マルチメディア通信と分散処理　97－6
コンピュータセキュリティ　8－6
（2000．3．21）

ＣＡ連携実現における課題およびその解決方策

今枝直彦　村田祐一　竹内宏典
ＮＴＴ情報流通プラットフォーム研究所

EDI・ECを安全に実現するためには、CAを用いた電子認証が必要となるが、広い取引範囲を扱うためには複数CA間の相互認証あるいは階層認証によるCA連携が必須となる。しかし、既存のCA連携技術をEDI・ECに適用するにあたっては、アクセス制限により他CAへのアクセスができないといったことや、CRL発行間隔が異なっていることにより公開鍵証明書の有効性確認の信頼性が低下するという問題点があった。また、CA連携技術は、簡易なコミュニケーション系業務だけではなく、EDI・ECにおけるリアルタイム系業務にも適用できなければならない。本稿では、上記課題を解決するとともに、リアルタイム系業務にも適用可能な“CAが公開鍵証明書とともに、更新日時をディレクトリに掲載する”ことを特徴とする方式を提案する。

A method to solve the subjects for interoperability between CAs

Naohiko IMAEDA　Yuichi MURATA　Hironori TAKEUCHI
NTT Information Sharing Platform Laboratories

This paper proposes a method of confirming the validity of certificates in an environment where multiple Certification Authorities (CAs) exist and the reliability of the confirmation is strictly required, such as in EDI or EC environment. A directory system is used for confirming certificates issued by different CAs as a common access point, and could hide differences in CA's access policy. The date of update made by each CA to the directory system is stored in the directory system for confirmation, which is effective when CRL issue intervals are different among CAs.

1．はじめに

EDI（Electronic Data Interchange）・EC（Electronic Commerce）を実現するためには、通信ネットワーク上でのユーザ認証が必須であり、その実現方法の１つとして、公開鍵暗号におけるディジタル署名とCA（Certification Authority）を利用したユーザ認証がある。また、現実社会の企業構造、企業間取引構造、対消費者取引を観察してみると、現実社会の取引範囲は非常に大きなものであり、この幅広い取引範囲を電子社会に置き換えた時、１つのCAにすべてのユーザが登録している状況というのは考えにくい。そのため、CAを利用したユーザ認証を用いてEDI・ECを実現するためには、各CAがお互いの公開鍵を認証し合う相互認証、あるいは、上位CAが下位CAを認証し、この上位CAが下位CAを認証する認証プロセスが集まることにより階層構造を形成する階層認証が必要になる。そして、この２つの認証方式により異なるCAが発行した公開鍵証明書を相互流通させるCA連携が必須となる。

しかし、今までにCA連携を行いEDIやECを行ったという実例はほとんどない。1998年７月にシンガポール政府とカナダ政府が主導で行ったG(Gevernment) to GのCA連携は存在するものの[1]、それに続くCA連携の実例はなく、ICAT実証実験（1998年９月終了）[2]，JapanNetと米国CommerceNet（1998年８月終了）[3]、ノルウェーUNINETT（現在実験中）[4]など未だ実

験レベルにとどまっている。

そこで本稿では、CA 連携を行う上での課題を分類・整理し、各検討団体における検討（標準化）の動向との比較を行うことにより、EDI・EC への CA 連携の適用に向けた課題を抽出した後に、抽出した課題に対して、EDI・EC への CA 連携に適用できるとともに、リアルタイム系業務にもコミュニケーション系業務にも適用できる“CA が公開鍵証明書とともに、更新日時をディレクトリに掲載する”ことを特徴とする方式を提案する。

2. CA 連携を行う上での課題

CA 連携を考慮するにあたり、CA 連携を行うための課題を、世の中の CA 連携関連の文献から抽出・分類・整理したものが図１である。

CA 連携を行うための課題には大きく分類して４種が存在する。

１－技術（接続）的課題

：CA 連携を行う上における技術的な課題。ここであげられる課題を解決することにより物理的な CA 間接続を行うことができる。具体的には、公開鍵証明書/CRL(Certificate Revocation List)フォーマット、DN(DistinguishedName)の表記法、公開鍵証明書管理状態（有効な公開鍵証明書のみ管理、あるいは、保留された公開鍵証明書も管理）などがこれにあたる。

