UPKI電子証明書発行サービスについて

2016年5月26日 NII学術情報基盤オープンフォーラム

https://certs.nii.ac.jp

今回お伝えしたいこと
ーーとくに新任の担当者へ

- 最初にサービスの概要を
  - NIIによる証明書発行事業
  - 有償サービスであること
- 利用のための体制
  - 機関内で役割を割り振ってください
- 発行できる証明書と用途を詳しく
- 道具箱（実務に向けて）
  - 必携ツール
  - いろいろな決まり
  - マニュアル
  - Webサービス
- 注意してほしいこと
- 皆様へのお願い
- お知らせ

UPKI電子証明書発行サービスの概要

- 前身の有期プロジェクトから、
  NIIの事業として安定的に提供(有償)
- 提供する証明書の種類
  - サーバ証明書(OV)，クライアント証明書，コード署名用証明書
    - 追加ドメインの制約を大幅に緩和
      - 50ドメインを超える機関もあります
- 費用
  - UPKI電子証明書発行サービス利用料 として設定（年間定額）
  - OV証明書
    - 発行枚数に制限なし
    - 組織の規模ごとに段階的に設定→次スライド
    - 追加ドメインはドメイン単位に課金
  - クライアント証明書，コード署名用証明書は当面無料
    - 普及啓蒙フェーズ

サービス利用料金

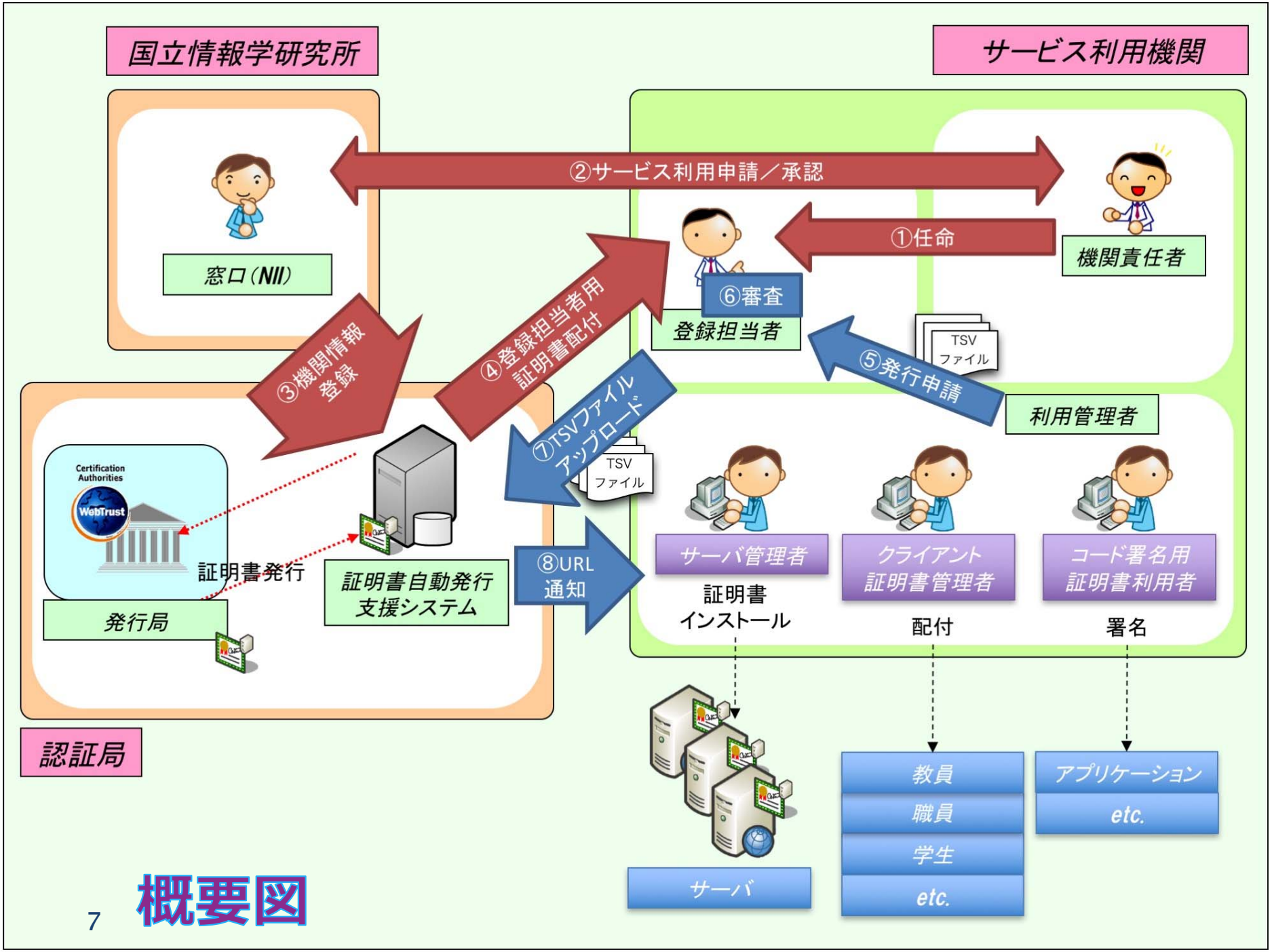
構成員数	年額(税別)
1–200	¥30,000
201–400	¥40,000
401–600	¥50,000
601–800	¥60,000
801–1000	¥70,000
1001–1200	¥80,000
1201–1400	¥90,000
1401–1600	¥100,000
1601–1800	¥110,000
1801以上	¥120,000
追加/ドメイン	¥20,000

