

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2013년 8월 1일 (01.08.2013)



(10) 국제공개번호
WO 2013/111992 A1

- (51) 국제특허분류: *H04W 4/22* (2009.01) *G06Q 40/02* (2012.01)
- (21) 국제출원번호: PCT/KR2013/000614
- (22) 국제출원일: 2013년 1월 25일 (25.01.2013)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보: 10-2012-0007873 2012년 1월 26일 (26.01.2012) KR
- (72) 발명자: 겸
- (71) 출원인: 김한석 (KIM, Han Seok) [KR/KR]; 138-879 서울시 송파구 강동대로 9길 12, Seoul (KR).
- (72) 발명자: 김성수 (KIM, Seong Soo); 138-879 서울시 송파구 강동대로 9길 12, Seoul (KR).
- (74) 대리인: 이은철 (LEE, Un Cheol); 135-748 서울시 강남구 테헤란로 123, 11층 5T 국제특허법률사무소, Seoul (KR).
- (81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO,

AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

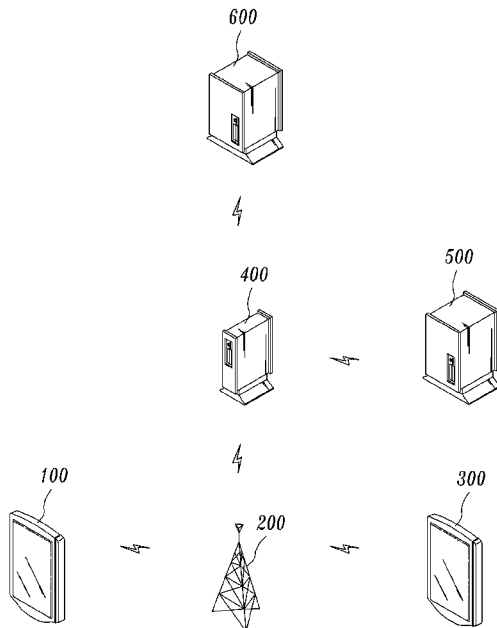
- (84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

공개:

- 국제조사보고서와 함께 (조약 제 21 조(3))

(54) Title: SYSTEM AND METHOD FOR PREVENTING ABUSE OF EMERGENCY CALLS PLACED USING SMARTPHONE

(54) 발명의 명칭: 스마트폰을 이용한 긴급호출 오남용 방지 시스템 및 그 방법



(57) Abstract: The present invention relates to a system and method for preventing the abuse of emergency calls placed using a smartphone. When emergency information is transmitted to a preset guardian terminal by pressing a plurality of emergency buttons, a guardian terminal verifies whether or not there is an emergency and transmits an emergency situation experienced by a smartphone user to a server of an organization, and an officer from the organization having the server is sent to the coordinates of the location of the smartphone user which were received from the mobile communication service provider, thus enabling an organization such as a police department or a fire department to react to an emergency in the shortest possible amount of time when the smartphone user experiences said emergency. An Internet bank account of the smartphone user is converted to a preset virtual Internet bank account so as to be provided with a virtual Internet banking procedure. A bank account connected to a debit card or check card corresponding to a smartphone identification number is converted to a preset virtual bank account so as to enable an offline banking service, thus preventing additional damage to the smartphone user as a result of a cash withdrawal using the smartphone. The credit card information of the smartphone user is registered as information on a lost card, thus preventing additional damage to the smartphone user resulting from a payment by a credit card or from a card loan being taken out.

(57) 요약서:

[다음 쪽 계속]



본 발명은 스마트폰을 이용한 긴급호출 오남용 방지 시스템 및 방법에 관한 것으로서, 복수개의 긴급버튼 감압에 의해 기 설정된 보호자단말기로 비상정보를 송출하는 경우, 보호자단말기가 비상상황여부에 대한 인증을 수행하여 스마트폰 사용자의 비상상황을 기관서버로 전송하고, 기관서버의 경찰관이 이동통신사로부터 수신한 스마트폰 사용자의 위치좌표로 출동함으로써, 스마트폰 사용자의 비상상황 발생 시 경찰서 또는 소방서를 포함하는 기관의 비상상황에 대한 대응을 최단시간에 수행토록 하고, 스마트폰 사용자의 인터넷뱅킹 계좌를 기 설정된 가상의 인터넷뱅킹 계좌로 전환시켜 가상의 인터넷뱅킹 업무를 제공하며, 스마트폰 식별번호와 대응하는 직불카드 또는 체크카드와 연동된 은행계좌를 기 설정된 가상의 은행계좌로 전환하여 오프라인뱅킹 서비스를 제공함으로써, 스마트폰 사용자의 현금인출에 따른 2차 피해를 미연에 방지하고, 스마트폰 사용자의 신용카드정보를 분실카드로 등록하여 스마트폰 사용자의 신용카드 결제 및 카드로 대출에 따른 2차 피해를 미연에 방지하는 효과가 있다.

명세서

발명의 명칭: 스마트폰을 이용한 긴급호출 오남용 방지 시스템 및 그 방법

기술분야

- [1] 본 발명은 스마트폰을 이용한 긴급호출 오남용 방지 시스템 및 그 방법에 관한 것으로 더욱 상세하게는, 스마트폰 사용자가 비상상황 발생시, 복수개의 긴급버튼 감압에 의해 비상정보를 송출하는 경우, 기 설정된 보호자 단말기를 통해 비상상황여부에 대한 인증을 수행하여 기관서버로 전송하고, 스마트폰 사용자의 인터넷뱅킹 계좌를 기 설정된 가상의 인터넷뱅킹 계좌로 전환시켜 가상의 인터넷뱅킹 업무를 제공하는 기술에 관한 것이다.

배경기술

- [2] 최근 이동통신 가입자의 폭발적인 증가로 인하여 이동통신 단말기는 요즘 가정 흔하게 주변에서 볼 수 있는 필수품으로써 인식하게 됨에 따라 이동통신 단말기 제조업체들은 보다 좋은 성능을 가지며 다기능성의 이동통신 단말기를 출시하고 있으며, 이에 발 맞춰 통신 서비스 업체에서는 보다 높은 수준의 통신 서비스 및 여러 부가서비스들을 제공하고 있다.
- [3] 이처럼, 근래에 출시되는 통신서비스 중에 이동통신 단말기의 발신지 추적을 통한 사용자의 위치를 확인할 수 있는 기술이 개발됨에 따라 사용자에게 응급상황이 발생하게 되면, 이를 사용자가 휴대한 이동통신 단말기에서 자동 발신되어 응급기관 또는 경찰서등의 사법기관에 구조를 요청하는 구조요청기능을 갖는 이동통신 단말기 및 이동통신서비스가 출시되고 있다.
- [4] 그러나, 이러한 기술내용이 대중에게 공개됨에 따라 실제 상황에서는 사용자의 비상신호를 발신 전 또는 후에 범죄자가 사용자의 단말기를 뺏고 파손해버려 구조신호가 더 이상 발생되지 않는 문제점과, 경찰관이 사용자의 위험상황을 실제 인지했다 하더라도 정확한 위치추적이 이루어질 수 없고, 또한, 실제 위치추적이 되어 있다하더라도 상황이 종료된 이후에나 현장에 도착하게 되는 문제점이 있다.
- [5] 상기와 같은 상황을 대비하여 이동통신 가입자가 직접 음성통화를 진행할 수 없거나 하는 경우, 버튼조작만을 통해 비상 연락처로 비상정보를 송출하여 사고 상황의 현장 상황을 알리도록 하는 비상호출 처리 방법이 시행되고 있지만, 이동통신 단말기의 잘못된 조작에 의하여 자신도 모르게 원치 않은 상황에서 위급 상황이 잘못 전달되어 지는 문제점이 많았다.
- [6] 또한, 이동통신 가입자가 위급한 상황이 되었을 때 상대방으로부터 송신된 위급 신호를 인지하지 못하는 경우가 발생되면, 구조를 원하는 사용자에게 전혀 도움을 줄 수가 없기 때문에 서비스의 신뢰성이 낮아지는 문제점이 빈번하게 발생하고 있는 실정이다.

- [7] 이러한 문제점을 개선하고자 산업계에서 다양한 연구개발이 이루어지고 있으며, 대한민국 등록특허 제10-0827709호(이동통신망을 이용한 긴급콜 오남용 방지 시스템 및 방법)외 다수개의 문헌이 공개되어 있다.
- [8] 도 1을 참조하여 전술한 선행특허를 살펴보면, 사용자의 긴급 상황을 위한 긴급 구조키가 형성된 구조요청자 단말기와; 구조요청자 단말기로부터 긴급 상황 정보를 입력받아 구조요청자 단말기와 구조자단말기간의 통화연결을 수행하고, 구조자단말기로부터 긴급 상황 정보가 보안 서버에 전달되면, 구조요청자 단말기와 보안 서버와의 통화로 전환되도록 하고, 구조요청자 전화번호 및 단문메시지 정보를 구조자단말기로 전송하도록 하는 통신사 서버와; 통신사 서버를 통해 입력된 구조요청자 단말기의 구조요청자 전화번호 및 단문메시지 정보를 입력받아 긴급 상황을 알리도록 하는 구조자단말기; 및 통신사 서버를 통해 구조요청자 단말기와 일방향 수신 상태로 2차 비상연락처(경찰, 소방서)와 접속되어 구조요청자 단말기와 통화가 가능하도록 한 보안 서버;를 포함하여 구성된다.
- [9] 그러나, 긴급 상황 발생시, 기 설정된 보호자와의 인증을 통해 2차 비상연락처에 긴급 상황을 알리더라도, 경찰관이 사건현장에 당도하기 전에, 범죄자가 구조요청자 단말기의 인터넷뱅킹과 접속하여 사용자 계좌에 예치된 예금을 제3자의 계좌로 이체하거나, 인근 은행의 CD/ATM기를 통해 현금을 인출해가는 등 2차 피해를 예방하지 못하는 문제점이 있다.
- [10] 또한, 스마트폰에 설치된 112앱(App)을 실행하거나 단축키를 입력하여 스마트폰 사용자의 긴급한 상황을 전화로 신고하는 것은 현실적으로 불가능하고, 스마트폰에 구비된 단일개의 긴급버튼 감압에 의해 비상정보를 송출하는 경우, 사용자의 부주의로 인해 비상정보 송출이 오남용 되는 문제점이 발생하고, 이로 인해 경찰관이 출동하는 등 공권력이 불필요하게 소모되는 단점이 있다.
- [11] 아울러, 긴급 상황 발생시, 비상정보 송출에 따라 스마트폰 사용자와 보호자 단말기간의 긴급 통화를 수행할 수 있으나, 이 경우 보호자 단말기가 보안 서버의 경찰관에게 스마트폰 사용자의 구조요청을 위한 전화통화를 위해 스마트폰 사용자와의 통화선로를 차단한 이후에 보안 서버의 경찰관과 전화통화를 수행해야 하는바, 스마트폰 사용자의 긴급한 상황을 지속적으로 모니터링할 수 없는 단점이 있다.

발명의 상세한 설명

기술적 과제

- [12] 본 발명은 상기와 같은 문제점을 해결하고자 안출된 것으로, 복수개의 긴급버튼 감압에 의해 기 설정된 보호자단말기로 비상정보를 송출하는 경우, 보호자단말기가 비상상황여부에 대한 인증을 수행하여 스마트폰 사용자의 비상상황을 기관서버로 전송하고, 기관서버의 경찰관이 이동통신사로부터

수신한 스마트폰 사용자의 위치좌표로 출동함으로써, 스마트폰 사용자의 비상상황 발생 시 경찰서 또는 소방서를 포함하는 기관의 비상상황에 대한 대응을 최단시간에 수행하도록 하는데 그 목적이 있다.

[13] 또한, 본 발명은 스마트폰 사용자가 비상상황 발생시 복수개의 긴급버튼 감압에 의해 기 설정된 보호자단말기로 비상정보를 송출하는 경우, 스마트폰 사용자의 인터넷뱅킹 계좌를 기 설정된 가상의 인터넷뱅킹 계좌로 전환시켜 가상의 인터넷뱅킹 업무를 제공함으로써, 스마트폰 사용자의 인터넷뱅킹 계좌이체에 따른 2차 피해를 미연에 방지함에 그 목적이 있다.

