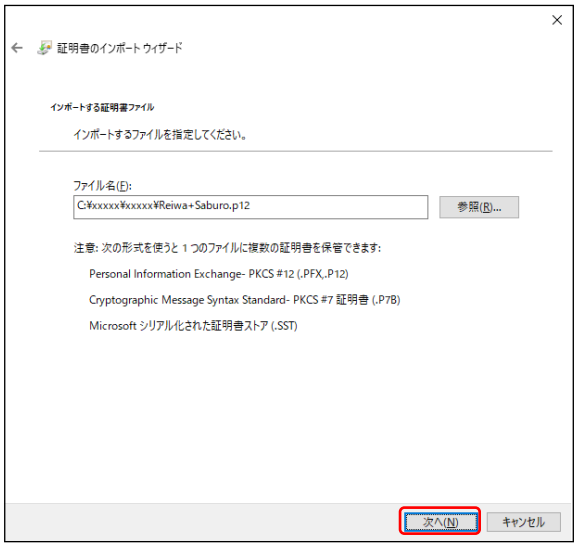
2-2 管理者用証明書をインストールする

1. 次にご利用のPCにダウンロードした管理者用証明書をインストールします。ダウンロードして保存した管理者用証明書（拡張子がp12のファイル）をダブルクリックします。

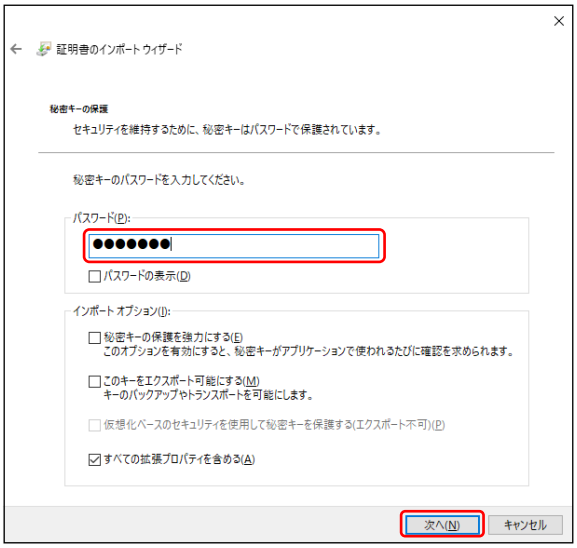
2. ［証明書のインポートウィザード］が起動します。保存場所で［現在のユーザー］を選択して［次へ］をクリックします。



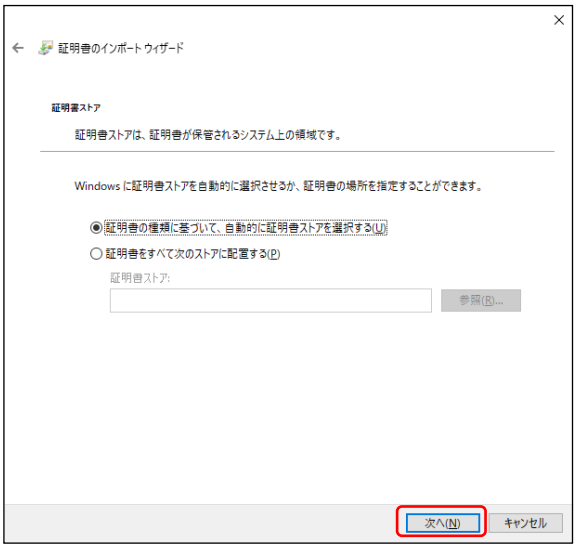
3. ファイル名に、ダウンロードした電子証明書ファイルが表示されていることを確認して、[次へ]をクリックします。



4. 秘密キーのパスワードに、「ID およびパスワード通知」画面で確認したパスワードを入力し、［次へ］をクリックします。



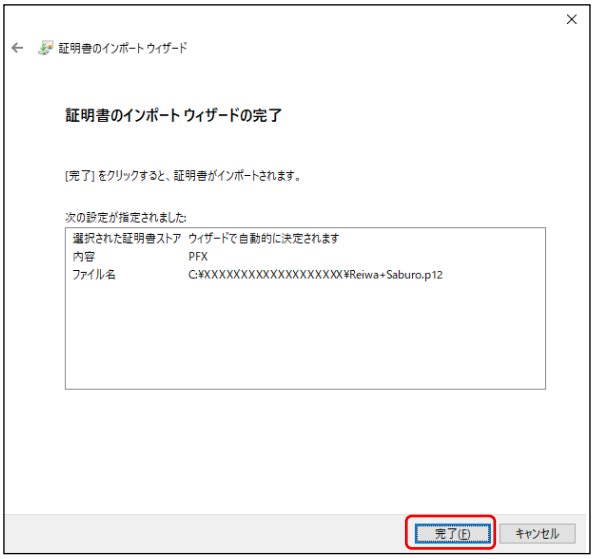
5. ［証明書の種類に基づいて、自動的に証明書ストアを選択する］が選択されていることを確認し、［次へ］をクリックします。



［このキーをエクスポート可能にする］のチェックボックスはオフにします。

オンにすると電子証明書は抜き取り可能となりますので脆弱になります。

6. ［完了］をクリックします。



7. 以上で、管理者用証明書のインストールは終了になります。

【補足】セキュリティ警告について

［完了］をクリックすると下図のセキュリティ警告ダイアログボックスが表示される場合があります。

赤枠内の拇印がNRA-PKIルート認証局証明書のフィンガープリント(SHA-1)と一致しているため［はい］を選択してください。

※［いいえ］を選択するとルート証明書がインストールされません。誤って［いいえ］を選択してしまった場合は、下記 URL の弊社 HP レポジトリよりルート証明書をダウンロード・インストールしてください。

日本RA NRA-PKI ルート認証局証明書（自己署名証明書）

NRA-PKIサービスが使用するルート証明局の証明書は以下の通りです。

証明書シリアル番号	01
認証局DN	CN = Nippon RA Root Certification Authority O = Nippon RA Inc. C = JP
証明書有効期間（JST）	2031年8月15日 11:28:56
フィンガープリント（SHA-1）	8f 36 9b f2 70 17 39 c8 22 c1 03 cf 43 8d a8 2a 7e 77 60 69
機関キー識別子（KeyID）	19 99 a6 4d e2 2f 79 1e 5b 4e 64 d9 80 e7 f7 c9 b0 9f 72 0e

（参考）弊社 HP　レポジトリ

https://www.nrapki.jp/client-certificate/repo/

3. NRA-PKI システム管理画面へログインする

利用者へのクライアント証明書の操作（新規発行/失効/再発行）は「NRA-PKI システム管理画面」にログインして行います。先ほどインストールした「管理者用証明書」を使ってログインしますので、ID やパスワードを入力する必要はありません。以下の手順で「NRA-PKI システム管理画面」にログインしてください。

3-1 NRA-PKI システム管理画面へログインする

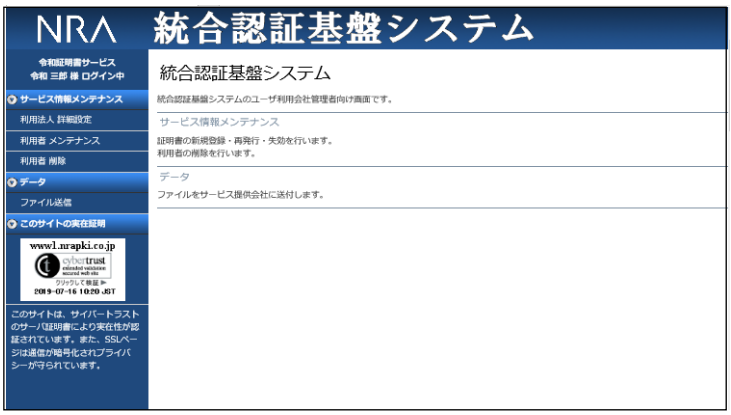
1. Microsoft Edge を起動し、以下の URL にアクセスします。
   https://www.nrapki.co.jp/NraPki/pki

2. 以下のような認証用の証明書の選択画面が表示されますので、先ほどインストールした「管理者用証明書」を選択して「OK」ボタンをクリックします。

【補足】

Microsoft Edge のバージョンによって、証明書の選択画面が表示されない場合があります。

3. 正しくログインできれば、以下の「NRA-PKI システム管理画面」が表示されます。



4. 以上で「NRA-PKI システム管理画面」へのログインは終了です。この画面から、クライアント証明書の発行、失効および再発行の操作を行います。

4. クライアント証明書を発行／配付する

「NRA-PKI システム管理画面」を使用してクライアント証明書を発行／配付する方法は、以下の３つがあります。

- **利用者情報を登録してクライアント証明書を発行／配付する**

  「NRA-PKI システム管理画面」で利用者情報を入力してクライアント証明書を発行／配付する最も基本的な操作になります。利用者にはメールでクライアント証明書のインストールに必要な情報が送信されます。

- **利用者情報を CSV で一括登録してクライアント証明書を発行／配付する**

  利用者情報の CSV ファイルを作成し「NRA-PKI システム管理画面」からインポートすることでクライアント証明書の発行／配付を行います。複数の利用者を一括で登録する場合に便利です。利用者にはメールでクライアント証明書のインストールに必要な情報を送信する方法と、管理者がクライアント証明書を一旦ダウンロードしてから利用者に個別に配付する方法のどちらかを選択できます。

- **ダウンロードサイトからクライアント証明書を配付する**

  利用者情報の登録とクライアント証明書の発行は上記のどちらかで実施しますが、クライアント証明書の配付は専用のダウンロードサイトから行います。管理者はダウンロードサイトの URL と ID／パスワードを利用者に通知し、利用者がダウンロードサイトにアクセスしてクライアント証明書を入手しインストールします。利用者のインストール作業を簡素化したい場合に便利です。

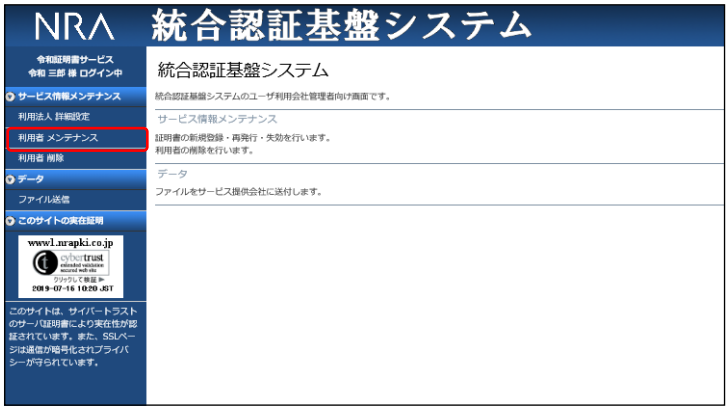
  【補足】

  - 「ダウンロードサイトからクライアント証明書を配付する」機能はデフォルトでは無効になっております。本機能のご利用を希望される場合は、別途弊社までお問い合わせください。

