(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년12월07일
(11) 등록번호 10-1208943
(24) 등록일자 2012년11월30일

(51) 국제특허분류(Int. Cl.)
G06Q 50/00 (2006.01) *G06F 21/00* (2006.01)
G06F 15/00 (2006.01)
(21) 출원번호 10-2006-7024774
(22) 출원일자(국제) 2005년03월29일
심사청구일자 2010년03월29일
(85) 번역문제출일자 2006년11월24일
(65) 공개번호 10-2007-0054144
(43) 공개일자 2007년05월28일
(86) 국제출원번호 PCT/US2005/010276
(87) 국제공개번호 WO 2005/109234
국제공개일자 2005년11월17일
(30) 우선권주장
10/832,407 2004년04월26일 미국(US)
(56) 선행기술조사문헌
US06266664 B1
US20020199095 A1
전체 청구항 수 : 총 38 항

(73) 특허권자
구글 잉크.
미국 캘리포니아 마운틴 뷰 앰피씨어터 파크웨이 1600 (우편번호 94043)
(72) 발명자
런드, 피터, 케이.
미국 캘리포니아 94105, 샌프란시스코, 1 스트리트 샵201, 346
페트리, 스콧, 엠.
미국 캘리포니아 94025, 멘로 파크, 올드 페이지 밀 로드 2102
티투스, 제이슨, 에이치.
미국 캘리포니아 94301, 팔로 알토, 하이 스트리트 344
(74) 대리인
장훈

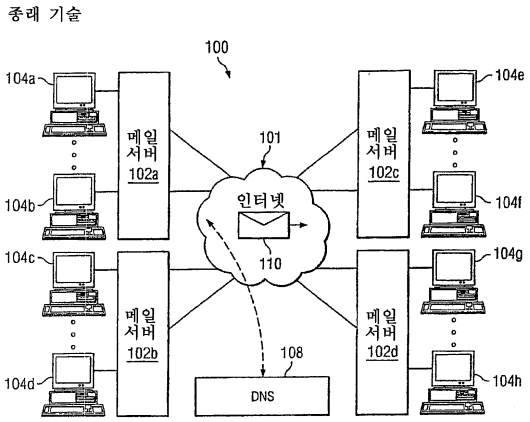
심사관 : 최석규

(54) 발명의 명칭 **비즈니스 휴리스틱들을 사용하여 전자 메시지들을필터링하는 시스템 및 방법**

(57) 요 약

본 발명은 비즈니스 휴리스틱을 사용하여 전자 메시지들을 필터링하는데 사용하는 시스템들 및 방법들에 관한 것이다. 일 양상에 있어서, 본 방법은 상기 전자 메시지가 적정 비즈니스와 연관되는지의 여부를 결정하는 단계; 및 상기 전자 메시지가 상기 적정 비즈니스와 연관되는 것으로 결정되는 경우에 상기 메시지의 의도된 수신자에게 상기 전자 메시지를 전송할 가능성을 조절하는 단계를 포함한다. 특정 실시예에 있어서, 본 방법은 상기 전자 메시지가 상기 의도된 수신자에 의하여 원해질 가능성에 기초하여 상기 전자 메시지에 스팸-스코어를 할당하는 단계; 상기 스팸-스코어가 전체 임계치를 초과하지 않을 때 상기 의도된 수신자로의 상기 전자 메시지의 전송을 차단하는 단계; 및 상기 전자 메시지가 상기 적정 비즈니스와 연관되는 것으로 결정될 때 상기 조절된 가능성에 기초하여 상기 의도된 수신자에게 상기 전자 메시지를 전송하는 단계를 더 포함한다.

대 표 도 - 도1



특허청구의 범위

청구항 1

비즈니스 휴리스틱(heuristic)들을 사용하여 전자 메시지를 필터링하는 방법에 있어서,

컴퓨터 네트워크상에서 작동하는 메시지 관리 서버에서 전자 메시지를 수신하는 단계;

상기 전자 메시지와 연관되는 소스가 적정(desirable) 비즈니스와 연관되는지의 여부를 결정하는 단계로서, 상기 결정은 비즈니스 휴리스틱에 기초하는, 상기 결정 단계;

상기 관리 서버와 연관된 메시지 핸들러를 이용하여, 상기 전자 메시지의 의도된 수신자에 대한 그것의 비적정성을 나타내는 특징에 대해 상기 전자 메시지를 검사하는 단계;

상기 검사에 기초하여 상기 전자 메시지에 스팸-스코어를 할당함으로써, 상기 검사에 기초하여 상기 메시지 핸들러를 가지고, 상기 전자 메시지를 상기 의도된 수신자에게 전송하는 것이 차단되어야 하는 가능성(likelihood)을 설정하는 단계;

상기 메시지 핸들러와 연관되는 하나 이상의 휴리스틱들 모듈들을 이용하여 상기 전자 메시지가 적정 비즈니스와 연관되는지의 여부를 결정하는 단계;

상기 전자 메시지가 상기 적정 비즈니스와 연관되는 것으로 결정되는 경우에, 비즈니스 임계치 양에 비례하는 양만큼 전체 임계치를 조절함으로써, 상기 전자 메시지를 상기 메시지의 상기 의도된 수신자에게 전송하는 것이 차단되어야 하는 가능성을 상기 메시지 핸들러를 가지고 자동으로 감소시키는 단계; 및

상기 스팸-스코어와 상기 조절된 전체 임계치의 비교에 따라 상기 의도된 수신자로의 상기 전자 메시지를 차단 또는 전송하는 단계로서, 상기 비즈니스 임계치의 양은 상기 의도된 수신자 또는 관리자에 의해 조절될 수 있는, 상기 차단 또는 전송 단계를 포함하는, 전자 메시지 필터링 방법.

청구항 2

제 1 항에 있어서, 상기 전자 메시지가 상기 의도된 수신자에 의하여 원해질 가능성에 기초하여 상기 전자 메시지에 스팸-스코어를 할당하는 단계;

상기 스팸-스코어가 전체 임계치를 초과하지 않을 때 상기 의도된 수신자로의 상기 전자 메시지의 전송을 차단하는 단계; 및

상기 전자 메시지가 상기 적정 비즈니스와 연관되는 것으로 결정될 때 상기 조절된 가능성에 기초하여 상기 의도된 수신자에게 상기 전자 메시지를 전송하는 단계를 더 포함하는, 전자 메시지 필터링 방법.

청구항 3

제 2 항에 있어서, 상기 전송 차단 단계는 상기 스팸-스코어가 전체 임계치를 초과하지 않을 때 상기 의도된 수신자로의 상기 전자 메시지의 전송을 차단하는 단계를 더 포함하는, 전자 메시지 필터링 방법.

청구항 4

제 3 항에 있어서, 상기 전자 메시지가 상기 적정 비즈니스와 연관되는 것으로 결정되는 경우에 상기 전송을 수행하기 위하여 상기 전체 임계치를 감소시키는 단계를 더 포함하는, 전자 메시지 필터링 방법.

청구항 5

제 1 항에 있어서, 상기 적정 비즈니스는 비즈니스의 유형인, 전자 메시지 필터링 방법.

청구항 6

제 1 항에 있어서, 상기 전자 메시지의 상기 소스가 상기 적정 비즈니스와 연관되는 것으로 결정되는 경우에 상기 전송을 수행하기 위하여 상기 전체 임계치를 감소시키는 단계를 더 포함하는, 전자 메시지 필터링 방법.

청구항 7

제 1 항에 있어서, 상기 적정 비즈니스는 법률 전문직과 연관되는 하나 이상의 비즈니스들과 연관되는, 전자 메

시지 필터링 방법.

청구항 8

제 1 항에 있어서, 상기 소스가 상기 적정 비즈니스와 연관되는지의 여부를 결정하는 단계는 상기 소스의 IP 어드레스를 상기 의도된 수신자의 IP 어드레스 중 적어도 하나와 비교하는 단계, 상기 소스 IP 어드레스에 의한 이전 접속 시도들을 비교하는 단계, 상기 소스 IP 어드레스와 상기 의도된 수신자 간의 이전 메시지 트래픽을 비교하는 단계, 소스 IP 어드레스가 외부 검증 프로세스들을 통해 특정 비즈니스와 관련되도록 할당되는 경우 또는 비즈니스 내에서 다른 의도된 수신자들과 상기 소스 IP 어드레스 간의 이전 메시지 트래픽을 비교하는 단계 중 하나 이상을 포함하는, 전자 메시지 필터링 방법.

청구항 9

제 1 항에 있어서, 비즈니스와 연관된 키 용어들 또는 어구들에 기초하여, 상기 적정 비즈니스에 의하여 사용될 전자 메시지에서 비즈니스 콘텐트의 존재를 결정하는 단계; 및 상기 전자 메시지가 상기 적정 비즈니스와 연관되는 비즈니스 콘텐트와 연관되는 것으로 결정되는 경우에 상기 전자 메시지를 상기 메시지의 상기 의도된 수신자에게 전송하는 것이 차단되어야 하는 가능성을 감소시키는 단계를 더 포함하는, 전자 메시지 필터링 방법.

청구항 10

제 9 항에 있어서, 상기 비즈니스 콘텐트의 존재에 기초하여 상기 전체 임계치를 조절함으로써 유효 임계치를 생성하는 단계; 및

상기 스팸-스코어가 상기 유효 임계치를 초과하지 않는 경우에 상기 의도된 수신자로의 상기 전자 메시지의 전송을 차단하는 단계를 더 포함하는, 전자 메시지 필터링 방법.

청구항 11

제 9 항에 있어서, 상기 비즈니스 콘텐트의 존재의 결정 단계를 관리하기 위하여 비즈니스 임계치를 설정하는 단계를 더 포함하는, 전자 메시지 필터링 방법.

청구항 12

제 11 항에 있어서, 상기 비즈니스 임계치 양에 비례하는 양만큼 상기 전체 임계치를 조절함으로써 유효 임계치를 생성하는 단계를 더 포함하는, 전자 메시지 필터링 방법.

청구항 13

제 11 항에 있어서, 상기 비즈니스 임계치 양은 상기 의도된 수신자에 기초하여 지정되는, 전자 메시지 필터링 방법.

청구항 14

제 9 항에 있어서, 적어도 하나의 기본 임계치에 대응하는 상기 전자 메시지에서 불쾌한(offending) 콘텐트의 존재를 결정하는 단계를 더 포함하며, 상기 불쾌한 콘텐트의 존재는 유효 임계치를 생성하기 전에 상기 전체 임계치를 조절하고,

상기 불쾌한 콘텐트는 성적으로 노골적인 콘텐트, 일확천금 콘텐트, 및 인종 차별적 콘텐트 중 적어도 하나를 포함하는, 전자 메시지 필터링 방법.

청구항 15

제 14 항에 있어서, 상기 적어도 하나의 기본 임계치 양은 상기 전자 메시지의 상기 의도된 수신자에 기초하여 지정되는, 전자 메시지 필터링 방법.

