



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2007-0098835
(43) 공개일자 2007년10월05일

(51) Int. Cl.

G06F 15/16(2006.01) H04L 9/32 (2006.01)

G06F 11/00(2006.01) H04L 9/32 (2006.01)

G06F 11/00(2006.01)

(21) 출원번호 10-2007-7014877

(22) 출원일자 2007년06월28일

심사청구일자 없음

번역문제출일자 2007년06월28일

(86) 국제출원번호 PCT/US2005/043035

국제출원일자 2005년11월28일

(87) 국제공개번호 WO 2006/058313

국제공개일자 2006년06월01일

(30) 우선권주장

60/631,449 2004년11월29일 미국(US)

(뒷면에 계속)

(71) 출원인

시그나서트, 인크.

미국 97205 오리건 포틀랜드 플로어 7 워싱턴 스트리트 에스.더블유. 707

(72) 발명자

블레이크만, 데이비드 마우리츠

미국 97214 오리건 포틀랜드 34 애비뉴 에스.이. 1907

스타네스, 윌리엄 와이어트

미국 97201 오리건 포틀랜드 엘리자베스 코트 에스.더블유. 1536

앤더슨, 브래들리 더글라스

미국 97224 오리건 타이가드 터너게인 드라이브 에스.더블유.15318

(74) 대리인

남승희

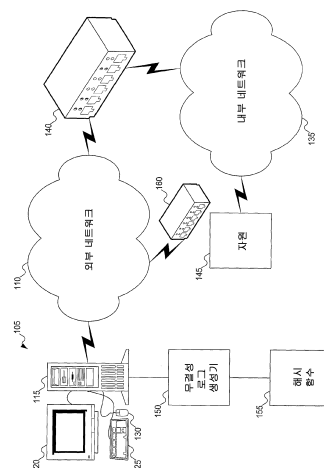
전체 청구항 수 : 총 20 항

(54) 정보 시스템 구성요소 분석에 의해 계산된 트러스트스코어에 기초하여 네트워크 단말간의 액세스를 제어하는방법

(57) 요약

컴퓨터 시스템에서 모듈에 대한 서명이 생성된다. 서명은 무결성 로그로 어셈블링될 수 있다. 무결성 검증 장치에서 서명은 데이터베이스 내의 서명과 비교된다. 서명이 검증되거나 검증되지 않은 경우, 트러스트 스코어가 생성될 수 있다. 트러스트 스코어는 상기 컴퓨터 시스템이 정책을 사용하여 자원에 대한 액세스 허가를 받아야 하는지를 결정하는데 사용될 수 있다.

대표도 - 도1



(30) 우선권주장

60/631,450 2004년11월29일 미국(US)

60/637,066 2004년12월17일 미국(US)

특허청구의 범위

청구항 1

복수의 제 1 모듈에 대한 복수의 제 1 서명을 저장하는 데이터베이스;

복수의 제 2 모듈에 대응하는 복수의 제 2 서명을 수신하는 수신기;

상기 수신된 복수의 제 2 서명 중 적어도 하나를 상기 데이터베이스 내에 저장된 하나 이상의 서명들과 비교하여, 상기 대응하는 서명이 상기 데이터베이스에서 발견된 상기 복수의 제 2 모듈의 제 1 서브 세트를 식별하고, 상기 대응하는 서명이 상기 데이터베이스에서 발견되지 않은 복수의 제 2 모듈의 제 2 서브 세트를 식별하는 검증 장치; 및

상기 대응하는 서명이 상기 데이터베이스에서 발견된 상기 복수의 제 2 모듈의 제 1 서브 세트와, 상기 대응하는 서명이 상기 데이터베이스에서 발견되지 않은 상기 복수의 제 2 모듈의 제 2 서브 세트에 기초하여, 상기 기계 장치에 대한 트러스트 스코어 (trust score)를 생성하는 트러스트 스코어 생성기를 포함하는 것을 특징으로 하는 장치.

청구항 2

제 1 항에 있어서,

상기 복수의 제 1 모듈에 대한 상기 복수의 제 1 서명은 상기 복수의 모듈에 대한 복수의 제 1 해시 (hash)를 포함하는 것을 특징으로 하는 장치.

청구항 3

제 1 항에 있어서,

상기 대응하는 서명이 상기 데이터베이스에서 발견되지 않은 상기 복수의 제 2 모듈의 제 2 서브 세트에 대응하는 서명을 제2 데이터베이스로 전송하는 송신기를 더 포함하며,

상기 수신기는 상기 제 2 데이터베이스로부터 제 2 트러스트 스코어를 수신하고;

상기 트러스트 스코어 생성기는 상기 대응하는 서명이 상기 데이터베이스에서 발견된 상기 복수의 모듈의 제 1 서브 세트와 상기 제 2 트러스트 스코어에 기초하여 트러스트 스코어를 생성하는 것을 특징으로 하는 장치.

청구항 4

제 1 항에 있어서,

상기 데이터베이스는 상기 복수의 제 1 모듈에 대한 복수의 제 1 식별자를 저장하고,

상기 수신기는 상기 복수의 제 2 모듈에 대한 복수의 제 2 식별자를 수신하고,

상기 검증 장치는 상기 기계 장치 내의 상기 복수의 모듈에 대한 복수의 제 2 식별자를 사용하여 상기 복수의 제 2 서명과 상기 데이터베이스 내의 복수의 서명을 비교하는 것을 특징으로 하는 장치.

청구항 5

제 1 항에 있어서,

상기 장치는 자원에 대한 액세스를 제어하는 정책(policy)을 더 포함하며,

상기 정책은 상기 자원에 대한 전면 액세스(full access)를 수신하기 위한 임계 스코어를 포함하는 것을 특징으로 하는 장치.

청구항 6

제 5 항에 있어서,

상기 정책은 상기 자원에 대한 부분적인 액세스를 수신하기 위한 제 2 임계 스코어를 더 포함하는 것을 특징으로 하는 장치.

청구항 7

제 1 항에 있어서,

상기 수신기는 상기 데이터베이스에 추가하기 위하여 모듈에 대한 서명을 수신하는 것을 특징으로 하는 장치.

청구항 8

네트워크;

상기 네트워크에 연결된 자원;

상기 네트워크에 연결되고, 복수의 제 1 모듈에 대한 복수의 제 1 서명을 포함하는 무결성 로그 (integrity log)를 생성하는 무결성 로그 생성기를 포함하는 컴퓨터; 및

상기 네트워크에 연결된 장치를 구비하고,

상기 장치는:

복수의 제 2 모듈에 대한 복수의 제 2 서명을 저장하는 데이터베이스;

상기 컴퓨터로부터 상기 무결성 로그를 수신하는 수신기;

상기 무결성 로그와 상기 복수의 제 1 서명과의 비교 결과에 근거하여 트러스트 스코어를 생성하는 트러스트 스코어 생성기; 및

상기 자원에 대한 액세스를 제어하며, 상기 자원에 대한 전면 액세스를 수신하기 위한 임계 스코어를 포함하는 정책을 포함하며,

상기 정책에 의해 상기 컴퓨터의 상기 자원에 대한 액세스가 제어되는 것을 특징으로 하는 시스템.

청구항 9

제 8 항에 있어서,

상기 시스템은 제 2 장치를 포함하며,

상기 제 2 장치는 복수의 제 3 모듈에 대한 복수의 제 3 서명을 저장하는 제 2 데이터베이스를 포함하고,

상기 장치는 상기 대응하는 서명이 상기 데이터베이스에서 발견되지 않은 상기 복수의 제 1 모듈의 서브 세트에 대응하는 서명을 상기 제 2 장치로 전송하는 송신기를 포함하는 것을 특징으로 하는 시스템.

청구항 10

제 9 항에 있어서,

상기 시스템은 제 2 네트워크를 더 포함하며,

상기 장치 및 상기 제 2 장치는 상기 제2 네트워크에 연결되는 것을 특징으로 하는 시스템.

청구항 11

복수의 모듈에 대응하는 복수의 제 1 서명을 수신하는 단계;

상기 복수의 모듈에 대한 상기 복수의 제 1 서명을 데이터베이스 내의 복수의 제 2 서명과 비교하는 단계;

상기 대응하는 서명이 상기 데이터베이스에서 발견된 상기 복수의 모듈의 제 1 서브 세트와 상기 대응하는 서명이 상기 데이터베이스에서 발견되지 않은 복수의 모듈의 제 2 서브 세트를 식별하는 단계; 및

상기 대응하는 서명이 상기 데이터베이스에서 발견된 상기 복수의 모듈의 제 1 서브 세트와 상기 대응하는 서명이 상기 데이터베이스에서 발견되지 않은 상기 복수의 모듈의 제 2 서브 세트에 기초하여, 트러스트 스코어 (trust score)를 생성하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 12

제 11 항에 있어서,

상기 트러스트 스코어에 기초하여 네트워크 상의 자원에 대한 액세스를 제어하는 단계를 더 포함하는 특징으로 하는 방법.

