개인정보 오남용 감사

어플리케이션 사용자에 대한 감사 및 모니터링 방안

목차

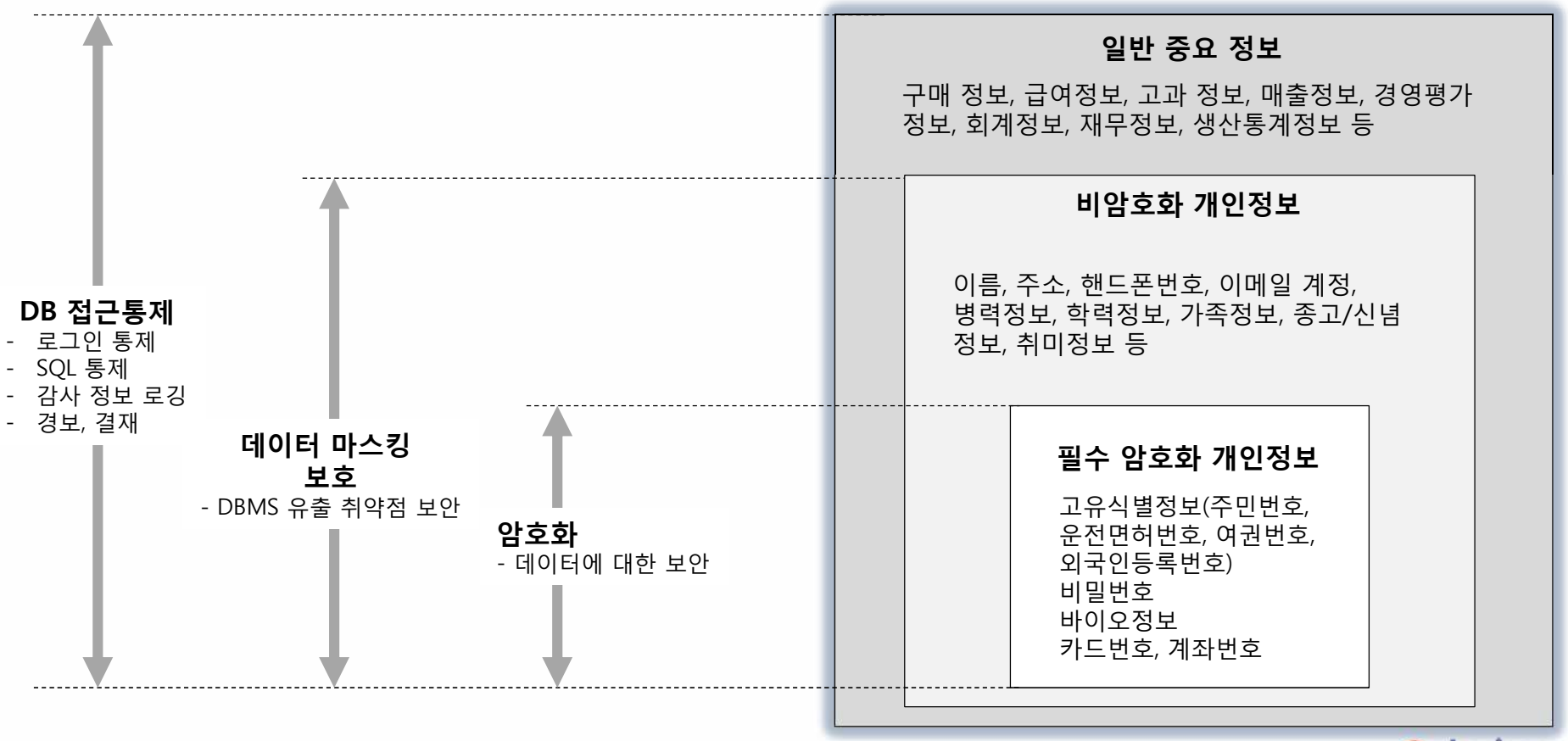
개인정보보호법에 대한 대응

[개인정보의 안전성 확보조치 기준 : 제정 2011.09.30.]

조항	항목	안정성 확보조치 기준	해 석
4조	1항	개인정보처리자는 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 **최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.**	DB접근통제
4조	2항	개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 **개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소**하여야 한다.	DB접근통제
4조	3항	개인정보처리자는 제1항 및 제2항에 의한 **권한 부여, 변경 또는 말소에 대한 내역을 기록**하고, 그 기록을 **최소 3년간 보관**하여야 한다.	DB접근통제
4조	4항	개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우, **개인정보취급자 별로 한 개의 사용자 계정을 발급**하여야 하며, **다른 개인정보취급자와 공유되지 않도록** 하여야 한다.	DB접근통제
5조	1항	개인정보처리자는 개인정보취급자 또는 정보주체가 **안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용**하여야 한다.	DB접근통제
7조	1항	영 제25조 및 영 제33조에 따라 암호화하여야 하는 **개인정보는 고유식별정보, 비밀번호 및 바이오정보**를 말한다.	암호화범위
7조	2항	개인정보처리자는 제1항에 따른 개인정보를 **정보통신망을 통하여 송.수신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화**하여야 한다.	DB암호화
7조	3항	개인정보처리자는 **비밀번호 및 바이오 정보는 암호화하여 저장**하여야 한다. **단 비밀번호를 저장하는 경우에는 복호화되지 않도록 일방향 암호화하여 저장**하여야 한다.	DB암호화
7조	4항	개인정보처리자는 인터넷 구간 및 **인터넷 구간과 내부망의 중간 지점**(DMZ : Demilitarized Zone)에 **고유식별정보를 저장하는 경우에는 이를 암호화**하여야 한다.	DB암호화
7조	5항	개인정보처리자가 내부망에 고유식별정보를 정장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다. 1.법 33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과 2.위험도 분석에 따른 결과	DB암호화 적용여부 (영향평가)
7조	6항	개인정보처리자는 제1항에 따른 개인정보를 암호화하는 경우 **안전한 암호알고리즘으로 암호화하여 저장**하여야 한다.	암호화 기준
7조	8항	개인정보처리자는 **업무용 컴퓨터**에 **고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화 저장**하여야 한다.	암호화
8조	1항	개인정보처리자는 개인정보취급자가 **개인정보처리시스템에 접속한 기록을 최소 6개월 이상 보관·관리**하여야 한다.	DB접근통제
8조	2항	개인정보처리자는 개인정보취급자의 **접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관**하여야 한다.	DB접근통제

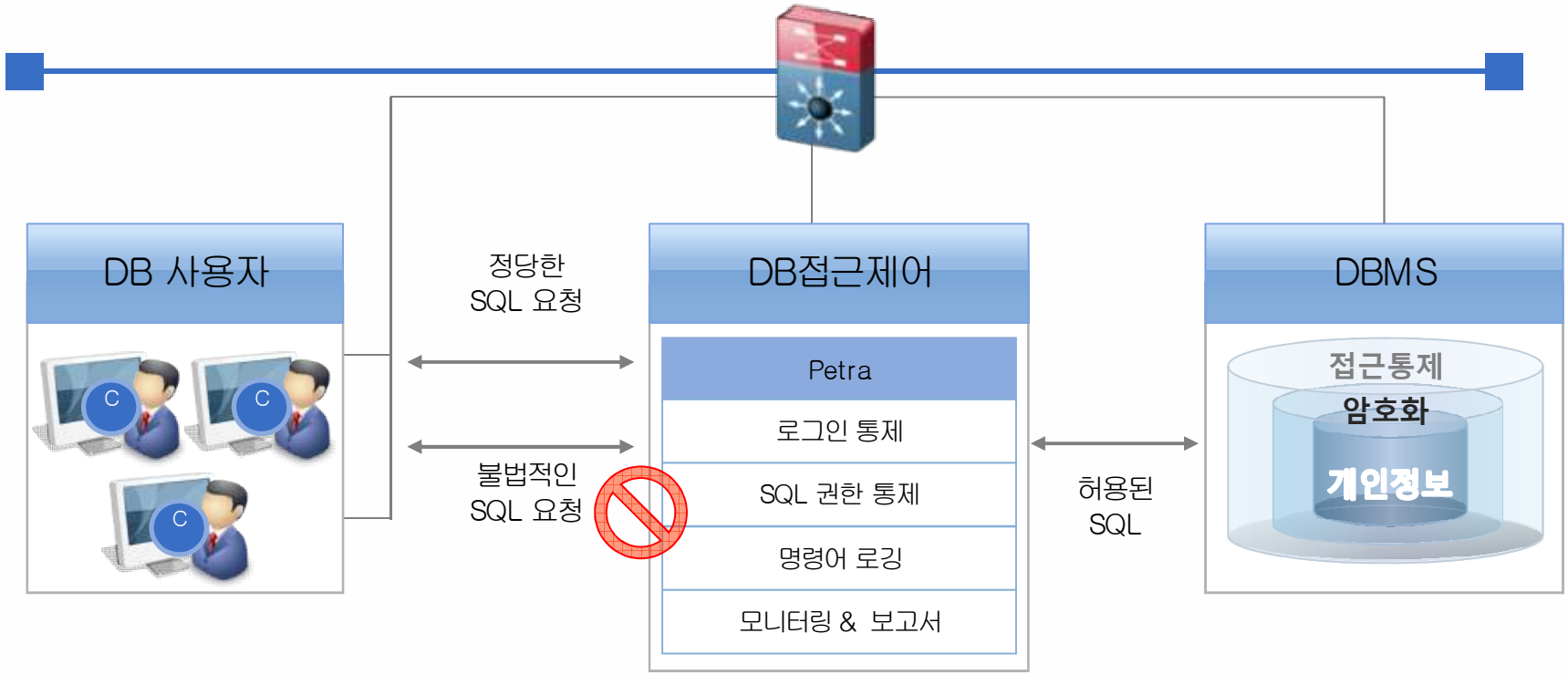
개인정보보호법에 대한 대응

- DB에 접근하여 수행하는 모든 SQL을 저장하고, 작업 수행에 꼭 필요한 권한만을 사용할 수 있도록 통제하기 위하여 DB접근제어 사용
- 법에서 규정한 암호화 대상 컬럼은 DB암호화 솔루션을 이용하여 암호화 후 복호화 권한 통제
- 비암호화 대상 개인정보는 데이터 마스킹을 적용하여 보호



DB 접근제어 및 암호화의 한계

DB서버에 직접적으로 접속할 수 있는 내부 사용자만을 대상으로 통제하도록 되어 있음. 어플리케이션을 통해 데이터를 취급하는 **개인정보취급자 전체를 포괄하지 못합니다.**



DB 접근제어 및 암호화의 한계

개인정보 유출 사고를 통해 기존 솔루션의 한계를 알 수 있습니다.

