(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2016년05월10일
(11) 등록번호 10-1619347
(24) 등록일자 2016년05월02일

(51) 국제특허분류(Int. Cl.)
*H04W 4/14* (2009.01) *G08B 21/02* (2006.01)
(21) 출원번호 10-2014-0046480
(22) 출원일자 2014년04월18일
심사청구일자 2014년04월18일
(65) 공개번호 10-2015-0120651
(43) 공개일자 2015년10월28일
(56) 선행기술조사문헌
KR1020130115018 A*
KR1020100086394 A*
KR1020130035572 A*
KR1020130053021 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
**주식회사 수산아이앤티**
서울특별시 강남구 밤고개로1길 10, 3층(수서동, 현대벤처빌)
(72) 발명자
**천세은**
서울시 강남구 밤고개로1길 10, 3층(수서동, 현대벤처빌)
**이용규**
서울시 강남구 밤고개로1길 10, 3층(수서동, 현대벤처빌)
*(뒷면에 계속)*
(74) 대리인
**특허법인 아이스퀘어**

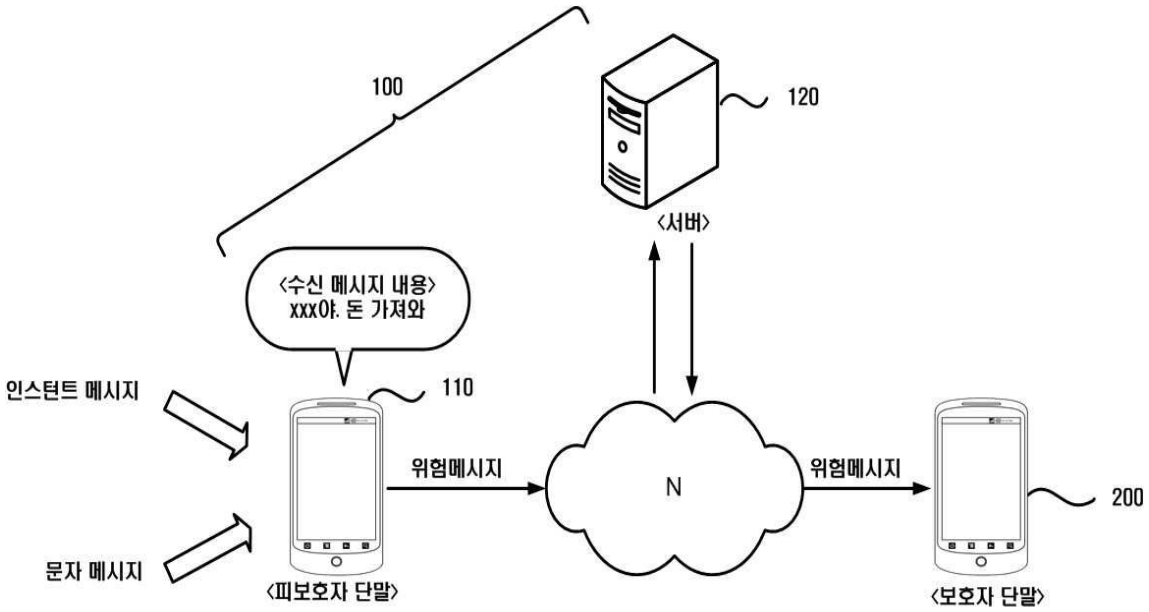
전체 청구항 수 : 총 19 항 심사관 : 김대일

(54) 발명의 명칭 **피보호자 안심 서비스 제공방법, 피보호자 안심 서비스 제공을 위한 위험메시지 감시 장치, 보호자 단말 및 컴퓨터 판독가능 기록매체**

## (57) 요 약

본 발명의 일실시예는 피보호자에게 수신된 위험메시지를 감시함으로써, 보호자로 하여금 피보호자의 위험상황(예를 들어, 학교폭력)을 미리 예측하거나 감지하게 할 수 있다. 특히, 본 발명의 일 실시예는 위험메시지를 발신한 가해자에 대한 이름이나 연락처 정보 및/또는 가해자와 연관된 다른 피보호자들의 이름이나 연락처 정보를 제공함으로써, 보호자가 가해자의 정보 및 가해자의 가해정보를 미리 알 수 있도록 하되, 이름이나 연락처 등의 무분별한 개인정보 노출을 고려하여 이름이나 연락처의 일부만을 보호자에게 보여줄 수 있다. 또한, 본 발명의 일 실시예는 피보호자가 수신한 위험메시지를 피보호자의 학교 단말로 송부하여 학교측에서도 위험상황이나 가해자의 정보를 미리 알 수 있도록 할 수 있으며, 위험메시지에 포함된 위험 단어가 농담과 같은 성격을 갖는 경우 필터링하여 보호자에게 제공할 수도 있다.

*대 표 도* - 도1



(72) 발명자

**이창배**

서울시 강남구 밤고개로1길 10, 3층(수서동, 현대벤처빌)

**강경태**

서울시 강남구 밤고개로1길 10, 3층(수서동, 현대벤처빌)

# 명 세 서

## 청구범위

### 청구항 1

(a) 위험메시지 감시 장치에서, 피보호자에게 발송된 메시지를 수신하는 단계;

(b) 상기 위험메시지 감시 장치에서, 상기 위험메시지 감시 장치의 메시지 저장영역 또는 애플리케이션 상태정보 저장영역을 참조하여 상기 수신된 메시지를 인식하는 단계;

(c) 상기 위험메시지 감시 장치에서, 상기 수신된 메시지와 미리 저장된 위험단어 리스트를 비교하여, 상기 수신된 메시지에 위험단어가 포함되어 있는지 판단하는 단계;

(d) 상기 위험메시지 감시 장치에서, 상기 수신된 메시지가 상기 위험단어를 포함한 위험메시지인 것으로 판단된 경우, 상기 위험메시지의 발신식별정보를 통하여 상기 위험메시지의 발신자의 이름 또는 발신자의 연락처를 추출하는 단계;

(e) 상기 위험메시지 감시 장치에서, 상기 피보호자에 대응하는 보호자의 단말로 상기 위험메시지와 상기 발신자의 이름 또는 연락처를 전송하는 단계; 및

(f) 상기 보호자의 단말에서, 상기 전송된 위험메시지와 상기 발신자의 이름의 일부나 연락처의 일부를 표시하는 단계를 포함하고,

상기 (d)단계는,

(k) 두 명 이상의 서로 다른 발신자로부터 각각 위험메시지가 상기 위험메시지 감시 장치에 수신된 경우, 상기 위험메시지 감시 장치에서, 상기 각 발신자의 위험메시지의 내용을 참조하여 상기 각 발신자 간의 연관성 유무를 제공하는 단계를 더 포함하는, 피보호자 안심 서비스 제공방법.

### 청구항 2

제 1 항에 있어서,

상기 피보호자 안심 서비스 제공방법은,

(g) 상기 (a)단계 전, 상기 위험메시지 감시 장치에 포함되는 상기 피보호자의 단말에 피보호자 안심 애플리케이션이 설치되고, 상기 피보호자의 단말의 상기 애플리케이션 상태정보 저장영역에 대한 상기 피보호자 안심 애플리케이션의 접근권한이 부여되는 단계를 더 포함하는, 피보호자 안심 서비스 제공방법.

### 청구항 3

제 2 항에 있어서,

상기 (b) 단계는,

상기 메시지 저장영역을 참조하여 SMS 또는 MMS 메시지를 인식하거나, 상기 애플리케이션 상태정보 저장영역을 참조하여 상기 피보호자의 단말에 설치된 채팅 애플리케이션으로 수신된 채팅 메시지를 인식하는 단계를 포함하는, 피보호자 안심 서비스 제공방법.

### 청구항 4

제 1 항에 있어서,

상기 (d) 단계는,

상기 수신된 메시지가 상기 위험메시지인 것으로 판단된 경우, 상기 위험메시지의 발신식별정보로부터 상기 위험메시지의 발신자의 연락처를 추출하는 단계; 및

상기 위험메시지의 발신자의 연락처에 대응하는 이름이 상기 위험메시지 감시 장치에 등록되어 있는 경우, 상기

등록된 이름으로부터 상기 발신자의 이름을 추출하는 단계;

를 포함하는, 피보호자 안심 서비스 제공방법.

**청구항 5**

제 4 항에 있어서,

상기 (e) 단계는,

상기 위험메시지 감시 장치에서, 상기 발신자의 이름의 일부 또는 연락처의 일부를 마스킹하여 전송하는, 피보호자 안심 서비스 제공방법.

**청구항 6**

제 4 항에 있어서,

상기 (f) 단계는,

상기 보호자의 단말에서, 상기 수신된 발신자의 이름의 일부 또는 연락처의 일부를 마스킹하여 표시하는, 피보호자 안심 서비스 제공방법.

**청구항 7**

제 1 항에 있어서,

상기 (d) 단계는,

상기 위험메시지가 상기 애플리케이션 상태정보 저장영역을 통하여 인식된 경우, 상기 애플리케이션 상태정보 저장영역으로 나타난 대화상대의 이름을 통하여 상기 발신자의 이름을 추출하는 단계를 포함하는, 피보호자 안심 서비스 제공방법.

**청구항 8**

제 1 항에 있어서,

상기 (e) 단계는, 상기 위험메시지 감시 장치에서,

상기 발신자의 이름 또는 연락처와 상기 피보호자 단말의 정보를 저장하는 단계; 및

상기 저장된 발신자의 이름 또는 연락처를 통하여, 상기 발신자로부터 위험메시지를 수신한 다른 피보호자를 검색하고, 상기 다른 피보호자의 정보를 상기 발신자의 이름 또는 연락처와 함께 상기 보호자 단말로 전송하는 단계;

를 포함하는, 피보호자 안심 서비스 제공방법.

