KOREA FOUNDATION 한국국제교류재단

외주인력 보안 위협 및 모니터링 강화 방안

2014. 09

KOREA FOUNDATION 한국국제교류재단 정보화지원팀 최재완

목차

I. 한국국제교류재단 소개

1. 재단소개
2. 주요사업

재단소개

- ✓ **설립근거 :** 한국국제교류재단법(법률 제4414호) 1991.12.14 제정
- ✓ **설립목적 :** 대한민국과 외국간의 각종 교류사업을 통해 **국제사회에서 한국에 대한 올바른 인식과 이해를 도모하고 국제적 우호친선을 증진**(한국국제교류재단법 제1조)
- ✓ 재단이 하는 일

  국제교류를 목적으로 하는 각종 **행사의 주관·지원 및 참가**
  국제교류를 목적으로 하는 **인사의 파견 및 초청**
  국외 한국연구의 지원 및 연구결과 보급
  국제사회에서의 한국에 대한 올바른 인식과 이해를 도모하기 위한 활동
  외국의 주요 **국제교류기관과의 교류·협력**을 통한 국제적 우호친선의 증진

주요사업

한국학

세계 대학에 한국학 교육 인프라를 구축
차세대 한국전문가를 양성, 대한민국을
국제사회에 널리 알립니다

문화교류

해외 유수 박물관에 한국실을 설치하고, 공연,
전시, Korea Festival을 개최하여 세계인에게
한국문화예술을 알리며, KF문화센터를 통해
한국과 세계의 쌍방향 문화교류를 추진합니다.

공공외교

세계 각국과의 다양한 형태의 인적(人的),
지적(知的) 교류를 통해 글로벌 지식공동체를
만들어갑니다

출판&영상

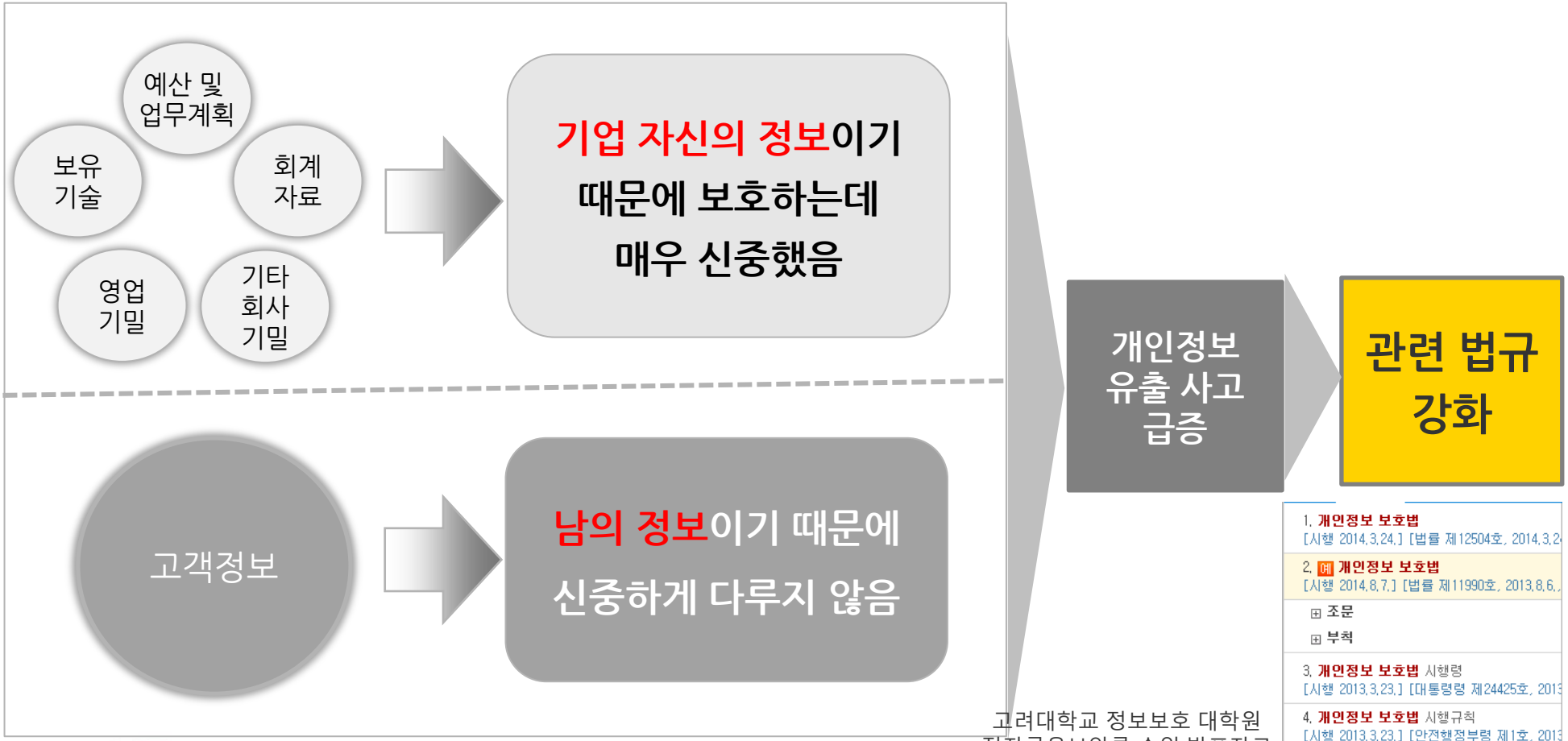
각종 출판물과 영상물로 대한민국을 전하며,
해외대학은 물론 도서관, 연구기관 등에 한국
관련 도서, 시청각 자료 지원을 통해 한국에
대한 이해와 심도 깊은 한국연구를 지원합니다.

II. 외주인력 보안위협 및 사고 사례

1. IT 외주용역 보안위협
2. 개인정보보호법 위탁 관련 사항

왜 개인정보가 보호되지 않을까?

기업은 기업 자신의 정보보호에는 매우 신중한 반면, 고객정보는 보호해야 할 정보가 아닌, 이용해야 할(마케팅 활용) 정보라는 생각으로 신중하게 다뤄지지 않음



고려대학교 정보보호 대학원
전자금융보안론 수업 발표자료

개인정보보호의 문화적 접근

흥미롭게도 미국/유럽 등 서양 기업과 한국/중국 등 아시아 기업의 개인정보 유출 양상은 명백한 차이가 있음

서양 기업 (Ex. 미국 / 유럽)

서버(HW), 운영체제(SW)의 보안 취약점을 통해
해커가 침입하는 시스템적 문제

"내부 직원이 개인정보를 빼돌릴 수 있다는 점을 인지➔ 대비"

문화적 접근 차이

"설마 직원이 개인정보를 빼돌리겠어라고 안이하게 대처"

시스템 문제와 함께 내부직원이 개인정보를
유출시키는 사람의 문제 (80% 이상)

아시아 기업 (Ex. 한국 / 중국)

핵심은 **人災!!**

"내부인가자도 의심하고 모니터링하자!"

주민번호번호 개선 방안

개선방안 원칙 : 개인정보호의 강화, 개편에 따른 비용 최소화, 국민불편 최소화
※ 정부, 민간, 학계에서는 현행 주민번호 체계를 보완하는 '보수적 개선책 ' 에 동의

주민번호 6개 개선안

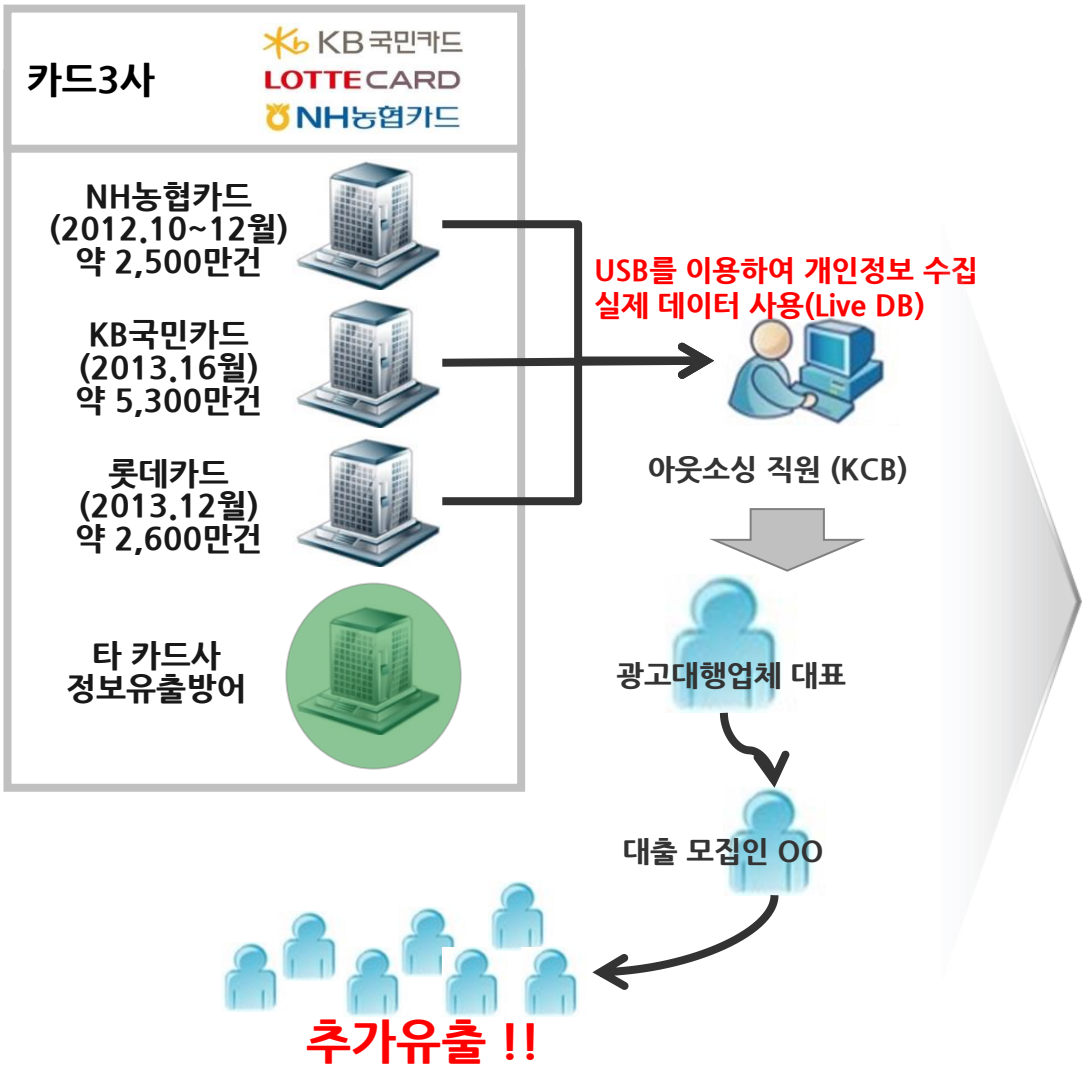
- 규칙성 신규 주민번호
- 무작위 신규 주민번호
- 현재 주민번호 + 주민증 발행번호
- 신규 주민번호 + 주민증 발행번호
- 규칙성 발행번호
- 무작위 발행번호

