

데이터 유출방지체계 구축 사례



교통안전공단

2013. 10





교통안전공단 소개



데이터 유출방지체계 구축방향



데이터 유출방지체계 구축사례



향후 계획

I. 교통안전공단 소개 - 전략 목표

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

비전

세계 최고의 교통안전전문기관

**핵심
가치**

안전, 도전, 신뢰

**전략
방향**

교통안전 선진화

(철도 및 항공 안전사업 역량 강화, 교통안전연구 강화 등)

자동차관리 첨단화

(스마트자동차관리정보시스템 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.

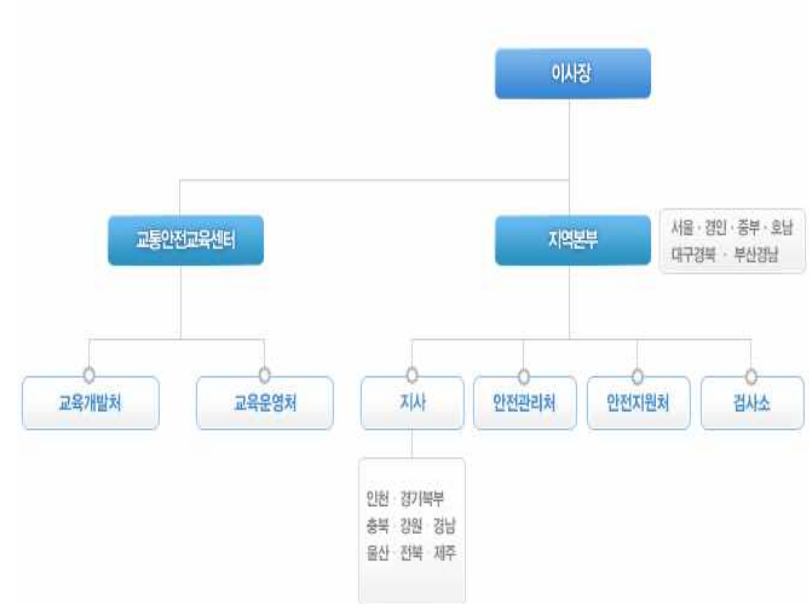
자동차검사	<ul style="list-style-type: none"> - 자동차의 정기검사, 신규검사, 자동차구조변경검사 - 자동차검사용기기의 정밀도 검사 등
철도, 항공안전	<ul style="list-style-type: none"> - 철도차량 운전면허시험, 종합안전검사 - 항공 및 초경량비행장치 안전 및 시험업무 등
자동차사고 피해가족 지원	<ul style="list-style-type: none"> - 자동차 사고로 사망하거나 중증 후유 장애를 입어 경제적인 어려움을 겪고 있는 피해자 및 그 가족을 지원
운수업체 교통안전 진단	<ul style="list-style-type: none"> - 사고다발 운수업체 등을 대상으로 교통안전 관리 업무실태 진단
자동차 성능 시험 연구	<ul style="list-style-type: none"> - 자동차제작결함조사(리콜), 자동차및 도로안전시설 안전도 평가 - 자동차안전도 조사, 연구 및 국제협력업무 등
안전운전 체험 연구교육	<ul style="list-style-type: none"> - 사업용 자동차 운전자의 안전운전 체험교육을 수행

I. 교통안전공단 소개 - 조직현황

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



[본사]



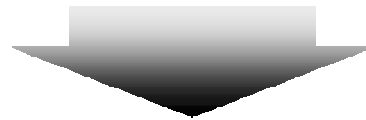
[지역본부 등]

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 발생한 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

