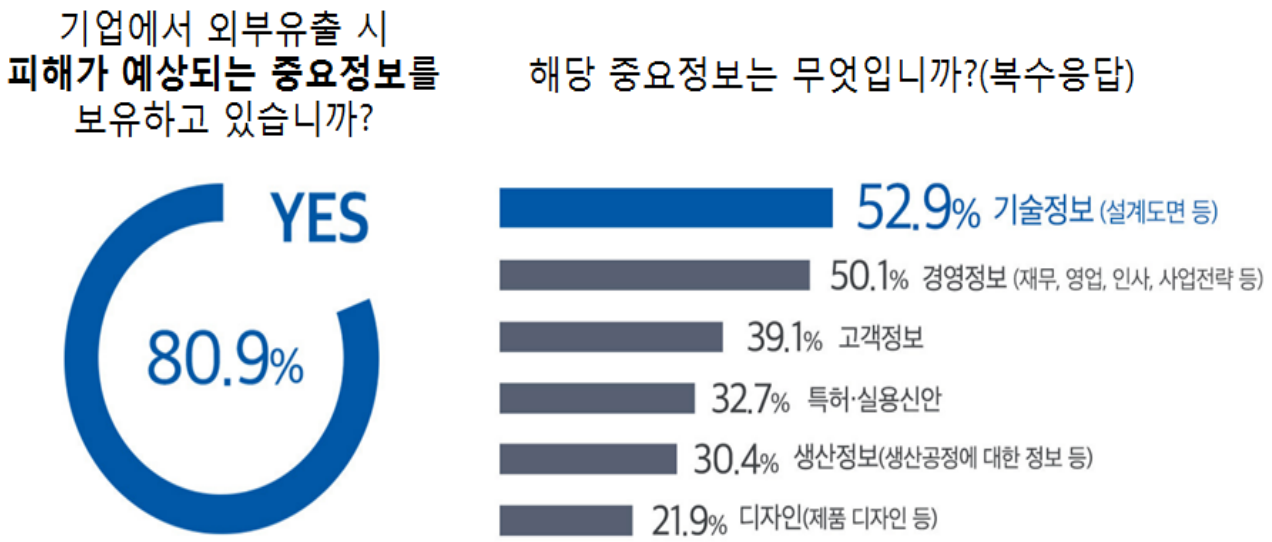
비대면 서비스 보안 지원을 위한 정보 등급화 방안

2020년 7월 16일

중앙대학교
산업보안학과 장 항 배 교수

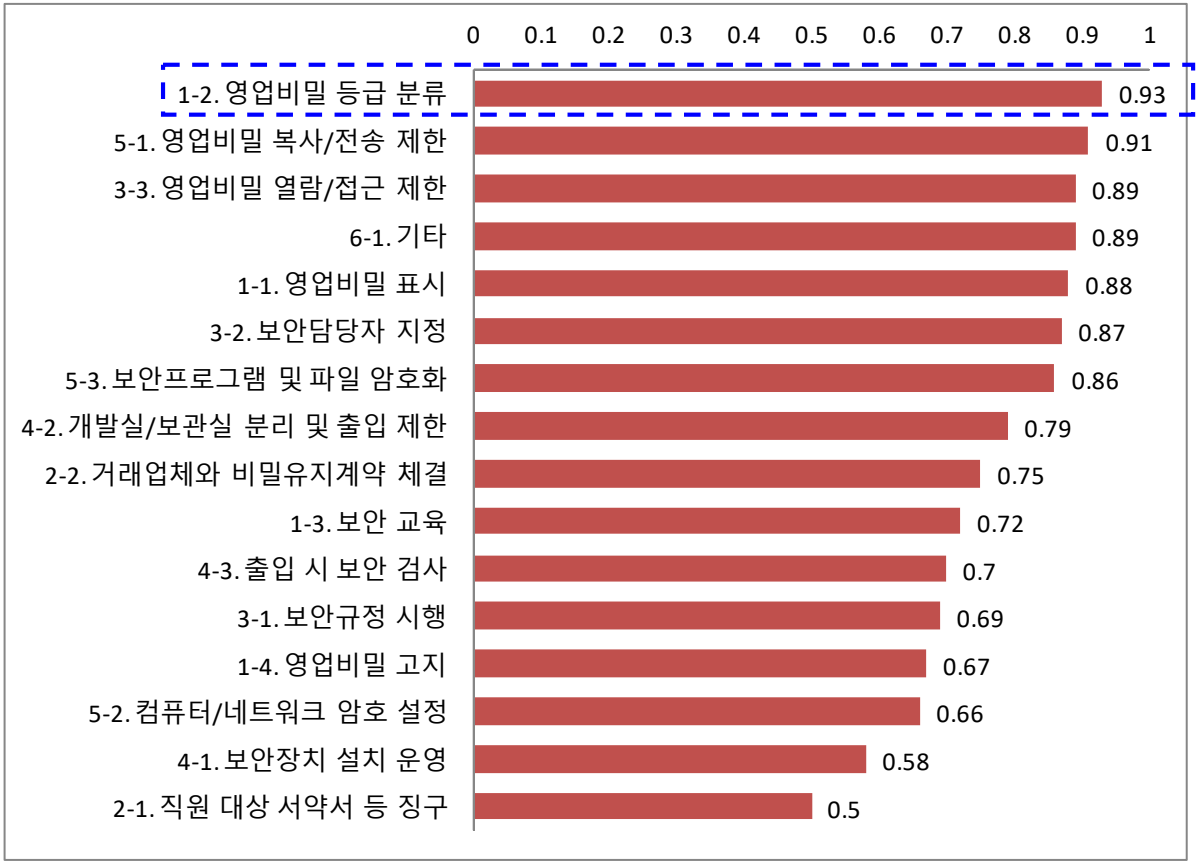
정보의 분류체계 필요성

- 조직(특히 기업) 내에서 생성되는 다양한 형태의 문서와 산출물들을 정보 자산이라 하고, 그 중 **조직의 가치(value)를 포함하고 있는 문서와 산출물들을 중요 정보**라고 정의
- 기업이 보유한 중요정보(기술상 또는 경영상)는 **그 기업의 경쟁력을 가늠할 수 있는 중요한 척도**
- 기업(규모와 업종 고려)은 **차별적 관리의 대상**이 되는 **정보를 등급화** 할 수 있는 **분류 체계를 마련하는 것이 선행적으로 요구**됨



