(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2014 년 10 월 9 일 (09.10.2014)

WIPO | PCT

(10) 국제공개번호
WO 2014/163355 A1

(51) 국제특허분류:
G06F 21/00 (2013.01) *G06F 21/50* (2013.01)

(21) 국제출원번호: PCT/KR2014/002741

(22) 국제출원일: 2014 년 3 월 31 일 (31.03.2014)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2013-0037465 2013 년 4 월 5 일 (05.04.2013) KR

(71) 출원인: 소프트캠프(주) (SOFTCAMP CO., LTD) [KR/KR]; 135-935 서울시 강남구 테헤란로 8 길 37,5F, Seoul (KR).

(72) 발명자: 배환국 (BAE, Steve); 463-420 경기도 성남시 분당구 판교역로 100, 602 동 1503 호 (백현동, 백현마을), Gyeonggi-do (KR). 박경옥 (PARK, Kyung ok); 464-902 경기도 광주시 중앙로 187 번길 37, Gyeonggi-do (KR).

(74) 대리인: 이상문 (LEE, Sang-moon) 등; 135-925 서울시 강남구 논현로 417, 501 호(역삼동, 화원빌딩), Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

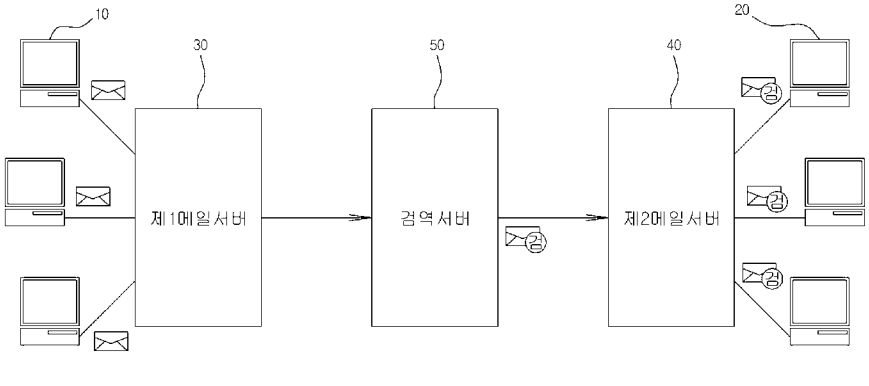
공개:

— 국제조사보고서와 함께 (조약 제 21 조(3))

— 청구범위 보정 기한 만료 전의 공개이며, 보정서를 접수하는 경우 그에 관하여 별도 공개함 (규칙 48.2(h))

(54) Title: METHOD AND SYSTEM FOR INSPECTING ELECTRONIC DOCUMENTS

(54) 발명의 명칭 : 전자문서 검역방법 및 검역시스템



30 ... First mail server
40 ... Second mail server
50 ... Inspection server

(57) Abstract: The present invention relates to a method and a system for inspecting an electronic document, which inspects a variety of viruses and malicious codes contained in an electronic mail and an attachment file. The method for inspecting an electronic document comprises: a first step for pre-receiving, by an inspection server, an electronic document transmitted to a receiving terminal; a second step for removing, by the inspection server, a setting macro within the electronic document; and a third step for transmitting, by the inspection server, the electronic document from which the setting macro has been removed.

(57) 요약서: 본 발명은 전자메일과 첨부파일에 포함된 각종 바이러스 및 악성 코드를 검역하는 전자문서 검역방법 및 검역시스템에 관한 것으로, 검역서버가 수신단말기로 발신된 전자문서를 사전 수신하는 제 1 단계; 상기 검역서버가 상기 전자문서 내 설정 매크로를 제거하는 제 2 단계; 및 설정 매크로가 제거된 상기 전자문서를 상기 검역서버가 발신하는 제 3 단계;를 포함하는 것이다.

WO 2014/163355 A1

명세서

발명의 명칭: 전자문서 검역방법 및 검역시스템

기술분야

[1] 본 발명은 전자메일과 첨부파일에 포함된 각종 바이러스 및 악성 코드를 검역하는 전자문서 검역방법 및 검역시스템에 관한 것이다.

배경기술

[2] 최근 인터넷과 같은 통신망이 발달하면서, 통신망을 이용한 상업적, 비상업적 서비스가 기하 급수로 증가하고 있다. 이와 같은 통신망 서비스 중의 하나가 전자메일이다. 전자메일은 송신자가 지정하는 수신자의 전자메일주소로 메시지를 전달할 수 있는 서비스이다. 상대방 전자메일의 주소는 통상적으로 사용자의 컴퓨터에 저장되므로, 메시지를 쉽게 송신할 수 있다.

[3] 한편, 컴퓨터 바이러스는 1980년대 중반 이후 개인용 컴퓨터를 바탕으로 본격적으로 발생하여 확산되었으며, 오늘날에는 개인용 컴퓨터뿐만 아니라 네트워크 컴퓨터와 통신망 등에서도 많은 피해를 발생시키고 있다. 즉, 바이러스에 미감염된 컴퓨터에 감염된 프로그램이 들어오면, 컴퓨터 시스템은 사용자가 의도하지 않은 동작들을 수행하는 경우가 발생하는 것이다. 예를 들면, 바이러스에 감염된 컴퓨터는 사용자의 의사와는 무관하게, 자신의 컴퓨터에 저장되어 있는 모든 전자메일의 주소로 바이러스를 포함하고 있는 메시지를 전송한다. 이와 같은 경우에, 바이러스를 포함하고 있는 메시지를 전송받은 또 다른 사용자의 컴퓨터도 감염되게 된다. 이와 같은 전자메일을 통한 바이러스의 확산은 엄청난 피해를 발생하게 되는데, 1999년에는 MELISSA 바이러스의 출현으로 미국에서는 약 3억 8천 오백만 달러의 피해를 보았다. 그리고, 2000년에 출현한 러브레터 바이러스는 약 150억 달러 정도의 피해를 발생시켰다. 따라서, 컴퓨터 바이러스에 감염된 컴퓨터로부터 사용자가 의도하지 않는 전자메일의 발송을 효과적으로 차단하는 것이 요구된다.

