엔소프테크놀러지

TScan 제품 소개서

(개인정보 접속이력 상시 모니터링 및 분석 솔루션)

2015.05.

PRODUCT
INTRODUCTION

제품개발 : ㈜엔소프테크놀러지 서울시 영등포구 여의도동 14-24 삼보호정빌딩 9F
제품공급 : ㈜스마트원씨앤에스 서울시 구로구 디지털로 31길 53 1005(구로3동 이앤씨벤처드림타워5차)
Tel : 02-862-0862, HP : 010-6351-7411, proyhkim@smartonecns.co.kr 김양현 영업대표

Contents

I 개인정보보호법

1. 개인정보보호법

개인정보보호법 추진배경

01 개인정보관련 사고 증가

- 외부해커에 의한 개인정보 유출
- 내부사용자의 업무거래를 통한 개인정보 유출사고
- IT개발자의 프로그램 실행을 통한 개인정보 유출사고

개인정보유출 사고

2011.04	H사 175만명 개인정보 유출
2011.04	S사 3천5백만명 유출
2011.08	E사 35만명 개인정보 유출
2013.12	K사 1억만건 개인정보 유출 등

02 개인정보보호 법규 강화

- 개인정보 접속기록의 생성 및 보관
  (법 제29조, 영 제30조, 개인정보의 기술적 관리적 보호조치기준 제 5조)
- 개인정보 유출통지 및 신고제
  (법 제34조, 영 제39조, 표준지침 27조)
- 개인정보 분쟁조정 및 단체소송 대비 (법 제43조)

개인정보보호법 시행

2008.11	개인정보보호법 정부안 국회제출
2011.04	국회 본 회의 통과
2011.09	개인정보보호법 시행
2013.06	개인정보보호법 개정
2014.08	개인정보보호법 개정안 시행

- 분실, 도난, 유출, 변조의 경우 최고 5억 과징금 부과
- 개인정보 법령 위반 시 CEO 징계권고

03 정보보호대책 IT 이행 과제

- 관리적 보안 강화
  정보보호 관리체계 강화, 보안관리 활동강화
- 기술적 보안 강화
  IT 인프라 보안 강화, 침해사고 대응 강화
  개인정보(고객정보) 유출방지

개인정보 안전성 확보 강화

- 개인정보 암호화
- 개인정보 접근통제
- 개인정보 접속기록 보관
- PC 사용환경 개선 등

개인정보보호법 준수를 위한 안전성 확보 조치

개인정보보호법 시행령 제30조 (개인정보의 안전성 확보 조치)

개인정보처리자는 법 제29조 [(안전조치의무) 개인정보처리자는 개인정보가 분실 · 도난 · 유출 · 변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적 · 관리적 및 물리적 조치를 하여야 한다] 에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.

개인정보 보호업무 조직 구성	개인정보의 안전한 처리를 위한 내부 관리계획의 수립 · 시행
시스템 및 DB접근제어	개인정보에 대한 접근 통제 및 접근 권한의 제한 조치
DB암호화 및 통신구간 암호화	개인정보를 안전하게 저장 · 전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치
개인정보 접속이력 생성 보관	개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조 · 변조 방지를 위한 조치
백신, DLP, PC 스캔 등을 통한 보안	개인정보에 대한 보안프로그램의 설치 및 갱신
시건 장치 등 물리적 보안	개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금 장치의 설치 등 물리적 조치

개인정보보호법 주요내용 – 접속기록의 생성 및 보관

개인정보보호법 시행령 제30조 (개인정보의 기술적 관리적 보호조치기준 제 5조)

개인정보 접속기록 보관/생성

접속기록 보관/생성

- 접속 기록은 월 1회 이상 정기적으로 확인, 감독
- 접속 기록은 6개월 또는 1년 이상 보존, 관리
- 위, 변조 방지를 위한 정기적인 백업을 수행

접속기록 보관예시

① 정보주체 식별정보	② 취급자 식별정보	③ 접속 일시	④ 접속지	⑤ 수행 업무
123456789	홍길동 (User1)	2014.01.24 17:00:00	192.108.10.1	대출신청