건강보험공단 개인정보 70여 만 건 유출 (2008. 11. 12)

- 경기지방경찰청 사이버수사대는 12일 건강보험 가입자와 금융기관 고객 등 70여만명의 개인정보를 빼내 채권추심에 이용한 채모(33)씨 등 12개 신용정보업체 직원 140명을 정보통신망 이용촉진 및 정보보호 등에 관한 법률 위반 등 혐의로 불구속 입건

- 채씨 등 신용정보업체 직원들은 지난해 1월부터 올해 1월까지 **2개 병원에서 훔친 건강보험공단 시스템 접속용 아이디와 비밀번호, 공인인증서로 공단시스템에 접속한 뒤 추심대상 채무자 70여만명의 개인정보를 조회**해 이를 채권 추심에 이용

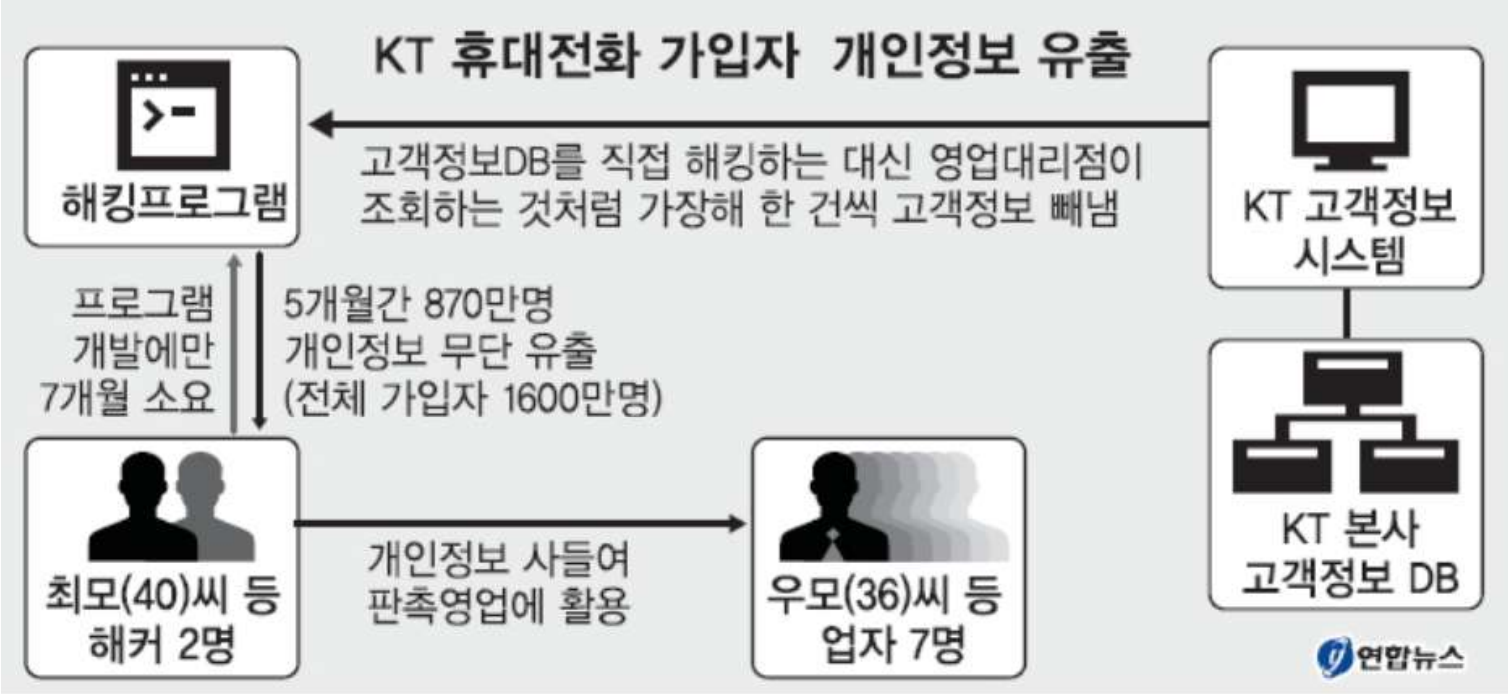
- **신용정보업체 직원들에게 돈을 받고 고객 2만여명의 금융거래정보를 유출한 혐의**(금융실명거래 및 비밀보장에 관한 법률 위반)로 은행원 전모(33)씨를 구속

- 구속된 전씨는 채권추심원들에게 1건당 700원에서 1천원씩 모두 1천500여만원을 받고 지난해 9월부터 지난달까지 자신이 근무하는 은행의 전산망에 접속해 채무자 2만여명의 계좌 개설 여부와 예치금액 등 금융거래정보를 유출한 혐의를

DB 접근제어 및 암호화의 한계

개인정보 유출 사고를 통해 기존 솔루션의 한계를 알 수 있습니다.

2012. 7. 30

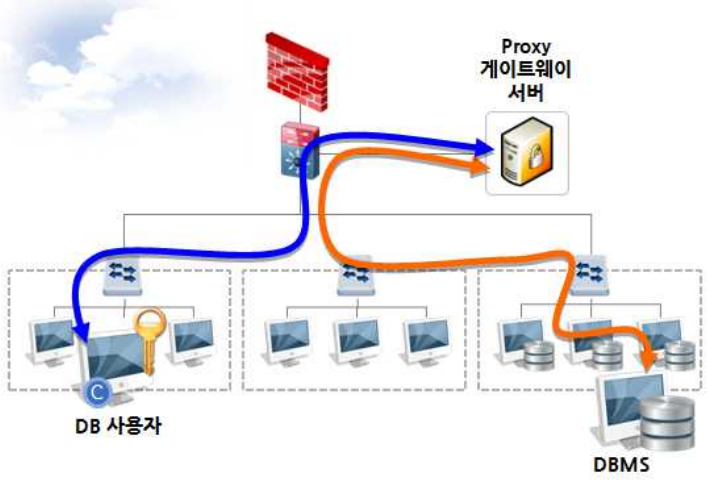


- 정보통신업체에서 10년간 프로그램 개발을 담당하는 등 베테랑 프로그래머였던 최씨는 영업대리점이 고객정보를 조회하는 것처럼 꾸며 한두 건씩 개인정보를 교묘하게 빼내
- KT는 5개월 동안이나 고객정보가 유출당한 사실을 알아차리지 못하다 뒤늦게 내부 보안점검을 통해 해킹 피해를 확인
- 유출된 개인정보에는 이름과 주민등록번호, 휴대전화 번호 및 모델명, 기본요금과 사용요금제, 요금합계액, 기기변경일 등 핵심정보가 대부분 포함
- 1분당 55명꼴로 정보를 빼냄,

DB 접근제어 및 암호화의 한계

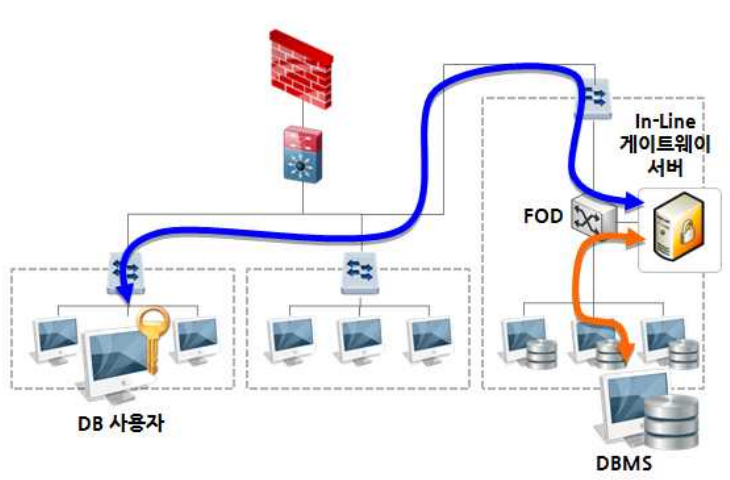
개인정보 유출 사고를 통해 기존 솔루션의 한계를 알 수 있습니다.

Proxy 방식 — Proxy 게이트웨이 방식



- 독립적인 IP를 가진 별도의 서버 설치
- Proxy Gateway 서버를 경유하도록 접속 경로 변경 필요
  (DB사용자 단말기에 클라이언트를 설치하거나, 단말기의 접속 정보를 변경(예: tnsname.ora 파일을 변경 하거나 ODBC 설정을 변경)
- 어플리케이션 서버는 Proxy Gateway 서버를 경유하지 않도록 설정

In-Line 방식 — In-Line 게이트웨이 방식



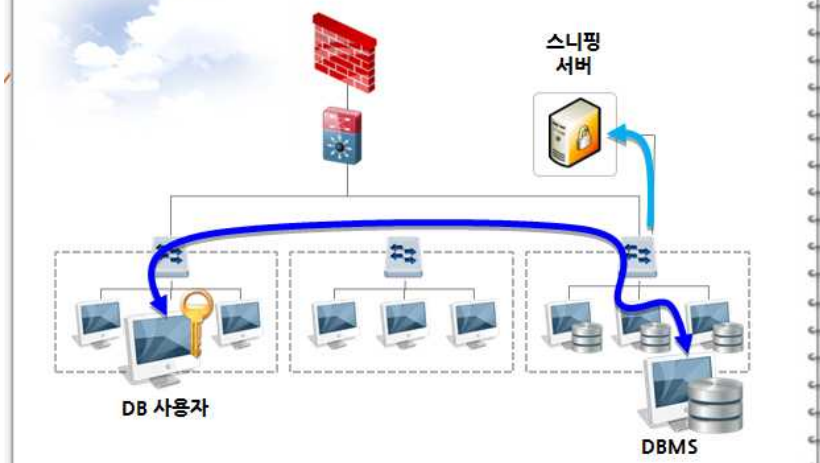
- DB서버 앞단에 FOD(Fail Over Device)를 설치해야 하므로 시스템 중단 필요
- FOD에 의해 자동으로 패킷 흐름이 In-Line 게이트웨이 서버를 경유하도록 변경되므로 DB사용자 단말에 변경 불필요
- 어플리케이션 서버의 패킷도 모두 In-Line 게이트웨이 서버를 경유하게 되어 속도 저하 및 장애 영향 발생

* DB에 직접 접속하지 않아 통제 대상에서 제외됨

DB 접근제어 및 암호화의 한계

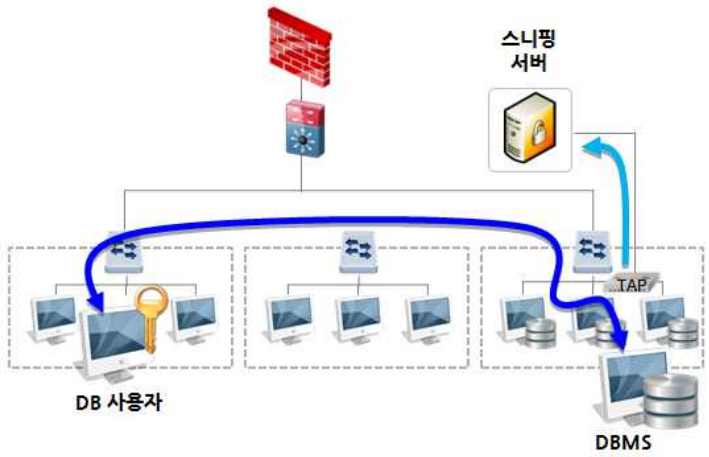
개인정보 유출 사고를 통해 기존 솔루션의 한계를 알 수 있습니다.

미러링 방식 스위치 미러링 방식 스니핑



- 네트워크 스위치의 미러링(Mirroring) 기능을 이용하여 패킷(packet)을 복사함. 스위치의 우선 순위에 따라 미러링 되지 않아 패킷 유실 가능
- 스위치에 따라 미러링 포트가 매우 제한 되어, 미러링 포트 여분이 없을 수 있음
- 스위치에 다수의 DBMS가 연결되어 있더라도 별도의 장치가 필요하지 않으므로 설치 용이

TAP 방식 TAP 방식 스니핑

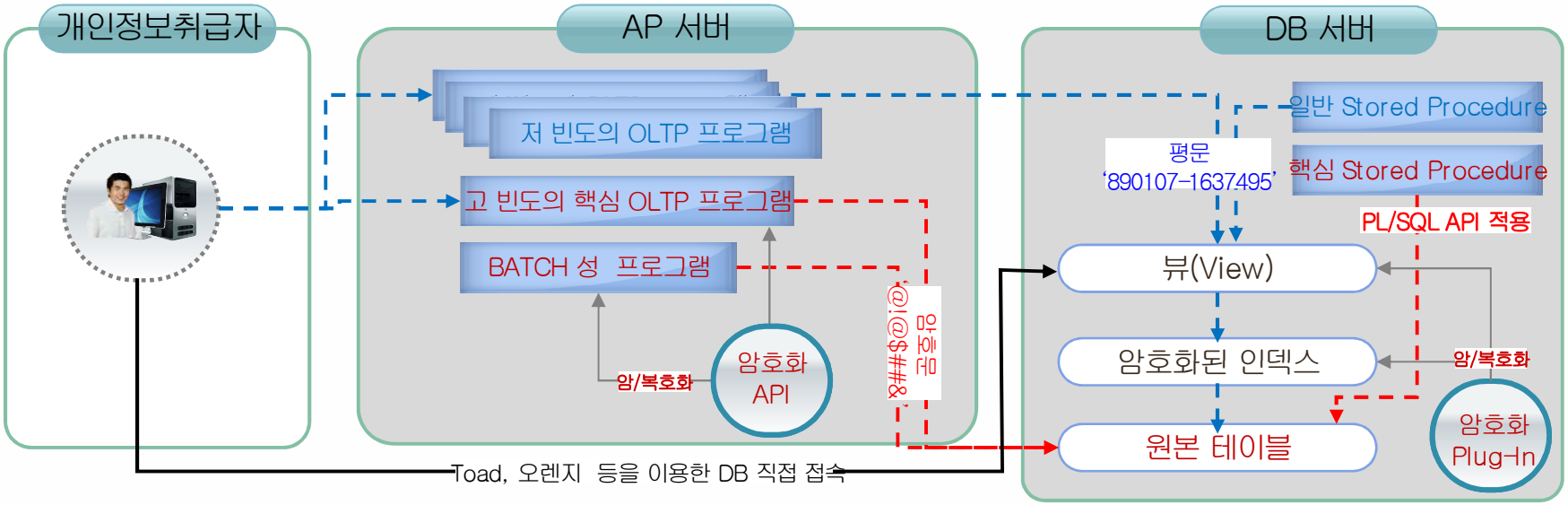


- DB서버 앞 부분 또는 스위치 앞 부분에 TAP 장치를 설치하여 패킷 복사 (DB 마다 TAP을 설치할 경우 TAP이 매우 많아져, 스니핑 서버의 수도 늘어남)
- 패킷(packet)에 대한 유실없이 스니핑 서버로 모두 전달 가능하므로 우수한 보안성

* 개개의 SQL은 1건씩 밖에 조회하지 않아 특이점을 발견할 수 없음

DB 접근제어 및 암호화의 한계

개인정보 유출 사고를 통해 기존 솔루션의 한계를 알 수 있습니다.



