HYUNDAI

사내한
RESTRICTED

정보자산 위험관리 절차 수립 가이드

현대자동차 보안관리팀

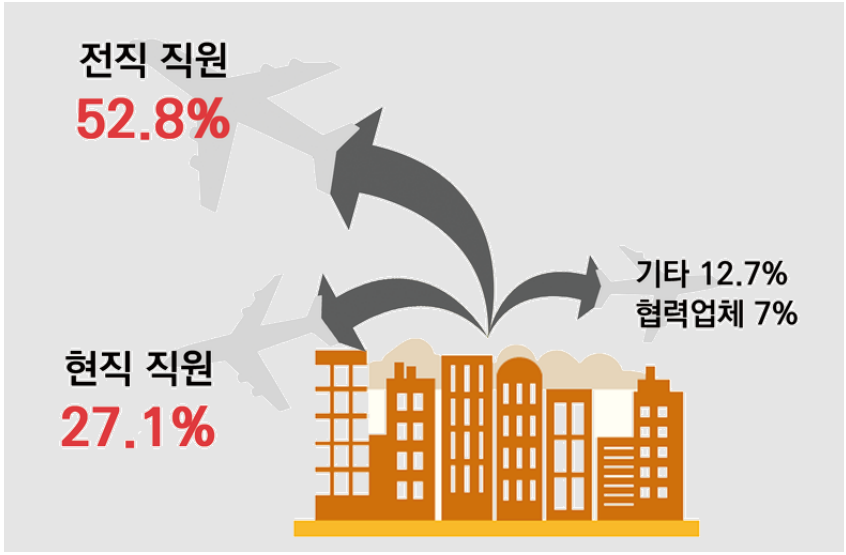
목차

정보자산 위험 관리의 필요성

정보자산 유출 동향

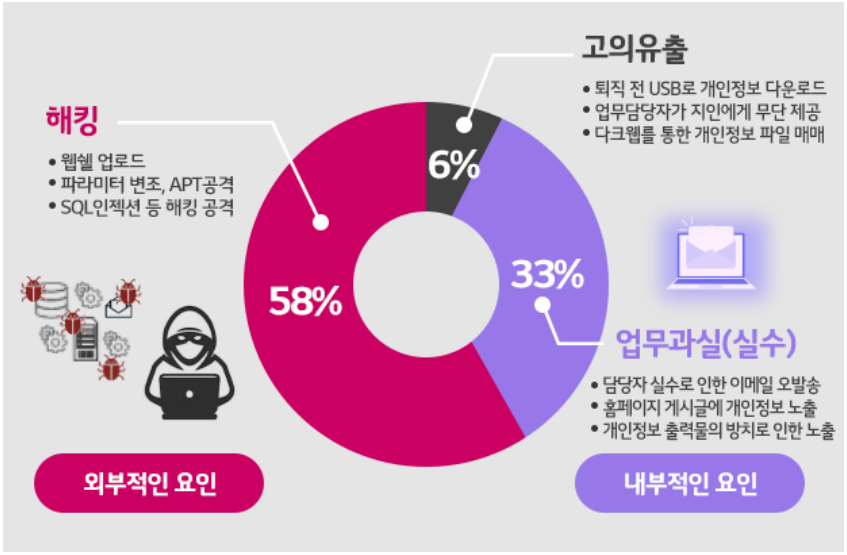
사이버 침해사고로 인한 기업 정보 유출 비중 급증 추세

내부자에 의한 고의성 정보 유출



출처: 한국산업기술보호협회(2016)

사이버공격으로 인한 비 고의성 정보 유출



출처: 한국인터넷진흥원(2021)

