# 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

01j080　坂野 文男
渡邊研究室

## 1. はじめに

公開鍵を用いた認証基盤である PKI（Public Key Infrastructure）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ている．企業内ネットワークにおいてもその利点に着目し，PKI による認証基盤を導入する傾向がある．そこで，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，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くみとなっている．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失効リストをサーバに保管する CRL（Certificate Revocation List）方式がよく使われる．しかし，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，次回の CRL が発行されるまでは失効情報が利用者に伝わらない．

## 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．

- 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

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．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し，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．最後に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することができ，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．

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．

## 4. 評価

本提案方式は，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．

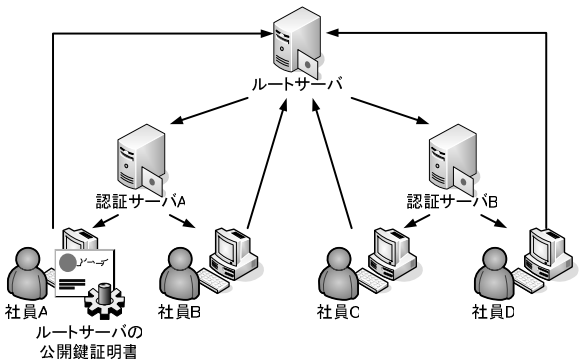



図 1　提案方式の信頼関係

### 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 隆一 (著), 稲田 龍 (著), 村井 純：PKI と電子社会のセキュリティ，p.233，共立出版(2001)

# 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

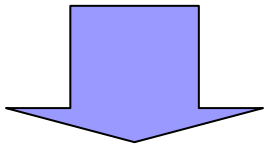
渡邊研究室

01j080　坂野文男

# 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

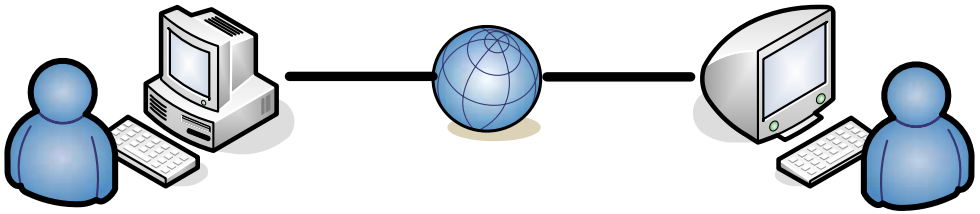
