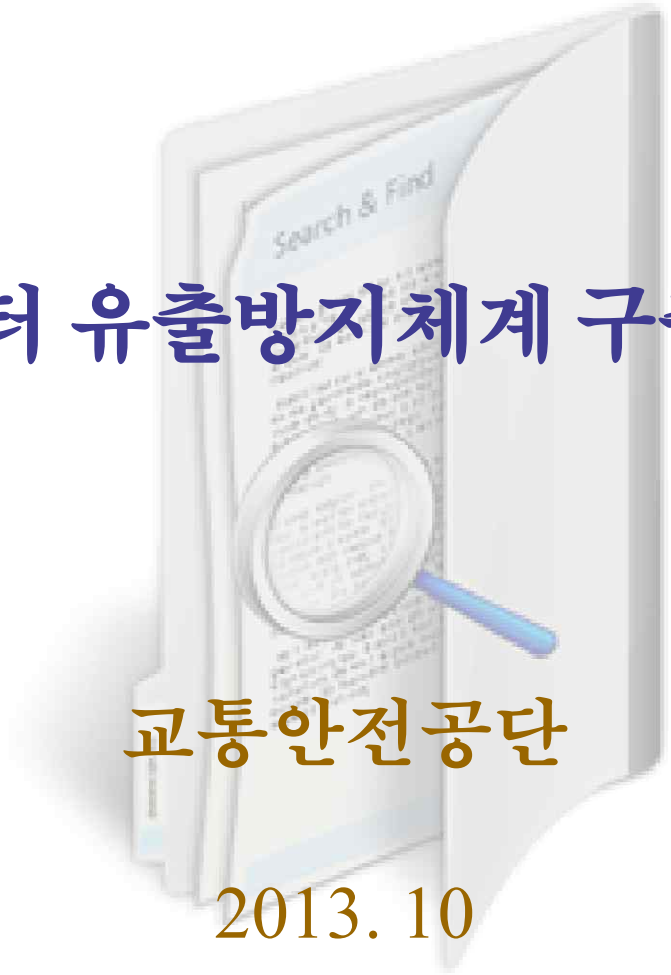
TS
교통안전공단



데이터 유출방지체계 구축 사례

교통안전공단

2013. 10

목차

Ⅰ. 교통안전공단 소개 - 전략 목표

교통사고 없는 밝은 미래를 위하여, 교통사고 예방을 위한 사업을 시행하여, 교통안전관리 효율화를 도모하고, 국민의 생명, 신체 및 재산 보호에 기여합니다.

비전	세계 최고의 교통안전전문기관
핵심가치	안전, 도전, 신뢰
전략방향	**교통안전 선진화** (철도 및 항공 안전사업 역량 강화, 교통안전연구 강화 등)
	자동차관리 첨단화 (스마트 자동차관리정보시스템 구축, 미래/고객지향 검사서비스 개발 등)
	미래 녹색교통 선도 (친환경 교통인프라 구축, 온실가스 감축사업 등)
	지속가능경영 실현 (청렴문화 정착, 고객감동 실현 등)

Ⅰ. 교통안전공단 소개 - 주요사업현황

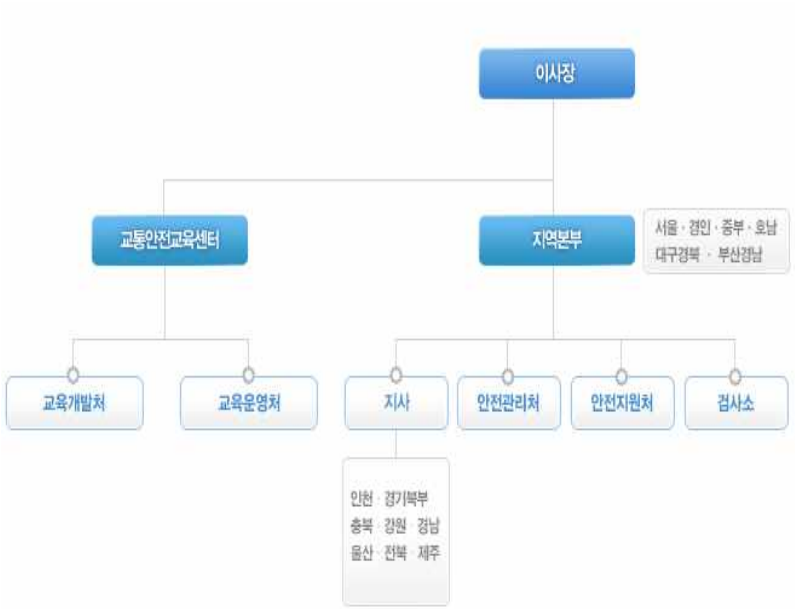
교통안전공단은 육상, 항공, 철도 등 교통 전분야에서 국민의 생명과 재산을 보호하기 위한 각종 교통안전사업을 펼칩니다.

자동차검사	- 자동차의 정기검사, 신규검사, 자동차구조변경검사 - 자동차검사용기기의 정밀도 검사 등
철도, 항공안전	- 철도차량 운전면허시험, 종합안전검사 - 항공 및 초경량비행장치 안전 및 시험업무 등
자동차사고 피해가족 지원	- 자동차 사고로 사망하거나 중증 후유 장해를 입어 경제적인 어려움을 겪고 있는 피해자 및 그 가족을 지원
운수업체 교통안전 진단	- 사고다발 운수업체 등을 대상으로 교통안전 관리 업무실태 진단
자동차 성능 시험 연구	- 자동차제작결함조사(리콜),자동차및도로안전시설안전도평가 - 자동차안전도 조사, 연구 및 국제협력업무 등
안전운전 체험 연구교육	- 사업용 자동차 운전자의 안전운전 체험교육을 수행

Ⅰ. 교통안전공단 소개 - 조직현황

교통안전공단은 크게 본사, 교통안전교육센터,지역본부 및 검사소로 구성되며, 미래교통IT본부의 교통정보처가 정보화기획, 정보시스템 운영 업무를 수행하고 있습니다.

[본사]



[지역본부 등]

Ⅱ. 데이터 유출방지체계 구축방향 – 추진 목적

내부 개인정보 유출방지 인프라 강화 및 외부침해 감시체계 강화 등을 통하여 전방위적 · 선제적 정보보호관리체계를 제고하고자 하였습니다.