２－運用的課題

：技術面の課題がクリアされた後に生じる課題であり、実際に CA 連携を行う上において両者の運営面でのハーモナイゼーションをとるための課題である。具体的には、CRL 更新タイミング、CA のセキュリティレベルなど Certificate Policy（CA がサービスを提供する上で公開鍵証明書ユーザに開示する方針/規定/基準）に関する事柄が含まれる。

３－方式的課題

：技術面、運用面での課題がクリアされた後に、現実社会での取引を電子社会に置き換えた時に、その取引を CA 連携を用いてどのような方式で実現するかといった課題である。具体的には、公開鍵証明書取得方法、公開鍵証明書有効性確認方法などがこれにあたる。

４－法制度課題

：CA 連携を行うにあたり、各 CA ドメイン(利用者に対し各 CA が公開鍵証明書を発行している空間)に登録するユーザが不利益を被った場合に、その責任は誰にあるのか、あるいはその電子署名に効力はあるのか、などを明確にするなどの法制度的な課題である。

3. 検討（標準化）の動向

実社会において CA 連携を行うためには、前述の４種の課題をクリアしていく必要があり、各検討団体においても４つの課題について取り組みを見せている。

１）APEC PKI Interoperability Expert Group

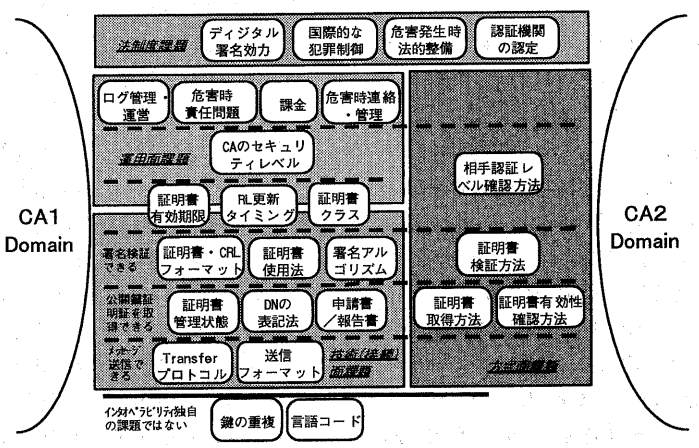


図１　CA 連携を行うための課題

[5]
：技術面の課題に関して検討
→PKIX や PKCS などで標準化が進められている
運用面の課題に関しても検討
→CertificatePolicy のハーモナイゼーションが複雑であり、ここに問題があるとし、Cross-Recognition なる新たな CA 連携方法を提案

2）ECOM “企業間電子商取引における認証･公証適用の考え方” [6]
：運用面の課題に関して検討
→CA 連携を行う団体が新規に共通 CertificatePolicy を作成する。あるいは、PKIX の RFC2527 で相互認証あるいは認証ポリシーの検証を目的に認証ポリシーの規定形式を標準の型として提供しているため、この RFC2527 に従って Certificate Policy が記述されているかを確認する

3）NIST “MISPC（PKI 要素における最低限のインタオペラビリティ仕様）” [7] および NIST “F-PKI 技術仕様書” [8]
：技術面と運用面、方式面（署名アルゴリズムの違いによる検証方法）に関して検討
→F-PKI（連邦 PKI）開発において問題となる課題について対策方法などを規定

4）郵政･通産･法務省 “電子署名･認証に関する法制度の整備について” [9] および 警察庁 “電子認証制度のセキュリティ確保方策についての基本的考え方” [10]
：法制度の課題について検討
→民間からコメントを求め、実社会に見合った電子署名法の成立を目指している

以上、各検討団体において CA 連携を実現するための検討が行われている。しかし、第 1 章で述べた通り、現状 CA 連携を用いて EDI や EC を行ったといった実例はほとんど見受けられない。その理由としては、EDI･EC で CA 連携を行うための方式面については何も検討されていないためであると考えられる。そこで以後では、この EDI･EC で CA 連携を行うための方式面について課題を明確にするとともに、それらの解決するための具体的方策を提案する。

4. 実業務への CA 連携の適用課題

現実社会における B(Business) to B、B to C (Consumer)における業務形態を考えてみると、以下の 2 種に分類できる。

1）基幹業務、契約書などリアルタイムにその文書自体の有効性を確認する必要のあるリアルタイム系業務
2）E-mail などリアルタイムに有効性確認を行う必要のないコミュニケーション系業務

