

平成19年度情報処理軽井沢セミナーレポート

針木剛
(京都大学情報環境部)

1. セミナー最終日に発表した 課題のタイトル

サーバ証明書申請手続きの検討

2. 1の概要

次ページ以降

現在の業務

Webホスティングサービス

大学の教職員向けに
学内組織(研究室、学科、学部など)の
Webサービスを共有サーバにて行っている

2007年7月現在で約160の組織が利用

業務内容

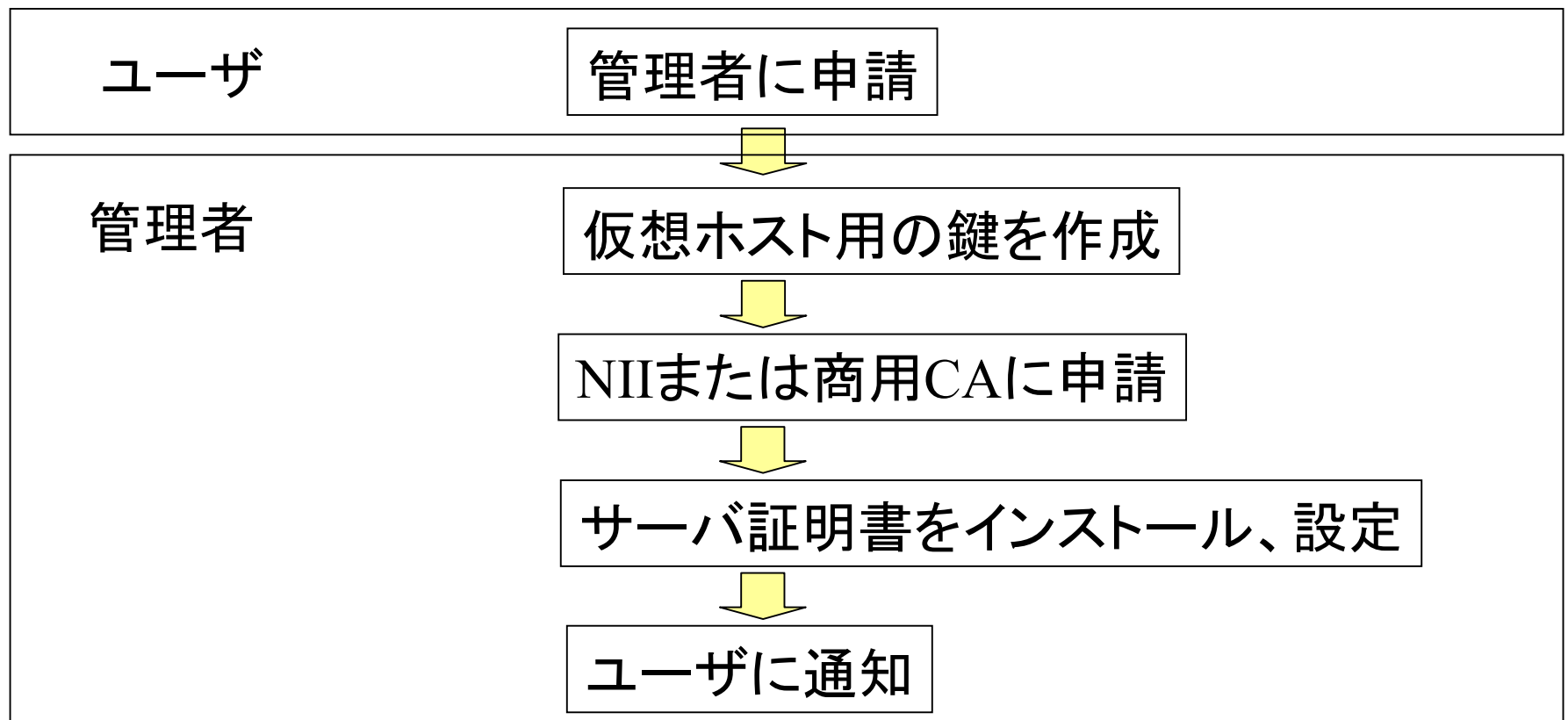
サーバのメンテナンス

新規サービスの技術検証、運用ポリシー規定

ユーザからの問い合わせ対応