- 현재와 같은 주민증을 새로 발급하는 데는 약 1600억원
- 전자증 형태로 발급 약 2700억원
- 주민등록 행정 시스템 변경에도 3100억~4000억원이 소요될 것으로 추정

검토대안별 장단점 분석

구분	내용
〈대안1〉 신규 주민번호 (규칙번호) 방식	현재 주민번호를 생년월 정보를 포함한 신규 주민번호로 단계적으로 일괄 교체
	장점:기 유출된 주민번호로 인한 국민 불안감 해소 가능, 실생활에서 나이확인 편의 (경로우대, 청소년 보호 등)
	단점:향후 유출될 경우 현재와 동일한 문제 발생, 번호에 일부 개인정보 포
〈대안2〉 신규 주민번호 (무작위번호) 방식	현재 주민번호를 신규 무작위 번호로 단계적으로 일괄 교체
	장점:기 유출된 주민번호로 인한 국민 불안감 해소 가능
	단점:향후 유출될 경우 현재와 동일한 문제 발생
〈대안3〉 현 주민번호 + 증 번호 방식	현재 주민번호를 관리번호로 유지하되 증에 주민번호 대신 증 번호를 기재하여 상용번호로 활용
	장점:민간분야 유출사고가 발생해도 주민번호 보호 가능, 체계 변경에 따른 사회적 불편 및 혼란 최소화 가능
	단점:기 유출로 인한 국민 불안감 해소 미흡
〈대안4〉 신규 주민번호 + 증 번호 방식	현재 주민번호를 신규 주민번호로 단계적으로 일괄 교체하되 증에 주민번호 대신 증 번호를 기재하여 상용번호로 활용
	장점:기 유출된 주민번호로 인한 국민 불안감 해소 가능, 향후 민간분야 유출사고가 발생해도 주민번호 보호 가능
	단점:가장 많은 비용과 사회적 불편 발생
〈대안5〉 발행번호 단독 (규칙번호) 방식	주민번호는 폐기 또는 주민등록표에만 기재(주민등록 업무용도로만 이용)하고 생년월 정보를 포함한 증 번호의 단독 활용
	장점:기 유출된 주민번호로 인한 국민 불안감 해소 가능, 나이 등 본인 확인절차 간소
	단점:수시 재발급에 따른 신분위장 등 사회적 혼란 우려
〈대안6〉 발행번호 단독 (무작위번호) 방식	주민번호는 폐기 또는 주민등록표에만 기재(주민등록 업무용도로만 이용)하고 주민증에 증 번호 기재·활용
	장점:기 유출된 주민번호로 인한 국민 불안감 해소 가능, 향후 민간분야 유출사고가 발생해도 희망자 재발급 용이
	단점:수시 재발급에 따른 신분위장 등 사회적 혼란 우려

사고 사례 〉 외주용역직원에 의한 개인정보 대량유출



시사점

- 외부인의 USB 사용 차단 부재
- 개인정보 실데이터를 테스트데이터로 사용 ➔ 외주 용역에 제공
- 외주용역 PC내 개인정보 보유 현황 및 개인정보 이용현황 관리 부재

아웃소싱(수탁사) PC 상 개인정보를 보유하고, USB 이용한 것 등을 이상행위로 알 수 있었다면?

고려대학교 정보보호 대학원
전자금융보안론 수업 발표자료

사고 사례 > 외주용역직원에 의한 개인정보 대량유출

개인정보 보호법 기준 - 위반 사항

[개인정보 보호법]

수탁자 관리감독 소홀	파견직원 업무수행 시, 카드사 담당 직원 감시 부재	제26조(업무위탁에 따른 개인정보의 처리 제한)
파기 미수행	탈퇴 회원의 고객정보 파기 미수행	제21조(개인정보의 파기)
암호화 미수행	테스트서버의 고객정보 암호화 미수행	제29조(안전조치의무)
매체제어 미수행	외부인의 USB사용 차단 미수행 보안USB 미사용	제29조(안전조치의무)
가상정보 미사용	프로그램 개발을 위해 필요한 가상정보(테스트 Data) 미제공 고객 개인정보 접근 가능성 차단 미수행	제29조(안전조치의무)
모니터링 미흡	주기적인 모니터링을 통한 **개인정보 유출사실 확인 미흡**	제29조(안전조치의무)

IT 외주인력 보안통제 현황

최근 기업의 보안사고는 "기술적 문제보다 관리적 측면의 인재가 많다."
(유지보수 업무를 수행하는 유형에 따라서 모든 IT 자원에 대한 접근이 가능하고 그에 따른 권한을 받음)

- 최근 정보통신서비스의 일반화로 인해 다양한 산업 및 서비스 분야의 기반 환경이 정보시스템을 기반으로 운영
- 외주 용역의 활용 증가

- 외주인력을 포함한 내부자에 의한 정보유출 및 보안사고 급증)
  (기업의 보안시스템은 외부자 공격대응 위주로 구축)
- 외주용역에 참여하고 있는 인력에 대한 적절한 기술적 · 관리적 보안대책 부재
- 내부인력 통제 관리부실이 원인이 된 기업의 막대한 피해 사례
  (농협, 네이트 개인정보 해킹 등)

시사점

- IT 외주인력 보안통제를 위한 필수 보호대책의 필요성
- 외주 용역 유형별 적용 가능한 기술적 · 관리적 대응방안 필요
- 외주용역 PC내 개인정보 보유 현황 및 개인정보 이용현황 관리 부재

기업이 수행하고자 하는 외주용역의 유형을 판단하여, 기술적 · 관리적 보호 대책을 선택적으로 적용
(KISA, IT외주인력 보안통제 안내서)

IT 외주인력 분류 및 특성

IT 자원, 자원 사용권한, 접근 경로에 따른 유형 정의(KISA, IT외주인력 보안통제 안내서)

- 재단 유지보수 상주 및 홈페이지 등은 유형 1,2 에 해당

IT 외부용역 유형		용역 특성				
		접근 IT 자원		자원 사용 권한		접근경로
1 유형1	운영 용역	내부 데이터	○	읽기	○	온라인
		IT 시스템	○	쓰기	○	
2 유형2	유지보수 용역	내부 데이터	○	읽기 (내부직원 동행)	× (○)	온라인
		IT 시스템	○	쓰기 (내부직원 동행)	× (○)	
유형3	SI 용역	내부 데이터	○	읽기	○	온라인
		IT 시스템	○	쓰기	×	
유형4	데이터 처리 용역	내부 데이터	○	읽기	○	온라인
		IT 시스템	×	쓰기	×	
유형5	오프라인 지원	내부 데이터	○	읽기	○	오프라인
		IT 시스템	×	쓰기	×	

IT 외주인력 사고사례 및 보안위협

외주용역을 활용하여 시스템을 운영하는 기업 중 외주용역 기관의 과실 등의 이유로 정보유출 등의 사고가 발생한 주요사례

일시	위치(기업)	유출 피해건수	시스템 운영방법	정보유출 방법
'10.9	OO교육 관리기관	630만명	외주업체에서 시스템 전반을 위탁 관리	서버 유지보수 업체 직원이 서버에 해킹 프로그램을 설치해 개인정보를 빼돌림
'11.3	OO캐피탈	175만명	외주업체에서 보안업무 위탁관리	업무성격상 불필요한 권한 부여 및 퇴직자 계정 정보 미삭제 등의 시스템 접근권한관리 미흡
'11.4	OO은행	—	외주업체에서 서버관리	외주업체 직원 노트북을 통한 해킹으로 전산망 마비
'11.5	OO증권사	2.7만명	외주업체에서 전산망 관리	외주업체에서 공격 탐지 후 모기업에 알렸으나, 안일하게 대처
'11.9	OO 국가기관	92만명	전자여권 발급기 시스템 운영을 외주업체에 맡김	여권발급기 부품교체 주기를 파악한다는 명목으로 신상정보를 매주 본사로 보내 여권발급에 필요한 개인의 신상정보가 무단으로 유출
'11.9	OO구청	60만명	구청 호적등본 자료의 전산화 작업을 외주업체에 맡김	문서고에서 호적등본을 전산화하는 과정에서 외주업체 직원이 주민정보를 스캔한 파일이 저장된 외장하드를 분실

