信州大学
大学院理工学系研究科

修士論文

2 変数 2 次多項式を用いた秘密分散法における一般アクセス構造の実現性について

指導教員　西新 幹彦 准教授

専攻　電気電子工学専攻
学籍番号　13TM236F
氏名　西山 達矢

2015 年 3 月 9 日

目次

1 序論

1.1 研究の背景と目的

個人情報や企業の機密情報の漏洩が社会問題になっていることから，電子情報の紛失と漏洩を防ぐことが企業に求められている．電子情報の紛失への対策として電子情報を複製した場合，それだけ多くの人の手による漏洩の危険性が高まる．一方，電子情報の漏洩への対策として電子情報を何らかの方法で分割した場合には，分割された電子情報を紛失すれば，元の電子情報を復元することができなくなる．このような電子情報の紛失と漏洩への対策を両立させることができる技術として秘密分散法がある．秘密分散法の実現法の一つとして Shamir の多項式補間法がある [1]．この方法では秘密情報からシェアと呼ばれる分散情報を n 個作成し，各シェアをユーザに分配する．そして，任意の k 人が集まれば，秘密情報を復元できるというものである．この方法では，秘密の復元の可否は集まったユーザが保持するシェアの個数のみによって決まることから (k, n) しきい値法と呼ばれる．

(k, n) しきい値法では秘密情報の復元の可否は集まったユーザの人数のみによって決まることから，任意のユーザの組み合わせに対して秘密を復元したいといった要求にこたえることができない．しかし，(k, n) しきい値法により生成されたシェアをユーザに複数割り当てる複数割り当て法により，任意のユーザの組み合わせに対して秘密情報を復元する方法が考案されている [2]．また，この方法は整数計画法に帰着されることが分かっている [3]．

本研究では Shamir の多項式補間法で用いられる 1 変数多項式を 2 変数に拡張し，2 変数 2 次多項式の補間法による秘密分散法を考える．この多項式を用いた秘密分散法ではシェアは x-y 平面上での位置により特徴付けられ，集まったシェアの個数やシェアの位置の組み合わせにより復元の可否が決まるようになる [4]．Shamir の多項式補間法では，秘密情報を復元することと多項式を復元することは同義であるが，2 変数 2 次多項式の補間法の場合では多項式を復元しなくても秘密情報を復元できる場合があるのが特徴である．複数割り当て法ではユーザに複数のシェアを割り当てる必要があるが，2 変数 2 次多項式の補間法による秘密分散法ではユーザの管理するシェアを 1 つとしたままで一部の一般アクセス構造を実現することができることが知られている．そこで本研究では，まだ実現性が判定されていない一般アクセス構造のうち，要素数 3 個のアクセス集合を含むアクセス構造が実現可能であるか調べた．

1.2 本論文の構成

本論文では次のような構成をとる．2 章では秘密分散法の概要と秘密分散法で用いられる用語の説明を行う．3 章では 2 変数に拡張した秘密分散法の説明を行う．4 章ではアクセス構造の実現性を判定する方法の説明を行う．5 章と 6 章では 4 章で示した判定法に従い，アクセス

構造の実現性の判定を行う．最後に 7 章でまとめを行う．

2　秘密分散法

この章では複数割り当て法によって一般アクセス構造を実現する方法について述べる．また複数割り当て法は (k,n) しきい値法に基づいていることから，(k,n) しきい値法について述べる．

秘密分散法は秘密情報の保有者とシェアを管理するユーザの間で行われる．秘密分散法は秘密情報からシェアを生成しユーザに分配する分散プロセスと，ユーザが集まりユーザの保持するシェアから秘密情報を復元する復元プロセスの 2 つの手順に分けられる．

ここで，ユーザの集合を $P = \{p_1, \cdots, p_n\}$ とする．また秘密情報を S とし，シェアを $v_1, \cdots, v_m$ と表すことにする．この P の部分集合のうち，秘密を復元できるユーザの組み合わせをアクセス集合と呼び，そうでないものを非アクセス集合と呼ぶ．ある集合の部分集合がアクセス集合を含むとき，その集合は部分集合に示されたユーザが集まれば秘密が復元されることからアクセス集合の超集合もまたアクセス集合となる．

すべてのアクセス集合からなる族をアクセス構造 $\mathcal{A} \subset 2^P$ と呼ぶ．なお，2^P は P の部分集合全体からなる族である．またアクセス構造の極小元のなす族を極小アクセス集合族 $\mathcal{A}^-$ と呼ぶ．極小アクセス集合族は極小なアクセス集合全体からなる族であり，アクセス集合の超集合もまたアクセス集合となることから，アクセス構造は極小アクセス集合族から完全に記述される．また非アクセス集合全体からなる族を非アクセス構造 $\mathcal{B} \subset 2^P$ と呼び，$\mathcal{B}$ の極大元のなす族を極大非アクセス構造 $\mathcal{B}^+ \subset 2^P$ と呼ぶ．$\mathcal{B}^+$ によって非アクセス構造は完全に記述されることになる．

秘密分散法のアクセス構造は完全型とランプ型の 2 つに大別できる [5]．n 個のシェアのうち非アクセス集合である m 個のシェアが集まったとき，秘密情報のエントロピーが $H(S|v_1, \cdots, v_m) = H(S)$ となるものを完全型と呼ぶ．完全型では，非アクセス集合からは秘密情報に関する情報が全く漏洩しない．対して，$H(S|v_1, \cdots, v_m) < H(S)$ となり，秘密情報に関する情報がいくらか漏洩してしまう場合があるものをランプ型と呼ぶ．本論文では完全型アクセス構造をもつ秘密分散法について説明する．

また秘密分散法はアクセス構造によってしきい値型と非しきい値型の 2 つに大別できる．n 個のシェアのうち任意の k 個のシェアによって秘密を復元でき，$k-1$ 個未満のシェアでは秘密を復元できないとき，アクセス構造を (k,n) しきい値型と呼ぶ．(k,n) しきい値型でないアクセス構造を非しきい値型と呼ぶ．アクセス構造として，(k,n) しきい値型または非しきい値型を含むアクセス構造を一般アクセス構造と呼ぶ．

2.1 Shamir の多項式補間法

複数割り当て法は (k,n) しきい値法に基づいているため，この節では複数割り当て法を説明するためにまず (k,n) しきい値型秘密分散法について述べる．

(k,n) しきい値型秘密分散法は (k,n) しきい値型アクセス構造を持っているから，n 個のシェア $v_1,\cdots,v_n$ のうち任意の k 個が集まれば秘密が復元でき，秘密情報のエントロピー $H(S|v_1,\cdots,v_k)=0$ となる．また任意の $k-1$ 個のシェアからは秘密に関する情報は何も得られないため，$H(S|v_1,\cdots,v_{k-1})=H(S)$ となる．

