情報セキュリティと仕様のオープン性に関する課題
－「IC･ID カードの相互運用可能性の向上に係る基礎調査」から－

セコム(株) IS研究所
JNSA PKI 相互運用技術 WG リーダー　松本　泰

ICカードのセキュリティの高さの根拠として、よく耐タンパー性などが説明されます。しかし、耐タンパー性や、ICカードで利用されている暗号のアルゴリズム等は、非常に重要な要素ではありますが、それらが評価されているからICカードは安全というのはかなり危ない発想です。それらにより何が保護されているか、どのように保護されているかといったことへの理解がより重要です。
ICカードを使った安全・安心なIT社会といったことがよく喧伝されていますが、その割にはICカードと、そのICカードを取り巻く技術は十分に知られておらず、情報セキュリティの専門家にも広く理解されているとは言いがたい面があります。
十分に知られていない理由のひとつに、ICカード自体や、ＩＣカードを利用する環境などに関して、セキュリティ上の理由として、その仕様が広く公開されていないことがあります。そもそも情報セキュリティの専門家にもあまり理解されていないものが、安全・安心なIT社会の基盤技術になるといったことがあり得るのでしょうか。
本稿では、IPAのサイトで公開された「IC・IDカードの相互運用可能性向上に係る基礎調査」に基づき、こうした問題の背景を探ってみることにします。

1. はじめに

独立行政法人 情報処理推進機構 セキュリティセンター（IPA/ISEC）の公募に、NPO JNSAの応募が採択された「IC・IDカードの相互運用可能性向上に係る基礎調査」の「調査報告書」が、2007年1月にIPAのサイトで公開されました。IPAのサイトでは、この調査を以下のように紹介しています。

> ICカードを利用し個人等を識別するIC・IDカードは、今後オンラインでの各種サービ等をセキュリティ面で支える社会インフラに成長する兆しを見せている。しかし、そのためには、クライアント環境や製造ベンダー等の違いによりサービス分野等をまたがっての利用に技術的な制約を受けない、相互運用可能性の確保が必要である。
> シーズ調査では相互運用可能性を実現する標準化動向や海外の取組みにおける技術体系の事例を、またニーズ調査では現在のIC･IDカードにおける相互運用可能性の実態と今後への展望を調査し、今後国内でIC･IDカードの相互運用可能性の向上に必要になる、国際標準を活用した関連技術の標準化やツール開発、普及方策の検討を行った

調査報告書のシーズ編においては、IC・IDカードの相互運用可能性(Interoperability)の課題を説明するため、フィンランドのFINIED、ベルギーのBELPIC、米国のPIVの3つのIC･IDカードの技術仕様を事例研究として取り上げています。これらの3つの事例を選択した理由は、技術仕様がオープンであることにつきます。FINEIDとBELPICは、日本の住基カードと公的個人認証サービス、米国のPIVは、国家公務員身分証明書ICカードに近いと考えられますが、公的個人認証サービスも国家公務員身分証明書ICカードも、調査報告書で説明しているレベルのIC･IDカードの技術仕様は、ほとんど何も公開されて

いません。従って、調査報告書で取り上げている3つの事例と同等レベルの技術的な説明を、これらのカードで行なうことはできません。

IC･IDカードに関して､｢仕様をオープンにすることで、安全・安心なIC・IDカードの普及を図る｣というアプローチと､｢仕様をオープンにしないことで、安全・安心なIC・IDカードを実現する｣という一見相反するとも思えるふたつの考えが根底にあるように思えます。

何が正しいかはともかくとして、今後の情報セキュリティにおいて重要なコンポーネントとなる可能性があるIC・IDカードの技術やアーキテクチャは、正しく理解される必要があります。本稿は､｢国家公務員身分証明書ICカードと米国のPIVの比較｣､｢公的個人認証サービスとベルギーのBELPICの比較｣を説明することにより、以下の観点を考察して見ることにします。

(1) 情報セキュリティと仕様のオープン性
(2) 政府調達と民間の情報セキュリティビジネス
(3) カード内の鍵に関する仕様

2. 国家公務員身分証明書 IC カードと米国の PIV の比較

米国においては、政府機関全体を対象とするセキュアで信頼性のある身分証標準を規定する大統領指令(HSPD-12｢連邦政府職員と契約業者の共通識別基準のためのポリシー｣)が2004年8月に発効されています。このHSPD-12により、各政府機関は、米国国立標準技術研究所(NIST)が策定したFIPS-201(｢連邦政府職員及び契約業者の個人識別情報の検証｣)に準拠するカード(PIVカード)の発行が義務付けられることとなりました。各政府機関は、このPIVカードの発行を2006年10月27日までに開始しています。FIPS-201の準拠性は、このPIVカードだけではなく、関連する様々な周辺装置やサービスにも要求されます。

