インターネット上の情報の与信システムについて

山崎重一郎*,**,***、荒木啓二郎*,**

*九州大学、**ISIT、***富士通研究所

概要

電子署名付き文書の信頼度は、使用された署名システムのセキュリティレベルや運営方法などに応じて一定の限界を持つ。電子署名の検証系は「正しい／誤り」の２値的評価しか返すことができないので、情報の信頼度の観点からの情報への与信とその評価を行なうための別のシステムが必要となる。

本論文では、インターネット上で交わされる情報に対する多値的な格付け評価を行う与信システムの構成方法について提案する。提案するシステムは、格付け機関(Rating Bureau)が情報の信頼度を評価することを前提にし、信用情報を署名付き情報本体とは独立したRDFで記述されたメタ情報として扱うことにより情報の信頼度の検証系と署名検証系とを分離することを特徴とする。情報の信頼度に関する判断は、受信者のポリシーを表現するルールとメタ情報に基づいて信頼度の判断を行なうTrust Engineが行う。

A Trust Management System for Signed Data

Shigeichiro Yamasaki*,**,*** ,Keijiro Araki*,**

*Kyushu University, **ISIT,***Fujitsu Laboratory

abstract

A verification system for digital signature can output only binary values "success or fail." As the acceptable usage of signed data is limited from the security level of the signature system utilized for it we should have another evaluation system for signed data.

In this paper we propose a trust management system for signed data that is exchanged in the Internet. The features of our proposal are (1) the rating of reliability of signed data is evaluated by some trusted third party called "Rating Bureau," (2) information about reliability of signed data is representated by RDF as a meta data which is separated from signed data itself. A program which we call "trust engine" judge the trust level for the signed data with rules and the meta data.

1. はじめに

インターネットが社会生活に浸透し、X.509デジタル証明書[1]を利用する認証基盤も広がりつつある。SSL[2]のような認証機能を用いた通信による情報やS/MIME[3]などによる電子署名がついた文書が、紙の有印文書などと同等の法的な効力を持つものになろうとしている。

電子署名付きの文書は署名検証システムによって「正しい／誤り」の２値的判断として評価される。しかしこの評価結果は、情報そのものの信頼度や署名者の信用度とは無関係である。一般にセキュリティシステムの信頼度は運用コストとのトレードオフによって決まる。署名付き文書の信頼度は、使用された署名システムの運用レベルが一つの用途の上限を与える。例えば、ある鍵が契約書のへの署名システムとして利用される場合、使用される鍵システムの包括的な安全性は、それで署名できる契約書の金額の上限の制限といった形で現れてくる。したがって、署名付き文書の信頼度の検証系は、単に文書に正しい署名が付いているというだけでなく、その用途に対して適切なレベルの署名が付いているということを、検証システムの利用者側のポリシーに基づいて検証できることが求められてくる。

認証機関によっては、CPS (Certification Practice Statement)という形で署名システムの運用方針の自己基準を公開し、発行する鍵や証明書のランク付けをしているものもあるが、発行者自身による信頼度の自己評価やランク付けは信用の根拠が曖昧であるために信用インフラとして恒久的に利用してゆくには問題がある。

情報の信頼度の検証システムは、署名付き文書

の発行者側ではなく、検証者側の視点から検証ポリシーを定義するための根拠となる信頼度に関する情報として構成すべきである。

この点においてPGPは、受信者側の完全な自己責任による信用を前提にしているので、ここで問題にしているような信用情報のインフラは必要としない。しかし、常に本人による信用度の判断が必要なので大規模なインフラとして利用することは困難である。

広域的な認証インフラの構築のために、認証局を階層的に組織化するなどの方法によりデジタル証明書の署名関係を推移的に利用する方法も検討されている。しかし、そのようなインフラを構築するときにも署名自体の検証だけでなく、遠隔地の認証局で証明書がどのような運用基準で発行されたのかという証明書の信頼度が問題になる。

署名付き文書への署名という関係と異なり、証明書に対する信頼度は一般に推移性を持たないので、広域分散環境における信用度の判断手段が問題になる。

以上のような問題意識に基づいて、我々は公開鍵証明書やさらに一般化してインターネット上で交わされる署名付き文書の信頼度を判断できるようにする情報への与信システムを考えた。

