

(19)대한민국특허청(KR) (12) 공개특허공보(A)

(51) 。 Int. Cl.⁷
G06F 17/60D0

(11) 공개번호
(43) 공개일자

10-2004-0092707
2004년11월04일

(21) 출원번호 10-2003-0026257
(22) 출원일자 2003년04월25일

(71) 출원인 주식회사 컴트루테크놀로지
서울특별시 서대문구 홍은동48-84 서대문구 신지식산업센타3층

(72) 발명자 진봉준
서울특별시서초구양재2동402-4윤남빌딩4층

심사청구 : 있음

(54) 온라인스팸차단필터와 IMAP서버 방식을 활용한 스팸메일 차단시스템

요약

본 발명은 특정MUA에서 스팸메일을 차단하기 위하여 인터넷등의 원격서버에서 MUA(Mail User Agency)로 온라인 스팸차단필터를 제공하는 시스템과 IMAP서버 /POP3서버를 이용하여 스팸메일과 정상메일로 구분하여 저장하는 방법과 저장된 스팸메일의 관리기능(개인스팸필터의 추가, 스팸메일의 보기, 삭제 등)의 제공을 통해서 스팸메일을 차단할 수 있는 시스템을 제공한다. 이와 같은 스팸메일방지시스템은 청소년들이 유해성인메일로부터 차단할 수 있도록 접근권한을 설정하는 방법을 제공한다.

대표도

도 1

색인어

스팸메일, spam mail, 성인메일, 온라인스팸차단필터, IMAP

명세서

도면의 간단한 설명

도 1은 메일수신과정 개념을 도시하는 블록 선도.

도 2는 스팸메일 차단시스템의 구성을 도시하는 블록 선도.

도 3은 원격서버의 구성 및 작동방식을 도시하는 블록 선도.

도 4는 온라인스팸차단필터의 구성을 도시하는 블록 선도.

도 5는 MUA에서 수행되는 스팸메일 분류방법을 도시하는 블록 선도.

도 6은 스팸메일 차단방식의 일례를 도시하는 플로우차트.

도 7은 스팸메일 차단방식의 다른 예를 도시하는 플로우차트

도 8은 스팸메일함에 대한 접근권한 설정을 설명하기 위한 블록 선도.

<도면의 주요부분에 대한 부호의 설명>

100 : 스팸메일 차단시스템

200 : 메일서버

300 : 인터넷망(네트워크)

400 : 원격서버

500 : 온라인스팸차단필터

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 온라인스팸차단필터와 IMAP 서버 방식을 활용한 스팸메일 차단시스템에 관한 것으로, 특히 기존의 클라이언트/서버 시스템 환경하에서 스팸메일의 정보를 분석한 온라인스팸차단필터를 개인PC의 MUA(Mail User Agency)에 전달함으로써 개인 사용자들이 별도의 설정없이도 주어진 온라인스팸차단필터만으로 스팸메일을 차단할 수 있는, 온라인스팸차단필터와 IMAP 서버 방식을 활용한 스팸메일 차단시스템에 관한 것이다.

현재 인터넷의 발달로 인해 이메일은 인터넷 이용자들의 보편적인 의사소통 수단이 되었다. 그러나 이메일 자체가 상업적인 목적으로 이용되면서 스팸메일, 정크메일(Junk mail) 등이 인터넷 환경을 오염시키고 있다. 수신자가 원하지 않음에도 불구하고 무작위로 추출된 메일주소로 전달되는 스팸메일로 인해 메일 수신자들은 일방적으로 시간적, 정신적, 경제적 손실비용을 지불하고 있다.

스팸메일 필터링을 위하여 메일서버의 SmtP(Simple Mail transfer Protocol)단에서 메일의 헤더부분을 파싱(parsing)하여 스팸메일을 필터링 해주는 기술이 사용되고 있다. 이는 서버기반의 메시지 필터링 기술이라고 불리며 현재 sendmail, qmail등의 상업적, 비상업적 메일서버에서 이용되고 있다. 그러나 대용량의 메일을 관리할 시 수신되는 메일마다 이러한 헤더 정보를 분석하여 스팸메일을 분석하는 작업은 부하와 시간이 많이 걸리는 작업이기 때문에 선별적으로만 사용되고 있다.

MTA(Mail Transfer Agent)는 정크메일(Junk mail) 혹은 스팸메일을 제한하기 위해서 헤더정보를 사용한다. 외국의 경우 알려진 스팸머(Spammer)의 주소목록을 제공하는 상용서비스와 무료서비스가 제공되고 있다. 따라서 특정 MTA에서는 자신의 메일서버를 통하여 전달요청된 메일에 대하여 스팸머목록(Black List and White List)을 적용하여 메시지 전달을 거부할 수 있다. MTA운영자는 임의의 지역으로부터 온 메시지를 중계하는 기능을 제한하고 있으며 일반적으로 메시지가 자신의 MTA자신의 도메인으로 부터 온 것일 경우에만 중계될 수 있도록 하고 있다. Sendmail과 일부MTA는 그러한 스팸방지 기능을 제공한다. MTA가 다른 MTA나 다른 사용자에게 전달하기 위해서는 MDA(Mail Delivery Agent)로 전달하며 MDA는 MTA로부터 메시지를 받고 그것을 로컬파일시스템에 있는 수신자의 우편함에 기록한다. 이 때 MDA는 자체적으로 스팸필터링을 수행하거나 필터링 기능을 수행할 외부프로그램을 호출해서 메일을 필터링한다. 메일 송부시에는 MUA(Mail User Agency)는 인터넷의 smtp를 사용해서 MTA로 메일을 보내는데 바이너리 첨부화일이 있는 경우는 MIME과 형태의 표준을 사용하여 전달한다.

상기와 같은 헤더정보를 파싱하는 방식 이외에 일반적으로 메일서버에서 사용되는 방식은 IP blocking기술이다. 이는 주로 대형ISP에서 사용하는 방식이며 이는 Junk메일 발송지로 의심되는 메일서버의 IP를 black list로 공유하여 이 곳에서 발신되는 메일은 모두 smtp단에서 거부하는 방식이다. 또한 spam메일 발송 IP를 자동으로 탐지하는 기능까지 보강하여 Dynamic IP blocking 이라고 하는 차단기술이 특허 출원중에 있다.