청구항 16

삭제

청구항 17

제 14 항에 있어서, 적어도 하나의 기본 임계치 양에 비례하는 양만큼 상기 전체 임계치를 조절하는 단계를 더 포함하는, 전자 메시지 필터링 방법.

청구항 18

제 2 항에 있어서, 상기 전체 임계치는 상기 전자 메시지의 상기 의도된 수신자에 기초하여 지정되는, 전자 메시지 필터링 방법.

청구항 19

제 1 항에 있어서, 상기 적정 비즈니스는 법률 전문직 및 금융 전문직들로 이루어진 그룹으로부터 선택되는, 전자 메시지 필터링 방법.

청구항 20

제 1 항에 있어서, 상기 의도된 수신자는 상기 적정 비즈니스와 연관되는, 전자 메시지 필터링 방법.

청구항 21

비즈니스 휴리스틱들을 사용하여 전자 메시지를 필터링하는 시스템에 있어서, 상기 시스템은 메시지 핸들러를 포함하고, 상기 메시지 핸들러는:

컴퓨터 네트워크상에서 작동하는 메시지 관리 서버에서 전자 메시지를 수신하고;

상기 전자 메시지와 연관되는 소스가 적정(desirable) 비즈니스와 연관되는지의 여부를 결정하고, 상기 결정은 비즈니스 휴리스틱에 기초하고;

상기 전자 메시지의 의도된 수신자에 대한 그것의 비적정성을 나타내는 특징에 대해 상기 전자 메시지를 검사하고;

상기 검사에 기초하여 상기 전자 메시지에 스팸-스코어를 할당함으로써 상기 전자 메시지를 상기 의도된 수신자에게 전송하는 것이 차단되어야 하는 가능성을 설정하고;

상기 메시지 핸들러와 연관되는 하나 이상의 휴리스틱들 모듈들을 이용하여 상기 전자 메시지가 적정 비즈니스와 연관되는지의 여부를 결정하고;

상기 전자 메시지가 상기 적정 비즈니스와 연관되는 것으로 결정되는 경우에, 비즈니스 임계치 양에 비례하는 양만큼 전체 임계치를 조절함으로써, 상기 전자 메시지를 상기 메시지의 상기 의도된 수신자에게 전송하는 것이 차단되어야 하는 가능성을 자동으로 감소시키며;

상기 스팸-스코어와 상기 조절된 전체 임계치의 비교에 따라 상기 의도된 수신자로의 상기 전자 메시지를 차단 또는 전송하고, 상기 비즈니스 임계치의 양은 상기 의도된 수신자 또는 관리자에 의해 조절될 수 있도록 구성되는, 전자 메시지 필터링 시스템.

청구항 22

제 21 항에 있어서, 상기 메시지 핸들러와 연관되고 상기 전자 메시지가 상기 전자 메시지의 상기 의도된 수신자에 의하여 원해질 가능성에 기초하여 상기 전자 메시지에 스팸-스코어를 할당하도록 구성된 소프트웨어 모듈을 더 포함하며, 상기 메시지 핸들러는 상기 스팸-스코어가 전체 임계치를 초과하지 않을 때 상기 의도된 수신자로의 상기 전자 메시지의 전송을 차단하도록 또한 구성되는, 전자 메시지 필터링 시스템.

청구항 23

제 22 항에 있어서, 상기 메시지 핸들러는 상기 스팸-스코어가 전체 임계치를 초과하지 않을 때 상기 의도된 수신자로의 상기 전자 메시지의 전송을 차단하도록 또한 구성되는, 전자 메시지 필터링 시스템.

청구항 24

제 23 항에 있어서, 상기 메시지 핸들러는 상기 전자 메시지가 상기 적정 비즈니스와 연관되는 것으로 결정되는 경우에 상기 전송을 수행하기 위하여 상기 전체 임계치를 감소시키도록 또한 구성되는, 전자 메시지 필터링 시스템.

청구항 25

제 21 항에 있어서, 상기 메시지 핸들러는:

상기 전자 메시지의 상기 소스가 상기 적정 비즈니스와 연관되는지의 여부를 결정하고;

상기 전자 메시지의 상기 소스가 상기 적정 비즈니스와 연관되는 것으로 결정되는 경우에 상기 의도된 수신자로의 상기 전자 메시지를 전송할 가능성을 증가시키도록 또한 구성되는, 전자 메시지 필터링 시스템.

청구항 26

제 25 항에 있어서, 상기 메시지 핸들러는 또한, 상기 전자 메시지의 상기 소스가 상기 적정 비즈니스와 연관되는 것으로 결정되는 경우에 상기 전송을 수행하기 위하여 상기 전체 임계치를 감소시키도록 또한 구성되는, 전자 메시지 필터링 시스템.

청구항 27

제 25 항에 있어서, 상기 소스는 상기 전자 메시지의 전송 서버의 인터넷 프로토콜(IP) 어드레스를 포함하는, 전자 메시지 필터링 시스템.

청구항 28

제 27 항에 있어서, 상기 메시지 핸들러는, 상기 소스의 IP 어드레스와 상기 의도된 수신자의 IP 어드레스 중 적어도 하나와의 비교, 상기 소스 IP 어드레스에 의한 이전 접속 시도들의 비교, 상기 소스 IP 어드레스와 상기 의도된 수신자 간의 이전 메시지 트래픽의 비교, 및 상기 소스 IP 어드레스가 외부 검증 프로세스들을 통해 특정 비즈니스와 관련되도록 할당되는 경우 또는 비즈니스 내에서 다른 의도된 수신자들과 상기 소스 IP 어드레스 간의 이전 메시지 트래픽의 비교 중 하나 이상에 의하여, 상기 소스가 상기 적정 비즈니스와 관련되는지의 여부를 결정하도록 구성되는, 전자 메시지 필터링 시스템.

청구항 29

제 21 항에 있어서, 상기 적정 비즈니스는 비즈니스의 유형인, 전자 메시지 필터링 시스템.

청구항 30

제 21 항에 있어서, 상기 메시지 핸들러는:

비즈니스 콘텐트의 존재에 기초하여 상기 전체 임계치를 조절함으로써 유효 임계치를 생성하고;

상기 스팸-스코어가 상기 유효 임계치를 초과하지 않는 경우에 상기 의도된 수신자로의 상기 전자 메시지의 전송을 차단하도록 또한 구성되는, 전자 메시지 필터링 시스템.

청구항 31

제 21 항에 있어서, 상기 메시지 핸들러는 비즈니스 콘텐트의 존재의 결정을 관리하기 위하여 비즈니스 임계치를 포함하는, 전자 메시지 필터링 시스템.

청구항 32

제 31 항에 있어서, 상기 메시지 핸들러는 상기 비즈니스 임계치 양에 비례하는 양만큼 상기 전체 임계치를 조절함으로써 유효 임계치를 생성하도록 또한 구성되는, 전자 메시지 필터링 시스템.

청구항 33

제 31 항에 있어서, 상기 비즈니스 임계치 양은 상기 의도된 수신자에 기초하여 지정되는, 전자 메시지 필터링 시스템.

청구항 34

제 21 항에 있어서, 적어도 하나의 기본 임계치에 대응하는 상기 전자 메시지에서 불쾌한 콘텐트의 존재를 결정하도록 구성되고, 상기 불쾌한 콘텐트의 존재에 기초하여 유효 임계치를 생성하기 전에 상기 전체 임계치를 조

절하도록 또한 구성되는 소프트웨어 모듈을 더 포함하고,

상기 불쾌한 콘텐트는 성적으로 노골적인 콘텐트, 일확천금 콘텐트, 및 인종 차별적 콘텐트 중 적어도 하나를 포함하는, 전자 메시지 필터링 시스템.

청구항 35

제 34 항에 있어서, 상기 적어도 하나의 기본 임계치 양은 상기 전자 메시지의 상기 의도된 수신자에 기초하여 지정되는, 전자 메시지 필터링 시스템.

청구항 36

삭제

청구항 37

제 34 항에 있어서, 상기 소프트웨어 모듈은 적어도 하나의 기본 임계치 양에 비례하는 양만큼 상기 전체 임계치를 조절하도록 또한 구성되는, 전자 메시지 필터링 시스템.

청구항 38

제 22 항에 있어서, 상기 전체 임계치는 상기 전자 메시지의 상기 의도된 수신자에 기초하여 지정되는, 전자 메시지 필터링 시스템.

청구항 39

제 21 항에 있어서, 상기 적정 비즈니스는 법률 전문직 및 금융 전문직들로 이루어진 그룹으로부터 선택되는, 전자 메시지 필터링 시스템.

청구항 40

제 21 항에 있어서, 상기 의도된 수신자는 상기 적정 비즈니스와 연관되는, 전자 메시지 필터링 시스템.

명 세 서

기 술 분 야

[0001] 본 출원은 본 발명의 개시자에게 양도되고, 본 명세서의 모든 목적들을 위해 전체적으로 참조문헌으로서 통합된 "이-메일 관리 서비스들"이라는 명칭으로 2003년 2월 19일에 출원된 공동-계류중인 특허출원번호 제10/370,118호에 관한 것이다.

[0002] 본 명세서에 기술된 실시예들은 일반적으로 전자 메시지들(이-메일)의 필터링, 특히 비즈니스 휴리스틱들을 사용하여 전자 메시지들을 필터링하는 시스템 및 방법에 관한 것이다.

배 경 기 술

[0003] 이-메일은 보통 사용자/가입자들을 가지는 ISP들에 의하여 또는 이-메일 사용자들이 고용된 시설들에 배치된 회사 서버들에 의하여 관리된다. 이-메일 관리의 일부분은 스팸 또는 바이러스를 제어하는 필터링 단계를 포함하며, 이러한 이-메일 관리가 ISP에서 또는 회사 서버 위치에서 수행될 때 적정 통신 대역폭 및 자원들의 계산은 가짜 이-메일 트래픽의 라우팅, 분석, 및 다른 조절시에 소비된다. 기존의 이-메일 관리 시스템들은 이-메일 트래픽 또는 SMTP 접속 상황들에 관한 규칙들의 실시간 모니터링, 피드백 및 업데이팅이 결여된 것에 특징이 있다. 따라서, 이-메일 트래픽 상황들의 관리 및 모니터링은 보통 인간의 개입을 통해 조절된다.

