デジタルデータに「署名」を

情報システム学部　情報セキュリティ学科
福光　正幸　准教授

日常生活の中で、契約書・同意書などに押印・署名する機会が多々あります。インターネット上でデジタルデータを利用するにあたっても、本人の意思表示やデータの作成者の保証等のニーズは、物理的な紙面と同様にあります。これを実現する代表的なセキュリティ技術が「デジタル署名」であり、私たちは何気ない日常生活の中で知らぬ間に、これを活用しています。例えば、オンラインサービスを利用する際、アクセスしたアドレスが本物のサービス提供者によるものであるかの確認のため、この技術が使われています。図1は、「sun.ac.jp」が実際に長崎県立大学のドメインであることを保証する、デジタル署名を用いた証明書の画面です。また近年、FIDO（Fast Identity Online）・パスキーと呼ばれるパスワードなしでオンラインサービスにログインできる仕組みが普及し始めていますが、この仕組みの中でも利用されています。すなわち、デジタル署名は、インターネット上の本人保証のための必須技術です。

一方で、世界標準のデジタル署名は、量子コンピュータが完成すると、容易に偽造できてしまうことが知られています。そのため、米国国立標準技術研究所は量子コンピュータに耐性のある次世代署名の標準化を現在進めています。

また、デジタル署名の機能は年々進化しており、単なる本人保証の機能にとどまらず、多くの機能を有する「多機能署名」と呼ばれる技術が研究されてきています。例えば、個人ではなく団体を保証する、いわば「代表印」をデジタルデータに対し施すことができる「グループ署名」と呼ばれる技術もその一種です。その特徴は図2の通りです。

以上の背景から、現在次の観点で研究しています。

- 量子コンピュータに耐性のある多機能署名の設計
- 実社会で利用されているデジタル署名の理論的安全性評価
- デジタル署名の応用

図1:sun.ac.jpの証明書

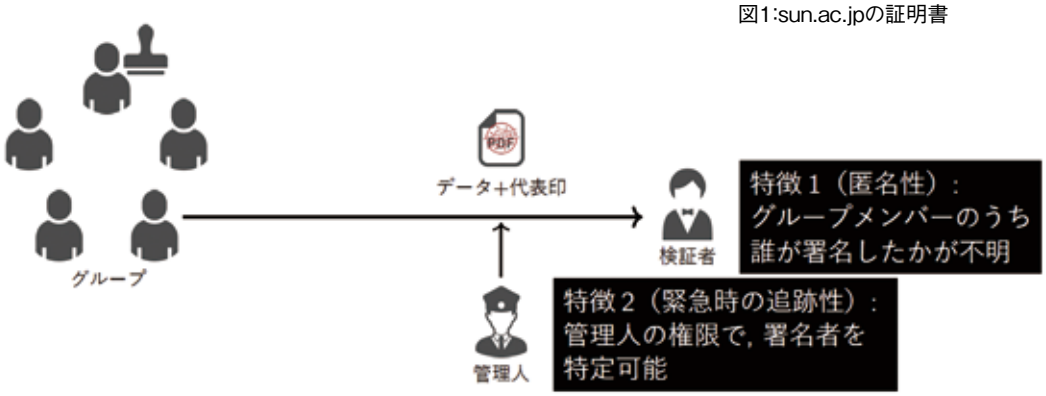

図2:グループ署名の特徴