特集 フォーマルメソッドの新潮流 6

Part III：新領域の開拓

匿名性とプライバシのためのフォーマルメソッド

真野　健 ● 日本電信電話（株）
NTT コミュニケーション科学基礎研究所

匿名性・プライバシって何だろう？

インターネットを利用してショッピングをしたり，オークションに参加したり，あるいは掲示版に書き込みをしたりする場合，そのことによって自分にかかわる情報，いわゆる個人情報やプライバシといったものが危険にさらされないかどうかを気にする人も多いだろう．情報通信技術の発展に伴い，ネットワークを介して我々の重要な情報がやりとりされる機会は増加している．もちろん，個人情報保護法などの法整備によって不必要な情報の保管・流通は避けられる傾向にあるが，それがどうしても必要な場面では，いかにして匿名性・プライバシを保護するか，そして，正しく保護されていることをどうやって確認するかは重要な問題だ．本特集のテーマであるフォーマルメソッドは，そのような問題に対する抜本的な解決となり得る技術の１つである．

では，フォーマルメソッドでシステムの匿名性やプライバシを検証するためには何が必要だろうか．数理論理学という理論的基礎，そしてモデル検査器や定理証明器などの検証支援のツールといった，フォーマルメソッドで従来用いられてきた道具立てが必須なのはいうまでもない．しかしその前に，匿名性・プライバシをフォーマルな議論に乗せるためには，そもそもまずそれらをフォーマルに(あるいは数理的に)定式化する必要がある．そして実は，現在のセキュリティのフォーマルメソッド研究において，そのような定式化や分類学自体もホットなテーマなのだ．

たとえば Hughes と Shimatikov は，匿名性やプライバシに関係するさまざまな性質を identity-related property と呼び，該当する数十の性質を，function view と protocol graph という独自の枠組みでフォーマルかつ統一的に分類／整理している[3]．また，匿名性に関してのみだが，知識論理と呼ばれる論理体系で一般的に記述するという Halpern と O'Neill の研究もある[2]（これについては，後でよりくわしく紹介する）．しかしそのような研究によって，匿名性・プライバシのフォーマルな定式化という問題が解決したかといえば，かならずしもそうとは言えない．たとえば前者の研究では，プライバシを通信の送信者と受信者の関係として捉えているのだが，そのような図式に当てはまらないプライバシの例はいくらでも挙げることができる．

フォーマルメソッドのための匿名性・プライバシの定式化は，フォーマルであることはもちろんだが，さらに一般性があるということも求められる．ここで一般性とは，ショッピングや掲示版といった個別具体的な事例・状況に依存しないという意味である．一般性のあるメソッドを構築するには，まず問題の定式化自体に一般性がなくてはならないことは明らかだろう．しかし，そのような定式化が本当に可能だろうか？

そもそもそれらの日常的な意味も，人により場合により，微妙にしかし確実に違っているように見える．たとえば，“匿名性とプライバシ”とひとくちに言うが，両者はどういう関係にあるのか？　匿名性はプライバシの一部だ，と考える人は多いかもしれない．また，“ネットワークの匿名性とプライバシ”などといった場合には，プライバシは守られるべきもの，匿名性はそのためのいわば必要悪，といった捉えられ方をされることもある．もちろん，もっと違った捉え方をする人もいるだろう．

解決への手がかりを求めて，まずはいったんフォーマルメソッドから離れ，目を法律へと向けてみたいと思う．なぜなら法律は，プライバシの問題を一般的に，かつフォーマルとは言わないまでも厳密に定式化した大先輩だからだ．ただし，単に法的な定義をフォーマルに焼き直そうというのではない．匿名性・プライバシの法的な取り扱いを知ることでそこに潜む問題の難しさを明確化するのが，次の章の目的である．そのあと“匿名性とプライバシのためのフォーマルメソッド概観”の章では，匿名性・プライバシ検証のためのフォーマルメソッドを，代表的な研究を取り上げて説明する．そして，“法的なプライバシふたたび”の章でふたたび法的な問題をフォーマルな見方で振り返り，最後にまとめを述べる．

法的な匿名性・プライバシ

本章では，日本の現行法と判例に基づく匿名性とプライバシについて概観する．ただし，筆者は法律には素人なので，記述・議論が至らない点も多いかと思う．法的なプライバシに関する詳しい説明は，たとえば文献 6）などを参考にされたい．なお，本章では特に断らないかぎり，“ プライバシ ” という言葉を，フォーマルな意味ではなく法的な意味で用いる．

