コンピュータセキュリティ　5－5
（1999．5．21）

# SPKI/SDSIの承認証明書のフレームワークを利用した電子学生割引証

菊池 浩明　　川倉 康嗣
東海大学　　東芝

**概要:** SPKI/SDSIは，本人認証と権限委託の二種類の証明を一様な証明書の枠組みで実現しようとする試みである．本発表では，この枠組みの学生運賃割引証への適用を考察する．

# Student discount problem in electronic tickets and SPKI/SDSI freamwork for authorization

Hiroaki Kikuchi　　Yasushi Kawakura
Tokai university　　TOSHIBA corporation

**Abstract:** SPKI/SDSI is a framework in which both user authentication and access authorization to be dealt with an uniform certificate format. In this paper we studies some issues in electrionic tickets in conjunction with student discount and present a solution made by the SPKI/SDSI framework.

## 1　はじめに

現在の電子商取引がひとつの技術的な課題に直面している．アクセス制御である．インターネットにおける有料のWebコンテンツ，小切手の発行権限などから，イントラネットでの機密データへのアクセス制限，稟議書の承認まで，サービスが多様化していけば行くほどのアクセス制御の壁を避けられなくなっている．もちろん，基本的なパスワード認証やX.509に従った公開鍵証明書による認証基盤PKIX (Public-key Infrastructure with X.509) を適用すれば，現状の技術である程度の解決は計れる．しかし，その適用には制約がある．なぜならば，PKIXはその利用者が誰であるかを保証する（認証）技術であり，権限をだれに与えるか（承認）は異なる独立の機能であるからだ．

例を示そう．ある会社では課長になったら自由にタクシーチケットを切れる．この例では,「課長」であることさえ示せば(認証),「タクシーチケット」(権限)を使える．課長であることを任命する人と課長の権限をみとめる人が一致しているからである．しかし，身元が明らかであるといってむやみに権限が与えられるわけではない．写真付の従業員証と課長の名刺を持っていても，そこに記されている会社名を知らない場合があるし，名刺を偽造しているかも知れないので，タクシー料金をツケにしておくわけにはいかない．たとえよく知られた会社名の従業員証を持っていても，そこでトラブルが起きたときにその会社が責任を持つことは全く保証されていない．それゆえ,「タクシーチケット」が必要なのである．

そこで，認証基盤に「タクシーチケット」の機能，すなわち，権限の証明書を加えることが試みられている．これには，1. X.509の枠組みを利用した属性証明書[1, 2, 3], 2. SPKI(Simple Public Key Infrastructure)[4], 3. SDSI(Simple Distributed Security Infrastructure)[5]の3つがある．後者2つは，PKIXの問題点に関して

共通の認識と設計思想を持っており，標準化作業を協調して進めている．これらと前者の PKIX の本質的な相違は何であろうか？Carl Ellison がわかりやすい説明をしている [6]．まず，証明書には次の 3 つの種類がある (図 1参照)．

1. ID 証明書
   認証のための証明書で，名前と公開鍵の対応を保証する．X.509 が代表例．

2. 属性証明書
   承認のための証明書．名前と権限の対応を保証する．

3. 権限証明書
   SPKI/SDSI で主に利用される証明書．権限と公開鍵の対応を保証する．

そして，PKIX は ID 証明書と属性証明書によるアクセス制御を目指すのに対し，SPKI/SDSI は権限証明書を基本とするアクセス制御を目標とする．

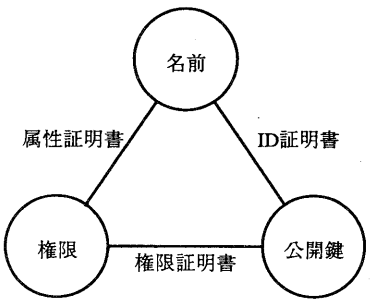


図 1: 属性証明書と権限証明書

さて，SPKI/SDSI は本当に PKIX を完全に置き換えるほど強力なセキュリティ基盤となり得るだろうか？我々の様々なアクセス制御の要求に適しているのはどちらのアプローチなのだろう？両技術を検証するために，本研究では，タクシーチケットの例を一般化した学生割引証モデルを考える．モデルの上で，アクセス制御に対する要請と問題点を抽出し，SPKI/SDSI の枠組みでの実現を検討する．その上に生じる課題を明らかにし，より現実的なセキュリティ基盤の構築に向けての提言をなす．

