# フォーマルメソッドによるセキュリティ&プライバシ

つかだ　やすゆき　　まの　　けん
塚田 恭章　/真野　健
さくらだ　ひでき
櫻田 英樹

NTTコミュニケーション科学基礎研究所

**本稿では，電子商取引・電子政府・電子医療などのサービスを提供するICTシステムから，重要な個人情報やプライバシ情報が漏洩しないことを，フォーマルメソッド（形式手法，数理的技法）を用いて厳密に証明する手法について解説します．**

## 安心・安全なネットワーク・サービスを目指して

インターネット上で電子商取引・電子政府・電子医療などのサービスを安心して利用するためには，セキュリティやプライバシの十分な確保が不可欠です．そのためには，これらのサービスを提供するICTシステムが，セキュリティやプライバシに関する要件を正しく実現できているかどうかを，厳密に検証できなければなりません．NTTコミュニケーション科学基礎研究所では，数理論理学を応用したフォーマルメソッドと呼ばれる手法を駆使し，セキュリティとプライバシを厳密に検証する技術の研究を行っています．

## フォーマルメソッドにより高いレベルの安全性を

フォーマルメソッド（形式手法，数理的技法）とは，対象となるシステムを厳密に（フォーマルに）記述・解析・検証することを通じて，バグやセキュリティホールの混入を著しく減少させる高信頼化手法の総称のことです（**図1**）．通常のシステム開発においては，システムが満たすべき仕様やセキュリティ要件は日本語などの自然言語で記述されることが多く，自然言語特有の曖昧さに起因するバグやセキュリティホールの混入が避けられません．一方，フォーマルメソッドによるシステム開発では，仕様やセキュリティ要件を数式を用いて厳密に記述します．これにより，開発の初期段階で仕様やセキュリティ要件の不備を発見・修正することができるのです．さらに，より高いレベルの安全性を求める場合には，この厳密に記述された仕様やセキュリティ要件をシステム本体が満たすことの数学的証明まで作成します．証明作成を完全に機械化・自動化することは原理的に困難ですが，現在では定理証明器やモデル検査器と呼ばれるさまざまな計算機ツールが開発され，これらを活用することが可能となっています．

フォーマルメソッドによるシステム開発は，通常のシステム開発に比べてコストは倍増しますが，高いレベルの安全性を保証することができるため，産業界でも広まりつつあります[(1), (2)]．宇宙・航空・鉄道・電力などの分野で使用されるいわゆるミッションクリティカルシステム，あるいは私たちの暮らしに欠かせない社会基盤たるICカードの類，さらにはオペレーティングシステム・コンパイラ・通信プロトコルといった基本的なソフトウェアなど，特に高いレベルの安全性が要求される領域に，フォーマルメソッドは積極的に適用されています．標準化も進展して

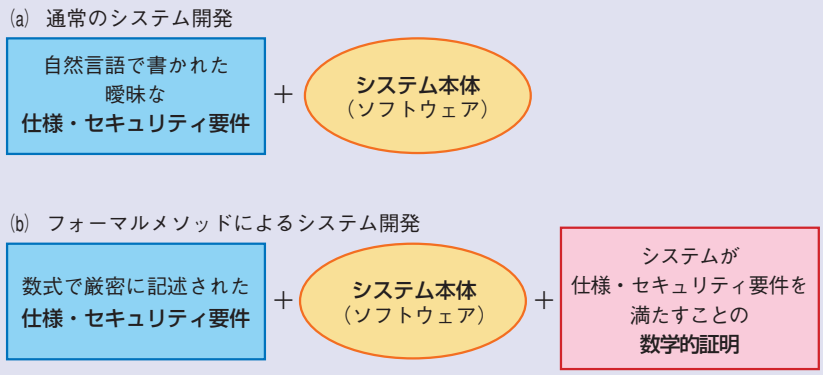


図1　フォーマルメソッドとは

おり，情報技術セキュリティ評価基準（ISO/IEC 15408）*1においてレベル5以上の高い評価保証レベルを達成するには，フォーマルメソッドの適用が不可欠になっています．

