企業ネットワークにおける認証基盤構築の一方式

坂野　文男　　保母　雅敏　　渡邊　晃
名城大学大学院理工学研究科

A Construction method of authentication infrastructure in an enterprise network

Fumio Banno　　Masatoshi Hobo　　Akira Watanabe
Graduate School of Science and Technology, Meijo University

1.　はじめに

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急激に進んでいる.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，否認といったネットワーク固有の脅威が存在する．そこで公開鍵暗号方式によるセキュリティの基盤である PKI（Public Key Infrastructure）が注目されている．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．企業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．

PKI では，各ユーザの公開鍵を認証局（CA : Certification Authority）が署名し，CA の公開鍵は更に上位の CA が署名する．しかし，最上位の CA（root CA）の公開鍵証明書を発行する機関がなく，通常は root CA 自身が自己署名する．そのため，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を被発行者に手渡してしまうため，証明書の有効性を確認するために証明書の失効を確認する必要がある．失効情報法の確認方法には CRL（Certificate Revocation List）[1]モデルと OCSP（Online Certificate Status Protocol）[2]モデルがあるが両者ともその情報が必ずしも最新とは限らないという課題が指摘されている．

そこで本稿では，PKI を参考に企業内ネットワークという閉じた世界において管理負荷の少ない新しい認証基盤の一方式を検討した．本稿の特徴は，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い，信頼関係をオンデマンドで検証を行う．これにより，管理が容易でリアルタイム性の高い認証基盤を提供できる．

2.　PKI

2.1　PKI の信頼関係と企業の業務形態

CA は公開鍵証明書を発行することにより信頼関係を構築することができる．信頼関係の構築とはいくつかの CA が連携することである．信頼関係の構築にはいろいろなモデルがあるが，例として図 1 に複数の CA を階層型（ツリー構造）に構成する階層型モデルを示す．ユーザの公開鍵証明書は CA 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．ユーザは root CA を信頼点とし，root CA の公開鍵証明書をあらかじめ所持しておく．信頼点とは公開鍵証明書の有効性検証時に信頼の基点となる機関のことである．

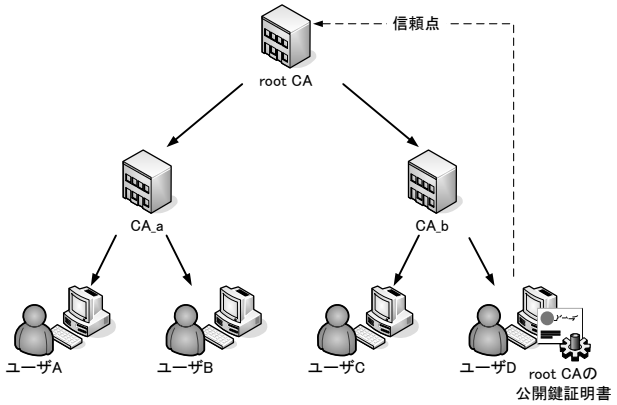


図 1　階層型モデルによる信頼関係の構築

階層型モデルは企業の業務形態と対応付けができる．例えば root CA を社長，root CA に公開鍵証明書を発行してもらった CA を各部署の部長，ユーザを部長の下で働く社員というように対応させることができる．また通常社長は各部署について把握していて，各部署の部長も下で働く社員について把握しているはずである．そこで企業に認証基盤を導入する際，信頼関係の構築を階層型モデルで行えば社員の人事異動等による公開鍵証明書の変更にも対応しやすいと考えられる．

2.2　公開鍵証明書の有効性検証

PKI の場合，公開鍵証明書の有効性検証は認証パスの構築と認証パスの検証の手順で行う．認証パスの構築では認証するユーザの公開鍵証明書から検証者の信頼点となる root CA までの公開鍵証明書を収集し，対象となる公開鍵証明書が信頼点と関連づけられていることを確認する．認証パスの検証では収集したすべての公開鍵証明書で，公開鍵証明書の署名が正しいか，公開鍵証明書の有効期間が切れていないか，公開鍵証明書が失効していないかなどを検証する．認証パスの構築と認証パスの検証が問題なく終了することにより公開鍵証明書の有効性検証が終了する．

例として図 1 でユーザ D がユーザ A の公開鍵証明書の有効性検証を行う場合の処理を図 2 に示す．まず検証するユーザ A の公開鍵証明書を収集する.ユーザ A の公開鍵証明書をチェックすることにより発行者は CA_a とわかり，CA_a の公開鍵証明書を収集する．次に CA_a の公開鍵証明書より発行者は root CA とわかるが，root CA はユーザ D の信頼点のためここで認証パスの構築を終了し,認証パスの検証へ移る．

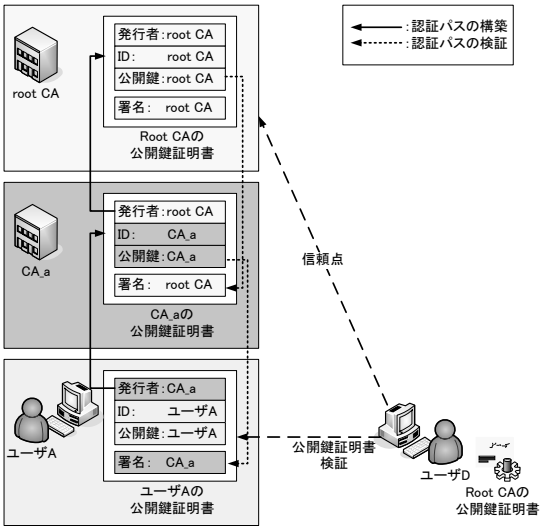


図 2　公開鍵証明書の有効性検証方法

認証パスの検証は認証パスの構築時に公開鍵証明書を手に入れた順序とは逆に行う．すなわち root CA，CA_a，ユーザ A の順番に公開鍵証明書の検証を行い，すべての公開鍵証明書で有効性検証が成功した場合，ユーザ A の公開鍵証明書が信頼できるものと判断する．

2.3　公開鍵証明書の失効情報

認証パスの検証には失効情報を管理する必要がある．失効情報の管理方法には CRL モデルと OCSP モデルがある．

CRL モデルの概要を図 3 に示す．まず公開鍵証明書を発行した CA が CRL（証明書失効リスト）を定期的な周期で発行する．各ユーザは公開鍵証明書の検証をする前にあらかじめ CA から CRL を収集しておく必要がある．各ユーザは公開鍵証明書の検証時に事前に収集した CRL に検証対象の公開鍵証明書が記載されていないことを確認することにより公開鍵証明書の有効性を確認する．

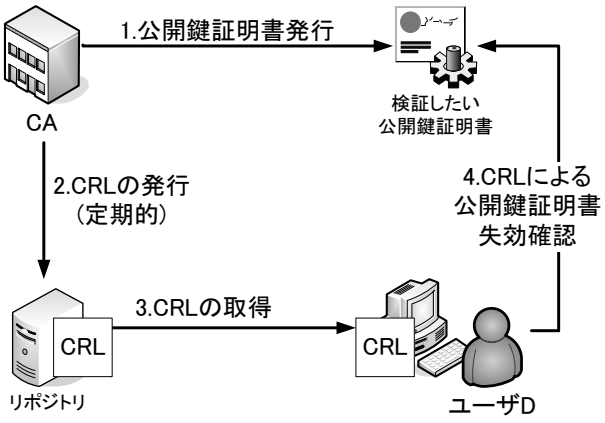


図 3　CRL モデルの概要

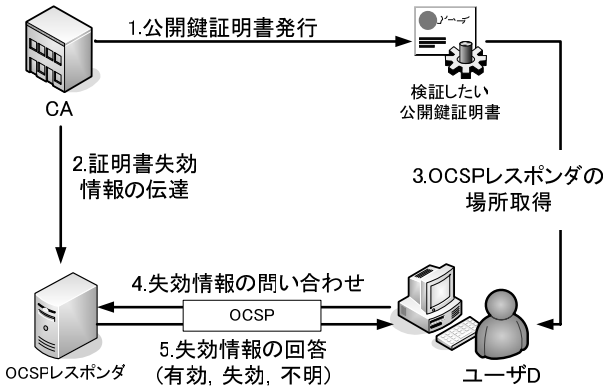


図 4　OCSP モデルの概要

OCSP モデルの概要を図 4 に示す．OCSP モデルは公開鍵証明書の検証時にリアルタイムで OCSP レスポンダへ有効性を確認するプロトコルである．各ユーザは検証対象の公開鍵証明書に記載されている OCSP レスポンダへ失効情報の問い合わせを行い，その回答により公開鍵証明書の状態を確認する．

