(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2013년11월20일
(11) 등록번호 10-1327317
(24) 등록일자 2013년11월04일

(51) 국제특허분류(Int. Cl.)
H04L 12/26 (2006.01) *H04L 29/06* (2006.01)
(21) 출원번호 10-2012-0138151
(22) 출원일자 2012년11월30일
심사청구일자 2012년11월30일
(56) 선행기술조사문헌
KR1020070122045 A*
US20050209876 A1*
KR1020110037645 A
US20060129670 A1
*는 심사관에 의하여 인용된 문헌

(73) 특허권자
(주)소만사
서울특별시 영등포구 영신로 220 (영등포동8가)
(72) 발명자
백승태
서울특별시 구로구 오류1동 13-72 LG 베스트빌 102호
허용필
서울특별시 영등포구 양평동 3가 13 이노플렉스 7층 소만사
(뒷면에 계속)
(74) 대리인
특허법인지명

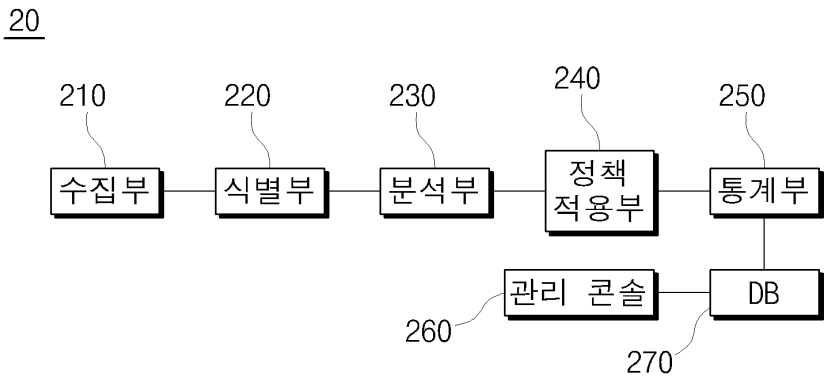
전체 청구항 수 : 총 14 항 심사관 : 전용해

(54) 발명의 명칭 **SAP 응용 트래픽 분석 및 모니터링 장치 및 방법, 이를 이용한 정보 보호 시스템**

(57) 요 약

본 발명은 트래픽 분석 장치 및 방법에 대하여 개시한다. 본 발명의 일면에 따른 트래픽 분석 장치는, 적어도 하나의 클라이언트와 서버 간의 네트워크 패킷이 기등록된 SAP 세션의 패킷인지를 확인하고, 상기 기등록된 SAP 세션의 패킷이 아니면, 신규 SAP 세션의 패킷인지를 확인하는 분석부; 및 상기 네트워크 패킷이 상기 기등록된 SAP 세션 또는 상기 신규 SAP 세션의 패킷이면, 상기 네트워크 패킷에 기정의된 감시정보가 포함되는지를 확인하고, 상기 감시정보가 포함되면, 기설정된 보안정책에 따른 대응 행동을 수행하는 정책 적용부를 포함하는 것을 특징으로 한다.

대 표 도 - 도2



(72) 발명자

김태완

서울특별시 마포구 상암동 월드컵파크 1010동 901호

이상만

대전광역시 유성구 도룡동 스마트시티주상복합아파트 502동 1702호

이 발명을 지원한 국가연구개발사업

과제고유번호 10041548

부처명 지식경제부

연구사업명 산업융합원천기술개발

연구과제명 트래픽 응용 판단을 위한 95% 이상의 분석률과 정확도를 지원하는 240 기가급 실시간 응용 시그니쳐 자동 생성 시스템 기술 개발

기 여 율 1/1

주관기관 (주) 시스메이트

연구기간 2012.06.01 ~ 2015.05.31

특허청구의 범위

청구항 1

적어도 하나의 클라이언트와 서버 간의 네트워크 패킷에 대하여 상기 네트워크 패킷의 4 튜플(Tuple)을 추출해 해시 처리하여 해시값을 생성하고, 생성된 상기 해시값을 기등록된 SAP 세션의 4 튜플에 대한 해시값과 비교한 다음, 비교 결과를 태깅하여 상기 네트워크 패킷을 전달하는 식별부;

상기 식별부로부터 상기 네트워크 패킷을 전달받아 태깅된 상기 비교 결과를 바탕으로 상기 네트워크 패킷이 상기 기등록된 SAP 세션의 패킷인지를 확인하고, 상기 기등록된 SAP 세션의 패킷이 아니면, 신규 SAP 세션의 패킷인지를 확인하는 분석부; 및

상기 네트워크 패킷이 상기 기등록된 SAP 세션 또는 상기 신규 SAP 세션의 패킷이면, 상기 네트워크 패킷에 기정의된 감시정보가 포함되는지를 확인하고, 상기 감시정보가 포함되면, 기설정된 보안정책에 따른 대응 행동을 수행하는 정책 적용부

를 포함하는 트래픽 분석 장치.

청구항 2

제1항에 있어서, 상기 분석부는,

상기 네트워크 패킷의 출발지 포트 정보, 목적지 포트 정보 및 시그니처 중 적어도 하나를 이용하여 상기 네트워크 패킷이 상기 신규 SAP 응용 세션의 패킷인지 여부를 판단하는 것인 트래픽 분석 장치.

청구항 3

제2항에 있어서, 상기 분석부는,

상기 네트워크 패킷의 상기 출발지 포트 정보 또는 상기 목적지 포트 정보가 이미 알고 있는 SAP 응용 서버의 포트 정보와 일치하면, 상기 네트워크 패킷이 상기 신규 SAP 응용 세션의 패킷이라고 판단하고,

상기 네트워크 패킷의 상기 출발지 포트 정보 또는 상기 목적지 포트 정보가 이미 알고 있는 SAP 응용 서버의 포트 정보와 일치하지 않으면, 상기 네트워크 패킷의 시그니처를 확인하여 전달받은 패킷이 신규 SAP 응용 세션의 패킷인지 여부를 판단하는 것인 트래픽 분석 장치.

청구항 4

제1항에 있어서, 상기 분석부는,

상기 네트워크 패킷이 상기 기등록된 SAP 세션 또는 상기 신규 SAP 세션의 패킷이면, 상기 네트워크 패킷을 상기 클라이언트로부터 상기 서버로 전송되는 요청 데이터 및 상기 서버로부터 상기 클라이언트로 전송되는 응답 데이터로 구분하는 것인 트래픽 분석 장치.

청구항 5

제4항에 있어서, 상기 정책 적용부는,

상기 요청 데이터로부터 트랜잭션 코드(Transaction Code)를 확인하면, 상기 요청 데이터로부터 확인된 출발지 IP 주소 및 사용자 ID를 기반으로 상기 요청 데이터에 대응하는 요청이 기승인되지 않은 트랜잭션 코드 요청인지를 확인하고, 확인결과 상기 기승인되지 않은 트랜잭션 코드 요청이면, 상기 보안정책에 따른 대응을 수행하는 것인 트래픽 분석 장치.