[14] 또한, 본 발명은 스마트폰 사용자가 비상상황 발생시 복수개의 긴급버튼 감압에 의해 기 설정된 보호자단말기로 비상정보를 송출하는 경우, 스마트폰 식별번호와 대응하는 직불카드 또는 체크카드와 연동된 은행계좌를 기 설정된 가상의 은행계좌로 전환하여 오프라인뱅킹 서비스를 제공함으로써, 스마트폰 사용자의 현금인출에 따른 2차 피해를 미연에 방지함에 그 목적이 있다.

[15] 그리고, 본 발명은 스마트폰 사용자가 비상상황 발생시 복수개의 긴급버튼 감압에 의해 기 설정된 보호자단말기로 비상정보를 송출하는 경우, 스마트폰 사용자의 신용카드정보를 분실카드로 등록함으로써, 스마트폰 사용자의 신용카드 결제 및 카드론 대출에 따른 2차 피해를 미연에 방지함에 그 목적이 있다.

과제 해결 수단

[16] 이러한 기술적 과제를 달성하기 위한 본 발명의 스마트폰을 이용한 긴급호출 오남용 방지 시스템은, 복수개의 긴급버튼 감압에 의해 생성한 긴급구조 요청정보 및 금융서비스 정지요청정보를 이통사서버(200)로 전송하고, 인터넷뱅킹 어플리케이션이 실행되는 경우, 인터넷뱅킹 접속을 위한 URL을 기 설정된 가상 접속 URL로 전환하여 가상의 인터넷뱅킹 URL 페이지에서 인터넷뱅킹 업무를 수행하도록 제어하는 스마트폰(100); 스마트폰(100)으로부터 긴급구조 요청정보 및 금융서비스 정지요청정보를 수신하여 생성한 인증번호를 금융서비스 정지요청정보와 함께 보호자단말기(300)로 전송하고, 보호자단말기(300)로부터 인증회신번호를 수신하여 GPS위성과 접속하여 수신한 스마트폰의 위치좌표 및 긴급구조 요청정보를 기관서버(400)로 전송하며, 보호자단말기(300)로부터 수신한 호접속 요청신호에 따라 스마트폰(100)과 보호자단말기(300)와의 전화통화 연결을 제어하는 이통사서버(200); 이통사서버(200)로부터 긴급구조 요청정보, 금융서비스 정지요청정보 및 인증번호를 수신하여 보호자의 조작을 통해 입력받은 인증회신번호를 이통사서버(200)로 전송하고, 긴급구조 요청정보 및 금융서비스 정지요청정보를 기관서버(400)로 전송하며, 스마트폰(100) 및 기관서버(400)와의 3자 통화연결을 위한 호접속 요청신호를 이통사서버(200)로 전송하는 보호자단말기(300); 및 이통사서버(200)로부터 스마트폰의 위치좌표

및 긴급구조 요청정보를 수신하고, 스마트폰 사용자의 구조를 위해 생성한 출동정보를 스마트폰의 위치좌표 반경에 위치한 경찰서 또는 소방서로 전송하고, 보호자단말기(300)로부터 수신한 금융서비스 정지요청정보에 포함된 계좌번호에 대한 금융서비스가 가상계좌를 통해 수행되도록 하는 은행거래 중지정보를 생성하여 긴급구조 요청정보와 함께 은행서버(500)로 전송하며, 보호자단말기(300)로부터 수신한 신용카드 식별번호에 대한 신용카드 도난정보를 생성하여 카드사서버(600)로 전송하는 기관서버(400);를 포함한다.

[17]

[18] 그리고, 전술한 바와 같은 시스템을 기반으로 하는 본 발명의 스마트폰을 이용한 긴급호출 오남용 방지 방법은, 스마트폰(100)이 복수개의 긴급버튼 감압에 의해 입력받은 긴급구조 요청정보 및 금융서비스 정지요청정보를 이통사서버(200)로 전송하는 (a) 단계; 이통사서버(200)가 긴급구조 요청정보를 수신하여 생성한 인증번호 및 금융서비스 정지요청정보를 긴급구조 요청정보에 포함된 보호자단말기(300)로 전송하는 (b) 단계; 이통사서버(200)가 보호자단말기(300)로부터 수신한 인증회신번호와 인증번호가 서로 대응하는 경우, GPS위성과 접속된 스마트폰의 위치좌표 및 긴급구조 요청정보를 기관서버(400)로 전송하는 (c) 단계; 기관서버(400)가 출동정보를 스마트폰의 위치좌표 반경에 위치한 경찰서 또는 소방서로 전송하는 (d) 단계; 보호자단말기(300)가 이통사서버(200)로부터 수신한 금융서비스 정지요청정보를 기관서버(400)로 전송하는 (e) 단계; 기관서버(400)가 보호자단말기(300)로부터 수신한 금융서비스 정지요청정보와 대응하는 은행거래 중지정보를 생성하여 긴급구조 요청정보와 함께 은행서버(500)로 전송하고, 보호자단말기(300)로부터 수신한 신용카드 식별번호에 대한 신용카드 도난정보를 생성하여 카드사서버(600)로 전송하는 (f) 단계; 은행서버(500)가 긴급구조 요청정보에 포함된 스마트폰 식별번호와 대응하는 बैं킹서비스를 감지하는 경우, 감지된 बैं킹서비스가 오프라인뱅크 서비스인지 온라인뱅크 서비스인지 여부를 판단하는 (g) 단계; (g) 단계의 판단결과, 은행서버(500)가 오프라인뱅크 서비스 이용을 감지하는 경우, 스마트폰 식별번호와 대응하는 은행계좌를 기 설정된 가상의 은행계좌로 전환하여 오프라인뱅크 서비스를 수행하도록 제어하는 (h) 단계; 카드사서버(600)가 기관서버(400)로부터 신용카드 도난정보를 수신하여 신용카드 도난정보에 포함된 신용카드 식별번호를 도난카드로 등록하는 (i) 단계; 및 신용카드 식별번호에 대응하는 신용카드 결제요청정보를 POS단말기 또는 인터넷 쇼핑몰서버로부터 수신하는 경우, 카드사서버(600)가 도난카드 결제불허정보를 POS단말기 또는 인터넷 쇼핑몰서버로 전송하는 (j) 단계;를 포함한다.

발명의 효과

[19] 상기와 같은 본 발명에 따르면, 복수개의 긴급버튼 감압에 의해 기 설정된

보호자단말기로 비상정보를 송출하는 경우, 보호자단말기가 비상상황여부에 대한 인증을 수행하여 스마트폰 사용자의 비상상황을 기관서버로 전송하고, 기관서버의 경찰관이 이동통신사로부터 수신한 스마트폰 사용자의 위치좌표로 출동함으로써, 스마트폰 사용자의 비상상황 발생 시 경찰서 또는 소방서를 포함하는 기관의 비상상황에 대한 대응을 최단시간에 수행토록 하는 효과가 있다.

[20] 또한, 본 발명에 따르면, 스마트폰 사용자가 비상상황 발생시 복수개의 긴급버튼 감압에 의해 기 설정된 보호자단말기로 비상정보를 송출하는 경우, 스마트폰 사용자의 인터넷뱅킹 계좌를 기 설정된 가상의 인터넷뱅킹 계좌로 전환시켜 가상의 인터넷뱅킹 업무를 제공함으로써, 스마트폰 사용자의 인터넷뱅킹 계좌이체에 따른 2차 피해를 미연에 방지하는 효과가 있다.

[21] 또한, 본 발명에 따르면, 스마트폰 사용자가 비상상황 발생시 복수개의 긴급버튼 감압에 의해 기 설정된 보호자단말기로 비상정보를 송출하는 경우, 스마트폰 식별번호와 대응하는 직불카드 또는 체크카드와 연동된 은행계좌를 기 설정된 가상의 은행계좌로 전환하여 오프라인뱅킹 서비스를 제공함으로써, 스마트폰 사용자의 현금인출에 따른 2차 피해를 미연에 방지하는 효과가 있다.

[22] 그리고, 본 발명에 따르면, 스마트폰 사용자가 비상상황 발생시 복수개의 긴급버튼 감압에 의해 기 설정된 보호자단말기로 비상정보를 송출하는 경우, 스마트폰 사용자의 신용카드정보를 분실카드로 등록함으로써, 스마트폰 사용자의 신용카드 결제 및 카드론 대출에 따른 2차 피해를 미연에 방지하는 효과가 있다.

도면의 간단한 설명

[23] 도 1은 종래의 이동통신망을 이용한 긴급콜 오남용 방지 시스템 및 방법을 도시한 구성도.

[24] 도 2는 본 발명에 따른 스마트폰을 이용한 긴급호출 오남용 방지 시스템을 도시한 구성도.

[25] 도 3은 본 발명에 따른 스마트폰을 이용한 긴급호출 오남용 방지 시스템의 스마트폰을 도시한 구성도.

[26] 도 4는 본 발명에 따른 스마트폰을 이용한 긴급호출 오남용 방지 시스템의 이통사서버를 도시한 구성도.

[27] 도 5는 본 발명에 따른 스마트폰을 이용한 긴급호출 오남용 방지 시스템의 보호자단말기를 도시한 구성도.

[28] 도 6은 본 발명에 따른 스마트폰을 이용한 긴급호출 오남용 방지 시스템의 기관서버를 도시한 구성도.

[29] 도 7은 본 발명에 따른 스마트폰을 이용한 긴급호출 오남용 방지 시스템의 은행서버를 도시한 구성도.

[30] 도 8은 본 발명에 따른 스마트폰을 이용한 긴급호출 오남용 방지 시스템의

카드사서버를 도시한 구성도.

- [31] 도 9는 본 발명에 따른 스마트폰을 이용한 긴급호출 오남용 방지 방법을 도시한 순서도.
- [32] 도 10은 본 발명에 따른 스마트폰을 이용한 긴급호출 오남용 방지 방법의 제S110단계를 도시한 순서도.
- [33] 도 11은 본 발명에 따른 스마트폰을 이용한 긴급호출 오남용 방지 방법의 제S30단계의 세부과정을 도시한 순서도.
- [34] 도 12는 본 발명에 따른 스마트폰을 이용한 긴급호출 오남용 방지 방법의 제S50단계 이후 과정을 도시한 순서도.
- [35] [부호의 설명]
- [36] S: 스마트폰을 이용한 긴급호출 오남용 방지 시스템
- [37] 100: 스마트폰 110: 긴급호출 감지모듈
- [38] 120: 어플리케이션 제어모듈 130: 통화연결모듈
- [39] 200: 이통사서버 210: 인증번호 생성모듈
- [40] 220: 인증번호 매칭모듈 230: GPS위성 연결모듈
- [41] 240: 전화통화 중개모듈 300: 보호자단말기
- [42] 310: 긴급정보 확인모듈 320: 긴급정보 전송모듈
- [43] 330: 긴급전화 연결모듈 400: 기관서버
- [44] 500: 은행서버 510: 뱅킹서비스 감지모듈
- [45] 520: 오프라인뱅킹 전환모듈 530: 온라인뱅킹 전환모듈
- [46] 600: 카드사서버

발명의 실시를 위한 최선의 형태

- [47] 본 발명의 구체적인 특징 및 이점들은 첨부도면에 의거한 다음의 상세한 설명으로 더욱 명백해질 것이다. 이에 앞서, 본 명세서 및 청구범위에 사용된 용어나 단어는 발명자가 그 자신의 발명을 가장 최선의 방법으로 설명하기 위해 용어의 개념을 적절하게 정의할 수 있다는 원칙에 입각하여 본 발명의 기술적 사상에 부합하는 의미와 개념으로 해석되어야 할 것이다. 또한, 본 발명에 관련된 공지 기능 및 그 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는, 그 구체적인 설명을 생략하였음에 유의해야 할 것이다.
- [48] 도 2에 도시된 바와 같이 본 발명에 따른 스마트폰을 이용한 긴급호출 오남용 방지 시스템(S)은 스마트폰(100), 이통사서버(200), 보호자단말기(300), 기관서버(400), 은행서버(500) 및 카드사서버(600)를 포함하여 구성된다.
- [49] 이하에서는 그 언급을 생략하겠으나, 본 발명에 따른 스마트폰(100), 이통사서버(200), 보호자단말기(300), 기관서버(400) 및 은행서버(500) 간의 정보 송수신은 정보통신망을 통해 수행되며, 정보통신망은 무선인터넷(3G망/4G망) 또는 와이파이(Wireless Fidelity) 중에 어느 하나의 통신에 의해 데이터 송수신이

가능한 무선망을 총칭한 것으로 이해함이 바람직하다.