정보의 분류체계 필요성(영업비밀)

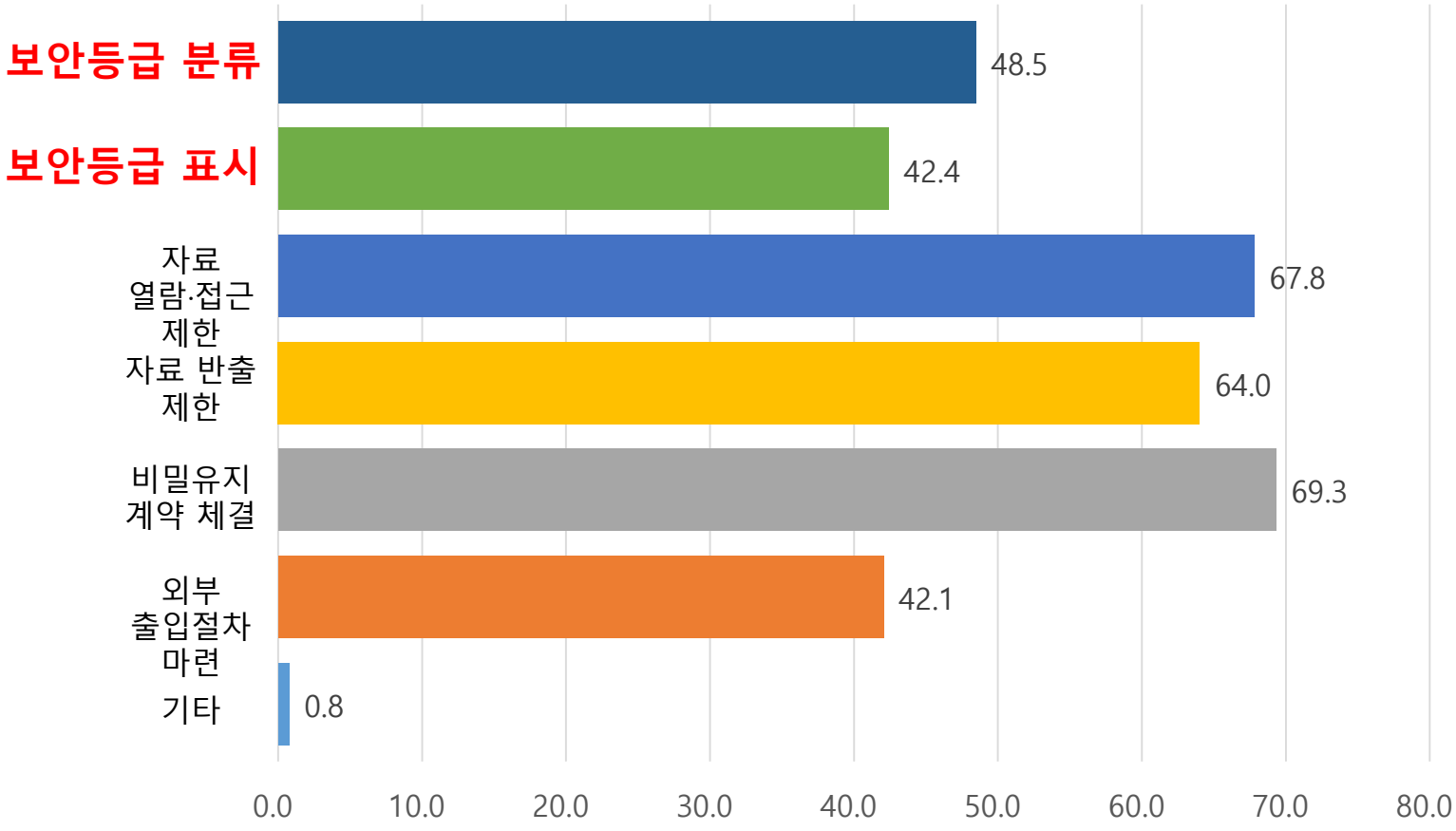
"비밀관리 노력여부는 **단일한 기준에 의하여 판단할 수 있는 것이 아니고**,
해당 정보의 양과 중요성, 이를 보유한 기업의 규모, 이를 비밀로 관리하는데 소요되는 비용을 **종합적으로 고려**하여 구체적인 사안별로 판단해야 한다(2012노1580)."



