社団法人 情報処理学会 研究報告
IPSJ SIG Technical Reports

2008－CSEC－42（26）
2008 / 7 / 25

一般秘匿性ポリシの束モデル

櫻庭 健年† 櫻井 幸一††

† 日立製作所システム開発研究所
215-0013 神奈川県川崎市麻生区王禅寺 1099
†† 九州大学大学院システム情報科学研究院
819-0395 福岡県福岡市西区元岡 744
E-mail: †taketoshi.sakuraba.hc@hitachi.com, ††sakurai@csce.kyushu-u.ac.jp

あらまし 情報フローポリシに基づくアクセス制御では，あらかじめ定められたセキュリティクラスの間のフロールールに従って，アクセスの可否を決定する．従来行われてきた，固定したセキュリティクラスによる情報フローポリシーは動的に秘匿情報が生じたり，秘匿範囲が頻繁に変わるような環境に適合しない．秘匿情報の属性を既存のセキュリティクラスに合わせて定めるのではなく，秘匿情報の実態に合わせてセキュリティクラスの構成を動的に変化させる必要がある．そこで，本論文では，与えた秘匿情報の属性の集大成である秘匿性ポリシに対して，適切な情報フロールールを動的に決定する方法を提案する．秘匿性ポリシの意味論によって，その妥当性を説明し，その諸性質を数学的に厳密に証明する．提案方法によって，束ベースの情報フローポリシが構成できるが，さらにその小型化を試みる．情報フローポリシを秘匿性ポリシとして解釈することができ，その場合は，情報フローポリシに対する Denning の束モデル [1] と同じ束モデルが得られる．

キーワード 情報フローポリシ，秘匿性ポリシ，アクセス制御，束モデル，ガロアコネクション

The Lattice Model of the Generalized Confidentiality Policy

Taketoshi SAKURABA† and Kouichi SAKURAI††

† Systems Development Laboratory, Hitachi, Ltd.
1099 Ohzenji, Asao-ku, Kawasaki, Kanagawa, 215-0013 Japan
†† Faculty of Information Science and Electrical Engineering, Kyushu University
744 Motooka, Nishi-ku, Fukuoka, Fukuoka, 819-0395 Japan
E-mail: †taketoshi.sakuraba.hc@hitachi.com, ††sakurai@csce.kyushu-u.ac.jp

Abstract An information flow policy is defined as a set of information flow rules among security-classes. Implementations of such flow control systems usually adopt fixed structures of security-classes such as multilevel security. In an environment in which secrets are dynamically generated, and permissions are frequently changed, such fixed structure however does not work. We need to change the structure dynamically based on attributes of confidential information but not to adjust the secrets to fixed security-classes. This paper proposes a method that derives an information flow rule from confidentiality policy, a set of attributes of all secrets. The adequacy of the method is explained by semantics of secrets, and its properties are proved in a mathematical manner. The proposed method provides a lattice-based flow rules. We try to reduce the size of the lattice. Also, we show that any information flow policies can be interpreted as a confidentiality policy, and that the lattice derived by Denning [1] from the information flow policy is same with the lattice derived from the interpreted confidentiality policy.

Key words Information Flow Policy, Confidentiality Policy, Access Control, Lattice Model, Galois Connection

1. はじめに

情報フロー制御ポリシに基づくアクセス制御は，秘匿性 [2] や完全性 [3] 等を目的として，昔から行われている．本論文は，秘匿性を目的とする情報フロー制御を対象としている．情報フロー制御では，情報の読み出しや書き込みによって生じる情報

の移動を情報フローととらえる．情報フローを許可したり，拒否したりすることにより，特定の主体や対象に，特定のの情報が渡らないようにすることができる．秘匿性を目的とする場合は，それによって，秘匿情報の開示を制限する．情報フローポリシの実装では，あらかじめセキュリティクラスを定め，それらの間の情報フロールールとしてポリシを表現する．また，システムの各エンティティ（ユーザやファイルなど）がどのセキュリティクラスに該当するかを定めておく．これはエンティティをあらかじめ分類しておくことと同等である．その上で，それらの間に発生した情報フロー要求を，対応するセキュリティクラス間の情報フロールールに従うように制御する．セキュリティクラスは，相当期間固定であり，新たなエンティティは，どのセキュリティクラスに該当するかを定めることにより，保護システムに組み込まれる．

このようなセキュリティポリシの問題点の一つは，秘匿情報が新たに発生したとき，その情報の開示先，あるいは秘匿先をあらかじめ与えられているセキュリティクラスの中から選択しなければならないことである．例えば，多階層セキュリティ[4]では，Unclassified，Confidential，Secret，Top Secret のいずれかに当てはめなければならない．しかし，このような固定されたセキュリティクラスによる情報フローポリシは，秘匿情報がダイナミックに発生し，またその秘匿範囲が頻繁に変化するような環境には適合していない．例えば，今，ある報告書の内容を秘匿することを決定したとする．秘匿するからには，秘匿の対象となるユーザ，あるいは開示しても良いユーザがあるはずである．秘匿対象としたいユーザの集合が，あるセキュリティクラスに丁度該当するならば，そのセキュリティクラスに情報が流入するようなところに，そのレポートを置かないようにすれば良い．しかし，一般には，これらが一致するとは限らない．極端な場合，秘匿したい相手と開示したい相手が，同じセキュリティクラスに同居しているならば，現在あるセキュリティクラスを用いて，意図通りのポリシを実現することはできない．また，例えば，あるユーザに，このレポートへのアクセスを許すことになったとする．これを実現するために，このユーザを別のセキュリティクラスを移したりすると，他のポリシに違反するなどの，副作用が避けられない．

上記の問題を解決するには，発生する秘匿情報の属性に合わせて，セキュリティクラスの構成を変更し，同時に，ユーザやファイルに対応させるセキュリティクラスを設定しなおす必要がある．セキュリティクラスの再構成は，グローバルな作業である．すなわち，全ての秘匿情報を考慮する必要がある．一方，そのために使用する情報は，ダイナミックな秘匿情報の発生を前提とすると，新たに秘匿情報を定義するユーザによって指定可能なものでなければならない．このようなユーザは，新たに定義する秘匿情報に関する情報，いわばローカルな情報しか持っていないと考えられる．本論文では，各秘匿情報について，それを誰に対して秘匿するか，あるいは誰に対して開示できるか，がわかる情報が利用可能であると仮定する．このような情報は，情報を秘匿しようとするユーザにとっては明らかなことであり，妥当な仮定であると考えられる．このような，秘匿情報とその開示先に関する情報の集合として与えられたポリシを秘匿性ポリシと呼ぶことにする．