청구항 6

제1항에 있어서, 상기 분석부는,

상기 네트워크 패킷이 상기 기등록된 SAP 세션 또는 상기 신규 SAP 세션의 패킷이면, 상기 네트워크 패킷으로부터 SAP 시스템 ID, 사용자 ID, SAP 응용 서비스를 위한 프로그램 이름, 트랜잭션 코드 및 메시지 중 적어도 하

나를 파싱하고, 파싱된 내용을 XML(eXtensible Markup Language) 포맷으로 객체화하는 것인 트래픽 분석 장치.

청구항 7

제6항에 있어서,

관리자의 요청에 따라, 객체화된 상기 네트워크 패킷을 이용하여 상기 네트워크 패킷에 대응하는 상기 클라이언트의 GUI(Graphic User Interface) 화면과 동일한 GUI 화면을 재현하는 인터페이스를 제공하는 관리 콘솔

을 더 포함하는 트래픽 분석 장치.

청구항 8

제1항에 있어서, 상기 정책 적용부는,

상기 대응 행동을 수행한 후 상기 대응 행동의 내역, 상기 대응 행동에 따른 결과 및 상기 대응 행동에 대응하는 네트워크 패킷 중 적어도 하나를 포함하는 로그를 DB에 저장하는 것인 트래픽 분석 장치.

청구항 9

제8항에 있어서, 관리 콘솔을 더 포함하고, 상기 관리 콘솔은,

관리자에게 상기 로그를 조회하여 IP 주소, 사용자 ID 및 트랜잭션 코드 중 적어도 하나를 확인하고, 확인된 상기 적어도 하나로부터 비정상적인 데이터의 변경이나 조회를 검색하는 인터페이스

를 제공하는 것인 트래픽 분석 장치.

청구항 10

제1항에 있어서, 상기 분석부는,

상기 네트워크 패킷이 상기 기등록된 SAP 세션 또는 상기 신규 SAP 세션의 패킷이 아니면, 상기 네트워크 패킷을 삭제하는 것인 트래픽 분석 장치.

청구항 11

적어도 하나의 클라이언트와 서버 간의 네트워크 패킷을 분석하는 장치에 의한 트래픽 분석 방법으로서,

상기 네트워크 패킷의 4 튜플(Tuple)을 추출해 해시 처리하여 해시값을 생성하고, 생성된 상기 해시값을 기등록된 SAP 세션의 4 튜플에 대한 해시값과 비교한 다음, 비교 결과를 태깅하는 단계;

태깅된 상기 비교 결과를 바탕으로 상기 네트워크 패킷이 기등록된 SAP 세션의 패킷인지를 확인하는 단계;

상기 네트워크 패킷이 상기 기등록된 SAP 세션의 패킷이 아니면, 신규 SAP 세션의 패킷인지를 확인하는 단계;

상기 네트워크 패킷이 상기 기등록된 SAP 세션 또는 상기 신규 SAP 세션의 패킷이면, 상기 네트워크 패킷에 기정의된 감시정보가 포함되는지를 확인하는 단계; 및

상기 네트워크 패킷에 상기 감시정보가 포함되면, 기설정된 보안정책에 따른 대응 행동을 수행하는 단계

를 포함하는 트래픽 분석 방법.

청구항 12

제11항에 있어서, 상기 신규 SAP 세션의 패킷인지를 확인하는 단계에서는,

상기 네트워크 패킷의 출발지 포트 정보, 목적지 포트 정보 및 시그니처 중 적어도 하나를 이용하여 상기 신규 SAP 세션의 패킷인지를 확인

하는 것인 트래픽 분석 방법.

청구항 13

제11항에 있어서,

상기 네트워크 패킷이 상기 기등록된 SAP 세션 또는 상기 신규 SAP 세션의 패킷이면, 상기 네트워크 패킷으로부

터 SAP 시스템 ID, 사용자 ID, SAP 응용 서비스를 위한 프로그램 이름, 트랜잭션 코드 및 메시지 중 적어도 하나를 파싱하는 단계; 및

상기 파싱하는 단계에서, 파싱된 내용을 XML(eXtensible Markup Language) 포맷으로 객체화하는 단계

를 더 포함하는 트래픽 분석 방법.

청구항 14

제13항에 있어서,

관리자의 요청에 따라, 객체화된 상기 네트워크 패킷을 이용하여 상기 네트워크 패킷에 대응하는 상기 클라이언트의 GUI 화면과 동일한 GUI 화면을 재현하여 디스플레이하는 단계

를 더 포함하는 트래픽 분석 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 트래픽 분석 장치에 관한 것으로서, 더 구체적으로는 클라이언트와 서버 간에 송/수신되는 특정 프로토콜의 트래픽을 분석할 수 있는 SAP 응용 트래픽 분석 및 모니터링 장치 및 방법에 관한 것이다.

배 경 기 술

[0002] 근래 들어, 개인정보 유출사고 및 그로 인한 개인정보 오남용 피해가 사회적 이슈가 되고 있다.

[0003] 따라서, 정부는 "정보통신망 이용촉진 및 정보보호 등에 관한 법률"의 정보통신 서비스 측면의 개인정보 보호 및 안전 조치에 대한 미비점을 보완하고, 법적 의무를 강화하기 위해, 2011년 9월 11일 별도의 "개인정보보호법"을 공고하여 시행하기에 이르렀다.

[0004] 또한, 동법의 시행령인 "개인정보의 안전성 확보조치 기준 고시"에 부합하는 개인정보의 기술적, 관리적 보호 조치에 관한 구체 지침 및 기술과 컴플라이언스 솔루션이 관련 정부 기관, 학계 및 민간 기업을 통해서 활발히 개발되고 있다.

[0005] 종래의 개인정보의 기술적, 관리적 보호 조치에 관한 기술과 컴플라이언스 솔루션은 주로 개인정보가 저장 및 가공되는 데이터베이스에 대한 접근 제어, 접근 이력과 내역에 대한 감사, 데이터베이스 암호화 기술 및 이를 이용한 컴플라이언스 솔루션이 주를 이루어 왔다.

[0006] 그러나, 종래의 기술 및 컴플라이언스 솔루션은 주로 상용 데이터베이스 시스템인 Oracle, Sybase, DB2, Informix, Altibase, MySQL, MSSQL나, Teradata 등에 한정되어 개발되었다.

[0007] 하지만, 전사자원관리(ERP) 시스템으로 널리 사용되고 있는 SAP와 같이, 상용 데이터베이스 시스템만을 이용하지는 않는 프로토콜이나, 서비스에 대한 개인정보보호 조치는 미비한 실정이다.

발명의 내용

해결하려는 과제

[0008] 본 발명은 전술한 바와 같은 기술적 배경에서 안출된 것으로서, 클라이언트와 서버 간의 SAP 응용 패킷을 분석 및 모니터링할 수 있는 트래픽 분석 장치 및 방법을 제공하는 것을 그 목적으로 한다.