この節ではしきい値型秘密分散法の実現法の一つである Shamir の多項式補間法を説明する．

まず，分散の手順を説明する．秘密情報の保持者をディーラと呼び，n 人のユーザの集合を $P=\{p_1,\cdots,p_n\}$ とする．秘密分散法での演算はすべて有限体 $\mathbb{F}$ の上で行い，相異なる n 個の要素 $x_1,\cdots,x_n$ を選ぶ．ディーラは $a_1,\cdots,a_{k-1}\in\mathbb{F}$ をランダムに選ぶ．次に 1 変数 $k-1$ 次多項式 $f(x)=a_1x+\cdots+a_{k-1}x^{k-1}+S$ を考え，ユーザ p_i に $(x_i,f(x_i))$ の形でシェアを分配する．ここで x_i は公開情報とし，$f(x_i)$ は各ユーザが管理する非公開情報とする．

次に復元の手順を説明する．k 人のユーザが集まることにより k 個のシェアを用いて多項式 f を復元することができる．これから $f(0)$ を求めれば秘密情報を得ることができる．$k-1$ 人以下のユーザが集まった場合には f を一意に復元することができず，また完全型であることから，秘密情報に関する情報は何も得られない．

2.2 複数割り当て法

(k,n) しきい値法により生成されたシェアをユーザに複数割り当てる複数割り当てることにより，任意のユーザの組み合わせによって秘密情報を復元する方法を複数割り当て法と呼ぶ．この方法によって一般アクセス構造を実現できることができる [2]．

複数割り当て法において n 人のユーザにシェアを割り当てる手順を説明する．秘密情報の保持者であるディーラが，秘密分散法を用いてあるユーザの組み合わせに対して秘密情報を復元したいと考えたとする．次にディーラは，秘密情報を復元できるユーザの組み合わせを表す極小アクセス集合族を指定する．例えば，4 人のユーザ $p_1,\cdots,p_4$ のうち p_1,p_2 によって秘密を戻したいと考え，また p_1,p_3,p_4 によっても秘密を戻したい場合には，極小アクセス集合族は $\mathcal{A}^-=\{\{p_1,p_2\},\{p_1,p_3,p_4\}\}$ と記述する．$\mathcal{A}^-$ から極大非アクセス構造 $\mathcal{B}^+=\{B_1,\cdots,B_l\}$ を考える．例で挙げた $\mathcal{A}^-$ に対しては $\mathcal{B}^+=\{\{p_1,p_3\},\{p_1,p_4\},\{p_2,p_3,p_4\}\}$ である．次に (l,l) しきい値法によって l 個のシェア $v_1,\cdots,v_l$ を生成する．ユーザ p_j に対するシェア割り当ては $g(p_j)=\{v_i\colon p_j\notin B_i\in\mathcal{B}^+\}$ $(j=1,\cdots,n)$ とする．

例で挙げた $\mathcal{A}^-$ に対するシェアの割り当ては

$$g(p_1) = \{v_3\},\ g(p_2) = \{v_1, v_2\},\ g(p_3) = \{v_2\},\ g(p_4) = \{v_1\}$$

となる．この例ではアクセス集合に記載されたユーザが集まったとき，3 個の相異なるシェアが集まるから秘密情報を復元できることがわかる．例で示したように複数割り当て法ではユーザの管理するシェアの個数が複数となることがある．

3　2 変数 2 次の多項式補間法のアクセス構造

本研究では，2 変数 2 次の多項式補間法による秘密分散法を考えている．この章では多項式補間法による秘密分散法でのシェア生成と秘密の復元を説明するためにアクセス構造を説明する．

2 変数 2 次多項式は，有限体 $\mathbb{F}$ の上の $f(x, y) = ax^2 + bx + cxy + dy + ey^2 + S$ と定義する．ここで各係数 a, b, c, d, e はランダムな値を用い，S は秘密情報である．シェアは $v_i = (x_i, y_i, f(x_i, y_i))$ の形で与えられ，(x_i, y_i) をシェアの位置と呼ぶ．またシェア v_i を保持するユーザを p_i と表す．シェアの位置は公開情報とし，$f(x_i, y_i)$ は各ユーザが管理する非公開情報とする．また秘密分散法の目的から原点に位置するシェアは生成しない．多項式 f によるアクセス構造は既に明らかになっている [4]．シェアの個数が 1,2 の集合は，非アクセス集合であることは自明である．多項式の項が 6 つであることから，極小のアクセス集合のサイズは高々 6 である．したがって，7 個以上のシェアが集まったときのアクセス集合の判定法は 6 個以下のアクセス集合の判定法に帰着される．そのため以下では極小のアクセス集合のみのアクセス構造を説明する．シェアの個数が 3,4,5,6 の場合のアクセス集合の判定するには以下のようにすればよい．

今後，演算はすべて有限体上で行うが，直感的なわかりやすさのため実数体であるかのような図を使って説明を行うことがある．

3.1　3 個のシェアのアクセス構造

定理 1　異なる 3 個のシェア v_1, v_2, v_3 がアクセス集合となるためには行列

$$V_3 = \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \\ x_3 & y_3 \end{pmatrix}$$

の階数が 1 となることが必要十分条件である．

この定理は，各シェアが x-y 平面上で原点を通る直線上に配置されていれば秘密を復元できることを示している．媒介変数 t を用いて $x = \alpha t, y = \beta t$ を多項式 f に代入すれば，f は 1

変数 2 次多項式となるため，直線上の異なる 3 個のシェアを用いれば秘密を復元できることがわかる．

3.2 4 個のシェアのアクセス構造

定理 2 異なる 4 個のシェアがアクセス集合であるための必要十分条件は，そのある真部分集合がアクセス集合であることである．

この定理は 4 個のシェアのうち，定理 1 によってアクセス集合と判定されるような 3 個のシェアが存在すれば秘密が復元できることを示している．

3.3 5 個のシェアのアクセス構造

定理 3 異なる 5 個のシェア v_1, v_2, v_3, v_4, v_5 がアクセス集合となるための必要十分条件は，ある真部分集合がアクセス集合であるか，または行列

$$V_5 = \begin{pmatrix} x_1^2 & x_1 & x_1y_1 & y_1 & y_1^2 \\ x_2^2 & x_2 & x_2y_2 & y_2 & y_2^2 \\ x_3^2 & x_3 & x_3y_3 & y_3 & y_3^2 \\ x_4^2 & x_4 & x_4y_4 & y_4 & y_4^2 \\ x_5^2 & x_5 & x_5y_5 & y_5 & y_5^2 \end{pmatrix}$$