PIVカードについては、関連した大量の技術ドキュメントが公開されています。また､PIVカードアプリケーション、PIVミドルウェアの認定制度であるNPIVP(The NIST Personal Identity Verification Program)があり、これらは､｢調査報告書｣で詳しく説明しています。

米国PIVと国家公務員身分証明書ICカードを比較すると下の表のような感じになります。

PIVは、米国の安全保障を達成する上で｢仕様をオープンにすることで、安全･安心なIC･IDカードの普及を図る｣というアプローチを取っていると言えます。逆に日本の国家公務員身分証明書ICカードについては､｢仕様をオープンにしないことで、安全・安心なIC・IDカードを実現する｣ため限定した範囲で使用するというアプローチに見えます。

比較項目	PIV	国家公務員身分証明書ICカード
配布対象	連邦政府職員と契約業者	国家公務員
配布枚数	2000万枚が予定されている	不明
プラットフォーム対応	規定なし	規定なし
IC･IDカードをサポートするミドルウェア	仕様、テスト仕様が公開されており認定制度がある ミドルウェアのレファレンス実装なども公開されている	不明
カードエッジI/F	NIST SP800-73	非公開 ※1
カード内のデータモデル	NIST SP800-73	非公開
格納されるEE（End Entity)証明書	認証用の証明書 署名用の証明書(Option) 暗号用の証明書(Option)	規定なし

※1 公的分野における連携ＩＣカード (http://www.kantei.go.jp/jp/singi/it2/others/iccard.html) の公的分野における連携ＩＣカード技術仕様（改定）に非常にアバウトなものがある。

3. 公的個人認証サービスとベルギーのBELPICの比較

BELPIC（Belgian Personal Identity Card）はベルギーの電子政府プロジェクトの一環として始まった国民IDカードのプロジェクトです。プロジェクトは2002年末より開始されており、パイロットプロジェクトを経て、2005年の9月からは新規に発行されるIDカードがすべてBELPICのカードとなっています。2009年末には12歳以上の全国民への配布を終える見込みを立てており、2006年10月の時点では400万枚を超えるカードが発行されています。ベルギーのBELPICと公的個人認証サービスを比較すると下の表ような感じになります。

比較項目	BELPIC	公的個人認証サービス
配布対象	12歳以上の全国民	15歳以上の希望者
配布枚数	400万枚（2006年11月現在）	18.3万枚（2006年10月末現在）
プラットフォーム対応	Windows,Mac,Linuxに対応	Windowsのみ Macの対応が一部なされている
ミドルウェアとユーティリティ	オープンソースが多く利用されており、専用ソフトのソースコードも数多く公開されている	バイナリコードを無償で配布
カードエッジI/F	カードエッジI/F	公開
7816-4,8に準拠		非公開
カード内のデータモデル	公開 PKCS#15に基づく	非公開
格納されるEE証明書	否認防止用の証明書 認証用の証明書	否認防止用の証明書のみ

BELPICで驚かされることのひとつに、政府が公認しているBELPICを利用するミドルウェアやアプリケーションの多くが、オープンソースとして公開されていることがあります。これは、BELPIC自体の仕様がオープンであることにも関係しています。BELPICは、「仕様をオープンにすることで、安全・安心なIC・IDカードの普及を図る」というアプローチだと言えます。公的個人認証サービスは、国家公務員身分証明書ICカードほどクローズドでないにせよ、「仕様をオープンにしないことで、安全・安心なIC・IDカードを実現する」というアプローチに見えます。

4. 情報セキュリティと仕様のオープン性

BELPIC、PIVは、「仕様をオープンにすることで、安全・安心なIC・IDカードの普及を図る」というアプローチを取っているといえます。技術仕様をオープンにすることにより、相互運用可能性の問題等が広く技術者等に理解されれば、これらの相互運用可能なIC・IDカードを使った環境が整備されて行く結果となります。BELPIC、PIVは政府主導のプロジェクトですが、いずれ、民間ビジネスにも波及して行く可能性もあります。広く利用されればコストが下がり、それがまた利用を促進し、結果として、IC・IDカードを使った安全・安心なIT社会を構築するといったアプローチになります。

我が国において、公的個人認証サービスの普及が問題になっています。そもそも使い道がないから普及しないとか、そんなものいらないといった議論もあるかと思います。

公的個人認証サービスの普及について、技術的な問題ではないと言う意見が大半かと思います。しか

し、本質的には、技術的な不透明さも問題点のひとつではないでしょうか。技術的な不透明さは、論理的な理解の不足となり、何がベストプラクティスなのかという議論を困難にするだけでなく、プライバシー問題、セキュリティ問題に対して脅威を煽るだけの議論や、感情的な議論に終始してしまう結果となっているように思います。

