UPKI電子証明書発行サービス アップデート

2016年5月26日 学術情報基盤オープンフォーラム2016

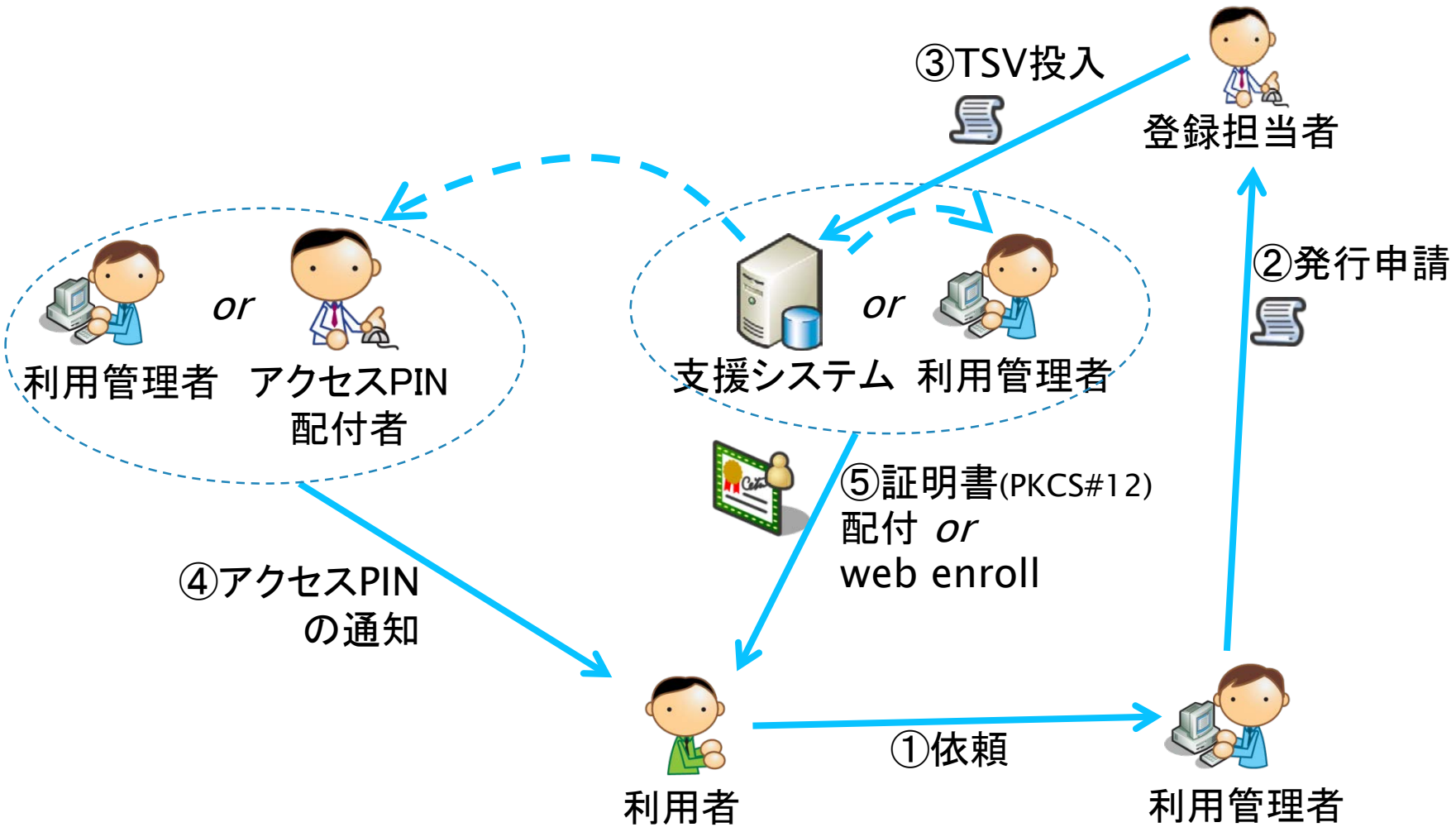
国立情報学研究所　西村 健

目次

この1年の証明書サービス関連の話題を取り上げます。

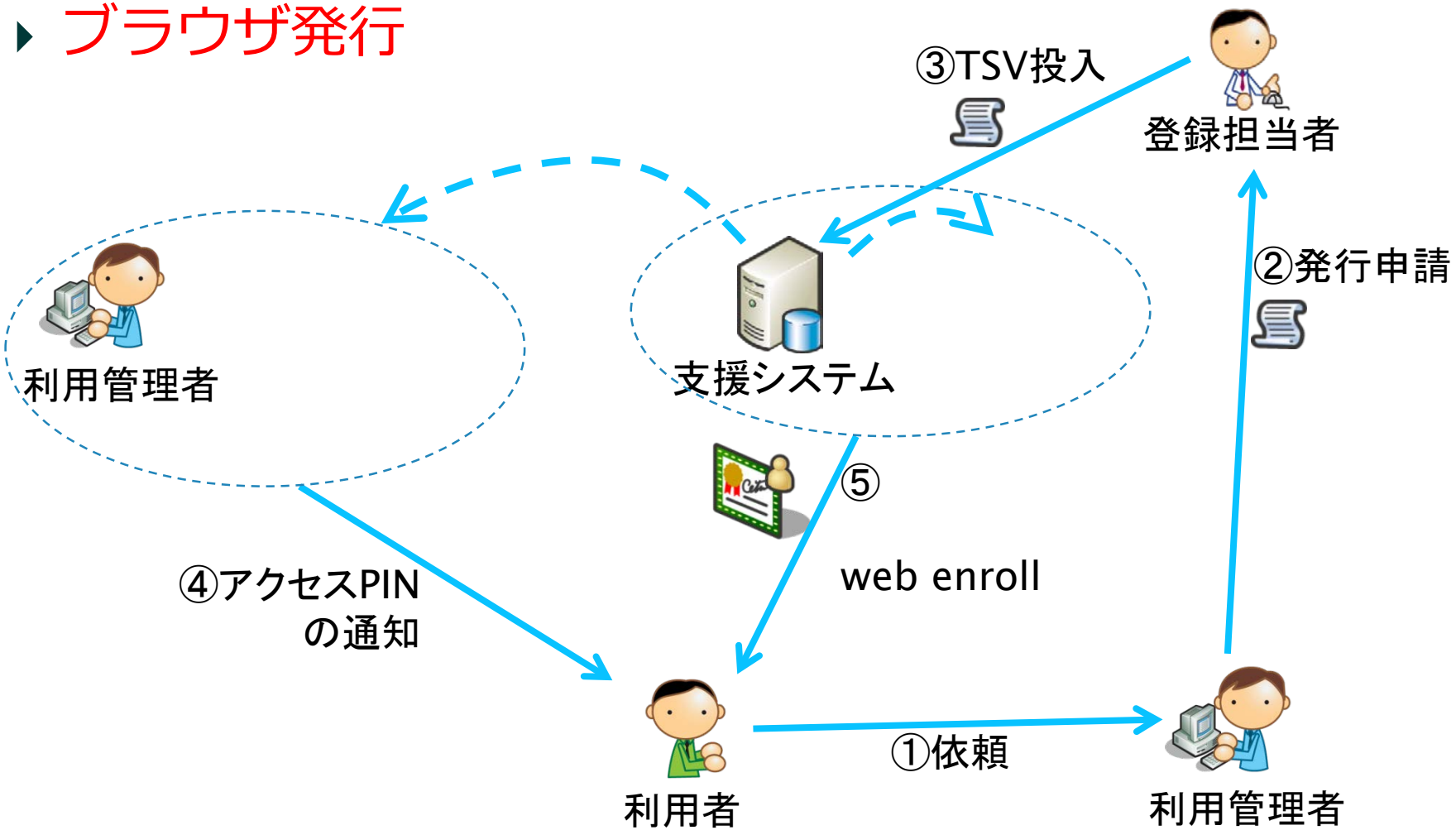
- クライアント証明書発行対象の拡充
- TSV作成ツールリニューアル
- Windows 10対応状況
- SHA-1証明書発行終了
- その他

