(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0066162
(43) 공개일자 2012년06월22일

(51) 국제특허분류(Int. Cl.)
*G06Q 50/00* (2006.01)
(21) 출원번호 10-2010-0127374
(22) 출원일자 2010년12월14일
심사청구일자 없음
기술이전 희망 : **기술양도**, **실시권허여**, **기술지도**

전체 청구항 수 : 총 17 항

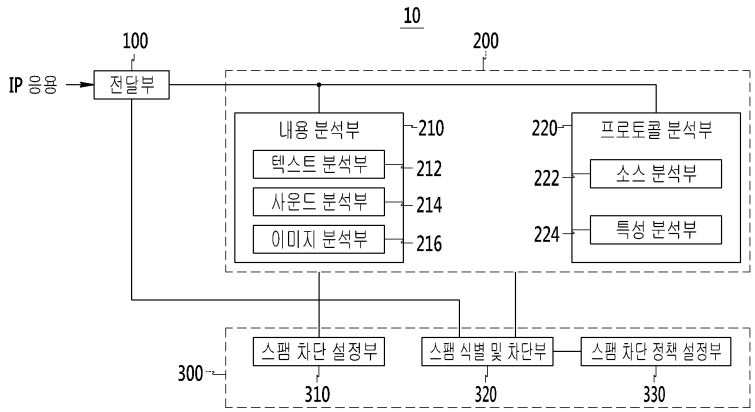
(71) 출원인
**한국전자통신연구원**
대전광역시 유성구 가정로 218 (가정동)
(72) 발명자
**박소영**
대전광역시 유성구 가정로 218, 통합망표준연구팀 (가정동, 한국전자통신연구원)
**김성혜**
대전광역시 유성구 송림로 13, 송림마을아파트 106동 603호 (하기동)
*(뒷면에 계속)*
(74) 대리인
**팬코리아특허법인**

(54) 발명의 명칭 **스팸 차단 방법 및 장치**

## (57) 요 약

IP 멀티미디어 스팸을 차단하기 위한 스팸 차단 장치에서, 전달부는 IP 응용을 수신하며, IP 응용이 스팸인 경우에 IP 응용을 차단한다. 스팸 식별부는 전달부로부터 IP 응용을 전달받으며, IP 응용의 콘텐츠와 IP 응용의 프로토콜 중 적어도 하나를 분석한다. 제어부는 스팸 차단을 위한 설정에 기초하여 스팸 식별부를 제어하며, 스팸 식별부의 IP 응용에 대한 분석 결과에 기초하여 IP 응용의 스팸 여부를 판단하고 판단 결과를 전달부로 전달한다.

*대 표 도* - 도1



(72) 발명자

**강신각**

대전광역시 유성구 은구비남로 34, 열매마을아파트 802동 801호 (노은동)

**현옥**

대전광역시 유성구 송림로 20, 송림마을아파트 206동 2302호 (하기동)

이 발명을 지원한 국가연구개발사업

| | |
|---|---|
| 과제고유번호 | 2010-P1-10 |
| 부처명 | 지식경제부/방송통신위원회 |
| 연구사업명 | 정보통신표준기술력향상사업 |
| 연구과제명 | MoIP 서비스 기반구조 및 응용 표준개발 |
| 주관기관 | 한국전자통신연구원 |
| 연구기간 | 2010.01.01~2010.12.31 |

## *특허청구의 범위*

**청구항 1**

인터넷 프로토콜(internet protocol, IP) 멀티미디어 스팸을 차단하기 위한 스팸 차단 장치로서,

IP 응용을 수신하며, 상기 IP 응용이 스팸인 경우에 상기 IP 응용을 차단하는 전달부,

상기 전달부로부터 상기 IP 응용을 전달받으며, 상기 IP 응용의 콘텐츠와 상기 IP 응용의 프로토콜 중 적어도 하나를 분석하는 스팸 식별부, 그리고

스팸 차단을 위한 설정에 기초하여 상기 스팸 식별부를 제어하며, 상기 스팸 식별부의 상기 IP 응용에 대한 분석 결과에 기초하여 상기 IP 응용의 스팸 여부를 판단하고 판단 결과를 상기 전달부로 전달하는 제어부

를 포함하는 스팸 차단 장치.

**청구항 2**

제1항에서,

상기 스팸 식별부는, 텍스트, 사운드 및 이미지 중 적어도 하나를 포함하는 상기 IP 응용의 콘텐츠를 분석하는 내용 분석부를 포함하는 스팸 차단 장치.

**청구항 3**

제1항에서,

상기 스팸 식별부는 상기 IP 응용의 프로토콜을 분석하는 프로토콜 분석부를 포함하며,

상기 프로토콜 분석부는 상기 IP 응용의 소스 정보를 분석하는 소스 분석부를 포함하는 스팸 차단 장치.

