

한국에너지기술평가원 DB보안 구축 사례발표

2013. 10.

이윤백



Contents



I

에너지기술평가원 소개

II

DB보안 추진내용

III

향후 DB보안 추진방향



한국에너지기술평가원 소개

I

설립 목적

- ▶ 에너지기술개발 및 에너지기술혁신 기반조성으로 안정적, 효율적, 환경친화적인 국가에너지 수급구조 실현

연혁

- ▶ 2009. 5월



- ▶ 2010. 1월 ▶ 위탁집행형 준정부기관 지정

- ▶ 2010. 4월 ▶ 녹색인증평가기관 지정

에너지기술 혁신을 통한 녹색성장 실현을 위한
에너지기술 R&D 통합전담기관으로
전주기적 관리기능 수행



R&D 정책개발

- + 에너지기술 정책개발 및 로드맵 수립
- + 에너지기술 수요조사 및 동향분석 등



에너지 기술개발

- + 에너지기술개발 기획·평가·관리, 성과확산
- + 에너지자원기술개발사업
- + 전력산업/원자력발전/방폐
- + 신재생에너지 기술개발사업
- + 기술사업화, R&D 환류 지원



에너지 인력양성

- + 목적지향적 에너지 인력양성사업
- + 미래 기초인력 역량개발
- + 연구개발 고급인력 양성 지원
- + 산업전문인력 역량강화
- + 국제 인력교류 활성화



국제협력

- + 국제협력 및 국제공동 연구 사업
- + 다자간/양자간 국제협력
- + 전략적 국제공동연구



정책 개발

저탄소 녹색성장 정책

- ▶ 신성장동력 및 일자리 창출 (대통령 경축사, '08. 8.15)
- ▶ 그린에너지 산업 성장동력화, 수출 산업화 (그린에너지산업 발전전략, '08. 9.11)



시장 요구를 반영한 R&D 전략적 투자계획 요구



종합적, 구체적인 전략적 에너지 R&D 추진

그린에너지 전략로드맵 수립 및 개선

- ▶ 산업-제품-기술분석을 통한 사업화 시나리오 구성
- ▶ 15대분야 56개 전략품목 도출 : 203개 Key Technology
- ▶ 국가에너지 기술개발 기본계획 연계



기획·평가·관리

신규과제 기획

수요조사 → 과제발굴 → 세부과제 기획 → 신규과제 확정

평가관리

신규평가 → 협약체결 → 마일스톤 관리
→ 최종성과평가

성과관리

기술료징수, 개발성과 발굴·홍보,
성과활용분석 및 평가 등

주요 R&D사업 분야

에너지자원기술개발사업

▶ 에너지자원 기술개발사업

- 에너지효율향상 : 에너지저장, 청정 연료, 산업공정, 그린카 등
- 온실가스 : 이산화탄소 처리기술 등
- 자원 : 석유, 가스 탐사, 자원활용 등

▶ 자원순환 기술개발사업

- 금속자원 회수, 저감, 대체
- 규제대응 : 지구온난화 물질 회수 등
- 원단위 절감 재제조



전력산업/원자력발전/방폐

▶ 전력산업원천 기술개발사업

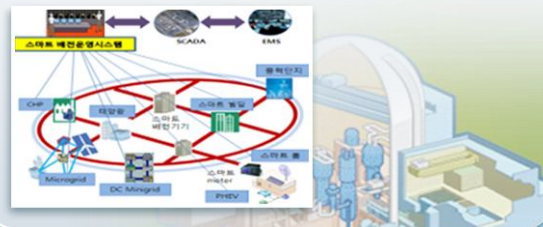
- 수·화력발전 기술개발
- 송·배전 기술개발
- 스마트그리드 기술개발

▶ 원자력발전 기술개발사업

- 원전해외 수출 기술개발
- 원전설비성능향상 기술개발

▶ 방사성폐기물관리 기술개발사업

- 사용 후 핵연료 관리 기술개발
- 중저준위방사성폐기물 관리 기술



신재생에너지 기술개발사업

▶ 신재생에너지 기술개발사업

- 태양광 : 박막, Si, CIGS, 유기태양광
- 풍력 : 육상풍력, 해상풍력
- 연료전지 : PEMFC, MCFC, SOFC
- IGCC : IGCC 핵심설비, 수출용 플랜트
- 수소, 바이오, 폐기물, 태양열, 지열 등