[4] 그런데 전자메일은 온라인 통신환경에서 널리 활용되는 통신매체로서, 컴퓨터 바이러스 또는 악성코드 등을 이유로 그 사용을 제한하는 것은 사실상 불가능하다. 따라서, 종래에는 전자메일의 바이러스 감염 여부 등을 확인해서, 전자메일을 통한 바이러스의 확산은 방지하고 전자메일의 이용은 활성화할 수 있는 다양한 방안이 제안되었다(선행기술문헌 참조).

[5] 하지만, 전자메일에 포함되는 바이러스의 감염형식은 너무나 다양하고 새로우므로, 전자메일의 감염 여부를 확인하기 위한 백신은 최신 바이러스의 감염형식을 뒤따르는 형태를 취할 수밖에 없었다. 특히 데이터의 내용 중에서 사용자가 의도하지 않은 매크로(이하 '악성매크로')의 경우에는 백신이 바이러스로 인식하지 못하고 검역하지도 못하므로, 사용자는 최신 바이러스를 자신의 컴퓨터에 그대로 감염시키거나 악성매크로를 실행시켜서 데이터 처리에

오류를 일으키는 문제가 있었다.

발명의 상세한 설명

기술적 과제

[6] 이에 본 발명은 상기와 같은 문제를 해소하기 위해 발명된 것으로서, 전자메일의 첨부파일인 문서파일 원문을 보호하면서도, 포함된 악성매크로를 확인해 제거할 수 있는 전자문서 검역방법 및 검역시스템의 제공을 해결하고자 하는 과제로 한다.

[7] 또한, 전자메일에 은닉된 각종 바이러스 또는 웹페이지 등을 확인 및 삭제할 수 있는 전자문서 검역방법 및 검역시스템의 제공을 해결하고자 하는 또 다른 과제로 한다.

과제 해결 수단

[8] 상기의 기술적 과제를 달성하기 위하여 본 발명은,

[9] 검역서버가 수신단말기로 발신된 전자문서를 사전 수신하는 제1단계;

[10] 상기 검역서버가 상기 전자문서 내 설정 매크로를 제거하는 제2단계; 및

[11] 설정 매크로가 제거된 상기 전자문서를 상기 검역서버가 발신하는 제3단계;

[12] 를 포함하는 전자문서 검역방법이다.

발명의 효과

[13] 상기의 본 발명은, 일반 컴퓨터 백신프로그램에서는 검역하거나 치료할 수 없었던 전자메일의 첨부파일 내 악성매크로를 제거할 수 있으므로, 해당 첨부파일로 인해 발생하는 수신단말기의 오작동과 각종 바이러스 등의 감염을 최소화할 수 있는 효과가 있다.

[14] 또한, 첨부파일 내 악성매크로 제거와 더불어 전자메일 본문에 은닉된 스크립트 또는 ActiveX 등의 실행을 원천적으로 차단하므로, 전자메일의 보안도를 높이는 효과가 있다.

도면의 간단한 설명

[15] 도 1은 본 발명에 따른 검역시스템을 도시한 블록도이고,

[16] 도 2는 본 발명에 따른 검역서버의 구성을 도시한 블록도이고,

[17] 도 3은 본 발명에 따른 검역방법을 순차 도시한 플로차트이고,

[18] 도 4는 본 발명에 따른 검역방법에서 첨부파일 검역단계를 구체적으로 도시한 플로차트이고,

[19] 도 5는 본 발명에 따른 검역시스템의 다른 실시 모습을 도시한 블록도이다.

발명의 실시를 위한 최선의 형태

[20] 상술한 본 발명의 특징 및 효과는 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해질 것이며, 그에 따라 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자가 본 발명의 기술적 사상을 용이하게 실시할 수 있을 것이다. 본 발명은 다양한 변경을 가할 수 있고 여러 가지 형태를 가질 수 있는바, 특정 실시예들을 도면에 예시하고 본문에 상세하게 설명하고자 한다. 그러나, 이는 본

발명을 특정한 개시형태에 대해 한정하려는 것이 아니며, 본 발명의 사상 및 기술 범위에 포함되는 모든 변경, 균등물 내지 대체물을 포함하는 것으로 이해되어야 한다. 본 출원에서 사용한 용어는 단지 특정한 실시 예들을 설명하기 위해 사용된 것으로, 본 발명을 한정하려는 의도가 아니다.

[21]

[22] 이하, 본 발명을 실시하기 위한 구체적인 내용을 첨부된 도면에 의거하여 상세히 설명한다.

[23] 도 1은 본 발명에 따른 검역시스템을 도시한 블록도이고, 도 2는 본 발명에 따른 검역서버의 구성을 도시한 블록도이다.

[24] 본 발명에 따른 검역시스템은 송신단말기(10)와 수신단말기(20)가 인터넷과 같은 통신망에 접속하여 전자메일을 송수신할 수 있도록 제1메일서버(30)와 제2메일서버(40)를 포함한다. 이를 좀 더 구체적으로 설명하면, 송신단말기(10)는 상기 통신망을 통해 제1메일서버(30)에 접속해서 전자메일을 작성 및 전송하고, 제2메일서버(40)는 제1메일서버(30)가 전송한 상기 전자메일을 수신해서 접속하는 수신단말기(20)가 상기 전자메일을 확인할 수 있도록 한다. 여기서, 제1메일서버(30)는 발신 전용 서버이고, 제2메일서버(40)는 수신 전용 서버로서, 제1,2메일서버(30, 40)는 동일한 메일시스템의 수발신 서버일 수도 있고, 서로 다른 메일시스템의 수발신 서버일 수도 있다.

[25] 본 발명에 따른 검역시스템은 제1메일서버(30)에서 제2메일서버(40)로 전송되는 전자메일을 필터링해서 악성매크로를 포함하는 첨부파일을 확인 및 삭제하는 검역서버(50)를 더 포함한다. 이를 통해 악성매크로는 수신단말기(20)에 무단 입력됨이 방지되고, 수신단말기(20)는 안정된 보안환경에서 전자메일의 첨부파일을 실행할 수 있다.

