個人情報の扱いを考慮したアクセス制御の一方法

齋藤 孝道† 梅澤健太郎† 奥乃 博†
Takamichi SAITO Kentaro UMESAWA Hiroshi G OKUNO

†東京理科大学
Science University of Tokyo

概 要

インターネットにおけるWWW (World Wide Web) サーバなどへのアクセスの際，個人情報漏洩などの不安から，匿名でアクセスをしたい要求がある．一方，それなりの対価が得られるのであれば，個人情報の一部をサーバに提供してもよいと考える利用者もいる．また，サービスの提供者の視点に立てば，年齢，性別などに応じて，違ったサービス内容を提供したいという要求もある．本論文では，このような，一見，背反するような要求を実現するアクセス制御方式を提案し，その適用例を示す．また，その利用についての安全性などの視点から考察をする．

1 はじめに

公開鍵暗号を用いた安全な通信のためにはインフラストラクチャの構築が不可欠である．それはPKI (Public Key Infrastructure) と呼ばれ，その枠組みの一つとして，PKIX (PKI with X.509) が提案され，複数の企業や機関でその実装が進められている．PKIXはX.509証明書のようなID証明書を発行する母体として認証局 (CA，Certificate Authority) を使用し，証明書としてはX.509 を用いる．PKIXは，元々は認証の枠組みとして提案されたが，次のようにその機能を分けて考えると，アクセス制御にも利用できる:

(1) 認証：公開鍵とID情報（名前など）の結びつきを保証するID証明書を用いて，本人であることを示す.
(2) 権限管理：属性証明書 (一般的にはサーバのACL (Access Control List)) を確認し，ID情報の属性である権限を決定する.

PKIX では, ID情報と公開鍵, 及び, ID情報と権限の結びつきが前提となっているので, 認証と権限管理が一体化している. つまり, 権限と公開鍵とを結び付けるのにID情報が必要なため, グローバルなID情報を保証するX.509証明書により権限管理を行う場合, 匿名サービスといったプライバシーを重視したネットワークサービスの実現は難しい.

プライバシー重視の権限管理とは他のサービスとどう異なるものなのかを振り返ってみる．SSLに代表される通信路上でのデータの暗号化は, 第三者に対して通信路を守るものである．しかし，これはサーバに対してクライアントが提供するID情報などの情報を秘匿するものではない.

我々は, ID情報を含まない，権限と公開鍵が直接結びついているSPKI (Simple Public Key Infrastructure) の権限証明書 (Authorization Certificate) を利用することによって，SPKIの特徴である簡潔なアクセス制御方式に，プライバシー重視のアクセス制御，つまり，認証を分離したアクセス制御の方式を提案した [5] [6] [7]. この方式により，利用者はサーバにID情報を晒さずにサービスの享受が可能になる.

一方，不用意にID情報をサーバに渡したくないが，自分にとって価値のあるものが得られるのであれば，必要に応じて，性別，年齢，趣味などの個人情報をサーバに与えてもよい，もしくは，サーバは，性別，年齢，趣味などの個人情報に応じたサービス提供をしたいという要求もある.

さて, ここで，プライバシーという概念を振り返る. プライバシーとは，19世紀のアメリカの学者によって提案された法概念である．これを「伝統的なプライバシー」と呼ぶ, その意味を「プライベートな情報」と定義する. しかし, ネットワークにおいて伝統的なプライバシーの概念を適用しようとすると, 電子メールアドレスは公の情報かプライベートな情報なのかといった混乱が生じる. よって, ネットワーク社会におけるプライバシーを, 伝統的な意味でのプライバシーと区別し，「ネットワーク・プライバシー」と呼ぶ. 以後，本稿に

おけるプライバシーとはこのネットワーク・プライバシーを指すこととする．では, プライバシーとはどのように定義されるべきものなのだろうか．憲法学者アラン・F・ウェストは, 著書『プライバシーと自由』の中で,「プライバシーとは, 個人, グループまたは組織が, 自己に関する情報を, いつ, どのように, またどの程度に他人に伝えるのかを自ら決定できる権利である」と定義した．ここから，**プライバシーの権利とは「自己にかかわる情報について一定のコントロールを及ぼす権利」**（**自己情報制御権**）であるという考え方が提案されている [1].

