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

053432018　坂野文男
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．PKI はユーザに秘匿，認証，完全性，否認拒否の機能を提供する．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 の信頼関係の構築と公開鍵証明書を認証するまでの検証方法については以下の課題がある．一つ目は，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．二つ目は，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公開鍵証明書の失効情報を利用する必要がある．しかし失効情報の管理には手間がかかり，その情報が必ずしも最新とは限らないという課題がある．

本稿では，PKI を参考に企業内ネットワークで利用できる管理負荷の少ない認証システム ASE(Authentication System for an Enterprise network)を提案する．ASE の特徴は，最上位機関の自己署名をやめて，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，信頼関係の検証をオンデマンドで行うことである．これにより，高セキュリティでありながら管理が容易でかつリアルタイム性の高い認証基盤を提供できる．

2. PKI の課題

2.1 公開鍵証明書の偽造

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，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．このことは，root CA の公開鍵は偽造される可能性があることを示している．Windows では root CA の公開鍵証明書がレジストリに保存されているが，このレジストリを直接操作することにより書き換えができる．通常 root CA の公開鍵証明書をインストールや削除を行う場合にはセキュリティ警告ウィンドウが表示されるが，レジストリから直接 root CA の公開鍵証明書を操作するとセキュリティ警告ウィンドウが表示されない．そこで悪意あるプログラムなどによりレジストリを操作されてもユーザはそのことに気づかない．

2.2 失効情報の管理

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．公開鍵証明書は発行者の手を離れ被発行者が所持しているため，特定のユーザの公開鍵証明書を失効させたくても対象のユーザが公開鍵証明書の削除を行わず使用し続ける可能性がある．従って，公開鍵証明書が失効していないかどうかを発行者に確認する必要がある．このために失効情報が必須となっている．

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．また失効情報の確認に証明書失効リスト CRL[1]が利用されるが，CRL をあらかじめ収集しておく必要がある．CRL は定期的に更新されるため，最新の情報が得られないことがある．

3. 提案方式 ASE

本稿では，企業内ネットワークに認証システム導入することを想定し，上記のような PKI の課題を解決する方式 ASE を提案する．

3.1 信頼関係の構築

ASE の信頼関係を図 1 に示す．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，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することができる．

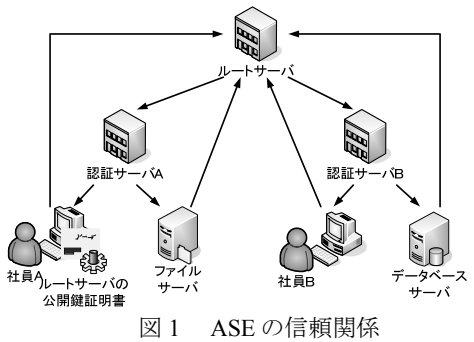


図 1　ASE の信頼関係

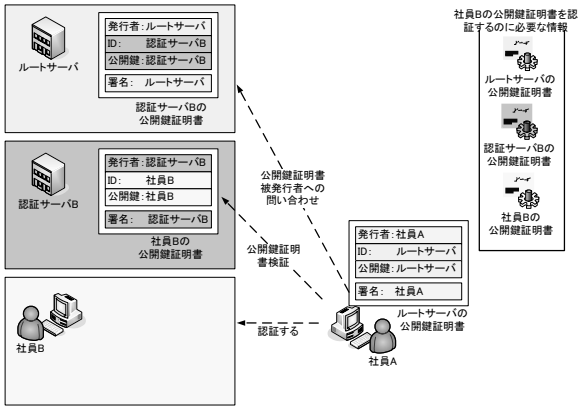


図 2　ASE の公開鍵証明書の管理方法

3.2 公開鍵証明書の管理

ASE の公開鍵証明書の管理方法を図 2 に示す．図 2 は，図 1 における社員 A が社員 B を認証する場合に必要となるデータのみを示している．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よい．

3.3 公開鍵証明書の有効性検証

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 の公開鍵証明書返答する．もし公開鍵証明書が失効していた場合はその旨を返答する．

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．検証が成功した場合，社員 B の公開鍵証明書は信頼することができる．

3.4 ルートサーバの負荷分散

ASE はルートサーバに対して各社員と各サーバが署名を行うという性質上，公開鍵証明書の検証時にすべてのユーザとサーバがルートサーバへ問い合わせを行う必要があるため，ルートサーバへの負荷が高くなる．この課題を次のよう負荷分散することにより解決する．図 1 のような信頼関係をルートサーバが確実に処理しきれる社員数で複数に分割する．そして構築されたルートサーバ同士を橋渡しするために新たにブリッジサーバを作成し，ルートサーバとブリッジサーバ間を相互に認証し信頼関係を構築する．これにより 1 つのルートサーバへの負荷が軽減される．

4. 実装

クライアント側の処理は，被検証者情報と許可する階層数を取得する処理，公開鍵証明書より問い合わせ先サーバの名前を取得する処理，サーバへ公開鍵証明書を問い合わせ，サーバから送られてきた情報を取得する処理，収集した公開鍵証明書を検証する処理が必要となる．

サーバ側はクライアントの問い合わせを受け付け，受け付けた情報に対応する公開鍵証明書を検索し，クライアントへ返答するプログラムが必要となる．

今回はサーバ側処理と，クライアント側の公開鍵証明書を収集する処理の部分を試作した．検証処理は書籍 [2]に掲載されているクライアントの公開鍵証明書の検証プログラムにより代用した．

表 1　PKI と ASE の比較

	PKI	ASE
公開鍵証明書の認証処理時間	76.1ms	78.3ms
最上位公開鍵証明書の検証	× 検証不可能	○ 検証可能
リアルタイム性	△	○
通常運用時の管理負荷	△	○

5. 評価

PKI と ASE の比較を表 1 に示す．

PKI の公開鍵証明書の認証処理時間は 76.1ms であるのに対し ASE の処理時間は 78.3ms と約 3%の増加であった．

最上位の公開鍵証明書の検証に関しては，PKI は自己署名のため発行者が正当であることを検証できないのに対し，ASE 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．

リアルタイム性については，PKI で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が，ASE ではオンデマンドで認証パスを構築するためユーザが最新の有効性を確認できる

通常運用時の管理負荷については，PKI 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が，ASE は失効情報が不要であり管理コストが低い．

6. まとめ

企業ネットワークにおける認証システム ASE を提案した．ASE では，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．評価結果より ASE は企業ネットワークには有効な方式であることがわかった．今後は ASE を完成させたるため検証プログラムを作成する予定である．

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] John Viega, Matt Messier, Pravir Chandra 共著，齋藤孝道 翻訳：OpenSSL-暗号・PKI・SSL/TLS ライブラリの詳細-，p.301，オーム社(2004).