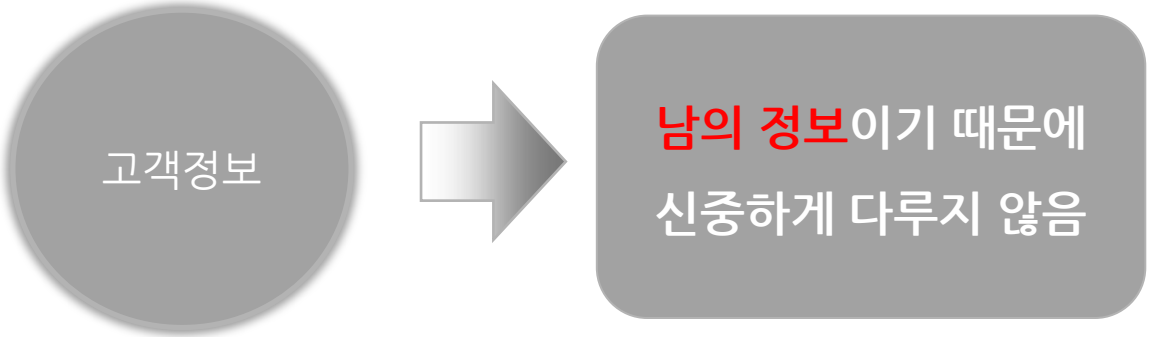
IT 자원 운영 용역(유형1)

- **유형1** - 기업내의 IT 자원을 운영하는 외주용역을 위탁하는 경우

❖ 업무지원시스템 운영 또는 네트워크 및 보안장비 운영 시 업무망에 대한 **온라인 접속권한을 이용하여 개인정보 탈취 및 보안설정을 우회 가능**

❖ **보안위협**

- 업무목적 이외의 기업 내부정보를 열람, 쓰기 권한을 사용하여 기업내부의 정보를 조작, 외부유출
- 백도어 구축 또는 해킹 프로그램 설치를 통해 무단으로 정보 유출
- 보안관리 업무 수행 시, 의도/비의도적인 보안 공격에 의해 업무망 마비 또는 데이터 손실



- 업무망 내 IT 시스템 네트워크 및 보안장비 운영
- 기업 내부망에 대한 취약점 점검 및 모의해킹

IT 외주용역 유형별 사고사례

보안위협1) IT 외주용역 수행자의 기업내부 정보 조작

◆ **사고개요**

- 포털게임 업체 A사의 고객 정보관련 DB업무를 위탁 관리하고 있는 외주용역 업체 직원이 업무 외의 목적으로 고객정보를 열람하고 조작 및 로그 등을 삭제하는 행위

- DB 접근권한을 이용하여 회원들의 게임머니를 조작하고 로그를 삭제하여 1억원 상당의 부당이득을 얻음

고객정보를 다루는 외주업체 직원의 보안의식 미흡 및 외주용역 지원의 행위에 대한 감사기능 미비

보안위협2) 외주직원의 보안관리 업무수행 시, 의도/비의도적인 공격

◆ **사고개요**

- OO기관은 보안관리를 위해 A보안 업체와 취약점 점검 및 모의해킹을 의뢰하여 업무 종료 후 작업에 들어갔으나 알 수 없는 악성코드로 인해 작업이 지연되어 전산망 문제 발생

- 취약점 점검 툴 설치 전 보안업체 직원의 USB 이용하였으나 이를 통해 전산망에 악성코드가 감염됨

외부에서 반입된 인가되지 않은 USB의 사용과 같이, 이동저장매체에 대한 관리적 · 기술적 통제대책 미흡

IT 외주용역 유형별 사고사례

보안위협3) IT 외주용역 수행자의 보안관리 업무 수행 시, 의도/비 의도적인 보안 공격

◆ **사고개요**

- 원격 취약점 점검 모의해킹 수행하는 외주용역 직원의 PC가 DOS공격과 관련된 악성코드에 감염되어 있었고, 원격 접속된 OO기관 시스템에도 퍼져 좀비PC로 이용
- 특정IP로 과도한 요청을 지속적으로 전송하여 OO기관 시스템에 장애가 발생함

외주직원의 보안의식 및 원격접속된 PC에 대한 관리 소홀

보안위협4)IT외주용역 업체 내 'IT 자원 접근권한이 없는자'에 의한 기업 내부정보 무단 열람 및 유출

◆ **사고개요**

- OO기관 시스템 운영업무를 담당하는 외주업체 직원이 특정인의 개인정보를 업무목적과는 다른 용도로 열람, 제3자에게 제공함

- **외주용역 지원의 기업 내 온라인 접속 및 개인정보 DB 접속 권한에 대한 통제 미흡**
- **직원의 업무목적과는 다른 용도로 열람한 사실은 개인정보취급자가 권한 없이 처리하지 못하도록 되어있는 법률에 위반**

IT 외주용역 유형별 사고사례

보안위협5) IT 외주용역 업체 내 취약한 IT 시스템에 의한 기업 내 IT 시스템의 감염 위협

◆ **사고개요**

- OO은행 전산 장애로 청구거래 등 전반적인 금융서비스가 마비된 사건이 발생하여 은행 고객의 카드 결제, 교통카드 사용, 체크카드 사용 내역 조회 등에 불편함을 겪음
- OO은행 서버관리 협력업체인 @@기업 직원의 노트북을 통해 OO은행 서버에 삭제명령이 입력된(경제적 피해 최소 80억원 규모로 추정)

금감원 감사 결과 시스템 계정의 비밀번호 변경관리 부실 외주직원의 보안인식 및 관리감독 소홀, 접근관리 미흡, 보유 노트북의 저장매체 관리에 대한 통제 미흡

보안위협6) IT외주용역 수행자에 의한 기업IT시스템 설정변경 및 시스템 정보유출

◆ **사고개요**

- OO업체에서 서비스 운영을 담당하던 외주업체 직원이 원격으로 관리자 권한을 부여 받아 업무를 수행하고 있으며, 고객들의 개인정보를 몰래 자신의 PC로 전송하여, 이를 대부업계에 팔아 넘김

외주직원의 핵심정보에 대한 원격접근 허용 및 관리적 · 기술적 통제대책 수립, 감사기능 미흡

IT 자원 운영 용역(유형2)

- **유형2 - 시스템과 내부 데이터 모두 접근할 수 있는 권한을 가지고 있으나 내부 직원과 동행 시에는 해당자원에 대한 읽기 및 쓰기 권한을 획득할 수 있는 경우**

❖ IT시스템 접근 권한이 제대로 관리되지 않는 경우, 보안인식이 미흡하거나 사적인 목적달성을 위하여 IT 시스템 접근권한을 소유한 IT 외주용역 수행자가 기업 **내부 IT시스템에 무분별하게 접근하여 시스템을 설정 변경 및 시스템 내 정보 유출 가능**

❖ **보안위협**

- 업무망 온라인 접속 권한으로 수행된 용역 업무에 대한 유지보수
- 기업 내 온라인으로 진행되는 IT 시스템 네트워크 및 보안 장비 유지보수
- 원격 시스템 네트워크 보안 장비 유지보수, 원격 유지보수 및 장애관리

고객이 안보기 때문에
신중하게 다루지 않음

- '눈에서 멀어지면 마음도 멀어진다.'
- 외주용역 직원에 의한 기업 내부 시스템 접근은 책임자 승인 하에 담당직원과 함께 조회, 외주직원의 무분별한 접근에 대한 관리적 · 기술적 통제대책 수립 및 감사기능 미흡

IT 외주용역 유형별 사고사례(유형2)

보안위협1) 업무 목적 외 기업 내부정보 열람, 외부유출
(OO기관 외주업체 직원에게 승인 없이 개인정보 열람 허용(2008.10))

◆ **사고개요**

- 서버 유지보수 업체 직원 등 IT업체 대표와 개발자 등이 OO기관이 관리하는 전자도서관 서버에 해킹 프로그램을 설치해 학생들의 개인정보를 탈취하고, 이를 독서통장 사업자에게 팔아 부당이득을 챙김
- 전자도서관 서버에 대한 유지보수를 위탁 받은 외주업체 직원들은 서버 점검 시 방화벽이 해체된 틈을 타 불법 프로그램을 설치하여 개인정보를 유출

유지보수 업체 직원에 대한 관리감독 및 기술적인 통제 부족

보안위협2) 업무 목적 외 기업 내부정보 열람, 외부유출
(전자여권 92만명 정보유출(2011.09)

◆ **사고개요**

- 전자여권 신청자의 주민번호와 여권번호 등 개인 신상정보 92만 여건이 여권 발급기 운용업체 직원들에 의해 무단 유출

- 여권 신상자의 신상정보는 여권제작 후 조폐공사 전사서버에서 삭제되어야 하지만, 해당 외주자 직원들은 여권발급기 부품 교체주기를 파악한다는 명목으로 신상정보를 매주 본사로 전송