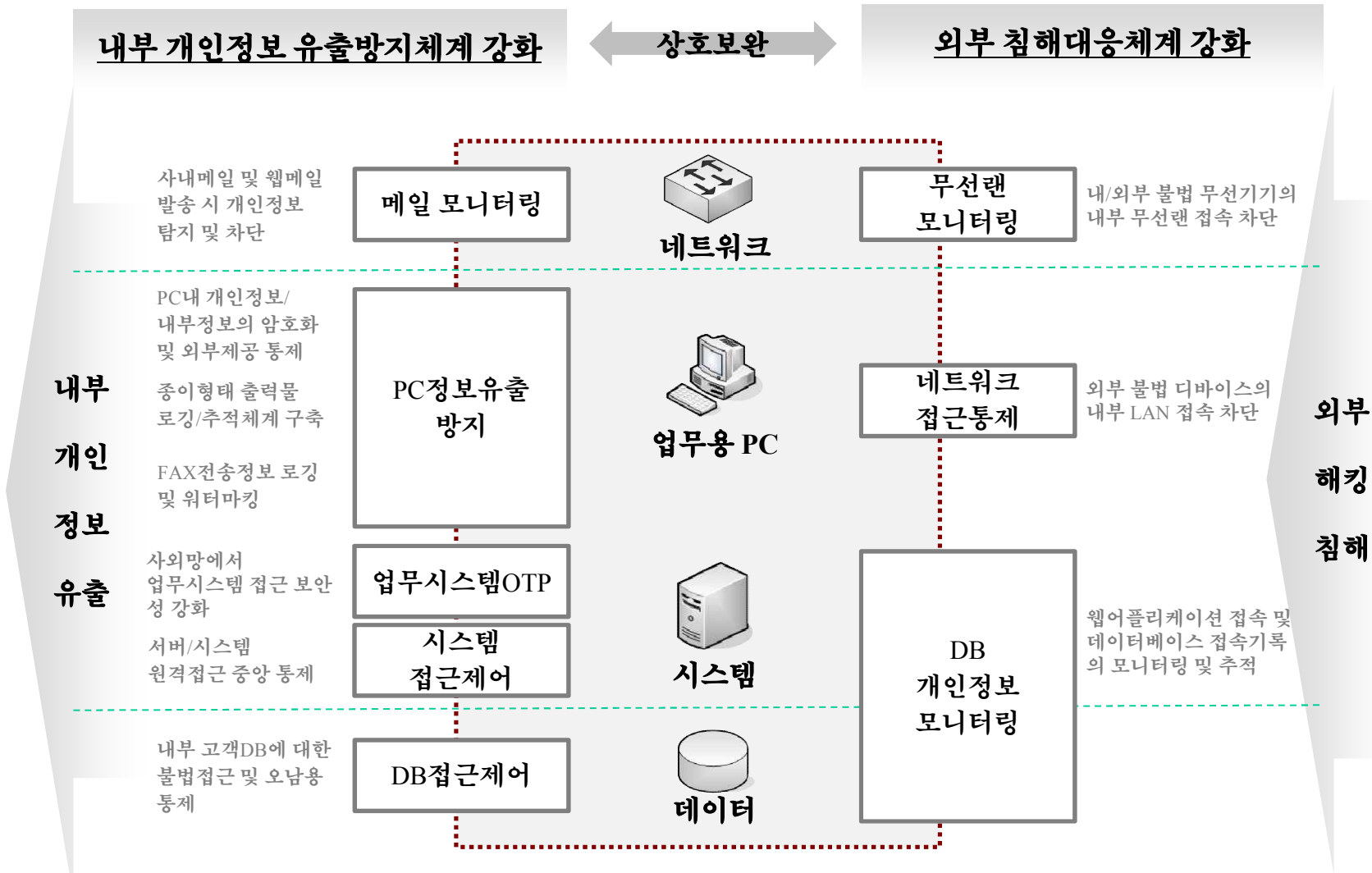
II. 데이터 유출방지체계 구축방향 - 추진방향

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**

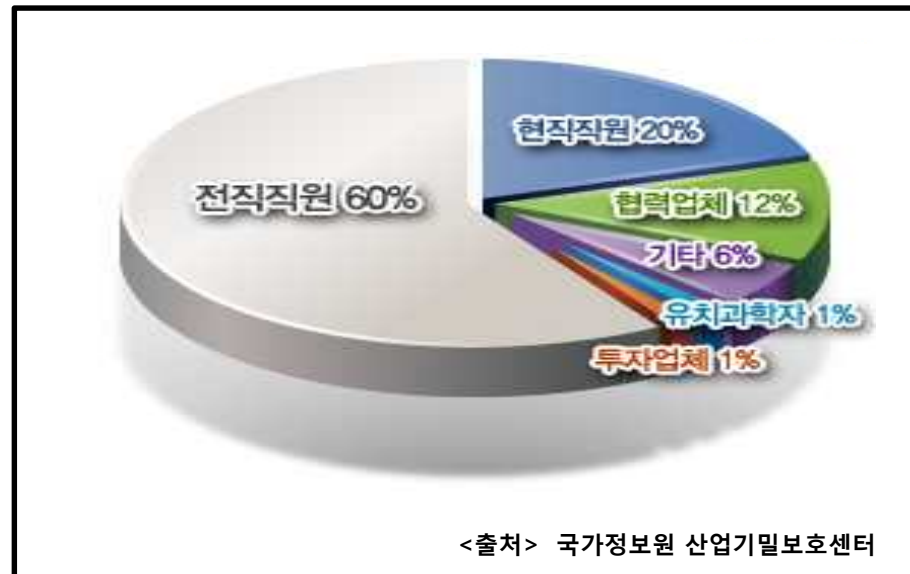


- 공단의 전방위적·선제적 **정보보호관리체계 제고**
- 개인정보 접근통제, 접속기록 보관 등 **안정성 확보조치 의무준수**

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**

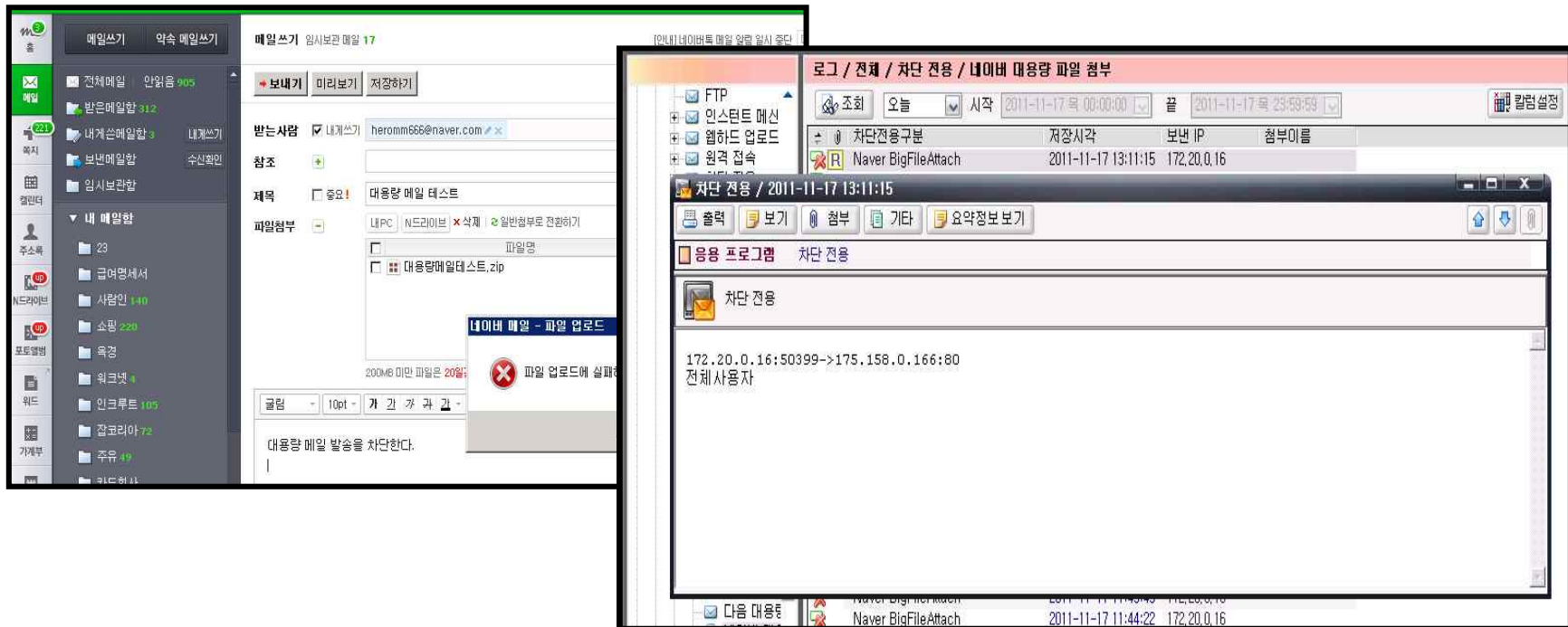


Ⅲ. 데이터 유출방지체계 구축사례 -메일 모니터링



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

The screenshot shows a web-based management interface for security policies. On the left is a tree view of the 'Privacy-i' system, with '기밀 데이터 검사 정책' highlighted. The main area shows the configuration for this policy, including a list of patterns and their details.