이 같은 서버방식의 스팸메일 차단방식을 이용할 경우 다음과 같은 문제가 발생한다.

1)한글문자의 경우 영문자와 구조가 다르기 때문에 외국에서 제공되고 있는 스팸목록 서비스를 이용한 방식은 스팸 메일 차단효과가 떨어진다는 점이다. 또한 스팸머들은 자신의 메일도메인, 메일주소, IP주소를 적절하게 변경하여 사용하고 있기 때문에 이 또한 스팸목록만으로는 효과적인 스팸메일 차단이 어렵다. 따라서 스팸차단율을 높이기 위해서는 본문필터링(contents filtering)기술이 필수적으로 요청된다.

2)자신에게 수신될 이메일을 적절하게 받지 못하여 정신적 물질적 피해를 받을 수 있다. 관련 사례를 보면, AOL은 무수한 스팸메일로부터 회원들을 보호하기 위한 조치로써 스팸메일 차단 시스템을 설치 운영하면서 스팸메일 감시 대 상업체중의 하나인 어스링크의 일부 고객들이 AOL 계정으로 보낸 수 십 만 건의 이메일이 예정된 수신자에게 전달되지 못하고 차단되거나 삭제되었다. 스팸메일로 수신된 메일이라고 하더라도 사용자가 이를 관리(사용자에 의해서 스팸메일 또는 정상메일로 처리, 스팸메일 보관, 삭제)할 수 있는 시스템의 제공이 필요하다.

3)서버방식의 스팸메일 차단 경우에는 개인프라이버시의 침해라는 상황이 발생한다. 즉, 단체가 기업체에서 이 같은 서버차원이 스팸메일 차단 시스템을 설치하기 위해서는 사용자들의 동의를 받아야 한다. 즉, 개인정보의 누설 또는 누락이 있더라도 이를 감수하고 시스템을 이용하겠다는 서면동의서를 개개인한테 모두 받아야 설치할 수 있다. 이는 개인 프라이버시의 심각한 문제가 발생할 소지를 안고 있으며 개인들은 이러한 피해를 감수할 수 밖에 없다.

4)인터넷 환경하에서 전자우편을 통하여 청소년들에게 유해한 성인메일들이 스팸메일/정크메일 형식으로 직접적으로 전달됨으로써 사회문제화 되고 있다. 기존의 스팸목록방식으로는 이러한 성인메일을 완전히 차단할 수 없는 한계가 있다.

발명이 이루고자 하는 기술적 과제

이에, 본 발명은 이러한 종래 기술의 문제점을 해결하기 위하여 이루어졌다. 본 발명의 목적은 기존의 클라이언트/서버 시스템 환경하에서 스팸메일의 정보를 분석한 온라인스팸차단필터를 개인PC의 MUA(Mail User Agency)에 전달함으로써 개인 사용자들이 별도의 설정없이도 주어진 온라인스팸차단필터만으로 스팸메일을 차단할 수 있는 시스템을 제공하기 위한 것이다.

본 발명의 다른 목적은 온라인스팸차단필터를 이용하여 검출된 스팸메일은 IMAP/POP3 메일수신 서버방식을 이용하여 프로토콜에 따라 별도로 저장하여 관리하고 최종적으로는 저장된 스팸메일의 관리(스팸메일의 선택권)를 사용자가 시행함으로써 스팸메일의 정상메일로의 환원, 스팸메일의 보관, 삭제등의 스팸메일 관리방법을 제공하여 스팸메일차단시스템으로 인한 오류를 수정할 수 있도록 하기 위한 것이다.

본 발명의 또 다른 목적은 청소년들이 유해한 성인메일에 대한 접근을 차단하기 위해 암호화 설정을 통한 관리자 기능을 제공하기 위한 것이다.

본 발명의 또 다른 목적은 스팸메일로 인해 발생하는 유/무형의 손실을 최소화하기 위한 기술적인 방법을 제공하기 위한 것으로, 원격서버에서 제공되는 온라인스팸필터를 이용하여 개인의 PC에서 스팸메일을 처리할 수 있는 방법을 제공하기 위한 것이다.

본 발명의 또 다른 목적은 처리된 스팸메일을 사용자가 확인함으로써 스팸메일차단시스템의 부정확성으로 인한 오류를 최소화할 수 있는 관리시스템을 제공하기 위한 것으로서, 메일서버에서의 차단방식으로 인한 개인의 프라이버시 침해를 방지할 수 있으며, 또한 음란메일/스팸메일들이 바로 청소년들한테 노출되지 않도록 하는 기술적 해결방식을 제공하기 위한 것이다.

발명의 구성 및 작용

본 발명의 목적을 달성하기 위한 본 발명의 스팸메일차단 시스템은 통계적으로 정의되는 메일본문기준(contents filtering)필터를 제공하는 온라인스팸차단필터 제공시스템; 온라인스팸차단필터의 보관 및 배포를 위해서 인터넷으로 연결된 원격서버시스템; 및 원격서버시스템으로부터 온라인스팸차단필터를 제공받아 스팸메일을 POP3 Proxy방식과 IMAP방식을 사용하여 스팸메일을 관리 할 수 있는 MUA시스템 을 포함한다.

양호하게는, 온라인스팸차단필터 제공시스템은, 상용database 또는 파일시스템에 저장,보관되어 갱신된 정보를 주기적으로 수신받아서 자신의 정보를 update할 수 있는 DB시스템; 및 메일헤더정보를 분석하여 스팸메일을 검출하기 위한 스팸필터 1 와 메일본문내용을 기준으로 스팸메일을 검출하기 위한 스팸필터 2 와 Junk메일을 검출하기 위한 스팸필터 3 로 구성하되 MUA의 주소록정보와 스팸필터_2의 방식을 우선 적용하여 스팸필터_1과 스팸필터_3을 보완 적용하는 온라인스팸차단필터시스템 을 포함한다.