我々はこれまで「認証の3権威分立モデル」[4],[5],[6] として公開鍵に基づく認証基盤を「本人確認」「与信」「ポリシー定義」の３層に分離することにより、１枚の公開鍵証明書に複数の属性情報を定義可能にし、利用者の固有のポリシーに基づいてその信用度を主観的に判断可能にしたモデルを提案し実証実験を行ってきたが、本研究で提案するシステムは、この認証モデルにおける「与信」と「ポリシー定義」のレイヤのモデルを拡張したものとなっている。

本論文による提案では、情報の発行者である署名機関以外に情報の信頼性に関するラベル付けやレーティングを行う信頼できる第3者機関（以降RB:Rating Bureau と略記する）という概念を追加し、情報の信頼度を署名検証系と分離したシステムで評価することによって公開鍵証明書だけでなく一般の署名付き文書の与信や利用ポリシー定義に適用可能なシステムを構成した。

発信者とは独立の機関であるRBが自由に信用情報の定義を行うためには、署名付き文書の中に属性情報が埋め込まれていては問題が生じる。このため、我々は、署名付きの文書実体とその属性や信用情報とを分離してメタ情報として管理することにした。

2. 認証の３権威分立モデル

まず、本研究の前提となっている認証の３権威分立モデルについて述べる。

インターネットの利用者は、自らの意志で世界中に存在している不特定のサーバーにアクセスしてサービスを利用する。このため、従来のようにサーバーごとにユーザー管理を行なうことは非現実的であり不合理になってきた。

インターネット上で電子商取引のようなセキュリティ要求の高いサービスを提供しようとするとユーザー認証とその信頼度の検証が必須であるため広域的な認証基盤が必要となるり、公開鍵暗号に基づくX.509デジタル証明書などを利用した認証基盤が整備されつつある。しかし、インターネットは、電子商取引だけでなく多くの利用分野があるために電子商取引だけに特化した認証基盤を整備するのは問題である。

我々は、認証の機能を「本人確認」「与信」「利用ポリシー定義」の３つに分離することによって、一つのデジタル証明書に複数の用途を定義可能にする認証基盤のモデルを提案し実証実験を行なってきた。

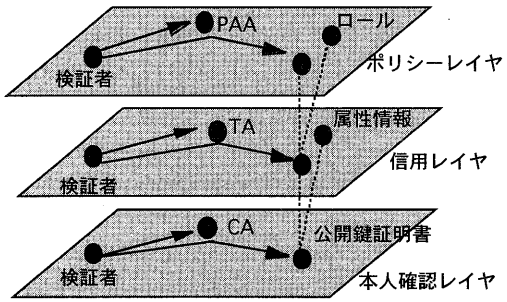

図1. 認証の３層モデル

我々のモデルでは、公開鍵証明書は「本人確認」のレイヤの実体である。検証者は公開鍵証明書の発行者であるCAの公開鍵を使って本人確認が可能である。このレイヤと独立した形で本人の属性情報を扱うのが信用レイヤである。例えば「医師である」というような属性を「医師会」というような権威機関が保証することを想定している。このような保証機関をTA(Trust Authority)と呼んでいる。一人の個人がいくつもの属性を持っているように、一つの公開鍵証明書に対して複数の属性情報が定義できる。

ポリシーのレイヤは、実際にサービスを提供する側の視点でユーザーをとらえたものである。実際のサービスにおける認証システムの利用は、最終的にはサービス側がユーザーに対して提供する利用権限として現われる。どのような属性を持つユーザーにどのような権限を与えるかという判断

基準を我々は「利用ポリシー」と呼んでいる。

例えば病院サーバーが医師という属性を持つ人だけに特別な操作を許可するという利用ポリシーを持っていた場合、そのポリシーにしたがってユーザーの属性を検証し、それに適合したユーザーには医師専用の権限を与える。またユーザーのタイプごとに与えられる権限の集まりのことを「ロール」と呼んでいる。またそのサービスのポリシーを定義することができる権威者をPAA(Policy Approving Authority)と呼んでいる。

我々はサービスという場所にユーザーがアクセスしたときにその場にふさわしいローカルなロールを与えることによってユーザーの権限管理システムを構成する「プレースモデル」を提案している。

