

03 웹 GUI 구성 보고서



진행 상태

읽기 전

Lockument Portal v1.5.0 (Demo) — 웹 GUI 공식 보고서

문서 상태: 초안(Draft) · 제품 상태: 데모(기능 제한/목업 데이터 포함)

대상: 교수진/의사결정자, 팀원, 향후 개발 참여자

작성일: 2025-09-05

0. 문서 개요

- **목적:** Lockument 포털의 웹 GUI(데모)의 배경·목표·구성·주요 기능·운영정책 제 3자가 이해하기 쉽도록 정리
- **용어**
 - *PII*: 개인식별정보(이메일, 연락처, 이름(성명 중 이름), 주민등록번호 등)
 - *Mask*: 문서 내 PII 마스킹(가림)
 - *Encrypt/Decrypt*: 파일 단위 암호·복호화
 - *Guest/User/Admin*: 미인증/일반사용자/관리자 역할

1. 배경

- **국내 유출 동향:** 2024년 유출신고 307건, **해킹 56%, 업무 과실 30%**, 시스템 오류 7%로 집계됨. ([개인정보보호위원회·KISA '2024년 개인정보 유출 신고 동향'](#)) www.pipc.go.kr경향신문
- **사례**
 - 통신사 대규모 유출에 **과징금 68억 원** 등 처분. ([LGU+ 사건, 개인정보보호위원회 보도자료](#)) www.pipc.go.kr
 - **이메일 오발송**으로 개인정보 유출 사례. ([LH, 2023.10.17 보도](#)) [MunhwaDaum](#)

- 대규모 내부 반출형 유출의 대표 사례가 존재(카드 3사, 2014). (*동아일보 판례 정리*) [Donga](#)
- 시사점: 해킹 및 업무 과실 모두 상위 원인으로, **사전 통제**(업로드 단계 보호)와 **사후 추적**(감사·접근·암복호 이벤트 로깅) 체계를 동시에 갖춘 **문서 중심 보안 UX** 필요. (유출 원인 다변화 근거) www.pipc.go.kr

2. 목적

1. 사용자는 드래그&드롭만으로 문서를 올리며, **PII 마스킹/파일 암호화**를 간단히 선택 적용.
2. 권한자(업로더/승인자/관리자)는 본인이 보호 처리한 문서를 **원문 복원(복호화)** 가능(모든 복원 이벤트는 감사 기록).
3. 관리자는 **감사·접근·암호화 작업·이상징후**를 한 화면에서 조회해 **책임 추적성**을 확보.
4. 세션/역할 기반 통제, 알림(성공/경고/오류), **다국어(한·영)**를 포함한 운영 친화 UI 제공.

3. 범위 및 구현 목적

- 범위(데모):
 - GUI 플로우, 로깅·세션·알림, 업로드 화이트리스트 정책, 권한별 뷰, i18n(한·영)
 - 관리자 콘솔(감사/접근(IP·MAC)/암호화 작업/이상징후/사용자·정책 관리)의 **화면/상호작용**
- 비범위: 실제 PII 탐지 엔진·암복호·KMS·SSO/QR 인증 연계, 영구 저장소, SIEM 연동 (= 표현/목업 단계)
- 구현 목적: 실서비스 전 **상호작용 프로토타입**으로 UX 검증·요건 정제

4. 핵심 요약(Executive Summary)

- **드래그&드롭 업로드**: DOCX/PPTX/PDF/HWP/XLSX/CSV/TXT/RTF/ODT 등 주요 오피스 포맷만 허용, 이미지 등은 **친절한 거부 메시지**.
- **보호 모드 전환**: **마스킹 | 파일암호화 | 원문복호화** 즉시 선택.
- **권한자 복원**: “본인이 마스킹/암호화한 파일”은 복원 가능(모든 이벤트 **감사 기록**).
- **관리자 콘솔**: 감사, 접근(IP/**MAC** 포함), 암호화 작업, 이상징후, 사용자·정책 관리.

- **안정 레이아웃·다국어:** 한/영 전환 시에도 프레임 고정 및 줄바꿈/스크롤 처리로 **가독성 유지**.
- **세션/알림:** User 30분·Admin 10분 카운트다운, 임박 경고, 상단 중앙 **3초 이상** 토스트 알림.

