PKI の課題を解決する認証システム　ASE の提案

050428468　川島隆太
渡邊研究室

1. はじめに

インターネットの普及に伴い，電子商取引や電子申請等の電子化が急激に進んでいる．しかし，インターネット上には盗聴，不正アクセス，なりすまし，改ざん，否認といった脅威がある．そこで公開鍵暗号方式によるセキュリティ基盤 PKI(Public Key Infrastructure)が注目されている．

本稿では，PKI を参考に企業内ネットワークで利用できる，セキュリティが高く管理負荷の少ない認証システム ASE(Authentication System for an Enterprise network) [1]を検討し，その実現を試みた．

2. PKI とその課題

PKI では，各ユーザの公開鍵を認証局（CA：Certification Authority）が署名し，公開鍵証明書を発行する．CA の公開鍵は更に上位の CA が証明書を発行する．PKI はこのように階層構造になっているが，最上位の root CA の公開鍵証明書を発行する機関がなく，root CA 自身が公開鍵証明書を発行（自己署名）している．しかし，この公開鍵証明書の発行者が正当であることを検証する方法がない．そのため，ユーザが気づかないうちにレジストリを操作され，root CA の公開鍵を偽造されてしまう可能性がある．

また，PKI では発行した公開鍵証明書を被発行者に渡してしまうため，有効性を確認するための失効情報を管理しなければならない．失効情報は原則的に増加し続けるため管理が大変であり，失効情報のデータが大きくなると，有効性の確認時に多くの時間を要するという課題がある．

3. ASE

そこで ASE では図１のように信頼関係を構築する．

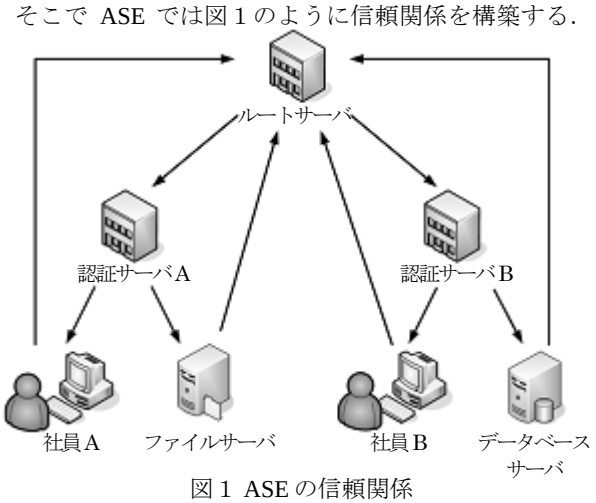


図１ ASE の信頼関係

まず，ルートサーバが部門ごとに設置された認証サーバに公開鍵証明書を発行する．次に，認証サーバが各部門の社員に公開鍵証明書を発行する．さらに，各社員はルートサーバに公開鍵証明書を発行する．このように信頼関係を環状にすることにより，公開鍵証明書の検証時に自分を最上位に位置づけすることができ，全ての公開鍵証明書が正しいことを検証できる．

また，ASE では発行した公開鍵証明書を被発行者に渡すのではなく発行者自身が管理保存することとする．このため，公開鍵証明書が失効した場合に失効情報などを必要とせず，証明書が無効となった場合は，管理している公開鍵証明書を単に削除するだけでよい．

ASE における公開鍵証明書の有効性検証は検証者が検証時にオンデマンドで必要な情報を収集することにより行う．図１の社員 A が社員 B を認証する場合には以下のようになる．社員 A はルートサーバへ社員 B の公開鍵証明書を問い合わせる．問い合わせに対しルートサーバは社員 B が所属している認証サーバ B の公開鍵証明書を返答する．社員 A は認証サーバ B へ社員 B の公開鍵証明書を問い合わせる．問い合わせに対し認証サーバ B は社員 B の公開鍵証明書を返答する．上記により認証パスの構築は終了し，検証が成功した場合，社員 B の公開鍵は信頼することができる．

4. ASE の実装

検証処理は OpenSSL[2]を用いた検証プログラムを参考に作成した．そのままでは階層構造を実現できないため，披検証者に至るまでの検証が一度にできるように改造した．また，有効性の確認など ASE では不要な部分を削除した．さらに，検証処理にあわせて，必要な公開鍵証明書をクライアントとサーバ間で送受信するプログラムを新規作成した．

上記のプログラムの動作を確認し，ASE の機能を検証した．

5. むすび

企業ネットワークにおいて認証基盤を導入するために，信頼関係を環状にし，公開鍵証明書は発行者が保持して自ら管理を行う ASE を検討しその実装を試みた．今後は ASE の評価を行う．

