

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2017년 1월 19일 (19.01.2017)



(10) 국제공개번호
WO 2017/010665 A1

- (51) 국제특허분류:
G06F 17/30 (2006.01) *G06F 9/455* (2006.01)
- (21) 국제출원번호: PCT/KR2016/004794
- (22) 국제출원일: 2016년 5월 9일 (09.05.2016)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
10-2015-0099837 2015년 7월 14일 (14.07.2015) KR
- (71) 출원인: 서울대학교 산학협력단 (SEOUL NATIONAL UNIVERSITY R&DB FOUNDATION) [KR/KR]; 08826 서울시 관악구 관악로 1, Seoul (KR).
- (72) 발명자: 백윤홍 (PAEK, Yun Heung); 08826 서울시 관악구 관악로 1, 302-530, Seoul (KR). 조영필 (CHO, Yeong Pil); 08826 서울시 관악구 관악로 1 302-516-1, Seoul (KR).
- (74) 대리인: 리엔목 특허법인 (Y.P.LEE, MOCK & PARTNERS); 06292 서울시 강남구 언주로 30길 13 대림아크로텔 12층, Seoul (KR).

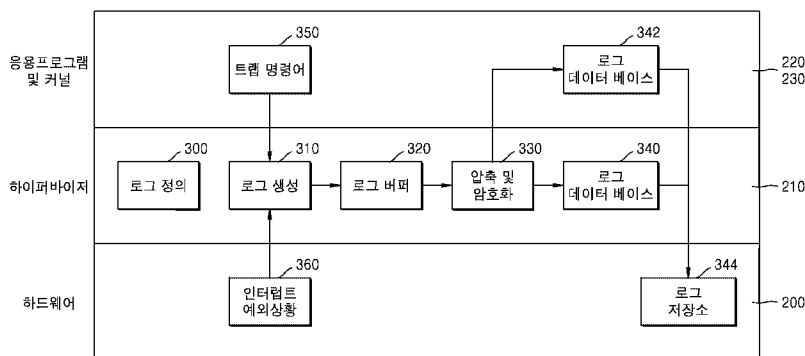
- (81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KZ, LA, LC, LK, LR, LS, LU, LY, 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, ST, 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))

(54) Title: LOGGING METHOD USING HYPERVISOR AND APPARATUS THEREOF

(54) 발명의 명칭 : 하이퍼바이저를 이용한 로깅 방법 및 그 장치



- 200 ... Hardware
210 ... Hypervisor
220, 230 ... Application program and kernel
300 ... Log definition
310 ... Log generation
320 ... Log buffer
330 ... Compression and encryption
340, 342 ... Log database
344 ... Log storage area
350 ... Trap command
360 ... Interrupt or exception

(57) Abstract: A logging method using a hypervisor and an apparatus thereof are disclosed. The hypervisor replaces, among the commands of an application program or a kernel, a command in a position defined by a log definition module with a trap command and, when the trap command is executed or if an interrupt or an exception occurs, stores the log data for the application program or the kernel after obtaining a system privilege and returns the system privilege.

(57) 요약서: 하이퍼바이저를 이용한 로깅 방법 및 그 장치가 개시된다. 하이퍼바이저는 응용 프로그램이나 커널의 명령어들 중 로그 정의 모듈에 정의된 위치의 명령어를 트랩 명령어로 대체하고, 트랩 명령어의 실행 또는 인터럽트나 예외상황 발생시 시스템 권한을 가져온 후 응용 프로그램이나 커널에 대한 로그 데이터를 저장하고 시스템 권한을 반환한다.

명세서

발명의 명칭: 하이퍼바이저를 이용한 로깅 방법 및 그 장치 기술분야

- [1] 본 발명은 로그 데이터를 저장하는 방법 및 그 장치에 관한 것으로서, 보다 상세하게는 마이크로 하이퍼바이저를 이용하여 커널 등의 로그 데이터를 저장하는 방법 및 그 장치에 관한 것이다.

배경기술

- [2] 마이크로 하이퍼바이저는 하나의 컴퓨터 시스템에 서로 다른 운영체제(Operating System)가 가동할 수 있도록 하는 일종의 소프트웨어이다. 다시 말해, 하이퍼바이저는 하드웨어와 운영체제 사이에 일종의 중간웨어로 사용되며, 하나의 컴퓨터에서 서로 다른 운영체제를 사용하는 가상 컴퓨터를 만들 수 있는 효과를 제공한다.

발명의 상세한 설명

기술적 과제

- [3] 본 발명이 이루고자 하는 기술적 과제는, 하이퍼바이저를 이용하여 커널이나 응용프로그램 등의 로그 데이터를 저장하는 방법 및 그 장치를 제공하는 데 있다.

과제 해결 수단

- [4] 상기의 기술적 과제를 달성하기 위한, 본 발명에 따른 하이퍼바이저를 이용한 로그 데이터 저장 방법의 일 예는, 하이퍼바이저, 커널, 응용프로그램을 포함하는 컴퓨팅 장치에서 상기 하이퍼바이저의 로깅 방법에 있어서, 상기 하이퍼바이저는, 응용 프로그램이나 커널의 명령어들 중 로그 정의 모듈에 정의된 위치의 명령어를 트랩 명령어로 대체하는 단계; 상기 트랩 명령어의 실행 또는 인터럽트나 예외상황 발생시, 시스템 권한을 가져오는 단계; 상기 응용 프로그램이나 커널에 대한 로그 데이터를 저장하는 단계; 및 상기 응용 프로그램이나 커널로 시스템 권한을 넘겨주는 단계;를 포함한다.
- [5] 상기의 기술적 과제를 달성하기 위한, 본 발명에 따른 컴퓨팅 장치의 일 예는, 응용 프로그램이나 커널의 명령어들 중 트랩 명령어로 대체할 명령어의 위치를 정의하는 로그정의모듈; 상기 로그정의모듈에 따라 상기 응용프로그램이나 커널의 명령어들을 트랩 명령어로 대체하는 명령어대체부; 및 상기 트랩 명령어가 수행되면 시스템 권한을 가져오고, 로그 데이터 저장이 완료되면 시스템 권한을 상기 응용 프로그램이나 커널로 넘겨주는 권한제어부; 및 상기 응용프로그램이나 커널의 로그 데이터를 파악하여 저장하는 로그저장부;를 포함한다.

발명의 효과

- [6] 본 발명에 따르면, 커널이나 응용프로그램의 동작, 시스템 인터럽트나 예외

상황 등에 따른 다양한 로그 데이터를 용이하게 파악하고 저장할 수 있다.

