数理解析研究所講究録
322巻 1978年 194-217

プロテクションシステムのセキュリティ判定問題

広島大学 工学部 菊野 亨
今川隆則

1. まえがき

現代の計算機システムにおいては，ユーザ間でメモリ，プロセッサ，データベースやソフトウェアなどの共有を許すということが重要視される．さまざまなユーザが共通のものを共有しようとする時，プロテクション（ユーザの同定，およびシステムの正常な動作が一ユーザの過失により妨げられないようにすること）やセキュリティ（プロテクションの機構をくぐり抜けようとする妨害に対する防御）の機能が要求され，それらの実現法について多くの試みがなされている[1]．

最近では，特にプロテクションの機構（以降，プロテクションシステムと呼ぶ）に対するモデルの提案も多く報告されている[2]~[6]．Harrison らは，プロテクションシステムの時点表示（configuration）Qと権利r（例えばファイルの中味の読み出し，ファイルへの書き込み等）が与えられ，Qに

おいてrを与えられていなかったあるユーザにその権利が与えられる時点表示Q'にQから到達可能なとき，Qはrをもらす（leak）と言い，Qはrに対しセイフでないと定義し，そうでない時セイフであるという．その時

〔F1〕 プロテクションシステムがセイフであるか否かの判定問題は一般には決定不能となる．

〔F2〕 ある条件を満たすシステムにおいては，セイフでないか否かの判定問題がNP－完全となる．

等は既に示されている[4]．

一方，Lipton らは，Harrison らのモデルのサブクラスに属するモデル $\mathcal{S}_0$ を提案し，

〔F3〕[5],[6] $\mathcal{S}_0$ に対するセキュリティ判定問題† は，$\max(n, e)$ のオーダのステップで解ける．ここでnは初期時点表示 G_0 の節点の総数，eは G_0 の枝の総数とする．

を示している．

---

† プロテクションシステムの時点表示Gと，（G上に存在する）特定のユーザp，qと特定の権利rが与えられ，Gではpはqに対し権利rを持たないとする．その時，もしpがqに対し権利rを持つ時点表示G'にGから到達可能であれば，GはP，q，rに対してセキュアでないと言い，そうでない時セキュアであるという．

本稿では，文献(5)，(6)で提案されているLiptonらのモデルの拡張を試みる．なお，拡張されたモデルにおいても，セキュアか否かの判定問題はデプスファーストサーチ(depth first search)[9]を用いればやはり線形時間で解ける．

2. モデルの定義

ここでは，我々が議論するモデルの定義を与える．

〔定義1〕 次の条件を満たす2項組をプロテクションシステム $\mathcal{S}$ とする．

$$\mathcal{S}=\langle \Sigma \cup \{\ell\}, R\rangle$$

(1) $\Sigma=\{r, w, C\}\cup\{\ell\}$：権利の有限集合．ここで $r=read$, $w=write$, $C=call$ とし，ℓ はある不活発(inert)な権利[6]†で，R の決め方からも分かるように，単に受け渡されるだけのものである．

(2) $R=\{R_1, R_2, R_3, R_4, R_5\}$：書き換えルールの有限集合(各 R_i の説明は後述)．

〔定義2〕 プロテクションシステム $\mathcal{S}$ の時点表示

† ℓ の具体的な例としては，プログラムの名前を変更する権利などを考えている．

(configuration) を有向グラフ G = (S, E) で定義する. ここで節点の集合Sはシステム $\mathcal{S}$ にその時点で存在しているサブジェクト (current subject) の集合を表し, $\mathcal{A}_1 \in S$ から $\mathcal{A}_2 \in S$ に向かう枝を $(\mathcal{A}_1, \mathcal{A}_2) \in E$ と書く. 各有向枝 $(\mathcal{A}_1, \mathcal{A}_2) \in E$ は $\Sigma \cup \{\ell\}$ の空(φ)でない部分集合αでラベル付けされており, αは $\mathcal{A}_1$ が $\mathcal{A}_2$ に対しその時点で持っている権利の全ての集合を表している.†

〔注1〕 オブジェクト[4]の集合をOと表す時, 通常のプロテクションシステムでは $O \supseteq S$ の関係が成立するが, $\mathcal{S}$ においては (定義2からも分かる様に) $O = S$ の場合だけを考えている.

時点表示の一例を図1に示す.