クライアント証明書発行フロー概要



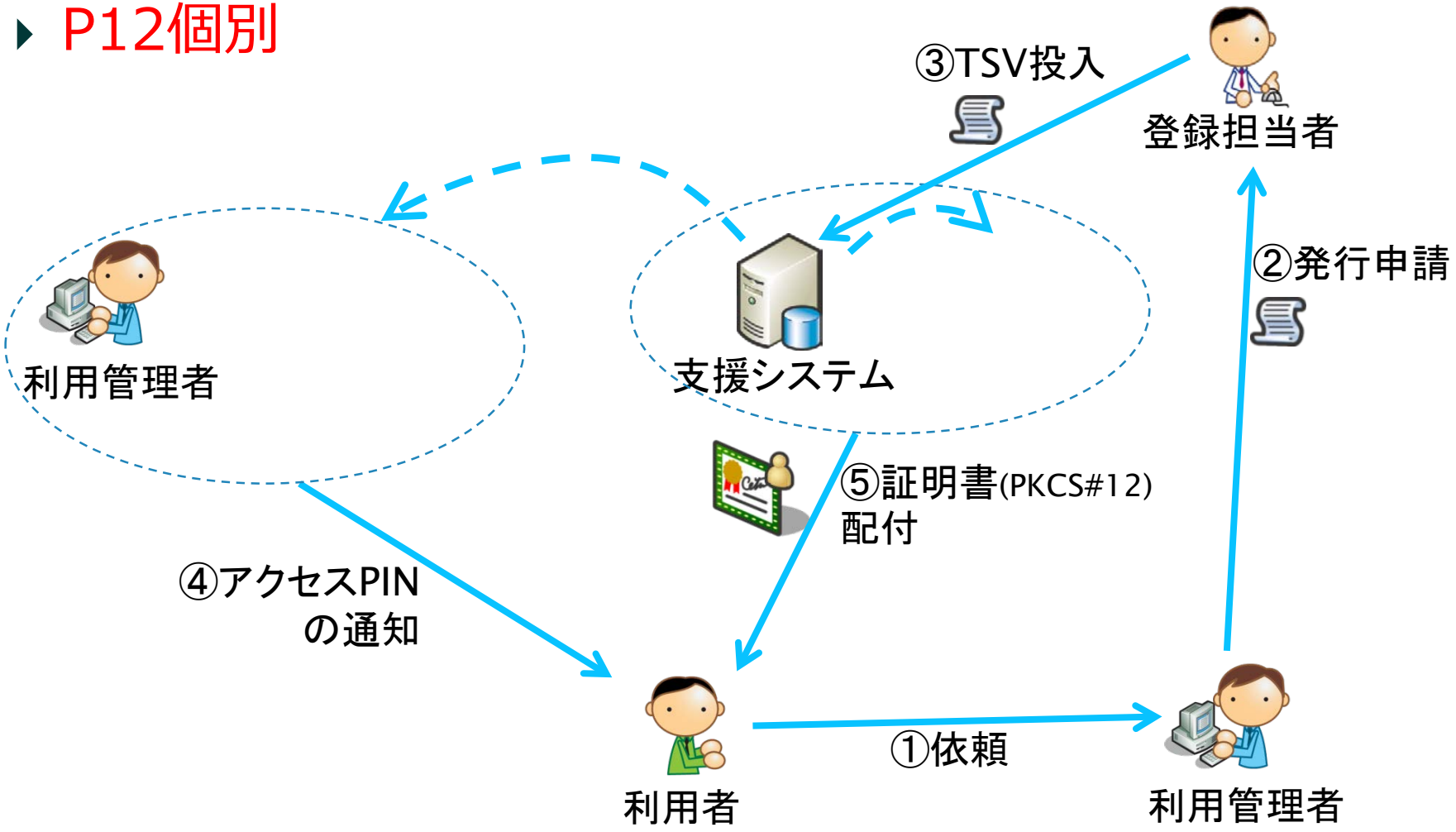
クライアント証明書発行フロー概要

- ブラウザ発行



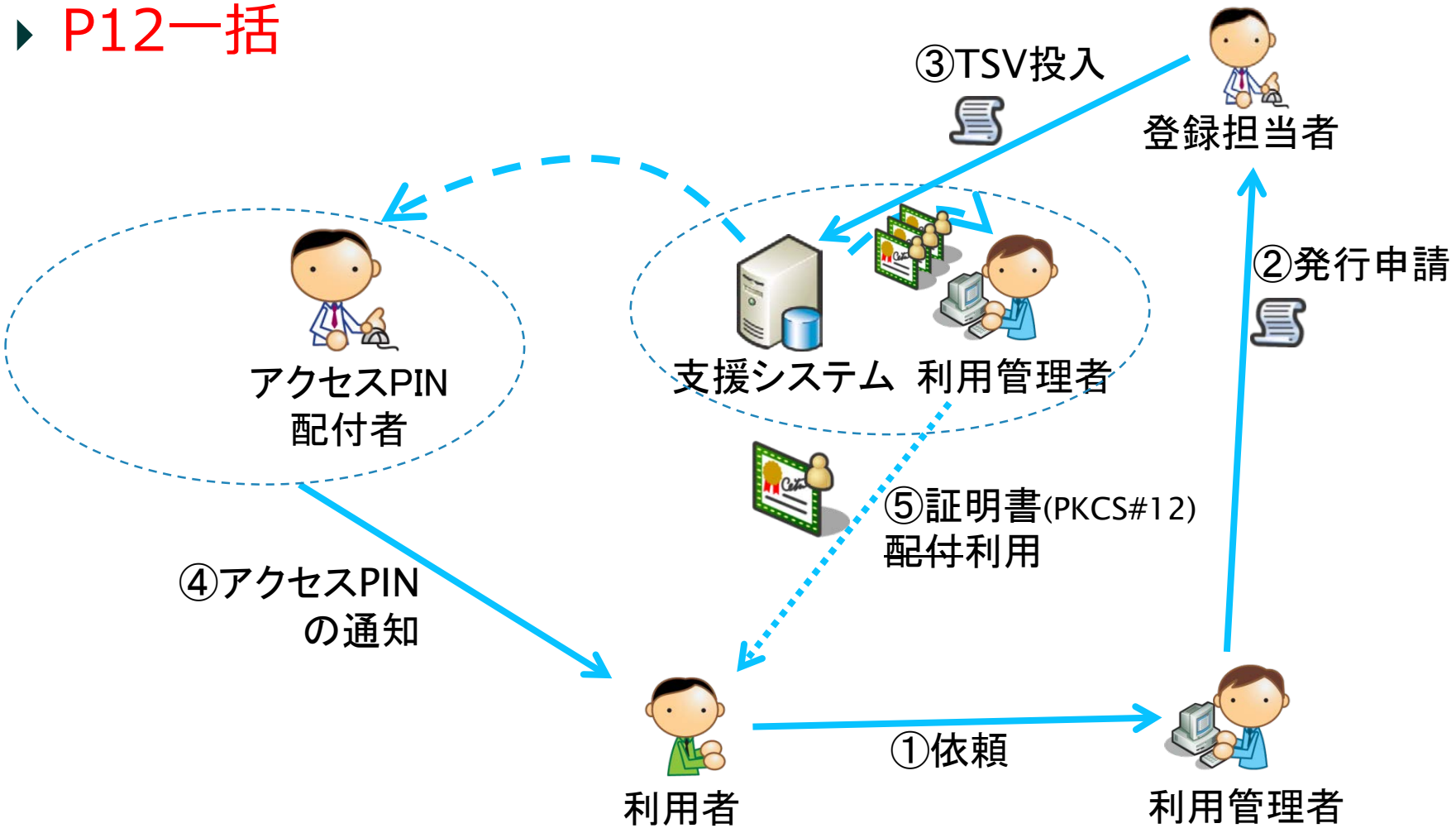
クライアント証明書発行フロー概要

- P12個別



クライアント証明書発行フロー概要

- P12一括



クライアント証明書発行対象の拡充

- クライアント証明書を利用しやすくするために、 CP（Certificate Policy：証明書ポリシ）を改訂いたしました
  - 2016年3月15日公開
  - 主な変更点
    - これまでは個人を対象としてしか発行できなかったものが、役職、組織（課や係など）を対象として発行できる
    - 当該機関に所属する者にしか発行出来なかったものが、たとえば業務委託や派遣の職員にも発行できる
