DVCS を利用した属性認証システムの実装
Implementation of the attribute authentication system using DVCS

岩崎 公寛† 中山 亮† 道坂 修†
Kimihiro Iwasaki Ryo Nakayama Osamu Dousaka

１．はじめに

近年 e-Japan 重点計画[1]により、電子申請や電子調達等の行政サービスの電子化とその実現に必要となる認証基盤が整備されている。現状の電子申請システムは、行政機関が申請者の本人性を確認するために PKI による電子署名を用いた認証を行っているが、特定の資格や条件を必要とする手続きに対してはこれを認証する手段がないため、対応が困難な状況にある。例えば飲食店営業許可証の発行申請を電子申請システムに対応させるためには、申請者本人の認証に加え、申請者が調理師の資格を保有していることを認証する必要がある。

本稿では、信頼できる第三者機関として電子文書の検証を行うデータ検証システム(以下 DVCS/RFC3029[2]で定義される)に属性認証機能を追加し、資格の認証を必要とする電子申請システムにおいて資格等の属性情報を認証する方式を提案する。

２．従来方式

資格等の属性情報を認証する方式として、次のような方式[3]が挙げられる。

(1)専用の属性認証システムを用いる方式

各個人の属性情報を格納した専用の属性認証システムに接続し、被認証者の属性情報の問合せを行う方式である。クレジットカードの信用情報を照合する CAFIS[4]等がこれに相当する。

(2)公開鍵証明書の拡張領域に属性情報を記述する方式

X.509 公開鍵証明書の拡張領域に属性情報を格納し証明書の発行者と拡張領域の記述内容を確認したり、証明書を発行する認証局を確認することで属性を認証する方式である。全国社会保険労務士会連合会認証局[5]や民間の属性認証サービス AccreditedSign パブリックサービス[6]がこれに相当する。

(3)属性証明書(RFC3281[7])を用いる方式

公開鍵証明書とは別に、属性を証明する属性認証局の発行する属性証明書を用いて属性を認証する方式である。

３．アプローチ

3.1 資格の認証を行う電子申請システムへの適用の要件

電子政府システムの持つ特性より、一般の属性認証システムに加え、以下の要件が求められるものと考える。

- 特定の製品に依存せず汎用性の高いものであること
- 認証過程や認証に用いた情報も合わせて保管でき、後の行政監査等のチェックに際し認証結果の正当性を検証できる等の証拠性を保有すること
- e-文書法[8]等の原本保管義務に則し、保管にあたり法定保存期間に耐えうるものであること

† 株式会社 NTT データ 技術開発本部

3.2 従来方式の問題点

前章で挙げた従来方式の問題点を考察する。

まず、(1)属性認証システムを用いる方式では、一般に属性認証システム毎に方式が異なりプロトコルベースで認証を行うため、前述の汎用性や証拠性の要件に反する。

次に(2)公開鍵証明書の拡張領域を用いる方式では、拡張領域の解釈の扱い(critical flag)や拡張領域の記述様式が統一されていないため、汎用性の要件に反する。さらに属性を追記したい場合に証明書の再発行が必要となるため、運用コストがかかる問題がある。

(3)属性証明書を用いる方式については、一通りの要件を満たすことができるが、一般に属性証明書の有効性は検証できるものの属性そのものの認証は定義されておらず、これに対する実装が必要である。また実装に際し証拠性や原本保管の要件を考慮し効率化を行う必要がある。

3.3 アプローチ

以上より本稿では、属性証明書を用いる方式をベースに、証拠性や原本保管の要件を考慮した属性認証方式を提案する。具体的には上記要件を電子公証サービスに見立て DVCS 上に属性認証機能を拡張し、DVCS における属性そのものを認証する方式を提案する。

４．提案方式

4.1 対象モデル

本稿では、資格を証明する属性証明書を予め行政機関が発行するものとし、図 1 に示すように各組織が属性証明書を発行するモデルを対象とする。また 1 つの資格につき、1 枚の属性証明書を発行し、複数の資格を所持する場合は複数の属性証明書を発行するものとする。

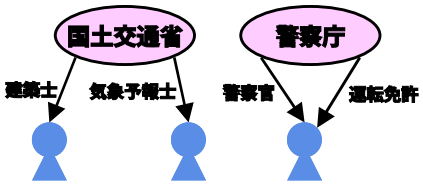

図 1 属性証明書発行モデル例

4.2 前提とする属性証明書のプロファイル

対象モデルで発行する属性証明書のプロファイルは RFC3281 に従うものとし、属性情報は①Issuer、②Group、③Role を組み合わせた属性情報ツリーとして表現されるものとする。ツリーの構成としては図 2 に示すように、属性 1 を属性認証局名（Issuer）とし、属性 2 を属性証明書に記載された資格情報（Group 属性）、属性 3 を資格の詳細情報（Role 属性）とする。

ここで資格情報は Group 属性・Role 属性に記載するが、RFC3281 の仕様では Group 属性には 1 つの情報しか格納出来ないため資格名を格納する。また Role 属性には複数の