## プライバシのフォーマルメソッドへ

フォーマルメソッドは1つあれば足りるというものではなく，検証対象となるシステムの種類や検証したい性質に応じて適切な手法を開発する必要があります．秘匿性（秘密情報が第三者に漏れないこと）や認証（通信の相手が本物であること）といったセキュリティの基本性質は，世界中の研究者による1980年代からの研究の蓄積により，現在ではそのフォーマルメソッドがほぼ確立しつつあるといえます．

通信プロトコルを例にとると，セキュリティに関するフォーマルメソッドの代表的なものに，Dolev-Yaoモデル，BAN論理，帰納的手法，ストランド空間，spi計算などがあり，実際にさまざまな通信プロトコルのセキュリティ評価に利用されてきました[3]（**図2**）．例えば，Webブラウザに組み込まれ広く普及している暗号通信プロトコルSSL（Secure Socket Layer）の後継であるTLS（Transport Layer Security）プロトコルなどは，そのセキュリティがフォーマルメソッドによって数学的に証明されています．

一方，秘匿性や認証に代表されるセキュリティと比較して，匿名性やプライバシと呼ばれる性質は，個人情報保護の気運の高まりとともに近年急速に関心が高まってきた，いわば「新しい」性質であり，そのフォーマルメソッドは依然として研究段階にあります．中でもプライバシは，それをどう厳密に検証するかという問題以前に，どう厳密に定義するかという問題がいまだ十分には解決されていませんでした．NTTコミュニケーション科学基礎研究所では，システムの匿名性・プライバシをそれぞれ「誰が」「何をした」の情報が漏洩しない性質として対称的（もしくは双対的）に定義し，知識論理と呼ばれる数理論理学の枠組みの中で両者を統一的に検証する技術を開発しました[4]．以下にその概略を紹介します．

## プライバシを匿名性の双対として定式化

ICTシステムにおけるプライバシとはいったいどのような性質なのでしょうか．私たちは，いくつかの先行研究によってすでに定式化が得られていた匿名性を足掛かりに，この問題への解答を探ることにしました（**図3**）．

