(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2021년03월31일
(11) 등록번호 10-2234514
(24) 등록일자 2021년03월25일

(51) 국제특허분류(Int. Cl.)
G06F 21/55 (2013.01)
(52) CPC특허분류
G06F 21/55 (2013.01)
(21) 출원번호 10-2020-0028286(분할)
(22) 출원일자 2020년03월06일
심사청구일자 2020년04월14일
(65) 공개번호 10-2020-0134143
(43) 공개일자 2020년12월01일
(62) 원출원 특허 10-2019-0059537
원출원일자 2019년05월21일
심사청구일자 2019년05월21일
(56) 선행기술조사문헌
KR101597935 B1*
KR1020180044693 A*
KR1020180076732 A*
KR1020190043923 A*
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
주식회사 제이슨
서울특별시 마포구 양화로 61 ,8층(서교동,두암빌딩)
(72) 발명자
김경화
경기도 김포시 김포한강11로 275, 304동 2302호 (운양동, 풍경마을 한강신도시 롯데캐슬)
(74) 대리인
특허법인비엘티

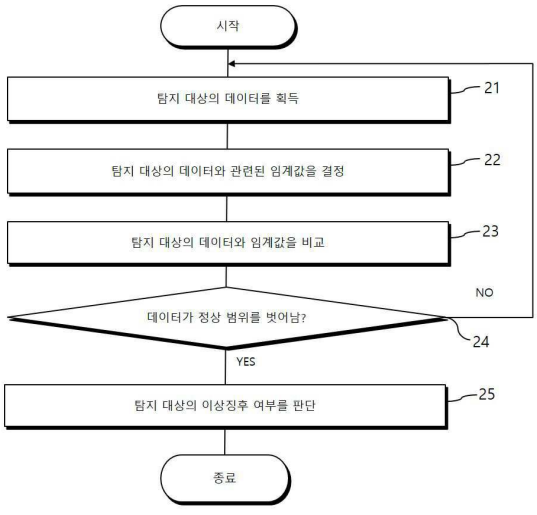
전체 청구항 수 : 총 7 항 심사관 : 정성훈

(54) 발명의 명칭 **인공지능형 통합 IT관제 방법 및 시스템**

(57) 요 약

본 발명의 다양한 실시 예는 통합 관제 방법에 관한 것이다. 본 발명의 일 실시예에 따른 통합 관제 방법은, 탐지 대상의 데이터를 획득하는 단계; 상기 탐지 대상의 상기 데이터와 관련된 임계값을 결정하는 단계; 상기 탐지 대상의 상기 데이터와 상기 임계값을 비교하는 단계; 및 상기 비교 결과 상기 탐지 대상의 상기 데이터가 정상 범위를 벗어날 경우, 상기 탐지 대상의 이상징후 여부를 판단하는 단계를 포함하고, 상기 임계값을 결정하는 단계는 상기 탐지 대상의 상기 데이터를 획득할 때마다 반복적으로 수행되고, 상기 임계값을 결정하는 단계는, 상기 데이터를 획득한 시점 이전부터 미리 설정한 기준 기간 동안 상기 탐지 대상의 과거 데이터를 추출하는 단계; 상기 과거 데이터에서 기준 값을 산출하는 단계; 및 상기 기준 값과 지정된 가중치에 기반하여 임계값을 결정하는 단계를 포함할 수 있다. 다른 실시 예들도 가능할 수 있다.

대 표 도 - 도2



명 세 서

청구범위

청구항 1

인공지능형 통합 IT관제 방법에 있어서,

복수의 탐지대상의 데이터를 획득하는, 데이터 획득 단계;

제1 탐지대상의 데이터와 관련된 제1 임계값을 결정하는, 제1 임계값 결정 단계;

상기 제1 탐지대상의 데이터와 상기 제1 임계값을 비교하되, 상기 비교 결과 상기 제1 탐지대상의 데이터가 상기 제1 임계값을 벗어나면 상기 제1 탐지대상에 대하여 이상징후가 발생한 것으로 판단하는, 제1 탐지대상 이상징후 판단 단계;

획득한 복수의 탐지대상의 데이터에 기반하여 복수의 탐지대상 간의 유사도를 결정하는 단계;

상기 제1 탐지대상에 대하여 이상징후가 발생한 것으로 판단된 경우, 상기 제1 탐지대상과 유사도가 높은 제2 탐지대상을 추출하는 단계; 및

상기 제2 탐지대상의 이상징후 발생 여부를 판단하는, 제2 탐지대상 이상징후 판단 단계를 포함하고,

상기 제1 임계값 결정 단계는,

상기 제1 탐지대상 데이터의 기준값과 상기 제1 탐지대상의 특성에 따라 지정된 제1 가중치에 기반하여 제1 임계값을 결정하는 것을 특징으로 하는, 통합 관제 방법.

청구항 2

제1 항에 있어서,

적어도 하나의 파라미터에 기반하여 복수의 탐지대상의 데이터를 군집화하는 단계를 더 포함하고,

상기 제1 탐지대상 이상징후 판단 단계는,

상기 제1 탐지대상의 데이터를 상기 제1 탐지대상이 속한 군집과 비교하되, 상기 제1 탐지대상의 데이터가 상기 군집으로부터 상기 제1 임계값을 벗어나면 상기 제1 탐지대상에 대하여 이상징후가 발생한 것으로 판단하는 것인, 통합 관제 방법.

청구항 3

삭제

청구항 4

제1 항에 있어서,

카메라의 촬영 영상, 출입 기록 또는 서로 공유된 동일한 파일의 개수 중 적어도 하나에 기반하여 복수의 탐지대상 간의 관계도를 결정하는 단계;

상기 제1 탐지대상에 대하여 이상징후가 발생한 것으로 판단된 경우, 상기 제1 탐지대상과 관계도가 높은 제2 탐지대상을 추출하는 단계; 및

상기 제2 탐지대상의 이상징후 발생 여부를 판단하는, 제2 탐지대상 이상징후 판단 단계를 더 포함하는, 통합 관제 방법.

청구항 5

제4 항에 있어서,

상기 제2 탐지대상 이상징후 판단 단계는,

상기 제2 탐지대상의 데이터와 관련된 제2 임계값을 결정하는 단계; 및

상기 제2 탐지대상의 데이터와 상기 제2 임계값을 비교하되, 상기 비교 결과 상기 제2 탐지대상의 데이터가 상기 제2 임계값을 벗어나면 상기 제2 탐지대상에 대하여 이상징후가 발생한 것으로 판단하는 단계를 포함하는, 통합 관제 방법.

청구항 6

제5 항에 있어서,

상기 제2 탐지대상의 데이터는, 상기 제1 임계값을 벗어난 상기 제1 탐지대상의 데이터 유형과 동일한 유형의 데이터인 것을 특징으로 하는, 통합 관제 방법.

청구항 7

하드웨어인 컴퓨터와 결합되어, 제1 항 내지 제2 항, 제4 항 중 어느 한 항의 방법을 실행시키기 위해 기록매체에 저장된, 통합 관제 프로그램.

청구항 8

인공지능형 통합 IT관제 시스템에 있어서,

탐지대상의 이상징후를 탐지 및 분석하는 메인 서버를 포함하고,

상기 메인 서버가 복수의 탐지대상의 데이터를 획득하고,

상기 메인 서버가 제1 탐지대상의 데이터와 관련된 제1 임계값을 결정하고,

상기 메인 서버가 상기 제1 탐지대상의 데이터와 상기 제1 임계값을 비교하되, 상기 비교 결과 상기 제1 탐지대상의 데이터가 상기 제1 임계값을 벗어나면 상기 제1 탐지대상에 대하여 이상징후가 발생한 것으로 판단하고,

상기 메인 서버가 카메라의 촬영 영상, 출입 기록, 서로 공유된 동일한 파일의 개수, 네트워크 트래픽, 메일 수발신 내용 및 메신저 수발신 내용 중 적어도 하나에 기반하여 복수의 탐지대상 간의 관계도를 결정하고,

상기 메인 서버가 상기 제1 탐지대상에 대하여 이상징후가 발생한 것으로 판단된 경우, 상기 제1 탐지대상과 관계도가 높은 제2 탐지대상을 추출하고,

상기 메인 서버가 상기 제2 탐지대상의 이상징후 발생 여부를 판단하고,

상기 제1 임계값은,

상기 제1 탐지대상 데이터의 기준값과 상기 제1 탐지대상의 특성에 따라 지정된 제1 가중치에 기반하여 제1 임계값을 결정되는 것을 특징으로 하는, 통합 관제 시스템.

청구항 9

삭제

청구항 10

삭제

발명의 설명

기 술 분 야

[0001] 본 발명은 통합 관제 방법 및 시스템에 관한 것으로, 보다 자세하게는 자동 가변 임계치를 이용하여 지능형 정밀 탐지를 구현하는 방법 및 시스템에 관한 것이다.

