(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2011 년 10 월 13 일 (13.10.2011)

PCT

(10) 국제공개번호
WO 2011/126254 A2

(51) 국제특허분류:
G06F 21/20 (2006.01) *G06F 17/00* (2006.01)
G06F 9/06 (2006.01) *G06F 15/00* (2006.01)

(21) 국제출원번호: PCT/KR2011/002339

(22) 국제출원일: 2011 년 4 월 5 일 (05.04.2011)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2010-0030939 2010 년 4 월 5 일 (05.04.2010) KR

(71) 출원인 (US 을(를) 제외한 모든 지정국에 대하여): **주식회사 안철수연구소 (AHNLAB, INC.)** [KR/KR]; 서울특별시 영등포구 여의도동 12 씨씨엠엠빌딩 6 층, 150-869 Seoul (KR).

(72) 발명자; 겸
(75) 발명자/출원인 (US 에 한하여): **황용석 (HWANG, Yong Seok)** [KR/KR]; 서울특별시 강동구 고덕동 217 번지 주공아파트 219 동 303 호, 134-757 Seoul (KR).

김정훈 (KIM, Jeong Hun) [KR/KR]; 서울특별시 마포구 도화동 376 도화현대아파트 102 동 807 호, 121-771 Seoul (KR). **김성현 (KIM, Sung Hyun)** [KR/KR]; 서울특별시 서대문구 북가좌동 459 두산위브 104-603, 120-130 Seoul (KR). **강경완 (KANG, Kyung Wan)** [KR/KR]; 서울특별시 종로구 숭인동 동부 센트레빌 105 동 104 호, 110-550 Seoul (KR).

(74) 대리인: **김문재 (KIM, Moon-Jae)**; 서울특별시 중구 서소문동 41-3 대한항공빌딩 3 층, 100-813 Seoul (KR).

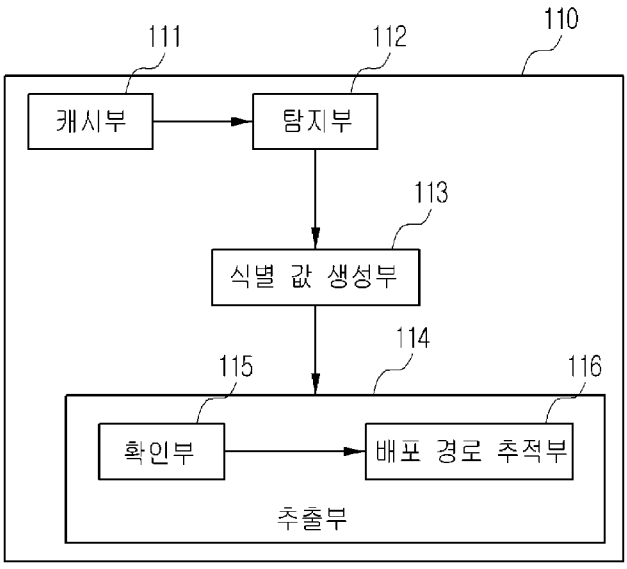
(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG,

[다음 쪽 계속]

(54) Title: TERMINAL DEVICE AND METHOD FOR CONFIRMING FILE DISTRIBUTOR OF SAME TERMINAL DEVICE

(54) 발명의 명칭 : 단말 장치 및 상기 단말 장치의 파일 배포처 확인 방법

[Fig. 1]



111 ... Cache unit
112 ... Search unit
113 ... Identification value generation unit
114 ... Extraction unit
115 ... Confirmation unit
116 ... Distribution path tracing unit

(57) **Abstract**: Disclosed are a terminal device and a method for confirming a file distributor of same terminal device. The present invention according to embodiments caches the files pre-executed through the terminal device and file distributor information and can previously prevent diffusion of malicious codes by comparing the cached files with a new file and extracting the distributor information of the new file when the new file is generated from the terminal device.

(57) **요약서**: 단말 장치 및 상기 단말 장치의 파일 배포처 확인 방법이 개시된다. 본 발명의 실시예들은 단말 장치에서 기 실행(pre-executed)되었던 파일들과 상기 파일들의 배포처 정보를 캐시(cache)해 두고, 상기 단말 장치에 신규 파일이 생성되는 경우, 상기 캐시되어 있는 파일들과 상기 신규 파일을 비교하여 상기 신규 파일의 배포처 정보를 추출함으로써, 악성 코드의 확산을 사전에 방지할 수 있다.

WO 2011/126254 A2

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, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, MD, 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, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서 없이 공개하며 보고서 접수 후 이를 별도 공개함 (규칙 48.2(g))

명세서

발명의 명칭: 단말 장치 및 상기 단말 장치의 파일 배포처 확인 방법

기술분야

[1] 본 발명의 실시예들은 악성코드의 확산을 사전에 방지하기 위해 사용자 단말기로 전달되는 파일의 배포처와 배포 경로를 확인하는 기술과 관련된다.

배경기술

[2] 최근, 초고속 인터넷 환경이 구축되면서, 프로그램이나 이-메일(e-mail) 등을 통해 유포되는 악성코드로 인한 피해가 급증하고 있다.

[3] 보통, 악성코드는 컴퓨터의 속도 저하시킬 수 있고, 웹 브라우저의 초기 페이지를 불건전 사이트로 고정할 수 있으며, 사용자의 컴퓨터를 스팸 메일 발송 서버로 사용하거나 DDoS(Distributed Denial of Service Attack) 공격의 거점 PC로 사용할 수 있고, 사용자의 개인 정보를 유출시킬 수 있다.

[4] 악성코드가 사용자의 컴퓨터에 설치되고 해를 입히는 방식은 ActiveX, Java Applet, Java WebStart, .NETClickOnce, Flash, UCC 등 다양하게 존재하나, 모두 외부로부터 파일을 다운로드 받는다는 점에서 동일하다..

[5] 최근에는 이러한 악성코드의 유포를 방지하기 위해 다양한 방어기제에 대한 연구가 진행되고 있다.

[6] 먼저, 악성코드 방지를 위한 설치형 프로그램은 각 개인 컴퓨터에 설치되는 프로그램으로 사전 제작하여 배포된 악성코드 시그니처 데이터베이스를 기반으로 악성코드나 바이러스 및 음란물의 실행을 감지하고, 이미 감염된 컴퓨터를 치료하는 형태로 작동되며, 일반적인 백신 프로그램이 이러한 방식에 해당한다.

[7] 또한, 악성코드를 방지하기 위한 방법으로 네트워크 앞단에 설치된 방화벽에서 불건전 사이트로 분류된 URL DB를 바탕으로 트래픽을 차단하는 방식이 있으며, URL을 수집하는 방식에 대해서는 여러가지 기법들이 존재한다.