바람직하게는, 온라인스팸차단필터시스템의 스팸필터_1은 메일발송자주소정보, 메일도메인주소정보, 메일발송일자 정보, 메일경로 정보, 및 return-Path정보를 기준으로 수집된 리스트를 포함하고; 스팸필터_2는 특정문자열포함여부, 특정링크포함여부, 및 특정문자셋을 검출하기 위하여 통계적으로 수집된 리스트를 포함하며; 스팸필터_3은 메일사이즈 제한, 수신자수 및 참조자수 제한, 및 첨부파일 사이즈 제한을 통해 스팸메일을 검출하기 위한 리스트를 포함한다.

스팸메일차단 시스템은 온라인스팸차단필터가 저장되어 있는 원격서버시스템과 이 서버에 접근하여 온라인스팸차단필터를 다운받을 수 있도록 인터넷이나 유,무선으로 연결된 네트워크를 통해서 연결된 MUA에서 온라인스팸차단필터를 자동업데이트하여 MUA에 반영할 수 있도록 구성될 수 있다.

MUA시스템은 인터넷이나 네트워크로 연결된 원격서버로부터 제공받은 온라인스팸차단필터를 이용하여 스팸메일과 정상메일을 분류하여 개인PC에서 POP3 Proxy서버방식을 이용하여 IMAP서버에는 스팸메일, 정상메일은 일반POP3서버에 저장하도록 구성될 수 있다.

양호하게는, 스팸메일차단 시스템은 IMAP서버에 저장된 스팸으로 간주된 메일은 특정한 암호화 방식을 적용하여 허락된 인가자만이 암호를 입력하여 조회할 수 있는 보안방식 수행 수단; POP3서버에 저장된 정상메일을 추후 스팸메일로 처리할 수 있는 기능의 피드백 방식 수행 수단; IMAP서버에 저장된 스팸메일을 추후 정상메일로 처리할 수 있는 수단; 및 IMAP서버에 저장된 스팸메일의 관리를 위해 스팸메일의 삭제주기 및 자동삭제 기능을 제공하는 수단을 포함한다.

이하, 본 발명의 양호한 실시예를 첨부 도면을 참조하여 상세히 설명하기로 한다.

본 발명은 POP3 및 IMAP프로토콜을 지원하는 기존의 MUA에 적용된다. 즉 POP3와 IMAP에서 MRA(Mail Retrieval Agent)를 구현하고 있는 클라이언트/서버시스템에 적용된다.

도 1은 일반적인 메일시스템에서 MUA로 메일이 전달되는 과정을 설명해주는 블록 선도이다. 메일서버(200)에서는 수신된 메일을 로컬MDA(200b)가 할당된 개인로컬함에 저장하고 TCP포트 110번으로 POP데몬(200d)과 연결하여 메시지를 MUA(100c)로 전송한다.

도 2는 본 발명에 따른 스팸차단시스템의 구성을 도시한다. 스팸차단시스템은 인터넷등의 네트워크로 연결되어 온라인스팸차단필터를 제공하는 원격서버(400), 메일서버로부터 메일을 수신하여 이를 처리하는 POP3 Proxy서버(100a), IMAP서버(100b), POP3를 지원하는 MUA(100c)로 구성된다. POP3 Proxy서버(100a)에서는 원격서버(웹서버)와 접속하여 최신의 온라인스팸차단필터의 버전을 확인한 후 MUA에서 보유하고 있는 온라인스팸차단필터가 구 버전일 경우 이를 다운받을 수 있다. MUA에서 별도로 스팸차단용 필터를 생성하지 않더라도 온라인상으로 제공되는 온라인스팸차단필터를 이용하여 스팸메일을 차단함을 특징으로 한다.

도 3은 도2의 원격서버(400)의 구성과 작동방식을 설명하기 위한 블록 선도이다. 원격서버는 관리자에 의한 새로운 온라인스팸차단필터를 제공해서 update하는 일을 담당하는 Presentation tool(400a), MUA와 연결되어 필터버전을 확인하는 작업을 담당하는 Logic Tool(400b), DataBase(400c), MUA에 온라인스팸차단필터를 제공하기 위한 웹서버 구조(400d)로 구성됨을 특징으로 한다. 원격서버는 LAN, WAN, 또는 인터넷망으로 연결된 개인PC에 온라인스팸차단필터를 전달할 수 있도록 인터넷과 연결된 네트워크 상에서 운영된다. 원격서버(400)의 작동방식을 보면 최신의 온라인스팸차단필터(500)를 원격서버에 업로드(upload)한다. 이는 Presentation Tool(400a)에 관련 정보를 update함으로써 가능하다. 다수의 POP3 Proxy서버(100a)는 지정된 원격서버에서 최신의 온라인스팸차단필터 버전을 자동으로 확인하거나 일정한 간격을 두고 원격서버(400)에 접속하여 MUA에서 보유하고 있는 온라인스팸차단필터 버전과 비교하여 update사항이 있을 경우 자신의 MUA로 온라인스팸차단필터의 새버전을 다운로드한다. 이와 같은 온라인스팸차단필터의 버전비교는 정기적인 시간간격을 두거나 MUA가 재시동시 일정한 원격서버로 로그인하여 버전을 확인할 수 있다.

도 4는 온라인스팸차단필터의 구성을 도시하는 블록 선도이다. 온라인스팸차단필터는 스팸정보DB를 기초로 통계적 분류방식과 적용횟수(Hit수)를 근거로 작성된 스팸메일차단용리스트이다. 유해사이트에 대한 URL정보 및 이메일주소 List를 포함하는 스팸머리스트(500a), 통계적으로 적용되는 본문필터(Contents filter) 리스트(500b), 인터넷 규약을 지키지 않은 메일들을 검출하는 junk메일필터(500c)로 구성됨을 특징으로 한다.

온라인스팸차단필터는 인터넷규약에 따른 메일이 아닐 경우 즉 즉, 발송자, 수신자가 명기되어 있지 않거나, 제목들이 없는 경우 스팸메일로 간주하는 방식까지 포함한다. 메일본문필터의 경우 성인그림을 검색하기 위하여 단순텍스트문과 HTML(Hyper Text Markup Language)문을 동시에 검사할 수 있음을 특징으로 한다.

