O-9 内部不正を防止する個人情報管理サービスの検討

The Personal Information Management Service that can Prevent The Inside Job

大西 真樹 Masaki ONISHI
岡田 浩一 Koichi OKADA

1. はじめに

近年、多くのWebサイトが名前などの個人情報の登録をユーザに要求しており、ユーザにとっては Web サイト毎に個別にこれらの個人情報を登録することが負担になっている。このような中、予めユーザの個人情報を外部の個人情報管理サーバに保管しておき、ユーザが必要とするときに個人情報を取り出し、個人情報を要求している Web サイトに配送するサービスが提供されている[1][2]。これらのサービスは、ユーザの端末内で個人情報を保管する場合に比べ、個人情報の一元管理が可能であることや PDA や携帯電話など多様な端末での利用が可能であるという利点がある。しかし、個人情報管理サーバに保管されている個人情報をサービス運営者等によって内部から不正流出される可能性がある。

本稿では、ユーザの個人情報を管理するサービスの運営者が内部流出を行なうことを防止する方法を提案する。

2. 従来方法のセキュリティと問題点

従来の個人情報管理サービスでは、ユーザと個人情報管理サーバ間の通信路を SSL[3]などによって暗号化したり、ファイアウォールなどを設置することよって、セキュリティ対策を行なっている。またサーバに保管している個人情報を、サーバが暗号化して保管することによって、セキュリティを向上させている場合もある。

しかし、この様に個人情報を暗号化して保管している場合においても、ユーザの個人情報を個人情報管理サービスの運営者が所有する暗号鍵によって暗号化しているため、保管されている個人情報がサービス運営者によって盗み見されたり、不正流出されるなどの不正行為が行なわれる恐れがある。

そこで本研究では上記の問題を解決し、サービス運営者による不正行為を防止することのできる個人情報管理サービスを提案することを目的とする。

3. 提案サービス

3.1 サービスの概要

本稿で提案する個人情報管理サービスでは、ユーザが個人情報を登録する際に、ユーザは本システムから送られる暗号処理プログラムを使って個人情報を暗号化し、暗号化した個人情報を登録する。また、ユーザが個人情報を必要とする際には、暗号化済み個人情報と復号処理プログラムがユーザに配送され、ユーザは配送された復号処理プログラムを使って暗号化済み個人情報を復号し、個人情報を取得する。

3.2 システム構成

本システムは、暗号化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)、ユーザから個人情報を取得する Web サイト(C)で構成される(図1)。

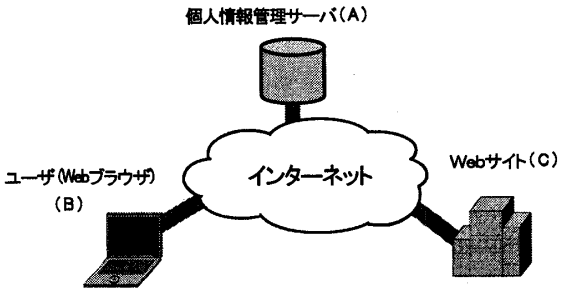

図1. システムの構成図

3.3 サービスの利用手順

本サービスの利用手順を以下に示す。まず、ユーザが個人情報を個人情報管理サーバに登録する際の利用手順について説明する(図 2)。

(i) 個人情報の登録要求

ユーザは、Web ブラウザを利用して個人情報管理サーバに個人情報の登録/変更要求を行なう。

(ii) ユーザの認証

個人情報管理サーバは、個人情報の登録/変更要求を行なったユーザを認証し、識別する。

(iii) 入力フォームと暗号処理プログラムの配送

ユーザからの個人情報の登録要求に対して、個人情報管理サーバは、個人情報を入力するための入力フォームと個人情報を暗号化するための暗号処理プログラムをユーザに配送する。

(iv) 個人情報の暗号化と配送

ユーザは、個人情報管理サーバから送られてきた暗号処理プログラムと所有する暗号鍵(パスフレーズなど)を使って記

*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
NTT Information Sharing Platform Laboratories, NTT Corporation