**청구항 4**

제3항에서,

상기 소스 정보는 상기 IP 응용의 발신자의 IP 주소, 도메인 이름 및 계정 이름 중 적어도 하나를 포함하는 스팸 차단 장치.

**청구항 5**

제1항에서,

상기 스팸 식별부는 상기 IP 응용의 프로토콜을 분석하는 프로토콜 분석부를 포함하며,

상기 프로토콜 분석부는 상기 IP 응용의 특성을 분석하는 특성 분석부를 포함하는 스팸 차단 장치.

**청구항 6**

제5항에서,

상기 특성 분석부는 상기 IP 응용의 특성을 분석하여서 상기 IP 응용의 대량성, 상기 IP 응용의 상호 작용성 및 상기 IP 응용의 레이블 중 적어도 하나의 정보를 확인하는 스팸 차단 장치.

**청구항 7**

제1항에서,

상기 제어부는 상기 스팸 식별부를 제어하기 위한 설정 정보를 가지며, 스팸 차단 정책에 기초하여 상기 IP 응용이 스팸인지를 판단하는 스팸 차단 장치.

**청구항 8**

스팸 차단 장치에서 인터넷 프로토콜(internet protocol, IP) 멀티미디어 스팸을 차단하기 위한 방법으로서,

IP 응용을 수신하는 단계,

스팸 차단을 위한 설정에 기초하여 상기 IP 응용의 콘텐츠와 상기 IP 응용의 프로토콜 중 적어도 하나를 분석하는 단계,

상기 IP 응용에 대한 분석 결과 및 스팸 차단 정책에 기초하여 상기 IP 응용의 스팸 여부를 판단하는 단계, 그리고

상기 스팸 여부에 대한 판단 결과에 기초하여 상기 IP 응용을 차단할지 통과시킬지 결정하는 단계

를 포함하는 스팸 차단 방법.

**청구항 9**

제8항에서,

상기 적어도 하나를 분석하는 단계는 상기 IP 응용의 콘텐츠에 포함된 텍스트, 사운드 및 이미지 중 적어도 하나를 분석하는 스팸 차단 방법.

**청구항 10**

제8항에서,

상기 적어도 하나를 분석하는 단계는 상기 IP 응용의 프로토콜 중 소스 정보를 분석하는 스팸 차단 방법.

**청구항 11**

제10항에서,

상기 소스 정보는 상기 IP 응용의 발신자의 IP 주소, 도메인 이름 및 계정 이름 중 적어도 하나를 포함하는 스팸 차단 방법.

**청구항 12**

제8항에서,

상기 적어도 하나를 분석하는 단계는 상기 IP 응용의 프로토콜로부터 상기 IP 응용의 특성을 분석하는 스팸 차단 방법.

**청구항 13**

제12항에서,

상기 적어도 하나를 분석하는 단계는 상기 IP 응용의 특성을 분석하여서 상기 IP 응용의 대량성, 상기 IP 응용의 상호 작용성 및 상기 IP 응용의 레이블 중 적어도 하나의 정보를 확인하는 단계를 포함하는 스팸 차단 방법.

**청구항 14**

응용 서버에 연결되어 있으며, 인터넷 프로토콜(internet protocol, IP) 멀티미디어 스팸을 차단하기 위한 프록시 서버로서,

IP 응용을 수신하며, 상기 IP 응용이 스팸인 경우에 상기 IP 응용을 차단하는 전달부, 그리고

상기 전달부로부터 상기 IP 응용을 전달받으며, 상기 응용 서버에서 제공하는 스팸 차단을 위한 설정에 기초하여 상기 IP 응용의 프로토콜을 분석하고, 상기 응용 서버에서 상기 IP 응용의 스팸 여부를 판단하도록 상기 IP 응용의 프로토콜에 대한 분석 결과를 상기 응용 서버로 제공하는 스팸 식별부

를 포함하며,

상기 전달부는 상기 응용 서버로부터 상기 IP 응용의 스팸 여부에 대한 정보를 전달받는

프록시 서버.

**청구항 15**

제14항에서,

상기 스팸 식별부는 상기 IP 응용의 소스 정보를 분석하는 소스 분석부를 포함하는 프록시 서버.

**청구항 16**

제14항에서,

상기 스팸 식별부는 상기 IP 응용의 특성을 분석하는 특성 분석부를 포함하는 프록시 서버.

**청구항 17**

제16항에서,

상기 특성 분석부는 상기 IP 응용의 특성을 분석하여서 상기 IP 응용의 대량성, 상기 IP 응용의 상호 작용성 및 상기 IP 응용의 레이블 중 적어도 하나의 정보를 확인하는 프록시 서버.

# *명 세 서*

## *기 술 분 야*

[0001] 본 발명은 스팸 차단 방법 및 장치에 관한 것으로, 특히 인터넷 프로토콜(internet protocol, IP) 멀티미디어 스팸의 차단 방법 및 장치에 관한 것이다.