以下それぞれの方法について説明します。

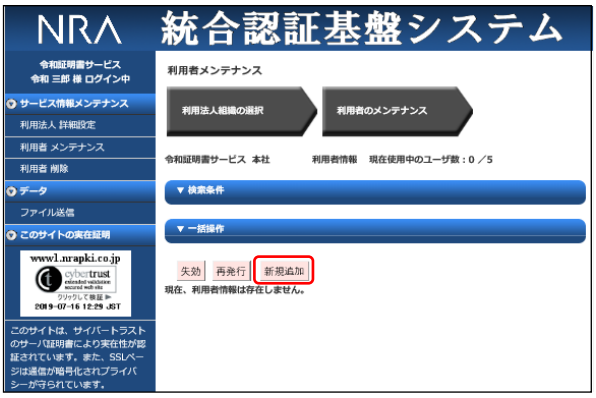
4-1 利用者情報を登録してクライアント証明書を発行/配付する

1. 「NRA-PKI システム管理画面」左メニューから［サービス情報メンテナンス］－［利用者メンテナンス］をクリックします。

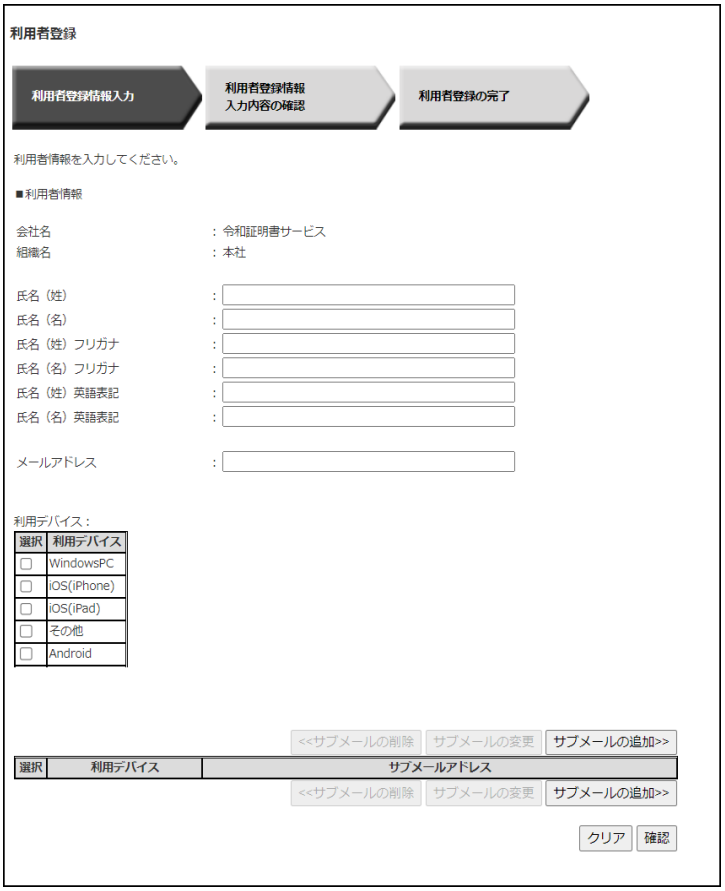


2. ［利用者メンテナンス］画面が表示されます。［以下のサービスを選択しています］で使用中のサービスが選択されていることを確認します。その下に表示される表の［組織名］列に表示されている組織名（特別な場合を除き「本社」と表示されています）のリンクをクリックします。

3. ［利用者のメンテナンス］画面が表示されます。利用者を新しく登録する場合は、［新規追加］ボタンをクリックします。



4. ［利用者登録］ウィンドウがポップアップします。以下の順序でクライアント証明書の利用者情報を入力します。



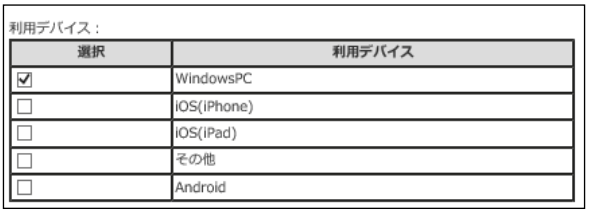
サービス提供会社によって、クライアント証明書の新規発行を利用法人の管理者に許可していない場合があります。その場合、［新規追加］ボタンは表示されません。

5. 利用者情報（氏名）とメールアドレスを入力します。

［氏名（姓）英語表記］、［氏名（名）英語表記］、[メールアドレス]の入力内容は、発行するクライアント証明書に格納されますので、正確に入力してください（利用者がクライアント証明書のインストールに必要な情報もこのメールアドレスに送信されます）。

メールアドレスに使用できる記号は半角でドット″.″、アンダーバー″_″、ハイフン″-″のみです。

6. 利用デバイス（クライアント証明書をインストールするデバイス）を選択します。



利用者が複数のデバイスでクライアント証明書を使用する場合は、複数のデバイスを選択します。たとえば［Windows PC］と［iOS(iPhone)］を選択した場合は、Windows PC 用と iOS(iPhone)用の 2 枚の電子証明書が発行されます。

【補足】

ご利用のサービスによって、入力項目が異なりますので以下ご確認ください。

■期間指定又は期間+時間指定をご利用の場合

利用デバイスと証明書有効期限を入力してください。期間指定は yyyy/mm/dd、期間+時間指定は yyyy/mm/dd hh:mm の形式で入力可能です。

「期間指定又は期間+時間指定」「O、OU 指定」「インストール制限」のサービスはデフォルトではご利用になれません。
ご希望の際は、弊社サポート窓口(support@nrapki.jp)迄お問い合わせください。

利用デバイス：

選択	利用デバイス	証明書有効期限(From)	証明書有効期限(To)
☑	WindowsPC	2021/09/21	2022/09/21
☐	iOS(iPhone)		
☐	iOS(iPad)		
☐	その他		
☐	Android		

■O、OU 指定をご利用の場合

利用デバイスと Organization、OrganizationUnit1、OrganizationUnit2 を入力してください。すべてに値を設定しない場合は、発行証明書のサブジェクト組織名に「利用法人会社名（英語表記）」が設定されます。

利用デバイス：

選択	利用デバイス	Organization	OrganizationUnit1	OrganizationUnit2
☑	WindowsPC	O	OU	OU2
☐	iOS(iPhone)			
☐	iOS(iPad)			
☐	その他			
☐	Android			

■インストール制限をご利用の場合

利用デバイスを WindowsPC、利用デバイス制限を任意で選択し、制限項目にインストールする端末の MAC アドレス、コンピュータ名、ログインユーザ名、端末(BIOS)シリアル番号を入力してください。制限項目が空欄の場合は該当の項目の制限は行いません。

※インストール制限機能は WindowsPC のみご利用いただけます。

利用デバイス：

選択	利用デバイス	利用デバイス制限	制限項目① MACアドレス	制限項目② コンピュータ名	制限項目③ ログインユーザ名	制限項目④ 端末(BIOS)シリアル番号
☑	WindowsPC	すべての条件と一致（AND）	111111111111	test-host	山田太郎	aaaaaaaaaaa
☐	iOS(iPhone)	制限なし				
☐	iOS(iPad)	制限なし				
☐	その他	制限なし				
☐	Android	制限なし				

利用デバイス制限

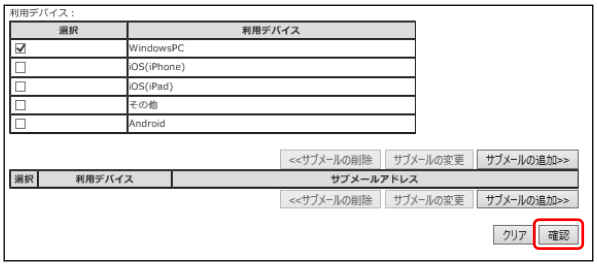
・制限なし
インストール時の制限無し

・どれかの条件と一致（OR）
入力した制限項目が 1 つ以上一致した端末のみインストール可能

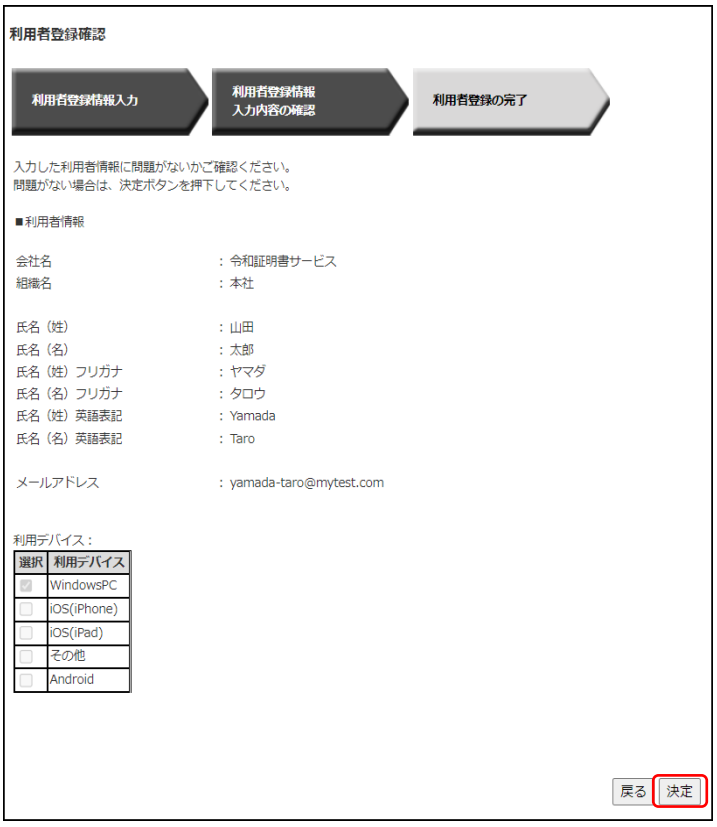
・すべての条件と一致（AND）
入力した制限項目すべて一致した端末のみインストール可能

