정보

- 정보란 '어떠한 출처로부터 유래된 지식'. 유의미하고 가치를 가진 것

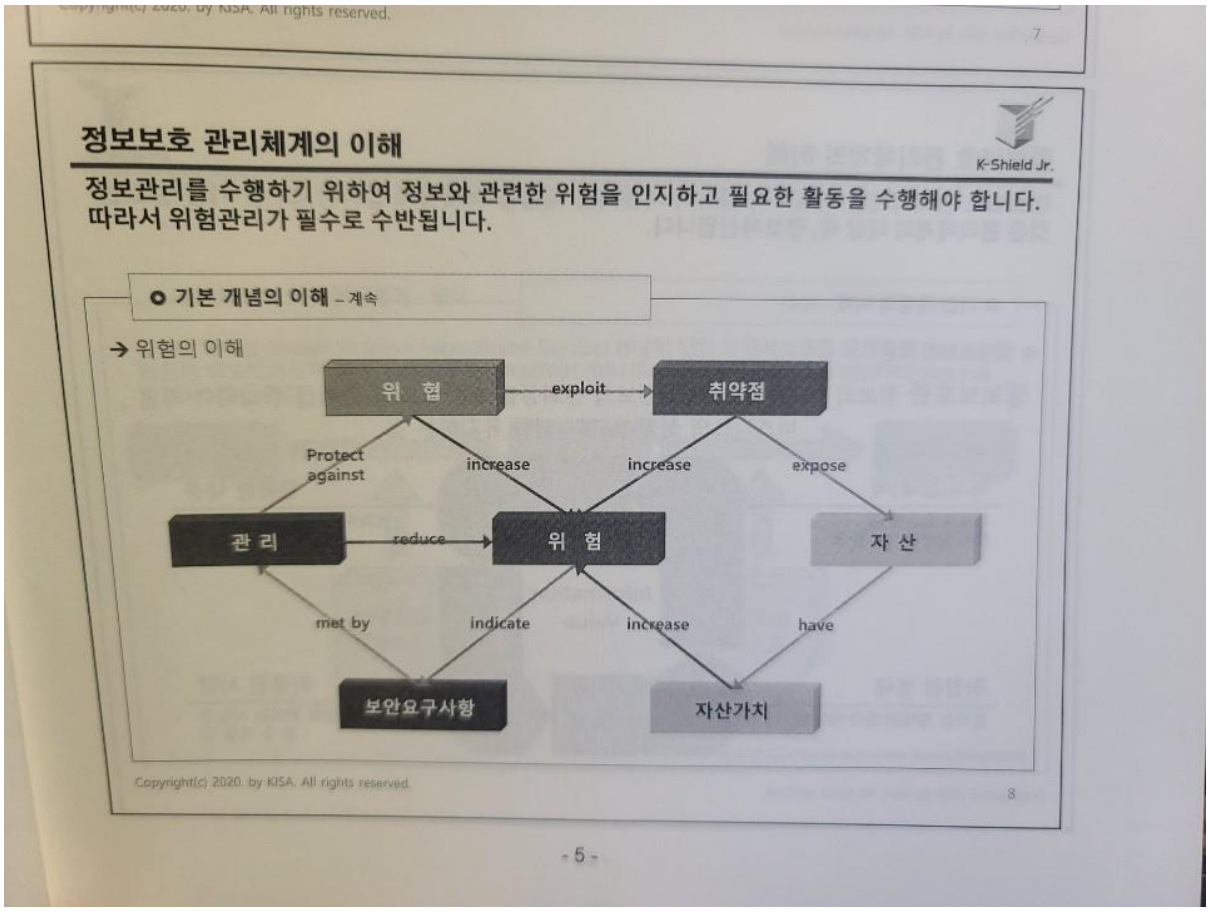
- 정보는 다른 중요 비즈니스 자산과 마찬가지로 조직에 있어 가치가 있고, 지속적으로 적절히 보호되어야 할 필요가 있는 자산이다.

- 정보의 특성 :

가용성(Availability) : 인가된 사용자가 필요 시 정보 및 관련 자산에 접근할 수 있도록 보장하는 것(파괴/지체로부터의 보호) (예) 통신사, 핸드폰)

무결성(Integrity) : 정보 및 처리방법의 정확성과 완전성을 보장하는 것(변조로부터의 보호)예)통장

기밀성(Confidentiality) : 접근이 인가된 자만이 해당 정보에 접근할 수 있다는 것을 보장하는 것(공개로부터의 보호)



위험에 영향을 줄 수 있는 변수들

- 자산 : 조직에 가치가 있는 유/무형의 경제적/비경제적 자원보호의 대상

- 위협 : 자산에 원치 않는 결과나 해악을 미칠 수 있는 사건이나 행위

- 취약점 : 위협이 발생하기 위한 사전 조건이나 상황

정보보호의 개념

- 정보보호란 정보의 "4R"을 확보하여 정보의 신뢰성을 보장하고 그 가치를 증대하여 기업 비즈니스의 성장 및 연속성을 유지하는 것.

- 적시에(정보가 필요할 때 즉시 활용이 가능할 것. **R**ight Time)

- 적절한 형태(원하는 형태로 활용 가능할 것. **R**ight Form)

- 정확한 내용(정확하고 신뢰할 수 있을 것. **R**ight Information)

- 허용된 사람(권한이 부여된 사람만 볼 수 있을 것. **R**ight People)

정보보호 관리체계

- 정의 : 조직에서 비즈니스의 연속성 확보를 위하여 각종 위협으로부터 정보자산을 보호하기 위한 위험관리 기반의 체계적이고 지속적인 프로세스 개선활동이다.

KISA-ISMS 인증제도

- 주요 정보자산 유출 및 피해를 사전 예방하고 대처할 목적으로 기업이 수립 및 운영 중인 ISMS가 인증심사 기준에 적합한 지를 인증하는 제도

- 법적 근거 : 정보통신망법 제 47조

- 인증유효기간 : 3년 (매년 1회 사후심사)

- 인증체계 : 과학기술정보통신부, 인증기관(KISA), 인증위원회, 인증심사원

- PDCA 모델을 기반으로 한 SPDCA 프로세스를 제시하고 있다. (Plan(계획) – Do(실행) – Check(평가) – Act(개선))

정보보호관리체계 Life Cycle

- 정보보호 정책수립 및 범위 설정 -> 경영진 책임 및 조직 구성 -> 위험관리 -> 정보보호 대책 구현 -> 사후관리 // 반복

정보보호 관리전략 TOP 10

1. 최고 경영자의 후원과 확약을 받아라

- 필요성 : 정보보호 프로그램은 임원진에 의해 공식적으로 추진되거나 지지를 받는 경우 더욱 성공적이다.

- 전략 : 위험 식별, 문제점의 수치화 (비용, 과태료 등 금전적 문제로 예측 가능하도록). 임원진을 위한 보고주기 확립. 사례 중심으로 이해할 수 있도록

2. 전사적인 지원과 참여를 이끌어라

- 필요성 : 정보보호 프로그램은 사업의 목표를 지원할 수 있어야 한다. 사업 단위의 적극적 참여 시 더욱 성공적이다.

- 전략 : 규칙적, 지속적인 장기활동 계획 개발. 조직 단위로 스스로 정보보호 활동에 참여할 수 있는 필요성을 인식하도록 계도. 이해관계자와의 관계 발전

3. 산업 표준들을 사용, 적용, 연계하라

- 필요성 : KISA ISMS와 같은 정보보호 관리표준을 채택. COBIT, ITIL과 같은 IT 표준 채택. 표준의 채택은 기업 간의 협력을 더욱 효과적이며 효율적으로 이끈다.

- 전략 : 산업 표준을 사용 (TTA, ITU-T, NIST 등 공식 표준 권장). IT 프레임워크 구축

4. 사람들이 쉽게 정당한 일을 하도록 만들어라

- 필요성 : 사람들이 정보보호 프로그램에 참여하고, 기업의 폭 넓은 지지를 얻는 간단하고 효과적인 기술. 정보보호는 업무를 방해하지 않아야 한다.

- 전략 : 정책과 표준은 명확하게 작성. 정보보호 업무 통합. 업무 프로세스가 적용된 정보보호 활동

5. 프로세스를 세련되게 다듬어서 문서화 후 공표하라

- 필요성 : 프로세스가 명백하게 문서화되어 있지 않을 경우, 불확실한 가정을 통한 결정을 내림. 프로세스는 역할과 책임, 활동, 적절한 서비스 수준 협약(SLA)을 정의

- 전략 : 프로세스의 시각적 문서화. 프로세스의 효과 측정

6. 훈련과 교육이 핵심임을 인지하라

- 필요성 : 훈련과 교육은 가장 효과적이고 강력한 기술. 기업은 전사적 정보보호 훈련과 인식제고 프로그램을 개발 / 유지. 운전면허가 없으면 LAMBORGHINI도 무쓸모

- 전략 : 조직의 전 계층을 훈련. 개개의 조직, 업무, 직군 등을 고려한 업무와 연계된 차별화된 훈련 시행

7. 보안이 아니라 위험을 관리하라

- 필요성 : 최대한의 보안의 강요가 아닌 위험관리, 법률과 규제에 대한 순응, 내부감사, 통제 등을 연계한 전사적인 위험관리가 필요함.

- 전략 : 기업의 사업전략의 이해. 위험평가를 수행하고 그 결과를 사업 결정 시 반영하도록 프로세스 수립

8. 사실과 수치들을 관리하라

- 필요성 : 측정지표에 따른 수집, 분석을 통해 기업은 객관화된 근거에 의하여 현명한 경영의사를 결정, 지시할 수 있다. 측정지표는 현 상황을 통해 용이한 의사결정, 상과 향상을 도와주는 도구

- 전략 : 측정지표 프레임워크에 대한 이해. 기업에 의미 있는 측정지표 개발. 측정지표 프로그램을 통해 얻고자 하는 바를 명확히 선정하고 파악

9. 내부 규정 준수를 지원하라

- 필요성 : 타율적인 규제 강조는 반발력만 키움. 기업 정보보호 프로그램을 개발하고 장지적으로 유지해야 함.

