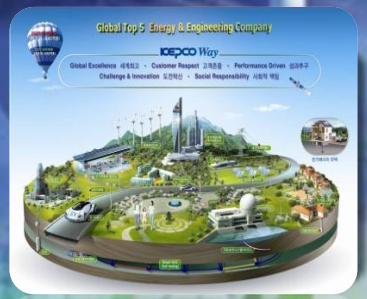
전력연구원

지리정보 DB보안 구축 사례

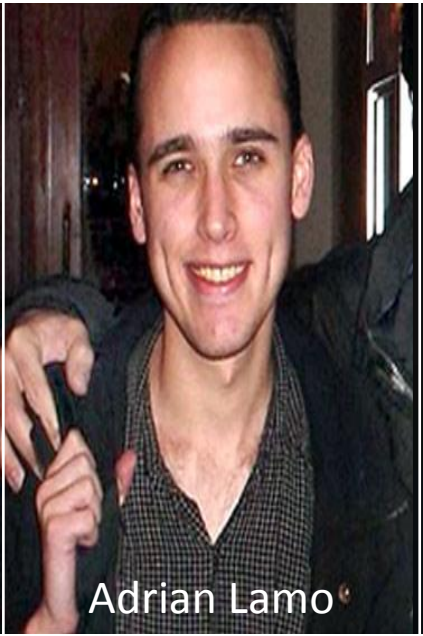
2014. 9. 30.

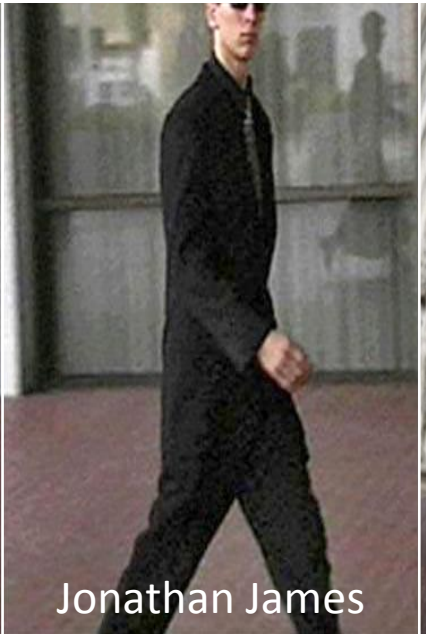


한국전력공사


Kevin Poulsen
Albert Gonazlez
Vladimir Levin
Robert Tappan Morris
Michael Calce
David Smith
Adrian Lamo
Gorge Hotz
Jonathan James
Gary McKinnon

Top 10 Notorious Black Hat Hackers





17세 어린 나이로 아이폰 최초 탈옥(1989년생)

AT&NT 이동통신사업자 반독점 쟁취

소니 플레이스테이션 3 해킹, 소송, 남미피신, 합의

페이스북 보안팀 거쳐
구글 보안드림팀 '프로젝트 제로' 합류
사이버 공격 중 방어 어려운 제로데이 공격 연구위한 팀

목 차

I. 한전 전력연구원 소개

Global Top Green & Smart Energy Pioneer

국민의 삶의 질 향상과 국가 및 글로벌 산업, 경제 사회 발전에 기여하고
지구를 아름답게, 인류를 행복하게 하는 기업

Global 글로벌 무대에서

Top 세계 최고의 경쟁력 확보하고

Green 녹색 기술 개발 사업화

Smart 지능형 전력공급시스템 구축하여

Energy 종합 에너지 사업 전개

Pioneer 미래 에너지 사업 선도

1898 한성전기회사 설립

1961 한국전력주식회사 발족

1982 한국전력공사 발족

1994 뉴욕증권거래소 상장

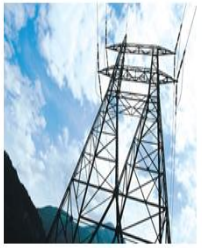
2001 발전부문 6개자회사로분리

2004 공기업 고객만족도 6년 연속 1위

2006 에디슨 대상 수상

2009 최초 해외 원전 수출

발전



송전

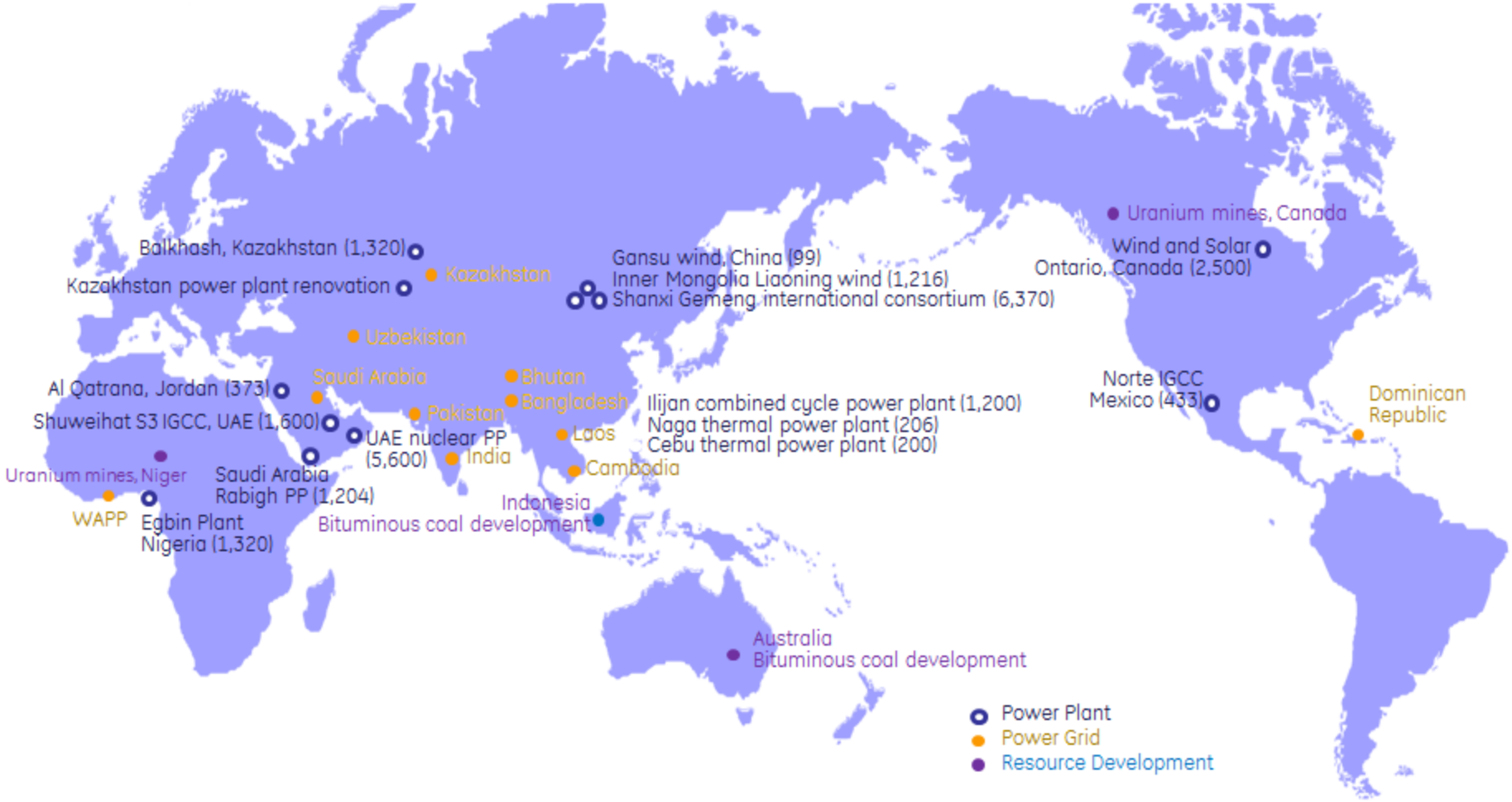
배전

자산총계	98.2 조원
부채총계	56.5 조원
발전설비용량	70,845 MW (IPP 86,968 MW 포함)
발전량	448,756 GWh (IPP 517,147 GWh 포함)

한국수력원자력주식회사	원자력 발전사업 (26 GW)
한국남동발전(주)	화력 발전사업 (8.2 GW)
한국중부발전(주)	화력 발전사업 (8.9 GW)
한국서부발전(주)	화력 발전사업 (8.9 GW)
한국남부발전(주)	화력 발전사업 (9.2 GW)
한국동서발전(주)	화력 발전사업 (9.3 GW)
한국전력기술(주)	발전소 설계 등
한전KPS(주)	전력설비 개보수 등
한전원자력연료(주)	원자력연료 가공
한전KDN(주)	전력 IT 서비스 등

* 58 Associates and 38 Joint Ventures in Korea and worldwide

I. 한전 전력연구원 소개

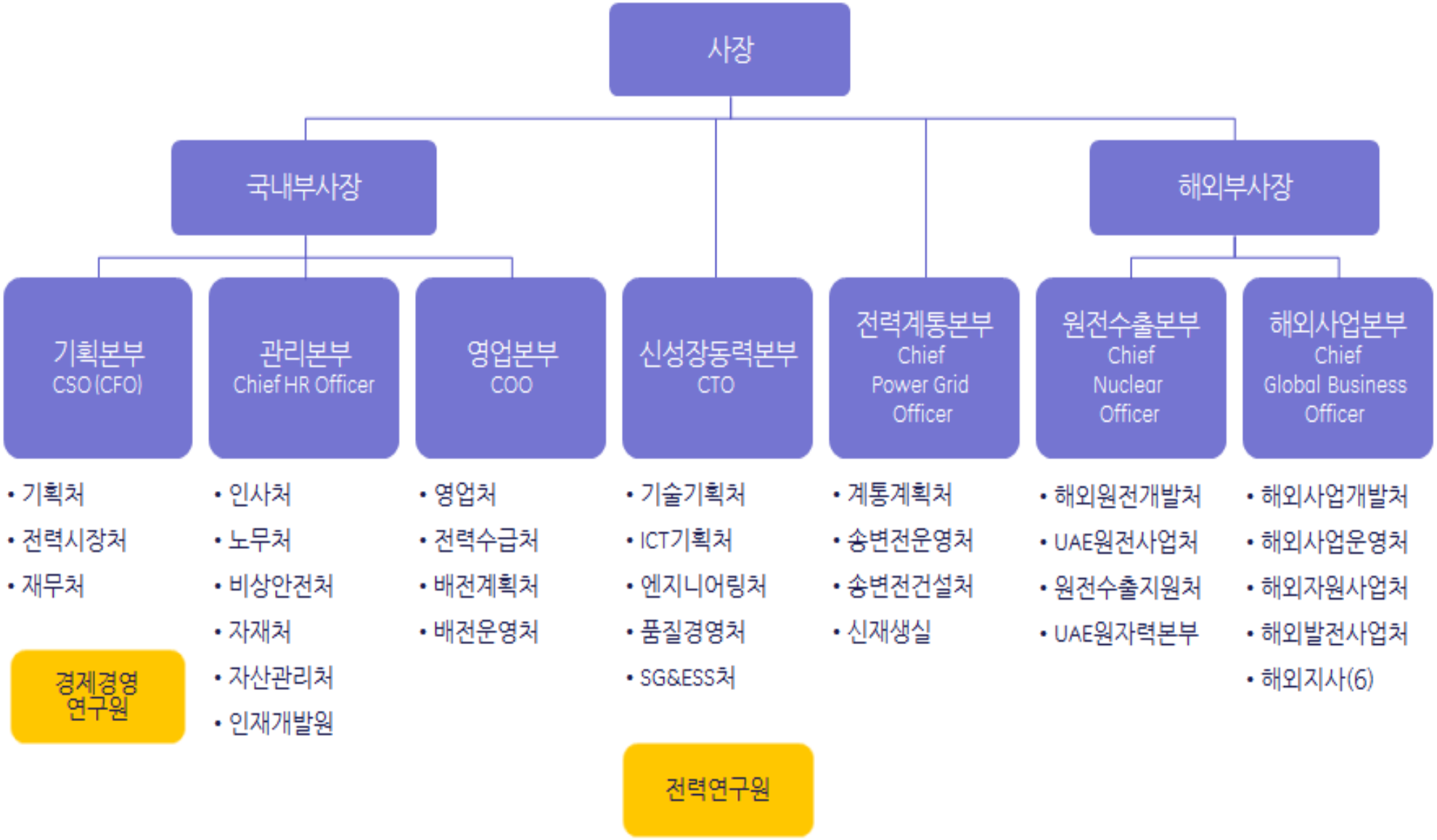

Balkhash, Kazakhstan (1,320)
Kazakhstan power plant renovation
Kazakhstan
Gansu wind, China (99)
Inner Mongolia Liaoning wind (1,216)
Shanxi Gemeng international consortium (6,370)
Uzbekistan
Uranium mines, Canada
Wind and Solar
Ontario, Canada (2,500)
Saudi Arabia
Bhutan
Bangladesh
Al Qatrana, Jordan (373)
Shuweihat S3 IGCC, UAE (1,600)
Pakistan
UAE nuclear PP
(5,600)
India
Laos
Cambodia
Ilijan combined cycle power plant (1,200)
Naga thermal power plant (206)
Cebu thermal power plant (200)
Norte IGCC
Mexico (433)
Dominican
Republic
Uranium mines, Niger
Saudi Arabia
Rabigh PP (1,204)
WAPP
Egbin Plant
Nigeria (1,320)
Indonesia
Bituminous coal development
Australia
Bituminous coal development
Power Plant
Power Grid
Resource Development

건국 이래 최대 규모, UAE 원전 수주(약 21조)

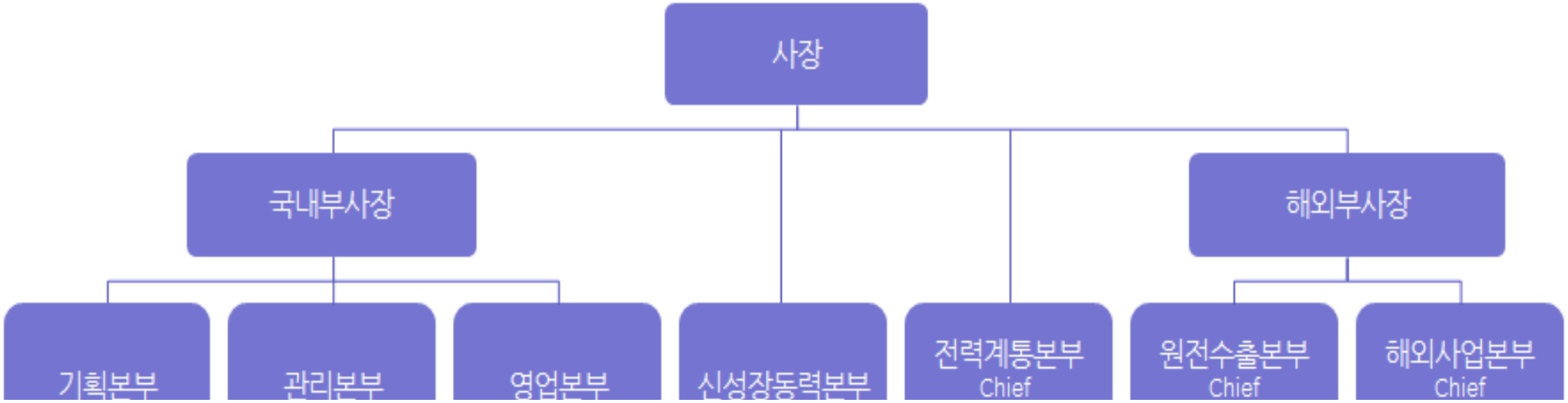
현재 21개국 총 42개 해외 프로젝트 진행중

중소기업과 협력관계 유지(협력기업중 중소기업 96% 이상)

Ⅰ. 한전 전력연구원 소개


사장
국내부사장
해외부사장
기획본부
CSO (CFO)
관리본부
Chief HR Officer
영업본부
COO
신성장동력본부
CTO
전력계통본부
Chief
Power Grid
Officer
원전수출본부
Chief
Nuclear
Officer
해외사업본부
Chief
Global Business
Officer
• 기획처
• 전력시장처
• 재무처
• 인사처
• 노무처
• 비상안전처
• 자재처
• 자산관리처
• 인재개발원
• 영업처
• 전력수급처
• 배전계획처
• 배전운영처
• 기술기획처
• ICT기획처
• 엔지니어링처
• 품질경영처
• SG&ESS처
• 계통계획처
• 송변전운영처
• 송변전건설처
• 신재생실
• 해외원전개발처
• UAE원전사업처
• 원전수출지원처
• UAE원자력본부
• 해외사업개발처
• 해외사업운영처
• 해외자원사업처
• 해외발전사업처
• 해외지사(6)
경제경영 연구원
전력연구원

Ⅰ. 한전 전력연구원 소개



본사조직 7개 본부 31처(실) 구성

사업소 조직 총 262개 사업소 구성

(전력연구원 등 10개 특수사업소 포함)

경제경영연구원

- 재무처

전력연구원

- 비상안전처
- 자재처
- 자산관리처
- 인재개발원
- 배전계획처
- 배전운영처
- 엔지니어링처
- 품질경영처
- SG&ESS처
- 송변전건설처
- 신재생실
- 원전수출지원처
- UAE원자력본부
- 해외자원사업처
- 해외발전사업처
- 해외지사(6)

R & D VISION

에너지 기술의 새로운 가치를 창조하는 Global Top 연구원

우리회사 중장기 전략방향

- 국내사업 신뢰성 강화
- 글로벌 사업역량 확대
- 신성장 동력 사업창출
- 전력사업 사회책임 완수

전략목표

- 전력수급 안정성제고
- 해외사업 수익확대
- 미래 성장동력 강화
- 사회 책임경영 선도

R & D 전략과제

- 효율향상+성능개선 (송배전+발전)
- 지능형 배전운영 분산전원연계기술
- 수요자원 시장 기반 DR 기술

- 설비진단 기술 (해외ROMM㈜사업)
- 설비이용률 향상 (해외 발전설비)
- 해외 기술컨설팅 (사업수주확대)

- 친환경 발전기술 (발전 CO_2 저감)
- 신재생에너지기술 (글로벌 경쟁력)
- 고효율 전력기술 (고수익창출 모델)

- 산학연 클러스터 중소기업 파트너십
- 新R&D 협력체계 (KEPCO-발전사)
- Global Network 국제 표준화 선도

주) ROMM : Rehabilitation Operation Maintenance and Management

연 혁

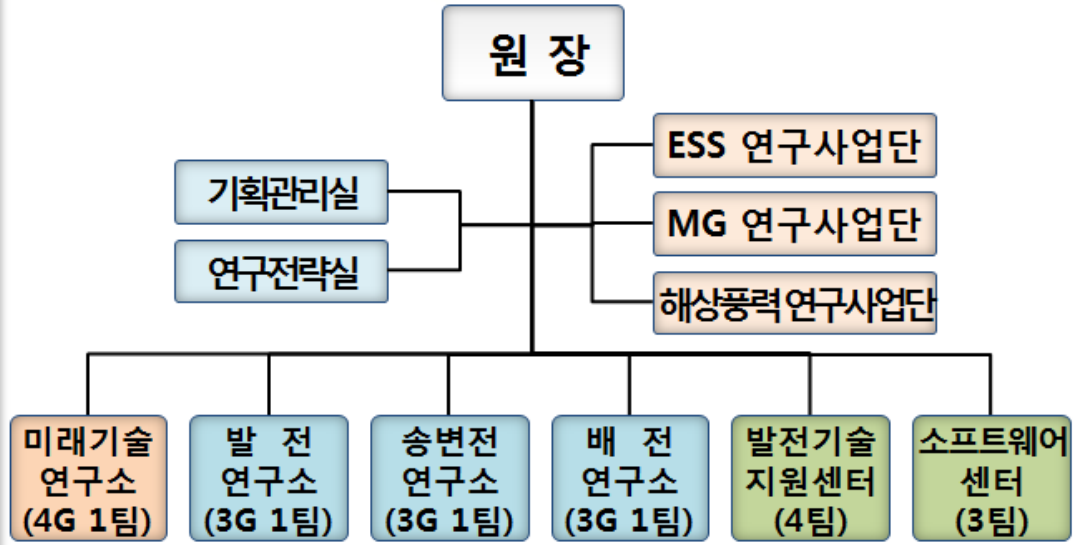
태 동 기 - 전기시험소 -
- 1961년~1970년
- 전기시험소 발족
- 시험업무 위주

성 장 기 - 기술연구원 -
- 1980년~1990년 초
- 현장기술지원 주력
- 대전(大田) 이전

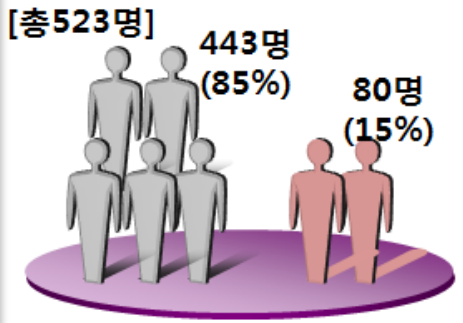
도 약 기 - 전력연구원 -
- 1990년 중~2012년
- 대덕연구단지 입주
- 우수 연구인력 확보
- 녹색기술 본격 연구

세계 최고수준 진 입 기
- 2013년~
- 제2의 연구원 혁신
- 글로벌 협력강화
- 세계최고 기술확보

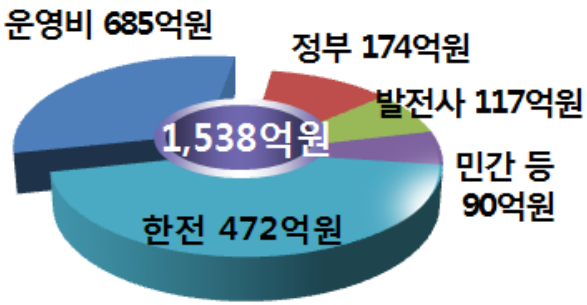
조직 및 예산



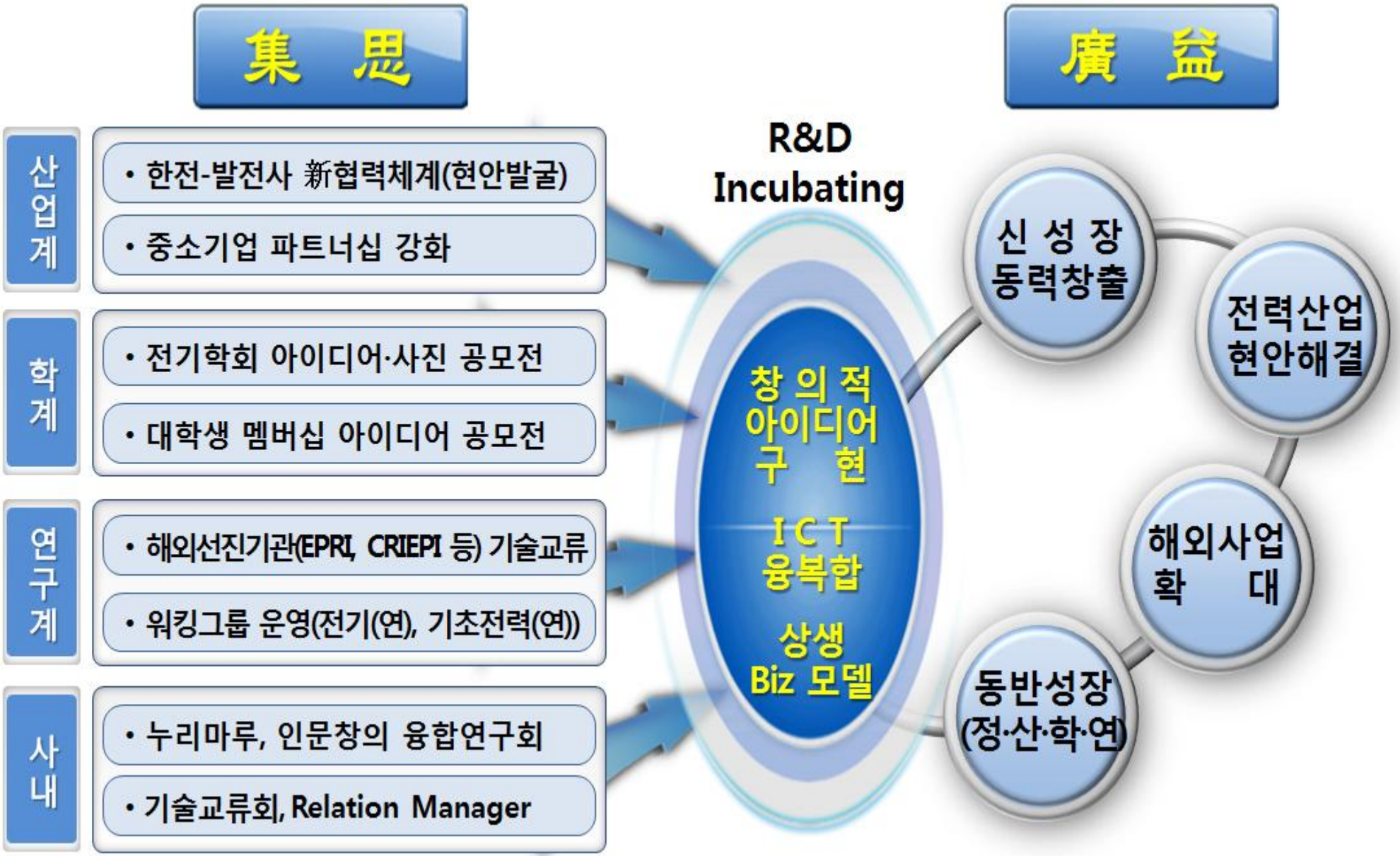
❖ 연구사업단 : 사업화 대상기술 개발, 원장직속으로 운영



[인력 현황]



['14년 예산 현황]


集 思
廣 益
산업계
• 한전-발전사 新협력체계(현안발굴)
• 중소기업 파트너십 강화
학계
• 전기학회 아이디어·사진 공모전
• 대학생 멤버십 아이디어 공모전
연구계
• 해외선진기관(EPRI, CRIEPI 등) 기술교류
• 워킹그룹 운영(전기(연), 기초전력(연))
사내
• 누리마루, 인문창의 융합연구회
• 기술교류회, Relation Manager
R&D
Incubating
창의적
아이디어
구 현
ICT
융복합
상생
Biz 모델
신성장
동력창출
전력산업
현안해결
해외사업
확 대
동반성장
(정·산·학·연)


토지 7만 9천 제곱미터(약 2만 3천 9백평)

매매가 10조 5500억

평당 가격 4억 4천 백만원


1.8128m

1평
1.8 * 1.8 = 3.3 제곱미터

1.8128m

5m

3.78평
2.5 * 5 = 12.5제곱미터

2.5m

1.8m

4.8m

Ⅰ 한전 전력연구원 소개

Ⅱ 기반시설과 지리정보 DB보안

Ⅲ 향후 DB보안 추진방향

❖ 국제해킹대회 PHD 2014 : 미국 데프콘과 함께 3대 해외 유명 해킹대회 중 하나

메인 이벤트 : 실제 사용되는 스카다 시스템 해킹

❖ 국제 해킹 & 컨퍼런스 2014 : 해커와 보안전문가 운영 국제 해킹 및 보안 컨퍼런스

POC

POC2014
2014년 11월 6~7일

주목할 만한 이벤트 : 스카다 시스템 해킹

홈 | 발표자 | 일정 | 이벤트 | 트레이닝 | 장소 | 아카이브 | 등록

POWER OF COMMUNITY

POC에 오신 것을 환영합니다. POC는 2006년부터 해커들과 보안 전문가들이 운영하고 있는 국제 해킹 & 보안 컨퍼런스입니다. POC는 이익을 추구하지 않습니다. POC는 기술 중심적이고 창의적인 발표와 실제 해킹과 보안 기술을 직접 보여줍니다. POC는 블랙햇과 화이트햇 성격을 모두 갖고 있습니다. POC는 'Power of Community' 정신 아래 지식을 공유합니다. '커뮤니티의 힘'을 통해 전세계를 더 안전하게 만들 수 있다고 믿습니다.