[26] 이를 위한 검역서버(50)를 좀 더 구체적으로 설명하면, 전자메일의 첨부파일에 포함된 악성매크로를 확인해서 이를 삭제하는 매크로모듈(51)과, 전자메일 본문의 스크립트 또는 ActiveX 무력화, 압축파일 처리, 컴퓨터바이러스 검사, 검역 후 인증처리 등을 실행하는 처리모듈(52)과, 검역 후 상기 전자메일이 지정된 제2메일서버(40)로 전송되도록 처리하는 통신모듈(53)을 포함한다.

[27] 매크로모듈(51)은 전자메일의 첨부파일인 문서파일에 형성된 매크로(Macro)를 확인하고 이를 삭제한다. '매크로'는 자주 사용하는 여러 개의 명령어를 묶어서 하나의 키 입력 동작으로 이루어지도록 설정하는 것으로서, 'MS OFFICE' 프로그램 중 'Excel'에서 그 기능이 대표적으로 예시될 수 있다. 상기 매크로는 사용자가 임의로 생성해서 해당 문서파일에 설정할 수 있고, 이렇게 설정된 매크로는 단축키로서 유용하게 활용된다.

[28] 그런데, 정작 사용자가 설정하지 않은 매크로(악성매크로)의 경우에는 사용자가 생각하지 못한 단축키 조작으로 인해서 원치 않는 컴퓨터 실행이 이루어질 수 있다. 따라서, 본 발명에 따른 검역서버(50)의 매크로모듈(51)은 전자메일의 첨부파일인 해당 문서파일에 설정된 매크로를 제거하는 기능을

포함한다.

[29] 'Excel'의 메뉴에서 확인할 수 있는 바와 같이, 매크로 기능을 갖는 전자문서 프로그램은 매크로 생성 및 삭제 기능을 포함하는데, 매크로모듈(51)은 해당 전자문서 프로그램의 매크로 기능을 구성시켜서, 전자메일의 첨부파일인 문서파일 내 매크로를 강제로 삭제할 수 있도록 한다.

[30] 이외에도 매크로모듈(51)은 매크로 삭제를 대신해서 전자문서를 이미지화할 수 있고, 이를 통해 매크로의 실행이 원천적으로 차단되도록 할 수 있다. 참고로, 전자문서의 이미지화는 PDF이미지 처리가 예시될 수 있다.

[31] 처리모듈(52)은 전자메일 본문의 스크립트 또는 ActiveX 무력화, 압축파일 처리, 컴퓨터바이러스 검사, 검역 후 인증처리 등을 실행한다. 이에 대해서는 본 발명에 따른 검역방법을 설명하면서 상세히 한다.

[32] 통신모듈(53)은 검역서버(50)에 수신한 전자메일을 제2메일서버(40)로 전송해서 수신단말기(20)가 수신할 수 있도록 한다. 즉, 통신모듈(53)은 기존 제1,2메일서버(30, 40)를 검역서버(50)가 중계하는 기능을 갖도록 하는 것이다.

[33]

[34] 도 3은 본 발명에 따른 검역방법을 순차 도시한 플로차트인 바, 이를 참조해 설명한다.

[35] S10; 전자메일 송부단계

[36] 송신자는 송신단말기(10)를 활용해서 제1메일서버(30)에 접속한 후, 전자메일 본문을 작성한다. 이때, 상기 전자메일의 첨부파일로 전자문서를 첨부한다.

[37] 제1메일서버(30)는 전술한 바와 같이 메일서버의 발신 전용 서버로서, 송신자는 제1메일서버(30)에 접속해서 수신자의 이메일주소를 입력하고, 상기 전자메일의 본문 작성 후 전자문서를 첨부파일로 첨부한다.

[38] 전자메일의 메일 발신 기술은 공지,공용의 기술이므로, 여기서는 그 설명을 생략한다.

[39] 제1메일서버(30)에 접속한 송신단말기(10)는 전자문서가 첨부된 전자메일을 업로드하고, 제1메일서버(30)는 해당 전자메일을 발신한다.

[40]

[41] S20; 첨부파일 검역단계

[42] 본 발명에 따른 검역시스템에서 제1메일서버(30)는 상기 전자메일을 지정된 검역서버(50)로 1차 전송하고, 검역서버(50)는 상기 전자메일을 수신한 후 절차에 따라 검역을 진행한다.

[43] 제1메일서버(30)에 위치한 전자메일을 검역서버(50)로 전송하기 위해서, 제1메일서버(30)의 DNS(domain name system)에 MX 레코드를 검역서버(50)로 설정함으로써 상기 전자메일이 검역서버(50)로 1차 전송되도록 할 수 있고, 제1메일서버(30)와 검역서버(50)를 브릿지모드로 연결해서 제1메일서버(30)에 입력된 상기 전자메일이 자동으로 검역서버(50)에 1차 전송되도록 할 수 있다.

[44] 전술한 바와 같이, 검역서버(50)는 전자메일의 첨부파일인 전자문서의

악성매크로가 실행되지 않도록, 상기 악성매크로를 강제로 삭제하거나, 상기 전자문서를 이미지파일로 변환한다.

[45] 검역서버(50)에서 이루어지는 검역기능에 대해 도면을 참조해 좀 더 구체적으로 설명한다.

[46]

[47] 도 4는 본 발명에 따른 검역방법에서 첨부파일 검역단계를 구체적으로 도시한 플로차트이다.

[48] S21; 압축파일 확인단계

[49] 검역서버(50)의 처리모듈(52)은 전자메일의 첨부파일이 압축파일 여부를 확인한다. 압축파일의 확장자는 공지된 바와 같이 *.zip, *.rar, *.7z, *.tar 등 다양하며, 처리모듈(52)은 첨부파일의 확장자를 확인해서 해당 파일이 압축파일인지 여부를 확인한다.

[50]

[51] S22; 압축해제 단계

[52] 압축파일 확인단계(S21)에서 첨부파일이 압축파일로 확인되면, 처리모듈(52)은 상기 첨부파일의 압축상태를 해제한다. 결국, 압축상태의 첨부파일은 해제되고, 이를 통해 실행가능한 하나 이상의 파일로 분리된다.