[0004] 비록 이들의 문제점들이 현대의 이-메일 관리 시스템들에서 해결될지라도, 전형적으로 원치 않는 스팸 메시지들을 필터링하기 위하여 사용되는 기술들은 전체적으로 비교적 비효율적이다. 특히, 종래의 기술들이 발전함에 따라, 스팸 메시지들의 송신자들에 의하여 사용되는 기술들은 가장 공격적인 방법들로 교묘하게 회피하고 있다. 게다가, 필터링 기술들이 의도된 수신자들에게 원치 않는 메시지들이 도달하는 것을 방지할 때 성공적인 상황들에서조차, 많은 다른 유효 메시지들이 전송시에 차단된다. 원치 않는 메시지들을 차단하기 위하여 종래의 시스템을 사용할 때 성가신 문제점들 중 하나는 메시지가 유효 전송자에 의하여 전송되는 것으로 믿도록 필터링 시스템을 속이는 이-메일 어드레스들의 스푸핑(spoofing) 현상이다. 그 결과, 그 사용자들에 의하여 "승인된 전

송자들"을 사용하는 필터링 시스템들은 상기의 공격들에 대하여 여전히 비효율적이다. 더욱이, 앞서 언급된 바와 같이, 종래의 시스템들이 상기 공격들을 방지할 때 지원하는 이용가능한 도구들로 업그레이드되는 경우에, 최종 결과는 전형적으로 많은 유효 메시지들이 사용자에게 도달되지 않는다는 점이며, 이는 시간 및 비용 측면에서 손실을 초래한다.

발명의 상세한 설명

[0005] 본 발명은 비즈니스 휴리스틱을 사용하여 전자 메시지들을 필터링하는데 사용하는 시스템들 및 방법들을 개시한다. 본 명세서에서 사용되는 바와 같이, 용어 "비즈니스"는 비즈니스 조직 또는 임의의 하나의 자본가 노력에 제한되지 않고, 오히려 임의의 및 모든 조직들을 포함하고 전문적, 산업적, 서비스-지향, 자선, 셀프-서비스 등을 포함하는 모든 노력들을 포함한다. 일 양상에 있어서, 본 방법은 전자 메시지가 적정(desirable) 비즈니스와 연관되는지의 여부를 결정하는 단계, 및 전자 메시지가 적정 비즈니스와 연관되는 것으로 결정되는 경우에 메시지의 의도된 수신자에게 전자 메시지를 전송하는 가능성을 조절하는 단계를 포함한다. 특정 실시예에 있어서, 본 방법은 전자 메시지가 의도된 수신자에 의하여 원한다는 가능성에 기초하여 전자 메시지에게 스팸-스코어를 할당하는 단계, 스팸-스코어가 전체 임계치를 넘지 않을 때 의도된 수신자에게 전자 메시지의 전송을 차단하는 단계, 및 전자 메시지가 적정 비즈니스와 연관되는 것으로 결정될 때 조절된 가능성에 기초하여 의도된 수신자에게 전자 메시지를 전송하는 단계를 포함한다.

[0006] 또 다른 양상에서는, 비즈니스 휴리스틱(heuristic)들을 사용하여 전자 메시지를 필터링하는 관련 시스템이 또한 기술된다. 일 실시예에 있어서, 시스템은 전자 메시지를 수신하도록 구성된 메시지 핸들러, 및 메시지 핸들러와 연관되고 전자 메시지가 적정 비즈니스와 연관되는지의 여부를 결정하도록 구성된 휴리스틱들 모듈을 포함한다. 이러한 실시예에 있어서, 메시지 핸들러는 전자 메시지가 적정 비즈니스와 연관되는 것으로 결정되는 경우에 전자 메시지가 의도된 수신자에게 전송되는 가능성을 조절하도록 또한 구성된다. 특정 실시예에 있어서, 이러한 시스템은 메시지 핸들러와 연관되며 전자 메시지가 전자 메시지의 의도된 수신자에 의하여 원해진다는 가능성에 기초하여 전자 메시지에 스팸-스코어를 할당하도록 구성된 소프트웨어 모듈을 포함하며, 여기서 메시지 핸들러는 스팸-스코어가 전체 임계치를 초과하지 않을 때 의도된 수신자에게 전자 메시지의 전송을 차단하도록 또한 구성된다.

[0007] 첨부된 도면들과 함께 이하의 바람직한 실시예들의 상세한 설명이 지금 참조된다. 다양한 특징들은 실제 크기로 도시되지 않음을 강조한다. 사실상, 다양한 특징들의 크기들은 논의를 명확하게 하기 위하여 임의적으로 증가 또는 감소될 수 있다. 첨부 도면들과 함께 이하의 상세한 설명이 지금 참조될 것이다.

실 시 예

[0015] 도 1을 먼저 참조하면, 인터넷(101) 또는 다른 컴퓨터 네트워크를 통해 이-메일 메시지들을 전송하는 종래 기술의 시스템(100)에 대한 일 실시예가 예시되어 있다. 전송 메일 서버들(102a, 102b)(연관된 소스 인터넷 프로토콜(IP) 어드레스들을 가짐) 및 수신 메일 서버들(102c, 102d)(연관된 목적지 IP 어드레스들을 가짐) 또는 다른 메시지 게이트웨이들은 전자 메일들(또는 "이-메일")과 같은 전자 메시지들이 전송 클라이언트 머신들(104a 내지 104d)로부터 수신 클라이언트 머신들(104e 내지 104h)로, 또는 셀 전화들, 페이저들, 및/또는 휴대용 컴퓨터들과 같은 다른 장치들로 전송되도록 한다. 종래의 시스템들에서, 이-메일들의 전송 방향은 반전될 수 있으며, 여기서 전송 머신들 및 서버들은 수신 머신들 및 서버들이 되고 역도 가능하다.

[0016] 이-메일 메시지들은 전형적으로 클라이언트 머신(104) 상에서 실행되는 애플리케이션에 의하여 구성된다. 메시지의 구성이 완료될 때, 사용자는 완료된 메시지를 메일 서버(102)에 업로드 한다. 일 실시예에 있어서, 메일 서버(102)는 인터넷 서버 제공자(ISP) 및 사용자가 일하는 개인 기업에 의하여 소유된다. 사용자 클라이언트 머신(104)은 다이얼-업, 디지털 가입자 루프(DSL), 케이블 인터넷을 통해 또는 다른 적절한 수단에 의하여 메일 서버(102)에 접속한다. 이-메일 포맷들에 대한 하나의 표준은 각각 인터넷 엔지니어링 태스크 포스("IETF")에 의하여 반포된 표준 및 제안된 표준인, RFC2822에 의하여 구식이 된 RFC 822에 의하여 기술된다. 이-메일 메시지들이 전송 메일 서버(102)로부터 수신 메일 서버(102)로 전송되는 프로토콜은 IETF의 표준 및 제안된 표준인, RFC2821에 의하여 구식이 된 RFC821에 의하여 기술된다. 이들 표준들은 www.ietf.org에서 발견될 수 있다. 본 설명은 RFC 821 및 RFC 822 표준들 및 RFC 2821 및 RFC 2822 제안된 표준들의 요지를 참조에 의하여 여기에 통합한다. 만일 제안된 표준들이 2001년 4월에 반포된 버전들로부터 업데이트 되면, 이는 여기에 참조문헌으로서 통합되는 이들 제안된 표준들의 2001년 4월 버전들의 요지이다. RFC 821 및 RFC 2821 문헌들은 이-메일 메시지들이 전형적으로 인터넷을 통해 전송되는 프로토콜인 단순 메일 전송 프로토콜("SMTP")을 기술하고 있다.

[0017] SMTP 서버들 및 SMTP 클라이언트들(SMTP 클라이언트들은 클라이언트 머신들(104)과 혼란되지 않을 네트워크 컴퓨터들)은 메일 전송 서비스를 제공하며 이에 따라 메일 전송 에이전트들("MTA")로서 작동한다. 메일 사용자 에이전트들("MUA" 또는 "UA")은 보통 메일의 소스들 및 목표들로서 생각된다. 소스에서, MUA는 사용자로부터 전송될 메일을 수집하여 이를 네트워크(101) 내의 MTA에 넘겨주는 소스 메일 서버(102a, 102b)일 수 있다. 최종("전송") MTA는 사용자의 인박스(inbox) 내에 사용자 메일을 보유하는 목적지 메일 서버(102c, 102d)일 수 있는 MUA로 넘겨주는 것으로 생각된다.

[0018] SMTP 메일 전송 프로토콜은 이메일의 전송자로부터 수신기로 메시지들을 라우팅하기 위하여 도메인 이름들을 사용한다. 특정 도메인 이름들에 대응하는 TCP/IP 어드레스들의 분산된 데이터베이스는 도메인 이름 서버들("DNS's")(108)에서 인터넷(101)을 통해 유지된다. 따라서, 그것의 목적지에 이-메일을 라우팅하기 위하여, 소스 메일 서버들(102a, 102b)은 전송 사용자에 의하여 특정된 어드레스를 선택하여 특정 어드레싱된 도메인 이름에 할당될 IP 어드레스를 DNS 서버(108)에 묻는다. 본 명세서에서 사용되는 바와 같이, "어드레스"는 메일이 전송될 사용자, 메일을 전송하는 사용자 또는 소스, 또는 메일이 부착될 위치를 식별하는 문자 스트링이다. 용어 "메일박스"는 저장소를 언급한다. 두개의 용어들은 전형적으로 메일이 배치되는 위치(메일박스) 및 메일에 대한 기준(어드레스) 간의 구별이 중요하지 않은 경우에 서로 교환하여 사용된다. 어드레스는 보통 사용자 및 도메인 규정들로 구성되나, 어드레스들은 어드레스의 사용 및 유형에 따라 다른 형태들을 가질 수 있다. 표준 메일박스 명명 규칙은 "local-part@domain"인 것으로 정의되며, 동시 사용은 단순한 "사용자 이름들"보다 훨씬 더 넓은 애플리케이션들의 세트를 허용한다. 어드레스의 로컬 부분은 전형적으로 어드레스의 도메인 부분에서 특정된 호스트에 의해서만 해석 및 할당된 시맨틱스이다. 대조적으로, 표준 IP 어드레스는 전형적으로 소스 또는 목적지 서버를 식별하는 숫자들의 특정 스트링이다.

[0019] 일단 이메일이 처리를 위하여 전송될 도메인을 소스 메일 서버(102a, 102b)가 어휘로 식별하면, DNS 룩업(lookup)은 DNS 서버(108)를 통해 도메인 이름을 분석하도록 수행된다. 그 후, 이메일(110)은 소스 메일 서버(102a, 102b)로부터 인터넷(101)을 통해 식별된 도메인으로 전송된다.

[0020] 도 2를 지금 참조하면, 액티브 전자 메시지(예컨대, 이-메일) 관리 시스템(EMS)(203)이 인터넷(101) 및 수신 메일 서버(202) 간에 제공되는 실시예를 기술한 블록도(200)가 예시되어 있다. 본 발명의 EMS(203)는 관리 프로세스의 다양한 단계들에서 인간이 개입할 필요성 없이 전자 메시지들의 시도된 전송들을 일정하게 관리하기 때문에 "액티브" 및 자동화된다. 이러한 의미에서, 본 명세서에 기술된 원리들에 따른 EMS(203)는 자동화되며, 실시간으로 메시지 전송을 관리하도록 구성된다.

