



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2024년07월30일
(11) 등록번호 10-2690046
(24) 등록일자 2024년07월25일

(51) 국제특허분류(Int. Cl.)
H04L 9/40 (2022.01)

(52) CPC특허분류
H04L 63/105 (2013.01)
H04L 63/102 (2013.01)

(21) 출원번호 10-2023-0157871
(22) 출원일자 2023년11월15일
심사청구일자 2023년11월15일

(56) 선행기술조사문헌
KR1020230072648 A*
US20080235811 A1*
US20160359913 A1*
US20220279009 A1*

*는 심사관에 의하여 인용된 문헌

(73) 특허권자

에스지엔 주식회사

서울특별시 마포구 월드컵북로 361, 한솔교육 1
3층 (상암동, 이안상암2단지)

(72) 발명자

구자일

경기도 안양시 동안구 달안로 124, 407동 1506호
업지회

경기도 고양시 일산서구 탄현로 136, 111동 1101
호

(74) 대리인

심찬, 강정빈

전체 청구항 수 : 총 9 항

심사관 : 문형섭

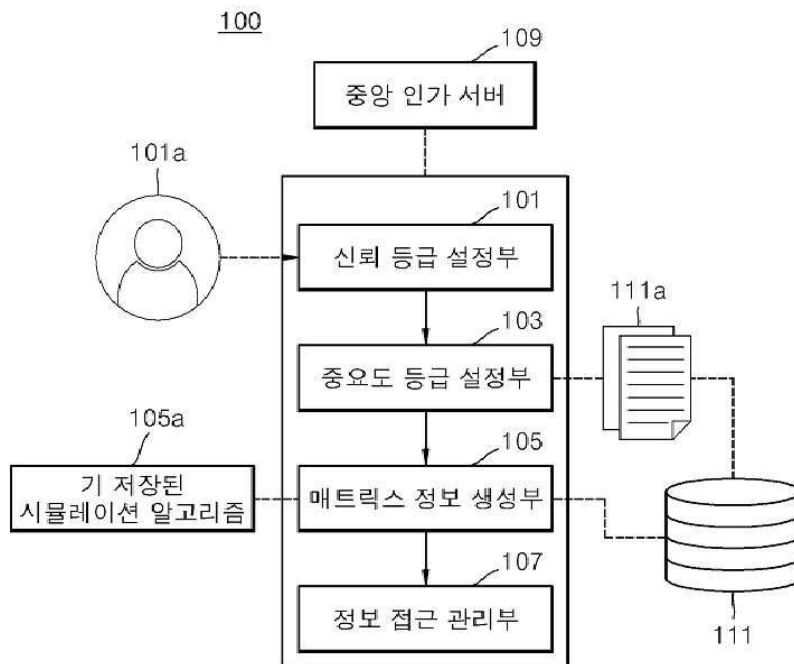
(54) 발명의 명칭 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템

(57) 요약

본 발명은 하나 이상의 프로세서 및 상기 프로세서에서 수행 가능한 명령들을 저장하는 하나 이상의 메모리를 포함하는 컴퓨팅 장치에서 구현되는 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템에 있어서, 복수의 사용자 계정 중 제1 사용자 계정이 기업에서 관리하는 중앙 인가 서버에 접속하는 것을

(뒷면에 계속)

대표도 - 도1



감지하는 경우, 상기 제1 사용자 계정의 신뢰 상태를 확인하기 위한 신뢰 확인 프로세스를 시작하여, 상기 제1 사용자 계정의 신뢰 등급을 설정하는 신뢰 등급 설정부; 상기 신뢰 등급 설정부의 기능이 수행되는 동안 기업에서 관리하는 복수 개의 자원 정보에 대한 중요도를 확인하기 위한 중요도 확인 프로세스를 시작하여, 상기 복수 개의 자원 정보 각각에 대한 중요도 등급을 설정하는 중요도 등급 설정부; 상기 신뢰 등급 설정부 및 상기 중요도 등급 설정부의 기능 수행이 완료되면, 기 저장된 복수 개의 보안 정책 정보에 상기 신뢰 등급 및 상기 중요도 등급을 반영하여, 상기 복수 개의 자원 정보 각각에 대한 제1 사용자 계정의 접근 여부를 판별 가능한 정책 매트릭스를 생성한 후, 기 저장된 시뮬레이션 알고리즘을 통해 상기 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 수행하여, 상기 수행된 시뮬레이션 결과에 기반해 접근 정책 매트릭스 정보를 생성하는 매트릭스 정보 생성부; 및 상기 접근 정책 매트릭스 정보의 생성이 완료되면, 상기 접근 정책 매트릭스 정보를 상기 중앙 인가 서버에 즉시 반영하여, 상기 반영된 접근 정책 매트릭스 정보에 기반해 상기 복수 개의 자원 정보 중 적어도 하나에 접근하는 상기 제1 사용자 계정의 접근 여부를 관리하는 정보 접근 관리부;를 포함하는 것을 특징으로 한다. 이 외에도 본 문서를 통해 파악되는 다양한 실시예들이 가능하다.

(52) CPC특허분류

HO4L 63/107 (2013.01)

HO4L 63/20 (2013.01)

명세서

청구범위

청구항 1

하나 이상의 프로세서 및 상기 프로세서에서 수행 가능한 명령들을 저장하는 하나 이상의 메모리를 포함하는 컴퓨팅 장치에서 구현되는 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템에 있어서,

복수의 사용자 계정 중 제1 사용자 계정이 기업에서 관리하는 중앙 인가 서버에 접속하는 것을 감지하는 경우, 상기 제1 사용자 계정의 신뢰 상태를 확인하기 위한 신뢰 확인 프로세스를 시작하여, 상기 제1 사용자 계정의 신뢰 등급을 설정하는 신뢰 등급 설정부;

상기 신뢰 등급 설정부의 기능이 수행되는 동안 기업에서 관리하는 복수 개의 자원 정보에 대한 중요도를 확인하기 위한 중요도 확인 프로세스를 시작하여, 상기 복수 개의 자원 정보 각각에 대한 중요도 등급을 설정하는 중요도 등급 설정부;

상기 신뢰 등급 설정부 및 상기 중요도 등급 설정부의 기능 수행이 완료되면, 기 저장된 복수 개의 보안 정책 정보에 상기 신뢰 등급 및 상기 중요도 등급을 반영하여, 상기 복수 개의 자원 정보 각각에 대한 제1 사용자 계정의 접근 여부를 판별 가능한 정책 매트릭스를 생성한 후, 기 저장된 시뮬레이션 알고리즘을 통해 상기 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 수행하여, 상기 수행된 시뮬레이션 결과에 기반한 접근 정책 매트릭스 정보를 생성하는 매트릭스 정보 생성부; 및

상기 접근 정책 매트릭스 정보의 생성이 완료되면, 상기 접근 정책 매트릭스 정보를 상기 중앙 인가 서버에 즉시 반영하여, 상기 반영된 접근 정책 매트릭스 정보에 기반해 상기 복수 개의 자원 정보 중 적어도 하나에 접근하는 상기 제1 사용자 계정의 접근 여부를 관리하는 정보 접근 관리부;를 포함하되,

상기 신뢰 등급 설정부는,

상기 제1 사용자 계정이 상기 중앙 인가 서버에 접속하는 것을 감지하는 경우, 상기 제1 사용자 계정이 상기 중앙 인가 서버에 접속함에 따라 생성되는 접속 이력 정보를 추출하는 계정 접속 감지부;

상기 접속 이력 정보의 추출이 완료됨에 따라 상기 신뢰 확인 프로세스가 시작되는 경우, 상기 추출된 접속 이력 정보에 포함된 복수 개의 카테고리 각각에 포함된 세부 정보를 확인하여, 상기 복수 개의 카테고리 각각에 대응되는 기 설정된 신뢰 요소 카테고리 각각에 설정되어 있는 복수 개의 신뢰 등급 산출 식을 식별하는 신뢰 등급 식 식별부; 및

상기 신뢰 등급 식 식별부의 기능 수행이 완료되면, 상기 식별된 복수 개의 신뢰 등급 산출 식을 통해 상기 기 설정된 신뢰 요소 카테고리 별로 상기 제1 사용자 계정이 상기 중앙 인가 서버에서 관리하는 상기 복수 개의 자원 정보에 접근 시 접근 여부를 확인하기 위해 활용되는 신뢰 등급을 산출해 상기 제1 사용자 계정에 대한 신뢰 등급의 설정을 완료하는 제1 등급 설정부;를 포함하는 것을 특징으로 하는 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템.

청구항 2

삭제

청구항 3

제1항에 있어서,

상기 기 설정된 신뢰 요소 카테고리는,

상기 복수 개의 카테고리 중 상기 제1 사용자 계정에 등록된 사용자의 개인 정보를 포함하는 제1 카테고리에 대응되는 카테고리로서, 상기 개인 정보가 반영되어 제1 신뢰 등급을 산출하는 제1 신뢰 등급 산출 식을 포함하는

제1 신뢰 요소 카테고리;

상기 복수 개의 카테고리 중 상기 제1 사용자 계정이 상기 중앙 인가 서버에 접속한 위치 및 접속 경로에 기반한 위치 경로 정보를 포함하는 제2 카테고리에 대응되는 카테고리로서, 상기 위치 경로 정보가 반영되어 제2 신뢰 등급을 산출하는 제2 신뢰 등급 산출 식을 포함하는 제2 신뢰 요소 카테고리;

상기 복수 개의 카테고리 중 상기 제1 사용자 계정이 상기 중앙 인가 서버에 접속하기 위해 사용한 인증 수단 및 전자 장치에 기반한 인증 장치 정보를 포함하는 제3 카테고리에 대응되는 카테고리로서, 상기 인증 장치 정보가 반영되어 제3 신뢰 등급을 산출하는 제3 신뢰 등급 산출 식을 포함하는 제3 신뢰 요소 카테고리; 및

상기 복수 개의 카테고리 중 상기 제1 사용자 계정에 등록된 사용자의 근무 부서, 직위 및 고용 형태에 기반한 사원 정보를 포함하는 제4 카테고리에 대응되는 카테고리로서, 상기 사원 정보가 반영되어 제4 신뢰 등급을 산출하는 제4 신뢰 등급 산출 식을 포함하는 제4 신뢰 요소 카테고리;를 포함하는 것을 특징으로 하는 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템.

청구항 4

제3항에 있어서,

상기 중요도 등급 설정부는,

상기 신뢰 등급 설정부의 기능이 수행되는 동안 상기 중요도 확인 프로세스를 시작하여, 상기 기업에서 관리하는 복수 개의 자원 정보에 포함된 복수 개의 자원 카테고리를 식별해 상기 복수 개의 자원 카테고리 및 대응되는 기 설정된 중요도 요소 카테고리 각각에 설정되어 있는 복수 개의 중요도 등급 산출 식을 식별하는 중요도 등급 산출 식 식별부; 및

상기 중요도 등급 산출 식 식별부의 기능 수행이 완료되면, 기 설정된 중요도 요소 카테고리 각각에 설정되어 있는 복수 개의 중요도 등급 산출 식 중 상기 식별된 자원 카테고리에 포함된 자원 요소 정보가 반영되는 적어도 하나의 중요도 등급 산출 식을 식별하여, 상기 식별된 적어도 하나의 중요도 등급 산출 식을 통해 상기 기 설정된 중요도 요소 카테고리 별로 중요도 등급을 산출해 상기 복수 개의 자원 정보 각각에 대해 중요도 등급의 설정을 완료하는 제2 등급 설정부;를 포함하는 것을 특징으로 하는 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템.

청구항 5

제4항에 있어서,

상기 기 설정된 중요도 요소 카테고리는,

상기 복수 개의 자원 카테고리 중 상기 복수 개의 자원 정보 각각에 입력된 다른 사용자의 개인 정보의 입력 여부에 기반한 입력 여부 정보를 포함하는 제1 자원 카테고리에 대응되는 카테고리로서, 상기 입력 여부 정보가 반영되어 제1 중요도 등급을 산출하는 제1 중요도 등급 산출 식을 포함하는 제1 중요도 요소 카테고리;

상기 복수 개의 자원 카테고리 중 상기 복수 개의 자원 정보 각각의 영업 기밀 등급에 기반한 기밀 등급 정보를 포함하는 제2 자원 카테고리에 대응되는 카테고리로서, 상기 기밀 등급 정보가 반영되어 제2 중요도 등급을 산출하는 제2 중요도 등급 산출 식을 포함하는 제2 중요도 요소 카테고리;

상기 복수 개의 자원 카테고리 중 상기 복수 개의 자원 정보 각각에 설정되어 있는 사용자 편집 기능에 기반한 기능 제한 정보를 포함하는 제3 자원 카테고리에 대응되는 카테고리로서, 상기 기능 제한 정보가 반영되어 제3 중요도 등급을 산출하는 제3 중요도 등급 산출 식을 포함하는 제3 중요도 요소 카테고리; 및

상기 복수 개의 자원 카테고리 중 상기 복수 개의 자원 정보 각각을 활용하는 주요 시스템의 등급에 기반한 시스템 등급 정보를 포함하는 제4 자원 카테고리에 대응되는 카테고리로서, 상기 시스템 등급 정보가 반영되어 제4 중요도 등급을 산출하는 제4 중요도 등급 산출 식을 포함하는 제4 중요도 요소 카테고리; 를 포함하는 것을 특징으로 하는 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템.

청구항 6

제5항에 있어서,

상기 매트릭스 정보 생성부는,

상기 신뢰 등급 설정부 및 상기 중요도 등급 설정부의 기능 수행이 완료되면, 기 저장된 복수 개의 보안 정책 정보를 기 설정된 접근 기준 별로 식별하여, 상기 기 설정된 접근 기준 별로 식별된 보안 정책 정보 각각에 상기 신뢰 등급 및 중요도 등급을 반영하는 등급 반영부;

상기 등급 반영부의 기능 수행에 의해 상기 기 설정된 접근 기준 별로 식별된 보안 정책 정보 각각에 상기 신뢰 등급 및 중요도 등급이 반영됨에 따라 상기 복수 개의 자원 정보 각각에 대한 상기 기 설정된 접근 기준 별로 제1 사용자 계정의 접근 여부가 반영된 정책 매트릭스를 생성하는 정책 매트릭스 생성부; 및

상기 정책 매트릭스 생성부의 기능 수행이 완료된 상태에서, 상기 기 저장된 시뮬레이션 알고리즘을 통해 상기 생성된 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 수행하여, 상기 접근 정책 시뮬레이션 결과에 기반해 상기 정책 매트릭스의 보정 여부를 결정하는 매트릭스 보정 결정부;를 포함하는 것을 특징으로 하는 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템.

청구항 7

제6항에 있어서,

상기 매트릭스 보정 결정부는,

상기 기 저장된 시뮬레이션 알고리즘을 통해 상기 생성된 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 수행하여, 상기 접근 정책 시뮬레이션 결과가 보안 위험 상태로 도출되는 경우, 상기 보안 위험 상태로 도출된 기 설정된 접근 기준에 기반한 신뢰 등급 및 중요도 등급 각각의 산출 식에 매칭되어 있는 가중치를 보정하는 가중치 보정부;

상기 기 저장된 시뮬레이션 알고리즘을 통해 상기 생성된 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 수행하여, 상기 접근 정책 시뮬레이션 결과가 보안 안전 상태로 도출되는 경우, 상기 보안 안전 상태로 도출된 정책 매트릭스에 기반한 접근 정책 매트릭스 정보를 생성하는 제1 접근 정책 매트릭스 정보 생성부;

상기 가중치 보정부의 기능이 완료된 상태에서, 상기 기 저장된 시뮬레이션 알고리즘을 통해 상기 가중치가 보정된 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 재수행하여, 상기 접근 정책 시뮬레이션의 결과가 상기 보안 안전 상태로 도출되는 경우, 상기 보안 안전 상태로 도출된 정책 매트릭스에 기반한 접근 정책 매트릭스 정보를 생성하는 제2 접근 정책 매트릭스 정보 생성부;를 포함하는 것을 특징으로 하는 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템.

청구항 8

제7항에 있어서,

상기 가중치는,

상기 중앙 인가 서버를 관리하는 관리자 계정에 의해 상기 기 설정된 신뢰 요소 카테고리 별로 설정되어 있는 제1 가중치 및 상기 기 설정된 중요도 요소 카테고리 별로 설정되어 있는 제2 가중치를 포함하며, 상기 복수 개의 자원 정보 각각에 대한 복수의 사용자 계정의 접근으로 인한 보안 위험 상태를 방지하기 위해 보정 가능한 구성인 것을 특징으로 하는 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템.

