ISSN 2186-5647

2-51

EAS として構成可能な管理者が 5 人以下のアクセス構造に関する考察

日大生産工(院)　○岡崎　太介　　日大生産工　栃窪　孝也

1. まえがき

情報化社会において、盗難対策と紛失対策の両方を実現する情報の安全な保管方法である秘密分散法は、重要な技術の一つであるといえる。1979年にShamir[1]とBlakleyは(k,n)しきい値法と呼ばれる秘密分散法をそれぞれ発表した。一方、2016年にKomargodski[2]らは管理者を追加可能なアクセス構造であるEASを提案した。

本稿では、Komargodskiらの手法により管理者4人のアクセス構造に管理者を1人追加することで、管理者4人のアクセス構造からEASとして構成可能な管理者5人のアクセス構造との対応関係を明らかにする。

2. 秘密分散法

(k,n)しきい値法とは、ディーラーが秘密情報をn個の分散情報(シェア)に分割して管理者に割り当て、k個以上のシェアを集めれば秘密情報が復元でき、k個未満のシェアからは秘密情報に関する情報は得られないという手法である。

$n \in \mathbb{N}$において$[n]$を集合$\{1,\dots,n\}$とする。n人の管理者の集合を$\mathcal{P}_n = \{1,\dots,n\}$とする。管理者集合$\mathcal{P}_n$の部分集合のうち、秘密情報を復号可能な権限を持つ集合をアクセス集合と呼び、アクセス集合から成る族$\mathcal{A} \subseteq 2^{\mathcal{P}_n}$をアクセス構造と呼ぶ。$\mathcal{A}$は空でない単調集合族である。つまり、$B \in \mathcal{A}$に対し、$B \subseteq C$ならば$C \in \mathcal{A}$となる。また、$\mathcal{A}$に含まれない$\mathcal{P}_n$の部分集合を非アクセス集合と呼ぶ。また、$\mathcal{A}$の極小集合族$\mathcal{A}^-$は次のように定義できる。

$$\mathcal{A}^- = \{A \in \mathcal{A} : A - \{P\} \notin \mathcal{A} \ for\ any\ P \in A\}$$

Komargodski らは管理者を追加可能なアクセス構造 Evolving Access Structure(EAS)を提案している。$\mathcal{A}$ を EAS としたとき、 $\mathcal{A} \subseteq 2^{\mathbb{N}}$は単調集合族であり、全ての$t \in \mathbb{N}$に対して$\mathcal{A}$の部分集合族

$$\mathcal{A}_t \triangleq \mathcal{A} \cap [t] \qquad (1)$$

はアクセス構造となる。つまり、t人目の管理者を追加しアクセス構造$\mathcal{A}_t$を構成する際、$\mathcal{A}_{t-1}$に含まれるアクセス集合は$\mathcal{A}_t$にも含まれる。

3. 管理者が4人と5人のアクセス構造の対応関係

3.1. EASの条件を考慮しない場合

管理者4人のアクセス構造を表1に、Jackson[3]らにより評価された管理者が5人の場合におけるアクセス構造を付録に示す。表1の3番はアクセス構造$\{\{a\},\ \{b,c\},\ \{b,d\}\}$を意味する。

表 1　管理者 4 人のアクセス構造

番号	アクセス構造	番号	アクセス構造
1	$a+b+c+d$	11	$ab+ac+bd$
2	$a+b+cd$	12	$ab+ac+bd+cd$
3	$a+bc+bd$	13	$ab+ac+bcd$
4	$a+bc+bd+cd$	14	$ab+cd$
5	$a+bcd$	15	$ab+acd$
6	$ab+ac+bc+ad$	16	$ab+acd+bcd$
7	$ab+ac+bc+ad+bd$	17	$abc+abd$
		18	$abc+abd+acd$
8	$ab+ac+bc+ad+bd+cd$	19	$abc+abd+acd+bcd$
9	$ab+ac+ad$	20	$abcd$
10	$ab+ac+ad+bcd$		

表1のアクセス構造を$\mathcal{A}_4$、付録のアクセス構造を$\mathcal{A}_5$とする。$\mathcal{A}_4$に管理者を1人追加し、$\mathcal{A}_5$を構成するとき、アクセス構造として構成可能とする条件を次に示す。

