大学における情報セキュリティ及び
電子認証基盤に関するワークショップ
平成１９年２月２６日（月）

大学向け認証局
スタートパックの開発について

国立情報学研究所
学術ネットワーク研究開発センター
片岡 俊幸

本開発の目的

- 大学向け認証局スタートパックの開発
  - 学内認証局の検討には、認証局システムの構築ノウハウ、運用ノウハウが必要。
  - そのため、実業務に即した認証局を手軽に導入・運用可能となるスタートパックの開発、配布を行う。
  - 構築、運用の実体験を通して、運用するアプリケーションや必要となるセキュリティレベルといった各大学の状況に最適な認証基盤の検討、構築、運用が可能となる。
  - 証明書を利用するアプリケーションを１つに限定することで、簡単に、かつ短期間に構築、運用を開始できるものとする。
  - 認証局システムは、実体験だけではなく、実運用も可能なレベルのものとする。

大学向け認証局スタートパックの構成

- 証明書を利用するアプリケーション
  - 学内無線LAN認証のための証明書発行に特化した、認証局スタートパックを実現する。
  - 認証方式はサーバ証明書とクライアント証明書を利用するIEEE802.1X EAP-TLS方式とする。
- 認証局システム
  - NAREGI (National Research Grid Initiative) で開発され、運用実績のあるNAREGI-CAを利用。
  - オープン・ソースであり、商用CA製品と同レベルの運用が可能なシステム。
  - 昨年度UPKIで開発した権限分離機能の拡張を含む。
- 無線LANシステム
  - FreeRadiusとOpenLDAPを利用する構成。

IEEE802.1Xの認証プロトコル

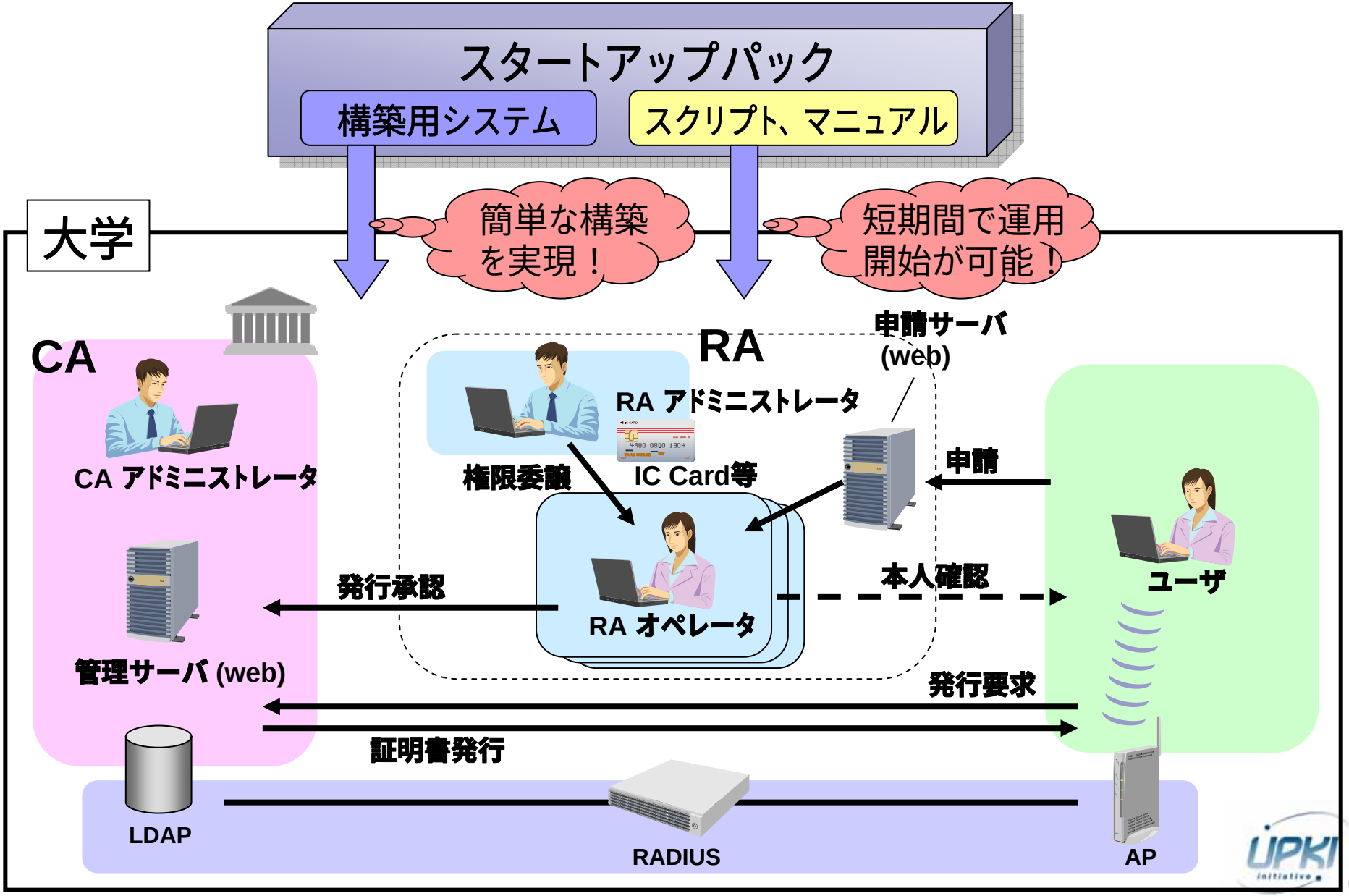
- EAP（Extensible Authentication Protocol）の種類