寄付を例に考えます．寄付を行った者が私なのか，太郎なのか，花子なの

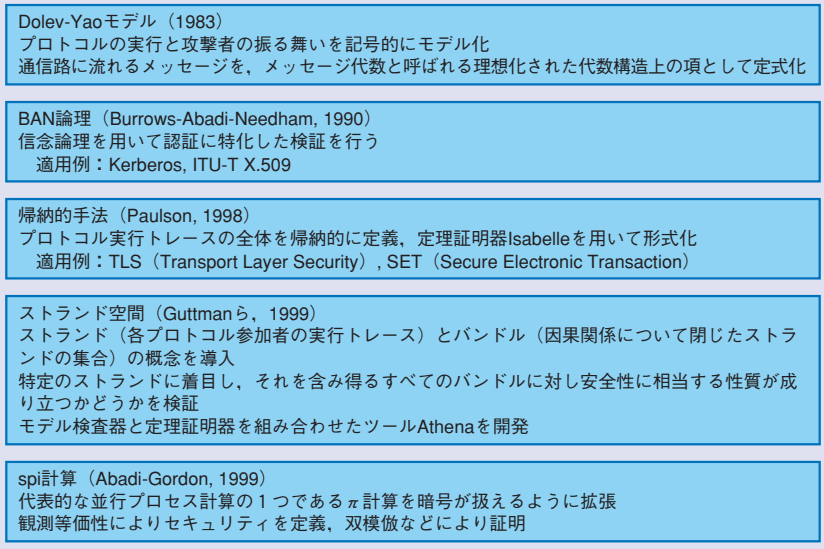


図2　通信プロトコルのフォーマルメソッド

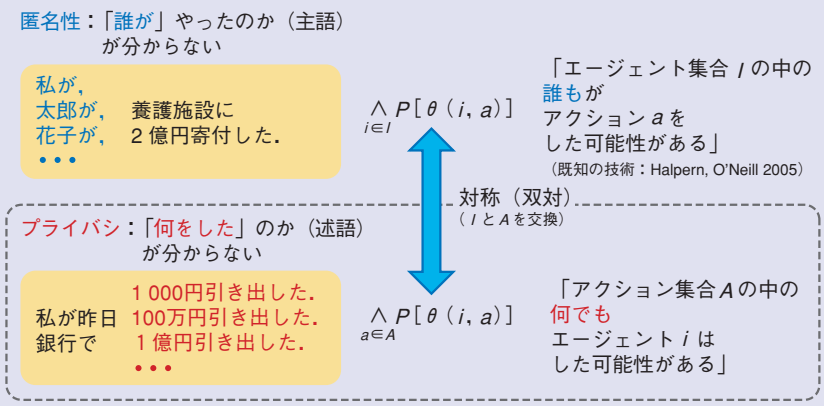


図3　プライバシを匿名性の双対として定式化

*1　ISO/IEC 15408：正式名称「情報技術セキュリティ評価のためのコモンクライテリア」．ICTシステムに対して，情報セキュリティを評価し認証するための基準を定めたもの．7段階の評価保証レベル（EAL: Evaluation Assurance Level）があり，上位3段階（EAL5～EAL7）にはフォーマルメソッドの適用が要求されます．

か分からないとき，その寄付は匿名であるといえます．言い換えますと，匿名性とは「誰が」の情報が漏洩しない性質であると一般的に定義できます．一方，私が昨日銀行で引き出した金額が1 000円なのか，100万円なのか，1億円なのか分からないとき，私の銀行引き出しに関するプライバシは保護されているといえるでしょう．すなわち，「何をした」の情報が漏洩しない性質がプライバシであると一般的に考えることができます．このように，匿名性・プライバシはそれぞれ「誰が」「何をした」の情報が漏洩しない性質として対称的にとらえることができます．

実は，HalpernとO'Neillの先行研究により，匿名性は知識論理と呼ばれる表現力の高い論理体系を用いて厳密に定式化できることが知られていました（図3）．私たちは，この匿名性の定式化の「双対」をとることにより，プライバシの厳密な定式化を得ることに成功しました．この定式化の一般性や妥当性についてはさらなる研究が必要と考えられますが，私たちもいくつかの視点から検討を重ね，法的なプライバシとの比較[5], [6]や，プライバシに関する標準的な分類学との対応関係[7]などについて考察を行っています．

## 役割交換可能性を介した証明手法

それでは，この互いに双対な関係にある匿名性とプライバシは，どのようにして厳密に証明することができるのでしょうか．私たちは，役割交換可能性と呼ばれる第三の性質を介して証明する手法を新たに考案し，それを代表的なインターネット電子投票プロトコルFOO[*2]の匿名性とプライバシの検証に適用し，その有効性を実証しました．

提案手法による検証の流れを，FOOへ適用した場合を例として説明します（**図4**）．

① まず，FOOの動作を状態遷移モデルとして記述します（**図5**）．FOOは，多くの投票者，選挙管理サーバ，集計サーバが，メッセージを送受信することにより，時々刻々と状態遷移していく系としてモデル化できます．

② 続いて，証明したい性質である匿名性とプライバシを，知識論理を用いて記述します．FOOの場合，匿名性は「誰もがその投票をした可能性がある」という性質に，またプライバシは「私がどの候補者にも投票した可能性がある」という性質になります．これらの性質を，図3の数式を用いて記述し