인력양성 및 국제협력

에너지 인력양성 사업

신성장 동력화 및 수출산업화 선도

고급 에너지기술
선도인력 양성

에너지 인력기반
강화

에너지 인력양성
글로벌화

에너지자원 및 전력·신재생분야
기초, 산업, 고급인력 양성 지원



국제협력사업 및 국제공동연구사업

에너지기술 조기 확보

에너지자원의 안정적 확보 협력

에너지기술 해외진출

국제사회 참여로 국가위상 제고

▶ 국제기구 협력사업

- IEA, APP 등 국제 에너지R&D 프로그램 참여

▶ 양자간 국제협력사업

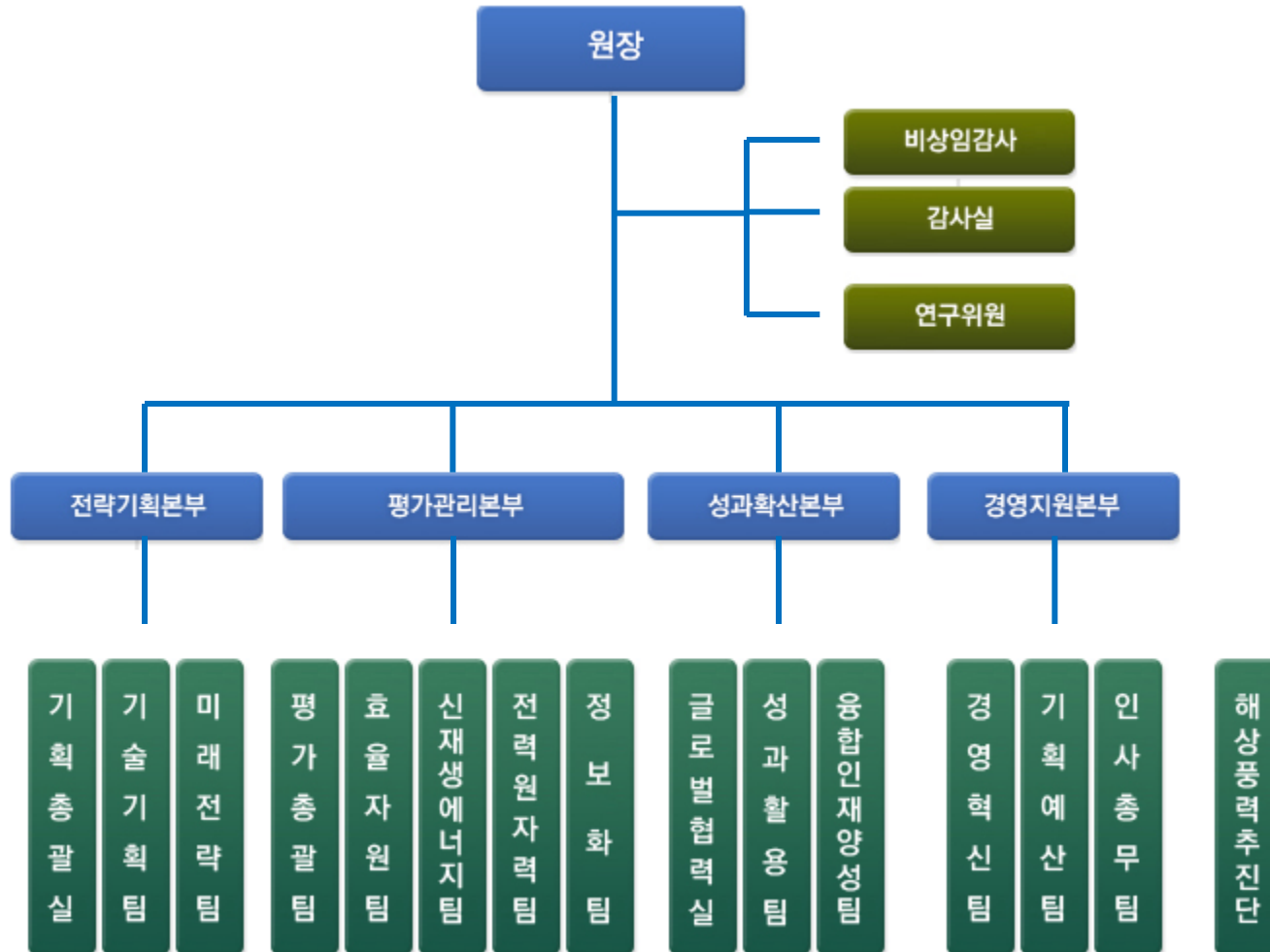
- 한·미 과학기술심포지엄 운영
- 한·중, 한·인도 협력관계 등

▶ 한·미 국제공동연구 프로그램

- 지식경제부·DOE 간 국제 공동연구추진 중

3. 조직 및 정원 현황

조직 : 4본부 · 1단 · 14팀, 정원 : 114명





II

DB보안 추진내용

경영비전 및 이에 따른 정보보호 실천전략

경영비전 및 목표



미션 에너지기술 혁신으로 녹색성장 실현에 기여

비전 에너지기술의 산업화 가치를 창출하는
Green KETEP

전략목표

1. 산업화 지향형 R&D 전략 수립
2. 성과중심의 R&D관리 환경 조성
3. 에너지기술 산업화 인프라강화
4. 효율적인 경영환경 조성

성과관리체계 상시 운영으로 핵심성과
및 피드백 강화

정보보호 핵심원칙 및 실천전략

정보보호 핵심원칙

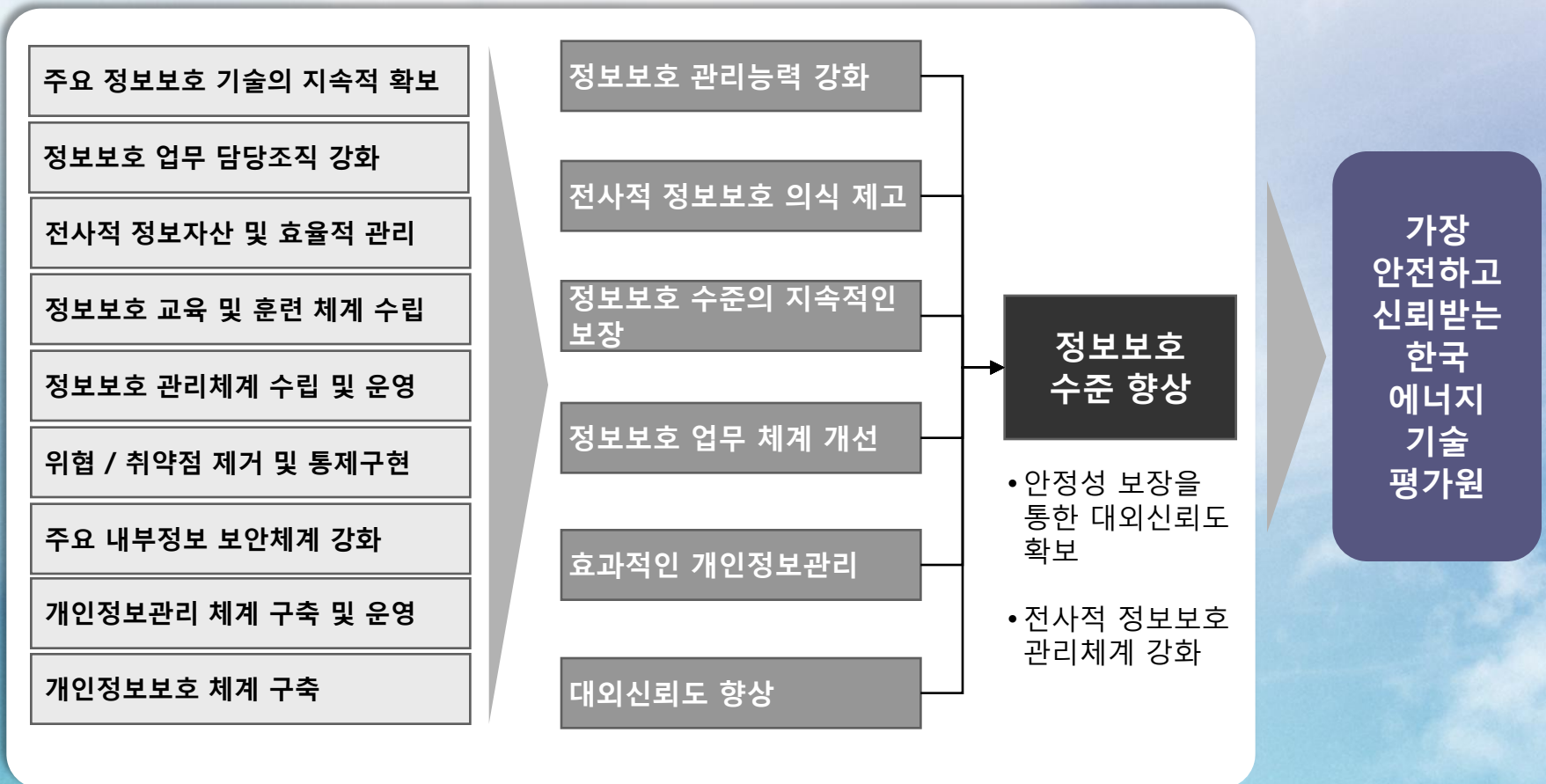
- 정보보호는 조직의 목표 달성 및 업무 수행을 지원해야 한다.
- 정보보호와 관련된 법적 요구사항을 준수하고 이를 지원하기 위한 제반 조치를 취한다.
- 정보자산에 대한 불법적인 접근, 유출, 변조, 장애를 예방하고 탐지하고 대응해야 한다.
- 모든 임직원은 정보보호의 중요성을 인식하고, 사고 방지를 위한 노력을 기울여야 한다.

정보보호 실천전략

- 정보보호는 조직의 목표 달성 및 업무 수행을 지원해야 한다.
- 최신의 보안 위험 및 이슈사항이 반영되고, 보안투자에 대한 투자 대비 효과 (ROI: Return On Investment)가 고려되어야 한다.
- 최근 정보보호에 관련한 법 제도에 대한 요건을 충실히 대응하고 법적 준거성 확보를 지원해야 한다.
- 정보자산의 보안성 확보를 위해 예방/탐지/대응 차원의 보안서비스가 상호 보완적으로 구현되어야 한다.
- 정보보호 과제 구현의 용이성 및 임직원의 이행활동에 대한 편리성이 확보되어야 한다.

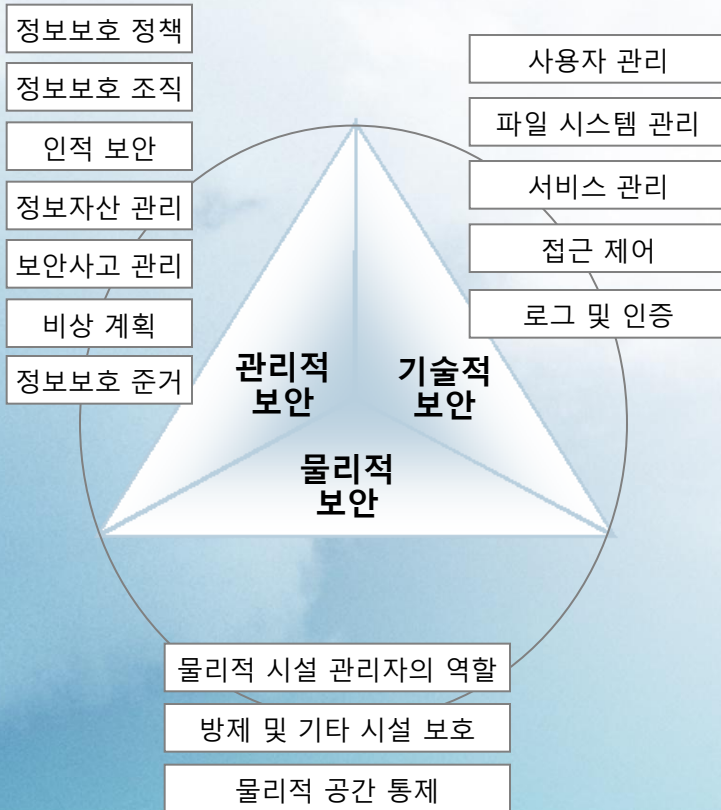
한국에너지기술평가원 정보보안 목표

정보보안 목표



관리적, 물리적, 기술적 항목 취약점 진단

보안 분야 별 개념도



분석 대상

1. 관리적 보안

보안 정책을 준수하며, 보안 거버넌스 구조 및 관리 프레임워크에 기반하여 체계적으로 보안관리를 수행하고 있는가?

