匿名性とプライバシ保護の数理的技法

つかだ やすゆき　ま の　けん
塚田 恭章 /真野 健
かわべ よしのぶ　さくらだ ひでき
河辺 義信 /櫻田 英樹
NTTコミュニケーション科学基礎研究所

電子投票や電子オークションなどで用いられるセキュリティプロトコルが，匿名性（「誰が」の情報が漏洩しないこと）やプライバシ（「何をした」の情報が漏洩しないこと）に関する要件を正しく実現できているかどうかを，数理論理学・計算機科学の手法を駆使して厳密に検証する技術を紹介します．

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投票やオークションなどのサービスを安心して利用するためには，匿名性やプライバシの十分な確保が不可欠です．そのためには，これらのネットワーク・サービスで用いられる暗号通信プロトコル（セキュリティプロトコル）が，匿名性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，厳密に検証できるようになっていなければなりません．私たちNTTコミュニケーション科学基礎研究所では，数理論理学・計算機科学の手法を駆使し，匿名性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．これまでに，FOO（藤岡・岡本・太田によって1992年に考案された，大規模インターネット電子投票プロトコル）の匿名性とプライバシ（誰が誰に投票したかが第三者に漏れないこと）の検証に成功しています．

数理的技法により高いレベルの安全性を

安全性が厳密に保証された情報システムへの需要が急速に高まってきています．現在，政府機関が情報システムを調達する際には，セキュリティに関する信頼度の高いシステムの構築を図る観点から，情報技術セキュリティ評価基準（ISO/IEC 15408）に基づいて，評価または認証された製品を利用することが推奨されています．ISO/IEC 15408において5以上の高い評価保証レベルを達成するには，数理的技法（Formal Methods，形式的手法とも訳されます）の適用が不可欠になっています（**表**）．

数理的技法とは

一般に情報システムの開発プロセスは，実現したいことを整理して仕様を抽出し，それを具体化・詳細化することで所望の実現を得る過程としてとらえることができます（**図1**）．数理的技法は，これらの過程を，数理論理学や計算機科学の分野で蓄積された技術を用いて厳密に（フォーマルに）行うことにより，バグ（bug）の発生を減少させる手法です．数理的技法の適用により，開発の初期段階で仕様の不備を発見・修正したり，従来型のテストでは発見困難なバグを見つけたりすることが可能となります．その効果に注目が集まり，数理的技法を活用する企業が増えてきています[(1)]．

セキュリティプロトコルの完璧な設計は難しい

電子投票や電子オークションなど，個人情報をインターネットで扱うセキュリティプロトコルにバグがあると，「誰が投票したか」「誰が参加したか」などのユーザ情報がネットワークに漏洩し，悪用されてしまう危険があります．個人情報の漏洩を防ぐ基本技術として暗号がありますが，暗号が完璧でも個人情報が安全とは限らないことが，最近指摘されるようになってきました．例えばインターネットによる政党総裁選挙で，投票サーバが党員の投票のみ受け付け返答する場合，サーバからの「返答の有無」によって個人情報が漏れてしまうケースがあり得ます（**図2**）．このようなタイプの情報漏洩の可能性

表　情報技術セキュリティ評価基準（ISO/IEC 15408）

EAL1	機能テスト
EAL2	構造化テスト
EAL3	方式的テスト，およびチェック
EAL4	方式的設計，テスト，およびレビュー
EAL5	準形式的設計，およびテスト
EAL6	準形式的検証済み設計，およびテスト
EAL7	形式的検証済み設計，およびテスト