[0021] EMS(203)는 조건들을 해석하고, 패턴들을 분석하며, 전송자 및 수신자 간의 SMTP 접속의 각각이 처리될 때 처리 단계들을 수행함으로써 수신 서버(202)에의 데이터 전송을 관리한다. 통상적인 이-메일 서버들은 전형적으로 메시지 데이터를 승인할 것이며 분석을 수행하기 전에 디스크에 메시지를 기록할 것이다. EMS(203)는 보안 및 관리를 제공하면서 목적지 서버(202)에 대한 충돌을 최소화하기 위하여 SMTP 트랜잭션의 각 스테이지에서 관리 단계들을 수행할 수 있다. 메일 서버(202), 및 수신 클라이언트의 터미널(204)을 위하여 의도된 메일이 EMS(203)를 통해 라우팅되도록, 목표 메일 서버(202)의 도메인 이름과 연관된 DNS(108)의 수치적 IP 어드레스는 EMS(203)의 수치적 어드레스를 반영하도록 업데이트된다. 예컨대, 메일 서버(202)의 도메인 이름이 "anywhere.com"이고 메일 서버(202) 및 EMS(203)에 대한 수치적 IP 어드레스들이 각각 "1234.5678.9876.5432" 및 "9876.5432.1234.5768"이라고 가정한다. 그 다음에, "anywhere.com"에 대한 분산된 DNS 데이터베이스(108)의 레코드들은 EMS의 수치적 어드레스 "1234.5678.9876.5432"보다 오히려 "9876.5432.1234.5768"를 반영하도록 업데이트된다.

[0022] 비록 도면이 메일 서버(202)에 물리적으로 인접한 것으로 EMS(203)을 도시할지라도, 이러한 배치는 단순히 예시 목적들로 제공된다. EMS(203)는 인터넷(101)상이 임의의 위치에 배치될 수 있다. EMS(203)는 위치 "A"(방화벽 외부) 또는 위치 "B"(방화벽 내부)에의 20방화벽(210)의 선택 위치설정(positioning)에 의하여 도시된 바와 같이 방화벽(210)과 연관된 메일 서버(202) 외부 또는 내부에 배치될 수 있다. 대안적으로, EMS(203)는 메일 서버(202)와 동일한 물리적 머신 상에서 실행될 수 있다.

[0023] 도 3을 지금 참조하면, 도 2에 도시된 EMS(203)의 블록도(300)를 포함하는 상세도가 예시되어 있다. 관리 콘솔(console)(기술되지 않음)은 EMS(203)가 입력 전자 메시지들을 처리하는 방법을 구성하는데 도움을 주는 관리 액세스 도구를 제공하는 실제 EMS 시스템(203)과 동일한 특정 서버 머신 상에 배치될 수 있다. EMS(203) 및 메일 서버들(102a, 102c) 간의 접속들은 인터넷 또는 SMTP 접속들을 통해 이루어질 수 있다. 이전에 언급된 바와 같이, EMS(203)는 메일 서버들(102a, 102c)을 가지거나 또는 가지지 않고 특정 방화벽 내부 또는 외부에 존재할

수 있다.

[0024] 일반적으로, 도 3에 도시된 시스템은 "전송" 메일 서버(102a)로부터의 이-메일을 조절한다. "전송자"로서의 하나의 메일 서버 및 "수신기"로서의 다른 메일 서버의 지정은 임의적이다. 실제로, 메일 서버들(102a, 102c)은 메일 서버(102a, 102c)로부터 그리고 메일 서버(102a, 102c)로의 전자 메시지를 클라이언트(104a, 104e)에 전송 및 수신하는 전송자 및 수신기로서 동작할 것이다. 기술된 실시예에 있어서, 메일 서버(102a, 102c)의 도메인 이름들 중 적어도 하나는 DNS 분산형 데이터베이스 및 이의 서버들(108)의 EMS(203)와 연관될 것이다. 관리 콘솔을 사용하는 실시예들에 있어서, 콘솔은 의심되는 바이러스들 및 스팸 이-메일들, 디렉토리 하베스트 공격들, 또는 사용자 또는 사용자들에게 전송된 원치 않는 콘텐트 또는 전송 시도들에 관한 정보와 같이 특정 사용자들 또는 사용자들의 그룹에 대하여 전송되는 전자 메시지들의 유형들에 관하여 EMS(203)로부터 정보를 수신한다.

[0025] EMS(203)는 전자 메시지들을 처리하는 소프트웨어 모듈들을 조절하는 여러 상호접속 메시지를 포함하는 것으로 도 3에 도시되어 있다. 더 상세한 논의를 위하여, 본 발명의 개시자에게 양도되었으며, 본 명세서의 모든 목적들을 위해 전체적으로 참조문헌으로 통합된 "이-메일 관리 서비스들"이라는 명칭으로 2003년 2월 19일에 출원된 공동 계류중인 특허출원번호 제10/370,118호를 참조한다. 이들 다양한 소프트웨어 모듈들의 레이아웃(layout)은 이들 소프트웨어 모듈들을 실행하는 머신의 임의의 특정 물리적 구조를 지시하지 않는다. 기술된 하나의 모듈은 접속 관리 모듈 또는 단순히 접속 관리자(322)이다. 접속 관리자(322)는 UA들/메일 서버들(102a)(또는 메일 전송 에이전트들)로부터의 입력 SMTP 접속들을 셋업 및 모니터링하는 역할을 한다. 접속 관리자(322)는 EMS(203)에 대한 엔트리 포인트이며, 또한 입력 SMTP 접속 시도들 및 이-메일 메시지들을 모니터링한다. 특정 처리들은 예컨대 소프트웨어 상주 프로그램에서 발견되며, 액티브될 수 있는 메시지들의 트래픽 내의 메시지들의 패턴들을 인식하기 위한 입력 메시지들 및/또는 접속 시도들로부터 수집된 데이터와 인터랙트한다. 특히, 접속 관리자(322), 이메일 핸들러(326), 플러그-인 애플리케이션들(332), 및 전송 관리 모듈(또는 단순히 전송 관리자(324)는 입력 전자 메시지들을 처리하기 위하여 모두 사용된다.

[0026] 이-메일 핸들러(326)는 입력 이-메일 메시지를 선택하여 메시지의 전송을 상당히 지연함이 없이 메시지로부터 정보를 "스크래프" 또는 추출할 수 있다. 이-메일 핸들러(326)는 그 자체에 따라 또는 명령들에 따라 전송 관리자(324)를 통해 메시지들을 조건부로 전송할 수 있다. 이-메일 핸들러(326)는 다목적 인터넷 메일 확장형(MIME) 디코더(328) 및 애플리케이션 인터페이스(330)에 개념적으로 접속된다. 애플리케이션 인터페이스(330)는 앞서 언급된 플러그-인 애플리케이션들(332) 및 이-메일 핸들러(326) 간에 인터페이스를 제공한다. 예컨대 연관된 데이터베이스에 저장된 규칙들에 의하여 설정된 구성에 뒤따라, 데이터의 패턴들은 배치 명령들의 형태로 정보를 처리하는 메시지가 생성될 수 있도록 결정될 수 있다. 만일 스팸 검출 애플리케이션과 같은 애플리케이션들(332) 중 하나가 메시지가 스팸이 아닐 가능성에 기초하여 메시지에 대한 값(즉, "스팸-스코어")을 리턴하면, 이-메일 핸들러(326)는 메시지를 검역 웹사이트에 라우팅하기 위하여 메시지의 전송을 구성할 수 있다.

[0027] 전자 메시지들이 통과되고 전환되고 연기되는지 등에 대한 결정들은 입력 메시지들의 모집단으로부터 생성된 메타데이터에 기초하고, EMS(203)가 구성되는 방식 및 메시지들을 처리하기 위하여 선택된 애플리케이션들(332)에 기초하여 이루어진다. 의도된 수신자로의 메시지의 전송을 막는 조건에 따르면, 비록 접속 관리자(322)에 의한 접속이 승인될지라도, 전송 관리자(324)는 메시지를 적절하게 배열하도록 명령될 수 있다.

[0028] 도 4를 지금 참조하면, 원치 않는 이-메일 메시지를 필터링하기 위하여 다중 임계치들을 설정하는 스크린 숏(screen shot)(400)의 일 실시예가 예시된다. 특히, 스크린 숏(400)은 입력 이메일들, 즉 "대용량 이-메일"에 대한 전체 임계치의 설정들을 조절할 기회를 기술한다. 더욱이, 스크린(400)은 특정 카테고리들, 즉 성적으로 노골적인, 일확천금, 특별 제공, 및 인종 차별적인 것에 기초하여 기본 임계치들의 설정들을 조절하도록 한다. 일단 사용자가 적정 선택 및 조절들을 수행하면, 스크린상의 "변화들을 저장" 버튼을 클릭함으로써 변화들이 저장될 수 있다. 더욱이, 만일 조절들이 유지되지 않으면, 사용자는 기술된 "삭제" 버튼을 클릭함으로써 단순히 변화들을 삭제할 수 있다.

[0029] "대용량 이-메일" 전체 임계치는 입력 이-메일 메시지들을 필터링하는 전체 허용 한계(tolerance)를 설정하기 위하여 사용된다. 특히, 이-메일 필터링 처리들은 전형적으로 이-메일이 스팸이 아닌 가능성(즉, 이-메일이 의도된 수신자에 의하여 반드시 원치 않는 것이 아닐 가능성)을 지시하는 모든 입력 이-메일들에 스팸-스코어를 할당한다. 물론, 스팸-스코어가 이메일이 스팸인 가능성에 기초하는 처리가 대안적으로 구성될 수 있다. 이러한 스팸-스코어들을 할당하기 위한 기본은 각각의 처리가 검사하도록 구성되는 기준에 기초하여 각각의 특정 필터링 처리에 대하여 다르다. 예컨대, 스팸-스코어는 이메일의 소스 IP 어드레스(예를 들어 스패머(spammer)로

알려진)에 의하여 또는 디렉토리 하베스트 공격과 같은 대용량 이-메일링 시도의 일부분인 것으로 결정되는 경우에 영향을 받을 수 있다. 따라서, 만일 입력 이-메일에 할당된 스팸-스코어가 사전에 설정된 전체 허용 한계 설정을 초과하지 않으면, 이-메일은 필터링되어 의도된 수신자에 도달되지 않는다. 기술된 바와 같이, 이러한 필터링에 대한 허용 한계 레벨은 "완화된 것"으로부터 "공격적인 것"까지의 범위 내에서 온-스크린 선택을 사용하여 조절될 수 있다. 예상될 수 있는 바와 같이, 이러한 전체 설정이 "공격" 측면 쪽으로 증가될 때, 더 많은 입력 이-메일 메시지들이 필터링될 것이다. 그러나, 필터링된 메시지들의 수가 허용 한계의 변화와 함께 증가될 때, 유효 및 적정 이-메일 메시지들이 스팸으로서 부적절하게 식별되어 필터링되는 스크리닝 처리에서의 "오인"에 대한 가능성이 존재한다. 따라서, 필터링 처리의 각각의 사용자는 개인의 전체 임계치를 조절할 수 있다.

