

保証された情報を扱う個人情報流通システムの検討*

2J-O1

大西 真樹 岡田 浩一†

日本電信電話株式会社 NTT情報流通プラットフォーム研究所‡

1. はじめに

近年、契約の締結やマーケティング等に利用するため、個人情報要求する Web サイトが増加している。また、インターネットを利用したオークションのように、個人同士での個人情報の受け渡しも行なわれている。このようにインターネットでは、個人情報の利用が頻繁に行なわれているが、その一方で個人情報を偽ったネット詐欺等の事件も増加している[1]。このような事件を防止するためには、第三者によって正当性が保証された個人情報の受け渡しが有効となるが、ユーザは無断で自分の個人情報が受け渡しされることを望まない。そこで本稿では、正当であると保証された個人情報を、ユーザが確認した上で提供するシステムを提案する。

2. 従来方法の問題点と本研究の目的

従来方法としては、CA によって正当性が保証された個人情報を電子証明書[2]に含めておき、SSL[3]におけるクライアント認証時に、通信先に提供する方法がある。しかし、この方法では、電子証明書に含まれている個人情報が固定されているため、氏名だけを必要とする場合や、氏名に加えて住所も必要とする場合等、目的に応じて必要とする個人情報だけを選択して受け渡しができないという問題がある。また、複数の端末を使い分ける際には、秘密鍵および証明書を事前に全ての端末に格納するか、秘密鍵および証明書を格納したメディア(ICカード等)の読取装置を全ての端末が持たなければならず、携帯電話や PDA 等、多様な端末での使用に適さないという問題がある。

本研究の目的は、上記の問題点を解決した、保証された個人情報の提供システムを提案することである。

3. 提案システム

3.1 システムの概要

本稿で提案するシステムは、第三者機関によって正当性が保証された情報をネットワーク上の個人情報管理サ

ーバに格納しておき、Web サイトからの要求に応じて、Web ブラウザを経由し、その情報を提供するというものである。Web ブラウザを経由する際に、ユーザは送信内容を確認することができる。

3.2 システム構成

本システムは、正当性が保証された個人情報を保管する個人情報管理サーバ(A)とユーザが利用する Web ブラウザ(B)、正当性が保証された個人情報を取得する Web サイト(C)で構成される(図1)。

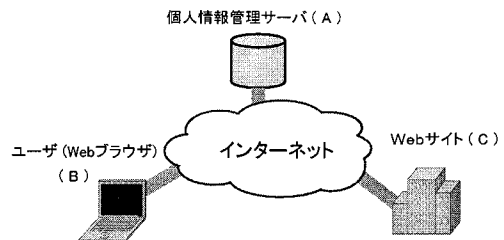


図1. システムの構成図

3.3 システムの利用手順

本システムの利用手順を以下に示す(図2)。

まず、事前準備として以下の作業を行なう。

- ・ユーザは、自分の個人情報を個人情報管理サーバに申請する。
- ・個人情報管理サーバは、申請された個人情報の正当性を身分証明書等により確認した上で、その個人情報を保管する。
- ・Web サイトは、個人情報管理サーバから署名を検証するための公開鍵を取得する。

次に、ユーザが本システムを利用して Web サイトに個人情報を提供するまでの手順を(1)から(7)に示す。

(1) サービスの要求

ユーザは、Web ブラウザを利用して Web サイトにサービスの要求を行なう。

(2) 個人情報の要求

Web サイトは、HTTP のリダイレクト等を利用して、ユーザの利用する Web ブラウザから個人情報管理サーバに個人情報を要求する。要求する個人情報の項目名およ

* A Sharing Platform for Verified Personal Information

† Masaki Onishi, Koichi Okada

‡ NTT Information Sharing Platform Laboratories,
NTT Corporation

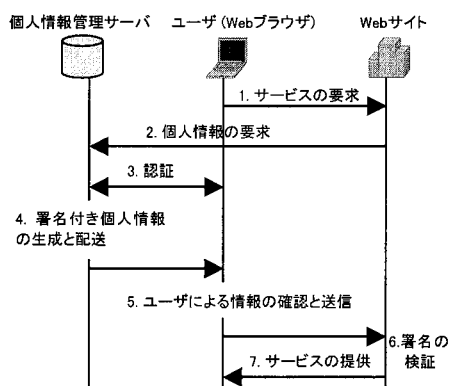


図2. システムの利用手順

び配送先 URL は、リダイレクト先の URL に埋め込まれた形で送信される。

(3) 認証

個人情報管理サーバは、要求をリダイレクトしてきたユーザの認証を行なう。

(4) 署名付き個人情報の生成と配送

要求された個人情報をデータベースから取り出し、この個人情報に配送先 URL とタイムスタンプを付加したものに署名を付与する。そして、その情報を配送先 Web サイトの URL に埋め込んだリンクを持つ HTML データを作成し、ユーザに配送する。

(5) ユーザによる情報の確認と送信

ユーザが受け取った HTML データには、送信される情報の内容が示されており、ユーザは送信してよいかどうかを確認する。送信に同意する場合は、配送先 Web サイトへのリンクをたどり、情報を送信する。

(6) 署名の検証

Web サイトは、署名の検証により正当性を確認する。

(7) サービスの提供

Web サイトは、ユーザにサービスを提供する。

3.4 セキュリティ

本システムでは、ユーザと Web サイト間、個人情報管理サーバ間で、サーバ認証に基づく SSL を利用することによって、経路における盗聴、改ざんを防止し、個人情報管理サーバにおけるユーザ認証により、なりすましを防止する。また、個人情報管理サーバの署名により、ユーザ自身による情報の改ざんを防止する。

さらに、個人情報管理サーバから送られる情報を不正ユーザが何らかの方法で取得した場合でも、不正ユーザ

がその情報を自分の情報であると偽って再利用することを防止するため、個人情報管理サーバは、タイムスタンプと配送先 URL を付与した個人情報をユーザに配送している。Web サイトは、タイムスタンプに示された有効期間内に送られた情報に同一の情報がないことを確認することにより、取得した情報が過去に自サイト宛てに送られた情報を再利用したものでないことを確認できる。また、配送先 URL を確認することにより、受け取った情報が、他の Web サイト宛ての情報を再利用したものでないことを確認できる。

3.5 システムの利点

本システムでは、Web サイトが要求した個人情報だけを提供することができるため、不必要な情報が個人情報管理サーバから Web サイトに提供されることはない。また、提供される情報の内容をユーザは確認でき、その内容に応じて提供しないことも可能である。本システムでは、ユーザの端末には Web ブラウザ以外の特別なソフトウェアを必要としないため、端末非依存性が高く、携帯電話や PDA 等の端末からの利用が可能である。また、ネットワーク上で個人情報を管理しているため、複数の端末の使い分けも容易である。

4. まとめ

本稿では、正当性が保証された個人情報を、ユーザが確認した上で提供するシステムを提案し、その実現方法について述べた。今後は、広義の個人情報としてアクセス権限等を扱う事を検討すると共に、本システムと[4]で提案している個人情報自動記入システムを共通化させ、個人情報流通のための総合的なプラットフォームの検討を行なっていく予定である。

参考文献

- [1] http://www.npa.go.jp/hightech/arrest_repo/kenkyo.2001.kamihanki.htm
- [2] R. Housley, et al.: "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC2459, 1999.
- [3] T. Dierks, et al.: "The TLS Protocol Version 1.0", RFC2246, 1999.
- [4] 大西、岡田: Web における個人情報自動記入システム、電子情報通信学会 2002 年総合大会、2002