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

川島　隆太*，渡邊　晃(名城大学)

Researches on Authentication System for an Enterprise network ASE having high security

Ryuta Kawashima, Akira Watanabe (Meijo University)

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)を提案する．

２．PKI の課題

PKI は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．さらに，失効情報は新たな情報が加わった際に更新するのではなく，定期的に更新されるため，最新の情報が手に入らない場合がある．

３．ASE

そこで ASE では Fig.1 のように信頼関係を構築する．

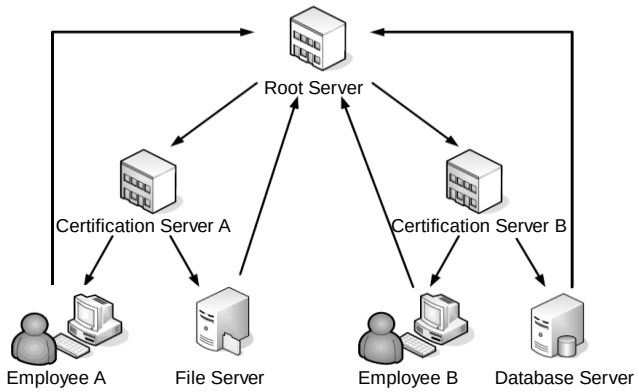


Fig.1. Trust relationship of ASE

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することができる．

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．このため，公開鍵証明書が失効した場合は失効情報などを必要とせず，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．Fig.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 の公開鍵証明書は信頼することができる．

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，ルートサーバへの負荷が高くなることが考えられる．これは複数のルートサーバを設置して全体の信頼関係を分割し，それらを繋ぐブリッジサーバを置くことで，負荷を分散できると考えられる．

提案方式を仮実装し，処理にかかる時間を測定したところ，PKI と同等の性能を得ることが確認できた．

４．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 を提案した．今後は ASE の実装と評価を行う．

文　献

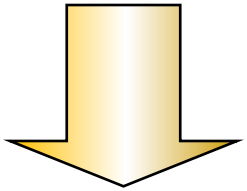
坂野文男，保母雅敏，渡邊晃 ：企業ネットワークにおける認証基盤構築の一方式， DICOMO2006， 2006.

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
川島隆太　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



暗号技術の重要性が高まっている

暗号技術

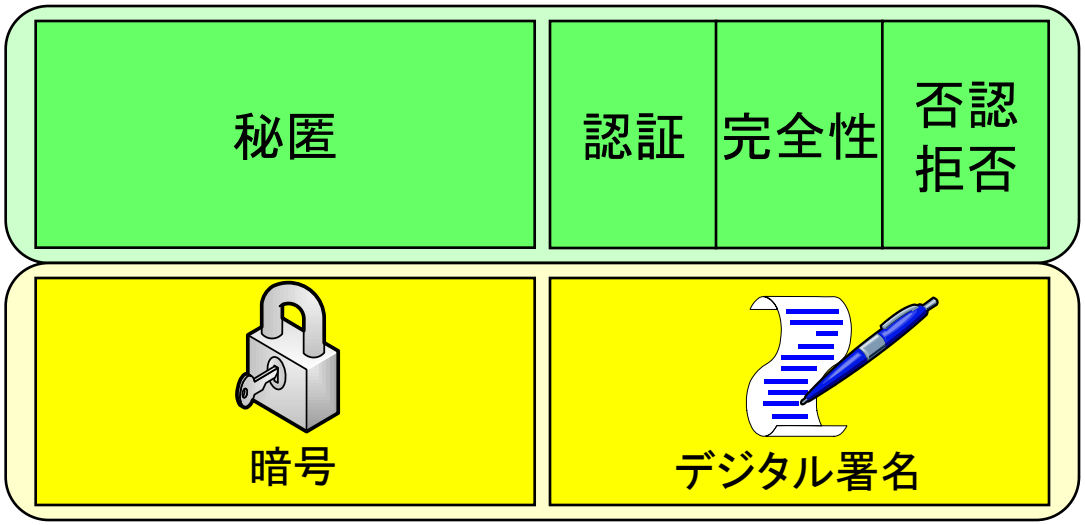
- 共通鍵暗号方式
  - 暗号化する時と復号する時に同じ鍵を利用
  - 鍵を秘密に管理する必要があり、データのやり取りする相手ごとに別の鍵を用意しなければならない
- 公開鍵暗号方式
  - 暗号化する時と復号する時に異なる鍵を利用
  - 一方の鍵を「公開鍵」と呼び，不特定多数のユーザに公開しても構わない