POC는 2006년부터 전세계의 해커, 스탭, 스폰서들이 함께 만들어 가고 있습니다.

POC 모토
- 해커는 자유로워야 한다.
- 우리는 보안을 위해 해킹을 한다.
- 우리는 '커뮤니티의 힘'을 믿는다.

POC2014
http://www.powerofcommuninty.net

CALL FOR PAPERS

REGISTER NOW

❖ 스턱스넷(StuxNet)

2011년 이란 원자력시설 원심분리기 1천여대 손상

❖ 스턱스넷(StuxNet)

원자력, 전기, 철강, 반도체 등 산업기반의 제어시스템 침투

오작동을 일으키게 만드는 악성프로그램

USB나 네트워크 공유 취약점 등 이용 몰래 설치

❖ 국내외 전자적 제어시스템 피해사례

시기	발생국	피 해 내 용	비고
2007년 3월	미국	• DHS 주관 미국 발전소 제어시스템을 모의해킹 • 발전기 가동 사이클을 변경하여 발전기 파괴 http://www.cnn.com/2007/US/09/26/power.at.risk/index.html#cnnSTCText	전력
2007년 8월	미국	• 전직 직원이 캘리포니아 주의 TCCA 운하 제어시스템에 악성프로그램 설치 • 운하 운영 마비, 5,000만 달러 이상 손실 http://www.computerworld.com.au/article/198630/insider_charged_hacking_california_canal_system/	수자원
2008년 1월	폴란드	• 14세 소년이 TV 리모컨을 개조하여 트램 교차로 불법 조작 • 4대의 트램 탈선 및 12명 부상 http://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html	교통
2008년 5월	미국	• 회계감사원(GAO) 주관 미국 최대 국립전력회사인 TVA사 제어시스템을 모의해킹 • 인터넷 발전소 제어시스템 침투 성공 • http://www.cnn.com/2008/US/05/21/cyber.attack/index.html	전력
2009년 8월	러시아	• 수력발전댐의 터빈 제어시스템 장애 • 발전기 터빈 폭발, 75명 사망 • http://en.wikipedia.org/wiki/2009_Sayano-Shushenskaya_hydro_accident	수자원
2010년 7월	이란	• 스턱스넷 바이러스 원자력발전소 제어시스템 침투 • 이란 나탄즈 원자력 원심분리기의 일부분 기능 마비 • http://en.wikipedia.org/wiki/Stuxnet	원자력

❖ 국내외 전자적 제어시스템 피해사례

시기	발생국	피 해 내 용	비고
2007년 3월	미국	• DHS 주관 미국 발전소 제어시스템을 모의해킹 • 발전기 가동 사이클을 변경하여 발전기 파괴 http://www.cnn.com/2007/US/09/26/power.	전력
2007년 8월	미국	• 전직 직원이 캘리포니아 주의 TCCA 운하 제어시스템에 악성프로그램 설치 • 운하 운영 마비, 5,000만 달러 이상 손실 http://www.computerworld.com.au/article/198630/insider_charged_hacking_california_canal_system/	수자원
2008년 1월	폴란드	• 14세 소년이 TV 리모컨을 개조하여 트램 교차로 • 4대의 트램 탈선 및 12명 부상 http://www.telegraph.co.uk/news/worldnew -into-citys-tram-system.html	교통
2008년 5월	미국	• 회계감사원(GAO) 주관 미국 최대 국립전력회사인 TVA사 제어시스템을 모의해킹 • 인터넷 발전소 제어시스템 침투 성공 • http://www.cnn.com/2008/US/05/21/cyber.attack/index.html	전력
2009년 8월	러시아	• 수력발전댐의 터빈 제어시스템 장애 • 발전기 터빈 폭발, 75명 사망 • http://en.wikipedia.org/wiki/2009_Sayano-S	수자원
2010년 7월	이란	• 스턱스넷 바이러스 원자력발전소 제어시스템 침투 • 이란 나탄즈 원자력 원심분리기의 일부분 기능 마비 • http://en.wikipedia.org/wiki/Stuxnet	원자력

발전기 파괴
5,000만 달러 손실

트램 탈선
12명 부상

발전기 터빈 폭발
75명 사망

❖ 국내외 전자적 제어시스템 피해사례

시기	발생국	피 해 내 용	
2010년 7월	이란	• 스턱스넷 바이러스 원자력발전소 제어시스템 침투 • 이란 나탄즈 원자력 원심분리기의 일부분 기능 마비 • http://en.wikipedia.org/wiki/Stuxnet	원자력
2011년 11월	미국	• 일리노이 주 상수도 시설 시스템 침투 • 펌프 작동 시스템 파괴 • http://www.bbc.co.uk/news/technology-15817335	수자원
2012년 5월	이란, 수단, 시리아 등	• 주요 중동국가의 컴퓨터에 침입하여 중요 데이터 유출 · 파괴 • http://www.washingtonpost.com/world/national-security/us-israel-developed -computer-virus-to-slow-iranian-nuclear-efforts-officialssay/2013/06/19/gJQA6xBPoV_story.html	국가 주요 시설
2012년 10월	미국	• 전력시설 터빈 제어시스템 악성코드 감염 • 3주간 운영 중단 • http://ics-cert.us-cert.gov/sites/default/files/ICS-CERT_Monthly_Monitor_Oct-Dec2012_2.pdf	전력
2013년 3월	한국	• 방송 및 금융 등 다수 기업 전산망 악성코드로 인한 시스템 파괴 등 장애 발생 • PC 및 시스템 4만8천여 대 피해 • http://www.yonhapnews.co.kr/bulletin/2013/04/10/0200000000AKR20130410104200017.HTML	방송 금융

전력, 수력, 원자력

국가주요시설 교통, 금융

❖ 국내외 전자적 제어시스템 피해사례

시기	발생국	피 해 내 용	비고
2007년 3월	미국	• DHS 주관 미국 발전소 제어시스템을 모의해킹 • 발전기 가동 사이클을 변경하여 발전기 파괴 http://www.cnn.com/2007/US/09/26/power.at.risk/index.html#cnnSTCText	전력
2007년 8월	미국	• 전직 직원이 캘리포니아 주의 TCCA 운하 제어시스템에 악성프로그램 설치 • 운하 운영 마비, 5,000만 달러 이상 손실 http://www.computerworld.com.au/article/198630/insider_charged_hacking_california_canal_system/	수자원
2008년 1월	폴란드	• 14세 소년이 TV 리모컨을 개조하여 트램 교차로 불법 조작 • 4대의 트램 탈선 및 12명 부상 http://[illegible]legraph.co.uk/news/worldnews/1575293/Schoolboy-hacks[illegible]ystem.html	교통
2[illegible]	[illegible]	[illegible]	[illegible]
2009년 8월	러시아	• 발전기 터빈 폭발, 75명 사망 • http://en.wikipedia.org/wiki/2009_Sayano-Shushenskaya_hydro_accident	수자원
2010년 7월	이란	• 스턱스넷 바이러스 원자력발전소 제어시스템 침투 • 이란 나탄즈 원자력 원심분리기의 일부분 기능 마비 • http://en.wikipedia.org/wiki/Stuxnet	원자력

14세 소년이 TV 리모컨을 개조하여 트램 교차로 불법 조작
4대의 트램 탈선 및 12명 부상


EUROPICS


SL
3034
3034
My giant personal train set!

4대 트램 탈선, 12명 부상

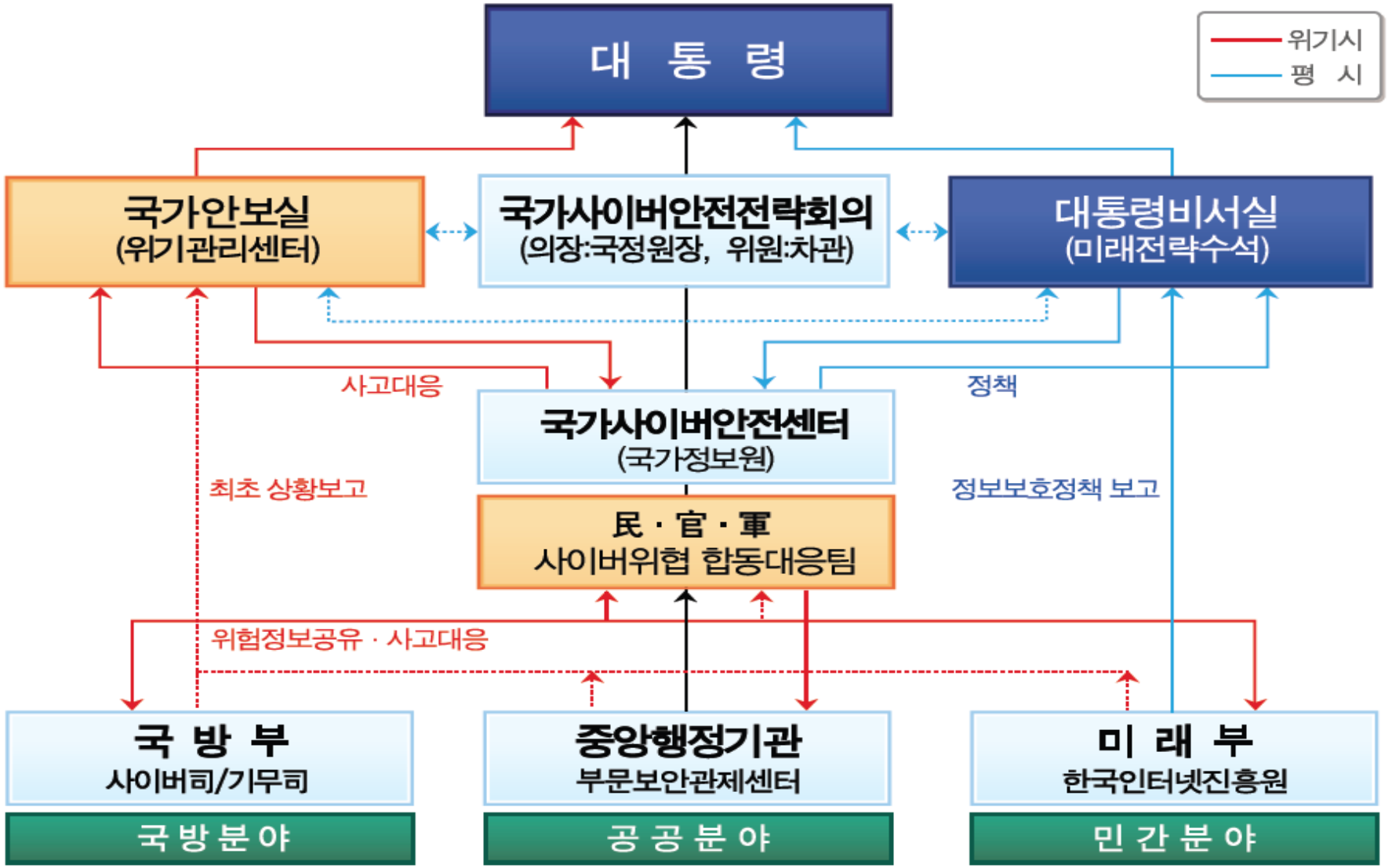
❖ 국내외 전자적 제어시스템 피해사례

시기	발생국	피 해 내 용	비고
2010년 7월	이란	• 스턱스넷 바이러스 원자력발전소 제어시스템 침투 • 이란 나탄즈 원자력 원심분리기의 일부분 기능 마비 • http://en.wikipedia.org/wiki/Stuxnet	원자력
2011년 11월	미국	• 일리노이 주 상수도 시설 시스템 침투 • 펌프 작동 시스템 파괴 • http://www.bbc.co.uk/news/technology-15817335	수자원
2013년 3월	한국	• 방송 및 금융 등 다수 기업 전산망 악성코드로 인한 시스템 파괴 등 장애 발생 • PC 및 시스템 4만8천여 대 피해 • http://www.yonhapnews.co.kr/bulletin/2013/04/10/0200000000AKR20130410104200017.HTML	방송 금융

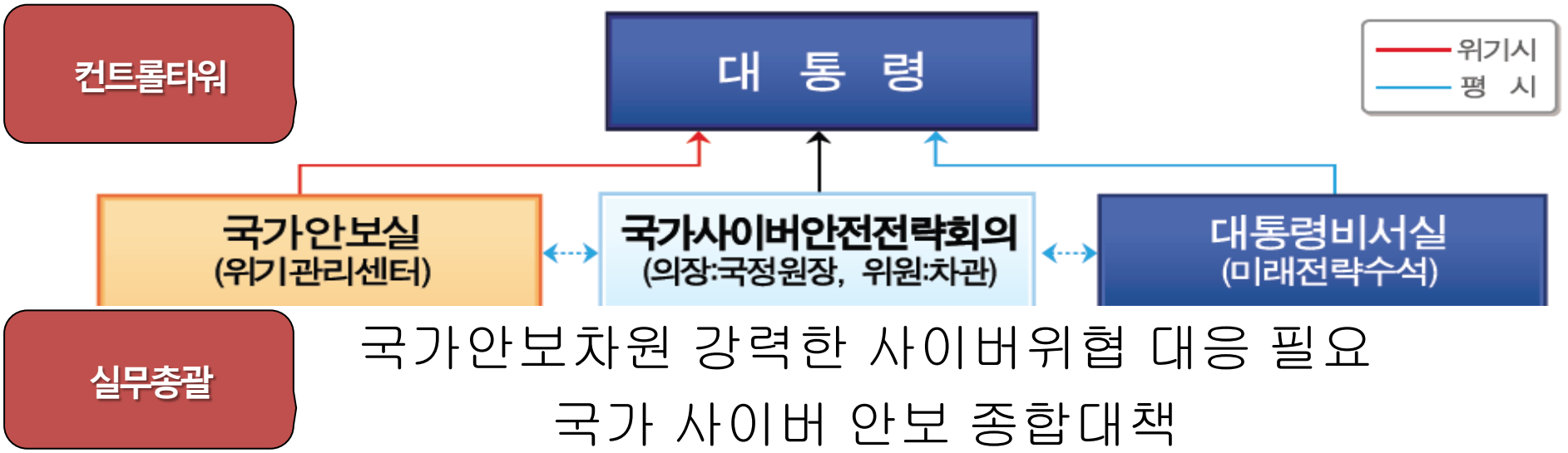
스카다(제어시스템)은 폐쇄망으로 운영
과거에는 물리적인 공격이나 조작실수 대부분
정보통신서비스와 연결, 운영되면 사이버 공격 피해 발생

320 인터넷 테러

❖ 사이버안보 업무수행체계 : 3.20 사이버터러, 6.25 사이버 공격 대규모 피해발생



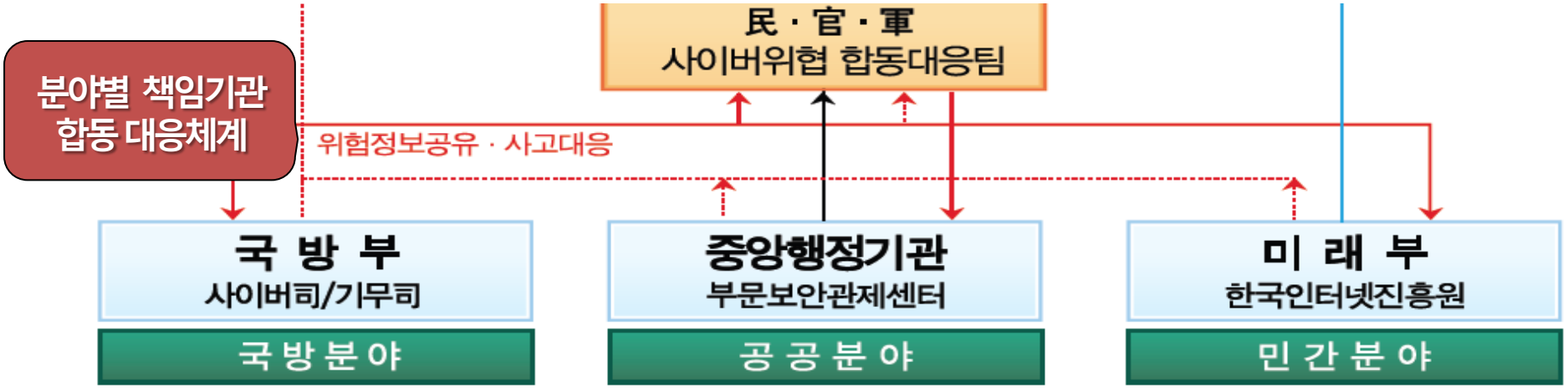
❖ 사이버안보 업무수행체계 : 3.20 사이버테러, 6.25 사이버 공격 대규모 피해발생



국가안보차원 강력한 사이버위협 대응 필요

국가 사이버 안보 종합대책

사이버안보 업무수행 체계 정립



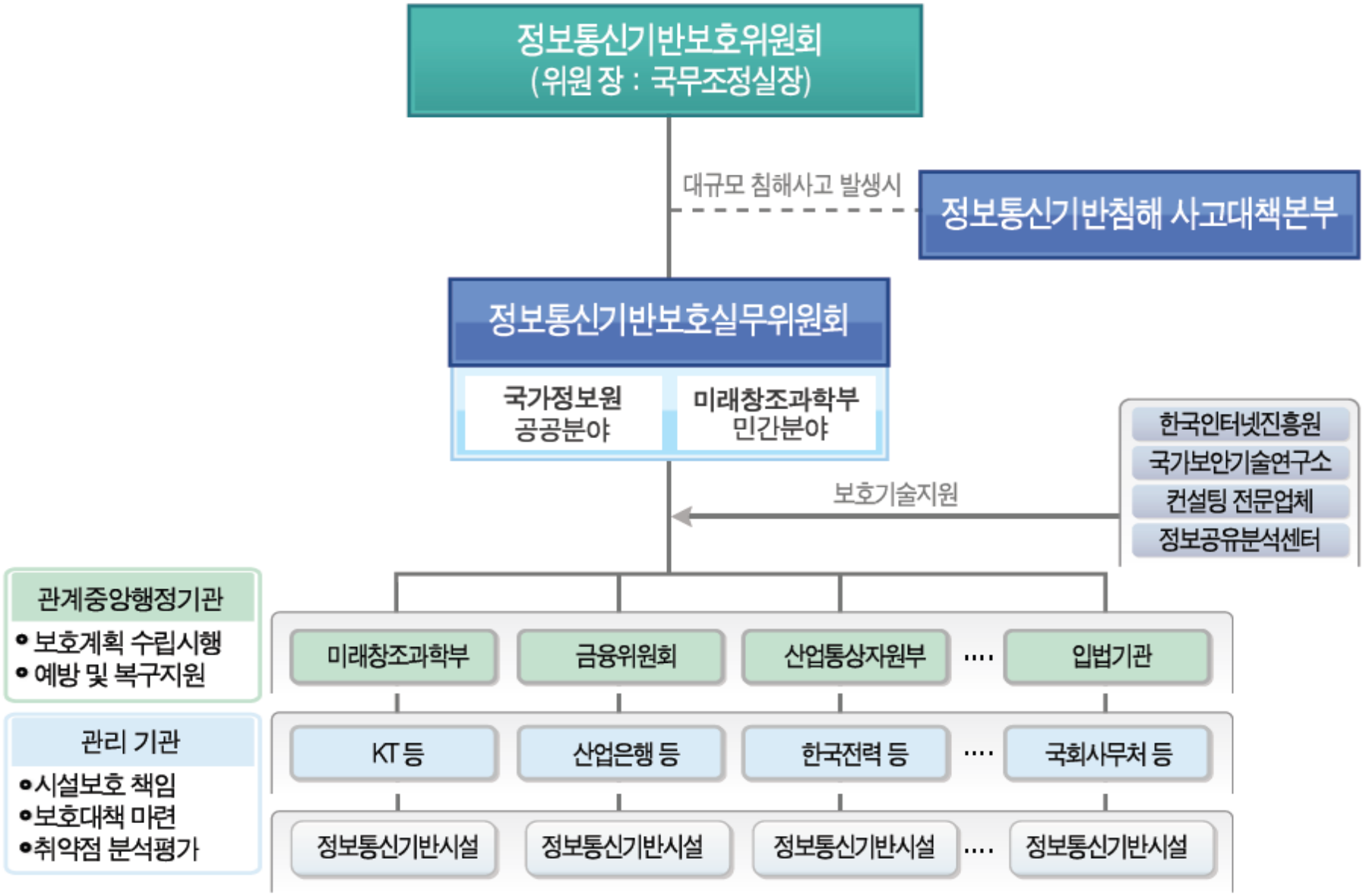
❖ 공공분야 : 보안관제센터 통해 사이버안보 업무 담당

부문	담당기관	관제센터
행정	안전행정부	정부통합전산센터(대전)
		정부통합전산센터(광주)
		사이버침해대응지원센터(G-CERT)
국토교통	국토교통부	국토교통 사이버안전센터
보건의료	보건복지부	보건의료 사이버안전센터
교육	교육부	교육 사이버안전센터
에너지	산업통상자원부	산업통상 사이버안전센터
통신과학	미래창조과학부	미래창조과학 사이버
금융	금융위원회	증권 ISAC(KOSCOM)

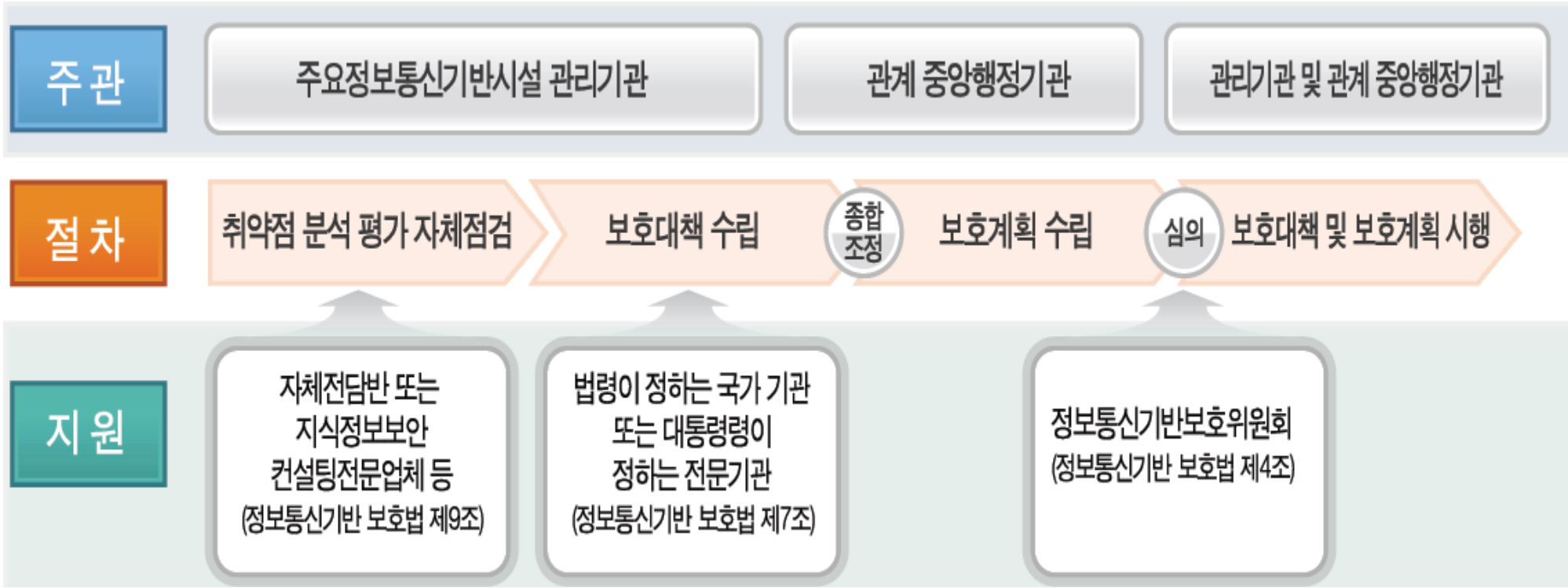
사이버위협 예방, 침해사고 대응, 정보보안 기술개발, 인력육성

산업통상 사이버안전센터

❖ 주요정보통신기반시설 보호체계 : 주요 기반시설의 인터넷 연결 확대로 해킹 시도 빈번해짐



❖ 주요정보통신기반시설 보호계획 수립절차



정보통신기반 보호법

- 관리기관 : 기반시설의 취약점 분석 평가 자체점검하고 보호대책 수립, 산업부 제출
- 행정기관 : 제출된 보안대책 종합조정하여 기반시설에 관한 보호계획 수립, 시행
- 보호위원회 : 보호계획 심의