方式	クライアント認証方式	サーバ認証方式	セキュリティレベル	運用工数
EAP-TLS	証明書	証明書	高	高
EAP-TTLS	ID/パスワード	証明書	中	中
EAP-PEAP	ID/パスワード	証明書	中	中
LEAP	ID/パスワード	ID/パスワード	低	低
EAP-MD5	ID/パスワード	無し	低	低

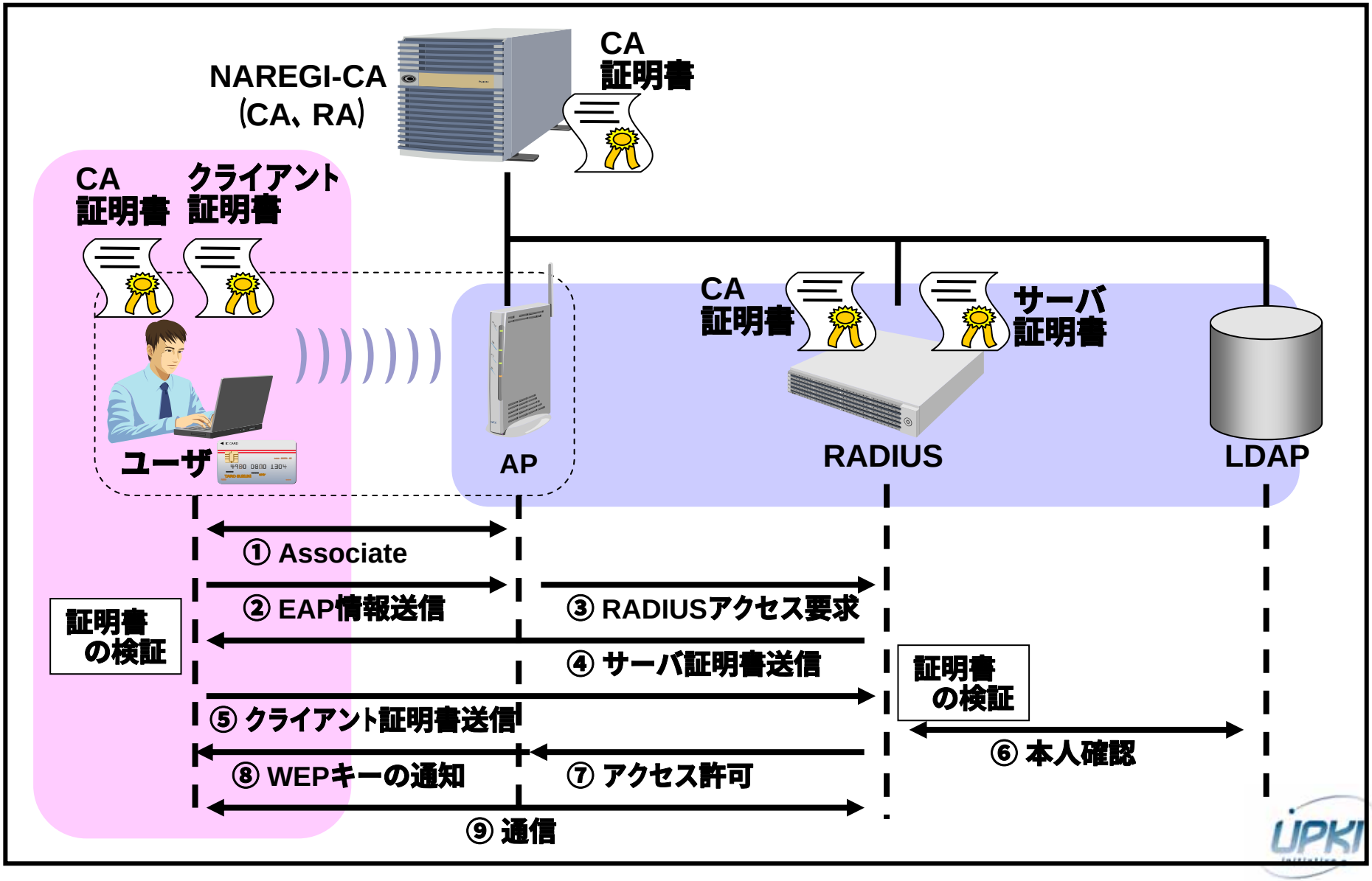
スタートパック内容

- スクリプト
  - インストール・スクリプト：
    - 認証局を簡単に構築するためのスクリプトを添付。
  - プロファイル：
    - 無線LAN認証の証明書発行のためのプロファイル、および、設定テンプレートを添付。
- ドキュメント
  - CSI認証局スタートアップガイド：
    - 認証局のインストール、および、無線LANと連携した認証に関する構成、設定を含めた構築方法を説明。
  - 無線LAN用認証局運用手順書：
    - 認証局の運用手順を説明。
  - 利用者用マニュアル：
    - 学内ユーザが構築した認証局を利用して証明書を取得し、これを用いて無線LANを利用する手順を説明。
- システム
  - NAREGI-CA　Ver2.2

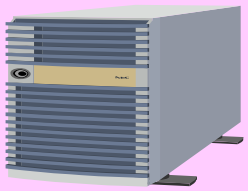
スタートアップパックのイメージ



無線LAN認証（EPA-TLS）の動作



最小構成（スペック）



サーバ

台数：　1台
性能：　（対応機種）PC/AT互換機（DOS/V）