[0009] 본 발명의 목적은 이상에서 언급한 목적으로 제한되지 않으며, 언급되지 않은 또 다른 목적들은 아래의 기재로부터 당업자에게 명확하게 이해될 수 있을 것이다.

과제의 해결 수단

[0010] 본 발명의 일면에 따른 트래픽 분석 장치는, 적어도 하나의 클라이언트와 서버 간의 네트워크 패킷이 기등록된 SAP 세션의 패킷인지를 확인하고, 상기 기등록된 SAP 세션의 패킷이 아니면, 신규 SAP 세션의 패킷인지를 확인하는 분석부; 및 상기 네트워크 패킷이 상기 기등록된 SAP 세션 또는 상기 신규 SAP 세션의 패킷이면, 상기 네트워크 패킷에 기정의된 감시정보가 포함되는지를 확인하고, 상기 감시정보가 포함되면, 기설정된 보안정책에

따른 대응 행동을 수행하는 정책 적용부를 포함하는 것을 특징으로 한다.

[0011] 본 발명의 다른 면에 따른 적어도 하나의 클라이언트와 서버 간의 네트워크 패킷을 분석하는 장치에 의한 트래픽 분석 방법은, 상기 네트워크 패킷이 기등록된 SAP 세션의 패킷인지를 확인하는 단계; 상기 네트워크 패킷이 상기 기등록된 SAP 세션의 패킷이 아니면, 신규 SAP 세션의 패킷인지를 확인하는 단계; 상시 네트워크 패킷이 상기 기등록된 SAP 세션 또는 상기 신규 SAP 세션의 패킷이면, 상기 네트워크 패킷에 기정의된 감시정보가 포함되는지를 확인하는 단계; 및 상기 네트워크 패킷에 상기 감시정보가 포함되면, 기설정된 보안정책에 따른 대응 행동을 수행하는 단계를 포함하는 것을 특징으로 한다.

발명의 효과

[0012] 본 발명에 따르면, 클라이언트와 서버 사이의 네트워크를 통해 송/수신되는 SAP 응용 패킷을 분석 및 모니터링 할 수 있고, SAP 응용 패킷을 통한 정보 유출을 방지할 수 있다.

도면의 간단한 설명

[0013] 도 1은 본 발명에 따른 SAP 응용 클라이언트와 SAP 응용 서버를 도시한 구성도.

도 2는 본 발명에 따른 트래픽 분석 장치를 도시한 구성도.

도 3a는 본 발명에 따른 클라이언트의 트랜잭션 코드 요청 과정을 도시한 도면.

도 3b는 본 발명에 따른 서버의 트랜잭션 코드 확인 과정을 도시한 도면.

도 4는 본 발명에 따른 클라이언트의 요청 데이터의 입력에 기반한 클라이언트의 GUI 화면 내용을 재현한 예시도.

도 5는 본 발명에 따른 클라이언트의 요청 데이터의 입력에 대응하는 서버의 응답 데이터에 기반한 클라이언트의 GUI 화면 내용을 재현한 예시도.

도 6은 본 발명에 따른 트래픽 분석 방법을 도시한 흐름도.

발명을 실시하기 위한 구체적인 내용

[0014] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 것이며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하며, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 한편, 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 구성소자, 단계, 동작 및/또는 소자는 하나 이상의 다른 구성소자, 단계, 동작 및/또는 소자의 존재 또는 추가를 배제하지 않는다.

[0015] 이제 본 발명의 실시예에 대하여 첨부한 도면을 참조하여 상세히 설명하기로 한다. 도 1은 본 발명의 실시예에 따른 SAP 클라이언트와 SAP 서버를 도시한 구성도이다.

[0016] 도 1에 도시된 바와 같이, 하나의 SAP 서버는 복수의 SAP 클라이언트와 네트워크를 통해 연결된다.

[0017] SAP 서버는 SAP 응용 서비스를 제공하는 서버로서, SAP 응용 서비스용 소프트웨어를 구비하되, 하드웨어는 통상의 서버와 동일 또는 유사할 수 있다. 예컨대, SAP 서버는 SAP 전사관리자원(ERP; enterprise resources planning) 시스템일 수 있다.

[0018] 각 SAP 클라이언트는 사용자의 조작에 따라, SAP 서버에 접속하여 SAP 서버에 의해 제공되는 SAP 응용 서비스를 사용자에 제공한다.

[0019] 각 SAP 클라이언트는 각 SAP 응용 서비스에 특화된 클라이언트일 수 있으며, SAP 응용 서비스용 소프트웨어를 구비한 범용 클라이언트(PC, 노트북 등)일 수도 있다. 이하의 명세서에서는 설명의 편의성을 위해서 SAP 서버를 서버로, SAP 클라이언트를 클라이언트로 줄여서 칭한다.

[0020] 각 클라이언트가 서버에 접속하여 SAP 응용 서비스를 위한 데이터를 요청하고, 그에 따라 서버가 클라이언트에

응답을 하는 과정을 다음과 같다.

[0021] 1. SAP 응용 서비스 사용자가 클라이언트를 통해 서버에 접속한다.

[0022] 2. SAP 사용자가 클라이언트 로그인 화면에서 사용자 ID(즉, 클라이언트의 사용자 계정)/패스워드를 입력함에 따라, 서버에 로그인(Log In)한다.

[0023] 3. 클라이언트는 서버로부터 수집된 SAP 응용 서비스 관련 데이터를 조회한다. 여기서, 클라이언트는 사용자의 접근 권한 범위에서 수집된 데이터를 조회할 수 있다.

[0024] 4. 클라이언트는 서버로부터 수집된 SAP 응용 서비스 관련 데이터를 필요에 따라 변경하고, 서버에 저장한다. 이때, 클라이언트는 사용자의 접근 권한 범위 내에서 수집된 데이터를 변경할 수 있다.

[0025] 5. 클라이언트는 서버로부터 로그아웃(Log Out)한다.

[0026] 전술한 과정에서, 클라이언트와 서버는 TCP/IP 통신을 통해 SAP 응용 세션의 패킷을 포함하는 정보를 송수신한다. 이때, SAP는 응용(Application) 단계에서 서버와 클라이언트 간의 SAP 응용 서비스 제공을 위해 이용된다.

[0027] 그런데, SAP는 기업의 경영자원에 관한 애플리케이션- 즉, 재고 및 구매관리, 생산관리, 판매관리, 인사관리, 재무관리, 관리회계 등을 위해 통합 데이터 베이스를 실시간으로 결합시키는 전사자원관리(ERP) 시스템 -으로 많이 사용된다.

[0028] 따라서, 클라이언트와 서버 간에 송/수신되는 SAP 응용 패킷에는 개인정보뿐만 아니라, 회계, 생산, 연구개발 등의 대외 보안이 필요한 기밀정보가 포함된다.

[0029] 그러므로, SAP 응용 패킷을 송수신하는 사용자의 행위를 기록하고, 이상 상황에서는 경고 또는 차단하는 기능은 매우 필요하며, 이상 상황에 따른 사용자의 행위를 화면으로 재현할 수 있다면 더욱 좋을 것이다.