- 암/복호화 권한이 있는 WAS 서버를 통해 데이터를 조회하였으므로, 통제할 수 있는 방법이 없음

개인정보 오남용, 감독하고 계십니까?

개인정보를 취급하는 조직의 책임자 또는 관리자이십니까? 그렇다면 **조직의 개인정보 오남용을 감독할 법적인 책임이 있습니다.**

개인정보보호법

'개인정보 유출 및 오용・남용 방지를 위한 내부통제시스템의 구축'
'의 책임이 있습니다.
(법 제 31조)

1. 개인정보 보호 계획의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보 유출 및 오용・남용 방지를 위한 내부통제시스템의 구축
5. 개인정보 보호 교육 계획의 수립 및 시행
6. 개인정보파일의 보호 및 관리・감독

자가 테스트 [Optional Page]

아래의 2가지 질문에 답하여 개인정보 오남용 감독업무를 잘 수행하고 있는지 평가해 보시기 바랍니다.

질문1

"사내의 모든 웹어플리케이션을 대상으로,
지난 1달동안 동료 직원보다 비업무 시간에 고객 주민등록번호 조회 건수가 3배 이상 증가한 직원을 찾아낼 수 있다"

NO

READ

끝까지 주의깊게
이 문서를 검토해 주십시오.

YES

질문2

"이와 유사한 오남용 사례들을
매일 자동으로 찾는다"

NO

YES

EXIT

이 문서를 읽는 것은
시간낭비가 될 수 있습니다.

법적 요구사항들

개인정보보호법은 **개인정보 접속기록의 보존 의무**와 **오남용 검토 및 보고 의무**를 명시하고 있습니다.

개인정보 접근기록의 보존 의무

"① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 6개월 이상 보관·관리하여야 한다." (개인정보의 안전성 확보조치 기준 고시 8조)

(개인정보의 안전성 확보조치 기준 고시 2조(정의))
13. "접속기록"이라 함은 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일기, 접속지를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다.

[개인정보 위험도 분석]

14. 상시적으로 DB 관리자 및 개인정보취급자의 접속기록을 남기고 있습니까?

취 지

- DB 접속 및 개인정보 처리내역 등을 자동으로 기록하는 로그 파일을 생성함으로써 불법적인 접근 및 행위를 확인 가능하고 유출사고 발생시 책임추적성을 확보합니다.

해 설

- 내부관리자가 DB관리툴, Telnet등을 이용해 DB에 직접 접속하는 경우와 개인정보취급자가 Web 또는 응용프로그램을 통해 접속하는 경우 모두 접속기록을 남겨야 합니다.

법적 요구사항들

개인정보보호법은 **개인정보 접속기록의 보존 의무**와 **오남용 검토 및 보고 의무**를 명시하고 있습니다.

개인정보 오남용 여부의 검토 및 보고 의무

개인정보처리시스템에 접속하여 개인정보를 처리한 업무내역에 대하여 정기적으로 확인.감독 할 책임이 있습니다.(개인정보의 안전성 확보조치 기준 고시 8조)

> 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우, 수행한 업무 내역에 대하여 식별자, 접속일시, 접속지를 알 수 있는 정보, 수행업무 등의 접속기록을 최소 6개월 이상 저장하고 정기적으로 확인.감독하여야 한다

[개인정보 위험도 분석]

15. DB 접속기록을 주기적으로 모니터링하여 통제하고 있습니까?

취 지

- DB접속기록에 대한 모니터링 과정 없이 단순히 DB접속기록을 남기는 것만으로는 DB접속자의 행위에 대한 효과적인 통제가 이루어진다고 할 수 없습니다. 접속기록의 주기적인 모니터링을 실시하면 DB접속에 대한 이상 징후를 파악하여 조치가 가능하고, DB에 접속하는 모든 사람에게 모니터링이 이루어지고 있음을 인지시킴으로써 불법적인 시도 자체를 줄일 수 있습니다.

해 설

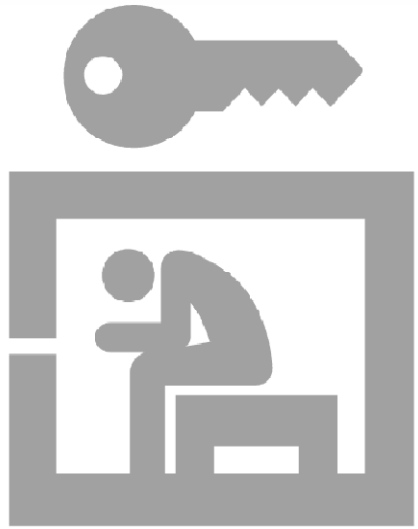
- 매주 DB 접속에 대한 이상 징후가 있는지 DB접속기록에 대해 최소 주 1회 이상 모니터링을 수행합니다.

지속적 사고사례들

하지만, 내부직원의 개인정보 **오남용을 감독하지 못하여 민형사상 처벌을 받게 되는 사고**사례는 매년 지속적으로 발생되고 있습니다.

회사	G정유사(2008)	H캐피털(2011)	S통신사 (2011)	S카드 (2012)
원인	내부자 유출	웹어플리케이션 관리부실	미동의 개인정보 사용	내부자 유출
규모	1,000만명	175만 명	1만8993명	47만 명
처벌	소송 중	대표이사의 사과 기자회견. 및 금감원의 징계	37억 5770만원 배상 판결 (지체 보상금 제외)	대표이사의 사과 기자회견.및 금감원의 징계

"개인정보보 안전성확보에 필요한 보호조치 미이행시, 2년 이하 징역 또는 3천만원 이하 과태료"



보안 담당자의 고민

DB를 암호화하고 접근제어 시스템도 설치 운영하고 있으나, 보안담당자들은 개인정보 오남용 감독은 여전히 어려운 일이라고 말합니다.

암호화

"DB를 암호화 해도 업무적으로 개인정보를 처리해야 하는 내외부 직원에게는 접근을 허용할 수밖에 없습니다"

A캐피탈

"웹어플리케이션 접속 개인정보 처리로그는 너무 방대하고 종류도 많아서 저장하고 검토할 엄두도 내지 못하고 있습니다."

B전자

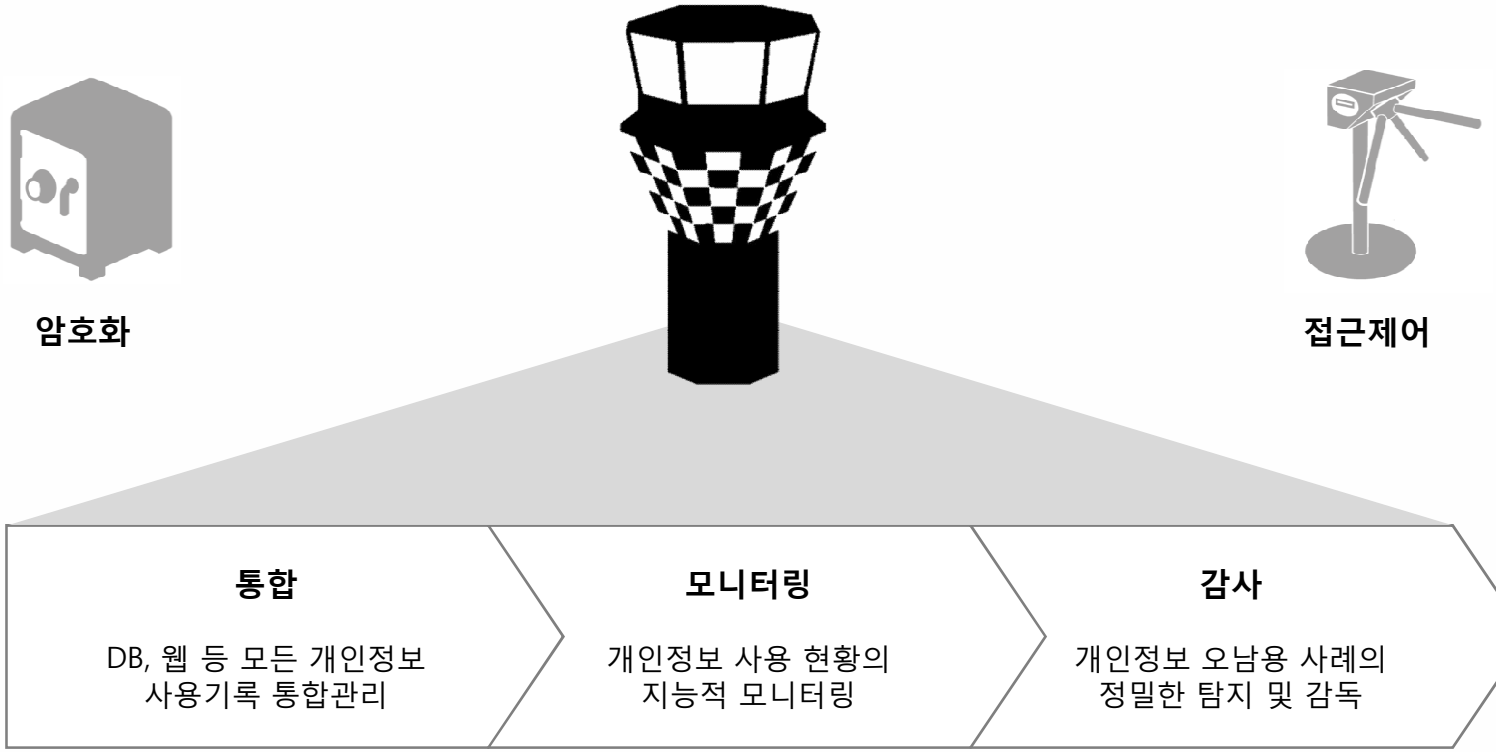
접근제어

"접근로그는 많은데, 여기에서 실제적인 오용 사례를 찾아내기 위해서는 상당한 시간과 노력이 필요합니다"

C공단

컨트롤 타워가 필요합니다

개인정보 오남용을 효과적으로 감독하기 위해서는 **개인정보 사용기록을 통합하여 모니터링 하고 지능적으로 오남용을 탐지하기 위한 컨트롤 타워**가 필요합니다.



목차

개인정보 범위 및 특성

개인정보는 고유식별정보 외에도 많은 종류의 개인정보가 있습니다.

"개인정보" 란 일반적으로 개인(자연인)에 관한 식별, 판단, 평가 등 개인의 사적 영역과 관련된 일체의 정보를 의미

당해 정보 만으로는 특정 개인을 알아 볼 수 없는 경우라도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함 !
(IP, e-mail 주소, 쿠키정보 등)

생존하는 개인에 관한 정보

- 사망하였거나 사망으로 추정되는 자에 대한 정보는 보호 대상이 아님
- 사망자와 유족과의 간계를 나타내는 정보는 유족에 대한 식별이 가능함으로 인정
- 해당 개인에 관한 판단, 평가, 견해 포함

개인을 식별할 수 있는 정보

- 다른 정보와 결합하여 개인을 식별할 수 있는 정보도 개인정보임
  예) 주소 + 서명 ➔ ***에 사는 특정인
  성명 + 전자메일 ➔ ***가 사용하는 메일
  (전자메일 ID 는 고유하게 부여되는 것임)

신분 관계 : 성명, 주민번호, 주소 등

사회 경력 : 학력, 직업, 전과 등

경제 관계 : 소득, 재산, 신용, 거래 내역 등

심신의 상태 : 신체적 특징, 병력, 장애 등

내면의 비밀 : 사상, 종교, 정치 성향 등

기타 : 생체정보, 위치정보, 인맥정보 등

개인정보 범위 및 특성

개인정보는 정해진 형식이 있는 개인정보와 일정한 형식이 없는 개인정보로 분류할 수 있습니다.

