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

坂野　文男

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）は様々な用途で利用されている．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．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．

Researches on the architecture of authentication infrastructure in an enterprise network

Fumio Banno

PKI(Public Key Infrastructure) that is the base of security by the public key cryptosystem is used by various usages. It pays attention to the advantage, and it tends to introduce the attestation base by PKI on a corporate network. Then, it is considered what problem you are in the introduction of the enterprise of PKI in this text, and, on the other hand, proposes the expression about the attestation base to solve the problem.

１．　はじめに

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．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，否認といった脅威がある．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．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，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

２．１　信頼関係の構築

認証局(CA：Certificate Authority)は公開鍵証明書を他の CA に発行することにより信頼関係を構築することができる.信頼関係の構築にはいろいろなモデルがあるが，例として図 1 に階層型モデルによる信頼関係の構築を示す.階層型モデルとは複数の CA を階層型(ツリー構造) に構成する方式である．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．そしてユーザは最上位の CA(root CA)を信頼点とし，公開鍵証明書を所持しておく.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 CA のことである.

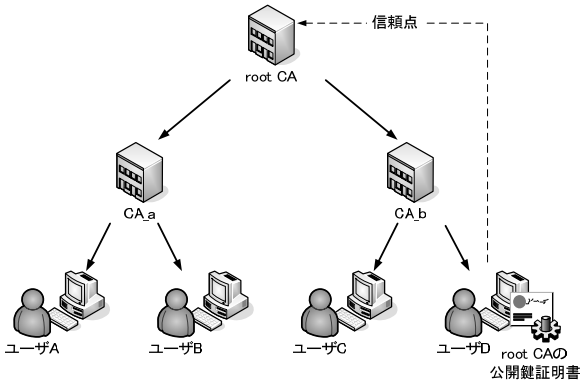

図 1　階層型モデルによる信頼関係の構築

２．２　公開鍵証明書の有効性検証

公開鍵証明書の有効性検証について説明する.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対象となる公開鍵証明書から信頼点までの公開鍵証明書を収集し，対象となる公開鍵が信頼点と関係あることを確認する.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時の処理を図 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.

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番の逆から行う.よって 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.

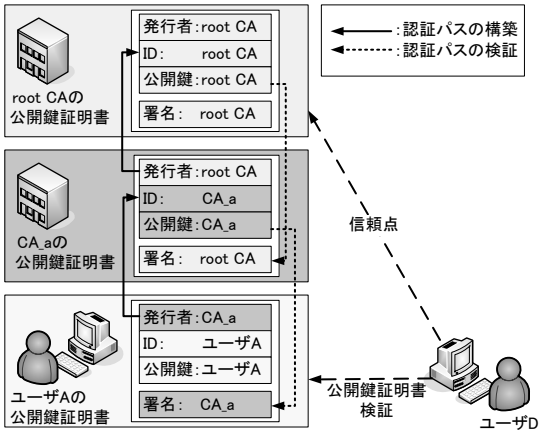

図 2　公開鍵証明書の有効性検証

２．３　公開鍵証明書の失効情報

認証パスの検証には公開鍵証明書が失効されていないか確認が必要だが，確認するために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 CRL（Certificate Revocation List）モデルと OCSP（Online Certificate Status Protocol）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を行う．そして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．各ユーザは公開鍵証明書の検証時に事前に取得した CRL に検証対象の公開鍵証明書が記載されていないかを確認することにより失効を確認する．