本論文では，秘匿性ポリシから，その秘匿要件を満たす情報フローポリシの構成方法を提案する．情報フローポリシについては，Denning による束フローポリシモデルが良く知られている[5]．束フローポリシとは，セキュリティクラスが情報フロー関係によって束構造[6]をなす情報フローポリシのことである．束フローポリシを用いると，情報フローの監視が容易になることがある[7]．提案方式によっても，束フローポリシが得られることを示す．また，情報フローポリシを秘匿性ポリシとして解釈するとき，提案方法によって構成される束フローポリシと，Denning が情報フローポリシから導いた束フローポリシ[1]が同等となることを，Galois Connection[6]の理論を用いて証明する．さらに，一般の秘匿性ポリシについては，提案方法による束構造は縮小可能であることを指摘し，縮小方法を提案する．

2. 情報フローポリシ

情報フローポリシとは，主体と対象をセキュリティクラスに分類し，各クラス間の情報フローを制限することにより，特定の情報が，特定の主体や対象にアクセスされないように定めた，アクセス制御ルールである．情報フローポリシ（Information Flow Policy）は，次のように，$FP = (S, O, SC, \psi, \rightarrow)$ としてモデル化される．

S： 主体の集合．主体とは，能動的にアクセスする実体であり，通常，ユーザやプロセスなどを指す．

O： 対象の集合．対象とは，アクセスにおいて受動的な実体であり，通常，ファイルや変数などを指す．

SC： セキュリティクラスの集合．主体および対象をセキュリティの観点から分類したときの類別の全体．

ψ： セキュリティクラス写像．$S \cup O \longrightarrow SC$．主体および対象がどのセキュリティクラスに分類されるかを示す．

$\rightarrow$： 情報フロー関係．SC 上の反射的(注2)かつ推移的(注3)な2項関係．$A, B \in S \cup O$ に対し，$\psi(A) \rightarrow \psi(B)$ とは，A から B への情報フローが許されることを意味する．

情報フローポリシ $FP = (S, O, SC, \psi, \rightarrow)$ がセキュアであるとは，主体や対象の間に，$\rightarrow$ に反する情報フローが発生し得ないことをいう．

情報フロー関係 $\rightarrow$ が擬順序であること，すなわち反射的かつ推移的であることは，情報フローとして自然である．なお，業務順序を規定したワークフローのような場合には $a \rightarrow b$ かつ $b \rightarrow c$ であっても，a から c への直接のフローを禁ずることがあるが，ここでは，情報漏洩の可能性の分析に特化し，$a \rightarrow c$ が従うものとする．

2つの情報フローポリシ $FP = (S, O, SC, \psi, \rightarrow)$ と $FP' = (S, O, SC', \psi', \rightarrow')$ が同等であるとは，両者が情報フローの可否について同じ判断を下すこと，すなわち任意の $A, B \in S \cup O$ について，$\psi(A) \rightarrow \psi(B) \Leftrightarrow \psi'(A) \rightarrow' \psi'(B)$ を満たすこと

(注2)：$a \rightarrow a$

(注3)：$(a \rightarrow b \text{ and } b \rightarrow c) \Rightarrow a \rightarrow c$

をいう．

情報フローポリシが半順序フローポリシであるとは，SC が半順序集合となること，すなわち情報フロー関係 $\rightarrow$ が，さらに反対称的[注4] であることをいう．また，半順序フローポリシが束フローポリシであるとは，SC が束をなすこと，すなわち SC の任意の2元 a,b に，$\rightarrow$ に関する上限 $a \vee b$ [注5] と下限 $a \wedge b$ が存在することをいう．

束フローポリシに従うと，情報フローのセキュリティ監視が容易になる[7]．例えば，$x_1 \rightarrow y, \ldots, x_n \rightarrow y$ なるフローの可否を検証するとき，上限 $x = x_1 \vee \ldots \vee x_n$ を用いて，単独の $x \rightarrow y$ の可否を検証すればよい．$x \rightarrow y_1 \ldots, x \rightarrow y_n$ の検証についても同様である．

3. 秘匿性ポリシの束モデル

3.1 秘匿性ポリシ

秘匿性ポリシ（confidentiality policy）とは，保護対象とする秘匿情報を定義し，各秘匿情報について，組織内のどのエンティティのアクセスを許すか，許さないかを定めたルールである．秘匿性ポリシを，次のように CP = (D, E, P) としてモデル化する．

D： 秘匿情報集合．保護対象とする秘匿情報の集合．

E： エンティティ集合．エンティティとは情報にアクセスする実体をいう．

P： 秘匿性関係．D と E の上の2項関係．$P \subseteqq D \times E$ である．$(d,\alpha) \in P$ は，α は d にアクセスしてよいことを意味する．

アクセス制御における通常の取り扱いでは，主体の集合 S と対象の集合 O を定め，情報へのアクセスは，情報を格納した対象へのアクセスによって間接的に表現するが，ここでは，情報と対象を区別している．情報を流れる水にたとえれば，主体や対象は，水路に相当する．

エンティティとは，主体や対象に該当する．主体による秘匿情報へのアクセスとは，主体がその情報を知ることであり，ユーザによる情報の読み出しなどが該当する．$S \subseteqq E$ である．

また，対象にその情報を格納することを，対象による秘匿情報へのアクセスと考える．ファイルへの書き込みや変数への代入などが該当する．この場合は，$O \subseteqq E$ である．このようにすると，Bell-LaPadula モデルの $*$-条件のような，秘匿情報のファイルへの格納ルールを導くことができるようになる．

一方，秘匿性ポリシとして，ファイルへの格納ルールを，あらかじめ与えるのが困難な場合が考えられる．その場合は，エンティティに対象を含めずに，以下を展開してもよい．

以上により，$E = S$ または $E = S \cup O$ と考えてよい．これらのケースをまとめて記述するため，これらを総称する概念としてエンティティということばを用いる．

秘匿性ポリシ CP = (D, E, P) がセキュアであるとは，主体や対象の間に，P に反するアクセスが発生し得ないことをいう．

表 1 秘匿性ポリシ集合の例

		D					$C(\cdot)$
		a	b	c	d	e	
E	α	○	○			○	abe
	β	○	○				bc
	γ	○		○	○	○	$acde$
	δ			○	○		cd
$A(\cdot)$		$\alpha\beta\gamma$	$\alpha\beta$	$\gamma\delta$	$\gamma\delta$	$\alpha\gamma$	

$D \times E$ は，一種のアクセス制御行列[8] である．ただし，D の元は対象ではなく，秘匿情報である点が通常のアクセス制御行列と異なる．その部分集合 P は，秘匿性ポリシの本体であり，アクセス制御の内容を表現する．P をポリシ集合と呼ぶ．$P \subseteqq D \times E$ をアクセス制御行列と考えると，次を定義するのは自然である．