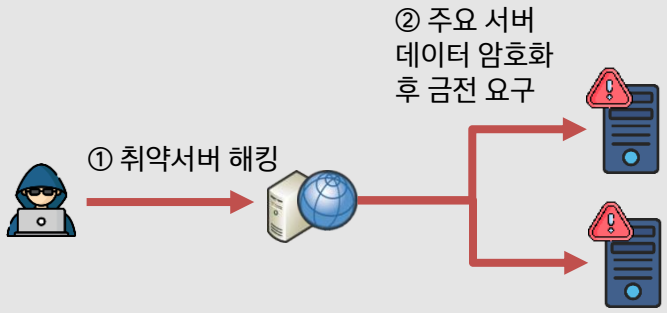
정보자산 위험 관리의 필요성

정보자산 유출 동향

**랜섬웨어 등의 공격으로 데이터 암호화에 따른 피해 뿐만 아니라
내부 정보 유출 및 판매로 인한 추가 피해 급증**

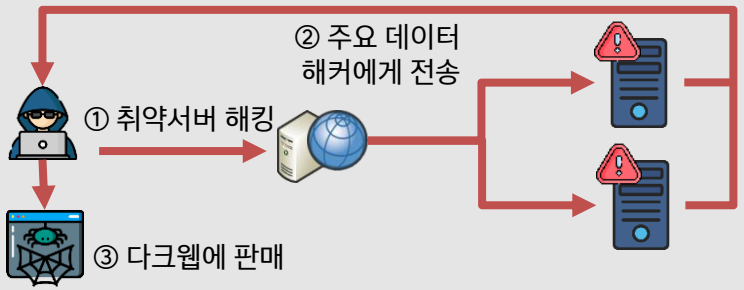
중요 데이터 암호화 후 암호 해제를 조건으로 금전 요구

'23년 협력사 주요 피해발생 유형



중요 데이터를 유출하여 불법 웹사이트(다크웹)에 판매

'24년 협력사 주요 피해발생 유형



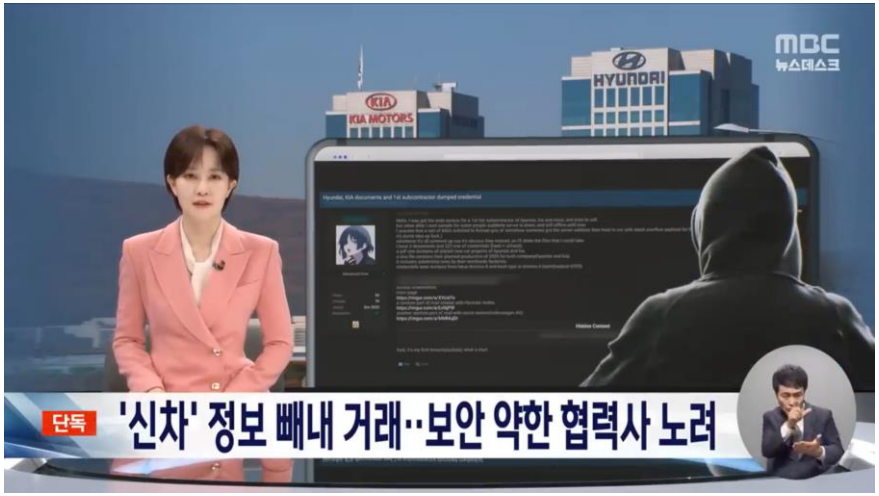
정보자산 위험 관리의 필요성

사내한
RESTRICTED

정보자산 유출 동향

랜섬웨어 등의 공격으로 데이터 암호화에 따른 피해 뿐만 아니라
내부 정보 탈취 · 거래로 인한 추가 피해 증가 추세

고객사 정보 동반유출 사례 증가



관리부재로 인한 유출사고가 계속 발생한다면…

- 피해 보상에 대한 이슈 발생 가능
- 고객사로부터 패널티 부여 가능
- 공급망 신뢰관계 훼손

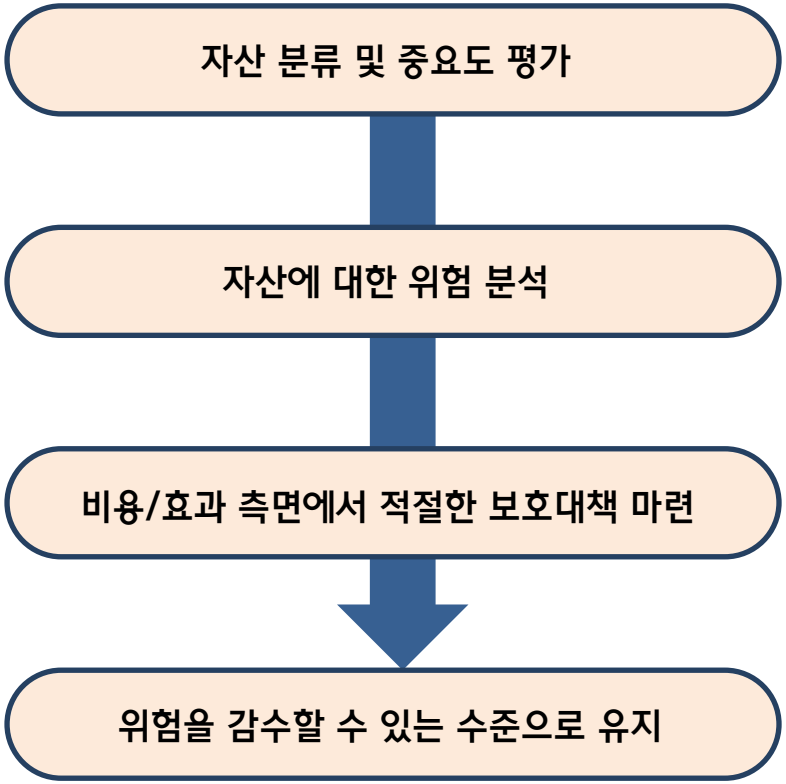
자사의 피해 뿐만 아니라, 고객사, 협력사 등 관계사의 정보 동반유출 발생으로 인한 영향을 대비해야 함

→ 체계적인 정보자산 위험 관리 필요

목차

■ 위험관리(Risk Management)란?

- 조직이나 기관의 자산에 대한 위험을 파악하고, 이를 수용할 수 있는 수준으로 유지하기 위한 활동
- 보안관리 활동의 핵심으로, 정보보호 정책을 바탕으로 조직에 적합한 전략을 결정하는 것



정보자산 위험관리 프로세스

자산 식별 → 위험분석 → 위험평가 → 위험처리 방안

1단계 : 정보자산 분류 및 중요도 평가

자산 식별 → 위험분석 → 위험평가 → 위험처리 방안

1) 정보 자산 식별 목적

- 기업의 보안활동의 궁극적 목표 → 자사가 보유한 중요자산 보호
- 자산의 식별과 평가 → 먼저 또는 무엇을 보호해야 할지 식별하기 위함

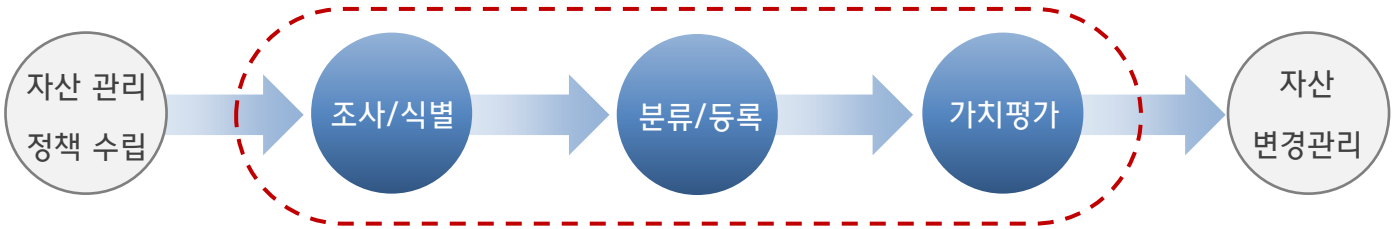
"자산목록 작성"

적절한 분류기준 정의 및 그룹핑/구분하여 중복 및 누락 최소화

2) 정보 자산의 관리 절차

- 조직에서 보유한 다양하고 방대한 자산을 체계적/효율적 관리 위함
- 자산의 도입, 변경, 폐기되는 전 과정(Life-cycle 관리)

▣ **자산관리 프로세스**



정보자산 식별 / 중요도 평가

1단계 : 정보자산 분류 및 중요도 평가

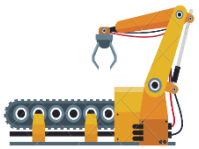
3) 정보 자산 조사 및 식별 대상

- 전자정보, 문서, 소프트웨어, 시설, 하드웨어, 지원설비, 인력 등 → 단, 기업별로 자산의 유형과 종류 다소 차이

  예) 제조사 : 설계도면 등 문서화된 출력물 또는 PC 저장파일, 설비 등
  IT회사 : 서버, 네트워크장비, 어플리케이션 등
  컨설팅/교육기관 : 전문가들, 인력

4) 정보 자산 분류 및 등록

- 유형적 자산(시스템 자산, 인력, 물리적 자산) / 무형적 자산(데이터/소프트웨어)로 분류
- 중요도에 따라 보안상 미미한 영향, 즉 중요도가 낮은 경우 세부 목록을 작성하지 않을 수 있음

정보	소프트웨어	하드웨어	설비/시설	인력
				
				