2. 기술적 보안

보호하여야 할 내부 기밀자료 및 중요 정보자산에 대해 보안 기술을 적용하여 통제 활동을 수행하고 있는가?

3. 물리적 보안

조직의 인프라, 인력, 작업 장소 및 시설에 대한 물리적 보안 통제가 적절히 수행되고 있는가?

분석 관점

- 정보보호 정책 준수
- 정보보호 조직 구성 및 운영
- 인적 보안
- 정보자산 분류 및 통제
- 비상 계획
- 정보보호 준거

- 사용자 관리
- 파일 시스템 관리
- 서비스 관리
- 접근 제어
- 로그 및 인증

- 물리적 시설 관리자의 역할
- 방제 및 기타 시설 보호
- 물리적 공간 통제

관리적, 물리적, 기술적 항목 취약점 개선

	현황	주요 이슈	개선
관리적 보안	<ul style="list-style-type: none"> • 보안 규칙, 개인정보보호업무처리 지침 존재 • 보안위원회 개최 • 자산목록은 통합 유지 • 반기별 전사 보안교육 	<ul style="list-style-type: none"> • 개발 및 도입 장비 보안취약점 확인. 제거 필요 • 소스코드 관리 미흡 • 외부 용역 사업 과정에서의 주요 산출물에 대한 보안 관리가 미흡 • Unix 시스템의 SSH, Telnet 관리 미흡 • 이동형 정보시스템 반출입 관리 미흡 • 보조기억매체 관리 미흡 • 응용 시스템의 로그 분석 미흡 	<ul style="list-style-type: none"> • 어플리케이션 보안 운영 절차 수립 • 소스코드 진단툴 도입 • 데이터 삭제 관련 프로그램 도입 • Telnet 사용금지 및 서버보안 (SecureOS) 도입 • 노트북 반출 절차 수립 • 보안USB 도입 • 로그관리 시스템 도입
물리적 보안	<ul style="list-style-type: none"> • ID 카드 기반의 출입통제 시스템 운영 • 정보통신실의 경우 출입대장 관리 • 전산실에 CCTV 설치 	<ul style="list-style-type: none"> • 장비 반출입 절차가 없음 • 개발 공간의 경우 접근통제 대책 미흡 • 층별 출입통제 미흡 • 문서고에 대한 출입통제 미흡 	<ul style="list-style-type: none"> • 반출입증 작성 • 개발공간 IC카드 설치 • 층별 출입문 시건 후 IC카드만 사용 • 문서고 IC카드 설치
기술적 보안	<ul style="list-style-type: none"> • 사이버 안전센터 취약점 분석 후 이행 조치 • 신규로 도입된 장비의 경우 보안 설정 미흡 • 일부 웹페이지 취약점 미조치 • 필수 보안시스템(FW/IDS/IPS/웹방화벽) 설치 	<ul style="list-style-type: none"> • 원격에서 레지스트리에 접근 가능 • 불필요한 공유 존재 • 일부 화면보호기 보안 미설정 • 로그/감사 관리 미흡 • 네트워크 SNMP 보안 설정 미흡 • 보안시스템 디폴트 계정 사용 및 주기적 모니터링 미흡 • 웹페이지에 XSS 등 웹 취약점 존재 	<ul style="list-style-type: none"> • 취약점 분석결과 HotFix 이행조치 • 서버보안 도입 • 로그관리시스템 도입 • 주기적 취약점분석, 소스코드 진단 및 모의해킹

개인정보 영향평가 진단 (배경 및 목적)

- 목적 : 개인정보보호법 발효(21011.09.30)와 지경부 정보보안 세부지침 개정(2012.06.13)에 따른 새로운 기준에 미흡한 제 규정 보완 및 현 수준 진단, 평가, 개선계획 수립을 목적으로 함
- 수행기간 : 1차 : 2012. 6. 15 ~ 2012. 08. 14(2개월), 2차 : 2013. 7(후속 조치 1개월)

추진 배경

- 강화된 개인정보 보안 정책에 대응할 수 있는 개인정보 관리체계 필요
- 환경분석과 사례조사 후, 침해사고 및 유출 대응 방안 수립
- 「개인정보보호법 제33조」에 따른 보유시스템의 개인정보 영향평가 수행

프로젝트 지향점

- 개인정보 침해 가능성 최소화 및 보유 개인정보에 대한 사회적 책임 강화
- 개인정보보호 관련 법령, 지침 준수 및 수준 강화를 통해 대외 신인도 향상
- 경영진의 개인정보보호 정책 수립 의사결정 지원
- 평가원 전 직원의 보안 의식 강화
- 개인정보보호 관리체계 강화로 보안위협성 제거 및 예방

추진 목표

1

- 개정법규를 반영한 정책 개정
 - 정보보안 지침
 - 개인정보보호 업무처리지침
 - 개인정보 처리방침
 - 개인정보보호 내부관리계획

2

- 행정안전부 지정 평가기관의 「영향평가」 수행 후 결과 제출
 - 개인정보 영향평가 결과보고서

3

- 수준진단 및 마스터플랜
 - 개인정보 보호 수준진단
 - 인력양성사업 보호수준 평가
 - 개인정보 침해사고 대응절차
 - 정보보호체계 마스터플랜 수립

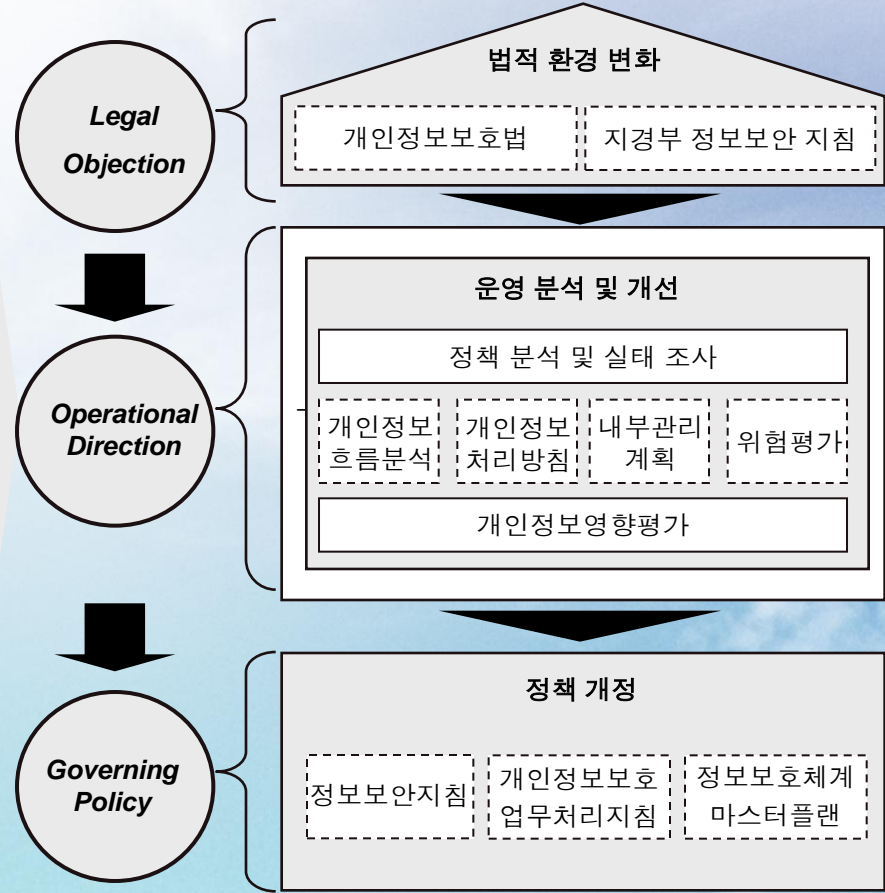
개인정보 영향평가 (추진 범위)

