マルチメディア通信と分散処理　45－18
（１９９０．５．２５）

ハイアラキー構造に適した鍵管理方式

中村　秀紀，南部　峰秀，岡田謙一，松下　温
慶應義塾大学

暗号法は情報へのアクセス制御に用いることができる。これは、正しい鍵を持たないユーザは暗号化された情報を復号化できないからである。しかし、多くの人々と通信を行う場合に一人のユーザが多数の鍵を管理しなければならない。この論文では、暗号法によるアクセス制御の応用について述べる。我々は階層グループ構造という典型的な組織構造を想定し、ピースの組み合わせによる鍵の生成に基づく階層グループ指向型鍵管理方式（ＨＧＫ方式）を提案する。この方法は、階層グループ構造において鍵管理の面から非常に優れているということを示す。

A Hierarchical Group Oriented Key Management Method

Hidenori Nakamura, Mineki Nanbu
Ken-ichi Okada, Yutaka Matsushita
Keio University
3-14-1 Hiyoshi, Kohoku-ku, Yokohama 223, Japan

A cryptographic scheme can be used for controlling access to information, since any user who does not have a proper key can not decipher. But for this purpose, a user would have to manage a huge number of keys when he trys to communicate with a lot of people. The practical utilization method of access controll by cryptography is discussed in this paper. We suppose a typical organization structure called hierarchical group oriented structure. After that, we propose a hierarchical group oriented key management method (HGK method) based on the multiple keys generated from the combination of pieces, and describe that this method is very desirable in terms of reducing the numbers of keys required for each user in the hierarchical group oriented structure.

1．はじめに

暗号法は、安全性、真実性、データの完全性を守るための方法であるが、それに加えて情報へのアクセス制御にも利用される。組織の中においては数多くの通信のための構造が考えられるが、一般的にはそのうちの少数の構造のみがみられる。すなわち、階層構造とグループ構造、および、その両方の構造的特徴を兼ね備えたものがその典型である。我々は『ボス』と『スタッフ』からなる『チーム』という構造を定義し（図１．１）、このチームを単位とした階層により構成される、全体的な構造を『階層グループ構造』と定義する（図１．２）。

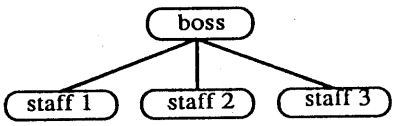

fig. 1.1　Team structure.

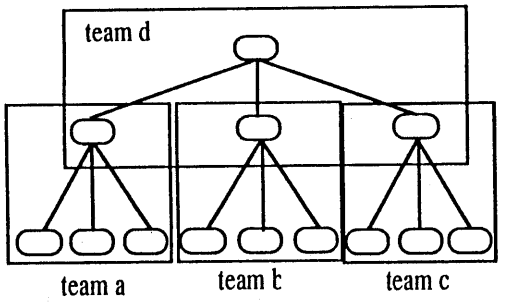

fig.1.2 A heap of team structure.

この構造において、３種類の通信形態すなわち、全同報通信、グループ通信、階層通信を想定する。『全同報通信』は、一回の通信においてシステム中の全てのメンバ間で行われる通信である。『グループ通信』は、一つのチーム内に限られる同報通信であり、『階層通信』は、異なるレベルの直系のメンバ間の同報通信である。従来のコピー鍵方式のような方法を用いて上述の全ての通信を行おうとすると、階層中の上層のメンバーは、莫大な数の鍵を管理しなければならない[3]。そこで我々は階層構造に適した階層グループ鍵管理方式（ＨＧＫ方式）を提案する。

ＨＧＫ方式では、『共通鍵』といくつかの『ピース』と呼ばれる鍵変更子の組み合わせから、多重鍵を生成する方法を採用した[7][8]。ピースの組み合わせの数は、ピース自身の数よりはるかに大きいので、少数のピースから多数の鍵を生成することができる。さらにこの方式において、ピースの数を最小にするために組織の構造に適したピースの配布法を提案する。最後に、通信効率、鍵の安全性、鍵更新の方法の面からコピー鍵方式と比較し、ＨＧＫ方式が有効的な方法であることを示す。

