マルチメディア通信と分散処理　111－28
コンピュータセキュリティ　20－28
（２００３．２．２８）

認証局の統合と分散の定式化とその考察

古賀 聡 *　　櫻井 幸一 †

概要　公開鍵暗号を利用した公開鍵認証基盤 (Public Key Infrastructure) においては、信頼のある機関として認証局 (Certification Authority) が本人性を保証する証明書を証明書ユーザーに発行する。実世界においてはこれら複数の認証局を用いた様々な信頼モデルが存在している。企業間の統合や、公開鍵認証基盤のグローバル化を踏まえ、異なる信頼モデルを統合化する必要性が求められている。また認証局のシステム面を考慮して、認証局が分散化した信頼モデルの構築の必要性も考えられる。よって本論文では認証局の統合、分散化について検討する。具体的には認証局の統合、分散化手順を定式化することで、証明書ユーザーへの影響や認証パス等の観点から考察を行う。

キーワード　公開鍵認証基盤, 認証局の統合化, 認証局の分散化

Formalization of Merger and Decentralization Methods of Certification Authority

Satoshi Koga *　　Kouichi SAKURAI †

Abstract— Public Key Infrastructures(PKIs) are very important techniques to support secure electronic commerce and digital communication on network. In real world, various PKI trust models exist and they need to be merge for some reasons. While, Certification Authority(CA) that issues the public key certificates need to be decentralize considering the aspect of security and system. In this paper, we study some methods of merger and decentralization CA and formalize these operations.

1　はじめに

公開鍵と所有者の本人性を保証する公開鍵証明書を発行する基盤である公開鍵認証基盤（Public Key Infrastructure）は、安全な電子商取引を実現するための技術として注目されている。その証明書を発行する信頼のある第三の機関は認証局 (Certification Authority) と呼ばれる。公開鍵認証基盤においては、様々な認証局が様々なポリシーのもとで運用されている。認証局が他の複数の認証局を信頼することで一つの信頼モデルを形成する。代表的な信頼モデルとして階層モデル、ブリッジ認証局モデルなどがあり、異なる信頼モデルが目的に応じて利用されている。

1.1　本研究の背景

世界規模でビジネスを展開する企業にとっては企業内のみではなく、企業外、または国を超えて安全な情報のやり取りが求められる。そのため、公開鍵認証基盤のグローバル化が進んでいる。即ち、世界中のいろいろな人と信頼関係の構築ができるような信頼モデルが要求される。それを実現する方法としては、異なる信頼モデルにおける認証局間で相互認証を確立する方法、ブリッジ認証局を用いる方法などが一般的に挙げられる。

また現実世界において、企業間での統合、買収などが頻繁に行われている。この場合、複数の組織を一つの組織に統合化するため、各々の企業が持つ信頼モデルについても同様のことが要求されることが考えられる。認証局間で相互認証を利用することで

* 九州大学工学部電気情報工学科 〒812-8581 福岡市東区箱崎 6-10-1, Department of Electrical Engineering and Computer Science, Kyushu University, 6-10- 1 Hakozaki, Higashi-ku, Fukuoka City, Japan, satoshi@tcslab.csce.kyushu-u.ac.jp
† 九州大学大学院システム情報科学研究院　〒812-8581 福岡市東区箱崎 6-10-1, Faculty of Information Science and Electrical Engineering, Kyushu University, 6-10-1 Hakozaki, Higashi-ku, Fukuoka City, Japan , sakurai@csce.kyushu-u.ac.jp

信頼モデルの統合化は達成できるが、認証パス構築、検証が複雑になるという問題点が指摘されている。そこで本論文では、相互認証を利用しない方法について検討する。具体的な方法として、複数の認証局を一つの認証局に統合化をすることで一つの信頼モデルを構築する。

一方で、認証局が分散した信頼モデルが要求される場合も考えられる。これからも電子署名が様々な場面に使われていくことを考慮した時、非常に多くの証明書を発行する必要がある。しかし、一つの認証局が発行できる証明書の数には限界があるため、利用者が増加するとともに認証局のシステム上の負荷も大きくなると考えられる。また別の理由として、セキュリティ面を考慮したときに一つの認証局の秘密鍵の漏洩した場合の影響の出るユーザーの数が多くなってしまうという問題点もある。また一つの組織内に複数の部門があるように、信頼モデルも複数の分散した認証局で管理したいという要求などが考えられる。