이름	종류	만료 일자
주민 등록 번호	기본 패턴	2020-12-31
신용 카드 번호	기본 패턴	2020-12-31
계좌 번호	기본 패턴	2020-12-31
핸드폰 번호	기본 패턴	2020-12-31
전화 번호	기본 패턴	2020-12-31
E-Mail 주소	기본 패턴	2020-12-31
여권	기본 패턴	2020-12-31
IP 주소	기본 패턴	2020-12-31
법인 등록 번호	기본 패턴	2020-12-31
사업자 등록 번호	기본 패턴	2020-12-31
건강 보험증 번호	기본 패턴	2020-12-31
운전 면허 번호	기본 패턴	2020-12-31
주민+계좌	사용자 정의 패턴	2013-04-11
키워드	사용자 정의 패턴	2013-04-08

정책이름 : DLP+
 수정시각 : 2012-06-08, 19:57:52
 패턴 : (7 건)
 주민 등록 번호 (10 건 이상)
 신용카드 번호 (50 건 이상)
 계좌 번호 (50 건 이상)
 핸드폰 번호 (100 건 이상)
 전화 번호 (100 건 이상)
 E-Mail 주소 (200 건 이상)
 여권 (1 건 이상)
 예약설정 : (0 건)

III. 데이터 유출방지체계 구축사례 -PC정보유출방지



PC정보 유출 방지 (3) - USB, 인쇄물

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

The screenshot displays the '데이터 유출 통제 정책 수정' (Data Leakage Control Policy Modification) interface. On the left, a sidebar lists various control categories such as '로그인 상태 통제' (Login State Control), '이동식 저장 매체' (Removable Storage Media), and '프린트 통제' (Print Control). The main area shows a tree view of policies for the '기밀팀' (Secret Team) department. The '사용자 계정' (User Account) policy is selected and highlighted with a red box. The right pane shows the details for the user '유정호' (Yoo Jung-ho), with fields for '구분' (Category: 사용자), '부서이름' (Department Name: 회사/기밀팀), '사용자 ID' (User ID: jhyu), and '사용자 이름' (User Name: 유정호). Below this, there are dropdown menus for '서버 접속 정책' (Server Access Policy) and '데이터 유출 통제 정책' (Data Leakage Control Policy).

III. 데이터 유출방지체계 구축사례 -PC정보유출방지



PC정보 유출 방지(4) - USB, 인쇄물

- 이동식 저장매체(USB 등) 복사/이동, 인쇄 작업 모니터링

유형	날짜	그룹	범주	사용자	IP 주소	이벤트 종류	원본
알림	2012-06-05, 23:28:30	파일	디스크 드라이브	테스트PC(Admi...	192.168.202.128	허용	PIAgent
알림	2012-06-05, 23:28:30	파일	디스크 드라이브	테스트PC(Admi...	192.168.202.128	허용	PIAgent
알림	2012-06-05, 23:28:30	파일	디스크 드라이브	테스트PC(Admi...	192.168.202.128	허용	PIAgent
알림	2012-06-05, 23:28:30	파일	디스크 드라이브	테스트PC(Admi...	192.168.202.128	허용	PIAgent
알림	2012-06-05, 23:28:30	파일	디스크 드라이브	테스트PC(Admi...	192.168.202.128	허용	PIAgent
알림	2012-06-05, 23:28:30	파일	디스크 드라이브	테스트PC(Admi...	192.168.202.128	허용	PIAgent
알림	2012-06-05, 23:28:30	파일	디스크 드라이브	테스트PC(Admi...	192.168.202.128	허용	PIAgent
알림	2012-06-05, 23:28:30	파일	디스크 드라이브	테스트PC(Admi...	192.168.202.128	허용	PIAgent
알림	2012-06-05, 23:28:30	파일	디스크 드라이브	테스트PC(Admi...	192.168.202.128	허용	PIAgent
알림	2012-06-05, 23:28:30	파일	디스크 드라이브	테스트PC(Admi...	192.168.202.128	허용	PIAgent
알림	2012-06-05, 22:32:11	인쇄	인쇄	유정호(jhyu)	192.168.145.1	허용	PIAgent
알림	2012-06-05, 22:32:03	인쇄	인쇄	유정호(jhyu)	192.168.145.1	허용	PIAgent

