2003-1-15

H. P. Report

第64号

発行責任者　稲崎義明

ｅ－Ｊａｐａｎの考察（６）

ネットワークを介して情報を取り合う場合、必要となるのが相手が本当に自分の相手なのかということです。この相手を確認するのが電子認証です。つまり、ネットワーク上でやり取りする情報の作成者が本人であるか、そしてその内容が改ざんされていないかを保証するものです。電子政府では、これまでの印鑑にあたる電子署名と、印鑑証明書にあたる電子証明書という技術が使われています。この電子証明書を発行し、その内容が正しいことを保証するのが認証局です。この技術は既に民間の電子取引などで利用されていますが、電子政府では、中央省庁、都道府県、各市町村などの自治体がこの認証局を用意して保証すことになっています。しかし、各自治体が認証局を持つことによって、同じネットワーク上に複数の認証局が乱立(都道府県だけでも４７の認証局がある)することになります。このままでは電子証明書を受け取ったところとしては、この証明書を発行した認証局がどこなのか判断できなくなります。そこで、ブリッジ認証局という認証局を総務省に設置することになっています。このブリッジ認証局と、各自治体の認証局の間で電子証明書を交換することによってお互いを信用できるようになっています。これですべての認証局が信用できることになります。一方ブリッジ認証局には、電子政府の枠組みに入る認証局すべての電子証明書が集まることになります。

電子政府における電子証明書は、行政側と申請側に分けることができます。行政側に割り当てられる電子証明書は、役職を証明するために使われます。つまり、役所の個人を保証するのではなく、役所の役職、「○○局△△課の課長」といったものを保証することになります。これは、公式文書が個人名で発行するのではなくて、こうした役職名の元に発行されるためです。この行政側の役職を証明するのは、中央省庁が設ける府省認証局や自治体の設ける行政向けの認証局です。一方申請側には企業と住民がありますが、企業側の認証は、法務省が設置する商業登記認証局があたります。これは、これまでの紙ベースの社印と法人登記をデジタル化したためです。住民の認証は、自治体が用意することになります。ここで利用するのが前回説明した住基カードです。実際は、住民票データを持っている市町村が設置する本人確認機関が本人であることを確認して、電子証明の発行依頼があれば、本人確認機関が認証局にそこで確認したデータを送り、認証局が電子証明書を発行することになっています。

住民が省庁に対して申請書を出す場合はどうなるかというと、まず作成した申請書に、その申請書をハッシュ関数というもので計算したハッシュ値(固定長のビット列)を、住基カードに記録された個人の秘密鍵で暗号化して電子署名として添付します。この申請書と、市町村の本人確認期間で発行された電子証明書(申請者証明書)を申請窓口へ送信することになります。電子証明書には、住民の公開鍵と証明書を発行した認証局の電子署名が入っています。受け取った省庁は、電子証明書の住民の公開鍵を使って申請書を復号し、復号化したデータと、申請書のハッシュ値が一致すれば、申請書は改ざんされていないことになります。また、鍵が一致することによって本人が書いたことも確認できます。次に、申請者証明書の認証局の電子署名を、普通なら発行した認証局に確認するところを、ブリッジ認証局に確認することで済ませることができます。つまり、どこからの申請であっても1つのブリッジ認証局に問い合わせればよいことになります。これで申請書は対処することができますが、戻ってきた書類は、同じ様にして官職証明書の確認を行うことになります。

（次回へ続く）

（情報誌トピックス）
○ＤＯＳ／Ｖｍａｇａｚｉｎｅ　２月１日号
特集　最強マザーの称号
→昨年後半から、ＦＳＢ３３３ＭＨｚ対応やＨｙｐｅｒ-Ｔｈｒｅａｄｉｎｇ対応の新ＣＰＵの発売などがあり、それに対応したマザーボードもオンボードにさまざまな機能を取り込んだりしている。現在最強のマザーボードはどれか。
特集　デスクトップオーディオ環境向上計画
→鳴っていればいいという時代から、５．１ｃｈ対応、サラウンド対応などＰＣのサウンド環境もちょっとしたことで格段によくなる。映画鑑賞、音楽鑑賞、ゲームプレイと場面を分けてサウンド環境の向上を検討する。
特集　ＢＩＯＳグッドナビ
→自動設定が進んでＢＩＯＳを意識することも少なくなったが知っているに越したことはない。ＢＩＯＳの基礎から設定メニューの解説、アップグレードまで。