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

渡邊研究室

053432018　**坂野文男**

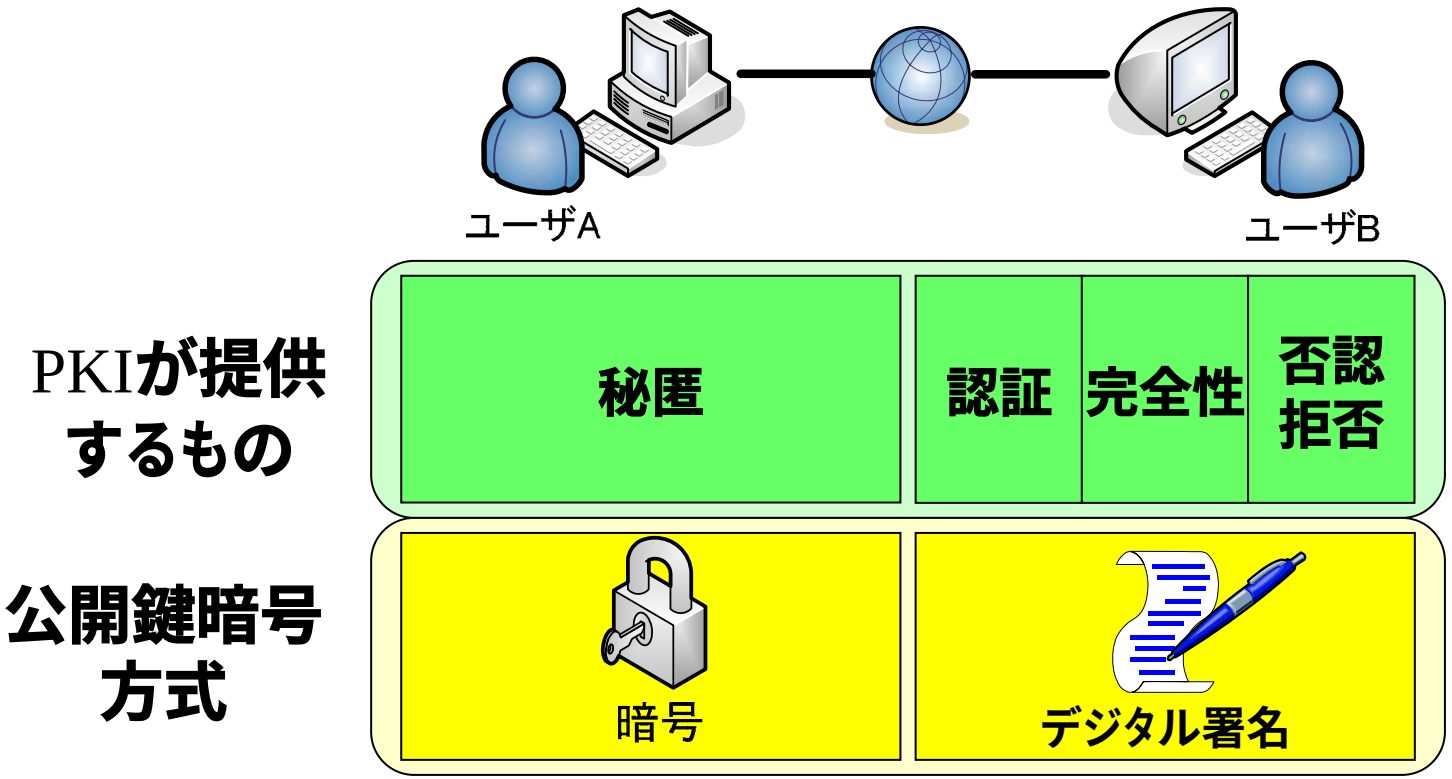
研究背景

- 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

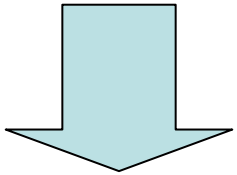
PKI（Public Key Infrastructure）

- **公開鍵暗号方式を利用したセキュリティの基盤**
  - **公開鍵暗号は暗号と復号に別々の鍵を利用**
- **PKIの構築により以下のものを提供できる**



企業への導入

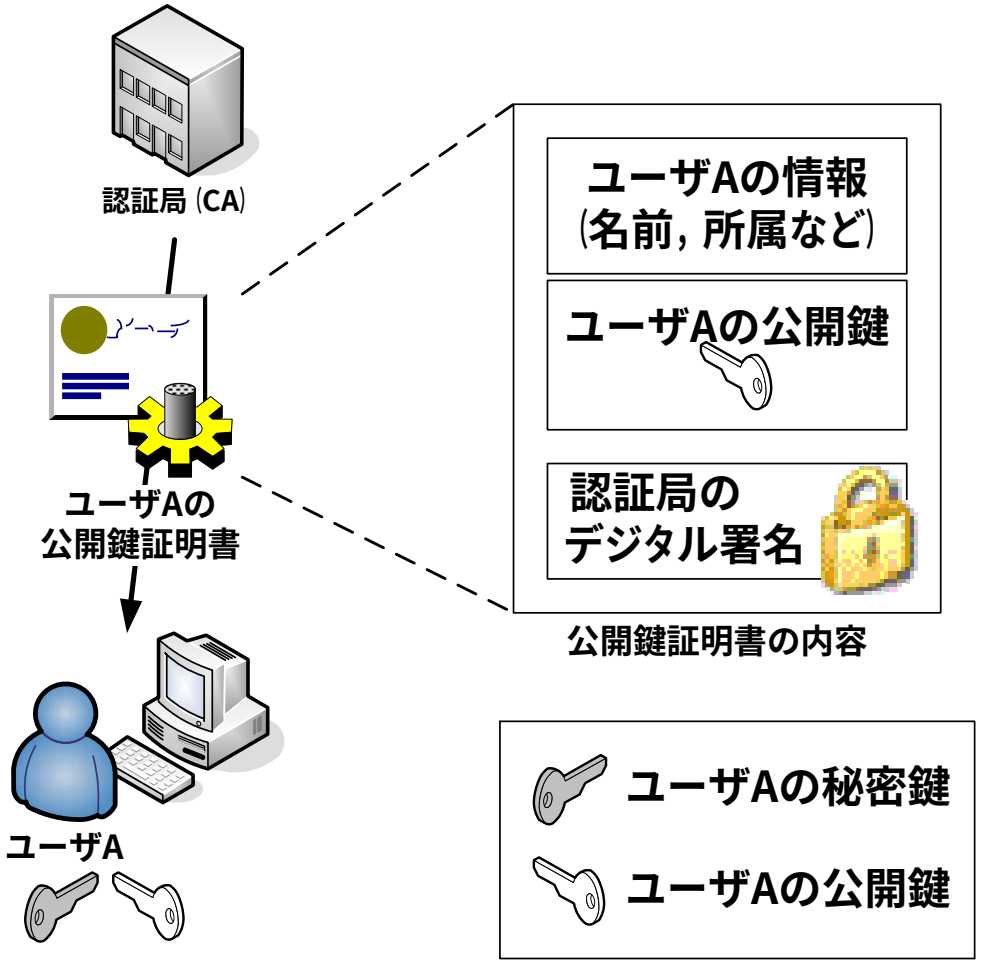
- **企業内ネットワークにおいてもPKIによる認証基盤を導入する傾向がある**
- PKI**には課題がある**



- PKI**を参考に企業内ネットワークで利用できる安全かつ管理負荷の少ない認証システム**ASE(Authentication System for an Enterprise network)**を提案する**