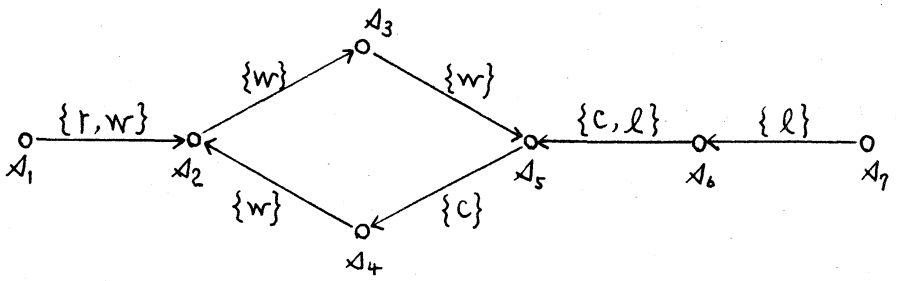


図1 時点表示の例

〔定義3〕 $\mathcal{S}$ で許す書き換えルール R について, 時点表

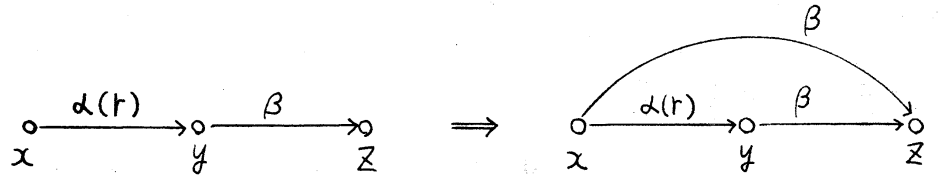
† したがって, Gにおいては任意の節点対 $\mathcal{A}_i$, $\mathcal{A}_j$ に対し, $\mathcal{A}_i$ から $\mathcal{A}_j$ に向かう枝は高々1本とする. 又 $\mathcal{A}_i$ から $\mathcal{A}_i$ への自己ループは禁じている.

示 $G=(S, E)$ を用いて説明する．なお，$\Sigma \cup \{l\}$ の空でない部分集合 α と $a \in \Sigma \cup \{l\}$ に対し，$a \in \alpha$ が成立する時 α の代りに $\alpha(a)$ と書く．

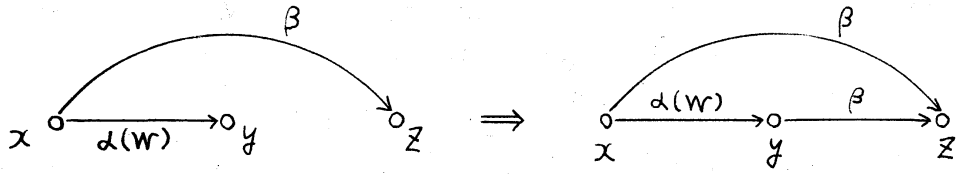
（1）ルール R_1

G において，異なる3つの節点 x，y，z（$\in S$）に対し，x から y にラベル $\alpha(r)$ の枝，y から z にラベル β の枝が存在する時，x から z にラベル β の枝を新たに追加した時点表示 G' を生成するルール．

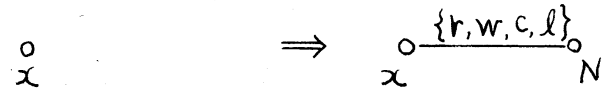
以上のことを次に示す図で表し，その時，ルールを節点 x に適用したという．



（2）ルール R_2

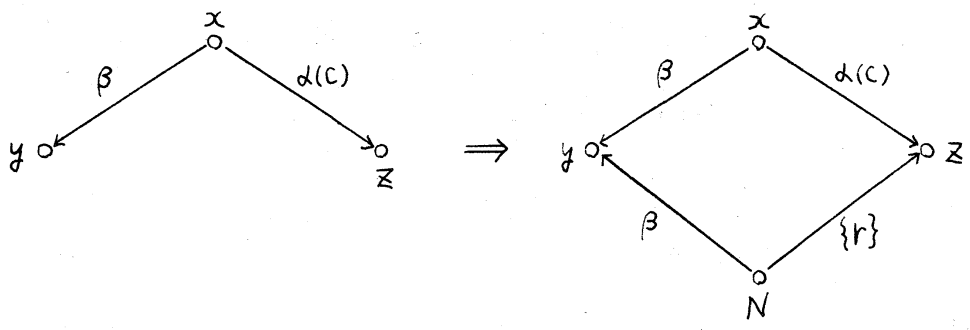


（3）ルール R_3

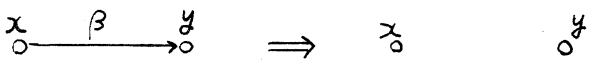


ここで，N は新しい節点とする．

(4) ルール R_4



(5) ルール R_5



〔定義4〕 時点表示Gに対し，ルールR_iを適用して，新しい時点表示G'が得られる時，$G \vdash_{R_i} G'$ あるいは単に $G \vdash G'$ と書く．Gに0回以上ルールを適用して行ってG'が得られるなら $G \vdash^{*} G'$ と書く．いずれの場合についても，G'はGから到達可能であるという．

〔定義5〕 (δに対するセキュリティ判定問題)