MAC アドレスは、ハイフン”-“、コロン”:”を省略した 12 桁の 16 進数（0～F）で入力してください。

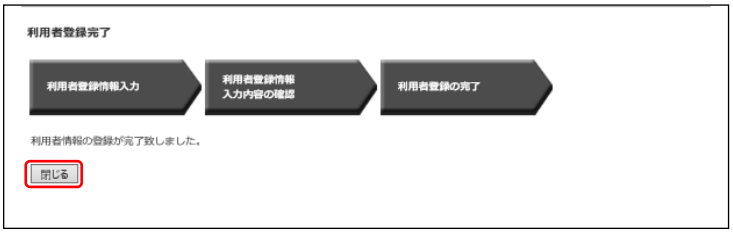
7. 以上の情報を入力後、［利用者登録］ウィンドウ下部にある［確認］ボタンをクリックします。



8. ［入力内容の確認］画面が表示されます。入力内容に間違いがなければ［決定］ボタンをクリックします。



9. ［利用者登録完了］画面が表示されます。［閉じる］ボタンをクリックします。



10. 以上で利用者の登録とクライアント証明書の発行は終了になります。

11. 登録した利用者のメールアドレスに以下の 2 通のメールが送信されます。

- **電子証明書の「秘密の鍵」を登録してください**
- **ログイン ID とパスワードのご案内（電子証明書の「秘密の鍵」登録ページ）**

利用者には、メールの内容にしたがってクライアント証明書をインストールさせてください（クライアント証明書のダウンロード／インストール手順については「利用者マニュアル」をご参照ください）。

【補足】インストール制限機能利用時の enroll.exe のエラー

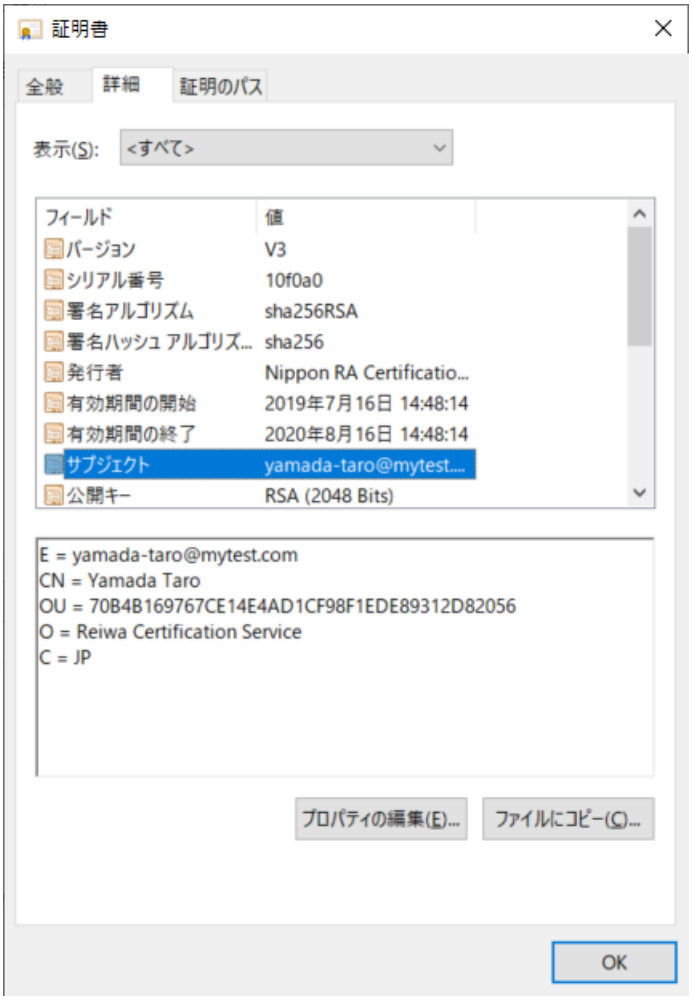
設定した制限項目と証明書をインストールした端末情報に差異がある場合は、enroll.exe を実行後に下図のようなエラー画面が表示されます。

■すべての条件と一致（AND）で MAC アドレスのみ一致している場合

【補足】証明書情報を確認する

インストールした証明書情報は、「certmgr.msc」を実行し、「個人」-「証明書」にて確認できます。
(「certmgr.msc」の実行方法は、Windows キー+R にて「ファイル名を指定して実行」のポップアップ画面が表示されますので、名前の部分に”certmgr.msc”と入力し、OK をクリックしてください)

対象の証明書をダブルクリックし、「詳細」-「サブジェクト」にて下図のように証明書の内容を確認できます。



証明書のサブジェクトに以下の値が登録されています。

E：証明書メールアドレス
CN：姓（英文）+名（英文）
OU：NRA-PKI が使用
O：利用会社名（英文）
C：JP

O、OU 指定のサービスをご利用の場合は、証明書のサブジェクトに以下の値が登録されています。

E：証明書メールアドレス
CN：姓（英文）+名（英文）
OU：NRA-PKI が使用
OU：OrganizationUnit1
OU：OrganizationUnit2
O：Organization
C：JP

4-2 利用者情報を CSV で一括登録してｸﾗｲｱﾝﾄ証明書を発行／配付する

1. 以下の表を参考にして一括登録用の CSV ファイルを作成します（利用者情報を CSV ファイルに記載します）。

NO	項目名	必須	説明
1	代表メールアドレス	○	利用者のメールアドレスを入力します。
2	利用者（姓）	○	利用者の姓を入力します。
3	利用者（名）	○	利用者の名を入力します。
4	利用者（姓）フリガナ	○	利用者の姓（フリガナ）を入力します。
5	利用者（名）フリガナ	○	利用者の名（フリガナ）を入力します。
6	利用者（姓）英語表記	○	利用者の姓（英語表記）を入力します。
7	利用者（名）英語表記	○	利用者の名（英語表記）を入力します。
8	利用デバイス用メールアドレス	○	通常は代表メールアドレスを入力します。利用者が使用するデバイス（スマートフォン等）で別のアドレスを使用している場合は、利用デバイス用のメールアドレスを入力します。
9	デバイスコード	○	利用者が使用するデバイスを NRA-PKI で使用するデバイスコードで指定します。 デバイスコードは右記の「デバイスコード一覧」を参照してください。
10	証明書有効期限(From)	-	入力の必要はありません。期間指定又は期間+時間指定の証明書を契約している場合にのみ有効です。
11	証明書有効期限(To)	-	入力の必要はありません。期間指定又は期間+時間指定の証明書を契約している場合にのみ有効です。
12	サービス連携用 ID	-	入力の必要はありません。サービス提供会社が使用する項目です。 サービスで利用している、利用者を識別するキー情報を入力します。
13	プリンシパル名	-	入力の必要はありません。スマートカードログオン用証明書、コンピューター証明書をご利用の場合にのみ有効です。ユーザー・プリンシパル名（User Principal Name：UPN）を入力します。

【CSV ファイルの例】

Yamada-Taro@mytest.jp,山田,太郎,ヤマダ,タロウ,
Yamada,Taro,Yamada-Taro@mytest.jp,01

No.1~8 に使用できる記号は半角でドット″.″、アンダーバー″_″、ハイフン″-″のみです。

利用者がクライアント証明書のインストールに必要な情報は「利用デバイス用メールアドレス」に送信されます。

【デバイスコード一覧】
デバイスコード：利用デバイス種別
01：WindowsPC
11：iOS(iPhone)
12：iOS(iPad)
20：Android
99：その他

No.10~13 は CSV の記載において省略することが可能です。

期間指定又は期間+時間指定のサービスをご利用の場合は、[証明書有効期限（From）]と［証明書有効期限（To）］は必須項目となります。

期間指定は yyyy/mm/dd 形式、期間+時間指定は yyyy/mm/dd hh:mm 形式で指定してください。

【入力例】
期間指定の場合　2020/01/01
期間+時間指定の場合　2020/01/01 10:00

未指定の場合は、証明書発行日が開始日となります。

■O、OU 指定をご利用の場合

NO	項目名	必須	説明
1	代表メールアドレス	○	利用者のメールアドレスを入力します。
2	利用者（姓）	○	利用者の姓を入力します。
3	利用者（名）	○	利用者の名を入力します。
4	利用者（姓）フリガナ	○	利用者の姓（フリガナ）を入力します。
5	利用者（名）フリガナ	○	利用者の名（フリガナ）を入力します。
6	利用者（姓）英語表記	○	利用者の姓（英語表記）を入力します。
7	利用者（名）英語表記	○	利用者の名（英語表記）を入力します。
8	利用デバイス用メールアドレス	○	通常は代表メールアドレスを入力します。利用者が使用するデバイス（スマートフォン等）で別のアドレスを使用している場合は、利用デバイス用のメールアドレスを入力します。
9	Organization	-	Organization を入力します。
10	OrganizationUnit1	-	OrganizationUnit1 を入力します。
11	OrganizationUnit2	-	OrganizationUnit2 を入力します。
12	デバイスコード	○	利用者が使用するデバイスを NRA-PKI で使用するデバイスコードで指定します。 デバイスコードは右記の「デバイスコード一覧」を参照してください。
13	証明書有効期限(From)	-	入力の必要はありません。期間指定又は期間+時間指定の証明書を契約している場合にのみ有効です。
14	証明書有効期限(To)	-	入力の必要はありません。期間指定又は期間+時間指定の証明書を契約している場合にのみ有効です。
15	サービス連携用 ID	-	入力の必要はありません。サービス提供会社が使用する項目です。 サービスで利用している、利用者を識別するキー情報を入力します。
16	プリンシパル名	-	入力の必要はありません。スマートカードログオン用証明書、コンピューター証明書をご利用の場合にのみ有効です。ユーザー・プリンシパル名（User Principal Name：UPN）を入力します。

【CSV ファイルの例】

Yamada-Taro@mytest.jp,山田,太郎,ヤマダ,タロウ,Yamada,Taro,
Yamada-Taro@mytest.jp,o,ou1,ou2,01

No.1~8 に使用できる記号は半角でドット″.″、アンダーバー″_″、ハイフン″-″のみです。

利用者がクライアント証明書のインストールに必要な情報は「利用デバイス用メールアドレス」に送信されます。

No.9~11 のすべてに値を設定しない場合は、発行証明書のサブジェクト組織名に「利用法人会社名（英語表記）」が設定されます。

【デバイスコード一覧】
デバイスコード：利用デバイス種別
01：WindowsPC
11：iOS(iPhone)
12：iOS(iPad)
20：Android
99： その他