- サービス利用機関においては、上記のような対象に発行したい場合、このための審査基準・手順を作成していただく必要があります
  - 発行対象は、たしかにその機関に実在するか
    - 実在することが客観的に証明できますか？信頼できるソースを探してください
  - 証明書の発行を申請した者は、たしかにその発行対象で間違いないか
    - ご本人からの申請ですか？なりすましではありませんか？

クライアント証明書発行対象 (新CPより)

- 利用者になれる人
  - 学術機関に所属する者

    もしくは
  - 学術機関が認めた役職、組織（係、班や課などを単位とするもの）

    もしくは
  - 学術機関が認めた、業務上証明書が必要な者

- コモンネーム（CN）に記載できる内容
  - 利用者氏名
  - 利用者識別子（文字列や数字）
  - 利用者に含まれる組織名
  - 利用者に含まれる役職名
  - 組織内のさまざまな部門名

ユースケース

- 学術基盤課長としてログイン（クライアント認証）する
  - 人が変わっても同じ証明書を引き継いで使い続けられる
- サービス窓口（実際はML）を差出人としてS/MIME署名する
  - 暗号化まで考慮すると同じ証明書・秘密鍵を共有するしかない
- 学内システムのシステム保守業者にログイン（クライアント認証）させる

（仮想の）運用例

例で考えます

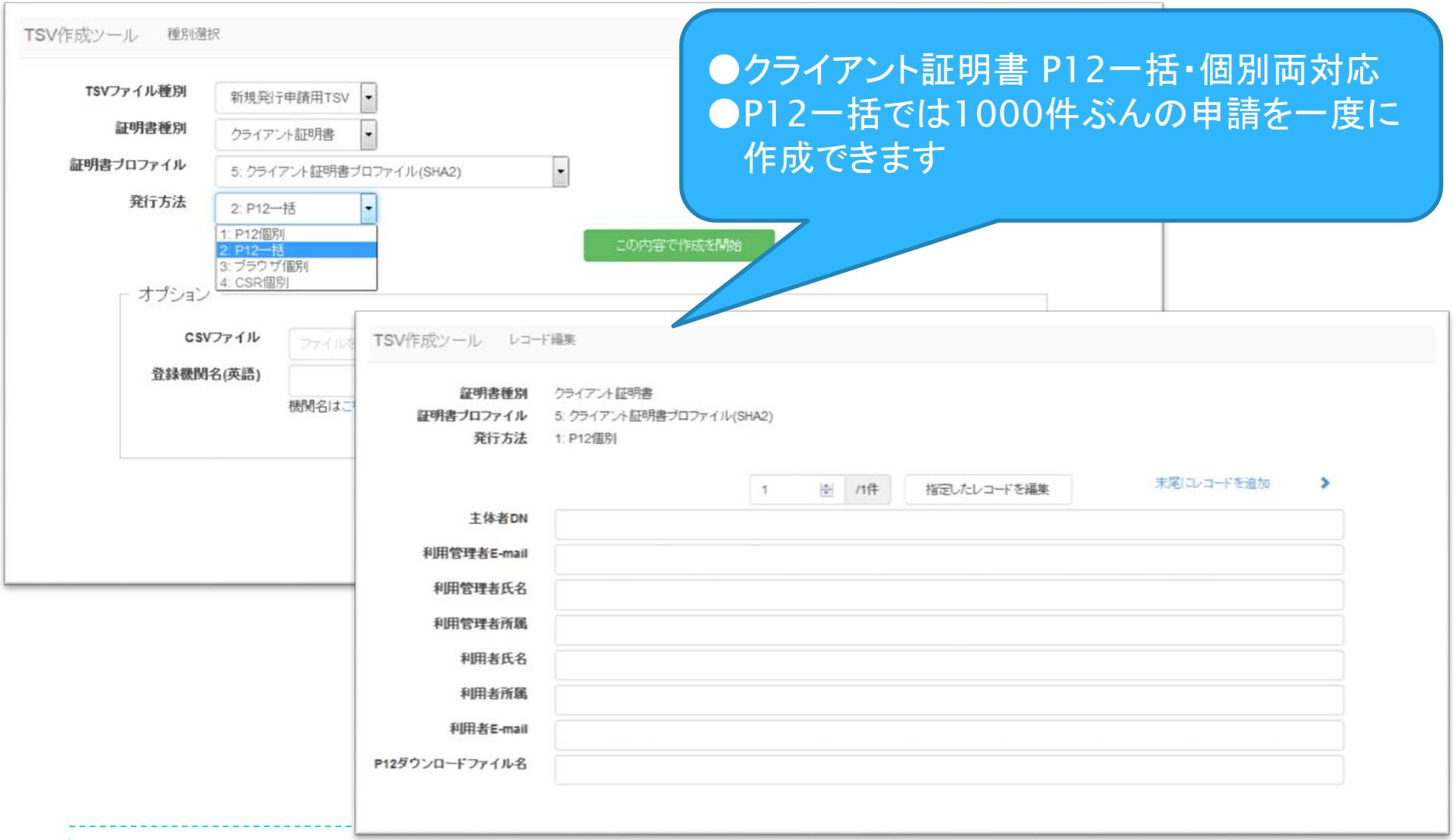
- 発行対象: 認証推進室
  - DN: CN=Academic Authentication Systems Office, …
  - 室の実在性、メンバーは企画課が把握している
  - 室の本人性は室長に確認
  - 申請TSV上の利用者も認証推進室とし、P12個別で発行
  - 室長が証明書取得手続きを行った後、取得した証明書および秘密鍵を共有する

