SET他の公開鍵証明証の検証方式の考察

5M－7

榊原 裕之　吉武 淳
三菱電機（株）情報技術総合研究所

1 はじめに

弊社参加の電子商取引実証実験プロジェクトであるJapanNetでは、認証局を運営し、SET用公開鍵証明証の発行、及び、SET[1]の実装を行っている。また、JapanNet 会員証明用の公開鍵証明証の発行も行っている。本稿ではこれらの公開鍵証明証（以降、証明証）の失効管理も含めた検証方式について検討・考察する。

2 CAの階層構造と証明証のChain

証明証はCAの署名により正当性が保証される。従って、証明証の署名をチェックすることが不可欠であるが、チェックする為のCAの公開鍵を取得する必要があり、その検証のためにはさらに上位のCA の公開鍵が必要となる。SET 及び、JapanNet会員証明用のCAは図１の様な階層構造をとっている。この構造では、root CAから順に１つ下のサブCA を含んだエンティティに対して証明証を発行していく(CAiが複数のi+1のレベルのサブCAに証明証を発行することも許す)。従って、あるエンティティの証明証を検証する場合は、直接上位のCAからroot CAまで、階層上に位置するCAの証明証を収集し、各証明証を順番に検証していく必要がある。また、失効のチェックにCRLを利用した場合、CRLにも署名が付加されており、この署名をチェックする為に必要な証明証を収集し、Rootまで溯って検証する必要がある。検証する証明証と必要な上位の証明証の一連を証明証のChainと呼ぶ。本稿では必要なCRLもChainに含めるものとする。通常、Rootの証明証署名用証明証はself-sign形式をとり、にせのルートでないことを、別の手段で確認する必要がある。以降、本稿ではCAの階層は図１の形式を前提とする。

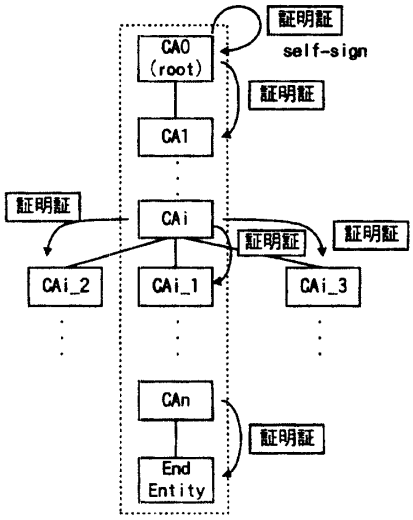

図１

3 証明証のChainのパターン

(1) 証明証の用途の影響

図2-1にCAの証明証が、証明証署名用とCRL署名用の証明証が兼用になっている場合の証明証のChainの構成例を示す。例では、EndEntityの証明証を検証する為に必要な証明証・CRLの構成を示してあり、最も簡単な証明証のChainを形成する。また、SETでは、CRL署名用証明証と、証明証署名用証明証が別に存在することを許している。この場合、図2-2のような証明証のChainを形成する。図2-1, 2-2の場合は、共に検証ロジックにおいて、証明証のextensionに鍵用途（keyUsage）が含まれている場合、適切な値であることをチェックする必要がある。

(2) 証明証の世代の違い

図2-2においては、CA2の証明証署名用証明証とCRL署名用証明証が、CA1の同一の証明証署名用証明証により検証されるケースであるが、CAが２つの証明証署名用証明証を持ち、各々が直接下位のCAの証明証署名用とCRL署名用の証明証の検証に

A verification scheme for public key certificates
Hiroyuki Sakakibara, Jun Yoshitake
Information Technology R&D Center, Mitsubishi Electric Corporation

