仮名を用いた匿名電子会議システムの設計と実装

3Y−2

福島茂之†, 廣瀬勝一††, 池田克夫†
†京都大学工学研究科情報工学専攻, ††京都大学工学研究科電子通信工学専攻

1 はじめに

今日，情報ネットワークの普及・拡大にともなって，遠隔会議のような電子会議が行われるようになってきている．遠隔会議では，参加者が直接顔を合わせないため，匿名で会議を行うことが可能となる．参加者が匿名で会議を行うことの利点は，地位や人間関係にとらわれることなく，自由に討論できることである．一方，匿名であることを悪用して，会議の進行を妨げる発言をするなどの不正の行われる可能性があるという欠点もある．本研究では，暗号技術を利用して，安全な匿名会議を可能とするシステムを提案する．

2 匿名会議における不正とその防止

匿名会議では，通常，各参加者は仮名を用いて会議に参加する．この仮名を用いた匿名会議では，次の三つの不正行為が起こりうる．

匿名性の悪用 匿名であることを悪用して，会議の進行を妨げる発言をするという不正．

なりすまし 他の参加者の仮名を用いて会議に参加するという不正．

本名の推測 ある利用者が同じ仮名を用いて複数の会議に参加する時，それらの会議に参加すると考えられる利用者の本名と仮名との対応を推測するという不正 (図 1)．

本稿で提案するシステムでは，次のようにしてこれらの不正を防止する．

匿名性の悪用については，仮名と本名の対応を管理し，参加者が不正を行った場合にのみ，その本名を必要に応じて特定できるようにする．なりすましについては，IDによるディジタル署名方式 [1] を利用して，各参加者が発言に対して仮名によって検証できる署名をつけるようにする．本名の推測については，仮名を随時変更できるようにする．

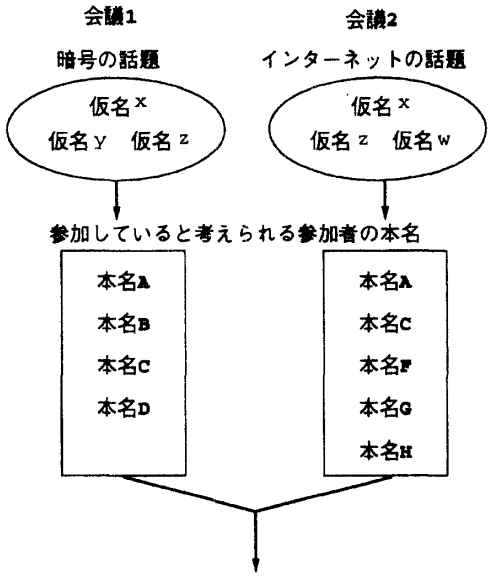

図 1: 仮名と本名の対応の推測

3 システムの構成

提案する匿名会議システムは，一つの信頼できる利用者管理センター(以下，センターと呼ぶ)と，会議ごとに用意される会議サーバ，利用者のインターフェースとなる会議クライアントから構成される(図 2)．センターでは，すべての利用者の本名と仮名の対応の管理を行う．利用者の不正があった場合は，必要に応じて，その利用者の本名を公開する．会議サーバは，会議の発言の暗号化・復号のためのセッション鍵の用意・配布 [2] [3] を行う．また，利用者の不正が生じた場合，センターにそれを通知する．会議クライアントでは，発言の暗号化・復号，発言に対する署名の付加・検証を行う．利用者は，

Design and Implementation of Anonymous Electronic Conference System with Pseudonyms

Shigeyuki FUKUSHIMA†, Shoichi HIROSE††, Katsuo Ikeda†

† Department of Information Science, Kyoto University, †† Department of Electronics and Communication, Kyoto University