入した個人情報を暗号化する。そして、暗号化した個人情報を個人情報管理サーバに配送する。

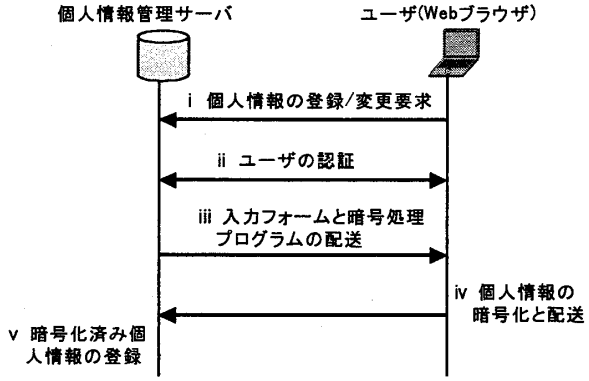

図2． 個人情報の登録

（v）暗号化済み個人情報の登録

ユーザから送信された個人情報を個人情報管理サーバは暗号化されたままの状態で保管する。

次に、ユーザが登録した個人情報を個人情報管理サーバから取得し、個人情報を配送先に送信するまでの利用手順について説明する(図3)。

（I）Webサイトからの個人情報の要求

Webサイトが個人情報の要求をユーザに行なう。

（II）個人情報の要求

ユーザは、個人情報の要求を個人情報管理サーバに行なう。

(III) ユーザの認証

個人情報管理サーバは、個人情報の要求を行なったユーザを認証し、識別する。

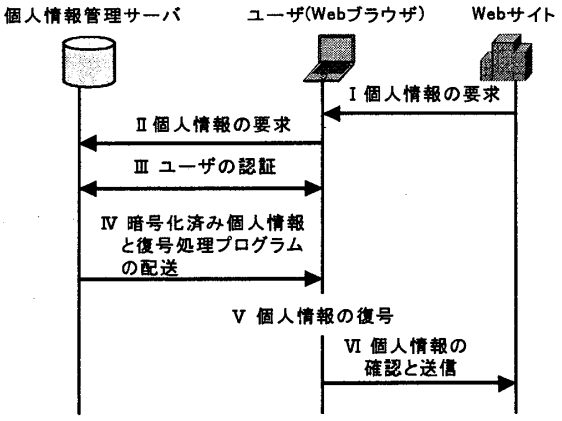

図3. 個人情報の取得

(IV) 暗号化済み個人情報と復号処理プログラムの配送

個人情報管理サーバは、認証したユーザが必要とする暗号化済み個人情報、および暗号化済み個人情報を復号するための復号処理プログラムを取り出し、ユーザに配送する。

(V) 個人情報の復号

ユーザは、個人情報管理サーバから配送された復号処理プログラムと所有する復号鍵(パスフレーズなど)を使って、暗号化済み個人情報を復号する。

(VI) 個人情報の確認と送信

ユーザは復号した個人情報を確認した上で、個人情報を配送先に送信する。

3.4 サービスの利点

本サービスでは、ユーザ自身で暗号化した個人情報を個人情報管理サーバに保管しているため、サービス運営者によってサーバに保管されているユーザの個人情報を閲覧されたり、不正利用されるなどの不正行為を防止することができる。また、本システムから配送される暗号処理プログラムは、ユーザのWebブラウザ上で暗号処理を行なうため、PCだけでなくWebブラウザを利用できるPDAなどの端末においても特別なクライアントソフトウエアをインストールすることなく、本サービスを利用することができる。さらに、個人情報とその情報を復号するための復号鍵を個人情報管理サーバとユーザで別々に管理しており、外部から個人情報管理サーバへ攻撃された場合に個人情報を奪われるなどのリスクを回避することができるため、個人情報管理サーバ自身で暗号化して管理する場合よりもセキュリティが向上する。

4. まとめ

本稿では、サービス運営者による不正行為を防止するための個人情報管理システムを提案し、その実現方法について述べた。今後は、ユーザが所有する暗号鍵を紛失した場合のリカバリーなどの暗号鍵の管理方法についての検討を行なうとともに、本システムと[2][4]で提案しているシステムを統合させ、個人情報管理のプラットフォームとして検討していく予定である。

参考文献

[1] http://www.passport.com/

[2] 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

[3] T. Dierks, et al.: "The TLS Protocol Version 1.0", RFC2246, 1999.

[4] 大西、岡田: 保証された情報を扱う個人情報流通システムの検討、第64回情報処理学会全国大会、2002