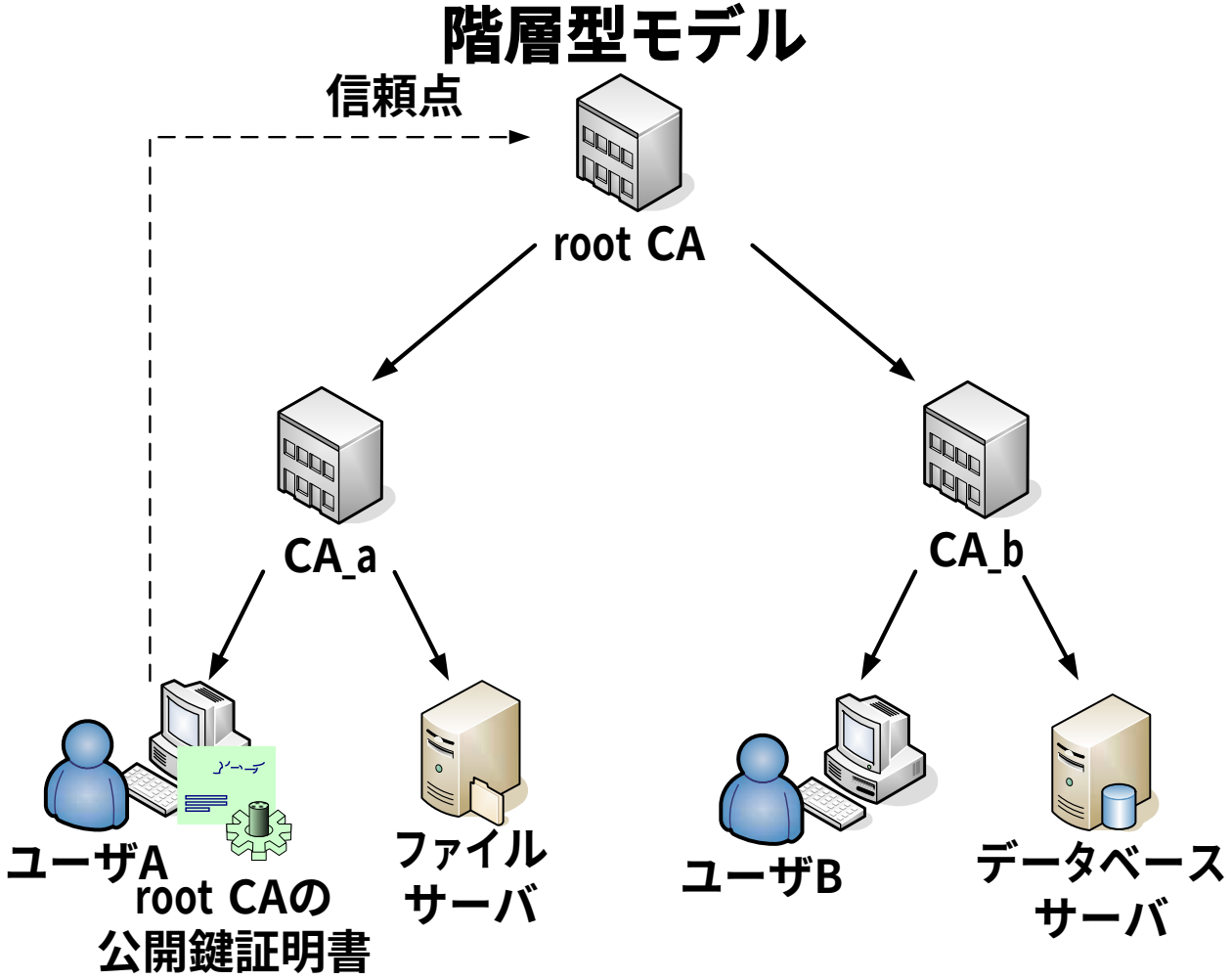
公開鍵証明書

- **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**



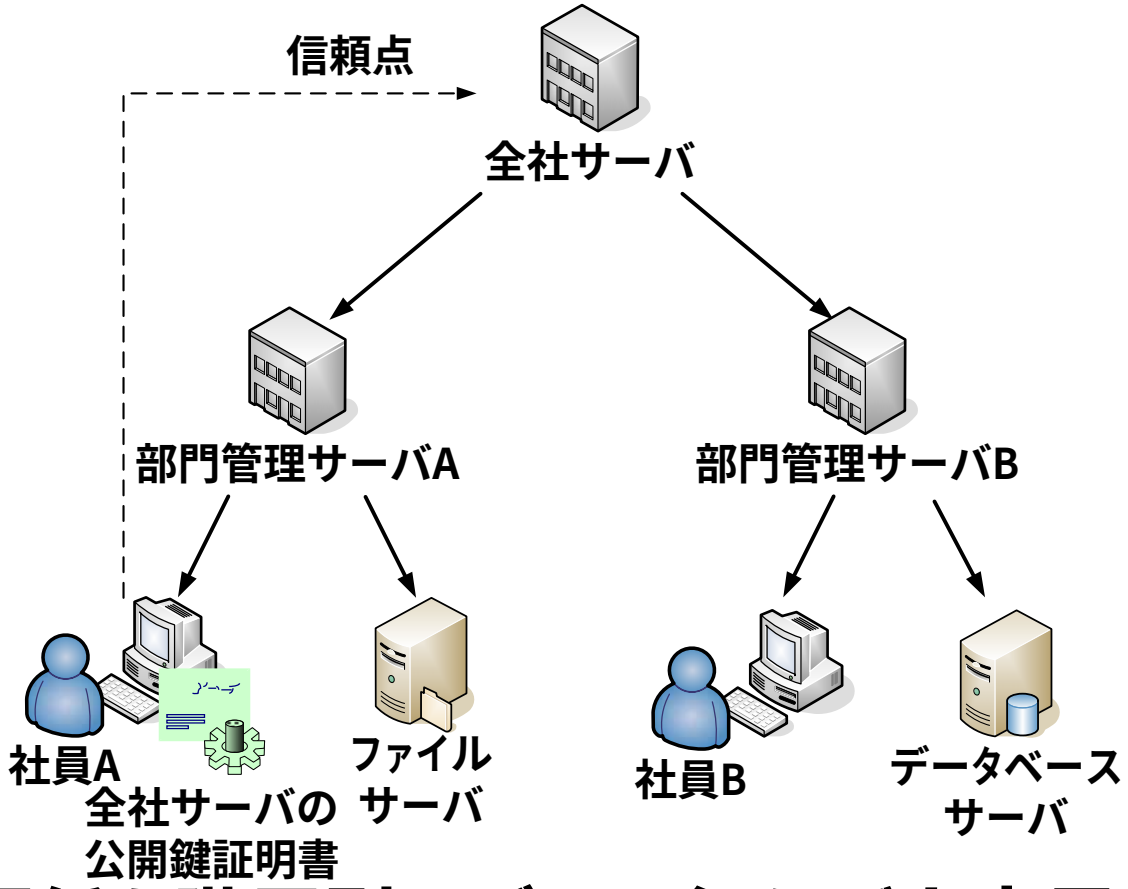
信頼関係の構築

- 