(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2010-0002273
(43) 공개일자 2010년01월06일

(51) Int. Cl.
H04M 3/436 (2006.01) *H04M 3/42* (2006.01)
H04M 11/06 (2006.01)
(21) 출원번호 10-2009-7023169
(22) 출원일자 2008년06월27일
심사청구일자 2009년11월05일
(85) 번역문제출일자 2009년11월05일
(86) 국제출원번호 PCT/KR2008/003720
(87) 국제공개번호 WO 2009/005253
국제공개일자 2009년01월08일
(30) 우선권주장
1020070065637 2007년06월29일 대한민국(KR)

(71) 출원인
충남대학교산학협력단
대전광역시 유성구 궁동 220번지 충남대학교
(72) 발명자
류재철
대전광역시 유성구 어은동 한빛아파트 132-801
신영찬
대전광역시 유성구 장대동 304-4
(뒷면에 계속)
(74) 대리인
김원준

전체 청구항 수 : 총 12 항

(54) 스팸전화 차단기능을 가진 인터넷 전화 시스템 및 이를 이용한 스팸차단방법

(57) 요 약

본 발명은, 복수의 단말기, 통신망 및 서버를 포함하는 인터넷전화 시스템에 적용되는 것으로서, **(A)** 상기 **서버**는, ① 송신단말기의 호연결 요청이 있으면, 상기 송신단말기 번호가 하기 서버블랙리스트DB에 존재하지 않는 경우 호연결 요청신호를 수신단말기에 전달하고, 존재하는 경우 호연결을 거부하는 연결제어모듈; ② 단말기의 번호, IP를 포함하는 회원정보를 저장/관리하는 회원정보관리모듈; ③ 수신단말기로부터 스팸신고가 된 송신단말기 번호 또는 송신단말기 번호와 스팸신고 시점을 하기 서버블랙리스트DB에 저장/관리하는 서버측관리모듈; 및 ④ 수신단말기로부터 스팸신고가 된 송신단말기 번호가 저장되는 서버블랙리스트DB;를 포함하며, **(B)** 상기 **단말기**는, 스팸신고신호를 입력받아 상기 서버측관리모듈에 스팸신고신호를 전달하는 단말측관리모듈;을 포함하는 스팸전화 차단장치 및 이를 이용한 스팸전화 차단방법에 관한 것이다.

본 발명에 의하면, 종래와는 달리 서버와 인터넷 전화 사용자의 참여를 통해 인터넷 전화 스팸에 대처할 수 있기 때문에 인터넷 전화 스팸 차단을 위해 초래되는 비용을 효과적으로 감소시킬 수 있다.

(72) 발명자

김규영

대전광역시 유성구 송강동 송강그린아파트 306-1305

김민영

대전광역시 유성구 궁동 465-9 두리빌라 302호

특허청구의 범위

청구항 1

복수의 단말기, 통신망 및 서버를 포함하는 인터넷전화 시스템에 적용되는 스팸전화 차단장치로서,

(A) 상기 서버는,

송신단말기의 호연결 요청이 있으면, 상기 송신단말기 번호가 하기 서버블랙리스트DB에 존재하지 않는 경우 호연결 요청신호를 수신단말기에 전달하고, 존재하는 경우 호연결을 거부하는 연결제어모듈;

단말기의 번호, IP를 포함하는 회원정보를 저장/관리하는 회원정보 관리모듈;

수신단말기로부터 스팸신고가 된 송신단말기 번호 또는 송신단말기 번호와 스팸신고 시점을 하기 서버블랙리스트DB에 저장/관리하는 서버측관리모듈; 및

수신단말기로부터 스팸신고가 된 송신단말기 번호가 저장되는 서버블랙리스트DB;를 포함하며,

(B) 상기 단말기는,

스팸신고신호를 입력받아 상기 서버측관리모듈에 스팸신고신호를 전달하는 단말측관리모듈;을 포함하는

것을 특징으로 하는 인터넷전화 시스템에 적용되는 스팸전화 차단장치.

청구항 2

제 1 항에 있어서,

(A) 상기 서버에는, 명백한 non-spam 송신단말기 번호가 저장되는 서버화이트리스트DB;가 추가로 포함되며,

상기 서버측관리모듈에는, 수신단말기로부터 스팸신고가 된 송신단말기 번호가 상기 서버화이트리스트DB에 존재하는 경우 스팸신고를 무시하는 기능이 추가되는 것을 특징으로 하는 인터넷전화 시스템에 적용되는 스팸전화 차단장치.

청구항 3

제 1 항에 있어서,

(B) 상기 단말기에는,

상기 연결제어모듈에서 전달된 호연결 요청신호에 대하여, 상기 송신단말기 번호가 하기 단말블랙리스트DB에 존재하지 않는 경우 착신신호를 발하고, 존재하는 경우 호연결을 거부하며, 통화 후 스팸신고신호가 입력되면 이를 상기 단말측관리모듈로 전달하는 통화제어모듈; 및

스팸 송신단말기 번호가 저장되는 단말블랙리스트DB;가 추가로 포함되며,

상기 단말측관리모듈에는, 통화 후 스팸신고신호가 입력되면 송신단말기 번호를 상기 단말블랙리스트DB에 저장하는 기능이 추가되는 것을 특징으로 하는 인터넷전화 시스템에 적용되는 스팸전화 차단장치.

청구항 4

제 3 항에 있어서,

(B) 상기 단말기는,

non-spam 송신단말기 번호가 저장되는 단말화이트리스트DB;를 추가로 포함하며,

상기 통화제어모듈에는, 연결제어모듈에서 전달된 호연결 요청신호에 대하여, 상기 송신단말기 번호가 ① 단말화이트리스트DB에 존재하는 경우 또는 단말블랙리스트DB에 존재하지 않는 경우 착신신호를 발하고, ② 블랙리스트DB에 존재하는 경우 호연결을 거부하는 기능이 추가되고, 상기 단말측관리모듈에는, 통화 후 스팸신고신호가 입력되지 않으면 송신단말기 번호를 상기 단말화이트리스트DB에 저장하는 기능이 추가되는 것을 특징으로 하는 인터넷전화 시스템에 적용되는 스팸전화 차단장치.

청구항 5

제 1 항, 제 3 항 또는 제 4 항에 있어서,

(A) 상기 서버에는,

non-spam 송신단말기 번호 및 통화연결되었던 송신단말기 번호 중 스팸신고되지 않은 번호가 저장되는 서버화이트리스트DB; 및

음성 혹은 영상으로 질문을 생성하여 이를 송신단말기에 전달하여 답신을 요청하고, ① 정답이 반송되면 상기 송신단말기 번호를 non-spam으로 ② 답이 반송되지 않거나 오답이 반송되면 상기 송신단말기 번호를 spam으로 결정하여 상기 서버측관리모듈에 전달하는 pre-filtering모듈(122);가 추가로 포함되며,

상기 연결제어모듈은, 송신단말기 번호가 상기 서버블랙리스트DB 및 서버화이트리스트DB 모두에 존재하지 않는 경우, 상기 pre-filtering모듈(122)을 작동시키는 기능이 추가되며,

상기 서버측관리모듈은 상기 pre-filtering모듈(122)로부터의 정보에 따라 상기 송신단말기 번호를 상기 서버화이트리스트DB 또는 서버블랙리스트DB에 저장하는 기능이 추가되는 것을 특징으로 하는 인터넷전화 시스템에 적용되는 스팸전화 차단장치.

청구항 6

제 5 항에 있어서,

상기 서버측관리모듈은, 수신단말기로부터 스팸신고가 된 송신단말기 번호가 상기 서버화이트리스트DB에 존재하는 경우 스팸신고를 무시하는 기능이 추가되는 것을 특징으로 하는 인터넷전화 시스템에 적용되는 스팸전화 차단장치.

청구항 7

제 1 항에 의한 장치를 이용한 스팸전화 차단방법으로서,

(A) 상기 서버가 송신단말기의 호연결 요청을 받는 단계;

(B) 상기 송신단말기 번호가 서버블랙리스트DB에 존재하지 않는 경우 호연결 요청신호를 수신단말기에 전달하고, 존재하는 경우 호연결을 거부하는 단계;

(C) 수신단말기로부터 스팸신고신호가 전달되면 송신단말기 번호 또는 송신단말기 번호와 스팸신고 시점을 서버블랙리스트DB에 저장는 단계;를 포함하는 것을 특징으로 하는 스팸전화 차단방법.

청구항 8

제 2 항에 의한 장치를 이용한 스팸전화 차단방법으로서,

(A) 상기 서버가 송신단말기의 호연결 요청을 받는 단계;

(B) 상기 송신단말기 번호가 서버화이트리스트DB에 존재하거나 서버화이트리스트DB와 서버블랙리스트DB에 모두 존재하지 않는 경우에만 호연결 요청신호를 수신단말기에 전달하고, 서버블랙리스트DB에 존재하는 경우 호연결을 거부하는 단계;

(C) 수신단말기로부터 스팸신고신호가 전달되면, 송신단말기 번호가 상기 서버화이트리스트DB에 존재하는 경우 스팸신고를 무시하고, 서버화이트리스트DB에 존재하지 않는 경우 송신단말기 번호 또는 송신단말기 번호와 스팸신고 시점을 서버블랙리스트DB에 저장는 단계;를 포함하는 것을 특징으로 하는 스팸전화 차단방법.