배 경 기 술

[0002] 시스템을 운영하는 기업들은 대부분 시스템을 모니터링하거나 Alerting을 받을 수 있는 다양한 형태의 소프트웨어를 사용하고 있다. 이러한 소프트웨어들은 시스템이나 데이터베이스의 특정 항목에 대하여 별도로 저장된 임계치를 통해 임계치 초과 여부를 검사하고, 임계치 초과 시 사용자에게 해당 사실을 Alerting 해주는 기능을 수행하고 있으나 현실적으로 많은 운영상의 문제점들을 가지고 있어 실질적인 효과를 기대하기 어려운 것이 사실이다. 특히, 1차원적인 획일적인 임계치 설정은 시스템이나 데이터베이스가 가지고 있는 다양한 운영상의 특성(Peak-Time, 결산, 마감작업 등이 몰리는 현상)을 반영할 수 없고, 탐지 기준인 임계치를 단순한 숫자만으로 활용하여 장애 또는 사고를 판단하는 것은 부정확한 탐지를 발생시킬 수 있고, 모든 탐지 대상에 대해 획일화된 임계치를 설정할 경우 탐지 대상 별 특성을 반영할 수 없어서 다량의 이상징후 이벤트 중 다수가 노이즈인 문제점이 있었다. 또한 설사 이상징후 검출에 따라 보안 사고 등이 발생한 탐지 대상을 발견하더라도 탐지 대상과 유사한 보안 사고를 일으킨 대상들 또는 공모자들을 함께 발견하기 어려운 문제점이 있었다.

발명의 내용

해결하려는 과제

[0003] 본 발명은 상기와 같은 문제점을 해결하기 위해 안출된 것으로서, 자동 가변 임계값을 이용하여 탐지 대상의 상태를 정확하게 반영하는 방법 및 시스템을 제공하는 데 목적이 있다.

[0004] 또한, 본 발명은 탐지 대상 별 개인화된 임계값을 설정함으로써 탐지대상의 이상징후를 정확하게 검출하는 방법 및 시스템을 제공하는 데 목적이 있다.

[0005] 또한, 본 발명은 복수의 군집을 이용하여 탐지 대상의 이상징후를 정확하게 검출하는 방법 및 시스템을 제공하는 데 목적이 있다.

[0006] 또한, 본 발명은 탐지 대상의 유사도 또는 관계도를 이용하여 동일한 사고를 발생시킨 모든 탐지 대상들을 검출하는 방법 및 시스템을 제공하는 데 목적이 있다.

[0007] 본 발명이 해결하고자 하는 과제들은 이상에서 언급된 과제로 제한되지 않으며, 언급되지 않은 또 다른 과제들은 아래의 기재로부터 통상의 기술자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0008] 본 발명의 일 실시예에 따른 통합 관제 방법은, 탐지 대상의 데이터를 획득하는 단계; 상기 탐지 대상의 상기 데이터와 관련된 임계값을 결정하는 단계; 상기 탐지 대상의 상기 데이터와 상기 임계값을 비교하는 단계; 및 상기 비교 결과 상기 탐지 대상의 상기 데이터가 정상 범위를 벗어날 경우, 상기 탐지 대상의 이상징후 여부를 판단하는 단계를 포함하고, 상기 임계값을 결정하는 단계는 상기 탐지 대상의 상기 데이터를 획득할 때마다 반복적으로 수행되고, 상기 임계값을 결정하는 단계는, 상기 데이터를 획득한 시점 이전부터 미리 설정한 기준 기간 동안 상기 탐지 대상의 과거 데이터를 추출하는 단계; 상기 과거 데이터에서 기준 값을 산출하는 단계; 및 상기 기준 값과 지정된 가중치에 기반하여 임계값을 결정하는 단계를 포함할 수 있다.

[0009] 본 발명의 일 실시예에 따른 통합 관제 시스템은, 탐지 대상의 이상징후를 탐지 및 분석하는 메인 서버를 포함하고, 상기 메인 서버가 탐지 대상의 데이터를 획득하고, 상기 메인 서버가 상기 탐지 대상의 상기 데이터와 관련된 임계값을 결정하고, 상기 메인 서버가 상기 탐지 대상의 상기 데이터와 상기 임계값을 비교하고, 상기 메인 서버가 상기 비교 결과 상기 탐지 대상의 상기 데이터가 정상 범위를 벗어날 경우, 상기 탐지 대상의 이상징후 여부를 판단하고, 상기 메인 서버는 상기 탐지 대상의 상기 데이터를 획득할 때마다 상기 임계값을 반복적으로 결정하고, 상기 메인 서버는 상기 데이터를 획득한 시점 이전부터 미리 설정한 기준 기간 동안 상기 탐지 대상의 과거 데이터를 추출하고, 상기 과거 데이터에서 기준 값을 산출하고, 상기 기준 값과 지정된 가중치에 기반하여 임계값을 결정함으로써 상기 임계값을 결정할 수 있다.

발명의 효과

[0010] 상기와 같은 본 발명에 따르면, 아래와 같은 다양한 효과들을 가진다.

[0011] 본 발명은 자동 가변 임계값을 이용하여 탐지 대상의 상태를 정확하게 반영할 수 있다.

[0012] 또한, 본 발명은 탐지 대상 별 개인화된 임계값을 설정함으로써 탐지대상의 이상징후를 정확하게 검출할 수 있

다.

[0013] 또한, 본 발명은 복수의 군집을 이용하여 탐지 대상의 이상징후를 정확하게 검출할 수 있다.

[0014] 또한, 본 발명은 탐지 대상의 유사도 또는 관계도를 이용하여 동일한 사고를 발생시킨 모든 탐지 대상들을 검출할 수 있다.

도면의 간단한 설명

[0015] 도 1 은 본 발명의 통합 관제 시스템을 나타낸 블록도이다.

도 2는 본 발명의 일 실시 예에 따른 통합 관제 방법을 설명하기 위한 흐름도이다.

도 3은 본 발명의 일 실시 예에 따른 임계값을 결정하기 위한 방법을 설명하기 위한 흐름도이다.

도 4는 본 발명의 일 실시 예에 따른 탐지 대상의 상태를 판단하는 방법을 설명하기 위한 흐름도이다.

도 5는 본 발명의 일 실시 예에 따른 탐지 대상의 상태를 판단하는 방법을 설명하기 위한 예시도이다.

도 6은 본 발명의 일 실시 예에 따른 텍스트를 포함하는 로그 데이터에서 임계값을 결정하는 방법을 설명하기 위한 흐름도이다.

도 7은 본 발명의 일 실시 예에 따른 군집을 이용하여 이상징후를 판단하는 방법을 설명하기 위한 흐름도이다.

도 8은 본 발명의 일 실시 예에 따른 군집을 이용하여 이상징후를 판단하는 방법을 설명하기 위한 예시도이다.

도 9는 본 발명의 일 실시 예에 따른 유사도를 이용하여 탐지 대상의 이상징후를 판단하는 방법을 설명하기 위한 흐름도이다.

도 10은 본 발명의 일 실시 예에 따른 관계도를 이용하여 탐지 대상의 이상징후를 판단하는 방법을 설명하기 위한 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0016] 이하, 첨부된 도면을 참조하여 본 발명의 바람직한 실시예를 상세히 설명한다. 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 게시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 게시가 완전하도록 하고, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 참조 부호는 동일 구성 요소를 지칭한다.

[0017] 다른 정의가 없다면, 본 명세서에서 사용되는 모든 용어(기술 및 과학적 용어를 포함)는 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 공통적으로 이해될 수 있는 의미로 사용될 수 있을 것이다. 또 일반적으로 사용되는 사전에 정의되어 있는 용어들은 명백하게 특별히 정의되어 있지 않는 한 이상적으로 또는 과도하게 해석되지 않는다.

[0018] 본 명세서에서 사용된 용어는 실시예들을 설명하기 위한 것이며 본 발명을 제한하고자 하는 것은 아니다. 본 명세서에서, 단수형은 문구에서 특별히 언급하지 않는 한 복수형도 포함한다. 명세서에서 사용되는 "포함한다(comprises)" 및/또는 "포함하는(comprising)"은 언급된 구성요소 외에 하나 이상의 다른 구성요소의 존재 또는 추가를 배제하지 않는다.

[0020] 도 1 은 본 발명의 통합 관제 시스템을 나타낸 블록도이다.

[0022] 도 1을 참조하면, 본 발명의 일 실시 예에 따른 통합 관제 시스템(10)은 L4 Switch(50) 또는 부하 분산 포워더(300)을 통해 사내 시스템(20)을 모니터링할 수 있다. 또한 통합 관제 시스템(10)은 사내 시스템(20)에서 획득한 데이터를 통해 임직원의 업무 내용과 업무 변화를 모니터링할 수 있다.