청구항 13

제 12 항에 있어서,

상기 트러스트 스코어에 기초하여 네트워크 상의 자원에 대한 액세스를 제어하는 단계는:

상기 네트워크 상의 자원에 액세스하기 위한 정책에 액세스하는 단계; 및

상기 트러스트 스코어에 기초하여 상기 자원에 대한 액세스를 제어하기 위하여 상기 정책을 사용하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 14

제 13 항에 있어서,

상기 트러스트 스코어에 기초하여 상기 자원에 대한 액세스를 제어하기 위하여 상기 정책을 사용하는 단계는, 상기 트러스트 스코어가 임계 스코어보다 큰 경우, 상기 정책에 따라 상기 자원에 대한 전면 액세스를 허용하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 15

제 13 항에 있어서,

상기 트러스트 스코어에 기초하여 상기 자원에 대한 액세스를 제어하기 위하여 상기 정책을 사용하는 단계는, 상기 트러스트 스코어가 제 1 임계 스코어보다 크고 제 2 임계 스코어보다 작은 경우, 상기 정책에 따라 상기 자원에 대한 부분적인 액세스를 허용하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 16

제 13 항에 있어서,

상기 트러스트 스코어에 기초하여 상기 자원에 대한 액세스를 제어하기 위하여 상기 정책을 사용하는 단계는, 상기 트러스트 스코어가 임계 스코어보다 작은 경우, 상기 정책에 따라 상기 자원에 대한 액세스를 거부하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 17

제 11 항에 있어서,

상기 트러스트 스코어를 생성하는 단계는 상기 트러스트 스코어 생성 시 적어도 제 2 모듈보다 제 1 모듈에 더 높은 가중치를 부여하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 18

제 11 항에 있어서,

상기 복수의 제 1 서명을 수신하는 단계는 상기 복수의 모듈에 대응하는 상기 복수의 제 1 서명을 포함하는 무결성 로그를 수신하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 19

제 11 항에 있어서,

상기 대응하는 서명이 상기 데이터베이스에서 발견되지 않은 상기 복수의 모듈의 제 2 서브 세트에 대응하는 서명을 제 2 데이터베이스로 전송하는 단계;

상기 대응하는 서명이 상기 제 2 데이터베이스에서 발견된 복수의 모듈의 제 3 서브 세트와, 상기 대응하는 서명이 상기 제 2 데이터베이스에서 발견되지 않은 복수의 모듈의 제 4 서브 세트를 상기 제 2 데이터베이스로부

터 수신하는 단계; 및

상기 대응하는 서명이 상기 데이터베이스에서 발견된 상기 복수의 모듈의 제 1 서브 세트와, 상기 대응하는 서명이 상기 제 3 데이터베이스에서 발견된 상기 복수의 모듈의 제 3 서브 세트에 기초하여, 트러스트 스코어를 생성하는 단계를 포함하는 것을 특징으로 하는 방법.

청구항 20

제 11 항에 있어서,

상기 복수의 모듈에 대응하는 복수의 제 1 서명을 수신하는 단계는 상기 복수의 제 1 서명과 상기 복수의 모듈에 대한 복수의 식별자를 수신하는 단계를 포함하고,

상기 복수의 모듈에 대한 복수의 제 1 서명을 데이터베이스 내의 복수의 제 2 서명과 비교하는 단계는 상기 복수의 모듈에 대한 복수의 식별자를 이용하여 상기 복수의 모듈에 대한 복수의 제 1 서명과 상기 데이터베이스 내의 복수의 제 2 서명을 비교하는 단계를 포함하는 것을 특징으로 하는 방법.

명세서

기술 분야

- <1> 본 발명은 컴퓨터 모듈의 검증에 관한 것으로, 더욱 상세하게는 네트워크 자원에 대한 컴퓨터 액세스를 승인하기 전에 컴퓨터의 무결성(integrity)을 결정하는 기술에 관한 것이다.

배경 기술

- <2> 과거에는 컴퓨터 네트워크가 불충분 했지만, 현재는 컴퓨터 네트워크가 널리 보편화되어 있다. 대부분의 기업은 네트워크로 서로 연결된 컴퓨터를 구비하고 있다. 예를 들어, 대기업들은 네트워크로 연결된 수백 또는 수천대의 컴퓨터를 구비하고 있다. 또한, 컴퓨터 네트워크는 가정으로까지 확산되고 있다. 각 가정에서는 개개인이 그들만의 컴퓨터를 갖고 싶어하기 때문에, 컴퓨터 자원을 공유하기 위하여 컴퓨터를 네트워크, 예를 들어, 인터넷으로 연결할 필요가 있다. 이에 대응하여, 라우터와 같은 컴퓨터 네트워크를 지원하기 위한 장비를 제조하는 회사들은 설치 및 사용이 편리한 장비들을 제조하고 있다. 사용자는 단지 그들의 컴퓨터를 라우터에 연결하고 라우터에 전원을 공급하기만 하면 되고, 장비에 관해서는 신경쓰지 않아도 된다.
- <3> 그러나 네트워크의 설치의 용이성으로 인해 컴퓨터는 여러 위험 요소에 노출되어 있다. 바이러스, 웜, 바이러스, 트로이 목마, 논리폭탄들은 점차 증가하는 빈도로 쓰여지고 있다. 인터넷과 인터넷에 연결된 네트워크들에 의해 이들이 쉽게 확산되고, 또한 확산될 가능성이 높아진다.
- <4> 바이러스나 이와 유사한 것에 의한 컴퓨터의 감염은 컴퓨터 사용자를 곤혹스럽게 만든다. 사용자는 기껏해야 그의 개인 네트워크상의 컴퓨터 중에서 어떤 것이 바이러스에 감염되었는지 확인하고 그 바이러스를 퇴치하는데에만 시간을 보낼 뿐이다. 최악의 경우, 컴퓨터가 바이러스에 의해 감염되었을 때, 하드 드라이브를 소거하고 손상된 소프트웨어를 수정해야 한다. 이 경우, 사용자는 감염된 컴퓨터에 저장된 모든 데이터를 잃게 될 수도 있다.
- <5> 개인 사용자의 컴퓨터에 저장된 데이터는 대체 불가능하고 매우 귀중한 것일 것이다 (예를 들어, 가족 사진 또는 개인 문서). 하지만, 생활을 계속적으로 지속되어야 하며, 기업에 있어서, 데이터의 손실은 치명적이다. 적소적소에 아카이브 (archive) 정책이 있더라도, 컴퓨터 시스템과 기업 네트워크를 재구축하는데 걸리는 많은 시간이 걸리고, 사업상의 손실 금액과 실제 컴퓨터와 네트워크를 재구축하는데 드는 비용을 포함하여 수천 달러 이상의 비용이 든다. 또한, 컴퓨터와 네트워크를 재구축하는 동안의 일시적 사업 중지에 의해 잠재적인 신용상의 손실이 발생한다.

발명의 상세한 설명

- <6> 따라서 컴퓨터가 네트워크 자원에 액세스하기 전에 잠재적으로 비정상적인 상태에 있는 컴퓨터들을 식별하여 종래의 기술이 가지고 있었던 이러한 문제점과 그 외의 문제점을 처리해야 할 필요가 있다.
- <7> 본 발명은 유효한 모듈 서명의 데이터베이스를 구축하고, 모듈 및 컴퓨터를 검증하는 방법 및 장치를 제공한다. 컴퓨터를 검증하기 위하여, 장치는 컴퓨터 내의 모듈에 대하여 생성된 서명을 수신한다. 서명은 무결성 로그와

어셈블링될 수 있다. 장치는 서명을 데이터베이스와 비교하여 각각의 서명이 정확한 지를 검증하려 시도한다. 서명이 검증되었든 아니든, 장치는 트러스트 스코어를 발생시키는데 이에 기초하여 컴퓨터에 수신된 서명을 검증하게 된다.

<8> 본 발명의 상기한 것 및 그 이외의 특징, 목적 및 이점들은 아래의 본 발명의 상세한 설명과 첨부된 도면에 의해 보다 분명해질 것이다.

