(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년05월06일
(11) 등록번호 10-1258834
(24) 등록일자 2013년04월23일

(51) 국제특허분류(Int. Cl.)
H04W 88/18 (2009.01) *H04W 12/00* (2009.01)
(21) 출원번호 10-2011-0096331
(22) 출원일자 2011년09월23일
심사청구일자 2011년09월23일
(65) 공개번호 10-2013-0032619
(43) 공개일자 2013년04월02일
(56) 선행기술조사문헌
KR1020090128979 A*
KR1020100069107 A*
WO2008157806 A1
KR1020080070391 A
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
삼성에스디에스 주식회사
서울특별시 강남구 테헤란로 318 (역삼동)
(72) 발명자
정현우
경기도 성남시 분당구 미금로 246, 대원아파트 812동 402호 (금곡동, 청솔마을)
김종삼
경기도 화성시 반송동 시범한빛마을금호어울림아파트 242동 402호
(뒷면에 계속)
(74) 대리인
송경근

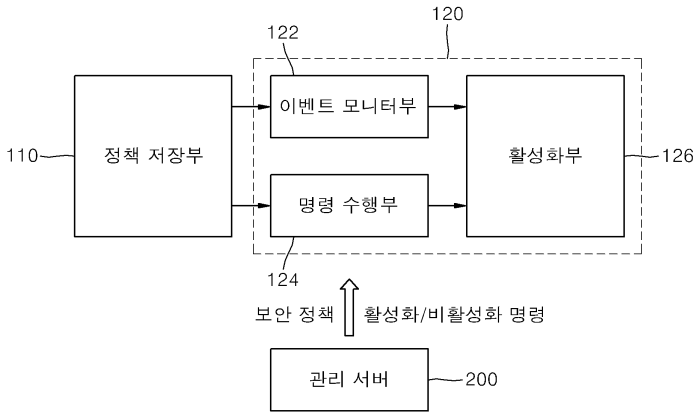
전체 청구항 수 : 총 22 항 심사관 : 복상문

(54) 발명의 명칭 **보안 정책에 의한 모바일 기기 관리장치 및 방법, 그리고 모바일 기기 관리를 위한 관리 서버**

(57) 요 약

보안 정책에 의한 모바일 기기 관리장치 및 방법, 그리고 모바일 기기 관리를 위한 관리 서버가 개시된다. 정책 저장부는 모바일 기기의 동작을 원격으로 관리하는 관리 서버로부터 활성화의 우선순위가 부여된 복수의 프로파일로 분류되며 모바일 기기의 기능에 대한 동작 상태가 정의된 복수의 보안 정책을 전송받아 저장한다. 정책 실행부는 모바일 기기에서 발생하는 이벤트 또는 관리 서버로부터 전송된 명령에 따라 복수의 프로파일 중에서 선택된 프로파일을 활성화하고, 활성화된 프로파일에 포함된 보안 정책들을 실행하여 모바일 기기의 기능을 제어한다. 본 발명에 따르면, 보안 정책의 내용이 변경될 때마다 관리 서버로부터 모바일 기기로 새로운 보안 정책을 전송하기 위한 통신 비용을 절감할 수 있고, 모바일 기기 내에서 독립적으로 적응적인 기능 제어를 수행할 수 있다.

대 표 도 - 도1



(72) 발명자

손호영

경기도 수원시 영통구 망포동 쌍용2차아파트 202동 1506호

길지중

서울특별시 송파구 송파대로8길 17, 907동 303호 (장지동, 송파파인타운 9단지)

김진용

서울특별시 송파구 올림픽로 435, 226동 2101호 (신천동, 파크리오)

특허청구의 범위

청구항 1

모바일 기기의 동작을 원격으로 관리하는 관리 서버로부터 복수의 프로파일로 분류되며 상기 모바일 기기의 기능에 대한 동작 상태가 정의된 복수의 보안 정책을 전송받아 저장하는 정책 저장부; 및

상기 모바일 기기에서 발생하는 이벤트 또는 상기 관리 서버로부터 전송된 명령에 따라 상기 복수의 프로파일 중에서 선택된 프로파일을 활성화하고, 상기 활성화된 프로파일에 포함된 보안 정책들을 실행하여 상기 모바일 기기의 기능을 제어하는 정책 실행부;를 포함하는 것을 특징으로 하는 모바일 기기 관리장치.

청구항 2

제 1항에 있어서,

상기 복수의 프로파일에는 활성화의 우선순위가 부여되고,

상기 정책 실행부는 상기 모바일 기기의 동일한 기능에 대한 동작 상태가 정의된 복수의 보안 정책이 복수의 상기 활성화된 프로파일에 각각 포함되어 있으면 상기 활성화된 프로파일들 중에서 상기 활성화의 우선순위가 가장 높은 프로파일에 포함된 보안 정책을 실행하는 것을 특징으로 하는 모바일 기기 관리장치.

청구항 3

제 1항 또는 제 2항에 있어서,

상기 복수의 프로파일은 각각 실행의 우선순위가 부여된 복수의 계층으로 분류되어 저장되며,

상기 정책 실행부는 상기 모바일 기기의 동일한 기능에 대한 동작 상태가 정의된 복수의 보안 정책이 상기 복수의 계층에 각각 포함되어 있으면 상기 활성화된 프로파일들 중에서 상기 실행의 우선순위가 가장 높은 계층에 포함된 프로파일의 보안 정책을 실행하는 것을 특징으로 하는 모바일 기기 관리장치.

청구항 4

제 3항에 있어서,

상기 복수의 계층은 항상 활성화된 상태를 유지하는 프로파일이 포함된 제1계층 및 상기 제1계층에 비해 상기 실행의 우선순위가 높으며 상기 모바일 기기에서 발생하는 이벤트 또는 상기 관리 서버로부터 전송된 명령에 대응하여 활성화되는 프로파일이 포함된 제2계층을 포함하는 것을 특징으로 하는 모바일 기기 관리장치.

청구항 5

제 4항에 있어서,

상기 복수의 계층은 사전에 설정된 긴급 이벤트에 대응하여 활성화되는 프로파일이 포함된 제3계층을 더 포함하는 것을 특징으로 하는 모바일 기기 관리장치.

청구항 6

제 5항에 있어서,

상기 제1계층에 포함된 프로파일은 상기 모바일 기기에서 발생하는 이벤트 또는 상기 긴급 이벤트와 각각의 이벤트에 대응하여 활성화되는 프로파일의 식별코드가 정의된 이벤트 정책을 더 포함하며,

상기 정책 실행부는 상기 이벤트 정책에 정의된 이벤트의 발생에 따라 상기 제2계층 및 상기 제3계층의 프로파일을 활성화하는 것을 특징으로 하는 모바일 기기 관리장치.

청구항 7

제 1항 또는 제 2항에 있어서,

상기 복수의 프로파일에는 상기 프로파일의 활성화 여부를 나타내는 활성화 지수가 부여되며,

상기 정책 실행부는,

상기 모바일 기기에서 발생하는 이벤트의 개시 및 종료에 따라 상기 각각의 프로파일에 부여된 활성화 지수를 산출하는 이벤트 모니터부;

상기 관리 서버로부터 전송된 활성화 또는 비활성화 명령에 따라 상기 각각의 프로파일에 부여된 활성화 지수를 산출하는 명령 수행부; 및

상기 이벤트 모니터부 및 상기 명령 수행부에 의해 산출된 상기 각각의 프로파일의 활성화 지수를 기초로 상기 복수의 프로파일 중에서 상기 활성화 지수의 값이 사전에 설정된 기준값 이상인 프로파일을 활성화하는 활성화부;를 포함하는 것을 특징으로 하는 모바일 기기 관리장치.

청구항 8

제 7항에 있어서,

상기 활성화부는 상기 이벤트 모니터부 또는 상기 명령 수행부로부터 갱신된 활성화 지수가 입력되면 상기 갱신된 활성화 지수를 기초로 상기 복수의 프로파일 중에서 활성화할 프로파일을 다시 선택하는 것을 특징으로 하는 모바일 기기 관리장치.

청구항 9

(a) 모바일 기기의 동작을 원격으로 관리하는 관리 서버로부터 복수의 프로파일로 분류되며 상기 모바일 기기의 기능에 대한 동작 상태가 정의된 복수의 보안 정책을 전송받아 저장하는 단계; 및

(b) 상기 모바일 기기에서 발생하는 이벤트 또는 상기 관리 서버로부터 전송된 명령에 따라 상기 복수의 프로파일 중에서 선택된 프로파일을 활성화하고, 상기 활성화된 프로파일에 포함된 보안 정책들을 실행하여 상기 모바일 기기의 기능을 제어하는 단계;를 포함하는 것을 특징으로 하는 모바일 기기 관리방법.