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

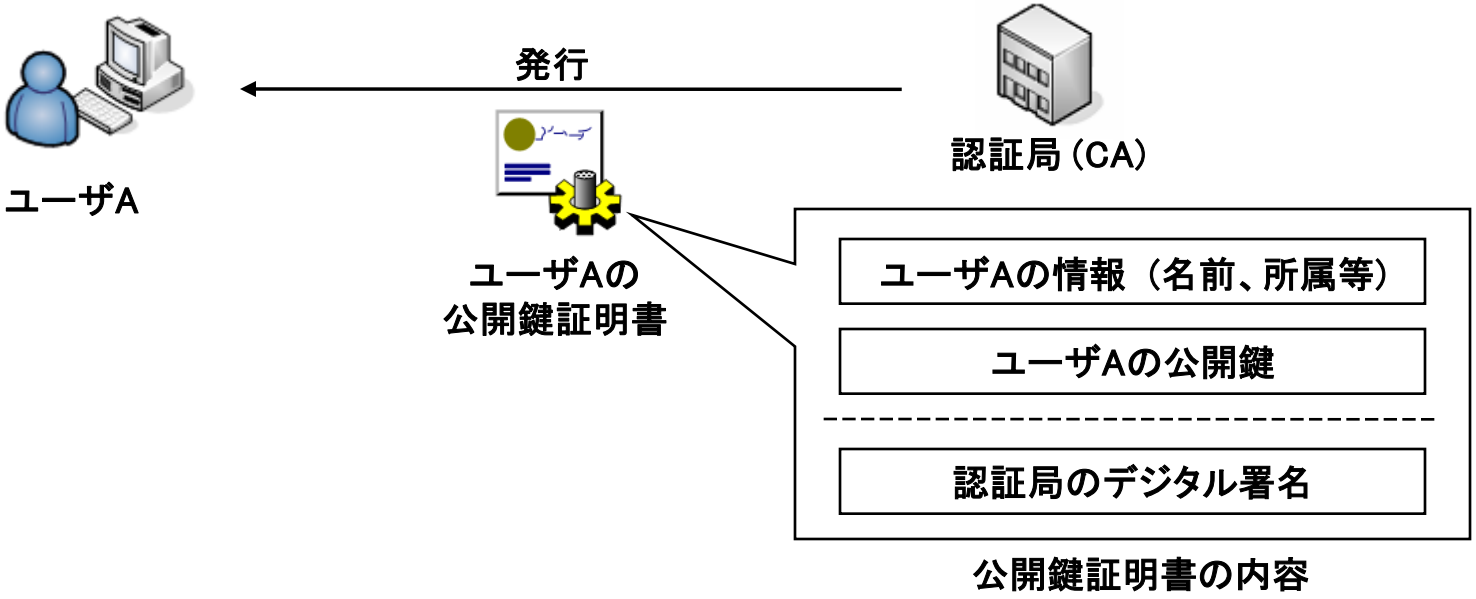
PKIが提供するもの

公開鍵証明書



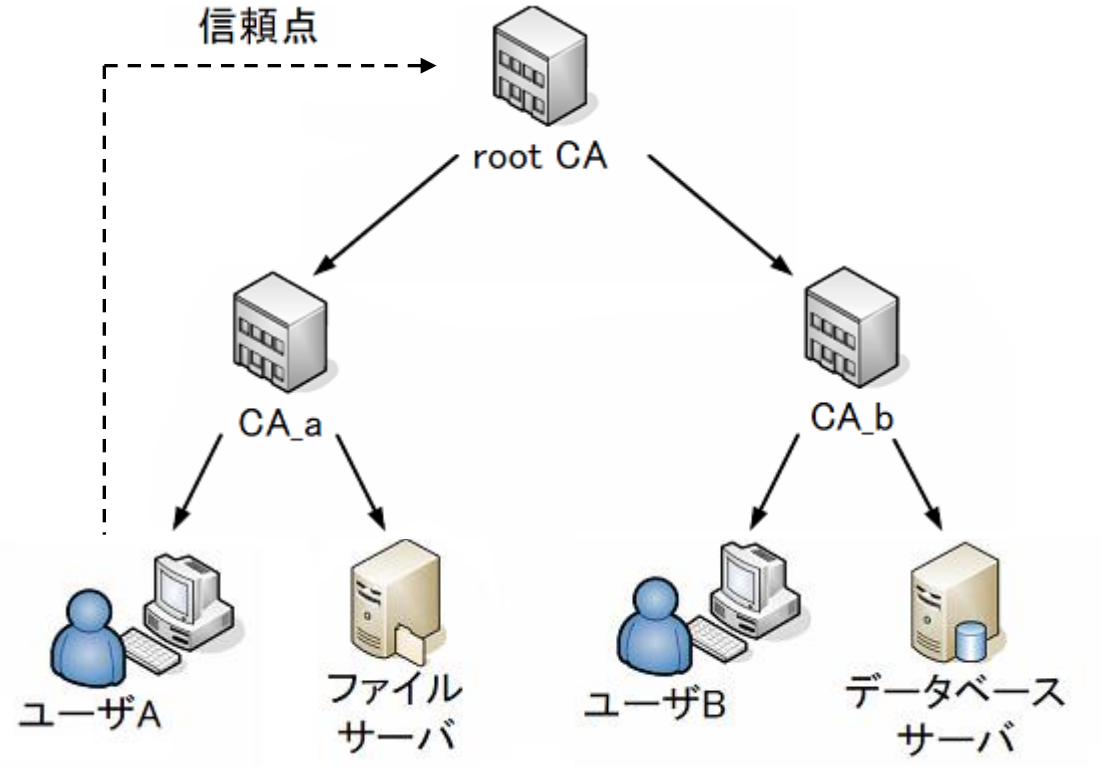