도면의 간단한 설명

- [7] 도 1은 본 발명이 적용되는 컴퓨팅 장치의 일 실시 예의 구성을 도시한 도면,
- [8] 도 2는 본 발명이 적용되는 컴퓨팅 장치의 시스템 권한 순서를 도시한 도면,
- [9] 도 3은 본 발명에 따른 하이퍼바이저를 이용한 로깅 방법의 개략적인 흐름을 도시한 도면,
- [10] 도 4는 본 발명에 따른 로그정의 모듈의 일 예를 도시한 도면,
- [11] 도 5는 본 발명에 따른 로그정의 모듈의 구현 예를 도시한 도면,
- [12] 도 6은 본 발명에 따른 로그정의 모듈에 따라 트랩 명령어를 삽입하는 일 예를 도시한 도면,
- [13] 도 7a 및 도 7b는 본 발명에 따른 로그정의 모듈에 따라 트랩 명령어를 삽입한 구현 예를 도시한 도면,
- [14] 도 8은 본 발명에 따른 하이퍼바이저의 일 예를 도시한 도면, 그리고,
- [15] 도 9는 본 발명에 따른 하이퍼바이저를 이용한 로깅 방법의 일 실시 예의 흐름을 도시한 도면이다.

발명의 실시를 위한 형태

- [16] 이하에서, 첨부된 도면들을 참조하여 본 발명에 따른 하이퍼바이저를 이용한 로깅 방법 및 그 장치에 대해 상세히 설명한다.
- [17] 도 1은 본 발명이 적용되는 컴퓨팅 장치의 일 실시 예의 구성을 도시한 도면이다.
- [18] 도 1을 참조하면, 컴퓨팅 장치(100)는 중앙처리부(110), 메모리(120), 저장부(130), 입출력부(140) 및 디스플레이부(150)를 포함한다. 중앙처리부(110)는 프로세서(processor)로서, 메모리(120), 저장부(130), 입출력부(140) 및 디스플레이부(150)를 각각 제어하며, 커널이나 응용 프로그램 또는 하이퍼바이저의 소프트웨어를 구동시킨다. 메모리(120)는 RAM(Random Access Memory), ROM(Read Only Memory) 등으로 구성되고, 저장부(130)는 하드 디스크, SSD(Solid State Disk) 등 다양한 형태로 구현된다. 입출력부(140)는 키패드나 터치스크린 등의 입력수단을 통해 사용자 명령을 입력받거나, 인터넷 등의 유무선 통신망을 통해 외부 장치와 통신을 수행하거나, USB(Universal Serial Bus) 포트 등을 통해 각종 외부 장치와 접속한다. 디스플레이부(150)는 LCD, LED, OLED 등으로 구성될 수 있다.
- [19] 도 2는 본 발명이 적용되는 컴퓨팅 장치의 시스템 권한 순서를 도시한 도면이다.
- [20] 도 2를 참조하면, 시스템 권한은 하드웨어(200), 하이퍼바이저(210), 커널(220), 응용프로그램(230)의 순으로 높다. 따라서 하이퍼바이저(210)는 커널(220) 및 응용프로그램(230)의 다양한 행위를 모니터링하고 제어할 수 있다.
- [21] 도 3은 본 발명에 따른 하이퍼바이저를 이용한 로깅 방법의 개략적인 흐름을

도시한 도면이다.

- [22] 도 3을 참조하면, 관리자는 응용 프로그램이나 커널(220,230), 하드웨어(200)의 인터럽트나 예외상황(360) 등의 다양한 동작들 중 로깅이 필요한 시점과 각 로깅 시점에 저장할 로그 데이터의 종류 등을 포함하는 로그정의(300)를 설정하고 저장한다. 여기서, 로깅은 응용프로그램이나 커널(220,230), 하드웨어 인터럽트(360) 등의 각종 동작과 관련된 데이터, 예를 들어 특정 메모리 영역의 데이터, 레지스터 값, 입출력 데이터 등을 기록하는 과정을 의미한다. 로그정의(300)를 포함하는 로그정의 모듈의 일 예에 대해서는 도 4 및 도 5에 도시되어 있다.
- [23] 하이퍼바이저(210)는 응용 프로그램이나 커널(220,230)의 수행 중 로깅이 필요한 시점에 시스템 권한을 가져오기 위하여 응용 프로그램이나 커널에 트랩 명령어(350)를 삽입하거나, 인터럽트나 예외상황에서 시스템 권한을 가져오기 위하여 제어 레지스터의 값을 변경한다. 하이퍼바이저(210)가 응용 프로그램이나 커널(220,230)에 트랩 명령어를 삽입하는 방법의 일 예에 대해서는 도 6, 도 7a,7b에 도시되어 있다.
- [24] 응용 프로그램이나 커널(220,230)이 동작 중에 하이퍼바이저(210)가 삽입한 트랩 명령어(350)를 만나면, 하이퍼바이저(210)는 시스템 권한을 가져온 후 응용 프로그램이나 커널(220,230) 등의 각종 동작과 관련된 로그 데이터를 생성(310)한다. 또한 하드웨어(200)의 인터럽트나 예외상황(360)이 발생하고, 해당 인터럽트나 예외상황에 대한 제어 레지스터의 값이 실행 흐름을 하이퍼바이저(210)로 변경되도록 설정되어 있다면, 하이퍼바이저(210)는 시스템 권한을 가져온 후 로그 데이터를 생성한다. 예를 들어, 가상 메모리 관련 상태값 변경이나 일반적인 인터럽트 발생 등의 특정 이벤트 발생시, 시스템 권한이 하이퍼바이저(210)로 넘어갈 수 있도록 제어 레지스터의 값을 변경할 수 있다.
- [25] 로그 데이터는 로그정의 모듈에 정의된 로그 데이터 종류와 더불어 로그 발생 시간, 로그 발생 위치, 로그 발생 원인 등 다양한 정보를 포함할 수 있다. 예를 들어, I/O 처리와 관련된 로그 데이터를 저장하는 로그정의가 설정되어 있는 경우에, 하이퍼바이저(210)는 I/O 처리와 연산 발생 시점에 트랩 명령어를 통해 시스템 권한을 가져온 후, 현 시점에서 실행 중인 프로세서가 무엇인지, 어떤 파일에 어떤 데이터를 남기려고 했는지 등을 수집할 수 있다. 로그 데이터 수집을 위하여 디지털 포렌식(Digital Forensic) 기법이 적용될 수 있다.
- [26] 하이퍼바이저(210)는 로깅 동작과 관련하여 시스템 성능에 미치는 영향을 최소화하기 위하여 로그 데이터를 로그 버퍼(320)에 저장한다. 로그 버퍼(320)는 로그 데이터가 발생한 시간순서에 따라 데이터를 기록하고, 일정량 이상의 데이터가 로그 버퍼(320)에 쌓이면, 압축 및 암호화 과정(330)을 통해 로그 데이터를 로그 데이터베이스(340,342)에 저장한다. 로그 데이터를 암호화하여 저장함으로써 관리자가 아닌 커널이나 응용프로그램 등에서 권한 없이 내용을 읽거나 수정하는 것을 방지할 수 있다.