- ネットワーク上には「盗聴」、「なりすまし」、「改ざん」等の脅威がある

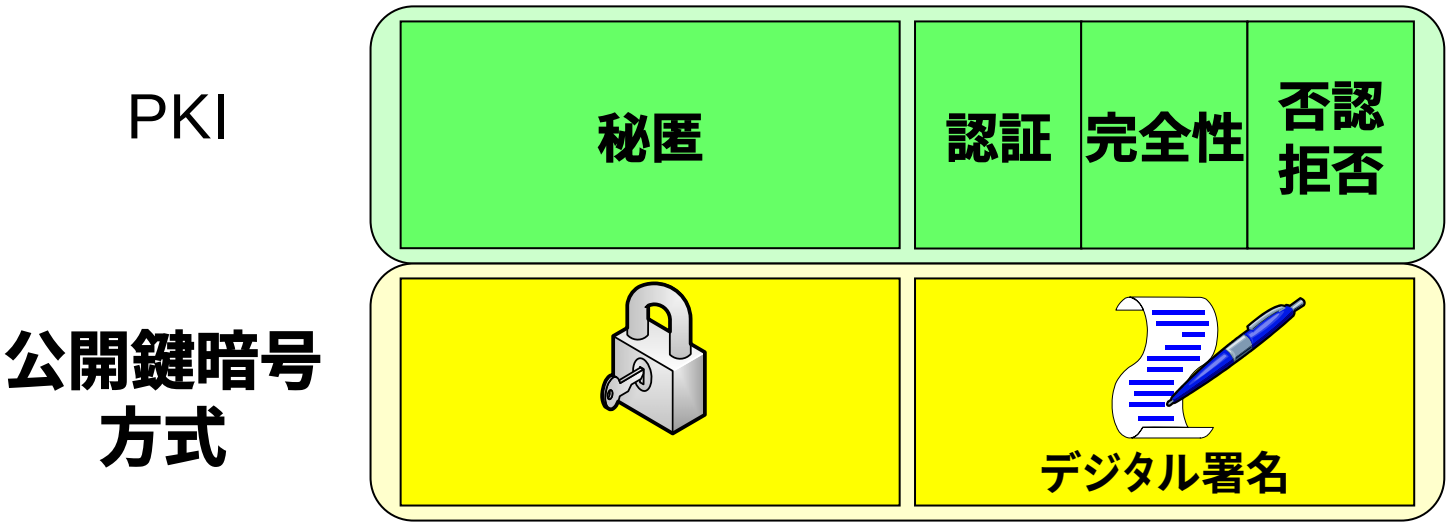


PKIの重要性が高まっている

# PKI（Public Key Infrastructure）

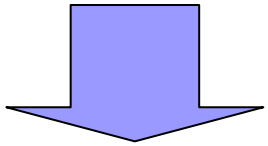
- **公開鍵暗号方式によるセキュリティの基盤**





# 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



- 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

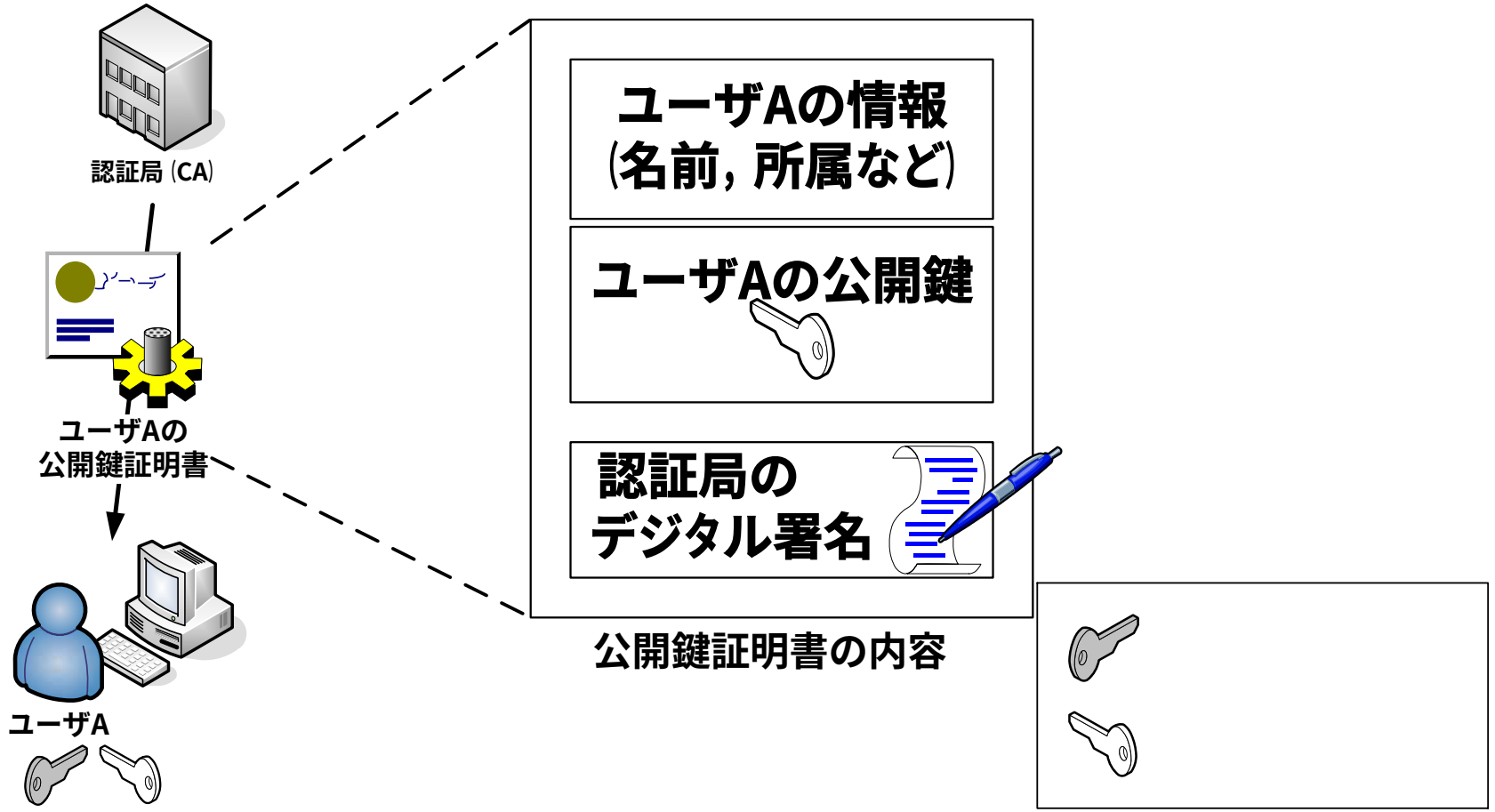
# 公開鍵暗号方式

- 対になる二つの鍵を使いデータの暗号化と復号を行う暗号方式
- 片方の鍵は本人だけがわかるように厳重に管理するため秘密鍵と呼ばれる
- もう片方は他人に公開するため公開鍵と呼ばれる
- 秘匿の場合、通信相手の公開鍵で暗号化
- 署名の場合、自分の秘密鍵で暗号化（デジタル署名）

**公開鍵暗号方式では公開鍵を偽造することが可能**

# 公開鍵証明書

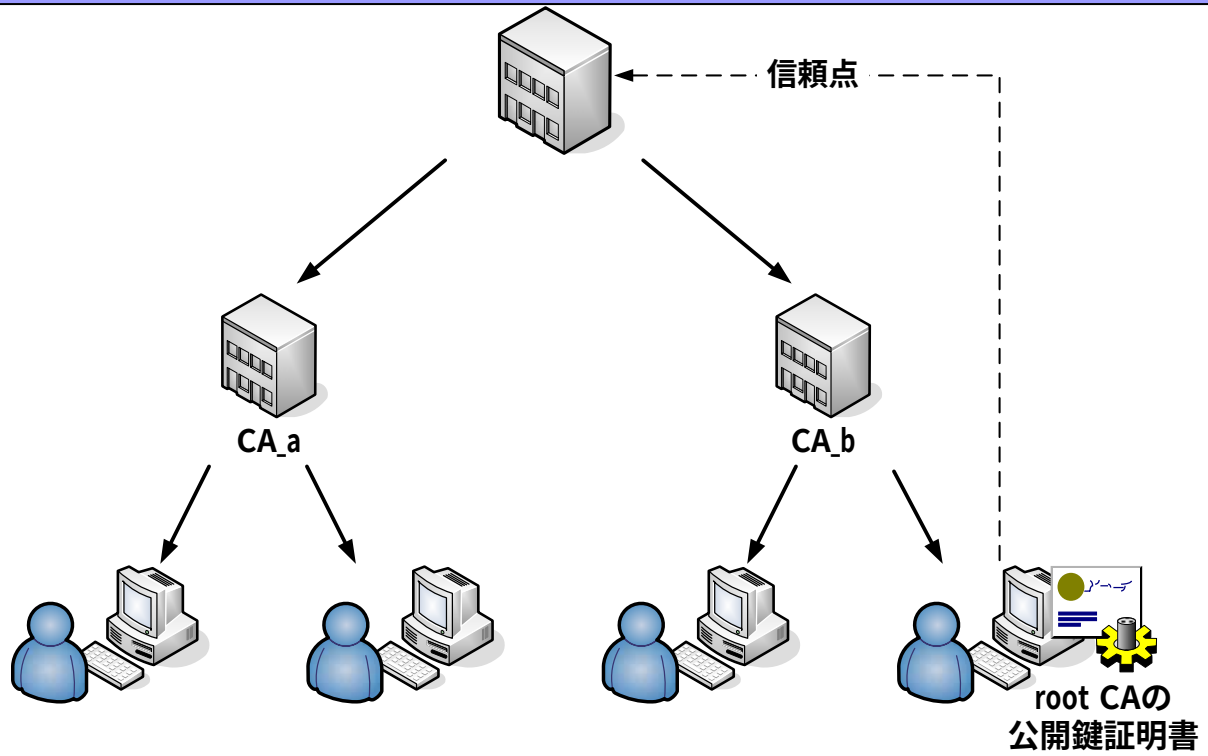
- **認証局**(CA：Certificate Authority)**という信頼できる第三者機関**(TTP： Trusted Third Party)**が公開鍵の所有者を保証したもの**