실시예

- <17> 도 1은 컴퓨터 검증을 실시하는 무결성 검증 장치를 포함하는 시스템을 나타낸다. 도 1에서, 컴퓨터 시스템(105)은 외부 네트워크(110)에 연결된다. 도시된 바와 같이, 컴퓨터 시스템(105)은 컴퓨터(115), 모니터(120), 키보드(125) 및 마우스(130)를 포함한다. 그러나 당업자라면 컴퓨터 시스템(105)이 상기한 구성요소 이외의 구성요소, 예를 들어, 프린터와 같은 입출력 장치를 구비할 수 있음을 이해할 수 있을 것이다. 또한, 도 1에는 종래의 컴퓨터 시스템(105)의 내부 구성요소의 일부, 예를 들어, 중앙 처리 장치와 메모리 등은 도시되지 않았다. 컴퓨터 시스템(105)은 노트북 컴퓨터, 전용 단말, 또는 개인 휴대 단말기(PDA)와 같은 다른 장치로 대체될 수 있다.
- <18> 그 이름으로부터 알 수 있는 바와 같이, 외부 네트워크(110)는 조직의 외부에 있는 네트워크이다. 반대로, 내부 네트워크(135)는 조직의 내부에 있는 네트워크이다. 무결성 검증 장치(140)는 조직 외부에 있지만 자원(145)과 같은 조직 내부의 자원으로 액세스를 요청하는 컴퓨터를 검증하기 위하여 외부 네트워크(110)와 내부 네트워크(135) 사이에 위치한다. 자원(145)은 예를 들어, 네트워크 드라이브, 디렉토리, 파일, 또는 웹 페이지 등이 될 수 있다. 이러한 검증을 지원하기 위해, 컴퓨터 시스템(105)은 컴퓨터 시스템에 대한 무결성 로그를 어셈블링하는 무결성 로그 생성기(150)를 포함한다. 무결성 검증 장치(140)는 무결성 로그를 사용하여 컴퓨터 시스템(105)을 검증한다.
- <19> 무결성 로그는 컴퓨터 시스템(105) 상의 다양한 모듈에 대한 서명으로 이루어진 집합이다. 일 실시예에서, 이들 서명은 모듈들의 해시(hash)이고, MD5, SHA-1, 또는 SHA-256과 같은 해시 함수(155)를 사용하여 생성될 수 있다. 일 실시예에서, 무결성 로그 생성기(150)는 시스템 부팅 시퀀스에 따라 조기에 (바람직하게는, 다른 드라이버들이 로딩되기 전에) 로딩되는 장치 드라이버이다. 무결성 로그 생성기(150)는 시스템 부팅 시퀀스 동안에 액세스 또는 로딩되는 각각의 모듈을 식별하여 이들 모듈에 대한 서명을 생성할 수 있다. 다른 실시예에서, 무결성 로그 생성기(150)는 전체 시스템의 잠재적인 모든 모듈을 스캐닝할 수 있다. 당업자라면 무결성 로그 생성기(150)가 다른 방법으로 동작할 수 있음을 이해할 수 있을 것이다.
- <20> 일 실시예에서, 무결성 로그 생성기(150)는 장치 드라이버 및 실행 가능한 모듈과 같이 실제로 로딩된 모듈에 대한 서명만을 생성한다. 다른 실시예에서, 무결성 로그 생성기(150)는 모듈 및 모든 지원 모듈 (예를 들어, 동적 링크 라이브러리(dynamic link library (DLL))에 대한 서명을 생성한다. 당업자라면 무결성 로그 생성기(150)가 다른 모듈에 대한 서명을 생성할 수 있고, 무결성 로그 생성기(150)가 다른 방법으로 동작할 수 있음을 이해할 수 있을 것이다.
- <21> 상기 설명으로부터 알 수 있는 바와 같이, 무결성 로그 생성기(150)는 소프트웨어 모듈 상에서만 동작한다. 통상적으로 소프트웨어 모듈은 무결성 로그 생성기(150)에 의해 그에 대한 서명이 생성되는 다수의 모듈을 포함하지만, 당업자라면 무결성 로그 생성기(150)가 하드웨어 모듈에 대한 서명도 생성할 수 있다는 것을 이해할 수 있을 것이다. 예를 들어, 무결성 로그 생성기(150)는 (예를 들면, 플래시 메모리, 읽기 전용 메모리(ROM), 프로그램 가능한 읽기 전용 메모리(PROM), 소거 가능한 PROM(EPROM), 전기적으로 소거 가능한 PROM(EEPROM), 강유전체 메모리(FRAM), 또는 자기 메모리(MRAM) 등에 저장되어) 컴퓨터 시스템의 기본 입출력 시스템(BIOS)에 사용되는 펌웨어 또는 하드웨어 모듈에 대한 서명을 생성할 수 있다.
- <22> 서명이 생성되면, 무결성 로그 생성기는 생성된 서명을 무결성 로그로 어셈블링한다. 무결성 로그는 서명이 생성된 모듈에 대한 식별자를 포함할 수 있다. 서로 다른 식별자들은 이하의 것을 포함한다.
- <23> • 모듈의 파일명과 절대 경로
- <24> • 모듈의 제조사
- <25> • 모듈을 포함하는 제품 또는 구성요소. 달리 말해서, 식별자는 모듈과 상호작용하는 제품 또는 구성요소를 식별할 수 있다.

- <26> · 모듈 또는 모듈을 포함하는 제품 또는 구성요소의 버전 및/또는 패치 레벨 - 동일한 모듈의 서로 다른 버전을 구별하기 위해 필요하다.
- <27> 당업자라면 다른 형태의 식별자가 사용될 수 있음을 이해할 수 있을 것이다.
- <28> 일 실시예에서, 무결성 검증 장치(140)는 내부 네트워크(135)에 직접 연결되지 않은 컴퓨터 시스템들을 검증하기 위해서만 사용된다. 본 실시예에서는 내부 네트워크(135)에 연결된 컴퓨터 시스템들은 안전하고 검증된 것으로 가정한다. 어떤 조직내의 컴퓨터 시스템이 통상적으로 그 조직에 의해 제어되기 때문에, 이러한 가정은 타당성이 있다. 따라서 조직내의 컴퓨터 시스템이 바이러스나 이와 유사한 것에 의해 감염될 가능성은 조직에 의해 제어되지 않는 컴퓨터 시스템보다 상대적으로 낮아진다. 이러한 가정하에서는 조직 내의 컴퓨터 시스템을 검증할 필요가 없기 때문에, 그러한 컴퓨터 시스템은 요청된 자원으로 더 신속한 액세스가 허용된다.
- <29> 그럼에도 불구하고, 제 2 실시예에서, 내부 네트워크(135)에 직접 연결된 컴퓨터 시스템 조차 (따라서 외부 네트워크(110)을 통해 자원을 요청하지 않은 컴퓨터 시스템 조차) 자원에 대한 액세스를 요구할 때, 컴퓨터 시스템에 대한 검증이 이루어진다. 요청된 자원에 대한 액세스는 지연될 수도 있지만, 조직 내의 컴퓨터 시스템 상에서도 악의적인 해킹 톨이나 바이러스를 검출할 수 있다는 점에서 이러한 검증 절차는 보다 우수한 안전성을 제공한다.
- <30> 도 1에 도시한 실시예에서, 무결성 검증 장치(140)는 내부 네트워크(135)에 직접 연결된 것으로 도시되어 있다. 조직 내의 컴퓨터 시스템이 대중에 이용할 수 없는 모듈을 포함하는 경우, 예를 들어, 모듈이 개발 중인 제품인 경우 또는 정부에 의해 기밀 취급되는 경우, 본 실시예는 효과적이다. 또한, 본 실시예는 상용화된 모듈만을 이용하는 조직에 효과적이다. 그러나, 이 경우, 조직은 무결성 검증 장치(140)를 시스템의 구성요소로서 구비할 필요가 있다. 다른 실시예에서, 조직이 상용화된 모듈만을 이용하는 경우에 유용하도록, 무결성 검증 장치(140)는 조직 전용의 무결성 검증 장치라기 보다는 공개적으로 접근 가능한 무결성 검증 장치일 수 있다. 이와 같은 무결성 검증 장치는 무결성 검증 장치(160)와 같이 외부 네트워크(110)에 연결될 수 있다. 무결성 로그가 외부 네트워크(110)을 통해서 무결성 검증 장치(160)로 전송되는 것을 제외하고, 상기 무결성 검증 장치(160)는 무결성 검증 장치(140)와 유사하게 동작한다.
- <31> 상기한 바와 같이, 본 발명의 일 실시예에서, 무결성 검증 장치(140)는 조직 내의 자원에 대한 네트워크 액세스를 검증한다. 무결성 검증 장치(140)가 컴퓨터 시스템 상의 각각의 잠재적인 모듈에 대한 서명을 저장할 수 있지만, 본 발명의 다른 실시예에서는, 무결성 검증 장치(140)는 조직에 고유한 모듈에 대한 서명만을 저장한다. 무결성 검증 장치(140)는 검증을 위해 표준 모듈 (또는 무결성 검증 장치(140)가 인식하지 못하는 모듈)에 대한 서명을 무결성 검증 장치(160)로 (외부 네트워크(110)을 통해서) 전송한다. 이러한 방식으로, 무결성 검증 장치(140)는 새로운 모듈이 설치되는 경우에도 업데이트 될 필요가 없다. 이들 모듈의 검증은 무결성 검증 장치(160)에 의해 처리될 수 있다.
- <32> 컴퓨터 시스템(105)이 내부 네트워크(135)에 직접 연결되지 않은 경우, 무결성 검증 장치(140)는 자원(145)이 암호화된 형태 또는 암호화되지 않은 형태로 요청되더라도 동작할 수 있다. 또한, 무결성 검증 장치(140)는 자원(145)이 암호화된 채널 또는 암호화되지 않은 채널을 사용하여 요청되더라도 동작할 수 있다. 예를 들어, 자원(145)은 패스워드로 보호되는 웹 페이지일 수 있다. 또는, 자원(145)은 자원에 대한 액세스를 확보하기 위해 사용되는 가상 사설망(VPN)을 통해서 요청될 수 있다. 당업자라면 자원(145)에 대한 액세스가 다양한 방법으로 관리될 수 있음을 이해할 수 있을 것이다.
- <33> 도 2는 컴퓨터 검증을 위해 사용되는 도 1의 무결성 검증 장치의 특징을 나타낸다. 도 2에 무결성 검증 장치(140)의 구성이 보다 상세히 도시되어 있지만, 당업자라면 도시된 상세도가 다른 무결성 검증 장치, 예를 들어, 무결성 검증 장치(160)에도 적용될 수 있음을 이해할 수 있을 것이다. 또한, 당업자라면 도 2에는 무결성 검증 장치(140)를 통한 데이터 흐름이 도시되지 않았음을 이해할 수 있을 것이다.
- <34> 무결성 검증 장치(140)는 데이터베이스(205)를 포함한다. 데이터베이스(205)는 도 3에 더욱 상세하게 도시되어 있다. 도 3에는 데이터베이스(205)가 테이블(305)로서 도시되어 있지만, 당업자라면 데이터베이스(205)가 다른 형태를 가질 수 있음을 이해할 수 있을 것이다. 테이블(305)은 도시된 바와 같이 다수의 엔트리(entry)(310, 315, 및 320)를 포함한다. 각각의 엔트리는 모듈 및 그에 대응하는 서명을 포함한다. 예를 들어, 엔트리(320)는 Windows XP 운영 체제의 가상 메모리 매니저(DLL)에 대한 서명을 나타낸다 (엔트리(320)에 나타난 서명은 진짜 서명이라기 보다는 서명을 나타내는 임의의 번호이다). 엔트리(310, 315, 및 320)는 마이크로소프트사의 윈도우즈 운영 체제의 버전으로 사용되는 모듈을 나타내지만, 당업자라면 본 발명의 실시예는 다른 운영

체제, 예를 들어, 리눅스 운영 체제의 버전에도 적용가능 함을 알 수 있을 것이다 (Microsoft 및 Windows는 미국 및 다른 나라에 있는 마이크로소프트사의 등록상표이며, Linux는 Linus Torvalds의 등록상표이다).