2.4　PKI の課題

PKI では，最上位の root CA の公開鍵証明書を発行する機関がなく，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．

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公開鍵証明書の失効情報を管理する必要がある．これは公開鍵証明書が発行者の手を離れ被発行者が所持していることに起因する．もし失効された公開鍵証明書が多くなると失効情報のデータが大きくなり，公開鍵証明書の有効性の確認時に失効情報をサーチする時間がかかる．失効情報の確認に CRL モデルを利用する場合，各ユーザが公開鍵証明書の検証をする前に CA から CRL をあらかじめ収集しておく必要がある．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．OCSP モデルを利用する場合においても，OCSP レスポンダ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.　企業ネットワークにおける認証基盤

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対象とする．上記のような PKI の課題を解決するために，以下のような方式を検討している．すなわち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い，信頼関係をオンデマンドで検証を行う．これにより，PKI よりも管理が容易でリアルタイム性の高い認証基盤を提供することが可能である．PKI（CRL）と本方式の相違点を表 1 に示す．

表 1　PKI と本方式の相違点

	PKI（CRL）	本方式
信頼関係	階層（検証の最上位は root　CA）	環状（検証の最上位は自分）
公開鍵証明書の管理方法	上位層が署名した自分の公開鍵証明書を管理	自分が発行した下位層の公開鍵証明書を管理
検証時の収集方法	CRL 等を事前に入手	オンデマンドで収集

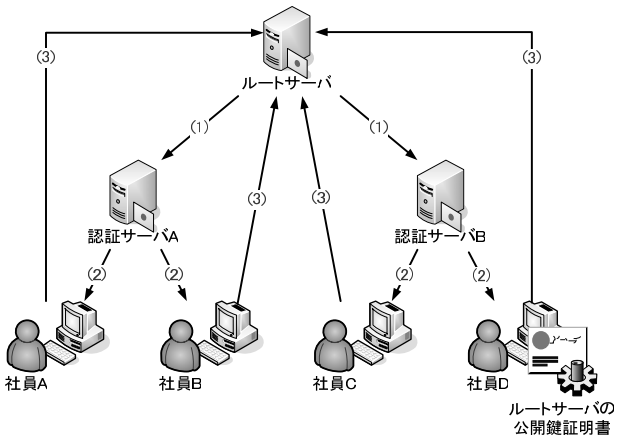


図 5　本方式の信頼関係

本方式の信頼関係を図 5 に示す．矢印は公開鍵証明書の発行の方向である．ルートサーバは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．認証サーバは各部門の社員に公開鍵証明書を発行する．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させることにより，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．環状の信頼関係を一度築けば全ての公開鍵証明書は偽造不可能になり，安全性が保証される．

次に本方式の公開鍵証明書の管理方法を図 6 に示す．図 6 は図 5 で社員 D が社員 A を認証する場合の公開鍵証明書の管理方法である．図 2 と図 6 は同じような図であるが,図 2 は PKI の公開鍵証明書の有効性検証方法の説明であり，図 6 は本方式の公開鍵証明書の管理方法について述べたものである．社員 D はルートサーバの公開鍵証明書を管理している．ルートサーバは認証サーバ A の公開鍵証明書を管理していて，認証サーバ A は社員 A の公開鍵証明書を管理している．社員 A の公開鍵証明書は認証サーバ A より取得できるため社員 A がオフライン状態でも社員 A の公開鍵証明書を得て社員 A の認証を行うことができる．このように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．この管理方法により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済む．

次に検証時の収集方法を図 7 に示す．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．また公開鍵証明書は発行者が管理し，失効時は対象の公開鍵証明書を削除するので失効情報の管理が不要になる．具体的なオンデマンドでの検証は以下のようになる．

(1)　社員 D は管理している公開鍵証明書の ID より被発行者のルートサーバへ社員 A の公開鍵証明書を問い合わせる
(2)　ルートサーバは問い合わせより社員 A が所属している認証サーバ A の公開鍵証明書を返答する
(3)　社員 D は認証サーバ A の公開鍵証明書の ID より認証サーバ A へ社員 A の公開鍵証明書を要求する
(4)　認証サーバ A は問い合わせより社員 A の公開鍵証明書返答する

上記により認証パスの構築は終了し，認証パスの検証へ移る．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 の公開鍵証明書は信頼することができ，社員 A の公開鍵証明書を利用し，

(5)　社員 D は共通鍵を作成して社員 A の公開鍵証明書で共通鍵を暗号化し，社員 A へ作成した暗号文を送る
(6)　社員 A は社員 A 本人の秘密鍵を利用し，暗号化された共通鍵を復号し，共通鍵を利用して社員 D へ共通鍵を取得したことを返答する

これにより社員 D は社員 A を認証することができ,以後の通信用の共通鍵を共有することができる．

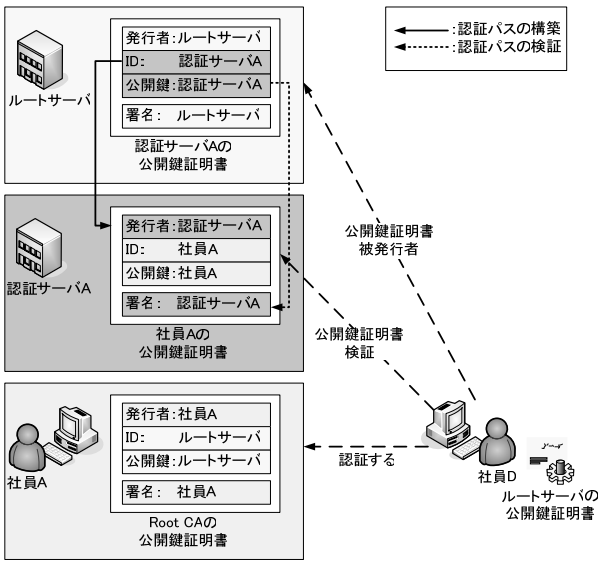


図 6　本方式の公開鍵証明書の管理方法

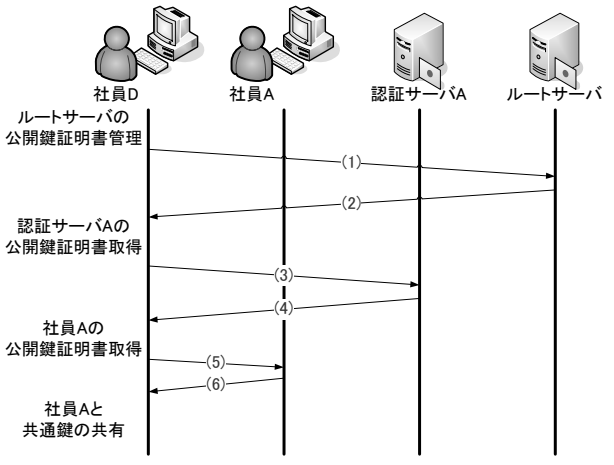


図 7　オンデマンド検証の流れ

4. 評価

PKI（CRL），PKI（OCSP）と本方式の比較を表 2 に示す．

リアルタイム性について，PKI（CRL）は失効情報が一定周期で発行され，公開鍵証明書検証者は前もって CRL を手に入れる必要があるため，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が，失効情報に CRL を利用している場合，ユーザが最新の有効性を確認できない場合がある．本方式では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，ユーザが最新の有効性を確認できる．