この業務形態を電子社会に置き換え、CA を用いた相手認証を適用した場合、リアルタイム系業務では契約書など重要文書がやり取りされるため、リアルタイムな署名検証が求められる。そのため、受信者側の署名検証時点で送信者の公開鍵証明書の有効性を確認できるためのインタフェースが CA 側で求められる。また一方、コミュニケーション系業務においては、文書自身の重要性がそれほど高くないため、それほどリアルタイムな有効性確認は求められない。そのため、受信者側の署名検証時点で送信者の公開鍵証明書の有効性を確認するためのインタフェースを CA 側で設ける必要はない。

現状、受信者側の署名検証時における送信者の公開鍵証明書の有効性確認を行う方法として、以下の 2 種が存在する。

Ⅰ）CA からの公開鍵証明書取得による有効性確認方法
送信者の公開鍵証明書をリアルタイムに管理している CA から何らかの方法で送信者の公開鍵証明書を取得することにより、公開鍵証明書の有効性確認を行う

Ⅱ）CRL による有効性確認方法
CA が事前作成した CRL をユーザが何らかの方法で取得し、その CRL を参照することにより公開鍵証明書の有効性確認を行う

しかし、上記従来方法による公開鍵証明書の有効性確認方法を EDI・EC で用いる状況において

は、以下の問題が存在する。

①公開鍵証明書を管理しているのは送信者の CA であり、その CA に登録しているユーザ以外からの申請を許可していない場合が存在したり、ファイアウォールなどによりアクセスできない場合がある

②各 CA により CRL 発行間隔が異なっている場合、CRL 発行間隔の短い CA に登録するユーザにとっては、自 CA より発行間隔が長く、無効化情報の反映頻度が低い CRL で通信相手の公開鍵証明書の有効性を確認することになり、信頼性の低下につながる可能性がある

これらの課題を解決しない限り EDI・EC において CA 連携を用いた相手認証を行うことはできない。

そこで著者は、これを解決する方法として、公開鍵証明書取得日時（タイムスタンプ）を用いて公開鍵証明書の有効性確認を行う“証明書取得日時保証（タイムスタンプ）方式”を提案した[11]。

本方式は、公開鍵証明書の有効性確認のための情報をユーザ間でやりとりするとともに、公開鍵証明書の有効性確認ポリシーをユーザにおき、そのユーザのポリシーのもとに公開鍵証明書の有効性確認を行うものであった。

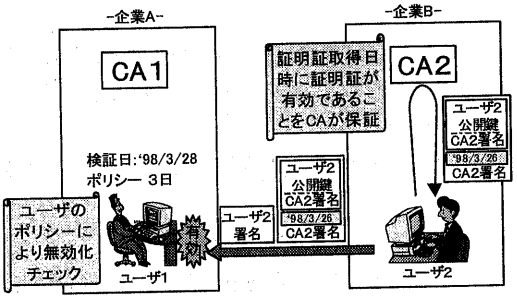


図2　証明書取得日時保証(タイムスタンプ)方式

しかし、本方式は、公開鍵証明書の有効性確認の手段となる証明書取得日時が文書の送信者により行われるため、検証時点においては既にある程度の時間が経過してしまう。そのため、リアルタイム系業務への適用はできないという問題点があった。

そこで、本論文においては、EDI・EC への CA 連携の適用を目指し、前記従来方法による公開鍵証明書の有効性確認方法における課題を解決するとともに、リアルタイム系業務にもコミュニケーション系業務にも適用可能な“ディレクトリを用いた公開鍵証明書有効性確認方式”を提案する。