- [50] 먼저, 스마트폰(100)은 복수개의 긴급버튼 감압에 의해 생성한 긴급구조 요청정보 및 금융서비스 정지요청정보를 이통사서버(200)로 전송하고, 인터넷뱅킹 어플리케이션이 실행되는 경우, 인터넷뱅킹 접속을 위한 URL을 기 설정된 가상 접속 URL로 전환하여 가상의 인터넷뱅킹 URL 페이지에서 인터넷뱅킹 업무를 수행하도록 제어하되, 긴급호출 감지모듈(110), 어플리케이션 제어모듈(120) 및 통화연결모듈(130)을 포함하여 구성된다.
- [51] 여기서, 본 발명에 따른 스마트폰(100)은 전화통화 및 인터넷접속이 가능한 인터넷폰 또는 태블릿PC(Tablet PC)를 포함하는 통신기기로 이해함이 바람직하다.
- [52] 구체적으로, 도 3을 참조하여 본 발명에 따른 스마트폰 인증을 이용한 긴급콜 서비스와 온오프라인뱅킹 보안 시스템(S)의 스마트폰(100)에 대해 살펴보면 아래와 같다.
- [53] 스마트폰(100)의 긴급호출 감지모듈(110)은 복수개의 긴급버튼 감압에 의해 입력받은 신호를 감지하여 스마트폰 식별번호 및 기 설정된 보호자단말기 식별번호를 포함하도록 생성한 긴급구조 요청정보와, 저장소에 기 저장된 계좌번호 및 신용카드 식별번호를 포함하는 금융서비스 정지요청정보를 정보통신망을 통해 접속된 이통사서버(200)로 전송한다.
- [54] 이때, 긴급호출 감지모듈(110)은 기 설정된 시간동안 스마트폰에 구비된 볼륨버튼 및 전원버튼에 대한 감압이 지속되는 경우, 긴급한 상황으로 판단하여 긴급구조 요청정보 및 금융서비스 정지요청정보를 생성하도록 구성되나, 본 발명이 이에 국한되는 것은 아니며, 특정 버튼에 대한 감압에 종속되지 아니하고, 기 설정된 시간동안 복수개의 버튼에 대한 감압이 이루어지는 경우, 긴급구조 요청정보 및 금융서비스 정지요청정보를 생성하는 것으로 이해함이 바람직하다.
- [55] 또한, 어플리케이션 제어모듈(120)은 긴급호출 감지모듈(110)로부터 긴급구조 요청정보를 인가받은 이후, 기 설치된 인터넷뱅킹 어플리케이션이 실행되는 경우, 인터넷뱅킹 접속을 위한 URL을 기 설정된 가상 접속 URL로 전환하여 가상의 인터넷뱅킹 URL 페이지에서 인터넷뱅킹 업무를 수행하도록 제어한다.
- [56] 그리고, 통화연결모듈(130)은 긴급호출 감지모듈(110)로부터 긴급구조 요청정보를 인가받은 이후, 이통사서버(200)로부터 수신한 호접속 요청신호를 감지하여 보호자단말기(300)와의 전화통화를 연결한다.
- [57] 또한, 통화연결모듈(130)은 호접속 요청신호 감지시 벨소리 출력 또는 진동이 발생하지 않도록 제어하며, 통화연결을 위한 별도의 키 입력 없이 호접속 요청신호 감지와 동시에 보호자단말기(300)와의 전화통화를 연결하도록 내장된 스피커 및 마이크를 제어한다.
- [58] 이때, 통화연결모듈(130)은 스피커를 통한 보호자단말기(300)로부터의 음성출력을 억제하며, 마이크로 입력되는 음성을 호접속이 연결된

보호자단말기(300)로 전송하도록 제어한다.

[59]

[60] 한편, 도 4를 참조하여 본 발명에 따른 스마트폰을 이용한 긴급호출 오남용 방지 시스템(S)의 이통사서버(200)에 대해 살펴보면 아래와 같다.

[61] 이통사서버(200)는 정보통신망을 통해 접속된 스마트폰(100)으로부터 긴급구조 요청정보 및 금융서비스 정지요청정보를 수신하여 생성한 인증번호를 금융서비스 정지요청정보와 함께 보호자단말기(300)로 전송하고, 보호자단말기(300)로부터 인증회신번호를 수신하여 GPS위성과 접속하여 수신한 스마트폰의 위치좌표 및 긴급구조 요청정보를 기관서버(400)로 전송하며, 보호자단말기(300)로부터 수신한 호접속 요청신호에 따라 스마트폰(100)과 보호자단말기(300)와의 전화통화 연결을 제어하되, 인증번호 생성모듈(210), 인증번호 매칭모듈(220), GPS위성 연결모듈(230) 및 전화통화 중개모듈(240)을 포함하여 구성된다.

[62] 구체적으로, 이통사서버(200)의 인증번호 생성모듈(210)은 정보통신망을 통해 접속된 스마트폰(100)으로부터 수신한 긴급구조 요청정보로부터 보호자단말기 식별번호를 추출하고, 난수발생기를 통해 임의로 생성한 인증번호를 SMS형태로 변환하여 긴급구조 요청정보 및 금융서비스 정지요청정보와 함께 보호자단말기(300)로 전송한다.

[63] 또한, 인증번호 매칭모듈(220)은 보호자단말기(300)로부터 수신한 인증회신번호와 인증번호 생성모듈(210)로부터 인가받은 인증번호가 서로 대응하는 경우, 인증완료정보를 생성한다.

[64] 또한, GPS위성 연결모듈(230)은 인증번호 매칭모듈(220)로부터 인증완료정보를 인가받아 GPS위성과 접속된 스마트폰의 위치좌표 및 긴급구조 요청정보를 기관서버(400)로 전송한다.

[65] 그리고, 전화통화 중개모듈(240)은 보호자단말기(300)로부터 스마트폰(100)과의 호접속 요청신호를 수신하는 경우, 스마트폰(100)과 보호자단말기(300)와의 전화통화 연결을 중개한다.

[66]

[67] 한편, 도 5를 참조하여 본 발명에 따른 스마트폰을 이용한 긴급호출 오남용 방지 시스템(S)의 보호자단말기(300)에 대해 살펴보면 아래와 같다.

[68] 보호자단말기(300)는 이통사서버(200)로부터 긴급구조 요청정보, 금융서비스 정지요청정보 및 인증번호를 수신하여 보호자의 조작을 통해 입력받은 인증회신번호를 이통사서버(200)로 전송하고, 긴급구조 요청정보 및 금융서비스 정지요청정보를 기관서버(400)로 전송하며, 스마트폰(100) 및 기관서버(400)와의 3자 통화연결을 위한 호접속 요청신호를 이통사서버(200)로 전송하되, 긴급정보 확인모듈(310), 긴급정보 전송모듈(320) 및 긴급전화 연결모듈(330)을 포함하여 구성된다.

[69] 구체적으로, 보호자단말기(300)의 긴급정보 확인모듈(310)은 정보통신망을

통해 접속된 이통사서버(200)로부터 긴급구조 요청정보, 금융서비스 정지요청정보 및 인증번호를 수신하고, 보호자의 조작을 통해 입력받은 인증회신번호를 이통사서버(200)로 전송한다.

[70] 또한, 긴급정보 전송모듈(320)은 기 설치된 긴급구조 어플리케이션의 실행에 따라 긴급정보 확인모듈(310)로부터 인가받은 긴급구조 요청정보 및 금융서비스 정지요청정보를 정보통신망을 통해 접속된 기관서버(400)로 전송한다.

[71] 그리고, 긴급전화 연결모듈(330)은 긴급정보 확인모듈(310)로부터 인가받은 긴급구조 요청정보와 대응하는 스마트폰(100) 및 기관서버(400)와의 3자 통화 연결을 위한 호접속 요청신호를 이통사서버(200)로 전송하여 스마트폰(100) 및 기관서버(400)와의 전화통화를 제어한다.

[72]

[73] 한편, 도 6을 참조하여 본 발명에 따른 스마트폰을 이용한 긴급호출 오남용 방지 시스템(S)의 기관서버(400)에 대해 살펴보면 아래와 같다.

[74] 기관서버(400)는 정보통신망을 통해 접속된 이통사서버(200)로부터 스마트폰의 위치좌표 및 긴급구조 요청정보를 수신하고, 스마트폰 사용자의 구조를 위해 생성한 출동정보를 스마트폰의 위치좌표 반경에 위치한 경찰서 또는 소방서로 전송하고, 보호자단말기(300)로부터 수신한 금융서비스 정지요청정보에 포함된 계좌번호에 대한 금융서비스가 가상계좌를 통해 수행되도록 하는 은행거래 중지정보를 생성하여 긴급구조 요청정보와 함께 은행서버(500)로 전송하며, 보호자단말기(300)로부터 수신한 신용카드 식별번호에 대한 신용카드 도난정보를 생성하여 카드사서버(600)로 전송한다.

[75]

[76] 또한, 도 7을 참조하여 본 발명에 따른 스마트폰을 이용한 긴급호출 오남용 방지 시스템(S)의 은행서버(500)에 대해 살펴보면 아래와 같다.

[77] 은행서버(500)는 정보통신망을 통해 접속된 기관서버(400)로부터 긴급구조 요청정보 및 은행거래 중지정보를 수신하고, 긴급구조 요청정보에 포함된 스마트폰 식별번호와 대응하는 은행계좌와 연동된 직불카드 또는 체크카드 중에 어느 하나를 포함하는 오프라인뱅킹 서비스 이용을 감지하는 경우, 스마트폰 식별번호와 대응하는 은행계좌를 기 설정된 가상의 은행계좌로 전환하여 오프라인뱅킹 서비스를 수행하도록 제어한다.

[78] 또한, 은행서버(500)는 정보통신망을 통해 접속된 기관서버(400)로부터 긴급구조 요청정보 및 은행거래 중지정보를 수신하고, 긴급구조 요청정보에 포함된 스마트폰 식별번호와 대응하는 인터넷뱅킹 서비스 이용을 감지하는 경우, 상기 스마트폰(100)이 인터넷뱅킹 접속을 위한 URL을 기 설정된 가상 접속 URL로 전환하여 가상의 인터넷뱅킹 URL 페이지에서 인터넷뱅킹 서비스를 수행하도록 제어한다.

[79] 구체적으로, 은행서버(500)의 뱅킹서비스 감지모듈(510)은 기관서버(400)로부터 긴급구조 요청정보 및 은행거래 중지정보를 수신한 이후,

은행에 구비된 ATM기로부터 스마트폰 식별번호와 대응하는 은행계좌와 연동된 직불카드 또는 체크카드 접속신호를 수신하는 경우, 오프라인 은행거래 감지정보를 생성하고, 정보통신망을 통해 스마트폰 식별번호와 대응하는 인터넷뱅킹 서비스 이용을 감지하는 경우, 온라인 은행거래 감지정보를 생성한다.

