

企業ネットワークにおける認証基盤の構築に関する研究

坂野 文男[†] 保母 雅敏[‡] 渡邊 晃[†]

名城大学理工学部[†] 名城大学大学院理工学研究科[‡]

1. はじめに

インターネット普及を受けて、電子商取引や、電子申請等の電子化が進んでいる。しかし、ネットワーク上には盗聴、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を用いた認証基盤である PKI (Public Key Infrastructure) が注目されている。PKI は本人認証、パケット偽造防止、否認拒否など様々な用途で利用され、企業内ネットワークにおいても PKI による認証基盤を導入する傾向がある。本稿では企業が PKI を導入するうえでどのような課題があるかを考察し、その課題を解決するための認証基盤の一方式について提案する。

2. PKI とその課題

PKI は現実社会における封書、印鑑、内容証明郵便、免許証に相当する機能を実現することができるネットワークインフラストラクチャのための規約であり、それに基づくシステム、システムの運用者、システムの運用ポリシーの総称でもある。現在では、電子社会に包括的セキュリティを提供する最有力候補の地位を得ている。

しかし PKI には以下のような課題がある。ユーザの公開鍵証明書は認証局 CA (Certificate Authority) により発行され、CA の公開鍵証明書は更に上位の CA により発行される。しかし、最上位の CA (root CA) の公開鍵証明書を発行する機関はなく、通常は root CA 自身が公開鍵証明書を発行 (自己署名) しているが、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。そこで、root CA の公開鍵はユーザがあらかじめ信頼できる方法で取得しておき、厳重に管理する必要がある。また、PKI では発行し

た公開鍵証明書の有効性を確認するために証明書の失効情報を管理する必要がある。この失効情報の確認方法には CRL (Certificate Revocation List) 方式と OCSP (Online Certificate Status Protocol) 方式がある。CRL 方式は各ユーザが公開鍵証明書の検証をする前に CA から CRL を取得しておく必要がある。また CRL は決められた周期で発行されるため、公開鍵証明書が失効された場合でも、次の CRL が発行されるまでは失効情報が利用者に伝わらない。OCSP 方式は公開鍵証明書の検証時にリアルタイムで OCSP サーバへ有効性を確認するプロトコルである。しかし、OCSP サーバの失効情報の更新は CRL を利用することが多く、必ずしも最新の情報であるとは限らない。

3. 提案方式

本稿では、企業内ネットワークという閉じた世界における認証基盤を検討する。上記 PKI の課題を解決するため以下のような特徴を持たせる。

- 1) 信頼関係を環状にする
- 2) 公開鍵証明書はその発行者が保持し、自ら管理する
- 3) 信頼関係はオンデマンドで検証する

提案方式の信頼関係を図 1 に示す。矢印は公開鍵証明書の発行の方向である。

- (1) 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
- (2) 認証サーバが各部門の社員に公開鍵証明書を発行する
- (3) 各社員がルートサーバに公開鍵証明書を発行する

この認証の方法により信頼関係が環状になるため、公開鍵証明書の検証時に自分を最上位に位置づけることができ、ルートサーバの公開鍵証明書が正しいことを検証することができる。

“Researches on the architecture of authentication infrastructure in an enterprise network”

[†]Fumio Banno & Akira Watanabe

Faculty of Science and Technology, Meijo University

[‡]Masatoshi Hobo

Graduate School of Science and Technology, Meijo University

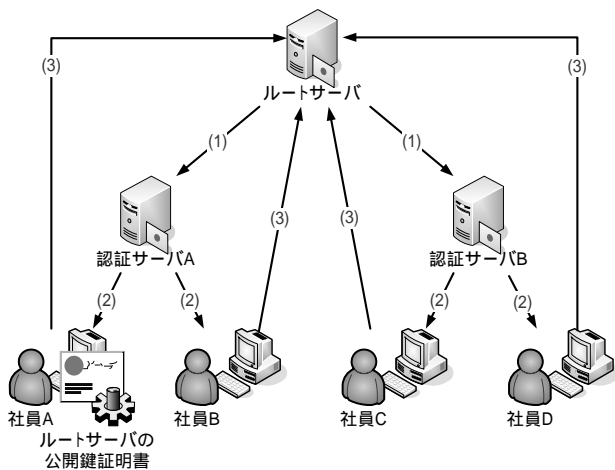


図1 提案方式の信頼関係

また本提案方式では、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。このため公開鍵証明書が失効した場合は、管理している公開鍵証明書を単に削除するだけである。公開鍵証明書の有効性はユーザが検証時に公開鍵証明書をオンデマンドで収集することにより確認することができる。このため失効情報の管理が不要になる。

例として社員 A が社員 D を認証する場合の認証パスの構築の流れを示す。

- 1) 社員 A は社員 D を認証するため、社員 D に対し社員 D の ID 情報と公開鍵証明書の所有者を問い合わせる
- 2) 社員 D は ID 情報と自分の公開鍵証明書の管理者（認証サーバ B）の ID 情報を社員 A へ返答する
- 3) 社員 A は認証サーバ B に対し社員 D の公開鍵証明書を要求するとともに認証サーバ B の公開鍵証明書の管理者を問い合わせる
- 4) 認証サーバ B は社員 D の公開鍵証明書が有効であれば、社員 D の公開鍵証明書及び認証サーバ B の公開鍵証明書の管理者（ルートサーバ）の ID 情報を社員 A へ返答する
- 5) 3) と 4) の処理を社員 A とルートサーバ間で行う