도 5는 본 발명에서 스팸메일차단시스템에서 원격서버를 제외한 부분을 설명하기 위한 블록 선도이다. 즉, 본 발명에

따라 스팸메일을 검출, 분류, 관리할 수 있는 방법을 제시한다. 메일서버로부터 수신한 메일에 대하여 MUA와 연동되는 POP3 Proxy 서버(100a)가 스팸메일을 판단, 검출하여 이를 IMAP서버(100b)에 저장하고, IMAP 프로토콜을 지원하는 MUA에서 해당 스팸메일을 확인할 수 있는 기술적 방식을 제공한다. MUA(100c)가 메일서버(200)로부터 메일을 수신하기 전 스팸차단시스템의 Proxy서버(100a)가 1차로 메일내용을 검사한다. 이 때 적용된 스팸메일의 검사기준은 온라인스팸차단필터, 개인스팸차단필터, MUA에 포함된 주소록이 될 수 있다. 이들 조합에 의해 스팸메일 판단이 이루어질 수 있음은 물론이다. 이때 스팸메일/정크메일로 검출된 메일은 스팸차단시스템의 IMAP서버(100b)로 전달되어 저장된다. 검출되지 않은 메일, 즉 정상메일이라고 판단한 메일들은 POP3 Proxy서버(100a)에서 바로 MUA(100c)로 전달된다. 이후 MUA는 IMAP서버에 접속해서 스팸메일들을 조회,관리한다. 이런 과정을 통해서 MUA 상에서는 정상메일과 스팸메일이 완전히 검출, 분류,관리된다. 스팸메일을 확인하여 추후에는 정상메일로 처리하고자 할 경우 MUA 상에서 바로 IMAP서버(100b)에 있는 메일을 선택하여 POP3폴더(100c)으로 이동이 가능하며 또한 반대의 경우도 가능하다. 이렇게 이동이 된 메일들은 이후 스팸메일 또는 정상메일로 처리가 된다. 본 방식을 이용할 경우 POP3와 IMAP간의 메일이동시에 사용자가 편리하게 사용할 수 있도록 MAU와 연동해서 drag&drop 방식을 지원함을 특징으로 한다.

도 6 도 4에서 설명한 POP3 Proxy서버에서 스팸메일을 검사하는 기준을 적용하는 플로우차트이다. 메일서버(200)에서 메일을 다운받으면 1차로 온라인스팸차단필터를 기준으로 스팸메일을 검출한다(S2). 검출된 스팸메일은 IMAP서버에 대응되는 스팸메일함(aa)에 저장되며 검출되지 않은 메일은 정상메일함(bb)으로 이동,저장된다. 각각의 정상메일함과 스팸메일함은 MUA(100c), IMAP서버(100b)에 대응된다.

도 7은 스팸메일을 차단하기 위한 플로우차트를 도시한다.도 4에서 설명한 POP3 Proxy서버에서 IMAP폴더 또는 POP3폴더로 전달되기 전에 스팸메일을 검출하기 위한 2단계로 구분된 스팸메일 검출기준을 도시한다. 메일서버(200)에서 메일을 다운받으면 1차로 주소록정보(S1)를 기준으로 스팸메일을 검출한다. 즉, MUA에서 보유하고 있는 메일 주소록을 기준으로 하여 전달받은 메일의 헤더 정보에 기록되어 있는 메일주소와 비교하여 공통된 메일주소를 검출하지 못할 경우 1차로 스팸메일로 간주되어 IMAP서버(100b)로 이동,저장된다. 2차 적용기준의 경우, 스팸메일로 검출된 메일에 대하여 온라인스팸차단필터(405)를 적용(s2), 이를 통하여 완전히 스팸메일로 검출된 메일은 완전스팸함(aa)에 , 검출되지 않은 메일은 불완전스팸메일함(cc)로 이동,저장된다. 즉, 메일함은 3가지, 즉 정상메일함(bb), 불완전스팸메일함(cc), 완전스팸메일함(bb)로 구분됨을 특징으로 한다. 또한 완전스팸메일함(aa), 불완전스팸메일함(cc)에 저장되어 있는 메일을 확인하여 사용자가 통과필터추가기능을 사용하여 추후 동일한 메일을 수신할 경우 스팸메일로 처리되지 않도록 할 수 있는 기능을 포함하고 있다. 여기서 통과필터란 특정메일에 한하여 온라인필터나 주소록 정보를 적용하지 않고 무조건 통과시킬 메일을 선택할 수 있도록 적용하는 필터이다. 따라서 불완전스팸메일함(cc) 또는 완전스팸메일함(aa)에 저장되어 있는 메일중에서 추후 정상메일로 처리하고자 할 경우 선택된 이메일주소 혹은 도메인주소를 등록하는 과정을 포함하여 처리함을 특징으로 한다.

도 8은 MUA에서 IMAP서버, POP3서버에 대응하는 메일함들의 접근권한 설정을 통하여 스팸메일, 특히 성인메일들이 청소년들에게 직접적으로 노출되지 않도록 관리 할 수 있는 방법을 도시한다. 사용자가 POP3서버에 접근할 경우 정상메일들이 보관되는 함들은 따로 비밀번호를 설정하지 않아도 누구나 접근이 가능하다. 그러나 사용자가 IMAP서버에 접근할 경우 관련 스팸메일함들에게 접근하기 위해서는 사용자 로그인과정이 요구된다(600).

본 발명에 의할 경우 IMAP서버의 경우 스팸메일,성인메일을 조회하지 못하도록 비밀번호를 부여하여 권한자만이 이를 접근하여 메일을 조회할 수 있는 기능을 제공한다.

발명의 효과

본 발명은 온라인스팸차단필터를 통해서 스팸메일을 차단해줄 수 있는 잇점을 제공하고 있다. 상기의 온라인스팸차단필터의 장점은 실시간으로 인터넷 또는 네트워크로 연결된 MUA에 필터리스트를 제공하기 때문에 사용이 편리하고, 실질적인 스팸정보DB를 기초로 통계적으로 분석, 제공됨으로 스팸차단 효과가 높다는 것이 장점이다. 온라인스팸차단필터에 의해 걸러진 스팸메일에 대하여 스팸메일의 유효성 판단 및 스팸메일 삭제,조회, 또는 정상메일로 처리 등의 최종권한을 사용자에게 부여함으로써 개인정보 침해사례를 해소할 수 있다.