- [27] 로그 데이터베이스(340,342))는 하이퍼바이저(210)에 구현되거나, 응용 프로그램이나 커널(220,230)에 구현될 수 있다. 하이퍼바이저에 구현된 로그 데이터베이스(340)는 메모리 사용량 및 복잡도를 높일 수 있으므로, 응용 프로그램이나 커널에 구현한 로그 데이터베이스(342)를 활용하는 것이 나을 수 있다. 데이터베이스 구조는 로깅 동작에 영향을 미치지 아니하므로, 실시 예에 따라 다양한 구조의 로그 데이터베이스(340,342)를 채택할 수 있다.
- [28] 로그 데이터베이스(340,342)는 수집된 로그 데이터들을 로컬에 위치한 로그 저장소(344)나 네트워크로 연결된 원격 저장소 및 서버에 백업할 수 있다.
- [29] 도 4는 본 발명에 따른 로그정의 모듈의 일 예를 도시한 도면이다.
- [30] 도 4를 참조하면, 로그정의 모듈은 관리자에 의해 정의된 적어도 하나 이상의 로그정의를 포함한다. 로그정의는 응용프로그램이나 커널, 시스템 인터럽트나 예외상황 등에서 로깅 작업이 필요한 시점(410), 저장할 로그 데이터의 종류(420) 등을 포함한다. 필요에 따라 해당 로깅 작업에 대한 주석문(400)을 포함할 수 있으며, 이 외에도 실시 예에 따라 다양한 정보가 정의될 수 있다.
- [31] 관리자는 도 5와 같이 다양한 프로그래밍 언어 등을 통해 로그정의를 설정하거나, 그래픽 사용자 인터페이스(GUI) 등을 통해 로그정의를 설정할 수 있다. 예를 들어, 컴퓨팅 장치는 그래픽 화면에서 주석문 입력 필드, 트랩 명령어를 삽입할 명령어 위치 입력 필드, 저장할 로그 데이터 종류 입력 필드를 화면에 표시하고, 각 필드에서 선택 가능한 메뉴 리스트를 사용자에게 제공하여, 사용자가 용이하게 로그정의를 설정할 수 있도록 한다. 이 외에도 관리자로부터 로그정의를 위한 각종 정보를 입력받는 다양한 방법이 존재할 수 있음은 물론이다.
- [32] 트랩 명령어를 삽입할 명령어 위치(410)는 응용 프로그램이나 커널이 시작될 때 메모리에 적재되는 명령어들 중 특정 명령어의 위치를 가리킨다. 명령어의 위치는 종래의 다양한 방법을 통해 관리자가 사전에 파악하고 있다고 가정한다. 예를 들어, 커널의 경우 메모리의 정해진 위치에 적재되고, 메모리 내 각 명령어의 위치는 고정되어 있으므로, 관리자는 종래의 디버깅(debugging) 과정 등의 다양한 방법을 통해 커널 내 명령어의 위치를 파악할 수 있다. 또 다른 예로, 응용 프로그램의 경우 실행시 메모리에 적재되는 위치는 매번 달라질 수 있으나 응용 프로그램 내의 각 명령어의 상대적 위치(오프셋(offset))는 고정적이므로, 관리자는 디버깅 과정 등 종래의 다양한 방법을 통해 응용 프로그램 내 명령어의 상대적 위치를 파악할 수 있다. 커널이나 응용 프로그램의 명령어 위치를 파악하는 방법 그 자체는 본 발명의 범위를 벗어나므로 이에 대한 추가적인 설명은 생략한다.
- [33] 로그 데이터 종류(420)는 관리자에 의해 다양하게 설정될 수 있다. 예를 들어, 응용프로그램이나 커널 등에서 메모리 할당이나 메모리 해제 작업을 수행하기 전의 메모리 상태를 저장하기를 원하는 경우에, 관리자는 응용프로그램이나 커널 등의 메모리 할당이나 해제와 관련된 명령어의 수행 전의 명령어의 위치를

트랩 명령어의 삽입 위치로 정의하고, 또한 저장할 로그 데이터를 메모리 할당이나 해제 작업이 수행되는 메모리의 해당 영역의 데이터로 정의하면 된다.

- [34] 하드웨어 인터럽트나 예외상황에 대한 로그정의를 설정하고자 하는 경우에, 관리자는 인터럽트나 예외상황의 특정 이벤트(예를 들어, 가상 메모리 관련 상태값 변경 등)와 관련된 제어 레지스터 종류와 저장할 로그 데이터 종류를 정의한다. 인터럽트나 예외상황에 대한 로그정의를 프로그래밍 언어로 정의되거나, 각종 GUI 환경을 통해 정의될 수 있다.
- [35] 도 5는 본 발명에 따른 로그정의 모듈의 구현 예를 도시한 도면이다.
- [36] 도 5를 참조하면, 로그정의 모듈(500)은 해당 로그 정의가 무엇에 관한 것인지 나타내는 주석문(400)과, 트랩 명령어가 삽입될 명령어 위치(410), 저장할 로그 데이터의 종류(420)를 포함한다. 도 5는 커널의 메모리 해제 전의 로깅 작업을 수행하는 일 예로서, 트랩 명령어의 삽입 위치(410)는 메모리의 '0xc011a060' 위치이고, 저장한 로그 데이터 종류(420)는 레지스터 번호 '0'번째 데이터임을 정의하고 있다.
- [37] 도 6은 본 발명에 따른 로그정의 모듈에 따라 트랩 명령어를 삽입하는 일 예를 도시한 도면이다.
- [38] 도 6을 참조하면, 응용 프로그램이나 커널이 실행되면, 하이퍼바이저는 메모리에 적재된 응용 프로그램이나 커널의 명령어들(600) 중 로그정의 모듈에 정의된 위치의 명령어(610)를 트랩 명령어(630)로 대체한다.
- [39] 예를 들어, 로그정의 모듈에서 트랩 명령어가 삽입될 명령어 위치가 N번째 명령어(610)의 위치로 정의되어 있다면, 하이퍼바이저는 응용프로그램이나 커널이 시작될 때에 N번째 명령어(610)를 트랩 명령어(630)로 대체한다. 따라서 응용프로그램이나 커널이 명령어를 수행하다가 대체된 트랩 명령어(630)를 만나면, 시스템 권한은 하이퍼바이저로 넘어간다. 시스템 권한을 넘겨받은 하이퍼바이저는 로그정의 모듈에 정의된 로그 데이터를 파악하여 저장한다.
- [40] 도 7a 및 도 7b는 본 발명에 따른 로그정의 모듈에 따라 트랩 명령어를 삽입한 구현 예를 도시한 도면이다.
- [41] 도 7a 및 도 7b를 참조하면, 메모리 해제에 대한 소스코드와 해당 소스코드의 실행을 위한 실제 명령어를 메모리에 적재한 예가 도시되어 있다. 관리자가 메모리 해제시점에 로깅을 수행하고자 한다면, 관리자는 메모리 해제 명령(_vummap(addr,1))에 대한 위치를 기초로 앞서 살핀 도 5의 로깅정의 모듈을 작성한다.
- [42] 도 5의 예를 다시 살펴보면, 메모리 해제 명령어(_vummap)의 위치는 '0xc011a64'이므로, 관리자는 로깅정의 모듈에 트랩 명령어가 삽입될 명령어 위치로 해제 명령어(710)의 수행 바로 이전 위치인 '0xc011a060'을 정의하고, 메모리 해제 위치를 가리키고 있는 레지스터 번호 '0'를 로그 데이터의 종류로 정의한다.
- [43] 다시 도 7을 참조하면, 하이퍼바이저는 커널 또는 응용프로그램이 시작될 때,