[0030] 앞서 식별된 4개의 기본 임계치들이 또한 조절될 수 있다. 그러나, "대용량 이메일" 임계치가 전형적으로 소스 또는 목적지 IP 어드레스들에 기초하여 입력 메시지들에 대하여 적용되는 경우에, 나머지 4개의 기본 임계치들은 전형적으로 콘텐트-기반 필터링 처리들을 사용한다. 이러한 콘텐트-기반 필터링 처리들은 도 3에 관하여 기술된 애플리케이션 모듈들(332) 내에서 구현될 수 있다. 전술한 바와 같이, 사용자들은 필터링되어야 하는 원치 않는 이-메일을 수신하는 개인의 허용 한계 또는 대안적으로 의도된 수신자의 인박스에 전송되도록 해야 하는 이-메일이 부적절한 필터링에 따라 이들 4개의 기본 임계치들의 각각의 허용 한계를 개별적으로 조절할 수 있다. 게다가, 이들 기본 임계치들은 스크린 숏(400)에 기술된 바와 같이 각각의 특정 필터 임계치를 차단하는 옵션을 제공한다.

[0031] 도 5를 지금 참조하면, 도 3에 관하여 논의된 EMS의 블록도(300)에 대한 상세도가 예시된다. 전술한 바와 같이, EMS는 메일 서버들로부터 입력 SMTP 접속들을 셋업하고 모니터링하며 입력 SMTP 접속 시도들 및 이-메일 메시지들을 모니터링하는 역할을 하는 접속 관리자(322)를 포함한다. EMS는 이-메일 핸들러(326), MIME 디코더, 전송 관리자(324), 및 플러그-인 애플리케이션(332)을 포함하며, 플러그-인 애플리케이션들(332)은 애플리케이션 인터페이스(330)를 통해 이-메일 핸들러(326)와 통신한다.

[0032] 기술된 실시예에 있어서, 입력 전자 메시지는 접속 관리자(322)에 의하여 처음 수신된다. 접속 관리자(322)는 메시지의 전송자의 소스 IP 어드레스를 결정하기 위하여 이-메일 핸들러(326)와 관련하여 작용하도록 전형적으로 구성된다. 일단 전송자의 소스 IP 어드레스가 결정되면, 비즈니스 휴리스틱 기반 소스 IP 어드레스 모듈(332a)의 형태인 비즈니스 휴리스틱들 기반(이후 단순히 휴리스틱들) 모듈은 메시지를 처리할 때 도움이 된다. 휴리스틱들 소스 IP 모듈(332a)은 여러 소프트웨어 애플리케이션 플러그-인들 중 하나로서 EMS에 포함될 수 있다. 특히, 휴리스틱 소스 IP 모듈(332a)은 입력 메시지의 이전에 결정된 소스 IP 어드레스를 데이터베이스(334)에 저장된 것들과 비교하기 위하여 소스 IP 어드레스 데이터베이스(334)를 액세스하도록 구성된다. 물론, 휴리스틱들 소스 IP 모듈(332a)은 출력 메시지의 목적지 IP 어드레스를 데이터베이스(334)에 저장된 것들과 비교하기 위하여 또한 구성될 수 있다. 따라서, 본 명세서에서 사용된 바와 같이, "소스 IP 어드레스"는 EMS 시스템 내로의 메시지의 전송자의 목적지 IP 어드레스뿐만 아니라 메시지를 전송중인 EMS 시스템의 사용자의 IP 어드레스를 포함한다. 일단 비교되면, 만일 메시지의 소스 IP 어드레스가 미리 선택된 필드 또는 비즈니스 유형(예컨대, 법률 산업)과 관련되는 것으로 결정되면, 사용자(또는 메시지 필터링 시스템의 관리자)에 의하여 설정된 전체 메시지 필터링 임계치는 메시지가 원치 않는 스팸을 필터링하는 것보다 오히려 의도된 수신자에게 전송될 가능성을 증가시키도록 조절될 수 있다. 이러한 임계치 조절은 이하에서 더 상세히 설명된다.

[0033] 또한, 본 실시예에 있어서, 휴리스틱들 기반 콘텐트 모듈(332b)의 형태의 다른 비즈니스 휴리스틱들 모듈은 EMS와 연관된 다중 애플리케이션들(332) 중에 추가된다. 이하에서 더 상세히 논의된 바와 같이, 휴리스틱들 콘텐트 모듈(332b)은 미리 결정된 산업들과 관련된 콘텐트의 존재를 결정하기 위하여 입력(또는 출력) 전자 메시지들의 콘텐트를 분석하도록 구성된 소프트웨어로 이루어질 수 있다. 예컨대, 메시지가 EMS에 의하여 수신될 때, 휴리스틱들 콘텐트 모듈(332b)은 휴리스틱 콘텐트 모듈(332b)에 의하여 제공된 명령 코드에 기초하여 메시지 내의 콘텐트를 탐색/추출하기 위하여 이-메일 핸들러(326)와 작용한다. 메시지의 IP 어드레스에 기초한 휴리스틱들 필터링에서와 같이, 만일 미리 선택된 비즈니스와 관련된 콘텐트가 검출되면, 사용자(및/또는 관리자)에 의하여 설정된 전체 메시지 필터링 임계치는 필터링되는 것보다 오히려 의도된 수신자에게 메시지가 전송될 가능성을 증가시키도록 조절될 수 있다. 따라서, 휴리스틱들 IP 어드레스 모듈(332a) 및 휴리스틱 콘텐트 모듈(332b)은 메시지가 적정 비즈니스와 어떻게든지 해서 연관되는지의 여부를 결정하기 위하여 사용될 수 있다.

[0034] 본 명세서에서 사용되는 바와 같이, "비즈니스와 연관됨"은 소스 또는 목적지 IP 어드레스, 제목 라인, 메시지 텍스트, 또는 임의의 첨부물들을 포함하는 메시지의 임의의 부분이 비즈니스 또는 비즈니스 내의 일과 어떤 방식으로 관련되는지를 결정하는 것을 의미한다. 예컨대, 메시지에 대한 소스 또는 목적지 IP 어드레스는 회사

또는 그 회사 내의 알려진 기관 또는 비즈니스와 관련된 기관에 속하거나, 또는 메시지의 일부분은 전송자 또는 의도된 수신자가 실제로 비즈니스 라인에서 사용되거나 또는 지원되는 경우와 무관하게 회사들 또는 회사 내의 다른 알려진 기관들 또는 상기 비즈니스와 관련된 다른 기관들에 의하여 사용되는 콘텐트를 포함할 수 있다. 마찬가지로, 기술된 휴리스틱들 처리는 특정 비즈니스 또는 직업과 연관되지 않은 두 사람들 간의 메시지들에 적용할 수 있으나, 메시지는 비즈니스의 지정된 유형 또는 필드와 연관되는 것으로 결정된 콘텐트(또는 IP 어드레스)를 포함한다. "비즈니스와 연관된"과 관련한 다른 예는 비즈니스와 관련된 직업들의 전문가 연합들과 연관된 것으로 발견된 콘텐트를 포함한다. 예컨대, 금융회사에서 근무하는 법률가는 비록 그가 금융회사 또는 다른 비법률 회사에서 근무하고 엄격하게 법률업계에 근무하지 않을지라도 법률 기반 휴리스틱들 필터링을 사용하여 이로부터 이득을 얻을 수 있다.

[0035] 하나의 특정 실시예에 있어서, 전체 임계치로의 조절은 입력 메시지에서 검출된 비즈니스-기반 콘텐트량 뿐만 아니라 의도된 수신자, 관리자 또는 이들 둘 다에 의하여 이루어진 휴리스틱들 콘텐트 모듈(332b)에 대한 임계치 설정에 기초하여 변화할 수 있다. 물론, 휴리스틱 콘텐트 모듈(332b) 및 휴리스틱들 소스 IP 모듈(332a)은 도 5에 기술된 정확한 실시예들 및 접속들에 제한되지 않는다. 마찬가지로, 당업자는 여기에 기술된 휴리스틱들에 기초하여 필터링하는 원리들의 범위에서 벗어나지 않고 상기 구성요소들 및/또는 다른 구성요소들에의 대응 접속들에서 이루어질 수 있는 변형들을 이해할 것이다. 모듈(332a, 332b)에 기초하여 이루어지는 조절들은 이하에서 더 상세히 논의된다.

[0036] 도 6을 지금 참조하면, 기술된 휴리스틱들 원리들에 따라 비즈니스-특정 임계치들을 설정하는 스크린 숏(600)의 일 실시예가 예시되어 있다. 특히, 두개의 비즈니스-기반 임계치들, 즉 "법률" 및 "금융"의 조절이 기술된다. 물론, 임의의 수 및/또는 임의의 유형의 비즈니스 임계치들이 제공되어 기술된 필터링 처리와 함께 사용될 수 있다. 또한, 전술한 바와 같이, 일단 임의의 조절들이 이루어지면, "변화들을 저장" 버튼 또는 스크린을 클릭함으로써 저장될 수 있거나 또는 기술된 "삭제" 버튼을 클릭함으로써 삭제될 수 있다.

[0037] 비즈니스-기반 임계치들은 그들이 의도된 수신자에게 전송되도록 이전 기본 임계치들의 설정들을 이-메일 메시지들이 만족하는지의 여부를 좌우하기 위하여 제공된다. 특히, 비즈니스 임계치들은 일반적으로 필터링되어 이-메일 메시지들이 비즈니스 휴리스틱들에 기초하여 의도된 수신자에게 전송되도록 한다. 이-메일 필터링에 있어서 이러한 휴리스틱들 접근에 대한 목적은 보편화된 스팸-필터링 기술을 사용할 때 문제점일 수 있는 오인의 문제점을 제거하는 것이다. 마찬가지로, 이-메일 메시지들이 기본 임계치들의 설정들에 기초하여 필터링되는 가능성은 비즈니스 임계치들의 설정들에 기초하여 감소될 수 있다. 더욱이, 바람직한 실시예들에 있어서, 비즈니스 임계치 조절들을 허용하는 스크린 숏(600)은 이-메일 필터링 서비스의 관리자들에게만 이용 가능하다. 이러한 실시예들에 있어서, 사용자 인터페이스는 사용자가 메시지들의 휴리스틱 필터링을 단순히 턴온 또는 턴오프하도록 하는 메시지들의 의도된 수신자들에게 제공될 수 있다. 물론, 다른 실시예들에 있어서, 입력 메시지들의 의도된 수신자들은 임계치 조절 바들에 액세스하도록 제공된다.

[0038] 도 6에는 비즈니스 임계치들의 허용 한계에 대한 변화성이 기술되어 있다. 기술된 실시예에 있어서, 허용 한계 조절이 "비-엑스트라 임포턴스"로부터 "엑스트라 임포턴스"로 이동할 때, 필터링된 이-메일 메시지가 의도된 수신자에게 전송될 가능성은 증가한다. 물론, 임계치 설정들의 가변 범위에 대한 다른 타이틀들이 사용될 수 있다. 이러한 임계치 설정들을 조절함으로써, "유효 임계치"는 비즈니스 임계치들의 설정들에 의하여 수정되는 것처럼 원래의 기본 임계치들의 설정들에 기초하여 생성된다. 수식(1)은 이와 같은 관계의 예를 기술한다.