① 정보주체 식별정보 ② 취급자 식별정보(사용자 ID)
③ 접속 일시 ④ 접속지 IP ⑤ 사용 업무

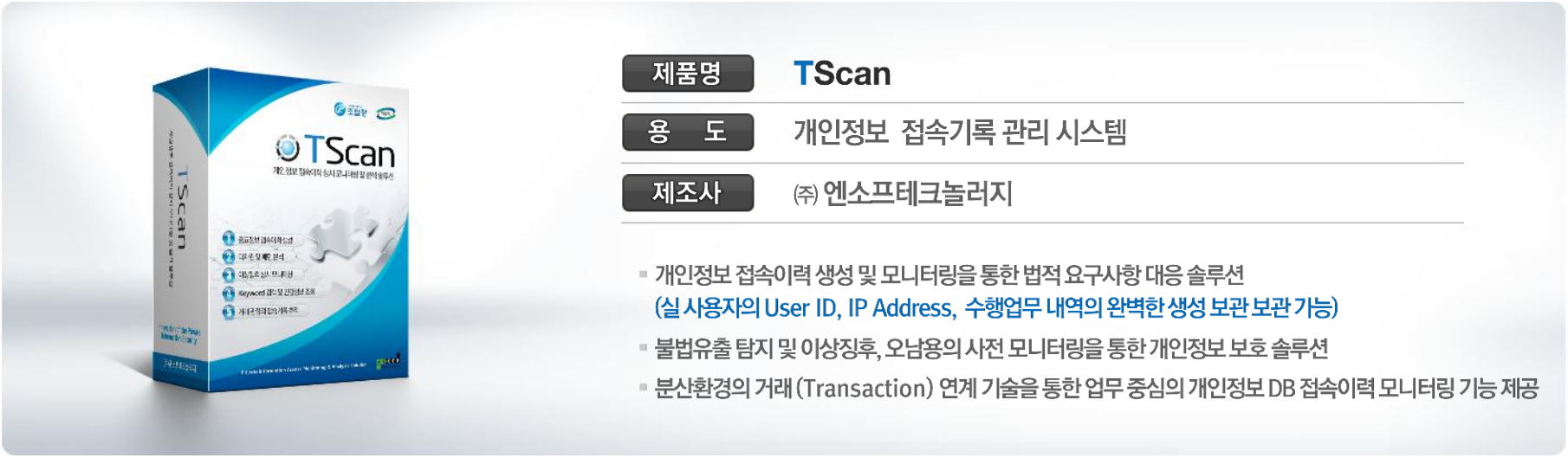
II TScan 소개

2.1 솔루션의 개요

2.2 솔루션 구성도

2.3 솔루션 개념도

2.1 솔루션의 개요



제품명	TScan
용 도	개인정보 접속기록 관리 시스템
제조사	㈜ 엔소프테크놀러지

- 개인정보 접속이력 생성 및 모니터링을 통한 법적 요구사항 대응 솔루션
  (실 사용자의 User ID, IP Address, 수행업무 내역의 완벽한 생성 보관 보관 가능)
- 불법유출 탐지 및 이상징후, 오남용의 사전 모니터링을 통한 개인정보 보호 솔루션
- 분산환경의 거래 (Transaction) 연계 기술을 통한 업무 중심의 개인정보 DB 접속이력 모니터링 기능 제공

Authentication (인증)

- 핵심 원천기술 특허 등록
- GS 인증 획득
- 조달청 조달등록

Authorization (권한)

- 암호화 통신을 통한 관리프로그램 제공
- 사용자 접근권한에 따른 정책설정
- C/S 환경의 관리자 환경설정 툴 별도제공
- 2 Factor 인증 제공 (2차, 지정맥 인증)

Administration (관리)

- 개인정보 처리현황분석 및 모니터링
- 개인정보 오남용 현황 분석 및 모니터링
- 개인정보 과다접근 모니터링
- 개인정보 접속이력 관리리포트 제공
- 개인정보 취급에 따른 사용 이력 관리
- 솔루션 사용자 변경내역 관리
- 개인정보 접근이력 상시 모니터링
- 인스턴스 상태 확인

2.2 솔루션 구성도

수집/분석

- 정보흐름의 전사가시성 확보
- 키워드, 상세내역 분석
- 위험분석및 다차원분석
- 통계기능 제공

접속이력 생성

- 일체의 SW 수정 없음(BCI 기술)
- 개인정보 포함거래 식별
- 5W1H 기반의 접속기록 생성
- 압축 및 암호화 적용 :
- 거래 중심의 TUID연계

DB 접속이력 생성

- 다양한 C/S 환경의 접속로그 생성
- (Orange, Toad, SQL Plus, Client SAS,VB, Delphi 등)