- OUに1、２、３、…等付けてDNを区別すれば、発行対象を同じくしてメンバーそれぞれに別の証明書を発行することも可能です。ご検討ください。

TSV作成ツールリニューアル

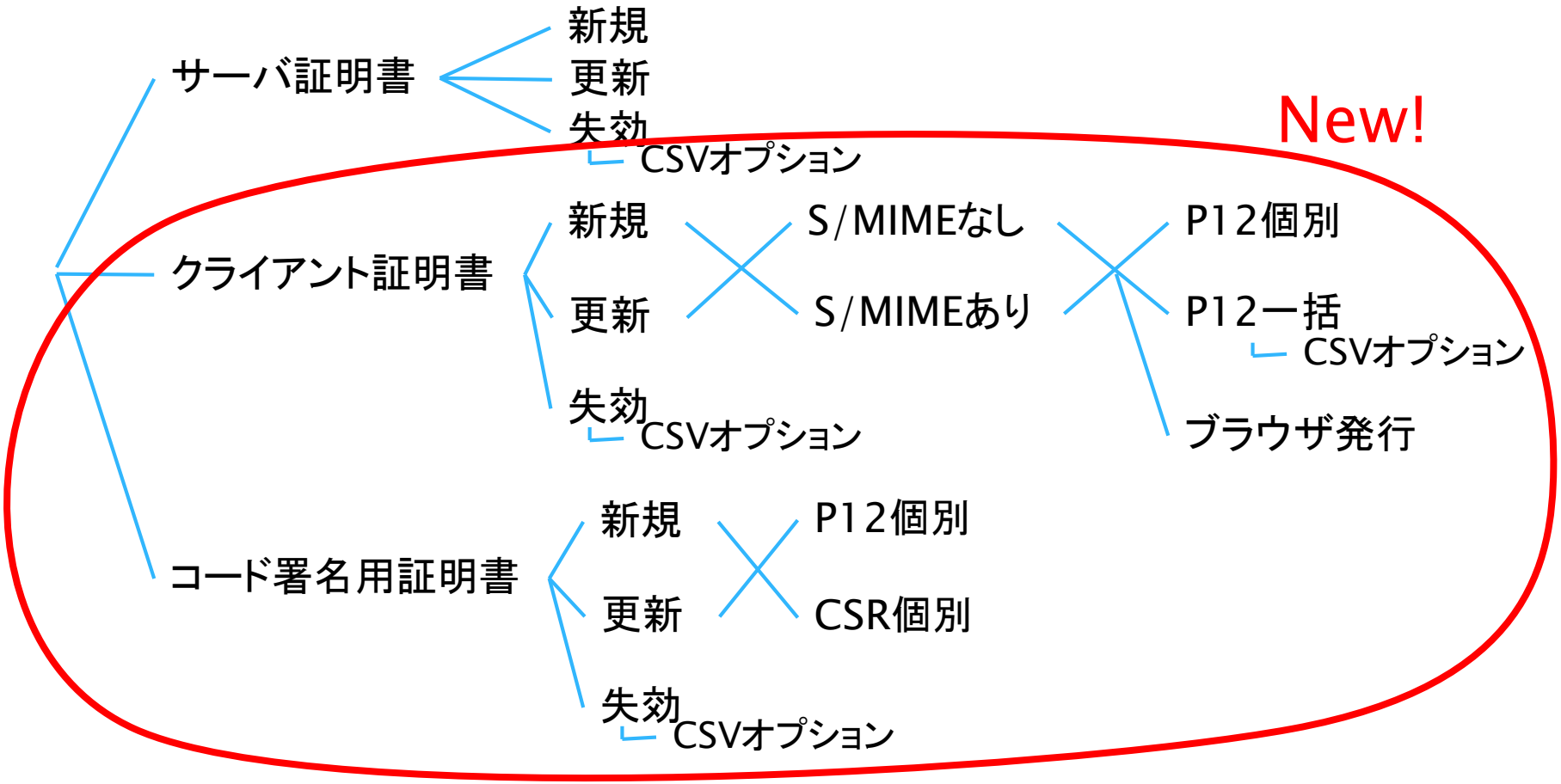
- 新TSV作成ツールの提供を開始しました
  - https://certs.nii.ac.jp/tsv-tool/
  - これまではサーバ証明書発行・更新・失効申請用TSVファイル作成のみでの提供でした
  - 新版ではクライアント証明書とコード署名用証明書の各申請用TSVファイル作成にも対応しました
  - ソースコードを Apache License 2.0 で提供します
    - サービス利用機関が機関内利用管理者向けにカスタマイズして提供することもできます