청구항 9

제 3 항에 의한 장치를 이용한 스팸전화 차단방법으로서,

(A) 상기 서버가 송신단말기의 호연결 요청을 받는 단계;

(B) 상기 송신단말기 번호가 서버블랙리스트DB에 존재하지 않는 경우 호연결 요청신호를 수신단말기에 전달하고, 존재하는 경우 호연결을 거부하는 단계;

(C) 상기 연결제어모듈에서 전달된 호연결 요청신호에 대하여, 상기 송신단말기 번호가 단말블랙리스트DB에 ① 존재하지 않는 경우 착신신호를 발하고, ② 존재하는 경우 호연결을 거부하는 단계;

(D) 통화 후 사용자로부터 스팸신고신호가 입력되면 이를 상기 단말측관리모듈로 전달하고, 동시에 송신단말기 번호를 상기 단말블랙리스트DB에 저장하는 단계;

(E) 수신단말기로부터 스팸신고신호가 전달되면 송신단말기 번호 또는 송신단말기 번호와 스팸신고 시점을 서버블랙리스트DB에 저장는 단계;를 포함하는 것을 특징으로 하는 스팸전화 차단방법.

청구항 10

제 4 항에 의한 장치를 이용한 스팸전화 차단방법으로서,

(A) 상기 서버가 송신단말기의 호연결 요청을 받는 단계;

(B) 상기 송신단말기 번호가 서버블랙리스트DB에 존재하지 않는 경우 호연결 요청신호를 수신단말기에 전달하고, 존재하는 경우 호연결을 거부하는 단계;

(C) 상기 연결제어모듈에서 전달된 호연결 요청신호에 대하여, 상기 송신단말기 번호가 단말블랙리스트DB에 ① 존재하지 않는 경우 착신신호를 발하고, ② 존재하는 경우 호연결을 거부하는 단계;

(D) ① 통화 후 사용자로부터 스팸신고신호가 입력되면 이를 상기 단말측관리모듈로 전달하고, 동시에 송신단말기 번호를 상기 단말블랙리스트DB에 저장하며, ② 통화 후 스팸신고신호가 입력되지 않으면 송신단말기 번호를 상기 단말화이트리스트DB에 저장하는 단계;

(E) 수신단말기로부터 스팸신고신호가 전달되면 송신단말기 번호 또는 송신단말기 번호와 스팸신고 시점을 서버블랙리스트DB에 저장는 단계;를 포함하는 것을 특징으로 하는 스팸전화 차단방법.

청구항 11

제 5 항에 의한 장치를 이용한 스팸전화 차단방법으로서,

(A) 상기 서버가 송신단말기의 호연결 요청을 받는 단계;

(B) 상기 송신단말기 번호가 ① 서버블랙리스트DB에 존재하는 경우 호연결을 거부하고, ② 서버블랙리스트DB에 존재하지 않으면서 서버화이트리스트DB에 존재하는 경우 호연결 요청신호를 수신단말기에 전달하고, ③ 서버블랙리스트DB 및 서버화이트리스트DB 모두에 존재하지 않는 경우, 음성 혹은 영상으로 질문을 생성하여 이를 송신단말기에 전달하여 답신을 요청하고, a) 정답이 반송되면 상기 송신단말기 번호를 서버화이트리스트DB에 저장하고 호연결 요청신호를 수신단말기에 전달하며, b) 답이 반송되지 않거나 오답이 반송되면 상기 송신단말기 번호를 서버블랙리스트DB에 저장하고 호연결을 거부하는 단계;

(C) 수신단말기로부터 스팸신고신호가 전달되면 송신단말기 번호 또는 송신단말기 번호와 스팸신고 시점을 서버블랙리스트DB에 저장하는 단계;를 포함하는 것을 특징으로 하는 스팸전화 차단방법.

청구항 12

제 11 항에 있어서,

단계 (C)에서, 상기 스팸신고신호가 전달된 송신단말기 번호가 상기 서버화이트리스트DB에 존재하는 경우 스팸신고를 무시하는 것을 특징으로 하는 스팸전화 차단방법.

명 세 서

기 술 분 야

<1> 본 발명은 개인용 컴퓨터와 전용 전화기 상에서 인터넷 전화(VoIP - Voice over IP : 이하 인터넷 전화)의 사용시 발생할 수 있는 인터넷 전화 스팸(VoIP Spam : 이하 스팸)을 효과적으로 차단하는 장치 및 방법에 관한 것이다.

배 경 기 술

<2> 인터넷 통신기술이 급속하게 발달하면서 인터넷 망에 기반한 전화(VoIP)의 보급이 증가되고 있다. 이에 비례하여 사용자가 원치 않는 정보를 일방적으로 제공하고자 하는 인터넷 전화 스팸 역시 증가하면서 사용상의 불편함이 문제로 되고 있다. 종래 다양한 방식의 인터넷 전화 스팸 차단을 위한 방안이 제시되고 있으나, 개별적으로

문제점을 안고 있는 것이 현실이다.

<3> (A) 컨텐츠 필터링 방식은, 이메일 스팸에서 사용되는 일반적인 형태의 스팸 대응 방법으로 콘텐츠의 내용을 파악하여 스팸 정보를 걸러내는 방식이다. 하지만 인터넷 전화의 경우 사용자 혹은 인터넷 전화 서비스 사업자가 전화를 받기 전까지는 컨텐츠의 내용을 파악할 수가 없다. 또한 인터넷 전화 상에는 음성전송을 위한 다양한 방법이 존재하며 컨텐츠가 음성과 비디오로 되어 있을 경우 음성과 비디오 인식 기술이 현재까지 정교하지 않기 때문에 컨텐츠를 분석하여 스팸인지 아닌지 판단하는데 어려움이 있다.

<4> (B) 블랙리스트 기반의 방식은 스패머의 주소를 리스팅 하여 주소 매핑에 의해 스팸을 차단하는 방식이다. 일반적인 블랙리스트 관리를 통한 인터넷 전화 스팸 차단의 경우, 인터넷 전화 스패머(이하 스패머)의 정보 등록을 통해 차단하는 방법이기 때문에 등록된 스패머가 정상적인 사용자일 경우 이를 해결하는 방법을 제공하지 못하였고 블랙리스트의 효과적인 갱신을 위한 방법이 제공되어지지 않았다. 또한 블랙리스트의 관리가 중앙 집중적으로 서버에 의해 유지었기 때문에 인터넷 전화 사용자의 특징을 반영하지 못하는 단점을 가지고 있다.

<5> (C) 화이트리스트 기반의 방식은 블랙리스트의 반대 방식으로 유효한 사용자의 이메일만 받아들인다. 하지만 이 방식의 경우 정당한 송신자가 사용자에게 처음으로 통신하고자 하는 경우 화이트리스트에 없기 때문에 통신을 할 수 없다.

<6> (D) 동의 기반(Consent-based) 통신방식은 사용자 A가 B와 통신할 때, B의 블랙 또는 화이트리스트에 A에 대한 정보가 없기 때문에 초기 통신과정은 거절되고, 동의를 요청한다. 이후에 다시 A가 B에게 통신을 시도하면 B는 A가 이전에 통신을 시도 했다는 것을 알고 A의 요청을 승낙하거나 거절한다. 이러한 동의기반 시스템은 전화 시스템에 효과적인것처럼 보이지만 스팸의 근본적인 특성만 바꿀뿐이다. 즉 스팸의 콘텐츠를 통해 불필요한 정보를 받는 것을 막을 수는 있지만 동의요청에 의한 사람을 성가시게 하는 것은 막을 수 없다.

<7> (E) 평판(Reputation) 시스템에 기반한 방식은 요청자의 아이디에 대한 스패머에 대한 구별을 평판도를 사용하여 판단하도록 한다. 예를 들면 사용자가 전화기 상에서 버튼을 누르게 되면 스패머 아이디가 중앙 평판 시스템에 전송된다. 연속적인 신고를 받은 아이디에 대해서 스패머로 판단을 하여 차단할 수 있다. 하지만 공모에 의해 나쁜 평판도를 받을 수 있다.

발명의 상세한 설명

<8> **기술적 과제**

<9> 본 발명은 인터넷 전화의 사용시 발생할 수 있는 인터넷 전화 스팸을 효과적으로 차단하는 기능을 가진 인터넷 전화 스팸 차단장치 및 차단방법을 제공하는 것을 목적으로 한다.