(i)　すべてのアクセス集合$A \in \mathcal{A}_4$に対し、$A \in \mathcal{A}_5$が成り立つ

例として、表1の13番のアクセス構造

$$\mathcal{A}_{4,13} : ab+ac+bcd$$

から、付録の48番のアクセス構造

$$\mathcal{A}_{5,48} : ab+ac+ad+bcd+ae$$

が構成可能かを判定する。

Some Considerations on Evolving Access Structure on 5 or less participants

Taisuke Okazaki and Kouya Tochikubo

$\mathcal{A}_{4,13}$のすべてのアクセス集合が$\mathcal{A}_{5,48}$に属しており、条件(i)を満たすため、$\mathcal{A}_{4,13}$から$\mathcal{A}_{5,48}$は構成可能である。表2は$\mathcal{A}_4$から構成可能な$\mathcal{A}_5$の対応関係を示したものである。どの$\mathcal{A}_4$からも構成不可能な$\mathcal{A}_5$は該当なしとしている。

表 2　$\mathcal{A}_4$から構成可能な$\mathcal{A}_5$の対応関係

番号	管理者 5 人のアクセス構造	番号	管理者 5 人のアクセス構造
1	1	11	21 – 33, 69 – 78
2	3, 4	12	21 – 24, 69, 70
3	6 – 13	13	48 – 58, 79 – 91
4	6 – 8	14	21 – 24, 69, 70, 100 – 104
5	17 – 19	15	105 – 129
6	21 – 43	16	105 – 117
7	21 – 33	17	133 – 170
8	21 – 24	18	133 – 157
9	21 – 43, 48 – 68	19	133 – 142
10	48 – 58	20	176 – 179
該当なし			2, 5, 14–16, 20, 44–47, 92–99, 130–132, 171, 171–175, 180

3.2. EASの条件を考慮する場合

$\mathcal{A}_4$からEASとして$\mathcal{A}_5$が構成可能かを判定する際は、条件(i)に加え、式(1)を考慮する必要があるため、次の条件(ii)を満たさなければならない。

(ii) すべてのアクセス集合$A \in \mathcal{A}_5 - \mathcal{A}_4$に対し、$\{e\} \subseteq A$が成り立つ

つまり、5人目の管理者を追加する際、$\mathcal{A}_4$に追加されるアクセス集合は、5人目の管理者eが含まれるアクセス集合でなければならない。3.1の例において、$\mathcal{A}_{5,48}$は$\mathcal{A}_{4,13}$にアクセス集合adとaeを追加したアクセス構造である。adは5人目の管理者eを含まず、条件(ii)を満たさないためEASとしては構成不可能である。また、EASとして構成可能な例としては、$\mathcal{A}_{4,13}$から

$$\mathcal{A}_{5,81} : ab + ac + bcd + bce + ade$$

を構成する場合が挙げられる。$\mathcal{A}_{5,81}$は、$\mathcal{A}_{4,13}$に5人目の管理者eが含まれるアクセス集合bceとadeを追加したアクセス構造であり、条件(i),(ii)をともに満たすため、EASとして構成可能である。これらの条件をもとに、$\mathcal{A}_4$からEASとして構成可能な$\mathcal{A}_5$の対応関係を表3に示す。

表 3　$\mathcal{A}_4$から EAS として構成可能な$\mathcal{A}_5$の対応関係

番号	管理者 5 人のアクセス構造	番号	管理者 5 人のアクセス構造
1	1	11	71 – 78
2	3, 4	12	69, 70
3	9 – 13	13	79 – 91
4	6 – 8	14	100 – 104
5	17 – 19	15	118 – 129
6	34 – 43	16	105 – 117
7	25 – 33	17	158 – 170
8	21 – 24	18	143 – 157
9	59 – 68	19	133 – 142
10	48 – 58	20	176 – 179
該当なし			2, 5, 14, 15, 16, 20, 44, 45, 46, 47, 92, 93, 94, 95, 96, 97, 98, 99, 130, 131, 132, 171, 172, 173, 174, 175, 180

4. $\mathcal{A}_4$から構成可能な$\mathcal{A}_5$の最大対応数

アクセス構造は管理者を並べ替えることで、異なるアクセス構造を表現できる。例として、$\mathcal{A}_{4,13}$は管理者を$\{a, b, c, d\}$から$\{a, d, b, c\}$のように並べ替えることで

$$\mathcal{A}_{4,13}' : ad + ab + dbc$$

というアクセス構造となる。4人の管理者の並べ替えで表現できるすべての$\mathcal{A}_4$について、$\mathcal{A}_4$から構成可能な$\mathcal{A}_5$の最大対応数を、3.1と3.2の条件でそれぞれ評価した結果を表4に示す。