3개 분야별 과제추진을 병행하여 기존 개인정보보호 체계 강화에 필요한 핵심 요소를 파악하고 새로운 기반을 구축하였음

추진범위

개인정보관리체계 보완 추진 방향

<p>1</p> <p>정책 분석 및 개선안 수립</p>	<p>[법률분석 및 실태조사]</p> <ul style="list-style-type: none"> • 지경부 정보보안 세부지침 개정안 분석 • 기존 보안규칙, 정보보안지침, 개인정보보호 업무처리지침 분석 • 기존 개인정보보호방침, 내부관리계획 분석, 평가 • 정보시스템 개인정보 보유 현황 및 평가시스템 조사 <p>[정책 및 지침 개정안 수립]</p> <ul style="list-style-type: none"> • 정보보안지침 개정안 • 개인정보보호 업무처리지침 개정안 • 개인정보 처리방침 개정안 • 개인정보보호 내부관리계획 개정
<p>2</p> <p>개인정보 영향평가, 수준진단</p>	<p>[개인정보 흐름분석]</p> <ul style="list-style-type: none"> • 개인정보 업무분석 • 업무 흐름표, 흐름도 작성 <p>[개인정보 침해요인분석]</p> <ul style="list-style-type: none"> • 평가항목 선정, 인터뷰 • 위험 평가 및 개선방안
<p>3</p> <p>세부추진 방안수립</p>	<p>[이행방안 수립]</p> <ul style="list-style-type: none"> • 침해사고 대응지침 • 유출사고 대응절차 <p>[마스터플랜 보완]</p> <ul style="list-style-type: none"> • 기존 마스터플랜 분석 및 현행화



개인정보 영향평가 (수행 방법)

정보보호 관리체계 분석 및 평가는 영향평가 영역1과 행안부 수준진단 점검항목 등을 기준으로 현황 파악, GAP 도출, 개정안 작성을 수행함

□ 점검 기준

개인정보보호법
개인정보 영향평가 점검항목 (114 항목)
지경부 보안업무세부지침 (128 조문)
행안부 수준진단 점검항목 (82 진단항목)
행안부 보안관리체계 (25 통제사항)

□ 점검 방법

기존 규정, 지침 검토

보안규칙, 정보보안지침, 개인정보보호방침, 내부관리계획 등 기존 보안규정문서를 검토하여 이행 수준, 개정 사유 등을 검토함

개정 상위법 반영

지경부 정보보안 세부지침, 개인정보보호법, 안전성확보조치기준 고시, 행안부 표준지침 등의 필수 적용 사항 도출

운영환경 적용 검증

평가원의 업무환경, 정보보호 요구수준, 관리체계수준 등을 고려하여 규정, 지침의 개정안 도출

정보보호 관리체계

구분	항목	구분	항목	구분	항목	구분	항목	구분	항목	
1	정보보호 방침	1.1	정보보호 방침	2	조직	2.1	조직	3	인력	
2	정책	2.1	2.1.1	정보보호 방침	3	3.1	3.1.1	정보보안 담당자	4	4.1
			2.1.2	정보보안 담당자			3.1.2	정보보안 담당자		
			2.1.3	정보보안 담당자			3.1.3	정보보안 담당자		
			2.1.4	정보보안 담당자			3.1.4	정보보안 담당자		
3	인력	3.1	3.1.1	정보보안 담당자	4	4.1	4.1.1	정보보안 담당자	5	5.1
			3.1.2	정보보안 담당자			4.1.2	정보보안 담당자		
			3.1.3	정보보안 담당자			4.1.3	정보보안 담당자		
			3.1.4	정보보안 담당자			4.1.4	정보보안 담당자		
4	인력	3.1	3.1.1	정보보안 담당자	4	4.1	4.1.1	정보보안 담당자	5	5.1
			3.1.2	정보보안 담당자			4.1.2	정보보안 담당자		
			3.1.3	정보보안 담당자			4.1.3	정보보안 담당자		
			3.1.4	정보보안 담당자			4.1.4	정보보안 담당자		
5	인력	3.1	3.1.1	정보보안 담당자	4	4.1	4.1.1	정보보안 담당자	5	5.1
			3.1.2	정보보안 담당자			4.1.2	정보보안 담당자		
			3.1.3	정보보안 담당자			4.1.3	정보보안 담당자		
			3.1.4	정보보안 담당자			4.1.4	정보보안 담당자		

개인정보 취약점 진단 (이슈 도출)

□ 주요 문제점

강화된 개인정보보호법의 기준에 미달하는 주요 현안을 도출하여 제도적, 기술적 해결방안을 모색함

보안영역

주요 문제점

관리적 부문

- 정보보호협의회 및 정보보안담당관 제도 운영 비활성화 및 활동 내역 부족
- 개인정보보호 점검활동 이력 미흡
- 용역사업 및 위탁운영의 보안관리 부족
- 개인정보보호 교육 및 원내 의식강화 활동 부족
- 개인정보 과다 보유 (홈페이지, 인력양성인증시스템)
- 학생 개인정보화일대장 미작성
- 처리정보 이용 및 제공 대장관리 부적합
- 주민번호 대체수단 미제공

기술적 부문

- 개인정보데이터 파기절차 부재
- 개인정보 평문 전송
- 주민번호 대체수단 미제공 (인력양성인증시스템)

개인정보 취약점 진단 (평가 결과)

□ 수준 평가(1차 : 76.8% -> 2차 : 91.8%)

평가 영역	평가 분야 (전체)	항목수	개인정보 영향평가 결과				이행률
			Y	P	N	N/A	
1. 대상기관 개인 정보보호 관리 체계	1.1 대상기관 개인정보 보호조직	4	4				100%
	1.2 개인정보 보호계획	2	2				100%
	1.3 개인정보 처리방침	7	4	3			78.6%
	1.4 개인정보 파일관리	6	6				100%
	1.5 개인정보 위탁 및 제공시 안전조치	2		1	1		25%
	1.6 개인정보 침해대응	4	4				100%
	1.7 정보주체 권익보호	3	1	1	1		50%
	1.8 개인정보 처리구역 보호	3	3				100%
2. 대상시스템의 관리체계	2.1 대상 시스템의 개인정보 관리	2	2				100%
	2.2 개인정보 취급내용 공개	6	4	1		1	90%
3. 개인정보 처리 단계별 보호	3.1 수집단계	12	6	2	3	1	63.6%
	3.2 저장 및 보유단계	4	3			1	100%
	3.3 이용 및 연계·제공단계	40	23	6	9	2	68.4%
	3.4 파기단계	3	1	1	1		50%
4. 특정IT기술	4.1 CCTV 활용	5	4			1	100%
합 계 (전체평균)		103	67	15	15	6	76.8%

대외 준거성 분석 및 준수사항 선정

관련 법령 및 규정

관련기관	관련 법령 / 지침	제/개정 일시
국정원	보안업무규정	2010.10.20
	국가사이버안전관리규정	2008.8.18
안행부	공공기관의 개인정보보호에 관한 법률	2008.2.2
	공공기관 개인정보보호 기본지침	2009.4
	개인정보보호법	2011
방통위	국가정보화기본법	2009.8.21
	전자정부법	2009.12.14
지경부	정보보안 기본지침	2009.11
	보안업무 취급요령	2009.2.18
	정보보안세부지침	2010.4.6
	지식경제 기술혁신사업 보안관리요령	2010.4.1

준수 사항 선정 기준

공공기관과
관련되어
준수해야
할 법령

- 공공기관이 준수해야 할 보안관리 관련 상위 법령 및 법규
 - 보안담당관, 보안위원회 구성
 - 보안구역설정, 보안교육
 - 정보통신망 자료관리, 보안성검토

개인정보보
호 관련되
어 준수해
야 할 법령

- 개인정보보호 관련된 상위 법령 및 법규
 - 개인정보 수집 시 동의절차
 - 개인정보 암호화 관리
 - 개인정보파일관리
 - PC저장 및 전송시 보안대책

상급기관에
서 지정하
는 행정 준
수 지침

- 상급기관에서 준수를 요구하는 행정 절차 및 규정과 지침
 - 보안심사, 사이버보안진단의날 행사
 - 자산반출입, 보조기억매체관리
 - 용역사업 보안관리

한국에너지기술평
가원의 준수해야
하는 규제 및 준수
사항 선정

최신 보안 Trend 분석 및 개선

최신 보안 Trend

기술적 보안	<ul style="list-style-type: none"> 해커 등에 의한 악의적 공격으로부터 기업의 정보자산을 보호하는 기술 			
	침입차단	PC보안	DDoS	무선/L2보안
정보유출 방지	<ul style="list-style-type: none"> 내부자의 고의 또는 실수에 의한 개인정보 및 기밀 유출방지 기술 			
	웹/메일 보안	DB/서버 보안	문서보안	망분리/가상화
전사 보안관리	<ul style="list-style-type: none"> IT 인프라에 대한 보안 현황을 모니터링, 분석 및 관리하기 위한 기술 			
	보안관제/ESM	통합로그/종합분석	정보보호관리체계 (G-ISMS)	
접근제어	<ul style="list-style-type: none"> 권한 Life Cycle에 따라 IT인프라 접근 및 사용을 자동 관리하는 기술 			
	인증/접근관리 (SSO/PKI)	네트워크접근 (NAC)	통합접근제어 (IAM)	유무선 통합 인증
융합보안 (물리+기술 보안)	<ul style="list-style-type: none"> IT 보안 기술 + 물리적 보안 기술(보안 장비) + BT 등의 신기술 			
	IT + 물리적 보안	IT + BT	물리적 보안 + BT	