<10> **기술적 해결방법**

<11> 전술한 목적을 달성하기 위한 본 발명은, 복수의 단말기, 통신망 및 서버를 포함하는 인터넷전화 시스템에 적용되는 것으로서, **(A)** 상기 **서버**는, ① 송신단말기의 호연결 요청이 있으면, 상기 송신단말기 번호가 하기 서버블랙리스트DB에 존재하지 않는 경우 호연결 요청신호를 수신단말기에 전달하고, 존재하는 경우 호연결을 거부하는 연결제어모듈; ② 단말기의 번호, IP를 포함하는 회원정보를 저장/관리하는 회원정보관리모듈; ③ 수신단말기로부터 스팸신고가 된 송신단말기 번호 또는 송신단말기 번호와 스팸신고 시점을 하기 서버블랙리스트DB에 저장/관리하는 서버측관리모듈; 및 ④ 수신단말기로부터 스팸신고가 된 송신단말기 번호가 저장되는 서버블랙리스트DB;를 포함하며, **(B)** 상기 **단말기**는, 스팸신고신호를 입력받아 상기 서버측관리모듈에 스팸신고신호를 전달하는 단말측관리모듈;을 포함하는 스팸전화 차단장치 및 이를 이용한 스팸전화 차단방법에 관한 것이다. 따라서 본 발명에서는 종래 알려진 인터넷 전화 시스템의 장치/구성 및 통화방법에 관한 기술을 포함한다. 본 발명에서 "단말기"란 인터넷 전화기로서 stand-alone 형 전화기뿐만 아니라 인터넷 전화용 프로그램이 실행되고 해드셋이 갖추어진 컴퓨터를 포함하는 개념이다. 본 발명에서 "서버"란 인터넷 전화 스팸 차단을 위한 서버를 의미하지만 반드시 물리적으로 독립된 서버를 지칭하는 것은 아니며, 통상 인터넷 전화를 위한 운영서버의 일부 기능일 수도 있다.

<12> **유리한 효과**

<13> 본 발명에 의하면, 인터넷 전화 사용자의 참여를 통해 인터넷 전화 스팸에 대처할 수 있기 때문에 인터넷 전화 스팸 차단을 위해 초래되는 비용을 효과적으로 감소시킬 수 있다.

<14> 또한 본 발명에 의하면 spam임이 명백한 녹음/녹화된 정보의 전달을 사전에 차단함으로써 전체적인 인터넷 전화

시스템의 부하를 감소시키고 사용자의 편의를 증대시킬 수 있다.

산업상 이용 가능성

<103> 본 발명에 의하면, 인터넷 전화 스팸 차단을 위해 초래되는 비용을 효과적으로 감소시킬 수 있으며 전체적인 인터넷 전화 시스템의 부하를 감소시키고 사용자의 편의를 증대시킬 수 있다.

도면의 간단한 설명

<15> 도 1는 본 발명에 의한 인터넷전화 시스템에 적용되는 스팸전화 차단장치의 개략 구성도.

<16> 도 2는 도 1의 차단장치를 이용한 스팸전화 차단방법의 흐름도.

<17> 도 3는 본 발명에 의한 인터넷전화 시스템에 적용되는 제2의 스팸전화 차단장치의 개략 구성도.

<18> 도 4는 도 3의 차단장치를 이용한 스팸전화 차단방법의 흐름도.

<19> 도 5는 본 발명에 의한 인터넷전화 시스템에 적용되는 제3의 스팸전화 차단장치의 개략 구성도.

<20> 도 6는 도 5의 차단장치를 이용한 스팸전화 차단방법의 흐름도.

<21> 도 7는 본 발명에 의한 인터넷전화 시스템에 적용되는 제4의 스팸전화 차단장치의 개략 구성도.

<22> 도 8는 도 7의 차단장치를 이용한 스팸전화 차단방법의 흐름도.

<23> 도 9는 본 발명에 의한 인터넷전화 시스템에 적용되는 제5의 스팸전화 차단장치의 개략 구성도.

<24> 도 10는 도 9의 차단장치를 이용한 스팸전화 차단방법의 흐름도.

<25> 도 11은 도 9의 차단장치를 이용한 제6의 스팸전화 차단방법의 흐름도.

<26> ********** 주요 도면부호의 설명 **********

<27> 110. 수신단말기 111. 통화제어모듈

<28> 112. 단말블랙리스트DB 113. 단말화이트리스트DB

<29> 114. 단말측관리모듈 115. 회원정보관리모듈

<30> 116. 회원정보DB

<31> 120. 서버 121. 연결제어모듈

<32> 122. pre-filtering모듈 123. 서버블랙리스트DB

<33> 124. 서버화이트리스트DB 125. 서버측관리모듈

<34> **발명의 실시를 위한 최선의 형태**

<35> 이하 단순한 구조/방법부터 복잡한 구조/방법 순으로 구분하여 본 발명을 설명한다.

<36> (1A) 블랙리스트를 관리하는 서버와 스팸신고기능의 단말기로 이루어지는 장치(제1항)

<37> 본 발명에 의한 스팸전화 차단장치는, 복수의 단말기, 통신망 및 서버를 포함하는 인터넷전화 시스템에 적용되는 스팸전화 차단장치로서, **(A)** 상기 **서버**(120)는, ① 송신단말기의 호연결 요청이 있으면, 상기 송신단말기 번호가 하기 서버블랙리스트DB(123)에 존재하지 않는 경우 호연결 요청신호를 수신단말기(110)에 전달하고, 존재하는 경우 호연결을 거부하는 연결제어모듈(121); ② 단말기의 번호, IP를 포함하는 회원정보를 저장/관리하는 회원정보관리모듈(115); ③ 수신단말기(110)로부터 스팸신고가 된 송신단말기 번호 또는 송신단말기 번호와 스팸신고 시점을 하기 서버블랙리스트DB(123)에 저장/관리하는 서버측관리모듈(125); 및 ④ 수신단말기(110)로부터 스팸신고가 된 송신단말기 번호가 저장되는 서버블랙리스트DB(123);를 포함하며, **(B)** 상기 **단말기**는, 스팸신고신호를 입력받아 상기 서버측관리모듈에 스팸신고신호를 전달하는 단말측관리모듈(114);을 포함한다. 도 1에 인터넷전화 시스템에 적용되는 스팸전화 차단장치의 관련 구성요소를 도시하였다. 본 발명에서 상기 서버(120)에는 단말기의 번호, IP 등의 회원정보가 저장되는 회원정보DB(116)를 둘 수 있다.

<38> 도면에서 각 구성요소들을 하기 표 1과 같은 약자로 표시(이하 모든 도면에서 동일함)하였으며, 상세한 설명에

서도 부분적으로 약자를 적용하였다.

<39> 표 1

구성요소	약자	구성요소	약자
연결제어모듈	CCM	통화제어모듈	LCM
단말기정보관리모듈	IMM	단말측관리모듈	TMM
단말기정보DB	I-DB	단말블랙리스트DB	TB-DB
서버측관리모듈	SMM	단말화이트리스트DB	TW-DB
서버블랙리스트DB	SB-DB		
서버화이트리스트DB	SW-DB		
pre-filtering모듈	PFM		

<40>

<41> 도시된 바와 같이, 본 발명에 의한 장치의 서버(120)에는 연결제어모듈(121), 회원정보관리모듈(115), 서버측관리모듈(125) 및 서버블랙리스트DB(123)가 포함되어 있고, 단말기-보다 정확하게는 본 발명에 의한 스팸 차단방법을 이용하기로 약정되어 있는 단말기-에는 단말측관리모듈(114)이 포함되어 있다.

<42> 연결제어모듈(121)은, 송신단말기로부터 타단말기(=수신단말기)로의 호연결 요청이 있으면 먼저 서버블랙리스트DB(123)를 조회하여 상기 송신단말기 번호가 존재하지 확인한다. 존재하지 않는 경우 호연결 요청신호를 수신단말기(110)에 전달하고, 존재하는 경우 호연결을 거부한다.

<43> 회원정보관리모듈(115)은, 본 발명에 의한 스팸 차단방법을 이용하기로 약정되어 있는 단말기들의 번호, IP를 포함하는 회원정보를 저장/관리한다.

<44> 서버측관리모듈(125)은, 서버블랙리스트DB(123)를 관리한다. 즉, 수신단말기(110)로부터 스팸신고가 된 송신단말기 번호 또는 송신단말기 번호와 스팸신고 시점을 하기 서버블랙리스트DB(123)에 저장/관리한다.

<45> 서버블랙리스트DB(123)는, 수신단말기(110)로부터 스팸신고가 된 송신단말기 번호가 저장된다. 물론 서버블랙리스트DB(123)에 저장되는 블랙리스트는 수신단말기(110)로부터 스팸신고가 된 송신단말기 번호가 자동 입력되도록 할 수도 있고, 명백한 spam인 경우 관리자에 의해 수동적으로 입력되도록 할 수도 있다.

<46> 한편, 경우에 따라서는 처음에는 명백한 spam이었다가 추후에 non-spam으로 전환된 송신단말기 번호가 존재할 수 있다. 이러한 상황에 대처하기 위해, 수신단말기(110)로부터 스팸신고가 된 경우, 송신단말기 번호 뿐 아니라 신고가 접수된 시점에 대한 정보를 함께 서버블랙리스트DB(123)에 저장하였다가 소정의 기간동안 동일 번호로 호연결 요청이 없는 송신단말기 번호는 서버블랙리스트DB(123)에서 자동으로 삭제되도록 하는 것도 바람직하다.