入力：1 初期時点表示 $G_0 = (S, E)$．

2 G_0上の相異なる2つの節点pとq．

3 権利 ℓ

判定：次の条件(i)，(ii)を共に満たす時点表示Gが存在するか否か．

(i) $G_0 \vdash^* G$

(ii) G上で，Pからgに向かうラベル$\alpha(\ell)$の枝が存在する．

3．セキュリティ判定問題

先ず，後で必要となる幾つかの記号および記法について説明しておく．

$\Sigma \cup \{\ell\}$の空でない部分集合αと$a \in \Sigma \cup \{\ell\}$に対し，$a \in \alpha$なら$\alpha(a)$と書く．又，$\alpha$と$\ell$に対し，$\alpha \cap \Sigma \neq \Phi$なら，$\alpha(\neg\ell)$と書き，$\ell \in \alpha$かつ$\alpha \cap \Sigma \neq \Phi$なら$\alpha(\not\ell)$と書くことにする．

時点表示$G=(S, E)$（有向グラフ）に対し，各枝の向きを無視した議論をすることが多い．先ず，$(x, y) \in E$あるいは$(y, x) \in E$の少なくとも一つが成立する時，xとyは直接接続していると言い，枝$\{x, y\}$がEに属しているとする．その時，(x, y)と(y, x)のラベルの和集合（有向枝がなければその枝のラベルは空と見做す）を$\{x, y\}$のラベルαと定義し，図2の様に書く．

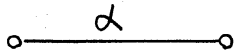
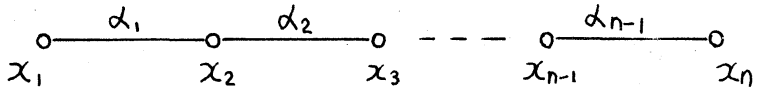


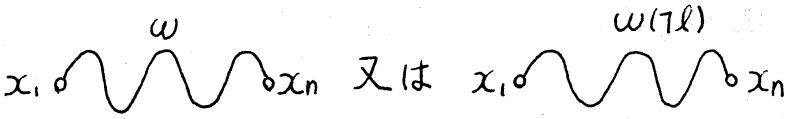
図2　枝$\{x, y\}$

又，G上で各 i ($1 \leq i \leq n-1$) に対し，節点 x_i と節点 x_{i+1} が直接接続しているなら（図3（a））Gで節点 x_1 と節点 x_n は接続していると言う．その時，系列 $[x_1, x_2][x_2, x_3]$ --- $[x_{n-1}, x_n]$ を x_1 と x_n の間の長さ $n-1$ の道† と呼び，$P[x_1, x_n]$ と表す．この時，各節点 x_i および各枝 $[x_i, x_{i+1}]$ は道 $P[x_1, x_n]$ に属するという．

道 $P[x_1, x_n] = [x_1, x_2][x_2, x_3]$ --- $[x_{n-1}, x_n]$ に対し，α_i ($1 \leq i \leq n-1$) を枝 $[x_i, x_{i+1}]$ のラベルとする時，系列 $a_1 a_2 \cdots a_{n-1}$ (各 $a_i \in \alpha_i$) をその道に付随する語と言い，それらの全ての集合をその道に付随する言語と言い，$\alpha_1 \alpha_2 \cdots \alpha_{n-1} (= \omega)$ と表す．特に，任意の i ($1 \leq i \leq n-1$) に対し，



（a）道 $P[x_1, x_n]$



（b）簡略表現（$\omega = \alpha_1 \alpha_2 \cdots \alpha_{n-1}$）

図3　道の説明

† 枝に関しては，一般性を失なうことなく，この道は単純である[8]と仮定する．但し，節点に関しては，必ずしも初等的[8]ではない．

$\alpha_i = \alpha_i(\gamma\ell)$ が成立するなら，ω の代わりに $\omega(\gamma\ell)$ と書き，その道を x_1 と x_n の間の $\gamma\ell$ 道と呼ぶ．

Gの中に図3(a)で示す道の部分があると，同図(b)の様に簡略表現をする．

〔補題1〕[5] 時点表示Gにおいて，異なる3つの節点 x，y，z に対し，x と y の間にラベル $\beta(\gamma\ell)$ の枝が，y から z に向かうラベル α の枝がそれぞれ存在するとする．この時，Gから到達可能なあるG'においてxからzにラベル α の枝が引ける．

補題1を便宜的に下に示す図4で表す．

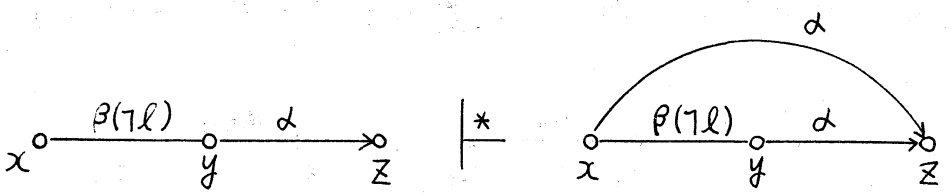
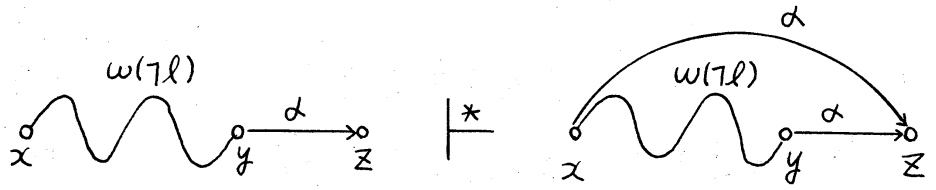