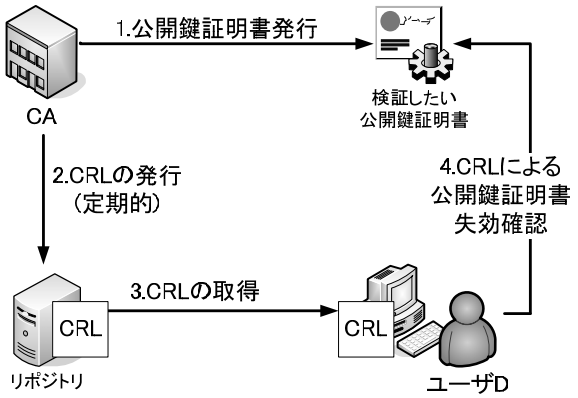

図 3　CRL モデルの概要

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，回答により公開鍵証明書の状態を確認する．

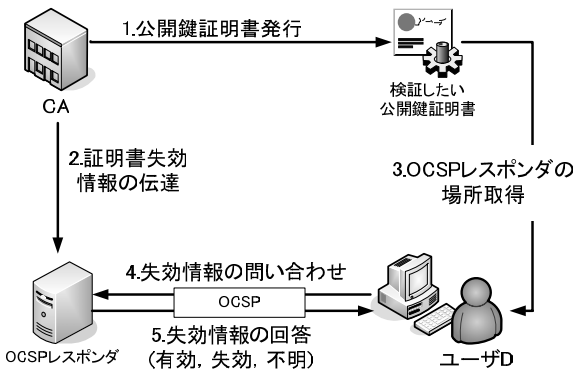

図 4　OCSP モデルの概要

２．４　PKI の課題

ここまで PKI について説明してきたが，PKI には以下のような課題がある．

まず，ユーザの公開鍵証明書は認証局 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．しかし，最上位の 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．

次に，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．

次に失効情報の確認に 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 を取得しておく必要があり，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，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．　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．提案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とにより，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できる．

提案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．

(1) 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

(2) 認証サーバが各部門の社員に公開鍵証明書を発行する

(3) 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.

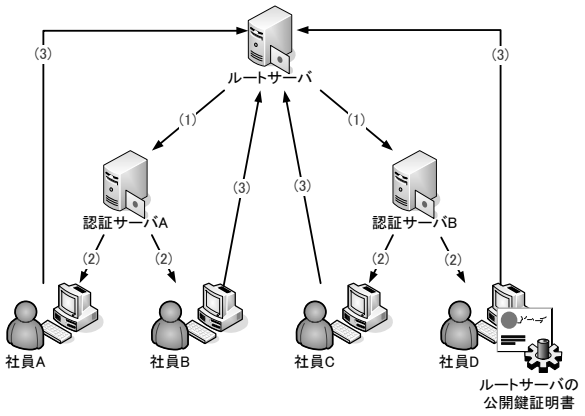

図 5　提案方式の信頼関係

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.

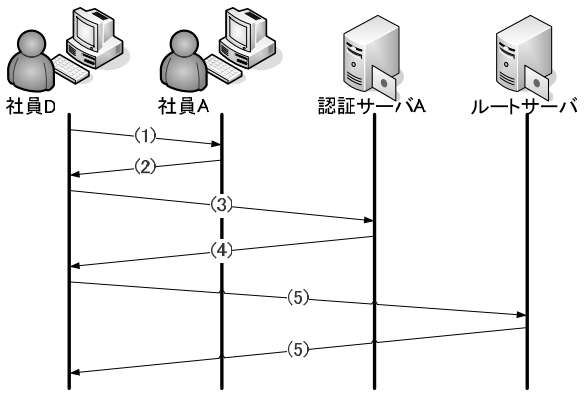

図 6　認証パスの構築の流れ

例として図5で社員Dが社員Aを認証する場合の認証パスの構築の流れを図6に示す.

(1) 社員 D は社員 A を認証するため, 社員 A に対し社員 A の ID 情報と公開鍵証明書の所有者を問い合わせる

(2) 社員 A は ID 情報と自分の公開鍵証明書の管理者（認証サーバ A）の ID 情報を社員 D へ返答する

(3) 社員Dは認証サーバAに対し社員Aの公開鍵証明書を要求するとともに認証サーバ A の公開鍵証明書の管理者を問い合わせる

(4) 認証サーバAは社員Aの公開鍵証明書が有効であれば,社員 A の公開鍵証明書及び認証サーバ A の公開鍵証明書の管理者（ルートサーバ）の ID 情報を社員 D へ返答する

(5) (3)と(4)の処理を社員 D とルートサーバ間で行う

社員 D はルートサーバの公開鍵証明書を所持しているためこれで認証パスの構築は終了し, 認証パスの検証へ移る. 即ち, 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Dは社員Aを認証することができる.

しかし社員 D が社員 A を認証する場合の(4)で公開鍵証明書をそのまま社員 D へ返答する場合, 図 7 にある偽造方法が考えられる.

