解説

プライバシー保護技術に関する最新動向

Technology Trend of Privacy Protection

土井　洋

Abstract

様々な情報が電子化され，パソコンやUSBメモリなどに格納されるようになっている．また，大量の情報がインターネット上を含む様々なところで活用されている．このように利便性が向上する一方，情報漏えいやプライバシー保護に関する問題なども表面化している．プライバシー保護を達成するためには，理論や技術だけではなく，システム化とその管理，法制度など，様々な角度からの取組みが必要となる．このうち，プライバシー保護技術については20年以上前から様々な概念が提案されており，その後の多くの改良の積み重ねの結果，より安全かつ高性能になり，実用化の研究が進みつつある．本稿ではプライバシー保護技術を，「情報とその発信者との結び付きを断つ技術」と，「情報を暗号化したまま活用する技術」に大別し，考え方を中心にできるだけ平易に解説する．また，最新動向と課題等についても述べる．

キーワード：暗号化技術，秘密分散，グループ署名，知識の署名，ミックスネット

1. はじめに

ここ数年，毎日のように個人情報漏えいの問題についてニュースなどで取り上げられている．その原因は多種にわたるが，紛失・置き忘れ，盗難を合わせると50%近くになるとの結果が報告されている[1]．このように様々な情報が漏えいする可能性があるという状況は，プライバシー保護の観点からは望ましくない．情報漏えい問題への対策の一つとして，暗号化の技術が古くから使われている．当然ながら，暗号化された情報を活用するタイミングでは一層厳重な情報管理が必要となる．

一方，電子化された情報とその発信者を結び付けることはそれほど容易ではない．実際，ネット上には様々な匿名掲示板が存在しており，そこでの誹謗中傷などによるトラブルも少なくない．この背景には，ネット上では相手の顔が見えないこと，発信者の匿名性が高いことなどがある．情報とその発信者の結び付けをサポートする技術の一つに電子署名技術があるが，電子署名付きの情報が与えられれば，だれでも情報とその発信者との結び付きを確認できてしまうため，プライバシー保護の観点からは好ましくない場合もある．

本稿では，プライバシー保護技術を，「情報とその発信者との結び付きを断つ技術」と，「情報を暗号化したまま活用する技術」に大別し，これらの考え方を中心に，プライバシー保護技術に関する最新動向を解説する．

2. 情報を秘匿する技術

情報漏えいに対する効果的な対策の一つとして，暗号化の技術が挙げられる[2]．情報を暗号化した状態で保存すれば，漏えいしたとしても，それは暗号化された状態であるので，復号しない限り情報を活用できなくなる．暗号化の方式は，共通鍵暗号方式と公開鍵暗号方式に大別できる．共通鍵暗号方式とは，暗号化と復号で同じ鍵を用いる方式であり，処理は高速で，例えばAES（Advanced Encryption Standard）は，現在広く使われている．現代の共通鍵暗号方式はアルゴリズム公開型であり，暗号化や復号のアルゴリズムは公開されている．また，暗号化を行う利用者Aと，復号を行う利用者Bは，秘密の鍵K_{AB}を共有していることを前提としている．そして，図1のように，鍵K_{AB}を用いて，暗号化と復号の

土井　洋　正員　情報セキュリティ大学院大学情報セキュリティ研究科
E-mail　doi@iisec.ac.jp
Hiroshi DOI, Member (Graduate School of Information Security, Institute of Information Security, Yokohama-shi, 221-0835 Japan).
電子情報通信学会誌　Vol.91 No.9 pp.792-797 2008年9月