# 信頼関係の構築

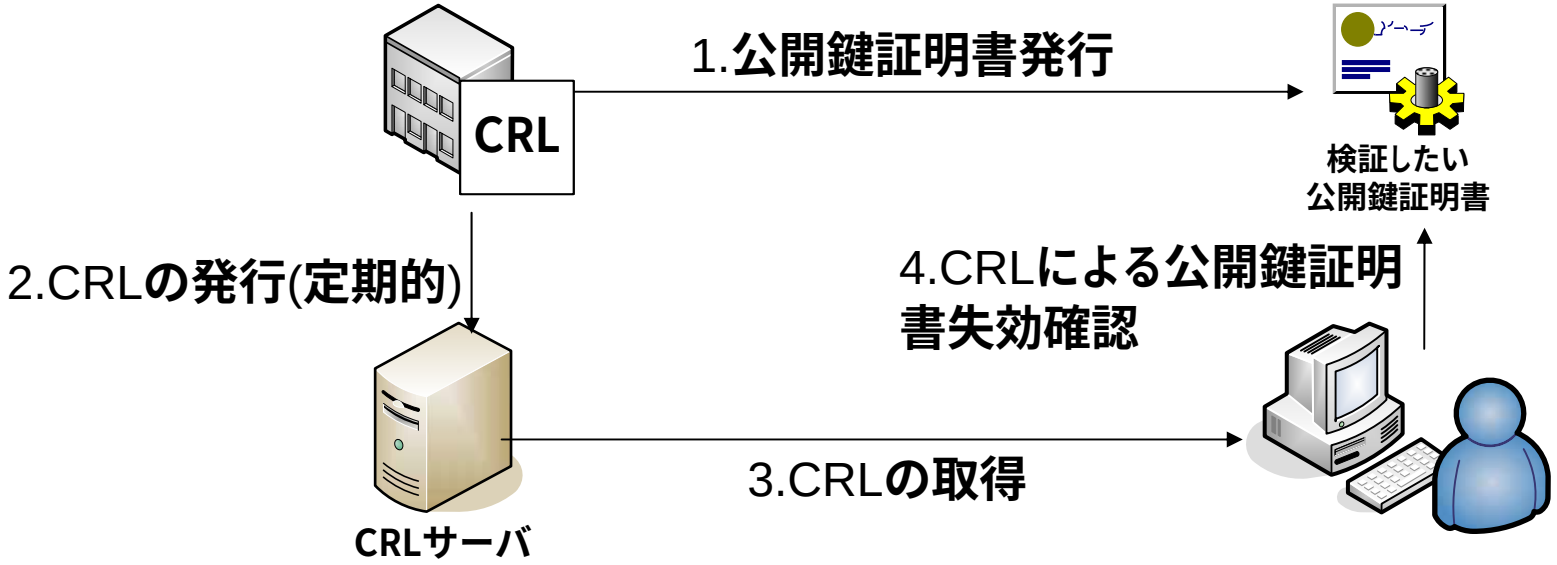
- CAは公開鍵証明書を他のCAに発行してもらうことにより信頼関係を構築することができる