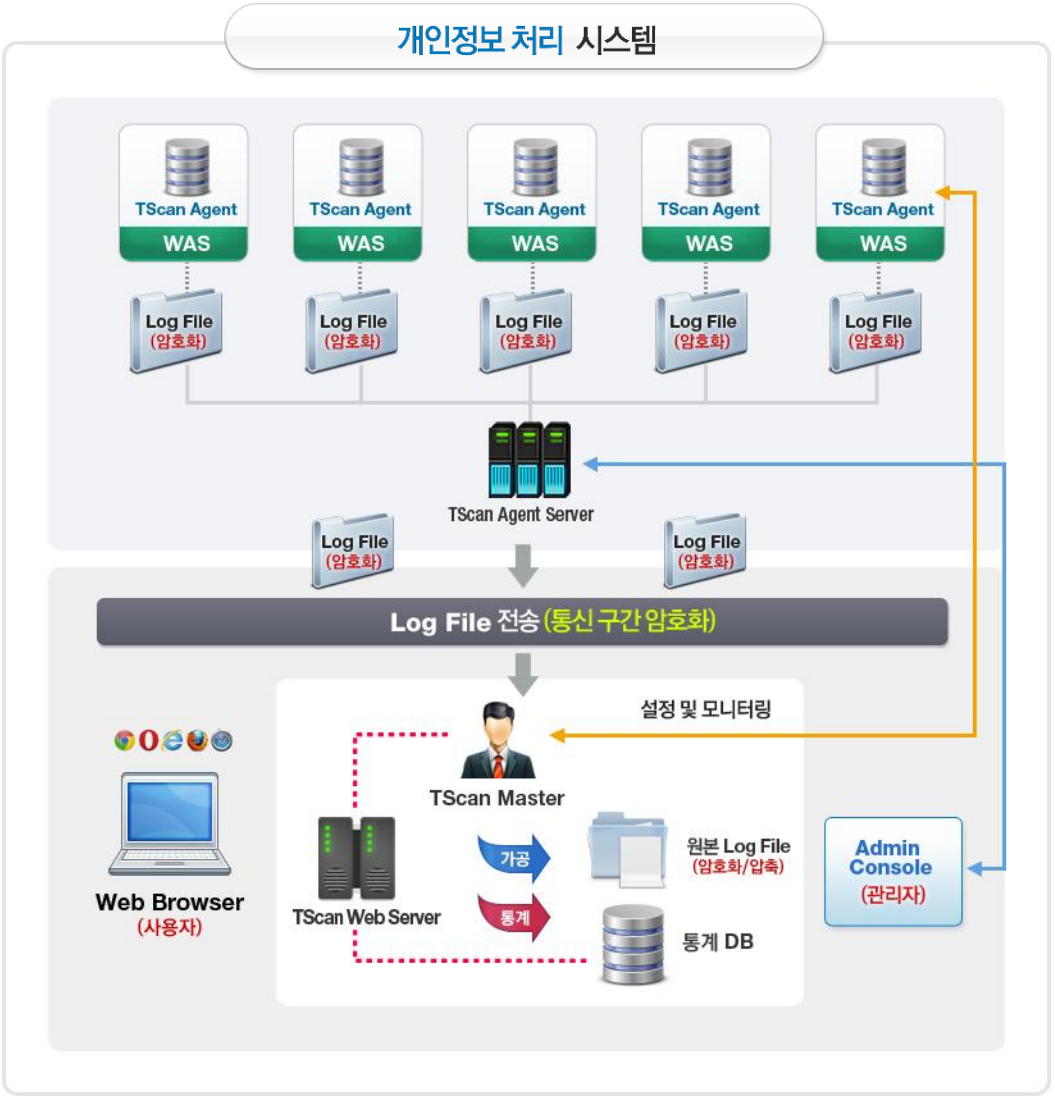
개인정보 상시 모니터링 시스템

- 대용량 원시로그 저장
- 개인정보 데이터 정제
- 개인정보 이상징후 분석
- 고속 (접속이력) 검색

DB Agent (option)

- 2tier 환경 개인정보 접속기록 생성

2.3 솔루션 개념도



1 TScan Agent

로그 생성(관리)