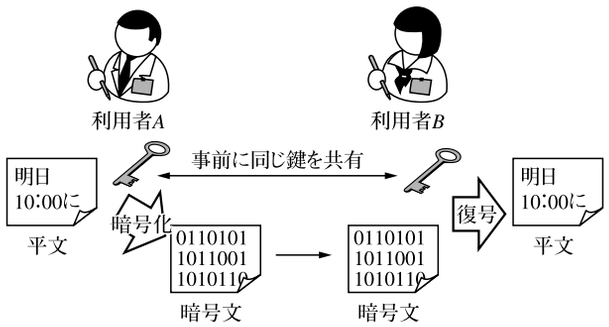

図1　共通鍵暗号方式

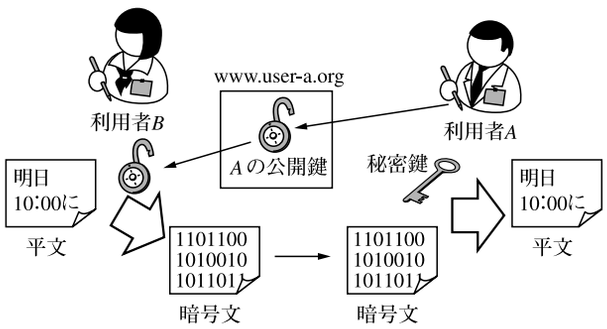

図2　公開鍵暗号方式

処理を行う．なお，利用者 A 及び C が暗号化通信を行う場合は（鍵 K_{AB} とは異なる）鍵 K_{AC} を共有しなくてはならない．このため，不特定多数のユーザの存在を想定する場合は，鍵を共有するためのプロトコルを互いに実行する必要がある．なお，パソコン上の情報を暗号化し，パソコンの利用者（多くの場合は一人）のみが復号できることを達成目標とするならば，鍵の共有問題は考えなくてよい． AES 等の共通鍵暗号方式を使う限り，鍵を利用することなく，暗号文から平文の情報を得ることはできないと考えてよい．

これに対して，公開鍵暗号方式は，暗号化と復号では異なる鍵を用いる．暗号化用の鍵を公開鍵と呼び，公開鍵 P_A はその名のとおり公開しても構わない．図 2 のように，直感的には，利用者 A が自分の公開鍵を自分のホームページに公開できることとなる．そして，公開鍵 P_A を用いてだれでも， A のみが復号できる暗号文を作ることができる．実際， A は秘密鍵 S_A を用いて復号できるが，第三者は秘密鍵 S_A を持っていないので，暗号文を復号できない．公開鍵暗号方式では，あらかじめ鍵を共有しておく必要がないため，インターネットのように不特定多数のユーザの存在を想定する環境に適した暗号方式といえる．このように使い勝手はよいのだが，暗号化や復号の処理性能は共通鍵暗号方式に比べて劣るので，現実的には，共通鍵暗号方式で用いる一時的な秘密鍵の送付等に使われる場合が多い．公開鍵暗号方式もアルゴリズム公開型であり，共通鍵暗号方式と同様に，秘密鍵を利用することなく，暗号文から平文の情報を得ることはできないと考えてよい．

さて，いずれの暗号方式も，安全性は鍵の適切な管理に依存するといってよい．実際，鍵が漏えいすれば暗号化の意味はなくなるし，鍵を失ってしまえば復号できなくなる．このような鍵の漏えいや紛失を解決する技術として，秘密分散方式がある．秘密分散方式の提案は 30 年近く前に行われたものであるが，その後も現在に至るまで様々な研究が行われている．また，最近は情報漏えい対策の方法の一つとしても研究がなされている．

目的　利用者のうち3人が協力すれば,秘密を復元できるようにする.

①$k=3$,秘密が$\underline{5}$の場合,定数項が5となるランダムな二次式を選ぶ.
②ユーザiには$f(i)$を渡す.
③3人が情報(例えば$f(1)$, $f(3)$, $f(4)$)を出せば,$f(x)$が一意に決まり,定数項を計算できる