형식이 있음

- 주민등록번호
- IP
- 여권번호
- 전화번호
- 외국인등록번호
- email
- 운전면허번호

**조회결과에 정규식을 적용하여,
처리 여부를 판정**

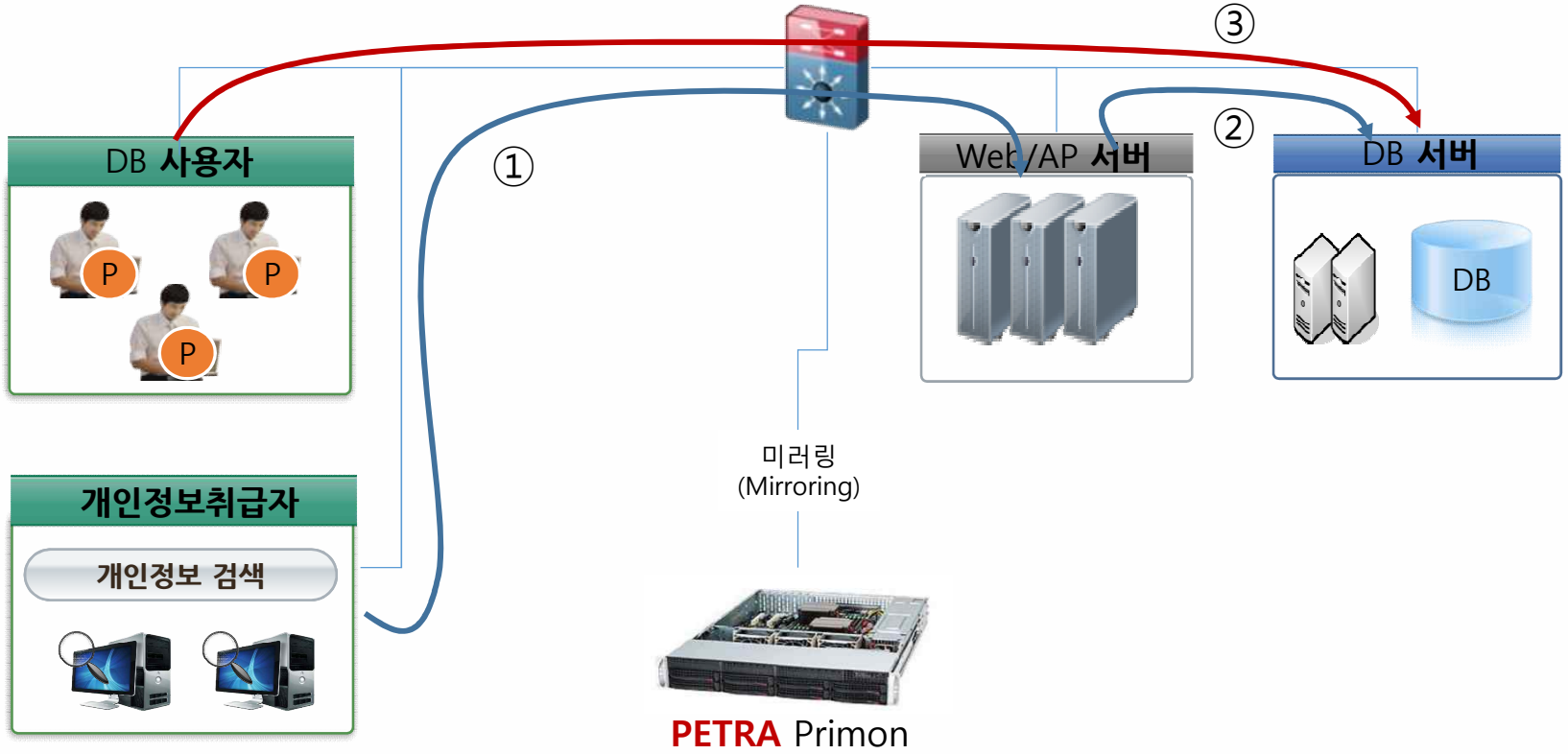
형식이 없음

- 사상정보
- 학력정보
- 병력정보
- 생체정보

**조회하는데 사용된 SQL을 분석하여
해당 정보가 저장된 테이블/컬럼을
사용하는지 여부 판정**

시스템 구성

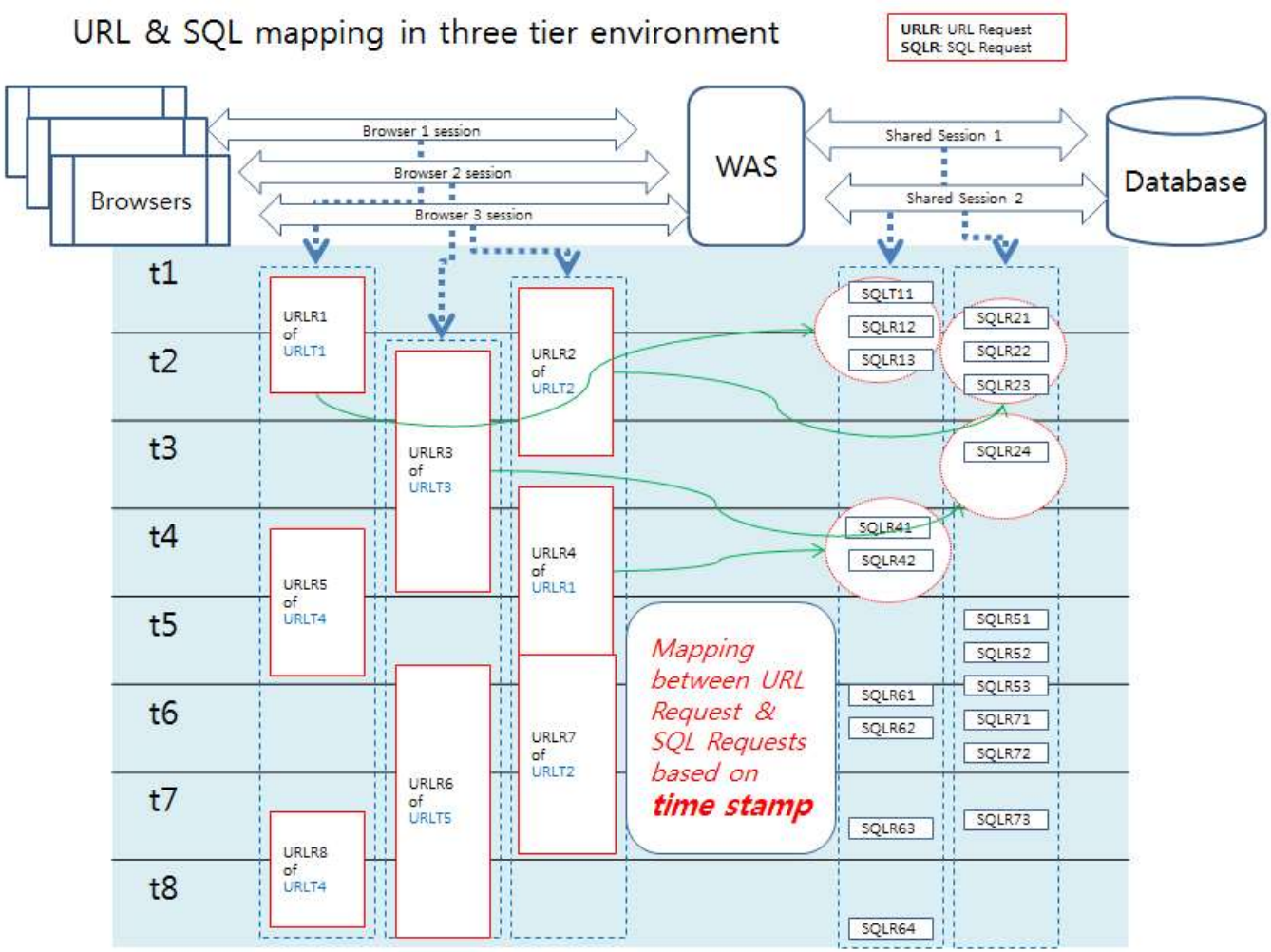
기존 시스템에 대한 영향이 없도록 **스니핑(Sniffing) 방식으로 패킷을 수집**하여 개인정보 사용여부를 분석합니다.



① 구간 : HTTP 프로토콜을 분석하여 웹을 통한 개인정보 취급 분석
(형식이 있는 개인정보 사용 분석)
②, ③ 구간 : DB 프로토콜을 분석하여 SQL 사용 분석
(형식이 없는 개인정보 분석)

웹 구간과 DB 구간 매핑

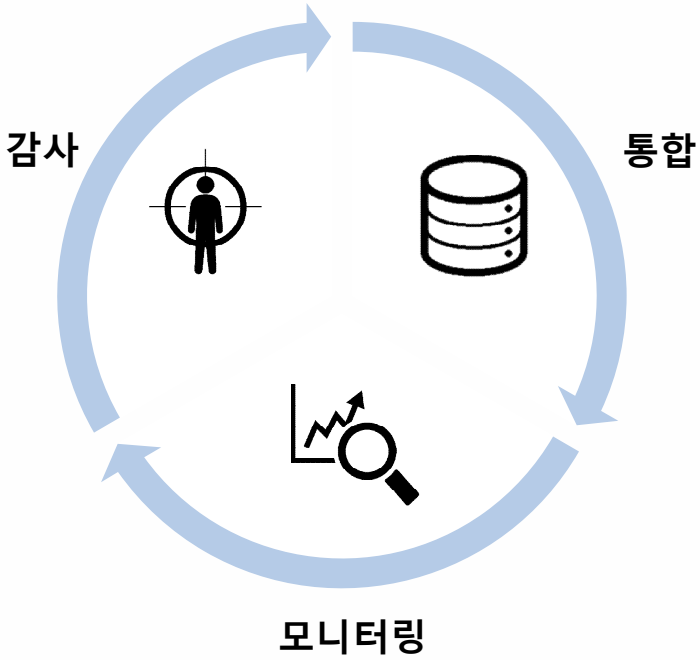
형식이 없는 개인정보에 대한 취급현황을 분석하기 위하여, 웹 구간과 DB 구간의 단절된 정보를 **시간 정보와 URL당 SQL 수행 이력 정보를 활용하여 정교하게 매핑**합니다.



