ハイパーメディア情報に対するデジタル署名方式の提案

3M－5

米田 健　勝山 光太郎
三菱電機（株）情報技術総合研究所

1．はじめに

今後普及が見込まれるオンラインショッピングシステムなどの電子契約システムにおいては、サービス提供者は、ユーザが契約内容を承認したことを確認後、契約内容に基づいたサービスをユーザに提供する。ユーザが契約内容を承認したことを確認するために、サービス提供者は、契約内容に対応するデータにユーザのデジタル署名[1]を付加させる。一般にオンラインショッピングシステムでは、サービス提供者の提示する契約内容は画面上にわかりやすく表示される。

しかし、画面に表示される契約内容と、実際にユーザがデジタル署名を付加するデータとの対応関係はユーザにとって必ずしも明確ではない。その結果ユーザは、デジタル署名を付加したデータが、実は画面で表示されている内容とは、異なる契約内容に対応しているのではないか、という不安を持つことになる。

そこで、本稿では、画面に表示される内容と、ユーザがデジタル署名を付加するデータの対応を明確にするために、画面内容をテキスト形式に変換し、その変換された情報に対してデジタル署名を付加する方式を提案する。

2．表示内容に対するデジタル署名の課題

ユーザが画面の表示内容を承認するためにデジタル署名処理を施す際の課題としては以下が挙げられる。

（1）署名対象データの内容をユーザが明確に把握できるようにする。

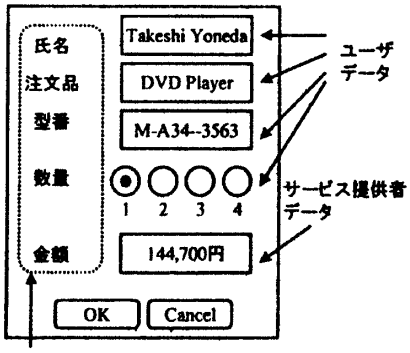

図1 画面の表示例

図1にオンラインショッピングシステムにおいて、ユーザの注文内容がユーザに提示されている例を示している。図1では、ユーザ Takeshi Yoneda が型番 M-A34-3563 の DVD Player 1個を 144,700 円で注文する例を示している。ユーザは、"Takeshi Yoneda","DVD Player","M-A34-3563" をキーボードから入力し、個数をボタンで選択している。これらユーザが与えた情報をユーザデータ、それ以外のサービス提供者が提示した情報をサービス提供者データと呼ぶことにする。

図2に図1の "OK"ボタンをクリックした際の好ましくない署名対象データを示している。この

署名対象のデータ

[HEX 表示]

235ab7eff63b32323cd45dba239a3
ee4ca87e3f4fa43ca543e2q3532123
cb87a9ef99ebfa3256b7ba4932

[ASCII表示]

.....Takeshi Yoneda...23vcat
]]-assd....DVD Player.....]]:[
...../.%s-.....3$.....

図2 好ましくない署名対象のデータ

署名対象データは、HEX 表示、ASCII 表示で見ても何を示しているかわからない。このように署名対象データの内容が不明確の場合、ユーザは署名

A Digital Signature Method for HyperMedia Information
Takeshi Yoneda, Kotaro Katsuyama
Mitsubishi Electric Corporation

対象データが画面の内容とは異なる契約内容に対応するのではないか、という不安を抱くことになる。

（2）署名対象データからユーザが承認した画面の表示内容を単純なプログラムで再生できるようにする。

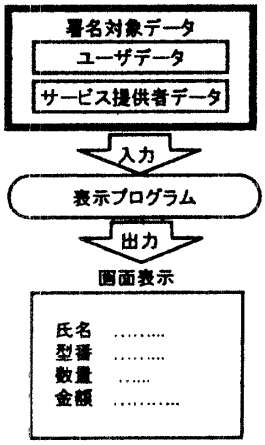

図3 署名対象データと画面表示

図3はデジタル署名の対象となったデータが表示プログラムに与えられて画面表示が再生される様子を示している。ユーザが承認した表示内容を再生するためには、表示プログラムが必要である。表示プログラムが改ざんされると、同一の署名対象データが異なる内容として表示される可能性がある。表示プログラムの改ざん防止に対処する方法として、表示プログラムも署名対象データに含めることが考えられる。しかし、この方法は、規模の大きな、頻繁にアップデートされる表示プログラムに対しては適用が困難である。したがって再生プログラムはできるだけ単純で変更の少ないものが望まれる。

3．テキスト変換を用いたデジタル署名方式

2．で述べた課題を解決する方式の概略を示す。

3．1 処理の流れ

（1）ユーザの署名要求を受け取ると、サービス提供側プログラムは、画面の表示内容をテキスト形式に変換し、テキスト表示プログラムを用いてユーザに再度提示する（図4参照）。

（2）テキスト変換された署名対象データからデジタル署名を生成する。

3．2 効果

氏名：Takeshi Yoneda
注文品：DVD Player
型番：M-A34-3563
数量：1
金額：144，700円

図4 テキスト変換された表示内容

本方式の効果を以下に示す。

a）署名対象データの明確化

ユーザは自分の署名対象データが、画面に表示されているテキスト情報であることを明確に理解することができる。

b）署名対象表示プログラムの単純化

ユーザの署名対象データは、テキスト形式である。テキスト形式は、文字コードと表示方法が国際的に標準化されている。また表示プログラムはあらゆる市販のコンピュータに標準添付されている。ユーザが異なるテキスト表示プログラムを用いて、署名対象データが同一に表示されるかどうかを確認することも容易である。したがって、表示プログラムに対しての改ざんチェックを省略することができる。

3．3 その他のシステムへの適用

本稿で述べた方式の応用分野としては、表計算文書やフォーム形式文書を用いた業務ワークフローシステム、オンライン納税システムなどが考えられる。これらのシステムでは、ユーザの否認を不可能にするために、ユーザのデジタル署名は、その署名対象データとともに長期にわたり保存される。したがって、ユーザ側も何に対して署名を付加したのか確認したいというニーズが高くなる。

4．今後の課題

本稿では、テキスト変換の例として、属性名と対応する属性値を単純にテキスト変換して列挙する例を挙げた。表計算文書などの表示内容によっては、1）属性名に対して複数の属性値が存在する、2）属性値がさらに、属性名と属性値から構成される

といった場合も考えらる。表示内容から署名対象の内容を抽出し、それを汎用的に表現できるテキスト表現形式を規定するのが今後の課題である。

参考文献 [1] B. Schneier "Applied CryptoGraphy"