定義 1. 写像 $A : D \longrightarrow 2^E$，および $C : E \longrightarrow 2^D$ を次のように定義する．

$$A(d) = \{\alpha \in E \mid (d,\alpha) \in P\} \quad (1)$$

$$C(\alpha) = \{d \in D \mid (d,\alpha) \in P\} \quad (2)$$

$A(d)$ は，秘匿情報 d の ACL（access control list）に相当する．そこで，写像 A を ACL 写像と呼ぶ．同様に $C(\alpha)$ は，エンティティ α のケーパビリティリスト（capability list, C-list）とみることができる．写像 C をケーパビリティ写像と呼ぶ．

ACL 写像 A，ケーパビリティ写像 C，およびポリシ集合 P には次の関係がある．

$$\alpha \in A(d) \;\Leftrightarrow\; d \in C(\alpha) \;\Leftrightarrow\; (d,\alpha) \in P \quad (3)$$

表1に，ポリシ集合の一例を示した．縦軸にエンティティ，横軸に秘匿情報が並んでいる．$E = \{\alpha,\beta,\gamma,\delta\}$，$D = \{a,b,c,d,e\}$ である．右端の列には，各エンティティのケーパビリティリストが並んでいる．たとえば，$C(\alpha) = \{a,b,e\}$ を abe のように略記している．また最下段の行には各秘匿情報のアクセス制御リストが並んでいる．同様に，たとえば $\alpha\gamma$ は，$\{\alpha,\gamma\}$ の略記である．表中，「○」のあるエントリが，ポリシ集合 P の元であることを表している．

3.2 秘匿性ポリシの情報フローモデル

本節では，与えられた秘匿性ポリシ CP = (D, E, P) から，情報フローポリシ FP_0 を導く．ただし，S を主体の集合，O を対象の集合とし，$E = S \cup O$ とする．

前節のように，$C(\alpha)$ をエンティティ α のケーパビリティリストと解釈すると，$C(\alpha) \subseteqq C(\beta)$ とは，α にアクセスが許された情報は β にもアクセスが許されることを表していると考えられる．したがって α から β への情報フローは，β がアクセスしてはならない情報を β にもたらすことはない，という意味でセキュアである．したがって α から β への情報フローが許される．以上を踏まえて，以下を定義する．

定義 2. 情報フロー関係 $\rightarrow$ を，ケーパビリティの包含関係に

(注4)：$(a \rightarrow b \text{ and } b \rightarrow a) \Rightarrow a = b$

(注5)：$a \rightarrow a \vee b \text{ and } b \rightarrow a \vee b \text{ and } \forall x((a \rightarrow x \text{ and } b \rightarrow x) \Rightarrow a \vee b \rightarrow x)$

よって定義する。

$$\alpha \to \beta \;\Leftrightarrow\; C(\alpha) \subseteqq C(\beta) \tag{4}$$

この情報フロー関係は明らかに反射的かつ推移的であるが，必ずしも反対称的ではないため，半順序とは限らない．そこで，反対称性を導入するために，E に同値関係 $\sim$ を $\alpha \sim \beta \;\Leftrightarrow\; \alpha \to \beta$ and $\beta \to \alpha$ と定めると，定義 2 により，$\alpha \sim \beta \;\Leftrightarrow\; C(\alpha) = C(\beta)$ である．したがって，$\sim$ による α の同値類は，$C(\alpha)$ と同一視できる．そこで，次を定める．

定義 3. ケーパビリティリストの全体を F とする．

$$\mathrm{F} = \mathrm{Im}C = \{C(\alpha) \mid \alpha \in \mathrm{E}\} \tag{5}$$

情報フロー関係 $\to$ は F 上の包含関係として自然に継承される．$(\mathrm{F}, \to)$ は半順序集合となる．

定理 1. $\mathrm{FP}_0 = (\mathrm{S}, \mathrm{O}, \mathrm{F}, C, \to)$ は秘匿性ポリシ $\mathrm{CP} = (\mathrm{D}, \mathrm{E}, \mathrm{P})$ と同等な，半順序フローポリシとなる．

F は，組織内にあるケーパビリティリストの全体である．FP_0 は，ケーパビリティリストそのものをセキュリティクラスとした情報フローポリシとなっている．

3.3 秘匿性ポリシの束モデル

本節では，与えられた秘匿性ポリシ $\mathrm{CP} = (\mathrm{D}, \mathrm{E}, \mathrm{P})$ から，束構造 AL，CL および BL を構成し，上記の半順序集合 F が，それらに埋め込めることを示す．

3.3.1 束構造 AL と CL の構成

前記のように，$A(d)$ を d の ACL と考えることができる．あるエンティティが，$A(a)$ と $A(b)$ の両方に属するということは，秘匿情報 a と b の双方にアクセスすることができることを意味し，$A(a)$ あるいは $A(b)$ のいずれか一方のみに属するエンティティと較べて，秘匿性に関し，より大きい権限を持っていると考えられる．この状況を $A(a) \subseteqq A(a) \cap A(b)$，$A(b) \subseteqq A(a) \cap A(b)$ と表すことが考えられる．以上を踏まえて，次を定義する．

定義 4. 写像 $\hat{\mathrm{A}} : 2^{\mathrm{D}} \longrightarrow 2^{\mathrm{E}}$，集合 AL，および AL 上の順序関係 $\leqq$ を次のように定義する．

$$\hat{\mathrm{A}}(S) = \bigcap_{d \in S} A(d) \tag{6}$$

$$\mathrm{AL} = \mathrm{Im}\hat{\mathrm{A}} = \{\hat{\mathrm{A}}(S) \mid S \subseteqq \mathrm{D}\} \subseteqq 2^{\mathrm{E}} \tag{7}$$

$$X \leqq Y \;\Leftrightarrow\; X \supseteqq Y \quad (X, Y \in \mathrm{AL}) \tag{8}$$

AL は集合の包含関係により，半順序集合となるが，AL の順序 $\leqq$ は，上記の考察に基づき，その双対として定義している．

次に，C を用いて，次のように定義する．

定義 5. 写像 $\tilde{\mathrm{C}} : 2^{\mathrm{E}} \longrightarrow 2^{\mathrm{D}}$，集合 CL，および CL 上の順序関係 $\leqq$ を次のように定義する．

$$\tilde{\mathrm{C}}(M) = \bigcup_{\alpha \in M} C(\alpha) \tag{9}$$

$$\mathrm{CL} = \mathrm{Im}\tilde{\mathrm{C}} = \{\tilde{\mathrm{C}}(M) \mid M \subseteqq \mathrm{E}\} \subseteqq 2^{\mathrm{D}} \tag{10}$$

$$U \leqq V \;\Leftrightarrow\; U \subseteqq V \quad (U, V \in \mathrm{CL}) \tag{11}$$

CL は集合の包含関係により，半順序集合となり，CL の順序 $\leqq$ はそれと一致するように定義する．

AL および CL は完備束になる．これを示すために，次の補題を用意する．

補題 1. $S \subseteqq \mathrm{D}$，および $M \subseteqq \mathrm{E}$ について，次が成り立つ．

$$\hat{\mathrm{A}}(S) = \{\alpha \in \mathrm{E} \mid S \subseteqq C(\alpha)\} \tag{12}$$

$$\tilde{\mathrm{C}}(M) = \{d \in \mathrm{D} \mid M \cap A(d) \neq \emptyset\} \tag{13}$$