또한 사용자가 최소한의 설정으로 스팸메일을 분류, 저장, 암호화할 수 있는 기능을 제공하여 스팸메일의 보기기능, 삭제기능등을 사용자의 권한에 따라서 선택적으로 부여할 수 있도록 하여 스팸메일을 처리하는 방식을 제공한다.

따라서 기존의 MUA에서 별다른 사용자 조작 없이도 스팸메일을 차단할 수 있는 시스템을 제공할 수 있다.

(57) 청구의 범위

청구항 1.

통계적으로 정의되는 메일본문기준(contents filtering)필터를 제공하는 온라인스팸차단필터 제공시스템 온라인스팸차단필터의 저장 및 배포를 위해서 인터넷으로 연결된 원격서버시스템 및 원격서버시스템으로부터 온라인스팸차단필터를 제공받아 스팸메일을 POP3 Proxy방식과 IMAP방식을 사용하여 스팸메일을 관리 할 수 있는 MUA시스템을 포함하는 것을 특징으로 하는 스팸메일차단 시스템.

청구항 2.

제1항에 있어서, 온라인스팸차단필터 제공시스템은, 상용database 또는 파일시스템에 저장,보관되어 갱신된 정보를 주기적으로 수신받아서 자신의 정보를 update할 수 있는 DB시스템 및 메일헤더정보를 분석하여 스팸메일을 검출하기 위한 스팸필터 1 와 메일본문내용을 기준으로 스팸메일을 검출하기 위한 스팸필터 2 와 Junk메일을 검출하기 위한 스팸필터 3 로 구성하되 MUA의 주소록정보와 스팸필터_2의 방식을 우선 적용하여 스팸필터_1과 스팸필터_3을 보완 적용하는 온라인스팸차단필터시스템 을 포함하는 것을 특징으로 하는 스팸메일차단 시스템.

청구항 3.

제2항에 있어서, 온라인스팸차단필터시스템의 스팸필터_1은 메일발송자주소정보, 메일도메인주소정보, 메일발송일자정보, 메일경로 정보, 및 return-Path정보를 기준으로 수집된 리스트를 포함하고 스팸필터_2는 특정문자열포함여부, 특정링크포함여부, 및 특정문자셋을 검출하기 위하여 통계적으로 수집된 리스트를 포함하며 스팸필터_3은 메일 사이즈 제한, 수신자수 및 참조자수 제한, 및 첨부파일 사이즈 제한을 통해 스팸메일을 검출하기 위한 리스트를 포함하는 것을 특징으로 하는 스팸메일차단 시스템.

청구항 4.

제1항에 있어서, 온라인스팸차단필터가 저장되어 있는 원격서버시스템과 이 서버에 접근하여 온라인스팸차단필터를 다운받을 수 있도록 인터넷이나 유,무선으로 연결된 네트워크를 통해서 연결된 MUA에서 온라인스팸차단필터를 자동 업데이트하여 MUA에 반영할 수 있도록 구성된 것을 특징으로 하는 스팸메일차단 시스템.

청구항 5.

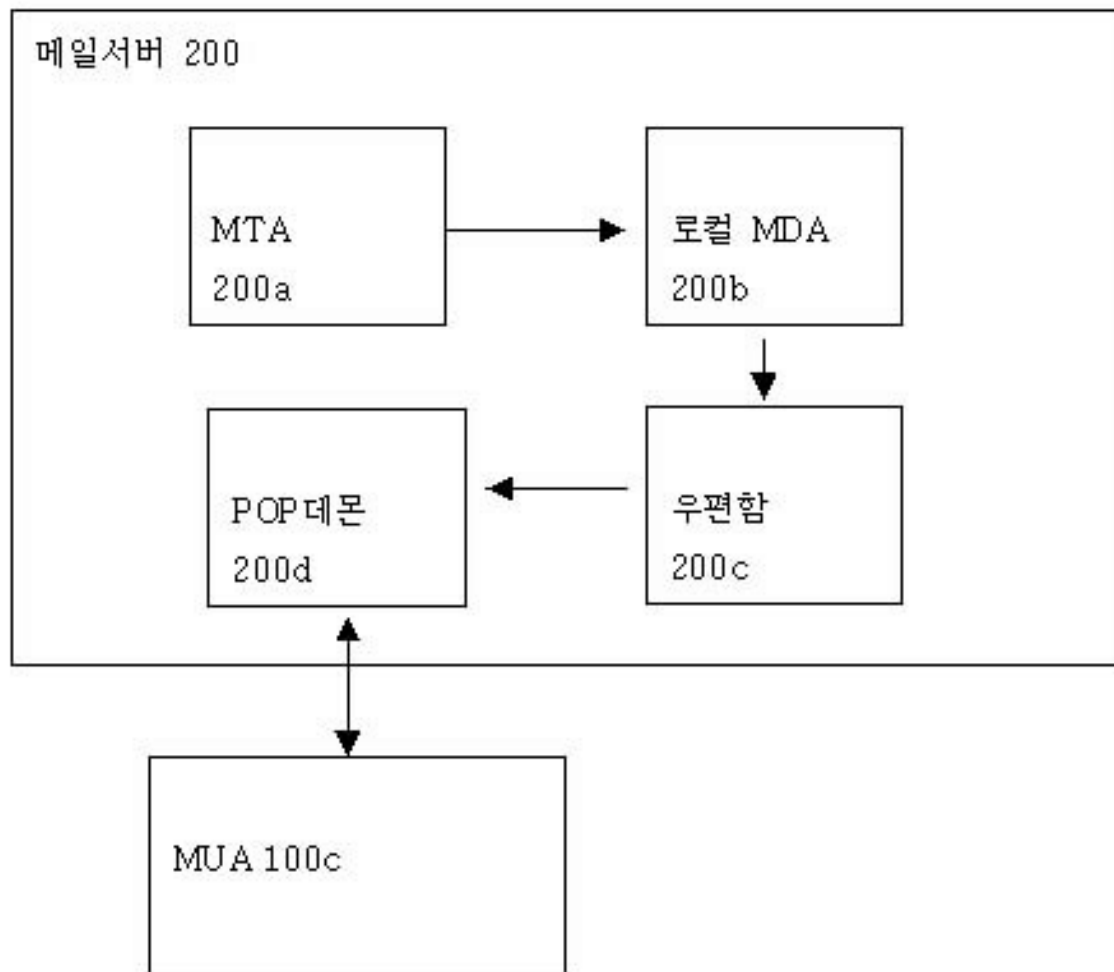
제1항에 있어서, MUA시스템은 인터넷이나 네트워크로 연결된 원격서버로부터 제공받은 온라인스팸차단필터를 이용하여 스팸메일과 정상메일을 분류하여 개인PC에서 POP3 Proxy서버방식을 이용하여 IMAP서버에는 스팸메일, 정상메일은 일반POP3서버에 저장하도록 구성된 것을 특징으로 하는 스팸메일차단 시스템.