No.13~16 は CSV の記載において省略することが可能です。

期間指定又は期間+時間指定のサービスをご利用の場合は、［証明書有効期限（From）］と［証明書有効期限（To）］は必須項目となります。

期間指定は yyyy/mm/dd 形式、期間+時間指定は yyyy/mm/dd hh:mm 形式で指定してください。

【入力例】
期間指定の場合　2020/01/01
期間+時間指定の場合　2020/01/01 10:00

未指定の場合は、証明書発行日が開始日となります。

■インストール制限をご利用の場合

NO	項目名	必須	説明
1	代表メールアドレス	○	利用者のメールアドレスを入力します。
2	利用者（姓）	○	利用者の姓を入力します。
3	利用者（名）	○	利用者の名を入力します。
4	利用者（姓）フリガナ	○	利用者の姓（フリガナ）を入力します。
5	利用者（名）フリガナ	○	利用者の名（フリガナ）を入力します。
6	利用者（姓）英語表記	○	利用者の姓（英語表記）を入力します。
7	利用者（名）英語表記	○	利用者の名（英語表記）を入力します。
8	利用デバイス用メールアドレス	○	通常は代表メールアドレスを入力します。利用者が使用するデバイス（スマートフォン等）で別のアドレスを使用している場合は、利用デバイス用のメールアドレスを入力します。
9	デバイスコード	○	利用者が使用するデバイスを NRA-PKI で使用するデバイスコードで指定します。 デバイスコードは右記の「デバイスコード一覧」を参照してください。
10	証明書有効期限(From)	-	入力の必要はありません。期間指定又は期間+時間指定の証明書を契約している場合にのみ有効です。
11	証明書有効期限(To)	-	入力の必要はありません。期間指定又は期間+時間指定の証明書を契約している場合にのみ有効です。
12	サービス連携用 ID	-	入力の必要はありません。サービス提供会社が使用する項目です。 サービスで利用している、利用者を識別するキー情報を入力します。
13	プリンシパル名	-	入力の必要はありません。スマートカードログオン用証明書、コンピューター証明書をご利用の場合にのみ有効です。ユーザー・プリンシパル名（User Principal Name：UPN）を入力します。
14	インストール端末制限	-	インストール制限における制限項目一致条件を指定します。 [0] 制限なし [1] 制限項目のどれかと一致(OR 一致) [2] 制限項目のすべてと一致(AND 一致)
15	端末制限項目① MAC アドレス	-	インストールを許可する端末の MAC アドレスを入力します。ハイフン"-"、コロン":"を除いた 12 桁の 16 進数(0～F)で指定してください。
16	端末制限項目② コンピュータ名	-	インストールを許可する端末のコンピュータ名を入力します。
17	端末制限項目③ ログインユーザ名	-	インストールを許可するログインユーザ名を入力します。
18	端末制限項目④ 端末(BIOS)シリアル番号	-	インストールを許可する端末の(BIOS)シリアル番号を入力します。

【CSV ファイルの例】

```
Yamada-Taro@mytest.jp,山田,太郎,ヤマダ,タロウ,Yamada,Taro,
Yamada-Taro@mytest.jp,01,,,,,2,111111111111,host-test,山田太郎,aaaaaaaaaaaaa
```

No.1~8 に使用できる記号は半角でドット"."、アンダーバー"_"、ハイフン"-"のみです。

利用者がクライアント証明書のインストールに必要な情報は「利用デバイス用メールアドレス」に送信されます。

【デバイスコード一覧】
デバイスコード：利用デバイス種別
01：WindowsPC
11：iOS(iPhone)
12：iOS(iPad)
20：Android
99：その他

期間指定又は期間+時間指定のサービスを利用していない場合は、No.10~13 の値は未指定としてください。

期間指定又は期間+時間指定のサービスをご利用の場合は、[証明書有効期限（From）]と［証明書有効期限（To）］は必須項目となります。

期間指定は yyyy/mm/dd 形式、期間+時間指定は yyyy/mm/dd hh:mm 形式で指定してください。

【入力例】
期間指定の場合　2020/01/01
期間+時間指定の場合　2020/01/01 10:00

未指定の場合は、証明書発行日が開始日となります。

No.14 を未指定にした場合は、「制限なし」になります。

No.15~18 で、値を未指定にした場合は制限項目に含まれません。

■ O、OU 指定+インストール制限をご利用の場合

NO	項目名	必須	説明
1	代表メールアドレス	○	利用者のメールアドレスを入力します。
2	利用者（姓）	○	利用者の姓を入力します。
3	利用者（名）	○	利用者の名を入力します。
4	利用者（姓）フリガナ	○	利用者の姓（フリガナ）を入力します。
5	利用者（名）フリガナ	○	利用者の名（フリガナ）を入力します。
6	利用者（姓）英語表記	○	利用者の姓（英語表記）を入力します。
7	利用者（名）英語表記	○	利用者の名（英語表記）を入力します。
8	利用デバイス用メールアドレス	○	通常は代表メールアドレスを入力します。利用者が使用するデバイス（スマートフォン等）で別のアドレスを使用している場合は、利用デバイス用のメールアドレスを入力します。
9	Organization	-	Organization を入力します。
10	OrganizationUnit1	-	OrganizationUnit1 を入力します。
11	OrganizationUnit2	-	OrganizationUnit2 を入力します。
12	デバイスコード	○	利用者が使用するデバイスを NRA-PKI で使用するデバイスコードで指定します。 デバイスコードは右記の「デバイスコード一覧」を参照してください。
13	証明書有効期限(From)	-	入力の必要はありません。期間指定又は期間+時間指定の証明書を契約している場合にのみ有効です。
14	証明書有効期限(To)	-	入力の必要はありません。期間指定又は期間+時間指定の証明書を契約している場合にのみ有効です。
15	サービス連携用 ID	-	入力の必要はありません。サービス提供会社が使用する項目です。 サービスで利用している、利用者を識別するキー情報を入力します。
16	プリンシパル名	-	入力の必要はありません。スマートカードログオン用証明書、コンピューター証明書をご利用の場合にのみ有効です。ユーザー・プリンシパル名（User Principal Name：UPN）を入力します。
17	インストール端末制限	-	インストール制限における制限項目一致条件を指定します。 [0] 制限なし [1] 制限項目のどれかと一致(OR 一致) [2] 制限項目のすべてと一致(AND 一致)
18	端末制限項目① MAC アドレス	-	インストールを許可する端末の MAC アドレスを入力します。ハイフン"-"、コロン":"を除いた 12 桁の 16 進数(0～F)で指定してください。
19	端末制限項目② コンピュータ名	-	インストールを許可する端末のコンピュータ名を入力します。
20	端末制限項目③ ログインユーザ名	-	インストールを許可するログインユーザ名を入力します。
21	端末制限項目④ 端末(BIOS)シリアル番号	-	インストールを許可する端末の(BIOS)シリアル番号を入力します。

No.1~8 に使用できる記号は半角でドット"."、アンダーバー"_"、ハイフン"-"のみです。

利用者がクライアント証明書のインストールに必要な情報は「利用デバイス用メールアドレス」に送信されます。

No.9~11 のすべてに値を設定しない場合は、発行証明書のサブジェクト組織名に「利用法人会社名（英語表記）」が設定されます。

【デバイスコード一覧】
デバイスコード：利用デバイス種別
01：WindowsPC
11：iOS(iPhone)
12：iOS(iPad)
20：Android
99：その他

期間指定又は期間+時間指定のサービスをご利用の場合は、[証明書有効期限（From）]と［証明書有効期限（To）］は必須項目となります。

期間指定は yyyy/mm/dd 形式、期間+時間指定は yyyy/mm/dd hh:mm 形式で指定してください。

【入力例】
期間指定の場合　2020/01/01
期間+時間指定の場合　2020/01/01 10:00

未指定の場合は、証明書発行日が開始日となります。

No.14 を未指定にした場合は、「制限なし」になります。

No.15~18 で、値を未指定にした場合は制限項目に含まれません。

【CSV ファイルの例】

Yamada-Taro@mytest.jp,山田,太郎,ヤマダ,タロウ,Yamada,Taro,
Yamada-Taro@mytest.jp,01,,,,,2,111111111111,host-test,山田太郎,aaaaaaaaaaaaa

【補足】CSV 作成時の注意点

CSV ファイルを作成する際はメモ帳などのテキストエディタをご利用ください。エクセルを使用すると、登録時にエラーが出る場合があります。詳細については以下サポートサイトの記事をご確認ください。

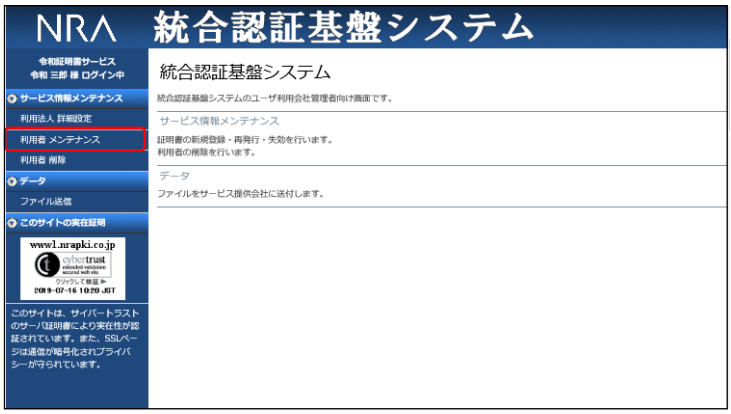
CSV 一括登録時のエラー「行:1 項目:1 入力形式が不正です。入力形式：メールアドレス形式のみ」
https://www.nrapki.jp/support/?p=555

その他の注意点等は以下サポートサイトの記事も併せてご確認ください。

CSV 一括登録時の補足や注意点
https://www.nrapki.jp/support/?p=885

一度削除した利用者を再度 CSV 一括登録する場合について
https://www.nrapki.jp/support/?p=583

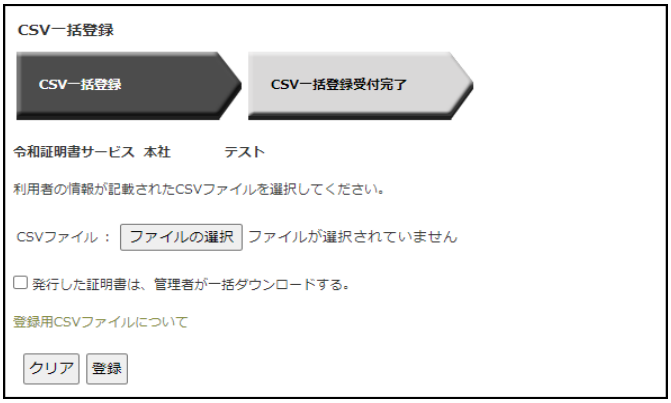
2. 準備した CSV ファイルを使って複数のユーザを一括登録しクライアント証明書を発行します。「NRA-PKI システム管理画面」左メニューから［サービス情報メンテナンス］－［利用者メンテナンス］をクリックします。