- ✓ 構成員数：常勤の教員・研究者数
- ✓ 年額には，OV証明書（1ドメイン分），クライアント証明書，コード署名用証明書を含む
  - ✓ 発行枚数に制限なし
  - ✓ クライアント証明書とコード署名用証明書は当面無償
- ✓ ドメイン追加時には，1ドメインごとに追加ドメインの額をプラス
  - ✓ 次スライドに計算例
- ✓ 改訂される可能性があります

料金計算の例

- 構成員数601-800，1ドメイン，
  年度初め（4月）から利用
  - ￥60,000 × 1.08 = ￥64,800
- 構成員数601-800，1ドメイン，
  年度途中（6月）から利用
  - ￥60,000 ÷ 12 × 10 × 1.08 = ￥54,000
- 構成員数601-800，3ドメイン，
  年度初め（4月）から利用
  - ￥60,000 × 1.08 + 20000 × 2 × 1.08 = ￥108,000

体制


国立情報学研究所
サービス利用機関
窓口(NII)
②サービス利用申請／承認
①任命
機関責任者
⑥審査
登録担当者
③機関情報登録
④登録担当者用証明書配付
⑤発行申請
TSV ファイル
⑦TSVファイルアップロード
利用管理者
Certification Authorities
WebTrust
証明書発行
証明書自動発行支援システム
⑧URL通知
サーバ管理者
クライアント証明書管理者
コード署名用証明書利用者
証明書インストール
配付
署名
発行局
認証局
サーバ
教員
職員
学生
etc.
アプリケーション
etc.

概要図

機関責任者

- 機関責任者は、所属する機関の長より委嘱を受け、本サービスの利用に関する責任を負います
- 機関ごとに、必ず1名必要です
- ドメイン申請と全ての変更申請の書類には、機関責任者の署名(自署)と印が必要です
- 課長もしくは准教授相当以上の方を選任してください

登録担当者

- 機関責任者から任命を受け、機関内での証明書発行・失効・更新等にかかる申請の審査（※）とその業務を担当します
- 証明書の発行・更新・失効の操作は「国立情報学研究所電子証明書自動発行支援システム」を使って行います。自動処理されるので、申請から数分で証明書を取得することができます
- 登録担当者は、ドメインごとに複数名任命することができます