"비밀 관리 활동" 판단 결과 상관 분석

<출처> 한국특허정보원, 판례분석을 통한 영업비밀 보호 가이드 연구(2013)

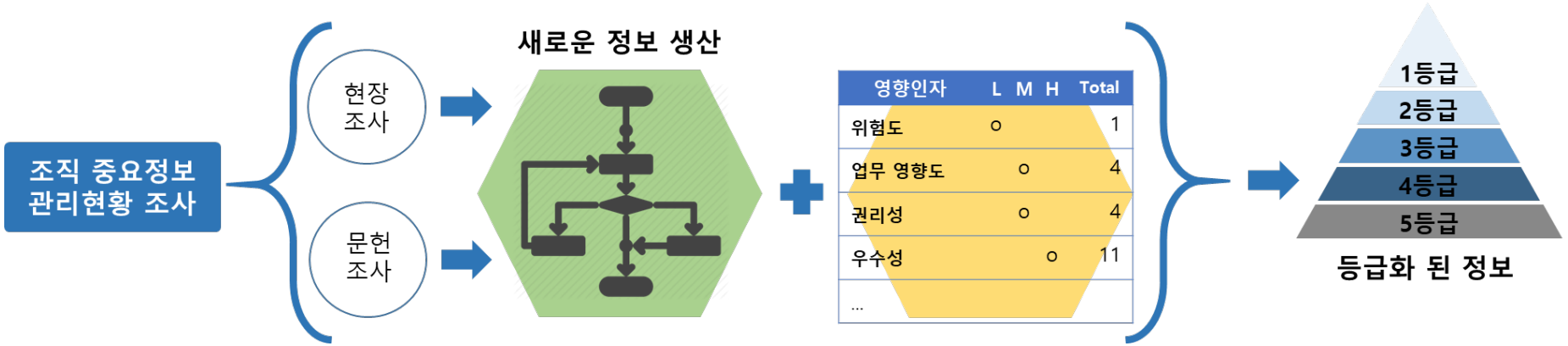
정보의 분류체계 필요성(영업비밀)



<출처> 한국산업기술보호협회, 기업 기술보호 역량조사(2015)

정보의 분류기준 설계

- 국내외 문헌을 참고하여 **정보 내용**과 **유형을 분류**(경영정보, 기술정보 등)
- **다양한 분야의 선행연구를(시스템, 정보, 기술 등)** 통해 등급분류(중요도) 영향인지를 도출
- **영향 인자의 수준**을 결정하여 등급 분류에 적용할 수 있는 정량적 형태로 기준 수립
- 조직의 새로운 정보가 생산되었을 때 **유형 분류 → 등급 분류(중요도) → 보안 서비스 대응** 순서로 진행할 수 있는 정보 등급분류 체계 마련



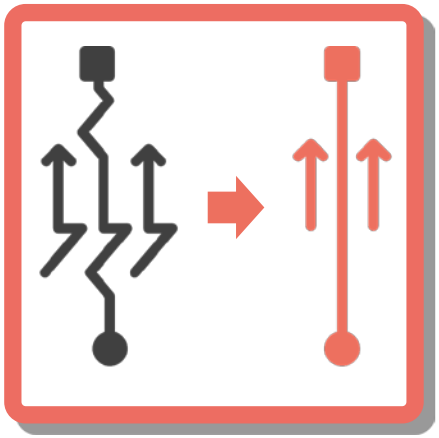
정보의 분류기준 설계

- **정보(information)**는 **무형**이고 **내용(contents) 그 자체**이며, 어떤 형태로 존재하는지에 따라 가치가 달라지지 않음. **자료(material)는 정보를 유형화**한 것으로서, 전자파일, 종이문서, 영상매체 등 **다양한 형태로 존재**
- 평가되는 정보의 가치는 보편적(일반적) 가치가 아닌, 조직 내 한정된(특화된) 정보가치이기 때문에 **상대적 가치 요소가 발생**됨
- **정보 자체(내용)를** 적절히 분류하여 관리할 수 있는 속성 체계 개발 필요**(Practically 정교한 수준)**

상대적 민감도 수준 결정

Low Sensitivity	**Medium** Sensitivity	**High** Sensitivity
Public website content, press releases	Emails and documents with no confidential data	Financial records, intellectual property, authentication data

