



(19)대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。 Int. Cl.

G06F 21/00 (2006.01)

G06F 17/40 (2006.01)

G06F 15/00 (2006.01)

(11) 공개번호 10-2007-0039478

(43) 공개일자 2007년04월12일

(21) 출원번호 10-2006-7020969

(22) 출원일자 2006년10월09일

심사청구일자 없음

번역문 제출일자 2006년10월09일

(86) 국제출원번호 PCT/US2005/004934

(87) 국제공개번호 WO 2005/093546

국제출원일자 2005년02월16일

국제공개일자 2005년10월06일

(30) 우선권주장 10/796,932 2004년03월09일 미국(US)

(71) 출원인 아이피록스, 인코포레이티드
미국 캘리포니아 샌어제이 슈트 110 노쓰 퍼스트 스트리트 2665 (우:95134)

(72) 발명자 사카모토, 아키오
미국 95014 캘리포니아 쿠퍼티노 메테올 플레이스 10564
초우, 청-궁
미국 94086 캘리포니아 써니베일 푸치시아 드라이브 1087
탕, 와니 지.
미국 95070 캘리포니아 사라토가 캐논 뷰 드라이브 20851
후, 징구오
미국 95054 캘리포니아 산타클라라 메종 코트 #201 510

(74) 대리인 남상선

전체 청구항 수 : 총 30 항

(54) 데이터베이스 유저 거동 감시 시스템 및 방법

(57) 요약

본 발명의 실시예들은 이례의 액티비티에 관해서 데이터베이스 시스템을 감시하는 기법을 제공한다. 감시중인 대상 데이터베이스에 관한 유저 거동 정보는, 이례의 액티비티를 검출하기 위해 자동적으로 수집되고, 분석되고, 1개 이상의 방침과 비교된다. 실시예는, 대상 데이터베이스에 관한 유저 거동 데이터를 감사 자취 및 동적 뷰를 포함하는 다양한 소스로부터 데이터베이스의 데이터베이스 관리 시스템과 협력하여 수집한다. 실시예는, 이례의 데이터베이스 액티비티를 검출하기 위해, 통계 기반의 침입 검출(SBID) 및 규칙 기반의 침입 검출(RBID) 중의 하나 이상을 채용한다. 정규의 사용 패턴으로부터 이탈하는 의심스러운 데이터베이스 액세스가 검출된다면, 책임을 갖는 기밀 보호 담당자에게의 경고, 보고 생성, e-메일 경고 등의 목표로 되는 동작이 행해진다.

대표도

도 3a

특허청구의 범위

청구항 1.

데이터베이스를 감시하기 위한 방법으로서,

1명 이상의 유저가 상기 데이터베이스를 어떻게 사용하는지를 나타내는 유저 거동 데이터를 수집하는 단계;

상기 데이터를 이력 데이터로서 처리하고 기억하는 단계;

거동 패턴을 결정하기 위해 상기 이력 데이터를 분석하는 단계;

1명 이상의 유저가 상기 데이터베이스를 어떻게 사용했었는지를 나타내는 새로운 1쌍의 데이터를 수신하는 단계;

상기 새로운 1쌍의 데이터와 상기 거동 패턴과의 비교를 행하는 단계;

상기 비교에 근거하여 상기 새로운 1쌍의 데이터가 1쌍의 기준을 충족시키는지 여부를 판단하는 단계;

상기 새로운 1쌍의 데이터가 상기 1쌍의 기준을 충족시키는 경우, 상기 새로운 1쌍의 데이터가 이례의 활동을 나타내고 있다고 판단하는 단계; 및

목표로 되는 동작을 행함에 의해 상기 판단에 따르는 단계를 포함하는, 데이터베이스 감시 방법.

청구항 2.

제1항에 있어서,

상기 새로운 1쌍의 데이터가 규칙 기반의 방침에 위반하고 있는지 여부를 판단하는 단계; 및

상기 새로운 1쌍의 데이터가 상기 규칙 기반의 방침에 위반하고 있는 경우, 상기 새로운 1쌍의 데이터는 이례의 활동을 나타내고 있다고 판단하는 단계를 더 포함하는, 데이터베이스 감시 방법.

청구항 3.

제2항에 있어서, 유저 거동 데이터를 수집하는 단계는 데이터베이스 매니저의 감사 자취 또는 동적 성능 뷰(view)로부터 정보를 읽는 단계를 더 포함하는, 데이터베이스 감시 방법.

청구항 4.

제3항에 있어서, 유저 거동 데이터를 수집하는 단계는, 감시 레벨에서,

1개 이상의 선택된 데이터베이스 오브젝트에 관한 데이터베이스 액세스에 관한 정보;

1개 이상의 선택된 데이터베이스 유저에 관한 데이터베이스 액세스에 관한 정보; 및

1개 이상의 선택된 데이터베이스 유저 섹션에 관한 데이터베이스 액세스에 관한 정보 중 하나 이상으로부터 선택된 정보를 수집하는 단계를 더 포함하는, 데이터베이스 감시 방법.

청구항 5.

제3항에 있어서, 유저 거동 데이터를 수집하는 단계는,

감시될 정보의 종류를 수신하는 단계;

상기 정보의 종류로부터 감시 레벨을 결정하는 단계; 및

결정된 상기 감시 레벨에 근거하여 상기 데이터베이스 매니저의 감사 옵션을 기동하는 단계를 더 포함하는, 데이터베이스 감시 방법.

청구항 6.

제2항에 있어서, 거동 패턴을 결정하기 위해 상기 이력 데이터를 분석하는 단계는, 상기 이력 데이터로부터 통계적 모델을 결정하는 단계를 더 포함하는, 데이터베이스 감시 방법.

청구항 7.

제6항에 있어서, 상기 이력 데이터로부터 통계적 모델을 결정하는 단계는,

상기 이력 데이터로부터 데이터베이스 액세스의 빈도를 결정하는 단계;

데이터베이스 액세스의 빈도에 관한 확률 함수를 결정하는 단계; 및

상기 확률 함수로부터 누적 확률 함수를 결정하는 단계를 더 포함하는, 데이터베이스 감시 방법.

청구항 8.

제7항에 있어서, 상기 새로운 1쌍의 데이터와 상기 거동 패턴과의 비교를 행하는 단계는,

상기 통계적 모델에 대하여 상기 새로운 1쌍의 데이터를 이용하여 가설을 검증하는 단계를 더 포함하는, 데이터베이스 감시 방법.

청구항 9.

제8항에 있어서, 상기 통계적 모델에 대하여 상기 새로운 1쌍의 데이터를 이용하여 가설을 검증하는 단계는,

상기 새로운 1쌍의 데이터에 관한 데이터베이스 액세스의 빈도를 결정하는 단계; 및

방호 기준 및 확률 함수 파라미터로부터 역치를 결정하는 단계를 더 포함하는, 데이터베이스 감시 방법.

청구항 10.

제9항에 있어서, 상기 통계적 모델 패턴에 대하여 상기 새로운 1쌍의 데이터를 이용하여 가설을 검증하는 단계는,

상기 새로운 1쌍의 데이터에 관한 데이터베이스 액세스의 빈도를 상기 역치와 비교하는 단계를 더 포함하는, 데이터베이스 감시 방법.

청구항 11.

제7항에 있어서, 이력 정보는 1개 이상의 선택된 데이터베이스 오브젝트에 관한 데이터베이스 액세스에 관한 것이고, 상기 이력 데이터로부터 데이터베이스 액세스의 빈도를 결정하는 단계는,

1일의 시간별의 오브젝트 액세스 빈도, 1일의 시간 및 오퍼레이팅 시스템 유저별의 오브젝트 액세스 빈도, 1일의 시간 및 데이터베이스 유저별의 오브젝트 액세스 빈도, 1일의 시간 및 장소별의 오브젝트 액세스 빈도, 1일의 시간 및 오퍼레이팅 시스템 유저, 데이터베이스 유저 및 장소 중의 2개 이상의 조합별의 오브젝트 액세스 빈도 중의 하나 이상의 빈도를 결정하는 단계를 더 포함하는, 데이터베이스 감시 방법.

청구항 12.

제7항에 있어서, 이력 정보는 1개 이상의 선택된 데이터베이스 유저에 관한 데이터베이스 액세스에 관한 것이고, 상기 이력 데이터로부터 데이터베이스 액세스의 빈도를 결정하는 단계는,

1일의 시간별의 유저 액세스 빈도, 1일의 시간 및 오퍼레이팅 시스템 유저별의 유저 액세스 빈도, 1일의 시간 및 데이터베이스 유저별의 유저 액세스 빈도, 1일의 시간 및 장소별의 유저 액세스 빈도, 1일의 시간 및 오퍼레이팅 시스템 유저, 데이터베이스 유저 및 장소 중의 2개 이상의 조합별의 유저 액세스 빈도 중의 하나 이상의 빈도를 결정하는 단계를 더 포함하는, 데이터베이스 감시 방법.

청구항 13.

제7항에 있어서, 상기 이력 정보는 1개 이상의 선택된 데이터베이스 유저 세션에 관한 데이터베이스 액세스에 관한 것이고, 상기 이력 데이터로부터 데이터베이스 액세스의 빈도를 결정하는 단계는,

세션마다의 페이지 판독의 수, 세션마다의 액세스 기간, 단위 시간마다의 페이지 판독의 수 중의 하나 이상의 빈도를 결정하는 단계를 더 포함하는, 데이터베이스 감시 방법.

청구항 14.

제1항에 있어서, 상기 목표로 되는 동작을 행하는 단계는,

경고를 발생시키는 단계, e-메일을 송신하는 단계, 보고를 생성하는 단계, 시각화를 행하는 단계 중의 하나 이상을 포함하는, 데이터베이스 감시 방법.

청구항 15.

장치의 장애에 따라 회복 설정으로 돌아오기 위한 명령의 1개 이상의 시퀀스를 구비하는 컴퓨터 판독 가능한 매체로서, 상기 명령은, 1개 이상의 프로세서에 의해 실행될 때, 상기 1개 이상의 프로세서에:

1명 이상의 유저가 상기 데이터베이스를 어떻게 사용하는지를 나타내는 유저 거동 데이터를 수집하는 단계;

상기 데이터를 이력 데이터로서 처리하고 기억하는 단계;

거동 패턴을 결정하기 위해 상기 이력 데이터를 분석하는 단계;

1명 이상의 유저가 상기 데이터베이스를 어떻게 사용했었는지를 나타내는 새로운 1쌍의 데이터를 수신하는 단계;

상기 새로운 1쌍의 데이터와 상기 거동 패턴과의 비교를 행하는 단계;

상기 비교에 근거하여 상기 새로운 1쌍의 데이터가 1쌍의 기준을 충족시키는지 여부를 판단하는 단계;

상기 새로운 1쌍의 데이터가 상기 1쌍의 기준을 충족시키는 경우, 상기 새로운 1쌍의 데이터가 이례의 활동을 나타내고 있다고 판단하는 단계; 및

목표로 되는 동작을 행함에 의해 상기 판단에 따르는 단계

를 실행시키는, 컴퓨터 판독 가능한 매체.

청구항 16.

제15항에 있어서, 상기 1개 이상의 프로세서에 의해 실행될 때, 상기 1개 이상의 프로세서에:

상기 새로운 1쌍의 데이터가 규칙 기반의 방침에 위반하고 있는지 여부를 판단하는 단계; 및

상기 새로운 1쌍의 데이터가 상기 규칙 기반의 방침에 위반하고 있는 경우, 상기 새로운 1쌍의 데이터는 이례의 활동을 나타내고 있다고 판단하는 단계를 실행시키는 명령을 더 포함하는, 컴퓨터 판독 가능한 매체.

청구항 17.

제16항에 있어서, 유저 거동 데이터를 수집하는 단계를 실행하는 명령은 데이터베이스 매니저의 감사 자취로부터 정보를 읽는 단계를 실행하는 명령을 더 포함하는, 컴퓨터 판독 가능한 매체.

청구항 18.

제17항에 있어서, 유저 거동 데이터를 수집하는 단계를 실행하는 명령은, 감시 레벨에서,

1개 이상의 선택된 데이터베이스 오브젝트에 관한 데이터베이스 액세스에 관한 정보;

1개 이상의 선택된 데이터베이스 유저에 관한 데이터베이스 액세스에 관한 정보; 및

1개 이상의 선택된 데이터베이스 유저 섹션에 관한 데이터베이스 액세스에 관한 정보 중 하나 이상으로부터 선택된 정보를 수집하는 단계를 실행하기 위한 명령을 더 포함하는, 컴퓨터 판독 가능한 매체.

청구항 19.

제17항에 있어서, 유저 거동 데이터를 수집하는 단계를 실행하는 명령은,

감시될 정보의 종류를 수신하는 단계;

상기 정보의 종류로부터 감시 레벨을 결정하는 단계; 및

결정된 상기 감시 레벨에 근거하여 상기 데이터베이스 매니저의 감사 옵션을 기동하는 단계를 실행하는 명령을 더 포함하는, 컴퓨터 판독 가능한 매체.

청구항 20.

제16항에 있어서, 거동 패턴을 결정하기 위해 상기 이력 데이터를 분석하는 단계를 실행하는 명령은, 상기 이력 데이터로부터 통계적 모델을 결정하는 단계를 실행하는 명령을 더 포함하는, 컴퓨터 판독 가능한 매체.

청구항 21.

제20항에 있어서, 상기 이력 데이터로부터 통계적 모델을 결정하는 단계를 실행하는 명령은,

상기 이력 데이터로부터 데이터베이스 액세스의 빈도를 결정하는 단계;

데이터베이스 액세스의 빈도에 관한 확률 함수를 결정하는 단계; 및

상기 확률 함수로부터 누적 확률 함수를 결정하는 단계를 실행하는 명령을 더 포함하는, 컴퓨터 판독 가능한 매체.

청구항 22.

제21항에 있어서, 상기 새로운 1쌍의 데이터와 상기 거동 패턴과의 비교를 행하는 단계를 실행하는 명령은,

상기 통계적 모델에 대하여 상기 새로운 1쌍의 데이터를 이용하여 가설을 검증하는 단계를 실행하는 명령을 더 포함하는, 컴퓨터 판독 가능한 매체.

청구항 23.

제22항에 있어서, 상기 통계적 모델에 대하여 상기 새로운 1쌍의 데이터를 이용하여 가설을 검증하는 단계를 실행하는 명령은,

상기 새로운 1쌍의 데이터에 관한 데이터베이스 액세스의 빈도를 결정하는 단계; 및

방호 기준 및 확률 함수 파라미터로부터 역치를 결정하는 단계를 실행하는 명령을 더 포함하는, 컴퓨터 판독 가능한 매체.

청구항 24.

제23항에 있어서, 상기 통계적 모델 패턴에 대하여 상기 새로운 1쌍의 데이터를 이용하여 가설을 검증하는 단계를 실행하는 명령은,

상기 새로운 1쌍의 데이터에 관한 데이터베이스 액세스의 빈도를 상기 역치와 비교하는 단계를 실행하는 명령을 더 포함하는, 컴퓨터 판독 가능한 매체.

청구항 25.

제21항에 있어서, 이력 정보는 1개 이상의 선택된 데이터베이스 오브젝트에 관한 데이터베이스 액세스에 관한 것이고, 상기 이력 데이터로부터 데이터베이스 액세스의 빈도를 결정하는 단계를 실행하는 명령은,

1일의 시간별의 오브젝트 액세스 빈도, 1일의 시간 및 오퍼레이팅 시스템 유저별의 오브젝트 액세스 빈도, 1일의 시간 및 데이터베이스 유저별의 오브젝트 액세스 빈도, 1일의 시간 및 장소별의 오브젝트 액세스 빈도, 1일의 시간 및 오퍼레이팅 시스템 유저, 데이터베이스 유저 및 장소 중의 2개 이상의 조합별의 오브젝트 액세스 빈도 중의 하나 이상의 빈도를 결정하는 단계를 실행하는 명령을 더 포함하는, 컴퓨터 판독 가능한 매체.

청구항 26.