●プライバシ権と個人情報保護

日本においてプライバシの侵害から個人を守る法的枠組みには，プライバシ権と個人情報保護法がある．個人情報保護法は，個人情報取扱事業者の義務を規定する法律であり，しばしば道路交通法に例えられる．つまり，交通事故を防ぐために道路交通法があるように，個人情報の取り扱いを巡るトラブルを防ぐためのルールが同法だということである．そこで規定される個人情報は，“ 生存する個人に関する情報であって，当該情報に含まれる氏名，生年月日その他の記述等により特定の個人を識別することができるもの ” とされ，法的にはプライバシとされない情報も含む．この法律のフォーマルな取り扱いも興味深いテーマだが，本稿ではこれ以上ふれないことにする．

プライバシを法的な権利として世界で最初に論じたのは，Harvard Law Review に 1890 年に発表された Warren と Brandeis の論文 “The Right to Privacy” だが，日本でそれが本格的に議論されるようになったのは 1960 年代以降である．日本におけるプライバシ権は，日本国憲法第 13 条（個人の尊重）によって保証されると解されているが，明文化はされていない．判例としては，1964 年に “ 私生活をみだりに公開されないという法的保証ないし権利 ” としてのプライバシ権を認める，いわゆる “ 宴のあと ” 事件に関する判決が出される（東京地判昭和 39 年 9 月 28 日判時 385 号 12 頁）．本事件は，同名の小説が原告有田八郎のプライバシを侵害したとして，著者の三島由紀夫と出版元の新潮社を被告として提起された民事訴訟である．その判決の中で，プライバシの侵害による不法行為の成立要件として，公開された内容が，

1. 私生活上の事実または私生活上の事実らしく受け取られるおそれのあることがらであること
2. 一般人の感受性を基準にして当該私人の立場に立つた場合公開を欲しないであろうと認められることがらであること
3. 一般の人々に未だ知られていないことがらであること

という判断が示された．

これらの要件は，基本的に現在でも踏襲されているが，若干の変遷もある．たとえば，1 つ目の要件には “ 私生活上の ” という条件（私事性）が含まれるが，これは現在では必須ではないとされている．たとえば，個人の犯罪経歴はプライバシに属するが，法的に有罪となっている以上公の事実であって私事ではあり得ないからである．また，上記の要件以外にも考慮されるべきこととして，表現の自由とプライバシの関係，公人とプライバシの関係などが挙げられる．

さらにもう 1 つ注意すべき点として，1 つ目の要件に関連して，明示的ではないが前提とされていることがある．それは，公開された内容によって当該個人を同定可能だということである．このことは，とりわけ特定の個人をモデルとした小説によるプライバシ侵害のときに問題となり，上記 “ 宴のあと ” 事件のほかにも，柳美里によるモデル小説に関する “ 石に泳ぐ魚 ” 事件の裁判（最高判平成 14 年 9 月 24 日判時 1802 号 60 頁）などでも争点の 1 つとなっている．

さて，個人を同定可能だということは，匿名ではないということである．逆に言えば，匿名性が成り立っている状況ではプライバシ侵害はあり得ないということになる．これは，匿名性とプライバシの法的な関係の 1 つと言える．しかし，この関係は常に妥当なのだろうか？

●完全に匿名ならプライバシは守られる？

問題の切実さを強調するため，あえてやや刺激的な例からはいることにする．目線入りのヌード写真，しかも自分の，を想像していただきたい．だれかに “ このとおり目線を入れるから，いやそれでも心配なら顔全部を黒塗りするから，この写真をネットで公開していい？ ” と聞かれたら，あなたはどう答えるだろうか．完全に匿名だったら構わない，と答える人ばかりではないと思う．あるいは別の例として，インターネット掲示版で，特定の個人の行動を多人数で監視し逐一掲示するといういたずらが行われているという．筆者はこれを悪質なプライバシ侵害だと考えるが，では仮にそのいたずらを，監視される個人の名前をふせて匿名で行ったらどうだろう．もはやプライバシ侵害ではないと言えるだろうか．たとえ監視されているのが誰かは分からなくても “ こいつ，こんなバカなことやってるよ！ ” といった誹謗中傷は可能だし，それがほかならぬ自分自身に向けられたものであることは，監視されている本人には分かるのである．