[0039] $$TH_{eff} = TH_{base} \bullet TH_{ind} \quad (1)$$

[0040] 여기서, TH_{eff}는 누적 기본 임계치인 TH_{base}와 비즈니스 임계치인 TH_{ind}를 곱함으로써 계산된 유효 임계치 결과이다. 다른 방식으로 언급하면, 원래의 전체 임계치가 기본 임계치들 중 하나를 설정하는 것을 사용하여 조절되기 때문에, 결과치는 기본 임계치 TH_{base}이다. 그 다음에, 이의 설정(들)에 기초한 비즈니스 임계치 TH_{ind}는 기본 임계치 TH_{base}를 조절하여 임의의 비즈니스 기반 상황들에 더 완화되도록 하며 그 결과 이전에 필터링된 메시지를 의도된 수신자에게 허용할 가능성이 증가된다. 일부 실시예들에 있어서, 비즈니스 임계치 TH_{ind}는 의도된 수신자에게 도달하는 것을 차단된 입력 메시지의 패시지(passage)를 가상적으로 결정한 극단적 설정으로 조절될 수 있다. 유효 임계치의 결정은 이하에서 더 상세히 논의된다.

[0041] 도 7을 지금 참조하면, 도 4의 스크린 숏(400) 및 도 6의 스크린 숏(600)을 참조하여 기술된 비즈니스 휴리스틱들 기반 필터링 기술에 대한 전형적인 프로세스의 흐름도가 예시되어 있다. 기술된 접근의 기능을 더 명확하게

이해하기 위하여, 도 7의 전형적인 프로세스는 특정 예와 관련하여 기술될 것이다. 그러나, 이러한 설명은 다양한 임계치들에 대한 값들 및 스코어들을 할당하는 기술을 포함하지만 이에 제한되지 않으며, 여기에 기술된 원리들의 구현을 제한하는 것으로 해석되지 않아야 한다. 도 7의 프로세스는 기술된 이-메일 필터링 처리가 초기화되는 시작 블록(710)에서 시작된다.

[0042] 블록(720)에서, 입력 전자 메시지(즉, 이-메일)는 필터링 처리에 의하여 인터셉트된다. 필터링 처리(예컨대, 전형적으로 소프트웨어로 구현됨)는 이-메일의 의도된 수신자로부터 지리적으로 떨어진 위치에서 이루어질 수 있거나 또는 수신자의 온-사이트 이-메일 서버 내에 위치할 수 있다. 블록(730)에서, 스팸-스코어는 앞서 언급된 바와 같이 입력 이-메일 메시지에 할당된다. 이-메일에 주어진 스팸-스코어는 전형적으로 여러 다른 기준에 기초하며 메시지가 스팸이 아닐 가능성을 지시하기 위하여 사용된다. 예컨대, 전송자의 소스 IP 어드레스 및/또는 도메인뿐만 아니라 목적지 IP 어드레스들의 도메인 및 이-메일의 제목 라인 및/또는 본문이 고려될 수 있다. 또한, 메시지가 대용량 메일링의 일부분이고 메시지가 디렉토리 하베스트 공격의 일부분이며 메시지의 전송자가 이전 스팸 메일링들과 링크되는지의 여부와 같이 메시지와 연관된 특징들이 고려될 수 있다. 프로세스의 이러한 부분에 대한 상세한 논의는 앞서 상호-참조된 공동 계류중인 특허 출원에 개시되어 있다. 이러한 특정 예에 있어서, 스팸-스코어는 0 또는 100의 범위를 가지며, 여기서 0은 이-메일이 스팸인 확실성을 지시하는 반면에 100의 스코어는 이-메일이 스팸이 아닌 확실성을 지시한다. 더욱이, 통과하는 각각의 메시지에 할당된 스팸-스코어는 전형적으로 필터링 처리를 통해 변화되지 않으며, 스팸-스코어가 임계치 이하로 떨어지는지를 결정하기 위하여 다양한 임계치들과 비교되며 이에 따라 의도된 수신자에서의 전송시 필터링되어야 한다. 물론, 다른 실시예들은 단독으로 또는 임계치의 조절을 수행하여 스팸-스코어를 조절할 수 있다.

[0043] 프로세스의 다른 측면에서 볼 때, 블록(740)에서, 기본 임계치들과 연관된 특정 카테고리가 결정된다. 도 4를 다시 참조하면, 이메일의 제목 라인 및/또는 본문(또는 임의의 연관된 부분)은 이메일이 콘텐트 구동 기본 임계치들(성적으로 노골적인, 일확천금, 특별 제공, 또는 인종 차별적)중 하나에 속하는 표시자(indicator)들을 찾기 위하여 스캐닝 될 수 있다. 이메일이 필터링될지의 여부를 할당된 스팸-스코어가 일반적으로 결정하기 위하여 사용되는 경우, 열거된 카테고리들 중 하나의 멤버십은 이메일이 필터링될 가능성을 증가시킨다. 특정 실시예에 있어서, 이들 4개의 카테고리들에 대한 각각의 가변하는 설정들은 스팸-스코어가 새로운(조절된) 임계치를 뛰어넘지 않을 기회를 증가시키기 위하여 사용된 승수(multiplier)를 나타낼 수 있고, 그러므로 메시지는 필터링된다. 예를 들어, 만약 사용자가 40의 본래 전체 임계치를 가지며, 입력 이메일이 성적으로 노골적인 자료를 포함하지만 불쾌한(offending) 카테고리에서 멤버십을 검출하지 않고 50의 스팸-스코어에만 할당되면, 이메일은 스팸-스코어가 임계치를 초과하기 때문에 사용자에게 전달될 것이다. 그러나, 만약 이메일이 속하는 카테고리에 대한 사용자의 설정이 높으면, 예를 들어 10 승수이면, 이러한 설정은 만약 이메일이 불쾌한 콘텐트를 포함하도록 결정되면, 사용자의 본래 전체 허용 한계가 승수에 의해 증가하게 할 것이다. 따라서, 스팸-스코어가 전체 임계치 이상에 속하는 경우, 이런 특정 이메일에 대한 동일한 스팸-스코어는 새롭게 조절된 임계치보다 작다. 그러므로, 이메일은 전달시 필터링될 것이다.

[0044] 사실상, 상기된 바와 같은 승수들을 생성하는 콘텐트 구동 기본 임계치들에 대한 설정들은 이메일들이 콘텐트 기반(즉, 불쾌한) 카테고리들에 속하는 것으로 결정될 때, 이메일들의 잘못된 필터링 가능성에 대한 사용자의 허용 한계를 가리킨다. 특히, 상기된 실시예에 있어서, 사용자는 만약 이메일의 콘텐트가 성적으로 노골적인 자료를 포함하는 것으로 결정되면 잘못된 가능성(10의 예시적인 승수)의 10배를 허용하는 것을 필수적으로 정한다. 이 때문에, 비록 이메일이 스팸이 아닌 실제상의 확실성(virtual certainty)을 가리키는 높은 스팸-스코어를 수신할지라도, 이메일은 각각의 카테고리에 대한 사용자에 의해 설정된 높은 레벨에 의해 영향을 받기 때문에, 불쾌한 카테고리(즉, 불쾌한 콘텐트)의 멤버십에 기초하여 여전히 필터링될 수 있다.

[0045] 블록(750)으로 이동하여, 메시지의 소스 IP 어드레스가 상기된 바와 같이 소프트웨어 플러그 인들을 사용함으로써 미해결의 임의의 특정 산업들과 연관되는지가 결정된다. 상기 "승인된 전송자들"의 리스트는 이들 전송자들로부터의 메시지들이 "승인된" 소스 IP 어드레스와의 연관성을 기초로 하여 사용자의 인박스에 보다 잘 전달될 수 있도록 잠재적 메시지 전송자들의 특정 소스 IP 어드레스들의 리스트를 포함한다. 예를 들어, 데이터베이스는 미국의 모든 법률 회사들에 대한 실질적으로 모든 공지된 IP 어드레스들을 포함하도록 유지될 수 있다. 따라서, 이런 데이터베이스는 입력 메시지에 대한 소스 IP 어드레스가 이 데이터베이스의 어드레스에 해당하는지 여부를 결정하기 위하여 검색될 수 있다. 만약 소스 IP 어드레스가 데이터베이스 내에 존재하는 것으로 결정되면, 사용자의 임계치들은 블록(740)과 관련해 상기된 바와 유사한 방식으로 이런 기준상에서 조절될 것이다. 유사한 실시예들은 은행 또는 심지어 금융 비즈니스와 연관되지 않은 전송자 및 수신자 사이 같은 금융 비즈니스와 연관된 소스 IP 어드레스들에 구상되지만, 메시지의 콘텐트는 금융 비즈니스(예를 들어, 전문 용어 또는

기타 등등)와 연관되는 것으로 여전히 발견된다.

[0046] 소스 IP 어드레스들의 데이터베이스는 전형적으로 생성되고 여기에 개시된 바와 같은 메시지 필터링을 관리하는 관리 조직에 의해 유지되고, 여기서 리스트는 전형적으로 사용자들 및 경쟁자로부터 숨겨지게 유지된다. 그러나, 여기에 개시된 필터링 시스템들 및 처리들은 메시지의 의도된 수신자가 리스트를 편집하거나 심지어 전체적으로 생성하는 실시예들을 포함하기에 충분히 넓다. 부가적으로, 상기 리스트를 사용하는 동안 필터링에 대한 임계치들은 관리자 또는 사용자의 조절시 변할 수 있다. 물론, 상기 임계치들은 만약 전송자의 IP 어드레스가 데이터베이스 리스트 상에 포함되는 것으로 발견되면 입력 메시지가 항상 전달되는 레벨들로 조절될 수 있다.

[0047] 게다가, 사용자의 전체 임계치에 대한 이런 조절은 전형적인 필터링 기술들에서 발견된 바와 같은 도메인 이름이 아닌 IP 어드레스들을 바탕으로 하여 이루어진다. 특히, 도메인 이름-기반 접근들은 전형적으로 "승인된 전송자들"의 리스트를 포함하고, 메시지 전송자에 대한 도메인 이름이 리스트의 도메인과 매칭할 때, 메시지는 의도된 수신자에 전송되도록 허용된다. 그러나, 상기 접근들은 메시지들을 전송하기 위한 "스푸핑" 기술들을 사용하는 원하지 않는 메시지들의 전송자들에 대해 효과적이지 않다. 이런 상황들에서, 원하지 않는 메시지는 메시지들을 전송하기 위하여 "승인된" 도메인 이름을 여전히 포함한다. 대신, 개시된 기술은 전송된 메시지가 필터링되어야 하는지 여부의 결정을 돕기 위하여 메시지 전송자들의 소스 IP 어드레스(통상적으로 구간들에 의해 분리된 4개의 다중 디지트 번호들)를 사용한다. 이러한 접근의 일 실시예는 데이터베이스에 저장된 공지된 유효 전송자들의 IP 어드레스들과 소스 IP 어드레스의 매칭을 포함하지만, 개시된 기술은 여기에 제한되지 않는다.