추진 목적

- 2012년 발생된 주요 금융기관 및 인터넷 기업의 침해사고 등으로 인해 **감시/모니터링체계 고도화 필요성 대두**

- 기 구축한 개인정보보호 인프라를 기반으로 **개인정보 이용 및 제공 등을 분석하고 모니터링**하기 위한 인프라의 연계 구축 필요

내부 개인정보 유출방지 및 외부 정보보안침해 대응을 위한
감시 및 모니터링 체계 고도화

Ⅱ. 데이터 유출방지체계 구축방향 – 추진방향

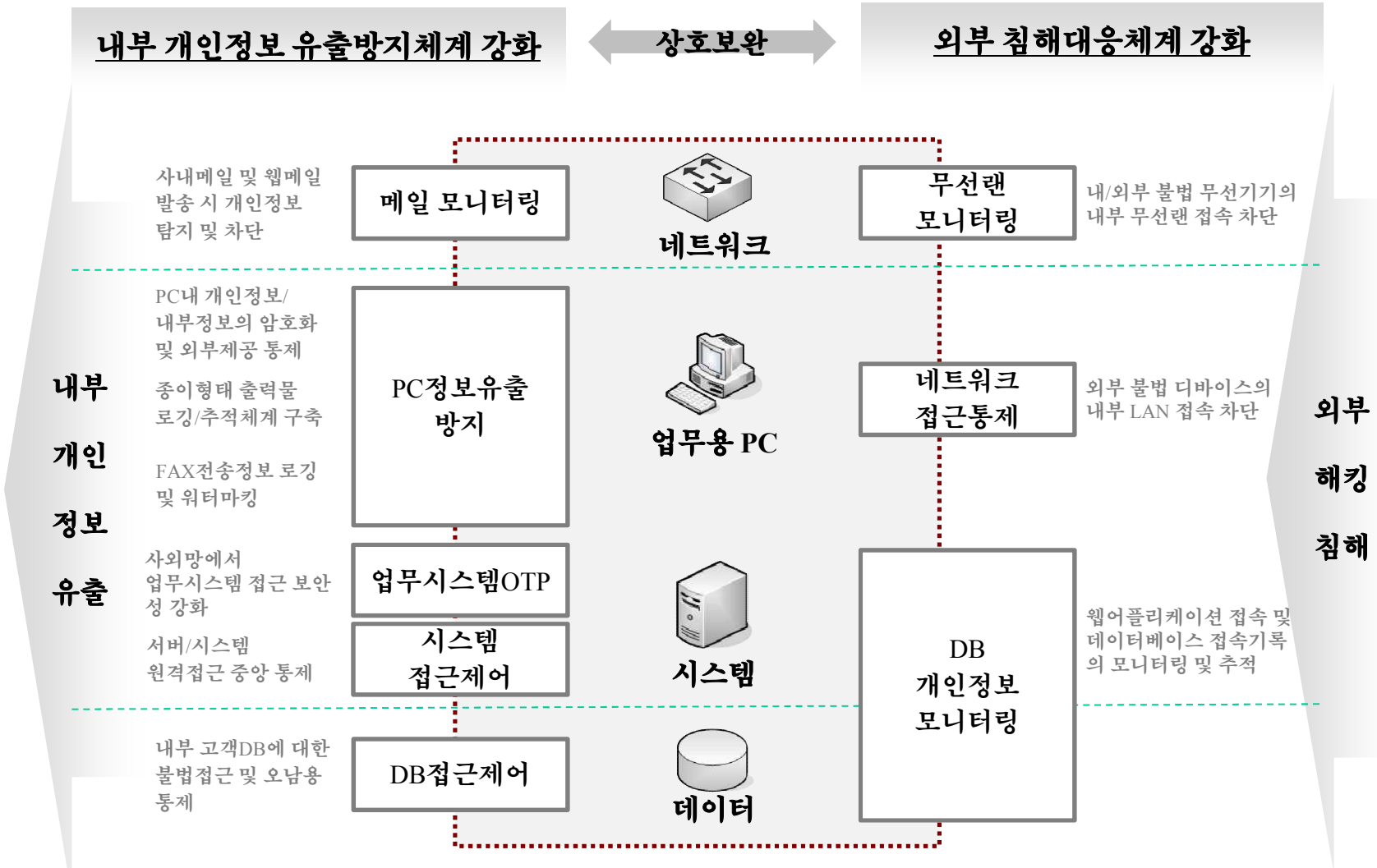
추진 방향

- 개인정보 유출방지를 위한 감시/모니터링 체계 강화
  - ✓ 메일 모니터링을 통한 개인정보 불법 외부전송 감시
  - ✓ USB, 외장하드 등을 통한 개인정보 불법 복사/이동 차단
  - ✓ 인쇄물 형태의 개인정보 사본 추적체계 구축
  - ✓ FAX 전송내용 로깅
  - ✓ 업무시스템 접속절차 보강을 통한 외부망 접속보안 강화
  - ✓ 서버 접속 및 작업현황의 통합 모니터링 적용
  - ✓ DB접근통제 미적용 서버에 대한 통제범위 확대

- 외부 침해사고 예방을 위한 감시/모니터링 체계 강화
  - ✓ 비인가 무선접속 및 무선침해사고 대응 인프라 구축
  - ✓ 비인가 단말기 등의 네트워크 접속 차단
  - ✓ 웹기반 업무시스템 및 DB접속기록의 모니터링 및 추적

Ⅱ. 데이터 유출방지체계 구축방향 - 구축범위

구축 범위

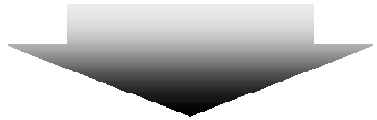


Ⅱ. 데이터 유출방지체계 구축방향 - 기대효과

기대효과

- 개인정보유출방지를 위한 모니터링 시스템 고도화로 **전방위적인 유출 감시체계 구축 및 법적 제도적 요구사항 충족**

- 외부 침해사고 감시체계 강화로 고도화되는 **외부 침해사고의 선제적 감시 및 추적체계 구현**

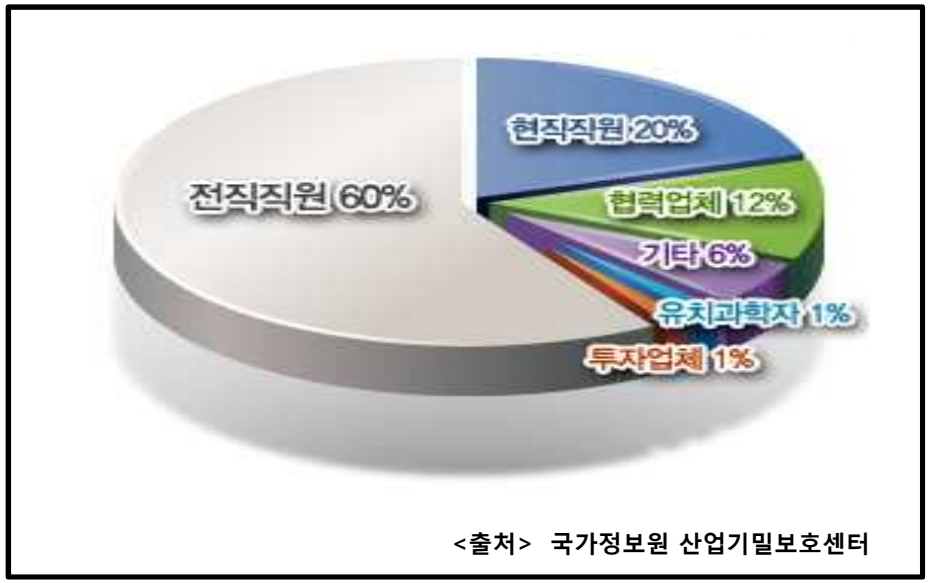


- 공단의 전방위적 · 선제적 **정보보호관리체계 제고**
- 개인정보 접근통제, 접속기록 보관 등 **안정성 확보조치 의무준수**

Ⅲ. 데이터 유출방지체계 구축사례-메일 모니터링

메일 모니터링(1) - 목표

- 웹메일(상용메일) 등 비공식 커뮤니케이션 채널 사용 현황 실시간 모니터링을 통하여 개인정보의 불법 외부전송 감시 및 사고 즉시 추적 가능한 체계 구축

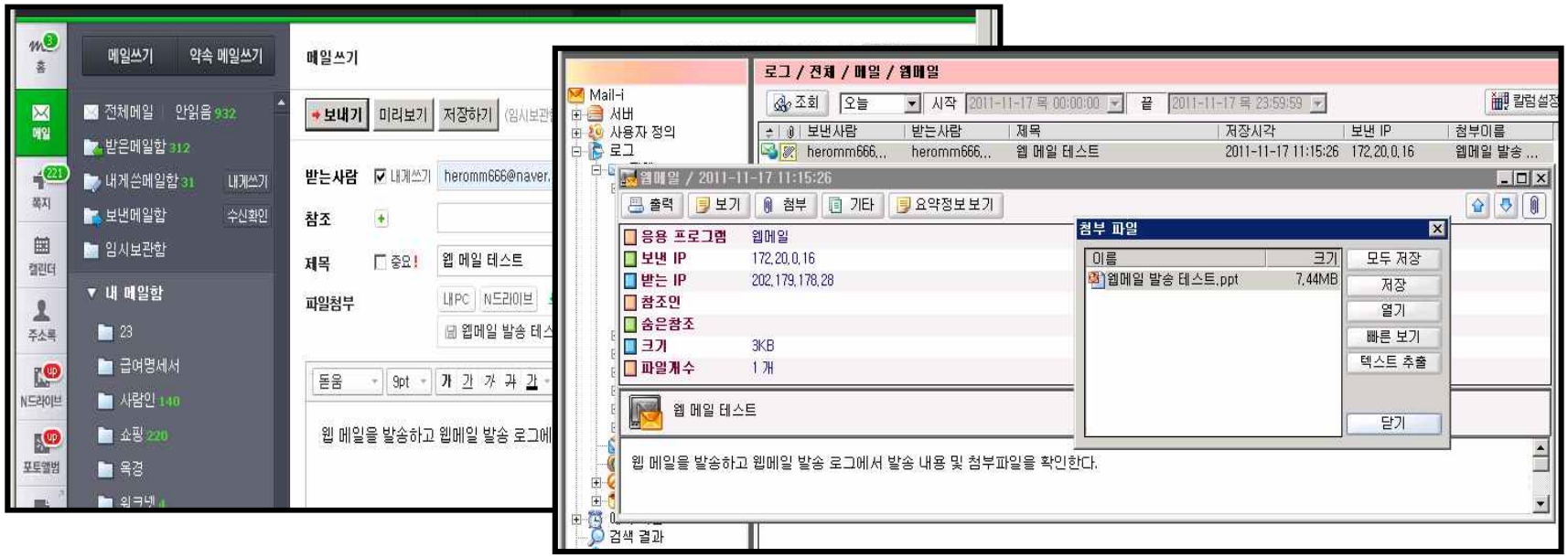


[최근 5년간(2008~2012) 기술유출 주체별 현황]