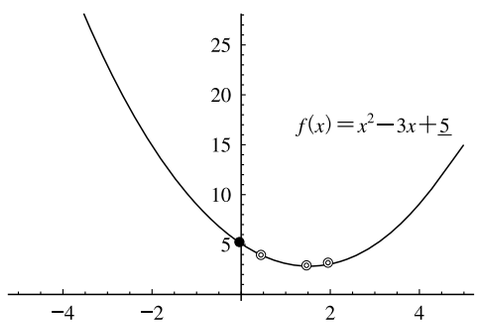

図3　Shamir の（k, n）しきい値法の原理

秘密分散方式の一つである Shamir の（k, n）しきい値法[3]は，管理者が秘密を分散し， n 人に配布する方式である．そして， n 人中任意の k 人が協力すれば秘密を復元することができる． Shamir の（k, n）しきい値法の場合， $k-1$ 人が協力しても，秘密に関する情報を全く得ることができない．秘密を復元するための基本的な原理は図 3 に示すように，「与えられた k 個の点を通る x の $k-1$ 次多項式の定数項を求めよ」という問題である．しきい値法は秘密を復元できる人数に関するパラメータ（k や n）を，そのシステムの管理体制等に応じて設定できるという点で興味深い．

なお，しきい値法の発展形であるしきい値復号法も，1990 年代以降，活発に研究されている．例えば，（k, n）しきい値復号法を用いると， n 人中 k 人が協力すれば，秘密鍵を復元しなくても与えられた暗号文の復号だけをできる．なお，異なる暗号文を復号するためには，再度 n 人中 k 人（以前協力した k 人とは異なってもよい）が協力する必要がある．

このように暗号方式や秘密分散方式を用いることにより，パソコンの紛失・盗難時の情報漏えいのリスクを低減させることは可能となる．

3. 電子署名とプライバシー保護

電子化された情報に対して署名を生成する技術を電子署名技術と呼ぶ．これは，公開鍵暗号方式で用いられる原理を利用することにより実現できる場合が多い．モデルは公開鍵暗号と同様で，公開鍵 P_A が公開されている．電子署名 σ は，署名者の秘密鍵 S_A と署名対象となる情報（以下，文書）M を用いて生成できる．図4に示すように，文書 M，電子署名 σ，公開鍵 P_A が同時に示されれば，文書 M に対して利用者 A が電子的な署名を行ったことをだれでも検証できる．なお，電子署名を生成した後に，文書 M が変更されていないことも検証できる．電子署名においては，署名者のみが所有する秘密鍵が漏えいしない限り，電子署名の偽造が不可能である．逆に，電子署名付き文書を示されたら，署名した事実を否定できなくなる．このように秘密鍵の管理が重要であるという点では，暗号化の技術と同様である．なお，現在では，電子署名及び認証業務に関する法律（いわゆる電子署名法）により，電子署名の有効性に対し，法的な根拠も与えられている．

電子署名の仕組みは，実名で情報発信を行う環境では極めて有効に働くと考えられる．例えば，発信権限を有する利用者の署名付き文書のみを掲示可能な掲示板を構築できれば，その掲示板において誹謗中傷などによるトラブルが発生した場合も，情報の発信者を確実に特定できることになる．なお，文書とその発信者の関連付けを行うために公開鍵が重要な役割を果たすので，秘密鍵の管理はもちろん，公開鍵の適切な管理も不可欠である．これは，PKI（Public Key Infrastructure）を用いて実現可能である．

その一方で，プライバシーの問題も発生し得る．例えば，ある特定の利用者が発信した情報を収集することにより，その利用者の趣味・し好を利用者が想定する以上に第三者が把握するといったことも可能となる．つまり電子署名付き文書が与えられると，文書と署名者の関連付けが完全になされることが逆に問題となる．このような問題点に対し，1980年代前半からプライバシー保護を意識した電子署名方式の研究が多数行われている．ブラインド署名やグループ署名と呼ばれるものがその代表であり，いずれも，署名者の匿名性を保証する特別な署名方式である．本稿では，グループ署名のみを簡単に解説する．グループ署名においては，署名生成可能な利用者のグループが設定されており，あらかじめ所定の登録処理を行う．そして，その達成目標は，図5に示すように

利用者Aは署名の検証のための公開鍵を公開している．
利用者Aが署名を生成し，利用者Bは（正確には，だれでも）署名の検証ができる．なお，第三者は署名を生成できない．