▲예시) 분류 가능한 정보자산 유형

5) 정보 자산 분류 및 등록

- 정보 자산 분류 기준표 작성(예시)

정보			소프트웨어		
자산번호	분류	비고	자산번호	분류	비고
ABCD-01	설계		OPQR-01	개발소스	
ABCD-02	승인도		OPQR-02	테스트	
ABCD-03	품질		OPQR-03	생산시스템	
ABCD-04	측정		OPQR-04	PLM	
ABCD-05	테스트		OPQR-05	QMS	
ABCD-06	생산		OPQR-06	ERP	
EFGH-01	구매		OPQR-07	금형관리	
LMNO-01	인사		OPQR-08	도면배포	
LMNO-02	마케팅		OPQR-09	그룹웨어	
LMNO-03	총무		OPQR-10	홈페이지	
LMNO-04	기획				
LMNO-05	특허				

No.	정보자산		
	유형	분류	자산명
1	정보	설계	PS-Roof-part2-2016
2	정보	설계	AC-Side-part10-2010
3	정보	승인도	hmc승인도(프로젝트명)(파트)*****
4	정보	테스트	부품(파트명)(테스트명)일시*****
5	정보	총무	월별 식단표
6	정보	마케팅	고객가치 세미나 발표자료 *****
7	소프트웨어	PLM	설계개발 모듈
8	소프트웨어	PLM	협업체계 모듈
9	소프트웨어	테스트	생산운영시스템 테스트 프레임
10	설비/시설	품질등	품질테스트 운영장비

※ 작성 유의사항

1. 식별번호, 자산유형, 자산 그룹 식별번호,
   - 자산명, 자산의 설명, 소유자, 중요도 명시

2. 분석이나 진단 시 활용하기 위한 추가 정보 포함
   - 서버/응용프로그램/OS명/아이피 등

1단계 : 정보자산 분류 및 중요도 평가

사내한
RESTRICTED

1) 정보 자산 중요도 평가

- 자산의 가치 평가 기준
- 식별된 자산의 중요도를 산정하고 등급을 선정하는 3가지 기준 : **기밀성 / 무결성 / 가용성**
- 기업의 특성에 따라 법적 준거성, 유출 영향도 등의 가치 평가 항목 포함 가능

기밀성 Confidentiality	➢ 인가된 당사자에 의해서만 접근하는 것을 보장 예) 정보시스템 관리자 권한
무결성 Integrity	➢ 인가된 당사자에 의해서 인가된 방법으로 변경 가능 예) 회사의 중요한 경영내역이 담긴 회계장부
가용성 Availability	➢ 자산이 적절한 시간에 인가된 당사자에게 접근 가능 예) 램섬웨어 감염으로 인한 정보 활용 불가
유출영향도 Effluent Impact	➢ 자산이 외부로 유출됐을 때 기업 이미지 및 존속에 영향을 미치는 정도

등급별
자산 중요도 평가

중요도 평가는 3개 등급 (상, 중, 하) 또는 5개 등급 (매우 중요, 중요, 보통, 낮음, 일반) 으로 분류
조직의 내/외부 공개 범위에 따라 사업 진행에 미치는 영향도 정도로 평가

2) 정보 자산 중요도 평가

- 4개 항목 총 10점 만점 기준 : 기밀성 (3), 무결성 (3), 가용성(2), 유출영향도(2)
- **점수 구간에 따라 3개 등급으로 구분 (극비 / 대외비 / 일반)**

기밀성 Confidentiality

배점	Extreme	High	Moderate	Low	Negligible
3점	3	2.3	1.5	0.8	0

무결성 Integrity

배점	Extreme	High	Moderate	Low	Negligible
3점	3	2.3	1.5	0.8	0

가용성 Availability

배점	High	Moderate	Negligible
2점	2	1	0

유출영향도 Effluent Impact

배점	Extreme	High	Moderate	Low	Negligible
2점	2	1.5	1	0.5	0

총 10점

예시

자산별 등급분류

점수 구간	등급
10 ~ 8 점	극비
8 ~ 4 점	대외비
4 ~ 0 점	일반

총 10점 만점 중 **극비 자산**은 10에서 8점, **대외비 자산은** 8에서 4점,
마지막으로 **일반 자산**은 4에서 0점으로 자산의 등급이 평가됩니다.

3) 정보 자산 중요도 평가 (예시)

No.	정보자산			중요도 평가 (Asset value)									등급 분류
	유형	분류	자산명	기밀성(C)		무결성(I)		가용성(A)		유출영향도(AI)		(합계)	
1	정보	설계	PS-Roof-part2-2016 ①	E	3.0	H	2.3	H	2.0	E	2.0	9.3	② 극비
2	정보	설계	AC-Side-part10-2010	H	2.3	E	3.0	M	1.0	M	1.0	7.3	대외비
3	정보	승인도	hmc승인도(프로젝트명)(파트)*****	H	2.3	H	2.3	H	2.0	H	1.5	8.1	극비
4	정보	테스트	부품(파트명)(테스트명)일시*****	H	2.3	E	3.0	M	1.0	E	2.0	8.3	극비
5	정보	총무	월별 식단표	Π		M	1.5	L		Π		1.5	관리제외
6	정보	마케팅	고객가치 세미나 발표자료 *****	M	1.5	M	1.5	M	1.0	M	1.0	5.0	일반
7	소프트웨어	PLM	설계개발 모듈	E	3.0	H	2.3	M	1.0	E	2.0	8.3	극비
8	소프트웨어	PLM	협업체계 모듈	H	2.3	H	2.3	H	2.0	H	1.5	8.1	극비
9	소프트웨어	테스트	생산운영시스템 테스트 프레임	H	2.3	M	1.5	L		L	0.5	4.3	일반
10	설비/시설	품질동	품질테스트 운영장비	H	2.3	H	2.3	L		H	1.5	6.1	대외비

자산별 중요도 평가
(기밀성 / 무결성 / 가용성 / 유출영향도)

→

합계 점수에 따른 등급 분류
(극비 / 대외비 / 일반)

* 추가 참고자료 : https://www.tradesecret.or.kr/info/secret/calculation.do

정보자산 위험관리 프로세스

자산 식별 → 위험분석 → 위험평가 → 위험처리 방안

■ 위험이란?

- 위협(Threat): 정보 혹은 시스템에 대해 피해를 유발하도록 취약성을 활용할 수 있는 가능
- 취약성(Vulnerability): 악용 당할 수 있는 결점 또는 안전장치의 부재
- 위험(Risk): 취약성의 악용으로 발생 가능한 잠재적 손실 가능성

바이러스 위협 | 병균에 취약 | 감기 위험

※ 취약성과 위협의 차이??