参考文献

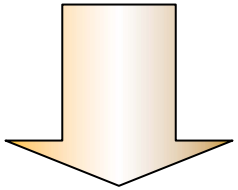
[1] 坂野文男, 保母雅敏, 渡邊晃：企業ネットワークにおける管理負荷の少ない認証システムＡＳＥの提案，SCIS2006 シンポジウム論文集(2006).
[2] OpenSSL “http://www.openssl.org/”

企業ネットワークにおける
高セキュリティ認証システム ASEの検討

名城大学理工学部情報工学科
渡邊研究室
050428468 川島隆太

研究背景

- 近年のインターネット普及に伴い、電子商取引や、電子申請等の電子化が進んでいる
- ネットワーク上には「盗聴」、「なりすまし」、「改ざん」等の脅威がある



暗号技術の重要性が高まっている

暗号技術

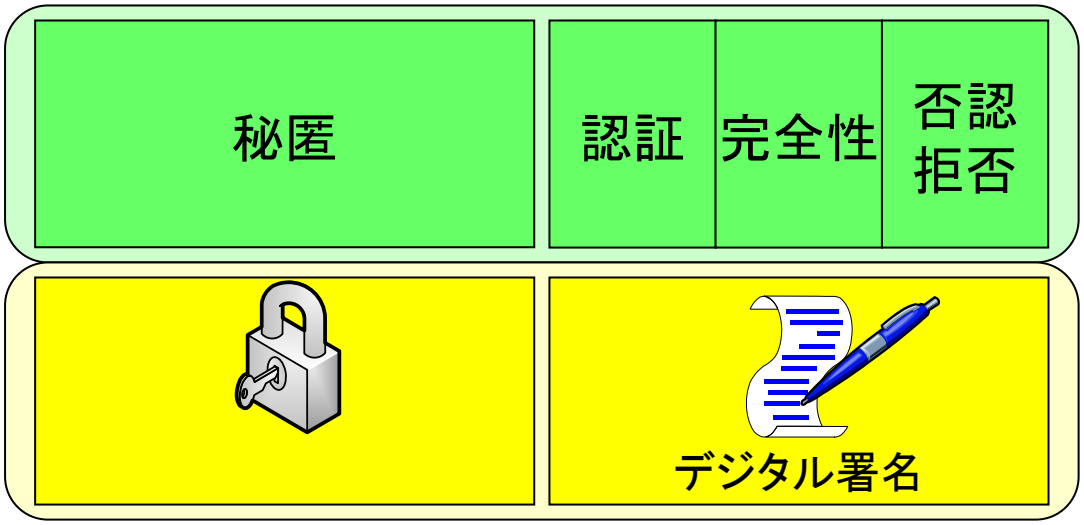
- 共通鍵暗号方式
  - 暗号化する時と復号する時に同じ鍵を利用
  - 鍵を秘密に管理する必要があり、データのやり取りする相手ごとに別の鍵を用意しなければならない
- 公開鍵暗号方式
  - 暗号化する時と復号する時に異なる鍵を利用
  - 一方の鍵を「公開鍵」と呼び，不特定多数のユーザに公開しても構わない
  - 公開鍵は正しいことが保証されていなければならない