청구항 10

제 9항에 있어서,

상기 복수의 프로파일에는 활성화의 우선순위가 부여되고,

상기 (b) 단계에서, 상기 모바일 기기의 동일한 기능에 대한 동작 상태가 정의된 복수의 보안 정책이 복수의 상기 활성화된 프로파일에 각각 포함되어 있으면 상기 활성화된 프로파일들 중에서 상기 활성화의 우선순위가 가장 높은 프로파일에 포함된 보안 정책을 실행하는 것을 특징으로 하는 모바일 기기 관리방법.

청구항 11

제 9항 또는 제 10항에 있어서,

상기 복수의 프로파일은 각각 실행의 우선순위가 부여된 복수의 계층으로 분류되어 저장되며,

상기 (b) 단계에서, 상기 모바일 기기의 동일한 기능에 대한 동작 상태가 정의된 복수의 보안 정책이 상기 복수의 계층에 각각 포함되어 있으면 상기 활성화된 프로파일들 중에서 상기 실행의 우선순위가 가장 높은 계층에 포함된 프로파일의 보안 정책을 실행하는 것을 특징으로 하는 모바일 기기 관리방법.

청구항 12

제 11항에 있어서,

상기 복수의 계층은 항상 활성화된 상태를 유지하는 프로파일이 포함된 제1계층 및 상기 제1계층에 비해 상기 실행의 우선순위가 높으며 상기 모바일 기기에서 발생하는 이벤트 또는 상기 관리 서버로부터 전송된 명령에 대응하여 활성화되는 프로파일이 포함된 제2계층을 포함하는 것을 특징으로 하는 모바일 기기 관리방법.

청구항 13

제 12항에 있어서,

상기 복수의 계층은 사전에 설정된 긴급 이벤트에 대응하여 활성화되는 프로파일이 포함된 제3계층을 더 포함하는 것을 특징으로 하는 모바일 기기 관리방법.

청구항 14

제 13항에 있어서,

상기 제1계층에 포함된 프로파일은 상기 모바일 기기에서 발생하는 이벤트 또는 상기 긴급 이벤트와 각각의 이벤트에 대응하여 활성화되는 프로파일의 식별코드가 정의된 이벤트 정책을 더 포함하며,

상기 (b) 단계에서, 상기 이벤트 정책에 정의된 이벤트의 발생에 따라 상기 제2계층 및 상기 제3계층의 프로파일을 활성화하는 것을 특징으로 하는 모바일 기기 관리방법.

청구항 15

제 9항 또는 제 10항에 있어서,

상기 복수의 프로파일에는 상기 프로파일의 활성화 여부를 나타내는 활성화 지수가 부여되며,

상기 (b) 단계는,

(b1) 상기 모바일 기기에서 발생하는 이벤트의 개시 및 종료에 따라 상기 각각의 프로파일에 부여된 활성화 지수를 산출하는 단계;

(b2) 상기 관리 서버로부터 전송된 활성화 또는 비활성화 명령에 따라 상기 각각의 프로파일에 부여된 활성화 지수를 산출하는 단계; 및

(b3) 상기 (b1) 단계 및 상기 (b2) 단계에서 산출된 상기 각각의 프로파일의 활성화 지수를 기초로 상기 복수의 프로파일 중에서 상기 활성화 지수의 값이 사전에 설정된 기준값 이상인 프로파일을 활성화하는 단계;를 포함하는 것을 특징으로 하는 모바일 기기 관리방법.

청구항 16

제 15항에 있어서,

상기 (b3) 단계에서, 상기 (b1) 단계 또는 상기 (b2) 단계에서 활성화 지수가 갱신되면 상기 갱신된 활성화 지수를 기초로 상기 복수의 프로파일 중에서 활성화할 프로파일을 다시 선택하는 것을 특징으로 하는 모바일 기기 관리방법.

청구항 17

관리 대상인 모바일 기기의 기능에 대한 동작 상태가 정의된 복수의 보안 정책을 생성하여 각각 활성화의 우선순위가 부여된 복수의 프로파일로 분류하는 정책 생성부; 및

상기 복수의 프로파일로 분류된 상기 복수의 보안 정책을 상기 모바일 기기로 전송하는 정책 전송부;를 포함하는 것을 특징으로 하는 관리 서버.

청구항 18

제 17항에 있어서,

상기 모바일 기기로 전송된 복수의 프로파일 중 선택된 프로파일에 대한 활성화 또는 비활성화 명령을 전송하여 상기 모바일 기기에서 활성화된 프로파일에 포함된 보안 정책이 실행되도록 하는 명령 전송부를 더 포함하는 것을 특징으로 하는 관리 서버.

청구항 19

제 18항에 있어서,

상기 정책 생성부는 상기 복수의 프로파일을 각각 실행의 우선순위가 부여된 복수의 계층으로 분류하며,

상기 복수의 계층은 항상 활성화된 상태를 유지하는 프로파일이 포함된 제1계층 및 상기 제1계층에 비해 상기 실행의 우선순위가 높으며 상기 모바일 기기에 발생하는 이벤트 또는 상기 활성화 또는 비활성화 명령에 대응하

여 활성화 또는 비활성화되는 프로파일이 포함된 제2계층을 포함하는 것을 특징으로 하는 관리 서버.

청구항 20

제 19항에 있어서,

상기 복수의 계층은 사전에 설정된 긴급 이벤트에 대응하여 활성화되는 프로파일이 포함된 제3계층을 더 포함하며,

상기 정책 생성부는 상기 모바일 기기에 발생하는 이벤트 또는 상기 긴급 이벤트와 각각의 이벤트에 대응하여 활성화되는 프로파일의 식별코드가 정의된 이벤트 정책을 더 생성하여 상기 제1계층의 프로파일에 포함시키는 것을 특징으로 하는 관리 서버.

청구항 21

제 17항 내지 제 20항 중 어느 한 항에 있어서,

상기 정책 생성부는 상기 모바일 기기의 사용자 정보에 대응하여 상기 보안 정책의 내용을 변경하기 위한 예외 프로파일을 더 생성하며,

상기 정책 전송부는 상기 모바일 기기의 접속이 개시되면 상기 예외 프로파일의 내용에 따라 상기 복수의 프로파일에 포함된 보안 정책의 내용을 변경하여 상기 모바일 기기로 전송하는 것을 특징으로 하는 관리 서버.

청구항 22

제 9항 또는 제 10항에 기재된 모바일 기기 관리방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

명 세 서

기 술 분 야

[0001] 본 발명은 보안 정책에 의한 모바일 기기 관리장치 및 방법, 그리고 모바일 기기 관리를 위한 관리 서버에 관한 것으로, 보다 상세하게는, 상황별 모바일 기기 제어방법이 보안 정책으로서 사전에 정의되어 상황 발생시마다 그에 대응하는 보안 정책에 정의된 내용에 따라 모바일 기기를 제어하는 장치 및 방법, 그리고 상황별 모바일 기기 제어방법을 정의하는 보안 정책을 생성, 유지 및 변경하고 모바일 기기를 제어하도록 제공하는 장치에 관한 것이다.

배 경 기 술

[0002] 최근 모바일 기기의 성능이 향상되고 모바일 기기에서 구현될 수 있는 다양한 프로그램들이 제공됨에 따라 기업에서 업무 처리에 모바일 기기를 사용하는 경우가 증가하고 있다. 이를 위해 기업에서는 자체적으로 개발한 프로그램을 모바일 기기에 설치하여 기업의 구성원들이 사용하도록 한다.

[0003] 그런데 모바일 기기를 통한 업무 처리가 확대됨에 따라 외부에서도 기업의 내부 자료에 접근 가능하게 되었고, 정보 유출 방지 및 모바일 기기의 보안에 관한 중요성이 대두되었다.

[0004] 보안을 위해 모바일 기기의 각종 기능을 관리하는 기술로서 보안 정책에 의한 모바일 기기 관리 기술이 있다. 예를 들면, 한국공개특허 제2010-0069107에는 기기 관리(Device Management : DM) 서버로부터 단말기로 단말기의 기능 및 관리 동작에 대한 DM 커맨드가 전달되면, 단말기는 DM 커맨드를 저장하였다가 단말기의 상태가 조건을 만족하는 상태가 되면 DM 커맨드를 실행하는 구성이 기재되어 있다. 또한 한국공개특허 제2008-0070391호에는 휴대 단말기가 외부로부터 제어 명령을 수신하고, 제어 명령 적용을 위해 로딩된 엔진에 제어 명령을 적용하여 활성화한 후 제어 명령에 따른 단말기 제어를 수행하는 구성이 기재되어 있다.