管理コストについて，PKI（CRL）と PKI（OCSP）は失効情報を確実に管理する必要があり管理コストが高い．本方式は公開鍵証明書を発行者が管理し，失効時は対象の公開鍵証明書を削除する．そしてオンデマンドで公開鍵証明書の有効性検証することにより失効情報の管理を行う必要がない．

最上位の公開鍵証明書の検証について，PKI（CRL）と PKI（OCSP）は自己署名のため検証が不可能であり偽造される可能性がある．本方式は検証者がルートサーバの公開鍵証明書を自ら検証できるため偽造が不可能になる．

公開鍵証明書の検証方法について，PKI（CRL）は検証者がオフラインでも公開鍵証明書の検証は可能である．PKI（OCSP）と本方式は検証者がオンラインでないと公開鍵証明書を検証することができない．

大規模ネットワークへの導入について，本方式はルートサーバを各社員が署名を行うという性質上，ルートサーバへの問い合わせが多くなり負荷がかかるため大規模ネットワークでは不向きだと考えられる．

以上のことから，本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．

表 2　PKI と本方式の比較

	PKI (CRL)	PKI (OCSP)	本方式
リアルタイム性	△	○	◎
管理コスト	△	△	○
最上位の公開鍵証明書	検証不可能	検証不可能	検証可能
公開鍵証明書の検証方法	オフライン	オンライン	オンライン
大規模ネットワーク	○	○	△

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い，信頼関係をオンデマンドで検証を行うことを検討した．また評価結果より本方式が企業ネットワークには有効な方式であると考えられる．しかし本方式のままでは公開鍵証明書が失効した日時がわからないため，公開鍵証明書の失効後は失効した公開鍵証明書に対応する秘密鍵で行われた署名は全て信用することができなくなるという課題がある．今後は，課題を解決する方法を検討するとともに，本方式を実装し，検証を行っていく予定である．

参考文献

1) R. Housley, W. Polk, W. Ford, D. Solo, “Internet X.509 Public Key Infrastructure Certificate and CRL Profile” , RFC 3280, April 2002.
2) M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams “X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP” , RFC 2560, June 1999.
3) C. Adams, S. Farrell, “Internet X.509 Public Key Infrastructure Certificate Management Protocols” , RFC 2510, March 1999.
4) M. Myers, C. Adams, D. Solo, D. Kemp, “Internet X.509 Certificate Request Message Format” , RFC 2511, March 1999.
5) J. Ross, D. Pinkas, N. Pope, “Electronic Signature Policies” , RFC 3125, September 2001.
6) W. Polk, R. Housley, L. Bassham, “Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” , RFC 3279, April 2002.
7) S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. Wu, “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” , RFC 3647, November 2003.
8) 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/
9) 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構築の一方式

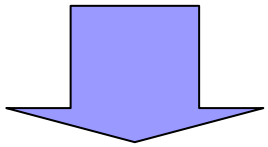
名城大学大学院理工学研究科

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

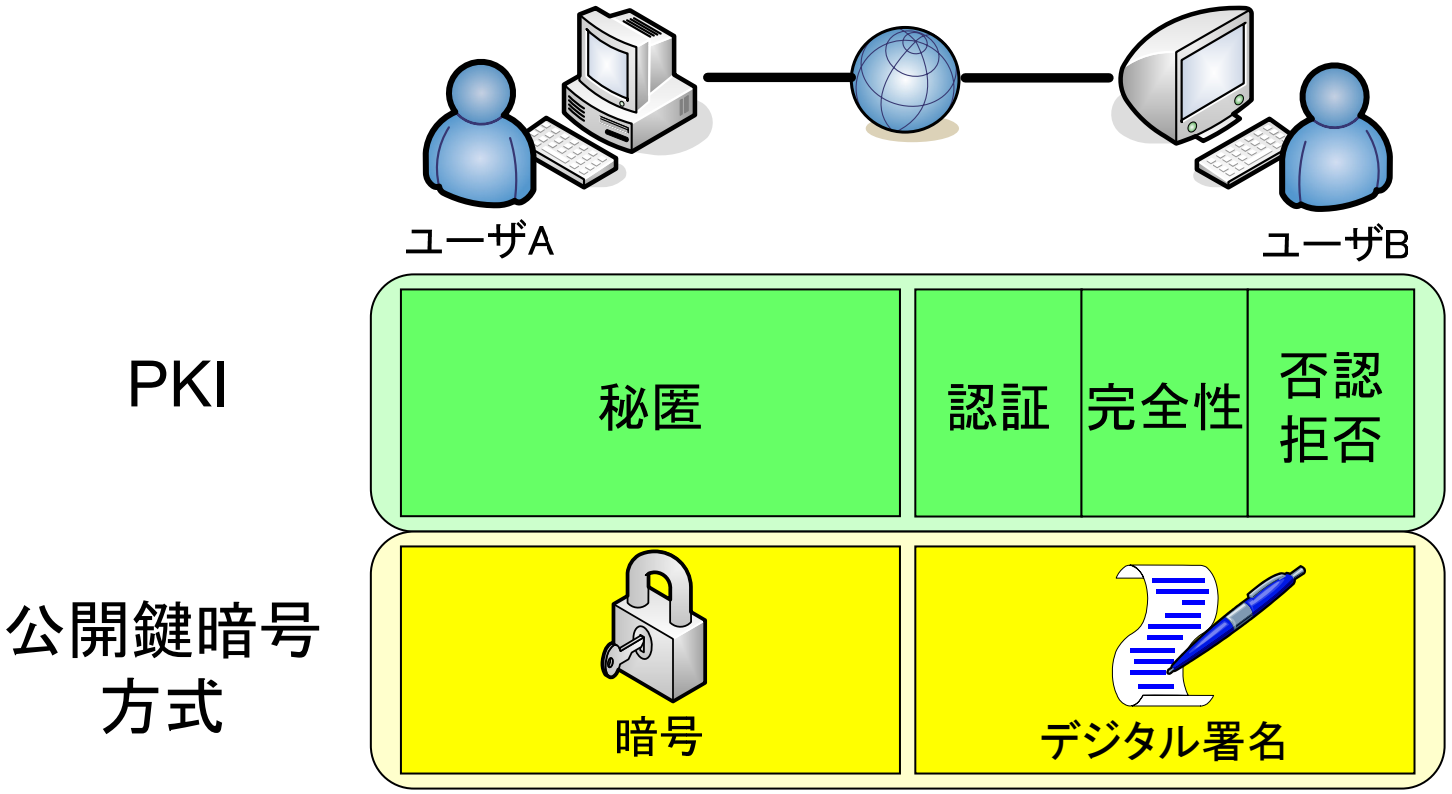
- ネットワーク上には「盗聴」、「なりすまし」、「改ざん」等の脅威がある



PKIの重要性が高まっている

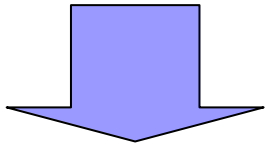
PKI（Public Key Infrastructure）

- 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
- 自己署名の公開鍵証明書は偽造可能
- 失効情報の管理が面倒

