WWWを用いたセキュアマルチメディアオンデマンドシステムの実装

3Aa－9　田中俊昭　羽田知史　山田　満
KDD研究所

１．はじめに

近年、ビデオオンデマンド（VOD）やマルチメディアオンデマンド（MOD）などの情報検索サービスにおいて有料配信や電子決済などを実現するエレクトロニックコマースが注目されている。上記の背景にともない、筆者らは、これまで、情報検索サービスを安全に行なうためのセキュリティ技術の要件や、電子署名技術に基づく否認防止のメカニズムなどの検討を進めてきた[1]。本稿では、上記サービスの実現性と有効性の検証を目的として、筆者らが検討したメカニズムに基づくセキュアマルチメディアオンデマンドシステム（以下、セキュアMODシステムと呼ぶ）をインターネットWWW上に実装したので報告する。

２．セキュアMODシステムのセキュリティ機能

本システムで提供するWWWクライアント/サーバ(C/S)間のセキュリティ機能を以下に示す。

２.１　相互認証機能

なりすまし攻撃などを防止するために本機能を有する。実現メカニズムとしてはISO9798-3に基づく公開鍵暗号を用いた２パスのプロトコルを採用する[2]。

２.２　鍵配送機能

C/S間のデータ通信において第３者による盗聴を防止するためにそのセッションで用いる情報秘匿のための鍵をサーバからクライアントに配送する。実現メカニズムとしては上記相互認証プロトコルの付加情報としてセッション鍵を送付する。

２.３　否認防止機能

有料情報の配信やテレショッピングなどを電子的に行う場合には、情報の送受あるいは商品の購入等の事実を第３者に提示できる証拠情報を利用者及び情報提供者側で保持する否認防止機能が必要となる。ここでは、相互署名に基づく電子契約プロトコルを用いて否認防止機能を実現する[1]。

３．セキュアMODシステムの実装方針

・方針１　ソフトウェアの効率的な開発を目的として、市販WWWクライアント（ブラウザ）及びC/S間のプロトコルであるハイパーテキスト転送プロトコル（http）にできるだけ変更を加えない構成を実現する。

・方針２　安全性の向上を目的として、WWWクライアント（ブラウザ）や端末に依存しない個人秘密情報の管理を実現する。

・方針３　検索情報毎あるいは検索情報の内部に関わる極め細かなセキュリティサービス（例えば、検索情報で必要な部分だけを暗号化する機能など）の提供を目的として、アプリケーション層におけるセキュリティ機能を実現する。

４．セキュアMODのシステム構成

３章の実装方針に基づく本システムの構成について以下に述べる（図１参照）。

４.１　クライアント端末

４.１.１　ブラウザ：　本部は、検索要求の結果として、各種サーバからの検索情報を利用者に表示するブラウザ機能を提供する。ここでは、実装方針１に従い、既存のWWWブラウザをそのまま利用する。このため、各社ブラウザに依存しない共通のセキュリティ機能の実現が可能となる。

４.１.２　暗号処理機能付きICカード：　実装方針２に従い、各利用者に暗号処理機能付きICカードを配付し、各利用者の個人情報（鍵情報等）の管理や、暗号アルゴリズムの処理をICカードの内部で行うこととする。ここで、ICカードの耐タンパー性によりクライアント端末上に各利用者の個人情報が露呈せず、システムの安全性が向上する。また、各利用者がICカードを携帯することにより、他のすべてのクライアント端末においても同一のサービスを享受でき、利便性が向上する。

４.１.３　セキュリティ用ローカルサーバ：　実装方針１に従い、クライアント端末内でのセキュリティ処理（例えば、クライアント端末に接続されるICカードとの連携動作など）は、すべてクライアント端末内に設けたセキュリティ処理専用の本ローカルサーバで行うこととする。

４.１.４　CGIプログラム群：　実装方針３及び実装方針１に従い、httpの上位アプリケーション層において各種セキュリティ機能（例えば、相互認証機能）を実現するため、上記ローカルサーバ上でのセキュリティ処理は、共通ゲートウェイインターフェース（CGI）を介して行う。ここで、本部はCGI経由で呼び出される各種セキュリティ処理プログラムの集合体である。

４.２　ゲートウェイサーバ

本部は、本システムの利用者が最初に接続する遠隔のサーバであり、（１）クライアント端末のブラウザと通信するためのハイパー文書サーバ、（２）各利用者のログ情報の取得や各情報提供者

Implementation of Secure Multimedia On Demand System using WWW
Toshiaki Tanaka, Satoshi Hada and Mitsuru Yamada
KDD R&D Labs.
2-1-15 Ohara, Kamifukuoka-shi, Saitama 356, Japan

