1F-4

相互認証における公開鍵証明書の検証

榊原 裕之 、辻 宏郷
三菱電機(株) 情報技術総合研究所

1 はじめに

電子商取引などにおいて、異なる PKI(Public Key Infrastructure) ドメイン間で認証を行う相互認証[1]の必要性が増している。相互認証においては、公開鍵証明書(以下、証明書)を利用するが、その正当性の検証は、安全性の確保の面で非常に重要である[1]。しかし、各 PKI ドメインの、CA(Certification Authority)の機能・安全性・運用は均一ではなく、CA 間の連携の不備が考えられる。本稿では、該不備により、証明書の安全性において問題が生じることを示し、解決方法を提案する。

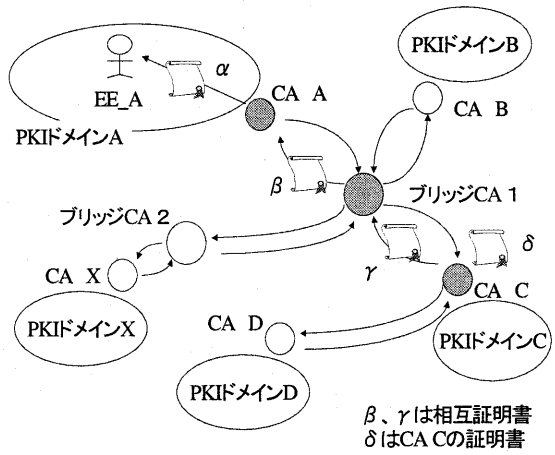

図1

2 相互認証の環境について

相互認証では、図1のように、異なる PKI ドメイン間において、各ドメインの CA が、直接2者間或いは、ブリッジ CA[2]と相互証明書を発行し合う。他ドメインのエンティティと認証を行う場合、他ドメインの認証相手の証明書から自ドメインの CA の証明書までの、相互証明書を含む"証明書の連鎖"(証明書パスと呼ぶ)を構築・検証する。その上で、相手の証明書を利用して認証を行う[2]。例えば、ドメイン C のエンティティが、EE_A の証明書 α を検証する場合、証明書パスは、$\alpha \leftarrow \beta \leftarrow \gamma \leftarrow \delta$ となる。

しかし、各ドメイン間で、CA の性能・安全性・運用に差があると考えられ、それが原因で、CA 間の連携に不備が生じた場合は、証明書パスの安全性に影響する。例えば、CA C とブリッジ CA1 の間は連携が正常でも、ブリッジ CA1 と CA A 間で不備があった場合、前述のパスの安全性が疑わしくなる。

そこで、安全性に影響を及ぼす CA 間の連携の不備の例を2つ挙げる。

2.1 証明書の失効状態の矛盾

第一の例は、相互証明書の被発行者の CA が元々保持する証明書と、相互証明書の間で失効状態が矛盾する場合である。

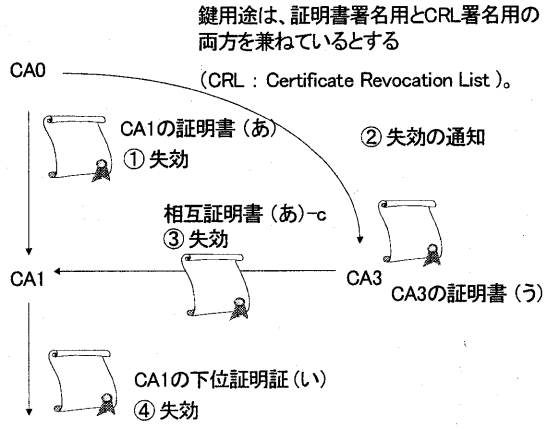

図2

図2において、CA1 は、自分のドメインにおいて、CA0 から証明書(あ)の発行を受けている。次に、異なるドメインの CA3 から相互証明書(あ)-c の発行を受ける。この時、(あ)と(あ)-c に含まれる CA1 の公開鍵は同一である。

①で CA0 が(あ)を失効させたとする。通常の運用であれば、②で CA3 に(あ)の失効が通知され、③で CA3 は相互証明書(あ)-c を失効させる。また、④では、CA1 が発行した下位証明書(い)を失効させる。ところが、CA0(または CA1)と CA3 間の連携に不備があり、②が速やかに行われなかった場合、③が実施されるまでの間、同じ公開鍵に対する証明書である、(あ)と(あ)-c の間では失効状態が異なる。この間、CA3 のドメインのの検証者が、(い)を検証した場合、証明書パスは、「(い) → (あ)-c → (う) …」となり、(あ)-c は失効していないので、検証が成功してしまう。

また、CA1 の秘密鍵が漏洩している場合、既に失効している(い)に関して、"失効していない"、最新の日付の偽造 CRL が生成・配布されている可能性がある。検証者がこの偽造 CRL を取得した場合、(い)は、失効していないと認識されてしまう。

2.1 相互証明書の矛盾(有効期限)

第二の例は、相互証明書の被発行者の CA が元々保

Public Key Certificate Validation for Cross Certification Environment
Hiroyuki SAKAKIBARA, Hirosato TSUJI
Information Technology R&D Center, Mitsubishi Electric Corporation

持する証明書と、相互証明書間で有効期限が矛盾する場合である。図3では、CA1は、自分のドメインにおいて、CA0 から証明書(ア)-1 の発行を受けている。次に、異なるドメインの CA3 から相互証明書(ア)-c の発行を受ける。この時、(ア)-1 と(ア)-c に含まれる公開鍵は同一である。CA1 は下位エンティティに対して(イ)の証明書を発行する。