これらの理由から複数の認証局を用いた分散化モデルが要求される。

1.2 本論文の概要

本論文では認証局の統合化と分散化について検討する。信頼モデルの統合化については、相互認証モデル、ブリッジ認証局モデルを構築する方法などがある。また効率的な認証パス構築、検証のために、複数の認証局を一つの認証局に統合化することで、一つの信頼モデルの構築を考える。特に二番目の方法について、統合化手順の定式化を行い考察をする。

認証局の分散化は、一つの認証局から複数の認証局に分散化した信頼モデルの構築を考える。この分散化手順についても、統合化と同様に定式化を行うことで考察を行う。

1.3 本論文の構成

2章で信頼モデルの統合化の一般的な方法について説明する。そして認証局の統合化、分散化について簡単に述べる。3章で統合化手順、分散化手順の定式化を記述し、考察を行う。最後にまとめと今後の課題について述べる。

2 信頼モデル、認証局の統合化

本論文で対象とする信頼モデルは、従属階層型モデルとする。このモデルは階層型モデルの構造をとり、上位の認証局のみが下位の認証局に証明書を発行する。このモデルの信頼ドメイン内の証明書を検証する際には、ルート認証局から検証する証明書まで辿るだけで良いため、認証パスが比較的短く、認証パスの構築、検証が効率的とされている [1]。

2.1 信頼モデルの統合化

信頼モデルの統合化の一般的な方法として、認証局間で相互認証を行う方法がある。一般的な信頼モデルとして相互認証 (Cross-Certification)、ブリッジ認証局モデルについて説明する。

(1) 相互認証 (Cross Certification)

相互認証とは、ある認証局が他の認証局に証明書を発行する行為のことである [4]。これにより二つの認証局間で信頼関係が確立され、認証局を信頼する証明書検証者は他の認証局の信頼ドメインに属する証明書を検証することができる。

どのようにして相互認証が構築されるかを図 1 に従って説明する。二つの認証局 1、2 は、それぞれ互いの認証局に証明書を発行する。それらの証明書は相互認証証明書 (Cross Certificate) と呼ばれる。証明書検証者は相互認証証明書を検証することで、他の信頼ドメインの証明書ユーザーの証明書を検証できる。

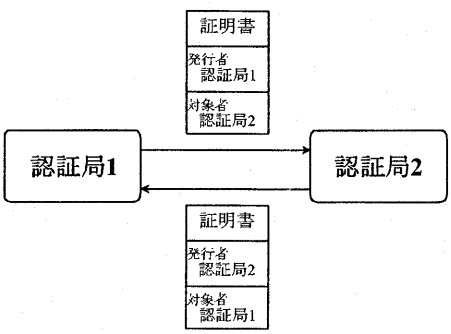

図 1: 相互認証モデル

相互認証を用いて信頼モデルの統合化を考える。各々の従属階層型モデルにおける一番信頼のある認証局 (ルート認証局) の間で相互認証を構築する。全ての信頼ドメイン間において信頼関係が確立できるようにするためには、全てのルート認証局間で相互認証を行う必要がある。

考察
このモデルの利点として以下のことが挙げられる [1]。
(1) 認証局間で相互認証を確立するだけで統合化が可能である。
(2) それぞれの信頼ドメインが別の信頼ドメインの影響を受けず独立に運用することが可能である。
(3) 一方のルート認証局の秘密鍵が危殆化しても、他方のルート認証局が発行する証明書に影響はない。

しかし、N 個の認証局の統合化を考えた時、構築するべき相互認証の数がオーダー N^2 必要となる。このようなモデルはメッシュモデルと呼ばれ [2]、認証パスは何通りも存在する。そのため、N が大きくなるほど認証パス構築が複雑化するという問題点がある [5]。

(2) ブリッジ認証局モデル
図 2 のように中心にブリッジ認証局をおくことで、メッシュモデルと比較して構築するべき相互認証の数を少なくすることができる。実際にこのモデルは広く利用されており、いくつかの実装が提案されている。具体的には、日本の政府認証基盤 (Government Public Key Infrastructure)、米国連邦政府の認証基盤 (Federal Public Key Infrastructure) 等で採用されている。