Ⅲ. 데이터 유출방지체계 구축사례 -메일 모니터링

메일 모니터링(2) -웹메일 발송 감시

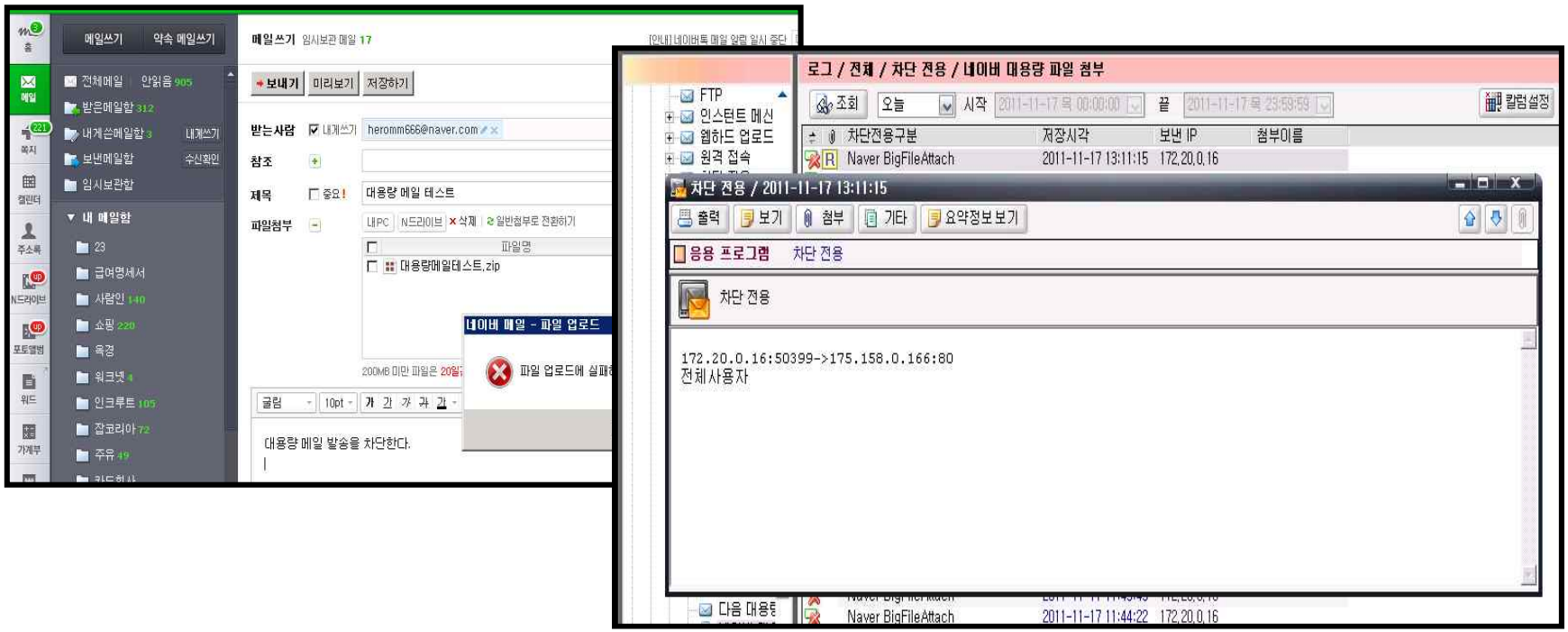
- 웹메일(상용메일)을 이용한 **메일 발송 모니터링**



Ⅲ. 데이터 유출방지체계 구축사례 -메일 모니터링

메일 모니터링(3) - 대용량 첨부 차단

- 웹메일(네이버 등)을 이용한 **대용량 파일 첨부 메일 발송 차단**



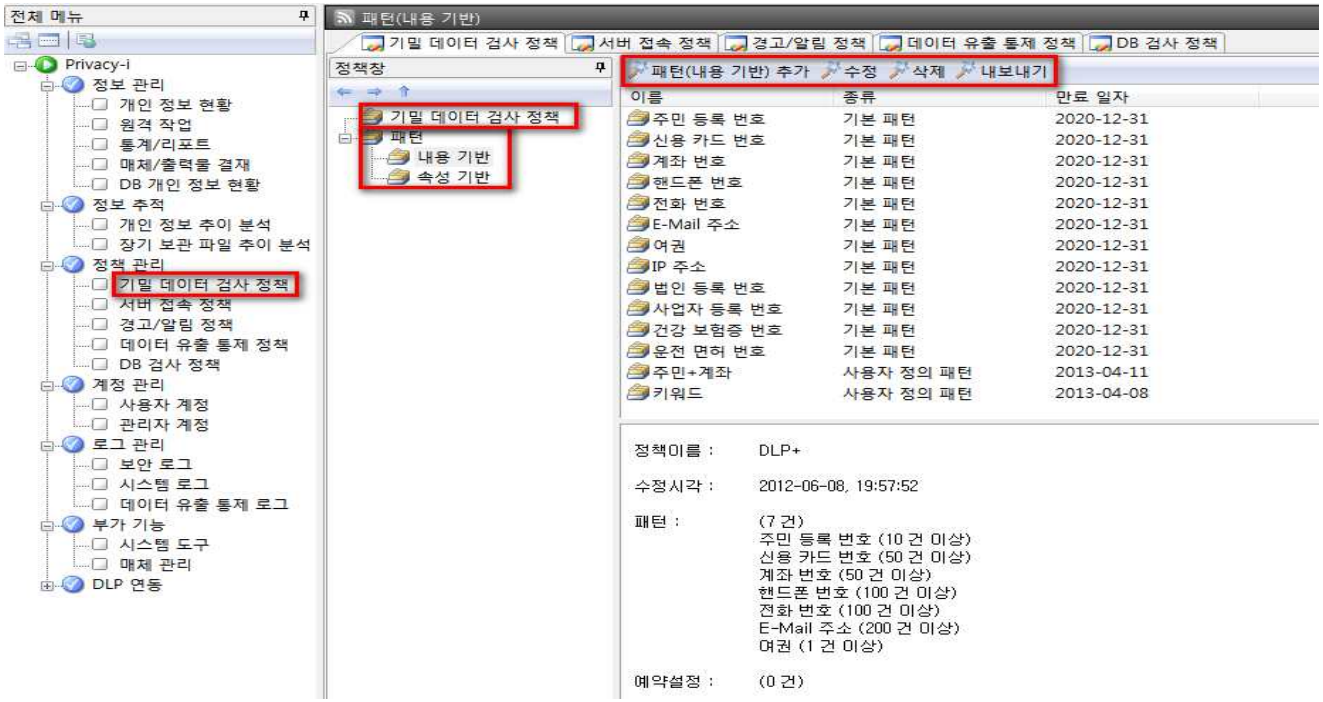
Ⅲ. 데이터 유출방지체계 구축사례 –PC정보유출방지

PC정보 유출 방지(1)-목표

- USB, 인쇄물 등을 통해 PC 외부로 복사/이동하는 행위를 감시하며, 모든 FAX 송신을 별도의 FAX 서버로 일원화하여 데이터 유출 감시

PC정보 유출 방지(2)- USB, 인쇄물

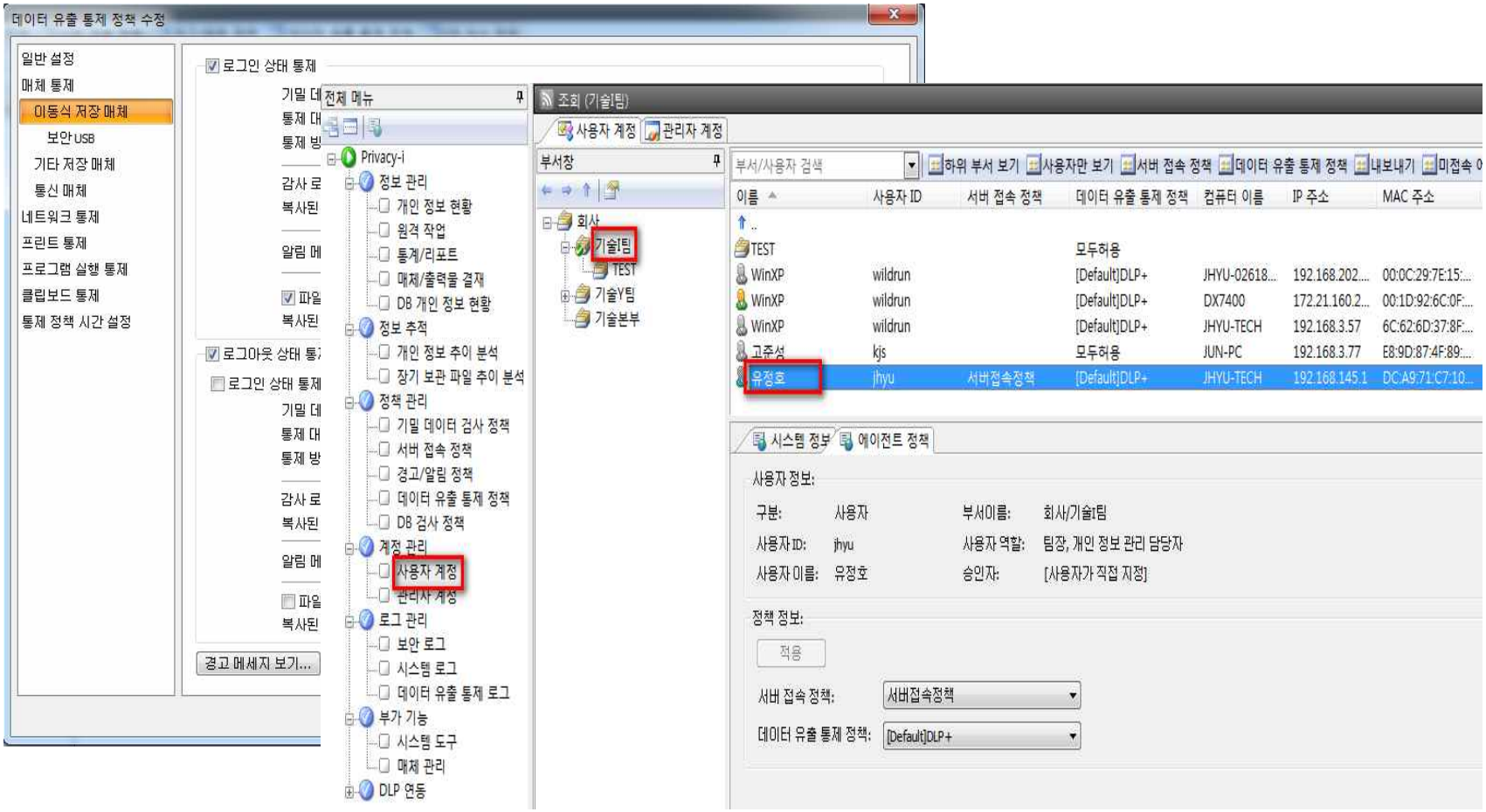
- 기밀데이터(개인정보 등) 검사 정책 수립



Ⅲ. 데이터 유출방지체계 구축사례 –PC정보유출방지

PC정보 유출 방지(3) – USB, 인쇄물

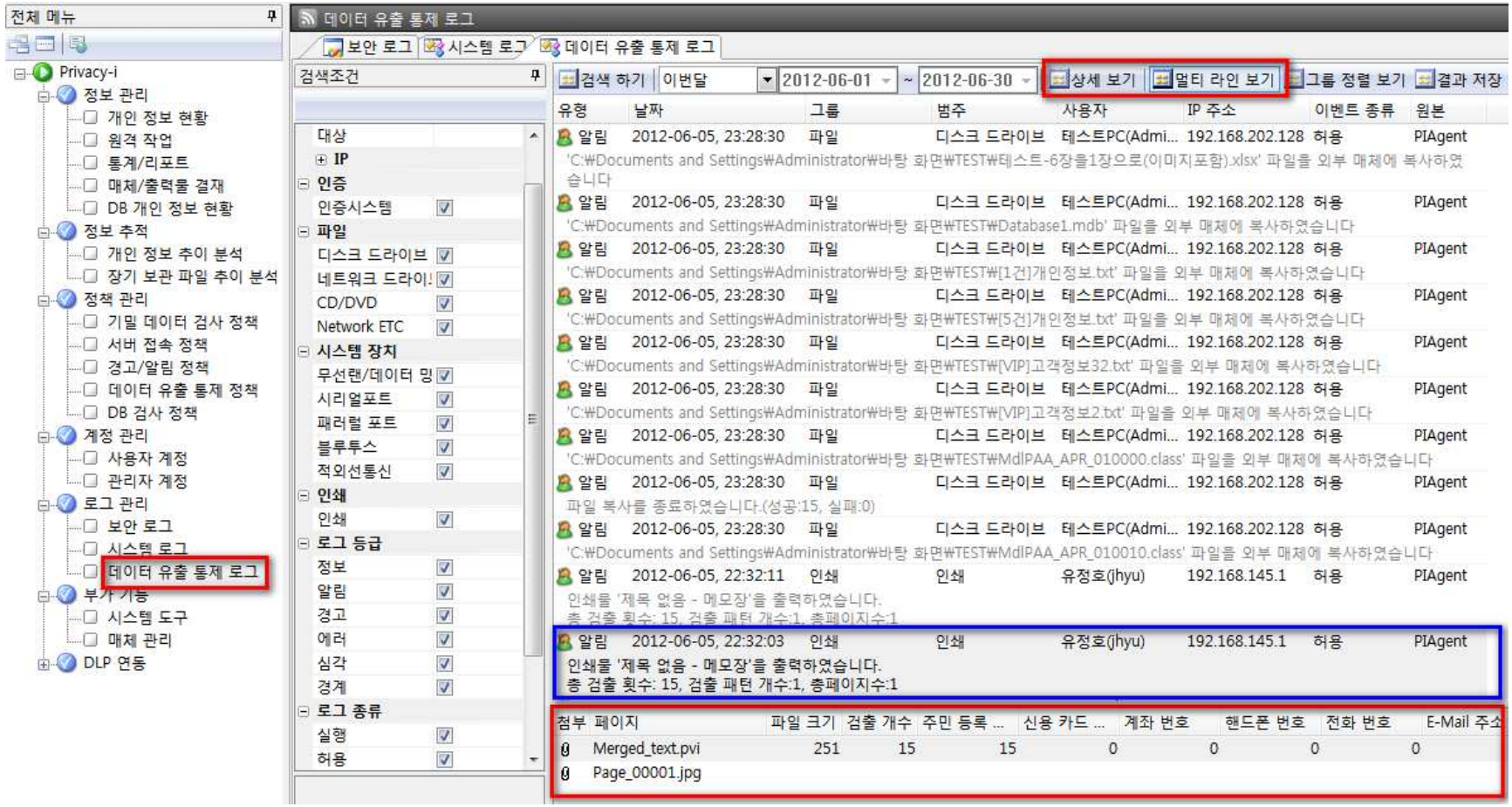
- 이동식 저장매체(USB 등), 프린트 통제 등 정책 수립(부서별, 사용자별)



