

# 가족기업을 위한 정보자산 보안관리 방법

2025. 11. 27

The world Leader in Digital Security



(주)디지털센스  
DigitalSense Co., LTD

최 주 호



# 목차

1. 기업에서 정보자산 관리의 어려움
2. 보안관리를 위한 필수 사항
3. 정보자산 보관 및 유출경로
4. 정보자산 관리 방법
5. 정보자산 보호 대책
6. 보안관리 방안
7. 보안시스템 구축 방안
8. SI도구 사용시 보안사항

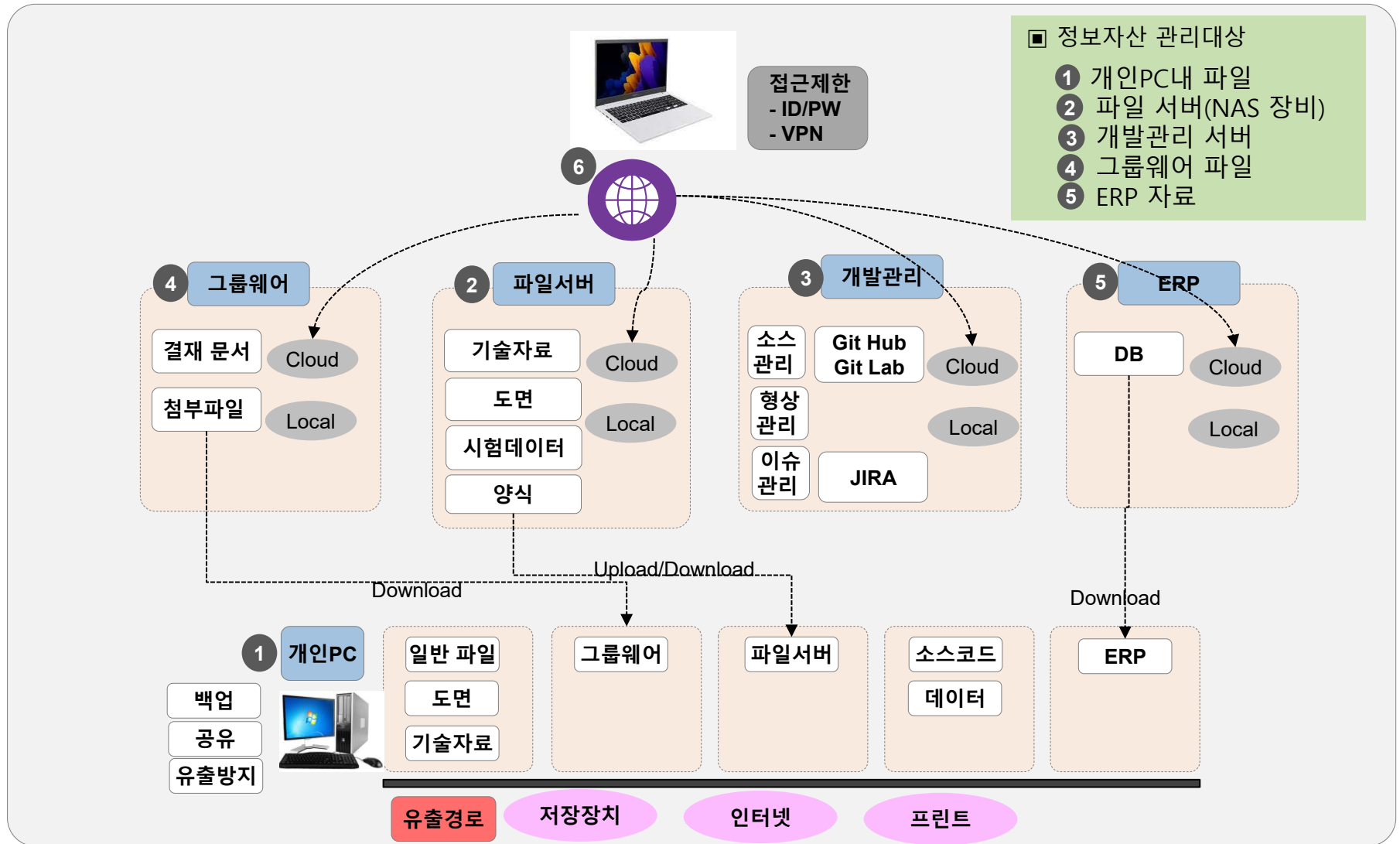
# 1. 기업의 정보자산관리 어려움

구분	문제점	대책
파일 관리	정보자산의 사유화	1. 파일 백업      문서중앙화
	파일 공유	
	파일 백업	파일 백업      문서중앙화
	랜섬웨어 감염	
	정보자산 파괴 (파일 파괴)	
유출 방지	정보 유출	3. DLP (유출방지)      DRM (암호화)