정보의 분류기준 설계

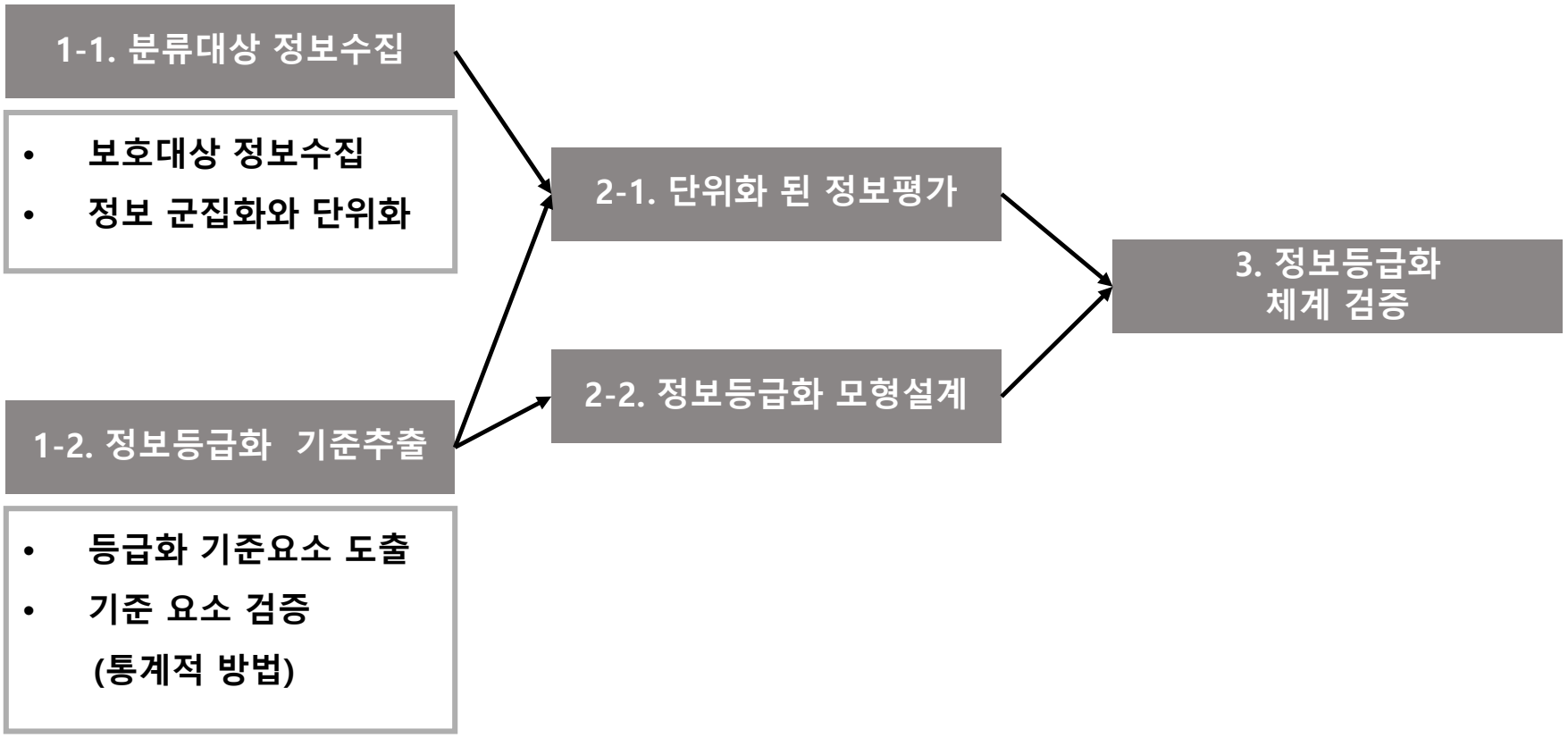


이해 복잡성 감소

업무처리 단축

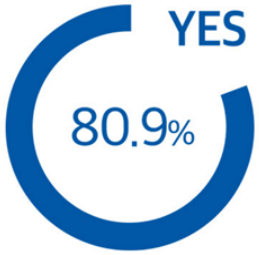
경제적 보안 투자

정보 등급화(중요도) 연구 방법론

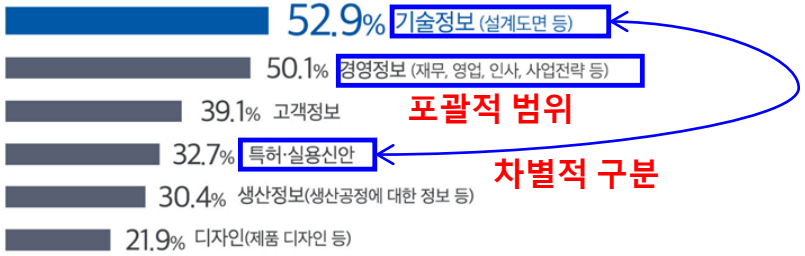


정보 단위화 필요성

기업에서 외부유출 시
피해가 예상되는 중요정보를
보유하고 있습니까?



해당 중요정보는 무엇입니까?(복수응답)



수평적 분류와 수직적 수준이 부적절함

경영 정보

- 단기, 중기, 장기 경영계획 및 전략
- 사업 계획
- 사업 투자 계획

→ 포함관계

- 경영(비즈니스 표준 운영) 계획
- 경영실적 및 분석자료
- 이사회 및 임원 회의 자료
- 자회사 및 하청업체의 사업정보
- 경영 진단 및 감사 보고서