EAL（Evaluation Assurance Level：評価保証レベル）

まで考慮したプロトコル設計に，数理的技法は威力を発揮します．

数理的技法により通信パターンの正しさを検証

NTTコミュニケーション科学基礎研究所では，数理的技法を発展させ，セキュリティプロトコルの匿名性を「ある通信参加者の特定の動作が他の任意の通信参加者も行い得ること」として数学的に定義し，これを定理証明器上で帰納法によって検証する技術を開発しました[2]．本技術では，まずプロトコルの設計図を論理式に変換し，続いて匿名性の条件（匿名シミュレーション関係）をコンピュータで半自動的に証明します（**図3**）．これにより，「返答の有無」などの通信パターンの正しさを厳密にチェックし，匿名性を数学的に保証できるようになりました．帰納法に基づく本技術は，全探索手法に基づく従来技術と異なり，通信参加者の総数に上限を置くことなく検証可能であるという特徴があります．この特徴を生かしつつ，さらに確率的な匿名性も検証可能なように本技術を拡張する研究も行っています[3]．

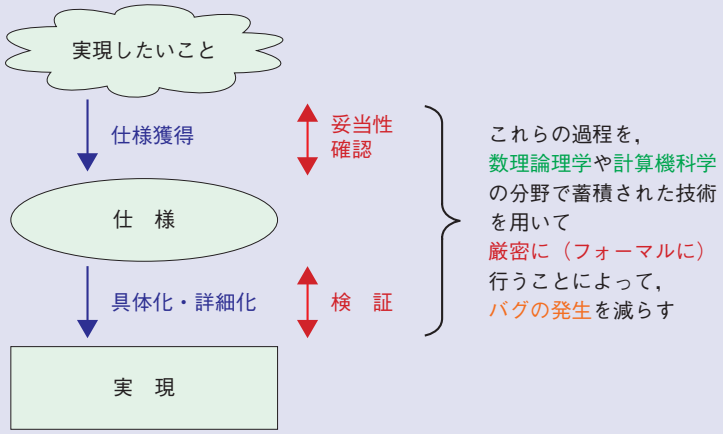


図1　数理的技法

インターネット電子投票プロトコルFOOの匿名性・プライバシ検証

本技術を用いて，インターネット電子投票プロトコルFOO（**図4**）の匿名性検証を行いました[4]．FOOは，ブラインド署名・ビットコミットメント・匿名通信路を主な要素技術とする複雑な3者間プロトコルです．本技術で匿名性を厳密に証明することにより強固なセキュリティをアピールし，競合プロトコルとの差別化にもつながると期待されます．特に本研究では，「投票しない有権者がいる」という現実的な仮定のもとで匿名性を検証しています．この仮定は自然なものですが，検証を複雑にするため従来研究では考慮されていませんでした．

一方，匿名性と関連の深い性質としてプライバシがあります．私たちは，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双対的に定義し，知識論理と呼ばれる枠組みの中で両者を統一的に検証する技術についても研究を進めています[5]．本技術を用いて，FOOの匿名性とプライバシを厳密かつ統一的に証明することができました．