TSV作成ツール 画面


TSV作成ツール　種別選択
TSVファイル種別
新規発行申請用TSV
証明書種別
クライアント証明書
証明書プロファイル
5: クライアント証明書プロファイル(SHA2)
発行方法
2: P12一括
1: P12個別
2: P12一括
3: ブラウザ個別
4: CSR個別
この内容で作成を開始
オプション
CSVファイル
登録機関名(英語)
●クライアント証明書 P12一括・個別両対応
●P12一括では1000件ぶんの申請を一度に作成できます
TSV作成ツール　レコード編集
証明書種別　クライアント証明書
証明書プロファイル　5: クライアント証明書プロファイル(SHA2)
発行方法　1: P12個別
1
/1件
指定したレコードを編集
末尾にレコードを追加
主体者DN
利用管理者E-mail
利用管理者氏名
利用管理者所属
利用者氏名
利用者所属
利用者E-mail
P12ダウンロードファイル名

TSV作成ツールで作成できる申請TSV

- 本サービスで扱う申請TSVを網羅的に対応



- ※情報更新申請TSVは未対応

TSV作成ツール: CSVオプション

- 必要最小限の情報をCSV形式で用意し共通項を入力すれば、容易に申請TSVが作成できます
  - 用意するCSVの例（クライアント証明書P12一括発行）：

p12bulkissue.csv								
CN	OU	利用者氏名	P12DLファイル名	利用者所属	利用者mail	利用管理者氏名	利用管理者所属	利用管理者mail
Mitsuhide Akechi	06T0731M	明智光秀	p12-download-file-name	テスト学部TSV課	akechi@example.ac.jp	管理太郎	テスト部管理課	tsv-test-admin@example.ac.jp

Windows 10 対応状況

- Windows 10搭載のInternet Explorer 11 及び Microsoft Edge を用いて検証を実施しました
  - 可能な操作
    - サーバ証明書の検証
    - 各証明書のダウンロード
    - 発行済みの証明書を用いたクライアント認証
  - Edgeでのみ不可能な操作
    - クライアント証明書 ブラウザ発行 / 登録担当者用証明書の取得
- Edgeでは、クライアント証明書のブラウザ発行ができません
- Windows10の対応状況については、随時ウェブサイト(https://certs.nii.ac.jp)でお知らせしていきます

サポート外

どうしても Edge が使いたいのですが…

- 前述の通り証明書取得の問題なので、この部分のみIEで代行すれば利用可能と思われます
  - P12個別であればマニュアルそのまま
  - 同様の理屈はWindows版ChromeやOperaにもあてはまります
- 取得をFirefoxで行えばSafariでもなんとか
  - 以前のSafariはクライアント証明書の扱いに難がありました

SHA-1を使用したサーバ証明書について

- CAブラウザフォーラムにて、SHA-1を利用したサーバ証明書の発行期限および利用期限が策定されました
  - 発行期限　：2015年12月31日まで
  - 利用期限　：2016年12月31日まで
- UPKIのSHA-1証明書の発行も、2015年末で終了しました
- すでにChromeでは…

