証明書検証とパス構築

PKIプロジェクト

情報基盤センター PKI プロジェクト
UT-CA

今後考えられるシナリオ（NII）

- 各大学にはCAが立ち上がる
  - インソースかもしれない
  - アウトソースかもしれない
  - 基幹校を決めて、業務委託するかもしれない（昔の国立大学の電算業務に例あり）
- それらの間の「大学間連携」が必要になる
- パス構築とパス検証の技術が必要になる

必要となる技術

- 利用者には証明書を検証する作業が必要になる
- 証明書検証は、パスの構築と検証をともなう

- Windowsでは現在ごく単純な場合しかできない

必要となる技術

- もし「できる」としても、クライアントがいちいち検証するのは正しい解か？
- ひとつのルートCAのもと、全部を収容するのは正しい解か？
- パス構築と検証は必要悪である。
- でも、クライアントが個々に負担を求められるのは正しくない

PKIプロジェクトの考えるシナリオ

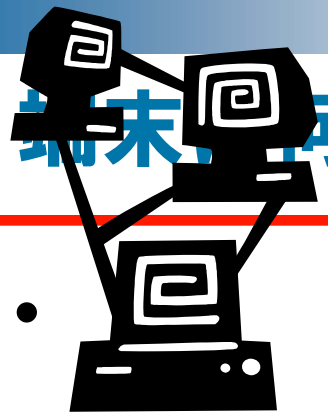
- パス構築と検証は必要悪である
- でも、検証サーバがそれらを代行するのがよいだろう
- 2006年度は日立のCVSを試用した

日立CVS

- 製品の特徴

- クライアントはCVSに検証対象の証明書を渡して検証をリクエスト
- CVSは、パスを構築して検証する
- クライアントに「Yes」（Yesの場合は構築されたパス）と「No」（Noの場合はエラーコードも）を返す