ALL-IN-ONE 솔루션

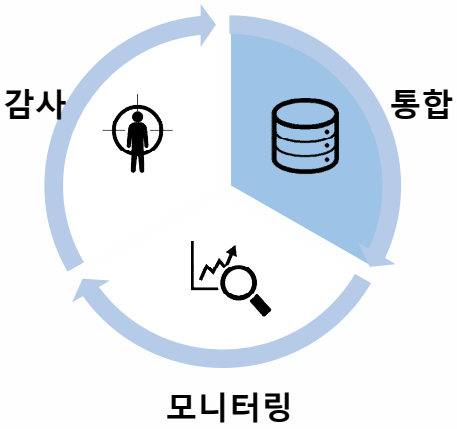
개인정보 오남용 감독에 관련된 요구사항을 만족하는 ALL-IN-ONE 솔루션

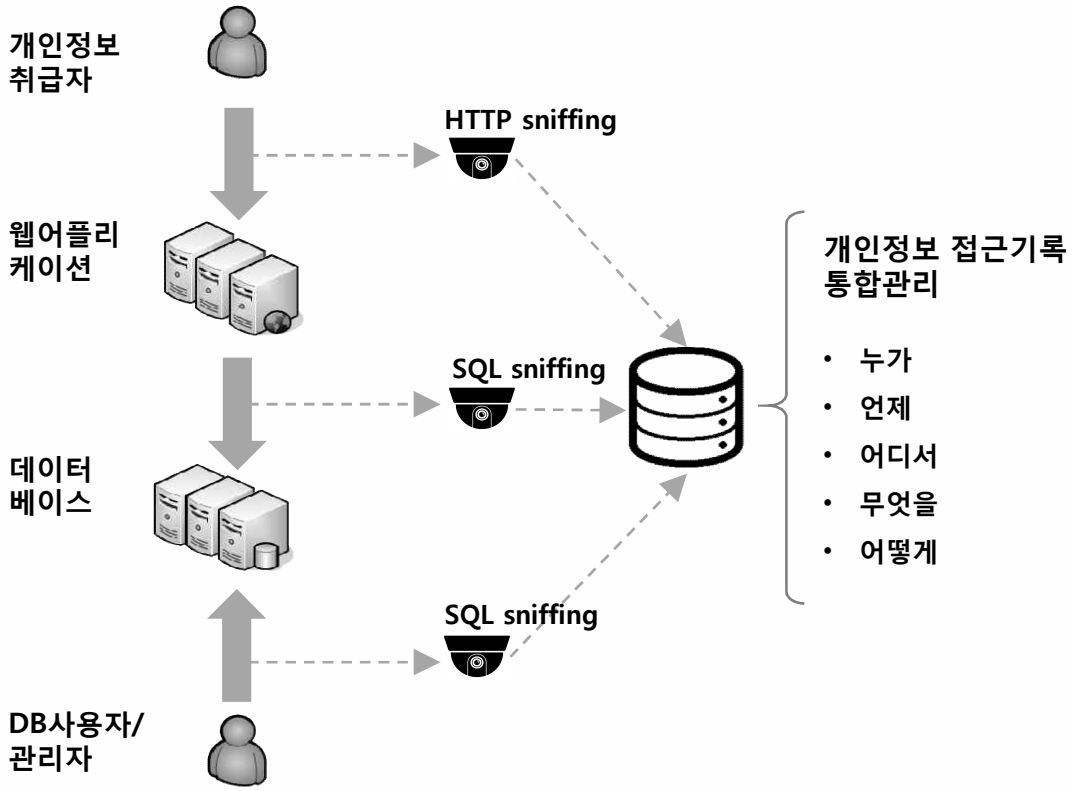
PETRA Primon



접근기록 통합

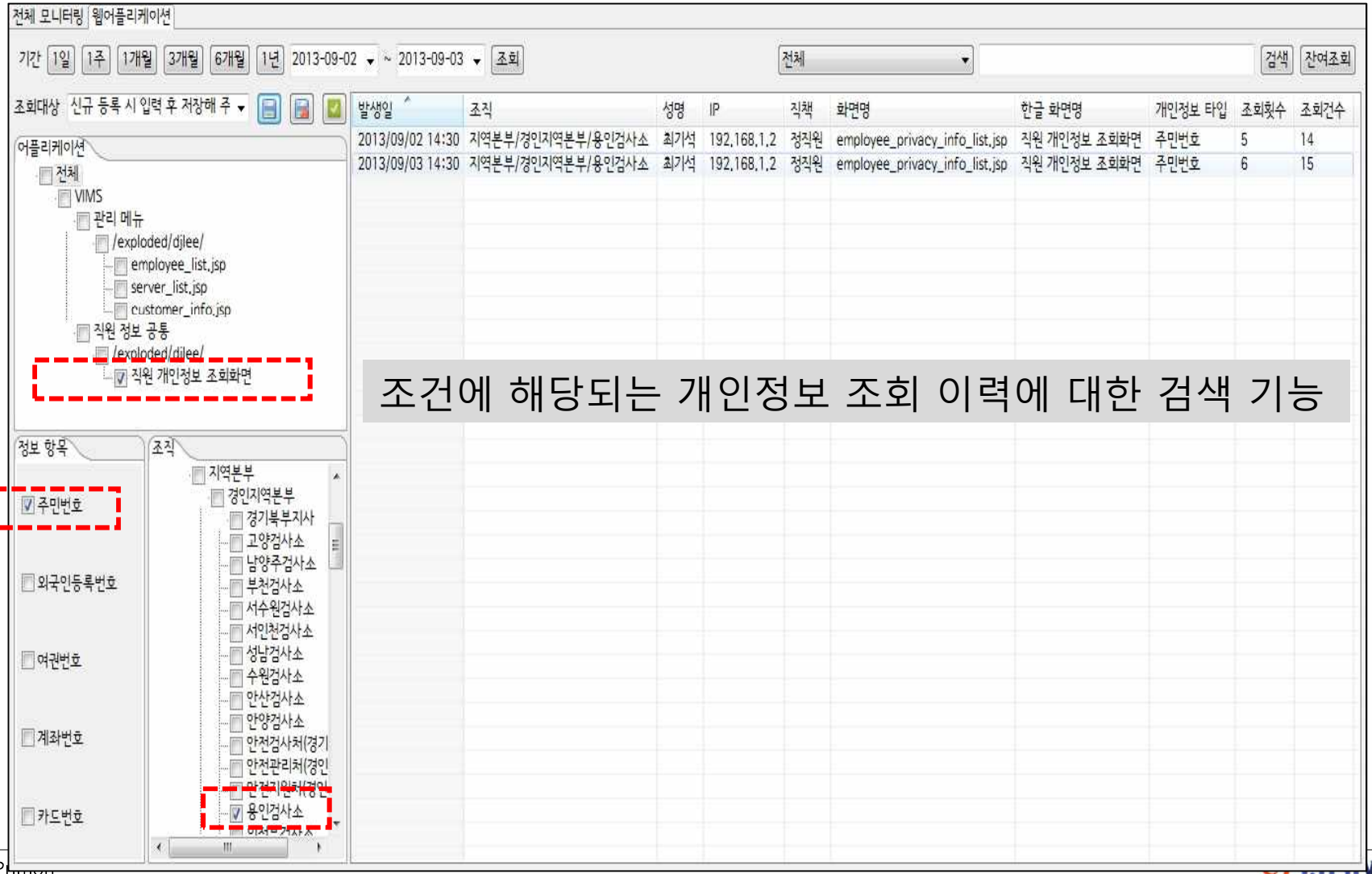
웹어플리케이션에서 데이터베이스에 이르는 **모든 사용자의 개인정보 접근기록을 수집하여 통합** 관리





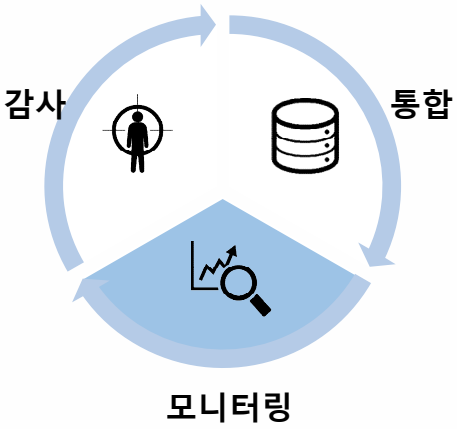
접근기록 통합

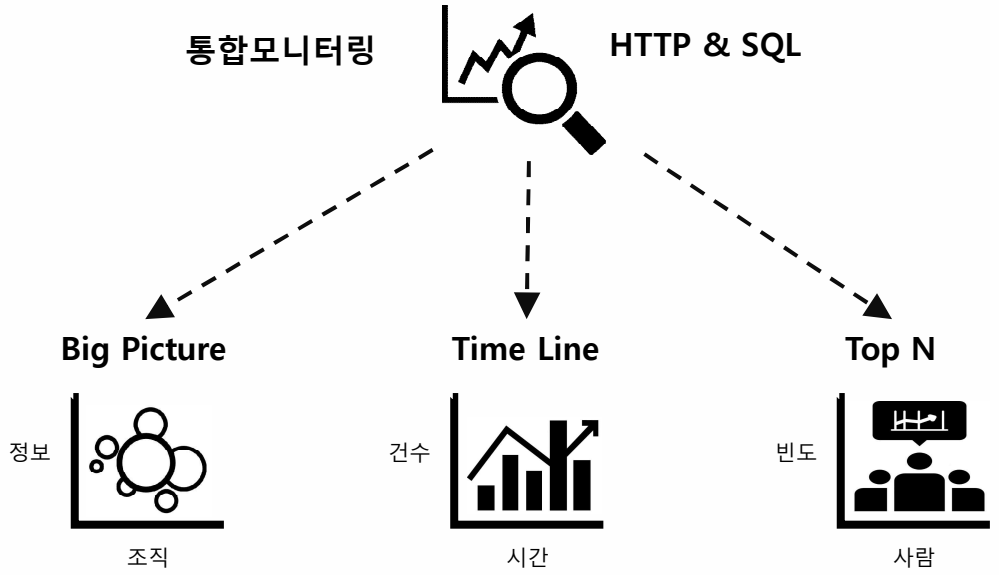
웹어플리케이션에서 데이터베이스에 이르는 **모든 사용자의 개인정보 접근기록을 수집하여 통합** 관리



사용현황 모니터링

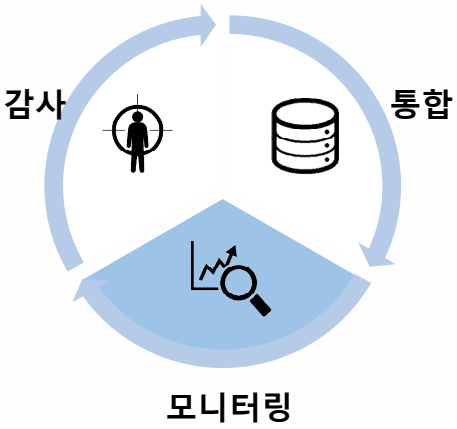
다양한 관점에서 웹어플리케이션과 데이터베이스에서 **개인정보에 접근/조회 하는 모든 행위를 통합적으로 모니터링**

