プライバシ保護技術

大久保 美也子（おおくぼ みやこ）
ネットワークセキュリティ研究所 セキュリティアーキテクチャ研究室 主任研究員

大学院修了後、日本電信電話株式会社を経て、2010年、NICT入所。暗号アルゴリズムやプロトコルの研究に従事。博士（工学）。

はじめに

ネットワークの用途が日々変化し拡大をし続けている昨今、これまで対面もしくは書面でしか扱えなかった契約・取引・売買などの手続きもインターネットを介して行えるようになってきました。このように利便性の向上に伴い、ネットワーク上で不正なくこれらの手続きが行えるよう、意識して防御しなければならないことも増えてきています。また、近年では、インターネットを活用することにより様々な情報が入手可能となり、簡単にほしい情報を集めたり調べたりすることができるようになりました。その一方で、自分で気がつかないうちにプライバシに関わる情報を侵害されうる可能性も高くなっています。

このような状況を踏まえ、私たちの研究室ではネットワークを本来の効率性や利便性を損ねることなく、安全性とプライバシ保護機能とをフレキシブルに提供できる大規模認証基盤の実現を目指して研究を進めています。

ネットワークの利用用途の変化と求められる機能

ネットワーク上で不正行為が行われないようにするためには様々な要求条件が満たされなければなりません。例えば、契約の場合では、ネットワーク上で通信している相手が本当に契約相手本人か？ 電子データで送られてくる契約書の内容は通信の途中で改ざんされていないか？ 本人の意思確認が出来ているか（本人印のようなものが確認できる）？ などをチェックできる仕組みが必要になります。

一方で、個人的な内容を含む契約・取引・売買などの場合には、必要以上には個人個人のプライバシに関わる情報は漏らしたくないという要求が出てきます。例えば、電子オークションなどでは、応札の手続きを匿名で進めたいなどの要求が出てきます。また、電子投票などでは、有権者が投票を行う際に誰であるかが特定されてはいけない、立候補者の誰に投票したのかが識別されてはいけない、などの要求が出てきます。

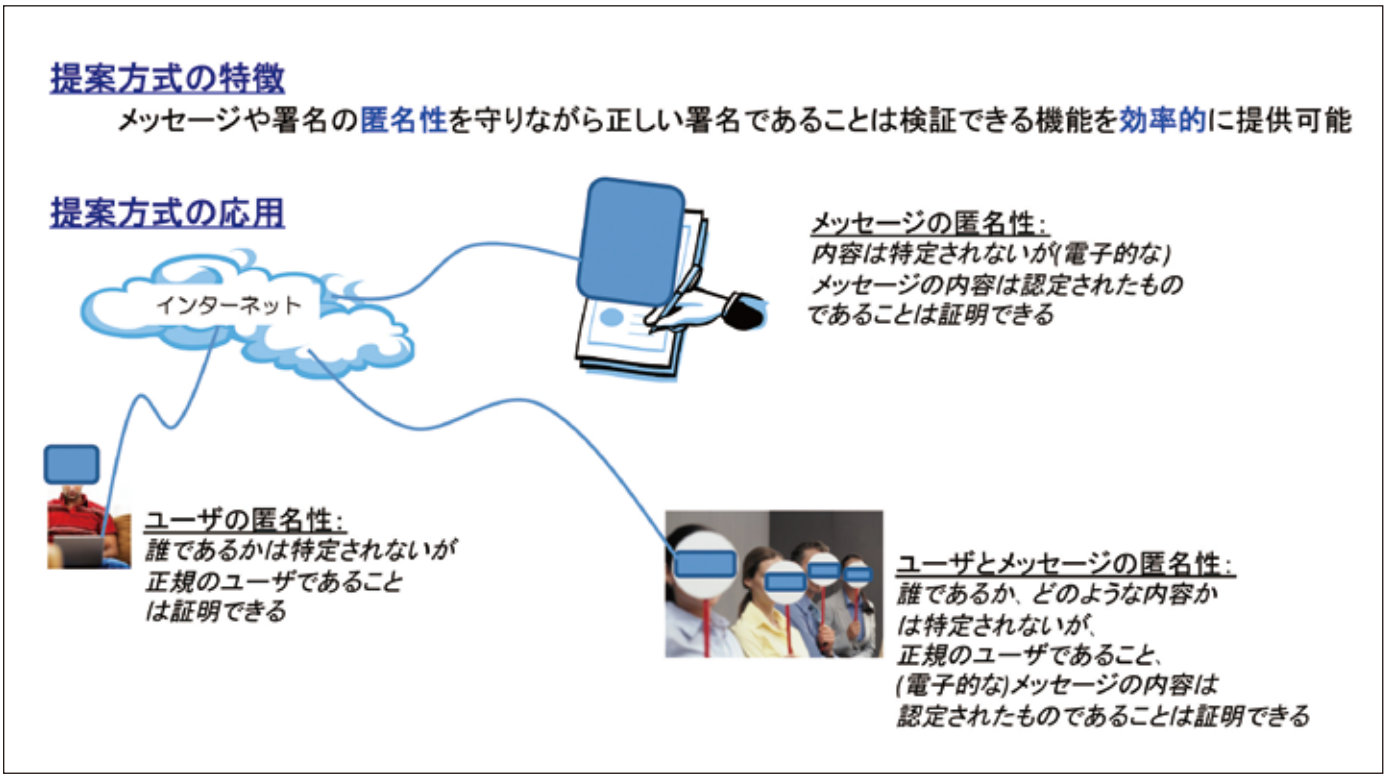
一見すると不正を防止し安全性を保つための要求条件とプライバシを保護するための要求条件が相反する要求事項に見えますが、暗号技術を活用することによりそれらの要求事項を両立させることができるようになります。