**root CAの公開鍵証明書が正当であることを検証する方法がない**



# 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**




**失効情報を管理する必要がある**

**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**

# 課題

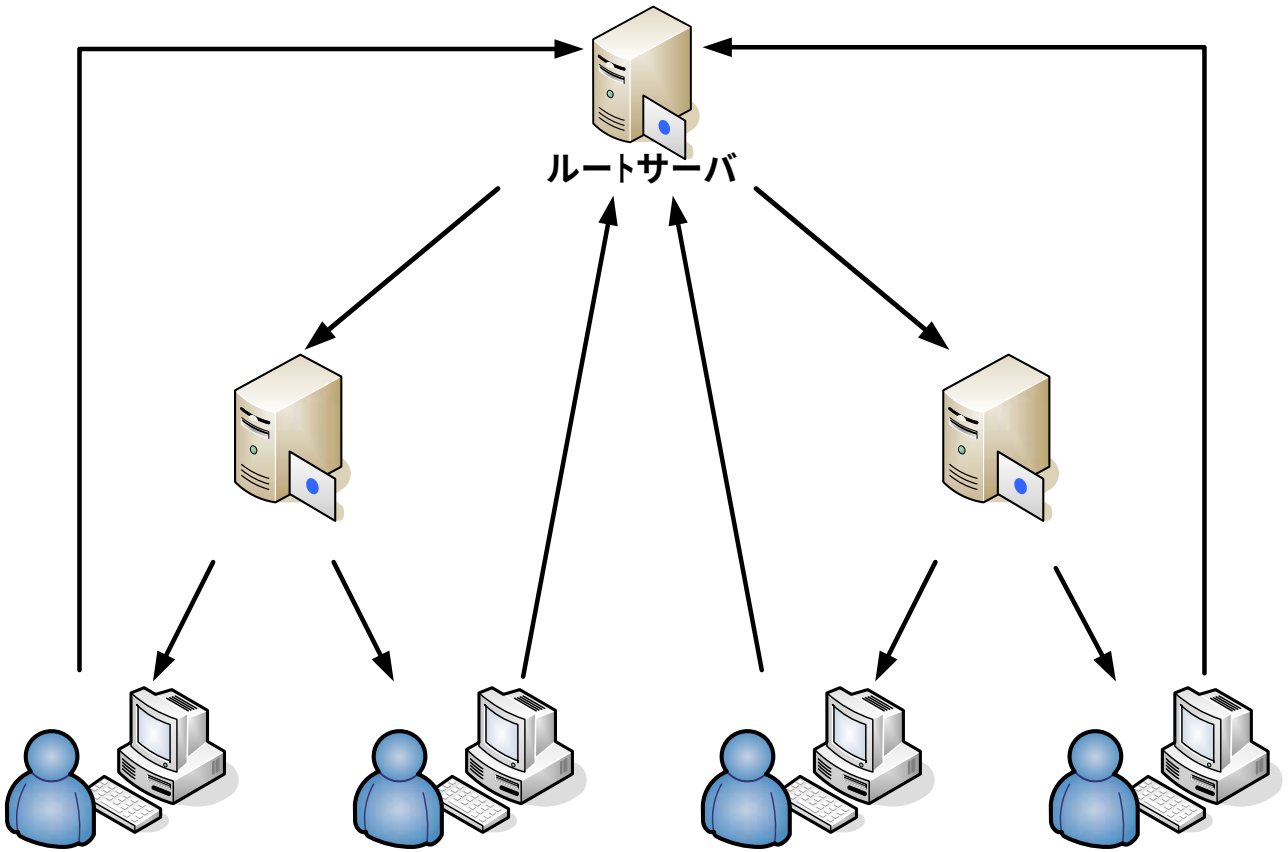
- 企業ネットワークでは以下のことが課題になると考えられる
  - 最上位のCAの公開鍵証明書が正当であることを検証する方法がない
  - 失効情報を管理する必要ある
  - 公開鍵証明書の状態について、必ずしも最新の情報とは限らない

