新しい決済手段のご提案

株式会社フュージョンシス

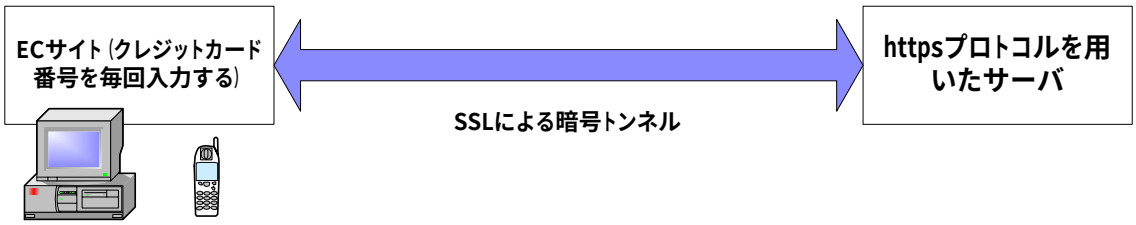
目次

現行のクレジットカード決済の問題点

問題点その1　　カード番号の漏洩

携帯端末がこれほど広く普及してきているので、クレジットカードの情報を携帯端末に持たせて、携帯端末をクレジットカードそのものとして使いたいということを考えるのは当然でしょう。しかし現行のクレジットカード決済には問題があります。

ECサイトにおける現行のクレジットカードの決済法

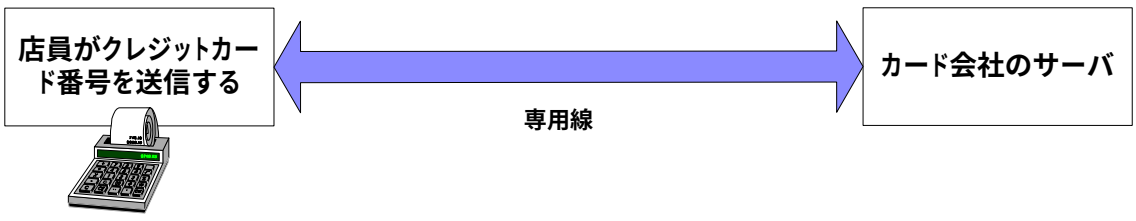


インターネットで買い物をするときには毎回クレジットカードの番号を入力する必要がある。

上の方法最大の問題点は、カード番号が第三者に漏洩してしまうと、そのカード番号を利用して第三者が本人の認証を必要としないショップなどで簡単に買い物をすることが簡単にできてしまうということです。確かに SSL などの暗号トンネルが盗聴を防ぐために広く用いられていますが、サーバの管理の杜撰さなどが原因でカードの番号やカードユーザの名前などが第三者に渡ってしまうことが頻発しています。

問題点その2　　個人情報の漏洩

実店舗における現行のクレジットカードの決済法



カード番号や名前（時には電話番号も）が店員に知られてしまう。

インターネットショップでない普通のショップでクレジットカードを使う時の問題点は、サインなどの個人認証をしていてもやはり第三者にカード番号が知られてしまう、電話番号、名前などの個人情報が店員に知られてしまうことです。

解決策

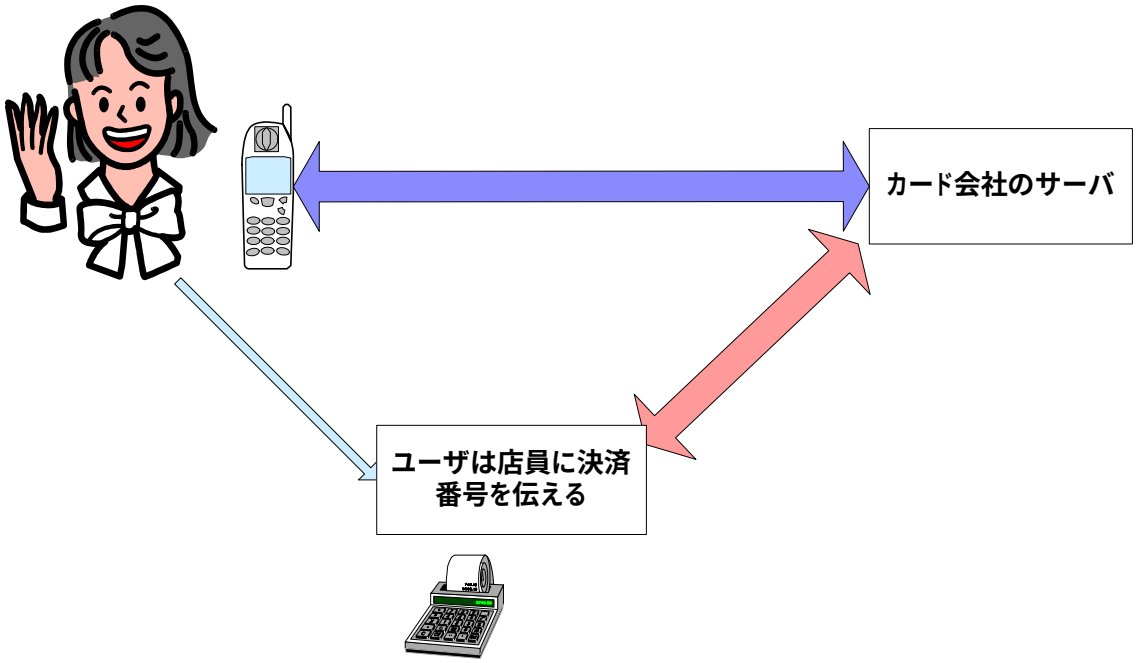
これらの問題を解決するには、決済そのものを可能な限り現金による決済に近づけることです。具体的には、たとえ第三者にクレジット決済会社とカードユーザとの通信内容がたとえ漏洩しても、それを用いて第三者が買い物ができないようにすることが必要です。