の階数が 4 でありかつ V_5 のある列の要素をすべて 1 にした行列が正則となることである．

原点を通る 2 次曲線上の 5 個のシェアは定理 3 からアクセス集合と判定することができる．

原点を通る 2 次曲線として，原点を通る直線と原点を通らない直線の組を考えた場合においても 5 個のシェアによって秘密情報を復元できる．この場合には，原点を通る直線上に 2 個のシェアがあり，3 個のシェアが原点を通らない直線の上にあるとき，5 個のシェアは定理 3 からアクセス集合と判定することができる．これは，原点を通らない直線上に配置された 3 個のシェアからその直線上の任意のシェアを得ることができるので，2 本の直線の交点のシェアを得ることができる．そうして得られたシェアと原点に配置された 2 個のシェアの 3 個のシェアから原点を通る直線上の復元できることができ，秘密を復元できるためである．

3.4　6 個のシェアのアクセス構造

定理 4　異なる 6 個のシェア $v_1, v_2, v_3, v_4, v_5, v_6$ がアクセス集合となるための必要十分条件は，ある真部分集合がアクセス集合であるか，または行列

$$V_6 = \begin{pmatrix} x_1^2 & x_1 & x_1y_1 & y_1 & y_1^2 & 1 \\ x_2^2 & x_2 & x_2y_2 & y_2 & y_2^2 & 1 \\ x_3^2 & x_3 & x_3y_3 & y_3 & y_3^2 & 1 \\ x_4^2 & x_4 & x_4y_4 & y_4 & y_4^2 & 1 \\ x_5^2 & x_5 & x_5y_5 & y_5 & y_5^2 & 1 \\ x_6^2 & x_6 & x_6y_6 & y_6 & y_6^2 & 1 \end{pmatrix}$$

が正則となることである．

これは多項式 f は 6 個の項を有していおり，V_6 が正則であれば V_6 の逆行列を考えることができ，秘密情報 S を復元することができるためである．

4　アクセス構造の実現性の判定

秘密の保持者であるディーラはアクセス構造 $\mathcal{A}$ を指定する．そして，$\mathcal{A}$ の実現性を判定する手順を説明する．

まず，指定されたアクセス構造から極小アクセス集合族 $\mathcal{A}^- = \{A_1, \cdots, A_n\}$ を作成する．

次に，極小アクセス集合族に含まれるアクセス集合の要素数が 1,2,4 または 7 以上であった場合，指定されたアクセス構造は実現不可能と判定する．それは，極小アクセス集合族に含まれるアクセス集合の要素数は定理 1，定理 2，定理 3，定理 4 から 3,5,6 のいずれかだからである．以下では，要素数が 3,5,6 のいずれかであるような極小アクセス集合からなるアクセス構造の実現性を判定する．そのため，今後は極小アクセス集合族としてすべて異なる 11 人のユーザ $p_1, \cdots, p_{11}$ による $\{\{p_1, p_2, p_3\}, \{p_4, p_5, p_6\}, \{p_7, p_8, p_9, p_{10}, p_{11}\}\}$ のような例を考える．この例では，各極小アクセス集合の要素数は 3,3,5 なので，このようなアクセス構造を 3-3-5 構造または 3^2-5 構造と表記する．

指定されたアクセス構造の実現性は，極小アクセス集合族から新たなアクセス集合が導出されるか判定すれば良い．

まず $\mathcal{A}^-$ からアクセス集合 $A_i = \{v_1, \cdots, v_m\}$ を取り出し，定理 1，定理 3，定理 4 に従いシェア $v_1, \cdots, v_m$ を x-y 平面上に配置する．シェアがアクセス集合となるための条件は定理 1，定理 3，定理 4 より与えられるが，定理 1，定理 3 は x-y 平面における幾何学的な条件として解釈することができる．そのため，シェアは以下の手順に従って配置する．$|A_i| = 3$ なら定理 1 に従い原点を通る直線上に A_i のシェアを配置する．$|A_i| = 5$ なら定理 3 に従い原点を通る 2 次直線上に A_i のシェアを配置する．$|A_i| = 6$ の場合にはシェア配置がアクセス集合とな

るための幾何学的な条件を考えることができないが，A_i の 6 個のシェアは定理 4 に従い秘密を戻せるように配置されており，また 5 個以下のシェアでは秘密が戻らないように配置する．このようにシェアを配置すれば，各アクセス集合に記載されたシェアを選択すれば秘密を復元することができる．

アクセス集合に記載されていない組み合わせのシェアを選択した場合には秘密を戻したくないので，次の手順を行う．まずアクセス集合に記載されていない組み合わせの 3 個のシェアを x-y 平面上から選択する．そして 3 個のシェアに定理 1 を適用し，3 個のシェアによって秘密を戻せない条件を求める．これを 5 個のシェア，6 個のシェアについて定理 3，定理 4 を適用し，秘密を戻せない条件を求める．各条件を満たすようにシェアを配置すれば，そのようなシェア配置からは新たにアクセス集合が導出されないため，指定されたアクセス構造は実現可能と判定される．各条件が矛盾している場合には，指定されたアクセス構造は実現不可能と判定される．

5　互いに素な極小アクセス集合族

この章では互いに素な極小アクセス集合族によって表されるアクセス構造の実現性の特徴と実現性の判定をしていく．

調べるべき互いに素な極小アクセス集合族のパターンは図 1 のように表される．図 1 では要素数 6 の極小アクセス集合族について，その極小アクセス集合族 に含まれる 6 個のアクセス集合の要素数を表している．例えば，図中の一行目は 3^6 構造を表し，二行目は 3^5-5 構造を表している．図 1 よりアクセス構造の数を求めると，要素数が 1 個の場合も含めると 83 個である．極小アクセス集合が 1 つのアクセス構造は実現可能である．この場合は定理 1，定理 3，定理 4 に従いシェアを配置すれば良いからである．