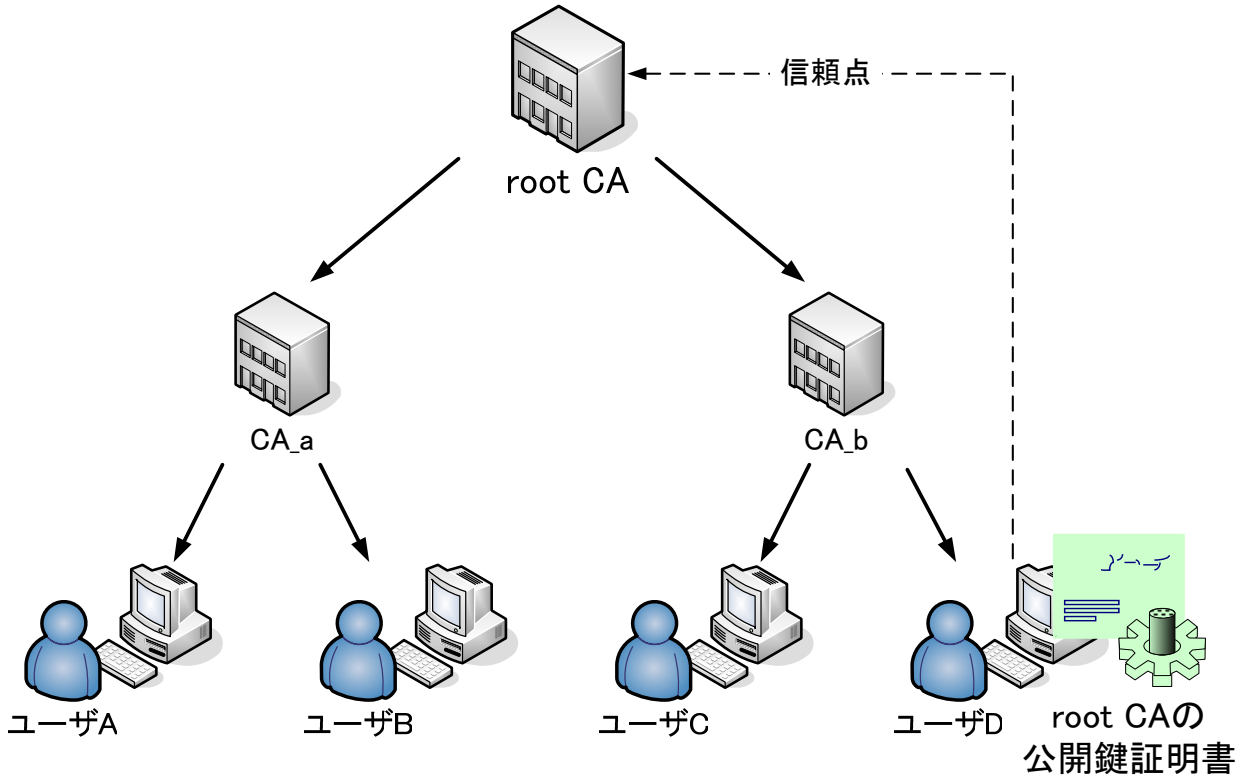


- PKIを参考に企業内ネットワークという閉じた世界において管理負荷の少ない新しい認証基盤の一方式を検討する

信頼関係の構築

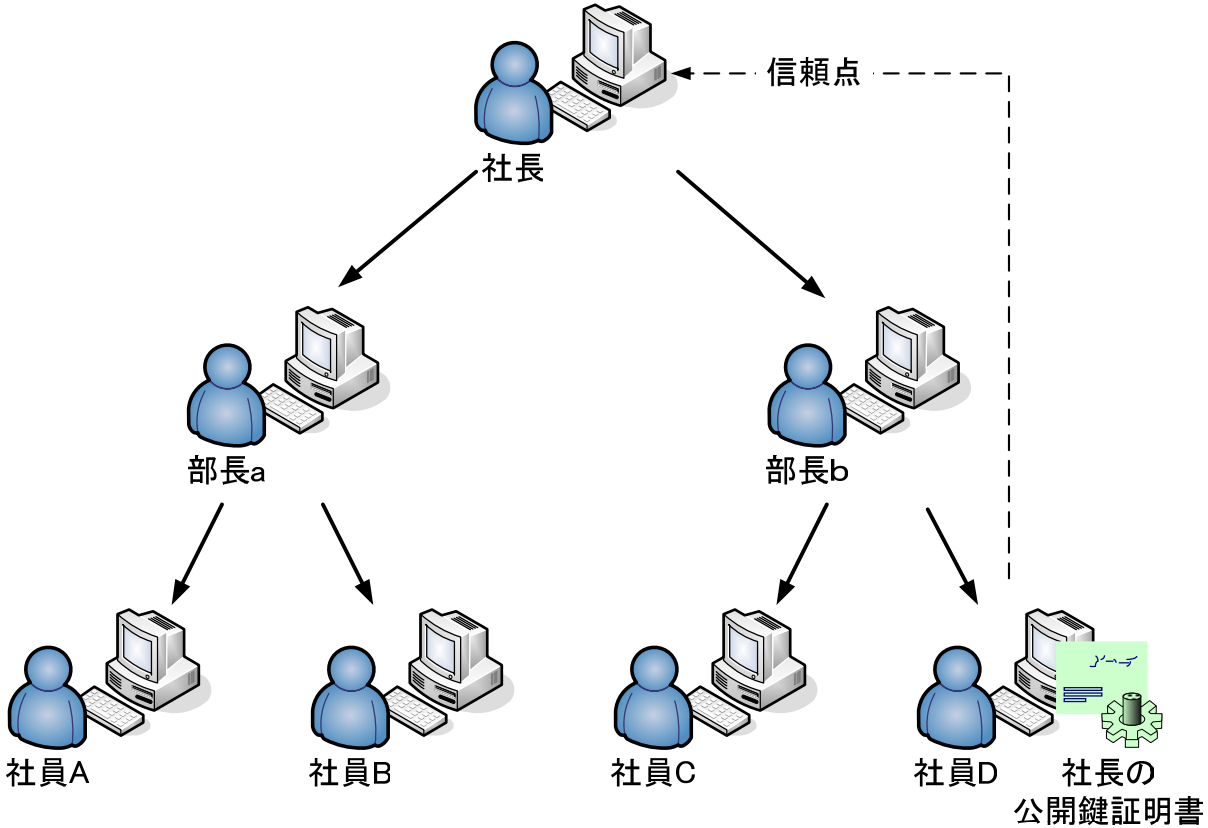
- 認証局CAは公開鍵証明書を他のCAに発行してもらうことにより信頼関係を構築する　(CA：Certificate Authority)