[0030] 그런데, SAP 서버는 WAS(Web Application Server)와 같은 자체 데이터베이스 또는 상용 데이터베이스와 SAP 클라이언트 사이에서, 중계 서버와 같은 미들웨어 형태로 SAP 응용 서비스를 제공하므로, 고객 정보나 비인가된 정보 조회 및 변경 작업 등에 대한 사용자 추적이 다소 어려운 면이 있다.

[0031] 이를 위하여, 본 발명의 실시예에 따른 트래픽 분석 장치는 클라이언트와 서버 간의 네트워크 구간에서, 패킷 미러링(Mirroring) 방식으로 SAP 프로토콜의 패킷을 분석한다.

[0032] 이하, 도 2 내지 3b를 참조하여 본 발명의 실시예에 따른 트래픽 분석 장치에 대해서 설명한다.

[0033] 도 2는 본 발명의 실시예에 따른 트래픽 분석 장치를 도시한 구성도이고, 도 3a는 본 발명의 실시예에 따른 클라이언트의 트랜잭션 코드 요청 과정을 도시한 도면이고, 도 3b는 본 발명의 실시예에 따른 서버의 트랜잭션 코드 확인 과정을 도시한 도면이다.

[0034] 도 2에 도시된 바와 같이, 본 발명의 실시예에 따른 트래픽 분석 장치(20)는 수집부(210), 식별부(220), 분석부(230), 정책 적용부(240), 통계부(250), DB(270) 및 관리 콘솔(260)을 포함한다. 여기서, DB(270)는 트래픽 분석 장치(20)의 구성요소일 수도 있지만, 그 외부에 구비되어, 트래픽 분석 장치(20)와 인터페이스할 수도 있다.

[0035] 수집부(210)는 패킷 미러링 방식으로 적어도 하나의 클라이언트와 서버 간의 네트워크에서 송/수신되는 패킷을 수집한다. 이때, 수집부(210)는 클라이언트와 서버 간에 송/수신되는 모든 패킷을 수집할 수 있다.

[0036] 식별부(220)는 수집된 패킷의 4 튜플(Soure IP, Source Port, Destination IP, Destination Port)을 추출하고, 이를 조합하여 해시 처리(Hashing)하여 해시값을 생성한다. 그리고, 식별부(220)는 수집된 패킷의 튜플 해시값을 기등록된 튜플 해시값 목록과 비교하고, 비교 결과를 태깅하여 분석부(230)로 전달한다. 여기서, 기등록된 해시값은 기등록된 SAP 응용 세션 목록의 각 세션의 4 튜플을 해시 처리한 결과 해시값 목록이다.

[0037] 식별부(220)는 비교 결과에 대한 정보 및 수집된 패킷의 튜플 해시값을 포함하는 정보를, 수집된 패킷에 태깅(Tagging)하여 분석부(230)로 전달한다. 이때, 식별부(220)는 수집된 패킷의 튜플 해쉬값과 기등록된 튜플 해쉬값 목록 중 하나가 일치하면, 일치함을 나타내는 정보(또는, 코드)를 수집된 패킷에 태깅한다.

[0038] 분석부(230)는 태깅된 패킷을 전달받으면, 태깅된 정보를 확인하여 해당 패킷이 기등록된 SAP 응용 세션의 패킷인지를 확인한다. 이때, 분석부(230)는 비교 결과로부터 수집된 패킷의 튜플 해쉬값과 기등록된 튜플 해쉬값 목록 중 하나가 일치한다는 것을 확인하면, 전달받은 패킷이 기등록된 SAP 응용 세션의 패킷이라고 확인한다.

[0039] 분석부(230)는 전달받은 패킷이 기등록된 SAP 응용 세션의 패킷이 아닐 경우, 출발지 포트 정보, 목적지 포트

정보 및 시그니처를 기반으로 사전 등록되지 않은 신규 SAP 응용 세션의 패킷인지를 판단한다.

[0040] 구체적으로, 분석부(230)는 전달받은 패킷의 출발지 또는 목적지 포트 정보가 이미 알고 있는 SAP 응용 서버의 포트 정보와 일치하는지를 확인하고, 일치하면 전달받은 패킷이 신규 SAP 응용 세션의 패킷이라고 판단한다. 반면, 분석부(230)는 전달받은 패킷의 출발지 또는 목적지 포트 정보가 이미 알고 있는 SAP 응용 서버의 포트 정보와 일치하지 않으면, 해당 패킷의 시그니처를 확인하여 전달받은 패킷이 신규 SAP 응용 세션의 패킷인지 여부를 판단한다. 이때, 분석부(230)는 전달받은 패킷이 압축되어 있으면, 압축을 해제하여 출발지 포트, 목적지 포트 또는 시그니처를 확인할 수 있다.

[0041] 이때, 분석부(230)는 전달받은 패킷이 기등록된 SAP 응용 세션은 물론, 신규 SAP 응용 세션의 패킷도 아니면, 해당 패킷을 삭제(Drop)한다.

[0042] 반면, 분석부(230)는 전달받은 패킷이 신규 SAP 응용 세션의 패킷이면, 세션 ID를 추출한 후 세션 ID를 기반으로 동일 세션의 신규 SAP 응용 세션의 패킷들을 TCP/IP(Transmission Control Protocol/Internet Protocol) 세션 형태로 재구성한다.

[0043] 분석부(230)는 세션 설정 이후 세션 ID 기반으로 클라이언트와 서버 간의 송/수신되는 신규 SAP 응용 세션의 패킷을 식별 및 추출한다. 또한, 분석부(230)는 추출된 세션 ID 및 그의 튜플 해시값을 포함하는 신규 SAP 응용 세션 정보를 포함시켜, 기등록된 튜플 해쉬값 목록(또는, 기등록된 SAP 응용 세션 목록)을 갱신한다.

[0044] 분석부(230)는 기등록된 SAP 응용 세션 또는 신규 SAP 응용 세션의 패킷을, 클라이언트에서 서버로 송신되는 요청(Request) 데이터와 서버에서 클라이언트로 송신되는 응답 데이터로 구분한다.

[0045] 분석부(230)는 해당 SAP 응용 세션의 패킷이 요청 데이터(즉, 클라이언트 송신 데이터)이면, SAP 시스템 ID, 사용자 ID, SAP 응용 서비스를 위한 프로그램 이름, 트랜잭션 코드 및 메시지 중 적어도 하나를 파싱(Parsing)하고, 파싱된 내용을 XML(eXtensible Markup Language) 포맷으로 객체화한다.

[0046] 분석부(230)는 해당 SAP 응용 세션의 패킷이 응답(Response) 데이터이면, 응답 패킷(즉, 서버 송신 데이터)으로부터 SAP 시스템 ID, 사용자 ID, 프로그램 이름, 트랜잭션 코드 및 메시지 중 적어도 하나를 파싱하고, 파싱된 내용을 XML 포맷으로 객체화한다.