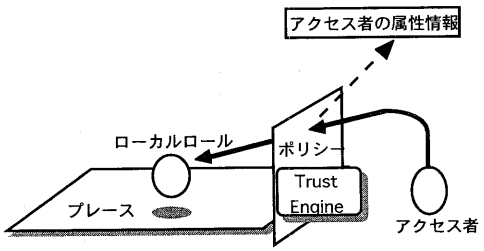

図2. プレースモデルによるポリシー定義

PAAは実装としては、一定のルールの集合と信用情報の参照に基づいて動作する処理系となる。このようなシステムを Trust Engine と呼ぶことができる。本稿で対象にするのは、このようなポリシー定義を行なう主体が、信用情報をどのように評価すべきかというモデルについてである。

3. TAをRBと見なすモデル

これまでの我々の「3権威分立モデル」の「与信」レイヤでは、与信を行なう機関であるTAが公開鍵証明書と属性情報すなわち信用情報と結びつけていた。これまでのTAの機能は、属性情報を安全に定義することであった。しかしTAの本来的な機能は公開鍵証明書に対応する個人や法人に対する与信である。

つまり、TAはデジタル署名をすることが本来の役割ではなく、本人を審査したうえで信用度を評価し、その評価結果を公開鍵証明書と何らかの手段で結びつけることである。

このように解釈すると、TAは属性定義のデーターに署名をするかしないかという2値的な判断を行なう機関ではなく、ラベル付けやレーティングのような多値的な評価を行なうRB (Rating Bureau) と見なすことができる。この解釈は、公開鍵証明書を単なる署名付き文書として考えるとより自然に見えてくる。CAは署名付き文書を作成し署名した情報の発行者ということになる。

次にポリシーのレイヤを考える。情報の信頼度は最終的には受信した側の主観によって判断される。発信者側は受信者が判断するための情報を署名などの形で付けることができるが、その情報の評価は受信者側の主観や環境によって変わるので、それを客観的な情報として扱うことはできない。

例えば、認証機関が自主的にレベル付けをして発行されたデジタル証明書のレベルは、発行者側のセキュリティ確保のための運用コストを反映していると主張されている。

しかし自己評価による格付けでは、その機関が本当にそれだけのコストをかけた運用をしているのかということを知ることは一般にはできない。

これに対して受信者側の利益を代表するRBがが実際にその認証機関を調査した上で証明書のレベル付けを行なった場合、その格付けの信頼度はずっと確かなものになる。

このモデルは、証券市場における、格付け機関に類似している。このアナロジーに従うと情報発信者が起債者、情報受信者が投資家、信頼できる第3者機関が格付け機関に対応する。

このため、ポリシーレイヤの処理は、RBが定義した信用情報に基づいて、受信した署名付き文書の情報をどのような水準の信頼度で評価するのかという判断を行なうことになる。もちろん、どのRBでも信用することはできないので、受信者の判断によって信用するRBが選択されることになる。また、ポリシーレイヤの処理は、実際にはPAAとしての受信者がポリシーを定義したTrust Engineによって実行されることになる。

4. 信用情報のメタ情報化

ここでは、RBによって定義される「情報の情報」をどのように定義すべきかということについて議論する。まず認証システムにおける属性情報の与信方法について議論したうえでその一般化方法について述べる。

我々の「3権威分立モデル」では、本人の公開鍵そのものを認証の主体を表わす実体と考えている。しかし、サービス側は、本人確認だけではその人にどういう権限を与えてよいのかわからないので、その公開鍵に対する「属性情報」つまりその人がどういう社会的権限を持っている人なのかという情報が必要になる。

現在最もに普及しているX.509デジタル証明書[1]では、この属性情報を証明書の中に埋め込んで

しまう形式になっている。したがって、一つの社会的な顔に対して１枚の証明書が必要になってしまう。SPKIの場合も同様である。

川倉らによるNetBill [8] や我々がISITの実験で採用したモデルでは[4]　　、公開鍵証明書とそれに対する属性情報を分離しているので、一つの公開鍵に複数の属性や信用を定義できるようになる。

