目次

概要 1
第 1 章　はじめに 2
第 2 章　PKI の課題 4
　第 2.1 節　root CA の公開鍵証明書の偽造 4
　第 2.2 節　失効情報の管理 5
第 3 章　提案方式 ASE 7
　第 3.1 節　概要 7
　第 3.2 節　信頼関係の環状化 8
　第 3.3 節　公開鍵証明書の管理方法 10
　第 3.4 節　公開鍵証明書の有効性検証 11
　第 3.5 節　ルートサーバの負荷分散 13
第 4 章　実装 14
第 5 章　評価 15
　第 5.1 節　性能評価 15
　第 5.2 節　PKI との比較 17
第 6 章　まとめ 18
謝辞 19
文献 20
研究実績 21

概要

企業ネットワークではサーバの確実な運用や社員同士の安全な通信が必須となっており，ユーザの確実な認証が重要な課題となっている．ユーザ認証には公開鍵認証基盤 PKI が注目されており，これを企業ネットワークに導入する試みがある．しかし PKI では root CA の公開鍵を偽造されると PKI の仕組みの前提が崩れてしまい認証基盤が成り立たなくなる. また, PKI では証明書の有効性を確認するために失効情報を利用する. 失効情報は管理が面倒なうえ, 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. 本稿ではこれら課題を解決するため，企業ネットワークに適した認証システム ASE(Authentication System for an Enterprise network)を提案する．ASE では，公開鍵証明書による信頼関係の構築を環状にする．また，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．ASE は，PKI に比べてセキュリティが高く，管理が容易でリアルタイム性の高い認証システムを提供できる．

第1章　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，否認といったネットワーク固有の脅威が存在する．これらの脅威を回避するために公開鍵暗号を用いたセキュリティ基盤 PKI（Public Key Infrastructure）が注目されている．PKI は公開鍵暗号方式の暗号化を利用してユーザに秘匿を提供し，署名を利用してユーザに認証，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 では，各ユーザやサーバの公開鍵を認証局（CA：Certificate Authority）が署名し公開鍵証明書を作成する．公開鍵証明書は現実社会における印鑑証明書や身分証明書に相当し，これを基にしてセキュリティの基盤を構築する．作成された公開鍵証明書を検証することにより公開鍵が正しい相手のものかを確認することができる．また，CA が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 が連携し検証対象の公開鍵証明書を確実に検証できるようにすることである．信頼関係の構築方法として，複数の CA を階層型（ツリー構造）に構成する階層型モデルが一般的である．階層型モデルでは，ユーザやサーバの公開鍵証明書は 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．各ユーザは最上位の root CA を信頼点とし，root CA の公開鍵証明書をあらかじめ安全な方法で取得し所持しておく．

階層型モデルは企業の業務形態と対応付けができる．例えば上記で説明した階層型モデルを企業の業務形態と対応づけると，root CA を社長，下位の CA を部長，ユーザを一般社員というように対応させることができる．社長は各部長について把握しており，部長は部下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導入しやすく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言える．

公開鍵証明書の有効性を検証するためには認証パスの構築と認証パスの検証が必要である．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において，署名内容が正しいか，有効期間が切れていないか，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．

認証パスの検証の中で実行される失効の確認方法には CRL（Certificate Revocation List）[1]モデルと OCSP（Online Certificate Status Protocol）[2]モデルがある．CRL モデルは CA が CRL を発行し，各ユーザは CRL に検証対象の公開鍵証明書が記載されていな

いことを確認する方法である. CA は CRL を定期的な周期で発行しリポジトリへ保存する．各ユーザは公開鍵証明書の検証をする前にあらかじめリポジトリから CRL を収集しておく必要がある．OCSP モデルは公開鍵証明書の検証時に公開鍵証明書の状態を集中管理する OCSP レスポンダに対しリアルタイムで確認する方法である．OCSP モデルでは公開鍵証明書を発行した CA は公開鍵証明書の失効情報を OCSP レスポンダに保存しておく．検証者は検証対象の公開鍵証明書を取得した後，OCSP レスポンダに対し公開鍵証明書の状態を問い合わせる．OCSP レスポンダは当該公開鍵証明書が失効していないか，失効情報との照合を行い，結果をユーザへ応答する．

PKI の信頼関係の構築と公開鍵証明書の検証方法では以下の様な課題がある．まず，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 の公開鍵証明書が偽造されてもそれを確認する術がない．次に，PKI では発行した公開鍵証明書を被発行者に手渡すのが原則であるため, 証明書の有効性を確認するために失効情報を利用し公開鍵証明書が失効していないかどうかを確認する必要がある．そのため，失効情報の管理が必須となる．PKI の管理は導入初期の管理と運用時の管理に分けられ失効情報の管理は運用時の管理に分類される. 運用時の管理は公開鍵証明書の管理が主な負荷になるが，失効情報の管理も軽視できない．また，失効情報の確認方法には CRL モデルと OCSP 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ある.