表 4　$\mathcal{A}_4$構成可能な$\mathcal{A}_5$の最大対応数

	最大対応数
3.1 の条件	44
3.2 の条件	15

謝辞　本研究はJSPS科研費18K11303の助成を受けたものです。

参考文献

1) Adi Shamir, “How to share a secret,” Communications of the ACM, vol.22, no.11, pp.612-613, 1979.
2) I. Komargodski, M. Naor, E. Yogev, “How to share a secret infinitely,” Theory of Cryptography Conference, pp.485-514, 2016
3) Wen-Ai Jackson and Keith M.Marin, “Perfect secret sharing schemes on five participants,” Designs, Codes and Cryptography, 9, pp.267-286, 1996

付録　管理者が 5 人の場合のアクセス構造

	アクセス構造		アクセス構造
1	$a + b + c + d + e$	46	$ab + ac + bc + ade + bde$
2	$a + b + c + de$	47	$ab + ac + bc + ade + bde + cde$
3	$a + b + cd + ce$	48	$ab + ac + ad + bcd + ae$
4	$a + b + cd + ce + de$	49	$ab + ac + ad + bcd + ae + bce$
5	$a + b + cde$	50	$ab + ac + ad + bcd + ae + bce + bde$
6	$a + bc + bd + cd + be$	51	$ab + ac + ad + bcd + ae + bce + bde + cde$
7	$a + bc + bd + cd + be + ce$	52	$ab + ac + ad + bcd + be$
8	$a + bc + bd + cd + be + ce + de$	53	$ab + ac + ad + bcd + be + ce$
9	$a + bc + bd + be$	54	$ab + ac + ad + bcd + be + ce + de$
10	$a + bc + bd + be + cde$	55	$ab + ac + ad + bcd + be + cde$
11	$a + bc + bd + ce$	56	$ab + ac + ad + bcd + bce$
12	$a + bc + bd + ce + de$	57	$ab + ac + ad + bcd + bce + bde$
13	$a + bc + bd + cde$	58	$ab + ac + ad + bcd + bce + bde + cde$
14	$a + bc + de$	59	$ab + ac + ad + ae$
15	$a + bc + bde$	60	$ab + ac + ad + ae + bcde$
16	$a + bc + bde + cde$	61	$ab + ac + ad + be$
17	$a + bcd + bce$	62	$ab + ac + ad + be + ce$
18	$a + bcd + bce + bde$	63	$ab + ac + ad + be + ce + de$
19	$a + bcd + bce + bde + cde$	64	$ab + ac + ad + be + cde$
20	$a + bcde$	65	$ab + ac + ad + bce$
21	$ab + ac + bc + ad + bd + cd + ae$	66	$ab + ac + ad + bce + bde$
22	$ab + ac + bc + ad + bd + cd + ae + be$	67	$ab + ac + ad + bce + bde + cde$
23	$ab + ac + bc + ad + bd + cd + ae + be + ce$	68	$ab + ac + ad + bcde$
24	$ab + ac + bc + ad + bd + cd + ae + be + ce + de$	69	$ab + ac + bd + cd + bce$
25	$ab + ac + bc + ad + bd + ae$	70	$ab + ac + bd + cd + bce + ade$
26	$ab + ac + bc + ad + bd + ae + be$	71	$ab + ac + bd + ce$
27	$ab + ac + bc + ad + bd + ae + be + cde$	72	$ab + ac + bd + ce + de$
28	$ab + ac + bc + ad + bd + ae + ce$	73	$ab + ac + bd + ce + ade$
29	$ab + ac + bc + ad + bd + ae + ce + de$	74	$ab + ac + bd + bce$
30	$ab + ac + bc + ad + bd + ae + cde$	75	$ab + ac + bd + bce + ade$
31	$ab + ac + bc + ad + bd + ce$	76	$ab + ac + bd + bce + ade + cde$
32	$ab + ac + bc + ad + bd + ce + de$	77	$ab + ac + bd + bce + cde$
33	$ab + ac + bc + ad + bd + cde$	78	$ab + ac + bd + cde$
34	$ab + ac + bc + ad + ae$	79	$ab + ac + bcd + bce$
35	$ab + ac + bc + ad + ae + de$	80	$ab + ac + bcd + bce + de$
36	$ab + ac + bc + ad + ae + bde$	81	$ab + ac + bcd + bce + ade$
37	$ab + ac + bc + ad + ae + bde + cde$	82	$ab + ac + bcd + bce + ade + bde$
38	$ab + ac + bc + ad + be$	83	$ab + ac + bcd + bce + ade + bde + cde$
39	$ab + ac + bc + ad + be + de$	84	$ab + ac + bcd + bce + bde$
40	$ab + ac + bc + ad + be + cde$	85	$ab + ac + bcd + bce + bde + cde$
41	$ab + ac + bc + ad + de$	86	$ab + ac + bcd + de$
42	$ab + ac + bc + ad + bde$	87	$ab + ac + bcd + ade$
43	$ab + ac + bc + ad + bde + cde$	88	$ab + ac + bcd + ade + bde$
44	$ab + ac + bc + de$	89	$ab + ac + bcd + ade + bde + cde$
45	$ab + ac + bc + ade$	90	$ab + ac + bcd + bde$