# 2 学生割引証モデル

## 2.1 学生割引証明書

学割証は，鉄道というサービスへの乗車 (アクセス) を制御する証明書の例である．各学校長への発行権限の委託や，分散処理された切符販売窓口など興味深い特徴を持っており，その性質はそのまま分散ネットワーク環境のアプリケーションに適用できる点でアクセス制御のモデルとして望ましい．

まず，実際の学割証について述べる．正式には「学校学生生徒旅客運賃割引証」といい，英語では，a certificate of qualification for a student(s') discount, つまり,「学生割引を受ける資格者であることの証明書」を意味する．学割証には表 1の情報が記載されている．これ以外に，乗車券購入の際に記載されると思

表 1: 学割証に記載されている情報

| | | |
|---|---|---|
| 1. | シリアル番号 | その大学での通し番号 |
| 2. | 乗車船区間 | ○駅から△駅まで□経由 |
| 3. | 乗車券の種類 | 片道，往復，連続，周遊 |
| 4. | 使用者 | 部科及び学年, 証明書番号, 氏名, 年齢 |
| 5. | 割引率 | 2 割り |
| 6. | 有効期限 | 発行から 3ヶ月 |
| 7. | 発行年月日 | |
| 8. | 発行者 | 所在地, 学校名, 代表者名, 代表者の印 |
| 9. | 証明 | 割り印 |

われる運賃などの情報を書く欄がある．

印をディジタル署名に置き換えて考えると，見事なほど X.509 証明書のフォーマットに似ている．最も大きな違いは，2,3,5 といったサービス（割引）の内容に関する情報である．ただし，2 と 3 は利用者が使うときに自分で記入する．割引の対象が「旅客鉄道会社線」の 1 種類しかないので，この情報を偽っても実害はないためであろう．裏面には，割引証の注意事項（利用ポリシー）が明記されている．

- 旅客鉄道会社の指定学校（通信教育の学校を除く）の学生が，片道 100km を越える区間を旅行する場合は，割引普通乗車券を一人一回に限って購入できる．
- 事項は発行者において記入し，発行者の職印がないと訂正出来ない．

- 記名人に限って利用でき，購入した乗車券を記名人以外は利用できない．
- 所定の証明書（つまり学生証）を携帯しないときは使用できない．

## 2.2 学割証への要求条件

学割の一般的な目的は，経済的に制約のある学生を援助して学業を奨励すること，にある．ただし，その目的に応じて次に示すいくつかの種類があることに注意が必要である．

a. 販売推進を目的とするもの．ボーリング場，床屋．

b. サービスの差別化を目的とするもの．スカイメイト（混雑時の顧客を空いている時期/時間帯にまわして，少しでも効率を稼ぐ）

c. 社会人になったときに還元されることを目的とするもの．ソフトウェアのアカデミックパッケージ（学生の頃から使わせておけば将来社会に分散したときに各々で利用者を増やすキャリアになってくれる）

d. 見返りがないもの．JR の乗車券．

e. その大学の学生だけにサービスしたいもの．ディジタルライブラリのサイトライセンス．

学割証モデルでは，この d あるいは c に近い．それゆえに，発行枚数を制限して，他人に譲与したりする不正行為を防止する必要がある．また，a,b,c のモデルでは割引の為の証明書は設けず，学生証を直接示すだけでサービス（割引）が提供される．なぜ，学生証だけでなく，学割証明書が必要なのだろうか？これにはいくつかの理由が考えらえる．

**理由 1.** 認められた学校の識別が困難であるから．学校にも様々な種類があり，社会人を対象とした通信教育のように学割が認められない学校もある．かといって，対象となる認可された学校を全て窓口で判断するのはコストがかかる．

**理由 2.** 学生証は定型ではなく，偽造されていても判断できないから．学校によってまちまちの形式をしていて，本物かどうか判定するのは困難である．

**理由 3.** 複雑な発行制約がある．一人に年間発行する学割の枚数に制約があり，それを判定するためには窓口で発行履歴を参照しなくてはならない．

## 2.3 ID 証明書による電子学割の実現

ここで，学割のサービスを電子的に実現する方法を考える．もし，

$$\text{学生} = \text{割引がある人}$$

を仮定すると，権限の問題が認証に帰着できるので，現在の PKIX の枠組みの範囲で次のように実現できる．

まず，次の主体を考える．

- 文部省: 認可された学校を管理する発行局．$ME$
- 学校: 学生を管理し，学生証を発行する発行局．$a_1, \ldots, a_m$
- 学生: どこかの学校に属する利用者．$c_1, \ldots, c_n$
- 窓口: 乗車券発行サービスの提供者．$m_1, \ldots, m_l$

