M_038

個人情報保護と利便性を両立する Webアプリケーションフレームワークに関する研究

Web Application framework for the protection of personal information and the convenience

瀬高 昌弘† 天野 直紀†
Masahiro Sedaka Naoki Amano

1. はじめに

2005年4月に個人情報が施行され、個人情報の漏洩がテレビ等で大きく報道されることが多くなった。

インターネット上のショッピングサイトでは、ユーザと企業間で名前や住所等の個人情報をやりとりしなければ商品を受け取ることができないが、個人情報をやりとりすると情報漏洩のリスクがある。

個人情報を漏洩した企業は、損害賠償費用等の金銭的な損失だけでなく、企業イメージ低下等の社会上の損失が発生するなど、その影響は計り知れないため、できる限り個人情報漏洩のリスクを軽減することが重要である。

個人情報漏洩のリスクをなくすための方法としてユーザとショッピングサイトの間を第三者が仲介する方法やユーザの個人情報について開示制御を行うといった方法がこれまでに示されている[1][2]が、個人情報を保護するためにセキュリティレベルを強化することと利便性を両立することは難しく、セキュリティレベルを強化すれば利便性が低下し、利便性が向上すればセキュリティレベルは低下する。

そこで、筆者らは個人情報の保護とユーザ、ショッピングサイトの利便性を両立する個人情報取り扱い代行サービス（以下代行サービス）を考案し、そのサービスの実現のために必要である個人情報を取り扱う部分をWebアプリケーションフレームワーク化することを提案した[3]。本稿では検証システムを構築し、検証システムを実装する上で気づいた今後検討すべき課題について述べる。

2. 個人情報の取り扱い

個人情報漏洩のリスクをなくす方法として、高倉ら[1]や西田ら[2]によって個人情報の保護と流通を実現するために、個人情報管理システムを構築し、ユーザショッピングサイト間の仲介やユーザがあらかじめ登録した個人情報の提供条件をもとに個人情報の開示制御をするといった方法が考えられてきた。

また、楽天市場[4]などのように、ユーザとショッピングサイトがあらかじめ登録し、注文やお金の流れ、個人情報の取り扱いを代行・集約するものもある。

これらの手法では、ユーザによる開示制御条件の登録が必要な点や一度でも開示された個人情報についてはその流出を防げないといった問題がある。また、ショッピングサイトにとっては代行サービスのシステムを利用・経由するためにサイトデザインの自由度が制限されるといった制約がある。

そこで本研究では、証明書を用い、これをユーザからショッピングサイトに受け渡すことによって個人情報の保護と利便性を両立する手法を提案した[3]。

証明書とはユーザとショッピングサイトの間でやりとりされるもので代行サービスが発行する。ユーザはあらかじめ代行サービスに名前や住所等の個人情報や決済に必要な情報を登録し、買い物をする際に代行サービスから証明書を発行する。この証明書にはユーザの個人情報を記載せず、代わりに代行サービスの連絡先や金額等が記載されており、図1のように、ユーザが証明書を購入品目とともにショッピングサイトに渡すことで決済と商品の配送を代行サービスが代行する。

代行サービスが決済と配送を代行することにより、ユーザの個人情報はショッピングサイトに開示せずにすむため、保護される。

この証明書を用いる部分について、Webアプリケーションフレームワーク化する。

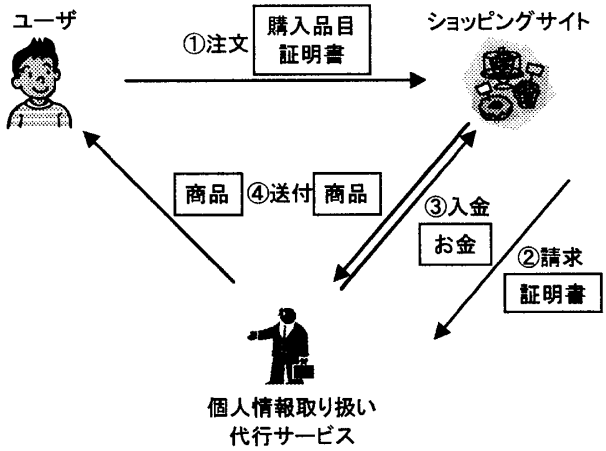

図1 提案手法

3. システム

前章で述べた手法を実現できることを確認するため、個人情報保護と利便性を両立するための検証システムを図2に示すようなWebアプリケーションベースのシステムとして実装した。

†東京工科大学 大学院 バイオ・情報メディア研究科,
Tokyo University of Technology Graduate School of Bionics, Computer and Media Sciences

