電子政府ガイドライン作成検討会　セキュリティ分科会（第7回）
議事概要

1．開催日時：平成21年5月18日（月）　18：00～19：53
2．場　　所：内閣府別館9階会議室
3．出席構成員：
　辻井セキュリティ分科会主査、
　荒木構成員、宇賀構成員、國井構成員、小松構成員、佐々木構成員、中尾構成員、満塩構成員、
　遠藤構成員
（オブザーバー）（敬称略）
　安心・安全インターネット推進協議会/日立製作所システム開発研究所　洲崎
　セコム株式会社IS研究所　松本
（参加府省）
　総務省行政管理局　長屋行政情報システム企画課長
　総務省行政管理局行政情報システム企画課　北川調査官
　総務省自治行政局地域政策課　館補佐（代理）
　総務省自治行政局　井上地域情報政策室長
　総務省情報流通行政局情報流通振興課　新井情報セキュリティ対策室長
　法務省民事局総務課　上村補佐官（代理）
　法務省民事局　杉浦補佐官（代理）
　国税庁長官官房　古賀情報技術室長（代理）
　厚生労働省大臣官房統計情報部企画課情報企画室長　林分析官（代理）
　厚生労働省労働基準局労働保険徴収課　千葉係長（代理）
　社会保険庁総務部総務課　澤田情報企画調整室長
　経済産業省商務情報政策局情報経済課　三角情報セキュリティ政策室長

4．議事次第
　(1) 開会
　(2) バイオメトリクス認証について
　(3) 認証に関する検討事項について
　(4) 閉会

5．資料
　＜配布資料＞
　　資料1　生体認証技術のセキュリティ評価：誤受入率の意味
　　資料2　バイオメトリクスのセキュリティ

資料3　認証の位置づけに係る検討
資料4　公的個人認証サービス普及拡大検討会開催要領
資料5　電子政府における電子署名用と認証用のPKI証明書について

＜席上配布資料＞
参考資料1　セキュリティ分科会（第6回）議事概要

6．議事概要：

○資料1「生体認証技術のセキュリティ評価：誤受入率の意味」及び資料2「バイオメトリクスのセキュリティ」について説明が行われ、以下のような質疑応答が行われた。

・ 指紋情報自身を ID として使うことについては、毎回変化のある指紋のアナログデータの一意のデジタルデータへの変換や、母集団が大きくなると他人受入率が高くなるなど、現在のところ技術的に難しいところがある。
・ バイオメトリクスのオンライン認証への利用は、ISO の SC27 において検討されているところであるが、方法としては端末上でその端末が使える本人かどうかをバイオメトリクスで確認し、端末の機器認証と合わせて本人認証とする方法と、ネットワーク経由でバイオメトリクス情報を送信する方法の2通りが考えられる。いずれの場合においても、認証したい本人の身近なところにバイオメトリクスを入力するスキャナが必要になるので、急激な普及はないと思われる。
・ バイオメトリクスは、利便性に優れるが、本人も拒否される割合が高い印象。本人しか使わないものとして装置を微調整すれば誤拒否率を下げられるが、不特定多数のユーザが利用する装置の場合は調整が難しい。
・ セキュリティレベルに応じた認証方式という点において、個々のバイオメトリクス手法のセキュリティレベルについては情報があまり公開されないため、使う側が自ら判断しなければいけない状況であるが、使う側が何らかの基準を設け、それを満たすように機能を作り込んでもらうなどするとよいのではないか。
・ 現在、実際に利用されているバイオメトリクス認証は、外部からはどういう仕組みがわからないので評価できないが、保守的な分野で利用されているものは、なんらかの評価を行ったものであるのだろうと推測。先端技術であり、評価方法が定まっていないところはあるが、もう少し情報がオープンになり、アカデミックな議論ができればと思う。

○資料3「認証の位置づけに係る検討」、資料4「公的個人認証サービス普及拡大検討会開催要領」及び資料5「電子政府における電子署名用と認証用のPKI証明書について」について説明が行われ、以下のような質疑応答が行われた。

・ 法学的に署名、認証について特段定義されているわけではない。行政手続法により申請や届出という行政手続についての一般的なルールを定めたが、認証（本人確認）については特段定めておらず、個別の法律で定めている例があるだけ。行政手続の一環として考えていく必要があ

るかもしれない。

- 署名と認証の用途誤認リスクは、かつては可能性も無いわけではなかったが、ポリシーネゴシエーションやプロトコル、ユーザインタフェース等の実装上の工夫により、今は殆ど無い。認証のメカニズムを悪用した攻撃により、署名の安全性が損なわれる可能性はあるかもしれない。
- 署名と認証のキーを分けるというよりは、セキュリティ評価の観点、つまり実装がどうなっているかが重要ではないか。ただし、署名システムや検証システムの実装についてのルール化や標準化はほとんどされていないのが現状である。
- 日本では、「電子署名」という用語が法律、技術などさまざまな場面で異なる意味で使われているため議論が混乱している印象がある。韓国では法律用語として電子署名や電子証明書について、「公認電子署名」と「公認証明書」といったように使い分けをしており、用語の意味を明確にするためにも何かしらの法的な整備が必要であることは理解できる。
- 電子署名法の推定効について、署名の効果がある・なしの議論はしたが、諸外国ではレベル分けがあり、ゼロイチの世界ではなくて、複数レベル感をもつことで社会に柔軟にあわせていくことも重要。
- 署名と認証を使い分けている海外事例において、利用者は実際に意識した上で使い分けているのか。

  →電子署名については、利用者が実印かどうか分からないとなれば、電子署名の否認防止としての効果はそもそもなくなる。否認防止が不要であれば、実印である必要もないので、分ける必要はない。例えば（IC カード上で署名用と認証用の証明書を使い分けている）ベルギーでは、電子署名する際には、画面上に、法律的な意味のある署名であるが、というダイアログが表示され、PIN 入力による署名文書へのユーザの同意を求めている。一方、認証の場合は、いったん本人が PIN を打つと、あとは勝手にどんどん署名を返す作りとなっている。電子署名に対するリテラシーの向上を目指すか、あるいは否認防止を不要とするかは、どんな社会とするかのコンセプトの問題となる。コンセプトの合意形成が必要で技術論ではなくなる。
- 署名のポリシーとして、何のために署名するのかを明らかにすることや、それらの目的に応じて署名する側と検証する側の間でどの認証局の証明書を承認することとするか、といったコミットメントルールを規定しないと、きちんとした仕組みはできない。また、これは認証の場合でも同様。

以上