[0005] 이와 같이 모바일 기기를 관리하기 위한 기존의 기술들은 정해진 정책들을 커맨드의 형태로 단말에 전송하고, 단말은 전송된 정책을 저장하였다가 조건에 따라 실행하는 방식을 사용한다. 이러한 방식들을 사용할 경우, 모바일 기기의 환경 변화에 따라 제어 내용, 즉 정책의 내용을 변경하기 위해서는 서버에서 다시 정책을 설정한 후 모바일 기기로 전송하여 정책을 갱신하여야 한다.

[0006] 따라서 기존의 모바일 기기 관리 기법들은 정책 내용 및 정책의 실행 조건이 서버에 의해 설정되므로 모바일 기

기에서 자체적으로 보안 정책을 변경하여 적용하거나 다양한 상황에 따른 보안 정책을 설정할 수 없다는 문제를 가진다.

발명의 내용

해결하려는 과제

[0007] 본 발명이 이루고자 하는 기술적 과제는, 서버와 매번 통신하지 않고 모바일 기기의 각종 기능을 제어할 수 있으며, 다양한 상황에 대응하는 보안 정책들을 사전에 설정하여 모바일 기기 내부에서 적응적으로 보안 정책을 실행할 수 있는 보안 정책에 의한 모바일 기기 관리장치 및 방법을 제공하는 데 있다.

[0008] 본 발명이 이루고자 하는 다른 기술적 과제는, 서버와 매번 통신하지 않고 모바일 기기의 각종 기능을 제어할 수 있으며, 다양한 상황에 대응하는 보안 정책들을 사전에 설정하여 모바일 기기 내부에서 적응적으로 보안 정책을 실행할 수 있는 보안 정책에 의한 모바일 기기 관리방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공하는 데 있다.

[0009] 본 발명이 이루고자 하는 또 다른 기술적 과제는, 모바일 기기의 다양한 상황에 대응하는 보안 정책들을 사전에 설정하여 모바일 기기에서 적응적으로 실행할 수 있도록 하는 모바일 기기 관리를 위한 관리 서버를 제공하는 데 있다.

과제의 해결 수단

[0010] 상기의 기술적 과제를 달성하기 위한, 본 발명에 따른 보안 정책에 의한 모바일 기기 관리장치는, 모바일 기기의 동작을 원격으로 관리하는 관리 서버로부터 활성화의 우선순위가 부여된 복수의 프로파일로 분류되며 상기 모바일 기기의 기능에 대한 동작 상태가 정의된 복수의 보안 정책을 전송받아 저장하는 정책 저장부; 및 상기 모바일 기기에서 발생하는 이벤트 또는 상기 관리 서버로부터 전송된 명령에 따라 상기 복수의 프로파일 중에서 선택된 프로파일을 활성화하고, 상기 활성화된 프로파일에 포함된 보안 정책들을 실행하여 상기 모바일 기기의 기능을 제어하는 정책 실행부;를 구비한다.

[0011] 상기의 기술적 과제를 달성하기 위한, 본 발명에 따른 보안 정책에 의한 모바일 기기 관리방법은, (a) 모바일 기기의 동작을 원격으로 관리하는 관리 서버로부터 활성화의 우선순위가 부여된 복수의 프로파일로 분류되며 상기 모바일 기기의 기능에 대한 동작 상태가 정의된 복수의 보안 정책을 전송받아 저장하는 단계; 및 (b) 상기 모바일 기기에서 발생하는 이벤트 또는 상기 관리 서버로부터 전송된 명령에 따라 상기 복수의 프로파일 중에서 선택된 프로파일을 활성화하고, 상기 활성화된 프로파일에 포함된 보안 정책들을 실행하여 상기 모바일 기기의 기능을 제어하는 단계;를 갖는다.

[0012] 상기의 다른 기술적 과제를 달성하기 위한, 본 발명에 따른 모바일 기기 관리를 위한 관리 서버는, 관리 대상인 모바일 기기의 기능에 대한 동작 상태가 정의된 복수의 보안 정책을 생성하여 각각 활성화의 우선순위가 부여된 복수의 프로파일로 분류하는 정책 생성부; 및 상기 복수의 프로파일로 분류된 상기 복수의 보안 정책을 상기 모바일 기기로 전송하는 정책 전송부;를 구비한다.

발명의 효과

[0013] 본 발명에 따른 보안 정책에 의한 모바일 기기 관리장치 및 방법, 그리고 모바일 기기 관리를 위한 관리 서버에 의하면, 모바일 기기에 대하여 발생 가능한 다양한 상황에 따라 서로 다르게 정의된 다양한 보안 정책을 미리 생성하여 모바일 기기에 저장한 후 적응적으로 모바일 기기의 기능을 제어함으로써, 보안 정책의 내용이 변경될 때마다 관리 서버로부터 모바일 기기로 새로운 보안 정책을 전송하기 위한 통신 비용을 절감할 수 있고, 모바일 기기 내에서 독립적으로 적응적인 기능 제어를 수행할 수 있다.

도면의 간단한 설명

[0014] 도 1은 본 발명에 따른 보안 정책에 의한 모바일 기기 관리장치에 대한 바람직한 실시예의 구성을 도시한 블록도,

도 2는 본 발명에 따른 관리 서버에 대한 바람직한 실시예의 구성을 도시한 블록도,

도 3은 관리 서버의 정책 생성부에 의해 생성되어 모바일 기기 관리장치의 정책 저장부에 저장되는 보안 정책들

의 계층별, 프로파일별 분류의 일 실시예를 도시한 도면,

도 4는 정책 저장부에 저장된 각 프로파일의 활성화 지수가 산출된 일 예를 도시한 도면,

도 5는 활성화부가 활성화된 프로파일들의 우선순위를 고려하여 각 보안정책의 정책값을 결정하는 예를 도시한 도면, 그리고,

도 6은 본 발명에 따른 보안 정책에 의한 에 대한 바람직한 실시예의 수행과정을 도시한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0015] 이하에서 첨부된 도면들을 참조하여 본 발명에 따른 보안 정책에 의한 모바일 기기 관리장치 및 방법, 그리고 모바일 기기 관리를 위한 관리 서버의 바람직한 실시예에 대해 상세하게 설명한다.

[0016] 도 1은 본 발명에 따른 보안 정책에 의한 모바일 기기 관리장치에 대한 바람직한 실시예의 구성을 도시한 블록도이다.

[0017] 도 1을 참조하면, 본 발명에 따른 모바일 기기 관리장치(100)는 정책 저장부(110) 및 정책 실행부(120)를 구비하며, 정책 실행부(120)는 이벤트 모니터부(122), 명령 수행부(124) 및 활성화부(126)를 통해 기능을 수행할 수 있다.

[0018] 본 발명에 따른 모바일 기기 관리장치(100)는 제어 대상인 모바일 기기 내부에 구현될 수 있으며, 모바일 기기의 동작을 원격으로 관리하는 관리 서버(200)와 통신한다. 본 발명에 따른 관리 서버(200)는 모바일 기기에 적용되는 보안 정책을 관리 및 유지하며, 필요에 따라 모바일 기기, 즉 본 발명에 따른 모바일 기기 관리장치(100)로 제어 명령 내지 보안 정책을 전송한다.

[0019] 또한 본 발명에 따른 모바일 기기 관리장치(100)는 동일한 조직에 속하는 구성원들의 모바일 기기를 제어하기 위해 사용될 수 있다. 예를 들면, 특정 회사에서 보안 유지를 위해 회사 구성원들의 모바일 기기에 본 발명에 따른 모바일 기기 관리장치(100)를 설치하여 각각의 구성원의 모바일 기기의 기능을 제어할 수 있다. 이러한 경우에 관리 서버(200)는 회사에서 자체적으로 구비하거나 보안 관련 업무를 대행하는 업체에서 구비할 수 있다.

[0020] 이하에서는 본 발명에 따른 모바일 기기 관리장치(100)가 특정 회사에 소속된 구성원들의 모바일 기기를 제어하도록 구현되는 경우를 대표적인 실시예로 하여 각 구성요소의 동작을 상세하게 설명한다.

[0021] 도 2는 본 발명에 따른 관리 서버(200)에 대한 바람직한 실시예의 구성을 도시한 블록도이다.

[0022] 도 2를 참조하면, 관리 서버(200)는 정책 생성부(210), 정책 전송부(220) 및 명령 전송부(230)를 구비한다. 관리 서버(200)의 각 구성요소가 수행하는 상세한 동작은 이하에서 모바일 기기 관리장치(100)의 각 구성요소의 동작과 함께 설명한다.