- <35> 상기한 바와 같이, 테이블(305)의 엔트리는 다양한 모듈에 대한 식별자를 포함한다. 테이블(305)에 모듈 식별자를 포함시킴으로써, 모듈 검증에 제공되는 서명은 모듈의 예상 서명과 비교되어 모듈이 적절히 검증되었음을 입증할 수 있다. 테이블(305)은 모듈의 파일명과 경로를 나타내는 단 하나의 모듈 식별자를 보여주고 있지만, 당업자라면 테이블(305)이 다른 모듈 식별자들 또는 식별자들의 조합을 사용할 수 있음을 이해할 수 있을 것이다.
- <36> 본 발명의 또다른 실시예에서, 테이블(305)은 모듈 식별자 없이 단지 유효 서명만을 포함한다. 이 경우, 모듈 검증을 위해 제공된 서명은 일치하는 것이 발견될 때까지 데이터베이스(205) 내의 모든 서명과 비교된다. 데이터베이스(205) 내에서 일치하는 서명이 발견되면, 모듈이 검증된 것으로 간주되고, 그렇지 않으면, 모듈이 검증되지 않은 것으로 간주된다. 서명을 산출하기 위해 선택된 함수(즉, 해시 함수)의 충돌 확률이 낮다고 가정하면, 검증되지 않은 모듈의 서명이 데이터베이스의 서명과 일치할 위험은 그다지 높지 않다. 그러나 이러한 위험은 모듈 식별자를 데이터베이스(205)에 포함시킴으로써 효과적으로 제거할 수 있다.
- <37> 다시 도 2를 참조하면, 무결성 검증 장치(140)는 다른 구성요소를 포함한다. 수신기(210)는 무결성 검증 장치(140)로 전송된 정보를 수신한다. 예를 들면, 수신기(210)는 검증되어야 할 컴퓨터 시스템으로부터의 무결성 로그, 데이터베이스(205)에 추가되는, 새롭게 검증되어야 할 모듈의 서명, 또는 데이터베이스(205)에 저장된 기존의 모듈에 대한 이전 서명을 대체하기 위한 대체 서명을 수신할 수 있다. 송신기(215)는 무결성 검증 장치(140)로부터의 정보를 전송한다. 예를 들어, 송신기(215)는 트러스트 스코어를 컴퓨터 시스템에 전송하거나, 서명을 다른 무결성 검증 장치로 전송할 수 있다 (무결성 검증 장치(140)가 이들 서명에 대응하는 모듈을 검증할 수 없는 경우).
- <38> 검증 장치(220)는 무결성 로그 검증 장치(140)가 수신한 서명을 검증한다. 검증 장치(220)는 하나 이상의 서명을 선택하여 어떤 서명이 유효한지 결정하고, 서명이 유효한지 아닌지를 나타내는 지시를 반송한다. 검증 장치(220)는 수신한 서명(들)을 데이터베이스(205)의 서명과 비교하여 서명이 데이터베이스(205) 내의 서명과 일치하는 지를 나타내는 비교기와 같이 그 구조가 단순할 수 있다. 또한, 검증 장치(220)는 필요하다면 보다 복잡한 기술을 수행하여 서명을 검증할 수 있다.
- <39> 트러스트 스코어 생성기(225)는 컴퓨터 시스템에 대한 트러스트 스코어를 생성한다. 트러스트 스코어는 컴퓨터 시스템의 신뢰도를 나타낸다. 트러스트 스코어는 많은 다른 방법으로 생성될 수 있다. 본 발명의 일 실시예에서, 트러스트 스코어는 컴퓨터 시스템 상의 (검증되었거나 그렇지 않은) 모듈의 총 수에 대한 검증된 모듈의 수의 비율이다. 본 발명의 다른 실시예에서, 트러스트 스코어는 0과 1000 사이의 수일 수 있다. 여기서, 0은 전혀 신뢰할 수 없는 컴퓨터 시스템을 나타내고, 1000은 완전히 신뢰할 수 있는 컴퓨터 시스템을 나타낸다. 본 발명의 또 다른 실시예에서는, 다른 모듈보다 중요 모듈에 더 높은 가중치를 부여할 수 있는데, 제 2 컴퓨터 시스템이 더 많은 수의 검증된 모듈을 구비하였다 하더라도, 검증된 중요 모듈을 많이 구비한 컴퓨터 시스템이 검증된 중요 모듈을 적게 구비한 컴퓨터 시스템보다 더 높은 스코어를 기록할 수 있다 ("중요"라는 용어는 조직에 대해 중요하다고 인정되는 모듈만큼 많이 수량적으로 절대적으로 필요한 모듈을 나타내는 것이 아니다. 따라서, 하나의 조직은 운영 체제에 관한 파일을 "중요"한 것으로 간주할 수 있다. 반면, 다른 조직은 (어떤 목적을 위해) 내부적으로 개발된 커스텀인 모듈을 "중요"한 것으로 간주할 수 있다.).
- <40> 트러스트 스코어 생성기(225)는 다른 방법으로 트러스트 스코어를 계산할 수 있다. 본 발명의 다른 실시예에서, 트러스트 스코어 생성기는 무결성 로그 내에서 다수의 검증된 모듈의 위치를 고려할 수 있다: 예를 들어, 초기에 무결성 로그에 등록된 모듈이 무결성 로그에 나중에 생성된 모듈보다 더 중요하게 고려될 수 있다. 본 발명의 다른 실시예에서, 트러스트 스코어 생성기(225)는 트러스트 스코어를 계산함에 있어서 모듈 식별자를 고려할 수 있다. 어떤 제조사에 의해 제작된 모듈들은 다른 제조사에 의해 제작된 모듈들보다 중요하게 고려될 수 있다. 예를 들어, 애플리케이션과 연동하는 모듈을 고려하자. 애플리케이션 제조사에 의해 제작된 모듈은 제3의 제조사에 의해 제작된 모듈보다 더 중요하게 고려될 수 있다.
- <41> 본 발명의 또 다른 실시예에서, 모듈의 버전 및/또는 패치 레벨이 트러스트 스코어를 계산하는데 있어서 하나의 요인이 될 수 있다. 예를 들어, 여러 버전을 갖는 모듈이 제공된 경우, 최근의 버전이 이전의 버전보다 중요한 것으로 고려될 수 있다. 만약 검증된 모듈이 구버전인 경우, 트러스트 스코어는 최신 버전의 모듈을 구비한 컴퓨터 시스템보다 낮을 수 있다.

