(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2009-0051147
(43) 공개일자 2009년05월21일

(51) Int. Cl.
G06Q 20/00 (2006.01) *G06F 21/20* (2006.01)
G06F 15/16 (2006.01)
(21) 출원번호 10-2008-7031300
(22) 출원일자 2008년12월23일
심사청구일자 없음
번역문제출일자 2008년12월23일
(86) 국제출원번호 PCT/JP2006/313658
국제출원일자 2006년07월10일
(87) 국제공개번호 WO 2008/004312
국제공개일자 2008년01월10일
(30) 우선권주장
JP-P-2006-188341 2006년07월07일 일본(JP)

(71) 출원인
가부시기가이샤제이씨비
일본국 도쿄 미나토쿠 미나미 아오야마 5가 1번 22호
(72) 발명자
타나카 슌
일본국 도쿄도 미나토쿠 미나미 아오야마 5쵸메 1반 22고 가부시기가이샤제이씨비 코쿠사이 인프라 스이신부 나이
카와카츠 미츠유키
일본국 도쿄도 미나토쿠 미나미 아오야마 5쵸메 1반 22고 가부시기가이샤제이씨비 코쿠사이 인프라 스이신부 나이
(74) 대리인
하영욱

전체 청구항 수 : 총 7 항

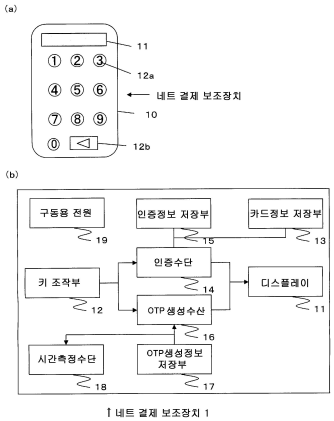
(54) 네트 결제 보조장치

(57) 요 약

(과제) 카드번호나 암증번호를 도청, 개찬당할 위험성이 없고, 보다 안정되게 네트 상거래를 행하는 것이 가능한 네트 결제 보조장치의 제공.

(해결수단) 디스플레이(11)와, 카드 계약자의 카드정보가 외부로부터 판독될 수 없는 상태로 미리 저장된 카드정보 저장부(13)와, 계약자의 인증정보가 외부로부터 판독될 수 없는 상태로 미리 저장된 인증정보 저장부(15)와, OTP 생성정보가 외부로부터 파독될 수 없는 상태로 미리 저장된 OTP 생성정보 저장부(17)와, 숫자키(12a)와, 숫자키(12a)로부터의 입력정보에 기초하여 조작자의 본인 인증을 행하여 카드정보를 디스플레이(11)에 표시하는 인증수단(14)과, 카드정보가 표시된 후 OTP 생성정보에 기초하여 일회용 패스워드를 생성하여 디스플레이(11)에 표시하는 OTP 생성수단(16)을 구비하고, 일회용 패스워드에 의해 계약자의 본인 인증이 행해져서 네트 상거래가 가능하게 된다.

대 표 도 - 도1



도1 네트 결제 보조장치 1

특허청구의 범위

청구항 1

가반형의 네트 결제 보조장치로서:

디스플레이와,

신용카드나 직불카드 등의 카드 계약자의 식별정보를 적어도 포함하는 카드정보가 외부로부터 판독될 수 없는 상태로 미리 저장된 카드정보 저장부와,

상기 계약자의 본인 인증을 행하기 위한 인증정보가 외부로부터 판독될 수 없는 상태로 미리 저장된 인증정보 저장부와,

상기 카드정보에 관련되어 상기 네트 결제 보조장치에 고유의 OTP 생성정보가 외부로부터 판독될 수 없는 상태로 미리 저장된 OTP 생성정보 저장부와,

상기 인증정보를 입력하는 입력수단과,

상기 입력수단으로부터 입력된 입력정보에 기초하여 상기 네트 결제 보조장치의 조작자가 상기 계약자인지 아닌지의 본인 인증을 행하고, 본인 확인이 되었을 경우에 상기 카드정보 중 적어도 상기 식별정보를 판독하여 상기 디스플레이에 표시하는 인증수단과,

상기 카드정보가 표시된 후에 상기 OTP 생성정보에 기초하여 일회용 패스워드를 생성하여 상기 디스플레이에 표시하는 일회용 패스워드 생성수단을 구비하고;

상기 일회용 패스워드에 의해 상기 계약자의 본인 인증이 행하여지고, 본인 확인이 되었을 경우에 상기 식별정보를 사용한 결제에 의한 네트 상거래가 가능하게 되는 것을 특징으로 하는 네트 결제 보조장치.

청구항 2

신용카드나 직불카드 등의 카드 계약자의 휴대전화나 퍼스널 컴퓨터 등의 계약자 단말과, 상기 계약자의 본인 인증을 행하는 인증 서버가 서로 네트워크 접속된 네트 결제 시스템에 있어서, 상기 계약자의 식별정보를 이용한 결제에 의한 네트 상거래를 행할 때에 사용되는 가반형의 네트 결제 보조장치로서:

상기 네트 결제 보조장치는,

디스플레이와,

상기 계약자의 식별정보를 적어도 포함하는 카드정보가 외부로부터 판독될 수 없는 상태로 미리 저장된 카드정보 저장부와,

상기 계약자의 본인 인증을 행하기 위한 인증정보가 외부로부터 판독될 수 없는 상태로 미리 저장된 인증정보 저장부와,

상기 카드정보에 관련되어 상기 네트 결제 보조장치에 고유의 OTP 생성정보가 외부로부터 판독될 수 없는 상태로 미리 저장된 OTP 생성정보 저장부와,

상기 인증정보를 입력하는 입력수단과,

상기 입력수단으로 입력된 입력정보에 기초하여 상기 네트 결제 보조장치의 조작자가 상기 계약자인지 아닌지의 본인 인증을 행하고, 본인 확인이 되었을 경우에 상기 카드정보 중 적어도 상기 식별정보를 판독하여 상기 디스플레이에 표시하는 인증수단과,

상기 카드정보가 표시된 후에 상기 OTP 생성정보에 기초하여 일회용 패스워드를 생성하여 상기 디스플레이에 표시하는 일회용 패스워드 생성수단을 구비하고;

상기 계약자 단말은 상기 일회용 패스워드를 상기 인증 서버에 송신함으로써 상기 계약자의 본인 인증이 행하여지고, 본인 확인이 되었을 경우에 상기 네트 상거래가 가능하게 되는 것을 특징으로 하는 네트 결제 보조장치.

청구항 3

제 1 항 또는 제 2 항에 있어서, 상기 인증정보는 상기 계약자가 미리 정한 암증번호이며,

상기 입력수단은 숫자키인 것을 특징으로 하는 네트 결제 보조장치.

청구항 4

제 1 항 또는 제 2 항에 있어서, 상기 인증정보는 상기 계약자의 지문·홍채·성대·얼굴 사진 등의 생체적 특징을 수치화한 생체정보인 것을 특징으로 하는 네트 결제 보조장치.

청구항 5

제 1 항 내지 제 4 항 중 어느 한 항에 있어서, 상기 OTP 생성정보는 공통 키이며;

상기 일회용 패스워드 생성수단은,

소정 조작키의 누름을 검출하여 상기 조작키가 눌려진 일시로 이루어지는 일시 데이터를 상기 공통 키에 의해 암호화해서 일회용 패스워드를 생성하는 것을 특징으로 하는 네트 결제 보조장치.

청구항 6

제 1 항 내지 제 4 항 중 어느 한 항에 있어서, 상기 OTP 생성정보는,

공통 키와, 상기 일회용 패스워드가 생성될 때마다 갱신되는 이용횟수 정보에 의해 구성되고;

상기 일회용 패스워드 생성수단은,

소정 조작키의 누름을 검출하여 상기 이용횟수 정보를 공통 키에 의해 암호화해서 일회용 패스워드를 생성하며;

상기 일회용 패스워드가 생성된 후, 상기 OTP 생성정보 저장부 내의 이용횟수 정보를 갱신하는 것을 특징으로 하는 네트 결제 보조장치.

청구항 7

제 1 항 내지 제 6 항 중 어느 한 항에 있어서, 상기 네트 결제 보조장치는 탬퍼링 방지성을 갖는 것을 특징으로 하는 네트 결제 보조장치.

명 세 서

기 술 분 야

<1> 본 발명은 네트 결제 보조장치에 관한 것이다.

배 경 기 술

<2> 종래, 휴대전화기에 신용카드나 은행카드 등의 카드 식별정보(카드번호) 및 암증번호를 저장해 두고, 휴대전화기에 입력된 암증번호와, 저장되어 있는 암증번호가 일치했을 때에 휴대전화기의 디스플레이 상에 카드번호를 표시함으로써 카드로서도 기능하는 휴대전화기가 있다(예를 들면 특허문헌 1 참조).

<3> 그러나, 이러한 카드 기능이 부여된 휴대전화기에는 이하에 설명하는 과제가 있었다.

<4> 특허문헌 1 : 일본 특허공개 2002-64597호 공보

발명의 상세한 설명

<5> 특허문헌 1에 기재된 카드 기능이 부여된 휴대전화기로의 데이터의 저장, 말소 등이 통신에 의해 행하여진다. 즉, 이 휴대전화기는 네트워크에 접속되는 것이 전제가 된다.

<6> 이와 같이, 네트워크에 접속 가능한 휴대전화기에 카드번호나 암증번호를 저장해 두면 부정 액세스 등에 의해 악의의 제3자에 의해 이들 카드번호나 암증번호가 도청, 개찬(改竄)될 위험성이 적지 않게 있어 시큐리티상 문제가 된다.

<7> 그래서, 휴대전화기를 네트워크에 접속 불가능한 구성으로 하면 상술의 도청이나 개찬의 우려는 없어질지도 모른다.

<8> 그러나, 휴대전화기는 기본이 되는 통화기능에 추가로 네트워크 통신기능을 갖는 것이 일반적이 되고 있는 작금, 휴대전화기를 네트워크에 접속 불가능한 구성으로 하는 것은 현실적으로 곤란하다. 또한, 현 상태의 휴대전화기의 구성을 유지한 채, 저장되어 있는 카드번호나 암증번호를 외부로부터 판독할 수 없도록 하기 위해서는 암호화 프로그램 등을 구비할 필요가 있어 구성이 복잡해진다.

<9> 또한, 특허문헌 1의 휴대전화기의 경우, 상술의 네트워크를 통한 부정 액세스에 의하지 않더라도 휴대전화기의 디스플레이에 표시된 카드번호를, 한번, 제3자에게 노출되어 버리면 제3자가 그 카드번호를 이용하여 인터넷 상에서 신용 결제에 의한 네트 상거래를 행하는 것이 가능해져 버려, 이 점에서의 시큐리티도 낮다.

<10> 또한, 본건 특허출원인은, 상기한 바와 같은, 카드번호만으로 네트 상거래를 행할 수 있다고 하는 사정을 감안하여, 카드번호의 제시에 추가로 카드 회원이 미리 정한 고정 패스워드의 제시에 의해 카드 회원의 본인 인증을 거치지 않으면 네트 상거래를 행할 수 없다고 하는 네트 결제 시스템의 운용을 개시하고 있다.

<11> 그러나, 이 고정 패스워드도 한번, 제3자에 알려져버리면, 역시 제3자가 카드 회원인 체해서 네트 상거래를 행하는 것이 가능해져 버려, 반드시 안전한 것이라고는 말할 수 없다.

<12> 본 발명은, 이상과 같은 종래의 문제점을 감안하여 이루어진 것으로서, 그 목적으로 하는 바는 부정 액세스 등에 의해 카드번호나 암증번호를 도청, 개찬당할 위험성이 없고, 또한 보다 안전하게 네트 상거래를 행할 수 있는 네트 결제 보조장치를 제공하는 것에 있다.

<13> 청구항 1의 발명은,

<14> 가반형의 네트 결제 보조장치로서, 디스플레이와, 신용카드나 직불카드(Debit Card) 등의 카드 계약자의 식별정보를 적어도 포함하는 카드정보가 외부로부터 판독될 수 없는 상태로 미리 저장된 카드정보 저장부와, 상기 계약자의 본인 인증을 행하기 위한 인증정보가 외부로부터 판독될 수 없는 상태로 미리 저장된 인증정보 저장부와, 상기 카드정보에 관련되어 상기 네트 결제 보조장치에 고유의 OTP 생성정보가 외부로부터 판독될 수 없는 상태로 미리 저장된 OTP 생성정보 저장부와, 상기 인증정보를 입력하는 입력수단과, 상기 입력수단으로부터 입력된 입력정보에 기초하여 상기 네트 결제 보조장치의 조작자가 상기 계약자인지 아닌지의 본인 인증을 행하고, 본인 확인이 되었을 경우에 상기 카드정보 중 적어도 상기 식별정보를 판독하여 상기 디스플레이에 표시하는 인증수단과, 상기 카드정보가 표시된 후, 상기 OTP 생성정보에 기초하여 일회용 패스워드를 생성하여 상기 디스플레이에 표시하는 일회용 패스워드 생성수단을 구비하고, 상기 일회용 패스워드에 의해 상기 계약자의 본인 인증이 행하여져 본인 확인이 되었을 경우, 상기 식별정보를 사용한 결제에 의한 네트 상거래가 가능하게 되는 것을 특징으로 하는 네트 결제 보조장치이다.

<15> 청구항 2의 발명은,

<16> 신용카드나 직불카드 등의 카드 계약자의 휴대전화나 퍼스널 컴퓨터 등의 계약자 단말과, 상기 계약자의 본인 인증을 행하는 인증 서버가 서로 네트워크 접속된 네트 결제 시스템에 있어서, 상기 계약자의 식별정보를 사용한 결제에 의한 네트 상거래를 행할 때에 사용되는 가반형의 네트 결제 보조장치로서, 상기 네트 결제 보조장치는 디스플레이와, 상기 계약자의 식별정보를 적어도 포함하는 카드정보가 외부로부터 판독될 수 없는 상태로 미리 저장된 카드정보 저장부와, 상기 계약자의 본인 인증을 행하기 위한 인증정보가 외부로부터 판독될 수 없는 상태로 미리 저장된 인증정보 저장부와, 상기 카드정보에 관련되어 상기 네트 결제 보조장치에 고유의 OTP 생성정보가 외부로부터 판독될 수 없는 상태로 미리 저장된 OTP 생성정보 저장부와, 상기 인증정보를 입력하는 입력수단과, 상기 입력수단으로 입력된 입력정보에 기초하여 상기 네트 결제 보조장치의 조작자가 상기 계약자인지 아닌지의 본인 인증을 행하고, 본인 확인이 되었을 경우에 상기 카드정보 중 적어도 상기 식별정보를 판독하여 상기 디스플레이에 표시하는 인증수단과, 상기 카드정보가 표시된 후, 상기 OTP 생성정보에 기초하여 일회용 패스워드를 생성하여 상기 디스플레이에 표시하는 일회용 패스워드 생성수단을 구비하고, 상기 계약자 단말이 상기 일회용 패스워드를 상기 인증 서버에 송신함으로써 상기 계약자의 본인 인증이 행하여지고, 본인 확인이 되었을 경우에 상기 네트 상거래가 가능하게 되는 것을 특징으로 하는 네트 결제 보조장치이다.

<17> 청구항 1 및 청구항 2의 발명에 의하면, 네트 결제 보조장치에 의해 계약자의 본인 인증의 결과, 본인 확인이 되지 않으면 계약자 자신이여도 카드정보를 알 수 없고, 카드정보는 외부로부터 판독될 수 없는 상태로 저장되어 있으므로 카드정보가 노출되어 있는 종래의 신용카드와 달리 카드정보의 비닉성(秘匿性)이 높아져서 네트 상거래에 있어서의 카드정보의 부정 사용이 방지된다.

<18> 또한 네트 결제 보조장치는 가반형이므로, 계약자가 어디에 있어도 휴대전화, 자택의 퍼스널 컴퓨터, 출장지의

퍼스널 컴퓨터를 이용하여 안전한 네트 상거래를 행할 수 있어 네트 상거래의 편리성이 증가한다.