各々公開鍵対を持ち，秘密鍵を管理する．文部省から学校，学校から学生へと公開鍵証明書を階層的に発行する．階層のルートは文部省であり，その公開鍵は全ての主体に知られている (図 2)．

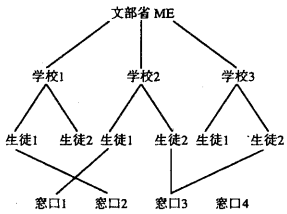


図 2: ID 証明書による学割の実現

このモデルの上では，前節の理由 2（学生証の偽造）が学生証へのディジタル署名で解決されている．文部省の公開鍵さえあれば誰でも検証できるので，窓口が分散されていてもコストの問題ない．学生が対応する秘密鍵を持っていることの証明は，窓口が任意に与えた乱数に署名することで示される．

しかし，文部省が認可する学校の中に通信教育などの例外があると，理由 1 への反証には不十分である．物理的な学生証のように発行枚数制限の情報を学生証に追加するわけにもいかないので（署名が棄却する），理由 3 にも対応できない．結局，文部省は学

割(窓口)のために学校を管理しているわけではなく，認証の仕組みを承認に使っているところに無理が生じている．

### 2.4 属性証明書による実現

そこで，ID 証明書に属性証明書を併用することで，よりもよりきめの細かいアクセス制御の実現を検討する．

属性証明書 (attribute certificate) とは，ID 証明書に属性を追加するための証明書であり，ID 証明書とは異なり対応する公開鍵対は持たない．属性証明書に関する標準化活動は，IETF の TLS (Transport Layer Security)-WG の中で進められており，いくつかのインターネットドラフト [1, 2] が提案されている．SIGNED オブジェクトである点や，OID に関する情報は X.509 と同一である．特徴的なのは，有効期限が GeneralizedTime(2000 年問題をクリアしている）ところや，属性証明書の持ち主の記述 (Subject) が，シリアル番号や GeneralName の選択子になっているところである．属性 (attributes) の定義は，単に Attribute オブジェクトの SET で記述されることになっているが，アプリケーションに依存するところも大きくまだ流動的である．

この属性証明書を ID 証明書と組み合わせると，先の学割証は表2で与えられる証明書の組で実現できる．$X_1, X_2, X_3$が ID 証明書で，$C_1, C_2$が属性証明書である．ACL はアクセスコントロールリストを意味する属性証明書であり，自己署名されていて各エンティティが “JR” のポリシーを正しく参照するために用意されている．“JR” は ID 証明書で識別される名前であり，グローバルな名前空間での一意性が保証されている．ここでは，前節と同様に，文部省 (ME)-学校 $a_i$-学生 $c_j$の階層構造を仮定する．

学生は，学割窓口に $X_1, X_2, X_3$を示して自分の ID を証明する．同時に，属性証明書 $C_1, C_2$を提示して学生割引を受ける権限を持っていることを証明する．ID 証明書だけでは適用できなかった理由 1(認可された学校) と理由 3(発行制約) は各々文部省と各学校に権利委託することで満足している．

ただし，属性証明書には次のような潜在的な問題が存在する．

1. 属性は ID よりも頻繁に変更される．役職やプロジェクトの委員などの例からも明らかで，それゆえに，ID 証明書の場合よりも CRL(失効リスト) の肥大化が深刻である．
2. 属性証明書によって，分散されたサーバの間でアクセス制御のための情報を無矛盾に同期しなければならない問題は解決される．しかし，その情報を，今度は利用者自身が管理して携帯するコストが代って生じる．もしも，公開ディレクトリーが普及していれば，属性証明書はそこに管理しておき，利用者は ID 証明書だけを管理すればいいのだが，公開ディレクトリでのアクセス制御などの問題が残る．
3. ID 証明書を権限の主体として流用する問題．文部省による名前空間の ID に対して JR が横から権限を与えることは正しいのだろうか?[1] 不正などによる問題が生じたときに，文部省名前空間の発行局はどこまで保証するのだろうか．CPS で用途を制限するポリシーを明記するのもこの点を避けるためである．
4. 果たしてグローバルな名前空間は本当に実現可能か．