<47> 단말측관리모듈(114)은, 스팸신고신호를 입력받아 상기 서버측관리모듈(125)에 스팸신고신호를 전달한다. 처음 상기 서버(120)를 통해 수신단말기(110)로의 호연결을 요청한 어떤 송신단말기는 그 번호가 서버블랙리스트DB(123)에 존재하지 않기 때문에 호연결 요청신호가 수신단말기(110)에 전달된다. 수신단말기(110) 사용자가 전화를 받은 후 spam임을 확인한 경우 이를 소정의 방법(예를 들면, 통화 종료 후 스팸신고버튼을 누르는 방법)으로 스팸신고하면 이 신호를 서버측관리모듈(125)로 전달하여 상기 송신단말기 번호를 서버블랙리스트DB(123)에 저장하도록 하는 것이다. 단말측관리모듈(114)이 스팸신고신호 전달시 송신단말기 번호를 함께 서버(120)로 전달할 수도 있지만, 상시 송신단말기 번호 정보가 (임시로) 서버(120)에 저장되어 있는 경우 단순히 스팸신고신호만 전달하도록 하는 것이 효율적이다.

<48> (1B) 서버에서 블랙리스트를 관리하고 단말기에서 스팸신고가 이루어지는 방법(제7항)

<49> 본 발명에 의한 스팸전화 차단방법은, 전술한 (1A)의 장치를 이용한 스팸전화 차단방법으로서, **(A)** 상기 서버(120)가 송신단말기의 호연결 요청을 받는 단계; **(B)** 상기 송신단말기 번호가 서버블랙리스트DB(123)에 존재하지 않는 경우 호연결 요청신호를 수신단말기(110)에 전달하고, 존재하는 경우 호연결을 거부하는 단계; 및 **(C)** 수신단말기(110)로부터 스팸신고신호가 전달되면 송신단말기 번호를 서버블랙리스트DB(123)에 저장는 단계;를 포함한다. 도 2에 본 발명의 스팸전화 차단방법에 따른 작동단계의 흐름도를 도시하였다.

<50> 먼저, 단계(101)에서 서버(120)는 송신단말기로부터 특정 번호의 수신자단말기(이하 '수신자단말기'라 표현함)로의 호(통화) 연결 요청을 받는다.

<51> 단계(102)에서 상기 서버(120)는 SB-DB를 조회하여 송신단말기의 호연결 요청을 수락할 것인지를 결정한다. 만일 송신단말기의 번호가 SB-DB에 존재하면 호연결을 거부(단계 103)하고, 존재하지 않으면 호연결 신호를 수신단말기(110)로 전달한다. 수신단말기(110)에서 통화연결(단계 104) 후 — 즉, 수신단말기(110)측 수신자가 전화를 받아 통화를 종료한 후 — 수신자로부터의 스팸신고신호의 입력여부를 확인한다(단계 105).

<52> 스팸신고신호가 입력된 경우 이를 서버(120)로 전달하여 상기 송신단말기 번호를 SB-DB에 기록하고(107), 스팸신고신호가 입력되지 않으면 아무런 액션을 취하지 않는다(106).

<53> 도시되지는 않았지만, 수신단말기(110)로부터 스팸신고가 된 경우, 송신단말기 번호 뿐 아니라 신고가 접수된 시점에 대한 정보를 함께 서버블랙리스트DB(123)에 저장하였다가 소정의 기간동안 호연결 요청이 없는 송신단말기 번호는 서버블랙리스트DB(123)에서 자동으로 삭제되도록 하는 단계가 추가될 수도 있다(이하 모두 동일).

<54> 한편, 특정 수신단말기(110)에 통화연결된 송신단말기 번호정보는 서버(120)에 저장되어 있을 수 있다. 구체적인 스팸신고 신호는 'spam 전화번호와, 그 것이 spam이라는 정보'로 이루어질 수도 있고, 단순히 최근 통화연결된 송신단말기 번호가 'spam이라는 정보'로 이루어질 수도 있다(이하 모두 동일).

<55> (2A) 서버에 화이트리스트DB가 추가된 차단장치(제2항)

<56> 전술한 (1A)의 장치나 (1B)의 방법에 의하면 일단 SB-DB에 입력된 송신단말기로부터의 호연결 요청은 계속 거부된다. 따라서 명백히 non-spam 송신단말기임에도 불구하고 수신단말기(110) 사용자의 착오나 고의에 따른 스팸신고에 의해 SB-DB에 입력되는 것을 방지할 필요가 있다.

<57> 이를 위해 본 발명은 전술한 (1A)의 장치에 일부 구성요소와 기능을 추가한 장치를 제공한다. 본 장치의 상기 서버(120)에는, 명백한 non-spam 송신단말기 번호가 저장되는 서버화이트리스트DB(124);가 추가로 포함되며, 상기 서버측관리모듈(125)에는, 수신단말기(110)로부터 스팸신고가 된 송신단말기 번호가 상기 서버화이트리스트DB(124)에 존재하는 경우 스팸신고를 무시하는 기능이 추가된다. 도 3에 본 스팸전화 차단장치의 관련 구성요소를 도시하였다.

<58> 도시된 바와 같이, 상기 서버(120)에는 SW-DB가 추가되는데, 여기에는, 예컨대 본 발명에 의한 스팸 차단방법을 운영하는 주체에 의해 수동으로 확인된, non-spam이 명백한 송신단말기 번호가 저장된다. SW-DB의 추가에 따라 이를 관리하는 SMM의 기능도, SW-DB에 기록된 번호에 대해 스팸신고가 전달된 경우 이를 무시(즉, 이 번호를 SB-DB에 기록하지도 않고, SW-DB에서 삭제하지도 않음)하는 기능이 추가된다.

<59> (2B) 서버에 화이트리스트 관리기능이 추가된 차단방법(제8항)

<60> 본 발명에 의한 스팸전화 차단방법은, 전술한 (2A)의 장치를 이용한 스팸전화 차단방법으로서, (A) 상기 서버(120)가 송신단말기의 호연결 요청을 받는 단계; (B) 상기 송신단말기 번호가 서버화이트리스트DB(124)에 존재하거나 서버화이트리스트DB(124)와 서버블랙리스트DB(123)에 모두 존재하지 않는 경우에만 호연결 요청신호를 수신단말기(110)에 전달하고, 서버블랙리스트DB(123)에 존재하는 경우 호연결을 거부하는 단계; (C) 수신단말기(110)로부터 스팸신고신호가 전달되면, 송신단말기 번호가 상기 서버화이트리스트DB(124)에 존재하는 경우 스팸신고를 무시하고, 서버화이트리스트DB(124)에 존재하지 않는 경우 송신단말기 번호 또는 송신단말기 번호와 스팸신고 시점을 서버블랙리스트DB(123)에 저장는 단계;를 포함한다. 도 4에 상기 차단방법에 따른 작동단계의 흐름도를 도시하였다.

<61> 먼저, 단계(201)에서 서버(120)는 송신단말기로부터 수신자단말기로의 호(통화) 연결 요청을 받는다.

<62> 이어서 상기 서버(120)는 SW-DB를 조회하여 송신단말기의 호연결 요청을 수락할 것인지를 결정한다(단계 202). 만일 송신단말기의 번호가 SW-DB에 존재하면 호연결 신호를 수신단말기(110)로 전달하고, 존재하지 않으면 다음 단계로 이동한다.

<63> 이어서 송신단말기 번호가 SB-DB에 존재하는지 확인하여(단계 203) 존재하면 호연결을 거부(단계 204)하고, 존재하지 않으면 호연결 신호를 수신단말기(110)로 전달한다.

<64> 수신단말기(110)에서 통화연결(단계 205) 후 수신자로부터의 스팸신고신호의 입력여부를 확인한다(단계 206). 스팸신고신호가 입력된 경우 이를 서버(120)로 전달하고, 스팸신고신호가 입력되지 않으면 아무런 액션을 취하지 않는다(단계 207).

<65> 스팸신고신호를 전달받은 서버(120)의 SMM은 스팸신고된 (송신단말기) 번호가 SB-DB에 존재하는지 확인하여(단계 208) 존재하는 경우 아무런 액션을 취하지 않고(단계 209) 존재하는 경우 상기 번호를 SB-DB에 저장한다(단

계 210).

<66> (3A) 수신단말기에 블랙리스트DB가 추가된 차단장치(제3항)

<67> 전술한 (1A)의 장치나 (1B)의 방법에 의하면 어떤 수신단말기 사용자에 의해서라도 spam신고되면 그 번호로부터의 수신단말기(110)에 대한 호연결요청은 모두 거부된다. 따라서 일반적으로는 non-spam이지만 특정 수신단말기(사용자)에게만 spam인 경우에 예기치 않게 타 수신단말기(사용자)에게 통화가 전혀 이루어지지 않는 현상이 발생할 수 있다. 이를 방지하기 위하여 특정 수신단말기(사용자)가 스팸으로 인식하는 정보를 수신단말기에 저장/관리하는 것이 바람직하다.