したがって，特に，$\hat{\mathrm{A}}(\emptyset) = \mathrm{E}$，$\tilde{\mathrm{C}}(\emptyset) = \emptyset$ である．

証明. 関係 (3) に注意して，定義を書き換える．

$$\begin{aligned}
\alpha \in \hat{\mathrm{A}}(S) &\;\Leftrightarrow\; \forall d \in S(\alpha \in A(d)) \\
&\;\Leftrightarrow\; \forall d(d \in S \Rightarrow d \in C(\alpha)) \\
&\;\Leftrightarrow\; S \subseteqq C(\alpha) \\
d \in \tilde{\mathrm{C}}(M) &\;\Leftrightarrow\; \exists \alpha \in M(d \in C(\alpha)) \\
&\;\Leftrightarrow\; \exists \alpha(\alpha \in M \text{ and } \alpha \in A(d)) \\
&\;\Leftrightarrow\; M \cap A(d) \neq \emptyset
\end{aligned}$$

□

補題 2. $\mathcal{W} \subseteqq 2^{\mathrm{D}}$，$\mathcal{Z} \subseteqq 2^{\mathrm{E}}$ について，次が成り立つ．

$$\bigcap_{S \in \mathcal{W}} \hat{\mathrm{A}}(S) = \hat{\mathrm{A}}\left(\bigcup_{S \in \mathcal{W}} S\right) \tag{14}$$

$$\bigcup_{M \in \mathcal{Z}} \tilde{\mathrm{C}}(M) = \tilde{\mathrm{C}}\left(\bigcup_{M \in \mathcal{Z}} M\right) \tag{15}$$

証明. 補題 1 により，

$$\begin{aligned}
\alpha \in \bigcap_{S \in \mathcal{W}} \hat{\mathrm{A}}(S) &\;\Leftrightarrow\; \forall S \in \mathcal{W}(\alpha \in \hat{\mathrm{A}}(S)) \\
&\;\Leftrightarrow\; \forall S \in \mathcal{W}(S \subseteqq C(\alpha)) \\
&\;\Leftrightarrow\; \bigcup_{S \in \mathcal{W}} S \subseteqq C(\alpha) \\
&\;\Leftrightarrow\; \alpha \in \hat{\mathrm{A}}\left(\bigcup_{S \in \mathcal{W}} S\right) \\
d \in \bigcup_{M \in \mathcal{Z}} \tilde{\mathrm{C}}(M) &\;\Leftrightarrow\; \exists M \in \mathcal{Z}(d \in \tilde{\mathrm{C}}(M)) \\
&\;\Leftrightarrow\; \exists M \in \mathcal{Z}(M \cap A(d) \neq \emptyset) \\
&\;\Leftrightarrow\; \bigcup_{M \in \mathcal{Z}}(M \cap A(d)) \neq \emptyset \\
&\;=\; \left(\bigcup_{M \in \mathcal{Z}} M\right) \cap A(d) \neq \emptyset \\
&\;\Leftrightarrow\; d \in \tilde{\mathrm{C}}\left(\bigcup_{M \in \mathcal{Z}} M\right)
\end{aligned}$$

□

補題 3. $\mathcal{Z} \subseteqq \mathrm{AL}$ の AL における上限，および下限は次のように与えられる．したがって AL は完備束をなす．

$$\bigvee \mathcal{Z} = \bigcap_{X \in \mathcal{Z}} X \tag{16}$$

$$\bigwedge \mathcal{Z} = \bigvee\{Z \in \mathrm{AL} \mid \forall X \in \mathcal{Z}(Z \leqq X)\} \tag{17}$$

CL についても，$\mathcal{W} \subseteqq \mathrm{CL}$ の上限，および下限は次のように表され，CL は完備束となる．

$$\bigvee \mathcal{W} = \bigcup_{U \in \mathcal{W}} U \tag{18}$$

$$\bigwedge \mathcal{W} = \bigvee\{W \in \mathrm{CL} \mid \forall U \in \mathcal{W}(W \leqq U)\} \tag{19}$$

証明. 2^{E} の双対における $\mathcal{Z}$ の上限は $\bigcap_{X \in \mathcal{Z}} X$ である．補題 2 (14) により，AL は，その部分集合の元（クラス）の共通部分をとる操作について閉じているから，$\bigcap_{X \in \mathcal{Z}} X \in \mathrm{AL}$ であ

り，ALにおける $\mathcal{Z}$ の上限と一致する．したがってALは上限演算について完備である．このとき，一般に，$\mathcal{Z}$ の下限は，上記(17)のように与えられる．同様に，補題2(15)により，CLは任意の元の和集合について閉じており，完備束となる． □

ポリシ集合Pに対して上記のように構成した束構造ALを，Pに関する A 束と呼び，AL(P)，あるいは単にALと書く(注6)．同様にCLをPに関する C 束と呼び，CL(P)，あるいはCLと書く．ALやCLの元は，元であると同時に，それ自身が集合である．言葉の混乱を避けるため，これらをクラスと呼ぶことにする．後に見るように，これらはセキュリティクラスに該当するからである．例えば，「ALのクラス」とは「ALの元」のことである．

3.3.2 束フローモデルの構成

これまで定義した主要な写像を整理しておく．

$$\mathrm{E} \xrightarrow{C} \mathrm{F} = \mathrm{Im}C \subseteqq \mathrm{Im}\widetilde{\mathrm{C}} = \mathrm{CL} \subseteqq 2^{\mathrm{D}} \xrightarrow{\widehat{\mathrm{A}}} \mathrm{AL} \subseteqq (2^{\mathrm{E}})^{\circ}$$

ここで，$(2^{\mathrm{E}})^{\circ}$ は，包含関係による束 2^{E} の双対，すなわち順序を逆にした束を表している．この順序について，$\widehat{\mathrm{A}}$ は順序を保つ．

直ちにわかるように，半順序集合Fは，束CLに順序関係も含めて埋め込まれている．従って，次がいえる．

定理 2. $\mathrm{FP}_C = (\mathrm{S}, \mathrm{O}, \mathrm{CL}, C, \leq)$ は，半順序フローポリシ $\mathrm{FP}_0 = (\mathrm{S}, \mathrm{O}, \mathrm{F}, C, \rightarrow)$ と同等の束フローポリシとなる．

次に束ALについて考える．$\widehat{\mathrm{A}}$ の定義域をCLに制限して，$\widehat{\mathrm{A}}$ を $\mathrm{CL} \longrightarrow \mathrm{AL}$ なる写像とみなすことができる．このとき，$\widehat{\mathrm{A}}|_{\mathrm{CL}}$ は単射，あるいは全射とは限らない．しかし，さらにFに制限すれば，単射となる．

