(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2005-521961
(P2005-521961A)
(43)公表日　平成17年7月21日(2005.7.21)

(51)Int.Cl.[7]	F I			テーマコード（参考）
G06F 17/60	G06F	17/60	414	3E044
G07F 7/12	G06F	17/60	318Z	5J104
H04L 9/32	G07F	7/08	C	
	H04L	9/00	673A	

審査請求 未請求　予備審査請求 有　（全 22 頁）

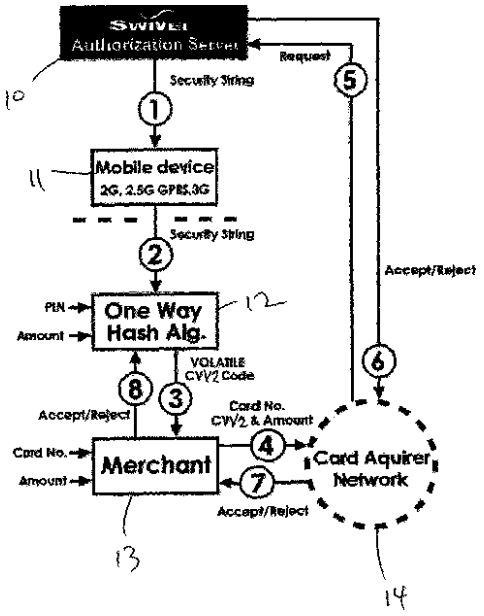
(21)出願番号	特願2003-581137 (P2003-581137)
(86)(22)出願日	平成15年3月14日 (2003.3.14)
(85)翻訳文提出日	平成16年10月1日 (2004.10.1)
(86)国際出願番号	PCT/GB2003/001075
(87)国際公開番号	WO2003/083793
(87)国際公開日	平成15年10月9日 (2003.10.9)
(31)優先権主張番号	0207705.5
(32)優先日	平成14年4月3日 (2002.4.3)
(33)優先権主張国	英国 (GB)
(31)優先権主張番号	10/131,489
(32)優先日	平成14年4月25日 (2002.4.25)
(33)優先権主張国	米国 (US)

(71)出願人　503089412
スイベル　セキュア　リミテッド
イギリス国、ノース　ヨークシャー、ナースバラ、　ヨーク　プレース、ヨーク　ハウス
(74)代理人　100066692
弁理士　浅村　皓
(74)代理人　100072040
弁理士　浅村　肇
(74)代理人　100094673
弁理士　林　鈺三
(74)代理人　100091339
弁理士　清水　邦明

最終頁に続く

(54)【発明の名称】クレジットカードおよびデビットカードの安全な取引のためのシステムと方法

(57)【要約】
顧客と商人との間でクレジットカードおよびデビットカードの安全な取引を行うための方法とシステムを開示する。顧客にはホストコンピュータにより疑似ランダムセキュリティストリングが発行される。疑似ランダムセキュリティストリングは顧客の移動電話機に送られる。移動電話機のＳＩＭカード内で動作する暗号アルゴリズムはセキュリティストリング、もしくはセキュリティストリング、顧客のＰＩＮ、および取引額から抽出された１回限りのコードに対してハッシュ（細切れ）を行う。顧客のＰＩＮおよび取引額は移動電話機のキーパッドを経由して入力される。暗号アルゴリズムにより３ディジットの応答コードが作成され、商人に送られる。次に、商人は応答コード、取引額、および顧客の口座番号（カード番号）をホストコンピュータに送信する。ホストコンピュータでは、疑似ランダムセキュリティストリングとＰＩＮがメモリから検索される。次に、ホストコンピュータは同じアルゴリズムをセキュリティストリング、ＰＩＮ、および取引額に適用してチェックコードを発生する。チェックコードが商人から送信された応答コードと



【特許請求の範囲】
【請求項１】
顧客と商人との間の安全な取引を許可する方法であって、
ｉ）　顧客の口座番号と、対応づけられた個人識別番号（ＰＩＮ）とを含む顧客情報をホストコンピュータ上に記憶し、
ｉｉ）　ホストコンピュータ内に疑似ランダムセキュリティストリングを発生させ、
ｉｉｉ）　ホストコンピュータから顧客の操作する少なくとも一つの遠隔電子装置に疑似ランダムセキュリティストリングを送信し、
ｉｖ）　顧客が商人と取引を行ったときに個人識別番号（ＰＩＮ）と取引額とを電子装置に入力し、
ｖ）　疑似ランダムセキュリティストリングと個人識別番号（ＰＩＮ）と取引額とに所定の暗号アルゴリズムを適用することにより電子装置内に応答コードを発生させ、
ｖｉ）　応答コードと取引額と顧客口座番号とをホストコンピュータに送信し、
ｖｉｉ）　ホストコンピュータ内で、顧客口座番号を使用することにより個人識別番号（ＰＩＮ）と疑似ランダムセキュリティストリングとを検索した後、疑似ランダムセキュリティストリングと個人識別番号（ＰＩＮ）と取引額とに所定の暗号アルゴリズムを適用することによりチェックコードを発生させ、
ｖｉｉｉ）　ホストコンピュータ内で、チェックコードと応答コードとを比較し、それらが合致すれば、取引を許可する、ステップ
を備えた方法。
【請求項２】
請求項１記載の方法であって、遠隔電子装置が移動電話機、携帯情報端末、またはページング装置である、方法。
【請求項３】
請求項１または２記載の方法であって、応答コードが顧客によって商人に送られ、次に商人はステップｖｉ）で応答コードと取引額と顧客口座番号とをホストコンピュータに送る、方法。
【請求項４】
請求項３記載の方法であって、応答コードは商人のウェブサイトを経由して顧客によって商人に送られる、方法。
【請求項５】
請求項３記載の方法であって、応答コードは顧客によって口頭または書かれたメッセードとして商人に送られる、方法。
【請求項６】
請求項３記載の方法であって、応答コードは顧客によって電子装置からの電子送信として商人に送られる、方法。
【請求項７】
任意の先行請求項記載の方法であって、応答コードと取引額と顧客口座番号とが中間サーバを経由してステップｖｉ）でホストコンピュータに送信される、方法。
【請求項８】
任意の先行請求項記載の方法であって、応答コードと取引額と顧客口座番号とがインタネット接続を経由してステップｖｉ）でホストコンピュータに送信される、方法。
【請求項９】
請求項１から７のいずれか１項記載の方法であって、応答コードと取引額と顧客口座番号とが商人が操作するＥＰＯＳまたはＥＦＴＰＯＳ機械を経由してステップｖｉ）でホストコンピュータに送信される、方法。
【請求項１０】
請求項１から７のいずれか１項記載の方法であって、応答コードと取引額と顧客口座番号とが商人が操作する移動電話機、携帯情報端末等を経由してステップｖｉ）でホストコンピュータに送信される、方法。

【請求項１１】
任意の先行請求項記載の方法であって、複数の疑似ランダムセキュリティストリングがステップｉｉｉ）でホストコンピュータから電子装置に同時に送信される、方法。
【請求項１２】
請求項２から１１のいずれか１項記載の方法であって、アルゴリズムが電子装置内に設けられたＳＩＭカード内のアプレットとして動作する、方法。
【請求項１３】
任意の先行請求項記載の方法であって、応答コードとチェックコードとが３桁の１０進数である、方法。
【請求項１４】
顧客と商人との間で行われる取引を許可する安全取引システムであって、該システムはホストコンピュータと顧客が操作する少なくとも一つの装置とを含み、
ｉ） 顧客の口座番号と、対応づけられた個人識別番号（ＰＩＮ）とを含む顧客情報がホストコンピュータ上に記憶され、
ｉｉ） ホストコンピュータが疑似ランダムセキュリティストリングを発生し、かつ、顧客の操作する少なくとも一つの電子装置に疑似ランダムセキュリティストリングを送信し、
ｉｉｉ） 顧客が商人と取引を行うときに個人識別番号（ＰＩＮ）と取引額とを含む顧客からの入力を電子装置が受信し、
ｉｖ） 疑似ランダムセキュリティストリングと個人識別番号（ＰＩＮ）と取引額とに所定の暗号アルゴリズムを適用することにより電子装置が応答コードを発生し、
ｖ） 応答コードと取引額と顧客口座番号とがホストコンピュータに送信され、
ｖｉ） ホストコンピュータは顧客口座番号を使用することにより個人識別番号（ＰＩＮ）と疑似ランダムセキュリティストリングとを検索した後、疑似ランダムセキュリティストリングと個人識別番号（ＰＩＮ）と取引額とに所定の暗号アルゴリズムを適用することによりチェックコードを発生し、
ｖｉｉ） ホストコンピュータはチェックコードと応答コードとを比較し、それらが合致すれば、取引を許可する、
安全取引システム。
【請求項１５】
請求項１４記載のシステムであって、遠隔電子装置が移動電話機、携帯情報端末、またはページング装置である、システム。
【請求項１６】
請求項１４または１５記載のシステムであって、応答コードが顧客によって商人に送られるように構成され、そして商人はステップｖ）で応答コードと取引額と顧客口座番号とをホストコンピュータに送信できるように構成された、システム。
【請求項１７】
請求項１６記載のシステムであって、顧客から応答コードを受信するように構成された商人のウェブサイトを更に含む、システム。
【請求項１８】
請求項１６記載のシステムであって、電子送信を経由して応答コードを商人に送信するように電子装置が構成される、システム。
【請求項１９】
請求項１４から１８のいずれか１項記載のシステムであって、応答コードと取引額と顧客口座番号とがそれを経由してステップｖ）でホストコンピュータに送信される中間サーバを更に含む、システム。
【請求項２０】
請求項１４から１９のいずれか１項記載のシステムであって、インタネット接続を経由してステップｖ）で応答コードと取引額と顧客口座番号とをホストコンピュータに送信するように構成された、システム。