[8] 전술한 바와 같이 악성코드를 방지하기 위한 여러가지 기법들이 존재하나 보통, 악성코드는 사용자의 부주의로 컴퓨터에 설치되는 경우가 많아서 악성코드의 설치를 사전에 방지할 수 있는 방어기법과 악성코드의 조기탐지 및 대응을 위한 악성코드의 배포처 추적에 대한 연구가 필요하다.

발명의 상세한 설명

기술적 과제

[9] 본 발명의 실시예들은 웹(Web) 등을 통해 사용자의 단말 장치로 전달되는 파일의 배포처와 배포 경로를 추적할 수 있는 기법을 제공함으로써, 악성코드의 확산을 원천적으로 차단할 수 있는 기틀을 마련하고자 한다.

과제 해결 수단

[10] 본 발명의 일실시예에 따른 단말 장치는 상기 단말 장치에서 기

실행된(pre-executed) 적어도 하나의 파일에 대한 식별 값과 상기 적어도 하나의 파일에 대한 배포처 정보가 저장된 캐시(cache)부, 상기 단말 장치에 신규 파일이 생성되는지 여부를 탐지하는 탐지부, 상기 신규 파일이 생성되었음이 탐지되는 경우, 상기 신규 파일의 식별 값을 생성하는 식별 값 생성부 및 상기 캐시부로부터 상기 신규 파일의 식별 값과 동일한 식별 값을 갖는 파일에 대한 배포처 정보를 추출하는 추출부를 포함한다.

[11] 또한, 본 발명의 일실시예에 따른 단말 장치의 파일 배포처 확인 방법은 상기 단말 장치에서 기 실행된(pre-executed) 적어도 하나의 파일에 대한 식별 값과 상기 적어도 하나의 파일에 대한 배포처 정보가 저장된 데이터베이스를 관리하는 단계, 상기 단말 장치에 신규 파일이 생성되는지 여부를 탐지하는 단계, 상기 신규 파일이 생성되었음이 탐지되는 경우, 상기 신규 파일의 식별 값을 생성하는 단계 및 상기 데이터베이스로부터 상기 신규 파일의 식별 값과 동일한 식별 값을 갖는 파일에 대한 배포처 정보를 추출하는 단계를 포함한다.

발명의 효과

[12] 본 발명의 실시예들은 단말 장치에서 기 실행(pre-executed)되었던 파일들과 상기 파일들의 배포처 정보를 캐시(cache)해 두고, 상기 단말 장치에 신규 파일이 생성되는 경우, 상기 캐시되어 있는 파일들과 상기 신규 파일을 비교하여 상기 신규 파일의 배포처 정보를 추출함으로써, 악성코드의 분석을 돕고, 악성 코드의 확산을 사전에 방지할 수 있다.

도면의 간단한 설명

[13] 도 1은 본 발명의 일실시예에 따른 단말 장치의 구조를 도시한 도면이다.

[14] 도 2는 본 발명의 일실시예에 따른 단말 장치가 파일의 배포 경로를 추적하는 방법을 설명하기 위한 도면이다.

[15] 도 3은 본 발명의 일실시예에 따른 단말 장치의 파일 배포처 확인 방법을 도시한 순서도이다.

[16] 도 4는 본 발명의 일실시예에 따른 단말 장치의 파일 배포 경로 추적 과정을 도시한 순서도이다.

발명의 실시를 위한 최선의 형태

[17] 이하에서, 첨부된 도면을 참조하여 본 발명에 따른 실시예들을 상세히 설명한다. 그러나, 본 발명이 실시예들에 의해 제한되거나 한정되는 것은 아니다. 또한, 각 도면에 제시된 동일한 참조 부호는 동일한 부재를 나타낸다.

[18] 전술한 바와 같이, 악성코드로 인한 피해가 급증하고 있는 상황에서 악성코드의 확산을 초기에 차단하기 위해서는 악성코드를 배포한 배포처를 확인하는 과정이 필요하다.

[19] 악성코드의 배포처를 알 수 있다면, 상기 배포처로부터 전달되는 파일의 실행을 원천적으로 차단함으로써, 악성코드의 확산을 방지할 수 있기 때문이다.

[20] 즉, 사용자의 단말 장치로 전달된 파일의 배포처가 신뢰할 수 있는

URL(Uniform Resource Locator)이거나 상기 파일이 전자서명이 되어 있는 cab 파일 또는 exe 파일로부터 추출된 파일인 경우, 상기 파일은 신뢰할 수 있는 파일로 판단할 수 있고, 반대로 상기 파일의 배포처가 악성코드를 유포하는 배포처인 경우, 상기 파일의 실행을 차단함으로써, 단말 장치에 악성코드가 설치되는 것을 원천적으로 방지할 수 있다.

[21] 여기서, 파일의 배포처란 URL을 포함하는 네트워크 경로, 기록매체, 압축파일, 다른 프로세스 등 파일이 유래한 곳(예를 들면 URL)이나 단말기에 파일이 생성될 때까지의 경로상에 존재하는 어떤 것(예를 들면 파일을 생성한 프로세스)을 지칭한다.

[22] 또한, 최근의 악성코드는 취약점을 공격하는 코드와 다운로더 및 본체 등 다수의 모듈로 구성되는 경우가 많기 때문에 이러한 악성코드의 배포경로를 알아내는 것 또한 중요하다.

[23] 따라서, 본 발명의 실시예들은 웹(Web) 등을 통해 사용자의 단말 장치로 전달되는 파일의 배포처와 배포 경로를 추적할 수 있는 기법을 제공함으로써, 악성코드의 확산을 원천적으로 차단할 수 있는 기틀을 마련하고자 한다.

[24] 먼저, 도 1을 참조하여 본 발명의 일실시예에 따른 단말 장치를 설명하기로 한다.

[25] 도 1은 본 발명의 일실시예에 따른 단말 장치의 구조를 도시한 도면이다.

[26] 도 1을 참조하면, 단말 장치(110)는 캐시(cache)부(111), 탐지부(112), 식별 값 생성부(113) 및 추출부(114)를 포함한다.

[27] 여기서, 단말 장치(110)는 퍼스널 컴퓨터, 서버, MP3 플레이어, PMP, 네비게이션 단말기, 모바일 단말기, PDA 등 마이크로 프로세서 기반의 장치를 통칭하는 개념이다.

[28] 캐시부(111)에는 단말 장치(110)에서 기 실행된(pre-executed) 적어도 하나의 파일에 대한 식별 값과 상기 적어도 하나의 파일에 대한 배포처 정보가 저장되어 있다.

[29] 이때, 상기 적어도 하나의 파일에 대한 식별 값은 상기 적어도 하나의 파일의 해시(hash) 값이거나 상기 적어도 하나의 파일의 일부 또는 전부가 될 수 있다.

[30] 또한, 캐시부(111)는 파일의 역추적에 필요한 경로정보 등도 포함할 수 있다.