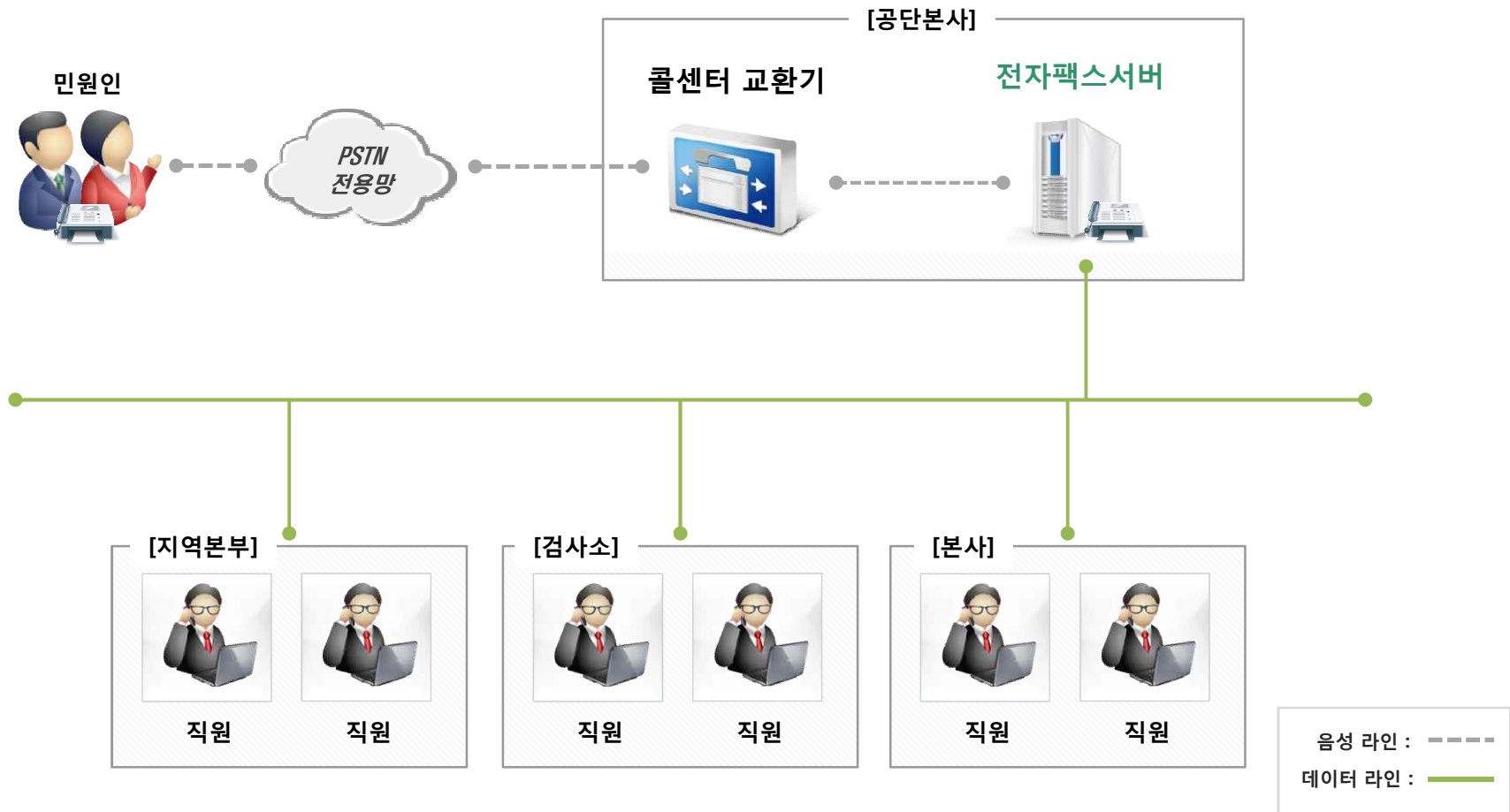
첨부 페이지	파일 크기	검출 개수	주인 등록	신용 카드	계좌 번호	핸드폰 번호	전화 번호	E-Mail 주소
0	Merged_text.pvi	251	15	15	0	0	0	0
0	Page_00001.jpg							