도 5의 로그정의 모듈에 정의된 메모리 위치 '0xc011a060'의 명령어(700)를 트랩 명령어(800)로 대체한다. 커널이나 응용프로그램이 시작되어 '0xc011a060'의 트랩 명령어(800)를 만나면, 시스템 권한은 하이퍼바이저로 넘어간다.

[44] 도 8은 본 발명에 따른 하이퍼바이저의 일 예를 도시한 도면이다.

[45] 도 8을 참조하면, 하이퍼바이저(210)는 로그정의모듈(800), 명령어 대체부(810), 로그 저장부(820), 권한 제어부(830)의 구성을 포함한다. 하이퍼바이저(210)는 일종의 소프트웨어로 구현가능하며, 도 1에서 살핀 컴퓨팅 시스템의 메모리, 중앙처리부 등의 하드웨어를 통해 실행될 수 있다.

[46] 로그정의모듈(800)은 트랩 명령어가 삽입될 응용프로그램이나 커널의 명령어 위치, 저장할 로그 데이터의 종류 등을 포함하는 적어도 하나 이상이 로그정의를 포함한다. 관리자는 디버깅 등 종래의 다양한 방법을 통해 응용 프로그램이나 커널의 각 명령어의 위치를 사전에 알고 있다고 가정한다.

[47] 명령어 대체부(810)는 로그정의 모듈에 따라 응용 프로그램이나 커널에 트랩 명령어를 삽입한다. 명령어 대체부(810)는 응용 프로그램이나 커널의 명령어들 사이에 트랩 명령어를 삽입할 수도 있으나, 보다 바람직하게는 응용 프로그램이나 커널의 기존 명령어를 트랩 명령어로 대체하여 삽입한다. 명령어 대체부(810)는 커널이 부팅되는 시점 또는 응용 프로그램이 시작되는 시점에 트랩 명령어를 삽입하는 과정을 수행한다.

[48] 로그 저장부(820)는 명령어 대체부(810)에 의해 응용 프로그램이나 커널 등에 삽입된 트랩 명령어가 수행되어, 시스템 권한이 하이퍼바이저로 넘어오면, 로그정의 모듈에 정의된 내용에 따라 저장할 로그 데이터를 파악하여 저장하는 로깅과정을 수행한다.

[49] 권한 제어부(830)는 응용 프로그램이나 커널 등에 삽입된 트랩 명령어가 수행되면 응용 프로그램이나 커널로부터 시스템 권한을 가져오고, 로그 저장부(820)에 의한 로깅 작업이 완료되면 시스템 권한을 응용 프로그램이나 커널 등에 다시 돌려준다.

[50] 응용 프로그램이나 커널의 명령어가 명령어 대체부(810)에 의해 기존 명령어에서 트랩 명령어로 대체된 경우에, 권한 제어부(830)가 로깅 작업 후 시스템 권한만을 넘겨주면 응용 프로그램이나 커널의 정상적인 동작이 불가능할 수 있다. 따라서 권한 제어부(830)는 응용 프로그램이나 커널에 권한을 넘겨주기 전에 트랩 명령어로 대체된 기존 명령어를 수행하거나, 기존 명령어를 디코딩하여 에뮬레이터를 통해 수행한 후 권한을 넘겨준다. 예를 들어, 도 7b의 트랩 명령어를 도 7a의 대체 전의 명령어를 수행한 후 시스템 권한을 넘겨준다.

[51] 트랩 명령어로 대체 전의 원 명령어를 디코딩하여 에뮬레이터를 통해 수행한 후 권한을 넘겨주는 경우, 하이퍼바이저가 원 명령어의 실행을 자유롭게 관리할 수 있고 관련된 모든 명령어를 처리할 수 있는 장점이 있으나 하이퍼바이저의 구현이 복잡해지는 단점이 있다. 단순히 원 명령어만을 수행한 후 권한을 넘겨주는 경우, 하이퍼바이저가 복잡하지 않게 구현될 수 있으며 원 명령어의

연산을 빠르게 수행할 수 있는 장점이 있으나, 스택 포인터와 관련된 연산과 같이 몇 가지 지원하지 못하는 연산이 있을 수 있다는 단점이 있다. 따라서 권한 제어부(830)는 상황에 따라 원 명령어만의 수행 또는 에뮬레이션 수행을 선택적으로 수행한다.