【請求項２１】
請求項１４から１９のいずれか１項記載のシステムであって、ステップｖ）でホストコンピュータに応答コードと取引額と顧客口座番号とを送信するように構成されたＥＰＯＳまたはＥＦＴＰＯＳ機械を更に含む、システム。
【請求項２２】
請求項１４から１９のいずれか１項記載のシステムであって、ステップｖ）でホストコンピュータに応答コードと取引額と顧客口座番号とを送信するように構成された、商人が操作する移動電話機、携帯情報端末等を更に含む、システム。
【請求項２３】
請求項１４から２２のいずれか１項記載のシステムであって、ステップｉｉ）で複数の疑似ランダムセキュリティストリングを電子装置に同時に送信するようにホストコンピュータが構成される、システム。
【請求項２４】
請求項１４から２３のいずれか１項記載のシステムであって、アルゴリズムが電子装置内に設けられたＳＩＭカード内のアプレットとして動作する、システム。
【請求項２５】
請求項１４から２４のいずれか１項記載のシステムであって、応答コードとチェックコードとが３桁の１０進数である、システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明はクレジットカードおよびデビットカードの取引等に関して安全性を改善するためのシステムと方法に関するものである。
【背景技術】
【０００２】
クレジットカードとデビットカードの詐欺（以後まとめて「カード詐欺」と言う）は、特にオンライン取引（電子商取引）で問題になりつつある。これに対して銀行業界は、より高性能のアプローチを開発できないうちは、短期的な解決策で詐欺と戦ってきた。この短期的な解決策は「ＣＶＶ２」アプローチとして知られており、比較的簡単である。ＣＶＶ２コードは３桁の１０進数であり、一般にカードの発行者がクレジットカードまたはデビットカードの裏面に印刷される。ＣＶＶ２コードはカード番号（「ＰＡＮ」すなわち支払い者口座番号（ｐａｙｅｒ　ａｃｃｏｕｎｔ　ｎｕｍｂｅｒ）とは分離されており、磁気ストリップまたは埋め込みチップにより、カード上に電子的にコーディングされることはない（これはＣＶＶ２コードが詐欺者によって「スキミングされる」のを防止するのに役に立つ）。ＣＶＶ２コードはカード上に印刷されるが、磁気ストライプから読み取ることはできない。オンライン源からカード番号を得て、これをチェックして、供給されたＣＶＶ２コードが正しいか見ることにより検証が行われる。
【０００３】
カード保有者がその場に居ない取引（たとえば、オンラインまたは電話での取引）を行っている商人は、カード保有者に支払い者口座番号、カード有効期限、配達住所とともにＣＶＶ２コードを要求する。次に、商人はオンラインチェックを行って、ＣＶＶ２コードと与えられたカード保有者の配達住所が、与えられた支払い者口座番号に対応するカードについてカード発行者が保持している詳細と符合することを確かめる。したがって、詐欺的取引を行おうとする者は支払い者口座番号、カード保有者住所、カード有効期限、およびＣＶＶ２コードを必要とする。したがって、ＣＶＶ２アプローチは、詐欺者が最初この情報の盗み方を知らないものと仮定している。支払い者口座番号を盗む多数の手法をわずかに拡張してＣＶＶ２コードとカード保有者の住所を盗むことができるので、ＣＶＶ２アプローチは比較的容易に圧倒されるのが欠点である。ＣＶＶ２はせいぜい、詐欺の拡大を遅くする一時的な方策である。
【０００４】

ＣＶＶ２アプローチを支援するために必要とされるインフラストラクチャ（基本的施設）は既に設置され、運用されている。これは、商人の装置（たとえば、ＥＰＯＳおよびＥＦＴＰＯＳ端末等）およびコンピュータ（ＩＴ）システムは既に設計され、付加的な安全方策として３桁の１０進数を要求するように構成されていることを意味する。本発明の各実施例は、この既存の基本的設備を使用することにより、新しいスマートカードに基づくアプローチと比べても高いレベルの詐欺防止の安全性を与えるように構成されている。

【０００５】

ある人、たとえばクレジットカードまたはデビットカード保有者の身元（ｉｄｅｎｔｉｔｙ）を確認するための改良された方法およびシステムが、本出願者の係属英国特許出願第００２１９６４２号、国際特許出願第ＰＣＴ／ＧＢ０１／０４０２４号、および米国特許出願第０９／６６３，２８１号と第０９／９１５，２７１号に開示されている。この方法およびシステムでは、カード取引を行う前にある人の移動電話機等に疑似ランダムストリングが送信される。その人は次に、個人識別番号（ＰＩＮ：ｐｅｒｓｏｎａｌ　ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　ｎｕｍｂｅｒ）の形式のマスクコードを所定の仕方で疑似ランダムストリングに印加して、揮発性の１回限りの取引識別コードを発生する。この揮発性の１回限りの取引識別コードは商人に送られた後、認証サーバに送られ、そこで独立に計算された揮発性の１回限りの識別コードと照合され、カード保有者の身元が確認される。

【発明の開示】

【発明が解決しようとする課題】

【０００６】

本発明の第１の側面によれば、顧客と商人との間の安全な取引を許可する方法であって、

ｉ）　顧客の口座番号と、対応づけられた個人識別番号（ＰＩＮ）とを含む顧客情報をホストコンピュータ上に記憶し、

ｉｉ）　ホストコンピュータ内に疑似ランダムセキュリティストリングを発生させ、

ｉｉｉ）　ホストコンピュータから顧客の操作する少なくとも一つの遠隔電子装置に疑似ランダムセキュリティストリングを送信し、

ｉｖ）　顧客が商人と取引を行ったときに個人識別番号（ＰＩＮ）と取引額とを電子装置に入力し、

ｖ）　疑似ランダムセキュリティストリングと個人識別番号（ＰＩＮ）と取引額とに所定の暗号アルゴリズムを適用することにより電子装置内に応答コードを発生させ、

ｖｉ）　応答コードと取引額と顧客口座番号とをホストコンピュータに送信し、

ｖｉｉ）　ホストコンピュータ内で、顧客口座番号を使用することにより個人識別番号（ＰＩＮ）と疑似ランダムセキュリティストリングとを検索した後、疑似ランダムセキュリティストリングと個人識別番号（ＰＩＮ）と取引額とに所定の暗号アルゴリズムを適用することによりチェックコードを発生させ、

ｖｉｉｉ）　ホストコンピュータ内で、チェックコードと応答コードとを比較し、それらが合致すれば、取引を許可する、ステップ

を含む取引許可方法を提供する。

【０００７】

本発明の第２の側面によれば、顧客と商人との間で行われる取引を許可する安全取引システムであって、システムはホストコンピュータと顧客が操作する少なくとも一つの装置とを含み、

ｉ）　顧客の口座番号と、対応づけられた個人識別番号（ＰＩＮ）とを含む顧客情報がホストコンピュータ上に記憶され、

ｉｉ）　ホストコンピュータ内に疑似ランダムセキュリティストリングを発生し、顧客の操作する少なくとも一つの電子装置に疑似ランダムセキュリティストリングを送信し、

ｉｉｉ）　顧客が商人と取引を行うときに個人識別番号（ＰＩＮ）と取引額とを含む顧客からの入力を電子装置は受信し、

ｉｖ）　疑似ランダムセキュリティストリングと個人識別番号（ＰＩＮ）と取引額とに所

定の暗号アルゴリズムを適用することにより電子装置は応答コードを発生し、
ｖ） 応答コードと取引額と顧客口座番号とがホストコンピュータに送信され、
ｖｉ） ホストコンピュータは顧客口座番号を使用することにより個人識別番号（ＰＩＮ）と疑似ランダムセキュリティストリングとを検索した後、疑似ランダムセキュリティストリングと個人識別番号（ＰＩＮ）と取引額とに所定の暗号アルゴリズムを適用することによりチェックコードを発生させ、
ｖｉｉ） ホストコンピュータはチェックコードと応答コードとを比較し、それらが合致すれば、取引を許可する、
取引許可方法を提供する。