청구항 6.

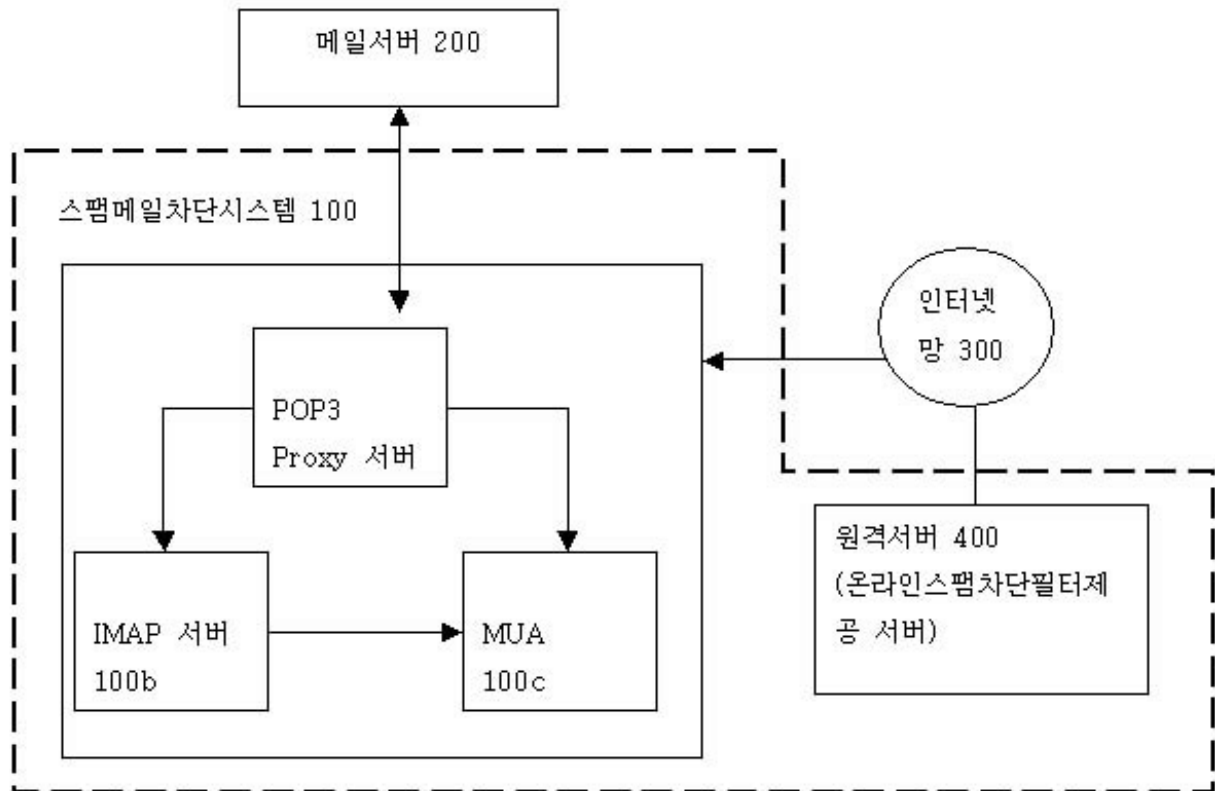
제5항에 있어서, IMAP서버에 저장된 스팸으로 간주된 메일은 특정한 암호화 방식을 적용하여 허락된 인가자만이 암호를 입력하여 조회할 수 있는 보안방식 수행 수단; POP3서버에 저장된 정상메일을 추후 스팸메일로 처리할 수 있는 기능의 피드백 방식 수행 수단; IMAP서버에 저장된 스팸메일을 추후 정상메일로 처리할 수 있는 수단 및 IMAP서버에 저장된 스팸메일의 관리를 위해 스팸메일의 삭제주기 및 자동삭제 기능을 제공하는 수단을 포함하는 것을 특징으로 하는 스팸메일차단 시스템.