## 3 SPKI/SDSI

### 3.1 概要

SPKI(Simple Public Key Infrastructure) は，Carl Ellison の論文 [4] をきっかけにした公開鍵基盤の試みであり，IETF を中心に現在標準化が行われている．一方，SDSI(Simple Distributed Security Infrastructure) も，同じ年同じ学会で発表された Rivest と Lampson の論文 [5] が発端であり，W3C で標準化が進められている．二つの試みは，共通の設計思想を持ち，協調して標準化されており，ここでも同一視して扱う．

**名前空間** X.509 公開鍵証明書のフォーマットでは、階層的な CA を想定した証明書で、X.500 のグローバルにユニークな名前を用いている。この名前スキームはユニークであるがゆえに柔軟性がない。それに対して SPKI/SDSI では、名前はローカルで相対的な名前やニックネームでも使えるようにして、柔軟性を持たせた。また、X.509

[1] AT&T 研究所の Joan Feigenbaum は，この問題を免許証が日常生活での認証手段として利用されていることに例えて否定している

表 2: 属性証明書による実現

| 証明書 | 発行者 | 主体 | 委任 | 権限 | 期限 | 署名者 |
|---|---|---|---|---|---|---|
| ACL | Self | "JR" | - | 学割 | 無期限 | $K_{JR}$ |
| $C_1$ | "JR" | "学校 $a_i$" | T | 学割 Issue | 無期限 | $K_{JR}$ |
| $X_1$ | "JR" | $K_{JR}$ | - | - | 年 | $K_{CA}$ |
| $C_2$ | "学校 $a_i$" | "学生 $c_j$" | F | 学割 Use | 3ヵ月 | $K_{p_i}$ |
| $X_2$ | "学校 $a_i$" | $K_{p_i}$ | - | - | 期 | $K_{ME}$ |
| $X_3$ | "学生 $c_j$" | $K_{c_j}$ | - | - | 4 年 | $K_{p_i}$ |

公開鍵証明書の階層構造に対して，SPKI/SDSIでは、任意の関連付けが可能であり、固定したCAを必要としない。逆にいえば、誰にでもCAになりうる柔軟性を持っている。

**S 式による表現** X.509 の ASN.1 抽象構文と BER 符号化に対して，SPKI/SDSI では S 式を用いて全ての証明書を表現する．公開鍵証明書に必要な項目には，発行者 (Issuer)，主体 (Subject)，権利委任 (Delegation)，権限 (Authorization)，有効期限 (Validity) の 5 つがあり，これを，

$$< I, S, D, A, V >$$

の "5-Tuple" で表す．

**権限縮約** 次のような場合、"5-Tuple"は縮約できる。

$$< I_1, S_1, D_1, A_1, V_1 > + < I_2, S_2, D_2, A_2, V_2 > \\ =< I_1, S_2, D_2, A, V >$$

ここで次を満たしている．

$$S_1 = I_2, D_1 > D_2$$
$$A = A_1 \cap A_2, V = V_1 \cap V_2$$

## 3.2 SPKI/SDSI による実現

ID 証明書と同様に，SPKI/SDSI を用いて学割証モデルを考える．まず，前節のモデルと同様に，次の主体をおく．

- $JR$: 権限委託者（JR の学割管理部）
- 校長: 学生を証明し，学割証を発行する人. $p_1, \ldots, p_m$
- 学生: どこかの学校に属する利用者. $c_1, \ldots, c_n$
- 窓口: 乗車サービス提供者. $m_1, \ldots, m_l$.

校長 $p_i$の公開鍵を $K_{p_i}$, 学生 $c_j$の公開鍵を $K_{c_j}$ とする．

学生 $c_j$が校長 $p_i$の学校に属するとき，次の 5-tupple 形式の証明書を各々が発行する (図 3).

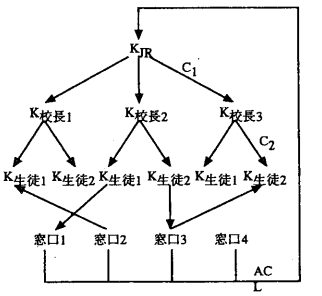


図 3: SPKI による学割証の実現

$ACL$: <Self, $K_{JR}$, N.A., 学割, 無期限>
$C_1$: < $K_{JR}$, $K_{p_i}$, T, 学割 Issue, 無期限>
$C_2$: < $K_{p_i}$, $K_{c_j}$, F, 学割 Use, 3ヶ月>