互いに素なアクセス構造 $\mathcal{A}_1$ が実現不可能であったとき，$\mathcal{A}_1$ のアクセス集合と互いに素なアクセス集合を追加したアクセス構造 $\mathcal{A}_2$ を考える．この $\mathcal{A}_2$ はまた実現不可能なアクセス構造となり実現不可能性は継承される．その理由を説明する．もし，極小アクセス集合族 $\mathcal{A}_1^-$ がアクセス集合 A_1, A_2 を要素として $\mathcal{A}_1^- = \{A_1, A_2\}$ と表されており，A_1,A_2 とも異なるアクセス集合 A_3 によって秘密が復元できたとする．A_1 と A_2 は互いに素であるが，A_3 は A_1 と A_2 のユーザを含んでいる．次に A_1,A_2 とも互いに素なアクセス集合 A_4 を $\mathcal{A}_1^-$ に追加した $\mathcal{A}_2^- = \{A_1, A_2, A_4\}$ を考える．$\mathcal{A}_2^-$ は $\mathcal{A}_1^-$ の超集合であるが，どちらも A_3 によって秘密が復元できるからである．

アクセス集合が 7 個以上の極小アクセス集合族が指定されたとき，そのアクセス構造の実現性は部分集合の実現性を調べればよいことになる．7 個以上の極小アクセス集合からなるアクセス構造の実現性の判定法を説明する．例えば極小アクセス集合族として $\mathcal{A}^- = \{A_1, \cdots, A_7\}$ が指定されたとする．そして $\mathcal{A}^-$ から 6 個のアクセス集合を選択し，そ

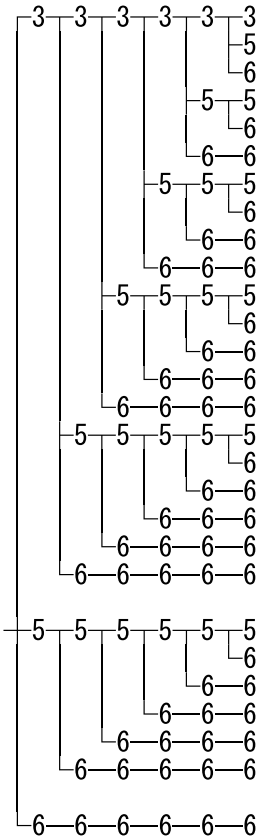

図 1　互いに素な極小アクセス集合族

の 6 個のアクセス集合からなる構造 $\mathcal{A}_i \subset \mathcal{A}^-$ の実現性を判定する．7 個のアクセス集合のうち 6 個選択するから ${}_7C_6 = 7$ 通りのアクセス構造の実現性を判定する．もし，実現不可能と判定される $\mathcal{A}_i$ があれば，実現不可能性が継承されることから $\mathcal{A}^-$ も実現不可能と判定される．全ての部分集合 $\mathcal{A}_i$ が実現可能と判断された時を考える．その時 $\mathcal{A}_i$ が実現可能となるためのシェア配置の条件が与えられるが，与えられたすべての条件を満たすようにシェア配置を行えるなら $\mathcal{A}^-$ は実現可能と判定される．各条件が矛盾する内容を含んでいるのであれば，$\mathcal{A}^-$ を実現するようなシェア配置を行えないので，$\mathcal{A}^-$ は実現不可能と判定される．

この章の以降では，互いに素な極小アクセス集合族によって表されるアクセス構造の実現性の判定を行う．

5.1 3-3 構造

極小アクセス集合族として $\{\{p_1, p_2, p_3\}, \{p_4, p_5, p_6\}\}$ が指定されたとする．

$\{p_1, p_2, p_3\}$ と $\{p_4, p_5, p_6\}$ によって秘密が復元できる条件から，各アクセス集合のシェアは定理 1 より原点を通る直線上に配置されている必要がある．そのため，各アクセス集合のシェアは図 2 のように原点を通る直線上に配置されなければならない．

まず 6 人のユーザから 3 人のユーザを選択することを考え，各アクセス集合からそれぞれ 1 人のユーザと 2 人のユーザを選択する．そのような 3 人として p_1, p_2, p_4 を選び，各ユーザに対応するシェア v_1, v_2, v_4 によって秘密が復元できるか考える．ここで，v_1, v_2, v_3 は原点を通る傾き α の直線上に配置されており，v_4, v_5, v_6 は原点を通る傾き β の直線上に配置されているとする．

定理 1 より

$$\mathrm{rank} \begin{pmatrix} x_1 & \alpha x_1 \\ x_2 & \alpha x_2 \\ x_4 & \beta x_4 \end{pmatrix} = \mathrm{rank} \begin{pmatrix} 1 & \alpha \\ 0 & \alpha - \beta \\ 0 & 0 \end{pmatrix}$$

の行列の階数が 1 の時，3 個のシェアにより秘密が復元されてしまうことを意味する．

α と β が異なる値のとき，行列の階数は 2 となる．v_1, v_2, v_3 が x 軸上に配置されており，または v_4, v_5, v_6 が y 軸上に配置されている場合でも行列の階数は 2 となる．そのため α と β が相異なるとき 3 人のユーザから秘密を復元されない．

5 人のユーザを選択した場合には，秘密を戻せる条件を判定すべき場合が存在しない．それは 6 人のユーザから 5 人を選択すると，必ず部分集合としてアクセス集合を含むからである．6 人の場合についても同様である．

よって，3-3 構造は実現可能であり，実現可能となるシェア配置の条件は v_1, v_2, v_3 と

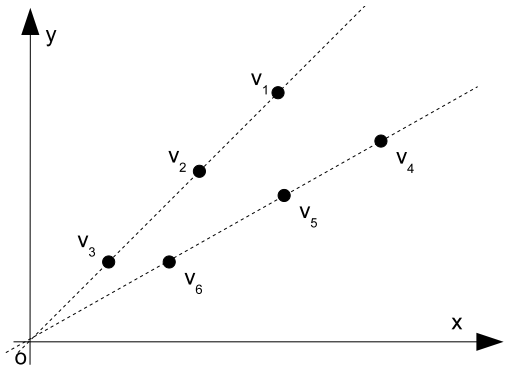

図 2　3-3 構造

v_4, v_5, v_6 がそれぞれ異なる傾きの原点を通る直線上に配置されていることである．

5.2 3-3-3 構造

極小アクセス集合族として $\{\{p_1, p_2, p_3\}, \{p_4, p_5, p_6\}, \{p_7, p_8, p_9\}\}$ が指定されたとする．

各アクセス集合のシェアは定理 1 より原点を通る直線上に配置される必要があるから，各シェアは図 3 のように配置されていなければならない．また前節の 3-3 構造の結果より，原点を通る直線の傾きはそれぞれ相異なる値でなければならない．

