通信グループの分散管理手法の一検討

4S－8

岡崎 直宣[1]，馬場 義昌[1]，朴 美娘[1]，井手口 哲夫[2]

[1]三菱電機(株)情報技術総合研究所　[2]愛知県立大学情報科学部

1. はじめに

イントラネット等では，特定のグループ内に閉じた通信（グループ通信）を行う必要がある．グループ通信を安全に実現する方法として，例えばグループで共通の暗号鍵を持ち，データを暗号化することにより，グループの構成員以外からの通信を行えないようにする方法などがある．

グループ通信を行う際には，グループの識別（グループID）や，メンバの登録，暗号鍵などを管理する必要がある．これまで，グループ管理装置がこれらの管理を集中的に行う方法[1]などが提案されている．この場合，例えばグループのメンバの変更などグループの構成内容が変化する毎にグループ管理装置の処理が発生するなど，グループ管理装置に処理が集中するため，多数のグループが存在する大規模なシステムへの適用には限界があった．

本稿では，特定のグループ管理装置に処理が集中しないような，各通信グループによる自律的なグループの管理手法について考察する．

2. 自律的なグループの管理手法

提案するグループ管理手法の概念について述べる．

2.1 通信グループ

ここでは，通信グループ（CG）を次のように定める．以下では，CGを構成するメンバをエンティティと呼ぶ．

CG: 1つ以上のエンティティによって構成され，2つの状態（発火状態：CGが有効である状態，および，非発火状態：CGが有効でない状態）のいずれかをとる．ただし，CGが1つだけのエンティティにより構成されるときは，そのCGは非発火状態しかとれないものとする．

CG内に閉じた通信を実現するために，ここではCGで共通のデータ暗号鍵（セッション鍵）を持ち，やりとりするデータを暗号化することにより，CGの構成員以外からの通信を行えないようにする方法[1]をとることとする．

2.2 グループサーバ

本手法では，グループ管理装置の代わりに，CGの構成情報の登録のみを行うグループサーバを設ける．グループサーバには，グループIDとそのCGを構成するエンティティ，およびそのCGを管理する管理エンティティの組を登録しておく．ここで，各CGの管理エンティティは，CG内のエンティティのメンバ管理，暗号通信のためのセッション鍵の管理，他のCGとの結合や分離などのオペレーションの制御や，その手順の際のグループサーバへの問い合わせなどを行う．

図1は，3つのCG，$G1, \ldots, G3$ およびそれらのどれにも属さないエンティティ$e5$から構成される例である．このうち，例えば$G1$にはエンティティ$em1$，$em2$，$e1$，$e2$が属し，$em1$がその管理エンティティである．$em1$は，自グループのID（$G1$），管理エンティティ名（$em1$），およびメンバであるエンティティのリスト（$\{em1, em2, e1, e2\}$）をグループサーバに登録する．また，CG内の各エンティティに対して，セッション鍵（$k1$）の配布を行う．

2.3 オペレーション

CGに対する可能なオペレーションを次のように定める．

（1）結合：n個（$n \geqq 1$）のエンティティから構成されるCGとm個（$m \geqq 1$）のエンティティから構成されるCGが1つのCGとなる．

（2）分離：n個（$n \geqq 2$）のエンティティから構成されるCGがx個とy個（$x+y=n$）のエンティティから構成される2つのCGに分裂する．この時，xもしくはyが1である場合，そのCGは非発火状態にとどまる．

他に，消滅，生成，発火状態／非発火状態間の状態遷移のオペレーションを別に定める．ここで，非発火状態にあるCGのみ分離，結合等のオペレーションが行えるものとする．

3. 管理エンティティ間プロトコル

上記のオペレーションを実現するための，各CGの管理エンティティ間のプロトコルについて定める．

3.1 諸定義

以下では，集合Xに対して次のように表記する．

X^*：Xの部分集合の集合，

$X^+ = X^* - \phi$：空でないXの部分集合の集合，

$X^{++} = X^+ - X$：2つ以上の要素からなるXの部分集合の集合，

$[X]$：Xの要素の個数．

［通信グループ］

$Gr = (g, em, M, p, k)$

ここで，

$g \in G$：グループID，

$em \in ME$　：管理エンティティ，

$M \in E^+$　：CGに属するエンティティ，

$e \in E$：エンティティ，

$p \in \{\text{active, inactive}\}$：CGの状態，

$k \in K$：セッション鍵．　□

各エンティティは，複数のCGに属することができるものとする．各エンティティはまた，それ自身が管理エンティティであるような単独のエンティティからなるCGを構成するものとする．

［グループサーバ］

$GS \subseteq G \times ME \times E^{++}$　□

A Study of Distributed Method for Communication Group Management

Naonobu OKAZAKI[1], Yoshimasa BABA[1], Mi Rang PARK[1] and Tetsuo IDEGUCHI[2]

[1]Information Technology R&D Center, Mitsubishi Electric Corporation

[2]Faculty of Information Science and Technology, Aichi Prefectural University

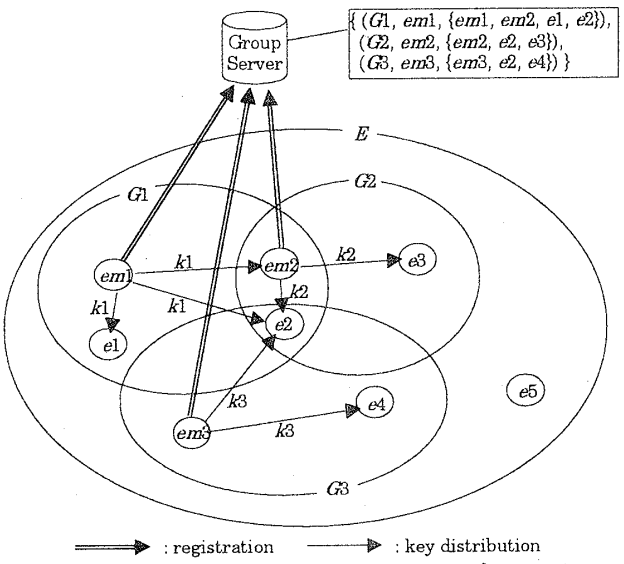

図１　通信グループおよびグループサーバ
Fig. 1　Communication Groups and Group Server.