社員 A はルートサーバの公開鍵証明書を所持しているためこれで認証パスの構築は終了し、認証パスの検証へ移る。即ち、収集した公開鍵証明書の正当性を検証し、検証が成功した場合、社員 A は社員 D を認証することができる。

4. PKI との比較検討

PKI と本提案の相違点を表 1 に示し、PKI (CRL)、PKI (OCSP) と本提案の比較を表 2 に示す。

PKI (CRL) は失効情報が一定周期で発行されるため、ユーザが最新の有効性を確認できない場合がある。

PKI (OCSP) は公開鍵証明書の有効性を検証時に問い合わせるため PKI (CRL) よりリアルタイム性に優れている。しかし、PKI (OCSP) は公開鍵証明書のみでなく OCSP からの有効性の回答も検証する必要があるためクライアントの負荷が大きくなる。また両方式とも失効情報の管理が必要である。

提案方式では、公開鍵証明書を発行者自身が保管するうえ、オンデマンドで認証パスを構築するためリアルタイム性に優れ、失効情報の管理を行う必要がない。また検証者は最上位に位置するルートサーバの公開鍵を自ら検証できる。

しかし提案方式では認証を行いたい場合、毎回認証パスの構築を行う必要があるため、初期遅延が大きくなる可能性がある。以上のことから、提案方式は小規模な企業ネットワークにおいては有効な方式であると考えられる。

5. むすび

PKI を導入するためにどのような課題があるかを検討しそれを解決するための方式を提案した。今後は、提案方式を実装し、検証を行っていく予定である。

表 1 PKI と提案方式の相違点

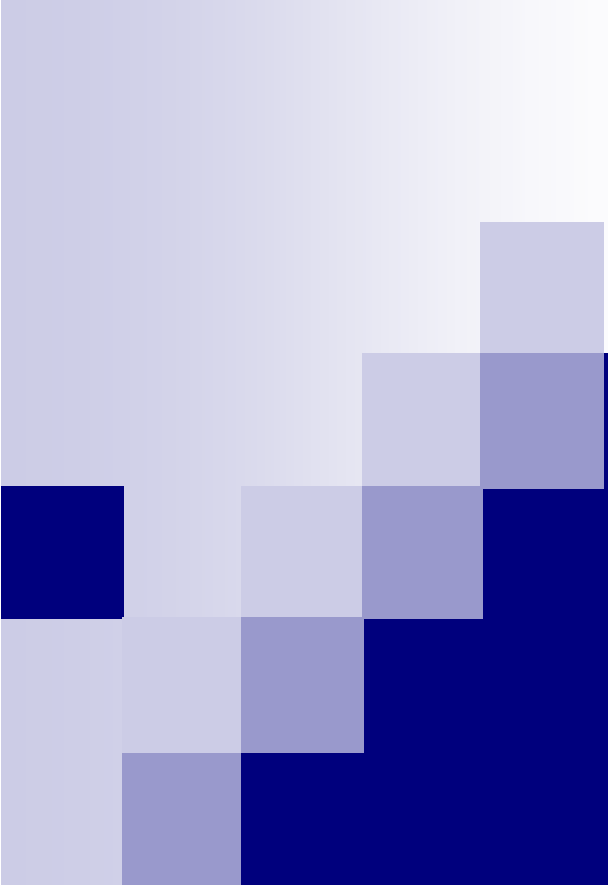
	PKI	提案方式
信頼関係	階層	環状
検証の最上位	root CA	自分
所持する公開鍵証明書	上位層が署名した自分の公開鍵証明書	自分が発行した下位層の公開鍵証明書

表 2 PKI と提案方式の比較

	リアルタイム性	クライアント負荷	管理コスト	初期遅延
PKI (CRL)				
PKI (OCSP)				
提案方式				

参考文献

- 1) 情報処理推進機構 セキュリティセンター
PKI 関連技術解説
<http://www.ipa.go.jp/security/pki/>
- 2) 青木他 PKI と電子社会のセキュリティ
共立出版 2001年10月25日