- 범례**
- 현재 대부분 도입이 완료된 추세
 - 현재 대부분 도입을 진행 중
 - 향후 도입이 예상됨

공공기관 최근 보안이슈

DDoS 공격 등에 의한 정부통합전산센터(나라장터) 마비
교과부 예하 기관 개인정보유출 사고 발생(600만건)
개인정보보호법 국회 통과에 따른 개인정보관리 강화(2010년 9월)
DDoS 공격의 원천적인 대응을 위한 좀비PC법 추진
PC통합보안/매체통제/DB암호화 등 개인정보/내부정보유출 방지 솔루션 도입 증가
공공기관 정보보호관리체계(G-ISMS) 인증 도입
스마트폰 활성화에 따른 모바일 보안 추진전략 수립

- BCP(업무연속성계획)차원에서 전략적으로 접근하는 보안IT투자
- 내부직원 PC의 개인정보 암호화 저장 등 개인정보보호조치 강화
- DDoS 등 해킹 대응, 무선랜 보안통제 강화(WPA2 적용)
- 정보유출 방지대책 마련 및 정보보호 인력·교육 강화
- 개인정보보호 강화 법규 대응 방안 마련
- 모바일 보안 대응체계 구축 준비

평가원 보안 솔루션 도입 현황

	~ 2010	2011	2012	2013
네트워크 보안	① 방화벽 ② 웹 방화벽 ③ IPS ④ Ddos ⑤ SSL-VPN	① NAC(접근제어) ② 게시판 필터링	① DLP (개인정보보호)	① 망분리(논리적) ② 망연계 ③ 좀비PC방지 (ATP대비)
DB 및 서버 보안	① Web보안 ② SSO	① DB암호화 ② SSL(구간암호화)		① DB접근제어 ② 서버보안 (secureOS)
PC클라이언트 보안	① 백신SW ② 보안USB ③ 키보드보안	① 모바일 인증 ② 모바일 가상키패드	① DRM(문서보안)	① 개인정보검색 ② PC보안규제SW

개요

DB 보안 프레임워크

분야	접근제어	암호화	작업결재	취약점 분석
기획	DB보안 정책 수립			
설계	접근제어 규칙 정의	복호화 권한 통제	작업결재 규칙 정의	취약점 분석 계획
		암호화키 및 알고리즘 정의		
구축	우회 접근 방지	원본 데이터 삭제	우회 결재 방지	모의 해킹
		제약 사항 유지		
		암호화 키 관리		
	환경 보완		내부보안 감사	
보안 적용 시험				
운영	보안규칙 관리		취약점 수집	
	사용자 로그 관리		취약점 제거	
	모니터링		취약점 개선 분석 비교	
	운영리뷰			

출처 : 한국데이터베이스진흥원 - 데이터베이스 보안 가이드라인

공통

DB 보안 현황				
목차	목차	목차	목차	목차
1. DB 시스템 백업 및 복구	1. DB 백업	2. DB 복구	1. 일반사항	2. 책임사항
3. 사후대응	1. 사고 시 내부 보고	2. 사고대응	3. 데이터베이스 인증	4. DB 접근제어 및 암호화
			5. DBMS 요구기능	6. 로깅 및 감사

DB 보안 정책 수립 및 지침

DB 보안 시스템 교육

목	
VII. DB 시스템 백업 및 복구	
1. DB 백업	
2. DB 복구	
VIII. 사고대응	
1. 사고 시 내부 보고	
2. 사고대응	
I. 일반사항	1. 목적
	2. 적용 범위
	3. 용어 정의
II. 책임사항	1. 데이터베이스 보안책임자
	2. 데이터베이스 보안담당자
III. 데이터베이스 인증	1. 인증정책 일반
	2. 계정의 생성 및 폐기
IV. DB 접근제어 및 암호화	1. 접근수준 및 권한부여
	2. 접근제어 설정 및 경신절차
	3. 접근제어 메커니즘
	4. DB 암호화
V. DBMS 요구기능	1. DB보안을 위한 DBMS 요구기능
VI. 로깅 및 감사	1. 로깅
	2. 감사



구분	구분	구분	구분
DBMS 접근 제어	DBMS 접근 제어	DBMS 접근 제어	DBMS 접근 제어
DBMS 접근 제어	DBMS 접근 제어	DBMS 접근 제어	DBMS 접근 제어
DBMS 접근 제어	DBMS 접근 제어	DBMS 접근 제어	DBMS 접근 제어
DBMS 접근 제어	DBMS 접근 제어	DBMS 접근 제어	DBMS 접근 제어
DBMS 접근 제어	DBMS 접근 제어	DBMS 접근 제어	DBMS 접근 제어
DBMS 접근 제어	DBMS 접근 제어	DBMS 접근 제어	DBMS 접근 제어
DBMS 접근 제어	DBMS 접근 제어	DBMS 접근 제어	DBMS 접근 제어
DBMS 접근 제어	DBMS 접근 제어	DBMS 접근 제어	DBMS 접근 제어
DBMS 접근 제어	DBMS 접근 제어	DBMS 접근 제어	DBMS 접근 제어

접근제어(기능 및 정책)

◆ DB접근제어 기능

- DBMS에 원격으로 접속하는 모든 Client 및 DBMS 내부에 접속하는 모든 Client의 작업행위 감시
- DB작업 통제를 위한 사용자 인증
- DBMS 및 DB서버에 작업하는 모든 행위를 기록, 통제
- WAS서버에 실행되는 비정형SQL(AD-Hoc)실행시도 감지
- 보호 대상 DBMS 성능 모니터링

◆ DB접근제어 정책

- 허용IP외 차단 정책 : 스니핑 방식을 통해 등록된 IP외 불법접근 차단
- 내부사용자 서버접근 차단: Agent 미설치 PC의 DB서버 및 DBMS로의 불법적 접근 차단
- Agent 사용자 Telnet 접근 차단 : Agent 설치PC의 우회 접근 차단
- 위 정책 외 DB접근제어 기본 차단 및 권고 정책 적용

접근제어(화면)

구분	대상	접근제어	접근제어
로그	통합DB_2에서 내부사용자 서버접근 차단 경고 발생	2013/09/05 20:13:33	통합DB_2에서 내부사용자 서버접근 차단 경고 발생
유지	유지 작업	2013/09/05 20:13:32	통합DB_2에서 내부사용자 서버접근 차단 경고 발생
알림	알림	2013/09/05 20:13:32	통합DB_2에서 내부사용자 서버접근 차단 경고 발생

접근제어 정책

Security Policy

All Security Policy Information

Level	Name	Activate	Policy Type	Chakra Mode	Protection	Start date	End date	R
Class: Alert Policy List								
	허용IP외 차단정책	Activate	Database access control	Sniffing		2013/02/04 00:00:00	2031/12/31 00:00:00	-
CRITICAL	내부사용자 서버접근 차단	Activate	System access control	Sniffing		2013/08/26 00:00:00	2031/12/31 00:00:00	-
CRITICAL	Agent 사용자 Telnet 접근 차단	Activate	System access control	Gateway	Kill session	2013/09/03 00:00:00	2031/12/31 00:00:00	-

접근제어(화면)

구분	접근제어	접근대상	접근일자	접근시간
사용자	관리자	관리자	2013.07.22	16:06:42
시스템	DBMS	DBMS	2013.07.22	16:06:40
접근원인	로그인 실패	로그인 실패	2013.07.22	14:51:16
접근결과	실패	실패	2013.07.22	14:51:16
접근위치	192.168.100.1	192.168.100.1	2013.07.22	14:51:16
접근대상	DBMS	DBMS	2013.07.22	14:51:16
접근유형	로그인 실패	로그인 실패	2013.07.22	14:51:16
접근이벤트	로그인 실패	로그인 실패	2013.07.22	14:51:16
접근이벤트	로그인 실패	로그인 실패	2013.07.22	14:51:16
접근이벤트	로그인 실패	로그인 실패	2013.07.22	14:51:16
접근이벤트	로그인 실패	로그인 실패	2013.07.22	14:51:16

접근제어 접속로그

MaxManager

Chakra Max

Monitor Policy Search Report System

Database System Alert Approval Work History

2013/08/05 17:29:39 통합DB_1(DBMS)에서 내부사용자외 차단정책 경고 발생 2013/07/22 16:06:42 통합DB_1에서 Login failed alert 경고 발생 2013/07/22 16:06:40 통합DB_1에서 Login failed alert 경고 발생 2013/07/22 14:51:16 통합DB_2에서 Login failed alert 경고 발생 2013/07/22 14:51:16 통합DB_2에서 Login failed alert 경고 발생

2013년 8월 11일 오후 2:29:51 부터 2013년 8월 12일 오후 2:29:51 까지 로그를 검색합니다.