제21항에 있어서, 이력 정보는 1개 이상의 선택된 데이터베이스 유저에 관한 데이터베이스 액세스에 관한 것이고, 상기 이력 데이터로부터 데이터베이스 액세스의 빈도를 결정하는 단계를 실행하는 명령은,

1일의 시간별의 유저 액세스 빈도, 1일의 시간 및 오퍼레이팅 시스템 유저별의 유저 액세스 빈도, 1일의 시간 및 데이터베이스 유저별의 유저 액세스 빈도, 1일의 시간 및 장소별의 유저 액세스 빈도, 1일의 시간 및 오퍼레이팅 시스템 유저, 데이터베이스 유저 및 장소 중의 2개 이상의 조합별의 유저 액세스 빈도 중의 하나 이상의 빈도를 결정하는 단계를 실행하는 명령을 더 포함하는, 컴퓨터 판독 가능한 매체.

청구항 27.

제21항에 있어서, 상기 이력 정보는 1개 이상의 선택된 데이터베이스 유저 세션에 관한 데이터베이스 액세스에 관한 것이고, 상기 이력 데이터로부터 데이터베이스 액세스의 빈도를 결정하는 단계를 실행하는 명령은,

세션마다의 페이지 관독의 수, 세션마다의 액세스 기간, 단위 시간마다의 페이지 관독의 수 중의 하나 이상의 빈도를 결정하는 단계를 실행하는 명령을 더 포함하는, 컴퓨터 판독 가능한 매체.

청구항 28.

제15항에 있어서, 상기 목표로 되는 동작을 행하는 단계를 실행하는 명령은,

경고를 발생시키는 단계, e-메일을 송신하는 단계, 보고를 생성하는 단계, 시각화를 행하는 단계 중의 하나 이상을 실행하는 명령을 포함하는, 컴퓨터 판독 가능한 매체.

청구항 29.

1명 이상의 유저가 상기 데이터베이스를 어떻게 사용하는지를 나타내는 유저 거동 데이터를 수집하는 수단;

상기 데이터를 이력 데이터로서 처리하고 기억하는 수단;

거동 패턴을 결정하기 위해 상기 이력 데이터를 분석하는 수단;

1명 이상의 유저가 상기 데이터베이스를 어떻게 사용했었는지를 나타내는 새로운 1쌍의 데이터를 수신하는 수단;

상기 새로운 1쌍의 데이터와 상기 거동 패턴과의 비교를 행하는 수단;

상기 비교에 근거하여 상기 새로운 1쌍의 데이터가 1쌍의 기준을 충족시키는지 여부를 판단하는 수단;

상기 새로운 1쌍의 데이터가 상기 1쌍의 기준을 충족시키는 경우, 상기 새로운 1쌍의 데이터가 이례의 활동을 나타내고 있다고 판단하는 수단; 및

목표로 되는 동작을 행함에 의해 상기 판단에 따르는 수단을 포함하는 장치.

청구항 30.

1명 이상의 유저가 상기 데이터베이스를 어떻게 사용하는지를 나타내는 유저 거동 데이터를 수집하며, 상기 데이터를 이력 데이터로서 처리하고 기억하며, 1명 이상의 유저가 상기 데이터베이스를 어떻게 사용했었는지를 나타내는 새로운 1쌍의 데이터를 수신하는 데이터 수집기;

거동 패턴을 결정하기 위해 상기 이력 데이터를 분석하는 데이터 분석기; 및

상기 새로운 1쌍의 데이터와 상기 거동 패턴과의 비교를 행하고, 상기 비교에 근거하여 상기 새로운 1쌍의 데이터가 1쌍의 기준을 충족시키는지 여부를 판단하고, 상기 새로운 1쌍의 데이터가 상기 1쌍의 기준을 충족시키는 경우, 상기 새로운 1쌍의 데이터가 이례의 활동을 나타내고 있다고 판단하고, 목표로 되는 동작을 행함에 의해 상기 판단에 따르는 이례 검출기를 포함하는 장치.

명세서

기술분야

본 발명은 데이터베이스 시스템을 관리하는 것에 관한 것이고, 특히, 본 발명은 데이터베이스 시스템을 감시하기 위한 방법 및 장치에 관한 것이다.

배경기술

네트워크화되는 시스템에 있어서 데이터를 보호하는 것은 중대하다. 네트워크시스템이 발전하는 것에 따라 귀중한 데이터의 기밀 보호를 위협할 수 있는 상황의 종류는 많고 증가하고 있다. 기밀 보호 위반이 일어나는 경우, 이를 검출할 수 있는 것이 중요하다. 그렇지 않으면, 종종 발생하는 것처럼, 데이터는 장래에 있어서 유사한 종류의 이벤트에 무방비인 상태로 된다.

네트워크 매니저가 귀중한 데이터를 보호할 때 직면하는 문제는, 예를 들어, 부정 침입 공격, 무단 사용, 인사이더(insider) 사기 또는 오용, 및 지식 정보 절도를 포함한다.

네트워크화되는 시스템이 겪는 공통의 문제의 일부에 관해서, 상이한 어프로치가 개발되어 왔다. 예를 들어, 방화벽 및 가상 프라이빗 네트워크는, 네트워크화되는 시스템을 외부 사이트로부터의 무단 액세스로부터 방호한다. 패스워드의 사용 또는 특권의 지정을 이용하는 액세스 제어는 일정 레벨의 보호를 제공한다. 그러나, 방화벽 및 가상 프라이빗 네트워크는, 데이터를 인사이더 절도로부터 보호할 수 없는데, 이는 패스워드가 도둑맞을 우려가 있기 때문이다; 특권은 관리가 어렵고, 유저는 자주 자신의 일의 범위 외의 데이터에 액세스할 수 있고, 비밀 보호는 쉽게 침해된다.

이 섹션에서 설명하는 어프로치는, 수행 가능한 어프로치지만, 반드시 이전에 생각되거나 수행된 어프로치는 아니다. 따라서, 달리 지시가 없는 한, 이 섹션에 기재된 어느 어프로치도 단지 이 섹션에 포함된다는 이유로 선행기술로서 적격인 것으로 가정되어서는 않된다.

발명의 상세한 설명

본 발명의 실시예들은 이례의 액티비티에 관해서 데이터베이스 시스템을 감시하는 기법을 제공한다. 감시중인 대상 데이터베이스에 관한 유저 거동 정보는, 이례의 액티비티를 검출하기 위해 자동적으로 수집되고, 분석되고, 1개 이상의 방침과 비교된다. 실시예는, 대상 데이터베이스에 관한 유저 거동 데이터를 감사 자취 및 동적 뷰를 포함하는 다양한 소스로부터 데이터베이스의 데이터베이스 관리 시스템과 협력하여 수집한다. 실시예는, 이례의 데이터베이스 액티비티를 검출하기 위

해, 통계 기반의 침입 검출(SBID) 및 규칙 기반의 침입 검출(RBID) 중의 하나 이상을 채용한다. 통계 기반의 침입 검출에서는, 수집되는 정보는 정규 사용 프로파일을 결정하기 위해 통계적 프로파일링을 이용하여 분석된다. 규칙 기반의 침입 검출에서는, 수집되는 데이터는 명시적인 기밀 보호 규칙과 비교된다. 정규 사용 패턴으로부터 이탈하는 의심스러운 데이터베이스 액세스가 검출된다면, 책임을 갖는 기밀 보호 담당자에게의 경고, 보고 생성, e-메일 경고등의 목표로 되는 동작이 행해진다.

일 실시예에서, 데이터베이스 액티비티에 관한 이력 정보로부터 정규 사용 패턴을 결정하는 메커니즘이 제공된다. 통계적으로 현저한 방식으로 정규 사용 패턴으로부터 이탈하는 데이터베이스 액세스는, 검출되고 경고된다. 사용 패턴의 일례는 1일의 시간별의 데이터베이스 액세스 빈도를 포함한다.

일 실시예에서, 사용자가 명시적인 기밀 보호 규칙을 특정할 수 있게 하는 메커니즘이 제공된다. 규칙에 위반하고 있는 데이터베이스 액세스가 검출되고 경고된다. 기밀 보호 규칙의 일부의 예는, 의심스러운 OS 유저 또는 장소를 포함한다.

일 실시예에서, 데이터베이스 액세스 정보는, 대상 데이터베이스를 제어하는 데이터베이스 관리 시스템에 의해서 제공되는 기능을 이용하여 수집된다. 예를 들어, 데이터베이스 관리 시스템은 감사 자취를 제공해도 좋고 이는 데이터베이스 액세스에 관한 정보를 포함하고 있다. 데이터베이스 관리 시스템은 또한, 현재의 유저 세션 및 리소스 이용과 같은 현재의 데이터베이스 사용에 관한 정보를 제공하는 동적 성능 뷰를 제공한다. 이 정보는 감사 자취로부터 얻어진 정보와 동시에 사용가능하다.

실시예는, 데이터베이스 오브젝트 레벨 감시, 데이터베이스 유저 레벨 감시, 및 데이터베이스 세션 레벨 감시를 포함하는 하나 이상의 레벨에서의 감시를 가능하게 한다. 데이터베이스 오브젝트 레벨, 어느 특정의 데이터베이스 오브젝트에 초점을 맞춘다. 데이터베이스 유저 레벨 감시는 데이터베이스 유저에게 초점을 맞춘다. 데이터베이스 세션 레벨 감시는, 데이터베이스 로그인 세션에 초점을 맞춘다. 실시예는, 다양한 침입 검출 어프로치에 근거하여 각 감시 레벨을 위한 다양한 기밀 보호 방침을 지원한다.

본 발명은 첨부 도면의 도면에 있어서 한정하기 위한 것이 아닌 예시적인 방법으로 설명되며, 동일한 도면 부호는 동일한 요소를 가리킨다.

실시예

개요

데이터베이스를 감시하는 방법 및 장치가 기재된다. 이하의 기재에서는, 설명을 위하여, 다수의 특정한 상세가 본 발명의 완전한 이해를 제공하기 위해 진술된다. 그러나, 본 발명은 이러한 특정 상세 없이 실행되어도 좋음은 명백하다. 다른 점에서는, 본 발명을 불필요하게 흐리는 것을 피하고자 주지의 구조 및 장치는 블록도의 형태로 도시된다.

도3a를 참조하면, 본 발명의 일 실시예에 따른 데이터베이스를 감시하기 위한 방법을 도시하고 있다. 도3a에 도시된 방법은 1명 이상의 유저가 데이터베이스를 어떻게 사용하는지를 나타내는 유저 거동 데이터를 수집하는 단계(블록 310)를 포함한다. 도시된 방법은 또한, 데이터를 이력 데이터로서 처리하고, 기억하는 단계(블록 320)를 포함한다. 거동 패턴을 결정하기 위해 이력 데이터를 분석하는 단계(블록 330)도 도시된 방법의 일부이다. 도시된 방법은 또한, 1명 이상의 유저가 데이터베이스를 어떻게 사용했는지를 나타내는 새로운 데이터 쌍을 수신하는 단계(블록 340)를 더 포함한다. 도시된 방법은 또한, 새로운 데이터 쌍과 거동 패턴과의 비교를 행하는 단계(블록 350)를 더 포함한다. 비교에 근거하여, 새로운 데이터 쌍이 1쌍의 기준을 충족시키는지 여부를 판단하는 단계(블록 360)도, 도시되는 방법의 일부이다. 도시되는 방법은 또한, 새로운 데이터 쌍이 1쌍의 기준을 충족시키는 경우에, 새로운 데이터 쌍이 이례적인 액티비티를 나타내고 있다고 판단하는 단계(블록 370)도 포함한다. 목표로 된 동작을 행하는 것에 의해 판단에 따르는 단계(블록 380)가 도시되는 방법에 포함되어도 좋다.

일 실시예에서, 유저 거동 데이터를 수집하는 단계는 데이터베이스 매니저의 감사 자취 또는 동적 성능 뷰(view)로부터 정보를 읽는 단계를 더 포함한다. 일 실시예에서는, 유저 거동 데이터를 수집하는 단계는, (1) 1개 이상의 선택된 데이터베이스 오브젝트에 관한 데이터베이스 액세스에 관한 정보, (2) 1개 이상의 선택된 데이터베이스 유저에 관한 데이터베이스 액세스에 관한 정보, 및 (3) 1개 이상의 선택된 데이터베이스 유저 섹션에 관한 데이터베이스 액세스에 관한 정보로부터 선택된 정보를 감시 레벨에서 수집하는 단계를 더 포함한다. 일 실시예에서는, 유저 거동 데이터를 수집하는 단계는, 감시될 정보의 종류를 수신하는 단계, 상기 정보의 종류로부터 감시 레벨을 결정하는 단계, 및 결정된 상기 감시 레벨에 근거하여 상기 데이터베이스 매니저의 감사 옵션을 기동하는 단계를 더 포함한다.

일 실시예에서는, 거동 패턴을 결정하기 위해 상기 이력 데이터를 분석하는 단계는, 상기 이력 데이터로부터 통계적 모델을 결정하는 단계를 더 포함한다. 일 실시예에서는, 상기 이력 데이터로부터 통계적 모델을 결정하는 단계는, 상기 이력 데이터로부터 데이터베이스 액세스의 빈도를 결정하는 단계, 데이터베이스 액세스의 빈도에 관한 확률 함수를 결정하는 단계, 및 상기 확률 함수로부터 누적 확률 함수를 결정하는 단계를 더 포함한다. 일 실시예에서는, 확률 함수는 푸아송 확률 분포, 또는 정규 확률 분포 등이라도 좋다.

일 실시예에서는, 상기 새로운 1쌍의 데이터와 상기 거동 패턴과의 비교를 행하는 단계는, 상기 통계적 모델에 대하여 상기 새로운 1쌍의 데이터를 이용하여 가설을 검증하는 단계를 더 포함한다. 일 실시예에서는, 상기 통계적 모델에 대하여 상기 새로운 1쌍의 데이터를 이용하여 가설을 검증하는 단계는, 상기 새로운 1쌍의 데이터에 관한 데이터베이스 액세스의 빈도를 결정하는 단계, 및 방호 기준 및 확률 함수 파라미터로부터 역치를 결정하는 단계를 더 포함한다. 일 실시예에서는, 상기 통계적 모델 패턴에 대하여 상기 새로운 1쌍의 데이터를 이용하여 가설을 검증하는 단계는, 상기 새로운 1쌍의 데이터에 관한 데이터베이스 액세스의 빈도를 상기 역치와 비교하는 단계를 더 포함한다.

이력 정보는 1개 이상의 선택된 데이터베이스 오브젝트에 관한 데이터베이스 액세스에 관한 정보를 포함한다. 다양한 실시예에 있어서, 상기 이력 데이터로부터 데이터베이스 액세스의 빈도를 결정하는 단계는, 1일의 시간별의 오브젝트 액세스 빈도, 1일의 시간 및 오퍼레이팅 시스템 유저별의 오브젝트 액세스 빈도, 1일의 시간 및 데이터베이스 유저별의 오브젝트 액세스 빈도, 1일의 시간 및 장소별의 오브젝트 액세스 빈도, 1일의 시간 또는 오퍼레이팅 시스템 유저, 데이터베이스 유저 및 장소 중의 2개 이상의 조합별의 오브젝트 액세스 빈도 중의 하나 이상의 빈도를 결정하는 단계 중의 하나 이상을 포함한다.

이력 정보는, 이력 정보는 1개 이상의 선택된 데이터베이스 유저에 관한 데이터베이스 액세스에 관한 정보를 포함한다. 다양한 실시예에 있어서, 상기 이력 데이터로부터 데이터베이스 액세스의 빈도를 결정하는 단계는, 1일의 시간별의 유저 액세스 빈도, 1일의 시간 및 오퍼레이팅 시스템 유저별의 유저 액세스 빈도, 1일의 시간 및 데이터베이스 유저별의 유저 액세스 빈도, 1일의 시간 및 장소별의 유저 액세스 빈도, 1일의 시간 또는 오퍼레이팅 시스템 유저, 데이터베이스 유저 및 장소 중의 2개 이상의 조합별의 유저 액세스 빈도 중의 하나 이상의 빈도를 결정하는 단계 중 하나 이상을 포함한다.