<68> 이를 위해 본 발명은 전술한 (1A)의 장치에 일부 구성요소와 기능을 추가한 장치를 제공한다. 즉 본 장치의 상기 단말기에는, 상기 연결제어모듈(121)에서 전달된 호연결 요청신호에 대하여, 상기 송신단말기 번호가 ① 하기 단말블랙리스트DB(112)에 존재하지 않는 경우 착신신호를 발하고, ② 존재하는 경우 호연결을 거부하며, 통화 후 스팸신고신호가 입력되면 이를 상기 단말측관리모듈(114)로 전달하는 통화제어모듈(111); 및 스팸 송신단말기 번호가 저장되는 단말블랙리스트DB(112);가 추가로 포함되며, 상기 단말측관리모듈(114)에는, 통화 후 스팸신고신호가 입력되면 송신단말기 번호를 상기 단말블랙리스트DB(112)에 저장하는 기능이 추가된다. 도 5에 관련 구성요소를 도시하였다.

<69> 단말블랙리스트DB(112)는, 수신단말기(110)에 위치하며 여기에 spam 송신단말기 번호가 저장/관리된다.

<70> 통화제어모듈(111)은, 수신단말기(110)에 위치하며, 다음과 같은 두 가지 기능을 수행한다. 첫째, 상기 연결제어모듈(121)에서 호연결 요청신호가 전달되면 상기 송신단말기 번호가 ① 단말블랙리스트DB(112)에 존재하지 않으면 벨소리 또는 진동 등과 같은 착신신호를 발하여 사용자가 전화를 받을 수 있도록 하고, ② 존재하면 호연결을 거부한다. 둘째, 상기 ①단계에서 전화를 받아 통화한 사용자로부터 스팸신고신호가 입력되면 이를 단말측관리모듈(114)로 전달한다.

<71> 본 장치에서 상기 단말측관리모듈(114)에는, 상기 통화제어모듈(111)로부터 스팸신고신호가 전달되면 송신단말기 번호를 단말블랙리스트DB(112)에 저장하는 기능이 추가된다.

<72> (3B) 단말기에 블랙트리스트 관리기능이 추가된 차단방법(제9항)

<73> 본 발명에 의한 스팸전화 차단방법은, 전술한 (3A)의 장치를 이용한 스팸전화 차단방법으로서, 상기 (1B) 방법의 단계 102와 104 사이에 TB-DB를 조회하는 순서(단계 301) 및 상기 단계 105와 107 사이에 스팸 번호를 TB-DB에 저장하는 순서(단계 303)이 추가된 것이다. 도 6에 상기 차단방법에 따른 작동단계의 흐름도를 도시하였다.

<74> 도시된 바와 같이, 상기 연결제어모듈(121)에서 호연결 요청신호가 전달되면 TB-DB에 송신단말기 번호가 존재하지 여부를 조회한다(단계 301). 상기 송신단말기 번호가 단말블랙리스트DB(112)에 존재하지 않으면 벨소리 또는 진동 등과 같은 착신신호를 발하여 사용자가 전화를 받을 수 있도록 하고(단계 104), 존재하면 호연결을 거부한다(단계 302).

<75> 또한 스팸신고신호가 입력되면(단계 105) 이를 단말측관리모듈(114)로 전달하여 상기 송신단말기 번호를 TB-DB에 저장한다(단계 303).

<76> 설명하지 않은 나머지 단계들의 기능과 작용은 상기 (1B) 방법과 동일하다.

<77> (4A) 수신단말기에 블랙리스트DB/화이트리스트DB가 추가된 차단장치(제4항)

<78> 전술한 (1A)의 장치나 (1B)의 방법에 의하면 개개의 수신단말기에 사용자가 non-spam이라고 정의한 번호, 예를 들면 사용자가 관리하는 사업상의 전화번호부 리스트 등을 적절히 취급할 여지가 없다. 따라서 수신단말기 사용자 개인이 수동으로 취급/관리할 수 있도록 하는 것이 바람직하다.

<79> 이를 위해 본 발명은 전술한 (3A)의 장치에 일부 구성요소와 기능을 추가한 장치를 제공한다. 즉 본 장치의 상기 단말기에는, (1) non-spam 송신단말기 번호가 저장되는 단말화이트리스트DB(113);가 추가로 포함되며, (2) 상기 통화제어모듈(111)에는, 연결제어모듈(121)에서 전달된 호연결 요청신호에 대하여, 상기 송신단말기 번호가 ① 단말화이트리스트DB(113)에 존재하는 경우 또는 단말블랙리스트DB(112)에 존재하지 않는 경우 착신신호를 발하고, ② 블랙리스트DB에 존재하는 경우 호연결을 거부하는 기능이 추가되고, (3) 상기 단말측관리모듈(114)에는, 통화 후 스팸신고신호가 입력되지 않으면 송신단말기 번호를 상기 단말화이트리스트DB(113)에 저장하는 기능이 추가된다. 도 5에 관련 구성요소를 도시하였다.

<80> 단말화이트리스트DB(113)에는, non-spam 송신단말기 번호, 예를 들면, 사용자가 단말에 수동입력한 '개인 전화번호부의 번호'가 저장된다.

<81> (4B) 단말기에 블랙트리스트/화이트리스트 관리기능이 추가된 차단방법(제10항)

<82> 본 발명에 의한 스팸전화 차단방법은, 전술한 (4A)의 장치를 이용한 스팸전화 차단방법으로서, 상기 (3B) 방법의 단계 102와 301 사이에 TW-DB를 조회하는 순서(단계 401) 및 TW-DB를 관리하는 순서(단계 402)가 추가된 것이다. 도 8에 상기 차단방법에 따른 작동단계의 흐름도를 도시하였다.

<83> 도시된 바와 같이, 상기 연결제어모듈(121)에서 호연결 요청신호가 전달되면 TW-DB에 송신단말기 번호가 존재하지 여부를 조회한다(단계 401). 상기 송신단말기 번호가 단말화이트리스트DB(113)에 존재하면 통화연결(착신신호를 발함)하고(단계 104), 존재하지 않으면 단말블랙리스트DB(112)를 조회하는 단계 304로 이동한다.

<84> 스팸신고신호 확인(단계 105) 전 또는 후에(도면에는 후에 이루어지는 케이스가 도시됨) 별도로 수신단말기(110) 사용자로 하여금 송신단말기 번호를 단말화이트리스트DB(113)(이는 개인 전화번호부일 수 있음)에 저장할 것인가를 질의하고(단계 402), 저장할 것이라는 신호가 입력되면 송신단말기 번호를 단말화이트리스트DB(113)에 저장하고(단계 403), 저장신호가 입력되지 않으면 아무런 조치를 취하지 않는다(단계 106).

<85> 한편, 통화 후 스팸신고신호가 입력되지 않으면, 상기 송신단말기 번호가 자동으로 단말화이트리스트DB(113)에 저장되도록 할 수도 있을 것이다(도시 생략).

<86> 설명하지 않은 나머지 단계들의 기능과 작용은 상기 (3B) 방법과 동일하다.

<87> 도시하지는 않았지만, 단말기 키입력에 의해 사용자가 TW-DB를 직접 관리할 수도 있을 것이다.

<88> (5A) pre-filter모듈이 추가된 차단장치(제5항 및 제6항)

<89> 통상 spam 전화는 spam mail과 마찬가지로, 대량으로 또한 무작위적으로 발송되므로 전달되는 정보는 사전에 녹음 또는 녹화된 일방향정보인 것이 일반적이다. 따라서 최초로 혹은 소정의 시간 간격만에 호연결 요청을 하는 송신단말기로부터의 정보가 일방향정보인지를 서버(120)에서 확인하여 spam으로 처리여부를 결정하는 것이 바람직하다.

<90> 이를 위해 본 발명은 전술한 (1A)~(3A)의 장치에 일방향정보를 구분할 수 있는 구성요소와 기능을 추가한 장치를 제공한다. 즉 본 장치의 상기 서버(120)에는, **(1)** 명백한 non-spam 송신단말기 번호 또는 통화연결되었던 송신단말기 번호 중 스팸신고되지 않은 번호가 저장되는 서버화이트리스트DB(124); 및 **(2)** 음성 혹은 영상 정보에 의한 질문을 생성하여 이를 송신단말기에 전달하여 답신을 요청하고, ① 정답이 반송되면 상기 송신단말기 번호를 non-spam으로 ② 답이 반송되지 않거나 오답이 반송되면 상기 송신단말기 번호를 spam으로 결정하여 상기 서버측관리모듈(125)에 전달하는 pre-filtering모듈(122);이 추가로 포함되며, **(3)** 상기 연결제어모듈(121)에는, 송신단말기 번호가 상기 서버블랙리스트DB(123) 및 서버화이트리스트DB(124) 모두에 존재하지 않는 경우, 상기 pre-filtering모듈(122)을 작동시키는 기능이 추가되며, **(4)** 상기 서버측관리모듈(125)에는 상기 pre-filtering모듈(122)로부터의 정보에 따라 상기 송신단말기 번호를 상기 서버화이트리스트DB(124) 또는 서버블랙리스트DB(123)에 저장하는 기능이 추가된다(제5항). 도 9에 관련 구성요소를 도시하였다.

<91> 서버화이트리스트DB(124)에는 스팸이라 판단하기 쉬운 non-spam 또는 non-spam이 명백한 송신단말기 번호가 사전에 입력되어 있거나, 과거 통화연결되었던 송신단말기 번호 중 스팸신고되지 않은 번호가 저장된다.