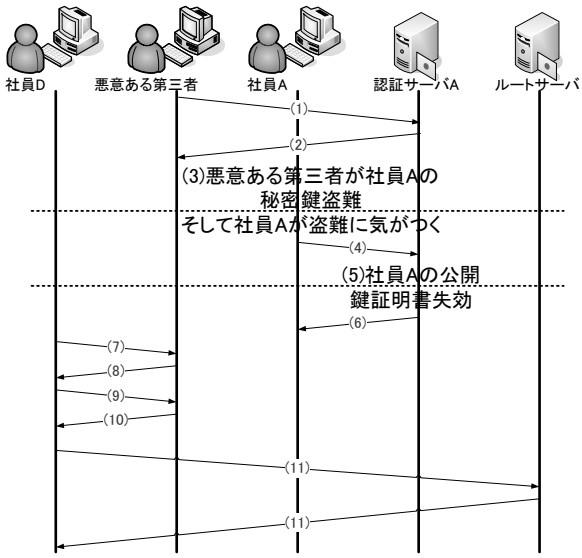

図 7　認証時の偽造

(1) 悪意ある第三者が社員 A の公開鍵証明書を認証サーバ A に要求する
(2) 認証サーバ A は社員 A の公開鍵証明書が有効なため悪意ある第三者に有効なときの情報を返答する
(3) 悪意ある第三者は社員 A の公開鍵証明書を盗難し，社員 A が盗難に気がづく
(4) 社員 A は認証サーバ A へ秘密鍵が漏洩したことを通知する
(5) 認証サーバ A は社員 A の公開鍵証明書を失効する
(6) 認証サーバ A は社員 A へ公開鍵証明書を失効したことを通知する
(7) 社員 D は社員 A を認証するため，社員 A に問い合わせるが，悪意ある第三者が通信を奪う
(8) 悪意ある第三者は社員 A の ID 情報と社員 A の公開鍵証明書の管理者の ID 情報を社員 D へ返答する
(9) 社員 D は認証サーバ A に問い合わせるが悪意ある第三者が通信を奪う
(10) 悪意ある第三者は(2)で手に入れた情報を社員 D へ返答する
(11) 社員 D はルートサーバと通信を行い認証パスの構築を行う

このようにして悪意ある第三者は盗難した秘密鍵に対応する公開鍵証明書を認証させることが可能である．

そこで提案方式ではノンス（nonce）を利用する．ノンスというのは乱数のことである．この nonce を公開鍵証明書の要求問い合わせに付け加え，公開鍵証明書の返答には要求時の nonce を付け加え署名行うこととする．これにより前もって取得した公開鍵証明書では nonce の値が違うため偽造を発見することができる．例として図 6 の(3)と(4)の公開鍵証明書の要求と返答を図 8 に示す．

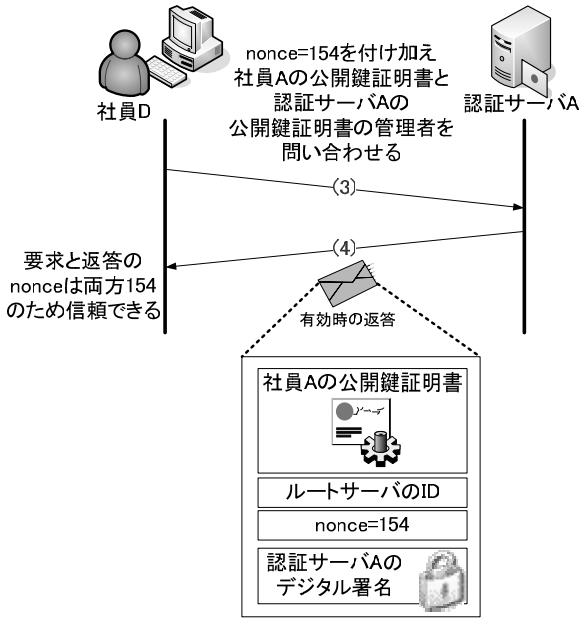

図 8　公開鍵証明書の要求と返答

4．　評価

PKI と本提案の相違点を表 1 に示し，PKI(CRL)，PKI（OCSP）と本提案の比較を表 2 に示す．

PKI（CRL）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．

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．しかし，PKI（OCSP）は公開鍵証明書のみでなく OCSP からの有効性の回答も検証する必要があるためクライアントの負荷が大きくなる．また両方式とも失効情報の管理が必要である．

提案方式では，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．

表 1　PKI と提案方式の相違点

	PKI	提案方式
信頼関係	階層	環状
検証の最上位	root　CA	自分
所持する公開鍵証明書	上位層が署名した自分の公開鍵証明書	自分が発行した下位層の公開鍵証明書

表 2　PKI と提案方式の比較

	PKI (CRL)	PKI (OCSP)	提案方式
リアルタイム性	△	○	◎
クライアント負荷	○	△	○
管理コスト	△	△	○
初期遅延	○	○	△

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．

参考文献

[1] M. Wahl, T. Howes, S. Kille, “Lightweight Directory Access Protocol (v3)” , RFC 2251, December 1997.