[0023] 일 실시예에서, 사내 시스템(20)은 보안 시스템(30), 인프라 시스템(40) 및 업무 시스템(50)을 포함할 수 있다. 보안 시스템(30)은 내부 보안 시스템과 외부 보안 시스템을 포함할 수 있고, 내부 보안 시스템은 DLP(Data Loss Prevention), DRM(Digital Right Management), PC 보안, IAM(Identity and Access Management) 또는 개인정보 검출 시스템 등과 같은 내부의 정보유출을 방지하기 위한 보안솔루션들을 포함할 수 있고, 외부 보안 시스템은 방화벽, WAF(Web Application Firewall), VPN(Virtual Private Network), IPS(Intrusion Prevention System)

또는 nDLP(Data Loss Prevention) 등과 같은 내외부의 해킹공격을 방어하기 위한 보안솔루션들을 포함할 수 있다. 인프라 시스템은 서버 OS, 데이터베이스, 네트워크, WAS, 클라우드 등 기업 인프라 시스템들을 포함할 수 있다. 업무 시스템은 개인정보 처리시스템, 본인 인증, 시스템 접속 기록, 사내 인트라넷 시스템 등 기업 업무를 지원하는 시스템들을 포함할 수 있다.

[0024] 일 실시 예에서, 통합 관제 시스템(10)은 메인 서버(100), 탐지 서버(200), 부하 분산 포워더(300), 수집 서버(400), 검색 서버(500) 및 분석 서버(600)를 포함할 수 있다. 통합 관제 시스템(10)에 포함된 각 서버들은 네트워크를 통해 서로 통신할 수 있다. 여기서 네트워크는 무선 네트워크 및 유선 네트워크를 포함할 수 있다. 예를 들어, 상기 네트워크는 근거리 통신 네트워크(예: 블루투스, WiFi direct 또는 IrDA(infrared data association)) 또는 원거리 통신 네트워크(예: 셀룰러 네트워크, 인터넷, 또는 컴퓨터 네트워크(예: LAN 또는 WAN))일 수 있다.

[0025] 일 실시 예에서, 메인 서버(100), 탐지 서버(200), 부하 분산 포워더(300), 수집 서버(400), 검색 서버(500) 및 분석 서버(600)는 서로 연동될 수 있고, 각 서버에서 획득한 정보들은 수집 서버(400)에 갱신될 수 있다.

[0026] 일 실시 예에서, 부하 분산 포워더(300), 수집 서버(400), 검색 서버(500)는 따로 빅데이터 시스템으로 구분될 수 있다.

[0027] 일 실시 예에서, 부하 분산 포워더(300)는 사내 시스템(10)으로부터 로우 데이터(Raw data)를 수집할 수 있다. 예를 들어, 부하 분산 포워더(300)는 무제한 데이터를 수집할 수 있고, 이기종 데이터(IT infra, application, Net streem 등)를 수집할 수 있다. 부하 분산 포워더(300)의 데이터 수집 방식은 Agent 수집, FTP 전송, Syslog 전송, SNMP, Network Packet 수집 또는 DB 쿼리 전송 등을 포함할 수 있다.

[0028] 일 실시 예에서, 수집 서버(400)는 부하 분산 포워더(300)로부터 모든 데이터를 수신할 수 있고, 데이터 무결성을 보장할 수 있고, 장기간 아카이빙 기능을 가질 수 있고, 압축 기술을 이용하여 저장 공간을 절약할 수 있다. 수집 서버(400)는 복수의 서버들을 무제한으로 확장할 수 있고, 각 복수의 서버들은 데이터가 동기화되고 데이터들이 분산 저장될 수 있다.

[0029] 일 실시 예에서, 검색 서버(500)는 수집 서버(400)로부터 수신한 모든 데이터를 조회할 수 있다. 예를 들어, 검색 서버(500)는 빅데이터 쿼리를 통한 데이터 통합 조회 기능을 수행할 수 있다. 검색 서버(500)는 동일 데이터를 검색할 수 있고, 검색 부하를 분산할 수 있다.

[0030] 일 실시 예에서, 메인 서버(100)는 탐지 대상의 이상징후를 탐지, 분석 및 대응을 하기 위한 전반적인 동작들을 제어할 수 있다. 메인 서버(100)는 탐지 서버(200)가 생략될 경우 탐지 서버(200)의 역할도 수행할 수 있다. 메인 서버(100)는 탐지 서버(200)에 탐지 대상의 탐지를 요청할 수 있고, 탐지 서버(200)로부터 탐지 결과 이벤트를 수신할 수 있다.

[0031] 일 실시 예에서, 탐지 서버(200)는 탐지 대상의 데이터에 기반하여 탐지한 결과를 메인 서버(100)에 전송할 수 있다. 탐지 서버(200)는 생략될 수 있다. 탐지 서버(200)는 단일 시나리오, 복합 시나리오, 시계열 분석, 상관분석, AI 이상징후 탐지 및 통계 분석 등을 탐지할 수 있다. 탐지 서버(200)는 일반 임계치 및 자동 가변 임계치를 이용하여 탐지 기능을 수행할 수 있다.

[0032] 일 실시 예에서, 분석 서버(600)는 인공지능 분석 전용 시스템을 구비할 수 있고, 인공지능 분석에 사용되는 인공신경망을 최적화 시킬 수 있다. 예를 들어, 분석 서버(600)는 메인 서버(100)로부터 인공지능 분석을 요청받을 수 있고, 인공지능 분석 결과를 보안 담당자 또는 운영 담당자가 볼 수 있도록 메인 서버(100)의 화면에 표시할 수 있다. 분석 서버(600)의 대시보드는 AI 이벤트 자동대응과 AI 인공신경망 최적화로 나뉠 수 있다. 메인 서버(100)의 데이터 기반 분석은 데이터 탐색 위저드, 데이터 비주얼라이져, 인프라 운영 탐색, 임직원 보안 탐색, 실시간 장애 예측, 시계열 장애 예측 등을 포함할 수 있다. 메인 서버(100)의 이벤트 분석 대응은 이벤트 분석 모니터, 시나리오 모니터, 조직 프로파일링, 고위험군 프로파일링, 임직원 프로파일링을 포함할 수 있으며, 분석 서버(600)는 유사도 분석, 관계도 분석 등을 포함할 수 있다. 한편, 도면에는 도시되지 않았지만 인공지능형 CCTV가 본 발명의 시스템(10)에 더 구비될 수 있고, 분석 서버(600)는 CCTV의 촬영 영상을 활용할 수 있다.

[0033] 일 실시 예에서, 메인 서버(100), 탐지 서버(200) 및 분석 서버(600)는 이상징후 관제 시스템으로 분류될 수 있다.

[0034] 한편, 도면에는 도시되지 않았지만, 본 발명의 시스템(10)은 AI 분석 서버와 AI 생성 시스템을 더 포함할 수 있

다. AI 생성 시스템은 머신 러닝과 딥 러닝 기술로 인공 신경망 또는 머신러닝 모델을 생성할 수 있다. 머신 러닝은 Supervised Leaning, Un-supervised Learning, Semi-supervides Learning, Statistical Algorithm을 포함할 수 있고, 딥 러닝은 Deep Neural Network, Convolution Neural Network, Recurrent Neural Network, Auto Encoder, LSTM, Generative Adversarial Nets 등 다수의 인공지능 알고리즘을 포함할 수 있다. AI 분석 서버는 자동 가변 임계치 산출, AI 이상징후 탐지, 유사도 분석, 관계도 분석, Face ID 분석, 이벤트 자동 대응 등을 수행할 수 있다.

[0036] 도 2는 본 발명의 일 실시 예에 따른 통합 관제 방법을 설명하기 위한 흐름도이다. 도 2의 동작들은 도 1에 개시된 메인 서버(100) 또는 탐지 서버(200)에 의해 수행될 수 있다. 하기에서 설명의 편의를 위해 메인 서버(100)가 각 동작들을 수행하는 일 예로 설명한다. 도 2의 동작들은 인공지능 알고리즘에 의해 수행될 수 있다.

[0038] 도 2를 참조하면, 일 실시 예에서, 동작 21에서, 메인 서버(100)는 탐지 대상의 데이터를 획득할 수 있다. 예를 들어, 탐지 대상은 임직원(예: 사번, 성명 등), IP 주소(예: 사내외 시스템의 IP 주소), 인프라 시스템(예: 사내 서버 OS, 네트워크 장비, 클라우드 노드 등의 IP주소 또는 호스트명) 또는 업무 시스템(예:사내 인트라넷 시스템, 전사자원관리 시스템, 프로젝트 메니징 시스템 등 회사 업무시스템의 IP주소 또는 호스트명) 중 적어도 하나를 포함할 수 있다. 탐지 대상의 데이터는 임직원 별 보안로그 데이터(예: DRM, DLP, USB사용이력, 개인정보탐지 솔루션 로그), 내외부 IP주소별 보안 시스템의 로그 데이터(예: 방화벽 로그, IPS/IDS 로그, 백신 탐지 로그, DDOS 로그), 인프라 시스템의 로그 데이터(예: syslog, access_log 등 로그데이터 및 네트워크 트래픽 로그) 그리고 인프라 시스템의 성능 데이터(예: 서버 CPU 사용량, 메모리 사용량, 각 인프라 시스템 별 자원 현황) 또는 업무 시스템의 로그 데이터 중 적어도 하나를 포함할 수 있다.