- [52] 예를 들어, 트랩 명령어로 덮어 씌어진 원 명령어가 'mov r1 r2'이고, 로깅 과정에서 r2를 사용한다면 로깅 작업이후 단순히 원 명령어 'mov r1 r2'를 수행하면 결과가 틀려진다. 따라서 권한 제어부는 로깅 작업에서 r2를 사용하지 않게 하거나 명령의 'operand'를 바꾸는 방법 등이 수행되어야 하므로 단순한 원 명령어의 수행이 아닌 정확한 결과 산출을 위한 여러 가지 과정을 수행하는 에뮬레이션을 수행한다.
- [53] 권한 제어(830)부는 인터럽트나 예외상황의 경우에도 시스템 권한을 넘겨주기 전에 추가적인 동작 수행 여부를 파악한다. 예를 들어, 인터럽트나 예외상황이 기존 커널이나 응용프로그램의 동작에 영향을 미치지 아니하고 단지 로깅을 위하여 커널이나 응용프로그램의 동작과 관련이 있는 인터럽트나 예외상황을 강제로 하이퍼바이저로 전달한 것이라면, 권한 제어부(830)는 시스템 권한을 반환하기에 앞서 커널 등에 대한 인터럽트 및 예외상황이 발생했음을 알리기 위하여 관련된 레지스터 및 메모리 값을 인터럽트 및 예외상황이 발생했을 때와 마찬가지로 설정한 후 권한을 반환한다.
- [54] 도 9는 본 발명에 따른 하이퍼바이저를 이용한 로깅 방법의 일 실시 예의 흐름을 도시한 도면이다.
- [55] 도 9를 참조하면, 하이퍼바이저는 관리자로부터 로그정의 입력받아 로그정의 모듈로 저장한다(S900). 하이퍼바이저는 응용프로그램이나 커널 등이 시작될 때, 로그정의 모듈을 기초로 응용프로그램이나 커널에 트랩 명령어를 삽입한다(S910).
- [56] 응용 프로그램이나 커널이 하이퍼바이저가 삽입한 트랩 명령어를 만나면(S920), 하이퍼바이저는 시스템 권한을 응용 프로그램이나 커널로부터 넘겨받는다(S930). 하이퍼바이저는 레지스터 등의 시스템 정보 등을 백업하고, 로그정의모듈의 정의에 따라 해당하는 로그 데이터를 파악하여 저장한다(S950). 로깅 작업이 완료되면, 하이퍼바이저는 백업한 레지스터를 이용하여 레지스터를 시스템 권한을 가져오기 전의 레지스터로 복원한다(S960). 하이퍼바이저는 응용 프로그램이나 커널의 트랩 명령어를 대체 전의 원 명령어를 단순히 수행하거나, 원 명령어를 에뮬레이터 등을 통해 수행하고(S970), 시스템 권한을 응용 프로그램이나 커널로 다시 돌려준다(S980).
- [57] 본 발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 컴퓨터가 읽을 수 있는 기록매체의 예로는 다양한 형태의 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광데이터 저장장치 등이 있다. 또한

컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

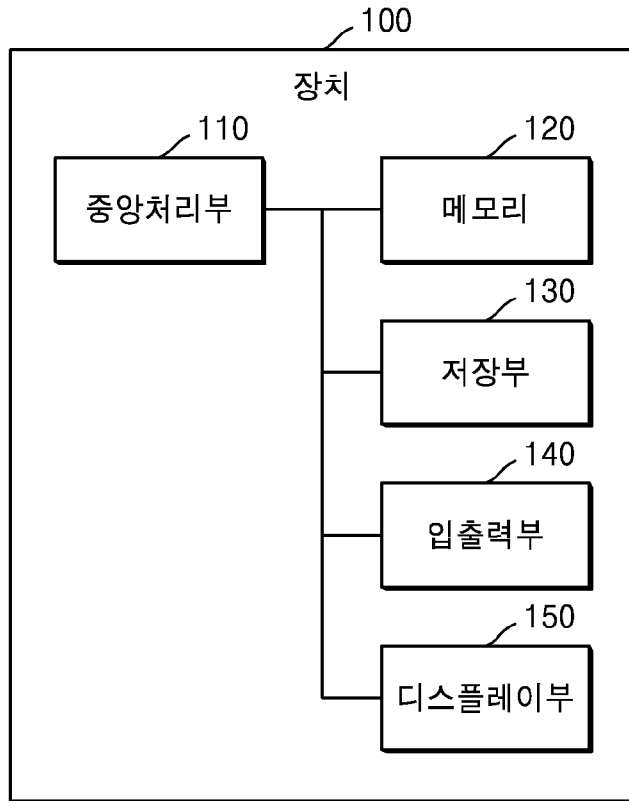
- [58] 이제까지 본 발명에 대하여 그 바람직한 실시예들을 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

청구범위

- [청구항 1] 하이퍼바이저, 커널, 응용프로그램을 포함하는 컴퓨팅 장치에서 상기 하이퍼바이저의 로깅 방법에 있어서, 상기 하이퍼바이저는, 응용 프로그램이나 커널의 명령어들 중 로그 정의 모듈에 정의된 위치의 명령어를 트랩 명령어로 대체하는 단계; 상기 트랩 명령어의 실행 또는 인터럽트나 예외상황 발생시, 시스템 권한을 가져오는 단계; 상기 응용 프로그램이나 커널에 대한 로그 데이터를 저장하는 단계; 및 상기 응용 프로그램이나 커널로 시스템 권한을 넘겨주는 단계;를 포함하는 것을 특징으로 하는 하이퍼바이저를 이용한 로깅 방법.
- [청구항 2] 제 1항에 있어서, 상기 로그 정의 모듈은 트랩 명령어로 대체할 응용 프로그램이나 커널의 명령어 위치, 저장할 로그 데이터의 종류를 포함하는 것을 특징으로 하는 하이퍼바이저를 이용한 로깅 방법.
- [청구항 3] 제 1항에 있어서, 상기 시스템 권한을 가져올 때 레지스터를 백업하고, 상기 시스템 권한을 넘겨줄 때 레지스터를 백업된 레지스터로 복원하는 단계;를 더 포함하는 것을 특징으로 하는 하이퍼바이저를 이용한 로깅 방법.
- [청구항 4] 제 1항에 있어서, 상기 시스템 권한을 넘겨주는 단계는, 상기 트랩 명령어로 대체된 상기 응용 프로그램이나 커널의 명령어를 대체 전의 원 명령어를 수행한 후 시스템 권한을 넘겨주는 단계;를 포함하는 것을 특징으로 하는 하이퍼바이저를 이용한 로깅 방법.
- [청구항 5] 제 1항에 있어서, 상기 로그 데이터를 저장하는 단계는, 로그 데이터를 하이퍼바이저의 버퍼에 저장하는 단계; 및 상기 버퍼에 저장된 로그 데이터의 크기가 임계치에 해당하면 상기 로그 데이터를 암호화하여 데이터베이스에 저장하는 단계;를 포함하는 것을 특징으로 하는 로깅 방법.
- [청구항 6] 응용 프로그램이나 커널의 명령어들 중 트랩 명령어로 대체할 명령어의 위치를 정의하는 로그정의모듈; 상기 로그정의모듈에 따라 상기 응용프로그램이나 커널의 명령어들을 트랩 명령어로 대체하는 명령어대체부; 및 상기 트랩 명령어가 수행되면 시스템 권한을 가져오고, 로그 데이터 저장이 완료되면 시스템 권한을 상기 응용 프로그램이나 커널로 넘겨주는 권한제어부; 및 상기 응용프로그램이나 커널의 로그 데이터를 파악하여 저장하는 로그저장부;를 포함하는 하이퍼바이저를 구동하기 위한 메모리, 중앙처리장치를 포함하는 컴퓨팅 장치.