[0048] 일부 실시예들에 있어서, 데이터베이스에서 하나 이상의 단순한 소스 IP 어드레스 "룩업"이 발생한다. 이러한 실시예에 있어서, 양쪽이 동일한 비즈니스의 멤버들인지를 결정하기 위하여 의도된 수신자의 어드레스와 전송 IP 어드레스의 비교 같은 다른 인자들이 고려될 수 있다. 만약 메시지가 스팸인 가능성이 보다 작다고 결정되면, 따라서 수신자의 전체 임계치는 이런 가능성을 반영하도록 조절(예를 들어, 낮추어짐)될 수 있다. 이들 및 다른 실시예들에 있어서, 메시지가 통과되도록 허용될 가능성을 증가시키도록 사용자의 전체 임계치가 조절되어야 하는지 여부를 결정하기 위해 이러한 비즈니스 기반 관점들을 사용하여 소스 IP 어드레스와의 다양한 비교들이 이루어질 수 있다. 예를 들어, 다른 결정들은 유효 메시지 전송자들보다 오히려 스팸 전송자들과 전형적으로 연관된 트래픽/시도들의 패턴들이 있는지 여부를 결정하기 위하여 전송 IP 어드레스(임의의 목적지 IP 어드레스들의 고려 하에 또는 고려없이)에 의한 예전 메시지 트래픽 또는 접속 시도들을 관찰하는 것을 포함할 수 있다. 다른 실시예들은 비즈니스 내에서 소스 IP 어드레스 및 다른 의도된 수신자들 간의 이전 메시지 트래픽을 비교하는 것, 또는 소스 IP 어드레스가 외부 검증 처리들을 통하여 특정 비즈니스에 관련된 것으로 할당되는 경우를 포함한다. 물론, 여기에 개시된 시스템 및 처리는 본 상세한 설명 및 상기 상세한 설명으로부터의 임의의 청구항들의 범위 내에 속하면서 임의의 상기 접근들을 포함할 수 있다.

[0049] 다음, 블록(760)에서, 이메일 메시지의 콘텐트가 특정 미리 결정된 산업들과 연관되는지 여부가 결정된다. 특히, 이 결정은 미리 선택된 산업들 중 하나에 대응하는 이메일에서 비즈니스 콘텐트가 있는지 여부에 기초하여 임계치 조절을 고려하여 이루어진다. 플러그 인 애플리케이션들(도 3 참조)은 전형적으로 상기 산업들과 연관된 키 용어들 또는 어구들을 찾는 이메일의 콘텐트를 분석하기 위하여 사용될 수 있다. 예를 들어, 만약 "난해한 법률 용어"의 몇몇 예들이 이메일의 콘텐트에서 검출되어 이메일이 법률 비즈니스와 충분히 연관된 것이 결정되면, 사용자의 임계치는 개시된 필터링 처리를 달성하기 위하여 메시지의 할당된 스팸-스코어와 비교를 위하여 조절될 수 있다. 결과적으로, 만약 충분한 비즈니스 콘텐트가 메시지에서 검출되면, 특정 임계치와 연관된 승수는 발견된 비즈니스 콘텐트가 없는 스팸-스코어(또는 다른 이유들)를 기초로 하여 메시지가 필터링될지라도, 의도된 수신자에 전달되도록 충분히 낮게 설정될 수 있다. 소스 IP 어드레스들에서, 데이터베이스는 비즈니스 콘텐트 결정을 달성하기 위하여 비즈니스와 연관된 키 용어들 및 어구들을 저장하기 위해 사용될 수 있고, 개시된 기술은 의도된 수신자가 작동하는 산업들로 제한되지 않는다. 게다가, 여기에 개시된 원리들에 따라 수행되는 처리는 임의의 순서로 블록들(750 및 760)을 포함할 수 있거나, 심지어 이 개시물의 범위에서 벗어나지 않고 동시에 수행될 수 있다.

[0050] 만약 비즈니스 관계가 이메일 콘텐트에서 발견되지 않으면, 처리는 블록(780)으로 이동한다. 이 블록에서, 이메일의 필터링은 현재 전체 임계치에 대해 할당된 스팸-스코어의 비교를 기초로 하여 수행된다. 만약 블록(740)에서 이메일의 콘텐트가 임의의 불쾌한 카테고리들 내의 멤버십으로 보장되지 않는 것이 결정되면, 필터링은 본래 전체 임계치를 사용하여 수행된다. 이 때문에, 만약 스팸-스코어가 본래 임계치를 초과하지 않으면, 의도된 수신자 쪽으로 이메일의 전송은 차단된다. 그러나, 만약 불쾌한 카테고리들 중 하나의 멤버십이 결정되면, 필터링은 할당된 스팸-스코어 및 조절된 전체 임계치들 사이의 비교를 바탕으로 이루어진다. 특히, 상기된

바와 같이, 카테고리 멤버십은 전체 임계치가 증가되게 하여(사용자 또는 시스템 관리자에 의해 설정된 설정에 따라), 이메일이 사용자에게 도달하도록 허용할 가능성을 감소시킨다. 따라서, 만약 스팸-스코어가 조절된 전체 임계치를 초과하지 않으면, 의도된 수신자 쪽으로 이메일의 전송은 차단된다. 반대로, 어느 경우에서나, 만약 스팸-스코어가 본래 또는 조절된 전체 임계치들을 초과하여야 한다면, 이메일은 사용자에게 전달될 것이다.

[0051] 만약 블록(760)에서 임의의 선택된 산업들과 관련성이 있다면, 비즈니스-관련 소스 IP 어드레스(블록 750) 및/또는 비즈니스 관련 콘텐트 결정을 기초로 하여, 처리는 대신에 블록(790)으로 이동한다. 이 블록에서, 이메일은 블록들(750 및 760)에 따라 조절된 바와 같이 유효 임계치 값들에 대한 할당된 스팸-스코어의 비교를 기초로 하여 필터링된다. 유효 임계치는 상기된 바와 같이 결정되고, 여기서 전체적인 임계치는 전형적으로 사용자 및/또는 시스템 관리자에 의해 설정된 설정들에 따라 감소된다. 기본 임계치들과 같이, 비즈니스 임계치들은 본래 전체 임계치의 승수들을 포함한다. 그러나, 기본 임계치들이 1 보다 큰 승수이면(이 실시예에서 전체 임계치를 증가시키고 메시지를 필터링하는 기회를 증가시키기 위해), 비즈니스 임계치들에 대한 승수는 모두 1 보다 작을 수 있다. 따라서, 이러한 실시예들에 있어서, 전체 임계치를 분수 승수와 곱셈하는 것은 전체 임계치를 감소시키고, 이것은 메시지가 필터링 처리를 통하여 허용되고 의도된 수신자에 전송될 기회를 증가시킨다.

[0052] 통과 가능성의 증가는 본래 전체 임계치 또는 조절된 전체 임계치가 사용되는지 여부와 무관하다. 개시된 접근의 이런 장점은 이메일이 불쾌한 카테고리들 중 하나로 분류되지만, 실제로 의도된 수신자가 가지고자 하는 중요하고 목표된 이메일일 때 특히 바람직하다. 특정 실시예에 있어서, 여기에서 다수의 인종 비방들을 포함하는 것으로 결정된 이메일은 "인종 차별적" 기본 임계치 아래로 분류될 것이다. 게다가, 수신자는 이 실시예에서 기본 임계치가 최대치로 설정되기 때문에, 이메일이 의도된 수신자에 도달할 기회가 작아진다.

[0053] 그러나, 만약 이메일이 실제로 인종 비방의 이용을 기초로 하여 소송에 속하는 법률 서류들을 포함하면, 이메일은 부적당하게 필터링된다. 상기 잘못된 가능성을 방지하기 위하여, 개시된 접근은 만약, 예를 들어, 법률 산업과 연관되면 이메일(또는 아마도 소스 IP 어드레스)의 콘텐트를 기초로 하여 임계치가 조절되게 한다. 필수적으로, 비즈니스 임계치 승수들의 사용은 만약 비즈니스 임계치들에서 선택된 산업들에 대한 연관이 존재하는 것으로 결정되면 잘못될 가능성이 덜 허용되도록 필수적으로 사용자가 지정하게 한다. 따라서, 만약 이메일이 상기 법률 콘텐트를 포함하면, 전체 임계치는 전형적으로 "법률" 비즈니스 임계치에서 설정된 설정에 해당하는 승수에 의해 이 실시예에서 감소될 것이다. 결과적으로, 이메일이 수신자에 도달할 가능성은 증가된다. 부가적으로, 승수 양(전체 임계치에 대한 조절 양)은 일 실시예에서, 각각의 비즈니스에 대한 개별 임계치들에 대한 설정들의 조절에 의해 의도된 수신자에 의해 설정될 수 있다.

[0054] 유사한 결과는 만약 소스 IP 어드레스 또는 도메인이 법률 산업과 연관되어 발견되면 얻어질 수 있다. 예를 들어, 유명한 법률 회사에 의해 사용된 도메인이 이메일에 포함된 소스(또는 목적지) IP 어드레스에서 식별되는 것이 가정된다. 이 실시예에서, 이메일이 인종 비방을 포함할 수 있지만, 유명한 법률 회사(소스 도메인이 이메일에서 식별되고 승인된 전송자들의 데이터베이스에 매칭됨)가 스팸으로서 인종 차별적 이메일을 전송(또는 전송함)할 가능성은 매우 미미하다. 바람직하지 않게, 콘텐트에 기초한 "인종 차별적인" 같은 이메일의 분류는 필터링 처리를 통하여 이메일이 통과될 가능성을 크게 감소시킨다. 그러나, 개시된 기술을 사용함으로써, 비록 카테고리 멤버십으로 인해 조절될지라도 전체 임계치는 보다 완화된 유효 임계치를 생성하기 위하여 결정된 비즈니스 관련성을 기초로 하여 감소되고, 따라서 이런 특정 이메일이 의도된 수신자에 도달할 기회를 증가시킨다. 물론, 몇몇 실시예들에 있어서, 상기 처리는 비록 승인이 개시된 원리들에 따라 미리 결정된 비즈니스와 관련성을 기초로 하지만, 만약 메시지의 소스 IP 어드레스가 미리 결정된 산업들 중 하나와 연관되도록 결정되면, 의도된 수신자에 입력 메시지를 명확하게 전송하도록 구성될 수 있다.

[0055] 여기에 개시된 비즈니스 휴리스틱들 기본 원리들에 따라 전자 메시지들을 필터링하는 시스템 및 방법들의 다양한 실시예들이 개시되었지만, 이들은 예시적으로 제공되고, 이에 제한되는 것이 아니라는 것이 이해되어야 한다. 따라서, 본 발명(들)의 넓이 및 범위는 상기된 예시적인 실시예들 중 임의의 것으로 제한되는 것이 아니고, 다음 청구항들 및 그 등가물들에 따라 정의되어야 한다. 게다가, 상기 장점들 및 특징들은 기술된 실시예들에서 실행되지만, 임의의 또는 모든 상기 장점들을 달성하는 처리들 및 구조들에 대한 청구항들의 애플리케이션을 제한하지 않는다.