[31] 탐지부(112)는 단말 장치(110)에 신규 파일이 생성되는지 여부를 탐지한다.

[32] 식별 값 생성부(113)는 상기 신규 파일이 생성되었음이 탐지되는 경우, 상기 신규 파일의 식별 값을 생성한다.

[33] 이때, 상기 신규 파일의 식별 값은 상기 신규 파일의 해시 값이거나 상기 신규 파일의 일부 또는 전부가 될 수 있다.

[34] 추출부(114)는 캐시부(111)로부터 상기 신규 파일의 식별 값과 동일한 식별 값을 갖는 파일에 대한 배포처 정보를 추출한다.

[35] 즉, 본 발명의 일실시예에 따른 단말 장치(110)는 이전에 실행되었었던 파일들의 식별 값과 상기 파일들의 배포처 정보를 캐시한 후 단말 장치(110)가 웹

등을 통해 신규 파일을 전송받은 경우, 상기 신규 파일의 식별 값과 이전에 캐시해 둔 파일들의 식별 값을 비교하여 상기 신규 파일의 식별 값과 동일한 식별 값을 갖는 파일에 대한 배포처 정보를 추출함으로써, 사용자가 상기 신규 파일의 배포처를 확인할 수 있도록 할 수 있다.

[36] 보통, 단말 장치(110)에 전달되는 파일의 배포처는 웹, 기록매체, 압축파일 또는 소정의 프로세스 등이 될 수 있다.

[37] 따라서, 이하에서는 파일의 배포처 종류에 따른 단말 장치(110)의 상세한 동작에 대해 설명하기로 한다.

[38]

[39] 웹을 통해 파일이 배포되는 경우의 실시예

[40] 먼저, 탐지부(112)는 네트워크 필터를 통해 단말 장치(110)로 수신되는 패킷(packet)을 조사하여 단말 장치(110)의 네트워크 연결이 HTTP 등 식별할 수 있는 연결인지 여부를 확인한다.

[41] 만약, 상기 네트워크 연결이 식별할 수 있는 연결인 경우, 캐시부(111)는 프로토콜에서 호스트(Host) 등의 정보를 캐시한다.

[42] 이때, 탐지부(112)가 단말 장치(110)로 수신되는 모든 패킷을 조사하면 그 성능이 떨어질 수 있으므로, 탐지부(112)는 단말 장치(110)가 네트워크와 연결된 이후 수신한 일부 패킷만을 조사할 수도 있다.

[43] 이때, 탐지부(112)는 상기 프로토콜이 HTTP1.1과 같이 지속적인 연결을 지원하는 프로토콜인 경우, 기존의 연결 상에서 신규 트랜젝션(transaction)이 시작되는 패킷을 감지하여야 한다.

[44] 만약, 단말 장치(110)가 패킷을 수신할 때, 프로토콜이 HTTP 등과 같이 파싱(parsing)가능한 프로토콜인 경우, 탐지부(112)는 상기 프로토콜을 파싱하여 파일이 포함되어 있는지 여부를 확인할 수 있다.

[45] 이때, 상기 프로토콜이 HTTP인 경우, 탐지부(112)는 헤더(header)의 컨텐츠 타입과 바디(body)의 데이터를 확인하여 파일의 포함여부 및 상기 파일의 유형을 파악할 수 있다.

[46] 하지만, 상기 프로토콜이 알 수 없는 프로토콜인 경우, 탐지부(112)는 수신되는 일부 패킷을 조사하여 알려진 파일 포맷이 있는지 여부를 확인할 수 있다.

[47] 이때, 탐지부(112)는 RAW 포맷의 실행파일이나 ZIP과 같은 압축포맷을 발견할 수 있다. 이때, 탐지부(112)가 발견한 파일이 압축포맷이거나 기타 다른 식별 가능한 포맷인 경우, 탐지부(112)는 이를 처리하여 내부의 파일을 탐지할 수 있다

[48] 탐지부(112)가 수신되는 패킷을 기초로 파일의 확인을 끝마치면, 식별 값 생성부(113)가 파일 헤더와 같은 파일의 일부 또는 파일 전체를 생성하고, 캐시부(111)는 상기 파일의 일부 또는 파일 전체를 캐시한다.

[49] 이때, 식별 값 생성부(113)가 파일의 해시 값을 생성하고, 캐시부(111)는 상기 해시 값을 캐시할 수도 있다.

[50] 또한, 캐시부(111)는 파일을 캐시함과 동시에 파일을 배포한 배포처의 URL, IP

(Internet Protocol) 주소 또는 Port 번호 등과 같은 네트워크 정보를 캐시한다.

[51] 즉, 탐지부(112)가 단말 장치(110)로 수신되는 패킷을 기초로 웹을 통해 배포되는 파일들 및 상기 파일들을 배포한 배포처의 네트워크 정보를 추출하고, 식별 값 생성부(113)가 상기 추출된 파일들의 식별 값을 생성하면, 캐시부(111)는 상기 식별 값과 네트워크 정보를 캐시할 수 있다.

[52] 이렇게 캐시부(111)가 단말 장치(110)에 전달되었던 파일들의 식별 값 및 상기 파일들을 배포한 배포처의 네트워크 정보를 캐시한 이후 단말 장치(110)에 신규 파일이 생성되면, 탐지부(112)가 상기 신규 파일의 생성여부를 탐지한다.

[53] 만약, 캐시부(111)에 파일의 일부 또는 파일의 전체가 저장되어 있는 경우, 추출부(114)는 캐시부(111)에 상기 신규 파일과 동일한 파일이 있는지 여부를 확인하고, 동일한 파일이 있는 경우, 캐시부(111)로부터 상기 동일한 파일을 배포한 배포처의 URL 정보 등과 같은 네트워크 정보를 추출할 수 있다.

[54] 또한, 캐시부(111)에 파일의 해시 값이 저장되어 있는 경우, 식별 값 생성부(113)가 상기 신규 파일의 해시 값을 생성하고, 추출부(114)는 캐시부(111)로부터 상기 신규 파일의 해시 값과 동일한 해시 값을 갖는 파일을 배포한 배포처의 네트워크 정보를 추출할 수 있다.

[55]

[56] <u>기록매체로부터 파일이 배포되는 경우의 실시예</u>

[57] 먼저, 탐지부(112)는 파일 필터를 통해 CD-ROM이나 USB 메모리 등과 같은 기록매체로부터 파일이 독출(read out)되는지 여부를 탐지하고, 파일이 상기 기록매체로부터 독출되는 경우, 상기 기록매체의 유형 정보 또는 파일 경로 등을 확인한다.

[58] 식별 값 생성부(113)는 상기 독출된 파일의 식별 값을 생성하고, 캐시부(111)는 상기 식별 값과 상기 기록매체의 유형 정보 또는 상기 파일 경로 등을 캐시한다.