- [80] 또한, 오프라인뱅킹 전환모듈(520)은 뱅킹서비스 감지모듈(510)로부터 오프라인 은행거래 감지정보를 인가받는 경우, 스마트폰 식별번호와 대응하는 은행계좌를 기 설정된 가상의 은행계좌로 전환하는 가상계좌 전환정보를 ATM기로 전송하여 ATM기가 가상계좌 환경에서 오프라인뱅킹 서비스를 수행하도록 제어한다.
- [81] 여기서, 가상의 은행계좌는 스마트폰(100) 사용자의 요청에 따라 기 생성되는 계좌로, 가상의 은행계좌 생성 시에 잔액을 '0원'으로 설정한 경우, 스마트폰 식별번호와 대응하는 은행계좌에서 현금이 인출되지 않도록 한다.
- [82] 그리고, 온라인뱅킹 전환모듈(530)은 뱅킹서비스 감지모듈(510)로부터 온라인 은행거래 감지정보를 인가받는 경우, 스마트폰(100)과 접속되는 인터넷뱅킹 URL을 기 설정된 가상의 인터넷뱅킹 URL로 전환하여 가상의 인터넷뱅킹 URL 페이지에서 인터넷뱅킹 서비스를 수행하도록 제어한다.
- [83] 여기서, 가상의 인터넷뱅킹 URL로의 전환은, 스마트폰(100)의 인터넷뱅킹 어플리케이션 구동에 따라 무선인터넷을 통해 인터넷뱅킹에 접속하는 경우, 스마트폰(100)이 본래의 인터넷뱅킹과 동일한 인터넷뱅킹 환경을 갖는 URL 페이지로 이동하여 인터넷뱅킹 서비스를 수행하도록 제어한다.
- [84] 이때, 스마트폰(100)이 계좌이체업무를 수행하는 경우, 스마트폰 식별번호와 대응하는 계좌에 예치된 금액에서 이체를 원하는 계좌로 이체요청금액을 이체하도록 제어하되, 인터넷뱅킹 서비스가 스마트폰 식별번호와 대응하는 가상계좌에서 수행됨에 따라 이체를 원하는 계좌에는 실제로 이체요청금액이 이체되지 않으나, 스마트폰(100)에 디스플레이되는 화면에는 이체요청금액이 이체를 원하는 계좌에 이체되는 것으로 디스플레이 된다.
- [85]
- [86] 그리고, 도 8을 참조하여 본 발명에 따른 스마트폰을 이용한 긴급호출 오남용 방지 시스템(S)의 카드사서버(600)에 대해 살펴보면 아래와 같다.
- [87] 카드사서버(600)는 정보통신망을 통해 접속된 기관서버(400)로부터 신용카드 도난정보를 수신하여 신용카드 도난정보에 포함된 신용카드 식별번호를 도난카드로 등록하고, 상기 신용카드 식별번호에 대응하는 신용카드 결제요청정보를 POS단말기 또는 인터넷 쇼핑몰서버로부터 수신하는 경우, 도난카드 결제불허정보를 상기 POS단말기 또는 인터넷 쇼핑몰서버로 전송한다.
- [88]
- [89] 이하, 도 9를 참조하여 본 발명에 따른 스마트폰을 이용한 긴급호출 오남용 방지 방법에 대해 살펴보면 아래와 같다.

- [90] 먼저, 스마트폰(100)이 복수개의 긴급버튼 감압에 의해 입력받은 긴급구조 요청정보 및 금융서비스 정지요청정보를 이통사서버(200)로 전송한다(S10).
- [91] 이어서, 이통사서버(200)가 긴급구조 요청정보를 수신하여 생성한 인증번호 및 금융서비스 정지요청정보를 긴급구조 요청정보에 포함된 보호자단말기(300)로 전송한다(S20).
- [92] 뒤이어, 이통사서버(200)가 보호자단말기(300)로부터 수신한 인증회신번호와 인증번호가 서로 대응하는 경우, GPS위성과 접속된 스마트폰의 위치좌표 및 긴급구조 요청정보를 기관서버(400)로 전송한다(S30).
- [93] 이어서, 기관서버(400)가 출동정보를 스마트폰의 위치좌표 반경에 위치한 경찰서 또는 소방서로 전송한다(S40).
- [94] 뒤이어, 보호자단말기(300)가 이통사서버(200)로부터 수신한 금융서비스 정지요청정보를 기관서버(400)로 전송한다(S50).
- [95] 이어서, 기관서버(400)가 보호자단말기(300)로부터 수신한 금융서비스 정지요청정보와 대응하는 은행거래 중지정보를 생성하여 긴급구조 요청정보와 함께 은행서버(500)로 전송하고, 보호자단말기(300)로부터 수신한 신용카드 식별번호에 대한 신용카드 도난정보를 생성하여 카드사서버(600)로 전송한다(S60).
- [96] 뒤이어, 은행서버(500)가 긴급구조 요청정보에 포함된 스마트폰 식별번호와 대응하는 뱅킹서비스를 감지하는 경우, 감지된 뱅킹서비스가 오프라인뱅킹 서비스인지 온라인뱅킹 서비스인지 여부를 판단한다(S70).
- [97] 제S70단계의 판단결과, 은행서버(500)가 오프라인뱅킹 서비스 이용을 감지하는 경우, 스마트폰 식별번호와 대응하는 은행계좌를 기 설정된 가상의 은행계좌로 전환하여 오프라인뱅킹 서비스를 수행하도록 제어한다(S80).
- [98] 뒤이어, 카드사서버(600)가 기관서버(400)로부터 신용카드 도난정보를 수신하여 신용카드 도난정보에 포함된 신용카드 식별번호를 도난카드로 등록한다(S90).
- [99] 그리고, 신용카드 식별번호에 대응하는 신용카드 결제요청정보를 POS단말기 또는 인터넷 쇼핑몰서버로부터 수신하는 경우, 카드사서버(600)가 도난카드 결제불허정보를 상기 POS단말기 또는 인터넷 쇼핑몰서버로 전송한다(S100).
- [100] 한편, 도 10에 도시된 바와 같이 상기 제S70단계의 판단결과, 은행서버(500)가 온라인뱅킹 서비스 이용을 감지하는 경우, 스마트폰(100)이 인터넷뱅킹 접속을 위한 URL을 기 설정된 가상 접속 URL로 전환하여 가상의 인터넷뱅킹 URL 페이지에서 인터넷뱅킹 서비스를 수행하도록 제어한다(S110).
- [101]
- [102] 한편, 도 11을 참조하여 본 발명에 따른 스마트폰을 이용한 긴급호출 오남용 방지 방법의 제S30단계의 세부과정을 살펴보면 아래와 같다.
- [103] 제S20단계 이후, 이통사서버(200)가 생성한 인증번호와 보호자단말기(300)로부터 수신한 인증회신번호가 서로 대응하는 경우,

인증완료정보를 생성한다(S31).

- [104] 그리고, 이동사서버(200)가 인증완료정보 생성에 따라 GPS위성과 접속하여 수신한 스마트폰의 위치좌표 및 긴급구조 요청정보를 기관서버(400)로 전송하고, 제S40단계로 절차를 이행한다(S32).

[105]

- [106] 또한, 도 12를 참조하여 본 발명에 따른 스마트폰을 이용한 긴급호출 오남용 방지 방법의 제S50단계 이후 과정을 살펴보면 아래와 같다.

- [107] 제S50단계 이후, 보호자단말기(300)가 스마트폰(100) 및 기관서버(400)와의 3자 통화연결을 위한 호접속 요청신호를 이동사서버(200)로 전송한다(S120).

- [108] 이어서, 이동사서버(200)가 보호자단말기(300)로부터 스마트폰(100)과의 호접속 요청신호를 수신하여 스마트폰(100)으로 전송한다(S130).

- [109] 뒤이어, 스마트폰(100)이 이동사서버(200)로부터 호접속 요청신호를 수신하여 벨소리 출력 또는 진동이 발생하지 않도록 제어하며, 보호자단말기(300)와의 전화통화를 연결한다(S140).

- [110] 그리고, 스마트폰(100)이 스피커를 통해 호접속이 연결된 보호자단말기(300)로부터의 음성출력을 억제하며, 마이크로 입력되는 음성을 호접속이 연결된 보호자단말기(300)로 전송하도록 제어하고 제S60단계로 절차를 이행한다(S150).

- [111] 이상으로 본 발명의 기술적 사상을 예시하기 위한 바람직한 실시예와 관련하여 설명하고 도시하였지만, 본 발명은 이와 같이 도시되고 설명된 그대로의 구성 및 작용에만 국한되는 것이 아니며, 기술적 사상의 범주를 일탈함이 없이 본 발명에 대해 다수의 변경 및 수정이 가능함을 당업자들은 잘 이해할 수 있을 것이다. 따라서 그러한 모든 적절한 변경 및 수정과 균등물들도 본 발명의 범위에 속하는 것으로 간주되어야 할 것이다.

청구범위

[청구항 1]

스마트폰을 이용한 긴급호출 오남용 방지 시스템에 있어서, 복수개의 긴급버튼 감압에 의해 생성한 긴급구조 요청정보 및 금융서비스 정지요청정보를 이통사서버(200)로 전송하고, 인터넷뱅킹 어플리케이션이 실행되는 경우, 인터넷뱅킹 접속을 위한 URL을 기 설정된 가상 접속 URL로 전환하여 가상의 인터넷뱅킹 URL 페이지에서 인터넷뱅킹 업무를 수행하도록 제어하는 스마트폰(100);

상기 스마트폰(100)으로부터 긴급구조 요청정보 및 금융서비스 정지요청정보를 수신하여 생성한 인증번호를 금융서비스 정지요청정보와 함께 보호자단말기(300)로 전송하고, 상기 보호자단말기(300)로부터 인증회신번호를 수신하여 GPS위성과 접속하여 수신한 스마트폰의 위치좌표 및 긴급구조 요청정보를 기관서버(400)로 전송하며, 상기 보호자단말기(300)로부터 수신한 호접속 요청신호에 따라 스마트폰(100)과 보호자단말기(300)와의 전화통화 연결을 제어하는 이통사서버(200);

상기 이통사서버(200)로부터 긴급구조 요청정보, 금융서비스 정지요청정보 및 인증번호를 수신하여 보호자의 조작을 통해 입력받은 인증회신번호를 이통사서버(200)로 전송하고, 상기 긴급구조 요청정보 및 금융서비스 정지요청정보를

기관서버(400)로 전송하며, 상기 스마트폰(100) 및 기관서버(400)와의 3자 통화연결을 위한 호접속 요청신호를 이통사서버(200)로 전송하는 보호자단말기(300); 및

상기 이통사서버(200)로부터 스마트폰의 위치좌표 및 긴급구조 요청정보를 수신하고, 스마트폰 사용자의 구조를 위해 생성한 출동정보를 스마트폰의 위치좌표 반경에 위치한 경찰서 또는 소방서로 전송하고, 상기 보호자단말기(300)로부터 수신한 금융서비스 정지요청정보에 포함된 계좌번호에 대한

금융서비스가 가상계좌를 통해 수행되도록 하는 은행거래 중지정보를 생성하여 상기 긴급구조 요청정보와 함께

은행서버(500)로 전송하며, 상기 보호자단말기(300)로부터 수신한 신용카드 식별번호에 대한 신용카드 도난정보를 생성하여 카드사서버(600)로 전송하는 기관서버(400);를 포함하는 것을 특징으로 하는 스마트폰을 이용한 긴급호출 오남용 방지 시스템.

[청구항 2]

제 1 항에 있어서,

상기 기관서버(400)로부터 긴급구조 요청정보 및 은행거래 중지정보를 수신하고, 긴급구조 요청정보에 포함된 스마트폰

식별번호와 대응하는 은행계좌와 연동된 직불카드 또는 체크카드 중에 어느 하나를 포함하는 오프라인뱅킹 서비스 이용을 감지하는 경우, 스마트폰 식별번호와 대응하는 은행계좌를 기 설정된 가상의 은행계좌로 전환하여 오프라인뱅킹 서비스를 수행하도록 제어하고, 상기 기관서버(400)로부터 긴급구조 요청정보 및 은행거래 중지정보를 수신하고, 긴급구조 요청정보에 포함된 스마트폰 식별번호와 대응하는 인터넷뱅킹 서비스 이용을 감지하는 경우, 상기 스마트폰(100)이 인터넷뱅킹 접속을 위한 URL을 기 설정된 가상 접속 URL로 전환하여 가상의 인터넷뱅킹 URL 페이지에서 인터넷뱅킹 서비스를 수행하도록 제어하는 은행서버(500); 및

상기 기관서버(400)로부터 신용카드 도난정보를 수신하여 신용카드 도난정보에 포함된 신용카드 식별번호를 도난카드로 등록하고, 상기 신용카드 식별번호에 대응하는 신용카드 결제요청정보를 POS단말기 또는 인터넷 쇼핑몰서버로부터 수신하는 경우, 도난카드 결제불허정보를 상기 POS단말기 또는 인터넷 쇼핑몰서버로 전송하는 카드사서버(600);를 더 포함하는 것을 특징으로 하는 스마트폰을 이용한 긴급호출 오남용 방지 시스템.