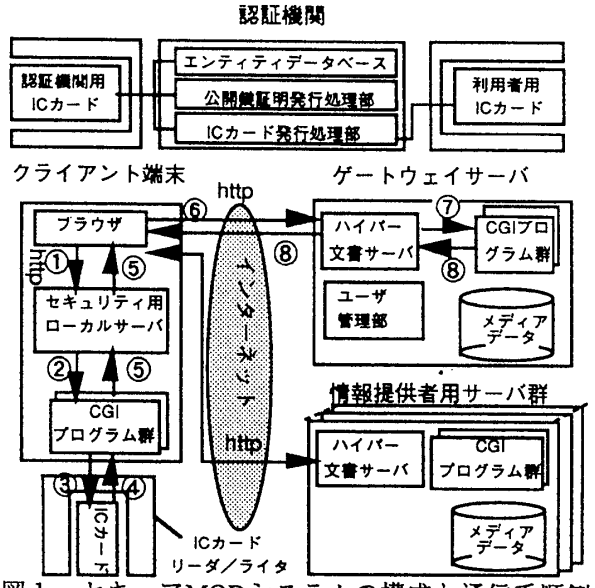

図１　セキュアMODシステムの構成と通信手順例

サーバへのアクセス制御を行うユーザ管理部、（３）ブラウザに表示されるHTML文書を構成する各メディア情報（例えば、静止画やテキスト情報など）を格納するメディアデータ、及び、（４）4.1.3節と同様に、クライアント端末からの要求に従い各種セキュリティ処理をCGI経由で実行する際に、その実行の対象となるCGIプログラム群から構成される。

4.3　情報提供者用サーバ群

本部は、利用者の要求に従い各種のコンテンツ（マルチメディア情報）を提供するためのサーバであり、複数のサーバからなる。各サーバはユーザ管理部を持たない点を除いて、ゲートウェイサーバと同じ構成をなす。

4.4　認証機関

本部は、各エンティティ（利用者や情報提供者用サーバなど）の公開鍵証明を発行するとともに、利用者に対しては、ICカードの発行処理も行う。本部は、（１）各エンティティの鍵生成処理及び公開鍵証明の生成を行う公開鍵証明発行処理部、（２）公開鍵証明を発行した各エンティティの登録及び検索などを行うエンティティデータベース、（３）生成された利用者の秘密鍵及び公開鍵証明をICカードの内部ファイルに書き込むICカード発行処理部、（４）認証機関のアプリケーションを起動する際、必要となる認証機関用ICカード、及び、（５）ICカード発行時に、当該利用者の秘密情報が書き込まれる利用者用ICカードから構成される。

但し、公開鍵証明の発行における発行要求／配付処理については、オフラインもしくは本システム外で行うこととする。

5．通信手順

図１を用いて、クライアント端末が作成した認証情報をゲートウェイサーバが検証する相手認証の手順を例にとり、通信手順の概要を述べる。

（１）クライアント端末での認証情報の作成

ブラウザに表示されたHTML文書上の認証要求リンクを利用者が起動すると、セキュリティ用ローカルサーバに対して、認証情報作成用CGIプログラムの実行を要求する(①)。セキュリティ用ローカルサーバでは当該CGIプログラムを実行する(②)。CGIプログラム内ではICカードに対して、認証情報の作成処理を依頼する(③)。ICカード内で利用者の秘密情報を基に認証情報を作成し、結果をCGIプログラムに返す(④)。CGIプログラムが認証情報を含むHTML文書を作成しブラウザに返す(⑤)。

（２）ゲートウェイサーバでの認証情報の検証

作成された認証情報を用いて、ブラウザからゲートウェイ上のハイパー文書サーバに対して、検証用CGIプログラムの実行要求を行う(⑥)。ハイパー文書サーバでは、当該CGIプログラムを実行する(⑦)。検証結果がもし正常あるいは異常な場合、認証が正常あるいは異常であることを示すHTML文書をそれぞれ生成し、ブラウザに返す(⑧)。

6．実装

上記のシステム構成に従い、実装を行った。クライアント端末及び認証機関はPC (IBM-AT互換機: OSはDOS/V及びWindows3.1）を、ゲートウェイサーバ及び情報提供者用サーバはSUNワークステーション（SS10相当:SUN OS4.1.3）を用いた。また、ICカードは公開鍵暗号(RSA)処理を内蔵したBULL社製を採用した。さらに、SUN上のハイパー文書サーバ及びPC上のセキュリティ用サーバとして、NCSA httpd及びWindows httpdをそれぞれ用い、ブラウザはMosaic及びNetscapeにて動作を確認した。セキュリティ処理のためのCGIプログラムはC言語を、認証機関におけるWindows上のユーザインタフェースはVisual Cを用いてそれぞれ開発した。

ICカードと連携したセキュリティ処理の応答時間については、認証情報の作成をブラウザからhttpを介してセキュリティ用ローカルサーバに依頼した場合（５章の①から⑤まで）、RSAの法が512ビット、秘密鍵の長さ509ビットの１ブロック処理で２秒程度であり、ほぼ実時間の処理が可能であった。

7．むすび

本稿では、オンデマンド型マルチメディア情報検索サービスで必要となるセキュリティ機能をWWW上に実装し、上記サービスの実現性と有効性を確認した。今後は、認証機関との各エンティティ間のプロトコル等について検討を進める予定である。最後に、日頃ご指導いただく、KDD研究所浦野所長、羽鳥グループリーダに感謝します。

参考文献

[1] 田中,山田 "オンデマンド型マルチメディア情報検索におけるセキュリティ機能の検討" 第51回情処全大(1995).　[2] ISO 9798-3(1994).