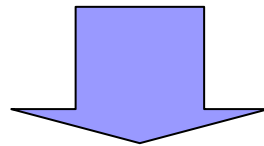
企業ネットワークにおける 認証基盤の構築に関する 研究

名城大学理工学部

坂野文男 保母雅敏 渡邊晃

研究背景

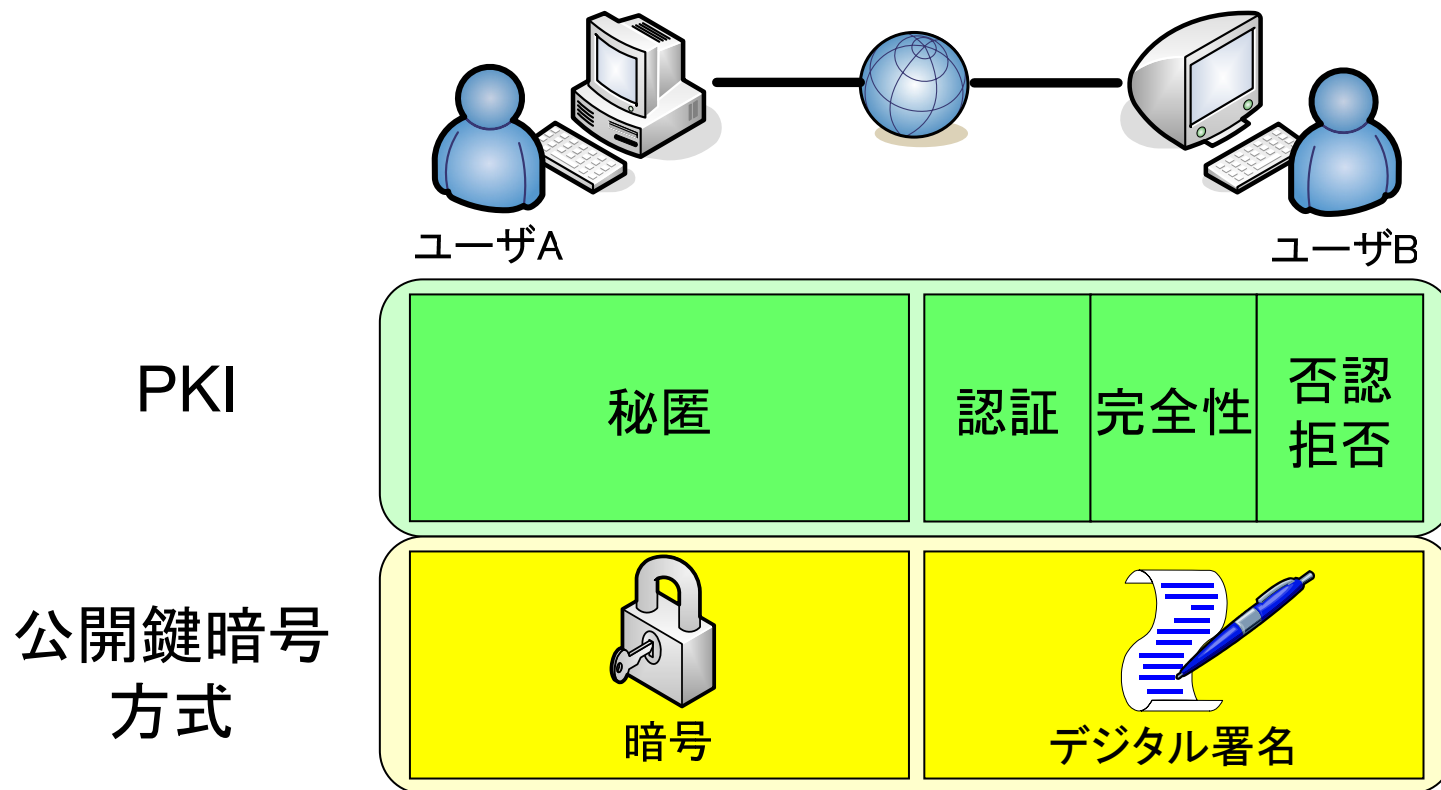
- 近年のインターネット普及に伴い、電子商取引や、電子申請等の電子化が進んでいる
- ネットワーク上には「盗聴」、「なりすまし」、「改ざん」等の脅威がある



PKIの重要性が高まっている

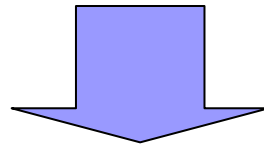
PKI (Public Key Infrastructure)