以上は，匿名性が成り立っていてもプライバシを侵害されていると感じられそうな例のつもりである．しかしながらこのような単純な例では，“ もしかすると，なに

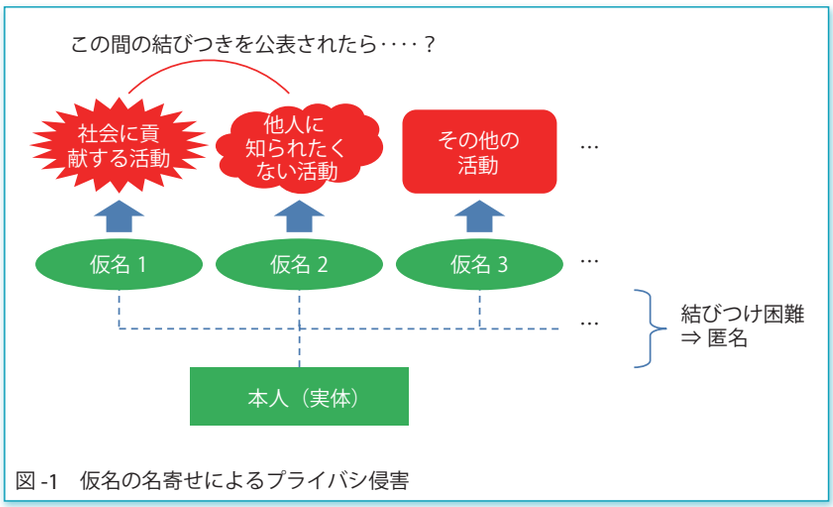

図 -1　仮名の名寄せによるプライバシ侵害

かのはずみで匿名でなくなってしまい，私を同定できてしまうかもしれない”という危惧に基づく不快・不安という要素が残ってしまうため，前節の終わりに指摘した関係の妥当性を議論するためには精度を欠く．そこで以下では，もうすこし凝った例を考えよう．“仮名(かめい)の名寄せ”の問題である．

インターネットでは，よくハンドルと呼ばれる仮名が用いられる．しかも 1 つではなく，複数のハンドルを使い分けている場合も多い．継続的に用いるハンドルはコテハン，一時的に利用してすぐに捨ててしまうハンドルは捨てハンなどと呼ばれる．ネットの匿名性を利用して，状況により複数のアイデンティティを使い分けているわけだ．また仮名でできることは，掲示版への書き込みのようなとるに足らないことだけではない．たとえばコンビニエンスストアでウェブマネーなどの電子現金を買えば，仮名だけである程度の経済活動もできる．ネット上で社会に貢献する活動を行ってはいるが，何らかの事情で実名を明かせず仮名を使っているといった状況（たとえば，独裁国家からの亡命者に対する情報提供など）もあり得るだろう．

しかしここでも，インターネットにおける仮名だの匿名性だのはしょせん絵空事であって，たとえばプロバイダの通信履歴照会などで個人が特定される可能性だってあるではないか，と思われるかもしれない．しかし現在の暗号技術を使えば，ある比較的弱い仮定のもとに，仮名と本人との結びつけができないことを理論的に証明できる仮名，つまり実質的に完全な仮名を作ることも不可能ではないのである．この，“ある比較的弱い仮定”を厳密に述べるには計算量理論などの準備が必要となるが，詳細は文献 1)などを参照されたい．

さて仮にいま，ある人が上記のような仮名を複数使い分け，仮名 1 でなにかしら社会に貢献する活動を，仮名 2 で他人に知られたくないプライベートな活動をしていたとする（図 -1）．そのとき，仮名 1 と仮名 2 が，実は同一人物のものだと公表されてしまうとしたらどうだろう．もし“仮名 1 を使って偉そうなことを言っていながら，その陰でこそこそ仮名 2 のようなことをしているなんて‥‥”などと他人から非難されることになれば不快だし，仮名 1 による活動も困難になってしまうかもしれない．公表してほしくないと感じるのが自然だろうし，少なくとも日常的な意味では，ある種のプライバシの侵害だと考えられるのではないだろうか．しかしながら，法的にはそれを公表することはプライバシ侵害にはあたらないはずである．理由はもちろん，本人の同定ができないからだ．現在の日本の判例に基づくと，仮名が完全であればあるほど，本人の同定が困難となるがゆえに，プライバシ侵害の要件を満たさなくなる．つまり，完全な仮名による完全な匿名性の実現が，結果としてプライバシを守るどころか，このケースに関しては逆に法によるプライバシ保護を完全に不能にしてしまうという，なんともパラドキシカルな状況なのである．なぜこのようなことが起こってしまうのだろう？　こういった事柄は法的に保護するにはおよばないのか，あるいはプライバシではなく何か別な枠組みで守られるべきことなのか．