各アクセス集合から 2 人ずつユーザを選択し，6 人のユーザ $p_1, p_2, p_4, p_5, p_7, p_8$ によって秘密が復元できるか考える．6 人のユーザに対応する $v_1, v_2, v_4, v_5, v_7, v_8$ から，定理 4 より

$$|V_6| = \begin{vmatrix} x_1^2 & x_1 & \alpha x_1^2, & \alpha x_1 & \alpha^2 x_1^2 & 1 \\ x_2^2 & x_2 & \alpha x_2^2, & \alpha x_2 & \alpha^2 x_2^2 & 1 \\ x_4^2 & x_4 & \beta x_4^2, & \beta x_4 & \beta^2 x_4^2 & 1 \\ x_5^2 & x_5 & \beta x_5^2, & \beta x_5 & \beta^2 x_5^2 & 1 \\ x_7^2 & x_7 & \gamma x_7^2, & \gamma x_7 & \gamma^2 x_7^2 & 1 \\ x_8^2 & x_8 & \gamma x_8^2, & \gamma x_8 & \gamma^2 x_8^2 & 1 \end{vmatrix}$$

が非零であれば 6 個のシェアは秘密を復元されてしまうことを意味する．なお，α, β, γ は各アクセス集合のシェアが配置されている原点を通る直線の傾きを表す．

そのため，$|V_6|$ が 0 になる条件を求める．$|V_6|$ を因数分解すると，$(x_2 - x_1)(x_5 - x_4)(x_8 - x_7)(\alpha - \beta)(\alpha - \gamma)(\beta - \gamma)$ が因数として現れる．またそれ以外に行列内の全ての変数を含む因数が現れるのでそれを $g(x_1, \cdots, x_8)$ とおく．因数 $(x_2 - x_1), (x_5 - x_4), (x_8 - x_7)$ は非零である．なぜなら x_i と x_j は同じ傾きの直線上に配置されているが，2 個のシェア v_i, v_j は互いに異なるシェアであり x_i と x_j は異なる値を持つためである．直線の傾きは相異なる値であり，$\alpha - \beta, \alpha - \gamma, \beta - \gamma$ は非零である．

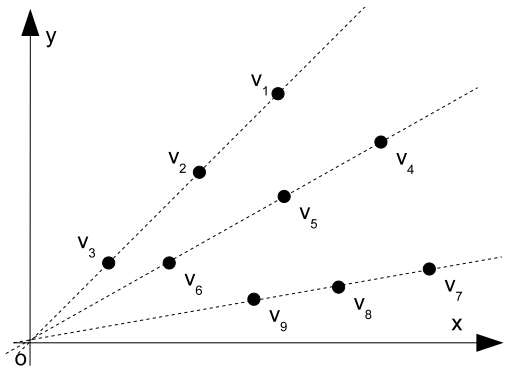

図 3　3-3-3 構造

$g(x_1, \cdots, x_8)$ は x_8 に関する一次式であり，$g = 0$ を x_8 について解き，$x_8 = h(x_1, \cdots, x_7)$ とすれば $|V_6|$ は 0 となる．ここで，x_9 は $x_9 \neq x_7$，$x_9 \neq x_8$ であり，$|V_6|$ の x_8 を x_9 に置き換えた行列式 $|V_6^{'}|$ は非零となる．なぜなら，$x_8 = h(x_1, \cdots, x_7)$，$x_9 \neq x_7$，$x_9 \neq x_8$ の条件の下で，背理法の仮定として $|V_6^{'}| = 0$ とすれば，$x_9 = x_8$ となり矛盾だからである．

以上のことは V_6 内に示した 6 個のシェア $v_1, v_2, v_4, v_5, v_7, v_8$ では秘密を復元できないが，v_8 を v_9 に取り替えた場合には秘密が復元できることを意味している．

よって，3-3-3 構造は実現不可能である．

5.3 3-5 構造

極小アクセス集合族として，$\{A_1, A_2\} = \{\{p_1, p_2, p_3\}, \{p_4, p_5, p_6, p_7, p_8\}\}$ が指定されたとする．

A_1 のシェアは原点を通る傾き α の直線上に配置されており，A_2 のシェアは原点を通る 2 次曲線の上に図 4 のように配置されていなければならない．

なお，指定された極小アクセス集合族は互いに素であるから，原点を通る直線と原点を通る 2 次直線上の交点にシェアを配置してはならない．それは例えば A_1 のシェア v_1 が交点上に配置されていれば，A_1, A_2 と互いに素であるシェアの集合 p_1, p_4, p_5, p_6, p_7 などによって秘密を復元されてしまうからである．A_2 のシェアが交点に配置されている場合も A_1, A_2 と互いに素である集合によって秘密が復元されてしまう．

指定されたアクセス構造の実現性を判定する．まず，A_1 から 1 人のユーザを選択し，A_2 から 4 人のユーザを選択する．そのような 5 人として p_1, p_4, p_5, p_6, p_7 を考え，各ユーザに対応するシェア v_1, v_4, v_5, v_6, v_7 によって秘密が復元されるか考える．5 個のシェアによって秘密を復元するには，5 個のシェアが原点を通る 2 次直線上に配置される必要がある．ここで，原

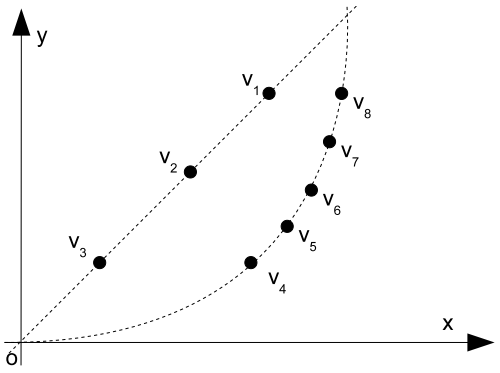

図 4　3-5 構造

点を通る直線と原点を通る 2 次直線の交点は高々 2 点であり，そのうち一点は原点である．今は互いに素な極小アクセス集合族を考えているので，もう一点の交点にシェアが配置されることはない．そのため 5 個のシェアは 2 次曲線上に配置されていないので秘密が復元されない．同様に A_1 から 2 人のユーザを選択し，A_2 から 3 人のユーザを選択した場合においても 5 人のユーザから 2 次曲線を復元することはできないため，秘密は復元されない．