2．階層グループ構造モデル

組織において通信を行う場合には、二つの典型的な構造が存在する。一つは階層構造であり、もう一つはグループ構造である。この章で、これらの構造について述べ、さらにこの二つの構造の特徴を兼ね備えた階層グループ構造モデルを定義する。

（１）階層構造[4][5][7]

政府や軍隊、会社などの組織において、各自が自分より下のレベルのスタッフを管理するという階層構造がみられる。この構造においては、自分宛でなくとも仕事上での自分のスタッフの通信を読める事が望ましい場合が起こり得る。我々はこの通信形態を『階層通信』と呼ぶ。

（２）グループ構造[1][8]

組織においては、例えばプロジェクトチームやＵＮＩＸユーザグループやテニスクラブのような沢山のグループが存在する。このような場合、グループ内の全てのメンバ間での同報通信が必要とされる。我々はこの通信形態を『グループ通信』と呼ぶ。

（3）階層グループ構造

組織においては、上述の二つの構造の融合した形態がよくみられる。我々は『ボス』と『スタッフ』からなる『チーム』という構造を定義し（図1．1）、このチームを単位とした階層により構成される、全体的な構造を『階層グループ構造』と定義する(図1．2)。それぞれのメンバは、ボスとスタッフを持つので、最上層と最下層を除く全てのメンバは、ボスとしてまた、スタッフとして二つのチームに属することになる。

メンバAから見た全体の構造を図2．1に示す。『下層メンバ』はAの下の部分木の全ての端点の集合であり、『上層メンバ』はAから順次上にたどれる直系の端点の集合である。『ボス』はAのすぐ上の端点であり、また上述の3種類以外の他のメンバは、『その他のメンバ』となる。

このような構造において3通りの通信形態、『全同報通信』、『グループ通信』、『階層通信』を想定する。階層通信においては、ボスは他のスタッフにその通信内容を見られることなしに、自分のスタッフと通信できる。

3．HGK方式

HGK方式において、メンバは暗号化や復号化に用いる鍵をそのままの形で保持するのではなく、鍵の代わりに『共通キー』とその変更子である『ピース』を保持する。メンバは通信に必要な鍵を、共通キーとピースから生成する。

3．1　鍵生成法[7][8]

HGK方式において平文を暗号化するための通信鍵K'は共通鍵Kとピースpによって以下のように生成される。

$$K' = f(K, P) \qquad (1)$$

ここでfは適当な暗号化関数である。PとK.の独自な組から、独自なK'を生成するためには、fはK空間からK'空間への1対1対応である必要がある。もしも、通信鍵を生成するために、複数個のピース $\{P_1, P_2, \ldots, P_i\}$ が用いられるのであれば、K'は以下のようにして生成される。

$$K' = f(\ldots f(f(K, P_1) P_2), \ldots, P_i) \qquad (2)$$

ここで，ピースPiは通し番号の昇順で代入される。もしもfが1対1対応であれば独自なピースの組み合わせによって独自な鍵が生成される。

3．2　ピース分配法[7]

まず始めに、我々は2章で述べたチーム内の階層通信だけを想定する。r個のピースから一度にi個のピースを選ぶときの組み合わせは、iが偶数のときはr=i/2のとき、またiが奇数のときはr=(i-1)/2のときに最大となり、この数をR（i）と定義する。

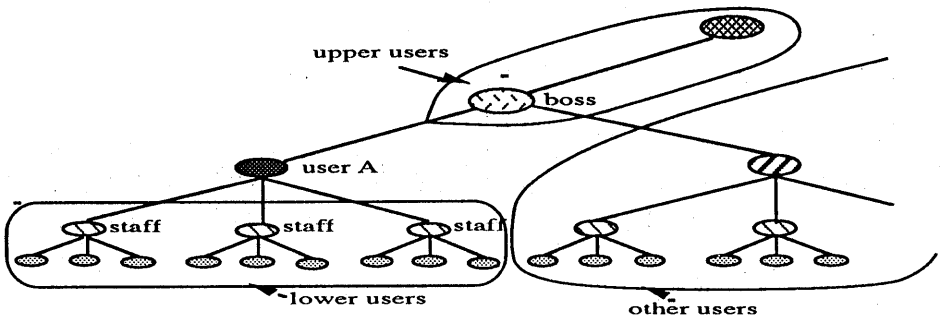

fig.2.1　Hierarchical group structure.