公開鍵証明書

- 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

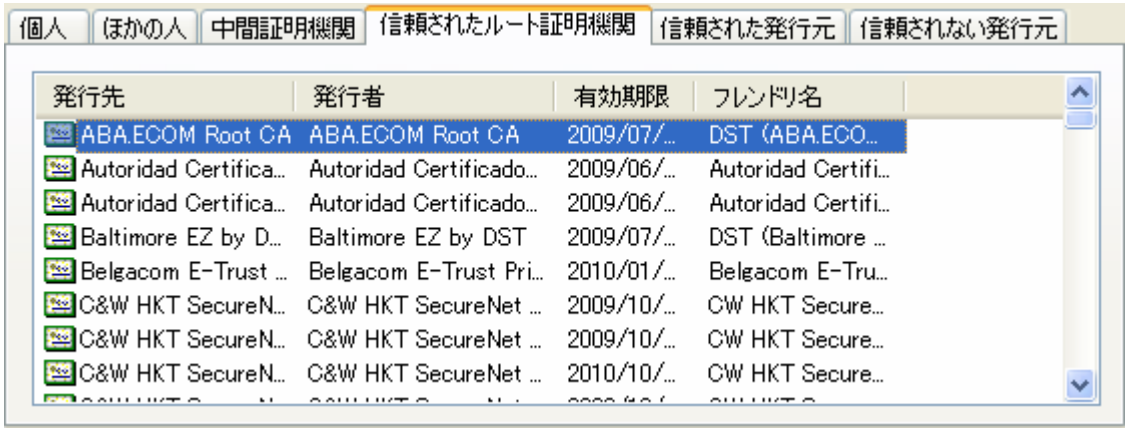
- 認証局CAは公開鍵証明書を上位のCAに発行してもらうことにより信頼関係ができる



