論　文

一般的なアクセス構造を実現する秘密共有法

非会員　伊藤　充[†]　非会員　斎藤　明[†]　正員　西関　隆夫[†]

Secret Sharing Scheme Realizing General Access Structure

Mitsuru ITO[†], Akira SAITO[†], *Nonmembers and* Takao NISHIZEKI[†], *Member*

あらまし　暗号鍵などの秘密を共有する方法としてShamirの(k, n)しきい値法がよく知られている．しかしこの方法では特殊なアクセス構造しか実現できない．本論文では(k, n)しきい値法の分散情報を各管理人に複数個与えれば任意のアクセス構造が実現できることを示す．また秘密管理人に変更があった場合の更新のしかた，およびしきい値グラフとの関連について考察する．

1. まえがき

データ通信の発展に伴い，電子為替システムや電子郵便など重要な通信が一般通信路を流れるようになっている．このため，通信情報に対する盗聴，改ざんを防止する手段として機密保護と認証性を保証する暗号が広く用いられつつある．実際に暗号を利用する場合にはDES, FEALに代表される慣用暗号はもちろん，公開鍵暗号においても復号鍵は秘密管理されなければならない．このため，秘密共有管理法が重要な問題の一つになっている[2]．

近年，Shamirは(k, n)しきい値法という興味深い秘密共有管理法を提案している[5]．これは秘密情報をn個に分割し，n人で分散保管する方法である．分散情報のうちk個以上が集れば秘密が復元され，k個未満の情報からは秘密に関する情報は全く得られない．このkをしきい値と呼ぶ．(k, n)しきい値法は同一グループ内の構成員に対する平等な秘密共有法である．これに対し，小山は対等あるいは上下関係にある複数グループ間の秘密共有法を(k, n)しきい値法を利用して構成することを試みている[3]．しかし，実際には秘密へのアクセスには特定の人々の許可が必要な場合，あるいは特定の管理人の組合わせに対しては秘密へのアクセスを認めたくないという場合もある．従ってより一般的なアクセス構造を有する秘密共有法を構築することが望まれる．上原，西関，岡本，中村はマトロイド理論を用いてこの問題の解決を試み，極小アクセス構造が線形表現可能なマトロイドの構造を持つならば，そのアクセス構造を有する秘密共有法が構成できることを示した[6]．

本論文では(k, n)しきい値法の分散情報を各構成員に複数個割り当てる複数割り当て法を提案し，この方法を用いればいかなるアクセス構造も理論的には実現可能であることを示す．

以下の章の内容は次の通りである．まず，2.では任意のアクセス構造がこの手法で実現できることを示す．3.ではアクセス構造が少し変更されたとき，管理人に与える分散情報をどう変更したらよいかについて述べる．4.では各分散情報が一人の管理人にだけ割り当てられる場合について，しきい値グラフとの関係について述べる．

2. 複数割り当て法

まず(k, n)しきい値法の概要を述べ，かつ本文において使われる用語の説明を行う．(k, n)しきい値法は秘密共有法の一種であり秘密情報Dをn個の分散情報$w_1, \cdots, w_n$に分割符号化して保管または伝送する方法で，以下のような秘密保護特性を持つ．すなわち$\{w_1, \cdots, w_n\}$のうちk個以上の任意の分散情報によりDは復元され，$k-1$個以下のどの分散情報からもDに関する情報は全く得られない．(k, n)しきい値法では$k-1$個以下の分散情報が盗まれても秘密は安全であり，$n-k$個以下の分散情報が破壊されても秘密の復元は可能である．

Shamirは多項式補間法を用いて(k, n)しきい値法を実現する次のような方法を与えた．

Shamirの(k, n)しきい値法

† 東北大学工学部通信工学科，仙台市
Faculty of Engineering, Tohoku University, Sendai-shi, 980 Japan

管理人の集合を $P=\{p_1, \cdots, p_n\}$ とする．かつ，秘密 D は非負整数であるとする．また $1 \leqq k \leqq n$ とする．

（1） $q>\max\{n, D\}$ なる素数幅 q を選び，$K=\mathrm{GF}(q)$ とする．以後のすべての演算は有限体 K 上で考える．$K-\{0\}$ から相異なる n 個の要素 $x_1, \cdots, x_n$ を選ぶ．

（2） $a_1, \cdots, a_{k-2} \in K$, $a_{k-1} \in K-\{0\}$ をランダムに選ぶ．

（3） 多項式 $f(x)=D+a_1x+a_2x^2+\cdots+a_{k-1}x^{k-1}$ を定める．

（4） $w_i=f(x_i)$ とし，各人 p_i に分割情報 (x_i, w_i) を与える．

f は $k-1$ 次の多項式なので，P の位数 k 以上の部分集合，すなわち k 人以上の管理人が集れば，それらの持つ w_i を用いて f を復元することができ，従って D を復元できる．しかし，P の位数 $k-1$ 以下の部分集合からは f の定数項 D に関する情報は何も得られない．