감기 바이러스는 어디에나 존재하지만 감기에 걸리는 사람이 있고 안 걸리는 사람이 있다. 그것은 그 사람의 건강상태에 의해 결정된다.
마찬가지로 위협(감기 바이러스)은 어디에나 있지만 취약성(건강상태) 여부 및 정도에 따라 위험(감기에 걸리는 상태)으로
바뀌어 지는지의 여부가 결정된다.

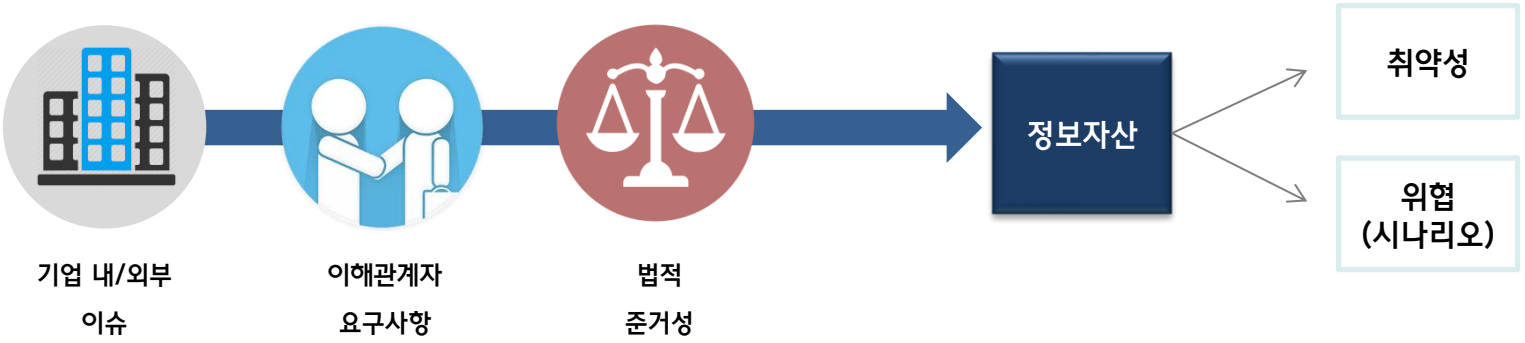
2단계 : 위협에 대한 약점은 무엇인가 – 위험 분석

자산 식별 → **위험분석** → 위험평가 → 위험처리 방안

- 자산식별을 통해 식별된 자산에 대한 위협, 취약성, 위험을 모두 도출하고 분류하여 자산의 가치에 대한 잠재적 손실에 대한 영향을 분석
- 자산에 대하여 위협과 취약성 두 가지 요소에 대해 컨텍스트 분석

컨텍스트(Context) 분석

기업이 연속적인 영업활동을 영위 하는데 있어서 발생하는 보안 위협 요소로 기업 내 · 외부에서 발생하는 이슈, 이해관계자, 법적 요구사항에 의해 식별되는 보안위협을 말한다.



2단계 : 위협에 대한 약점은 무엇인가 – 위험 분석

사내한 RESTRICTED

시나리오 기반 위험분석 사례

예시

위험 분석 예시

김 과장

업무 관련한 가장 중요한 정보는 입사지원자의 인사정보 입니다. (자산)
온/오프라인으로 받는 서류를 채용이 확정될 때까지 안전하게 보관해야 합니다

사고가 생긴다면 아마도 채용 시스템 장애가 있을 수 있습니다. (위협)
시스템 장애로 입사지원 데이터가 손실된다면 큰 문제입니다. 입사서류 분실 문제도 마찬가지 입니다. (위협)
또한, 지금까지 입사 지원서를 통해 주민등록번호를 수집해왔는데 이는 개인정보보호법에 위배된다고 하더라고요. (위협)

자산 중요도 평가 결과

주요 자산	책임자	자산 중요도	비고
입사지원정보(온라인)	김과장	3	※ 중요도 평가 기준(자체적) 3 : 회사 전체에 치명적 영향 2 : 사업 일부에 영향 1 : 조직 일부에 영향
입사지원서류	김과장	2	
기업 평판	사장	3	

취약성 및 위협 평가

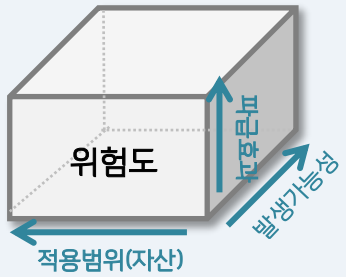
취약성	대응 위협
채용 시스템 백업부재	채용 시스템 장애
배포된 채용 서류 관리 부실	채용 서류 분실
	채용과정 법규 위반
주민번호 수집 채용 시스템	채용과정 법규 위반
법적준거성 판단 역량 부재	채용과정 법규 위반

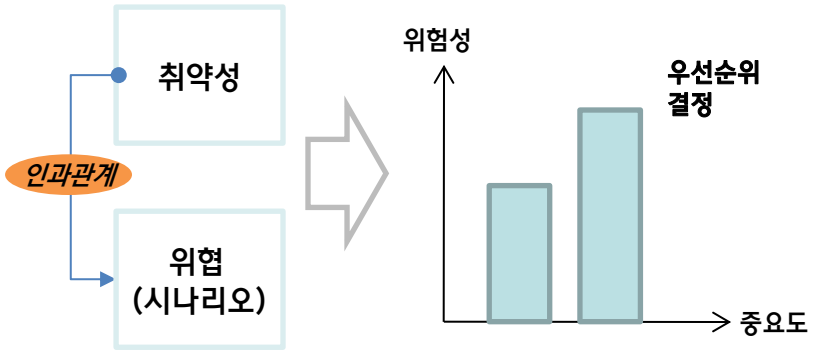
3단계 : 얼마나 위험한 것인가 – 위험 평가

자산 식별 → 위험분석 → **위험평가** → 위험처리 방안

위험도 평가 및 DoA (Degree of Acceptance)

- 보안위협에 대한 위험도를 적용범위, 발생가능성, 파급효과 등 비즈니스 영향 관점에서 수치화
- 위험정보를 측정한 뒤, '수용할 수 있는 수준' 이상의 위험에 대해서만 비용을 들여 대응하는 것으로 결정
- 위험도 = 적용범위(자산) X 발생가능성 X 파급효과 ▶ ex) DoA ≥ 6 경우 해당 위험대응 (위험처리)
- 분석한 데이터를 통해 미리 설정한 목표위험수준과 비교하여 각 위험의 대응여부와 우선순위 결정(경영진)