3. ［利用者メンテナンス］画面が表示されます。［以下のサービスを選択しています］で使用中のサービスが選択されていることを確認します。その下に表示される表の［組織名］列に表示されている組織名（特別な場合を除き「本社」と表示されています）のリンクをクリックします。

4. 登録されている利用者の一覧表が表示されます。［▼一括操作］をクリックすると、実行できる一括操作コマンドの一覧が表示されます。［CSV 一括登録］の［実行］ボタンをクリックします。

5. ［CSV 一括登録］ウィンドウがポップアップします。



6. ［CSV ファイル］の［参照］ボタンをクリックして作成した CSV ファイルを選択します。
7. 発行した証明書を管理者が一括ダウンロードする場合は、［発行した証明書は、管理者が一括ダウンロードする］のチェックボックスをチェックします。
8. 以上の入力後［登録］ボタンをクリックします。

情報システム部で端末に証明書をキッティングしたり、MDM で証明書を配布する場合は、管理者側で証明書を一括ダウンロードすることができます。
管理者一括ダウンロードをご利用の場合は、インストール制限機能はご利用いただけません。

9. ［CSV 一括登録受付完了］画面が表示されたら、［閉じる］ボタンをクリックします。

10. 以上で利用者情報の CSV 一括登録は終了になります。利用者登録処理が正常に完了すると管理者宛に「利用者一括登録受付通知」が届きます。エラー等で正常完了できなかった場合は、「利用者一括登録受付エラー通知」が届きます。エラーの原因などが記載されていますので、内容にしたがって、再度、登録作業を行ってください。

11. 利用者登録処理が正常に完了した場合、登録した利用者のメールアドレスに以下の 2 通のメールが送信されます。

   - **電子証明書の「秘密の鍵」を登録してください**
   - **ログイン ID とパスワードのご案内（電子証明書の「秘密の鍵」登録ページ）**

   利用者には、メールの内容にしたがってクライアント証明書をインストールさせてください（クライアント証明書のダウンロード／インストール手順については「利用者マニュアル」をご参照ください）

【補足】発行した証明書を管理者が一括ダウンロードする場合

上記 8 項で［発行した証明書は、管理者が一括ダウンロードする］をチェックして「登録」した場合、利用者にはクライアント証明書のインストールに必要なメールは送信されず、代わりに管理者にクライアント証明書の一括ダウンロード URL がメールで送信されます。

管理者はメールにあるダウンロード URL にアクセスしてクライアント証明書の圧縮ファイルを取得します。ダウンロードしたファイルを解凍すると、各利用者用に以下のファイルがあります。

- クライアント証明書ファイル（「.P12」形式）
- クライアント証明書インストール時に入力するパスワードが記載されたファイル（「.PIN」拡張子のテキストファイル）

クライアント証明書ファイル（「.P12」形式）は該当デバイス上で実行することでインストールが開始されます。インストール途中のパスワード入力では「.PIN」ファイルに記載されているパスワードを入力してください。

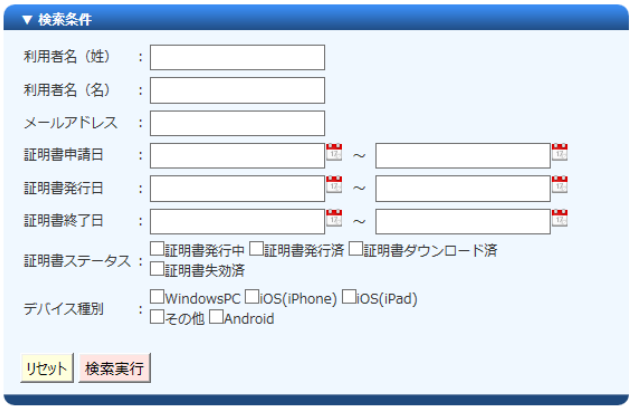
※「iPhone」、「iPad」を選択した場合、「.mobileconfig」というファイルがダウンロードされる場合があります。（販売店様の設定により異なります）

「.mobileconfig」がある場合、「.P12」を使用せず「.mobileconfig」を使用して証明書をインストールしてください。

【補足】クライアント証明書（利用者）を検索する

管理画面では、以下の手順で特定の利用者やクライアント証明書を検索することができます。

1. 「NRA-PKI システム管理画面」左メニューから［サービス情報メンテナンス］－［利用者メンテナンス］をクリックします。
2. ［利用者メンテナンス］画面が表示されます。
3. ［以下のサービスを選択しています］で使用中のサービスが選択されていることを確認します。
4. ［組織名］の列に表示されている組織名（特別な場合を除き「本社」と表示されています）のリンクをクリックします。
5. 登録されている利用者の一覧表が表示されます。
6. ［▼検索条件］をクリックすると、指定できる検索条件の一覧が表示されます。検索条件を指定して、［検索実行］ボタンをクリックします。



【 検索の例 】

［例 1］特定の証明書を失効または再発行する場合の検索

・証明書メールアドレスを［メールアドレス］欄に入力

・デバイス種別を選択

［例 2］来月に更新期限をむかえる証明書を調べる場合の検索

・［証明書終了日］に来月 1 日と末日の日付を入力

［例 3］ダウンロードされていない証明書を調べる場合の検索

・［証明書ステータス］欄で［証明書発行済み］をチェック

4-3 ダウンロードサイトからクライアント証明書を配付する

クライアント証明書の配付をメールではなく専用のダウンロードサイトから行う手順を以下の順序で説明します。本機能はデフォルトでは無効になっておりますので、ご利用を希望される場合は、弊社サポート窓口(support@nrapki.jp)迄お問い合わせください。

- 事前準備
- 利用者情報の登録とクライアント証明書の発行
- 専用のダウンロードサイトからクライアント証明書を配付

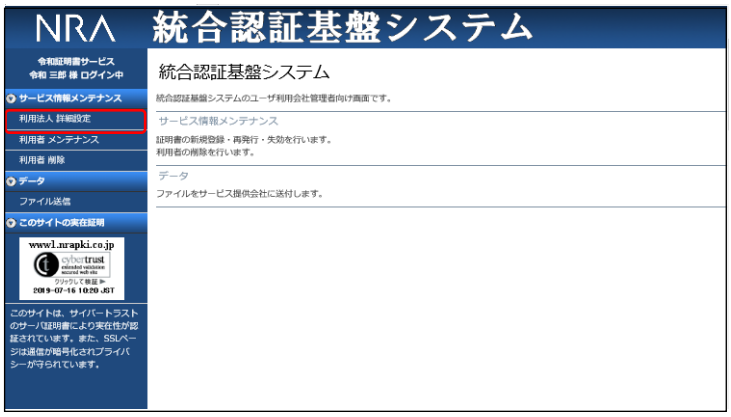
4-3-1 事前準備

事前準備として以下の設定を行います。

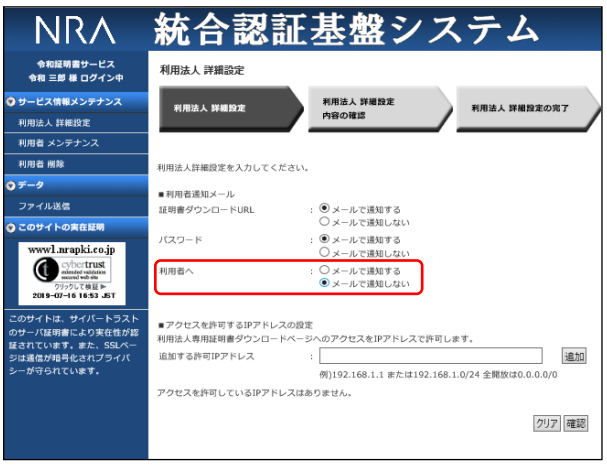
・利用者にクライアント証明書の配付メールを通知しない設定

・専用ダウンロードサイトにアクセスできる IP アドレス制限設定

1. 「NRA-PKI システム管理画面」左メニューから［サービス情報メンテナンス］－［利用法人 詳細設定］をクリックします。

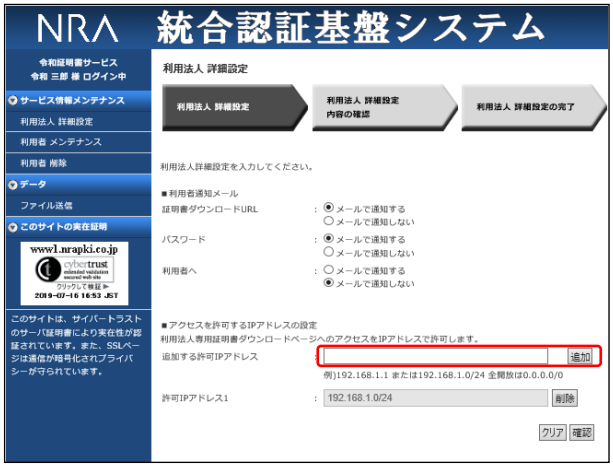


2. 「利用法人 詳細設定」画面が表示されます。「利用者へ」の設定を「メールで通知しない」にします（これにより、利用者にクライアント証明書の配付メールが送信されなくなります）。



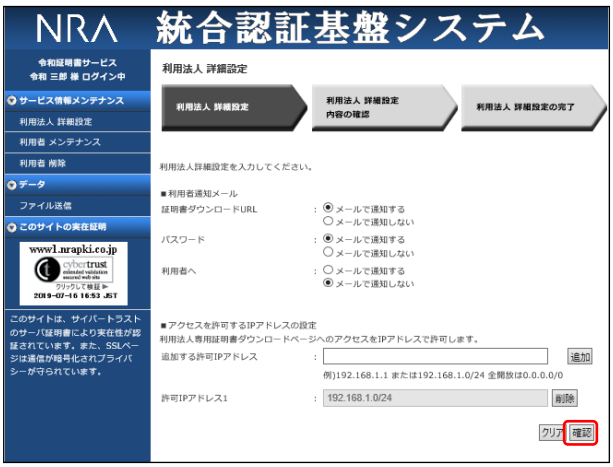
3. 次に専用ダウンロードサイトにアクセスを許可する IP アドレス（もしくはネットワークアドレス）を設定します。「追加する許可 IP アドレス」の例にある形式の IP アドレス（もしくはネットワークアドレス）が設定可能です。すべてのアクセスを許可する場合は「0.0.0.0/0」を設定してください。デフォルトは「すべてアクセス拒否」です。「追加する許可 IP アドレス」に IP アドレス（もしくはネットワークアドレス）を入力し「追加」ボタンをクリックします。