상기 이력 정보는 1개 이상의 선택된 데이터베이스 유저 세션에 관한 데이터베이스 액세스에 관한 정보를 포함한다. 다양한 실시예에 있어서, 상기 이력 데이터로부터 데이터베이스 액세스의 빈도를 결정하는 단계는, 세션마다의 페이지 판독의 수, 세션마다의 액세스 기간, 단위 시간마다의 페이지 판독의 수 중의 하나 이상의 빈도를 결정하는 단계 중 하나 이상을 포함한다.

다양한 실시예에서, 상기 목표로 되는 동작을 행하는 단계는, 경고를 발생시키는 단계, e-메일을 송신하는 단계, 보고를 생성하는 단계, 시각화를 행하는 단계 중의 하나 이상을 포함한다.

일 실시예에서는, 상기 새로운 1쌍의 데이터가 규칙 기반의 방침에 위반하고 있는지 여부를 판단하는 단계가 행해진다. 상기 새로운 1쌍의 데이터가 상기 규칙 기반의 방침에 위반하고 있는 경우, 상기 새로운 1쌍의 데이터는 이례의 활동을 나타내고 있다고 판단된다. 일 실시예에서는, 이례의 액티비티는 의심스러운 액티비티를 포함한다.

다른 점에서는, 본 발명의 실시예는, 전술의 프로세스를 실행하도록 설정되는 장치 및 컴퓨터 판독 가능한 매체를 포함한다.

용어

"데이터베이스"는 어떤 편성에 따라 데이터를 기억하기 위해 사용되는 임의의 데이터 구조를 포함한다. 데이터베이스는 관계 데이터베이스, 오브젝트(object) 데이터베이스, 계층형 데이터베이스, 네트워크 데이터베이스, 다차원 데이터베이스 등을 포함한다.

"데이터베이스 트리거(trigger)"는 데이터베이스 오브젝트에 관하여는 어느 특정의 이벤트에 따라, 예를 들면, 테이블 또는 뷰(view)가 선택 또는 수정되는 경우에는 언제든지, 자동적으로 호출되는 기억된 데이터베이스 절차를 가리킨다.

"데이터베이스 세션"은 유저 프로세서를 이용한, 유저의 데이터베이스에의 특정한 접속을 가리킨다. 세션은, 유저가 데이터베이스 애플리케이션에 접속한 시점으로부터, 유저가 데이터베이스 애플리케이션과의 접속을 해제하거나 데이터베이스 애플리케이션으로부터 나오는 시점까지 계속된다.

"자바 데이터베이스 연결(JDBC) API"은 사용자가 자바 프로그래밍 언어로부터 어느 데이터 소스에도 액세스할 수 있게 하는, 표준 SQL 데이터베이스 액세스 인터페이스이다.

"푸아송(Poisson) 분포"는 이벤트간의 대기시간이 지수적으로 분포하고 있는 경우의 간격에 있어서 이벤트의 수의 확률 분포이다.

"감사 자취(Audit Trail)"는 컴퓨터 이벤트의 일련의 기록이다. 이는, 시스템 액티비티(activity)를 감시하는 감사 시스템에 의해서 생성된다. 기록은, 컴퓨터 파일 또는 데이터베이스 테이블을 포함하지만, 이들로 한정되지 않는 다양한 형태로 기억되어도 좋다.

"특권"은, 네트워크 또는 데이터베이스의 사용자가 실행하도록 허가되는 1쌍의 액션(action) 또는 동작을 가리킨다. 또, 이에 대신하여, 특권은 인가 또는 1쌍의 인가로 언급될 수 있다.

시스템 설명

도1은 일 실시예에 있어서 데이터베이스를 감시하기 위한 기법이 실현될 수 있는 네트워크 컴퓨팅 시스템의 하이레벨 개요를 나타내는 블록도이다. 도1에 나타내는 일 실시예에 의하면, 데이터베이스 서버(130) 및 데이터베이스(132)로 구성된 데이터베이스 시스템에 네트워크(106)에 의해 결합되어 있다. 일 실시예에서는, 네트워크(106)는, 방화벽(124) 및 라우터(122)를 이용하여 인터넷(108)에 접속되어 있다. 방화벽(124)은 네트워크(106) 및 관련된 구성요소를, 인터넷(108)을 통해 송신되는 유해한 프로그램으로부터 보호하도록 설정되어 있다. 라우터(122)는 인터넷(108)과 네트워크(106) 사이의 네트워크 트래픽을 관리하고 제어한다.

데이터베이스 서버(130)는 데이터베이스(132)내의 데이터를 유지한다. 데이터베이스(132) 내에 있는 데이터의 일부는 네트워크(106)상에 있는 1명 이상의 유저들에게 중요할 수 있다. 중요한 데이터는 예를 들면 감사 기록, 고객 계정 정보, 및 종업원 급여 정보를 포함하나 이에 제한되지는 않는다. 데이터베이스(132)는 일부 실시예에서는 데이터베이스 서버(130)의 통합된 부분일 수 있다. 관리자 스테이션(144)은 관리자가 네트워크(106)상에서 관리 기능을 실현할 수 있게 해준다. 관리 기능은 유저의 액티비티를 포함하는, 네트워크(106)의 비밀보호를 감시하는 것을 포함해도 좋다. 일부 실시예에서는, 다른 엘리먼트 및 컴포넌트(도1에는 비도시)가 네트워크(106)와 연결되어도 좋다.

일 실시예에서 데이터베이스 감사 엔진(110)은 데이터 수집기(112), 데이터 분석기(114) 및 이레 검출기(116)를 포함한다. 데이터 수집기(112)는 데이터베이스(132)에 액세스하는 것에 관한 유저 거동 데이터를, 데이터베이스 서버(130)로부터, 지정된 간격으로, 또는 지정된 조건(수동 명령)의 발생시에 읽거나, 상기 데이터를 이력 데이터로서 기억하도록 설정되어 있다. 데이터 분석기(114)는, 데이터 수집기(112)에서 기억되는 이력 데이터에 대하여 분석 동작을 행하고, 데이터베이스(132)에 액세스하는 것에 관한 거동 패턴을 결정한다. 신규 데이터가 수신된다면, 이레 검출기(116)는, 이력 데이터로부터 결정되는 거동 패턴과, 신규 데이터와의 비교에 근거하여, 신규 데이터가 이레의 액티비티를 나타내고 있는지 여부를 판단한다. 일부 실시예에서는, 데이터베이스 감사 엔진(110)이, 데이터베이스 서버(130)의 성능에 현저한 영향을 주지 않고, 경고를 수집하고, 분석하고, 신호로 보내는 능력을 제공한다. 데이터 수집기(112), 데이터 분석기(114), 및 이레 검출기(116)에 의해서 행해지는 처리의 일례의 보다 상세한 설명이 도3a 내지 도3e를 참조하여 이하에 논의된다.

도2는 일 실시예에 있어서 예시적인 데이터베이스 감사 엔진내에서의 처리의 하이레벨 개요를 나타내는 블록도이다.

일 실시예에서 데이터베이스 감사 엔진(110)은 데이터베이스 서버와의 간섭을 감소시키기 위해 데이터베이스 서버(130)의 외부에서 작동한다. 일 실시예에서, 데이터 수집기(112)는, 예를 들면 데이터베이스 서버(130)상에서 에이전트를 실행해야 하는 것 없이 작동한다. 이러한 실시예에서 데이터 수집기(112)는 유저 거동에 관한 정보를, 데이터베이스 서버(130)에 의해 유지되는 감사 자취(84)로부터 수집하고/수집하거나 데이터베이스(132)로의 "관독 전용" 액세스를 채용하여 데이터를 수집한다. 일 실시예에서는, 데이터 수집기(112)는 감시될 정보의 종류에 근거하여 감시 레벨을 결정하고, 이 감시 레벨에 근거하여 데이터베이스 매니저(130)의 감사 옵션을 기동한다. 그 후, 데이터 수집기(112)는, 설정된 감사 옵션을 위해 데이터베이스 서버에 의해 작성되고 유지되는 감사 자취를 읽는다. 일부 실시예에서 데이터 수집기(112)는, 유저 섹션 및 데이터베이스 관리 시스템(DBMS)에 의해 유지되는 리소스 이용과 같은 데이터베이스 사용에 관한 정보를 포함하는 동적 성능 뷰(86)도 포함한다. 데이터 수집기(112)는 감사 자취(84) 및 동적 성능 뷰(86)로부터 얻는 유저 거동 데이터를 이력 데이터(88)로서 기억한다. 유저 거동 데이터를 수집하고, 이를 이력 데이터(88)로서 기억하기 위한 처리의 일례의 보다 상세한 설명이 도3b를 참조하여 이하에 논의된다.

데이터 분석기(114)는, 데이터 수집기(112)에 의해 기억되는 이력 데이터(88)에 대하여 1개 이상의 분석 프로세스를 실행한다. 일 실시예에서, 데이터 분석기(114)는 이력 데이터(88)의 분석을 포함하는 일련의 동작을 실행하여 거동 패턴(90)을 결정한다. 일 실시예에서, 데이터 분석기(114)는 데이터베이스 액세스의 빈도를 이력 데이터(88)로부터 결정한다. 데이터베이스 액세스의 빈도는 1일의 시간 등의 시간 단위에 관해서 계산되어도 좋다. 그 후 데이터 분석기(114)는 데이터베이스 액세스의 빈도에 관한 확률 함수를 결정한다. 이력 데이터를 분석하는 처리의 일련의 보다 상세한 설명이 도3c를 참조하여 이하에 논의된다.

새로운 1쌍의 데이터가 데이터베이스 서버(130)로부터 수신된다면, 이례 검출기(116)는 이 새로운 1쌍의 데이터를 이력 데이터로부터 결정되는 거동 패턴과 비교한다. 이례 검출기(116)는 신규 데이터와 이력 데이터(88)로부터 결정되는 거동 패턴과의 비교에 근거하여, 신규 데이터가 이례의 액티비티를 나타내고 있는지 여부를 판단한다. 일 실시예에서, 이례검출기(116)는 규칙 기반의 침입 검출을 행하기 위해, 신규 데이터를 기밀 보호 규칙(92)과 비교한다. 분석 동작의 1개 이상은, 기밀 보호 규칙(92) 또는 다른 규칙의 사용과, 데이터베이스 서버(130)의 관리자 또는 오퍼레이터(operator)에 의해 지정된 조건의 사용을 필요로 할 수 있다. 기밀 보호 규칙(92)은, 기밀 보호 위반이 일어나는지 여부를 이례 검출기(116)가 판단할 수 있게 하기 위한 메커니즘을 제공한다. 관리자 스테이션(144)은 기밀 보호 규칙(92)의 관리를 가능하게 한다. 이례적인 데이터가 일단 식별된다면, 이례 검출기(116)는 목표로 하는 동작을행한다. 예를 들어, 이례 검출기(116)는 e-메일 경고를 송신하고, 관리자 스테이션(144)에 침입을 신호로 알려도 좋다. 이례 검출기(116)는 또한 또는 이에 더하여, 보고(94)를 제공하거나 시각화를 생성해도 좋다.

일 실시예에서, 데이터베이스 감사 엔진(110)은 이벤트가 언제 데이터베이스 서버(130)에 의해 유지되는 데이터에 악영향을 줄 지를 검출한다. 예를 들어, 데이터베이스 감사 엔진(110)은, 인터넷(108)을 통해 네트워크(106)에 액세스하는 신원 불명의 유저로부터의, 데이터베이스 서버에 의하여 유지되는 데이터의 무단 액세스 및/또는 조작을 검출해도 좋다. 데이터베이스 감사 엔진(110)은 또한, 네트워크(106)의 유저가 언제, 데이터베이스 서버(130)에 의해서 기억되는 데이터를 고의로 또는 의도하지 않고 손상시킬지를 판단해도 좋다. 데이터베이스 감사 엔진(110)은, 네트워크를 통과하여 건네받았던 "멀웨어(malware)"의 존재를, 그 멀웨어가 데이터베이스 서버(130)에 의해 유지되는 데이터에 영향을 주는 때에 검출해도 좋다. 데이터베이스 서버(130)에 영향을 주고, 데이터베이스 감사 엔진(110)에 의해서 검출가능한 이벤트의 다른 예는, 도둑맞은 패스워드를 이용한 무단 액세스, 인사이드(insider) 사기, 오용, 또는 특권 남용을 포함하지만 이들로 한정되지 않는다. 인사이드 사기의 일례는, 은행의 출납계(teller)에 의한 귀중한 고객 계좌 정보의 복제이다. 특권 남용의 일례는 데이터베이스 관리자(DBM)에 의한 종업원 급여 정보의 액세스이다.

도3a는 일 실시예에 있어서 데이터 수집, 분석 및 이례 검출 처리의 하이레벨 개요를 나타내는 흐름도이다. 블록 31에서, 유저 거동 데이터를 포함하는 데이터 세트가 데이터베이스 서버로부터 수집된다. 블록 320에서, 유저 거동 데이터는 이력 데이터로서 기억된다. 블록 30에서, 이력 데이터는, 거동 패턴을 결정하기 위해 분석된다. 블록 340에서, 데이터베이스 서버로부터 새로운 1쌍의 데이터가 수신된다. 블록 350에서, 새로운 1쌍의 데이터는 거동 패턴과 비교된다. 블록 360에서, 비교에 근거하여 새로운 데이터 세트가 1쌍의 기준을 충족시키는지에 대한 판단이 내려진다. 블록 370에서, 신규 데이터가 이례의 액티비티를 나타내고 있는지에 대한 판단이 내려진다. 블록 380에서, 블록 370에 의해서 이례의 액티비티가 검출되는 경우에는, 목표로 하는 동작이 행해진다. 목표로 하는 동작은 다양한 실시예에 있어서, e-메일 경고를 송신하는 단계, 보고를 작성하는 단계, 시각화를 행하는 단계 등 중의 하나 이상을 포함하고 있어도 좋다.

본 발명의 실시예는, 데이터베이스 액세스에 관한 정보를 수집하고, 정보를 내부 데이터베이스에 이력 데이터로서 기억하기 위한 다양한 기법 중의 1개 이상을 이용한다. 데이터베이스 액세스에 관한 정보를 데이터베이스 관리 시스템으로부터 수집하는 다양한 방법은, 데이터베이스 트리거(trigger), 데이터베이스 트랜잭션(transaction) 변경 로그, 데이터베이스 감사 기능, 및 데이터베이스 동적 시스템 뷰를 포함하지만 이들로 한정되지 않는다.

감사 기능은, 다양한 시판되는 데이터베이스 관리 시스템에 의해 제공되어도 좋다. 이 감사 기능은 다양한 이벤트를 감사하도록 설정 가능하다. 감사 기능은, 데이터베이스 액세스 정보를 포함하는 감사 자취를 생성한다. 통상, 감사 기능에 따라서 추적되는 데이터베이스 액세스 정보는 데이터베이스 관리 시스템에 의존하지만, 많은 데이터베이스 관리 시스템은 유저 이름, 오브젝트 이름, 액션, 단말, 타임스탬프(time stamp)등의 감사 정보의 추적을 제공한다.

상업적으로 입수가능한 다양한 데이터베이스 관리 시스템은 또한 동적 시스템 뷰도 제공한다. 동적 시스템 뷰는 현재의 유저 세션(session) 및 리소스 이용에 관한 정보를 제공한다. 예를 들면, 어느 인기 있는 데이터베이스 관리 시스템은, 기밀 보호에 관련되는 몇 개의 동적 성능 뷰를 제공하고, V-\$SESSION은 각각의 현재 유저 세션에 관한 정보를 열거하고, V-\$

SESS_IO는 각 유저 세션에 관한 I/O 통계를 열거하고, V-\$SESSTAT는 유저 세션 통계를 열거하고, V-\$ACCESS는, 현재 로크되어 있는 오브젝트와 그에 액세스중인 세션을 나타내고, V-\$SQL은 SQL 풀에 있는 SQL 명령 텍스트를 나타내고 있다.

