



UPKI電子証明書発行サービス 年度末調査から

2016.5.26 NII オープンフォーラム
国立情報学研究所 末永光弘



2015年度UPKI年度末調査

- ▶ 年度末調査へのご協力ありがとうございました
 - ▶ 全機関様よりご回答いただくことができました
- ▶ 年度末調査実施概要
 - ▶ 実施期間：2016/2/15～3/16
 - ▶ 回答機関数：281機関
 - ▶ 回答ドメイン数：378ドメイン

- ▶ 確認実施手順に関するアンケート項目について
 - ▶ 証明書発行に関して、規則と手順に従っているか調査
 - ▶ 問題なく統制されていることが確認できました
- ▶ これからも確認実施手順に則った証明書発行をお願いします

- ▶ Q18.インシデントが発生していた場合、その内容について教えてください。
 - ▶ 公開鍵と間違えて秘密鍵をメールで送ってしまった
 - ▶ 秘密鍵を保存したメディアを紛失した・盗難された
- ▶ ……といったようなインシデント報告はなし
 - ▶ 皆様の日々の努力に感謝いたします。
- ▶ ちなみに、証明書の設定間違えた、といった「トラブル」の報告ばかりでした。

- ▶ Q20.UPKIのいいところ・悪いところ
 - ▶ いいところ
 - ▶ 証明書発行が早い、簡単にできる
 - ▶ NIIの証明書なので信頼性がある
 - みなさまのご協力のたまものです
 - ▶ 悪いところ
 - ▶ DNの制約で証明書を使えないことがある
 - 「ST」がなくて使えない機材があるようです
 - 一部機材やソフトウェアでCSRを作成すると「ST」が強制的に入るようです
 - ▶ TSVファイルの作成が難しい
 - 最新版TSVツールを提供開始しました！



アンケートから

- ▶ Q23.クライアント証明書のご用途
 - ▶ 選択肢以外の用途としては以下のとおり
 - ▶ リモートアクセスクライアントによる利用
 - ▶ 無線LAN接続やVPN接続の認証
- ▶ クライアント証明書については本日のセッションをご参考になさってください
- ▶ みんなで使いましょう！

- ▶ Q24.コード署名用証明書の用途
 - ▶ 具体的な用途としては以下のとおり
 - ▶ サーバの構成プロファイルへの署名
 - ▶ 利用者に配布するWi-Fi設定プログラムへの署名
- ▶ コード署名用証明書の活用については
坂根先生のご講演を参考にしてください



アンケートから

- ▶ Q27.UPKIに提供してほしいサービス
 - ▶ ワイルドカード証明書
 - ▶ 数台程度ならば、SANに複数ホスト名を記載した証明書で対応
 - ▶ 解説は https://certs.nii.ac.jp/faq/Q4/#_651 (Q4-4)
 - ▶ 5年など長期間のサーバ証明書がほしい
 - ▶ サーバ証明書は最大39か月
 - <https://cabforum.org/baseline-requirements-documents/>
 - ▶ 役職名・業務委託先への証明書発行
 - ▶ CPの改定でできるようになりました！
 - ▶ PDF署名
 - ▶ クライアント証明書で署名できます



アンケートから

- ▶ Q27.UPKIに提供してほしいサービス
 - ▶ 独自CAで出してるクライアント証明書を切り替えたい
 - ▶ ぜひともやってください！
 - ▶ なにか問題点があればご相談ください。

今後ともUPKI電子証明書発行サービスを
よろしくお願いいたします。