# 提案方式

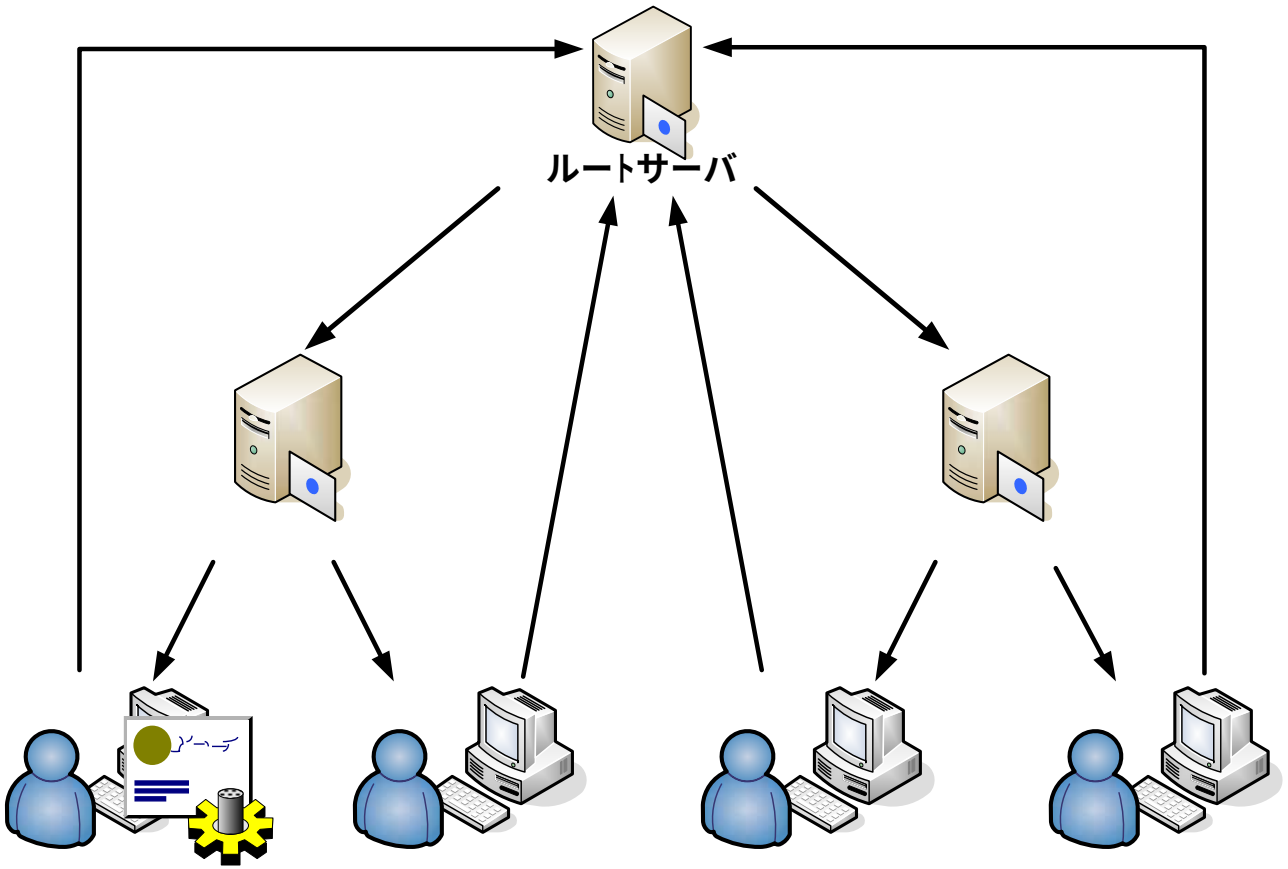
- 企業ネットワークという閉じた世界における認証基盤を検討する
  - 信頼関係を環状にする
  - 公開鍵証明書は発行者が保持し，自ら管理する
  - 信頼関係はオンデマンドで検証する