통상은 상주 기록인 감사 증거와 비교하여, 데이터베이스 동적 뷰는 통상, 비상주 데이터를 포함한다. 데이터베이스 동적 뷰는 데이터베이스의 정기적 샘플링을 취하는 것에 의해 감시 가능하다. 정기적 샘플링을 이용하는 어프로치는 감시 간격간에서 발생하는 어느 의심스러운 데이터베이스 액세스를 검출하는 데 실패할 수 있다. 이 가능성을 최소한으로 하기 위해서, 샘플링 간격이 꽤 짧아지도록 설정되어도 좋다. 이에 의해, 감사 어프로치는 감사되는 전 이벤트를, 추방(purge)될 때까지 감사 자취에 출현하도록 제공한다. 또한, 동적 뷰는, 데이터베이스 액세스에 관한 일반적인 정보를 비교적 조잡한(coarse) 세분성으로 제공하는 한편, 감사 자취는 비교적 보다 상세하고 특정한 정보를 데이터베이스 오브젝트 레벨의 세분성으로 제공한다. 일 실시예에서, 동적 뷰는 감사 자취를 이용할 수 없는 경우, 예를 들어, 데이터베이스 감사 기능이 액티브하지 않은 경우 등에, 보조 정보로서 또는 정보의 대체적인 원천으로서 사용가능하다.

데이터베이스 트리거는, 감시중의 데이터베이스로부터 정보를 수집하기 위한 다른 기법이고, 이는 실시간 감시가 데이터베이스의 유저에 의해서 매우 침입적이라고 생각되고 있지 않은 애플리케이션에 있어서 유용할 수 있다. 데이터베이스 트랜잭션 재실행 로그는, 관독 전용 액세스에 관한 정보가 필요로 되지 않는 애플리케이션에 있어서 유용할 수 있는, 데이터 변경에 관한 정보를 수집하기 위한 추가적인 기법이다.

도3b는 일 실시예에 있어서, 데이터 수집 처리의 하이레벨 개요를 나타내는 흐름도이다. 블록 311에서, 감시될 정보의 종류가 수신된다. 블록 312에서, 감시될 정보의 종류에 근거하여 감시 레벨이 결정된다. 블록 313에서, 감시 레벨에 근거하여 데이터베이스 매니저의 감사 옵션이 기동된다. 블록 314에서, 데이터 세트가 감사 자취로부터 독출된다. 블록 315에서, 데이터 세트가 처리된다. 블록 316에서 독출될 데이터가 더 있는지 여부를 판단하기 위해 검증이 행해진다. 독출될 데이터가 더 있는 경우, 제어는 블록 314에 돌아와 계속된다. 그 밖의 경우, 제어는 호출기로 돌아온다.

데이터 수집기는, 감사 자취 또는 동적 성능 뷰로부터 유저 거동 데이터를 수집하고, 정보를 처리하고, 그 데이터를 이력 데이터로서 기억한다. 이력 데이터는 예를 들면 내부 데이터베이스에 보존 가능하다. 일 실시예에서, 대상으로 되어 있는 각 액션에 관해서, 다양한 속성이 이력 데이터에 기억된다. 예를 들어, SELECT 또는 LOGIN 액션은, (1) 오퍼레이팅 시스템 유저 식별자(OSUSER), (2) 액션을 행하는 유저의 데이터베이스 유저 식별자(DBUSER), (3) 대상 개요 식별자(OBJECT), (4) 오브젝트의 소유자(OWNER), (5) 클라이언트 시스템 식별자(LOCATION), (6) 액션 식별자(ACTION), (7) 액션의 시점(TIMESTAMP), (8) 세션용 논리 관독의 수(READ), (9) 세션용 논리 기록의 수(WRITE), 및 (10) 성공 또는 실패 이유 코드(RETURNCODE) 등의 속성을 포함하지만, 이들로 한정되지 않는다.

데이터베이스 유저 거동 감시는 예를 들어, 데이터베이스 오브젝트 레벨, 데이터베이스 유저 레벨, 및 데이터베이스 세션 레벨을 포함하는 다른 초점을 각각 가지는 다른 관점으로부터 실행가능하다.

예를 들어, 일 실시예에서, 데이터베이스 오브젝트 레벨 감시는, 선택되는 중대한 또는 민감한 데이터베이스 오브젝트에 관해서 데이터베이스 액세스를 감시하는 것을 포함한다. 데이터베이스 오브젝트는 데이터베이스 테이블, 데이터베이스 뷰 또는 데이터베이스에 기억되는 절차일 수 있다. 데이터베이스 감시는, 이 오브젝트가 누구에게, 언제, 어디서, 및 어느 정도의 빈도로 임의의 유저에 의해서 액세스될지를 추적한다. 중대한 데이터베이스 오브젝트의 일례는 기업의 "중요원" 테이블이며, 이는 중요원의 급여 정보를 포함하고 있다.

다른 예에서, 일 실시예에 있어서, 데이터베이스 유저 레벨 감시는, 선택된 데이터베이스 유저에 의한 데이터베이스 오브젝트 액세스를 감시하는 것을 포함한다. 데이터베이스 감시는, 이 유저가 무엇에, 언제, 어디에서, 및 어느 정도의 빈도로 임의의 오브젝트에 액세스하는지를 추적한다. 선택된 데이터베이스 유저의 일례는 데이터베이스로부터 정보를 훔친 의심을 받고 있는, 불만을 갖는 종업원일 수 있다.

또한, 추가적인 예에서, 일 실시예에 있어서, 데이터베이스 세션 레벨 감시는 선택된 데이터베이스 유저에 의한 데이터베이스 접속 또는 로그인 세션을 감시하는 것을 포함한다. 데이터베이스 감시는, 이 유저에 의한 로그인 기간, 로그인 실패, 및 리소스 이용을 추적한다.

일 실시예에서, 데이터베이스 내에 있는 1개 이상의 다른 감사 옵션이, 데이터베이스 감사 엔진에 의해 실행될 감시의 레벨에 근거하여 자동적으로 인에이블(enable)된다. 인에이블되는 감사 옵션은 대상 데이터베이스의 데이터베이스 관리 시

시스템에 의존하고 있다. 예를 들면, 일 실시예에서는, 데이터베이스 오브젝트 레벨 감시를 지원하기 위해, 데이터베이스 감시 시스템은, 어느 특정 오브젝트에 관한 오브젝트 감사를 자동적으로 인에이블한다. 데이터베이스 유저 레벨 또는 세션 레벨 감시를 지원하기 위해, 이 시스템은, 어느 특정 유저에 관한 성명(statement) 감사를 자동적으로 인에이블한다.

데이터 분석

본 발명의 실시예는, 침입 검출 데이터 분석으로 1개 이상의 어프로치를 실현해도 좋다. 일 실시예에서는, 이례의 데이터베이스 액세스를 검출하기 위해, 통계 기반의 침입 검출(SBID) 및 규칙 기반의 침입 검출(RBID)이 모두 사용되어도 좋다. 통계 기반의 침입 검출을 이용하는 실시예에서는, 유저 거동 정보의 이력의 통계적 분석이, 유저 거동 패턴을 생성하기 위해 행해진다. 이러한 패턴으로부터 현저하게 일탈하는 그 뒤의 어느 데이터베이스 액세스는 이례의 액티비티를 나타내고 있다고 판단된다. 규칙 기반의 침입 검출을 이용하는 실시예는, 방침으로서도 알려지는 기밀 보호 규칙 또는 제약으로 구성된 지식 기반을 유지한다. 방침에 위반하는 데이터베이스 액세스는, 이례의 액티비티를 나타내고 있다고 판단된다.

도3c는 일 실시예에 있어서, 통계 기반의 침입 검출을 실현하는 데이터 분석 처리의 하이레벨 개요를 나타내는 흐름도이다. 블록 331에서, 데이터베이스 액세스의 빈도가 이력 데이터로부터 결정된다. 이례 데이터에 의거하여, 통계적 모델이 구축되고, 이례적인 액티비티의 검출에 사용하기 위해 타당성이 검증되어도 좋다. 이력 데이터의 통계적 분석은, 정규의 데이터베이스 액세스 레이트를 결정할 수 있다.

블록 332에서, 블록 331에서 결정되는 데이터베이스 액세스의 빈도로부터, 데이터베이스 액세스의 빈도에 관한 확률 함수가 결정된다. 데이터베이스 액세스의 빈도는 확률 분포에 적합 가능하다. 특정의 실시예에서는, 정규 확률 분포 또는 푸아송 확률 분포 등을 포함하지만 이들로 한정되지 않는 다양한 확률 분포가 사용되어도 좋다.

일례에서, 유저는 주간 또는 야간 동안 일정한 레이트로 랜덤하게 데이터베이스에 액세스한다. 데이터베이스 액세스의 레이트는, 주간과 야간에서 다른 경우가 있다. 이 1쌍의 기준 하에서, 푸아송 분포를 이용하여 이벤트간의 시간이 지수 분포에 따르는 데이터베이스 액세스 빈도를 기술해도 좋다. X는 간격마다의 랜덤 발생의 수, m은 간격마다의 랜덤 발생의 평균 수, P는 간격 내에서 n회 발생하는 X의 확률이라고 한다면, 아래와 같이 된다:

$$P(X = n) = e^{-m} \left[\frac{m^n}{n!} \right] \quad (1)$$

블록 333에서, 누적 분포 함수(CDF: Cumulative Distribution Function)가 결정 가능하다. 푸아송 분포를 이용하는 실시예에서는, 누적 분포 함수는, 식(2)에 나타나듯이 n보다 작거나 같은 값을 가지는 X의 확률을 준다.

$$F(n) = P(X \leq n) = \sum_{i=0}^n e^{-m} \left[\frac{m^i}{i!} \right] \quad (2)$$

데이터 분석기는, 확률 분포 함수의 패러미터값을 결정한다. 푸아송 분포의 경우, 이것은 이력데이터를 위한 간격마다의 랜덤 발생의 평균 수 m의 값이다.

예를 들어, 발생은 데이터베이스에 대하여 발행되는 SELECT 명령의 수로서 정의될 수 있고, 간격은 1일에 1시간으로 정의되어도 좋다. 다른 구현예에서, 발생은 다른 종류의 명령 또는 이벤트로서 정의되어도 좋고, 간격은 다른 시간 주기로서 정의되어도 좋다. 다음에 계속되는 처리에서는, 이례 검출기가 확률 함수에 근거하여 새로운 데이트 포인트를 이력 데이터와 비교한다.

다양한 실시예에 있어서, 데이터 분석기는 OS 유저, 데이터베이스 유저, 장소, 및 오브젝트를 포함하지만 이들로 한정되지 않는 다수의 차원의 속성에 근거하여 이력 데이터를 분석한다. 액세스 빈도는, 각 OS 유저, 데이터베이스 유저, 장소, 오브젝트, 또는 다수의 속성의 조합에 관해서 계산 가능하다. 다양한 차원에 근거하는 측정이 정량적인 비교를 위해 사용되어도 좋다.

예를 들어, 일 실시예에서는, 오브젝트 레벨 감시는 1일의 시간별의 오브젝트 액세스 빈도, 1일의 시간 및 OS 유저별의 오브젝트 액세스 빈도, 1일의 시간 및 데이터베이스 유저별의 오브젝트 액세스 빈도, 1일의 시간 및 장소별의 오브젝트 액세스 빈도, 1일의 시간 및 속성(OS 유저, 데이터베이스 유저, 및 장소)의 조합별의 오브젝트 액세스 빈도를 포함하는 다중차원의 오브젝트 액세스 빈도 규칙과 같은 측정치 중의 1개 이상을 포함하고 있어도 좋지만, 이들로 한정되지는 않는다.

다른 예에서, 일 실시예에 있어서, 유저 레벨 감시는, 1일의 시간별의 유저 액세스 빈도, 1일의 시간 및 OS 유저 액세스 빈도, 1일의 시간 및 데이터베이스 유저별의 유저 액세스 빈도, 1일의 시간 및 장소별의 유저 액세스 빈도, 1일의 시간 및 속성(OS 유저, 데이터베이스 유저, 및 장소)의 조합별의 유저 액세스 빈도를 포함하는 다중차원의 오브젝트 액세스 빈도 규칙과 같은 측정치 중의 1개 이상을 포함하고 있어도 좋지만, 이들로 한정되지는 않는다.

오브젝트 또는 유저 액세스 빈도에 더하여, 다양한 실시예에 있어서 다른 측정치가 세션 레벨 감시를 위해 사용가능하고, 예를 들어, 세션마다의 페이지 판독의 수에 의해서 측정되는 세션별 액세스 빈도, 세션마다의 시간 수에 의해서 측정되는 세션별 액세스 기간, 및 분당의 페이지 판독의 수에 의해서 측정되는 액세스 비율을 포함하지만, 이들로 한정되지는 않는다.

이레 검출

도3d는 일 실시예에 있어서, 이레 검출 처리의 하이레벨 개요를 나타내는 흐름도이다. 블록 351에서, 데이터베이스 액세스의 빈도가 새로운 1쌍의 데이터로부터 결정된다.

블록 352에서, 역치 빈도가 방호 기준 및 확률 함수 파라미터로부터 결정된다. 일 실시예에서, 확률 함수 파라미터는, 블록 331에서 데이터 분석기에 의해 미리 결정되는 이력 데이터의 액세스 빈도이다. 일 실시예에서는, 액세스 빈도는 1일의 시간별의 SELECT 동작의 평균 수이다.

예를 들어, 오전 2시에 관한 평균 액세스 빈도가 1.5인 것으로 데이터 분석기가 이력 데이터로부터 판단하고, 오전 2시에 관한 현재의 액세스 빈도가 7인 것을 나타내는 신규 데이터가 수신되는 경우 그 신규 데이터는 이상한가? 대답은 방호 기준에 의한다. 일 실시예에서는, 방호 기준은 확률 백분 등급으로서 표현되어도 좋다. 이레 검출기는 역치 액세스 빈도치를 방호 기준 확률 백분 등급 및 확률 함수 파라미터, 즉 블록 331에서 데이터 분석기에 의해 계산되는 이력 액세스 빈도로부터 결정된다. 역치를 넘는 빈도치는 어느 것도 검증에 합격하지 않고, 이레라고 생각된다. 방호 등급이 낮아짐에 따라, 이벤트가 이레라고 분류되는 것은 더욱 어려워지고, 실패 경고의 발생이 보다 적어진다.

예를 들어, 방호확률 기준이 0.1%로 특정되는 경우, 이레 검출기는 역치 n 을 식(3)에 나타나듯이 n 을 넘는 값을 가지는 확률이 0.1%보다 작아지도록 계산한다.

$$P(X > n) \approx 1 - P(X \leq n) < 0.1\% \quad (3)$$

이것은 식(4)에 나타난 것처럼 n 보다 작거나 같은 값을 가지는 확률이 99.9%보다 커지도록 역치 n 을 정하는 것과 동등하다.

$$F(n) = P(X \leq n) > 99.9\% \quad (4)$$

식(2)의 누적 분포 함수를, 식(4)로부터의 $F(n) > 99.9\%$, 및 값이 1.5인 m (확률 함수 파라미터, 이력 데이터의 평균 액세스 빈도)으로 대체하면, n 이 6인 것에 대하여 역치로 된다.

신규 데이터 세트의 액세스 빈도는 7로, 액세스 빈도 역치 6을 상회하기 때문에, 이레가 검출된다.

블록 353에서, (블록 351로부터의) 현재의 액세스 빈도의 값이, (블록 352로부터의) 역치 액세스 빈도와 비교된다.

일 실시예에서, 이레 검출기는 동적인 통계 패턴 및/또는 정적인 규칙 기반 방침의 어느 한쪽에 근거하여 이력 데이터에 있어서 의심스러운 데이터베이스 액세스를 검출하고 e-메일 경고를 생성한다. 보고 또는 그래프도 생성가능하다.