[0056] 부가적으로, 여기의 서두 단락은 37 CFR 1.77하에서의 제안들과 일관성 및 구조적 단서들을 제공하기 위하여 제공된다. 이들 서두들은 이 개시물로부터 발생할 수 있는 임의의 청구항들을 나타내는 본 발명을 제한 또는 특정하지 않는다. 특히, 예로서, 비록 서두가 "기술적 분야"를 참조하지만, 청구항들은 소위 기술 분야를 기술하기 위한 서두에서 선택된 언어로 제한되지 않는다. 게다가, "배경" 기술의 설명은 기술이 본 개시물의 임의의

발명에 대한 종래 기술인 것을 시인하는 것으로서 해석되지 않는다. "요약서"는 본 명세서에서 발견되는 청구항들에 나타나는 본 발명의 특성으로 고려되지 않는다. 게다가, 하나의 "발명"에 대한 본 개시물의 임의의 참조는 본 개시물에 하나의 신규성만이 청구되었다는 것을 주장하기 위하여 사용되어서는 안된다. 다수의 발명들은 본 개시물과 연관된 다수의 청구항들의 제한들에 따라 나타나고, 이에 따라 청구항들은 본 발명, 및 등가물들을 정의하고, 이에 따라 보호된다. 모든 예들에서, 청구항들의 범위는 명세서로 미루어 보아 이들 자신의 장점으로 고려되지만, 본원에 나타난 서두에 의해 제한되어서는 안된다.

도면의 간단한 설명

[0008] 도 1은 인터넷 또는 다른 컴퓨터 네트워크를 통해 이-메일 메시지들을 전송하는 종래 기술의 시스템에 대한 일 실시예를 예시한 도면.

[0009] 도 2는 액티브 전자 메시지 관리 시스템이 인터넷 및 수신 메일 서버 간에 제공되는 실시예에 대한 블록도를 예시한 도면.

[0010] 도 3은 도 2에 도시된 EMS의 블록도를 포함하는 상세 블록도를 예시한 도면.

[0011] 도 4는 원치 않는 이-메일 메시지들을 필터링하는 다중 임계치들을 설정하는 스크린 숏(screen shot)의 일 실시예를 예시한 도면.

[0012] 도 5는 도 3과 관련하여 기술된 EMS의 블록도에 대한 상세도를 예시한 도면.

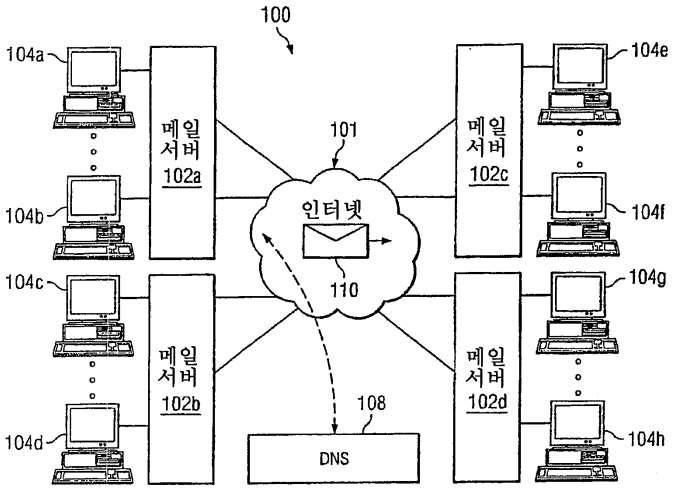
[0013] 도 6은 기술된 원리들에 따라 앞서 기술된 기본 임계치 외에 비즈니스-특정 임계치들을 설정하는 스크린 숏의 일 실시예를 예시한 도면.

[0014] 도 7은 기술된 비즈니스 휴리스틱-기반 필터링 기술에 대한 전형적인 프로세스의 흐름도를 예시한 도면.

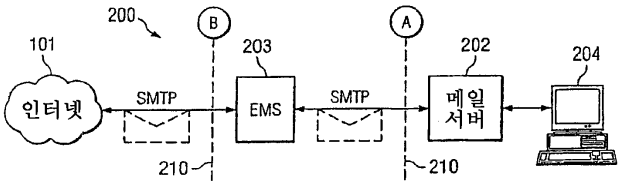
도면

도면1

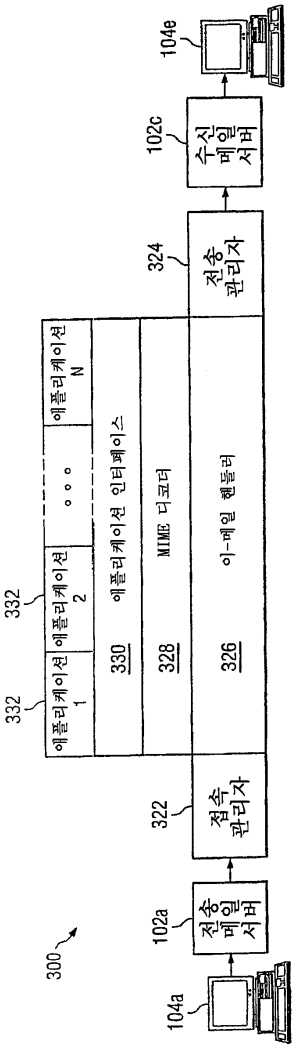
종래 기술



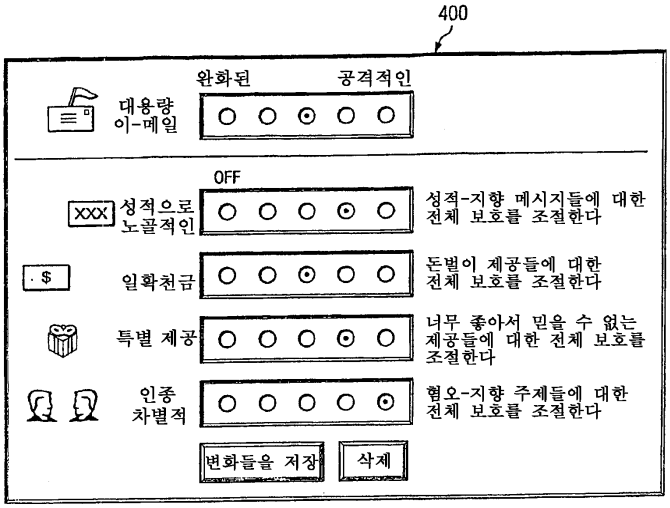
도면2


200
B
A
101
203
202
204
인터넷
SMTP
EMS
SMTP
메일 서버
210
210

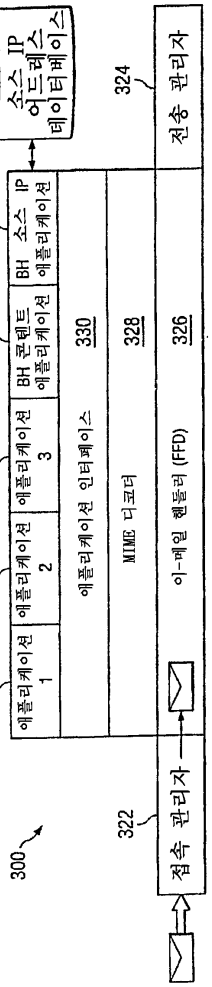
도면3


104e
102c
수신 메일 서버
324
전송 관리자
332
332
애플리케이션 1
애플리케이션 2
ㅇㅇㅇ
애플리케이션 N
330
애플리케이션 인터페이스
328
MIME 디코더
326
이-메일 핸들러
322
접속 관리자
300
102a
전송 메일 서버
104a

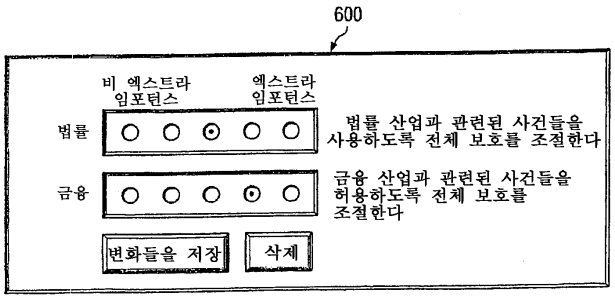
도면4


400
완화된
공격적인
대용량 이-메일
OFF
성적으로 노골적인
성적-지향 메시지들에 대한 전체 보호를 조절한다
일확천금
돈벌이 제공들에 대한 전체 보호를 조절한다
특별 제공
너무 좋아서 믿을 수 없는 제공들에 대한 전체 보호를 조절한다
인종 차별적
혐오-지향 주제들에 대한 전체 보호를 조절한다
변화들을 저장
삭제

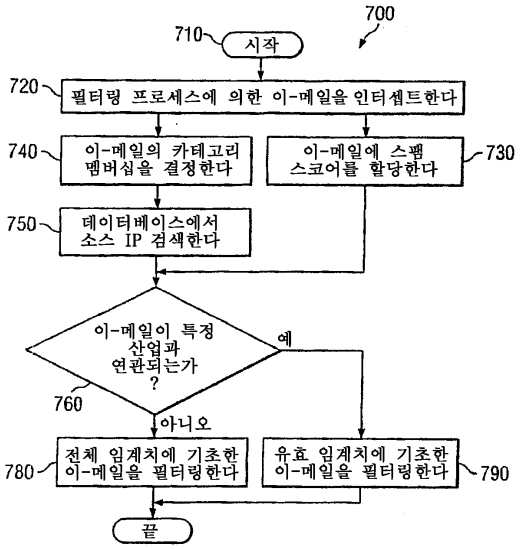
도면5


300
322
접속 관리자
이-메일 핸들러 (FFD)
326
MIME 디코더
328
에플리케이션 인터페이스
330
332
에플리케이션 1
332
에플리케이션 2
332
에플리케이션 3
332b
BH 콘텐트 에플리케이션
332a
BH 소스 IP 에플리케이션
334
소스 IP 어드레스 데이터베이스
324
전송 관리자

도면6


600
비 엑스트라 임포턴스
엑스트라 임포턴스
법률
법률 산업과 관련된 사건들을 사용하도록 전체 보호를 조절한다
금융
금융 산업과 관련된 사건들을 허용하도록 전체 보호를 조절한다
변화들을 저장
삭제

도면7


700
710
시작
720
필터링 프로세스에 의한 이-메일을 인터셉트한다
740
이-메일의 카테고리 멤버십을 결정한다
이-메일에 스팸 스코어를 할당한다
730
750
데이터베이스에서 소스 IP 검색한다
이-메일이 특정 산업과 연관되는가 ?
760
예
아니오
780
전체 임계치에 기초한 이-메일을 필터링한다
유효 임계치에 기초한 이-메일을 필터링한다
790
끝