- **외주직원에 대한 보안의식 교육 및 관리감독이 미흡함**
- **기관의 보안규정에 맞게 개인정보 데이터가 제대로 관리되지 않음**

IT 외주용역 유형별 사고사례(유형2)

보안위협3) 외주직원의 업무 목적 외 기업 내부정보 열람 및 변조, 외부유출 (외주직원, 서버 접근계정 공유하여 부당이득 취득)

◆ **사고개요**

- A업체 서버 유지보수를 담당하고 있는 외주업체 직원이 A업체에 상주하지 않고 본사에서 원격으로 A업체 서버에 접근하기 위한 계정을 소유함
- 외주직원은 A업체 서버에 접근하기 위한 관지라 계정을 제3자에게 유출하여 A업체 서버 내 정보가 유출되고, 서버접근 계정을 공유한 대가로 부당이득을 취함

외주용역 직원에 대한 관리자 계정, 암호 공유 및 원격접속 허용 등 적절한 시스템 접속 권한 관리 미흡

보안위협4) 외주용역 직원에 의한 기업IT 시스템 설정 변경 및 시스템 내 정보 유출
(시스템 유지보수 직원이 백도어 설치.. 외부로 개인정보 유출)

◆ **사고개요**

- 외주용역 업체 직원이 전산망 구조도와 개인정보가 저장된 서버의 관리자 권한을 소유한 업체 직원이 내부 담당자에게 악성코드가 포함된 이메일을 전송, 메일을 열어본 내부 담당자의 PC에 백도어가 설치됨
- 설치된 백도어를 이용하여 외주 직원은 외부의 특정서버로 개인정보 전송

- **외주용역 직원에 대한 신원조회, 보안교육 등 관리가 소홀하며, 이메일에 대한 보안통제 대책 미흡**

IT 외주용역관련 - 개인정보보호법 사항

재단은 위탁사업자에 대한 관리감독의 책임, 위탁사업자는 유지보수 업체에 대한 관리감독의 책임을 갖는다.

〈안전행정부 개인정보관리실태 점검표 기준〉

제26조(**업무위탁**에 따른 처리 제한)	27. 위탁 계약 시 문서(계약서)에 의한 계약 여부
	28. 문서(**계약서**)에 필수 반영사항(6개*) 포함 여부 * 6개 : **목적외 처리금지, 기술·관리적 보호조치, 목적·범위, 재위탁 제한, 접근제한 등 안전조치, 관리·감독사항**
	29. 수탁자에 대한 **교육** 실시 여부
	30. 처리현황 점검 등 수탁자 **관리·감독 여부**
제28조(개인정보취급자에 대한 **감독**)	31. 개인정보취급자에 대한 **관리·감독(접근권한 관리, 통제 등 포함)** 여부
	32. 개인정보취급자에 대한 **보안서약서** 징구 여부
	33. 개인정보취급자에 대한 **정기적인 교육 실시** 여부

III. 데이터베이스 모니터링을 통한 보안강화 방안

1. DB 보안 이슈사항 과 필요성
2. DB 보안 프레임워크
3. 모니터링 정책 및 작업결재

DB 보안 이슈

- 지금까지의 네트워크, 시스템, 어플리케이션 보안만으로는 데이터 보안 전략에 부족

- 최근 정보통신서비스의 일반화로 인해 다양한 산업 및 서비스 분야의 기반 환경이 정보시스템을 기반으로 운영
- 외주 용역의 활용 증가, 부분적 솔루션 도입과 의존성

- 외주인력을 포함한 내부자에 의한 정보유출 및 보안사고 급증)
  (내부자(협력사 포함) 소행의 범죄 및 사고 증가)
- 미흡한 정책, 감시, 관리 소홀
- 보안의식 및 윤리의식 부족
- 방화벽, 네트워크, 시스템 레벨의 침입탐지 시스템(내부망 사용자에게 데이터베이스는 열린 공간)

시사점

- 정보를 보호하기 위해서 네트워크, 시스템, 어플리케이션 등의 보안에 집중
- 민감한 데이터가 집중되어 있는 DB에 대해서는 상대적으로 보호 정책 취약
- 강화된 법규의 적용

데이터보호를 위한 견고하고 체계적인 심층방어 전략이 필요
의식이 바뀌지 않으면 무용지물

DB 보안의 필요성

DB 정보보호에 대한 컴플라이언스
- 개인정보보호법(2011.9.30 시행)
- Sarbanes-Oxley Acts(2002년)

내부자에 의한 정보유출 및 보안사고
- 협력업체 및 내부개발자에 대한 관리 미흡
- 보안사고 중 내부자에 의한 정보유출 사고 비율 증가(70~80% 이상)

개인정보 유출에 따른 사회적 비용
- 보안사고 발생 시 피해 복구, 소송 등 비용발생으로 인한 Risk 관리 필요
- 피해규모 확대와 빠른 확산 속도

데이터 자산가치 증가
- 정보자산이 기업의 생존과 직결
- 데이터에 대한 방어는 상대적으로 취약

전통적 IT 보안체계의 취약성
- OS, Network, 시스템 중심의 탐지 및 모니터링에 치중
- 관리적인 보안체계 정비 필요

어플리케이션 구축 및 운영 취약점

어플리케이션, 데이터베이스 설계 시 보안 고려 미흡

데이베이스 레벨의 보안 문제 경시

전략적 DB 보안정책 필요성 대두

구분	주요내용	적용 예
관리적 보안 통제 (Administrative Security Controls)	보안 활동에 대한 **정책, 표준, 지침, 기준, 절차** 등을 정의하고 준수하도록 하는 보안관리 활동	보안정책 수립, 보안 교육, 보안점검 및 개선 조치 등
논리적 보안 통제 (Logical Security Controls) 또는 **기술적 보안 통제** (Technical Security Controls)	DB에 발생할 수 있는 보안위협을 파악하고 **보안 통제 시스템을 구축·운영**하는 등의 활동 DBMS 또는 DB 상에 존재하는 **취약점 제거** 등의 활동	**암호화, 접근제어, 감사 및 모니터링, 취약점 분석, 작업결재, 사용자 인증**, 운영/개발/ 테스트 환경의 분리 등
물리적 보안 통제 (Physical Security Controls)	정보자산이 위치한 시설에 대해 허가되지 않은 접근 또는 사용을 차단하고 모니터링하기 위한 물리적 보안관리 활동	시건장치, CCTV, 소화기 등

DB 보안 프레임워크

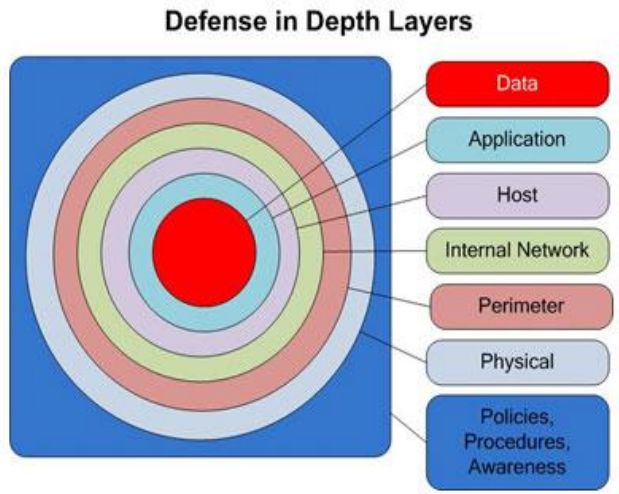
- DB 보안을 체계적이고 효과적으로 구축하여 운영할 수 있는 전문인력의 부재, 실제적이며 효용성 있는 구체적인 DB 보안 구축 가이드라인 필요
- DB 보안을 구축하는데 따른 효과적인 통제 수단과 이들의 구축절차 및 주요 태스크 등을 정리한 것이 DB 보안 프레임워크

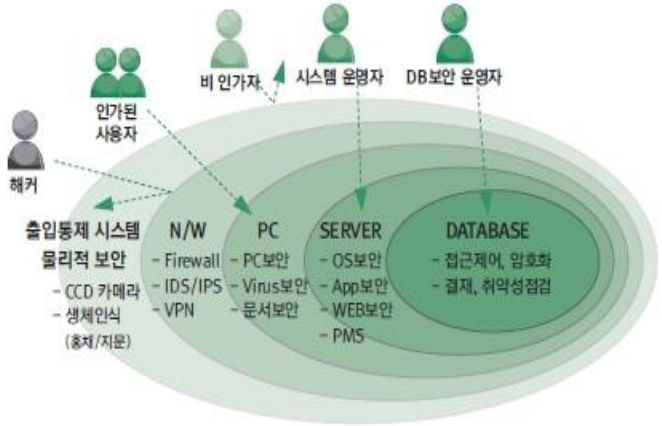
[그림 1-2-1] DB 보안 기술 요소의 도출

DB 보안 - 심층방어(DID) 모델

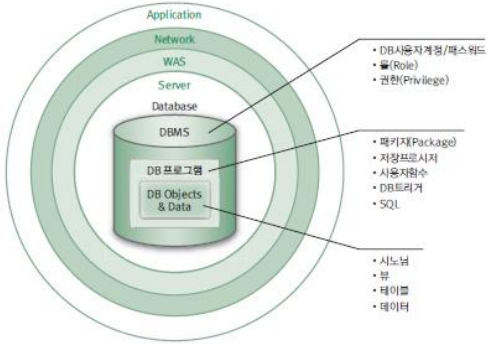
- **DB 보안은 정보보안의 범주에서도 데이터베이스내의 데이터보호에 특화하여 집중**

