コンピュータセキュリティ 1－5
（1998. 5. 29）

X.500ディレクトリサービスを用いた複数の認証ドメイン間の相互認証方式の一提案

須賀 祐治[†‡] 山崎 重一郎[†] 村上 美幸 荒木 啓二郎[†*]

[†]（財）九州システム情報技術研究所

〒814-0001 福岡市早良区百道浜2丁目1番22号 Phone:(092)852-3454, Fax:(092)852-3465

[‡]（株）エクシーズ，*九州大学大学院 システム情報科学研究科

概要 現在、インターネット上のプロトコル，アプリケーションはセキュリティを確保するために公開暗号鍵技術を使用しているが、それらが利用できる公開暗号鍵インフラ (public-key infrastructure, PKI) の整備が急務となっている。X.509 標準 [2] はこのインフラのベースとなるもので、認証の基本的な枠組みおよび証明書のフォーマットが規定されている。また X.509 デジタル証明書はすでに多くのアプリケーションで利用されている。本報告では、異なる認証ドメインの証明書の検証が可能になり、結果的に PKI クライアントのサービス有効範囲を拡大することができる相互認証技術をディレクトリサービスを用いた方式で提案する。

A proposal for cross-certification over several certificate domains using the X.500 Directory

Yuji SUGA[†‡] Shigeichiro YAMASAKI[†] Miyuki MURAKAMI Keijiro ARAKI[*‡]

[*]Institute of Systems & Information Technologies/KYUSHU

2-1-22, Momochihama Sawara-ku, Fukuoka City 814-0001, Japan

Phone:+81-92-852-3454 Fax:+81-92-852-3465

[†]Xseeds Co., Ltd.

[‡]Department of Computer Science and Communication Engineering, kyushu University

Abstract Many Internet protocols and applications employ public-key technology forsecurity purposes and also require a public-key infrastructure (PKI in short) to manage public keys. The X.509 standard constitutes a basis for such an infrastructure, defining data formats and authentication framework. X.509 certificates are already used in multiple appliations. This document proposes cross-certification by using the X.500 Directory, and it is possible to verify certificates on another domain and also extend scopes which PKI users can receive services.

1 はじめに

現在、インターネットなどを介して通信を行う際には共有鍵暗号方式とともにＲＳＡなどの公開鍵暗号方式が広く使用されている。公開鍵暗号方式では所有者のみ保持する秘密鍵と、一般に公開される公開鍵の２つの対となる鍵を使用する。通信相手の公開鍵があれば、その相手だけが復号化できる情報を送信することができる。また逆に、送信者が自身の秘密鍵を用いて暗号化した情報を、受信者が送信者の公開鍵を用いて復号化できるかどうか検証することでデジタル署名が可能になる。

このような情報の暗号化，署名の検証を実現するには、公開鍵は広く配布されるべきである。その際には通信相手の正しい公開鍵の入手を保証するしくみが必要であり、その実現方法の一つとしてデジタル証明書を用いる方法がある。

デジタル証明書は認証局 (Certificate Authority, CA) という信頼のおける第三者機関から発行され配布される。証明書には識別名（X.500 [1] で規定された木構造の名前空間）と公開鍵が含まれており、これらに対して認証局のデジタル署名が施されたものである。認証局の署名により改竄を防止しているとともに、証明書を受け取った検証者は認証局を信頼することにより、証明書内の公開鍵が証明書の被署名者自身のものであることを確認し、正しい公開鍵を入手することができる。

X.509 [2] はこのような認証の基本的な枠組みおよび証明書のフォーマットが規定された公開暗号鍵インフラ (public-key infrastructure, PKI) のベースとなるものである。X.509 デジタル証明書はすでに PEM (Privacy Enhancement Mail, [5]) や SSL、S/MIME などといったセキュリティプロトコルの「通信情報の暗号化、ユーザ認証」機能で利用されている。

このようにデジタル証明書を使った通信プロトコル、またそれに準拠したアプリケーションはすでに提供されているが、証明書の検証においては次のような問題が残されている。同じ認証局配下の PKI クライアント間は同じ証明書パスを保持しているので、お互いの証明書の検証は可能である。しかし、異なる認証ドメインの（つまり検証者の知らない認証局から発行された）証明書を検証することはできない。他ドメインの認証局の証明書を入手する必要があるからである。しかもその証明書の正当性を保証する手だてはなく、フォーマットとしては正しい証明書と判断したとしても、認証のしくみから考えても何の意味もなさない。