そこで本稿では，PKI を参考にして，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．ASE の特徴は，信頼関係の構築を環状にする．また公開鍵証明書は発行者が保持して自ら管理を行う．さらに信頼関係の検証はオンデマンドで行う．性能評価の結果，提案方式による処理時間は許容範囲であることを確認した.

以降，2 章で PKI の課題について述べ，3 章で ASE の原理と詳細について述べる．4 章で ASE の実装方式について述べ，5 章で評価について述べ，6 章でまとめる.

第2章　PKI の課題

第2.1節　root CA の公開鍵証明書の偽造

PKI では，最上位に位置する 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）するが，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. すなわち, root CA の公開鍵は偽造される可能性がある. Windows では root CA の公開鍵証明書がレジストリに保存されており，このレジストリを直接操作することにより書き換えが可能である．通常 root CA の公開鍵証明書をインストールしたり削除を行う場合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ため書き換えられたことに気づかない. また自己署名の公開鍵証明書は容易に作成することができる．即ち，ウィルスなど悪意あるプログラムによりレジストリを操作され公開鍵証明書を入れ替えれたり新たな公開鍵証明書を登録されてもユーザはそのことに気づかない可能性がある．

root CA の公開鍵証明書が偽造されると下記のように悪用される．即ち，悪意ある第三者が極秘データを取得する権限を持つユーザになりすまし，ユーザへ問い合わせる．問い合わせを受けたユーザは送られてきた公開鍵証明書で通信相手の検証を行うが, その検証は問題なく終了する．そこで，問い合わせを受けたユーザは極秘データを悪意ある第三者に渡してしまうことになる．

このように root CA の公開鍵証明書が偽造されると，PKI の仕組みの前提が崩れ重大な問題に発展する可能性がある．

第2.2節　失効情報の管理

次に PKI の管理負荷が大きい一つの要因として失効情報の管理があげられる．PKI で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．そのため，公開鍵証明書が失効していないかどうかを失効情報として別途管理する必要がある．CRL は失効情報の管理方法の一つであり失効情報のリストに失効情報管理者の CA が署名したものである．

図 1 に階層型モデルにおける公開鍵証明書検証に必要なデータを示す. 図 1 は root CA が CA_b に公開鍵証明書を発行し，CA_b がユーザ B に公開鍵証明書を発行し，ユーザ A が root CA を信頼点としてユーザ B に対する信頼関係の構築を行う場合において，ユーザ A がユーザ B の公開鍵証明書を検証するときに必要となるデータを示している．ユーザ B の公開鍵証明書はユーザ B 自身が持っているため，ユーザ B の公開鍵証明書を検証するためには CA_b から公開鍵証明書の失効情報を取得し, ユーザ B の公開鍵証明書が失効していないことを確認する必要がある．

失効情報は原則的に増加し続けるため管理が面倒であり, 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．失効情報の確認に CRL モデルを利用する場合は，検証者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ず，最新の情報が得られない場合がある．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．