청구항 9

제8항에 있어서,

상기 매트릭스 보정 결정부는,

상기 가중치 보정부의 기능이 완료된 상태에서, 상기 기 저장된 시뮬레이션 알고리즘을 통해 상기 가중치가 보정된 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 수행하여, 상기 접근 정책 시뮬레이션의 결과가 상기 보안 위험 상태로 도출되는 경우, 상기 가중치가 보정된 정책 매트릭스에 대응되는 보안 정책 정보의 정책을 비정상 정책으로 판단하여, 상기 비정상 정책으로 판단된 보안 정책 정보를 정상 정책의 보안 정책 정보로 보정하는 것을 특징으로 하는 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템.

청구항 10

제9항에 있어서,

상기 정보 접근 관리부는,

상기 접근 정책 매트릭스 정보의 생성이 완료되면, 상기 접근 정책 매트릭스 정보를 상기 중앙 인가 서버에 즉시 반영하는 정책 매트릭스 서버 반영부; 및

상기 정책 매트릭스 서버 반영부의 기능 수행이 완료되면, 상기 반영된 접근 정책 매트릭스 정보에 기반해 상기 복수 개의 자원 정보 중 적어도 하나에 접근하는 상기 제1 사용자 계정의 접근 여부를 관리하는 모니터링 접근 제어부;를 포함하는 것을 특징으로 하는 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템.

발명의 설명

기술 분야

[0001] 본 발명은 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템에 관한 것으로서, 구체적으로는 중앙 인가 서버에 접속하는 사용자 계정의 신뢰 등급 및 기업에서 관리하는 복수 개의 자원 정보의 중요도 등급을 산출하여, 기 저장된 복수 개의 보안 정책 정보를 기반으로 신뢰 등급 및 중요도 등급이 반영된 정책 매트릭스를 생성하고, 기 저장된 시뮬레이션 알고리즘을 통해 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 수행해 정책 매트릭스에 대한 이상 유무를 판단하고, 정책 매트릭스에 대한 이상이 없을 시 접근 정책 매트릭스 정보를 생성해 중앙 인가 서버에 즉시 반영하여, 추가 네트워크 요소를 소비하지 않고 복수 개의 자원 정보에 대한 사용자 계정의 접근 여부를 관리하기 위한 기술에 관한 것이다.

배경 기술

[0002] 현재는 종식된 팬데믹 바이러스로 인해 우리 주변의 생활 패턴이 많이 변화였다. 그 중 업무적으로는 재택 근무가 보편화되었는데, 재택 근무와 같은 비대면 원격 근무 환경을 이용해 기업의 보안 취약점을 노리는 사이버 범죄 사례 또한 급증하고 있다. 더불어, 해외에서도 비대면 원격 근무가 보편화됨에 따라 기업의 클라우드 활용이 늘어나고 주요 시스템이 클라우드로 전환되는 가운데, 클라우드 기반의 악성 코드가 발견되고 클라우드 설정 오류로 인한 공황 데이터 유출, 10억 명의 개인 정보가 유출되는 등 클라우드 관련 보안 사고도 점차적으로 증가하고 있다.

[0003] 이에 따라, 업계에서는 업무 서버에 접속하는 사용자에 대한 검증을 수행해 사용자가 요청하는 정보를 제공하기 위한 다양한 보안 관련 기술들을 개발하고 있다.

[0004] 일 예로서, 한국등록특허 10-2586870(클라우드 환경에서 보호 대상에 대한 AI 기반 보안위험 예측 시스템 및 방법)에는 보호 대상에 대한 클라우드 로그와 시스템 로그를 AI 알고리즘을 통해 분석하여, 신규 활동에 대한 위험도 점수를 통해 보호 대상에 대한 보안 위험을 예측하는 기술이 개시되어 있다.

[0005] 그러나, 상술한 선행기술에서는 단순히 보호 대상에 대한 보안 위험을 예측하는 기술만이 개시되어 있을 뿐, 중앙 인가 서버에 접속하는 사용자 계정의 신뢰 등급 및 기업에서 관리하는 복수 개의 자원 정보의 중요도 등급을 산출하여, 기 저장된 복수 개의 보안 정책 정보를 기반으로 신뢰 등급 및 중요도 등급이 반영된 정책 매트릭스

를 생성하고, 기 저장된 시뮬레이션 알고리즘을 통해 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 수행해 정책 매트릭스에 대한 이상 유무를 판단하고, 정책 매트릭스에 대한 이상이 없을 시 접근 정책 매트릭스 정보를 생성해 중앙 인가 서버에 즉시 반영하여, 추가 네트워크 요소를 소비하지 않고 복수 개의 자원 정보에 대한 사용자 계정의 접근 여부를 관리하는 기술은 개시되어 있지 않아, 이를 해결할 수 있는 기술의 필요성이 대두되고 있다.

발명의 내용

해결하려는 과제

[0006] 이에 본 발명은 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템을 통해 중앙 인가 서버에 접속하는 사용자 계정의 신뢰 등급 및 기업에서 관리하는 복수 개의 자원 정보의 중요도 등급을 산출하여, 기 저장된 복수 개의 보안 정책 정보를 기반으로 신뢰 등급 및 중요도 등급이 반영된 정책 매트릭스를 생성하고, 기 저장된 시뮬레이션 알고리즘을 통해 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 수행해 정책 매트릭스에 대한 이상 유무를 판단하고, 정책 매트릭스에 대한 이상이 없을 시 접근 정책 매트릭스 정보를 생성해 중앙 인가 서버에 즉시 반영하여, 추가 네트워크 요소를 소비하지 않고 복수 개의 자원 정보에 대한 사용자 계정의 접근 여부를 관리하여, 기업에서 관리하는 자원 정보에 대한 보안성을 유지함과 동시에 추가적인 네트워크 요소를 소비하지 않고 인증 프로세스를 수행하는 것에 그 목적이 있다.

과제의 해결 수단

[0007] 본 발명의 일 실시예에 따른 하나 이상의 프로세서 및 상기 프로세서에서 수행 가능한 명령들을 저장하는 하나 이상의 메모리를 포함하는 컴퓨팅 장치에서 구현되는 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템에 있어서, 복수의 사용자 계정 중 제1 사용자 계정이 기업에서 관리하는 중앙 인가 서버에 접속하는 것을 감지하는 경우, 상기 제1 사용자 계정의 신뢰 상태를 확인하기 위한 신뢰 확인 프로세스를 시작하여, 상기 제1 사용자 계정의 신뢰 등급을 설정하는 신뢰 등급 설정부; 상기 신뢰 등급 설정부의 기능이 수행되는 동안 기업에서 관리하는 복수 개의 자원 정보에 대한 중요도를 확인하기 위한 중요도 확인 프로세스를 시작하여, 상기 복수 개의 자원 정보 각각에 대한 중요도 등급을 설정하는 중요도 등급 설정부; 상기 신뢰 등급 설정부 및 상기 중요도 등급 설정부의 기능 수행이 완료되면, 기 저장된 복수 개의 보안 정책 정보에 상기 신뢰 등급 및 상기 중요도 등급을 반영하여, 상기 복수 개의 자원 정보 각각에 대한 제1 사용자 계정의 접근 여부를 판별 가능한 정책 매트릭스를 생성한 후, 기 저장된 시뮬레이션 알고리즘을 통해 상기 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 수행하여, 상기 수행된 시뮬레이션 결과에 기반해 접근 정책 매트릭스 정보를 생성하는 매트릭스 정보 생성부; 및 상기 접근 정책 매트릭스 정보의 생성이 완료되면, 상기 접근 정책 매트릭스 정보를 상기 중앙 인가 서버에 즉시 반영하여, 상기 반영된 접근 정책 매트릭스 정보에 기반해 상기 복수 개의 자원 정보 중 적어도 하나에 접근하는 상기 제1 사용자 계정의 접근 여부를 관리하는 정보 접근 관리부;를 포함하는 것을 특징으로 한다.

[0008] 상기 신뢰 등급 설정부는, 상기 제1 사용자 계정이 상기 중앙 인가 서버에 접속하는 것을 감지하는 경우, 상기 제1 사용자 계정이 상기 중앙 인가 서버에 접속함에 따라 생성되는 접속 이력 정보를 추출하는 계정 접속 감지부; 상기 접속 이력 정보의 추출이 완료됨에 따라 상기 신뢰 확인 프로세스가 시작되는 경우, 상기 추출된 접속 이력 정보에 포함된 복수 개의 카테고리 각각에 포함된 세부 정보를 확인하여, 상기 복수 개의 카테고리 각각에 대응되는 기 설정된 신뢰 요소 카테고리 각각에 설정되어 있는 복수 개의 신뢰 등급 산출 식을 식별하는 신뢰 등급 식 식별부; 및 상기 신뢰 등급 식 식별부의 기능 수행이 완료되면, 상기 식별된 복수 개의 신뢰 등급 산출 식을 통해 상기 기 설정된 신뢰 요소 카테고리 별로 상기 제1 사용자 계정이 상기 중앙 인가 서버에서 관리하는 상기 복수 개의 자원 정보에 접근 시 접근 여부를 확인하기 위해 활용되는 신뢰 등급을 산출해 상기 제1 사용자 계정에 대한 신뢰 등급의 설정을 완료하는 제1 등급 설정부;를 포함하는 것이 바람직하다.

[0009] 상기 기 설정된 신뢰 요소 카테고리는, 상기 복수 개의 카테고리 중 상기 제1 사용자 계정에 등록된 사용자의 개인 정보를 포함하는 제1 카테고리에 대응되는 카테고리로서, 상기 개인 정보가 반영되어 제1 신뢰 등급을 산출하는 제1 신뢰 등급 산출 식을 포함하는 제1 신뢰 요소 카테고리; 상기 복수 개의 카테고리 중 상기 제1 사용자 계정이 상기 중앙 인가 서버에 접속한 위치 및 접속 경로에 기반한 위치 경로 정보를 포함하는 제2 카테고리에 대응되는 카테고리로서, 상기 위치 경로 정보가 반영되어 제2 신뢰 등급을 산출하는 제2 신뢰 등급 산출 식을 포함하는 제2 신뢰 요소 카테고리; 상기 복수 개의 카테고리 중 상기 제1 사용자 계정이 상기 중앙 인가 서버에 접속하기 위해 사용한 인증 수단 및 전자 장치에 기반한 인증 장치 정보를 포함하는 제3 카테고리에 대응

되는 카테고리로서, 상기 인증 장치 정보가 반영되어 제3 신뢰 등급을 산출하는 제3 신뢰 등급 산출 식을 포함하는 제3 신뢰 요소 카테고리; 및 상기 복수 개의 카테고리 중 상기 제1 사용자 계정에 등록된 사용자의 근무 부서, 직위 및 고용 형태에 기반한 사원 정보를 포함하는 제4 카테고리에 대응되는 카테고리로서, 상기 사원 정보가 반영되어 제4 신뢰 등급을 산출하는 제4 신뢰 등급 산출 식을 포함하는 제4 신뢰 요소 카테고리;를 포함하는 것이 가능하다.

[0010] 상기 중요도 등급 설정부는, 상기 신뢰 등급 설정부의 기능이 수행되는 동안 상기 중요도 확인 프로세스를 시작하여, 상기 기업에서 관리하는 복수 개의 자원 정보에 포함된 복수 개의 자원 카테고리를 식별해 상기 복수 개의 자원 카테고리 및 대응되는 기 설정된 중요도 요소 카테고리 각각에 설정되어 있는 복수 개의 중요도 등급 산출 식을 식별하는 중요도 등급 산출 식 식별부; 및 상기 중요도 등급 산출 식 식별부의 기능 수행의 완료되면, 기 설정된 중요도 요소 카테고리 각각에 설정되어 있는 복수 개의 중요도 등급 산출 식 중 상기 식별된 자원 카테고리에 포함된 자원 요소 정보가 반영되는 적어도 하나의 중요도 등급 산출 식을 식별하여, 상기 식별된 적어도 하나의 중요도 등급 산출 식을 통해 상기 기 설정된 중요도 요소 카테고리 별로 중요도 등급을 산출해 상기 복수 개의 자원 정보 각각에 대해 중요도 등급의 설정을 완료하는 제2 등급 설정부;를 포함하는 것이 가능하다.

[0011] 상기 기 설정된 중요도 요소 카테고리는, 상기 복수 개의 자원 카테고리 중 상기 복수 개의 자원 정보 각각에 입력된 다른 사용자의 개인 정보의 입력 여부에 기반한 입력 여부 정보를 포함하는 제1 자원 카테고리에 대응되는 카테고리로서, 상기 입력 여부 정보가 반영되어 제1 중요도 등급을 산출하는 제1 중요도 등급 산출 식을 포함하는 제1 중요도 요소 카테고리; 상기 복수 개의 자원 카테고리 중 상기 복수 개의 자원 정보 각각의 영업 기밀 등급에 기반한 기밀 등급 정보를 포함하는 제2 자원 카테고리에 대응되는 카테고리로서, 상기 기밀 등급 정보가 반영되어 제2 중요도 등급을 산출하는 제2 중요도 등급 산출 식을 포함하는 제2 중요도 요소 카테고리; 상기 복수 개의 자원 카테고리 중 상기 복수 개의 자원 정보 각각에 설정되어 있는 사용자 편집 기능에 기반한 기능 제한 정보를 포함하는 제3 자원 카테고리에 대응되는 카테고리로서, 상기 기능 제한 정보가 반영되어 제3 중요도 등급을 산출하는 제3 중요도 등급 산출 식을 포함하는 제3 중요도 요소 카테고리; 및 상기 복수 개의 자원 카테고리 중 상기 복수 개의 자원 정보 각각을 활용하는 주요 시스템의 등급에 기반한 시스템 등급 정보를 포함하는 제4 자원 카테고리에 대응되는 카테고리로서, 상기 시스템 등급 정보가 반영되어 제4 중요도 등급을 산출하는 제4 중요도 등급 산출 식을 포함하는 제4 중요도 요소 카테고리; 를 포함하는 것이 가능하다.

[0012] 상기 매트릭스 정보 생성부는, 상기 신뢰 등급 설정부 및 상기 중요도 등급 설정부의 기능 수행이 완료되면, 기 저장된 복수 개의 보안 정책 정보를 기 설정된 접근 기준 별로 식별하여, 상기 기 설정된 접근 기준 별로 식별된 보안 정책 정보 각각에 상기 신뢰 등급 및 중요도 등급을 반영하는 등급 반영부; 상기 등급 반영부의 기능 수행에 의해 상기 기 설정된 접근 기준 별로 식별된 보안 정책 정보 각각에 상기 신뢰 등급 및 중요도 등급이 반영됨에 따라 상기 복수 개의 자원 정보 각각에 대한 상기 기 설정된 접근 기준 별로 제1 사용자 계정의 접근 여부가 반영된 정책 매트릭스를 생성하는 정책 매트릭스 생성부; 및 상기 정책 매트릭스 생성부의 기능 수행이 완료된 상태에서, 상기 기 저장된 시뮬레이션 알고리즘을 통해 상기 생성된 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 수행하여, 상기 접근 정책 시뮬레이션 결과에 기반해 상기 정책 매트릭스의 보정 여부를 결정하는 매트릭스 보정 결정부;를 포함하는 것이 가능하다.

[0013] 상기 매트릭스 보정 결정부는, 상기 기 저장된 시뮬레이션 알고리즘을 통해 상기 생성된 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 수행하여, 상기 접근 정책 시뮬레이션 결과가 보안 위험 상태로 도출되는 경우, 상기 보안 위험 상태로 도출된 기 설정된 접근 기준에 기반한 신뢰 등급 및 중요도 등급 각각의 산출 식에 매칭되어 있는 가중치를 보정하는 가중치 보정부; 상기 기 저장된 시뮬레이션 알고리즘을 통해 상기 생성된 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 수행하여, 상기 접근 정책 시뮬레이션 결과가 보안 안전 상태로 도출되는 경우, 상기 보안 안전 상태로 도출된 정책 매트릭스에 기반한 접근 정책 매트릭스 정보를 생성하는 제1 접근 정책 매트릭스 정보 생성부; 상기 가중치 보정부의 기능이 완료된 상태에서, 상기 기 저장된 시뮬레이션 알고리즘을 통해 상기 가중치가 보정된 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 재수행하여, 상기 접근 정책 시뮬레이션의 결과가 상기 보안 안전 상태로 도출되는 경우, 상기 보안 안전 상태로 도출된 정책 매트릭스에 기반한 접근 정책 매트릭스 정보를 생성하는 제2 접근 정책 매트릭스 정보 생성부;를 포함하는 것이 가능하다.