PKI（Public Key Infrastructure）

- 公開鍵暗号方式を利用したセキュリティの基盤
- PKIの構築により以下のものを提供できる

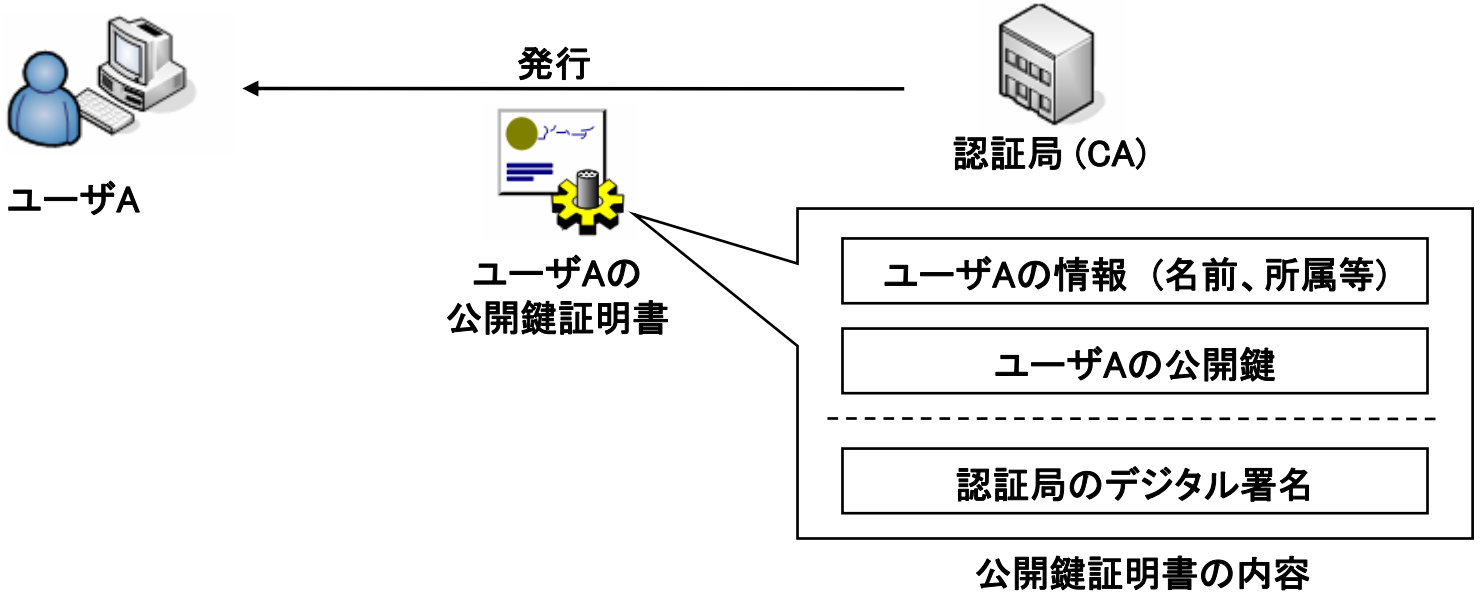
PKIが提供するもの

公開鍵証明書



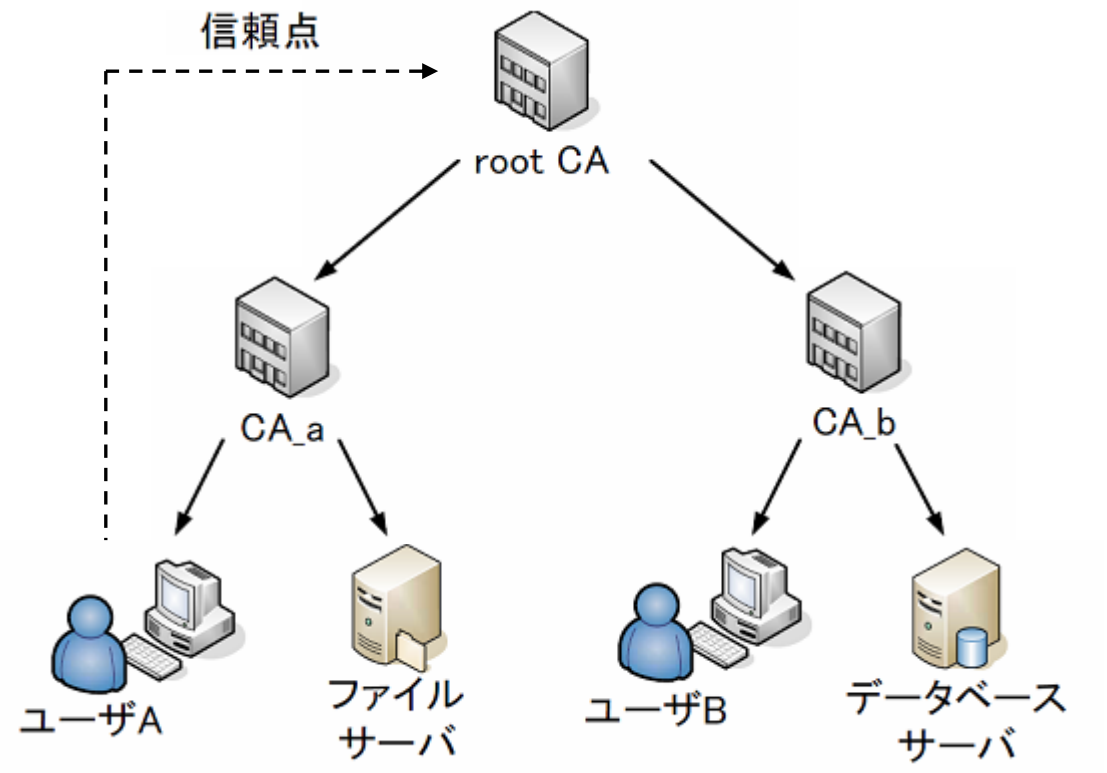
公開鍵証明書

- 認証局CA(Certificate Authority)という信頼できる第三者機関が公開鍵の所有者を保証したもの
- 公開鍵が、正当なものか、他人のものでないか、改ざんされていないかを検証できる