【０００８】
電子装置が発生する応答コードは好ましくは、電子装置のディスプレイにディスプレイされ、口頭で、または別の方法で、顧客が取引を行っている商人に送信される。その代わりに、応答コードは顧客が操作する電子装置から直接、商人が操作する電子装置（たとえば、ＥＰＯＳまたはＥＦＴＰＯＳ端末）に、何か都合のよい技術（たとえば、Ｂｌｕｅｔｏｏｔｈ（登録商標）、または通常、変調された電磁放射信号を使用する他の標準通信技術）により送信してもよい。商人のウェブサイト等を経由して取引が行われている場合、応答コードをウェブサイトの適当なフィールドに入力して、商人に送信してもよい。

【０００９】
応答コード、取引額、および顧客の口座番号は一般に、認証のため顧客ではなくて商人によりホストコンピュータに、多分ＥＰＯＳまたはＥＦＴＰＯＳ端末を経由して、または何か適切なコンピュータ装置を経由して送信される。

【００１０】
電子装置は好ましくは、移動電話機、携帯情報端末（ＰＤＡ：ｐｅｒｓｏｎａｌ ｄｉｇｉｔａｌ ａｓｓｉｓｔａｎｔ）、ページング装置、または類似の電子通信装置である。疑似ランダムセキュリティストリングはホストコンピュータから電子装置に、短メッセージングサービス（ＳＭＳ：ｓｈｏｒｔ ｍｅｓｓａｇｉｎｇ ｓｅｒｖｉｃｅ）プロトコルを経由して、または音声メッセージング、電子メール等の手段を含む何か他の適当な通信プロトコルを経由して送信してもよい。

【００１１】
本発明のシステムおよび方法を使用するためには、まず通常の仕方で顧客にクレジットカードまたはデビットカードが割り当てられ、発行される。カードにはその顧客特有の口座番号が印刷される。次に、顧客は、ホストコンピュータを維持する認証センタにカードを登録し、カード番号、顧客の電子装置に対する通信アドレス（たとえば、顧客の移動電話機、携帯情報端末（ＰＤＡ）番号、電子アドレス等）、および個人認証番号（ＰＩＮ）を登録する。個人認証番号（ＰＩＮ）は顧客が選択してもよいし、コンピュータが顧客に割り当ててもよいが、第三者には漏らさない。個人認証番号（ＰＩＮ）は一般に１０進数であり、長さは４桁であることが多いが、他の長さであってもよく、多分、英数字ストリングであってもよい。顧客の口座番号、通信アドレス、および個人認証番号（ＰＩＮ）はホストコンピュータに互いに関連づけられて記憶される。これが行われると、たとえば、ＳＭＳプロトコルを経由して疑似ランダムセキュリティストリングを顧客の移動電話機に送ることにより、ホストコンピュータは疑似ランダムセキュリティストリングを顧客の電子装置に送信する。疑似ランダムセキュリティストリングはランダムに発生されたｎ桁の１０進数であってもよく、英数字ストリング等であってもよい。

【００１２】
本発明のシステムおよび方法は電子商取引シナリオで、またはより伝統的なショッピングシナリオで使用してもよい。

【００１３】
電子商取引シナリオでは、顧客は通常の仕方で商人のウェブサイトから商品やサービスを選択する。ウェブサイトでチェックアウトページに達したとき、顧客は自分のカード番号（顧客の口座番号）を入力するか、または別の方法で与え、支払うべき総額を決める。

次に、顧客は自分の個人認証番号（ＰＩＮ）と一緒に支払うべき総額を電子装置に入力する。そしてこれらは、所定の暗号アルゴリズムによって疑似ランダムセキュリティストリングと細切れ（ハッシュ：ｈａｓｈ）にされるか、または所定の暗号アルゴリズムによって疑似ランダムセキュリティストリングから抽出された「１回限りのコード」と細切れにされることにより、応答コードが作成される。特に好適な実施例では、応答コードは公知のクレジットカードまたはデビットカードの裏面に印刷された既存のＣＶＶ２型コードと同じフォーマットの３桁の１０進数である。しかし、使用される暗号アルゴリズムの性質に応じて、応答コードは任意の長さであってもよく、１０進数でなくてもよく、あるいは英数字ストリングであってもよい。通常程度の当業者には明らかなように、三つの入力に対してハッシュ（ごた混ぜ）機能を遂行できる多数の型の適切なアルゴリズムがあり、したがって本発明はこのようなアルゴリズムの細目に関係しない。しかし、例証として、周知の標準のＳＨＡ－１暗号ハッシュ［ＦＩＰＳ　ＰＵＢ　１８０－１］アルゴリズムを使用して１６０ビットの値を作成してもよく、このときこれを１０００で割るとき剰余が決まる。

【００１４】

電子装置が移動電話機である場合、暗号アルゴリズムは電話機の加入者インタフェースモジュール（ＳＩＭ：Ｓｕｂｓｃｒｉｂｅｒ　Ｉｎｔｅｒｆａｃｅ　Ｍｏｄｕｌｅ）カード上に、または多分、移動電話機の一部を形成する別個のメモリ装置に記憶してもよい。暗号アルゴリズムは好ましくはＳＩＭカードのアプレット（ａｐｐｌｅｔ）として動作し、電話機が受ける疑似ランダムセキュリティストリングを一つの入力として、支払い総額を第２の入力として、個人認証番号（ＰＩＮ）を第３の入力とする。第２の入力および第３の入力は通常の仕方で移動電話機に設けられたキーパッドを経由して手動で行ってもよい。暗号アルゴリズムは標準のメモリと処理装置を使用して、類似の仕方で任意の適当な電子装置（たとえば、携帯情報端末（ＰＤＡ）、ページング装置、パソコン等）上で動作させてもよい。

【００１５】

応答コードはアルゴリズムによって計算された後、電子装置のディスプレイに表示してもよい。次に、顧客は商人のウェブサイトの適当なデータ入力フィールドに応答コードを入力（このデータ入力フィールドは標準のＣＶＶ２コードの入力に現在使用されるデータフィールドであってもよい）した後、適当な操作を行って、顧客の口座番号、取引額、および応答コードを商人が運用するウェブサーバを経由して通常の仕方で商人に送信してもよい。カード有効期日および顧客住所のような付加的な安全情報を設けてもよい。

【００１６】

次に商人は、カード発行者が運用する検証サーバに顧客の口座番号、取引額、応答コード、および任意の他の安全情報を送ることにより、通常の仕方でカード発行者から取引に対する許可を得ることができる。検証サーバは顧客の口座番号から当該カードは本発明の一部を形成するホストコンピュータに登録されていることを確認した後、ホストコンピュータに接触して顧客の口座番号、取引額、および応答コードを送ることができる。

【００１７】

この情報を受信すると、ホストコンピュータは顧客の口座番号を使用して、顧客の電子装置に最初に発行された疑似ランダム安全コードと、顧客の個人認証番号（ＰＩＮ）を検索する。これらはどちらもホストコンピュータに記憶されているからである。このとき、ホストコンピュータが、電子装置で使用されているような同じ所定の暗号アルゴリズムを動作させて、疑似ランダム安全ストリング、取引額、および顧客の個人認証番号（ＰＩＮ）に作用してチェックコードを発生するのは簡単なことである。次に、ホストコンピュータはチェックコードを受信した応答コードと比較して一致するか調べる。一致すれば、ホストコンピュータはカード発行者の検証サーバに取引が許可されたことを報告する。次に、カード発行者は通常の仕方で顧客のカードの借方に記入し、商人の口座の貸方に記入することができる。

【００１８】

チェックコードと応答コードが一致しない場合には、取引は許可されず、カード発行者の検証サーバはこのときその取引を拒絶することができる。特定の顧客口座番号について開始された所定の回数（たとえば、３回）を超える取引の試みが許可手続きに失敗した場合、顧客の口座番号をホストコンピュータ、および選択的にカード発行者の検証サーバによって阻止してもよい。検証失敗が繰り返されるのは、そのカードが盗まれて、顧客の個人認証番号（ＰＩＮ）または疑似ランダム安全ストリングの知識のなく許可されていない者によって使用されているということを示す。顧客／カード保有者、カード発行者と認証センタの一方または両方の間の更なる通信だけでは顧客の口座番号は阻止されないかも知れない。顧客には新しい口座番号で新しいカードが発行される結果になるかも知れない。

