本資料について

- 本資料は下記文献を基にして作成されたものです。文書の内容は保障できないため、正確な知識を求める方は原本を参考にしてください。

  - 著者: 山崎　重一郎　　荒木　啓二郎
  - 論文名: 信用情報と利用ポリシーの管理が可能な相互認証を実現する認証基盤の提案
  - 出展: 情報処理学会論文誌　Vol.40 No.1
  - 発表日: 1999年1月

Jan.1999

信用情報と利用ポリシーの管理が可能な相互認証を実現する認証基盤の提案

山崎　重一郎*　　荒木　啓二郎**
* 財団法人九州システム情報技術研究所
** 九州大学大学院システム情報科学研究科

名城大学理工学部情報科学科
01J080　坂野　文男

研究背景

- インターネットの浸透とともにセキュリティの保護やプライバシーの保護のために公開鍵暗号に基づくデジタル認証の必要性が認識されるようになってきた
  - 認証局によって組織的に発行されるX.509デジタル証明書を用いた認証基盤は、SSL（Secure Sockets Layer）やS/MIME（Secure Multipurpose Internet Mail Extension）などのアプリケーションを中心として普及し始めている

デジタル認証システム

- 現在、実用化されているデジタル認証システムは、主に暗号化電子メールや電子商取引など単一の利用領域を前提に設計されている物がほとんどである

- 利点
  - 認証局とサービスを行う機関が同一になり運用が単純になる
- 課題
  - 利用するサービスに応じた公開鍵証明書を所持しなければならない
  - 利用ポリシーが1つの用途に限定されてしまうと、複数のサービスを連携させて利用することができない