	유출 근거(법률적)	4. DLP (근거유지)

## 2. 보안관리를 위한 필수 사항

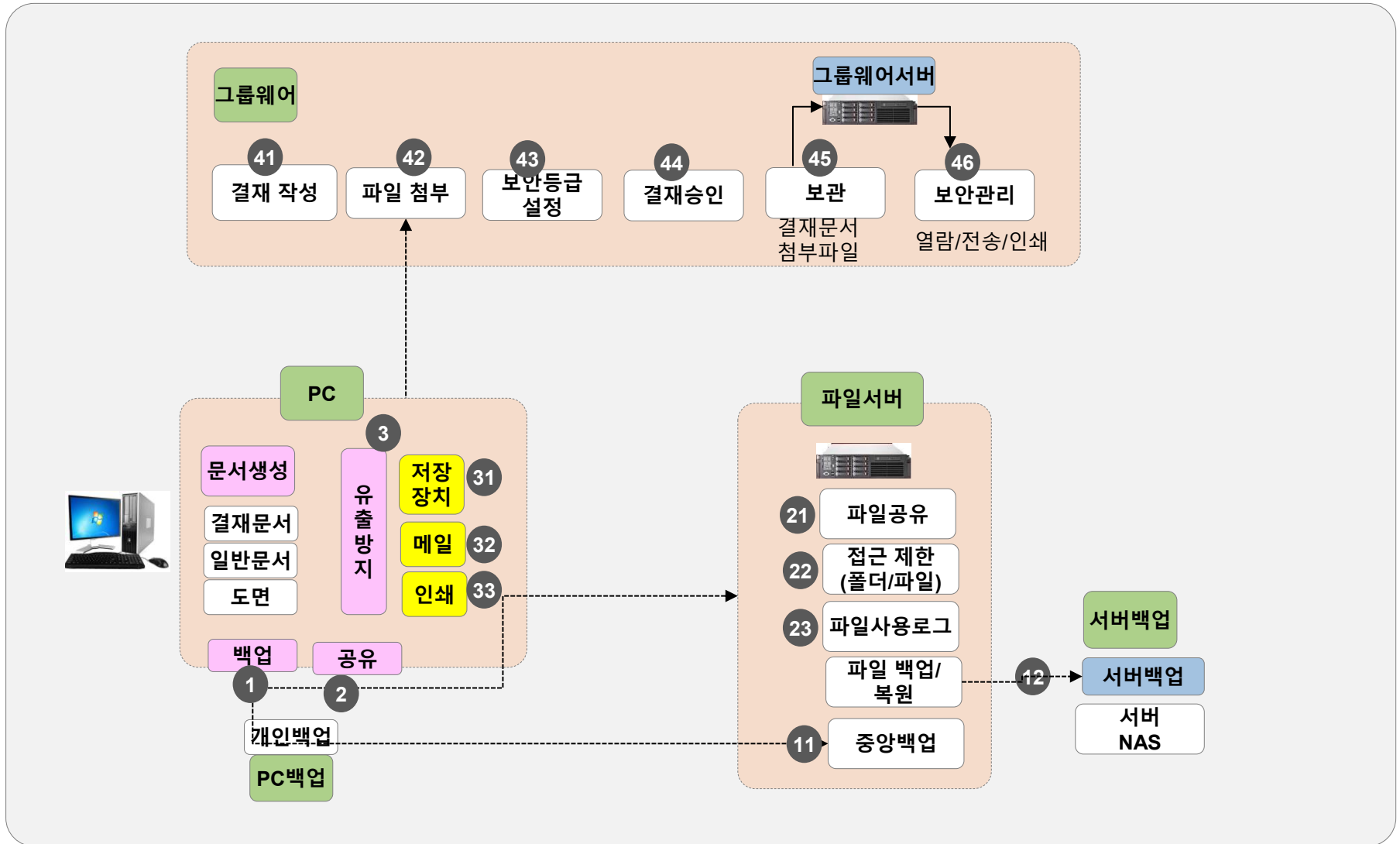
법규	<ul style="list-style-type: none"><li>❖ 영업비밀 보호법</li><li>❖ 개인정보보호법</li><li>❖ 방위산업 등</li></ul>
보안 규정 지침,절차서, 양식	<ul style="list-style-type: none"><li>❖ 보안규정/지침/절차서</li><li>❖ 보안관련 양식</li></ul>
보안교육	<ul style="list-style-type: none"><li>❖ 보안의식 제고</li><li>❖ 법규, 규정, 지침</li></ul> <ul style="list-style-type: none"><li>❖ 보안 시스템 구축후 관리/운영 교육</li></ul>
보안 시스템 구축	<ul style="list-style-type: none"><li>❖ 물리보안<ul style="list-style-type: none"><li>- 출입통제</li><li>- CCTV</li></ul></li><li>❖ 정보자산<ul style="list-style-type: none"><li>- DLP/DRM/문서중앙화</li><li>- 네트워크 보안 등</li></ul></li></ul>
사고 대비 근거(증거) 확보	<ul style="list-style-type: none"><li>❖ 정보 유출 로그<ul style="list-style-type: none"><li>- 복사, 전송, 인쇄 등</li></ul></li><li>❖ 포렌식</li></ul>
사고 발생	<ul style="list-style-type: none"><li>❖ 법적 조치</li></ul>