[청구항 3]

제 1 항에 있어서,
상기 스마트폰(100)은,
복수개의 긴급버튼 감압에 의해 입력받은 신호를 감지하여 스마트폰 식별번호 및 기 설정된 보호자단말기 식별번호를 포함하도록 생성한 긴급구조 요청정보와, 저장소에 기 저장된 계좌번호 및 신용카드 식별번호를 포함하는 금융서비스 정지요청정보를 정보통신망을 통해 접속된 이통사서버(200)로 전송하는 긴급호출 감지모듈(110);
상기 긴급호출 감지모듈(110)로부터 긴급구조 요청정보를 인가받은 이후, 기 설치된 인터넷뱅킹 어플리케이션이 실행되는 경우, 인터넷뱅킹 접속을 위한 URL을 기 설정된 가상 접속 URL로 전환하여 가상의 인터넷뱅킹 URL 페이지에서 인터넷뱅킹 업무를 수행하도록 제어하는 어플리케이션 제어모듈(120); 및
상기 긴급호출 감지모듈(110)로부터 긴급구조 요청정보를 인가받은 이후, 이통사서버(200)로부터 수신한 호접속 요청신호를 감지하여 보호자단말기(300)와의 전화통화를 연결하되, 상기 호접속 요청신호 감지시 벨소리 출력 또는 진동이 발생하지 않도록 제어하며, 통화연결을 위한 별도의 키 입력 없이 호접속 요청신호 감지와 동시에 보호자단말기(300)와의 전화통화를

[청구항 4]

연결하도록 내장된 스피커 및 마이크를 제어하고, 스피커를 통한 보호자단말기(300)로부터의 음성출력을 억제하며, 마이크로 입력되는 음성을 호접속이 연결된 보호자단말기(300)로 전송하도록 제어하는 통화연결모듈(130);을 포함하는 것을 특징으로 하는 스마트폰을 이용한 긴급호출 오남용 방지 시스템.

제 1 항에 있어서,
 상기 이통사서버(200)는,
 상기 스마트폰(100)으로부터 수신한 긴급구조 요청정보로부터 보호자단말기 식별번호를 추출하고, 난수발생기를 통해 임의로 생성한 인증번호를 SMS형태로 변환하여 긴급구조 요청정보 및 금융서비스 정지요청정보와 함께 상기 보호자단말기(300)로 전송하는 인증번호 생성모듈(210);
 상기 보호자단말기(300)로부터 수신한 인증회신번호와 인증번호 생성모듈(210)로부터 인가받은 인증번호가 서로 대응하는 경우, 인증완료정보를 생성하는 인증번호 매칭모듈(220);
 상기 인증번호 매칭모듈(220)로부터 인증완료정보를 인가받아 GPS위성과 접속된 스마트폰의 위치좌표 및 긴급구조 요청정보를 상기 기관서버(400)로 전송하는 GPS위성 연결모듈(230); 및
 상기 보호자단말기(300)로부터 스마트폰(100)과의 호접속 요청신호를 수신하는 경우, 상기 스마트폰(100)과 보호자단말기(300)와의 전화통화 연결을 중개하는 전화통화 중개모듈(240);을 포함하는 것을 특징으로 하는 스마트폰을 이용한 긴급호출 오남용 방지 시스템.

[청구항 5]

제 1 항에 있어서,
 상기 보호자단말기(300)는,
 상기 이통사서버(200)로부터 긴급구조 요청정보, 금융서비스 정지요청정보 및 인증번호를 수신하고, 보호자의 조작을 통해 입력받은 인증회신번호를 상기 이통사서버(200)로 전송하는 긴급정보 확인모듈(310);
 기 설치된 긴급구조 어플리케이션의 실행에 따라 상기 긴급정보 확인모듈(310)로부터 인가받은 긴급구조 요청정보 및 금융서비스 정지요청정보를 상기 기관서버(400)로 전송하는 긴급정보 전송모듈(320); 및
 상기 긴급정보 확인모듈(310)로부터 인가받은 긴급구조 요청정보와 대응하는 스마트폰(100) 및 기관서버(400)와의 3자 통화 연결을 위한 호접속 요청신호를 상기 이통사서버(200)로 전송하여 상기 스마트폰(100) 및 기관서버(400)와의 전화통화를 제어하는 긴급전화 연결모듈(330);을 포함하는 것을 특징으로

[청구항 6]

하는 스마트폰을 이용한 긴급호출 오남용 방지 시스템.
 제 2 항에 있어서,
 상기 은행서버(500)는,
 상기 기관서버(400)로부터 긴급구조 요청정보 및 은행거래
 중지정보를 수신한 이후, 은행에 구비된 ATM기로부터 스마트폰
 식별번호와 대응하는 은행계좌와 연동된 직불카드 또는 체크카드
 접속신호를 수신하는 경우, 오프라인 은행거래 감지정보를
 생성하고, 정보통신망을 통해 스마트폰 식별번호와 대응하는
 인터넷뱅킹 서비스 이용을 감지하는 경우, 온라인 은행거래
 감지정보를 생성하는 뱅킹서비스 감지모듈(510);
 상기 뱅킹서비스 감지모듈(510)로부터 오프라인 은행거래
 감지정보를 인가받는 경우, 스마트폰 식별번호와 대응하는
 은행계좌를 기 설정된 가상의 은행계좌로 전환하는 가상계좌
 전환정보를 ATM기로 전송하여 ATM기가 가상계좌 환경에서
 오프라인뱅킹 서비스를 수행하도록 제어하는 오프라인뱅킹
 전환모듈(520); 및
 상기 뱅킹서비스 감지모듈(510)로부터 온라인 은행거래
 감지정보를 인가받는 경우, 상기 스마트폰(100)과 접속되는
 인터넷뱅킹 URL을 기 설정된 가상의 인터넷뱅킹 URL로 전환하여
 가상의 인터넷뱅킹 URL 페이지에서 인터넷뱅킹 서비스를
 수행하도록 제어하는 온라인뱅킹 전환모듈(530);을 포함하는 것을
 특징으로 하는 스마트폰을 이용한 긴급호출 오남용 방지 시스템.
 제 6 항에 있어서,
 상기 가상의 인터넷뱅킹 URL로의 전환은,
 상기 스마트폰(100)의 인터넷뱅킹 어플리케이션 구동에 따라
 무선인터넷을 통해 인터넷뱅킹에 접속하는 경우, 상기
 스마트폰(100)이 본래의 인터넷뱅킹과 동일한 인터넷뱅킹 환경을
 갖는 URL 페이지로 이동하여 인터넷뱅킹 서비스를 수행하도록
 제어하고,
 상기 스마트폰(100)이 계좌이체업무를 수행하는 경우, 스마트폰
 식별번호와 대응하는 계좌에 예치된 금액에서 이체를 원하는
 계좌로 이체요청금액을 이체하도록 제어하되, 인터넷뱅킹
 서비스가 스마트폰 식별번호와 대응하는 가상계좌에서 수행됨에
 따라 이체를 원하는 계좌에는 실제로 이체요청금액이 이체되지
 않으나, 상기 스마트폰(100)에 디스플레이되는 화면에는
 이체요청금액이 이체를 원하는 계좌에 이체되는 것으로
 디스플레이하도록 제어하는 것을 특징으로 하는 스마트폰을
 이용한 긴급호출 오남용 방지 시스템.

[청구항 7]

[청구항 8]

스마트폰을 이용한 긴급호출 오남용 방지 방법에 있어서,
 (a) 스마트폰(100)이 복수개의 긴급버튼 감압에 의해 입력받은
 긴급구조 요청정보 및 금융서비스 정지요청정보를
 이통사서버(200)로 전송하는 단계;
 (b) 이통사서버(200)가 긴급구조 요청정보를 수신하여 생성한
 인증번호 및 금융서비스 정지요청정보를 긴급구조 요청정보에
 포함된 보호자단말기(300)로 전송하는 단계;
 (c) 이통사서버(200)가 보호자단말기(300)로부터 수신한
 인증회신번호와 인증번호가 서로 대응하는 경우, GPS위성과
 접속된 스마트폰의 위치좌표 및 긴급구조 요청정보를
 기관서버(400)로 전송하는 단계;
 (d) 기관서버(400)가 출동정보를 스마트폰의 위치좌표 반경에
 위치한 경찰서 또는 소방서로 전송하는 단계;
 (e) 보호자단말기(300)가 이통사서버(200)로부터 수신한
 금융서비스 정지요청정보를 기관서버(400)로 전송하는 단계;
 (f) 기관서버(400)가 보호자단말기(300)로부터 수신한 금융서비스
 정지요청정보와 대응하는 은행거래 중지정보를 생성하여
 긴급구조 요청정보와 함께 은행서버(500)로 전송하고,
 보호자단말기(300)로부터 수신한 신용카드 식별번호에 대한
 신용카드 도난정보를 생성하여 카드사서버(600)로 전송하는 단계;
 (g) 은행서버(500)가 긴급구조 요청정보에 포함된 스마트폰
 식별번호와 대응하는 बैं킹서비스를 감지하는 경우, 감지된
 बैं킹서비스가 오프라인 बैं킹 서비스인지 온라인 बैं킹 서비스인지
 여부를 판단하는 단계;
 (h) 상기 (g) 단계의 판단결과, 은행서버(500)가 오프라인 बैं킹
 서비스 이용을 감지하는 경우, 스마트폰 식별번호와 대응하는
 은행계좌를 기 설정된 가상의 은행계좌로 전환하여 오프라인 बैं킹
 서비스를 수행하도록 제어하는 단계;
 (i) 카드사서버(600)가 기관서버(400)로부터 신용카드 도난정보를
 수신하여 신용카드 도난정보에 포함된 신용카드 식별번호를
 도난카드로 등록하는 단계; 및
 (j) 신용카드 식별번호에 대응하는 신용카드 결제요청정보를
 POS단말기 또는 인터넷 쇼핑몰서버로부터 수신하는 경우,
 카드사서버(600)가 도난카드 결제불허정보를 상기 POS단말기
 또는 인터넷 쇼핑몰서버로 전송하는 단계;를 포함하는 것을
 특징으로 하는 스마트폰을 이용한 긴급호출 오남용 방지 방법.
 제 8 항에 있어서,
 상기 (g) 단계의 판단결과,

[청구항 9]

(k) 상기 은행서버(500)가 온라인뱅킹 서비스 이용을 감지하는 경우, 상기 스마트폰(100)이 인터넷뱅킹 접속을 위한 URL을 기 설정된 가상 접속 URL로 전환하여 가상의 인터넷뱅킹 URL 페이지에서 인터넷뱅킹 서비스를 수행하도록 제어하는 단계;를 포함하는 것을 특징으로 하는 스마트폰을 이용한 긴급호출 오남용 방지 방법.

[청구항 10]

제 8 항에 있어서,

상기 (c) 단계는,

(c-1) 상기 이통사서버(200)가 생성한 인증번호와

보호자단말기로부터 수신한 인증회신번호가 서로 대응하는 경우, 인증완료정보를 생성하는 단계; 및

(c-2) 상기 이통사서버(200)가 인증완료정보 생성에 따라

GPS위성과 접속하여 수신한 스마트폰의 위치좌표 및 긴급구조 요청정보를 상기 기관서버(400)로 전송하는 단계;를 포함하는 것을 특징으로 하는 스마트폰을 이용한 긴급호출 오남용 방지 방법.