<92> pre-filtering모듈(122)은 송신단말기 번호가 상기 서버블랙리스트DB(123) 및 서버화이트리스트DB(124) 모두에 존재하지 않는 경우에 작동된다. PFM은 송신단말기가 기계적 장치에 의해 작동되고 정보를 전달하는지를 확인하기 사람이 인지할 수 있는 음성 혹은 영상에 의한 질문을 생성하고(이때, 송신단말기측이 기계적으로 질문을 인식하는 것을 방지하기 위하여 다양한 음성, 영상과 노이즈를 첨부시킬 수 있음) 이를 송신단말기에 전달하여 답신을 요청한다. 이어서 ① 정답이 반송되면 상기 송신단말기 번호를 non-spam으로, ② 답이 반송되지 않거나 오답이 반송되면 상기 송신단말기 번호를 spam으로 결정하여 상기 서버측관리모듈(125)에 전달하는 역할을 한다.

<93> 한편, 명백히 non-spam 송신단말기임에도 불구하고 수신단말기 사용자의 착오나 고의에 따른 스팸신고에 의해 SB-DB에 입력되는 것을 방지하기 위하여, 상기 서버측관리모듈(125)에는, 수신단말기(110)로부터 스팸신고가 된 송신단말기 번호가 상기 서버화이트리스트DB(124)에 존재하는 경우 스팸신고를 무시하는 기능이 추가되도록 하는 것이 바람직하다(제6항). 이 경우 관련 구성요소는 도 9와 동일하다.

<94> (5B) pre-filter 기능이 추가된 차단방법(제11항 및 제12항)

<95> 본 발명에 의한 스팸전화 차단방법은, 전술한 (5A)의 장치를 이용한 스팸전화 차단방법이다. 즉, 본 발명은 (A) 상기 서버(120)가 송신단말기의 호연결 요청을 받는 단계; (B) (B) 상기 송신단말기 번호가 ① 서버블랙리스트DB(123)에 존재하는 경우 호연결을 거부하고, ② 서버블랙리스트DB(123)에 존재하지 않으면서 서버화이트리스트DB(124)에 존재하는 경우 호연결 요청신호를 수신단말기(110)에 전달하고, ③ 서버블랙리스트DB(123) 및 서버화이트리스트DB(124) 모두에 존재하지 않는 경우, 음성 혹은 영상으로 질문을 생성하여 이를 송신단말기에 전달하여 답신을 요청하고, □ 정답이 반송되면 상기 송신단말기 번호를 서버화이트리스트DB(124)에 저장하고 호연결 요청신호를 수신단말기(110)에 전달하며, □ 답이 반송되지 않거나 오답이 반송되면 상기 송신단말기 번호를 서버블랙리스트DB(123)에 저장하고 호연결을 거부하는 단계; 및 (C) 수신단말기(110)로부터 스팸신고신호가 전달되면 송신단말기 번호 또는 송신단말기 번호와 스팸신고 시점을 서버블랙리스트DB(123)에 저장하는 단계;를 포함하는 스팸전화 차단방법이다. 도 4에 상기 차단방법에 따른 작동단계의 흐름도를 도시하였다.

<96> 먼저, 단계(501)에서 서버(120)는 송신단말기로부터 수신자단말기로의 호(통화) 연결 요청을 받는다.

<97> 이어서 상기 서버(120)는 SB-DB를 조회하여 송신단말기의 호연결 요청을 거부할 것인지를 결정한다(단계 502). 만일 송신단말기의 번호가 SB-DB에 존재하면 호연결을 거부하고(단계 503), 존재하지 않으면 SW-DB를 조회하는 단계 504로 이동한다.

<98> SW-DB를 조회하여(단계 504) 송신단말기의 번호가 SW-DB에 존재하면 호연결 신호를 수신단말기(110)로 전달하고, 존재하지 않으면 다음 단계 505로 이동한다.

<99> 단계 505는 pre-filtering 단계로서, 음성 혹은 영상으로 질문을 생성하여 이를 송신단말기에 전달하여 답신을 요청하여 정답이 반송되는지, 답이 반송되지 않거나 오답이 반송되는지를 확인한다. 정답이 반송되면 상기 송신단말기 번호를 서버화이트리스트DB(124)에 저장하고(단계 506) 호연결 요청신호를 수신단말기(110)에 전달하며, 답이 반송되지 않거나 오답이 반송되면 상기 송신단말기 번호를 서버블랙리스트DB(123)에 저장하고(단계 107) 호연결을 거부한다(단계 503).

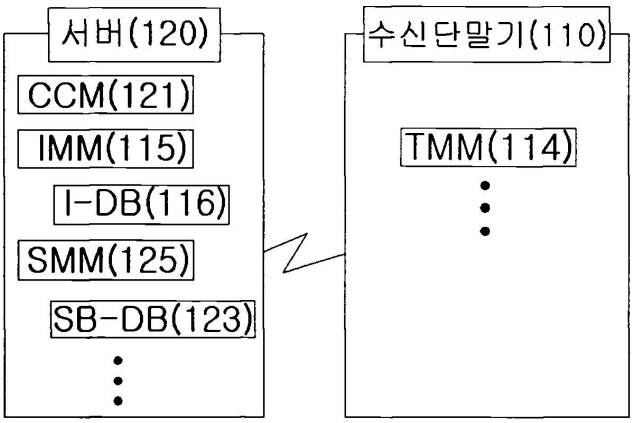
<100> 단계 504 또는 506에서 호연결 요청신호를 전달받은 수신단말기(110)에서 진행되는 흐름은 (4B)의 방법에서 수신단말기(110)에서 진행되는 흐름과 동일하다. 따라서 추가적인 설명을 생략한다. (이상 제11항에 대한 설명)

<101> 한편, 스팸신고를 무시하는 기능이 추가된 장치(제6항)를 이용한 스팸 차단방법(제12항)의 작용흐름도를 도 11에 도시하였다.

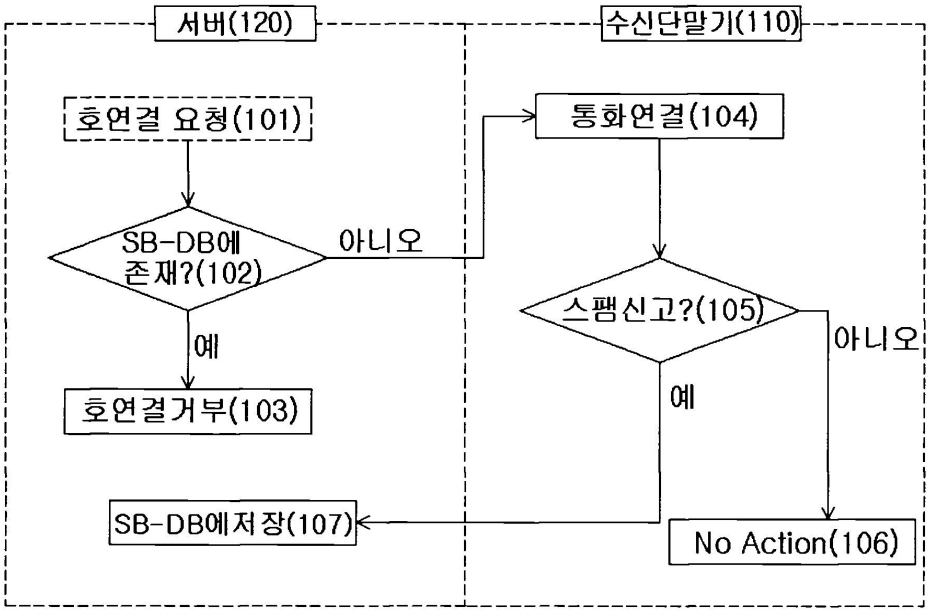
<102> 상기 도 10의 단계 105와 단계 107 사이에 도 4에 도시된 단계 208, 209 및 210이 추가된다는 점 외에는 상기 도 10와 동일하다. 즉, 스팸신고신호를 전달받은 서버(120)의 SMM은 스팸신고된 (송신단말기) 번호가 SB-DB에 존재하는지 확인하여(단계 208) 존재하는 경우 아무런 액션을 취하지 않고(단계 209) 존재하는 경우 상기 번호를 SB-DB에 저장한다(단계 107).