<19> 또한 계약자의 본인 인증에 네트 결제 보조장치에 저장된 계약자 고유의 OTP 생성정보에 의거하여 작성된 일회용 패스워드를 사용하므로, 제3자가 가령 일회용 패스워드를 입수해도 다음 네트 상거래에는 상용할 수 없다.

<20> 일회용 패스워드 생성용의 OTP 생성정보는 외부로부터 판독될 수 없는 상태로 저장되어 있으므로, 계약자 본인이여도 OTP 생성정보를 알 수는 없고, 네트 결제 보조장치를 조작하고 있는 계약자 본인만이 생성 결과의 일회용 패스워드를 알 수 있다. 즉, 제3자에 의한 일회용 패스워드 생성은 불가능하므로 네트 상거래의 안전성이 보다 보증된다.

<21> 또한, 이 일회용 패스워드의 생성은 네트 결제 보조장치에 카드정보가 표시된 후가 아니면 행하여지지 않게 되어 있으므로, 네트 결제 보조장치를 갖고 있지 않은 제3자는 식별정보만을 알고 있어도 일회용 패스워드의 생성을 할 수 없다. 또한 제3자가 네트 결제 보조장치를 훔쳤다고 해도 네트 결제 보조장치에 입력하는 인증정보가 없으면 일회용 패스워드의 생성을 할 수 없다.

<22> 즉, 계약자는 네트 결제 보조장치의 인증수단에 의해 본인 인증을 받은 후, 인증 서버에 의해 본인 인증을 더 받게 되고, 최종적으로 네트 상거래가 가능해 질 때까지 2종류의 다른 인증정보에 기초하는 본인 인증을 거치지 않으면 안되므로 제3자에 의한 행세가 보다 방지되어 네트 상거래의 안전성이 높아진다.

<23> 청구항 3의 발명은,

<24> 상기 인증정보는 상기 계약자가 미리 정한 암증번호이며, 상기 입력수단은 숫자키인 것을 특징으로 하는 네트 결제 보조장치이다.

<25> 청구항 3의 발명에 의하면, 입력수단 및 인증수단을 비교적 저렴하게 구성할 수 있으므로 네트 결제 보조장치의 이용 촉진이 도모된다.

<26> 청구항 4의 발명은,

<27> 상기 인증정보는 상기 계약자의 지문·홍채·성대·얼굴 사진 등의 생체적 특징을 수치화한 생체정보인 것을 특징으로 하는 네트 결제 보조장치이다.

<28> 청구항 4의 발명에 의하면, 고정밀도로 계약자의 본인 인증을 행할 수 있게 되므로, 가령 네트 결제 보조장치를 도둑 맞아도 악용될 우려가 없는 네트 결제 보조장치가 된다.

<29> 청구항 5의 발명은,

<30> 상기 OTP 생성정보는 공통 키이며, 상기 일회용 패스워드 생성수단은 소정 조작키의 누름을 검출하여 상기 조작키가 눌려진 일시로 이루어지는 일시 데이터를 상기 공통 키에 의해 암호화해서 일회용 패스워드를 생성하는 것을 특징으로 하는 네트 결제 보조장치이다.

<31> 청구항 6의 발명은,

<32> 상기 OTP 생성정보는 공통 키와, 상기 일회용 패스워드가 생성될 때마다 갱신되는 이용횟수 정보에 의해 구성되고, 상기 일회용 패스워드 생성수단은 소정 조작키의 누름을 검출하여 상기 이용횟수 정보를 공통 키에 의해 암호화해서 일회용 패스워드를 생성하고, 상기 일회용 패스워드가 생성된 후에 상기 OTP 생성정보 저장부 내의 이용횟수 정보를 갱신하는 네트 결제 보조장치이다.

<33> 여기에서 생성되는 일회용 패스워드는 공통 키를 이용하여 소정 키가 눌려진 일시로 이루어지는 일시 데이터 또는 일회용 패스워드의 생성때마다 갱신되는 이용횟수 정보를 암호화한 것이다. 즉, 네트 결제 보조장치를 조작하고 있는 계약자만이 작성 가능한 패스워드이기 때문에, 네트 결제 보조장치를 소지하고 있지 않은 제3자가 계약자인 체해서 네트 상거래를 행할 수는 없어 네트 상거래의 안전성이 더욱 향상된다.

<34> 청구항 7의 발명은,

<35> 상기 네트 결제 보조장치는 탬퍼링 방지성(Tamper Resistance)을 갖는 것을 특징으로 하는 네트 결제 보조장치이다.

<36> 청구항 7의 발명에 의하면, 네트 결제 보조장치가 탬퍼링 방지성을 구비하므로 제3자에 의한 카드정보, 인증정보, OTP 생성정보의 도청, 개찬에 대한 더나은 시큐리티 향상이 도모된다.

<37> (발명의 효과)

<38> 본 발명의 네트 결제 보조장치에 의하면, 네트 결제 보조장치에 의해 계약자의 본인 인증의 결과 본인 확인이 되지 않으면, 계약자 자신이여도 카드정보를 알 수 없고, 카드정보는 외부로부터 판독될 수 없는 상태로 저장되어 있으므로 카드정보가 노출되어 있는 종래의 신용카드와 달리 카드정보의 비닉성이 높아져서 네트 상거래에 있어서의 카드정보의 부정 사용이 방지된다.

<39> 또한 네트 결제 보조장치는 가반형이므로 계약자가 어디에 있어도 휴대전화, 자택의 퍼스널 컴퓨터, 출장지의 퍼스널 컴퓨터를 이용하여 안전한 네트 상거래를 행할 수 있어 네트 상거래의 편리성이 증가한다.

<40> 또한, 계약자의 본인 인증에 네트 결제 보조장치에 저장된 계약자 고유의 OTP 생성정보에 기초하여 작성된 일회용 패스워드를 사용하므로, 제3자가 가령 일회용 패스워드를 입수해도 다음 네트 상거래에는 사용할 수 없다.

<41> 일회용 패스워드 생성용의 OTP 생성정보는 외부로부터 판독될 수 없는 상태로 저장되어 있으므로, 계약자 본인이여도 OTP 생성정보를 알 수는 없고, 네트 결제 보조장치를 조작하고 있는 계약자 본인만이 생성 결과의 일회용 패스워드를 알 수 있다. 즉, 제3자에 의한 일회용 패스워드 생성은 불가능하므로, 보다 네트 상거래의 안전성이 보증된다.

<42> 또한, 이 일회용 패스워드의 생성은 네트 결제 보조장치에 카드정보가 표시된 후가 아니면 행하여지지 않게 되어 있으므로, 네트 결제 보조장치를 갖고 있지 않은 제3자는 식별정보만을 알고 있어도 일회용 패스워드의 생성을 할 수 없다. 또한 제3자가 네트 결제 보조장치를 훔쳤다고 해도 네트 결제 보조장치에 입력하는 인증정보가 없으면 일회용 패스워드의 생성이 불가능하다.

<43> 즉, 계약자는 네트 결제 보조장치의 인증수단에 의해 본인 인증을 받은 후, 인증 서버에 의해 본인 인증을 더 받게 되고, 최종적으로 네트 상거래가 가능해질 때까지 2종류의 다른 인증정보에 기초한 본인 인증을 거치지 않으면 안되므로, 제3자에 의한 행세가 보다 방지되어 네트 상거래의 안전성이 높아진다.

실 시 예

<62> 이하, 본 발명의 바람직한 실시형태에 대해서 첨부 도면에 기초하여 상세하게 설명한다. 도 1(a)는 네트 결제 보조장치(1)의 외관도이며, 도 1(b)는 네트 결제 보조장치(1)의 전기적 하드웨어의 구성도이다.

<63> 네트 결제 보조장치(1)는 신용카드나 직불카드 등의 카드 계약자의 계약자 단말(휴대전화나 퍼스널 컴퓨터 등)과, 계약자의 본인 인증을 행하는 인증 서버(통상, 카드회사가 보유)가 서로 네트워크 접속된 네트 결제 시스템에 있어서, 계약자가 해당 계약자의 식별정보를 사용한 결제에 의해 네트 쇼핑 등의 네트 상거래를 행할 때에 사용되는 것이며, 도 1(a)에 나타내는 바와 같이, 손바닥에 수용될 정도의 외형을 갖고, 초박형이며 운반이 가능한 하우징(10)으로 구성되고, 하우징(10)의 외표면에 디스플레이(11)와, 키 조작부(12)가 노출되어 있다.

<64> 또한, 본 실시예의 디스플레이(11)는 8자리수의 표시 디스플레이이며, 키 조작부(12)는 0~9까지의 숫자키(12a)와, 스타트 키(12b)로 구성된다.

<65> 하우징(10)의 내부는, 도 1(b)에 나타내는 바와 같이, 디스플레이(11), 키 조작부(12) 외에 카드정보 저장부(13), 인증정보 저장부(15), 인증수단(14), OTP 생성수단(16), OTP 생성정보 저장부(17), 시간측정수단(18)으로서 각각 기능하기 위한 하드웨어(CPU, 메모리)와, 이들 하드웨어 전기부품[디스플레이(11), 키 조작부(12), CPU, 메모리]을 구동하기 위한 구동용 전원(19)(전지)에 의해 구성된다.

<66> 또한, 본 실시예의 하우징(10)에는 디스플레이(11)와 키 조작부(12)와 구동용 전원(19) 외에 SIM 등의 IC카드를 내장하는 슬롯(slot)이 형성되어 있고, 상기 슬롯에 IC카드를 삽입해서 사용한다. 그리고, 상기 CPU와 메모리는 이 IC카드에 포함되는 것을 사용한다. 후술하는 바와 같이, 카드정보 저장부(13), 인증정보 저장부(15), OTP 생성정보 저장부(17)에는 계약자마다 다른 정보가 기억되므로, 이러한 정보를 IC카드의 메모리에 저장하여 슬롯에 삽입해서 사용함으로써 하우징(10) 자체는 계약자에 의하지 않고 공통의 것이면 되고, 또한 하우징(10) 자체에 개인정보를 보유하지 않으므로 하우징(10)의 생산성이 향상됨과 아울러 하우징(10)의 취급, 관리가 용이하게 된다.

<67> 또한, 본 실시예의 구동용 전원(19)은 버튼 전지이지만, 태양 전지나 충전지 등이어도 된다. 또한 네트 결제 보조장치(1)는 통상시는 전원 오프 상태로 해 두고, 예를 들면 키 조작부(12) 중 어느 하나의 키 조작이 있었을 경우에 전원 기동하도록 되어 있어도 된다.

<68> 본 실시예의 카드정보 저장부(13), 인증정보 저장부(15), OTP 생성정보 저장부(17)는, 구체적으로는 후술하는 카드정보, 인증정보, OTP 생성정보를 각각 저장하는 메모리로 구성되어 있고, 메모리는 물리적으로는 이들 정보

를 정리해서 저장하는 1개의 메모리이여도 좋고, 2개 이상의 메모리이여도 좋다.

<69> 본 실시예의 인증수단(14) 및 OTP 생성수단(16)은, 구체적으로는 메모리에 저장된 프로그램에 의해 구성되어 있고, 네트 결제 보조장치(1) 내의 CPU가 그 프로그램을 메모리로부터 판독하여 실행함으로써 이들 인증수단(14) 및 OTP 생성수단(16)의 기능이 실현되게 된다. 또한, CPU, 메모리를 구비하지 않는 네트 결제 보조장치에 있어서는, 인증수단(14), OTP 생성수단(16)의 기능이 전자부품을 이용하여 회로적으로 실현되어도 좋다.

<70> 본 실시예의 네트 결제 보조장치(1)는 신용카드 브랜드와의 라이센스 계약 에 기초하여 신용카드를 발행하는 카드 발행회사(직불카드이면 직불카드를 발행하는 은행 또는 카드 발행회사)로부터 개개의 카드 회원인 계약자에 대하여, 카드 발행회사에 있어서 계약자마다 고유의 카드정보, 인증정보, OTP 생성정보가 메모리에 기록된 상태에서 배포(배포 형태는 대여, 양도 어느 것이나 좋음)되는 것이며, 배포 후는 메모리[카드정보 저장부(13), 인증정보 저장부(15), OTP 생성정보 저장부(17)]의 저장 내용을 외부로부터 판독할 수 없도록 구성되어 있다.

<71> 또한, 네트 결제 보조장치(1)를 배포받은 계약자 자신이여도 메모리의 기록 내용을 외부로부터 판독할 수는 없다. 계약자 자신은 계약자의 본인 인증이 행하여져 본인이라 확인된 경우에 한하여, 카드정보가 디스플레이(11)에 표시됨으로써 해당 카드정보만 알 수 있고, 그 이외의 상태에 있어서는 카드정보는 비닉화되어 있다.

<72> 메모리의 저장 내용을 외부로부터 판독할 수 없도록 되어 있는 것은 네트 결제 보조장치(1)가 인터넷 등의 네트워크에 접속되는 인터페이스를 구비하고 있지 않은 네트 비접속형의 단말이기 때문이다.

<73> 또한, 메모리의 저장 내용의 도청, 개찬에 대한 새로운 시큐리티 향상을 위해 네트 결제 보조장치(1) 또는 네트 결제 보조장치(1)에 내장되는 SIM 등의 IC카드가, 탬퍼링 방지성(분해하여 메모리로부터 직접 기록 내용을 판독하려고 하면 메모리의 기록 내용이 소거되거나, 프로그램이 기동하지 않게 되는 성질)을 구비하고 있어도 된다.

<74> 이하, 네트 결제 보조장치(1)의 각 부의 상세에 대하여 설명한다.

<75> 카드정보 저장부(13)는 계약자의 식별정보를 적어도 포함하는 카드정보가 외부로부터 판독될 수 없는 상태로 미리 저장된 메모리이며, 본 실시예의 카드정보는 계약자 고유의 식별정보(카드번호)와, 유효기한과, 시큐리티 코드(security code; 소정의 방법에 의해 미리 암호화한 3자리수의 10진수. 통상, 플라스틱 타입의 신용카드의 사인 패널에 인자되어 있다. 이 숫자에 의해 카드의 진정성을 확인할 수 있다)로 구성된다. 또한 명의인 이름이 포함되어 있어도 된다. 또한 단지 카드정보가 식별정보만으로 구성되어 있어도 된다. 또한 유효기한, 시큐리티 코드, 명의인 이름의 모두를 카드정보가 포함할 필요는 없고, 적당하게 1개 이상 조합하여 카드정보가 구성되어 있어도 된다.

<76> 인증정보 저장부(15)는 계약자가 정한 암증번호나, 계약자의 지문, 홍채, 성대, 얼굴 사진 등의 생체적 특징을 수치화한 생체정보 등, 계약자의 본인 인증을 행하기 위한 인증정보가 외부로부터 판독될 수 없는 상태로 미리 저장된 메모리이다.

<77> 또한, 인증정보 저장부(15)에 저장되는 인증정보는 네트 결제 시스템에 있어서의 인증 서버가 계약자의 본인 인증에 사용하는 인증정보와는 달리, 네트 결제 보조장치(1)가 계약자의 본인 인증을 행하기 위해서 필요한 인증정보이다. 또한 인증 서버에 있어서의 인증정보와 네트 결제 보조장치(1)에 있어서의 인증정보는 종류가 다른 것이다.

<78> OTP 생성정보 저장부(17)는 네트 결제 보조장치(1)에 고유한 OTP 생성정보가 외부로부터 판독될 수 없는 상태로 미리 저장된 메모리이며, 본 실시예의 OTP 생성정보는 네트 결제 보조장치(1)에 고유의 공통 키이며, 공통 키는 OTP 생성수단(16)에서 생성된 일회용 패스워드의 검증을 행하는 서버(후술의 실시예에 있어서의 인증 서버)에 있어서, 카드정보 저장부(13)에 저장되어 있는 식별정보와 관련지어져 있다.

<79> 또한, 공통 키는 네트 상거래에 있어서 계약자의 본인 인증을 행하는 인증 서버와, 네트 결제 보조장치(1)에만 저장된 키이며, 본 실시예에서는 후술의 OTP 생성수단(16)이 일회용 패스워드를 생성하는데에 사용된다.