[0023] 본 발명에 따른 모바일 기기 관리장치(100)의 정책 저장부(110)는 관리 서버(200)로부터 활성화의 우선순위가 부여되며 모바일 기기의 기능에 대한 동작 상태가 정의된 복수의 보안 정책을 전송받아 저장한다.

[0024] 정책 저장부(110)에 저장되는 보안 정책은 모바일 기기의 각종 기능, 구체적으로 카메라, 와이파이(wi-fi), 블루투스(bluetooth) 동작 제어, 화면 잠금 및 각종 소프트웨어의 실행 제어 등과 같은 동작 상태를 정의하도록 관리 서버(200)의 정책 생성부(210)에 의해 생성 및 전송되며, 모바일 기기 관리장치(100)의 정책 실행부(120)는 각각의 보안 정책에 정의된 내용에 따라 모바일 기기의 기능을 제어한다. 예를 들면, 정책 실행부(120)에 의해 활성화된 보안 정책에 카메라 기능의 차단이 정의되어 있다면 정책 실행부(120)는 모바일 기기의 사용자가 카메라 기능을 사용할 수 없도록 차단한다.

[0025] 이때 각각의 기능을 차단 또는 차단 해제하는 방법은 특정한 한 가지의 방법에 한정되지 않으며, 가능한 모든 방법이 사용될 수 있다. 또한 모바일 기기의 기능을 제어하는 구체적인 방법이 관리 서버(200)의 정책 생성부(210)에 의해 보안 정책이 생성될 때 관리자의 설정에 따라 함께 정의될 수도 있다.

[0026] 모바일 기기의 기능을 제어하는 구체적인 방법의 예로서, 자원을 선점하는 방법이 있다. 이는 모바일 기기의 특정 기능을 사용하는 프로그램이 다양하여 프로그램의 실행을 제약하는 방법을 사용하기 어려울 경우, 해당 기능을 수행하는 시스템의 자원을 선점하는 방식이다. 예를 들면, 모바일 기기의 카메라의 경우에는 카메라 기능을 필요로 하는 각종 프로그램이 실행될 때 특정한 브로드캐스트 인텐트가 발생하지 않으며 카메라 기능을 사용하는 프로그램이 매우 다양하다. 따라서 정책 실행부(120)는 카메라 기능의 차단이 정의된 보안 정책을 활성화할

경우에 시스템의 카메라 자원을 선점하여 카메라 기능을 필요로 하는 프로그램이 동작할 수 없도록 한다.

[0027] 모바일 기기의 기능을 제어하는 다른 방법으로서, 브로드캐스트 감시 방법이 있다. 브로드캐스트 감시 방법은 모바일 기기의 특정 기능이 실행되었을 때 발생하는 브로드캐스트 인텐트를 사용하는 방법이다. 예를 들면, 블루투스의 경우에 블루투스를 활성화하거나 페어링 시도 또는 연결 등의 동작이 발생하면 시스템이 자동으로 브로드캐스트 인텐트를 전송하므로, 정책 실행부(120)는 브로드캐스트 인텐트를 감지하여 보안 정책에 정의된 대로 블루투스 기능을 차단 또는 차단 해제할 수 있다. 이러한 브로드캐스트 감시 방법은 모바일 기기의 기능들 중에서 마이크로SD, 와이파이 및 테더링 기능에 적용할 수 있다.

[0028] 또한 정책 실행부(120)는 스레드 감시 방법에 의해 모바일 기기의 기능을 제어할 수 있다. 스레드 감시 방법은 자원을 선점할 수 없으며 특정한 이벤트 브로드캐스트가 존재하지 않는 경우에 사용할 수 있는 방법이다. 예를 들면, 모바일 기기에서 항상 실행되어 있어야 하는 소프트웨어 프로그램이 종료되었는지 또는 지속적으로 실행되고 있는지 여부를 스레드를 통해 감시할 수 있다.

[0029] 이상에서 설명한 여러 가지 방법에 의해 모바일 기기의 각종 기능을 제어하도록 정의된 보안 정책은 관리 서버(200)의 정책 생성부(210)에 의해 생성되고 이후 지속적으로 관리되면서 그 내용이 유지 및 변경된다. 또한 회사에서 구성원들의 모바일 기기를 제어하고자 할 경우 정책 생성부(210)는 관리자의 설정에 따라 개별 구성원의 구체적 개인 정보, 예를 들면 소속 부서 및 직급 등과 같은 정보에 적합하도록 보안 정책을 적응적으로 생성하며, 정책 전송부(220)는 이와 같이 적응적으로 생성된 보안 정책을 각 구성원의 모바일 기기에 설치된 모바일 기기 관리장치(100)로 전송한다.

[0030] 앞에서 설명한 바와 같이 정책 생성부(210)는 모바일 기기의 각종 기능의 동작 상태를 정의하는 보안 정책을 일반적으로 생성한다. 그 밖에 정책 생성부(210)는 보안 정책 외에도 모바일 기기에서 보안 정책이 활성화되는 경우를 정의하는 이벤트 정책을 별도로 생성할 수 있다. 이벤트 정책은 모바일 기기에서 발생하는 이벤트 또는 사전에 설정된 긴급 이벤트와 각각의 이벤트에 대응하여 활성화되는 프로파일의 식별코드를 정의한다. 이벤트 정책의 활성화에 따른 모바일 기기의 제어에 관하여는 뒤에서 상세하게 설명한다.

[0031] 한편, 정책 생성부(210)에 의해 생성되는 복수의 보안 정책은 활성화의 우선순위가 부여된 복수의 프로파일로 분류될 수 있다. 프로파일은 한 개 이상의 보안 정책의 묶음을 정의하며, 동일 프로파일에 속하는 보안 정책들은 동시에 활성화 또는 비활성화된다. 각각의 프로파일에는 식별코드 및 활성화의 우선순위가 부여된다. 활성화의 우선순위는 모바일 기기의 동일한 기능에 대한 동작 상태가 정의된 보안 정책이 각각 서로 다른 프로파일에 포함되고 복수의 프로파일이 모두 활성화되었을 때, 모바일 기기의 기능을 제어하는 데 있어 어떠한 프로파일에 포함된 보안 정책의 내용을 따를 것인지 결정하기 위해 사용된다. 또한 우선순위는 숫자로 부여될 수 있으며, 그 값이 작을수록 우선순위가 높음을 나타낼 수 있다.

[0032] 예를 들면, 모바일 기기의 카메라 기능을 제어하는 복수의 보안 정책이 복수의 프로파일에 각각 포함되어 있을 때 우선순위가 1인 프로파일 A에 포함된 보안 정책은 카메라 기능을 차단하는 동작을 정의하며 우선순위가 2인 프로파일 B에 포함된 보안 정책은 카메라 기능의 차단을 해제하는 동작을 정의하는 경우, 두 개의 프로파일이 모두 활성화되면 서로 상반된 동작 상태가 정의된 보안 정책이 동시에 활성화된다. 이러한 경우에 정책 실행부(120)는 우선순위가 더 높은 프로파일 A에 포함된 보안 정책의 내용에 따라 카메라 기능을 차단한다.

[0033] 이와 같이 관리 서버(200)의 정책 생성부(210)가 모바일 기기의 동일한 기능에 대한 다양한 동작을 정의하는 복수의 보안 정책을 생성하고, 보안 정책들을 복수의 프로파일로 분류하는 것은 모바일 기기와 관련된 다양한 상황에 따라 모바일 기기의 각 기능이 다르게 제어되어야 할 필요성에 따른 것이다.

[0034] 앞에서 설명한 바와 같이 기존에는 모바일 기기의 각 기능에 대한 동작 상태를 변경하고자 하는 경우에 매번 새로운 제어 명령을 모바일 기기로 전송하여야 하는 문제가 있었다. 그러나 본 발명에 따른 관리 서버(200)의 정책 생성부(210)는 모바일 기기의 각 기능이 서로 다르게 제어될 수 있는 다양한 상황을 반영하여 복수의 프로파일을 생성하고, 각각의 프로파일마다 동시에 활성화되는 복수의 보안 정책을 포함시킨다.

[0035] 그에 따라 보안 정책을 전송받은 모바일 기기에서 본 발명에 다른 모바일 기기 관리장치(100)의 정책 실행부(120)는 각각의 상황에 맞는 프로파일을 활성화하여 모바일 기기의 기능을 제어함으로써 모바일 기기와 서버 간의 데이터 통신 비용을 감소시킬 수 있으며, 보안 정책의 구성의 유연성 및 용이성을 향상시킬 수 있다.