5. 기능-목표-역할-결과 매핑

기능	사용자 목표	시스템 역할	결과(가치)
업로드 게이트(화이트리스트)	쉽고 안전한 등록	파일 확장자 검증·정책 적용	오발송/오첨부 감소
PII 마스킹	문서 내 개인정보 즉시 가림	PII 패턴 탐지→마스킹(데모 가시화)	유출 리스크 선제 차단
파일 암호화	파일 단위 보호	(데모 표기) AES-GCM 등	외부 반출/무단 열람 억제
원문/복호화	권한자 복원	수행자·시간·사유 로그	책임 추적성 확보
최근 문서 리스트	상태 한 눈에 파악	PII/보호/작업 아이콘 정렬	생산성·가시성 향상
활동 내역	최신 이벤트 확인	내림차순·스크롤	상황 인지
관리자 로그	거버넌스	Audit/Access/Encrypt/Anomaly	준법·사후분석
사용자/정책 관리	운영 통제	계정·정책 화면	운영 표준화
세션 타임아웃	장기 미사용 차단	카운트다운·임박 경고	계정 안전
알림(Toast)	즉시 피드백	3초 이상 표시	오류 감소
i18n	해외/내부 혼용 대응	고정폭·줄바꿈·스크롤	레이아웃 안정

업무 과실형 사고 대응 논리: 게시·동보발송·오첨부·오발송 등 세부 유형이 다수 보고됨 → 업로드 게이트와 마스킹 기본값, 감사 로그가 실무형 보호조치로 적합. (개인정보보호위 2024 '업무과실편' 카드뉴스) www.pipc.go.kr

6. 화면 및 동작 개요 (캡처 지점 표시)

6.1 헤더 인사 카드 (캡처)

- 로그인 사용자 **이름/소속/사번/역할**(영문: Org / Emp.No / Role)
- **현재 시각, 업로드/QR/설정** 아이콘

- 좌측 상단 **Lockument** 로고 클릭→홈(내 파일)

6.2 업로드 프레임 (캡처)

- "여기에 문서를 드롭하거나, 파일 탐색"
- 허용 확장자 안내(위) / 비허용 형식은 거부 메시지
- 상단 모드 스위처: **마스킹 | 파일암호화 | 원문복호화**

6.3 최근 문서 (캡처)

- 컬럼: 이름·형식·크기·수정일·보호·작업(아이콘 3×2 그리드)
- 긴 이름 자동 줄바꿈, 크기·수정일 폭 축소, 보호/작업은 가독성 우선

6.4 알림 (캡처)

- 상단 중앙 **3초 이상** 표시(성공/경고/오류 색상), 다건 시 순차/병렬 배치

6.5 사이드바 (캡처)

- **Files:** 내 파일/팀/네트워크
- **가이드 & 문서:** 사용설명서/기능 설명서/버전 정보(기본 접힘)
- **관리자 전용:** 감사 로그, 접근 이벤트(IP/MAC), 암호화 작업, 이상 징후, 사용자·정책 관리

6.6 관리자 콘솔 (캡처: 각 표 상단)

- **감사 로그(Audit):** 시간·행위자·파일·행위·결과·IP·위치·디바이스
- **접근 이벤트(Access):** 리소스·행위·결과·IP/MAC·지점/위치(긴 경로는 줄바꿈+가로 스크롤)
- **암호화 작업(Crypto):** ENCRYPT/DECRYPT/MASK, 상태, 소요, Key ID
- **이상 징후(Anomaly):** 심각도 배지(낮음/중간/높음)
- **사용자 관리/정책 관리:** 계정/정책 토글(데모는 표시용)

7. 보안·운영 정책(데모 시나리오)

- **인증과 역할:**
 - *Guest:* 열람 제한, 업로드 불가(로그인 유도)
 - *User/Admin:* 업로드 가능, 권한자는 자신이 보호 처리한 파일에 한해 복원 가능

- **세션**: User 30분 / Admin 10분, 임박(User 10분/Admin 2분) 시 가시적 경고 후 타임아웃 자동 로그아웃
- **QR/SSO**: QR 코드 60초 유효(데모 안내), 실서비스 연동 시 OIDC/기관SSO 고려
- **로그**: 업로드/마스킹/암·복호화/공유/다운로드/로그인 시도(성공·실패) 시각·주체·리소스 기록
- **파일 정책**: 지정 확장자만 허용, 미허용은 **정중한 안내 문구**
- **i18n**: 한·영 전환 시 프레임 고정폭, `overflow-x-auto` 와 줄바꿈으로 **영문 길이 이슈 방지**

8. 기대효과

- **사전 차단**: 업로드 단계에서 PII 마스킹·암호화 적용 → **2차 노출** 방지
- **책임 추적성**: 누가·언제·어디서(IP/MAC)·무엇을(파일)·어떻게(복호화/공유) 했는지 재현
- **규정 준수**: 기술·관리적 보호조치를 UI 레벨에서 내재화 → 사고 유형(해킹/과실) 동시 대응. (*유출 원인 통계 근거*) www.pipc.go.kr
- **운영 효율**: 한 화면에서 파일 현황·보호 상태·최근 작업·활동·감사 로그까지 확인