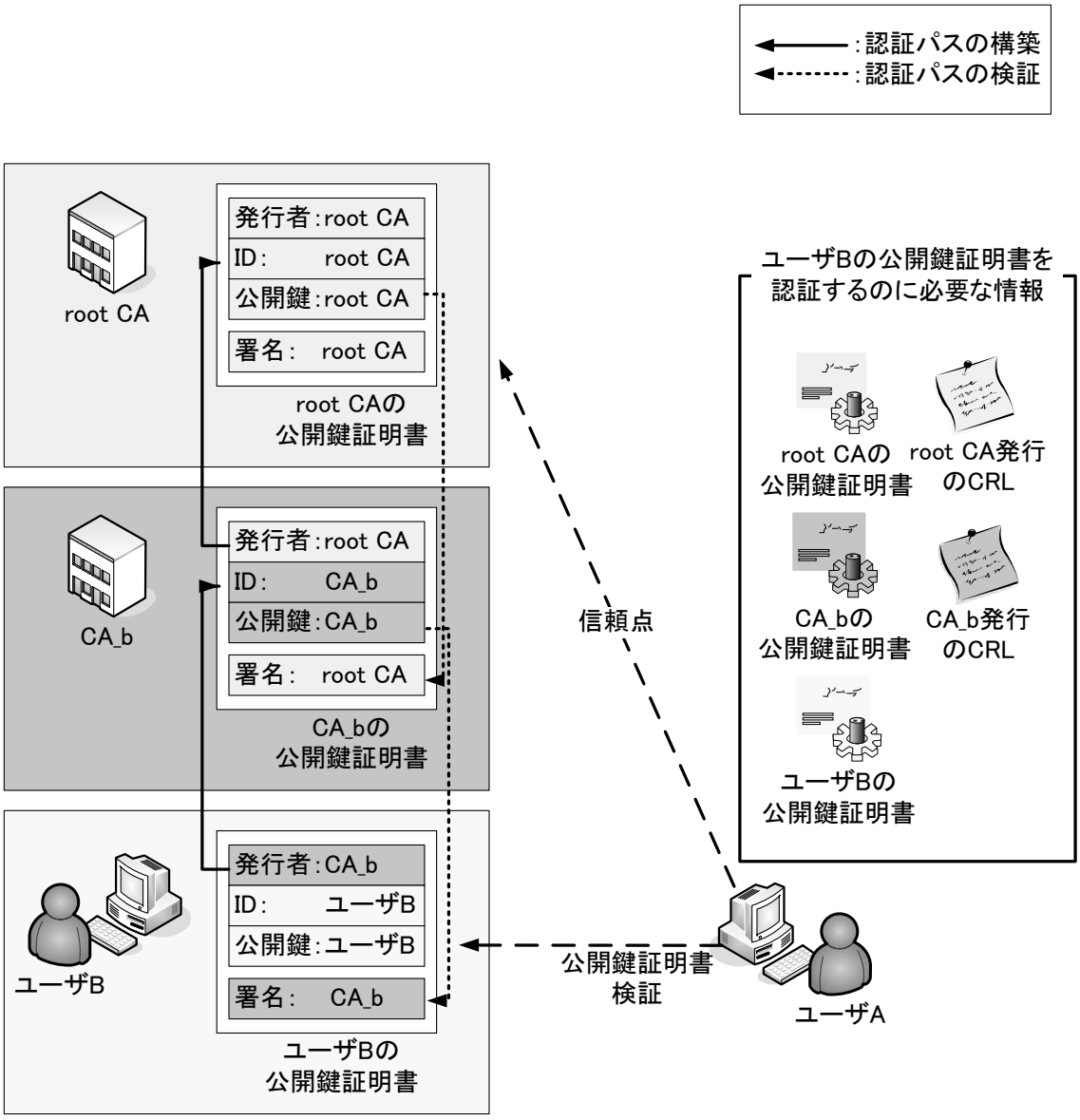

図 1　公開鍵証明書検証に必要なデータ

第3章　提案方式 ASE

第3.1節　概要

本稿では，企業内ネットワークに認証システムを導入することを想定し，PKI の課題を解決する ASE(Authentication System for an Enterprise network)を提案する．

ASE は以下の方法で実現する．まず PKI では信頼関係を root CA の公開鍵証明書を信頼点として階層的に構築するのに対し，ASE では信頼関係を環状に構築する．これにより，root CA の公開鍵証明書にも署名がなされることになり公開鍵証明書の偽造を検出できるようになる．次に PKI では公開鍵証明書が発行者の手を離れ，被発行者へ渡されるのに対し，ASE では発行者自らが保持/管理する．また，PKI では公開鍵証明書の有効性確認に失効情報を事前に入手するか問い合わせる必要があるのに対し，ASE では公開鍵証明書をオンデマンドで収集し，その時点で失効の有無を確認する．これらの方式により，失効情報の管理が不要となり，更にリアルタイム性の高い認証基盤を提供することが可能となる．

第3.2節　信頼関係の環状化

ASE の信頼関係を図 2 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や各サーバに公開鍵証明書を発行する. 各社員や各サーバ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構築することにより, 公開鍵証明書の検証時に自分を最上位に位置づけることができる. 公開鍵証明書の収集時に, 自分の持つ秘密鍵を信頼点とすることにより, 全ての公開鍵証明書が正しいことを検証できる. 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を検出できるようになり, 安全性が保証される.

ASE では検証者以外の社員の公開鍵証明書は発行者の公開鍵証明書として使用しないこととする. これは, 認証基盤に社員が加わると認証基盤のセキュリティ強度が落ちることを防止するためである. これにより, 社員の秘密鍵が悪意ある第三者に盗難され, 公開鍵証明書を発行されても, 検証時に盗難された社員の公開鍵証明書は発行者として扱わないので悪意ある第三者により作成された公開鍵証明書は認証されない.

公開鍵証明書の発行手順は以下のように行う. まずルートサーバは自身の公開鍵ペアおよび認証サーバの公開鍵ペアを作成する. ルートサーバは自身の秘密鍵で認証サーバの公開鍵証明書を作成し, 認証サーバへ認証サーバの公開鍵ペアとルートサーバの公開鍵をオフラインで手渡す. 認証サーバは社員の公開鍵ペアを作成する. 認証サーバは自身の秘密鍵で社員の公開鍵証明書を作成し, 社員の秘密鍵でルートサーバの公開鍵証明書を作成する. 認証サーバは社員へ社員の公開鍵ペアとルートサーバの公開鍵証明書をオフラインで手渡すことにより公開鍵証明書の発行を行う.