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



業務形態への対応

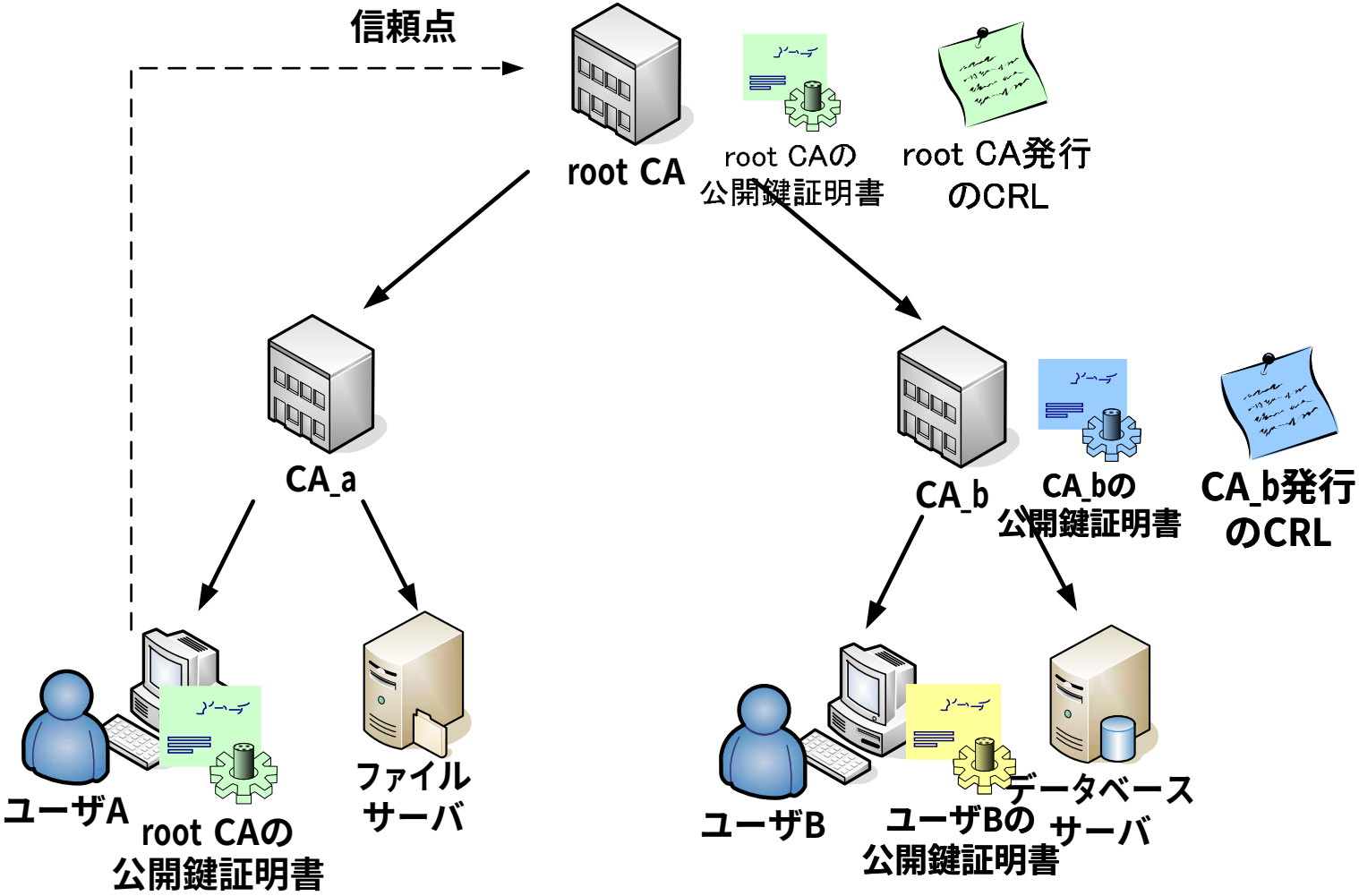
- 階層型モデルは業務形態と対応付けできる



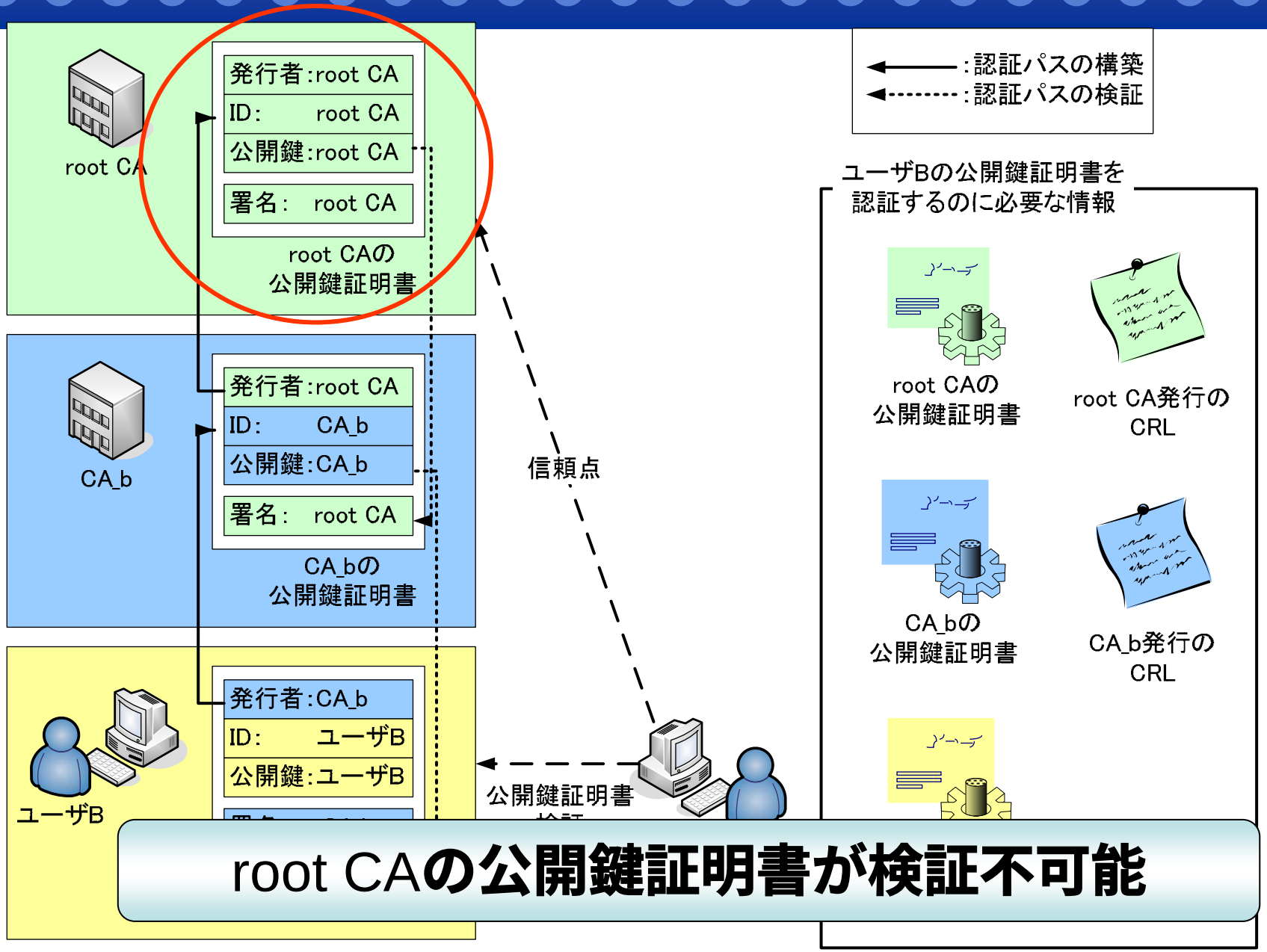
- 信頼関係を階層型モデルで行えば人事異動等による公開鍵証明書の変更にも対応しやすい