したがって，本論文では，**「自己情報制御権を保証する枠組み」として，サーバに対して利用者の個人情報開示を自由に制御する方式を提案する．**つまり，クライアントのID情報を晒さずに，クライアントがよいと思う程度にクライアントの個人情報をサーバに与え，それに応じたアクセス制御を行うことを実現する方式を提案する．また，株主優待券の利用をその適用例として示す．さらに，提案方式の安全性についての議論を与える．

2 SPKIの概要

SPKIは，Carl Ellisonの論文 [2] を切っ掛けに始まり，現在，RFC2962，2963で規定されている [3] [4]. RFCの中では，名前空間に関する記述が多いが，我々のアイデアは，SPKI 権限証明書が，利用者の名前などのID情報を含まないという事実に着目し，シンプルで効率的でかつ，プライバシーを重視した権限管理の実現を目指したことにある．SPKIにおいて権限証明書と呼ばれる証明書が用いられる．これは，公開鍵と権限の対応に，権限証明書の発行者が電子署名を付加したものである．権限証明書は，公開鍵と権限の結び付きを発行者に対する信頼のもとで保証するものであり，それ自身にID情報を含んでいない．具体的な**SPKI権限証明書**（以降，**権限証明書**と呼ぶ）の様式は，以下のような5-tupleに発行者の電子署名を付加したものとなっている:

$$\langle I, S, D, A, V \rangle$$

I：Issuer. 権限証明書の発行者の公開鍵.

S：Subject. 権限を行使する主体の公開鍵.

D：Delegation. ブール値．True，または，False. Sが更に権限を委譲することが可能かどうかを示している.

A：Authorization. 権限を表現している.

V：Validity. 証明書の有効期限.

また，複数の権限証明書の簡略化に関しては，RFC2963 [4] に従う.

3 アクセス制御システムの仕様

この章では，我々の目指すアクセス制御システムの仕様を与え，その仕様を満たす構成とその利用概要について説明する.

本論文の提案システムは，文献 [5] [6] [7] を基に，**サーバに対して利用者の個人情報開示を自由に制御する方式を新たに導入したものである．**

まず，最初に匿名アクセス制御に関して振り返る [5] [6] [7]: サービス享受における利用者のサーバに対する匿名性は，ID情報を含まない権限証明書の利用と，証明書の発行過程と行使過程の分離という概念に基づいている．この分離のために善意の第三者，つまり，Issuing Agent（後述）を導入した．これにより，発行におけるクライアントの選別と行使における匿名アクセスを可能にしている．また，Issuing Agent により，だれにどのような権限証明書 (権限) を発行したかを管理することも出来る.

つぎに，クライアントの個人情報開示の自由な制御について述べる．クライアントの個人情報というのは，ID証明書のID情報と同じでサーバにとって信頼できる善意の第三者によって，証明書の形で発行される必要がある．さらに，クライアントの年齢，性別などの個別の情報を個別の証明書という形でを発行して貰う必要がある．この機能を実現するために**個人情報証明書発行サーバ**（以降，**Privacy Server**と呼ぶ）を導入する．これは．事前にクライアントのID情報，年齢，性別などの個人情報の登録をしておき，クライアントからの要求時にクライアントの認証を行い，その**個人情報と公開鍵の対応を保証する証明書** (以降 **個人情報証明書**と呼ぶ) を発行するものである．Privacy Server は，Issuing Agent と同じである場合も想定できるが，概念的に別のものとする.

3.1 証明書

提案システムおいて，使用される2種類の証明書を以下の通りに定める.

(1) **権限証明書**：“ 2 SPKIの概要 ”で与えた権限証明書を，検証を効率的に行うために以下のように拡張する:

$$\langle I, S, D, A, V, N \rangle_{S(I)}$$

ここで，N は，システム管理上に用いる Number（シリアル番号）とする．また，この権限証明書の発行者 I の秘密鍵を $S(I)$ とする.