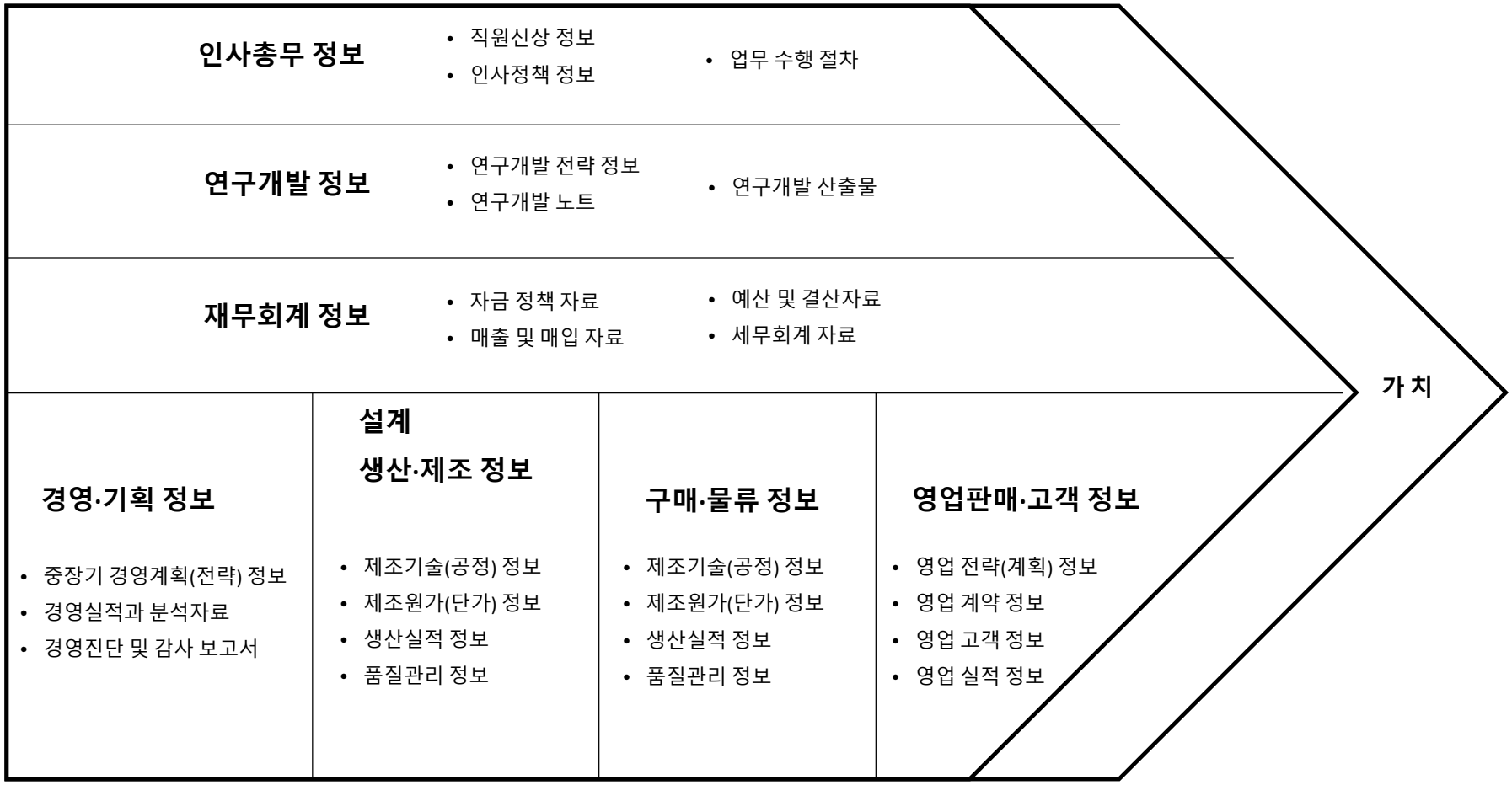
회계 정보

- 자금정책 자료
- 재무제표
- 결산서

→ 유사관계

- 세무 관련 자료
- 결산 관련 정책 및 보고서
- 매출 관련 자료
- 자산 관리 자료

정보 단위화 과정


인사총무 정보
직원신상 정보
인사정책 정보
업무 수행 절차
연구개발 정보
연구개발 전략 정보
연구개발 노트
연구개발 산출물
재무회계 정보
자금 정책 자료
매출 및 매입 자료
예산 및 결산자료
세무회계 자료
가 치
경영·기획 정보
중장기 경영계획(전략) 정보
경영실적과 분석자료
경영진단 및 감사 보고서
설계
생산·제조 정보
제조기술(공정) 정보
제조원가(단가) 정보
생산실적 정보
품질관리 정보
구매·물류 정보
제조기술(공정) 정보
제조원가(단가) 정보
생산실적 정보
품질관리 정보
영업판매·고객 정보
영업 전략(계획) 정보
영업 계약 정보
영업 고객 정보
영업 실적 정보

정보 단위화 과정

대 분류	중 분류	소 분류 1	소분류2	유사어
생산제조	생산계획 정보	생산 추진전략		신제품 생산계획 시험생산 계획
		생산설비 정보	설비 보유현황	장치 보유현황 장비 리스트
			설비 배치도	장치배치도 기계장치 배치도
	생산공정 정보	생산공정 설계도		작업 방법 작업 표준서 작업표준 일람표 공정에 대한 통합 프로세스 흐름 파일
		생산도면		제품 도면 제조 방법 제품가공 방법 제품조립 방법 제품배합 방법(배합순서/배합비율) 기술시방서 기술시방도면 소스코드 회로도 기판 설계도

정보 등급화 선행연구

다양한 등급분류 대상에 따른 **영향 인자를 도출하여 정리한 내용**

선행 연구	분류 대상	영향 인자
1. 공개 위험 측도를 활용한 군 개인정보 등급 분류 개선	군 개인정보	개인정보의 식별 여부, 개인정보 노출 위험도, 개인정보 이용 빈도
2. 정보보안 모범사례 가이드	정보자산 가치	정보의 무결성, 정보의 기밀성, 정보의 가용성
3. 범정부 정보보호 등급제	정보시스템	정보시스템이 업무에 미치는 영향 범위, 정보시스템의 정보 처리도(량), 정보시스템의 타 시스템 연계 영향도, 업무 연속성 보장 정도, 정보시스템의 보유 정보량
4. 정보자원 유지보수 등급 측정 매뉴얼	정보자원	정보 자원이 지원하는 정보시스템의 업무 중요도(업무영향범위, 데이터 중요도, 이용자 수/처리 건수) 정보자원의 고유한 특성, 정보자원의 유지보수 특성(유지보수 복잡도, 유지보수 업무 형태)
5. 특허기술의 기술 사업성 가치 평가를 위한 범주형 평가지표 모델 개발	특허기술	기술의 관리성(특허기술의 권리화 상황 등), 기술의 혁신성(기술수준, 기술개발 난이도) 사업성(시장 규모, 시장경쟁 구도, 상용화 가능 시기)
6. 미국 국립기술이전센터 TOP Index	기술	기술의 상태, 기술의 신규성, 기술의 범위와 심도, R&D 지원사항, 기술 보호, 경쟁 기술, 상업화 시기, 상업화에 필요한 자금, 예상 매출액, 환경적인 문제들
7. Dow Chemical	기술	기술의 가치를 평가하기 위한 유용성과 경쟁성 평가항목
8. 일본 기술평가정보센터	기술	기술의 신규성(기술경쟁력, 기술 우위성), 실현가능성(기술 신뢰성), 시장성(기술 수명, 수용 안정성)
9. 일본 특허청	지적재산권	권리고유평가(권리의 존속기간, 대체기술과의 기술 우위성), 이전유통성평가(기술이전의 신뢰성, 권리의 안정성), 사업성 평가(사업화가능성, 사업규모, 수익성)
10. 일본 IS Rating	기업 내 정보	기업 내 정보 자산의 침해행위에 대한 영향도(국내외, 사회 인프라, 조직, 개인)

정보 등급화 선행연구

범 정부 정보보호 등급제(2016)

중요도가 낮은 **정보시스템**에 대해서도 동일한 보안관리 기준을 적용하여 관리비용이 과다 발생하는 것을 방지하고자 **시스템 특성**(**서비스 영향범위, 정보 처리수준, 연계시스템 정도, 업무연속성 보장 수준, 보유 정보량**)과 **기관의 특성(기관신뢰도)**을 고려하여 정보보호 등급을 산정함

