5R－8

マルチメディアサーバシステム(4)
－ セキュリティ管理 －

井上淳　清原良三
三菱電機(株)情報技術総合研究所

1　はじめに

クライアント/サーバ(以下 C/S と示す)型のマルチメディアサーバシステムでは、システムがサービスする動画や静止画などのデータは課金や著作権保護の対象であることが多い。このようなデータを取り扱うシステムでは、必要に応じてユーザを特定し、また特定のユーザによるデータの利用を制限できる仕組みが必要である。

本稿ではまず、イントラネット環境で使用するマルチメディアサーバシステム[1]に必要なセキュリティ機能のうち、特にデータのアクセス権制御とダウンロード制御について述べる。

2　マルチメディアサーバのアクセス権制御

イントラネットで使用する C/S 型マルチメディアサーバシステムにおいて必要なアクセス権制御機能を次に示す。

①実行権制御
システムの提供するサービスの実行はユーザ/サービス毎に許可/不許可を制御する。

②データアクセス権制御
予め設定したアクセス制御情報に基づきユーザ毎にデータへのアクセスを制限する。

③データダウンロード制御
マルチメディアサーバに格納するデータは課金対象、著作権保護の対象であることが多い。このため、必要に応じてシステム外へのデータの取り出し(他媒体へのコピー、クライアントへのダウンロード)を抑止する。

④接続権制御
ユーザからのシステム接続要求に対して、許可していないユーザの接続を制限する。

3　アクセス権制御の統合化

本システムは、PC プラットフォームを使用した普及型システムであり、必要に応じてビデオサーバを追加することにより動画配信数をスケーラブルに向上可能なシステムである[1]。システムは以下に示す機能別の複数サーバで構成する。

- ビデオサーバ(動画サービス)
- ファイルサーバ(静止画サービス)
- データベースサーバ(データ管理)
- コントロールサーバ(システム管理)

これらのサーバは PC プラットフォームにおいて標準的な第三者 S/W であり、独自のセキュリティ機能を持っている。例えばデータベースサーバの接続権制御やテーブルへのアクセス権制御の機構は、ビデオサーバのデータへのアクセス権制御と方式は同一ではない。よって各サーバへのアクセス手段の違いをアプリケーションに意識させず、またユーザに対して必要なアクセス権制御機能を提供するため、各サーバのアクセス権制御をシステムが統合して提供すべきである。

図 1にセキュリティシステムの構成図を示す。複数

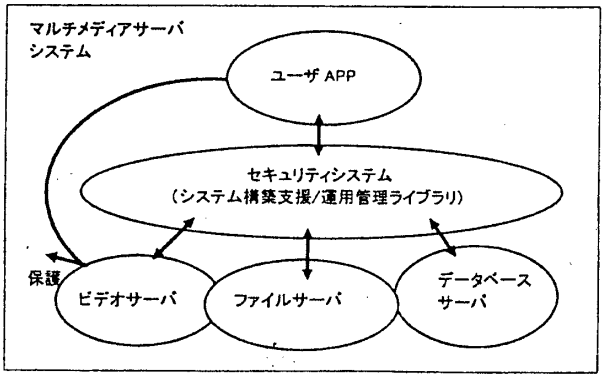

図1 セキュリティシステム構成図

Multimedia Server System(4) -Security Control-
Jun Inoue, Ryozo Kiyohara
Information Technology R&D Center, Mitsubishi Electric Corporation

サーバの統合アクセス権制御実現のため、クライアントアプリケーションとサーバの間にセキュリティ処理を行う階層を設けた。

本システムでは、アプリケーションからのマルチメディアサーバへのアクセスは、必ずクライアントに搭載したシステム構築支援ライブラリ、コントロールサーバで動作する運用管理ライブラリを経由させる。またライブラリを使用しないアプリケーションからのアクセスに対して、各サーバはパスワードなどによる単体の保護機能によりそのデータとリソースの利用を禁止する。

ライブラリは、アプリケーションからの処理要求に対し、各サーバへの必要なデータへのアクセスを実行する。アプリケーションは各サーバを意識することなく、各種データへのアクセスを実行する。セキュリティ機能は、このライブラリに実装する。それぞれのサーバとの接続やデータの転送に関して、マルチメディアサーバ・セキュリティシステムが、アプリケーションに対して、各サーバとの接続を透過的に提供できる。

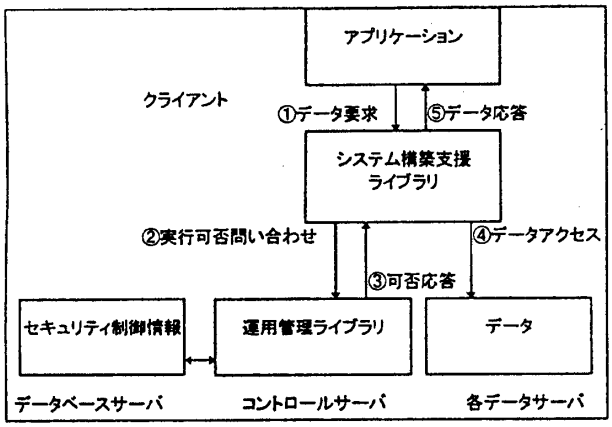

図2 処理の流れ

コントロールサーバ上の運用管理ライブラリと、クライアント上のシステム構築支援ライブラリで実行するアクセス権制御処理を図2に示す。

①アプリケーションはシステム構築支援ライブラリに対してデータの転送要求を行う。

②システム構築支援ライブラリは実行する処理について実行の可否を運用管理ライブラリに問い合わせる。

③運用管理ライブラリはクライアントからの問い合わせを、データベースの内容と照合して、クライアントに実行可否を応答する。

④システム構築支援ライブラリは応答結果に基づいて各サーバへの処理を実行する。

⑤アプリケーションはシステム構築支援ライブラリよりデータを受取る。

このように、処理実行問い合わせと実際のデータアクセスの実行をクライアントライブラリ内部で連続して実行することにより、これらの処理はアプリケーションに対して透過的となる。

4 データダウンロード制御

一般的なビデオサーバでは、ファイルを見ることと、複写することを特に区別していない。2-③で示したデータダウンロード制御機能を実現するためには、OS やサーバの制御するデータダウンロードを抑止しなければならい。

これについては、3と同様に各サーバの接続パスワードをセキュリティライブラリが秘匿することにより、ユーザやアプリケーションがサーバと直結してデータ転送を行うことを禁止可能である。ダウンロード機能は各単体サーバとクライアントのシステム構築支援ライブラリ間のデータ複写として実現する。

5 おわりに

マルチメディアサーバの必要とするデータのアクセス権制御を、機能別複数サーバからなるシステムをターゲットとして実装した。現在、さまざまなデータ型やそれを扱うことのできるサーバが数多くあり、その盛衰は激しい。機能別複数サーバシステムを使ったシステムでは、その実装において調整すべき点は多いが、システム構成を大きく変えずに新たな機能を取り入れられることの意義は大きい。

参考文献

[1] 清原他、"マルチメディアサーバ(1)概要"、情報処理学会第53回全国大会論文集(本誌)、5R-05