- <42> 또한, 무결성 검증 장치(140)는 정책(policy)(230)을 포함할 수 있다. 정책(230)은 어떤 방법으로 또한 어떤 조건하에서 컴퓨터 시스템이 도 1의 자원 (145)과 같은 자원에 액세스할 수 있는지를 나타낸다. 본 발명의 일 실시예에서, 정책 (230)은 임계 스코어(235)를 포함한다. 자원에 대한 액세스를 허가받기 위하여, 컴퓨터 시스템은 적어도 임계 스코어(235)만큼 높은 트러스트 스코어를 가져야만 한다. 만약 컴퓨터 시스템에 대한 트러스트 스코어가 임계 스코어(235) 미만인 경우, 컴퓨터 시스템의 자원에 대한 액세스는 거절된다.
- <43> 본 발명의 다른 실시예에서, 정책(230)은 다수의 임계 스코어를 포함할 수 있다. 예를 들어, 도 2에는, 정책 (230)이 두 개의 임계 스코어(235 및 240)를 갖는 것으로 도시되어 있다. 컴퓨터 시스템에 대한 트러스트 스코어가 임계 스코어(235) 이상이면, 컴퓨터 시스템의 자원에 대한 전면 액세스가 허용될 수 있다. 컴퓨터 시스템에 대한 트러스트 스코어가 임계 스코어 (235) 미만이고 임계 스코어 (240) 이상이면, 컴퓨터 시스템의 자원에 대한 부분적인 액세스가 허용될 수 있다. 컴퓨터 시스템에 대한 트러스트 스코어가 임계 스코어 (240) 보다 작으면, 컴퓨터 시스템의 자원에 대한 액세스가 거절될 수 있다 (비록 컴퓨터 시스템의 액세스가 보조 자원으로 변경되어 컴퓨터 시스템이 왜 이와 같이 낮은 트러스트 스코어를 가져야하는지를 결정할 수 있는 경우라도).
- <44> 이상 하나의 자원 및 2개의 임계 스코어에 관한 정책(230)을 설명하였지만, 당업자라면 정책(230)이 다른 방법으로 정의될 수 있음을 이해할 수 있을 것이다. 예를 들어, 정책(230)은 동일한 네트워크 상의 서로 다른 자원에 대한 각각의 정책을 나타낼 수 있다. 또는, 자원에 대한 액세스의 허용은 컴퓨터 시스템의 트러스트 스코어와 하나 이상의 임계 스코어를 직접 비교하는 방법 외의 다른 방법으로 결정될 수 있다. 또한, 정책(230)은 특별한 조직에 대한 자원의 액세스를 위한 정책이었지만, 만약 무결성 검증 장치 (140)가 다수의 조직에 의해 사용되는 경우 (예를 들어, 무결성 검증 장치(140)이 외부 네트워크에 무결성 검증 장치(160)로서 연결되는 경우), 무결성 검증 장치(140)는 다수의 조직에 대한 정책을 저장할 수 있다.
- <45> 도 2에 무결성 검증 장치(140)가 트러스트 스코어와 정책(230)을 생성하는 두 가지 특징을 갖는 것으로 도시되었지만, 당업자라면 무결성 검증 장치(140)는 이러한 특징들이 결합될 필요가 없음을 이해할 수 있을 것이다. 예를 들어, 무결성 검증 장치(140)는 트러스트 스코어를 생성하고, (생성된 트러스트 스코어에 기초한) 정책의 관리는 다른 곳에서 처리하도록 구성할 수 있다.
- <46> 도 4는 도 1에 도시된 무결성 검증 장치가 도 2의 데이터베이스를 어셈블링하는 절차를 나타내는 순서도이다. 도 4의 단계(405)에서, 모듈이 식별된다. 도 4는 컴퓨터 시스템을 검증하는데 사용되는 데이터베이스의 어셈블링과 관련되기 때문에, 모듈의 식별은 거의 수동으로 실시된다: 예를 들어, 모듈 제조사는 서명을 생성하고 생성된 서명을 데이터베이스에 추가하도록 모듈을 설정할 수 있다. 그러나 당업자라면 모듈 식별은 자동적으로 실행될 수 있음을 이해할 수 있을 것이다. 단계(410)에서, 식별된 모듈에 대한 서명이 생성된다. 단계(415)에서, 서명이 데이터베이스에 추가된다. 최종적으로, 단계(420)에서, 모듈에 대한 식별자가 서명과 연관되도록 데이터베이스에 추가되어, 이후의 모듈 검증에 도움을 준다. 화살표(425)로 표시된 바와 같이, 단계(420)은 선택적이며, 또한 생략될 수도 있다.
- <47> 도 5a와 도 5b는 도 1의 무결성 검증 장치가 각각의 모듈에 대한 서명을 검증하는 절차를 나타내는 순서도이다. 도 5a의 단계(505)에서, 무결성 검증 장치는 모듈에 대한 서명 및 잠재적으로는 식별자를 수신한다. 단계(510)에서, 상기 서명은 데이터베이스 내의 서명과 비교된다. 모듈 식별자가 제공되는 경우, 모듈 식별자는 데이터베이스의 검색 공간을 줄이는데 사용될 수 있다. 단계(515)에서, 무결성 검증 장치는 서명이 데이터베이스에서 발견되었는지를 판단한다. 서명이 발견되었다면, 단계(520)에서 서명은 유효하게 된다.
- <48> 무결성 검증 장치가 데이터베이스에서 서명을 발견하지 못한 경우, 단계(525)에서, 무결성 검증 장치는 서명을 검증할 수 있는 다른 데이터베이스 (또는 무결성 검증 장치)가 있는지를 판단한다. 다른 데이터베이스가 존재하지 않는 경우, 단계(530)에서, 서명은 무효인 것으로 거절되고, 처리는 종료된다. 만약, 다른 데이터베이스가 존재하면, 단계(535)에서, 무결성 검증 장치는 상기 서명을 다른 데이터베이스 (또는 무결성 검증 장치)로 전송한다. 단계(540)에서, 무결성 검증 장치는 상기 서명이 다른 데이터베이스에서 발견되었는지를 판단한다. 만약 그렇다면, 처리는 단계(520)으로 복귀하고, 서명은 유효한 것이 된다. 그렇지 않으면, 처리는 단계(525)로 복귀하여 상기 서명이 전송될 수 있는 다른 데이터베이스 (또는 무결성 검증 장치)가 있는지를 결정한다.
- <49> 도 6은 도 1에 도시된 컴퓨터와 같은 컴퓨터에 의한 무결성 로그의 어셈블링과 도 1에 도시된 무결성 검증 장치를 이용한 컴퓨터의 검증 절차를 나타내는 순서도이다. 단계(605)에서, 무결성 로그 생성기는 컴퓨터 시스템 상의 모듈을 식별한다. 단계(610)에서, 무결성 로그 생성기는 모듈에 대한 서명을 생성한다. 단계(615)에서, 무결성 로그 생성기는 선택적으로 서명을 무결성 로그로 어셈블링할 수 있다. 화살표(620)으로 표시된 바와 같이, 단계(615)는 선택적으로 실행된다: 서명은 무결성 로그로 어셈블링되지 않아도 된다. 최종적으로, 단계

(625)에서, 무결성 로그 생성기는 검증을 위해 서명을 무결성 검증 장치로 전송한다. 이 경우, 무결성 로그 생성기는 선택적으로 모듈 식별자를 무결성 검증 장치로 전송한다.

<50> 도 7a와 도 7b는 도 1의 무결성 검증 장치가 컴퓨터를 검증하는 절차를 나타내는 순서도이다. 도 7a의 단계(705)에서, 무결성 검증 장치는 검증을 위해 모듈에 서명을 수신하고, 또한 선택적으로 모듈 식별자를 수신한다. 단계(710)에서, 무결성 검증 장치는 검증을 위하여 서명을 선택한다. 서명은 차례로 선택될 수 있거나, 여러 다른 기준에 의해 선택될 수 있다. 단계(715)에서, 도 5a와 도 5b를 참조하여 설명한 바와 같이, 무결성 검증 장치는 서명의 검증을 시도한다.

<51> 단계(720)(도 7b)에서, 무결성 검증 장치는 서명이 검증되었는지를 판단한다. 서명이 검증되었다면, 단계(725)에서, 무결성 검증 장치는 서명을 데이터베이스에서 발견된 서명들의 집합에 추가한다. 서명이 검증되지 않았다면, 단계(730)에서, 무결성 검증 장치는 서명을 데이터베이스에서 발견되지 않은 서명들의 집합에 추가한다. 어떤 경우이든, 단계(735)에서 무결성 검증 장치는 검증해야 할 서명이 남아 있는지 확인한다. 만약 그렇다면, 처리는 도 7a의 단계(710)으로 복귀한다. 그렇지 않다면, 단계(740)에서, 무결성 검증 장치는 트러스트 스코어를 생성한다. 도 2를 참고하여 설명한 바와 같이, 트러스트 스코어를 생성함에 있어서, 트러스트 스코어는 임의의 서명에 다른 서명 보다 높은 가중치가 부여될 수 있다.

<52> 상기한 바와 같이, 단계(715)는 컴퓨터 시스템에 대한 서명을 검증하는 방법에 있어서 도 5a와 도 5b를 참조한다. 상기한 바와 같이, 도 5a와 도 5b는 제 1 무결성 검증 장치가 서명을 검증할 수 없는 경우에 하나의 서명을 처리하고 서명을 다른 무결성 검증 장치로 전송하는 방법을 도시한다. 이러한 방법은 무결성 로그에 있는 다수의 서명중에서 개별적인 서명에 대하여 효과적이다. 이와 달리, 제 1 무결성 검증 장치를 이용하여 가능한 많은 서명을 처리하고, 검증되지 않은 서명을 하나의 그룹으로서 제 2의 무결성 검증 장치로 전송하는 것도 가능하다.

<53> 도 8은 도 1의 무결성 검증 장치가 도 1의 컴퓨터와 같은 컴퓨터의 네트워크 자원에 대한 액세스를 허가 또는 거부하는 절차를 나타내는 순서도이다. 도 8의 단계(805)에서, 도 7a와 도 7b를 참조하여 설명한 바와 같이, 무결성 검증 장치는 컴퓨터 시스템에 대한 트러스트 스코어를 생성한다. 단계(810)에서, 무결성 검증 장치는 원하는 자원에 대한 정책에 액세스한다. 단계(815)에서, 무결성 검증 장치는 트러스트 스코어를 정책과 비교한다. 최종적으로, 단계(820)에서, 무결성 검증 장치는 정책을 사용하여 컴퓨터 시스템의 자원에 대한 적절한 액세스 레벨을 결정한다.

<54> 이하에서, 본 발명의 측면들을 실행하기에 적합한 기계 장치를 간략히 설명한다. 통상적으로, 기계 장치는 시스템 버스를 포함하고, 시스템 버스에는 프로세서, 메모리 (예를 들어, RAM, ROM, 또는 다른 저장 매체), 기억 장치, 비디오 인터페이스, 및 입출력 인터페이스 포트들이 접속된다. 상기 기계 장치는 키보드, 마우스 등의 종래의 입력 장치로부터의 입력에 의해 적어도 부분적으로 제어될 수 있고, 또한 다른 기계 장치로부터 입력된 지시, 가상 현실 (VR) 환경과의 상호 작용, 생체 측정 피드백 (biometric feedback), 또는 다른 입력 신호에 의해 제어될 수 있다. 본 명세서에서 사용되는 용어인 "기계 장치"는 넓은 의미에서 단일한 기계 장치 또는 서로 통신 가능하게 연결되어 함께 동작하는 기계 장치나 디바이스를 포함한다. 예를 들어, 이러한 기계 장치는 자가용, 열차, 택시 등의 자가 또는 공공 운송 수단뿐만 아니라 퍼스널 컴퓨터, 워크스테이션, 서버, 휴대용 컴퓨터, 휴대용 기기, 전화기, 태블릿 (tablet) 등의 연산 장치를 포함한다.

<55> 기계 장치는 프로그램 가능한 또는 프로그램 불가능한 논리 장치나 어레이, 주문형 반도체 (ASIC), 내장형 컴퓨터, 스마트 카드 등의 내장형 제어기를 포함할 수 있다. 상기 기계 장치는 네트워크 인터페이스, 모뎀, 및 다른 통신 연결 장치 등 하나 이상의 원격 장치와의 연결을 위한 하나 이상의 접속 장치를 이용할 수 있다. 기계 장치들은 인트라넷, 인터넷, LAN (local area network), WAN (wide area network) 등의 물리적 및/또는 논리적 네트워크에 의해 상호 연결될 수 있다. 당업자라면 무선 주파수 (RF), 위성 마이크로파, IEEE 545.11, 블루투스, 광, 적외선, 케이블, 레이저를 포함하는, 다양한 무선 및/또는 유선 단거리 또는 장거리 반송파와 프로토콜을 이용하여 네트워크 통신이 이루어질 수 있음을 이해할 것이다.