公開鍵証明書の検証

- ユーザAがユーザBを認証する場合



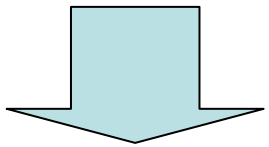
公開鍵証明書の検証



root CAの公開鍵証明書が検証不可能

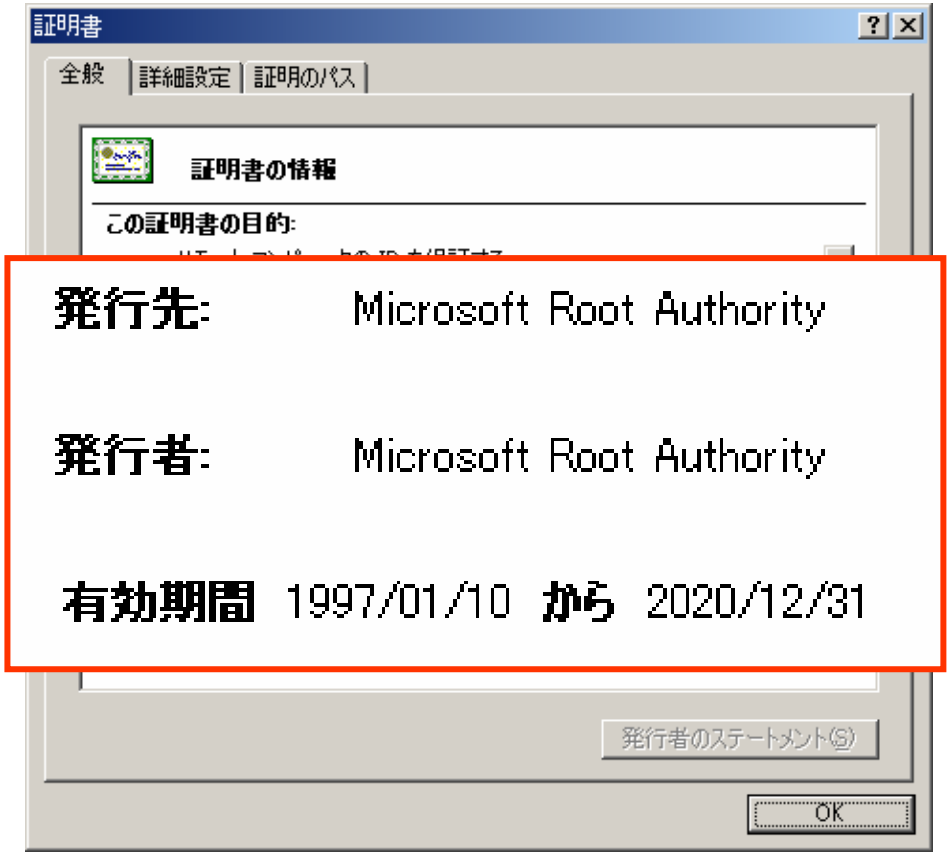
root CAの公開鍵証明書の偽造

- Windowsではroot CA の公開鍵証明書がレジストリに保存されている
- レジストリはコマンドラインで書き換え可能
- レジストリを操作しroot CAの公開鍵証明書の書き換えを行うと確認画面が表示されない