調査報告書では、BELPIC、PIVの事例を説明していますが、これらは全て公開された情報に基づいて記述しています。少なくとも日本の公的個人認証サービス、国家公務員身分証明書ICカード等では、ここまでの情報は公開されていません。これらの仕様の入手などには機密保持契約の締結などが必要になります。これは「仕様をオープンにしないことで、安全・安心なIC・IDカードを実現する」というアプローチです。こうしたアプローチの問題点は、技術が広く理解されないことにより、相互運用可能性の問題解決を阻害し、それが、安全、安心を提供するとされているIC・IDカードの普及の阻害要因となっているかもしれないという点にあります。次に説明する政府調達等においては、適正な競争を阻害するといった可能性もあります。

5. 政府調達と民間の情報セキュリティ

米国連邦政府におけるIT関係の調達は、民間のビジネスをドライブすることも念頭においているように思われます。これは、国家のIT戦略とも言えます。米国のPIVに関しても、幅広い技術仕様の公開、認定制度と、その認定製品の調達と言った調達のフレームワークを整備しており、民間のビジネスを育成する狙いも感じられます。それに対して、公的個人認証サービス（のICカードとしての仕様）、国家公務員身分証明書ICカード等では、その仕様のほとんどは公開されておらず、それぞれの用途に閉じています。行政関係の調達と言うビジネスがあっても、民間の情報セキュリティビジネスにとって規範となるようなものは提供していないと言えます。

PIVの仕様であるFIPS-201、SP800-73と言った技術文書は原案段階においても公開されているのですが、この原案に対して80を超える個人と組織から1900以上のパブリックコメントが寄せられています（http://csrc.nist.gov/piv-program/FIPS201-Public-Comments.html）。こうしたことは、PIVの相互運用可能性の課題を解決し、PIVが広く受け入れられる土壌を作っていると言えます。

HSPD-12「連邦政府職員と契約業者の共通識別基準のためのポリシー」と言う一見仰々しい大統領指令も民間のビジネスを大いに刺激しています。FIPS-201認定製品は、GSAのFIPS-201評価制度ウェブサイト（http://fips201ep.cio.gov/, http://fips201ep.cio.gov/apl.php）において、公開されていますが、2007年2月現在、195もの製品やサービスが公表されています。

PIV（PIVカードとPIVミドルウェア）に関しては、NPIVPという認定制度が立ち上がっています。NPIVPは、暗号製品の評価基準FIPS-140の評価認定制度であるCMVPに似た制度となっています。FIPS-140は、米国政府機関が暗号製品を調達する際の基準ですが、暗号製品の評価の難しさ故、客観的な評価がもとめられ、CMVPのような評価・認定制度が重要な意味を持つ様になりました。FIPS-140の基準のクリアーは、暗号製品ベンダーにとっては、高いハードルだったのですが、ハードル越えを米国政府が支援することにより、暗号製品ベンダーを育成した側面があります。そして米国連邦政府機関の調達等がドライブ役となり、米国企業の開発した暗号製品が世界の市場を席巻する大きな原動力となったと言えます。

同様に、IC・IDカードの相互運用可能性を確保した製品も非常に評価が難しい面があります。NPIVPのような評価・認定制度がデファクトの標準を作り出す可能性があるし、そうした狙いがある、また、民間企業はそれを求めているように感じられます。

6. カード内の鍵に関する仕様

ICカードの耐タンパー性や、ICカードで利用されている暗号のアルゴリズム等が、保護すべき重要なものに、カード内の「鍵」があります。公開鍵暗号ベースのIC・IDカードの場合、プライベート鍵(Private Key)の扱いが重要だと言えます。IC・IDカードの技術仕様として、JavaカードやMULTOSカードといったものが仕様として重要と思われているかもしれません。しかし、例えば米国のPIVの場合、その実装として、JavaカードもMULTOSカードもネイティブOSカードも存在します。論理的な意味で重要な技術仕様としては、カード内のプライベート鍵や証明書に関する仕様があります。「カード内のプライベート鍵」の操作が、カード保有者の「署名」「認証」「暗号」にどう結び付くかが非常に重要なポイントです。下の表に、BELPICとPIVと公的個人認証サービスの「カード内の鍵や証明書の仕様の違い」を説明します。