一時的に有効な情報の活用

決済会社とカードユーザとの間に交わされる情報が現在のように固定的（カードユーザはカード番号を毎回送る）であることが、現在のクレジットカード決済を危険なものにしています。カードを最後に使った時のユーザID（決済会社またはカードユーザの端末がその時ランダムに生成したID）、カードユーザがその場で勝手に決めた番号、時刻など決裁者（決済会社や銀行など）と個人の両者が共有することのできる情報などを決済会社とカードユーザは交換するとよいことが分かります。本方法ではユーザIDは使い捨てになりますので、たとえ第三者に漏洩してもその第三者は自己の決済に用いることができなくなります。

新しい決済法

新しい決済法は次のような構成になります。



ユーザの携帯端末が持つべき性質

✓　ユーザの持っているクレジットカードの番号を保存している必要はない（後述、”携帯端末が持っている情報”を参照してください）。
✓　前回のユーザ ID（例えば 8 桁）を保存している。
✓　ユーザの固定の 4 桁のパスワードを保存している。
✓　今回のユーザ ID（例えば 8 桁）を生成する。
✓　前回のユーザ ID、今回のユーザ ID、前回の決済開始時間など（他に情報をつけてもよい）を暗号化し、決済会社に送る。
✓　決済会社から送られてくる（例えば）3 桁程度の数字（決済番号と呼ぶことにします）を表示する。
✓　前回のユーザ ID を消去し、今回のユーザ ID を保存する。

これらの機能は JAVA のプログラムによって実現できます（決済番号を生成するアルゴリズムに関しては“ユーザ ID の生成方法”を参照してください）。

店舗側の機器が持つべき性質

ユーザの携帯端末が表示した3桁（決済番号）の数字とユーザが購入しようとしている商品の値段を決済会社などの決済会社に送信することが必要です。現在使われている装置の若干の変更によってこの機能が実現可能です。

決済の流れ
実店舗における決済の流れは次のようになります。

ユーザ	ユーザの携帯端末	店舗	決済会社
ユーザは携帯で決済を開始するボタンを押す。			
ユーザは自分の4桁の暗証番号を入力する。			
	ユーザIDを適当な方法で生成する（方法については“ユーザIDの生成方法“を参照してください）。		
	前回のユーザIDと今回のユーザIDと前回の決済開始時間などを暗号化して決済会社に送る。		
			前回のユーザIDと前回の決済開始時間などをキーにして検索し、もしあれば1回目の認証は成功。決済番号（例えば3桁）を発行し、ユーザの携帯端末に送る。
	決済会社から送られてきた決済番号をそのまま表示する。		
決済番号を店員に伝える。			
		店員は決済番号の数字とユーザが購入しようとしている商品の金額を決済会社に送る。	
			その決済番号が例えば

			過去 3 分以内に発行されたものであれば、有効とする
			店舗から送られてきた決済番号をキーにしてユーザ ID を探す。もしあれば 2 回目の認証は成功。
			認証がされると、ユーザが店舗側から送られてきた金額をユーザが払うことができるかどうかを審査する。
			払うことが可能であれば、店側とユーザ側に決済可能であることを通知する。
		ユーザに品物を渡す。	
店舗から品物を受け取る。			
	前回のユーザ ID を消去し、今回のユーザ ID を前回のユーザ ID として保存する。		前回のユーザ ID を消去し、今回のユーザ ID を前回のユーザ ID として保存する。
	前回の決済開始時間を消去し、今回の決済開始時間を保存する（他の情報を使う時も同様）。		前回の決済開始時間を消去し、今回の決済開始時間を保存する（他の情報を使う時も同様）。