<56> 본 발명은 함수, 절차, 데이터 구조, 및 애플리케이션 프로그램 등을 포함하는 연관 데이터와 관련하여 설명될 수 있다. 그 결과, 기계 장치가 액세스하는 경우, 기계 장치는 태스크를 실행하거나 요약 데이터 타입이나 낮은 레벨의 하드웨어 컨텍스트를 정의할 수 있다. 연관 데이터는 예를 들어 RAM, ROM 등의 휘발성 및/또는 비휘발성 메모리 또는 다른 저장 장치, 및 하드 드라이브, 플로피 디스크, 광학적 저장 장치, 테이프, 플래시 메모리, 메모리 스틱, 디지털 비디오 디스크, 생물학적 저장 장치 등의 저장 매체에 저장될 수 있다. 연관 데이터는 물리적 및/또는 논리적 네트워크를 포함하는 전송 환경을 통해서 패킷, 직렬 데이터, 병렬 데이터, 전송 신

호 등의 형태로 전송될 수 있고, 압축 또는 암호화된 형태로 사용될 수 있다. 연관 데이터는 분산 환경에서 사용되고, 기계 장치의 액세스를 위해 국부적 및/또는 원격적으로 저장될 수 있다.

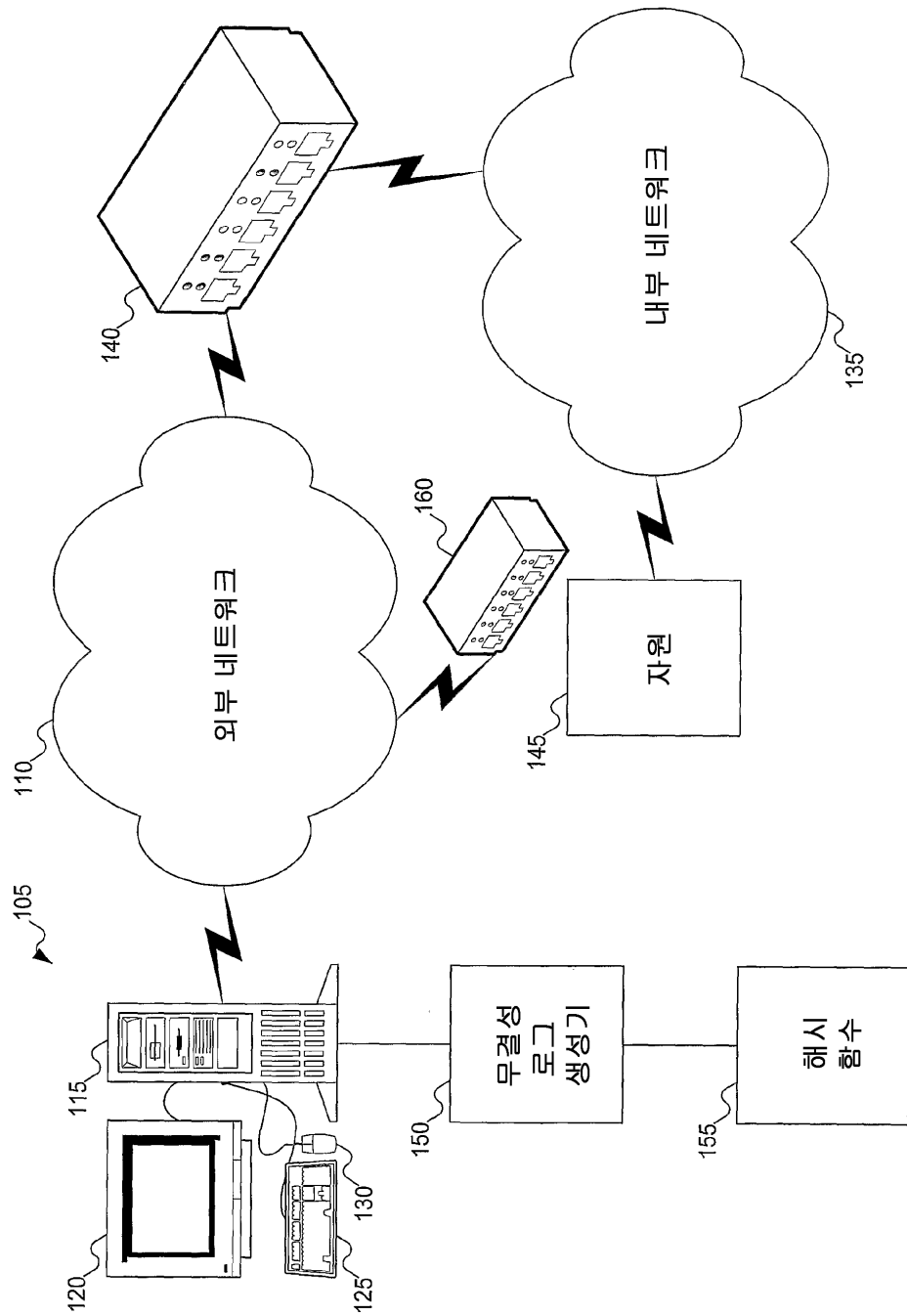
- <57> 본 발명의 원리를 상기한 실시예를 참조하여 설명하였지만, 상기 실시예들은 이와 같은 원리를 벗어나지 않는 범위 내에서 다양한 형태로 변형 가능하고 어떤 원하는 방법으로 결합될 수 있음을 당업자라면 이해할 수 있을 것이다. 또한, 상기에서는 특정한 실시예에 초점을 맞추어 설명하였지만, 다른 구성이 고려될 수 있다. 특히, "본 발명의 일 실시예에 따른"이라는 표현이 본 명세서에 사용되었지만, 이러한 표현은 일반적으로 가능한 실시예를 의미하고, 본 발명을 특정한 실시예로 제한하고자 하는 것은 아니다. 본 명세서에서 사용되는 이들 용어들은 서로 다른 실시예로 결합될 수 있는 동일 또는 다른 실시예를 언급할 수 있다.
- <58> 따라서, 본 명세서에 기재된 실시예들의 다양한 변경의 관점에서, 본 발명의 상세한 설명 및 첨부 자료는 단지 본 발명의 설명을 위한 것이지, 본 발명의 범위를 제한하고자 하는 것은 아니다. 그러므로 하기의 청구범위의 범위와 의미 및 그 등가 개념으로부터 도출되는 모든 변형예가 본 발명의 범위에 포함된다.

도면의 간단한 설명

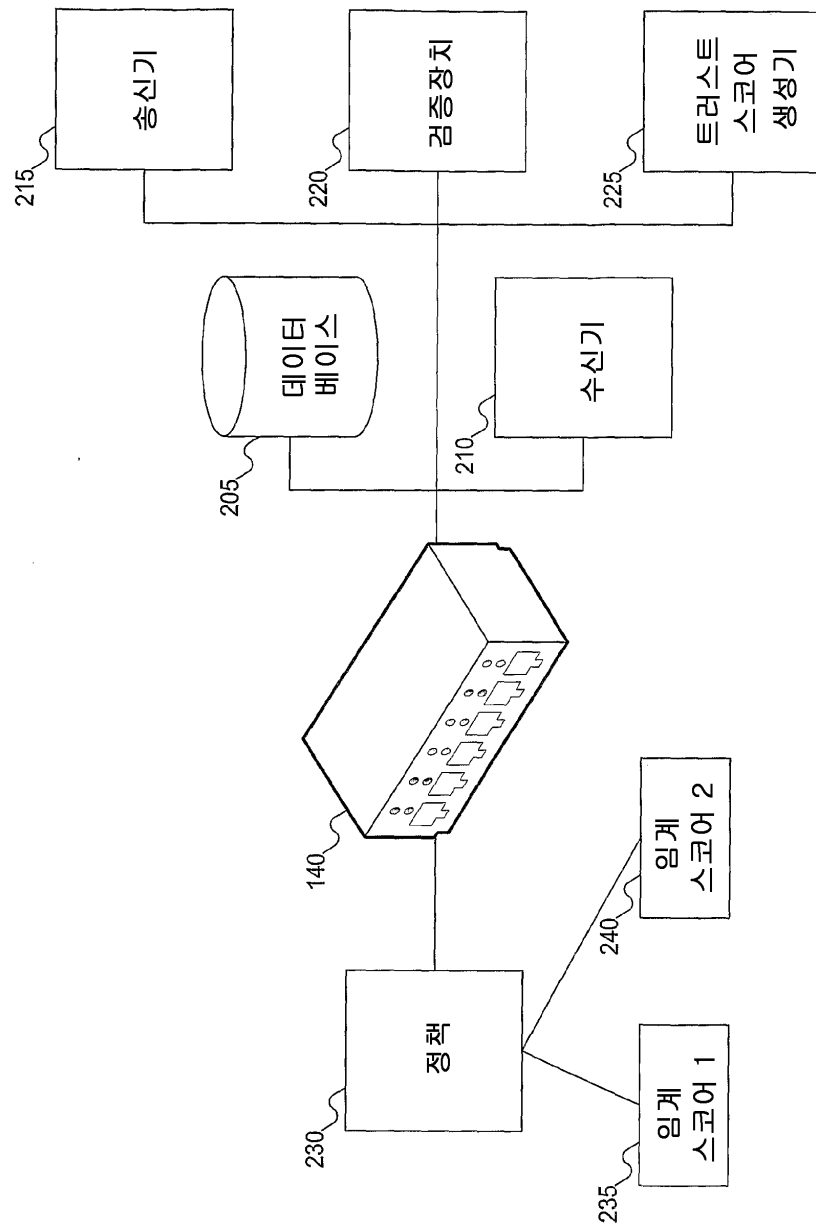
- <9> 도 1은 컴퓨터 검증을 실시하는 무결성 검증 장치를 포함하는 시스템을 나타내는 도면이다.
- <10> 도 2는 도 1에 도시된 컴퓨터 검증을 실시하는 무결성 검증 장치의 상세도이다.
- <11> 도 3은 도 2에 도시된 데이터베이스의 상세도이다.
- <12> 도 4는 도 1에 도시된 무결성 검증 장치가 도 2에 도시된 데이터베이스의 데이터를 어셈블링하는 절차를 도시하는 순서도이다.
- <13> 도 5a 및 도 5b는 도 1에 도시된 무결성 검증 장치가 개별적인 모듈의 서명을 검증하는 절차를 도시하는 순서도이다.
- <14> 도 6은 도 1에 도시한 컴퓨터 시스템과 같은 컴퓨터 시스템이 무결성 로그를 어셈블링하고 도 1의 무결성 검증 장치를 이용하여 컴퓨터 시스템을 검증하는 절차를 도시하는 순서도이다.
- <15> 도 7a 및 도 7b는 도 1의 무결성 검증 장치가 컴퓨터 시스템을 검증하는 절차를 도시하는 순서도이다.
- <16> 도 8은 도 1의 무결성 검증 장치가 도 1에 도시된 바와 같은 컴퓨터 시스템을 승인 또는 부정하여 네트워크에 대한 액세스를 제어하는 절차를 도시한 순서도이다.