- 5H1W기반 접속로그 생성
- 거래 중심의 TUID 연계
- 시스템 리소스 점검
- 서비스 로그 압축 및 암호화 지원

2 TScan Agent Server (수집서버)

로그 수집

- 실시간 로그 수집
- 능(수)동적 로그 수집
- 암호화 구간 지원

3 TScan Master (분석서버)

위험도 산정관리

- 위험요소 도출
- 위험도 기준설정

백업

- 압축 저장 관리
- 암호화 저장관리

기반구조확장

- 위험 알림 연동
- 이중화 지원
- 기 운영 솔루션 로그 연동

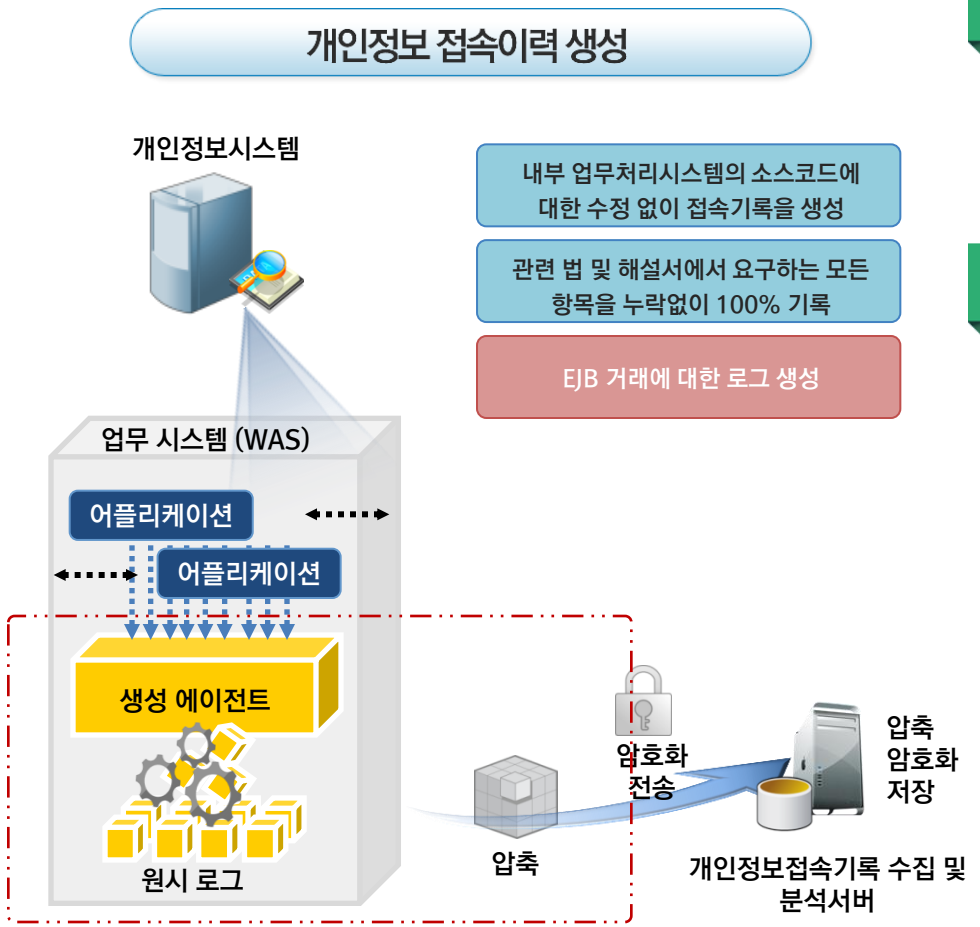
4 Admin Tool

관리

- 로그 레벨설정
- 토폴로지 제공
- 2 Factor 인증
- Agent 상태점검
- 시스템 리소스 정보
- 로그 포멧 정규화
- 연계규약 정의
- 통계 데이터 관리
- 배치/백업 프로세스

Ⅲ TScan 주요기능

"일체의 업무 프로그램 수정 없는" 안정적인 접속기록 생성 방식



개인정보 접속이력 생성

- 거래연계 TUID
- 관련법 준수를 위한 5W 1H 기반
- 호환성 (H/W,OS 관계없이 생성)
- BCI 기술 기반 생성기술 적용

주요 적용기술

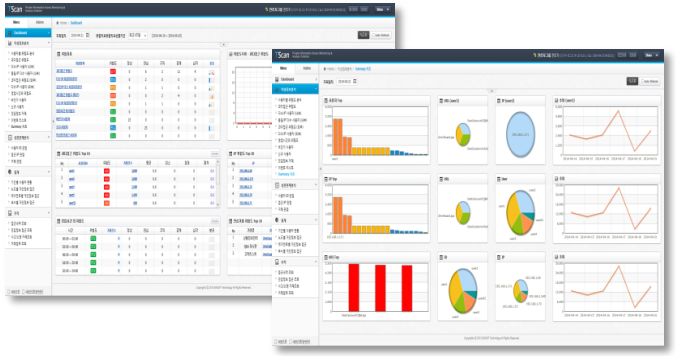
동적인 BCI 기술 적용	실시간 E2E 트랜잭션 연계기술
소스 수정없이 적용	End-to-End 트랜잭션 추적
자동으로 필요 코드 삽입	TUID(연계 아이디) 생성 및 유지
업무프로세스와 독립된 프로세스	EJB 등 분산환경 지원

WAS 무중단 기술 적용	생성모듈 무효화/압축 암호화
접속로그 추출 룰 적용 기능	Agent 기능 무효화 By pass
원격 일괄 Config/Rule 적용 기능	저장공간 최소화 7-ZIP 알고리즘
접속기록 관리시스템 정책 설정	DES,SEED,AES128 이상 제공

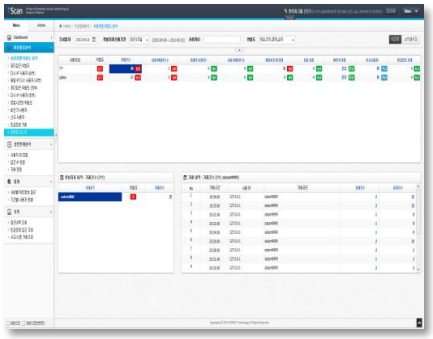
3.2 개인정보접속이력 분석 및 모니터링

TScan은 개인정보의 오남용 현황을 상시 관리하여 이상징후 발생시 **개인정보 유출 위험에 대한 신속한 대응**이 가능하도록 지원합니다.