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

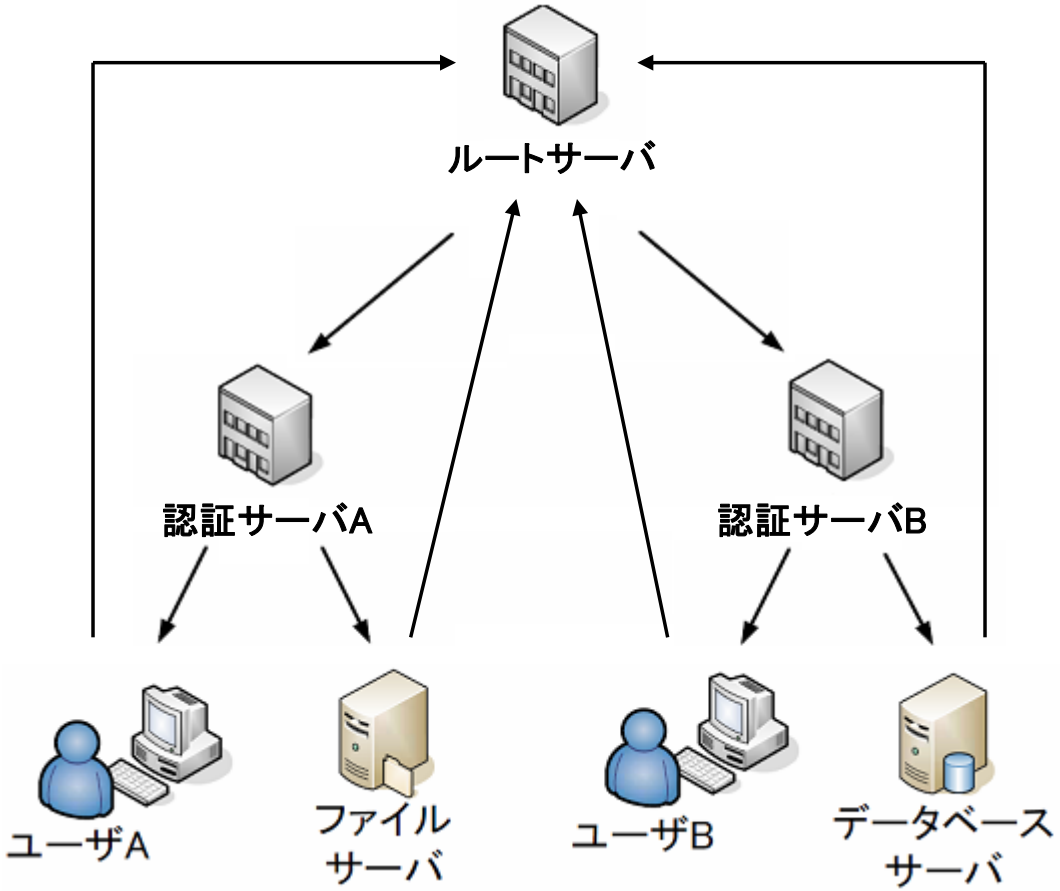
- 企業ネットワークでは以下のことが課題になると考えられる
  - 自己署名の公開鍵証明書を偽造可能
  - 失効情報の管理負荷が多い
  - 公開鍵証明書の状態について、必ずしも最新の情報とは限らない

提案方式

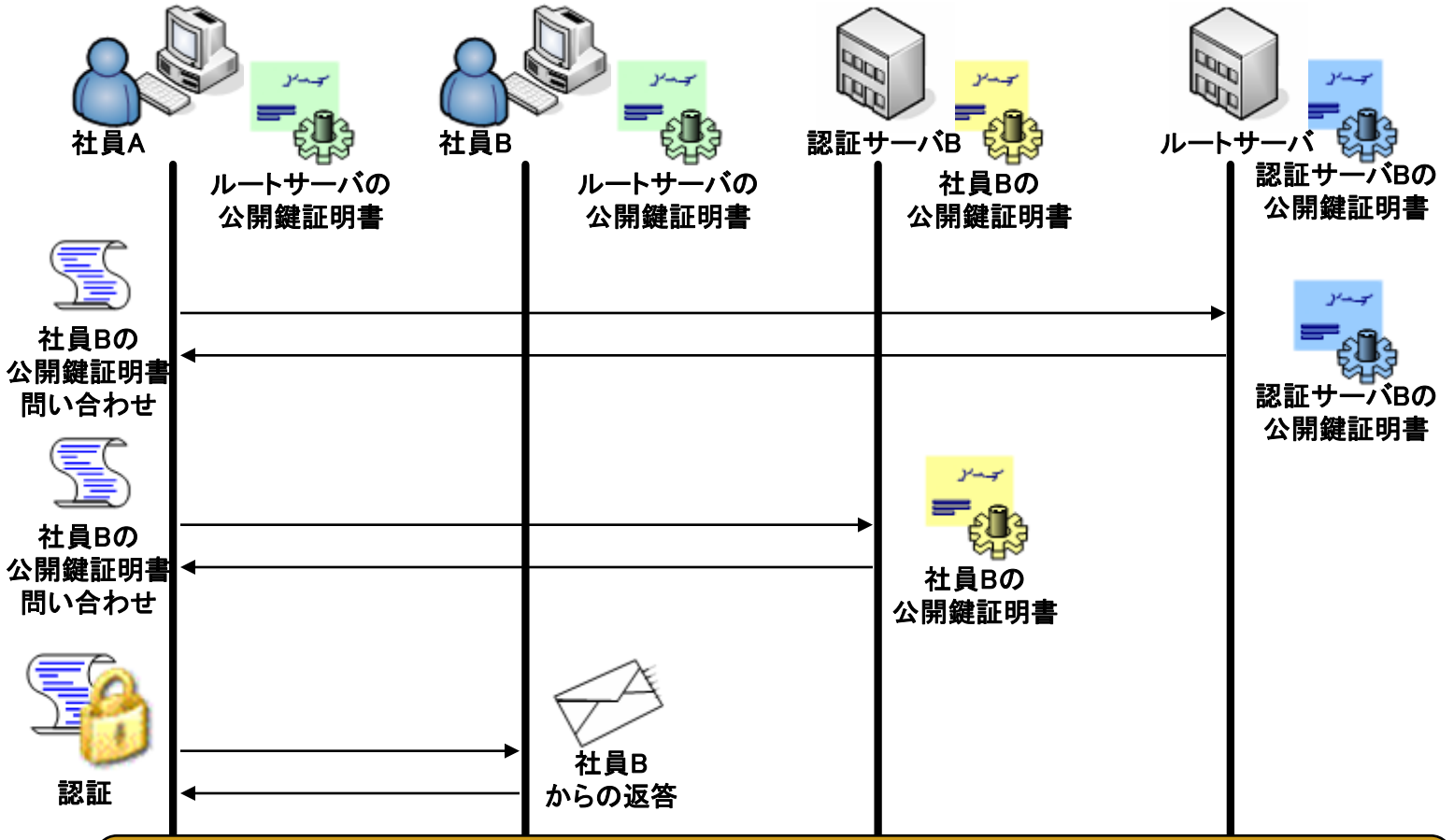
- 企業内ネットワークで利用できる認証システムASE(Authentication System for an Enterprise network)を提案する
  - 信頼関係を環状にする
  - 公開鍵証明書は発行者が保持し，自ら管理する
  - 信頼関係をオンデマンドで検証する