## *배 경 기 술*

[0002] 과거 이메일 스팸과 이동 전화에서의 단문 메시지 서비스(short message service, SMS) 스팸이 대량으로 발생하여, 서비스 제공 업자 및 서비스 이용자에 큰 피해를 주어 왔다. 이에 대응하기 위하여 이메일 및 SMS 스팸 차단을 위한 다양한 기술이 개발되어 왔다.

[0003] 최근에는 인터넷 전화, 인스턴트 메시징 서비스(instant messaging service, IMS) 등의 IP 멀티미디어 응용 상에서 발생할 수 있는 IP 멀티미디어 스팸이 새로운 위협으로 떠오름에 따라, 이들 스팸을 차단하기 위한 기술이 요구된다. 그러나 기존의 이메일 및 SMS 스팸을 차단하기 위하여 개발된 기술을 IP 멀티미디어 스팸에 적용하는 데는 한계가 있다.

## *발명의 내용*

### *해결하려는 과제*

[0004] 본 발명이 해결하려는 과제는 IP 멀티미디어 스팸을 효율적으로 차단할 수 있는 방법 및 장치를 제공하는 것이다.

### *과제의 해결 수단*

[0005] 본 발명의 한 특징에 따르면, IP 멀티미디어 스팸을 차단하기 위한 스팸 차단 장치가 제공된다. 상기 스팸 차단 장치는 전달부, 스팸 식별부 및 제어부를 포함한다. 상기 전달부는 IP 응용을 수신하며, 상기 IP 응용이 스팸인 경우에 상기 IP 응용을 차단한다. 상기 스팸 식별부는 상기 전달부로부터 상기 IP 응용을 전달받으며, 상기 IP 응용의 콘텐츠와 상기 IP 응용의 프로토콜 중 적어도 하나를 분석한다. 상기 제어부는 스팸 차단을 위한 설정에 기초하여 상기 스팸 식별부를 제어하며, 상기 스팸 식별부의 상기 IP 응용에 대한 분석 결과에 기초하여 상기 IP 응용의 스팸 여부를 판단하고 판단 결과를 상기 전달부로 전달한다.

[0006] 상기 스팸 식별부는, 텍스트, 사운드 및 이미지 중 적어도 하나를 포함하는 상기 IP 응용의 콘텐츠를 분석하는 내용 분석부를 포함할 수 있다.

[0007] 상기 스팸 식별부는 상기 IP 응용의 프로토콜을 분석하는 프로토콜 분석부를 포함할 수 있으며, 상기 프로토콜 분석부는 상기 IP 응용의 소스 정보를 분석하는 소스 분석부를 포함할 수 있다.

[0008] 상기 소스 정보는 상기 IP 응용의 발신자의 IP 주소, 도메인 이름 및 계정 이름 중 적어도 하나를 포함할 수 있다.

[0009] 상기 스팸 식별부는 상기 IP 응용의 프로토콜을 분석하는 프로토콜 분석부를 포함할 수 있으며, 상기 프로토

콜 분석부는 상기 IP 응용의 특성을 분석하는 특성 분석부를 포함할 수 있다.

[0010] 상기 특성 분석부는 상기 IP 응용의 특성을 분석하여서 상기 IP 응용의 대량성, 상기 IP 응용의 상호 작용성 및 상기 IP 응용의 레이블 중 적어도 하나의 정보를 확인할 수 있다.

[0011] 상기 제어부는 상기 스팸 식별부를 제어하기 위한 설정 정보를 가지며, 스팸 차단 정책에 기초하여 상기 IP 응용이 스팸인지를 판단할 수 있다.

[0012] 본 발명의 다른 특징에 따르면, 스팸 차단 장치에서 IP 멀티미디어 스팸을 차단하기 위한 방법이 제공된다. 상기 스팸 차단 방법은, IP 응용을 수신하는 단계, 스팸 차단을 위한 설정에 기초하여 상기 IP 응용의 콘텐츠와 상기 IP 응용의 프로토콜 중 적어도 하나를 분석하는 단계, 상기 IP 응용에 대한 분석 결과 및 스팸 차단 정책에 기초하여 상기 IP 응용의 스팸 여부를 판단하는 단계, 그리고 상기 스팸 여부에 대한 판단 결과에 기초하여 상기 IP 응용을 차단할지 통과시킬지 결정하는 단계를 포함한다.

[0013] 상기 IP 응용의 콘텐츠와 상기 IP 응용의 프로토콜 중 적어도 하나를 분석할 때, 상기 IP 응용의 콘텐츠에 포함된 텍스트, 사운드 및 이미지 중 적어도 하나를 분석할 수 있다.

[0014] 상기 IP 응용의 콘텐츠와 상기 IP 응용의 프로토콜 중 적어도 하나를 분석할 때, 상기 IP 응용의 프로토콜 중 소스 정보를 분석할 수 있다.