[59] 이렇게 캐시부(111)가 단말 장치(110)에 전달되었던 파일들의 식별 값 및 상기 파일들을 배포한 기록매체 유형 정보를 캐시한 이후 단말 장치(110)에 신규 파일이 생성되면, 탐지부(112)가 상기 신규 파일의 생성여부를 탐지한다.

[60] 그리고 나서, 식별 값 생성부(113)는 상기 신규 파일의 식별 값을 생성한다.

[61] 마지막으로 추출부(114)는 캐시부(111)에 저장되어 있는 파일들의 식별 값과 상기 신규 파일의 식별 값을 비교하여 캐시부(111)에 상기 신규 파일의 식별 값과 동일한 식별 값을 갖는 파일이 존재하는 경우, 캐시부(111)로부터 상기 동일한 식별 값을 갖는 파일을 배포한 기록매체 유형 정보를 추출한다.

[62]

[63] <u>압축파일로부터 파일이 배포되는 경우의 실시예</u>

[64] 먼저, 탐지부(112)는 파일 필터를 통해 압축파일로부터 데이터가 읽어 들여지고 있는 것을 탐지한다.

[65] 이때, 상기 파일이 순차적으로 독출되거나 유사하게 독출되는 경우, 탐지부(112)는 상기 압축파일 또는 상기 독출된 파일을 다시 읽어서 압축을

해제할 수 있다.

[66] 그리고 나서, 탐지부(112)는 압축이 해제될 때, 상기 압축파일의 정보를 확인한다.

[67] 식별 값 생성부(113)는 압축이 해제되면서 발견된 파일들의 식별 값을 생성하고, 캐시부(111)는 상기 식별 값과 상기 압축파일의 정보를 캐시한다.

[68] 이렇게 캐시부(111)가 단말 장치(110)에 전달되었던 파일들의 식별 값 및 상기 파일들을 배포한 압축파일 정보를 캐시한 이후 단말 장치(110)에 신규 파일이 생성되면, 탐지부(112)가 상기 신규 파일의 생성여부를 탐지한다.

[69] 그리고 나서, 식별 값 생성부(113)는 상기 신규 파일의 식별 값을 생성한다.

[70] 마지막으로 추출부(114)는 캐시부(111)에 저장되어 있는 파일들의 식별 값과 상기 신규 파일의 식별 값을 비교하여 캐시부(111)에 상기 신규 파일의 식별 값과 동일한 식별 값을 갖는 파일이 존재하는 경우, 캐시부(111)로부터 상기 동일한 식별 값을 갖는 파일이 담겨있는 압축파일 정보를 추출한다.

[71]

[72] 소정의 프로세스가 파일을 생성하는 경우의 실시예

[73] 먼저, 소정의 프로세스가 파일을 생성하는 경우라 함은 setup.exe 등과 같은 설치본 파일로부터 파일이 생성되거나 기타 다른 파일로부터 파일이 생성되는 경우를 의미한다.

[74] 탐지부(112)는 소정의 프로세스로부터 파일이 생성되는지 여부를 탐지하고, 상기 프로세스로부터 파일이 생성되는 경우, 상기 프로세스의 정보를 확인한다.

[75] 식별 값 생성부(113)는 상기 생성된 파일의 식별 값을 생성하고, 캐시부(111)는 상기 생성된 식별 값과 상기 파일을 배포한 프로세스의 정보를 캐시한다.

[76] 이렇게 캐시부(111)가 단말 장치(110)에 전달되었던 파일들의 식별 값 및 상기 파일들을 배포한 프로세스의 정보를 캐시한 이후 단말 장치(110)에 신규 파일이 생성되면, 탐지부(112)가 상기 신규 파일의 생성여부를 탐지한다.

[77] 그리고 나서, 식별 값 생성부(113)는 상기 신규 파일의 식별 값을 생성한다.

[78] 마지막으로 추출부(114)는 캐시부(111)에 저장되어 있는 파일들의 식별 값과 상기 신규 파일의 식별 값을 비교하여 캐시부(111)에 상기 신규 파일의 식별 값과 동일한 식별 값을 갖는 파일이 존재하는 경우, 캐시부(111)로부터 상기 동일한 식별 값을 갖는 파일을 배포한 프로세스 정보를 추출한다.

[79] 또한, 본 발명의 일실시예에 따르면, 설치본 파일 등과 같이 소정의 프로세스로부터 파일이 생성되는 경우에는 설치본 파일로부터 파일을 생성하는 프로세스의 이미지 파일을 확인함으로써, 상기 신규 파일의 배포처를 확인할 수도 있다.

[80] 이때, 파일명에 "setup"나 "install" 등이 포함되어 있으면 설치본으로 간주할 수 있다.

[81] 또한, 인스톨쉴드(installshield) 등 널리 사용되는 설치본 생성 프로그램의 특성을 확인하여 설치본으로 간주할 수 있다.

[82] 지금까지 파일의 배포처 종류에 따른 단말 장치(110)의 동작을 상세히 설명하였다.

[83] 여기서, 전술한 실시예들은 설명의 편의를 위해 각각 별개로 설명되어 있을 뿐 상기 실시예들이 단말 장치(110)에 각각 별개로 적용되어야 함을 의미하지는 않는다.

[84] 즉, 전술한 실시예들이 하나의 단말 장치(110)에 동시에 적용될 수 있음은 당업자에게 자명한 일이다.

[85]

[86] 본 발명의 일실시예에 따르면, 단말 장치(110)는 앞서 설명한 방식을 이용하여 확인한 신규 파일의 배포처를 기초로 상기 신규 파일의 배포 경로를 추적할 수 있다.

[87] 이와 관련하여, 추출부(114)는 확인부(115) 및 배포 경로 추적부(116)를 포함할 수 있다.

[88] 확인부(115)는 추출부(114)에서 추출된 신규 파일의 배포처 정보를 기초로 상기 신규 파일이 다른 파일로부터 배포된 파일인지 여부를 확인한다.

[89] 이때, 상기 신규 파일이 다른 파일로부터 배포된 파일인 경우, 배포 경로 추적부(116)는 상기 다른 파일의 식별 값을 기초로 캐시부(111)로부터 상기 다른 파일에 대한 배포처 정보를 추출하여 상기 신규 파일의 배포 경로를 추적한다.

[90] 이하에서는 도 2를 참조하여 단말 장치(110)가 파일의 배포 경로를 추적하는 과정을 상세히 설명하기로 한다.

[91] 도 2는 본 발명의 일실시예에 따른 단말 장치가 파일의 배포 경로를 추적하는 방법을 설명하기 위한 도면이다.

[92] 여기서, 파일의 식별 값은 파일의 해시 값으로 가정한다.

[93] 먼저, 단말 장치(110)에 배포된 신규 파일이 도면부호 230에 도시된 "c.exe"라고 가정한다.

