(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0017429
(43) 공개일자 2020년02월18일

(51) 국제특허분류(Int. Cl.)
*G06F 21/56* (2013.01) *G06F 21/55* (2013.01)
*G06F 21/85* (2013.01)
(52) CPC특허분류
*G06F 21/565* (2013.01)
*G06F 21/554* (2013.01)
(21) 출원번호 10-2019-7038286
(22) 출원일자(국제) 2018년06월14일
심사청구일자 없음
(85) 번역문제출일자 2019년12월24일
(86) 국제출원번호 PCT/US2018/037560
(87) 국제공개번호 WO 2019/005496
국제공개일자 2019년01월03일
(30) 우선권주장
15/731,536 2017년06월26일 미국(US)

(71) 출원인
**나스 프리탐**
미국 캘리포니아주 91405 로스앤젤레스 14924 룰 스트리트
(72) 발명자
**나스 프리탐**
미국 캘리포니아주 91405 로스앤젤레스 14924 룰 스트리트
(74) 대리인
**특허법인아주김장리**

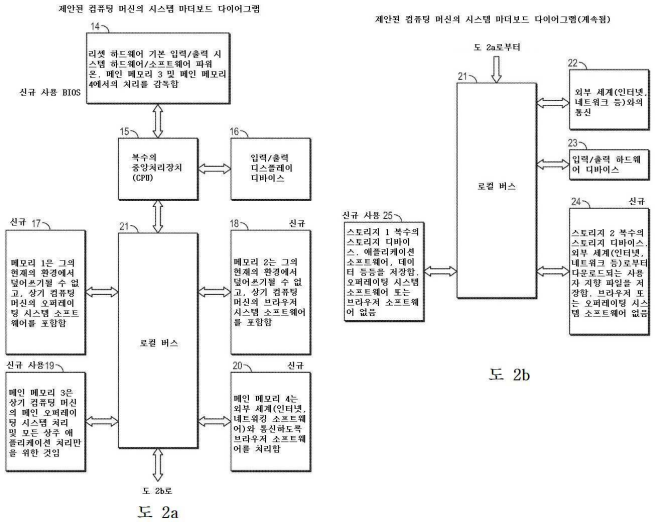
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **해커, 하이재커, 바이러스, 멀웨어 등의 염려 없이 정보를 처리, 조작, 수신, 송신 및 저장하기 위한 수단을 제공하는 안전하고 보안성이 있는 인터넷 또는 네트워크 연결 컴퓨팅 머신**

## (57) 요 약

소프트웨어 바이러스 및 멀웨어와 같은 외부 파일로부터의 문제점을 최소화하는 컴퓨팅 머신이 개시된다. 컴퓨팅 머신은 외부 동작과 분리되는 로컬 동작을 가지며, 그 결과 외부 파일은 로컬 동작과 관련되는 하드웨어로부터 분리된다. 로컬 측 하드웨어는 메모리 1, 메인 메모리 3, 및 스토리지 1 디바이스를 포함할 수도 있다. 외부 측 하드웨어는 메모리 2, 메인 메모리 4, 및 스토리지 2 디바이스를 포함할 수도 있다. 내부 측 하드웨어는 외부 측 하드웨어와 통신하지 않는다. 오퍼레이팅 시스템 소프트웨어는 메모리 1에 또는 스토리지 1 디바이스의 보안 파티션에 저장될 수도 있다. 로컬 애플리케이션 프로그램 및 로컬 동작으로부터의 데이터는 스토리지 1 디바이스에 저장될 수도 있다. 인터넷 브라우징 소프트웨어는 메모리 2에 또는 스토리지 2 디바이스의 보안 파티션에 저장될 수도 있다.

## 대 표 도



(52) CPC특허분류
*G06F 21/562* (2013.01)
*G06F 21/566* (2013.01)
*G06F 21/567* (2013.01)
*G06F 21/85* (2013.01)

# 명 세 서

## 청구범위

### 청구항 1

외부 동작으로부터 분리되는 로컬 동작을 갖는 컴퓨팅 머신으로서,

복수의 중앙처리장치;

메인 메모리 3으로서, 상기 복수의 중앙처리장치와 통신하는, 상기 메인 메모리 3;

상기 복수의 중앙처리장치와 통신하는 메인 메모리 4;

상기 복수의 중앙처리장치와 통신하는 데이터 및 애플리케이션 프로그램의 비일시적 저장을 위한 스토리지 1 디바이스; 및

상기 복수의 중앙처리장치와 통신하는 다른 데이터 및 다른 애플리케이션 프로그램의 비일시적 저장을 위한 스토리지 2 디바이스를 포함하되;

상기 메인 메모리 3 및 상기 스토리지 1 디바이스는 모두 동작적으로 독립적이며 상기 메인 메모리 4와 통신하지 않고 상기 스토리지 2 디바이스와도 통신하지 않으며;

상기 메인 메모리 3 및 상기 스토리지 1 디바이스는 모두 상기 로컬 동작을 위한 것이며; 그리고

상기 메인 메모리 4 및 상기 스토리지 2 디바이스는 모두 외부 동작을 위한 것이고; 상기 외부 동작은 상기 컴퓨팅 머신 외부로부터의 통신과 관련되고; 외부 동작으로부터의 외부 파일은 상기 메인 메모리 3으로부터 그리고 상기 스토리지 1 디바이스로부터 격리되는, 컴퓨팅 머신.

### 청구항 2

제1항에 있어서, 상기 스토리지 1 디바이스는 덮어쓰기될 수 없는 보안 파티션 영역을 포함하되; 상기 보안 파티션 영역은 메인 오퍼레이팅 시스템 소프트웨어의 비일시적 저장을 포함하고; 그리고 상기 스토리지 2 디바이스는 덮어쓰기될 수 없는 상이한 보안 파티션 영역을 포함하되; 상기 상이한 보안 파티션 영역은 적어도 하나의 인터넷 브라우징 애플리케이션 프로그램의 비일시적 저장을 포함하는, 컴퓨팅 머신.

### 청구항 3

제1항에 있어서, 상기 컴퓨팅 머신은 메인 오퍼레이팅 시스템 소프트웨어의 비일시적 저장을 포함하는 메모리 1을 더 포함하되; 상기 메모리 1은 상기 복수의 중앙처리장치와 통신하고; 그리고 상기 스토리지 2 디바이스는 덮어쓰기될 수 없는 보안 파티션 영역을 포함하되; 상기 보안 파티션 영역은 적어도 하나의 인터넷 브라우징 애플리케이션 프로그램의 비일시적 저장을 포함하고; 상기 메모리 1은 동작적으로 독립적이며 메인 메모리 4와 통신하지 않고 스토리지 2 디바이스와도 통신하지 않으며; 상기 메모리 1은 상기 로컬 동작을 위한 것이고; 상기 외부 파일은 상기 메모리 1과 격리되는, 컴퓨팅 머신.

### 청구항 4

제3항에 있어서, 상기 메모리 1은 덮어쓰기될 수 없는, 컴퓨팅 머신.

### 청구항 5

제1항에 있어서, 상기 스토리지 1 디바이스는 덮어쓰기될 수 없는 보안 파티션 영역을 포함하되; 상기 보안 파티션 영역은 메인 오퍼레이팅 시스템 소프트웨어의 비일시적 저장을 포함하고; 그리고 상기 컴퓨팅 머신은 적어도 하나의 인터넷 브라우징 애플리케이션 프로그램의 비일시적 저장을 포함하는 메모리 2를 더 포함하되; 상기 메모리 2는 상기 복수의 중앙처리장치와 통신하고; 상기 메인 메모리 3과 상기 스토리지 1 디바이스는 모두 동작적으로 독립적이고 상기 메모리 2와 통신하지 않으며; 그리고 상기 메모리 2는 외부 동작을 위한 것인, 컴퓨팅 머신.

**청구항 6**

제5항에 있어서, 상기 메모리 2는 덮어쓰기될 수 없는, 컴퓨팅 머신.

**청구항 7**

제1항에 있어서, 상기 컴퓨팅 머신은 메인 오퍼레이팅 시스템 소프트웨어의 비일시적 저장을 포함하는 메모리 1을 더 포함하되; 상기 메모리 1은 상기 복수의 중앙처리장치와 통신하고; 그리고 상기 컴퓨팅 머신은 적어도 하나의 인터넷 브라우징 애플리케이션 프로그램의 비일시적 저장을 포함하는 메모리 2를 더 포함하되; 상기 메모리 2는 상기 복수의 중앙처리장치와 통신하고; 상기 메모리 1은 동작적으로 독립적이며 상기 메모리 2와 통신하지 않고, 상기 메인 메모리 4와 통신하지 않으며, 상기 스토리지 2 디바이스와 통신하지 않고; 상기 메모리 1은 상기 로컬 동작을 위한 것이며; 그리고 상기 메모리 2는 상기 외부 동작을 위한 것이고; 상기 외부 파일은 상기 메모리 1과 격리되는, 컴퓨팅 머신.

**청구항 8**

제7항에 있어서, 상기 메모리 1과 상기 메모리 2는 각각 덮어쓰기될 수 없는, 컴퓨팅 머신.

**청구항 9**

제1항에 있어서, 상기 컴퓨팅 머신은 상기 복수의 중앙처리장치와의 통신을 용이하게 하기 위한 로컬 버스를 더 포함하되; 상기 로컬 버스는 상기 복수의 중앙처리장치와 통신하고; 그리고 상기 로컬 버스는 메모리 1; 메모리 2; 상기 메인 메모리 3; 상기 메인 메모리 4; 상기 스토리지 1 디바이스; 및 상기 스토리지 2 디바이스 중 적어도 두 개와 통신하고; 상기 메모리 1은 상기 로컬 동작을 위한 것이고; 상기 메모리 2는 상기 외부 동작을 위한 것이며; 상기 외부 파일은 상기 메모리 1과 격리되는, 컴퓨팅 머신.