ここでは秘密共有管理システムを単にシステムと書くことにする．P をそのシステムにおける管理人の集合とする．一つのシステムを定めると P の部分集合は秘密 D を復元できるものと，復元できないものの二つに類別される．秘密 D を復元できる P の部分集合をアクセス集合と呼ぶ．すべてのアクセス集合から成る族 $\mathcal{A} \subset 2^P$ をそのシステムのアクセス構造と呼ぶ．秘密 D を復元できない P の部分集合を非アクセス集合と呼び，すべての非アクセス集合から成る族をそのシステムの非アクセス構造 $\mathcal{B} \subset 2^P$ と呼ぶ．いま，$\mathcal{A} \cup \mathcal{B}=2^P$, $\mathcal{A} \cap \mathcal{B}=\phi$ である．

P の部分集合の族 $\mathcal{F} \subset 2^P$ が与えられたとき，その極大元のなす族を $\mathcal{F}^+$ と表すことにする．すなわち $\mathcal{F}^+=\{F \in \mathcal{F} : F' \neq F$ なる任意の $F' \in \mathcal{F}$ に対して，$F \not\subseteq F'\}$

また F の極小元のなす族を $\mathcal{F}^-$ で表すことにする．

$\mathcal{F}^-=\{F \in \mathcal{F} : F' \neq F$ なる任意の $F' \in \mathcal{F}$ に対して，$F' \not\subseteq F\}$

$\mathcal{A}$ があるシステムのアクセス構造であるとき，$\mathcal{A}^-$ を極小アクセス構造と呼ぶ．$\mathcal{B}$ があるシステムの非アクセス構造であるとき，$\mathcal{B}^+$ を極大非アクセス構造と呼ぶ．任意の $\mathcal{A} \subset 2^P$ が与えられたとき，それをアクセス構造として持つシステムが存在するわけではない．$\mathcal{A} \subset 2^P$ があるシステムのアクセス構造ならば，$\mathcal{A}$ は次の自明な条件（a）を満足しなければならない．

条件（a）

$A \in \mathcal{A}$ かつ $A \subset A'$ ならば $A' \in \mathcal{A}$

条件（a）よりアクセス構造はその極小アクセス構造のみから完全に記述されることがわかる．本章では，与えられた $\mathcal{A}$ が上の条件（a）を満たす限り，$\mathcal{A}$ をアクセス構造として持つシステムが必ず構成できることを示す．ここで提案する構成方法は (k, n) しきい値法の分散情報を各管理人に複数個割り当てる方法である．以下にその方法を述べる．

複数割り当て法

（1） $0<k \leqq l$ なる k, l を適当に選ぶ．$q>\max\{l, D\}$ なる素数幅をとり，$K=\mathrm{GF}(q)$ とする．相異なる $x_1, \cdots, x_l \in K-\{0\}$ を選ぶ．

（2） $a_1, \cdots, a_{k-2} \in K$, $a_{k-1} \in K-\{0\}$ をランダムに選ぶ．

（3） 多項式 $f(x)=D+a_1x+a_2x^2+\cdots+a_{k-1}x^{k-1}$ を定める．$S=\{w_1, \cdots, w_l\}$, $w_i=f(x_i)$ とし，n 個の部分集合 $s_1, \cdots, s_n \subset S$ を選ぶ．

（4） 各管理人 p_i に分散情報の部分集合 s_i を与える．

Shamir の (k, n) しきい値法は上の複数割り当て法の特別な場合である．すなわち，$l=n$ で，各集合 s_i の位数が1の場合に相当する．

上記の複数割り当て法の（3）における各管理人 p_i への s_i の割り当ては $g(p_i)=s_i$ なる関数 $g : P \to 2^S$ と考えられる．上のシステムのアクセス構造 $\mathcal{A}_g$ および非アクセス構造 $\mathcal{B}_g$ は次のように記述される．

$$\mathcal{A}_g=\{Q \subset P : |\bigcup_{p \in Q} g(p)| \geqq k\}$$

$$\mathcal{A}_g=\{Q \subset P : |\bigcup_{p \in Q} g(p)| \leqq k-1\}$$

$$=2^P-\mathcal{A}_g$$

上の自明な条件（a）を満足する $\mathcal{A} \subset 2^P$ が与えられたとき，g と S を適当に選ぶことにより $\mathcal{A}_g=\mathcal{A}$ なる複数割り当て法が実現できることを次の定理で示す．

［定理1］ $\mathcal{A} \subset 2^K$ をアクセス構造として持つ複数割り当てシステムが存在するための必要十分条件は $\mathcal{A}$ が条件（a）を満足することである．

（証明） 必要性は明らかであるので十分性を示そう．$\mathcal{A}$ は条件（a）を満足するとし，$\mathcal{B}=2^P-\mathcal{A}$ とする．$\mathcal{B}$ は次の性質を満足する．

条件（b）

$B \in \mathcal{B}$ かつ $B' \subset B$ ならば $B' \in \mathcal{B}$.