図4 補題1の説明図

以下の議論においても，今の場合と同じ解釈の下で，図を用いて述べていく．

〔系1－1〕



〔補題2〕 時点表示 $G=(S, E)$ において，節点 $z \in S$ はそこから出る枝は m ($m \geq 0$) 本あるが，そこに入る枝は無いものとする．その時，G から到達可能な任意の G' において，z に入る枝を引けない．

(証明) 与えられている G と z に対し，グラフの系列 $G=G_1 \vdash G_2 \vdash \cdots \vdash G_p$ なる G_p で初めて z に入る枝が引けたと仮定する．

その時，$G_{p-1} \vdash G_p$ で用いられたルール R に注目する．R が R_1, R_2 あるいは R_4 のいずれかであるとすれば，G_{p-1} で既に z に入る枝が存在していたことになり矛盾．又，R が残りの R_3 および R_5 では z に入る枝を引くことは不可能である．

(証明終)

次の補題3の準備として，ラベル ℓ による G の分解について述べておく．

〔ℓ による分解〕

時点表示 $G=(S, E)$ 上に2つの異なる節点 x_0 と y_0 が存在し，x_0 と y_0 の間に道があり，かつ，それらの道には全て，ラベル $\{\ell\}$ の枝が少なくとも1つ属しているものとする．

その時，この G から x_0 と y_0 を利用して，次の条件①～④を満たす3つの部分グラフ $G^{(i)}=(S^{(i)}, E^{(i)})$ $(1 \leq i \leq 3)$ を構成し (図5参照)，これを G の ℓ による分解と呼ぶ．

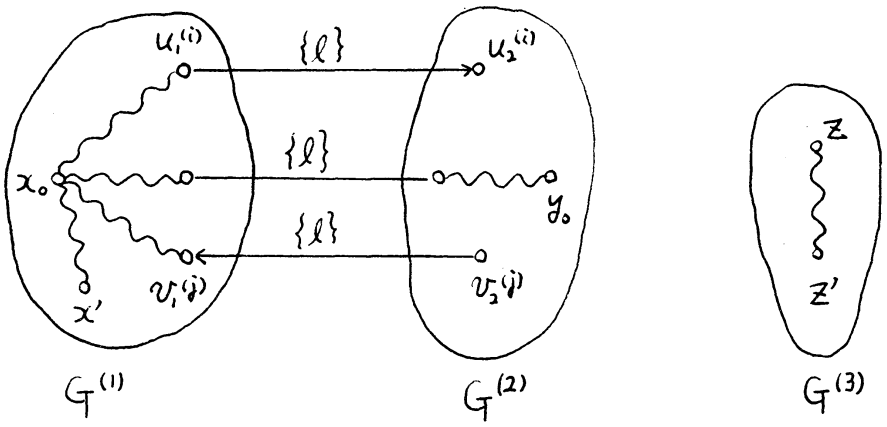


図5　Gのlによる分解

① $x_0 \in S^{(1)}$ かつ $y_0 \in S^{(2)}$ とする.

② 任意の $x' \in S^{(1)}$ に対し x_0 から $S^{(1)}$ の節点だけを含む道がある.

③ 任意の $z' \in S^{(3)}$ に対し，x_0 および y_0 のいずれからも道がない.

④ $S^{(1)}$ と $S^{(2)}$ の節点間にはラベル $\{l\}$ の枝だけが $m+n$ 本存在する. 今，各 i $(1 \leq i \leq n)$ に対し，$u_1^{(i)} \in S^{(1)}$ から $u_2^{(i)} \in S^{(2)}$ へラベル $\{l\}$ の枝があり，逆に，各 j $(1 \leq j \leq m)$ に対し，$v_2^{(j)} \in S^{(2)}$ から $v_1^{(j)} \in S^{(1)}$ へラベル $\{l\}$ の枝があるものとする†.

---

† 特に $n=0$ あるいは $m=0$ も許し，その場合は対応する枝が1本も存在しないことを表す. 但し，仮定より $n=m=0$ ということはない.

更に，上述の通り分解されたGから到達可能な任意のG'に対しても次の通り3つの$G^{(i)}$に分ける．

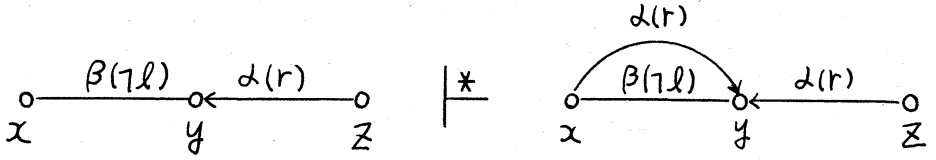
〔分解ルール〕

G　G'とする時，Rに注目し，Gに対する$G^{(i)}$を利用してG'の各$G^{(i)}$を次の通り定める．先ず，$R=R_3$と$R=R_4$の場合Rが節点xに適用されたなら，新しく生成される節点Nは，xがGの分解で$G^{(i)}$に属していたのならG'でも$G^{(i)}$に入れる．又，$R=R_5$の場合には孤立する節点が生じた時だけ，それを新たにG'の$G^{(3)}$に移し，そうでなければそのままとする．$R=R_1$と$R=R_2$の場合は各$G^{(i)}$に属する節点に変化はない．$G=G_1 \vdash G_2 \vdash \cdots \vdash G_n=G'$なるG'に対しては，$G_1$, G_2, ---の順に上述の手続きを繰り返し適用して行って，各$G^{(i)}$を決定するものとする．