**청구항 10**

외부 동작으로부터 분리되는 로컬 동작을 갖는 컴퓨팅 머신으로서,

복수의 중앙처리장치;

메인 오퍼레이팅 시스템 소프트웨어의 비일시적 저장을 포함하는 메모리 1로서, 상기 복수의 중앙처리장치와 통신하는, 상기 메모리 1;

적어도 하나의 인터넷 브라우징 애플리케이션 프로그램의 비일시적 저장을 포함하는 메모리 2로서, 상기 복수의 중앙처리장치와 통신하는, 상기 메모리 2;

메인 메모리 3으로서, 상기 복수의 중앙처리장치와 통신하는, 상기 메인 메모리 3;

상기 복수의 중앙처리장치와 통신하는 메인 메모리 4;

상기 복수의 중앙처리장치와 통신하는 데이터 및 애플리케이션 프로그램의 비일시적 저장을 위한 스토리지 1 디바이스; 및

상기 복수의 중앙처리장치와 통신하는 다른 데이터 및 다른 애플리케이션 프로그램의 비일시적 저장을 위한 스토리지 2 디바이스를 포함하되;

상기 메모리 1, 상기 메인 메모리 3 및 상기 스토리지 1 디바이스는 모두 동작적으로 독립적이며 상기 메모리 2와 통신하지 않고, 상기 메인 메모리 4와 통신하지 않으며, 상기 스토리지 2 디바이스와 통신하지 않고;

상기 메모리 1, 상기 메인 메모리 3 및 상기 스토리지 1 디바이스는 모두 상기 로컬 동작을 위한 것이며; 그리고

상기 메모리 2, 상기 메인 메모리 4 및 상기 스토리지 2 디바이스는 모두 상기 외부 동작을 위한 것이고; 상기 외부 동작은 상기 컴퓨팅 머신 외부로부터의 통신과 관련되고; 외부 동작으로부터의 외부 파일은 상기 메모리 1로부터, 상기 메인 메모리 3으로부터, 그리고 상기 스토리지 1 디바이스로부터 격리되는, 컴퓨팅 머신.

**청구항 11**

제10항에 있어서, 상기 컴퓨팅 머신은 상기 복수의 중앙처리장치와의 통신을 용이하게 하기 위한 로컬 버스를

더 포함하되; 상기 로컬 버스는 상기 복수의 중앙처리장치와 통신하고; 그리고 상기 로컬 버스는 상기 메모리 1, 상기 메모리 2, 상기 메인 메모리 3, 상기 메인 메모리 4, 상기 스토리지 1 디바이스 및 상기 스토리지 2 디바이스와 통신하는, 컴퓨팅 머신.

**청구항 12**

제10항에 있어서, 상기 메모리 1과 상기 메모리 2는 각각 덮어쓰기될 수 없는, 컴퓨팅 머신.

**청구항 13**

제10항에 있어서, 상기 메모리 1와 상기 메모리 2는 각각 판독 전용 메모리인, 컴퓨팅 머신.

**청구항 14**

제10항에 있어서, 상기 컴퓨팅 머신의 초기 전력 인가(power up) 이후, 상기 컴퓨팅 머신의 BIOS는, 상기 복수의 중앙처리장치에 의한 동작 및 액세스를 위해, 상기 메인 오퍼레이팅 시스템 소프트웨어로 하여금, 상기 메모리 1로부터 상기 메인 메모리 3으로 복사되게 하는, 컴퓨팅 머신.

**청구항 15**

제10항에 있어서, 상기 컴퓨팅 머신 초기 전력 인가 이후, 상기 컴퓨팅 머신의 BIOS는, 상기 복수의 중앙처리장치에 의한 동작 및 액세스를 위해, 상기 적어도 하나의 인터넷 브라우징 애플리케이션 프로그램으로 하여금, 메모리 2로부터 상기 메인 메모리 4로 복사되게 하는, 컴퓨팅 머신.

**청구항 16**

제10항에 있어서, 상기 스토리지 1 디바이스는: 상기 애플리케이션 프로그램 또는 상기 데이터 파일 중 하나 이상을 비일시적으로 저장하는, 컴퓨팅 머신.

**청구항 17**

제10항에 있어서, 상기 스토리지 2 디바이스는, 상기 다른 애플리케이션 프로그램 또는 상기 다른 데이터 파일 중 하나 이상을 비일시적으로 저장하는, 컴퓨팅 머신.

**청구항 18**

제10항에 있어서, 상기 컴퓨팅 머신은, 상기 복수의 중앙처리장치와 통신하는 입력/출력 디스플레이 디바이스를 더 포함하는, 컴퓨팅 머신.

**청구항 19**

외부 동작과 분리되는 로컬 동작을 갖는 단일의 컴퓨팅 머신을 위해 컴퓨팅하는 방법으로서,

입력 및 출력 디바이스를 개시하는 파워 온 입력을 수신하는 단계;

복수의 중앙처리장치가 메인 오퍼레이팅 시스템 소프트웨어에 액세스하도록 상기 메인 오퍼레이팅 시스템 소프트웨어를 메모리 1로부터 메인 메모리 3으로 복사하는 단계로서, 상기 메모리 1은 덮어쓰기될 수 없는, 상기 메인 오퍼레이팅 시스템 소프트웨어를 복사하는 단계;

적어도 하나의 인터넷 브라우징 애플리케이션 프로그램을 메모리 2로부터 메인 메모리 4로 복사하는 단계로서, 상기 복수의 중앙처리장치는 상기 적어도 하나의 인터넷 브라우징 애플리케이션 프로그램에 액세스하고, 상기 메모리 2는 덮어쓰기될 수 없으며 상기 메모리 1과 상기 메인 메모리 3은 동작적으로 독립적이고 분리되며 상기 메모리 2와 통신하지 않으며 상기 메인 메모리 4와 통신하지 않으며;

상기 메인 오퍼레이팅 시스템 소프트웨어 및 상기 적어도 하나의 인터넷 브라우징 애플리케이션 프로그램의 감독이 상기 단일의 컴퓨팅 머신의 BIOS에 의해 수행되는, 상기 적어도 하나의 인터넷 브라우징 애플리케이션 프로그램을 복사하는 단계;

상기 메인 오퍼레이팅 시스템 소프트웨어의 감독 하에 상기 복수의 중앙처리장치가 애플리케이션 소프트웨어에 액세스하는 것에 의해 상기 로컬 동작을 처리하는 단계로서; 상기 애플리케이션 소프트웨어 및 상기 메인 오퍼레이팅 시스템 소프트웨어 둘 다는 상기 메인 메모리 3에서 처리되고; 상기 애플리케이션 소프트웨어는 스토리

지 1 디바이스에 비일시적으로 저장되는, 상기 상기 로컬 동작을 처리하는 단계; 및

상기 적어도 하나의 인터넷 브라우징 애플리케이션 프로그램의 감독 하에 상기 복수의 중앙처리장치가 외부 애플리케이션 소프트웨어에 액세스하는 것에 의해 상기 외부 동작을 처리하는 단계로서; 상기 외부 애플리케이션 소프트웨어 및 상기 적어도 하나의 인터넷 브라우징 애플리케이션 프로그램 둘 다는 상기 메인 메모리 4에서 처리되고; 상기 외부 애플리케이션 소프트웨어는 스토리지 2 디바이스에 비일시적으로 저장되고; 상기 스토리지 1 디바이스는 동작적으로 독립적이며 분리되고 상기 스토리지 2 디바이스와 통신하지 않는, 상기 외부 동작을 처리하는 단계를 포함하되;

상기 단일의 컴퓨팅 머신은 상기 메모리 1, 상기 메인 메모리 3, 상기 스토리지 1 디바이스, 상기 메모리 2, 상기 메인 메모리 4 및 상기 스토리지 2 디바이스를 포함하는, 단일의 컴퓨팅 머신을 위해 컴퓨팅하는 방법.

**청구항 20**

제19항에 있어서, 상기 애플리케이션 소프트웨어와 관련되는 데이터 파일은 상기 스토리지 1 디바이스에 비일시적으로 저장되며; 그리고 상기 적어도 하나의 인터넷 브라우징 애플리케이션 프로그램과 관련되는 또는 상기 외부 애플리케이션 소프트웨어와 관련되는 다른 데이터 파일은 상기 스토리지 2 디바이스에 비일시적으로 저장되되; 상기 다른 데이터 파일은 상기 메모리 1로부터, 상기 메인 메모리 3으로부터, 그리고 상기 스토리지 1 디바이스로부터 격리되는, 단일의 컴퓨팅 머신을 위해 컴퓨팅하는 방법.

## *발명의 설명*

### *기 술 분 야*

[0001] 우선권 통지

[0002] 본 출원은 2017년 6월 26일자로 출원된 미국 특허 출원 제15/731,536호에 대한 우선권을 주장하는데, 그 특허 출원의 개시내용은 참조에 의해 그들 전체가 본 명세서에 통합된다.

[0003] 저작권 및 상표 고지

[0004] 본 명세서에 언급되는 특정한 상표(mark)는 본 출원인 또는 양수인과 제휴한 또는 제휴하지 않은 제3자의 일반적인 법적 상표 또는 등록 상표일 수도 있다. 이들 상표의 사용은 예시적인 것이며, 그러한 상표와만 관련되는 재료로 본 발명의 범주를 설명하는 것으로 또는 제한하도록 해석되지 않아야 한다.

[0005] 본 발명의 기술적 분야

[0006] 본 발명은 일반적으로, 인터넷, 네트워크(들) 등과 같은 외부 세계 통신에 연결될 수 있는 또는 그들과 연결되는 컴퓨팅 머신에 관한 것으로; 그러한 컴퓨팅 머신은, 개인용 컴퓨터, 랩탑, 서버, 메인프레임 컴퓨터, 태블릿, 전화기, 셀 또는 이동 전화, TV, 보안 시스템, 원격 데이터 센서 등을 포함할 수도 있지만, 그러나 그들로 제한되지는 않을 수도 있다.

### *배 경 기 술*

[0007] 본 출원 목적을 위해, 컴퓨팅 머신은 인터넷 또는 네트워크(들)를 통해 정보를 계산, 저장, 조작, 수신 및/또는 송신하는 인터넷 또는 네트워크 연결 디바이스(Internet or Network connected device)로서 정의될 수도 있다. 인터넷 또는 네트워크 연결 컴퓨팅 머신의 몇몇 예는 다음의 것을 포함할 수도 있지만, 그러나 이들로 제한되지는 않을 수도 있다: 개인용 컴퓨터, 컴퓨터 랩탑, 컴퓨터 서버, 메인프레임 컴퓨터, 셀 폰, 태블릿 등.