$|\mathcal{B}^+|=l$ として，$\mathcal{B}^+=\{B_1, B_2, \cdots, B_l\}$ とおく．$\mathcal{B}^+$ に対応して $S=\{w_1, w_2, \cdots, w_l\}$ を作る．但し S は (l, l) しきい値法により作られる分散情報の集合とする．よって，$w_1, w_2, \cdots, w_l$ が全部得られたとき秘密 D を再生

でき，一つでも得られないものがあれば D は全く再生できない．

管理人 $p_1, p_2, \cdots, p_n$ に対して，割り当て $g(p_j)$ を

$$g(p_j)=\{w_i : p_j \notin B_i \in \mathcal{B}^+\} \quad (j=1, 2, \cdots, n)$$

とする．このとき $\mathcal{A}_g=\mathcal{A}$ が成り立つこと，すなわち，

$Q\in\mathcal{A}$ ならば $\bigcup_{p\in Q} g(p)=S$ (1)

$Q\in\mathcal{B}$ ならば $\bigcup_{p\in Q} g(p)\subsetneqq S$ (2)

が成立することを示そう．

まず(1)を証明する．$Q\in\mathcal{A}$ にもかかわらず，$\bigcup_{p\in Q} g(p)\subsetneqq S$ と仮定する．このとき $w_t\in S-\bigcup_{p\in Q} g(p)$ なる $w_t\in S$ が存在する．このとき任意の $p\in Q$ に対し $p\in B_t\in\mathcal{B}^+$ である．つまり，$Q\subseteqq B_t$ である．$\mathcal{B}$ の前述の性質(b)より，$Q\in\mathcal{B}$ である．しかし，このとき $Q\in\mathcal{A}\cap\mathcal{B}$ となり，矛盾である．

次に(2)を証明する．$Q\in\mathcal{B}$ とする．このとき $Q\subseteqq B_t\in\mathcal{B}^+$ なる B_t が存在する．任意の $p\in Q$ について $p\in B_t$ であり，$w_t\notin g(p)$ である．従って，$w_t\notin\bigcup_{p\in Q} g(p)$ であり，$\bigcup_{p\in Q} g(p)\subsetneqq S$ である． (証明終)

例を一つ示そう．

[例1] P および $\mathcal{A}^-$ を

$P=\{p_1, p_2, p_3, p_4\}$

$\mathcal{A}^-=\{\{p_1, p_2, p_3\},\ \{p_1, p_4\}, \{p_2, p_4\}, \{p_3, p_4\}\}$

とする．このとき $\mathcal{B}^+$ は

$\mathcal{B}^+=\{\{p_1, p_2\},\ \{p_2, p_3\}, \{p_1, p_3\},\ \{p_4\}\}$

である．この $\mathcal{B}^+$ に対応して $S=\{w_1, w_2, w_3, w_4\}$ を(4, 4) しきい値法により作る．割り当ては

$g(p_1)=\{w_2, w_4\}$

$g(p_2)=\{w_3, w_4\}$

$g(p_3)=\{w_1, w_4\}$

$g(p_4)=\{w_1, w_2, w_3\}$

となる． (例終)

今までは実現したいアクセス構造 $\mathcal{A}$ が完全に与えられるとしていた．しかし，秘密共有法を実際に設計するとき，アクセス構造 $\mathcal{A}$ が完全に記述されないことがあろう．特に $|P|=n$ が大きいときに，$\mathcal{A}$ または $\mathcal{A}^-$ の要素全部が列挙されるとするのは現実的ではない．より現実的な状況として，次のような問題が考えられる．すなわち，$\mathcal{A}^*, \mathcal{B}^*\subseteqq 2^P$ が与えられたときに，$\mathcal{A}^*\subseteqq\mathcal{A}, \mathcal{B}^*\subseteqq 2^P-\mathcal{A}$ となるアクセス構造 $\mathcal{A}$ を持つ複数割り当てシステムを構成せよという問題である．この問題に関し，次の定理が成り立つ．

[定理2] $\mathcal{A}^*, \mathcal{B}^*\subseteqq 2^P$ が与えられるとする．$\mathcal{A}^*\subseteqq\mathcal{A}$, $\mathcal{B}^*\subseteqq 2^P-\mathcal{A}$ なるアクセス構造 $\mathcal{A}$ を持つ複数割り当てシステムが存在するための必要十分条件は，次の条件(c)が満足されることである．

条件(c)：任意の $A\in\mathcal{A}^*, B\in\mathcal{B}^*$ に対して $A\nsubseteqq B$ である．

(証明) 必要性：$\mathcal{A}^*\subseteqq A$ かつ $\mathcal{B}^*\subseteqq 2^P-\mathcal{A}$ なるアクセス構造 $\mathcal{A}$ を持つシステムがあるにもかかわらず，条件(c)が満足されていないとする．このときある $\mathcal{A}\in\mathcal{A}^*$ と $B\in\mathcal{B}^*$ に対し，$A\subseteqq B$ である．$A\in\mathcal{A}^*\subset\mathcal{A}$ より $B\in\mathcal{A}$，よって $\mathcal{A}\cap\mathcal{B}^*\neq\phi$ となり仮定に矛盾する．

十分性：与えられた $\mathcal{A}^*, \mathcal{B}^*\subseteqq 2^P$ が条件(c)を満足しているとする．$\mathcal{A}'$ を次のように定義する．