(2) **個人情報証明書**：Privacy Server（後述）によって発行される個人情報に関する証明書．個人情報と公開鍵の組をPrivacy Server が電子署名したもの．つまり，以下の通りとする:

$$\langle P(P), P(C), SI, V \rangle_{S(P)}$$

ここで，Privacy Server P の公開鍵を $P(P)$，秘密鍵 $S(P)$, Client（後述）C の公開鍵 $P(C)$ とする．SI は，Client の個人情報，例えば，年齢，性別など，また，V は, 証明書自体の有効期限を示している．

3.2 システムを構成する主体

システムを構成する主体を以下の通りに定める:

(1) **Server**：サーバ．Client に対してサービスを提供する主体．権限証明書，個人情報証明書を検証できる．Client に対して，個人情報を要求する．

(2) **Client**：クライアント．Server に対してサービスを要求する主体で, 自己の ID 情報を Issuing Agent に登録してある主体．また自己の ID 情報と, その他の個人情報についてを Privacy Server に登録してある．

(3) **Issuing Agent**：Server からの委託により, Client に対して権限証明書を発行する主体．Server，Client 共に信頼する存在．ACL を保持しており, そこにはユーザの ID 情報と鍵及び権限の対応が記されている．適切な Client C からの要求を受けて, 権限証明書の発行を行う．また，Client 間の権限証明書を委譲する際に仲介を行う．

(4) **Privacy Server**：Client からの委託の下に, Client に対して個人情報証明書を発行する．Server，Client 共に信頼する存在．Client の ID 情報を保持しており, さらにはその他の個人情報 (年齢, 性別など) の情報も保持している．適切な Client からの要求を受けて, 要求された個人情報を保証する個人情報証明書の発行を行う．

ここでの‘Server’と‘Client’は，本論文で提案する方式を構成する各主体を指し，一般のサーバ・クライアントモデルにおけるそれらと区別出来るように，前者を英字で，後者をカタカナでそれぞれ表記することにする．

3.3 システム仕様

上述の主体によって構成されるシステムの仕様を以下の通りに定める:

(1) Client は，権限証明書を Server に提出することにより権限の行使をする．

(2) この際に，Server は Client を認証しない. つまり，この時，ID 情報を一切利用しない．

(3) Server は，Issuing Agent に,『Client に権限を委譲する権限』を権限証明書を用いて委譲する．

(4) Issuing Agent は，Client に権限証明書を用いて適切な権限を委譲する．

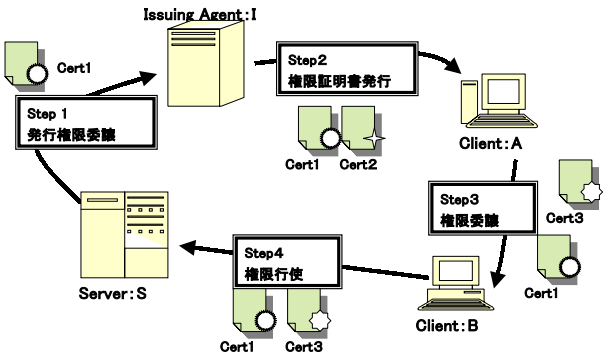

図 1　権限証明書の発行から利用までの処理の概要図

(5) この際，Issuing Agent が Client に委譲する権限は，Server が Issuing Agent に与えた権限を越えないこととする．つまり,『Issuing Agent が Client に委譲する権限』によって行うことが可能であれば，常に,『Server が Issuing Agent に与えた権限』で行うことが可能である．

(6) Issuing Agent は，Client 間の権限証明書委譲の仲介を行う．つまり，既に発行された証明書を基に新たな証明書を生成する．

(7) Issuing Agent が Client に証明書を発行する際, Issuing Agent は，Client を認証し，発行する権限証明書と Client との対応関係を保存する．

(8) Client は，前もって個人情報を Privacy Server に登録しておく．

(9) Privacy Server は，Client を認証し，Client から要求された個人情報に対応する個人情報証明書の発行を行う．

(10) Client は，Server が要求してきた個人情報を Privacy Server が発行した証明書の形で提出する．

(11) 以上のことを，安全な通信を用いて行う．

4 権限行使までの流れ

この章では，具体的な権限の行使までの流れを説明する．以下での各ステップは，Figure 1と対応している．

4.1 Step1: 発行権限委譲

Server S は, Issuing Agent I に自身のリソースに対するアクセスについての権限証明書を発行する権利を与える．つまり，S はその権限をあらわす証明書 $Cert1$ を I に発行する．この結果，S の保持する ACL には,『I に対して権限証明書発行権限を与えた』というエントリが追加される．