기밀 보호 방침을 이용하여 데이터베이스 유저 거동을 감시하는 것이 가능하다. 예를 들어, 일 실시예에서는, 기밀 보호 방침의 2개의 다른 카테고리, 즉 (1) 액세스 빈도 방침과 (2) 액세스 위반 방침이 있다. 액세스 빈도 방침은, 데이터베이스감사 엔진이 다양한 차원에 근거하여 1일의 시간별의 액세스 수를 방호할 수 있게 한다. 그러한 침입 검출은 전술한 것처럼 통계 기반이어도 좋고, 및/또는 규칙 기반이어도 좋다. 일 실시예에서, 방호 역치는 1일의 시간별의 액세스 수 등의 점에서 절대치로서 특정가능하다. 액세스 위반 방침은, 데이터베이스 감사 엔진이 명시적인 기밀 보호 규칙을 이용하여 각각의 데이터베이스 액세스를 방호할 수 있게 한다. 표1은 일 실시예에 있어서 데이터베이스 유저 거동을 감시하기 위해 사용한 다양한 기밀 보호 방침을 나타낸다.

[표 1]

기밀 보호 방침			
감시 레벨	분류	기밀 보호 방침	침입 검출 방법
오브젝트 레벨 감시	액세스 빈도	1일의 시간별의 오브젝트 액세스 빈도	통계 기반 또는 규칙 기반
		1일의 시간 및 OS 유저별의 오브젝트 액세스 빈도	통계 기반 또는 규칙 기반
		1일의 시간 및 데이터베이스 유저별의 오브젝트 액세스 빈도	통계 기반 또는 규칙 기반
		1일의 시간 및 장소별의 오브젝트 액세스 빈도	통계 기반 또는 규칙 기반
		다중차원 오브젝트 액세스 빈도 규칙	통계 기반 또는 규칙 기반
	액세스 위반	오브젝트 액세스 기밀보호 위반	규칙 기반
		의심이 가는 OS유저에 의한 오브젝트 액세스	규칙 기반
		의심이 가는 데이터베이스 유저에 의한 오브젝트 액세스	규칙 기반
		의심이 가는 장소로부터의 오브젝트 액세스	규칙 기반
		다중 차원 오브젝트 액세스 위반 규칙	규칙 기반
유저 레벨 감시	액세스 빈도	1일의 시간별의 유저 액세스 빈도	통계 기반 또는 규칙 기반
		1일의 시간 및 OS 유저별의 유저 액세스 빈도	통계 기반 또는 규칙 기반
		1일의 시간 및 데이터베이스 오브젝트별 유저 액세스 빈도	통계 기반 또는 규칙 기반
		1일의 시간 및 장소별의 유저 액세스 빈도	통계 기반 또는 규칙 기반
		다중차원 유저 액세스 빈도 규칙	통계 기반 또는 규칙 기반
	액세스 위반	유저 액세스 기밀보호 위반	규칙 기반
		의심스러운 OS 유저에 의한 유저 액세스	규칙 기반
		의심스러운 데이터베이스 오브젝트의 유저 액세스	규칙 기반
		의심스러운 장소로부터의 유저 액세스	규칙 기반
		다중 차원 유저 액세스 위반 규칙	규칙 기반
세션 레벨 감시	액세스 빈도	높은 독출율(페이지/분)	통계 기반 또는 규칙 기반
		과도한 독출 액티비티	통계 기반 또는 규칙 기반

		과도하게 긴 로그인 세션	통계 기반 또는 규칙 기반
	액세스 위반	로그인 실패	규칙 기반

		의심스러운 시간 프레임에서의 로그인	규칙 기반
		의심스러운 OS 유저에 의한 로그인	규칙 기반
		의심스러운 장소로부터의 로그인	규칙 기반
		다중 차원 세션 규칙	규칙 기반

예를 들어, 다양한 실시예에 있어서, 이하의 액세스 위반 규칙이 오브젝트 레벨 감시에 대하여 특정 가능하다. (1) 오브젝트 액세스 비밀 보안 위반 : 적절한 허용 없는 특정 오브젝트를 판독하고자 하는 실패한 시도는 어느 것이나 경고된다 (2) 의심스러운 OS 유저에 의한 오브젝트 액세스 : 무효인 OS 유저에 의한 특정 오브젝트의 성공적인 판독은 어느 것도 경고된다. 일 실시예에서는, 유효한 OS 유저의 리스트가 정의 가능하고, 리스트에 없는 OS 유저에 의한 액세스는 어느 것도 경고된다. 또 다른 실시 예로는, 무효인 OS 유저의 리스트가 정의 가능하고, 리스트에 있는 OS 유저에 의한 액세스는 어느 것도 경고된다 (3) 의심스러운 데이터베이스 유저에 의한 오브젝트 액세스 : 무효인 데이터베이스 유저에 의한 특정의 오브젝트의 성공적인 판독은 어느 것도 경고된다. 일 실시예에서는, 유효한 및/또는 무효인 데이터베이스 유저의 리스트가 정의 가능하다. (4) 의심스러운 장소로부터의 오브젝트 액세스 : 무효인 클라이언트 시스템으로부터의 특정의 오브젝트의 성공적인 판독은 어느 것도 경고된다. 일 실시예에서는 유효한 및/또는 무효인 장소의 리스트가 정의 가능하다. (5) 다중 차원 오브젝트 액세스 규칙 : 속성(OS 유저, 데이터베이스 유저, 및 장소)의 무효인 조합으로의 특정의 오브젝트의 성공적인 판독은 어느 것도 경고된다.

다른 예에서는, 다양한 실시예에 있어서, 이하의 액세스 위반 규칙이 유저 레벨 감시에 대하여 특정 가능하다. (1) 유저 액세스 기밀 보호 위반 : 특정의 데이터베이스 유저가 적절한 허가 없이 읽으려고 하는 실패한 시도는 어느 것도 경고된다. (2) 의심스러운 OS 유저에 의한 유저 액세스 : 무효인 Os 유저로부터의 특정의 데이터베이스 유저에 의한 성공적인 판독은 어느 것도 경고된다. 일 실시예에서는, 유효한 및/또는 무효인 OS 유저의 리스트가 정의 가능하다. (3) 의심스러운 데이터베이스 오브젝트의 유저 액세스 : 특정의 데이터베이스 유저에 의한 무효인 데이터베이스 오브젝트에의 성공적인 판독은 어느 것도 경고된다. 일 실시예에서는, 유효한 및/또는 무효인 오브젝트의 리스트가 정의 가능하다. (4) 의심스러운 장소로부터의 유저 액세스 : 무효인 클라이언트 시스템으로부터의 특정의 데이터베이스 유저에 의한 성공적인 판독은 어느 것도 경고된다. 일 실시예에서는, 유효한 및/또는 무효인 장소의 리스트가 정의 가능하다. (5) 다중 차원 유저 액세스 규칙 : 속성(OS 유저, 데이터베이스 오브젝트, 및 장소)의 무효인 조합으로의 특정의 데이터베이스 유저에 의한 성공적인 판독은 어느 것도 경고된다.

또한 추가적인 예에서는, 다양한 실시예에 있어서, 이하의 액세스 위반 규칙이 세션 레벨 감시에 대하여 특정 가능하고, 이의 액세스 위반 규칙은 다음과 같이 특정 가능하다: (1) 로그인 실패 : 무효 패스워드에 의한 로그인의 실패는 경고된다. (2) 의심스러운 시간 프레임에서의 로그인 : 특정된 정규의 시간 외의 로그인 시간은 경고된다. (3) 의심스러운 OS 유저에 의한 로그인 : 특정의 데이터베이스 유저 및 무효인 OS 유저에 의한 성공적인 로그인은 어느 것도 경고된다. 일 실시예에서는 유효한 및/또는 무효인 OS 유저의 리스트가 정의 가능하다. (4) 의심스러운 장소로부터의 로그인 : 무효의 클라이언트 시스템으로부터의 특정의 데이터베이스 유저에 의한 성공적인 로그인은 어느 것도 경고된다. 일 실시예에서는 유효한 및/또는 무효인 장소의 리스트가 정의 가능하다. (5) 다중 차원 세션 규칙 : 속성(OS 유저 및 장소)의 무효인 조합으로의 성공적인 로그인은 어느 것도 경고된다.

감시 예

일 실시예에 있어서, 데이터베이스 감시의 동작을, 도3e의 흐름도 및 도6a~도6m으로 도시되는 스크린 샷을 참조하여 기재되는 데이터베이스용 감시 동작을 설정하고 사용하는 일례를 이용하여 나타낸다. 일 실시예에서는, 감시 동작의 설정은, 그래픽 유저 인터페이스가 웹 브라우저를 이용하여 실현되는 상태로 행해진다. 도6a 내지 도6m에 도시되는 예시적인 유저 인터페이스 스크린에서는, 유저가 이전/다음의 유도 화살표에 따라 감시 동작을 설정하는 프로세스를 통하여 1스텝씩 실행할 수 있다. 또한 이에 대신하여, 유저는 패널 상부의 메뉴바로부터 항목을 선택하거나, 패널 좌측의 계층형 트리 뷰로부터 링크를 클릭해도 좋다.

유저는 도3e, 블록 410에 도시된 것처럼 감시될 데이터베이스를 여는 것에 의해 프로세스를 개시해도 좋다. 일 실시예에서는, 데이터베이스를 여는 단계는, 도6a에 도시된 것처럼, 호스트 이름, 데이터베이스 이름, 유저 이름 및 패스워드를 특정하는 것에 의해 데이터베이스 접속을 정의하는 단계를 포함한다. 유저는, 도6b에 도시된 것처럼, 특정된 데이터베이스에 접속한다.

블록 420에서, 유저는, 특정된 데이터베이스를 위한 감시 스케줄을 설정한다. 감시 스케줄을 설정하는 프로세스 동안 유저는, 그림 6c에 도시된 것처럼, 데이터 분석기가 어느 정도의 빈도로 유저 거동 데이터를 "학습"하고, 통계적 모델을 재구축할 지를 특정한다. 유저는 또한 도6c에 도시되는 스크린을 재차 이용하여, 이레 검출이 어느 정도의 빈도로 이레 데이터에 대하여 "방호"하고, 경고를 송신할지를 특정한다.

블록 430에서, 유저는 e-메일 수신자를 설정한다. 유저는, 예시적인 일 실시예에서, 도6d에 도시된 스크린을 이용하여 이레가 생긴 때에 누구에게 경고 e-메일을 송신할지를 특정한다.

블록 440에서, 유저는 감시 방침을 설정한다. 도6e 내지 도6f 에 도시된 스크린은, 예시적인 일 실시예에 있어서 감시 방침의 설정을 나타내고 있다. 유저는, 도6e에 도시된 것처럼, 감시하는 "중대한" 오브젝트를 설정한다. 유저는, 도6f에 도시된 것처럼, 이 오브젝트를 위해 기동하는 액세스 위반 방침을 선택한다. 유저는, 누가 이 오브젝트에 액세스하는 것이 허가될지를 특정한다. 다중 차원 오브젝트 규칙에 관해서는, 속성의 조합으로서 정의가능하다. 예를 들어, 도6g에 도시된 것처럼, 데이터베이스 유저 WANI는 자신이 OS 유저 IPLOCK/WTANG으로서, 클라이언트 시스템 W LINUX로부터 로그인되는 경우로 제한하여 이 오브젝트에 액세스 가능하다. 이 유저는 또한 그림 6h에 도시된 것처럼, 이 오브젝트를 감시하기 위해 기동하는 액세스 빈도 방침도 특정한다.

블록 450에서, 유저는 감시를 개시한다. 일 실시예에서는, 감시는, 도6i에 도시된 것과 같은 상태 스크린의 체크 박스를 클릭하는 것에 의해 개시된다.

블록 460에서, 유저는 경고 및/또는 그래프를 본다. 계층형의 일례에서는, 데이터베이스 유저 WANI에 속하는 데이터베이스 패스워드가 도둑맞고, 불법행위자가 도둑맞은 패스워드를 이용하여 그 패스워드가 사용을 위해 할당된 것 이외의 머신으로부터 데이터베이스 오브젝트에 액세스하려고 한다. 불법행위자가 사용을 시도한다면, 도6j에 도시된 것처럼 다중 차원 오브젝트 규칙의 액세스 위반을 일으킨다. 예를 들어, 설정된 다중 차원 오브젝트 규칙은, (도6g에 도시된 것처럼) 데이터베이스 유저 WANI가, OS 유저 IPLOCK/WANI에 의해서 그리고 장소 W LINUX로부터 이외에는 오브젝트 HR.EMP에 액세스할 수 없는 것을 나타내고 있다. 불법행위자는, 데이터베이스 유저 WANI로서, 다른 OS 유저 IPLOCK/CKCHOU에 의해서, 그리고 다른 장소 CKDESCTOP으로부터, 오브젝트에 액세스하려고 한다면, 이는 액세스 위반을 일으킨다. 목표로 되는 동작이 트리거 되어도 좋다. 도6j에 도시된 예에서는, 도6d에 도시된 스크린을 이용하여 정의되는 e-메일 수신자에게, e-메일 경고가 송신된다. 유저는 도6k에 도시된 것처럼 그래픽 유저 인터페이스를 이용하여 경고를 본다. 유저는 또한 도6l에 도시된 것처럼, 임의의 유저에 의한 임의의 오브젝트에 관한 액세스 패턴을 본다. 유저가 액세스 빈도 역치 또는 백분 등급에 위반하고 있는 경우, 경고가 마찬가지로 송신된다.

블록 470에서, 유저는 보고를 생성한다. 유저는 경고에 관한 개요 보고를 생성하고, 이는 도6m에 도시된 것처럼 문제의 분석을 지원할 수 있다. 도3e 및 도6a 내지 도6m을 참조하여 상술한 프로세스는 단지 일 실시예를 이용한 일례이다. 다른 실시예는, 간략화하기 위해 여기에서는 진술되지 않는 다른 프로세스 및 스크린을 포함하고 및/또는 스크린의 일부를 생략할 수 있다.

도4는 일 실시예에 있어서, 데이터베이스로의 액세스의 예시적인 확률 분포를 나타내는 그래프이다. 도4는, 24시간의 기간 동안의 어느 특정의 유저에 의한 데이터베이스 액세스 액티비티의 일례를 나타내고 있다. 도4에서 각 바(bar)는 이 유저에 의한 1시간당의 오브젝트 액세스의 수를 나타내고 있다. 도4에 도시된 예시적인 확률 분포에는, 유저가 데이터베이스에 액세스하는 확률의 2개의 피크를 갖고, 한편의 피크는 오전의 중반쯤의 시간에 일어날 가능성이 있고, 다른 피크는 오후의 중반쯤의 시간에 일어날 가능성이 있다. 이러한 시간 프레임 밖의 과도의 데이터베이스 액세스 액티비티는 의심스러울 수 있다.

도5는, 일 실시예에 있어서, 데이터베이스 감시 시스템의 하이레벨 개요를 나타내는 블록도이다. 도5에 도시된 것처럼, 데이터베이스 감시 시스템은 4층 아키텍처를 포함한다. 제1층에서는, 데이터베이스 감시 시스템은, 데이터베이스 감시 기능성으로의 액세스를 제공하기 위한 웹 브라우저를 포함한다. 일 실시예에서, 자바 서버 페이지(JSP)가 유저 인터페이스를 제공한다.

제2층에서는, 데이터베이스 감시 시스템은, 일 실시예에서는, 아파치 톰캣(Apache Tomcat)을 이용하여 실현되는 웹 서버와, 일 실시예에서는 포스트그레(Postgre) SQLTM 데이터베이스를 이용하여 실현되는 이력 데이터의 기억용의 내부 데이터베이스를 이용한다. 본 발명의 실시예는, 안전한 리눅스 오퍼레이팅 시스템과 동시에 실행되는 펜티엄(Pentium)TM 또는 동등의 하드웨어 플랫폼을 포함하지만, 이들에 한정되지 않는 임의의 컴퓨팅 플랫폼상에 있을 수 있다. 데이터베이스

감시 시스템의 구성요소는, 데이터 수집기, 데이터 분석기, 및 이레 검출기를 포함한다. 지지 구성요소는, (1) 유저가 스케줄 설정 및 방침 설정과 같은 실현화에 특유의 필요성에 의해서 데이터베이스 감시 시스템을 커스터마이즈(customize)할 수 있게 하는 콘피규레이터(configurator), (2) 지정된 기밀 보호 담당자에게 경고 메시지를 송신하는 e-메일 경고, (3) 진단 보고를 생성하는 보고 매니저, (4) 데이터베이스 유저 거동 패턴의 그래픽 표현을 생성하는 비주얼라이저(visualizer) 중의 1개 이상을 포함한다.