구분	등급	배점	평가요소		설명	
1 서비스 영향범위	1(VH)	20	붙임 참고*		시스템별 업무 영향범위 평가기준	
	2(H)	16				
	3(M)	12				
	4(L)	8				
	5(VL)	4				
2 정보처리도	1(VH)	20	50% 이상	50만 이상	기관 내 이용자수 (일 최댓값)	대국민서비스 이용자수 (일 최댓값)
	2(H)	16	25%~%미만	10만 이상~50만 미만		
	3(M)	12	5~%미만	1만 이상~10만 미만		
	4(L)	8	5% 미만	1만 미만		
	5(VL)	4	오프라인 업무수행 대체가능	-		
3 연계시스템 영향도	1(VH)	20	5개 시스템 이상		시스템 연계성	
	2(H)	16	4개 시스템			
	3(M)	12	3개 시스템			
	4(L)	8	2개 시스템			
	5(VL)	4	1개 시스템 이하			
4 업무 연속성 보장	1(VH)	20	4시간		최대 업무 복구 기대시간 (업무의 지속성 보장정책)	
	2(H)	16	12시간			
	3(M)	12	24시간			
	4(L)	8	1주일			
	5(VL)	4	1개월			
5 보유 정보량	1(VH)	20	100만 이상		개인정보 등 민감정보 보유건수	
	2(H)	16	50만~100만 미만			
	3(M)	12	1만~50만 미만			
	4(L)	8	1만 미만			
	5(VL)	4	1천 이하			
6 기관 신뢰도 평가수준						

정보활용 정도(use)

+ 정보활용 영향수준(outcome) 평가

정보 등급화 선행연구

정보자원 유지보수 등급 측정 매뉴얼(2013)

- 정보자원 유지보수 등급 측정 매뉴얼에서는 정보자원의 등급을 결정하기 위한 측정 관점을 **업무 중요도, 자원 특성, 유지보수특성**으로 구성함

구분	측정관점	배점	측정항목	배점	측정기준
HW	업무 중요도	40	업무영향범위	60	▪ 업무분야별 서비스 제공에 따른 영향범위
			데이터 중요도	10	▪ 업무에서 생산된 데이터의 보존기간
			이용자수/처리건수	30	▪ 서비스 이용자수(대국민/내부) 및 처리건수
	자원 특성	35	HW 유형	100	▪ HW 유형을 구분하고 동일 유형내 용량 · 용도 기준
	유지보수 특성	25	유지보수 난이도	70	▪ 이중/단일, 개별/공용 등 정보자원 구성기준에 따른 유지보수업무 난이도
			유지보수 항목	30	▪ 유지보수 서비스의 범위
상용 SW	업무 중요도	60	업무영향범위	60	▪ 업무분야별 서비스 제공에 따른 영향범위
			데이터 중요도	10	▪ 업무에서 생산된 데이터의 보존기간
			이용자수/처리건수	30	▪ 서비스 이용자수(대국민/내부) 및 처리건수
	유지보수 특성	40	유지보수 난이도	70	▪ 이중/단일, 개별/공용 등 정보자원 구성기준에 따른 유지보수업무 난이도
			유지보수 항목	30	▪ 유지보수 서비스의 범위
정보 시스템	업무 중요도	50	업무영향범위	60	▪ 업무분야별 서비스 제공에 따른 영향범위
			데이터 중요도	10	▪ 업무에서 생산된 데이터의 보존기간
			이용자수/처리건수	30	▪ 서비스 이용자수(대국민/내부) 및 처리건수
	자원 특성	15	타 시스템 연계수	70	▪ 해당 정보시스템과 연계된 타 시스템 개수
			백업장비 구성체계	30	▪ 해당 정보시스템을 지원하는 백업장비의 구성체계
	유지보수 특성	35	유지보수 난이도	70	▪ 개발 프레임워크 사용 여부 및 정보시스템 구조화 정도
			유지보수 규모	30	▪ 정보시스템 전체 기능수 대비 유지보수 대상 기능수 (비율)

정보 등급화 선행연구

특허기술의 기술 사업성 가치평가를 위한 범주형 평가지표모델 개발

- 33개 국내외 기술 가치 평가모형 중 평가 요인 및 항목의 구조화를 위해 평가 요인을 **기술성부문**과 **사업성부문**으로 분류

부문	중항목	평가 항목
기술성	기술의 권리성	특허기술의 권리화 상황 특허기술의 권리범위 특허기술 권리의 존속기간 대체특허가능성
	기술의 혁신성	기술수준 기술개발 난이도 기술의 우수성 기술의 신규성 기술의 완성도 기술의 활용범위
	기술의 환경성	기술 인프라 기술 지원 및 규제 기술의 구현가능성 기술 제약성 기술적 파급효과 대체기술 출현가능성
사업성	산업 및 시장 특성	시장 규모 시장 성장성 시장 수명
	경쟁 특성	시장 진입장벽 시장 경쟁 구조 시장 경쟁 정도
	상업화 특성	상용화 가능시기 추가 기술개발 및 기술향유도 생산 설비 및 공정 투자비용 및 매출 규모 수익 규모 성장성 및 안정성