[0015] 상기 IP 응용의 콘텐츠와 상기 IP 응용의 프로토콜 중 적어도 하나를 분석할 때, 상기 IP 응용의 프로토콜로부터 상기 IP 응용의 특성을 분석할 수 있다.

[0016] 상기 IP 응용의 콘텐츠와 상기 IP 응용의 프로토콜 중 적어도 하나를 분석할 때, 상기 IP 응용의 특성을 분석하여서 상기 IP 응용의 대량성, 상기 IP 응용의 상호 작용성 및 상기 IP 응용의 레이블 중 적어도 하나의 정보를 확인할 수 있다.

[0017] 본 발명의 또 다른 특징에 따르면, 응용 서버에 연결되어 있으며, IP 멀티미디어 스팸을 차단하기 위한 프록시 서버가 제공된다. 상기 프록시 서버는 전달부와 스팸 식별부를 포함한다. 상기 전달부는 IP 응용을 수신하며, 상기 IP 응용이 스팸인 경우에 상기 IP 응용을 차단한다. 상기 스팸 식별부는 상기 전달부로부터 상기 IP 응용을 전달받으며, 상기 응용 서버에서 제공하는 스팸 차단을 위한 설정에 기초하여 상기 IP 응용의 프로토콜을 분석하고, 상기 응용 서버에서 상기 IP 응용의 스팸 여부를 판단하도록 상기 IP 응용의 프로토콜에 대한 분석 결과를 상기 응용 서버로 제공한다. 상기 전달부는 상기 응용 서버로부터 상기 IP 응용의 스팸 여부에 대한 정보를 전달받는다.

## *발명의 효과*

[0018] 본 발명의 한 실시예에 따르면, 인터넷 전화, 메시징 서비스 등의 다양한 IP 응용 서비스에서 발생할 수 있는 IP 멀티미디어 스팸을 효과적으로 식별 및 차단할 수 있다.

## *도면의 간단한 설명*

[0019] 도 1은 본 발명의 한 실시예에 따른 IP 멀티미디어 스팸 차단 장치의 개략적인 블록도이다.

도 2는 본 발명의 한 실시예에 따른 IP 멀티미디어 스팸 차단 방법의 개략적인 흐름도이다.

도 3 내지 도 5는 각각 본 발명의 한 실시예에 따른 IP 멀티미디어 스팸 차단 장치를 구현한 예를 나타내는 도면이다.

## *발명을 실시하기 위한 구체적인 내용*

[0020] 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 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.

[0021] 이제 본 발명의 한 실시예에 따른 IP 멀티미디어 스팸 차단 장치 및 방법에 대해서 도면을 참고로 하여 상세하게 설명한다.

[0022] 본 발명의 한 실시예에서 IP 멀티미디어 스팸은 인터넷 전화, 메시징 서비스 등의 IP 멀티미디어 응용 상에서

발생할 수 있는 다양한 형태의 스팸을 의미한다.

[0023] 도 1은 본 발명의 한 실시예에 따른 IP 멀티미디어 스팸 차단 장치의 개략적인 블록도이다.

[0024] 도 1을 참고하면, IP 멀티미디어 스팸 차단 장치(10)는 전달부(100), 스팸 식별부(200) 및 제어부(300)를 포함한다.

[0025] 전달부(100)는 외부로부터 IP 응용을 전달받아 스팸 식별부(200)로 전달한다.

[0026] 스팸 식별부(200)는 전달부(200)로부터 전달받은 IP 응용이 스팸인지 식별하기 위하여 IP 응용을 분석한다. 이러한 스팸 식별부(200)는 내용 분석부(210) 및 프로토콜 분석부(220)를 포함한다.

[0027] 내용 분석부(210)는 스팸 식별을 위하여 IP 응용의 콘텐츠, 즉 페이로드를 분석하며, 텍스트 분석부(212), 사운드 분석부(214) 및 이미지 분석부(216)를 포함한다. 텍스트 분석부(212)는 IP 응용의 콘텐츠 중 텍스트를 분석하고, 사운드 분석부(214)는 IP 응용의 콘텐츠 중 사운드를 분석하고, 이미지 분석부(216)는 IP 응용의 콘텐츠 중 이미지를 분석한다. 즉, 내용 분석부(210)는 IP 응용의 콘텐츠가 스팸에 해당하는지를 판단하기 위해서, IP 응용의 콘텐츠에 포함된 텍스트, 사운드 및 이미지 중 적어도 하나의 내용을 분석한다.