次に 5 人のユーザによって秘密が復元されるか考える．A_1 から 2 人のユーザを選択し，A_2 から 4 人のユーザを選択する．このような 6 人として $p_1, p_2, p_4, p_5, p_6, p_7$ を選択する．このとき，各ユーザに対応するシェアによって行列式

$$|V_6| = \begin{vmatrix} x_1^2 & x_1 & \alpha x_1^2, & \alpha x_1 & \alpha^2 x_1^2 & 1 \\ x_2^2 & x_2 & \alpha x_2^2, & \alpha x_2 & \alpha^2 x_2^2 & 1 \\ x_4^2 & x_4 & x_4 y_4, & y_4 & y_4^2 & 1 \\ x_5^2 & x_5 & x_5 y_5, & y_5 & y_5^2 & 1 \\ x_6^2 & x_6 & x_6 y_6, & y_6 & y_6^2 & 1 \\ x_7^2 & x_7 & x_7 y_7, & y_7 & y_7^2 & 1 \end{vmatrix}$$

が非零であれば秘密が復元されてしまうことを意味する．そのため $|V_6| = 0$ となる条件を求める．$|V_6|$ を因数分解すると 2 つの因数を含む．1 つは $x_2 - x_1$ で，もう一方の因数は行列内の全ての変数を含む式である．後者の因数を $g(x_1, \cdots, x_7, y_4, \cdots, y_7)$ と表す．原点を通る直線上のシェアは異なる場所に配置するため，$x_2 - x_1$ は非零となる．

g は x_1 について 1 次式であり，3-3-3 構造の時と同様に考えて，原点を通る直線から 2 人のユーザを選択し，原点を通る 2 次直線から 4 人のユーザを選択した場合には，秘密が復元されてしまうことが分かる．

よって，3-5 構造は実現不可能と判定される．

5.4 3-6 構造

極小アクセス集合族として，$\{A_1, A_2\} = \{\{p_1, p_2, p_3\}, \{p_4, p_5, p_6, p_7, p_8, p_9\}\}$ が指定されたとする．ここで，v_1, v_2, v_3 は定理 1 から原点を通る傾き α の直線上に配置されているとする．また A_2 のシェアは定理 4 より 6 個のシェアによってのみ秘密が復元できるように配置されているとする．

A_1 から 1 人のユーザを選択し，A_2 から 5 人を選択する．そのような 6 人として $p_1, p_4, p_5, p_6, p_7, p_8$ を考え，次の行列式

$$|V_6| = \begin{vmatrix} x_1^2 & x_1 & \alpha x_1^2, & \alpha x_1 & \alpha^2 x_1^2 & 1 \\ x_4^2 & x_4 & x_4 y_4, & y_4 & y_4^2 & 1 \\ x_5^2 & x_5 & x_5 y_5, & y_5 & y_5^2 & 1 \\ x_6^2 & x_6 & x_6 y_6, & y_6 & y_6^2 & 1 \\ x_7^2 & x_7 & x_7 y_7, & y_7 & y_7^2 & 1 \\ x_8^2 & x_8 & x_8 y_8, & y_8 & y_8^2 & 1 \end{vmatrix}$$

が非零であれば秘密が復元されてしまうことを意味する．この行列式は x_1 についての 2 次式なので，x_1 に関する $|V_6| = 0$ の解は高々 2 個である．これは，行列式が零となるような x_1 のシェアの位置は 2 か所存在することを意味している．原点を通る直線上には 3 個のシェア $\{p_1, p_2, p_3\}$ を配置する必要があり，そのうち 2 個は行列式が零になるように配置しても，残る 1 個のシェアを用いれば行列式は非零となる．

よって行列式が零となるようにシェアを配置することはできず，3-6 構造は実現不可能である．

5.5 この章のまとめ

この章では，要素数 3 のアクセス集合を含むアクセス構造の実現可能性について判定した．その結果，3-3 構造は各アクセス集合のシェアがそれぞれ異なる傾きの原点を通る直線上に配置されているとき，実現可能であることが分かった．3-3-3 構造，3-5 構造，3-6 構造は実現不可能であることが分かった．

また，前章で例として挙げた 3-3-5 構造 $\{\{p_1, p_2, p_3\}, \{p_4, p_5, p_6\}, \{p_7, p_8, p_9, p_{10}, p_{11}\}\}$ は部分集合として 3-5 構造を含んでいることから，3-3-5 構造は実現不可能であることが分かる．

本論文で実現可能性を調べていないアクセス構造を列挙すると図 5 となる．

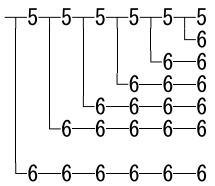

図 5　実現可能性を調べていない互いに素な極小アクセス集合族

6 互いに素でない極小アクセス集合族

調べるべき互いに素でない極小アクセス集合族のパターンは，互いに素な場合に比べ多いことが予想される．3-3 構造は互いに素な場合では $\{\{p_1, p_2, p_3\}, \{p_4, p_5, p_6\}\}$ の 1 通りだけであった．しかし，互いに素で無い場合には，1 個のユーザ p_1 を共有した $\{\{p_1, p_2, p_3\}, \{p_1, p_4, p_5\}\}$ と 2 個のシェア p_1, p_2 を共有した $\{\{p_1, p_2, p_3\}, \{p_1, p_2, p_4\}\}$ の 2 通りを考えることができるためである．

互いに素でない極小アクセス集合族として $\mathcal{A}_1^- = \{\{p_1, p_2, p_3\}, \{p_1, p_4, p_5\}\}$ と $\mathcal{A}_2^- = \{\{p_1, p_2, p_3\}, \{p_2, p_4, p_5\}\}$ を考える．A_2^- は p_1 と p_2 の添え字を交換すれば，$\mathcal{A}_1^-$ と同じ極小アクセス集合族となり，どちらのアクセス構造も実現可能性は同一である．そのため，アクセ

ス構造の実現性を調べる際にはどちらかの実現性を調べればよい．しかし一般に，添え字の交換で実現可能性が保存される構造をすべて列挙するには時間がかかる．[*1]

また，互いに素な極小アクセス集合族と異なる性質として，互いに素でない極小アクセス集合族では実現不可能性の継承を考えることができないことがあげられる．実現不可能性が継承されない理由を説明する．もし，極小アクセス集合族 $\mathcal{A}^-$ が $\mathcal{A}^- = \{A_1, A_2\}$ と表されており，A_1,A_2 とも異なるアクセス集合によって秘密が復元できるシェアの配置があれば，$\mathcal{A}^-$ は実現不可能と判定される．しかし，その配置のシェアが $\{A_1, A_2, A_3, \cdots, A_m\}$ という極小アクセス集合族をもてば，このアクセス構造は実現可能と判定される．すなわち，$\{A_1, A_2\}$ は実現不可能だが，$\{A_1, A_2, A_3, \cdots, A_m\}$ は実現可能である．