# 信頼関係を環状化

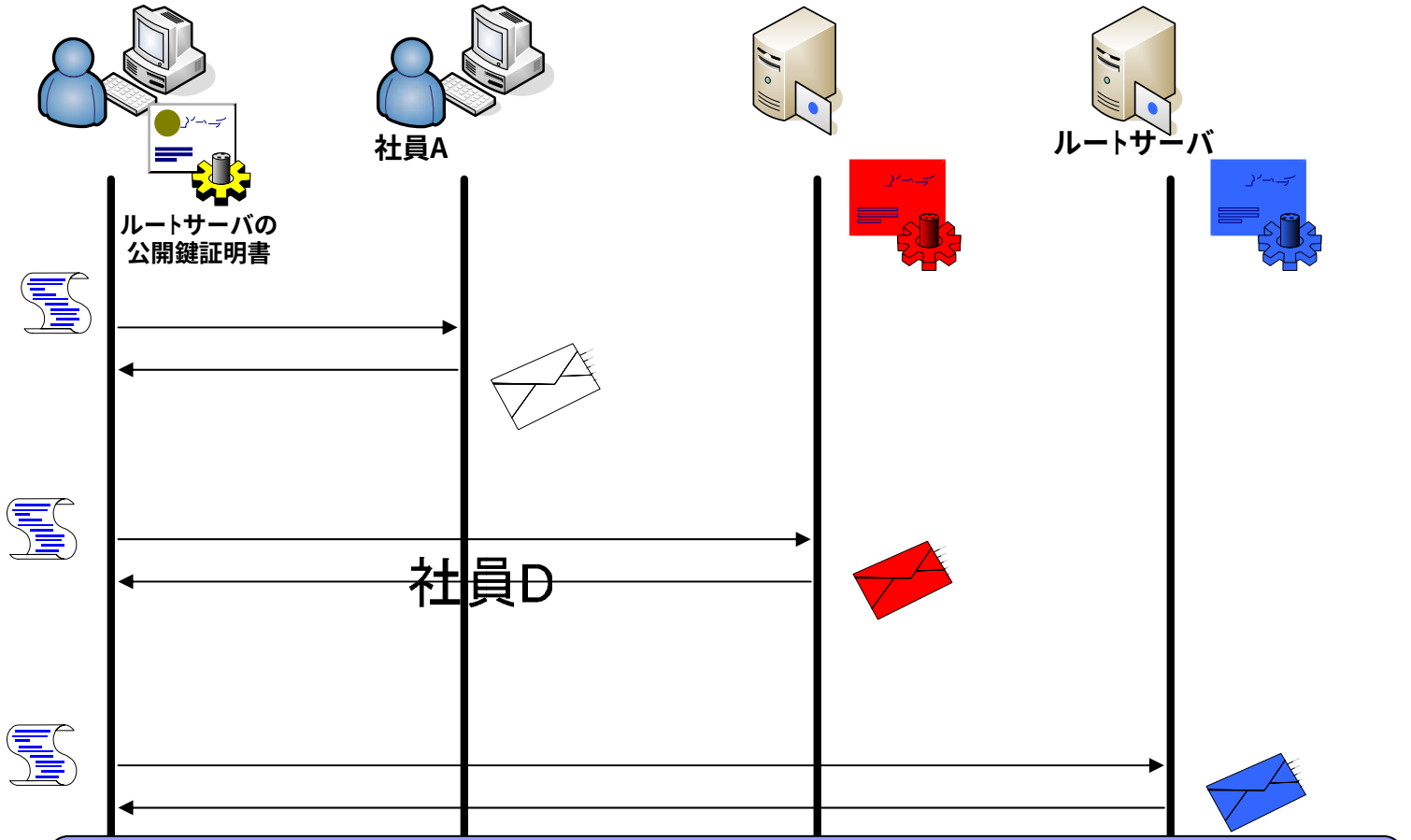
**ルートサーバの公開鍵証明書が検証可能**



# 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

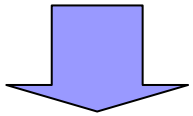
失効情報の管理を行う必要がない

社員A

# 評価

| | リアル<br>タイム性 | 管理コスト | 最上位の<br>公開鍵証明書 | 初期遅延 | 大規模<br>ネットワーク |
|---|---|---|---|---|---|
| PKI(CRL) | △ | △ | 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
- 今後は現在取り上げた課題が実際に問題になるのかPKIを運用し検証を行う予定である

# おわり