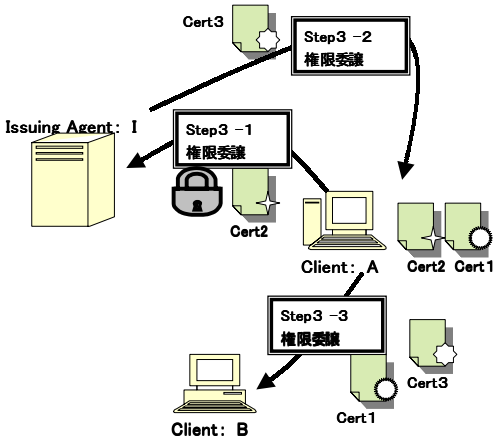

図2　権限委譲の詳細図

4.2　Step2: 権限証明書発行

Issuing Agent Iは，Client A の要求に対応した権限証明書を発行する．Iは，ACLを保持し，A のID情報と権限の対応付けをエントリとして持つ．また，A のID情報と公開鍵の対応も保持する．

まず，認証を行い A を確定する．次に I の保持するACLを参照し，ID情報の属性となる権限を確定する．A の要求する権限が，ACLの許すものであれば，Aに対して権限証明書 $Cert2$ を発行し，認証によって確保したセキュアチャネル上で，$Cert1, Cert2$ を A に対して発行する．具体的な手順は以下のようになる:

(1) Issuing Agent I は，Client Aの認証をする．
(2) Iは，A に与える権限と対応する公開鍵に，自分の公開鍵，証明書の有効期限，及び権限委譲の可否を示す情報を付加して，権限証明書 $Cert2$ を作成する．
(3) Iは，電子署名を$Cert2$に施し，$Cert1$と共に A に発行する．

4.3　Step3: 権限委譲

Client A は，$Cert2$のDelegationがTrueの場合に，自分のもつ権限 (またはその一部) を委譲することができる．この委譲の詳細は，Figure 2で示す．以下の説明は図2と対応している．

4.3.1　Step3-1

Client A は，権限の委譲者となり，$Cert2$ を基にして，権限を委譲する相手 Client B の公開鍵 $P(B)$，B に委譲する権限，有効期限などの情報と自分自身が発行された権限証明書 $Cert2$ を Issuing Agent I に送る．

4.3.2　Step3-2

Issuing Agent Iは，権限証明書 $Cert2$などを基に，権限証明書 $Cert3$ を作成し，それを自分の秘密鍵 $S(I)$ で電子署名する．さらに，$Cert2$ を破棄する．また，I 自身の対応リストに，A の公開鍵 $P(A)$ から B の公開鍵 $P(B)$ へ権限が移ったことを記録する．そして I は A に $Cert3$ を渡す．ここで，公開鍵$P(B)$は，I にとって，BのID情報を表すものではないことに注意する．I が知りえる情報は，A が，$P(B)$ を持つ人物に権限を委譲したということのみである．勿論，I が BのID情報を取得するような実装も考えられる．ここで，以上はサーバを介さないことに注意.

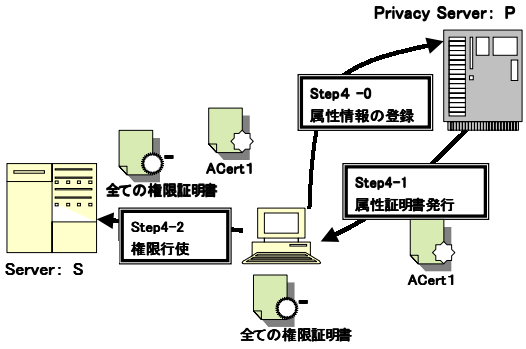

図3　権限行使の詳細図

4.3.3　Step3-3

ここで，$Cert3$ を受け取った A は，$Cert1$ と $Cert3$ を B に委譲する．B は A と同様，$Cert1$，$Cert3$ を S に提示することで $Cert3$ の示す権限を行使できる．また，$Cert3$　の権限委譲が可能な場合，$Cert3$ で指定された権限の範囲内で，さらに権限の委譲をすることもできる．その場合はStep3-1に戻る．また，B がIssuing Agentに登録されていない主体である時でも委譲は可能であるが，Issuing Agentに登録されていない主体が更に委譲することは出来ないとする．