階層型（ツリー構造）に構成する階層型モデル



業務形態への対応

階層型モデルは業務形態と対応付けできる

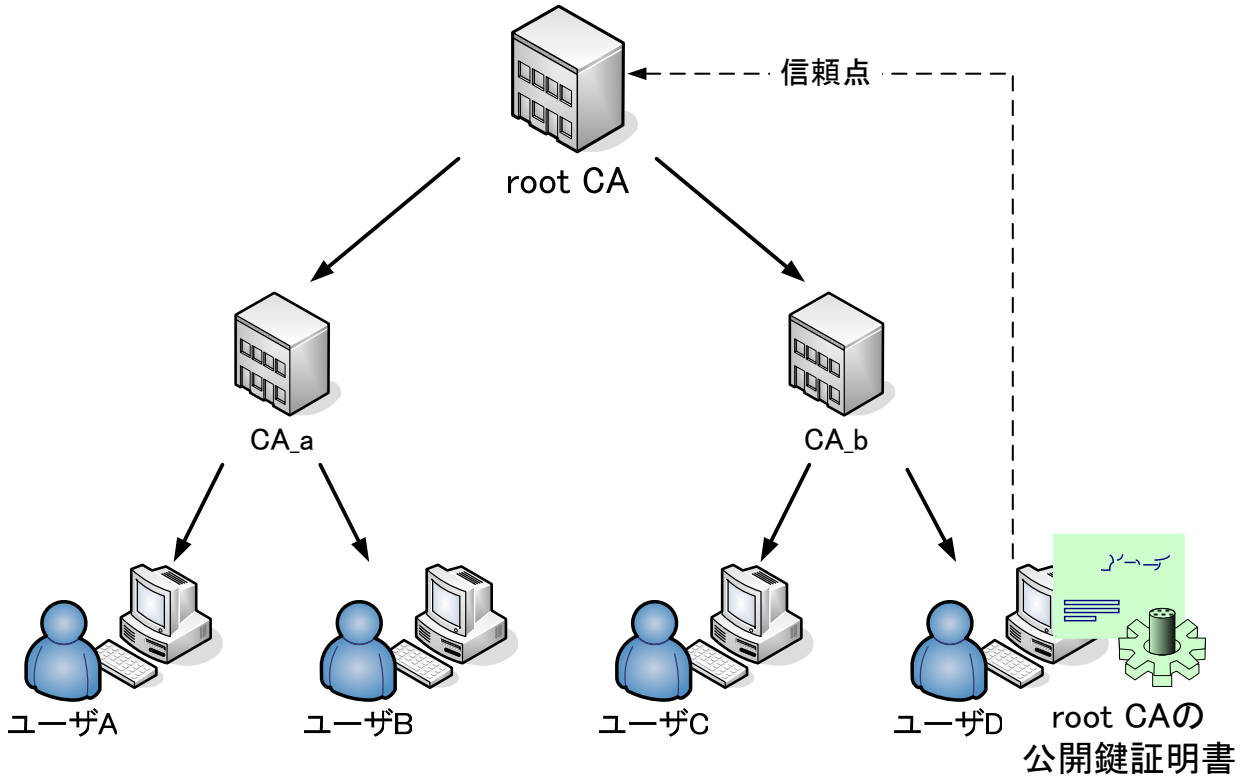


- 信頼関係を階層型モデルで行えば人事異動等による公開鍵証明書の変更にも対応しやすい

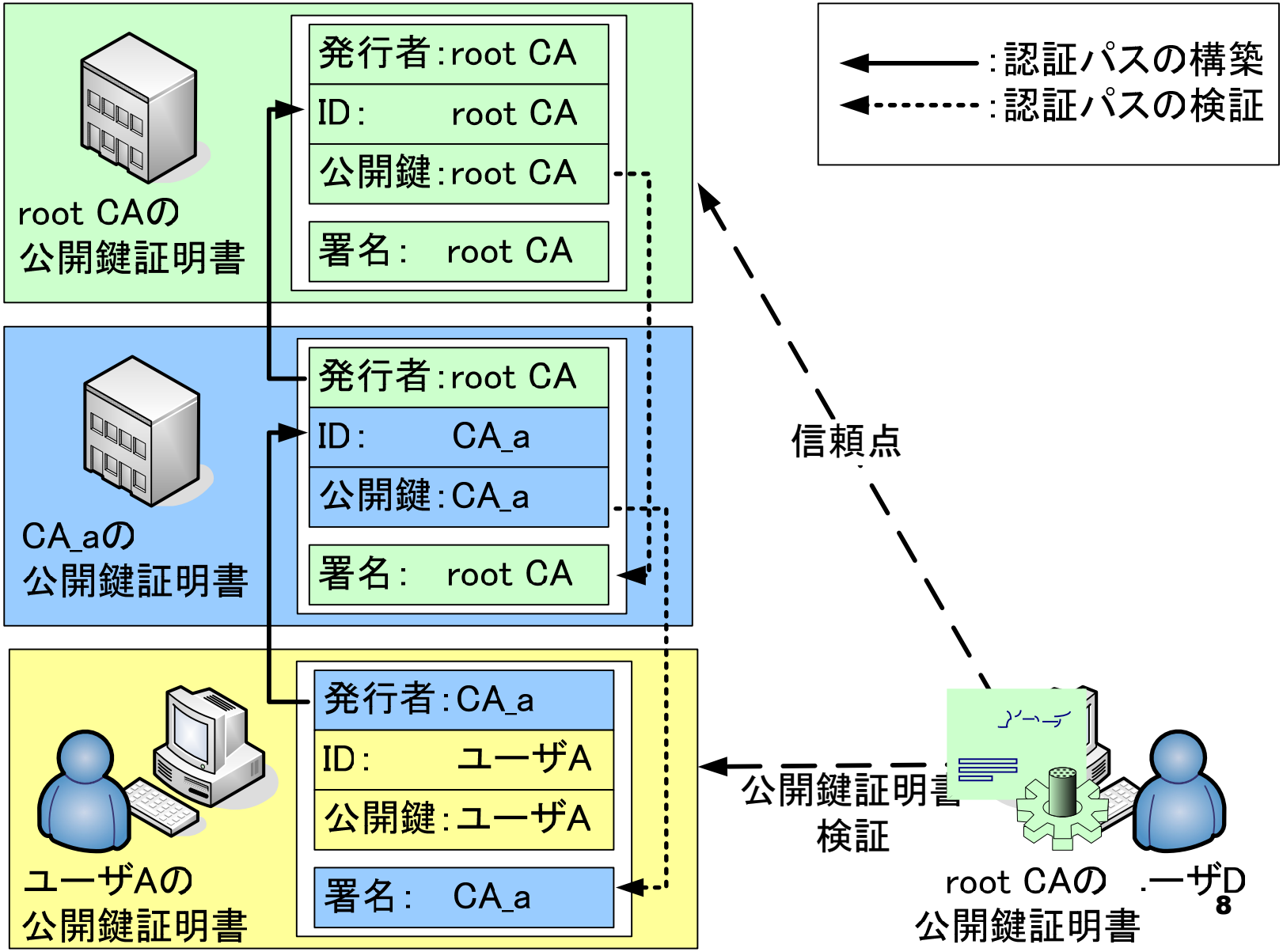
信頼関係の構築

- 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)