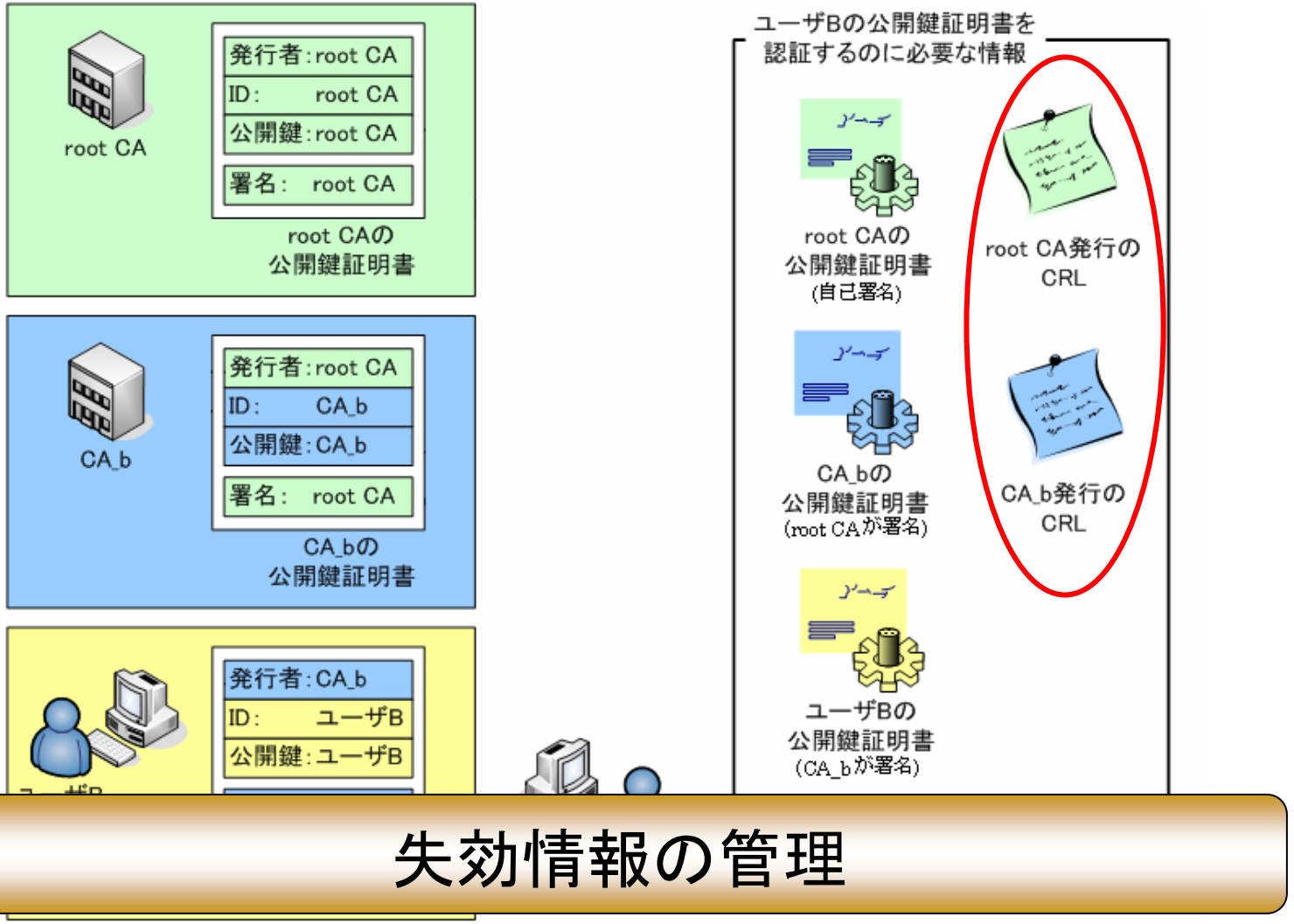


信頼関係の構造

- 認証局CAは公開鍵証明書を上位のCAに発行してもらうことにより信頼関係ができる



公開鍵証明書の検証に必要な情報

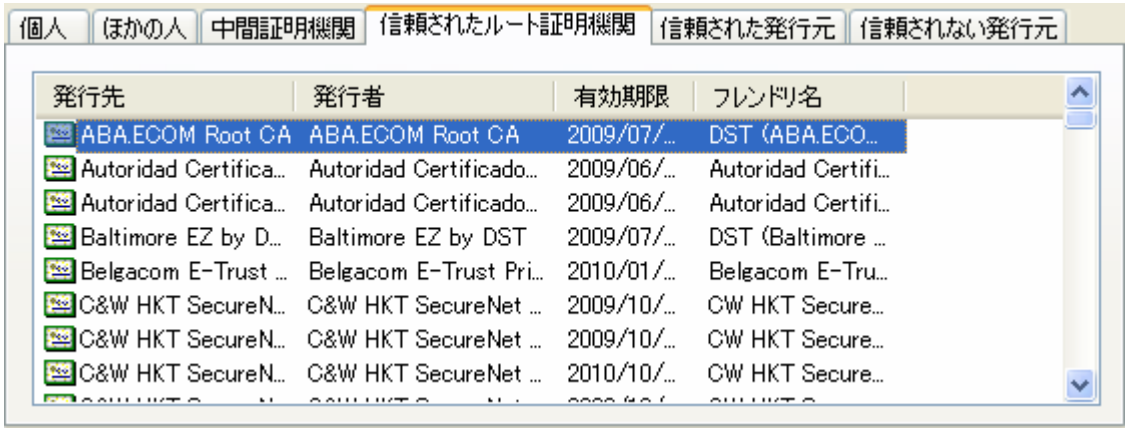


失効情報の管理

CRL（Certificate Revocation List）

- 失効された証明書の情報を列挙したリスト
- PKIでは、公開鍵証明書がCRLに掲載されていないことをもって有効性を確認する