- ※審査について
  - サービス利用申請時に提出した、「確認実施手順調査票」の手順に基づいて、実在性・本人性を確認しなければなりません

利用管理者

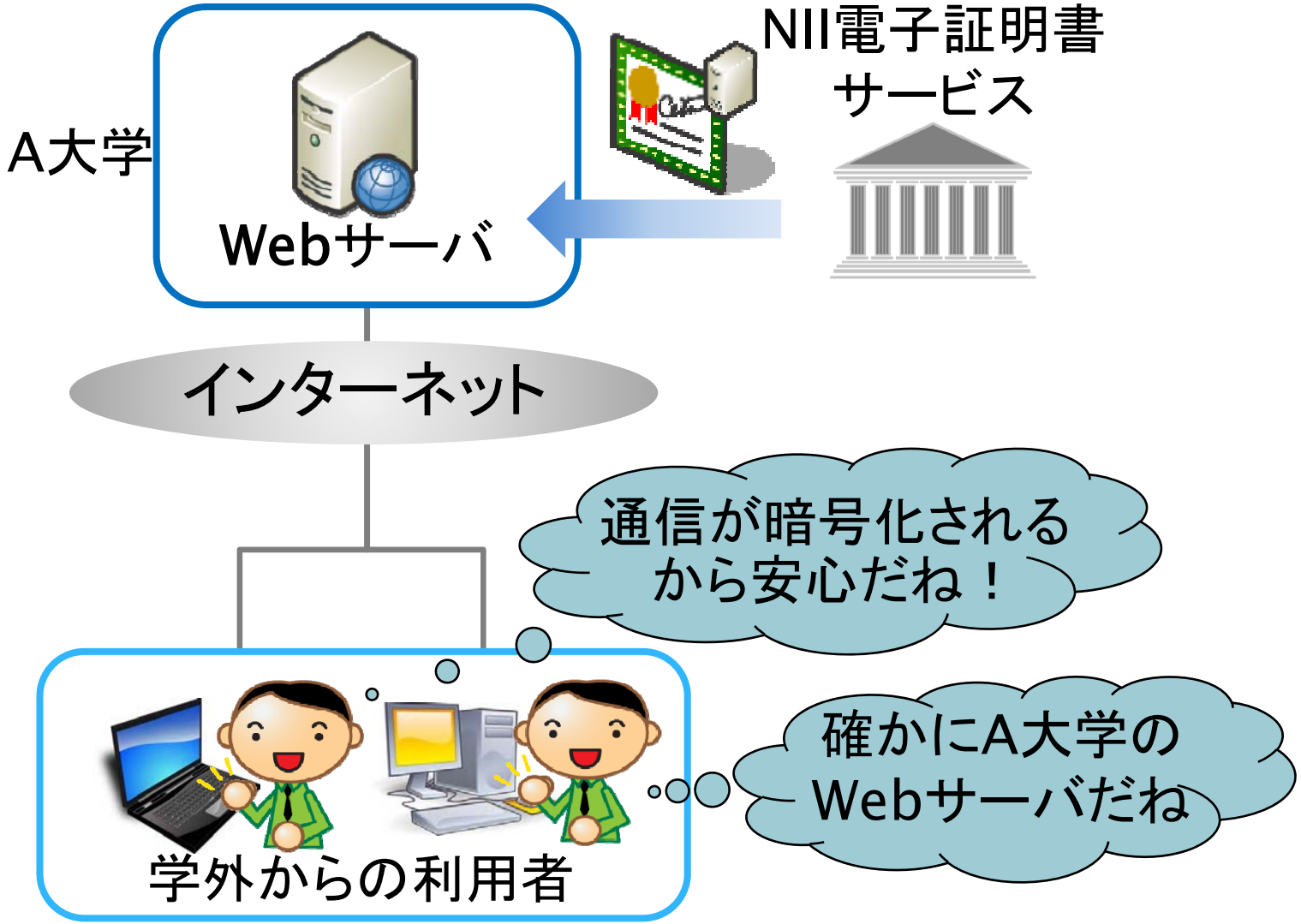
- NII が定める各種規定に合意し、証明書に記載された公開鍵と対になる秘密鍵を管理する人、組織をいいます
- 登録担当者を介して証明書の発行申請を行います
  - サーバ証明書の場合、利用管理者はサーバ管理者であることが多いです
- 利用管理者の範囲
  - 教員、職員等の学術機関に所属する者であり、本 CA 又は登録担当者が本人性及び実在性を確認できる者
  - 学術機関と何らかの契約関係にある等、学術機関に所属する者が当該利用管理者の実在性、本人性を確認できる者