[0008] 예를 들면, 개인용 컴퓨터는 컴퓨팅에서 무거울 수도 있고 정보의 입력 또는 출력에서 가벼울 수도 있다. 또는 컴퓨팅 머신은, 종종, 개인용 컴퓨터의 소형화된 버전에 불과한, 인터넷 연결 랩탑 컴퓨터일 수도 있다. 또는 컴퓨팅 머신은, 입력 및 출력 기능에서 무거울 수도 있고 컴퓨팅 기능에서 가벼울 수도 있는 인터넷 연결 서버 컴퓨터일 수도 있다. 또는 컴퓨팅 머신은, 음성, 데이터 및/또는 비디오를 수신 및/또는 송신하기 위해 사용될 수도 있는, 인터넷 연결 이동 전화 또는 셀 폰일 수도 있다. 또는 컴퓨팅 머신은, 예컨대 TV 및 게임 등을 위해 사용되는 인터넷 연결 엔터테인먼트 디바이스일 수도 있다. 또는 컴퓨팅 머신은, 정보 처리에서 무겁고 입력/출력에서 매우 가벼운, 인터넷 연결 메인프레임 컴퓨터일 수도 있다. 또는 컴퓨팅 머신은, 컴퓨터 랩탑의 제한적이고 가벼운 버전일 수도 있는 컴퓨터 태블릿일 수도 있다. 또는 컴퓨팅 머신은, 물리적 위치를 모니터링하기 위해 및/또는 침입을 검출하기 위해 인터넷 또는 네트워크에 연결될 수도 있는 기업 및 홈 보안 시스템

(business & home security system)일 수도 있다. 또는 컴퓨터는, 원격 위치에서 데이터를 수집하기 위한 인터넷 또는 네트워크 연결 디바이스일 수도 있는 원격 데이터 센서일 수도 있다.

[0009] 현재의 인터넷 또는 네트워크 연결 컴퓨팅 머신의 통상적인 동작 양태는 다음과 같을 수도 있다. 현존하는 컴퓨팅 머신의 "POWER ON(파워 온)" 버튼(또는 등가물)은 현존하는 컴퓨팅 머신의 마더보드에 존재하는 BIOS(Basic input and output system: 기본 입력/출력 시스템)와 소프트웨어 패키지를 기동시킨다. 이 소프트웨어는 컴퓨팅 머신에 내장되는 모든 입력/출력 디바이스를 초기화한다(도 1의 항목 5 참조). 일단 모든 입력/출력 디바이스가 동작하게 만들어지면, 오퍼레이팅 시스템은 스토리지 디바이스(들)(도 1, 항목 13)로부터 메인 메모리(도 1, 항목 8)로 복사된다. 상기 현존하는 컴퓨팅 머신의 제어는, 메인 메모리(도 1, 항목 8)에 상주하는 오퍼레이팅 시스템 소프트웨어로 전가된다. 오퍼레이팅 시스템 소프트웨어는 인터넷 브라우저 또는 네트워크 소프트웨어 및/또는 여러 애플리케이션 소프트웨어를 실행한다. 실행 준비가 된 또는 실행하고 있는 다양한 애플리케이션 소프트웨어 패키지를 보여주는 여러 개의 윈도우가 모니터(도 1, 항목 7) 상에서 나타난다. 이것은 인터넷 브라우저, 네트워크 소프트웨어 및 임의의 다른 사전 지정된 애플리케이션 소프트웨어를 포함한다. "POWER ON" 버튼(도 1, 항목 5)를 사용하기 이전에, 모든 소프트웨어, 오퍼레이팅 시스템 소프트웨어, 인터넷 브라우저 소프트웨어, 애플리케이션 소프트웨어 등이 스토리지 디바이스(도 1, 항목 13) 상에 있다. 시장에는 마이크로소프트 윈도우(Microsoft Windows), 애플(Apple) 오퍼레이팅 시스템, 시스템 10(System 10), (엑스 윈도우)(X-Windows) 등과 같은 여러 오퍼레이팅 시스템이 있다. 시장에는 구글(Google), 야후(Yahoo), 빙(Bing), 사파리(Safari), 모질라 파이어폭스(Mozilla Firefox) 등과 같은 여러 인터넷 브라우저가 있다.

[0010] 사용자는 이 현존하는 컴퓨팅 머신을 동작시켜 그의/그녀의 처리를 행한다. 일단 사용자가 처리를 마치면, 사용자는 현존하는 컴퓨팅 머신을 턴오프한다. 모든 시스템 소프트웨어, 오퍼레이팅 시스템 소프트웨어, 인터넷 브라우저 소프트웨어, 애플리케이션 소프트웨어 등은, 데이터 파일(이것은 현재의 세션에서 사용자에 의해 생성되는 새로운 또는 수정된 데이터를 포함함)과 함께, 스토리지 디바이스(도 1, 항목 13)로 다시 자동적으로 복사된다.

[0011] 그러한 현존하는 인터넷 또는 네트워크 연결 컴퓨팅 머신은 많은 문제점을 가지고 있다. 그러한 현존하는 인터넷 또는 네트워크 연결 컴퓨팅 머신의 무단 변경(tampering) 또는 해킹 또는 하이재킹의 수 많은 문제점이 있다. 소프트웨어 바이러스 및 멀웨어가 인터넷을 통해 현존하는 컴퓨팅 머신에 주입되고, 그에 의해, 현존하는 컴퓨팅 머신을 차단 또는 손상시켜, 그것이 올바르게 기능할 수 없게 만들 수도 있다. 때로는 현존하는 컴퓨팅 머신은 복수(vengeance) 목적으로 하이재킹될 수도 있다. 인터넷을 통해 설치되는 멀웨어는 현존하는 컴퓨팅 머신의 제어를 취하여, 패스워드 등을 포함하는 사용자 개인 정보를 훔칠 수도 있다. 그 다음, 사기꾼(crook)은 신용 카드 사기, 은행 계좌 사기 등을 저지를 수도 있다. 일단 개인 식별 정보가 잘못된 사람의 손에 있으면, 그것은 사용되어 피해자에 대한 문제점 - 여기에서 언급하기에는 너무 많음 - 전체를 생성하게 된다. 다양한 기업, 은행, 대학, 의료 기관, 도시, 주, 및 연방 정부 부서가 해킹의 피해자였다. 말할 필요도 없이, 문제점은 방대하고 이런 식으로 매년 수십억 달러가 손실된다.

[0012] 다양한 현재 사용되는 다양한 오퍼레이팅 시스템(현존하는 컴퓨팅 머신을 제어 및 동작시키는 소프트웨어)은 수천 마일 떨어진 누군가에 의한 현존하는 컴퓨팅 머신의 원격 제어를 허용할 수도 있다. 현존하는 컴퓨팅 머신의 내부 작업에 대해 잘 알고 있는 누군가가 그러한 원격 액세스를 사용하여 이들 현존하는 컴퓨팅 머신으로부터 정보를 훔치기는 매우 쉽다.

[0013] 외부 세계에 연결되는 인터넷 또는 네트워크를 통해 바이러스 또는 멀웨어가 시스템 안으로 침입할 수 있는 많은 방식이 존재한다. 일단 바이러스 또는 멀웨어가 현존하는 컴퓨팅 머신을 장악하면, 그것을 제거하는 것은 매우 어렵고 시간 소모적이다. 대부분의 사용자 및 기업은 문제점을 핸들링할 수 없다. 문제점을 제거하기 위해, 그들은 많은 돈, 다른 리소스, 및 시간을 지출한다. 이들 문제점을 해결하기 위한 서비스를 제공하는 많은 보안 회사가 존재한다. 그들은 때로는 일을 하고, 때로는 그들은 일을 하지 않는다. 많은 경우에, 현존하는 컴퓨팅 머신 상의 모든 것이 삭제되어야 하고 모든 소프트웨어가 다시 설치되어야 하며, 결국 문제점이 반복해서 발생한다.

[0014] 해커는 또한, 현존하는 컴퓨팅 머신을 제어를 취하고, 개인 정보를 훔치고, 현존하는 컴퓨팅 머신을 동작 불가능하게 만들며, 그들의 제어를 해제할 배상금(ransom)을 요구할 수도 있다.

[0015] 현재의 오퍼레이팅 시스템은, 선한 목적 및 나쁜 목적을 위해 소프트웨어를 어설프게 만지기(tinker) 위해 사용되는 내장 백도어를 갖는다.

[0016] 본 기술 분야에서는 이들 문제점이 없는 새로운 타입의 인터넷 또는 네트워크 연결 컴퓨팅 머신에 대한 필요성이 존재한다.

[0017] 본 발명이 개발된 것은 이들 목적 때문이다.

## 발명의 내용

[0018] 크게 개선되고 보안이 이루어진 컴퓨팅 머신은 인터넷 및 또는 네트워크 등에 연결될 때 자신의 동작에 대한 하이재킹 및 무단 변경의 문제점을 해결한다.

[0019] 본 발명은 어떠한 방식으로든 컴퓨팅 머신의 유효성을 조금도 감소시키지는 않는다. 본 발명의 실시형태는 개인용 컴퓨터, 컴퓨터 랩탑, 컴퓨터 서버, 메인프레임 컴퓨터, 임의의 종류의 셀 폰 등과 같은 디바이스에 적용된다. 본 발명의 실시형태는 인터넷 및/또는 네트워크를 통해 정보를 컴퓨팅 또는 전송하는 임의의 컴퓨팅 머신에 적용된다.

[0020] 새로운 컴퓨팅 머신은 디바이스가 바이러스 및/또는 멀웨어에 감염되게 되면, 수많은 수리 시간, 돈, 좌절, 성가심, 자극, 및 충격의 사용자 손실을 절약한다. 새로운 컴퓨팅 머신은 또한, 사용자의 정보가 안전하고 건전하다는 그리고 그들이 신뢰 가능한 컴퓨팅 머신을 갖추고 있다는 편안함과 마음의 평화를 제공한다. 드문 감염의 경우, 그 초기에 문제점을 해결하는 사용자 친화적인 소프트웨어가 존재한다.