筆者はこれが何らかの不備に起因するものかどうかすら判断する力を持たないし，ここでの目的はそのようなことではない．しかしながら，前節の終わりに指摘した匿名性とプライバシの関係の妥当性には何かしら困難な問題が存在し，以上のような込み入った議論がつきまとうということはご確認いただけたと思う．

問題が 1 つ確認されたところで，つけ焼き刃の法律論はいったん終わりにし，以降は本題のフォーマルメソッドに話をもどす．そして最後に，フォーマルな見方でふたたびこの問題を眺めてみたいと思う．

匿名性とプライバシのためのフォーマルメソッド概観

匿名性・プライバシ検証のためのフォーマルメソッドには，大きく分けて 2 つのアプローチがある．1 つは状態遷移モデルに基づくアプローチで，セキュリティを記述する様式とそれを検証する方法をともに与えるという意味において，工学的に高い有用性を持つ．もう 1 つは知識論理に基づくアプローチで，その高い表現力によって，さまざまなセキュリティ要件の微妙な違いの書き分けや，関係する性質の間の比較を容易にするというメリットを持つ．本章では，それぞれについて代表的な研究

を取り上げつつ説明する．

●状態遷移モデルに基づくアプローチ

本アプローチは，状態遷移モデルでシステムの動作を記述し，さらにその動作の等価性に基づいて匿名性・プライバシを記述するというものである．また，その等価性を証明するのに，模倣あるいは双模倣と呼ばれる証明技法を用いるという特徴もある．本節では，代表的な研究として Kremer と Ryan のもの[4]を取り上げ，このアプローチについて概説する☆1．

まず，匿名性・プライバシは他のセキュリティと同じく，だれかに対して何らかの情報を隠すことである．隠したい相手は通常“攻撃者”と呼ばれる．この攻撃者がどういう能力を持つと想定するかが，セキュリティの記述にも検証にも重要であるが，それを規定するために，多くの検証で Dolev-Yao モデルというある種の理想化された攻撃者のモデルが採用されている．これにはいくつかのバリエーションが存在するが，基本的な特徴は以下の 2 つの仮定を置くことである：

1. システムで用いる暗号は“完全”である，すなわち，攻撃者は復号鍵を知らないかぎり，暗号化されたメッセージを解読できない．
2. 攻撃者は，通信路を“完全”に支配する，すなわち，攻撃者はすべてのメッセージを盗聴できるだけでなく，遅延させたり，不達にしたり，あるいは改竄・偽造したメッセージを送り込んだりすることができる．

ただし，2 でできる盗聴や改竄は，あくまで 1 に定める能力の範囲内のことのみである．たとえばもし，メッセージが暗号化されていて，かつその復号鍵を攻撃者が知らないならば，盗聴はできてもその内容まで知ることはできない．Dolev-Yao に基づくフォーマルな検証のためには，これら 2 つの仮定をフォーマルに定式化する必要がある．

仮定 1 の定式化には，主にメッセージ代数と呼ばれる方法が用いられる．メッセージ代数では，暗号化／復号化操作を enc, dec といった関数記号で表す．たとえば，123 を鍵 k で暗号化したものは $enc(123, k)$ という項になる．そして，たとえば単純な対称鍵暗号の場合，それらの性質を次のようなたった 1 つの等式で表現する：

$$dec(enc(x, k), k) = x$$

☆1 この研究は applied pi-calculus と呼ばれるプロセス計算に基づいているが，本稿でこれについての技術的内容を厳密に述べることはできない．以下の説明でプロセス計算といったら，彼らが用いた体系を本稿のために筆者が大胆に単純化したものであり，正確さに欠ける部分もあることをあらかじめご容赦願いたい．

0 ：何もしないプロセス
$P + Q$ ：プロセス P と Q を非決定的に選択して実行
$P \mid Q$ ：P と Q を並行に実行
$\bar{c}(d).P$ ：通信チャネル c へ値 d を送信
$c(x).P$ ：通信チャネル c から x の値を受信
$(\nu c)P$ ：新しい定数の生成
$!P$ ：replication，P のコピーを無限個生成（ループ構文の代わり）

図 -2 プロセス式のプリミティブ

同値関係 ≡（抜粋）

$$P \mid 0 \equiv P, P + P \equiv P,$$
$$(\nu c_1)(\nu c_2)P \equiv (\nu c_2)(\nu c_1)P,$$
$$!P \equiv P \mid !P$$