[0028] 프로토콜 분석부(220)는 스팸 식별을 위하여 IP 응용의 프로토콜 부분을 분석하며, 소스 분석부(222) 및 특성 분석부(224)를 포함한다. 소스 분석부(222)는 IP 응용이 스팸으로 등록된 발신자에서 전송되었는지를 판단하기 위해서, 발신자의 IP 주소, 도메인 이름, 계정 이름 등 IP 응용의 소스 정보를 분석한다. 특성 분석부(224)는 스팸 식별을 위해서 IP 응용이 가지는 고유의 특성을 분석한다. 예를 들면 IP 응용의 대량성을 분석하거나 IP 응용의 상호 작용성을 확인하거나 IP 응용의 레이블을 확인해서, 해당 IP 응용이 스팸의 특성을 가지는지 확인할 수 있다.

[0029] 제어부(300)는 전달부(100)와 스팸 식별부(200)를 제어하고 전달부(100)와 스팸 식별부(200)의 제어를 위한 설정 정보를 입력받는다. 제어부(300)는 스팸 차단 설정부(310), 스팸 식별 및 차단부(320) 및 스팸 차단 정책 설정부(330)를 포함한다.

[0030] 스팸 차단 설정부(310)는 전달받은 IP 응용에 대하여 어떤 종류의 분석을 수행할 것인지에 대한 설정 정보를 가지며, 이 설정 정보를 이용하여 스팸 식별부(200)를 제어한다. 스팸 식별 및 차단부(320)는 스팸 식별부(200)의 IP 응용 분석 결과를 전달받으며, 스팸 차단 정책 설정부(330)의 지원 하에서 분석된 IP 응용이 스팸인지 판단한다. 스팸 차단 정책 설정부(330)는 IP 응용이 스팸인지를 판단하는 데 필요한 스팸 차단 정책을 스팸 식별 및 차단부(320)에 제공한다.

[0031] 도 2는 본 발명의 한 실시예에 따른 IP 멀티미디어 스팸 차단 방법의 개략적인 흐름도이다.

[0032] 도 2를 참고하면, 먼저 스팸 차단 설정부(310)와 스팸 차단 정책 설정부(320)가 스팸 차단을 위한 기본적인 설정을 한다(S210, S212). 구체적으로, 스팸 차단 설정부(310)는 외부에서 입력받은 스팸 차단 설정에 관한 정보를 스팸 식별부(200)에 전달한다(S210). 또한 스팸 차단 정책 설정부(330)는 스팸 차단 정책에 관한 설정을 외부로부터 입력받는다(S212).

[0033] 이러한 기본적인 설정이 이루어진 상태에서, 전달부(100)가 IP 응용을 전달받으면(S220), 이를 스팸 식별부(200)으로 전달한다(S222). 스팸 식별부(200)는 스팸 차단 설정에 기초하여 전달받은 IP 응용을 분석하고(S230), 분석 결과를 스팸 식별 및 차단부(320)에 전달한다(S232). 스팸 식별 및 차단부(320)는 전달받은 분석 결과로부터 해당 IP 응용이 스팸인지를 판단하기 위하여, 스팸 차단 정책 설정부(330)에 스팸 차단 정책에 관한 정보를 요청하고(S240) 스팸 차단 정책 설정부(330)로부터 해당 정보를 전달받는다(S242). 스팸 식별 및 차단부(320)는 전달받은 스팸 차단 정책에 관한 정보에 기초하여 해당 IP 응용이 스팸인지를 판별하고(S250), 판별 결과를 전달부(100)로 전달한다(S252).

[0034] 전달부(100)는 스팸 식별 및 차단부(320)가 스팸으로 판단한 IP 응용을 차단하고(S260), 그렇지 않은 IP 응용에 대해서 정상적으로 서비스가 이루어지도록 해당 IP 응용을 전달한다.

[0035] 한편 도 1을 참고하여 설명한 것처럼, 본 발명의 한 실시예에 따른 IP 멀티미디어 스팸 차단 장치(10)의 전달부(100), 스팸 식별부(200) 및 제어부(300)는 각각 적어도 하나의 모듈 및/또는 기능으로 이루어질 수 있다. 개별 기능 및/또는 모듈은 논리적으로 구분될 수 있으며, 물리적으로 분리되거나 통합된 형태로 구현될 수 있다. 또한 하나의 모듈 및/또는 기능은 네트워크 상의 여러 엔터티 상에 구현될 수 있다. 아래에서는 이러한 실시예에 대해서 도 3 내지 도 5를 참고로 하여 설명한다.

[0036] 도 3 내지 도 5는 각각 본 발명의 한 실시예에 따른 IP 멀티미디어 스팸 차단 장치를 구현한 예를 나타내는 도면이다.

[0037] 도 3을 참고하면, IP 멀티미디어 스팸 차단 장치가 응용 서버(31)와 프록시 서버(32)에 구현된다.

[0038] 구체적으로, 전달부(100a), 스팸 식별부(200a)의 적어도 일부 기능 및 제어부(300a)가 응용 서버(31)에 구현되고, 전달부(100b) 및 스팸 식별부(200b)의 적어도 일부 기능이 프록시 서버(32)에 구현된다. 예를 들면 스팸 식별부(200a)의 내용 분석부(210a) 및 프로토콜 분석부(220a) 중 특성 분석부(224a)가 응용 서버(31)에 구현되고, 스팸 식별부(200b)의 프로토콜 분석부(220b)가 프록시 서버(32)에 구현될 수 있다.