- 전략 : 규제 준수의 자율성 강조. 애매한 요구사항은 명확하게 수정하고 법적 요구사항을 중재. 규정 준수에 따른 징계보다는 이득이 있도록 설정

10. 새로운 기업 비즈니스의 창의적 시도를 지원하라

- 필요성 : 정보보호는 기업의 반드시 필요한 부분임을 인식해야 함. 위협을 줄이고, 기존의 비즈니스 내에 정보보호 프로그램이 투명하게 통합

- 전략 : 정보보호 관련 회의에 경영진 참석 유도. 비즈니스 위험의 관점에서 정보보호를 설명.

정보보호 관리체계 수립 절차

- 정보보호 정책수립 및 범위설정(정보보호 정책의 수립. 범위 설정)

-> 경영진 책임 및 조직구성(경영진 참여. 정보보호 조직 구성 및 자원 할당)

-> 위험관리(위험관리 방법 및 계획 수립. 위험 식별 및 평가. 정보보호대책 선정 및 이행계획 수립)

-> 정보보호 대책구현(정보보호대책의 효과적 구현. 내부 공유 및 교육)

-> 사후관리(법적 요구사항 준수검토. 정보보호 관리체계 운영현황 관리. 내부 감사)

사전 단계

- 수행조직을 구성한다. 통상적으로 TFT 형식으로 구성.

운영 절차 수립 방법

- Step#1. 정책 분석 및 요구사항 확인

-> 정보보호 정책 및 지침 등에서 적용될 가능성이 있는 조항 확인

-> 해당 조항에서의 요구조건 및 관련 보안 요구사항 확인

- Step#2. 절차 정리 및 시뮬레이션

-> 결재처리, 공문 등 반드시 수행해야 할 절차 확인

-> 각 절차의 프로세스화 작성

-> 해당 프로세스의 이행 시 발생 가능한 제약사항, 문제점 등 도출

- Step#3. 필요 양식 개발

-> 요구사항 등에서 확인된 반드시 기록해야 할 사항 등의 존재여부 확인

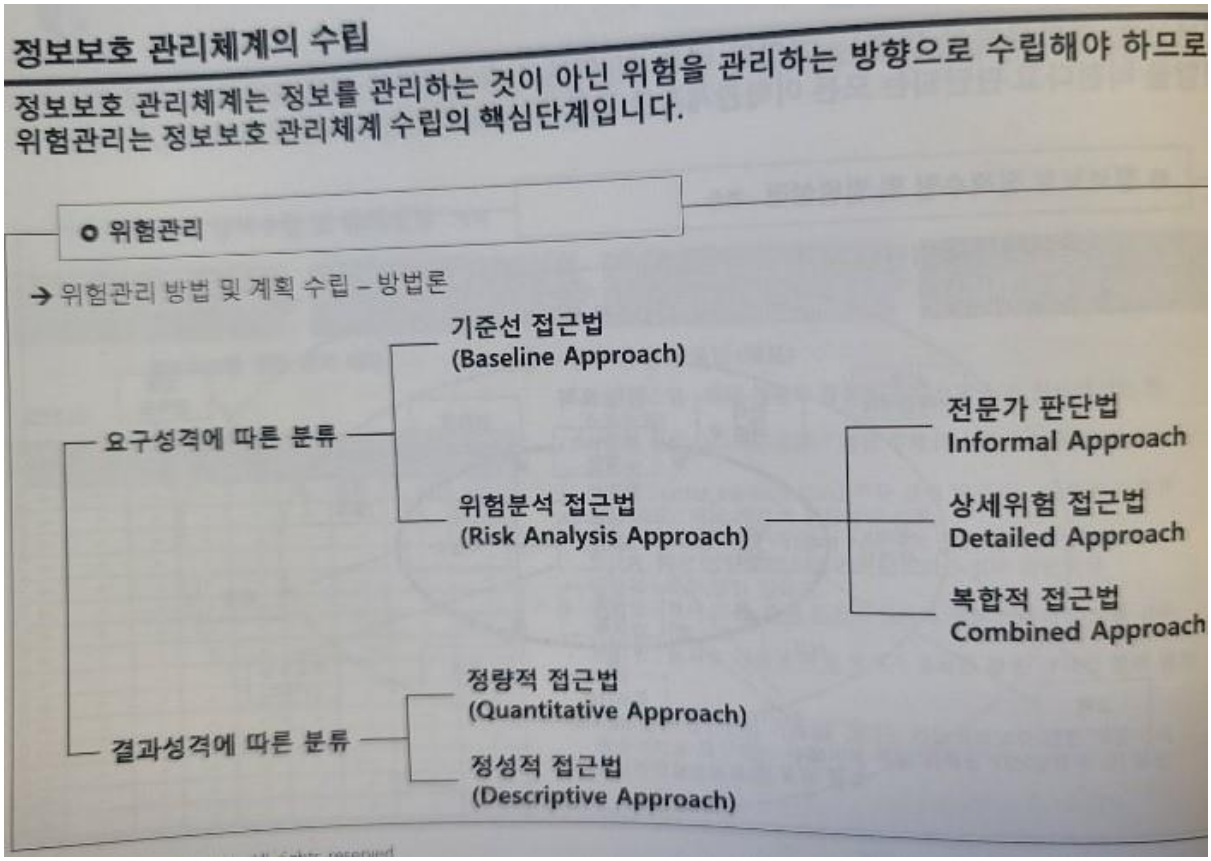
-> 해당 기록사항을 효율적으로 작성 및 관리할 수 있는 양식 개발(필요 시)

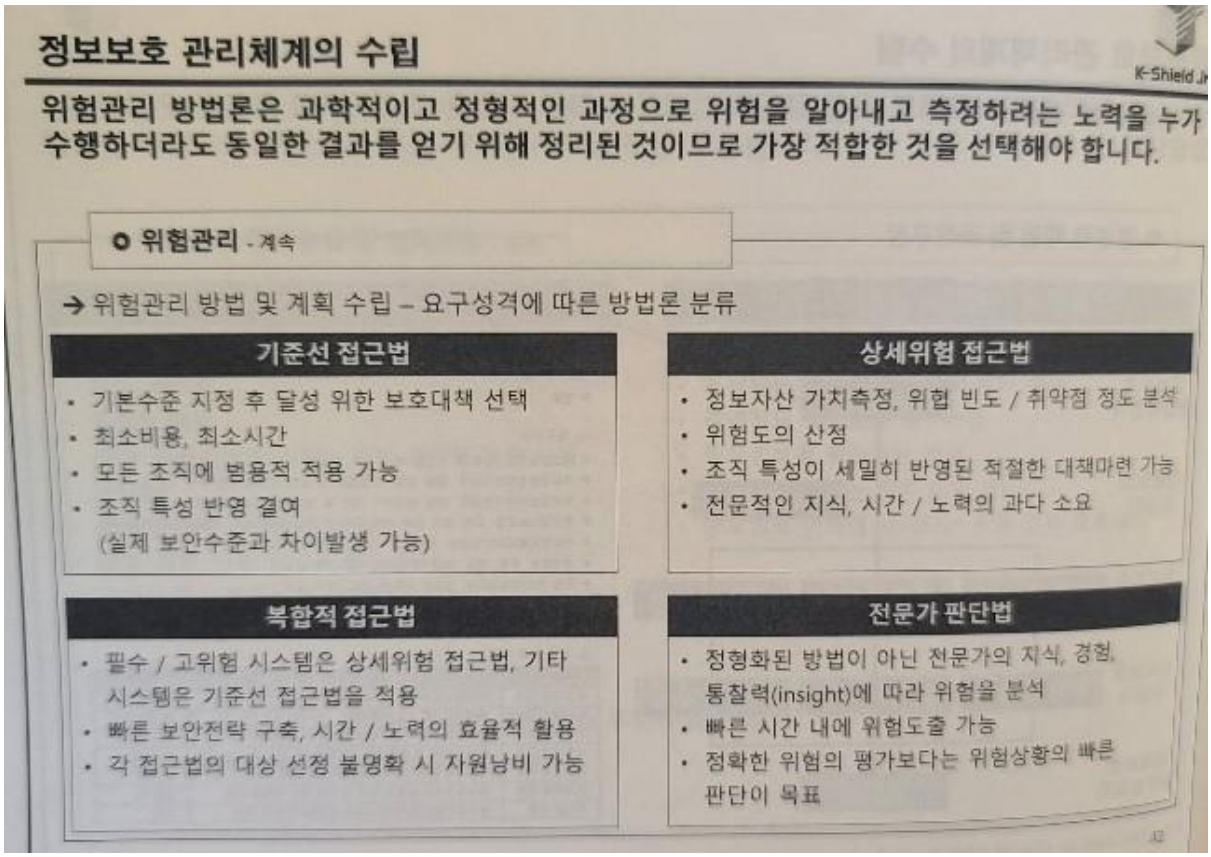
- Step#4. 절차 운영 및 피드백

-> 해당 절차 및 양식을 관련 부서에게 전달하고 충분히 설명

-> 계도기간 등을 적용하여 숙지할 수 있도록 지원

위험관리


정보보호 관리체계의 수립
정보보호 관리체계는 정보를 관리하는 것이 아닌 위험을 관리하는 방향으로 수립해야 하므로
위험관리는 정보보호 관리체계 수립의 핵심단계입니다.
위험관리
→ 위험관리 방법 및 계획 수립 – 방법론
요구성격에 따른 분류
기준선 접근법
(Baseline Approach)
위험분석 접근법
(Risk Analysis Approach)
전문가 판단법
Informal Approach
상세위험 접근법
Detailed Approach
복합적 접근법
Combined Approach
결과성격에 따른 분류
정량적 접근법
(Quantitative Approach)
정성적 접근법
(Descriptive Approach)