[청구항 11]

제 8 항에 있어서,

상기 (e) 단계 이후,

(l) 상기 보호자단말기(300)가 상기 스마트폰(100) 및

기관서버(400)와의 3자 통화연결을 위한 호접속 요청신호를 상기 이통사서버(200)로 전송하는 단계;

(m) 상기 이통사서버(200)가 보호자단말기(300)로부터

스마트폰(100)과의 호접속 요청신호를 수신하여 상기

스마트폰(100)으로 전송하는 단계;

(n) 상기 스마트폰(100)이 상기 이통사서버(200)로부터 호접속

요청신호를 수신하여 벨소리 출력 또는 진동이 발생하지 않도록 제어하며, 상기 보호자단말기(300)와의 전화통화를 연결하는 단계; 및

(o) 상기 스마트폰(100)이 스피커를 통해 호접속이 연결된

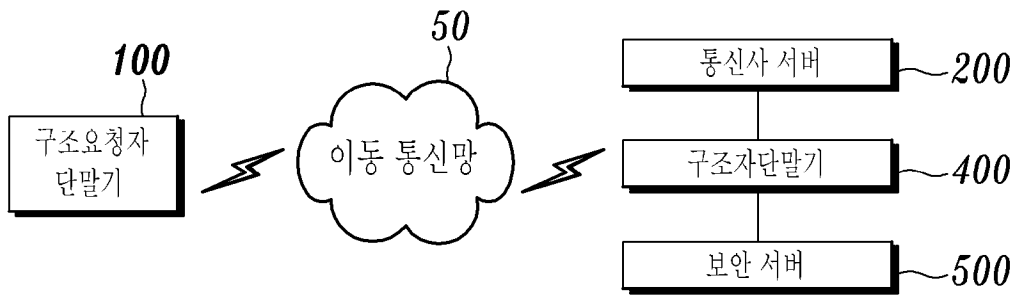
보호자단말기(300)로부터의 음성출력을 억제하며, 마이크로

입력되는 음성을 호접속이 연결된 보호자단말기(300)로

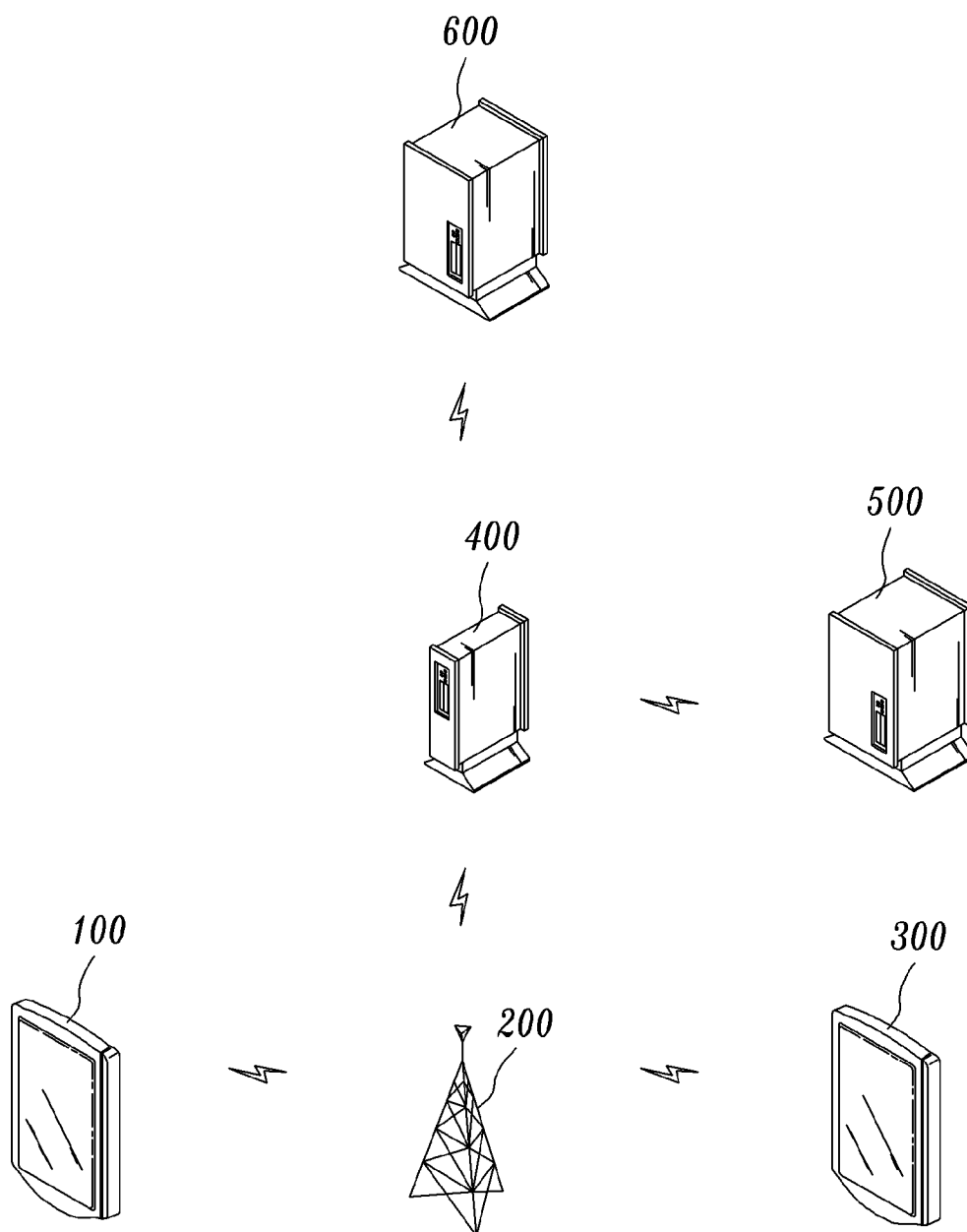
전송하도록 제어하고 상기 (f) 단계로 절차를 이행하는 단계;를

포함하는 것을 특징으로 하는 스마트폰을 이용한 긴급호출 오남용 방지 방법.

[Fig. 1]

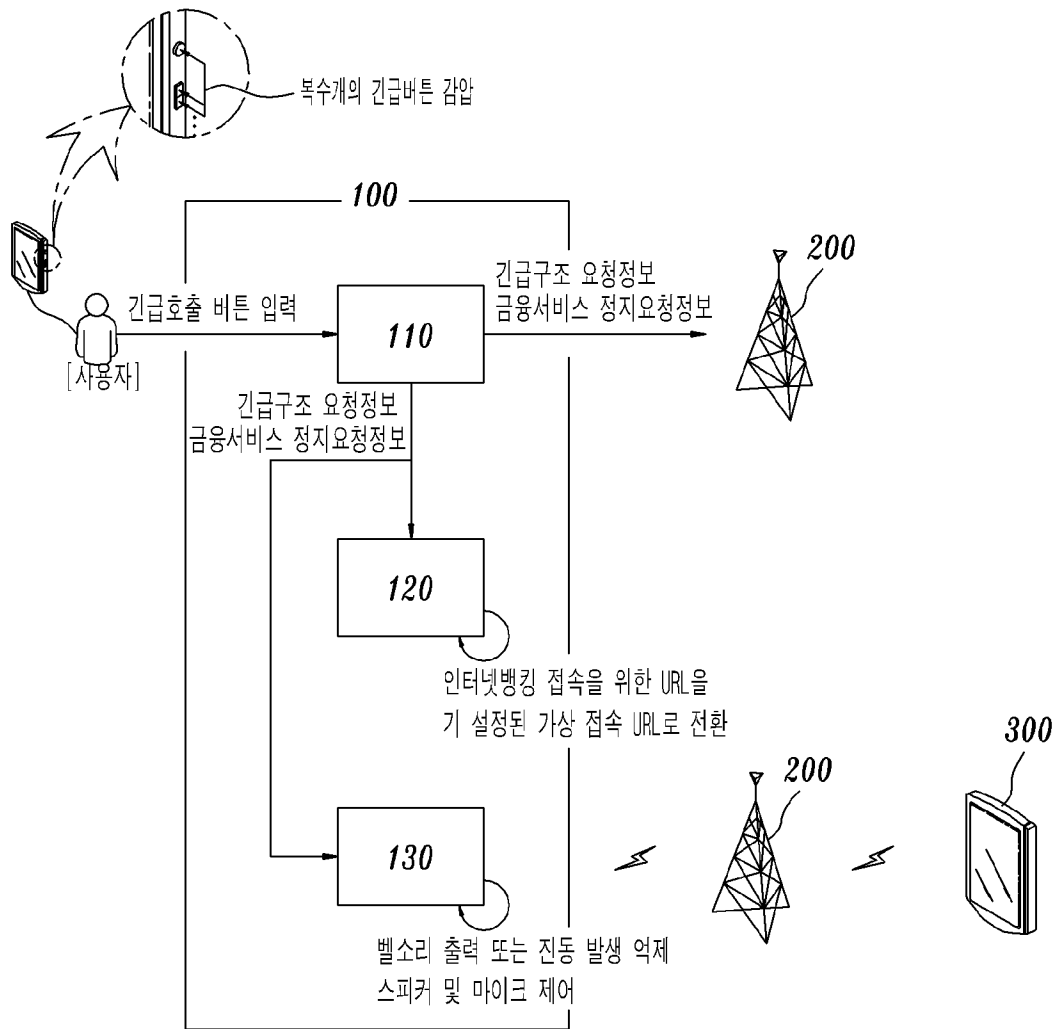


[Fig. 2]