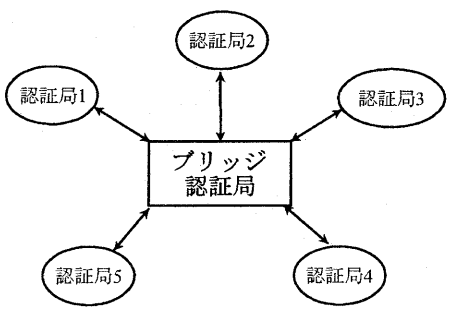

図 2: ブリッジ認証局モデル

統合化手順としては、各々の信頼モデルにおけるルート認証局とブリッジ認証局との間で相互認証を構築する。異なる信頼ドメインの証明書を検証するためには、ルート認証局とブリッジ認証局の間の相互認証証明書を検証する必要がある。

考察
統合化の際には、ブリッジ認証局と相互認証行えばよいため比較的容易に実現できる。また、新たに統合化したい信頼モデルがあった時、ブリッジ認証局と相互認証を行うだけでよいため、柔軟な統合化が可能である。

これら二つの方法は、認証局間で相互認証を構築することで実現できる。しかし、相互認証を用いることで異なる信頼ドメインの証明書を検証する際の認証パス構築、検証が複雑化するという問題点がある [5]。証明書を検証するためには証明書発行者の署名、証明書の失効情報等の検証を行う必要がある [6]。そのため、認証パスが長くなるほど証明書検証者の負担が大きくなってしまう。

2.2 認証局の統合化

相互認証を用いる信頼モデルでは、認証パスの構築、検証に手間がかかってしまうという問題点があった。そこで相互認証を用いないで他の信頼ドメイン間で信頼関係が構築できるようにするために、本論文では複数の認証局を一つの認証局の統合化することを考える。

統合後のルート認証局を決定し、そのルート認証局は他のルート認証局が発行していたエンティティ (中間認証局、証明書ユーザー) に新しい証明書を発行する (図 3)。本論文の 4 章で統合化手順の詳細について定式化を行う。

2.3 認証局の分散化

1 章で述べたように、認証局の分散化が必要とされる場面が考えられる。本論文では従属階層モデルにおける一つの認証局の分散化を行う (図 4)。分散化後の信頼モデルは、分散前と同じ従属階層型モデルの構築を考える。この分散化手順の詳細については 4 章で定式化して説明する。

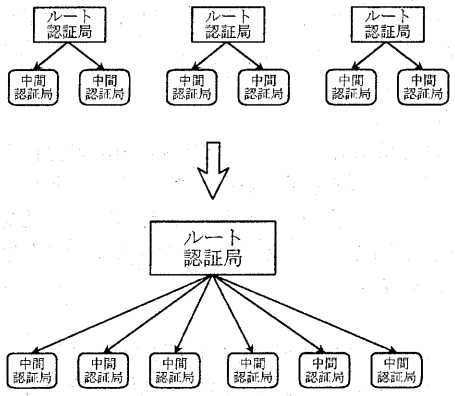

図 3: 認証局の統合化

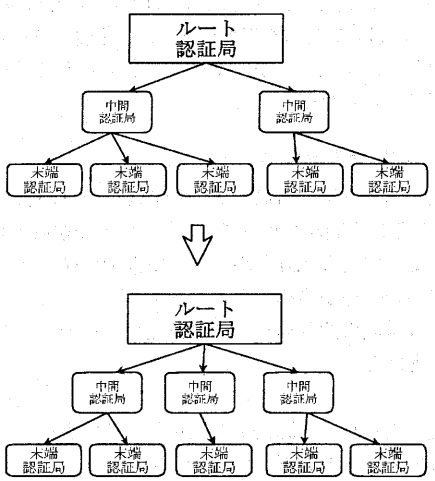

図 4: 一つの認証極を複数の認証局に分散化

3 定式化

公開鍵認証基盤における信頼モデルの定式化が文献 [2] で行われている。本論文では、文献 [2] で利用されている関数、定義を利用し、より簡単な形式で定義した。

3.1 定義

基礎となる集合を定義する。

ENT:エンティティ(entity) の集合。ここでのエンティティは証明書ユーザー、認証局を含む。

CERT:証明書 (certificate) の集合

CA:証明書の発行、管理等を行う認証局 (Certification Authority) の集合を表し、集合 **ENT** の部分集合である。

証明書の定義

認証局が発行する証明書は対象者の公開鍵を証明するもので、発行者の秘密鍵による署名が施されている。ここでの証明書は以下の簡単な形式をとる。

$$(x, y)$$

$x \in$ **CA** は証明書の発行者 (Issuer)