- 悪意あるプログラムで公開鍵証明書を偽造されるとユーザは気がつかない可能性が高い

自己署名の公開鍵証明書偽造

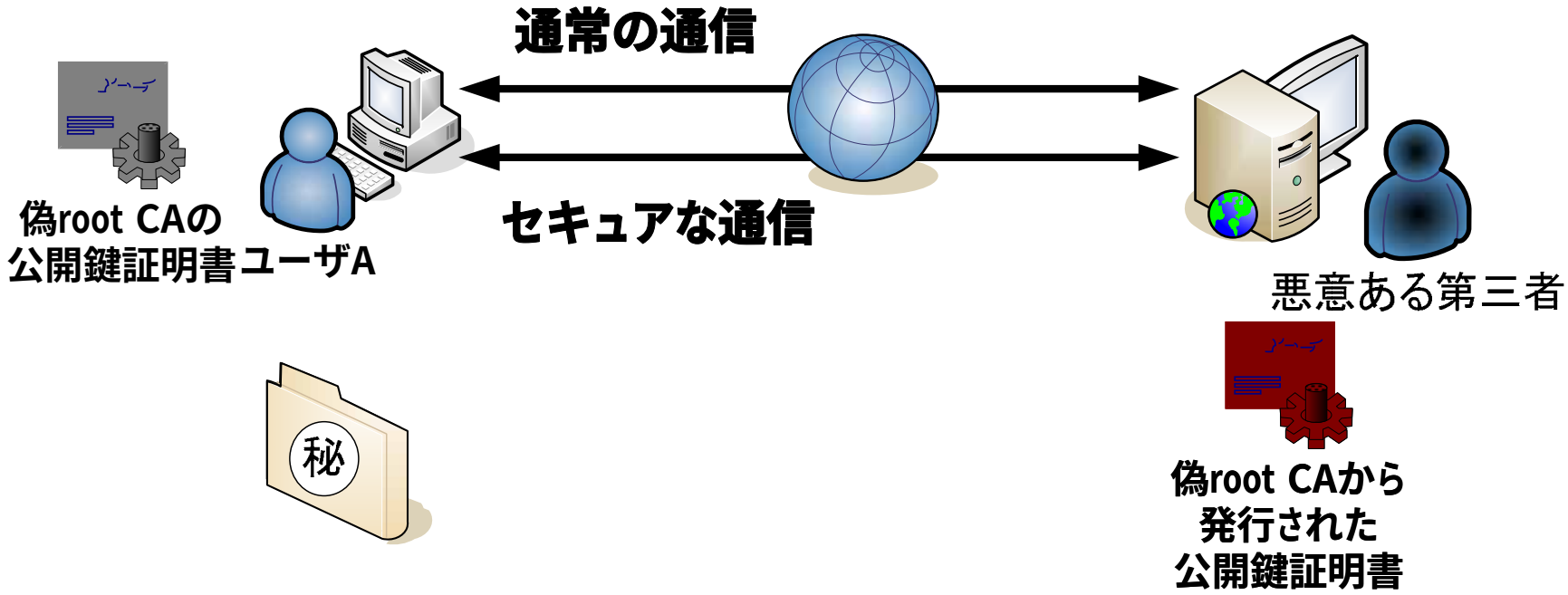


偽造前

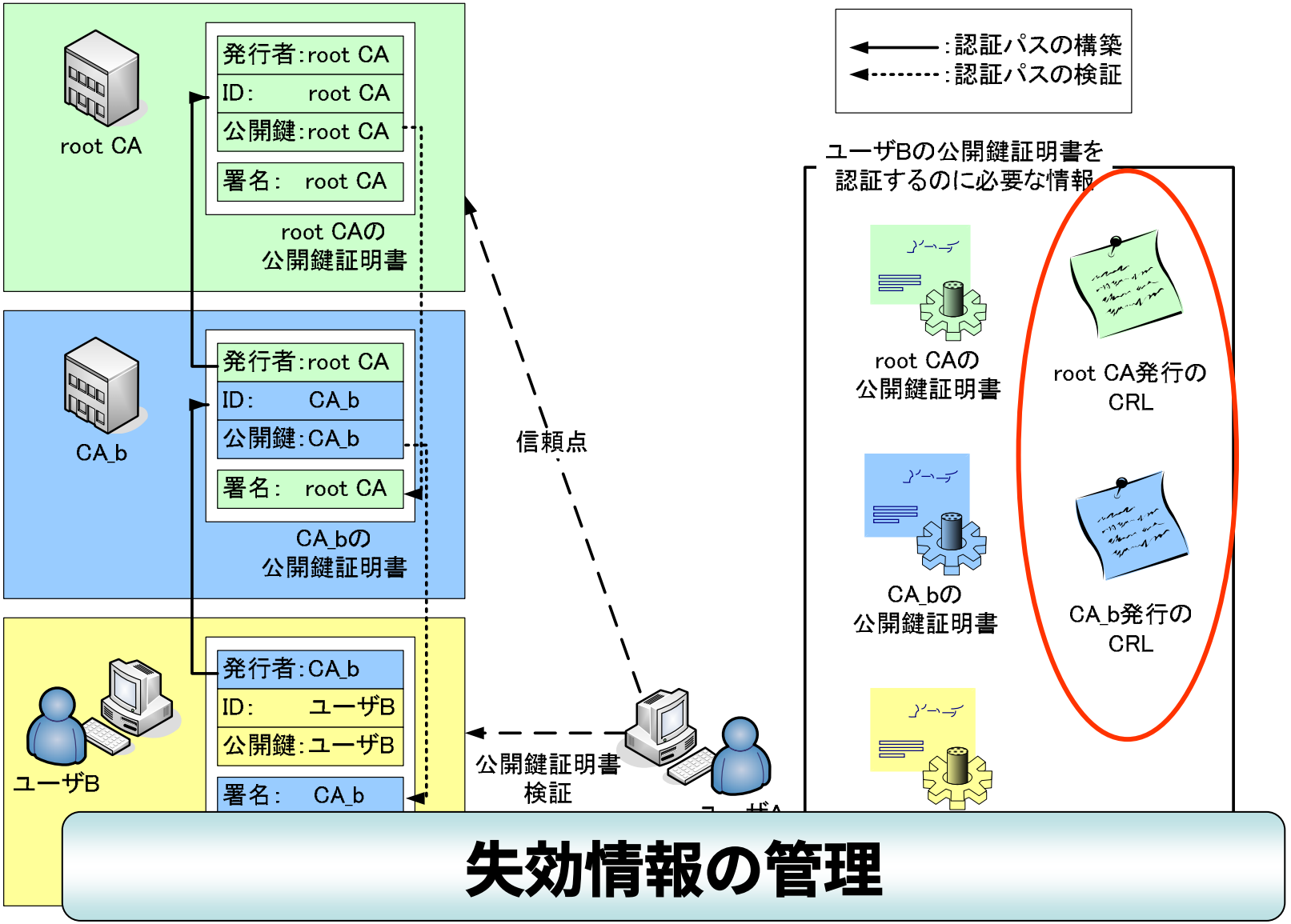
偽造後

偽造されたときの問題

- セキュアな通信を行う際，警告メッセージが表示されないため通信相手を信頼してしまう



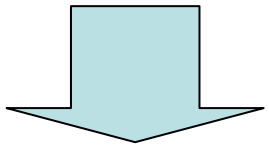
公開鍵証明書の検証に必要な情報



失効情報の管理

失効情報

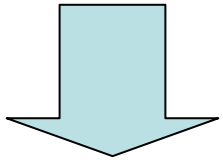
- 発行した公開鍵証明書が失効していないか確認するための情報
- 失効した公開鍵証明書や失効日時など記載



- 失効情報自体の管理が面倒

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**
- **事前にCRLを取得しておく**
- **決められた周期で発行される**



- **最新の情報ではない可能性がある**

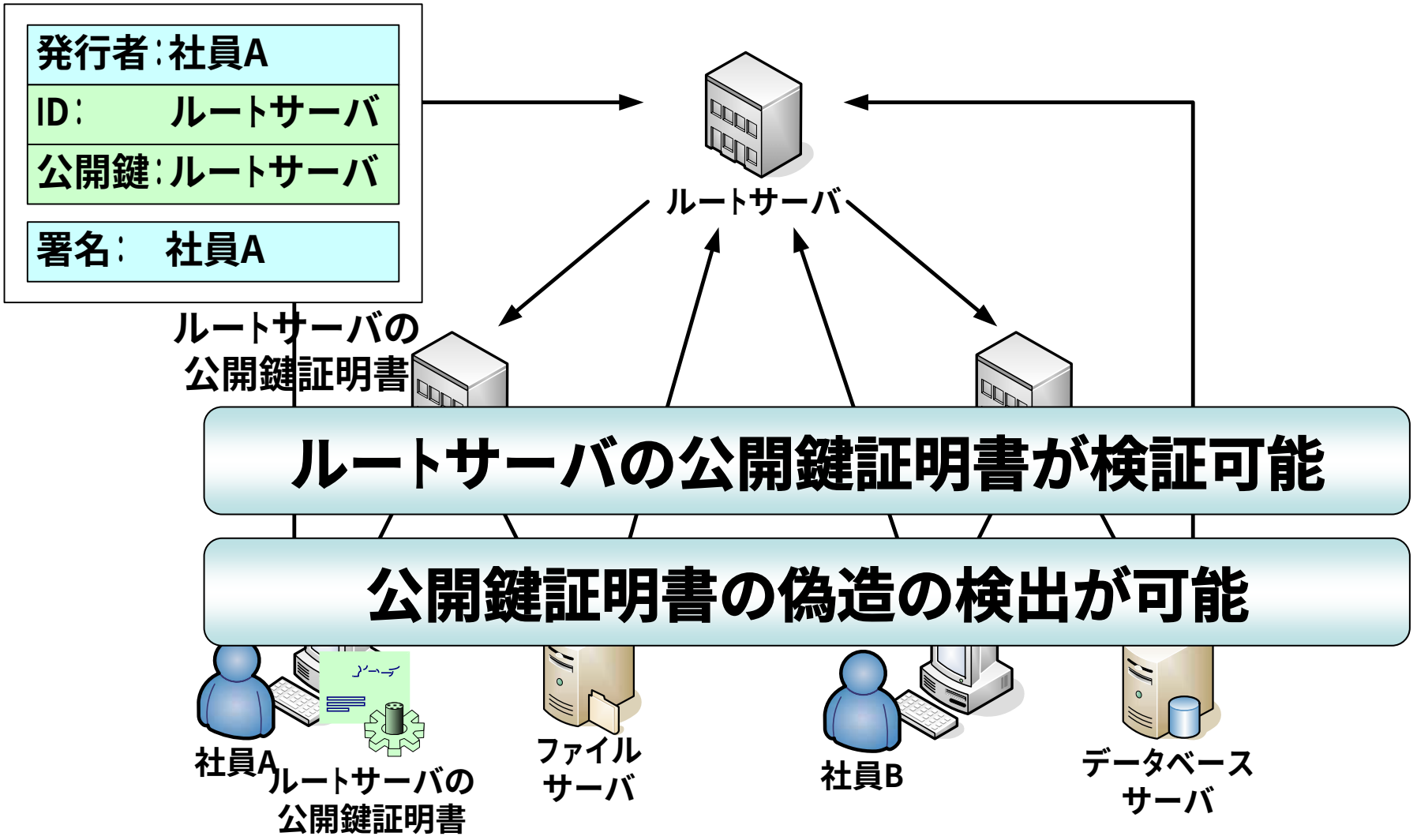
課題

- 企業ネットワークではPKIを適用するために以下のことが課題になる
  - 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