[0014] 상기 가중치는, 상기 중앙 인가 서버를 관리하는 관리자 계정에 의해 상기 기 설정된 신뢰 요소 카테고리 별로 설정되어 있는 제1 가중치 및 상기 기 설정된 중요도 요소 카테고리 별로 설정되어 있는 제2 가중치를 포함하며, 상기 복수 개의 자원 정보 각각에 대한 복수의 사용자 계정의 접근으로 인한 보안 위험 상태를 방지하기 위해 보정 가능한 구성인 것이 가능하다.

[0015] 상기 매트릭스 보정 결정부는, 상기 가중치 보정부의 기능이 완료된 상태에서, 상기 기 저장된 시뮬레이션 알고리즘을 통해 상기 가중치가 보정된 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 수행하여, 상기 접근 정책 시뮬레이션의 결과가 상기 보안 위험 상태로 도출되는 경우, 상기 가중치가 보정된 정책 매트릭스에 대응되는 보안 정책 정보의 정책을 비정상 정책으로 판단하여, 상기 비정상 정책으로 판단된 보안 정책 정보를 정상 정책의 보안 정책 정보로 보정하는 것이 가능하다.

[0016] 상기 정보 접근 관리부는, 상기 접근 정책 매트릭스 정보의 생성이 완료되면, 상기 접근 정책 매트릭스 정보를 상기 중앙 인가 서버에 즉시 반영하는 정책 매트릭스 서버 반영부; 및 상기 정책 매트릭스 서버 반영부의 기능 수행이 완료되면, 상기 반영된 접근 정책 매트릭스 정보에 기반해 상기 복수 개의 자원 정보 중 적어도 하나에 접근하는 상기 제1 사용자 계정의 접근 여부를 관리하는 모니터링 접근 제어부;를 포함하는 것이 가능하다.

발명의 효과

[0017] 본 발명인 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템은 기업에서 관리하는 자원 정보에 대한 사용자들의 무분별한 접근을 방지하여, 기업에서 관리하는 사내 자원 정보에 대한 보안성을 유지할 수 있다.

[0018] 또한, 접근 정책 매트릭스 정보를 중앙 인가 서버에 즉각적으로 반영하여, 추가 네트워크 요소를 소비하지 않고 복수 개의 자원 정보에 대한 사용자 계정의 접근 여부를 관리할 수 있다.

도면의 간단한 설명

[0019] 도 1은 본 발명의 일 실시 예에 따른 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템을 설명하기 위한 블록도이다.

도 2는 본 발명의 일 실시 예에 따른 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템의 신뢰 등급 설정부를 설명하기 위한 블록도이다.

도 3은 본 발명의 일 실시 예에 따른 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템의 중요도 등급 설정부를 설명하기 위한 블록도이다.

도 4는 본 발명의 일 실시 예에 따른 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템의 매트릭스 정보 생성부를 설명하기 위한 블록도이다.

도 5는 본 발명의 일 실시 예에 따른 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템의 매트릭스 보정 결정부를 설명하기 위한 블록도이다.

도 6은 본 발명의 일 실시 예에 따른 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템의 정보 접근 관리부를 설명하기 위한 블록도이다.

도 7은 본 발명의 일 실시 예에 따른 컴퓨팅 장치의 내부 구성의 일 예를 설명하기 위한 도면이다.

발명을 실시하기 위한 구체적인 내용

[0020] 이하에서는, 다양한 실시 예들 및/또는 양상들이 이제 도면들을 참조하여 개시된다. 하기 설명에서는 설명을 목적으로, 하나 이상의 양상들의 전반적 이해를 돕기 위해 다수의 구체적인 세부사항들이 개시된다. 그러나, 이러한 양상(들)은 이러한 구체적인 세부사항들 없이도 실행될 수 있다는 점 또한 본 발명의 기술 분야에서 통상의 지식을 가진 자에게 인식될 수 있을 것이다. 이후의 기재 및 첨부된 도면들은 하나 이상의 양상들의 특정한 예시적인 양상들을 상세하게 기술한다. 하지만, 이러한 양상들은 예시적인 것이고 다양한 양상들의 원리들에서의 다양한 방법들 중 일부가 이용될 수 있으며, 기술되는 설명들은 그러한 양상들 및 그들의 균등물들을 모두 포함하고자 하는 의도이다.

[0021] 본 명세서에서 사용되는 "실시 예", "예", "양상", "예시" 등은 기술되는 임의의 양상 또는 설계가 다른 양상 또는 설계들보다 양호하거나, 이점이 있는 것으로 해석되지 않을 수도 있다.

[0022] 또한, "포함한다" 및/또는 "포함하는"이라는 용어는, 해당 특징 및/또는 구성요소가 존재함을 의미하지만, 하나 이상의 다른 특징, 구성요소 및/또는 이들의 그룹의 존재 또는 추가를 배제하지 않는 것으로 이해되어야 한다.

[0023] 또한, 제 1, 제 2 등과 같이 서수를 포함하는 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기

구성요소들은 상기 용어들에 의해 한정되지는 않는다. 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다. 예를 들어, 본 발명의 권리 범위를 벗어나지 않으면서 제 1 구성요소는 제 2 구성요소로 명명될 수 있고, 유사하게 제 2 구성요소도 제 1 구성요소로 명명될 수 있다. 및/또는 이라는 용어는 복수의 관련된 기재된 항목들의 조합 또는 복수의 관련된 기재된 항목들 중의 어느 항목을 포함한다.

- [0024] 또한, 본 발명의 실시 예들에서, 별도로 다르게 정의되지 않는 한, 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 모든 용어들은 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가지고 있다. 일반적으로 사용되는 사전에 정의되어 있는 것과 같은 용어들은 관련 기술의 문맥 상 가지는 의미와 일치하는 의미를 가지는 것으로 해석되어야 하며, 본 발명의 실시 예에서 명백하게 정의하지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다.
- [0025] 도 1은 본 발명의 일 실시 예에 따른 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템을 설명하기 위한 블록도이다.
- [0026] 도 1을 참조하면, 하나 이상의 프로세서 및 상기 프로세서에서 수행 가능한 명령들을 저장하는 하나 이상의 메모리를 포함하는 컴퓨팅 장치로 구현되는 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템(100)(이하, 접속 및 접근 관리 시스템으로 칭함)은 신뢰 등급 설정부(101), 중요도 등급 설정부(103), 매트릭스 정보 생성부(105) 및 정보 접근 관리부(107)를 포함할 수 있다.
- [0027] 일 실시예에 따르면, 상기 신뢰 등급 설정부(101)는 복수의 사용자 계정 중 제1 사용자 계정(101a)이 기업에서 관리하는 중앙 인가 서버(109)에 접속하는 것을 감지하는 경우, 상기 제1 사용자 계정의 신뢰 상태를 확인하기 위한 신뢰 확인 프로세스를 시작하여, 상기 제1 사용자 계정의 신뢰 등급을 설정할 수 있다.
- [0028] 일 실시예에 따르면, 상기 중앙 인가 서버(109)는 기업에서 관리하는 서버 데이터베이스로, 기업에서 관리하고 있는 복수 개의 사내 자원 정보에 사용자들이 접근 시, 사용자들에 대한 기업 소속 여부, 부서 소속 여부, 개인 정보 등을 확인해 사용자에게 대한 자격증명을 수행하기 위한 서버일 수 있다.
- [0029] 일 실시예에 따르면, 상기 신뢰 등급 설정부(101)는 상기 중앙 인가 서버(109)에 상기 제1 사용자 계정(101a)이 접속하는 것을 감지 시, 상기 제1 사용자 계정(101a)이 상기 기업에서 관리하는 복수 개의 자원 정보에 접근 가능한 신뢰 상태를 보유하고 있는지를 확인하기 위한 신뢰 확인 프로세스를 시작할 수 있다.
- [0030] 이 때, 상기 신뢰 등급 설정부(101)는 상기 제1 사용자 계정(101a)의 신뢰 등급을 확인하기 위한 신뢰 확인 프로세스를 시작 시, 기 설정된 신뢰 요소 카테고리 별로 상기 제1 사용자 계정(101a)의 신뢰 등급을 확인 및 설정할 수 있다.
- [0031] 일 실시예에 따르면, 상기 중요도 등급 설정부(103)는 상기 신뢰 등급 설정부(101)의 기능이 수행되는 동안 기업에서 관리하는 복수 개의 자원 정보(111a)에 대한 중요도를 확인하기 위한 중요도 확인 프로세스를 시작하여, 상기 복수 개의 자원 정보(111a) 각각에 대한 중요도 등급을 설정할 수 있다.
- [0032] 일 실시예에 따르면, 상기 중요도 등급 설정부(103)는 상기 기업 데이터 베이스(109)에 저장된 복수 개의 자원 정보(111a) 각각을 기 설정된 중요도 요소 카테고리 별로 중요도 등급을 확인하기 위한 중요도 확인 프로세스를 시작할 수 있다. 상기와 관련하여, 중요도 등급은 상기 복수 개의 자원 정보(111a) 각각에 설정되어 있는 구성으로, 상기 신뢰 등급이 설정된 제1 사용자 계정(101a)이 접근 가능한 정보인지를 구분하기 위한 기준이 되는 구성일 수 있다.
- [0033] 일 실시예에 따르면, 매트릭스 정보 생성부(105)는 상기 신뢰 등급 설정부(101) 및 상기 중요도 등급 설정부(103)의 기능 수행이 완료되면, 기 저장된 복수 개의 보안 정책 정보에 상기 신뢰 등급 및 상기 중요도 등급을 반영하여, 상기 복수 개의 자원 정보(111a) 각각에 대한 제1 사용자 계정의 접근 여부를 판별 가능한 정책 매트릭스를 생성한 후, 기 저장된 시뮬레이션 알고리즘(105a)을 통해 상기 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 수행하여, 상기 수행된 시뮬레이션 결과에 기반해 접근 정책 매트릭스 정보를 생성할 수 있다.
- [0034] 일 실시예에 따르면, 상기 기 저장된 복수 개의 보안 정책 정보는 제1 사용자 계정(101a)이 상기 복수 개의 자원 정보(111a) 각각에 접근 가능 여부를 구별하기 위한 정책에 기반한 정보로써, 기 설정된 중요도 요소 카테고리 별로 확인된 복수 개의 자원 정보(111a) 각각의 중요도 등급에 대한 상기 기 설정된 신뢰 요소 카테고리 별로 확인된 제1 사용자 계정(101a)의 신뢰 등급을 정책 별로 매칭하기 위한 기준 정보일 수 있다.
- [0035] 예를 들어, 상기 기 저장된 복수 개의 보안 정책 정보 중 제1 보안 정책 정보는 상기 복수 개의 자원 정보(111a) 중 제1 자원 정보에 대한 제1 사용자 계정(101a)의 접근 가능 여부를 식별 가능한 정책이 반영되어 있는

정보으로써, 제1 자원 정보에 대한 제1 사용자 계정(101a)의 접근 가능 여부에 대한 정책 내용(예: 제1 사용자 계정의 제1 신뢰 등급이 1등급일 때 중요도 등급 1등급인 제1 자원 정보에 접근 허용, 예: 제1 사용자 계정의 제1 신뢰 등급이 1등급 및 제2 신뢰 등급이 2등급일 때 제1 자원 정보에 접근 허용)이 포함되어 있는 정보일 수 있다.

- [0036] 일 실시예에 따르면, 상기 매트릭스 정보 생성부(105)는 상기 기 저장된 복수 개의 보안 정책 정보에 상기 신뢰 등급 및 상기 중요도 등급을 반영하여, 상기 복수 개의 자원 정보(111a)에 대한 제1 사용자 계정(101a)의 접근 여부를 판별 가능한 정책 매트릭스를 생성할 수 있다. 상기와 관련하여, 정책 매트릭스는 상기 기 저장된 복수 개의 보안 정책 정보에 상기 신뢰 등급 및 상기 중요도 등급을 반영됨에 따라, 상기 복수 개의 자원 정보(111a)에 대한 제1 사용자 계정(101a)의 접근 여부를 판별 가능한 행렬 정보일 수 있다.
- [0037] 일 실시예에 따르면, 상기 매트릭스 정보 생성부(105)는 상기 정책 매트릭스의 생성이 완료되면, 기 저장된 시뮬레이션 알고리즘(105a)을 통해 상기 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 수행할 수 있다.
- [0038] 일 실시예에 따르면, 기 저장된 시뮬레이션 알고리즘(105a)은 다른 정책 매트릭스, 다른 정책 매트릭스에 기반한 접근 정책 매트릭스 정보 및 다른 접근 정책 매트릭스 정보에 대한 정책 성공 이력 정보(자원 정보에 대한 보안성이 유지된 이력에 기반한 정보), 다른 접근 정책 매트릭스 정보에 대한 정책 실패 이력 정보(자원 정보에 대한 보안성 유지에 실패 이력에 기반한 정보) 및 상기 정책 실패 이력 정보에 기반해 보정된 접근 정책 매트릭스 정보 간의 상관 관계를 학습 및 분석하는 알고리즘일 수 있다.
- [0039] 이에 따라, 상기 기 저장된 시뮬레이션 알고리즘(105a)은 상기 매트릭스 정보 생성부(105)에 의해 생성된 정책 매트릭스에 기반한 시뮬레이션을 수행하여, 상기 복수 개의 자원 정보 각각에 대한 보안성 성공 및 보안성 실패에 따른 이벤트를 감지하기 위한 시뮬레이션을 수행하기 위하여, ANN(artificial neural network) 알고리즘, DNN(deep neural network) 알고리즘, CNN(convolution neural network) 알고리즘 및 RNN(recurrent neural network) 중 적어도 하나를 포함할 수 있다.
- [0040] 예를 들어, 상기 매트릭스 정보 생성부(105)는 상기 정책 매트릭스의 생성이 완료되면, 기 저장된 시뮬레이션 알고리즘(105a)을 통해 상기 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 수행할 수 있다. 이 때, 상기 정책 매트릭스는 상기 제1 자원 정보에 대한 제1 사용자 계정의 접근이 허용된 정책을 포함하고 있는 정보일 수 있다.
- [0041] 상기와 관련하여, 상기 기 저장된 시뮬레이션 알고리즘(105a)은 상기 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 수행하여, 상기 제1 자원 정보에 대한 제1 사용자 계정(101a)의 접근이 허용되면, 제1 사용자 계정(101a)이 중앙 인가 서버(109)에 접속 시 사용한 접속 경로에서 상기 제1 자원 정보의 보안 유출이 발생하는 이벤트를 감지할 수 있다.
- [0042] 이에 따라, 상기 매트릭스 정보 생성부(105)는 상기 기 저장된 시뮬레이션 알고리즘(105a)을 통해 감지된 이벤트에 기반한 접속 경로에서의 제1 자원 정보의 보안 유출을 방지하기 위하여, 상기 제1 사용자 계정의 접속 경로에 기반해 설정되는 제2 신뢰 등급의 산출 식을 보정 및 제1 자원 정보에 대한 중요도 등급의 산출 식을 보정하여, 기존의 제2 신뢰 등급보다 높은 제2 신뢰 등급을 가지는 사용자 계정이 상기 제1 자원 정보에 접근 가능하도록 정책을 수정할 수 있다.
- [0043] 이 후, 상기 매트릭스 정보 생성부(105)는 상기 기 저장된 시뮬레이션 알고리즘(105a)을 통해 상기 수정된 정책 내용을 포함하는 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 재수행하여, 제1 자원 정보에 대한 보안 유출이 발생하지 않은 시뮬레이션 결과를 확인하는 경우, 상기 확인된 시뮬레이션 결과에 기반해 접근 정책 매트릭스 정보를 생성할 수 있다. 즉, 상기 접근 정책 매트릭스 정보는 복수 개의 자원 정보 각각에 대해 사용자 계정의 접근함에 따라 발생 가능한 보안 유출을 방지 완료한 정책을 포함하는 정보일 수 있다.
- [0044] 일 실시예에 따르면, 상기 정보 접근 관리부(107)는 상기 접근 정책 매트릭스 정보의 생성이 완료되면, 상기 접근 정책 매트릭스 정보를 상기 중앙 인가 서버(109)에 즉시 반영하여, 상기 반영된 접근 정책 매트릭스 정보에 기반해 상기 복수 개의 자원 정보 중 적어도 하나에 접근하는 상기 제1 사용자 계정의 접근 여부를 관리할 수 있다.
- [0045] 즉, 상기 접근 정책 매트릭스 정보는 상기 중앙 인가 서버(109)에 즉시 반영되어, 상기 중앙 인가 서버(109) 측에서 추가 네트워크 요소를 소비하지 않고 복수 개의 자원 정보에 대한 사용자 계정의 접근 여부를 관리하기 위해 활용되는 기준이 되는 정보일 수 있다.