제3층에서는, 데이터베이스 감시 시스템은 자바 데이터베이스 연결(JDBC) API를 이용하여 타깃 데이터베이스에 액세스한다.

하드웨어 개요

일 실시예에서는, 도1에 도시된 컴퓨팅 환경(100)의 다양한 구성요소는, 1개 이상의 프로세서에 의해서 실행가능한 명령의 쌍으로 실현 가능하다. 도7은, 이러한 구성요소를 실현시키기 위해 사용될 수 있는 컴퓨터 시스템(700)의 블록도를 나타낸다. 컴퓨터 시스템(700)은, 정보를 통신하기 위한 버스(702) 또는 다른 통신 메커니즘과 정보를 처리하기 위해 버스(702)와 결합되는 프로세서(704)를 포함한다. 컴퓨터 시스템(700)은, 또한 프로세서(704)에 의해 실행될 명령 및 정보를 기억하기 위해 버스(702)에 결합됐던, 랜덤 액세스 메모리(RAM) 또는 다른 동적 기억 장치와 같은 메인 메모리(706)도 포함한다. 메인 메모리(706)는, 프로세서(704)에 의해 실행될 명령의 실행중에 일시적인 변수 또는 다른 중간 정보를 기억하기 위해서도 사용되어도 좋다. 컴퓨터 시스템(700)은 또한, 프로세서(704)용의 명령 및 정적 정보를 기억하기 위해 버스(702)에 결합되는 리드 온리 메모리(ROM)(708) 또는 다른 정적 기억장치를 포함한다. 자기 디스크 또는 광디스크와 같은 기억장치(710)가, 정보 및 명령을 기억하기 위해 제공되고, 버스(702)에 결합되어 있다.

컴퓨터 시스템(700)은, 정보를 컴퓨터 유저에 표시하기 위한 음극선관(CRT) 등의 디스플레이(712)에 버스(702)를 이용하여 결합되어도 좋다. 영숫자 키 및 다른 키를 포함하는 입력 장치(714)는, 정보 및 명령 선택을 프로세서(704)에 통신하는 버스(702)에 연결되어 있다. 유저 입력 장치의 다른 종류는, 방향 정보 및 명령 선택을 프로세서(704)에 통신하고, 디스플레이(712)상의 커서의 움직임을 제어하기 위한, 마우스, 트랙볼, 또는 커서 방향키와 같은 커서 제어(716)이다. 이 입력 장치는 통상 2개의 축, 즉 제1축(가령 x) 및 제2축(가령 y)에 있어서 2개의 자유도를 갖고, 이에 의해 상기 장치는 평면에 장소를 특정할 수 있다.

일 실시예에 의하면, 본 발명의 기능성은, 프로세서(704)가 메인 메모리(706)에 포함되는 1개 이상의 명령의 1개 이상의 시퀀스를 실행하는 것에 응답하여 컴퓨터 시스템(700)에 의해 제공된다. 그러한 명령은, 기억 장치(710)와 같은 다른 컴퓨터 판독 가능한 매체로부터 메인 메모리(706)에 판독되어도 좋다. 메인 메모리(706)에 포함되는 명령의 시퀀스의 실행에 의하여, 프로세서(704)는 본원에 기재된 프로세서 단계를 행하게 된다. 대안의 실시예에서는, 본 발명을 실현하기 위해, 소프트웨어 명령 대신에 또는 소프트웨어 명령과 조합하여 배선 접속 회로가 사용되어도 좋다. 따라서, 본 발명의 실시예는, 하드웨어 회로와 소프트웨어와의 어느 특정의 조합에 한정되지 않는다.

본원에 사용된 용어 "컴퓨터 판독 가능한 매체"는, 프로세서(704)에 명령을 실행용으로 제공하는 것에 관여하는 모든 매체를 가리킨다. 그러한 매체는, 불휘발성 매체, 휘발성 매체, 및 통신 매체를 포함하지만 이들로 한정되지는 않는 많은 형태를 취할 수 있다. 불휘발성 매체는 예를 들어, 기억 장치(710) 등의 광디스크 또는 자기 디스크를 포함한다. 휘발성 매체는, 메인 메모리(706) 등의 동적 메모리를 포함한다. 통신 매체는 버스(702)를 구성하는 배선을 포함하는, 동축 케이블, 동선, 및 광파이버를 포함한다. 통신 매체는 또한, 무선 주파수 및 적외선 데이터 통신중에 발생하는 것과 같은 음파 또는 광파의 형태도 취할 수 있다.

컴퓨터 판독 가능한 매체의 일반적인 형태는, 예를 들면 플로피디스크, 플렉시블 디스크, 하드디스크, 자기테이프, 또는 임의의 다른 자기 매체, CD-ROM, 임의의 다른 광 매체, 펀치카드, 종이테이프, 구멍의 패턴을 가지는 임의의 다른 물리적 매체, RAM, PROM, EPROM, FLASH-EPROM, 임의의 다른 메모리 칩 또는 카트리지, 이하에 설명할 반송파, 또는, 컴퓨터가 이로부터 판독할 수 있는 임의의 다른 매체를 포함한다.

컴퓨터 판독 가능한 매체의 다양한 형태는, 프로세서(704)에 1개 이상의 명령의 1개 이상의 시퀀스를 실행하는 데 관여하고 있어도 좋다. 예를 들면, 명령은 우선, 원격 컴퓨터의 자기 디스크상에 유지되어도 좋다. 원격 컴퓨터는 명령을 그 동적 메모리에 로드하고, 전화 회선을 통하여 모뎀을 이용하여 명령을 송신할 수 있다. 컴퓨터 시스템(700)에 국부적인 모뎀은, 전화 회선상의 데이터를 수신하고, 적외선 송신기를 이용하여 데이터를 적외선 신호로 변환할 수 있다. 적외선 검출기는 적외선 신호로 반송되는 데이터를 수신할 수 있고, 적절한 회로가 데이터를 버스(702)상에 배치할 수 있다. 버스(702)는

데이터를 메인 메모리(706)에 반송하고, 이로부터 프로세서(704)가 명령을 검색하고 실행한다. 메인 메모리(706)에 의해서 수신되는 명령은, 프로세서(704)에 의한 실행의 앞 또는 뒤의 어느 한쪽으로, 기억장치(710)에 선택적으로 기억되어도 좋다.

컴퓨터 시스템(700)은 또한, 버스(702)에 결합되는 통신 인터페이스(718)도 포함한다. 통신 인터페이스(718)는, 로컬 네트워크(722)에 접속되는 네트워크 링크(720)에 쌍방향 데이터 통신 결합을 제공한다. 예를 들어, 통신 인터페이스(718)는 데이터통신 접속을 대응하는 종류의 전화 회선에 제공하는 종합 정보 통신망(ISDN) 카드 또는 모뎀일 수 있다. 다른 예로서, 통신 인터페이스(718)는, 데이터통신 접속을 호환성 있는 LAN에 제공하는 근거리 통신망(LAN) 카드일 수 있다. 무선 링크도 실현될 수 있다. 임의의 그러한 실현예에서, 통신 인터페이스(718)는, 다양한 종류의 정보를 나타내는 디지털 데이터 스트림을 반송하는 전기신호, 전자신호, 또는 광신호를 송수신한다.

네트워크 링크(720)는, 통상 1개 이상의 네트워크를 이용하여, 다른 데이터 장치에 데이터 통신을 제공한다. 예를 들어, 네트워크 링크(720)는, 로컬 네트워크(722)를 이용하여, 호스트컴퓨터(724)에, 또는 인터넷 서비스 제공자(ISP)(726)에 의해 운용되는 데이터 장치에 접속을 제공해도 좋다. ISP(726)는 다음에, 현재 일반적으로 "인터넷"(728)이라고 불리는 전 세계적 패킷 데이터 통신 네트워크를 이용하여, 데이터 통신 서비스를 제공한다. 로컬 네트워크(722) 및 인터넷(728)은 모두 디지털 데이터 스트림을 반송하는, 전기신호, 전자신호, 또는 광신호를 사용한다. 컴퓨터 시스템(700)에, 그리고 컴퓨터 시스템(700)으로부터, 디지털 데이터를 반송하는 다양한 네트워크를 통한 신호, 네트워크 링크(720)상의 신호, 및 통신 인터페이스(718)를 통한 신호는, 정보를 운반하는 반송파의 예시적인 형태이다.

컴퓨터 시스템(700)은, 네트워크, 네트워크 링크(720), 및 통신 인터페이스(718)를 이용하여, 메시지를 송신하고, 프로그램 코드를 포함하는 데이터를 송신한다. 인터넷의 예에서는, 서버(730)는 애플리케이션 프로그램용의 요구되는 코드를, 인터넷(728), ISP(726), 로컬 네트워크(722), 및 통신 인터페이스(718)를 이용하여 송신해도 좋다. 수신된 코드는, 수신되는 때에 프로세서(704)에 의해서 실행되어도 좋고, 및/또는 이후의 실행을 위해 기억장치(710) 또는 다른 불휘발성 기억장치에 기억되어도 좋다. 이처럼, 컴퓨터 시스템(700)은, 반송파의 형태로 애플리케이션 코드를 취득할 수 있다.

전술한 명세서에 있어서, 본 발명의 특징의 실시예를 참조하여 기재되었지만, 이는 그와 같이 한정되어 해석되지 않아야 하는 점에 유의하여야 한다. 다양한 수정이 당업자에 의해서, 본 개시의 이점을 이용하고, 본 발명의 일탈하지 않고 행해져도 좋다. 따라서, 본 발명은, 이를 예시하기 위해 사용된 특징의 실시예에 의해서 한정되지 않아야 하고, 발행되는 특허청구범위의 범위에 의해서만 한정되어야 한다. 따라서, 명세서 및 도면은, 한정적이라기보다는 오히려 예시적이라고 생각되어야 한다.

도면의 간단한 설명

도1은 데이터베이스를 감시하는 기법이 일 실시예에서 실현될 수 있는 네트워크 컴퓨팅 시스템의 하이레벨 개요를 나타내는 블록도이다.

도2는 일 실시예에 있어서 예시적인 데이터베이스 감사 엔진에서의 프로세스의 하이레벨 개요를 나타내는 블록도이다.

도3a 내지 도3e는 일 실시예에 있어서 수집, 분석 및 이레 검출 처리의 하이레벨 개요를 나타내는 블록 흐름도이다.

도4는 일 실시예에 있어서 데이터베이스로의 액세스의 예시적인 확률 분포를 나타내는 그래프이다.

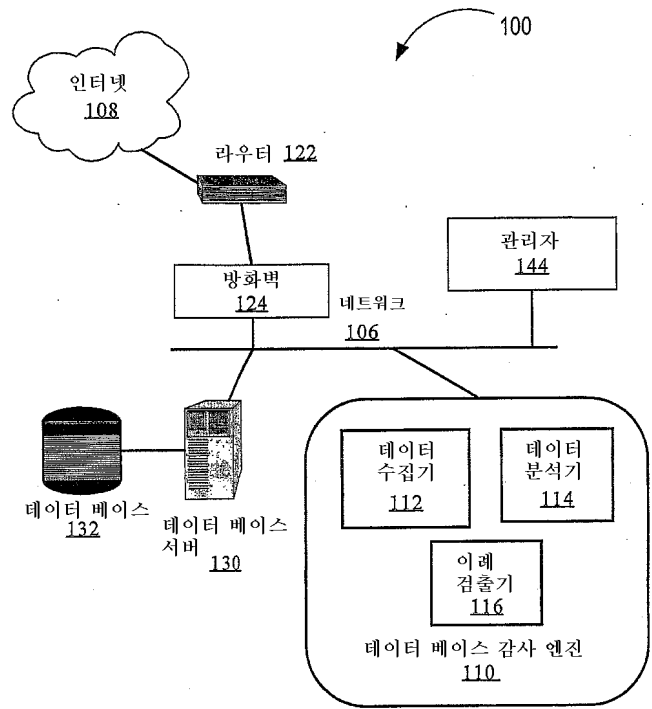
도5는 일 실시예에 있어서 데이터베이스 감시 시스템의 하이레벨 개요를 나타내는 블록도이다.

도6a 내지 도6m은 일 실시예에 있어서 감시 동작을 설정하는 일례를 나타내는 스크린 샷이다.

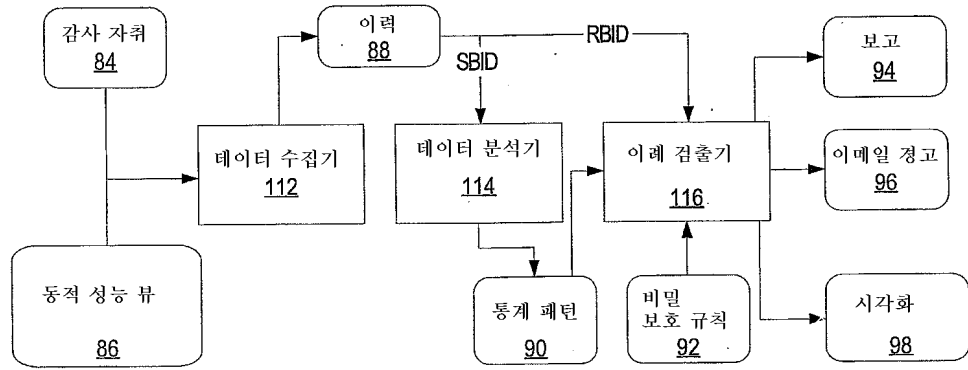
도7은 일 실시예의 1개 이상의 구성요소를 구체화하기 위해 사용될 수 있는 대표적인 컴퓨팅 시스템을 나타내는 하드웨어 블록도이다.