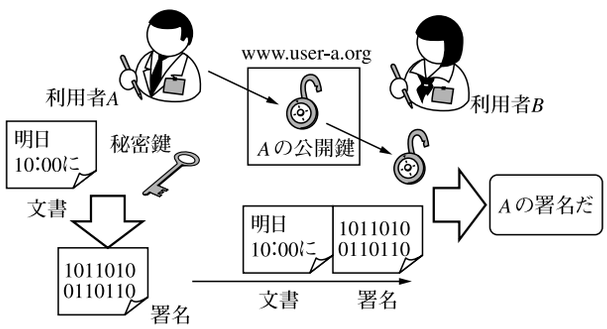

図4　電子署名方式

目的　ある利用者のグループが定められ，文書に対してグループのメンバーのみが署名生成が可能で，グループのメンバーのいずれかが署名を生成したことのみをだれでも検証可能とする．また不適切な情報発信に対しては，署名生成者を特定可能とする．

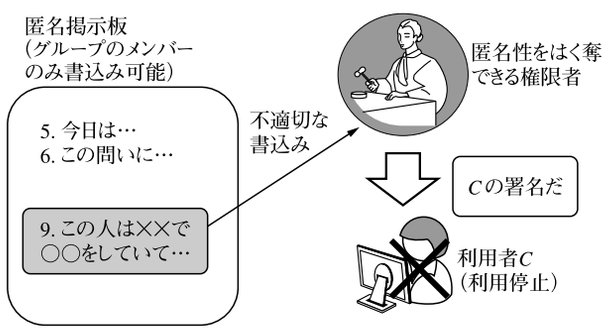

図5　グループ署名の機能（匿名性とそのはく奪）

① 署名を生成できるのはグループのメンバーに限られること
② グループのメンバーのいずれかが署名を生成したことを検証できること（署名者がだれかは分からないこと）
③ 特殊な手段により，匿名性をはく奪できること

である．最後の条件③は，例えば誹謗中傷などの不適切なグループ署名付き文書が発信された場合，その署名者がグループのどのメンバーであるかを，匿名性をはく奪できる権限者が特定できることを意味する．グループ署名では，2組の文書，グループ署名の対，すなわち（M_1，σ_1）及び（M_2，σ_2）が与えられた場合，これらが同一のユーザにより生成されたかどうかを知ることもできない．この性質をアンリンカビリティと呼ぶ．このような強力な機能を有するグループ署名を用いて，発信権限を有する利用者のグループ署名付き文書のみを掲示可能な掲示板を構築できれば，掲示された文書の発信者の匿名性を維持するとともに，誹謗中傷などが行われた場合に，署名者すなわち発信者を特定するといった運用も

可能となる．さて，グループ署名はこのように有用な機能を有しているが，署名長や署名生成コストが通常の電子署名と比較して大きいなどの問題があった．しかし，署名長や署名コストに関しては2000年以降様々な改良がなされている．また，フォーマルな安全性に関する議論も進んでいる．更に，グループ署名をはじめとする匿名性を有する署名について，リンカビリティの機能を制御できる方式などが提案されるなど，セキュリティ，プライバシー，利便性を両立させるような方式の提案もなされている．

なお，電子署名と相手認証には密接な関係があり，ここで挙げたグループ署名などの原理は，匿名性を有する相手認証の機能の実現にも適用できる．

4. 情報を秘匿したまま活用する技術

情報漏えいやプライバシー保護の観点からは情報を何らかの形で秘匿することが望ましい．しかしながら，情報は活用するために存在するものである．活用するために秘匿していた情報を復元するタイミングが存在するが，そこで情報漏えいが発生すれば情報を秘匿した効果がなくなってしまう．

これに対し，暗号化した情報を復号することなく，情報を活用するという方向性の研究も多くなされている．関係する研究の中で，ゼロ知識対話証明とセキュア分散コンピューティングについて解説する．いずれの研究も歴史は古く，基本的な考え方は1980年代前半に示されている．