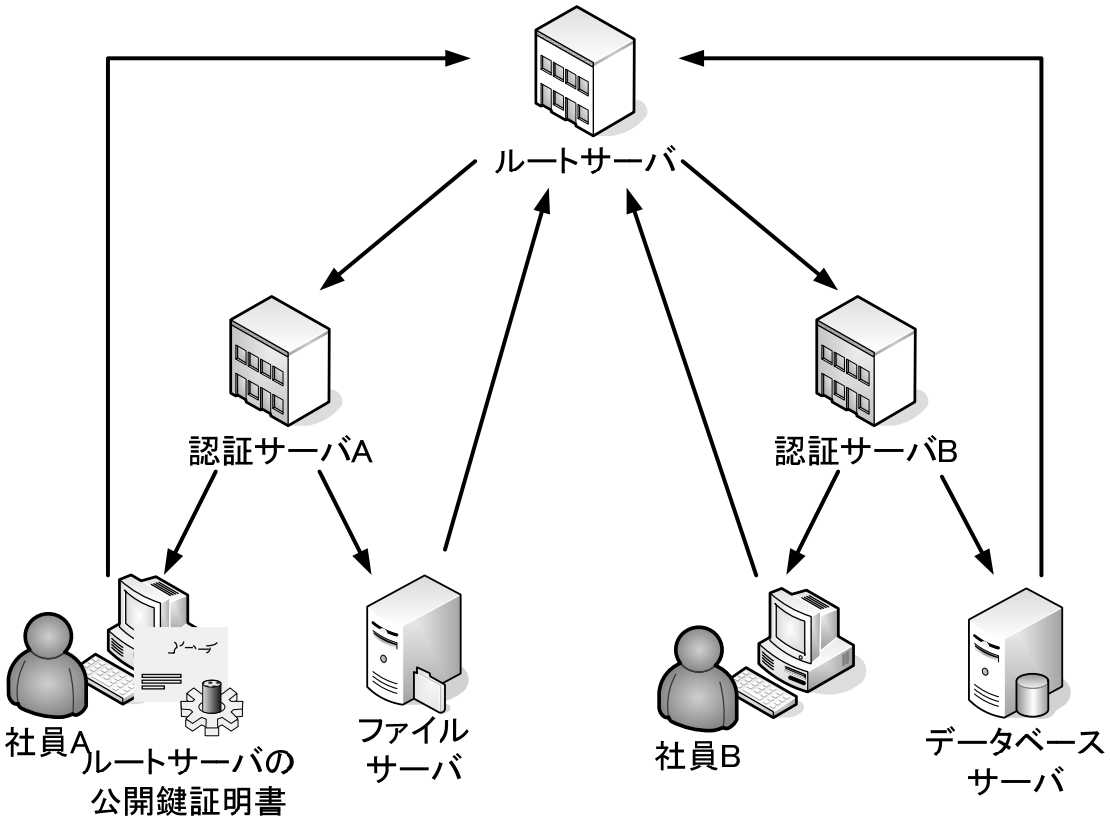
ルートサーバ
認証サーバA
認証サーバB
社員A
ルートサーバの
公開鍵証明書
ファイル
サーバ
社員B
データベース
サーバ

図 2　ASE の信頼関係

第3.3節　公開鍵証明書の管理方法

ASE の公開鍵証明書の管理方法を図 3 に示す. 図 3 は, 図 2 において社員 A が社員 B を認証する場合に必要となるデータを表示している. PKI では社員 B の公開鍵証明書を, 被発行者の社員 B 自体が保持/管理しているのに対し，ASE では社員 B の公開鍵証明書を発行者の認証サーバ B が保持/管理している．同様に認証サーバ B の公開鍵証明書は発行者のルートサーバが保持/管理し，ルートサーバの公開鍵証明書は発行者の社員 A が保持/管理する．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保持/管理する. 認証時には第 3.4 節に示すようにオンデマンドで必要となる公開鍵証明書をすべて収集するため, 管理方法をこのように改めても特に問題は発生しない. 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.