**청구항 9**

제 8 항에 있어서,

상기 (f) 단계는,

상기 다른 피보호자의 정보 중 상기 다른 피보호자의 이름의 일부나 연락처의 일부를 상기 발신자의 이름의 일부나 연락처의 일부와 함께 제공하는 단계를 포함하는, 피보호자 안심 서비스 제공방법.

**청구항 10**

제 1 항에 있어서,

상기 피보호자 안심 서비스 제공방법은,

(i) 상기 (e) 단계 후, 상기 위험메시지와 상기 위험메시지의 발신자의 이름이나 연락처를 상기 피보호자의 학교 단말로 전송하는 단계를 더 포함하는, 피보호자 안심 서비스 제공방법.

**청구항 11**

제 1 항에 있어서,

상기 미리 저장된 위험단어 리스트에 포함된 위험 단어는,

폭력성, 협박성, 유해성 중 적어도 하나에 따라 복수의 서로 다른  위험등급이 지정되어 있는, 피보호자 안심 서비스 제공방법.

**청구항 12**

제 11 항에 있어서,

상기 피보호자 안심 서비스 제공방법은,

(j) 상기 위험메시지 감시 장치 또는 상기 보호자 단말에서, 상기 위험메시지의 발신자가 발신한 위험메시지의 총 개수, 위험메시지에 포함된 위험단어의 개수, 위험메시지에 포함된 위험단어의 위험등급 중 적어도 하나에 따라, 상기 발신자의 위험도를 제공하는 단계를 더 포함하는, 피보호자 안심 서비스 제공방법.

**청구항 13**

삭제

**청구항 14**

제 1 항에 있어서,

상기 피보호자 안심 서비스 제공방법은, 상기 위험메시지 감시 장치에서,

(1-1) 상기 (c) 단계 후, 상기 수신된 메시지에 위험단어가 포함되어 있는 것으로 판단된 경우, 상기 위험단어가 폭력이나 협박성 단어인지 농담이나 친근감 표시성 단어인지 구분하는 단계; 및

(1-2) 상기 위험단어가 폭력이나 협박성 단어인 경우, 상기 수신된 메시지를 상기 위험메시지인 것으로 판단하는 단계;

를 더 포함하는, 피보호자 안심 서비스 제공방법.

**청구항 15**

제1항 내지 제12항 및 제14항 중 어느 한 항에 따르는 방법을 구현하기 위한 프로그램 명령어가 기록된, 피보호자 안심 서비스 제공을 위한 컴퓨터 판독가능한 기록매체.

**청구항 16**

피보호자에게 발송된 메시지를 수신하는 메시지 수신부;

메시지 저장영역 또는 애플리케이션 상태정보 저장영역을 참조하여 상기 수신된 메시지를 인식하는 메시지 인식부;

상기 수신된 메시지와 미리 저장된 위험단어 리스트를 비교하여, 상기 수신된 메시지에 위험단어가 포함되어 있는지 판단하는 위험메시지 판단부;

상기 수신된 메시지가 상기 위험단어를 포함한 위험메시지인 것으로 판단된 경우, 상기 위험메시지의 발신식별정보를 통하여 상기 위험메시지의 발신자의 이름 또는 발신자의 연락처를 추출하는 발신자 정보 추출부;

상기 피보호자에 대응하는 보호자의 단말로 상기 위험메시지와 상기 발신자의 이름 또는 발신자의 연락처를 전송하는 위험정보 전송부; 및

두 명 이상의 서로 다른 발신자로부터의 위험메시지가 수신된 경우, 상기 각 발신자의 위험메시지의 내용을 참조하여 상기 각 발신자 간의 연관성 유무를 제공하는 발신자 연관성 판단부를 포함하는, 피보호자 안심 서비스 제공을 위한 위험메시지 감시 장치.

**청구항 17**

제 16 항에 있어서,

상기 위험메시지 감시 장치는,

상기 피보호자에게 발송된 메시지를 수신하기 전, 상기 위험메시지 감시 장치에 포함되는 상기 피보호자 단말에 설치된 피보호자 안심 애플리케이션으로 상기 피보호자 단말의 애플리케이션 상태정보 저장영역에 대한 접근권한을 설정하는 접근권한 설정부를 더 포함하는, 피보호자 안심 서비스 제공을 위한 위험메시지 감시 장치.

**청구항 18**

제 16 항에 있어서,

상기 메시지 인식부는,

상기 메시지 저장영역을 참조하여 SMS 또는 MMS 메시지를 인식하거나, 상기 애플리케이션 상태정보 저장영역을 참조하여 상기 피보호자의 단말에 설치된 채팅 애플리케이션으로 수신된 채팅 메시지를 인식하는, 피보호자 안심 서비스 제공을 위한 위험메시지 감시 장치.

**청구항 19**

제 16 항에 있어서,

상기 위험정보 전송부는,

상기 발신자의 이름의 일부 또는 연락처의 일부를 마스킹하여 전송하는, 피보호자 안심 서비스 제공을 위한 위험메시지 감시 장치.

**청구항 20**

제 16 항에 있어서,

상기 위험메시지 감시 장치는,

상기 발신자의 이름 또는 연락처와 상기 피보호자 단말의 정보를 저장하고, 상기 저장된 발신자의 이름 또는 연락처를 통하여 상기 발신자로부터 위험메시지를 수신한 다른 피보호자를 검색하며, 상기 다른 피보호자의 정보를 상기 발신자의 이름 또는 연락처와 함께 상기 보호자 단말로 전송하는 발신자 가해정보 추출부를 더 포함하는, 위험메시지 감시 장치.

**청구항 21**

삭제

**청구항 22**

삭제

**청구항 23**

삭제

## *발명의 설명*

### *기 술 분 야*

[0001] 본 발명은 피보호자 안심 서비스 제공방법, 피보호자 안심 서비스 제공을 위한 위험메시지 감시 장치, 보호자 단말 및 컴퓨터 판독가능 기록매체에 관한 것으로, 보다 상세하게는 피보호자에게 수신되는 유해 메시지, 폭력 메시지 등을 감시하고 위험상황을 미리 차단하기 위한 피보호자 안심 서비스 제공방법, 피보호자 안심 서비스 제공을 위한 위험메시지 감시 장치, 보호자 단말 및 컴퓨터 판독가능 기록매체에 관한 것이다.

### *배 경 기 술*

[0002] 최근 들어, 날이 갈수록 학교폭력 문제가 심화되고 심각한 사회문제로 부상하고 있다. 특히 이러한 학교폭력은

학생의 학부모에게 알려지지 않는 경우가 많아서, 학부모의 입장에서는 학교폭력 사건이 심화되고 나서야 알게 되는 경우가 많다.

[0003] 이러한 학교폭력에 대하여 각 학교마다 학생들의 폭력, 고민, 왕따, 학교에 대한 불만사항을 신고하도록 신고함이 교내 출입구나 복도에 설치되어 있으나, 이는 교사가 순찰하여 신고함을 열어 확인해야 하므로 학생이 편지를 신고함에 투입, 신고하더라도 신고한 사실을 즉시 알지 못하여 학생들의 애로사항을 신속하게 해결해 주지 못하고 있다. 이처럼 기존에는 신고함을 제대로 활용하지 못하였기에 현재 이 신고함은 방치되고 있는 실정이다.

[0004] 이에, 전화를 이용하여 학생들의 애로사항을 직접 교장실이나 교무실에 신고하는 방법도 있으나, 이는 직접 학생이 교사에게 말로써 신고해야 하기 때문에 학생의 입장이 난처하여 전화신고를 기피하고 있다. 이에 따라, 학생들의 애로사항을 해결하지 못하여 학교의 폭력, 가출, 왕따 등의 생활문제 사고는 날로 증가되고 있다.

[0005] 한편, 국내공개특허공보 제10-2013-0119551호는 학생들의 위치와 영상을 실시간으로 확보하여 학교 폭력을 방지하기 위한 구성들이 개시되어 있으나, CCTV와 같은 영상장치가 배치되지 않은 사각지대에서 학교 폭력이 발생하는 경우, 이를 방지할 수 없다는 측면에서 한계가 있다.

[0006] 한편, 전술한 배경기술은 발명자가 본 발명의 도출을 위해 보유하고 있었거나, 본 발명의 도출 과정에서 습득한 기술 정보로서, 반드시 본 발명의 출원 전에 일반 공중에게 공개된 공지기술이라 할 수는 없다.

## 발명의 내용

### 해결하려는 과제

[0007] 따라서, 본 발명의 일 실시예는 상술한 문제점을 해결하기 위하여, 피보호자(예를 들어, 자녀)에게 수신되는 문자를 감시하고, 수신되는 문자에 위험단어(예를 들어, 학교폭력 단어)가 있는 것으로 판단되는 경우, 보호자에게 이러한 사실을 알림으로써 피보호자에게 일어날 수 있는 위험상황을 방지하는 데에 목적이 있다.

[0008] 또한, 본 발명의 일실시예는 피보호자의 가해자에 대한 부가 정보나 가해자와 연관된 다른 피보호자들의 정보를 제공함으로써, 해당 가해자에 대한 학교폭력의 심각성을 보호자가 쉽게 알 수 있게 하는 데에 목적이 있다.

[0009] 또한, 본 발명의 일 실시예는 피보호자가 위험메시지가 수신될 경우, 이를 피보호자의 학교 단말로 전송하여, 학교 측에서도 위험상황을 인지할 수 있도록 하는 데에 목적이 있다.

[0010] 또한, 본 발명의 일 실시예는 가해자의 위험도를 판단하여, 보호자에게 이러한 위험도를 알려줌으로써 위험상황의 경중을 예측할 수 있도록 하거나, 농담이나 친근감 표시성의 위험단어는 필터링함으로써 보호자에게 필요한 위험정보만을 알리는 것을 목적으로 한다.