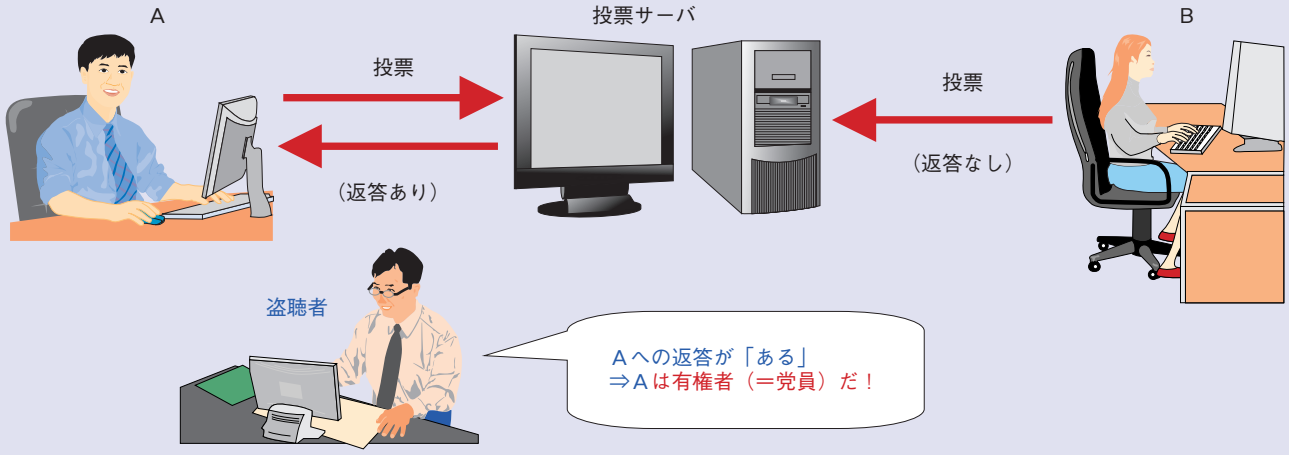


図2　「返答の有無」による個人情報の漏洩

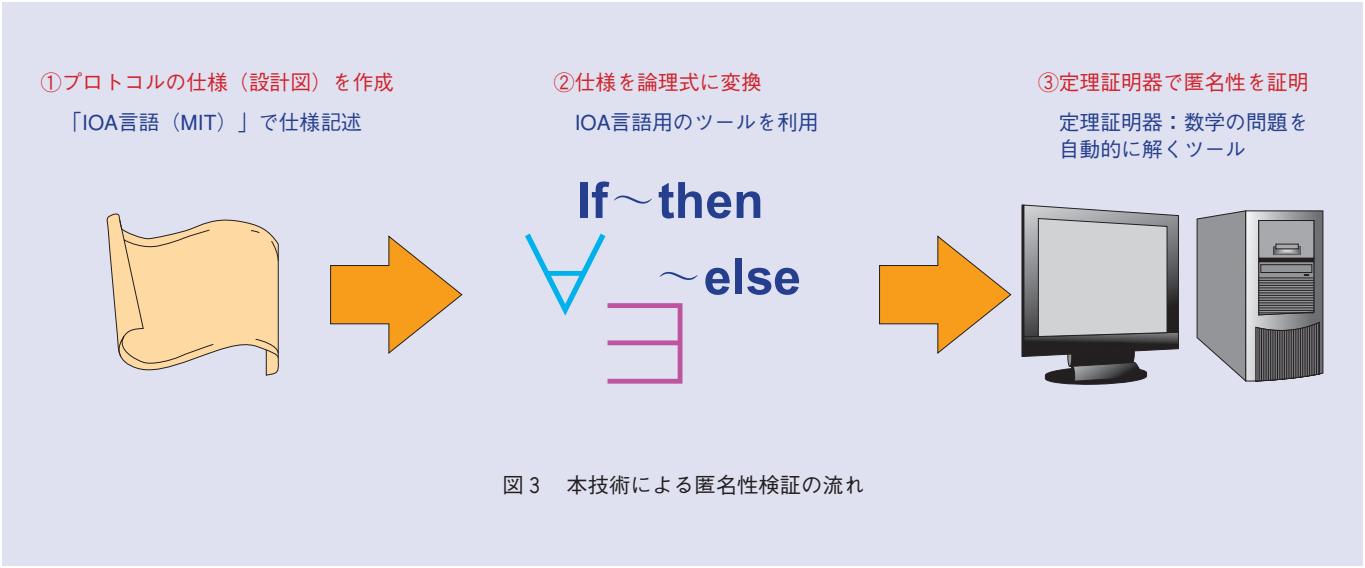


図3　本技術による匿名性検証の流れ

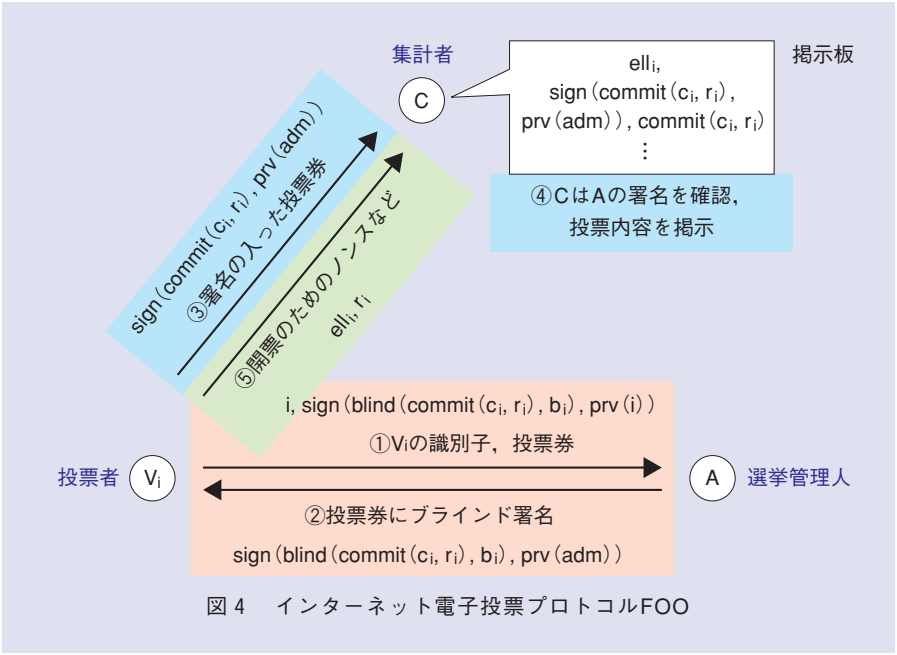


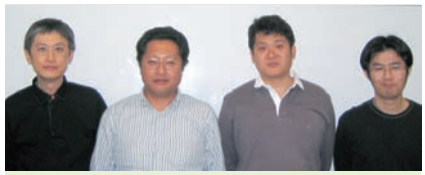
図4　インターネット電子投票プロトコルFOO

今後の展望

近年，数理的技法と暗号理論の境界領域の開拓が急速に進んでいます[6), 7)]．数理的技法の強力な検証技術を活用し，暗号理論に裏付けされた匿名性・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) 北郷：“特集：バグ・ゼロ目指し脚光浴びる「形式手法」，”日経コンピュータ，2006年7月24日号，pp. 60-64, 2006.
(2) Y. Kawabe, K. Mano, H. Sakurada, and Y. Tsukada：“Theorem-proving anonymity of infinite-state systems，” Inf. Process. Lett., Vol. 101, Issue 1, pp. 46-51, 2007.
(3) I. Hasuo and Y. Kawabe：“Probabilistic anonymity via coalgebraic simulations，” Proc. 16th European Symposium on Programming（ESOP'07），Springer LNCS, Vol. 4421, pp. 379-394, 2007.