【００１９】

取引がホストコンピュータによって許可されると、ホストコンピュータは新しい疑似ランダム安全ストリングを発生し、これを前と同様に顧客の電子装置に送信する。顧客は同一または異なる商人と同様に以後の取引を行ってもよい。しかし、疑似ランダム安全ストリングは取引毎に異なるので、詐欺者またはハッカーが遮断された通信を使用することによりシステムを破ることは非常に難しい。最も最近の取引の詳細、勘定残高、残りの貸出限度額等のような、それ以上の情報を含むメッセージの一部として、新しい疑似ランダム安全ストリングを送信してもよい。

【００２０】

本発明は、伝統的な取引のシナリオで使用されるとき、たとえば、顧客が店で買い物をする場合、または電話で取引を行う場合に、非常に類似の仕方で動作する。このシナリオでは、ウェブサイトを経由した商人とのインタフェースの代わりに、対面して、または電話で取引が行われる。顧客が買い物をしたいとき、顧客は商人に取引総額を尋ね、これを個人認証番号（ＰＩＮ）と一緒に電子装置に入力した後、演算された応答コードを商人に送る。顧客は顧客の口座番号および選択的なセキュリティの細部（たとえば、カードの有効期日）を商人に送る。これは一般に、クレジットカードまたはデビットカードを商人に引き渡して、ＥＰＯＳまたはＥＦＴＰＯＳ機器のような電子カードリーダに通すことにより行われる。演算された応答コードは口頭で商人に与えてもよいし、あるいは電子装置から電子的にたとえば、ＥＰＯＳまたはＥＦＴＰＯＳ機器に直接送信してもよい。次に、商人はＥＰＯＳまたはＥＦＴＰＯＳ機器等を使用して、通常の仕方でカード発行者が運用する検証サーバに顧客の口座番号、取引額、および応答コードを送信し、検証および許可プロセスが前と同様に進む。

【００２１】

商人がＥＰＯＳまたはＥＦＴＰＯＳ端末をそなえていない場合でも、本発明のシステムおよび方法を都合のよい仕方で具体化してもよい。周知のように、商人が検証センタに電話して、口頭で顧客の口座番号と取引額の詳細を伝えることによりカード許可を行ってもよい。したがって、商人が通常通りこれを行うことは容易であり、顧客から伝えられた応答コードも与えられる。次に、前と同様に許可と検証を進めることができる。

【課題を解決するための手段】

【００２２】

次に、本発明の利点のいくつかを説明するために、既存のカード検証プロトコルを参照して多数の安全上の問題を探索する。

【００２３】

（カードスキミング）

安全性に対するこの攻撃では、犯人が（多分、商人のウェブサイトにハッキングするか、または番号が入っている捨てられた取引領収書を拾い上げることにより）クレジットカード（顧客口座）番号を得た後、詐欺的取引を行おうとする。本発明ではこの攻撃が成功する見込みは低い。犯人は有効な応答コードを推測しなければならないからである（たとえば、３桁の１０進数の応答コードを成功裏に推測することには１：１０００の見込みである）。取引を行おうとして所定回数（たとえば、３回）失敗した後、ホストコンピュータはカードを阻止し（多分、ＳＭＳメッセージ等を介してカード保有者に通告し）、カー

ド発行者に通知する。カード発行者はカード保有者との対話に入って、カードの阻止を解除することができる。

【００２４】

（中間の人）

この攻撃では、犯人がクレジットカード番号と有効な応答コードを入手する。たとえば、犯人はレストランのウェータ（または堕落したウェブサイト）であり、顧客のカード番号と有効な応答コードにアクセスする。犯人のウェータは顧客が許可したのと同じ値に対する詐欺的な取引を行うことができるが、真正の取引は成功することはできない。これは、犯人のウェータはレストランの食事とちょうど同じ総額になる商品に対する１回の詐欺的取引を行うことができるが、レストランの取引は失敗することを意味する。この詐欺は容易に検出される（レストランのオーナがじきに金の紛失に気がつく）ので、起こりそうにないシナリオである。

【００２５】

（肩サーフィン）

この攻撃では、犯人はカード保有者の肩越しに、電子装置上で顧客が押すキーを見ることにより、顧客の個人認証番号（ＰＩＮ）を得る。詐欺的取引を成功裏に行うために、犯人はクレジットカード番号を必要とし、またカード保有者の電子装置（たとえば、移動電話機）も所有していなければならない。これは身体的な犯罪であり、犯人は個人認証番号（ＰＩＮ）を見た後、クレジットカードと電子装置を盗む必要がある。これは、個人認証番号（ＰＩＮ））の安全性を改善したり、カード保有者に関連の安全事項を助言したり（たとえば、カード保有者はカードと電子装置を決して一緒に持つべきでなく、また他の誰にも個人認証番号（ＰＩＮ）の入力を見せるべきでない）することにより克服される。

【００２６】

（応答コードの計算）

この攻撃では、犯人はクレジットカード番号を入手した後、有効な応答コードを計算する。応答コードを計算するために、犯人は個人認証番号（ＰＩＮ）と疑似ランダムセキュリティストリングの両方を知る必要がある。個人認証番号（ＰＩＮ）を推測するこのアプローチは、多分対象カード保有者が頻繁に訪れるウェブサイトを堕落させることにより多数の応答コードを入手することに依存する。しかし、個人認証番号（ＰＩＮ）を推測するためには、セキュリティストリングを知る必要がある（このストリングは事実上、はぎ取り式のパッドの中のランダム数のブロックで構成される１回限りのパッドであり、メッセージ毎にシートがはぎ取られ、これは完全に安全であることが知られている暗号技術である。セキュリティストリングを入手するためには、犯人はＧＳＭネットワーク上で暗号を攻撃するか、直接ホストコンピュータを攻撃するか、またはホストコンピュータと移動ネットワーク運用者の、対応するＳＭＳメッセージセンタ（ＳＭＣ）との間のリンクを攻撃する必要がある。成功する応答コード計算攻撃を開始するためには、犯人は（対面で、または電子商取引の状況での）取引を妨害するのと同時に安全なインフラストラクチャを攻撃することができる必要がある。したがって、この形式の攻撃は成功したり、やりがいのあることになる可能性は極めて低い。

【発明の効果】

【００２７】

本発明の実施例は、クレジットカードとデビットカードの取引を検証するための安全な方法およびシステムに下記の利点のいくつかまたは全てを与える。

・　商人またはカード保有者の新しいインフラストラクチャは必要としない。商人がＣＶＶ２プロトコルを稼働していれば、本発明のコンテキストで規定されているように顧客のカードがホストコンピュータに登録されているか知る必要がない。スマートカードの必要はないので、カード発行コストは低く維持される。

・　取引値が保証される。これは、商人が許可されない取引を行ったり、取引に隠された料金を上乗せすることはできない。

【００２８】

・　カード保有者はＳＭＳメッセージ等により自動的に各取引について知らされる。
・　カード保有者は移動電話機または同等の電子装置を必要とする。しかし、特別の移動電話機または装置の必要はない。カード保有者は、所定の暗号アルゴリズムを含むアプレットで電話機のＳＩＭカードをプログラミングする必要がある。移動電話の運用者によっては、「オーバ・ザ・エア（ＯＴＡ：ｏｖｅｒ　ｔｈｅ　ａｉｒ）プログラミングを使用する適当なアプレットを既存のＳＩＭにインストールすることができる。本発明で使用するのに適したアプレットは非常に簡単にすることができるので、ＳＩＭカードの大きなスペースを使用する必要はない。

【００２９】

・　販売時点情報管理（ＰＯＳ：ｐｏｉｎｔ－ｏｆ－ｓａｌｅ）での移動電話のカバレージは必要でない。カード保有者は取引と取引との間でＳＭＳメッセージを受信することができなければならない（したがって、取引と取引との間でカバレージ内になければならない。
・　移動電話機内のＳＩＭカードはカード保有者特有の個人認証番号（ＰＩＮ）、キー、または証明書を記憶する必要はない。したがって、カード保有者の設定には、（上記のアプレットが確実にＳＩＭにインストールされるようにする以外は）ＳＩＭプログラミングを必要としない。したがって、（たとえば、紛失またはサービス拒絶攻撃による）カード再発行のプロセスには、ＳＩＭカードの変更は必要でない。

【００３０】

以上説明してきたように、本発明のいくつかの実施例では、取引毎に新しい疑似ランダムセキュリティストリングが使用される（事実上、前に説明したように、セキュリティストリングは１回限りのパッドである）。各取引後にＳＭＳメッセージ等を介して疑似ランダムセキュリティストリングを配信することができる。しかし、場合によっては、次の取引を行うためにカード保有者は新しいＳＭＳメッセージ等を待たなければならないのは不便である（たとえば、カード保有者は移動電話のカバレージを備えていない店にいるが、二つ以上の取引を行うことを希望するかも知れない）。この状況に対処するため、多数の取引を行えるように本発明の実施例を構成してもよい。