[0036] 나아가 정책 생성부(210)는 복수의 보안 정책을 각각 포함하고 있는 복수의 프로파일을 다시 복수의 계층으로 분류할 수 있으며, 각각의 계층에는 실행의 우선순위가 부여될 수 있다. 정책 전송부(220)는 계층별, 프로파일별로 분류된 보안 정책들을 모바일 기기로 전송하며, 본 발명에 다른 모바일 기기 관리장치(100)의 정책 저장부

(110)는 정책 전송부(220)로부터 전송된 계층별, 프로파일별 분류를 유지하여 보안 정책들을 저장한다.

[0037] 복수의 프로파일이 분류되는 계층은 정책 실행부(120)에 의해 항상 활성화된 상태를 유지할 필요가 있는 프로파일이 포함된 제1계층 및 제1계층에 비해 실행의 우선순위가 높으며 정책 실행부(120)에 의해 선택적으로 활성화 또는 비활성화되는 제2계층으로 이루어진 제2계층으로 구분할 수 있다.

[0038] 제1계층의 프로파일이 모바일 기기에서 항상 활성화되므로, 앞에서 설명한 이벤트 정책은 제1계층의 프로파일에만 포함되도록 정책 생성부(210)에 의해 생성된다. 또한 이벤트 정책 내에서 각각의 이벤트에 대응하여 정의된 프로파일은 제2계층에 포함된 프로파일만 해당된다. 제1계층의 프로파일은 이벤트 발생에 무관하게 항상 활성화되기 때문이다.

[0039] 즉, 정책 실행부(120)는 관리 서버(200)로부터 전송된 보안 정책들이 계층별, 프로파일별로 정책 저장부(110)에 저장된 후 모바일 기기에 대한 보안 프로세스가 개시되면 제1계층의 프로파일을 우선적으로 활성화하여 항상 활성화된 상태로 유지하고, 모바일 기기에서 이벤트 정책에 정의된 이벤트가 발생하면 발생한 이벤트에 대응하여 정의된 식별코드를 가지는 프로파일을 활성화한다.

[0040] 제2계층에 포함된 프로파일은 앞에서 설명한 이벤트 정책에 정의된 이벤트 중 모바일 기기에서 발생한 이벤트 또는 관리 서버(200)의 명령 전송부(230)로부터 전송된 활성화/비활성화 명령에 따라 정책 실행부(120)에 의해 활성화 또는 비활성화될 수 있다.

[0041] 도 3은 관리 서버(200)의 정책 생성부(210)에 의해 생성되어 모바일 기기 관리장치(100)의 정책 저장부(110)에 저장되는 보안 정책들의 계층별, 프로파일별 분류의 일 실시예를 도시한 도면이다. 도 3에서 각각의 프로파일에 포함된 보안 정책들은 그 도시를 생략하였다.

[0042] 도 3의 우측에 도시된 프로파일들은 관리 서버(200)의 정책 생성부(210)에 의해 생성된 보안 정책들을 나타내며, 좌측에 도시된 프로파일들은 모바일 기기 관리장치(100)의 정책 저장부(110)에 저장되는 보안 정책들을 나타낸다.

[0043] 도 3을 참조하면, 복수의 보안 정책을 각각 포함하는 복수의 프로파일은 B(Base) 계층, W(Wrapper) 계층 및 E(Emergency) 계층으로 분류된다. B 계층은 모바일 기기 내에서 항상 활성화된 상태를 유지하는 프로파일이 포함된 계층으로, 앞에서 설명한 제1계층에 대응한다. 또한 W 계층은 B 계층의 프로파일에 포함된 이벤트 정책에 의해 정의된 이벤트의 발생 또는 관리 서버(200)로부터의 명령에 따라 활성화 또는 비활성화되는 프로파일이 포함된 계층으로, 앞에서 설명한 제2계층에 대응한다.

[0044] 한편, 도 3에 도시된 계층에는 B 계층 및 W 계층 외에 E 계층이 더 포함되어 있는데, E 계층은 이벤트 정책에 정의된 정책들 중에서 사전에 설정된 긴급 이벤트, 즉 모바일 기기가 정상적으로 동작하는 경우에는 발생하지 않는 긴급/비상 사태를 의미하는 이벤트의 발생에 따라 활성화되는 프로파일이 포함된 계층이다. E 계층은 B 계층 및 W 계층에 비해 실행의 우선순위가 높게 설정된다.

[0045] 관리 서버(200) 측에 도시된 각각의 계층 중에서 B 계층 및 W 계층에는 보안 정책이 포함된 프로파일 외에 '예외 프로파일'이 더 포함되어 있다. 예외 프로파일은 모바일 기기의 관리 편의성을 위하여 관리자에 의해 설정된 보안 정책으로 구성된다. 예를 들면, 모바일 기기들을 특정한 기준에 따라 복수의 그룹으로 분류하여 관리할 때 각 그룹별로 모바일 기기의 기능에 대하여 필요한 예외적인 제어 동작을 보안 정책으로 정의하여 예외 프로파일에 포함시킬 수 있다. 이러한 예외 프로파일은 모바일 기기의 그룹별 제어뿐 아니라 특정 사용자의 모바일 기기에 대하여 예외적인 제어 동작이 필요한 경우에도 설정될 수 있다.

[0046] 관리 서버(200)의 정책 생성부(210)는 관리자의 설정에 따라 일반적인 보안 정책을 생성하여 프로파일별, 계층별로 분류하고, B 계층 및 W 계층에 포함되는 프로파일에 대하여는 예외 프로파일을 생성한다. 정책 전송부(220)는 모바일 기기의 접속이 확인되면 접속한 모바일 기기의 사용자 정보를 기초로 예외 프로파일의 보안 정책을 각 계층에 포함된 프로파일에 적용하여 모바일 기기로 전송한다. 그에 따라 모바일 기기 관리장치(100)의 정책 저장부(110)에는 예외 처리가 이미 적용된 프로파일들이 계층별로 저장된다.

[0047] 정책 저장부(110)에 저장되는 복수의 계층 중에서 B 계층과 E 계층에는 프로파일이 한 개씩만 포함되어 있다. 그러나 W 계층의 프로파일은 이벤트 발생 또는 관리 서버(200)로부터의 명령에 따라 선택적으로 활성화/비활성화되므로 모바일 기기의 다양한 상황을 모두 반영할 수 있도록 복수의 프로파일이 W 계층에 저장된다. 도 3에서 B 계층 및 E 계층에 포함된 프로파일에는 식별코드(BC, EC)만 부여되며, W 계층에 포함된 프로파일들에는 각각 식별코드(WC)와 함께 우선순위(1~N)이 부여된다. 우선순위를 나타내는 숫자는 그 값이 작을수록 높은 우선순위

를 나타냄을 앞에서 설명한 바 있다.

[0048] 이하에서는 모바일 기기 관리장치(100)의 정책 실행부(120)가 이벤트 정책에 정의된 이벤트의 발생 또는 관리 서버(200)로부터 전송된 명령에 따라 정책 저장부(110)에 저장된 각각의 프로파일을 활성화/비활성화하는 구체적인 동작에 대하여 상세하게 설명한다.

[0049] 먼저 정책 실행부(120)의 활성화부(126)는 앞에서 설명한 바와 같이 모바일 기기에 대한 보안 프로세스가 개시되면 정책 저장부(110)에 저장된 B 계층의 프로파일을 활성화한다. 예를 들면, B 계층의 프로파일에 포함된 보안 정책은 카메라 사용 가능, 와이파이 사용 가능, 트위터 사용 불가, 마이크로SD 사용 가능에 관한 것이고, 이벤트 정책으로서 모바일 기기에서의 업무 프로그램 실행 이벤트 및 V3 프로그램 삭제 이벤트가 각각 정의된다.

[0050] 또한 W 계층의 프로파일들 중 우선순위가 가장 높은 WC1 프로파일에는 카메라 사용 가능, 와이파이 사용 불가, 마이크로SD 사용 가능의 상태가 각각 정의된 보안 정책들이 포함되며, WC1 프로파일보다 우선순위가 낮은 WC2 프로파일에는 카메라 사용 불가, 와이파이 사용 불가, 마이크로SD 사용 불가의 상태가 각각 정의된 보안 정책들이 포함된다. 한편, E 계층의 프로파일에는 카메라 사용 불가, 와이파이 사용 불가, 마이크로SD 사용 불가, 블루투스 사용 불가, 단말 잠금 활성화, 테더링 사용 불가의 상태가 각각 정의된 보안 정책들이 포함된다.

[0051] B 계층의 프로파일이 활성화되어 활성화부(130)가 B 계층의 프로파일에 포함된 보안 정책에 따라 모바일 기기의 기능을 제어한 후, 정책 실행부(120)의 이벤트 모니터부(122)는 모바일 기기에 발생하는 이벤트의 개시 및 종료에 따라 각각의 프로파일에 부여된 활성화 지수를 산출한다.