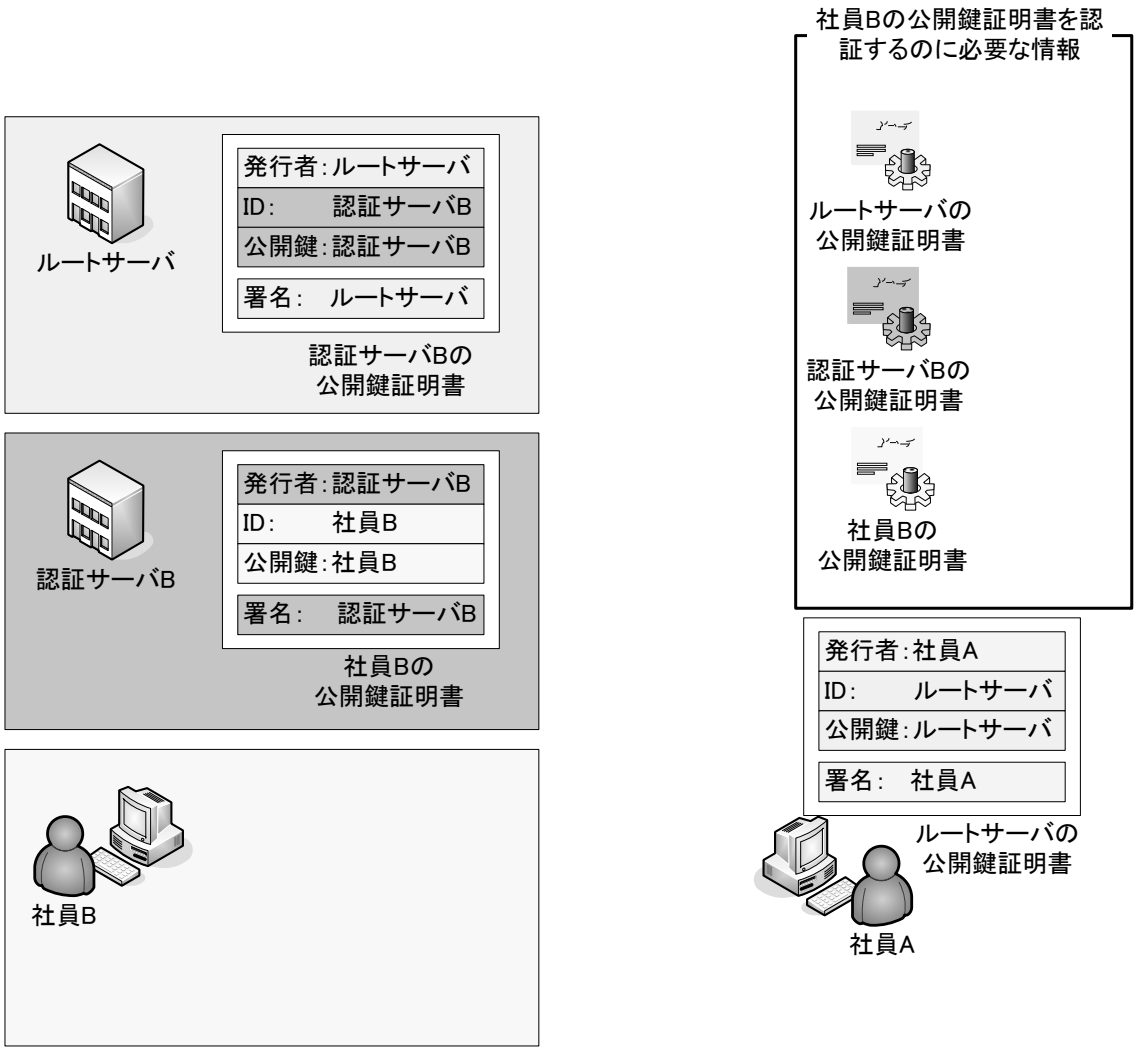

図 3　公開鍵証明書の管理方法

第3.4節　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方法を図 4 に示す. 公開鍵証明書の有効性検証に必要となる情報は，検証者が検証時にオンデマンドで収集する．具体的な検証方法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 の公開鍵証明書を応答する．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 の公開鍵証明書を応答する．

以上により認証パスの構築は終了し，認証パスの検証へ移る．認証パスの検証は社員 A の公開鍵でルートサーバの公開鍵証明書を検証し，ルートサーバの公開鍵証明書で認証サーバ B の公開鍵証明書を検証し，認証サーバ B の公開鍵証明書で社員 B の公開鍵証明書を検証し，すべての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．このように公開鍵証明書を発行者自身が保持/管理し，オンデマンドで公開鍵証明書を取得することにより，問い合わせた公開鍵証明書で最新の状態が確認できるため失効情報の確認作業は不要である．社員 B の認証のためには更に下記手順を実行する．