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

FAX수발신현황 > 받은 팩스함

받은 팩스함 [받은 팩스함] 팩스 보내기

상세검색 · 보낸날짜 2013-08-07 ~ 2013-08-07 확인여부(전체) 검색

· 제목

· 보낸사람

FAX수발신현황 > 보낸 팩스함

[보낸 팩스함] 받은 팩스함 팩스 보내기

상세검색 · 보낸날짜 2013-08-07 ~ 2013-08-07 처리상태 검색

· 제목

· 받는사람

자동갱신사용안함 10줄로 보기

번호	제목	보낸사람	받는사람	보낸시간(시)	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	

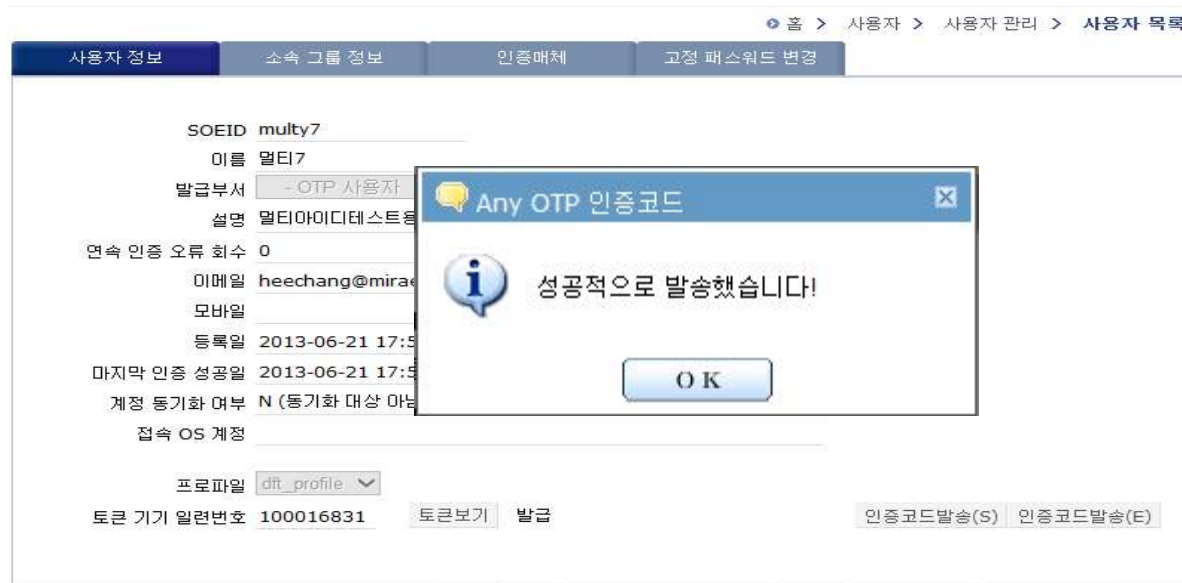
Ⅲ. 데이터 유출방지체계 구축사례 - 업무시스템 OTP

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



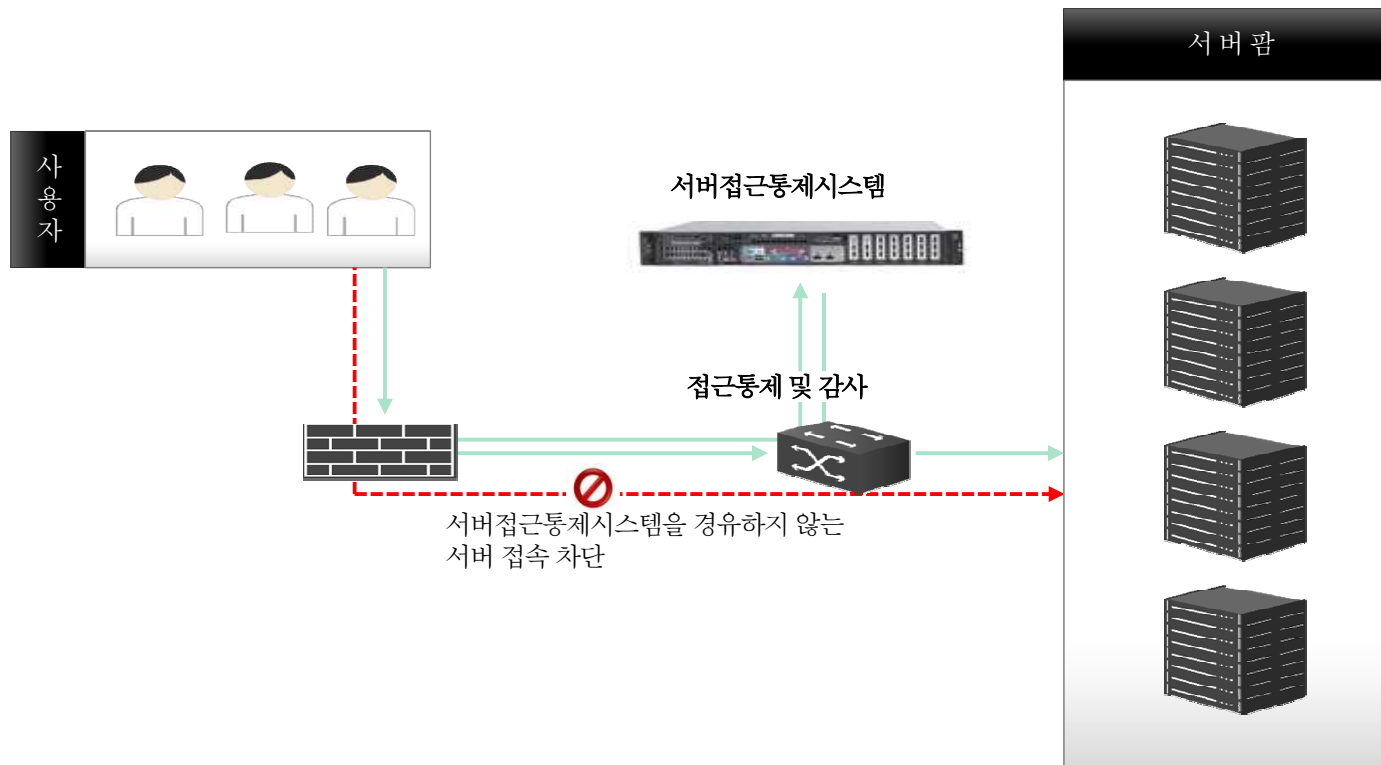
Ⅲ. 데이터 유출방지체계 구축사례 -시스템 접근제어



시스템 접근제어(1) - 목표

- 서버 접속 및 작업의 통합 모니터링으로 통제수준 강화

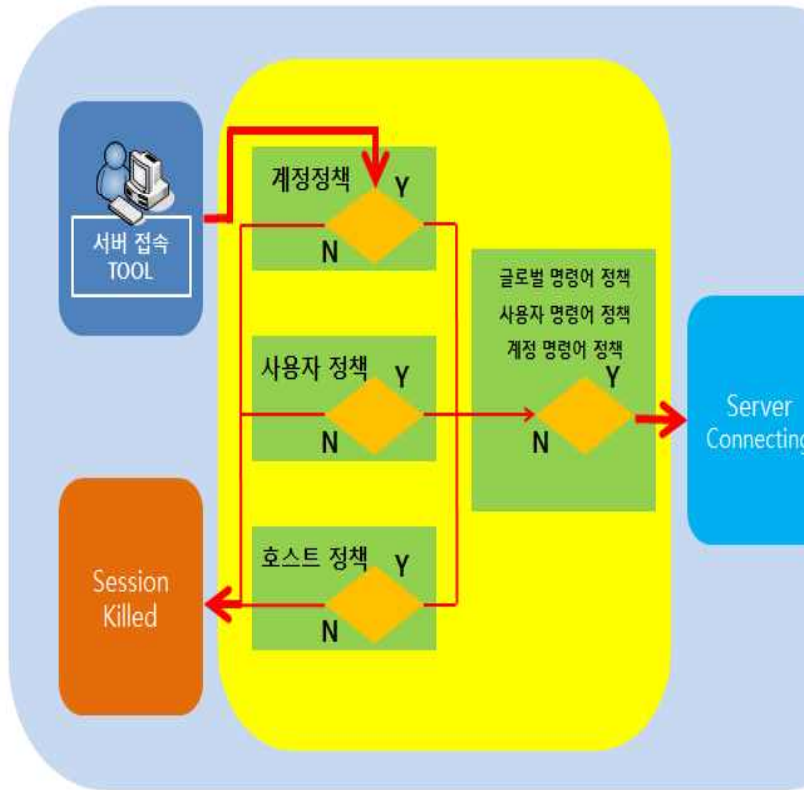
시스템 접근제어(2) - 구성도



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



호스트 정책 추가	
호스트 정보(+)	호스트명: <input type="text"/> IP: <input type="text"/> CONFID: <input type="text"/> <small>(호스트 정보 입력 *호스트명은 한글과 특수문자를 사용하지할 수 없습니다. 단, "." 또는 "-"는 사용가능)</small>
1차 로그인	계정명: <input type="text"/> 패스워드: <input type="password"/> 확인: <input type="password"/> <small>(1차 로그인 계정 정보 입력)</small>
2차 로그인	계정명: <input type="text"/> 패스워드: <input type="password"/> 확인: <input type="password"/> <small>(2차 로그인 계정 정보 입력)</small>
계정 기본값 설정	<input type="button" value="계정 기본값 설정"/> <small>(생성될 계정의 기본값 설정)</small>
숨인 정보	서버그룹: <input type="text"/> 어플리케이션: <input type="text"/> <small>(서버그룹과 어플리케이션을 선택)</small>
다운로드 정보	프로토콜: <input type="text"/> 인종: <input type="text"/> 포트: <input type="text"/> 도메인: <input type="text"/> <small>(계정 다운로드 프로토콜/포트 및 도메인 입력)</small>