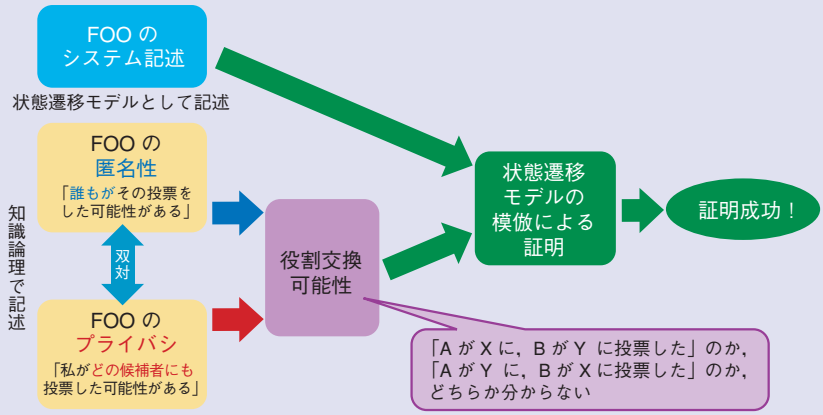


図4　役割交換可能性を介した証明手法（FOOに適用した場合）

$phase2(Ph, null)$
Precondition:
$phase = 1$
Effect:
$phase := 2$

$phase3(Ph, null)$
Precondition:
$phase = 2$
Effect:
$phase := 3$

$auth(i, Ad, req)$
Precondition:
$phase = 1 \wedge voter(i).authed = false \wedge$
$req = \sigma_i(voter(i).cand)$
Effect:
$voter(i).authed := true$
$abuff := pair(i, req) \text{-:} abuff$

For any $\Gamma$,
$ack(Ad, i, sreq)$
Precondition:
$phase = 1 \wedge pair(i, \Gamma) \in abuf \wedge$
$sreq = \sigma'_{Ad}(\sigma_i^{-1}(\Gamma))$
Effect:
$abuff := delete(pair(i, \Gamma), abuff)$
if
$voter(i).authed = true$
then
$voter(i).sreq := sreq$
fi

$cast(i, Co, svote)$
Precondition:
$phase = 2 \wedge voter(i).sreq \neq null \wedge$
$voter(i).casted = false \wedge$
$svote = \chi^{-1}(voter(i).sreq, voter(i).b)$
Effect:
$voter(i).casted := true$
$vbuff := svote \text{-:} vbuff$

$pub(Co, null, l, svote)$
Precondition:
$phase = 2 \wedge svote \in vbuff \wedge l = line$
Effect:
$vbuff := delete(svote, vbuff)$
$line := line + 1$
For any $\theta = 1, \ldots, vmax$,
if
$voter(\theta).casted = true \wedge$
$svote = \chi^{-1}(voter(\theta).sreq, voter(\theta).b)$
then
$voter(\theta).line := l$
fi

$key(i, Co, l, r)$
Precondition:
$phase = 3 \wedge voter(i).line \neq null \wedge$
$voter(i).keyed = false \wedge$
$l = voter(i).line \wedge r = voter(i).r$
Effect:
$voter(i).keyed := true$
$kbuff := pair(l, r) \text{-:} kbuff$

$vote(i, null)$
Precondition:
$phase = 3 \wedge voter(i).sreq \neq null \wedge$
$voter(i).line = null \wedge voter(i).finish = false$
Effect:
$voter(i).finish := true$

$vote(i, j)$
Precondition:
$phase = 3 \wedge voter(i).keyed = true \wedge$
$voter(i).finish = false \wedge$
$j = \xi^{-1}(\sigma_{Ad}^{-1}(\chi^{-1}(\sigma'_{Ad}(voter(i).cand), voter(i).b)),$
$voter(i).r)$

Effect:
$voter(i).finish := true$

図5　FOOのシステム記述（状態遷移モデル）

＊2　FOO：NTT情報流通プラットフォーム研究所の藤岡，岡本，太田（現電通大）が考案した電子投票プロトコル．ブラインド署名と呼ばれる暗号技術を応用することによって，実用的なインターネット電子投票を可能にしています．

ます．

③　匿名性とプライバシの対称性を利用し，これら2つの性質を役割交換可能性と呼ばれる第三の性質に帰着させます．FOOの場合，AとBを任意の投票者，XとYを任意の候補者として，役割交換可能性は，「AがXに，BがYに投票した」か，「AがYに，BがXに投票した」か，どちらであるか分からない，という性質になります．役割交換可能性も，匿名性やプライバシと同様に，知識論理の数式として記述することができます．役割交換可能性が成り立てば（ある条件のもとで）匿名性とプライバシが成立することが示せますので，役割交換可能性に帰着させるこの証明手法は，証明すべき性質を2つから1つに減らし，証明の効率化を達成しているといえます．

④　状態遷移モデルとして記述されたFOOの動作が，役割交換可能性を満たしていることを，状態遷移モデルの模倣（シミュレーション）と呼ばれる技法によって証明します（**図6**）．証明は部分的に機械化・自動化することが可能です．