정보 등급화 선행연구

정보 손실(기본전제)에 따른 업무영향 정도를 평가

자산번호	자산명	목적/기능	소유부서	자산 위치	관리자	담당자	자산 민감도 평가			
							기밀성	무결성	가용성	평가 합계
P-S-001	Server_U_001	A 서비스 WAS 서버 01	온라인팀	서울 IDC	OOO팀장	OOO과장	3	3	1	7
P-S-002	Server_U_002	A 서비스 WAS 서버 02	온라인팀	서울 IDC	OOO팀장	OOO과장	3	3	1	7
P-S-003	Server_W_001	A 서비스 WEB 서버 01	온라인팀	서울 IDC	OOO팀장	OOO과장	2	2	1	5
P-S-004	Server_W_002	A 서비스 WEB 서버 02	온라인팀	서울 IDC	OOO팀장	OOO과장	2	2	1	5
P-S-005	Server_W_003	A 서비스 WEB 서버 03	온라인팀	서울 IDC	OOO팀장	OOO과장	2	2	1	5

산술 평균

산술 합산

산술 곱셈

추상적 개념으로 평가되는 관계로 평가者 변화에 따른 평가결과에 대한

일관성 부족(← 형식적 평가로 한정될 가능성)

정보에 대한 절대적 가치로만 평가됨(←상대적 가치)

영업비밀 정보의 중요도를 최종적으로 산출하는 것인데,

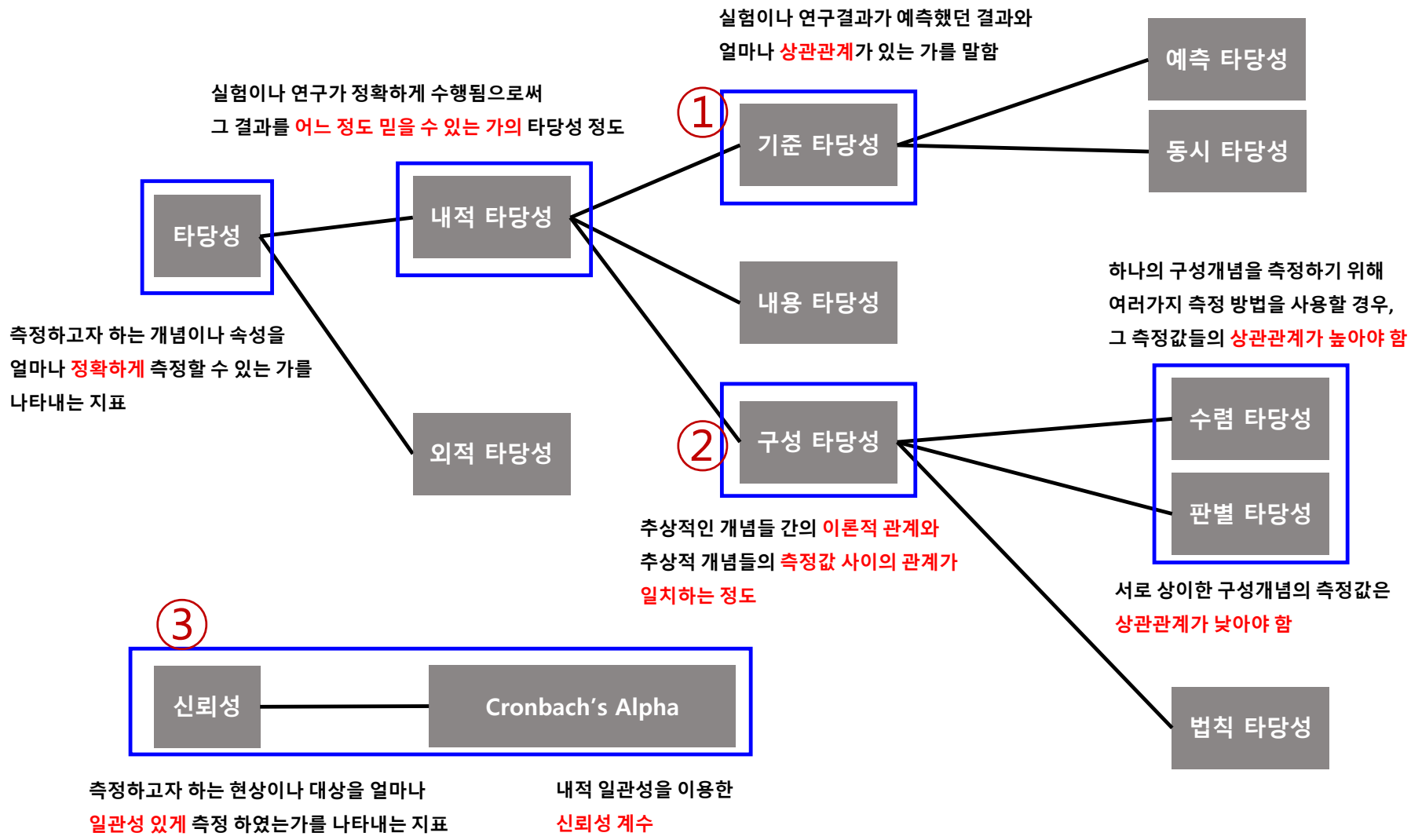
기밀성에는 이미 정보등급화를 포함하고 있음(← 결과변수를 원인변수로 활용)

The total influence score	Security (risk) grade		Description
9	1	High Confidential	As top grade, Level allowed only very limited small number
7~8	2	Confidential	As senior grade, Level allowed only personnel with limited access to services such as security managers
6	3	High Restricted	Departments and the top administrator, Security department only allowed access
4~5	4	Restricted	Internal staff and allow access only to a group of employees that the company does not apply to special restrictions in the corporate
3	5	Public	No matter the External open

정보 등급화 선행연구

영향 인자				Total
정보 가치	절대적 가치	정보 수준	난이도, 보유량, 혁신 정도, 사용자 중요도, 신규성 품질 수준, 신뢰도	10
		정보 창출 비용	자금, 시장규모	3
	상대적 가치	정보 속성	복제 용이성, 내용, 특성, 상태, 식별 용이성	5
		정보 활용도	유용성, 이용 빈도, 가용성, 정보처리도, 이용자 수	5
		가치 창출 능력	지속적인 개발 전망, 경 쟁 성, 사업성	9
유출 가능성			위험도, 장애요인, 침해행위, CIA, 기술보호정도	8
유출(훼손) 위험도(업무 영향도)			영향도, 업무 영향 범위, 활용 범위, 파급효과, 기술 범위, 업무 연속성	7