$\mathcal{A}'=\{A'\subset P : A\subseteqq A'$ なる $A\in\mathcal{A}^*$ が存在する$\}$

この $\mathcal{A}'$ は条件(a)を満足するので，定理1より $\mathcal{A}'$ はある複数割り当てシステムのアクセス構造である．$\mathcal{A}^*\subseteqq\mathcal{A}'$ かつ $\mathcal{B}^*\subseteqq 2^P-\mathcal{A}'$ であることを示そう．$\mathcal{A}^*\subseteqq\mathcal{A}'$ は $\mathcal{A}'$ の定義より明らかである．$\mathcal{B}^*\nsubseteqq 2^P-\mathcal{A}'$ であると仮定すると，$Q\in\mathcal{A}'\cap\mathcal{B}^*$ なる Q が存在する．$Q\in\mathcal{A}'$ より $A\subseteqq Q$ なる $A\in\mathcal{A}^*$ が存在する．しかし $Q\in\mathcal{B}^*$ なのでこれは条件(c)に矛盾する．

(証明終)

3. 複数割り当てシステムの更新

複数割り当て法には管理人が保管する分散情報の量ざ増えるという欠点がある．しかし，本章で述べるように，管理人が増加した場合には特殊な場合を除いて容易に更新ができるという特徴がある．

今まで n 人で管理していた情報 D に対し，新たに u 人の管理人を増やして $n+u$ 人で D を管理したい $(u\geqq 1)$．その $n+u$ 人にどのような分散情報の割り当てを行えばよいかを考察する．

まず，初期の管理人の集合を P_1 とし，その上のアクセス構造を $\mathcal{A}_1\subset 2^{P_1}$ とする．次に増加後の管理人の集合を P_2 とし，新たなアクセス構造を $\mathcal{A}_2\subset 2^{P_2}$ とする．また $\mathcal{A}_1, \mathcal{A}_2$ に対応する非アクセス構造を $\mathcal{B}_1, \mathcal{B}_2$ とする．すなわち

$\mathcal{B}_i=2^{P_i}-\mathcal{A}_i \quad (i=1, 2)$

である．ここで $\mathcal{A}_2$ と $\mathcal{B}_2$ はそれぞれ $\mathcal{A}_1$ と $\mathcal{B}_1$ の拡張である．すなわち次の条件(d)を満足すると仮定する．この仮定は妥当であろう．

条件(d)

$\mathcal{A}_1\subset\mathcal{A}_2$ かつ $\mathcal{B}_1\subset\mathcal{B}_2$

管理人が増加したとき定理1の（割り当て）関数 g が大幅に変化しないかという疑問が起こる．しかし，実はそのようなことは起こらず，割り当て関数は管理人の増加に対し自然に拡張される．まず，P_1 と P_2 を次のようにおく．

$P_1=\{p_1, p_2, \cdots, p_n\}$

$P_2=P_1\cup\{p_{n+1}, \cdots, p_{n+u}\}$

定理1と同様に，$\mathcal{B}_1$, $\mathcal{B}_2$ に対応して，$\mathcal{B}_1^+$, $\mathcal{B}_2^+$ を作る．このとき，次の定理が成り立つ．

［定理3］条件(d)が成立しているとする．$B_i\in\mathcal{B}_1^+$ ならば $B_i\cup Q\in\mathcal{B}_2^+$ かつ $Q\subseteq\{p_{n+1}, \cdots, p_{n+u}\}$ なる Q が存在する．

（証明）$B_i\in\mathcal{B}_1^+$ であるから，$B_i\in\mathcal{B}_1$ である．条件(d)により，$B_i\in\mathcal{B}_2$ である．よって $B_i\subseteq B_j\in\mathcal{B}_2^+$ なる B_j が存在する．$B_j-B_i=Q$ とおき，$Q\subseteq\{p_{n+1}, \cdots, p_{n+u}\}$ を証明する．$Q\not\subseteq\{p_{n+1}, \cdots, p_{n+u}\}$ であると仮定する．このとき $p_t\in Q$ なる $p_t(t\leqq n)$ が存在する．$B_i\cup\{p_t\}\subseteq B_j$ なので $B_i\cup\{p_t\}\in\mathcal{B}_2$ である．しかし $B_i\in\mathcal{B}_1^+$ であるから $B_i\cup\{p_t\}\in\mathcal{A}_1\subset\mathcal{A}_2$ である．よって $B_i\cup\{p_t\}\in\mathcal{A}_2\cap\mathcal{B}_2$ となり，$\mathcal{A}_2$, $\mathcal{B}_2$ の定義に矛盾する．従って $Q\subseteq\{p_{n+1}, \cdots, p_{n+u}\}$ である．　（証明終）

上の定理より，明らかに $|\mathcal{B}_1^+|=l_1\leqq l_2=|\mathcal{B}_2^+|$ である．すなわち，複数割り当て法で使われる分散情報の種類が減ることはない．また，定理3から，増加前の分散情報の割り当てについて，次の定理が成り立つ．

［定理4］管理人の集合を $P_1=\{p_1, p_2, \cdots, p_n\}$ とする．もし P_1 上のアクセス構造 $\mathcal{A}_1$ が定理1の証明の割り当て関数 g_1：$g_1(p_j)=\{w_i : p_j\in B_{1i}\in\mathcal{B}_1^+\}$ により実現されていたとする．但し $\mathcal{B}_1^+=\{B_{11}, \cdots, B_{1l_1}\}$, 分散情報の集合 $S_1=\{w_1, \cdots, w_{l_1}\}$ とする．もし条件(d)が成立していれば増加後の管理人の集合 $P_2=\{p_1, \cdots, p_n, p_{n+1}, \cdots, n_{n+u}\}$ 上のシステムの割り当て関数 g_2 および分散情報 S_2 が次の条件ⓐおよびⓑを満足するようにできる．

ⓐ$S_1\subset S_2$.