- [0046] 일 실시예에 따르면, 상기 정보 접근 관리부(107)는 상기 중앙 인가 서버(109)에 상기 접근 정책 매트릭스 정보를 반영하여, 상기 복수 개의 자원 정보에 접근하는 사용자 계정 중 상기 복수 개의 자원 정보에 대한 보안성이 위협되는 상황을 유발하는 사용자 계정의 접근을 방지해 상기 복수 개의 자원 정보에 대한 보안성을 유지 및 관리할 수 있다.
- [0047] 도 2는 본 발명의 일 실시 예에 따른 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템의 신뢰 등급 설정부를 설명하기 위한 블록도이다.
- [0048] 도 2를 참조하면, 하나 이상의 프로세서 및 상기 프로세서에서 수행 가능한 명령들을 저장하는 하나 이상의 메모리를 포함하는 컴퓨팅 장치로 구현되는 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템(예: 도 1의 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템(100))(이하, 접속 및 접근 관리 시스템으로 칭함)은 신뢰 등급 설정부(200)(예: 도 1의 신뢰 등급 설정부(101))를 포함할 수 있다.
- [0049] 일 실시예에 따르면, 상기 신뢰 등급 설정부(200)는 복수의 사용자 계정 중 제1 사용자 계정(201a)이 기업에서 관리하는 중앙 인가 서버(201b)에 접속하는 것을 감지하는 경우, 상기 제1 사용자 계정의 신뢰 상태를 확인하기 위한 신뢰 확인 프로세스를 시작하여, 상기 제1 사용자 계정의 신뢰 등급(205a)을 설정할 수 있다.
- [0050] 일 실시예에 따르면, 상기 신뢰 등급 설정부(200)는 상술한 기능을 수행하기 위한 세부 구성으로, 계정 접속 감지부(201), 신뢰 등급 식 식별부(203) 및 제1 등급 설정부(205)를 포함할 수 있다.
- [0051] 일 실시예에 따르면, 상기 계정 접속 감지부(201)는, 상기 제1 사용자 계정(201a)이 상기 중앙 인가 서버(201b)에 접속하는 것을 감지하는 경우, 상기 제1 사용자 계정(201a)이 상기 중앙 인가 서버(201b)에 접속함에 따라 생성되는 접속 이력 정보를 추출할 수 있다.
- [0052] 일 실시예에 따르면, 상기 접속 이력 정보는, 상기 제1 사용자 계정(201a)이 상기 중앙 인가 서버(201b)에 접속함에 따라 활동한 이력에 기반해 생성되는 정보일 수 있다. 상기와 관련하여, 접속 이력 정보는 복수 개의 카테고리 구성된 정보일 수 있다.
- [0053] 일 실시예에 따르면, 복수 개의 카테고리는 제1 사용자 계정(201a)에 등록된 사용자의 개인 정보(예: 성명, 성별, 나이, 신장, 체중 등)를 포함하는 제1 카테고리, 상기 제1 사용자 계정(201a)이 상기 중앙 인가 서버(201b)에 접속한 위치(사내 망 위치, 외부 망 위치 등) 및 접속 경로에 기반한 위치 경로 정보를 포함하는 제2 카테고리, 상기 제1 사용자 계정(201a)이 상기 중앙 인가 서버(201b)에 접속하기 위해 사용한 인증 수단(ID/PW 인증, 생체 인증, OTP 인증 등) 및 전자 장치(스마트 폰, 사내 인증 태블릿, 사내 인증 스마트 폰 등)에 기반한 인증 장치 정보를 포함하는 제3 카테고리 및 상기 제1 사용자 계정(201a)에 등록된 사용자의 근무 부서, 직위 및 고용 형태에 기반한 사원 정보를 포함하는 제4 카테고리를 포함할 수 있으며, 상기 중앙 인가 서버(201b)를 관리하는 관리자 계정의 요구사항에 의해 별도의 추가 카테고리를 더 포함할 수 있다.
- [0054] 일 실시예에 따르면, 상기 신뢰 등급 식 식별부(203)는 상기 접속 이력 정보의 추출이 완료됨에 따라 상기 신뢰 확인 프로세스가 시작되는 경우, 상기 추출된 접속 이력 정보에 포함된 복수 개의 카테고리 각각에 포함된 세부 정보를 확인하여, 상기 복수 개의 카테고리 각각에 대응되는 기 설정된 신뢰 요소 카테고리 각각에 설정되어 있는 복수 개의 신뢰 등급 산출 식을 식별할 수 있다.
- [0055] 일 실시예에 따르면, 상기 신뢰 확인 프로세스는 상기 접속 이력 정보를 구성하는 복수 개의 카테고리 별로 포함된 세부 정보를 기 설정된 신뢰 요소 카테고리(203b) 각각에 설정된 신뢰 등급 산출 식에 반영하여, 상기 기 설정된 신뢰 요소 카테고리(203b) 별로 세부 신뢰 등급을 산출하고, 상기 산출된 세부 신뢰 등급을 통해 제1 사용자 계정에 대한 신뢰 등급을 산출하기 위한 프로세스일 수 있다.
- [0056] 일 실시예에 따르면, 상기 기 설정된 신뢰 요소 카테고리(203b)는 제1 신뢰 요소 카테고리, 제2 신뢰 요소 카테고리, 제3 신뢰 요소 카테고리 및 제4 신뢰 요소 카테고리를 포함할 수 있다.
- [0057] 일 실시예에 따르면, 상기 제1 신뢰 요소 카테고리는 상기 복수 개의 카테고리 중 상기 제1 사용자 계정에 등록된 사용자의 개인 정보를 포함하는 제1 카테고리에 대응되는 카테고리로서, 상기 개인 정보가 반영되어 제1 신뢰 등급을 산출하는 제1 신뢰 등급 산출 식을 포함할 수 있다.
- [0058] 일 실시예에 따르면, 상기 제2 신뢰 요소 카테고리는 상기 복수 개의 카테고리 중 상기 제1 사용자 계정이 상기 중앙 인가 서버에 접속한 위치 및 접속 경로에 기반한 위치 경로 정보를 포함하는 제2 카테고리에 대응되는 카테고리로서, 상기 위치 경로 정보가 반영되어 제2 신뢰 등급을 산출하는 제2 신뢰 등급 산출 식을 포함할 수 있다.

다.

- [0059] 예를 들어, 상기 제2 신뢰 요소 카테고리는 위치 경로 정보가 반영되는 복수 개의 신뢰 등급 산출 식이 포함된 상태일 수 있다. 이 때, 상기 제2 신뢰 요소 카테고리에 포함된 복수 개의 신뢰 등급 산출 식 중 외부 IP 항목에 대응되는 신뢰 등급 산출 식은 외부 IP를 통해 상기 중앙 인가 서버(201b)에 접속한 제1 사용자 계정(201a)으로부터 추출된 접속 이력 정보의 위치 경로 정보가 반영되는 구성일 수 있다.
- [0060] 일 실시예에 따르면, 상기 제3 신뢰 요소 카테고리는 상기 복수 개의 카테고리 중 상기 제1 사용자 계정이 상기 중앙 인가 서버에 접속하기 위해 사용한 인증 수단 및 전자 장치에 기반한 인증 장치 정보를 포함하는 제3 카테고리에 대응되는 카테고리로서, 상기 인증 장치 정보가 반영되어 제3 신뢰 등급을 산출하는 제3 신뢰 등급 산출 식을 포함할 수 있다.
- [0061] 일 실시예에 따르면, 상기 제4 신뢰 요소 카테고리는 상기 복수 개의 카테고리 중 상기 제1 사용자 계정에 등록된 사용자의 근무 부서, 직위 및 고용 형태에 기반한 사원 정보를 포함하는 제4 카테고리에 대응되는 카테고리로서, 상기 사원 정보가 반영되어 제4 신뢰 등급을 산출하는 제4 신뢰 등급 산출 식을 포함할 수 있다.
- [0062] 일 실시예에 따르면, 상기 신뢰 등급 식 식별부(203)는 상기 기 설정된 신뢰 요소 카테고리 각각에 설정되어 있는 복수 개의 신뢰 등급 산출 식 중 상기 접속 이력 정보에 포함된 세부 정보(예: 개인 정보, 위치 경로 정보, 인증 장치 정보, 사원 정보)가 매칭되는 적어도 하나의 신뢰 등급 산출 식을 식별하여, 상기 식별된 적어도 하나의 신뢰 등급 산출 식을 통해 상기 기 설정된 신뢰 요소 카테고리 별로 세부 신뢰 등급을 산출할 수 있다.
- [0063] 일 실시예에 따르면, 상기 신뢰 등급 식 식별부(203)는 상기 기 설정된 신뢰 요소 카테고리 각각에 설정되어 있는 복수 개의 신뢰 등급 산출 식 중 상기 접속 이력 정보에 기반한 세부 정보가 반영되는 항목을 가지는 적어도 하나의 신뢰 등급 산출 식을 식별할 수 있다.
- [0064] 상기와 관련하여, 상기 신뢰 등급 식 식별부(203)는 상기 식별된 적어도 하나의 신뢰 등급 산출 식을 통해 상기 기 설정된 신뢰 요소 카테고리 별로 세부 신뢰 등급을 산출할 수 있다.
- [0065] 예를 들어, 상기 신뢰 등급 식 식별부(203)는 상기 접속 이력 정보에 기반한 세부 정보로써, 위치 경로 정보를 식별한 경우, 기 설정된 신뢰 요소 카테고리 중 제2 신뢰 점수 산출 카테고리를 식별할 수 있다. 상기와 관련하여, 상기 제2 신뢰 점수 산출 카테고리는 위치 경로 정보가 반영되는 복수 개의 신뢰 등급 산출 식이 포함된 상태일 수 있다.
- [0066] 상기와 관련하여, 상기 제2 신뢰 점수 산출 카테고리에 포함된 복수 개의 신뢰 등급 산출 식 중 외부 IP 항목에 대응되는 신뢰 등급 산출 식은 외부 IP를 통해 상기 중앙 인가 서버(201b)에 접속한 제1 사용자 계정(201a)으로부터 추출된 접속 이력 정보의 위치 경로 정보가 반영되는 구성일 수 있다.
- [0067] 즉, 상기 신뢰 등급 식 식별부(203)는 상기 접속 이력 정보에 포함된 위치 경로 정보의 내용을 확인하여, 상기 확인된 위치 경로 정보의 내용이 외부 IP 위치로 확인되는 경우, 상기 제2 신뢰 점수 산출 카테고리에 포함된 복수 개의 신뢰 등급 산출 식 중 외부 IP 항목에 대응되는 신뢰 등급 산출 식을 식별할 수 있다.
- [0068] 일 실시예에 따르면, 상기 제1 등급 설정부(205)는 상기 신뢰 등급 식 식별부(203)의 기능 수행이 완료되면, 상기 식별된 복수 개의 신뢰 등급 산출 식을 통해 상기 기 설정된 신뢰 요소 카테고리 별로 상기 제1 사용자 계정이 상기 중앙 인가 서버에서 관리하는 상기 복수 개의 자원 정보에 접근 시 접근 여부를 확인하기 위해 활용되는 신뢰 등급을 산출해 상기 제1 사용자 계정에 대한 신뢰 등급의 설정을 완료할 수 있다.
- [0069] 예를 들어, 상기 제1 등급 설정부(205)는 상기 신뢰 등급 식 식별부(203)의 기능 수행에 의해 상기 위치 경로 정보가 반영되는 외부 IP 항목에 대응되는 신뢰 등급 산출 식의 식별이 완료되면, 상기 식별된 신뢰 등급 산출 식에 매칭되어 있는 수치를 확인하여, 상기 제2 신뢰 요소 카테고리에 대한 세부 신뢰 등급을 산출할 수 있다. 예를 들어, 상기 위치 경로 정보가 반영되는 외부 IP 항목에 대응되는 신뢰 등급 산출 식에 매칭되어 있는 수치를 0.5로 확인할 수 있다.
- [0070] 다른 예를 들어, 상기 제3 신뢰 요소 카테고리는 인증 수단 정보가 반영되는 복수 개의 신뢰 등급 산출 식이 포함된 상태일 수 있다. 이 때, 상기 제3 신뢰 요소 카테고리에 포함된 복수 개의 신뢰 등급 산출 식 중 ID/PW 인증 항목에 대응되는 신뢰 등급 산출 식은 ID/PW를 입력해 상기 중앙 인가 서버(201b)에 접속한 제1 사용자 계정(201a)으로부터 추출된 접속 이력 정보의 인증 수단 정보가 반영되는 구성일 수 있다.
- [0071] 이 때, 상기 제1 등급 설정부(205)는 제1 사용자 계정(201a)의 사용자가 추가적으로 OTP 인증을 수행한 경우,

상기 제3 신뢰 요소 카테고리에 포함된 복수 개의 신뢰 등급 산출 식 중 OTP 인증 항목에 대응되는 신뢰 등급 산출 식에 상기 인증 수단 정보를 반영할 수 있다.

- [0072] 즉, 상기 제1 등급 설정부(205)는 상기 인증 수단 정보가 반영되는 ID/PW 인증 항목에 대응되는 신뢰 등급 산출 식 및 상기 인증 수단 정보가 반영되는 OTP 인증 항목에 대응되는 신뢰 등급 산출 식에 매칭되어 있는 수치를 각각 확인할 수 있다.
- [0073] 이 후, 상기 제1 등급 설정부(205)는 ID/PW 인증 항목에 대응되는 신뢰 등급 산출 식을 통해 확인된 수치와 및 상기 인증 수단 정보가 반영되는 OTP 인증 항목에 대응되는 신뢰 등급 산출 식을 통해 확인된 수치를 합산해 상기 제3 신뢰 점수 산출 카테고리에 대한 세부 신뢰 점수를 산출할 수 있다.
- [0074] 상기와 관련하여, 상기 기 설정된 신뢰 요소 카테고리 각각에 포함된 복수 개의 신뢰 등급 산출 식은 각각이 다른 수치가 매칭된 상태일 수 있다. 예를 들어, 상기 제3 신뢰 점수 산출 카테고리에 포함된 복수 개의 신뢰 등급 산출 식은 각각 ID/PW 인증 항목에 대한 신뢰 등급 산출 식, OTP 인증 항목에 대한 신뢰 등급 산출 식, FIDO 생체 인증 항목에 대한 신뢰 등급 산출 식을 포함할 수 있다.
- [0075] 이 때, 상기 ID/PW 인증 항목에 대한 신뢰 등급 산출 식, OTP 인증 항목에 대한 신뢰 등급 산출 식, FIDO 생체 인증 항목에 대한 신뢰 등급 산출 식에 매칭되어 있는 수치는 보안성이 높은 순서인 FIDO 생체 인증 항목에 대한 신뢰 등급 산출 식, OTP 인증 항목에 대한 신뢰 등급 산출 식, ID/PW 인증 항목에 대한 신뢰 등급 산출 식 순으로 높은 수치가 매칭된 상태일 수 있다.
- [0076] 상기와 관련하여, 산출된 세부 신뢰 등급은 이후에 후술할 기 저장된 복수 개의 보안 정책 정보에 반영될 수 있다. 즉, 상기 세부 신뢰 등급은 상기 기 저장된 복수 개의 보안 정책 정보 각각에 기반한 보안 정책 별로 반영될 수 있으며, 상기 세부 신뢰 등급을 합산해 산출된 상기 제1 사용자 계정(201a)에 대한 종합적인 신뢰 등급인 종합 신뢰 등급도 상기 기 저장된 복수 개의 보안 정책 정보 각각에 기반한 보안 정책 별로 반영될 수 있다.
- [0077] 일 실시예에 따르면, 상기 제1 등급 설정부(205)는 상기 세부 신뢰 등급의 산출이 완료되면, 상기 기 설정된 신뢰 요소 카테고리 별로 설정되어 있는 가중치를 상기 세부 신뢰 등급에 적용한 후, 상기 가중치가 적용된 세부 신뢰 등급을 합산하여, 상기 제1 사용자 계정(201a)에 대한 종합 신뢰 등급을 산출할 수 있다.
- [0078] 이 때, 상기 제1 등급 설정부(205)는 기 설정된 신뢰 요소 카테고리 별로 설정되어 있는 가중치를 식별할 수 있다. 상기와 관련하여, 가중치는 상기 중앙 인가 서버(201b)를 관리하는 관리자 계정에 의해 상기 기 설정된 신뢰 요소 카테고리 별로 설정되어 있는 구성으로, 상기 복수 개의 자원 정보 각각에 대한 복수의 사용자 계정의 접근을 통제 및 관리하기 위해 변경 가능한 구성일 수 있다.
- [0079] 이에 따라, 상기 제1 등급 설정부(205)는 상기 기 설정된 신뢰 요소 카테고리 별로 설정되어 있는 가중치와 상기 기 설정된 신뢰 요소 카테고리 별로 산출된 세부 신뢰 등급에 기반해 제1 사용자 계정에 대한 종합 신뢰 등급을 산출할 수 있다.
- [0080] 도 3은 본 발명의 일 실시 예에 따른 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템의 중요도 등급 설정부를 설명하기 위한 블록도이다.
- [0081] 도 3을 참조하면, 하나 이상의 프로세서 및 상기 프로세서에서 수행 가능한 명령들을 저장하는 하나 이상의 메모리를 포함하는 컴퓨팅 장치로 구현되는 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템(예: 도 1의 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템(100))(이하, 접속 및 접근 관리 시스템으로 칭함)은 중요도 등급 설정부(300)(예: 도 1의 중요도 등급 설정부(103))를 포함할 수 있다.
- [0082] 일 실시예에 따르면, 상기 중요도 등급 설정부(300)는 신뢰 등급 설정부(예: 도 1의 신뢰 등급 설정부(101))의 기능이 수행되는 동안 기업에서 관리하는 복수 개의 자원 정보(301a)에 대한 중요도를 확인하기 위한 중요도 확인 프로세스를 시작하여, 상기 복수 개의 자원 정보(301a) 각각에 대한 중요도 등급(303a)을 설정할 수 있다.
- [0083] 일 실시예에 따르면, 상기 중요도 등급 설정부(300)는 상술한 기능을 수행하기 위한 세부 구성으로, 중요도 등급 산출 식 식별부(301) 및 제2 등급 설정부(303)를 포함할 수 있다.
- [0084] 일 실시예에 따르면, 상기 중요도 등급 산출 식 식별부(301)는 상기 신뢰 등급 설정부의 기능이 수행되는 동안 상기 중요도 확인 프로세스를 시작하여, 상기 기업에서 관리하는 복수 개의 자원 정보(301a)에 포함된 복수 개의 자원 카테고리를 식별해 상기 복수 개의 자원 카테고리 및 대응되는 기 설정된 중요도 요소 카테고리 각각에