정보보호 관리체계의 수립
위험관리 방법론은 과학적이고 정형적인 과정으로 위험을 알아내고 측정하려는 노력을 누가 수행하더라도 동일한 결과를 얻기 위해 정리된 것이므로 가장 적합한 것을 선택해야 합니다.
위험관리 - 계속
→ 위험관리 방법 및 계획 수립 – 요구성격에 따른 방법론 분류
기준선 접근법
• 기본수준 지정 후 달성 위한 보호대책 선택
• 최소비용, 최소시간
• 모든 조직에 범용적 적용 가능
• 조직 특성 반영 결여
(실제 보안수준과 차이발생 가능)
상세위험 접근법
• 정보자산 가치측정, 위협 빈도 / 취약점 정도 분석
• 위험도의 산정
• 조직 특성이 세밀히 반영된 적절한 대책마련 가능
• 전문적인 지식, 시간 / 노력의 과다 소요
복합적 접근법
• 필수 / 고위험 시스템은 상세위험 접근법, 기타 시스템은 기준선 접근법을 적용
• 빠른 보안전략 구축, 시간 / 노력의 효율적 활용
• 각 접근법의 대상 선정 불명확 시 자원낭비 가능
전문가 판단법
• 정형화된 방법이 아닌 전문가의 지식, 경험, 통찰력(insight)에 따라 위험을 분석
• 빠른 시간 내에 위험도출 가능
• 정확한 위험의 평가보다는 위험상황의 빠른 판단이 목표

○ 위험관리 - 계속

→ 위험관리 방법 및 계획 수립 – 결과성격에 따른 방법론 분류

정성적 접근법

구분	기밀성	무결성	가용성
기준	외부에 공개 / 유출	변조 또는 오류발생	접근 및 서비스 중단
높음(3)	심각한 또는 치명적인 영향 초래		
중간(2)	상당한 영향 초래		
낮음(1)	피해를 무시할 수 있는 수준		

- [상], [중], [하]와 같은 설명 변수에 따라 위험을 표시
- 위험의 크기는 주관적 지표로 표시
- Risk RoI에 대한 객관적 산정의 어려움 존재

정량적 접근법

자산명	회계정보	구분	정보	단위	안전	기밀성	무결성	가용성	
						√	√		
위협/취약성			잠재적 영향			위험			
위협/취약성	발생가능성		잠재적 영향		피해	C	I	A	ALE
패스워드 추측으로 타인이 사용자 아이디를 도용	연1회		회계정보노출/변경		1,000	√	√		1,000
백신이 감지 못하는 바이러스/웜 발생	월1회		3일 이내의 업무 손실		10	√	√		120
불법 소프트웨어 다운로드 및 사용으로 인한 PC 장애	분기1회		3일 이내의 업무 손실		10			√	40
인가자의 의도적인 정보 수출/변경	10년 1회		접근 기록 및 감사 부재		10,000	√	√		1,000

- 위험발생 확률과 손실크기에 대한 기대가치 분석
- 복잡한 산술식에 의한 계산

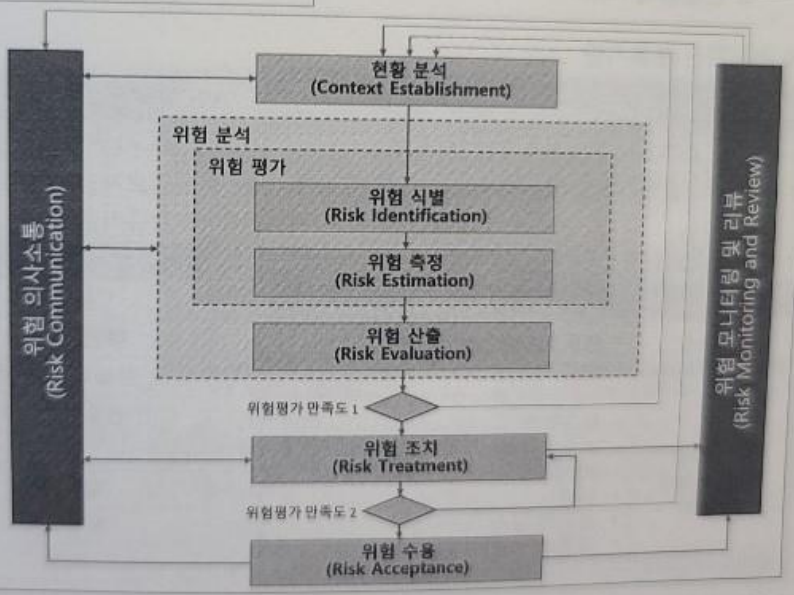
정보보호 관리체계의 수립

K-Shield Jr.

위험관리를 위한 방법론에 대한 이해도 중요하지만 어떠한 방법론이라도 위험관리 프로세스를 벗어날 수는 없습니다.

○ 위험관리 - 계속

→ ISO/IEC 27005에서는 위험관리를 위한 프로세스를 제시하고 있으며, 거의 모든 국가 및 관련 기준에서 이 위험관리 프로세스를 준용하고 있음



○ 위험관리 - 계속

정보자산 식별

정보자산 식별

자산분류체계 수립

- 조직의 유형 또는 무형 정보자산 파악
- 정보자산 분류 기준 및 절차 도출
- 정보자산 분류 및 계층화 실시
- 조직의 자산가치와 중요성 평가
- 정보자산의 중요성, 보안성에 따라 차별화된 운용 및 관리
- 분류 기준에 따른 자체 자산관리 시스템 및 체계 개발 및 유지보수
- 조직의 유형 또는 무형 정보자산 파악

정보자산 목록 작성

NO	자산번호	구분	자산명	용도	OS	응용프로그램	IP	중요도등급	위치	소유자	관리자
1	SV-08-001	서버	DB1 서버	데이터베이스	windows 2003	356.0	192.x.x.x	가등급	서버실	홍길동 부장	김길동정장
2	SV-08-002		DB2 서버	데이터베이스	windows 2000	MS-SQL	192.x.x.x	가등급	서버실	홍길동 부장	김길동정장
3	SW-08-001	네트워크	L4	로드밸런싱	windows 2000	-	194.x.x.x	나등급	IDC	홍길동 부장	김길동정장
4	SW-08-002		일반스위치	스위칭	windows 2000	-	195.x.x.x	가등급	서버실	홍길동 부장	김길동정장
6	SS-08-001	보안장비	방화벽	방화벽	windows 2003	VPN-XXX	196.x.x.x	가등급	서버실	홍길동 부장	김길동정장
7	SS-08-002		방화벽	통합방화벽	windows 2000	통합방화벽XXX	197.x.x.x	다등급	서버실	홍길동 부장	김길동정장
8	SQ-09-001	시설	에어컨	공조조절	windows 2000	D-Com	198.x.x.x	다등급	서버실	홍길동 부장	김길동정장

※ 유의사항

- 조직의 일반적인 자산과 구분하여 관리할 필요 없음
- 누락됨 없고, 중복되지 않게 파악
- 각 자산을 고유하게 식별할 수 있는 번호체계, ownership 등 기록

○ 위험관리 - 계속

→ 정보자산 분류기준

ISO/IEC 27005의 예시

- ISO/IEC 27005는 정보보호 위험관리 기준
- 정보자산 분류기준의 예시는 Appendix B.에 수록

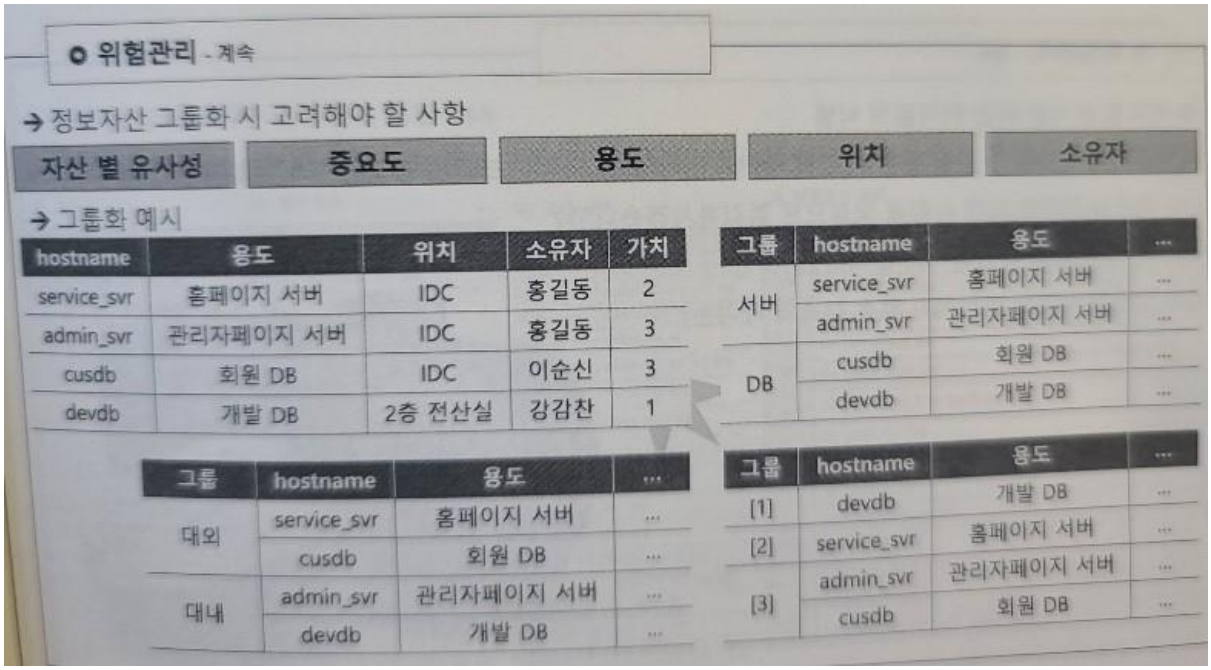
- 분류기준 (예시)