- 公開鍵暗号方式によるセキュリティの基盤



企業への導入

- 企業ネットワークにおいてもPKIによる認証基盤を導入する傾向がある

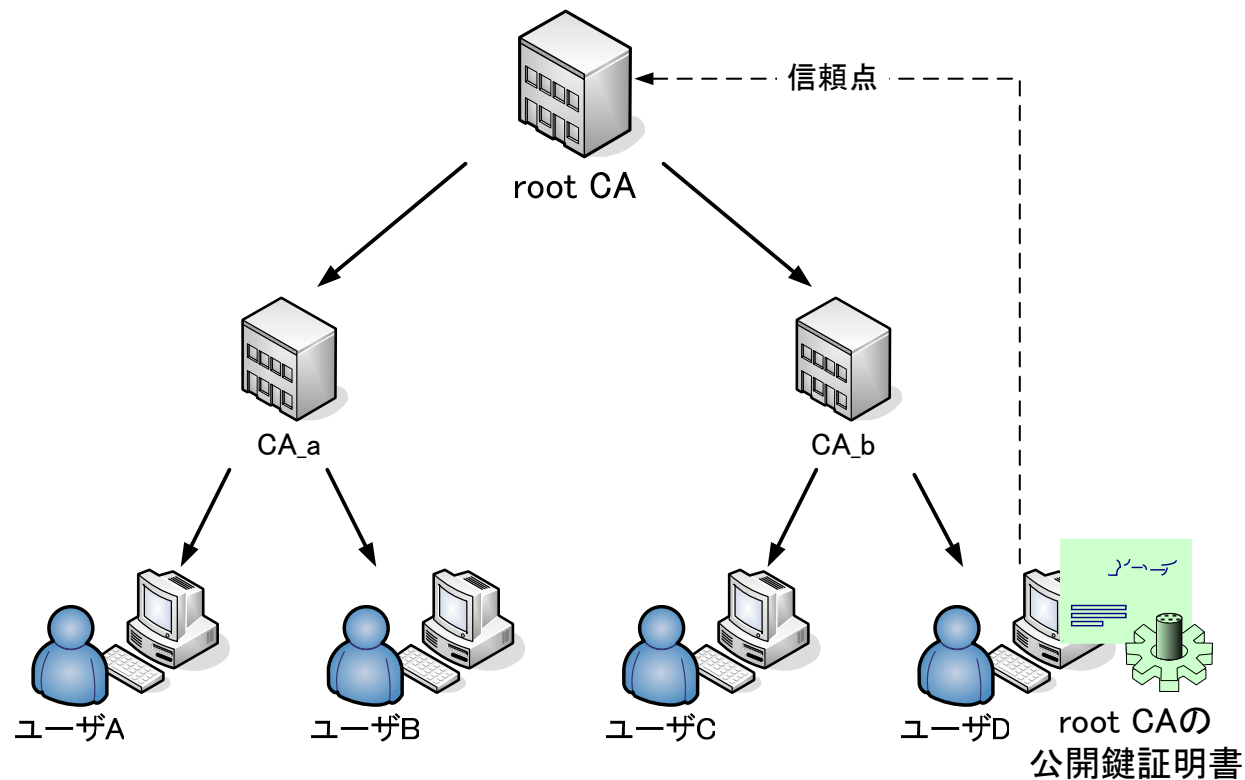


- 企業がPKIを導入するうえでどのような課題があるかを考察し、その課題を解決するための認証基盤の一方式について提案する