[0021] 이들 제안된 새로운 컴퓨팅 머신은, 데스크탑, 개인용 컴퓨터(Personal Computer: PC), 랩탑, 서버, 메인프레임, 이동 전화 또는 셀 폰, 전화기, 엔터테인먼트 디바이스, 원격 감지 디바이스, 및/또는 등등에 직접적으로 적용 가능하다. 즉, 그러한 새로운 컴퓨팅 머신은 데스크탑, 개인용 컴퓨터(PC), 랩탑, 서버, 메인프레임, 이동 전화 또는 셀 폰, 전화기, 엔터테인먼트 디바이스, 원격 감지 디바이스, 및/또는 등등으로서 구현될 수도 있다. 그러한 데스크탑 또는 개인용 컴퓨터(PC)는, 인터넷 또는 외부 네트워크에 연결될 수도 있고; 컴퓨팅 면에서 무거울 수도 있고 데이터의 입력/출력의 송신에서 가벼울 수 있다. 그러한 랩탑 컴퓨터는 인터넷 또는 외부 네트워크에 연결될 수도 있고 데스크탑 또는 개인용 컴퓨터의 소형 버전일 수도 있으며; 컴퓨팅 면에서 무거울 수도 있고 데이터의 입력/출력의 송신에서 가벼울 수 있다. 그러한 서버는 인터넷 또는 외부 네트워크에 연결될 수도 있고 컴퓨팅 면에서 가볍고 데이터의 입력/출력의 송신에서 무거울 수도 있다. 그러한 서버는, 현장의(onsite) 또는 현장 밖의(offsite) 위치에 위치되는 사용자에게 정보를 배포하기 위해 기업 및 모든 종류의 조직에서 사용될 수도 있다. 그러한 메인프레임은 인터넷 또는 외부 네트워크에 연결될 수도 있고 컴퓨팅 면에서 무겁거나 또는 가벼울 수도 있으며, 이 컴퓨팅 머신의 사용에 따라 데이터의 입력/출력의 송신에서 무겁거나 또는 가벼울 수도 있다. 그러한 이동 전화 또는 셀 폰 또는 유선 전화는 인터넷 또는 외부 네트워크에 연결될 수도 있으며, 음성 및 데이터의 입력/출력의 송신에서 무거울 수도 있고 데이터 컴퓨팅에서 가벼울 수도 있다. 그러한 엔터테인먼트 디바이스는 TV, 컴퓨팅 태블릿, 게이밍 디바이스 등을 포함할 수도 있고; 인터넷 또는 네트워크에 연결될 수도 있다. 그러한 원격 감지 디바이스는 인터넷 또는 네트워크에 연결될 수도 있다. 인터넷 또는 네트워크에 연결되어 데이터를 계산하거나 또는 상이한 물리적 위치로 그리고 상이한 물리적 위치로부터 데이터를 송신하는 임의의 과거의, 현재의 또는 미래의 그러한 컴퓨팅 머신은 본 발명의 범위 내에 속하는 것으로 고려된다. 네트워크는 전자적 수단에 의해 두 개 이상의 별개의 물리적 위치로의 그리고 그 물리적 위치로부터의 데이터의 송신을 용이하게 하기 위한 시스템으로서 정의된다.

[0022] 이들 고려되는 새로운 컴퓨팅 머신의 이점은 다음의 것을 포함할 수도 있다: 새로운 컴퓨팅 머신은 손상될 수 없다; 새로운 컴퓨팅 머신은 일시적으로 또는 영구적으로 쓸모 없게 될 수 없다; 새로운 컴퓨팅 머신은 하이재킹될 수 없다; 새로운 컴퓨팅 머신은 원격으로 무단 변경될 수 없다; 메인 오퍼레이팅 시스템 소프트웨어는, 인터넷, 다른 네트워크 등과 같은 외부 통신 디바이스를 통해 임의의 외부 침입자에 의해 수정, 손상, 또는 삭제될 수 없다; 인터넷 브라우저 소프트웨어는, 인터넷, 다른 네트워크 등과 같은 외부 통신 디바이스를 통해 임의의 외부 침입자에 의해 수정, 손상, 또는 삭제될 수 없다; 및/또는 등등.

[0023] 몇몇 드문 경우에 바이러스 또는 멀웨어가 상기 새로운 컴퓨팅 머신 안으로 몰래 들어가는 경우, 그것은, 브라우저 시스템 소프트웨어에는 영향을 줄 수도 있지만, 그러나, 메인 오퍼레이팅 시스템 소프트웨어에는 어떤 식으로든 영향을 끼치지 않을 것이다. 그것이 발생하는 경우, 사용자 친화적인 시스템 소프트웨어는 문제점을 분석하고, 바이러스 또는 멀웨어 파일을 식별 및 삭제하고, 미래의 다운로드를 위해, 그러한 파일 및 그것이 유래했던 IP 어드레스를 차단한다. 사용자는 어떤 국가 및 어떤 IP 어드레스는 유입이 허용되고 어떤 것은 금지되는지에 대한 제어를 갖는다.

[0024] 새로운 컴퓨팅 머신에 대해 설명되는 셋업 및 프로세스는 보통 사용자에게 보안성 및 마음의 평화를 제공할 것

이다. 기업은, 개인 또는 금융 정보와 같은 그들의 기밀 정보가 해커 등을 포함하는 범죄자로부터 보호된다는 확신을 가질 것이다. 은행 계좌, 의료 정보와 같은 개인 기록, 연방 및 주 소득세 정보와 같은 정부 정보, 사회 보장 정보, 사용자 및 기업의 신용 카드 정보는 안전할 것이다.

[0025] 독자는, 본 명세서에서 설명되는 바와 같이, 인터넷, 네트워크, 원격 감지 디바이스, 이동 전화 또는 셀 폰 등과 같은 외부 세계 통신에 연결되는 임의의 현재의 또는 미래의 컴퓨팅 머신 상에서 사용자의 정보를 보호하기 위해 본 발명이 사용될 수 있다는 것을 알 것이다.

[0026] 게다가, 소프트웨어 바이러스, 멀웨어, 스파이웨어, 해커 등이 사용자의 정보를 무단 변경, 변경, 또는 도용하려고 할 때 사용자는 보호된다.

[0027] 새로운 컴퓨팅 머신 및 그것의 프로세스는, 본 명세서에서 설명되는 바와 같이, 바이러스 및 멀웨어 시도의 가시적인 증거 및 흔적을 생성할 것이다.

[0028] 외부 세계 통신(예를 들면, 인터넷, 네트워크 등)은, 모든 컴퓨팅 머신의 애플리케이션, 데이터 파일, 및 메인 소프트웨어와 함께, 상기 컴퓨팅 머신의 오퍼레이팅 시스템에 액세스할 수 없다.

[0029] 임의의 바이러스, 멀웨어 또는 해커의 소프트웨어는, 혹시라도 그것이 브라우저 측을 통해 그러저럭 진입하면, 격리될 것이고 악성 소프트웨어는 자체적으로 실행하도록 허용되지 않는다.

[0030] 현존하는 컴퓨팅 머신과 비교하여 본 발명의 상기의 이점 때문에, 사용자는 흘깃거리는 눈으로부터 그들의 개인 정보가 안전하게 된다는 마음의 평화를 즐길 수 있다.

[0031] 본 발명은 다음과 같이 시간과 비용을 절약한다:

[0032] - 보안(예를 들면, 바이러스 방지 및 제거) 소프트웨어 및 서비스에 대한 월별 또는 연간 구독에 대한 필요성을 최소화함;

[0033] - 데이터 파일을 복구하는 데 소요되는 무수한 시간과 비용을 최소화함;

[0034] - 바이러스, 멀웨어, 스파이웨어, 데이터 파일의 복구 또는 복원에 대한 현지 수리점 또는 기술 지원 서비스에 대해 소요되는 비용을 최소화함;

[0035] - 바이러스를 제거하고 컴퓨팅 머신을 공장 설정 또는 바이러스가 디바이스를 감염시키고 시스템을 손상시키거나 또는 원치 않는 활동을 유발한 때 이전의 상태로 복원하기 위해 하드 드라이브를 다시 포맷하는 데 소요되는 수많은 시간 또는 비용을 최소화함;

[0036] - 달리 절대 복구 불가능할 수도 있는 중요한 파일이 손실되는 것을 방지함;

[0037] - 애플리케이션, 메인 오퍼레이팅 시스템 및 데이터 파일이 브라우저 측 상호 작용과는 분리되기 때문에, 사용자 시스템을 하이재킹한 해커로부터의 배상금 요구를 방지함;

[0038] - 브라우저 측이 악성 소프트웨어로 감염되는 경우, 악성 소프트웨어가 완전히 제거되도록 사용자는 컴퓨터를 종료하여 메모리를 깨끗하게 삭제할 수 있음;

[0039] - 브라우저 측은 메인 오퍼레이팅 시스템 소프트웨어 측(중요한 애플리케이션 및 데이터 파일을 포함함)과는 독립적으로 동작하고 결과적으로 상기 컴퓨팅 디바이스는 항상 동작함;

[0040] - 악의적인 소프트웨어가 브라우저 저장 영역 안으로 들어갈 수 있는 경우, 그것은 격리되고 자체적으로 실행하는 것이 금지됨; 및

[0041] - 컴퓨팅 머신은, 브라우저 처리 측 및 메인 애플리케이션 처리 측의 전용 메모리 및 전용 스토리지 때문에 더 빠른 처리를 제공한다.

## *도면의 간단한 설명*

[0042] 도면에서의 엘리먼트는, 그들의 명확성을 향상시키고 본 발명의 다양한 실시형태의 이해를 향상시키기 위해 반드시 일정한 비율로 묘사되는 것은 아니다. 더구나, 본 발명의 다양한 실시형태에 대한 명확한 견해를 제공하기 위해 업계에 공통적이고 널리 이해되는 것으로 알려진 엘리먼트는 묘사되지 않는다. 상세한 설명에 수반되는 도면은 다음과 같이 간략하게 설명될 수 있다:

도 1은 통상적인 최신의 개인용 컴퓨터, 랩탑, 또는 서버에 대한 현존하는 컴퓨팅 머신의 설계의 블록도이다.

도 2는 본 발명의 한 실시형태에 따른 제안된 컴퓨팅 머신의 블록도이다.

도 3은 본 발명의 한 실시형태에 따른 제안된 상기 컴퓨팅 머신의 동작의 블록도 플로우차트이다.

도 4는 제안된 컴퓨팅 머신의 실시형태 1의 블록도이다.

도 5는 제안된 컴퓨팅 머신의 실시형태 2의 블록도이다.

도 6은 제안된 컴퓨팅 머신의 실시형태 3의 블록도이다.