[0039] 이와 같이, 프록시 서버(32)에 제어부가 구현되지 않은 경우, 프록시 서버(32)의 스팸 식별부(200b)는 응용 서버(31)의 제어부(300a)에서 제공하는 스팸 차단을 위한 설정에 기초하여 IP 응용의 프로토콜을 분석하고, 분석 결과를 응용 서버(31)의 제어부(300a)로 전달한다. 그러면 응용 서버(31)의 제어부(300a)가 프록시 서버(32)의 분석 결과 및/또는 응용 서버(31)의 분석 결과에 기초하여 해당 IP 응용이 스팸인지를 판단하고, 그 결과를 프록시 서버(32)의 전달부(100b)로 전달한다.

[0040] 도 4를 참고하면, IP 멀티미디어 스팸 차단 장치가 응용 서버(40)에 구현된다.

[0041] 구체적으로, 전달부(100c), 스팸 식별부(200c) 및 제어부(300c)가 응용 서버(40)에 구현되고, 특히 스팸 식별부(200c)의 내용 분석부(210c) 및 프로토콜 분석부(220c)의 소스 분석부(222c)와 특성 분석부(224c)가 모두 응용 서버(40)에 구현될 수 있다.

[0042] 도 5를 참고하면, IP 멀티미디어 스팸 차단 장치가 프록시 서버(51)와 사용자 단말(52)에 구현된다.

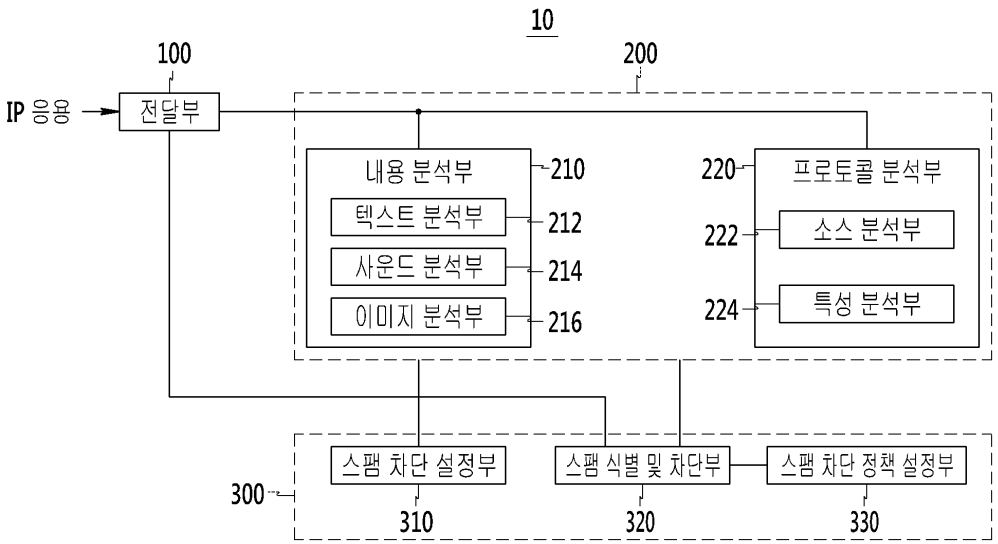
[0043] 구체적으로, 전달부(100d), 스팸 식별부(200d)의 적어도 일부 기능 및 제어부(300c)가 프록시 서버(51)에 구현되고, 전달부(100e), 스팸 식별부(200e)의 적어도 일부 기능 및 제어부(300e)가 사용자 단말(52)에 구현된다. 예를 들면 스팸 식별부(200d)의 프로토콜 분석부(220d), 즉 소스 분석부(222d)와 특성 분석부(224d)가 프록시 서버(51)에 구현되고, 스팸 식별부(200e)에서 내용 분석부(210e)의 텍스트 분석부(212e)와 프로토콜 분석부(220e)의 소스 분석부(222e)가 사용자 단말(52)에 구현될 수 있다.

[0044] 이와 같이 본 발명의 한 실시예에 따르면, IP 멀티미디어 스팸을 차단하기 위한 모듈 및/또는 기능을 IP 응용 서비스를 제공하는 네트워크 상의 적절한 엔터티에 구현함으로써, 인터넷 전화, 메시징 서비스 등의 다양한 IP 응용 서비스에서 발생할 수 있는 IP 멀티미디어 스팸을 효과적으로 식별 및 차단할 수 있다.