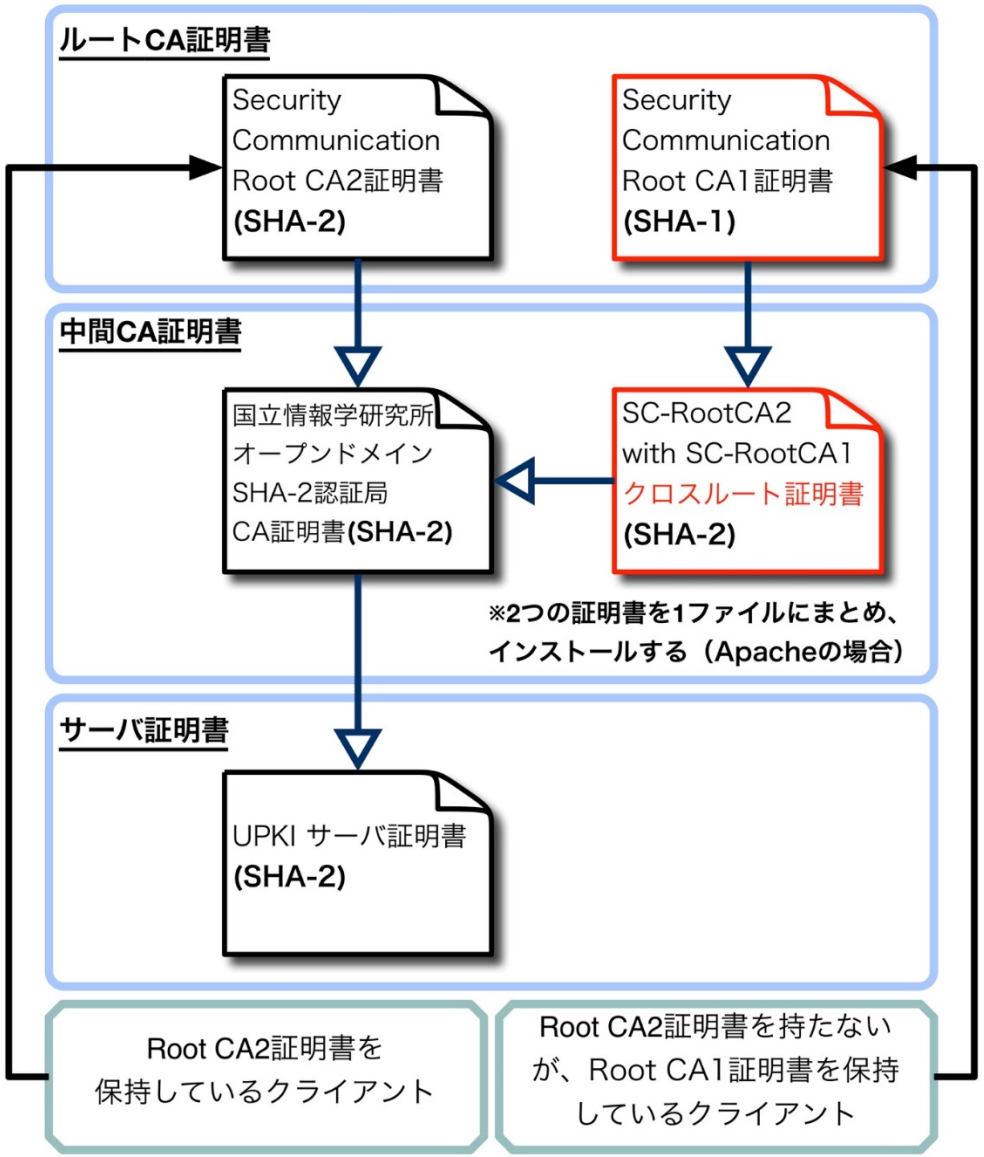
- **安全を示す錠アイコンが出ない**（もちろんEVの緑にもならない）
- IE/Edgeも追従予定(*)
- お早めにSHA-2への移行をすすめてくださいますようお願いします

(*) – https://blogs.technet.microsoft.com/jpsecurity/2016/05/06/sha-1_deprecation_roadmap/

SHA-1証明書並のカバー範囲をSHA-2証明書で：クロスルート証明書

- SHA-1 のルート証明書で署名した SHA-2 認証局証明書(SC-RootCA2 with SC-RootCA1クロスルート証明書)を提供開始しました
  - SHA-2証明書を使いたいがカバー範囲が心配、という場合に、少しでもカバー範囲を広くすることができます
  - SHA-1の認証局情報のみを保持している端末を、SHA-2証明書を使用する環境に対応させたい場合に利用できます
  - SHA-2アルゴリズム自体に非対応の端末は対象外
- カバー範囲
  - スマートフォン
    - Windows phone ver7以上
    - Android ver1.5以上
    - iOS ver2.0以上
    - BlackBerry ver.5.0以上
  - フィーチャーフォン
    - 一覧を下記URLに掲載しております

https://certs.nii.ac.jp/cross-root/



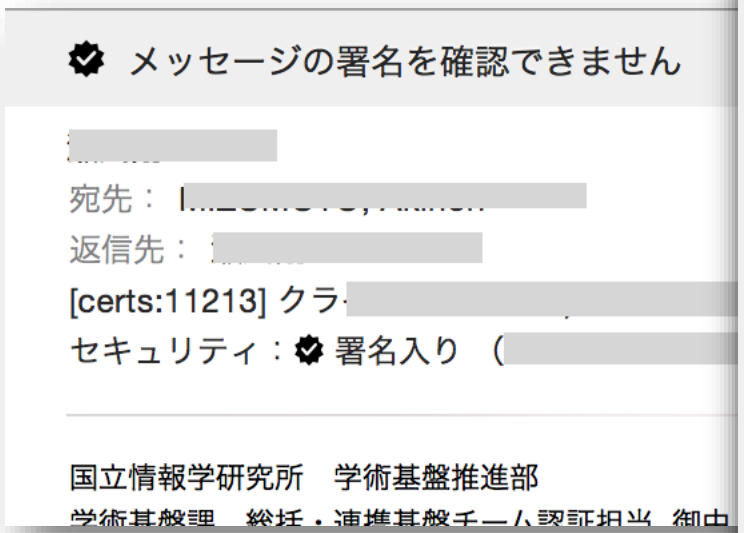
クロスルート証明書は時機を見てはずしてください

- そのままにしていると危険（？）
  - https://knowledge.symantec.com/jp/support/ssl-certificates-support/index?page=content&id=ALERT2009
  - 詳細は不明ながら、将来SHA-1ルートCAがトラストアンカーから除かれるタイミングで署名検証に失敗するようになる可能性があります
  - 安全側に倒せばクロスルートを解除しておくのが無難です