Target System : DBMS,

User IP Address Application SQL

검색 Advanced Search

여러 IP주소를 동시 검색하기 위해 세미콜론(";")사용이 가능합니다.
또한, 192.168.100.* 와 같이 와일드카드를 활용한 검색이 가능합니다.

SQL Search Result(5)

Search operation was finished successfully. : 696 SQL (4.003초)

Show Detail Pane Object Usage Analysis Execut

ID	Hostname	Terminal	Client IP	Application	Client Port	Server IP	Server Port	Client Mac Address	DB Sessio...	Serial#	SQL Type	SQL
271	EUX	EUX	192.168.100.1	TOAD.EXE	49942	192.168.100.1	1521	00:00:00:00:00:00	393	36817	DCL	COMMIT
272	EUX	EUX	192.168.100.1	TOAD.EXE	49942	192.168.100.1	1521	00:00:00:00:00:00	393	36817	DCL	SAVEPOINT LOCK_QRY
273	EUX	EUX	192.168.100.1	TOAD.EXE	49942	192.168.100.1	1521	00:00:00:00:00:00	393	36817	Query	SELECT * FROM "TPE_SDIV_ESTM_CMTM" WHERE "ROWID" = :;"OLD_ROWID"
274	EUX	EUX	192.168.100.1	TOAD.EXE	49942	192.168.100.1	1521	00:00:00:00:00:00	393	36817	DML	UPDATE "TPE_SDIV_ESTM_CMTM" SET "SECU_SIGN_DT" = :;"SECU_SIGN_DT"
275	EUX	EUX	192.168.100.1	TOAD.EXE	49942	192.168.100.1	1521	00:00:00:00:00:00	393	36817	Query	SELECT "TESTM_CMTM_ID" AS "1", "SDIV_ID" AS "2", "CMTM_ID" AS "3"
276	EUX	EUX	192.168.100.1	TOAD.EXE	49942	192.168.100.1	1521	00:00:00:00:00:00	393	36817	DCL	COMMIT
277	TOAD.EUX	EUX	192.168.100.1	TOAD.EXE	49942	192.168.100.1	1521	00:00:00:00:00:00	393	36817	DCL	COMMIT
278	정원중-PC	정원중-PC	192.168.100.1	DBANY.EXE	1791	192.168.100.1	1521	00:00:00:00:00:00	0	0	PL/SQL	BEGIN NULL; END;
279	EUX	EUX	192.168.100.1	TOAD.EXE	49942	192.168.100.1	1521	00:00:00:00:00:00	393	36817	Query	SELECT GET_PRJT_CLSF_NM(SUBSTR(A.PRJT_CLSF_CODE,0,2)) AS PRJT...
280	EUX	EUX	192.168.100.1	TOAD.EXE	49942	192.168.100.1	1521	00:00:00:00:00:00	393	36817	Query	SELECT GET_PRJT_CLSF_NM(SUBSTR(A.PRJT_CLSF_CODE,0,2)) AS PRJT...
281	EUX	EUX	192.168.100.1	TOAD.EXE	49942	192.168.100.1	1521	00:00:00:00:00:00	393	36817	Query	SELECT GET_PRJT_CLSF_NM(SUBSTR(A.PRJT_CLSF_CODE,0,2)) AS PRJT...
282	EUX	EUX	192.168.100.1	TOAD.EXE	49942	192.168.100.1	1521	00:00:00:00:00:00	393	36817	Query	SELECT GET_PRJT_CLSF_NM(SUBSTR(A.PRJT_CLSF_CODE,0,2)) AS PRJT...
283	정원중-PC	정원중-PC	192.168.100.1	DBANY.EXE	1791	192.168.100.1	1521	00:00:00:00:00:00	0	0	PL/SQL	BEGIN NULL; END;
284	EUX	EUX	192.168.100.1	TOAD.EXE	49942	192.168.100.1	1521	00:00:00:00:00:00	393	36817	Query	SELECT GET_PRJT_CLSF_NM(SUBSTR(A.PRJT_CLSF_CODE,0,2)) AS PRJT...
285	EUX	EUX	192.168.100.1	TOAD.EXE	49942	192.168.100.1	1521	00:00:00:00:00:00	393	36817	Query	SELECT GET_PRJT_CLSF_NM(SUBSTR(A.PRJT_CLSF_CODE,0,2)) AS PRJT...
286	EUX	EUX	192.168.100.1	TOAD.EXE	49942	192.168.100.1	1521	00:00:00:00:00:00	393	36817	Query	SELECT GET_PRJT_CLSF_NM(SUBSTR(A.PRJT_CLSF_CODE,0,2)) AS PRJT...

접근제어(화면)

구분	접근제어	접근제어	접근제어	접근제어
구분	접근제어	접근제어	접근제어	접근제어
구분	접근제어	접근제어	접근제어	접근제어
구분	접근제어	접근제어	접근제어	접근제어
구분	접근제어	접근제어	접근제어	접근제어
구분	접근제어	접근제어	접근제어	접근제어
구분	접근제어	접근제어	접근제어	접근제어
구분	접근제어	접근제어	접근제어	접근제어
구분	접근제어	접근제어	접근제어	접근제어
구분	접근제어	접근제어	접근제어	접근제어

접근제어 모니터링

MaxManager

Chakra Max

Monitor Policy Search Report System

Overview Session Trend Alert

Search

5:50:44 통합DB_1(DBMS)에서 Login failed alert 경고 발생 2013/09/16 15:32:59 통합DB_1에서 Login failed alert 경고 발생 2013/09/16 15:32:46 통합DB_1에서 Login failed alert 경고 발생 2013/09/16 15:28:31 통합DB_2에서 Login failed alert 경고 발생

Alert Calendar Unconfirmed Alert

최근 3일 조회 검색 Total Count: 8 Auto Refresh Alert by Gateway & Sniffing

Alert Level	Alert Name	Time	Server	Datab...	Service Type	IP Address	Application	Hostname	Max U...	Group	OS User	DB User	Sessio...	SQL (o...	Protec...	SMS R...	Mail R...	Script ...	SNMP
Warning	Login failed alert	2013/09/16 15:28:31	통합DB_2		SSH	192.		서버접속용PC-1	서버...				2013/0...		N/A				
Warning	Login failed alert	2013/09/16 15:32:46	통합DB_1		SSH	192.		서버접속용PC-1	서버...				2013/0...		N/A				
Warning	Login failed alert	2013/09/16 15:32:59	통합DB_1		SSH	192.		서버접속용PC-1	서버...				2013/0...		N/A				
Warning	Login failed alert	2013/09/16 15:50:44	통합DB_1	DBMS	ORACLE	192.	TOAD.EXE	KCSONG	송교...		ADMIN...	KETEP...	2013/0...		N/A				
Warning	Login failed alert	2013/09/17 09:38:47	통합DB_1	DBMS	ORACLE	192.	JAWAW.EXE	kcsong	송교...		Admini...	KETEP...	2013/0...		N/A				
Warning	Login failed alert	2013/09/17 09:38:47	통합DB_1	DBMS	ORACLE	192.	JAWAW.EXE	kcsong	송교...		Admini...	KETEP...	2013/0...		N/A				
Warning	Login failed alert	2013/09/17 09:50:36	통합DB_2	DBMS	ORACLE	192.	TOAD.EXE	KCSONG	송교...		ADMIN...	KETEP...	2013/0...		N/A				
Critical	Agent 사용자Telnet 접근 차단	2013/09/17 12:00:57	통합DB_1		TELNET	192.		UNKNOWN	정원...	전산실			2013/0...		Kill Ses...				