- DB 접근제어에서 고려해야 할 것은 보안은 **심층방어(Defense-in-Depth)**라는 개념으로 구성해야 한다
- 조직에서 관리하는 모든 정보 기기를 하나의 (Instruction Detection System)/IPS(Instruction Prevention System), PKI, VPN(Virtual Private Network) 등 다양한 솔루션을 통해 여러 겹의 방어막을 구축하여 방어를 한다. 이것은 거시적으로 정보시스템에 대한 방어를 바라보는 관점이지만 DB자체에 대한 보안에도 동일한 개념이 적용되어야 한다.
- DB 보안을 위해 DB 접근제어, DB 암호화, DB 작업결재, DB 취약점 분석 등의 다양한 솔루션을 구축할 수 있는데, 이런 솔루션의 구축과 더불어 **DB 자체에 제공하고 있는 기능을 이용한 보안의 강화도 필수적**이다





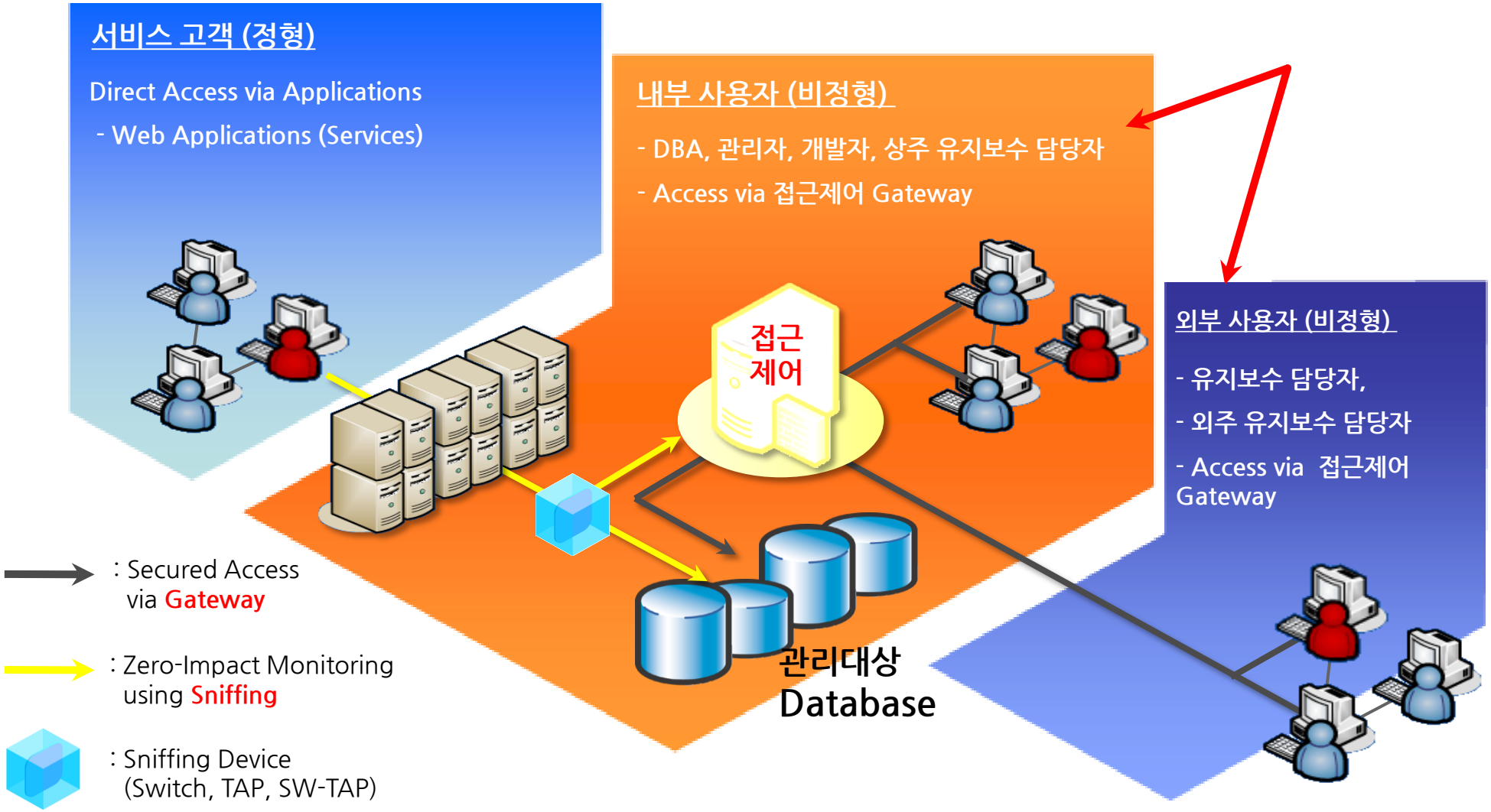
[그림 3-1-1] 보안 시스템 흐름



[그림 1-1-6] 데이터 액세스 흐름 관점에서의 DB 영역 구분

* DQC-S 가이드 참조

모니터링 정책 재단 사례 - DB 접근제어 정책



* DB 접근제어 시스템 구성(HYBRID OPERATION=GATEWAY + SNIFFING)

모니터링 정책 재단 사례 - DB 접근제어 정책

기본적으로 Application 을 제외한 모든 관리자, 개발자는 DB 접속 시 GW(Gateway) 모드로 접속하여 관리가 되며, 주요 정보에 대한 차단 및 감사 정책을 적용하여 사용 중 입니다.

* GW(GateWay 모드), SF(Sniffing 모드)

구분	방안	접근제어 정책	동작방식	제어 범위	정책 분류
접근제어	DB 접근 통제 - 비 인가자의 DB 접근 차단 - DB 접근 실시간 감시, 차단, 추적	등록된 관리자 IP 외에 관리자 계정으로 DB 접속 차단	GW,SF	DB전체	차단
		WAS, WEB 서버 등의 Application 이외 DB 접근차단	SF	DB전체	차단
		DB 내 주요 정보가 속한 TABLE 조회 시 감사	GW, SF	테이블	Alert
		정의된 업무 시간 외 주요 테이블 접근 차단	GW, SF	테이블	X
		주요 테이블 데이터 1천건 이상 조회 감사	GW, SF	테이블	Alert
		주요 개인정보 데이터 100건 이상 조회 감사	GW	테이블	Alert
		DDL 작업 행위 감사	GW,SF	테이블	Alert
		사용자 별 DB 접근 계정 할당(1인 1 ID)	GW	DB 전체	차단
		특정 사용자 Query 차단(Drop, Truncate)	GW	DB 전체	차단
		인가된 DB Tool 외 접근차단(App 서버 제외)	GW	DB 전체	X
		SQL 수행시간 15분 이상 경보	GW	DB 전체	Alert

모니터링 정책 재단 사례 - DB 접근제어 정책

- ❖ 주요 DML, DDL 작업에 대해서는 작업결재를 이용하여 로깅 및 통제, 감시를 수행하고 있습니다.
- ❖ 작업 결재 정책은 단순 DB 작업 내용을 기록하는 것이라, 변경 전/후 데이터의 기록 및 데이터의 형상관리 측면에서도 중요한 관리 Point가 될 수 있습니다.

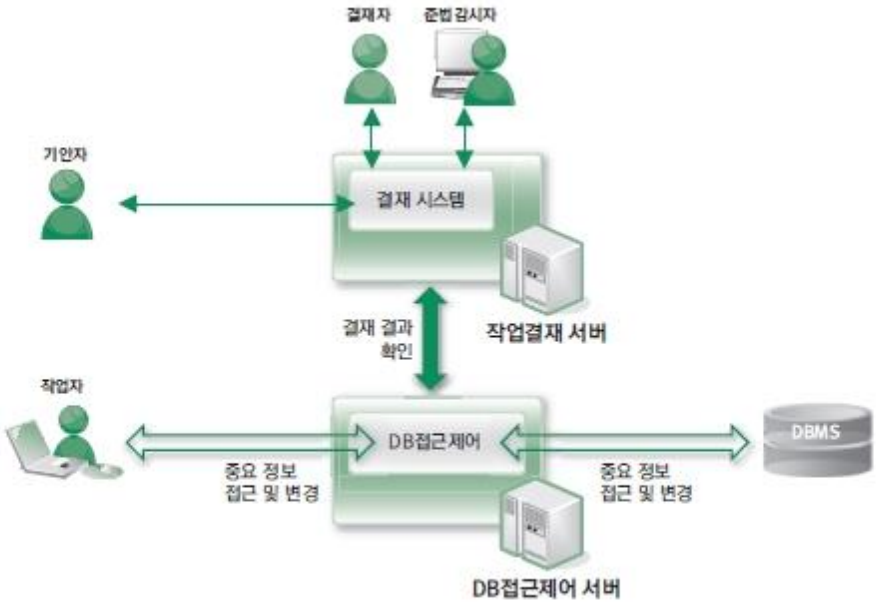
* GW(GateWay 모드), SF(Sniffing 모드)