発行出来る証明書

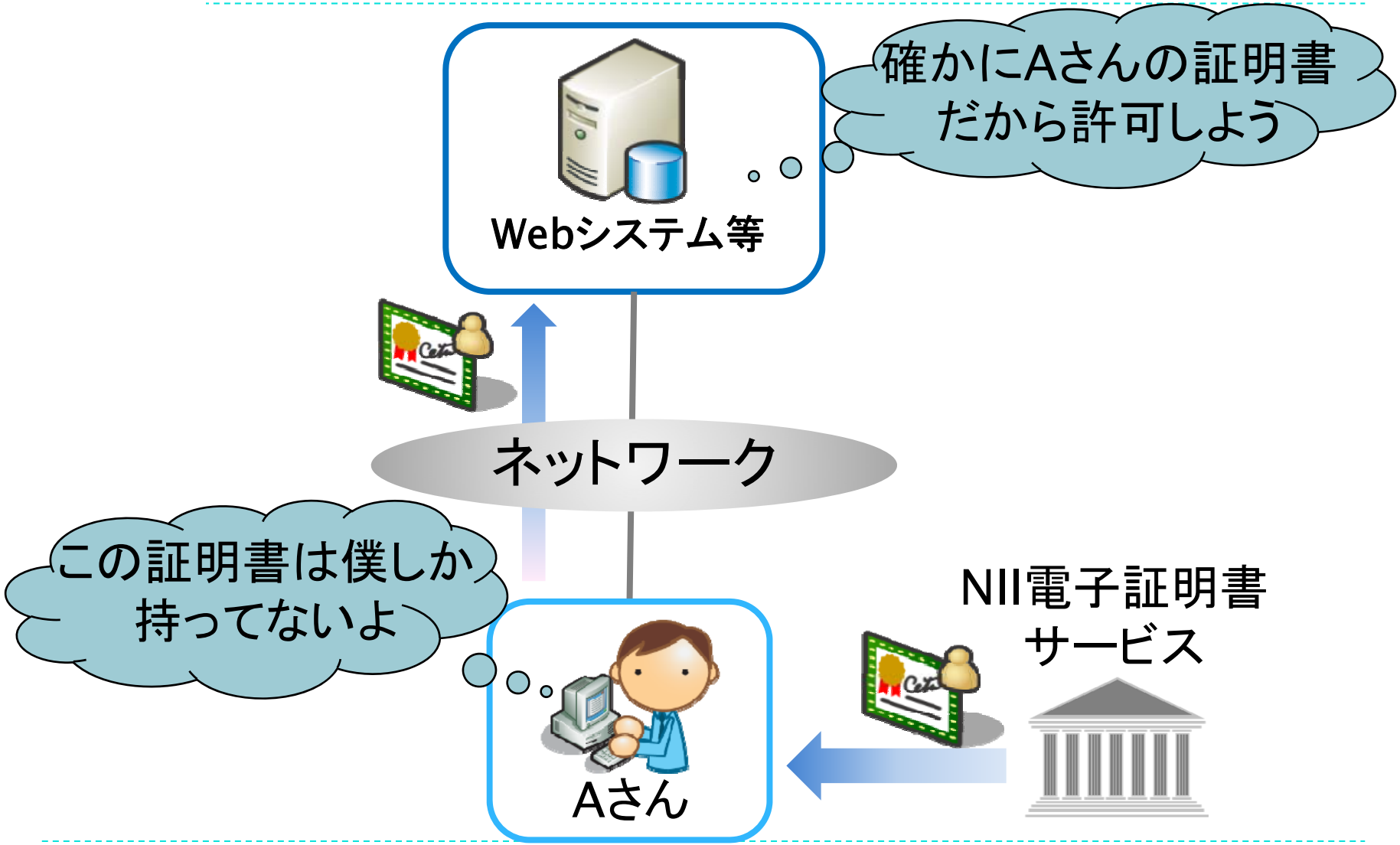
種別と用途

- サーバ証明書（OV）
  - Webサイトを提供する機関の身元を証明できます
  - Webサイトが、その名前において、機関の責任の下で運用されていることを保証できます
  - SSL/TLSで、サーバと利用者間の通信を暗号化し、盗聴を防ぐことができます
  - DV, OV, EVの違い
- クライアント証明書
  - 文書と電子メールへの署名
    - 送信もとを保証し、なりすましと改ざんを防止することができます
  - 電子メールの暗号化
    - 盗聴を防ぎ、情報漏洩などを防ぐことができます
  - 個人認証
    - パスワードに変わる、安全で強固な認証に利用できます
- コード署名用証明書
  - プログラムやアプリケーション、スクリプトへの署名
    - これらの提供元を保証することができます
    - 電子署名が必須なシステムに、署名済みのアプリケーションを提供できます