<80> 인증수단(14)은 네트 결제 보조장치(1)의 조작자가 카드정보 저장부(13)에 저장되어 있는 식별정보를 이용 가능한 계약자(카드 회원)인지의 여부의 본인 인증을 행하는 수단이며, 입력수단[본 실시예에서는 숫자키(12a)]으로부터 입력된 입력정보와, 인증정보 저장부(15)에 저장되어 있는 인증정보가 일치하는지 확인하고, 일치했을 경우에 네트 결제 보조장치(1)의 조작자가 해당 계약자 본인인 것으로 해서 카드정보 저장부(13)에 저장되어 있는 카드정보 중, 적어도 식별정보를 판독하여 디스플레이(11)에 표시하는 수단이다.

<81> 본 실시예의 인증수단(14)은 조작자가 키 조작부(12)의 스타트 키(12b)를 누름으로써 스타트 키(12b)의 누름 검

출을 받아서 기동한다. 또한 그 후에 조작자가 입력수단에 상당하는 숫자키(12a)를 눌러서 4자리수의 숫자를 입력하면, 인증수단(14)은 입력된 숫자가 인증정보 저장부(15)에 저장되어 있는 암증번호와 일치하는지의 여부를 확인하고, 일치했을 경우에 디스플레이(11)에 카드정보를 표시한다.

<82> 인증정보가 본 실시예와 같이 암증번호이면 입력수단으로서 숫자키가 있으면 되고, 입력정보와 인증정보의 일치 판정 처리도 용이하게 행하여지므로 비교적 저렴한 구성으로 네트 결제 장치(1)가 실현되어, 네트 결제 장치(1)의 이용 촉진이 도모된다.

<83> 본 실시예의 인증정보는 4자리수의 암증번호로 되지만, 인증 방법 및 인증정보는 이에 한정되지 않고, 복수의 인증 방법에 의한 인증수단이 적당하게 조합되어도 좋고, 복수의 인증수단을 채용하면 그만큼 인증 정밀도가 높아져서 제3자에 의한 네트 결제 보조장치의 악용이 방지된다.

<84> 예를 들면, 인증수단(14)이 생체인식(Biometrics) 인증 방법을 채용하고 있으면 인증정보는 생체인식 정보(지문, 홍채, 성대, 얼굴 사진 등의 생체적 특징을 수치화한 데이터)로 되고, 또한 입력수단은 이들 생체인식 정보를 입력하는 스캐너, 마이크, 디지털 카메라 등이 된다.

<85> 생체인식 인증 방법은 고정밀도의 인증 방법이기 때문에, 가령 네트 결제 보조장치(1)를 제3자에게 도둑맞아도, 네트 결제 보조장치(1)가 배포된 계약자가 아니면 네트 결제 보조장치(1)를 사용할 수 없어 악용이 방지된다.

<86> 또한, 본 실시예의 인증정보인 암증번호에는 숫자 외에, 알파벳이 포함되어 있어도 좋고, 그 경우는 숫자키 이외에 알파벳 키를 네트 결제 보조장치가 구비할 필요가 있다.

<87> OTP 생성수단(16)은 인증수단(14)에 의해 카드정보가 표시된 후, OTP 생성정보 저장부(17)에 저장된 OTP 생성정보(본 실시예에서는, 공통 키)에 기초하여 일회용 패스워드를 생성하여 디스플레이(11)에 표시하는 수단이다.

<88> 이 일회용 패스워드는 계약자 단말로부터 인증 서버에 송신되어, 인증 서버가 계약자의 본인 인증을 행할 때에 인증 서버에서 OTP 생성정보에 기초하여 생성된 일회용 패스워드와의 대조에 사용된다. 그리고, 이들 일회용 패스워드의 대조 결과가 일치하고, 인증 서버에 의해 본인 확인이 이루어졌을 경우, 해당 계약자의 식별정보를 사용한 결제에 의한 네트 상거래가 가능해진다.

<89> 본 실시예에서는, 인증수단(14)에 의한 인증이 행하여지고 카드정보가 디스플레이(11)에 표시된 후에 조작자가 스타트 키(12b)를 누르면, 스타트 키(12b)를 누른 것이 OTP 생성수단(16)을 기동시키는 계기가 되어 일회용 패스워드가 생성·표시된다.

<90> 또한, 본 실시예의 OTP 생성수단(16)은, 상세한 것은 후술하는 시간 동기방식에 의해 일회용 패스워드를 생성하는 것으로 하지만, 그 밖의 생성 방식, 예를 들면 카운터 동기방식이나, 시도 응답(challenge and response) 방식에 의해 일회용 패스워드가 생성되어도 좋다.

<91> 시간측정수단(18)은 본 실시예의 OTP 생성수단(16)이 시간 동기방식에 의해 일회용 패스워드를 생성하기 위해서 필요로 하는 수단이며, 시간을 측정하는 수단이다. 또한, 시간측정수단(18)은 리얼 타임 클록(real time clock)으로 구성되어 있어도 좋고, 또한 시간측정 프로그램이 메모리에 저장되어, 그 시간측정 프로그램을 CPU가 판독하고 실행하여 시간측정 기능을 실현하게 되어 있어도 된다. 또한 OTP 생성수단(16)이 시간 동기방식 이외의 방식으로 일회용 패스워드를 생성할 경우에는 시간측정수단(18)은 불필요하고, 대신에 각 생성 방식에 필요한 수단이 부가되게 된다.

<92> 본 실시예에서는, OTP 생성수단(16)은 상술한 바와 같이, 인증수단(14)이 디스플레이(11)에 카드정보를 표시한 것을 받아서 스타트 키(12b)의 누름 검출 대기상태로 된다. OTP 생성수단(16)은 스타트 키(12b)의 누름이 검출되면 누름 검출을 시간측정수단(18)에 전달한다. 시간측정수단(18)은 스타트 키(12b)가 누름 검출된 일시를 시간측정하고, 일시 데이터(연 월 일 시 분 초. 초는 30초 단위)를 OTP 생성수단(16)에 넘겨준다.

<93> 그리고, OTP 생성수단(16)은 OTP 생성정보 저장부(17)로부터 공통 키를 판독하고, 넘겨진 일시 데이터를 판독한 공통 키로 암호화하고, 이것을 10진수로 변환하여 디스플레이(11)에 표시한다. 또한, 본 실시예의 암호화 방식은 공통 키 암호방식을 채용하고 있지만, 그 밖의 암호화 방식이어도 좋다.

<94> 이상 설명한 네트 결제 보조장치(1)에 의하면, 네트 결제 보조장치(1)에 의해 계약자의 본인 인증이 행하여져 본인이라 확인되었을 경우에, 인증수단(14)이 표시한 카드정보는 카드 결제가 가능한 가맹점의 웹 사이트 또는 인증 서버로부터 송신되어 계약자 단말에 표시되는 카드정보 입력화면에 입력된 후, 웹 사이트 또는 인증 서버에 송신 가능하게 된다.

<95> 이와 같이, 네트 결제 보조장치(1)에 의해 계약자의 본인 인증이 행하여져 본인이라 확인되지 않으면, 즉, 입력된 입력정보가 네트 결제 보조장치에 저장되어 있는 인증정보와 일치하지 않으면 계약자 자신이여도 카드정보를 알 수 없고, 카드정보는 외부로부터 판독될 수 없는 상태로 저장되어 있으므로 카드정보가 노출되어 있는 종래의 신용카드와 달리, 카드정보의 비닉성이 높아져서 네트 상거래에 있어서의 카드정보의 부정 사용이 방지된다.

<96> 또한 네트 결제 보조장치는 가반형이므로 계약자가 어디에 있어도 휴대전화, 자택의 퍼스널 컴퓨터, 출장지의 퍼스널 컴퓨터를 이용하여 안전한 네트 상거래를 행할 수 있어 네트 상거래의 편리성이 증가한다.

<97> 또한 OTP 생성수단(16)이 표시한 일회용 패스워드는 계약자의 본인 인증을 행하는 인증 서버로부터 송신되어 계약자 단말에 표시되는 일회용 패스워드 입력 화면에 입력된 후 인증 서버에 송신 가능하게 됨과 아울러, 인증 서버가 생성한 일회용 패스워드와의 대조에 의해 일치했을 경우에 본인 확인이 되어 계약자의 식별정보를 사용한 결제에 의한 네트 상거래가 가능하게 된다.

<98> 이와 같이, 계약자의 본인 인증에 네트 결제 보조장치에 저장된 계약자 고유의 OTP 생성정보에 의거하여 작성된 일회용 패스워드를 사용하므로, 제3자가 가령 일회용 패스워드를 입수해도 다음 네트 상거래에는 상용할 수 없다.

<99> 일회용 패스워드 생성용의 OTP 생성정보는 외부로부터 판독될 수 없는 상태로 저장되어 있으므로 계약자 본인이여도 OTP 생성정보를 알 수는 없고, 네트 결제 보조장치를 조작하고 있는 계약자 본인만이 생성 결과의 일회용 패스워드를 알 수 있다. 즉, 제3자에 의한 일회용 패스워드 생성은 불가능하므로, 보다 네트 상거래의 안전성이 보증된다.

<100> 또한, 이 일회용 패스워드의 생성은 네트 결제 보조장치에 카드정보가 표시된 후가 아니면 행하여지지 않게 되어 있으므로, 네트 결제 보조장치를 갖고 있지 않은 제3자는 식별정보만을 알고 있어도 일회용 패스워드의 생성을 할 수 없다. 또한 제3자가 네트 결제 보조장치를 훔쳤다고 해도 네트 결제 보조장치에 입력하는 인증정보가 없으면 일회용 패스워드의 생성을 할 수 없다.

<101> 즉, 계약자는 네트 결제 보조장치의 인증수단에 의해 본인 인증을 받은 후, 인증 서버에 의해 본인 인증을 더 받게 되고, 최종적으로 네트 상거래가 가능해 질 때까지 2종류의 다른 인증정보에 기초한 본인 인증을 거치지 않으면 안되므로, 제3자에 의한 행세가 보다 방지되어 네트 상거래의 안전성이 높아진다.

<102> 또한, 인증정보 저장부(15)는 상술한 인증정보의 외에 인증수단(14)이 행하는 일치 판정 처리에서, 입력정보와 인증정보가 일치하지 않았을 경우에 입력정보의 재입력을 접수하는 횟수(에러 허용 횟수)를 미리 저장하여도 좋다. 그 경우, 네트 결제 보조장치(1) 또는 인증수단(14)은 계수수단(카운터)도 구비하는 구성으로 된다.

<103> 그리고, 인증수단(14)이 일치 판정 처리를 행하는 플로우에 있어서, 입력정보와 인증정보가 일치하지 않았을 경우, 그 때마다 계수수단이 1부터 카운트 업을 행하고, 카운트 업된 숫자와 에러 허용 횟수를 비교하여 카운트 업된 숫자가 에러 허용 횟수를 상회했을 경우에는, 이후, 인증수단(14)은 자신의 처리가 행하여지지 않도록 하고, 또한 OTP 생성수단(16)이 기동하지 않도록 하여, 인증 플로우 및 OTP 생성 플로우가 행하여지지 않도록 한다.

<104> 이에 따라, 악의의 제3자가 네트 결제 보조장치(1)를 도용하여 인증정보를 닥치는 대로에 입력한 결과, 카드정보나 일회용 패스워드가 디스플레이(11)에 표시되어버리는 것을 방지할 수 있다.

<105> 또한, 카운트 업된 숫자가 에러 허용 횟수를 상회하지 않고 입력정보와 인증정보가 일치했을 경우에는, 인증수단(14)은 디스플레이(11)에 카드정보의 표시를 행하게 하지만, 이 때에, 카운트 업된 숫자는 0으로 리셋(초기화)되는 것으로 한다.

<106> 여기에서, 네트 결제 보조장치(1)를 조작 순서 및 디스플레이(11)의 화면 천이의 일례를 도 5에 나타낸다. 또한, 본 실시예의 디스플레이(11)는 8자리수의 영숫자·기호 표시용 디스플레이이다.

<107> 우선, 조작자에 의해 스타트 키(12b)가 눌려지면 네트 결제 보조장치(1)의 전원이 기동하고(S200), 디스플레이(11)에 「APPLI」로 표시되므로(S210), 또한 스타트 키(12b)가 눌린 후(S225) 카드정보를 표시시키고 싶은 경우에는 조작자는 숫자키(12a)의 「1」을 누르고(S230), 인증정보(암증번호)의 변경을 행하고 싶은 경우에는 숫자키(12a)의 「2」를 누른다(S330).

<108> 「1」이 눌린 경우(S230), 디스플레이(11)에 「PIN」이라고 표시되므로, 조작자는 인증정보로서 4자리수의 암증번호를 숫자키(12a) 중에서 선택해서 누른다(S240). 그 후에 스타트 키(12b)가 눌리고(S245), 눌린 암증번호가

인증정보 저장부(15)에 저장되어 있는 인증정보와 일치하면 카드정보 저장부(13)에 저장되어 있는 카드정보 중, 우선, 식별정보(이하, 카드번호라고 함)의 위 8자리수가 디스플레이(11)에 표시된다(S250).

<109> 계속해서, 스타트 키(12b)가 눌리면(S255) 카드번호 아래 8자리수가 디스플레이(11)에 표시된다(S260).

<110> 계속해서, 스타트 키(12b)가 눌리면(S265) 유효기한과 시큐리티 코드가 디스플레이(11)에 표시된다(S270). 또한, S265와 S270의 플로우는 필수가 아니라 카드정보 중 카드번호만이 표시되는 것이어도 된다.

<111> 계속해서, 스타트 키(12b)가 눌리면(S275) 디스플레이(11)에 「OTP=1」이라고 표시되고, 일회용 패스워드를 생성·표시할 것인지, 종료할 것인지의 여부의 선택이 이루어진다. 여기에서, 스타트 키(12b)가 눌린 후(S290) 숫자키(12a)의 「1」이 눌려지면(S295), 디스플레이(11)에 인증정보의 입력을 촉구하는 「PIN」이 표시되므로(S305), 조작자는 다시 4자리수의 암증번호를 숫자키(12a)로부터 누르고 스타트 키(12b)를 누른다(S310).

<112> 눌려진 암증번호가 인증정보 저장부(15)에 저장되어 있는 인증정보와 일치하면, OTP 생성정보 저장부(17)에 저장되어 있는 OTP 생성정보에 기초하여 일회용 패스워드가 생성되고, 이것이 디스플레이(11)에 표시된다(S315).

<113> 다시, 스타트 키(12b)가 눌리면(S320) 네트 결제 보조장치(1)의 전원이 차단된다.

<114> 숫자키(12a)의 「1」 이외의 키가 눌리거나, 어떠한 키도 눌리지 않고 미리 결정된 소정 시간이 경과했을 경우에는(S300), 자동적으로 네트 결제 보조장치(1)의 전원이 차단된다.

<115> 또한, S240과 S305에서 입력되는 암증번호는 카드정보 표시용과 일회용 패스워드 생성용으로, 각각의 암증번호이어도 좋고, 그 경우에는 인증정보 저장부(15)에 각각의 암증번호가 구별해서 저장되어 있다.

<116> 또한 본 실시예에서는 일회용 패스워드를 디스플레이(11)에 표시하는 플로우(S315) 전에, S305에서 조작자에게 다시 인증정보의 입력을 촉구했지만, S305 를 생략하고, S310의 스타트 키(12b)의 누름만으로 일회용 패스워드가 생성되어도 좋다.

<117> S225의 뒤, 숫자키(12a)의 「2」가 눌려진 경우에는(S330), 디스플레이(11)에 「CHANGE?」이라고 표시된다(S335).

<118> 스타트 키(12b)가 눌려지면(S340) 디스플레이(11)에 「PIN」이라고 표시되어 암증번호의 입력이 재촉되므로, 조작자는 숫자키(12a)로부터 4자리수의 암증번호를 누른 후(S345), 또한 스타트 키(12b)를 누르고(S350), 눌러진 암증번호가 인증정보 저장부(15)에 저장되어 있는 인증정보와 일치하면 변경 후의 암증번호의 입력을 재촉하는 「NEW1」이 디스플레이(11)에 표시되므로, 조작자는 변경 후의 암증번호를 숫자키(12a)로부터 누르고(S355), 또한 스타트 키(12b)를 누른다(S360).