ⓑ任意の $p_j\in P_1$ について $g_1(p_j)\subset g_2(p_j)$

かつ $g_2(p_j)-g_1(p_j)\subset S_2-S_1$.

（証明）ⓐ定理3より $1\leqq i\leqq l_1$ なる各 $B_{1i}\in\mathcal{B}_1^+$ について，$B_{1i}\cup Q_i\in\mathcal{B}_2^+$ かつ $Q_i\subseteq\{p_{n+1}, \cdots, p_{n+u}\}$ なる Q_i が存在する．$|\mathcal{B}_2^+|=l_2$ とし，$\mathcal{B}_2^+=\{B_{2i} : 1\leqq i\leqq l_2\}$ とする．但し，$B_{2i}=B_{1i}\cup Q_i(1\leqq i\leqq l_1)$ とおく．($l_2\geqq l_1$ に注意せよ．) $B_{1i}\in\mathcal{B}_1^+$ に対応していた分散情報 w_i を，新しいシステムでは $B_{2i}\in\mathcal{B}_2^+$ に対応させ，定理1の証明にある方法で g_2 を構成する．すなわち $g_2(p_j)=\{w_i : p_j\in B_{2i}\}$, $w_i=f(x_i)(1\leqq i\leqq l_2)$, $S_2=\{w_1, w_2, \cdots, w_{l_2}\}$ とする．このとき明らかに $S_1\subset S_2$ である．

ⓑまず $g_1(p_j)\subset g_2(p_j)(1\leqq j\leqq n)$ を示そう．$w_i\in g_1(p_j)$ とすると，$p_j\in B_{1i}\in\mathcal{B}_1^+$ である．$1\leqq j\leqq n$ だから，$p_j\in Q_i$ である．よって，$p_j\in B_{2i}=B_{1i}\cup Q_i\in\mathcal{B}_2^+$ である．従って $w_i\in g_2(p_j)$ である．

次に $g_2(p_j)-g_1(p_j)\subset S_2-S_1$ を示そう．そのためには $w_i\in g_1(p_j)$ なる $w_i\in S_1$ は $w_i\in g_2(p_j)$ であることを示せばよい．$w_i\in g_1(p_j)$ なので，$p_j\in B_{1i}\in\mathcal{B}_1^+$ である．よって $p_j\in B_{2i}=B_{1i}\cup Q_i\in\mathcal{B}_2^+$ であり，$w_i\in g_2(p_j)$ である　（証明終）

［例2］P_1 および $\mathcal{A}_1^-$ を

$P_1=\{p_1, p_2, p_3, p_4\}$

$\mathcal{A}_1^-=\{\{p_1, p_2, p_3\}, \{p_1, p_4\}, \{p_2, p_4\}, \{p_3, p_4\}\}$

とする．このとき $\mathcal{B}_1^+$ は

$B_1^+=\{\{p_1, p_2\}, \{p_2, p_3\}, \{p_1, p_3\}, \{p_4\}\}$

である．この $\mathcal{B}_1^+$ に対応して $S=\{w_1, w_2, w_3, w_4\}$ を(4, 4) しきい値法より作る．割り当ては

$g_1(p_1)=\{w_2, w_4\}$

$g_1(p_2)=\{w_3, w_4\}$

$g_1(p_3)=\{w_1, w_4\}$

$g_1(p_4)=\{w_1, w_2, w_3\}$

となる．管理人が一人増え P_2 および $\mathcal{A}_2^-$ が

$P_2=\{p_1, p_2, p_3, p_4, p_5\}$

$\mathcal{A}_2^-=\{\{p_1, p_2, p_3\}, \{p_1, p_4\}, \{p_2, p_4\}, \{p_3, p_4\}, \{p_1, p_2, p_5\}, \{p_3, p_5\}\}$

となるとする．このとき $\mathcal{B}_2^+$ は

$\mathcal{B}_2^+=\{\{p_1, p_2\}, \{p_2, p_3\}, \{p_1, p_3\}, \{p_4, p_5\}, \{p_1, p_5\}, \{p_2, p_5\}\}$

である．この $\mathcal{B}_2^+$ に対応して $S=\{w_1, w_2, w_3, w_4, w_5, w_6\}$ を (6, 6) しきい値法より作る．割り当ては

