先端技術キーワード解説

知っておきたい最新の動き

[電子署名]

今月（2013 年 2 月）は、確定申告の時期です。国税庁は e-Tax（インターネットによる申告）を推進しています。この申告では、本人であること、改ざんされていないことを確認するために、電子署名が採用されています。この電子署名とは、どのようなものでしょうか。

１．電子署名とは

電子署名とは、電磁的記録（電子文書）に付与する電子的な徴証です。作成者本人の確認、及び、偽造・改ざんの防止のために用いられます。

２．電子署名の仕組み

（１）全体像

送信者（電子文書作成者）は、事前に「秘密鍵」と「公開鍵」を作成しておきます。そして、以下の図に示すように、「秘密鍵」を用いて電子文書と電子証明書を作成、送信します。

受信者は、「公開鍵」を用いて、「ハッシュ値の比較」を行い、電子証明書と電子文書の検証を行います。

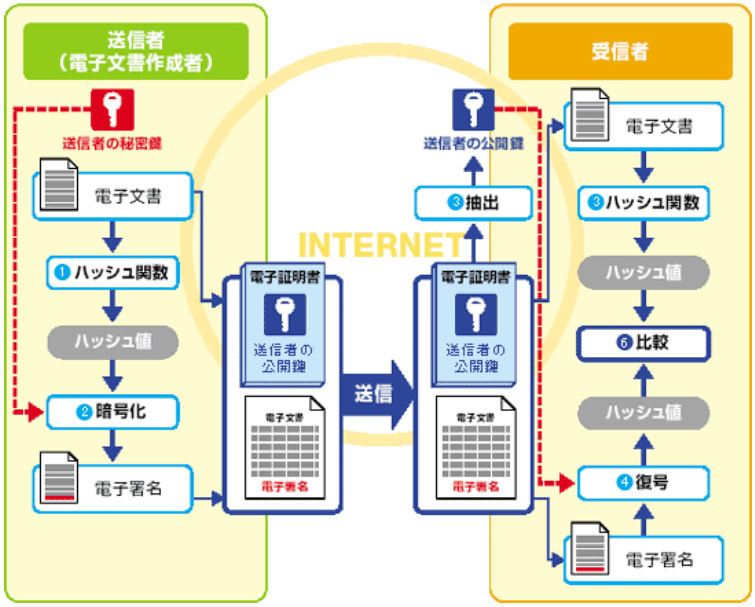

図１　電子署名の仕組み（文献 1）から引用）

（２）公開鍵暗号方式

電子署名では、公開鍵暗号方式を採用しています。これは、暗号化と復号とで異なる 2 つの鍵（「公開鍵」と「秘密鍵」）を使用する方式で、片方の鍵で暗号化したものは、それと対になるもう一方の鍵でなければ復号できないようになっています。

「秘密鍵」は、本人固有の鍵で厳密に管理されます。「公開鍵」は複数の受信者が利用します。

（３）ハッシュ関数

データの改ざんを容易に検知するための関数で、計算された値はハッシュ値と呼ばれます。ハッシュ値

は、元データ（電子文書）の長さに関係なく一定長のデータとなります。また、改ざんが行われると、値が大きく変わるため、容易に検知できます。

３．最近の動向

今月(2013 年 2 月)、日立製作所が秘密鍵に生体認証を用いる電子署名技術を開発したと発表しました。

現在、「秘密鍵」の管理には、IC カードなどが利用されています。このため、盗難、紛失などにより使えなくなる恐れがありました。これに対して、最も確実なのが生体情報（指紋、虹彩など）です。ところが、環境条件や本人の体調などによる変動（誤差）が避けられず、「秘密鍵」として使えませんでした。

これに対して、今回、「秘密鍵」を、誤差を許容したまま作成する技術と、検証時に「秘密鍵」を秘匿したまま誤差を訂正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できたとしています。

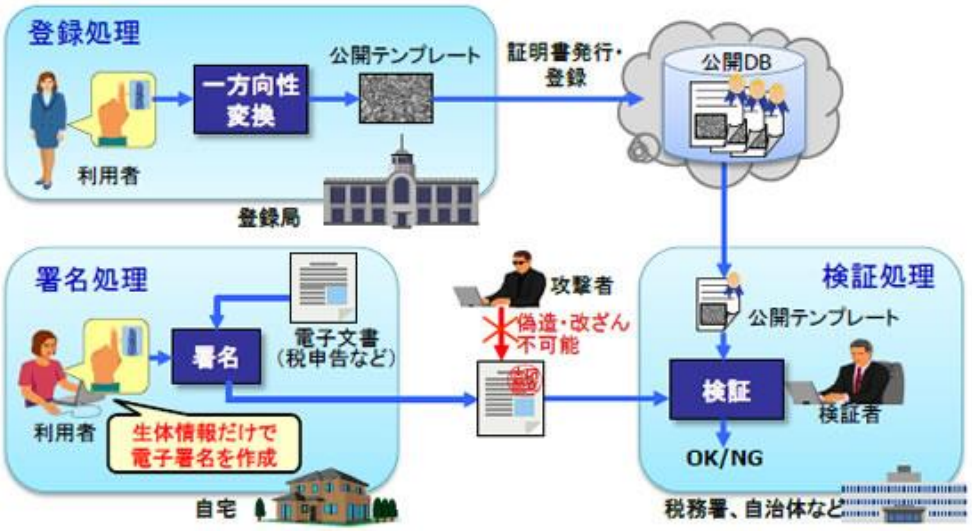

図２　生体情報を用いた電子署名の手順（文献 2）から引用）

電子署名は、税務申告に限らず、電子行政サービス、電子決済サービスの拡大とともに、利用が広がることが予想されています。さらに、技術の進展で電子署名はますます便利で安全になりそうです。

（参考文献、および一部、図を引用）

1) JIPDEC 電子署名・認定センター　http://www.jipdec.or.jp/esac/intro/shikumi.html　（図を引用）

2) 生体情報を用いた電子署名技術の開発に成功、日立製作所ニュース・リリース　（図を引用）
http://www.hitachi.co.jp/New/cnews/month/2013/02/0218.html　（2013 年 2 月 18 日）

（注）

本解説は、執筆当時の状況に基づいて解説をしております。ご覧になる時には、状況が変わっている可能性がありますので、ご注意をお願いします。

技術・経営の戦略研究・トータルサポータ
ティー・エム研究所
工学博士
中小企業診断士
社会保険労務士（登録予定）
代表　芳賀　知
E-Mail：info_tm-lab@mbn.nifty.com　URL：http://tm-lab@a.la9.jp/