補題 4. $\widehat{\mathrm{A}}|_{\mathrm{F}} : \mathrm{F} \longrightarrow \mathrm{AL}$ は順序を保った埋め込みになっている．

証明. $\widehat{\mathrm{A}}(C(\alpha)) = \widehat{\mathrm{A}}(C(\beta))$ を仮定して，$C(\alpha) = C(\beta)$ を示す．補題1 (12) により，$\alpha \in \widehat{\mathrm{A}}(C(\beta)) \Leftrightarrow C(\beta) \subseteqq C(\alpha)$ であるから，特に $\alpha \in \widehat{\mathrm{A}}(C(\alpha))$ である．$\widehat{\mathrm{A}}(C(\alpha)) = \widehat{\mathrm{A}}(C(\beta))$ とすると，$\alpha \in \widehat{\mathrm{A}}(C(\beta))$ かつ $\beta \in \widehat{\mathrm{A}}(C(\alpha))$．したがって，補題1 (12) により，$C(\alpha) \subseteqq C(\beta)$ かつ $C(\beta) \subseteqq C(\alpha)$．よって，$C(\alpha) = C(\beta)$． □

よって，Fは $\widehat{\mathrm{A}}$ により，束ALに順序関係も含めて埋め込むことができる．したがって，次が示された．

定理 3. $\mathrm{FP}_A = (\mathrm{S}, \mathrm{O}, \mathrm{AL}, \widehat{\mathrm{A}} \circ C, \leq)$ は，半順序フローポリシ $\mathrm{FP}_0 = (\mathrm{S}, \mathrm{O}, \mathrm{F}, C, \rightarrow)$ と同等の束フローポリシとなる．

3.3.3 束構造ALとCLの最適化

Fを束に埋め込めることを示すだけならば，$\mathrm{F} \subseteqq 2^{\mathrm{D}}$ とすれば十分である．以上では，Fを，より小さな束構造AL，CLに埋め込めることを示したことに注意されたい．本節では，ALとCLから，それらよりさらに小さな束BLを構成する．

(注6)：A 束は，著者の一人が以前に構成した束構造[9]と同じものである．

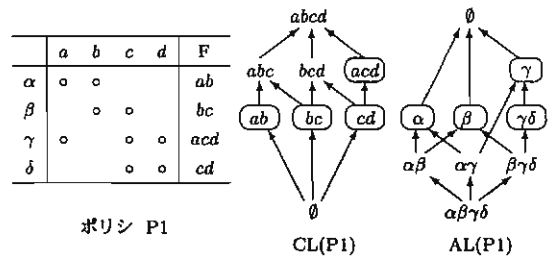

図1 余分なクラスが発生したCLとALの例

束フローポリシを実際に運用する場合，メモリ領域やサーチ処理の効率の観点から，束構造は小さい方が好ましい．しかし，ALやCLがFを埋め込むのに必要最小限の大きさであるとは限らない．実際，CLは，Fの元の全ての組み合わせについて，その合併を加えることによって，束になっている．そのため，余分な和集合がクラスとして発生することがある．同様に，ALは，$A(d)$ の形の集合のすべての組み合わせについて，共通部分を付け加えることによって，束となるようにしているそのため，余分な共通部分集合をクラスとして付け加えているおそれがある．

図1は，秘匿性ポリシP1と，それに対するCL(P1)およびAL(P1)を示している．図の中の ab，α，$\alpha\beta$ などは，それぞれクラス $\{a,b\}$，$\{\alpha\}$，$\{\alpha,\beta\}$ の略記である．束構造はハッセ図として表されている．すなわち，直接の順序関係についてのみ矢印が明示されており，推移性による間接的な，例えば $\beta\gamma\delta$ から γ への矢印は，表示されていない．ポリシP1の半順序フローポリシF(P1)は $\{ab, bc, acd, cd\}$ である．CL(P1)の中の長円で囲まれたクラスは，CL(P1)に埋め込まれたF(P1)を示している．同様に，AL(P1)に埋め込まれたF(P1)も，長円によって示されている．図は，2つの束におけるF(P1)が対応するように書かれている．すなわち，$\widehat{\mathrm{A}}(ab) = \alpha$，$\widehat{\mathrm{A}}(bc) = \beta$，$\widehat{\mathrm{A}}(cd) = \gamma\delta$，$\widehat{\mathrm{A}}(acd) = \gamma$ となっている．これら次のようにしてポリシP1の表から求めることができる．例えば，$\widehat{\mathrm{A}}(ab) = A(a) \cap A(b)$ である．$A(a)$，および $A(b)$ は，表の a の列と b の列である．2つの列に共通に ∘ が付いているのは α の欄だけである．よって，$\widehat{\mathrm{A}}(ab) = \alpha$ となる．

この例の場合，F(P1)に $abcd$ と $\emptyset$ を付加するだけで，束になる．従って，CL(P1)の abc，bcd は不要であり，余分なクラスが発生していることがわかる．同様にAL(P1)の $\alpha\beta$，$\alpha\gamma$，$\beta\gamma\delta$ も余分なクラスである．

以下では，Fを埋め込んだまま，ALおよびCLから余分なクラスを削除してできる束構造BLを構成する．

定義 6. BLを，$\widehat{\mathrm{A}}$ によるCLの像とする．

$$\mathrm{BL} = \mathrm{Im}(\widehat{\mathrm{A}}|_{\mathrm{CL}}) = \{\widehat{\mathrm{A}}(U) \mid U \in \mathrm{CL}\} \tag{20}$$

BLでは，$\widehat{\mathrm{A}}(U) = \widehat{\mathrm{A}}(V)$ となるような $U, V \in \mathrm{CL}$ は同一視したことになる．また，$\widehat{\mathrm{A}}$ の像に入らないALの元はBLに含まれない．したがって，$\widehat{\mathrm{A}}$ が単射でなければ，BLはCLより小さく，全射でなければ，ALより小さくなる．一方，FはCL，ALのどちらにも埋め込まれており，したがってBLにも

F が埋め込まれている．さらに，BL は，以下に示すように束となる．

補題 5. $\widehat{\mathrm{A}}|_{\mathrm{CL}} : \mathrm{CL} \longrightarrow \mathrm{AL}$，$\mathcal{W} \subseteqq \mathrm{CL}$ について，

$$\widehat{\mathrm{A}}\left(\bigvee_{U\in\mathcal{W}} U\right) = \bigvee_{U\in\mathcal{W}} \widehat{\mathrm{A}}(U) \tag{21}$$

$$\widehat{\mathrm{A}}\left(\bigwedge_{U\in\mathcal{W}} U\right) \leqq \bigwedge_{U\in\mathcal{W}} \widehat{\mathrm{A}}(U) \tag{22}$$

証明. (21) は，補題 2 (14) による．それゆえ，$\widehat{\mathrm{A}}$ は順序を保つ．(22) は，順序を保つ写像について一般に成り立つ． □