# 3. 정보자산 및 유출경로



- ▣ 정보자산 관리대상
- 1 개인PC내 파일
  - 2 파일 서버(NAS 장비)
  - 3 개발관리 서버
  - 4 그룹웨어 파일
  - 5 ERP 자료

# 4. 정보자산 관리방법



# 5. 정보자산 보호 솔루션

## DLP 방식 (Data Loss Prevention)

- ❖ 파일의 저장/전송 차단하여 유출을 원천적으로 방지
- ❖ 저장장치나 통신을 통하여 외부로 유출 시 로그 생성하여 유출 추적성이나 근거성 확보

## DRM 방식 (파일 암호화)

- ❖ 문서(파일)를 저장시 암호화하며, 외부 유출시 노출을 방지

## 문서중앙화 방식

- ❖ 개인컴퓨터에 파일 저장을 최소화하고 중앙서버에 저장하여 유출 위험을 최소화
- ❖ 중앙서버에 폴더별 접근 권한 부여
- ❖ 중앙서버에 파일 Upload/DownLoad 로그 관리

## 네트워크 보안

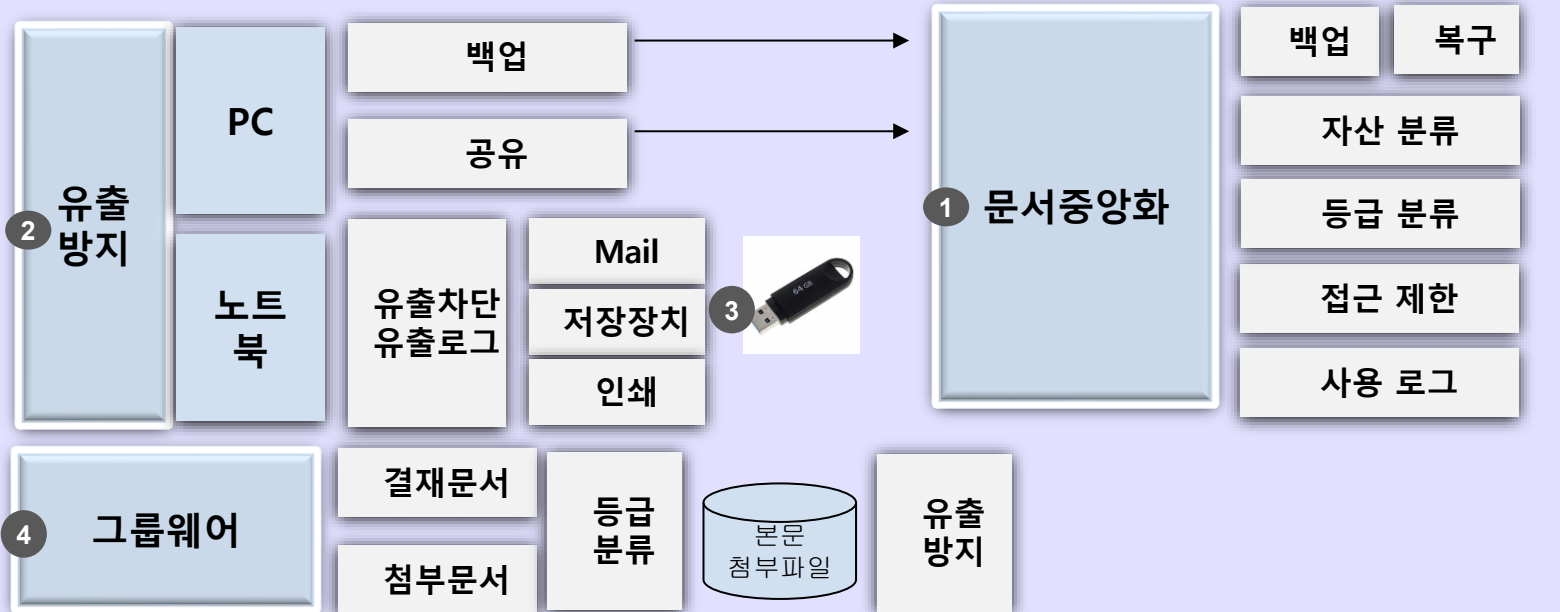
- ❖ 네트워크 침입에 대한 보안
- ❖ 파일서버등 내부 정보자산에 대한 보호
- ❖ 방화벽/UPS