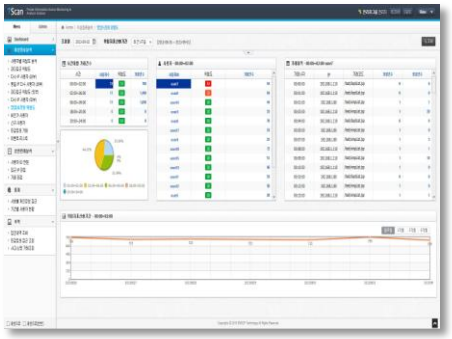
개인정보 접속이력 이상징후 현황 및 분석



개인정보 이상징후 모니터링



사용자 별 이상징후 모니터링



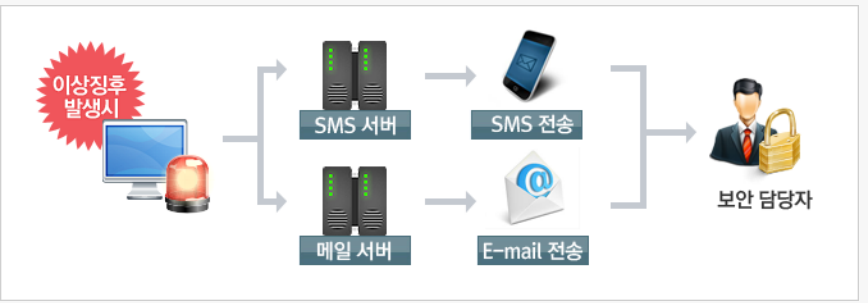
업무시간외 이상징후 모니터링

이상징후

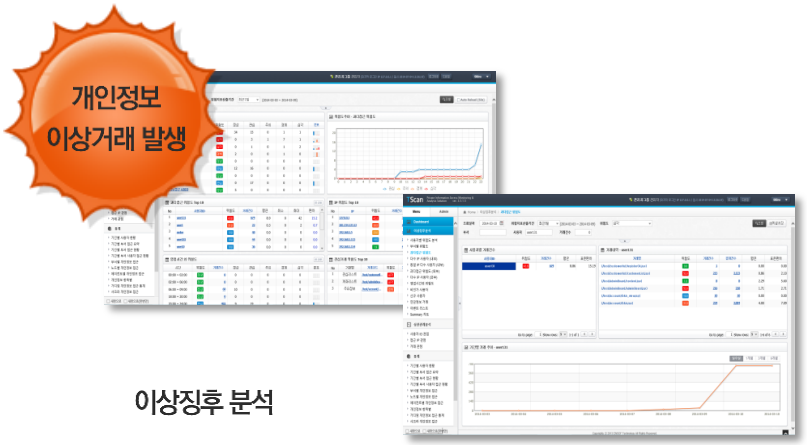
- 개인정보 과다 거래
- 비인가 사용자 거래
- 업무시간외 거래
- ID, IP 중복 사용 거래 등

이상징후 대응

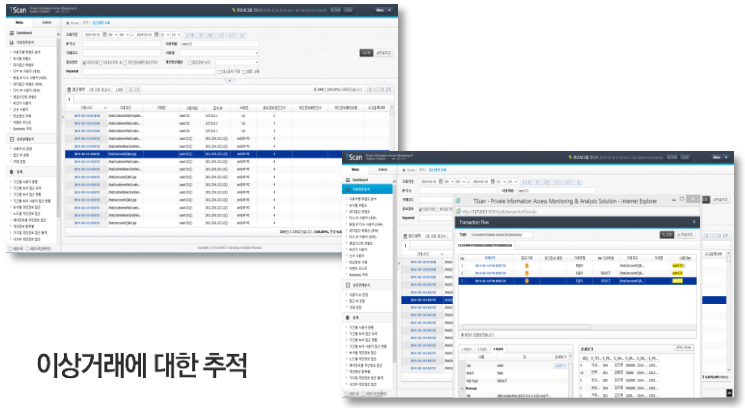
- 사용자 별 개인정보 오남용 현황 제공
- 사용자 별 개인정보 접근 (이상징후) 현황제공
  다수의 IP 사용자, 외부 IP 사용자 등
- 사용자의 업무시간외 거래에 대한 (이상징후) 현황제공
- 동일 IP 다수사용자에 대한(이상징후)현황제공
- 비인가 사용자의 개인정보 접근에 대한 (이상징후) 현황제공
- 이상징후 발생시 알람을 통한 신속 대응지원 (SMS, Email, 화면경보)
- 이상징후 의심 시 소명기능을 통한 개인정보처리자의 소명요청 기능 제공



3.3 이상거래 추적 및 상세조회



이상징후 분석



이상거래에 대한 추적

TScan의 개인정보접근이력 대한 검색기능(역 추적) 및 상세내역 확인을 통해 개인정보 접근 정보를 정확하게 확인 할 수 있도록 합니다.