### 과제의 해결 수단

[0011] 상술한 기술적 과제를 달성하기 위한 기술적 수단으로서, 본 발명의 제 1 측면에 따르면, 피보호자 안심 서비스 제공방법은 (a) 위험메시지 감시 장치에서, 피보호자에게 발송된 메시지를 수신하는 단계; (b) 상기 위험메시지 감시 장치에서, 상기 위험메시지 감시 장치의 메시지 저장영역 또는 애플리케이션 상태정보 저장영역을 참조하여 상기 수신된 메시지를 인식하는 단계; (c) 상기 위험메시지 감시 장치에서, 상기 수신된 메시지와 미리 저장된 위험단어 리스트를 비교하여, 상기 수신된 메시지에 위험단어가 포함되어 있는지 판단하는 단계; (d) 상기 위험메시지 감시 장치에서, 상기 수신된 메시지가 상기 위험단어를 포함한 위험메시지인 것으로 판단된 경우, 상기 위험메시지의 발신식별정보를 통하여 상기 위험메시지의 발신자의 이름 또는 발신자의 연락처를 추출하는 단계; (e) 상기 위험메시지 감시 장치에서, 상기 피보호자에 대응하는 보호자의 단말로 상기 위험메시지와 상기 발신자의 이름 또는 연락처를 전송하는 단계; 및 (f) 상기 보호자의 단말에서, 상기 전송된 위험메시지와 상기 발신자의 이름의 일부나 연락처의 일부를 표시하는 단계;를 포함한다.

[0012] 또한, 상기 피보호자 안심 서비스 제공방법은, (g) 상기 (a)단계 전, 상기 위험메시지 감시 장치에 포함되는 상기 피보호자의 단말에 피보호자 안심 애플리케이션이 설치되고, 상기 피보호자의 단말의 상기 애플리케이션 상태정보 저장영역에 대한 상기 피보호자 안심 애플리케이션의 접근권한이 부여되는 단계를 더 포함한다.

[0013] 또한, 상기 (b) 단계는, 상기 메시지 저장영역을 참조하여 SMS 또는 MMS 메시지를 인식하거나, 상기 애플리케이

션 상태정보 저장영역을 참조하여 상기 피보호자의 단말에 설치된 채팅 애플리케이션으로 수신된 채팅 메시지를 인식하는 단계를 포함한다.

[0014] 또한, 상기 (d) 단계는, 상기 수신된 메시지가 상기 위험메시지인 것으로 판단된 경우, 상기 위험메시지의 발신식별정보로부터 상기 위험메시지의 발신자의 연락처를 추출하는 단계; 및 상기 위험메시지의 발신자의 연락처에 대응하는 이름이 상기 위험메시지 감시 장치에 등록되어 있는 경우, 상기 등록된 이름으로부터 상기 발신자의 이름을 추출하는 단계;를 포함한다.

[0015] 또한, 상기 (e) 단계는, 상기 위험메시지 감시 장치에서, 상기 발신자의 이름의 일부 또는 연락처의 일부를 마스킹하여 전송한다.

[0016] 또한, 상기 (f) 단계는, 상기 보호자의 단말에서, 상기 수신된 발신자의 이름의 일부 또는 연락처의 일부를 마스킹하여 표시한다.

[0017] 또한, 상기 (d) 단계는, 상기 위험메시지가 상기 애플리케이션 상태정보 저장영역을 통하여 인식된 경우, 상기 애플리케이션 상태정보 저장영역으로 나타난 대화상대의 이름을 통하여 상기 발신자의 이름을 추출하는 단계를 포함한다.

[0018] 또한, 상기 (e) 단계는, 상기 위험메시지 감시 장치에서, 상기 발신자의 이름 또는 연락처와 상기 피보호자 단말의 정보를 저장하는 단계; 및 상기 저장된 발신자의 이름 또는 연락처를 통하여, 상기 발신자로부터 위험메시지를 수신한 다른 피보호자를 검색하고, 상기 다른 피보호자의 정보를 상기 발신자의 이름 또는 연락처와 함께 상기 보호자 단말로 전송하는 단계;를 포함한다.

[0019] 또한, 상기 (f) 단계는, 상기 다른 피보호자의 정보 중 상기 다른 피보호자의 이름의 일부나 연락처의 일부를 상기 발신자의 이름의 일부나 연락처의 일부와 함께 제공하는 단계를 포함한다.

[0020] 또한, 상기 피보호자 안심 서비스 제공방법은, (i) 상기 (e) 단계 후, 상기 위험메시지와 상기 위험메시지의 발신자의 이름이나 연락처를 상기 피보호자의 학교 단말로 전송하는 단계를 더 포함한다.

[0021] 또한, 상기 미리 저장된 위험단어 리스트에 포함된 위험 단어는, 폭력성, 협박성, 유해성 중 적어도 하나에 따라 복수의 서로 다른 위험등급이 지정되어 있을 수 있다.

[0022] 또한, 상기 피보호자 안심 서비스 제공방법은, (j) 상기 위험메시지 감시 장치 또는 상기 보호자 단말에서, 상기 위험메시지의 발신자가 발신한 위험메시지의 총 개수, 위험메시지에 포함된 위험단어의 개수, 위험메시지에 포함된 위험단어의 위험등급 중 적어도 하나에 따라, 상기 발신자의 위험도를 제공하는 단계를 더 포함한다.

[0023] 또한, 상기 피보호자 안심 서비스 제공방법은, (k) 두 명 이상의 서로 다른 발신자로부터 각각 위험메시지가 상기 위험메시지 감시 장치에 수신된 경우, 상기 위험메시지 감시 장치에서, 상기 각 발신자의 위험메시지의 내용을 참조하여 상기 각 발신자 간의 연관성 유무를 제공하는 단계를 더 포함한다.

[0024] 또한, 상기 피보호자 안심 서비스 제공방법은, 상기 위험메시지 감시 장치에서, (l-1) 상기 (c) 단계 후, 상기 수신된 메시지에 위험단어가 포함되어 있는 것으로 판단된 경우, 상기 위험단어가 폭력이나 협박성 단어인지 농담이나 친근감 표시성 단어인지 구분하는 단계; 및 (l-2) 상기 위험단어가 폭력이나 협박성 단어인 경우, 상기 수신된 메시지를 상기 위험메시지인 것으로 판단하는 단계;를 더 포함한다.

[0025] 한편, 본 발명의 제 2 측면에 따르는, 컴퓨터 판독가능한 기록매체는 상기에서 서술된 피보호자 안심 서비스제공방법을 구현하기 위한 프로그램 명령어가 기록되어 있을 수 있다.

[0026] 한편, 본 발명의 제 3 측면에 따르면, 피보호자 안심 서비스 제공을 위한 위험메시지 감시 장치는, 피보호자에게 발송된 메시지를 수신하는 메시지 수신부; 메시지 저장영역 또는 애플리케이션 상태정보 저장영역을 참조하여 상기 수신된 메시지를 인식하는 메시지 인식부; 상기 수신된 메시지와 미리 저장된 위험단어 리스트를 비교하여, 상기 수신된 메시지에 위험단어가 포함되어 있는지 판단하는 위험메시지 판단부; 상기 수신된 메시지가 상기 위험단어를 포함한 위험메시지인 것으로 판단된 경우, 상기 위험메시지의 발신식별정보를 통하여 상기 위험메시지의 발신자의 이름 또는 발신자의 연락처를 추출하는 발신자 정보 추출부; 및 상기 피보호자에 대응하는 보호자의 단말로 상기 위험메시지와 상기 발신자의 이름 또는 발신자의 연락처를 전송하는 위험정보 전송부;를 포함한다.

[0027] 또한, 상기 위험메시지 감시 장치는, 상기 피보호자에게 발송된 메시지를 수신하기 전, 상기 위험메시지 감시 장치에 포함되는 상기 피보호자 단말에 설치된 피보호자 안심 애플리케이션으로 상기 피보호자 단말의 애플리케

이션 상태정보 저장영역에 대한 접근권한을 설정하는 접근권한 설정부를 더 포함한다.

[0028] 또한, 상기 메시지 인식부는, 상기 메시지 저장영역을 참조하여 SMS 또는 MMS 메시지를 인식하거나, 상기 애플리케이션 상태정보 저장영역을 참조하여 상기 피보호자의 단말에 설치된 채팅 애플리케이션으로 수신된 채팅 메시지를 인식한다.

[0029] 또한, 상기 위험정보 전송부는, 상기 발신자의 이름의 일부 또는 연락처의 일부를 마스킹하여 전송한다.

[0030] 또한, 상기 위험메시지 감시 장치는, 상기 발신자의 이름 또는 연락처와 상기 피보호자 단말의 정보를 저장하고, 상기 저장된 발신자의 이름 또는 연락처를 통하여 상기 발신자로부터 위험메시지를 수신한 다른 피보호자를 검색하며, 상기 다른 피보호자의 정보를 상기 발신자의 이름 또는 연락처와 함께 상기 보호자 단말로 전송하는 발신자 가해정보 추출부를 더 포함한다.

[0031] 또 한편, 본 발명의 제 4 측면에 따르면, 피보호자 안심 서비스 제공을 위한 보호자 단말은, 위험메시지 감시 장치로부터 피보호자에게 수신된 위험단어를 포함하는 위험메시지와 상기 위험메시지의 발신자의 이름이나 연락처를 수신하는 위험정보 수신부; 및 상기 위험메시지와 상기 발신자의 이름의 일부나 연락처의 일부를 표시하는 위험정보 제공부;를 포함한다.

[0032] 또한, 상기 위험 단어는, 폭력성, 협박성, 유해성 중 적어도 하나에 따라 복수의 서로 다른 위험등급이 지정되어 있을 수 있다.

[0033] 또한, 상기 보호자 단말은, 상기 위험메시지의 발신자가 발신한 위험메시지의 총 개수, 위험메시지에 포함된 위험단어의 개수, 위험메시지에 포함된 위험단어의 위험등급 중 적어도 하나에 따라, 상기 발신자의 위험도를 제공하는 위험도 제공부를 더 포함한다.