[53] 물론, 압축파일 확인단계(S21)에서 첨부파일이 압축파일이 아닌 것으로 확인되면, 처리모듈(52)은 상기 첨부파일의 압축 해제 과정을 진행하지 않고 다음 단계를 진행한다.

[54]

[55] S23; 매크로 제거단계

[56] 매크로모듈(51)은 첨부파일로 확인된 전자문서에서 악성매크로를 강제로 제거한다. 상기 전자문서에서 악성매크로를 강제로 제거하는 방법으로, 해당 전자문서에 설정된 모든 매크로를 삭제해서 악성매크로까지 일괄적으로 제거하는 제1방법과, 해당 전자문서를 이미지파일로 변환해서 악성매크로의 실행을 원천적으로 차단하는 제2방법이 제안된다. 따라서, 매크로모듈(51)은 상기 제1방법을 실시하기 위해서 해당 전자문서를 실행하기 위한 프로그램의 매크로 실행 기능을 갖출 수 있다. 또한, 매크로모듈(51)은 상기 제2방법을 실시하기 위해서 해당 전자문서를 출력한 후 이미지파일로 변환하는 기능을 갖출 수 있다. 결국, 매크로모듈(51)은 악성매크로로부터 수신단말기(20)를 보호하기 위해서, 상기 악성매크로를 포함하는 전자문서의 실행 프로그램의 기능을 갖추어야 한다.

[57]

[58] S24; 전자메일 본문 무력화단계

[59] 처리모듈(52)은 전자메일의 본문에 구성된 스크립트(script) 또는 ActiveX의 실행이 이루어지지 않도록 제한한다.

[60] HTML(HyperText Markup Language) 형식의 전자메일 본문에는 특정

URL(uniform resource locator)이 링크된 은닉된 스크립트가 포함될 수 있고, 전자메일 수신자는 이를 인지하지 못하고 전자메일 내 해당 링크 내용을 클릭해서 악성 사이트에 접속할 수 있다. 따라서 처리모듈(52)은 전자메일 본문에 링크된 모든 스크립트를 무력화하고, 상기 본문 전체를 텍스트화한다. 결국, 전자메일의 본문은 어디에도 링크기능이 없는 텍스트만 남고, 이를 통해 수신단말기(20)는 악성 사이트로의 무단 접속이 방지된다.

[61] 한편, 처리모듈(52)은 전자메일의 본문에 설정된 ActiveX를 삭제해서 악성코드로서 전자메일에 설정된 ActiveX까지 일괄적으로 삭제될 수 있도록 한다. 결국, 전자메일의 본문은 악성 ActiveX에 의해서 수신자가 의도하지 않는 형태로 동작하거나, 상기 전자메일을 수신한 수신단말기(20)가 특정 사이트 등에 무단 접속하는 것을 방지할 수 있다.

[62]

[63] S25; 컴퓨터바이러스 검사단계

[64] 처리모듈(52)은 전자메일 및 첨부파일의 컴퓨터바이러스 감염 여부를 검사하고, 컴퓨터바이러스 감염이 확인되면 이를 자동 또는 질의 후 치료한다. 전자메일 및 첨부파일에 대한 컴퓨터바이러스 감염 여부 검사 기능을 갖는 일명 컴퓨터백신프로그램은 공지,공용의 기술이므로, 여기서는 그 동작과 구성에 대한 설명은 생략한다.

[65]

[66] S26; 검역필 인증단계

[67] 악성매크로 제거 또는 컴퓨터바이러스 검사 중 선택된 하나 이상의 검역과정이 완료되면, 처리모듈(52)은 도 1에서 보인 바와 같이 첨부파일의 아이콘이미지에 검역필 인증마크를 삽입한다. 결국, 수신자는 수신한 전자메일의 첨부파일 아이콘이미지에서 인증마크를 확인함으로써 상기 전자메일에 대한 신뢰감을 느낄 수 있고, 더불어서 상기 전자메일을 클릭해 열람할 수 있게 된다.

[68] 본 발명에 따른 실시 예에서는 첨부파일 아이콘이미지에 인증마크가 삽입되도록 하였으나, 이외에도 첨부파일 명을 "인증"을 추가 기재할 수도 있다.

[69]

[70] S27; 압축대상 확인단계

[71] 처리모듈(52)은 첨부파일이 압축대상인지를 확인한다. 즉, 해당 첨부파일들이 압축파일 확인단계(S21)에서 압축파일로 확인된 파일이었는지를 확인하는 것이다.

[72]

[73] S28; 압축단계

[74] 압축대상 확인단계(S27)에서 압축대상으로 확인되면, 처리모듈(52)은 해당 첨부파일을 압축해서 최초 첨부파일 형태가 되도록 한다. 한편, 처리모듈(52)은 압축된 첨부파일의 아이콘이미지에도 인증마크를 삽입해서, 수신자가 신뢰를 갖고 압축을 해제하도록 할 수 있다.

[75]

[76] S30; 전자메일 복원단계

[77] 통신모듈(53)은 검역이 완료된 전자메일을 SMTP(simple mail transfer protocol)를 이용해서 제2메일서버(40)로 2차 전송한다.

[78] 상기 전자메일의 최종 수신지는 제2메일서버(40)의 지정 어드레스로 이미 입력되어 있으므로, 검역이 완료된 해당 전자메일은 지정 어드레스에 따라 제2메일서버(40)로 전송한다.

[79]

[80] S40; 전자메일 수신단계

[81] 제2메일서버(40)는 상기 전자메일을 수신하고, 수신단말기(20)는 제2메일서버(40)에 접속해서 상기 전자메일의 수신을 확인한다. 계속해서, 수신단말기(20)는 상기 전자메일의 본문을 실행하고, 아울러 첨부파일을 다운로드해서 해당 프로그램을 통해 실행한다.

[82] 참고로, 상기 전자메일의 본문은 스크립트 및 ActiveX의 무력화를 통해 해당 텍스트만이 출력되고, 첨부파일은 그 실행시 악성매크로의 실행을 제한할 수 있다.

[83]

[84] 도 5는 본 발명에 따른 검역시스템의 다른 실시 모습을 도시한 블록도인 바, 이를 참조해 설명한다.