IC・IDカード	カード保有者の証明書	証明書に対応した「プライベート鍵」の利用に関する説明
BELPICベルギー	認証用の証明書	認証(のための署名)に使用する 復号には使用できない(暗号には利用できない)
	否認防止の署名用証明書	署名操作のみ 署名操作毎にPINによるカード保有者の認証が必要。
PIV米国	認証用の証明書	認証(のための署名)に使用する。
	否認防止の署名用証明書 (オプション)	署名操作のみ 署名操作毎にPINによるカード保有者の認証が必要
	暗号用の証明書 (オプション)	発行者により「鍵」のバックアップがなされる
公的個人 認証サービス	否認防止の署名用証明書	署名操作のみ 否認防止用の証明書のみ発行される

BELPICのような欧州の電子身分証ICカードは、一般的にeIDと呼ばれていますが、このeIDは、IASすなわちIdentification、Authentication とelectronic Signature と言ったコンセプトで仕様が作成されています。eIDは、電子認証(Authentication)、電子署名(electronic Signature)、に利用できるものですが、その使い分けを明確にしています。例えば、BELPICでは、カードに格納される(否認防止の)署名用の証明書は、18歳以上に発行されています。BELPICは、2009年までに12歳以上の全国民に配布される予定ですが、責任能力の観点から18歳以下の国民には、IASの「S」を提供していません。否認防止の署名は「責任の所在」を示すので責任能力が必要な訳です。

BELPICの場合、認証用のプライベート鍵は、カード保有者がカードのPIN を入力し保有者認証を行なった以降は、カードに格納された認証用のプライベート鍵が認証要求の都度自動的に使われます(署名を行います)。こうしたことにより、シングルサインオン等、カード保有者に利便性を提供します。正当なカード保有者の認証(Authentication)時の認証用のプライベート鍵の利用は、カード保有者に不利益をもたらすことはありません。認証(Authentication)をするのはサービス提供者側であり、カード保有者が認証されるためにプライベート鍵を使うことにより責任が生じると言うことはない訳です。

これに対して否認防止の署名のプライベート鍵では、1回の否認防止の署名操作、つまりひとつの文書の否認防止の署名毎に「カード保有者の同意確認」(User Consent)のためのPIN の入力が必要な仕様になっています。これはカード自体が、「内容(文書など)

を理解せずに否認防止の署名してしまうこと」を防ぐ仕組みを有していると言えます。署名は、「カード保有者が行う」ものであり、この署名には、その署名文書等にはカード保有者の責任が生じるということを理解する必要があります。

日本の公的個人認証サービスでは、否認防止目的の証明書のみが発行されています。従って、公的個人認証サービスの発行する証明書を、認証（Authentication）として利用すべきではありません。否認防止目的のプライベート鍵を安易に責任の生じない認証（Authentication）として利用することは、責任が生じる署名に対するカード保有者のリテラシーの低下につながるからです。

7. おわりに

情報セキュリティ業界のビジネス上の難題に、その技術的な複雑さなどから、顧客にROI（費用対効果）や、ベストプラクティスを説明することが難しいことがあります。そのため、特に初期の頃は、必要以上に脅威を煽る傾向がありました。これは行き過ぎると長期的には、業界としての信頼を失う結果となるかと思います。

次に、情報セキュリティに関連した制度面の整備により、基準、規範などが整備され、今度は、コンプライアンスをビジネス上の武器にしている傾向があります。これは、もちろん間違いではありません。しかし、「情報セキュリティに関連した制度の整備」には、まだまだ、限界があり、実質的、現実的な情報セキュリティの問題点は、様々なところに存在します。制度面だけからの視点は、情報セキュリティの技術に対する正しい認識を歪めるようなところがあります。JNSA Press Vol.18の「現場まかせにしないセキュリティ設計、評価、実装のあり方について」の記事は、正に、そうした問題を指摘しています。

ICカード（ないしIC・IDカード）に関して言えば、耐タンパー性や暗号アルゴリズムの評価が、制度的にも整いつつありますが、情報セキュリティの専門家としては、これら以外にも解決すべき重要な課題があることを理解する必要があります。この理解の妨げになっているものにICカードの仕様の閉鎖性があります。確かに、リーズナブルなコストの範囲で、セキュリティを担保しようとすると、その仕様の公開範囲に妥協が必要な面はあります。しかし、仕様の閉鎖性は、ICカードの相互運用を阻害するなど、弊害が大きいことを理解する必要があります。

特に、行政の調達などにおいては、オープンシステムであってもセキュリティが保たれる仕様作りへの努力が必要でしょう。また、情報セキュリティの専門家としても、複雑さに負けず、あるべき姿を提案、提言していく必要があるでしょう。

IC・IDカードの技術やアーキテクチャが正しく理解されるために、本稿や「IC・IDカードの相互運用可能性向上に係る基礎調査」の「調査報告書」が少しでもお役に立てることがあれば幸いです。

参　考

IC・ID カードの相互運用可能性の向上に係る基礎調査
http://www.ipa.go.jp/security/fy18/reports/ICID/index.html