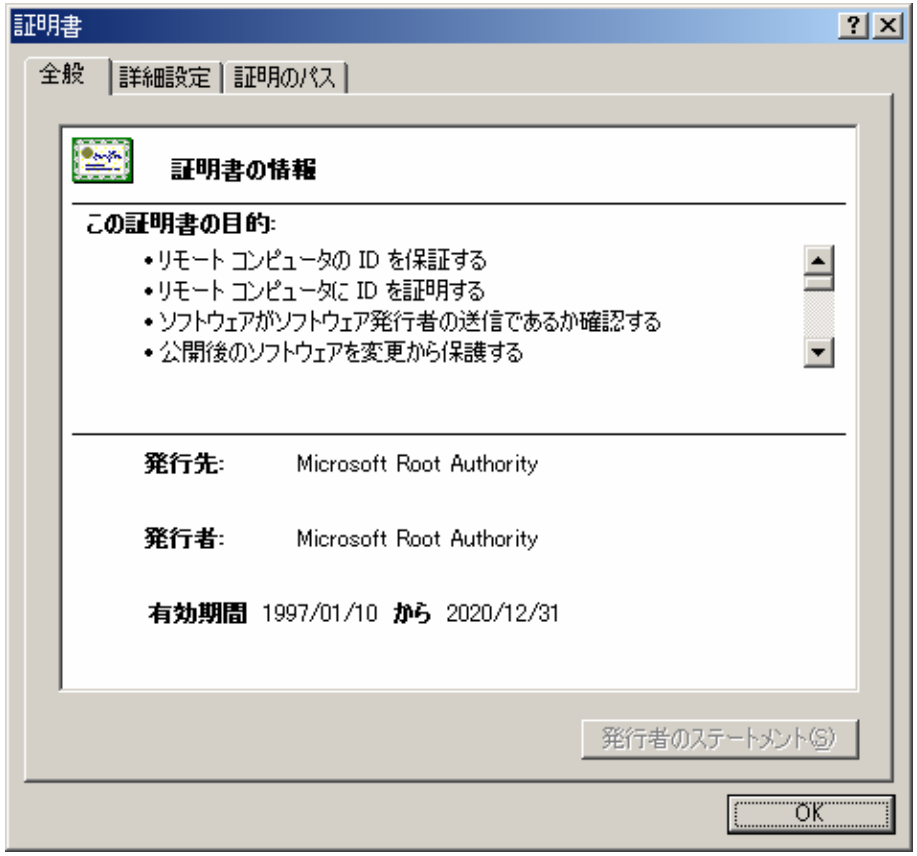
階層型（ツリー構造）に構成する階層型モデル



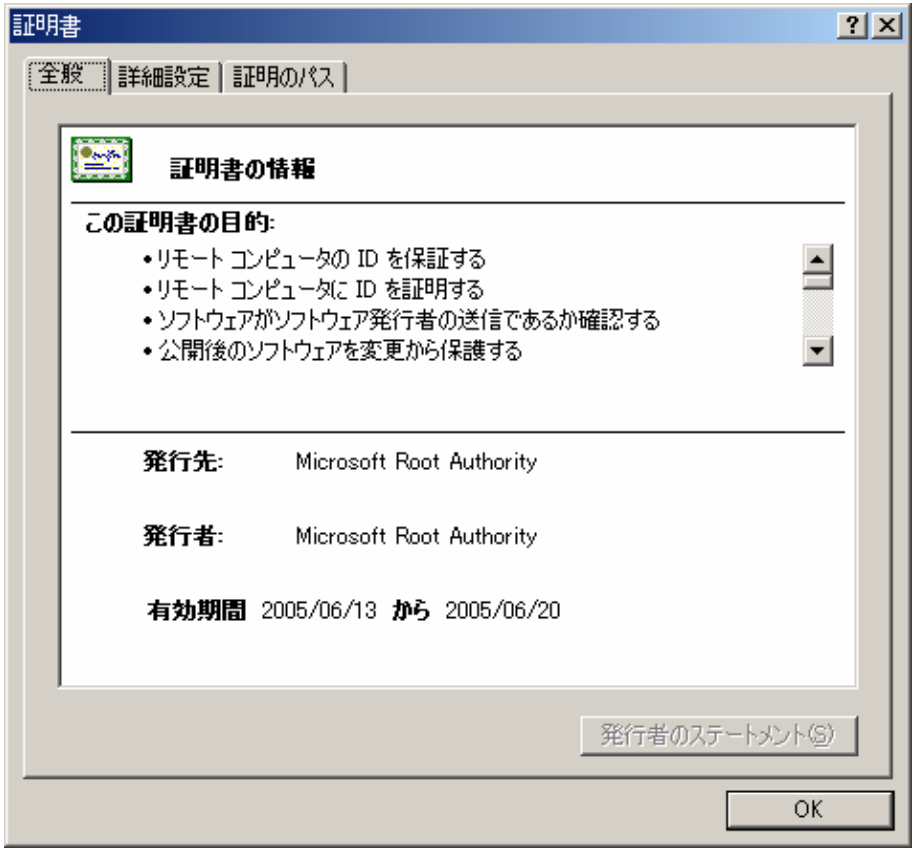
公開鍵証明書の検証


発行者:root CA
ID: root CA
公開鍵:root CA
署名: root CA
root CAの
公開鍵証明書
発行者:root CA
ID: CA_a
公開鍵:CA_a
署名: root CA
CA_aの
公開鍵証明書
発行者:CA_a
ID: ユーザA
公開鍵:ユーザA
署名: CA_a
ユーザAの
公開鍵証明書
:認証パスの構築
:認証パスの検証
信頼点
公開鍵証明書
検証
root CAの
公開鍵証明書

自己署名の公開鍵証明書偽造



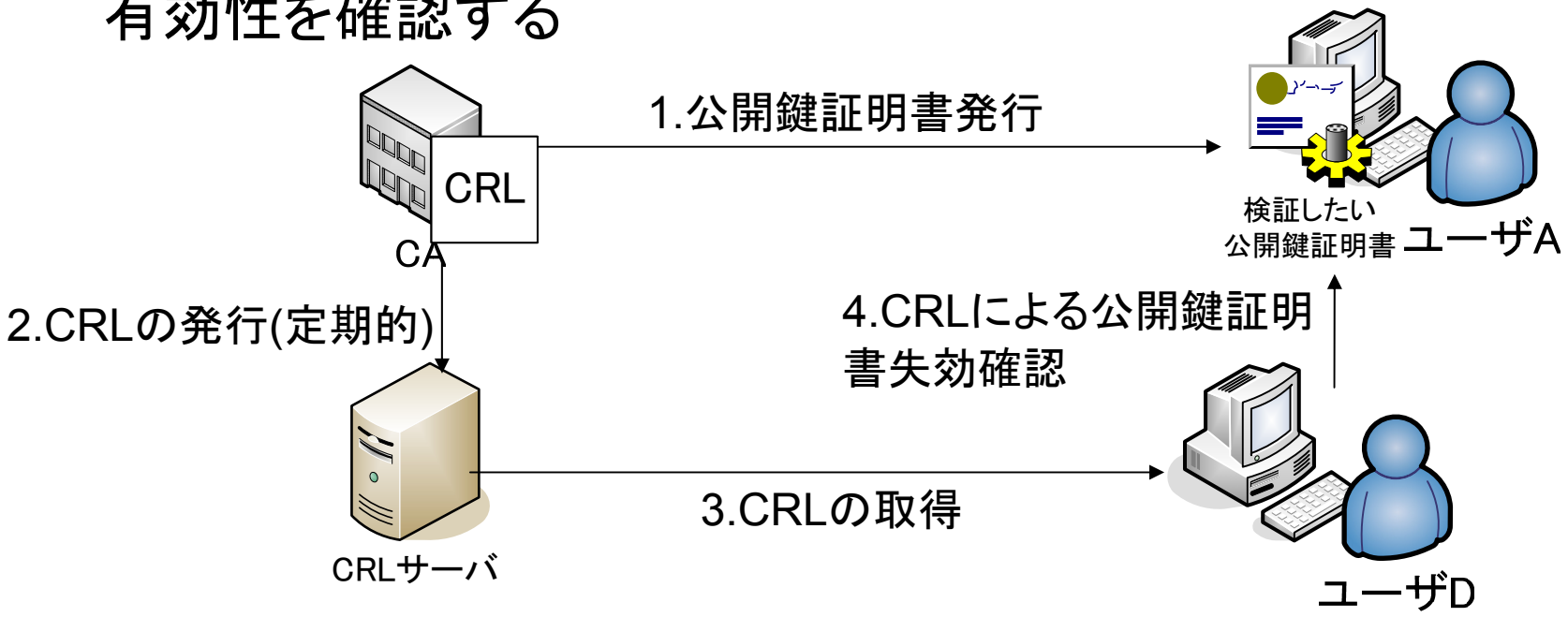
偽造前



偽造後

CRL（Certificate Revocation List)