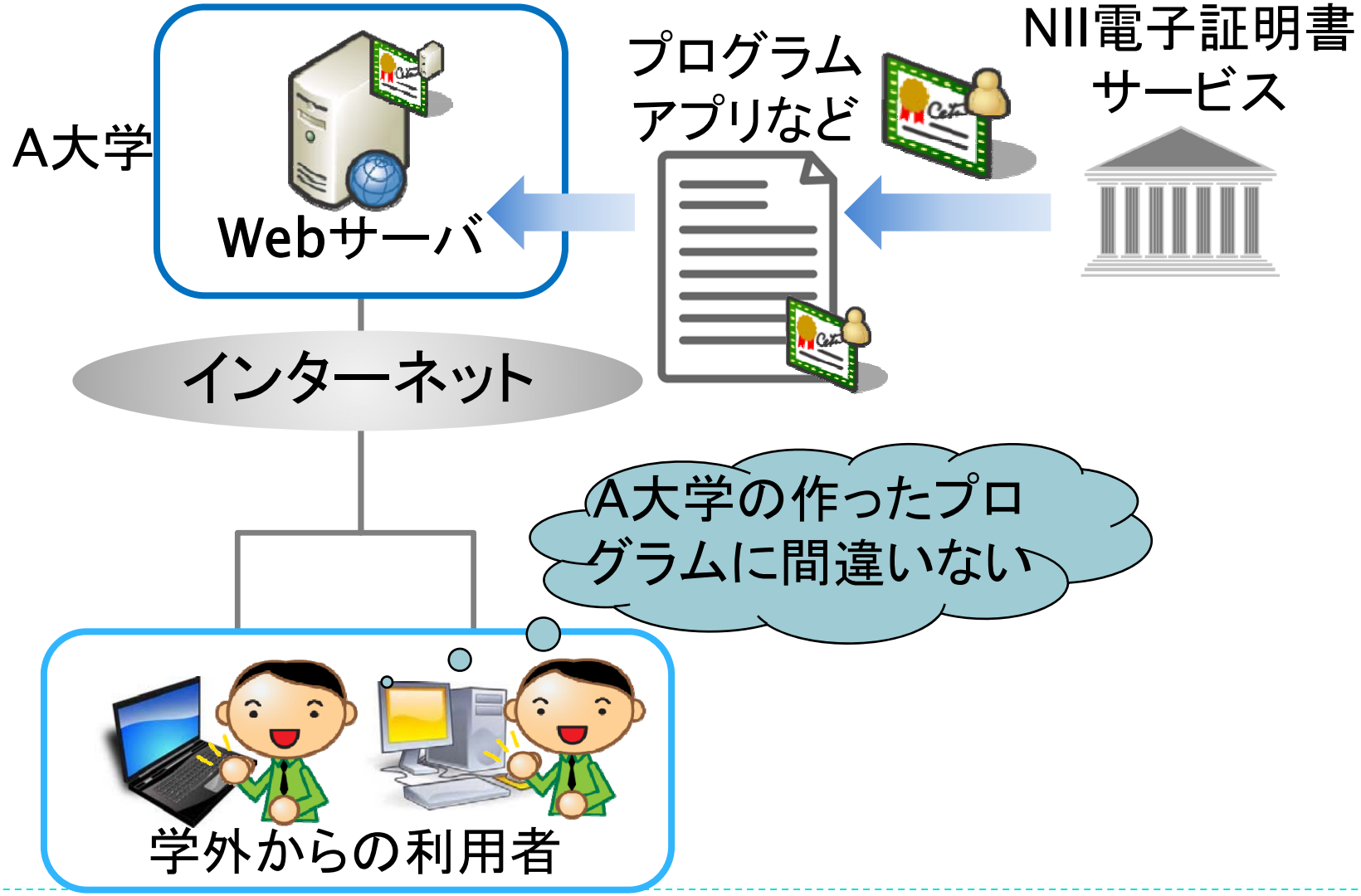
サーバ証明書


NII電子証明書
サービス
A大学
Webサーバ
インターネット
通信が暗号化される
から安心だね！
確かにA大学の
Webサーバだね
学外からの利用者

クライアント証明書


確かにAさんの証明書
だから許可しよう
Webシステム等
ネットワーク
この証明書は僕しか
持ってないよ
NII電子証明書
サービス
Aさん

コード署名用証明書

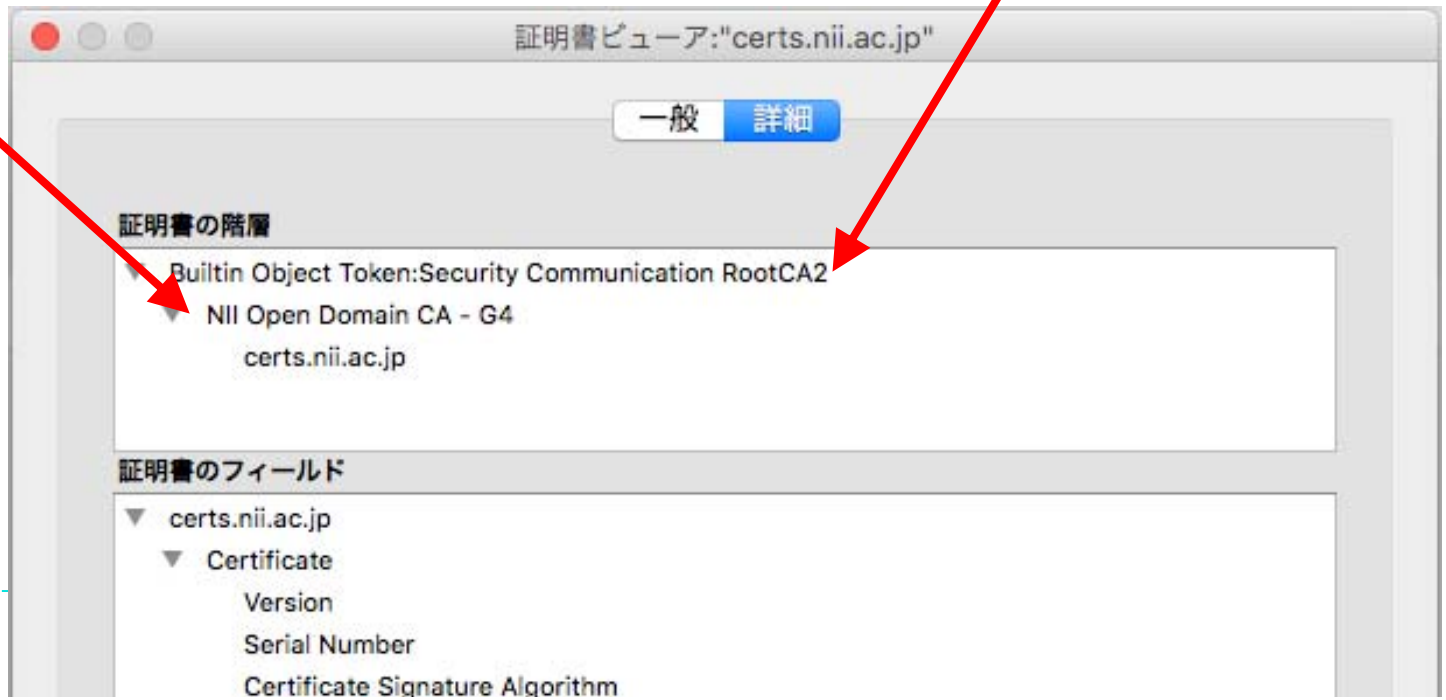

A大学
Webサーバ
プログラム
アプリなど
NII電子証明書
サービス
インターネット
A大学の作ったプロ
グラムに間違いない
学外からの利用者

UPKI証明書の特徴

- 商用水準の電子証明書
  - 商用として実績のある電子証明書と同等のものを提供しています
- SHA-256対応
  - UPKI電子証明書発行サービスの証明書はSHA-256に対応し、安全性の高い署名アルゴリズムを使用しています
- 証明書取得までのタイムラグを軽減
  - 電子証明書の発行申請は、1枚あたり最短10分以内で処理されます。迅速な証明書発行が可能です