[94] 탐지부(112)가 "c.exe"의 생성을 탐지하면, 식별 값 생성부(113)는 "c.exe"의 해시 값 "0013"을 생성한다.

[95] 그리고 나서, 추출부(114)는 캐시부(111)로부터 "c.exe"의 해시 값 "0013"와 동일한 해시 값을 갖는 파일의 배포처 정보를 추출한다.

[96] 도면부호 230에서는 "c.exe"의 해시 값 "0013"와 동일한 해시 값을 갖는 파일의 배포처로 "setup.exe"가 도시되어 있으므로, 추출부(114)는 캐시부(111)로부터 "setup.exe"를 추출한다.

[97] 추출부(114)가 "setup.exe"를 추출하였으면, 확인부(115)는 "c.exe"가 다른 파일로부터 배포된 파일인지 여부를 확인한다.

[98] "setup.exe"는 파일에 해당하므로, 확인부(115)는 "c.exe"가 다른 파일로부터 배포된 파일인 것으로 확인하고, 배포 경로 추적부(116)는 "setup.exe"의 해시 값 "000c"를 기초로 캐시부(111)로부터 "setup.exe"의 배포처 정보를 추출한다.

[99] 도면부호 220에는 "setup.exe"의 배포처로 "abcd.cab"이 도시되어 있으므로,

배포 경로 추적부(116)는 캐시부(111)로부터 "abcd.cab"을 추출한다.

[100] 이때, 확인부(115)는 "setup.exe"가 "abcd.cab"으로부터 배포되었음을 확인하고, 배포 경로 추적부(116)가 "abcd.cab"의 해시 값 "0001"을 기초로 캐시부(111)로부터 "abcd.cab"의 배포처 정보를 추출한다.

[101] 도면부호 210에는 "abcd.cab"의 배포처로 "http://www.abcdefg.com/download.asp"가 도시되어 있으므로, 배포 경로 추적부(116)는 캐시부(111)로부터 "http://www.abcdefg.com/download.asp"을 추출한다.

[102] 이때, 확인부(115)는 "abcd.cab"이 다른 파일로부터 배포된 파일이 아님을 확인하고, 배포처 정보 추출 과정을 마친다.

[103] 전술한 과정을 통해 배포 경로 추적부(116)는 "c.exe"의 최초 배포처로 "http://www.abcdefg.com/download.asp"을 추적할 수 있을 뿐만 아니라, 최초 배포처로부터 "abcd.cab"이 배포되고, "abcd.cab"으로부터 "setup.exe"이 배포되었으며, 최종적으로 "setup.exe"로부터 단말 장치(110)에 신규 생성된 파일인 "c.exe"가 배포되었음을 추적할 수 있다.

[104] 즉, 배포 경로 추적부(116)는 파일의 해시 값을 연결고리로 사용하여 신규 파일의 배포처를 추적할 수 있다.

[105] 본 발명의 일실시예에 따르면, 단말 장치(110)는 단말 장치(110)에 생성된 신규 파일이 다양한 배포 경로를 가지는 경우, 해당 경로 중에서 신뢰할 수 있는 배포처가 하나 이상 포함되어 있으면, 상기 신규 파일을 신뢰할 수 있는 파일로 식별할 수 있다.

[106]

[107] 도 3은 본 발명의 일실시예에 따른 단말 장치의 파일 배포처 확인 방법을 도시한 순서도이다.

[108] 단계(S310)에서는 단말 장치에서 기 실행된 적어도 하나의 파일에 대한 식별 값과 상기 적어도 하나의 파일에 대한 배포처 정보가 저장된 데이터베이스를 관리한다.

[109] 단계(S320)에서는 상기 단말 장치에 신규 파일이 생성되는지 여부를 탐지한다.

[110] 만약, 단계(S330)에서 단계(S320)에 대한 판단을 수행한 결과, 상기 신규 파일이 생성되지 않은 것으로 탐지되는 경우, 본 과정을 종료한다.

[111] 하지만, 단계(S330)에서 단계(S320)에 대한 판단을 수행한 결과, 상기 신규 파일이 생성되었음이 탐지되는 경우, 단계(S340)에서 상기 신규 파일의 식별 값을 생성한다.

[112] 단계(S350)에서는 상기 데이터베이스로부터 상기 신규 파일의 식별 값과 동일한 식별 값을 갖는 파일에 대한 배포처 정보를 추출한다.

[113] 본 발명의 일실시예에 따른 단말 장치의 파일 배포처 확인 방법은 단계(S350)이후에 소정의 단계를 더 포함함으로써, 상기 신규 파일의 배포 경로를 추적할 수 있다.

[114] 이와 관련하여, 도 4를 참조하여 상기 신규 파일의 배포 경로를 추적하는 과정을 설명한다.

[115] 도 4는 본 발명의 일실시예에 따른 단말 장치의 파일 배포 경로 추적 과정을 도시한 순서도이다.

[116] 단계(S410)에서는 단계(S350)에서 추출된 배포처 정보를 기초로 상기 신규 파일이 다른 파일로부터 배포된 파일인지 여부를 확인한다.

[117] 만약, 단계(S420)에서 단계(S410)에 대한 판단을 수행한 결과, 상기 신규 파일이 다른 파일로부터 배포된 파일이 아닌 것으로 확인되는 경우, 본 과정을 종료한다.

[118] 하지만, 단계(S420)에서 단계(S410)에 대한 판단을 수행한 결과, 상기 신규 파일이 다른 파일로부터 배포된 파일인 것으로 확인되는 경우, 단계(S430)에서 상기 다른 파일의 식별 값을 기초로 상기 데이터베이스로부터 상기 다른 파일의 배포처 정보를 추출하여 상기 신규 파일의 배포 경로를 추적한다.

[119] 이상, 도 3 및 도 4를 참조하여 본 발명의 일실시예에 따른 단말 장치의 파일 배포처 확인 방법에 대해 설명하였다. 여기서, 본 발명의 일실시예에 따른 단말 장치의 파일 배포처 확인 방법은 도 1 및 도 2를 이용하여 설명한 단말 장치의 구성과 대응될 수 있으므로, 이에 대한 보다 상세한 설명은 생략하기로 한다.

[120] 본 발명의 일실시예에 따른 단말 장치의 파일 배포처 확인 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 본 발명의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.

[121] 이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양한 수정 및 변형이 가능하다.

[122] 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

청구범위

[청구항 1] 단말 장치에 있어서,
상기 단말 장치에서 기 실행된(pre-executed) 적어도 하나의 파일에 대한 식별 값과 상기 적어도 하나의 파일에 대한 배포처 정보가 저장된 캐시(cache)부;
상기 단말 장치에 신규 파일이 생성되는지 여부를 탐지하는 탐지부;
상기 신규 파일이 생성되었음이 탐지되는 경우, 상기 신규 파일의 식별 값을 생성하는 식별 값 생성부; 및
상기 캐시부로부터 상기 신규 파일의 식별 값과 동일한 식별 값을 갖는 파일에 대한 배포처 정보를 추출하는 추출부
를 포함하는 단말 장치.