⑤　状態遷移モデルの模倣による証明が成功した場合，FOOの匿名性とプライバシが保証されます．私たちは，この手法により，実際にFOOの匿名性とプライバシを厳密に証明することに成功しました．

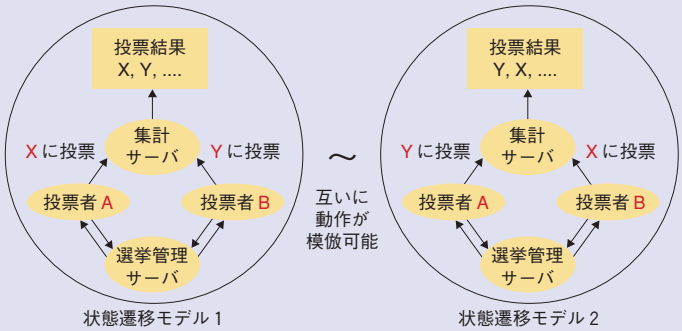


図6　状態遷移モデルの模倣による証明

## 今後の展望

今後は，提案手法の実システムへのさらなる適用を目指します．提案手法のコスト（証明に要する手間と時間）に見合うだけの，非常に高いレベルのプライバシが要求されるシステムの実例を，電子政府・電子商取引・電子医療などの領域に求めていきたいと考えています．

また，技術的にもさらなる検討が必要な重要課題があります．本提案手法を含め，これまでのフォーマルメソッドでは，証明の機械化・自動化のため，ベースとなる暗号は理想的である（すなわち，暗号は絶対に破られない）と仮定しています．しかし，この仮定は明らかに強すぎるものと考えられます．今後のフォーマルメソッドは，暗号の現実的な仮定（例えば，攻撃者が計算時間t内に暗号を破る確率は高々pである）を置いたモデルにおいても，証明の機械化・自動化を実現することが求められます．このような，いわば暗号理論に裏付けされた高精度のフォーマルメソッドは，近年世界的に活性化している研究分野となっています[8]．フォーマルメソッドの強力な検証技術を活用し，暗号理論的な強いセキュリティやプライバシを確立することにも，積極的に取り組んでいきます．

■参考文献


(1) http://www.nttdata.co.jp/dsf/index.html
(2) 特集：“フォーマルメソッドの新潮流，”情報処理，Vol. 49，No. 5，pp. 491-543，2008.
(3) 塚田：“数理的技法による安全性証明，”電子情報通信学会知識ベース，1群3編（暗号理論）10章，2010.
(4) K. Mano, Y. Kawabe, H. Sakurada, and Y. Tsukada: “Role Interchange for Anonymity and Privacy of Voting,” Journal of Logic and Computation，Vol.20，No.6，pp.1251-1288，2010.
(5) 真野：“匿名性とプライバシのためのフォーマルメソッド，”情報処理，Vol.49，No.5，pp. 530-536，2008.
(6) 真野：“プライバシ侵害に係る定義の検討における数理的表現方法の利用ー同定可能性の問題を中心としてー，”情報ネットワーク・ローレビュー，Vol. 9，No. 2，pp. 54-66，2010.
(7) Y. Tsukada, K. Mano, H. Sakurada, and Y. Kawabe: “Anonymity, Privacy, Onymity, and Identity: A Modal Logic Approach,” Transactions on Data Privacy，Vol. 3，No.3，pp. 177-198，2010.
(8) 萩谷・塚田：“数理的技法による情報セキュリティ，”共立出版，2010.



（左から）塚田　恭章／真野　健／
櫻田　英樹


フォーマルメソッドの可能性のさらなる探求を通じて，高いレベルのセキュリティとプライバシが要求されるサービスの実現に貢献していきたいと思います．


◆問い合わせ先
NTTコミュニケーション科学基礎研究所
協創情報研究部
情報基礎理論研究グループ
TEL　046-240-3635
FAX　046-240-4709
E-mail　tsukada.yasuyuki@lab.ntt.co.jp
URL　http://www.brl.ntt.co.jp/cs/souri-g/ja/dsc.html