その他

S/MIMEメールアドレスは大文字小文字を揃えてください

- メールソフトに設定されている差出人メールアドレスとS/MIME証明書に設定するメールアドレスの大文字小文字を揃えてください。
- そうでなければ一部メールソフトで問題になる可能性があります

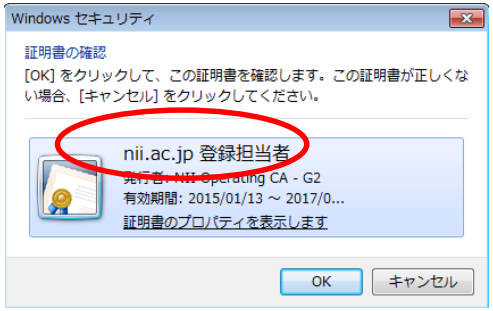


Windows転送ツール問題

- Windows転送ツール、もしくは以下でMicrosoftより案内されている「引越しExpress」ツールは、正常に秘密鍵を移行できないことが確認されております
- これらのツールを使うご予定の方でクライアント証明書をお持ちの方は、別途手順に従って秘密鍵のエクスポート・インポートを行うようにしてください
  - エクスポート: ブラウザ発行マニュアルの4. http://id.nii.ac.jp/1344/00000010/
  - インポート: 各Webブラウザへのインストールマニュアル https://certs.nii.ac.jp/archive/manuals/#_698
- http://windows.microsoft.com/ja-jp/windows-10/windows-easy-transfer-is-not-available-in-windows-10

複数ドメインを担当している場合の問題

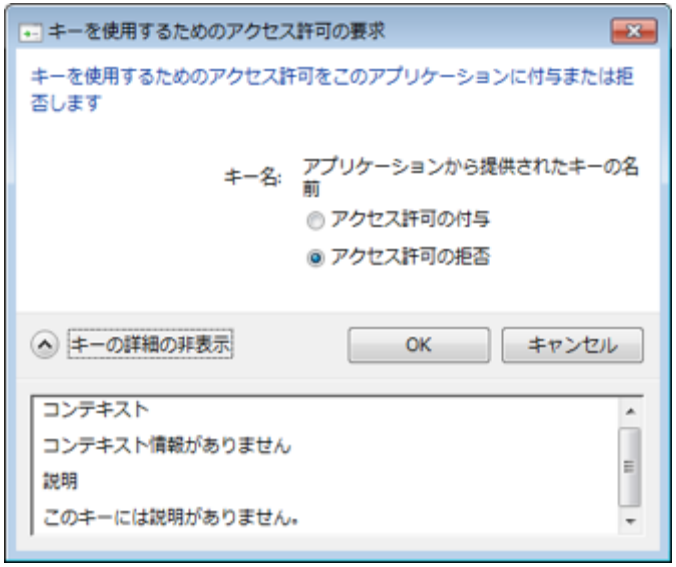
- Q. 別のドメインの申請を処理する際にいちいちブラウザを閉じるのが面倒なのですが…
  - A. プライベートウィンドウ内で支援システムにアクセスするようにすれば、当該ウィンドウを開き直すだけで登録担当者用証明書を切り替えられます。
    ※プライベートウィンドウは、InPrivateブラウズ、シークレットウィンドウ等ブラウザによって呼び方が異なります
- Q. IEだと複数の登録担当者用証明書の見分けがつきません。
  - A. フレンドリ名を設定してみてください。



手順: https://certs.nii.ac.jp/faq/Q6/#_773

「秘密キーの保護を強力にする」チェック時の動作

- クライアント証明書のマニュアルに従って上記項目にチェックを入れると、利用時毎回「アクセス許可の要求」ダイアログが表示されます
- 不都合のある機関はインポート時にこのチェックを外すようにご案内ください



サポート外

OS Xの秘密鍵削除問題

- OS Xのキーチェーンアクセスにて、証明書・鍵ペアを削除したつもりができていなかったという報告があります。
- 「自分の証明書」分類の一覧で削除しても満足せず、「鍵」分類の一覧もチェックしてください。

サポート外

OCSP問題

- サーバ証明書の失効確認のために多くのブラウザでOCSPが使われるが、レスポンダが反応しない時のタイムアウト時間、つまり待たされる時間が異なるようです。（厳密でなく体感のみでスミマセン…）
  - Edge/Win10 30秒程度
  - IE11/Win10 15秒程度
  - Firefox 2,3秒
  - Chrome OCSP見ていない
  - Opera 遅延気にならない
  - Safari 遅延気にならないが錠アイコンが出るのが8秒程度後
- ネットワーク障害時等の参考になれば。
- サーバ側でOCSP Stapling機能が使えれば使ったほうがよい。

おわりに

この1年の証明書サービス関連の話題を取り上げました。

- クライアント証明書発行対象の拡充
- TSV作成ツールリニューアル
- Windows 10対応状況
- SHA-1証明書発行終了
- その他諸々