❖ 주요정보통신기반시설 지정현황

국가기반 시설 지정현황 (2013년 7월 기준)

구분	행정	통신	금융	에너지	보건복지	운송	기타	계
시설수	63	35	49	30	8	14	10	209

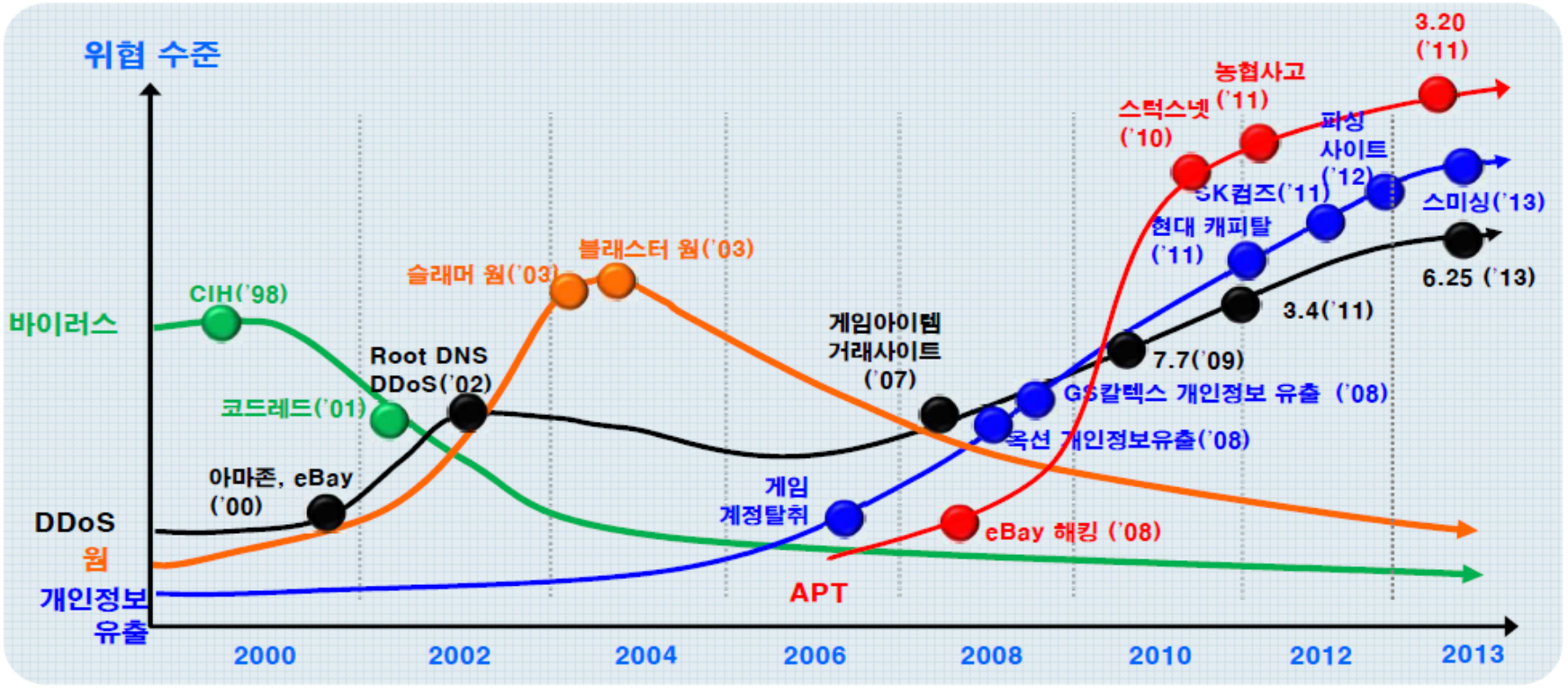
주요정보통신기반시설의 명칭	관리기관	수행업무	지정사유
배전자동화시스템	한국전력공사	배전선로의 상태감시 및 최적 계통전환	전력 수용가를 대상으로 안정적인 전력을 공급하기 위한 감시 및 운영
공			

주요정보통신기반시설의 명칭	관리기관	수행업무	지정사유
고리원자력발전소 제어시스템	한국수력원자력	전력생산을 위한 원자력발전소 운전·제어·감시	
영광원자력발전소 제어시스템			
울진원자력발전소 제어시스템			
월성원자력발전소 제어시스템			
보령			
인천			
양양			
당진			
울산			
태안			
평택			
서인천			
하동			
부산			
신인천			
삼천포			
영흥			
송유			

지정번호	기반시설명	관리기관명	주요 기능
1	송변전원방감시제어시스템(SCADA)	한국전력공사	전력설비 운전정보를 실시간으로 취득하여 송변전 설비를 제어조작
2	급전자동화시스템	한국전력거래소	전력계통 운영정보를 실시간 취득하여 제공함으로써 경제적인 전력생산과 안정적인 전력공급 달성
3	천연가스배관망 원격감시제어시스템	한국가스공사	전국 천연가스 생산 및 공급계통을 감시·제어하고 공급계통분석 및 종합정보를 제공

※ SCADA : Supervisory Control And Data Aquisition

❖ 국내 해킹사고의 동향

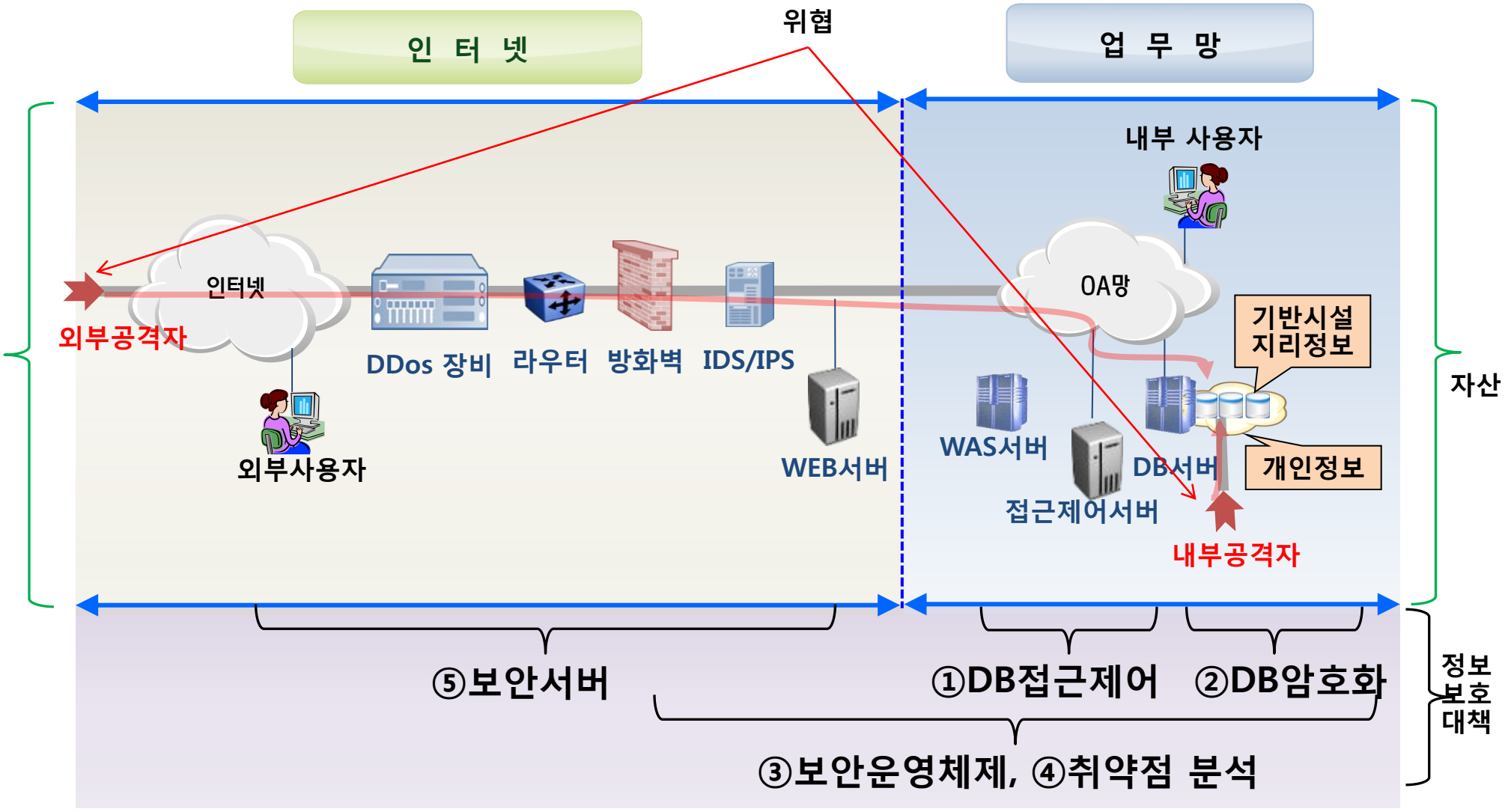


1986 Brain
1988 Morris Worm
1992 Michelangelo
1998 CIH
1999 Melissa
2003 Slammer
2004 Cabir
2006 Leap
2007 Storm
2008 Koobface Conficker
2010 Stuxnet Fakeplayer
2011 Duqu
2012 Flame

해커 동기 : 호기심, 자기과시 → 금품 갈취 → 사회혼란, 사이버테러
해커 기법 : 수동 → 은닉, 자동화 → 조직적, 지능화
피해 범위 : 개별시스템 → 대규모 네트워크 → 사회기반시설, 국가

❖ 주요정보통신기반시설 보안

❖ 지리정보 데이터베이스 보안



❖ 자산, 위협, 취약점, 위험

컴플라이언스

- 개인정보보호법
- 국가정보보안기본지침
- 보안가이드라인
- 한전보안업무처리지침(지리정보)
- 정보보호설비운영절차서
- 전력사이버안전센터 업무절차서

점검 체크리스트

- 정보보안기본활동
- PC 및 서버 보안관리
- 네트워크 보안관리
- 정보통시설보안 및 대도청
- 암호장비.논리.보안자재관리
- 보안관제 등 해킹 대응활동
- DB보안관리

취약점 분석툴

- 자동화된 취약점 분석툴
  - Host-based Vulnerability Tool
  - Network-based Vulnerability Tool

개인정보보호법

국가지리정보 보안관리지침

제9조 (지리정보 데이터베이스 보호대책) ① 관리부서의 장은 구축.관리하고 있는 지리정보 데이터베이스에 대하여 훼손.파괴.유출 등으로부터 보호하기 위한 대책을 강구하여야 한다.

② 제1항의 보호대책에 포함되어야 한 [illegible] 가.다.

1. 지리정보 관리책임자(정 [illegible]
2. 출입문 카드키, 이중문 [illegible]
3. 데이터베이스 복제본은 [illegible]
4. 지리정보 데이터베이스에 [illegible]

가. 부서 및 사용자별 ID.비 [illegible]

나. 작업범위는 소관업무에 따라 [illegible]

다. 열람은 필요내용에 따라 기본항목.전항목 등으로 구분

라. 지리정보 취급자 이외에 업무상 필요에 의하여 "비공개" 또는 "공개제한" 지리정보 데이터베이스를 이용하고자 하는 자는 관리책임자의 사전허가후 접근

5. 비공개 또는 공개제한 지리정보 자료 목록 관리대장 작성.관리
6. 해킹 등 불법접근 및 컴퓨터 바이러스 예방대책 강구

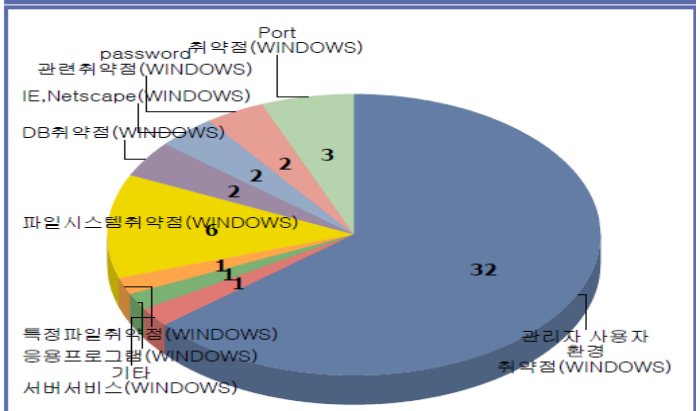
③ 전자매체에 수록된 지리정보 자료는 열람.전송.출력 등 사용내역을 확인할 수 있도록 검색시스템을 구축.관리하여야 한다.

국가지리정보 데이터베이스 보안 관리 지침

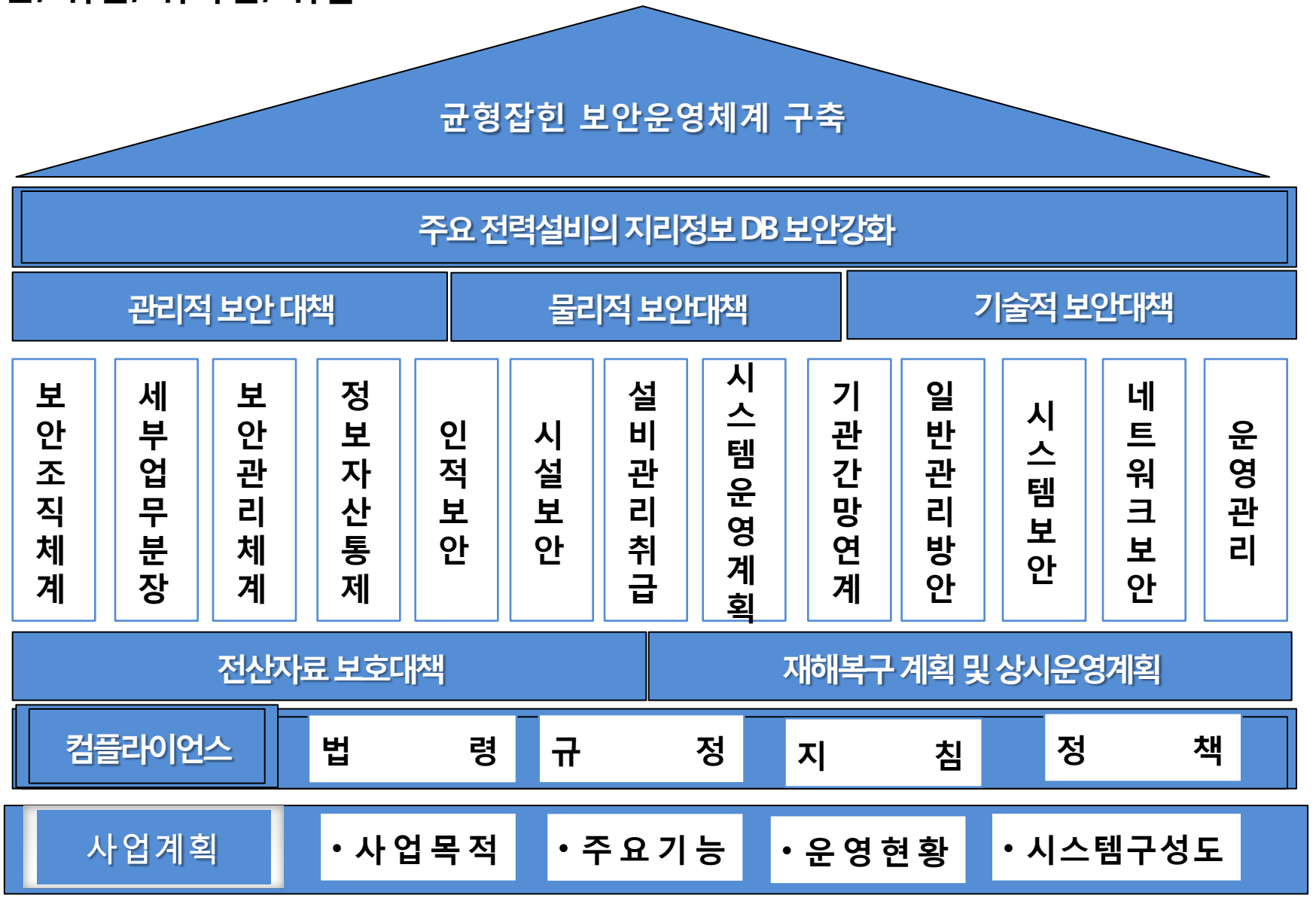
7. DB보안 관리

순 번	세부 점검사항	비 고
1	DBA 권한이 불필요한 계정이 제거되어 있는가?	O
2	기본 계정 및 패스워드를 변경하거나 제거하였는가?	X
3	DataDictionary 접근 제한을 하였는가?	O
4	SYSDBA 권한 제한이 적절하게 이루어 졌는가?	O
5	Default Listener Port 사용을 적절하게 설정하였는가?	O
6	Oracle 중요 파일(*.ctl, *.log, *.dbf)의 접근 권한을 적절히 설정하였는가?	X
7	Audit Trail을 기록하도록 설정하였는가?	O
8	SQL*PLUS 명령 히스토리를 검사하고 있는가?	X
9	Oracle 버전이 적절한가?	O
10	DB 계정의 로그인 실패 횟수에 따른 잠금 시간이 적절히 설정되어 있는가?	O
11	DB 계정의 로그인 실패 횟수에 따른 잠금 시간이 적절히 설정되어 있는가?	O
12	원격 OS 인증 방식을 제한하였는가?	X
13	패스워드의 복잡도를 설정하였는가?	O
14	패스워드를 주기적으로 변경하도록 설정하였는가?	O
15	Listener 패스워드 설정을 하였는가?	X
16	보안에 허약한 PL/SQL 패키지를 제거하였는가?	O

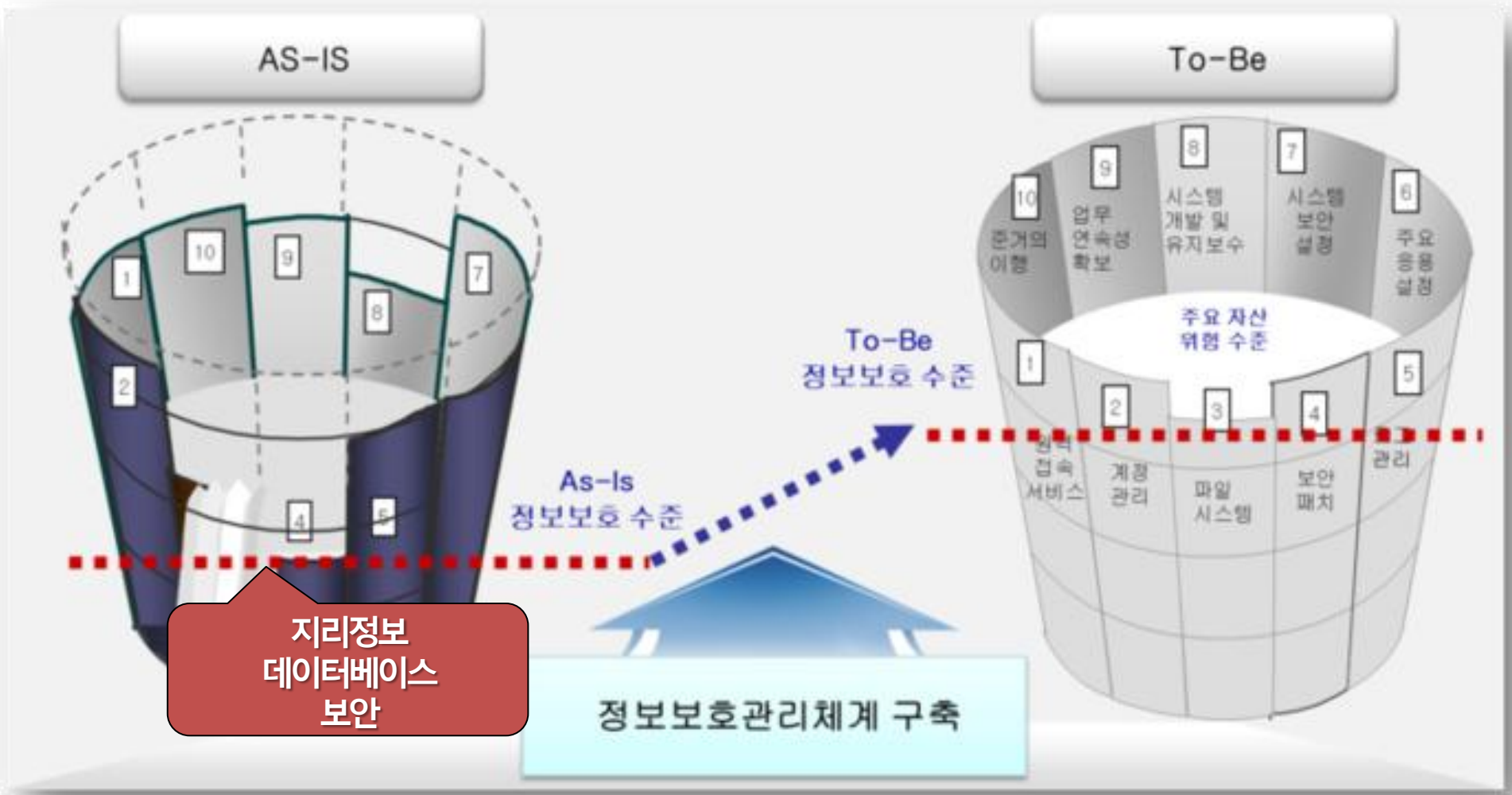
점검그룹별 취약점 분포



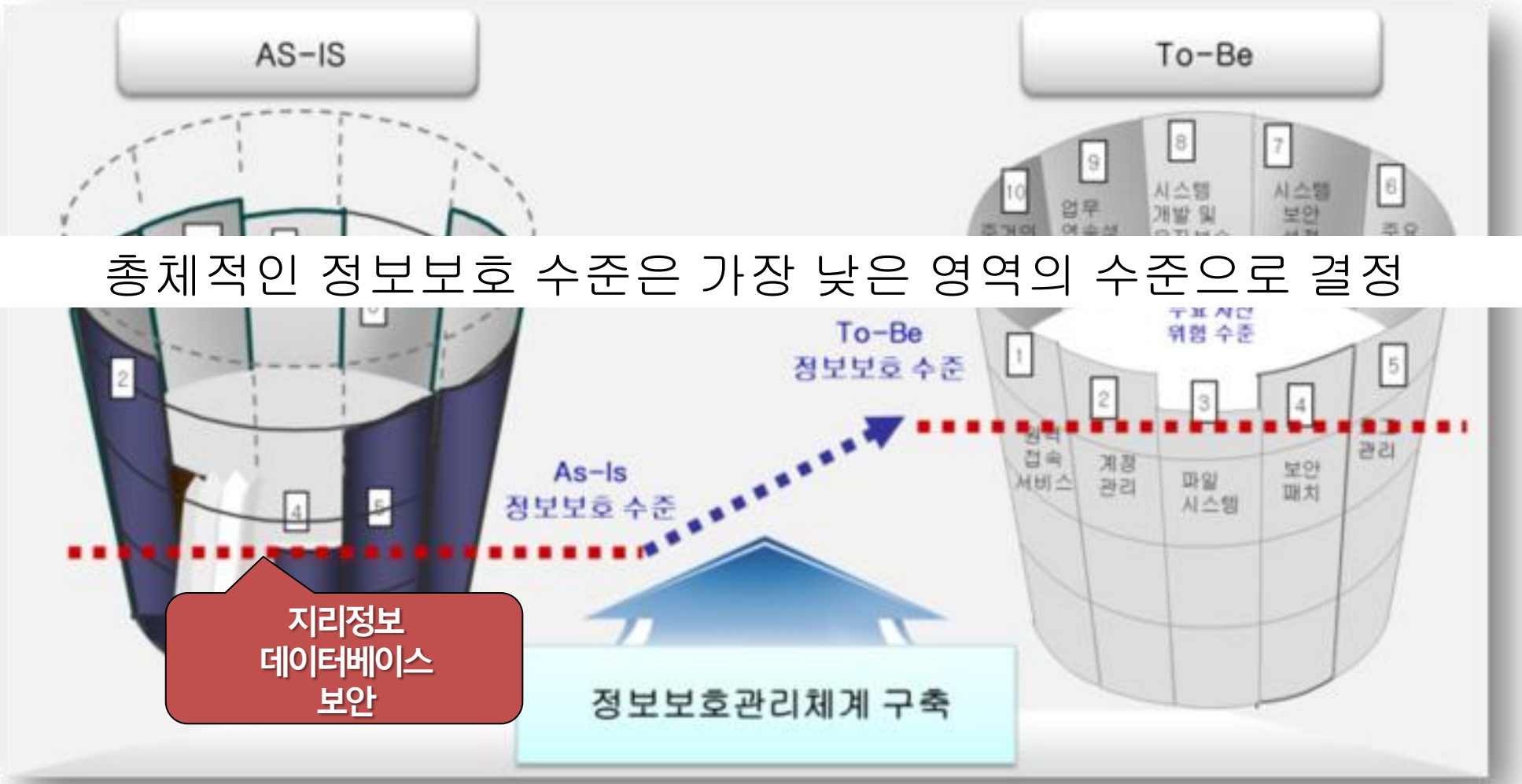
❖ 자산, 위협, 취약점, 위험


균형잡힌 보안운영체계 구축
주요 전력설비의 지리정보 DB 보안강화
관리적 보안 대책
물리적 보안대책
기술적 보안대책
보안조직체계
세부업무분장
보안관리체계
정보자산통제
인적보안
시설보안
설비관리취급
시스템운영계획
기관간망연계
일반관리방안
시스템보안
네트워크보안
운영관리
전산자료 보호대책
재해복구 계획 및 상시운영계획
컴플라이언스
법 령
규 정
지 침
정 책
사업계획
• 사업목적
• 주요기능
• 운영현황
• 시스템구성도