[85] 앞서 설명한 검역시스템은 전자메일에 적용된 경우를 예시하였으나, 본 발명에 따른 실시 예에서의 검역시스템은 인터넷 등의 공중망과, 이더넷 등의 내부망 간에 교환되는 전자문서 만에 대한 검역 기능을 수행할 수 있다.

[86] 이를 좀 더 구체적으로 설명하면, 공중망과 내부망은 공지,공용의 망연계서버(70)를 매개로 연결돼 통신하고, 이를 통해 내부망의 수신단말기(20)는 공중망으로부터 유입되는 각종 전자문서를 명연계서버(70)를 통하여 수신한다. 여기서, 검역서버(50)는 전자문서가 내부망으로 수신되기 전 전술한 검역 절차를 통해 검역을 완료하고, 해당 검역이 완료되면 망연계서버(70)의 통상적인 수신절차를 통해 내부망의 수신단말기(20)가 이를 수신할 수 있도록 한다.

[87] 결국, 내부망은 검역서버(50)를 통해 악성매크로에 의한 오작동 또는 컴퓨터바이러스 등에 의한 각종 감염 등의 위험을 최소화하고, 이를 통해 해당 통신환경을 안정적으로 유지할 수 있다.

[88]

[89] 앞서 설명한 본 발명의 상세한 설명에서는 본 발명의 바람직한 실시 예들을 참조해 설명했지만, 해당 기술분야의 숙련된 당업자 또는 해당 기술분야에 통상의 지식을 갖는 자라면 후술될 특허청구범위에 기재된 본 발명의 사상 및 기술영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

서열목록 Free Text

[90] 10; 발신단말기 20; 수신단말기 30; 제1메일서버

[91] 40; 제2메일서버 50; 검역서버 60,60'; 제1,2외부서버

[92] 70; 망연계서버

청구범위

[청구항 1] 검역서버가 수신단말기로 발신된 전자문서를 사전 수신하는 제1단계;
상기 검역서버가 상기 전자문서 내 설정 매크로를 제거하는 제2단계; 및
설정 매크로가 제거된 상기 전자문서를 상기 검역서버가 발신하는 제3단계;
를 포함하는 것을 특징으로 하는 전자문서 검역방법.

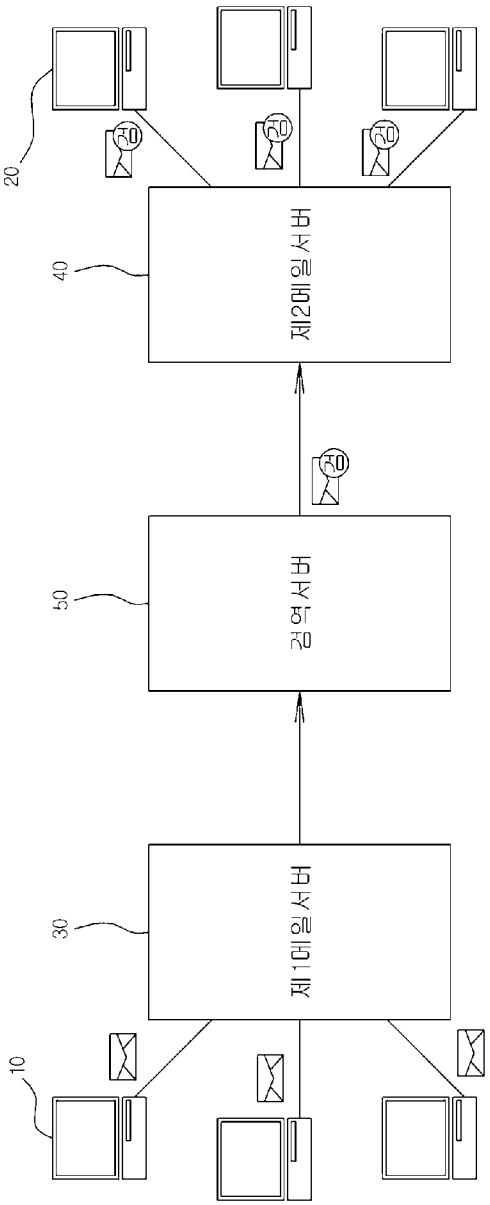
[청구항 2] 제 1 항에 있어서,
상기 전자문서는 전자메일의 첨부파일인 것을 특징으로 하는 전자문서 검역방법.

[청구항 3] 제 1 항 또는 제 2 항에 있어서,
상기 제2단계는
상기 전자문서의 설정 매크로가 제거되도록 상기 전자문서를 이미지화해서 이미지파일로 변환하는 단계를 더 포함하는 것을 특징으로 하는 전자문서 검역방법.

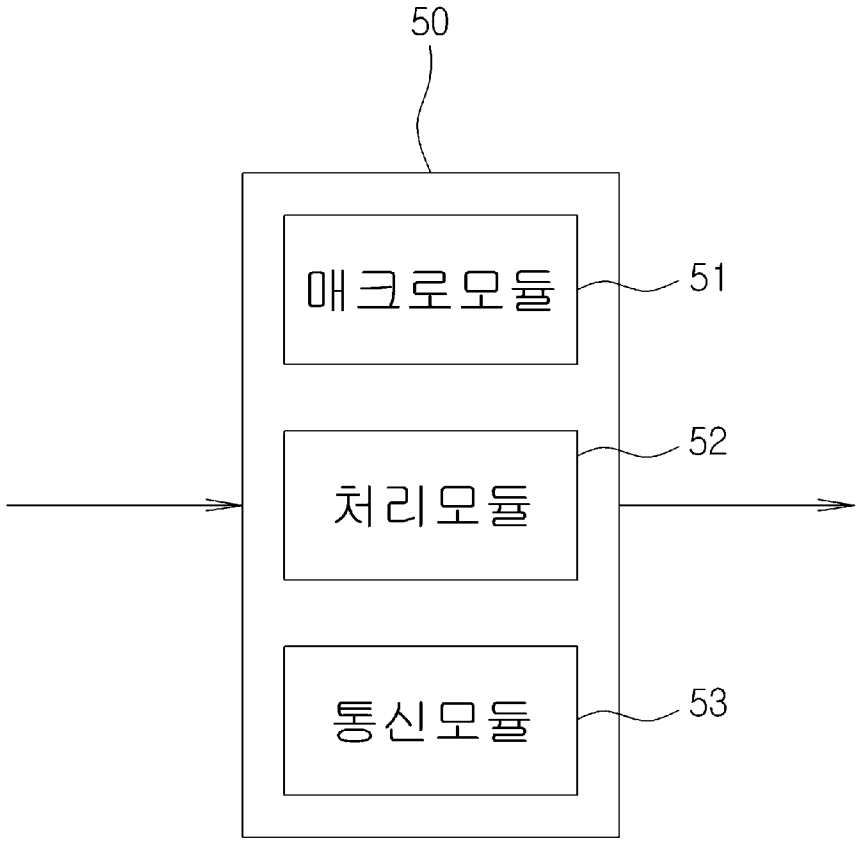
[청구항 4] 제 2 항에 있어서,
상기 제3단계 이전에, 상기 검역서버는 상기 전자메일 본문의 스크립트 동작이 정지되도록, 상기 본문을 텍스트화하는 것을 특징으로 하는 전자문서 검역방법.