この章の以降では，互いに素でない極小アクセス集合族によって表されるアクセス構造の実現性の判定を行う．

6.1 3-3 構造

極小アクセス集合族として，$\{A_1, A_2\} = \{\{p_1, p_2, p_3\}, \{p_1, p_4, p_5\}\}$ が指定されたとする．

A_1 と A_2 によって秘密が復元できる条件から，各アクセス集合のシェアは原点を通る直線上に配置されている必要がある．また，ユーザ p_1 を共有していることから，2 つの直線の傾きは同じである．そのため，5 人のユーザから任意に 3 人のユーザを選択すると秘密を復元することができる．よって 1 人のユーザを共有する 3-3 アクセス構造は実現不可能である．

また，2 人のユーザを共有する 3-3 構造も実現不可能となる．

よって，3-3 構造は実現不可能である．

6.2 共有ユーザが 1 人の 3-5 構造

極小アクセス集合族として，ユーザ p_1 を共有する $\{\{p_1, p_2, p_3\}, \{p_1, p_4, p_5, p_6, p_7\}\}$ が指定されたとする．v_1, v_2, v_3 は原点を通る傾き α の直線上に配置されており，v_1, v_4, v_5, v_6, v_7 は原点を通る 2 次曲線の上に配置する必要がある（図 6）．また v_1 は原点を通る直線と原点を通る 2 次曲線の交点に配置する．

7 人のユーザのうち 3 人のユーザによって秘密が戻るか考える．このとき 3 人のユーザの選択は次の 4 パターン存在する

(1) $\{p_1, p_2, p_4\}$

[*1] 例で挙げた 2 つのアクセス構造 $\mathcal{A}_1^-, \mathcal{A}_2^-$ の実現可能性が同じと判定するには，$\mathcal{A}_2^-$ の 2 つのシェア間の添え字同士を交換し，$\mathcal{A}_1^-$ と同じ添え字の組み合わせになるか調べる．もし添え字の交換によって極小アクセス集合族の表現が同じになれば，2 つの実現可能性は同一と判断される．このとき添え字を取り換える作業は最大で 4! 回行う必要がある．

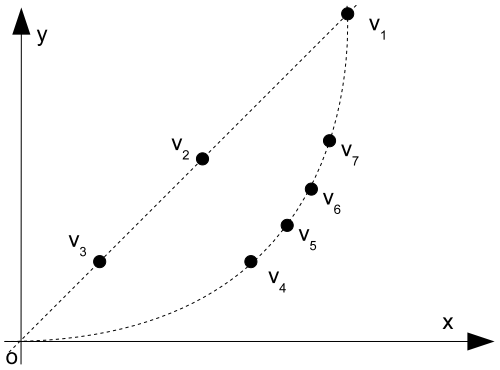

図 6　共有ユーザが 1 人の 3-5 構造

(2) $\{p_1, p_4, p_5\}$
(3) $\{p_2, p_4, p_5\}$
(4) $\{p_2, p_3, p_4\}$

(1) は共有ユーザの p_1 と直線上の p_2, p_3 から一人を選択し，2 次曲線上の v_4, v_5, v_6, v_7 から 1 人を選択した場合である．(2) は p_1 と v_4, v_5, v_6, v_7 から 2 人を選択する場合である．(3) は p_2, p_3 から 1 人選択し，v_4, v_5, v_6, v_7 から 2 人選択する場合である．(4) は p_2, p_3 と v_4, v_5, v_6, v_7 から 1 人選択する場合である．どのパターンも原点を通る直線上に 3 個のシェアが存在していないことから 3 個のシェアによって秘密を復元することはできない．

7 人のユーザから極小アクセス集合族に記載されていない 6 人のユーザの組み合わせは $\{p_2, p_3, p_4, p_5, p_6, p_7\}$ の 1 通りだけである．このとき，5.2 節の 3-3-3 構造で示した関数 g を用いて，v_2 を $x_2 = g(x_3, x_4, y_4, \cdots, y_7)$ で決まる位置に配置すれば 6 個のシェアから秘密は復元されない．

7 人のうちアクセス集合に記載されていない 5 人のユーザの選択は 3 パターン存在する．

(1) $\{p_2, p_4, p_5, p_6, p_7\}$
(2) $\{p_1, p_2, p_4, p_5, p_6\}$
(3) $\{p_2, p_3, p_4, p_5, p_6\}$

(1) は直線上の p_2, p_3 のうち 1 人を選択し，2 次曲線上の v_4, v_5, v_6, v_7 の 4 人を選択する場合である．(2) は p_1, p_2 を選択し，v_4, v_5, v_6, v_7 から 3 人選択する場合である．(3) は p_2, p_3 を選択し，v_4, v_5, v_6, v_7 から 3 人選択する場合である．

(1),(2) の場合には秘密は復元されない．2 次曲線の一般式は $ax^2 + bx + cxy + dy + ey^2 + f = 0$ であるが，原点を通る 2 次曲線に限定すると，$f = 0$ であり，a で割れば

$x^2 + b'x + c'xy + dy + e'y^2 = 0$ となる．よって，4 点の位置情報があれば原点を通る 2 次曲線は復元できる．ここで，4 個のシェア v_4, x_5, v_6, v_7 または v_1, v_5, v_6, v_7 によって復元された 2 次曲線上に v_2 が存在すれば秘密を戻すことができるが，v_2 は 2 次曲線上にないためである．

v_2 は $g(x_3, y_3, \cdots, y_7)$ で決まる場所に配置した．そのため，(3) による秘密復元の可否を調べるためには v_2 が v_3, v_4, v_5, v_6 で復元した原点を通る 2 次曲線上に存在するか調べればよい．復元された原点を通る 2 次曲線上に v_2 が配置されていれば秘密は復元されてしまうことを意味する．

2 次曲線と直線との交点は高々 2 点（原点ともう 1 点）である．よって，4 個のシェア v_3, v_4, v_5, v_6 によって復元した 2 次曲線上に v_2 は存在しない．なぜなら，復元された原点を通る 2 次曲線と原点を通る直線との交点は 2 点あり，それは原点と v_3 だからである．