# 6. 보안관리 방안

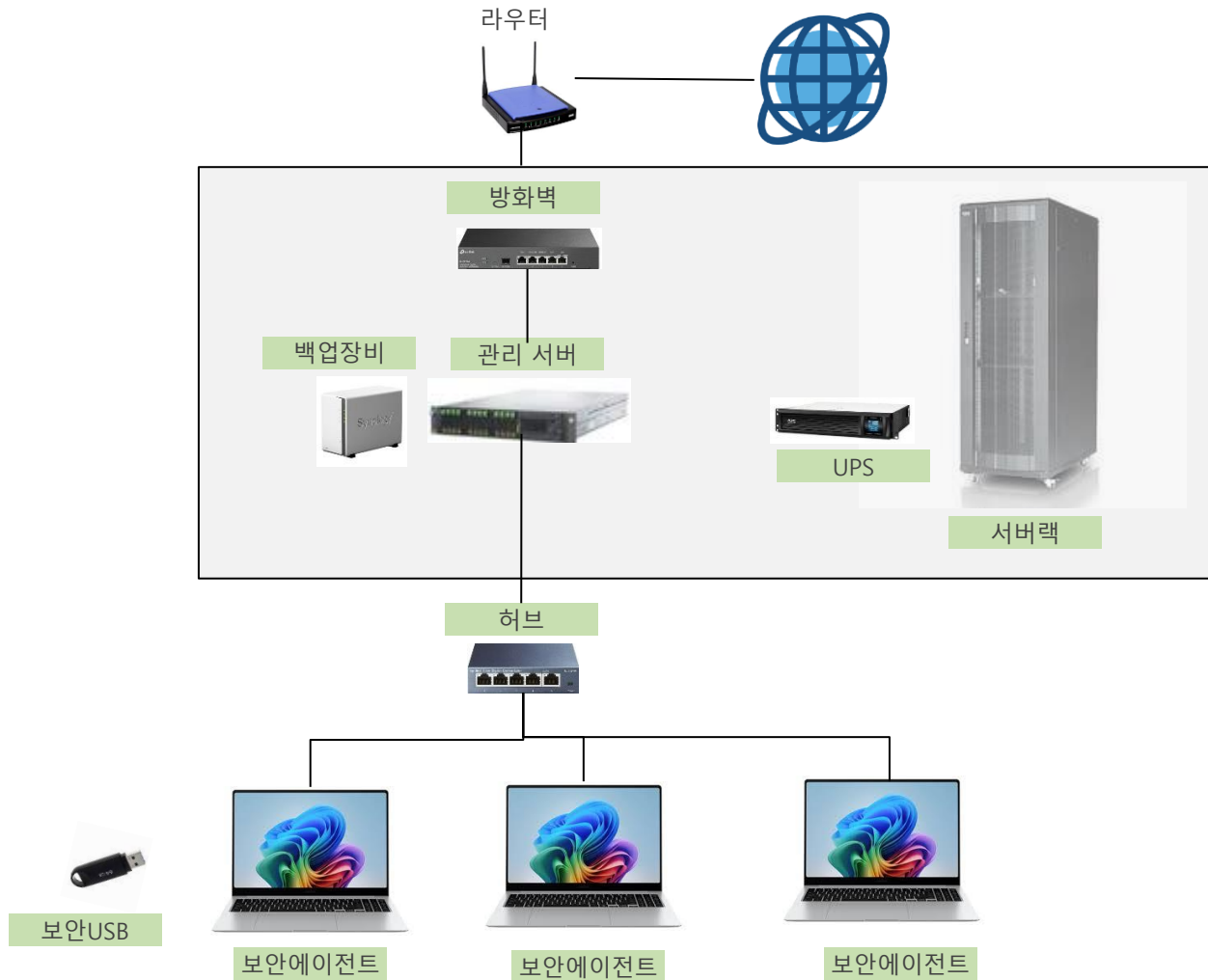
## 권고 내용

- 1 문서증양화
  - 개인PC 파일 백업
  - 파일 공유
- +
- 2 정보유출방지
  - 외부로 파일의 유출을 방지
  - 노트북 사외 반출후 유출방지
- +
- 3 보안USB
  - 개인 휴대용 저장매체 사용 제한
  - USB분실시 파일 유출(노출)방지
- +
- 4 그룹웨어 연동 보안
  - 결재 문서/첨부 파일 유출방지
  - 개인 PC에 파일 저장 최소화

## 구축방법



# 7. 보안시스템 구축 방안



# 8. AI 사용시 보안사항



## Input

- 내부 문서, 고객정보, 소스코드, 도면, 기술자료, 비밀번호, API Key 입력 또는 Upload
- 개인정보/회사 보안자료 유출

## Output

- 잘못된/조작된 정보 생성
- 저작권 침해 데이터 포함
- 외부 URL 포함 / 피싱 위험
- 개인정보 재노출
- 오류가 포함된 Source Code 사용

## 설정

성능개선

서버  
저장금지