구분	방안	접근제어 정책	동작방식	제어범위	정책 분류
작업 결재	주요 테이블 조회 시 통보	주요 테이블 데이터 조회 시 사전 결재(업무시간)	GW	테이블	X
		주요 테이블 데이터 조회 시 사후 결재(업무 외 시간)	GW	테이블	X
	DB 데이터 변경 방지	운영 DB DML/PLSQL 작업 시 사전 결재	GW	함수, 프로시저	사전 결재
		운영 DB 데이터 변경 시 사후 결재	GW	테이블	사후 결재
	DB 구조 변경에 대한 통제 방안	운영 DB DDL 작업 시 사전 결재	GW	운영DB	사전 결재
		개발 DB DDL 작업 시 사후 결재	GW	개발DB	X
	사용자에 대한 통제방안	주요 Data Return row 값 Export, Copy 차단	GW	DB 전체	결재
마스킹	중요 개인정보 데이터	개인정보 데이터 컬럼 단위 마스킹 처리	GW	테이블	마스킹
백업	DB 운영자 작업 이력 로깅 - 6개월 이상 보관 - DB 실시간 감시, 차단, alert	고객정보, DB 접근, 정책 위반 이력 접근제어 서버 내 6개월 이상 보관	GW/SF	DB 전체	이력 관리

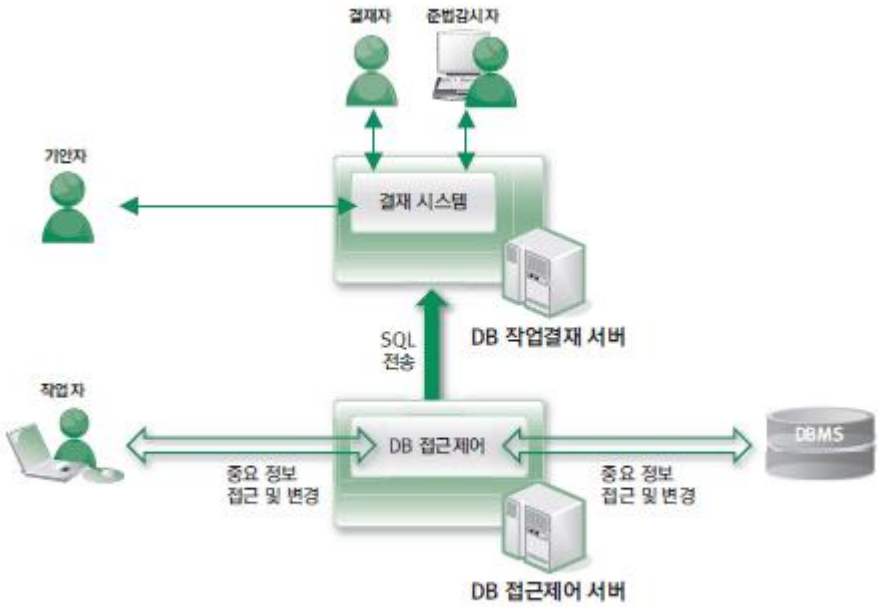
DB 작업결재

- DB 유저의 작업에 따라 결재가 필요한 SQL 명령에 한하여 자동적으로 결재 프로세스를 기동 (사전확인이 필요한 SQL 명령의 경우, 승인자의 허가를 받은 후에만 SQL 명령이 실행)

- 결재 프로세스의 기록, 관리, 휴먼에러 방지 등 관리강화



[그림 3-3-3] 사전 결재 구성



[그림 3-3-7] 사후 결재 구성

* DQC-S 가이드 참조

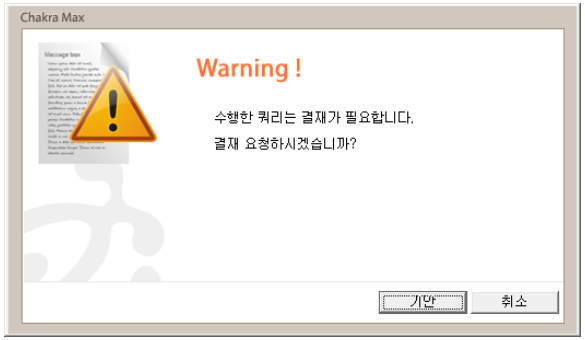
작업결재 Demo - 사후결재

- 운영 DB 의 간단한 데이터 변경 작업
- 사후결재 + 변경 전후 데이터 관리

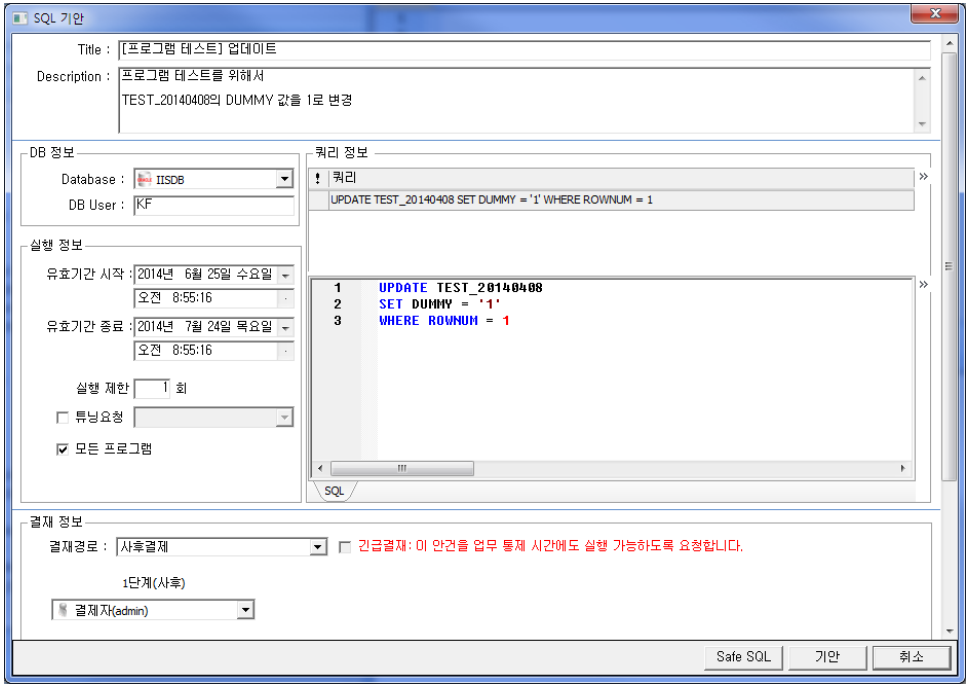
① SQL문으로 데이터 업데이트 작업

```
UPDATE TEST_20140408
SET DUMMY = '1'
WHERE ROWNUM = 1
```

② SQL 문 실행 시 결재창 => 기안선택



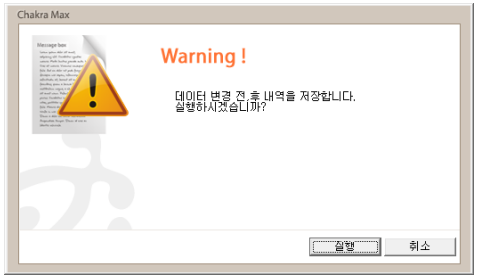
③ SQL 기안 내용 입력 후 기안버튼 클릭
- TITLE : 업무명, 목적 등을 간략히 기술
- Description : SQL 작업 내용을 가능한 상세히 기술 (5W 1H)
- 사후결재는 결제자가 Admin(감시자)으로 고정됨.