도면

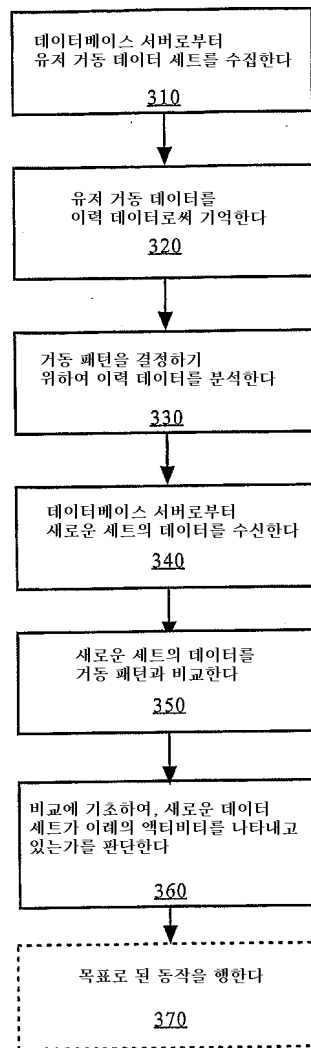
도면1



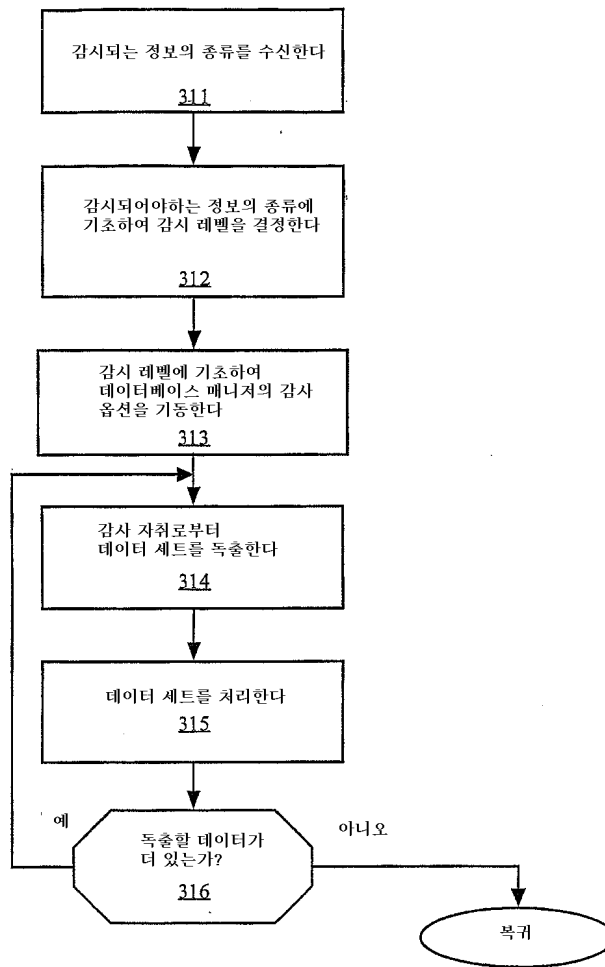
도면2



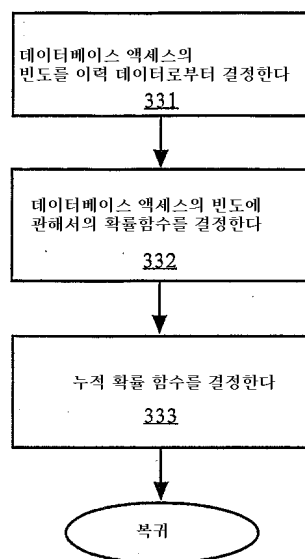
도면3a



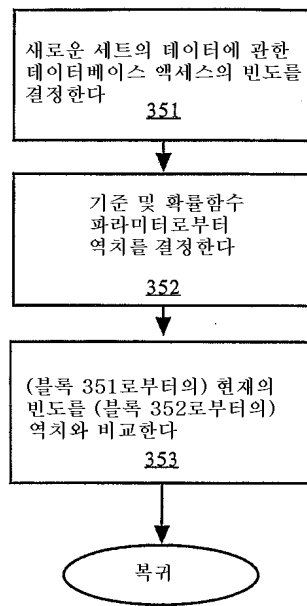
도면3b



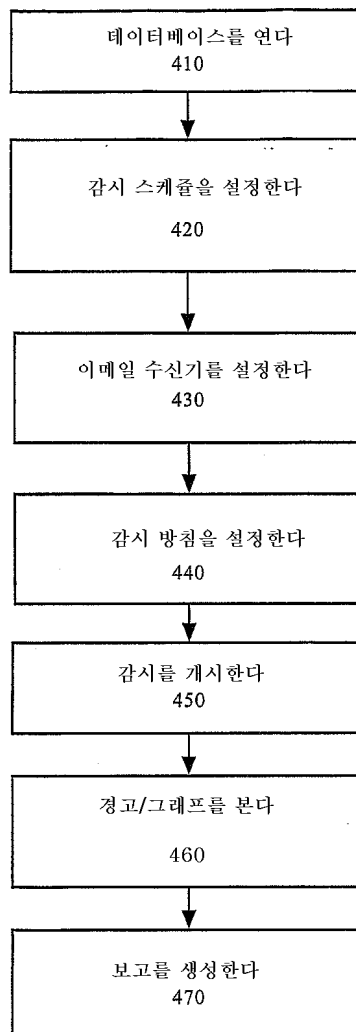
도면3c



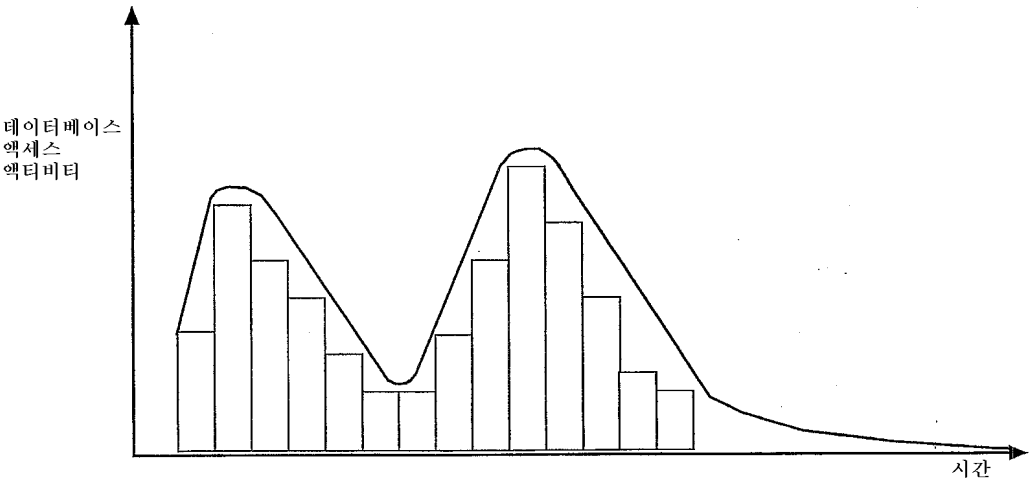
도면3d



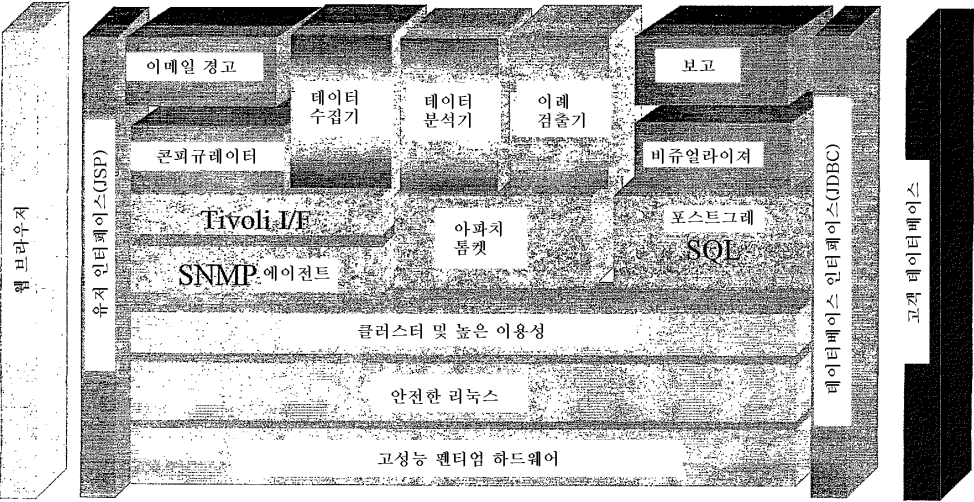
도면3e



도면4



도면5



도면6a

iPLOCKS User Behavior Monitor - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address http://dardzsoftphiles.com/fsp/figar/home.asp

Back Forward Stop Search Media

iPLOCKS Database Set Defaults Set Policies Analyze Help

My Account About iPLOCKS Product Overview Documentation Logout

Create New Database Connection

* required fields

Database Connection Name *	Database Server Type *	Monitored Application Name	Database Location
ctxstc2	Oracle		
Database Name *	Database Server Password *	Region	
198.245.1.32:1521	system	Division	
ctxstc2	*****	Business Unit	
Oracle	DBA1 Name	Usage	
	DBA1 Tel	DBA2 Name	
	DBA1 Email	DBA3 Tel	
		DBA2 Email	

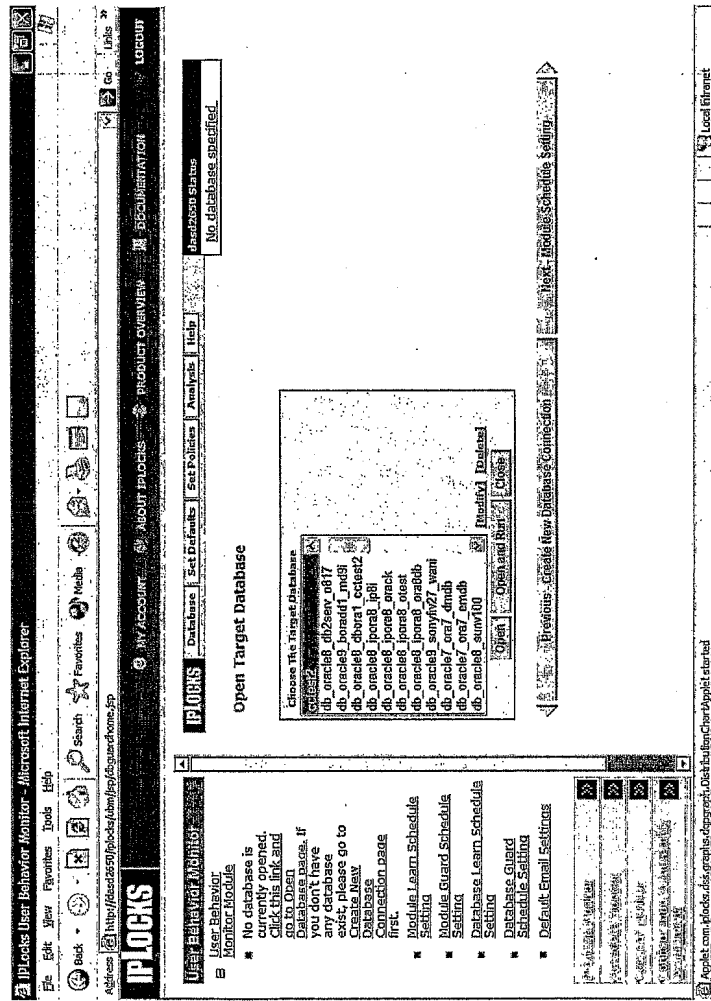
[Create] [Update]

No database specified.

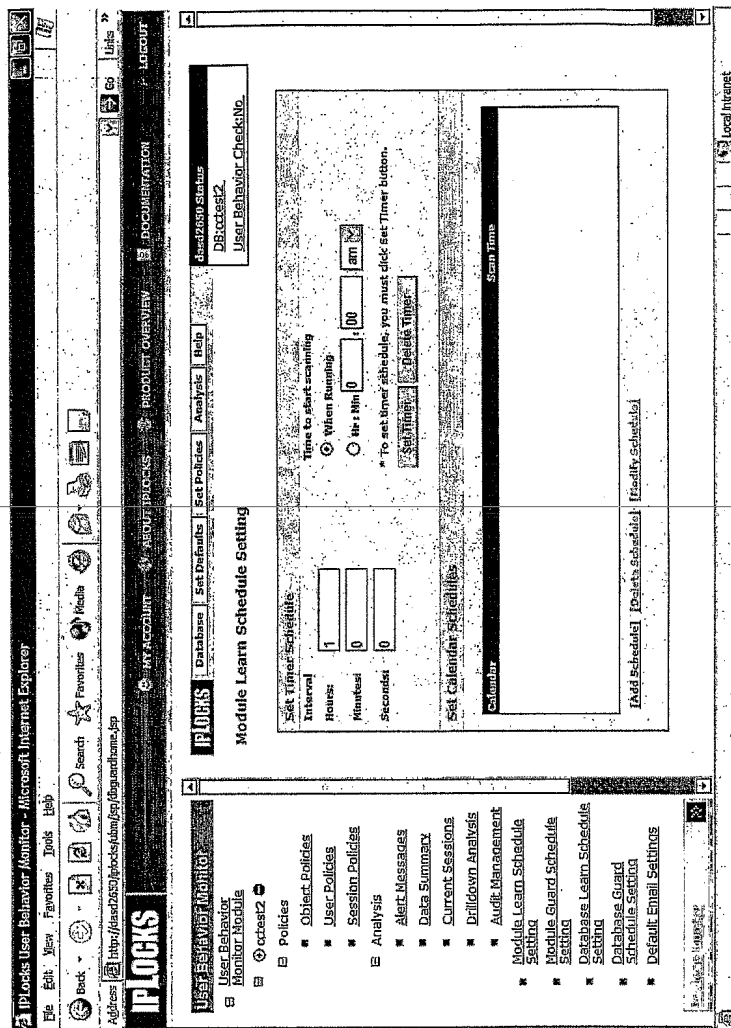
User Behavior Monitor

- User Behavior Monitor Module
 - No database is currently loaded.
Click this link and go to Open Database page. If you don't have any database connection, click Create New Database Connection page first.
- Module Learn Schedule Setting
- Module Guard Schedule Setting
- Database Learn Schedule Setting
- Database Guard Schedule Setting
- Default Email Settings