$g_2(p_1)=\{w_2, w_4, w_6\}$

$g_2(p_2)=\{w_3, w_4, w_5\}$

$g_2(p_3)=\{w_1, w_4, w_5, w_6\}$

$g_2(p_4)=\{w_1, w_2, w_3, w_5, w_6\}$

$g_2(p_5)=\{w_1, w_2, w_3\}$

となる．　（例終）

定理4は複数割り当て法における割り当て関数が管理人の増加に対し容易に更新されることを示しているが，しかしここで注意しなければならないことがある．例2にも見られるように，一般には増加後必要とされる分散情報の数が増えるので S_1, S_2 の符号構成が変わる．すなわち，増加前の分散情報の集合 S_1 は (l_1, l_1) 符号の構造を持つが，増加後の分散情報の集合 S_2 は $(l_2,$

l_2) 符号の構造をもち，$l_1 \leqq l_2$ である．よって，もともとの分散情報の値そのものを変えずに (l_2, l_2) 符号を構成することが望まれる．これを達成するためには次のような方法が考えられる．

増加前の暗号共有多項式 f_1 を

$f_1(x)=D+a_{11}x+\cdots+a_{1l_1-1}x^{l_1-1}$

とする．増加後の暗号共有多項式 f_2 を

$f_2(x)=D+a_{21}x+\cdots+a_{2l_2-1}x^{l_2-1}$

とする．但し，各 $1 \leqq j \leqq l_1$ について $f_2(x_j)=f_1(x_j)$ であるように係数 $a_{21}, a_{22}, \cdots, a_{2l_2-2} \in K$, $a_{2l_2-1} \in K-\{0\}$ を選ぶ．つまり係数 $a_{21}, a_{22}, \cdots, a_{2l_2-1}$ が次の式を満足するように選ぶ．

$$\begin{pmatrix} x_1 & x_1^2 & \cdots & x_1^{l_2-1} \\ x_2 & x_2^2 & \cdots & x_2^{l_2-1} \\ \vdots & \vdots & \ddots & \vdots \\ x_{l_1} & x_{l_1}^2 & \cdots & x_{l_1}^{l_2-1} \end{pmatrix} \begin{pmatrix} a_{21}-a_{11} \\ \vdots \\ a_{2l_1-1}-a_{1l_1-1} \\ a_{2l_1} \\ \vdots \\ a_{2l_2-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

もし $l_2 \geqq l_1+1$ ならば上式の左辺の $l_1 \times (l_2-1)$ 行列の階数は l_1 である．従って $l_2 > l_1+1$ ならば上式を満足する $a_{21}, a_{22}, \cdots, a_{2l_2-1}$ が選べる．一方，$l_2=l_1+1$ のときは上の等式より $a_{2i}=a_{1i}(1 \leqq i \leqq l_1-1)$, $a_{2l_1}=a_{2l_2-1}=0$ でなければならなく，特に多項式 f_2 の最高次の係数 a_{2l_2-1} が零でなければならず，(l_2, l_2) 符号にならない．$l_2=l_1$ のときも同様に $a_{21}, a_{22}, \cdots, a_{2l_2-1}$ の解は唯一に決まり $f_1=f_2$ となる．しかしこの場合 $S_1=S_2$ なので問題はない．一方もし $l_2 > q$ ならば相異なる $x_1, \cdots, x_{l_2}$ が選べないので，体の構成から始めなければならない．

以上のことから，定理1の証明にある方法を用いて複数割り当てを行って，管理人の増加した場合次の定理が成り立つ．

［定理5］ 定理4において，計算は体 GF(q) 上で行われているとする．もし $|S_2|=|S_1|$, あるいは $q \geqq |S_2| > |S_1|+1$ であれば，S_1 の符号構成を変えることなく S_2 に$(|S_2|, |S_2|)$− しきい値法の構造を持たせることができる．

定理5からわかるように，管理人が増加したとき，各管理人に与えてあって分散情報をとりあげる必要はなく，いくつか分散情報の数を増やして，それらを管理人に追加配分すればよい．また，その際の符号構成の変更も可能である．

4. 重複なし複数割り当て法

今までは同じ分散情報 w_i が複数の管理人に割り当てられていた．しかしどの w_i も一人の管理人にしか割り当てられていないとしたら，どういうことが起きるか興味が持たれる．この方法を重複なし割り当て法と呼ぶことにする．例えば複数割り当ての場合のように任意のアクセス構造がこの制約のもとで実現できるであろうか．この問題がしきい値グラフ，あるいは線形分離性の問題に帰着できることを示す．

同じ分散情報は一回しか使用されないものであるから，任意の $Q \subseteqq P$ に対して，

$$\left|\bigcup_{p \in Q} g(p)\right| = \sum_{p \in Q} |g(p)|$$

が成り立つ．容易にわかるように，結局 $|g(p)|$ の値だけが問題となり，具体的に何が割り当てられているかは問題ではない．そこで，関数 $g: P \to 2^S$ を考えるかわりに次のような関数 h を考える．