4.4　Step4: 権限行使

Client A は, 権限証明書を S に対して提示することで権限を行使できる，ここで, A に対するサービスの提供は，A が提示した権限証明書に含まれる Client A 自身の公開鍵 $P(A)$ を用いて暗号化する．したがって，この暗号化されたサービスを復号できるのは，$P(A)$ に対応する秘密鍵 $S(A)$ を保持する主体のみであることに注意する．この部分の詳細はFigure 3で示す．以下の説明は図3と対応している．

4.4.1　Step4-0

Client Aは，あらかじめ Privacy Server P に，自分自身のID情報と，個人情報（年齢，性別，etc）を登録してあるとする．さらに，それらの個人情報と結びつける公開鍵を登録しておく．

4.4.2 Step4-1

Privacy Server S は，Client A からのリクエストに対応した個人情報証明書 $ACert$ を発行する．具体的な手順は以下のようになる:

(1) Privacy Server S は，Client A を認証する．

(2) P は，A がどのような個人情報証明書を必要としているのかを確認する（ここでは，例えば，A は年齢（19歳）という個人情報の証明書を欲しているとする）．この場合，P は以下のように自身の秘密鍵 $S(P)$ を用いて署名したものを個人情報証明書 $ACert$ となる:

$\langle P(P), P(A), `Age19', `20001225000000' \rangle_{S(P)}$

ここで，これは年齢に関する証明書で，2000年12月25日0時0分0秒まで有効なものである．

P は，$ACert$ を A に送信する．この通信は，(1) の認証において成立するセキュアチャネルを用いる．

4.4.3 Step4-2

Client A は，自分が持つ権限証明書のうち，行使する権限に関連したすべての証明書，及び，Server S に要求された個人情報に対応する個人情報証明書 $ACert$ を，S に渡す．まず，S は，提出された権限証明書，及び，個人情報証明書に含まれる公開鍵に対応する秘密鍵を所持していることを，チャレンジ・レスポンスなどにより確認する．その後，S は，与えられた証明書の正当性を検証する（具体的な権限証明書の検証の方法は，論文 [5] [6] [7] を参照）．ここでは $ACert$ の検証方法を簡潔に述べる．個人情報証明書 $ACert$ の正当性は，S が $P(P)$ を用いて $ACert$ の署名を検証することで示すことができる．以上の検証から，2種類の証明書が正当と判断され，Server S が Client C を適切である（例えば，年齢）と判断した場合，S は C に対して権限に応じたサービスを提供する．

5 適用例

この章では，提案方式を用いた『株主優待券の利用』の実現について説明する．

今回実装したシステムは，株主優待券の発行，及び，その行使を扱うものである．株主優待券とは，ある会社の株式を保持する人物に対して発行されるもので，その券の持ち主に対し会社側から何らかのサービスを提供するものである．通常の株主優待券は，入場券，割引券などの役割を持つ，さらに，今回の実装のように個人情報証明書と組み合わせることで，個人情報の必要なサービス (酒・たばこのネット販売，男性または女性限定サイトへの入場) の実現も可能になる．ここで，株主優待券は匿名性を持ち，委譲可能であること，及び，株主優待券として発行された権限はその会社に戻ることに注意する．優待券は会社から発行されるのではなく，その会社の株式の手続きを代行する証券会社が発行する．これにより，会社が証券会社に対して発行権限を与えているという解釈が成り立つ．