[0039] 일 실시 예에서, 동작 22에서, 메인 서버(100)는 탐지 대상의 데이터와 관련된 임계값을 결정할 수 있다. 임계값은 탐지 대상별 특성을 고려하여 결정될 수 있다. 예컨대, 임계값은 임직원별 업무 특성 또는 시스템별 용도 특성을 고려하여 결정될 수 있다. 임계값을 결정하는 구체적인 동작은 도 3에서 후술한다. 한편, 임계값을 결정하는 동작은 탐지 대상의 데이터를 획득할 때마다 반복적으로 수행할 수 있다. 따라서, 본 발명의 임계값은 임직원별 직무 변화 또는 시스템별 용도 변경을 고려하여 탐지 대상의 상태 변화가 반영된 임계값으로 자동 조정될 수 있다.

[0040] 일 실시 예에서, 동작 23에서, 메인 서버(100)는 탐지 대상의 데이터와 임계값을 비교할 수 있다. 예를 들어, 탐지 대상이 임직원 중 어느 한 직원이고 데이터가 DRM 보안 해제 횟수일 경우, 해당 직원의 DRM 보안 해제 횟수의 임계값과 데이터를 비교할 수 있다.

[0041] 일 실시 예에서, 동작 24에서, 메인 서버(100)는 비교 결과 탐지 대상의 데이터가 정상 범위를 벗어난 지 확인할 수 있다. 예를 들어, 탐지 대상이 임직원 중 어느 한 직원이고 데이터가 DRM 보안 해제 횟수일 경우, 해당 직원의 DRM 보안 해제 횟수의 임계값이 6이고 데이터가 7이라면 정상 범위를 벗어난 것으로 확인할 수 있다.

[0042] 일 실시 예에서, 비교 결과 탐지 대상의 데이터가 정상 범위를 벗어나지 않을 경우, 메인 서버(100)는 동작 21 내지 동작 23을 지속적으로 반복할 수 있다.

[0043] 일 실시 예에서, 동작 25에서, 메인 서버(100)는 비교 결과 탐지 대상의 데이터가 정상 범위를 벗어날 경우, 탐지 대상의 이상징후 여부를 판단할 수 있다. 예를 들어, 상기 상황과 같이 해당 직원의 DRM 보안 해제 횟수가 임계값보다 높은 7일 경우, 임계값을 벗어난 횟수가 1회일 경우에도 이상징후로 판단할 수 있고, 이와 달리 임계값을 벗어난 횟수가 기준 횟수 이상일 경우에 이상징후로 판단할 수 있고, 횟수 여부에 상관 없이 해당 직원의 DRM 보안이 해제된 문서가 외부로 반출된 지 여부를 메일 시스템, USB 접속 여부, 프린트 여부 등을 종합적으로 분석하여 비밀 유지 의무가 없는 외부에 반출된 것이 확인된 경우에 이상징후로 판단할 수 있다. 즉, 이상징후로 판단하는 기준은 해당 탐지 대상의 업무 특성 또는 성능 특성을 고려하고, 미리 설정한 기준에 기반하여 이상징후를 판단할 수 있다.

[0044] 한편, 이상징후는 미리 설정된 시나리오에 따라 결정될 수 있다. 예를 들어, 임직원의 PC에서 USB를 통한 파일 반출, DRM 보안 해재 결제자를 본인으로 지정하여 해제한 횟수가 기준 횟수 이상일 경우 등 다양한 이상징후 판단 시나리오가 미리 설정될 수 있다.

[0045] 한편, 예를 들어, 이상징후는 사용자의 유해 IP 접근, E-DLP 고의 중단, PC내 개인정보 탐지, 업무시스템 계정 공유, 복수계정, 비인가 서버 권한 상승/획득 시도, USB 과다 사용, 동일 부서 내 개인정보 보유 평균 건수, 사용자의 유해 IP 접근, 출력물 보안 우회 등을 포함할 수 있고, 이외에도 인프라 시스템 또는 업무 시스템의 성능 저하 등을 포함할 수 있다. 물론 이상징후는 상기 예에 한정되지 아니하고 모니터링 대상인 사내 시스템(10)

관련하여 비정상적인 모든 이벤트를 포함할 수 있다.

[0047] 도 3은 본 발명의 일 실시 예에 따른 임계값을 결정하기 위한 방법을 설명하기 위한 흐름도이다. 도 3의 동작들은 도 1에 개시된 메인 서버(100) 또는 탐지 서버(200)에 의해 수행될 수 있다. 도 3의 동작들은 도 2의 동작 22를 구체화한 동작들이다. 하기에서 설명의 편의를 위해 메인 서버(100)가 각 동작들을 수행하는 일 예로 설명한다. 도 3의 동작들은 인공지능 알고리즘에 의해 수행될 수 있다.

[0049] 도 3을 참조하면, 일 실시 예에서, 동작 31에서, 메인 서버(100)는 데이터를 획득한 시점 이전부터 미리 설정한 기준 기간 동안 탐지 대상의 과거 데이터를 추출할 수 있다. 예를 들어, 상기 미리 설정한 기준 기간은 직원별 업무 특성 또는 시스템별 용도 특성을 고려하여 결정될 수 있다. 예를 들어, 데이터가 어느 한 직원의 메일 발송 건수일 경우, 현재 측정 시점의 이전일 기준으로 과거 한달간의 해당 직원의 메일 발송 건수를 추출할 수 있다.

[0050] 일 실시 예에서, 동작 32에서, 메인 서버(100)는 과거 데이터에서 기준 값을 산출할 수 있다. 예를 들어, 기준 값은 과거 데이터의 평균, 분산, 표준편차, 왜도(Skewness), 첨도(Kurtosis), 피크 투 피크(Peak-to-Peak)값, 크래스트 팩터(Crest Factor), 케이 팩터(K-Factor), 마할라노비스 거리(Mahalnobis Distance), 변동계수(Coefficient of Variance) 중 어느 하나를 이용하거나 이들의 조합을 이용하여 산출될 수 있다. 예를 들어, 여기서 평균은 모니터링 대상 데이터의 일정 구간에서의 평균을 의미할 수 있고, 표준편차는 모니터링 대상 데이터가 평균으로부터 얼마나 떨어져 있는 지를 나타내는 산포도일 수 있다.

[0051] 일 실시 예에서, 동작 33에서, 메인 서버(100)는 기준 값과 지정된 가중치에 기반하여 임계값을 결정할 수 있다. 예를 들어, 지정된 가중치는 데이터의 특성에 따라 결정되는 민감도 수치일 수 있다. 예컨대, 외부 업체과 업무가 많은 A 직원의 DRM 보안 해제와 보안 해제된 메일 발송 건수는 외부 업체와 업무가 전혀 없는 B 직원에 비해 매우 많을 수 있다. 따라서, A 직원의 가중치는 높게 주고 B 직원의 가중치는 낮게 줄 수 있다. 설명의 편의를 위해 숫자로 설명하면, 기준 값이 3이고 지정된 가중치가 2배일 경우 임계 값은 그 상한 값인 6이 될 수 있다.

[0052] 물론 상기와 다르게 탐지 대상의 특성을 고려하여 다양한 방식으로 임계값을 설정할 수 있고, 본 발명의 임계값은 해당 탐지 대상의 데이터 획득 시점마다 산출될 수 있다.

[0054] 도 4는 본 발명의 일 실시 예에 따른 탐지 대상의 상태를 판단하는 방법을 설명하기 위한 흐름도이다. 도 5는 본 발명의 일 실시 예에 따른 탐지 대상의 상태를 판단하는 방법을 설명하기 위한 예시도이다. 도 4의 동작들은 도 1에 개시된 메인 서버(100) 또는 탐지 서버(200)에 의해 수행될 수 있다. 하기에서 설명의 편의를 위해 메인 서버(100)가 각 동작들을 수행하는 일 예로 설명한다. 도 4의 동작들은 인공지능 알고리즘에 의해 수행될 수 있다.

[0056] 도 4를 참조하면, 일 실시 예에서, 동작 41에서, 메인 서버(100)는 미리 설정한 주기마다 탐지 대상의 데이터의 시계열 패턴을 확인할 수 있다. 예를 들어, 미리 설정한 주기는 임직원의 업무 특성 또는 시스템별 용도 특성을 고려하여 결정될 수 있다. 예컨대, 도 5와 같이 메인 서버(100)는 탐지 대상의 데이터의 시계열 패턴(50)을 확인할 수 있고, 데이터의 임계값 시계열 패턴(53)을 확인할 수 있다.

[0057] 일 실시 예에서, 동작 42에서, 메인 서버(100)는 탐지 대상의 데이터가 정상 범위를 벗어난 시점을 확인할 수 있다. 예를 들어, 데이터가 임계값을 벗어난 시점(54)을 정상 범위를 벗어난 시점으로 확인할 수 있다.

[0058] 일 실시 예에서, 동작 43에서, 메인 서버(100)는 정상 범위를 벗어난 시점 이전의 데이터의 제1 시계열 패턴(51)과 시점 이후의 데이터의 제2 시계열 패턴(52)을 비교할 수 있다. 예를 들어, 정상 범위를 벗어난 시점(54) 이후로 일정 기간 동안 그 정상 범위를 벗어난 데이터의 추세가 이어질 경우, 제2 시계열 패턴(52)의 존재를 확인할 수 있다.