NetBillやISITのモデルの重要なポイントは、属性情報が本人公開鍵証明書に対するメタ情報として定義されていることである。

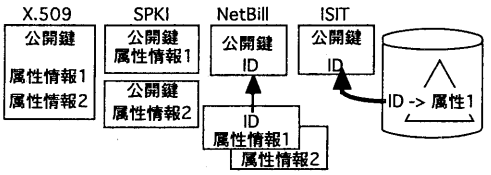

図3.　公開鍵証明書における属性情報の管理方法

属性情報や信用情報を同一の公開鍵証明書を参照するメタ情報として定義することによって、複数の属性や信用度を定義することができる。属性情報や信用情報は、与信者の主観的な判断が不可欠なので、このような外部システムとして多重に定義できることが望ましい。

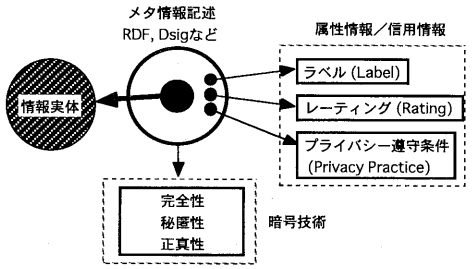

図4.　情報実体に対するメタ情報としての信用情報

この考え方を認証システムから、より一般的な情報へのラベル付けやレーティングといった情報の信頼度の定義システムへ拡張することができる。

電子化文書のメタ情報の記述の枠組みとして、DSig [10] やXML(Extensible Markup Language)[9]のRDF (Resource Description Framework)[12] がある。RDFは、文書のメタデーターを記述する汎用的な枠組みであり、「文書実体.プロパティ型=値」という形の宣言の集合として定義される。一つの文書実体に複数のプロパティ型を対応させることもできる。次のRDFの記述例は、URLで示された文書実体に著者と日付をメタデータとして宣言したものである。

```
<RDF:assertions RDF:href="http://www.k-isit.or.jp/>
        <BIB:author>やまさき</BIB:author>
        <BIB:date>1999.0614</BIB:date>
<RDF:assertions>
```

図6.　RDFによるメタ情報の記述の例

RDFによるメタ情報の記述は、実体に対して外付けなので、実体そのものを更新する必要がない。これは署名付き文書に情報を付加する場合は、重要な要件になる。

XMLにおけるデジタル署名の枠組みとしてDOMHash[11] がある。これはXML文書そのものに対する署名を行なうためのものである。RBによるメタ情報にはDOMHASHを利用した署名を付ける。

5. 提案する情報への与信システム

本論文では、情報への与信システムを次のようなメタ情報システムとして構成することを提案する。与信の主体はRBであり、ポリシー定義の主体は情報の受信者である。実際のWebなどのシステムへこのモデルのマッピングを行うときには、受信者がサーバーになることもクライアントになることもある。この与信システムは、情報実体つまり署名付き文書そのものを扱うものではなく、そのメタ情報を扱うシステムである。

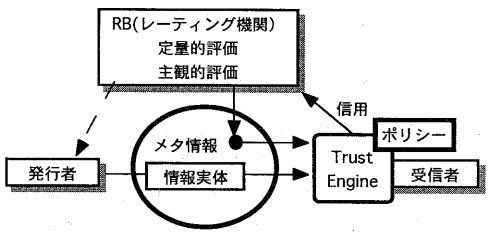

図5.　RBによる情報への与信モデル

RBによる情報の信頼性の定義は、情報の発行者の信頼度やラベル付けと情報実体に対するレーティングの値の宣言である。これらの宣言文はRBによって生成されRBのサーバーもしくは格付け公開用のサーバーを通じて公開される。

Trust Engineが参照するのは、受信者つまりPAAが作成したポリシー定義と、そのPAAが信用するRB が定義した信用評価である。

Trust Engineは、必ずしもプログラムである必

要はなく、ポリシーに基づいて判断を行う人間でもよい。例えば、信用情報が受信者のプライバシー権にかかわる判断を要求する場合、本人が確認するという手段がより望ましいであろう。