SSL対応

昨年度よりSSLのサービスを開始

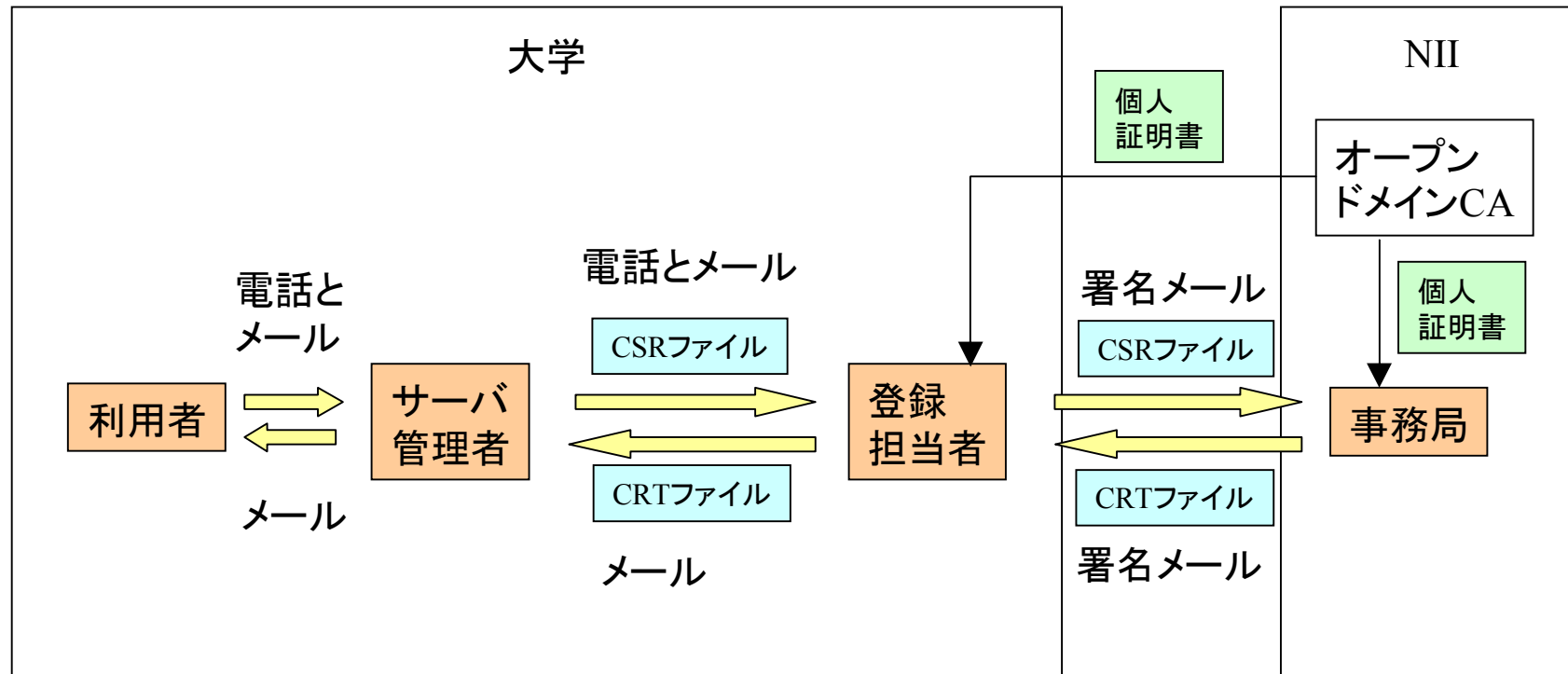


管理者はユーザの代行

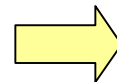


ユーザの本人確認、申請ログ

現在のサーバ証明書申請手続き

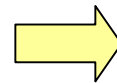


電話にて本人確認、メールでログ



煩雑、ログ信頼性低い

メール添付ファイル



データ信頼性低い

前提

大学CA

教職員に個人証明書が配布(ICカードなど)