참조 번호 목록/일람

항목 5 기본 입력/출력 소프트웨어(BIOS) 파워 온(Power On)

항목 6 중앙처리장치(들)

항목 7 입력/출력 디스플레이 디바이스

항목 8 메인 메모리

항목 9 마더보드의 백도어 제어

항목 10 로컬 버스

항목 11 외부 세계와의 통신

항목 12 입력/출력 하드웨어 디바이스

항목 13 스토리지

항목 14 신규 사용 BIOS

항목 15 중앙처리장치(들)

항목 16 입력/출력 디스플레이 디바이스

항목 17 메모리 1

항목 18 메모리 2

항목 19 메인 메모리 3

항목 20 메인 메모리 4

항목 21 로컬 버스

항목 22 외부 세계와의 통신

항목 23 다양한 입력/출력 디바이스 하드웨어

항목 24 스토리지 2

품목 25 스토리지 1(Storage One)

항목 26 감시 BIOS 소프트웨어

항목 27 입력/출력 디바이스 하드웨어

항목 28 메모리 1

항목 29 메모리 2

항목 30 메모리 1을 복사하기 위한 커맨드

항목 31 메모리 2를 복사하기 위한 커맨드

항목 32 메인 메모리 3이 오퍼레이팅 시스템을 수신함

항목 33 메인 메모리 4가 브라우저 소프트웨어를 수신함

항목 34 상기 머신이 사용자의 커맨드를 처리함

항목 35 스토리지 1

품목 36 스토리지 2

항목 37 메모리 3이 세션의 파일을 저장함

항목 38 메모리 4가 사용자 승인 파일을 저장함

항목 39 사용자가 로그 아웃함

항목 40 파워 오프 시퀀스

항목 41 파워 오프

## *발명을 실시하기 위한 구체적인 내용*

[0043] 본 발명의 다수의 실시형태 및 애플리케이션을 다루는 다음의 논의에서, 본 발명이 실시될 수도 있는 특정한 실시형태의 묘사가 예시로서 이루어지는, 본 발명의 일부를 형성하는 첨부의 도면에 대한 참조가 이루어진다. 다른 실시형태가 활용될 수도 있고 본 발명의 범위를 벗어나지 않고 변경이 이루어질 수도 있다는 것이 이해되어야 한다.

[0044] 제안된 새로운 컴퓨팅 머신의 본 발명의 바람직한 실시형태는 도 2(하드웨어 설계) 및 도 3(동작)에서 예시된다. 이 새로운 컴퓨팅 머신은 신규 사용 BIOS(기본 입출력 시스템)(도 2, 항목 14 참조)를 구비한다. 리셋 하드웨어 "파워 온" 외에도, 이 신규 사용 BIOS는 메인 메모리 3(도 2, 항목 19) 및 메인 메모리 4(도 2, 항목 20)에서의 처리를 감독한다. 이 새로운 컴퓨팅 머신은, 신규 사용 BIOS(도 2, 항목 14), 입력/출력 디스플레이 디바이스(도 2, 항목 16), 및 로컬 버스(도 2, 항목 21)에 연결되는 복수의 중앙처리장치(central processing unit: CPU)(도 2, 항목 15)를 포함한다. 로컬 버스(도 2, 항목 21)는 CPU와의 다양한 하드웨어(예를 들면, 항목 23 및/또는 항목 27)의 통신을 용이하게 한다. 이 새로운 컴퓨팅 머신은, 자신의 현재의 환경에서 덮어쓰기 또는 변경될 수 없는 복수의 메모리 디바이스인 메모리 1(도 2, 항목 17) 및 메모리 2(도 2, 항목 18)를 구비한다. 다시 말하면, 일단 이 메모리가 전자 디바이스 상에 설치되면, 그것은 사용자의 승인 없이는 임의의 다른 디바이스 또는 소프트웨어에 의해 덮어쓰기 또는 변경될 수 없다. 메모리 1(도 2, 항목 17)은 상기 새로운 컴퓨팅 머신의 메인 오퍼레이팅 시스템을 포함한다. 메모리 2(도 2, 항목 18)는 하나 이상의 공급 업체로부터의 임의의 인터넷 브라우저 소프트웨어를 포함한다.

[0045] 이 새로운 컴퓨팅 머신은 두 세트의 메인 메모리를 사용한다. 한 세트의 메인 메모리 3(도 2, 항목 19)는 메인 컴퓨터 처리를 위해 배타적으로 사용된다. 다른 세트의 메인 메모리 4(도 2, 항목 20)는 임의의 인터넷 브라우저 또는 네트워크(들) 처리를 위해 배타적으로 사용된다. 이들 복수의 메모리 세트(도 2, 항목 19 및 도 2, 항목 20)는 서로 연결되지 않는다. 그들은 서로 완전히 독립적이며 서로에게 또는 서로로부터 정보를 전송 또는 수신할 수 없다.

[0046] 이 새로운 컴퓨팅 머신은 내부적으로 및/또는 외부적으로 연결되는 스토리지 디바이스(하드 드라이브 등등)의 복수의 세트를 구비한다. 한 세트의 스토리지 디바이스(들)인 스토리지 1(도 2, 항목 25)은 상기 새로운 컴퓨팅 머신의 로컬 처리의 배타적인 사용을 위한 것이다. 스토리지 1(항목 25)은 모든 종류의 애플리케이션 소프트웨어 패키지 및 관련된 또는 독립형 데이터 파일을 포함한다. 스토리지 디바이스(들)의 다른 세트인 스토리지 2(도 2, 항목 24)는 임의의 인터넷 브라우저 또는 네트워크(들)의 배타적인 사용을 위한 것이다. 스토리지 2(도 2, 항목 24)는, 인터넷 브라우징을 용이하게 하는 데 필요한 모든 파일을 포함하지만 그러나 인터넷 브라우저 소프트웨어 패키지는 포함하지 않는다. 스토리지 2(도 2, 항목 24)는 다운로드된 인터넷 파일을 포함할 수도 있다. 스토리지 1(도 2, 항목 25), 및 스토리지 2(도 2, 항목 24)는 서로 연결되지 않으며, 정상적인 동작 환경하에서 서로에게 또는 서로로부터 어떠한 정보도 전송될 수 없다.

[0047] 임의의 다운로드된 실행 파일은 식별 목적을 위해 전송자의 IP 어드레스로 태그가 지정되고 및 또는 다운로드된 실행 파일 폴더에 격리될 것이다. 인터넷 다운로드 가능 파일은 자동적으로 또는 혼자 힘으로 실행될 수 없다. 인터넷 다운로드 가능 파일은, 사용자가 특별히 보호된 커맨드를 사용하여 실행을 개시하는 경우에만 실행될 수 있다.

[0048] 도 3은 제안된 새로운 상기 컴퓨팅 머신의 시스템(예를 들면, 도 2에서 도시되는 새로운 컴퓨팅 머신)의 동작의 블록도 플로우차트이다. 신규 사용 BIOS(Basic Input and Output System) 소프트웨어(도 3, 항목 26)는: 모든 입력 및 출력 디바이스를 개시하고; 오퍼레이팅 시스템 소프트웨어를 메모리 1(도 3, 항목 28)로부터 메인 메모

리 3(도 3, 항목 32)로 복사하여 동작을 시작하고; 인터넷 브라우저 메모리 2(도 3, 항목 29)로부터 인터넷 브라우저 메인 메모리 4(도 3, 항목 33) 안으로 인터넷 브라우저 소프트웨어를 복사한다. 오퍼레이팅 시스템 소프트웨어 및 인터넷 브라우저 소프트웨어는 상기 신규 사용 BIOS(도 3, 항목 26)의 감독하에 실행된다. 모든 애플리케이션 소프트웨어는, 메인 메모리 3(도 3, 항목 32)에서의 오퍼레이팅 시스템 소프트웨어 처리의 감독 하에 실행된다.

[0049] 파워 오프는 상기 신규 사용 BIOS(도 3, 항목 26)에 의해 제어된다. 파워 오프 이전에 애플리케이션 소프트웨어 패키지가 아닌 처리 동안 생성되는 데이터 파일만이 메인 메모리 3(도 3, 항목 32)으로부터 스토리지 1(도 3, 항목 35)로 다시 복사된다. 실행 파일이 아닌 데이터 파일만이 메인 메모리 4(도 3, 항목 33)로부터 스토리지 2(도 3, 항목 36)로 다시 복사된다.

[0050] (IP 어드레스의 허용된 목록 상에 있는) IP 어드레스는 사용자에 의해 명시되는 바와 같은 구체적으로 제어된 방식으로 임의의 정보를 수신할 수 있다. 사용자에 의해 IP 어드레스를 금지하는 규정이 존재한다.

[0051] 상기 신규 사용 BIOS(도 3, 항목 26)는 오퍼레이팅 시스템 소프트웨어 및 인터넷 브라우징 소프트웨어를 감독함에 있어서 확장된 역할을 가질 수도 있다.

[0052] 복수의 스토리지 디바이스인 스토리지 1(도 3, 항목 35)은 애플리케이션 소프트웨어 처리를 위해 오퍼레이팅 시스템 소프트웨어에 대해 사용된다.

[0053] 다른 복수의 스토리지 디바이스인 스토리지 2(도 3, 항목 36)는 인터넷 브라우저 소프트웨어 처리를 위해 사용된다.

[0054] 자신의 현재의 환경에서 덮어쓰기 또는 변경될 수 없는 메모리 디바이스인 메모리 1(도 3, 항목 28)은 오퍼레이팅 시스템 소프트웨어를 저장하기 위해 사용된다.

[0055] 자신의 현재의 환경에서 덮어쓰기 또는 변경될 수 없는 다른 메모리 디바이스인 메모리 2(도 3, 항목 29)는 인터넷 브라우저 소프트웨어를 저장하기 위해 사용된다.

[0056] 한 세트의 메인 메모리 3(도 3, 항목 32)은 오퍼레이팅 시스템 처리를 제공하고 다른 세트의 메인 메모리 4(도 3, 항목 33)는 인터넷 브라우저 처리를 제공한다.

[0057] 각각의 세션의 시작에서, 오퍼레이팅 시스템 소프트웨어는, 자신의 현재의 환경에서 덮어쓰기 또는 변경될 수 없는 디바이스인 상기 메모리 1(도 3, 항목 28)로부터 상기 메인 메모리 3(도 3, 항목 32)으로 복사된다.

[0058] 인터넷 브라우저 소프트웨어는 자신의 현재의 환경에서 덮어쓰기 또는 변경될 수 없는 디바이스인 메모리 2(도 2, 항목 29)로부터 메인 메모리 4(도 3, 항목 33)로 복사된다.

[0059] 오퍼레이팅 시스템 소프트웨어 및 인터넷 브라우저 소프트웨어는, 스토리지 디바이스(도 3, 항목 35 및 도 3, 항목 36) 중 임의의 것 상에서 각각 유지되지 않는다.

[0060] 각각의 세션의 끝에서, 오퍼레이팅 시스템 소프트웨어와 인터넷 브라우저 소프트웨어는, 각각, 스토리지 디바이스(도 3, 항목 35 및 도 3, 항목 36) 중 임의의 것으로 다시 복사되지 않는다.