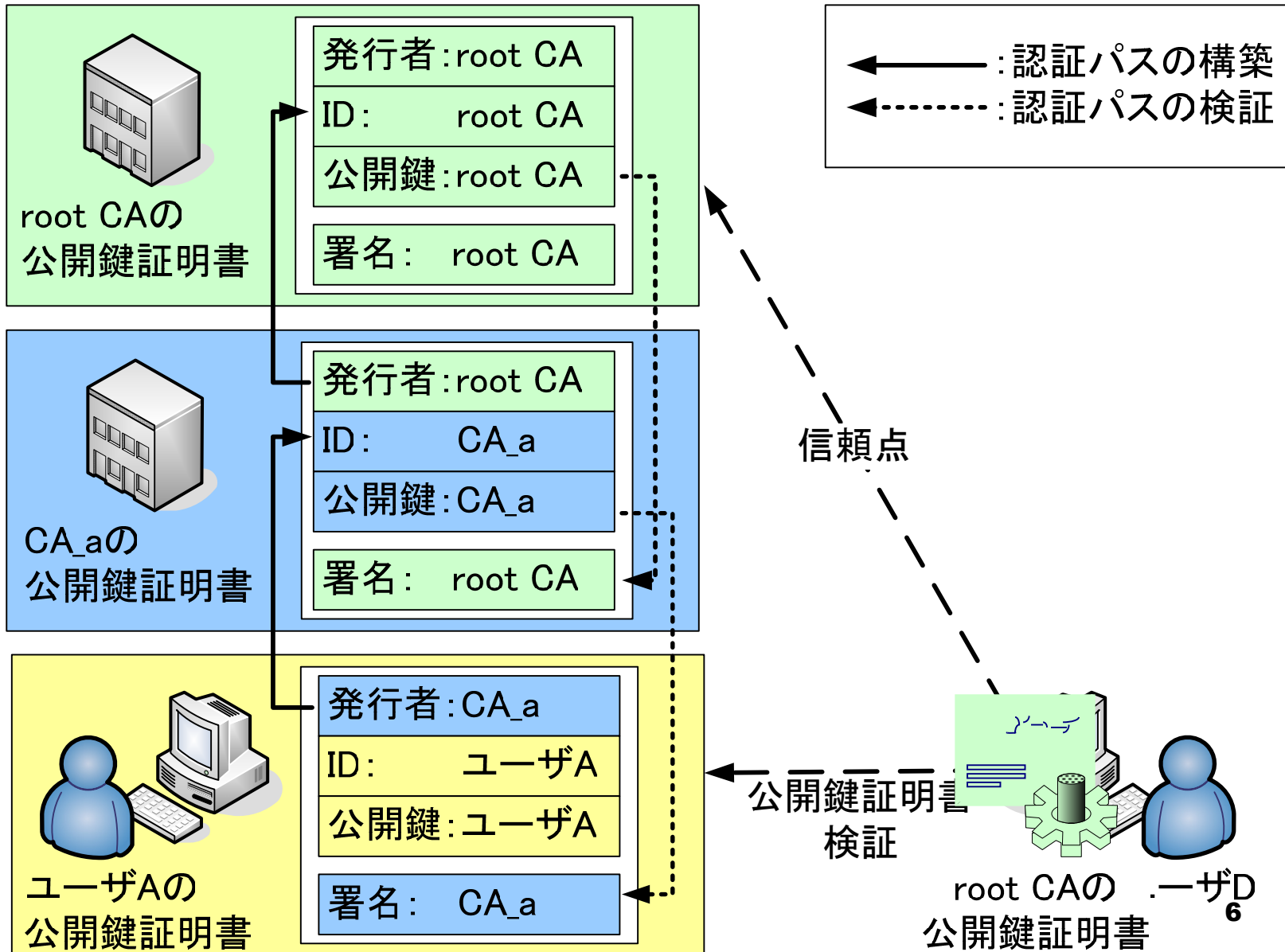
信頼関係の構築

- 認証局CAは公開鍵証明書を他のCAに発行してもらうことにより信頼関係を構築する

(CA: Certificate Authority)

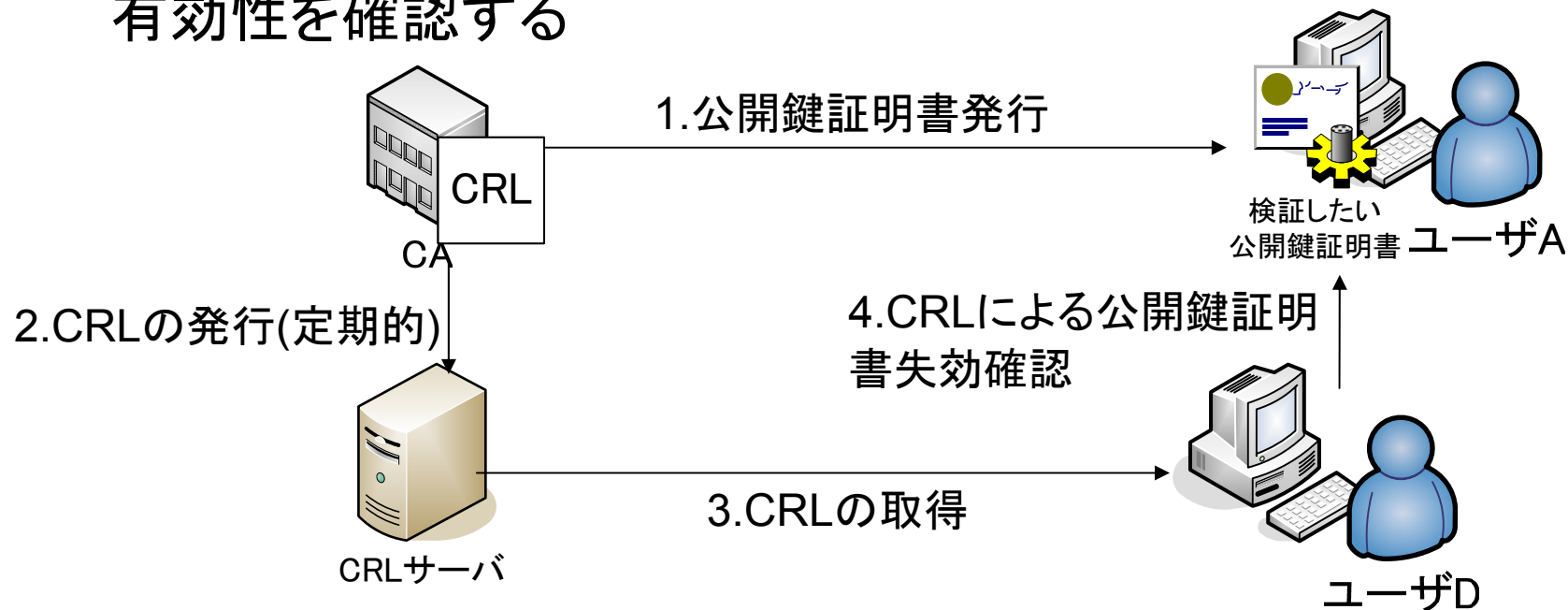


公開鍵証明書を検証



CRL (Certificate Revocation List)