$$R(i) = {}_{i}C_{i/2} \quad \text{for } i=\text{even}$$
$$= {}_{i}C_{(i-1)/2} \quad \text{for } i=\text{odd} \quad (3)$$

この式はR（i）と同じ個数の鍵が、i個のピースから生成されることを意味する。

チーム内の各スタッフは、ボスとの通信用に独自なピースの組み合わせを保持するため、ボスとの秘密通信が可能となる。そして、ボスは自分のスタッフ全員のピースを保持することにより、部下全員との秘密通信が可能となる。スタッフの数がR（i－1）より大きく、R（i）以下の場合には、i個のピースを用いることによりボスの保持するピースの数を最小にすることが可能である。その場合、ボスはi個のピースを保持し、各スタッフは、iが偶数時にはi/2個、奇数時には(i-1)/2個のピースを保持することになる。

この方法を拡張することにより木構造全体に対して必要となるピースの数を決定することができる。ここで、nレベルのスタッフと、n＋1レベルのボスを含むチームを『レベルnチーム』と定義すると、式（3）よりレベルnチームのピース『レベルnピース』の数を決定することができる。これらのピースは下層メンバから上層メンバへと継承される。

多くの場合、メンバは直接に自分の下層メンバ全てを管理することは少ないので、下層メンバ全員のピースを保持することが必要だとは限らない。実際の管理形態においては、継承を1か2のレベルに制限しても十分実用的であると考えられる。我々はこのようなレベルを『継承レベル』と呼ぶ。継承レベルは管理形態により、それぞれのメンバに独立に設定する事が可能である。

階層通信のためのピース『階層ピース』に加え、それぞれのメンバは自分のチーム内でのグループ通信に用いる『グループピース』を保持する。レベルnチームにおいて、各スタッフはボスの持つレベルn＋1ピースを継承し、それをグループピースとして使用する。

加えて、全同報のための共通キーKが全てのメンバーに分配される。最終的にそれぞれのメンバーのピースは図3に示すように決定される。この例では継承レベルは1になっている。

3．3　通信方法[7][8]

通信文は、通信に必要とされるピースから生成された通信鍵を用いて暗号化される。そのときに使用したピースの通し番号は共通キーKによって暗号化され、ヘッダとして通信文の先頭に付加され、電文となる。各メンバはヘッダを復合化し、ピース番号を知ることにより通信文

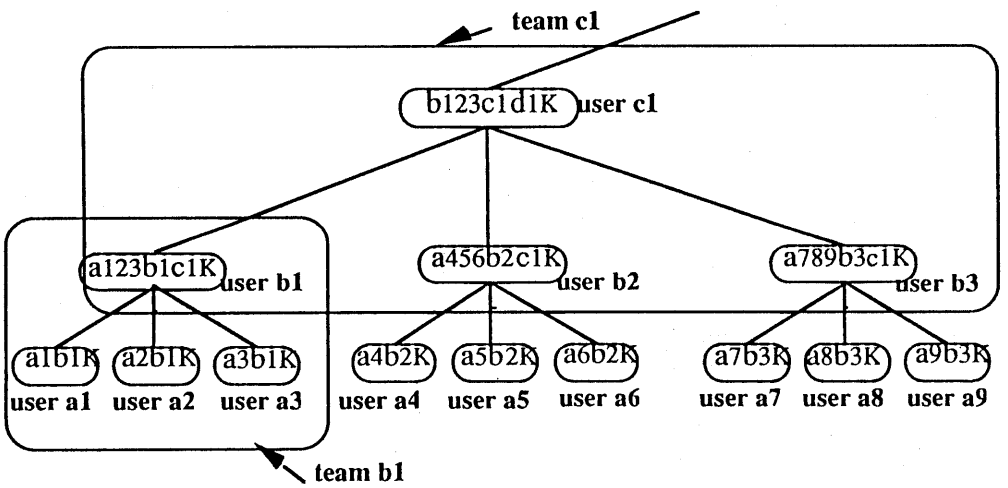

fig.3　Piece distribution.