[청구항 5] 제 1 항 또는 제 2 항에 있어서,
상기 제2단계와 제3단계 사이에서, 상기 전자문서의 아이콘이미지에 인증마크를 삽입하는 단계를 더 포함하는 것을 특징으로 하는 전자문서 검역방법.

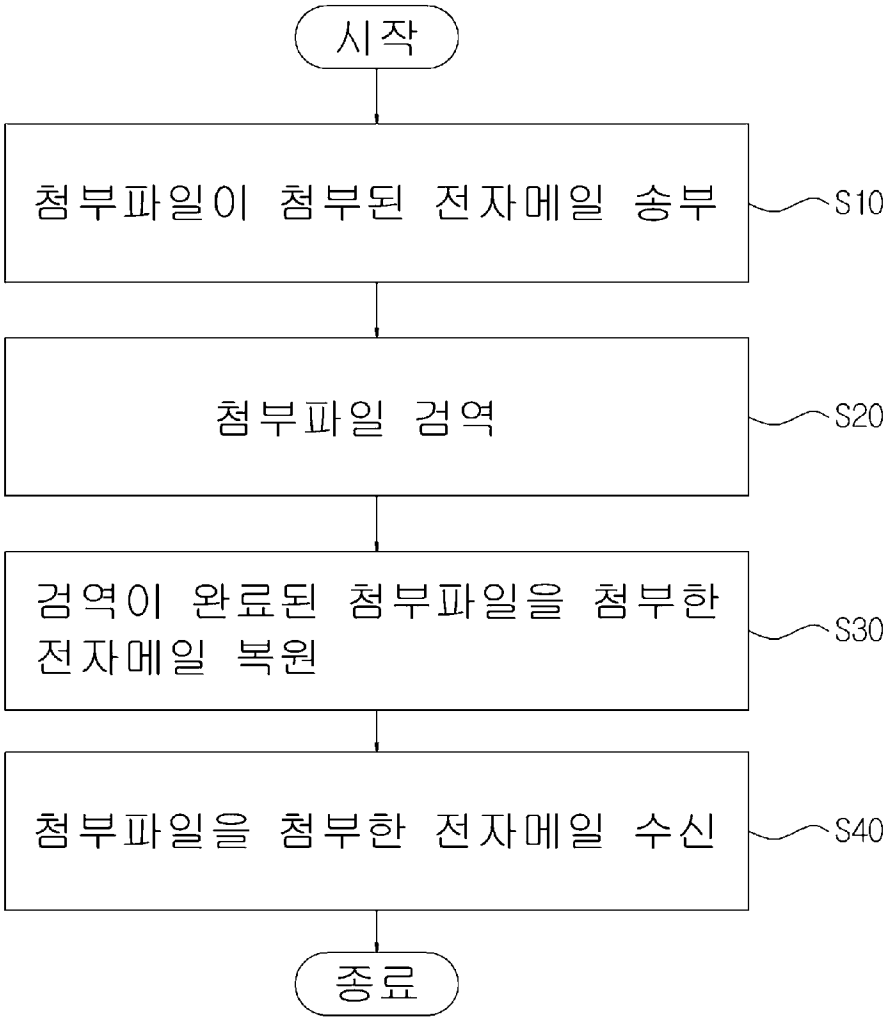
[Fig. 1]