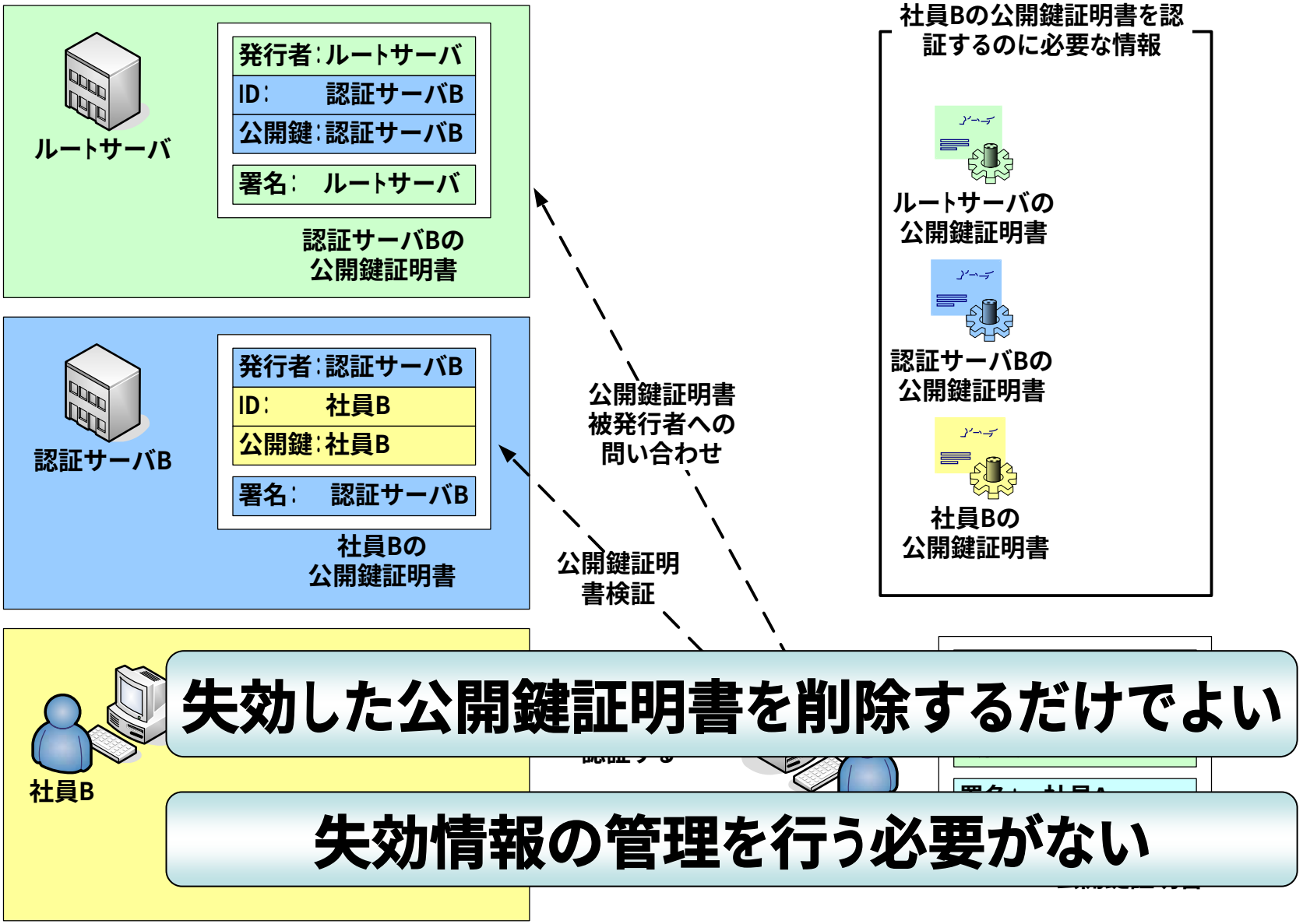
提案方式ASE

- 企業内ネットワークで利用できる認証システムASEを提案する
  - 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

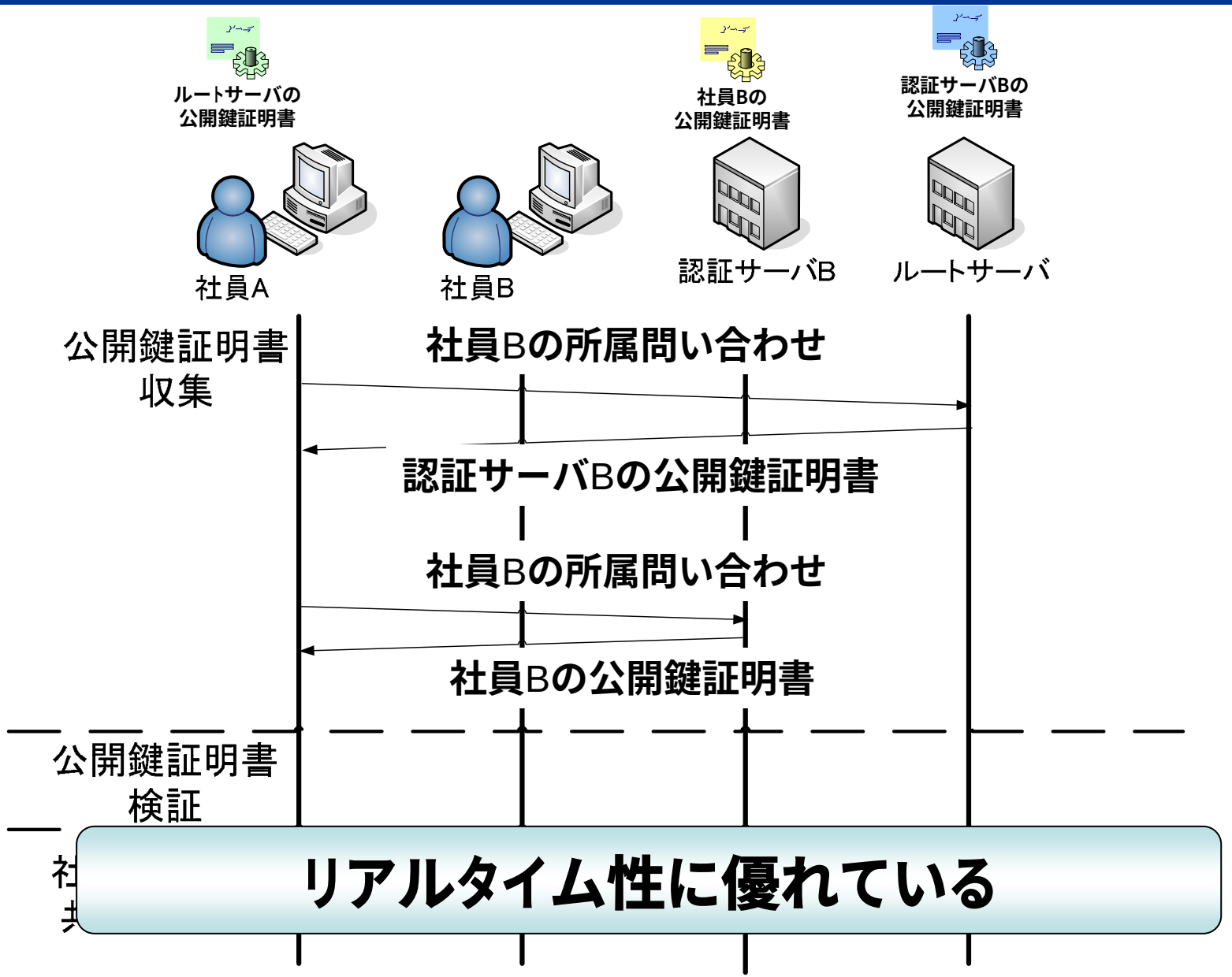
信頼関係を環状化


発行者：社員A
ID：　ルートサーバ
公開鍵：ルートサーバ
署名：　社員A
ルートサーバ
ルートサーバの
公開鍵証明書
ルートサーバの公開鍵証明書が検証可能
公開鍵証明書の偽造の検出が可能
社員A
ルートサーバの
公開鍵証明書
ファイル
サーバ
社員B
データベース
サーバ