この問題を解決する方法として相互認証技術がある。相互認証により、異なる認証局が発行した証明書を相互に流通させることで、他ドメインの証明書の検証を可能にする。また、PKI クライアントが受けられるサービス利用範囲を拡大することができる。本報告では X.500 ディレクトリサーバを用いてこれらの問題を解決した事例を紹介する。

本稿ではまず２章で従来の階層型認証モデルを、３章にて X.500 Directory の概要について紹介する。そして４章においてディレクトリを介した相互認証方式を提案し、５章で実際の運用の概要と問題点，今後の課題について報告する。

2 従来の認証モデル

RFC 1422 [5] は X.509 に基づいた PKI を提案しているが、実際の運用の際には支障をきたしている面も見受けられる。その一つに証明書の検証時における問題がある。

2.1 証明書の検証

証明書の検証とは、証明書の issure（署名者）による署名が issure 自身が subject （被署名者）となっている証明書に含まれる公開鍵による署名であるかどうか確かめることを指す。このようにして証明書を連鎖させ自己署名の証明書（つまり issure と subject が一致する証明書）までの検証をすべてクリアすると、対象となる証明書内の情報が保証される。このような認証モデルは階層型と呼ばれる。

RFC 1422 の規則ではどのユーザ証明書に対しても、最上位認証局までに至る経路はひとつしかないと定められている。この規則は、検証者から見ると正しい連鎖かどうか検証する際には便利である。しかし、実際には検証経路をショートカットする証明書を利用するほうが便利なことがある。例えば、相互に検証し合う PKI クライアントの多い２つの認証局間では検証する時間が短いこと、すなわち検証経路が短いことが要求されるであろう。

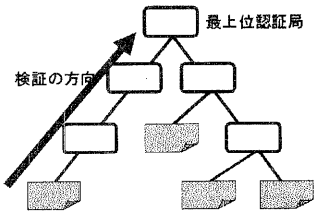

図 1: 階層型認証モデル

2.2 証明書の廃棄

証明書を実際に運用する際には、秘密鍵の漏洩など何らかの事由により証明書を無効にすることがある。この処理は認証局が行い、一般的には定期的に廃棄証明書リスト（Certificate Revocation List, CRL）を公開することが多い [7] 。

しかし CRL は廃棄情報がきちんと伝達されるまでに時間的なロスが生じ、有効に見える証明書でも実際には廃棄されている可能性もある。そのため、即時性の必要なアプリでの利用は難しいと考えられる。これを解決する方法としてオンラインでの検証プロトコル [12] やそのための証明書のフォーマット拡張 [13] が提案されている。これらを実装した検証サーバの構築が急務となっている。

3 X.500 ディレクトリサービス

X.509 標準は X.500 ディレクトリサーバの環境で機能するように設計されている。しかし、証明書のリポジトリとして必ずしも利用しなければならないと規定しているわけではない。

3.1 X.500 Directory

ディレクトリとは広域ネットワーク上の巨大な分散データベースである。X.500 [1] はこの情報データベースを構築するための枠組みの標準の一つである。元々は情報通信のグローバル化に伴って、通信に必要な情報を一元的に管理し必要に応じて情報案内サービスを提供するために開発されたものである。今回、証明書および CRL のリポジトリとしてこのディレクトリを用いる。

X.500 で規定されている分散協調オペレーションには chaining（連鎖）、referral（紹介）、replication（複製）がある。chaining とは情報提供の依頼を受けたサーバが自サーバにその情報がない場合に、その情報を持つサーバにアクセスして情報を得、その情報をクライアントに返却する方式である。

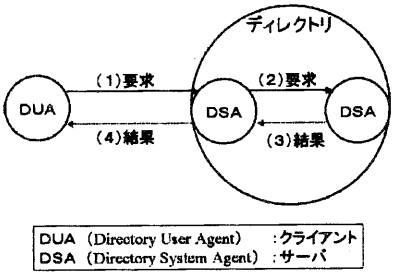

図 2: chaining

referral とは情報提供の依頼を受けたサーバが自サーバにその情報がない場合に、その情報を持つサーバのロケーションを紹介する方式である。この場合クライアントは紹介されたサーバに直接アクセスして情報を得る。