[0047] 정책 적용부(240)는 객체화된 요청 데이터 및 응답 데이터를 확인하면, 보안정책에 위반되는지를 확인하고, 보안정책에 위반되면, 보안정책에 대응하는 대응 행동을 수행한다.

[0048] 정책 적용부(240)는 객체화된 요청 데이터의 내용에서, 도 3b와 같이, 트랜잭션 코드(T-Code) 정보를 확인하면(도 3b의 점선 박스 참조), 해당 요청 패킷의 출발지 IP 주소 및 사용자 ID를 기반으로 해당 요청이 기승인되지 않은 트랜잭션 코드 요청인지를 확인한다. 이때, 정책 적용부(240)는 기등록된 보안정책을 기반으로 해당 요청이 사전 승인되지 않은 트랜잭션 코드 요청인지를 확인할 수 있다. 이때, 클라이언트는 도 3a와 같이 소정 메뉴(도 3a의 실선 박스 참조)를 선택함에 따라 트랜잭션 코드 요청을 송신할 수 있다.

[0049] 정책 적용부(240)는 확인된 트랜잭션 코드에 따른 요청이 기승인되지 않은 트랜잭션 코드 요청인 경우, 보안정책에 따른 기정의된 대응행동을 처리한다. 여기서, 기정의된 대응 행동은 관리자에 경고 메시지 발송이나, 해당 세션 차단 등일 수 있다.

[0050] 정책 적용부(240)는 객체화된 요청 데이터와 응답 데이터의 내용에 개인정보패턴, 민감정보패턴 및 기정의된 텍스트 스트링 중 적어도 하나의 감시정보가 포함되는지를 검사하고, 각 감시정보별 총 검출건수를 산출한다.

[0051] 여기서, 개인정보패턴은 주민등록번호(외국인 등록번호 포함), 여권 번호 및 운전면허 번호와 같은 다양한 개인정보를 정규 표현식(Regular Express)으로 정의한 것일 수 있으며, 민감정보패턴은 회계, 생산, 연구개발에 관련된 정보를 정규 표현식으로 정의한 것일 수 있다. 또한, 텍스트 스트링은 관리자에 의해 정의될 수 있으며, 예컨대, 민감정보나 개인정보에 포함되는 특정 텍스트의 조합일 수 있다.

[0052] 정책 적용부(240)는 각 감시정보별 총 검출건수에 대응하는 기정의된 보안정책에 따른 대응 행동을 수행한다.

[0053] 예를 들어, 정책 적용부(240)는 응답 데이터로부터 특정 감시정보가 총 10건 검출된 경우, 관리자에게 경고 메시지 발송, 또는 해당 세션 차단 등을 수행할 수 있다. 이때, 정책 적용부(240)는 감시정보가 포함된 응답 패킷 또는 요청 패킷에 대응하는 세션의 정보를 관리자에게 제공함은 물론이다.

[0054] 정책 적용부(240)는 대응 행동을 수행한 후 대응 행동의 수행 내역과 그 결과, 대응 행동에 대응하는 객체화된

응답 데이터 및 그 응답 데이터에 대응하는 객체화된 요청 데이터 중 적어도 하나를 포함하는 로그를 DB(270)에 저장한다. 여기서, 대응 행동의 수행 내역의 결과는 관리자에게 경고 메시지를 발송하는 등의 대응 행동을 수행한 이후 그에 따른 변화 예컨대, 관리자에 의한 대응 설정일 수 있다.

[0055] 통계부(250)는 저장된 로그를 이용하여 사용자 ID별 감시정보의 조회내역(즉, 감시정보의 총 검출건수를 이용함)에 대한 일별 통계 데이터를 생성하고, 생성된 일별 통계 데이터를 일정 기간별로(예컨대, 1주나, 1일 등) 누적 및 평균하여 일정기간별 통계 데이터를 생성한다. 이때, 통계부(250)는 일 단위로 사용자 ID별로 감시정보가 포함된 요청의 총 횟수 및 감시정보가 포함된 응답의 총 검출건수에 대해 일별 통계 데이터를 산출할 수 있다.

[0056] 통계부(250)는 일정기간별 통계 데이터를 이용하여 사용자 ID별 감시정보 조회패턴을 산출하여 DB(270)에 저장한다.

[0057] 예를 들어, 통계부(250)는 사용자 ID "A"인 사용자는 한 달 내에 주민번호를 1번 이상 송신 또는 수신하며, 카드번호는 2번 이상 송신 또는 수신함을 나타내는 감시정보 조회패턴을 산출하여 DB(270)에 저장할 수 있다.

[0058] 이때, 사용자 ID별 감시정보 조회패턴은 보안정책의 임계값으로 사용될 수 있다.

[0059] 예를 들어, 관리자는 기설정된 감시정보 조회패턴을 초과한 개인정보 조회패턴이 감지될 경우, 관리자에 경고메시지를 전송하도록 보안정책을 설정할 수 있으며, 더 강력한 통제를 원할 경우에는 해당 세션을 차단하도록 보안정책을 설정할 수도 있다.

[0060] 다만, 감시정보 조회패턴은 최초 가동 시점을 기준으로 익일 통계가 산출된 직후부터 사용 가능하고, 이상 발생의 검출 기준이라기보다는 이상 징후의 검출 기준인 성격이 강하므로, 감시정보 조회패턴에 의해 이상 발생상황과 동일한 강력 대응(예컨대, 세션의 차단)을 수행하는 것은 주의할 필요가 있다.

[0061] 한편, 객체화된 요청 데이터 및 응답 데이터는 입력 필드(input field), 출력 필드(output field), 프레임(frame), 테이블(table) 및 각종 버튼(button) 정보 등을 포함하는 클라이언트의 GUI(Graphic User Interface) 화면에 대응하는 GUI 화면을 서버의 화면에서 재현하는데 이용될 수 있다. 이는 관리 콘솔(260)을 통해서 가능한데, 이하에서 이에 대해서 설명한다.

[0062] 관리 콘솔(260)은 보안정책의 설정과 적용을 위한 제1 인터페이스 및 클라이언트의 GUI 화면 내용에 대한 재현을 요청하는 제2 인터페이스를 제공한다. 여기서, 보안정책은 감시정보, 승인된 트랜잭션 코드 요청의 정보, 승인되지 않은 트랜잭션 코드를 확인했을 때의 대응 행동 및 각 감시정보의 총 검출건수에 따른 대응 행동 등을 포함한다.

[0063] 구체적으로, 관리자에 의해 제2 인터페이스가 선택되면, 관리 콘솔(260)은 객체화된 요청 데이터 및 응답 데이터 중 적어도 하나를 이용하여, 사용자 ID별 로그인 내역, 로그인 이후 클라이언트에서 서버로의 요청 내역 및 요청 내역에 대응하는 서버의 응답 내역 중 적어도 하나를 클라이언트의 GUI 화면 내용과 동일하게 재현하여 화면에 출력할 수 있다.