ここで，$ACL$ の "Self" は主体が自己署名していることを表す．$C_1$は「学割発行委任証明書」であり，$C_2$が「学割証」に相当する．前節のモデルの「学生証」に相当する証明書は，$C_2$を発行するときに $p_i$に示すときに使われるだけで，ここには明に出てこない．

学生 $c_j$は，$C_1$, $C_2$を窓口に提示する．このとき，$K_{c_j}$の持ち主であることを証明するために，窓口からのチャレンジに対して秘密鍵で署名してみせる．

窓口は，まず，受取った証明書を検証する．$C_1$の検証に必要な $JR$ の公開鍵は $ACL$ に書いてある。$C_2$の検証に必要な校長 $p_i$ の鍵は $C_1$ に書いてある。次に，自分が持っている $ACL$ を含めて縮約して

$R$ : <Self, $K_{c_j}$, F, 学割 Use, 3 ヶ月>

を得る．ただし,「学割 Issue」は「学割 Use」を包含する属性とする．こうして乗車サービスに関するアクセス制御が実現する．

表 3: 実現方式

| | ユーザ | 検証者 | ボトルネックと適用限界 |
|---|---|---|---|
| 1. | ID 証明書 | 列挙型 ACL | ACL 管理、単一検証者 (非分散) |
| 2. | ID 証明書+属性証明書 | 条件型 ACL | 名前空間管理, クローズドな分散環境 |
| 3. | 権限証明書 | 条件型 ACL | 鍵管理、オープンな分散環境 |

### 3.3 考察

- SPKI/SDSI と X.509 の最も大きな違いは，権限委託が閉じているか否かという点である．X.509 では窓口と文部省が異なる主体であったのに対して，SPKI/SDSI による実現では権限の委託が窓口自身に返ってきている．これにより，認証の責任範囲を明確にしている．
- 上のモデルでは問題を分かりやすくするため，校長が直接学割を発行することにしたが，校長が更に学生課に学割発行の権限を委託する証明書を発行しても良い．学生が管理しなくてはならない証明書の数は増えるが，縮約の結果は変らない．
- 縮約は窓口しか出来ないことに注意せよ．従って，学生は $C_1$ から $C_2$ までの全ての証明書を管理して窓口に提出しなくてはならない．
- SPKI/SDSI のモデルには名前の概念がない．従って，校長が代ったりした場合には新たに証明書を発行し直す必要がある．
- 学割に関する権限として，Issue は Use を包含すると定義するのは正しいか．SPKI の delegation とは，自分の権利の一部を他人にも分け与える場合の考え方であり，学割証のように発行者 (校長) は利用する権限を持たない場合には適用できないのではないか。

### 3.4 実現方式の整理

電子学割証を実現するには，表 3の方法がある．

- 1 と 2 の差．権限の証明者 (校長) と検証者 (窓口) とを分離して，証明者を限定するためのアクセス制御を JR から校長に委託した．
- 2 と 3 の差．名前をなくすことにより認証基盤が不要になった．ただし、秘密鍵管理が新たに負担となっている．
- 3 より 2 が有利になる場合．既存の認証局によって (ローカルに) 名前空間が確立できている場合．

## 4 おわりに

ネットワーク環境のアクセス制御の問題を，学割証モデルに定式化し，要求条件を明らかにした．そのうえで，X.509 による ID 証明書による実現と，属性証明書による実現，及び，SPKI/SDSI のフレームワークによる権限証明書による実現を示し，検証効率などの点から比較検討を行った．

## 参考文献


[1] Farrell, S., "An Internet AttributeCertificate Profile for Authorization", `draft-ietf-tls-ac509prof-00.txt`, 1998

[2] Farrell, S., "TLS extensions for AttributeCertificate based authorization," `draft-ietf-tls-attr-cert-01.txt`, 1998

[3] 川倉，ID 証明書と属性証明書の併用によるアクセス制御方式，コンピューターセキュリティシンポジウム'98, pp.97-102, 1998

[4] C. Ellison, Establishing Identity Without Certification Authority, proc. of USENIX Security Symposium, 1996

[5] R. Rivest and B. Lampson, SDSI - A Simple Distributed Security, 1996 USENIX Security Symposium, proc. of USENIX Security Symposium, 1996

[6] C. Ellison, Raising The Security Bar, IETF 発表資料, 1998 (*http://www.clark.net/pub/cme/jhuapl.ppt*)

[7] Inetnet Public Key Infrastructure, Part I: X.509 Certificate and CRL Profile, 1996,