会議クライアントと会議サーバを介してメッセージ通信を行う．

3.1 仮名の計算

センターは，疑似ランダム関数を用いて各利用者の本名から仮名を計算することにより，本名と仮名を対応づける．以下に仮名の計算法を述べる．

$F(k,x)$を疑似ランダム関数とする．ここで，kはインデックス，xは入力である．実用的には，例えば，秘密鍵暗号の暗号化関数が疑似ランダム関数として利用できる．

利用者の登録

本システムの利用者iは，あらかじめ，センターに自分の本名(個人情報) $name_i$を登録して，仮名と仮名によって検証されるディジタル署名のための秘密鍵を発行してもらう．利用者iの登録を受けたセンターは，k_iを秘密かつランダムに選び，以下のようにして，仮名pn_i^0を定める．

$$pn_i^0 = F(k_i, name_i)$$

ディジタル署名の秘密鍵s_i^0は，用いる方式に応じてp_i^0より計算される．

仮名の変更

利用者iは，別の会議に参加するときなど必要に応じて，センターから新しい仮名$pn_i^1, pn_i^2, \ldots$とそれに対応するディジタル署名のための秘密鍵$s_i^1, s_i^2, \ldots$を順次発行してもらう．$pn_i^j (j = 1, 2, \cdots)$は以下のようにして計算される．

$$pn_i^j = F(k_i, pn_i^{j-1})$$

s_i^jは，s_i^0と同様の方法で，pn_i^jより計算される．

以上のように，仮名$pn_i^0, pn_i^1, \ldots$と本名$name_i$の間に，k_iを用いて対応付けがなされる．k_iは秘密であるので，各利用者は通常，他の利用者の本名と仮名，ならびに仮名どうしの対応を知ることができない．

利用者iが不正を行った場合，センターはk_iを公開する．各利用者はk_iを用いて，利用者iの本名と仮名の対応を知ることができる．

4 実装

本システムの暗号処理部分は，AT&TのCryptolib [4]という暗号ライブラリを用いて実装した．発言などのメッセージの暗号化にはDES，IDに基づくディジタル署名にはShamirの方式 [1]，セッション鍵の配付には岡本の方式 [2] を用いた．Sun Ultra-1 160MHz互換機において，発言の暗号化・復号，署名の作成・検証の所要時間を計測したところ，合計1.08秒程度となった．但し，この値はネットワーク遅延を含んでいない．

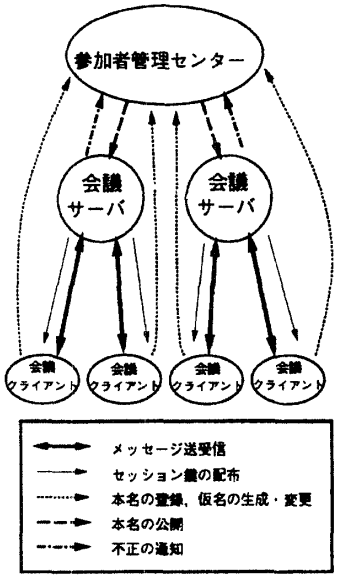

図 2: 匿名会議システムの構成

5 まとめ

本研究では，匿名会議において生じ得る不正を挙げ，それらを暗号技術を用いて防止する匿名会議システムを提案，実装した．今後の課題として，利用者のインターフェースの改良や実際の会議に対する適用などが考えられる．

参考文献

[1] A. Shamir, *Identity-Based Cryptosystems and Signatuer Schemes*, Proc. of *CRYPTO'84*, Lecture Notes in Computer Science 196, pp. 47 – 53 (1985).

[2] 岡本 栄司, IDに基づく鍵配送方式, 信学技報, IT 86–53 (1986).

[3] M. Burmester and Y. Desmedt, *A Secure and Efficient Conference Key Distribution System*, Proc. of EUROCRYPT'94, Lecture Notes in Computer Science 950, pp. 275 – 286 (1994).

[4] J. Lacy, D. Mitchell and M. Blaze, *CryptoLib Version 1.1*, AT&T (1995).