$y \in$ **ENT** は証明書の対象者 (Subject)

$C = (x, y)$ のとき以下の関数を定義する [2]。

$$I(C) = x, S(C) = y$$

本論文の中で用いる関数、手続きについて定義する。

(1)

関数 $ancestor(x)(x \in \mathbf{ENT})$ は x に証明書を発行しているエンティティの集合を返す。(文献 [2])

$$ancestor(x) = \{y \in \mathbf{ENT} \mid \exists cert \in \mathbf{CERT} \bullet S(cert) = x \wedge I(cert) = y\}$$

(2)

関数 $chillen(x)(x \in \mathbf{ENT})$ は x が証明書を発行しているエンティティの集合を返す。

$$childlen(x) = \{y \in \mathbf{ENT} \mid \exists cert \in \mathbf{CERT} \bullet I(cert) = x \wedge S(cert) = y\}$$

(3)

$NewCert(x, y), x \in \mathbf{CA}, y \in \mathbf{ENT}$ は発行者 x が対象者 y へ新しい証明書を発行する手続き。

$$NewCert(x, y)$$

3.2 認証局の統合化

統合化の対象となる信頼モデルを $\{PKI_1, ..., PKI_n\}$ と定める。これらは従属階層型モデルである。これらに属する全てのエンティティ、認証局、証明書をそれぞれ **ENT**、**CA**、**CERT** とする。PKI_i における一番信頼のあるルート認証局を $RCA_i(\in \mathbf{CA})$、そのルート認証局の集合 $\{RCA_1, ..., RCA_n\}$ を **RCA** とする。統合後も従属階層型モデルとなるため、そのルート認証局を決定する必要がある。このルート認証局を **RCA** から選んで決定する方法、もしくは新

しくルート認証局を構築する方法が考えられる。どちらの方法においても、統合後は一つの従属階層型モデルとなるが、後者は新しい認証局を構築するコストがかかるため、本論文では前者の方法を考える。

統合後にルート認証局となる認証局を $NCA \in \mathbf{RCA}$ とする。この統合化は以下の手順に従って行われる。

(統合化手順)

B1: $\mathbf{RCA} \leftarrow \mathbf{RCA} - \{NRCA\}$
B2:for $0 \leq i \leq n-1$
　$childlen(RCA_i) = \{C_{1i}, ..., C_{ki}\} = \mathbf{C}$
B3: $NewCert(NRC, NRC)$
　for $0 \leq i \leq n-1$
　　$NewCert(RCA_i, NRCA)$
　　$NewCert(NRCA, RCA_i)$
B4:for $1 \leq i \leq k$
　　$NewCert(NRCA, C_i)$

B1 でどの認証局を統合後のルート認証局とするかを決定する。
B2 でルート認証局が発行していたエンティティ($\in$ **ENT**) を求める。

B3 では、認証局の鍵更新のプロセスを利用して考える。認証局の鍵更新では以下の 4 種類の証明書を考える [2]。

$NewWithNew$:新しい認証局の公開鍵証明書 (自己署名証明書)
$NewWithOld$:以前の認証局から新しい認証局への証明書
$OldWithNew$:新しい認証局から以前の認証局への証明書
$OldWithOld$:以前の認証局の公開鍵証明書 (自己署名証明書)

B3 で以下のように 3 種類の証明書を生成する。新しいルート認証局の自己証明書 ($NewWithNew$) を生成し、全証明書ユーザーに配布する。また、RCA_i が $NRCA$ へ証明書 ($NewWithOld$) を発行する。この証明書により、RCA_i の信頼ドメインに属する証明書ユーザーは RCA_i の公開鍵証明書 ($OldWithOld$) により、新しいルート認証局 $NRCA$ を信頼することができる。それとは逆に、$NRCA$ が RCA_i へ証明書 ($OldWithNew$) を発行する。これは、新しいルート認証局を信頼している証明書ユーザーと、まだ信頼プロセスを行っていないユーザー間で証明書検証ができるようにするためである。全ての証明書ユーザーが新しいルート認証局を検証して信頼するプロセスが終了したら、この証明書は廃棄してよい。
B4 では **B2** で求めた集合全体に対し、$NRCA$ が証明書を発行する。

(考察)
(1) 統合後の信頼モデル
統合後は従属階層型モデルとなる。このモデルでは認証局間で相互認証を用いないため、認証パスの構築、検証が統合前の信頼モデルと同様に複雑になることはない。また、認証パスの長さも統合前と同じとなる。