[0061] 각각의 세션의 끝에서, 메인 메모리 3(도 3, 항목 32) 및 인터넷 메인 메모리 4(도 3, 항목 33)는 깨끗하게 지워진다.

[0062] 이제 실시형태 1의 도 4를 논의한다. 실시형태 1에서, 메모리 1(도 2, 항목 17)은 새로운 컴퓨팅 머신으로부터 제거되었다. 오퍼레이팅 시스템 소프트웨어는, 스토리지 1(도 4, 항목 25)에서, 어떠한 소프트웨어에 의해서도 덮어쓰기 또는 삭제될 수 없는 보안 영역 또는 파티션 상에 상주한다. 상기 컴퓨팅 머신 실시형태 1의 동작 동안, 오퍼레이팅 시스템 소프트웨어는 스토리지 1(도 4, 항목 25)로부터 메인 메모리 3(도 4, 항목 19)으로 복사되고, 처리는 평소와 같이 시작된다. 이 변경 이외에, 상기 컴퓨팅 머신의 동작은 도 2 및 도 3에서와 동일하게 유지된다.

[0063] 이제 실시형태 2의 도 5를 논의한다. 실시형태 2에서, 메모리 2(도 2, 항목 18)는 새로운 컴퓨팅 머신으로부터 제거된다. 브라우저 소프트웨어는, 스토리지 2(도 5, 항목 24)에서, 어떠한 소프트웨어에 의해서도 덮어쓰기 또는 삭제될 수 없는 보안 영역 또는 파티션 상에 상주한다. 상기 컴퓨팅 머신 실시형태 2의 동작 동안 브라우저 소프트웨어는 스토리지 2(도 5, 항목 24)로부터 메인 메모리 4(도 5, 항목 20)로 복사되고, 처리는 평소와 같이 시작된다. 이 변경 이외에, 상기 컴퓨팅 머신의 동작은 도 2 및 도 3에서와 동일하게 유지된다.

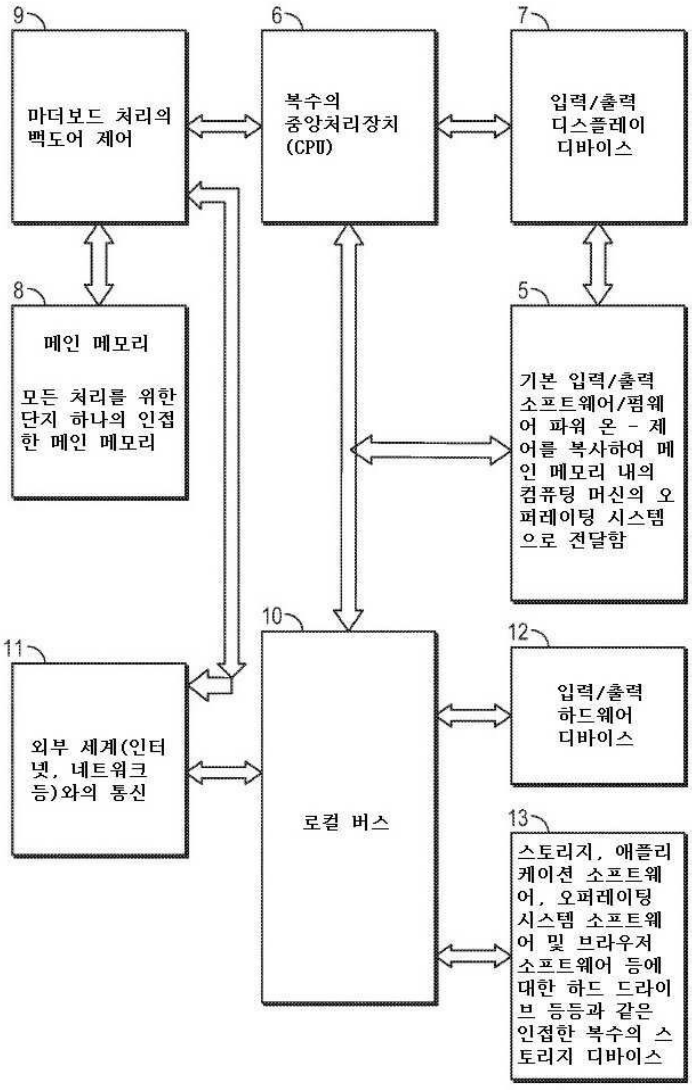
[0064] 이제 실시형태 3의 도 6을 논의한다. 실시형태 3에서, 메모리 1(도 2, 항목 17) 및 메모리 2(도 2, 항목 18) 둘 다가 새로운 컴퓨팅 머신으로부터 제거된다. 오퍼레이팅 시스템 소프트웨어는, 스토리지 1(도 6, 항목 25)에서, 어떠한 소프트웨어에 의해서도 덮어쓰기 또는 삭제될 수 없는 보안 영역 또는 파티션 상에 상주한다. 브라우저 소프트웨어는, 스토리지 2(도 6, 항목 24)에서, 어떠한 소프트웨어에 의해서도 덮어쓰기 또는 삭제될 수 없는 보안 영역 또는 파티션 상에 상주한다. 상기 컴퓨팅 머신 실시형태 3의 동작 동안, 오퍼레이팅 시스템 소프트웨어는 스토리지 1(도 6의 항목 25)로부터 메인 메모리 3(도 6의 항목 19)으로 복사된다. 상기 컴퓨팅 머신 실시형태 3의 동작 동안, 브라우저 소프트웨어는 스토리지 2(도 6, 항목 24)로부터 메인 메모리 4(도 6, 항목 20)으로 복사된다. 그리고 처리는 평소와 같이 시작된다. 이들 변경 이외에, 상기 컴퓨팅 머신의 동작은 도 2 및 도 3에서 동일하게 유지된다.

[0065] 새로운 컴퓨팅 머신이 설명되었다. 본 발명의 다양한 예시적인 실시형태의 전술한 설명은 예시 및 개시의 목적을 위해 제시되었다. 그것은 망라하도록 또는 본 발명을 개시되는 정확한 형태로 제한하도록 의도되지는 않는다. 본 발명의 취지를 벗어나지 않으면서 상기의 교시에 비추어 많은 수정 및 변형이 가능하다.

