WWWにおけるコンテンツアクセス制御の提案

2Y－7

岩崎　晃也　森廣　政治
NTT情報通信研究所

1. はじめに

近年、インターネットやイントラネットにおいてWWWを利用した多様な情報サービスが急速に展開されつつある。WWWはもともと不特定多数の利用者への情報公開を意図したものであったが、サービスの多様化に伴い公開する情報の範囲を利用者毎に制限することのできるアクセス制御方式が求められている。

本稿ではこれを簡易に実現するいくつかのアクセス制御方式について考察する。

2. 利用者の集合に応じたアクセス制御

製品情報などをWWWで提供する場合、不特定多数の「一般ユーザ」、メールアドレスなど簡単な登録をすませた「登録ユーザ」、製品を購入した「正規ユーザ」といった図1に示すような利用者の集合に対応して情報（以下コンテンツと呼ぶ）へのアクセス制御を実現する必要がある。ただし、各コンテンツは1つのファイルからなるものとする。このとき重視すべき条件として以下のものがある。

要求条件

条件1：コンテンツのアクセス権限情報の管理が容易であること

条件2：URLがコンテンツのアクセス権限に依存しないこと

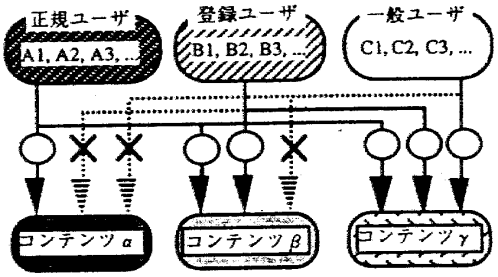

図1　利用者の集合に応じたアクセス制御

3. アクセス制御方式

上述のような条件を満たす制御方式として以下のものが考えられる。

案1：サーバプログラムがコンテンツアクセス権限情報を独自に持つ方式

案1-1：ディレクトリ毎にアクセス権限情報を持つ方式

案1-2：ファイル毎にアクセス権限情報を持つ方式

案2：OSのファイルアクセス権限情報を用いる方式

案2-1：OSがアクセスを制御する方式

案2-2：CGI[1]プログラムがアクセスを制御する方式

以下で各々の方式の概要を示す。

3.1 サーバプログラムがアクセス権限情報を持つ方式

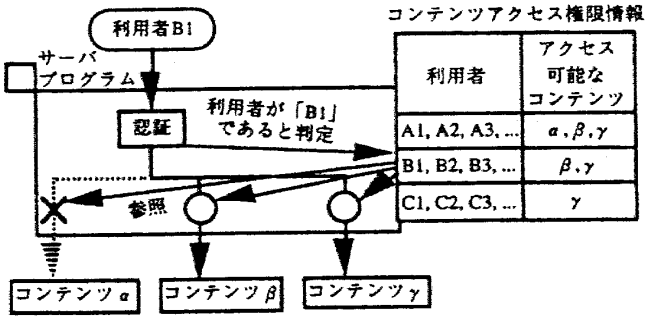

図2　サーバプログラムがアクセス権限情報を持つ方式

各利用者ごとのアクセス可能コンテンツのリストをサーバプログラム独自の情報として用意し、利用者を認証してそれに基づきアクセスを制限する方式で、現在最も一般的な方式である[2][3]。コンテンツの管理単位により、同じ公開範囲を持つファイルを同一ディレクトリに格納しディレクトリごとにアクセス権限情報を用意する方式（案1-1）、図2に示すようにファイルごとにアクセス権限情報を用意する方式がある（案1-2）。これらの方式では、コンテンツは公開範囲によらずOS上でサーバプログラムにアクセス権限があればよい。

3.2 OSがアクセスを制御する方式

利用者の集合ごとに対応するアクセス権限を持つOSのユーザアカウントを新たに用意し、それぞれのユーザの権限で動くサーバプログラムを用いることにより、OSのアクセス制御機能でコンテンツへのアクセスを制御する方式である（図3）。利用者はURL中でポート番号を指定して自分自身の権限に

A Study on Access Control Mechanism for WWW
Akiya Iwasaki and Masaharu Morihiro
NTT Information and Communication Systems Labs.
1-1 Hikarinooka, Yokosuka, Kanagawa 239, Japan

対応するサーバプログラムを特定する。各サーバプログラムは利用者を認証して権限を持たない利用者のアクセスを排除する。また、他のサーバからリンクを張る際にポート番号の差異を隠蔽するため標準ポートのサーバプログラムを用意し、利用者に各々のサーバプログラムへのリンク情報を提示させる。