<119> 다음에, 디스플레이(11)에는 다시 변경 후의 암증번호의 입력을 재촉하는 「NEW2」가 디스플레이(11)에 표시되므로, 조작자는 변경 후의 암증번호를 다시 숫자키(12a)로부터 누르고(S365), 또한 스타트 키(12b)를 누른다(S370).

<120> S355에서 눌려진 암증번호와 S365에서 눌려진 암증번호가 일치하고 있으면, 디스플레이(11)에 암증번호의 변경이 완료된 취지를 나타내는 「COMPLETE」가 표시되므로(S375), 그 확인을 거친 후에 스타트 키(12b)가 눌려지면(S380) 암증번호의 변경 수속이 완료되고, 전원이 차단된다.

<121> 또한, 시큐리티 향상을 위해서 S355와 S365에서 숫자키(12a)로부터 입력이 이루어져도, 입력된 값은 디스플레이(11) 상에 표시되지 않는 것이 바람직하다.

<122> 실시예 1

<123> 이하, 도 1에 나타낸 네트 결제 보조장치(1)를 배포된 신용카드 계약자인 신용카드 회원(이하, 카드 회원이라고 한다)이, 해당 네트 결제 보조장치(1)를 이용하여 통신기능을 갖는 퍼스널 컴퓨터이나 휴대전화로부터, 해당 카드 회원의 카드번호를 사용한 결제에 의해 네트 쇼핑 등의 네트워크 상거래(이하, 네트 상거래라고 한다)를 행할 경우의 하나의 실시예에 대하여 설명한다.

<124> 본 실시예의 네트 결제 시스템의 시스템 구성과 네트워크 접속 관계를 도 2의 시스템 구성도에 나타낸다. 또한 본 실시예의 네트 결제 시스템에 있어서의 네트 상거래의 플로우를, 도 3의 플로우챠트에 나타낸다.

<125> 또한, 본 실시예에서 네트 결제 시스템에 있어서의 네트 상거래 서비스를 제공하는 것은 신용카드 브랜드이다.

<126> 카드 회원은, 미리 카드 발행회사에 대하여 신용카드의 신청을 행하여 신용카드의 발행을 받음과 아울러, 카드

발행회사로부터 개개의 카드 회원에 고유의 인증정보(카드 회원이 신용카드 신청시에 등록한 암증번호나 지문정보 등의 생체정보), 카드정보(개개의 카드 회원에 고유의 카드번호, 유효기한), OTP 생성정보(공통 키)가 저장된 네트 결제 보조장치(1)의 배포를 받고 있는 것으로 한다.

<127> 또한 본 실시예에서는, 도 1(b)에 나타낸 네트 결제 보조장치(1)의 구성 중, 디스플레이(11)와 키 조작부(12)와 구동용 전원(19)을 제외하는 구성은 SIM 등의 IC카드에 미리 저장되어 있고, 하우징(10)에 형성된 IC카드 슬롯(도시 생략)에 해당 IC카드가 삽입됨으로써 네트 결제 보조장치(1)의 기능이 실현되지만, 반드시 네트 결제 보조장치가 IC카드를 구비하고 있지 않아도 되고, IC카드를 구비하고 있지 않은 경우에는 네트 결제 보조장치 자신이 CPU나 메모리를 구비하고 있으면 된다.

<128> 또한, 본 실시예의 네트 결제 보조장치(1)는 카드 회원의 식별정보를 이용한 결제, 즉, 카드 결제를 이용한 네트 상거래에 사용되는 것으로 하지만, 카드 회원이 네트 상거래만을 희망하고, 종래의 플라스틱 타입의 자기카드, IC카드 등으로 이루어지는 신용카드에 의한 리얼(real)의 대면 거래를 희망하지 않을 경우에는 신용카드의 발행은 받지 않아도 좋다.

<129> 또한 신용카드 브랜드가 카드 발행회사의 업무도 행하고 있는 경우에는 신용카드 브랜드로부터 네트 결제 보조장치(1)가 배포되어도 좋다.

<130> 회원 단말(2)은 계약자의 단말이며, 카드 회원이 네트 결제 보조장치(1)를 이용하여 네트 상거래를 행하기 위한 단말이며, 통신 기능과 브라우저 표시 기능을 적어도 갖는 퍼스널 컴퓨터, 휴대전화 등의 단말이다.

<131> 가맹점 단말(3)은 회원 단말(2)에 가상 점포(웹 사이트)를 제공하고, 상품이나 서비스의 주문을 접수함과 아울러 주문한 카드 회원의 본인 인증을 카드 발행회사측에 의뢰하고, 카드 회원의 본인 인증이 행하여진 후, 가맹점 관리회사[신용카드 브랜드와의 라이센스 계약에 기초하여 가맹점의 획득·계약·관리 업무를 행함]에 대하여 오소리제이션(authorization)[주문된 상품이나 서비스의 금액분의 크레디트라인(credit line)이 카드 회원에 남아있는지의 여부를 조사하고, 크레디트라인이 남아있을 경우에 그 금액분을 결제용으로 확보하는 것]을 의뢰하는 단말이다.

<132> 가맹점 관리회사 단말(4)은 가맹점 단말(3)로부터 받은 오소리제이션 의뢰를 카드 발행회사측에 재의뢰(오소리제이션 재발송)하는 단말이다.

<133> 중개 서버(5)는 가맹점 단말(3)과 후술의 인증 서버(7)의 중개역할을 담당하는, 즉 회원 단말(2)과 가맹점 단말(3) 사이에서 카드 회원의 인증 서비스를 중개하는 역할을 담당하는 서버이다.

<134> 중개 서버(5)는, 본 실시예에서는 신용카드 브랜드가 운영하는 서버이며, 네트 결제 보조장치(1)를 사용한 네트 상거래 서비스에 대응하고 있는 가맹점을 식별하는 가맹점 식별정보와, 네트 결제 보조장치(1)를 사용한 네트 상거래 서비스에 대응하고 있는 카드 발행회사를 식별하는 카드 발행회사 식별정보를 저장하고 있다.

<135> 또한, 본 실시예의 네트 결제 시스템에 있어서 네트 결제 보조장치(1)를 사용하지 않는 네트 상거래 서비스가 혼재할 경우에는, 중개 서버(5)는 네트 결제 보조장치(1)를 사용한 네트 상거래 서비스에 미대응의 가맹점 및 카드 발행회사의 식별정보를, 상기 가맹점 식별정보 및 카드 발행회사 식별정보와 구별해서 자장해 둘 필요가 있다.

<136> 카드 발행회사 단말(6)은 가맹점 관리회사 단말(4)로부터 받은 오소리제이션 의뢰를 접수하여 오소리제이션을 행하는 단말이다.

<137> 인증 서버(7)는 네트 상거래를 행할 때에 오소리제이션에 앞서, 카드 회원의 본인 인증을 행하는 서버이다. 본 실시예에서는 인증 서버(7)는 카드 발행회사가 운영하는 서버이며, 카드 발행회사 단말(6)에 접속되어 있고, 네트 결제 보조장치(1)를 이용하여 네트 상거래를 행하는 것이 가능한 카드 회원의 카드정보(카드번호, 유효기한) 및 OTP 생성정보[네트 결제 보조장치(1)에 고유한 공통 키]를, 서로 관련지은 상태에서 저장하고 있다. 즉, 1 카드 회원에 대해 카드정보와 OTP 생성정보가 관련지어져 인증 서버(7)에 저장되어 있다.

<138> 또한, 인증 서버(7)로의 이들 정보의 저장은, 카드 회원에 네트 결제 보조장치(1)를 배포하는 것과 같은 시기, 또는 그 전후에 행하여진다.

<139> 도 2에 있어서, 회원 단말(2), 가맹점 단말(3), 중개 서버(5), 인증 서버(7)간은 각각 인터넷 등의 네트워크(9a)에 의해 접속되어 있고, 가맹점 단말(3), 가맹점 관리회사 단말(4), 카드 발행회사 단말(6)은 각각 전용 회선(9b)에 의해 접속되어 있다.

<140> 또한, 카드 발행회사 단말(6) 및 인증 서버(7)는 카드 발행회사마다 개별적으로 준비되어, 각각이 회원 단말(2), 가맹점 관리회사 단말(4), 중개 서버(5)에 네트워크(9a), 전용 회선(9b)에 의해 접속되게 된다.

<141> 또한 가맹점 단말(3)도 가맹점마다 개별적으로 준비되어, 각각이 회원 단말(2), 중개 서버(5), 가맹점 관리회사 단말(4)에 네트워크(9a), 전용 회선(9b)에 의해 접속되게 된다.

<142> 이하, 도 3의 플로우챠트 및 도 2의 시스템 구성도에 기초하여 네트 결제 보조장치(1)를 사용한 네트 상거래의 흐름을 설명한다. 카드 회원은 회원 단말(2)로부터 네트워크(9a)를 통해서 가상 점포(Web 사이트)인 가맹점 단말(3)에 액세스하고, 상품이나 서비스를 열람한다. 그리고, 주문하는 상품이나 희망의 서비스가 결정되면, 회원 단말(2)은 가맹점 단말(3)에 주문 상품이나 희망 서비스에 관해서 카드 결제에 의한 네트 상거래를 희망하는 취지를 송신한다.

<143> 가맹점 단말(3)은 회원 단말(2)에, 도 4(a)에 나타내는 바와 같은 카드정보 입력화면(100)을 표시시키고, 회원 단말(2)에 카드번호 및 카드의 유효기한을 입력하여 송신하도록 의뢰한다.

<144> 그래서, 카드 회원이 네트 결제 보조장치(1)의 스타트 키(12b)를 누르면, 네트 결제 보조장치(1)의 인증수단(14)이 기동하여 네트 결제 보조장치(1)가 인증 대기 상태로 된다. 계속해서, 카드 회원은 본인 인증을 위해 필요한 입력정보(본 실시예에서는 4자리수의 암증번호)를 숫자키(12a)로부터 입력한다. 또한, 여기에서 입력되는 4자리수의 암증번호는, 미리 카드 회원이 카드 신청시에 정해 두고, 이미 네트 결제 보조장치(1) 내의 인증정보 저장부(15)에 저장되어 있는 것이다.

<145> 인증수단(14)은 인증정보 저장부(15)에 저장되어 있는 인증정보를 판독하여 숫자키(12a)로부터 입력된 입력정보와 일치하는지의 여부를 확인한다. 그리고, 양자가 일치했을 경우에 인증수단(14)은 카드정보 저장부(13)로부터 카드정보로서의 카드번호와 유효기한을 판독하여 디스플레이(11)에 표시한다.

<146> 그리고, 카드번호와 유효기한을 모두 디스플레이(11)에 표시 완료하면, 인증수단(14)은 표시가 끝난 취지를 OTP 생성수단(16)에 전달한다. 이것에 의해, OTP 생성수단(16)은 후술하는 일회용 패스워드 생성 대기 상태로 된다.

<147> 또한, 본 실시예에서는 디스플레이(11)의 표시 가능 자리수가 8자리수에 한정되어 있기 때문에, 인증수단(14)은 카드정보 저장부(13)로부터 판독한 카드번호를 위 8자리수와 아래 8자리수로 분할 처리한 후에, 디스플레이(11)에 우선 카드번호 위 8자리수를 표시한다. 카드 회원은 그 표시에 기초하여 카드정보 입력화면(100)의 카드번호 입력란(100a)에 카드번호 위 8자리수를 입력한다.

<148> 카드번호 위 8자리수의 입력이 끝나면 카드 회원은 스타트 키(12b)를 누른다. 인증수단(14)은 스타트 키(12b)의 누름 검출을 받고, 카드번호 아래 8자리수를 디스플레이(11)에 표시한다. 카드 회원은 그 표시에 기초하여 카드정보 입력화면(100)의 카드번호 입력란(100a)에 카드번호 아래 8자리수를 입력한다.

<149> 카드번호 아래 8자리수의 입력이 끝나면 카드 회원은 스타트 키(12b)를 누른다. 인증수단(14)은 스타트 키(12b)의 누름 검출을 받고, 유효기한을 4자리수[MM(월)/YY(년)]로 표시한다. 카드 회원은 그 표시에 기초하여 카드정보 입력화면(100)의 유효기한 입력란(100b)에 유효기한을 입력한다.

<150> 또한, 디스플레이의 표시 영역, 표시 가능 자리수에 여유가 있을 경우에는 당연히 카드번호가 한번에 모두 디스플레이에 표시되어도 좋고, 또한 카드번호와 유효기한이 한번에 모두 표시되어도 좋다. 또한 반대로, 디스플레이의 표시 가능 자리수가 8자리수보다 적은 경우에는 인증수단(14)은 표시 가능 자리수에 맞추어 카드정보 저장부(13)로부터 판독한 카드정보를 미리 분할해 두고, 스타트 키(12b) 기타, 임의의 키의 누름 검출에 의해 순차 분할된 카드정보를 표시해도 좋다.

<151> 이상과 같이, 네트 결제 보조장치(1)는 입력된 입력정보가 인증정보 저장부(15)에 저장되어 있는 인증정보와 일치했을 경우에만 디스플레이(11) 상에 카드정보를 표시하므로, 인증정보를 모르면 제3자가 네트 결제 보조장치(1)를 훔쳤다고 해도 내부의 카드정보를 알 수 없다. 따라서, 카드정보가 인자되어 있는 종래의 신용카드에 비해서 안전성이 높고, 카드정보가 네트 상거래에 악용될 우려가 없다.

<152> 카드 회원이 카드번호 및 유효기한의 입력을 끝내면[또한, 도 4의 카드정보 입력화면(100)에는 나타내어져 있지 않지만, 주문한 상품·서비스명, 금액, 주문일, 가맹점명, 상품의 발송처 등의 정보가 동일 화면 내에 표시되어 있어도 됨], 카드정보 입력화면(100) 내의 송신 버튼(100c)을 클릭한다. 송신 버튼(100c)이 클릭됨으로써 가맹점 단말(3)측에 입력된 카드정보가 송신된다(S10).

<153> 회원 단말(2)에서 주문한 상품·서비스명, 금액, 주문일, 가맹점명, 상품의 발송처 등에 관한 주문정보와, 주문

상품의 결제에 사용하는 카드의 카드번호나 유효기한 등의 카드정보를 수신한 가맹점 단말(3)은, 수신한 카드정보에 추가로 가맹점마다 부여된 가맹점 식별정보를 네트워크(9a)를 통해서 접속된 중개 서버(5)에 송신하고, 카드 회원이 네트 결제 보조장치(1)를 사용한 네트 상거래 서비스를 받을 수 있는 회원인지의 여부의 확인(인증 실행 여부 확인)을 요구한다(S20).

<154> 중개 서버(5)는 수신한 가맹점 식별정보가 보유하고 있는 가맹점 식별정보와 일치하는지의 여부의 확인(가맹점 인증)을 행한다. 이들 정보가 일치하면 네트 결제 보조장치(1)를 사용한 네트 상거래 서비스에 참가하고 있는 가맹점의 가맹점 단말(3)로부터 중개 서버(5)에 액세스가 있었다고 하게 된다. 일치하지 않으면 네트 결제 보조장치(1)를 사용한 네트 상거래 서비스에 참가하고 있지 않은 가맹점 단말(3)로부터의 액세스이거나, 부정 액세스이기 때문에 이후의 플로우로는 진행되지 않는다.

<155> 중개 서버(5)는 네트 결제 보조장치(1)를 사용한 네트 상거래 서비스에 참가하고 있는 가맹점 단말(3)로부터 수신한 카드 회원의 카드정보에 기초하여 상기 카드 회원의 카드번호가 발행된 카드 발행회사를 특정하고, 특정된 카드 발행회사의 인증 서버(7)에 카드정보를 송신하고, 카드 회원이 네트 결제 보조장치(1)를 사용한 네트 상거래 서비스를 받을 수 있는 회원인지의 여부의 확인(인증 실행 여부 확인)을 요구한다(S30).

