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

7F－6　田中俊昭　山田　満
KDD研究所

1．はじめに

近年、VOD（ビデオオンデマンド）やMOD（マルチメディアオンデマンド）などの情報検索サービスが広帯域通信での有望なマルチメディア通信サービスと考えられている。ここで、上記サービスを安全に行なうには情報セキュリティ技術が必須となる。そのなかでも、電子署名技術に基づく否認防止機能は、今後、テレショッピングなどのネットワーク上で多様なマルチメディアサービスを実現するために重要な技術と考えられる。そこで、本稿ではオンデマンド型マルチメディア情報検索における否認防止機能を実現するための要件や実現メカニズムについて述べる。

2．オンデマンド型情報検索の通信モデル

オンデマンド型情報検索は、複数のクライアントと1つあるいは複数のサーバがネットワークを経由して接続される。このようなシンプルな通信モデルを利用して、ビデオオンデマンド、テレショッピング、ネットワークゲームや電子決済など多種多様なサービスを実現する。

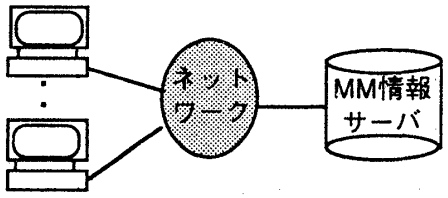


図1　オンデマンド型情報検索の通信モデル

3．オンデマンド型情報検索のセキュリティ基本要件

上記の通信モデルを用いて多種多様なマルチメディアサービスを構築する際、以下に示すセキュリティ機能を考慮する必要がある。

（1）相手認証機能

不正なりすましを防止するために相手認証機能が必要となる。相手認証機能としては、サーバ認証／クライアント認証／相互認証が考えられ、目的に応じて使い分ける必要がある。例えば、クライアントの秘密情報をサーバに提示する場合はサーバ認証を行い、閉じたグループ内で情報を提供する場合はクライアント認証を行うなど。

（2）情報秘匿機能

情報検索の結果得られる付加価値の高いマルチメディア情報が盗聴され無断で複製されることを防止する、また、利用者固有の秘密情報（例えば、パスワードなど）や個人の嗜好などのプライバシー情報が第3者に露呈することを防止するため、情報秘匿機能が必要となる。

（3）否認防止機能

情報授受の過程において、不正が行われると情報提供者と情報享受者の間で利害が生じる場合（例えば、テレショッピングや電子契約など金銭的な授受が発生する場合など）、送信者／受信者の送信／受信事実を第3者に証明できる否認防止機能が必要となる。

本稿では否認防止機能に着目し、オンデマンド型情報検索に有効な否認防止メカニズムの検討を行う。

4．否認防止機能が利用される情報検索AP

否認防止機能が利用される情報検索として以下のアプリケーション（AP）が考えられる。

（1）APダウンロード　エンタテイメントなどのアプリケーションソフトウェアを一括してクライアントに転送し、すべてのデータを転送し終えた後、アプリを実行するAP。

（2）VOD　クライアントの要求に従い、所望の映像をMM情報サーバから取得するAP。本形態では、広帯域情報である映像を符号化アルゴリズムにより圧縮して伝送するため通常ハードウェアにより処理される。また、映像は数時間程度のデータを扱うため、クライアント側で受信と同時に再生を行うストリーミング転送方式が用いられる。さらに、クライアントの所望の再生位置で停止し、リプレイのために巻戻すといった映像の遠隔制御も行われる。

（3）電子契約　従来、紙ベースで行われていた契約をネットワーク上で行うAP。すなわち、ネットワーク上で相互（例えば2者間）に、契約書に記載されている各項目を確認し同意した後、双方が契約書に対して電子署名を施す。

各APの実行結果として、上記の（1）及び（2）では、ネットワークを介して所望のデータが得られる。但し、（1）は常に一括転送されクライアントに蓄積されるデータがサーバ上に存在するAPデータと同一であるのに対し、（2）は、クライ

Study on Security Mechanism for On Demand Multimedia Information Retrieving System
Toshiaki Tanaka and Mitsuru Yamada
KDD R&D Labs.
2-1-15 Ohara, Kamifukuoka-shi, Saitama 356, Japan

アントが停止／巻戻しなどの遠隔制御を伴うため、サーバに蓄積されている映像データと伝送される映像データが完全に同一ではない場合がある。一方（3）は、契約の結果、金銭・物品などの授受は本情報検索サービスとは独立して行われる。

5．否認防止メカニズム

本稿では、処理やプロトコルの簡易性を考慮し、4章で示した各種情報検索APに汎用的に適用できる否認防止メカニズムを検討する。ここで、MM情報サーバは、信頼できるものと仮定する。