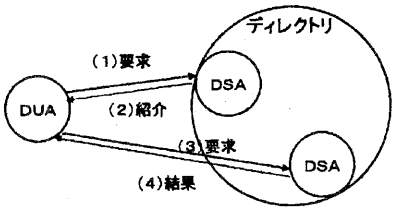

図 3: referral

今後、管理する証明書数，参照などのアクセス

数が増大し、ディレクトリへの負荷が大きくなる可能性があるが replication（複製）サーバを構築することで回避できると考えられる。

3.2 その他のリポジトリ

その他のリポジトリとして FTP や HTTP を用いる方式 [11] も提案されている。これらのプロトコルはディレクトリにアクセスするためのプロトコル LDAP [6] に比べ普及しているため利用される範囲は大きいと期待される。また、証明書, CRL ともに認証局による署名が施されているという理由から、特に安全な通信路で配布する必要がないため、これらの配布の際には十分である。

しかし今回提案する方式では、ディレクトリ情報は安全に守られているという仮定が必要となる。つまりディレクトリにアクセスする際にも情報の正当性を保証する手だてが必要になってくる。そのため LDAP+SSL というセキュリティプロトコルでの使用を仮定する。これはディレクトリサーバ自体が公開鍵すなわちサーバ用証明書を持てば実現できる。

4 相互認証

すでに企業／部署内などで認証局を構築し、ローカルな閉じた世界でのみ通用する証明書を発行している事例も少なくない。しかしこのローカルドメイン内の PKI クライアントは、やはり閉じたドメイン内のサービスしか受けられない。異なる認証ドメインの証明書を検証する方法がないからである。異なる認証ドメインの証明書の検証には、そのドメインの認証局の証明書を入手する必要がある。しかも「安全に」入手されなければならない。

4.1 相互認証証明書対

X.509 にはディレクトリに登録される証明書の形式として、ユーザ用証明書 (userCertificate) 、認証局証明書 (cACertificate) の他に、相互認証証明書対 (crossCerificatePair) という属性 (attribute) が規定されている。

```
crossCerificatePair ATTRIBUTE ::= {
  WITH SYNTAX  CertificatePair
  ID           id-at-crossCertificatePair }
```

```
CertificatePair  := SEQUENCE {
  forward  [0]  Certificate OPTONAL,
  reverse  [1]  Certificate OPTONAL }
```

相互に署名した 2 枚の証明書を新たに発行することにより、相手認証局が発行した証明書を検証する際の正しい証明書経路を得ることができる。

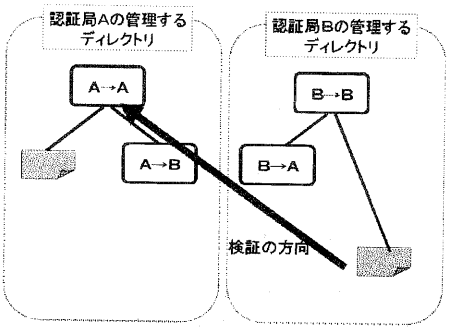

図 4: 相互認証証明書対のしくみ

しかしこの方式では、一つの認証局の証明書が複数存在するため、検証時の証明書経路が複数になる可能性があり、最短の経路を見つけるための別のしくみが必要となる。

4.2 提案方式

以下の提案方式は、認証局ごとにセキュアなディレクトリサービスを提供していること、ディレクトリ情報は安全に守られていることを仮定する必要がある。PKI クライアントはローカルディレクトリを信頼するだけで、証明書の検索などはすべてディレクトリ間の相互オペレーションに任せる。認証局ごとに構築されたディレクトリ間の情報交換により、他の認証局下にある証明書の取得，有効性の検証が可能になる。

また、本報告ではお互いの認証局ポリシーの違いのすりあわせについては言及しない。

4.2.1 属性拡張

4.1 と同様に自ディレクトリに相互認証している認証局の証明書を保持しておく方式であるが、新たに相互認証用の証明書を発行しない。その代わりに

相手の自己署名証明書を保持しておく。その証明書用に crossCerificatePair 属性内の CertificatePair の形式を次のように拡張する。

```
CertificatePair  := SEQUENCE {
  forward      [0]  Certificate OPTONAL,
  reverse      [1]  Certificate OPTONAL,
  selfsigned   [2]  Certificate OPTONAL }
```

[2]selfsigned がある場合には [0]forward および [1]reverse の証明書は無視する。ディレクトリに保持しておく証明書の数は変わらないが、検証経路を短くすることができる。