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

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

[4] 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.

[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] R. Housley, W. Polk, W. Ford, D. Solo, “Internet X.509 Public Key Infrastructure Certificate and CRL Profile” , RFC 3280, 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] 坂本憲広，“公開鍵証明書を用いた国立大学病院保健医療情報利用者認証システムの開発”，電子情報通信学会論文誌 (D-I), VOL.J84-D-I, No.6, pp.830-839, June 2001.

[10] 藤城孝宏，鍛忠司，羽根慎吾，熊谷洋子，手塚悟，“証明書検証サービスの開発”，電子情報通信学会論文誌 (D-I), VOL.J87-D-I, No.8, pp.833-840, August 2004.

[11] 榊原裕之，吉武淳，“公開鍵証明証の検証法式の考察”，情報処理学会研究報告−コンピュータセキュリティ，Vol.1998, No.054, pp.53-58, 1998

[12] 菊池浩明，“Catbell　WWW における公開鍵証明書に基づくユーザ認証”，情報処理学会研究報告−マルチメディア通信と分散処理，Vol.1996, No.012, pp.233-238, 1996

[13] 山崎重一郎，荒木啓二郎，“信用情報と利用ポリシの管理が可能な相互認証を実現する認証基盤の提案”，情報処理学会論文誌，Vol.40, No.01, pp.296-309, 1999

[14] 齋藤孝道，萩谷昌己，溝口文雄，“公開鍵を用いた認証プロトコルについて”，情報処理学会論文誌，Vol.42, No.08, pp.2040-2048, 2001

[15] 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，Vol.43, No.08, pp.2659-2664, 2002

[16] 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，Vol.45, No.12, pp.2824-2833, 2004

[17] 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/

[18] 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

付　録

A.　共通鍵暗号と公開鍵暗号

暗号には共通鍵暗号方式と公開鍵暗号方式がある.

共通鍵暗号方式とは暗号化と復号で同じ鍵を使う暗号方式である(図 9). 共通鍵暗号方式は扱いが簡単であり, 処理速度が速いという利点があるが, 相手先ごとに固有の鍵を作成しなければならない. また鍵はあらかじめ安全な方法で相手に渡さなければならない. そのため, 限られた特定の相手とのやり取りに向いているが, 通信相手が複数の場合や, 鍵を安全な方法で渡すことができない場合には向いていない.

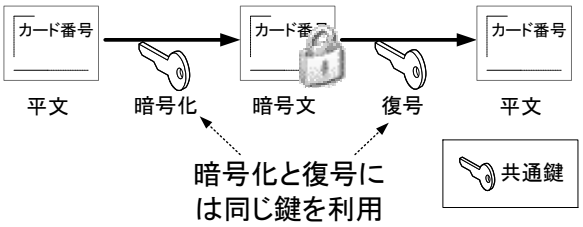

図 9　共通鍵暗号方式の暗号化と復号

公開鍵暗号方式とは, 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であり, 非対称暗号とも呼ばれる. 片方の鍵は他人に公開するため公開鍵と呼ばれ, もう片方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(図 10). 公開鍵で暗号化されたデータは対応する秘密鍵でないと復号することができない(図 11). また, 秘密鍵で暗号化されたデータは対応する公開鍵でないと復号することができない.

鍵ペア（公開鍵と秘密鍵）は, どちらの鍵を暗号化に使うかによって用途と意味が変わる. 第三者にデータの内容をわからなくする暗号に使う場合は通信相手の公開鍵を使用し, データの正当性を保証するデジタル署名として使う場合は自分の秘密鍵を使用する.