インターネット店舗における決済の流れも基本的に実店舗の場合と変わりません。いずれの場合にせよユーザは店舗側に自分の名前やカード番号など一切教える必要のない点が、これまでのクレジットカード決済と大きく異なる点です。

決済番号について

決済番号はユーザの携帯端末から送られてきた前回のユーザ ID **や前回の決済開始時間などの情報が、決済会社のサーバに保存された前回のユーザ** ID **や前回の決済開始時刻と一致した、すなわち認証が成功したユーザに対してのみ、発行されます。この番号は乱数として発生させるのではなく、例えば** 000,001,002….**というように連番として発行することもできます。短い時間内に決済を使うユーザが** 1000 **人をこえることがほとんどありえないのならば、**3 **桁の数字で十分です。**4 **桁の数字にすれば同時に** 10000 **人のユーザが決済しようとしても大丈夫です。もしアルファベットも使うことにすれば（**1**と** l,0**と** o,2**と** z**といった間違いをしやすい文字は省く必要があるでしょう）、**3 **文字で** 46656 **人まで、**4 **文字で** 1679616 **人まで決済番号を同時に発行できます。決済番号は使いまわしができますので、決済が終了したならば、また別の決済に使います。**

特長

1. **この方法においては、固定的なカード番号に相当する部分がないので、たとえ第三者に決済会社とカードユーザとの通信内容が漏洩しても、第三者がそれを使って買い物をすることはできません。また店舗側にカード所有者の名前などの個人情報もわたりません。**
2. **本方法はいわゆる非接触型といわれるものであり、機械的な磨耗や情報の漏洩を意図した悪質な装置からの攻撃も考える必要がありません。**
3. **暗号法は（**DES **や** Rijndael **などの）共通鍵形式のものを任意に選択可能です。**
4. **特長**1）2）**は現金が本来持っている性質であり、その意味でこの決済は、より現金による決済に近いといえるでしょう。**

携帯端末をクレジットカードとして使うまでのユーザの手続き

携帯電話ををクレジットカードとして使うためには、ユーザは次のような手続きをとる必要があります。

1. **決済用の** JAVA **アプリケーションをダウンロードする。**
2. **決済会社に携帯端末による決済を行ないたい旨を、郵便などのインターネットによらない方法で伝える。**
3. **決済会社から** OK **の通知がきたら、自分の暗証番号を入力し、第一回目の決済に使うための情報のユーザ** ID **を生成する。**

4. **この 2 つのユーザ ID と ID の生成時刻は携帯端末によって自動的に決済会社に送信される。**

一回目の決済では、2 つのユーザ ID がユーザの携帯端末において暗号化され、決済会社に送られることになります。

携帯端末をユーザが紛失してしまった、あるいは盗まれた場合
現行のシステムの下では、ユーザがクレジットカードを紛失した場合には、すぐに決済会社に連絡してカードを無効化してもらいますが、本方法では無効化は基本的に必要ありません。というのは携帯端末にもともとクレジットカードの番号が含まれていないからです。仮に第三者があるユーザの携帯端末を盗んでも、正しい暗証番号を知りえませんから、その第三者はユーザの携帯端末を使って決済を行なうことはできません。

携帯端末がユーザに関して持っている個人情報
本方法において、携帯端末がユーザについて持っている情報は 4 桁の固定されたパスワードだけです。続けて5回誤ったパスワードを入力すると決済機能は無効化されるなどの機能を付加することにより、でたらめにパスワードをいれて使おうとする攻撃からも安全になります。
クレジットカード番号や名前などの個人情報が一切保存されていないので、セキュリティーに関しても従来の方法より優れていることがわかります。

暗証番号の保存について
ソフトウェアがハッキングされることを考慮すると、(ファイルなどを使って) ソフトウェア的に持つのではなくハードウェア内に保存するのが望ましいので、携帯が持っている番号登録機能を用います。

この決済方法を使ったビジネスモデルのご提案
ビジネスモデルが他の方法に比べ優れているのは、携帯側に新たな装置をつける必要がないので、事業化に際してコストがかからないことです。一方決済会社ではシステムに変更を加えることが必要になります。

携帯端末	店舗	決済会社
新たな装置をつける必要がない。	新たな装置をつける必要がない。(一番安い方法は決済会社のサーバに https プロトコルで常時つなぎ、購買者からの決済番号と購入しようとしている商品の価格を入力する端末があればよい)	システムに変更が必要。