UPKIの認証局？

- ルート認証局
  - セコムトラストシステムズが提供
- 中間認証局
  - 国立情報学研究所 オープンドメイン認証局



道具箱

登録担当者・利用管理者必須ツール

- Firefox
  - 登録担当者には、UPKIに関する各システムを操作する場合、Firefoxをおすすめしています
    - 「腕に自信あり」の方は、この限りではありません
  - 登録担当者用証明書取得時、面倒な設定がいりません
- OpenSSL
  - 証明書発行申請のための準備に使います
    - マニュアルでも、OpenSSLを用いた手順をご案内しています
  - 証明書の中身を見ることもできます
- Microsoft Excel
  - 証明書発行支援システム（後述）から証明書一覧を取得できるのですが、そのファイルの内容を一覧するのに用います
  - TSVファイルをコピー＆ペーストすると、読みやすくなります

利用規程・細則

- UPKI電子証明書発行サービス利用規程
  - http://id.nii.ac.jp/1344/00000040/
  - サービスの対象などが書かれています
- UPKI電子証明書発行サービス利用細則
  - http://id.nii.ac.jp/1344/00000034/
  - 諸々の申請について
  - 責任の所在
  - 緊急時のNIIによる証明書失効 などが書かれています

- これらに同意した上で、サービスをご利用いただいています

CP/CPS

- これは何？
  - CP(Certificate Policy)
    - 発行する証明書の利用目的、適用範囲、利用申請手続など、証明書に関する決まり
  - CPS(Certification Practice Statement)
    - 認証局、登録局、リポジトリなどの運用規則
- 守らないとどうなるの？
  - 前提として、証明書の発行を受ける者は、CP/CPSの内容を承諾しているものとしています
  - 年度末のアンケート（後述）で、CPに準拠できていないな、ということになったら、改善をお願いすることになります
- どこにあるの？
  - 本サービスのリポジトリで公開しています
    - https://repo1.secomtrust.net/sppca/nii/odca3/index.html

マニュアル

- 電子証明書発行支援システム操作手順書
  - https://certs.nii.ac.jp/archive/regulations/sciaoperation/
- インストール・利用マニュアル
  - サーバ証明書
    - インストールマニュアル
  - クライアント証明書
    - ブラウザへのインストールマニュアル
    - ブラウザ発行マニュアル
    - 各メーラへのS/MIME証明書インストールマニュアル
  - コード署名用証明書
    - 利用マニュアル

  - PDFとWordの双方で公開中
  - https://certs.nii.ac.jp/archive/manuals/

各システム

- UPKI申請システム
  - https://certs-office.nii.ac.jp/
- 電子証明書発行支援システム
  - https://scia.secomtrust.net/upki-odcert/lra/SSLLogin.do
- TSV作成ツール
  - https://certs.nii.ac.jp/tsv-tool/

UPKI申請システム

- これまでExcelファイルで作成いただいていた各申請書が、Webサービスで作成できるようになりました
- https://certs-office.nii.ac.jp
- UPKIに関する全ての申請書が作成できます
  - ドメイン申請
  - 機関情報変更申請
  - 登録担当者情報変更申請
  - 利用期間更新申請（新）
  - サービス利用申請
  - 確認実施手順調査票 提出・変更
  - 体制図 提出・変更
- 各申請に、登録担当者と窓口担当者がコメントをつける形で、修正点などやりとりできます

UPKI申請システム 画面

登録担当者用証明書を用いてログイン

- 登録済みの機関情報、ドメイン情報が確認できます
- 申請書の作成、事前チェック依頼が可能です
- 提出済みの申請書の状態が表示されます

機関責任者によるオンラインチェック

- 機関責任者によるオンラインチェック（自署押印の代替）ができるようになりました
  - UPKIのクライアント証明書が発行されていることが必須です
  - 初回のみ、主体者DN登録のために「機関情報変更申請書」の提出が必要です
  - 承認された後、機関責任者によるオンラインチェックが可能になります
  - 利用期間更新申請のみ、オンラインチェック不可となります
    - 請求に関する書類なので、自署押印（機関責任者）と郵送をお願いします
    - お手数をおかけしますがご諒承ください

電子証明書発行支援システム

- 登録担当者だけがアクセスできます
  - 専用のクライアント証明書（登録担当者用証明書）が必要です
- 発行・更新・失効の申請が出来ます
  - TSVファイル（次スライド）をつかいます
- 発行済みの証明書一覧を取得出来ます
  - マニュアルに、このファイルの読み方がかかれています