ゼロ知識対話証明とは，我々が普通に連想する「紙に書いた証明」を拡張するものであり，

① 証明者と検証者による対話が発生すること
② 確率的な証明であること
③ 証明したい事実以外の情報は一切漏れないこと

という特徴が挙げられる．例えば公開鍵に対する秘密鍵の知識を証明者が有していると仮定する．ゼロ知識対話証明を用いると，証明者は検証者に知識を有していることのみを証明できる．公開鍵に対する秘密鍵の知識は，公開鍵を作成した利用者だけのものであるから，ゼロ知識対話証明を用いることにより，ユーザ認証を行うことも可能となる．更に，より複雑な知識に関する証明を行うといった応用も可能となる．

既に電子署名と相手認証には密接な関係があると述べた．実はある条件を満たすゼロ知識対話証明は，方式を若干修正することにより，対話，すなわちデータのやり取りをなくして証明者から一方的にデータを送る方式に変形することができる．また，そのデータに任意の情報(文書)を関連付けることが可能であることが知られている．このように変形した証明は，知識の署名とも呼ばれており，電子署名と同様に扱うことができる．例えば，「公開鍵に対する秘密鍵を知っていること」のゼロ知識対話証明は「情報(文書)と秘密鍵の知識を関連付けることができる」電子署名に変形できることになる．

さて，ここまで示した例では，秘匿したまま活用する情報は「秘密鍵の知識」という単純なものであった．これに対して，複数のエンティティが存在し，各エンティティが各々の秘密情報を秘匿しつつ，協力して秘密情報を利用した計算結果を出力することを考えよう．これは，秘密情報を秘匿しつつ結果を計算する方式をまず作り，次に各エンティティの計算が正しいことを検証可能とする仕組みを組み合わせることにより，構成できる場合が多い．

最も基本となるものは，入力を秘密としたままANDの結果，及びNOTの結果を計算することである．すべての論理回路は，ANDとNOTを使って構成することができることから，これらを繰り返し利用することにより，求める計算結果を得ることができるはずである．これについては，1980年代に肯定的な結果が得られている．

しかし，効率を考慮すると，ANDとNOTを繰り返し利用するよりも行いたい計算に特化した最適化が望まれる場合が多い．例えば，各エンティティが所有している秘密の数値の合計値を計算する場合について考えよう．この場合，以下のような準同形性を有する暗号化関数を用いることにより実現できる．$\mathbf{M}$，$\mathbf{C}$，$\mathbf{R}$を各々平文，暗号文，乱数の空間とする．暗号化関数を

$$E : \mathbf{M} \times \mathbf{R} \rightarrow \mathbf{C},$$

復号関数を

$$D : \mathbf{C} \rightarrow \mathbf{M}$$

とする．もちろん，$D(E(m_1, r_1)) = m_1$を満たす．また，平文空間での加算，暗号文空間での乗算を定義できるとする．この場合，準同形を有するとは，

$$D(E(m_1, r_1) \times E(m_2, r_2)) = m_1 + m_2$$

を満たすこととして定義できる．すると秘密の値の合計値の計算は，図6に示すように，

① 各エンティティiが所有している秘密の値m_iの暗号文$c_i = E(m_i, r_i)$を出力し，
② 出力されたc_iを掛け合わせた$S = \prod c_i$を作り，
③ 復号能力を有するエンティティが$D(S)$を計算し，結果を得る

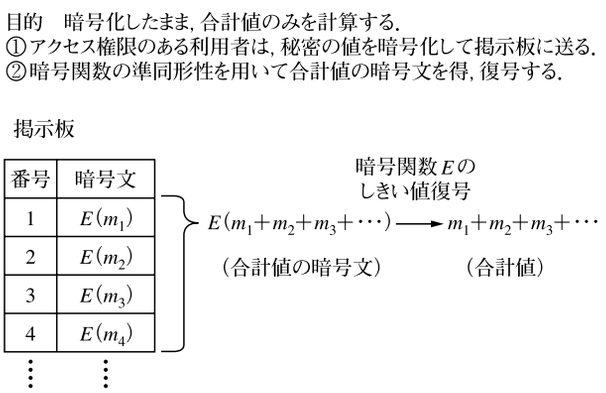

図6　暗号化したまま合計値のみを計算

ことにより実現できる．

なお，復号能力を有するエンティティが手順①で出力された暗号文を入手すると，エンティティiの秘密の値m_iを復号できてしまう．これを防ぐには2.で紹介した（k，n）しきい値復号が適用可能となるように，暗号化関数E，復号関数Dを設計すればよい．このような関数の例は幾つか知られている．