도면

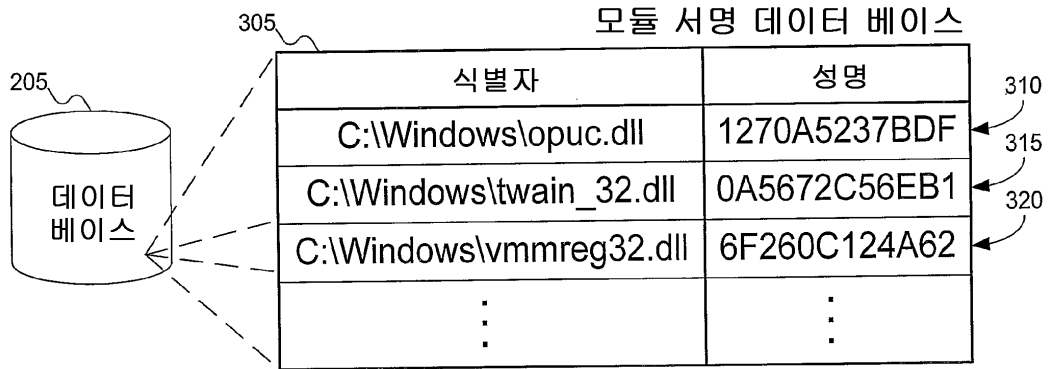
도면1



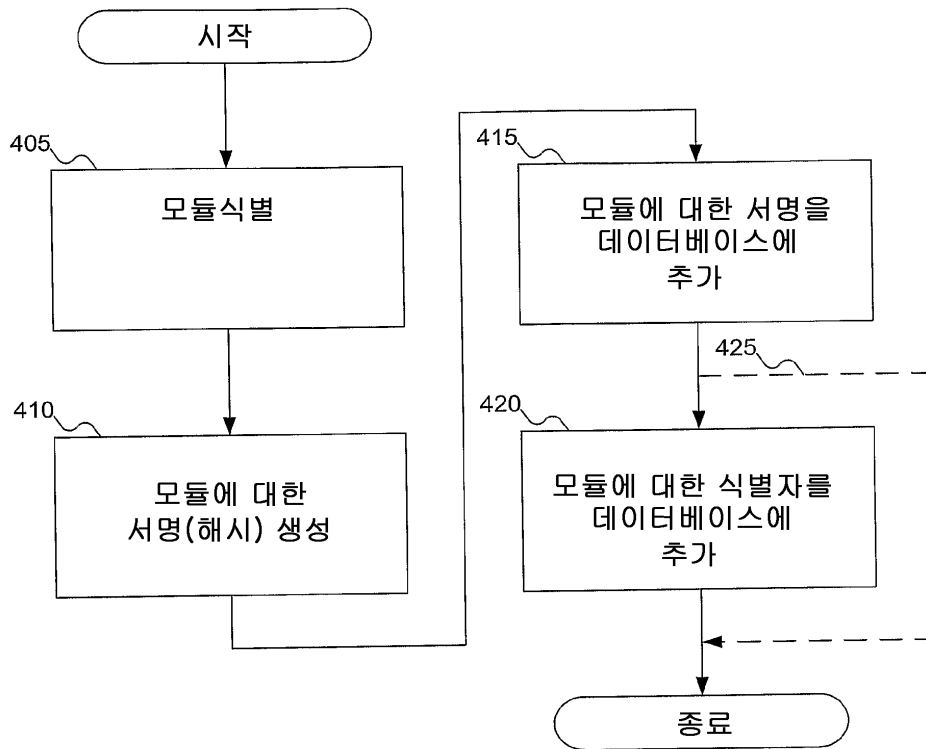
도면2



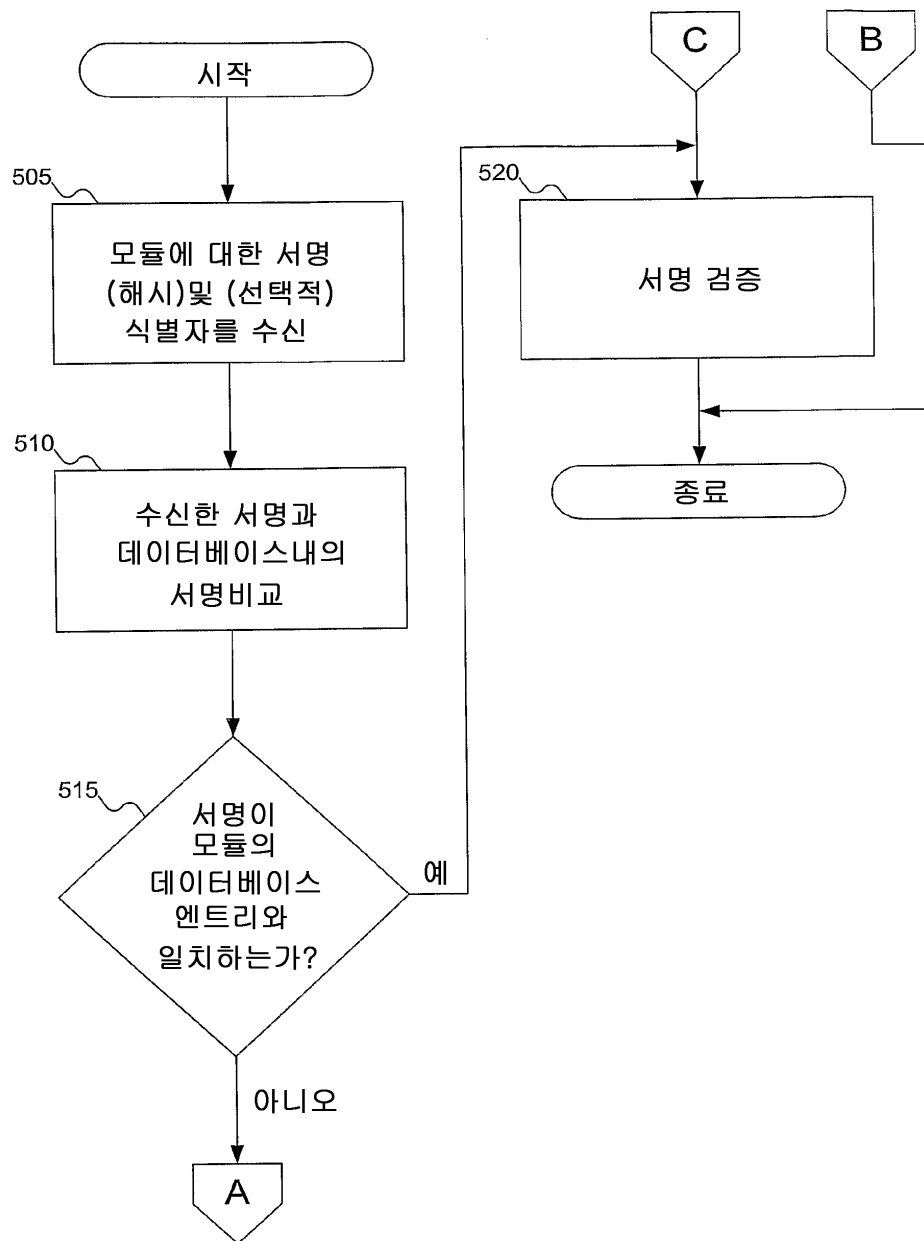
도면3



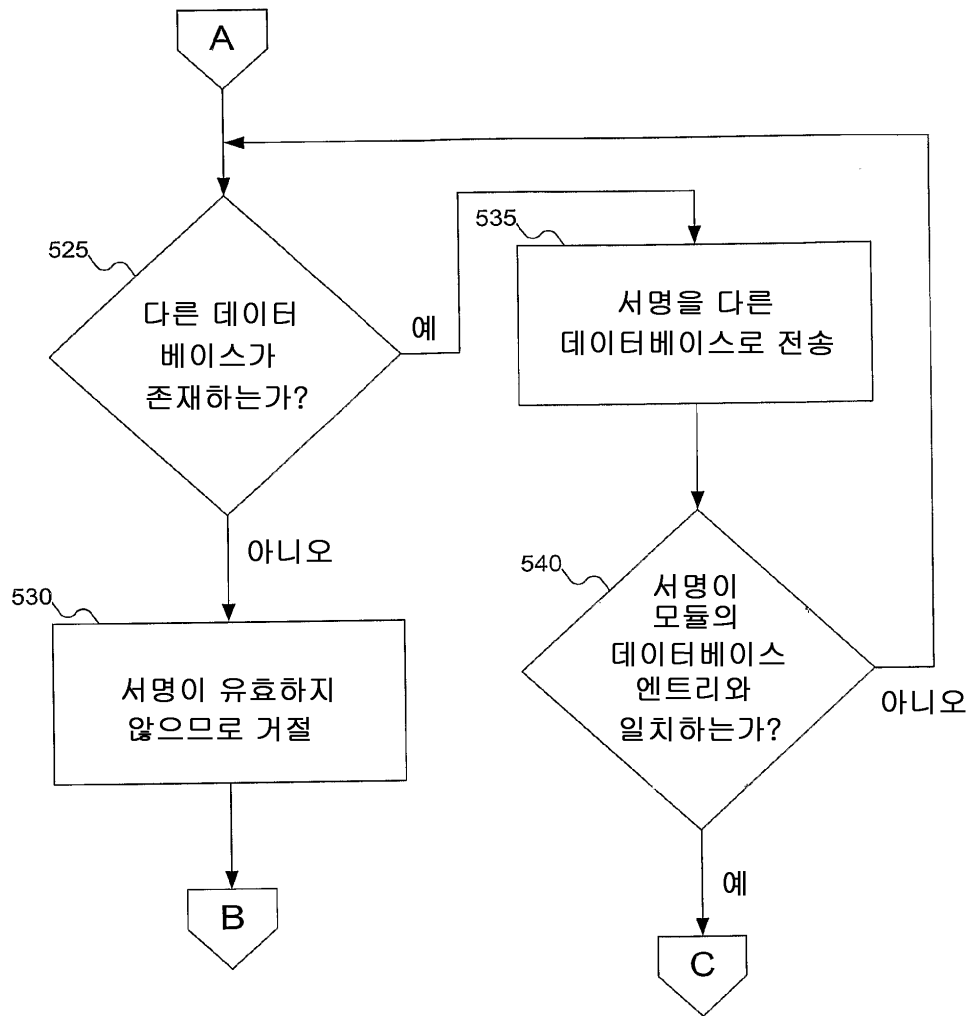