$h: P \to Z^+$ $\quad (Z^+$ は非負の整数$)$

このとき実際の割り当て関数 $g: P \to 2^S$ は

$|g(p_j)|=h(p_j)$ $\quad (j=1, \cdots, n)$

$g(p_j) \cap g(p_i)=\phi$ $\quad (1 \leqq i \leqq j \leqq n)$

となるように定めればよい．今，適当に h を定め，h に応じて g による割り当てを行う．分散情報の総数 l は

$$l=\sum_{j=1}^{n} h(p_j)$$

である．$k \leqq l$ なる (k, l) 符号を用いるとすると，アクセス構造 $\mathcal{A}_h$ と非アクセス構造 $\mathcal{B}_h$ は

$$\mathcal{A}_h=\{Q \subset P : \sum_{p \in Q} h(p) \geqq k\}$$

$$\mathcal{B}_h=\{Q \subset P : \sum_{p \in Q} h(p) \leqq k-1\}$$

$$=2^P-\mathcal{A}_h$$

である．与えられた $\mathcal{A} \subset 2^P$ が必要条件(a)を満足するならば h と S を適当に選ぶことにより $\mathcal{A}_h=\mathcal{A}$ とすることができるかという問題を考えよう．実は必ずしも実現できるとは限らない．例を一つ挙げよう．

［例3］ P と $\mathcal{A}^-$ を

$P=\{p_1, p_2, p_3, p_4\}$

$\mathcal{A}^-=\{\{p_1, p_2\}, \{p_2, p_3\}, \{p_3, p_4\}\}$

とする．このとき $\mathcal{B}^+$ は

$\mathcal{B}^+=\{\{p_1, p_3\}\}, \{p_1, p_4\}, \{p_2, p_4\}\}$

である．もしこのアクセス構造が上記のシステムにより実現できたとすると，ある k が存在して

$h(p_1)+h(p_2) \geqq k > h(p_1)+h(p_3)$

でなければならない．すなわち

$h(p_2)>h(p_3)$

である．また

$h(p_3)+h(p_4)\geqq k>h(p_2)+h(p_4)$

でなければならない．すなわち

$h(p_3)>h(p_2)$

である．これは矛盾である．　　（例終）

上記のような h の存在を問う問題がいわゆる線形分離性問題に帰着されることを示そう．n 次元ユークリッド空間 R^n 内の点集合が二つ与えられたとする．この二つの点集合を一つの超平面で分けられるときこれらは線形分離可能であると言う．つまり二つの点集合を $\mathcal{F}_1, \mathcal{F}_2$ としたとき，$\boldsymbol{x}\in\mathcal{F}_1$ ならば $F(\boldsymbol{x})\geqq 0$ であり，$\boldsymbol{x}\in\mathcal{F}_2$ ならば $F(\boldsymbol{x})<0$ となる超平面 $F(\boldsymbol{x})=h_1x_1+h_2x_2+\cdots+h_nx_n-k=0(\boldsymbol{x}\in R^n)$ が存在するとき，$\mathcal{F}_1$, $\mathcal{F}_2$ は線形分離可能であると言う．線形分離性問題とは，n 次元空間の有限点集合が二つ与えられたときに，これらが線形分離可能であるか否かを判定し線形分離可能であるならばそれらを分ける超平面 $F(\boldsymbol{x})$ を求めよという問題である．

いま $P=\{p_1,\cdots,p_n\}$ の部分集合 Q に対し，ベクトル $\boldsymbol{x}(Q)=(x_1,\cdots,x_n)\in R^n$ を，

$p_i\in Q$ ならば $x_i=1$

$p_i\notin Q$ ならば $x_i=0$

により対応させる．いま $h(p_i)=h_i$, $\boldsymbol{h}=(h_1,\cdots,h_n)$, とおけば，$Q\subset P$ に対し，$\sum_{p\in Q}h(p)=\ll\boldsymbol{x}(Q),\boldsymbol{h}\gg$ である．ここで $\ll\boldsymbol{x}(Q),\boldsymbol{h}\gg$ はベクトルの内積を表す．この章のはじめで述べた問題は R^n の部分集合に対する線形分離性問題に帰着する．$\mathcal{F}_1$ と $\mathcal{F}_2$ を

$\mathcal{F}_1=\{\boldsymbol{x}(A):A\in\mathcal{A}\}$

$\mathcal{F}_2=\{\boldsymbol{x}(B):B\in\mathcal{B}\}$

とする．また $h_1,\cdots,h_n,k$ が非負であるという条件で線形分離性問題を解き $F(\boldsymbol{x})$ を求めることができれば，その $h_1,\cdots,h_n$ が各個人割り当て分散情報数となり，k がしきい値となる．しかし例3にある通り，$\mathcal{F}_1$ と $\mathcal{F}_2$ は線形分離可能とは限らない．ここでは，この方法で実現されるアクセス構造が満たすべき必要条件を挙げよう．

[定理6]重複なし複数割り当て法で実現できるシステムのアクセス構造 $\mathcal{A}$ は次の条件(e)を満足する．

条件(e)

各 $p_i, p_j\in P$ に対して

$\mathcal{F}_{ij}=\{Q\subset P-\{p_i,p_j\}:Q\cup\{p_i\}\in\mathcal{A}\}$

$\mathcal{F}_{ji}=\{Q\subset P-\{p_i,p_j\}:Q\cup\{p_j\}\in\mathcal{A}\}$

とおくと，各 $1\leqq i<j\leqq n$ について $F_{ij}\supseteqq F_{ji}$ あるいは $F_{ij}\subseteqq F_{ji}$ である．