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



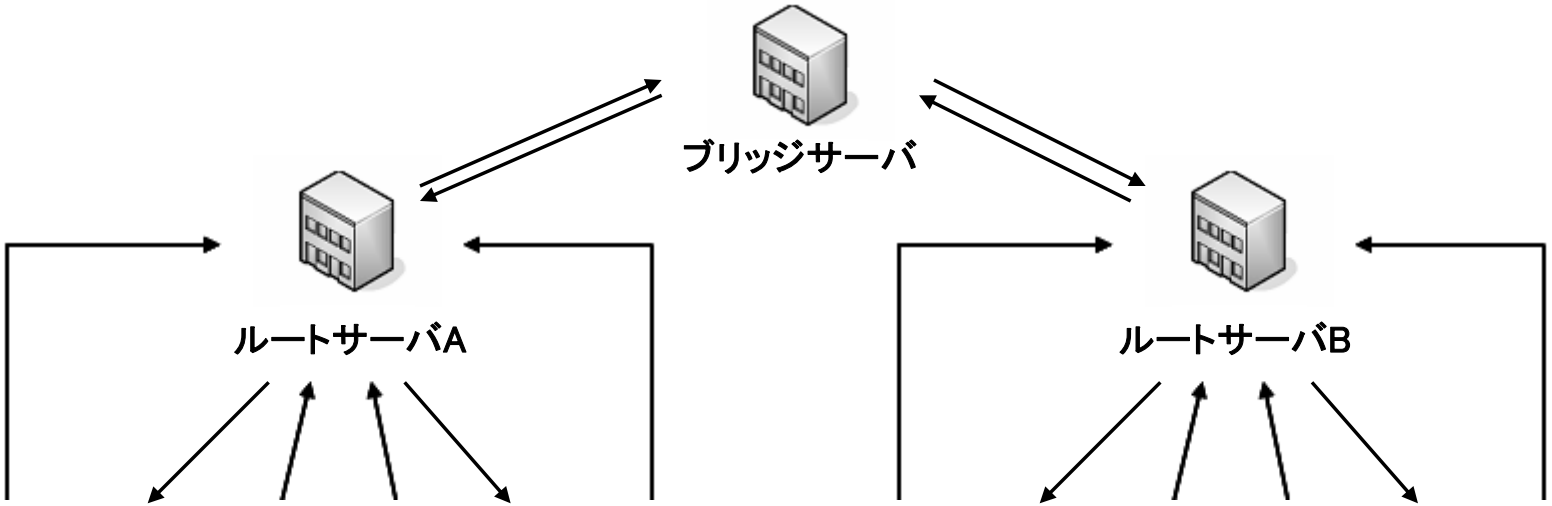
オンデマンド検証



リアルタイム性に優れている

負荷分散

- 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
- 全体の信頼関係を分割し，それらを繋ぐブリッジサーバを置くことで，負荷を分散できる



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 の実装と評価を行う