このように、信用情報は、プログラムだけでなく人間によっても処理できるように、ヒューマンリーダブルなデーター形式を持つ必要がある。

信用情報は、RBの署名検証の成否といった2値的な情報ではなく、RBから見てこの程度の信頼度であるという情報となっている。

情報に対する信用情報の形式は、次のような構造を持つ宣言のリストである。

情報実体：ラベル.評価属性=評価値

5.1 個人証明書への与信の例

このモデルを個人のX.509証明書への与信システムとして適用する例について述べる。この例の場合、従来のTAによるモデルとほとんど変わらない。メタ情報の定義はXMLによるRDF形式として標準化する。この、NetBillの属性証明書を利用する方式に近いが、この属性証明書をディレクトリーに格納しておくこともできる。

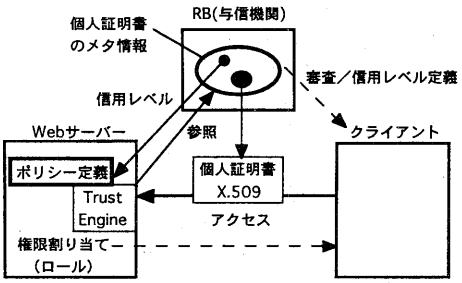

図6. 本モデルによるユーザー権限の割り当て

WebサーバーのTrust Engineは、個人のメタ情報をキャッシュしておくこともできる。ただし、メタ情報は個人証明書と独立に書き換えられるので、長期間のキャッシュを持つと実態と食い違う危険性が増大する。

5.2 Webページへのラベル付けへの適用例

このモデルをWebページの情報の信頼度をユーザーが確認するためのシステムとして利用する例について述べる。

これは、Webページに「プライバシー保護認証取得サイト」などのバナーをより信頼できるものにする。この例では、RBによる与信情報は、クライアントに渡されるが、クライアントにプログラムとしてのTrust Engineが存在するとは限らない。このため、RBから提供される信用情報は人間に可読な形式で送られる。ユーザーは、その信用情報を元に判断を行い、Webサーバーの情報の信頼度を決定する。

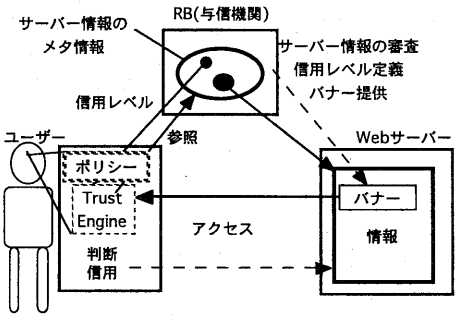

図7. Webサーバーの情報への与信

6. 関連研究

本論文で提案するような情報へのレーティングや与信の枠組みを与える既存のメタ情報システムとして、PICS[9]、P3P[14]、PolicyMaker[13]などがあげられる。ここではそれぞれのシステムについて特徴を述べる。

5. 1 PICS

PICS(Platform for Internet Content Selection) [9] は、WWWのページを対象にしたレーティング情報の記述言語である。インナーネット上の有害情報などの児童に対するブラウジングのフィルタリングを想定して作られている。

PICSはRBによるレーティングサービスを想定しており、通常はブラウザにレーティングサービス機関のURLが入った定義ファイルを設定して使用する。

ユーザがある何らかのページにアクセスしようとしたとき、Trust Engineはそれに割り込む形で処理を開始する。そのエンジンに登録されているポリシー定義に基づいてレーティングサービス機関にアクセスし、そのページを閲覧してよいレベルのものになっているかどうか調べる。その結果可能であればアクセス処理が継続され、拒否された場合は、アクセス処理が中断される。

PICSのラベル付けやルールの記述は、S式の連想リストで表現することになっている。

5. 2 P3P

P3P (Platform for Privacy Preferences) [14] は、WWWサーバー上にある個人情報を一定のプライバシー保護規定 (Privacy Prctice) に準じて正当なユーザーにのみアクセスを許可するように

管理することを目的にしている。

P3Pでは、メタ情報は、XMLのRDFの枠組みを使用して記述する。ユーザーがWWWサーバー上の個人情報にアクセスしようとするときに、Trust Engineは、プライバシー保護機関が認定したガイドライン従ってアクセスのための条件を提示する。ユーザーがそれを受理し合意が成立した場合にのみプライバシー情報へのアクセスが許可される。