❖ 균형잡힌 정보호체계 구축



❖ **균형잡힌 정보호체계 구축**



❖ 목표 및 추진 과제

목표

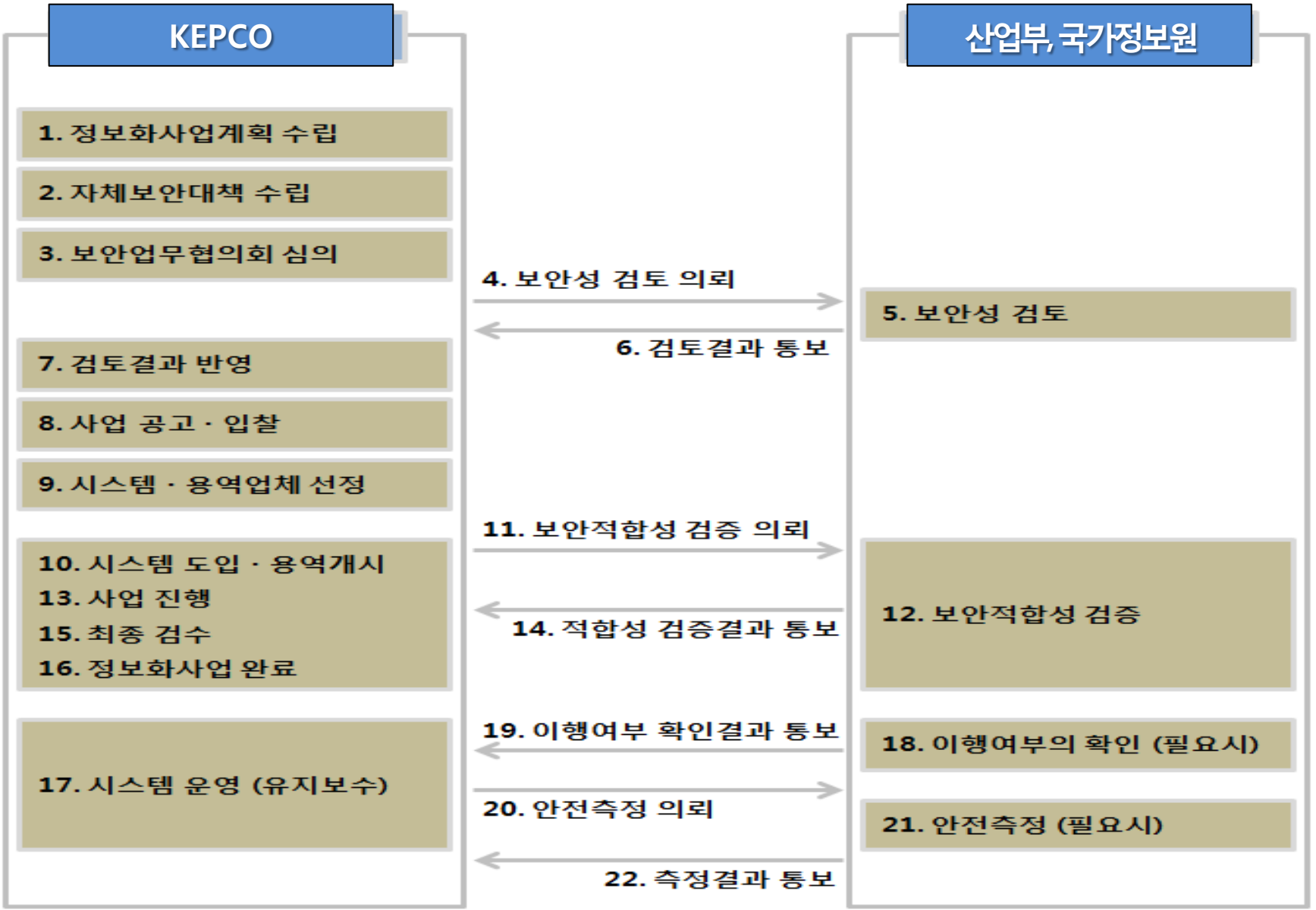
지리정보 DB 강화를 통한
『균형잡힌 정보보안 체계 구축』

분야

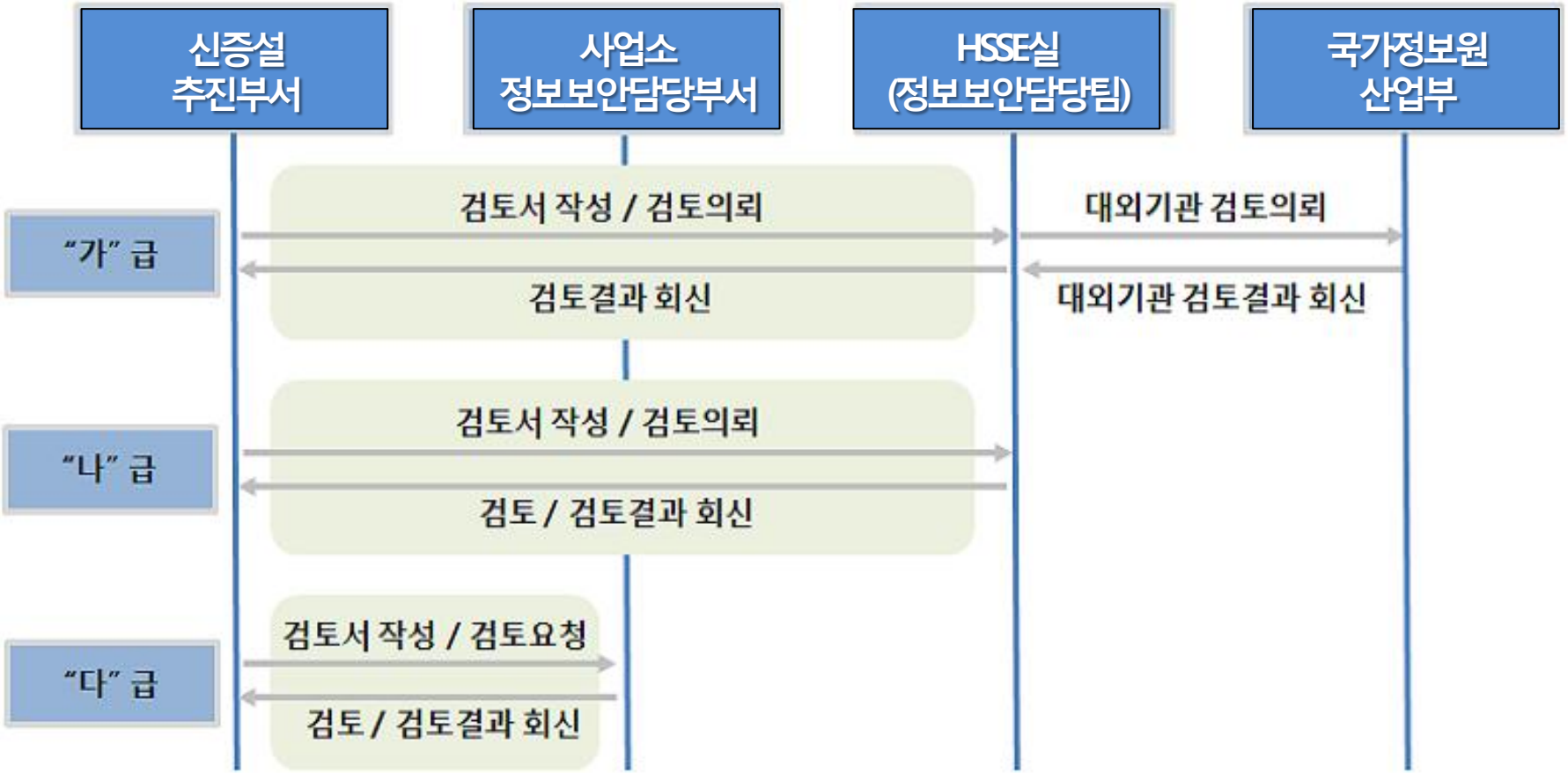
추진 과제

네트워크 보안대책	시스템 보안대책	DB 보안대책
보안 서버 구축 취약점 분석	보안운영체제 취약점 분석	접근제어 DB암호화
FireWall DDos IPS IDS	로그온 및 계정관리 접근제어/SSH, TCP Wrap 시스템설정 및 관리 감사 및 침입탐지	로그온 및 계정관리 시스템설정 및 관리 감사 및 로그

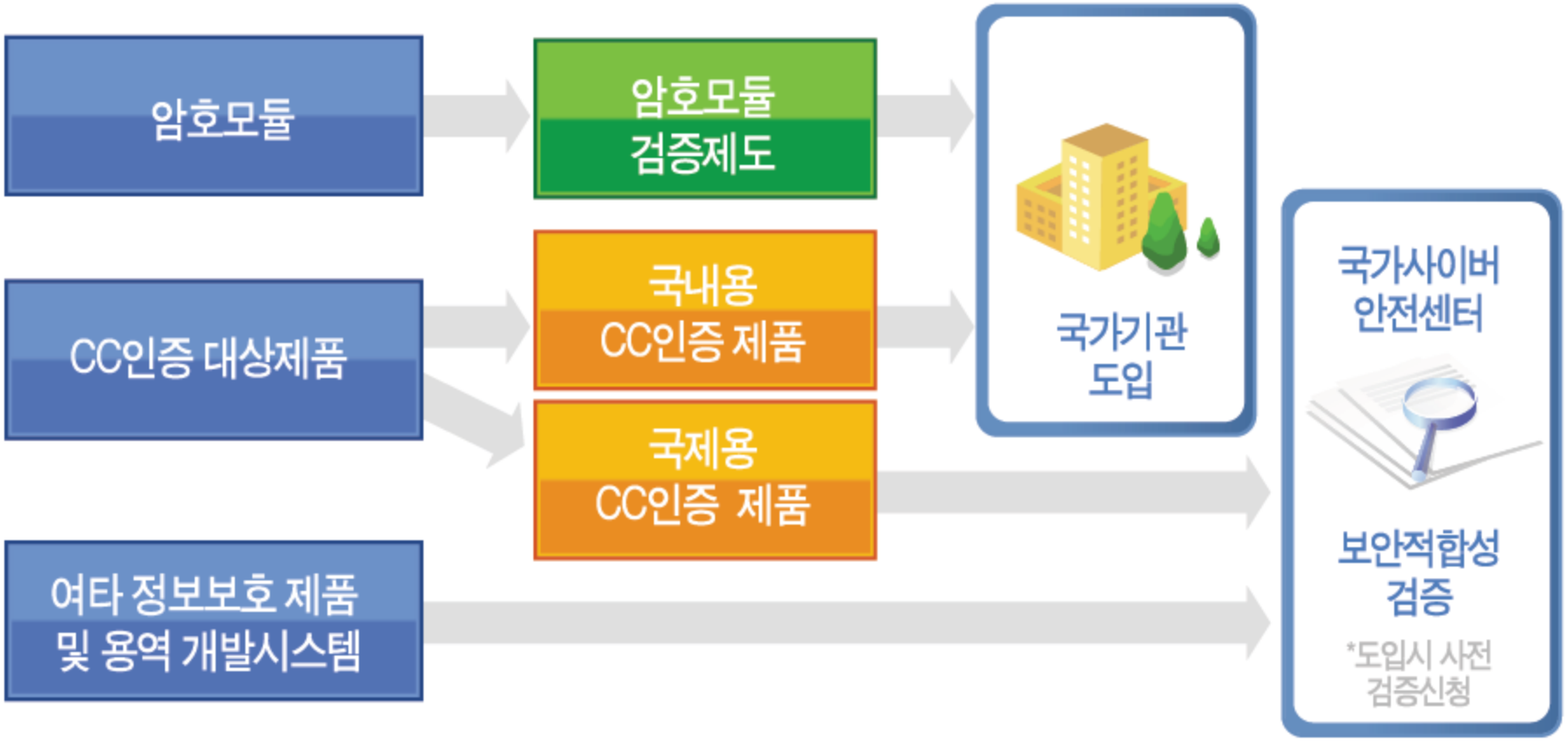
❖ 정보화 사업 추진 절차


KEPCO
산업부, 국가정보원
1. 정보화사업계획 수립
2. 자체보안대책 수립
3. 보안업무협의회 심의
4. 보안성 검토 의뢰
5. 보안성 검토
6. 검토결과 통보
7. 검토결과 반영
8. 사업 공고 · 입찰
9. 시스템 · 용역업체 선정
11. 보안적합성 검증 의뢰
10. 시스템 도입 · 용역개시
13. 사업 진행
15. 최종 검수
16. 정보화사업 완료
12. 보안적합성 검증
14. 적합성 검증결과 통보
19. 이행여부 확인결과 통보
18. 이행여부의 확인 (필요시)
17. 시스템 운영 (유지보수)
20. 안전측정 의뢰
21. 안전측정 (필요시)
22. 측정결과 통보

❖ 보안성 검토 절차


신증설
추진부서
사업소
정보보안담당부서
HSSE실
(정보보안담당팀)
국가정보원
산업부
"가" 급
검토서 작성 / 검토의뢰
대외기관 검토의뢰
검토결과 회신
대외기관 검토결과 회신
"나" 급
검토서 작성 / 검토의뢰
검토 / 검토결과 회신
"다" 급
검토서 작성 / 검토요청
검토 / 검토결과 회신

❖ **정보보호제품 국가.공공기관 도입 절차**



정보보호시스템 도입 시 보안적합성 검증 신청

❖ 보안적합성 검증 제도

제품(모듈)명	용도	CC등급
침입차단시스템	네트워크 유입 및 유출 트래픽 통제	EAL2
침입탐지시스템	네트워크 유해트래픽 자동탐지	EAL2
침입방지시스템	네트워크 유해트래픽 침입탐지 및 자동차단	EAL2
통합보안관리 제품	복수의 관리대상 시스템 중앙통제, 보안이벤트 통합모니터링 및 분석	EAL2
웹 응용프로그램 침입차단 제품	웹기반 유해트래픽 침입탐지 및 자동차단	EAL2
가상사설망 제품	IPSec 또는 SSL 방식 가상사설망	EAL2
서버 접근통제 제품	서버 접근권한 통제 및 주요 파일 보안설정	EAL2
DB 접근통제 제품	DB 접근통제 및 데이터 유출방지	EAL2
네트워크 접근통제 제품	보안프로그램 설치 PC만 네트워크 접속허용	EAL2
인터넷전화보안 제품	인터넷전화 관련 유해트래픽 탐지 및 침입차단	EAL2
무선침입방지시스템	무선랜 환경에서 보안위협, 침입탐지 및 침입차단	EAL2
무선랜 인증 제품	인증된 사용자만 무선랜 접속을 허용	EAL2
스팸메일 차단시스템	스팸메일 유입 탐지 및 차단	EAL2
네트워크 자료유출방지 제품	네트워크 간 전송되는 트래픽을 통제하여 중요 데이터의 외부유출 차단	EAL2
호스트 자료유출방지 제품	호스트에 설치되어 매체제어 등을 통해 중요 데이터의 외부유출 차단	EAL2
안티바이러스 제품	PC에 존재하는 악성코드 탐지 및 제거	EAL2
PC 침입차단 제품	PC에 설치되어 PC로의 유입 및 유출 트래픽 통제	EAL2

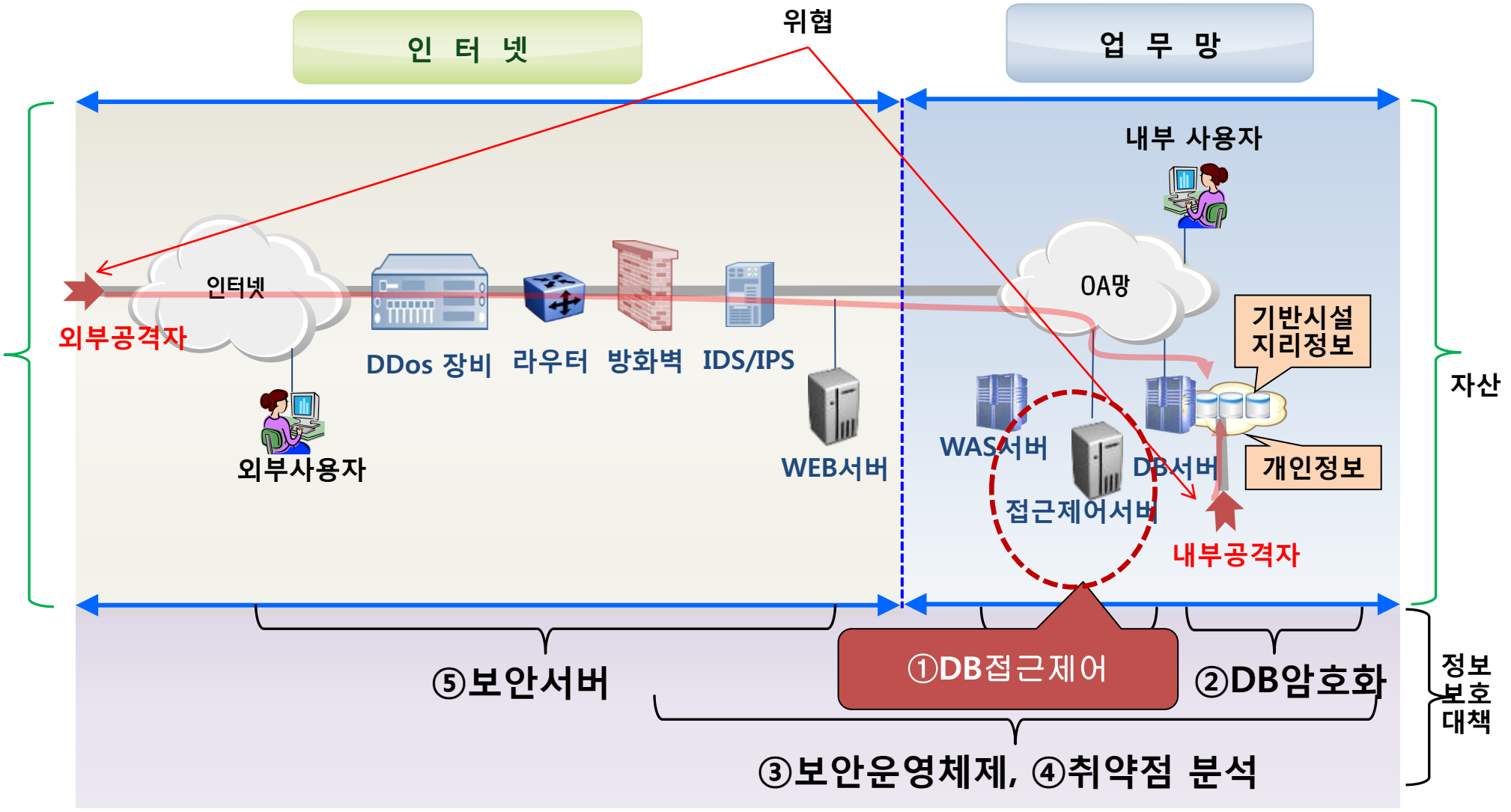
검증 생략 : 국가정보원 CC인증 제품

❖ 보안적합성 검증 제도

제품군	CC 등급	검증필 암호모듈 탑재
• 메일 암호화 모듈 • 구간 암호화 모듈 • PKI 제품 • SSO 제품 • 디스크 · 파일 암호화 제품 • 문서 암호화 제품(DRM) • 키보드 암호화 모듈 • DB 암호화 제품	해당사항 없음	필수
• 하드웨어 보안 토큰 • 기타 암호화 제품		