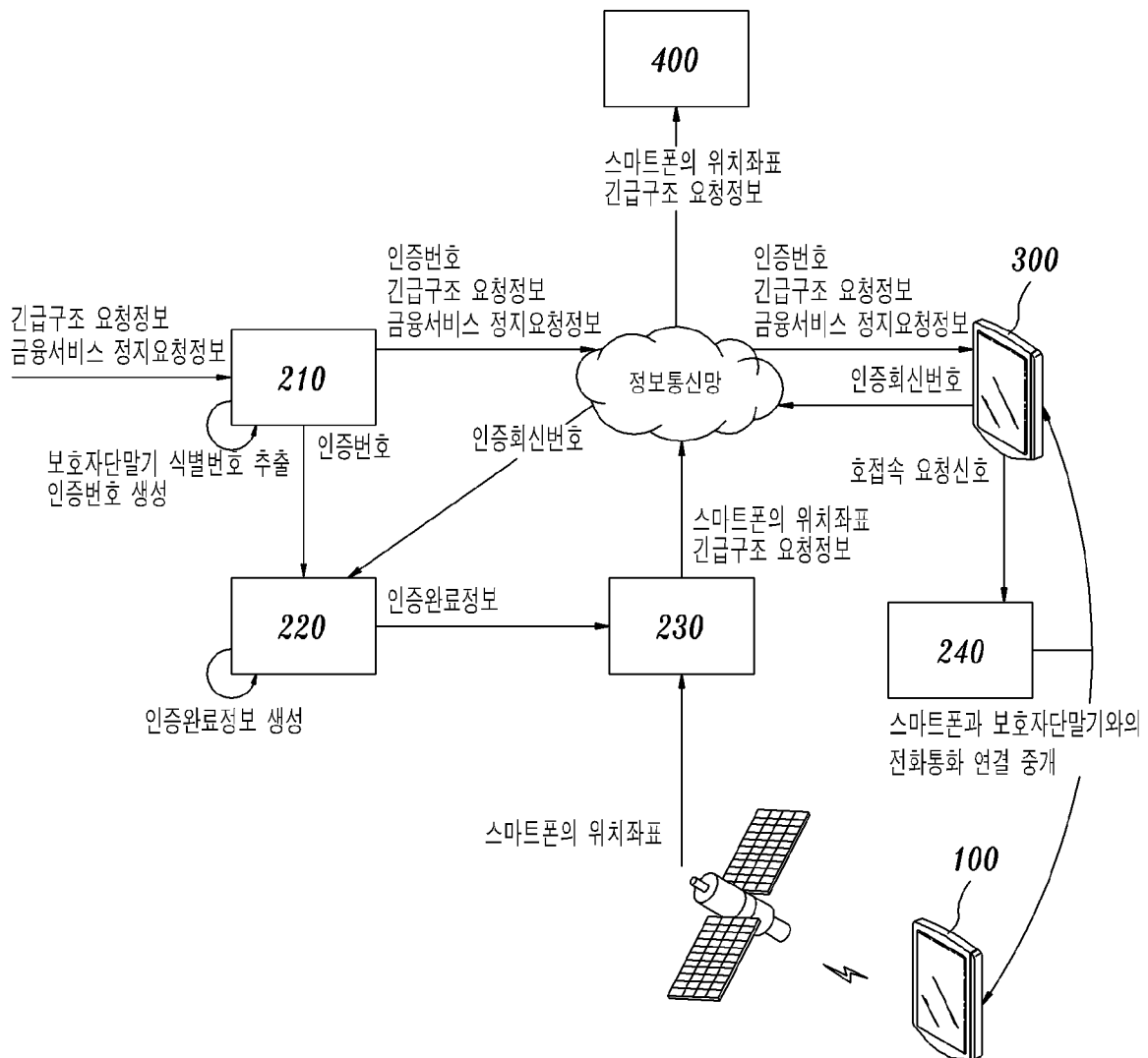


S

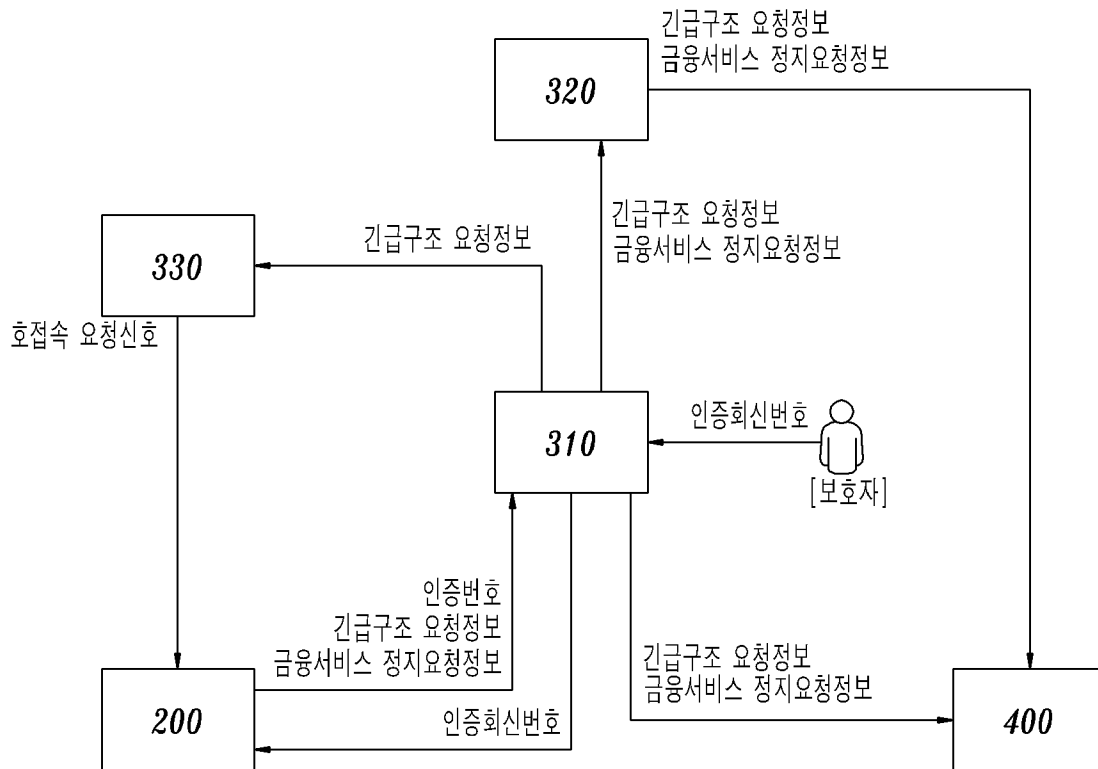
[Fig. 3]



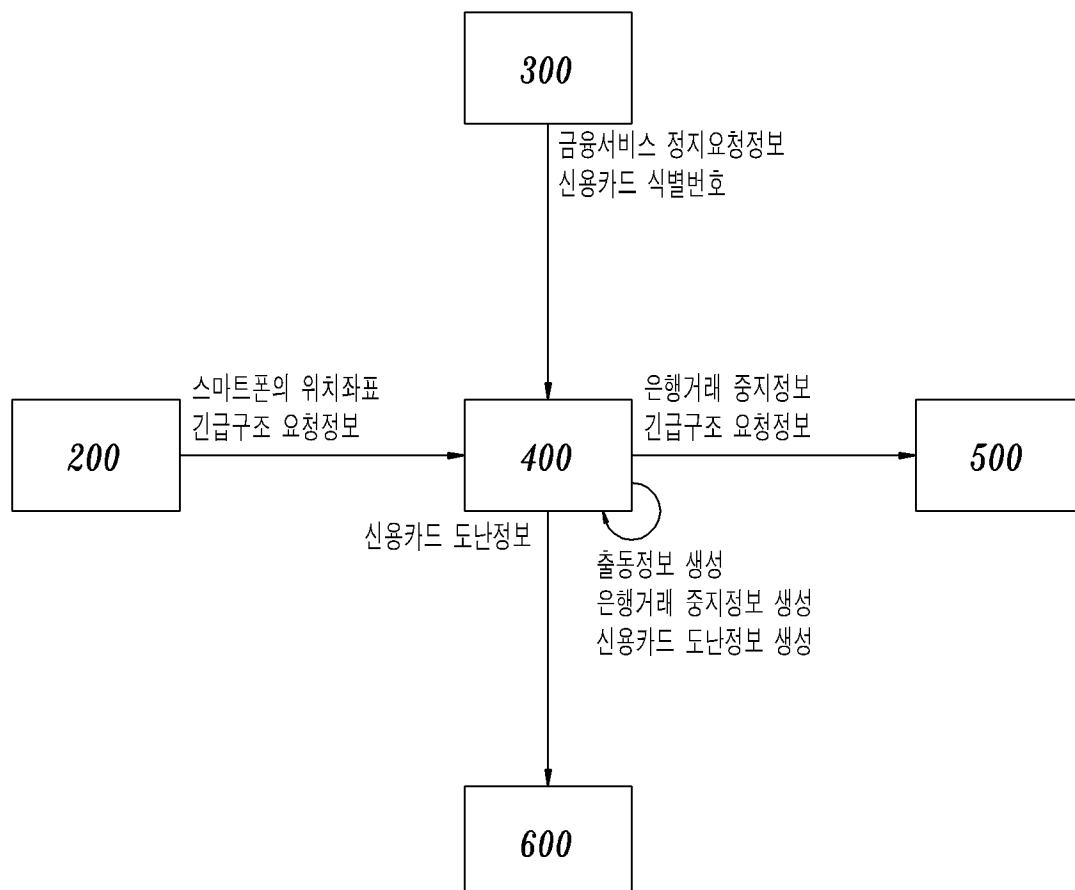
[Fig. 4]



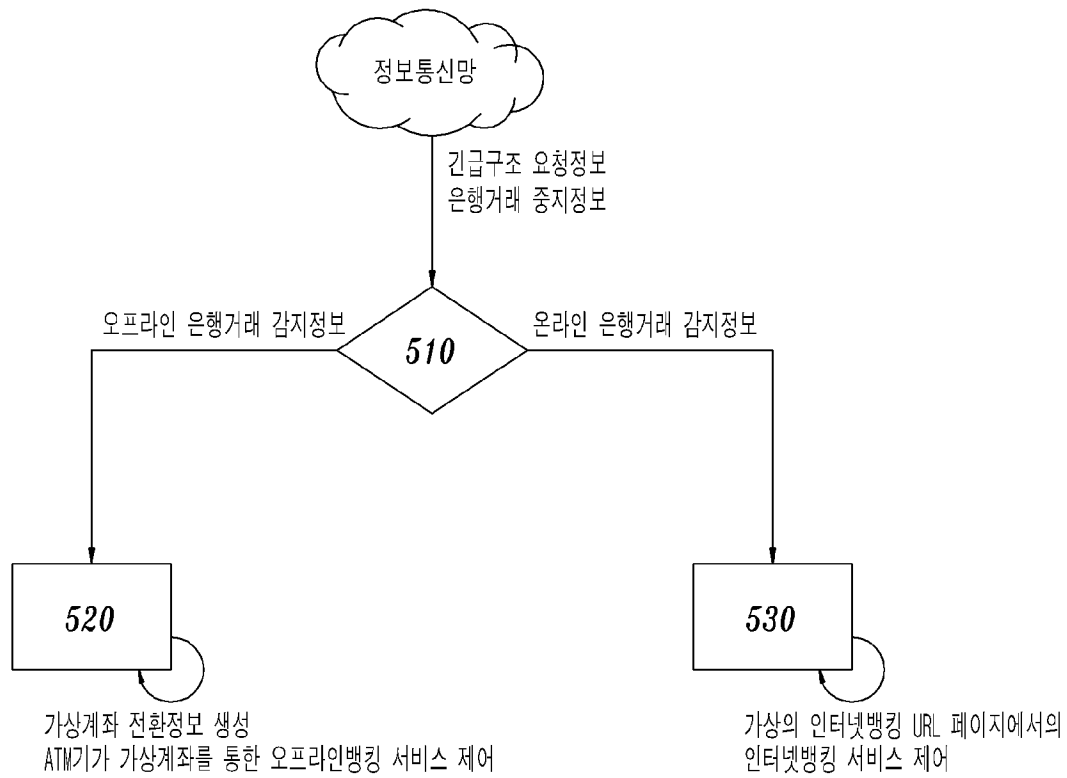
[Fig. 5]



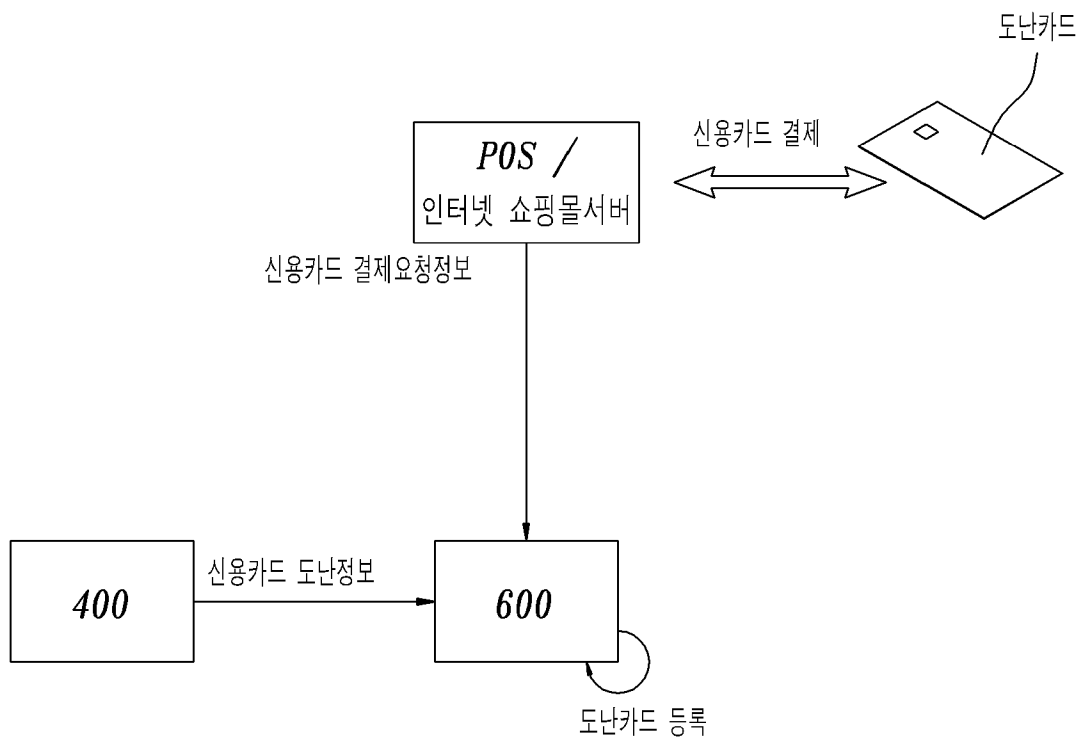
[Fig. 6]