さて，これらの例のように，適切な暗号関数を利用すれば，情報漏えいを防止しつつ結果を計算する方式を構築することができる．これに加え，各エンティティの計算が正しいことを検証可能とする仕組みが必要である．この例では，手順①で得られた暗号文c_iを各エンティティが掲示板等に掲示するのなら，掲示板上で手順②を行うことにより，（秘密を用いる計算はないので）Sの計算が正しく行われたことをだれでも検証できる．手順③については，しきい値復号に協力するk人のエンティティが，所有する秘密鍵を用いて正しくしきい値復号の処理をしていることを，（秘密鍵を知られることなく）検証できる仕組みが必要となる．なお，①において，平文m_iの範囲が与えられている場合は，（平文m_iを知られることなく）平文m_iが与えられた範囲内であることを検証できる仕組みも必要となる．これらは，知識の署名を用いることにより実現でき，効率の良い知識の署名の構成方法も知られている．

5.　情報と発信者の関係を隠ぺいする技術

暗号化したまま情報を処理して結果を得る技術は，現在も様々な改良がなされている．しかし，複雑な処理を行う場合は，暗号化したまま情報を扱うよりも，一度復号して結果を処理する方が効率が良い場合が多い．匿名性を完全に保証できる通信路があれば，それを利用すればよい．現時点で，匿名掲示板などが存在し，匿名性を保ちつつ情報を発信することが可能といわれている．しかしながら，厳密な匿名性を求めることは容易ではない．厳密にするなら，情報とその発信者の関連付けを知られないようにする技術の一つである匿名通信路を用いる必要がある．

暗号研究における匿名通信路の代表例としてミックスネットが知られている．ミックスネットは，図7に示すように，複数の管理者から構成され，暗号化された複数の暗号文を入力，復号結果すなわち平文を出力とし，

① すべての管理者が結託しない限り，（もちろん何らかの数論問題が解けない限り）入力された暗号文と出力結果の平文の対応関係が分からないこと，
② 管理者が不正を行っていないことが検証できること

が設計目標とされる．条件②は，管理者により，データが不正に入れ替えられていないことなどの保証を求めるものであり，実はこの検証に要するコストは小さくなかった．しかし，最近様々な改良がなされた結果，性能

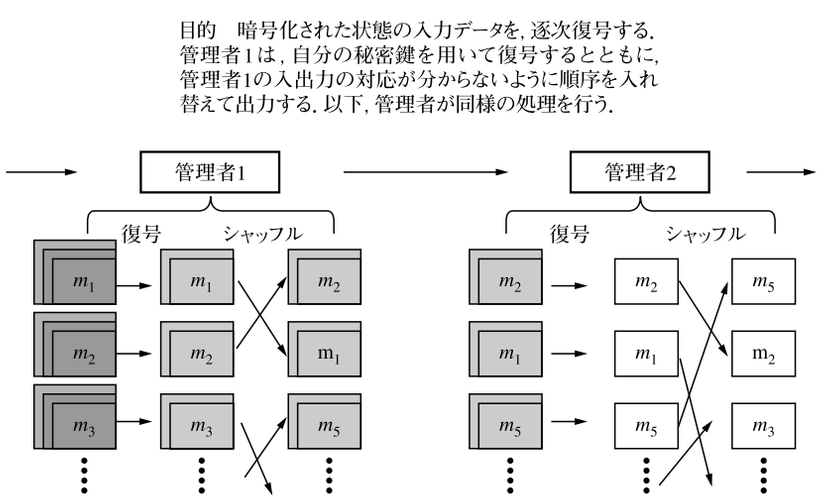

図7　ミックスネットの基本形

面でも実用に耐え得るものが開発されつつある．安全性については，既に説明したしきい値復号方式のように，システムの管理や運用の状況を考慮し，管理者数を適切に設定することにより，結託が事実上不可能となるように設計できる．