## *발명의 효과*

[0034] 전술한 본 발명의 과제 해결 수단 중 어느 하나에 의하면, 본 발명의 일실시예는 피보호자에게 수신된 위험메시지를 감시함으로써, 보호자로 하여금 피보호자의 위험상황(예를 들어, 학교폭력)을 미리 예측하거나 감지하게 할 수 있다.

[0035] 또한, 본 발명의 과제 해결 수단 중 어느 하나에 의하면, 가해자에 대한 이름이나 전화번호 정보를 제공함으로써 보호자가 가해자의 정보를 예측할 수 있도록 하며, 가해자로부터 가해행위를 받은 다른 피보호자들의 정보도 보호자에게 제공함으로써, 가해자에 대한 추가 위험정보를 제공할 수 있다.

[0036] 또한, 본 발명의 과제 해결 수단 중 어느 하나에 의하면, 피보호자가 수신한 위험메시지를 피보호자의 학교 단말로 송부하여 학교측에서도 위험상황이나 가해자의 정보를 미리 알 수 있도록 할 수 있다.

[0037] 또한, 본 발명의 과제 해결 수단 중 어느 하나에 의하면, 위험메시지의 위험도를 보호자에게 알림으로써, 보호자가 위험상황을 경중을 미리 예측할 수 있게 하거나, 위험메시지 이더라도 농담이나 친근감 표시성의 위험단어가 포함된 경우는 필터링함으로써, 보호자가 필요한 위험메시지만 인지할 수 있도록 할 수 있다.

[0038] 본 발명에서 얻을 수 있는 효과는 이상에서 언급한 효과들로 제한되지 않으며, 언급하지 않은 또 다른 효과들은 아래의 기재로부터 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 명확하게 이해될 수 있을 것이다.

## *도면의 간단한 설명*

[0039] 도 1은 본 발명의 일실시예에 따른 피보호자 안심 서비스 제공을 위한 시스템의 구성도이다.

도 2는 본 발명의 일실시예에 따른 위험메시지 감시 장치의 내부 구성을 도시한 블록도이다.

도 3은 본 발명의 일실시예에 따른 보호자 단말의 내부 구성을 도시한 블록도이다.

도 4는 본 발명의 일실시예에 따른 추가 실시예에 따르는 구성을 도시한 블록도이다.

도 5는 본 발명의 일 실시예에 따르는 보호자 단말에서의 위험정보 제공 인터페이스의 예시화면이다.

도 6은 본 발명의 일실시예에 따른 피보호자 안심 서비스 제공방법을 설명하기 위한 순서도이다.

도 7은 본 발명의 다른 실시예에 따른 피보호자 안심 서비스 제공방법을 설명하기 위한 순서도이다.

## *발명을 실시하기 위한 구체적인 내용*

[0040] 아래에서는 첨부한 도면을 참조하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 본 발명의 실시예를 상세히 설명한다. 그러나 본 발명은 여러 가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.

[0041] 명세서 전체에서, 어떤 부분이 다른 부분과 "연결"되어 있다고 할 때, 이는 "직접적으로 연결"되어 있는 경우뿐 아니라, 그 중간에 다른 소자를 사이에 두고 "전기적으로 연결"되어 있는 경우도 포함한다. 또한 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.

[0042] 본 발명의 일 실시예를 설명하기에 앞서, 이하에서 사용되는 용어들의 의미를 먼저 정의한다.

[0043] “위험”이란, 유해, 폭력, 협박, 음란, 금지, 성인 등 미성년자나 기타 보호 대상자들에게 공개되기에 부적합한 게재물의 성격을 의미하는 것이다. 따라서, “위험단어”는 이러한 부적합한 성격을 지닌 단어를 의미하며, “위험메시지”는 위험단어를 포함한 메시지를 의미한다. 따라서, 피보호자가 수신한 욕설이나 폭력성 또는 협박성 단어가 포함된 메시지는 위험메시지라고 할 수 있다.

[0044] 이하, 도면을 참조하여 본 발명의 일 실시예를 구체적으로 설명하도록 한다.

[0045] 도 1을 참조하면, 본 발명의 일 실시예에 따르는 피보호자 안심 서비스 제공을 위한 시스템은 위험메시지 감시 장치(100) 및 보호자 단말(200)을 포함한다. 위험메시지 감시 장치(100)는 피보호자 단말(110)과 서버(120)로 구성될 수 있다.

[0046] 피보호자 단말(110)은 피보호자가 소지하는 단말로서, 써드파티 서버(미도시)로부터 문자 메시지(예를 들어, SMS, MMS 메시지)나 인스턴트 메시지(예를 들어, 메신저 애플리케이션의 메시지), SNS 메시지, 이메일 등을 수신할 수 있다. 이어서, 피보호자 단말(110)은 수신된 메시지 중 “XXX야, 돈 가져와”와 같은 위험단어가 포함된 것이 감지되었을 경우, 위험단어가 포함된 위험메시지를 서버(120)로 전송한다.

[0047] 서버(120)는 위험메시지를 수신하여 이를 보호자 단말(200)로 전송한다. 서버(120)는 위험메시지를 발송한 피보호자 단말(110)의 정보를 참고하여, 상기 피보호자 단말(110)과 대응하여 서버(120)에 등록되어 있는 보호자 단말(200)의 식별정보를 검색할 수 있다. 이어서, 서버(120)는 검색된 보호자 단말(200)로 위험메시지를 전송할 수 있다.

[0048] 보호자 단말(200)은 서버(120)로부터 위험메시지를 수신하여 표시함으로써, 보호자에게 피보호자가 수신한 위험메시지를 제공한다. 이를 통하여, 보호자 단말(200)을 소지한 보호자는 자신의 피보호자가 어떤 위험 상황에 노출되어 있는지 확인할 수 있다. 예를 들어, 자신의 자녀가 “XXX야, 돈 가져와”와 같은 협박성 메시지를 수신한 것을 알게됨으로써, 자녀가 직접 부모에게 말하지 않더라도 자녀가 현재 처한 위험상황을 인지할 수 있게 되므로, 학교폭력이 더 심각한 상황으로 흘러가지 않도록 적절한 조치를 미리 취할 수 있는 계기가 제공될 수 있다.

[0049] 이러한, 피보호자 단말(110)과 보호자 단말(200)에는 피보호자용 및 보호자용 피보호자 안심 애플리케이션이 각각 설치됨으로써, 피보호자 안심 애플리케이션의 동작에 의해 상기와 같은 위험메시지 감시 및 알림 동작이 수행될 수 있다.

[0050] 여기서 피보호자 단말(110), 서버(120), 보호자 단말(200) 사이의 통신을 중계하는 네트워크(N)는 근거리 통신망(Local Area Network; LAN), 광역 통신망(Wide Area Network; WAN), 부가가치 통신망(Value Added Network; VAN), 개인 근거리 무선통신(Personal Area Network; PAN), 이동 통신망(mobile radio communication network), Wibro(Wireless Broadband Internet), Mobile WiMAX, HSDPA(High Speed Downlink Packet Access) 또는 위성 통신망 등과 같은 모든 종류의 유/무선 네트워크로 구현될 수 있다.

[0051] 또한, 피보호자 단말(110)과 보호자 단말(200)은 네트워크(N)를 통해 원격지의 서버(120)에 접속하거나, 타 단말 및 서버(120)와 연결 가능한 컴퓨터나 휴대용 단말기, 텔레비전으로 구현될 수 있다. 여기서, 컴퓨터는 예를 들어, 웹 브라우저(WEB Browser)가 탑재된 노트북, 데스크톱(desktop), 랩톱(laptop) 등을 포함하고, 휴대용 단말기는 예를 들어, 휴대성과 이동성이 보장되는 무선 통신 장치로서, PCS(Personal Communication System),

PDC(Personal Digital Cellular), PHS(Personal Handyphone System), PDA(Personal Digital Assistant), GSM(Global System for Mobile communications), IMT(International Mobile Telecommunication)-2000, CDMA(Code Division Multiple Access)-2000, W-CDMA(W-Code Division Multiple Access), Wibro(Wireless Broadband Internet), 스마트폰(Smart Phone), 모바일 WiMAX(Mobile Worldwide Interoperability for Microwave Access) 등과 같은 모든 종류의 핸드헬드(Handheld) 기반의 무선 통신 장치를 포함할 수 있다. 또한, 텔레비전은 IPTV(Internet Protocol Television), 인터넷 TV(Internet Television), 지상파 TV, 케이블 TV 등을 포함할 수 있다.

[0052] 이하에서는, 도 2를 참조하여, 위험메시지 감시 장치(100)의 내부 구성을 구체적으로 설명하도록 한다. 위험메시지 감시 장치(100)는 피보호자 단말(110)과 서버(120)를 포함하여 구성되는 것으로서, 도2를 통하여 설명되는 구성들은 피보호자 단말(110) 또는 서버(120)에 선택적으로 채용될 수 있다.

[0053] 접근권한 설정부(101)는 피보호자 단말(110)에 설치된 피보호자 감시 애플리케이션이 피보호자 단말(110)로 수신된 메시지를 감시할 수 있도록 피보호자 감시 애플리케이션에 대한 접근권한을 설정한다. 접근권한이란 피보호자 단말(110)의 애플리케이션 상태정보 저장영역에 대한 접근권한을 의미할 수 있다.