[0052] 정책 저장부(110)에 저장된 프로파일에는 각각 활성화 지수가 부여되며, 활성화 지수는 프로파일의 활성화 여부를 결정하는 데 사용된다. 이벤트 모니터부(122)는 이벤트 정책에 정의된 이벤트가 발생하면 해당 이벤트에 대응하여 활성화되는 것으로 정의된 프로파일의 활성화 지수를 증가시키고, 이벤트가 종료하면 해당 이벤트에 대응하여 정의된 프로파일의 활성화 지수를 감소시킨다.

[0053] 바람직하게는, 이벤트 모니터부(122)는 이벤트의 발생 및 종료시마다 프로파일의 활성화 지수를 1만큼 증가 또는 감소시킬 수 있다. 또한 하나의 프로파일이 2 이상의 이벤트에 동시에 대응되며, 대응되는 복수의 이벤트가 모두 발생한 경우에는 해당 프로파일의 활성화 지수를 발생한 이벤트의 개수만큼 증가시킨다.

[0054] 앞에서 설명한 이벤트 정책의 예와 같이 모바일 기기에 설치된 업무 프로그램의 실행이 감지되면 해당 모바일 기기의 사용자가 모바일 기기를 통해 회사의 업무 관련 서버에 접속하는 것을 의미하므로 모바일 기기의 각종 기능을 제한하는 프로파일이 활성화될 필요가 있다. 이때 업무 프로그램의 실행 이벤트는 W 계층의 프로파일들 중 WC2 프로파일에 대응된다.

[0055] 따라서 이벤트 모니터부(122)는 업무 프로그램의 실행 이벤트에 대응하여 정의된 WC2 프로파일의 활성화 지수를 증가시킨다. 또한 모바일 기기에서 업무 프로그램이 종료되면 WC2 프로파일의 활성화 지수를 감소시킨다.

[0056] 한편, 앞에서 예로 든 이벤트 정책 중 모바일 기기에서 V3 프로그램 삭제 이벤트는 긴급 이벤트에 해당하며, 긴급 이벤트에 대응하여 정의된 프로파일은 E 계층의 프로파일이다. 이벤트 모니터부(122)는 모바일 기기에서 V3 프로그램이 삭제되는 이벤트가 발생하면 그에 대응하는 E 계층의 프로파일의 활성화 지수를 1만큼 증가시킨다.

[0057] 명령 수행부(124)는 관리 서버(200)로부터 전송된 활성화 또는 비활성화 명령에 따라 각각의 프로파일에 부여된 활성화 지수를 산출한다. 구체적으로, 활성화 또는 비활성화 명령은 관리 서버(200)의 명령 전송부(230)로부터 전송된다. 관리 서버(200)에서 활성화 또는 비활성화 명령을 전송하는 일 예로는 모바일 기기가 특정 구역에 진입하는 경우가 있다.

[0058] 모바일 기기의 특정 구역으로의 진입 여부는 해당 구역에 설치된 게이트에 모바일 기기의 사용자가 출입카드 또는 모바일 기기 자체를 인식하거나 관리자의 수작업을 통해 알 수 있다. 이러한 모바일 기기의 진입은 관리 서버(200)로 전달되며, 관리 서버(200)의 명령 전송부(230)는 해당 모바일 기기로 특정 프로파일, 예를 들면 W 계층의 WC1 프로파일의 활성화 명령을 전송한다. 명령 수행부(124)는 전송된 활성화 명령에 따라 WC1 프로파일의 활성화 지수를 증가시킨다.

[0059] 도 4는 정책 저장부(110)에 저장된 각 프로파일의 활성화 지수가 산출된 일 예를 도시한 도면이다. 도 4를 참조하면, B 계층의 프로파일은 이벤트 발생 여부 또는 관리 서버(200)로부터의 명령 전송 여부에 무관하게 항상 활성화되므로 별도의 활성화 지수가 부여되지 않으며, W 계층 및 E 계층의 프로파일에 대하여만 활성화 지수가 산출된다.

[0060] 활성화 지수의 산출은 이벤트 모니터부(122) 및 명령 수행부(124)에 의해 이루어지며, 도 4의 예에서 활성화 지수는 이벤트 발생 또는 관리 서버(200)로부터의 명령 전송에 따라 1만큼 증가 또는 감소된다. W 계층의 프로파일들 중에서 WC3 프로파일의 활성화 지수가 2인 것은 해당 프로파일에 대응하여 정의된 이벤트의 발생 또는 해당 프로파일의 활성화 명령이 중복된 것을 의미한다.

[0061] 활성화부(126)는 이벤트 모니터부(122) 및 명령 수행부(124)에 의해 산출된 각각의 프로파일의 활성화 지수를 기초로 복수의 프로파일 중에서 활성화 지수의 값이 사전에 설정된 기준값, 예를 들면 1 이상인 프로파일을 활성화하고, 활성화된 프로파일에 포함된 보안 정책들을 실행한다. 즉, 도 4에 도시된 예에서는 W 계층의 프로파일들 중에서 WC2 및 WC3 프로파일 및 E 계층의 프로파일의 활성화 지수가 1 이상이므로 활성화부(126)에 의해 활성화된다.

[0062] 앞에서 설명한 바와 같이 모바일 기기의 동일한 기능에 대한 동작 상태가 정의된 복수의 보안 정책이 복수의 활성화된 프로파일에 동시에 포함된 경우가 발생할 수 있다. 따라서 활성화부(126)는 각 프로파일이 포함된 계층에 부여된 실행의 우선순위 및 각 프로파일에 부여된 활성화의 우선순위를 고려하여 정책값, 즉 구체적인 기능 제어 방법을 결정한다.

[0063] 도 5는 활성화부(126)가 활성화된 프로파일들의 우선순위를 고려하여 각 보안정책의 정책값을 결정하는 예를 도시한 도면이다.

[0064] 도 5를 참조하면, B 계층의 프로파일은 항상 활성화되어 있으며, W 계층의 프로파일들 중에서 WC1, WC3 및 WC4 프로파일이 활성화되고, E 계층의 프로파일은 비활성화 상태이다. 또한 각각의 프로파일에 포함된 보안 정책은 식별 코드 및 정책값을 가진다. 정책값은 해당 보안 정책이 정하는 모바일 기기의 기능을 어떤 동작 상태로 제어할 것인가를 나타내는 값으로, 그 값은 관리자가 임의로 설정할 수 있다.

[0065] 예를 들면, 활성화부(126)는 B 계층의 프로파일에 포함된 각 보안 정책의 정책값을 결정하여 결과 프로파일을 생성한다. 구체적으로, B 계층의 P1 보안 정책은 W 계층에서 활성화된 WC1 및 WC4 프로파일에도 동시에 포함되어 있으며, 세 개의 프로파일 중에서 WC1 프로파일의 우선순위가 가장 높으므로 WC1 프로파일에 포함된 P1 보안 정책의 정책값인 11이 최종 정책값으로 결정될 수 있다.

[0066] 활성화부(126)는 이상의 과정을 P2 내지 P6 보안 정책에 대하여도 반복적으로 수행하여 각각 최종 정책값이 결정된 보안 정책들로 이루어진 결과 프로파일을 생성한다. 이때 B 계층의 프로파일에 포함되어 있던 E1 이벤트 정책은 결과 프로파일에 그대로 반영된다.

[0067] 한편, 이벤트 모니터부(122) 및 명령 수행부(124)는 이벤트 정책에 정의된 이벤트의 발생 여부 또는 관리 서버(200)로부터의 명령 전송 여부에 따라 실시간으로 각 프로파일의 활성화 지수를 갱신한다. 갱신된 활성화 지수는 활성화부(126)로 입력되고, 활성화부(126)는 갱신된 활성화 지수를 기초로 앞에서 설명한 프로파일 활성화 및 보안 정책의 정책값 설정 과정을 다시 수행한다.

[0068] 도 6은 본 발명에 따른 보안 정책에 의한 에 대한 바람직한 실시예의 수행과정을 도시한 흐름도이다.

[0069] 도 6을 참조하면, 모바일 기기가 관리 서버(200)에 접속하면 관리 서버(200)의 정책 전송부(220)는 정책 생성부(210)에 의해 생성된 보안 정책들을 계층별, 프로파일별로 분류하여 모바일 기기 관리장치(100)로 전송하고, 정책 저장부(110)는 전송된 보안 정책들을 저장한다(S610).