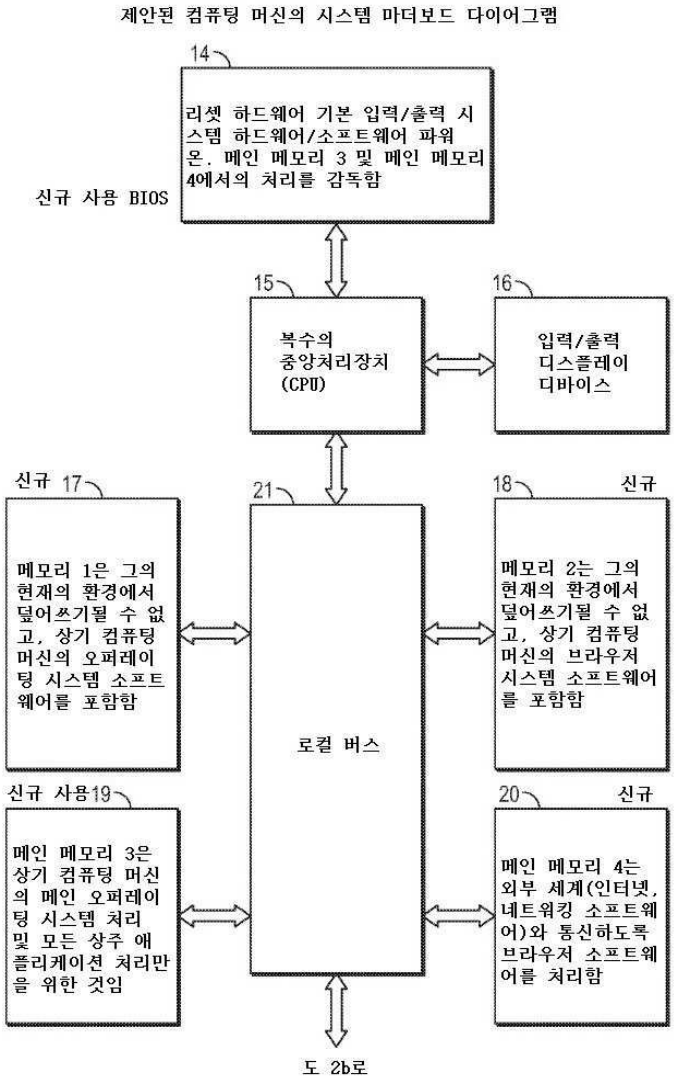
## 도면

### 도면1

통상적인 현존하는 컴퓨팅 머신 시스템 다이어그램

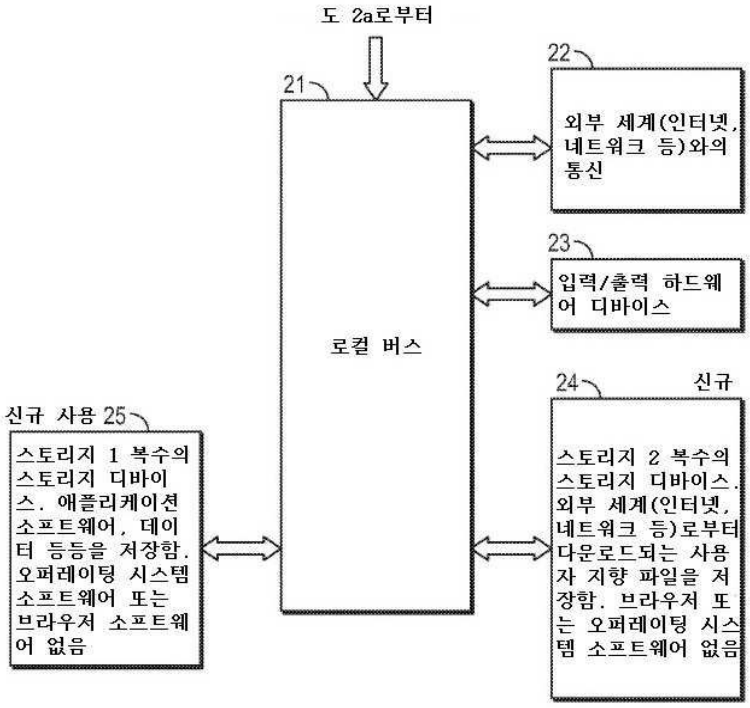


도면2a

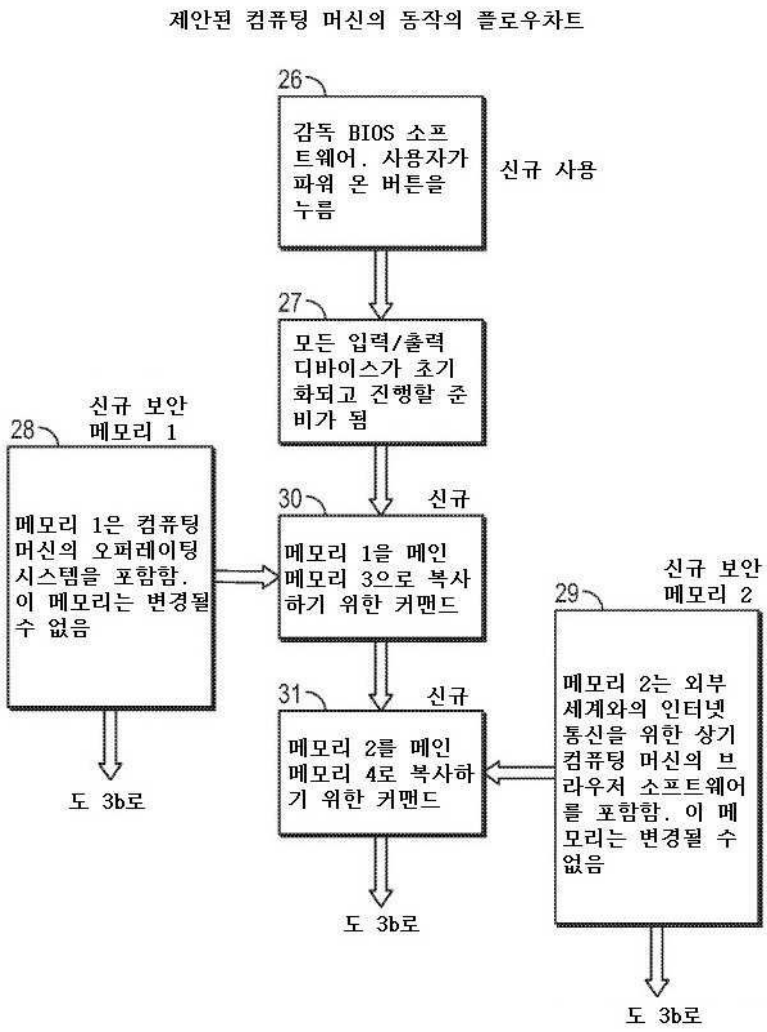

제안된 컴퓨팅 머신의 시스템 마더보드 다이어그램
14
리셋 하드웨어 기본 입력/출력 시스템 하드웨어/소프트웨어 파워 온. 메인 메모리 3 및 메인 메모리 4에서의 처리를 감독함
신규 사용 BIOS
15
복수의 중앙처리장치 (CPU)
16
입력/출력 디스플레이 디바이스
신규 17
메모리 1은 그의 현재의 환경에서 덮어쓰기될 수 없고, 상기 컴퓨팅 머신의 오퍼레이팅 시스템 소프트웨어를 포함함
21
로컬 버스
18 신규
메모리 2는 그의 현재의 환경에서 덮어쓰기될 수 없고, 상기 컴퓨팅 머신의 브라우저 시스템 소프트웨어를 포함함
신규 사용19
메인 메모리 3은 상기 컴퓨팅 머신의 메인 오퍼레이팅 시스템 처리 및 모든 상주 애플리케이션 처리만을 위한 것임
20 신규
메인 메모리 4는 외부 세계(인터넷, 네트워킹 소프트웨어)와 통신하도록 브라우저 소프트웨어를 처리함
도 2b로

도면2b

제안된 컴퓨팅 머신의 시스템 마더보드 다이어그램(계속됨)

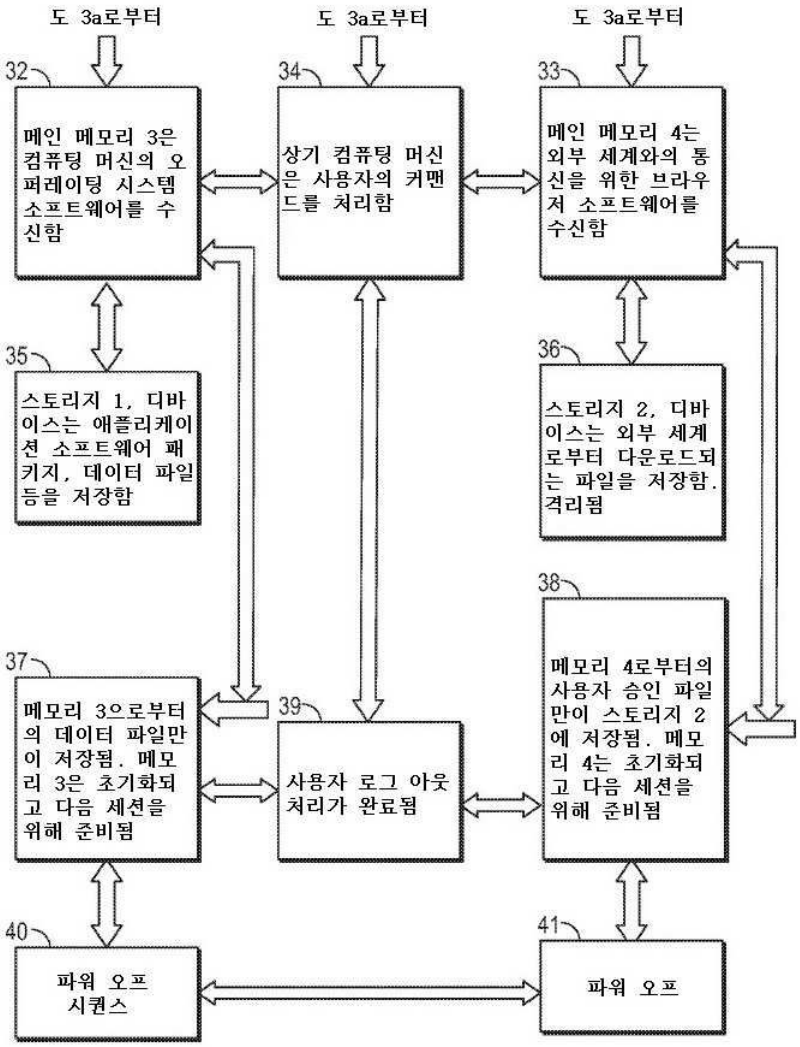


도면3a


제안된 컴퓨팅 머신의 동작의 플로우차트
26
감독 BIOS 소프트웨어. 사용자가 파워 온 버튼을 누름
신규 사용
27
모든 입력/출력 디바이스가 초기화되고 진행할 준비가 됨
신규 보안 메모리 1
28
메모리 1은 컴퓨팅 머신의 오퍼레이팅 시스템을 포함함. 이 메모리는 변경될 수 없음
30
신규
메모리 1을 메인 메모리 3으로 복사하기 위한 커맨드
신규 보안 메모리 2
29
메모리 2는 외부 세계와의 인터넷 통신을 위한 상기 컴퓨팅 머신의 브라우저 소프트웨어를 포함함. 이 메모리는 변경될 수 없음
31
신규
메모리 2를 메인 메모리 4로 복사하기 위한 커맨드
도 3b로
도 3b로
도 3b로

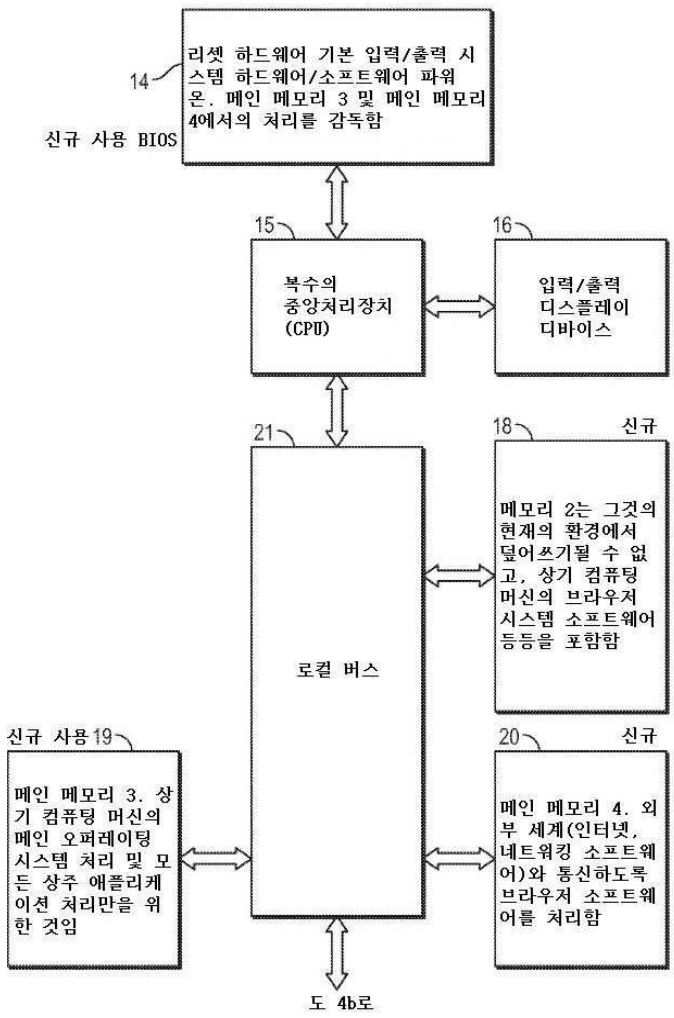
도면3b

제안된 컴퓨팅 머신의 동작의 플로우차트(계속됨)