5.1 システム構成

ここで,“ 3 アクセス制御システムの仕様 ”で示したアクセス制御システムと株主優待券の利用のためのシステムの対応を与える．

5.1.1 システムを構成する主体

サーバ S : “ 3.2 システムを構成する主体 ”の ‘Server’ に対応する．ある株式会社 $\mathcal{COM}$ のリソースである．$\mathcal{COM}$ は，S を用いて自社の株主優待券を保持するものに対してサービスを提供する．この際，$\mathcal{COM}$ は，誰が株主優待券を用いたのかということには関心がなく，株主優待券の偽造などによる損害を防ぐことができればよい．株主優待券の発行管理は，株式の販売を代行している証券会社 $\mathcal{FIRM}$ に委託する．この結果，S において，株主優待券発行サーバ I の公開鍵 $P(I)$ と，株主優待券発行サーバに対して与える権限の対応が記録される．株主（もしくは，権限を委譲された者）が株主優待券を提出してきたときに，この記録を参照して，I の発行した株主優待券が正しいものかを判断する．

株主優待券発行サーバ I : “ 3.2 システムを構成する主体 ”の ‘Issuing Agent’ に対応する．証券会社 $\mathcal{FIRM}$ に属する．$\mathcal{FIRM}$ は株主 C のID情報を保持しており，また，各株主が株取引に際して用いているIDに関連付けられた公開鍵 $P(C)$ を保持する．さらに, 株主優待券の発行に関して S から権限を与えられており，保有株式数に応じて各株主に対して割り当てられる株主優待券 (権限証明書) の情報を持つ．ここで注意することは，株主の実際のID情報と $P(C)$ の対応は，S の知るところではないことである．また， I は株主優待券の委譲に際しても役割を持つ．

株主 C : “ 3.2 システムを構成する主体 ”の ‘Client’ に対応する．証券会社 $\mathcal{FIRM}$ を通じて，株式会社 $\mathcal{COM}$ の株式を保有する主体である．$\mathcal{FIRM}$ の公開鍵は事前に保持してあるとする．実際に，本人，もしくは，委譲された者は，株式優待券を行使して，サービスを享受する．また，別の主体に対して, 株主優待券を委譲することも可能.

プライバシ保護サーバ P : “ 3.2 システムを構成する主体 ”の ‘Privacy Server’ に対応する．株主 C からの要求に応じて，個人情報に関する証明書

を発行する．P は，C のID情報だけでなく，その他の個人情報 (年齢, 性別など) を保持している．

5.1.2 株主優待券, 個人情報証明書

ここでは，システムを実装する上で2つの証明書の仕様を与える．

株主優待券は，3.1で定めた権限証明書 $\langle I, S, D, A, V, N\rangle_{P(I)}$ とする．ただし，I は，株主優待券発行者の公開鍵．S は株主優待券を行使する主体の公開鍵．D は株主優待券を委譲許可．A は，具体的に享受できるサービス．V は株主優待券の有効期限. yyyymmddhhmmssの形式の文字列．N はシリアル番号．株主優待券の委譲・失効管理で使用する．

個人情報証明書は，同様に，3.1で定めたものとする．ただし，Client は，株主 C に対応する．

5.2 実装システム

実装は, **JDK1.2, JSDK2.0, ApacheJServ1.1, IAIK2.51** によって行った．株主優待券発行サーバ S, サーバ I のインターフェースは Servlet を用いてWWWサーバとして実装した．

株主優待券の発行, 検証のロジック，及び，株主優待券使用者が復号, 委譲などに用いるツールは, 以前我々が作成したライブラリ [5] [6] [7] の一部を修正し利用した．具体的には, 権限証明書の検証・生成を行うためのライブラリVERIFY, ISSUEを拡張し, 株主優待券，及び，個人情報証明書の形式も扱えるようした．さらに, 権限証明書の委譲を行うためのアプリケーションであったDELEGATERを, 共通ライブラリ化してServletからも利用できるようにした．また, 株主優待券発行に際してのサーバ S と株主 C のセキュアチャネルの確保，及び，個人情報証明書発行に際しての株主優待券発行サーバ P と株主 C のセキュアチャネルの確保にはSSL化したWWWサーバと．CAにより発行された個人証明書を組み込んだブラウザを使用することを前提としている．

5.3 株主優待券の利用

5.3.1 個人情報の登録

株主優待券の利用者（株主など）C は，予めプライバシ保護サーバ P に，自分自身のID情報と個人情報（年齢, 性別,..etc）を登録する．さらに，それらの個人情報情報と結びつける公開鍵を登録しておく．