4.2.2 サーバ証明書の相互発行

相互認証証明書対を発行する代わりに、お互いに相手ドメインのディレクトリサーバに証明書を発行する方式である。

ディレクトリサーバでは、どのドメインの PKI クライアントからのアクセスなのか、つまりどの認証局から発行された証明書を持つクライアントなのかを判断して、そのクライアントの issure と同じ認証局から発行されたサーバ証明書を SSL のセッションで提示する。これにより PKI クライアントは相手ドメインのディレクトリ情報を安全に得ることができる。

5 実験運用と問題点

5.1 ISIT での運用

当研究所では認証局の運営とともに発行した証明書のリポジトリとして X.500 ディレクトリを公開している。福岡オンライン認証WG [15] で結成されたＲＡ友の会メンバーにより現在 8 地点からのＲＡが運用され、このディレクトリを中心とした運用実験を行っている。ディレクトリ情報には最新の CRL も格納されており、証明書と同様に自由に閲覧できるようになっている（図５）。

昨年度に引き続き ICAT CA [14] の下位認証局の運用とともに、今年度からは自己認証局の運営も開始している。手始めに、この２つの認証局間の相互運用実験を行っていく。いずれも実験の枠内での運用ではあるが、ここで浮き出てきた新たな問題を見い出し、検討したいと考えている。

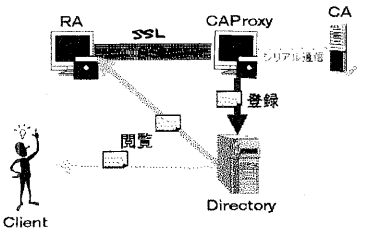

図 5: ISIT での運用形態

5.2 X.500 名前空間

ディレクトリの相互運用をする際には X.500 名前空間の取り決めが問題になってくる。証明書内には issure の 識別名 (Distinguished Name, DN) が含まれているが、同じ DN を持つ認証局が複数存在する場合、検証時に不都合が起きる。また subject の DN のバッティングも問題である。

証明書発行時にディレクトリ内で検索して、DN のバッティングが起こっていないか確認する方法は実現できるが非効率であろう。現在のドメイン名の管理と同様に、RFC1422 で規定されているような登録制度のしくみが必要になるかもしれない。X.500 DN にドメイン名を用いる方法 [8] も提案されている。いずれにせよ、この問題を解決するためにはまだ検討の余地があると思われる。

参考文献

[1] ITU-T Recommendation X.500, "Info. tech. - OSI - The Directory: Overview of concepts, models and services", 1993.

[2] ITU-T Recommendation X.509, "Info. tech. - OSI - The Directory: Authentication framework", 1993.

[3] ITU-T Recommendation X.520, "Info. tech. - OSI - The Directory: Selected attribute types", 1993.

[4] ITU-T Recommendation X.521, "Info. tech.

- OSI - The Directory: Selected object classes", 1993.

[5] Kent, S., "Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management", RFC 1422, Feb., 1993.

[6] W. Yeong, T. Howes, S. Kille, "Lightweight Directory Access Protocol", RFC 1777, BBN, Mar., 1995.

[7] N. Berge, "UNINETT PCA Policy Statements", RFC 1875, Norweign Computing Center, Dec., 1995.

[8] S. Kille, M. Wahl, A. Grimstad, R. Huber, S. Sataluri, "Using Domains in LDAP/X.500 Distinguished Names", RFC2247, Jan., 1998.

[9] R. Housley , W. Ford, W. Polk, D. Solo, "Internet Public Key Infrastructure X.509 Certificate and CRL Profile", draft-ietf-pkix-ipki-part1-07.txt, 1998 (work in progress).

[10] C. Adams, S. Farrell, "Internet X.509 Public Key Infrastructure Certificate Management Protocols", draft-ietf-pkix-ipki3cmp-07.txt, 1998 (work in progress).

[11] R. Housley, "Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP", draft-ietf-pkix-opp-ftp-http-03.txt, 1998 (work in progress).

[12] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", draft-ietf-pkix-ocsp-03.txt, 1998 (work in progress).

[13] http://home.netscape.com/eng/security/comm4-cert-exts.html, Netscape Certificate Extensions.

[14] http://www.icat.or.jp/, 認証実用化実験協議会 (ICAT)

[15] http://www.k-isit.or.jp/dccf/, 福岡オンライン認証WG