〔補題3〕　図5に示すGが与えられ，上述の分解ルールに従うなら，Gから到達可能な任意のG'において（G'の$G^{(1)}$, $G^{(2)}$, $G^{(3)}$上で），任意の$x \in S^{(1)}$と，$U_2^{(i)}$ $(1 \leq i \leq n)$と異なる任意の節点$y \in S^{(2)}$に対し，xからyに向かう枝は引けない．

証明略（文献(7)参照）

〔補題4〕[5]



〔補題5〕(5)

〔補題6〕(5)

〔補題7〕 次の条件①，②を満たす道とその間に存在する節点 x，y を含む時点表示 $G=(S, E)$ が与えられているとする（図6参照）．その道を $[x_1, x_2]$ --- $[x_{n-1}, x_n]$（但し，$x_1=x$，$x_n=y$）とする時，

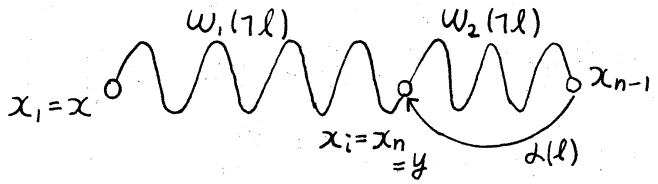
① x_1 と x_{n-1} の間に 7ℓ 道があり

② 枝 $[x_{n-1}, x_n]$ に対応し，G上でラベル $\alpha(\ell)$ の枝 (x_{n-1}, x_n) が存在する．

が成立する．

この時，Gから到達可能なあるG'において，xからyに向かう，ℓ をその要素として含むラベルの枝が引ける．

(a) $y \neq x_i$ $(1 \leq i \leq n-1)$ の場合



（b）　あるiに対し，$y=x_i$が成立する場合

図6　補題7の説明図

（証明）図6の（a），（b）に示す通り，yがx_n以外のx_iと一致するか否かによって分けて考える．

（a）の場合は系1－1に帰着される．

（b）の場合，枝$[x_{n-2}, x_{n-1}]$（そのラベルを$\beta(\gamma\ell)$とする）に注目する．先ず，$(x_{n-2}, x_{n-1})\in E$ならば，系1－1より，xからx_{n-1}に向かうラベル$\beta(\gamma\ell)$が引け，更に補題1より，xからyに向かうラベル$\alpha(\ell)$の枝が引ける．次に，$(x_{n-1}, x_{n-2})\in E$ならば，補題4～6より，x_{n-3}からx_{n-2}に向かうラベル$\beta(\gamma\ell)$の枝が引け，更に，系1－1を用いると，xからx_{n-2}に向かうラベル$\beta(\gamma\ell)$の枝が引ける．一方，補題1より，x_{n-2}からx_nに向かうラベル$\alpha(\ell)$の枝が引ける．ここで再び補題1を用いると，xからyに向かうラベル$\alpha(\ell)$の枝が引ける．　（証明終）

〔系7－1〕　補題7における条件②のラベル$\alpha(\ell)$を$\{\ell\}$としても，補題7は成立する．

〔補題8〕　次の条件①～③を満たす道とその間に存在す

る節点x，yを含む時点表示G＝（S，E）が与えられているとする（図7参照）．その道を〔x_1，x_2〕---〔x_{n-1}，x_n〕（但し，x_1＝x，x_n＝y）とする時，

① x_1とx_nの間に7l道があり．

② xとyの間のどの道上にも属さない，ある節点z∈Sに対し，枝（z，y）∈Eが存在し，かつ，そのラベルがα(l̂)である．

この時，Gから到達可能なあるG'においてxからyに向かう，lをその要素として含むラベルの枝が引ける．

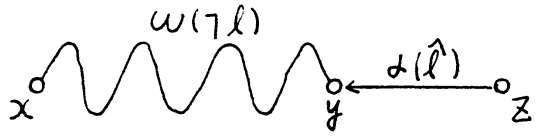


図7　補題8の説明図

補題1と4～6を利用して，道P〔x，y〕＝〔x_1，x_2〕〔x_2，x_3〕---〔x_{n-1}，x_n〕の長さに関する帰納法で証明できる．

〔定理1〕　任意の時点表示G＝（S，E）と異なる2つの節点p，q（∈S）が与えられたとする．この時，pからqに向かうlを含むラベルをもつ枝†が存在する時点表示G'にGから到達可能であるための必要十分条件は次の条件1と条件2の少なくとも1つが成立することである．

