高セキュリティを実現したエレクトロニック・コマース向け認証局システム

1T－2　梅澤克之　洲崎誠一　梅木久志　宮崎誠治
（株）日立製作所 システム開発研究所

1. はじめに

情報・通信分野の新展開として，インターネットを利用した電子商取引など新しいサービスを実現しようとする動きが活発である。インターネットにおける安全な電子商取引を実現する標準プロトコルとして SET，および国内共通 EC プラットフォームとして SECE が提案されている。SET/SECE では，電子決済時に証明書を用いることで本人認証を行い安全な電子商取引を可能にしている。この証明書を発行・管理するのが認証局システムである。正当な証明書を用いることが電子商取引の安全性の要であるので，認証局自身のセキュリティは重要である。そこにはLAN・DBの盗聴・改ざん，オペレータの不正操作などの脅威が存在する。

このようなセキュリティ上の脅威に対し，ファイアウォールによるサーバの分離や内部 LAN，DB の暗号化，オペレータ合議制アクセス制御，ログ管理などの対策を施した認証局システムを開発した。本稿では上記対策のうち，特にユーザ権限レベル，処理権限レベルに基づく合議制アクセス制御機能について報告する。

2. 認証局のセキュリティ

安全な電子商取引は証明書の正当性を前提として成り立つものであるので，それを発行・管理する認証局の安全性が保証されていなければならない。このような要求に対し，外部からの不正に加えて，内部オペレータの不正も考慮して設計する必要があると考え，認証局のセキュリティを高めるために以下のような機能を実現した。

1. ファイアウォールによるインターネットからの証明書発行を受け付けるためのフロントエンドサーバと，認証局内部を管理するバックエンドサーバの分離機能。
2. 認証局内部 LAN 上のデータと証明書データベース内のデータの暗号化機能。
3. 単独オペレータによる不正を防止するため，重要情報に対する処理操作では複数のオペレータによる確認を行い，合意がとれた場合にのみサービスを実行する合議制アクセス制御機能。
4. 不正アクセスや各種内部処理について，事後になっても確認できるようにするログ管理機能。

High Security Certification Authority for Electronic Commerce,
Katsuyuki UMEZAWA, Seiichi SUSAKI, Hisashi UMEKI, Seiji MIYAZAKI,
Systems Development Laboratory, Hitachi Ltd.

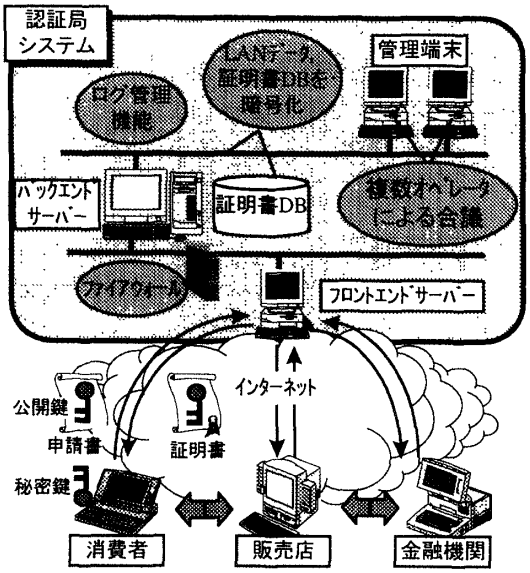

図1 認証サービスの構成

3. 合議制アクセス制御機能

本章では前述の各種セキュリティ機能のうち合議制アクセス制御機能について詳しく述べる。

合議制アクセス制御機能とは，オペレータに与えられたユーザ権限レベルとその機能を利用するために必要な処理権限レベルにより，単独のオペレータによる不正処理を防ぐための管理端末サービスの利用を制限する機能である。

以下に静的な定義情報としてのユーザ権限レベルと処理権限レベルについて，さらに動的なログイン情報について例を用いて示し，その後それらを用いた複数ユーザの合議について述べる。

3.1 ユーザ権限レベルと処理権限レベル

ユーザ権限レベルとは，管理端末サービスの利用を制御する要素の一つであり，各オペレータ毎に付与されたアクセス制御用データである。ユーザ権限ファイルは，ユーザ ID，パスワード，ユーザ権限レベル，名前（オプション）のリストである。

表１ ユーザ権限ファイル

ユーザ ID	パスワード	ユーザ権限レベル	名前
umezawa	********	レベル３	梅澤
susaki	********	レベル１	洲崎
umeki	********	レベル２	梅木

処理権限レベルとは，管理端末サービスの利用を制御する要素の一つであり，個々の管理端末サービス毎に付与されたアクセス制御用データである。処理権限ファイルは，管理端末サービス，ユーザ権限レベル，およびユーザ数(ユーザ数が2以上の場合は，それらユーザ権限レベルを持った人の合議が必要であることを示す)のリストである。