<156> 본 실시예의 중개 서버(5)에는 카드 발행회사를 식별하는 카드 발행회사 식별정보가 저장되어 있고, 중개 서버(5)는 수신한 카드정보에 의거하여 카드 발행회사 식별정보를 검색하고, 카드 발행회사를 특정한다.

<157> 즉, 본 실시예의 중개 서버(5)는 직접, 인증 실행 여부 확인을 행하는 것은 아니고, 가맹점 인증을 행함과 아울러 가맹점 단말(3)로부터 수신한 카드정보에 기초하여 카드 회원의 카드번호가 발행된 카드 발행회사를 특정하고, 특정된 카드 발행회사의 인증 서버(7)에 카드정보를 전송하고, 해당 인증 서버(7)로부터 수신한 인증 실행 여부 확인 결과를 가맹점 단말(3)에 전송하는 역할을 담당하고 있다.

<158> 또한, 본 실시예에서는, 중개 서버(5)는 신용카드 브랜드가 운영하고 있는 서버이지만, 이것을 개개의 가맹점 단말(3)이 구비하고 있어도 되고, 그 경우에는 직접, 가맹점 단말(3)로부터 인증 서버(7)에 인증 실행 여부 확인이 요구되게 된다. 또한 인증 서버(7)에 있어서 가맹점 인증이 행하여져도 좋다.

<159> 인증 서버(7)는 중개 서버(5)로부터 수신한 카드정보가 인증 서버(7)에 등록되어 있는지의 여부를 확인함으로써 해당 카드정보를 갖는 카드 회원이 네트 결제 보조장치(1)를 사용한 네트 상거래 서비스를 받을 수 있는 카드 회원인지의 여부의 확인(인증 실행 여부 확인)을 행하고, 그 결과를 중개 서버(5)에 회신한다(S40). 또한, 인증 실행 여부 확인 결과는 중개 서버(5)로부터 수신한 카드정보가 인증 서버(7)에 등록되어 있으면 「가능」이며, 등록되지 않고 있으면 「불가능」이다.

<160> 그리고, 인증 실행 여부 확인 결과를 수신한 중개 서버(5)는 그 결과를 가맹점 단말(3)에 전송한다(S50).

<161> 카드 회원의 인증 실행 여부 확인 결과가 「가능」일 경우에는 이 카드 회원이 네트 결제 보조장치(1)를 사용한 네트 상거래 서비스를 받을 수 있다고 하는 것이기 때문에, 가맹점 단말(3)은 이 카드 회원의 본인 인증 요구를 행하는 플로우로 진행한다(S60). 구체적으로는, 가맹점 단말(3)은 회원 단말(2)에 대하여 인증 실행 여부 결과와 함께, 먼저 인증 실행 여부 확인을 행한 카드 발행회사의 인증 서버(7)의 URL 정보를 송신한다.

<162> 가맹점 단말(3)로부터 인증 요구를 받은 회원 단말(2)은 수신한 URL에 기초하여, 먼저 중개 서버(5)가 액세스한 것과 동일한 인증 서버(7)에 액세스하여 인증 요구를 행한다(S70). 또한, S70의 플로우는 S60으로부터 일련의 흐름으로서 행하여지고, 회원 단말(2)로서 사용되는 퍼스널 컴퓨터나 휴대전화의 브라우저가 일반적으로 구비하는 리다이렉트(redirect) 기능 등을 이용하여 실현 가능하고, 카드 회원이 의식하는 않고 회원 단말(2) 내부에서 자동적으로 처리되는 플로우이다.

<163> 인증 서버(7)는 회원 단말(2)에 일회용 패스워드의 송신을 촉구하고, 회원 단말(2)로부터 수신한 일회용 패스워드에 기초하여 카드 회원의 인증을 행한다(S80).

<164> 구체적으로는, 인증 서버(7)는 액세스해 온 회원 단말(2)로부터 카드정보 및 주문정보를 수신하고, 이 카드정보를 갖는 카드 회원이 조금 전에 가맹점 단말(3)로부터 중개 서버(5)를 통해서 인증 실행 여부 확인 요구를 받은 카드 회원인지의 여부를 확인한다. 이 확인은, 미리 정해진 소정시간 전에 중개 서버(5)로부터 해당 카드 회원의 카드정보를 수신한 것인가 아닌가의 로그를 남겨 두고, 회원 단말(2)로부터 수신한 카드 회원의 카드정보가 소정시간 전에 로그에 남겨진 카드정보에 일치하는지의 여부를 확인함으로써 행하여진다.

<165> 또한, 주문정보는 회원 단말(2)로부터가 아니라 S20,30의 플로우에 있어서 가맹점 단말(3)로부터 중개 서버(5)를 통해서 인증 서버(7)에 송신되고 있어도 되고, 가맹점 단말(3)로부터 회원 단말(2)에 인증 서버(7)의 URL 정

보가 송신될 때 함께 송신되어, 회원 단말(2)이 인증 서버(7)에 액세스할 때에 인증 서버(7)에 전송되게 되어 있어도 된다.

<166> 또한 인증 서버(7)가 액세스해 온 회원 단말(2)의 카드 회원과, 가맹점 단말(3)로부터 인증 실행 여부 확인 요구를 받은 카드 회원이 동일한지의 여부의 확인은, 카드정보의 대조뿐만 아니라 주문정보를, 회원 단말(2) 및 가맹점 단말(3)[직접적으로는 중개 서버(5)]의 쌍방으로부터 수신하고, 그것들의 대조를 병용해서 행하여져도 좋다.

<167> 인증 서버(7)가, 먼저 인증 실행 여부 확인 요구를 받은 카드 회원의 네트 결제 보조장치(1)로부터의 액세스인 것을 확인하면, 인증 서버(7)는 수신한 주문정보에 기초하여, 도 4(b)에 나타내는 바와 같은 일회용 패스워드 입력화면(101)을 작성하고, 액세스가 있은 회원 단말(2)에 송신한다.

<168> 도 4(b)의 일회용 패스워드 입력화면(101)에는 카드 회원이 네트 상거래를 행하는 상대인 가맹점명과, 주문하려고 하고 있는 상품·서비스의 금액, 주문일이 표시되어 있다.

<169> 회원 단말(2)에 일회용 패스워드 입력화면(101)이 표시되면, 카드 회원은 네트 결제 보조장치(1)의 스타트 키(12b)를 누른다. 네트 결제 보조장치(1)의 OTP 생성수단(16)은 스타트 키(12b) 누름을 검출하면 일회용 패스워드 생성 대기 상태로부터 일회용 패스워드 생성 플로우로 이행한다.

<170> OTP 생성수단(16)은 OTP 생성정보 저장부(17)에 저장된 공통 키를 판독하여 시간측정수단(18)에 의해 시간측정된 스타트 키(12b)가 눌린 일시로 이루어지는 일시 데이터(연월일초, 초는 30초 단위)를, 이 공통 키로 암호화함으로써 일회용 패스워드를 생성하고, 이것을 10진수로 하여 디스플레이(11)에 표시한다. 또한, 본 실시예의 암호화 방식은 공통 키 암호방식을 채용하고 있다. 또한 본 실시예의 디스플레이(11)의 표시 가능 자리수는 8자리수이므로, 디스플레이(11)에는 생성된 일회용 패스워드 위 6~8자리수를 표시하는 것으로 한다.

<171> 카드 회원은 회원 단말(2)에 표시된 일회용 패스워드 입력화면(101)의 패스워드 입력란(101a)에 네트 결제 보조장치(1)의 디스플레이(11)에 표시된 일회용 패스워드를 입력하고, 송신 버튼(101b)을 클릭하면 입력된 일회용 패스워드가 인증 서버(7)에 송신된다.

<172> 또한, 일회용 패스워드의 입력이 끝난 후는 카드 회원이 네트 결제 보조장치(1)의 스타트 키(12b)를 다시 누름으로써 네트 결제 보조장치(1)의 디스플레이(11)에 표시된 일회용 패스워드를 비표시로 하는 것이 시큐리티의 관점에서 바람직하다. 또 동시에 전원도 오프되는 것이 에너지 절약의 관점에서 바람직하다.

<173> 회원 단말(2)로부터 일회용 패스워드를 수신한 인증 서버(7)는, 우선 이 회원 단말(2)이 먼저 일회용 패스워드의 송신을 요구한 상대인 것을, 회원 단말(2)의 식별 번호 등의 대조나, 해당 회원 단말(2) 개별적으로 생성되어서 송신된 일회용 패스워드 입력화면(101)에 대한 회신인지의 여부의 확인에 의해 확인한다.

<174> 확인 후, 인증 서버(7)는 일회용 패스워드의 송신을 요구하기 전에 수신하고 있던 카드 회원의 카드정보에 기초하여, OTP 생성정보 중에서 이 카드번호에 관련되어서 등록되어 있는 공통 키를 인출하고, 인증 서버(7)가 회원 단말(2)로부터 일회용 패스워드를 수신한 일시로 이루어지는 일시 데이터(연월일초, 초는 30초 단위)를, 이 공통 키로 암호화해서 일회용 패스워드를 생성하고, 이것을 10진수로 변환한다. 또한, 본 실시예의 암호화 방식은 공통 키 암호방식을 채용하고 있다.

<175> 이와 같이 하여 인증 서버(7)는, 인증 서버(7)에서 생성된 일회용 패스워드와, 먼저 회원 단말(2)로부터 수신한 일회용 패스워드가 일치하는지의 여부를 확인한다. 일치하면, 이 일회용 패스워드는 확실히 네트 결제 보조장치(1)와 인증 서버(7)에만 저장된 공통 키에 의해, 거의 같은 시각에 작성된 일회용 패스워드인 것이 증명된다.

<176> 즉, 일회용 패스워드를 인증 서버(7)에 송신한 회원 단말(2)의 조작자가, 해당 일회용 패스워드의 생성에 사용된 공통 키 및, 해당 공통 키에 관련된 카드정보가 저장된 네트 결제 보조장치(1)의 조작자이며, 또한, 해당 카드정보를 이용 가능한 카드 회원 본인이며, 이것에 의해 네트 상거래를 의뢰해 온 카드 회원의 본인 확인이 이루어지게 된다.

<177> 또한, 일회용 패스워드 생성 방식이 본 실시예와 같이 시간 동기방식을 채용하고 있을 경우, 네트 결제 보조장치(1)가 일회용 패스워드 생성에 사용하는 일시와, 인증 서버(7)가 일회용 패스워드 생성에 사용하는 일시는 엄밀하게는 같아지지 않고, 따라서, 인증 서버(7)가 일회용 패스워드를 생성하고나서 카드 회원이 네트 결제 보조장치(1)의 스타트 키(12b)를 누르고, 네트 결제 보조장치(1)가 일회용 패스워드를 생성할 때까지의 시간차를 고려하여, 본 실시예에서는 일시 데이터의 초 분해능을 30초로 하고 있다.

<178> 그러나, 양자에 의해 생성된 일회용 패스워드가 완전하게 일치하지 않는 한, 카드 회원의 진정성을 인정하지 않는다고 하는 것에서는 카드 회원이 네트 결제 보조장치(1)의 스타트 키(12b)를 눌러서 일회용 패스워드가 생성되고나서, 인증 서버(7)가 회원 단말(2)로부터 일회용 패스워드를 수신하기까지의 동안, 30초 이상 경과해버렸을 경우에, 그것만으로 일회용 패스워드가 불일치가 되어 인증되지 않는다고 하는 사태가 증가하여, 오히려 네트 상거래의 편리성이 손상되게 되어 버린다.

<179> 따라서, 인증 서버(7)는 회원 단말(2)로부터 수신한 일회용 패스워드가 일치하지 않은 경우에도 회원 단말(2)로부터 일회용 패스워드를 수신한 일시를, 전후 N회×30초분 어긋나게 하여 인증 서버(7)측에서 일회용 패스워드를 다시 생성하고, 회원 단말(2)측에서 생성된 일회용 패스워드와 일치하면 카드 회원의 본인 확인이 된 것으로 한다.

<180> 또한, N은 시큐리티 정밀도를 고려하여 미리 결정해 둔다. 즉, 시큐리티 정밀도를 높게 하고 싶을 때에는 N을 작게 설정하고, 시큐리티 정밀도를 낮게 해서 카드 회원측의 편리성을 우선하고 싶은 경우에는 N을 크게 설정해 둔다.

<181> 인증 서버(7)는 일회용 패스워드 대조에 의한 카드 회원의 인증 결과를 회원 단말(2)에 송신한다(S90). 또한, 구체적으로는, 인증 서버(7)는 회원 단말(2)에 대하여 인증 결과에 추가로 가맹점 단말(3)의 URL 정보를 송신하고, 회원 단말(2)로부터 가맹점 단말(3)에 인증 결과가 전송되도록 해 둔다.

<182> 인증 결과를 수신한 회원 단말(2)은 해당 인증 결과(본인 인증 OK, 본인 인증 NG)를 또한 가맹점 단말(3)에 전송한다(S100). 또한, S100의 플로우는 S70과 마찬가지로 S90으로부터 일련의 흐름으로서 행하여져, 회원 단말(2)의 브라우저의 리다이렉트 기능에 의해 실현 가능하고, 실제로는 카드 회원이 의식하지 않고 회원 단말(2)내부에서 자동적으로 처리되는 플로우이다.

<183> 가맹점 단말(3)은 회원 단말(2)로부터 인증 결과를 수신하고, 인증의 결과, 카드 회원의 본인 확인이 되었을 경우(본인 인증 OK)에는 가맹점 관리회사에 해당 카드 회원의 오소리제이션 요구를 하기 위해서, 가맹점 관리회사 단말(4)에 카드 회원의 카드정보와, 결제 희망 금액(카드 회원이 주문하려고 하고 있는 상품·서비스의 금액)으로 이루어지는 거래 데이터에 추가로, 해당 인증 결과를 송신한다(S110). 또한, 거래 데이터는 S10에서 회원 단말(2)로부터 주문정보와 카드정보의 송신이 있은 시점에서 이미 생성되어서, 가맹점 단말(3)에 기억된 것이 판독되어도 좋다.

<184> 가맹점 관리회사 단말(4)은 가맹점 단말(3)로부터 수신한 거래 데이터와 인증 결과에 기초하여 본인 인증 OK의 카드 회원의 카드번호에 기초하여 카드 발행원(발행자)인 카드 발행회사를 특정하고, 특정된 카드 발행회사의 카드 발행회사 단말(6)에 거래 데이터와 인증 결과를 전송한다(S120).

<185> 거래 데이터와 인증 결과를 수신한 카드 발행회사 단말(6)은, 도면에 나타나 있지 않은 회원 데이터 베이스에 저장되어 있는 회원마다의 회원정보나 여신 정보에 기초하여 거래 데이터에 포함되는 결제 희망 금액이, 오소리제이션을 의뢰받은 카드 회원의 크레디트라인의 범위 내인지의 여부를 확인한다. 결제 희망 금액이 크레디트라인의 범위 내이면 오소리제이션 OK로 해서, 결제 희망 금액분의 크레디트라인을 확보한다.

<186> 그리고, 카드 발행회사 단말(6)은 오소리제이션의 결과(오소리제이션 OK, 오소리제이션 NG)를 가맹점 관리회사 단말(4)에 송신하고(S130), 또한 가맹점 관리회사 단말(4)은 가맹점 단말(3)에 오소리제이션 결과를 전송한다(S140).

<187> 그리고, 가맹점 단말(3)은 가맹점 관리회사 단말(4)로부터 오소리제이션 결과를 수신한 후, 그 결과를 회원 단말(2)에 통지한다(S150). 구체적으로는, 오소리제이션 결과가 OK이었을 경우에는, 가맹점과 카드 회원 사이에서 해당 카드 회원의 카드번호를 사용한 결제에 의한 네트 상거래가 성립된 취지의 화면을 회원 단말(2)에 송신하고, 회원 단말(2)에 표시한다. 또한 오소리제이션 결과가 NG이었을 경우에는, 네트 상거래가 불성립된 취지의 화면을 회원 단말(2)에 송신, 표시한다.