Ⅲ. 데이터 유출방지체계 구축사례 –PC정보유출방지

PC정보 유출 방지(4) – USB, 인쇄물

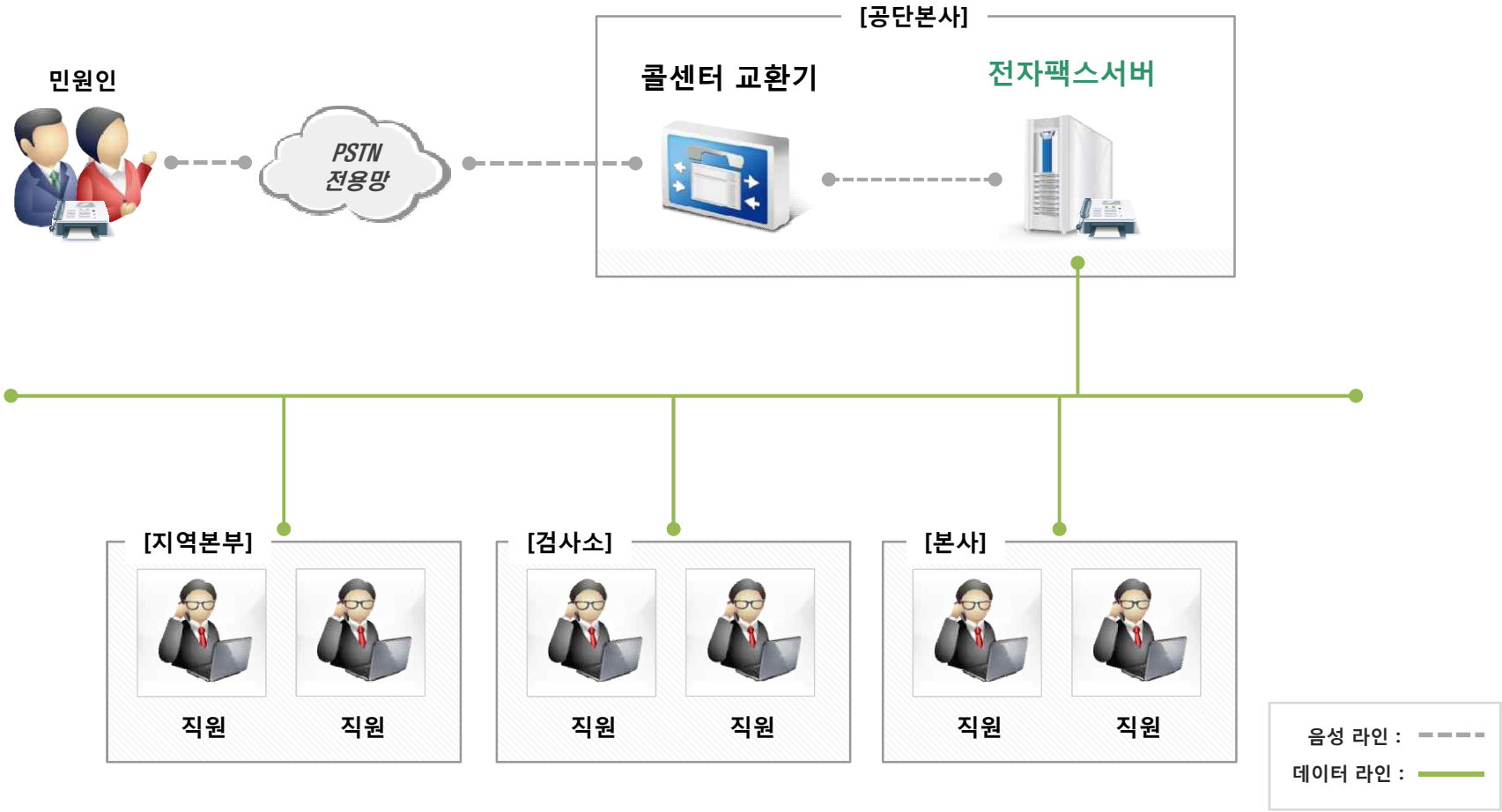
- 이동식 저장매체(USB 등) 복사/이동, 인쇄 작업 모니터링



Ⅲ. 데이터 유출방지체계 구축사례 –PC정보유출방지

PC정보 유출 방지(5) - FAX 전송

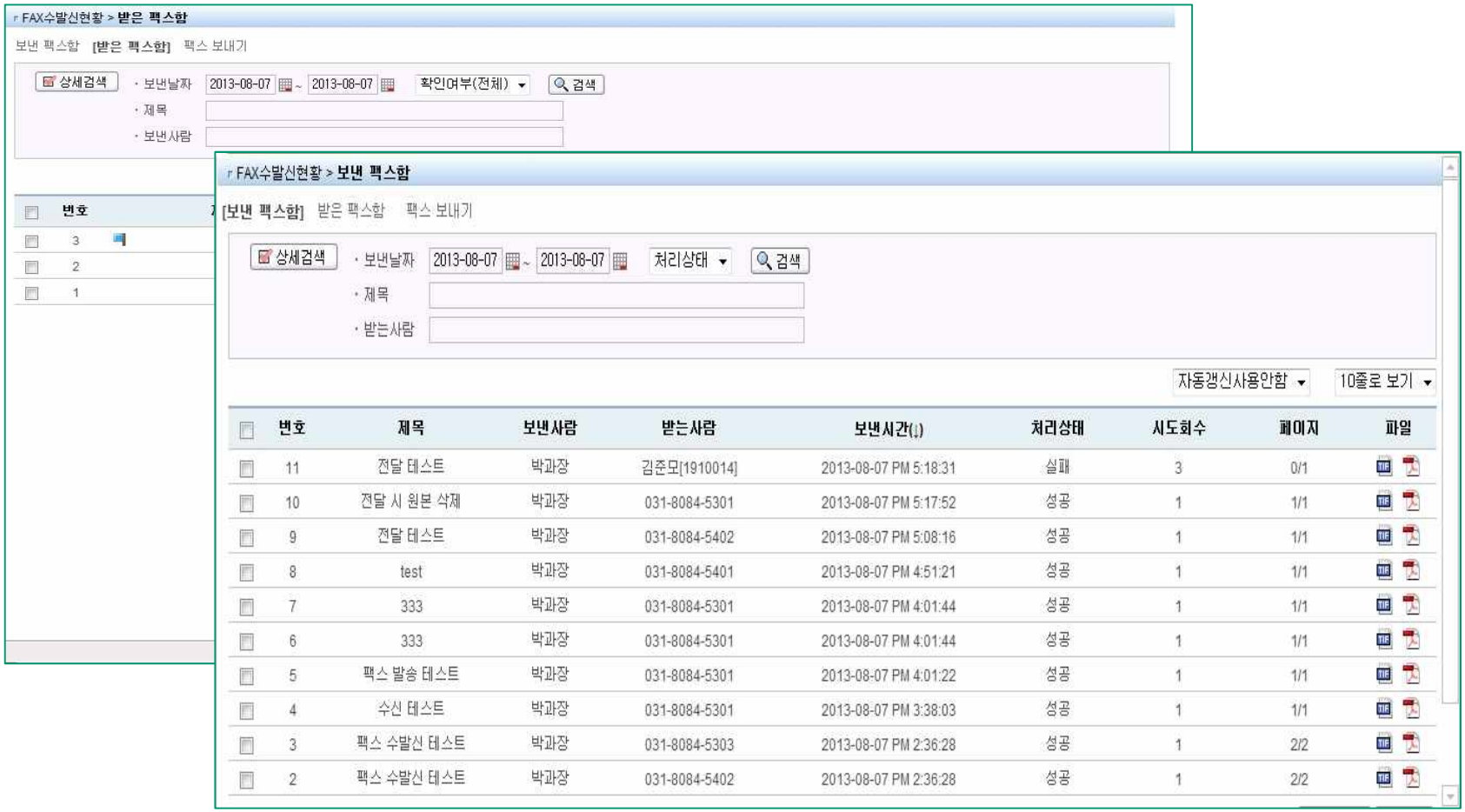
- 구성도



Ⅲ. 데이터 유출방지체계 구축사례 –PC정보유출방지

PC정보 유출 방지(6) - FAX 전송

- 업무포탈 연동 및 FAX 수발신 현황 모니터링



번호	제목	보낸사람	받는사람	보낸시간(↓)	처리상태	시도회수	페이지	파일
11	전달 테스트	박과장	김준모[1910014]	2013-08-07 PM 5:18:31	실패	3	0/1	
10	전달 시 원본 삭제	박과장	031-8084-5301	2013-08-07 PM 5:17:52	성공	1	1/1	
9	전달 테스트	박과장	031-8084-5402	2013-08-07 PM 5:08:16	성공	1	1/1	
8	test	박과장	031-8084-5401	2013-08-07 PM 4:51:21	성공	1	1/1	
7	333	박과장	031-8084-5301	2013-08-07 PM 4:01:44	성공	1	1/1	
6	333	박과장	031-8084-5301	2013-08-07 PM 4:01:44	성공	1	1/1	
5	팩스 발송 테스트	박과장	031-8084-5301	2013-08-07 PM 4:01:22	성공	1	1/1	
4	수신 테스트	박과장	031-8084-5301	2013-08-07 PM 3:38:03	성공	1	1/1	