社員 A は共通鍵を作成した後社員 B の公開鍵で共通鍵を暗号化し，社員 B へ作成した暗号文を送る

社員 B は社員 B 自身の秘密鍵を利用し，暗号化された共通鍵を復号し，共通鍵を利用して社員 A へ共通鍵を取得したことを応答する

以後の通信には上記共通鍵を用いて暗号化通信が可能となる．

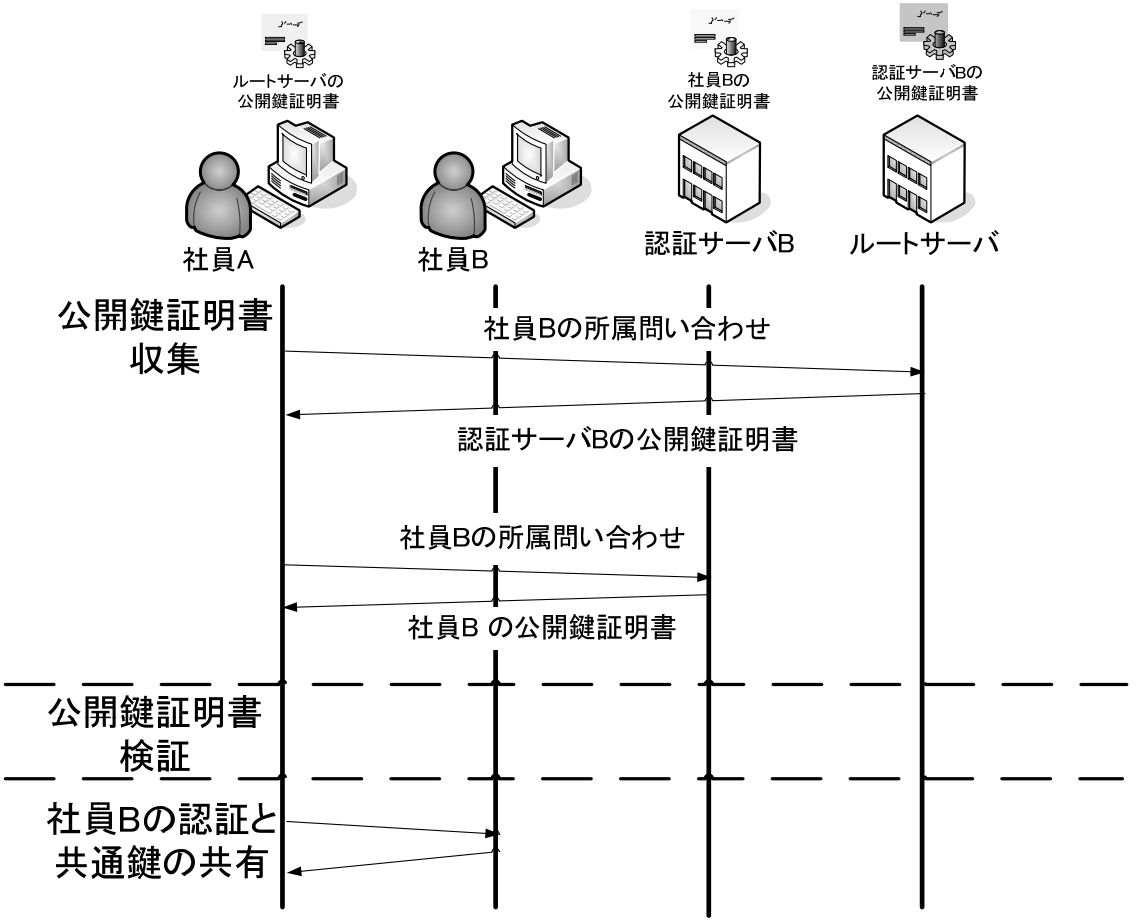

図 4　公開鍵証明書の有効性検証方法

第3.5節　ルートサーバの負荷分散

ASE は公開鍵証明書の検証時にすべてのユーザがルートサーバへ問い合わせを行う必要があり，ルートサーバへかかる負荷が多くなると考えられる．この課題を解決するためルートサーバは以下のような負荷分散を行う．

図 5 にブリッジサーバによるルートサーバの負荷分散方法を示す. ブリッジサーバとはルートサーバと相互認証を行い複数のルートサーバの橋渡しをするサーバである. 社員 A は公開鍵証明書検証時ルートサーバ A へ問い合わせる．ルートサーバ B 配下のユーザやサーバを検証するときはルートサーバ A からブリッジサーバを経由してルートサーバ B へ問い合わせる．このようにルートサーバが処理可能な社員数に分割することにより，負荷分散することができる．

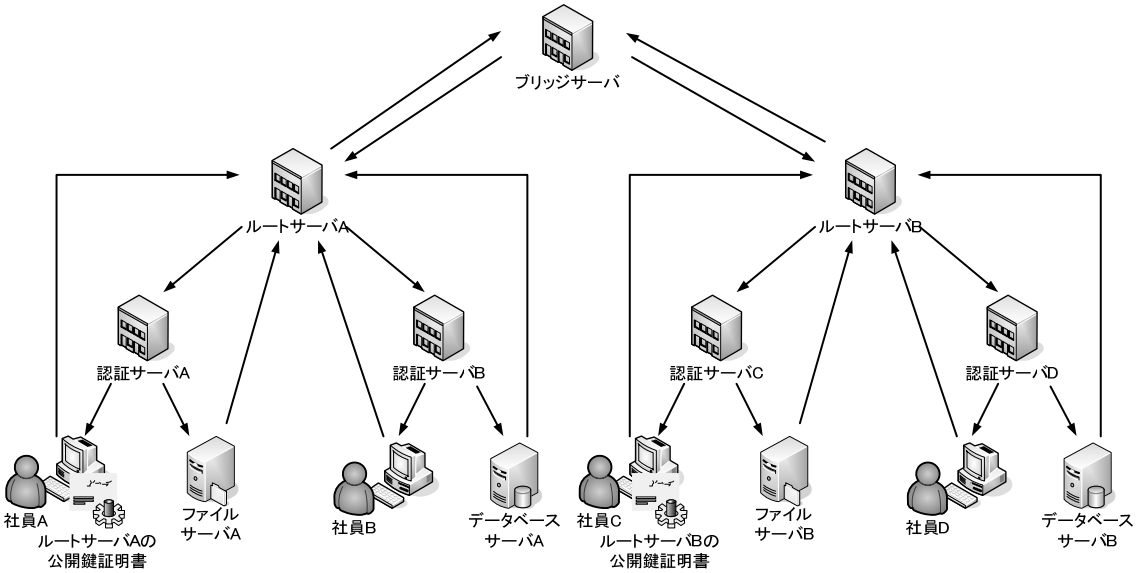

図 5　ルートサーバの負荷分散方法

第4章　実装

提案方式を検証するために社員端末用とサーバ用に ASE 対応のプログラムを実装した.