  - 失効情報は増加し続けていくため、データが大きくなると有効性の確認時に多くの時間がかかる
  - CRLの内容は定期的に更新されるため、常に最新の失効情報とは限らない

自己署名の公開鍵証明書偽造



偽造前

偽造後

PKIの課題

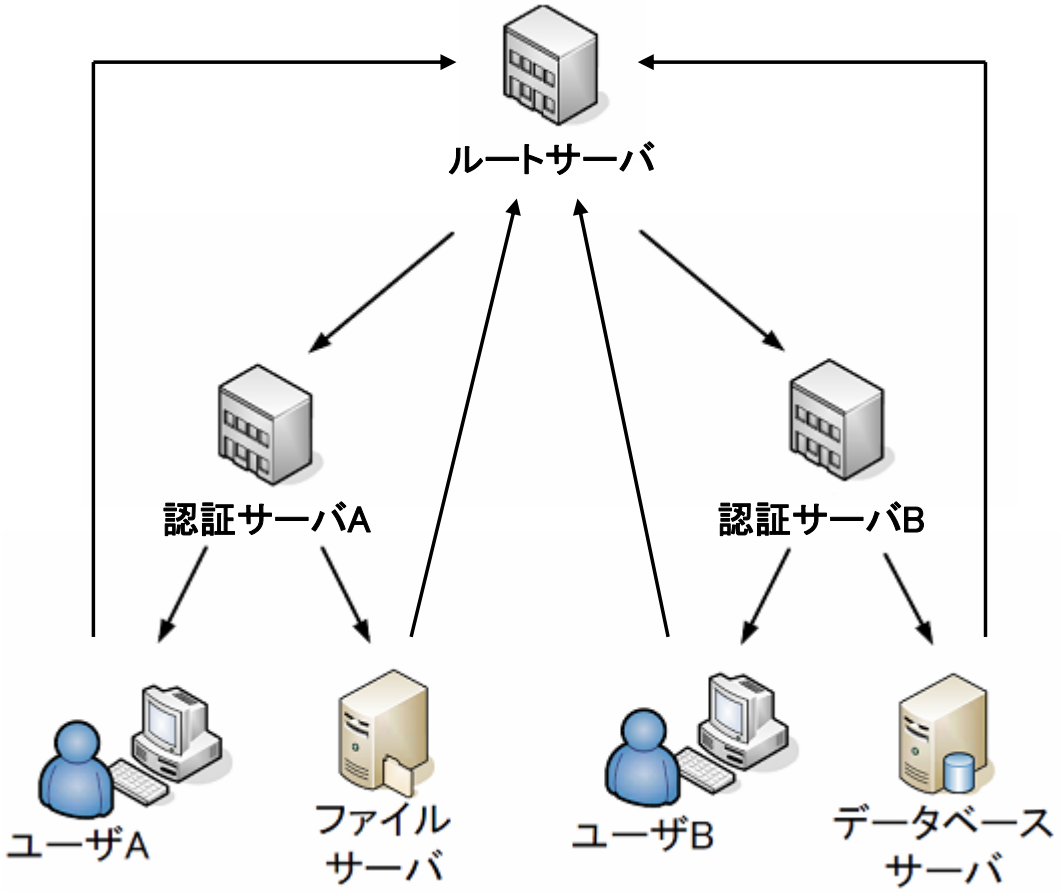
- 企業ネットワークでは以下のことが課題になると考えられる
  - 自己署名の公開鍵証明書を偽造可能
  - 失効情報の管理負荷が多い