表2 処理権限ファイル

項目	管理端末サービス	ユーザ権限レベル	ユーザ数
1	公開鍵，秘密鍵を作成する	0	1
		1	1
		2	3
		3, 4, 5	0
2	証明を与える	0	1
		1	1
		2	2
		3, 4, 5	0
:	:	:	:

この例では，ユーザ権限レベルとユーザ数による処理権限の設定を示しているが，グループや役割などを指定することにより，更に細かくユーザの制御を行うことができる。

3.2 ログイン情報

以上の 2 つのファイルは静的な定義情報であるが，現在，管理端末サーバにログインしているユーザ情報を把握するために動的にログイン情報を管理する。

表3 ログイン情報

ユーザ ID	ユーザ権限レベル	IP アドレス	ポート番号
susaki	レベル1	123.123.123.123	10000
umeki	レベル2	123.123.123.124	10000

ログイン情報は，ユーザ ID，ユーザ権限レベル，ログイン元の管理端末クライアントの IP アドレス，及びポート番号のリストである。これは各管理端末クライアントから管理端末サーバにログインしたときに管理端末サーバによって更新される。

3.3 複数ユーザの合議

ある管理端末サービスについて，処理権限ファイルの対応するユーザ数の項目が n(n≧2)の場合には，必要なユーザ権限レベルがある n 人のユーザが認めた場合にのみ，その管理端末サービスが実行可能となる。例えば前節の例で，“証明を与える”という処理は洲崎は 1 人で行えるが，梅木が行おうとした場合，レベル 2 以上の他のオペレータによる合議が必要であることを示している。

このような複数オペレータの合議が必要な場合の管理端末サービスの処理フローを図 2 に示す。図 2 において，オペレータ A がある管理端末サービスを行おうとした場合，ユーザ権限レベルおよび処理権限レベルから合議が必要と判断されたとき，管理端末サーバはログ

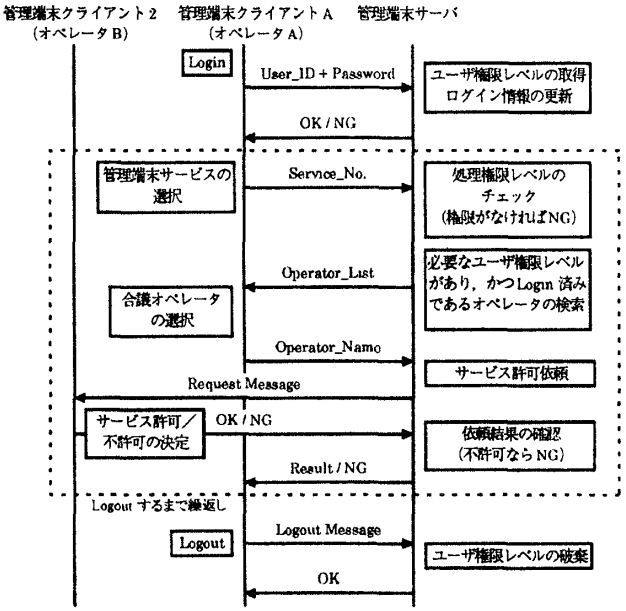

図2 複数オペレータの合議が必要な場合の処理フロー

イン情報から必要なユーザ権限レベル以上のオペレータを検索し，そのリストをオペレータ A に返す。オペレータ A は合議を求めるオペレータを指定人数分選択し，管理端末サーバに送る。管理端末サーバは選択されたオペレータ(この場合オペレータ B)に合議要求メッセージを送り管理端末サービスの許可／不許可が決定される。合議を求めたすべてのオペレータが許可しなければ，その管理端末サービスを実行することはできない。また合議を行う各オペレータがそれぞれ個別の管理端末からすでにログインしている必要があり，合議を行えるユーザ権限レベルを持ったオペレータが必要な人数以上ログインしていない場合は，合議を行うことはできずその管理端末サービスは実行することはできない。

4. おわりに

SET 及び SECE に準拠する証明書発行機関である認証局を開発し，内部 LAN や個人情報データベースの盗聴や改ざんに対しての，LAN 上のメッセージ暗号化やデータベース暗号化機能に加え，オペレータの不正操作に対して，ユーザ権限レベルや処理権限レベルの設定を可能とし，複数人の合議による操作などの利用制限機能を実現した。これにより外部からの不正に対してのみならず，内部不正に対しても安全性を向上することができた。

参考文献

(1) SET Secure Electronic Transaction Specification. Book 1, Book 2, Book 3. Version 1.0. May 31, 1997.

(2) CCITT X シリーズ勧告(その 5)

(3) 宝木他，“マルチメディア向け高速暗号アルゴリズム Hisecurity-Multi2 の開発と利用方法”，1989 年情報理論とその応用，暗号と情報セキュリティジョイントワークショップ資料，電子情報通信学会，pp. 167-173(平 1-8)