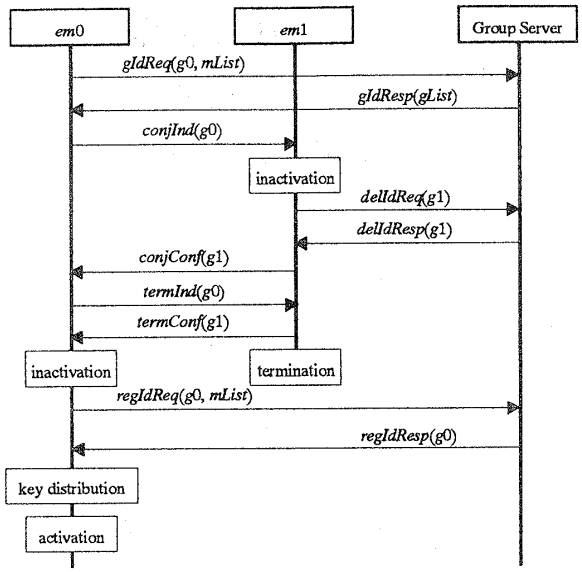

図２　結合手順
Fig. 2　Sequence of a conjunction procedure.

グループサーバには，グループIDと管理エンティティ，およびそのCGを構成するエンティティの集合の組が登録されている．ただし，単独のエンティティからなるCGは登録されない．

3.2　管理エンティティ間プロトコル

ここでは，結合アクションに関する手順について述べる．

［結合手順］

結合アクションを起動する側のCG $Gr0 = (g0, em0, M0, p0, k0)$の管理エンティティ（イニシエートエンティティ）が，新たなエンティティをメンバとしてCGに加える際の動作である（図２）．

ステップ１：

イニシエートエンティティ（*em0*）が，グループID（*g0*）と，新たに含みたいエンティティのリスト（*mList*）をグループサーバに送る（*gIdReq*）．

$mList \in (E - M0)^+$.

ステップ２：

グループサーバは，登録されている情報の中から，次のようにして結合する候補となるCGのリスト*gList*を作り，*em0*に応答する（*gIdResp*）．

$$gList = \{ (g, em, M) \mid (g, em, M) \in GS, \\ M \in (mList + M0)^+ - M0^+ \}.$$

ステップ３：

em0 は，*gList*で示されたCGの情報から，[*tgList*]が最小になるようにCGの組合わせ（*gSet*）を選ぶ．ここで，

$tgList = gSet \cup LG$,

$gSet \in TG^+$,

$TG = \{ g \mid (g, em, M) \in gList \}$,

$LG = \{ g \mid {}^{\exists}Gr = (g,e,\{e\},p,k) \quad e \in (mList - TE) \}$,

$TE = \{ e \mid {}^{\exists}W \in TM \quad e \in W \}$,

$TM = \{ M \mid {}^{\exists}g \in TG \quad (g, em, M) \in gList \}$.

ステップ４：

em0 は，*tgList*（$= \{g1, \ldots, gk\}$）に含まれるCGのうちの一つ（*g1*）の管理エンティティ（*em1*）に対して結合を要求する（*conjInd*）．

ステップ５：

要求されたエンティティ（レスポンダエンティティ）*em1* は非発火状態に遷移し，グループサーバへの登録を削除（*delIdReq, delIdResp*）し，*em0* に確認応答する（*conjConf*）．ただし，レスポンダエンティティが単独のエンティティからなるCGの管理エンティティである場合には，*em0* への確認応答のみ行う．

ステップ６：

em0 は確認応答を受け，*em1* に消滅を要求する（*termInd*）．

ステップ７：

em1 は*em0* からの消滅要求を受け，確認応答（*termConf*）後消滅する．ただし，レスポンダエンティティが単独のエンティティからなるCGの管理エンティティである場合には，確認応答のみ行う．

ステップ８：

*tgList*に含まれる残りのCG（$g2, \ldots, gk$）について，ステップ４からステップ７を行う．

ステップ９：

em0 は，結合相手の全てのエンティティの消滅を受け，非発火状態に遷移し新たなメンバとなるエンティティを含めてグループサーバに登録する．

ステップ１０：

新たなメンバとなるエンティティに対してセッション鍵の配布を行い発火状態に遷移する．□

なお，セッション鍵の配布の手順については別に定めるものとする．

4．まとめ

本稿では，グループ通信に関して，特定のグループ管理装置に処理が集中しないような，各通信グループによる自律的なグループの管理手法について考察した．

今後は，グループのセキュリティレベルを考慮した動作定義などについて検討する予定である．

参考文献

[1] M. Park, et al, "Proposal of a Key Sharing Method for Secure Communication Systems," TJCOM98, p113-118(1998).

[2] 岡崎　他, "通信グループの分散管理手法の検討," 情処DICOMO99 シンポジウム(1999).