5. 提案方式：ディレクトリを用いた公開鍵証明書有効性確認方式

本提案方式では、第4章で述べた課題を解決する手段として、CA が公開鍵証明書とともに、更新日時をディレクトリに掲載する。

5.1 全体構成

本提案方式の全体構成を図3に示す。

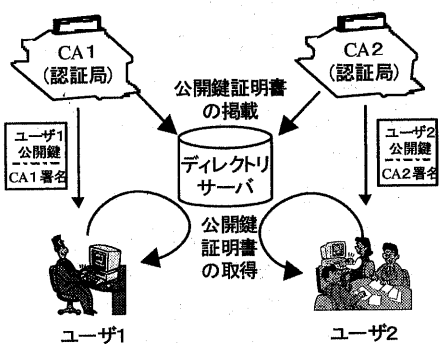


図3　全体構成

このディレクトリを用いた公開鍵証明書の有効性確認方式では、各 CA が自システム内で発行した公開鍵証明書を管理しておくとともに，ディレクトリに公開鍵証明書を掲載する。また、発行した公開鍵証明書が無効化されたあるいは有効期限切れになった場合、その公開鍵証明書をディレクトリから削除する。そして，ユーザは名前や電子メールアドレスなどのパラメータに基づいて LDAP[12]によりアクセスし，公開鍵証明書をディレクトリから検索する。こうして、相手ユーザ（通信相手）の署名を検証するための公開鍵証明書を取得し、その公開鍵証明書を用いて相手ユーザの署名を検証する。ディレクトリを用いる際の

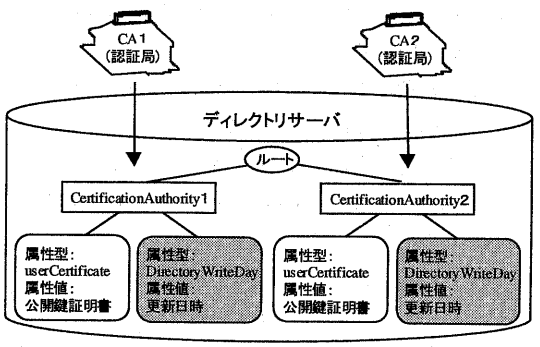
スキーマおよびプロトコルは標準として規定されており[13]、これを用いることにより、すべてのユーザがこのディレクトリから公開鍵証明書などを取得することが出来る。

5.2 実現方式

本提案方式は以下の方式により実現される。

5.2.1 CA 側処理

CA がディレクトリに公開鍵証明書を更新する際、CA 側において，その更新日時をディレクトリの CA-DN 配下に記載する。また、ディレクトリ更新時に公開鍵証明書の無効化および有効期限切れがない場合に、前記ディレクトリに保持する更新日時をそのときの時刻に更新する。これにより、ディレクトリ更新が行われた日時にその公開鍵証明書が有効であったことを CA が保証する。



※1 CAにおいて登録、無効化および有効期限切れがない場合にも更新日時のみ更新

図4 CA 側処理

その実現方式としては、CA 側において CA 内で管理されている公開鍵証明書情報の変化の発生、あるいはディレクトリを更新する時間間隔に達したことによりディレクトリ更新が起動された際、CA 内に設定されているシステムクロックをもとに更新日時を作成した後、この更新日時に対し CA の秘密鍵により署名をふる。そして、ディレクトリへ公開鍵証明書情報を掲載するとともに、各 CA-DN（オブジェクトクラス CertificationAuthority）の配下に属性型：userCertificate、属性値：ユーザ公開鍵証明書とともに、属性型：DirectoryWriteDay、属性値：更新日時を記載することでディレクトリに公開鍵証明書および更新日時を掲載する。

なお、本方式の実現には、現在の属性型に加え、新たに更新日時を示す属性型 DirectoryWriteDay を定義する必要がある。

5.2.2 ユーザにおける公開鍵証明書の有効性確認方法

ユーザは各利用者と通信を行う事前作業として公開鍵証明書の有効性を認める更新日時の許容時間を端末 AP に設定しておく。そして、通信相手から署名がふられた文書を受け取った際、ユーザはディレクトリに格納されている通信相手の公開鍵証明書を取得するとともに、CA-DN 配下に掲載されている更新日時を取得し、その更新日時から現在時刻までの差がユーザが事前に設定した許容時間より短いならば、その公開鍵証明書を有効であるとみなし、その公開鍵証明書により相手ユーザから送信された文書にふられている署名を検証する。