補題 6. BL は完備束をなす．

証明. $\mathcal{Z} \subseteqq \mathrm{BL}$ について，$\mathcal{W} = \widehat{\mathrm{A}}^{-1}(\mathcal{Z})$ とおくと，$\mathcal{Z} = \{\widehat{\mathrm{A}}(U) \mid U \in \mathcal{W}\}$ である．補題 5 により，$\bigvee\mathcal{Z} = \bigvee_{U\in\mathcal{W}} \widehat{\mathrm{A}}(U) = \widehat{\mathrm{A}}\left(\bigvee_{U\in\mathcal{W}} U\right) \in \mathrm{BL}$ よって，BL は，任意の部分集合の上限をとる操作について閉じている．したがって，補題 3 と同様にして，下限についても閉じている． □

以上により，次が示された．

定理 4. $\mathrm{FP}_{\mathrm{BL}} = (\mathrm{S}, \mathrm{O}, \mathrm{BL}, \widehat{\mathrm{A}} \circ C, \leqq)$ は，半順序フローポリシ $\mathrm{FP}_0 = (\mathrm{S}, \mathrm{O}, \mathrm{F}, C, \rightarrow)$ と同等の束フローポリシとなる．BL の大きさ（濃度）は，AL，CL の大きさ以下である．

図 1 の例では，$\widehat{\mathrm{A}}(abc) = \widehat{\mathrm{A}}(bcd) = \widehat{\mathrm{A}}(abcd) = \emptyset$ となっており，余分なクラス abc，bcd は $abcd$ に吸収される．また，$\alpha\beta$，$\alpha\gamma$ および $\beta\gamma\delta$ は，$\widehat{\mathrm{A}}$ の像に含まれない．その結果 $\mathrm{BL} = \{\emptyset, \alpha, \beta, \gamma, \gamma\delta, \alpha\beta\gamma\delta\}$ となり，F を含む，最小の束となっている．このほか，小規模な実験をいくつか試みた限りでは，最小の束が BL として得られた．しかし，これが一般に成り立つかどうかは，残念ながらわかっていない．

未解決問題 一般の P について，BL(P) は，F(P) を埋め込める最小の束か？

4. 情報フローポリシへの適用

情報フローポリシも秘匿性ポリシの一形態である．本節では，両者の関係について述べる．

4.1 情報フローポリシの秘匿性ポリシとしての解釈

本項では情報フローポリシを秘匿性ポリシとして解釈する方法を示す．

$\mathrm{FP} = (\mathrm{S}, \mathrm{O}, \mathrm{SC}, \psi, \rightarrow)$ を情報フローポリシとする．以下では，これと同等の秘匿性ポリシ $\mathrm{CP} = (\mathrm{D}, \mathrm{E}, \mathrm{P})$ を構成する．

まず，E については，$\mathrm{E} = \mathrm{S} \cup \mathrm{O}$ である．一方，D については，具体的な秘匿情報はないが，秘匿情報の E への開示パターンを考え，それを秘匿情報とみなすことができる．例えば，ある秘匿情報をエンティティ α に開示すると，この情報は，情報フロー関係 $\rightarrow$ によって，他のエンティティにも開示されることになる．このようにして，実際に開示先となるエンティティを集めたものが一つの開示パターンである．与えられた情報フローポリシのもとで発生しうるすべての開示パターンを列挙する．相異なる開示パターンについて，それらを開示先とする秘匿情報がそれぞれ存在する，と仮定して D の元とする．

$\alpha \in \mathrm{E}$ がアクセスできる秘匿情報は，$\psi(\alpha) \in \mathrm{SC}$ で決まる．従って，秘匿情報の開示先を列挙するには，SC の部分集合を考えておけばよい．秘匿情報を $M \subseteqq \mathrm{SC}$ に開示すると，実際に開示先となるのは M の $\rightarrow$ に関する推移的閉包である．開示パターンはすべて，このような推移的閉包 (transitive closure) である．これを $\mathrm{TC}(M)$ と書くと，$M \subseteqq \mathrm{SC}$ について $\mathrm{TC}(M) = \bigcup_{X\in M} \mathrm{TC}(\{X\})$ である．従って，各 $X \in \mathrm{SC}$ に関する開示パターン $\mathrm{TC}(\{X\})$ があれば，$\mathrm{TC}(M)$ を構成でき，情報フローポリシに関する情報は十分である．さらに，$\mathrm{TC}(\{X\})$ は $X \in \mathrm{SC}$ と 1 対 1 に対応するから，D は SC とみなしてよい．このとき，ポリシ集合 P は，$\mathrm{P} = \{(X, \alpha) \mid X \in \mathrm{SC}, \alpha \in \mathrm{S} \cup \mathrm{O}, X \rightarrow \psi(\alpha)\}$ となる．

以上により，秘匿性ポリシ $\mathrm{CP} = (\mathrm{SC}, \mathrm{S} \cup \mathrm{O}, P)$ が得られた．しかし，その束フローポリシを構成する場合には，$\psi(\alpha) = \psi(\beta)$ となる α と β を区別する必要はない．すなわち，$\mathrm{E} = \mathrm{SC}$ として良く，このとき P は $\rightarrow$ に一致し，秘匿性ポリシは $\mathrm{CP} = (\mathrm{SC}, \mathrm{SC}, \rightarrow)$ となる．

以上の議論をまとめておく．二つの秘匿性ポリシが同じ束構造を導くとき，相似であるということにする．

定理 5. 情報フローポリシ $\mathrm{FP} = (\mathrm{S}, \mathrm{O}, \mathrm{SC}, \psi, \rightarrow)$ を秘匿性ポリシ $\mathrm{CP}(\mathrm{FP}) = (\mathrm{SC}, \mathrm{S} \cup \mathrm{O}, \mathrm{P})$ として自然に解釈することができ，$\mathrm{CP} = (\mathrm{SC}, \mathrm{SC}, \rightarrow)$ と相似になる．

4.2 Denning の束モデル

Denning は，一般の情報フローポリシから，それと同等の半順序フローポリシ，および束フローポリシを以下のように導出した [1]．

情報フローポリシ $\mathrm{FP} = (\mathrm{S}, \mathrm{O}, \mathrm{SC}, \psi, \rightarrow)$ について，$h : \mathrm{SC} \longrightarrow 2^{\mathrm{SC}}$，および $\mathrm{DL}_0 \subseteqq 2^{\mathrm{SC}}$ を次のように定める．

$$h(a) = \{x \in \mathrm{SC} \mid x \rightarrow a\} \tag{23}$$

$$\mathrm{DL}_0 = \{h(a) \mid a \in \mathrm{SC}\} \cup \{\emptyset, \mathrm{SC}\} \tag{24}$$