【００３１】

原理は簡単である。顧客がホストコンピュータに登録することにより自分のカードを作動すると、ホストコンピュータから電子装置に単一の送信（たとえば、ＳＭＳメッセージ）が行われ、これにはｍ個の疑似ランダムセキュリティストリングのセットが含まれる（ここで、ｍは整数、たとえば、１２である）。アプレットは各取引を処理する毎にストリングを一つづつ消費する。電子装置内のアプレットに次のセキュリティストリングに進むように命令するために、カード保有者は「確認（ｃｏｎｆｉｒｍ）」メニューを選択する必要があるかも知れない（これは本発明の前に説明した実施例とは異なる。本発明の実施例では、単一のセキュリティストリングで新しいＳＭＳメッセージの受信によって確認は暗示的に選択される）。

【００３２】

所定のｎ番目（ｎは電子装置に最初に送信されるセキュリティストリングの総数ｍより小さい。たとえば、ｎは６であるかも知れない）の取引がホストコンピュータによって許可されたとき、ホストコンピュータからセキュリティストリングのもう一つのセットを含む電子装置に新しいメッセージが送られる。このアプローチにより、カード保有者はホストコンピュータからいかなる送信を受信する必要もなく、ｍ個までの買い物を行うことができる。これは、たとえば、移動電話ネットワークのカバレージがない等のときに有用である。各送信後に、ホストコンピュータからカード保有者の電子装置に簡単なメッセージを送って、確認と（商人、取引額、現在の残高、および残りのクレジットを示す）ミニステートメントとして作用させることができる。

【００３３】

このアプリケーションでは、最初の商人が販売時点情報管理（ＰＯＳ：ｐｏｉｎｔ－ｏｆ－ｓａｌｅ）での取引処理に失敗したとき、電子装置内で動作するアプレットとホスト

コンピュータが歩調を乱して、次の商人が次の取引を処理しないようにすることがある。もちろん、最初の商人にはこれを行う動機がない。処理は後で失敗するかも知れないからである（たとえば、ユーザが正しくない応答コードを引き渡したかも知れない）。それにも拘わらず、この状況は（多分、カード保有者または商人から認証センタへの呼に続いて）ホストコンピュータでカードをリセットすることにより処理することができる。次に、ホストコンピュータは新しいセキュリティストリングのセットを送って、プロセスを再開することができる。

【００３４】

最初の商人が取引を処理するようになったとき（または場合）、ホストコンピュータはその取引を受け入れるべきか、拒絶すべきか判定できる可能性が非常に高い。再設定がトリガされたときに残っているセキュリティストリング（すなわち、取引を有効にするためにまだ使用されていないストリング）はｎ個とｍ個との間である。ホストコンピュータはこれらのセキュリティストリングのレコードを備えており、最初の商人からの取引は残っているセキュリティストリングの中の最も古いセキュリティストリングに対してランして、合致するか見ることができる。合致の失敗には次の二つの可能性がある。（ｉ）取引が失敗した（取引が詐欺的である、またはカード保有者が間違いをした、または商人が間違いをした）、もしくは（ｉｉ）直ちに処理されなかった二つ以上の取引がある。（ｉｉ）の場合には、ホストコンピュータは別のセキュリティストリングに対して取引をランするように試みることができる。もちろん、商人が正しい手順に従うのに失敗したために取引が単に拒絶されることもあり得る。

【００３５】

（ＥＰＯＳまたはＥＦＴＰＯＳ端末としての移動電話機等の使用）

本発明を採用することにより、取引で処理されている情報のセキュリティ状態が変化する（たとえば、カード番号と応答コードを知ることは詐欺的な取引を行うには不充分である）。これは、必要な取引情報（カードまたは顧客の口座番号、応答コード、取引額等）をホストコンピュータに供給する代わりの方法を使用できるということを意味する。

【００３６】

移動電話機または携帯情報端末（ＰＤＡ）等が、商人が処理システムにアクセスできるようにする優れた手段を提供する。取引は（予め規定されたフォーマットを使用して）ＳＭＳメッセージ等に記述して、適当な取得ネットワークによって設定された電話番号に送ることができる。メッセージを受信する取得ネットワークは取引情報を抽出し（移動電話機等の発信元電話番号から商人の身元（ｉｄｅｎｔｉｔｙ）を推測し）た後、通常の仕方で取引を処理する（貸出限度額のチェック、ホストコンピュータのアクセス等）。取引の容認または拒絶がもとの移動電話機等へのＳＭＳメッセージ等を介して商人に返送される。

【００３７】

このアプローチは商人にカード処理ネットワークの一部となる低コストの方法を提供し、投下資本の少ない小企業に特に有用である。このアプローチにより、一定ラインのインフラストラクチャを得ることが難しい領域（たとえば、タクシー内で）カードを処理することもできる。

【実施例】

【００３８】

本発明のより良き理解のためと、またどのように実施するかを示すために、付図を参照して例を説明する。

【００３９】

図１に、ホストコンピュータ１０が示されており、これは許可サーバとして動作する。カード発行者により顧客にカードが発行されたとき、顧客はまずそのカードをホストコンピュータ１０に登録し、顧客の口座番号（カード番号）、個人識別番号（ＰＩＮ）、移動電話番号等、および他の任意の有用な情報、たとえば、顧客名と住所といった詳細を与える。これが行われると、ホストコンピュータ１０は少なくとも一つの疑似ランダムセキュ

リティストリングを発生し、これをステップ１を介して、顧客が操作する移動通信装置１１に送信する。移動通信装置１１は移動電話機、携帯情報端末（ＰＤＡ）、ページング装置等であってよい。送信１はＳＭＳメッセージ、電子メール等を経由して行ってよい。ホストコンピュータ１０はそのメモリ内でこの少なくとも一つの疑似ランダムセキュリティストリングを顧客の口座番号および個人識別番号（ＰＩＮ）と対応づける。

【００４０】

顧客が商人１３と取引を行いたいときは、顧客はキーパッド等を経由して取引額および個人識別番号（ＰＩＮ）を移動通信装置１１に入力する。装置１１内に設けられ、片方向暗号ハッシュアルゴリズム１２とプログラミングされたＳＩＭカード等の中で動作するアプレットは、ステップ２を介して与えられる疑似ランダムセキュリティストリングと一緒に、ユーザが入力した取引額および個人識別番号（ＰＩＮ）を取り入れ、これらを一緒に細切れにして、３桁の応答コードを発生する。この３桁の応答コードはステップ３を経由して商人１３に送られる。応答コードは対面して、または電話取引において口頭で、もしくは電子商取引をおこなっているとき商人のウェブサイトを経由して商人１３に与えてもよい。

【００４１】

一方、商人１３は、多分、カードをＥＰＯＳまたはＥＦＴＰＯＳ端末に通して強打するか、または他の適当な手段により顧客の口座番号および取引額を取り入れた後、ステップ４を経由して公知の仕方でこの情報を応答コードと一緒にカード取得ネットワークサーバ（ＣＡＮＳ：Ｃａｒｄ　Ａｃｑｕｉｒｅｒ　Ｎｅｔｗｏｒｋ　Ｓｅｒｖｅｒ）１４に送る。商人１３はステップ４を経由してカード取得ネットワークサーバ（ＣＡＮＳ）１４に商人身元情報も送信する。これにより、カード取得ネットワークサーバ（ＣＡＮＳ）１４は取引を（顧客口座番号により）顧客と対応づけるだけでなく、商人１３とも対応づけることができる。

【００４２】

カード取得ネットワークサーバ（ＣＡＮＳ）１４はステップ５を経由して公知の仕方で顧客の口座番号、取引額、および応答コードをホストコンピュータ１０に送る。次に、ホストコンピュータ１０はカード取得ネットワークサーバ（ＣＡＮＳ）１４から受信した顧客口座番号を使用して、そのメモリから顧客の個人識別番号（ＰＩＮ）および（最初にステップ１で移動通信装置１１に送信された）疑似ランダムセキュリティストリングを検索した後、疑似ランダムセキュリティストリング、顧客の個人識別番号（ＰＩＮ）、および取引額を片方向暗号ハッシュアルゴリズム１２に入力する。この片方向暗号ハッシュアルゴリズム１２は、今度はアルゴリズム１２がホストコンピュータ１０の中で動作する点を除けば、移動通信装置１１内のアプレットで動作する片方向暗号ハッシュアルゴリズム１２と同じである。アルゴリズムは３ディジットのチェックコードを出力し、これは取引が有効なとき、与えられた応答コードと合致する。ホストコンピュータ１０の中で動作するアルゴリズム１２は移動通信装置１１内のアプレットで動作するアルゴリズム１２と同一の入力に対して動作するからである。したがって、与えられた応答コードと計算されたチェックコードとが合致することがホストコンピュータ１０により検出されれば、取引は許可され、ステップ６を経由して許可信号がホストコンピュータ１０からカード取得ネットワークサーバ（ＣＡＮＳ）１４に送られる。