<188> 또한, 본 실시예에서는, 인증 서버(7)에 있어서의 일회용 패스워드를 사용한 본인 인증은 회원 단말(2)과 가맹점 단말(3) 사이에서 네트 상거래가 행하여질 때마다 행하여진다. 즉, 본 실시예의 OTP 생성수단(16)에서 생성되는 일회용 패스워드는 1회 한도의 네트 상거래에 유효한 것이기 때문에, 가령 네트 결제 보조장치를 소지하지 않는 제3자가 일회용 패스워드를 도청해도 제3자가 카드 회원인 체해서 이후의 네트 상거래를 행할 수는 없어 네트 상거래의 안전성이 더욱 향상된다.

<189> 실시예 2

<190> 다음에 네트 결제 보조장치(1a)(도시 생략)를 배포받은 카드 회원이, 해당 네트 결제 보조장치(1a)를 이용하여 통신기능을 갖는 퍼스널 컴퓨터나 휴대전화로부터 해당 카드 회원의 카드번호를 사용한 결제에 의해, 네트 상거래를 행할 경우의 일실시예에 대하여 설명한다.

<191> 앞의 실시예 1과 본 실시예의 차이점은, 네트 결제 보조장치가 구비하는 OTP 생성수단(16)의 일회용 패스워드 생성 방법과, OTP 생성정보 저장부(17)의 저장 내용과, 도 3에 있어서의 회원 단말(2)과 인증 서버(7)[본 실시예에서는 인증 서버(7a)라고 함] 사이의 인증 플로우(S80, S90)의 내용이다.

<192> 즉, 앞의 실시예 1에서는 일회용 패스워드 생성 방법을 시간 동기방식으로 하고 있었지만, 본 실시예에서는 이용 횟수 동기방식을 채용한다. 이것에 따라, 본 실시예의 네트 결제 보조장치(1a)에 있어서는, 도 1에 기재되어 있었던 시간측정수단(18)이 계수수단(18a)(도시 생략)으로 바뀐다.

<193> 네트 결제 보조장치(1, 1a)와 인증 서버(7, 7a)에 관하여, 상술한 차이점 이외의 구성 및, S80, S90 이외의 플로우에 대해서는 도 1~도 3에 나타내어진 실시예와 동일하므로, 이하, 도 1~도 3을 이용하여 도 3의 S80, S90의 부분만의 상세 플로우를 설명한다.

<194> 본 실시예의 OTP 생성정보 저장부(17)에 저장되는 OTP 생성정보는 네트 결제 보조장치(1a)에 고유의 공통 키와, 이용횟수 정보로 구성된다.

<195> 이 중, 공통 키는 OTP 생성정보 저장부(17) 내에 재기록 불가능한 상태로 저장되고, OTP 생성수단(16)에서 생성된 일회용 패스워드의 검증을 행하는 인증 서버(7a)에 있어서, 카드정보 저장부(13)에 저장되어 있는 카드번호와 관련지어져 있다.

<196> 이용횟수 정보는 공통 키와 마찬가지로 인증 서버(7a)에 있어서 카드정보 저장부(13)에 저장되어 있는 카드번호와 관련지어져 있다.

<197> 즉, 이들 OTP 생성정보는 카드번호와 관련지어진 상태에서 인증 서버(7a)에도 저장되어 있고, 인증 서버(7a)가 회원 단말(2)로부터 일회용 패스워드를 수신했을 때에 회원 단말(2)과 마찬가지로 인증 서버(7a)에서도 일회용 패스워드를 생성하고, 이들이 일치하는지의 여부를 확인함으로써 일회용 패스워드의 타당성 검증, 카드 회원의 인증을 행한다.

<198> 또한 이용횟수 정보는 OTP 생성수단(16)으로부터의 재기록 지령이 있었을 경우에만 재기록이 가능한 정보이며, 계수수단(18a)에 의해, 0회, 1회, 2회라고 하는 것과 같이 1씩 가산되거나, 또는 100회, 99회, 98회라고 하는 것과 같이 1씩 감산된 후, 가산 또는 감산 후의 수치가 OTP 생성정보 저장부(17)에 저장되어서 이용횟수 정보가 갱신된다. 또한, 가산일지 감산일지는 미리 정해져 있다.

<199> 또한, 계수수단(18a)은 OTP 생성수단(16)에 포함되어 있어도 되고, OTP 생성수단(16)과 별도로 형성되어 있어도 되지만, 후자의 경우에는 OTP 생성수단(16)이 계수수단(18a)을 제어하여 이용횟수 정보의 재기록이 행하여질 필요가 있다.

<200> 도 3의 S80에 있어서, 우선 인증 서버(7a)는 회원 단말(2)에 일회용 패스워드의 송신을 재촉하고, 회원 단말(2)로부터 수신한 일회용 패스워드에 기초하여 카드 회원의 인증을 행한다.

<201> 구체적으로는, 인증 서버(7a)는 액세스하여 온 회원 단말(2)로부터 카드정보 및 주문정보를 수신하고, 이 카드정보를 갖는 카드 회원이 조금 전에 가맹점 단말(3)로부터 중개 서버(5)를 통해서 인증 실행 여부 확인 요구를 받은 카드 회원 인지의 여부를 확인한다. 이 확인은, 미리 정해진 소정시간 전에 중개 서버(5)로부터 상기 카드 회원의 카드정보를 수신했는지의 여부의 로그를 남겨 두고, 회원 단말(2)로부터 수신한 카드 회원의 카드정보가 소정시간 전에 로그에 남겨진 카드정보에 일치하는지의 여부를 확인함으로써 행하여진다.

<202> 또한, 주문정보는 회원 단말(2)로부터가 아니라 S20,30의 플로우에 있어서 가맹점 단말(3)로부터 중개 서버(5)를 통해서 인증 서버(7a)에 송신되고 있어도 좋고, 가맹점 단말(3)로부터 회원 단말(2)에 인증 서버(7a)의 URL 정보가 송신될 때에 함께 송신되어, 회원 단말(2)이 인증 서버(7a)에 액세스할 때에 인증 서버(7a)에 전송되게 되어 있어도 된다.

<203> 또한 인증 서버(7a)가 액세스하여 온 회원 단말(2)의 카드 회원과, 가맹점 단말(3)로부터 인증 실행 여부 확인 요구를 받은 카드 회원이 동일한지의 여부의 확인은, 카드정보의 대조뿐만 아니라 주문정보를 회원 단말(2) 및 가맹점 단말(3)[직접적으로는 중개 서버(5)]의 쌍방으로부터 수신하고, 그것들의 대조를 병용해서 행하여져도 좋다.

<204> 인증 서버(7a)가, 먼저 인증 실행 여부 확인 요구를 받은 카드 회원의 네트 결제 보조장치(1)로부터의 액세스인 것을 확인하면, 인증 서버(7a)는 수신한 주문정보에 기초하여 도 4(b)에 나타내는 바와 같은 일회용 패스워드 입력화면(101)을 작성하고, 액세스가 있은 회원 단말(2)에 송신한다.

<205> 도 4(b)의 일회용 패스워드 입력화면(101)에는 카드 회원이 네트 상거래를 행하는 상대인 가맹점명과, 주문하려고 하고 있는 상품·서비스의 금액, 주문일이 표시되어 있다.

<206> 회원 단말(2)에 일회용 패스워드 입력화면(101)이 표시되면 카드 회원은 네트 결제 보조장치(1)의 스타트 키(12b)를 누른다. 네트 결제 보조장치(1)의 OTP 생성수단(16)은 스타트 키(12b) 누름을 검출하면, 일회용 패스워드 생성 대기 상태로부터 일회용 패스워드 생성 플로우로 이행한다.

<207> OTP 생성수단(16)은 OTP 생성정보 저장부(17)에 저장된 공통 키와 이용횟수 정보를 판독하고, 해당 이용횟수 정보를 공통 키로 암호화해서 일회용 패스워드를 생성하고, 이것을 10진수로 하여 디스플레이(11)에 표시한다.

<208> 또한, 본 실시예에서는 이용횟수 정보를 소정의 일회용 패스워드 생성 알고리즘을 이용하여 일회용 패스워드를 생성하고 있다.

<209> 또한 본 실시예의 디스플레이(11)의 표시 가능 자리수는 8자리수므로, 디스플레이(11)에는 생성된 일회용 패스워드 위 6~8자리수를 표시하기로 한다.

<210> 또한, OTP 생성정보는 상기 이용횟수 정보와 공통 키의 이외에, 기타 네트 결제 보조장치(1a)와 인증 서버(7a)의 양자밖에 알 수 없는 임의의 정보[예를 들면 팔러시(policy) 등]를 포함하고 있어도 되고, 그 경우, 이용횟수 정보와 해당 임의의 정보가 공통 키로 암호화되어 일회용 패스워드가 생성되어도 좋다.

<211> OTP 생성수단(16)은 일회용 패스워드를 생성한 후, 계수수단(18a)에 먼저 판독한 이용횟수 정보를 1, 가산 또는 감산시켜서 OTP 생성정보 저장부(17)의 이용횟수 정보를 재기록하여 갱신한다.

<212> 카드 회원은 회원 단말(2)에 표시된 일회용 패스워드 입력화면(101)의 패스워드 입력란(101a)에 네트 결제 보조장치(1)의 디스플레이(11)에 표시된 일회용 패스워드를 입력하고 송신 버튼(101b)을 클릭하면, 입력된 일회용 패스워드가 인증 서버(7a)에 송신된다.

<213> 또한, 일회용 패스워드의 입력이 끝난 후는, 카드 회원이 네트 결제 보조장치(1)의 스타트 키(12b)를 다시 누름으로써 네트 결제 보조장치(1)의 디스플레이(11)에 표시되어 있는 일회용 패스워드를 비표시로 하는 것이 시큐리티의 관점에서 바람직하다. 또 동시에, 전원도 오프되는 것이 에너지 절약의 관점에서 바람직하다.

<214> 회원 단말(2)로부터 일회용 패스워드를 수신한 인증 서버(7a)는, 우선 이 회원 단말(2)이 먼저 일회용 패스워드의 송신을 요구한 상대인 것을, 회원 단말(2)의 식별 번호 등의 대조나, 해당 회원 단말(2) 개별적으로 생성되어서 송신된 일회용 패스워드 입력화면(101)에 대한 회신인지의 여부의 확인에 의해 확인한다.

<215> 확인 후, 인증 서버(7a)는 일회용 패스워드의 송신을 요구하기 전에 수신하고 있던 카드 회원의 카드정보에 기초하여 OTP 생성 정보 중에서 이 카드번호에 관련되어서 등록되어 있는 공통 키와 이용횟수 정보를 인출하고, 이용횟수 정보를 공통 키로 암호화해서 일회용 패스워드를 생성하고, 이것을 10진수로 변환한다.

<216> 또한, 본 실시예에서는 이용횟수 정보를 소정의 일회용 패스워드 생성 알고리즘을 이용하여 일회용 패스워드를 생성하고 있다. 또한 OTP 생성정보에 임의의 정보가 포함되어 있으면, 이용횟수 정보에 추가로 상기 임의의 정보도 아울러 공통 키로 암호화한다.

<217> 이렇게 하여, 인증 서버(7a)는 인증 서버(7a)에서 생성된 일회용 패스워드와, 먼저 회원 단말(2)로부터 수신한 일회용 패스워드가 일치하는지의 여부를 확인한다. 일치하면 이 일회용 패스워드는 확실히 네트 결제 보조장치(1)와 인증 서버(7a)에만 저장된 이용횟수 정보와 공통 키에 의하여 작성된 일회용 패스워드인 것이 증명된다.

<218> 즉, 일회용 패스워드를 인증 서버(7a)에 송신한 회원 단말(2)의 조작자가 상기 일회용 패스워드의 생성에 사용된 이용횟수 정보와 공통 키 및, 상기 이용횟수 정보와 공통 키에 관련된 카드정보가 저장된 네트 결제 보조장치(1)의 조작자이며, 또한 상기 카드정보를 이용 가능한 카드 회원 본인이며, 이것에 의해 네트 상거래를 의뢰해 온 카드 회원의 본인 확인이 이루어지게 된다.

<219> 인증 서버(7a)는 일회용 패스워드 대조에 의한 카드 회원의 인증 결과(본인 인증 OK, 본인 인증 NG)를 회원 단말(2)에 송신함과 아울러 앞의 일회용 패스워드 생성에 사용한 이용횟수 정보를, 미리 결정된 연산 방법에 의해 가산 또는 감산하고, 그 연산 결과를 인증 서버(7a) 내의 이용횟수 정보로서 재기록, 갱신한다(S90).

<220> 또한, 일회용 패스워드 생성 방식이 본 실시예와 같이 이용횟수 동기방식을 채용하고 있을 경우, 회원 단말(2) 및 네트 결제 보조장치(1a)의 조작자가 정당한 카드 회원이었다고 해도 네트 결제 보조장치(1a)가 일회용 패스워드 생성에 사용하는 이용횟수 정보와, 인증 서버(7a)가 일회용 패스워드 생성에 사용하는 이용횟수 정보가 다르고, 일회용 패스워드가 일치하지 않을 경우가 있다.

<221> 카드 회원이 네트 결제 보조장치(1a)에서 일회용 패스워드를 생성해도, 그것이 반드시 인증 서버(7a)에 송신될 보증은 없고, 카드 회원이 네트 상거래를 도중에 중단해 버릴 경우나, 또한 애당초 네트 상거래를 행하지 않고 있음에도 불구하고 네트 결제 보조장치(1a)를 조작하여, 헛되이 일회용 패스워드를 생성해버릴 경우가 있다. 그러한 경우에는, 네트 결제 보조장치(1a)의 이용횟수 정보는 갱신되는데도 인증 서버(7a)의 이용횟수 정보는 갱신되지 않으므로, 당연히 생성되는 일회용 패스워드도 다른 것으로 되어 버린다.

<222> 그러나, 양자에 의해 생성된 일회용 패스워드가 완전하게 일치하지 않는 한, 카드 회원의 진정성을 인정하지 않는다고 하는 것에서는, 인증 NG가 증가하여 오히려 네트 상거래의 편리성이 손상되게 되어 버린다.

<223> 따라서, 인증 서버(7a)는 회원 단말(2)로부터 수신한 일회용 패스워드가 일치하지 않은 경우에도 인증 서버(7a)에 저장되어 있는 이용횟수 정보를 소정 범위(예를 들면 이용횟수 정보+N)에서 변경하고, 인증 서버(7a)측에서 일회용 패스워드를 고쳐서 생성하여, 회원 단말(2)측에서 생성된 일회용 패스워드와 일치하면 카드 회원의 본인 확인이 된 것으로 한다.

<224> 또한, N은 시큐리티 정밀도를 고려하여 미리 결정해 둔다. 즉, 시큐리티 정밀도를 높게 하고 싶을 때에는 N을 작게 설정하고, 시큐리티 정밀도를 낮게 해서 카드 회원측의 편리성을 우선하고 싶은 경우에는 N을 크게 설정해 둔다.

<225> 이상과 같이, 본 발명의 네트 결제 보조장치를 이용하여 네트 상거래를 행하면 카드정보를 카드정보 입력화면에 입력할 때에 네트 결제 보조장치에 입력된 입력정보가 네트 결제 보조장치에 저장되어 있는 인증정보와 일치하지 않으면 카드 회원 자신이여도 카드정보를 알 수 없으므로, 카드정보가 노출되어 있는 종래의 신용카드와 달리 카드정보의 비닉성이 높아지고, 네트 상거래에 있어서의 카드정보의 부정 사용이 방지된다.

<226> 또한 네트 결제 보조장치는 가반형이므로, 카드 회원이 어디에 있어도 휴대전화, 자택의 퍼스널 컴퓨터, 출장지의 퍼스널 컴퓨터를 이용하여 안전한 네트 상거래를 행할 수 있고, 네트 상거래의 편리성이 증가한다.

<227> 또한 네트 상거래가 행하여질 때의 카드 회원의 본인 인증은 네트 결제 보조장치에서 생성되는 일회용 패스워드와, 인증 서버에서 생성되는 일회용 패스워드가 일치하는지의 여부에 의해 행하여진다.