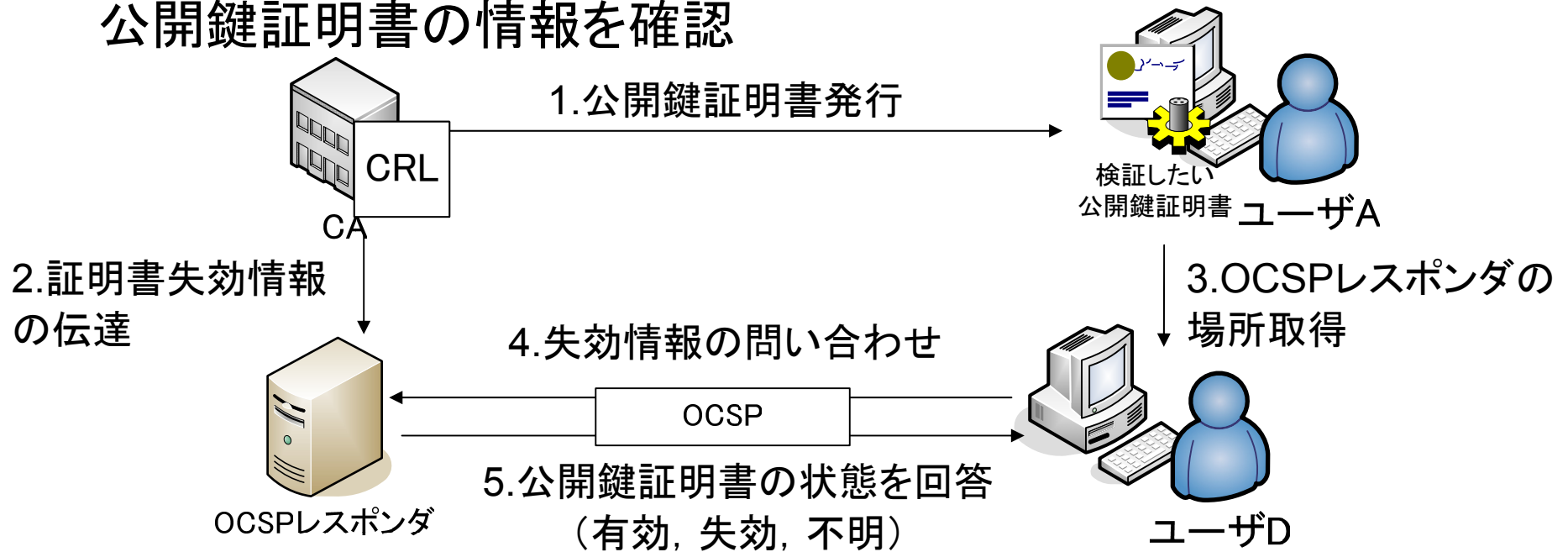
- 公開鍵証明書がCRLに掲載されていないことをもって有効性を確認する



公開鍵証明書の状態について、
必ずしも最新の情報とは限らない

OCSP (Online Certificate Status Protocol)

- 公開鍵証明書の検証時にリアルタイムでOCSPレスポンスへ公開鍵証明書の情報を確認



公開鍵証明書の状態について、
必ずしも最新の情報とは限らない



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
 - 管理が複雑なため、敷居が高い
 - 公開鍵証明書の状態について、必ずしも最新の情報とは限らない