구분	세부 유형
중요 자산 (Primary Assets)	• 업무 프로세스 및 활동 • 정보
지원 자산 (Supporting Assets)	• 하드웨어 • 소프트웨어 • 네트워크 • 인력 • 물리적 장소 • 조직의 구조

KISA-ISMS의 예시

- 대부분의 기업에서 KISA-ISMS의 예시를 기반으로 정보자산 현황을 유지하고 있음
- 분류기준 (예시)

구분	
데이터	서버
데이터베이스	WEB/WAS
정보보호시스템	네트워크 장비
응용프로그램	소프트웨어
PC	문서
지원설비	인력
저장매체	지원서비스
시설	기타



위험관리 - 계속

→ 정보자산 그룹화 시 고려해야 할 사항

자산 별 유사성	중요도	용도	위치	소유자

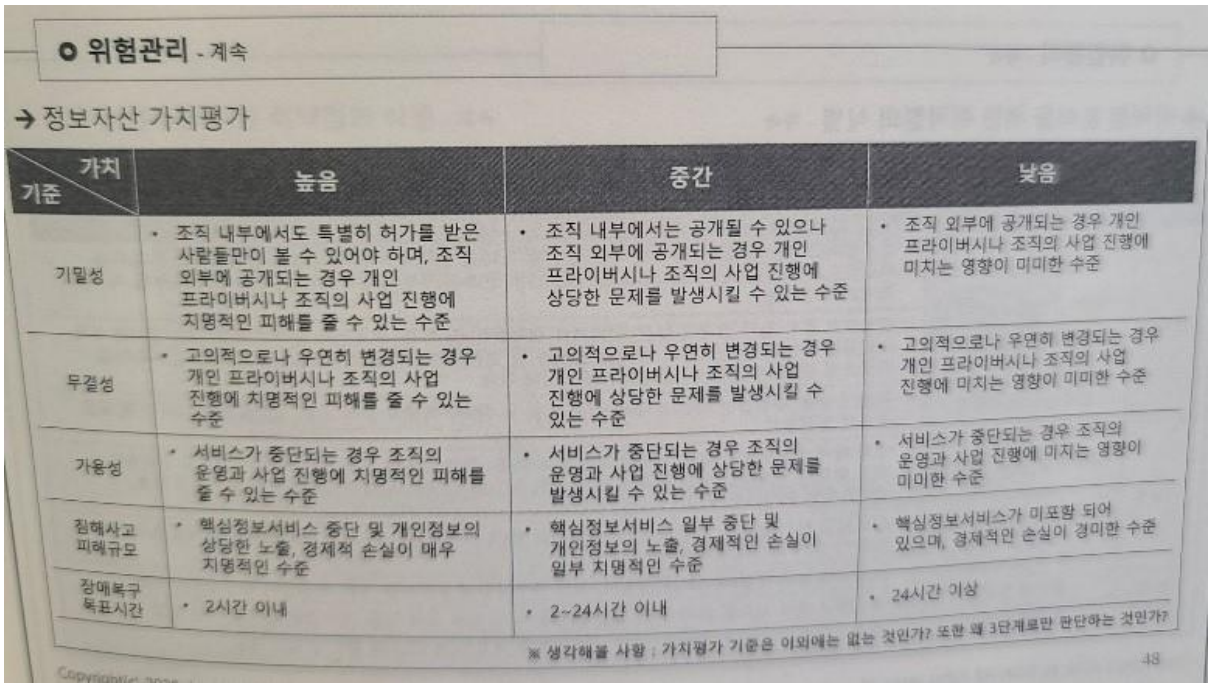
→ 그룹화 예시

hostname	용도	위치	소유자	가치
service_svr	홈페이지 서버	IDC	홍길동	2
admin_svr	관리자페이지 서버	IDC	홍길동	3
cusdb	회원 DB	IDC	이순신	3
devdb	개발 DB	2층 전산실	강감찬	1

그룹	hostname	용도	...
서버	service_svr	홈페이지 서버	...
	admin_svr	관리자페이지 서버	...
DB	cusdb	회원 DB	...
	devdb	개발 DB	...

그룹	hostname	용도	...
대외	service_svr	홈페이지 서버	...
	cusdb	회원 DB	...
대내	admin_svr	관리자페이지 서버	...
	devdb	개발 DB	...

그룹	hostname	용도	...
[1]	devdb	개발 DB	...
[2]	service_svr	홈페이지 서버	...
[3]	admin_svr	관리자페이지 서버	...
	cusdb	회원 DB	...



위험관리 - 계속

→ 정보자산 가치평가

가치 / 기준	높음	중간	낮음
기밀성	• 조직 내부에서도 특별히 허가를 받은 사람들만이 볼 수 있어야 하며, 조직 외부에 공개되는 경우 개인 프라이버시나 조직의 사업 진행에 치명적인 피해를 줄 수 있는 수준	• 조직 내부에서는 공개될 수 있으나 조직 외부에 공개되는 경우 개인 프라이버시나 조직의 사업 진행에 상당한 문제를 발생시킬 수 있는 수준	• 조직 외부에 공개되는 경우 개인 프라이버시나 조직의 사업 진행에 미치는 영향이 미미한 수준
무결성	• 고의적으로나 우연히 변경되는 경우 개인 프라이버시나 조직의 사업 진행에 치명적인 피해를 줄 수 있는 수준	• 고의적으로나 우연히 변경되는 경우 개인 프라이버시나 조직의 사업 진행에 상당한 문제를 발생시킬 수 있는 수준	• 고의적으로나 우연히 변경되는 경우 개인 프라이버시나 조직의 사업 진행에 미치는 영향이 미미한 수준
가용성	• 서비스가 중단되는 경우 조직의 운영과 사업 진행에 치명적인 피해를 줄 수 있는 수준	• 서비스가 중단되는 경우 조직의 운영과 사업 진행에 상당한 문제를 발생시킬 수 있는 수준	• 서비스가 중단되는 경우 조직의 운영과 사업 진행에 미치는 영향이 미미한 수준
침해사고 피해규모	• 핵심정보서비스 중단 및 개인정보의 상당한 노출, 경제적 손실이 매우 치명적인 수준	• 핵심정보서비스 일부 중단 및 개인정보의 노출, 경제적인 손실이 일부 치명적인 수준	• 핵심정보서비스가 미포함 되어 있으며, 경제적인 손실이 경미한 수준
장애복구 목표시간	• 2시간 이내	• 2~24시간 이내	• 24시간 이상

※ 생각해볼 사항 : 가치평가 기준은 이외에는 없는 것인가? 또한 왜 3단계로만 판단하는 것인가?

48

취약점 분석을 위한 취약점의 식별

- KISA-KSMS, ISO27001 등의 정보보호 관리체계 인증기준을 근거하여 식별하는 경우가 많음

- [주요 정보통신기반시설 취약점 분석, 평가 기준], [전자금융기반시설 취약점 분석 평가 항목]

- 미국 국립표준연구소(NIST)의 자료를 활용하기도 한다.

- 웹 취약점인 경우OWASP에서 발표하는 취약점을 활용한다.

○ 위험관리 - 계속

→ 취약점의 평가

취약점 평가 기준은 명확한 기준을 수립하여 평가할 수도 있으나, 취약점 목록에 따라 지정되어 있는 경우가 많습니다.

평가	내용
매우 취약 (Very High)	• 자산의 복구가 불가능하거나 피해규모가 매우 큰 경우
비교적 취약 (High)	• 최고 경영자나 상급관리자의 정밀한 검색 및 승인을 필요로 하는 위험을 발생시킬 수 있는 경우 • 자산의 복구는 가능하나 그 피해규모가 비교적 큰 경우
보통 (Medium)	• 취약점이 상급관리자의 검토 및 승인을 필요로 하는 정도의 위험을 발생시킬 수 있는 경우
취약하지 않음 (Low)	• 취약점이 자산에 별다른 영향을 끼치지 않는 경우 • 취약점이 자산에 약간의 영향은 끼치지만 그 영향이 미미하여 해당 자산이 하위관리자의 조치만으로 문제 해결이 가능한 경우

○ 위험관리 - 계속

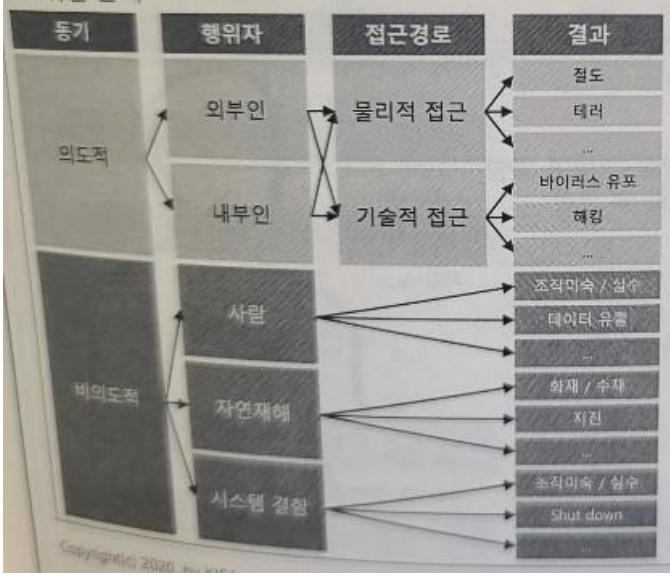
→ 위협 식별

- 자산에 대하여 발생했거나 발생할 가능성이 있는 보안 위협들을 조사하고 성질 유형 분류
- 피해규모 산출을 위하여 발생빈도, 피해종류, 발생가능성, 피해대상(자산)등을 모두 고려