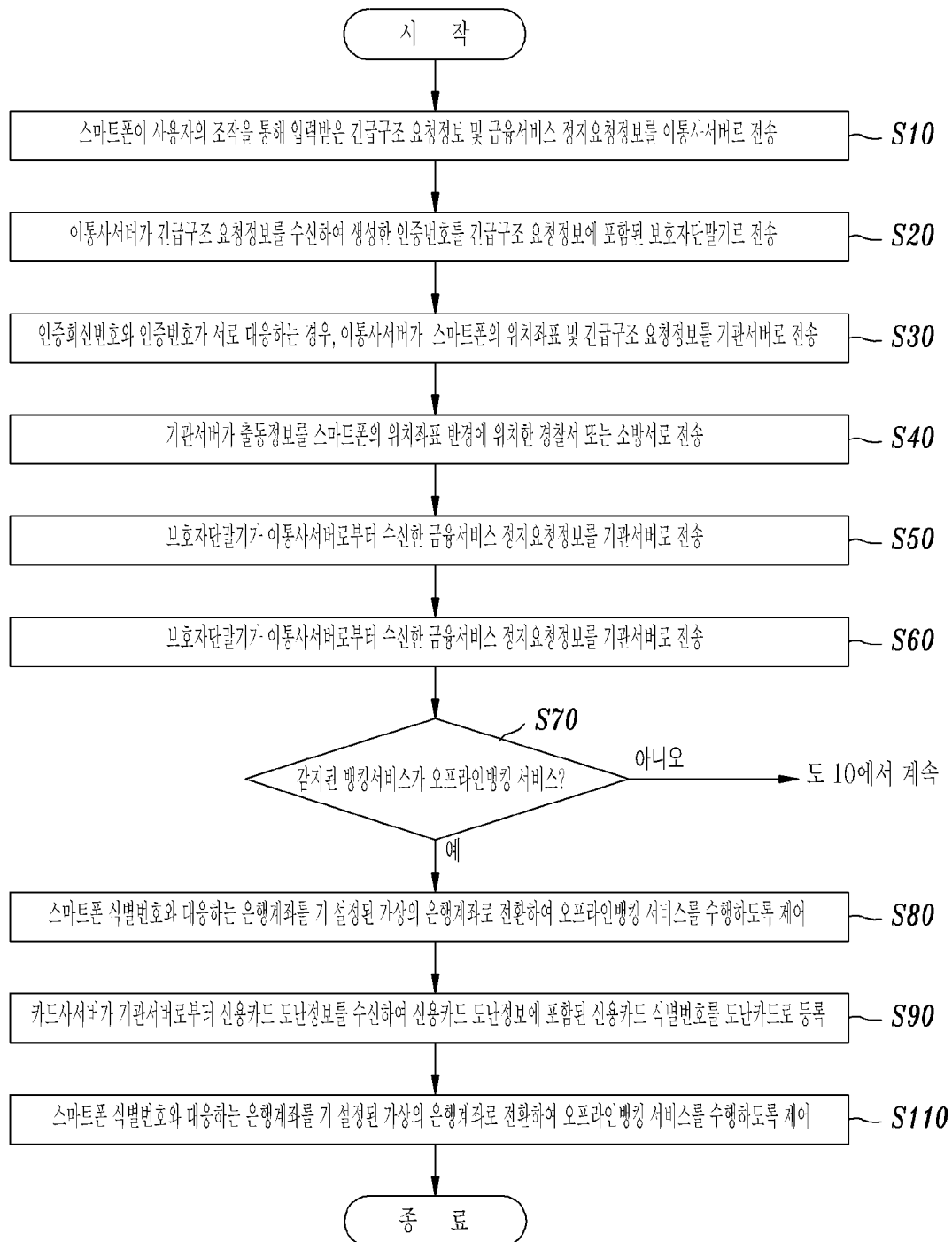
[Fig. 7]



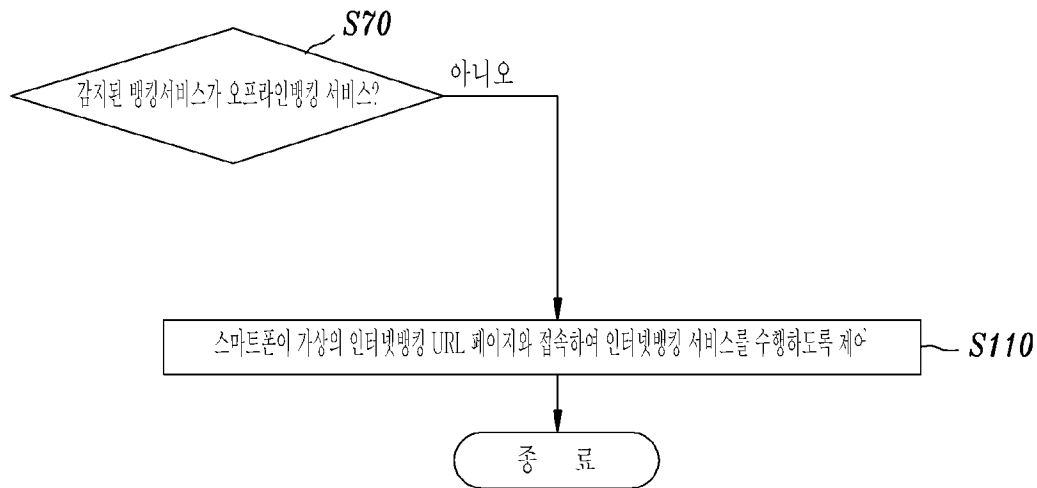
[Fig. 8]



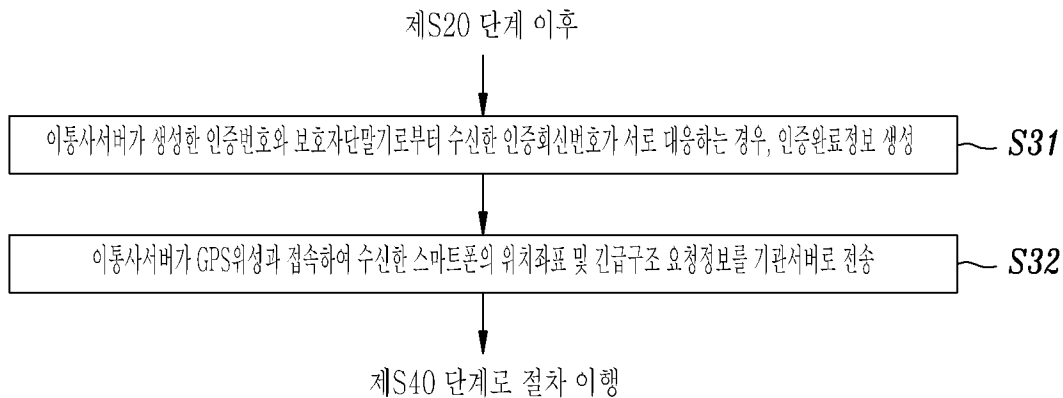
[Fig. 9]



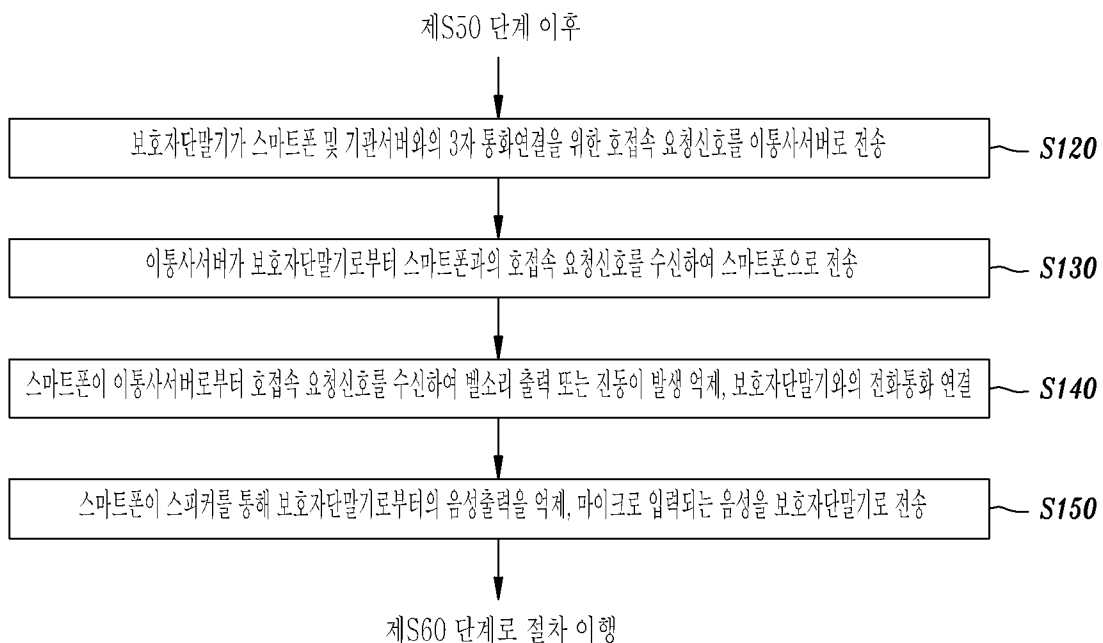
[Fig. 10]



[Fig. 11]



[Fig. 12]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2013/000614**A. CLASSIFICATION OF SUBJECT MATTER****H04W 4/22(2009.01)i, G06Q 40/02(2012.01)i**

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)

H04W 4/22; G07F 19/00; H04W 4/02; G06Q 40/02

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

Korean Utility models and applications for Utility models: IPC as above

Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: emergency, virtual account

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KR 10-2003-0028517 A (KIM, Han seok et al.) 08 April 2003 See abstract, claims 12, 25-26, paragraphs <90>-<91>, <103>.	1-2,4-10
A	KR 10-2008-0007781 A (KTFREETEL CO., LTD.) 23 January 2008 See abstract, claim 1, figures 6, 7.	1-11
A	KR 10-2001-0037271 A (BAEK, Kyung hun) 07 May 2001 See abstract, claim 1, figures 2, 3.	1-11



Further documents are listed in the continuation of Box C.



See patent family 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 application or patent 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

18 APRIL 2013 (18.04.2013)

Date of mailing of the international search report

19 APRIL 2013 (19.04.2013)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701,
Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2013/000614

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-2003-0028517 A	08.04.2003	EP 1529411 A1 US 2005-0239477 A1 US 7349706 B2 WO 2004-016030 A1	11.05.2005 27.10.2005 25.03.2008 19.02.2004
KR 10-2008-0007781 A	23.01.2008	EP 2050296 A2 JP 2009-545897 A KR 10-0767584 B1 KR 10-0817779 B1 US 2009-0247123 A1 WO 2008-010661 A2 WO 2008-010661 A3	22.04.2009 24.12.2009 17.10.2007 31.03.2008 01.10.2009 24.01.2008 24.01.2008
KR 10-2001-0037271 A	07.05.2001	NONE	

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04W 4/22(2009.01)i, G06Q 40/02(2012.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04W 4/22; G07F 19/00; H04W 4/02; G06Q 40/02

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드: 긴급, 가상 계좌

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X	KR 10-2003-0028517 A (김한석 외 1명) 2003.04.08 요약, 청구항 12, 25-26, 단락 <90>-<91>, <103> 참조.	1-2, 4-10
A	KR 10-2008-0007781 A (주식회사 케이티프리텔) 2008.01.23 요약, 청구항 1, 도 6, 7 참조.	1-11
A	KR 10-2001-0037271 A (백경훈) 2001.05.07 요약, 청구항 1, 도 2, 3 참조.	1-11

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

“A” 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

“T” 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

“E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

“X” 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

“L” 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

“Y” 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

“O” 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

“&” 동일한 대응특허문헌에 속하는 문헌

“P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

국제조사의 실제 완료일

2013년 04월 18일 (18.04.2013)

국제조사보고서 발송일

2013년 04월 19일 (19.04.2013)

ISA/KR의 명칭 및 우편주소

 대한민국 특허청
(302-701) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)
팩스 번호 82-42-472-7140

심사관

이다나

전화번호 82-42-481-3451



국제조사보고서에서
인용된 특허문헌

공개일

대응특허문헌

공개일

KR 10-2003-0028517 A

2003.04.08

EP 1529411 A1

2005.05.11

US 2005-0239477 A1

2005.10.27

US 7349706 B2

2008.03.25

WO 2004-016030 A1

2004.02.19

KR 10-2008-0007781 A

2008.01.23

EP 2050296 A2

2009.04.22

JP 2009-545897 A

2009.12.24

KR 10-0767584 B1

2007.10.17

KR 10-0817779 B1

2008.03.31

US 2009-0247123 A1

2009.10.01

WO 2008-010661 A2

2008.01.24

WO 2008-010661 A3

2008.01.24

KR 10-2001-0037271 A

2001.05.07

없음