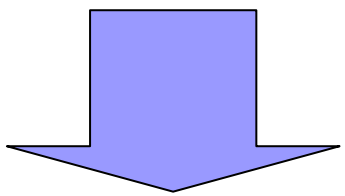
提案方式

- 従来の認証基盤との相互性を保ちつつ、異なる利用ポリシーや信用情報を要求するサービスを統合的に利用することを可能にする相互認証基盤の提案をする

証明書と利用ポリシーの分離

- 有効な利用方法や権限をサービス側から定義したもの

- 認証と利用ポリシーが一体化されているデジタル証明書は、他の用途には利用できない

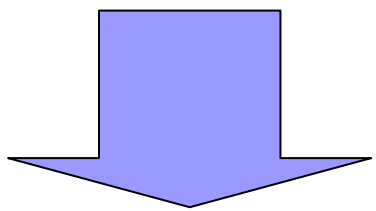


- 公開鍵証明書の中に利用ポリシーを埋め込まず外付けで管理する。

認証と与信の分離

- 与信とは権威のある機関がそれが真実であると保証すること

- 与信情報にはその人の所属団体の情報なども含むことがあるが、このような情報の寿命は公開鍵の寿命と比較すると頻繁に変わる

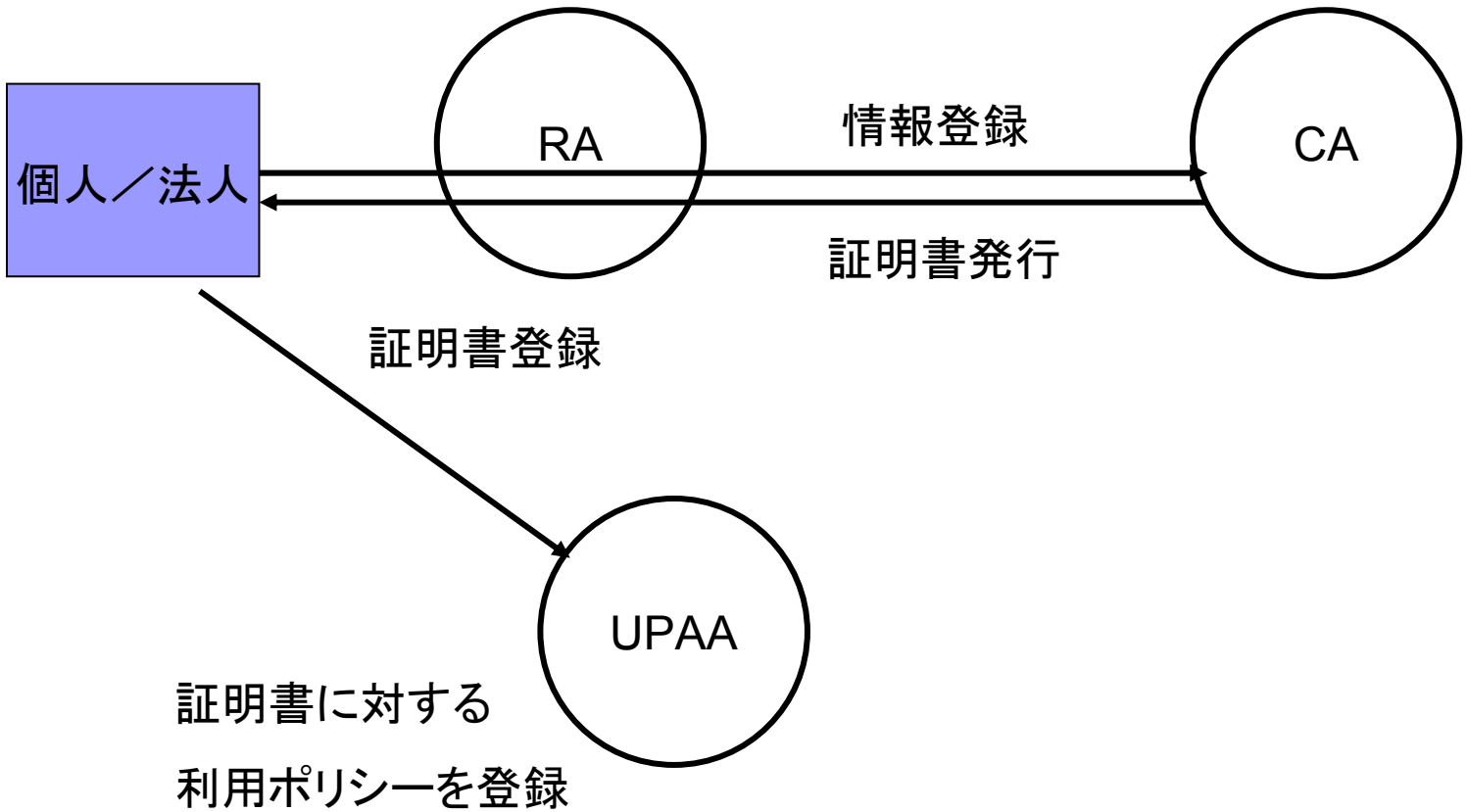


- デジタル証明書の中に与信情報を埋め込まず、外付けで管理する

3権分立モデルの構成

- 認証局の証明書発行に関する機能を、
  証明書発行局（CA：Certification Authority）、
  登録機関（RA：Registration Authority）、
  利用ポリシー定義機関
  （UPAA：Use Policy Approval Authority）
  の3つに分ける

3権分立モデル



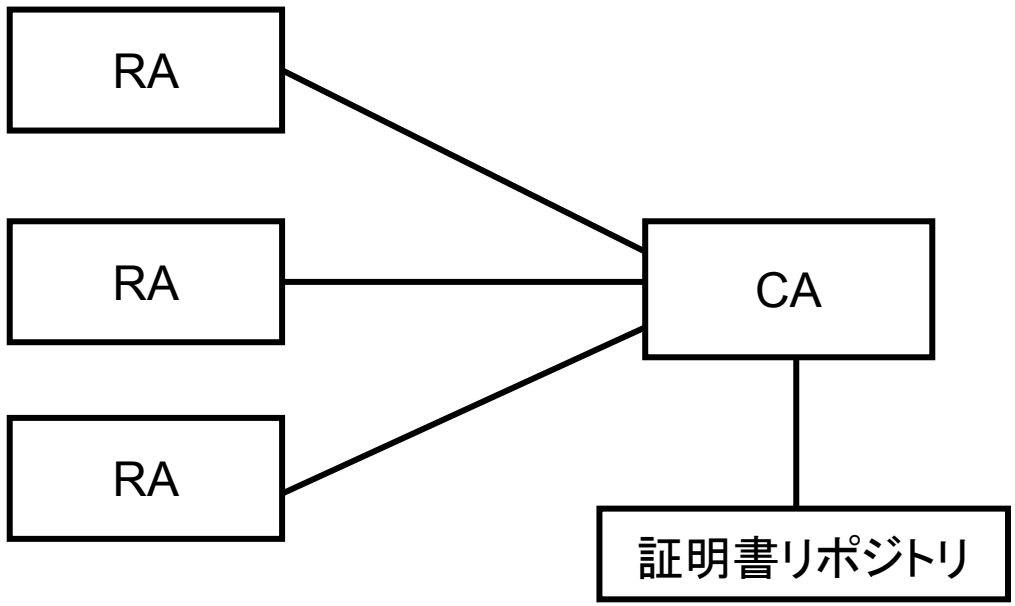
CA：証明書発行局

- 公開鍵証明書の発行のみを行う
- 証明書リポジトリへの公開鍵証明書の登録の権限を持つ
- 責任は、秘密鍵の管理と技術的なセキュリティの確保に限定される
  - 3権分立モデルでは1つの証明書で様々なレベルの証明書として使用されるため、非常に高いレベルの安全性が要求される