遷移規則（抜粋）

$$\text{COMM: } (\cdots + x(y).P) \mid (\cdots + \bar{x}(z).Q) \to P\{y := z\} \mid Q$$

$$\text{PAR: } \frac{P \to P'}{P \mid Q \to P' \mid Q} \qquad \text{STRUCT: } \frac{Q \equiv P \quad P \to P' \quad P \equiv Q'}{Q \to Q'}$$

図 -3 プロセス式の動作（構造操作的意味論）

これは直観的には“鍵 k で暗号化したものを同じ鍵で復号化すると元に戻る”ということを表現しているが，さらに，前提とする性質が上の等式のみならば，k と同値でない項を $enc(x, k)$ といかように組み合わせても x を作ることはできない．このことを，“k なしに $enc(x, k)$ を解読できない”ことに対応させるのである．ほかにも，たとえば公開鍵暗号の場合なら，秘密鍵から公開鍵への関数を記号 pub で表して $dec(enc(x, pub(k)), k) = x$ という等式を用いるといった具合に，さまざまな暗号要素技術がこの方法でフォーマルに定式化できる．

次に，仮定 2 の定式化では通信を伴うシステムの動作の記述方法が重要だが，一般には状態遷移モデルが用いられる．状態遷移モデルには，オートマトン，ペトリネット，プロセス計算などがあるが，ここでは文献 4）で用いられているプロセス計算を説明する．

プロセス計算とは，通信プロセスを記述するのに必要なプリミティブを代数の演算子として表現し，それら演算子を組み合わせることによって，代数的体裁の式として通信プロセスを記述することができる理論的体系である．プロセス計算のプリミティブとしては，図 -2 に示したものがある．プロセス式の動作は，構造操作的意味論と呼ばれるある種の推論体系によって定義される（図 -3）．

たとえば，通信チャネル c から暗号化されたデータ $enc(d, k)$ を送信して止まるプロセスは $\bar{c}(enc(d, k)).0$，c からデータを受け取って変数 x に格納し R という後続処理を行うプロセスは $c(x).R$，それらを並行に動作させたものは，

$$\bar{c}(enc(d, k)).0 \mid c(x).R$$

と書く．

プロセス計算をシステムの記述に用いる最大のメリットの１つは，合同性と呼ばれるプロセスの等価性に関する研究の蓄積を利用できることである．いまプロセス間のある等価性を≈で表すとすると，その等価性が合同的であるとは，$P \approx Q$ ならば，任意の文脈 $C[\ ]$（これもプロセス式で表現される）について $C[P] \approx C[Q]$ となることを言う．代数的な体裁の記述にこのような等価性が定まることを期待するのはきわめて自然であり，当たり前だと感じられるかもしれない．しかし，並行システムの記述においてそれが決して自明ではないことは，プロセス計算研究の初期からよく知られた事実であり，多くの研究がなされている．

この合同性は，セキュリティの記述にも役立つ．たとえば上に挙げた例で，攻撃者が鍵 k を知らないときに暗号化されたメッセージの内容が洩れないことは，プロセス計算でどのように定式化できるだろう？　この場合，合同性を用いて記述するために問題を次のように読み替える：データ d の代わりに他の任意の d' を使っても，いかなる攻撃者もそれを識別できない．これは以下の合同式で表現できる：

$$\begin{aligned} & (\nu k)(\bar{c}(enc(d,k)).\,0 \mid c(x).\,R) \\ \approx\ & (\nu k)(\bar{c}(enc(d',k)).\,0 \mid c(x).\,R) \end{aligned}$$

つまり，どういう攻撃者でもその動作がプロセス式で記述できるかぎり一種の文脈なので，合同性から識別できないということだ．ここで両辺を (νk) で囲っているのは，k を知っているとする範囲を限定し，攻撃者が k を知らないという条件を規定するためである．

では，匿名性やプライバシはどうだろう．たとえば電子投票システムでは，匿名性・プライバシに関する性質として，“どの有権者が，どの候補者に投票したか”という情報の秘密が守られることが期待される．仮にいま，有権者 v_1，v_2 がそれぞれ，候補者 c_1，c_2 に投票したとする．P を，投票者 x が候補者 y に投票する際の投票クライアントシステムの動作を表すプロセス式とすると，その投票状況は，

$$P\{x := v_1, y := c_1\} \mid P\{x := v_2, y := c_2\}$$

という式になる．さらに，それ以外の投票システム全体を S とすると，電子投票に期待される先の性質は，次の合同式で表すことができる：

$$\begin{aligned} & S \mid P\{x := v_1, y := c_1\} \mid P\{x := v_2, y := c_2\} \\ \approx\ & S \mid P\{x := v_1, y := c_2\} \mid P\{x := v_2, y := c_1\} \end{aligned}$$