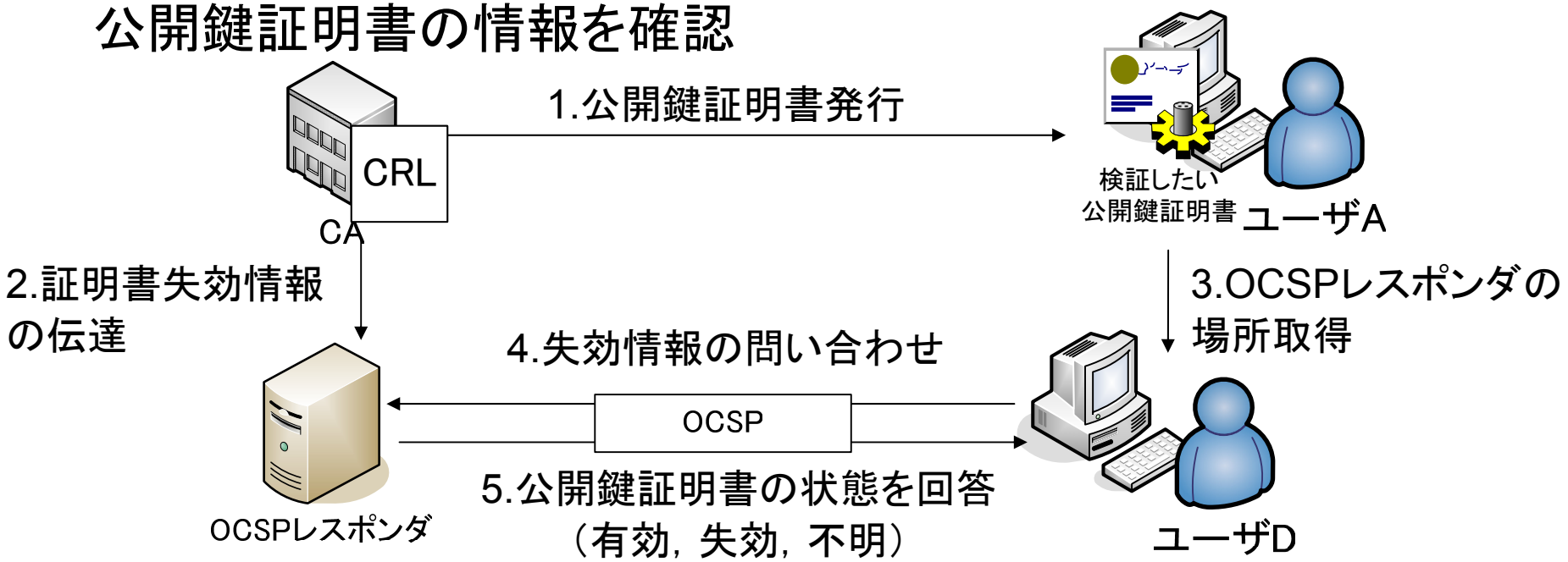
- 公開鍵証明書がCRLに掲載されていないことをもって有効性を確認する



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レスポンダ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
  - 自己署名の公開鍵証明書を偽造可能
  - 失効情報の管理が面倒
  - 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