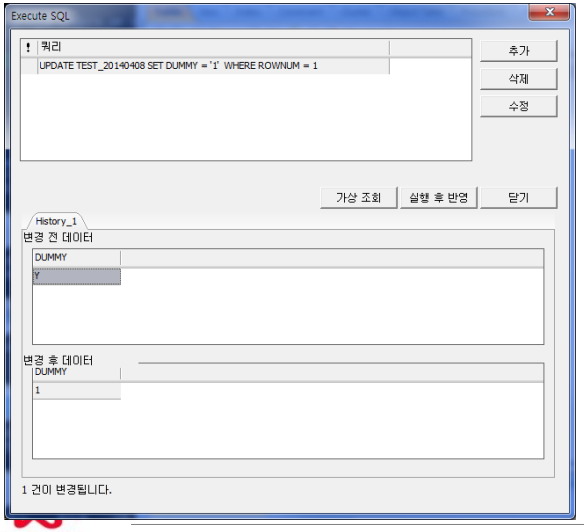
작업결재 Demo - 사후결재

- 운영 DB 의 간단한 데이터 변경 작업
- 사후결재 + 변경 전후 데이터 관리

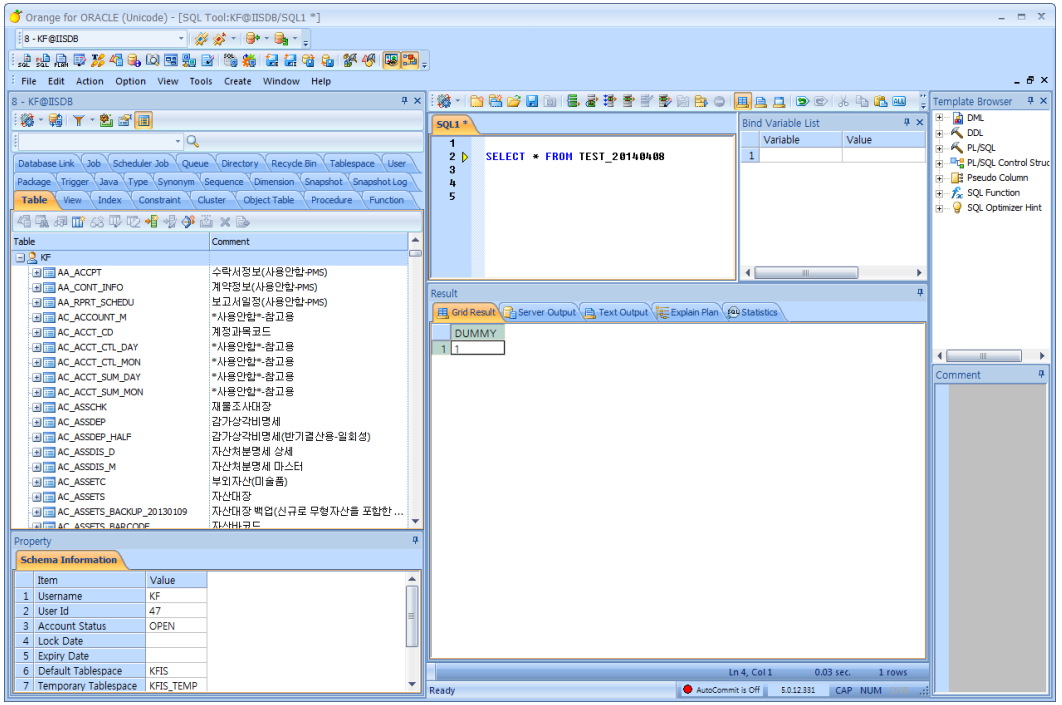
④ SQL문으로 데이터 업데이트 작업



가상조회(변경전 데이터, 변경 후 데이터 확인)



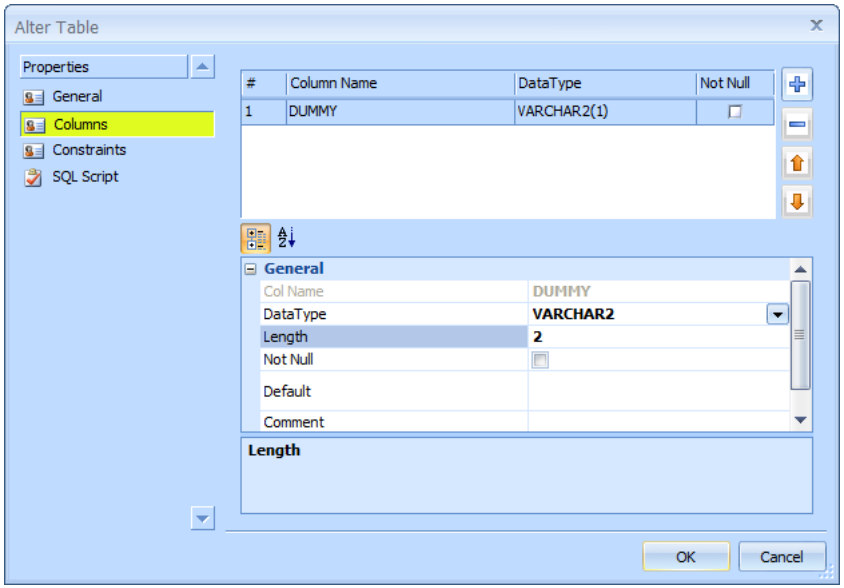
⑤ 실행(데이터 변경) 후 확인



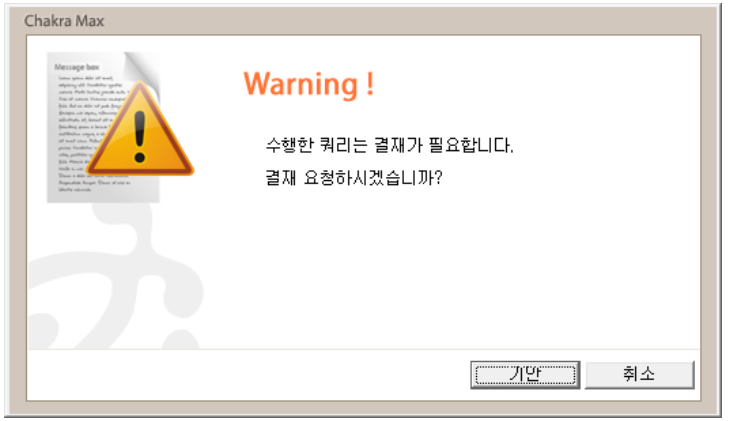
작업결재 Demo - 사전결재

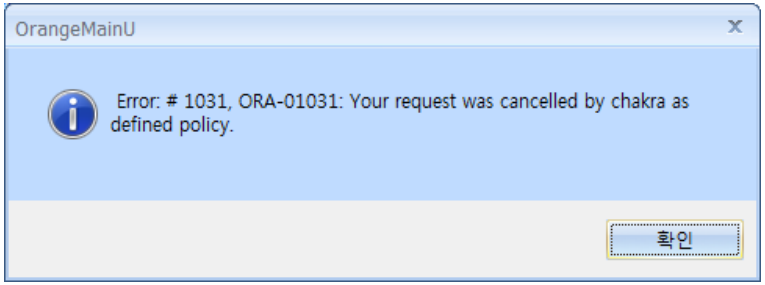
- 운영 DB 의 간단한 DCL, DDL, PL-SQL(function, Procedure 등) 작업
- Drop, Truncate 는 원칙적으로 차단(별도의 작업계획서로 진행)

① Alter Table – Column Length 변경



② 사전결재 기안 및 샤크라 차단 메시지

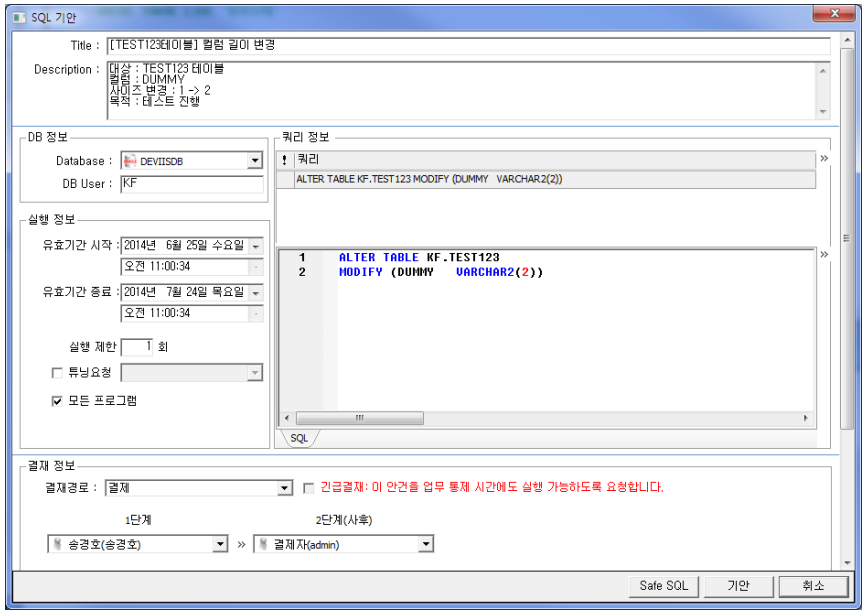




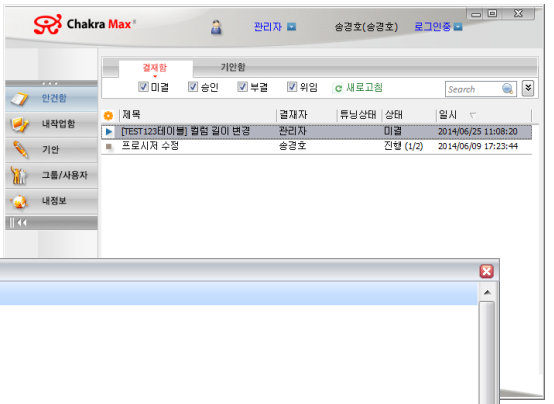
작업결재 Demo - 사전결재

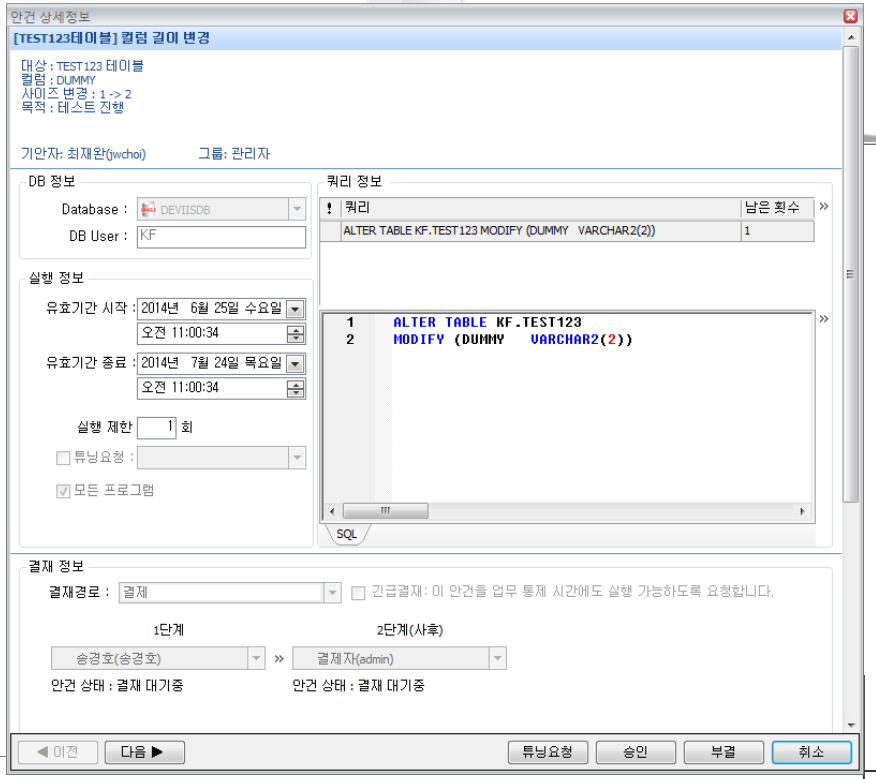
- 운영 DB 의 간단한 DCL, DDL, PL-SQL(function, Procedure 등) 작업
- Drop, Truncate 는 원칙적으로 차단(별도의 작업계획서로 진행)