식별 방법	위협 내용
자산에 대한 행위자	• 인간과•비인간으로 분류 - 인간 : 내부자, 외부자, 제3자 - 비인간 : 기술, 환경(사회적 문제), 자연(자연재해)
자산 접근 경로	• 네트워크 : 네트워크를 통해 접근(원격) • 물리 : 물리적으로 직접접근(로컬)
자산 접근 동기	• 우연 : 목적 없이 우연히 접근 • 고의 : 어떤 목적을 달성하기 위해 접근
위협이 자산에 미치는 결과	• 변경 : 자산의 내용이 수정되거나 변경된 상태 • 노출 : 자산의 내용이 공개 • 손실/파괴 : 자산이 손실되거나 파괴 • 방해 : 자산이 다른 방향으로 방해 받는 경우

○ 위험관리 - 계속

→ 위협 분석



위협 유형	위협 내용
내/외부의 인가된 인력에 대한 위협	• 내부 인력에 의한 정보 및 정보자산 유출 • 내부 인력에 의한 정보자산 비인가 조작 • 내부 인력에 의한 정보자산의 오남용 • 운영인력의 처리능력 미흡 • 운영인력의 실시
내/외부의 인가되지 않은 인력에 대한 위협	• 해커에 의한 정보 및 정보자산 유출 • 비인가 물리적 침입 • 비인가 자산 반입/반출 • 비인가자에 의한 정보자산 접근
시스템적 위협	• 웜/바이러스 침투 • 트래픽 과부하 • 유해사이트 접속 및 다운로드 • P2P사용
물리 / 환경적 위협	• 고온/고습 • 전원공급 중단 • 전압 불안정 • 환경적 오염
복합적 위협	• 보안사고 발생(타 위협사항 공동발생)

위협은 위험관리의 다른 변수와는 다르게 발생 빈도(얼마나 자주 발생하는가 또는 얼만큼 발생할 수 있는가)**를 측정하고 이를 계량화합니다.**

○ 위험관리 - 계속

→ 위협 평가기준

평가	빈도(발생주기 및 가능성)	계량화
매우 높음 (Very High)	시스템의 lifecycle 동안 매우 자주 발생함	4
높음 (High)	시스템의 Lifecycle 동안 다섯 번 이상 발생할 수 있음	3
중간 (Medium)	시스템 자신이 Lifecycle 동안 두세 차례 손해를 입을 수 있음	2
낮음 (Low)	자산의 Lifecycle 동안 거의 발생하지 않음	1

→ 상황에 따라 위협을 평가하는 경우 위협에 의한 영향을 추가로 고려하는 경우도 존재함

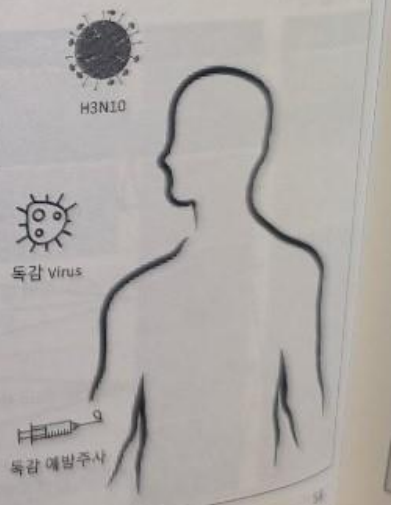
→ 하지만, 취약점을 동시에 고려하여 위험이 식별되는 경우 위험평가 시 중복이 발생함

위협은 위험관리에서 독립적으로 작용하는 변수일 수 없으며, 취약점에 종속적인 변수이므로 취약점과 동시에 고려할 수도 있습니다.

o 위험관리 - 계속

→ 우려사항(Concern)

- 위협은 취약점을 이용하여 자산에 영향을 끼치고 있으므로, 위협과 취약점을 구분하지 않고 일련의 시나리오의 형태로 도출 가능하며 이를 우려사항(Concern)이라 함
- 즉, 특정 자산이 가지고 있는 취약점과 해당 취약점 때문에 영향 받을 수 있는 위협으로 '상황을 가정한다'로 판단할 수 있음



※ 사람의 예시

독감 예방주사를 맞은 사람은 독감에 걸리지 않는다.

올해 새로운 바이러스가 발견되었다.

새로 발견된 바이러스는 백신이 개발되지 않았다.

- 독감 항체가 없어 독감에 걸릴 가능성
- 신종 바이러스의 백신개발 체계가 미약하여 사망할 가능성(?)

- Concern은 시나리오 형태로 도출.

정보보호 관리체계의 수립

K-Shield Jr.

위험평가의 모든 변수를 식별하고 평가했다면 위험도를 산정할 수 있으며 이 과정을 '위험 산출' 또는 '위험도 산정'이라고 하며, 계산식을 적용합니다.

o 위험관리 - 계속

→ 위험도 산정 계산식

위험도 = 정보자산 가치 (+/x) 취약점의 정도 (+/x) 위협의 빈도

= 정보자산 가치 (+/x) 우려도(x2/^2)

→ 계산식에서 더하기(+)를 쓰는 이유

- 3가지 변수가 모두 위험도를 높이는 요인이 되므로 잠재적 위험이 존재한다는 개념에서 출발
- 새로 발견된 취약점은 공격이 없었더라도 위험할 수 있음

→ 계산식에서 곱하기(x)를 쓰는 이유

- 3가지 변수 중 하나라도 전혀 없음(0)으로 측정된다면 위험도가 산정되지 않는가는 개념에서 출발
- 무수히 많은 위협이 존재하더라도 취약점이 전혀 없으면 위험이 없음

→ 어떻게 계산할 것인가는 논리와 선택의 문제

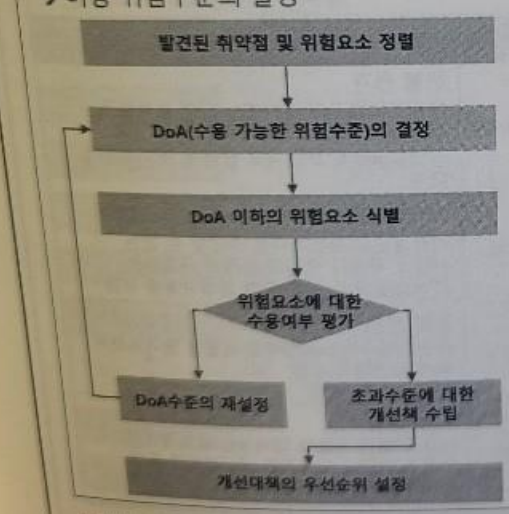
정보보호 관리체계의 수립

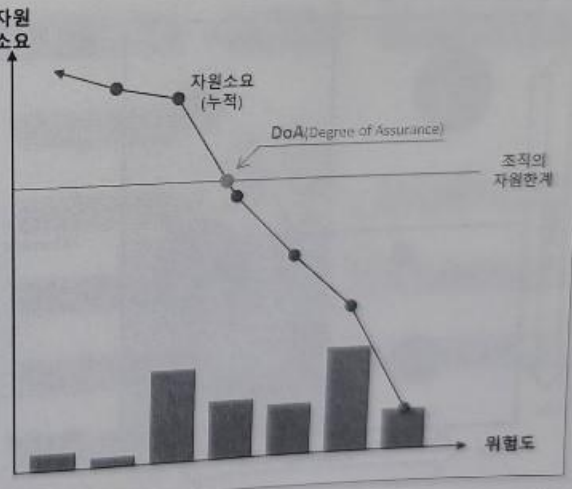
K-Shield Jr.

위험도를 산정한 후 수치화된 위험은 모두 조치되는 것이 바람직하겠으나, 조직의 예산이나 인력운영 등의 한계가 있으므로 할 수 있는 최대한을 정하여 조치할 기준이 필요합니다.

○ 위험관리 - 계속

→ 허용 위험수준의 결정





정보보호 관리체계의 수립

K-Shield Jr.

수용할 수 있는 기준(DoA)를 결정하고 DoA 이상의 위험에 대해서는 보호대책을 수립해야 합니다. 이 경우 조직의 문화, 임직원의 인식수준 등 다양한 사항을 고려해야 합니다.