表 1 に ASE のプログラムを示す. 情報取得プログラムはサーバが公開鍵証明書の検索に必要となる被検証者情報と許可する検証の階層数を取得する処理を行う. 名前取得プログラムは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を行う. 送受信プログラムは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を行う. 検証プログラムは収集した公開鍵証明書を検証する処理を行う. 送受信プログラムと名前取得プログラムを複数回実行することにより階層化されたシステムにも対応できる.

公開鍵証明書検索応答プログラムは社員からの問い合わせを受け, それに対応する公開鍵証明書を検索し, 存在すれば公開鍵証明書を応答し, 存在しなければその旨を応答する.

今回は社員の検証プログラム以外の必要となるプログラムを作成した. 社員の検証プログラムはクライアントの証明書の検証プログラム[11]を利用した.

表 1　ASE のプログラム

プログラム名	実装	内容
情報取得プログラム	社員側	被検証者情報と許可する階層数を取得する
名前取得プログラム		問い合わせ先サーバの名前を取得する
送受信プログラム		サーバと情報の送受信をする
検証プログラム		収集した公開鍵証明書を検証する
公開鍵証明書 検索応答プログラム	サーバ側	社員の問い合わせを受け，受けた情報に対応する 公開鍵証明書を検索し，社員へ応答を行う

第5章　評価

第5.1節　性能評価

社員側とサーバ側で以下の時間を測定した．実験では，社員と認証サーバをそれぞれ 1 台だけの構成とし，公開鍵証明書の収集時間を測定した．

図 6 に認証サーバへの問い合わせから公開鍵証明書検証までの処理時間を示す．公開鍵証明書で利用する鍵サイズは 512Bits とした．処理時間は 100 回試行した平均の値で表 2 に装置仕様を示す．

測定の結果，社員側の問い合わせデータ作成処理に 0.1ms，送受信処理に 1.9ms，検証処理に 76.1ms の時間がかかった．サーバ側は 0.2ms の時間がかかった．今回使用した検証処理プログラムは PKI の公開鍵証明書の検証処理と同じ処理を行っているため，この時間は PKI の検証処理時間と同様である．

以上から社員側の処理時間は合計 78.1ms となり．PKI に必要となる検証処理時間 76.1ms と比較すると約 3%の増加である．PKI に比べて検証に必要となる処理時間の増加はわずかであると言える．

信頼関係が多階層になり複数の公開鍵証明書を検証する場合でも同じ処理を繰り返すため，検証に必要な階層の数を今回の処理時間に掛けるだけでよいと考えられる．

表 2　装置仕様

	社員	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	Fedora Core 5	Fedora Core 6
暗号化機能	Openssl 0.9.8a	

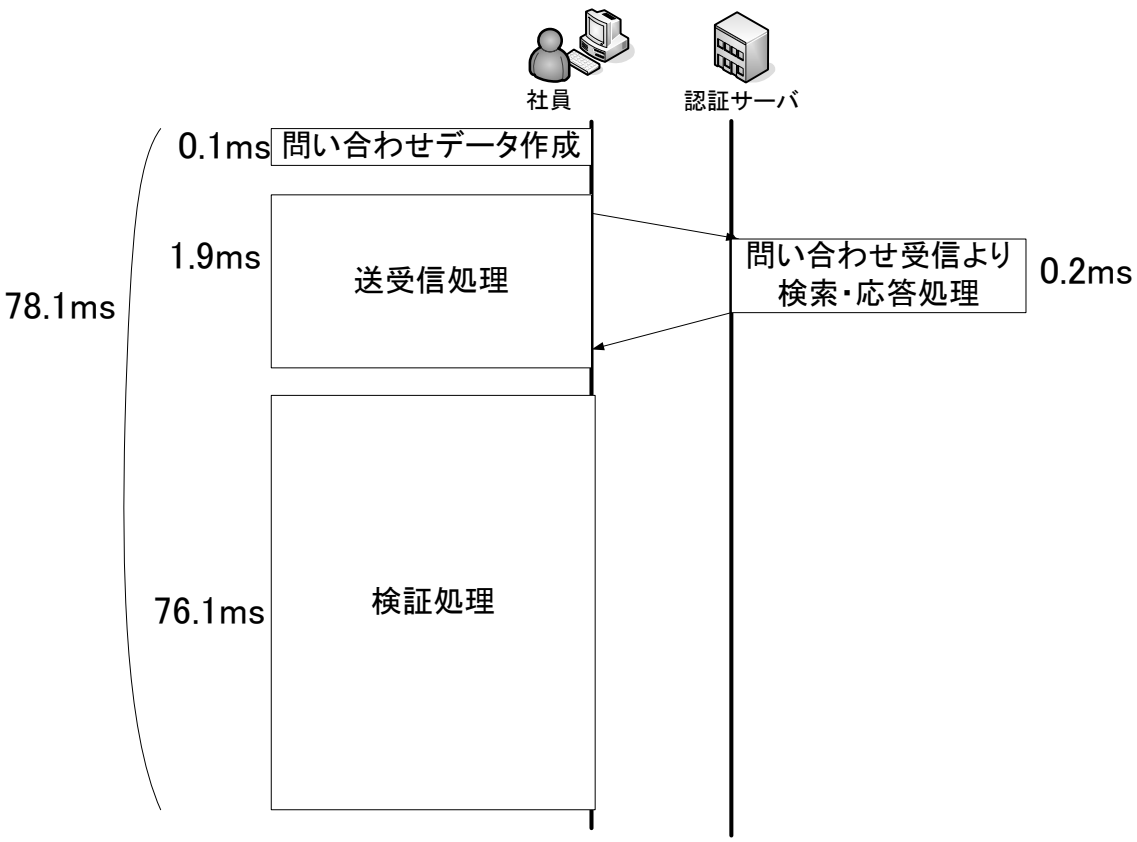
社員
認証サーバ
0.1ms
問い合わせデータ作成
1.9ms
送受信処理
78.1ms
問い合わせ受信より
検索・応答処理
0.2ms
76.1ms
検証処理