[0054] 애플리케이션 상태정보 저장영역은 피보호자 단말(110)의 운영체제에 포함되거나 운영체제와는 독립적으로 구성된 영역으로서, 운영체제의 하위에 배치된 다양한 애플리케이션들이 수신하는 텍스트, 메시지, 파일 등이 일시적으로 또는 영구적으로 저장되는 영역이다. 애플리케이션 상태정보 저장영역에 저장된 정보는 단말의 일반 사용자가 상기 저장된 정보의 열람요청을 함으로써 일반 사용자에게도 보여질 수 있는 정보일 수 있다. (예를 들어, 애플리케이션 상태정보 저장영역에 저장된 정보는 스마트 기기에서 상단에서 하단으로 드래그하는 사용자 입력에 따라 나타나는 애플리케이션 상태창에 나열된 정보일 수 있다. 일반적으로, 애플리케이션 상태창에 등록된 애플리케이션에 대하여 업데이트 상태가 존재하는 경우, 푸쉬 알림이 단말로 송출되도록 구성될 수 있으며, 사용자는 애플리케이션 상태창을 열람함으로써 업데이트 상태 정보를 확인할 수 있다.) 예를 들어, 채팅 애플리케이션으로 수신된 A의 채팅 메시지나 SNS 애플리케이션으로 수신된 B의 SNS 메시지는 애플리케이션 상태정보 저장영역에도 저장되는 것으로서, 피보호자 안심 애플리케이션의 감시 대상에 포함될 수 있다.

[0055] 이러한 접근권한 설정은 피보호자 감시 애플리케이션의 설치와 동시에 자동으로 수행될 수도 있으나, 피보호자나 보호자의 입력에 따라 수동으로 수행될 수도 있다. 예를 들어, 보호자가 피보호자 감시 애플리케이션의 접근권한 설정 버튼을 입력함으로써, 접근권한 설정부(101)는 피보호자 단말(110)의 애플리케이션 상태정보 저장영역에 대한 접근권한을 피보호자 감시 애플리케이션에 부여할 수 있다.

[0056] 메시지 수신부(102)는 외부(즉, 외부 서버나 외부 단말)로부터 메시지를 수신한다. 메시지 수신부(102)가 수신하는 메시지는 문자 메시지(예를 들어, SMS, MMS 등), 인스턴트 메시지(예를 들어, 채팅 애플리케이션의 채팅 메시지), SNS 메시지 및 이메일 중 어느 하나가 될 수 있다. 예를 들어, 메시지 수신부(102)는 카카오톡, 라인, 틱톡, 네이트온 등과 같은 채팅 애플리케이션의 메시지와 피보호자 단말(110)에 설치되어 있는 메시지 애플리케이션의 단문 메시지를 수신할 수 있다.

[0057] 메시지 인식부(103)는 수신된 메시지의 내용을 인식한다. 구체적으로, 문자 메시지의 경우, 위험메시지 감시 장치(100)의 메시지 저장영역을 참조함으로써 인식할 수 있다. 또한, 인스턴트 메시지의 경우, 애플리케이션 상태정보 저장영역을 참조함으로써 인식할 수 있다. 일반적으로 현재 보급되고 있는 단말에서, 문자 메시지를 저장하는 메시지 저장영역에 대한 접근은 단말에 설치된 임의의 애플리케이션도 가능하도록 설정되어 있다. (예를 들어, 가계부 애플리케이션들 중 카드 거래내역 문자 메시지를 참조하여 자동으로 가계 내역을 계산하는 애플리케이션이 있음) 그러나, 애플리케이션 마켓 스토어로부터 다운받은 개별적인 애플리케이션(예를 들어, 카카오톡이나 라인과 같은 채팅 애플리케이션)에서 수신되는 메시지의 경우, 각각의 애플리케이션의 서버(미도시)에 대한 접근권한을 얻지 않는 다면, 개별적인 애플리케이션이 수신한 메시지에 대하여 접근할 수 없도록 설정되어 있었다. 그러나 각각의 애플리케이션의 서버에 대한 접근권한을 얻기 위해서는 해당 서비스 제공자와 제휴협약을 맺어야 하는 등의 어려움이 따른다. 그러나, 본 발명의 일 실시예는, 각각의 채팅 애플리케이션 서버에 대한 접근권한을 얻지 않고도, 애플리케이션 상태정보 저장영역에 대한 접근권한을 부여받음으로써, 문자 메시지 이외의 인스턴트 메시지를 인식할 수 있다.

[0058] 위험메시지 판단부(104)는 수신된 메시지가 위험메시지인지 판단한다. 위험메시지 판단부(104)는 수신된 메시지와 위험단어 리스트를 비교하여, 수신된 메시지에 위험단어가 포함되어 있는 경우 수신된 메시지를 위험메시지로서 판단한다. 예를 들어, “돈 가져와”라는 단어가 위험단어 리스트에 포함되어 있으며, 상기 단어를 포함한 메시지가 수신된 경우, 위험메시지 판단부(104)는 수신된 메시지가 위험메시지인 것으로 판단할 수 있다.

[0059] 위험단어 저장부(105)는 위에서 언급된 위험단어 리스트를 저장한다. 위험단어 리스트는 복수 개의 카테고리 별로 분류되어 있는 위험단어들의 집합이다. 복수 개의 카테고리는 예를 들어, ① 폭력/협박 ② 음란/성인 ③ 유해/비속어 ④ 자살/ 탈선 ⑤ 기타 유해단어를 포함할 수 있다. 위험단어 저장부(105)는 정기적으로 또는 비정기적으로 위험단어 리스트를 갱신하여 저장할 수 있다. 예를 들어, 위험단어 저장부(105)는 서비스 관리자에 의하여 입력된 위험단어 리스트를 갱신 저장하거나, 피보호자 단말(110)이 수신한 위험메시지 중 위험단어로 인식된 단어들을 반영하도록 갱신 저장할 수 있다.

[0060] 발신자 정보 추출부(106)는 위험메시지의 발신식별정보로부터 위험메시지의 발신자 정보를 추출한다. 구체적으로, 발신자 정보 추출부(106)는 위험메시지의 발신 주소를 통하여 위험메시지의 발신자의 연락처(예를 들어, 전화번호, 이메일, SNS 계정 주소, 채팅 애플리케이션의 아이디)를 파악할 수 있다. 이어서, 발신자 정보 추출부(106)는 발신자의 연락처가 위험메시지 감시 장치(100)에 등록되어 있는지 판단하고, 등록되어 있는 경우, 등록된 발신자의 연락처에 대응하여 저장된 발신자의 이름(또는 별명)을 검색함으로써 발신자의 이름을 파악할 수 있다. 한편, 발신자 정보 추출부(106)는 수신된 메시지가 인스턴트 메시지이며, 애플리케이션 상태정보 저장영역에 인스턴트 메시지의 대화상대 정보가 저장되어 있는 경우, 상기 대화상대의 정보를 참조함으로써, 발신자의 이름이나 연락처를 파악할 수 있다.

[0061] 위험정보 전송부(107)는 위험메시지, 발신자의 정보를 피보호자 단말(110)로 전송한다. 전송되는 발신자의 정보는 발신자의 이름 또는 연락처를 포함한다. 여기서, 발신자의 이름이나 연락처는 개인정보에 해당하는 것으로서, 여과없이 전송하는 경우, 무분별한 개인정보 노출의 우려가 있을 수 있다. 따라서, 위험정보 전송부(107)는 발신자의 이름의 일부나 발신자의 연락처의 일부를 마스킹 처리하여 보호자 단말(200)로 전송할 수도 있다. 예를 들어, 발신자의 이름의 가운데 음절이나 발신자의 연락처의 가운데 영역에 적어도 하나의 “*”를 삽입하여 전송할 수 있다.

[0062] 발신자 가해정보 추출부(108)는 위에서 정보가 추출된 위험메시지의 발신자가 상기 피보호자 이외에 다른 피보호자에게도 발신한 위험메시지가 있는 경우, 다른 피보호자에 대한 가해정보를 추출하여 제공할 수 있다. 발신자 가해정보 추출부(108)는 바람직하게 위험메시지 감시 장치(100) 중 서버(120)에 포함되는 구성일 수 있다. 발신자 가해정보 추출부(108)는 각각의 피보호자 단말(110)에서 위험메시지가 보호자 단말(200)로 전송될 때, 위험메시지의 발신자 정보(이름이나 연락처) 및 위험메시지를 전송한 피보호자 단말(110)의 정보를 대응하여 저장할 수 있다. 따라서, 발신자 가해정보 추출부(108)는 하나의 가해자(즉, 위험메시지 발신자)에 대하여 여러 명의 피해자(즉, 피보호자 단말(110)의 사용자)의 정보를 저장할 수 있다. 따라서, 발신자 가해정보 추출부(108)는 발신자 정보를 통하여, 해당 발신자와 연관된 다른 피보호자들의 정보를 추출할 수 있다. 예를 들어, A라는 발신자가 위험메시지를 보낸 피보호자들이 B, C, D가 있음이 파악될 수 있다. 발신자 가해정보 추출부(108)는 추출된 다른 피보호자들의 정보를 보호자 단말(200)로 전송할 수 있다. 여기서 다른 피보호자들의 이름이나 연락처는 일부가 마스킹 처리되어 전송될 수도 있으며, 보호자 단말(200)로 편집없이 전송된 후 보호자 단말(200)에서 마스킹 처리되어 표시될 수도 있다.

[0063] 도 3을 참조하면, 위험메시지 감시 장치(100)와 대응하는 보호자 단말(200)은 위험정보 수신부(201)와 위험정보 제공부(202)를 포함한다.

[0064] 위험정보 수신부(201)는 위험메시지 감시 장치(100)가 전송한 위험정보를 수신한다. 즉, 위험정보 수신부(201)는 피보호자 단말(110)로부터 수신한 위험메시지와 위험메시지의 발신자 정보를 수신할 수 있다.