○ 위험관리 - 계속

→ 정보보호대책 수립 시 고려사항

① 위험의 내용과 규모에 따라 제시된 통제사항의 내용 중에서 더 세부적이고 강력한 대책이 필요할 경우가 있음

② 구체적으로 제시되지 않은 대책을 강구해야 할 경우도 있음

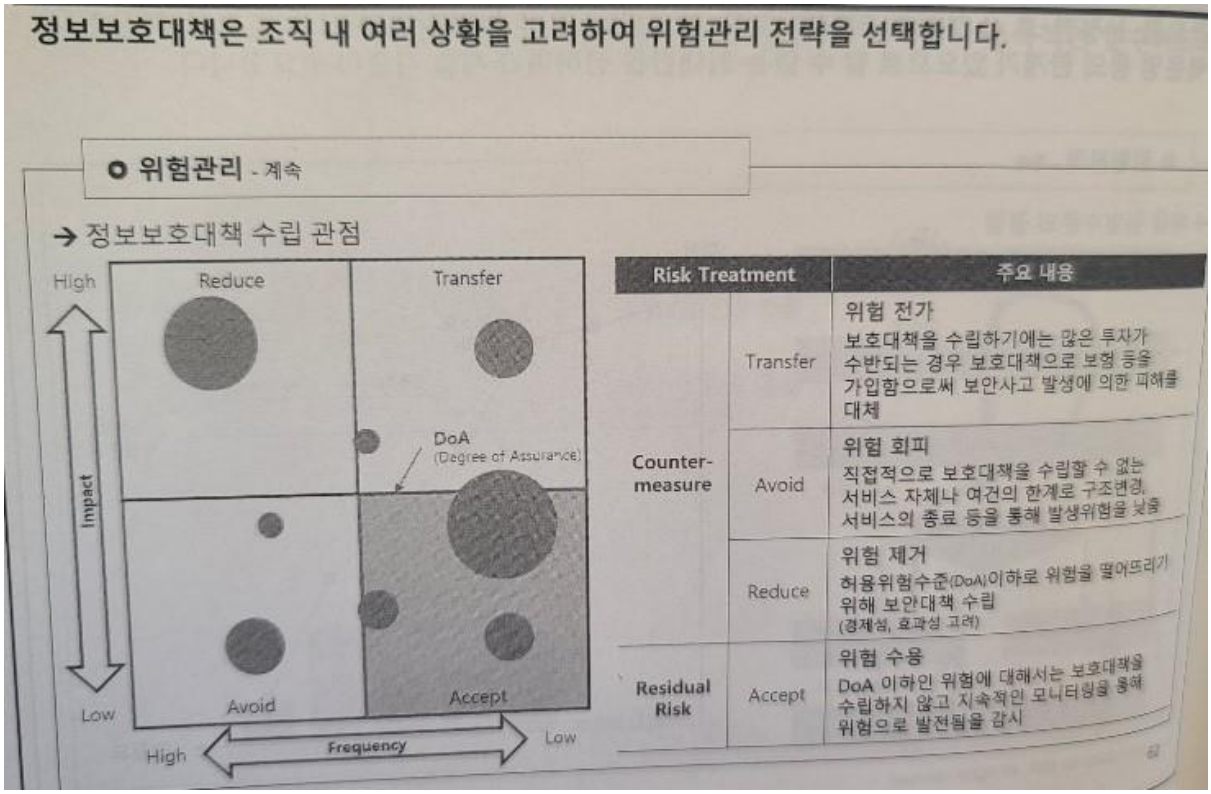
③ 정보보호관리체계 인증을 염두에 두고 있다면 관련된 통제사항을 선택하고 구체적인 대책을 명시해야 함

④ 선택된 통제사항은 다른 기존 통제사항과 함께 계획, 구현, 사후 관리의 관리과정 요구사항을 적용

⑤ 통제사항 선정 시에는 전략 선정 시 적용된 기술, 예산, 적용되는 법 제도, 시간, 조직문화 등 여러 가지 제약조건들을 고려

⑥ 선택된 각 통제사항은 비용・효과 분석을 통해 정당화되어야 함

⑦ 통제의 구현과 유지에 들어가는 비용이 해당 위험의 감소량보다 적어야 함



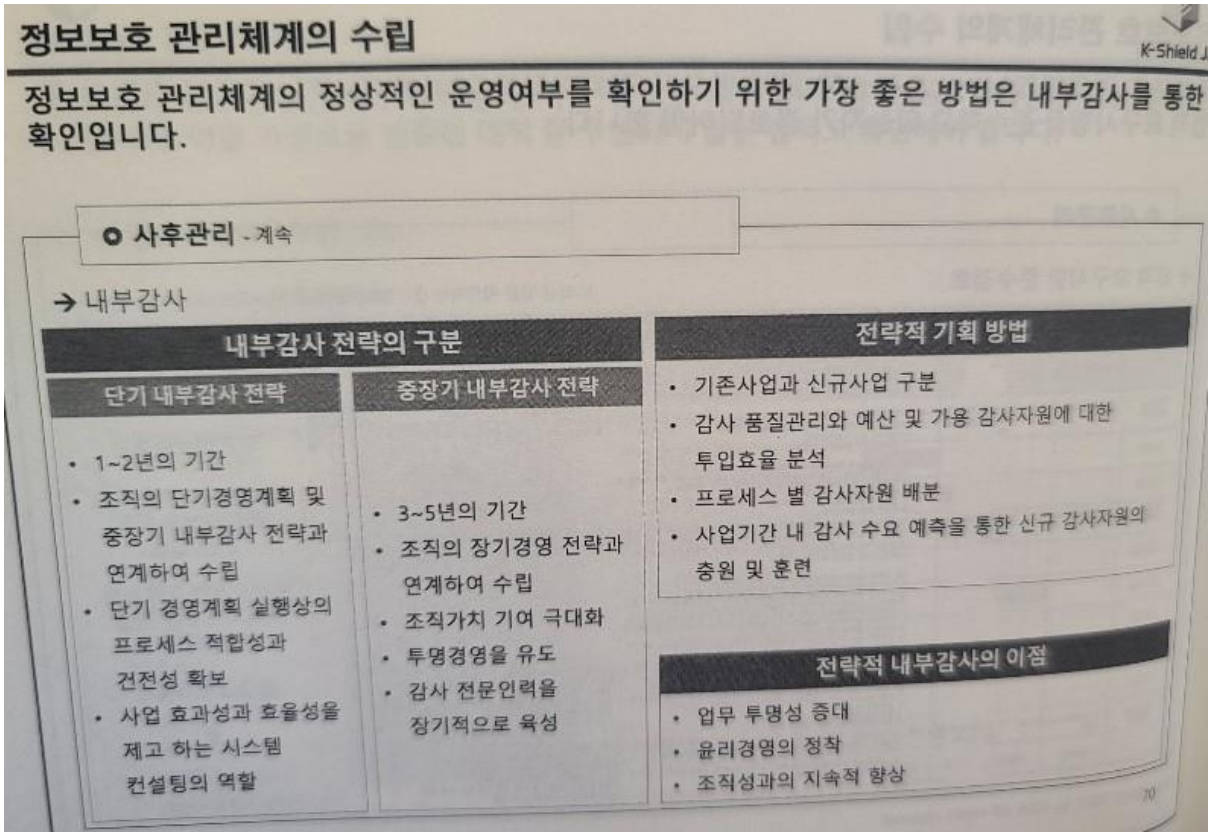
위험조치 과제 수립 / 이행

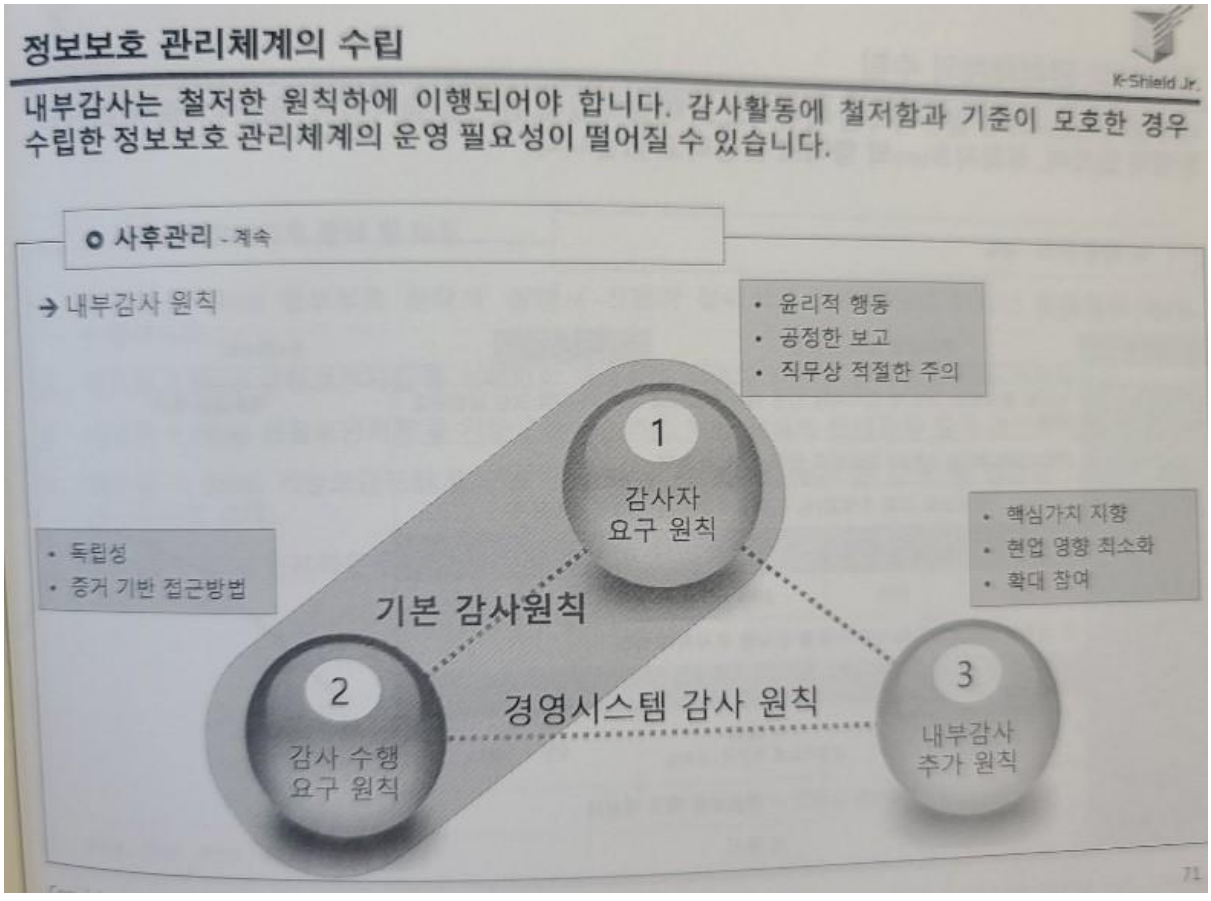
- 위험처리 방법이 결정된 이슈 및 문제점을 해결하기 위한 구체적인 계획을 수립 후 이행 가능하도록 영역을 구분하여 과제화 한다.

- 수립된 이행조치 과제는 조직 내 사업단위 활동으로 구성하여 구체적인 추진 조직과 목표, 이행 세부계획, 예산, 일정 등을 수립한다.