すべての IP アドレスからのアクセスを許可する場合「0. 0. 0. 0/0」が設定可能ですが推奨はしません。

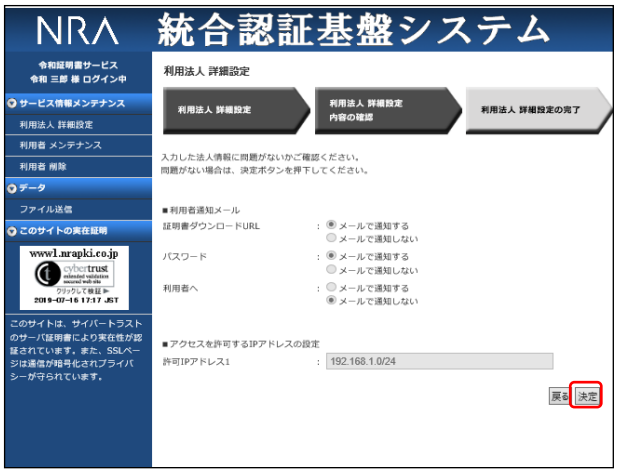


「追加する許可 IP アドレス」に IP アドレス（もしくはネットワークアドレス）を入力し「追加」ボタンをクリックすると、左図のように「許可 IP アドレス」が表示されます。

4. 以上の入力後「利用法人 詳細設定」画面下部にある「確認」ボタンをクリックします。



5. 確認画面が表示されますので、内容を確認したのち［決定］ボタンをクリックします。



以上で事前準備は終了になります。

4-3-2 利用者情報の登録とクライアント証明書の発行

次に利用者情報の登録とクライアント証明書の発行を行います。この手順は先に説明した以下の章と同じになります。以下を参照し実施してください。

- 4-1 利用者情報を登録してクライアント証明書を発行／配付する
- 4-2 利用者情報を CSV で一括登録してｸﾗｲｱﾝﾄ証明書を発行／配付する

4-3-3 専用のダウンロードサイトからクライアント証明書を配付

専用のダウンロードサイトからクライアント証明書を配付するために管理者は「利用者情報の登録とクライアント証明書の発行」後、以下の情報を「NRA-PKI システム管理画面」から取得します。

・クライアント証明書のダウンロードサイト URL

・クライアント証明書をダウンロードするための ID とパスワード

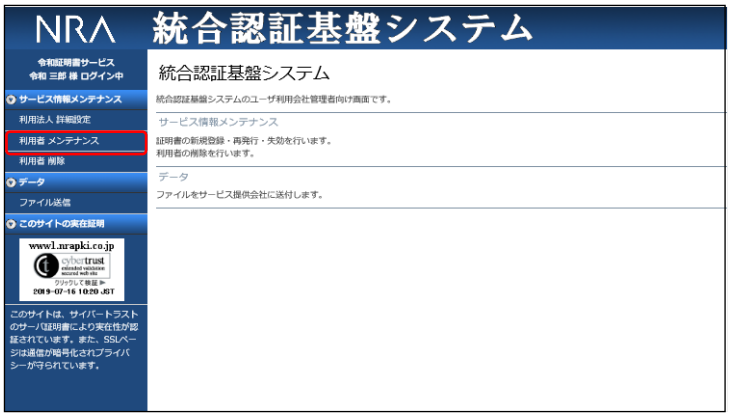
利用者には、ダウンロードサイトの URL とダウンロードするための ID とパスワードを提供しクライアント証明書をインストールさせてください（クライアント証明書ダウンロード後のインストール手順については「利用者マニュアル」をご参照ください）

【補足】クライアント証明書をインストールするときに入力するパスワード

クライアント証明書をインストールするときに入力するパスワード（秘密の鍵）は「ダウンロードするためのパスワード」と同じになります。

【クライアント証明書のダウンロードサイト URL の取得】

1. 「NRA-PKI システム管理画面」左メニューから［サービス情報メンテナンス］－［利用者メンテナンス］をクリックします。



2. ［利用者メンテナンス］画面が表示されます。［以下のサービスを選択しています］で使用中のサービスが選択されていることを確認します。その下に表示される表の［組織名］の列に表示されている組織名（特別な場合を除き「本社」と表示されています）のリンクをクリックします。

3. 登録されている利用者の一覧表が表示されます。[▼一括操作]をクリックし、［証明書ダウンロード画面の表示］の［実行］ボタンをクリックします。

4. 利用法人専用のダウンロードサイト（証明書のダウンロードログイン画面）ウィンドウがポップアップします。

表示されている URL が「クライアント証明書のダウンロードサイト URL」になります。これを利用者に通知します。利用者はこのサイトにアクセスして、このあと説明する ID とパスワードを入力し「ログイン」ボタンをクリックすることでクライアント証明書をダウンロードできます。モバイルデバイスなどでは、QR コードを読み取ることでこのサイトを表示することができます。

【クライアント証明書をダウンロードするための ID とパスワードの取得】

以下の２つの方法があります。

■その１：利用者リストから取得する方法

「利用者メンテナンス」の登録されている利用者の一覧表が表示されている画面で［▼一括操作］をクリックし、［利用者リストダウンロード］の［実行］ボタンをクリックします。

利用者リストの CSV ファイルをダウンロードし Excel でオープンします。次の項目の値がクライアント証明書をダウンロードするための ID とパスワードになります。

- ID　　：証明書メールアドレス（証明書ダウンロード用 ID）
- パスワード：証明書ダウンロード用パスワード

【補足】

利用者リストの CSV ファイルには、ID／パスワード以外にもクライアント証明書の重要な情報がリストされていますので取り扱いに注意してください。

■その２：NRA-PKI パスワード通知書から取得する方法

「利用者メンテナンス」の登録されている利用者の一覧表が表示されている画面で ID／パスワードを取得したい利用者をチェックした後、［▼一括操作］をクリックし、［NRA-PKI パスワード通知書の発行］の［実行］ボタンをクリックします。

「NRA-PKI パスワード通知書（PDF ファイル）」が作成されブラウザでオープンします。「NRA-PKI パスワード通知書（PDF ファイル）」２ページの表にある次の項目の値がクライアント証明書をダウンロードするための ID とパスワードになります。

- ID　　：メールアドレス（ID）欄の値
- パスワード：パスワード欄の値

5. クライアント証明書を失効する

クライアント証明書をインストールしたデバイスの紛失や、使用しなくなった場合は、それらのデバイスにインストールしたクライアント証明書を失効して使用不可にします。

「NRA-PKI システム管理画面」から直接失効する方法と、CSV ファイルを指定してまとめて失効する方法があります。

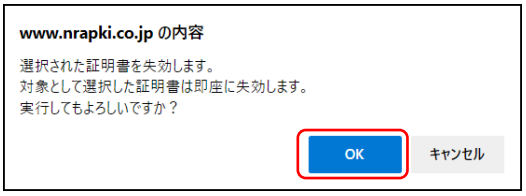
失効した証明書のシリアル番号は失効リスト（CRL）に登録されます。Web サーバーや VPN 装置は失効リストを参照していますので、失効した証明書ではアクセスが拒否されます。

5-1 NRA-PKI システム管理画面からクライアント証明書を失効する

1. 「NRA-PKI システム管理画面」左メニューから［サービス情報メンテナンス］－［利用者メンテナンス］をクリックします。
2. ［利用者メンテナンス］画面が表示されます。
3. ［以下のサービスを選択しています］で使用中のサービスが選択されていることを確認します。
4. ［組織名］の列に表示されている組織名（特別な場合を除き「本社」と表示されています）のリンクをクリックします。
5. 登録されている利用者の一覧表が表示されます。
6. 失効するクライアント証明書の［選択］欄をチェックします（複数の証明書を失効する場合は、複数チェックできます）。
7. ［失効］ボタンをクリックします。

8. ［利用者証明書一括失効］ウィンドウが開き、選択したクライアント証明書の一覧が表示されます。［ただちに、失効する］、［日付を指定して、失効する］のいずれかを選択し［失効］ボタンをクリックします。

9. 確認のメッセージが表示されます。［OK］ボタンをクリックします。



10. 選択したクライアント証明書が失効され、管理者宛に「電子証明書失効通知」が届きます。以上でクライアント証明書の失効処理は終了になります。

失効日を日付で指定したい場合は、［日付を指定して、失効する］を選択して、失効日を指定します。(30 日以内で指定可能)
指定した失効日の午前 0 時ごろにシステムによって自動的に失効されます。

5-2 CSV ファイルを読み込んでクライアント証明書をまとめて失効する

CSV ファイルを指定して、まとめて失効処理を行うことができます。取り扱っているクライアント証明書の数が多い場合は、CSV を使った失効処理のほうが簡単で確実です。

1. 失効処理用の CSV ファイルを作成します。必要なフィールドは以下の 3 フィールドです。

NO	項目名	必須	説明
1	代表メールアドレス	○	利用者のメールアドレスを入力します。
2	利用デバイス用メールアドレス	○	利用デバイス用のメールアドレスを入力します。
3	デバイスコード	○	利用者が使用するデバイスを NRA-PKI で使用するデバイスコードで指定します。

【CSV ファイルの例】

代表メールアドレスと利用デバイス用メールアドレスが同一の場合

```
Yamada-Taro@mytest.jp,Yamada-Taro@mytest.jp,01
```

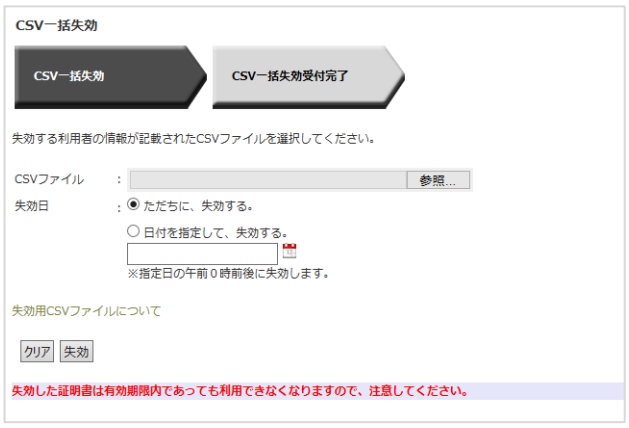
代表メールアドレスと利用デバイス用メールアドレスが別の場合

```
Yamada-Taro@ mytest.jp,nra012@softbank.ne.jp,11
```