도면

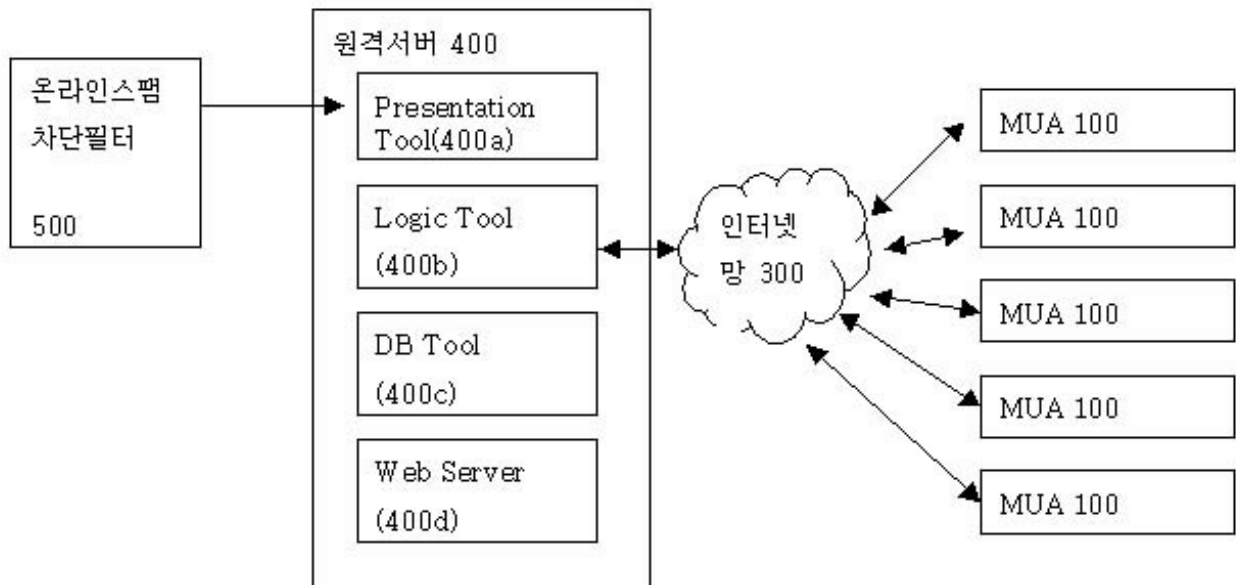
도면1



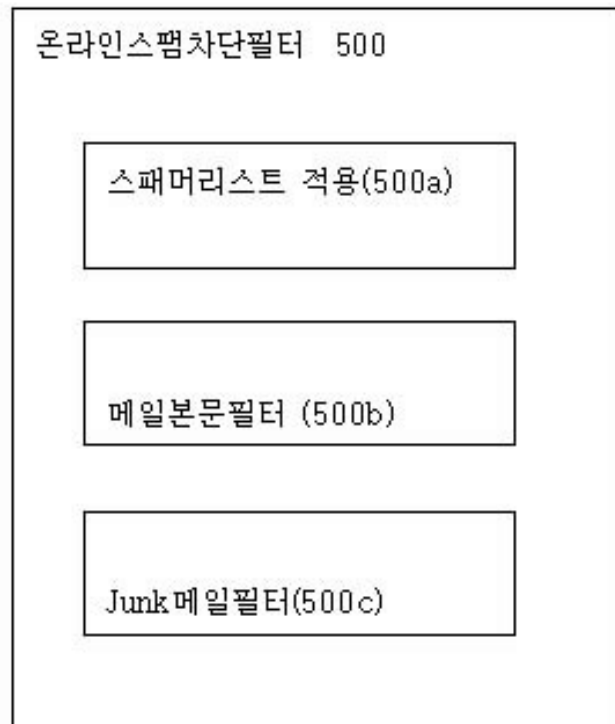
도면2



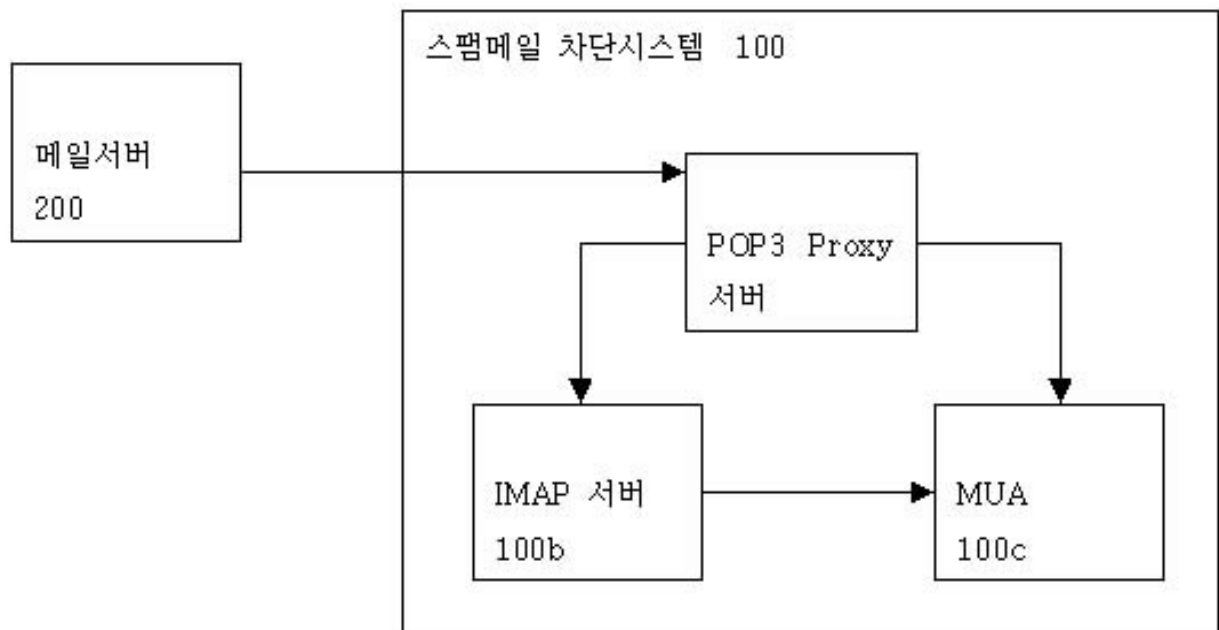
