2013 年 2 月 18 日
株式会社日立製作所

生体情報を用いた電子署名技術の開発に成功

ICカードやパスワードを用いずに公開鍵基盤（PKI）と同様の機能を実現

株式会社日立製作所(執行役社長:中西 宏明／以下、日立)は、このたび、電子署名の作成に指の静脈パターンなどの生体情報を用いることのできる、安全性を証明可能な電子署名技術を開発しました。本技術により、標準的な電子認証の仕組みである公開鍵基盤*1（以下 PKI: Public Key Infrastructure）と同様の機能を持つ情報セキュリティ基盤を、IC カードやパスワードを使わずに個人の生体情報で実現することができます。今後、国民 ID システムや電子行政サービス、電子決済サービスの拡大とともに、便利で安全な電子署名技術として、実用化をめざします。

なお本技術の一部は、総務省委託研究の「災害に備えたクラウド移行促進セキュリティ技術の研究開発」における研究成果です。

近年、拡大しつつある電子行政システムや企業情報システム、電子商取引の安全性を保つためには、なりすましの防止や電子文書の偽造・改ざんの防止が必須です。現在、このための情報セキュリティ基盤として、PKI が広く用いられています。PKI に用いられている電子署名技術では、「秘密鍵」を用いて電子文書に付与する電子署名を作成し、「公開鍵」を用いて電子署名を検証することで、電子文書の作成者の証明および偽造・改ざんの防止を実現します。しかし「秘密鍵」の管理には、IC カードやパスワードが利用されているため、盗難により他人になりすまされるリスクや、紛失や忘却により使えなくなる可能性がありました。仮に、指紋や虹彩、静脈などの生体情報を「秘密鍵」として利用できれば、IC カードやパスワードが不要になり、より便利で安全な PKI が実現できます。ところが、生体情報は、照明や気温などの環境条件や本人の体調などによって変動するアナログデータであり、取得する度に誤差を含みます。これまでの電子署名技術では、「秘密鍵」に誤差の含まれる情報を利用することができないため、生体情報を「秘密鍵」として利用できませんでした。

そこで今回日立は、生体情報のように誤差を含む情報を「秘密鍵」として利用することのできる、安全性を証明可能な電子署名技術を開発しました。開発技術を用いると、IC カードやパスワードを使わずに個人の生体情報に基いて、安心・安全な国民 ID システムや電子行政サービス、電子決済サービスを実現することが可能になります。

なお、本内容は、2013 年 1 月 22 日から 25 日まで京都府京都市で開催される「暗号と情報セキュリティシンポジウム(SCIS2013)」において発表しました。

■開発技術の詳細

（1）生体情報を「秘密鍵」とする電子署名方式

電子署名や公開鍵暗号などの暗号技術において、「秘密鍵」はデジタル情報として扱われるため、1 ビットでも誤ると正しく利用できなくなります。今回、「秘密鍵」に誤差を許容したまま署名を作成する技術と、署名の検証時に「秘密鍵」を秘匿したまま誤差を訂正することのできる技術を開発しました。これ

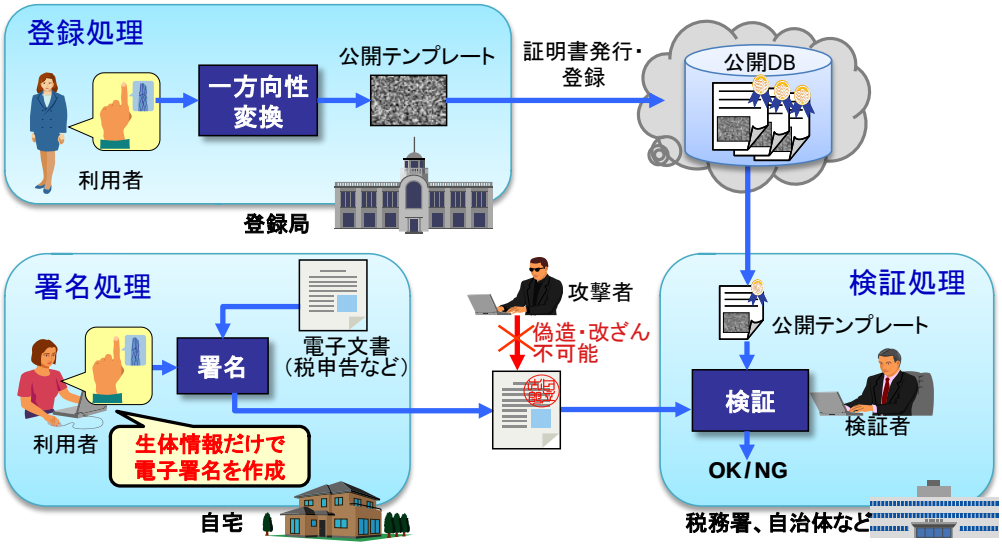
により、生体情報のように誤差を含む情報を「秘密鍵」として用いる署名の作成と、誤差を許容した署名検証を実現しました。

(2)安全性を数学的に証明

日立が今回開発した電子署名方式の安全性は、Waters署名*2と呼ばれる署名方式の安全性に帰着させることで証明可能です。そこで、仮に開発方式を破ることができるなら、Waters署名も破ることができるということを示しました。

Waters署名の安全性は既に数学的に証明されているため、これにより開発方式の安全性が証明されたことになります。

■生体情報を用いた電子署名の手順(テンプレート公開型生体認証基盤の概要)



■用語

*1 PKI (Public Key Infrastructure, 公開鍵基盤): 公開鍵暗号技術に基づいて、電子認証、電子署名、暗号の機能を提供する情報セキュリティ基盤。

*2 Waters 署名: 2005 年に Brent Waters が発表した電子署名方式。電子署名方式の安全性の定義として広く受け入れられている EUF-CMA (選択文書攻撃に対する存在的偽造不可能性)を満たすことが証明されている。

■照会先

株式会社日立製作所 横浜研究所 企画室 [担当:吉田]
〒244-0817 神奈川県横浜市戸塚区吉田町 292 番地
電話 050-3135-3409 (直通)

以 上