- ✓ 개인정보 오남용 사용자에 대한 상세 거래내역을 조회
- ✓ **KeyWord** 검색 기능 등 제공
  개인정보 이상거래 판단

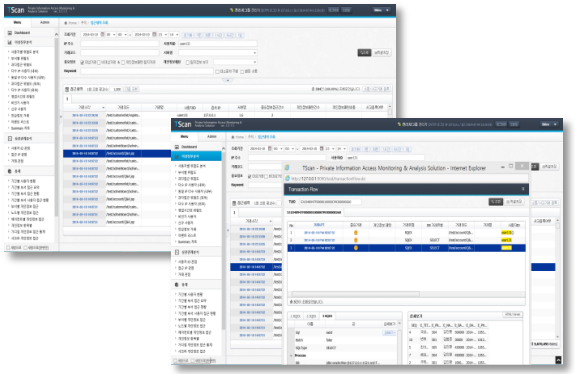
개인정보 모니터링 » 이상징후 발생(알림) » 이상거래 분석 » 이상거래 추적 » 이상거래 소명(판정)

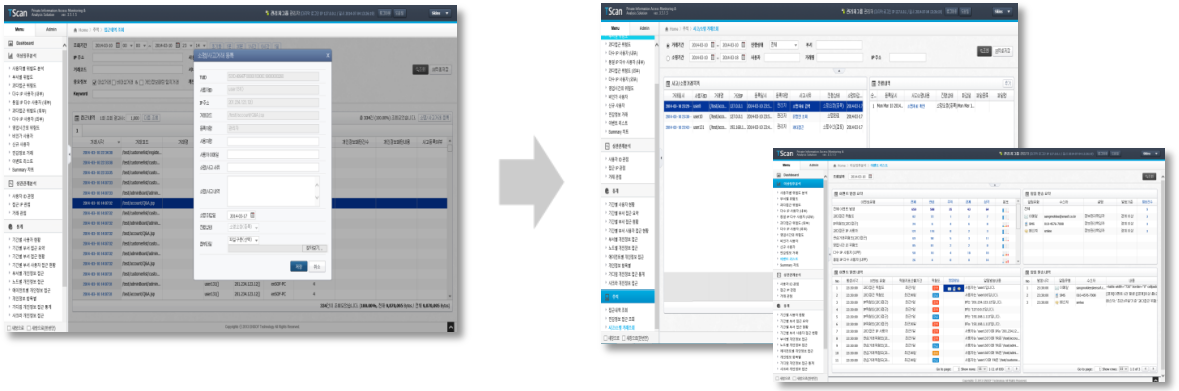
개인정보 유출통지 및 신고제 (법 제34조, 표준지침 27조, 영 제39조)관련 개인정보 Access 내역 통지의무에 대응 할 수 있는 상세 정보 제공.

- ✓ **TUID**, 거래시각, 거래유형, 중요거래
- ✓ **Process**
  - End Time, Protocol, DBIO, Error
  - InputDataType, OutputDataType
  - DetailCount, DAO, DB, StatementID
  - Result, ResultID
- ✓ **Parameter**
  - SqlConstanceValues, Parameter
- ✓ **SQL**
  - SqlID, SqlDescription, Sql, Batch

3.4 이상거래 소명 판정

이상거래에 대한 추적 및 소명/판정을 통하여 개인정보 유출에 대한 사전 대응이 가능하도록 지원합니다.





이상거래에 대한 추적

①사용자의 거래내역 분석

- 사용자의 거래 분석, 기간별 거래추이 분석

②접근내역에 대한 상세 추적

- IP, ID, 코드 별, 서버명, Keyword, 개인정보패턴

③상세내역 확인 (RQEX, SQEX)

이상거래에 대한 소명 / 판정

①확인된 이상거래에 대한 소명 등록

②소명된 내용 확인 및 판정

- 소명요청, 소명수신,(검토), 소명완료, 마감일 관리

VI 구축사례

4.1 TScan 구축사

4.2 P생명 구축사례

4.1 TScan 구축사

한국남동발전(주)
- 23여 개 업무시스템
- DB접근제어 솔루션 연동
- Oz Report 연동

한국중부발전(주)
- 10여 개 업무시스템
- DB접근제어 솔루션 연동
- DMZ(IIS환경)

한국장애인고용공단
- 다수의 업무시스템
- 최단 기간 구축 (구축 2주/안정화 2주)

Sky Life
- 다수의 업무시스템
- 인사DB연동, 그룹웨어 연동(Email)