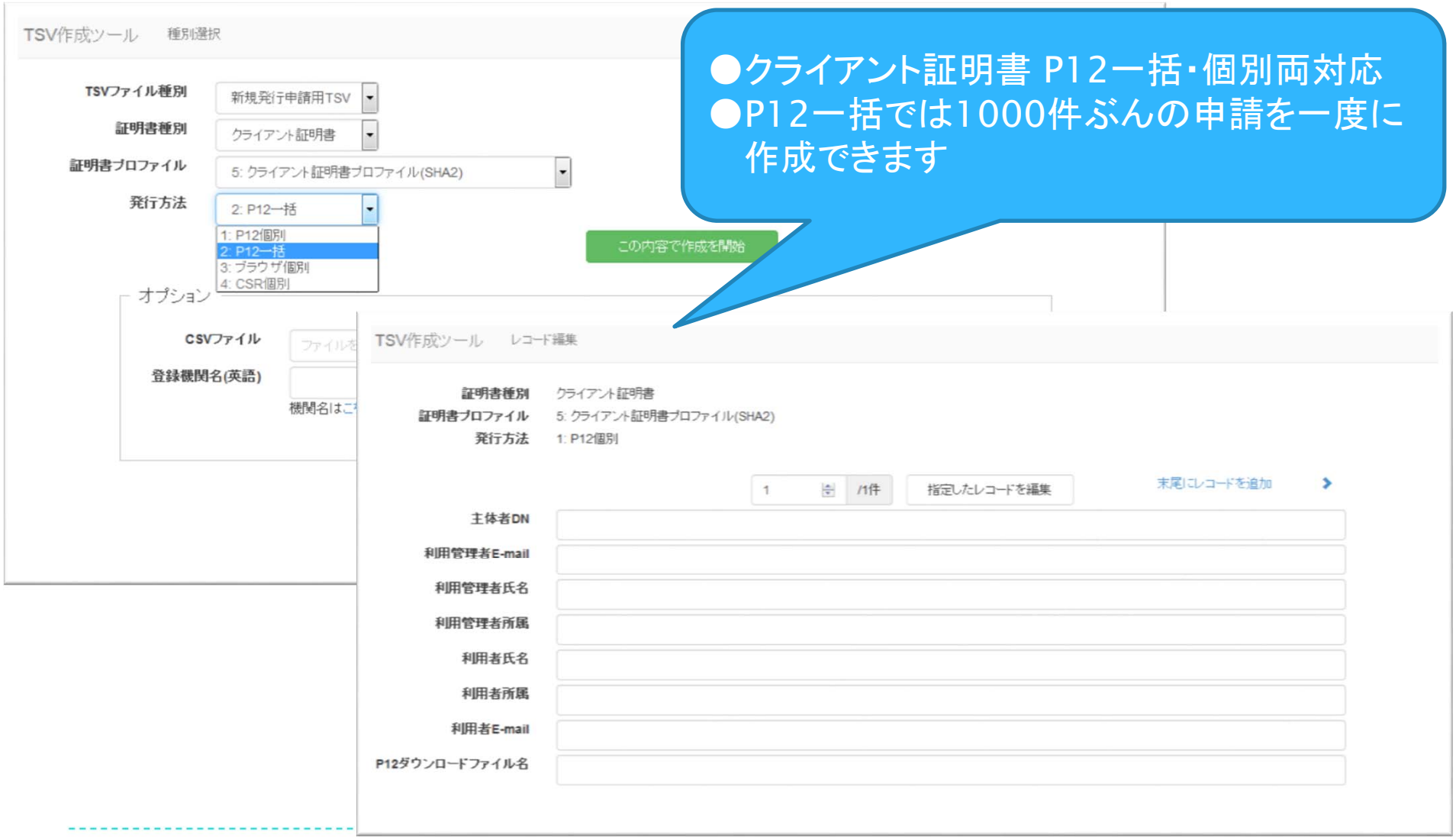
TSVファイル

- 発行支援システムで使用する、タブ区切りのテキストファイルです
  - CSVに似ています
  - 区切り文字（カンマではなくタブ）が違うだけです
- 文字コード・改行コードが決まっているので気をつけてください
- テキストエディタで作ることもできますが・・・
  - TSV作成ツールを使うのが楽です
- フォーマットは下記で確認できます
  - https://certs.nii.ac.jp/archive/TSV_File_Format/

TSV作成ツール

- 新TSV作成ツールを提供しています
  - 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
  - Apache License 2.0 で提供します
    - サービス利用機関が自前で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

P12一括・個別、ブラウザ発行って何？（クライアント証明書）

- クライアント証明書を機関の構成員に配付するとき、用途にあわせた発行形態をとることができます

- バルクでまとめて発行
  - P12一括
    - ZIPでまとめて利用管理者が取得する方法です
- 一枚ずつ個別に発行
  - P12個別
    - メールで個々人宛に、取得用URLが通知され、ダウンロードする方法です
    - ファイルで取得できますが、インストールのお手間があります
  - ブラウザ発行
    - ブラウザ（IE、Firefox）に、Webアプリケーションから直接インストールする方法です
    - P12個別のようなインストールの手間はありませんが、バックアップ方法などを別に、利用者に案内する必要があります

注意してほしいこと

発行と更新と失効

- 発行と失効はそのままでわかりやすいのですが、更新は注意が必要です
  - 有効期限切れを間近にひかえた証明書で主に更新処理を行いますが・・・
- 一度でも使った主体者DN(※)を再利用する場合は、証明書が 有効/失効済み/有効期限切れ のいずれの場合でも、更新申請を行う必要があります