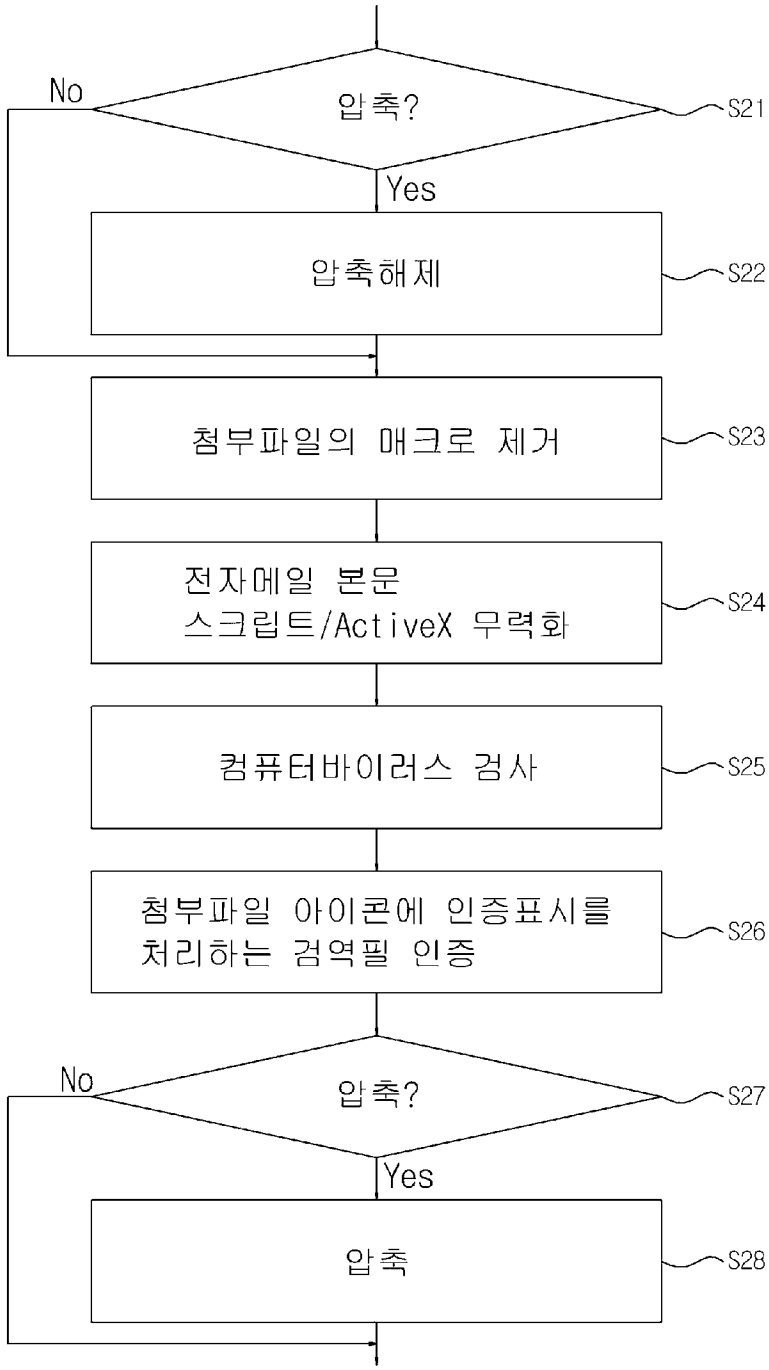
[Fig. 2]



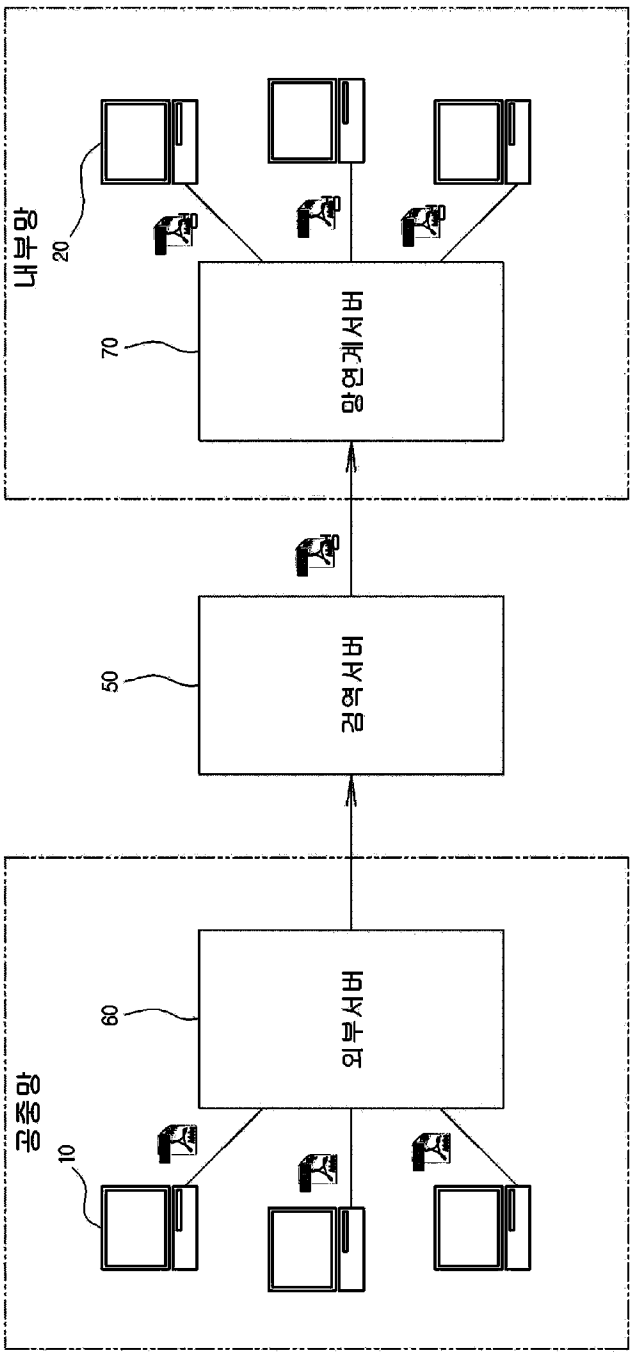
[Fig. 3]


시작
첨부파일이 첨부된 전자메일 송부
S10
첨부파일 검역
S20
검역이 완료된 첨부파일을 첨부한 전자메일 복원
S30
첨부파일을 첨부한 전자메일 수신
S40
종료

[Fig. 4]


No
압축?
S21
Yes
압축해제
S22
첨부파일의 매크로 제거
S23
전자메일 본문
스크립트/ActiveX 무력화
S24
컴퓨터바이러스 검사
S25
첨부파일 아이콘에 인증표시를
처리하는 검역필 인증
S26
No
압축?
S27
Yes
압축
S28

[Fig. 5]



INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR2014/002741

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/00(2006.01)i, G06F 21/50(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F 21/00; G06F 15/16; G06F 11/30; G06F 15/00; G06F 12/14; G06F 1/00; H04L 9/00; G06F 11/00; G06F 21/50

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean Utility models and applications for Utility models: IPC as above
Japanese Utility models and applications for Utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & Keywords: server, attachment, macro, removal, transmission

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	EP 1237065 A2 (CHEYENNE SOFTWARE INTERNATIONAL SALES CORP.) 04 September 2002 See claim 1; paragraphs [0049]-[0051]; and figure 3.	1-2 3-5
Y	US 7506155 B1 (STEWART, Walter Mason et al.) 17 March 2009 See claim 1; column 3, lines 53-54; and column 4, lines 36-39.	3-5
A	US 6697950 B1 (KO, Cheuk W.) 24 February 2004 See claim 1; column 5, lines 50-67; and figure 3.	1-5
A	US 7409425 B2 (NAICK, Indran et al.) 05 August 2008 See claim 1; column 9, line 48 - column 11, line 39; and figure 4.	1-5
A	WO 2010-090435 A2 (AHNLAB., INC.) 12 August 2010 See claim 1; paragraphs [0056]-[0059]; and figure 4.	1-5

