4T−1

マルチメディア分散在席会議システム MERMAID
—— グループ情報管理 ——

福岡 秀幸*　広明 敏彦*　東 浩**　柳生弘之**　渡部 和雄*
*日本電気(株) 関西C&C研究所　**日本電気技術情報システム開発(株)

1 はじめに

近年、企業の分散化・国際化、業務の多様化が急速に進むにつれて、組織や場所を越えたコミュニケーション手段が必要になってきており、ネットワークを介してグループ協同作業を支援するグループウェアに注目が集められてきている。「グループ」という概念を考えると利用者や資源の属性情報の管理がより複雑になり、グループウェアの大きな問題となってきている。

筆者らはグループウェアの基盤環境として、広域・多者間で利用可能なメディアを全て扱える、WSを利用したリアルタイム型の会議システムの研究を進めてきた[1][2]。本稿では、マルチメディア分散在席会議システムMERMAID (Multimedia Environment for Remote Multiple Attendee Interactive Decision-making) のグループ情報管理について述べる。

2 グループ情報管理の問題

グループウェアの世界では、グループ情報管理をどのようにして行なうかということが大きな問題となってきている。従来の1対1の通信の世界では、「何処」にある「どの」情報を「誰」に「どういう」経路で送るかというディレクトリの問題や、「どの」情報を「誰」が触っても良いかというアクセス制御の問題は古くから大きな問題として取り扱われてきたが、グループウェアではそれに複数の人が集まった「グループ」という概念が加わり、「誰と誰」が「何処と何処」にということを考えねばならないためセキュリティの問題が複雑である。

2.1 管理すべき利用者情報

1対1のトランスペアレントな通信が保証されていることを前提にしても、その上にグループウェアのアプリケーション(AP)を構築していくためには色々なグループ情報を独自に管理することが要求される。管理すべき情報を大きく分類すると次の3つが挙げられる。

利用者の属性情報　氏名、所属、電話番号、メールアドレス、グループ名、パスワード、他

共有APに依存する情報　会議名、キャビネ名、フォルダ名、文書名、利用者の状態情報、グループの状態情報、他

インフラに依存する情報　マシン名、ネットワーク名、デバイス名、他

2.2 グループ情報とセキュリティ

グループウェアのAPを実行するためには、それに先立ってグループという関係を生成しなければならない。グループメンバ招集時に「誰と誰をどういう名前で呼び出すか?」ということが問題となる。使い勝手から言えば、招集者は電話番号やアドレスを知らなくても、グループメンバの氏名やグループ名だけを知っていて簡単に呼び出すことが出来れば理想的であるが、反面、そういった識別情報を集中管理してアクセスを容易にするとセキュリティが守りにくい。

また、グループウェアではグループで共有される共有文書という概念が存在するが、「共有文書は誰の所有物か?」という問題がある。例えば会議文書は、利用者個人の所有物であるとすると他のグループメンバが読むことができなくなるし、会議の所有物であるとするとグループ以外の人に読まれない工夫をする必要がある。

アクセス権の管理は、使い勝手とセキュリティのトレードオフということになる。OSやインフラにも依存する部分がかなり多く出て来るため、共有される全ての情報を暗号化しない限り本気でセキュリティを守ることは困難であるが、今後グループウェアを世の中に普及させるためには、このジレンマは避けて通れない問題である。

3 MERMAIDにおけるグループ情報管理

MERMAIDはグループ通信アーキテクチャに基づいて設計されており、会議及び利用者に関する情報は会議情

Multimedia Distributed Multiparty Desktop Conferencing System "MERMAID" —— Group Information Management ——
Hideyuki FUKUOKA*, Toshihiko HIROAKI*, Hiroshi AZUMA**, Hiroyuki YAGYU**, Kazuo WATABE*
*KANSAI C&C Research Laboratory, NEC Corporation
**NEC Scientific Information System Development, Ltd.