6. ま と め

本稿で解説した技術の多くのアイデアは 10 年以上前に提案されたものである．しかし，理論，実装両面での継続的な研究により，最近になって実用に耐え得るものが利用できるようになりつつある．

共通鍵暗号を用いた守秘技術や，共通鍵暗号と公開鍵暗号と組み合わせた守秘技術は，ファイルの暗号化，TLS などのインターネット上で通信を暗号化して送受信するプロトコルなどでよく使われている．秘密分散法を用いて，情報の秘匿を実現する場合は，その処理性能が問題となることが多い．これらに対しても，排他的論理和のみを用いて秘密を分散，復元する方法などの研究[4]も行われている．

プライバシー保護に関連する研究も注目が集まりつつあり，プライバシー保護に関する技術・アーキテクチャなどに関する総合的な研究[5],[6]が行われる一方，情報を秘匿したまま活用する技術（例えばプライバシープリザービングマイニング技術）が経済産業省の情報大航海プロジェクトの開発項目[7]として挙げられている．

また，秘密の数値の合計値を計算する方法や，匿名通信路を実現するミックスネット方式は，インターネットを利用した各自のパソコンから利用できる電子投票方式の基盤技術となり得る．ミックスネットを用いた電子投票は，コンピュータセキュリティシンポジウム CSS2007 においてデモ展示優秀賞などの，2008 年暗号と情報セキュリティシンポジウム（SCIS2008）において論文賞の投票[8]に，一部利用された．後者については，本学会の基礎・境界ソサイエティ機関誌 Fundamentals Review に詳細な解説論文[9]が掲載されているので，興味のある方は御参照頂きたい．

このように，プライバシー保護に関する技術は長年改良が積み重ねられてきたが，ついに実用化される段階に入りつつあると感じられる．しかしながら，理論に関する研究のほかにも，実際に使うためのライブラリー化やシステム化，具体的なアプリケーションに関する研究，法制度の研究など今後更に検討すべき課題も多い．プライバシー保護は，情報を安全に活用するために不可欠であり，重要でもある．今後も当該分野の研究，開発が継続的に，かつ活発に行われることを期待したい．

文 献

（1） NPO 日本ネットワークセキュリティ協会，2006 年情報セキュリティインシデントに関する調査報告書，Oct. 2007.
（2） 独立行政法人情報処理推進機構セキュリティセンター，情報漏洩対策のしおり ver.2, May 2006. http://www.ipa.go.jp:80/security/antivirus/documents/5_roei_v2.pdf
（3） A. Shamir, “How to share a secret,” Commun. ACM, vol.22, no.11, pp.162-163, Nov. 1979.
（4） 保坂範和，多田美奈子，加藤岳久，“秘密分散法とその応用，”東芝レビュー，vol.62, no.7, pp.23-26, July 2007.
（5） 小松文子，“プライバシ保護のためのアーキテクチャ，”情報処理，vol.48, no.7, pp.737-743, July 2007.
（6） 岡本栄司，“プライバシ保護のための要素技術の動向，”情報処理，vol.48, no.7, pp.744-749, July 2007.
（7） 経済産業省，情報大航海プロジェクト：共通技術，2008. http://www.igvpj.jp:80/tech_map/pdf/C-2.pdf
（8） 2008 年暗号と情報セキュリティシンポジウム（SCIS2008），開催案内，Jan. 2008. http://scis2008.cs.dm.u-tokai.ac.jp/
（9） 佐古和恵，森 健吾，“ミックスネットを用いた SCIS 論文賞電子投票実験について，”Fundamentals Review, vol.2, no.1, pp.48-57, July 2008.

（平成 20 年 5 月 7 日受付）

土井 洋（正員）

昭 63 岡山大・理・数学卒．同年日立ソフト入社．平 6 北陸先端大大学院博士前期課程了，平 12 岡山大大学院博士課程了．以後，暗号理論と情報セキュリティの研究に従事．中大研究開発機構を経て，現在情報セキュリティ大学院大学教授．博士（理学）．