（証明）　$\mathcal{A}_h=\mathcal{A}$ なる $h:P\to Z^+$ が存在する．このとき任意の $p_i, p_j\in P$ に対し，

$\mathcal{F}_{ij}=\{Q\subset P-\{p_i,p_j\}:\sum_{p\in Q}h(p)\geqq k-h(p_i)\}$

$\mathcal{F}_{ji}=\{Q\subset P-\{p_i,p_j\}:\sum_{p\in Q}h(p)\geqq k-h(p_j)\}$

である．$h(p_i)\geqq h(p_j)$ ならば，明らかに $\mathcal{F}_{ij}\supseteqq\mathcal{F}_{ji}$ である．一方 $h(p_i)\leqq h(p_j)$ ならば，明らかに $\mathcal{F}_{ij}\subseteqq\mathcal{F}_{ji}$ である．　　（証明終）

さて，$\mathcal{A}\in 2^P$ が重複なし複数割り当て法で実現できるための条件(e)が必要条件であることはわかったが，十分条件であるかどうかについてはわかっていない．但し，任意の $A\in\mathcal{A}^-$ について $|A|=2$ のときは，点集合 P, 辺集合 $\mathcal{A}^-$ を持つグラフを考えて，Chvátal と Hammer は条件(e)が必要十分条件であることを示した[1]．またこの問題に対してOrlinは割り当てる整数の総和が最小となるような最適解を求めている[4]．

A^- の要素が位数2とは限らない一般の場合は，しきい値ハイパーグラフの問題に帰着するが，これに関してはいまのところ何も知られていない．

5. むすび

本論文では，(k,n) しきい値構造を含むより一般的なアクセス構造を実現する秘密共有法を考案した．すなわち，各管理人に複数個の分散情報を割り当てる複数割り当て法を提案し，それがあらゆるアクセス構造を実現できることを示した．ところが，その証明のなかで示した方法は管理人一人あたりの分散情報の数が管理人の人数に対して指数関数的に増えてしまうという欠点がある．一方，この方法を用いると，管理人が増えた場合，きわめて特殊な場合を除いて，以前に渡した分散情報を変える必要がないという特徴がある．

後半では，複数割り当て法の特別な場合として，重複なし複数割り当て法を考えた．この方法によるアクセス構造の実現問題はしきい値グラフ，あるいは線形分離性の問題に帰着できることを示した．

今後の課題としては，与えられたアクセス構造を実現する複数割り当て法のなかで分散情報の総数が最小のものを求めることがまず挙げられる．

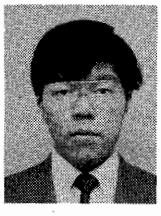
謝辞　背益な御助言をいただいた東北大学工学部通信工学科斎藤伸自教授，日本電気 C & C 研中村勝洋博士ならびに NTT 基礎研究所小山謙二氏に深謝いたします．また日頃ご討論していただいた東北大工学部

通信工学科斎藤研究室の金丸直義氏に深謝いたします．なお本研究の一部分は電気通信普及財団および文部省科学研究費補助金：奨励研究(A)62780017の援助のもとに行われた．

文　献

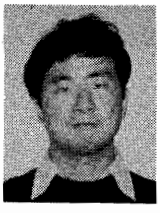
(1) V. Chvátal, and P. L. Hammer："Aggregation of inequalities in integer programming", Ann. Discrete Math., 1, pp. 145-162 (1977).
(2) D. E. Denning："Cryptography and Data Security", Addison-Wesley, Reading, Mass. (1982).
(3) 小山謙二：複数グループ間の暗号鍵共有法とその解析", 情報学論, **22**, 2, pp. 81-88 (昭56-03).
(4) J. Orlin："The minimal integral separator of a threshold graph", Ann. Discrete Math, 1, pp. 415-419 (1977).
(5) A. Shamir："How to share a secret", Commun. ACM, **22**, 11, pp. 612-613 (1979).
(6) 上原, 西関, 岡本, 中村：マトロイド的アクセス構造を持つ秘密共有法", 信学論, **J69-A**, 9, pp. 1124-1132 (昭和61-09).

(昭和63年1月13日受付，4月1日再受付)



伊藤　充

昭61東北大・工・電通卒．昭63同大学院修士課程了．現在，三菱電機に勤務．



斎藤　明

昭56年東大・理・情報卒．昭61年同大学院博士課程了，理博．同年東北大・工・通信助手．以来グラフ理論，組合せ理論に関する研究に従事．AMS，日本数学会，オセアニア組合せ論学会各会員，昭63年4月よりニュジーランド，オタゴ大学客員研究員．

西関　隆夫

昭44東北大・工・通信卒．昭49同大学院博士課程了，工博．同年同大助手．昭51同助教授．現在同教授．アルゴリズム，グラフ理論，回路網理論の研究と教育に従事．IEEEシニア会員，ACM，情報処理学会員．