ASE

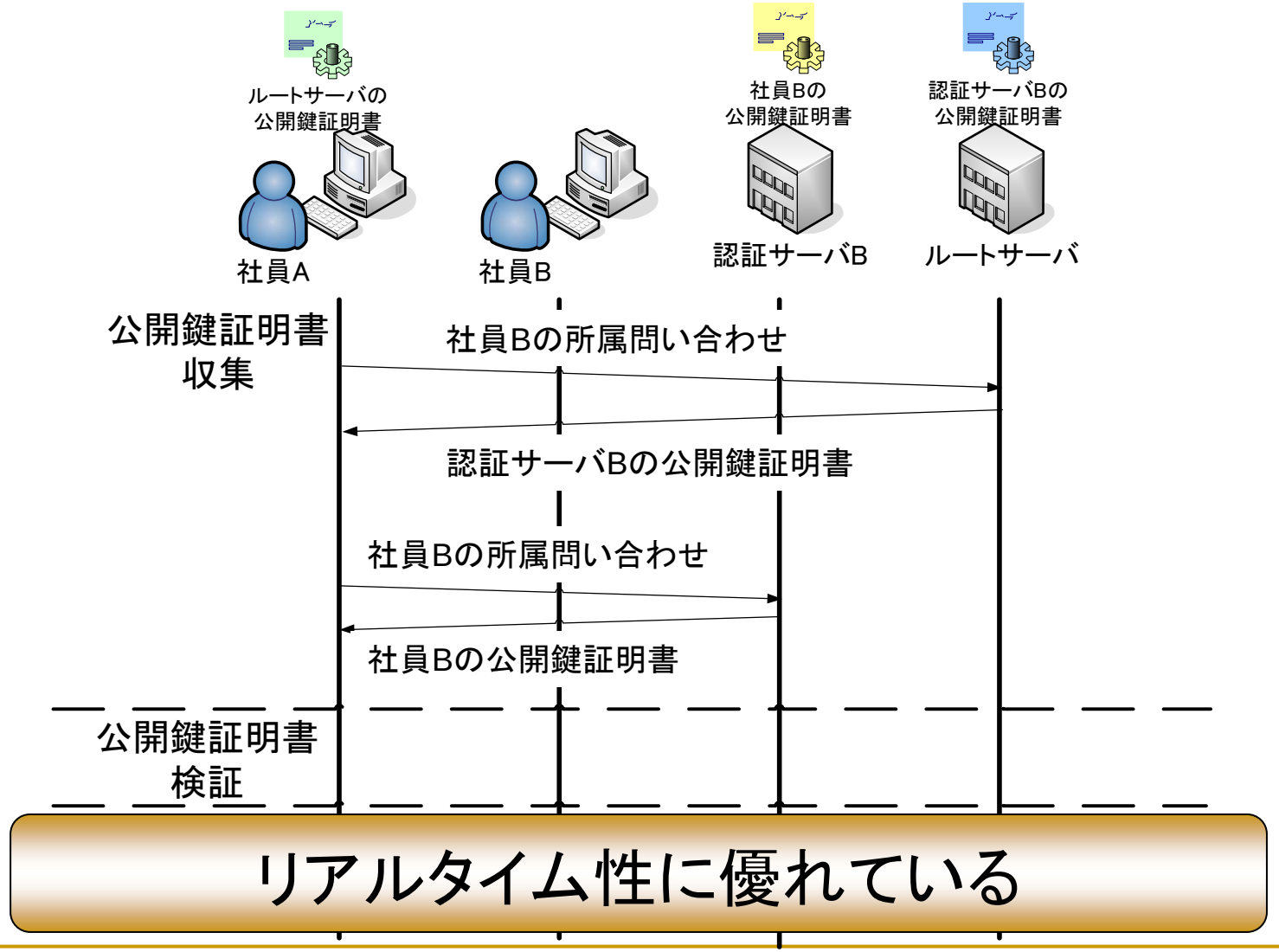
- 認証システムASE(Authentication System for an Enterprise network)を検討し、実現を試みた
  - 信頼関係を環状にする
  - 公開鍵証明書は発行者が保持し、自ら管理する
  - 信頼関係をオンデマンドで検証する