2. メニューから［サービス情報メンテナンス］－［利用者メンテナンス］をクリックします。
3. ［利用者メンテナンス］画面が表示されます。
4. ［以下のサービスを選択しています］で使用中のサービスが選択されていることを確認します。
5. ［組織名］の列に表示されている組織名（特別な場合を除き「本社」と表示されています）のリンクをクリックします。

6. 登録されている利用者の一覧表が表示されます。[▼一括操作]をクリックし、［CSV 一括失効］の［実行］ボタンをクリックします。

7. ［CSV 一括失効］ウィンドウが表示されます。



8. ［CSV ファイル］の［参照］ボタンをクリックして、CSV ファイルを指定します。

9. ［ただちに、失効する］、［日付を指定して、失効する］のいずれかを選択し、［失効］ボタンをクリックします。

失効日を日付で指定したい場合は、［日付を指定して、失効する］を選択して、失効日を指定します。(30 日以内で指定可能)
指定した失効日の午前 0 時ごろにシステムによって自動的に失効されます。

10. ［CSV 一括失効受付完了］画面が表示されます。［閉じる］ボタンをクリックしてウィンドウを閉じます。

11. 処理が正常に完了しますと、管理者宛に「利用者一括失効受付通知」が届きます。以上でクライアント証明書の一括失効処理は終了になります。

6. クライアント証明書を再発行する

失効したクライアント証明書を再発行することができます。再発行は、管理画面から失効したクライアント証明書を選択して直接再発行する方法と CSV ファイルを指定してまとめて再発行する方法があります。

失効していないクライアント証明書に対して再発行を行った場合、使用中のクライアント証明書は失効されて新しいクライアント証明書が再発行されます。

6-1 NRA-PKI システム管理画面からクライアント証明書を再発行する

1. 「NRA-PKI システム管理画面」左メニューから［サービス情報メンテナンス］－［利用者メンテナンス］をクリックします。
2. ［利用者メンテナンス］画面が表示されます。
3. ［以下のサービスを選択しています］で使用中のサービスが選択されていることを確認します。
4. ［組織名］の列に表示されている組織名（特別な場合を除き「本社」と表示されています）のリンクをクリックします。
5. 登録されている利用者の一覧表が表示されます。
6. 再発行するクライアント証明書の［選択］欄をチェックします（複数の証明書を再発行する場合は、複数チェックできます）。
7. ［再発行］ボタンをクリックします。

8. ［利用者証明書一括再発行］ウィンドウが開き、選択したクライアント証明書の一覧が表示されます。［ただちに、失効する］、［日付を指定して、失効する］のいずれかを選択し［再発行］ボタンをクリックします。

失効日を日付で指定したい場合は、［日付を指定して、失効する］を選択して、失効日を指定します。(30 日以内で指定可能)
指定した失効日の午前 0 時ごろにシステムによって自動的に失効されます。

【補足】

ご利用のサービスによって、入力項目が異なりますので以下ご確認ください。

■期間指定又は期間+時間指定をご利用の場合

証明書有効期限を入力してください。期間指定は yyyy/mm/dd、期間+時間指定は yyyy/mm/dd hh:mm の形式で入力可能です。

「期間指定又は期間+時間指定」「O、OU 指定」「インストール制限」のサービスはデフォルトではご利用になれません。
ご希望の際は、弊社サポート窓口(support@nrapki.jp)迄お問い合わせください。

■O、OU 指定をご利用の場合

O、OU の値を変更して再発行する場合は、下図の赤枠部分を変更後に［再発行］ボタンをクリックしてください。

■インストール制限をご利用の場合

インストール制限の設定を変更して再発行する際は、下図の赤枠部分を変更後に［再発行］ボタンをクリックしてください。

利用デバイス制限

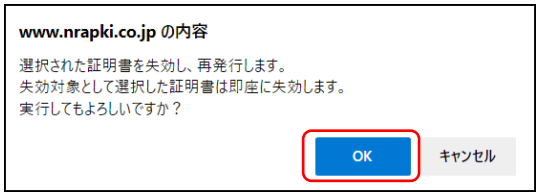
・制限なし
インストール時の制限無し

・どれかの条件と一致（OR）
入力した制限項目が 1 つ以上一致した端末のみインストール可能

・すべての条件と一致（AND）
入力した制限項目すべて一致した端末のみインストール可能

MAC アドレスは、ハイフン”-“、コロン”:”を省略した 12 桁の 16 進数（0～F）で入力してください。

9. 確認メッセージが表示されます。［OK］ボタンをクリックします。



10. 選択したクライアント証明書が再発行され、管理者宛に「電子証明書再発行通知」が届きます。以上でクライアント証明書の再発行処理は終了になります。

失効していない証明書に対して再発行を行った場合は、使用中の証明書は自動的に失効されます。

6-2 CSV ファイルを読み込んでｸﾗｲｱﾝﾄ証明書をまとめて再発行する

CSV ファイルを指定して、まとめてクライアント証明書の再発行を行うことができます。取り扱っているクライアント証明書の数が多い場合は、CSV を使った再発行のほうが簡単で確実です。

1. 再発行用の CSV ファイルを作成します。必要なフィールドは以下のフィールドです。

NO	項目名	必須	説明
1	代表メールアドレス	○	利用者のメールアドレスを入力します。
2	利用デバイス用メールアドレス	○	利用デバイス用のメールアドレスを入力します。
3	デバイスコード	○	利用者が使用するデバイスを NRA-PKI で使用するデバイスコードで指定します。
4	証明書有効期限(From)	-	入力の必要はありません。期間指定又は期間+時間指定の証明書を契約している場合にのみ有効です。
5	証明書有効期限(To)	-	入力の必要はありません。期間指定又は期間+時間指定の証明書を契約している場合にのみ有効です。

期間指定又は期間+時間指定の証明書をご利用の場合は、［証明書有効期限（From）］と［証明書有効期限（To）］は必須項目となります。

期間指定は yyyy/mm/dd 形式、期間+時間指定は yyyy/mm/dd hh:mm 形式で指定してください。

【入力例】
期間指定の場合　2020/01/01
期間+時間指定の場合　2020/01/01 10:00

未指定の場合は、証明書発行日が開始日となります。

【CSV ファイルの例】

```
Yamada-Taro@mytest.jp,Yamada-Taro@mytest.jp,01
```

■O、OU 指定をご利用の場合

NO	項目名	必須	説明
1	代表メールアドレス	○	利用者のメールアドレスを入力します。
2	利用デバイス用メールアドレス	○	利用デバイス用のメールアドレスを入力します。
3	Organization	-	Organization を入力します。
4	OrganizationUnit1	-	OrganizationUnit1 を入力します。
5	OrganizationUnit2	-	OrganizationUnit2 を入力します。
6	デバイスコード	○	利用者が使用するデバイスを NRA-PKI で使用するデバイスコードで指定します。
7	証明書有効期限(From)	-	入力の必要はありません。期間指定又は期間+時間指定の証明書を契約している場合にのみ有効です。
8	証明書有効期限(To)	-	入力の必要はありません。期間指定又は期間+時間指定の証明書を契約している場合にのみ有効です。

No.3~5 のすべてに値を設定しない場合は、ひとつ前に発行された証明書と同じ値のサブジェクト組織名（O）、組織単位名（OU）で新しい証明書を発行します。

期間指定又は期間+時間指定の証明書をご利用の場合は、［証明書有効期限（From）］と［証明書有効期限（To）］は必須項目となります。

期間指定は yyyy/mm/dd 形式、期間+時間指定は yyyy/mm/dd hh:mm 形式で指定してください。

【入力例】
期間指定の場合　2020/01/01
期間+時間指定の場合　2020/01/01 10:00

未指定の場合は、証明書発行日が開始日となります。

【CSV ファイルの例】

```
Yamada-Taro@mytest.jp,Yamada-Taro@mytest.jp,o,ou1,ou2,01
```

■インストール制限をご利用の場合

NO	項目名	必須	説明
1	代表メールアドレス	○	利用者のメールアドレスを入力します。
2	利用デバイス用メールアドレス	○	利用デバイス用のメールアドレスを入力します。
3	デバイスコード	○	利用者が使用するデバイスを NRA-PKI で使用するデバイスコードで指定します。
4	証明書有効期限(From)	-	入力の必要はありません。期間指定又は期間+時間指定の証明書を契約している場合にのみ有効です。
5	証明書有効期限(To)	-	入力の必要はありません。期間指定又は期間+時間指定の証明書を契約している場合にのみ有効です。
6	インストール端末制限	-	インストール制限における制限項目一致条件を指定します。 [0] 制限なし [1] 制限項目のどれかと一致(OR 一致) [2] 制限項目のすべてと一致(AND 一致)
7	端末制限項目① MAC アドレス	-	インストールを許可する端末の MAC アドレスを入力します。ハイフン"-"、コロン":"を除いた 12 桁の 16 進数(0～F)で指定してください。
8	端末制限項目② コンピュータ名	-	インストールを許可する端末のコンピュータ名を入力します。
9	端末制限項目③ ログインユーザ名	-	インストールを許可するログインユーザ名を入力します。
10	端末制限項目④ 端末(BIOS)シリアル番号	-	インストールを許可する端末の(BIOS)シリアル番号を入力します。

【CSV ファイルの例】

```
Yamada-Taro@mytest.jp,Yamada-Taro@mytest.jp,01,,,1,1234567890ab,hosttest,山田太郎,bbbbbbbbbbbb
```