が復合化可能であるかどうかを判定する。

（１）全同報通信

全同報通信では、通信文はシステム中の全てのメンバが持つ共通キーＫによって暗号化される。

（２）グループ通信

グループ通信では、通信文はそのチーム内で共有されるグループピースと共通鍵Ｋによって生成される通信鍵によって暗号化される。この場合、チーム内のメンバとボスの上位メンバだけが通信文を復号化することが可能である。例えば図３のチームｂ１ではグループピースｂ１と共通鍵Ｋからグループ通信用の通信鍵が生成される。

（３）階層通信

レベルｎメンバとその上位メンバ間の階層通信では、レベルｎメンバによって保持されるレベルｎピースとレベルｎ＋１ピース、そして共通キーＫが鍵生成のために用いられる。継承レベルがｍである場合には、レベルがｎ＋ｍ＋１以下の上位メンバのみが通信文を復号化できることになる。例を挙げると、図３におけるメンバｂ１とｃ１の通信にはｂ１、ｃ１、Ｋが用いられる。

４．鍵の安全性

本論文ではＤＥＳのような慣用暗号方式を、暗号化や復号化のために想定しており、ここでは暗号方式自体の安全性は考慮しないこととする[2]。また、表記Kij...nは複数個のピースPi,Pj,...,Pnと共通キーＫから生成される通信鍵を表す。

４．１　不正なメンバからの攻撃

ピースは暗号化に直接に使用されないので、不正なメンバがピースを手に入れることは困難である。そこで、不正なユーザが複数の鍵を手に入れた場合の他の鍵の安全性が問題となる。式(2)のｆは一方向関数であるので、K1もK2もK12から生成することは不可能である。よって一つの鍵が露見しても他の鍵の安全は保たれる[6]。

不正なメンバーが二つ以上の鍵を手にいれた場合、鍵生成に用いられたピースの通し番号からピースを手に入れることが可能である。例えばK1とK12が露見した場合、K1を平文とみなしてK12を暗号文とみなす既知平文攻撃によって、P2を手に入れることができる。しかし、この攻撃方法は全探索を必要とし、しかもピースの通し番号は共通鍵Ｋによって暗号化されているため容易に入手できない。従って二つ以上の鍵が露見した場合でも、他の鍵は安全である。

一方、共通鍵は頻繁に直接暗号化のために使われるので、システムの安全性を高めるためには定期的に取り替える必要がある。

４．２　正規メンバの攻撃

正規メンバが自分自身のピースと通し番号を知っている場合には、ある鍵から他のピースを手に入れることが可能である。例えばP1とP2を持つ正規メンバがK123を手にいれたとき、既知平文攻撃によってP3を手に入れることが可能である。しかし、それには前述したように全探索が必要となるので、暗号文は正規メンバの攻撃に対しても安全に保たれる。また下位メンバが共謀して自分達の全てのピースを集めたとしても、上位メンバ間の通信を復号化することは不可能である。なぜならばレベルｎメンバが上層メンバ宛ての通信文を暗号化するときには、下位レベルのメンバが保持しないレベルｎ＋１ピースを使用するからである。さらに、全てのピースを所有者にも不可視にすることによって鍵の安全性はより強化される。

５．評価

５．１　鍵数

ピースのサイズは鍵のサイズと同様であるため、ピースの数を鍵の数とみなすことが可能である。ここでは、各端点がs個のノードを持つ完全s本木構造において全通信に必要なピースの数を従来方式と比較してみる。sがR（n－1）より大きく、R（n）以下であるならば、それぞれのグループにおいてn個のピースが必要とされる。継承レベルが制限されないならば、それぞれのメンバは、自分の下層メンバが持つ全てのピースを保持するので、レベルiメンバが持つピースの数AP（i）は次式で示される。