[0059] 일 실시 예에서, 동작 44에서, 메인 서버(100)는 비교 결과 제1 시계열 패턴(51)과 제2 시계열 패턴(52)이 다를 경우, 탐지 대상의 상태가 변경된 것으로 판단할 수 있다. 예를 들어, 메인 서버(100)는 정상 범위를 벗어난 시점(54)을 임직원별 직무 변화 시점 또는 시스템별 용도 변경 시점으로 판단할 수 있고, 정상 범위를 벗어난 시점(54) 이후를 신규 업무 구간 또는 신규 용도 구간으로 판단할 수 있다.

[0061] 도 6은 본 발명의 일 실시 예에 따른 텍스트를 포함하는 로그 데이터에서 임계값을 결정하는 방법을 설명하기 위한 흐름도이다. 도 6의 동작들은 도 1에 개시된 메인 서버(100) 또는 탐지 서버(200)에 의해 수행될 수 있다. 하기에서 설명의 편의를 위해 메인 서버(100)가 각 동작들을 수행하는 일 예로 설명한다. 도 6의 동작들은 인공

지능 알고리즘에 의해 수행될 수 있다.

[0063] 도 6을 참조하면, 일 실시 예에서, 동작 61에서, 메인 서버(100)는 탐지 대상의 로그 데이터를 획득할 수 있다. 예를 들어, 로그 데이터는 임직원의 발송 메일 내용일 수 있다.

[0064] 일 실시 예에서, 동작 62에서, 메인 서버(100)는 로그 데이터에 포함된 텍스트를 추출할 수 있다. 예를 들어, 텍스트는 발송 메일에 포함된 텍스트일 수 있다.

[0065] 일 실시 예에서, 동작 63에서, 메인 서버(100)는 텍스트에 포함된 복수의 단어들을 각각 벡터화함으로써 복수의 단어들에 각각 대응하는 수치를 획득할 수 있다. 예를 들어, 메인 서버(100)는 유사한 의미를 갖는 성함, 이름, 성명 등의 단어를 유사한 수치인 100, 101, 102에 매칭시킬 수 있다.

[0066] 일 실시 예에서, 동작 64에서, 메인 서버(100)는 각각 대응하는 수치에서 기준 값을 추출할 수 있다. 예를 들어, 기준 값은 과거 데이터의 평균, 표준편차 또는 중앙값과 같은 기술통계 기반 수치뿐만 아니라, 로그 데이터의 벡터 수치 배열값을 Auto Encoder나 PCA 등의 차원축소(Dimension Reduction) 방법 등을 이용하여 산출될 수 있다.

[0067] 일 실시 예에서, 동작 65에서, 메인 서버(100)는 추출한 기준 값과 지정된 가중치에 기반하여 임계 값을 결정할 수 있다. 이는 동작 33과 동일한 방식으로 결정될 수 있다.

[0069] 도 7은 본 발명의 일 실시 예에 따른 군집을 이용하여 이상징후를 판단하는 방법을 설명하기 위한 흐름도이다. 도 8은 본 발명의 일 실시 예에 따른 군집을 이용하여 이상징후를 판단하는 방법을 설명하기 위한 예시도이다. 도 7의 동작들은 도 1에 개시된 메인 서버(100) 또는 탐지 서버(200)에 의해 수행될 수 있다. 하기에서 설명의 편의를 위해 메인 서버(100)가 각 동작들을 수행하는 일 예로 설명한다. 도 7의 동작들은 인공지능 알고리즘에 의해 수행될 수 있다.

[0071] 도 7을 참조하면, 일 실시 예에서, 동작 71에서, 메인 서버(100)는 탐지 대상의 데이터를 획득할 수 있다. 예를 들어, 탐지 대상의 데이터는 DRM 보안 해제 횟수와 보안 해제된 문서의 발송 건수일 수 있고, 외부 보안 시스템의 패킷 차단 건수 일 수 있고, 인프라 시스템의 CPU 사용량이나 메모리 성능일 수 있다. 한편, 임직원 별 데이터는 하루 단위, IP 주소는 한시간 단위, 인프라 시스템의 성능 데이터도 한시간 단위로 획득될 수 있다.

[0072] 일 실시 예에서, 동작 72에서, 메인 서버(100)는 적어도 하나의 파라미터에 기반하여 탐지 대상의 데이터를 군집화(clustering, 기계학습의 한 종류)할 수 있다. 파라미터는 임직원의 다양한 로그 데이터, 보안 시스템, 인프라 시스템 또는 업무 시스템의 어느 하나 또는 여러개의 데이터 일 수 있고, 예를 들어, 파라미터는 DRM 보안 해제 횟수와 보안 해제된 문서의 발송 건수이거나 이 둘 모두일 수 있다.

[0073] 일 실시 예에서, 동작 73에서, 메인 서버(100)는 군집화된 군집과 데이터를 비교할 수 있다. 예를 들어, 메인 서버(100)는 군집들(81, 82, 83, 84)를 확인할 수 있고, 각각의 군집들은 동일한 업무를 수행하는 팀원들이 속한 군집들일 수 있다. 또한, 데이터(86, 87, 88, 89)는 동일한 업무를 수행하는 팀원임에도 군집에서 벗어난 경우일 수 있고, 예컨대, 평소 업무보다 보안 해제된 문서를 외부에 많이 발송한 경우일 수 있다.

[0074] 일 실시 예에서, 동작 74에서, 메인 서버(100)는 비교 결과 데이터 중 적어도 하나가 기준 범위를 벗어날 경우, 적어도 하나에 대응하는 탐지 대상에서 이상징후가 발생한 것으로 판단할 수 있다. 예를 들어, 데이터(86, 87, 88, 89)는 동일한 업무를 수행하는 팀원임에도 군집에서 벗어난 경우, 해당 데이터(86, 87, 88, 89)를 갖는 임직원의 보안 사고 유무 등을 확인하거나 시스템의 성능을 점검함으로서 이상징후 발생 여부를 판단할 수 있다.

[0076] 도 9는 본 발명의 일 실시 예에 따른 유사도를 이용하여 탐지 대상의 이상징후를 판단하는 방법을 설명하기 위한 흐름도이다. 도 9의 동작들은 도 1에 개시된 메인 서버(100) 또는 탐지 서버(200)에 의해 수행될 수 있다. 하기에서 설명의 편의를 위해 메인 서버(100)가 각 동작들을 수행하는 일 예로 설명한다. 도 9 동작들은 인공지능 알고리즘에 의해 수행될 수 있다.

[0078] 도 9를 참조하면, 일 실시 예에서, 동작 91에서, 메인 서버(100)는 데이터의 시계열 패턴 또는 데이터에 기반한 군집을 확인할 수 있다.

[0079] 일 실시 예에서, 동작 92에서, 메인 서버(100)는 시계열 패턴, 군집 또는 미리 설정한 유사도 기법에 기반하여 탐지 대상의 유사도를 결정할 수 있다. 예를 들어, 유사한 시계열 패턴을 갖거나 동일한 군집에 속하는 임직원 또는 시스템은 높은 유사도를 가질 수 있다. 또한, 코사인 유사도(Cosine Similarity), 유클리드 거리(Euclidean distance), 자카드 유사도(Jaccard similarity) 등의 유사도 기법을 이용하여 탐지 대상의 유사도

를 결정할 수 있다.

[0080] 일 실시 예에서, 동작 93에서, 메인 서버(100)는 탐지 대상 중 어느 하나의 이상징후를 검출할 수 있다. 예를 들어, 보안 해제된 문서 발송 건수가 지나치게 많은 어느 한 직원을 검출할 수 있다.

[0081] 일 실시 예에서, 동작 94에서, 메인 서버(100)는 이상징후가 검출된 어느 하나와 유사도가 높은 적어도 하나의 탐지 대상을 추출할 수 있다. 예를 들어, 상기 어느 한 직원과 보안 해제된 문서 발송 건수 면에서 동일한 시계열 패턴을 갖거나 유사도 기법에 근거하여 높은 유사도를 갖는 다른 직원들을 추출할 수 있다.

[0082] 일 실시 예에서, 동작 95에서, 메인 서버(100)는 유사도가 높은 적어도 하나의 탐지 대상의 이상징후를 판단할 수 있다. 예를 들어, 추출한 다른 직원들도 동일한 이상징후가 있는 지 확인할 수 있다.

[0084] 도 10은 본 발명의 일 실시 예에 따른 관계도를 이용하여 탐지 대상의 이상징후를 판단하는 방법을 설명하기 위한 흐름도이다. 도 10의 동작들은 도 1에 개시된 메인 서버(100) 또는 탐지 서버(200)에 의해 수행될 수 있다. 하기에서 설명의 편의를 위해 메인 서버(100)가 각 동작들을 수행하는 일 예로 설명한다. 도 10의 동작들은 인공지능 알고리즘에 의해 수행될 수 있다.