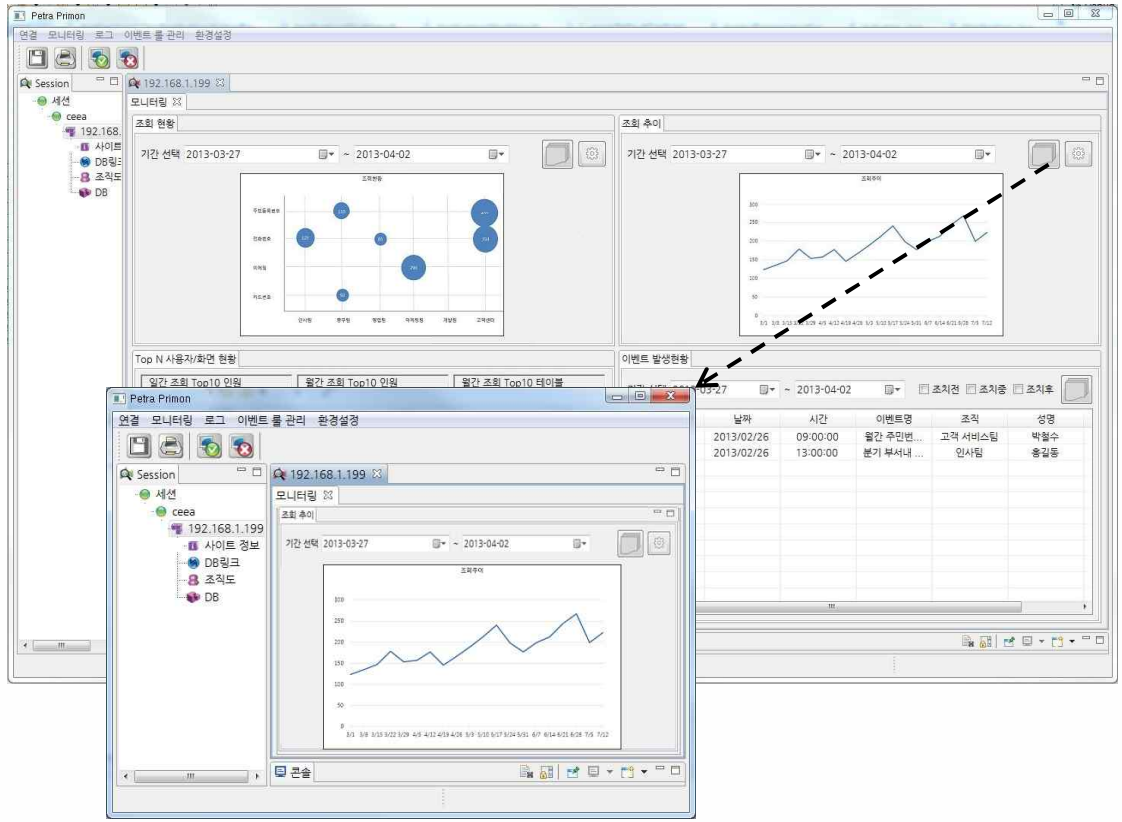




사용현황 모니터링

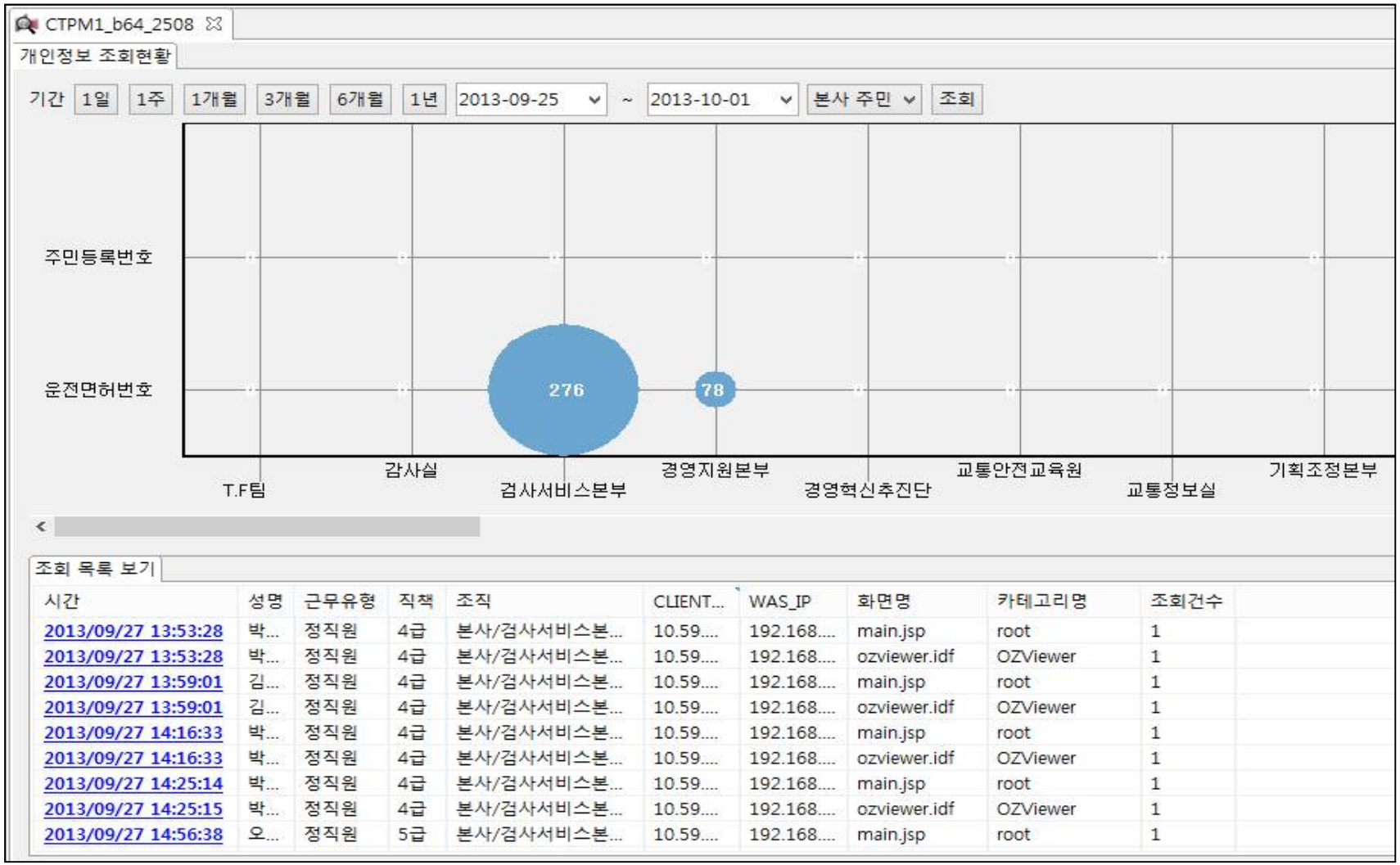
다양한 관점에서 웹어플리케이션과 데이터베이스에서 **개인정보에 접근/조회 하는 모든 행위를 통합적으로 모니터링**





사용현황 모니터링

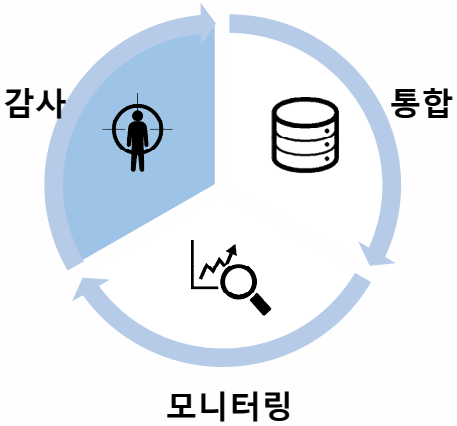
다양한 관점에서 웹어플리케이션과 데이터베이스에서 **개인정보에 접근/조회 하는 모든 행위를 통합적으로 모니터링**



시간	성명	근무유형	직책	조직	CLIENT...	WAS_IP	화면명	카테고리명	조회건수
2013/09/27 13:53:28	박...	정직원	4급	본사/검사서비스본...	10.59....	192.168....	main.jsp	root	1
2013/09/27 13:53:28	박...	정직원	4급	본사/검사서비스본...	10.59....	192.168....	ozviewer.idf	OZViewer	1
2013/09/27 13:59:01	김...	정직원	4급	본사/검사서비스본...	10.59....	192.168....	main.jsp	root	1
2013/09/27 13:59:01	김...	정직원	4급	본사/검사서비스본...	10.59....	192.168....	ozviewer.idf	OZViewer	1
2013/09/27 14:16:33	박...	정직원	4급	본사/검사서비스본...	10.59....	192.168....	main.jsp	root	1
2013/09/27 14:16:33	박...	정직원	4급	본사/검사서비스본...	10.59....	192.168....	ozviewer.idf	OZViewer	1
2013/09/27 14:25:14	박...	정직원	4급	본사/검사서비스본...	10.59....	192.168....	main.jsp	root	1
2013/09/27 14:25:15	박...	정직원	4급	본사/검사서비스본...	10.59....	192.168....	ozviewer.idf	OZViewer	1
2013/09/27 14:56:38	오...	정직원	5급	본사/검사서비스본...	10.59....	192.168....	main.jsp	root	1

오남용 자동감사

내부직원의 개인정보 오남용을 탐지하기 **위한 정밀한 오남용 탐지룰 제공 및 자동화 감사 기능**을 통해 효과적인 감사/소명관리 환경을 제공



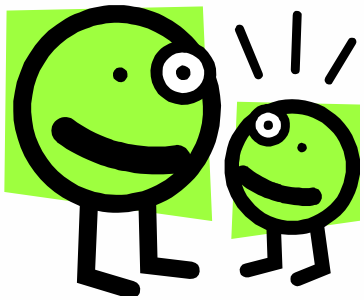
정밀한 오남용 탐지룰
개인정보 접근 횟수, 조회수, 빈도, 시간, 추이 등을 종합적으로 반영한 오남용 추론/탐지 룰 탑재

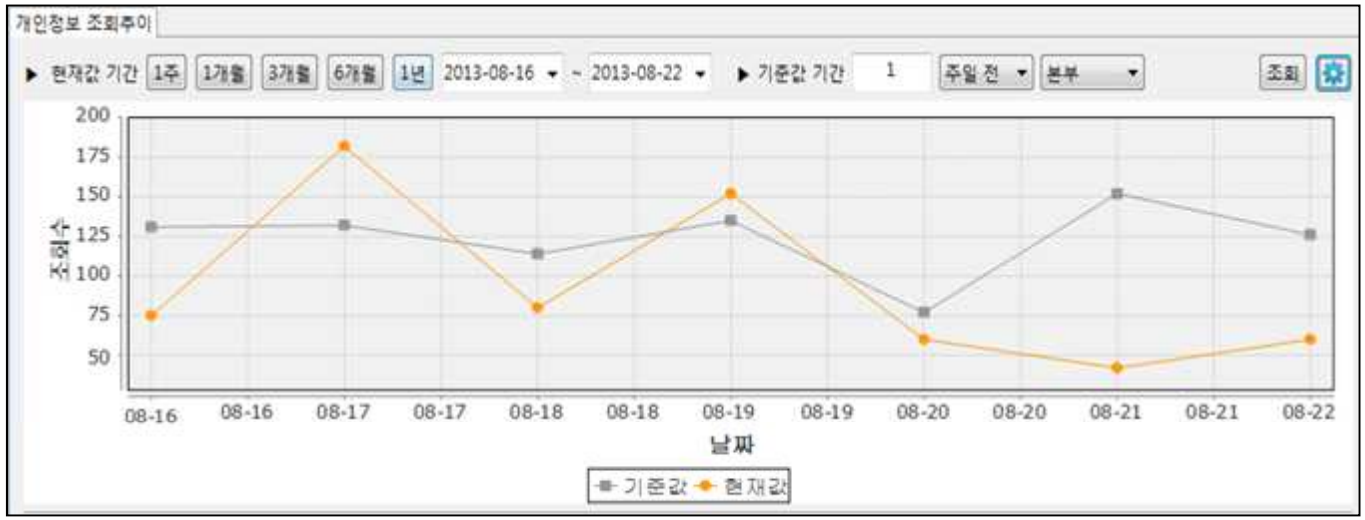
자동화 감사
개인정보 오남용 탐지엔진을 정기적으로 실행하여 오남용 의심사례 발견 시 자동적으로 감사 리스트 작성

소명 관리
개인정보 오남용 감사 케이스에 대한 소명업무를 기록하고 보고하기 위한 관리환경 제공

오남용 자동감사 – 정밀한 오남용 탐지률

유연한 탐지 규칙 설정을 통해 개인정보 오남용에 대한 정밀한 탐지를 수행합니다.





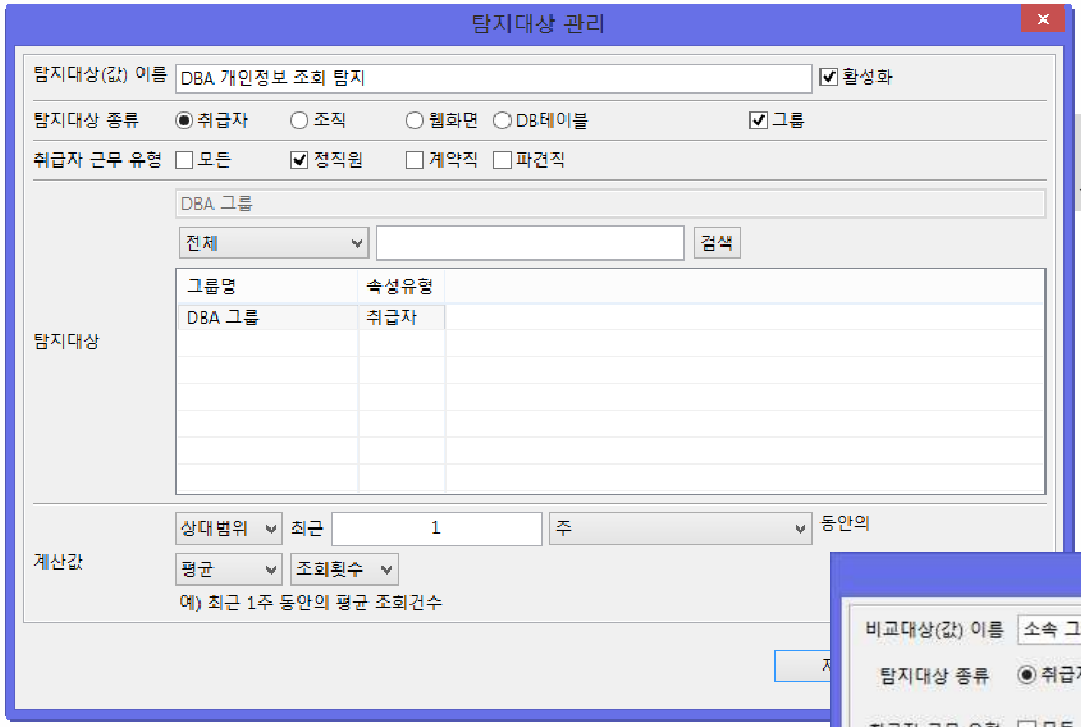
개인정보 오남용 : f1(탐지대상) > f1(비교대상) + 범위값

오남용 탐지는 탐지대상의 지표값이 비교대상의 지표값보다 범위값 이상 차이 나는 경우를 식별함.