(2) 認証局の運用コスト
統合後、認証局の数は減少する。そのため、認証局の運用コストが軽減できる。

(3) エンドユーザーの負担
エンドユーザーは新しいルート認証局を信頼するために、$NewWithOld$ 証明書、$NewWithNew$ 証明書を検証する必要があるため、証明書の入手、検証する手間がかかってしまう。また、エンドユーザーの数が非常に多い場合、新しいルート認証局を全エンドユーザーが信頼するまで時間がかかることが予想され、その間は $OldWithNew$ 証明書を用いて認証する必要がある。

(4) 安全性
ルート認証局の秘密鍵危殆化はすべてのエンドユーザーに影響が出てしまうため、秘密鍵の管理は厳重かつ慎重に行う必要がある。

認証局の統合化を行う場合、相互認証を用いる方法と比較して認証パス構築、検証を効率的に処理することができる。しかし、相互認証を用いる方法と比較して、エンドユーザーの負担がかかることが欠点として挙げられる。そのため、相互認証を用いるモデルと比較して柔軟性が低いと考えられる。

3.3 認証局の分散化

統合化と同様に従属階層モデルの場合を考える。分散したい認証局を $B \in \mathbf{CA}$ とし、複数の分散した認証局 $\{B_1, ..., B_n\}$ を構築する。認証パス構築、検証の効率化を考慮して、相互認証を用いない方法で実現する。

(分散化手順)

D1:ENT $\leftarrow \{\mathbf{ENT}\} \cup \{B_1, ..., B_n\}$
D2:$ancestor(B) = A \in \mathbf{CA}$
D3:for$0 \leq i \leq n$
$NewCert(A, B_i)$

D2 では分散前の認証局に証明書を発行していた認証局を求める。
D3 で **D2** で求めた認証局から分散する複数に認証局に証明書を発行する。

(1)B = 中間認証局の場合
上記の分散化手順により、複数の認証局が同じ階層の深さに構築される。

(2)B = ルート認証局の場合
ルート認証局の公開鍵証明書は自身の秘密鍵により発行者、対象者が同一である。ゆえに、B がルート認証局の場合、**D2** において $ancestor(B) = B$ となり、結果的にルート認証局 B の階層の下に新しい中間認証局 $\{B_1, ..., B_n\}$ が構築される。

(考察)
(1) 分散化後の信頼モデル
分散化後は一つの従属階層型モデルとして機能する。そのため認証パスが相互認証を用いる方法と比較して効率的に処理できる。また、複数の分散した認証局によるモデルの構築が実現できるため、1章で取り上げたシステム、セキュリティ面の問題点が改善できる。

(2) 認証局の運用コスト
認証局の数が増加するため、認証局の運用コストは大きくなる。

(3) エンドユーザーの負担
状況に応じて他の中間認証局、エンドユーザーは新しく構築された認証局から証明書を発行してもらう。新しい認証局は新規のユーザーにのみ証明書を発行するようにすれば、既存の信頼モデルを利用していたエンドユーザーに負担はない。

4 おわりに

本論文では認証局の統合化、分散化の要求に対して、相互認証を利用しない統合化、分散化手順の定式化を記述し、考察を行った。一般的な信頼モデルである従属階層型モデルについて考えたが、今後の課題として様々な信頼モデルにおける統合化、分散化について検討する必要がある。

参考文献

[1] 谷口, 金融業界における PKI・電子認証について, 日本銀行金融研究所/金融研究, 2002.4.

[2] A. Nash, W. Duane, C. Joseph and D. Brink, PKI - Implementating and Managing E-Security, Osborne Media Group, 2001.

[3] M. Henderson, R. Coulter, E. Dawson and E. Okamoto,Modelling Trust for Public Key Infrastractures,The 7th Australasian Conference on Information Security and Privacy (ACISP 2002), Lecture Note in Computer Science, 2384, 2002, 56-70.

[4] "PKI 関連技術解説", 情報処理振興事業協会セキュリティセンター, http://www.ipa.go.jp/security/pki/

[5] C. Adams, S. Lloyd, PKI 公開鍵インフラストラクチャの概念, 標準, 展開, (株) ピアソン・エデュケーション, 2000.

[6] Internet X.509 Public Key Infrastructure Certificate and CRL profile, RFC3280, 2002.4.