[청구항 2] 제1항에 있어서,
상기 탐지부는
상기 적어도 하나의 파일이 웹(Web)을 통해 배포되는 경우,
수신되는 패킷을 기초로 상기 적어도 하나의 파일 및 상기 적어도 하나의 파일을 배포한 배포처의 네트워크 정보를 추출하고,
상기 식별 값 생성부는
상기 추출된 적어도 하나의 파일에 대한 식별 값을 생성하며,
상기 캐시부는 상기 적어도 하나의 파일에 대한 식별 값과 상기 네트워크 정보를 캐싱(caching)하는 단말 장치.

[청구항 3] 제1항에 있어서,
상기 탐지부는
상기 적어도 하나의 파일의 배포처가 기록매체인 경우, 상기 적어도 하나의 파일이 상기 기록매체로부터 독출(read out)될 때 상기 기록매체의 유형 정보를 확인하고,
상기 식별 값 생성부는
상기 적어도 하나의 파일에 대한 식별 값을 생성하며,
상기 캐시부는 상기 적어도 하나의 파일에 대한 식별 값과 상기 기록매체의 유형 정보를 캐싱하는 단말 장치.

[청구항 4] 제1항에 있어서,
상기 탐지부는
상기 적어도 하나의 파일의 배포처가 압축파일인 경우, 상기 압축파일의 압축이 해제될 때 상기 압축파일의 정보를 확인하고,
상기 식별 값 생성부는
상기 적어도 하나의 파일에 대한 식별 값을 생성하며,
상기 캐시부는 상기 적어도 하나의 파일에 대한 식별 값과 상기

압축파일의 정보를 캐싱하는 단말 장치.

[청구항 5] 제1항에 있어서,
상기 탐지부는
상기 적어도 하나의 파일이 소정의 프로세스(process)를 통해 생성되는 경우, 상기 적어도 하나의 파일이 상기 프로세스로부터 생성될 때 상기 프로세스의 정보를 확인하고,
상기 식별 값 생성부는
상기 적어도 하나의 파일에 대한 식별 값을 생성하며,
상기 캐시부는 상기 적어도 하나의 파일에 대한 식별 값과 상기 프로세스의 정보를 캐싱하는 단말 장치.

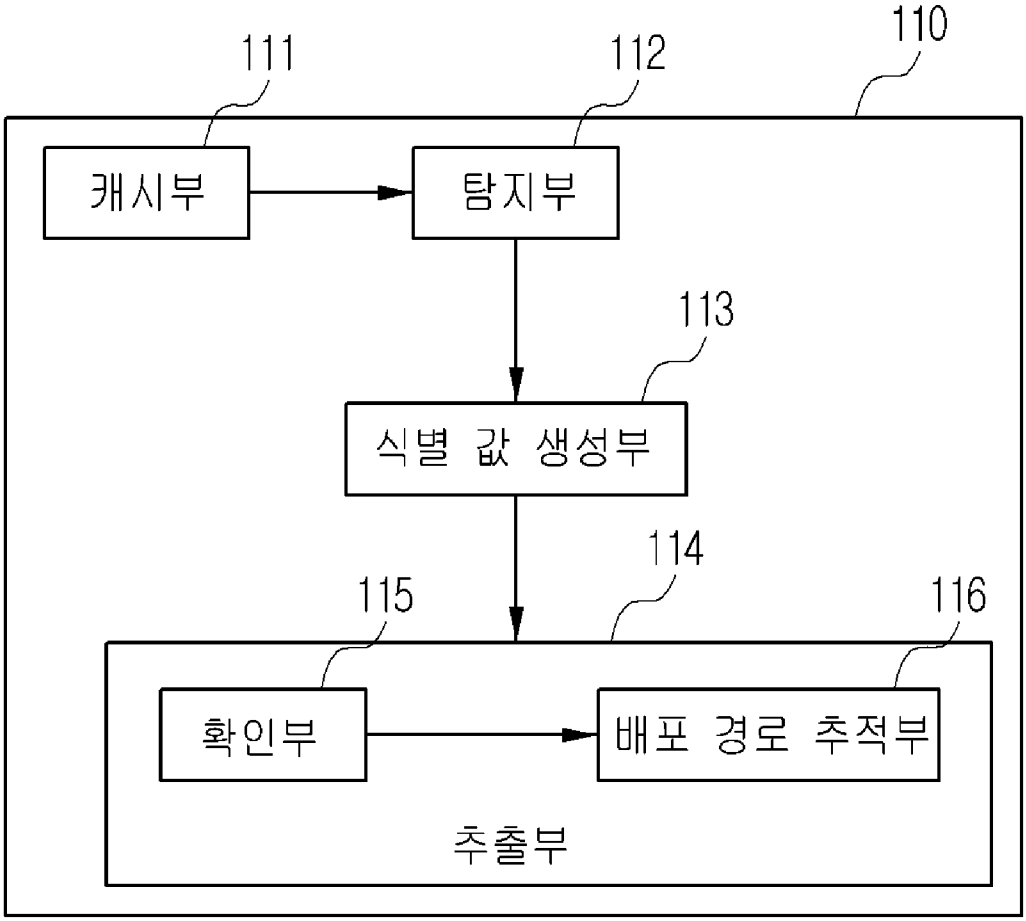
[청구항 6] 제1항에 있어서,
상기 추출부는
상기 추출된 배포처 정보를 기초로 상기 신규 파일이 다른 파일로부터 배포된 파일인지 여부를 확인하는 확인부; 및
상기 신규 파일이 상기 다른 파일로부터 배포된 파일인 경우, 상기 다른 파일의 식별 값을 기초로 상기 캐시부로부터 상기 다른 파일에 대한 배포처 정보를 추출하여 상기 신규 파일의 배포 경로를 추적하는 배포 경로 추적부
를 포함하는 단말 장치.

[청구항 7] 단말 장치에서 기 실행된(pre-executed) 적어도 하나의 파일에 대한 식별 값과 상기 적어도 하나의 파일에 대한 배포처 정보가 저장된 데이터베이스를 관리하는 단계;
상기 단말 장치에 신규 파일이 생성되는지 여부를 탐지하는 단계;
상기 신규 파일이 생성되었음이 탐지되는 경우, 상기 신규 파일의 식별 값을 생성하는 단계; 및
상기 데이터베이스로부터 상기 신규 파일의 식별 값과 동일한 식별 값을 갖는 파일에 대한 배포처 정보를 추출하는 단계
를 포함하는 단말 장치의 파일 배포처 확인 방법.