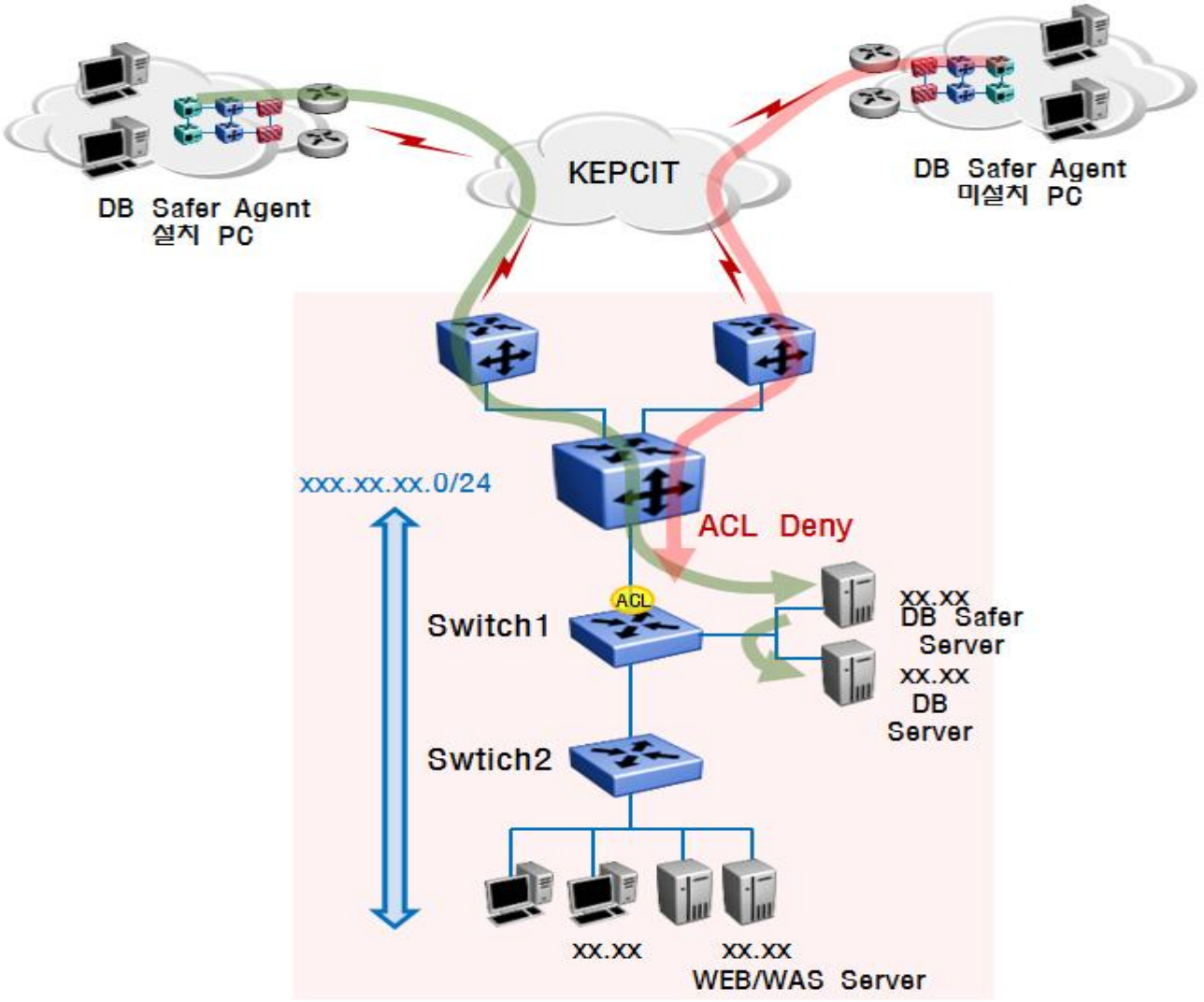
검증 생략 : 국가정보원의 안전성 확인 암호제품

❖ 지리정보 데이터베이스 보안

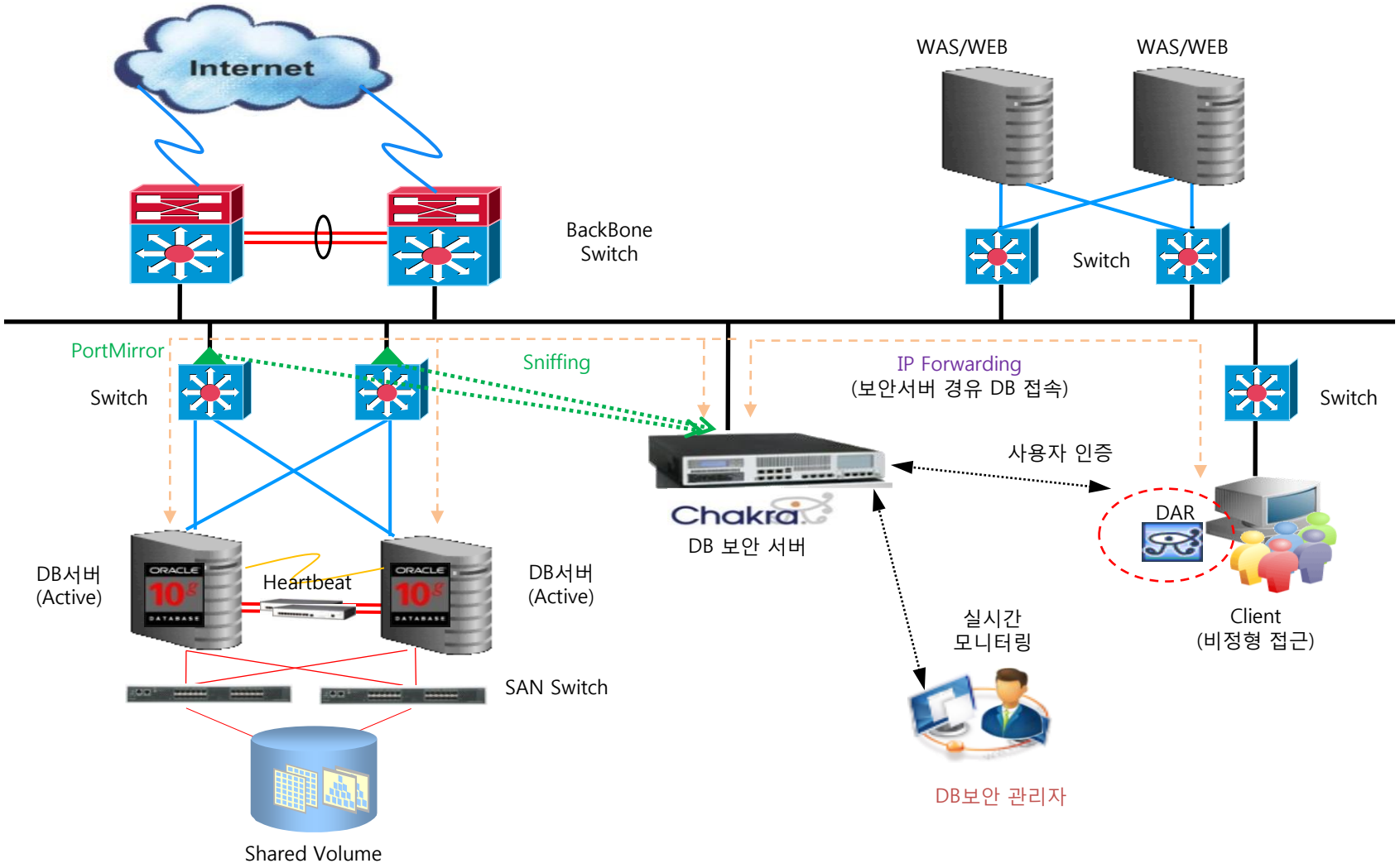


❖ 접근제어

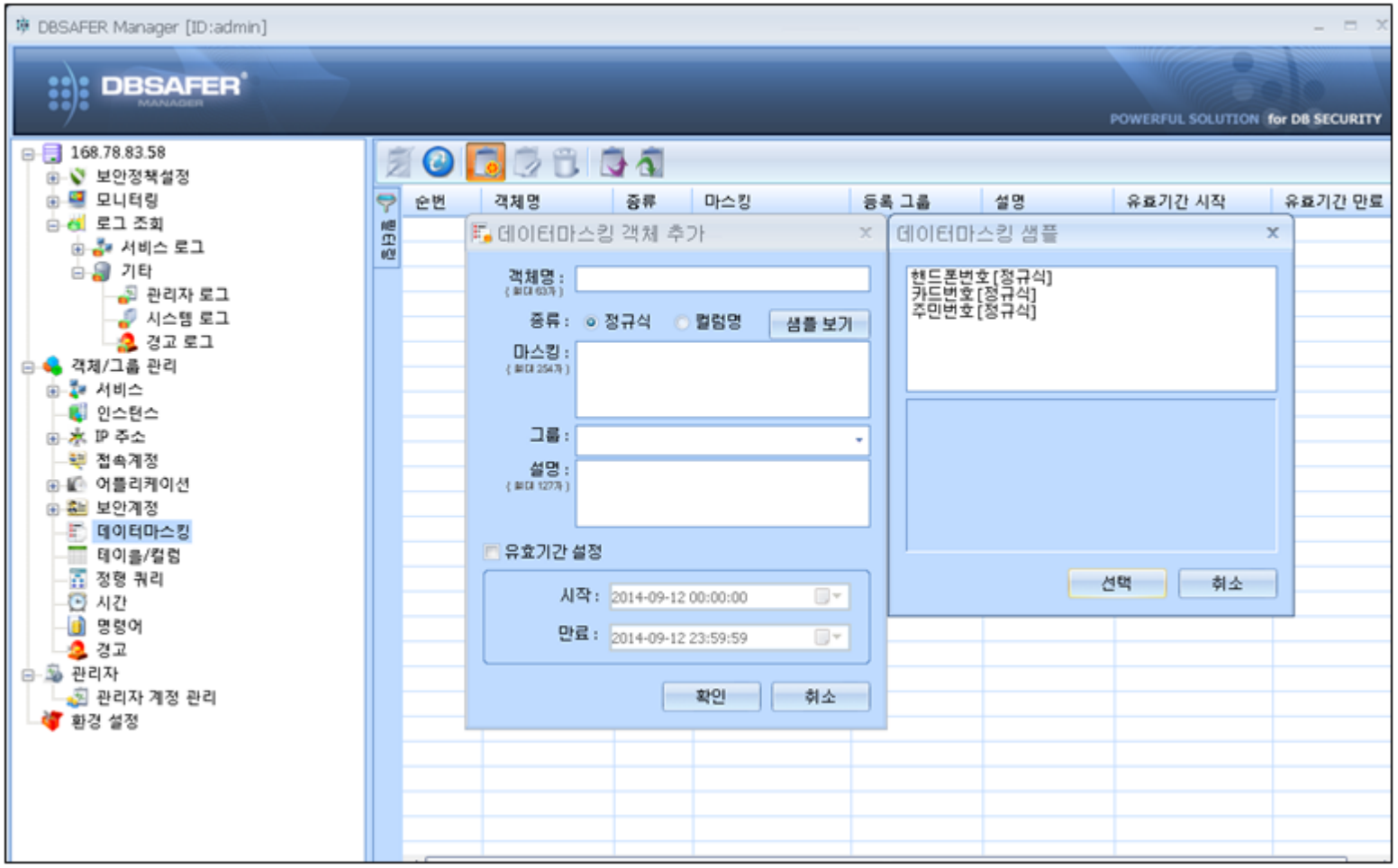
DB 접근통제 제품	DB 접근통제 및 데이터 유출방지	EAL2



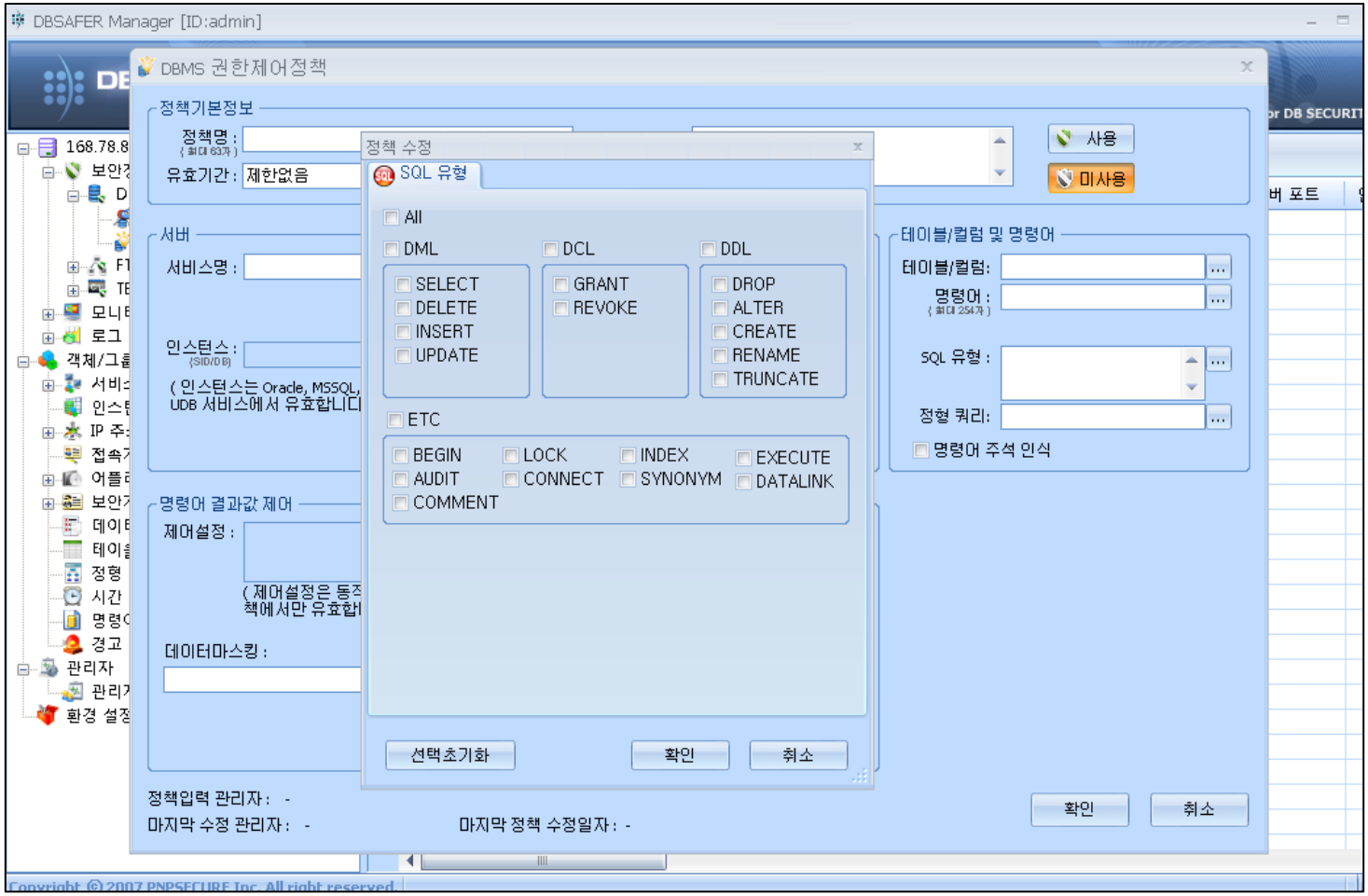
❖ 접근제어


Internet
BackBone
Switch
WAS/WEB
WAS/WEB
Switch
PortMirror
Switch
Sniffing
IP Forwarding
(보안서버 경유 DB 접속)
Switch
사용자 인증
Chakra
DB 보안 서버
DAR
DB서버
(Active)
Heartbeat
DB서버
(Active)
SAN Switch
실시간
모니터링
Client
(비정형 접근)
DB보안 관리자
Shared Volume

❖ 접근제어 : 민감정보,개인정보 마스킹



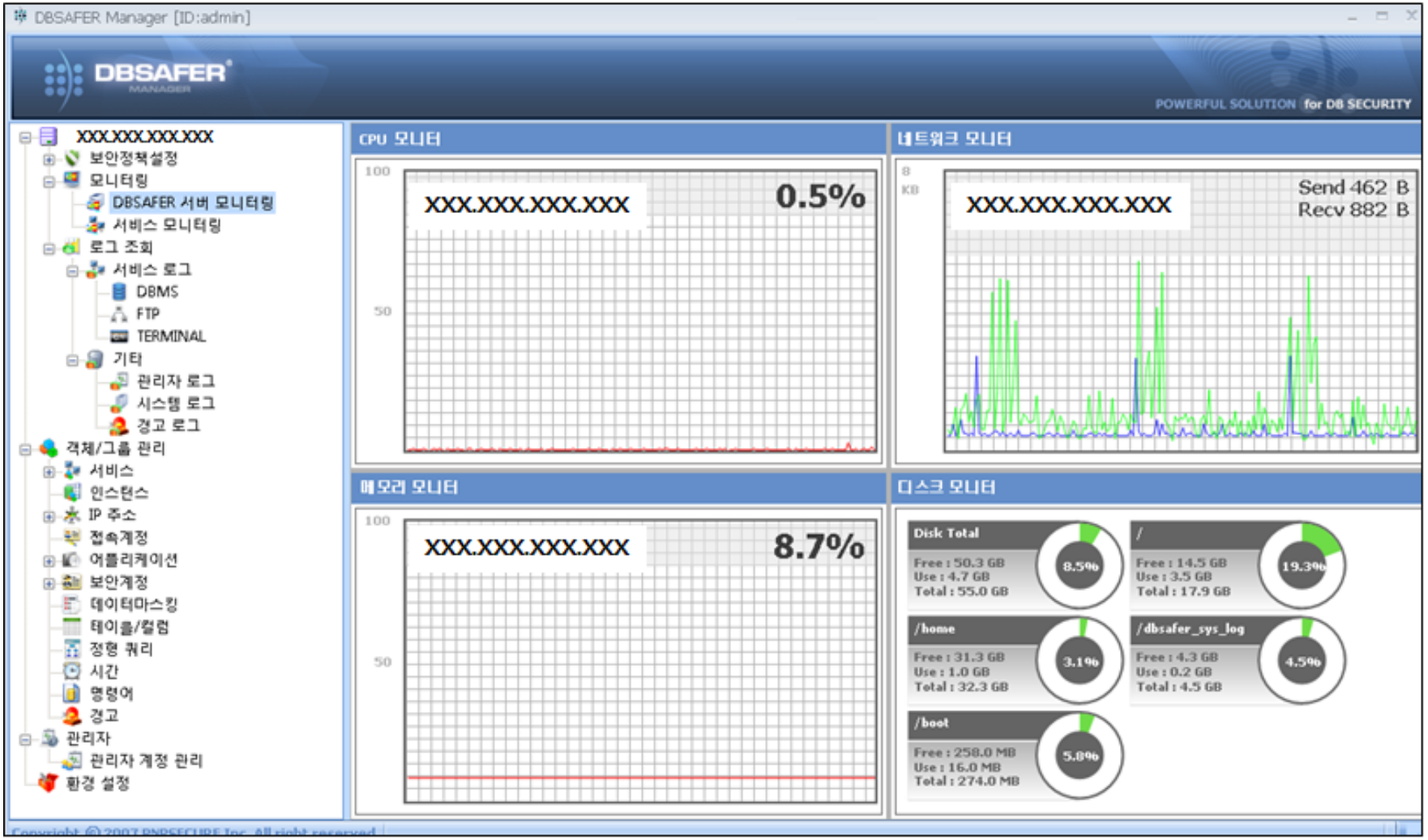
❖ 접근제어 : SQL종류별 통제



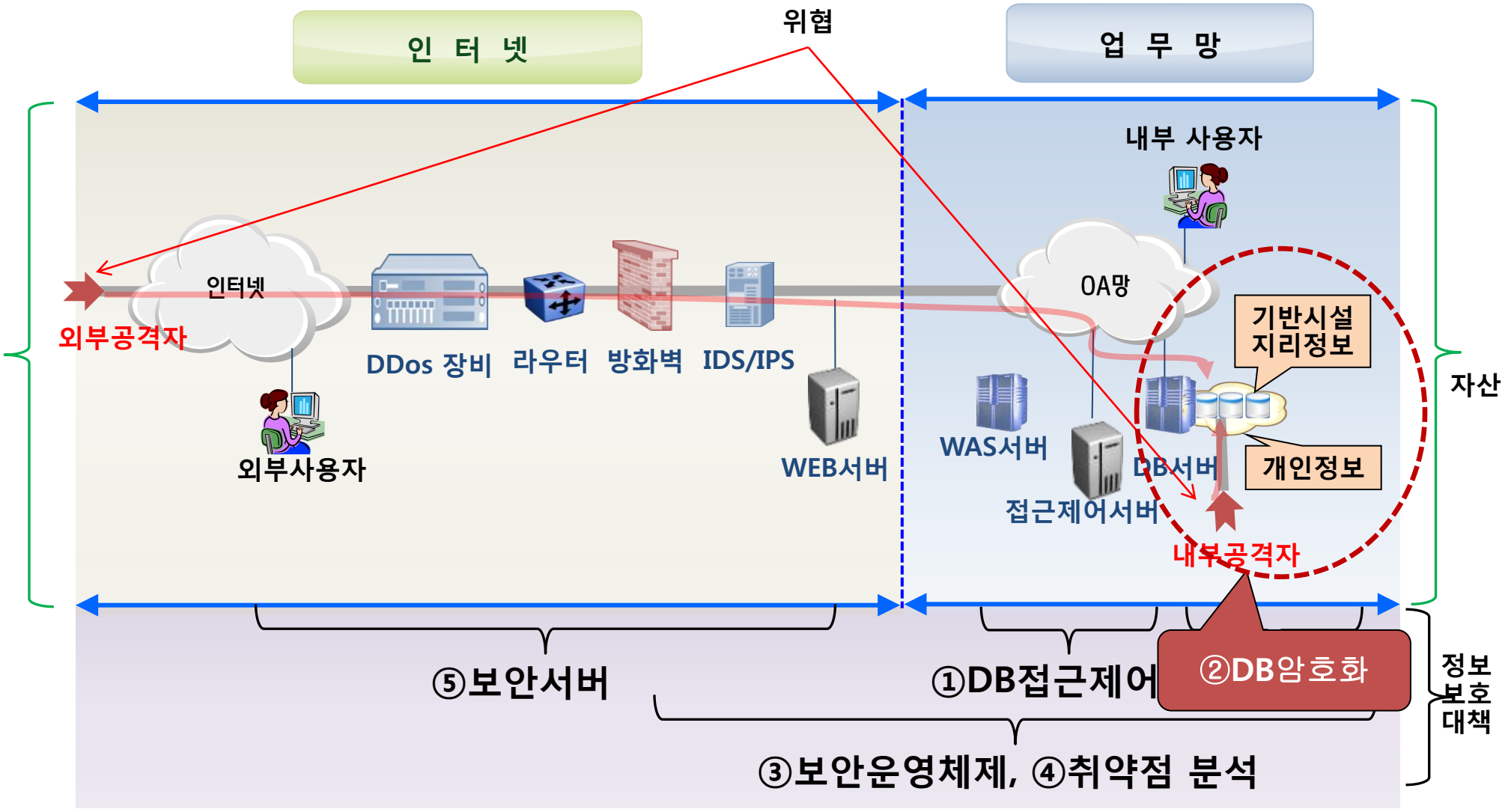
❖ 접근제어 : 수행이력로그


DBSAFER Manager [ID:admin]
DBSAFER MANAGER
POWERFUL SOLUTION for DB SECURITY
168.78.83.58
보안정책설정
DBMS
FTP
TERMINAL
모니터링
로그 조회
서비스 로그
DBMS
FTP
TERMINAL
기타
객체/그룹 관리
서비스
인스턴스
IP 주소
접속계정
어플리케이션
보안계정
데이터마스킹
테이블/컬럼
정형 쿼리
시간
명령어
경고
관리자
관리자 계정 관리
환경 설정
세션
명령어
세션상세
초기화
조회
검색조건
2014-09-12 00:00:00 ~ 2014-09-12 23:59:59 동작 전체 로그등급 1등급... 결과내 검색
명령어없는 세션 제외
서비스
전체
서버 IP:Port
IP 주소
보안계정
추가 상세 조회 >>
그룹화하여 출력시킬 로그의 컬럼을 아래에서 선택하여 여기에 끌어 놓으십시오
동작
순번
로그등급
접속계정
IP 주소
서비스 객체명
동작 모드
서버 IP주소[포트]
보안계정

❖ 접근제어 : 통계보고서

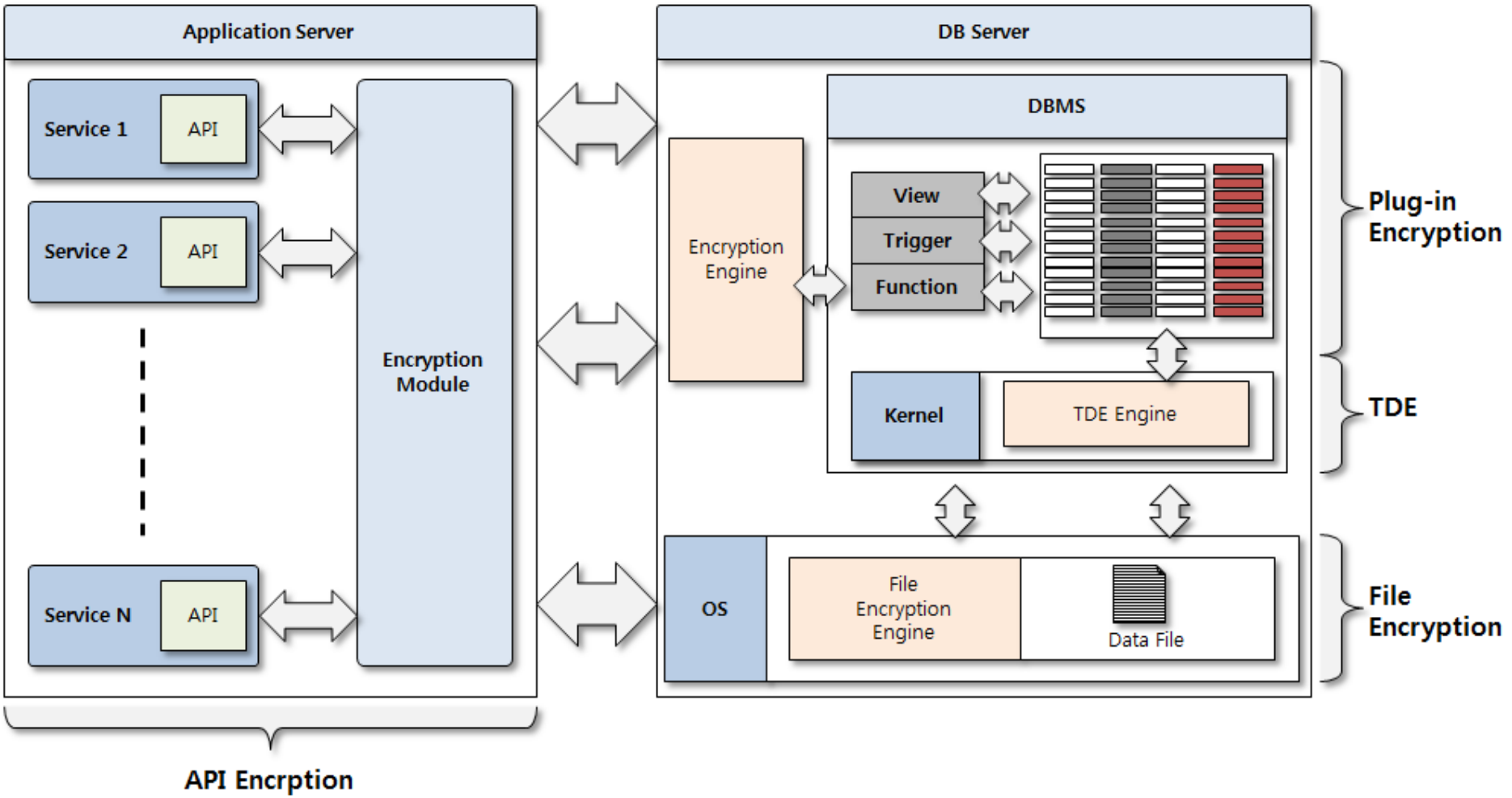

DBSAFER Manager [ID:admin]
DBSAFER
MANAGER
POWERFUL SOLUTION for DB SECURITY
XXX.XXX.XXX.XXX
보안정책설정
모니터링
DBSAFER 서버 모니터링
서비스 모니터링
로그 조회
서비스 로그
DBMS
FTP
TERMINAL
기타
관리자 로그
시스템 로그
경고 로그
객체/그룹 관리
서비스
인스턴스
IP 주소
접속계정
어플리케이션
보안계정
데이터마스킹
테이블/컬럼
정형 쿼리
시간
명령어
경고
관리자
관리자 계정 관리
환경 설정
CPU 모니터
100
50
XXX.XXX.XXX.XXX
0.5%
네트워크 모니터
8
KB
XXX.XXX.XXX.XXX
Send 462 B
Recv 882 B
메모리 모니터
100
50
XXX.XXX.XXX.XXX
8.7%
디스크 모니터
Disk Total
Free : 50.3 GB
Use : 4.7 GB
Total : 55.0 GB
8.5%
/
Free : 14.5 GB
Use : 3.5 GB
Total : 17.9 GB
19.3%
/home
Free : 31.3 GB
Use : 1.0 GB
Total : 32.3 GB
3.1%
/dbsafer_sys_log
Free : 4.3 GB
Use : 0.2 GB
Total : 4.5 GB
4.5%
/boot
Free : 258.0 MB
Use : 16.0 MB
Total : 274.0 MB
5.8%