위험도	개수	
9	1	처리해야 할 위험 (위험감소)
8	3	
7	6	
6	4	
DoA		
5	4	잔여위험으로 관리 (위험수용)
4	2	
3	3	
2	2	
1	0	

위험도 높음

위험도 낮음

정보자산 위험관리 프로세스

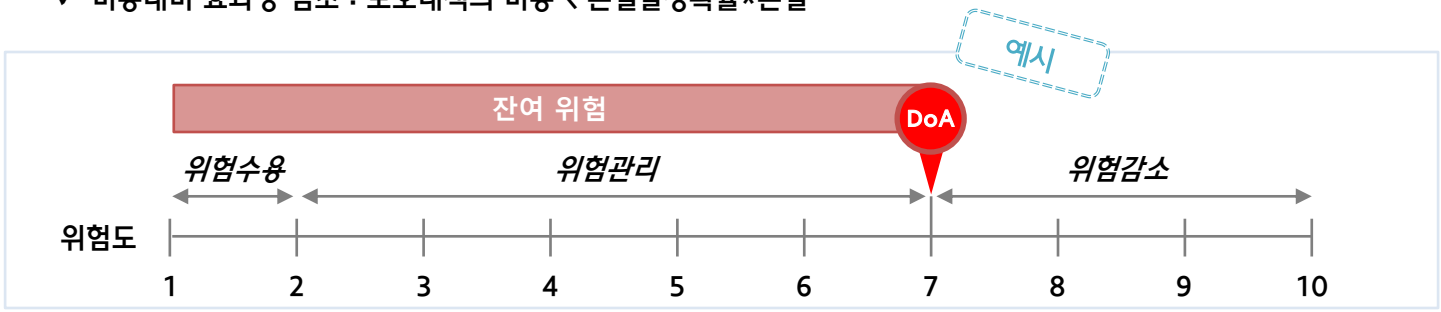
자산 식별 → 위험분석 → 위험평가 → 위험처리 방안

4단계 : 어떻게 위험에 대응할 것인가 – 위험처리 방안

자산 식별 → 위험분석 → 위험평가 → **위험처리 방안**

✓ 보장수준 이하로 위험을 낮추기 위하여 정보보호 대책을 선정함 (Root Cause 에 집중)

✓ 비용대비 효과성 검초 : 보호대책의 비용 < 손실발생확률*손실

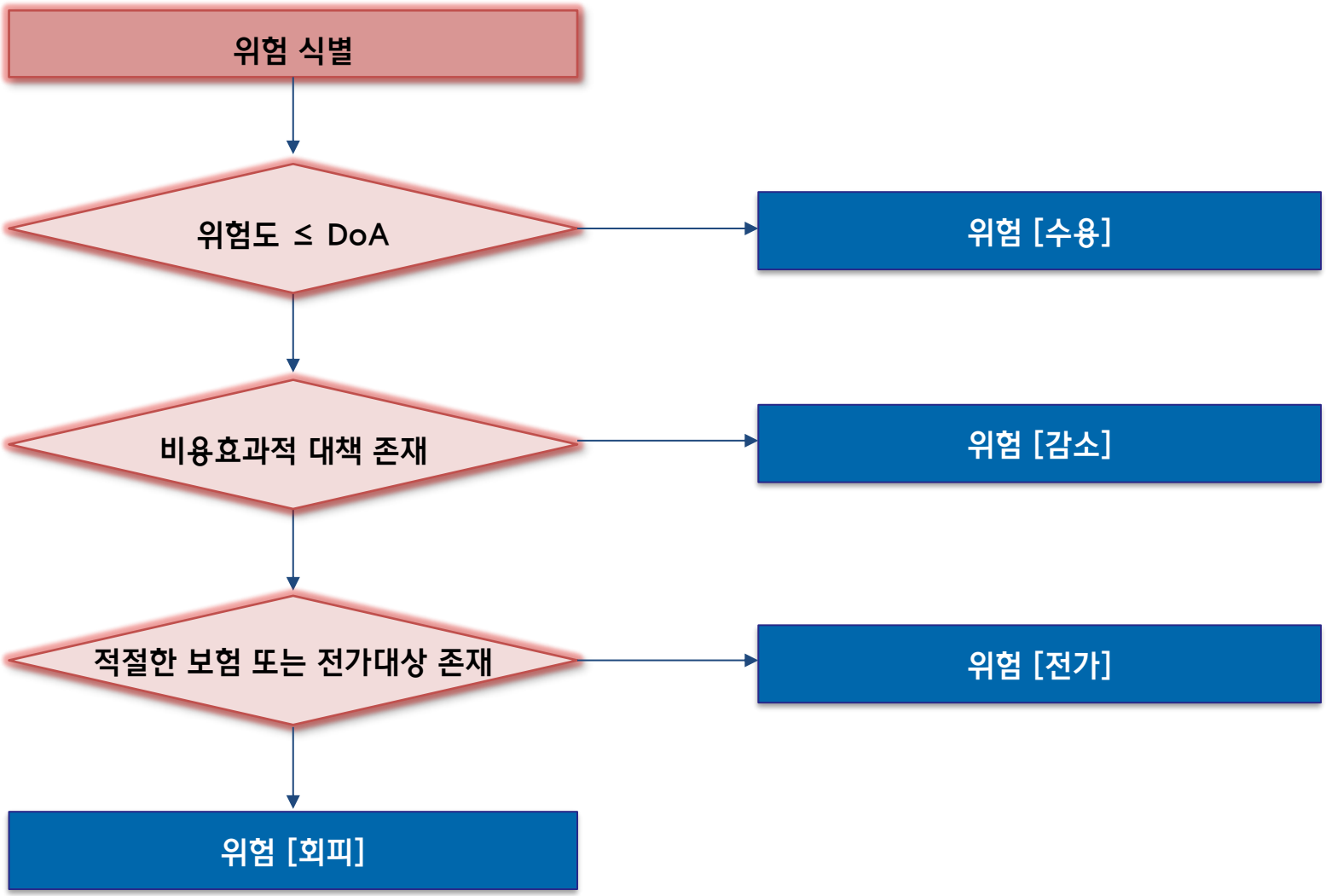


구 분	내 용	비 고
위험 [회피]	위험이 발생할 수 있는 자산 등 요인을 근본적으로 제거	사업포기 등
위험 [전가]	잠재 손실의 결과를 제3자 등에게 이전	보험 가입 등
위험 [감소]	보안대책을 적용하여 취약성 제거 등을 통해 위험을 감소시킴	보안조치 적용
위험 [수용]	위험을 받아들이고 별도의 조치를 취하지 않음	조치 미적용

위험으로 인한 '손실'이 위험을 억제하는데 드는 비용보다 적다면, 그 손실은 감수하는 편이 낫다는 것이 기본 논리

위험관리의 목적은 **위험을 아예 제거하는 것이 아니라 수용할 수 있는 수준까지 낮추는 것**.