SUN MICROSYSTEMS SPARCマシン
（CPU）　Pentium II 500MHz以上　（メモリ）　128MB以上
（HDD）　1GB以上　（表示）　800 × 600 ドット以上
OS:　Turbolinux Server 6.5以上、Solaris 2.6以上、
Miracle Linux Standard Edition V2.1以上、RedHat 7.3以上
APソフト: NAREGI-CA Ver2.2
FreeRadius 1.1.4以上
OpenLDAP　2.2.13-6以上

アクセスポイント

台数：　必要台数分
機能：　EAP-TLS認証方式をサポートしていること
Radius認証に対応していること

クライアント

台数：　（管理者端末）1台以上　（ユーザ端末）必要台数分
性能：　（対応機種）PC/AT互換機（DOS/V）
（CPU）　Pentium II 500MHz以上　（メモリ）　128MB以上
（HDD）　100MB以上　（表示）　800 × 600 ドット以上
OS:　Windows XP SP1、SP2　/　Windows 2000 Professional SP4
APソフト: Internet Explorer 6.0

開発、および配布計画

- 開発：
  - ２００７年３月中
- 配布：
  - ２００７年春 配布開始予定
  - 配布方法： UPKIイニシアティブからダウンロード

    ＊：認証局システム（NAREGI-CA Ver2.2）は
    NAREGIのダウンロードサイトにリンク