- [청구항 7] 제 6항에 있어서, 상기 명령어대체부는,
인터럽트 및 예외상황 발생시 시스템 권한을 넘겨받을 수 있도록 컨트롤 레지스터의 값을 변경하는 것을 특징으로 하는 컴퓨팅 장치.
- [청구항 8] 제 6항에 있어서, 상기 로그저장부는,
상기 시스템 권한을 넘겨받을 때 레지스터를 백업하고, 상기 시스템 권한을 넘겨줄때 레지스터를 백업된 레지스터로 복원하는 것을 특징으로 하는 컴퓨팅 장치.
- [청구항 9] 제 6항에 있어서, 상기 권한제어부는,
상기 시스템 권한을 넘겨줄 때, 상기 응용프로그램이나 커널에 위치한 트랩 명령어를 대체 전의 원 명령어로 수행한 후 시스템 권한을 넘겨주는 것을 특징으로 하는 컴퓨팅 장치.
- [청구항 10] 제 6항에 있어서, 로그 저장부는,
로그 데이터를 하이퍼바이저의 버퍼에 저장하고, 상기 버퍼에 저장된 로그 데이터의 크기가 임계치에 해당하면 상기 로그 데이터를 암호화하여 데이터베이스에 저장하는 것을 특징으로 하는 컴퓨팅 장치.
- [청구항 11] 제 1항 내지 제 5항 중 어느 한 항에 기재된 방법을 수행하기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

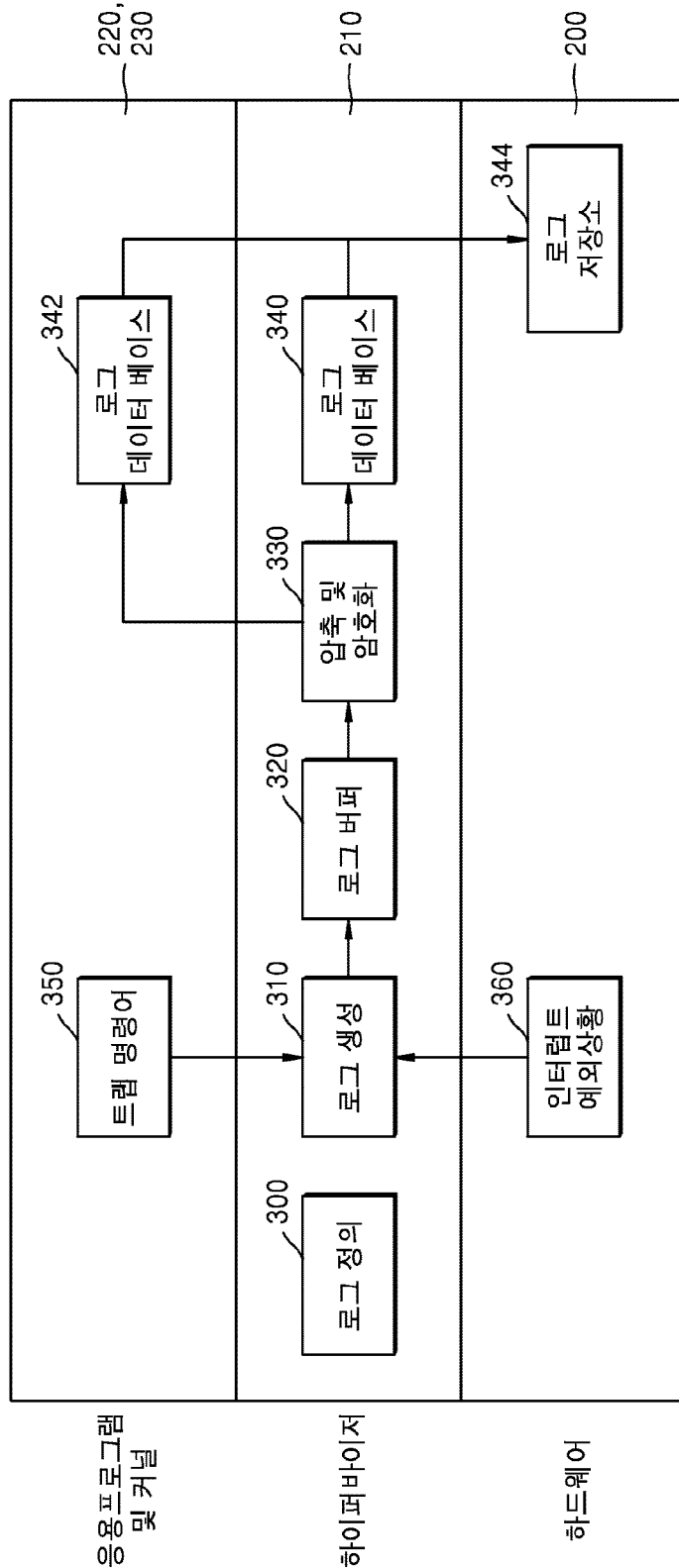
[도1]



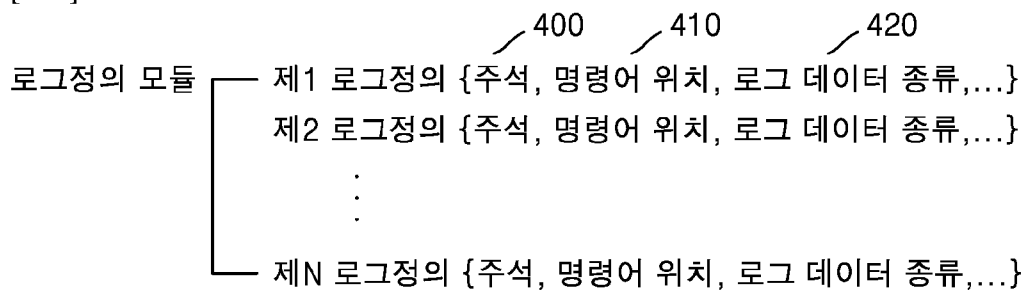
[도2]



[도3]



[도4]



[도5]