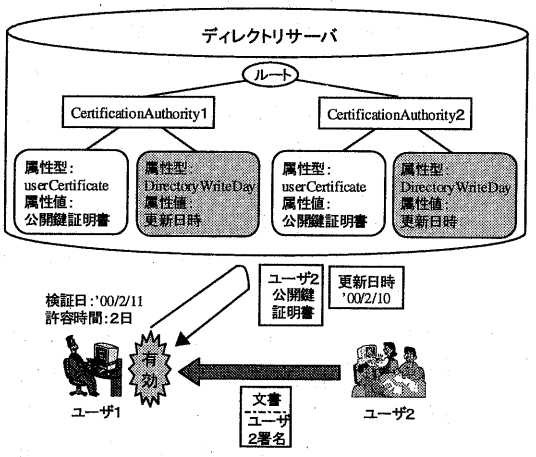


図5 公開鍵証明書の有効性確認

6. 考察

以上、ディレクトリを用いた公開鍵証明書有効性確認方式を用いることにより、公開鍵証明書のみで公開鍵証明書の有効性確認を行うことが可能となる。また、ディレクトリを用いているため、

すべてのユーザがこのディレクトリから公開鍵証明書などを取得することが出来る。これにより、以下が可能となる。

① ファイアウォールによるアクセス制限あるいはそのCAに登録しているユーザ以外の申請は受け付けないといったCAのアクセス条件に依存しない公開鍵証明書有効性確認ができる

② また、公開鍵証明書の有効性確認の信頼性を常に一定に保つことができる

本提案方式の付加的な効果として、公開鍵証明書のみで公開鍵証明書の有効性確認を行うことが可能であるため、従来のCRLの課題であった無効化された公開鍵証明書情報が多い場合におけるCRL取得の際の転送時間およびCRL内の公開鍵証明書情報の検索時間が非常に大きくなるという問題点も解決できる。

また、本提案方式は、以下のようにリアルタイム系業務、コミュニケーション系業務それぞれに適した公開鍵証明書有効性確認方式が実現できる。

1）CAからのディレクトリへの公開鍵証明書の更新を公開鍵登録や公開鍵証明書の無効化など公開鍵証明書状態の変化が起こるたびにディレクトリを更新しているCAを利用しているユーザ間通信においては、常にリアルタイムな公開鍵証明書有効性確認ができるとともに、たとえCAからディレクトリへの掲載において通信障害が発生したとしても、その情報をユーザは更新日時により得ることができる

2）また、あらかじめCAが設定したある時間間隔をおいて一定間隔でディレクトリの更新を行っているCAを利用している状況においても、リアルタイムな公開鍵証明書有効性確認は出来ないが、ユーザのポリシーの下に公開鍵証明書有効性確認が可能になり、各CAのポリシーに依存しない公開鍵証明書有効性確認ができる

この結果から明らかなように，本稿で述べた提案方式は、EDI・ECに必要なCA連携を実現する際に非常に有用な方式であるといえる。

7. 今後の課題

本稿では、EDI･ECへのCA連携に適用できるとともに、リアルタイム系業務にもコミュニケーション系業務にも適用できるディレクトリを用いた公開鍵証明書有効性確認方式を提案した。

今後は、本提案方式の実装方法について検討し、その実現性について評価を行っていく。

【参考文献】

[1] CROSS-CERTFICATION WITHIN APEC http://www.pecc.org/ptiif/crosscert.doc

[2] ICAT http://www.icat.or.jp/

[3] JapanNet http://www.japannet.or.jp/

[4] UNINETT http://www.uninett.no/pca/

[5] Achieving PKI Interoperability APEC(1997)

[6] 企業間電子商取引における認証・公証適用の考え方 ECOM(1998)

[7] MISPC(Minimum Interoprability Specification for PKI Components, Version1 NIST(1997)

[8] FEDERAL PUBLIC KEY INFRASTRACTURE (PKI) TECHNICAL SPECIFICA-TION:PART D-INTEROPRABILITY PROFILES NIST(1995)

[9] 電子署名･認証に関する法制度の整備について 郵政･通産･法務省(1999)

[10] 電子認証制度のセキュリティ確保方策についての基本的考え方 警察庁(1999)

[11] エクストラネット向け証明証有効性確認方式 今枝直彦 電子情報通信学会総合大会(1999)

[12] RFC2559(LDAPv2) IETF PKIX-WG(1999)

[13] RFC2587(LDAPv2スキーマ) IETF PKIX-WG (1999)

[14] X.500ディレクトリ入門 大山実、戸部美春、田中博巳、千田昇一、窪田光裕、空一弘 東京電機大学出版局(1997)