$$AP(1) = n + 1$$

$$AP(i) = \sum_{k=1}^{i-1} (nk + n + 1) \qquad (i > 1) \qquad (4)$$

一方、コピー鍵方式を用いた場合には、階層通信に必要な鍵の数HK（i）は次式のようになる。

$$HK(i) = (s^i - s)/(s - 1) + 1 \qquad (5)$$

また、グループ通信に必要な鍵の総数GK（i）は次式のようになる。

$$GK(i) = (s^{i-1} - s)/(s - 1) + 1 \qquad (6)$$

HK（i）、GK（i）に加えて、全同報用の共通キーが必要となるので、レベルiメンバーが最終的に必要とする鍵の総数AK（i）は次式で示される。

$$AK(i) = HK(i) + GK(i) + 1$$
$$= (s^i + s^{i-1} - 2s)/(s - 1) + 3 \qquad (7)$$

例えば、完全10本木5層構造を考える場合、式（4），（7）は各々次のように計算される。

$$AP(i) = (5^i - 5)/4 + 6 \qquad (4)'$$
$$AK(i) = (10^i + 10^{i-1} - 20)/9 + 3 \qquad (7)'$$

上で示したように、iが1以外のときAP（i）はAK（i）よりも小さく、iまたはsを大きくするとこの傾向はさらに顕著になる。例えばiが5であると、AP（5）は786で、AK（5）は12223となりAP（5）のほぼ16倍になる。

しかし、786個のピースは一人のメンバが持つには多すぎるので、適切な個数にするために継承レベルを設定する。継承レベルがmであるとき式（4）、（5）は次のように書き換えられる。

$$AP = (n^m - n)/(n - 1) + n + 1 \qquad (8)$$
$$AK = (s^m + s^{m-1} - 2s)/(s - 1) + 3 \qquad (9)$$

これらの等式はiには無関係である。継承レベルが2であり、他の状態を変えないときにはAPは36で、AKは123になりAPの約3．4倍になる。

5．2　鍵の更新

システムを安全に保つために、鍵の更新が不可欠である。コピー鍵方式においては全ての鍵が更新されるが、全ての鍵の再分配には非常に手間がかかる。一方HGK方式においては、鍵の更新に二通りの方法が用意されている。一つは共通キーKだけを更新する方法である。共通キーKは全ての鍵生成に関わっているので、この方法を用いることによってシステム外部の人間に対して鍵を安全に保つことができ、しかも容易に実現できるために頻繁に実行することができる。ただしシステム内の人間に対しては効果がなく、共通鍵が盗まれても当然効果がなくなる。もう一つの方法は全てのピースを更新してしまう方法で、これによりシステムの外の人間及びシステム内の不正メンバに対して鍵を安全に保つことが可能である。この方法は共通鍵Kだけを更新する方法に比べると実現に手間がかかるために、より長期的な周期で実行するのが有効と思われる。このようにHGK方式においては必要に応じて両者の方法を使い分けることができるということが大きなメリットとなる。

5．3　ピースの再分配

レベルnチームに新しいメンバをスタッフとして登録する場合を想定する。チームに登録されているメンバの数が、チーム内のレベルnピースから生成される組み合わせの数の最大値よりも小さい場合には、このチームに新しいメンバをスタッフとして加えることは簡単で、ピースの再分配を必要としない。

図5(a)で示す例では、チーム内のピースの数が4で4人のスタッフが存在し、2人のメンバーをピースを再分配することなく登録することができる。新しいメンバには、まだ使われていないピースの組み合わせが分配される。

新しいメンバを登録する場所がない場合には、チーム内のピース数を変化させて再分配する必要が生じる。このとき図5(c)に示すように、ピースの数が偶数であれば1個の新しいピースをボスのみに配送し、新しいピースを含む新しい組み合わせの内の1個が新しいメンバに分配される。もしもピースの数が図5(d)に示されるように奇数であれば、1個の新しいピースをそれぞれのメンバに分配され、新しいピースの組み合わせが新しいメンバに分配される。

5．3　通信効率

（1）暗号文の長さ

コピー鍵方式とHGK方式において、平文を暗号化するためには同じアルゴリズムが用いられるため、暗号文の長さは平文の長さと等しい。

（2）計算回数

コピー鍵方式とHGK方式の両方式において、平文を暗号化、復号化するためには同じ計算ステップを必要とするが、HGK方式はピースから鍵を生成するために余分なステップを必要とする。このステップは3章1節に記述した関数fに依存するが、鍵生成に用いられるピースのサイズは、通常通信文のサイズよりも十分に小さいので、適切な関数を用いることによって、この余分なステップ数が全体のステップ数にほとんど影響を与えないようにすることが可能である。