[0086] 도 10을 참조하면, 일 실시 예에서, 동작 1001에서, 메인 서버(100)는 카메라의 촬영 영상, 출입 기록 또는 서로 공유된 동일한 파일의 개수 중 적어도 하나에 기반하여 탐지 대상의 관계도를 결정할 수 있다. 예를 들어, 동일한 팀원 내에서 사수 관계일 경우 두 직원은 높은 관계도를 가질 수 있고, 임원과 비서일 경우 동일한 파일을 많이 공유할 수 있으므로 높은 관계도르 가질 수 있다.

[0087] 일 실시 예에서, 동작 1002에서, 메인 서버(100)는 탐지 대상 중 어느 하나의 이상징후를 검출할 수 있다. 예를 들어, 상기 사수 직원 또는 임원의 이상징후를 검출할 수 있다.

[0088] 일 실시 예에서, 동작 1003에서, 메인 서버(100)는 이상징후가 검출된 어느 하나와 관계도가 높은 적어도 하나의 탐지 대상을 추출할 수 있다. 예를 들어, 상기 사수 직원의 부사수 직원 또는 비서를 추출할 수 있다.

[0089] 일 실시 예에서, 동작 1004에서, 메인 서버(100)는 관계도가 높은 적어도 하나의 탐지 대상의 이상징후를 판단할 수 있다. 예를 들어, 상기 사수 직원의 부사수 직원 또는 비서도 동일한 이상징후가 있는 지 확인하고 보안 사고 등의 사고 발생 여부를 판단할 수 있다.

[0091] 본 발명의 일 실시예에 따른 통합 관제 방법은, 탐지 대상의 데이터를 획득하는 단계; 상기 탐지 대상의 상기 데이터와 관련된 임계값을 결정하는 단계; 상기 탐지 대상의 상기 데이터와 상기 임계값을 비교하는 단계; 및 상기 비교 결과 상기 탐지 대상의 상기 데이터가 정상 범위를 벗어날 경우, 상기 탐지 대상의 이상징후 여부를 판단하는 단계를 포함하고, 상기 임계값을 결정하는 단계는 상기 탐지 대상의 상기 데이터를 획득할 때마다 반복적으로 수행되고, 상기 임계값을 결정하는 단계는, 상기 데이터를 획득한 시점 이전부터 미리 설정한 기준 기간 동안 상기 탐지 대상의 과거 데이터를 추출하는 단계; 상기 과거 데이터에서 기준 값을 산출하는 단계; 및 상기 기준 값과 지정된 가중치에 기반하여 임계값을 결정하는 단계를 포함할 수 있다.

[0092] 다양한 실시 예에 따르면, 미리 설정한 주기마다 상기 탐지 대상의 상기 데이터의 시계열 패턴을 확인하는 단계를 더 포함할 수 있다.

[0093] 다양한 실시 예에 따르면, 상기 탐지 대상의 이상 징후를 판단하는 단계는, 상기 탐지 대상의 상기 데이터가 상기 정상 범위를 벗어난 시점을 확인하는 단계; 상기 정상 범위를 벗어난 상기 시점 이전의 상기 데이터의 제1 시계열 패턴과 상기 시점 이후의 상기 데이터의 제2 시계열 패턴을 비교하는 단계; 및 비교 결과 상기 제1 시계열 패턴과 상기 제2 시계열 패턴이 다를 경우, 상기 탐지 대상의 상태가 변경된 것으로 판단하는 단계;를 포함할 수 있다.

[0094] 다양한 실시 예에 따르면, 상기 탐지 대상의 로그 데이터를 획득하는 단계; 상기 로그 데이터에 포함된 텍스트를 추출하는 단계; 상기 텍스트에 포함된 복수의 단어들을 각각 벡터화함으로써 상기 복수의 단어들에 각각 대응하는 수치를 획득하는 단계; 상기 각각 대응하는 수치에서 상기 기준 값을 추출하는 단계; 및 상기 추출한 기준 값과 상기 지정된 가중치에 기반하여 상기 임계값을 결정하는 단계;를 포함할 수 있다.

[0095] 다양한 실시 예에 따르면, 적어도 하나의 파라미터에 기반하여 상기 탐지 대상의 상기 데이터를 군집화하는 단계; 상기 군집화된 군집과 상기 데이터를 비교하는 단계; 및 상기 비교 결과 상기 데이터 중 적어도 하나가 기준 범위를 벗어날 경우, 상기 적어도 하나에 대응하는 탐지 대상에서 이상징후가 발생한 것으로 판단하는 단계;를 더 포함할 수 있다.

[0096] 다양한 실시 예에 따르면, 상기 데이터의 시계열 패턴 또는 상기 데이터에 기반한 군집을 확인하는 단계; 상기 시계열 패턴, 상기 군집 또는 미리 설정한 유사도 기법에 기반하여 상기 탐지 대상의 유사도를 결정하는 단계; 상기 탐지 대상 중 어느 하나의 이상징후를 검출하는 단계; 상기 이상징후가 검출된 어느 하나와 유사도가 높은 적어도 하나의 탐지 대상을 추출하는 단계; 및 상기 유사도가 높은 상기 적어도 하나의 탐지 대상의 이상징후를 판단하는 단계;를 더 포함할 수 있다.

[0097] 다양한 실시 예에 따르면, 카메라의 촬영 영상, 출입 기록 또는 서로 공유된 동일한 파일의 개수 중 적어도 하나에 기반하여 상기 탐지 대상의 관계도를 결정하는 단계; 상기 탐지 대상 중 어느 하나의 이상징후를 검출하는 단계; 상기 이상징후가 검출된 어느 하나와 관계도가 높은 적어도 하나의 탐지 대상을 추출하는 단계; 및 상기 관계도가 높은 상기 적어도 하나의 탐지 대상의 이상징후를 판단하는 단계;를 더 포함할 수 있다.

[0098] 다양한 실시 예에 따르면, 상기 탐지 대상은 임직원, 보안 시스템, 인프라 시스템 또는 업무 시스템 중 적어도 하나를 포함할 수 있다.

[0099] 다양한 실시 예에 따르면, 상기 탐지 대상의 상기 데이터는 임직원 별 로그 데이터, 보안 시스템의 로그 데이터, 인프라 시스템의 로그 데이터, 인프라 시스템의 성능 데이터 또는 업무 시스템의 로그 데이터 중 적어도 하나를 포함할 수 있다.

[0100] 본 발명의 일 실시예에 따른 통합 관제 시스템은, 탐지 대상의 이상징후를 탐지 및 분석하는 메인 서버를 포함하고, 상기 메인 서버가 탐지 대상의 데이터를 획득하고, 상기 메인 서버가 상기 탐지 대상의 상기 데이터와 관련된 임계값을 결정하고, 상기 메인 서버가 상기 탐지 대상의 상기 데이터와 상기 임계값을 비교하고, 상기 메인 서버가 상기 비교 결과 상기 탐지 대상의 상기 데이터가 정상 범위를 벗어날 경우, 상기 탐지 대상의 이상징후 여부를 판단하고, 상기 메인 서버는 상기 탐지 대상의 상기 데이터를 획득할 때마다 상기 임계값을 반복적으로 결정하고, 상기 메인 서버는 상기 데이터를 획득한 시점 이전부터 미리 설정한 기준 기간 동안 상기 탐지 대상의 과거 데이터를 추출하고, 상기 과거 데이터에서 기준 값을 산출하고, 상기 기준 값과 지정된 가중치에 기반하여 임계값을 결정함으로써 상기 임계값을 결정할 수 있다.

[0102] 이상, 첨부된 도면을 참조로 하여 본 발명의 실시예를 설명하였지만, 본 발명이 속하는 기술분야의 통상의 기술자는 본 발명이 그 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 실시될 수 있다는 것을 이해할 수 있을 것이다. 그러므로, 이상에서 기술한 실시예들은 모든 면에서 예시적인 것이며, 제한적이 아닌 것으로 이해해야만 한다.