決済に関して通信にかかる料金は、キャッシュバックのような形式で決済会社が負担すると、より多くのユーザが使うことができるでしょう。

ユーザ ID を生成する方法

ユーザ ID として何を使うか

使い捨てのユーザ ID を生成する方法にはいろいろと考えられます。例えば決済の開始時刻だけでもある程度使い捨てのユーザ ID として使えます。ただ偶然複数の人が決済を同時に開始することも起こりえます。従って開始時刻だけではなく、終了時刻や金額といった情報も併せて使うことも考えられます。8桁のユーザ ID はこういった情報を複数個使えば必要ないとも考えられます。ただ人為的に生成させるユーザ ID は生成が簡単なので、本方法では決済開始時刻も併せて使うことを提案しています。つまり決済開始時刻とユーザ ID という事実上 2 つの使い捨て ID を使っていることになります。

ユーザ ID を人為的に生成する方法

ユーザ ID を人為的に生成させる方法には、大きく分けて 2 つあります。

1. ユーザ ID はある固定された擬似乱数列または周期解を全く持たない微分方程式の解をつかう。
2. ユーザ ID は毎回適当な方法で乱数を発生させる。

1) の方法については次のようなことがいえます。ある携帯端末が生成する2回の連続するユーザ ID が、他のユーザの携帯端末が生成する 2 回の連続するユーザ ID と決して同じになることはないという条件は、現在知られている方法で実現可能です (擬似乱数列や周期解を全く持たない微分方程式の解を使います) 。しかしその場合す

べてのユーザのユーザ ID の系列が異なったものであることを保証するためにおのおののユーザがすべて異なるシリアル番号を作ってやることが必要になります (擬似乱数列の seed や周期解を全く持たない微分方程式の初期値やパラメータとして使うことになります)。

2) を使った場合は、衝突、つまり二人の携帯端末が2回連続して同じユーザ ID を生成することは確率的に0ではないが、その確率は非常に小さいので、それを無視する方法です。前回のユーザ ID ではなく、前回のユーザ ID と前々回のユーザ ID とそれぞれの決済開始時間も最新の決済と同時に送ることにすれば、衝突の可能性は非常に小さくなります。この方法のメリットは、ユーザ ID は毎回異なる seed を使ってシリアル番号が不要になることです。また本方法では決済開始時刻も併せて使うので、事実上衝突が起こることはまず起こらないと考えられます。

1) を衝突を許さない方法と考え、2) を衝突が起こる確率を許容する方法と考えることができます。

衝突を許さない方法

シリアル番号

各ユーザに異なったユーザ ID の系列を生成させるために、シリアル番号が必要となります。これはユーザが携帯による決済を申し込んできた時に、決済会社が中身を隠せるシール付きのはがきなどでユーザに知らせます。もちろんクレジットカードの番号をこのシリアル番号として使うこともできます。その場合一回目のユーザ ID を生成する時に“あなたが入力したクレジットカード番号はこの端末のどこにも保存されませんし、携帯からどこかへ送られることもありません。”とか”ユーザ ID の生成が済んだので、クレジットカード番号はこの携帯端末から完全に消去されました”といったメッセージを出すことが必要でしょう。

最初のユーザ ID

最初のユーザ ID はシリアル番号だけから生成されるので、シリアル番号を生成した時点で、決済会社はユーザが生成するユーザ ID の系列を知ることができます。従って決済会社にユーザからユーザ ID が送られてきた時に本人がユーザ ID を生成したという認証もあわせて行っています。ユーザ ID の管理が決済会社にとってはやりやすい利点があります。

2回目以降のユーザ ID

2回目以降のユーザ ID もアルゴリズムに従って生成するので、決済会社は完全にどのユーザが何回目にはどの番号を送ってくるか分かっています。

衝突が起こる確率を許容する方法

最初のユーザ ID

4桁の暗証番号およびその他の情報からユーザ ID を生成することになります。このユーザ ID を決済会社に送る時何らかの形で本人認証が必要になります。本人の認証は決済会社は、ユーザからユーザ ID が送られてきたときに初めてそのユーザ ID を知ることになります。

2回目以降のユーザ ID

2回目以降も4桁の暗証番号や時刻など他の情報も併せてユーザ ID を生成しますが、2回目以降は本人認証は前回のユーザ ID を通じてできますので、他の本人認証は必要がありません。

	衝突を絶対に許さない方法	衝突が起こる確率を許容する方法
シリアル番号	必要	不要
最初のユーザ ID	シリアル番号から生成	暗証番号などから生成
最初のユーザ ID 送出時における他の手段による本人認証	不要	必要
決済会社はユーザ ID の系列を知っているか	Yes	No
2回目以降のユーザ ID	決定論的に決まる	非決定論的に決まる
2回目以降のユーザ ID 送出時における他の手段による本人認証	不要	不要