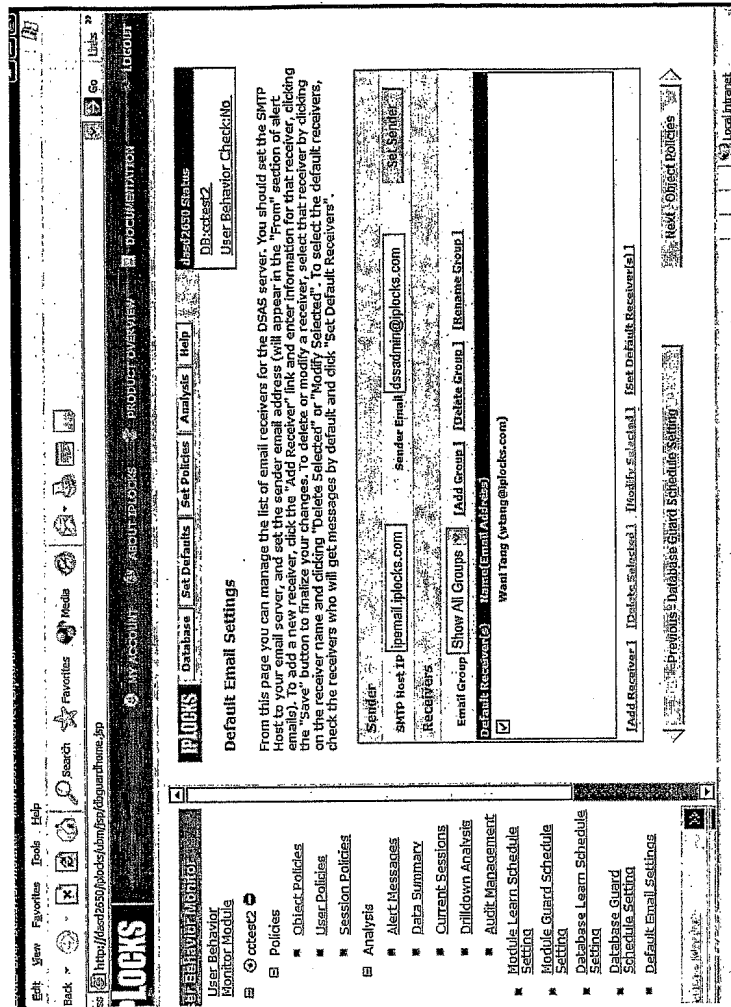
도면6b



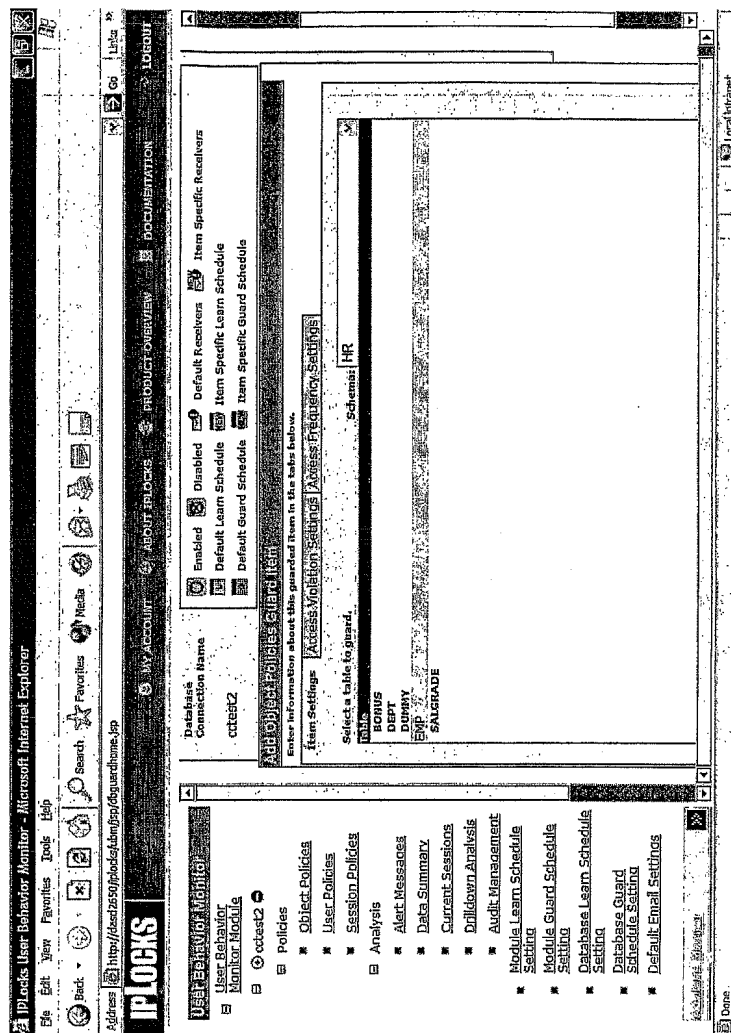
도면6c



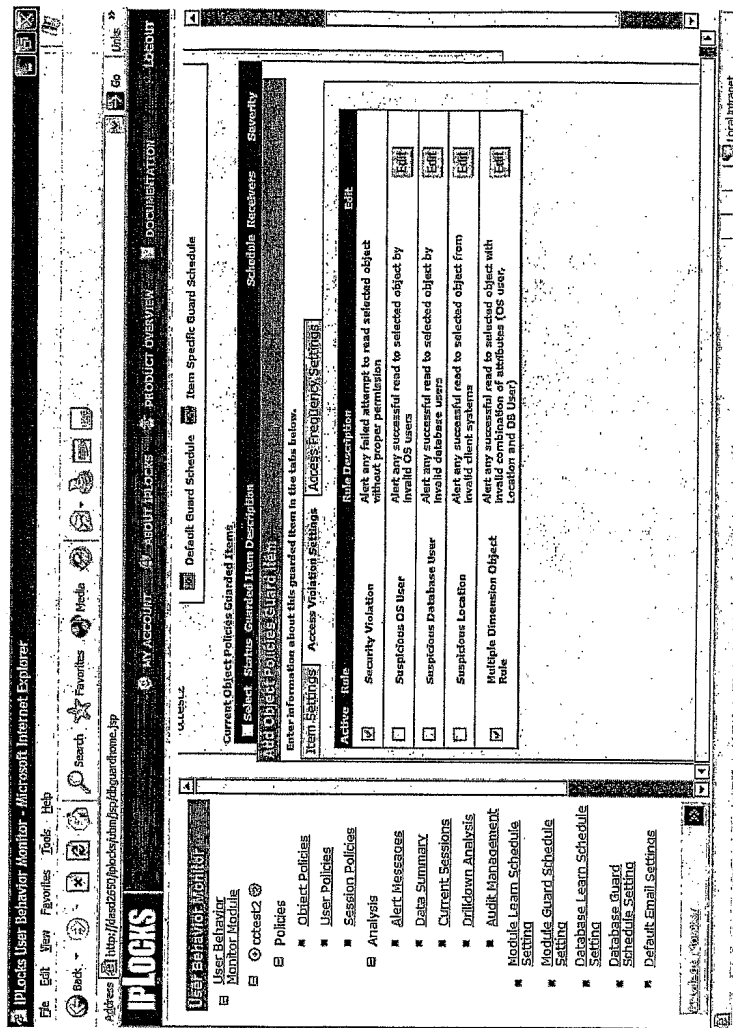
도면6d



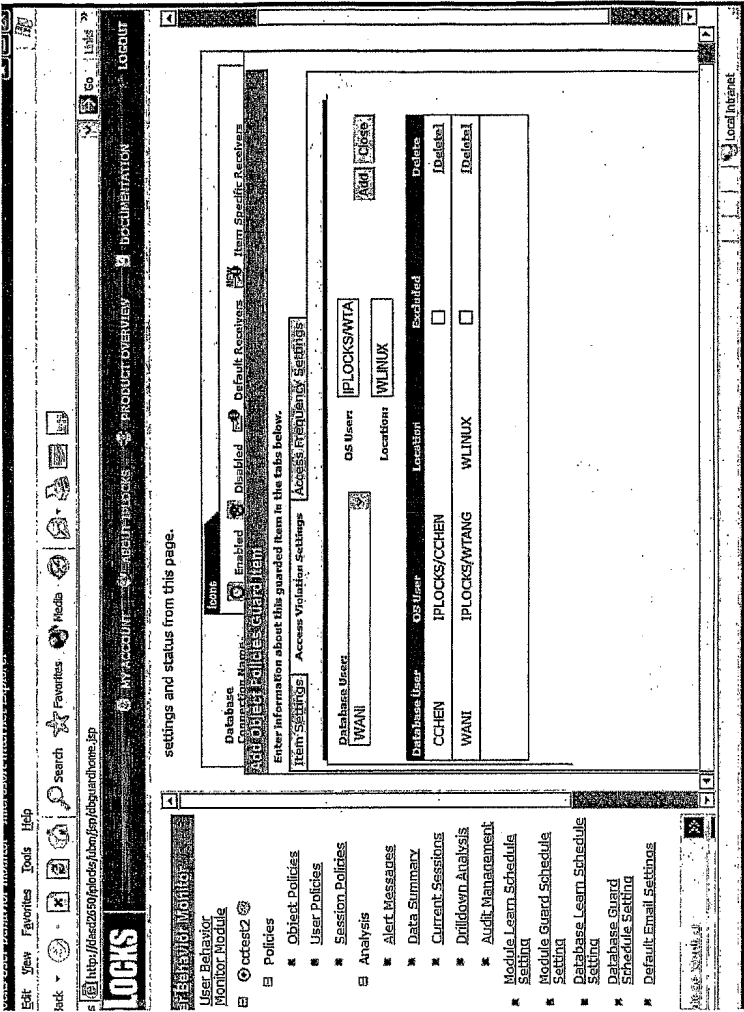
도면6e



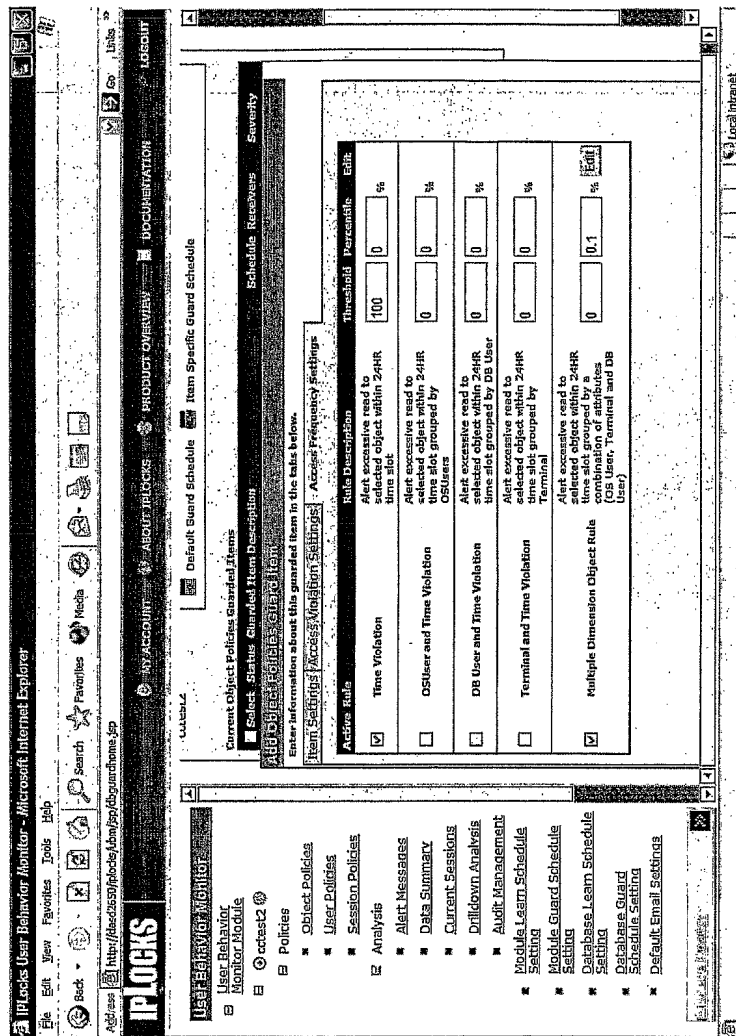
도면6f



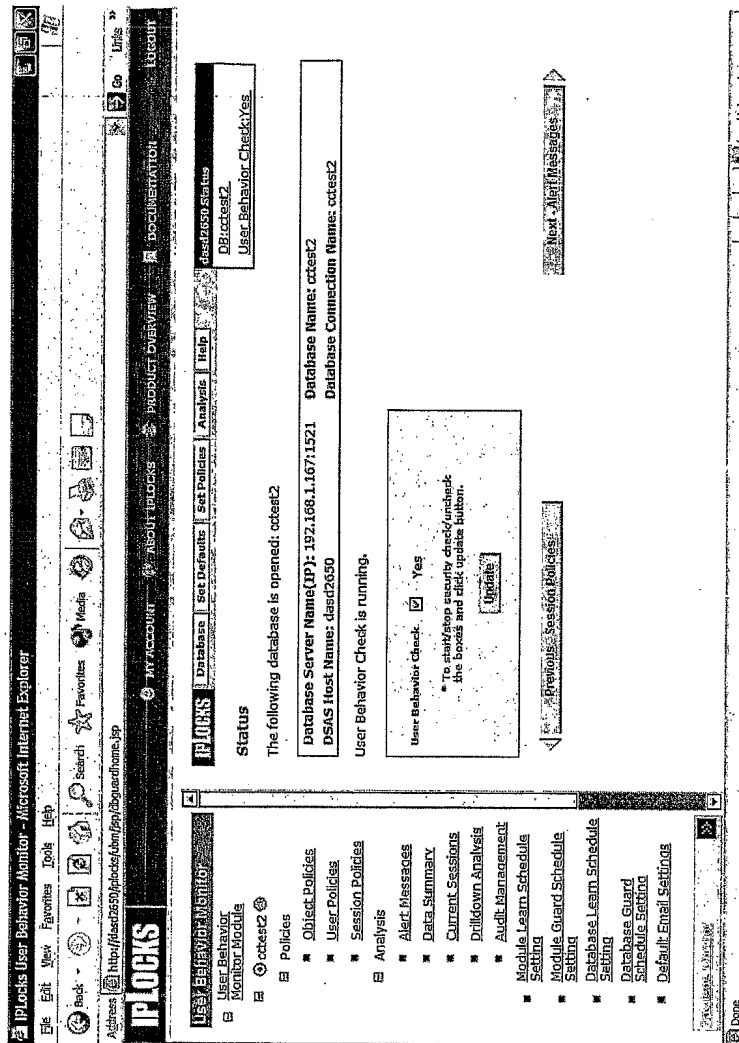
도면6g



도면6h



도면6i



도면6j

cautionary UBM alert raised from cctest2 (Object Policies:HR EMP) - Message (HTML) - Unicode (UTF-8)

File Edit View Insert Format Tools Actions Help

Reply Reply to All Forward

Sent: Fri 1/23/2004 2:11 PM

From: dsadmin@iplodes.com

To: Wan Tang

Cc:

Subject: cautionary UBM alert raised from cctest2 (Object Policies:HR EMP)

Brief Description:

Alarm ID: 1,782

Severity: cautionary

Violated Policy: Object Policies

Guarded Item: HR EMP

Alarm Generated Time: 2004-01-23 14:24:22

Application: UBM@dascl2650:80

Database: CCTEST2@192.168.1.166:1521

Detailed Description:

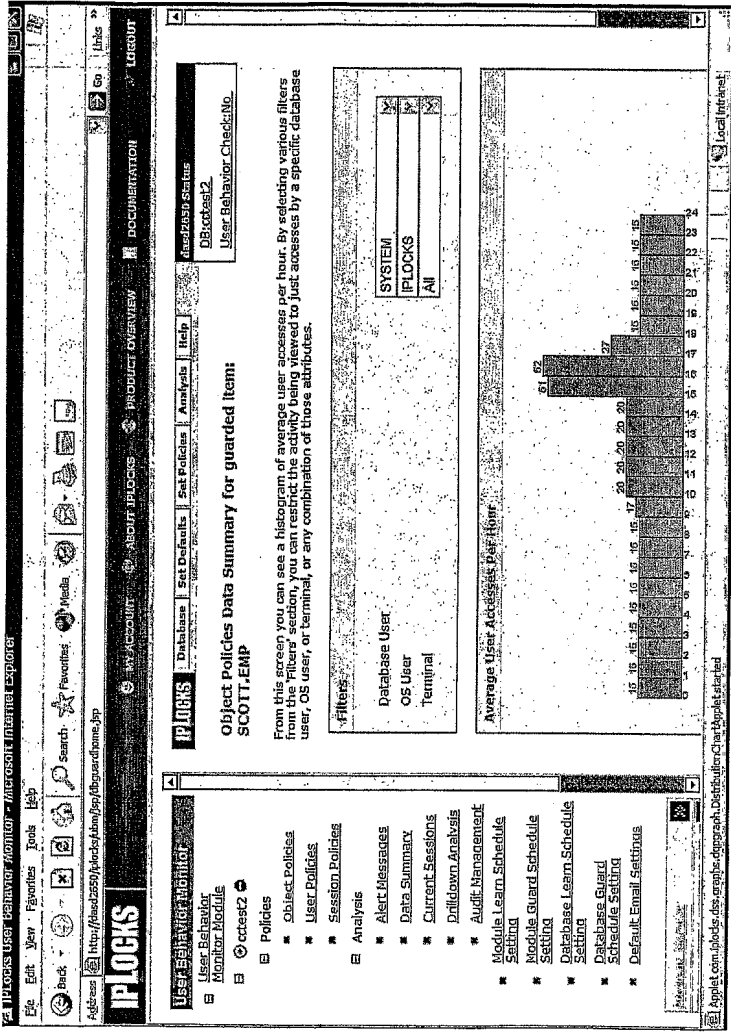
Database object HR EMP is accessed by DB user WANI at 1/23/04 2:11 PM with suspicious attribute combination:

Terminal=CKDESKTOP, OS User=IPLOCKSCKCHOU and DB User=WANI

To update alarm status use the link: [Update Status](#)



도면61



도면6m

IPLOCKS Alarm Report Manager - Microsoft Internet Explorer

Address: http://head250iplocks/destreport/asp/bugandchase.asp

IPLOCKS

File Edit View Favorites Tools Help

Back Search Favorites Media Print

IPLOCKS Alarm Report Manager

- Alarm Report Manager
- Current Reports
- Schedule Setting
- Default Email Settings

Preview Report Setting

Report Information

Report Name: UBM-ccast2
 Date Generated: 2004-01-16 14:17:10
 Applications: UBM
 Database: ccast2

Report Status

Number of Alarms Meeting Criteria: 5

To sort column click on header.

ID	App	Database	Policy	Guarded Item	Severity	Status	Time
1155	UBM	ccast2	User Policies	CCHEN	cautionary	Error_Corrected	2003/12/19 21:54
1157	UBM	ccast2	Session Policies	SCOTT	cautionary	Not Handled	2003/12/19 11:53
1516	UBM	ccast2	Session Policies	SCOTT	cautionary	Not Handled	2004/01/16 19:36
1518	UBM	ccast2	Object Policies	SCOTT-EMP	cautionary	Not Handled	2004/01/16 13:54
1519	UBM	ccast2	Session Policies	WANI	cautionary	Acknowledged	2004/01/16 14:11

Informational Cautionary Major Critical

Export to Excel Tab Delimited Comma Delimited

Previous Current Report

Done

도면7