[0065] 위험정보 제공부(202)는 수신된 위험메시지와 발신자 정보를 보호자가 볼 수 있도록 제공한다. 여기서, 위험정보 제공부(202)는 피보호자에 대한 위험정보의 내용과 통계를 제공할 수 있다. 구체적으로, 위험정보 제공부(202)는 피보호자가 수신한 위험메시지의 총 건수, 발신자의 정보(예를 들어, 발신자의 이름, 연락처, 해당 발신자가 전송한 위험메시지의 총 건수, 해당 발신자가 전송한 최근 위험메시지를 피보호자가 수신한 일자), 위험메시지의 정보(예를 들어, 위험메시지를 수신한 애플리케이션의 종류, 위험메시지 수신시각, 위험메시지에 포함된 위험단어의 카테고리, 위험메시지의 내용)을 제공할 수 있다.

[0066] 도 5를 참고하면, 보호자 단말(200)에서 표시되는 위험정보 제공 인터페이스가 도시되어 있다. 위험정보 제공 인터페이스의 R1 영역에는 보호자 단말(200)이 수신한 위험메시지의 총 건 수가 표시되어 있다. 여기서, 전체 위험메시지의 건수와 최근 수신한 위험메시지의 건수가 같이 표시될 수 있다. 또한, R2 영역에는 발신자의 정보가 표시되어 있다. 여기서, 발신자의 이름과 연락처는 일부 영역이 마스킹 처리되어 제공되며, 각각의 발신자에 대하여 수신된 메시지의 총 건수가 함께 표시되어 있다. 이때, 위험정보 제공부(202)는 위험메시지 감시 장치(100)로부터 마스킹 처리가 된 발신자의 이름이나 연락처를 그대로 표시하거나, 위험메시지 장치로부터 본래의

발신자의 이름이나 연락처를 수신한 뒤, 마스킹 처리하여 표시할 수도 있다. 또한, R3 영역에는 위험메시지가 SMS나 MMS와 같은 문자 메시지이거나 카카오톡 메시지와 같은 인스턴트 메시지임을 알리는 정보가 제공되어 있으며, 위험메시지 수신일자와 위험메시지에 포함된 위험단어가 어떠한 카테고리에 속하는지도 함께 제공되어 있다.

[0067] 이하, 도 4를 참고하면, 본 발명의 일 실시예에 따르는 피보호자 안심 서비스 제공을 위한 시스템은 위험도 제공부(301), 위험단어 목적 판단부(302) 및 발신자 연관성 판단부(303)를 추가로 포함할 수도 있다. 위험도 제공부(301)와 위험단어 목적 판단부(302)는 위험메시지 감시 장치(100)나 보호자 단말(200) 중 어느 하나에 포함되도록 구현될 수 있다.

[0068] 위험도 제공부(301)는 위험메시지의 발신자의 위험도를 결정하여 보호자에게 제공할 수 있다. 위험도는 위험메시지의 발신자가 피보호자에게 가해하는 행위에 대한 위험의 정도를 나타내는 것으로서, 수치나 색상으로 산출될 수 있다. 예를 들어, 위험도의 등급을 0에서 10으로 두고, 이 수치 중 어느 하나의 값으로 표현하거나, 위험도의 등급을 노란색, 초록색, 빨간색으로 두고, 이 색상 중 어느 하나의 색상을 표시하는 것으로 표현할 수 있다. 이러한 위험도는 발신자가 발신한 위험메시지의 총 개수, 위험메시지에 포함된 위험단어의 개수, 위험메시지에 포함된 위험단어의 위험등급 중 적어도 하나에 따라 결정될 수 있다. 여기서 위험등급이란 위험단어의 위험상황에 대한 경중을 나타내는 등급으로서, 위험메시지 감시 장치(100)에 저장된 위험단어 리스트의 단어들은 폭력성, 협박성, 유해성 중 적어도 하나에 따라 서로 다른 레벨로 위험등급이 지정되어 있을 수 있다. 예를 들어, “꺼져”, “지랄”, “또라이”, “존나” 등과 같은 단어는 흔히 가해목적없이 언급될 수 있는 용어일 수 있으므로 낮은 위험등급을 가지도록 설정되고, “돈 가져와”, “칼빵”, “뻥 뜯겨볼래” 등과 같은 단어는 높은 위험등급을 갖도록 설정될 수 있다.

[0069] 위험도 제공부(301)가 서버(120) 내에 구현될 경우, 하나의 발신자가 여러 명의 피보호자에게 보낸 위험메시지를 기준으로 위험도가 결정될 수 있으며, 위험도 제공부(301)가 보호자 단말(200) 내에 구현될 경우, 하나의 발신자가 하나의 피보호자에게 보낸 위험메시지를 기준으로 위험도가 결정될 수 있다.

[0070] 이러한 위험도를 보호자에게 제공함으로써, 보호자는 위험메시지를 보낸 발신자가 어느 정도로 위험한 대상인지 미리 예측할 수 있다. 예를 들어, 위험도가 낮은 경우, 보호자는 친구 사이의 농담이나 약간 지나친 언어 사용을 하는 것으로 생각하거나, 위험도가 높은 경우, 보호자는 해당 발신자의 학교폭력 행위가 심각한 것으로 곧바로 인지할 수 있다.

[0071] 위험단어 목적 판단부(302)는 위험단어가 폭력이나 협박성 등의 성격을 지닌 단어인지, 농담이나 친근감 표시성 등의 성격을 지닌 단어인지 판단하여, 후자인 경우 필터링함으로써 보호자에게 해당 위험메시지를 제공하지 않거나 보호자에게 위험성격이 낮은 메시지임을 알려주는 기능을 수행할 수 있다. 일반적으로, 청소년들의 경우, 욕설이나 비속어 등을 아무런 의미없이 습관적으로 사용하거나 친근감 표시로 사용하기도 한다. 이러한 경우까지 위험메시지로 인식하여 보호자에게 알린다면, 보호자 입장에서는 불필요한 메시지를 수신하게 되며, 피보호자 입장에서는 불필요한 영역에 대해서까지 사생활 침해를 받게 된다. 앞서 설명한 위험도 제공부(301)가 이러한 문제점을 개선하기 위한 일부 기능을 제공하기는 하나 불필요한 위험메시지의 완벽한 필터링 기능은 수행하지 못할 수 있다.

[0072] 따라서, 이러한 불필요한 점을 제거하기 위하여, 위험단어 목적 판단부(302)는 수신된 메시지와 피보호자가 입력한 메시지 간의 패턴 분석을 통하여 위험단어의 목적을 판단할 수 있다. 예를 들어, 위험메시지가 피보호자 단말(110)로 수신된 이후, 피보호자가 일정 시간 이내에 위험단어를 포함한 메시지를 입력하였다거나, “ㅋㅋ”, “ㅎㅎ”, “웃겨” 등과 같은 긍정적인 단어가 포함된 메시지를 입력한 경우, 피보호자가 수신한 위험메시지를 농담이나 친근감 표시성의 메시지로 판단할 수 있다. 또는, 위험등급이 높은 위험단어를 포함한 메시지가 연속적으로 일정횟수 이상 수신된 경우, 폭력이나 협박성 목적의 위험메시지인 것으로 판단할 수 있다.

[0073] 위험단어 목적 판단부(302)가 위험메시지 감시 장치(100) 내에 구현될 경우, 농담이나 친근감 표시성의 메시지는 보호자 단말(200)로 전송하지 않도록 구현될 수 있다. 또는, 위험단어 목적 판단부(302)가 보호자 단말(200) 내에 구현될 경우, 보호자 단말(200) 내에 수신된 메시지 중 농담이나 친근감 표시성의 메시지는 표시하지 않도록 구현될 수도 있다.

[0074] 발신자 연관성 판단부(303)는 두 명 이상의 서로 다른 발신자로부터의 위험메시지가 위험메시지 감시 장치(100)에 수신된 경우, 상기 각 발신자의 위험메시지의 내용을 참조하여 상기 각 발신자 간의 연관성 유무를 제공한다. 예를 들어, A와 B라는 발신자로부터 각각 위험메시지가 수신되었으며, A와 B의 메시지에 공통된 명사(예를

들어, 친구 이름, 학교, 학원 등)가 포함되어 있는 경우, A와 B는 서로 연관성이 있다고 판단할 수 있다. 또한, A의 위험메시지에 B의 이름이나 연락처가 포함되어 있거나, B의 위험메시지에 A의 이름이나 연락처가 포함되어 있는 경우 A와 B는 서로 연관성이 있다고 판단할 수 있다.

[0075] 이하, 도6 및 도 7을 통하여, 본 발명의 일 실시예에 따르는 피보호자 안심 서비스 제공방법에 대하여 구체적으로 설명하도록 한다.

[0076] 먼저, 도 6을 참고하면, 위험메시지 감시 장치(100)는 이미 설치되어 있는 피보호자 안심 애플리케이션으로 애플리케이션 상태정보 저장영역에 대한 접근권한을 부여할 수 있다(S110). 접근권한 부여하기 위한 설정은 피보호자 안심 애플리케이션의 설치와 동시에 자동으로 수행되거나, 피보호자나 보호자의 입력에 따라 수행될 수 있다. 이러한 애플리케이션 상태정보 저장영역에는 위험메시지 감시 장치(100)에서 수신하는 인스턴트 메시지가 저장될 수 있으므로, 접근권한 설정에 따라 위험메시지 감시 장치(100)에서 수신하는 인스턴트 메시지를 감시할 수 있게 된다.

[0077] 이어서, 위험메시지 감시 장치(100)는 메시지를 수신한다(S120). 예를 들어, 위험메시지 감시 장치(100)는 다른 단말이나 서버로부터 문자 메시지 또는 인스턴트 메시지를 수신할 수 있다.

[0078] 위험메시지 감시 장치(100)는 메시지 저장영역이나 애플리케이션 상태정보 저장영역을 참조하여 수신된 메시지의 내용을 인식할 수 있다(S130). 위험메시지 감시 장치(100)는 메시지 저장영역을 참조하여 SMS나 MMS 메시지를 인식할 수 있으며, 애플리케이션 상태정보 저장영역을 참조하여 위험메시지 감시 장치(100)에 설치된 채팅 애플리케이션의 인스턴트 메시지를 인식할 수 있다.