【００４３】

これに反して、計算されたチェックコードと与えられた応答コードとが合致しなければ、取引はホストコンピュータ１０により拒絶され、ステップ６を経由して拒絶信号がカード取得ネットワークサーバ（ＣＡＮＳ）１４に送られる。

カード取得ネットワークサーバ（ＣＡＮＳ）１４がホストコンピュータ１０から許可信号を受信すると、顧客のカード口座の借方に取引額が通常の仕方で記入される。借方に記入される取引額は商人１３の身元と対応づけられる。更に、カード取得ネットワークサーバ（ＣＡＮＳ）１４は商人の口座の貸方に取引額を通常の仕方で記入する。カード取得ネットワークサーバ（ＣＡＮＳ）１４はステップ７を経由して商人１３に許可信号も送る。

次に、商人はステップ７を経由して取引が許可されたことを顧客に通知する。

【００４４】

一方、ホストコンピュータ１０が取引を許可すると、ホストコンピュータ１０はステップ１を経由して、取引の許可、取引額、およびカード口座の残高を確認する選択的情報と一緒に新しい疑似ランダムセキュリティストリングを顧客の移動通信装置１１に送信する。

【００４５】

応答コードと計算されたチェックコードとが合致しないことがホストコンピュータ１０によって検出されたために取引が許可されない場合、カード取得ネットワークサーバ（ＣＡＮＳ）１４はステップ７を経由して商人１３に拒絶信号を送り、顧客のカード口座の借方に記入したり、商人の口座の貸方に記入したりすることはない。拒絶信号を受信すると、商人１３は取引を拒絶するか、または顧客からもう一つの応答コードを要求することができる。ホストコンピュータ１０で計算されたチェックコードと合致し損なう３個の応答コードを顧客が相次いで与えた場合、ホストコンピュータ１０は顧客の口座を阻止し、その旨の信号をカード取得ネットワークサーバ（ＣＡＮＳ）１４に送ることができる。このようにして、顧客がホストコンピュータ１０を運用している認証センタに連絡するまで、カードのそれ以上の使用が妨げられる。顧客のカードが盗まれ、個人識別番号（ＰＩＮ）または疑似ランダムストリングを知らない第三者によって詐欺的に使用されているということかも知れない。新しいカードを発行する必要があるかも知れない。

【００４６】

本発明の各実施例の利点を更に説明するために、次に代表的なシナリオを説明する。

【００４７】

アリスは本発明とともに使用するためのカードを入手しようと決心した。彼女はこれを二つの理由で行う。第１に、彼女はインタネットで安全に買い物できることを確かめることを希望する（ハッカーがウェブサイトに侵入し、クレジットカード番号、名前、住所、電話番号等を盗むことがどんなに容易かということについて読んでいた）。第２に、彼女はカードを希望し、他の誰も彼女にカードを与えない。アリスは１５才であり、クレジットカードを入手するには若過ぎる。しかし、本発明により保護されるカードは商人１３とカード保有者を生じ得る相互の不正行為から保護するので、いくつかの銀行はティーンエージャに前払いの保護されたカードを発行する用意ができている。

【００４８】

学校に居る間に、アリスは（彼女のインタネットバンキング口座を使用して）彼女の銀行のウェブサイトに進み、カードを送るように要求する。彼女は銀行に彼女の移動電話番号（および彼女の移動の運用者が誰であるか）も伝え、個人識別番号（ＰＩＮ）を選択する。彼女は彼女のカードに特別な絵をそなえるオプションをチェックし、彼女のパソコンからディジタル写真をアップロードする（カーボン紙上に強打されることはないので彼女のカードは浮き彫りになっていない）。

【００４９】

銀行はカードに対する要求の処理を開始する。本発明で使用するための適当なアプレットでプログラミングされたＳＩＭを移動運用者が使用することを銀行は確認する。次に銀行はアリスのためのカードを作成し、カード番号、アリスの個人識別番号（ＰＩＮ）、および彼女の移動電話番号を独立の認証センタが運用するホストコンピュータ１０に送信する（ホストコンピュータ１０は他のいかなる情報も必要としない）。

【００５０】

２、３日後にアリスのカードが郵便箱に到達する。アリスは彼女のインタネット銀行口座に進んで、カードが到着したということを銀行に告げる。彼女は１５０ユーロもカードに移す。彼女は２、３秒後に彼女の電話機１１で彼女のカードの使用の用意ができたというテキストメッセージを受ける（ステップ１）（このメッセージは１２個のセキュリティストリングも含んでいるが、彼女は必ずしもこれに気がつかない）。

【００５１】

アリスはウェブでショッピングを行い、彼女の母に誕生日プレゼントを買おうとしている。彼女は、園芸装置を販売するウェブサイト１３を訪れ、理想的なプレゼントである金メッキされたじょうろを見つける。代価は郵便料金込みで５０．００ユーロである。彼女は「チェックアウト」ページに進み、支払いのため彼女のカードを取り出す。サイトは彼女のカードの裏面の最後の３ディジットを求める。彼女のカード上では、最後の３ディジットは「＊＊＊」と表示されている。彼女はより綿密に見て、カードに「＊＊＊に対する応答コードを使用」という表現を含んでいるということに気がつく。彼女は、カードと一緒に送られた情報リーフレットでこれについて読んだことを思い出す。彼女は彼女の移動電話機１１を取り出し、メニューから「カード支払い」を選択し（これはアプレットを起動する）、彼女の個人識別番号（ＰＩＮ）を入力し（ステップ２）、「ＯＫ」キーを押す。次に、彼女は５０．００の取引額をキーインし（ステップ２）、「ＯＫ」を押す。次に、電話機１１のＳＩＭカードで動作するアプレットはアルゴリズム１２を個人識別番号（ＰＩＮ）、取引額、および（ステップ２で与えられた）セキュリティストリングに適用して３ディジットの応答コードを発生し、電話機１１は「応答コード：１３２」を表示する。彼女は３ディジットを要求しているウェブサイト１３のボックスに「１３２」とタイプする（ステップ３）。ウェブサイト１３は「処理指示・・・」と表示する。

【００５２】

ウェブ商人のサーバは取引の詳細（カード番号、額、アリスの住所、そしてそれが考えている３ディジットのコードはＣＶＶ２コードである）をカード処理コンピュータに引き渡す（ウェブ商人はサービス会社を使用してカード取引を処理している）。次に、このコンピュータはカード番号を見て、適当なカード取得ネットワークサーバ（ＣＡＮＳ）１４にコンタクトする（ステップ４）。コンピュータは同じ取引の詳細を引き渡す。

【００５３】

カード取得ネットワークサーバ（ＣＡＮＳ）１４は支払いをするのに充分な金がカード上にあることをチェックする。このチェックは合格する（カード口座には１５０ユーロ入っており、取引は５０ユーロである）。次に、カード取得ネットワークサーバ（ＣＡＮＳ）１４はカード番号、額、および３ディジットの応答コードでホストコンピュータ１０を呼び出す（ステップ５）。ホストコンピュータ１０はカード番号を使用して、それがアリスの移動電話機１１に発行したアリスの個人識別番号（ＰＩＮ）およびセキュリティストリングを捜す。ホストコンピュータ１０は（それが捜したセキュリティストリングと個人識別番号（ＰＩＮ）の他にカード取得ネットワークサーバ（ＣＡＮＳ）１４が引き渡した取引額を使用して）アリスの移動電話機１１のＳＩＭ内のアプレットが動作しているのと同じ暗号ハッシュアルゴリズム１２を動作させる。ホストコンピュータ１０は、アリスが移動電話機のディスプレイから読出した応答コードに対応するチェックコードを算定する。演算されたチェックコードとカード取得ネットワークサーバ（ＣＡＮＳ）１４によってホストコンピュータ１０に与えられた応答コードが合致するので、取引は有効であるとみなされ、許可される。

【００５４】

ホストコンピュータ１０はセキュリティチェックに合格したことをカード取得ネットワークサーバ（ＣＡＮＳ）１４に伝え（ステップ６）、新しいセキュリティストリングを作成する。カード取得ネットワークサーバ（ＣＡＮＳ）１４はホストコンピュータ１０に商人１３の身元および彼女のカード上の現在の残高を伝える。ホストコンピュータ１０はこの情報を取り込み、これを新しいセキュリティストリングとともにテキストメッセージ（ステップ１）でアリスの移動電話機１１に送る。カード取得ネットワークサーバ（ＣＡＮＳ）１４は取引が決済されたことをカード処理コンピュータに伝える。カード処理コンピュータはこれをウェブ商人のサーバ１３に伝える。ウェブサーバ１３は支払いが容認されたことをアリスに伝える。２、３秒後にアリスはホストコンピュータ１０から彼女の移動電話機１１でテキストメッセージを得る（ステップ１）。テキストメッセージは「プレゼント直接５０．００ユーロ。残高１００．００ユーロ」と表示される。