DL_0 には，包含関係により順序が与えられる．$a \rightarrow b \Leftrightarrow h(a) \subseteqq h(b)$ であり，この順序は FP のセキュリティポリシと両立している．$a \rightarrow b$ かつ $b \rightarrow a$ ならば，$h(a) = h(b)$ となる．DL_0 は，このような a，b を同一視して SC に反対称性を導入し，さらに最小元と最大元を加えたものになっている．$\mathrm{FP}_0 = (\mathrm{S}, \mathrm{O}, \mathrm{DL}_0, h \circ \psi, \subseteqq)$ は FP と同等の半順序フローポリシである．

次に，各 $X, Y \in \mathrm{DL}_0$ について，それらの上限として次を追加する(注7)．

$$X \vee Y = \bigcap\{Z \in \mathrm{DL}_0 \mid X \cup Y \subseteqq Z\} \tag{25}$$

これを，DL_0 の元および追加された元について，新たな上限の追加が不要になるまで繰り返す．SC を有限集合であると仮定すると，有限個の上限の追加で，この手続きは終了する．得られた集合を DL (Denning's lattice) とする．DL は上限演算について閉じており，SC が有限と仮定しているので DL も有限

(注7)：DL_0 に SC を加えてあるので，$\bigcap$ の中の集合は空ではない．

である．したがって，DL は上限演算について完備，すなわち任意の部分集合 $\mathcal{W} \subseteqq \mathrm{DL}$ の上限 $\bigvee \mathcal{W}$ が存在する．すると，下限演算が次のように定義でき(注8)，DL は完備束になる．

$$X \wedge Y = \bigvee\{Z \in \mathrm{DL} \mid Z \to X \text{ and } Z \to Y\} \tag{26}$$

以上により，$i : \mathrm{DL}_0 \longrightarrow \mathrm{DL}$ を包含写像とすると，$\mathrm{FP}_{\mathrm{DL}} = (\mathrm{S}, \mathrm{O}, \mathrm{DL}, i \circ h \circ \psi, \subseteqq)$ は FP と同等の束フローポリシとなる．

4.3 Galois Connection

Denning の束フローポリシと，秘匿性ポリシにおける束フローポリシは似ているところもあるが，詳細において異なっている．本節では，両者の関係を明確にするために，Galois Connection の理論 [10] を援用する．

定義 7. $\mathrm{P} \subseteqq \mathrm{D} \times \mathrm{E}$, $d \in \mathrm{D}$, $\alpha \in \mathrm{E}$, $S \in \mathrm{D}$, $M \in \mathrm{E}$ とする．P を中間述語として用いる．また，写像 $\lambda : \mathrm{D} \longrightarrow 2^{\mathrm{E}}$，ないし $\lambda : 2^{\mathrm{D}} \longrightarrow 2^{\mathrm{E}}$，および，$\rho : \mathrm{E} \longrightarrow 2^{\mathrm{D}}$，ないし $\rho : 2^{\mathrm{E}} \longrightarrow 2^{\mathrm{D}}$ を定義する．

$$d\,\mathrm{P}\alpha \;\Leftrightarrow\; (d, \alpha) \in \mathrm{P} \tag{27}$$

$$S\,\mathrm{P}\alpha \;\Leftrightarrow\; \forall d \in S(d\,\mathrm{P}\alpha) \tag{28}$$

$$d\,\mathrm{P}M \;\Leftrightarrow\; \forall \alpha \in M(d\,\mathrm{P}\alpha) \tag{29}$$

$$\lambda(d) = \{\alpha \in \mathrm{E} \mid d\,\mathrm{P}\alpha\} \tag{30}$$

$$\rho(\alpha) = \{d \in \mathrm{D} \mid d\,\mathrm{P}\alpha\} \tag{31}$$

$$\lambda(S) = \{\alpha \in \mathrm{E} \mid S\,\mathrm{P}\alpha\} \tag{32}$$

$$\rho(M) = \{d \in \mathrm{D} \mid d\,\mathrm{P}M\} \tag{33}$$

$$\rho\lambda(S) = \{d \in \mathrm{D} \mid d\,\mathrm{P}\{\alpha \mid S\,\mathrm{P}\alpha\}\} \tag{34}$$

$$\lambda\rho(M) = \{\alpha \in \mathrm{E} \mid \{d \mid d\,\mathrm{P}M\}\,\mathrm{P}\alpha\} \tag{35}$$

$$\lambda\mathrm{P} = \{\lambda(S) \mid S \subseteqq \mathrm{D}\} \tag{36}$$

$$\rho\mathrm{P} = \{\rho(M) \mid M \subseteqq \mathrm{E}\} \tag{37}$$

$$\rho\lambda\mathrm{P} = \{\rho\lambda(S) \mid S \subseteqq \mathrm{D}\} \tag{38}$$

$$\lambda\rho\mathrm{P} = \{\lambda\rho(M) \mid M \subseteqq \mathrm{E}\} \tag{39}$$

補題 7 (Galois Connections)．$\rho\lambda\mathrm{P}$，$\rho\mathrm{P}$，$\lambda\rho\mathrm{P}$，$\lambda\mathrm{P}$ は，包含関係により，束をなす．
これらについて，次の等式と束の同型が成り立つ．

$$\rho\lambda\mathrm{P} = \rho\mathrm{P} \cong (\lambda\rho\mathrm{P})^{\circ} = (\lambda\mathrm{P})^{\circ} \tag{40}$$

証明． 各集合が束をなすことの証明は省略する．
(40) を証明する．定義より次が成り立つ．

$$S \subseteqq T \subseteqq \mathrm{D} \;\Rightarrow\; \lambda(S) \supseteqq \lambda(T) \tag{41}$$

$$M \subseteqq N \subseteqq \mathrm{E} \;\Rightarrow\; \rho(M) \supseteqq \rho(N) \tag{42}$$

$$S \subseteqq \rho\lambda(S) \tag{43}$$

$$M \subseteqq \lambda\rho(M) \tag{44}$$

(43) より $S \subseteqq \rho\lambda(S)$．よって (41) より $\lambda(S) \supseteqq \lambda\rho\lambda(S)$ である．一方，(44) より $\lambda(S) \subseteqq \lambda\rho\lambda(S)$ であるから

$$\lambda(S) = \lambda\rho\lambda(S) \tag{45}$$

同様に $\rho(M) = \rho\lambda\rho(M)$ (46)

$\lambda(S) \in \lambda\mathrm{P}$ について，$\lambda(S) = \lambda\rho\lambda(S) \in \lambda\rho\mathrm{P}$．よって $\lambda\mathrm{P} \subseteqq \lambda\rho\mathrm{P}$．また $\lambda\mathrm{P} \supseteqq \lambda\rho\mathrm{P}$ は明らか．よって $\lambda\mathrm{P} = \lambda\rho\mathrm{P}$ が示された．$\rho\mathrm{P} = \rho\lambda\mathrm{P}$ も同様に示される．
(45) および (46) から，$\rho : \lambda\mathrm{P} \longrightarrow \rho\lambda\mathrm{P}$，と $\lambda : \rho\mathrm{P} \longrightarrow \lambda\rho\mathrm{P}$ が互いに逆の対応になっていることが分かる．またこれらは，(41) および (42) により，包含関係が逆転する．よって，$\rho\mathrm{P} \cong \lambda\rho\mathrm{P}^{\circ}$ となる． □