③ 사전결재
- TITLE : 업무명, 목적 등을 간략히 기술
- Description : SQL 작업 내용을 가능한 상세히 기술 (5W 1H)
- 사후결재는 업무별로 현재 결제가 가능한 담당자를 선택(* 업무별 담당자 지정 예정)
- 2단계 결제자는 Admin 고정



④ 관리자 승인

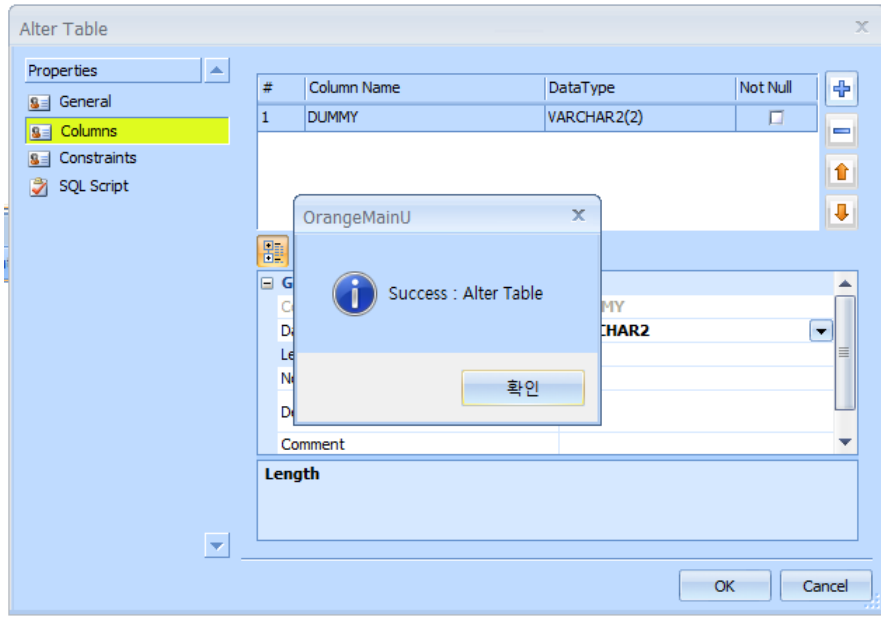




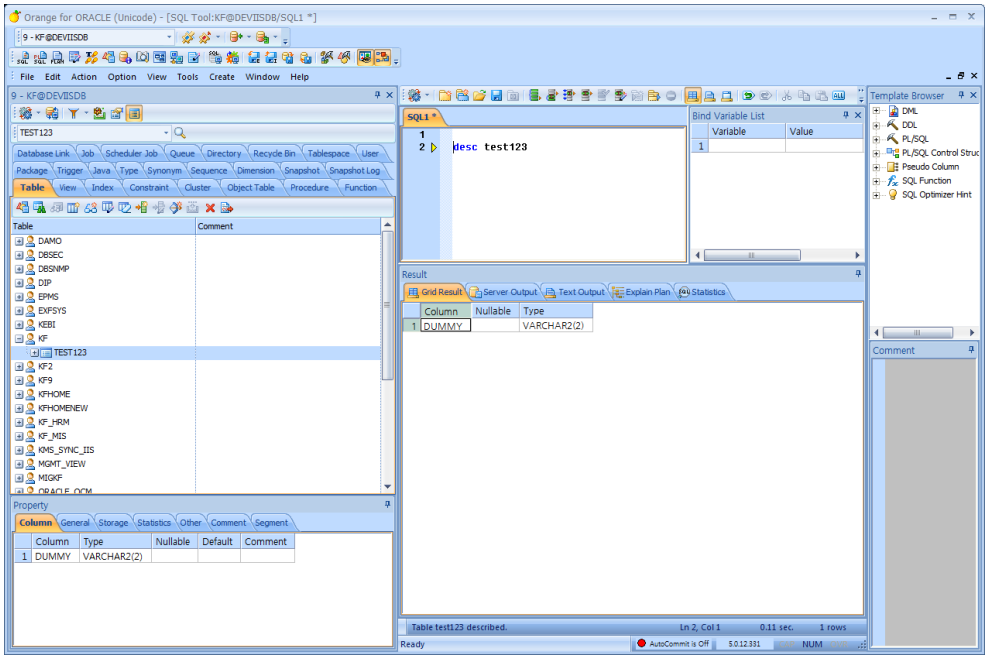
작업결재 Demo - 사전결재

- 운영 DB 의 간단한 DCL, DDL, PL-SQL(function, Procedure 등) 작업
- Drop, Truncate 는 원칙적으로 차단(별도의 작업계획서로 진행)

⑤ 관리자 승인 후 테이블 컬럼 길이 수정

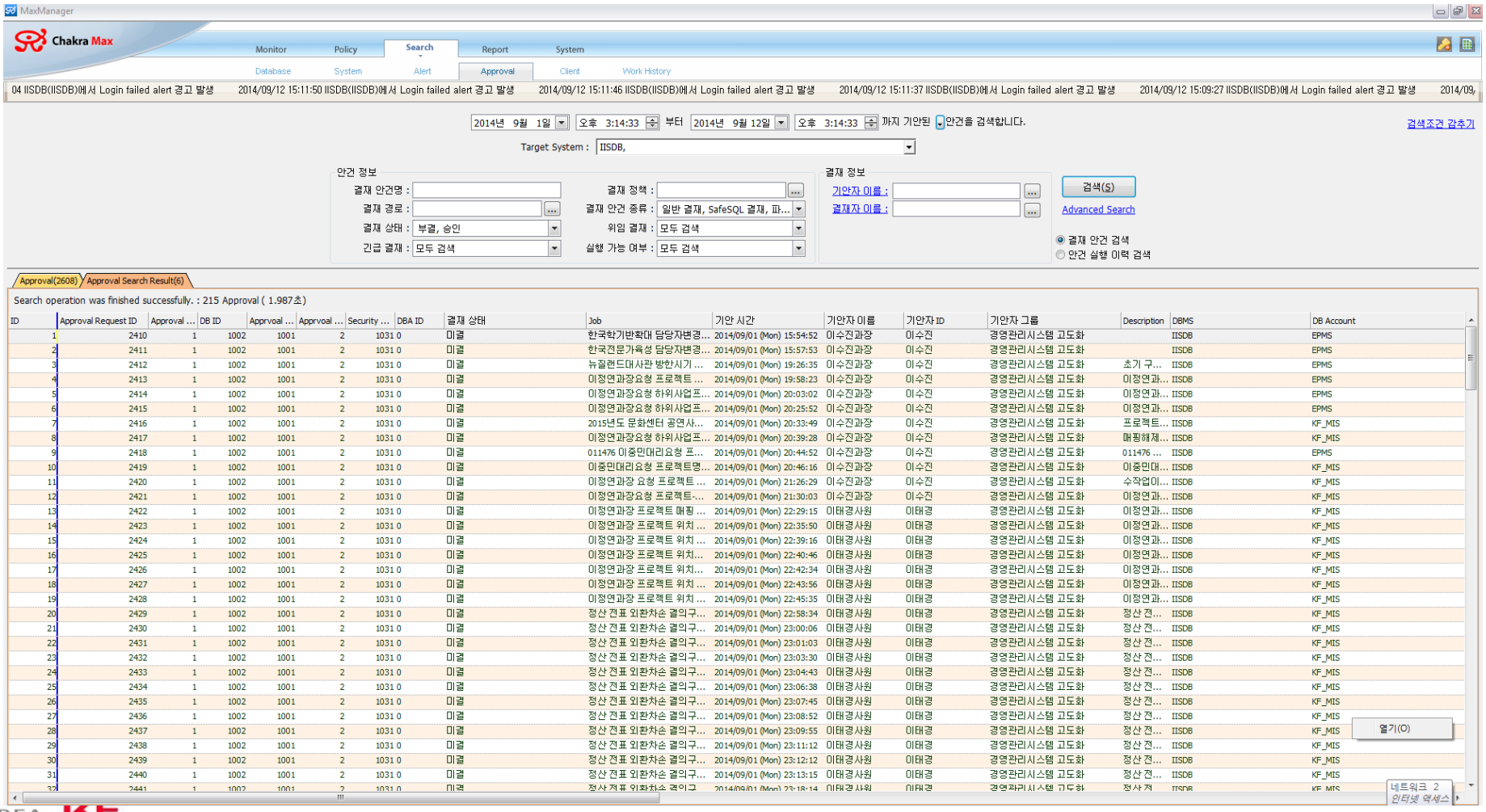


⑥ 변경 내역 확인



작업결재 Demo - 모니터링

- 보안규칙 관리, 결재 내역 확인, 운영 상황 모니터링



Q & A

감사합니다