[0070] 이후 정책 실행부(120)의 활성화부(126)는 복수의 계층 중에서 B 계층의 프로파일을 우선 활성화하여 항상 활성화 상태를 유지하도록 한다(S620). 다음으로 이벤트 모니터부(122) 및 명령 수행부(124)는 각각 B 계층의 프로파일에 포함된 이벤트 정책에 의해 정의된 이벤트의 개시 및 종료 또는 관리 서버(200)로부터 전송된 활성화 및 비활성화 명령에 따라 대응하는 프로파일의 활성화 지수를 증가 또는 감소시킨다(S630).

[0071] 활성화부(126)는 산출된 활성화 지수를 기초로 활성화 지수가 사전에 설정된 기준값 이상인 프로파일을 활성화시키고(S640), 활성화된 프로파일들의 우선순위를 참조하여 보안 정책의 정책값, 즉 모바일 기기의 기능 제어 방식을 결정한다(S650). 마지막으로 활성화부(126)는 정책값이 결정된 보안 정책들을 실행하여 모바일 기기의 각 기능을 제어한다(S660).

[0072] 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 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광데이터 저장장치 등이 있으며, 또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현되는 것도

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

[0073] 이상에서 본 발명의 바람직한 실시예에 대해 도시하고 설명하였으나, 본 발명은 상술한 특정의 바람직한 실시예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자라면 누구든지 다양한 변형 실시가 가능한 것은 물론이고, 그와 같은 변경은 청구범위 기재의 범위 내에 있게 된다.