<228> 이 일회용 패스워드는 네트 결제 보조장치에 고유이며, 네트 결제 보조장치 및 인증 서버에만 저장되고, 또한 카드 회원 자신조차도 알 수 없는 공통 키를 이용하여 소정 키의 누름이 검출된 일시로 이루어지는 일시 데이터 혹은 일회용 패스워드의 생성때마다 갱신되는 이용횟수 정보를 암호화한 것이다.

<229> 결국은, 네트 결제 보조장치를 조작하고 있는 카드 회원만이 작성 가능한 인증정보이기 때문에 네트 결제 보조장치를 소지하지 않는 제3자가 카드 회원인 체해서 네트 상거래를 행할 수는 없고, 네트 상거래의 안전성이 더욱 향상된다.

<230> 또한, 이 일회용 패스워드의 생성은 네트 결제 보조장치에 카드정보가 표시된 후가 아니면 행하여지지 않게 되어 있으므로, 네트 결제 보조장치를 갖고 있지 않은 제3자는 카드번호만을 알고 있어도 일회용 패스워드의 생성을 할 수 없다. 또한 제3자가 네트 결제 보조장치를 훔쳤다고 해도 네트 결제 보조장치에 입력하는 인증정보가 없으면 일회용 패스워드의 생성을 할 수 없다. 즉, 제3자는 네트 결제 보조장치의 입수 유무에 관계 없이, 카드 회원인 체한 네트 상거래를 행할 수 없으므로 네트 상거래의 안전성이 보증된다.

<231> 또한, 일회용 패스워드의 생성 방법은 상기 실시예의 시간 동기방식에 한하지 않고, 네트 결제 보조장치와 인증 서버 사이에서 네트 결제 보조장치를 소유하는 카드 회원의 본인 인증을 행할 수 있는 방식이면 된다.

<232> 또한 네트 결제 보조장치는 네트 비접속형의 구성을 채용하고 있기 때문에 한번, 네트 결제 보조장치에 저장된 카드정보, 인증정보, OTP 생성정보는 부정 액세스 등에 의해 판독할 수 없고, 네트 결제 보조장치를 배포받은 카드 회원조차도 판독할 수 없게 되어 있다.

<233> 가령, 네트 결제 보조장치가 퍼스널 컴퓨터나 휴대전화 등의 단말에 접속가능하다고 하면, 네트 결제 보조장치와 단말을 접속 중에 어떠한 불량이 발생했을 경우, 불량의 원인이 네트 결제 보조장치측에 있는 것인가, 단말측에 있는 것인가라고 하는 책임 분해점이 불명확하게 된다. 따라서, 네트 비접속형의 구성을 채용하고 있는 네

트 결제 보조장치는 책임 분해점이 명확하게 되는 의미에서도 유효하다.

<234> 여기에서, 네트 결제 보조장치를 가지지 않는 카드 회원이 본 실시예의 네트 결제 시스템으로 네트 상거래를 행할 경우의 사전등록의 시스템 구성 및 플로우를 도 6에 나타낸다.

<235> 카드 회원은 회원 PC로부터 카드회사(신용카드 브랜드 또는 카드 발행회사)가 운영하는 카드 회원 대상의 WEB 사이트에 액세스하고, 카드 회원만이 아는 회원정보(생년월일, 전화번호, 구좌번호 등)를 입력하고, WEB 사이트에 송신한다[도 6중, (1)].

<236> 회원정보를 수신한 카드회사의 WEB 사이트는 해당 회원정보가 등록되어 있는 카드회사의 기간 시스템에 액세스하고, 수신한 회원정보와 기간 시스템에 등록되어 있는 회원정보의 대조를 기간 시스템에 의뢰한다[도 6 중, (2)]. 기간 시스템은 WEB 사이트에 대조 결과를 회신한다[도 6 중, (3)].

<237> 대조 결과가 OK이면 카드 회원의 본인 확인이 행하여진 것으로 되어 WEB 사이트에서 회원 PC에 패스워드의 등록을 요구한다. 회원 PC는 패스워드를 WEB 사이트에 송신한다[도 6 중, (4)].

<238> 회원 PC로부터 패스워드를 수신한 WEB 사이트는 해당 패스워드를 카드회사의 인증 서버(7)에 등록한다[도 6 중, (5)].

<239> 여기에서 등록되는 패스워드는 고정 패스워드이며, 네트 결제 보조장치에서 생성되는 바와 같은 일회용 패스워드는 아니다. 즉, 네트 결제 보조장치를 가지지 않는 카드 회원이 네트 결제 시스템 상에서 네트 결제를 행할 경우의, 카드 회원의 인증 방법은 고정 패스워드에 의한 방법밖에 없고, 카드번호와 고정 패스워드가 제3자에 한번 알려져 버리면, 이후는 제3자가 카드 회원인 체해서 네트 결제를 행하는 것이 가능해져 버린다.

<240> 또한 네트 결제 보조장치를 가지지 않는 카드 회원은 패스워드를 등록하기 위해서 카드회사의 WEB 사이트에 액세스하고, 본인 인증을 거친 후에 패스워드 등록 작업을 행하지 않으면 안되어 카드 회원측의 부담이 크다.

<241> 또한 카드 회원뿐만 아니라, 카드회사측에 있어서도 패스워드를 카드 회원에 등록시키기 위한 WEB 사이트의 구축, 카드 회원의 본인 인증을 행하기 위한 기간 시스템의 구축이 필요하게 된다.

<242> 또한 네트 결제 보조장치는, 통상 카드번호가 노출되어 있지 않고, 카드 회원만이 알 수 있거나, 또는 카드 회원만이 갖는 인증정보의 입력이 없으면 카드번호가 표시되지 않는 구성으로 되어 있고, 또한 네트 결제시에 카드 회원의 본인 인증에 사용되는 패스워드는 고정 패스워드가 아니라 일회용 패스워드이므로, 제3자가 카드 회원인 체해서 네트 상거래를 행하는 것은 매우 곤란하게 된다.

<243> 이상, 네트 결제 보조장치(1)의 실시예에 대해서 설명했지만, 본 발명의 네트 결제 보조장치는 상기 실시예에서 설명한 구성 요건의 모두를 구비한 네트 결제 보조장치(1)에 한정되는 것은 아니고, 각종의 변경 및 수정이 가능하고, 개개의 목적 실현에 필요한 구성 요건을 임의로 조합하여 본 발명의 네트 결제 보조장치를 구성하는 것이 가능하다. 또, 이러한 변경 및 수정에 대해서도 본 발명의 특허청구의 범위에 속하는 것은 말할 필요도 없다.

<244> 예를 들면, 실시예에서는 신용카드의 카드번호를 사용한 네트 결제에 대하여 설명했지만, 적어도 카드번호에 의해 네트 결제를 행하는 것이 가능한 카드이면, 신용카드 이외에 직불카드 등의 카드에 의한 실시예도, 본 발명의 특허청구의 범위에 속한다.

<245> 또한 본 실시예에서는 카드 결제를 이용한 네트 상거래에 사용되는 것으로 했지만, 카드 회원이 네트 상거래만을 희망하고, 종래의 플라스틱 타입의 자기카드, IC카드 등으로 이루어지는 신용카드에 의한 리얼의 대면 거래를 희망하지 않을 경우에는, 신용카드의 발행은 받지 않아도 좋고, 본 발명의 네트 결제 보조장치의 소유자가 종래의 플라스틱 타입의 신용카드를 반드시 갖고 있을 필요는 없다.

<246> 또한 예를 들면 실시예에서는, 1개의 네트 결제 보조장치(1)의 카드정보 저장부(13)에 1종류의 카드정보를 갖는 1카드 회원의 카드정보를 저장하고, 인증정보 저장부(15)에 1종류의 인증정보를 저장하였을 경우를 설명했지만, 복수의 카드번호가 카드정보 저장부(13)에 저장되어도 좋다. 그 경우의 인증정보는 복수의 카드번호를 표시하기 위해서 공통인 인증정보이여도 좋고, 카드번호와 인증정보가 각각 대응하고, 입력된 인증정보에 따라 디스플레이(11)에 표시되는 카드번호가 다르게 되어 있어도 된다.

<247> 또한 가족카드 등, 동일 또는 복수의 카드번호를 복수인이 사용하는 경우에는 각각의 사람에 따라 다른 인증정보가 인증정보 저장부(15)에 저장되어 있어도 좋고, 공통의 인증정보가 저장되어 있어도 된다.

<248> 또한 상기 실시예에 있어서는 카드정보와 OTP 생성정보가 네트 결제 보조장치(1, 1a) 및 인증 서버(7, 7a)에서, 각각 관련지어져 있는 취지를 서술했지만, 카드정보의 도청을 방지하기 위해서 카드정보와 OTP 생성정보가 직접적이 아니라 간접적으로 관련지어져 있어도, 특허청구의 범위에 포함되는 것으로 한다.

<249> 구체적으로는, 도 3의 S10에 있어서 회원 단말(2)에서 입력된 카드정보가 S20,30에서, 가맹점 단말(3), 중개 서버(5)를 경유하고, 최종적으로 인증 서버(7, 7a)에 송신되게 되지만, 인증 서버(7, 7a)는 이 때, 수신한 카드정보 중, 카드번호를 해당 카드번호와는 다른 유니크(unique)한 번호로 변환하고, 중개 서버(5)를 경유하여 가맹점 단말(3)에 송신한다(S40,50에 있어서).

<250> 또한 이 유니크한 번호는 가맹점 단말(2)로부터 회원 단말(2)에 송신되고, 회원 단말(2)을 경유해서 인증 서버(7, 7a)에 송신된다(S60,70에 있어서).

<251> 상기 유니크한 번호를 수신한 인증 서버(7, 7a)는 최초에 카드번호를 유니크한 번호로 변환한 것과는 반대의 변환 룰에 의해 유니크한 번호를 카드번호로 변환하고, 변환된 카드번호에 관련되어 있는 OTP 생성정보를 일회용 패스워드의 생성에 사용하게 된다.

<252> 이렇게, 카드번호와 카드번호 이외의 유니크한 번호와 OTP 생성정보를 관련지음으로써 S10, S20, S30에서 카드번호가 송신되는 이외는, 네트워크(9a) 상을 카드번호가 흐르는 일이 없으므로, 카드번호가 도청될 가능성이 대폭 낮아져서 시큐리티 향상에 기여한다.

<253> 또한 상기 실시예에서는, 회원 단말(2)이 가맹점 단말(3)에 카드정보를 송신하고, 인증 서버(7, 7a)가 가맹점 단말(3)로부터의 의뢰에 기초하여 도 2의 S80에 있어서 카드 회원의 본인 인증을 행할 경우에 대하여 설명했지만, 본 발명은 반드시 이것에 한정되지 않는다.

<254> 예를 들면, 앞의 회원 단말(2)이 인증 서버(7, 7a)에 액세스하고, 인증 서버(7, 7a)가 카드 회원 전용의 인증정보 입력화면을 회원 단말(2)에 송신하고, 상기 인증 입력화면에 입력된 카드정보와 일회용 패스워드에 기초하여 회원 단말(2)과 인증 서버(7, 7a) 사이에서 카드 회원의 본인 인증을 행해 두고, 그 결과, 본인이라 확인되어서 이후, 소정 조건(예를 들면 소정 시간, 소정 횟수, 소정 가맹점 등) 내에서 회원 단말(2)이 가맹점 단말(3)의 웹 사이트에 액세스하고, 네트 상거래를 행할 수 있게 되어 있어도 좋다.

<255> 즉, 본 발명의 네트 결제 보조장치는 회원 단말(2)과, 카드회사측의 인증 서버(7, 7a) 사이에서 카드 회원의 본인 인증에 사용되고, 인증 후, 실제로 가맹점의 웹 사이트 등에 있어서 네트 상거래를 할 수 있게 되는 것을 기본으로 하고 있고, 반드시, 가맹점 단말(2)로부터의 본인 인증 의뢰를 전제로 하고 있는 것은 아니다.

<256> 본 발명에 있어서의 각 수단, 데이터 베이스는, 그 기능이 논리적으로 구별되어 있을 뿐이며, 물리상 혹은 사실상은 동일한 영역을 하고 있어도 된다. 또 데이터 베이스 대신에 테이터 파일이어도 되는 것은 말할 필요도 없고, 데이터 베이스라는 기재에는 데이터 파일도 포함하고 있다.

<257> 상기 실시예에서는, 네트 결제 시스템 상의 단말이나 서버가 신용카드 브랜드(네트 상거래 서비스의 제공 주체), 카드 발행회사(카드 회원의 획득·카드 회원으로의 카드 발행 주체), 가맹점 관리회사(가맹점의 획득·계약·관리 주체), 가맹점의 각각이 운영하는 것인 취지를 설명했지만, 이것들은 모두 개념상·역할상 구별되는 것이며, 물리적으로는 카드 발행회사와 가맹점 관리회사가 동일할 경우도 있고, 또한 신용카드 브랜드, 카드 발행회사, 가맹점 관리회사가 동일할 경우도 있다.

<258> 따라서, 예를 들면 본 명세서에 있어서 네트 결제 보조장치(1, 1a)는 카드 발행회사로부터 배포되는 것에 한정되는 것은 아니다. 또한 반드시 네트 결제 시스템의 제공 주체가 신용카드 브랜드일 필요도 없다. 또한 카드 발행회사 단말(6)과 인증 서버(7, 7a)와 가맹점 관리회사 단말(4)이 동일하여도 된다. 또한 중개 서버(5)가 그 밖의 단말이나 서버 중 어느 하나와 동일하여도 된다.

<259> 또한, 본 발명을 실시함에 있어서 본 실시형태의 기능을 실현하는 소프트웨어의 프로그램을 기록한 기억매체를 시스템에 공급하고, 그 시스템의 컴퓨터가 기억매체에 저장된 프로그램을 판독하여 실행함으로써도 실현된다.

<260> 이 경우, 기억매체로부터 판독된 프로그램 자체가 상기한 실시형태의 기능을 실현하게 되고, 그 프로그램을 기억한 기억매체는 본 발명을 구성한다.

<261> 프로그램을 공급하기 위한 기억매체로서는, 예를 들면 자기디스크, 하드디스크, 광디스크, 광자기디스크, 자기테이프, 비휘발성의 메모리 카드 등을 사용할 수 있다.

<262> 또, 컴퓨터가 판독한 프로그램을 실행함으로써 상술한 실시형태의 기능이 실현될 뿐만 아니라, 그 프로그램의

지시에 기초하여 컴퓨터 상에서 가동하고 있는 오퍼레이팅 시스템 등이 실제의 처리의 일부 또는 전부를 행하고, 그 처리에 의해 상기한 실시형태의 기능이 실현될 경우도 본 발명에 포함된다.

<263> 또한, 기억매체로부터 판독된 프로그램이 컴퓨터에 삽입된 기능 확장 보드나 컴퓨터에 접속된 기능 확장 유닛에 구비되는 비휘발성 혹은 휘발성의 기억 수단에 기록된 후, 그 프로그램의 지시에 기초하여 기능 확장 보드 혹은 기능 확장 유닛에 구비되는 연산처리장치 등이 실제의 처리의 일부 혹은 전부를 행하고, 그 처리에 의해 상기한 실시형태의 기능이 실현될 경우도 본 발명에 포함된다.

도면의 간단한 설명

<44> 도 1은 본 발명의 네트 결제 보조장치의 외관 및 전기적 하드웨어 구성을 나타내는 구성도이다.

<45> 도 2는 네트 결제 보조장치를 사용한 네트 결제 시스템의 개략 접속 구성도이다.

<46> 도 3은 네트 결제 시스템에 있어서의 네트 상거래의 프로세스 플로우의 일례를 도시한 도면이다.

<47> 도 4는 네트 결제 시스템에 있어서의 네트 상거래의 프로세스 플로우에 있어서, 회원 단말에 표시되는 화면의 일례를 도시한 도면이다.

<48> 도 5는 네트 결제 보조장치의 조작 순서 및 디스플레이 화면 천이를 도시한 도면이다.