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
24 JULY 2014 (24.07.2014)	**31 JULY 2014 (31.07.2014)**
Name and mailing address of the ISA/KR Korean Intellectual Property Office Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/KR2014/002741

Patent document cited in search report	Publication date	Patent family member	Publication date
EP 1237065 A2	04/09/2002	AT 241169 T	15/06/2003
		AU 4253597 A	26/03/1998
		AU 735236 B2	05/07/2001
		BR 9711990 A	13/10/1999
		CA 2264816 A1	12/03/1998
		CA 2264816 C	15/11/2005
		CN 1160616 C	04/08/2004
		CN 1236451 A	24/11/1999
		DE 69722266 D1	26/06/2003
		DE 69722266 T2	08/04/2004
		EP 1010059 A2	21/06/2000
		EP 1010059 B1	21/05/2003
		EP 1237065 A3	15/03/2006
		ES 2199372 T3	16/02/2004
		HK 1023826 A1	29/04/2005
		JP 2001-500295 A	09/01/2001
		KR 10-0554903 B1	24/02/2006
		RU 2221269 C2	10/01/2004
		US 05832208 A	03/11/1998
		WO 98-10342 A2	12/03/1998
		WO 98-10342 A3	14/05/1998
		ZA 9707970 A	23/03/1998
US 7506155 B1	17/03/2009	US 2009-0165138 A1	25/06/2009
		US 2011-0231669 A1	22/09/2011
		US 6901519 B1	31/05/2005
		US 7913078 B1	22/03/2011
		US 7979691 B2	12/07/2011
US 6697950 B1	24/02/2004	NONE	
US 7409425 B2	05/08/2008	US 2005-0108335 A1	19/05/2005
		US 2008-0189379 A1	07/08/2008
		US 7840642 B2	23/11/2010
WO 2010-090435 A2	12/08/2010	KR 10-0985074 B1	04/10/2010
		KR 10-2010-0089968 A	13/08/2010
		US 2011-0296526 A1	01/12/2011
		WO 2010-090435 A3	14/10/2010

국 제 조 사 보 고 서

국제출원번호
PCT/KR2014/002741

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06F 21/00(2006.01)i, G06F 21/50(2013.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

G06F 21/00; G06F 15/16; G06F 11/30; G06F 15/00; G06F 12/14; G06F 1/00; H04L 9/00; G06F 11/00; G06F 21/50

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC
일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드: 서버, 첨부파일, 매크로, 제거, 전송

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
X	EP 1237065 A2 (CHEYENNE SOFTWARE INTERNATIONAL SALES CORP.) 2002.09.04 청구항 1; 단락 [0049]-[0051]; 및 도면 3 참조.	1-2
Y		3-5
Y	US 7506155 B1 (WALTER MASON STEWART 외 2명) 2009.03.17 청구항 1; 컬럼 3, 라인 53-54; 및 컬럼 4, 라인 36-39 참조.	3-5
A	US 6697950 B1 (CHEUK W. KO) 2004.02.24 청구항 1; 컬럼 5, 라인 50-67; 및 도면 3 참조.	1-5
A	US 7409425 B2 (INDRAN NAICK 외 1명) 2008.08.05 청구항 1; 컬럼 9, 라인 48 - 컬럼 11, 라인 39; 및 도면 4 참조.	1-5
A	WO 2010-090435 A2 (AHNLAB., INC.) 2010.08.12 청구항 1; 단락 [0056]-[0059]; 및 도면 4 참조.	1-5

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

"A" 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

"E" 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

"L" 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

"O" 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

"P" 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

"T" 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

"X" 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

"Y" 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

"&" 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일	국제조사보고서 발송일
2014년 07월 24일 (24.07.2014)	2014년 07월 31일 (31.07.2014)

ISA/KR의 명칭 및 우편주소
대한민국 특허청
(302-701) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사)
팩스 번호 +82-42-472-7140

심사관
안정환
전화번호 +82-42-481-8440

국제조사보고서
대응특허에 관한 정보

국제출원번호
PCT/KR2014/002741

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
EP 1237065 A2	2002/09/04	AT 241169 T	2003/06/15
		AU 4253597 A	1998/03/26
		AU 735236 B2	2001/07/05
		BR 9711990 A	1999/10/13
		CA 2264816 A1	1998/03/12
		CA 2264816 C	2005/11/15
		CN 1160616 C	2004/08/04
		CN 1236451 A	1999/11/24
		DE 69722266 D1	2003/06/26
		DE 69722266 T2	2004/04/08
		EP 1010059 A2	2000/06/21
		EP 1010059 B1	2003/05/21
		EP 1237065 A3	2006/03/15
		ES 2199372 T3	2004/02/16
		HK 1023826 A1	2005/04/29
		JP 2001-500295 A	2001/01/09
		KR 10-0554903 B1	2006/02/24
		RU 2221269 C2	2004/01/10
		US 05832208 A	1998/11/03
		WO 98-10342 A2	1998/03/12
		WO 98-10342 A3	1998/05/14
		ZA 9707970 A	1998/03/23
US 7506155 B1	2009/03/17	US 2009-0165138 A1	2009/06/25
		US 2011-0231669 A1	2011/09/22
		US 6901519 B1	2005/05/31
		US 7913078 B1	2011/03/22
		US 7979691 B2	2011/07/12
US 6697950 B1	2004/02/24	없음	
US 7409425 B2	2008/08/05	US 2005-0108335 A1	2005/05/19
		US 2008-0189379 A1	2008/08/07
		US 7840642 B2	2010/11/23
WO 2010-090435 A2	2010/08/12	KR 10-0985074 B1	2010/10/04
		KR 10-2010-0089968 A	2010/08/13
		US 2011-0296526 A1	2011/12/01
		WO 2010-090435 A3	2010/10/14