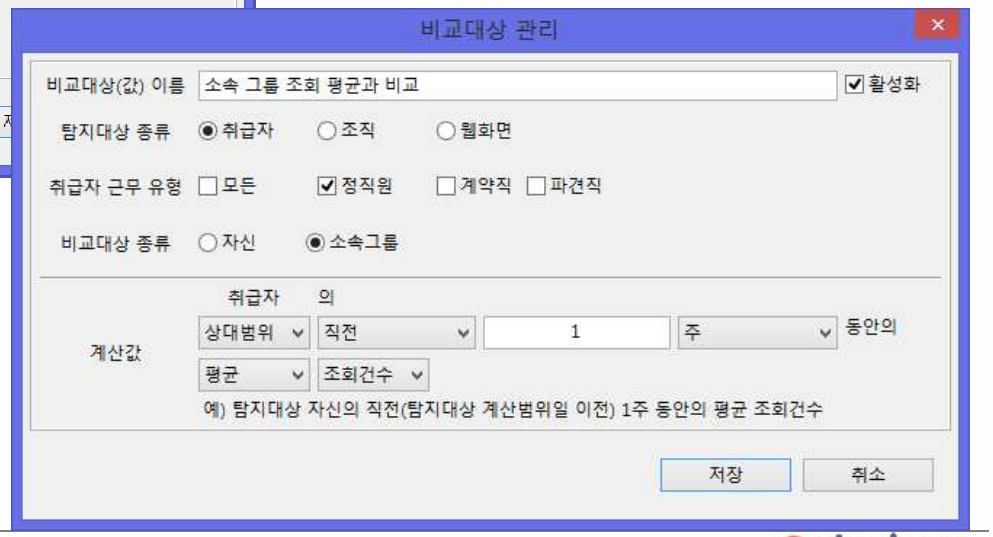
비교대상 예)
- 탐지대상의 3개월 평균값
- 탐지대상 소속 조직의 최근 1개월 평균값

오남용 자동감사 – 정밀한 오남용 탐지률

미리 정의된 개인정보 패턴 이외에 고객사에서 필요한 패턴을 등록하여 개인정보 취급을 인식할 수 있도록 합니다.



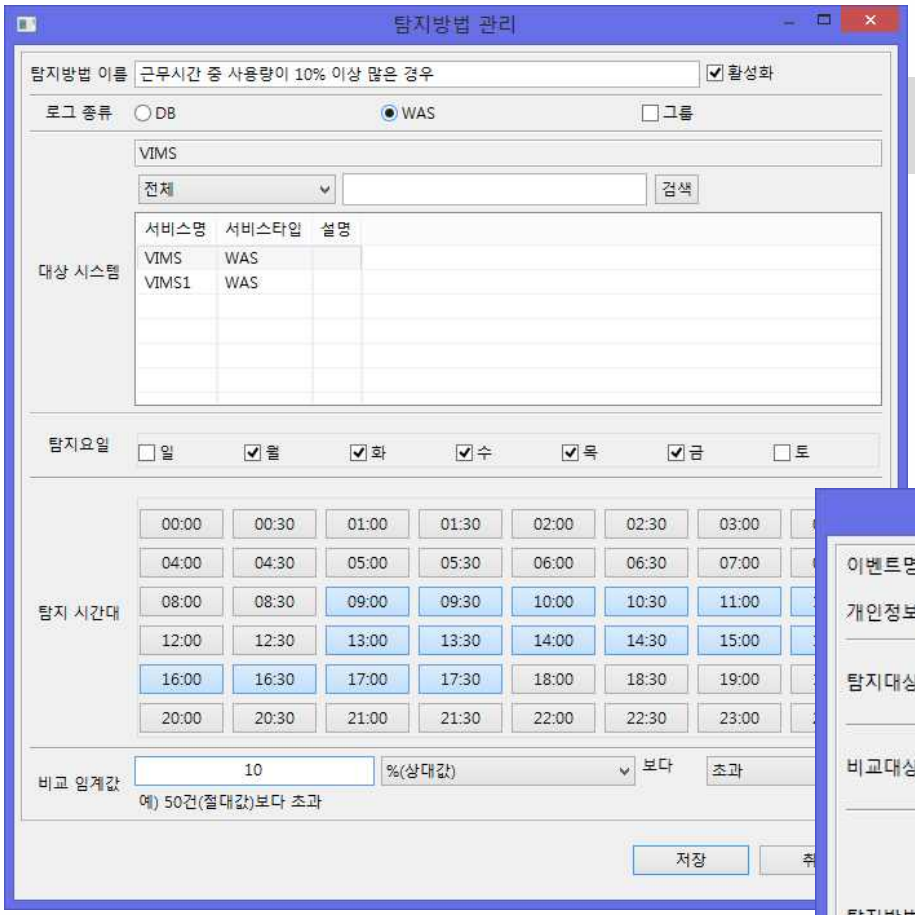
탐지대상 : 개인정보 오남용을 하고 있는 사람에 대한 탐지 범위



비교대상 : 개인정보 오남용을 하고 있는 사람에 대한 탐지할 때, 비교할 수 있는 기준값을 구하기 위한 대상

오남용 자동감사 – 정밀한 오남용 탐지률

미리 정의된 개인정보 패턴 이외에 고객사에서 필요한 패턴을 등록하여 개인정보 취급을 인식할 수 있도록 합니다.

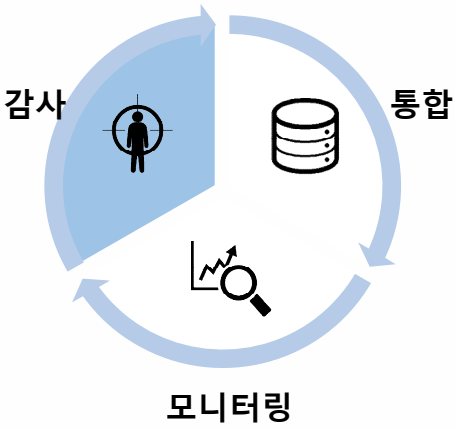


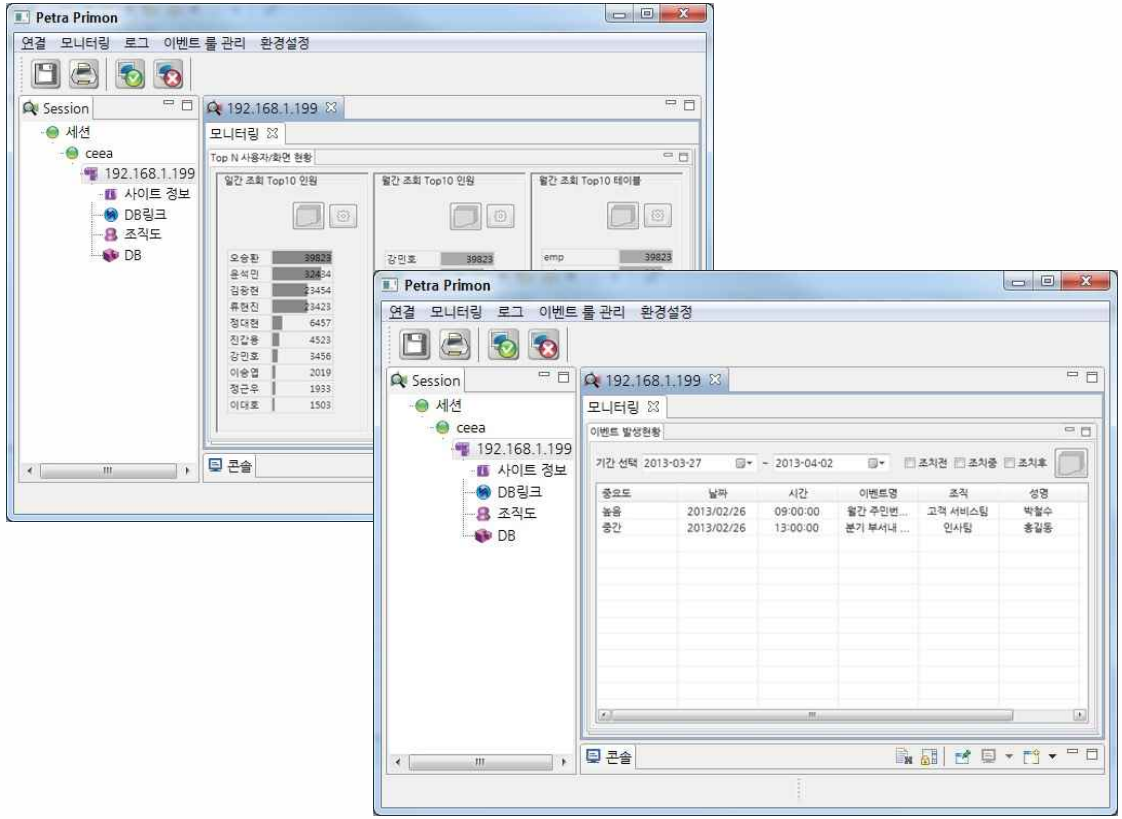
탐지대상과 비교대상을 비교하는 조건 설정

이벤트 규칙 = 탐지대상 + 비교대상 + 탐지 방법

오남용 자동감사

내부직원의 개인정보 오남용을 탐지하기 **위한 정밀한 오남용 탐지를 제공 및 자동화 감사 기능**을 통해 효과적인 감사/소명관리 환경을 제공





거의 모든 업무환경 지원

대부분의 상용 DBMS환경 및 표준 HTTP 프로토콜 기반의 모든 웹 서버와 브라우저 환경을 지원

SQL

ORACLE
MySQL
SYBASE
Informix SOFTWARE
Microsoft SQL Server
TIBERO
IBM DB2
TERADATA
ALTIBASE PERFORMANCE SOLUTIONS
PostgreSQL
CUBRID

HTTP

bea

JEUS Web Application Server

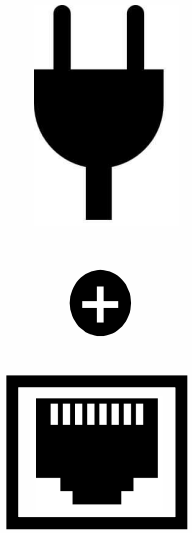
ORACLE

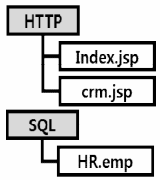
WebSphere

Plug & Play

감사 대상 네트워크의 웹어플리케이션과 DB를 자동으로 프로파일링하며, 사전 정의 감사룰이 설정되어 있어 **설치 즉시 운영이 가능**

To-do list





자동 프로파일링

모니터링 대상 네트워크의 HTTP 웹어플리케이션 및 데이터베이스를 자동으로 감지하여 프로파일링합니다.