도면

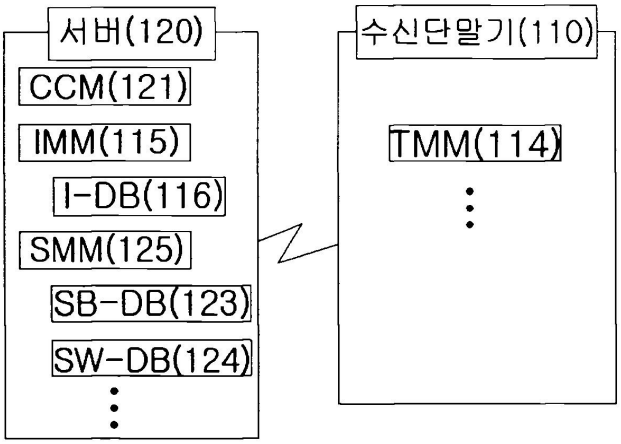
도면1



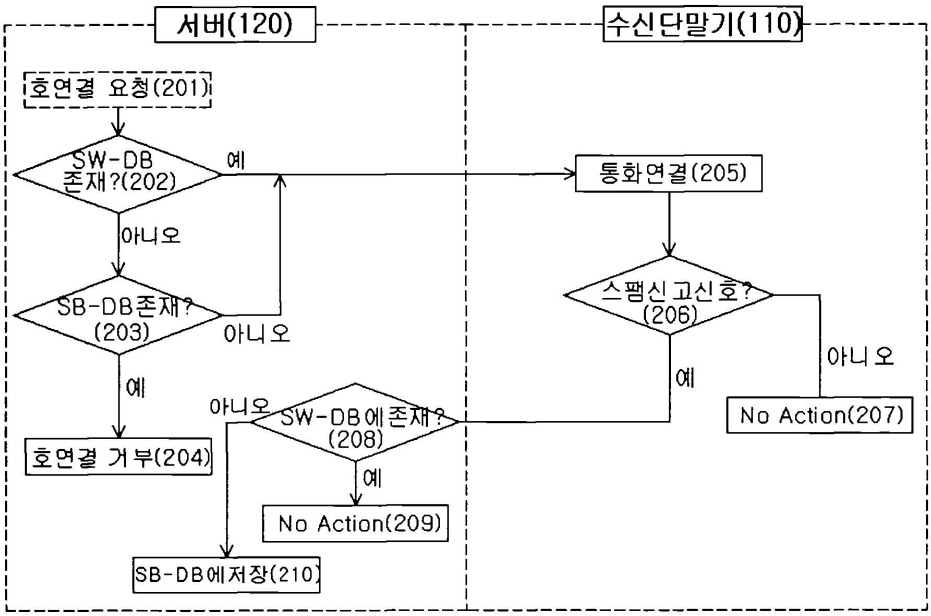
도면2


서버(120)
수신단말기(110)
호연결 요청(101)
SB-DB에 존재?(102)
아니오
예
호연결거부(103)
통화연결(104)
스팸신고?(105)
아니오
예
No Action(106)
SB-DB에저장(107)

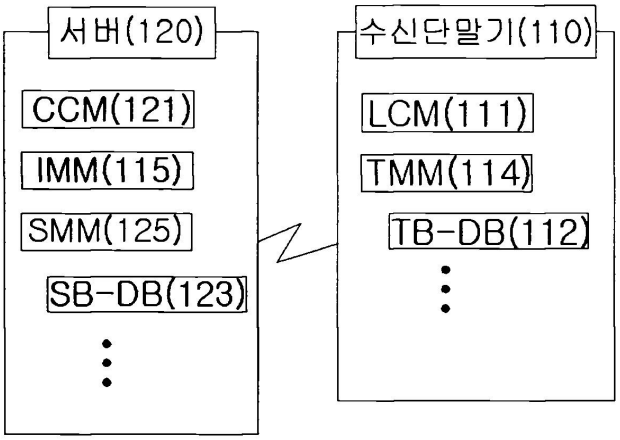
도면3


서버(120)
CCM(121)
IMM(115)
I-DB(116)
SMM(125)
SB-DB(123)
SW-DB(124)
수신단말기(110)
TMM(114)

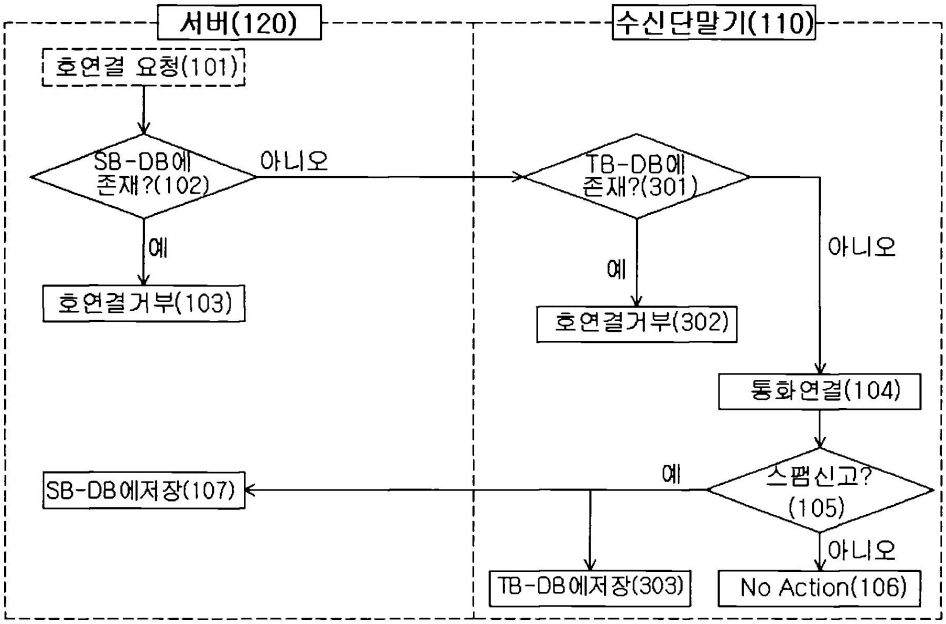
도면4


서버(120)
수신단말기(110)
호연결 요청(201)
SW-DB 존재?(202)
예
통화연결(205)
아니오
SB-DB존재? (203)
아니오
스팸신고신호? (206)
아니오
예
No Action(207)
아니오
SW-DB에존재? (208)
예
호연결 거부(204)
No Action(209)
SB-DB에저장(210)

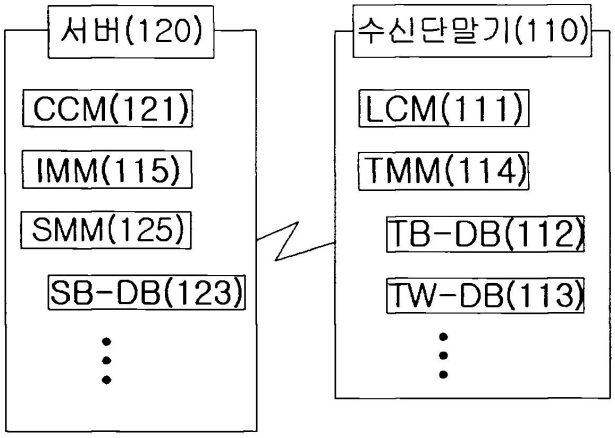
도면5


서버(120)
CCM(121)
IMM(115)
SMM(125)
SB-DB(123)
수신단말기(110)
LCM(111)
TMM(114)
TB-DB(112)

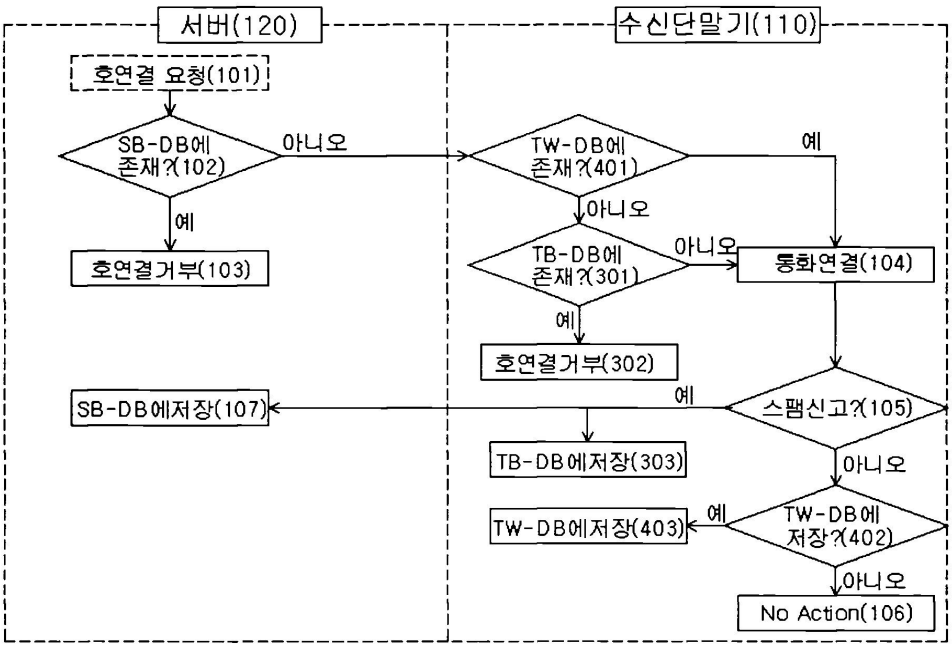
도면6


서버(120)
수신단말기(110)
호연결 요청(101)
SB-DB에 존재?(102)
아니오
예
호연결거부(103)
TB-DB에 존재?(301)
예
호연결거부(302)
아니오
통화연결(104)
스팸신고?(105)
예
SB-DB에저장(107)
아니오
TB-DB에저장(303)
No Action(106)