RA：登録機関

- 実際に本人確認を行い、証明書を本人に渡す窓口になる機関
- 発行された証明書に関する基本的な責任をもつ
  - 与信機関としても機能する
- 発行済みの証明書に対して、信用情報のみを定義することもできる

RAとCAの関係



1つのCAに対して複数のRAが対応することができる。

よって、CAにかかるセキュリティーコストを分散することができる

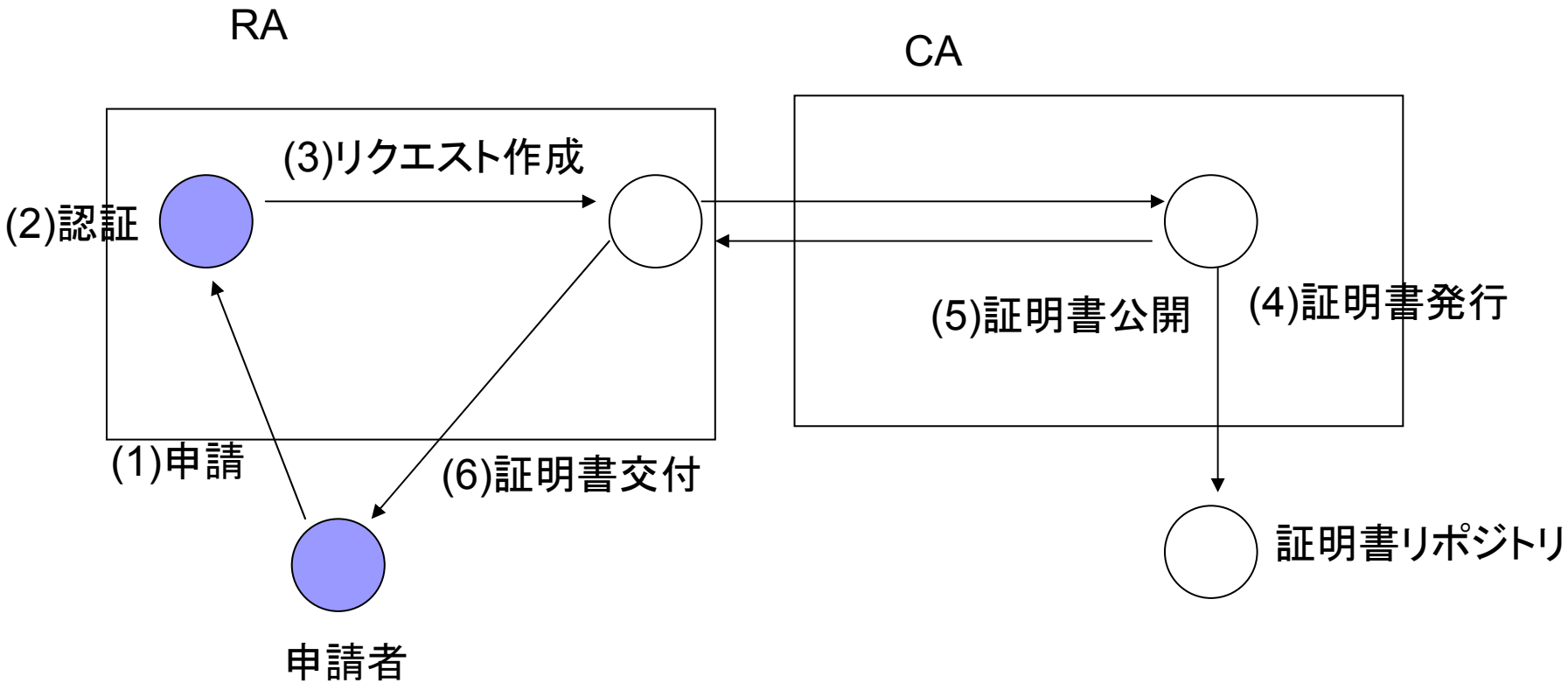
UPAA：利用ポリシー定義機関

- 各サービスが運営するサービスであり、ユーザの証明書に対してそのサービスに対する利用ポリシーを定義するもの

証明書リポジトリ

- CAが発行した公開鍵証明書を公開する公的なサービスを行う
  - 相手の公開鍵証明書を入手したいときに利用される
- 信用情報の公開も証明書リポジトリを介して行われる
- 証明書リポジトリを通じて名前空間の管理が行われる

公開鍵証明書の発行



(2)
(3)
(4)
(5)
(6)