정보 등급화 모형 설계


타당성
측정하고자 하는 개념이나 속성을
얼마나 정확하게 측정할 수 있는 가를
나타내는 지표
내적 타당성
실험이나 연구가 정확하게 수행됨으로써
그 결과를 어느 정도 믿을 수 있는 가의 타당성 정도
외적 타당성
1
기준 타당성
실험이나 연구결과가 예측했던 결과와
얼마나 상관관계가 있는 가를 말함
예측 타당성
동시 타당성
내용 타당성
2
구성 타당성
추상적인 개념들 간의 이론적 관계와
추상적 개념들의 측정값 사이의 관계가
일치하는 정도
하나의 구성개념을 측정하기 위해
여러가지 측정 방법을 사용할 경우,
그 측정값들의 상관관계가 높아야 함
수렴 타당성
판별 타당성
서로 상이한 구성개념의 측정값은
상관관계가 낮아야 함
법칙 타당성
3
신뢰성
Cronbach's Alpha
측정하고자 하는 현상이나 대상을 얼마나
일관성 있게 측정 하였는가를 나타내는 지표
내적 일관성을 이용한
신뢰성 계수

정보 등급화 모형 설계

절대 가치	정보창출과 유지비용(input) (Information Making cost)		정보 창출 난이도
	산출된 정보수준(output) (Information Maturity)		외형적 정보 속성
			내재적 정보 속성
상대 가치	정보 활용도(use) (Information Sharing)		활용 빈도(정보 사용량)
			활용 범위
	정보활용 파급효과(outcome) (Information Potential Impact)	내부활용을 통한 효과	가치창출 가능성(경쟁우위)
		외부유출에 따른 위험	업무 연속성(복구)
			경쟁 가능성

정보 등급화 기반 보안서비스

1. 문서 선택

① 문서 구분 선택
(top down 방식 등급화)

② 문서 양식 선택
(워드, 엑셀, 파워포인트 등)

- 고용 계약서 — 2등급
- 중장기 경영계획 — 2등급
- 거래 명세서 — 2등급
- 연구노트 — 1등급

클릭 시, 작업 유형별 템플릿을 불러옴

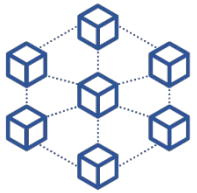
2. 정보등급산정 수행

③ 문서 작성 및 저장
(bottom up 방식 등급화)

등급화 평가 항목
1. 정보 창출과 유지비용
2. 산출된 정보 수준
3. 정보 활용도
4. 내부 활용 효과
5. 외부 유출 위험

- 문서 작성 후 처음 저장 시, 문서 작성자가 직접 등급화(점수화)
- Top down 방식 등급과 점수화에 따른 등급을 종합하여 정보등급산정 수행

④ 등급별 보안서비스 반영

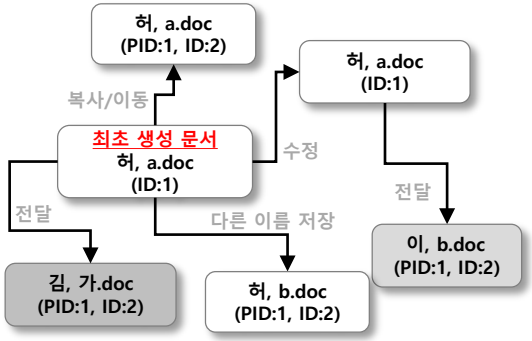


블록체인서비스

문서보안 서비스

3. 보안관리

⑤ 문서 추적 관리(등급 변경)



- 최초 업로드 시, 문서 ID 부여
- 다른 이름으로 저장, 복사, 이동, 전달, 수정 등의 행위 발생 시 문서를 추적 관리하고 + (필요 시)등급 변경
- 각 기업의 특급기밀은 국가 차원으로 관리(블록체인 활용)

⑥ 경제적 보안 활동

제도적 관리

- 중요정보구분 및 등급 분류
- 중요정보 표시
- 보안관리 전담인력 지정
- 보안관련 규정 마련 및 시행

물리적 관리

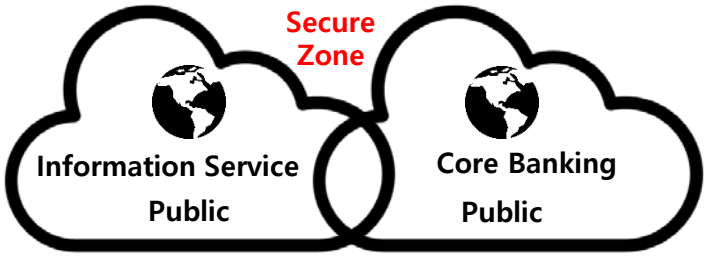
- 별도의 중요정보 개발/보관 장소 지정 및 관리
- 중요정보 접근/사용 권한 제한
- 분쟁 대비 중요정보 증거 확보

인적 관리

- 비밀유지서약서/비밀 유지약정 등 중요정보 보호의무 부과
- 중요정보 해당여부 및 보호의무 고지
- 중요정보 보안교육 실시

정보 등급화 기반 보안서비스

DATA PROTECTION: KNOWING IS HALF THE BATTLE



클라우드 정보민감도

망 분리 규제, 데이터 중요도 중심 개편 필요

데이터 중요도 별 망 분리 적용 시작해야

경청해 주셔서 감사 드립니다.

hbchang@cau.ac.kr