端末、何もしない



CVS

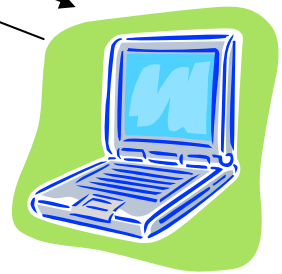
パス検証を行う

Yes/No

Request

S/MIMEにおいて、相手側の
証明書の検証をする必要がある

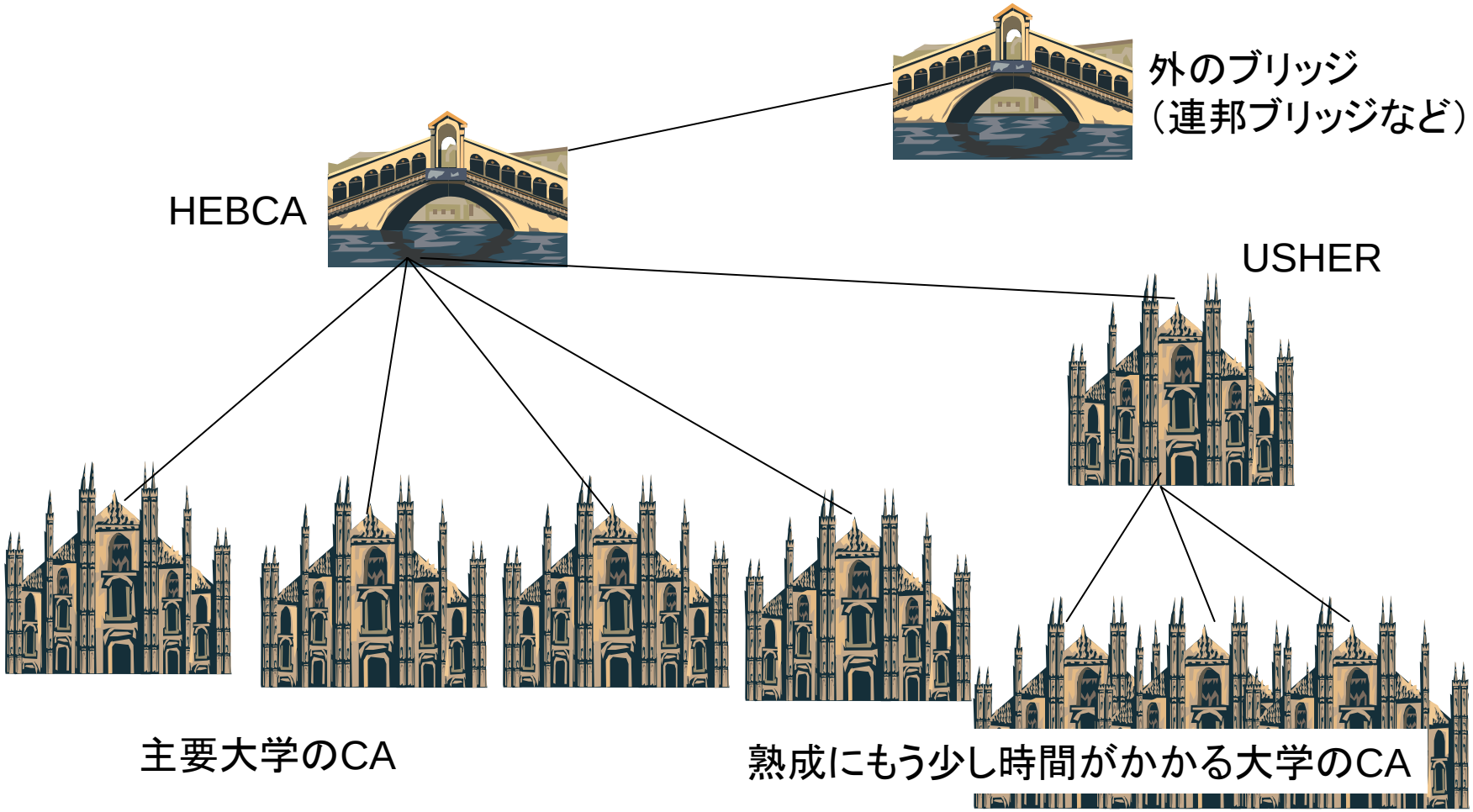
自分でパスを構築して検証する
のではなく、CVSに丸投げする



日立CVSの試用

- 現在はデータの収集が終わったところ
- （Outlookに対する）プラグインを日立が作っている
- ブリッジ、メッシュを含む複数のトポロジーで実験