5.3.2 発行権限委譲

株式会社 $\mathcal{COM}$ のサーバ S は，証券会社 $\mathcal{FIRM}$ の株主優待券発行サーバ I に，自身のリソースに対する株主優待券を発行する権利を権限証明書の形で委譲する．今回の実装においてこの委譲は，すでに行われているものとする．この結果，$\mathcal{COM}$ におけるサーバ S が保持するACLには,『$\mathcal{FIRM}$ の I に対して，株主優待券の発行権限を与えた』というエントリが追加される．

5.3.3 株主優待券発行

証券会社 $\mathcal{FIRM}$ の I は, 株主 C の要求に応じて, 株主優待券を発行する．証券会社 $\mathcal{FIRM}$ は，株主 C の株取引から C の保有する株式を把握しており，また, C が用いている公開鍵 $P(C)$ も所有している．C に対して発行できる株主優待券についての情報とIDの対応付けをACLエントリとして持つ．また，株主優待券を発行する相手のIDと公開鍵の対応も保持する．具体的な発行手順は，4.2と同様に行う．

5.3.4 株主優待券委譲

株主 C は，$Cert2$ の委譲が可能である場合に，株主優待の権利 (またはその一部) を委譲することができる．具体的な手順は, 4.3で述べた枠組みをそのまま適用する．ここで，証明書を破棄したプライバシー保護サーバ I は，その破棄された株主優待券のシリアル番号を，S に通知することに注意する．これは二重使用を防ぐためである．

5.3.5 株主優待券の利用

株主優待の権利保持者（株主 C など）は, 株主優待券に相当する権限証明書の組を $\mathcal{COM}$ のサーバ S に対して提示することで自分の保持する権限を行使できる．また株主優待券の使用に関して，20歳以上であることなどの個人情報の提出を求められる場合は，個人情報証明書も併せて提出する．今，株主優待券利用者である株主 C が株主優待券を利用しようとしていて, $\mathcal{COM}$ のサーバ S が利用者の年齢情報を要求しているとする:

(1) 株主優待券利用者である株主 C は，プライバシ保護サーバにアクセスし，個人情報証明書 $ACert$ を取得する．
(2) 株主 C は，株主優待券，及び，$ACert$ を $\mathcal{COM}$ のサーバ S に渡す．
(3) $\mathcal{COM}$ のサーバ S は，与えられた権限証明書と $ACert$ を検証する．正当と判断された場合, 適切な個人情報（年齢など）を持っているときに，$\mathcal{COM}$ の S は，株主に対して優待券に記載された権限に応じたサービスを提供する．

6 議論

6.1 提案方式の再考

SPKIを利用した我々の提案する方式についての特徴を示す．それらによる我々の提案する方式の利点について述べる．

(1) **ID 情報を利用しないアクセス制御:** サーバにクライアントの ID 情報を晒さないアクセス制御を可能にする．個人情報の漏洩を考慮したアクセス制御を実現する際，一つの解決策になるであろう．

(2) **権限を持つサーバにより証明書が発行される:** 権限を持つサーバ，つまりサービスを提供するサーバは，委譲する権限証明書を自分の支配下に置ける．PKIX における CA による発行と違い，証明書は最終的に発行者に戻ってくる．つまり，最終的に，証明書が発行者の所へ帰ってくるため，例えば，権限証明書のフォーマットなどの変更を容易に出来る．

(3) **サーバは独自の名前空間を持たず，信頼できる第三者の持つ名前空間を利用する:** 権限を持つサーバは，アクセスしてくる主体の ID 情報のデータベースを持たなくて良い．サーバは，クライアントの管理から開放されるなどの利点が考えらる．

6.2 安全性

本論文で提案したシステムにおいて考慮すべき点,『通信路中での安全性』と『権限証明書に関わる安全性』，さらに,『個人情報証明書に関わる安全性』について述べる．

6.2.1 通信路中での安全性

証明書発行サーバ ⇔ クライアント : ここでの通信は, クライアントが最初に提供する認証データによってセキュアチャネルを張ることで，完全性・機密性を確保できる．

サーバ ⇔ クライアント : サーバから提供されるデータは, 権限証明書に含まれる公開鍵で暗号化されるため, そのデータは，秘密鍵を所持する主体のみが享受可能．また，サーバに提出する証明書は，それぞれ電子署名されている．

6.2.2 権限証明書にかかわる安全性

改竄 : 発行者により電子署名がなされているので不可．

本人のコピーによる二重使用 : サーバが, 権限証明書に付加されたシリアル番号を記録しておき, それを検証することで防ぐことが可能.