사전정의 감사 룰

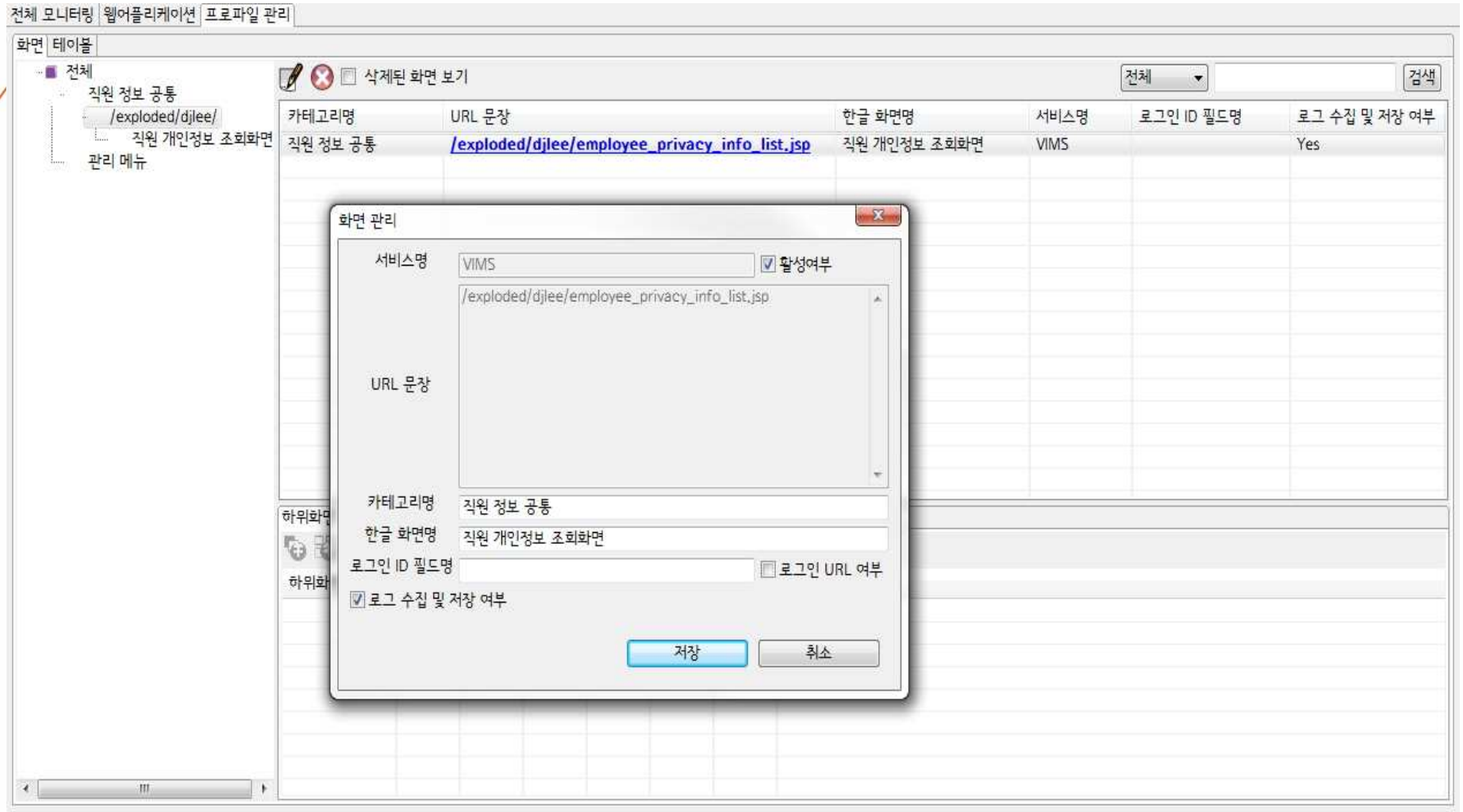
개인정보 오남용을 신속하게 탐지하기 위한 오남용 탐지 룰이 사전 정의되어 있습니다.

강력한 커스터마이징

조직의 상황에 적합하게 무한히 커스터마이징 가능한 감사,모니터링 룰셋 환경설정이 가능합니다.

Plug & Play – 자동 프로파일링

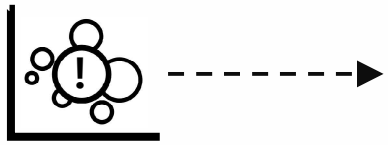
감사 대상 네트워크의 웹어플리케이션과 DB를 자동으로 프로파일링하며, 사전 정의 감사룰이 설정되어 있어 **설치 즉시 운영이 가능**



감사 시나리오

자동화된 모니터링 및 감사기능은 아래의 시나리오와 같이 보안담당자의 시간과 노력 절감

Am 9:00



이상 징후

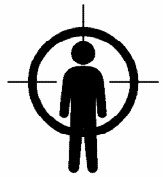
출근하여 전체현황 모니터링 화면을 보니 A부서 버블이 유난히 큰 것을 발견합니다.

Am 9:05

추이 확인

A부서의 시계열 모니터링을 보니 지난 3일 사이에 조회건수가 증가한 것이 보입니다.

Am 9:10



자동화 감사

자동감사창에 '1주일 사이에 부서 평균의 3배이상을 비업무시간에 조회'해 의심사례로 K직원이 올라와 있습니다.

Am 9:20

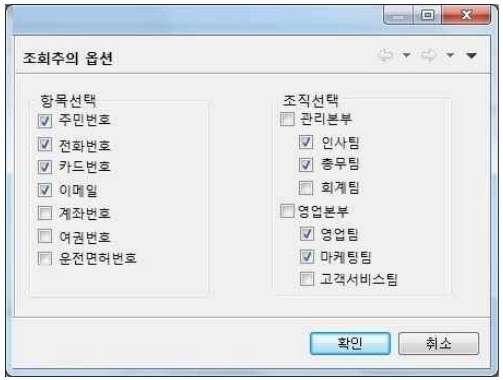
소명 & 레포팅

보안담당자는 해당 직원에게 소명메일을 보내고 해당 이벤트를 오전중에 팀장에게 레포팅 합니다.

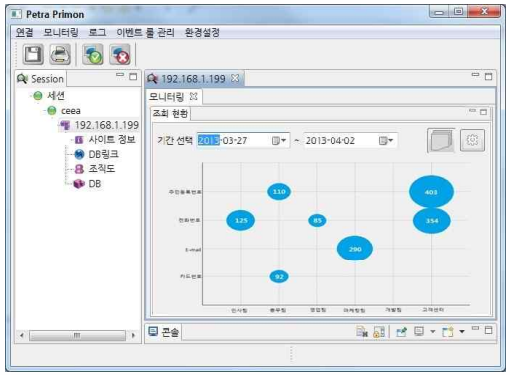
User Interface

직관적이고 편리한 소프트웨어 사용자 인터페이스를 제공

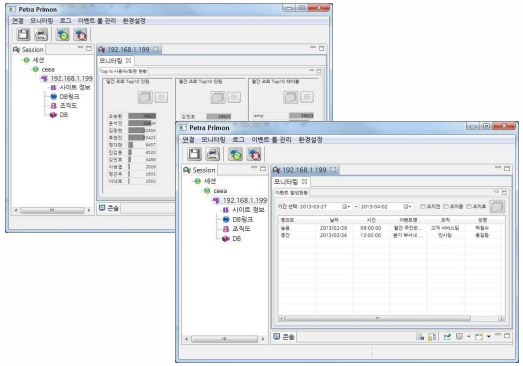
환경설정



모니터링



감사



레포팅

The Benefits

개인정보관련 제반 법규 준수와 함께 시간과 자원을 절약하는 효과적인 보안관리 환경

준법

개인정보보호법 '개인정보의 안전성 확보 조치기준' 및 정보통신망법 '개인정보의 관리적 기술적 보호조치 기준'상의 개인정보 오남용 감독 요구를 만족시킵니다.

효율

개인정보의 오남용 감시와 모니터링을 위한 시간과 자원을 대폭 절감시켜 효율적인 업무처리를 가능하게 합니다

여유

보안담당자/책임자 로써 조직의 중요한 보안 위협을 탐지하고 예방는 업무에 집중하여 업무의 여유를 누리세요

목차

Sinsiway

차별화된 기술력으로 시장을 선도합니다.

회사 연혁

- CEO : 이희상
- 설립일 : 2005. 01. 25.
- 직원수 : 43 명

통합된 DB보안 구축 능력

DB암호화 및 DB 접근제어 제공

"접근제어와 암호화 CC인증 기업은 '신시웨이'가 국내 유일"

이희상 (주)신시웨이 대표이사 사장

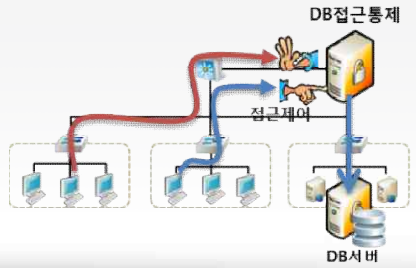
(주)신시웨이는 기술력으로 승부하는 DB보안 전문 기업으로 평가된다. 신시웨이는 '접근제어'와 '암호화' 두 개 부문에서 CC인증을 받은 국내 유일한 기업이다. 쉽지 않은 CC인증 두 개 부문에서 받았다는 것은 그만큼 기술력이 높음을 입증해 준 셈이다. 때문인지 신시웨이는 2005년 설립 이후 4년여 동안 줄곧 성장만을 거듭했다. 후발주자였지만 기술력에서 만큼은 신시웨이를 따라잡을 경쟁사들이 드물었기 때문이다. 그러나 시장에서의 치열한 경쟁은 신시웨이를 곤혹스럽게 해 지난 2009년부터는 성장세가 다소 주춤해졌다. 기술력만 믿고 마케팅과 영업에 다소 소홀했기 때문이다. 신시웨이는 이를 보완하고, 글로벌 시장을 향한 더 큰 기업으로 성장 발전하기 위해 이희상 한국오라클 전무를 공동대표 사장으로 지난해 11월 영입했다. 이 사장은 추진력과 리더십이 뛰어날 뿐만 아니라 기획력을 바탕으로 한 영업을 잘 하는 인물. 그이말로 철학을 가진 비즈니스맨으로 평가되기도 한다. 때문인지 이 사장을 만난 고객들은 '갑'과 '을'이 아닌 동반자라는 느낌이 더 든다고 자처한다. 이 사장이 영업 바이블이자 마당발로 평가되는 이유가 바로 여기에 있겠다.

사실 이희상 대표이사는 한국오라클에서도 잘 나가는 인물 가운데 한 사람으로 지목됐었다. 그런 그가 유망도 작고 설립 기준에 맞에 안 된 신시웨이를 선택했다. 이 사장은 "DB와 희망이 있기 때문이다"라고 한 마디로 잘라 말했지만, 그만큼 "글로벌 기업으로 성장할 가능성이 높고, 또한 반드시 그렇게 만들고 싶은 이유 때문이었다"고 귀띔했다. 신시웨이는 설립자이자 연구원들을 진두지휘하는 장재호 연구소장을 비롯해 공동대표인 최연준 사장, 그리고 컨설팅본부를 맡고 있는 김광열 상무 등이 글로벌 기업에서도 특출을 낼만큼 뛰어난 기술력을 가진 인물들로 화합이 잘 되는 기업으로 평가되기도 한다. 그런 조직에 이 사장의 역량을 접가한다면 글로벌 기업으로의 성장은 시간문제라는 게 주변 관계자들의 공통된 지적이다. 이희상 신임 대표를 만나본다.

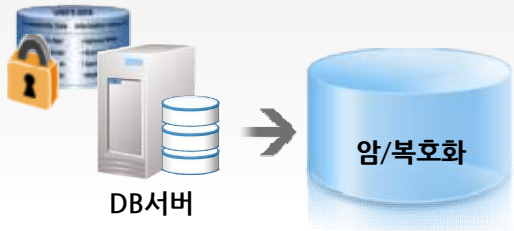
Sinsiway

개인정보보호 솔루션 개발과 보안인증 컨설팅을 수행합니다.

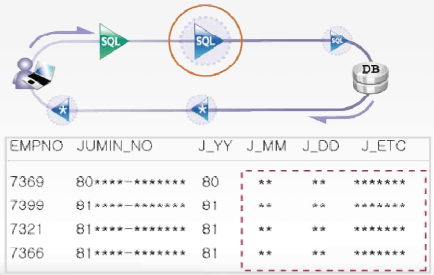
DB접근제어 솔루션



DB암호화 솔루션

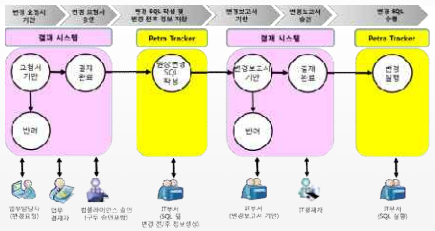


SQL Masking 솔루션

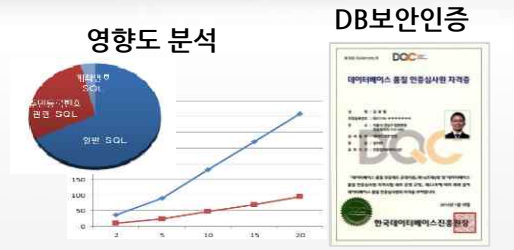


"개인정보보호"

원장변경관리 솔루션



개인정보보호 컨설팅



개인정보 감사 및 모니터링

개인정보보호법 '개인정보의 안전성 확보 조치기준' 및 정보통신망법 '개인정보의 관리적 기술적 보호조치 기준'을 만족하는 개인정보 감사 모니터링 솔루션

PETRA Primon

감사합니다