図 6　処理時間

第5.2節　PKI との比較

表 3 に PKI と ASE の比較を示す. PKI では root CA の公開鍵証明書が自己署名のため発行者が正当であることを検証できず，偽造されても検出ができない．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ため偽造が検出できる．

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. ASE 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．

管理負荷としては，導入初期と運用時の 2 種類を考える必要がある．導入初期において，ASE では各社員と各サーバから署名を行う分負荷が増える．しかし運用時においては，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くなると考えられる．これに対し, ASE は失効時は対象となる公開鍵証明書を削除するだけでよいため失効情報の管理を行う必要がなく管理負荷が軽減される．

表 3　PKI と ASE の比較

		PKI	ASE
セキュリティ		偽造検出不可能 ×	偽造検出可能 ○
リアルタイム性		△	○
管理負荷	導入初期	○	△
	運用時	△	○

第6章　まとめ

PKI では root CA の公開鍵証明書の偽造を検証できないという課題がある．また，失効情報の管理が面倒であり，最新の情報が得られない場合がある．そこで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認証システム ASE を提案した．評価結果より，ASE はセキュリティ面，管理負荷の面で優れ，性能も PKI と比較し問題ないことがわかった．そこで ASE は企業ネットワークにおける認証システムとしては有効な方式であると考えられる．

謝辞

本研究に関して, 研究の方向や進め方など終始御熱心なご指導と御教示を賜りました, 名城大学理工学部情報工学科　渡邊晃教授に心より厚く御礼申し上げます.

本研究を進めるにあたり, 研究内容に関して終始御熱心なご指導と御教示を賜りました，名城大学理工学部情報工学科　小川明教授に心より厚く御礼申し上げます.

本研究を進めるにあたり, 研究内容に関して終始御熱心なご指導と御教示を賜りました，名城大学理工学部情報工学科　柳田康幸教授に心より厚く御礼申し上げます.

本研究を進めるにあたり, 研究内容に関して終始御熱心なご指導と御教示を賜りました，名城大学理工学部情報工学科　宇佐見庄五講師に心より厚く御礼申し上げます.

最後に，本研究を行うにあたり，有益なご助言，適切なご検討をいただいた，名城大学理工学部情報科学科渡邊研究室の皆様に心より感謝いたします.

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, P. Cain, D. Pinkas, R. Zuccherato, “Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)”, RFC 3161, August 2001

[4] C. Adams, S. Farrell, “Internet X.509 Public Key Infrastructure Certificate Management Protocols” , RFC 2510, March 1999.

[5] M. Myers, C. Adams, D. Solo, D. Kemp, “Internet X.509 Certificate Request Message Format” , RFC 2511, March 1999.

[6] J. Ross, D. Pinkas, N. Pope, “Electronic Signature Policies” , RFC 3125, September 2001.

[7] 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.

[8] 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.

[9] 菊池 浩明, 中西 祥八郎, “オンライン証明書検証プロトコルのスケーラビリティ”, 情報処理学会論文誌，2002 年 8 月

[10] 田中 直樹，飯野 陽一郎，“PKI の証明書失効に必要な通信量の確率論的評価”，情報処理学会論文誌，2004 年 12 月

[11] 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-”，オーム社，2004 年 8 月

[12] 村山 公保，“基礎からわかる TCP/IP ネットワーク実験プログラミング第 2 版”，オーム社，2004 年 10 月

研究実績

1.学術論文

なし

2.国際学会

なし

3.口頭発表

[1] 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の構築に関する研究”，電気関係学会東海支部連合大会，Sep.2004.

[2] 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の構築に関する研究”，第 67 回情報処理学会全国大会，Mar.2005.

[3] 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”，DICOMO2005 シンポジウム論文集，Vol.2005，No.6，pp.93-96，Jul.2005.

[4] 坂野文男，保母雅敏，渡邊晃，“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”，SCIS2006 予稿集，Jan.2006.