[0064] 관리자는 저장된 로그를 이용하여 클라이언트의 IP 주소, 클라이언트의 사용자 ID 또는 트랜잭션코드를 기반으로 비정상적인 데이터의 변경 및 조회 내역과 같은 비정상 요청 행위에 대해 감사할 수 있으며, 에러 메시지를 조회 및 검색할 수 있다. 이때, 로그는 대응 행동, 대응 행동에 대응하는 요청 데이터 및 요청 데이터에 대응하는 응답 데이터를 포함하므로, 관리자는 로그로부터 IP 주소, 사용자 ID, 트랜잭션 코드를 확인할 수 있다.

[0065] 한편, 정책 적용부(240)는 객체화된 요청 데이터 또는 응답 데이터로부터 SAP 에러 메시지를 확인하면, 에러 메시지에 관련된 객체화된 요청 데이터 또는 응답 데이터에 대한 로그를 저장한다. 이때, 정책 적용부(240)는 관리자에게 에러 발생을 통보할 수도 있다.

[0066] 따라서, 관리자는 시스템 에러를 해결하기 위해서 관리 콘솔(260)을 통해 클라이언트의 GUI 화면에 따른 시스템 에러 발생의 상황을 재현할 수도 있다.

[0067] 이와 같이, 본 발명의 실시예는 전사자원관리(ERP) 시스템 등을 위한 프로토콜로 이용되는 SAP 응용 패킷을 분석 및 모니터링할 수 있고, 그에 대한 개인정보 보호조치 기술 및 솔루션을 제공할 수 있어, SAP 응용 패킷을 통한 정보 유출을 방지할 수 있다.

[0068] 또한, 본 발명의 실시예는 SAP 시스템에서 발생된 에러 메시지나, 클라이언트의 요청 내역 및 그에 대응하는 응답 내용을 클라이언트의 GUI 화면과 동일하게 재현해줄 수 있어, 관리자의 시스템 에러 확인 및 감시정보의 유

출 상황 확인을 도울 수 있다.

[0069] 이하, 도 4 및 5를 참조하여 본 발명의 실시예에 따른 관리 콘솔에 의한 GUI 화면 재현의 예에 대해서 설명한다.

[0070] 도 4는 본 발명의 실시예에 따른 클라이언트의 요청 데이터에 기반한 클라이언트의 GUI 화면 내용을 서버에서 재현한 예시도이고, 도 5는 본 발명의 실시예에 따른 클라이언트의 요청 데이터의 입력에 대응하는 서버의 응답 데이터에 기반한 클라이언트의 GUI 화면 내용을 재현한 예시도다.

[0071] 도 4와 같이, 본 발명에 따른 트래픽 분석 장치(20)는 저장된 로그에 포함된 클라이언트 요청 데이터를 기반으로 해당 요청 데이터를 송신할 당시의 클라이언트 GUI 화면을 동일하게 재현할 수 있다.

[0072] 도 4의 재현된 GUI 화면에서 관리자는 감시정보의 유출 당시에 "60.100.126.131" IP를 사용하는 클라이언트에서 사용자 ID가 "LEELAND"인 사용자가 "121.252.69.82" IP를 사용하는 서버로 로그인을 요청하고 있었음을 알 수 있다.

[0073] 마찬가지로, 도 5와 같이, 본 발명에 따른 트래픽 분석 장치(20)는 저장된 로그에 포함된 서버 응답 데이터를 기반으로 해당 응답 데이터를 수신할 당시의 클라이언트 GUI 화면을 동일하게 재현할 수 있다.

[0074] 도 5의 재현된 GUI 화면에서, 관리자는 감시정보의 유출 당시 "192.168.5.87" IP를 사용하는 클라이언트가 "1.235.156.65" IP를 사용하는 서버로부터 "허용필" 및 "홍길동"의 개인정보를 제공받고 있음을 알 수 있다.

[0075] 이와 같이, 본 발명의 실시예에는 단순히 유출된 민감정보나, 그에 대한 대응행동 등을 포함하는 로그 정보뿐만 아니라, 클라이언트의 GUI 화면도 재구성할 수 있어, 법정분쟁이 발생한 경우 등에 명확한 근거자료를 제공할 수 있다.

[0076] 또한, 본 발명의 실시예는 SAP 시스템에서 발생된 에러 메시지나, 클라이언트의 요청 내역 및 그에 대응하는 응답 내용을 클라이언트의 GUI 화면과 동일하게 재현해줄 수 있어, 관리자의 시스템 에러 확인 및 감시정보의 유출 상황 확인을 도울 수 있다.

[0077] 이하, 도 6을 참조하여 본 발명의 실시예에 따른 트래픽 분석 방법에 대해서 설명한다. 도 6은 본 발명의 실시예에 따른 트래픽 분석 방법을 도시한 흐름도이다.

[0078] 도 6을 참조하면, 트래픽 분석 장치(20)는 클라이언트와 서버 간의 패킷을 미러링 방식으로 수집한다(S610).

[0079] 트래픽 분석 장치(20)는 수집된 패킷이 기등록된 SAP 응용 세션의 패킷인지를 확인한다(S620). 이때, 트래픽 분석 장치(20)는 수집된 패킷의 4 튜플의 해쉬값이 기등록된 SAP 응용 세션의 4 튜플의 해쉬값과 일치하는지를 확인함에 따라 수집된 패킷이 기등록된 SAP 응용 세션의 패킷인지 여부를 확인할 수 있다.

[0080] 트래픽 분석 장치(20)는 수집된 패킷이 기등록된 SAP 응용 세션의 패킷이 아니면, 신규 SAP 응용 세션의 패킷인지를 확인한다(S630). 이때, 트래픽 분석 장치(20)는 수집된 패킷의 출발지 포트, 목적지 포트 및 시그니처 중 적어도 하나가 SAP 응용 세션의 포트 정보 및 시그니처와 대응하는지를 확인함에 따라 수집된 패킷이 신규 SAP 응용 세션의 패킷인지를 확인할 수 있다.

[0081] 트래픽 분석 장치(20)는 수집된 패킷이 신규 SAP 응용 세션의 패킷이면, 신규 SAP 응용 세션의 정보를 등록한다(S640). 이때, 신규 SAP 응용 세션의 정보는 해당 세션의 4 튜플을 해쉬 처리한 해쉬값일 수 있다.

[0082] 트래픽 분석 장치(20)는 기등록된 SAP 응용 세션 및 신규 SAP 응용 세션의 패킷이 클라이언트에서 서버로 송신되는 클라이언트 송신 데이터(=요청 데이터)인지를 확인한다(S650).

[0083] 트래픽 분석 장치(20)는 해당 SAP 응용 세션의 패킷이 요청 데이터이면, 그 내용으로부터 SAP 시스템 ID, 사용자 ID, SAP 응용 서비스를 위한 프로그램 이름, 트랜잭션 코드 및 메시지 중 적어도 하나를 파싱(Parsing)한다(S660).