❖ 지리정보 데이터베이스 보안

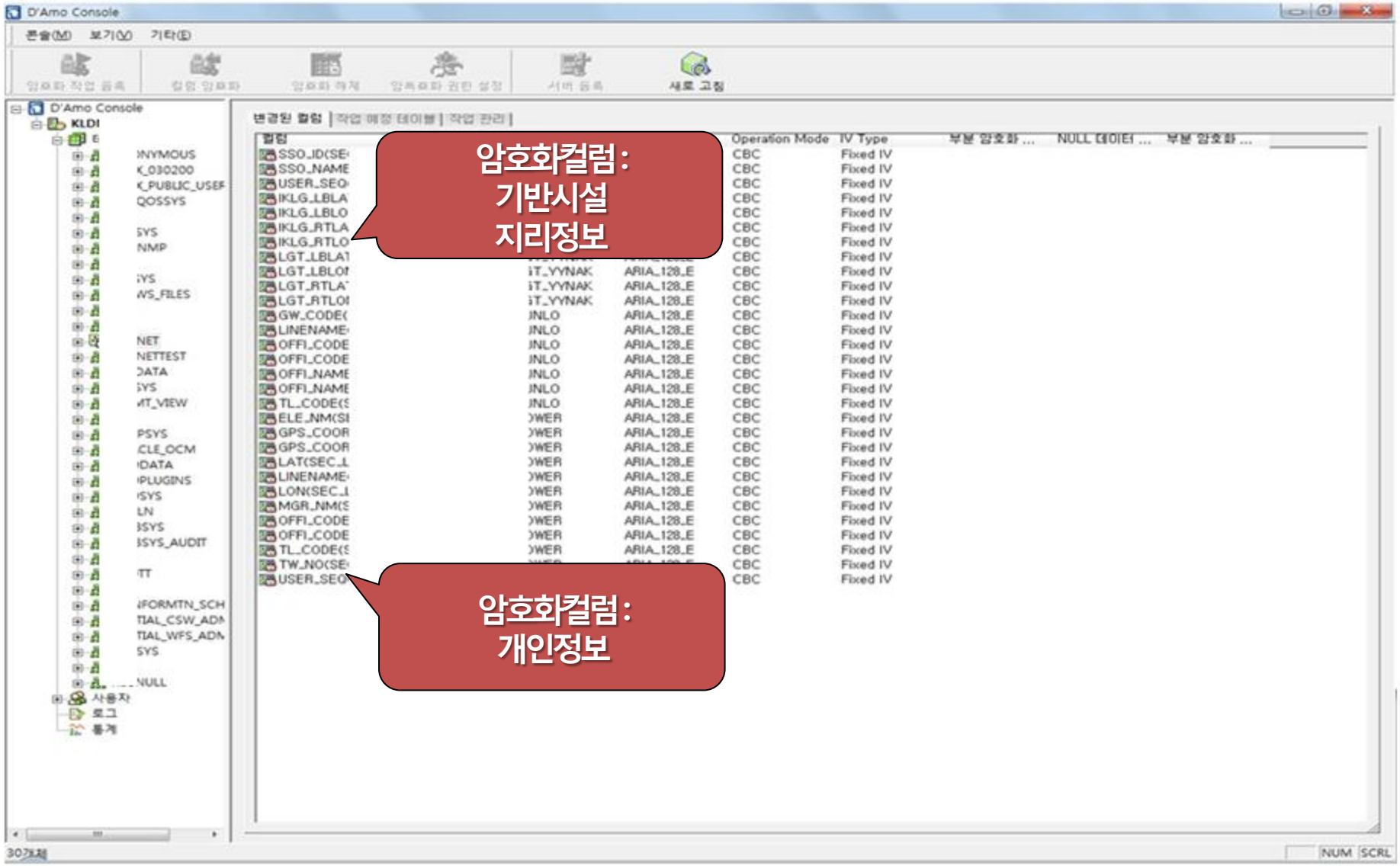


❖ DB암호화

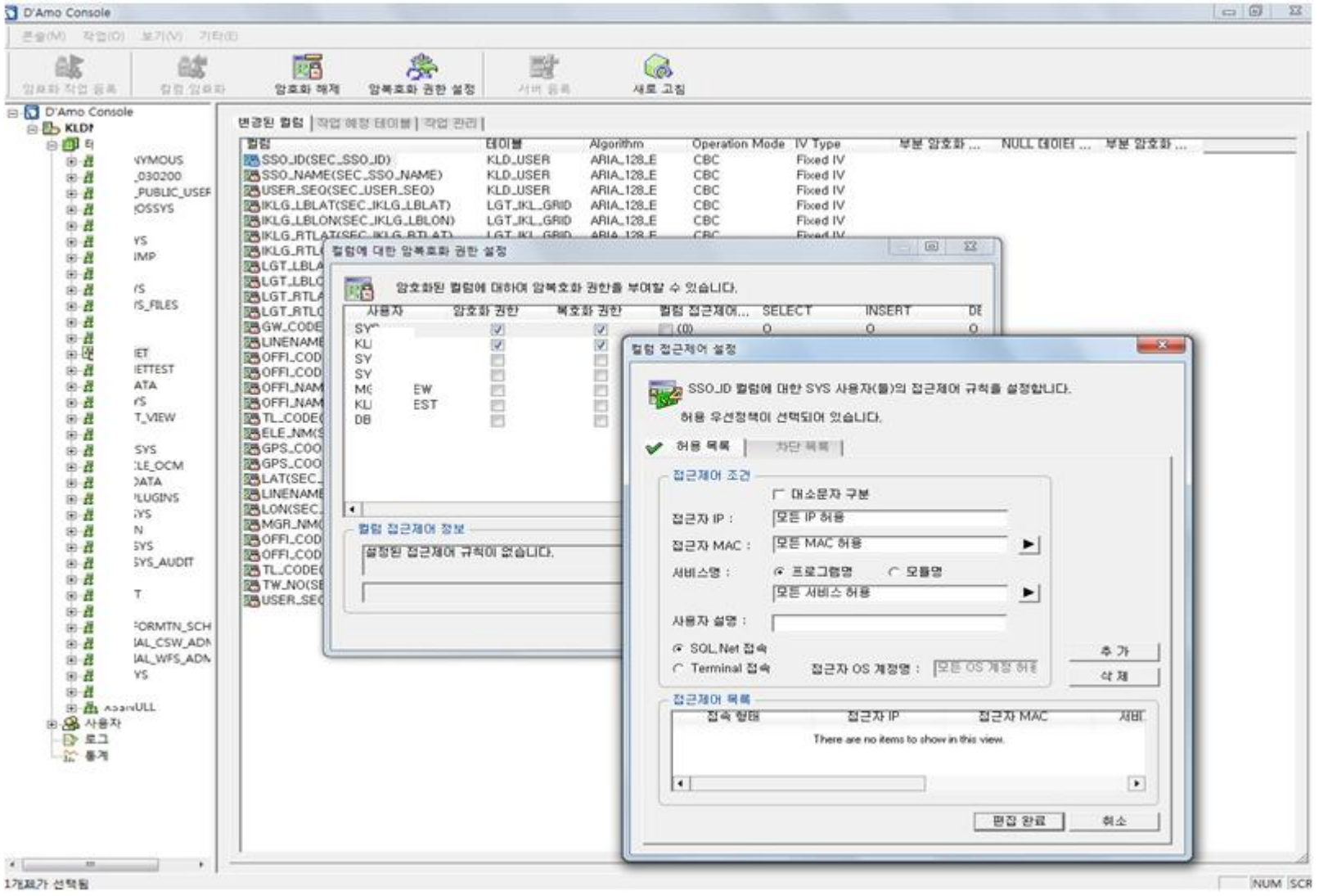
제품군	CC 등급	검증필 암호모듈 탑재
• DB 암호화 제품	해당사항 없음	필수



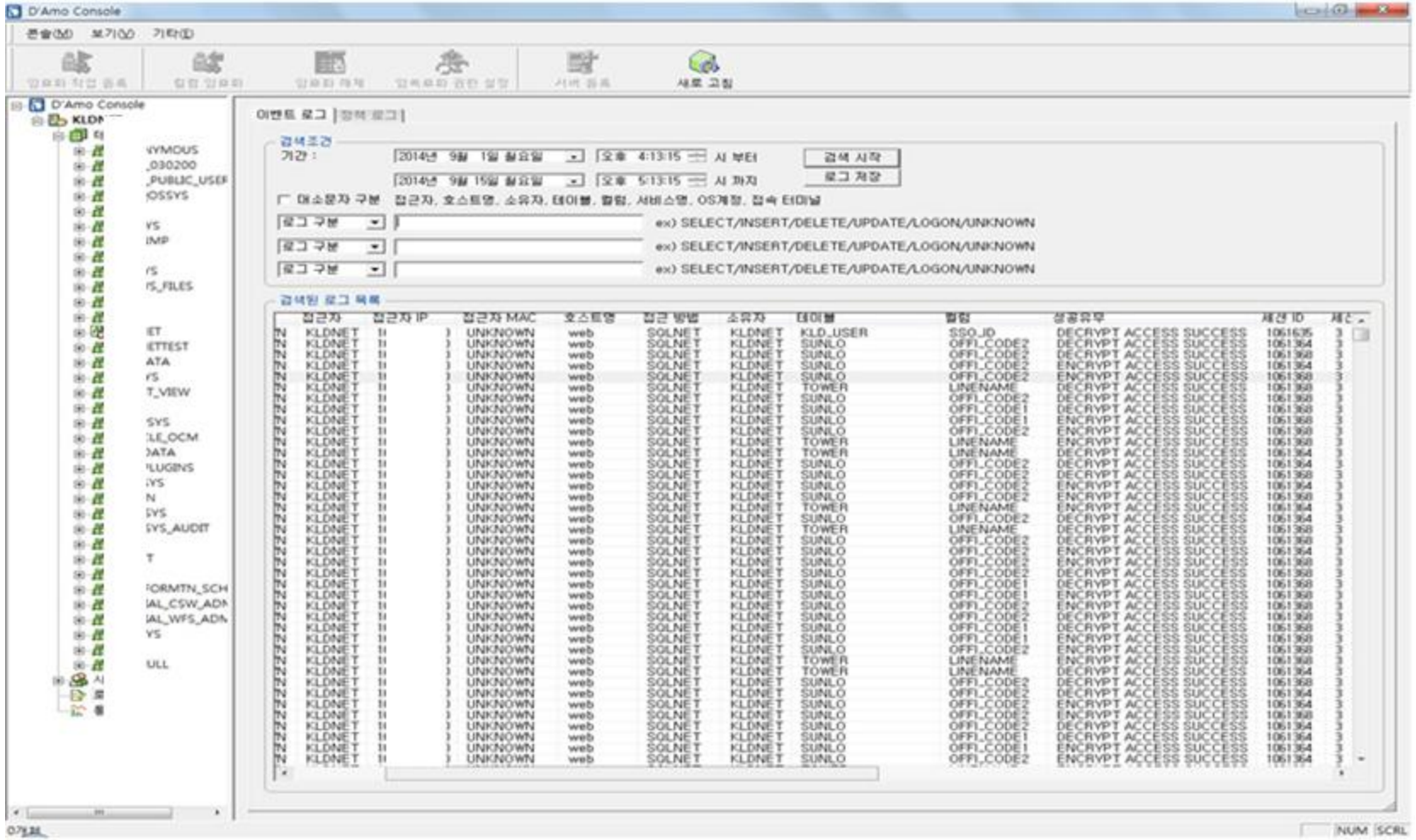
❖ DB암호화 : 암호화컬럼



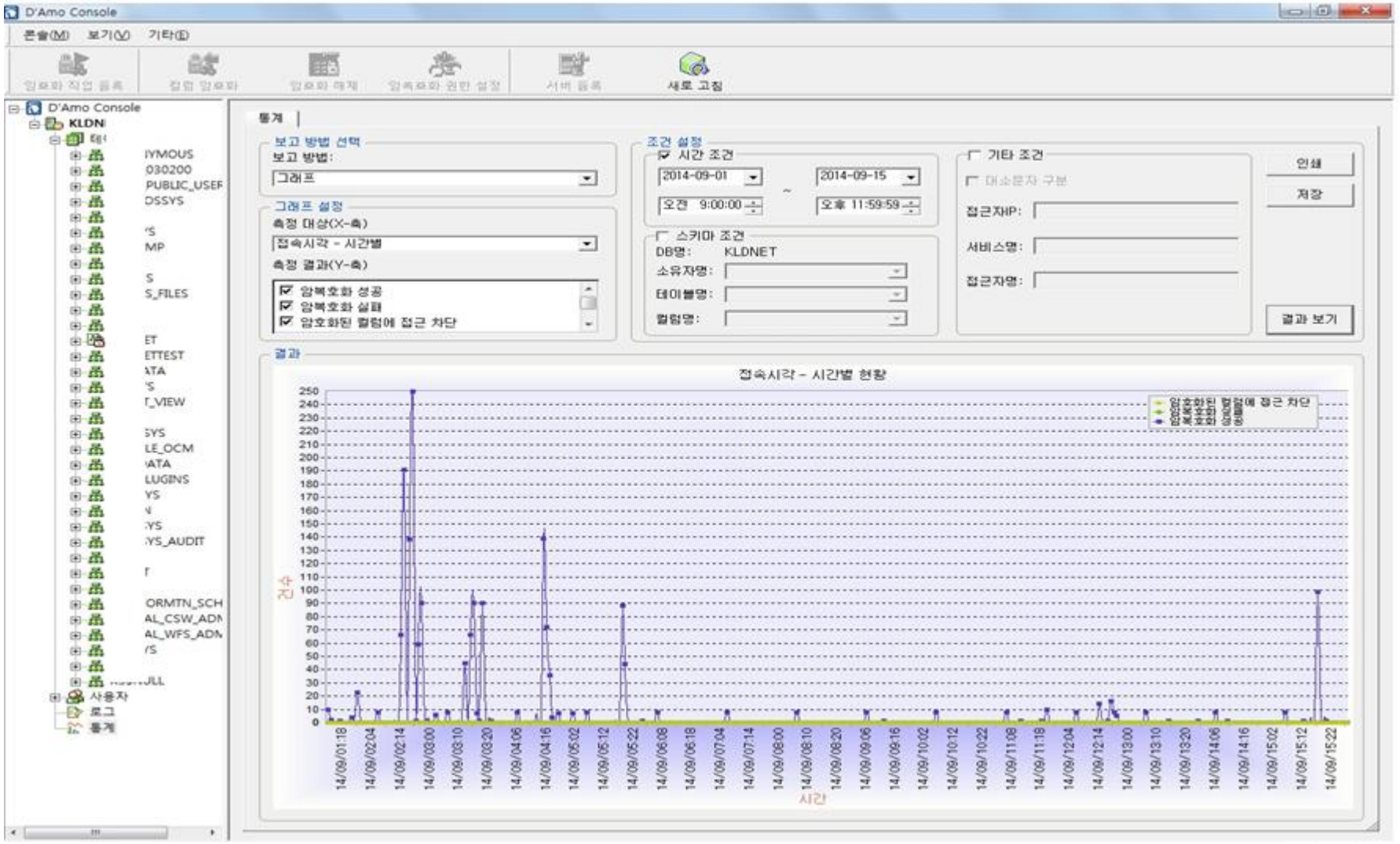
❖ DB암호화 : 암호화정책


D'Amo Console
암호화 해제
암복호화 권한 설정
새로 고침
변경된 컬럼
작업 예정 테이블
작업 관리
컬럼 Algorithm Operation Mode IV Type
SSO_ID(SEC_SSO_ID) KLD_USER ARIA_128_E CBC Fixed IV
SSO_NAME(SEC_SSO_NAME) KLD_USER ARIA_128_E CBC Fixed IV
USER_SEQ(SEC_USER_SEQ) KLD_USER ARIA_128_E CBC Fixed IV
IKLG_LBLAT(SEC_IKLG_LBLAT) LGT_IKL_GRID ARIA_128_E CBC Fixed IV
IKLG_LBLON(SEC_IKLG_LBLON) LGT_IKL_GRID ARIA_128_E CBC Fixed IV
컬럼에 대한 암복호화 권한 설정
암호화된 컬럼에 대하여 암복호화 권한을 부여할 수 있습니다.
사용자 암호화 권한 복호화 권한 컬럼 접근제어... SELECT INSERT
컬럼 접근제어 정보
설정된 접근제어 규칙이 없습니다.
컬럼 접근제어 설정
SSO_ID 컬럼에 대한 SYS 사용자(들)의 접근제어 규칙을 설정합니다.
허용 우선정책이 선택되어 있습니다.
허용 목록
차단 목록
접근제어 조건
대소문자 구분
접근자 IP : 모든 IP 허용
접근자 MAC : 모든 MAC 허용
서비스명 : 프로그램명 모듈명
모든 서비스 허용
사용자 설명 :
SQL.Net 접속
Terminal 접속
접근자 OS 계정명 : 모든 OS 계정 허용
추 가
삭 제
접근제어 목록
접속 형태 접근자 IP 접근자 MAC 서버
There are no items to show in this view.
편집 완료
취소
NUM SCR

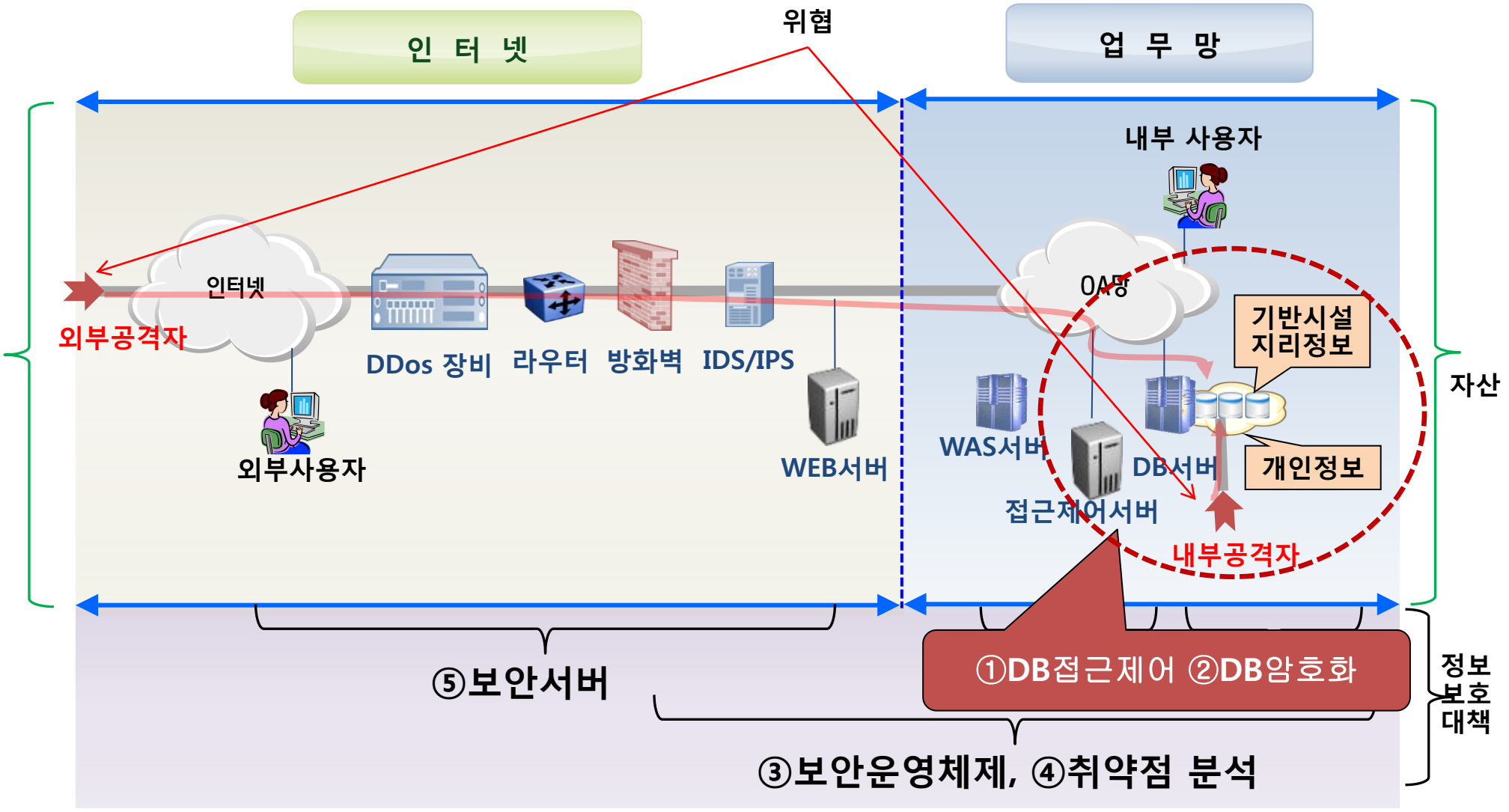
❖ **DB암호화 : 암호화로그**


D'Amo Console
새로 고침
이벤트 로그
검색조건
검색 시작
로그 저장
ex) SELECT/INSERT/DELETE/UPDATE/LOGON/UNKNOWN
검색된 로그 목록

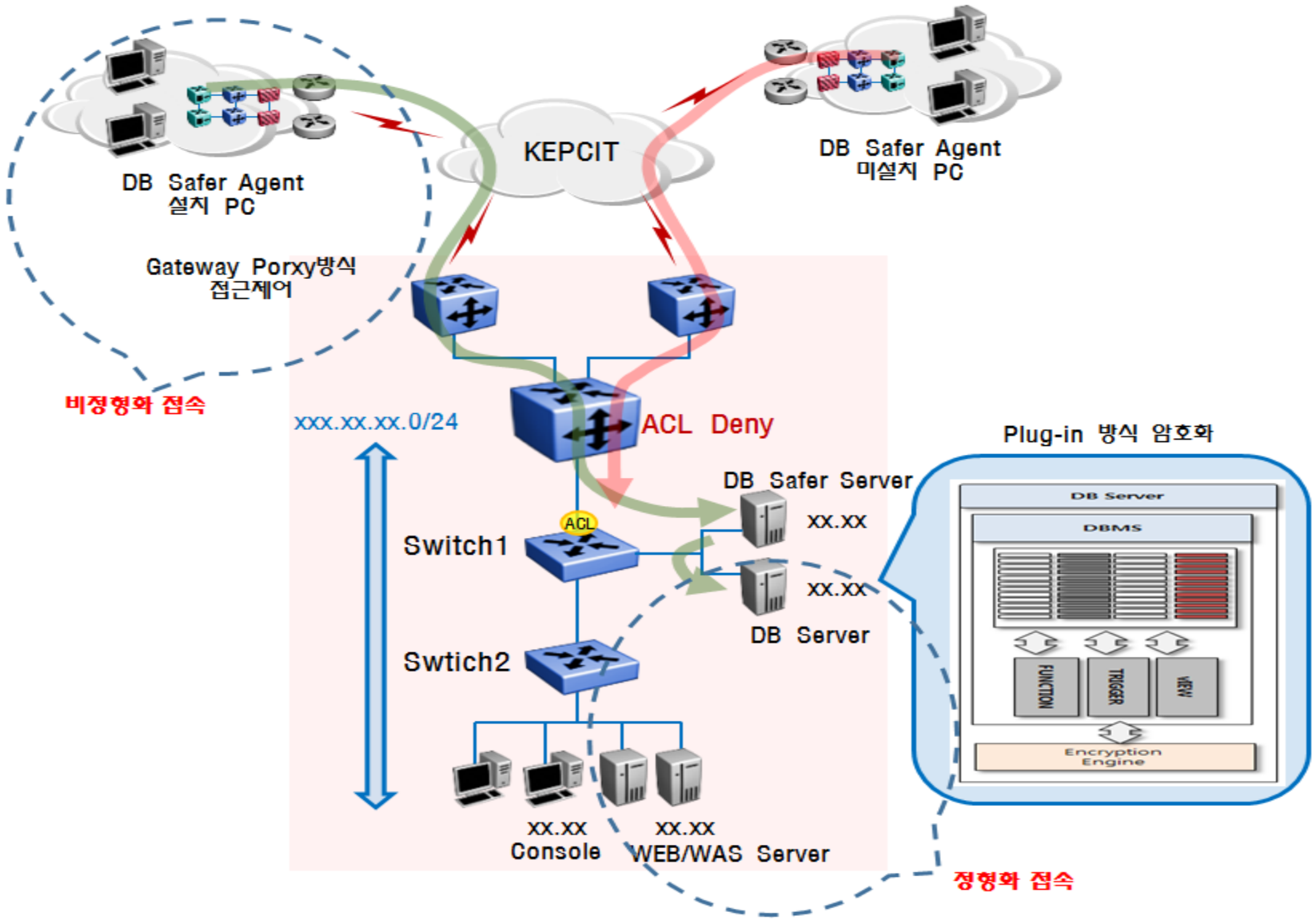
❖ DB암호화 : 통계보고서


D'Amo Console
콘솔(M) 보기(V) 기타(E)
새로 고침
D'Amo Console
KLDN
사용자
로그
통계
통계
보고 방법 선택
보고 방법:
그래프
그래프 설정
측정 대상(X-축)
접속시각 - 시간별
측정 결과(Y-축)
암복호화 성공
암복호화 실패
암호화된 컬럼에 접근 차단
조건 설정
시간 조건
2014-09-01
2014-09-15
오전 9:00:00
오후 11:59:59
스키마 조건
DB명: KLDNET
소유자명:
테이블명:
컬럼명:
기타 조건
대소문자 구분
접근자IP:
서비스명:
접근자명:
인쇄
저장
결과 보기
결과
접속시각 - 시간별 현황
건수
시간