ここでは先の性質を，“v_1，v_2 がそれぞれ c_1，c_2 に投票した状況と，それらの役割を入れ換えた状況とを，いかなる攻撃者も識別できない”と読み替えているわけである．

実際文献 4）では，上記のような合同式をプライバシと呼び，弱ラベル付き双模倣という証明技法を用いて，FOO と呼ばれる電子投票システムに関してそれが成り立つことをフォーマルに検証している．

●知識論理に基づくアプローチ

前節で紹介した，情報隠蔽をある種の識別不能性に読み替えて合同関係の形で定式化し，模倣証明技法で検証するアプローチは，セキュリティを記述する様式とそれを検証する方法をともに与えるという意味で，有用性が高い．実際，多くの検証ケーススタディがこのアプローチで得られている．しかし，問題がないわけではない．

１つの問題は，識別不能性に基づく定式化と，我々が思い描く匿名性・プライバシは，本当に合致しているのかということである．少なくとも，“法的な匿名性・プライバシ”の章で見たプライバシの定義と前節の定式化の間を埋めるのは，かならずしも容易な作業ではない．“攻撃者に . . . が分からない”といった性質を，もっとダイレクトに記述する方法はないだろうか．

もう１つの問題は，性質を記述した個々の等式自体が（前節の例では電子投票という）個別具体的なシステムに依存していることである．冒頭の章でも述べたように，一般性のあるメソッド構築のために，“匿名性自体”，“プライバシ自体”をもっと一般的な形で記述できないだろうか．

本節で紹介する知識論理に基づくアプローチは，上のような疑問に答えられる可能性を持つ．ここでは，代表的な研究である Halpern と O'Neill の研究[2] をもとに解説する．彼らは，セキュリティの“. . . が分からない”という性質を記述するために，知識論理という体系を用いる．知識論理とは，広くは様相論理と呼ばれる論理体系の１つであり，知っている／知らないを表現する様相オペレータを導入することで一般の述語論理を拡張したものである．

知識を表現するオペレータは K_i と書く．K は“know”の頭文字，i はその知識の持ち主を表す．たとえば，知識論理式 $K_i(Beautiful(rose))$ は，“バラは美しい，ということを i さんは知っている”を表す，といった具合である．知識オペレータに否定を組み合わせると，可能性を表現することもできる．たとえば，$\neg K_i \neg (Delicious(grasshopper))$ は，“バッタはおいしくない，ということを i さんは知っているわけではない”ということだが，言い替えれば“バッタはおいしいかもしれないと i は思っている”となる．このことから $\neg K_i \neg$ を possibility の頭文字を使って P_i と略記する．

知識論理の特長の１つは，その高い表現力によってさ

まざまなセキュリティ要件の微妙な違いまで書き分けられることである．たとえばHalpernらは，極小匿名性と呼ばれる性質を以下のように定式化した：

$$\neg K_j\,[\,\theta(i,a)]$$

ここで，$\theta(i,a)$は，“iさんがaというアクションを行った”ということ，つまり行為者と行為内容の結びつきだけを抽象的に表現する述語である．具体的な事例の匿名性を考えるときには，それに合わせてθの解釈を定めるとすることによって，個別具体的な事例に依存しない形で匿名性を定式化している．式全体の意味は，“iがaを行ったことを，jは知っているわけではない”である．

匿名性には，ほかにもいろいろなバリエーションがある．たとえば，“iがaを行ったとき，I_Aという集合の中の誰でもそれを行った可能性がある，とjは思っている”ということは，こんな風に書ける：

$$\theta(i,\ a) \Rightarrow \bigwedge_{i' \in I_A} P_j\,[\theta(i',a)]$$

この性質は，集合I_A中での匿名性と呼ばれている．$\theta(i,a)$という前提の必要性に関して，Halpernらは“疑われない性質”(unsuspectibility)との違いを指摘しているが，次章では別の側面にも触れる☆2．

ところで，上記の匿名性と，前節の最後に示した等式とはどういう関係にあるだろう．これに関しては，文献5)で議論されている．等式は，投票者v_1とv_2の役割が逆だったとしてもそれを識別できないということを表していたが，このような性質も知識論理で一般的に定式化できる：

$$(\theta(i,\ a\,)\wedge\theta(i',\ a\,')) \Rightarrow P_j[\theta(i',\ a\,)\wedge\theta(i,\ a\,')]$$