USのトポロジー



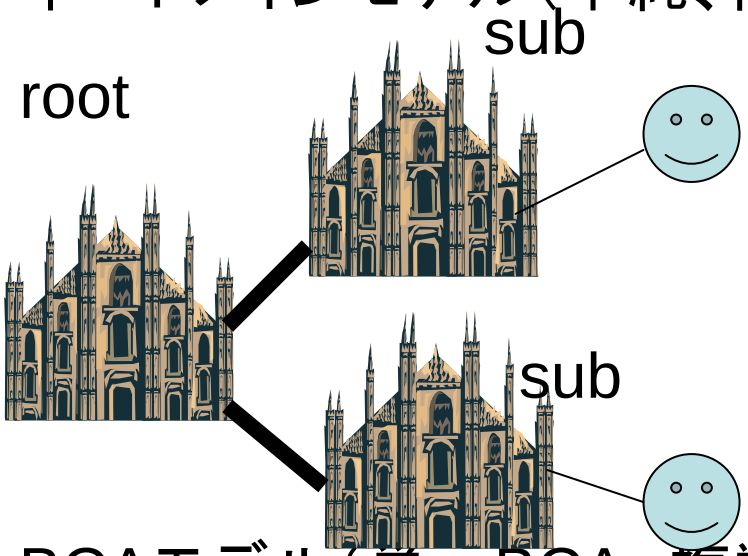
日本では？

？

東大CA

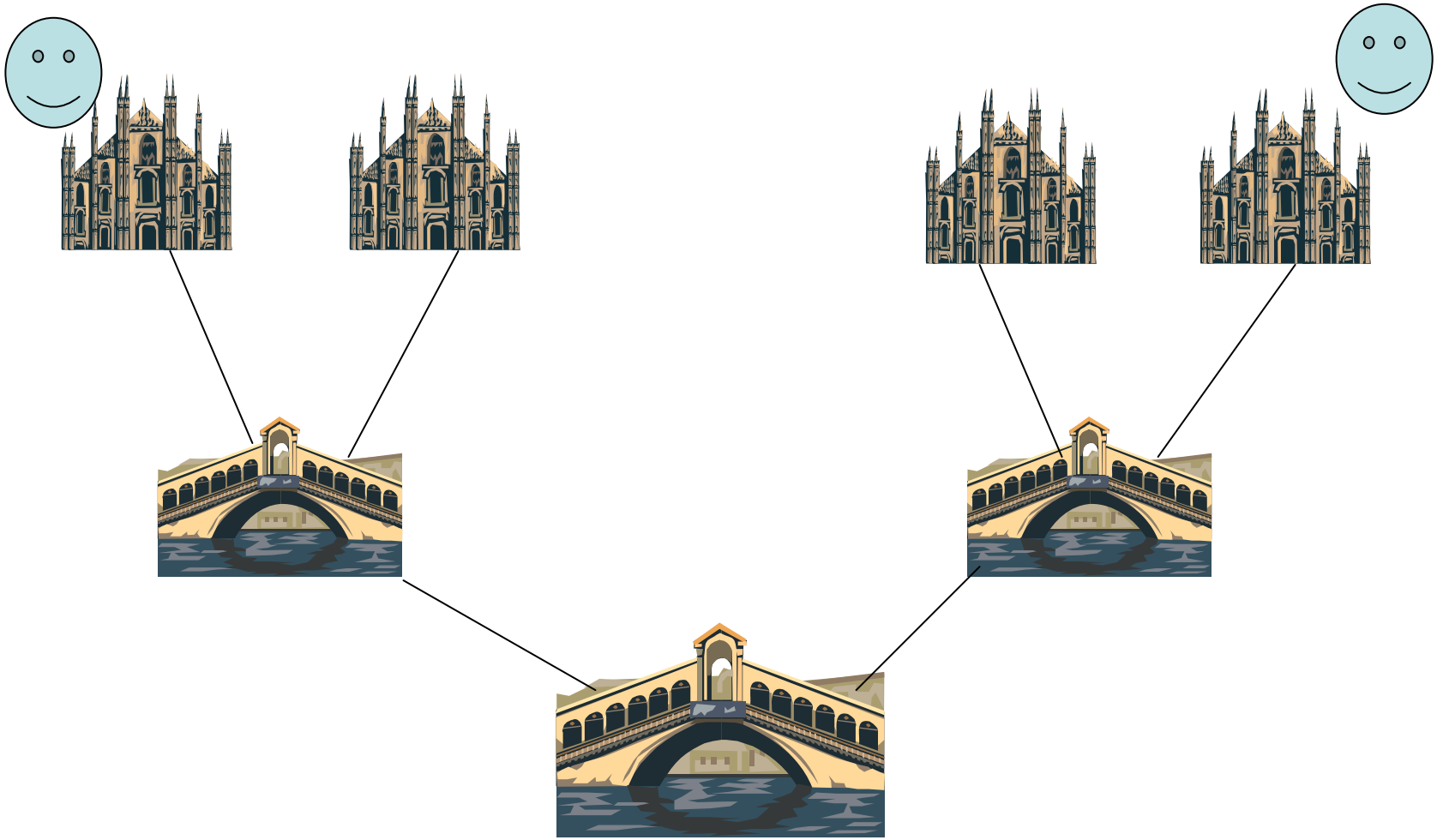
実験のシナリオ

- 信頼モデルの種類
  - 単一ドメインモデル（単純、階層）

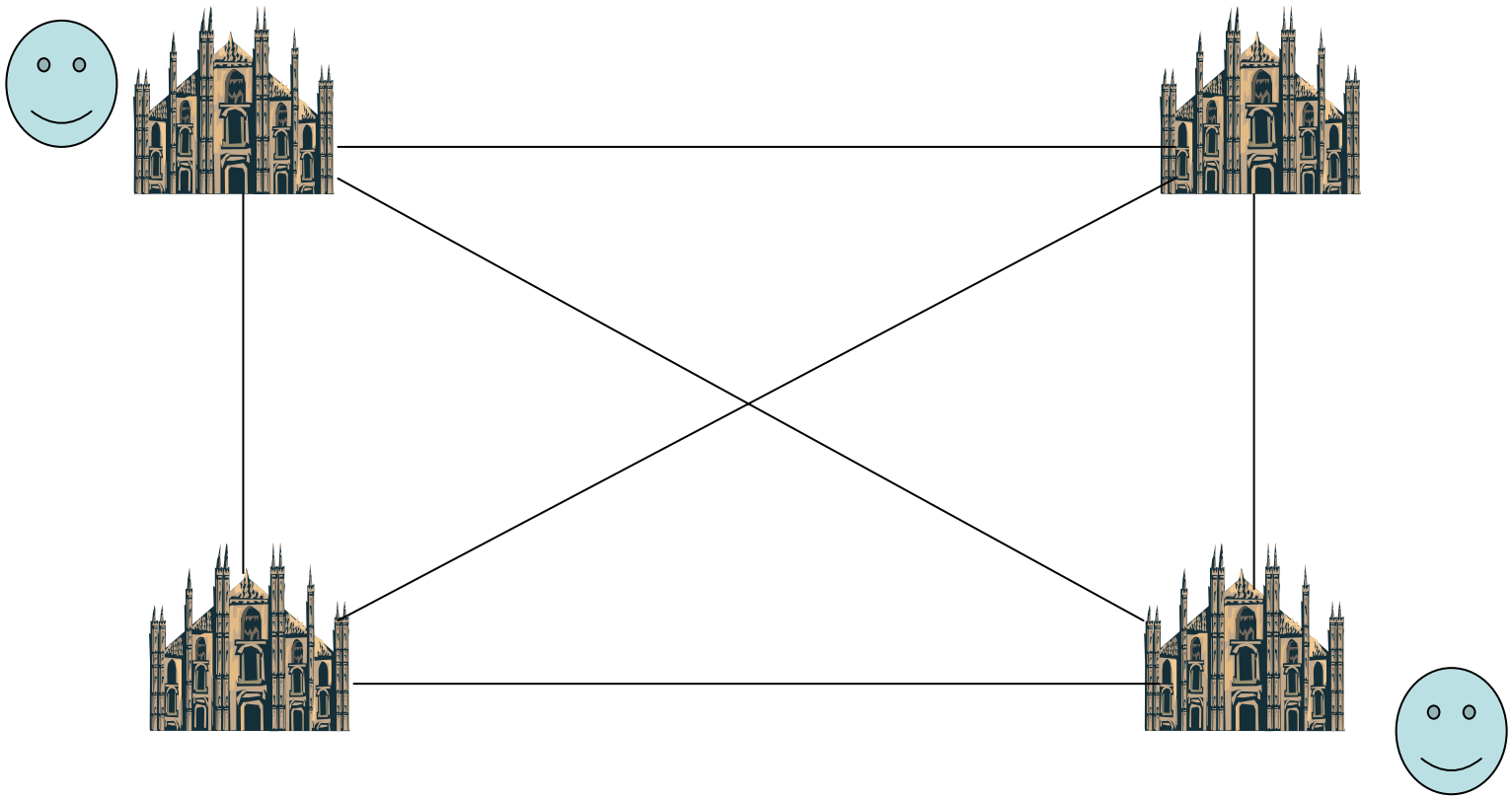


  - BCAモデル（単一BCA、複数BCA）
  - メッシュモデル

BCAモデル



メッシュモデル



対象アプリケーション

- S/MIME
- SSLクライアント証明書を使ったWeb認証

考えられる将来

- 大学において「相互信頼網」を作ることは必要か？需要はどこにあるか？
  - 大学院の3割シーリングなど、大学間で学生の流動性を促す動き
  - 大学間共同研究の常態化
- 需要がある場合、USの先行事例は注目に値する
- Single Big Rootは動かないのではないか？

とりあえずの結論

- パス検証を行うサーバの試用とログ採取を行った
- 将来の大学間認証基盤のトポロジーの最適化などを考えるときの解析材料にしたい

- パス検証を行う需要があるかどうかが、将来の採用の鍵だろう