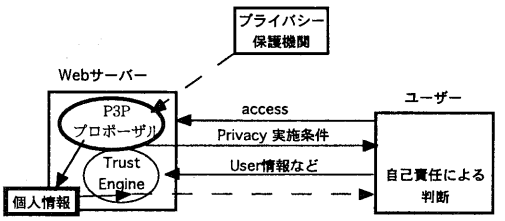

図8. P3Pに基づく個人情報アクセスの典型例

5. 2 PolicyMaker

Blazeらは、我々と同様に公開鍵暗号の署名検証システムとポリシー管理用のTrust Engineを分離するアーキテクチャーを提案している。これを広域分散環境におけるモバイルコードのセキュリティポリシーを定義する PolicyMakerシステムとして提案している[13]。

PolicyMakerは、JAVAアプレットに代表されるモバイルコードの受信側での計算機資源の要求量やアクセス権限の許容ポリシーの定義を行うための環境である。

7. おわりに

インターネット上で交わされる情報の信頼度を署名検証の成否といった2値的な判断だけでなく、信頼できるレーティング機関の格付け与信情報によって判断できるようにするためのシステムを提案した。

提案したシステムの特徴は、与信機関として署名者以外に格付けを行なう信頼できる打3者機関を設定したことと、このような与信情報を定義、ルールの記述、処理の含めてすべてメタ情報システムとして構成したことである。

本論文では、広域的な信用基盤を構成するための分散化について言及しなかったが、認証システムにおける相互認証と同じ問題が相互信用の問題として存在する。また、ポリシーに関する判断も本人だけでなく、より正確な判断ができる機関に委譲する必要が生じる場合があるが、これについても今後の課題となっている。

参考文献

[1] ITU Rec. X.509 (1993) | ISO/IEC 9594-8: , including Draft Amendment 1: Certificate Extensions (Version 3 certificate).1995
[2] Alan O. Freier ,Netscape Communications: "INTERNET-DRAFT The SSL Protocol Version 3.0", 1996
[3] S. Dusse RSA Data Security: "RFC2311 IETF, S/MIME Version 2 Message Specification", 1998
[4] 山崎重一郎、荒木啓二郎:信用情報と利用ポリシーの管理が可能な相互認証を実現する認証基盤の提案:情報処理学会論文誌 第40巻第1号平成11年1月 pp.296-309
[5]インターネットにおける「信用」と「評判」宮川祥子、山崎重一郎:-相互与信システムの社会的応用--橋ビジネスレビュー Vol.46 No.2 Nov.1998 pp.50-74一橋大学イノベーションセンター発行 千倉書房
[6]山崎重一郎、須賀祐治、村上美幸、荒木啓二郎:認証、証明書発行、利用ポリシー適用の"3権威分立モデル"に基づくデジタル認証システムについて:情報処理学会マルチメディアと分散処理研究会報告98-DPS-86-8pp.43-48 1998
[7]山本薫、山崎重一郎、須賀祐治、荒木啓二郎：インターネット上で与信された情報に基づくアクセス制御方法について、情報処理学会コンピュータセキュリティシンポジウム'98論文集、Oct, 1998.
[8] 川倉康嗣：ID証明書と属性証明書の併用によるアクセス制御方式、情報処理学会コンピュータセキュリティシンポジウム'98論文集、Oct, 1998.
[9] Tim Bray, Jean Paoli and C.M Sperberg-McQueen: Extensible Markup Language (XML) 1.0, W3C , http://www.w3.org/TR/REC-xml, Recommendation 10-February-1998
[10] Yang-hua Chu, et al.: PICS Signed Labels (DsSig) 1.0 Specification, W3C Recommendation,http://www.w3.org/TR/REC-DSig-label/, W3C Recommendation 27-May-1998
[11] Hiroshi Maruyama, Kebnt Tamura and Naohiko Uramoto: Digest Values for DOM (DOMHASH) Proposal, http://www.trl.ibm.co.jp/projects/xml/dsig_j.htm, 1998
[12] W3C: Resource Description Framework (RDF) Schema Specification, http://www.w3.org/TR/PR-rdf-schema/, W3C Proposed Recommendation 03 March 1999
[13] Matt Blaze, Joan Feigenbaum Jack Lacy: Decentralized Trust Management, Proc. IEEE Conference on Security And Privacy, CA, May 1996
[14]Massimo Marchiori : Platform for Privacy Preference (P3P) Syntax Specification, W3C Working Draft 7 April 1999