これは役割交換可能性と呼ばれている性質である．では，たとえば役割交換可能性から集合中での匿名性を導くことはできるだろうか？　厳密な証明は参照論文にあたっていただくとして，電子投票に即して直観的に言えば，I_Aとして“絶対に棄権しない有権者”の集合を取ればいい．知識論理による記述には，以上のように関係する性質の間の厳密な比較を容易にするメリットもある．

次に，プライバシについて考えてみよう．上と同じく文献5）に基づいて説明する．ここではHalpernらにならって，述語$\theta(i,a)$を使って定式化できるプライバシを考える．つまり，“公開を欲しない”という意図や“未だ知られていない”といった条件をあえて捨象し，行為者と行為内容の結びつきだけに着目してプライバシという問題の構造を表現することを試みる．このような設定では，行為者iのプライバシは，攻撃者に“iがどういう行為をしたか”が分からないといった性質になるが，これも匿名性と同様に知識論理でうまく表現できる．たとえば，“iがaを行ったとき，彼はアクションの集合A_Iの中でどれをも行った可能性がある，とjは思っている”という性質，すなわち集合A_I中でのプライバシは，以下のように書ける：

$$\theta(i,\ a\,) \Rightarrow \bigwedge_{a' \in A_I} P_j[\theta(i,\ a\,')]$$

この式は，先に示した集合I_A中での匿名性と対称的な形をしていることが見て取っていただけると思う．実はこの対称性は，ある種構造的なものである．たとえば，役割交換可能性から集合中での匿名性を導出できたように，役割交換可能性から集合中でのプライバシを導ける．再度電子投票の例で言えば，A_Iとして“絶対に1票は得票する候補者への投票”を取ればいい．しかも図-4のように，それら匿名性とプライバシの導出過程全体が対称的になっているのである．こういった対称性を数学ではしばしば双対と呼ぶ．つまりこのような見方では，匿名性とプライバシは双対だ，ということになる．

この双対性は，単にものの見方として面白いだけではなく，工学的な有用性も持つ．実は，同じく図-4で，上下の役割交換可能性は同一の性質である．なぜならば，役割交換可能性はそれ自身対称的な形をしているからだ．この性質に着目して，匿名性とプライバシの検証を効率良く行う方法を文献5)では示している．

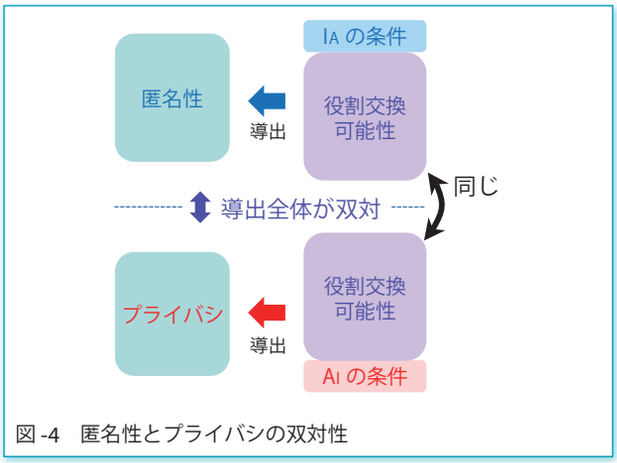

図-4　匿名性とプライバシの双対性

法的なプライバシふたたび

前節で紹介した，フォーマルに定式化された匿名性とその双対としてのプライバシを，法的なプライバシと比較してみよう．

いろいろな食い違いがある．たとえば，法的なプライ

☆2　極小匿名に同様の前提を追加してもその意味が変わらないことは，容易に証明できる．

バシは基本的に１つだが，双対としてのプライバシの方は知識論理の記述力を生かしてさまざまなバリエーションを記述し分けられることを特長とする．また，法的なプライバシには，“公開を欲しない”という意図や“未だ知られていない”といった条件が明示されているが，双対としてのプライバシではそれらは捨象され，具体的なプライバシを定める際のある種のパラメタとなっている．また，何かが公開されることと特定の攻撃者がそれを知ることとは，法的には違いがあるだろう．しかし，筆者がさらに大きな違いだと考えるのは，法的には匿名性侵害(厳密には個人の同定可能性)がプライバシ侵害の要件になっているのに対して，フォーマルな匿名性とその双対としてのプライバシとは対称的でむしろ対等だ，ということである．