[0084] 트래픽 분석 장치(20)는 파싱된 내용을 XML(eXtensible Markup Language) 포맷으로 객체화한다(S665). 이후, 트래픽 분석 장치(20)는 관리자의 요청시에 객체화된 요청 데이터를 이용하여 SAP 사용자 입력 데이터에 대응하는 GUI 화면을 재현할 수 있다.

[0085] 트래픽 분석 장치(20)는 해당 SAP 응용 세션의 패킷이 응답 데이터(=서버 송신 데이터)이면, SAP 시스템 ID, 사용자 ID(= 클라이언트의 사용자 계정), SAP 응용 서비스를 위한 프로그램 이름, 트랜잭션 코드 및 메시지 중 적

어도 하나를 파싱(Parsing)한다(S670).

[0086] 트래픽 분석 장치(20)는 파싱된 내용을 XML(eXtensible Markup Language) 포맷으로 객체화한다(S675). 이후, 트래픽 분석 장치(20)는 객체화된 응답 데이터를 이용하여 응답 데이터를 수신한 클라이언트 GUI 화면에 대응하는 GUI 화면을 재구성할 수 있다.

[0087] 트래픽 분석 장치(20)는 객체화된 응답 데이터 및 요청 데이터 중 적어도 하나가 기설정된 보안정책에 위반되는지를 확인하고, 위반되면 보안정책에 대응하는 대응 행동을 수행한다(S680).

[0088] 트래픽 분석 장치(20)는 대응 행동, 대응 행동에 대응하는 응답 데이터 및 요청 데이터를 포함하는 로그를 DB(270)에 저장한다(S690).

[0089] 한편, 트래픽 분석 장치(20)는 (S630)단계의 확인결과, 수집된 패킷이 신규 SAP 응용 세션의 패킷이 아니면, 해당 패킷을 삭제한다(S700).

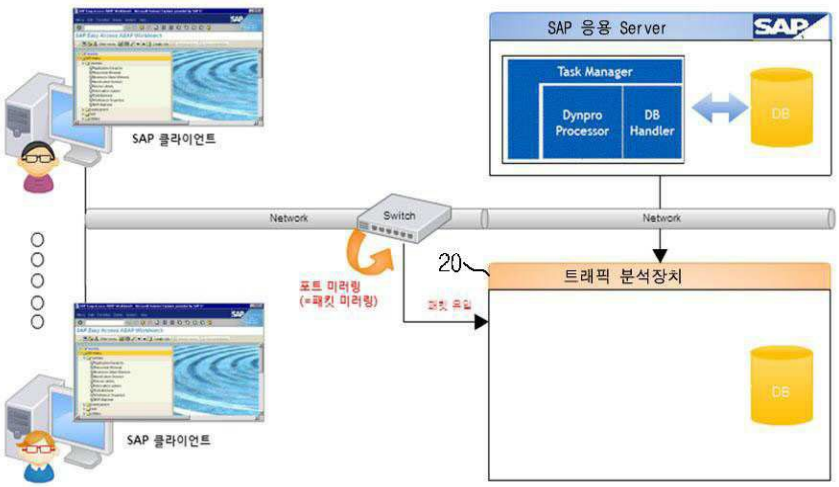
[0090] 이와 같이, 본 발명의 실시예는 SAP 전사자원 시스템 등과 같이 개인정보, 민간정보의 송수신이 많은 시스템에 접속한 클라이언트의 IP 주소, 사용자 ID, 트랜잭션 코드 등을 기반으로 비정상적인 요청 행위를 감사할 수 있다.

[0091] 또한, 본 발명의 실시예는 SAP 시스템에서 발생된 에러 메시지나, 클라이언트의 요청 내역 및 그에 대응하는 응답 내용을 클라이언트의 GUI 화면과 동일하게 재현해줄 수 있어, 관리자의 시스템 에러 확인 및 감시정보의 유출 상황 확인을 도울 수 있다.

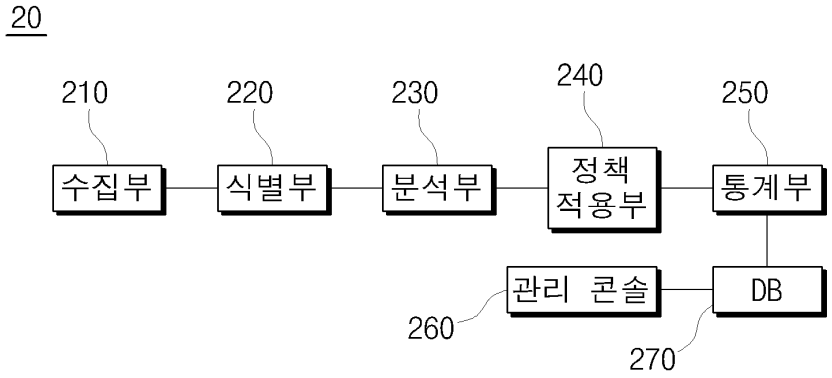
[0092] 이상, 본 발명의 구성에 대하여 첨부 도면을 참조하여 상세히 설명하였으나, 이는 예시에 불과한 것으로서, 본 발명이 속하는 기술분야에 통상의 지식을 가진자라면 본 발명의 기술적 사상의 범위 내에서 다양한 변형과 변경이 가능함은 물론이다. 따라서 본 발명의 보호 범위는 전술한 실시예에 국한되어서는 아니되며 이하의 특허청구범위의 기재에 의하여 정해져야 할 것이다.