用いられるケースも存在しうる。

例えば、ある認証系において以下のシナリオに従った場合、図 2-3 の様な証明証の Chain が形成される。

1. CA1 が証明証署名用証明証を root に更新してもらった。新しい証明証の世代は i+1 である

2. CA2 の CRL 署名用証明証（世代 i）が失効した。CA2 は新しい CRL 署名用の鍵対を生成し、CRL 署名用証明証を CA1 に発行し直してもらった。CA1 は世代 i+1 の証明証署名用証明証と対の秘密鍵を署名に用いた。

3. CA2 は新しい CRL 署名用証明証（i+1 世代）と対の秘密鍵を用いてで新しく CRL を発行し、公開した。

この例では、CA2 の i+1 世代の CRL 署名用証明証の検証には **CA1 の i+1 世代**、CA2 の i 世代の証明証署名用証明証の検証には **CA1 の i 世代**の証明証署名用証明証が必要となるケースである。このようなケースを想定し、一般的な例を示したのが、図 2-4 であり、複雑な Chain を形成する。

4 考察

SET においては、BCI（Brand CRL Identifier）の利用が Chain の簡潔化に貢献している。BCI では、各 CA が発行する最新の CRL の番号を項目として持つ。失効している証明証がない状態では、その項目の値を NULL にすることで、CRL の検証自体の必要をなくし、その結果 Chain の構造を簡潔にしようとしている。また、図 2-5 の様に証明証署名用と CRL 署名用を兼用することも、Chain の簡素化に貢献する。

5 おわりに

CA が更新のポリシー等で、同時に同じ用途の複数の証明証を持つ場合、証明証の Chain の構造が複雑になることを示した。証明証を利用するシステムはこのような形態の認証系に対しても確実な証明証検証機能を持たなくてはならない。今後、JapanNet プロジェクトでは Chain の構造の簡潔化に貢献するような証明証・CRL の管理方式を提案していきたい。

<参考文献>

[1]Secure Electronic Transaction Specification
Book1, Book2, Book3, version1.0 May 31, 1997

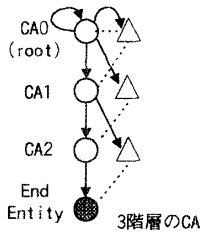

図 2-1

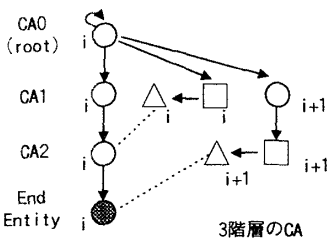

図 2-3

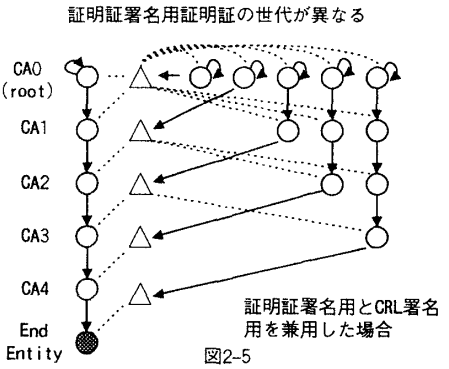

図2-5

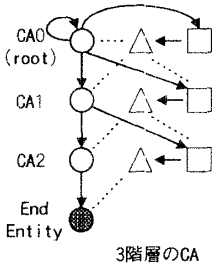

図 2-2

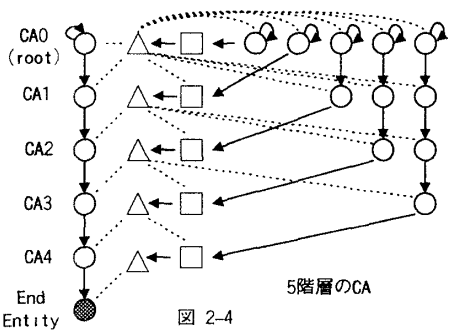

図 2-4

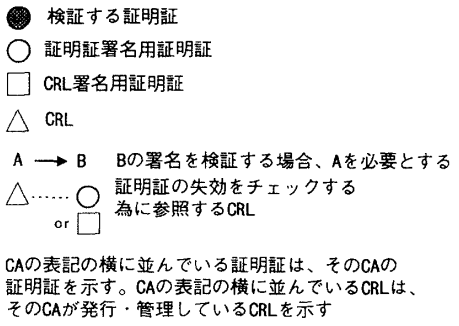

図 2