(4) Y. Kawabe, K. Mano, H. Sakurada, and Y. Tsukada：“Backward simulations for anonymity，” Proc. Sixth IFIP WG 1.7, ACM SIGPLAN and GI FoMSESS Workshop on Issues in the Theory of Security (WITS '06), pp. 206-220, 2006.
(5) K. Mano, Y. Kawabe, H. Sakurada, and Y. Tsukada：“Role interchangeability and verification of electronic voting，” 2006年暗号と情報セキュリティシンポジウム，電子情報通信学会，2006.
(6) 萩谷・岡本：“数理的技法による情報セキュリティについて，”「数理的技法による情報セキュリティ」研究部会第2回研究集会，日本応用数理学会，2006.
(7) 真野・櫻田・河辺・塚田：“ゲーム列による安全性証明の形式化と自動化，”「数理的技法による情報セキュリティ」研究部会第2回研究集会，日本応用数理学会，2006.



（左から）塚田　恭章/ 真野　健/
河辺　義信/ 櫻田　英樹

数理的技法の探求を通じて，高度な安全性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
人間情報研究部
情報基礎理論研究グループ
TEL　046-240-3638
FAX　046-240-4709
E-mail　tsukada@theory.brl.ntt.co.jp
URL　http://www.brl.ntt.co.jp/cs/ninri-g/security/index-j.html