4단계 : 어떻게 위험에 대응할 것인가 – 위험처리 절차



위험 평가 + 처리방안 (예시)

김 과장

DoA를 7로 정했으며, 7을 초과하는 항목에 대해 대응 전략을 수립할 예정입니다.
또한 그 이하 위험에 대해서는 감수하거나 잠정적으로 대책을 보류하는 것으로 결정합니다.

1. DoA를 초과하는 위험 (DoA 7초과 이상 취약성 대응)

자산	취약성	대응 위협	자산중요도	파급효과	발생가능성	위험도
기업평판	주민번호 수집 채용 시스템	채용과정 법규 위반	3	3	4	10
입사지원정보 (온라인)	채용 시스템 백업부재	채용 시스템 장애	3	1	2	6
입사지원서류	배포된 채용 서류 관리 부실	채용 서류 분실	2	2	2	6
		채용과정 법규 위반	2	2	1	5
기업평판	법적준거성 판단 역량 부재	채용과정 법규 위반	2	2	1	5

위험도 높음 (DoA 이상)

위험도 낮음 (DoA 미만)

2. 대응 전략

대응전략	상세 방안	고려사항 및 비용	결정안
회피	채용시스템 사용 중지	채용 시 경쟁력 약화	
전가	민사소송에 대비한 손해배상 보험 가입	보험비용 과다 및 형사처벌 불가피	
감소	채용시스템 개선	약 2개월 소요 + 비용 발생	●
수용	기존 시스템 운영	적발 시 민형사상 책임 수위 높음	

※ 첨부 : 기본통제 정책 (Annex)

✓ 정보보호관리 요구사항

- 정보보호에 관련된 위험을 통제하기 위한 요구사항
- 향후 위험평가를 통하여 조직이 수용 가능한 위험 수준을 달성할 수 있도록 선택

▣ Annex (통제정책) 및 적용대상 선정 : 관리영역

①

분류		통제정책
관리 영역	정책	정책, 세부지침, 전담조직 운영
	보안활동	정기감사, 로그기반감사, 서약서, 자율보안점검, 퇴직자보안관리
	인식제고	교육, 협의체회의, 홍보활동, 위반자징계
	문서보안	문서고운영, 등급표기, 워터마크, 암호화, 유통통제
	정보자산보관	저장통제(분류), 파일서버운영, QMS, 문서중앙화
	유통관리	로그관리, PLM, 도면배포시스템, 2차사 점검, 문서폐기확인

통제 정책 선정

②

분류		통제정책
관리 영역	정책	정책, 세부지침
	보안활동	서약서, 자율점검, 퇴직자관리
	인식제고	교육, 홍보
	문서보안	문서고, 등급표기, 워터마크
	정보자산보관	저장통제(분류), 파일서버운영, PLM
	유통관리	로그관리, 도면배포시스템,

통제 정책 적용대상 선정

③

적용대상					
정보	S/W	H/W	설비	인력	기타
●	●	●	●	●	
●	●			●	
				●	
●					
●	●				
●					

※ 첨부 : 기본통제 정책 (Annex)

✓ 정보보호관리 요구사항

▣ Annex (통제정책) 및 적용대상 선정 : 물리영역

①

분류		통제정책
물리 영역	보호구역	보호구역설정, 구역별 출입통제, 출입이력관리
	상황감시	CCTV운영, 촬영통제, 차량출입통제, 경비운영
	전산장비	장비반출입통제, HDD탈부착방지, HDD폐기관리
	외부인원	방문자통제, 상주인원보안조치

통제 정책 선정

②

분류		통제정책
물리 영역	보호구역	보호구역설정, 구역별 출입통제
	상황감시	CCTV운영, 촬영통제, 차량출입통제, 경비운영
	전산장비	장비반출입통제, HDD탈부착방지, HDD폐기관리
	외부인원	방문자통제

③ 통제 정책 적용대상 선정

적용대상					
정보	S/W	H/W	설비	인력	기타
			●	●	●
	●	●	●	●	
●	●	●	●		
				●	

※ 첨부 : 기본통제 정책 (Annex)

✓ 정보보호관리 요구사항

▣ Annex (통제정책) 및 적용대상 선정 : 기술영역

①

분류		통제정책
기술 영역	사용자인증	사용자 인증, 부가인증, 패스워드관리, 세션타임아웃, 서버접근관리
	침입차단	백신, 방화벽, IPS, IDS, 웹방화벽
	유출통제	매체제어, 사이트차단, DLP, 대용량파일송수신, 개인정보암호화, DB암호화
	네트워크보안	무선AP PW설정, AD, IP통제, NAC, OA · FA분리, 이중화
	시스템보안	시간동기화, VPN, 자산관리
	백업복구	비상계획수립, 소스코드형상관리, 백업시스템 구성
	모니터링	장애대책, 성능용량관리, 로그관리 · 분석, 상시보안관제

통제 정책 선정

②

분류		통제정책
기술 영역	사용자인증	사용자 인증, 부가인증, 패스워드관리, 세션타임아웃
	침입차단	백신, 방화벽
	유출통제	매체제어, 사이트차단, DLP
	네트워크보안	무선AP PW설정, AD, IP통제
	시스템보안	시간동기화, VPN, 자산관리
	백업복구	비상계획수립
	모니터링	장애대책, 성능용량관리

③ **통제 정책 적용대상 선정**

적용대상					
정보	S/W	H/W	설비	인력	기타
●	●			●	
●	●				
●	●				
●	●				
●	●	●			
●	●				
●	●			●	

목차

전자문서 유출 통제 방안

사이버 침해사고로 인한 전자문서 외부 유출 상황을 고려하여
‘위험 감소’ 측면의 예방 조치 필요

관리적 통제 방안

- 유통 통제
- 접근권한 통제
- 파기 관리
- 암호 설정

+

기술적 통제 방안

- DRM 적용
- DLP 적용
- 문서 중앙화 시스템 적용
- 대용량 파일 전송 시스템

전자문서 유출 통제 방안

관리적 통제 방안

위험평가 결과 위험도가 높은 문서유형을 대상으로 유출 통제를 위한 세부 기준 마련 필요

[예시: 유출통제 관리 대상 항목]