설정되어 있는 복수 개의 중요도 등급 산출 식을 식별할 수 있다.

- [0085] 일 실시예에 따르면, 상기 중요도 등급 산출 식 식별부(301)는 상기 복수 개의 자원 정보(301a) 각각에 포함된 복수 개의 자원 카테고리를 식별할 수 있다.
- [0086] 일 실시예에 따르면, 상기 복수 개의 자원 정보(301a) 각각은 상기 복수 개의 자원 카테고리로 구성된 정보로써, 상기 복수 개의 자원 카테고리 각각은 요소 정보를 포함하고 있는 상태일 수 있다. 이 때, 상기 복수 개의 자원 카테고리는 제1 자원 카테고리, 제2 자원 카테고리, 제3 자원 카테고리 및 제4 자원 카테고리를 포함할 수 있다.
- [0087] 일 실시예에 따르면, 상기 제1 자원 카테고리는 상기 복수 개의 자원 카테고리 중 상기 복수 개의 자원 정보(301a) 각각에 입력된 다른 사용자의 개인 정보의 입력 여부에 기반한 입력 여부 정보를 포함할 수 있다. 상기 와 관련하여, 다른 사용자에 대한 개인 정보는 다른 사용자의 성명, 성별, 생년월일, 소속 기업, 소속 기업 내 부서 및 직위 등을 포함할 수 있으며, 이외에도 다른 개인 정보를 요소 정보로 포함할 수 있다.
- [0088] 일 실시예에 따르면, 상기 제2 자원 카테고리는 상기 복수 개의 자원 카테고리 중 상기 복수 개의 자원 정보(301a) 각각의 영업 기밀 등급에 기반한 기밀 등급 정보를 포함할 수 있다. 상기 기밀 등급 정보는 상기 기업에서 규정한 기준에 따라 책정된 기밀 등급에 대한 정보일 수 있다.
- [0089] 일 실시예에 따르면, 상기 제3 자원 카테고리는 상기 복수 개의 자원 카테고리 중 상기 복수 개의 자원 정보(301a) 각각에 설정되어 있는 사용자 편집 기능에 기반한 기능 제한 정보를 포함할 수 있다. 상기 기능 제한 정보는 복수 개의 자원 정보(301a) 각각의 편집 여부, 복수 개의 자원 정보(301a) 각각에 대한 직급 별 편집 여부 등을 포함하는 정보일 수 있다.
- [0090] 일 실시예에 따르면, 상기 제4 자원 카테고리는 상기 복수 개의 자원 카테고리 중 상기 복수 개의 자원 정보(301a) 각각을 활용하는 주요 시스템의 등급에 기반한 시스템 등급 정보를 포함할 수 있다. 상기 시스템 등급 정보는 상기 복수 개의 자원 정보(301a)를 활용하는 시스템을 상기 기업에서 규정한 기준에 따라 책정된 등급에 대한 정보일 수 있다.
- [0091] 일 실시예에 따르면, 상기 중요도 등급 산출 식 식별부(301)는 상기 자원 정보에 포함된 복수 개의 자원 카테고리를 식별하여, 상기 복수 개의 자원 카테고리 별 요소 정보를 식별할 수 있다. 이후, 상기 프로세서는 상기 식별된 복수 개의 자원 카테고리 및 대응되는 기 설정된 중요도 요소 카테고리를 식별할 수 있다.
- [0092] 상기와 관련하여, 상기 기 설정된 중요도 요소 카테고리(301b)는 제1 중요도 요소 카테고리, 제2 중요도 요소 카테고리, 제3 중요도 요소 카테고리 및 제4 중요도 요소 카테고리를 포함할 수 있다.
- [0093] 일 실시예에 따르면, 상기 제1 중요도 요소 카테고리는 상기 복수 개의 자원 카테고리 중 상기 복수 개의 자원 정보 각각에 입력된 다른 사용자의 개인 정보의 입력 여부에 기반한 입력 여부 정보를 포함하는 제1 자원 카테고리에 대응되는 카테고리로서, 상기 입력 여부 정보가 반영되어 제1 중요도 등급을 산출하는 제1 중요도 등급 산출 식을 포함할 수 있다.
- [0094] 예를 들어, 상기 제1 중요도 요소 카테고리는 입력 여부 정보가 반영되는 복수 개의 제1 중요도 등급 산출 식이 포함된 상태일 수 있다. 이 때, 상기 제1 중요도 요소 카테고리에 포함된 복수 개의 제1 중요도 등급 산출 식 중 입력 확인 항목에 대응되는 제1 중요도 등급 산출 식은 상기 제1 자원 정보에 다른 사용자의 개인 정보가 입력되어 있음이 확인됨에 따라 상기 요소 정보 중 하나인 입력 여부 정보가 반영되는 구성일 수 있다.
- [0095] 또한, 상기 제1 중요도 요소 카테고리에 포함된 복수 개의 제1 중요도 등급 산출 식 중 입력 미확인 항목에 대응되는 제1 중요도 등급 산출 식은 상기 제1 자원 정보에 다른 사용자의 개인 정보가 미 입력되어 있음이 확인됨에 따라 상기 요소 정보 중 하나인 입력 여부 정보가 반영되는 구성일 수 있다.
- [0096] 일 실시예에 따르면, 상기 제2 중요도 요소 카테고리는 상기 복수 개의 자원 카테고리 중 상기 복수 개의 자원 정보 각각의 영업 기밀 등급에 기반한 기밀 등급 정보를 포함하는 제2 자원 카테고리에 대응되는 카테고리로서, 상기 기밀 등급 정보가 반영되어 제2 중요도 등급을 산출하는 제2 중요도 등급 산출 식을 포함할 수 있다.
- [0097] 일 실시예에 따르면, 상기 제3 중요도 요소 카테고리는 상기 복수 개의 자원 카테고리 중 상기 복수 개의 자원 정보 각각에 설정되어 있는 사용자 편집 기능에 기반한 기능 제한 정보를 포함하는 제3 자원 카테고리에 대응되는 카테고리로서, 상기 기능 제한 정보가 반영되어 제3 중요도 등급을 산출하는 제3 중요도 등급 산출 식을 포함할 수 있다.

- [0098] 일 실시예에 따르면, 상기 제4 중요도 요소 카테고리는 상기 복수 개의 자원 카테고리 중 상기 복수 개의 자원 정보 각각을 활용하는 주요 시스템의 등급에 기반한 시스템 등급 정보를 포함하는 제4 자원 카테고리에 대응되는 카테고리로서, 상기 시스템 등급 정보가 반영되어 제4 중요도 등급을 산출하는 제4 중요도 등급 산출 식을 포함할 수 있다.
- [0099] 이에 따라, 상기 중요도 등급 산출식 식별부(301)는 상기 기업에서 관리하는 복수 개의 자원 정보(301a)에 포함된 복수 개의 자원 카테고리를 식별해 상기 복수 개의 자원 카테고리들과 대응되는 기 설정된 중요도 요소 카테고리와 각각에 설정되어 있는 복수 개의 중요도 등급 산출 식을 식별 완료할 수 있다.
- [0100] 일 실시예에 따르면, 상기 제2 등급 설정부(303)는 상기 중요도 등급 산출 식 식별부(301)의 기능 수행의 완료되면, 기 설정된 중요도 요소 카테고리(301b) 각각에 설정되어 있는 복수 개의 중요도 등급 산출 식 중 상기 식별된 자원 카테고리에 포함된 자원 요소 정보가 반영되는 적어도 하나의 중요도 등급 산출 식을 식별하여, 상기 식별된 적어도 하나의 중요도 등급 산출 식을 통해 상기 기 설정된 중요도 요소 카테고리 별로 중요도 등급을 산출해 상기 복수 개의 자원 정보(301a) 각각에 대해 중요도 등급의 설정을 완료할 수 있다.
- [0101] 일 실시예에 따르면, 상기 제2 등급 설정부(303)는 상기 기 설정된 중요도 요소 카테고리 각각에 설정되어 있는 복수 개의 중요도 등급 산출 식 중 상기 식별된 복수 개의 자원 카테고리에 포함된 요소 정보가 매칭되는 적어도 하나의 중요도 등급 산출 식을 식별하여, 상기 식별된 적어도 하나의 중요도 등급 산출 식을 통해 상기 기 설정된 중요도 요소 카테고리 별로 세부 중요도 등급을 산출할 수 있다.
- [0102] 예를 들어, 상기 중요도 등급 산출 식 식별부(301)는 상기 제1 자원 정보를 구성하는 복수 개의 자원 카테고리 중 제1 자원 카테고리에 대응되는 제1 중요도 요소 카테고리의 식별이 완료됨에 따라, 상기 식별된 제1 중요도 요소 카테고리에 포함된 복수 개의 제1 중요도 등급 산출 식 중 상기 제1 자원 카테고리에 포함된 요소 정보인 입력 여부 정보가 반영되는 항목을 가지는 제1 중요도 등급 산출 식을 식별할 수 있다.
- [0103] 보다 정확하게, 상기 제2 등급 설정부(303)는 상기 입력 여부 정보를 통해 상기 제1 자원 정보에 다른 사용자의 개인 정보가 입력되어 있음이 확인한 경우, 상기 제1 중요도 요소 카테고리에 포함된 복수 개의 제1 중요도 등급 산출 식 중 입력 확인 항목에 대응되는 제1 중요도 등급 산출 식을 식별하여, 상기 식별된 제1 중요도 등급 산출 식에 상기 입력 여부 정보를 반영할 수 있다.
- [0104] 상기와 관련하여, 상기 제2 등급 설정부(303)는 상기 입력 여부 정보가 반영되는 입력 확인 항목에 대응되는 제1 중요도 등급 산출 식에 매칭되어 있는 수치를 확인할 수 있다. 이후, 상기 제2 등급 설정부(303)는 상기 제1 중요도 등급 산출 식에 매칭되어 있는 수치를 확인하면, 상기 확인된 수치를 상기 제1 중요도 점수 산출 카테고리에 대한 세부 중요도 등급으로 산출할 수 있다.
- [0105] 다만, 상기 제2 등급 설정부(303)는 상기 요소 정보가 상기 기 설정된 중요도 요소 카테고리(301b) 중 하나에 포함된 복수 개의 제1 중요도 등급 산출 식 중 두 개 이상 반영되는 경우, 상기 요소 정보가 각각 반영되는 제1 중요도 등급 산출 식에 대한 수치를 확인하여, 상기 확인된 수치를 합산해 상기 기 설정된 중요도 요소 카테고리에 대한 세부 중요도 등급으로 산출할 수 있다.
- [0106] 상기와 관련하여, 산출된 세부 중요도 등급은 이후에 후술할 기 저장된 복수 개의 보안 정책 정보에 반영될 수 있다. 즉, 상기 세부 중요도 등급은 상기 기 저장된 복수 개의 보안 정책 정보 각각에 기반한 보안 정책 별로 반영될 수 있으며, 상기 세부 중요도 등급을 합산해 산출된 상기 자원 정보에 대한 종합적인 중요도 등급인 종합 중요도 등급도 상기 기 저장된 복수 개의 보안 정책 정보 각각에 기반한 보안 정책 별로 반영될 수 있다.
- [0107] 도 4는 본 발명의 일 실시 예에 따른 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템의 매트릭스 정보 생성부를 설명하기 위한 블록도이다.
- [0108] 도 4를 참조하면, 하나 이상의 프로세서 및 상기 프로세서에서 수행 가능한 명령들을 저장하는 하나 이상의 메모리를 포함하는 컴퓨팅 장치로 구현되는 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템(예: 도 1의 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템(100))(이하, 접속 및 접근 관리 시스템으로 칭함)은 매트릭스 정보 생성부(400)(예: 도 1의 매트릭스 정보 생성부(105))를 포함할 수 있다.
- [0109] 일 실시예에 따르면, 상기 매트릭스 정보 생성부(400)는 신뢰 등급 설정부(예: 도 1의 신뢰 등급 설정부(101)) 및 중요도 등급 설정부(예: 도 1의 중요도 등급 설정부(103))의 기능 수행이 완료되면, 기 저장된 복수 개의 보안 정책 정보(401c)에 상기 신뢰 등급(401a) 및 상기 중요도 등급(401b)을 반영하여, 상기 복수 개의 자원 정보

각각에 대한 제1 사용자 계정의 접근 여부를 판별 가능한 정책 매트릭스(403b)를 생성한 후, 기 저장된 시뮬레이션 알고리즘(405a)을 통해 상기 정책 매트릭스(403b)에 기반한 접근 정책 시뮬레이션을 수행하여, 상기 수행된 시뮬레이션 결과에 기반해 접근 정책 매트릭스 정보를 생성할 수 있다.