사용자 정책 추가	
호스트	<input type="text"/> <input type="button" value="중복확인"/>
사용자ID(+)	<input type="text"/> <small>(사용자 ID 입력)</small>
사용자명(+)	<input type="text"/> <input type="checkbox"/> 다음 로그인시 패스워드 변경 사용함 <small>(사용자명 입력 및 패스워드 변경 설정)</small>
기본	기본허용프로토콜 <input type="checkbox"/> TELNET <input type="checkbox"/> RLOGIN <input type="checkbox"/> RSH <input type="checkbox"/> FTP <input type="checkbox"/> SSH <input type="checkbox"/> SFTP <input type="checkbox"/> WINDOWS <input type="checkbox"/> WEB <input type="checkbox"/> MAINFRAME <small>(허용할 프로토콜을 선택해주세요)</small>
명령어 통제	<input type="text"/> <small>(실행 제한할 명령어를 적어주세요)</small>
명령어 결과 통제	<input type="text"/> <small>(실행 결과를 제한할 명령어를 적어주세요)</small>
감사설정	<input type="text"/> ALL <input type="text"/> <small>(감시 유형을 선택해 주세요)</small>
OTP	<input type="checkbox"/> WEB <input type="checkbox"/> SERVER (OTP인증 사용 옵션을 선택해 주세요)
접근기간	시작날짜: 0000-00-00 00:00:00 종료날짜: 0000-00-00 23:59:59 <input type="button" value="초기화"/> <small>(접근 허용 기간을 설정해 주세요)</small>
요일설정	<input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun <small>(로그인 허용할 요일을 선택해주세요)</small>
설명	<input type="text"/> <small>(설명을 적어주세요)</small>

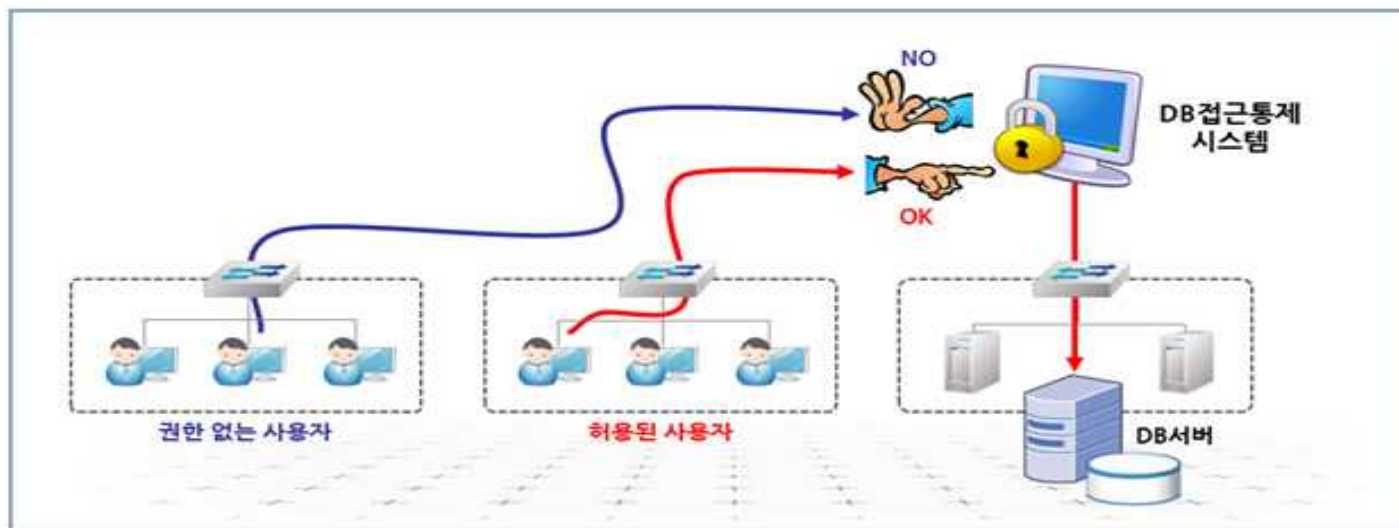
Ⅲ. 데이터 유출방지체계 구축사례 -DB 접근제어

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
- 과도한 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

The screenshot displays a comprehensive wireless LAN monitoring dashboard. On the left, there are navigation menus for '센서' (Sensors) and 'AP' (Access Points) with status indicators for '인가' (Authorized) and '미분류' (Unclassified). The main area features several charts: a bar chart for '보안위협 이벤트 분포' (Security Threat Event Distribution) showing counts for Rogue (102), Soft AP (17), 해킹 Device (11), and Mobile AP (4); a 'Signature 이벤트 분포' (Signature Event Distribution) chart showing 3 events for Broadcast Deauthentication; and a '장치 관리' (Device Management) table listing detected APs with columns for AP Type, Name, MAC, SSID, IP, Security, Protocol, Channel, Location, and Last Activity. A context menu is open over the table, showing options like '수정' (Edit), '삭제' (Delete), and 'AP종류 변경' (Change AP Type). Below the table, there are three bar charts: '내보내기' (Export) showing counts for In-branch, Temporary, Rogue, External, and Unclassified AP types; '보안규격' (Security Standard) showing counts for NONE, OPEN, WEP, WPA, and WPA2; and '프로토콜' (Protocol) showing counts for 'a', 'b', 'b/g', and 'b/g/n'.

Ⅲ. 데이터 유출방지체계 구축사례 -네트워크 접근통제



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

The screenshot shows a web-based management interface for network access control. The main area displays the configuration for a '단말무결성 정책' (Endpoint Integrity Policy). A dropdown menu for '템플릿' (Template) is open, listing various security software templates such as 'System보안', 'PMS', 'PC보안', '자산관리', 'Window보안', 'DRM', 'VMS', and '기타'. The 'VMS' option is currently selected. The interface also shows a list of ACL rules on the left and a '기본 설정' (Basic Settings) button in the top right.