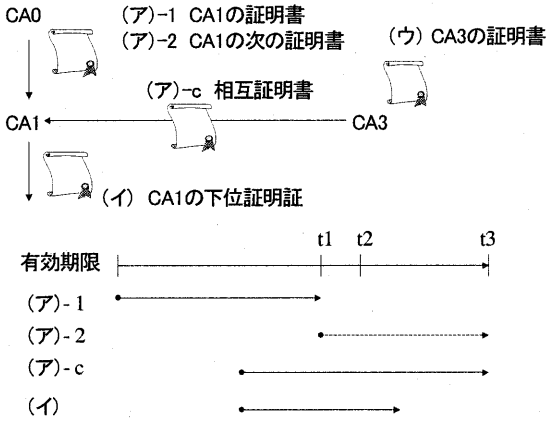

図3

各証明書の有効期限に着目すると、(イ)の有効期限は、(ア)-1を超えている。しかし、CA1 は t1 の時点で、自身の鍵対に問題が無ければ、同じ鍵対を継続して使用し、(ア)-1 と同じ公開鍵を保証した(ア)-2 の発行を受けることを予定している。当運用は、CA1 の下位証明書を、(ア)-1 の有効期限内に納める必要が無いので、t1 以前のどの日時で発行しても、同じ長さの有効期間の証明書を発行能であり、利便性が良い。

相互証明書の有効期限については、CA1 として、自身の証明書(ア)-1 の有効期限を越えた相互証明書の発行を許さない運用が考えられる。ここで、相互証明書(ア)-c を、(ア)-2 の発行を期待して、(ア)-1 の有効期限を超えて発行した場合を考える。すると、もし、(ア)-2 の発行が中止された場合、(ア)-2 が存在しないにも関わらず、t2 の時点では、相互認証の証明書パス「(イ) → (ア)-c → (ウ) …」が構築されてしまうことがある。

3 解決方式の提案

■ 相互認証の運用ルールの策定

第一に、前述の連携の不備の防止も含めた、相互認証における確実な運用ルールを策定し、各ドメインはルールに従う必要がある。

■ 運用ルールが守られなかった場合

しかしながら、正常運用時は運用ルールに従ったとしても、連携の不備は CA のシステム障害や、操作ミスにより発生する可能性がある。問題は、自ドメインが運用ルールを守っても、相手ドメインが、故意あるいは事故で運用ルールを守らなかった場合に、結果として、証明書の状態に矛盾が生じることにある。

■ 検証者による矛盾の検出機能

従って、証明書の検証者が、これらの矛盾を検出可能な仕組みがあれば、矛盾に伴う被害を予防・軽減可能である。以下にその具体的な方法を示す。

3.1 失効状態の矛盾への対策

2.1 で示した問題に関しては、図1の CA0 が発行する CRLを利用して、(あ)の失効状態の検査を行えばよい。しかし、この場合、以下の2つの課題が存在する。

(1) (あ)が見つからなかった場合、検証者の立場では、元々、(い)の上位に(あ)が存在しないのか、リポジトリに偶然存在しなかったのか判断不可能。

(2) (あ)の失効状態については、CA0 の“署名が正しい CRL”を調べる必要がある。

そこで、相互証明書(あ)-c に、以下の3つの情報をエクステンションとして含ませる。

(a) (あ)の有無(有る場合は識別子)

(b) CA0 の証明書の識別子とハッシュ値

(c) 失効していた場合の処理(検証拒否／続行など)

検証者は、(a)で(あ)が存在する事が分かった場合、(あ)を取得する。次に、(b) の識別子で示される CA0 の証明書を取得し、ハッシュ値を比較することで、正しい CA0 の証明書を入手する。続いて、CA0 の CRL を入手し、その署名を、該証明書で検証する。最後に、(あ)の失効状態を検査し、(c)に従って処理する。

3.2 有効期限の矛盾への対策

2.2 で示した問題に関しては、(ア)-1または 2 を入手し、(ア)-c と有効期限を比較すれば良い。しかし、以下の課題が存在する。

・(ア)-1 または 2 が見つからなかった場合、検証者の立場では、元々、(イ)の上位に(ア)-1 または 2 が存在しないのか、リポジトリに偶然存在しなかったのか判断不可能。

そこで、(イ)に、以下の2つの情報をエクステンションとして含ませる。

(d) (ア)-1 または 2 の有無(有る場合は識別子)

(e) 相互証明書の有効期限が(ア)-1 または 2 と矛盾している場合の処理

検証者は、当エクステンションを参照し、矛盾に対して対処する。

※ 各例では、CA1 は CA0 から証明書の発行を受けているが、CA0 が存在せず、CA1 が self-sign の証明書を保持している場合もある。この場合も、提案方式を応用することで、self-sign証明書の失効や有効期限を、相互証明書に対してチェックする。

4 おわりに

相互認証において、異なるドメイン間の CA の連携の不備により、同じ公開鍵を保証した複数の証明書の状態が矛盾し、安全性を損なう可能性がある問題を示した。さらに、当矛盾を検証者が検出可能な手法を示した。

[参考文献]

[1] ITU-T Recommendation X.509(1997E): Information Technology - Open Systems Interconnection – The Directory : Authentication Framework, 1997

[2] Public Key Infrastructure (PKI) Technical Specifications: Part A - Technical Concept of Operations, NIST PKI-TWG,September, 1998