- [0110] 일 실시예에 따르면, 상기 매트릭스 정보 생성부(400)는 상술한 기능을 수행하기 위한 세부 구성으로, 등급 반영부(401), 정책 매트릭스 생성부(403) 및 매트릭스 보정 결정부(405)를 포함할 수 있다.
- [0111] 일 실시예에 따르면, 상기 등급 반영부(401)는 상기 신뢰 등급 설정부 및 상기 중요도 등급 설정부의 기능 수행이 완료되면, 기 저장된 복수 개의 보안 정책 정보(401c)를 기 설정된 접근 기준 별로 식별하여, 상기 기 설정된 접근 기준 별로 식별된 보안 정책 정보 각각에 상기 신뢰 등급(401a) 및 중요도 등급(401b)을 반영할 수 있다.
- [0112] 일 실시예에 따르면, 상기 기 저장된 복수 개의 보안 정책 정보(401c)는 보안 정책 내용이 기 설정된 접근 기준 별로 설정된 상태일 수 있다. 예를 들어, 복수 개의 보안 정책 정보(401c) 중 제1 보안 정책 정보의 제1 접근 기준은 위치 기준의 세부 신뢰 등급과 기밀 기준의 세부 중요도 등급이 매칭되어 있는 기준일 수 있다.
- [0113] 예를 들어, 상기 등급 반영부(401)는 상기 제1 접근 기준을 기반으로, 제1 사용자 계정의 세부 신뢰 등급 중 위치 기준에 해당되는 제2 신뢰 등급과 상기 제1 사용자 계정이 접근하려는 자원 정보의 세부 중요도 등급 중 기밀 기준에 해당되는 제2 중요도 등급을 상기 제1 보안 정책 정보에 반영할 수 있다.
- [0114] 일 실시예에 따르면, 상기 정책 매트릭스 생성부(403)는 상기 등급 반영부(401)의 기능 수행에 의해 상기 기 설정된 접근 기준(403a) 별로 식별된 보안 정책 정보 각각에 상기 신뢰 등급 및 중요도 등급이 반영됨에 따라 상기 복수 개의 자원 정보(401c) 각각에 대한 상기 기 설정된 접근 기준(403a) 별로 제1 사용자 계정의 접근 여부가 반영된 정책 매트릭스(403b)를 생성할 수 있다.
- [0115] 를 생성할 수 있다.
- [0116] 예를 들어, 상기 정책 매트릭스 생성부(403)는 상기 등급 반영부(401)의 기능 수행에 의해 제1 사용자 계정의 세부 신뢰 등급 중 위치 기준에 해당되는 제2 신뢰 등급과 상기 제1 사용자 계정이 접근하려는 자원 정보의 세부 중요도 등급 중 기밀 기준에 해당되는 제2 중요도 등급을 상기 제1 보안 정책 정보에 반영됨에 따라 상기 제1 보안 정책 정보에 대한 제1 접근 기준에 기반한 제1 사용자 계정의 접근 여부가 반영된 정책 매트릭스(403b)를 생성할 수 있다.
- [0117] 이 때, 제1 보안 정책 정보는, 제2 중요도 등급이 1등급으로 설정된 제1 자원 정보에 접근하기 위한 사용자 계정의 제2 신뢰 등급은 1등급으로 설정된 보안 정책을 포함하고 있는 상태일 수 있다.
- [0118] 이에 따라, 상기 정책 매트릭스 생성부(403)는 제1 사용자 계정의 제2 신뢰 등급이 1등급임에 따라 제2 중요도 등급이 1등급으로 설정된 제1 자원 정보에 접근 가능하도록 보안 정책이 설정된 정책 매트릭스(403b)를 생성할 수 있다.
- [0119] 일 실시예에 따르면, 상기 매트릭스 보정 결정부(405)는 상기 정책 매트릭스 생성부(403)의 기능 수행이 완료된 상태에서, 상기 기 저장된 시뮬레이션 알고리즘(405a)을 통해 상기 생성된 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 수행하여, 상기 접근 정책 시뮬레이션 결과에 기반해 상기 정책 매트릭스(403b)의 보정 여부를 결정할 수 있다.
- [0120] 일 실시예에 따르면, 상기 기 저장된 시뮬레이션 알고리즘(405a)은 다른 정책 매트릭스, 상기 다른 정책 매트릭스에 대한 보정 이력 정보, 상기 다른 정책 매트릭스에 기반한 접근 정책 매트릭스 정보 및 상기 다른 정책 매트릭스에 대응되는 보안 정책 정보에 대한 보정 이력 정보(정책 성공 이력 정보, 정책 실패 이력 정보 및 실패 이력 정보에 기반해 보정된 접근 정책 매트릭스 정보) 간의 상관 관계를 분석 및 학습하여, 상기 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 수행해 상기 접근 정책 시뮬레이션에서 발생하는 이벤트 중 보안 위험 상태에 대응되는 자원 정보의 유출 이벤트 및 자원 정보의 해킹 이벤트 여부를 식별하고, 식별 결과에 따라 상기 기 설정된 접근 기준에 기반한 신뢰 등급 및 중요도 등급 각각의 산출 식에 매칭되어 있는 가중치를 보정하거나 상기 비정상 정책으로 판단된 보안 정책 정보를 정상 정책의 보안 정책 정보로 보정하는 알고리즘일 수 있다.
- [0121] 일 실시예에 따르면, 상기 매트릭스 보정 결정부(405)는 상기 정책 매트릭스 생성부(403)의 기능 수행이 완료된 상태에서, 상기 기 저장된 시뮬레이션 알고리즘(405a)을 통해 상기 생성된 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 수행하여, 상기 접근 정책 시뮬레이션 결과에 기반해 상기 정책 매트릭스의 보정 여부를 결정할

수 있다.

- [0122] 상기와 관련하여, 상기 매트릭스 보정 결정부(405)는 상기 정책 매트릭스 생성부(403)의 기능 수행이 완료된 상태에서, 상기 기 저장된 시뮬레이션 알고리즘(405a)을 통해 상기 생성된 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 수행하여, 상기 접근 정책 시뮬레이션의 결과를 확인할 수 있다.
- [0123] 일 실시예에 따르면, 상기 매트릭스 보정 결정부(405)는 상기 확인된 접근 정책 시뮬레이션의 결과가 보안 위험 상태로 도출된 경우, 상기 보안 위험 상태로 도출된 정책 시뮬레이션에 기반한 신뢰 등급 및 중요도 등급을 산출하기 위한 산출 식에 매칭된 가중치를 보정하거나 상기 보안 위험 상태로 도출된 정책 시뮬레이션에 대응되는 비정상 정책(비정상 보안 정책)의 보안 정책 정보를 정상 정책의 보안 정책 정보로 보정할 수 있다. 상기와 관련하여, 보안 위험 상태는 자원 정보의 유출 이벤트 및 자원 정보의 해킹 이벤트를 포함하는 상태일 수 있다.
- [0124] 도 5는 본 발명의 일 실시 예에 따른 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템의 매트릭스 보정 결정부를 설명하기 위한 블록도이다.
- [0125] 도 5를 참조하면, 하나 이상의 프로세서 및 상기 프로세서에서 수행 가능한 명령들을 저장하는 하나 이상의 메모리를 포함하는 컴퓨팅 장치로 구현되는 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템(예: 도 1의 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템(100))(이하, 접속 및 접근 관리 시스템으로 칭함)은 매트릭스 보정 결정부(500)(예: 도 4의 매트릭스 보정 결정부(403))를 포함할 수 있다.
- [0126] 일 실시예에 따르면, 상기 매트릭스 보정 결정부(500)는 정책 매트릭스 생성부(예: 도 4의 정책 매트릭스 생성부(403))의 기능 수행이 완료된 상태에서, 상기 기 저장된 시뮬레이션 알고리즘(501a)을 통해 상기 생성된 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 수행하여, 상기 접근 정책 시뮬레이션 결과에 기반해 상기 정책 매트릭스의 보정 여부를 결정할 수 있다.
- [0127] 일 실시예에 따르면, 상기 매트릭스 보정 결정부(500)는 상술한 기능을 수행하기 위한 세부 구성으로, 가중치 보정부(501), 제1 접근 정책 매트릭스 정보 생성부(503) 및 제2 접근 정책 매트릭스 정보 생성부(505)를 포함할 수 있다.
- [0128] 일 실시예에 따르면, 상기 가중치 보정부(501)는 상기 기 저장된 시뮬레이션 알고리즘(501a)을 통해 상기 생성된 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 수행하여, 상기 접근 정책 시뮬레이션 결과가 보안 위험 상태로 도출되는 경우, 상기 보안 위험 상태로 도출된 기 설정된 접근 기준에 기반한 신뢰 등급 및 중요도 등급 각각의 산출 식에 매칭되어 있는 가중치(501b)를 보정할 수 있다.
- [0129] 일 실시예에 따르면, 상기 가중치(501b)는 상기 중앙 인가 서버를 관리하는 관리자 계정에 의해 상기 기 설정된 신뢰 요소 카테고리 별로 설정되어 있는 제1 가중치 및 상기 기 설정된 중요도 요소 카테고리 별로 설정되어 있는 제2 가중치를 포함하며, 상기 복수 개의 자원 정보 각각에 대한 복수의 사용자 계정의 접근으로 인한 보안 위험 상태를 방지하기 위해 보정 가능한 구성일 수 있다.
- [0130] 즉, 상기 제1 가중치는 기 설정된 신뢰 요소 카테고리 별로 포함된 복수 개의 신뢰 등급 산출 식 각각에 매칭되어 있는 구성일 수 있으며, 상기 제2 가중치는 기 설정된 중요도 요소 카테고리 별로 포함된 복수 개의 중요도 등급 산출 식 각각에 매칭되어 있는 구성일 수 있다.
- [0131] 예를 들어, 상기 가중치 보정부(501)는 상기 기 저장된 시뮬레이션 알고리즘(501a)을 통해 제1 사용자 계정의 제2 신뢰 등급이 1등급임에 따라 제2 중요도 등급이 1등급으로 설정된 제1 자원 정보에 접근 가능하도록 보안 정책이 설정된 정책 매트릭스에 대한 접근 정책 시뮬레이션을 수행하여, 상기 접근 정책 시뮬레이션 결과가 보안 위험 상태로 도출되는 것을 확인할 수 있다. 이 때, 상기 가중치 보정부(501)는 상기 보안 위험 상태로 도출된 원인이 사용자의 접속 경로에 존재하는 것으로 판단할 수 있다.
- [0132] 이에 따라, 상기 가중치 보정부(501)는 상기 제2 신뢰 등급을 산출하기 위한 신뢰 등급 산출 식의 제1 가중치를 보정해 이후에 산출되는 제2 신뢰 등급의 수치가 낮게 산출되도록 변경할 수 있다.
- [0133] 상기와 관련하여, 상기 가중치 보정부(501)는 제2 중요도 등급을 산출하기 위한 중요도 등급 산출 식의 제2 가중치를 보정에 제2 중요도 등급의 수치가 1등급보다 높은 등급으로 산출되도록 변경해 자원 정보에 대한 사용자 계정의 접근 기준을 높일 수 있다.
- [0134] 일 실시예에 따르면, 상기 제1 접근 정책 매트릭스 정보 생성부(503)는 상기 기 저장된 시뮬레이션 알고리즘

(501a)을 통해 상기 생성된 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 수행하여, 상기 접근 정책 시뮬레이션 결과가 보안 안전 상태로 도출되는 경우, 상기 보안 안전 상태로 도출된 정책 매트릭스에 기반한 접근 정책 매트릭스 정보를 생성할 수 있다.

- [0135] 즉, 상기 제1 접근 정책 매트릭스 정보 생성부(503)는 상기 기 저장된 시뮬레이션 알고리즘(501a)을 통해 상기 생성된 정책 매트릭스에 기반한 접근 정책 시뮬레이션의 결과가 유출 이벤트 및 해킹 이벤트가 발생하지 않아 보안이 유지되는 보안 안전 상태로 도출되는 경우, 보안 안전 상태로 도출된 정책 매트릭스에 기반하여 접근 정책 매트릭스 정보를 생성할 수 있다.
- [0136] 일 실시예에 따르면, 상기 제2 접근 정책 매트릭스 정보 생성부(505)는 상기 가중치 보정부(501)의 기능이 완료된 상태에서, 상기 기 저장된 시뮬레이션 알고리즘(503a)을 통해 상기 가중치가 보정된 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 재수행하여, 상기 접근 정책 시뮬레이션의 결과가 상기 보안 안전 상태로 도출되는 경우, 상기 보안 안전 상태로 도출된 정책 매트릭스에 기반한 접근 정책 매트릭스 정보(507)를 생성할 수 있다.
- [0137] 예를 들어, 상기 제2 접근 정책 매트릭스 정보 생성부(505)는 상기 가중치 보정부(501)의 기능 수행에 의해 상기 제2 신뢰 등급을 산출하기 위한 신뢰 등급 산출 식의 제1 가중치를 보정해 이후에 산출되는 제2 신뢰 등급의 수치가 낮게 산출되도록 변경하거나 상기 제2 중요도 등급을 산출하기 위한 중요도 등급 산출 식의 제2 가중치를 보정해 제2 중요도 등급의 수치가 1등급보다 높은 등급으로 산출되도록 변경 완료한 경우, 가중치가 변경됨에 따라 자원 정보에 대한 사용자 계정의 접근 기준이 높아진 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 재수행할 수 있다.
- [0138] 이 때, 상기 제2 접근 정책 매트릭스 정보 생성부(505)는 상기 접근 정책 시뮬레이션의 결과가 상기 보안 안전 상태로 도출되는 경우, 상기 보안 안전 상태로 도출된 정책 매트릭스에 기반한 접근 정책 매트릭스 정보(507)를 생성할 수 있으며, 상기 정책 매트릭스에 대응되는 자원 정보에 접근을 시도한 제1 사용자 계정이 자원 정보에 접근하지 못하도록 차단할 수 있다. 이 때, 상기 정책 매트릭스는 도 5의 제1 접근 정책 매트릭스 정보 생성부(503)와 연동되어 있는 구성으로, 자원 다(예: 제1 자원 정보)에 대한 계정 B(예: 제1 사용자 계정)의 접근을 차단한 정책일 수 있다.
- [0139] 상기와 관련하여, 상기 보안 안전 상태로 도출된 정책 매트릭스에 기반한 접근 정책 매트릭스 정보(507)를 생성이 완료되면, 생성된 접근 정책 매트릭스 정보(507)는 기 저장된 복수 개의 보안 정책 정보에 반영되어, 이후에 진행되는 다른 사용자 계정들에 대한 매트릭스 정보 생성부(예: 도 1의 매트릭스 정보 생성부(105))의 기능에 활용되도록 할 수 있다.
- [0140] 일 실시예에 따르면, 상기 매트릭스 보정 결정부(500)는 상기 가중치 보정부(501)의 기능이 완료된 상태에서, 상기 기 저장된 시뮬레이션 알고리즘(501a)을 통해 상기 가중치가 보정된 정책 매트릭스에 기반한 접근 정책 시뮬레이션을 수행하여, 상기 접근 정책 시뮬레이션의 결과가 상기 보안 위험 상태로 도출되는 경우, 상기 가중치가 보정된 정책 매트릭스에 대응되는 보안 정책 정보의 정책을 비정상 정책으로 판단하여, 상기 비정상 정책으로 판단된 보안 정책 정보를 정상 정책의 보안 정책 정보로 보정할 수 있다.
- [0141] 상기와 관련하여, 상기 매트릭스 보정 결정부(500)는 상기 가중치 보정부(501)의 기능이 완료됨에 따라 가중치가 보정된 정책 매트릭스에 대한 접근 정책 시뮬레이션의 결과가 재차 보안 위험 상태로 도출 시, 상기 가중치가 보정된 정책 매트릭스에 대응되는 보안 정책 정보의 정책을 비정상 정책으로 판단할 수 있다. 이 때, 상기 매트릭스 보정 결정부(500)는 상기 가중치가 보정된 정책 매트릭스에 대응되는 보안 정책 정보의 정책을 비정상 정책으로 판단 시, 상기 보안 정책 정보에 기반한 보안 내용에 대한 보정을 시작할 수 있다.
- [0142] 예를 들어, 상기 매트릭스 보정 결정부(500)는 상기 제1 사용자 계정의 제2 신뢰 등급이 1등급임에 따라 제2 중요도 등급이 1등급으로 설정된 제1 자원 정보에 접근 가능하도록 보안 정책이 설정된 정책 매트릭스(가중치가 보정된 정책 매트릭스)에 대응되는 보안 정책 정보의 정책이 비정상 정책으로 판단되는 경우, 상기 보안 정책 정보의 정책을 상기 제1 사용자 계정의 제2 신뢰 등급 및 제3 신뢰 등급이 1등급임에 따라 제2 중요도 등급이 2등급으로 설정된 제1 자원 정보에 접근 가능하도록 보안 내용을 조정하여, 정상 정책의 보안 정책 정보로 보정할 수 있다.
- [0143] 도 6은 본 발명의 일 실시 예에 따른 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템의 정보 접근 관리부를 설명하기 위한 블록도이다.
- [0144] 도 6을 참조하면, 하나 이상의 프로세서 및 상기 프로세서에서 수행 가능한 명령들을 저장하는 하나 이상의 메모리를 포함하는 컴퓨팅 장치로 구현되는 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근

관리 시스템(예: 도 1의 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템(100))(이하, 접속 및 접근 관리 시스템으로 칭함)은 정보 접근 관리부(600)(예: 도 1의 정보 접근 관리부(107))를 포함할 수 있다.