관리항목		내용
출처		내부조직/고객사/협력사 등 원본 출처
문서유형		문서분류체계 상의 문서 유형 명칭
보안등급		중요도 평가 결과 상의 보안등급
보존연한		파기 관리를 고려한 문서 보존 연한
암호화		암호화된 상태로 저장되어야 대상 여부
접근권한	사용자	접근 허용 대상(임직원, 내부 조직, 협력사 등)
	접근권한	읽기/편집/복사/유통 등 사용 권한
내부유통	유통범위	사내 유통 가능한 범위
	유통수단	사내 메일, 사내 메신저 등 유통 수단 한정

관리항목		내용
내부유통	유통승인	유통시 승인 필요 여부 및 승인 필요 조건
	승인권자	유통 승인권자
외부유통	유통범위	사외 유통 가능한 범위
	유통수단	사내 메일, 사내 메신저 등 유통 수단 한정
	유통승인	유통시 승인 필요 여부 및 승인 필요 조건
	승인권자	유통 승인권자
파기	파기확인	파기확인 필요 여부
	확인주기	파기확인 실시 주기
	확인담당	파기확인 담당

[예시: 유출통제 관리 양식]

출처	문서유형	보안등급	보존연한	암호화	접근 권한					내부 유통 통제				외부유통 통제				파기 관리		
					사용자	읽기	편집	복사	유통	유통범위	유통수단	유통승인	승인권자	유통범위	유통수단	유통승인	승인권자	파기확인	확인주기	확인담당
OO팀	OO	사내한	3	대상	생성자	O	O	O	O	상생실	사내메일	대상	팀장	현대차 기아차	사내메일	대상	실장	대상	1개월	생성자
					OO팀	O	O	X	X											
					OO실	O	X	O	O											
					OOO 책임	O	X	X	X											
고객사																				
협력사																				

전자문서 유출 통제 방안

관리적 통제 방안

문서작성 애플리케이션이 제공하는 암호설정 기능을 활용하여 암호화된 상태로 보관

[암호설정 기능 지원 문서작성 애플리케이션]

▲ Word 2021 ▲ Excel 2021 ▲ PowerPoint 2021

▲ 한글 2022 ▲ 한셀 2022 ▲ 한쇼 2022

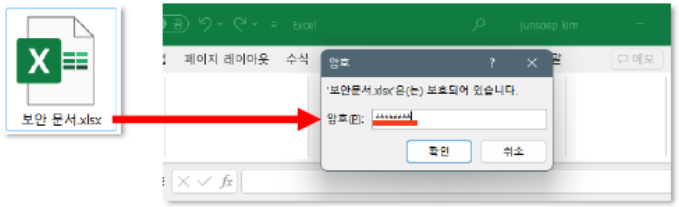
※ 애플리케이션 별 암호설정 방법은 별도 배포 예정인
"중소기업 기술 유출 방지 IT보안 가이드라인(임직원편)"
78p~92p 참조

[예시: 엑셀 파일 암호설정]

1 [좌측 상단 '파일' 클릭]

2 ['정보'탭 클릭] > ['문서 보호' 클릭] > ['암호 설정' 클릭] > [암호 입력] > ['확인' 클릭]

3 [보호 파일 실행] > [암호 입력]



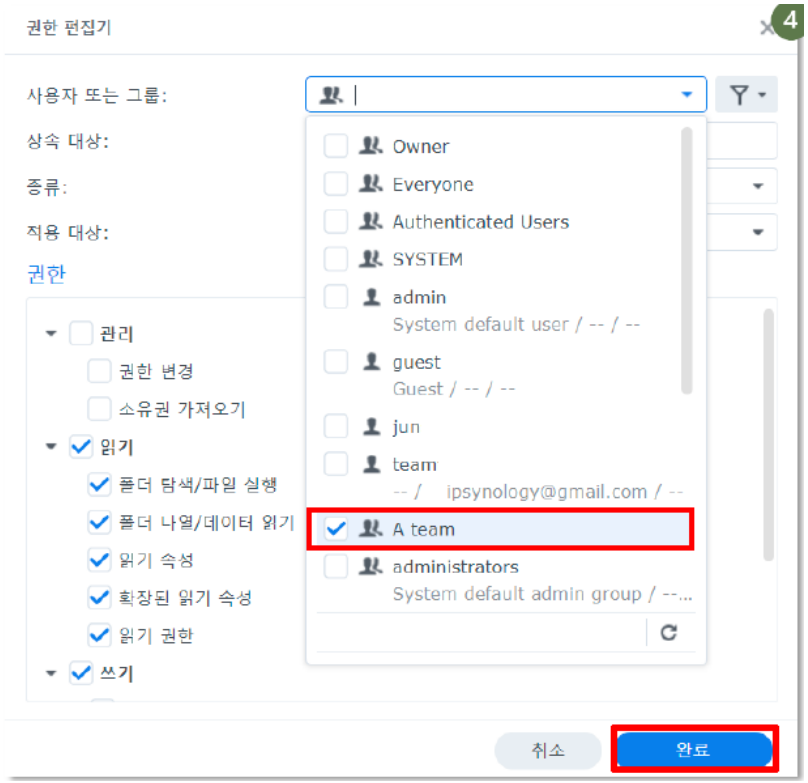
전자문서 유출 통제 방안

사내한
RESTRICTED

관리적 통제 방안

비정형 파일이 보관되는 파일서버, NAS서버, 문서 중앙화 시스템등 파일/폴더 접근권한 관리 강화

[예시: NAS 접근권한 설정 화면]



[주요 고려사항]

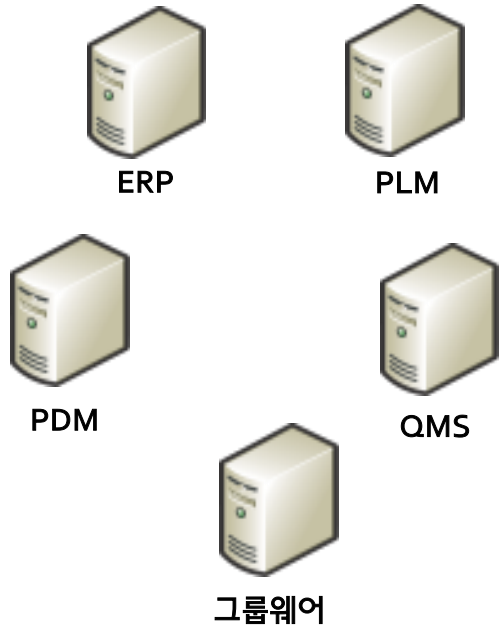
- 중요파일 접근권한 제한
  - 업무상 반드시 필요한 사용자에 한하여 접근권한 허용
- 중요파일 복사권한 제한
  - 무분별한 복제, 다운로드로 인해 복제된 파일 유출 위험 최소화
- 중요파일 편집권한 제한
  - 파일 수정을 불가토록 설정 하여 랜섬웨어로 인한 피해 최소화