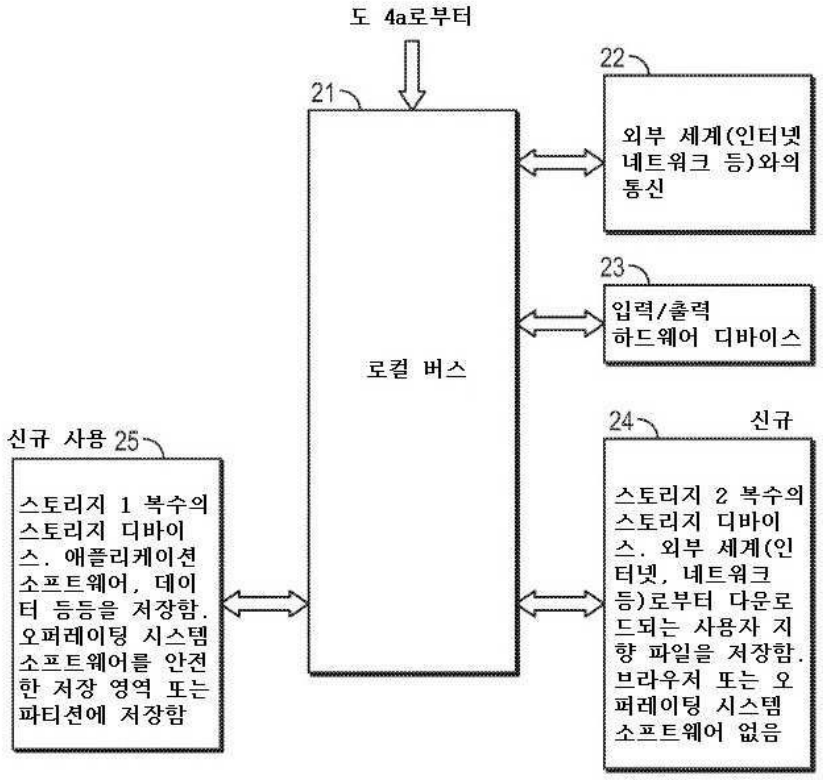
도면4a

제안된 컴퓨팅 머신의 시스템 마더보드 다이어그램 - 실시형태 1, 여기서는 항목 17이 원래의 것으로부터 삭제됨



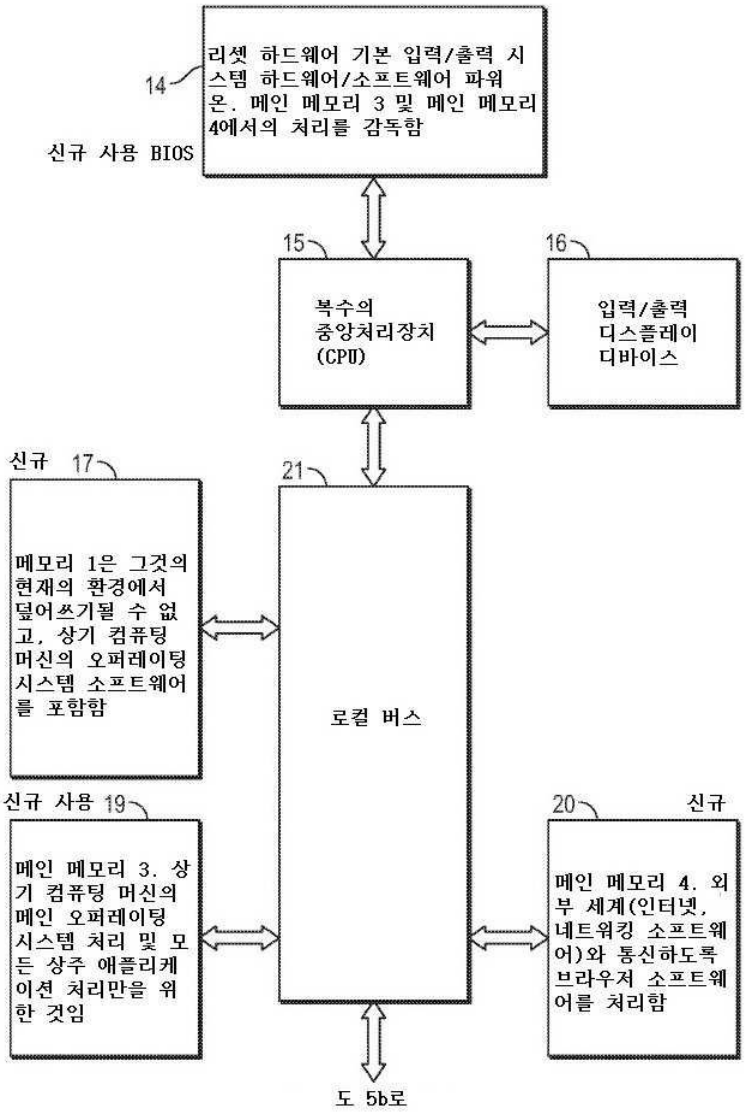
도면4b

제안된 컴퓨팅 머신의 시스템 마더보드 다이어그램(계속됨)
실시형태 1



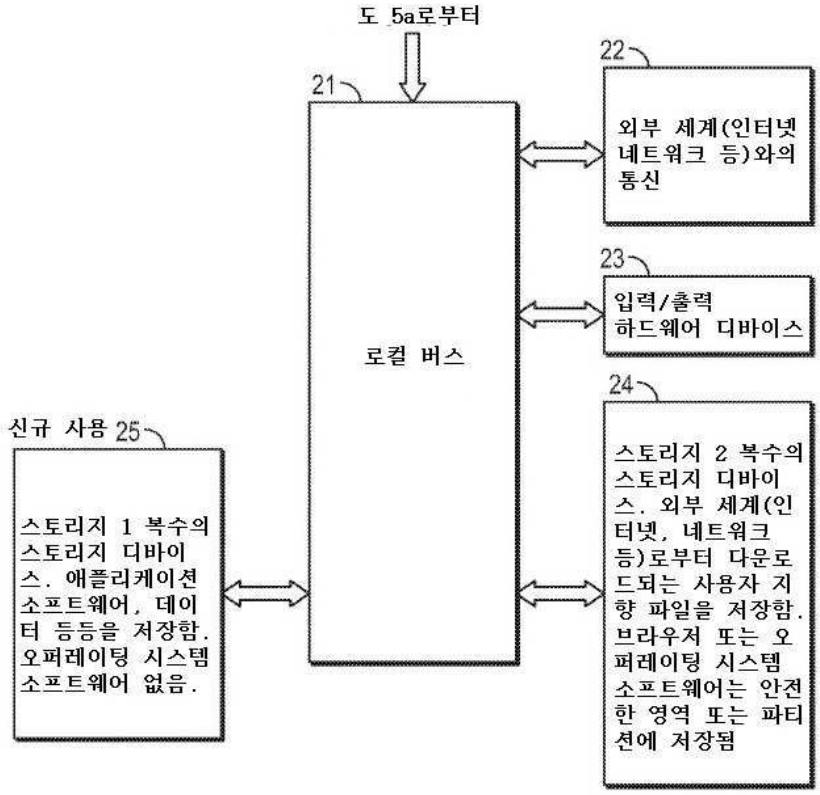
도면5a

제안된 컴퓨팅 머신의 시스템 마더보드 다이어그램 - 실시형태 2, 여기서는 항목 18이 원래의 것으로부터 삭제됨



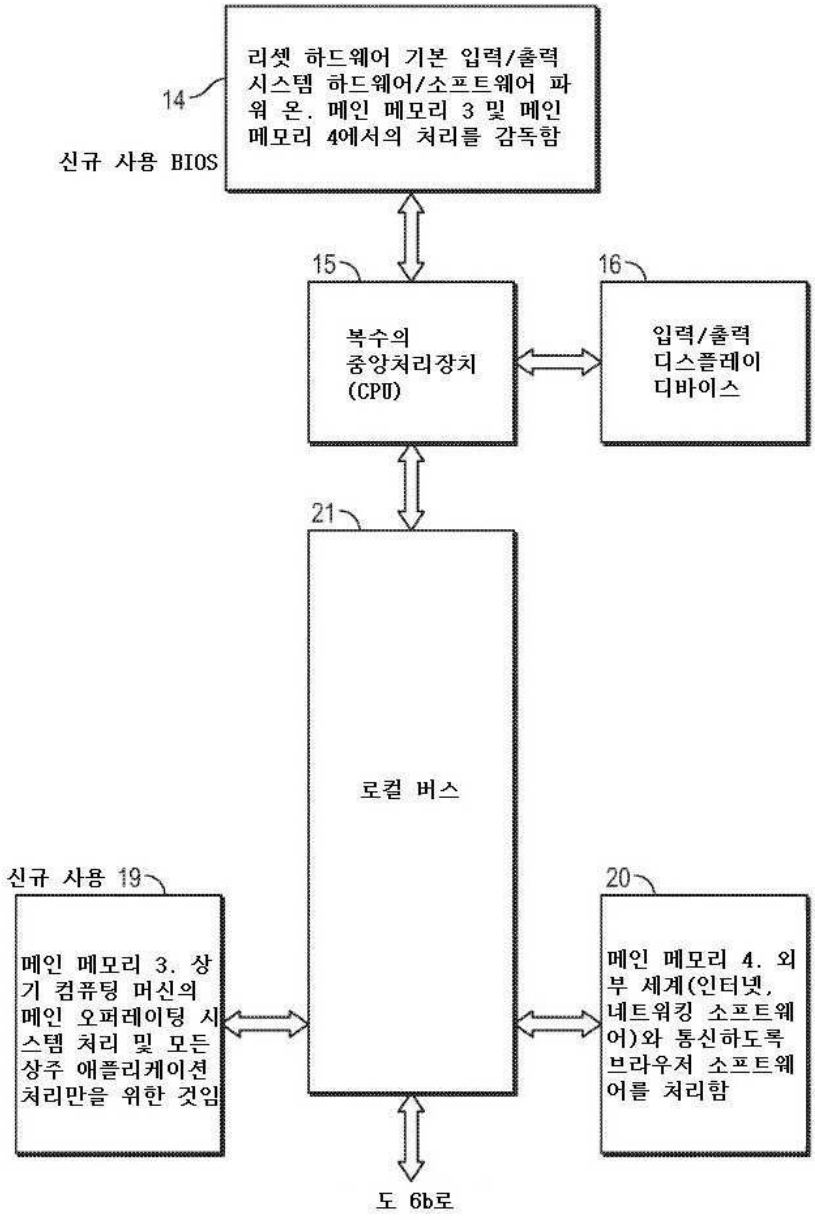
도면5b

제안된 컴퓨팅 머신의 시스템 마더보드 다이어그램(계속됨) 실시형태 2



도면6a

제안된 컴퓨팅 머신의 시스템 마더보드 다이어그램 - 실시형태 2, 여기서는 항목 17 및 18이 원래의 것으로부터 삭제됨



도면6b

제안된 전기 머신의 시스템 마더보드 다이어그램(계속됨) 실시형태 3