[0079] 위험메시지 감시 장치(100)는 수신된 메시지가 위험단어를 포함한 위험메시지인지 판단한다(S140). 위험메시지 감시 장치(100)는 위험단어 리스트를 참조하여 수신된 메시지에 위험단어가 포함되어 있는 경우, 위험메시지인 것으로 판단하고, 그렇지 않은 경우, 위험메시지가 아닌 것으로 판단한다.

[0080] 수신된 메시지가 위험메시지인 것으로 판단된 경우, 위험메시지 감시 장치(100)는 위험메시지의 발신자의 정보를 추출한다(S150). 위험메시지 감시 장치(100)는 위험메시지의 발신식별정보(예를 들어, 발신 주소나 인스턴트 메시지의 대화상대에 대한 정보)를 통하여 발신자의 이름이나 연락처를 파악할 수 있다. 여기서, 위험메시지 감시 장치(100)가 위험메시지의 발신 주소로부터 발신자의 연락처만을 파악한 경우, 파악된 연락처에 대응하여 위험메시지 감시 장치(100)에 저장된 이름이 있는지 검색함으로써, 발신자의 이름 추출할 수 있다.

[0081] 위험메시지 감시 장치(100)는 위험메시지와 발신자의 정보를 보호자 단말(200)로 전송한다(S160). 발신자 정보 중 이름이 추출되지 않은 경우, 연락처만 전송될 수 있으며, 이름이 추출된 경우, 이름과 연락처 중 적어도 하나가 전송될 수 있다. 구체적으로, 위험메시지 감시 장치(100)의 피보호자 단말(110)이 위험메시지와 발신자의 정보를 서버(120)로 전송한 후, 서버(120)가 전송받은 정보를 보호자 단말(200)로 전송할 수 있다.

[0082] 보호자 단말(200)은 수신한 위험메시지를 제공하고, 발신자의 정보의 일부를 보호자에게 제공할 수 있다. 구체적으로, 위험메시지와 관련된 통계적인 내용은 여과없이 보호자 단말(200)을 통하여 표시할 수 있으나, 발신자 정보 중 이름이나 연락처의 경우 개인정보에 해당하므로, 일부영역을 마스킹 처리하여 표시할 수도 있다. 예를 들어, 이름의 가운데 부분이나, 연락처의 가운데 부분을 적어도 하나의 “*”로 표시하여 제공할 수 있다.

[0083] 나아가, 본 발명의 일 실시예에 따르는 위험메시지 감시 장치(100)는 위험메시지 발신자의 가해정보를 추가로 제공할 수도 있다.

[0084] 도 7을 참조하면, 위험메시지 감시 장치(100), 바람직하게, 서버(120)는 피보호자 단말(110)로부터 수신한 위험메시지와 발신자의 정보와 피보호자 단말(110)의 정보를 저장할 수 있다(S210). 따라서, 서버(120)에는 발신자와 피보호자 간의 관계가 대응되어 저장될 수 있다. 예를 들어, A라는 발신자가 B,C,D에게 위험메시지를 발송한 경우, 서버(120)에는 A와 B,C,D의 정보가 서로 연관되어 저장될 수 있다.

[0085] 서버(120)는 발신자의 정보를 바탕으로 발신자와 연관된 다른 피보호자 단말(110)의 정보를 검색한다(S220). 예를 들어, B가 A로부터 위험메시지를 받은 경우, 서버(120)는 B외에 A로부터 위험메시지를 받은 C,D의 정보를 검색할 수 있다. 여기서 C, D에 관한 정보가 발신자의 가해정보가 될 수 있다.

[0086] 서버(120)는 발신자와 연관된 다른 피보호자 단말(110)의 정보를 보호자 단말(200)로 전송한다(S230).

[0087] 보호자 단말(200)은 발신자 정보와 함께 수신한 다른 피보호자 단말(110)의 정보를 표시할 수 있으며, 이때, 다른 피보호자 단말(110)의 정보 중 일부만 표시할 수 있다(S240). 예를 들어, 다른 피보호자 단말(110)의 정보가

A로부터 위험메시지를 받은 C,D의 이름이나 연락처인 경우, 무분별한 개인정보 노출의 우려가 있을 될 수 있으므로, 일부 영역을 마스킹 처리하여 표시할 수 있다.

[0088] 이 경우, 보호자는 A라는 발신자가 자신의 자녀인 B 이외에 C,D라는 다른 학생들에게 까지 가해행위를 한 것을 알 수 있게 된다. 또한, C,D의 정보로부터 A라는 발신자의 정보를 유추할 수도 있게 된다.

[0089] 한편, 본 발명의 추가 실시예에 의할 때, 도 6의 S150 단계 이후, 위험메시지 감시 장치(100)는 피보호자의 학교 단말로 위험메시지와 발신자의 정보를 전송할 수도 있다. 학교측에서도 학교폭력 사건을 인지하지 못하는 경우가 많기 때문에 이를 학교 단말로도 전송하여 학교 관계자나 선생님들이 미리 학교폭력을 인지하게 할 수 있다.

[0090] 또 한편, 본 발명의 추가 실시예에 의할 때, 도 6의 S160과 S170사이의 단계에서 위험메시지의 발신자의 위험도를 결정하여 보호자에게 제공할 수도 있다. 위험도는 위험메시지의 발신자가 피보호자에게 가해하는 행위에 대한 위험의 정도를 나타내는 것으로서, 수치나 색상으로 산출될 수 있다. 이러한 위험도는 발신자가 발신한 위험메시지의 총 개수, 위험메시지에 포함된 위험단어의 개수, 위험메시지에 포함된 위험단어의 위험등급 중 적어도 하나에 따라 결정될 수 있다. 여기서 위험등급이란 위험단어의 위험상황에 대한 경중을 나타내는 등급이다.

[0091] 또 한편, 본 발명의 추가 실시예에 의할 때, 도 6의 S140 단계에서 혹은 S170 단계에서 위험단어가 폭력이나 협박성 등의 성격을 지닌 단어인지, 농담이나 친근감 표시성 등의 성격을 지닌 단어인지 판단하여, 후자인 경우 필터링함으로써 보호자에게 해당 위험메시지를 제공하지 않거나 보호자에게 위험성격이 낮은 메시지임을 알려주는 기능을 수행할 수도 있다. 구체적으로, 수신된 메시지와 피보호자가 입력한 메시지 간의 패턴 분석을 통하여 위험단어의 목적을 판단하거나, 위험등급이 높은 위험단어를 포함한 메시지가 연속적으로 일정횟수 이상 수신된 경우, 폭력이나 협박성 목적의 위험메시지인 것으로 판단할 수 있다.

[0092] 또 한편, 본 발명의 추가 실시예에 의할 때, 도 6의 S160과 S170사이의 단계에서, 두 명 이상의 서로 다른 발신자로부터의 위험메시지가 위험메시지 감시 장치(100)에 수신된 경우, 상기 각 발신자의 위험메시지의 내용을 참조하여 상기 각 발신자 간의 연관성 유무를 제공할 수 있다.

[0093] 도 6 내지 도 7을 통해 설명된 실시예에 따른 피보호자 안심 서비스 제공방법은 컴퓨터에 의해 실행되는 프로그램 모듈과 같은 컴퓨터에 의해 실행가능한 명령어를 포함하는 기록 매체의 형태로도 구현될 수 있다. 컴퓨터 판독 가능 매체는 컴퓨터에 의해 액세스될 수 있는 임의의 가용 매체일 수 있고, 휘발성 및 비휘발성 매체, 분리형 및 비분리형 매체를 모두 포함한다. 또한, 컴퓨터 판독가능 매체는 컴퓨터 저장 매체 및 통신 매체를 모두 포함할 수 있다. 컴퓨터 저장 매체는 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈 또는 기타 데이터와 같은 정보의 저장을 위한 임의의 방법 또는 기술로 구현된 휘발성 및 비휘발성, 분리형 및 비분리형 매체를 모두 포함한다. 통신 매체는 전형적으로 컴퓨터 판독가능 명령어, 데이터 구조, 프로그램 모듈, 또는 반송파와 같은 변조된 데이터 신호의 기타 데이터, 또는 기타 전송 메커니즘을 포함하며, 임의의 정보 전달 매체를 포함한다.

[0094] 전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.

[0095] 본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

## *부호의 설명*

[0096]

| | |
|---|---|
| 100 : 위험메시지 감시 장치 | 101 : 접근권한 설정부 |
| 102 : 메시지 수신부 | 103 : 메시지 인식부 |
| 104 : 위험메시지 판단부 | 105 : 위험단어 저장부 |
| 106 : 발신자 정보 추출부 | 107 : 위험정보 전송부 |