この最後の食い違いに関しても，とりあえず，フォーマルな匿名性とプライバシの両方が成立する状況ならば法的なプライバシも保証されている，といった関係は成り立ちそうである．しかし逆に，法的なプライバシ侵害における同定可能性という要件は絶対なのだろうか．実際“法的な匿名性・プライバシ”の章で私事性に関しても見たように，プライバシの要件には変遷がある．専門家にうかがったところ，現在のところ同定可能性を要件から外した判例は存在しないとのことである．しかし一方，たとえば重度の皮膚病の医学写真などと関連して，高度にセンシティブな情報にかかわる場合は目線を入れて匿名にしさえすればいいとはいえないのではないか，といった議論もあるようだ．また，仮名の名寄せの例が現実に問題となるような社会状況になれば，要件の再検討が必要になるかもしれない．

しかし私事性と違い，同定可能性に関しては単に条件を外せばいいというわけではない．ある人のプライバシを広く保証することは，裏を返せばその他の人の知る権利を制限することになるが，同定可能性を単に外してしまうことは，法的なプライバシの範囲を過度に広げてしまう恐れがある．では，どうすればいいだろう？

以下はあくまで可能性としての議論だが，たとえば代わりに，公開された情報が確かに自分の情報であるということを証明できること，すなわち“自己情報証明”可能性を要件とするのはどうだろう．すなわち，私のプライバシ侵害に関して，他人から見てその行為の行為者たる私を同定できるかどうかを問題とする代わりに，私がたしかにその行為を行ったのだということをなんらかの方法で証明する，ということである．これは，法的なプライバシに関して近年注目されている自己情報コントロール権という考え方☆3 とも親和性が高いと思われる．また自己情報証明は，フォーマルな定義との対応もはっきしりている．実は，双対としてのプライバシの定義にある $\theta(i, a)$ という前提が成立することの確認に相当するのである．

繰り返すが，以上はあくまで１つの可能性としての議論であって，現実の法的なプライバシがかくあるべきだ，と述べているわけではない．実際たとえば，日本では匿名での訴訟が認められていないため，公にすることなく自己情報証明を行うことは現状の法制度では困難だ，といった問題もある．しかしながら，匿名性・プライバシのフォーマルな定式化が，法的な込み入った議論を見通しよく行うのに資する場合もある，ということを示す例ではあると筆者は考える．

☆3 公権力による情報の収集に対して，個人がそれらの情報をコントロール(開示，変更，消去など)できるという考え方．

おわりに

本稿では，匿名性とプライバシのためのフォーマルメソッド，とりわけそれらの定式化に焦点をあて，さらに妥当性や一般性を法律との対応を通して見てきた．法律とフォーマルメソッドとのこのような対応を議論することは，近年注目されている法令工学との関連でも重要となるだろう．他のセキュリティと比べて，匿名性とプライバシのフォーマルな研究の歴史は浅く，今後ますます発展していくことが期待される．

謝辞　筆者との拙い法律談義におつき合いくださり，また貴重な助言をくださった，岡村久道先生と壇俊光先生に感謝いたします．

参考文献

1) Chaum, D. L. : Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, Communication of the ACM, Vol.24, No.2, pp.84-90 (1981).
2) Halpern, J. Y. and O'Neill, K. R. : Anonymity and Information Hiding in Multiagent Systems, J. Computer Security, Vol.13, No.3, pp.483-514 (2005).
3) Hughes, D. and Shmatikov, V. : Information Hiding, Anonymity and Privacy : A Modular Approach, J. Computer Security, Vol.12, No.1, pp.3-36 (2004).
4) Kremer, S. and Ryan, M. : Analysis of An Electronic Voting Protocol in the Applied Pi Calculus, In European Symposium on Programming-ESOP 2005, pp.186-200, 2005. LNCS 3444.
5) Mano, K., Kawabe, Y., Sakurada, H. and Tsukada, Y. : Role Interchangeability and Verification of Electronic Voting, In 2006 Symposium on Cryptography and Information Security (SCIS'06)(2006).
6) 新保史生：プライバシの権利の生成と展開，成文堂 (2000).

(平成 20 年 3 月 25 日受付)

真野　健(正会員)
mano@theory.brl.ntt.co.jp
1989 年名古屋大学大学院工学研究科情報工学専攻修士課程修了．同年日本電信電話 (株) 入社．現在コミュニケーション科学基礎研究所主任研究員．項書換え系，プロセス計算，数理的技法による情報セキュリティの研究に従事．電子情報通信学会，日本ソフトウェア科学会各会員．