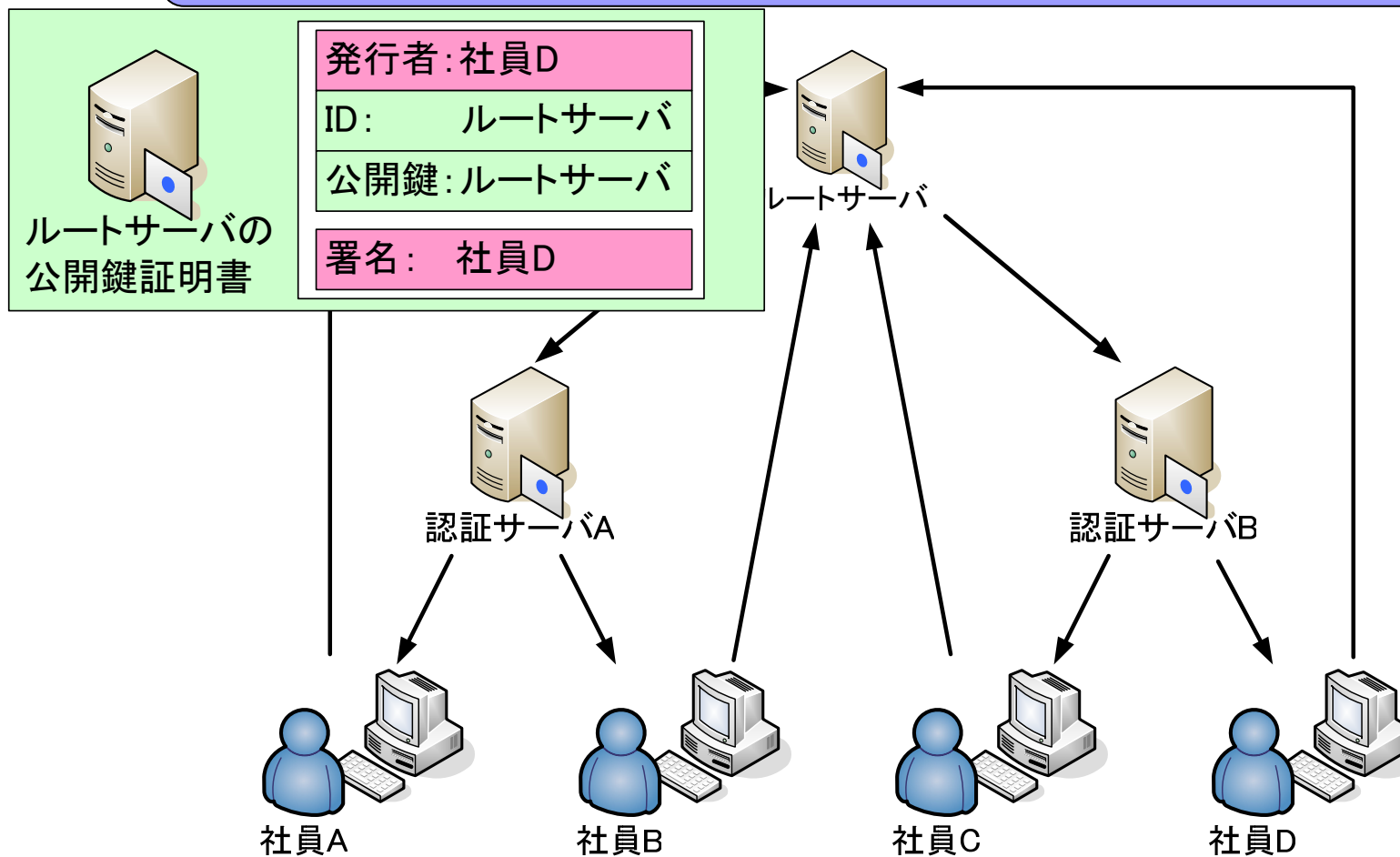


提案方式

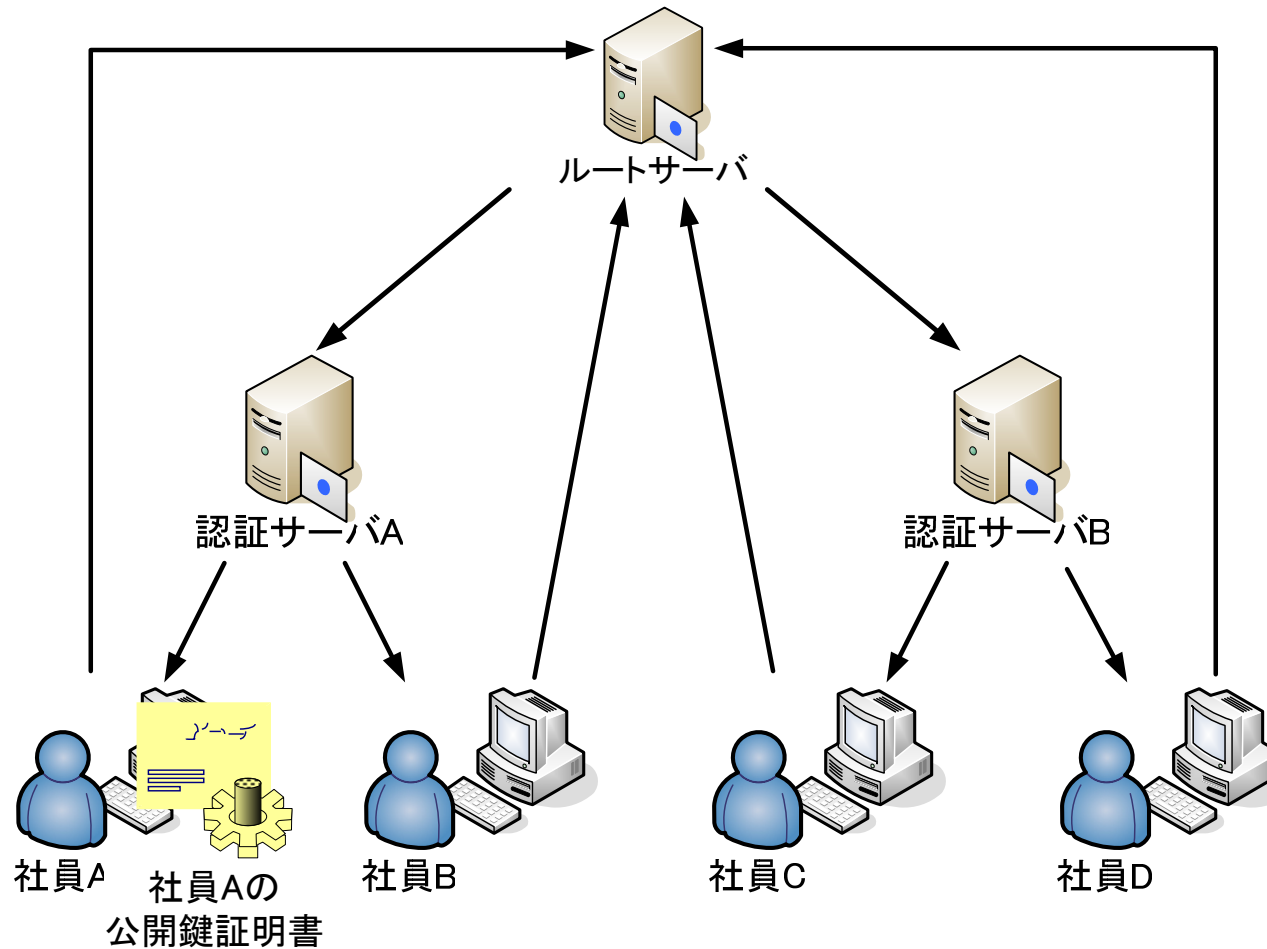
- 企業ネットワークという閉じた世界における
認証基盤を検討する
 - 信頼関係を環状にする
 - 公開鍵証明書は発行者が保持し, 自ら管理する
 - 信頼関係はオンデマンドで検証する