전자문서 유출 통제 방안

관리적 통제 방안

ERP, PLM, PDM 등 중요 문서가 저장된 시스템에 파일 다운로드 권한 통제 강화

[예시: 다운로드 통제 대상 주요 시스템]



[주요 조치방안]

- 메뉴/페이지 별 접근권한 통제 적용
- 첨부된 파일 다운로드 권한 통제 적용
- 데이터베이스 암호화

전자문서 유출 통제 방안

기술적 통제 방안

파일 암호화(DRM) 솔루션도입

[주요 기능]

자동 복호화
인증된 사용자와 인가된 어플리케이션만 자동 복호화

S/W 암호화 설정
관리자가 쉽게 어플리케이션 S/W 단위로 암호화 여부를 스위치로 끄거나 켤 수 있음

개인정보처리
위험치를 자동으로 계산하여 보여줌.
문서 삭제, 필요시 서버에 보관

문서 백업 및 다운로드
정책에 의해 사용자가 저장하는 문서를 중앙 서버로 백업

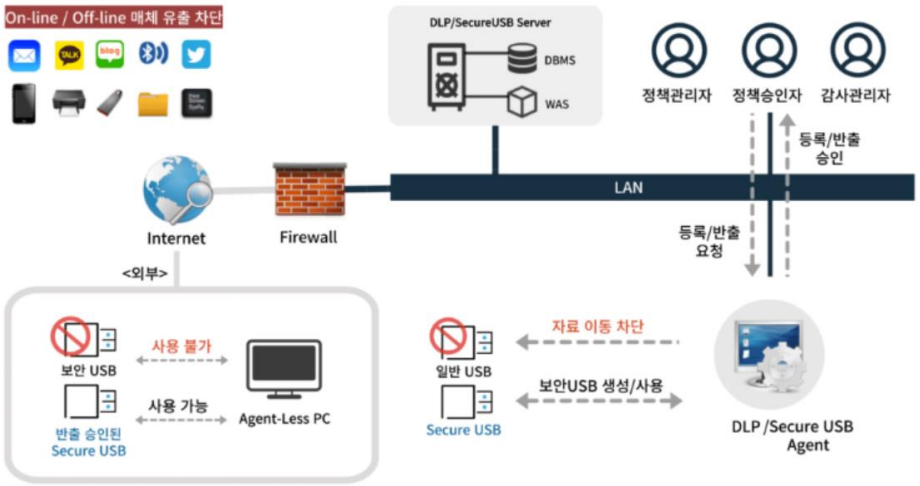
전자결재
사용자는 전자결재 기능을 사용하여 파일 복호화 및 격리해제 요청 가능

모바일 뷰어
개인 정보를 가중치에 따라 기록, 암호화, 격리, 삭제 기능 제공

전자문서 유출 통제 방안

기술적 통제 방안

정보유출 방지(DLP) 솔루션 도입



[주요 기능]

차단 및 경고
On-Off Line 통제
(메일, 사이트, 메신저,
USB, 프린터, 스마트폰 등)

녹화
정보 유출 시점 동영상 녹화 및
재현(법적 증적 자료 활용)

파일흐름보기
이름 및 확장자 변경에 대한
유출 내역 추적

SecureUSB Module
일반 USB를 암호화하여
로그인/로그아웃 방식으로
보안영역을 제공

SSL통제
SSL 통신으로 발송되는 모든
파일 및 메일 통제(별도 SSL
가시화 장비구축 없이 통제)

Discovery Module
개인 정보를 가중치에 따라
기록, 암호화, 격리, 삭제 기능
제공

WISEBEAM
대시보드를 통한 정보
유출 관제 시스템 구축

사본저장
유출 파일에 대한 사본 및 다운
로드 기능 제공

감사 및 모니터링
유출 횟수가 잦아진 특정 구성
원 및 특정 유출 형태에 대한
실시간 감시

전자문서 유출 통제 방안

사내한
RESTRICTED

기술적 통제 방안

문서 중앙화 솔루션 도입

[주요 기능]

보안기능

- 네트워크락 기능으로 내부망, 외부망 차단 가능
- 어플리케이션, 확장자, 경로 등 로그 취득 대상 제한
- 협력사에 암호화된 파일(파일/폴더/링크) 전달 가능

업무지원기능

- 유연한 보안 정책으로 반출 및 정보 유출 통제
- 문서 및 3D CAD 등 종류 관계없이 보전 관리 유용
- 검출 문서 통제를 통한 개인정보

인공지능 지식관리 솔루션

- 검색어 설정을 통해 문서 카테고리 및 상세 검색 가능
- 자동문서 카테고리 분류가 가능한 지식관리 솔루션

빅데이터 기능

- 전체/월별/연도별 문서 현황, 시간별/부서별/사용자별 반출 현황을 빅데이터로 분석 가능

목차

’25년 사이버 침해사고 예방을 위한 주요 추진 과제

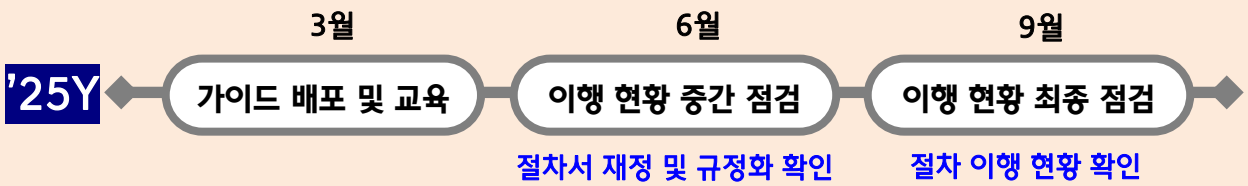
1. 문서관리 절차서 재정

- 문서 유형분류, 중요도평가, 위험분석, 위험평가, 통제 방안을 포함하는 기준, 절차, 양식 문서화

2. 문서 위험관리 절차 이행

- 정보자산 분류 (자산 유형 리스트, 유형별 보안등급 포함)
- 위험 분석 및 위험평가 결과 (위험평가 점수 산출, 위험처리 방안 포함)
- 위험처리 방안 적용 (핵심관리 대상 전자문서 선정 및 통제방안 적용 이력 포함)

정보자산 위험관리 이행 점검 계획



Thank you