6．結論

本論文で、我々は階層グループ通信のための

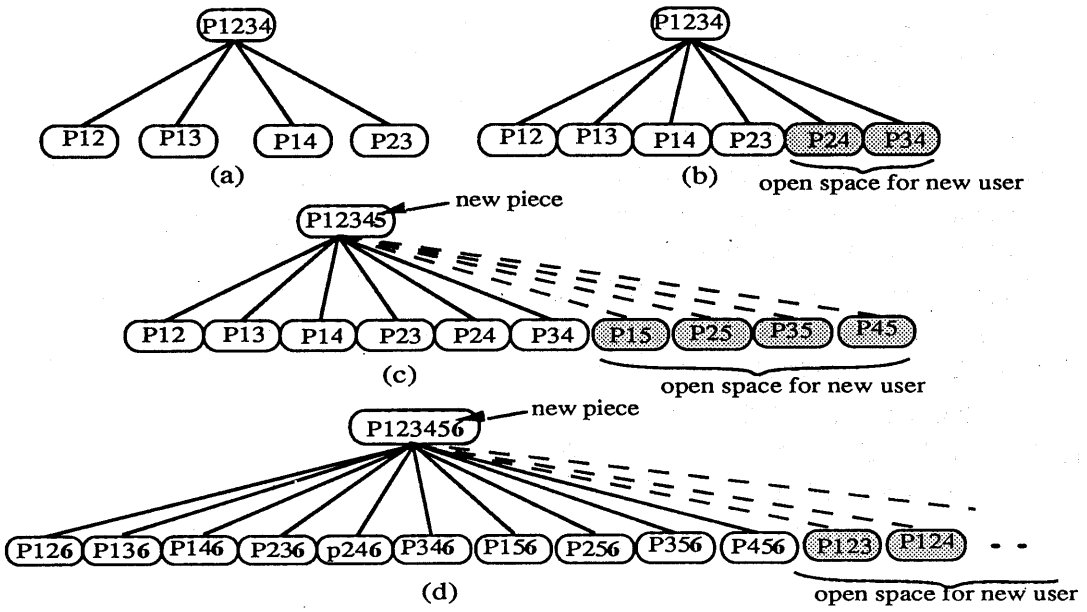

fig.5　Entry of the new user.

ＨＧＫ方式を提案した。この方式を用いることにより、現実に広く存在するような通信形態に即したアクセスコントロールが実現でき、各ユーザが管理しなければならない鍵の数を減らすことが可能である。この効果は、ユーザの数が多い状態や、継承レベルが高い状態になるほど著しくなる。また、通信効率や鍵の安全性に関しても従来方式より有利であり、総合的にみてもＨＧＫ方式は非常に優れていると言える。

参考文献

[1] Desmedt,Y.,"SOCIETY AND GROUP ORIENTED CRYPTOGRAPHY: A NEW CONCEPT", Lect Notes Comput Sci,293, pp120-127,1988.

[2] "Data Encryption Standard",FIPS PUB 46, National Bureau of Standards, Washington,D.C.,1977.

[3]太田和夫、"効率の良い同報暗号通信" 信学技法、Vol.87,No.12 pp.43-48,1987

[4] Akl,S.G.and Taylor,P.D.,"Cryptographic Solution to a Problem of Access Control in a Hierarchy", ACM Trans.Comput.Syst.,Vol.1, No.3, pp.239-248,Aug,1983.

[5] Mackinnon,S.J.,Taylor,P.D.,Meijer.H.and Akl, S.G.,"An Optimal Algolithm for Assigning Cryptographic Keys to Control Access in a Hierarchy",IEEE Trans.Comput., Vol.C-34,No9, pp.797-802,Sept,1985.

[6] Shamer,A.,"How to Share a Secret",Commun. ACM,Vol.22,NO.11, pp.612-613,Nov,1979.

[7]関口絵美子他、"階層構造における鍵管理法" 情報処理学会第４０回全国大会

[8]高木和幸他、"新しいグループ指向鍵管理方式" 情報処理学会第４０回全国大会