保護したいプライバシ情報は、ユーザごとに、また利用シーンごとに異なります。さらに大規模ネットワークへ多数の端末が接続するこれからのネットワーク上では、考慮すべき状況が複雑化・多様化します。同一ユーザであったとしても用いる端末やデバイスが異なる場合や異なるサービス間でユーザ情報の交換などが行われる場合など、起こりうる複合的な事象を全て踏まえた上で、守られるべきセキュリティレベルを保ちつつ個々のプライバシを保護されることが望まれます。例えば、複数のサービス間で同一ユーザであることが識別される必要がある場合、同一ユーザであることを識別されることがプライバシの侵害につながる場合等も出てきます。また、複数の異なるデバイスを用いていても、同一ユーザであることが識別されることによりプライバシ侵害などの可能性も出てきます。

ある用途や目的に特化し、保護すべきプライバシ情報を確定するようなシステム設計であれば、従来からある暗号技術などを複数用いることにより、ある程度構成することができます。しかし、目的が多様化し、また保護すべきプライバシ情報も画一的でなくなってきている昨今、それらの方向性の異なる要求事項を1つのシステムで実現することは困難もしくは構成することが出来たとしてもシステムの肥大化を招いてしまいます。

我々の目指す安全かつ利便性の高いセキュリティ技術

そこで私たちの研究室では、プラットフォーム上でのユーザおよびサービス提供側などの様々な要求条件にフレキシブルに応えられるプライバシ保護機能を備えた認証方法の提供を可能にする暗号技術を研究対象としています。



●プライバシ保護のための提案方式の活用イメージ

例えば1つのプラットフォームで、電子投票や申請システムやアンケートなどそれぞれの目的・保護したいものの要求条件に沿った機能を提供可能となる総合情報基盤を目指しています。

これらの実現により、コスト面では、1システム数百万から数億円かかる複数システムを1システム分のコストで提供することが可能となります。また、機能面では、1つのプラットフォーム上でユーザ・サービス提供側双方の安全性を保持した上で、個別ユーザごとの、またサービス提供者ごとの異なる要求事項や、ユーザの利用目的や提供サービスごとに異なる必要な機能などをフレキシブルに実現できるプライバシ保護機能を備えた認証の提供が可能となります。

具体的には、図に示すように、目的により異なるプロトコル（メッセージの内容を匿名にするブラインド署名、署名者のIDを匿名にするグループ署名など）を構成するために、それぞれのプロトコルを個別に構成するのではなく、1つのディジタル署名を活用することにより、両方のプロトコルの機能を同一のプラットフォーム上で提供することが可能となります。また、効率面では従来技術を複数用いた構成に比べ、システム全体としてのコンパクト化を実現でき、利便性についても、用途ごとへのフレキシブルな機能提供が可能となります。

今後の展望

ネットワークの利用用途は限りなく広がっていく可能性を秘めています。私たちの研究室ではその可能性を最大限に伸ばしていけるよう、セキュリティの技術を防御するためだけの手段として用いるのではなく、その可能性を促進する手段として活かしていきたいと考えています。

Column　様々な暗号技術の応用

暗号技術は、一般的には秘密にしたい情報を隠すためだけに利用すると思われがちですが、暗号技術を応用することで通信相手を確認する相手認証や、文章がある時刻に確かに存在したことを証明するタイムスタンプなどにも応用されています。

相手認証を行う方法は、IDとパスワードを用いる方法がよく見られますが、暗号技術を使う場合、暗号化のための鍵を秘密に持っていることを利用します。具体的には、一時的な乱数を送り、通信相手にその乱数を暗号化して送り返してもらいます。送り返してもらったデータが正しく復号できれば、相手は正しい鍵の持ち主、つまり正しい通信相手ということがわかります。

タイムスタンプを実現するには、文書にサインをするのと同じ機能を電子文書に実現する暗号技術である、電子署名を利用します。NICTのように正確な時刻を保持している機関（TSA: Time Stamping Authority）において、電子文書に時刻のデータを追加して、そのデータに対してTSAの電子署名を付与します。すると、電子署名を検証することで、その電子文書がどの時点には少なくとも存在したかを確認することができます。このサービスを電子公証とも呼びます。

近年では、ネットワーク利用者の行動などのプライバシを守りながら、電子データの正当性を保証するセキュリティ機能が重要になっています。本ページで書かれているプライバシ保護機能付き電子署名などは、その機能を実現する技術になります。