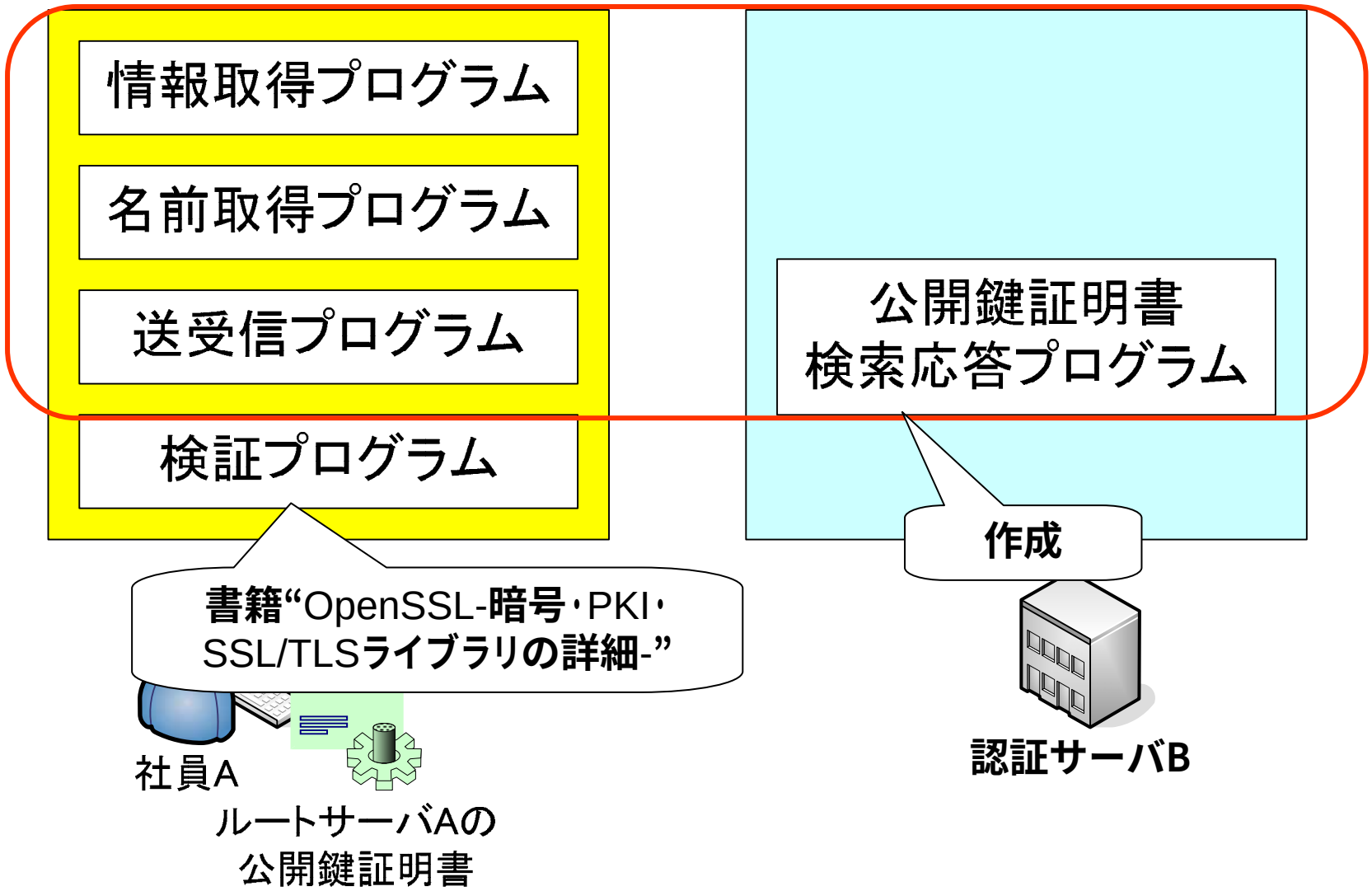
公開鍵証明書は発行者が保持し，自ら管理する



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

実装


情報取得プログラム
名前取得プログラム
送受信プログラム
検証プログラム
公開鍵証明書
検索応答プログラム
作成
書籍“OpenSSL-暗号・PKI・
SSL/TLSライブラリの詳細-”
社員A
ルートサーバAの
公開鍵証明書
認証サーバB

性能評価

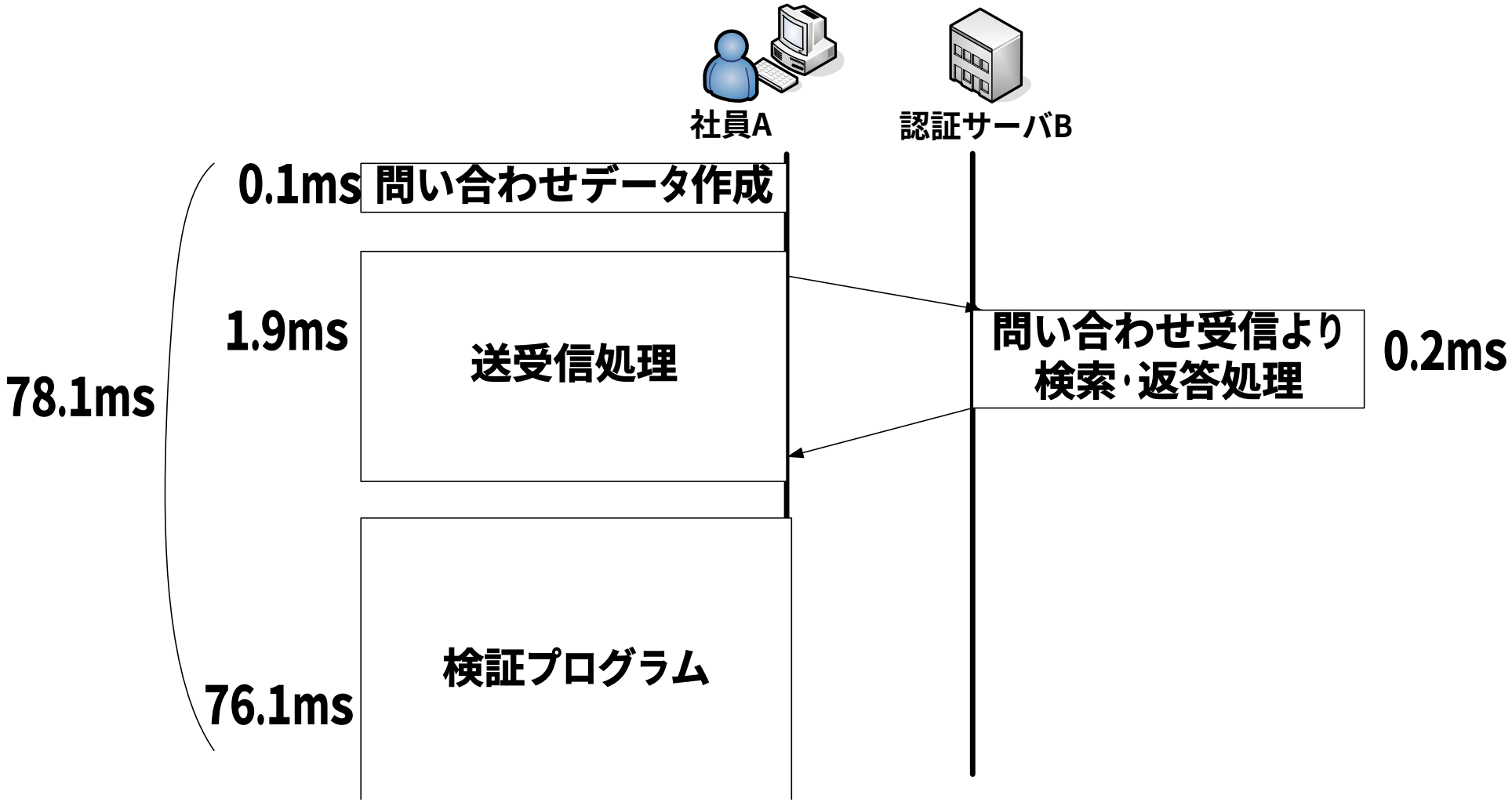
- 1階層の検証処理時間を測定

装置仕様

	クライアント	サーバ
PC Model	Endeavor NA101	
CPU	Core Solo U1400(1.20GHz)	
メモリ	512MB(PC2-4200)	
ネットワーク	100BASE-T	
OS	Linux	Linux
暗号化機能	Openssl	

性能評価

- **提案方式はPKIより3%処理時間増加**



評価

	PKI(CRL)	ASE
性能	76.1ms	78.1ms
最上位の公開鍵証明書	×	○
リアルタイム性	△	○
通常運用時の管理負荷	△	○
スケーラビリティ	○	△

- **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**
- **すべてのユーザがルートサーバへ問い合わせるため 大規模ネットワークではルートサーバの負荷が多くなる**

企業ネットワークで十分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認証システムASEを提案
  - 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，ASEを完成させたるため検証プログラムを作成する予定である