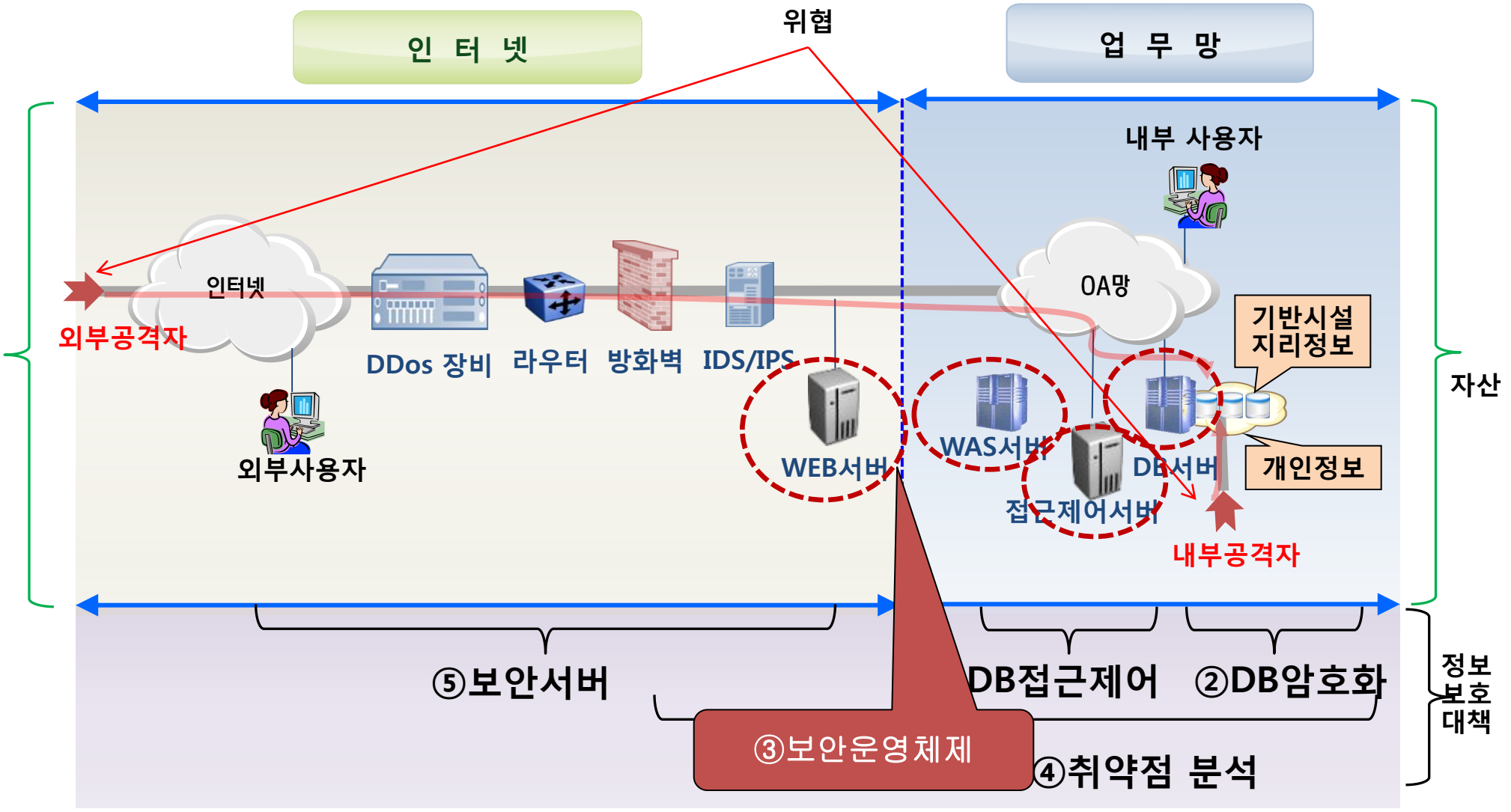
❖ 지리정보 데이터베이스 보안



❖ DB접근제어, DB암호화

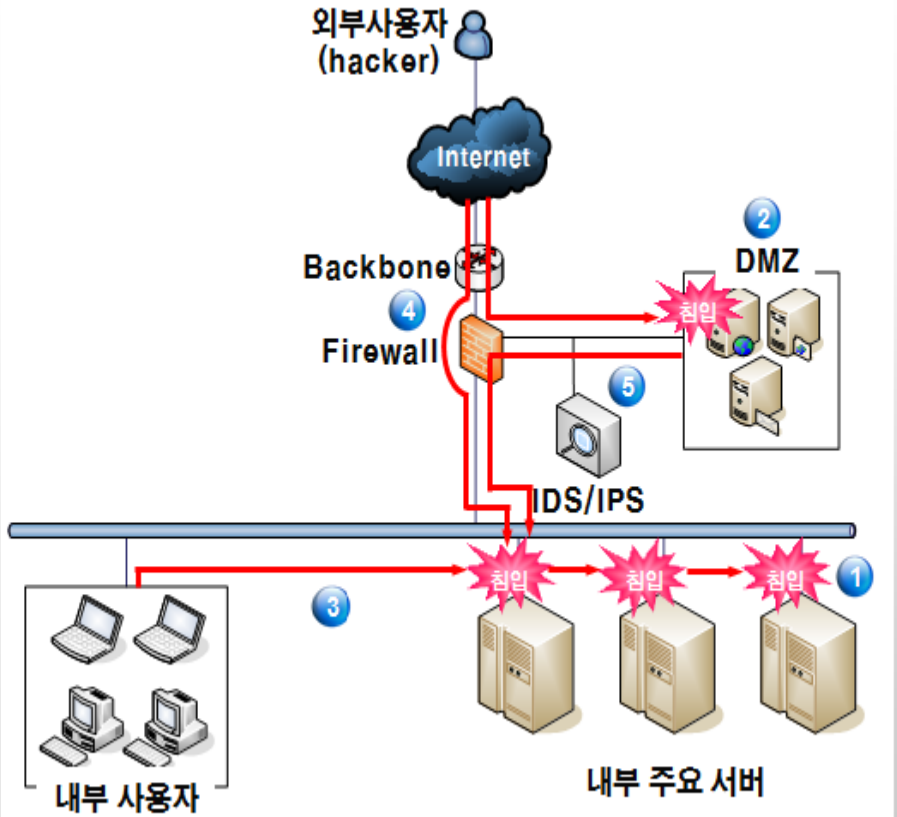


❖ 지리정보 데이터베이스 보안

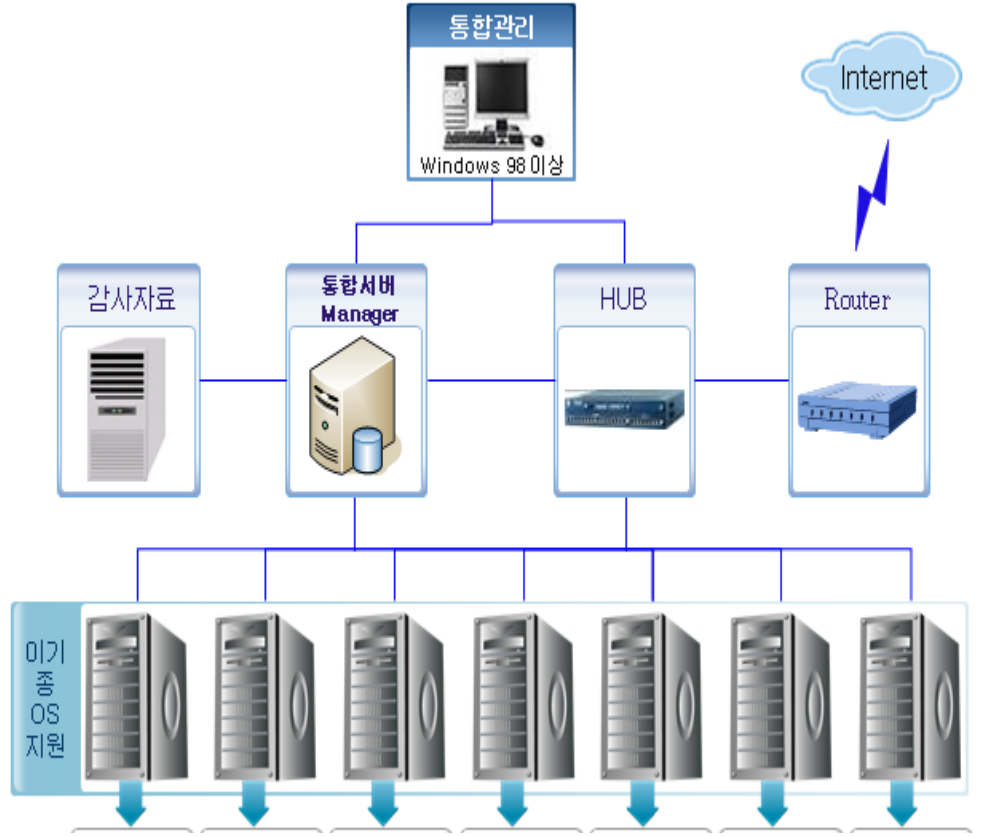


❖ 보안운영체제

네트워크 보안시스템의 한계



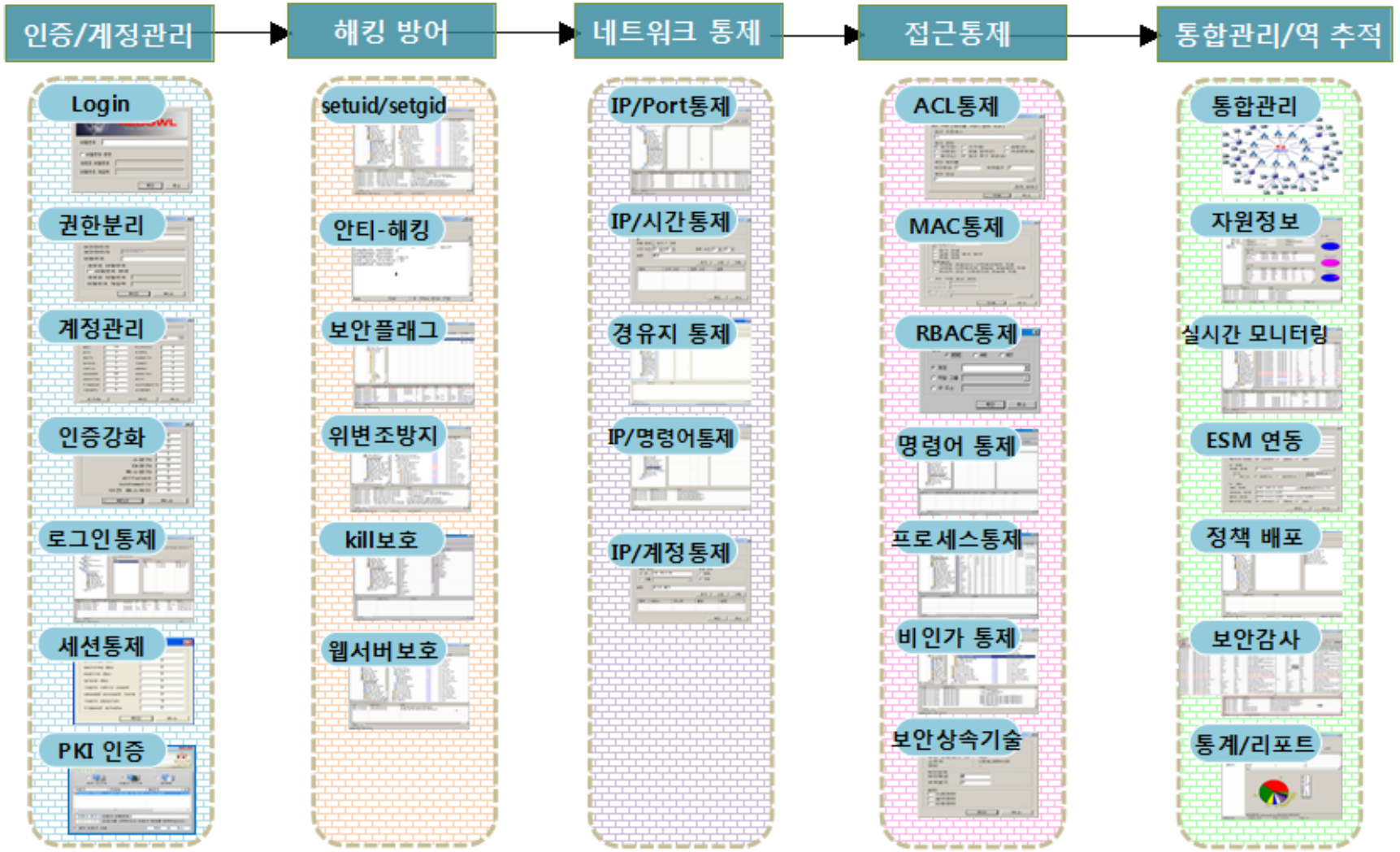
REDOWL 시스템 구성도



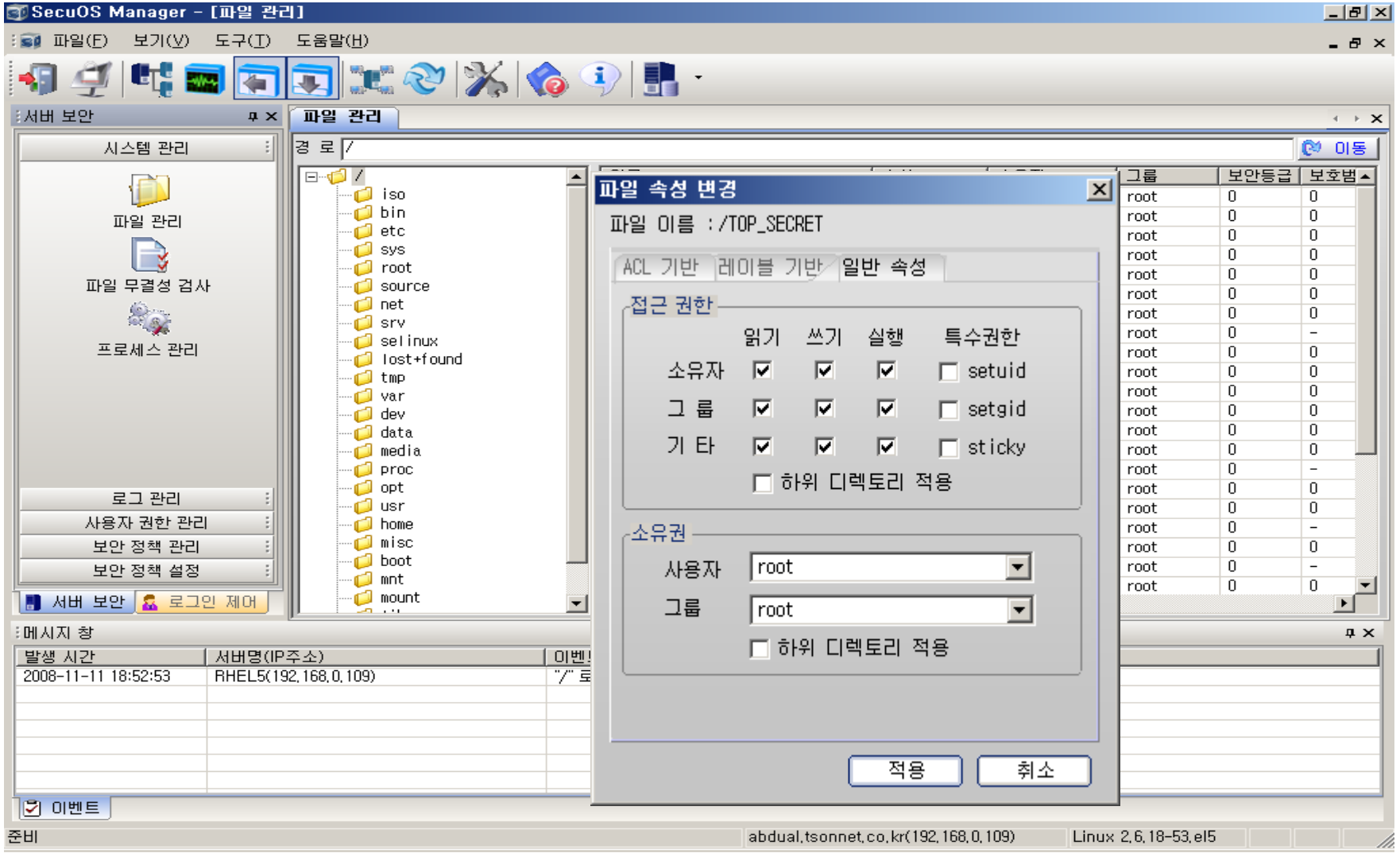
운영체제의 커널에 부가적인 보안 기능 추가한 운영체제

OS자체에 대한 보안체제, 접근제어, 해킹방지기능, 상세 로그확보 통합관리기능

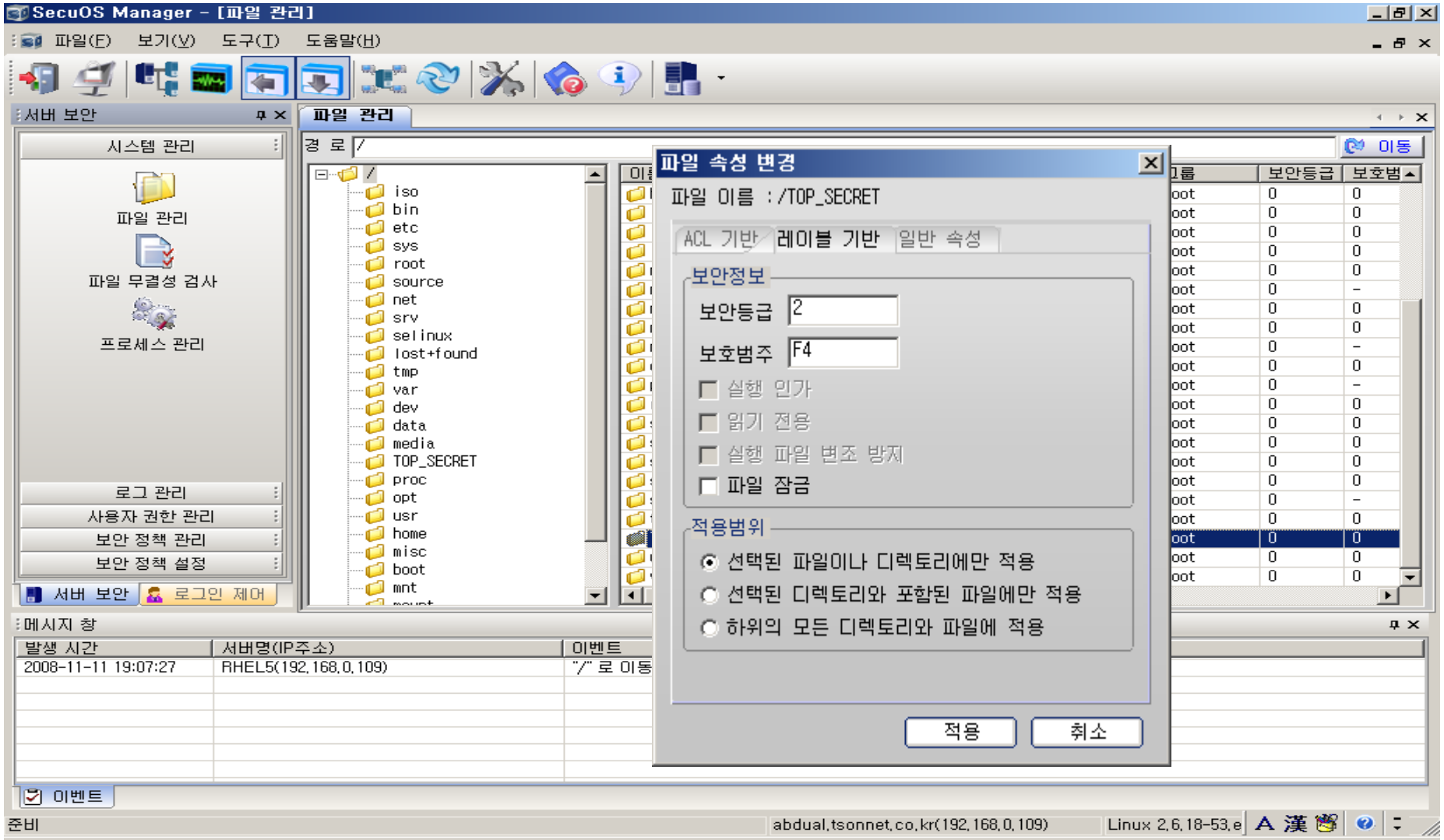
❖ 보안운영체제 주요기능


인증/계정관리
해킹 방어
네트워크 통제
접근통제
통합관리/역 추적
Login
권한분리
계정관리
인증강화
로그인통제
세션통제
PKI 인증
setuid/setgid
안티-해킹
보안플래그
위변조방지
kill보호
웹서버보호
IP/Port통제
IP/시간통제
경유지 통제
IP/명령어통제
IP/계정통제
ACL통제
MAC통제
RBAC통제
명령어 통제
프로세스통제
비인가 통제
보안상속기술
통합관리
자원정보
실시간 모니터링
ESM 연동
정책 배포
보안감사
통계/리포트

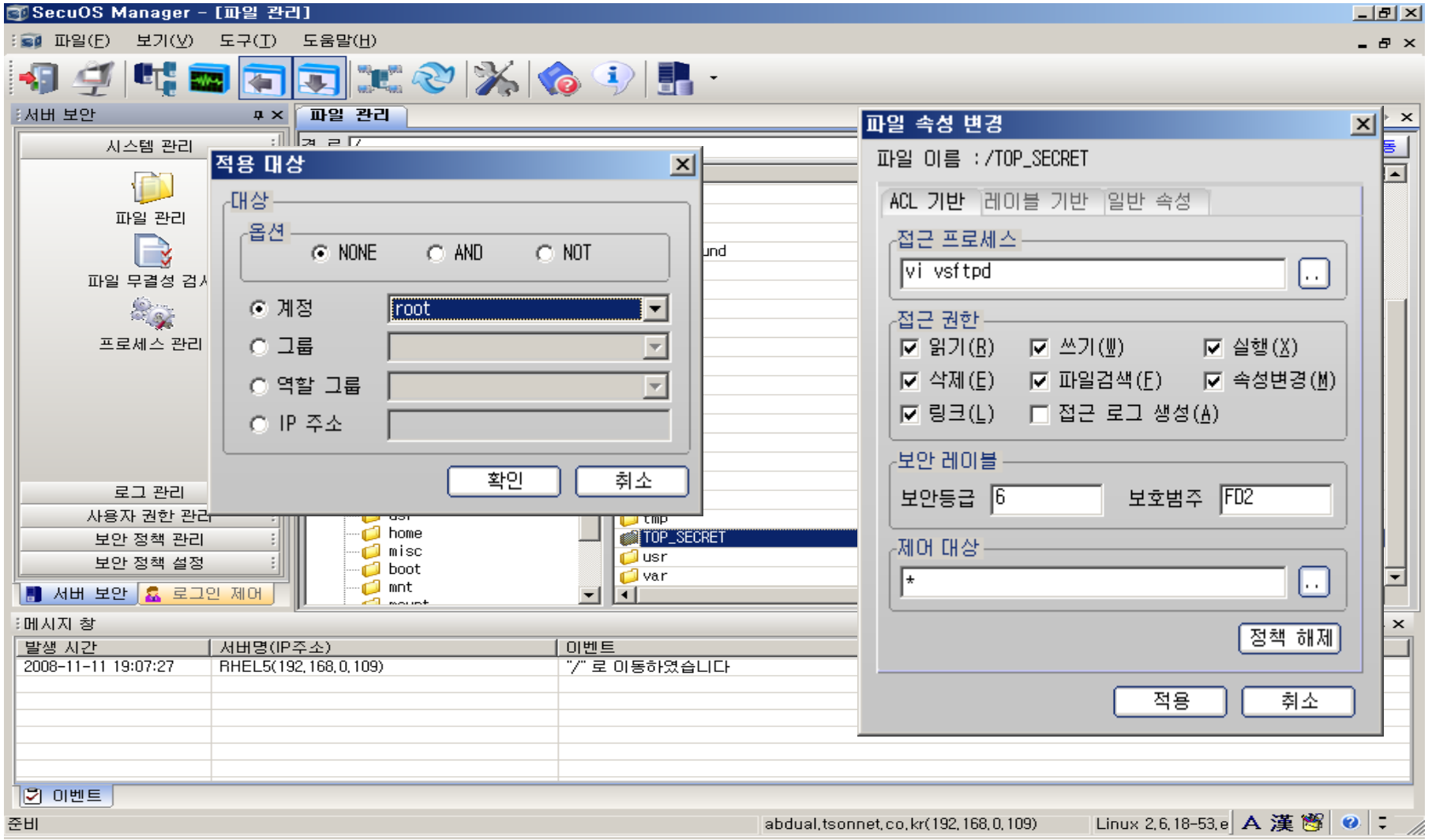
❖ 보안운영체제 : 임의적 접근제어



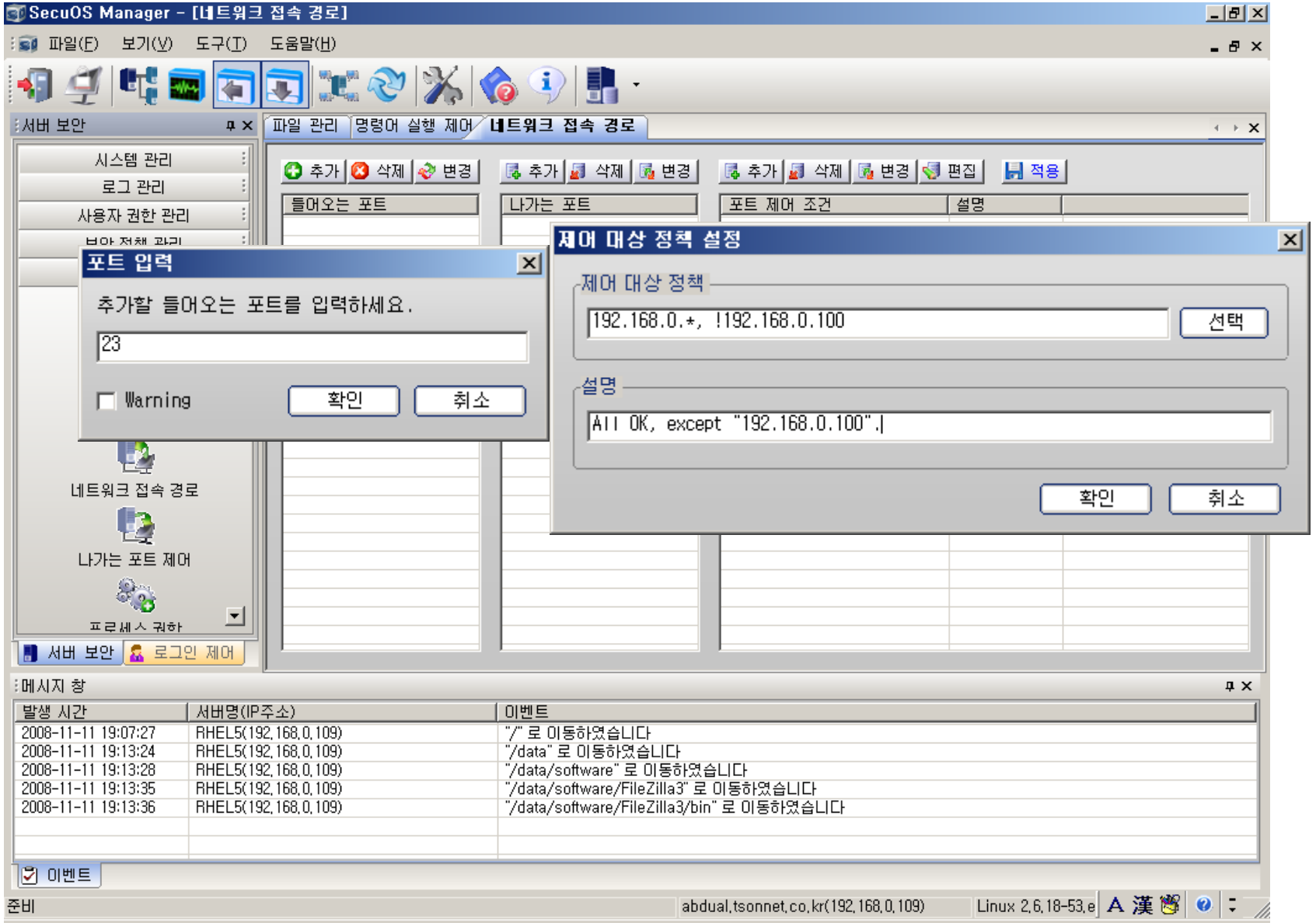
❖ 보안운영체제 : MLS


SecuOS Manager - [파일 관리]
파일(F) 보기(V) 도구(T) 도움말(H)
서버 보안
시스템 관리
파일 관리
파일 무결성 검사
프로세스 관리
로그 관리
사용자 권한 관리
보안 정책 관리
보안 정책 설정
서버 보안
로그인 제어
파일 관리
경 로 /
이동
/
iso
bin
etc
sys
root
source
net
srv
selinux
lost+found
tmp
var
dev
data
media
TOP_SECRET
proc
opt
usr
home
misc
boot
mnt
보안등급
보호범
파일 속성 변경
파일 이름 :/TOP_SECRET
ACL 기반
레이블 기반
일반 속성
보안정보
보안등급 2
보호범주 F4
실행 인가
읽기 전용
실행 파일 변조 방지
파일 잠금
적용범위
선택된 파일이나 디렉토리에만 적용
선택된 디렉토리와 포함된 파일에만 적용
하위의 모든 디렉토리와 파일에 적용
적용
취소
메시지 창
발생 시간
서버명(IP주소)
이벤트
2008-11-11 19:07:27
RHEL5(192.168.0.109)
"/" 로 이동
이벤트
준비
abdual.tsonnet.co.kr(192.168.0.109)
Linux 2.6.18-53.e