도면

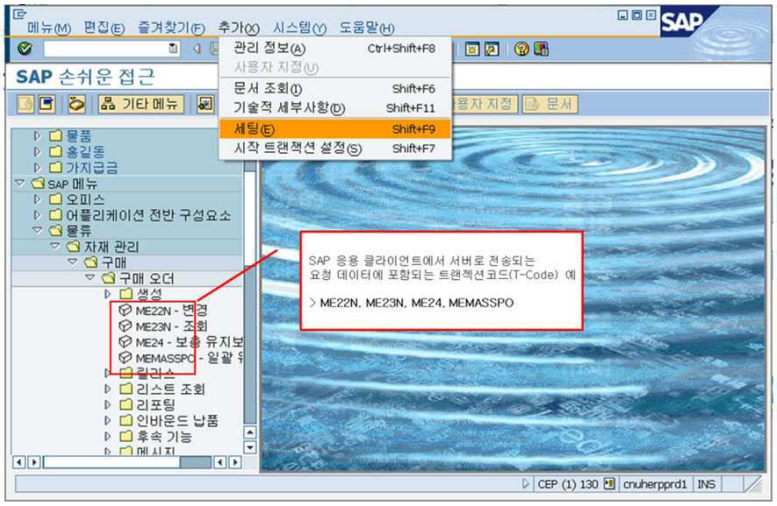
도면1



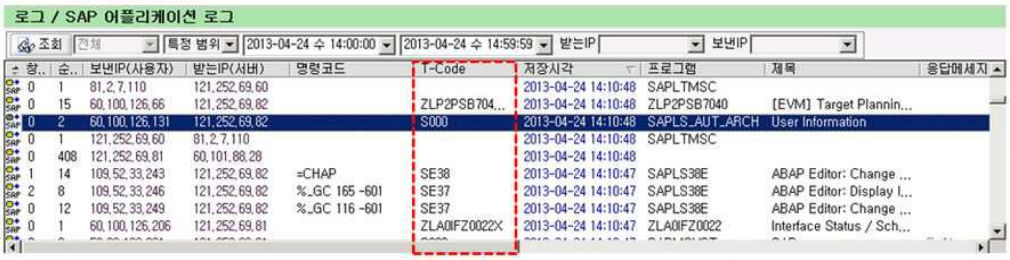
도면2



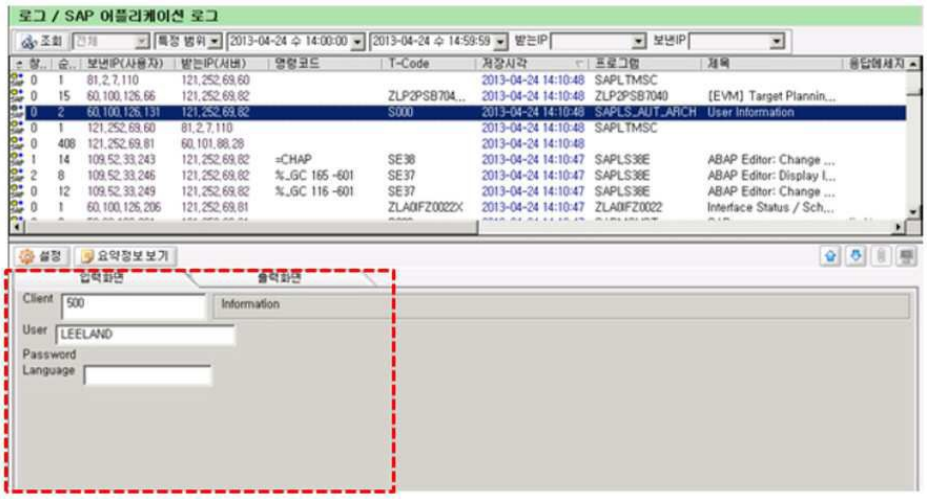
도면3a



도면3b



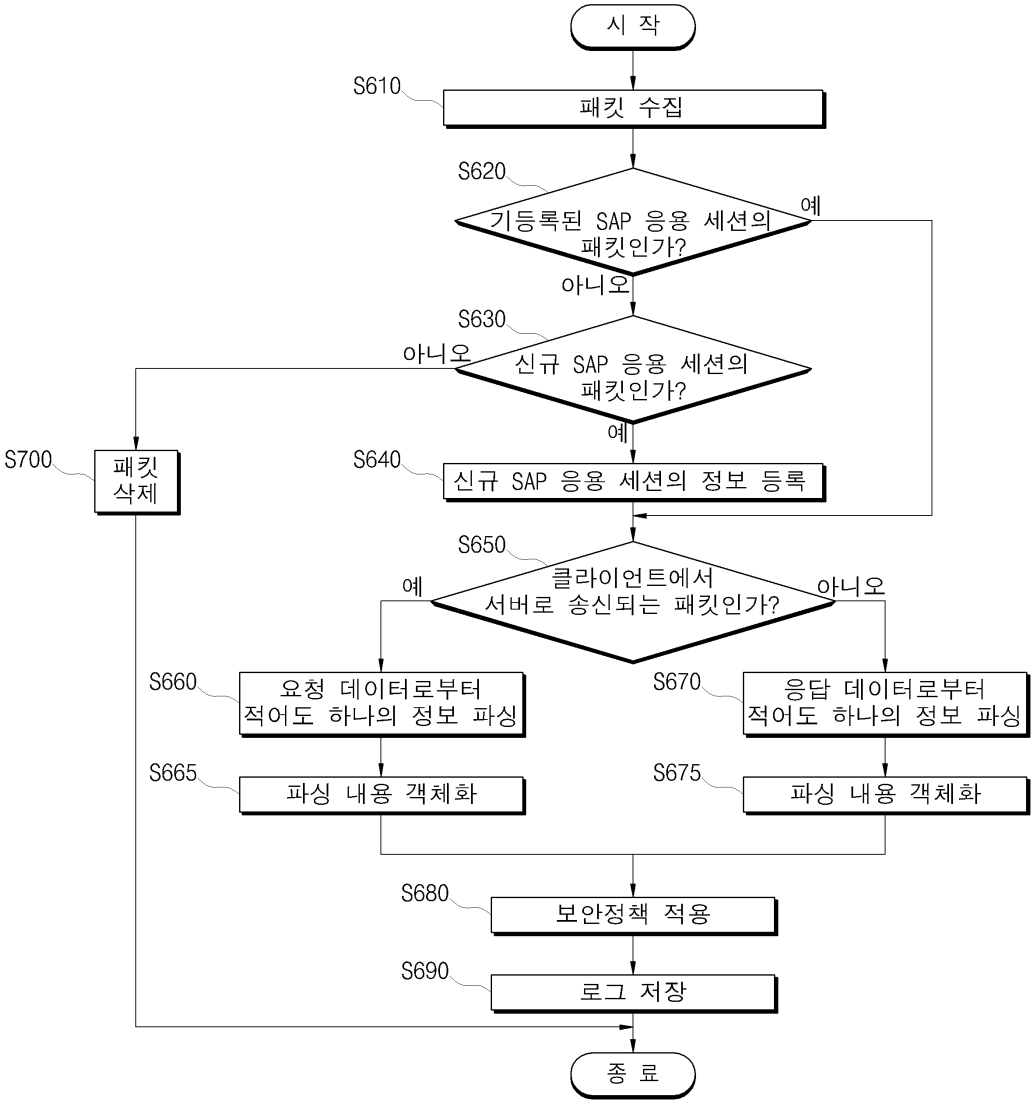
도면4


로그 / SAP 어플리케이션 로그
조회
설정
요약정보보기
입력화면
출력화면
Client
500
Information
User
LEELAND
Password
Language

도면5


로그 / SAP 어플리케이션 로그
조회
설정
요약정보보기
입력화면
출력화면

도면6



【심사관 직권보정사항】

【직권보정 1】

【보정항목】 청구범위

【보정세부항목】 청구항 제2항 2번째 줄

【변경전】

"상기 목적지 포트 정보"

【변경후】

"목적지 포트 정보"

【직권보정 2】

【보정항목】 청구범위

【보정세부항목】 청구항 제12항 2번째 줄

【변경전】

"상기 목적지 포트 정보"

【변경후】

"목적지 포트 정보"

【직권보정 3】

【보정항목】 청구범위

【보정세부항목】 청구항 제11항 10번째 줄

【변경전】

"상시 네트워크 패킷이 상기 기등록된 SAP 세션"

【변경후】

"상기 네트워크 패킷이 상기 기등록된 SAP 세션"