

オンラインゲームのセキュアなログイン認証 ICカード myuCard の開発

1. 背景

ID パスワードによる認証では、必要とされるセキュリティ基準に満たないが、ID パスワード認証を利用している場合が多くある。実際、オンラインゲームではアカウントハッキングによる被害が発生し、警察機関による捜査が行われる場合があるようになってきている。ICカードによるログイン認証であれば、このような被害が未然に防がれるはずであるにもかかわらず、ICカードを使っているオンラインゲームは、現在、ほとんどない。ICカードを使ったセキュアな認証が望まれている。

2. 目的

オンラインゲームに限らず IC カードが利用されない理由として考えられるのは、

- (1) ICカードの API が MS-CAPI としてある程度、標準化されているものの IC カードメーカーによって実装にばらつきあり、IC カードアプリケーションの開発の障壁となっている。
- (2) 現状、IC カードが 1 個単位で小売されることはほとんどなく、10 個単位での購入になる場合が多いため、個人で IC カードを持っているという前提でシステム(Web のログイン認証など)を構築することができない。

そこで Microsoft が IC カード用に標準化した MS-CAPI Microsoft Base Smart Card CSP の仕様を使って IC カードエミュレータ myuToken を開発し、フリーウェアとしてダウンロードできるようにし、無料で利用できるようにする。IC カードアプリケーションは、MS-CAPI Microsoft Base Smart Card CSP の API をターゲットとして開発すれば良く、IC カードエミュレータは、無料なので、普及しやすく、開発コスト低減になる。

また、MS-CAPI Microsoft Base Smart Card CSP 対応の IC カード myuCard を開発し、1 個単位での小売ができるようにする。

上記の IC カードエミュレータ myuToken、IC カード myuCard を「オンラインゲームのログイン認証」へ適応する。このとき IC カードによるセキュリティの向上だけでなく、「面白さ」の向上を支援する機能を考えることで、導入をさらに容易する。

3. 開発内容

3-1. ICカードドライバ Card Minidriver の開発

Card Minidriver とは、ICカードのハードウェア依存の部分を実装するユーザーモードドライバで、DLL(ダイナミックリンクライブラリ)ファイル1個で構成される。Card Minidriver は、Microsoft によってリターンコードまで厳格に規定され、Microsoft の動作検証ソフトウェアによって検証することができる。

ICカードアプリケーション
MS-CAPI
Microsoft Base Smart Card CSP
Card Minidriver
WinSCard I/F
PC/SC ドライバ

図 1. Card Minidriver 構成

ICカードエミュレータ版と、ICカード myuCard 版の Card Minidriver を開発する。ICカードエミュレータ版では、ICカードエミュレーション PC/SC ドライバを利用する。

ICカードアプリケーション	ICカードアプリケーション
MS-CAPI	MS-CAPI
Microsoft Base Smart Card CSP	Microsoft Base Smart Card CSP
Card Minidriver	Card Minidriver
WinSCard I/F	WinSCard I/F
エミュレーション PC/SC ドライバ	カードリーダー付属の PC/SC ドライバ

図 2. エミュレーション版と myuCard 版の Card Minidriver 構成

ICカードエミュレーション PC/SC ドライバは、開発者が数年前に開発した Windows のデバイスドライバで USB メモリやフラッシュメモリカードの USB カードリーダーを ICカードとしてエミュレーションする。