信頼関係を環状化

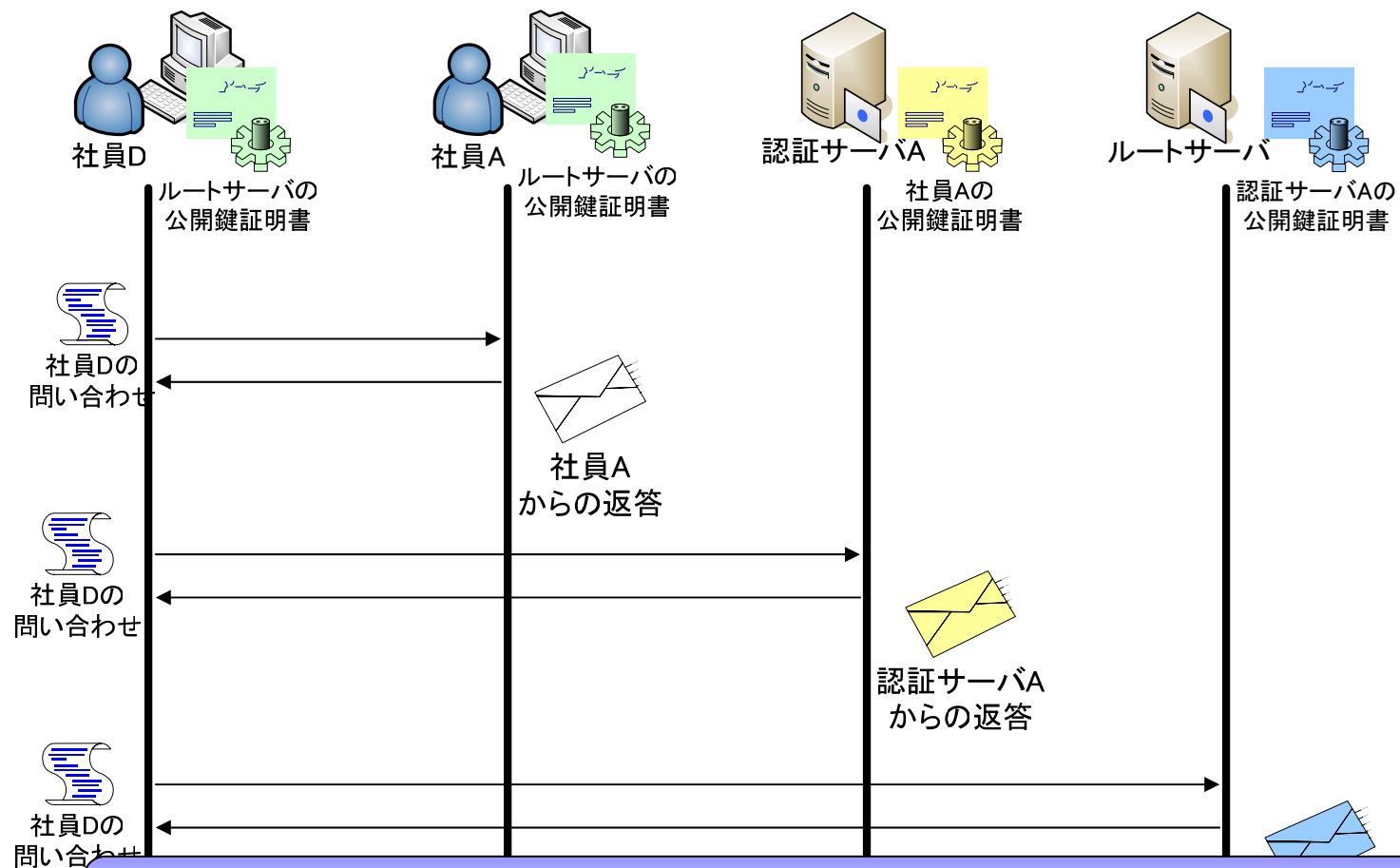
ルートサーバの公開鍵証明書が検証可能



公開鍵証明書は発行者が保持し、 自ら管理



公開鍵証明書のオンデマンド検証



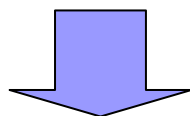
リアルタイム性に優れている

失効情報の管理を行う必要がない

評価

	リアルタイム性	管理コスト	最上位の公開鍵証明書	初期遅延	大規模ネットワーク
PKI (CRL)	△	△	検証不可能	○	○
PKI (OCSP)	○	△	検証不可能	△	○
提案方式	◎	○	検証可能	△	△

- 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
- 検証者は最上位に位置するルートサーバの公開鍵証明書を自ら検証できる
- 認証を行いたい場合、毎回オンデマンドの検証を行う必要があるため、初期遅延が大きくなる可能性がある
- 大規模ネットワークは信頼の環状化が難しい



企業ネットワークで有効な手段だと考えられる



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ことを提案した
 - 信頼関係を環状にする
 - 公開鍵証明書はその発行者が保持し、自ら管理する
 - 信頼関係はオンデマンドで検証する

- 今後は、提案方式を実装し、検証を行っていく予定である



おわり