부호의 설명

[0074] 100 - 모바일 기기 관리장치

110 - 정책 저장부

120 - 정책 실행부

122 - 이벤트 모니터부

124 - 명령 수행부

126 - 활성화부

200 - 관리 서버

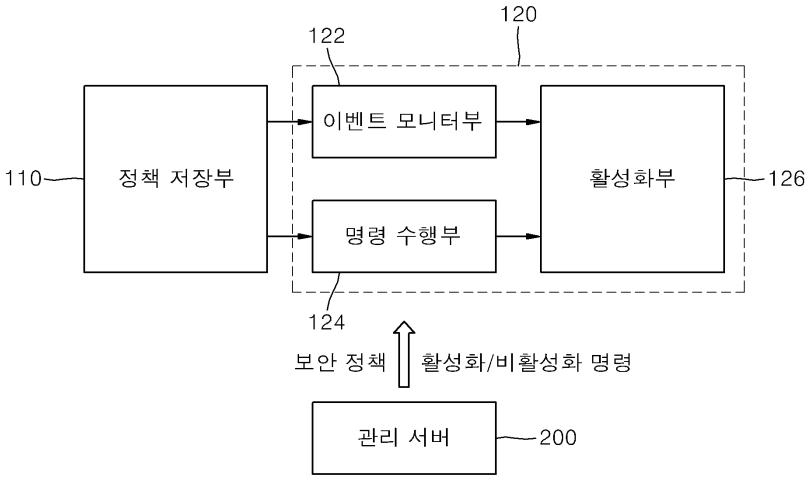
210 - 정책 생성부

220 - 정책 전송부

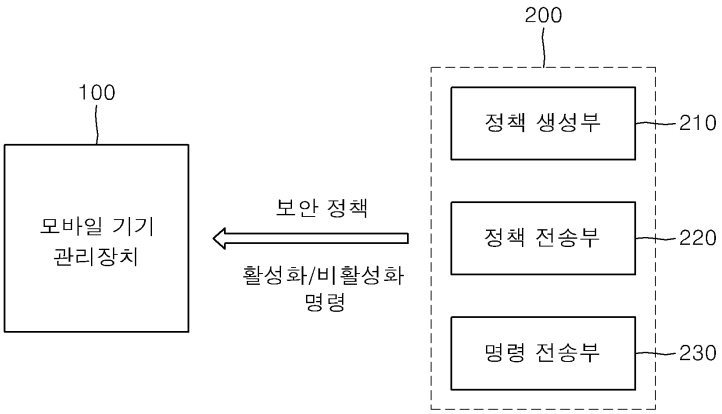
230 - 명령 전송부

도면

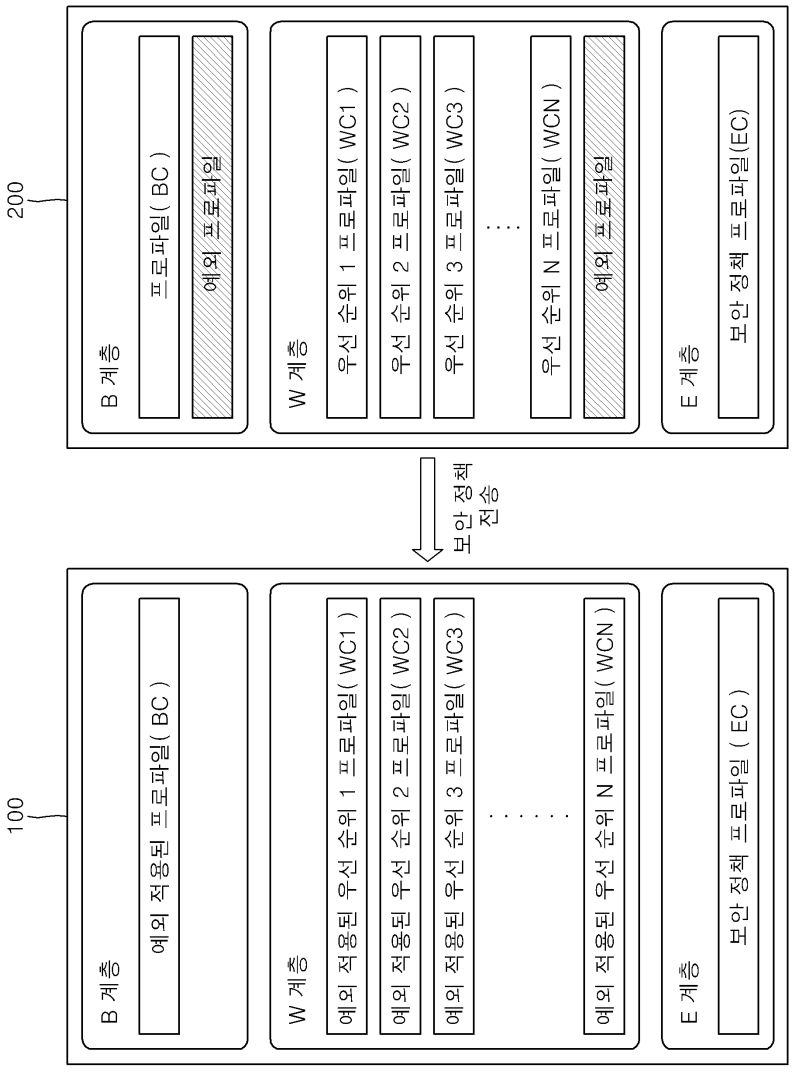
도면1



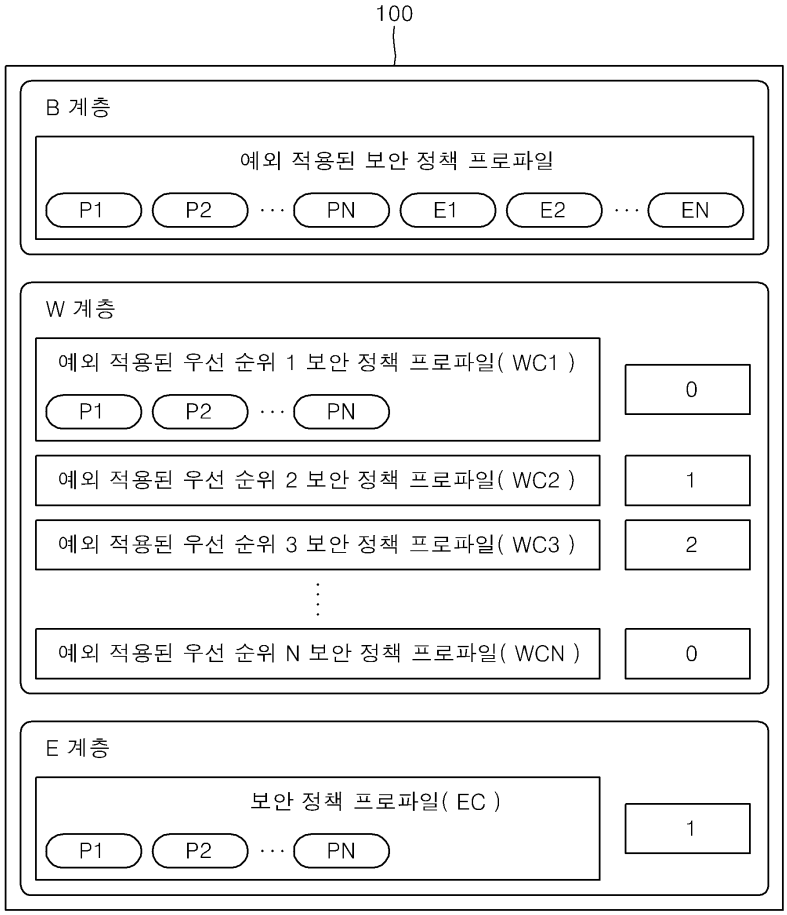
도면2


200
100
정책 생성부
210
모바일 기기
관리장치
보안 정책
정책 전송부
220
활성화/비활성화
명령
명령 전송부
230

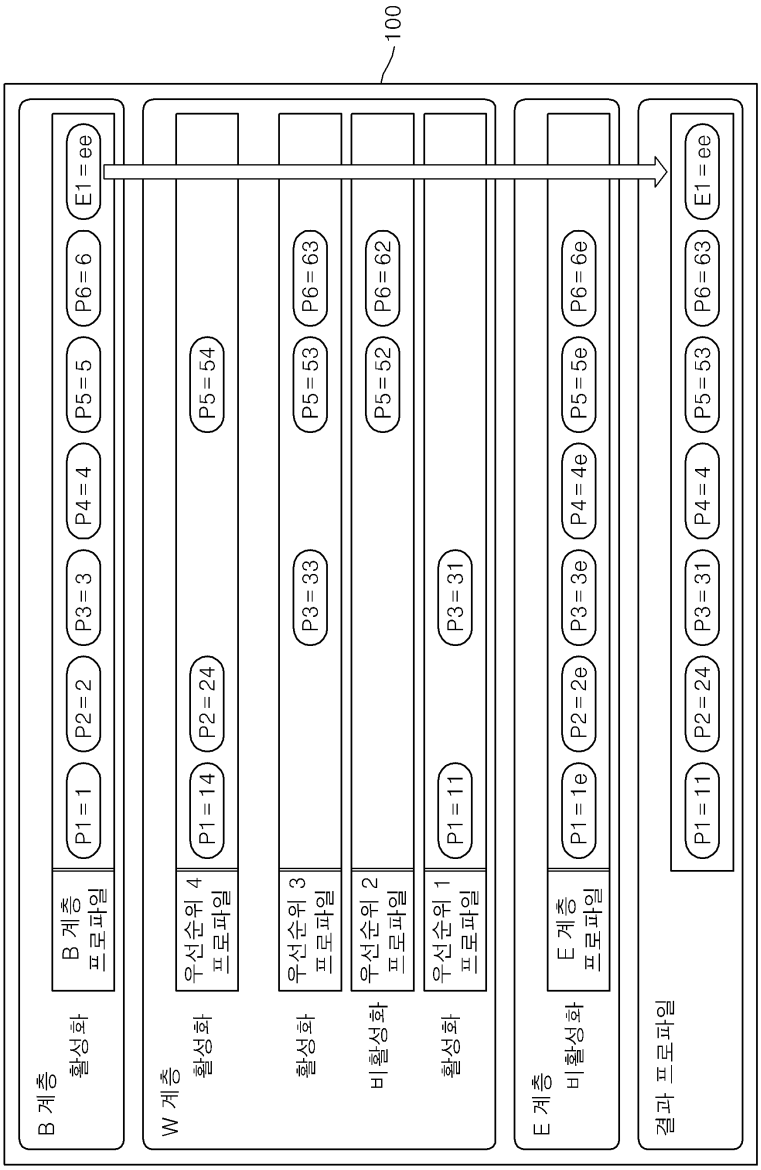
도면3


200
B 계층
프로파일(BC)
예외 프로파일
W 계층
우선 순위 1 프로파일(WC1)
우선 순위 2 프로파일(WC2)
우선 순위 3 프로파일(WC3)
우선 순위 N 프로파일(WCN)
예외 프로파일
E 계층
보안 정책 프로파일(EC)
보안 정책
전송
100
B 계층
예외 적용된 프로파일(BC)
W 계층
예외 적용된 우선 순위 1 프로파일(WC1)
예외 적용된 우선 순위 2 프로파일(WC2)
예외 적용된 우선 순위 3 프로파일(WC3)
예외 적용된 우선 순위 N 프로파일(WCN)
E 계층
보안 정책 프로파일 (EC)

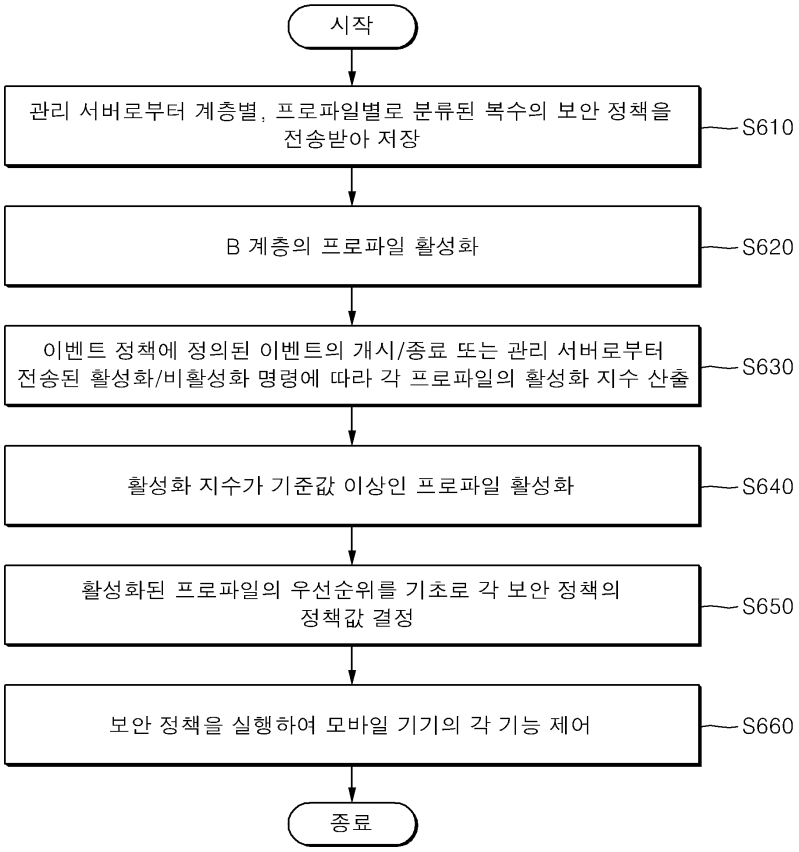
도면4


100
B 계층
예외 적용된 보안 정책 프로파일
P1
P2
···
PN
E1
E2
···
EN
W 계층
예외 적용된 우선 순위 1 보안 정책 프로파일(WC1)
P1
P2
···
PN
0
예외 적용된 우선 순위 2 보안 정책 프로파일(WC2)
1
예외 적용된 우선 순위 3 보안 정책 프로파일(WC3)
2
예외 적용된 우선 순위 N 보안 정책 프로파일(WCN)
0
E 계층
보안 정책 프로파일(EC)
P1
P2
···
PN
1

도면5


100
B 계층
활성화
B 계층 프로파일
P1 = 1
P2 = 2
P3 = 3
P4 = 4
P5 = 5
P6 = 6
E1 = ee
W 계층
활성화
우선순위 4 프로파일
P1 = 14
P2 = 24
P5 = 54
활성화
우선순위 3 프로파일
P3 = 33
P5 = 53
P6 = 63
비활성화
우선순위 2 프로파일
P5 = 52
P6 = 62
활성화
우선순위 1 프로파일
P1 = 11
P3 = 31
E 계층
비활성화
E 계층 프로파일
P1 = 1e
P2 = 2e
P3 = 3e
P4 = 4e
P5 = 5e
P6 = 6e
결과 프로파일
P1 = 11
P2 = 24
P3 = 31
P4 = 4
P5 = 53
P6 = 63
E1 = ee

도면6


시작
관리 서버로부터 계층별, 프로파일별로 분류된 복수의 보안 정책을 전송받아 저장
S610
B 계층의 프로파일 활성화
S620
이벤트 정책에 정의된 이벤트의 개시/종료 또는 관리 서버로부터 전송된 활성화/비활성화 명령에 따라 각 프로파일의 활성화 지수 산출
S630
활성화 지수가 기준값 이상인 프로파일 활성화
S640
활성화된 프로파일의 우선순위를 기초로 각 보안 정책의 정책값 결정
S650
보안 정책을 실행하여 모바일 기기의 각 기능 제어
S660
종료