条件1：G上で，ある節点z∈Sに対し，pとzの間に7l

† Gにおいてそうした枝は存在していないものとする．

道が存在し，かつ，zからgに向かうラベル$\{l\}$の枝が存在する．

条件2：G上で，pとgの間にl道が存在し，かつ，ある$z \in S$に対し，枝(z, g)がEに属し，しかもそのラベルをλとすると$\lambda = \lambda(l)$が成立する．

(証明) 十分性：補題7，系7-1，補題8より示される．

必要性：(i) Rの性質より，その間に道のない節点同志を接続することはできないので，G上でpとgの間に道が存在することが必要である．しかも補題2よりgに入る枝が存在していなければならない．

(ii) 今，$G_1 \vdash^* G_i \vdash^* G_n = G'$とし，$G_n$で初めて，pから$g$に向かう，ラベル$l$を含む枝が引けたとする．その$G_{n-1} \vdash G_n$で用いられたルールに注目すると，それは$R_1$か$R_2$のいずれかである．いずれの場合にも，ある$G_i$ $(1 \leq i < n)$において既にgに入るラベルlを含む枝が存在していることが要求される．しかも$G_i = G_1$でなければならない．なぜならば，G_1ではそうした枝がなかったとし，ある$G_{i'}$ $(i' \geq 2)$で初めて現れたとすると，$G_{i''}$ $(i'' < i')$で既に存在していたことになり矛盾が導ける．そこで$G_1 = G$において存在している，gに入るラベルlを含む枝を(t_j, g) $(j = 1, 2, \cdots, K)$と書く．

(iii) 次に，(i)で述べたpとgの間の道によって次の3

つの場合に分ける．G上でPとgの間に長さ1の道だけが1つ存在する（場合1），どの道も長さが2以上である（場合2），それら2つが共に存在する（場合3）とする．

場合1：表1にその結果を示す．なお表1で〔P，g〕のラベル＝{ℓ}は〔P，g〕のラベルがℓ単独，ℓ̂はℓ以外にもある権利a（≠ℓ）が含まれていること，≠ℓはℓが含まれていないことを意味する．又，（t_g，g）のラベルで＝{ℓ}は全ての（t_g，g）のラベルが{ℓ}であること，≠{ℓ}は少なくとも1つの（t_g，g）に対し，ℓ以外にも権利a（≠ℓ）が必ずラベルに含まれていることを示す．又，表には各場合を区別する目的で整数1，2，---を付け，それぞれの場合に，もしGから到達可能なあるG'においてPからgに向かう，ラベルℓを含む枝が引けるなら○印を，そうでないなら×印

〔P，g〕 （t_g，g）のラベル		＝{ℓ}	≠{ℓ}
枝の向き	ラベル		
(P，g)∈E	≠ℓ	1 ×	5 ○
(g，P)∈E	＝{ℓ}	2 ×	6 ×
&(P，g)∉E	ℓ̂	3 ×	7 ○
	≠ℓ	4 ×	8 ○

表1　場合1の結果

を記入している.

先ず1の場合, 各(t_j, g)の枝(そのラベルは全て$\{l\}$である)を用いて図5で示した"lによる分解"を行なう. $p, g \in S^{(1)}$かつ, 全ての$t_g \in S^{(2)}$となるように, Gを$G^{(i)} = (S^{(i)}, E^{(i)})$ $(1 \leq i \leq 3)$に分ける. この時, 上の仮定より$S^{(1)}$に属するどの節点からもgに入る, ラベルがlを含む枝はない. $G = G_1 \vdash^* G_i \vdash^* G_n = G'$とし, G_nでpからgに向かう, ラベルlを含む枝が引けたとすると, (ii)と同様, あるG_iで既にgに入る, ラベルlを含む枝(Δ, g)が存在していなければならない. 分解ルールの決め方より, $\Delta \in S^{(2)}$あるいは, $\Delta \in S^{(1)}$のいずれかである. 今, $\underline{\Delta \in S^{(2)}}$とすると, $G_i \vdash^* G_n$の過程で, Δ(あるいはΔと直接接続しているΔ')にR_1(あるいはR_2)を適用してできる, ラベルがlを含む任意の枝(Δ', g)に対し, $\Delta' \in S^{(1)}$とはなり得ない. したがって, G_nで枝が引けたとする仮定に反する. 他のR_i $(i \neq 1, 2)$では明らかに不可能. 次に$\underline{\Delta \in S^{(1)}}$とし, ある$G_{i'}$ $(i' \leq i)$で初めてgに入るラベルlを含む枝が引けたとすると, やはり初めてという仮定に対し, 容易に矛盾が導ける. したがって1の場合の×印が証明できる. 2〜4の場合は1と全く同じ. 6の場合は枝(g, p)を用いて"lによる分解"を行なった後, 補題3を適用すると直ちに得られる. 5, 7, 8

はいずれも補題4～6より成立する.