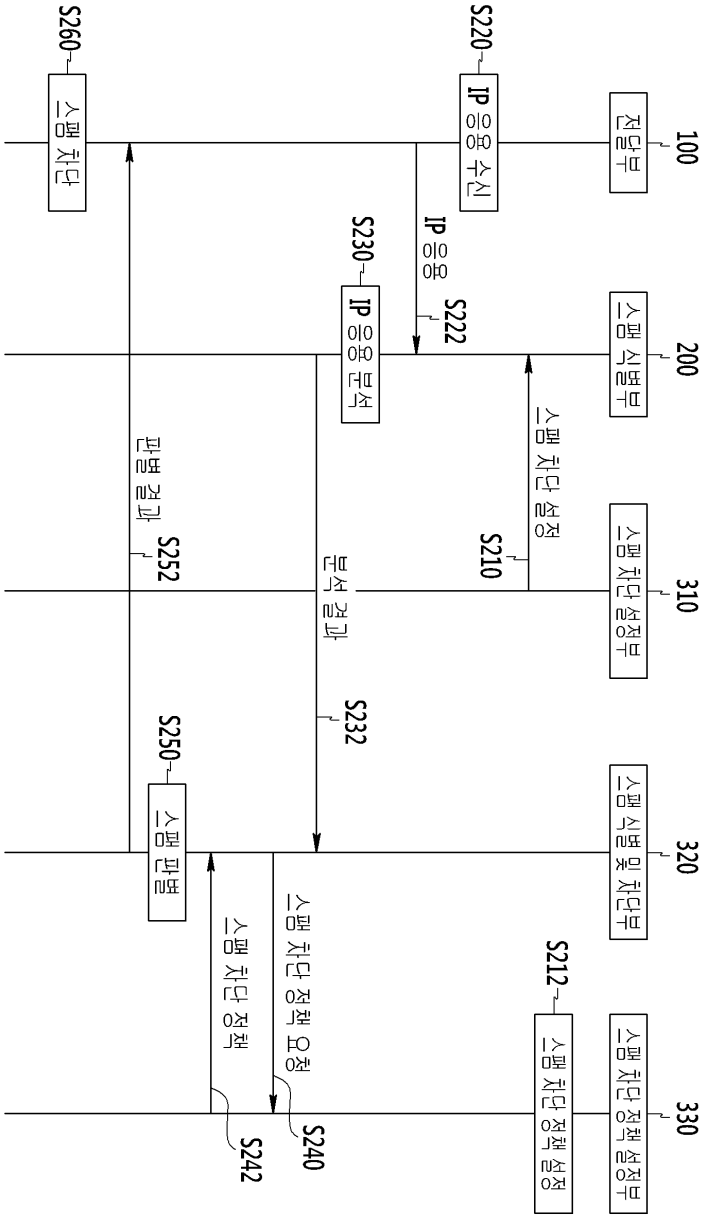
[0045] 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