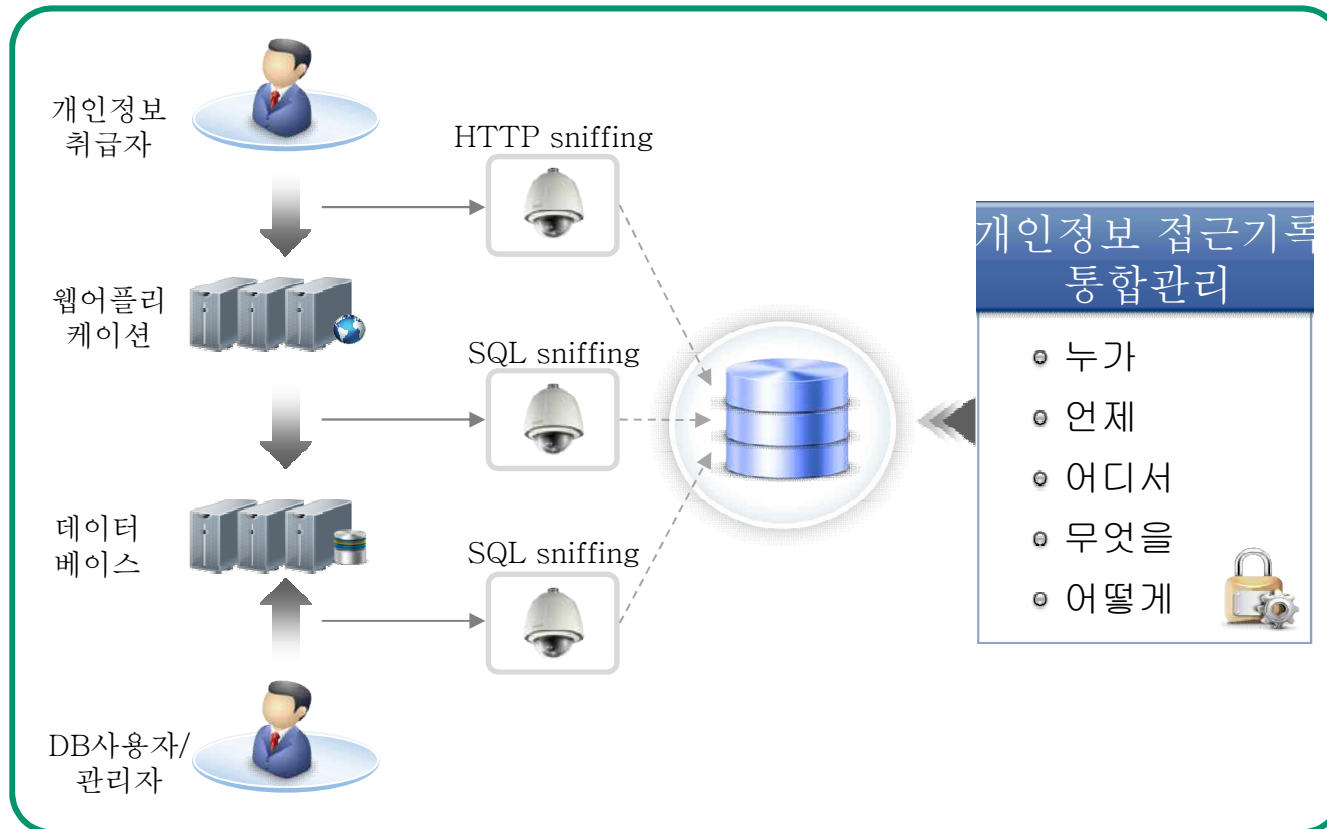
III. 데이터 유출방지체계 구축사례 - DB개인정보 모니터링



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





DB개인정보 모니터링(4)-자동화 감사

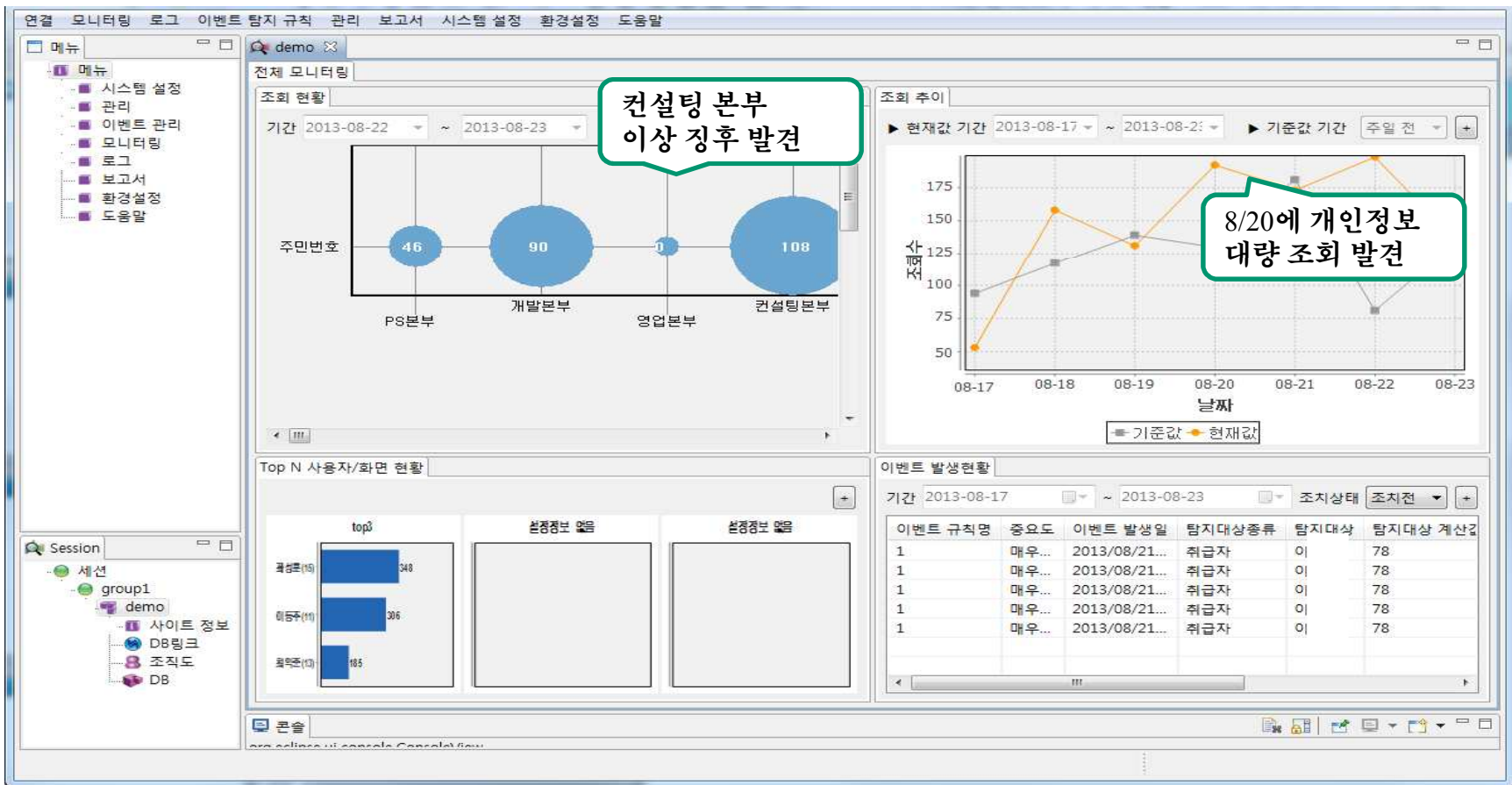
• 감사 시나리오





DB개인정보 모니터링(4)-자동화 감사

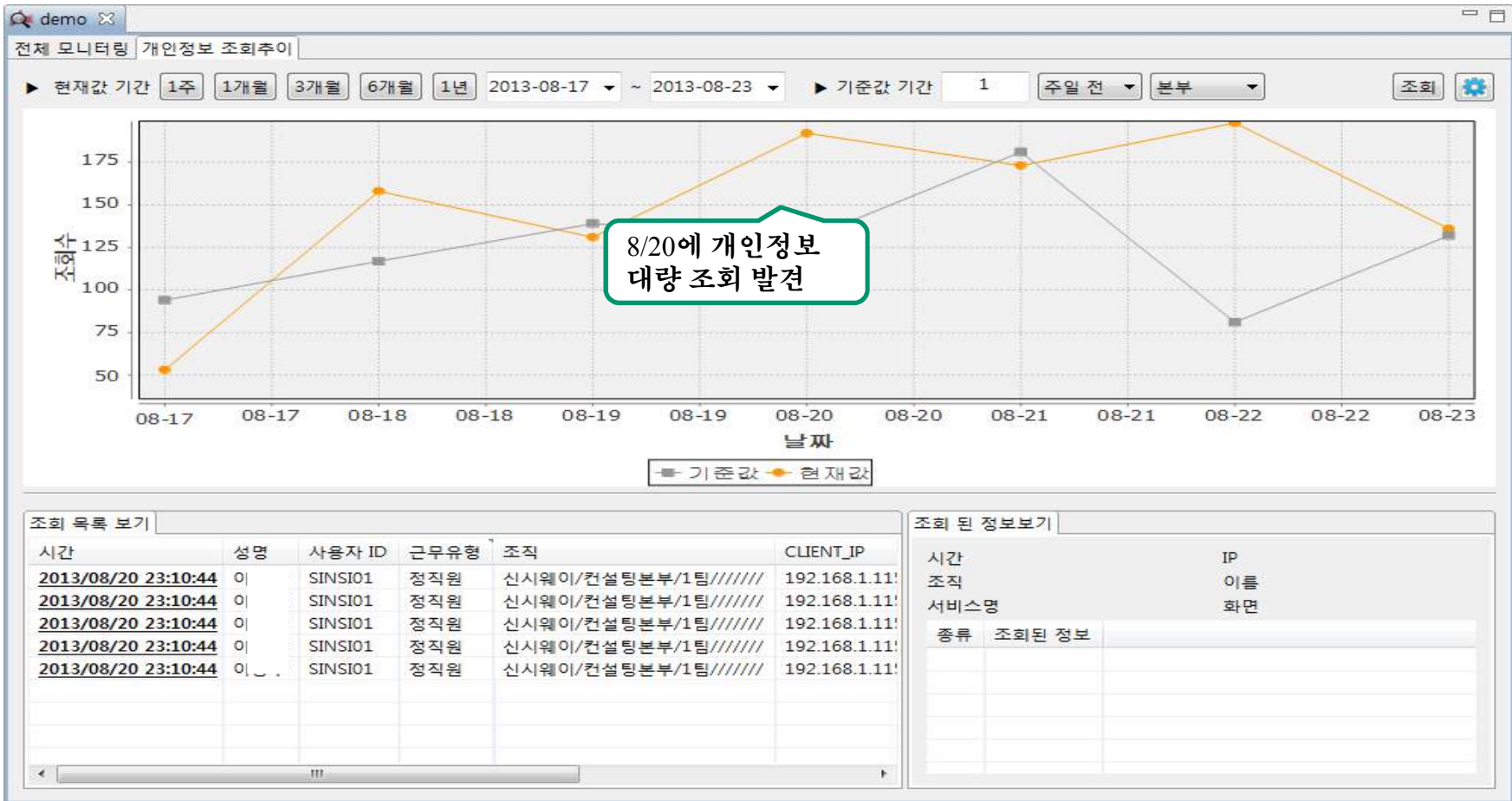
- 이상징후 발견





DB개인정보 모니터링(4)-자동화 감사

- 추이 확인





DB개인정보 모니터링(4)-자동화 감사

- 자동화 감사

이벤트 탐지현황

기간 **1일** 1주 1개월 3개월 6개월 1년 2013-08-16 ~ 2013-08-23 조치상태 조치전 잔여조회

이...	중요도	이벤트 발생일	탐지대상종류	탐지대상	탐지대상 계산값	비교대상값	이벤트 내용	조치상태	조치내용
1	매우 높음	2013/08/20 13:10:32	취급자	이	78	48			
1	매우 높음	2013/08/20 12:20:21	취급자	이	78	48			
1	매우 높음	2013/08/20 10:24:12	취급자	이	78	48			
1	매우 높음	2013/08/20 10:23:23	취급자	이	78	48			
1	매우 높음	2013/08/20 09:32:11	취급자	이	78	48			

8/20 10:24:12에 이○○ 취급자가 개인정보 대량조회 발견

조회 목록 보기

시간	성명	사용자 ID	근무유형	조직	CLIENT_IP

조회된 정보보기

시간	IP
조직	이름
서비스명	화면
종류	조회된 정보

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)



감사합니다.