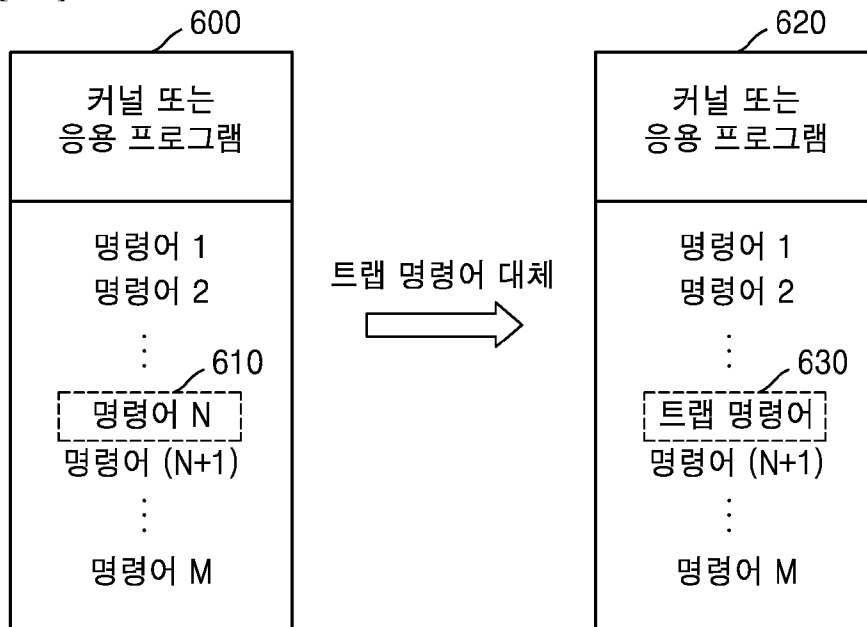
500

```

struct sormon_trap_data sormon_trap_targets[] = {
...
    {SORMON_TRAP_GATHER_DEALLOC_INFO, 0xc011a060, 0},
...
};
    
```

400
410
420

[도6]



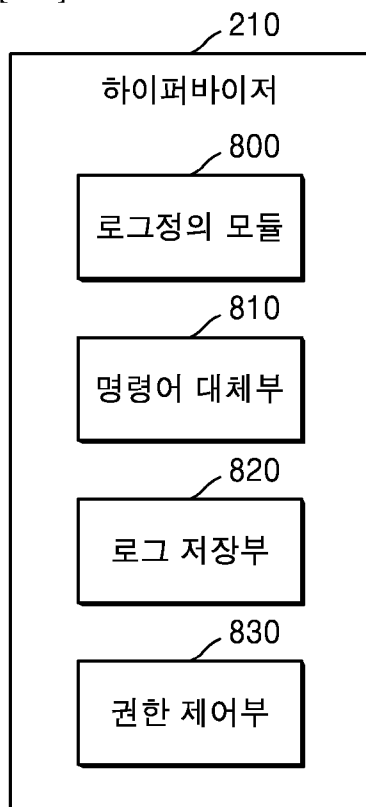
[도7a]

메모리 주소	<pre> c011a034 <vfree>: c011a034: mov ip, sp c011a038: push {fp, ip, lr, pc} c011a03c: sub fp, ip, #4 c011a040: mov r2, sp c011a044: bic r3, r2, #8128 ; 0x1fc0 c011a048: bic r3, r3, #63 ; 0x3f c011a04c: ldr r3, [r3, #4] c011a050: bic r3, r3, #-134217728 ; 0xf8000000 c011a054: bic r3, r3, #255 ; 0xff c011a058: cmp r3, #0 c011a05c: bne c011a06c <vfree+0x38> c011a060: mov r1, #1] — 700 c011a064: bl c0119e78 <__vunmap>] — 710 c011a068: ldm sp, {fp, sp, pc} c011a06c: ldr r0, [pc, #4] ; c011a078 <vfree+0x44> c011a070: movw r1, #1498 ; 0x5da c011a074: bl c004d52c <__bug> c011a078: .word 0xc068acac </pre>
소스 코드	<pre> void vfree(const void *addr) { BUG_ON(in_interrupt()); kmemleak_free(addr); __vunmap(addr, 1); } </pre>

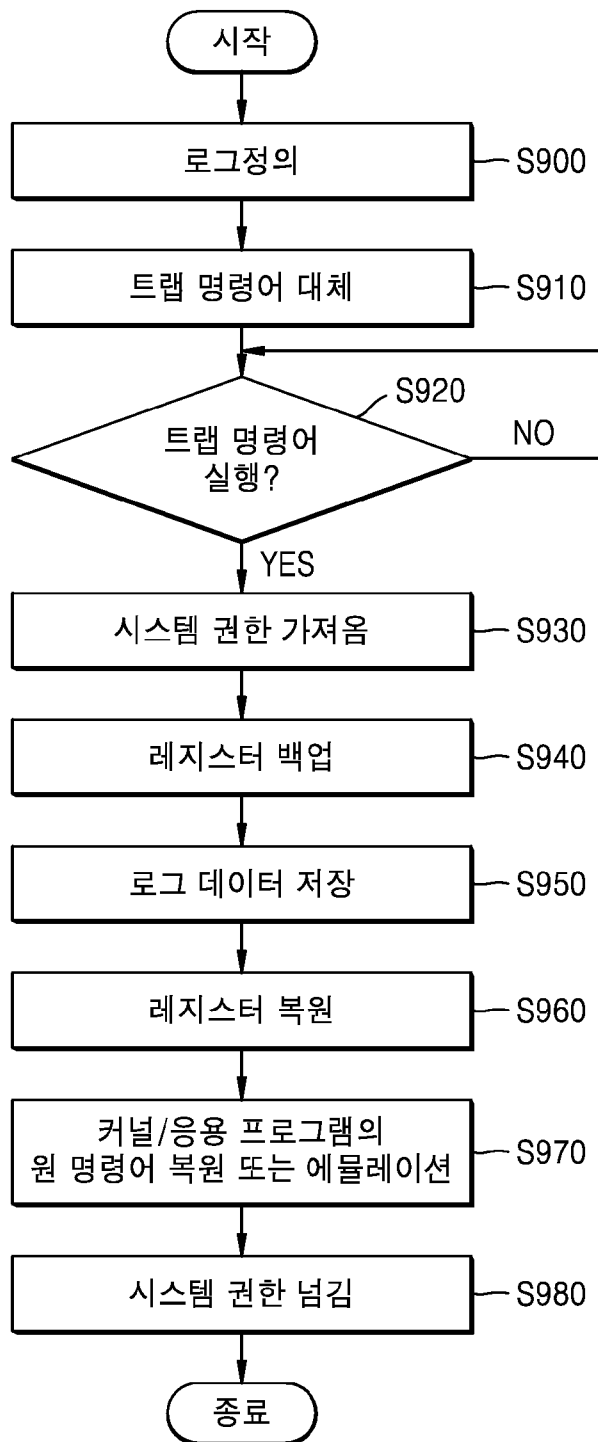
[도7b]

c011a034 <vfree>:	
c011a034:	mov ip, sp
c011a038:	push {fp, ip, lr, pc}
c011a03c:	sub fp, ip, #4
c011a040:	mov r2, sp
c011a044:	bic r3, r2, #8128 ; 0x1fc0
c011a048:	bic r3, r3, #63 ; 0x3f
c011a04c:	ldr r3, [r3, #4]
c011a050:	bic r3, r3, #-134217728 ; 0xf8000000
c011a054:	bic r3, r3, #255 ; 0xff
c011a058:	cmp r3, #0
c011a05c:	bne c011a06c <vfree+0x38>
c011a060:	hvc #0 — 800
c011a064:	bl c0119e78 <__vunmap> — 710
c011a068:	ldm sp, {fp, sp, pc}
c011a06c:	ldr r0, [pc, #4] ; c011a078 <vfree+0x44>
c011a070:	movw r1, #1498 ; 0x5da
c011a074:	bl c004d52c <__bug>
c011a078:	.word 0xc068acac