UPAAによる利用ポリシーの登録

- 利用したいサービスのUPAAに自分のデジタル証明書に一定の権限を登録してもらう

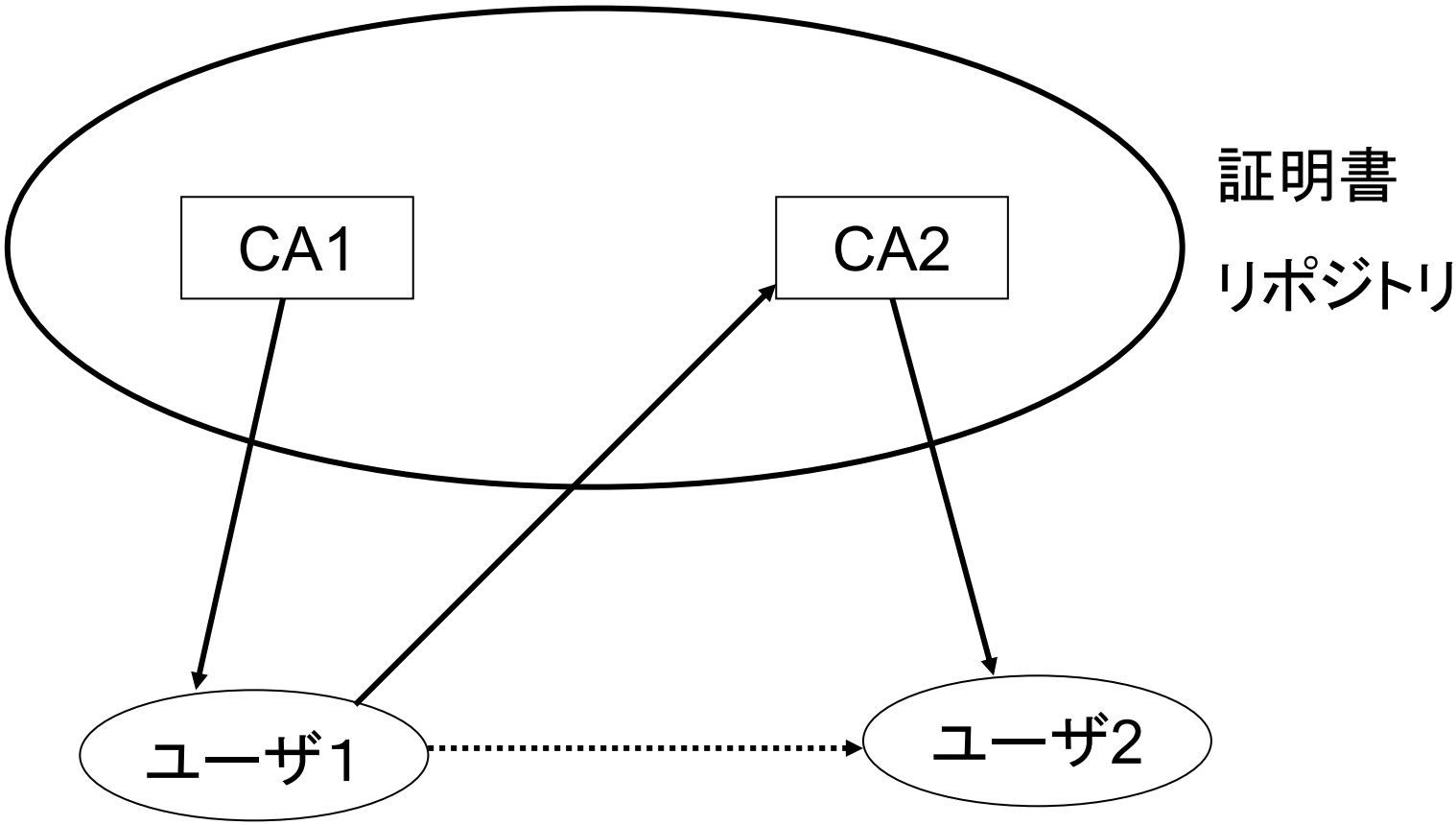
RAによる信用情報の登録

- 保証を受けたい場合、窓口に自分の公開鍵証明書を持ち込んで信用情報の登録を依頼する

相互認証

- 証明書リポジトリを利用して認証を行う
- 自分と異なる認証局から認証されている公開鍵証明書を検証する場合、相手の認証局の公開鍵証明書を信頼できる証明書リポジトリから入手する
- 信頼できるリポジトリとはSSL上のLDAP（Lightweight Directory Access Protocol ）で通信を行う

証明書リポジトリによる相互認証



まとめ

- 信用や利用ポリシーの制御を含む相互認証を実現する統合的な認証基盤モデルを提案

- 認証と利用ポリシーや認証と与信の分離により信用情報や利用ポリシーの管理が単純化され、デジタル証明書の汎用化できた

終わり