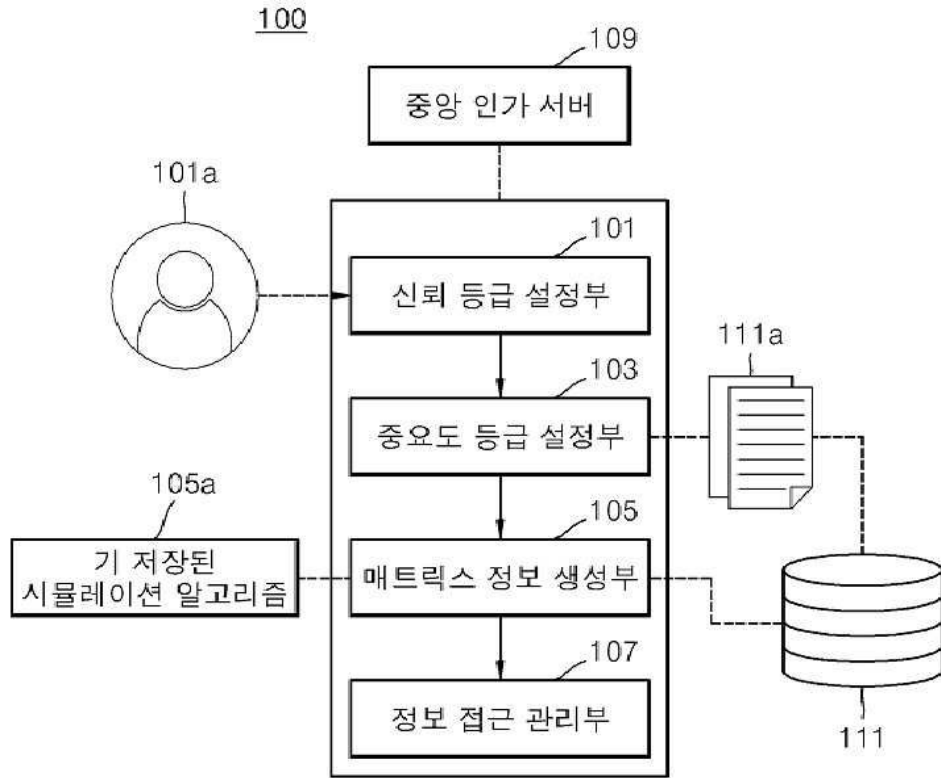
- [0145] 일 실시예에 따르면, 상기 정보 접근 관리부(600)는 접근 정책 매트릭스 정보(601a)의 생성이 완료되면, 상기 접근 정책 매트릭스 정보(601a)를 상기 중앙 인가 서버(601b)에 즉시 반영하여, 상기 반영된 접근 정책 매트릭스 정보(601a)에 기반해 상기 복수 개의 자원 정보 중 적어도 하나에 접근하는 상기 제1 사용자 계정(603a)의 접근 여부를 관리할 수 있다.
- [0146] 일 실시예에 따르면, 상기 정보 접근 관리부(600)는 상술한 기능을 수행하기 위한 세부 구성으로, 정책 매트릭스 서버 반영부(601) 및 모니터링 접근 제어부(603)를 포함할 수 있다.
- [0147] 일 실시예에 따르면, 상기 정책 매트릭스 서버 반영부(601)는 상기 접근 정책 매트릭스 정보(601a)의 생성이 완료되면, 상기 접근 정책 매트릭스 정보(601a)를 상기 중앙 인가 서버(601b)에 즉시 반영할 수 있다.
- [0148] 일 실시예에 따르면, 상기 모니터링 접근 제어부(603)는 상기 정책 매트릭스 서버 반영부(601)의 기능 수행이 완료되면, 상기 반영된 접근 정책 매트릭스 정보(601a)에 기반해 상기 복수 개의 자원 정보 중 적어도 하나에 접근하는 상기 제1 사용자 계정(603a)의 접근 여부를 관리할 수 있다.
- [0149] 상기와 관련하여, 상기 모니터링 접근 제어부(603)는 상기 중앙 인가 서버(601b)에 접근 정책 매트릭스 정보(601a)가 반영되는 경우, 상기 제1 사용자 계정(603a)이 복수 개의 자원 정보 중 하나에 접근 시, 상기 제1 사용자 계정(603a)이 자원 정보에 접근 가능한 지 여부를 상기 반영된 접근 정책 매트릭스 정보(601a)에 기반한 보안 정책을 기준으로 판단할 수 있다.
- [0150] 이에 따라, 본원발명은 중앙 인가 서버(601b)에 상기 접근 정책 매트릭스 정보(601a)를 반영함으로써, 추가 네트워크 요소를 소비하지 않고 복수 개의 자원 정보에 대한 사용자 계정의 접근 여부를 관리할 수 있다.
- [0151] 도 7은 본 발명의 일 실시 예에 따른 컴퓨팅 장치의 내부 구성의 일 예를 설명하기 위한 도면이다.
- [0152] 도 7은 본 발명의 일 실시 예에 따른 컴퓨팅 장치의 내부 구성의 일 예를 도시하였으며, 이하의 설명에 있어서, 상술한 도 1 내지 6에 대한 설명과 중복되는 불필요한 실시 예에 대한 설명은 생략하기로 한다.
- [0153] 도 7에 도시한 바와 같이, 컴퓨팅 장치(10000)은 적어도 하나의 프로세서(processor)(11100), 메모리(memory)(11200), 주변장치 인터페이스(peripheral interface)(11300), 입/출력 서브시스템(I/O subsystem)(11400), 전력 회로(11500) 및 통신 회로(11600)를 적어도 포함할 수 있다. 이때, 컴퓨팅 장치(10000)은 측각 인터페이스 장치에 연결된 유저 단말기(A) 혹은 전술한 컴퓨팅 장치(B)에 해당될 수 있다.
- [0154] 메모리(11200)는, 일례로 고속 랜덤 액세스 메모리(high-speed random access memory), 자기 디스크, 에스램(SRAM), 디램(DRAM), 롬(ROM), 플래시 메모리 또는 비휘발성 메모리를 포함할 수 있다. 메모리(11200)는 컴퓨팅 장치(10000)의 동작에 필요한 소프트웨어 모듈, 명령어 집합 또는 그밖에 다양한 데이터를 포함할 수 있다.
- [0155] 이때, 프로세서(11100)나 주변장치 인터페이스(11300) 등의 다른 컴포넌트에서 메모리(11200)에 액세스하는 것은 프로세서(11100)에 의해 제어될 수 있다.
- [0156] 주변장치 인터페이스(11300)는 컴퓨팅 장치(10000)의 입력 및/또는 출력 주변장치를 프로세서(11100) 및 메모리(11200)에 결합시킬 수 있다. 프로세서(11100)는 메모리(11200)에 저장된 소프트웨어 모듈 또는 명령어 집합을 실행하여 컴퓨팅 장치(10000)을 위한 다양한 기능을 수행하고 데이터를 처리할 수 있다.
- [0157] 입/출력 서브시스템(11400)은 다양한 입/출력 주변장치들을 주변장치 인터페이스(11300)에 결합시킬 수 있다. 예를 들어, 입/출력 서브시스템(11400)은 모니터나 키보드, 마우스, 프린터 또는 필요에 따라 터치스크린이나 센서 등의 주변장치를 주변장치 인터페이스(11300)에 결합시키기 위한 컨트롤러를 포함할 수 있다. 다른 측면에 따르면, 입/출력 주변장치들은 입/출력 서브시스템(11400)을 거치지 않고 주변장치 인터페이스(11300)에 결합될 수도 있다.
- [0158] 전력 회로(11500)는 단말기의 컴포넌트의 전부 또는 일부로 전력을 공급할 수 있다. 예를 들어 전력 회로(11500)는 전력 관리 시스템, 배터리나 교류(AC) 등과 같은 하나 이상의 전원, 충전 시스템, 전력 실패 감지 회로(power failure detection circuit), 전력 변환기나 인버터, 전력 상태 표시자 또는 전력 생성, 관리, 분배를 위한 임의의 다른 컴포넌트들을 포함할 수 있다.

- [0159] 통신 회로(11600)는 적어도 하나의 외부 포트를 이용하여 다른 컴퓨팅 장치와 통신을 가능하게 할 수 있다.
- [0160] 또는 상술한 바와 같이 필요에 따라 통신 회로(11600)는 RF 회로를 포함하여 전자기 신호(electromagnetic signal)라고도 알려진 RF 신호를 송수신함으로써, 다른 컴퓨팅 장치와 통신을 가능하게 할 수도 있다.
- [0161] 이러한 도 7의 실시 예는, 컴퓨팅 장치(10000)의 일례일 뿐이고, 컴퓨팅 장치(11000)은 도 7에 도시된 일부 컴포넌트가 생략되거나, 도 7에 도시되지 않은 추가의 컴포넌트를 더 구비하거나, 2개 이상의 컴포넌트를 결합시키는 구성 또는 배치를 가질 수 있다. 예를 들어, 모바일 환경의 통신 단말을 위한 컴퓨팅 장치는 도 7에 도시된 컴포넌트들 외에도, 터치스크린이나 센서 등을 더 포함할 수도 있으며, 통신 회로(1160)에 다양한 통신방식(WiFi, 3G, LTE, Bluetooth, NFC, Zigbee 등)의 RF 통신을 위한 회로가 포함될 수도 있다. 컴퓨팅 장치(1000)에 포함 가능한 컴포넌트들은 하나 이상의 신호 처리 또는 어플리케이션에 특화된 집적 회로를 포함하는 하드웨어, 소프트웨어, 또는 하드웨어 및 소프트웨어 양자의 조합으로 구현될 수 있다.
- [0162] 본 발명의 실시 예에 따른 방법들은 다양한 컴퓨팅 장치를 통하여 수행될 수 있는 프로그램 명령(instruction) 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 특히, 본 실시 예에 따른 프로그램은 PC 기반의 프로그램 또는 모바일 단말 전용의 어플리케이션으로 구성될 수 있다. 본 발명이 적용되는 어플리케이션은 파일 배포 시스템이 제공하는 파일을 통해 이용자 단말에 설치될 수 있다. 일 예로, 파일 배포 시스템은 이용자 단말 이기의 요청에 따라 상기 파일을 전송하는 파일 전송부(미도시)를 포함할 수 있다.
- [0163] 이상에서 설명된 장치는 하드웨어 구성요소, 소프트웨어 구성요소, 및/또는 하드웨어 구성요소 및 소프트웨어 구성요소의 조합으로 구현될 수 있다. 예를 들어, 실시 예들에서 설명된 장치 및 구성요소는, 예를 들어, 프로세서, 콘트롤러, ALU(arithmetic logic unit), 디지털 신호 프로세서(digital signal processor), 마이크로컴퓨터, FPGA(field programmable gate array), PLU(programmable logic unit), 마이크로프로세서, 또는 명령(instruction)을 실행하고 응답할 수 있는 다른 어떠한 장치와 같이, 하나 이상의 범용 컴퓨터 또는 특수 목적 컴퓨터를 이용하여 구현될 수 있다. 처리 장치는 운영 체제(OS) 및 상기 운영 체제상에서 수행되는 하나 이상의 소프트웨어 어플리케이션을 수행할 수 있다. 또한, 처리 장치는 소프트웨어의 실행에 응답하여, 데이터를 접근, 저장, 조작, 처리 및 생성할 수도 있다. 이해의 편의를 위하여, 처리 장치는 하나가 사용되는 것으로 설명된 경우도 있지만, 해당 기술 분야에서 통상의 지식을 가진 자는, 처리 장치가 복수 개의 처리 요소(processing element) 및/또는 복수 유형의 처리 요소를 포함할 수 있음을 알 수 있다. 예를 들어, 처리 장치는 복수 개의 프로세서 또는 하나의 프로세서 및 하나의 콘트롤러를 포함할 수 있다. 또한, 병렬 프로세서(parallel processor)와 같은, 다른 처리 구성(processing configuration)도 가능하다.
- [0164] 소프트웨어는 컴퓨터 프로그램(computer program), 코드(code), 명령(instruction), 또는 이들 중 하나 이상의 조합을 포함할 수 있으며, 원하는 대로 동작하도록 처리 장치를 구성하거나 독립적으로 또는 결합적으로(collectively) 처리 장치를 명령할 수 있다. 소프트웨어 및/또는 데이터는, 처리 장치에 의하여 해석되거나 처리 장치에 명령 또는 데이터를 제공하기 위하여, 어떤 유형의 기계, 구성요소(component), 물리적 장치, 가상장치(virtual equipment), 컴퓨터 저장 매체 또는 장치에 영구적으로, 또는 일시적으로 구체화(embodiment)될 수 있다. 소프트웨어는 네트워크로 연결된 컴퓨팅 장치상에 분산되어서, 분산된 방법으로 저장되거나 실행될 수도 있다. 소프트웨어 및 데이터는 하나 이상의 컴퓨터 판독 가능 기록 매체에 저장될 수 있다.
- [0165] 실시 예에 따른 방법은 다양한 컴퓨터 수단을 통하여 수행될 수 있는 프로그램 명령 형태로 구현되어 컴퓨터 판독 가능 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능 매체는 프로그램 명령, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다. 상기 매체에 기록되는 프로그램 명령은 실시 예를 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 당업자에게 공지되어 사용 가능한 것일 수도 있다. 컴퓨터 판독 가능 기록 매체의 예에는 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체(magnetic media), CD-ROM, DVD와 같은 광 기록 매체(optical media), 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 롬(ROM), 램(RAM), 플래시 메모리 등과 같은 프로그램 명령을 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다. 프로그램 명령의 예에는 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드를 포함한다. 상기된 하드웨어 장치는 실시예의 동작을 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.
- [0166] 이상과 같이 실시 예들이 비록 한정된 실시 예와 도면에 의해 설명되었으나, 해당 기술 분야에서 통상의 지식을 가진 자라면 상기의 기재로부터 다양한 수정 및 변형이 가능하다. 예를 들어, 설명된 기술들이 설명된 방법과 다른 순서로 수행되거나, 및/또는 설명된 시스템, 구조, 장치, 회로 등의 구성요소들이 설명된 방법과 다른 형

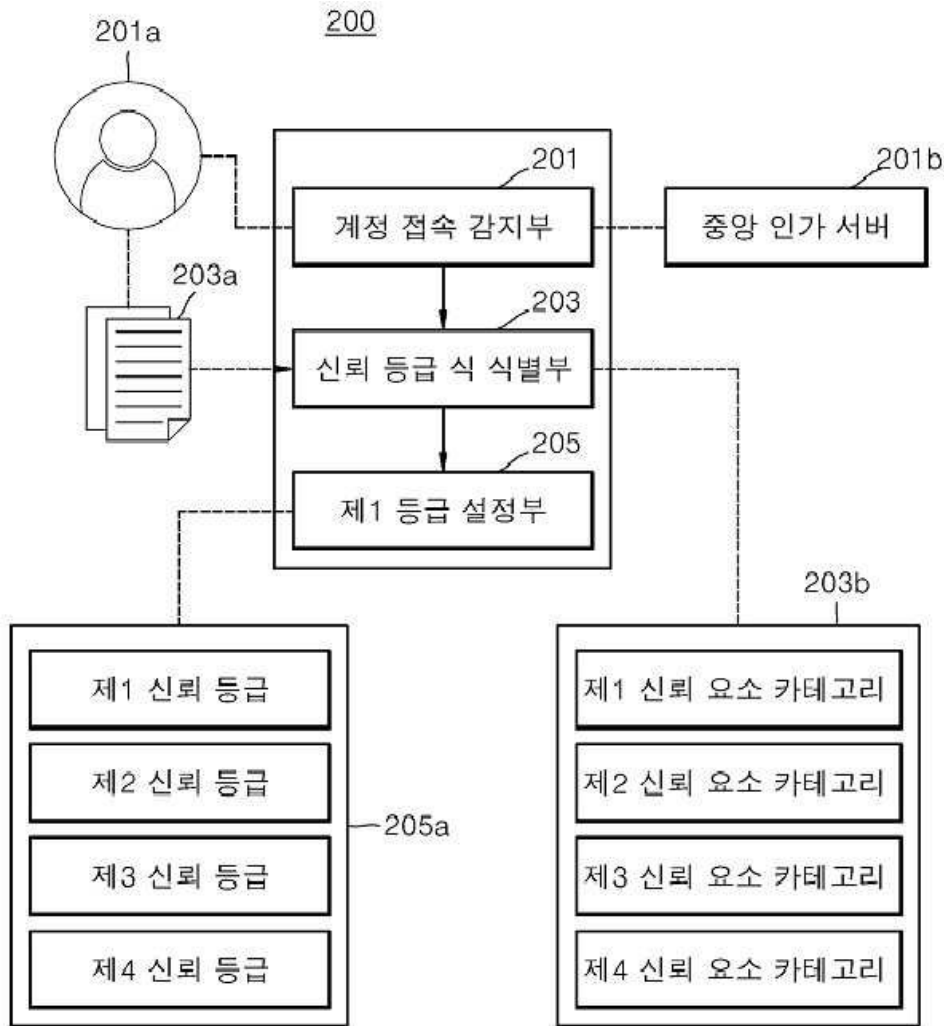
태로 결합 또는 조합되거나, 다른 구성요소 또는 균등물에 의하여 대치되거나 치환되더라도 적절한 결과가 달성될 수 있다. 그러므로, 다른 구현들, 다른 실시 예들 및 특허청구범위와 균등한 것들도 후술하는 특허청구범위의 범위에 속한다.