3	팩스 수발신 테스트	박과장	031-8084-5303	2013-08-07 PM 2:36:28	성공	1	2/2	
2	팩스 수발신 테스트	박과장	031-8084-5402	2013-08-07 PM 2:36:28	성공	1	2/2	

Ⅲ. 데이터 유출방지체계 구축사례 –업무시스템 OTP

업무시스템 OTP(1) - 목표

- 외부망에서의 업무시스템 접속절차 보강(ID/PW + OTP)을 통한 외부망 접속보안 강화

업무시스템 OTP(2) - 문자, APP 발송

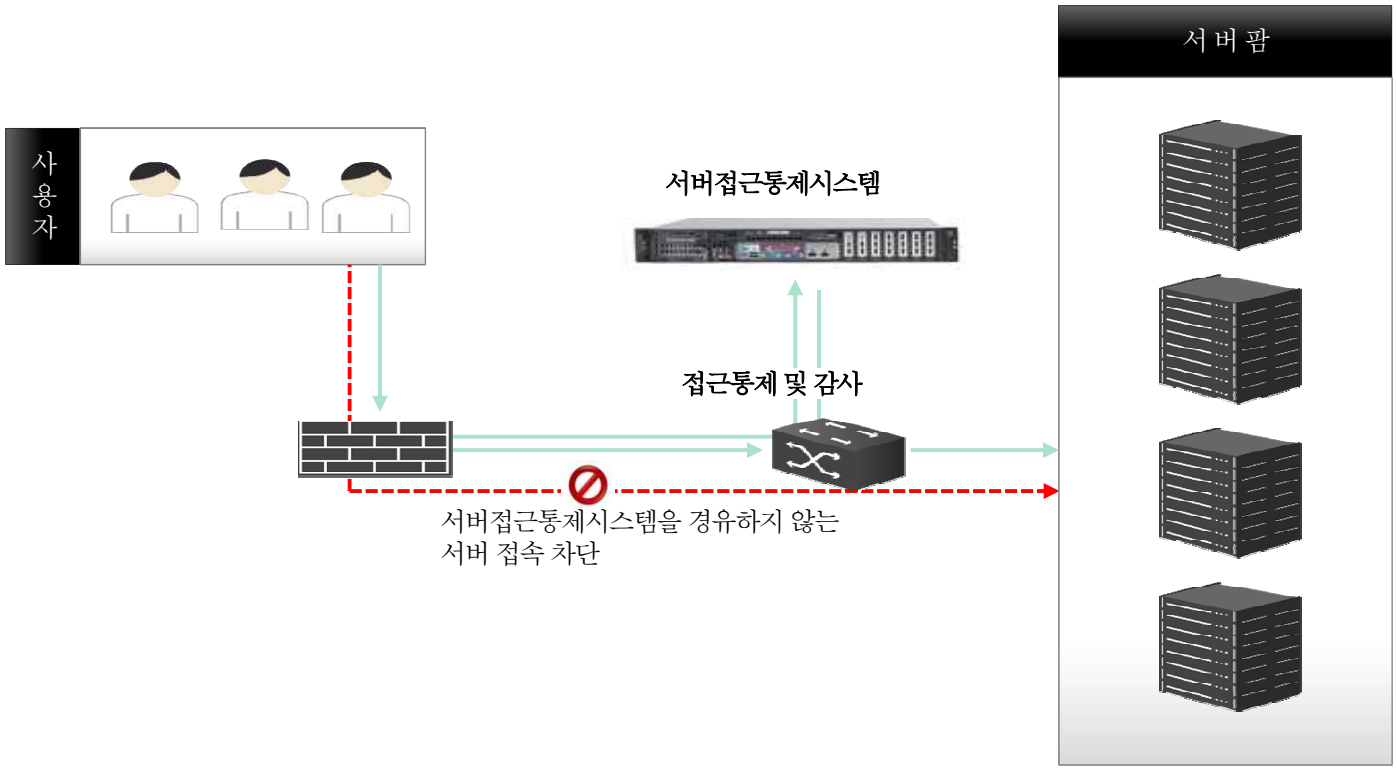
- 외부망에서 접속 시 1차로 ID/PW 인증 후, 2차로 문자메시지 또는 스마트폰 APP에서 생성되는 OTP입력

Ⅲ. 데이터 유출방지체계 구축사례 –시스템 접근제어

시스템 접근제어(1) - 목표

- 서버 접속 및 작업의 통합 모니터링으로 통제수준 강화

시스템 접근제어(2) - 구성도



Ⅲ. 데이터 유출방지체계 구축사례 –시스템 접근제어

시스템 접근제어(3) – 주요 정책

- 서버 접속 권한 및 계정 통합 관리
- 시스템 접속 이력 및 시스템 내에서의 작업내역 저장

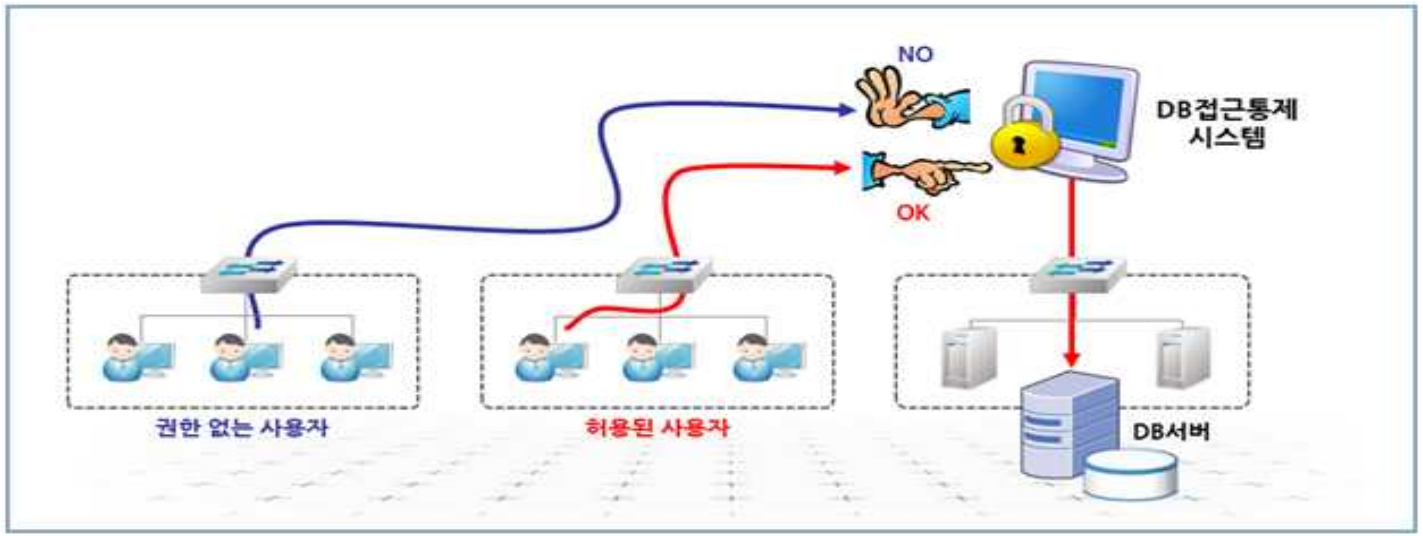
Ⅲ. 데이터 유출방지체계 구축사례 –DB 접근제어

DB 접근제어(1) – 목표

- 내부 고객 DB에 대한 불법접근 및 오남용 통제체계 구축
  * 자동차검사통합정보시스템(VIMS) DB 대상 확대 구축

DB 접근제어(2) – 주요 정책

- DB서버 내 고객 정보의 조회, 복사 등의 작업로그 저장
- 과다한 고객정보 조회 요청 건으로 판단시 사전 통제
- 작업결과 리턴되는 고객정보의 일부를 마스킹