구분	현황	향후 추진	비고
DB	중요정보에 대한 데이터 및 패턴 암호화	중요정보에 대한 데이터 및 패턴 암호화	향후 추진
쿼리	쿼리 결과물에 대한 데이터 마스킹	쿼리 결과물에 대한 데이터 마스킹	향후 추진
암호화 키	암호화 키 위변조 방지	암호화 키 위변조 방지	향후 추진

DB 암호화(기능 및 정책)

◆ DB암호화 기능

- ▶ 중요정보에 대한 데이터 및 패턴 암호화
- ▶ 운영환경에 따른 API 및 Plug-In 방식의 유연 적용
- ▶ 쿼리 결과물에 대한 데이터 마스킹
- ▶ 암호화 키 위변조 방지

◆ DB암호화 키 정책

- ▶ 전체 암호화(normal)와 1, 7, 8 자리 이후 암호화가 되는 부분암호화 적용
- ▶ 매니저를 통해 복호화 권한 통제
- ▶ 암호화 키는 국정원 및 국제 표준에서 권고하는 바와 같이 일정 수준의 엔트로피 이상에서 Random 함수를 실행하여 생성
- ▶ 생성 알고리즘은 ARIA 방식 적용

DB 암호화(화면)

구분	항목	현황	비고
암호화	데이터베이스 암호화	완료	
인증	사용자 인증	완료	
접근	접근 권한 관리	완료	
백업	백업/복구	완료	
로그	로그 관리	완료	
모니터링	모니터링	완료	
합계			

암호화 정보

The screenshot shows the SecureDB Manager interface for 'ktep_DB_1'. The left pane displays a tree view with 'XDB_SERVER' expanded to show '암호화 컬럼 정보', '사용자', and '암호화 키'. The main pane displays a table of encryption details for the 'KETEP_DB' database.

데이터베이스 / 소유자	테이블	컬럼	암호화 키ID	암호 알고리즘	랜덤 이니셜백터	무결성 알고리즘	생성 일자	최근 수정 일자	테이블 유형
KETEP_DB / KETEP_OW	KETEP_TB	NORMAL	ketep_key	ARIA	No	사용안함	2013/03/11 14:47:02	2013/03/11 14:47:02	테이블
KETEP_DB / KETEP_OW	KETEP_TB	PATTERN1	ketep_key	ARIA	No	사용안함	2013/05/31 20:36:15	2013/05/31 20:36:15	테이블
KETEP_DB / KETEP_OW	KETEP_TB	PATTERN7	ketep_key	ARIA	No	사용안함	2013/03/11 14:47:44	2013/03/11 14:47:44	테이블
KETEP_DB / KETEP_OW	KETEP_TB	PATTERN8	ketep_key	ARIA	No	사용안함	2013/03/11 14:48:23	2013/03/11 14:48:23	테이블

DB 암호화(화면)

구분	항목	현황	비고
DB	암호화 여부	완료	
DB	암호화 키 ID	ketep_key	
DB	암호화 알고리즘	ARIA	
DB	랜덤 이니셜 벡터	<input type="checkbox"/>	
DB	Integrity 알고리즘	사용안함	
DB	생성 일자	2013/05/31 20:36:15	
DB	최근 수정 일자	2013/05/31 20:36:15	

암호화 컬럼정보

The screenshot shows the XecureDB Manager interface. On the left, a tree view shows the database structure: ktep_DB_1(서비스 서버) > XDB_SERVER > 암호화 컬럼 정보. The main area displays a table of users with columns for '사용자', '생성 일자', and '최근 수정 일자'. The user 'KETEP_USER' is selected, and a dialog box titled '암호화된 컬럼 등록정보' is open, showing encryption details for this user.

사용자	생성 일자	최근 수정 일자
KETEP_USER	2013/03/11 14:46:15	2013/03/11 16:11:12

암호화된 컬럼 등록정보	
암호화 키 ID	ketep_key
암호 알고리즘	ARIA
랜덤 이니셜 벡터	<input type="checkbox"/>
Integrity 알고리즘	사용안함
생성 일자	2013/05/31 20:36:15
최근 수정 일자	2013/05/31 20:36:15

DB 암호화(화면)

구분	연속적	일회적	적용일자	취급일자
기타				
암호화	2013/03/11 14:47:02	2013/03/11 14:47:02	2013/03/11 14:47:02	2013/03/11 14:47:02
복구	2013/03/11 14:47:44	2013/03/11 14:47:44	2013/03/11 14:47:44	2013/03/11 14:47:44
생성	2013/03/11 14:48:23	2013/03/11 14:48:23	2013/03/11 14:48:23	2013/03/11 14:48:23

암호화 정책백업

The screenshot shows the XecureDB Manager interface. The main window displays a list of databases with their encryption policies. A dialog box titled '서비스 서버 복구 대화창' (Service Server Backup Confirmation) is open, showing a list of backup files and their details.

데이터베이스명	소유자	테이블	컬럼	암호화 키ID	암호 알고...	랜덤 이니셜...	무결성 알고...	생성 일자	최근 수정 일자	테이블...
KETEP_DB	KETEP_OW	KETEP_TB	NORMAL	ketep_key	ARIA	No	사용안함	2013/03/11 14:47:02	2013/03/11 14:47:02	테이블
KETEP_DB	KETEP_OW	KETEP_TB	PATTERN1	ketep_key	ARIA	No	사용안함	2013/05/31 20:36:15	2013/05/31 20:36:15	테이블
KETEP_DB	KETEP_OW	KETEP_TB	PATTERN7	ketep_key	ARIA	No	사용안함	2013/03/11 14:47:44	2013/03/11 14:47:44	테이블
KETEP_DB	KETEP_OW	KETEP_TB	PATTERN8	ketep_key	ARIA	No	사용안함	2013/03/11 14:48:23	2013/03/11 14:48:23	테이블

서비스 서버 백업 파일 리스트	세부정보						
<table border="1"> <thead> <tr> <th>백업 파일 이름</th> <th>백업 날짜</th> <th>설명</th> </tr> </thead> <tbody> <tr> <td>backup_20130809</td> <td>2013/08/09 13:45:28</td> <td>정책백업</td> </tr> </tbody> </table>	백업 파일 이름	백업 날짜	설명	backup_20130809	2013/08/09 13:45:28	정책백업	세부정보 백업파일 이름 backup_20130809 생성 일자 2013/08/09 13:45:28 설명 정책백업
백업 파일 이름	백업 날짜	설명					
backup_20130809	2013/08/09 13:45:28	정책백업					

DB 암호화(화면)

구분	구분	구분	구분
구분	구분	구분	구분
구분	구분	구분	구분
구분	구분	구분	구분
구분	구분	구분	구분
구분	구분	구분	구분
구분	구분	구분	구분
구분	구분	구분	구분
구분	구분	구분	구분
구분	구분	구분	구분

암호화 키 관리

암호화 키	참조횟수	생성 일자	최근 수정 일자
ketep_key	4	2013/03/11 14:46:31	2013/03/11 14:46:31

DB 암호화(화면)

구분	항목	내용	비고
DB	암호화 대상 DB	암호화 대상 DB	암호화 대상 DB
	암호화 대상 테이블	암호화 대상 테이블	암호화 대상 테이블
암호화	암호화 방법	암호화 방법	암호화 방법
	암호화 옵션	암호화 옵션	암호화 옵션
암호화 결과	암호화 성공	암호화 성공	암호화 성공
	암호화 실패	암호화 실패	암호화 실패