信頼関係を環状化

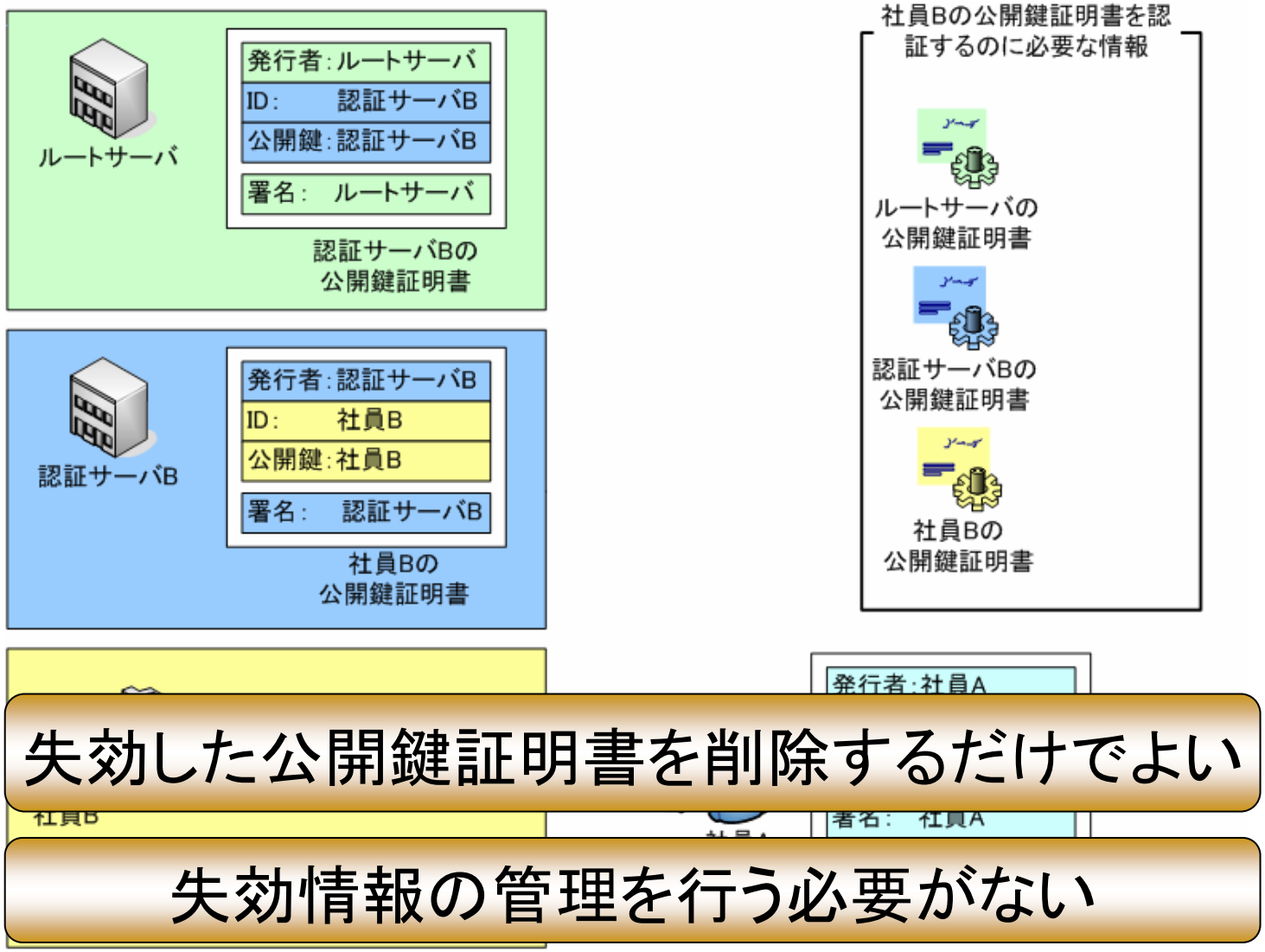
- ルートサーバの公開鍵証明書が検証可能



オンデマンド検証

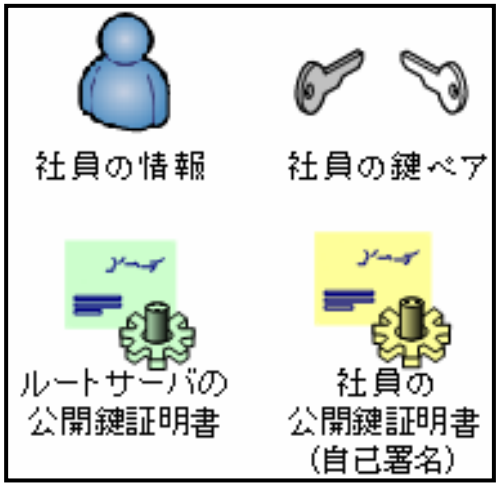

ルートサーバの
公開鍵証明書
社員Bの
公開鍵証明書
認証サーバBの
公開鍵証明書
社員A
社員B
認証サーバB
ルートサーバ
公開鍵証明書
収集
社員Bの所属問い合わせ
認証サーバBの公開鍵証明書
社員Bの所属問い合わせ
社員Bの公開鍵証明書
公開鍵証明書
検証
リアルタイム性に優れている