도면

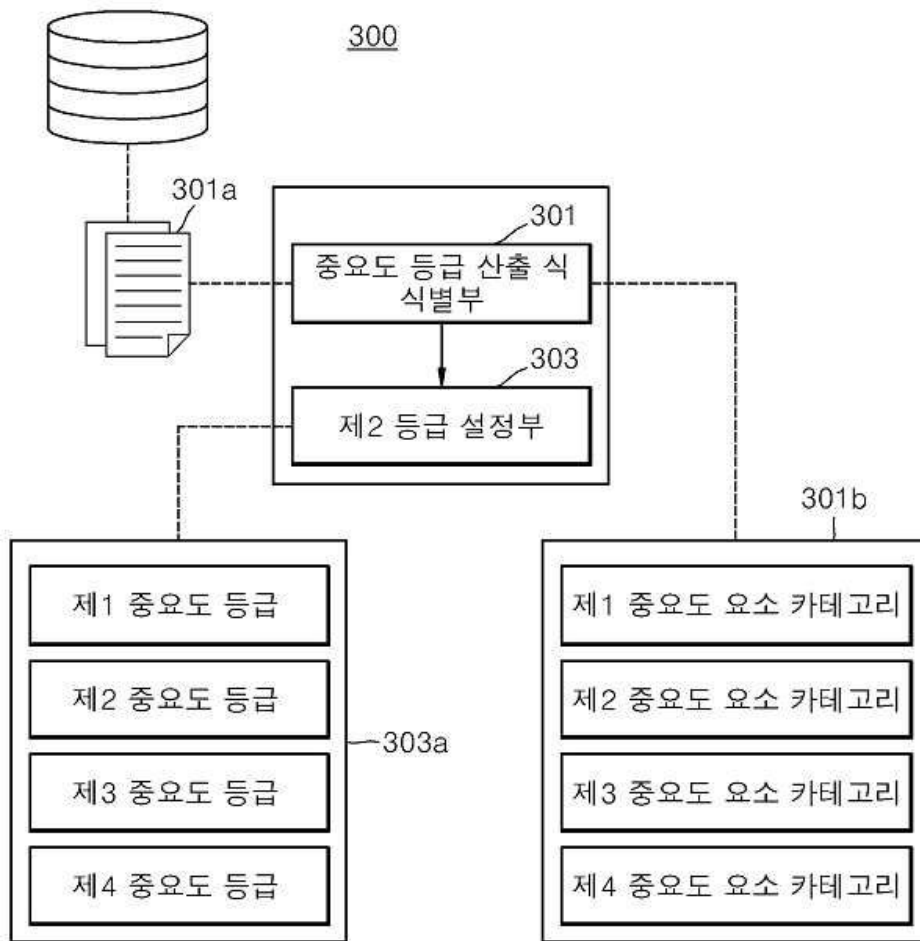
도면1



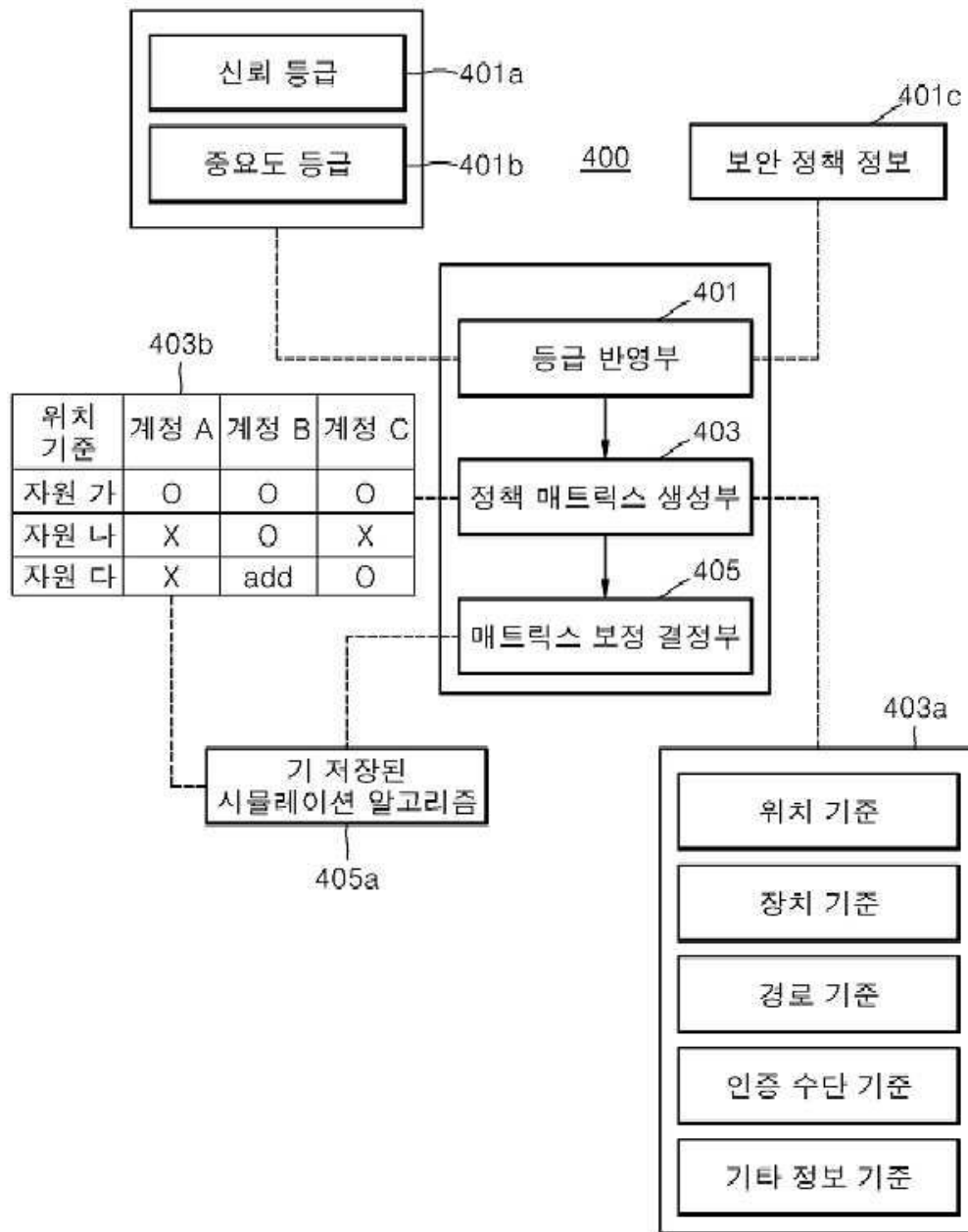
도면2



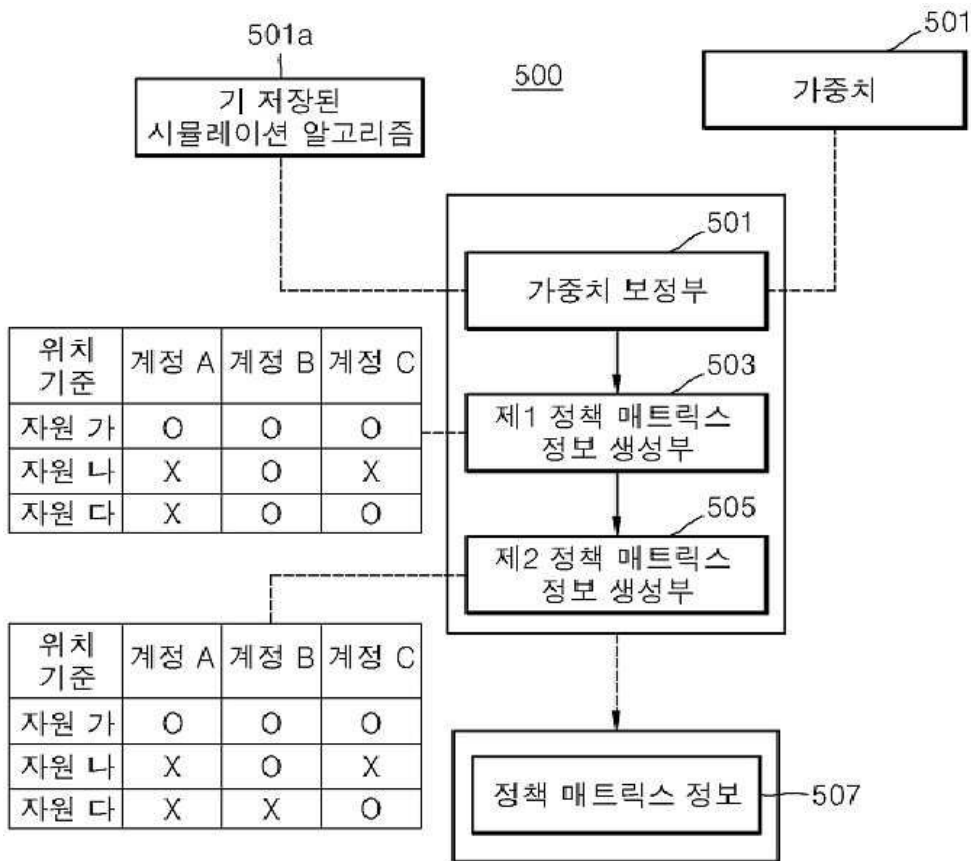
도면3



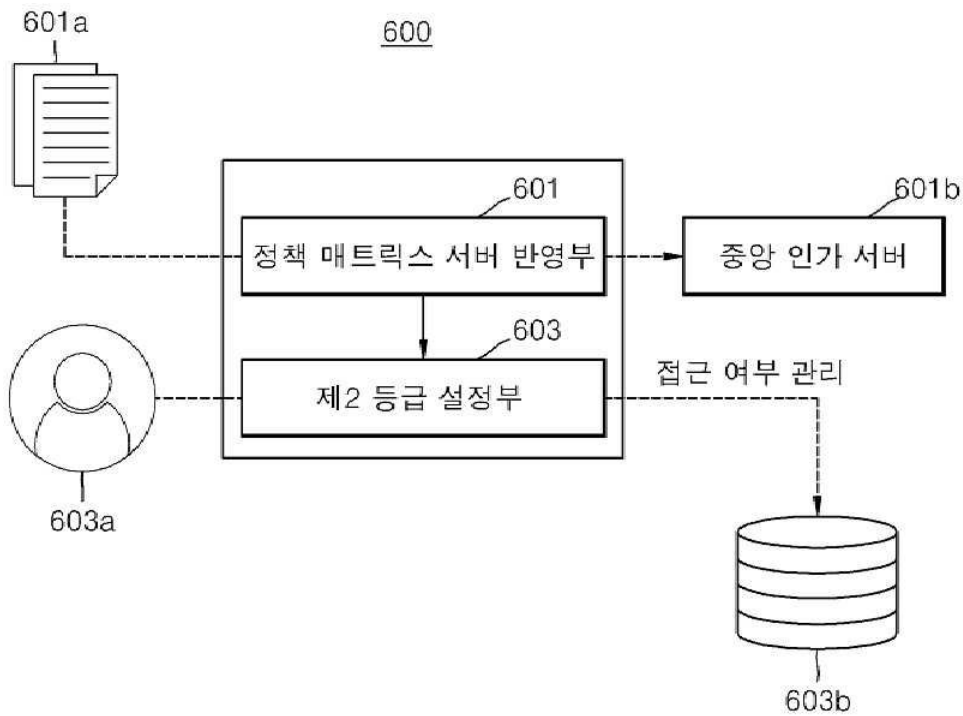
도면4



도면5

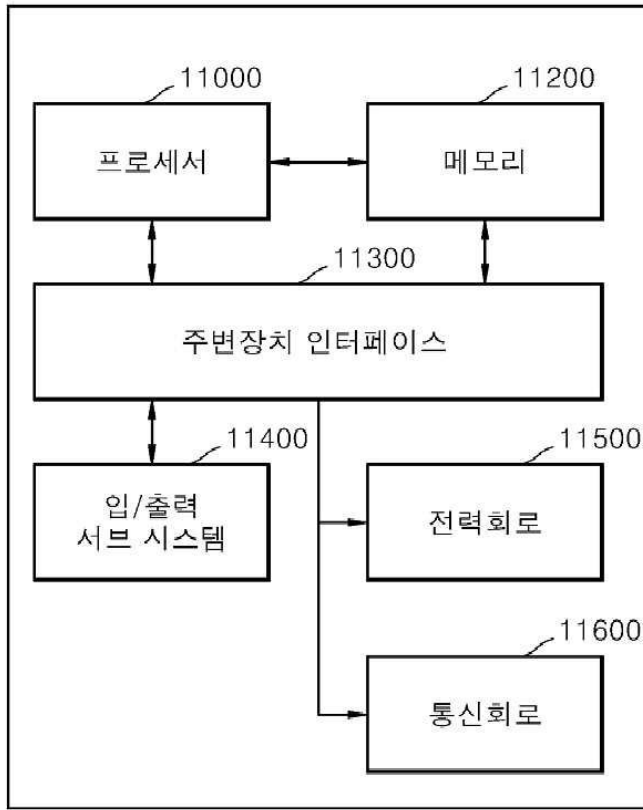


도면6



도면7

10000



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 4

【변경전】

제3항에 있어서,

상기 중요도 등급 설정부는,

상기 신뢰 등급 설정부의 기능이 수행되는 동안 상기 중요도 확인 프로세스를 시작하여, 상기 기업에서 관리하는 복수 개의 자원 정보에 포함된 복수 개의 자원 카테고리를 식별해 상기 복수 개의 자원 카테고리 및 대응되는 기 설정된 중요도 요소 카테고리 각각에 설정되어 있는 복수 개의 중요도 등급 산출 식을 식별하는 중요도 등급 산출 식 식별부; 및

상기 중요도 등급 산출 식 식별부의 기능 수행의 완료되면, 기 설정된 중요도 요소 카테고리 각각에 설정되어 있는 복수 개의 중요도 등급 산출 식 중 상기 식별된 자원 카테고리에 포함된 자원 요소 정보가 반영되는 적어도 하나의 중요도 등급 산출 식을 식별하여, 상기 식별된 적어도 하나의 중요도 등급 산출 식을 통해 상기 기 설정된 중요도 요소 카테고리 별로 중요도 등급을 산출해 상기 복수 개의 자원 정보 각각에 대해 중요도 등급의 설정을 완료하는 제2 등급 설정부;를 포함하는 것을 특징으로 하는 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템.

【변경후】

제3항에 있어서,

상기 중요도 등급 설정부는,

상기 신뢰 등급 설정부의 기능이 수행되는 동안 상기 중요도 확인 프로세스를 시작하여, 상기 기업에서 관리하는 복수 개의 자원 정보에 포함된 복수 개의 자원 카테고리를 식별해 상기 복수 개의 자원 카테고리 및 대응되는 기 설정된 중요도 요소 카테고리 각각에 설정되어 있는 복수 개의 중요도 등급 산출 식을 식별하는 중요도 등급 산출 식 식별부; 및

상기 중요도 등급 산출 식 식별부의 기능 수행이 완료되면, 기 설정된 중요도 요소 카테고리 각각에 설정되어 있는 복수 개의 중요도 등급 산출 식 중 상기 식별된 자원 카테고리에 포함된 자원 요소 정보가 반영되는 적어도 하나의 중요도 등급 산출 식을 식별하여, 상기 식별된 적어도 하나의 중요도 등급 산출 식을 통해 상기 기 설정된 중요도 요소 카테고리 별로 중요도 등급을 산출해 상기 복수 개의 자원 정보 각각에 대해 중요도 등급의 설정을 완료하는 제2 등급 설정부;를 포함하는 것을 특징으로 하는 중앙 인가 서버에 대한 사용자의 접속 여부를 확인 및 사내 자원 접근 관리 시스템.