【００５５】

アリスは更に買い物をするため町に行く。彼女の気に入りの書店で、彼女は信号がないため彼女の移動電話機１１で友達を呼び出せないことに気がつく（彼女は店の外側にカバレージがあるのでこれは奇妙だと思う。しかし、店は鋼鉄の枠組みになっており、鉄筋コンクリートで覆われているので、移動電話機の信号が阻止されることに気がついていない）。とにかく彼女は欲しい本を見つけて、支払おうとする。チェックアウトで店員が彼女に総額が２０．５５ユーロであると告げる。彼女はカードを店員に渡した後、自分の移動電話機１１を取り出す。彼女はメニューから「カード支払い」を選択し（これはアプレットを起動する）、自分の個人識別番号（ＰＩＮ）をキーインした（ステップ２）後、「ＯＫ」を押す。次に、彼女は２０．５５の取引額を入力し（ステップ２）、「ＯＫ」を押す。次に、アプレットは１２個の最初に与えられたセキュリティストリングのセットの中の一つのセキュリティストリングを第３の入力として取り込み、アルゴリズム１２により応答コードを計算する。電話機１１は「応答コード：４５１」と表示する。

【００５６】

一方、店員はＥＰＯＳ機械１３の中でアリスのカードを強打した。機械１３はカード番号を読み取り、アリスの銀行が使用するカード取得ネットワークサーバ（ＣＡＮＳ）１４に電話をかける。電話呼の他方の端にあるカード取得ネットワークサーバ（ＣＡＮＳ）１４はＥＰＯＳ機械１３に取引額を読み取るように求める。店員は２０．５５をキーインする。次に、店員は応答コードをＥＰＯＳ機械１３に入力し、応答コードはカード取得ネットワークサーバ（ＣＡＮＳ）１４に送られる（ステップ４）。

【００５７】

カード取得ネットワークサーバ（ＣＡＮＳ）１４は支払いをするのに充分な金がカード上にあることをチェックし、カード番号、額、および応答コードでホストコンピュータ１０を呼び出す（ステップ５）。ホストコンピュータ１０はチェックコード４５１を算定する。このチェックコードは、アリスが自分の移動電話機のディスプレイから読出した応答コードと合致するはずである。演算されたチェックコードとカード取得ネットワークサーバ（ＣＡＮＳ）１４によってホストコンピュータ１０に与えられた応答コードが合致することが見出されるので、取引は有効である。ホストコンピュータ１０はセキュリティチェックに合格したことをカード取得ネットワークサーバ（ＣＡＮＳ）１４に伝え（ステップ６）、新しいセキュリティストリングを作成する。カード取得ネットワークサーバ（ＣＡＮＳ）１４はホストコンピュータ１０に商人１３の身元および彼女のカード上の現在の残高を伝える。ホストコンピュータ１０はこの情報を取り込み、これを新しいセキュリティストリングとともにテキストメッセージでアリスの移動電話機１１に送る（ステップ１）。

【００５８】

カード取得ネットワークサーバ（ＣＡＮＳ）１４は取引が決済されたことをＥＰＯＳ機械１３に伝える（ステップ７）。ＥＰＯＳ機械１３は「ＯＫ」メッセージを表示することにより、取引が決済されたことを店員に知らせる。店員はアリスに彼女のカードと本が入ったバッグを渡す。アリスは店を出て、雨が激しく降っていることを知る。彼女はタクシーで帰宅することに決め、通りを横断する。ちょうど反対側に着いたとき、電話機１１でテキストメッセージを得る（ステップ１）。テキストメッセージは「アクメ書店２０．５５ユーロ。残高７９．４５ユーロ」と表示される。彼女が見ないことは、メッセージにより彼女の移動電話機１１に新しいセキュリティストリングも入り、彼女が自分のカードを使う次回に備えたということである。

【００５９】

到着すると、タクシー運転手は料金が２２．５０ユーロであると彼女に告げる。彼女はチップ込みで２５．００ユーロを取るように彼に告げる。彼女は運転手に彼女のカードを渡し、自分の移動電話機１１上のメニューから「カード支払い」を選択し、自分の個人識別番号（ＰＩＮ）を入力して、「ＯＫ」を押す。次に彼女は２５．００をキーインし（ステップ２）、「ＯＫ」を押す。電話機１１はアルゴリズム１２を個人識別番号（ＰＩＮ）、取引額、およびセキュリティストリングに適用した後、「応答コード：７２２」とディ

スプレイする。一方、タクシー運転手は彼の移動電話機１３に新しいテキストメッセージを書き込み始めた。彼はアリスのカード番号と２５．００の処理額をキーインする。彼はアリスに彼女の応答コードを尋ね、彼女は「７２２」と言う（ステップ３）。彼はメッセージ中に７２２をタイプし、これを（彼の電話機１３のアドレス帳に記憶されたカード取得ネットワークサーバ（ＣＡＮＳ）１４の移動番号に送る（ステップ４）。

【００６０】

カード取得ネットワークサーバ（ＣＡＮＳ）１４はメッセージを受信する。カード取得ネットワークサーバ（ＣＡＮＳ）１４は送り手の電話番号を捜し、それがタクシー運転手（彼一人の会社である）に登録されていることを知る。カード取得ネットワークサーバ（ＣＡＮＳ）１４はアリスのカード口座に取引に充分な金があることを確認する（口座に７９．４５ユーロがあり、取引額は２５．００ユーロである）。次に、カード取得ネットワークサーバ（ＣＡＮＳ）１４はホストコンピュータ１０にコンタクトし、カード番号、額（２５．００ユーロ）、および応答コード（７２２）を伝える（ステップ５）。ホストコンピュータ１０は応答コードを独立に計算されたチェックコードと比較することにより応答コードが有効であることを確認し、カード取得ネットワークサーバ（ＣＡＮＳ）１４に成功を示す（ステップ６）。カード取得ネットワークサーバ（ＣＡＮＳ）１４はタクシー運転手の電話機１３に取引が成功したことを示すＳＭＳメッセージを送り（ステップ７）、ホストコンピュータ１０に商人の身元と新しいカード残高（５４．４５ユーロ）を伝える。

【００６１】

タクシー運転手は「取引は許可された」というテキストメッセージをカード取得ネットワークサーバ（ＣＡＮＳ）１４から受ける（ステップ７）。彼はアリスに支払いはＯＫであると告げ（ステップ８）、彼女はタクシーを降りる。２、３秒後に彼女は彼女の移動電話機１１でテキストメッセージを得る（ステップ１）。テキストメッセージは「ジョンのタクシー２５．００ユーロ。残高５４．４５ユーロ」と表示される。アリスは自分の家に入る。

【００６２】

翌日、アリスは町にいるとき、彼女は自分のカードが紛失していることに気がつく。タクシー運転手がカードを彼女に返すのを忘れたに違いない。彼女は彼女の銀行を呼び出して告げる。銀行は問題がないこと、そして直ちにもう１枚のカードを彼女の家に送ると彼女に告げる。翌日、新しいカードが郵便箱に到達する。銀行はアリスのためカード番号を変更したり、新しい個人識別番号（ＰＩＮ）を作成しょうとしない。犯人が古いカードで支払いを行うことはできないということを銀行は知っている。アリスは喜ぶ。彼女は自分のカードの詳細が変わったり、新しい個人識別番号（ＰＩＮ）を覚えなければならないという面倒を望んでいない。銀行にも都合がよい。カードのもう一つのコピーを印刷してこれをポストに入れる以外の作業をする必要がない。

【産業上の利用可能性】

【００６３】

したがって、本発明の各実施例は既存のＣＶＶ２プロトコルに対して大幅に改善されている。それらはすべての関係者について詐欺から保護する。たとえば、カード保有者はまちがった商人（またはそれらのスタッフ）から保護され、そして商人は盗まれたカードまたは詐欺的カード保有者から保護される。

【００６４】

（カード発行者と商人に都合のよい）カード詐欺を無くすとともに、本発明の各実施例はカード保有者に直接の利益を与える。紛失または盗まれたカードを取り替えることはやっかいでなく、またカードのステートメントを綿密に調べることは重要でない。

【００６５】

本発明の各実施例の安全性の性質はインフラストラクチャの更なる進展の可能性を開く。たとえば、低コストで簡単な商人施設の導入方法は、カードの使用を今日実現可能でない地域に拡張できるということを意味する（皮肉なことに、多くの開発途上国は素晴らし

く立派な無線電信のインフラストラクチャを備えているが、固定線路のインフラストラクチャは貧弱なままである）。このアプローチは普通の個人にカードでの支払いを行う可能性も提供する（中古の自動車またはコンピュータ装置のような品物に対して高額の支払いをするのに極めて有用である）。