도면4



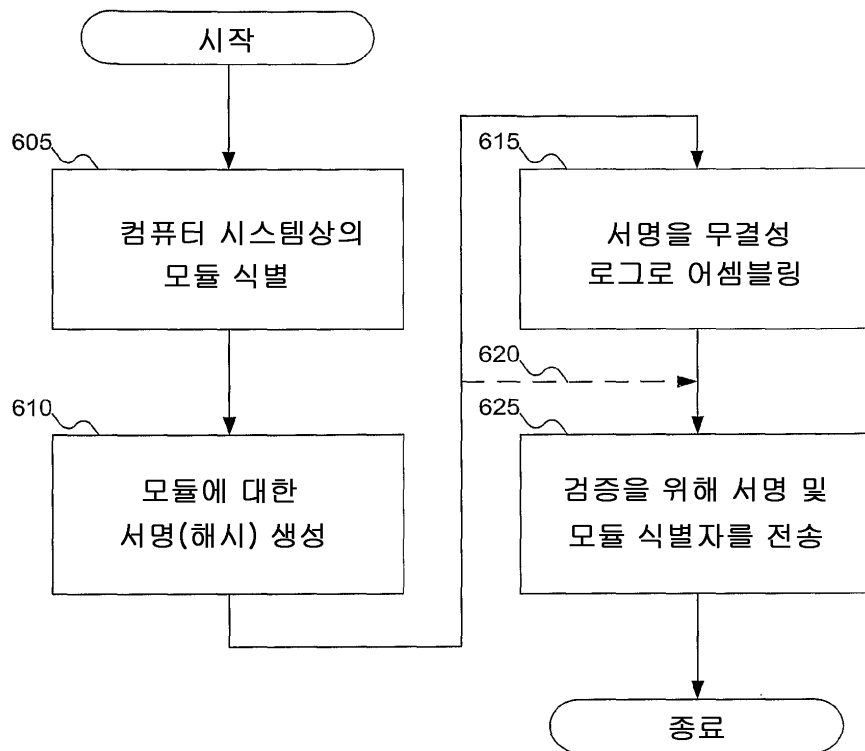
도면5a



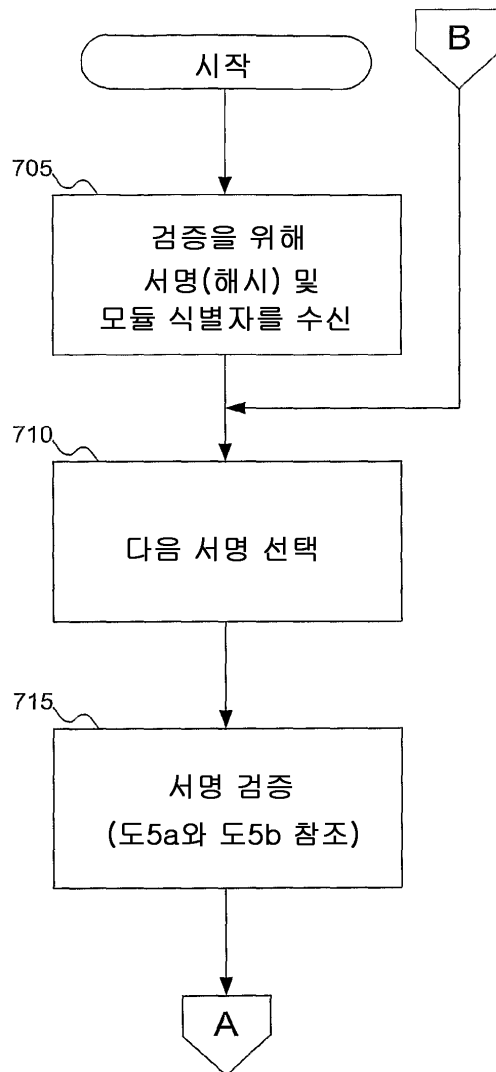
도면5b



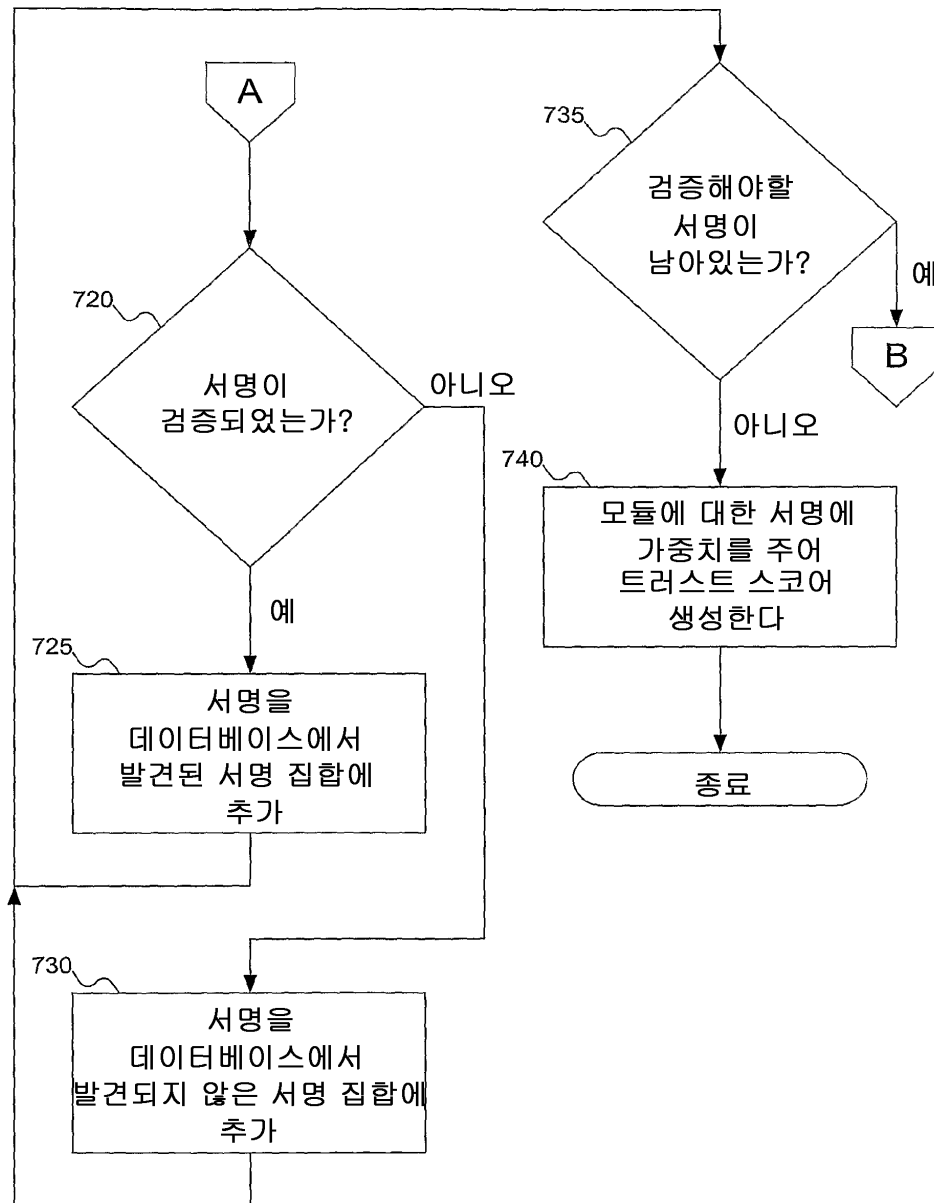
도면6



도면7a



도면7b



도면8