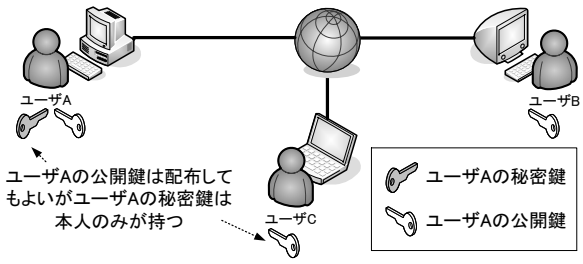

図 10　公開鍵と秘密鍵の所持

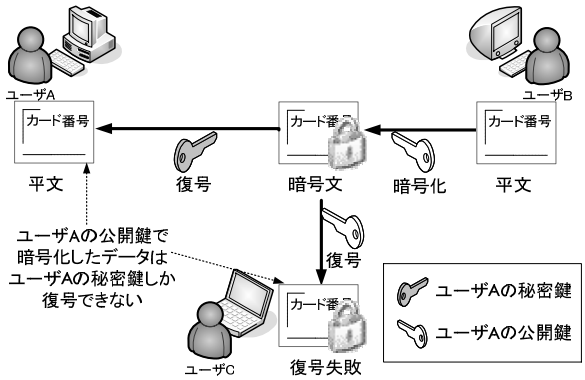

図 11　公開鍵暗号方式の暗号化と復号

B.　公開鍵暗号方式の問題点

PKI では公開鍵暗号方式を利用されている.

公開鍵暗号方式は共通鍵暗号方式と比べ, 鍵を安全な方法で渡す必要がない. しかし公開鍵暗号方式も鍵の配布時に問題が存在する. 図 12 はユーザ A がユーザ B へ公開鍵を配布時するときの問題を表した図である. ユーザ A はユーザ A の公開鍵を送るが, 通信路の途中でユーザ C がユーザ A の公開鍵をユーザ C の公開鍵と置き換えて送信する. ユーザ B は置き換えられたことがわからないため, 受け取ったユーザ C の公開鍵をユーザ A の公開鍵と勘違いする. そのため受け取った公開鍵でデータの暗号化を行うと第三者であるユーザ C にデータを見られてしまう.

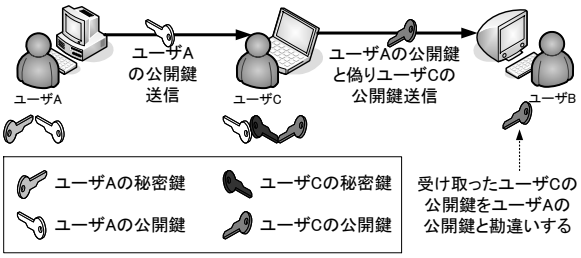

図 12　公開鍵配布時の問題

C．　公開鍵証明書

公開鍵の問題を解決するために公開鍵所有者を確認する方法が必要になる.そこで公開鍵の所有者を保証する公開鍵証明書がある.公開鍵証明書とは認証局(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である. 公開鍵証明書の内容を図 13 に示す.公開鍵証明書は被発行者の情報と被発行者が利用する公開鍵に発行者がデジタル署名を行う.そして公開鍵を利用したい場合,公開鍵証明書の有効性を検証し公開鍵の所有者を確認することができる.

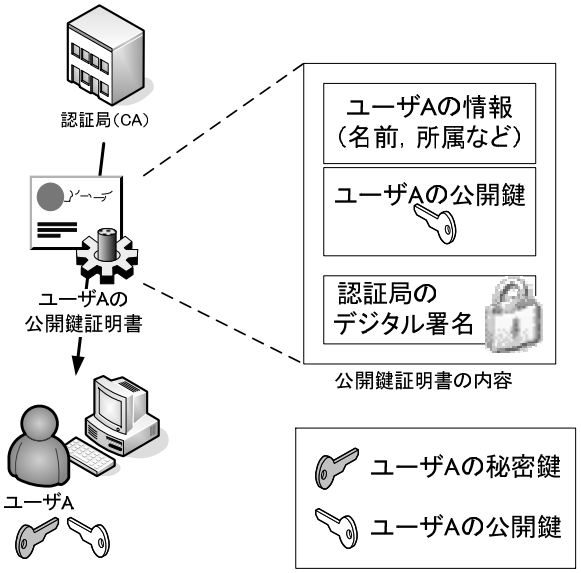

図 13　公開鍵証明書の内容