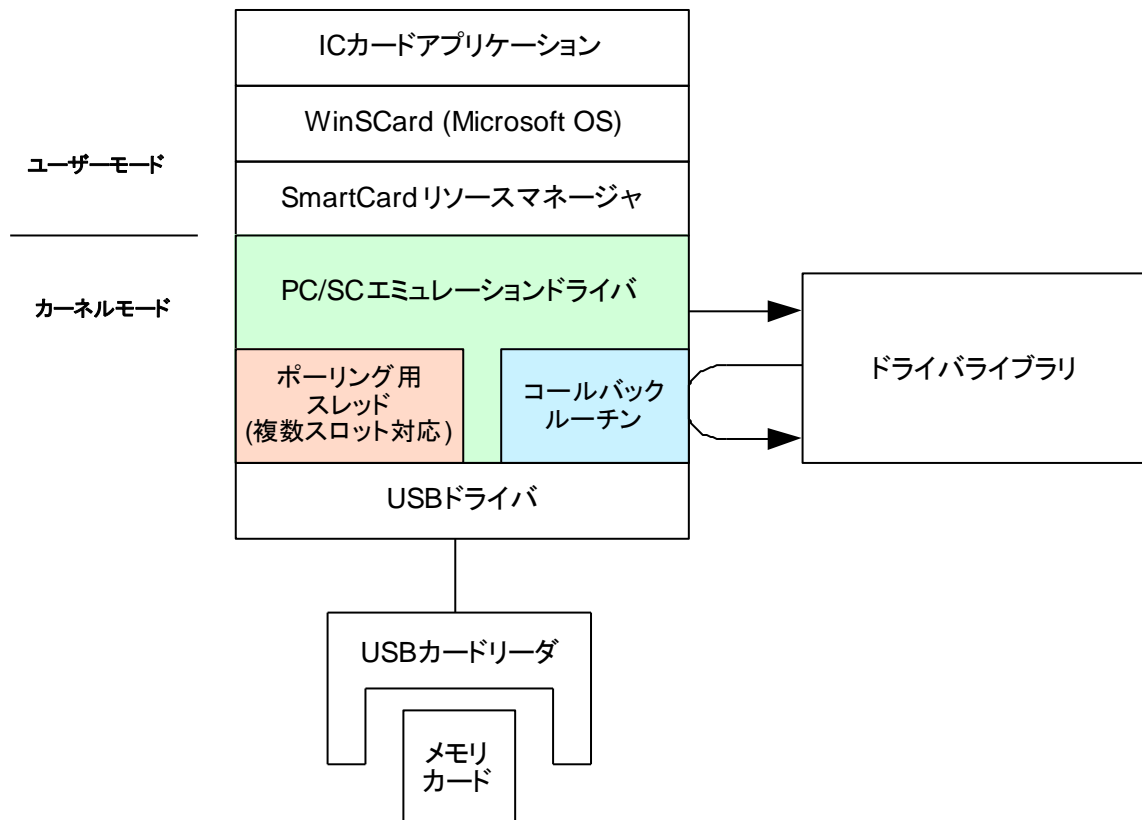


図 3. IC カードエミュレーション PC/SC ドライバ

3-2. ライブラリ CharonRing の開発

ゲーム機では、専用のメモリカードがあるので、仲間とゲームデータを交換する場合に、セキュリティが問題になることはなかった。PC用オンラインゲームでは、USBメモリなどを利用して、ゲームデータを交換することは可能であるが、USBメモリの自動起動でウイルスに感染する恐れがあり、安心してゲームデータの交換をすることができなかった。そこでICカードをメモリカードとしても利用できるようなデータ格納機能をもつCharonRingライブラリを開発。ICカードの電子署名を利用することで、よりセキュリティの高いデータ交換を実現することも可能である。

4. 従来の技術との相違

4-1. Card Minidriver 編

電子証明書を入れることができる汎用用途のICカード myuCardを開発。従来製品のAladdin社のeToken、SafeNet社のiKey1000、FAITIAN社のePass1000、アテナスマートカードソリューションズ社のASECardCryptoなどと同様の製品である。

myuCardは、USBメモリやフラッシュメモリカードをICカードエミュレーションするソフトウェアmyuTokenで操作することが可能。ICカードエミュレータと同じ操作でmyuCardを操作することができることが特徴である。ICカードエミュレータがフ

リーウェアで無料であるため、ICカードアプリケーションの開発コストも低減できる。またICカードアクセスインターフェースも業界標準のMS-CAPI Microsoft Base Smart Card CSPであるため、MicrosoftのOfficeなどのアプリケーションが将来にわたっても安定して動作すると思われる。

4-2. CharonRing 編

ICカードにデータを格納するインターフェースとして、従来からPKCS#11があるが、かなり実装にばらつきのあるインターフェースであり、ハードウェアごとに動作検証することが必須であった。そこでデータ格納形式の仕様を新規に開発し、一般公開するということを考えるが、Card Minidriverのインターフェースをそのまま利用する方法が簡単である。Card Minidriverのインターフェースは、Microsoftの検証ソフトウェアによって、厳格にチェックされるため、実装のばらつきは、非常に小さなものとなる。(当然、格納できるファイル数や容量は、ICカードによって異なる)

5. 期待される効果

競合他社製品が2000年頃から存在していたにもかかわらず、あまり普及していない。普及に対して優れた特徴を持つmyuCardによって、ICカードのパソコン市場の開拓が見込まれる。

6. 普及の見通し

ICカードエミュレータ myuToken は既に Web からダウンロードすることが可能で、ICカード myuCard も、2008年4月下旬には、小売される予定。

7. 開発者名(所属)

平山 直紀 (株式会社 iCanal
/ 早稲田大学 IT 研究機構 アドバンスチップマルチプロセッサ研究所)

(参考) 開発者 URL

株式会社 iCanal	http://www.icanal.co.jp/
早稲田大学 IT 研究機構	http://www.it.waseda.ac.jp/project/itpj01.html
myuToken のダウンロード	http://www.icanal.co.jp/myutoken/myutoken_down.html