한국보건복지정보개발원
- 다수의 업무시스템
- 기 운영 중인 솔루션과 연동
- 일 트랜잭션 350만건

한국폴리텍대학
- 10여 개 업무시스템
- 기 운영 중인 솔루션과 연동
- 분석 및 수집 서버 이중화 구현

삼성꿈장학재단
- 20여 개 업무시스템
- 통합로그관리 솔루션과 연계

부산교통공사
- 10여 개 업무시스템
- 인사DB연동

4.1 TScan 구축사

한국전기안전공사
- 35여 개 업무시스템
- 인사조직도 연동

한국연구재단
- 69여 개 업무시스템
- DB접근제어 솔루션 연동
- 인사 조직도 연동

SK트레이딩 인터내셔널
- 다수의 업무시스템
- 기 운영 중인 통합로그관리 솔루션과 연동
- 인사 조직도 연동, 그룹웨어 연동(Email)

SK에너지
- 다수의 업무시스템
- 기 운영 중인 통합로그관리 솔루션과 연동
- 인사 조직도 연동, 그룹웨어 연동(Email)

SK종합화학
- 다수의 업무시스템
- 기 운영 중인 통합로그관리 솔루션과 연동
- 인사 조직도 연동, 그룹웨어 연동(Email)

SK루브리컨츠
- 다수의 업무시스템
- 기 운영 중인 통합로그관리 솔루션과 연동
- 인사 조직도 연동, 그룹웨어 연동(Email)

SK인천석유화학
- 다수의 업무시스템
- 기 운영 중인 통합로그관리 솔루션과 연동
- 인사 조직도 연동, 그룹웨어 연동(Email)

SBI 저축은행
- 44여 개 업무시스템
- TScan DB agent 도입

4.1 TScan 구축사

IBK 연금보험
- 30여 개 업무시스템
- 통합로그관리 솔루션과 연계
- RMI 환경

PCA 생명
- 23여 개 업무시스템
- WAS-EJB-DB 거래정보 및 중요정보 접근기록 보관 및 모니터링

메트라이프 생명
- 30여 개 업무시스템
- WAS-EJB-DB 거래정보 및 중요정보 접근기록 보관 및 모니터링

삼육보건대학교
- 12여 개 업무시스템
- 인사DB연동

에이스생명
- 다수의 업무시스템
- 인사 조직도 연동, 그룹웨어 연동(Email)

친애저축은행
- 다수의 업무시스템
- 인사 조직도 연동, 그룹웨어 연동(Email)

공평저축은행
- 다수의 업무시스템
- 인사 조직도 연동, 그룹웨어 연동(Email)