- 위험 평가 결과 -> 대책 선정 -> 프로젝트 선정 -> 우선순위 결정 -> 이행계획 정리

사후관리


정보보호 관리체계의 수립
K-Shield J
정보보호 관리체계의 정상적인 운영여부를 확인하기 위한 가장 좋은 방법은 내부감사를 통한 확인입니다.
사후관리 - 계속
→ 내부감사
내부감사 전략의 구분
단기 내부감사 전략
• 1~2년의 기간
• 조직의 단기경영계획 및 중장기 내부감사 전략과 연계하여 수립
• 단기 경영계획 실행상의 프로세스 적합성과 건전성 확보
• 사업 효과성과 효율성을 제고 하는 시스템 컨설팅의 역할
중장기 내부감사 전략
• 3~5년의 기간
• 조직의 장기경영 전략과 연계하여 수립
• 조직가치 기여 극대화
• 투명경영을 유도
• 감사 전문인력을 장기적으로 육성
전략적 기획 방법
• 기존사업과 신규사업 구분
• 감사 품질관리와 예산 및 가용 감사자원에 대한 투입효율 분석
• 프로세스 별 감사자원 배분
• 사업기간 내 감사 수요 예측을 통한 신규 감사자원의 충원 및 훈련
전략적 내부감사의 이점
• 업무 투명성 증대
• 윤리경영의 정착
• 조직성과의 지속적 향상
70


정보보호 관리체계의 수립
K-Shield Jr.
내부감사는 철저한 원칙하에 이행되어야 합니다. 감사활동에 철저함과 기준이 모호한 경우 수립한 정보보호 관리체계의 운영 필요성이 떨어질 수 있습니다.
사후관리 - 계속
→ 내부감사 원칙
• 윤리적 행동
• 공정한 보고
• 직무상 적절한 주의
• 독립성
• 증거 기반 접근방법
1
감사자 요구 원칙
기본 감사원칙
2
감사 수행 요구 원칙
경영시스템 감사 원칙
3
내부감사 추가 원칙
• 핵심가치 지향
• 현업 영향 최소화
• 확대 참여
71

정보보호 관리체계의 수립

K-Shield J

내부감사의 원활한 이행을 위해서는 내부감사 계획을 수립하여 이행해야 합니다. 단, 내부감사라고 하여 반드시 내부직원이 감사활동을 이행할 필요가 없습니다.

사후관리 - 계속

→ 내부감사 계획 수립절차

감사 대상의 결정

- 사업부 또는 부문 및 팀 별 업무 프로세스 별로 파악하여 결정
- 정기감사 : 조직의 직간접 분야를 막론하고 경영시스템의 범위 내에서 활동이 이루어지는 모든 사업영역이 감사 대상에 포함
- 비정기감사 : 필요성이 인정되는 상황이 발생되면 정기감사 계획과는 별개로 감사조직을 편성하여 운영

감사 우선순위 및 주기의 결정

- 감사 우선순위 및 주기 결정
  - ✓ 동일한 조건에서는 성과에 가장 큰 영향을 미치는 핵심조직과 관련 프로세스를 우선순위
  - ✓ 상대적으로 짧은 주기
- 감사 우선순위 및 주기 방법
  - ✓ 위험의 정량화하여 실질 위험수준을 고려
    → 실질위험 = 고유위험 – 통제수준
  - ✓ 직전 감사일정 및 전회의 감사결과 고려

일정계획 및 감사자원 배분

- 감사 시기 결정
  - ✓ 우선순위 및 주기를 고려하여 중점 감사대상 그룹과 A등급으로 파악된 6개월 주기의 감사부하를 균등분할
  - ✓ 연주기 및 격년주기 감사대상을 파악된 우선순위에 따라 순차적으로 배분
- 감사 기간 결정
  - ✓ 해당 프로세스의 등급에 따라 결정되도록 하고 과거 감사 이력에 따라 일정범위 내에서 가감이 가능하도록 결정
- 감사자원 배분
  - ✓ 내부감사 전담인력을 운영하는 조직의 경우
  - ✓ 감사독립성 검토
  - ✓ 선호 감사자 요구 시 이유 파악

물리 보안 운영

물리적 보안요구사항

- 눈으로 보이는 사전에 허가된 사람, 차량, 장비만 사업장에 드나들 수 있도록 통제하는 것이다.

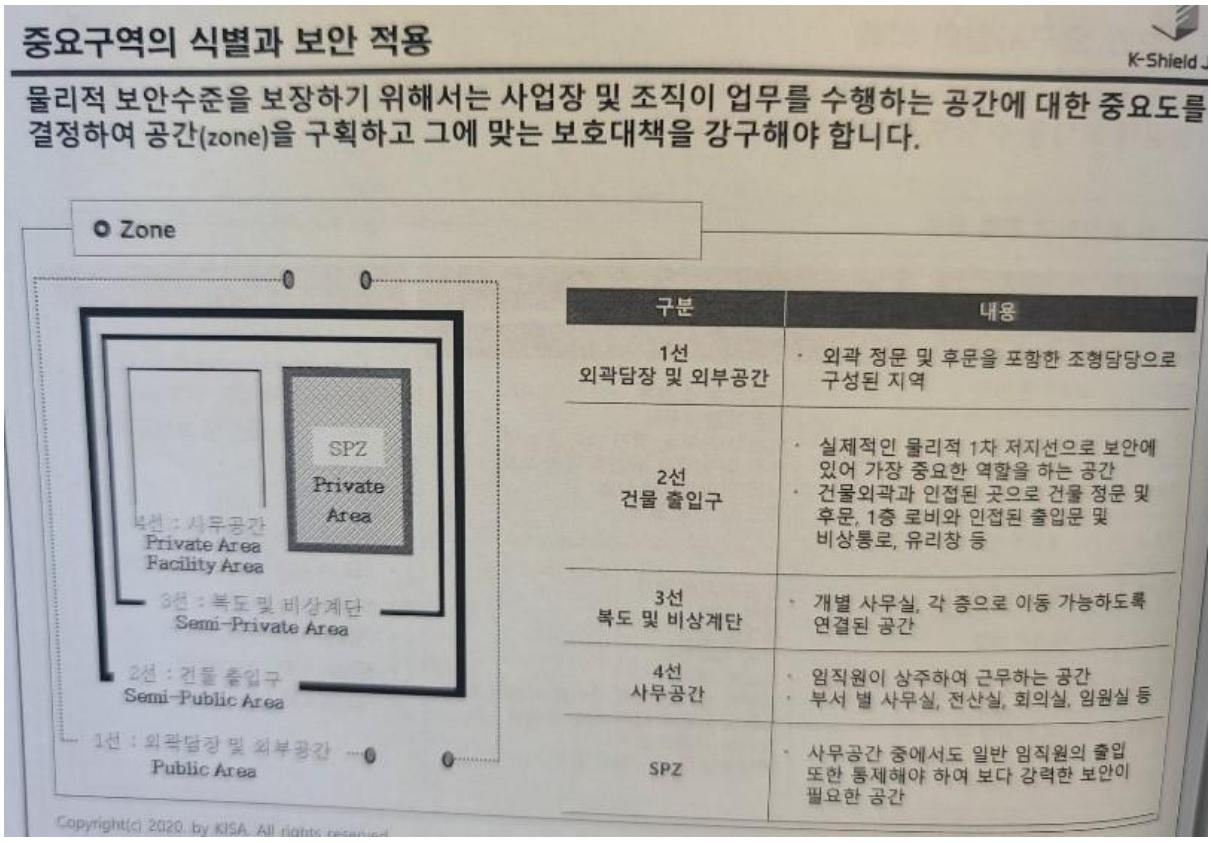
물리적 보안체계의 구성

- Zone(+ Special Protection Zone)

-> Entrance

-> Access Control (+ Vehicle)

-> Perimeter Detection (주변 감시)(cctv 등)



중요구역의 식별과 보안 적용

다양한 물리적 보안장비를 모두 설치할 필요는 없습니다. 필요한 곳에 필요한 요건에 맞추어 통제 체계를 갖추는 것이 필요합니다.