## 도면

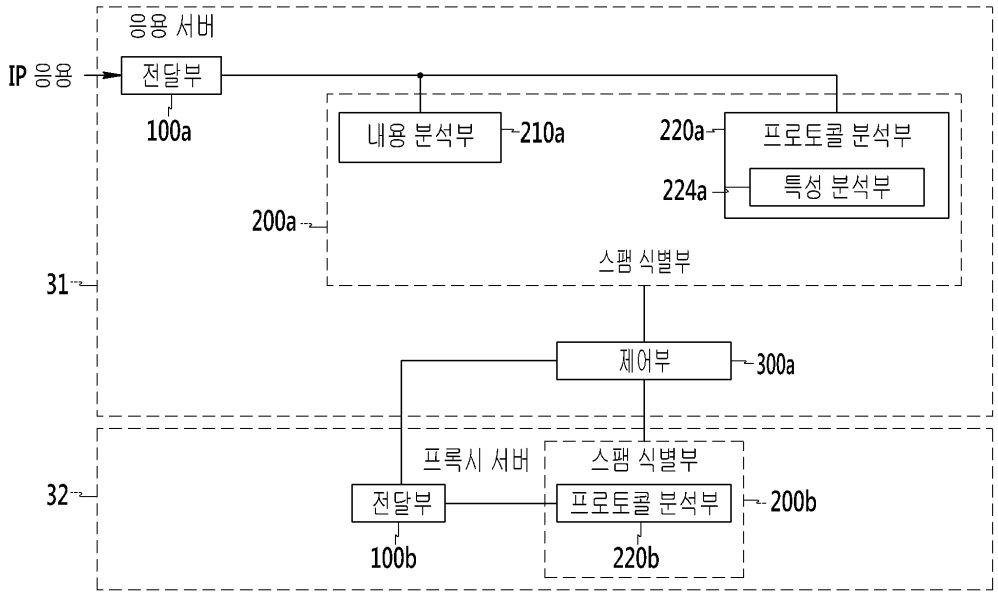
### 도면1



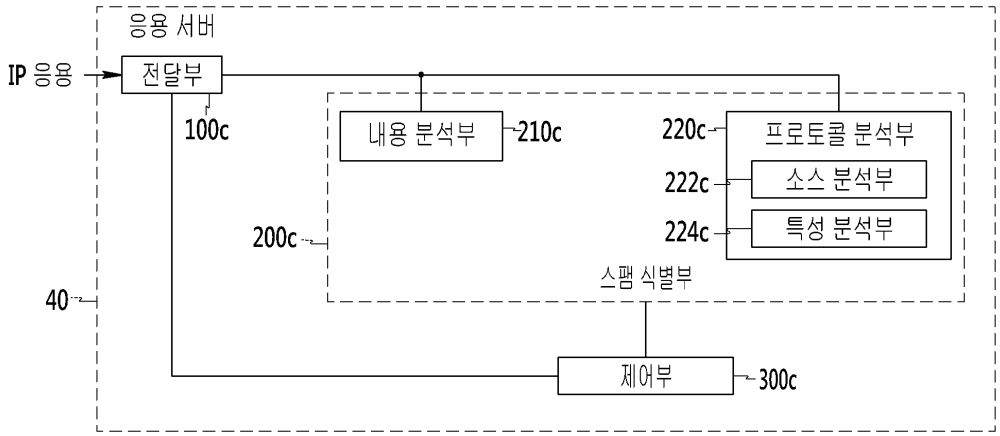
도면2


100
전달부
200
스팸 식별부
310
스팸 차단 설정부
320
스팸 식별 및 차단부
330
스팸 차단 정책 설정부
S220
IP 응용 수신
S230
IP 응용 분석
S260
스팸 차단
S222
IP 응용
S210
스팸 차단 설정
S252
판별 결과
분석 결과
S232
S250
스팸 판별
S212
스팸 차단 정책 설정
스팸 차단 정책 요청
S240
스팸 차단 정책
S242

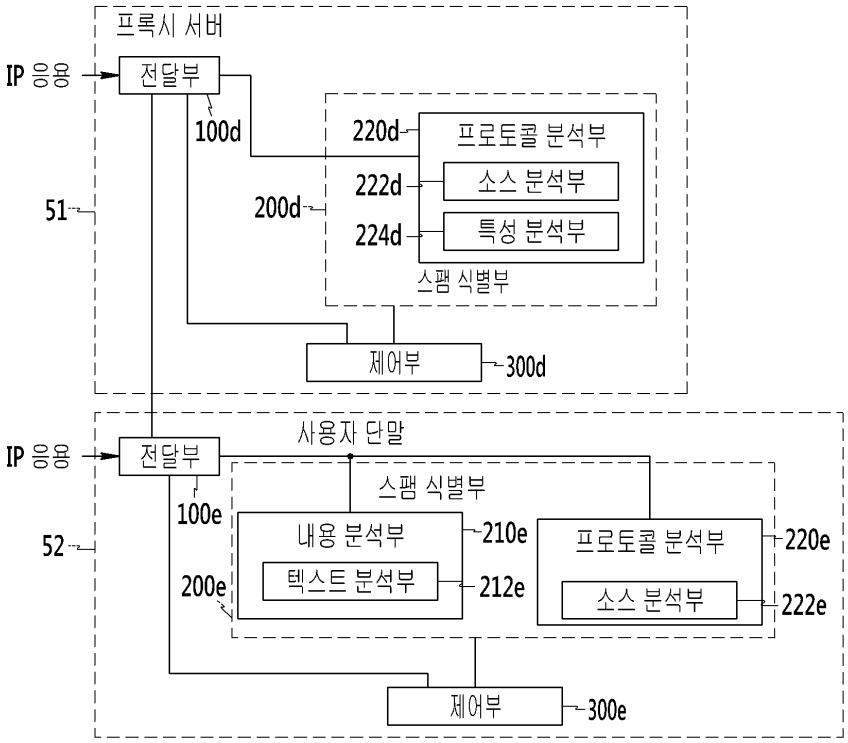
도면3


응용 서버
IP 응용
전달부
100a
내용 분석부
210a
220a
프로토콜 분석부
224a
특성 분석부
200a
스팸 식별부
31
제어부
300a
프록시 서버
스팸 식별부
32
전달부
프로토콜 분석부
200b
100b
220b

도면4


응용 서버
IP 응용
전달부
100c
내용 분석부
210c
220c
프로토콜 분석부
222c
소스 분석부
224c
특성 분석부
200c
스팸 식별부
40
제어부
300c

도면5


프록시 서버
IP 응용
전달부
100d
220d
프로토콜 분석부
222d
소스 분석부
200d
224d
특성 분석부
51
스팸 식별부
제어부
300d
사용자 단말
IP 응용
전달부
스팸 식별부
100e
내용 분석부
210e
프로토콜 분석부
220e
52
200e
텍스트 분석부
212e
소스 분석부
222e
제어부
300e