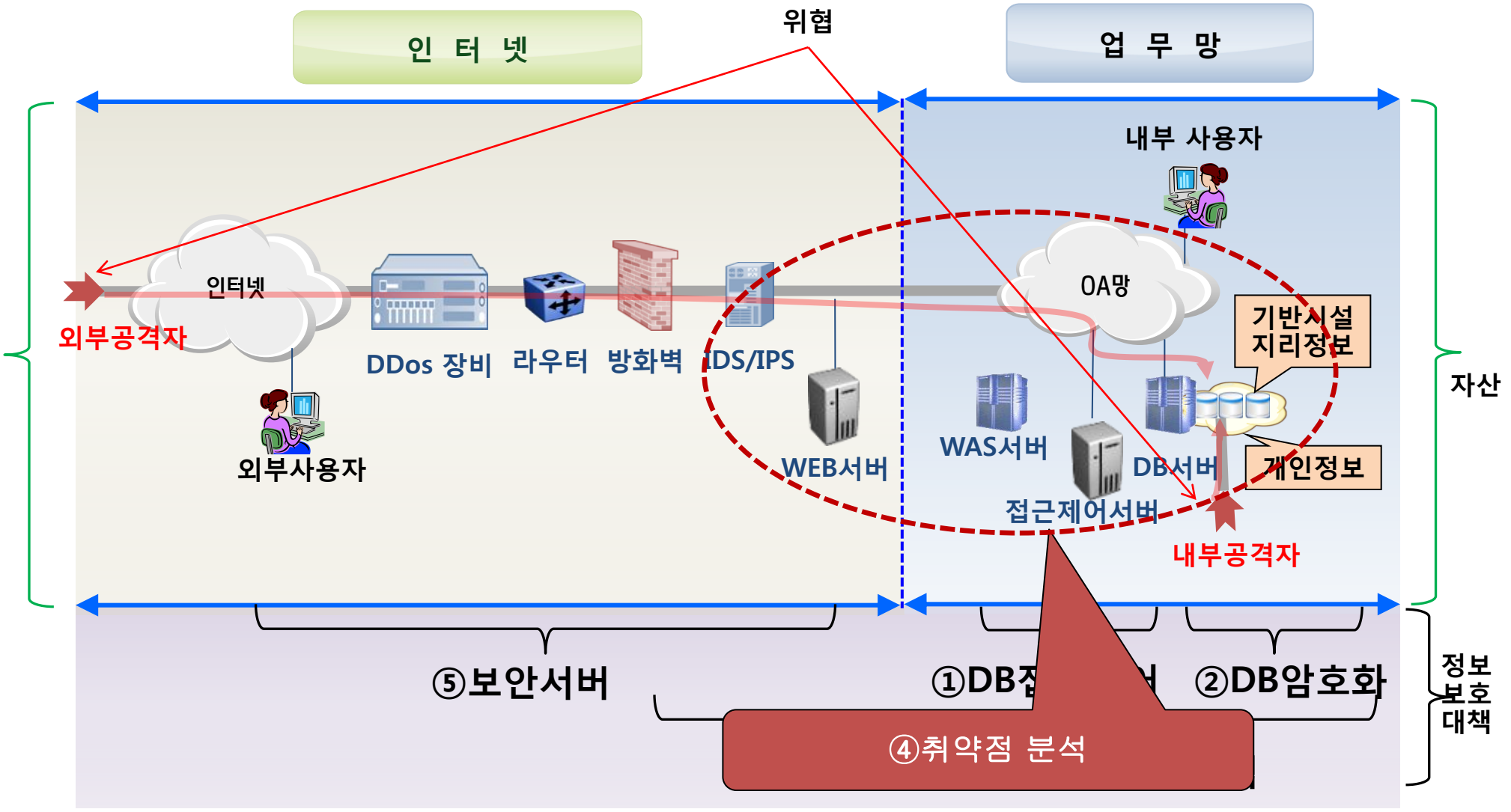
❖ 보안운영체제 : ACL


SecuOS Manager - [파일 관리]
파일(F) 보기(V) 도구(T) 도움말(H)
서버 보안
시스템 관리
파일 관리
파일 무결성 검사
프로세스 관리
로그 관리
사용자 권한 관리
보안 정책 관리
보안 정책 설정
서버 보안
로그인 제어
파일 관리
적용 대상
대상
옵션
NONE
AND
NOT
계정
root
그룹
역할 그룹
IP 주소
확인
취소
home
misc
boot
mnt
tmp
TOP_SECRET
usr
var
파일 속성 변경
파일 이름 :/TOP_SECRET
ACL 기반
레이블 기반
일반 속성
접근 프로세스
vi vsftpd
접근 권한
읽기(R)
쓰기(W)
실행(X)
삭제(E)
파일검색(F)
속성변경(M)
링크(L)
접근 로그 생성(A)
보안 레이블
보안등급
6
보호범주
FD2
제어 대상
*
정책 해제
적용
취소
메시지 창
발생 시간
서버명(IP주소)
이벤트
2008-11-11 19:07:27
RHEL5(192.168.0.109)
"/" 로 이동하였습니다
이벤트
준비
abdual.tsonnet.co.kr(192.168.0.109)
Linux 2.6.18-53.e

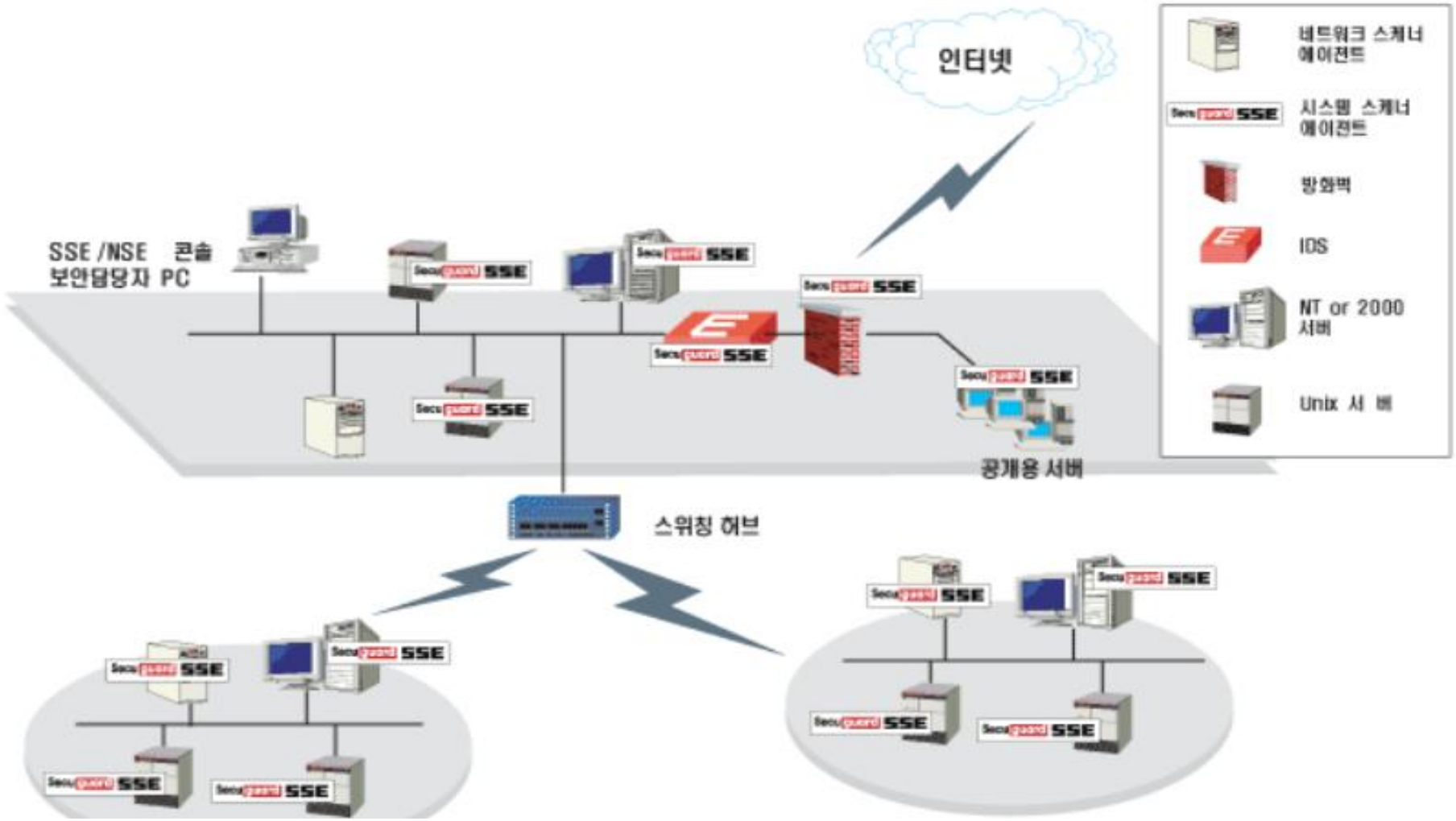
❖ 보안운영체제 : 네트워크 접근제어



❖ 지리정보 데이터베이스 보안



❖ **취약점 분석**



시스템 보안 취약점 자동점검, 발견된 문제점 해결방법 제공

=> 해킹과 보안사고 예방 시스템(시스템 내부 점검용 에이전트 설치)

❖ 취약점 분석 : 주요기능

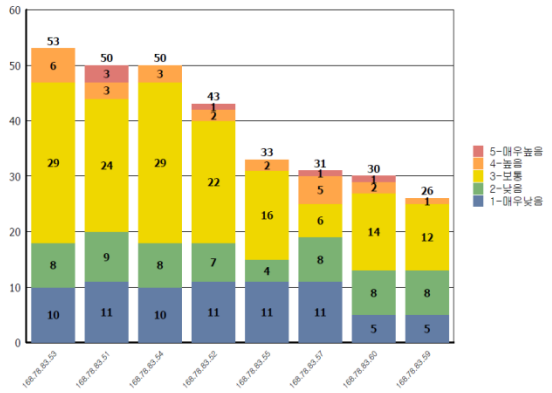
UNIX / Linux 계열	Windows 계열
* Password 관련 취약점 * XWindows 관련 취약점 * 관리자 및 사용자 환경 취약점 * 유틸리티 취약점 * 파일 시스템 취약점 * DB 취약점 * 데몬 취약점 * 특정 파일 취약점 * FTP 취약점 * SMTP 와 Mail 관련 취약점 * RPC취약점 * WWW/HTTP와 CGI 취약점 * DNS /BIND 관련 취약점 * 원격접속 명령어 취약점 * 패킷 관련 취약점 * 네트워크에 관련된 명령 취약점 * NIS /NIS+ 취약점 * Firewalls/Filters/Proxies 취약점 * Port 취약점	* Password 관련 취약점 * 관리자 및 사용자 환경 취약점 * 파일 시스템 취약점 * DB 취약점 * 특정 파일 취약점 * 서버 서비스 취약점 * 기타 서버 서비스 취약점 * 응용 프로그램 취약점 * 기타 응용 프로그램 취약점 * Exchange server 취약점 * Registry 취약점 * WWW/HTTP와 CGI 취약점 * 패킷 관련 취약점 * Firewalls/Filters/Proxies 취약점 * Port 취약점 * Internet Explorer 취약점 * Internet Information Server 취약점 * SMTP와 Mail관련 취약점 * Backdoors 취약점

CERTCC-KR, CERTCC, BUGTRAQ, MITRE

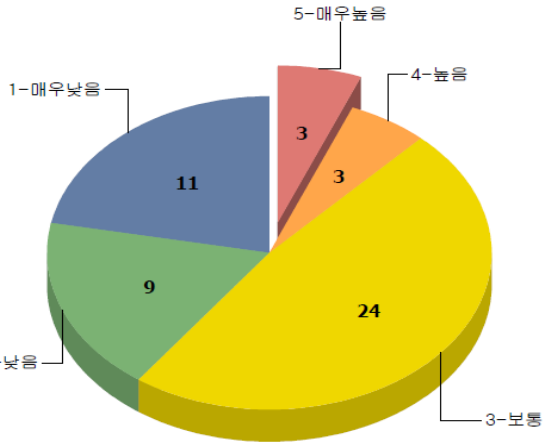
전문적 지식 요구, 많은 취약점, 여러장비 산재, 시간/인력 부족

❖ 취약점분석 : 결과 보고서

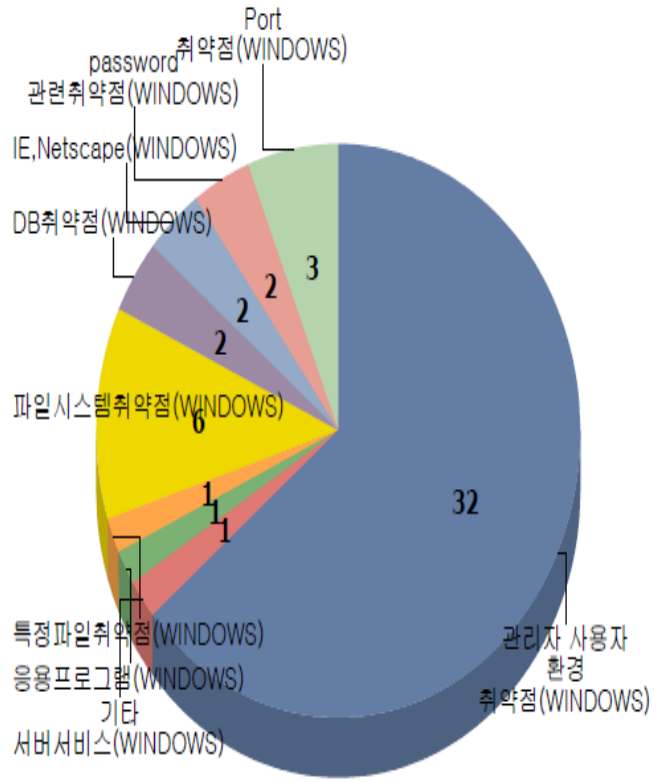
에이전트 및 위험도별 취약점 분포



위험도별 취약점 분포

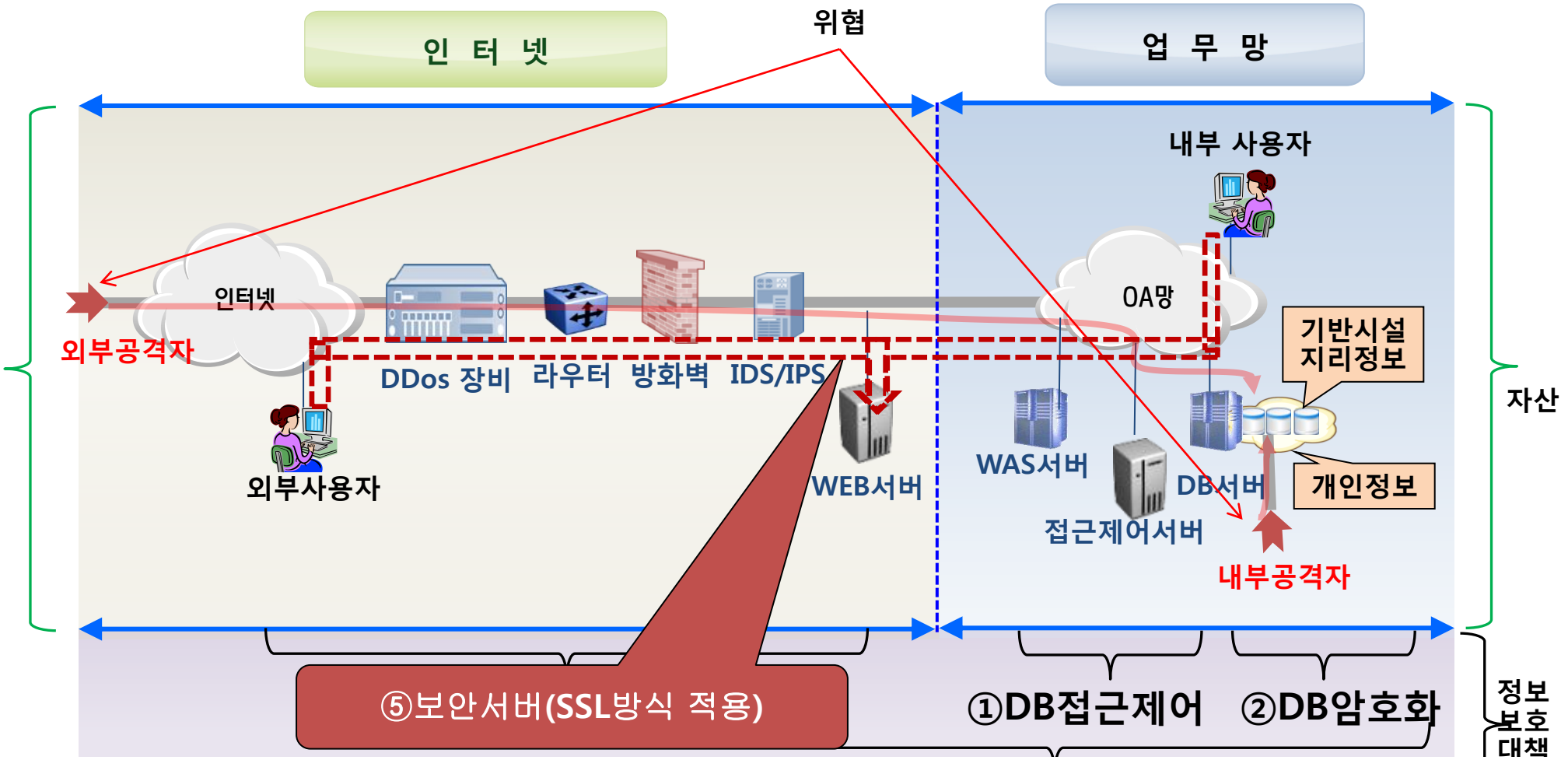


점검그룹별 취약점 분포



점검 그룹명	점검항목명	위험도
password 관련취약점(WINDOWS)	[301002] 관리자 권한을 가진 사용자의 패스워드 취약점	5-매우높음
	[301005] 패스워드 취약점(패스워드 설정되어 있지 않은 사용자)	5-매우높음
관리자 사용자 환경 취약점(WINDOWS)	[302010] Administrator 계정 취약점	2-낮음
	[302012] Password 길이 제한 설정 취약점	3-보통
	[302586] 세션을 중단하기 전에 필요한 유휴 시간 체크 진단	1-매우낮음
파일시스템취약점(WINDOWS)	[303014] Windows 커널 다중 취약점	4-높음
	[303080] Microsoft 커널 로컬 권한 상승 취약점(8)	3-보통
	[303084] Microsoft Windows Ancillary 드라이버 권한 상승 취약점	3-보통
	[303088] Windows Ancillary 기능 드라이버 권한 상승 취약점	2-낮음
	[303091] Microsoft 커널 로컬 권한 상승 취약점(10)	2-낮음
	[303554] Error Reporting 시 중요 정보 유출 가능 취약점	3-보통
DB취약점(WINDOWS)	[304035] Microsoft Jet 엔진 MDB 파일 구문 분석 스택 오버플로우 취약점	5-매우높음
	[304037] ODBC 데이터 소스 및 드라이브 진단	1-매우낮음
특정파일취약점(WINDOWS)	[305036] Microsoft Windows HSC 인증 우회 및 XSS 취약점	4-높음
기타 서버서비스(WINDOWS)	[307534] Computer Browser 서비스 실행 취약점	1-매우낮음
응용프로그램(WINDOWS)	[308028] 윈도우즈 아웃룩 주소록 연락처 레코드 취약점	3-보통
Port 취약점(WINDOWS)	[315002] 네트워크 TCP 포트 진단	1-매우낮음
	[315003] 네트워크 UDP 포트 진단	1-매우낮음
	[315004] Routing 진단	1-매우낮음
IE,Netscape(WINDOWS)	[316152] Microsoft Windows Messenger ActiveX 컨트롤 코드실행 취약점	4-높음

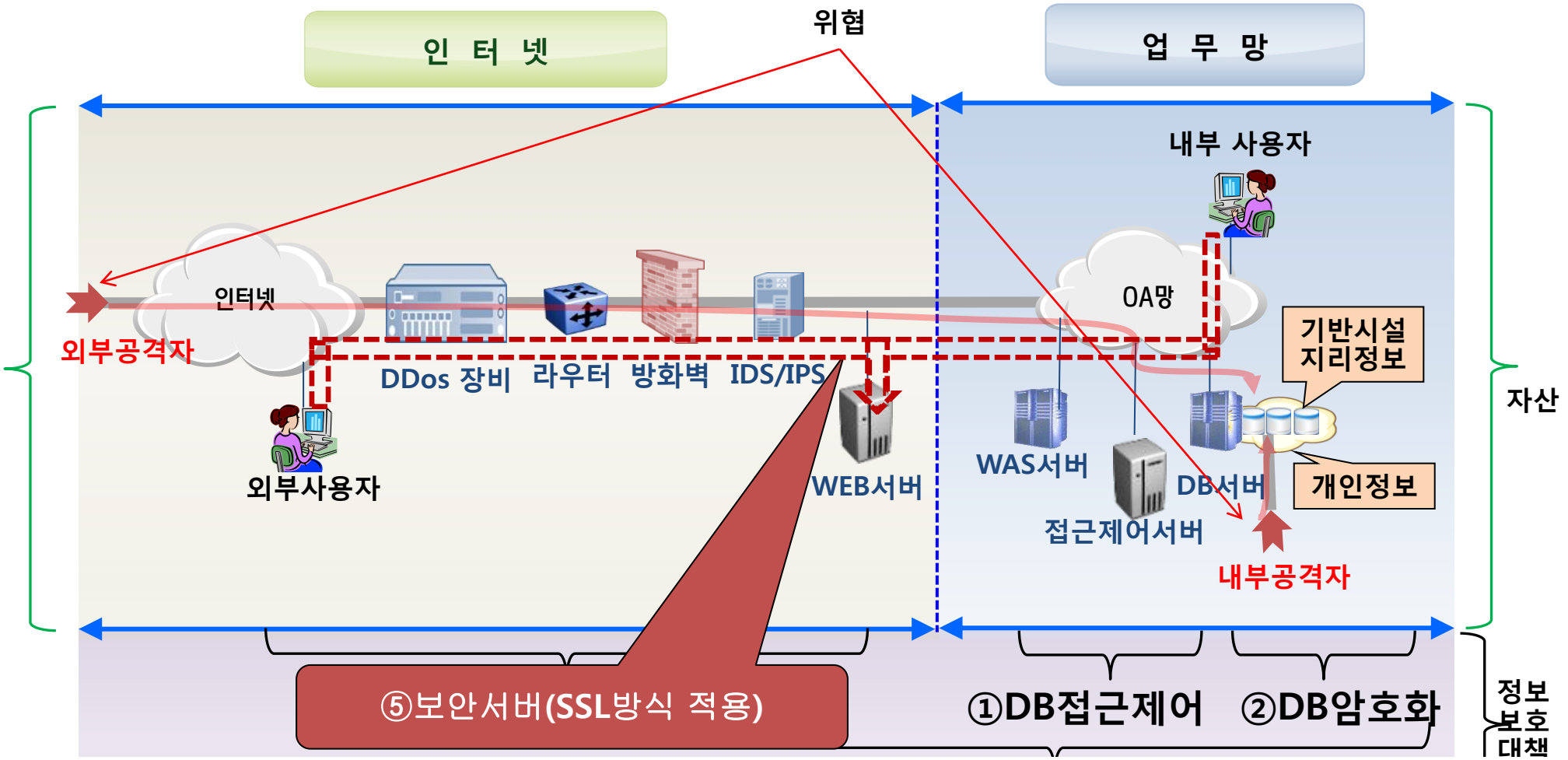
❖ 지리정보 데이터베이스 보안



SSL: Scure Socket Layer 웹브라우저와 웹서간 안전한 통신 지원

TCP/IP프로토콜 보안 취약 해결위한 웹 솔루션(실질적 표준)

❖ 지리정보 데이터베이스 보안



별도의 프로그램 설치 필요없고, 웹서버 설치된 SSL인증서 통해 암호화 송수신, 소요 비용 상대적 저렴, 주기적 인증서 갱신 비용 소요

Ⅰ 한전 전력연구원 소개

Ⅱ 기반시설과 지리정보 DB보안

☑ Ⅲ 향후 DB보안 추진방향

WORST PASSWORDS OF 2013

rank	password	change from 2012
#01	123456	⇈1
#02	password	⇊1
#03	12345678	—
#04	qwerty	⇈1
#05	abc123	⇊1
#06	123456789	new
#07	111111	⇈2
#08	1234567	⇈5
#09	iloveyou	⇈2
#10	adobe123	new

legend:
unchanged — up ⇈# down ⇊#

source data from: splashdata

유기적으로 결합된 통합 정보보호체계 구축

(1) 정밀한 정보보호 위험도 분석

➡ 조직의 핵심 자산 파악, 적정비용의 효과적인 정보보호 대책 수립

(2) 핵심 자산을 보호하기 위한 보안 솔루션 도입

➡ 최근 지능화, 자동화된 공격에 대비한 보안 솔루션 도입

(3) 체계적인 보안을 위해 관리체계 구축

➡ DQC-S 등 필요한 관리체계 구축 강화

(4) 지속적인 정보보안 활동 수행

➡ 보안업데이트, 최신 백신설치, 허가된 프로그램 사용, 주기적인 교육

단기간 일회적 정보보호 체계

단순하고 획일화된 솔루션