4.4 Denning の束と秘匿性ポリシの束との関係

情報フローポリシ $\mathrm{FP} = (\mathrm{S}, \mathrm{O}, \mathrm{SC}, \psi, \to)$ について，Denning による束 DL と秘匿性ポリシ $\mathrm{CP} = (\mathrm{SC}, \mathrm{SC}, \to)$ の束である AL を比較する．

定理 6. DL および AL は，Galois Connection における構成の一つとなっており，次が成り立つ．

$$\mathrm{DL} = \rho\lambda\mathrm{P} \tag{47}$$

$$\mathrm{AL} = \lambda\mathrm{P}^{\circ} \tag{48}$$

$$\mathrm{DL} \cong \mathrm{AL} \tag{49}$$

証明． $\mathrm{P} = \to$ とすると，DL における $h(x)$ と $h(y)$ の上限は次のように計算される．

$$\begin{aligned} h(x) \vee h(y) &= \bigcap\{h(z) \mid h(x), h(y) \subseteqq h(z)\} \\ &= \bigcap\{\rho(z) \mid \{x, y\} \to h(z)\} \\ &= \rho\lambda(\{x, y\}) \end{aligned}$$

よって $\mathrm{DL} = \rho\lambda\mathrm{P}$ である．一方，定義より $\mathrm{AL} = \lambda\mathrm{P}^{\circ}$ は明らか．すると，補題 7 により，$\mathrm{DL} \cong \mathrm{AL}$ が従う． □

4.5 計算時間に関する考察

$\lambda\mathrm{P}$ や $\rho\lambda\mathrm{P}$ などの実際の計算では，ρ および λ の計算量が支配的であると考えられる．例えば，λ の計算では，D の各部分集合 S について $\lambda(S)$ を計算しなければならない．すなわち，λ の計算時間は D の大きさの指数関数である．同様に ρ の計算時間は E の大きさの指数関数である．

従って，定理 6 によれば，AL の計算の方が DL の計算より有利であることが分かる．また，補題 7 により，$\mathrm{AL} \cong \lambda\mathrm{P}^{\circ} \cong \rho\mathrm{P}$ であるから，AL の計算では，E より D の方が小さければ，$\lambda\mathrm{P}^{\circ}$ を，逆ならば，$\rho\mathrm{P}$ を計算することにより，計算時間の最適化を図ることができる可能性がある．

4.6 *C* 束と *A* 束の関係

CL 束は Galois Connection の構成に現れないが，次に示すように，無関係ではないことがわかったので紹介する．

定義 8. 秘匿性ポリシのポリシ集合 $\mathrm{P} \subseteqq \mathrm{D} \times \mathrm{E}$ について，P の $\mathrm{D} \times \mathrm{E}$ における補集合 $-\mathrm{P} \subseteqq \mathrm{D} \times \mathrm{E}$ で表される秘匿性ポリシを，P の補ポリシという．

ポリシ P に対する写像を C_{P} のように書くことにする．すると補ポリシ $-\mathrm{P}$ については，$C_{-\mathrm{P}}$ と書ける．

(注8)：$\emptyset \in \mathrm{DL}$ なので，$\bigvee$ の中の集合は空ではない．

定理 7. 次が成り立つ.

$$\mathrm{CL}(-\mathrm{P}) \cong \mathrm{AL}(P)^{\circ} \tag{50}$$

証明. $C_{\sim\mathrm{P}}(\alpha) = -C_{\mathrm{P}}(\alpha)$, $C_{\mathrm{P}}(\alpha) = \rho(\alpha)$ であることに注意すると, $C_{-\mathrm{P}}(M) = -\rho(M)$ を得る. よって, 写像 $\mathrm{CL}(-\mathrm{P}) \ni X \longmapsto -X \in \rho\mathrm{P}$ は全単射となり, また包含関係を逆転する. 従って $\mathrm{CL}(-\mathrm{P}) \cong \rho\mathrm{P}^{\circ}$ である. 一方, $\mathrm{AL} = \lambda\mathrm{P}^{\circ}$ であるから, 補題 7 により, (50) が得られる. □

5. ま と め

情報フローポリシでは, あらかじめセキュリティクラスを定め, セキュリティクラスの構造に合わせて秘匿情報を管理するため, 動的な秘匿情報の発生, 柔軟な秘匿ポリシの設定には適合していなかった.. そこで本論文では, 秘匿情報を定義したユーザが与えた, 秘匿情報を誰に開示するかという秘匿性ポリシ情報のみを用いて, それに適合する情報フローポリシを動的な構成した. 提案方法では, 情報フローポリシの場合と同様に, 束フローポリシを導くことができる. 特に, 情報フローポリシを秘匿性ポリシとして解釈すると, 従来と同じ束フローポリシを導くことができることを, Galois Connection の理論を用いて示した. 一般の秘匿性ポリシに対する, 提案方法による束構造は必ずしも最小ではないが, 縮小化する方法も提案した. ただし, 提案のものが最小の束構造をとなるかどうかについては, 現在未解決である. 本問題の解決, および適用システムの検討が今後の課題である.

文 献

[1] D. E. Denning: "On the derivation of lattice structureed information flow policies", Technical Report CSD TR180, Purdue University (1976).

[2] D. Bell and L. LaPadula: "Secure computer system: Unified exposition and "multics" interpretation", Technical Report MTR-2997, The MITRE Corporation (1976).

[3] K. Biba: "Integrity considerations for secure computer systems", Technical Report MTR-3153, The MITRE Corporation (1975).

[4] DoD: "Trusted computer system evaluation criteria", Dod 5200.28-std, Department of Defense (1985).

[5] D. E. Denning: "A lattice model of secure information flow", Commun. ACM, **19**, 5, pp. 236–243 (1976).

[6] B. A. Davey and H. A. Priestley: "Introduction to Lattices and Order 2nd Edition", Cambridge University Press (2002).

[7] D. E. Denning and P. J. Denning: "Certification of programs for secure information flow", Commun. ACM, **20**, 7, pp. 504–513 (1977).

[8] B. Lampson: "Protection", Proc. of the 5th Annual Princeton Conference on Information Sciences and Systems, Princeton University, pp. 437–443 (1971).

[9] T. Sakuraba and S. Domyo: "Lattice-based information flow model compatible with given security policy", Proc. of The Third International Conference on Information, pp. 282–285 (2004).

[10] J. B. Nation: "Notes on lattice theory". http://www.math.hawaii.edu/ jb/books.html.