委譲と同時の使用 : この場合, サーバがシリアル番号をチェックした後に，発行者からも，委譲により破棄された同じシリアル番号が通知されることになる．このことから検出可能.

他人のコピーによる二重使用 :サーバから提供されるデータは，本当の所持者が所有する秘密鍵によってのみ復号できるので，その秘密鍵をも入手しない限り不可能．秘密鍵が盗まれた場合においても，サーバは一度使用されたシリアル番号を記録しているため，同一の証明書が提示された際に検証できる．そのためサーバ側に実害はない．秘密鍵が漏洩した場合の責任はユーザにあることに注意する．

二重委譲の防止 : 委譲の際には，発行サーバに戻し，もとの権限証明書を破棄するため．ある主体が，同一の一枚の権限証明書を二人以上に対して委譲することは出来ない.

破棄された権限証明書の使用 : これは権限証明書の委譲後の利用ともいえる．この場合，権限証明書を破棄した発行サーバは，そこに含まれるシリアル番号をサーバに対して通知するため，破棄された権限証明書の使用は検出可能.

6.2.3 個人情報証明書にかかわる安全性

改竄 : プライバシ保護サーバにより電子署名がなされているので不可.

他人の個人情報証明書をコピー使用 : サーバは，クライアントとの通信の際に，チャレンジを行い，個人情報証明書中の公開鍵に対応する秘密鍵を持つ主体かどうか確認する.

過去の個人情報証明書の使用 : 証明書自身に，有効期限が含まれているのでサーバにより検出可能.

基本的に，個人情報証明書は，本人の個人情報を保証するものであるため委譲されることはない．よって，委譲に際しての問題点を考える必要はなくなる．

7 さいごに

本論文では,『クライアントの自己情報制御を重視したアクセス制御の方式』を提案し, 株主優待券に適用し実装を行った．この方式によりクライアントの ID 情報を晒さずに，クライアントがよいと思う程度にクライアントの個人情報をサーバに与え，それに応じたアクセス制御を行うことを実現できることを示した．また，その適用例として，株主優待券の利用へ適用し実装した．さらに，提案方式の安全性などの議論も与えた．実装の詳細とその評価については別の機会に報告する．

今回の枠組みにおいて問題となりうるのは, 権限証明書の委譲に Issuing Agent が関与する必要があることである．このことから, Issuing Agent の処理速度が遅い場合, そこに負荷が集中し, 委譲における通信にオーバヘッドが生じる可能性がある．また, 委譲の枠組みは, 場合によってはクライアント間で行えることが望ましいと考えられる．

参考文献

[1] 浜田 良樹： ”プライバシーの権利とインターネット”, CyberSecurityManagement, JapanCyberSecurityInstitute,Vol3,5,6,2000

[2] C. Ellison : Establishing Idetity Without Certification Authority, *Proc. of USENIX Security Symp.*, '96.

[3] C.Ellison : SPKI Requirements, RFC2692, Sep. 1999.

[4] C. Ellison, *et al.* : SPKI Certificate Theory, RFC2693, May 1999.

[5] T.Saito, K.Umesawa, and H.G.Okuno, Privacy Enhanced Access Control by SPKI, Proc. of the Seventh International Conference on Parallel and Distributed Systems: International Workshop on Next-Generation Internet Technologies and Applications 2000 (NGITA00), pp301-306, ISBN 0-7695-0571-6, IEEE, Iwate, July 2000.

[6] T. Saito, K. Umesawa, W. Wen, H. G. Okuno, Access Control by SPKI Certificate, *JWISC2000*,pp.143-150, 沖縄, Jan. 2000.

[7] 梅澤 健太郎, 齊藤　孝道, 奥乃 博 : SPKI (Simple Public Key Infrastructure) によるプライバシー重視の権限管理の提案とJavaを用いた実装, 情報処理学会第60回全国大会, 3Q-03, Mar. 2000.