公開鍵証明書の管理方法



ICカードの導入

- 社員のICカードは認証サーバが発行する
- 認証サーバにて社員で行う公開鍵証明書の発行手順を済ませてしまうため、社員は発行に関する作業が不要になる



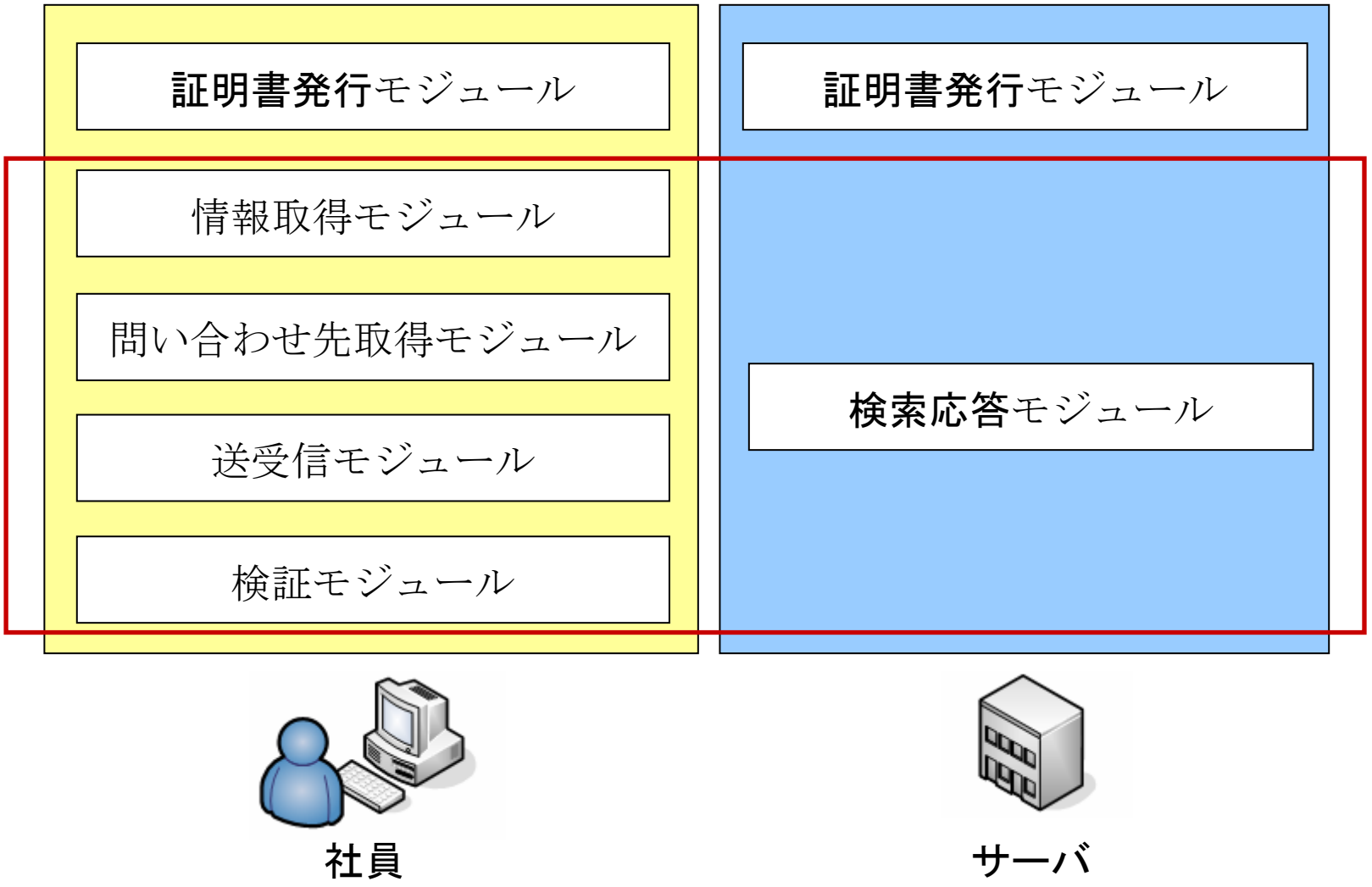
ICカードが持つべき情報

PKIとの比較

		PKI	ASE
最上位の公開鍵証明書		×	○
リアルタイム性		△	○
管理負荷	導入初期	○	△
	通常運用時	△	○

- 最上位に位置するルートサーバの公開鍵証明書偽造を検証できる
- 公開鍵証明書を発行者自身が保管しオンデマンドで検証するため、リアルタイム性に優れている
- 失効情報の管理を行う必要がない

モジュール構成


証明書発行モジュール
情報取得モジュール
問い合わせ先取得モジュール
送受信モジュール
検証モジュール
証明書発行モジュール
検索応答モジュール
社員
サーバ

むすび

- 企業ネットワークにおいて認証基盤を導入するために以下の認証システムASEの機能を検証
  - 信頼関係を環状にする
  - 公開鍵証明書は発行者が保持し，自ら管理する
  - 信頼関係をオンデマンドで検証する

- 今後は、ASE の性能測定、評価を行う