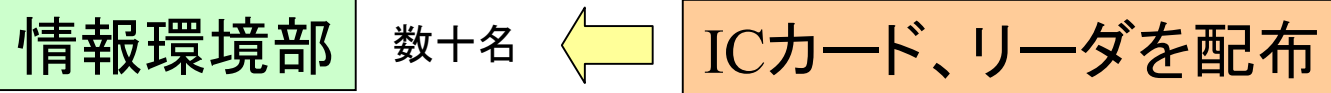
教職員が個人証明書を利用できる

カードリーダー、MUA

教職員、学生が大学CAの証明書を利用できる

MUA、Webブラウザ

ICカード試験導入

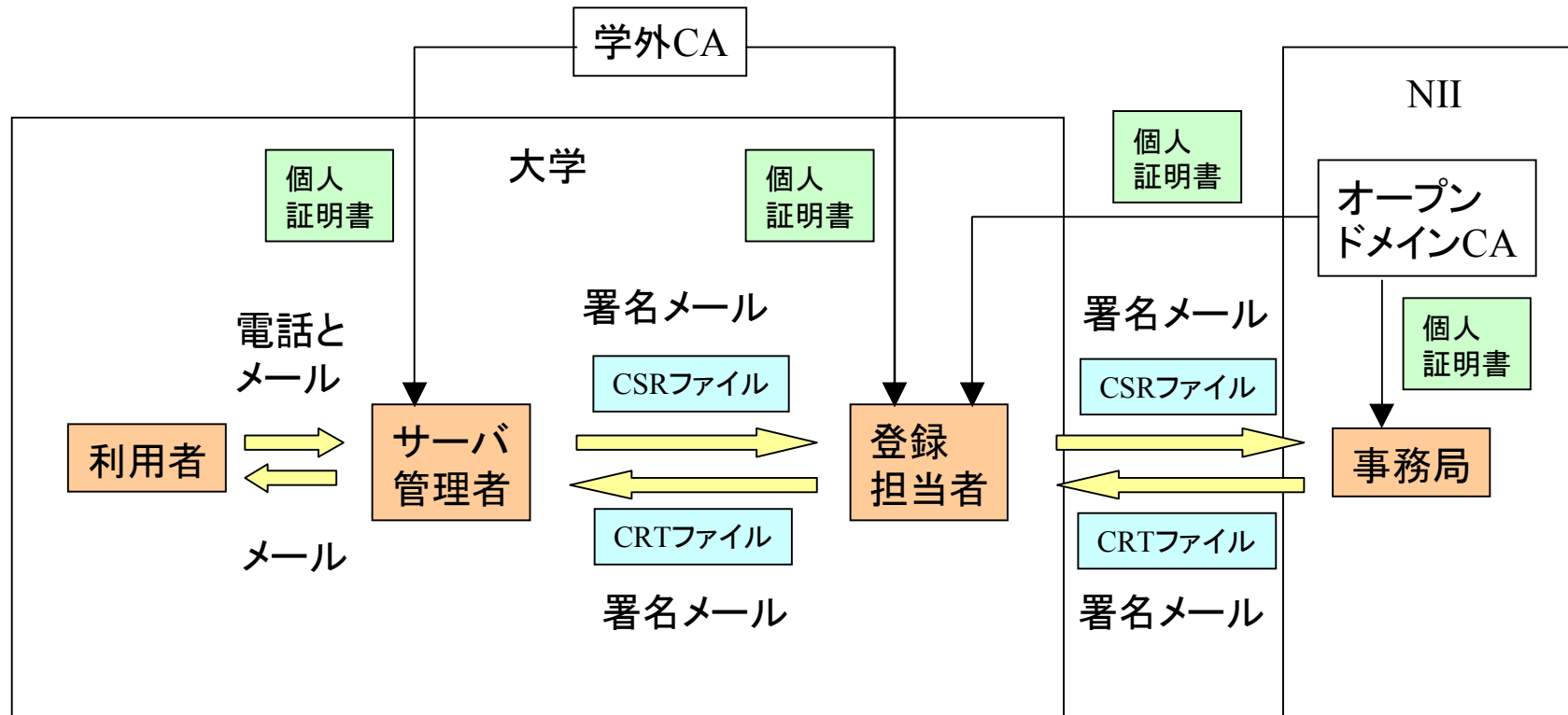


CAはアウトソース

各部署の一部の教員、技術職員がヘルプデスク

情報環境部で全学に先行して導入、検証試験

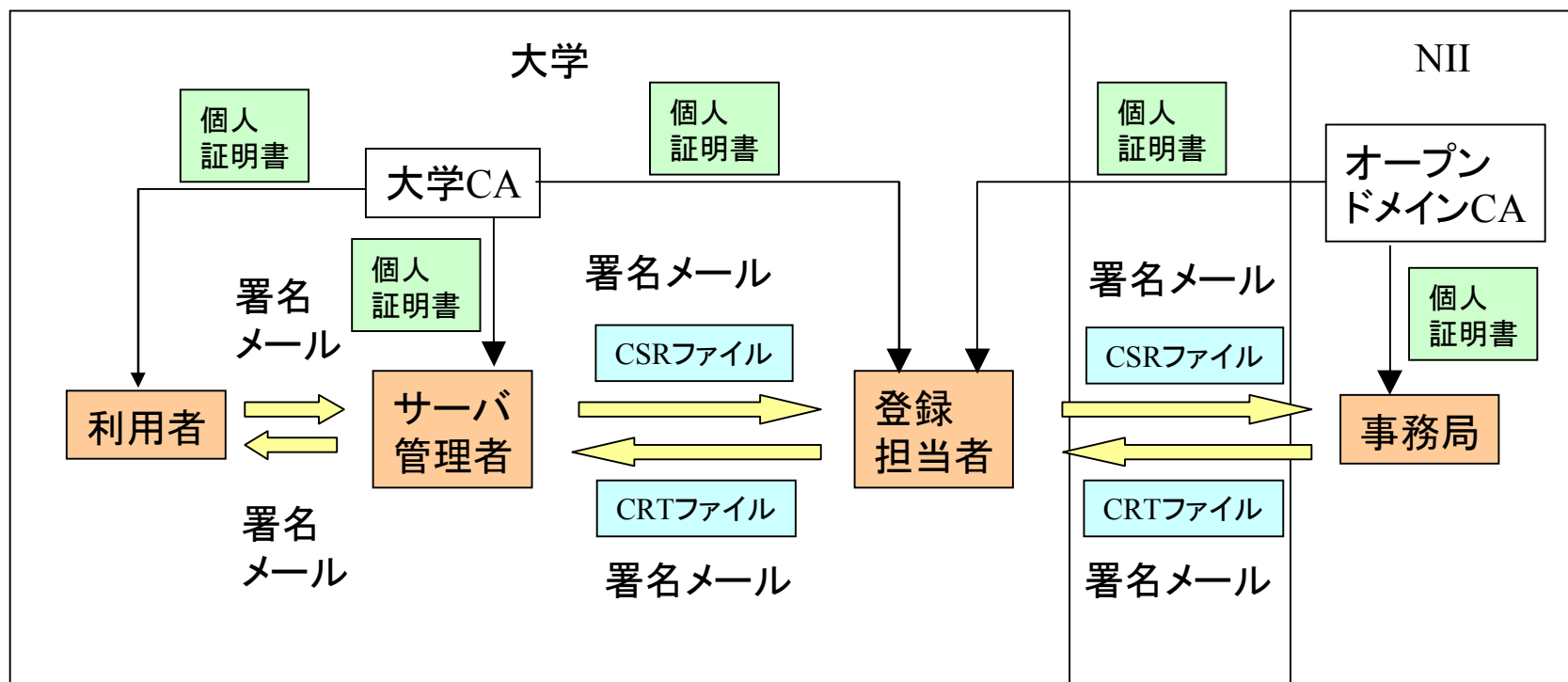
試験導入後の申請手続き



サーバ管理者、登録担当者・・・ 情報環境部職員

まずは添付ファイルの信頼性は確保