場合2：pとqの間の長さ(n_i-1)の各道$P[p, q]$を$[x_1, x_2][x_2, x_3]$ --- $[x_{n_i-1}, x_{n_i}]$ ($p=x$, $x_{n_i}=q$)と表す. 特にqと直接接続している節点x_{n_i-1}(=xとおく)に注目し, 上述の道の最初の長さ(n_i-2)の部分を$P[p, x]$

(辺, q)のラベル / 枝の向き		ラベル	$=\{l\}$		$\neq\{l\}$	
$(x, q)\in E$	$x=^{\exists}_{t_{ij}}$	$=\{l\}$	1	○	13	○
		$\hat{l}$	2	○	14	○
		$\neq l$	3	○	15	○
	$x\neq^{\forall}_{t_{ij}}$	$=\{l\}$	4	○	16	○
		$\hat{l}$	5	○	17	○
		$\neq l$	6	×	18	○
$(q, x)\in E$	$x=^{\exists}_{t_{ij}}$	$=\{l\}$	7	○	19	○
		$\hat{l}$	8	○	20	○
		$\neq l$	9	○	21	○
	$x\neq^{\forall}_{t_{ij}}$	$=\{l\}$	10	×	22	×
		$\hat{l}$	11	×	23	○
		$\neq l$	12	×	24	○

表2　場合2の結果

と書く.

この時, pとxの間に少なくとも1つlℓ道が存在しなければならない. なぜならば, もし全ての道P〔p, x〕がラベル{ℓ}の枝を少なくとも1つ含んでいるとすると, それらの枝を利用し,"ℓによる分解"を行ない, 補題3を適用すると, pからgに向かうラベルℓを含む枝が引けないことが結論されてしまう.

そこで, 道P〔p, x〕としては上述の条件を満たすものについてだけ考える. 道P〔p, g〕からP〔p, x〕を除いた枝〔x, g〕の向き, および各枝(t_g, g)のラベルによって場合分けをし得られる結果を表2に示している.

表2で$x=\exists t_g$はあるt_gがxと一致していること, $x\neq\forall t_g$はどのt_gもxと一致していないことをそれぞれ表し, それ以外の記号については表1と同じとする.

表2でX印の付いている箇所の内, 先ず10と22は補題3より, 又, 6, 11, 12は表1の1の場合と同様の議論で証明できる. 次に○印の付いている残りの箇所は全て, 補題7, 系7-1と補題8より容易に導ける.

場合3: 各表における○印に対応する, 場合1と場合2(表で指定する)条件のうち少なくとも1つが, 与えられたGについて成立しておれば, あるG'($G \vdash^{*} G'$)においてその

枝は引けるが，場合1および場合2の条件が共にGで成立しないなら，どのようなG'（G⊢*G'）においても，その枝は決して引けない．

（iv）以上の結果を（表1および表2を利用して），G上でgに入っている枝のラベルによって分けて表2の1～4，7～9と13，16が条件1に，表1の5，7，8および表2の2，5，13，17～21，23，24が条件2にそれぞれまとめられる．