4.2 P생명보험 구축사례

주관사

㈜엔소프테크놀러지

고객사 P 생명보험 요구사항

① 전자금융감독규정 및 개인정보보호법 등 관련법에서 요구하는 개인정보 접속기록에 대한 규정 준수

② 개인정보 사용현황 확인 및 유출 시 통지를 위한 역 추적 기능

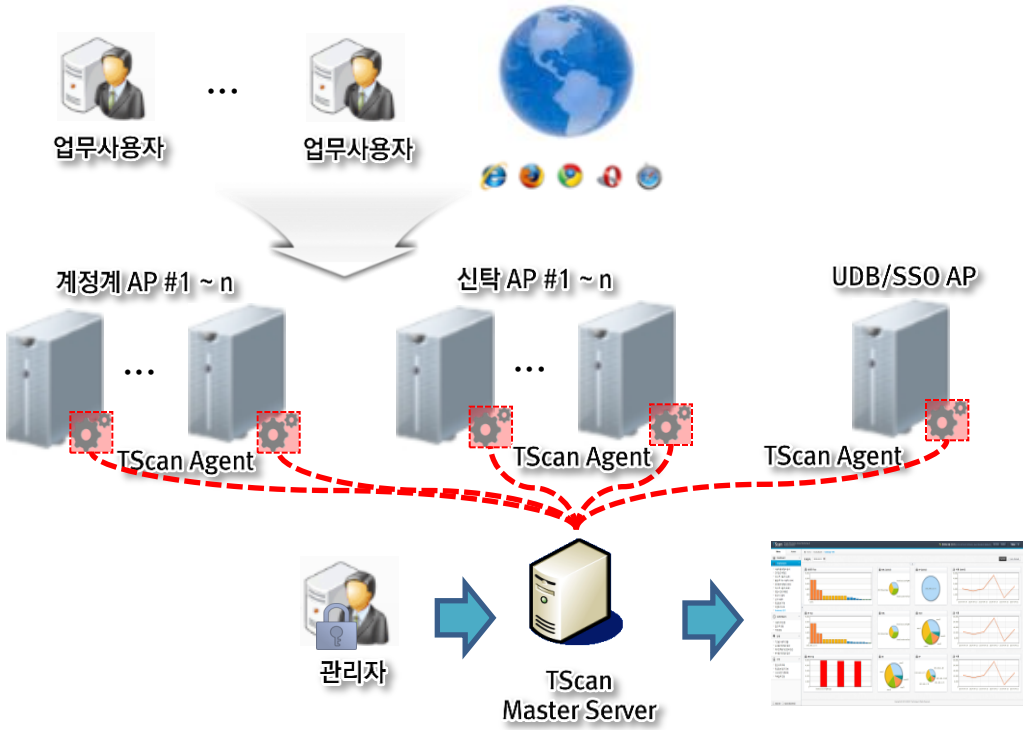
③ W사 구매 적합성 불 충족 사유로 최단 기간 도입 솔루션 교체

W사 → 엔소프(TScan)

핵심 성공 요소

- 노하우(경험) Know-How
- 준법성 Compliance
- 전문성 Knowledge
- 연속성 Continuity

구성도



- 구축기간

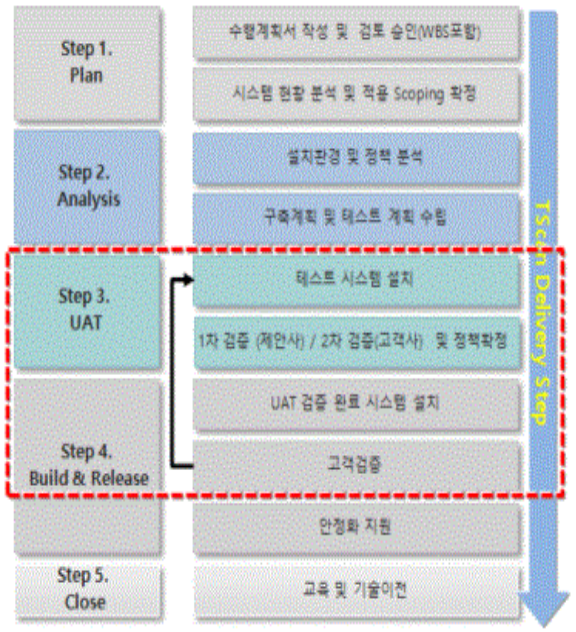
2013.03 ~ 2013.04

- 서비스요약

개인정보보호법 등 관련법규 준수를 위한 솔루션 도입으로 기존 W 사의 솔루션을 구축 중이었으나 프로젝트 중간보고 중 구매 적합성 불 충족 사유로 엔소프테크놀러지의 TScan 으로 교체 구축

4.2 P생명보험 구축사례

구축절차



주요성과

① 전자금융감독규정 및 개인정보보호법 등 관련법규 준수
② 개인정보 접근기록 감시 및 분석을 통한 정보유출사고 사전 대응 체계 마련
③ 개인정보 업무 취급자들에 대한 보안의식 수준 향상
④ 개인정보보호 실태조사 대응

내용

1 Plan

- 구축일정 계획 수립
  ▶구축일정 계획서 작성
  ▶구축 일정계획서 검토, 승인

2 Analyze

- 고객환경분석
  ▶설치환경 조사서양식 제공
  ▶대상 시스템 확정
- TScan Rule 정의
  ▶대상 시스템 Table Filter 정의
  ▶Table Filter 정의서 양식 제공
  ▶Table Filter 정의 확정
- Data Catch Rule 정의
  ▶ Data Catch Rule 정의서 양식 제공
  ▶ Data Catch Rule 정의 확정
- 구축 계획 보고
- 테스트 계획 수립
  ▶ 계획 및 검증 Check List 작성
  ▶ 테스트 시나리오/케이스 작성 – LMS
  ▶ 테스트 시나리오/케이스 작성 – LMS외 정체

3 UAT

- 1개 시스템
  ▶설치, 검증
- 3개 시스템 (점진적 확산)
  ▶설치, 검증
- 4개 시스템 (점진적 확산)
  ▶설치, 검증

4 Build & Release

- 1차 적용(4개 시스템)
  ▶설치작업 요청, 승인, 수행
  ▶고객 검증, 안정화 지원
- 2차 적용(4개 시스템)
  ▶설치작업 요청, 승인, 수행
  ▶고객 검증, 안정화 지원

5 Close

- 교육 및 기술이전
  ▶운영자 교육계획 수립
  ▶기술이전 계획 수립
  ▶운영자 교육 및 기술이전
- 완료보고

감사합니다

제품개발 : ㈜**엔소프테크놀러지** 서울시 영등포구 여의도동 14-24 삼보호정빌딩 9F

제품공급 : ㈜**스마트원씨앤에스** 서울시 구로구 디지털로 31길 53 1005호 (구로3동 이앤씨벤처드림타워5차)
Tel : 02-862-0862, HP : 010-6351-7411, 김양현 영업대표 proyhkim@smartonecns.co.kr