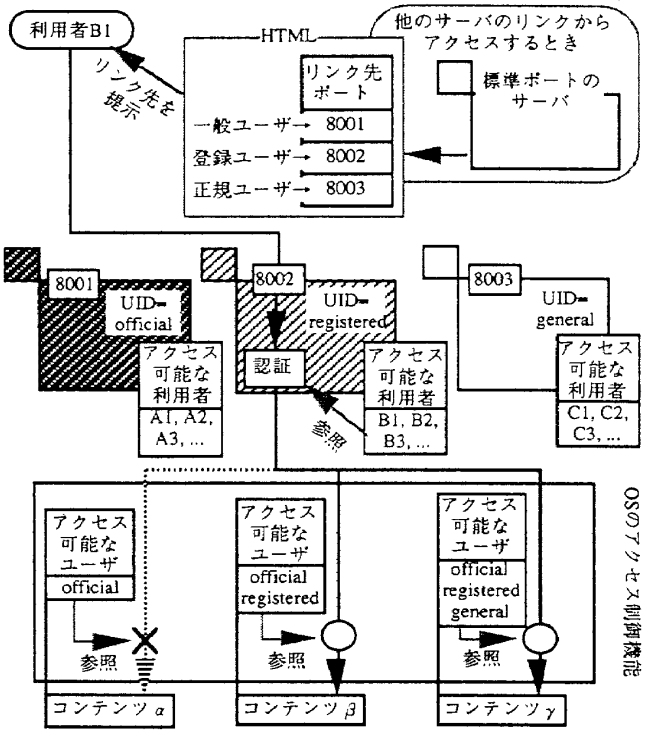

図3　OSがアクセスを制御する方式

3.3 CGIプログラムがアクセスを制御する方式

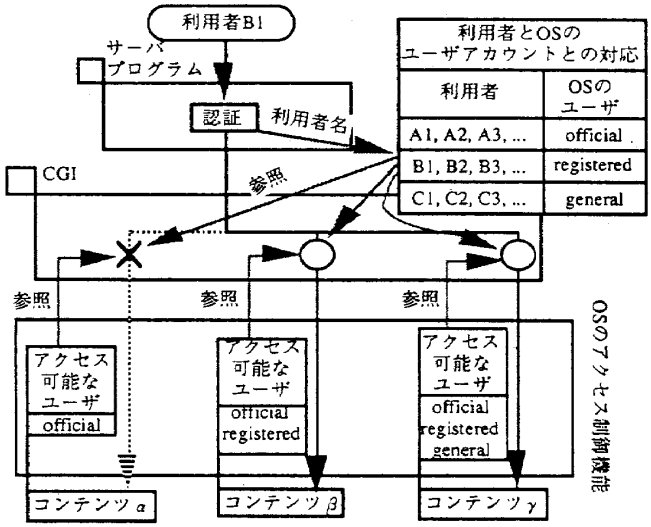

図4　CGIプログラムがアクセスを制御する方式

CGIがWWWにおける利用者のアクセス権限とOS上でのコンテンツのアクセス権限を対応づけることによりアクセスを制御する方式である（図4）。サーバプログラムはCGIにアクセスする利用者の認証を行い、利用者名をCGIに渡す。CGIは、利用者名とOSのユーザアカウントとの対応情報、及びOSのファイルアクセス権限情報を参照してアクセス制御を行う。

4. 評価

先に述べた要求条件に基づく各方式の比較を表1に示す。

表1　各方式の比較

	案1-1	案1-2	案2-1	案2-2
条件1	△	△	○	○
条件2	×	○	×	○

案1-1では同じアクセス権限を持つコンテンツを同じディレクトリに格納すれば必要なアクセス権限情報の量が少なくて済むが、コンテンツのアクセス権限変更の際ディレクトリを移動させなければならず、URLが変わってしまう。案1-2ではコンテンツ毎にアクセス権限情報を作成するのに稼動がかかり、アクセス権限の管理が煩雑である。一方案2-1及び案2-2ではOSの機能を利用しているのでOS付属のユーティリティで容易にアクセス権限の管理ができるが、案2-1では他のサーバのリンクから利用者の集合に対応するポート番号のサーバプログラムにアクセスする際に標準ポートのサーバプログラムを経由するため2回の動作が必要になる。これらを考慮すると、CGIプログラムを作成する必要はあるが案2-2がWWWにおけるアクセス制御方式として最適である。

5. まとめ

CGIを用いてOSのアクセス制限情報を利用する、WWWにおけるコンテンツアクセス制御方式を提案した。今後はこれらを実装し、システムへの負担や実行性能を含めて各方式を評価する。

参考文献

[1] D. Connolly, *"CGI: Common Gateway Interface"*, http://www.w3.org/hypertext/WWW/CGI/Overview.html

[2] *"Mosaic User Authentication Tutorial"*, http://hoohoo.ncsa.uiuc.edu/docs/utorials/user.html

[3] *"Apache Week Feature: Using User Authentication"*, http://www.apacheweek.com/features/userauth