期間指定又は期間+時間指定の証明書をご利用の場合は、［証明書有効期限（From）］と［証明書有効期限（To）］は必須項目となります。

期間指定は yyyy/mm/dd 形式、期間+時間指定は yyyy/mm/dd hh:mm 形式で指定してください。

【入力例】
期間指定の場合　2020/01/01
期間+時間指定の場合　2020/01/01 10:00

未指定の場合は、証明書発行日が開始日となります。

現在発行されている証明書と同様の条件でインストールを制限する場合、No.6~10 は省略可能です。

No.6 を指定し No.7~10 の値を未指定にした場合、未指定の項目は制限項目に含まれません。

■ O、OU 指定+インストール制限をご利用の場合

NO	項目名	必須	説明
1	代表メールアドレス	○	利用者のメールアドレスを入力します。
2	利用デバイス用メールアドレス	○	利用デバイス用のメールアドレスを入力します。
3	Organization	-	Organization を入力します。
4	OrganizationUnit1	-	OrganizationUnit1 を入力します。
5	OrganizationUnit2	-	OrganizationUnit2 を入力します。
6	デバイスコード	○	利用者が使用するデバイスを NRA-PKI で使用するデバイスコードで指定します。
7	証明書有効期限(From)	-	入力の必要はありません。期間指定又は期間+時間指定の証明書を契約している場合にのみ有効です。
8	証明書有効期限(To)	-	入力の必要はありません。期間指定又は期間+時間指定の証明書を契約している場合にのみ有効です。
9	インストール端末制限	-	インストール制限における制限項目一致条件を指定します。 [0] 制限なし [1] 制限項目のどれかと一致(OR 一致) [2] 制限項目のすべてと一致(AND 一致)
10	端末制限項目① MAC アドレス	-	インストールを許可する端末の MAC アドレスを入力します。ハイフン"-"、コロン":"を除いた 12 桁の 16 進数(0～F)で指定してください。
11	端末制限項目② コンピュータ名	-	インストールを許可する端末のコンピュータ名を入力します。
12	端末制限項目③ ログインユーザ名	-	インストールを許可するログインユーザ名を入力します。
13	端末制限項目④ 端末(BIOS)シリアル番号	-	インストールを許可する端末の(BIOS)シリアル番号を入力します。

【CSV ファイルの例】

```
Yamada-Taro@mytest.jp,Yamada-Taro@mytest.jp,,,,01,,,1,1234567890ab,hosttest,山田太郎,bbbbbbbbbbbb
```

No.3~5 のすべてに値を設定しない場合は、ひとつ前に発行された証明書と同じ値のサブジェクト組織名（O）、組織単位名（OU）で新しい証明書を発行します。

期間指定又は期間+時間指定の証明書をご利用の場合は、［証明書有効期限（From）］と［証明書有効期限（To）］は必須項目となります。

期間指定は yyyy/mm/dd 形式、期間+時間指定は yyyy/mm/dd hh:mm 形式で指定してください。

【入力例】
期間指定の場合　2020/01/01
期間+時間指定の場合　2020/01/01 10:00

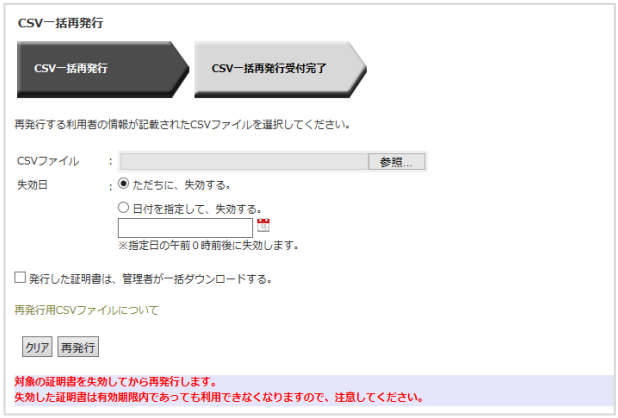
未指定の場合は、証明書発行日が開始日となります。

現在発行されている証明書と同様の条件でインストールを制限する場合、No.9~13 は省略可能です。

No.9 を指定し No.10~13 の値を未指定にした場合、未指定の項目は制限項目に含まれません。

2. メニューから［サービス情報メンテナンス］－［利用者メンテナンス］をクリックします。
3. ［利用者メンテナンス］画面が表示されます。
4. ［以下のサービスを選択しています］で使用中のサービスが選択されていることを確認します。
5. ［組織名］の列に表示されている組織名（特別な場合を除き「本社」と表示されています）のリンクをクリックします。
6. 登録されている利用者の一覧表が表示されます。[▼一括操作]をクリックし、［CSV 一括再発行］の［実行］ボタンをクリックします。

7. ［CSV 一括再発行］ウィンドウが表示されます。



8. ［CSV ファイル］の［参照］ボタンをクリックして、CSV ファイルを指定します。
9. ［ただちに、失効する］、［日付を指定して、失効する］のいずれかを選択し、［再発行］ボタンをクリックします。

失効日を日付で指定したい場合は、［日付を指定して、失効する］を選択して、失効日を指定します。(30 日以内で指定可能)
指定した失効日の午前 0 時ごろにシステムによって自動的に失効されます。

10. ［CSV 一括再発行受付完了］画面が表示されます。［閉じる］ボタンをクリックしてウィンドウを閉じます。

11. 処理が正常に完了しますと、管理者宛に「利用者一括再発行受付通知」が届きます。以上でクライアント証明書の一括再発行処理は終了になります。

7. 利用者を削除する

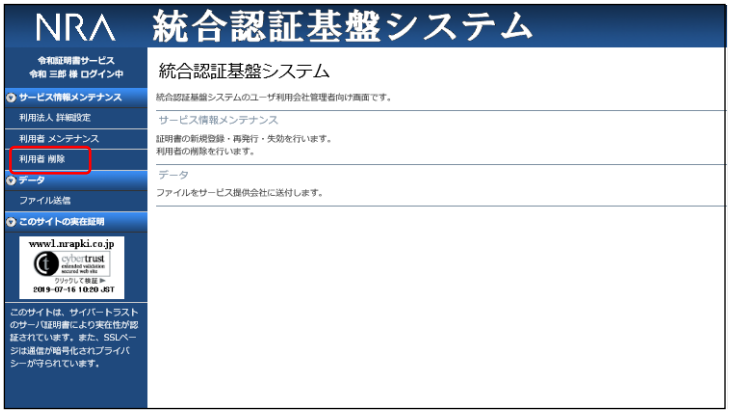
登録した利用者の情報に誤り（スペルミス等）があった場合や、サービスを利用していない利用者を削除してライセンス数を管理することができます。

利用者を完全に削除するには、「1 次削除」「2 次削除」と 2 段階の操作が必要となります。

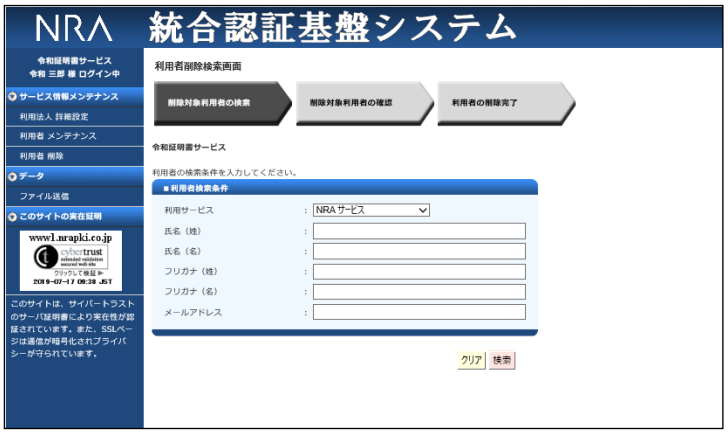
2 次削除まで完了しますと、利用者の証明書がすべて失効され、利用者情報が一覧から削除されます。

7-1 利用者を 1 次削除する

1. 「NRA-PKI システム管理画面」左メニューから［サービス情報メンテナンス］－［利用者 削除］をクリックします。

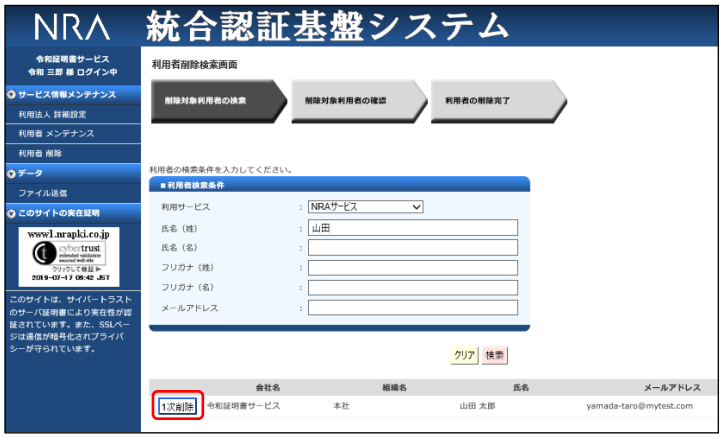


2. ［利用者削除検画面］が表示されます。



サービス提供会社によって、電子証明書の新規発行を利用会社管理者に許可していない場合があります。その場合、［利用者 削除］をクリックしても「利用者追加削除が許可されたサービスが存在しません。」とのメッセージが表示され、利用者の削除はできません。

3. ［利用サービス］で使用中のサービスが選択されていることを確認します。
4. 検索条件を指定して、［検索］ボタンをクリックします。
5. 検索条件に該当する利用者の一覧表が表示されます。削除したい利用者の［1次削除］ボタンをクリックします



6. ［利用者 1 次削除確認画面］が表示されます。削除したい利用者情報が表示されていることを確認して［決定］ボタンをクリックします。

7. 確認のメッセージが表示されます。［OK］をクリックします。
8. ［利用者 1 次削除完了画面］が表示され、管理者宛に「利用者 1 次削除通知」が届きます。以上で利用者の 1 次削除は終了になります。づづけて 2 次削除を実施します。

7-2 利用者を 2 次削除する

1. 1 次削除と同様に「NRA-PKI システム管理画面」左メニューから［サービス情報メンテナンス］－［利用者 削除］をクリックします。
2. ［利用者削除検画面］が表示されます。
3. ［利用サービス］で使用中のサービスが選択されていることを確認します。
4. 検索条件を指定して、［検索］ボタンをクリックします。
5. 検索条件に該当する利用者の一覧表が表示されます。削除したい利用者の［2 次削除］ボタンをクリックします

6. ［利用者 2 次削除確認画面］が表示されます。削除対象の利用者情報が表示されていることを確認して［決定］ボタンをクリックします。

7. 確認のメッセージが表示されます。［OK］をクリックします。

サービス提供会社によって、電子証明書の新規発行を利用会社管理者に許可していない場合があります。その場合、［利用者 削除］をクリックしても「利用者追加削除が許可されたサービスが存在しません。」とのメッセージが表示され、利用者の削除はできません。

トップ画面にも［利用者 2 次削除待ち一覧］が表示されます。

誤って削除対象ではない利用者を 1 次削除していた場合、［1 次削除を解除する］ボタンをクリックすると解除されます。

8. ［利用者 2 次削除完了画面］が表示され、管理者宛に「利用者マスター削除通知」が届きます。以上で利用者の削除は終了になります。

以上