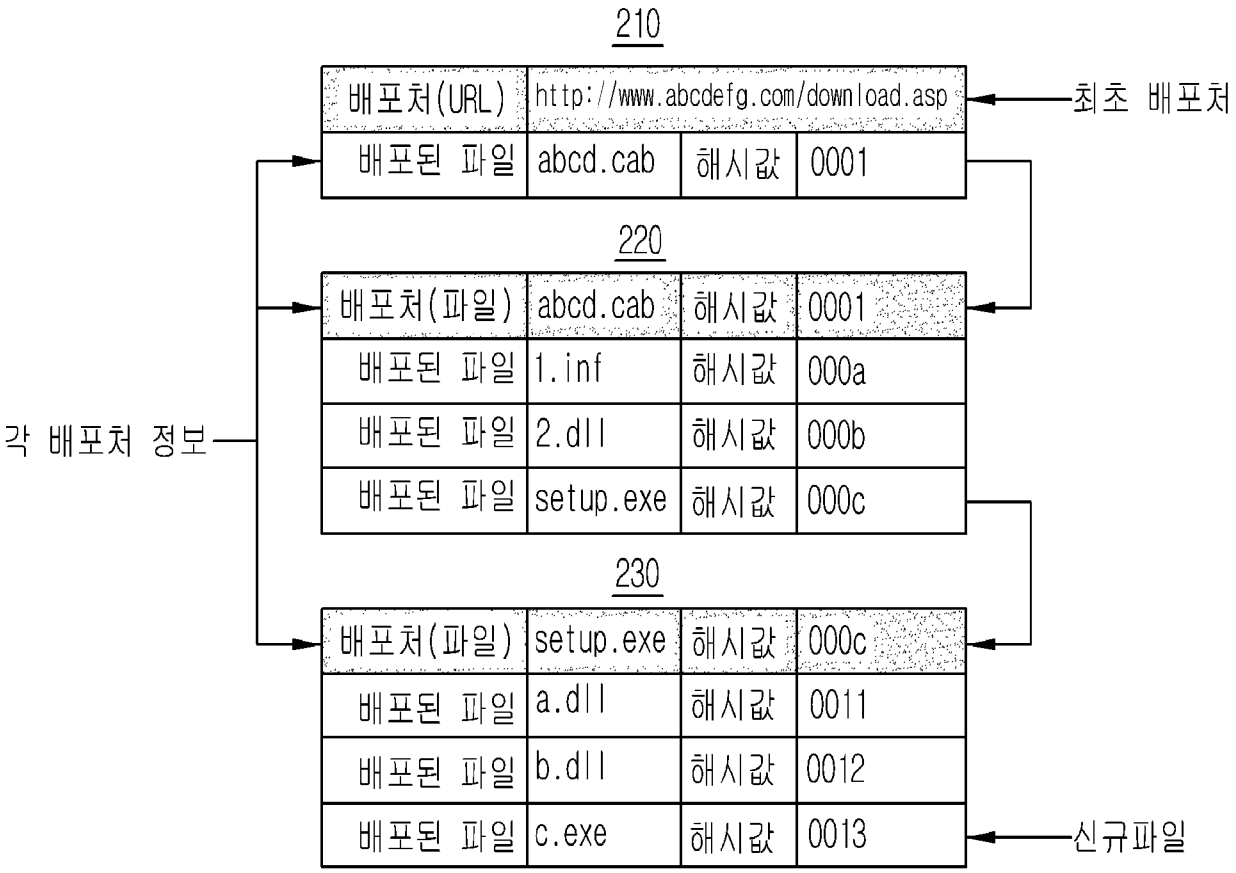
[청구항 8] 제7항에 있어서,
상기 추출된 배포처 정보를 기초로 상기 신규 파일이 다른 파일로부터 배포된 파일인지 여부를 확인하는 단계; 및
상기 신규 파일이 상기 다른 파일로부터 배포된 파일인 경우, 상기 다른 파일의 식별 값을 기초로 상기 데이터베이스로부터 상기 다른 파일에 대한 배포처 정보를 추출하여 상기 신규 파일의 배포 경로를 추적하는 단계
를 포함하는 단말 장치의 파일 배포처 확인 방법.

[청구항 9] 제7항 또는 제8항 중 어느 한 항의 방법을 수행하는 프로그램을 기록한 컴퓨터 판독 가능 기록 매체.

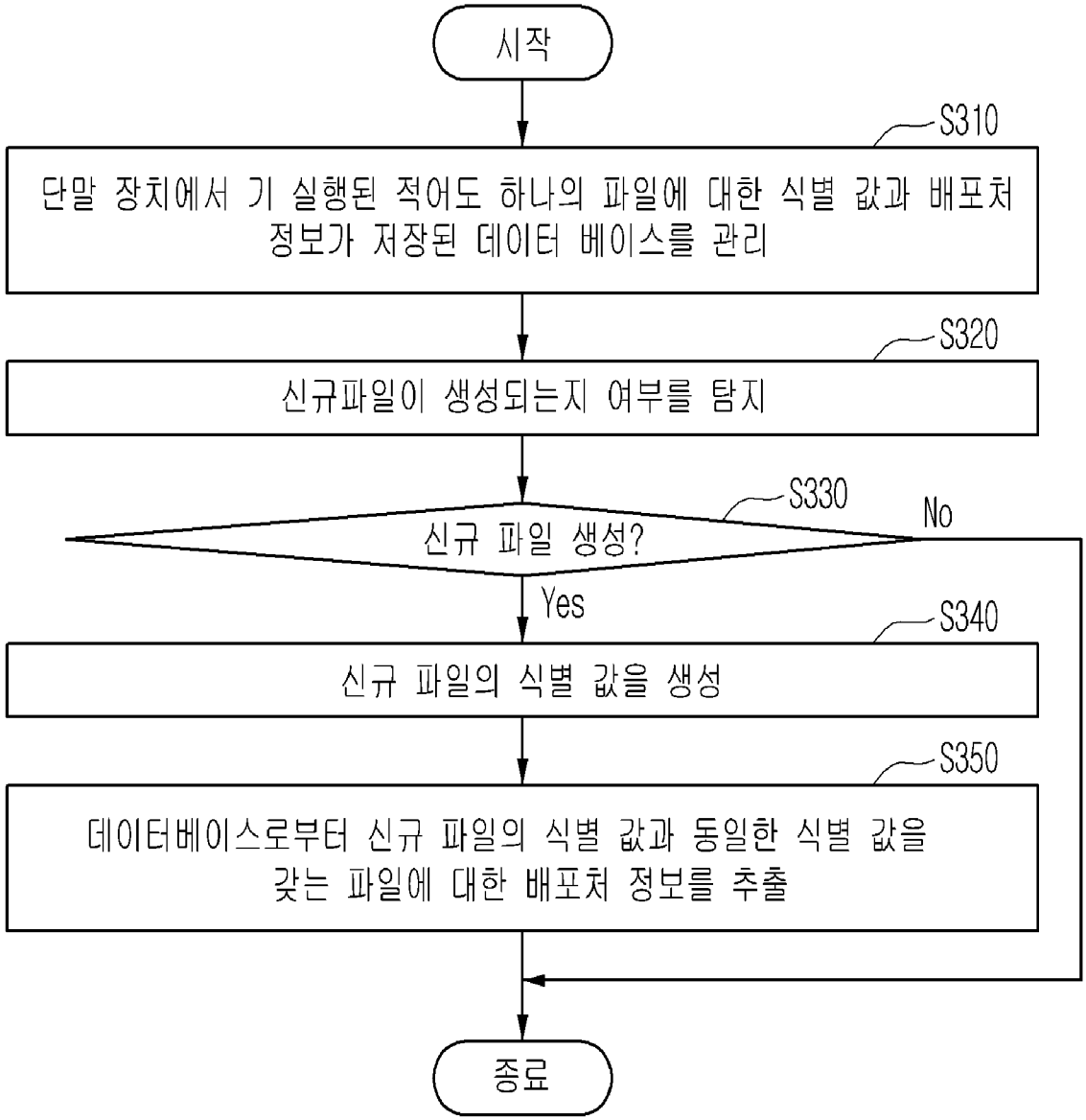
[Fig. 1]