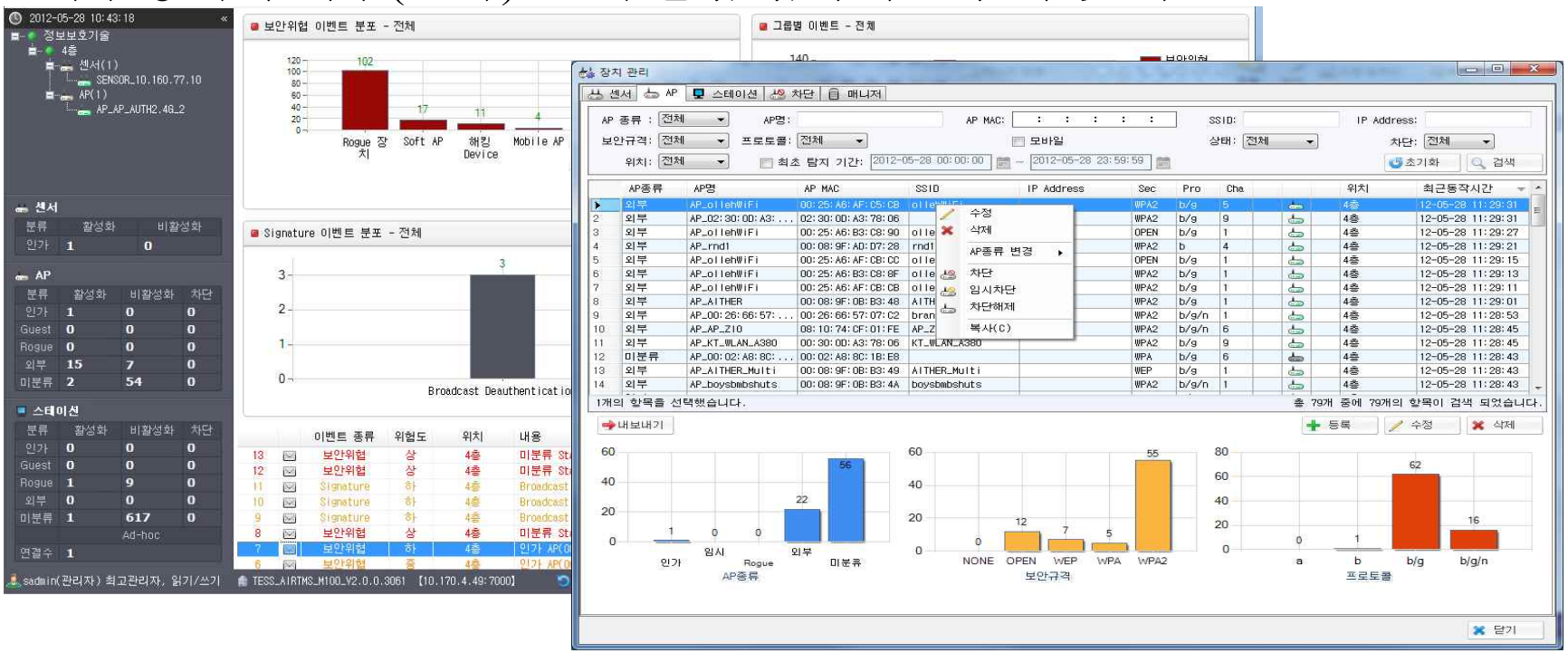
Ⅲ. 데이터 유출방지체계 구축사례 –무선랜 모니터링

무선랜 모니터링(1) – 목표

- 비인가 무선접속 및 무선침해사고 대응 인프라 구축

무선랜 모니터링(2) – 주요정책

- 개인이 임의 구축한 사설 무선랜 공유기(AP) 탐지 및 차단
- 외부망에서 내부(인가) AP에 불법 접속시도 탐지 및 차단



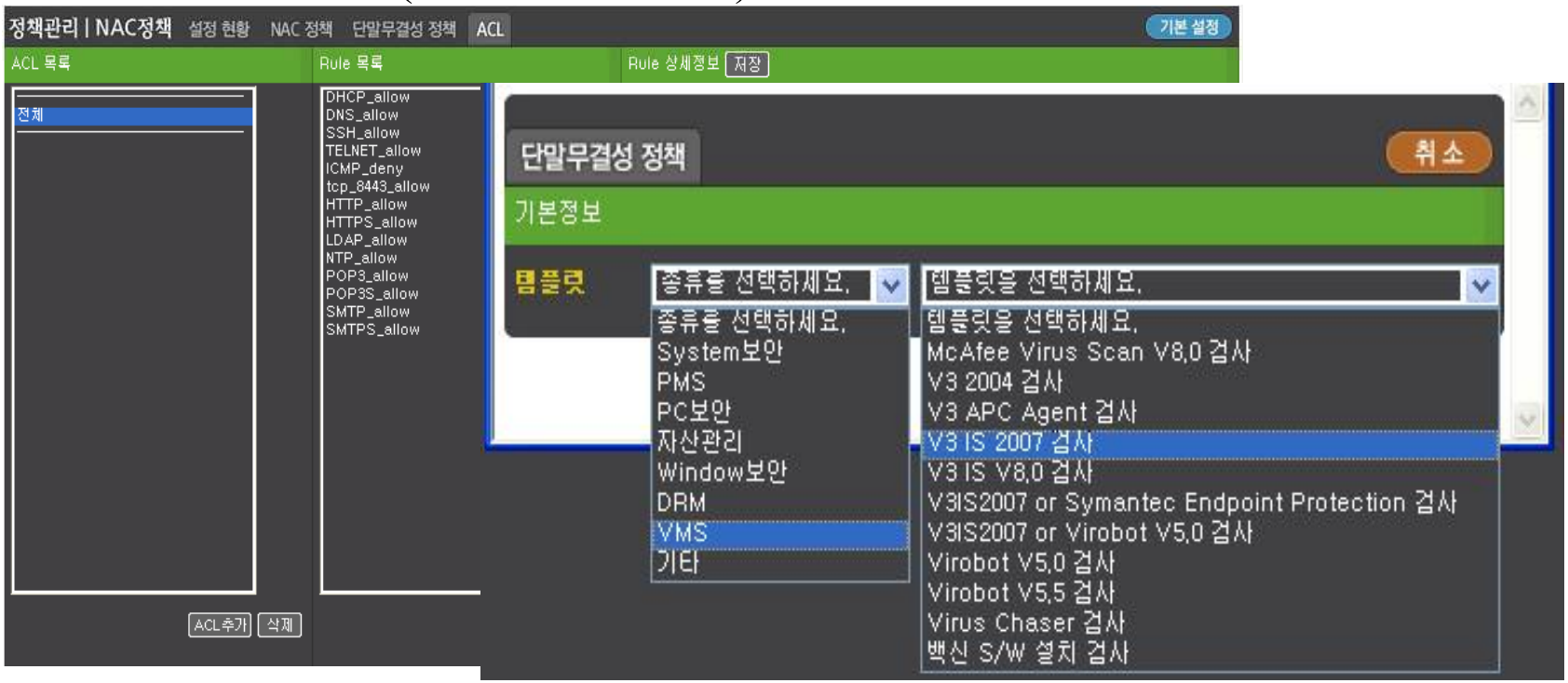
Ⅲ. 데이터 유출방지체계 구축사례 –네트워크접근통제

네트워크 접근통제(1) - 목표

- 비인가 단말(PC, 노트북 등) 내부 네트워크 접속 통제

네트워크 접근통제(2) - 주요 정책

- 사용자ID, IP 등 정식으로 허용되지 않은 단말의 LAN 접속 차단
- 보안수준 미충족(백신 미설치 등) 단말 탐지 및 설치 유도

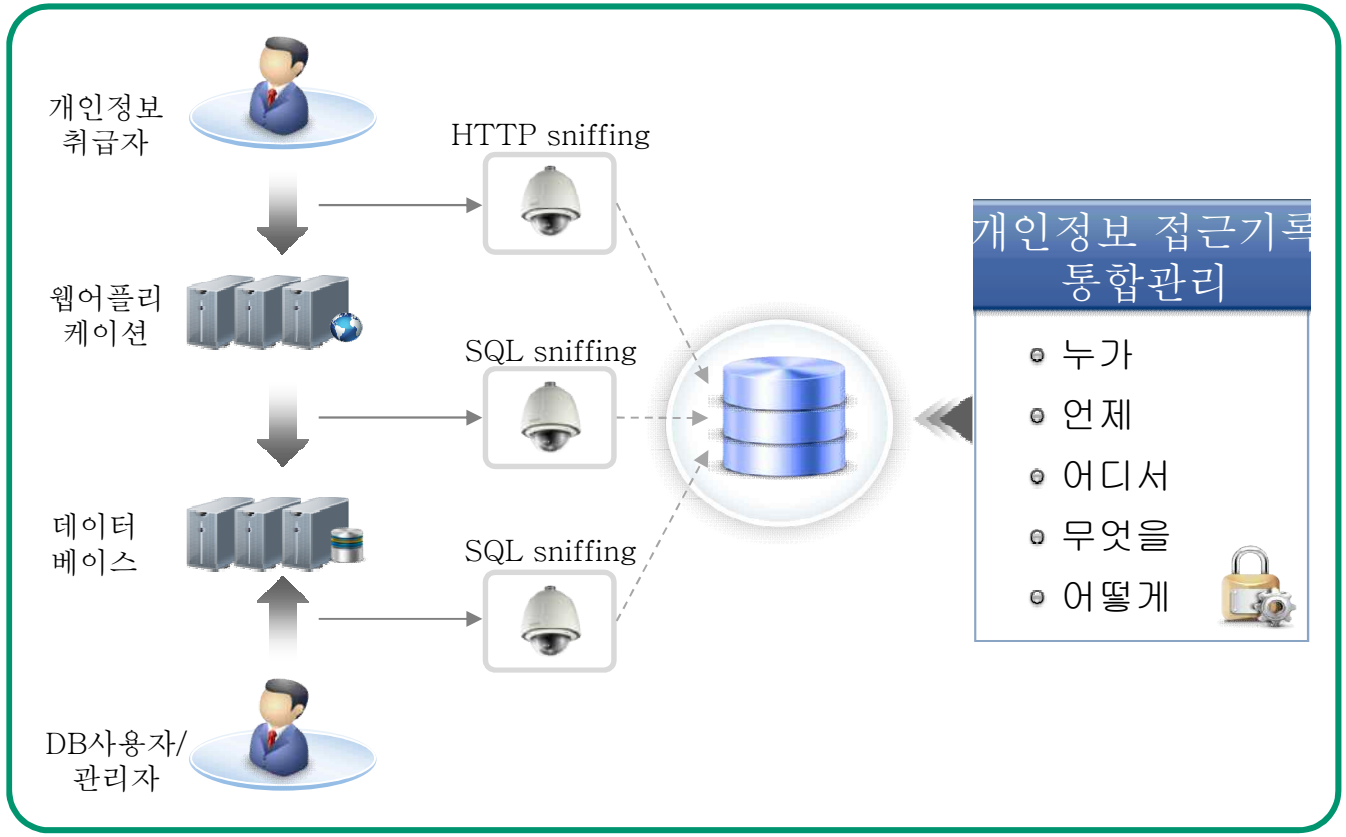


Ⅲ. 데이터 유출방지체계 구축사례 –DB개인정보 모니터링

DB개인정보 모니터링(1) - 목표

- 웹기반 업무시스템 및 DB에 대한 접속기록 모니터링 및 추적