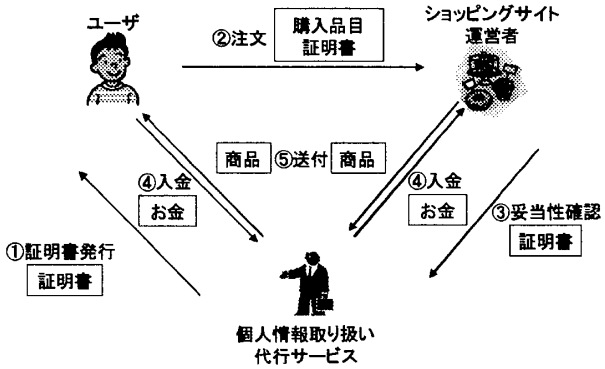

図2　システム構成

今回は提案手法が実現可能かを検証するため、ユーザが代行サービスの Web ページより証明書をファイルとしてダウンロードし、そのファイルをショッピングサイトの Web ページでアップロードすることによって、証明書をやりとりするものとする。

証明書は表1に挙げる項目を有するものである。この中で、「代行サービスの連絡先」とあるが、今回は証明書の妥当性を確認するために代行サービスシステムが用意したページの URL を記載する。また、「証明書の妥当性を確認できるもの」とあるが、今回は証明書の他の項目を元に、SHA-1 によって求めたハッシュ値を記載し、それによって証明書の妥当性を確認することにした。また、動作検証用のため、証明書の暗号化といった安全性の面は考慮しないこととする。

表1　証明書の項目

項目名
証明書を一意に示す番号
発行日
有効期限
金額
ユーザを識別する番号
代行サービスの連絡先
妥当性を確認できるもの

検証システムでの処理の流れは、以下の通りである。

1. ユーザがショッピングサイトを訪れ、購入する商品を決定
2. ユーザが代行サービスシステムへ購入金額を入力し、証明書発行手続きを行い、証明書を取得
3. ユーザがショッピングサイトシステムに注文内容と証明書を送付
4. 確認
   - 4.1. ショッピングサイトは代行業者システムにより、証明書の妥当性を確認
   - 4.2. 代行サービスはユーザからの入金を確認し、ショッピングサイトに入金
   - 4.3. ショッピングサイトは代行業者の入金を確認
5. 商品発送・到着
   - 5.1. ショッピングサイトは確認後、商品を発送
   - 5.2. 代行サービスは商品が到着次第、ユーザへ商品を発送
   - 5.3. ユーザへ商品が到着

ユーザが代行サービスの Web ページより証明書ファイルをダウンロードし、その証明書ファイルを注文内容と共にショッピングサイトの Web ページにアップロードする。ショッピングサイトはアップロードされた証明書ファイルを代行サービスの Web ページで証明書の妥当性を確認する。ショッピングサイトでは証明書の妥当性が確認後、代行サービスに商品の配送の代行を依頼する。依頼された代行サービスは商品が到着次第、ユーザへ商品を発送する。

この流れにおいて、ショッピングサイトを経由する通信においては注文内容と証明書ファイル、商品以外はやりとりされていない。証明書ファイルにはユーザを識別するための番号以外の名前や住所といった個人情報は含まれていないが、ショッピングサイトは代行サービスに商品配送の代行を依頼することで商品はユーザに到着する。よってショッピングサイトはユーザの名前や住所といった個人情報を知ることがない。

4. まとめ

本稿では個人情報の保護と利便性を両立する個人情報取り扱い代行サービス実現のために必要な個人情報を取り扱う部分を Web アプリケーションフレームワーク化することを提案し、構築した検証システムについて報告した。

検証システムでは、ユーザが代行サービスにより発行された証明書を用い、ショッピングサイトで買い物をする仕組みを実現し、個人情報の保護とユーザ、ショッピングサイトの利便性を両立することを確認した。

今後の課題としては、証明書の安全性についてと証明書受け渡しの実現方法がある。検証システムでは証明書の妥当性の確認方法として SHA-1 によって求めたハッシュ値により確認する方法をとった。この方法では妥当性は確認できるが、ネットワーク経路上で盗まれた場合には証明書を不正に利用される可能性がある。ネットワーク経路の暗号化や証明書の暗号化を検討する。また、証明書の受け渡し方法として、ユーザが代行サービスから証明書を発行する際に証明書ファイルをダウンロードし、買い物をする際にショッピングサイトに対して証明書ファイルをアップロードする方法をとった。ファイルのダウンロードやアップロードの手間を省く方法を検討する。

参考文献

[1] 高倉健, 西田玄, 林良一, 櫻井紀彦：IC カードサービスのための個人情報管理システムの検討, 情処研報 DPS-104-5, pp.25-30 (2001)

[2] 西田玄, 林良一, 高倉健：個人情報の保護と流通の両立を目指した個人情報活用システム, 情処研報 DPS-107-9, pp.49-54 (2002)

[3] 瀬高昌弘, 天野直紀：個人情報の取り扱いを代行・集約するための Web アプリケーションフレームワークに関する研究, 情処全国大会予稿集第3分冊, pp.305–306 (2006)

[4] 楽天市場 http://www.rakuten.co.jp/