（1）及び（2）において、所望データの受信証明を送信側に提示する手法としては、受信データに対して、受信者の秘密鍵を用いてディジタル署名を施し、これを受信証明として提示する方法が提案されている[(1)]。しかしながら、受信者の不正（故意に受信証明を提示しない）が容易であることや、（2）の場合には、映像という多量なデータにディジタル署名を施す点、クライアントからの遠隔制御の結果伝送されるデータがサーバに蓄積された映像データと異なる点、さらに、映像データがハードウェアで処理される点を考慮すると、受信データに対してディジタル署名を施して受信証明を作成するのは、現実的ではない。従って、本稿では、契約書を用いて事前に相互にディジタル署名を行った後に、所望のデータをネットワークを介してクライアントに送信するメカニズムを提案する。以下にVODを例にした手順を示す。

[情報検索手順]

1）MM情報サーバ（IP）からクライアント（A）に対してメニューが表示され、各メニューには所望のデータに関連する映像のタイトルや上映時間、金額、発行時間TIPなどが表示されるとともに、Aの識別子A、IPの識別子IP、及びIPが発信元であることを証明するためIPの秘密鍵によるディジタル署名（SIGIP）が付与される。

2）クライアントAが所望のメニューを選択すると、そのメニューに付与されたMM情報サーバの署名情報（SIGIP）の正当性をMM情報サーバの公開鍵を用いて検証する。

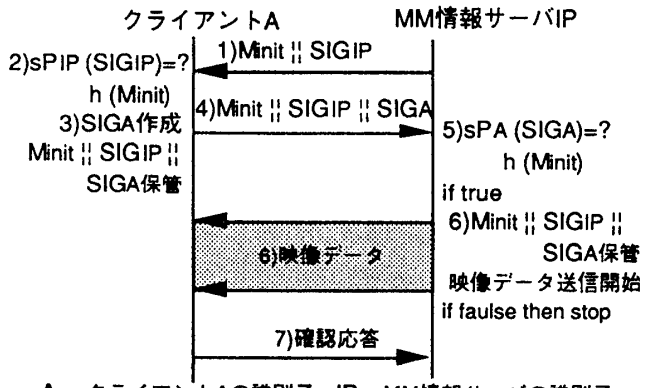
3）上記2）の検証が正しい場合は、クライアントAの秘密鍵を用いて初期メニュー情報Minitに対してディジタル署名を作成する（SIGA）。本情報を受信情報（Minit ‖ SIGIP）と結合し、結合データ（Minit ‖ SIGIP ‖ SIGA）を保管する。2）の結果が正しくない場合には処理を中断する。

4）上記結合データをMM情報サーバに送信する。

5）MM情報サーバでは、付与されたクライアントAの署名情報（SIGA）の正当性をクライアントAの公開鍵を用いて検証する。

6）上記5）が正しい場合には、受信データ（Minit ‖ SIGIP ‖ SIGA）を保管し、所望の映像データの送信を開始する。5）の結果が正しくない場合には処理を中断する。

7）映像データを正常に受信するとクライアントAは確認応答をMM情報サーバに送信する。



A = クライアントAの識別子，IP = MM情報サーバの識別子，
TIP = IPが付与する時変情報，‖：データの結合処理，
Title-Info = 映像に関する情報
（タイトル、上映時間、金額など），
sSxx：xxの秘密鍵を用いた公開鍵
アルゴリズムによる復号処理，
sPxx：xxの公開鍵を用いた公開鍵
アルゴリズムによる暗号処理，
h( )：ハッシュ関数，Minit = A ‖ IP ‖ TIP ‖ Title-Info，
SIGIP = sSIP (h (Minit))，SIGA = sSA (h (Minit))

図2　否認防止プロトコル（VODの例）

6．実現メカニズムの安全性

本方式は、クライアントが情報を享受する前に契約書にディジタル署名を行うため、受信の証拠はMM情報サーバに得られ、その結果クライアントでの受信の否認などの不正は不可能となる。また、契約書が時変情報やクライアントとMM情報サーバの識別子を含む署名情報を作成しているため、情報検索の度にクライアントがMM情報サーバを認証していることになり、不正なMM情報サーバがクライアントとの間で5章の手順を成功させることは不可能となる。

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におけるセキュリティ機能に関して、否認防止機能に着目し、多様なアプリケーションに適用可能なメカニズムの提案を行った。今後は、本メカニズムを実装するとともに、その他、認証機能や情報秘匿機能についても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、村上次長、羽鳥グループリーダに感謝します。

参考文献

[1] CD13888-3 Non-Repudiation Part3: Using asymmetric techniques (1995).