3 人のユーザと 6 人のユーザによって秘密が戻らないことと，6 人によって秘密が戻らないようにシェアを配置した条件の下で 5 人のユーザによって秘密が戻らないことがわかった．よって共有ユーザが 1 人の 3-5 構造は実現可能である．

6.3 共有ユーザが 2 人の 3-5 構造

極小アクセス集合族として，2 人のユーザ p_1, p_2 を共有する $\{\{p_1, p_2, p_3\}, \{p_1, p_2, p_4, p_5, p_6\}\}$ が指定されたとする．原点を通る直線と原点を通らない直線の組を 2 次曲線として用い，シェアは図 7 のように配置されていなければならない．

6 個のシェアのうち，原点を通る直線上に配置されている 3 個のシェアは v_1, v_2, v_3 だけである．これは極小アクセス集合族に記載されたアクセス集合であり，そのほかのシェアの組み合わせでは秘密を戻すことはできない．そのため，図 7 のようにシェアを配置した場合 3 個のシェアによって秘密を戻すことはできない．

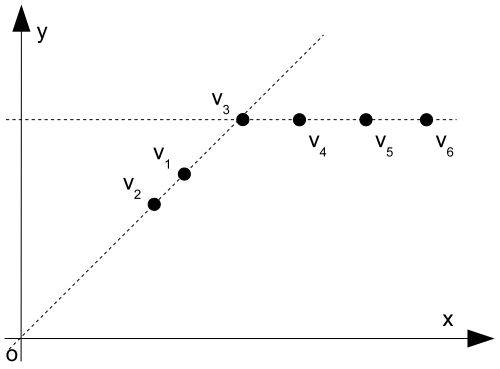

図 7　共有ユーザが 2 人の 3-5 構造

アクセス集合に記載されていない 5 個のシェアの組み合わせは $\{v_1, v_3, v_4, v_5, v_6\}$, $\{v_2, v_3, v_4, v_5, v_6\}$ の 2 通りであり，どちらも定理 3 より 5 個のシェアによって秘密を戻すことはできない．

次に 6 個のシェアからなる集合を考えると，その集合はシェア全体だから 6 個のシェアによる実現性を判定すべき場合が存在しない．

そのため，共有ユーザが 2 人の 3-5 構造は図 7 のようにシェアを配置すれば実現可能となる．

6.4 この章のまとめ

この章では，要素数 3 のアクセス集合を含むアクセス構造の実現可能性について判定した．その結果，3-3 構造はどのようなシェア配置を行っても実現不可能であることが分かった．3-5 構造は共有ユーザが 1 人，2 人どちらも実現可能であることが分かった．

7 まとめと今後の課題

2 変数 2 次の多項式補間法による秘密分散法において，一部の一般アクセス構造を実現するためのシェア配置の条件を求めた．

互いに素な極小アクセス集合族については，要素数 3 のアクセス集合を含むアクセス構造の実現可能性について判定した．その結果，2 個の要素数 3 の極小アクセス集合からなるアクセス構造は実現可能であることが分かった．他の場合はどのようなシェア配置を行っても実現不可能となることが分かった．

互いに素でない極小アクセス集合族についても同様に検討を行った．その結果，2 個の要素数 3 の極小アクセス集合からなるアクセス構造は，どのようにシェアを配置しても実現不可能であることが分かった．要素数 3 個と 5 個の極小アクセス集合それぞれ 1 つからなるアクセス構造については，共有シェアが 1 個，2 個どちらも実現可能であることが分かった．

本論文では一部の一般アクセス構造の実現性について判定したが，残りの一般アクセス構造の実現性を判定することが今後の課題である．

乱数の生成はコストがかかることから，使用する乱数はなるべく少ないほうがよい．複数割り当て法と 2 変数多項式による秘密分散法では使用する乱数の数が異なる場合があるので，使用する乱数の数を比較する．互いに素な 3-3 構造の極大非アクセス構造 $\mathcal{B}^+$ は

$$\{\{p_1, p_2, p_4, p_5\}, \{p_1, p_2, p_4, p_6\}, \{p_1, p_2, p_5, p_6\},$$
$$\{p_1, p_3, p_4, p_5\}, \{p_1, p_3, p_4, p_6\}, \{p_1, p_3, p_5, p_6\},$$
$$\{p_2, p_3, p_4, p_5\}, \{p_2, p_3, p_4, p_6\}, \{p_2, p_3, p_5, p_6\}\}$$

となる．複数割り当て法によって 3-3 構造を実現するためには $|\mathcal{B}^+| = 9$ より $(9, 9)$ しきい値

法によりシェアを生成するので，1 変数多項式の係数を決めるため乱数は 8 個必要とされる．対して，2 変数多項式の場合には 2 変数多項式の係数を決めるため 5 個の乱数を必要とする．従って，3-3 構造では 2 変数多項式による秘密分散法のほうが乱数の数の点で優っている．

1 人のユーザを共有する 3-5 構造は，複数割り当て法では 8 個の乱数を必要とし，2 変数多項式による秘密分散法のほうが乱数の数の点で優っている．

しかし，2 人のユーザを共有する 3-5 構造は，複数割り当て法では 4 個の乱数を必要とし，乱数の数の観点では 2 変数多項式の秘密分散法のほうが劣っていることになる．

今後の課題として，本論文では実現性を判定しなかったアクセス構造についても，複数割り当て法に比べ乱数を必要とするか調べていきたい．

謝辞

本研究を行うにあたって，細かく指導してくださった指導教員の西新幹彦准教授に感謝の意を表する．

参考文献

[1] A.Shamir, “How to share a secret,” Comm.ACM, vol.22, no.11, pp.612–613, 1979.

[2] 伊藤充, 斎藤明, 西関隆夫, “一般的なアクセス構造を実現する秘密共有法”, 電子情報通信学会論文誌 A, Vol.J71-A, pp.1592–1598, 1988.

[3] Mitsugu Iwamoto, Hirosuke Yamamoto and Hirohisa Ogawa, “Optimal multiple assignment based on integer programming in secret sharing with general access structures,” IEICE Trans. Fundamentals, vol.E90-A, no.1, pp.101–112, Jan.2007.

[4] 柏倉英明, 西新幹彦, “2 変数 2 次の多項式補間法による秘密分散法のアクセス構造”, IEICE Technical Report, col.111, no.51, pp.11–24, 2011.

[5] 山本博資, “秘密分散法とそのバリエーション”, 数理解析研究所講究録, 1361 巻, pp.19–31, 2004.