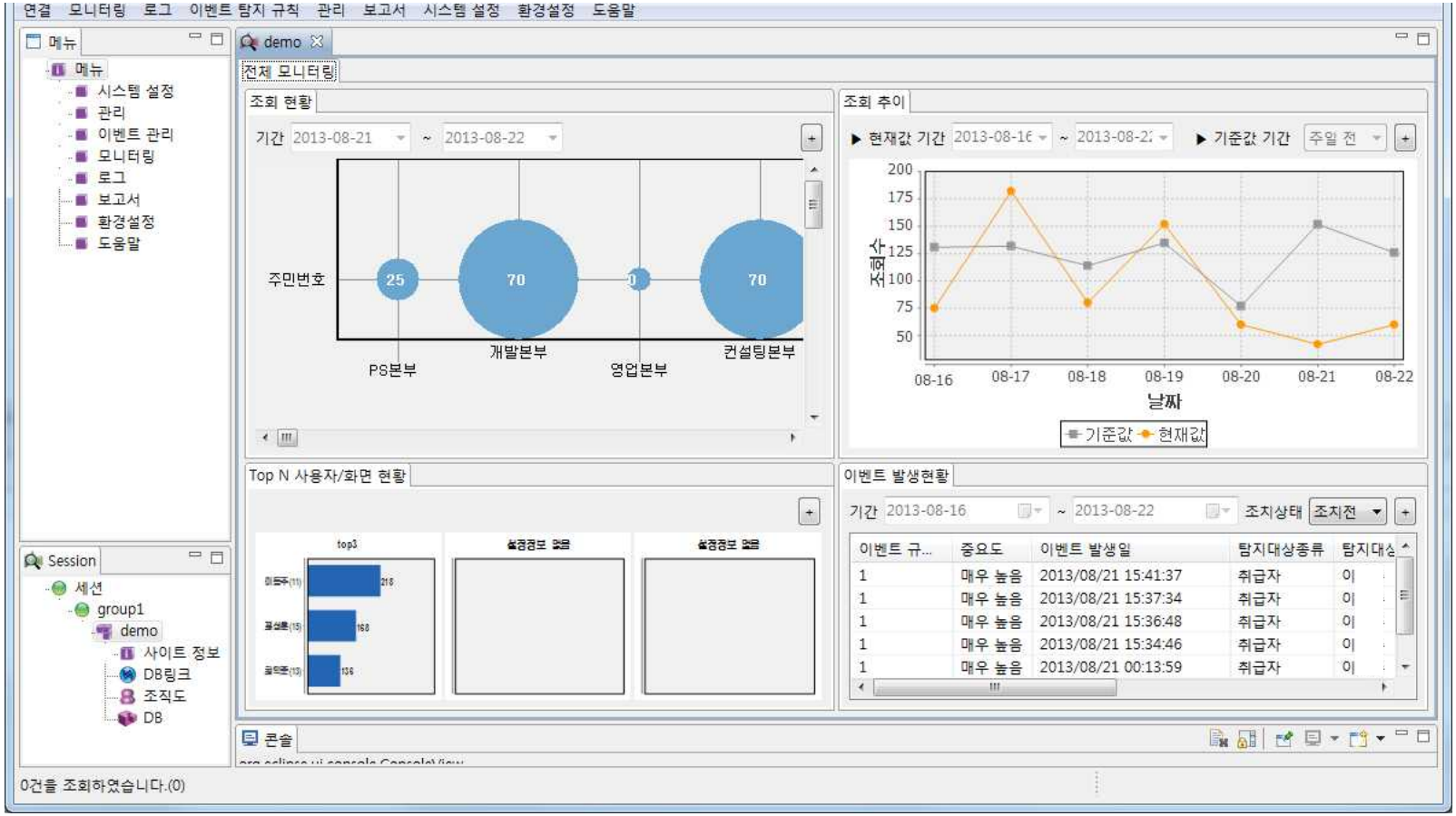
DB개인정보 모니터링(2) - 구성도



Ⅲ. 데이터 유출방지체계 구축사례 –DB개인정보 모니터링

DB개인정보 모니터링(3) - 이력 조회

- 부서별, 기간별, TOP N 사용자별 개인정보 접속 이력 조회

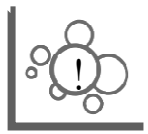


Ⅲ. 데이터 유출방지체계 구축사례 –DB개인정보 모니터링

DB개인정보 모니터링(4) –자동화 감사

- 감사 시나리오

Am 9:00



이상 징후

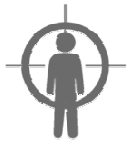
출근하여 전체현황 모니터링 화면을 보니 A부서 버블이 유난히 큰 것을 발견합니다.

Am 9:05

추이 확인

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

Am 9:10



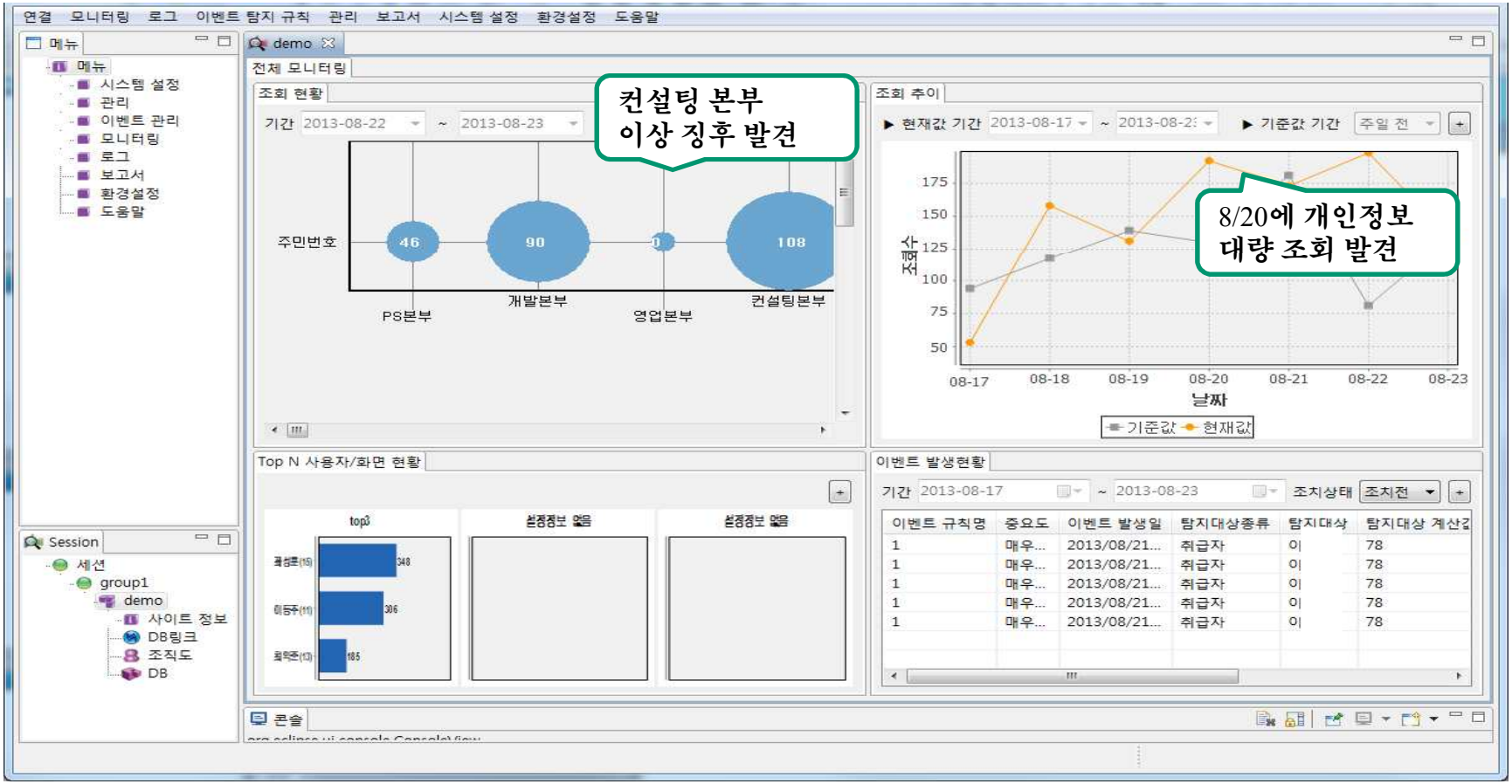
자동화 감사

자동 감사(Audit)창에 '1주일 사이에 부서 평균의 3배이상을 비업무시간에 조회'해 의심사례로 K직원이 올라와 있습니다.