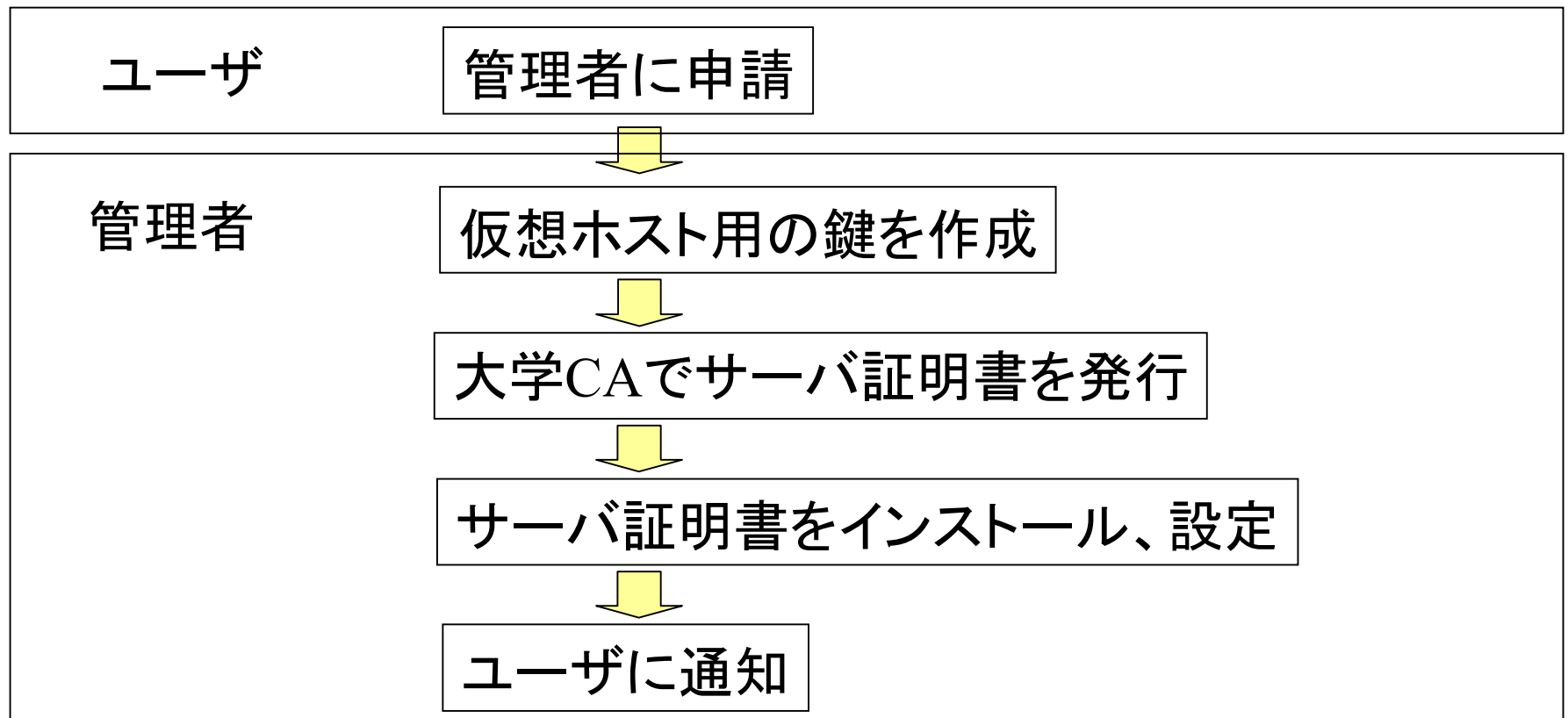
本格導入後の申請手続き



電話確認の煩雑な作業の簡略

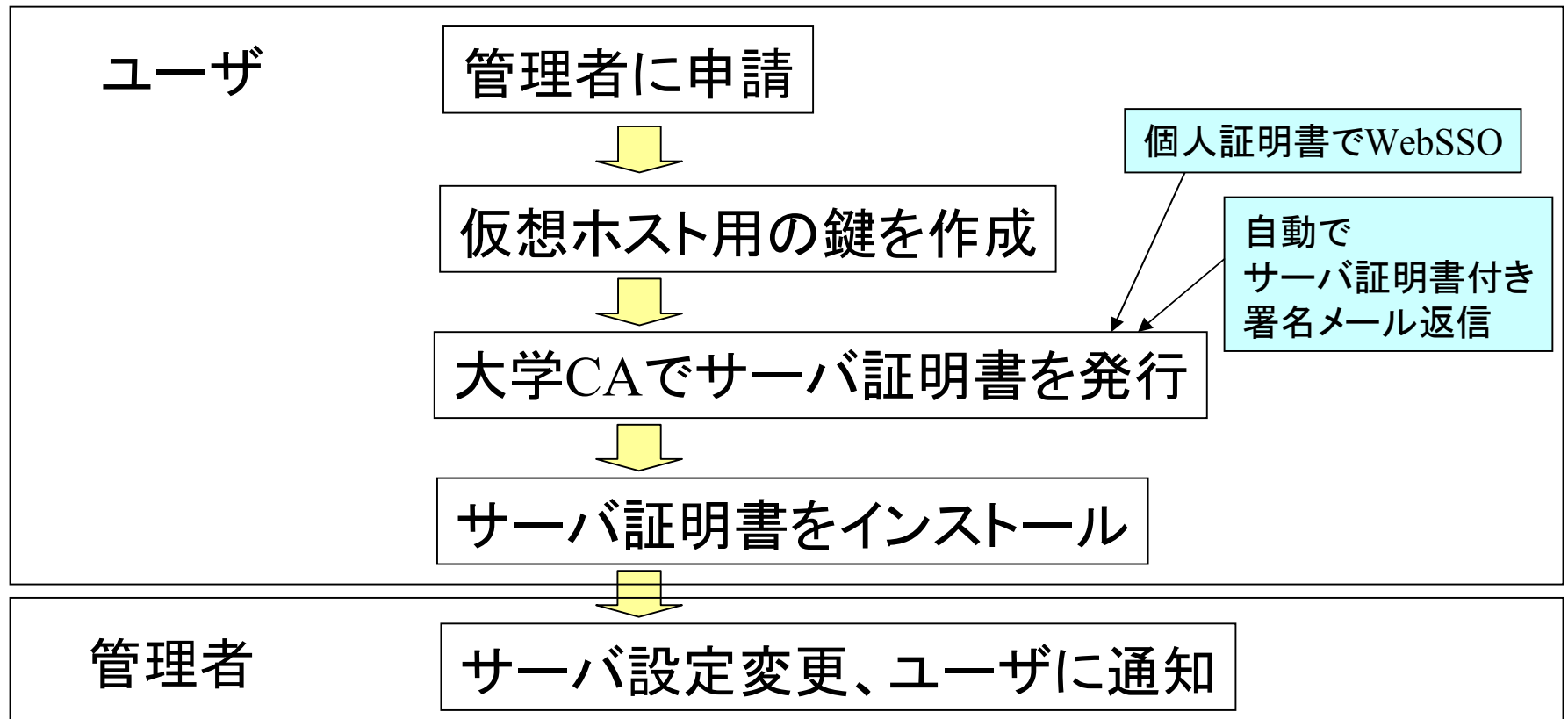
メールログの信頼性

大学CAのサーバ証明書(案1)



学内向けのWebサービス構築可能

大学CAのサーバ証明書(案2)



まとめ

サーバ証明書申請手続きが

大学CA導入により

電話確認作業の簡略

メール添付ファイル、メールログの信頼性向上

学内向けWebサーバも可能

3. セミナーで学んだ技術及び知識

- PKIの基礎
 - 暗号化、電子署名、認証局
- UPKI概要
 - 3階層のPKI