91	$ab + ac + bcd + bde + cde$	136	$abc + abd + acd + bcd + abe + ace + bce + ade$
92	$ab + ac + de$	137	$abc + abd + acd + bcd + abe + ace + bce + ade + bde$
93	$ab + ac + ade$	138	$abc + abd + acd + bcd + abe + ace + bce + ade + bde + cde$
94	$ab + ac + ade + bde$	139	$abc + abd + acd + bcd + abe + ace + ade$
95	$ab + ac + ade + bde + cde$	140	$abc + abd + acd + bcd + abe + ace + bde$
96	$ab + ac + ade + bcde$	141	$abc + abd + acd + bcd + abe + ace + bde + cde$
97	$ab + ac + bde$	142	$abc + abd + acd + bcd + abe + cde$
98	$ab + ac + bde + cde$	143	$abc + abd + acd + abe$
99	$ab + ac + bcde$	144	$abc + abd + acd + abe + ace$
100	$ab + cd + ace$	145	$abc + abd + acd + abe + ace + ade$
101	$ab + cd + ace + bce$	146	$abc + abd + acd + abe + ace + ade + bcde$
102	$ab + cd + ace + bce + ade$	147	$abc + abd + acd + abe + ace + bde$
103	$ab + cd + ace + bce + ade + bde$	148	$abc + abd + acd + abe + ace + bde + cde$
104	$ab + cd + ace + bde$	149	$abc + abd + acd + abe + ace + bcde$
105	$ab + acd + bcd + ace$	150	$abc + abd + acd + abe + bce$
106	$ab + acd + bcd + ace + bce$	151	$abc + abd + acd + abe + bce + cde$
107	$ab + acd + bcd + ace + bce + ade$	152	$abc + abd + acd + abe + cde$
108	$ab + acd + bcd + ace + bce + ade + bde$	153	$abc + abd + acd + abe + bcde$
109	$ab + acd + bcd + ace + bce + ade + bde + cde$	154	$abc + abd + acd + bce$
110	$ab + acd + bcd + ace + bce + ade + cde$	155	$abc + abd + acd + bce + bde$
111	$ab + acd + bcd + ace + bce + cde$	156	$abc + abd + acd + bce + bde + cde$
112	$ab + acd + bcd + ace + ade$	157	$abc + abd + acd + bcde$
113	$ab + acd + bcd + ace + ade + cde$	158	$abc + abd + abe$
114	$ab + acd + bcd + ace + bde$	159	$abc + abd + abe + cde$
115	$ab + acd + bcd + ace + bde + cde$	160	$abc + abd + abe + acde$
116	$ab + acd + bcd + ace + cde$	161	$abc + abd + abe + acde + bcde$
117	$ab + acd + bcd + cde$	162	$abc + abd + ace$
118	$ab + acd + ace$	163	$abc + abd + ace + ade$
119	$ab + acd + ace + ade$	164	$abc + abd + ace + ade + bcde$
120	$ab + acd + ace + ade + cde$	165	$abc + abd + ace + bde$
121	$ab + acd + ace + ade + bcde$	166	$abc + abd + ace + bde + cde$
122	$ab + acd + ace + bde$	167	$abc + abd + ace + bcde$
123	$ab + acd + ace + bde + cde$	168	$abc + abd + cde$
124	$ab + acd + ace + cde$	169	$abc + abd + acde$
125	$ab + acd + ace + bcde$	170	$abc + abd + acde + bcde$
126	$ab + acd + bce$	171	$abc + ade$
127	$ab + acd + bce + cde$	172	$abc + ade + bcde$
128	$ab + acd + cde$	173	$abc + abde$
129	$ab + acd + bcde$	174	$abc + abde + acde$
130	$ab + cde$	175	$abc + abde + acde + bcde$
131	$ab + acde$	176	$abcd + abce$
132	$ab + acde + bcde$	177	$abcd + abce + abde$
133	$abc + abd + acd + bcd + abe$	178	$abcd + abce + abde + acde$
134	$abc + abd + acd + bcd + abe + ace$	179	$abcd + abce + abde + acde + bcde$
135	$abc + abd + acd + bcd + abe + ace + bce$	180	$abcde$