암호화 로그

로그보기

정책로그 전체보기 Master

날짜 : 2013년 8월 12일 이전 오늘 다음 2013-08-12 ~ 2013-08-12 검색 저장

시스템 로그	날짜	IP	UserID	DBName	Table	Owner	Column	Command	Result	Result V...	비고
키변경 로그	20130812080001	127.0.0.1	KETEP_U...	KETEP_DB	KETEP_TB	KETEP_OW	NORMAL	Sync Con...	요청 시도	0	
	20130812080001	127.0.0.1	KETEP_U...	KETEP_DB	KETEP_TB	KETEP_OW	NORMAL	Sync Con...	요청 성공	0	
에러 로그	20130812080007	127.0.0.1	KETEP_U...	KETEP_DB	KETEP_TB	KETEP_OW	NORMAL	Sync Con...	요청 시도	0	
	20130812080007	127.0.0.1	KETEP_U...	KETEP_DB	KETEP_TB	KETEP_OW	NORMAL	Sync Con...	요청 성공	0	
ktep_DB_1	20130812080517	127.0.0.1	KETEP_U...	KETEP_DB	KETEP_TB	KETEP_OW	NORMAL	Sync Con...	요청 시도	0	
	20130812080517	127.0.0.1	KETEP_U...	KETEP_DB	KETEP_TB	KETEP_OW	NORMAL	Sync Con...	요청 성공	0	
	20130812080750	192.	KETEP_U...	KETEP_DB	KETEP_TB	KETEP_OW	PATTERN7	Sync Con...	요청 시도	0	
	20130812080750	192.	KETEP_U...	KETEP_DB	KETEP_TB	KETEP_OW	PATTERN7	Sync Con...	요청 성공	0	
	20130812080916	192.	KETEP_U...	KETEP_DB	KETEP_TB	KETEP_OW	PATTERN7	Sync Con...	요청 시도	0	
	20130812080916	192.	KETEP_U...	KETEP_DB	KETEP_TB	KETEP_OW	PATTERN7	Sync Con...	요청 성공	0	
	20130812080926	127.0.0.1	KETEP_U...	KETEP_DB	KETEP_TB	KETEP_OW	NORMAL	Sync Con...	요청 시도	0	
	20130812080926	127.0.0.1	KETEP_U...	KETEP_DB	KETEP_TB	KETEP_OW	NORMAL	Sync Con...	요청 성공	0	
	20130812080927	127.0.0.1	KETEP_U...	KETEP_DB	KETEP_TB	KETEP_OW	NORMAL	Sync Con...	요청 시도	0	
	20130812080927	127.0.0.1	KETEP_U...	KETEP_DB	KETEP_TB	KETEP_OW	NORMAL	Sync Con...	요청 성공	0	
	20130812081404	127.0.0.1	KETEP_U...	KETEP_DB	KETEP_TB	KETEP_OW	NORMAL	Sync Con...	요청 시도	0	
	20130812081404	127.0.0.1	KETEP_U...	KETEP_DB	KETEP_TB	KETEP_OW	NORMAL	Sync Con...	요청 성공	0	
	20130812081406	127.0.0.1	KETEP_U...	KETEP_DB	KETEP_TB	KETEP_OW	NORMAL	Sync Con...	요청 시도	0	
	20130812081406	127.0.0.1	KETEP_U...	KETEP_DB	KETEP_TB	KETEP_OW	NORMAL	Sync Con...	요청 성공	0	
	20130812081406	127.0.0.1	KETEP_U...	KETEP_DB	KETEP_TB	KETEP_OW	NORMAL	Sync Con...	요청 시도	0	

작업결재(기능 및 정책)

구분	연관대상	실시내용	적용대상	유지관리 방법
기능	연관대상 관리	연관대상 관리	연관대상 관리	유지관리 방법
정책	연관대상 관리	연관대상 관리	연관대상 관리	유지관리 방법
구분	연관대상 관리	연관대상 관리	연관대상 관리	유지관리 방법
구분	연관대상 관리	연관대상 관리	연관대상 관리	유지관리 방법
구분	연관대상 관리	연관대상 관리	연관대상 관리	유지관리 방법
구분	연관대상 관리	연관대상 관리	연관대상 관리	유지관리 방법
구분	연관대상 관리	연관대상 관리	연관대상 관리	유지관리 방법
구분	연관대상 관리	연관대상 관리	연관대상 관리	유지관리 방법
구분	연관대상 관리	연관대상 관리	연관대상 관리	유지관리 방법

◆ DB작업결재 기능

- SQL의 불법적인 변경을 방지하기 위해 사전 승인 후 변경
- 특정 테이블/컬럼 단으로 SQL문 질의 시 결재 통하여 해당 실행 권한 획득 후 실행

◆ DB작업결재 정책

- Agent 사용자 한정하여 SQL TYPE 별로 결재 시스템 적용
- 에이전트 사용자 외 접근 차단 정책 적용하여 우회 접근 방지

작업결재

구분	구분명	구분명	구분명	구분명
구분	구분명	구분명	구분명	구분명
구분	구분명	구분명	구분명	구분명
구분	구분명	구분명	구분명	구분명
구분	구분명	구분명	구분명	구분명
구분	구분명	구분명	구분명	구분명
구분	구분명	구분명	구분명	구분명
구분	구분명	구분명	구분명	구분명
구분	구분명	구분명	구분명	구분명
구분	구분명	구분명	구분명	구분명

작업 기안 관리

SQL 기안

Title :

Description :

DB 정보

Database :

DB User :

쿼리 정보

! 쿼리

There are no items to show.

실행 정보

유효기간 시작 :

유효기간 종료 :

실행 제한 회

튜닝요청 :

모든 프로그램

결재 정보

결재경로 :

긴급결재: 이 안건을 업무 통제 시간에도 실행 가능하도록 요청합니다.

구분	항목	현황	비고
DB	DB 접근 제어	접근 제어	접근 제어
	DB 보안	DB 보안	DB 보안
DB	DB 접근 제어	접근 제어	접근 제어
	DB 보안	DB 보안	DB 보안
DB	DB 접근 제어	접근 제어	접근 제어
	DB 보안	DB 보안	DB 보안

작업결재

서버보안 적용

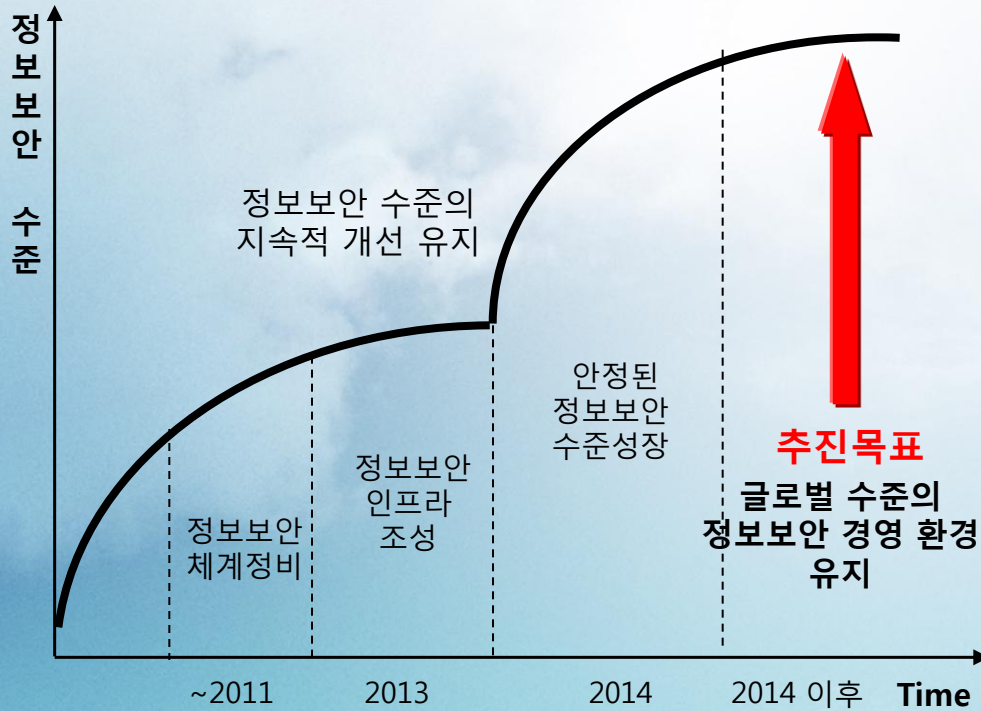
대상	접근제어목록	자동권한	상속 횟수	하위디...	설명
/usr/sbin/halt	deny_shutdown	none	0	No	Deny system shutdown
/usr/sbin/reboot	deny_shutdown	none	0	No	Deny system shutdown
/usr/sbin/shutdown	deny_shutdown	none	0	No	Deny system shutdown
/usr/sbin/init	deny_shutdown	none	0	No	Deny system shutdown
/usr/sbin/fasthalt	deny_shutdown	none	0	No	Deny system shutdown
/usr/sbin/fastboot	deny_shutdown	none	0	No	Deny system shutdown
/usr/sbin/syslogd	antikill_default_root	none	0	No	로그데몬보호
/etc/init	deny_shutdown	none	0	No	Deny system shutdown



III

향후 DB보안 추진방향

연도별 추진목표



DQC-S 인증

구분	수준
4레벨	취약점 분석
3레벨	작업결재
2레벨	암호화
1레벨	접근제어



* 상위레벨의 수준은 하위레벨 수준 충족전제

정보보안 관리체계 글로벌 수준화

글로벌 수준의 한국에너지기술평가원의
개선된 정보보호관리체계 (TO-BE)



감사합니다

KOREA INSTITUTE OF ENERGY TECHNOLOGY
EVALUATION AND PLANNING