도면3



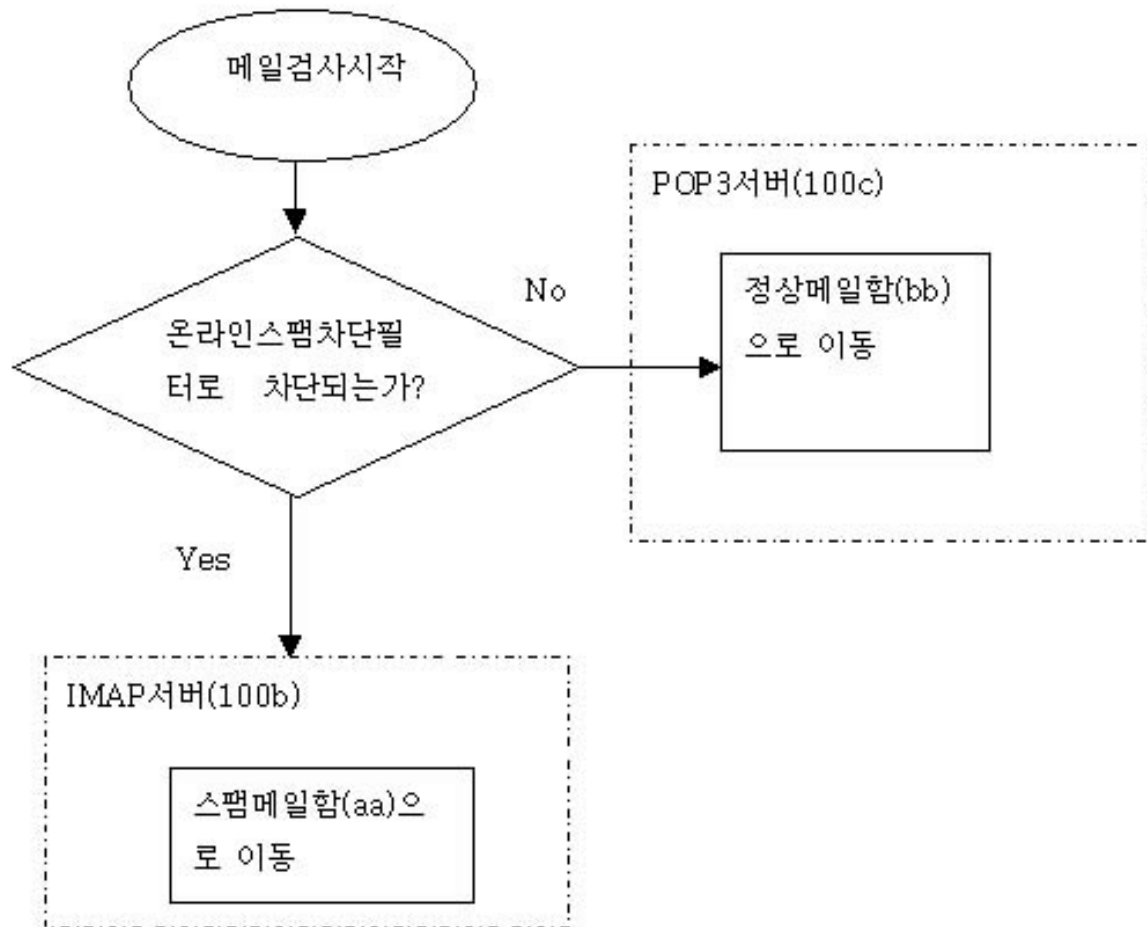
도면4



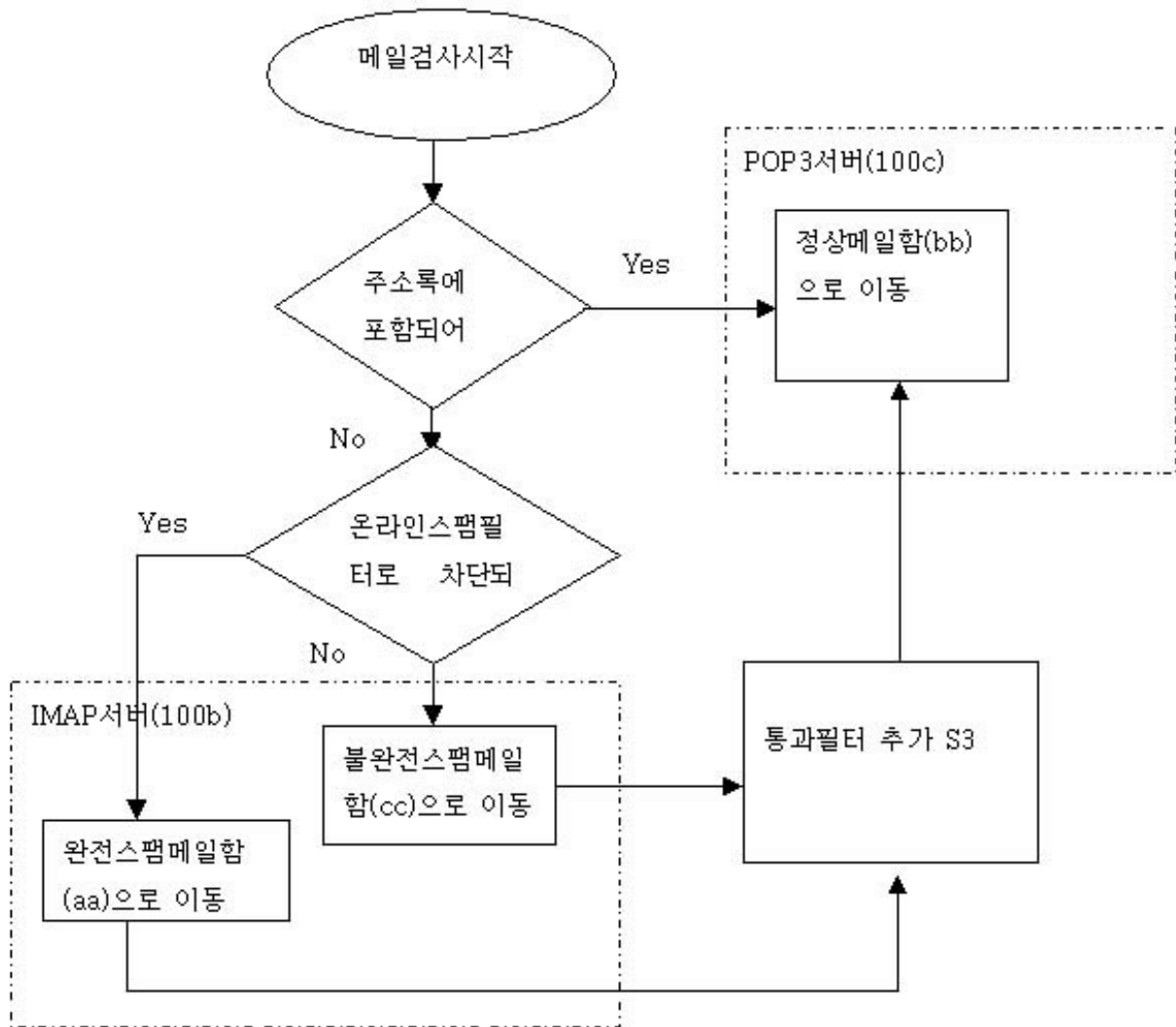
도면5



도면6



도면7



도면8