報サーバ (CIS: Conference Information Server) によって管理されている [3]。CIS は MERMAID システムで 1 つだけ存在し、全ての会議の運営管理と全ての利用者の情報管理を行なう。

3.1 会議運営管理

CIS は全ての会議の開始、終了、予約、参加、退席などの状態を常に監視し、全ての会議の名称、参加者名、会議状態を CIS のプログラム内部に持つテーブルで管理する。図 1. に示すように、利用者や他のサーバからの要求に応じてこれらの情報を提供する。

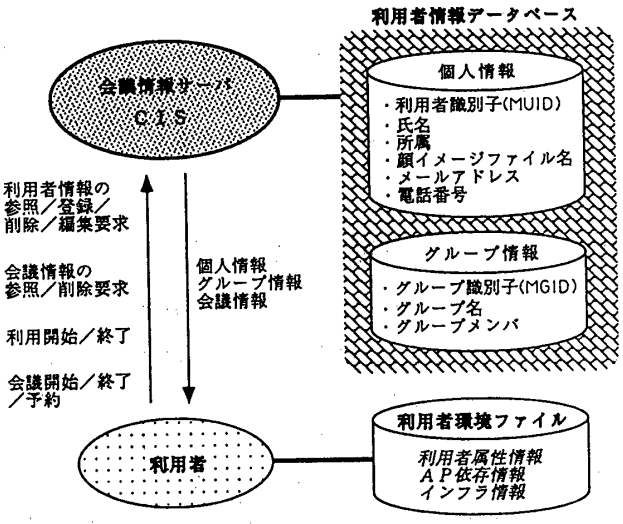

図 1. 会議情報サーバによるグループ情報管理

3.2 利用者情報管理

MERMAID では、会議招集時に利用者の利用場所を特定するために CIS が全ての利用者の状態を常に監視しており、CIS のプログラム内部に持つテーブルで管理している。また、利用者に関する属性情報は CIS が管理する「利用者情報データベース」と、利用者自身が管理する「利用者環境ファイル」に納められている (図 1.)。

利用者情報データベースには、全ての MERMAID 利用者の個人属性情報 (識別子、氏名、所属、顔イメージファイル名、メールアドレス、電話番号) と、グループ属性情報 (識別子、グループ名、メンバ) が格納されている。

利用者環境ファイルには、利用者情報データベースで管理されている利用者個人の属性情報に加えて、接続するサーバ名や利用キャビネ名など AP に依存する情報、マシン・ネットワーク環境や入出力デバイス名など利用者の WS や利用形態に依存する情報が管理されている。これらの情報を利用者自身は読むことが出来るが、会議開始時に AP 側で参照するため利用者は特に意識する必要はない。

3.3 アクセス権管理

MERMAID の利用者は、利用者識別子 (MUID) を持っている。これは CIS が乱数を発生させて利用者一人一人に固有の番号を割り当てるものであり、利用者情報データベースの中と、その MUID の利用者自身の環境ファイルにのみ書かれている。利用者は自分の MUID だけは知ることができるが、通常は MUID の存在を全く意識せずに会議に参加することができる。

同様に、MERMAID の利用者間でグループが形成されると、CIS がグループに固有のグループ識別子 (MGID) を割り当てる。会議に先立ってグループを登録することによって、利用者は MGID を用いてグループメンバを会議に呼び出すことができる。また MGID を利用することにより、会議文書をグループの所有物とすることができる。

MERMAID のアクセス権管理はこの MUID と MGID を用いて実現されている。利用者がデータベースに新規に利用者情報を登録したり、削除したり、或いは変更を加えたりする場合には、MUID と MGID がパスワードの役割を果たし、CIS がそれを照合することによりデータベースをアクセスする権限が利用者或いはグループに与えられる。

4 まとめ

グループウェアにおけるグループ情報管理の問題点を指摘し、マルチメディア分散在席会議システム MERMAID における会議運営管理、利用者情報管理、アクセス権管理について述べた。今後は、ヒューマンインタフェースとセキュリティの両方の側面を考慮に入れながら、本稿の中で述べたグループ情報管理の問題点を解決していく予定であり、広くグループ協同作業を支援するための汎用的なグループ情報管理・アクセス権管理方式の実現を目指している。

参考文献

[1] 福岡他「マルチメディア分散在席会議システム MERMAID」国際シンポジウム Computer World '90 論文集、(1990.11).

[2] 渡部他「マルチメディア分散在席会議システム MERMAID」情処学会マルチメディア情報と分散協調シンポジウム、(1989.11).

[3] 阪田他「グループ通信アーキテクチャ −マルチメディア分散会議システム構築のための基本概念−」信学オフィスシステム技報 OS89-4、(1989.9).