情報を格納可能であるため、資格情報の詳細を格納することとする。

例として自動車運転免許証の場合、Group 属性には自動車運転免許証、Role 属性には自動二輪、大型、原付などの運転可能である車種情報を格納する。

属性の認証を行う場合には、認証条件として指定する属性情報ツリーに対して属性証明書の記載内容からこれら項目上位の階層から順に比較検証を行う。

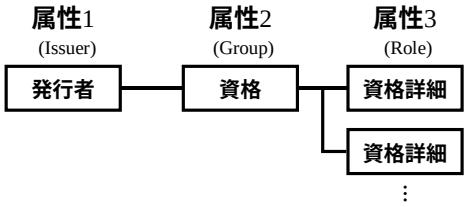

図 2属性情報ツリー

4.4 属性認証プロトコル

属性の認証を行うためのプロトコルとして、RFC3029 で定義される既存の VSD サービスに対し、さらに公開鍵証明書に対応する属性証明書と認証条件である属性情報ツリー(前節4.2)を指定できるよう、DVCS リクエストに対して以下の拡張を行う。

AcceptAttributes :: = SEQUENCE OF Attribute

なお RFC3029 では Extensions に関して定義されていないため、RFC3280[9]で定められた Extensions に従った。また Attribute に関しては RFC3281 に従う。

4.5 属性認証フロー

以上より、本稿による属性認証システムを電子申請業務に適用する場合、以下の流れとなる。

(1) 申請者は、資格保有を必要とする電子申請において申請書を作成後、これに対する公開鍵証明書による電子署名を付与し、公開鍵証明書と属性証明書を電子申請受付システムへ送信する。

(2) 次に電子申請システムは申請者から受理した申請データより、今回拡張した DVCS プロトコルを用いて①署名付き申請書、②公開鍵証明書、③属性証明書と④資格の認証条件を指定した属性情報ツリーを DVCS に送付する。

(3) DVCS は、まず署名付き申請書に対し公開鍵証明書の有効性検証および電子署名の検証を行い、VSD サービスを完了する。次に属性証明書の有効性を検証した後、属性証明書の証明する資格情報に対し確かに申請者が保有していることを認証するため、属性証明書と公開鍵証明書とのリンクを確認する。

(4) 属性証明書の有効性および公開鍵証明書とのリンクが確認できた場合、指定された属性情報ツリーに基づき属性証明書の Issuer 項目、Group 属性項目、Role 属性項目の値を比較することで、電子申請システムが意図する属性と一致するかを検証する。

(5) 以上の処理がすべて成功した場合、DVCS は検証結果をデータ検証証明書(DVC)として電子申請システムに返却し、申請者の本人性と資格の保有を認証できたものとする。

(6) (5)で得られた DVC と申請データを原本保管システム（本稿で拡張した DVCS を利用してもよい）に保管、管理させることで、証拠性と原本保管の要件に対応させるものとする。

５．考察

本稿ではモデルを絞り込み、そのモデルで取り扱われる属性情報を対象として属性情報ツリーを構築した。また DVCS で属性認証を行うために、既存のプロトコルを拡張して DVCS リクエストに属性情報を含めた。その際に属性情報を持たせる項目として Extensions を使用したが、同内容は requestPolicy に記載することも可能であるため、requestPolicy を利用する方式についても検討を行う必要がある。

また今後は TOEIC で 800 点以上を有していないと許可されないような属性とその程度を表現するようなモデルへの適用など、より汎用的な属性情報の表現方法や属性証明書プロファイルについて精査を行う必要がある。

属性証明書に含まれる属性情報や DVCS が所持する情報については、属性情報の認証を行うために属性情報をカテゴリ別に分類したり属性情報の表記方式を定めるなど、効率化に向けての対応策を検討する。更に DVCS の運用や社会的立場を考え、DVCS で所持する情報や検証時のリクエストに含まれる情報を整理し、場合によっては DVCS の仕様も含めて見直す必要がある。

さらに提案手法を用いたデータ検証システムを運用する際には、システムやその検証結果に対して社会的信頼性を確保するため、法制度の観点から属性証明書や属性認証局、DVCS について検討する必要がある。

６．まとめ

終わりに、本稿では今後の電子申請業務において、属性情報の認証を含めた方式について検討を行った。ここではまず電子行政手続きにおける要件を定め、その要件を満たす認証システムとして DVCS を用いたシステムについて検討した。さらに属性認証プロトコルを拡張することで属性証明書を用いた属性検証機能を追加し、様々な電子申請業務に対応できるようなシステムを構築した。

今後は考察の結果より判明した課題について取り組み、汎用的で信頼性の高い属性認証システムの構築を目指す。

参考文献

[1] eJapan 重点計画 : http://www.kantei.go.jp/jp/it/network/dai3/3siryou40.html
[2] RFC3029 : http://www.ietf.org/rfc/rfc3029.txt
[3] ECOM : 証明書利用形態に関する考察(2) 属性情報の分析,平成 15 年 3 月
[4] CAFIS : http://www.cafis.jp/
[5] 全国社会保険労務士会連合会認証局 : http://www.shakaihokenroumushi.jp/
[6] AccreditedSign パブリックサービス : http://www.jcsinc.co.jp/service/a_sign.html
[7] RFC3281 : http://www.ietf.org/rfc/rfc3281.txt
[8] e-Japan 戦略Ⅱ加速化パッケージ(素案)のポイント : http://www.kantei.go.jp/jp/singi/it2/dai22/22siryou3.pdf
[9] RFC3280: http://www.ietf.org/rfc/rfc3280.txt