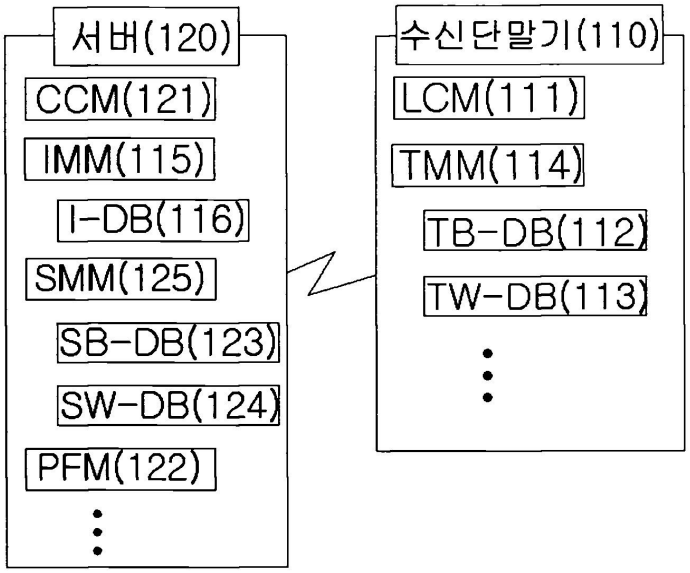
도면7


서버(120)
CCM(121)
IMM(115)
SMM(125)
SB-DB(123)
수신단말기(110)
LCM(111)
TMM(114)
TB-DB(112)
TW-DB(113)

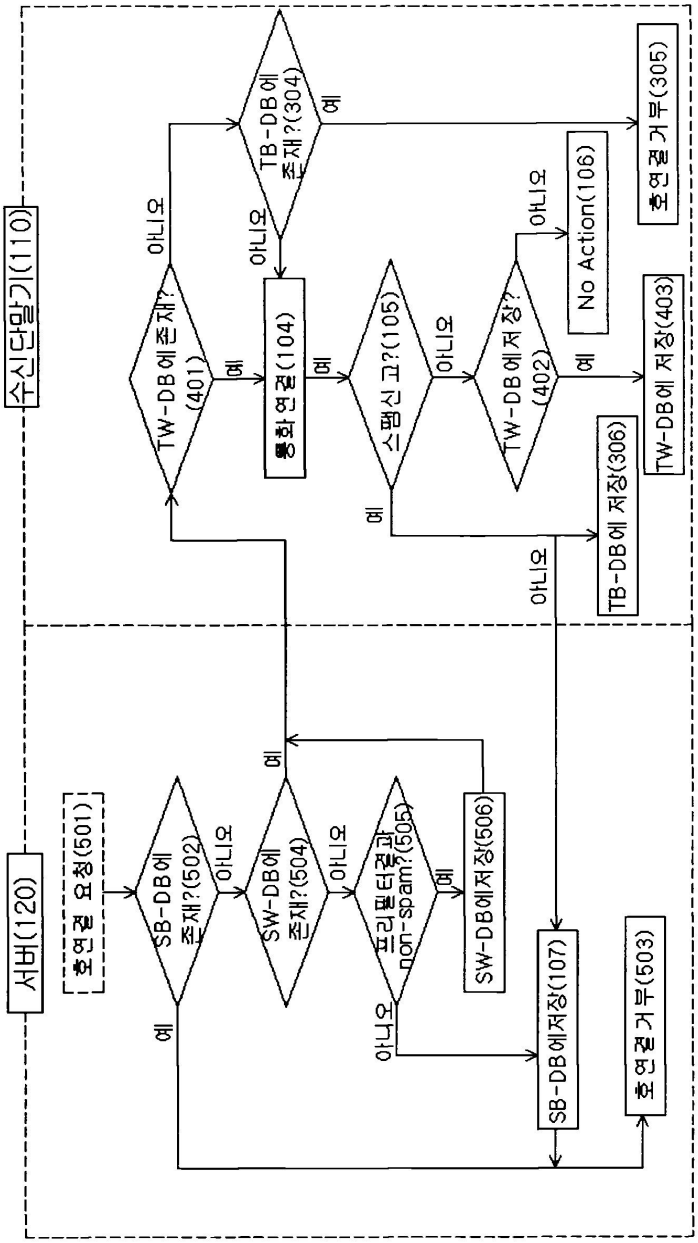
도면8


서버(120)
수신단말기(110)
호연결 요청(101)
SB-DB에 존재?(102)
아니오
예
호연결거부(103)
TW-DB에 존재?(401)
예
아니오
TB-DB에 존재?(301)
아니오
통화연결(104)
예
호연결거부(302)
SB-DB에저장(107)
예
스팸신고?(105)
TB-DB에저장(303)
아니오
TW-DB에저장(403)
예
TW-DB에 저장?(402)
아니오
No Action(106)

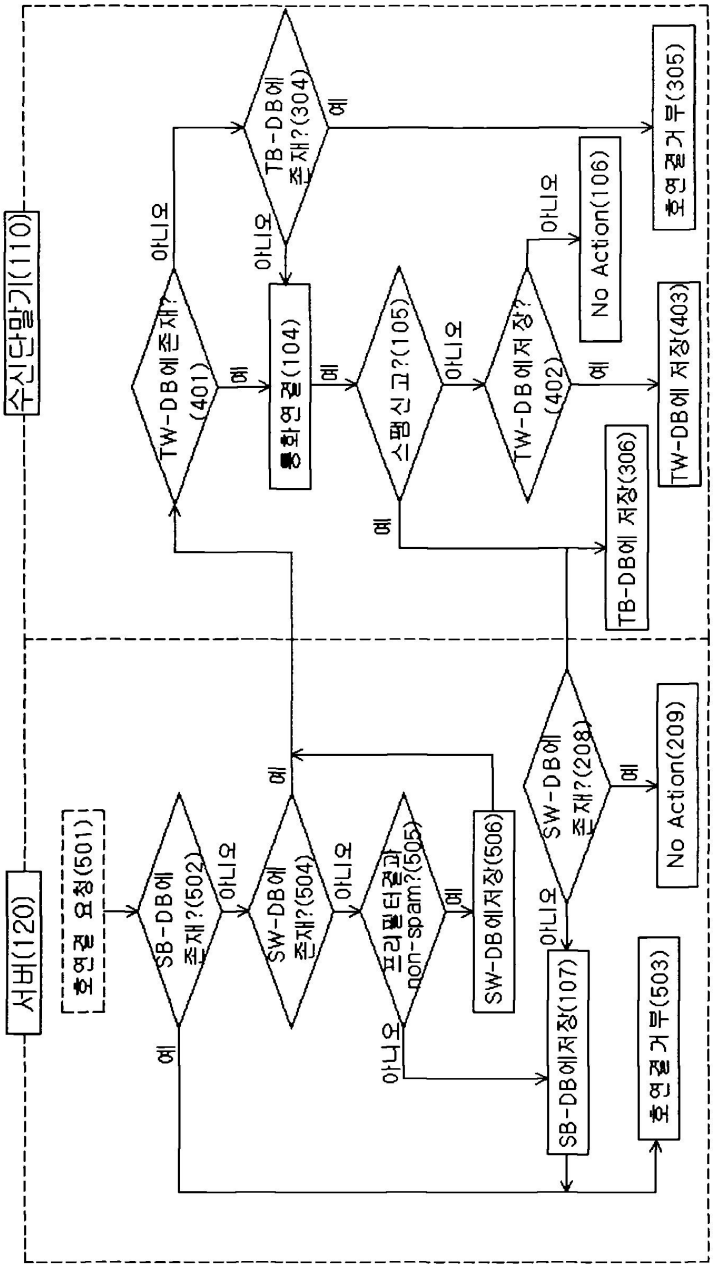
도면9


서버(120)
CCM(121)
IMM(115)
I-DB(116)
SMM(125)
SB-DB(123)
SW-DB(124)
PFM(122)
수신단말기(110)
LCM(111)
TMM(114)
TB-DB(112)
TW-DB(113)

도면10


수신단말기(110)
서버(120)
호연결 요청(501)
SB-DB에 존재?(502)
아니오
예
SW-DB에 존재?(504)
아니오
예
프리폰터결과 non-spam?(505)
아니오
예
SW-DB에저장(506)
SB-DB에저장(107)
호연결거부(503)
TW-DB에 존재?(401)
아니오
예
통화연결(104)
스팸신고?(105)
아니오
예
TW-DB에 저장?(402)
아니오
No Action(106)
예
TW-DB에 저장(403)
TB-DB에 저장(306)
TB-DB에 존재?(304)
아니오
예
호연결거부(305)

도면11


수신단말기(110)
서버(120)
호연결 요청(501)
SB-DB에 존재?(502)
아니오
예
SW-DB에 존재?(504)
아니오
예
프리필터결과 non-spam?(505)
아니오
예
SW-DB에저장(506)
SW-DB에 존재?(208)
예
No Action(209)
아니오
SB-DB에저장(107)
호연결거부(503)
TW-DB에 존재? (401)
아니오
예
통화연결(104)
스팸신고?(105)
아니오
예
TW-DB에저장? (402)
아니오
No Action(106)
예
TW-DB에 저장(403)
TB-DB에 저장(306)
TB-DB에 존재?(304)
아니오
예
호연결거부(305)