 - キャンパスPKIの事例紹介
- shibbolethの紹介
 - shibbolethの最新動向
 - 認証の実習
 - 海外動向の紹介
- グリッドでの認証技術の利用
 - GSI、プロキシ証明書、仮想組織

4. セミナーの成果

- PKIに関して断片的な知識しか持たなかったが基礎から体系的に学ぶことができた。
- UPKIに関する詳細な内容を実際にキャンパスPKIを導入した事例を紹介して頂けた。
- 複数大学でのIDと属性利用を実現するshibbolethを実習を通して学ぶことができた。
- グリッドでの認証について詳細で平易に説明して頂けた。

5. セミナーの事前、事後において、 参考になったURLとその簡単な内容紹介

- UPKIに関して
<http://upki-portal.nii.ac.jp/>
- PKI関連技術
<http://www.ipa.go.jp/security/pki/>

6. 事前準備として知っておいた方が良かったと思われること

- PKIに関する基礎的知識
- UNIXやLinuxの操作、ネットワークの基礎的知識

7. セミナーの感想

- PKIに関して基礎から体系的に学べ、またNIIや他大学の動向、最新の技術の紹介など非常に有意義なセミナーであった。
- 他大学の受講生のみなさまとPKI以外にもさまざまな情報交換ができ有意義な時間を過ごすことができた。
- 軽井沢のすばらしい環境も講義や情報交換に集中できた1つの要因であったと思う。