（証明終）

〔例1〕　定理1の条件1が満たされている場合の一例．

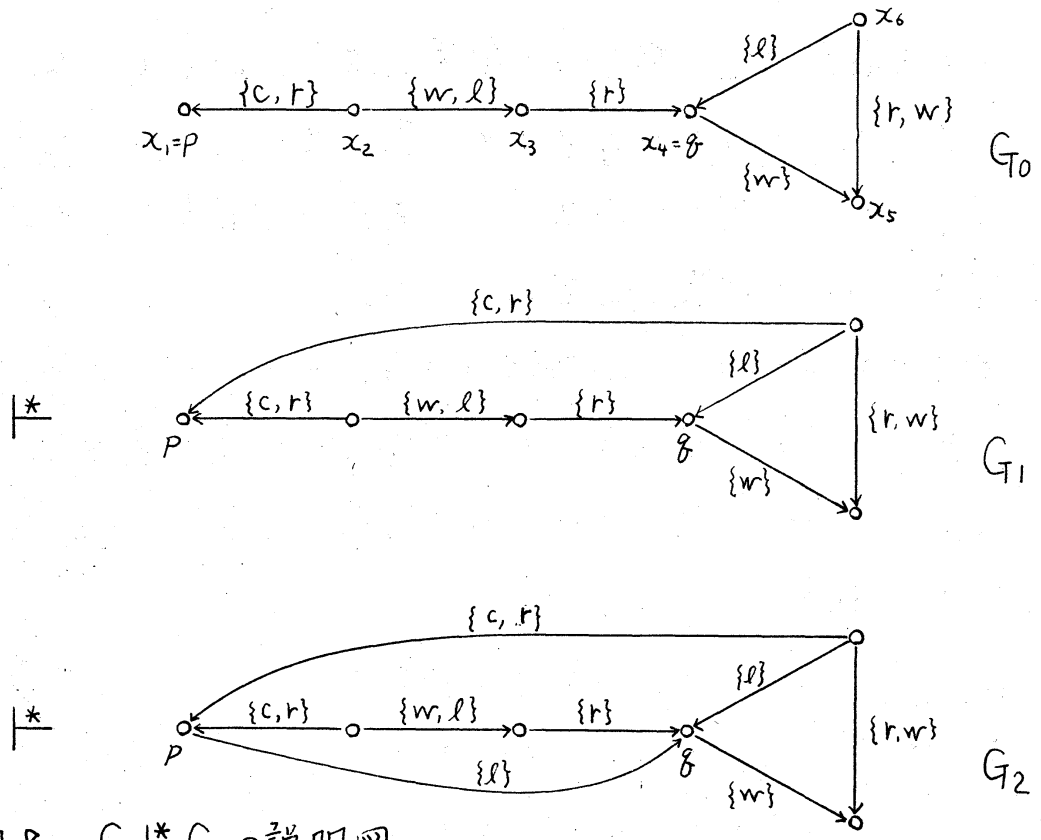


図8　$G_0 \vdash^* G_2$の説明図

定理1で与えた条件を利用して，gに対するセキュリティ判定問題（定義5）を解くアルゴリズムを与えることができる．詳細は文献（7）に譲ることにして，ここではその基本方針についてだけ述べる．

〔アルゴリズム〕

ステップ1　$G_0=(S, E)$とp，gに対し

$V(\ell)=\{u \mid$ ラベルが$\{\ell\}$の枝$(u, g)\in E\}$

$V(\hat{\ell})=\{v \mid (v, g)\in E$，かつ，枝$(v, g)$のラベル$\lambda$に対し$\lambda=\alpha(\hat{\ell})\}$

を計算する．

ステップ2　$V(\ell)\neq\Phi$なら先ずL1へ，$V(\ell)=\Phi$，かつ，$V(\hat{\ell})\neq\Phi$ならL2へ，$V(\ell)=V(\hat{\ell})=\Phi$なら"NO"を出力する．

L1：各$u\in V(\ell)$に対し，デプスファースサーチ（以降DFSと略す）を利用し，pとuの間にℓ道が存在するか否か調べる．もし道が見付かれば"YES"を出力する．見付からなければ，$V(\hat{\ell})\neq\Phi$の場合に限りL2に，それ以外の場合"NO"と出力する．

L2：DFSを利用し，pとgの間にℓ道が存在するか否か調べる．もし道が見付かれば"YES"を，見付からなければ"NO"をそれぞれ出力する．

〔定理2〕 プロテクションシステム$\mathcal{S}$に対するセキュリティ判定問題は，上述のアルゴリズムを用いると，$\max(n, e)$のオーダのステップで解ける．ここでnは初期時点表示G_0の節点の総数，eは枝の総数とする．

4. むすび

Lipton らのモデル$\mathcal{S}_0$に対し，権利lを導入することにより拡張されたモデル$\mathcal{S}$を定義し，$\mathcal{S}$に対するセキュリティ判定問題が線形時間で解けることを示した．なお，本稿では権利lを固定して議論したが，lを一般の権利$\lambda \in \Sigma \cup \{l\}$に置き換えた判定問題に対しても，容易に拡張できる(7)．

又，注1でも触れた様に，$\mathcal{S}$ではサブジェクトだけを考えていた．そこで，現在，オブジェクトも含む様にモデルを拡張することについて検討中である．しかしルールR_2の適用（定義3参照）において，もしyがサブジェクトでなくオブジェクトであったとすればR_2の適用は許されないもの（invalid）となってしまうため，オブジェクトも含む場合のモデルの解析はかなり難しくなると予想される．

謝辞 熱心にご討論いただいた田中一正君に深謝する．

文献

(1) 嵩忠雄:"ソフトウェアの進歩とその基礎理論の発展", 電子通信学会誌, 60, 8, pp. 868-876 (1977).

(2) ACM Computing Surveys,8,3 and 4,Reliable Software (1976).

(3) G.S.Graham and P.J.Denning:"Protection principles and practices",Proc. AFIPS SJCC 40,pp.417-426 (1972).

(4) M.A.Harrison,W.L.Ruzzo and J.D.Ullman:"Protection in operating systems", CACM,19,8,pp.461-471 (1976).

(5) R.J.Lipton and L.Snyder:"A linear time algorithm for deciding subject security", JACM,24,3,pp.455-464 (1977).

(6) A.K.Jones, R.J.Lipton and L.Snyder:"A linear time algorithm for deciding security", Proc. 17th Annual FOCS Conf.pp.33-44 (1976).

(7) 今川隆則:"プロテクションシステムのセキュリティ判定問題について",広島大学工学部卒業論文 (昭53-3 発表予定).

(8) C.L. リウ著, 伊理訳:"組合せ数学入門-II" 共立全書542 (昭47).

(9) A.V.Aho,J.E.Hopcroft and J.D.Ullman:"The design and analysis of computer algorithms", Addison-Wesley (1974).