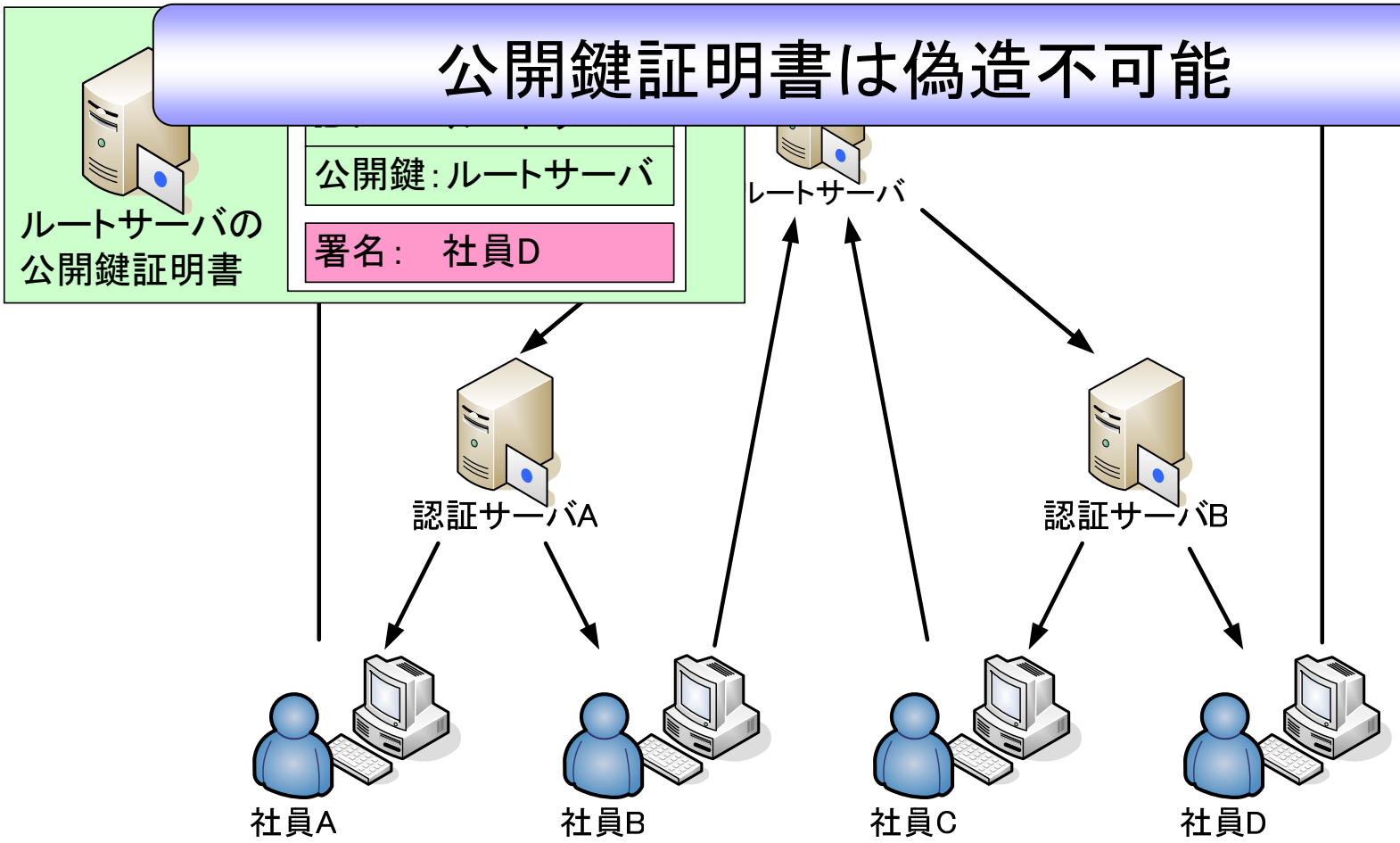
本方式

- 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

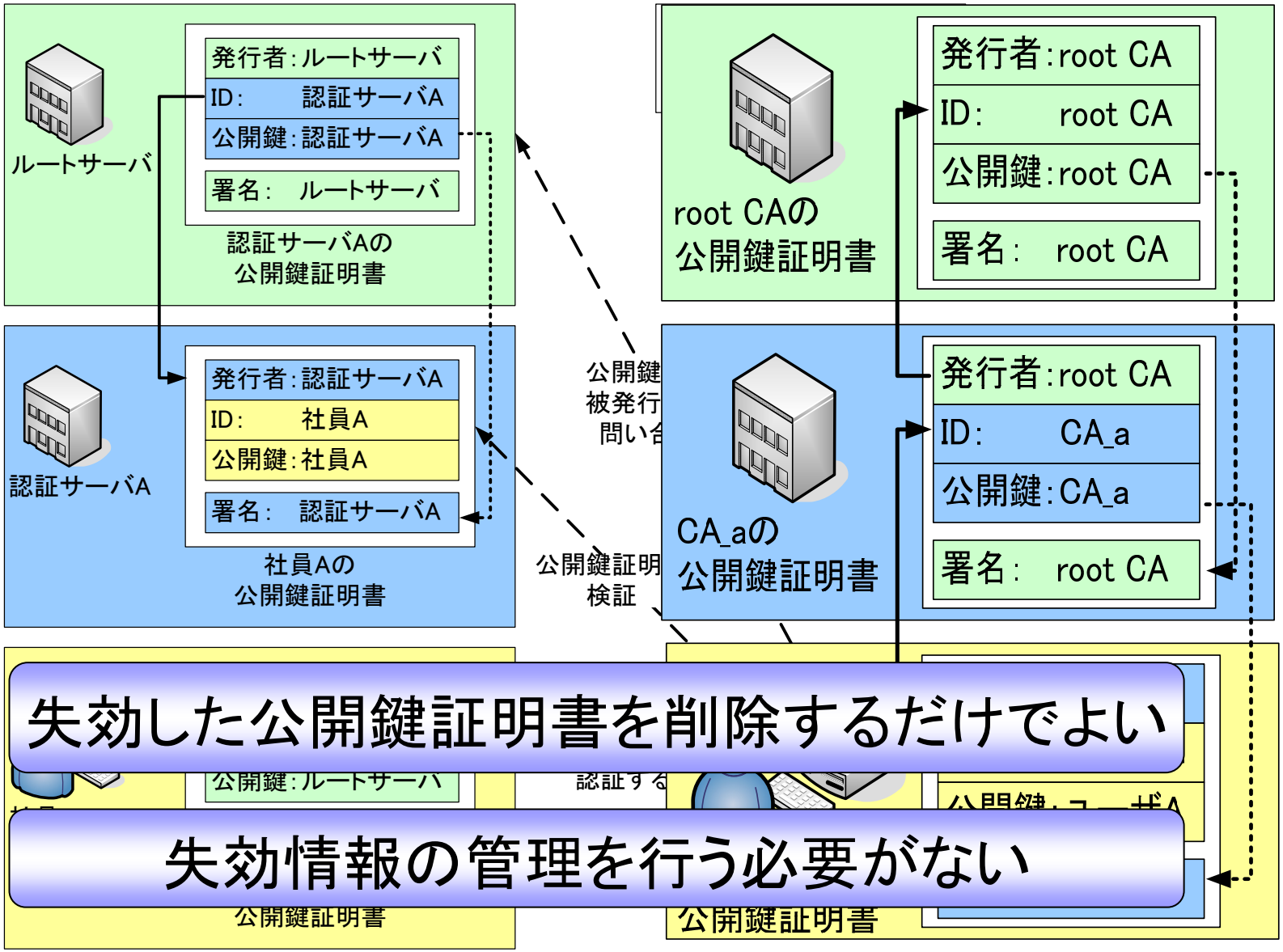
信頼関係を環状化

ルートサーバの公開鍵証明書が検証可能

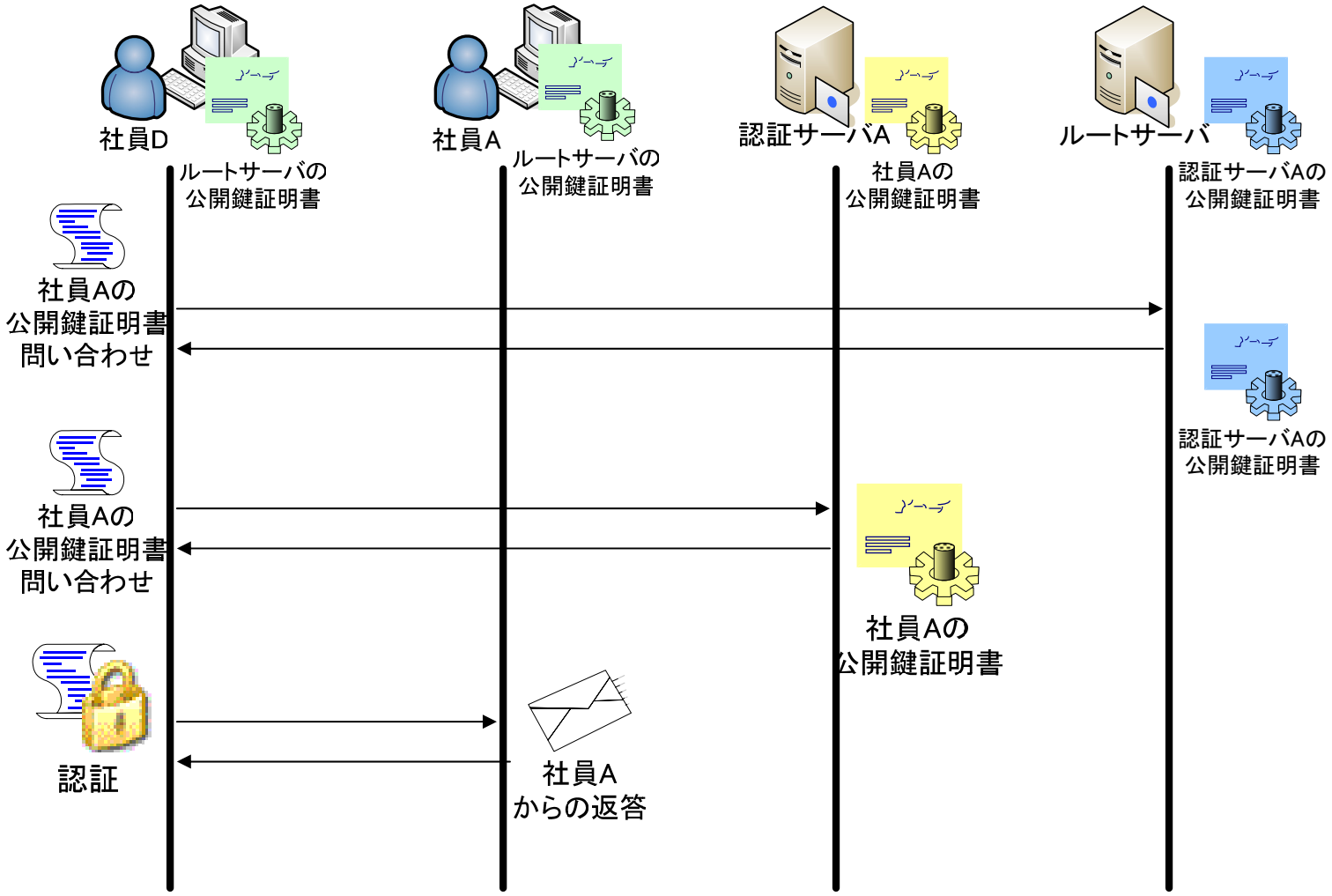
公開鍵証明書は偽造不可能



公開鍵証明書の管理方法



検証時の収集方法



リアルタイム性に優れている

評価

	リアルタイム性	管理コスト	最上位の公開鍵証明書	公開鍵証明書の検証方法	ルート機関の負荷
PKI(CRL)	△	△	検証不可能	オフラインとオンライン	○
PKI(OCSP)	○	△	検証不可能	オンラインのみ	○
本方式	◎	○	検証可能	オンラインのみ	△

- 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
- オンラインでのみ公開鍵証明書を検証できる
- ルート機関の負荷が大きくなる

小規模な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検討した
  - 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，本方式を実装し，検証を行っていく予定である

おわり