부호의 설명

[0103] 100 : 메인 서버 200 : 탐지 서버

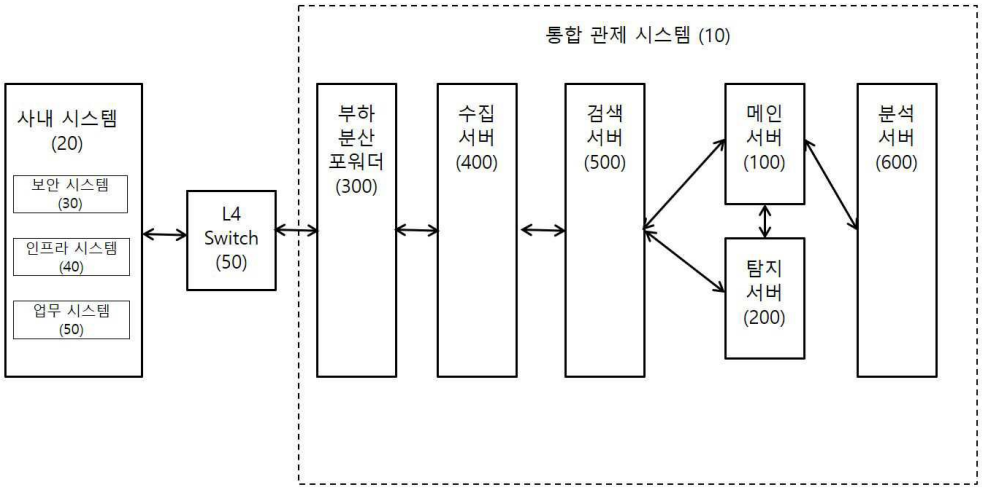
300 : 부하 분산 포워더 400 : 수집 서버

500 : 검색 서버 600 : 분석 서버

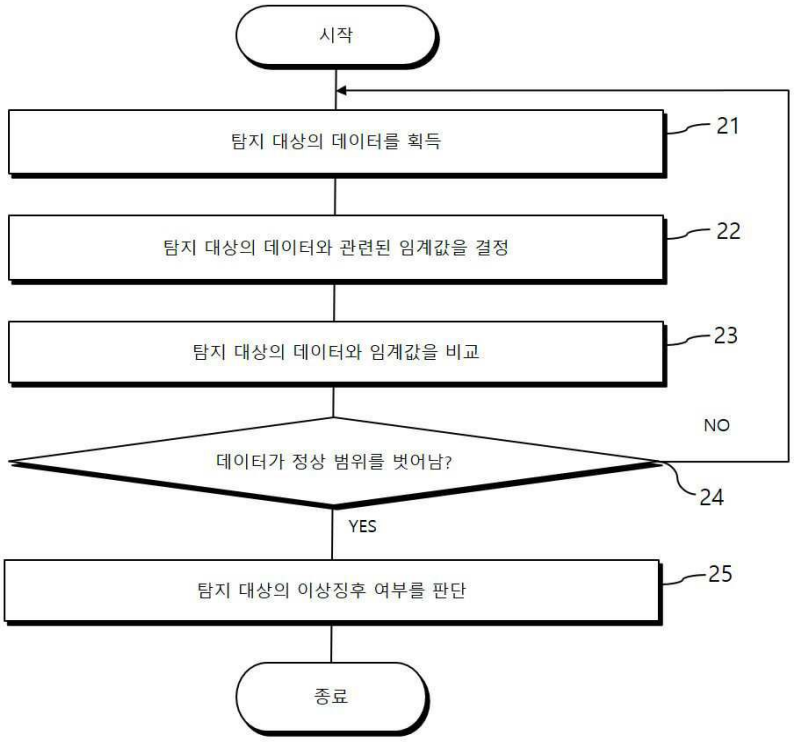
10 : 통합 관제 시스템

도면

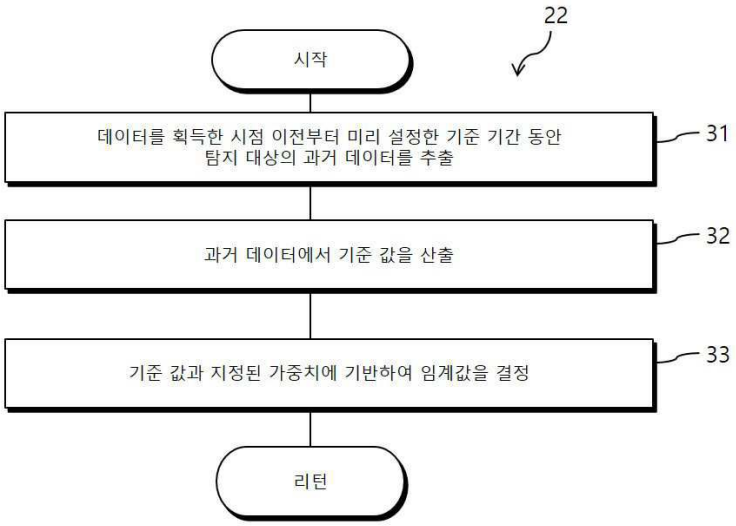
도면1


통합 관제 시스템 (10)
사내 시스템 (20)
보안 시스템 (30)
인프라 시스템 (40)
업무 시스템 (50)
L4 Switch (50)
부하 분산 포워더 (300)
수집 서버 (400)
검색 서버 (500)
메인 서버 (100)
탐지 서버 (200)
분석 서버 (600)

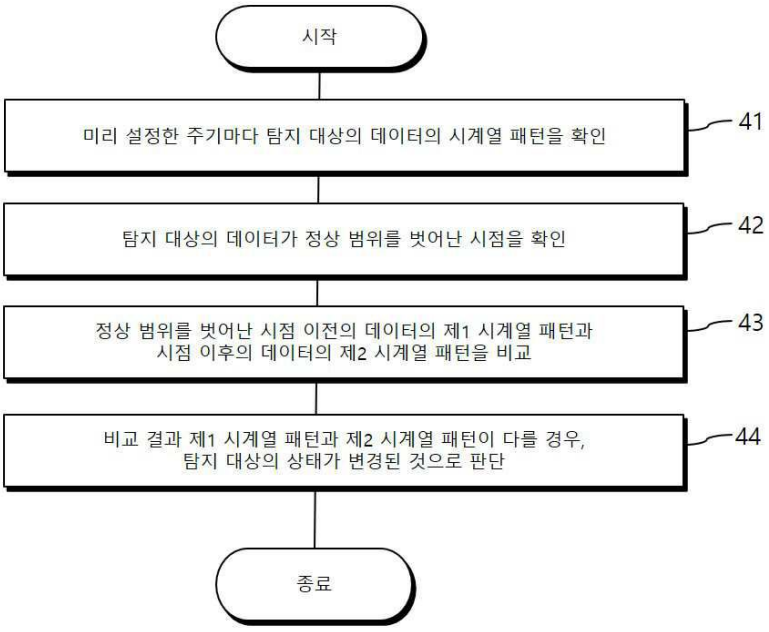
도면2


시작
탐지 대상의 데이터를 획득
21
탐지 대상의 데이터와 관련된 임계값을 결정
22
탐지 대상의 데이터와 임계값을 비교
23
데이터가 정상 범위를 벗어남?
NO
24
YES
탐지 대상의 이상징후 여부를 판단
25
종료

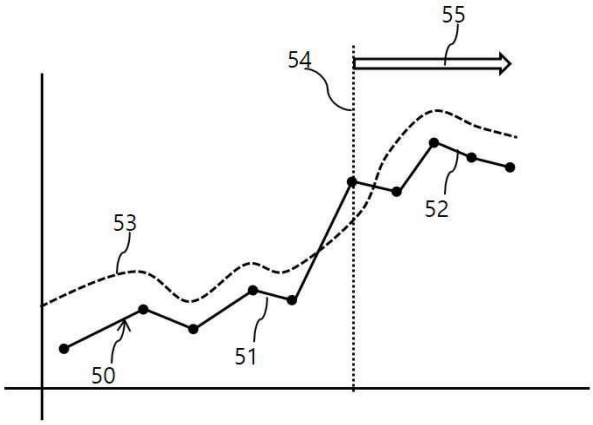
도면3


22
시작
데이터를 획득한 시점 이전부터 미리 설정한 기준 기간 동안
탐지 대상의 과거 데이터를 추출
31
과거 데이터에서 기준 값을 산출
32
기준 값과 지정된 가중치에 기반하여 임계값을 결정
33
리턴

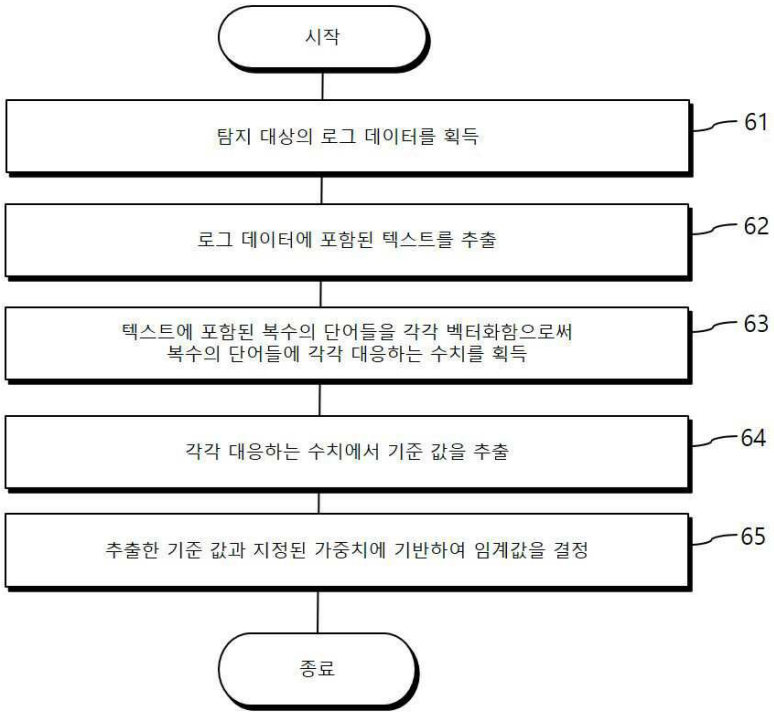
도면4


시작
미리 설정한 주기마다 탐지 대상의 데이터의 시계열 패턴을 확인
41
탐지 대상의 데이터가 정상 범위를 벗어난 시점을 확인
42
정상 범위를 벗어난 시점 이전의 데이터의 제1 시계열 패턴과
시점 이후의 데이터의 제2 시계열 패턴을 비교
43
비교 결과 제1 시계열 패턴과 제2 시계열 패턴이 다를 경우,
탐지 대상의 상태가 변경된 것으로 판단
44
종료