【００６６】

本発明の各実施例のもっとも重要な利点の一つはこれらの利益があまりインフラストラクチャ投資せずに得られるということである。したがって、個人金融産業に新しい可能性を開くのと同時に詐欺を減らす優れた機会が得られる。

【００６７】

本発明の好適な各特徴は本発明のすべての側面に適用可能であり、可能な任意の組み合わせで使用してもよい。

【００６８】

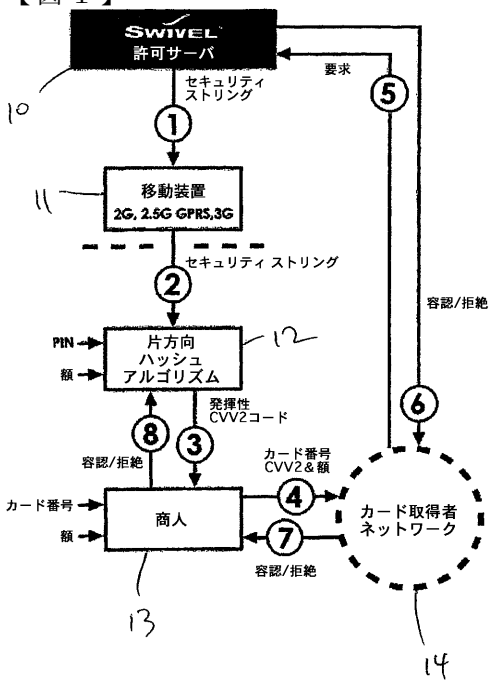
明細書の説明および請求の範囲を通じて、「含む」および「備える」という表現、そしてこれらの表現の変形、たとえば「含んでいる」および「備えている」等は「を含んでいるが、それらに限定されない」ということを意味し、他の構成要素、完全体、部分、付加物、またはステップを排除することを意図していない（そして排除しない）。

【図面の簡単な説明】

【００６９】

【図１】本発明の一実施例のインフラストラクチャの概略図を示す。

【図１】



【手続補正書】
【提出日】平成16年6月18日(2004.6.18)
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】０００５
【補正方法】変更
【補正の内容】
【０００５】
ある人、たとえばクレジットカードまたはデビットカード保有者の身元（ｉｄｅｎｔｉｔｙ）を確認するための改良された方法およびシステムが、本出願者の係属英国特許出願第００２１９６４２号、国際特許出願第ＰＣＴ／ＧＢ０１／０４０２４号、および米国特許出願第０９／６６３，２８１号と第０９／９１５，２７１号に開示されている。この方法およびシステムでは、カード取引を行う前にある人の移動電話機等に疑似ランダムストリングが送信される。その人は次に、個人識別番号（ＰＩＮ：ｐｅｒｓｏｎａｌ　ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　ｎｕｍｂｅｒ）の形式のマスクコードを所定の仕方で疑似ランダムストリングに印加して、揮発性の１回限りの取引識別コードを発生する。この揮発性の１回限りの取引識別コードは商人に送られた後、認証サーバに送られ、そこで独立に計算された揮発性の１回限りの識別コードと照合され、カード保有者の身元が確認される。
ＷＯ０１／９９３７８は顧客からサービスプロバイダへの委任の認証のための方法およびシステムを開示する。これによれば、一組のランダムに発生されたコードワードが、移動電話機の加入に対応してデータベースと同様移動電話機の加入に対応するメモリ回路に記憶される。この方法は、顧客の身元を確認し、顧客の身元に基づいて移動電話機の加入を識別し、メモリ回路からコードワードを検索し、委任を認証するために移動電話機の加入に対応づけられたデータベース内に設定されたコードワード内のコードワードの存在をチェックする、ステップとを含む。しかし、この方法およびシステムでは、移動電話機のメモリ回路は安全なサーバにより安全なロケーションで、かつコードワードの完全なセットで予めプログラミングされていなければならない。そして、メモリ回路（たとえば、ＳＩＭカード）は安全性の高い条件下で移動電話機の小売商人に配送されなければならない。その上にプログラミングされたコードワードのセットは非常に価値があり、遠隔手段によって変更できないからである。
ＷＯ９８／３７６６３は、取引の要素、なかでも取引の額を示したり認証するために、ＳＩＭカードを使用して演算を行うための方法を開示する。
ＧＢ２　３２８　３１０は、許可すべき取引に関する情報および１回限りの予測不可能なコードを受信するための電子ページング装置を含む電子取引と許可のシステムを開示する。取引情報が正しいことを確認した後、取引を認証するために直接または被支払者を経由してユーザはコードを認証センタに送信する。このシステムでは、取引を行うとき、ユーザはページング装置のカバレージ区域内にいなければならない。情報の送受信は取引の場所で実時間で行われなければならないからである。ページング装置が無線通信を受信できない位置ではシステムは動作しない。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Interna Application No
PCT/GB 03/01075

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10 G07F19/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F H04Q G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 4 862 501 A (T. KAMITAKE ET ALL.) 29 August 1989 (1989-08-29)	1,14
A	abstract; claims; figures column 5, line 26 -column 7, line 35	9,21
Y	WO 98 37663 A (POSTGIROT BANK) 27 August 1998 (1998-08-27)	1,14
A	the whole document	2,12,15, 24
Y	WO 95 19593 A (M.J. KEW ET ALL.) 20 July 1995 (1995-07-20)	1,14
A	abstract; claims; figures	2,7-9, 11-13, 15, 19-21, 23-25

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 October 2003	23/10/2003

Name and mailing address of the ISA
European Patent Office, P.B. 5818 Patentlaan 2
NL – 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer
David, J

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interm Application No
PCT/GB 03/01075

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	GB 2 328 310 A (HO KEUNG TSE) 17 February 1999 (1999-02-17) abstract; claims; figures page 5, paragraph 2 -page 8, paragraph 2	1,2,8,9, 11,14, 15,20, 21,23
X,P	WO 02 082387 A (MICROCELL 15) 17 October 2002 (2002-10-17) abstract; claims; figures page 8, line 1 -page 12, line 27	1,2,7,8, 14,15, 19,20
A	DE 198 20 422 A (GIESECKE & DEVRIENT) 11 November 1999 (1999-11-11)	
A	WO 01 99378 A (ICL INVIA) 27 December 2001 (2001-12-27)	

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Internati Application No
PCT/GB 03/01075

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 4862501 A	29-08-1989	DE 3672854 D1	30-08-1990
		EP 0194839 A2	17-09-1986
		JP 1961230 C	10-08-1995
		JP 6091526 B	14-11-1994
		JP 62000140 A	06-01-1987
		KR 9000123 B1	20-01-1990
WO 9837663 A	27-08-1998	SE 508844 C2	09-11-1998
		AU 725952 B2	26-10-2000
		AU 6126898 A	09-09-1998
		BR 9807372 A	14-03-2000
		CN 1248367 T	22-03-2000
		EP 0962071 A1	08-12-1999
		JP 2001513274 T	28-08-2001
		NO 993939 A	19-10-1999
		SE 9700587 A	20-08-1998
		WO 9837663 A1	27-08-1998
		US 6556680 B1	29-04-2003
WO 9519593 A	20-07-1995	AU 1390395 A	01-08-1995
		WO 9519593 A1	20-07-1995
		GB 2300288 A	30-10-1996
GB 2328310 A	17-02-1999	NONE	
WO 02082387 A	17-10-2002	WO 02082387 A1	17-10-2002
		US 2003055738 A1	20-03-2003
DE 19820422 A	11-11-1999	DE 19820422 A1	11-11-1999
		AU 3824199 A	23-11-1999
		CN 1299497 T	13-06-2001
		WO 9957689 A1	11-11-1999
		EP 1076887 A1	21-02-2001
		JP 2002514024 T	14-05-2002
WO 0199378 A	27-12-2001	FI 20001497 A	23-12-2001
		FI 20010291 A	23-12-2001
		AU 7257501 A	02-01-2002
		EP 1305926 A1	02-05-2003
		WO 0199378 A1	27-12-2001
		US 2003128822 A1	10-07-2003

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IT,LU,MC,NL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NI,NO,NZ,OM,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

(72)発明者 キーチ、ウィンストン、ドナルド
イギリス国、ノース ヨークシャー、ウィットビー、 リトル ベック、ブリーチ ガース

Ｆターム(参考) 3E044 BA05 DA06 DD01 DE01
5J104 KA03 PA01 PA07 PA10

【要約の続き】
合致した場合には、取引が許可される。本発明の各実施例は既存のＣＶＶ２セキュリティインフラストラクチャを使用するが、著しく高い安全性を提供する。本発明の各実施例は普通の対面または電話での取引で使用してもよいが、（ウェブに基づく）電子商取引および（移動電話機に基づく）移動商取引で使用してもよい。