Ⅲ. 데이터 유출방지체계 구축사례 –DB개인정보 모니터링

DB개인정보 모니터링(4) –자동화 감사

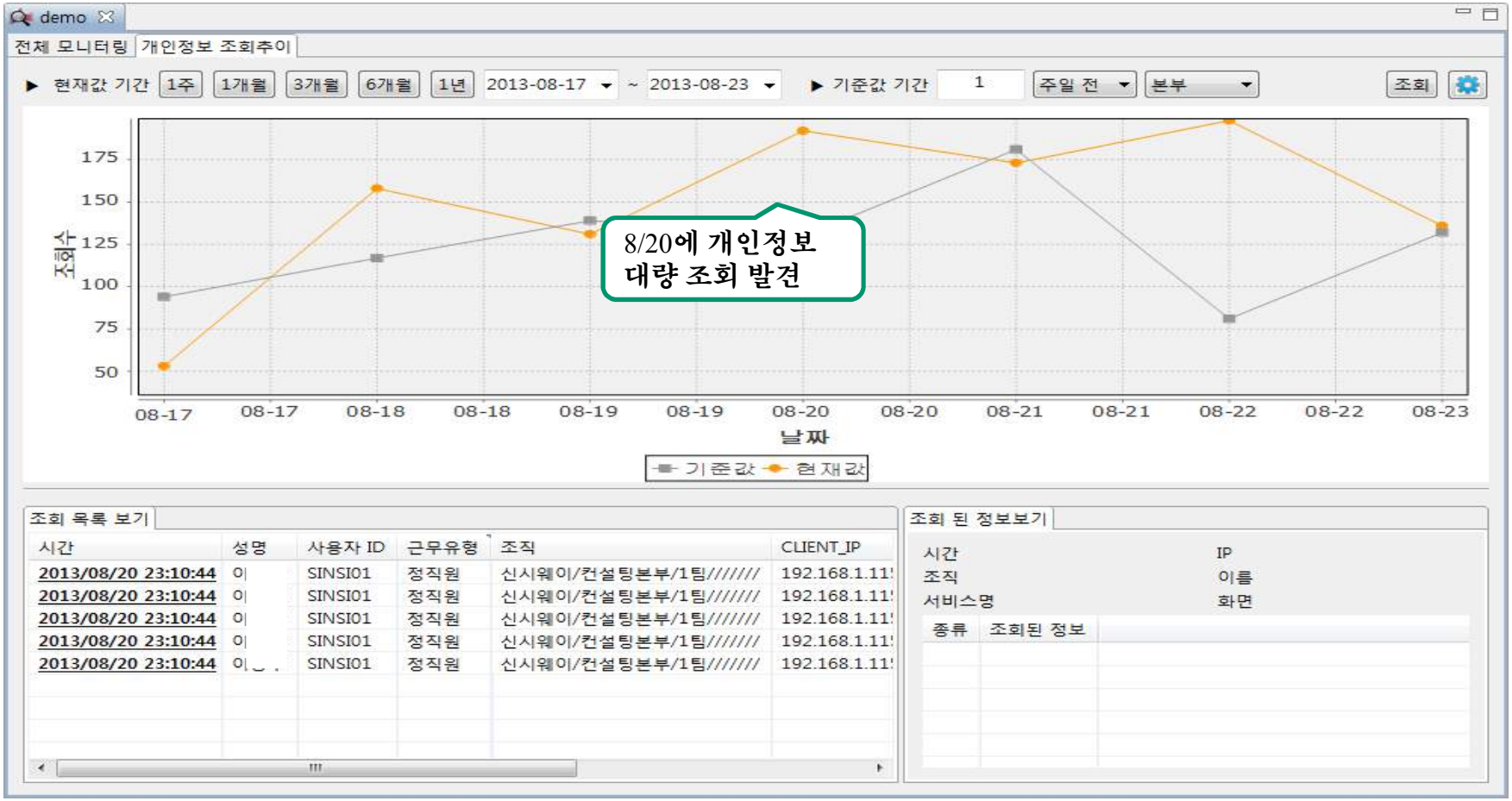
- 이상징후 발견



Ⅲ. 데이터 유출방지체계 구축사례 –DB개인정보 모니터링

DB개인정보 모니터링(4) –자동화 감사

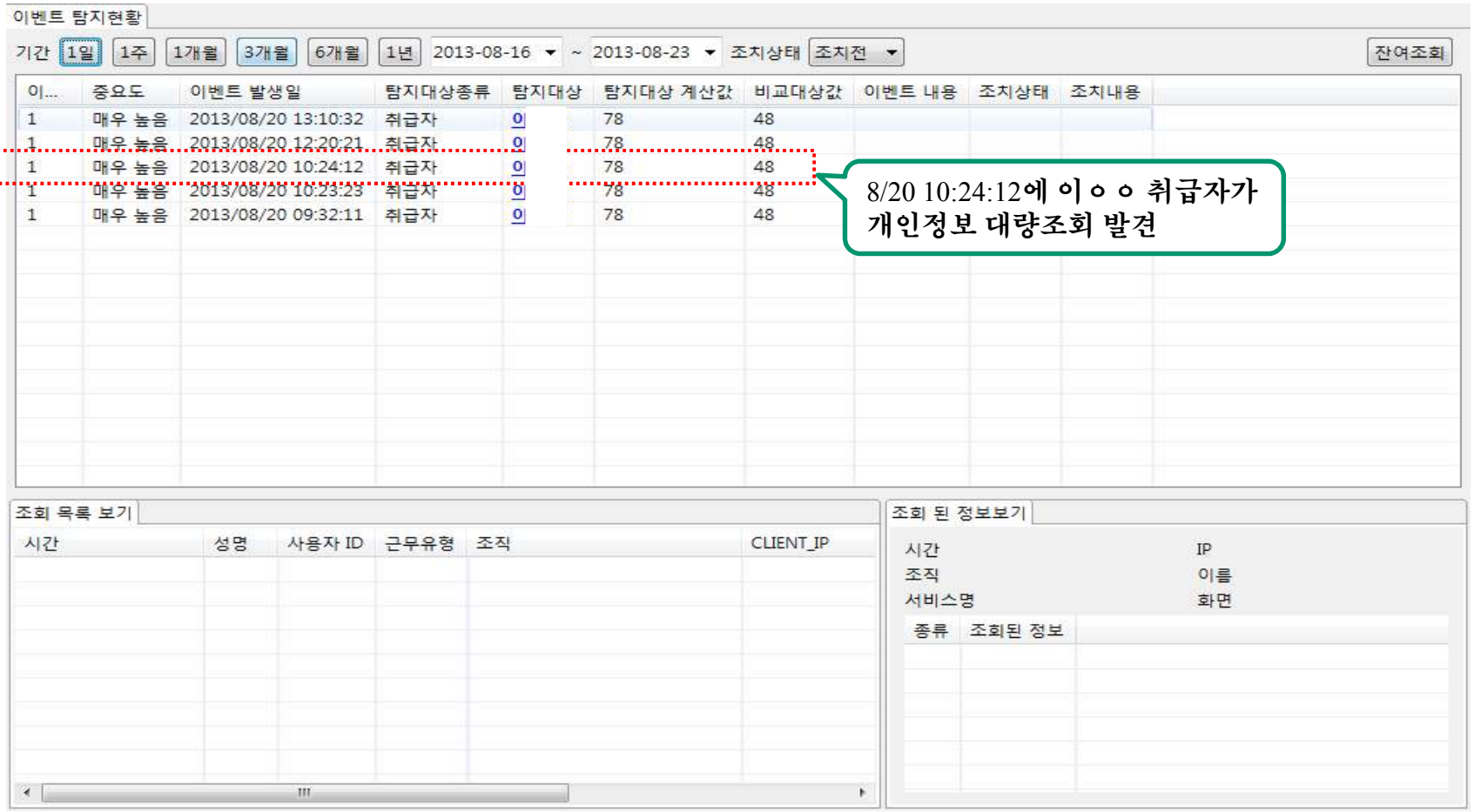
- 추이 확인



Ⅲ. 데이터 유출방지체계 구축사례 –DB개인정보 모니터링

DB개인정보 모니터링(4) –자동화 감사

- 자동화 감사



Ⅳ. 향후 계획

1. 데이터 유출방지시스템 운영관리체계 강화 필요

2. 직원 정보보안인식 제고 노력 필요
   (서비스로서의 정보보안)

3. 통합보안관제 체제 강화 필요
   (예방, 식별 및 분석, 대응 영역 지속적 강화)

TS
교통안전공단

감사합니다.