110
111
112
캐시부
탐지부
113
식별 값 생성부
114
115
116
확인부
배포 경로 추적부
추출부

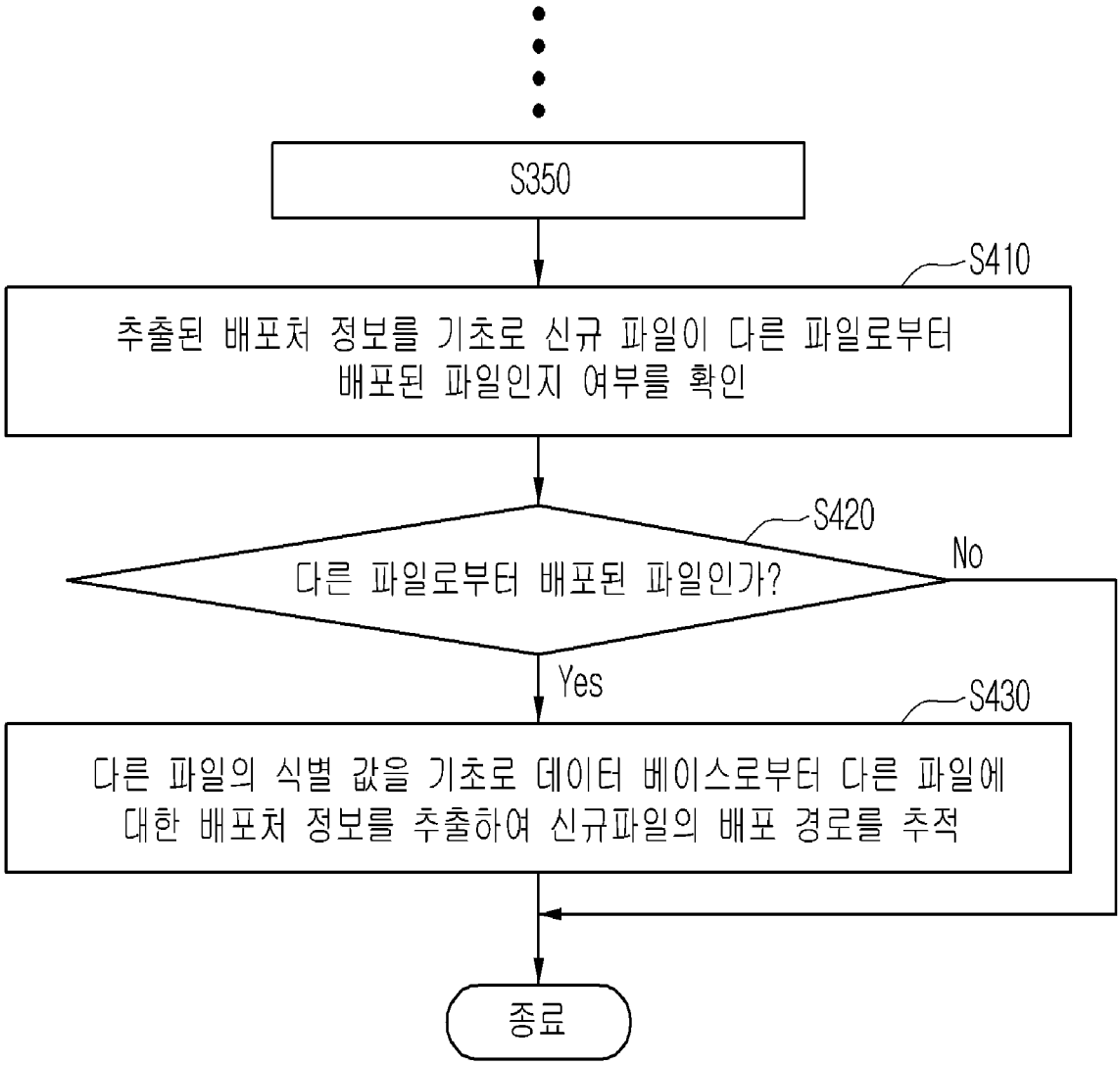
[Fig. 2]


210
배포처(URL)
http://www.abcdefg.com/download.asp
최초 배포처
배포된 파일
abcd.cab
해시값
0001
220
배포처(파일)
abcd.cab
해시값
0001
배포된 파일
1.inf
해시값
000a
각 배포처 정보
배포된 파일
2.dll
해시값
000b
배포된 파일
setup.exe
해시값
000c
230
배포처(파일)
setup.exe
해시값
000c
배포된 파일
a.dll
해시값
0011
배포된 파일
b.dll
해시값
0012
배포된 파일
c.exe
해시값
0013
신규파일

[Fig. 3]


시작
S310
단말 장치에서 기 실행된 적어도 하나의 파일에 대한 식별 값과 배포처 정보가 저장된 데이터 베이스를 관리
S320
신규파일이 생성되는지 여부를 탐지
S330
신규 파일 생성?
No
Yes
S340
신규 파일의 식별 값을 생성
S350
데이터베이스로부터 신규 파일의 식별 값과 동일한 식별 값을 갖는 파일에 대한 배포처 정보를 추출
종료

[Fig. 4]


S350
S410
추출된 배포처 정보를 기초로 신규 파일이 다른 파일로부터 배포된 파일인지 여부를 확인
S420
다른 파일로부터 배포된 파일인가?
No
Yes
S430
다른 파일의 식별 값을 기초로 데이터 베이스로부터 다른 파일에 대한 배포처 정보를 추출하여 신규파일의 배포 경로를 추적
종료