- ※主体者DN（Subject DN）
  - 証明書の主体、発行対象の識別名といった意味です
  - UPKI サーバ証明書の例
    - CN=certs.nii.ac.jp,
      OU=Cyber Science Infrastructure Development Department,
      O=National Institute of Informatics,
      L=Academe,
      C=JP

秘密鍵の管理

- 電子証明書は、1対1で対応する秘密鍵とペアで扱われます
  - 秘密鍵は文字通り、他者に開示せず、流出しないよう細心の注意をはらって取り扱ってください
    - まれにメールでサービス窓口宛に送信される方がいらっしゃいます（旧プロジェクトでのケースです）
  - 強固なパスフレーズで保護することも忘れないでください
- 奪われるとどうなるのか？
  - お家の鍵、クルマの鍵、ロッカーの鍵

登録担当者用の証明書

- 登録担当者用証明書はとても大事です
  - 登録担当者それぞれに、登録しているドメインごとに1枚ずつ発行されます
  - もし盗まれると、当該ドメインの証明書が出し放題になってしまいます
  - 厳重に管理してください
  - 何者かに奪われた、またはその疑いがある場合は、サービス窓口まで再発行を依頼してください
- 必ずバックアップしておいてください
  - ブラウザをリセットすると、削除されてしまうことがあります

皆様へのお願い

皆様へのお願い ――備忘を兼ねて

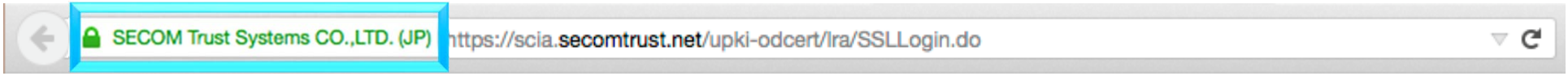
- 変更申請・変更届
  - とくに異動のシーズンに集中します
  - 異動が決まったら、後任への引き継ぎと、各種変更の届出をお願いします
- 利用期間更新申請
  - サービスは年度ごとに継続の意思確認を行います
  - 年度末頃に、下記アンケートとあわせてこの申請書の作成をお願いします
- 年度末アンケート
  - 証明書の発行状況についての、内部監査のような役割です
  - 全”ドメイン”でそれぞれ回答必須です

- 年度末～年度初めに集中しています

最後にお知らせを

EV証明書について

- 本サービス利用機関(※)に対し，証明書発行もとであるセコムトラストシステムズより，EV証明書が有償で提供されます



※サービスに登録したドメインである必要はありません

- ご希望の機関には，セコムトラストシステムズより提供された「申請ガイド」を送付いたします
  - certs@nii.ac.jp までご依頼ください！
  - 「申請ガイド」受領以降のEV証明書についてのお問い合わせ，発行手続き，お支払い等は，セコムトラストシステムズと直接行ってください

EV SSL証明書(セコムパスポートforWeb EV2.0) の特徴

信頼される安心を、社会へ。
SECOM
セコムトラストシステムズ株式会社

◆ 機能　　アドレスバーが緑色に変化し、安全性をアピール

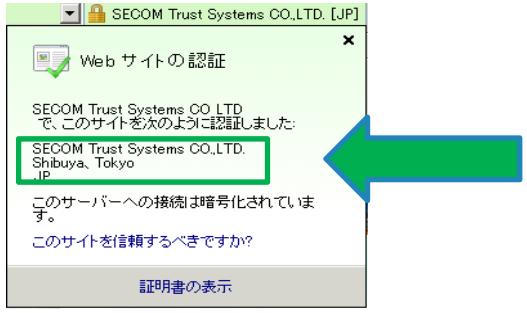
EV SSL証明書対応ブラウザでアクセスすると、アドレスバーが緑色に変化

OV(組織認証)証明書(セコムパスポートforWeb SR3.0)では、https://でアクセスしてもアドレスバーの色は白色のままです。

危険なサイトはアドレスバーが赤色に変化

https://でアクセスしたとき、「失効されている」「有効期限が切れている」「WebサイトのURLと一致していない」疑わしいサイトの場合には、危険なサイトとして、アドレスバーが赤色に変化します。

◆ 効果　　識別情報の表示で運営組織を確認、 フィッシング対策に有効



従来、ブラウザの鍵マークをクリックしなければ確認できなかった「**サーバー証明書に記載されている組織名**」がアドレスバーの横に表示されます。

EV SSL証明書は、実在証明としてより一層安全性をアピールすることができます。

Secured by SECOM

セコムのWebステッカーがEV SSL証明書の更なる安全性を訴求

午後の予定

- 午後も、証明書関連のセッションを開催します
  - 5月26日 10:00-12:00 学認、UPKI、eduroam 初めの一歩
  - 5月26日 14:00-17:00 クライアント証明書の活用術

おわりに

- ご連絡・お問い合わせ先
  - 国立情報学研究所　学術基盤課総括・連携基盤チーム（認証担当）
    - Mail：　certs@nii.ac.jp
    - 電話：　03-4212-2218
    - Web：　https://certs.nii.ac.jp
  - 原則，サービス利用機関または利用予定機関の機関責任者・登録担当者からお願いします