ISMS에서의 물리적 보안 요구사항

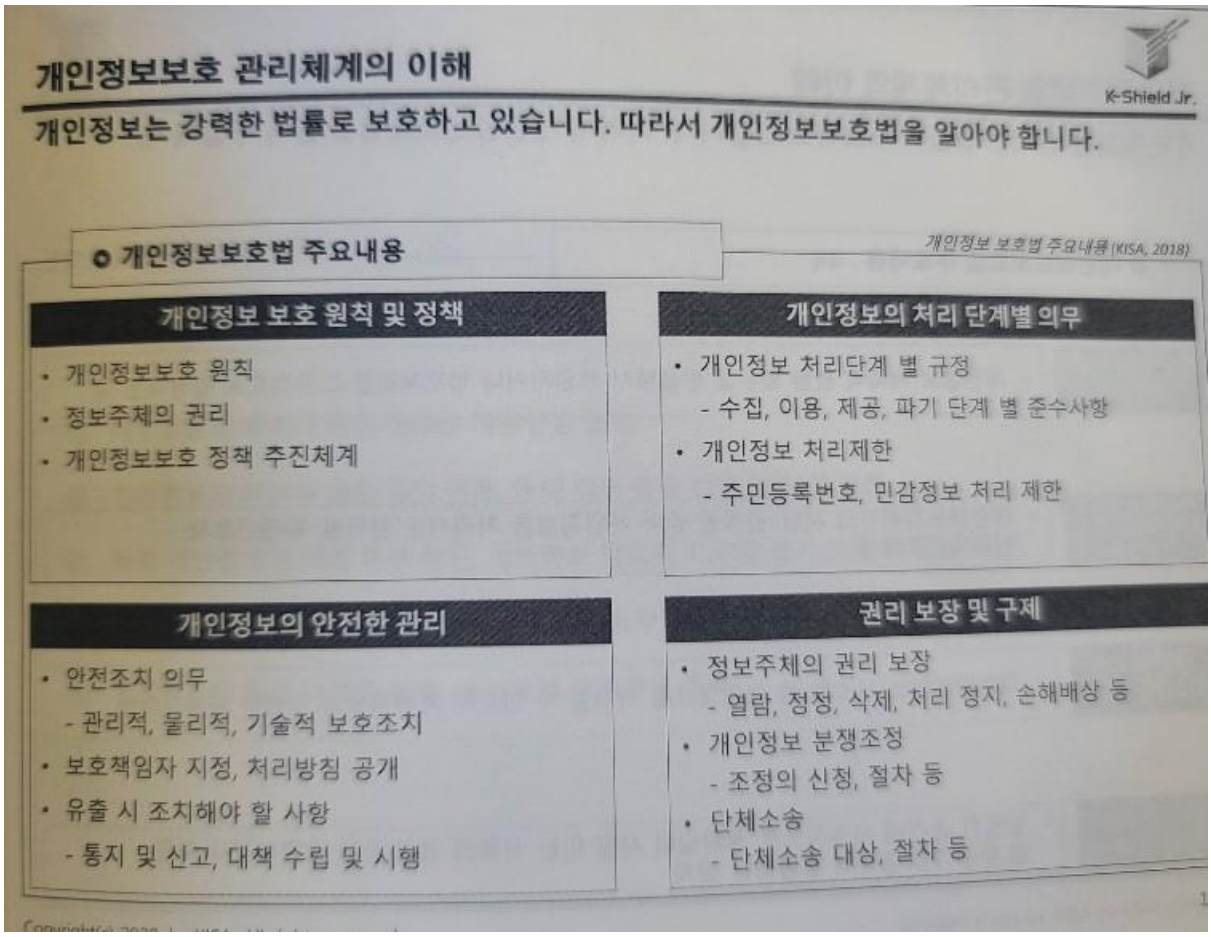
No.	통제항목	주요 내용
7.1.1	보호구역 지정	· 주요 설비 및 시스템을 보호하기 위하여 물리적 보호구역을 정의하고 구역별 보호대책을 수립·이행해야 함
7.1.2	보호설비	· 각 보호구역의 중요도 및 특성에 따라 화재, 수해, 누수, 온도 및 습도, 전력공급 등의 정보시스템 가용성 보장을 위한 설비를 구축 및 운영해야 함 · 외부 집적정보통신시설(IDC)에 위탁 운영하는 경우, 물리적 보호에 필요한 요구사항을 계약서에 반영하고 운영상태를 주기적으로 검토해야 함
7.1.3	보호구역 내 작업	· 시스템 도입, 유지보수 등으로 보호구역 내 작업이 필요한 경우 사전 승인 및 작업기록을 유지하고 주기적으로 검토해야 함
7.1.4	출입통제	· 보호구역 별 출입통제 절차가 있어야 하며, 출입 가능한 임직원 현황을 관리해야 함 · 모든 출입기록과 출입권한은 주기적으로 검토되어야 함 · 장비, 문서, 매체 등의 반출입 내역도 관리되어야 함
7.1.5	모바일기기 반출입	· 모바일기기의 사용 빈도의 증가에 따른 반출입 통제 및 반출입 이력을 점검해야 함
7.2.1	케이블 보안	· 전력 및 통신케이블이 외부로부터의 물리적 손상, 전기적 영향으로 부터 보호되어야 함
7.2.2	시스템 배치 및 관리	· 정보시스템은 그 측정을 고려하여 배치장소를 분리해야 하며, 손쉽게 그 물리적 위치를 확인할 수 있어야 함
7.3.1	개인업무 환경 보안	· 자리 이석 시 중요문서/저장매체 등 방치 금지, 컴퓨터 화면보호기 / 패스워드 설정
7.3.2	사무실 보안	· 공용 OA기기, 공용공간 등에 대한 보호대책 수립 및 주기적 검토

개인정보보호 운영

- 가명정보 vs 익명정보

가명정보란 가명처리를 함으로써 원래 상태로 복원하기 위해서 추가정보를 사용하거나 결합하는 그런게 없으면 개인을 알아볼 수 없는 정보

익명정보란 누군지 알아볼수 없도록 마스킹처리한 정보



개인정보보호 관리체계의 이해

K-Shield

개인정보는 강력한 법률로 보호하고 있습니다. 따라서 개인정보보호법을 알아야 합니다.

○ 개인정보보호법 주요내용 - 계속

개인정보 보호법 주요내용 (KISA, 2018)

→ 용어 정리

개인정보	• 성명, 주민등록번호 등을 통하여 살아있는 개인을 알아볼 수 있는 정보 • 다른 정보와 쉽게 결합하여 개인을 알아볼 수 있는 정보
정보주체	• 처리되는 정보에 의해 알아볼 수 있는 그 정도의 주체가 되는 사람(자연인)
개인정보 파일	• 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물
처리	• 개인정보의 수집, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위
개인정보 처리자	• 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체, 개인 등

○ 개인정보보호법 주요내용 - 계속

개인정보 보호법 주요내용 (KISA, 2018)

→ 용어 정리 - 계속

개인정보보호 책임자	• 개인정보 처리에 관한 업무를 총괄해서 책임지거나 업무처리를 최종적으로 결정하는 자
개인정보 취급자	• 개인정보처리자의 지휘. 감독을 받아 개인정보를 처리하는 임직원, 파견근로자, 시간제근로자 등
개인정보 처리시스템	• 데이터베이스 시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성한 응용시스템
영상정보 처리기기	• 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유.무선망을 통하여 전송하는 장치

○ 개인정보보호법 주요내용 - 계속

→ 개인정보 보호 원칙 (제3조)

① **처리 목적의 명확화**, 목적 내에서 **적법하고 정당하게 최소 수집**

② 처리 목적 내에서 처리, **목적 외 활용 금지**

③ 처리 목적 내에서 **정확성. 완전성. 최신성** 보장

④ 정보주체의 권리침해 위험성 등을 고려하여 **안전하게 관리**

⑤ 개인정보 처리사항 공개, **정보주체의 권리보장**

⑥ **사생활 침해 최소화** 방법으로 처리

⑦ 가능한 경우 **익명 처리**

⑧ 개인정보처리자의 **책임 준수**, 정보주체의 **신뢰성 확보**

○ 개인정보보호법 주요내용 - 계속

→ 정보주체의 권리 (제4조)

① 개인정보의 처리에 관한 정보를 **제공받을 권리**

② 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 **선택, 결정할 권리**

③ 처리 개인정보의 처리 여부 확인, 개인정보 **열람을 요구할 권리** (사본의 발급 포함)

④ 개인정보의 **처리 정지, 정정.삭제 및 파기를 요구할 권리**

⑤ 개인정보의 처리 **피해를 신속, 공정하게 구제받을 권리**

Quiz : 개인정보보호법, 정보통신망법, 신용정보 보호법 중 어느 법이 우선 적용되나요?

K-Shield Jr

○ 개인정보보호법 주요내용 - 계속

개인정보 보호법 주요내용 (KISA, 2018)

→ 개인정보 수집에 대한 동의를 받을 때 [정보통신망법]과 [신용정보보호법]은 각각 별도의 규정이 존재하므로 이에 대하여는 [개인정보 보호법]보다 우선하여 적용

→ 그러나 [정보통신망법]과 [신용정보보호법] 등에는 영상정보처리기기 설치운영 제한, 분쟁 조정, 단체소송 등의 규정이 없으므로 이에 대하여는 [개인정보 보호법]이 우선하여 적용

※ 특별법 우선 원칙 : 일반법과 특별법에 중복되는 규정이 존재할 경우 특별법을 적용하는 원칙

→ 개인정보 보호법은 개인정보 보호 분야의 일반법

- 사회전반의 개인정보 보호를 규율
- 모든 공공기관, 사업자, 법인, 단체, 개인 등

→ 타 법률에 특별한 규정이 있는 경우 해당 법률의 규정을 우선 적용

108

개인정보보호 관리체계의 이해

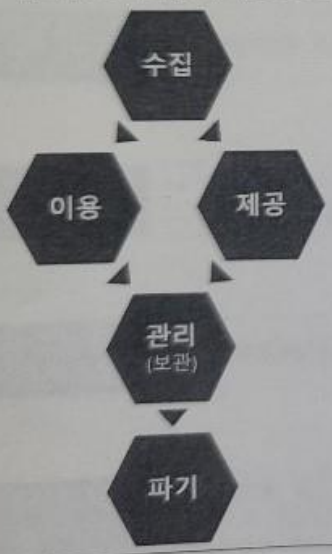
K-Shield Jr.

개인정보는 강력한 법률로 보호하고 있습니다. 따라서 개인정보보호법을 알아야 합니다.

○ 개인정보보호법 주요내용 - 계속

개인정보 보호법 주요내용 (KISA, 2018)

→ 개인정보 처리단계 별 보호조치



수집.이용 (15조) 만 14세 미만 법정 대리인 동의 (22조) 최소 수집 (16조)	- 처리제한 - 민감정보 (23조), 고유식별정보 (24조), 주민등록번호 (24조의2)
목적 외 이용.제공 제한 (18조) 제3자 제공 (17조) 처리위탁 (26조)	영업양도양수 (27조, 민간) 국외이전 (17조)
안전조치 의무 (29조) 처리방침 (30조), 보호책임자 (31조)	개인정보 유출 통지.신고 (34조) 개인정보파일 등록 (32조, 공공)
파기 (21조)	

○ 개인정보보호법 주요내용 - 계속

→ 개인정보 처리제한 (제23조, 제24조)

"민감정보 및 고유식별정보는 원칙적으로 처리 금지 "

정보주체에게 별도 동의를 얻거나,

법령에서 구체적으로 처리를 요구하거나 허용하는 경우에 한하여 처리

민감정보

사상, 신념, 노동조합 및 정당가입,
건강정보, 유전정보,
범죄경력 정보 등

고유식별정보

주민등록번호,
여권번호,
운전면허번호,
외국인등록번호

분실, 도난, 유출, 위조, 변조, 훼손되지 않도록 안전성 확보조치 의무 이행 필요

위 규정에도 불구하고 주민등록번호는 법률 또는 시행령에 구체적으로 처리근거가 있어야 처리가 가능함 (제24조의2)