108 : 발신자 가해정보 추출부　　110 : 피보호자 단말

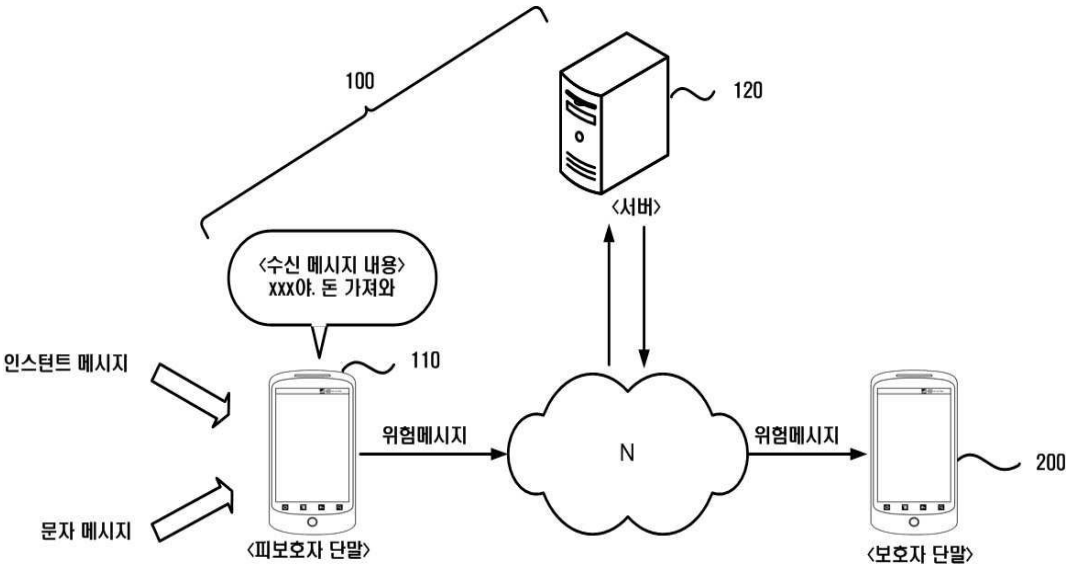
120 : 서버　　200 : 보호자 단말

201 : 위험정보 수신부　　202 : 위험정보 제공부

301 : 위험도 제공부　　302 : 위험단어 목적 판단부

## 도면

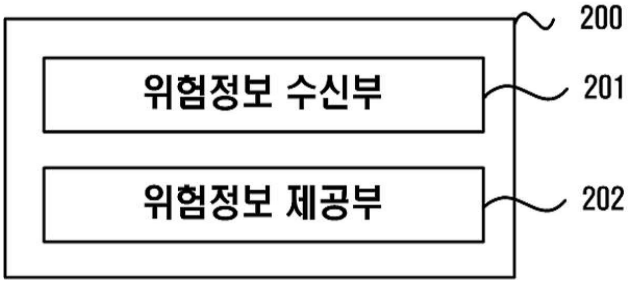
### 도면1



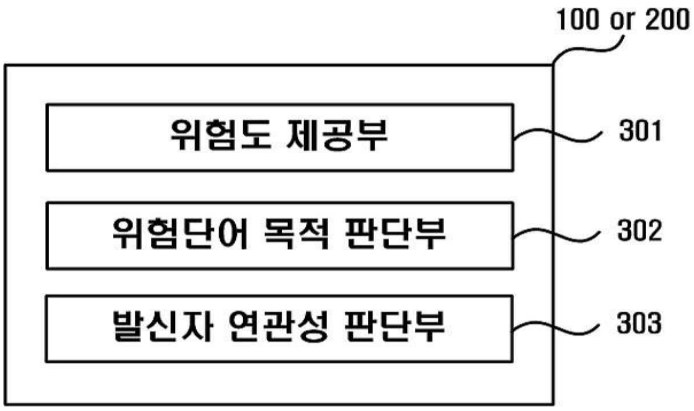
도면2


100
접근권한 설정부
101
메시지 수신부
102
메시지 인식부
103
위험메시지 판단부
104
위험단어 저장부
105
발신자 정보 추출부
106
위험정보 전송부
107
발신자 가해정보 추출부
108

도면3


200
위험정보 수신부
201
위험정보 제공부
202

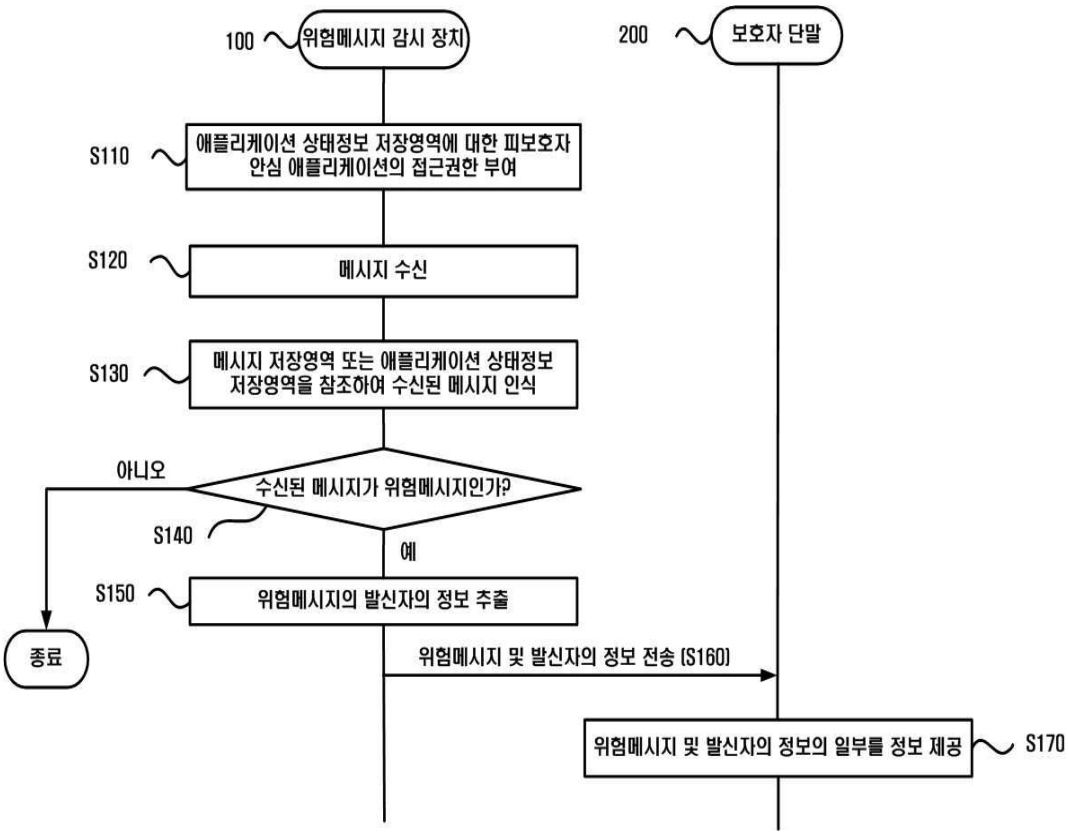
도면4


100 or 200
위험도 제공부
301
위험단어 목적 판단부
302
발신자 연관성 판단부
303

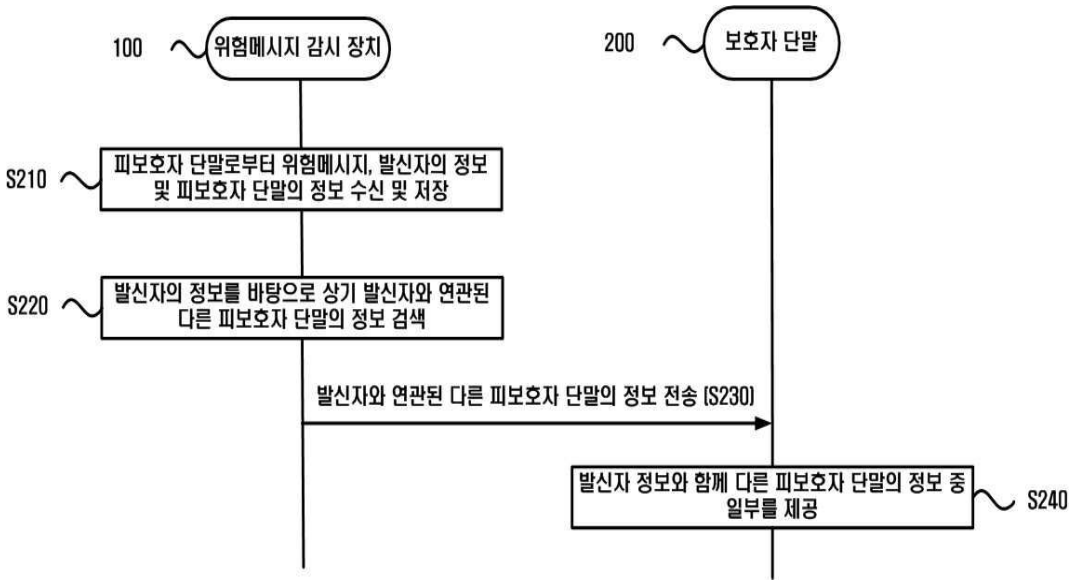
도면5


오후 5:36
이전
[QA]지프로] 사용 통계
차단 사이트
차단 앱
위협 문자
• 수신 된 위험 문자를 최근 1,000개까지 저장해 보여 줍니다.
• 수신 내역은 30일간 보관됩니다.
위협 문자 (총 11/1,000건)
R1
발신자 : 천* 은 (총 6건)
최근 수신 일자 : 2014년 01월 27일 15시 59분
발신자 : 010-****-3282 (총 5건)
최근 수신 일자 : 2014년 01월 27일 15시 51분
R2
문자내용
2014-01-27 15:51:54
R3
2014-01-27 15:47:19
정보
사용관리
사용통계
위치조회

도면6


100
위험메시지 감시 장치
200
보호자 단말
S110
애플리케이션 상태정보 저장영역에 대한 피보호자 안심 애플리케이션의 접근권한 부여
S120
메시지 수신
S130
메시지 저장영역 또는 애플리케이션 상태정보 저장영역을 참조하여 수신된 메시지 인식
아니오
수신된 메시지가 위험메시지인가?
S140
예
S150
위험메시지의 발신자의 정보 추출
종료
위험메시지 및 발신자의 정보 전송 (S160)
위험메시지 및 발신자의 정보의 일부를 정보 제공
S170

도면7


100
위험메시지 감시 장치
200
보호자 단말
S210
피보호자 단말로부터 위험메시지, 발신자의 정보 및 피보호자 단말의 정보 수신 및 저장
S220
발신자의 정보를 바탕으로 상기 발신자와 연관된 다른 피보호자 단말의 정보 검색
발신자와 연관된 다른 피보호자 단말의 정보 전송 (S230)
발신자 정보와 함께 다른 피보호자 단말의 정보 중 일부를 제공
S240