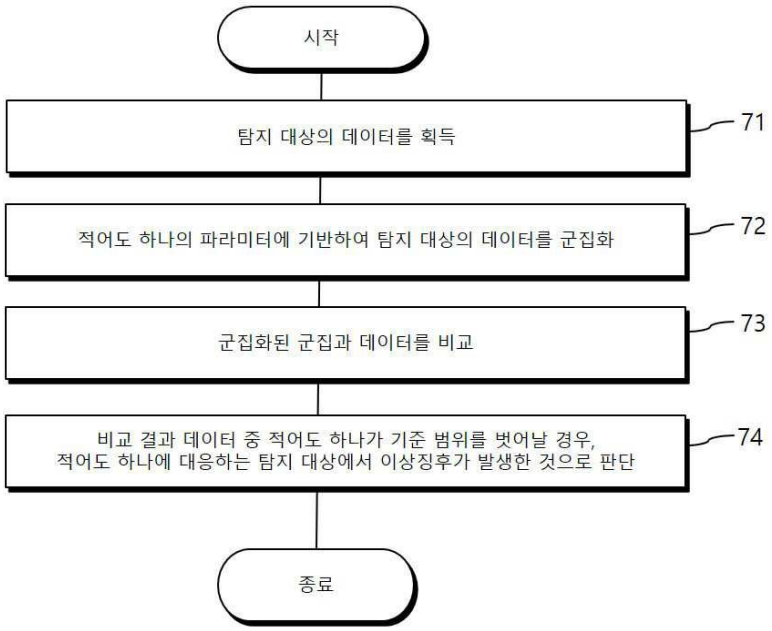
도면5


55
54
53
52
51
50

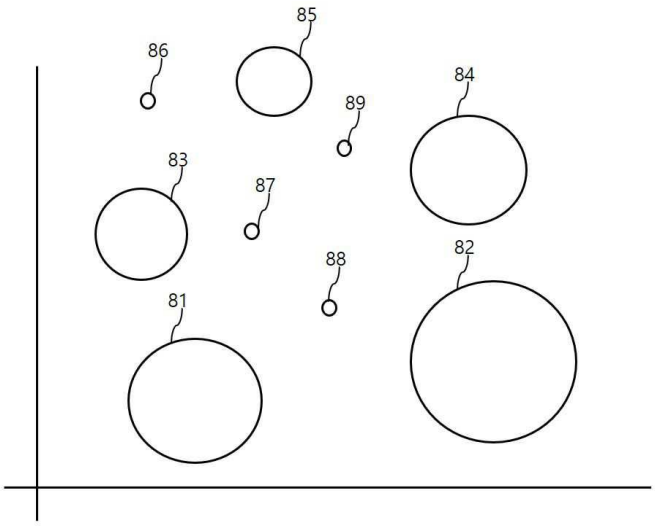
도면6


시작
탐지 대상의 로그 데이터를 획득
61
로그 데이터에 포함된 텍스트를 추출
62
텍스트에 포함된 복수의 단어들을 각각 벡터화함으로써
복수의 단어들에 각각 대응하는 수치를 획득
63
각각 대응하는 수치에서 기준 값을 추출
64
추출한 기준 값과 지정된 가중치에 기반하여 임계값을 결정
65
종료

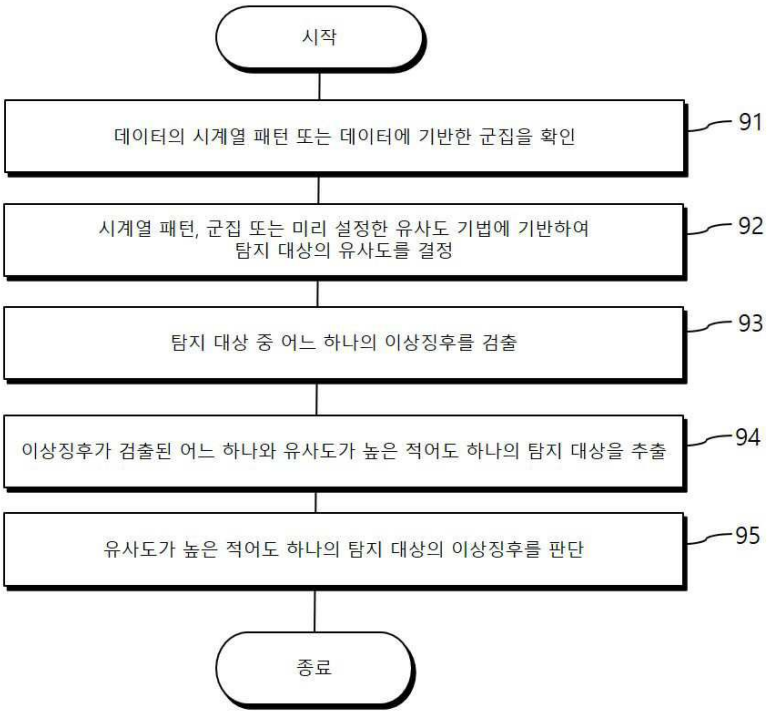
도면7


시작
탐지 대상의 데이터를 획득
71
적어도 하나의 파라미터에 기반하여 탐지 대상의 데이터를 군집화
72
군집화된 군집과 데이터를 비교
73
비교 결과 데이터 중 적어도 하나가 기준 범위를 벗어날 경우,
적어도 하나에 대응하는 탐지 대상에서 이상징후가 발생한 것으로 판단
74
종료

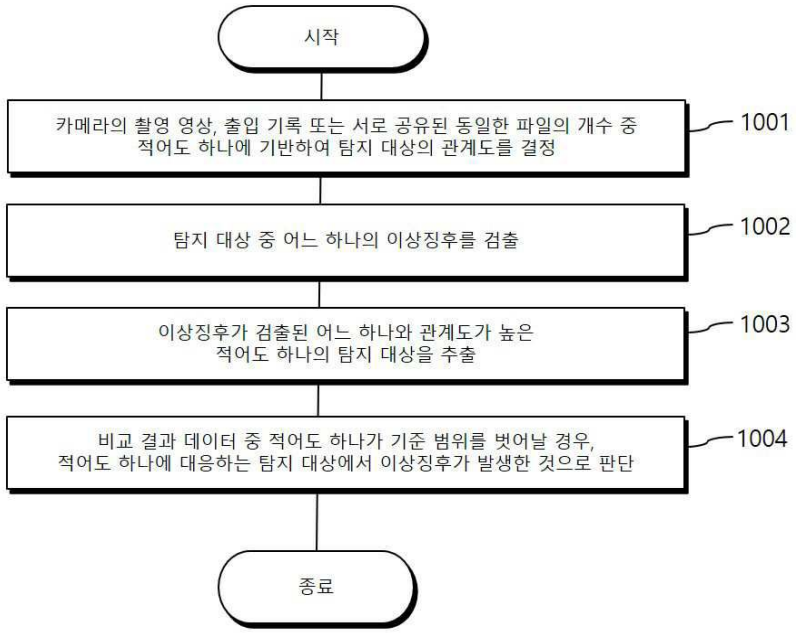
도면8


85
86
84
89
83
87
88
82
81

도면9



도면10



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 5

【변경전】

제3 항 또는 제4 항에 있어서,

상기 제2 탐지대상 이상징후 판단 단계는,

상기 제2 탐지대상의 데이터와 관련된 제2 임계값을 결정하는 단계; 및

상기 제2 탐지대상의 데이터와 상기 제2 임계값을 비교하되, 상기 비교 결과 상기 제2 탐지대상의 데이터가 상기 제2 임계값을 벗어나면 상기 제2 탐지대상에 대하여 이상징후가 발생한 것으로 판단하는 단계를 포함하는, 통합 관제 방법.

【변경후】

제4 항에 있어서,

상기 제2 탐지대상 이상징후 판단 단계는,

상기 제2 탐지대상의 데이터와 관련된 제2 임계값을 결정하는 단계; 및

상기 제2 탐지대상의 데이터와 상기 제2 임계값을 비교하되, 상기 비교 결과 상기 제2 탐지대상의 데이터가 상기 제2 임계값을 벗어나면 상기 제2 탐지대상에 대하여 이상징후가 발생한 것으로 판단하는 단계를 포함하는, 통합 관제 방법.

【직권보정 2】

【보정항목】 청구범위

【보정세부항목】 청구항 7

【변경전】

하드웨어인 컴퓨터와 결합되어, 제1 항 내지 제4 항 중 어느 한 항의 방법을 실행시키기 위해 기록매체에 저장된, 통합 관제 프로그램.

【변경후】

하드웨어인 컴퓨터와 결합되어, 제1 항 내지 제2 항, 제4 항 중 어느 한 항의 방법을 실행시키기 위해 기록매체에 저장된, 통합 관제 프로그램.