[도8]



[도9]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2016/004794**A. CLASSIFICATION OF SUBJECT MATTER****G06F 17/30(2006.01)i, G06F 9/455(2006.01)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 17/30; G06F 3/00; G06F 7/00; G06F 9/46; G06F 9/455; G06F 9/00

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: hypervisor, log data, trap instruction word, application program, kernel, system authority.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KR 10-0984203 B1 (INTEL CORP.) 28 September 2010 See paragraphs [0027]-[0033] and [0044]-[0061]; claim 13; and figures 3-5.	1-11
Y	US 2009-0007111 A1 (NELSON, Michael et al.) 01 January 2009 See paragraphs [0005]-[0006] and [0010]-[0025]; and figures 1-3.	1-11
A	US 2013-0036093 A1 (HEISER, Gernot et al.) 07 February 2013 See paragraphs [0028]-[0038] and figures 2-4.	1-11
A	WO 2014-004747 A2 (LYNXWORKS, INC.) 03 January 2014 See page 3, lines 6-25; page 20, line 15-page 21, line 20; and figures 6A-6B.	1-11
A	US 2005-0076155 A1 (LOWELL, David E.) 07 April 2005 See paragraphs [0008]-[0009] and [0018]-[0023]; and figures 1-2.	1-11



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

29 AUGUST 2016 (29.08.2016)

Date of mailing of the international search report

29 AUGUST 2016 (29.08.2016)

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.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2016/004794

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-0984203 B1	28/09/2010	CN 101076781 A	21/11/2007
		EP 1839142 A1	03/10/2007
		JP 2008-523511 A	03/07/2008
		JP 5042848 B2	03/10/2012
		KR 10-2007-0086843 A	27/08/2007
		US 2006-0130060 A1	15/06/2006
		US 7757231 B2	13/07/2010
		WO 2006-063274 A1	15/06/2006
US 2009-0007111 A1	01/01/2009	NONE	
US 2013-0036093 A1	07/02/2013	AU 2010-333716 A1	26/07/2012
		AU 2010-333716 B2	16/06/2016
		EP 2513821 A1	24/10/2012
		EP 2513821 A4	27/05/2015
		WO 2011-072340 A1	23/06/2011
WO 2014-004747 A2	03/01/2014	EP 2864876 A2	29/04/2015
		EP 2864876 A4	20/07/2016
		US 2013-347131 A1	26/12/2013
		US 2015-007326 A1	01/01/2015
		US 2015-213264 A1	30/07/2015
		US 8745745 B2	03/06/2014
		US 9218489 B2	22/12/2015
		WO 2014-004747 A3	01/05/2014
US 2005-0076155 A1	07/04/2005	US 7793287 B2	07/09/2010

A. 발명이 속하는 기술분류(국제특허분류(IPC))

G06F 17/30(2006.01)i, G06F 9/455(2006.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

G06F 17/30; G06F 3/00; G06F 7/00; G06F 9/46; G06F 9/455; G06F 9/00

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: 하이퍼바이저, 로그 데이터, 트랩 명령어, 응용 프로그램, 커널, 시스템 권한.

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	KR 10-0984203 B1 (인텔 코오퍼레이션) 2010.09.28 단락 [0027]-[0033]과 [0044]-[0061]; 청구항 13; 및 도면 3-5 참조.	1-11
Y	US 2009-0007111 A1 (MICHAEL NELSON 등) 2009.01.01 단락 [0005]-[0006]과 [0010]-[0025]; 및 도면 1-3 참조.	1-11
A	US 2013-0036093 A1 (GERNOT HEISER 등) 2013.02.07 단락 [0028]-[0038] 및 도면 2-4 참조.	1-11
A	WO 2014-004747 A2 (LYNXWORKS, INC.) 2014.01.03 페이지 3, 라인 6 - 25; 페이지 20, 라인 15 - 페이지 21, 라인 20; 및 도면 6A-6B 참조.	1-11
A	US 2005-0076155 A1 (DAVID E. LOWELL) 2005.04.07 단락 [0008]-[0009]와 [0018]-[0023]; 및 도면 1-2 참조.	1-11

☐ 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

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

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

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

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

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

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

“&” 동일한 대응특허문헌에 속하는 문헌

“P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

국제조사의 실제 완료일

2016년 08월 29일 (29.08.2016)

국제조사보고서 발송일

2016년 08월 29일 (29.08.2016)

ISA/KR의 명칭 및 우편주소

대한민국 특허청
(35208) 대전광역시 서구 청사로 189,
4동 (둔산동, 정부대전청사)

팩스 번호 +82-42-481-8578

심사관

노지명

전화번호 +82-42-481-8528



국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-0984203 B1	2010/09/28	CN 101076781 A EP 1839142 A1 JP 2008-523511 A JP 5042848 B2 KR 10-2007-0086843 A US 2006-0130060 A1 US 7757231 B2 WO 2006-063274 A1	2007/11/21 2007/10/03 2008/07/03 2012/10/03 2007/08/27 2006/06/15 2010/07/13 2006/06/15
US 2009-0007111 A1	2009/01/01	없음	
US 2013-0036093 A1	2013/02/07	AU 2010-333716 A1 AU 2010-333716 B2 EP 2513821 A1 EP 2513821 A4 WO 2011-072340 A1	2012/07/26 2016/06/16 2012/10/24 2015/05/27 2011/06/23
WO 2014-004747 A2	2014/01/03	EP 2864876 A2 EP 2864876 A4 US 2013-347131 A1 US 2015-007326 A1 US 2015-213264 A1 US 8745745 B2 US 9218489 B2 WO 2014-004747 A3	2015/04/29 2016/07/20 2013/12/26 2015/01/01 2015/07/30 2014/06/03 2015/12/22 2014/05/01
US 2005-0076155 A1	2005/04/07	US 7793287 B2	2010/09/07