<49> 도 6은 네트 결제 보조장치를 사용하지 않는 네트 결제 시스템을 카드 회원이 이용할 때에, 사전에 카드 회원의 본인 인증을 위한 패스워드를 등록하기 위해서 필요한 시스템의 개략 접속 구성도이다.

<50> < 도면의 주요부분에 대한 부호의 설명 >

<51> 1 : 네트 결제 보조장치 10 : 하우징

<52> 11 : 디스플레이 12: 키 조작부

<53> 12a : 숫자키 12b : 스타트 키

<54> 13 : 카드정보 저장부 14 : 인증수단

<55> 15 : 인증정보 저장부 16 : OTP 생성수단

<56> 17 : OTP 생성정보 저장부 18 : 시간측정수단

<57> 19 : 구동용 전원 2 : 회원 단말

<58> 3 : 가맹점 단말 4 : 가맹점 관리회사 단말

<59> 5 : 중개 서버 6 : 카드 발행회사 단말

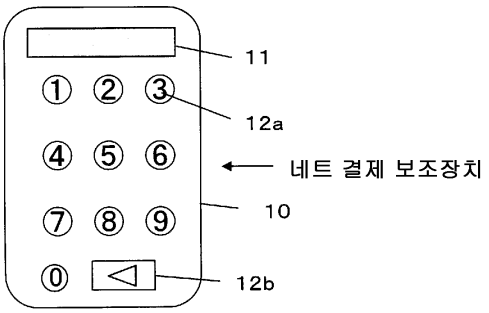
<60> 7 : 인증 서버 9a : 네트워크

<61> 9b : 전용 회선

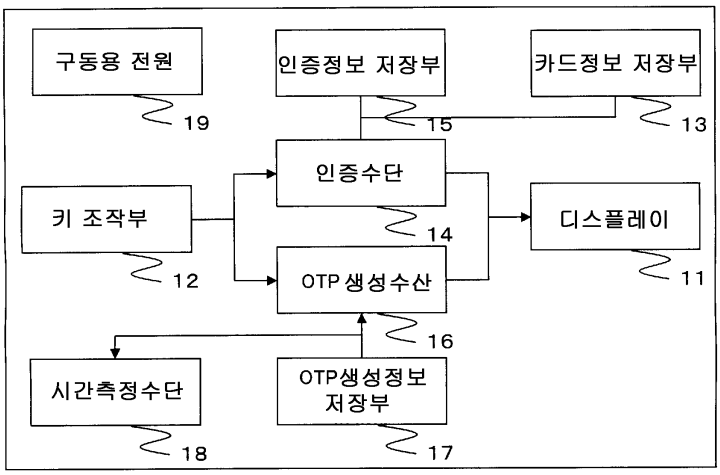
도면

도면1

(a)

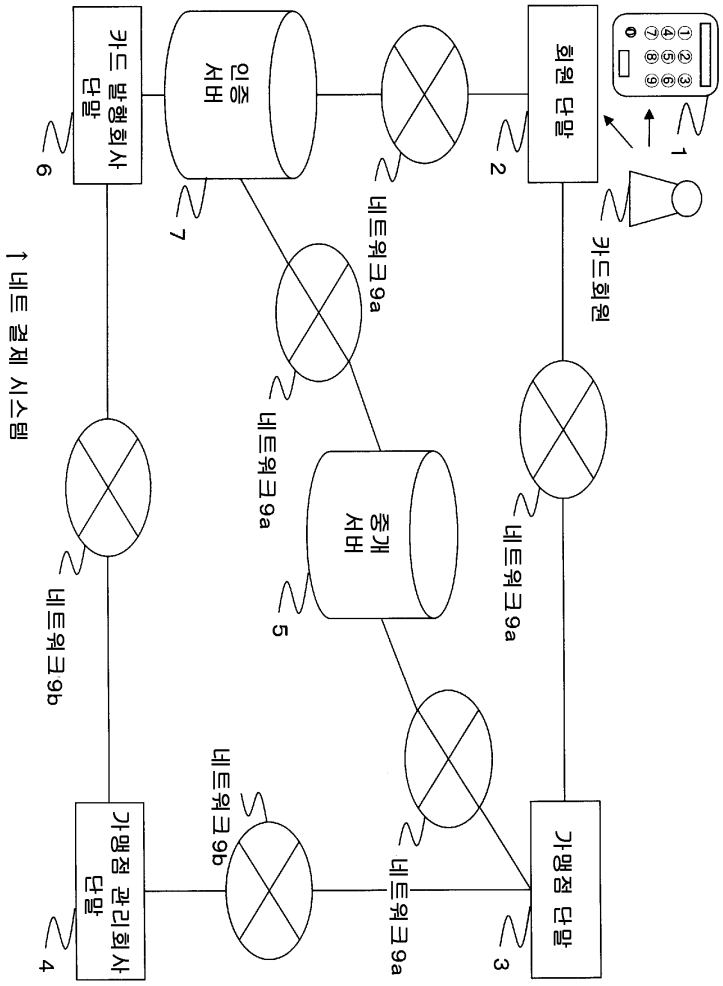


(b)

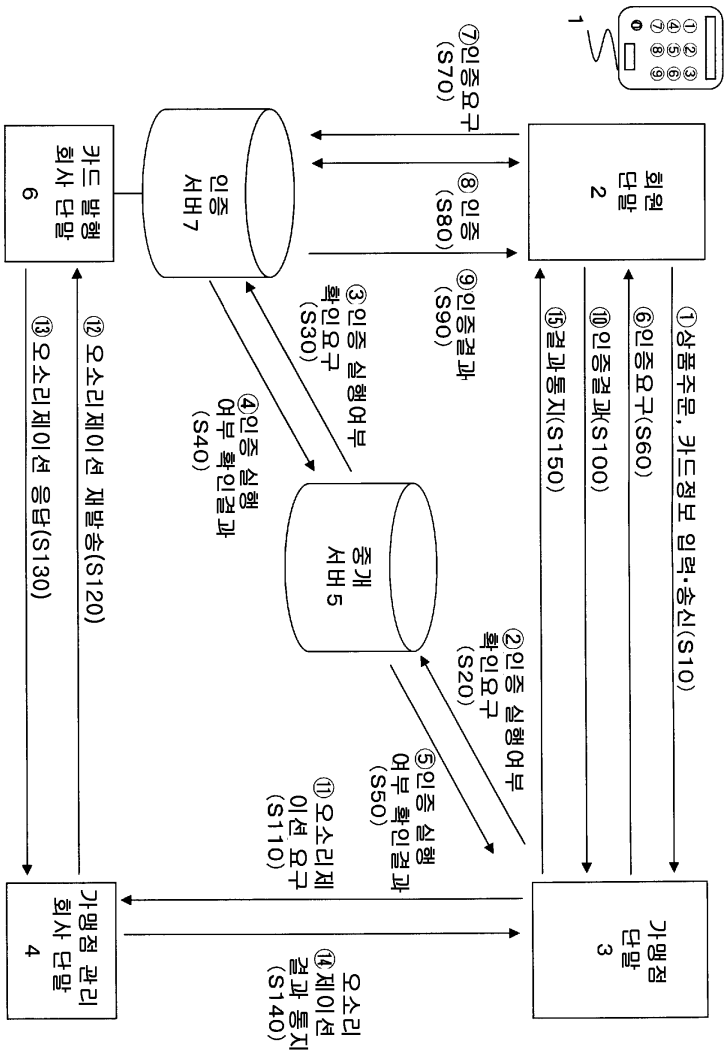


↑ 네트 결제 보조장치 1

도면2

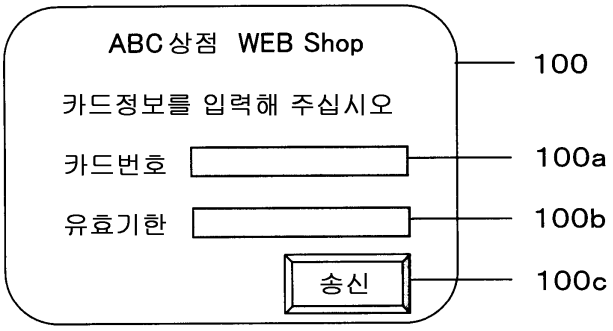

회원 단말
1
카드회원
2
네트워크 9a
인증 서버
7
카드 발행회사 단말
6
네트워크 9a
중개 서버
5
네트워크 9a
네트워크 9b
가맹점 단말
3
네트워크 9a
네트워크 9b
가맹점 관리회사 단말
4
네트 결제 시스템

도면3

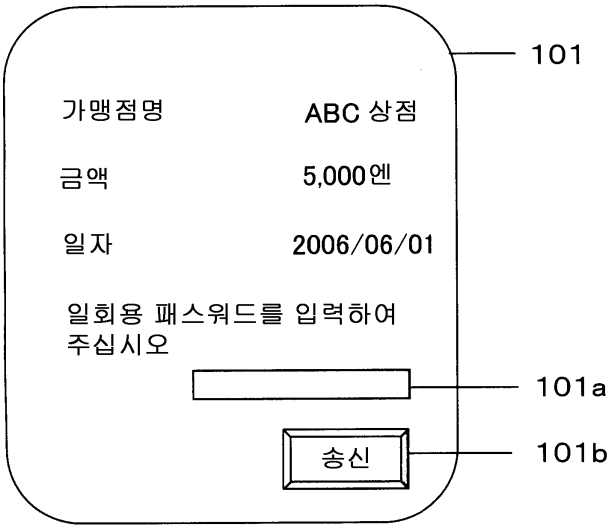

1
회원 단말 2
가맹점 단말 3
가맹점 관리 회사 단말 4
중개 서버 5
카드 발행 회사 단말 6
인증 서버 7
①상품주문, 카드정보 입력·송신(S10)
⑥인증요구(S60)
⑩인증결과(S100)
⑮결과통지(S150)
②인증 실행여부 확인요구 (S20)
⑤인증 실행 여부 확인결과 (S50)
⑪오소리제이션 요구 (S110)
⑭제이션 결과 통지 (S140)
③인증 실행여부 확인요구 (S30)
④인증 실행 여부 확인결과 (S40)
⑦인증요구 (S70)
⑧인증 (S80)
⑨인증결과 (S90)
⑫오소리제이션 재발송(S120)
⑬오소리제이션 응답(S130)

도면4

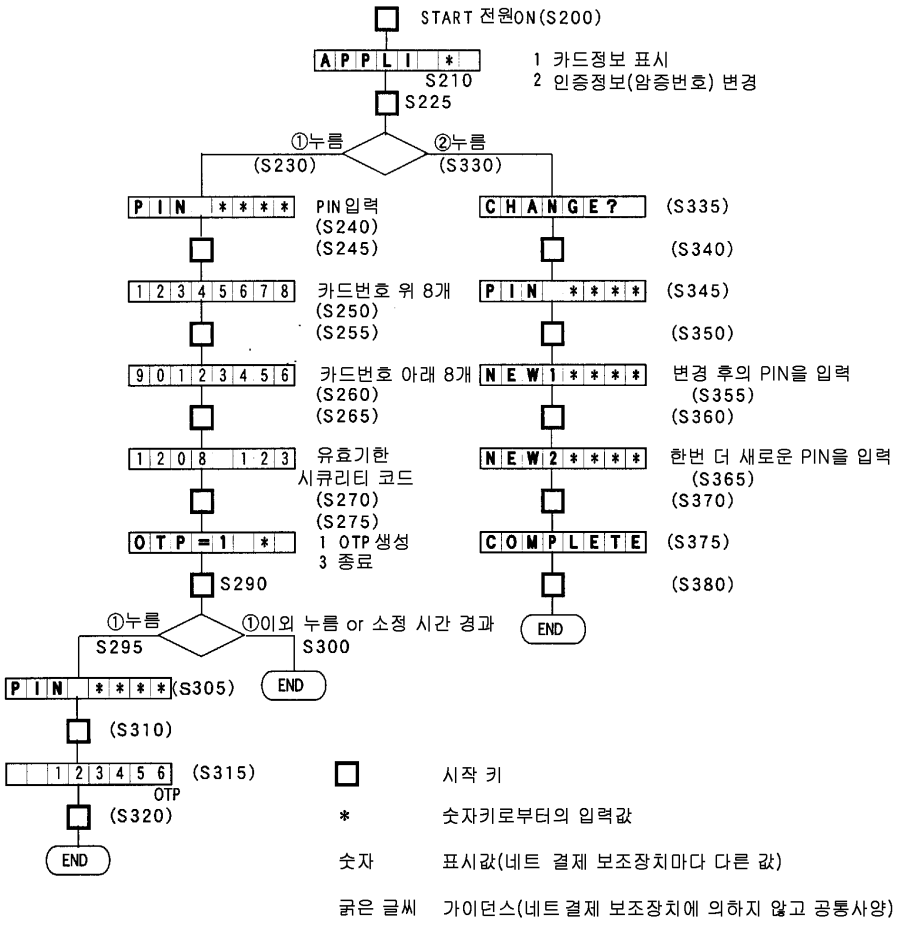
(a)


ABC상점 WEB Shop
카드정보를 입력해 주십시오
카드번호
유효기한
송신
100
100a
100b
100c

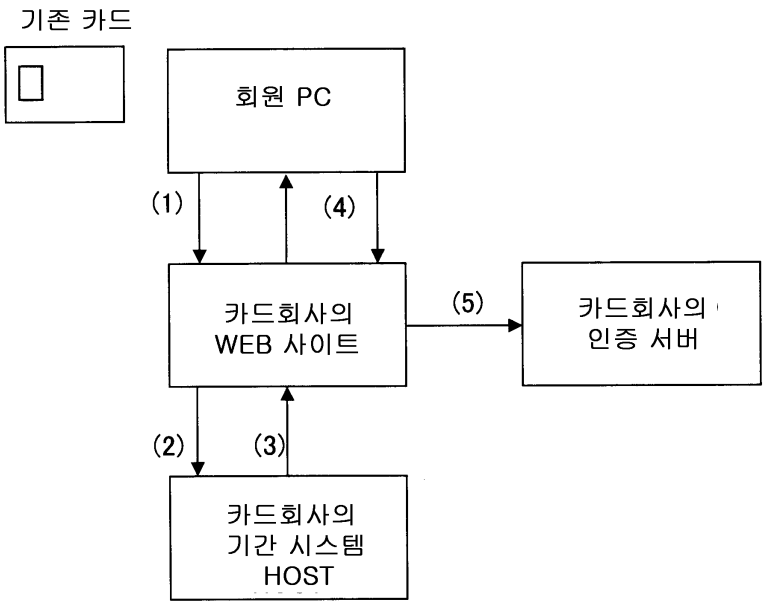
(b)


가맹점명
ABC 상점
금액
5,000엔
일자
2006/06/01
일회용 패스워드를 입력하여 주십시오
송신
101
101a
101b

도면5


START 전원ON(S200)
APPLI *
S210
1 카드정보 표시
2 인증정보(암증번호) 변경
S225
①누름
(S230)
②누름
(S330)
PIN ****
PIN입력
(S240)
(S245)
1 2 3 4 5 6 7 8
카드번호 위 8개
(S250)
(S255)
9 0 1 2 3 4 5 6
카드번호 아래 8개
(S260)
(S265)
1 2 0 8 1 2 3
유효기한
시큐리티 코드
(S270)
(S275)
OTP=1 *
1 OTP생성
3 종료
S290
CHANGE?
(S335)
(S340)
PIN ****
(S345)
(S350)
NEW1 ****
변경 후의 PIN을 입력
(S355)
(S360)
NEW2 ****
한번 더 새로운 PIN을 입력
(S365)
(S370)
COMPLETE
(S375)
(S380)
END
①누름
S295
①이외 누름 or 소정 시간 경과
S300
END
PIN ****
(S305)
(S310)
1 2 3 4 5 6
OTP
(S315)
(S320)
END
시작 키
*
숫자키로부터의 입력값
숫자
표시값(네트 결제 보조장치마다 다른 값)
굵은 글씨
가이던스(네트결제 보조장치에 의하지 않고 공통사양)

도면6


기존 카드
회원 PC
(1)
(4)
카드회사의
WEB 사이트
(5)
카드회사의
인증 서버
(2)
(3)
카드회사의
기간 시스템
HOST