정량 KPI 제안

- 민감정보 포함 문서 **사전 보호율 ≥ 90%**
- 오탐/미탐 피드백 반영 후 **검출 정밀도 ≥ 95%**
- 무권한 복원 시도 **100% 차단**(로그 적재)
- 사용자 작업 3클릭 이내 완료 **≥ 85%** 케이스

9. 제약 및 리스크(데모 고지)

- 실제 **PII 탐지/암복호화/키관리**는 현재 **모의 처리(표현/로그)** 단계로, 상용 적용 시 **엔진·KMS·저장소** 연동 필요
- QR·SSO·감사 저장소·SIEM 연계 없음(데모)
- 브라우저/접근성 심화 검증·대용량 처리 최적화 미수행

10. 향후 과제(우선순위)

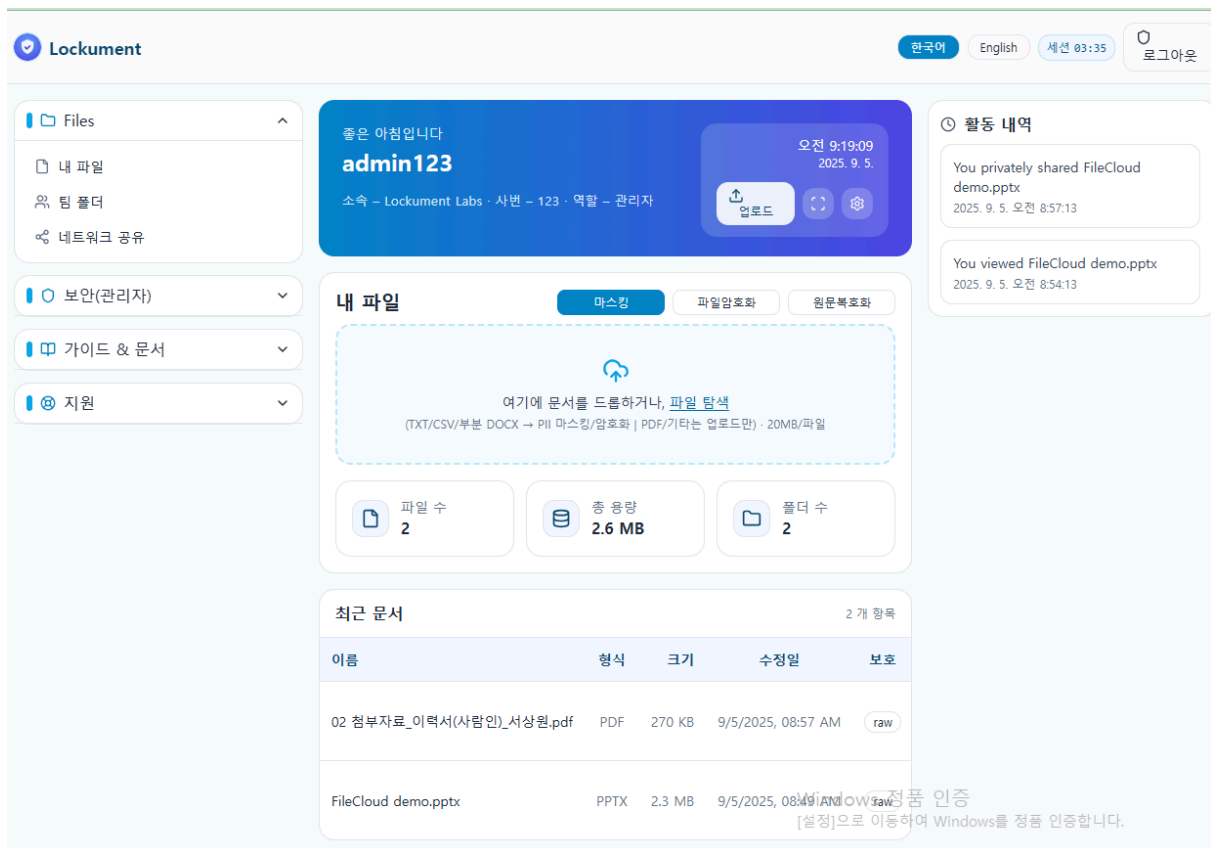
1. **엔진 연동**: 정규식+NER 기반 PII 탐지, AES-GCM 암복호화, 컨텍스트 필터, KMS

2. 인증: OIDC/기관SSO, QR 로그인(모바일 카메라/앱 연계)
3. 권한/정책: 부서/프로젝트/폴더별 RBAC, 예외 승인 워크플로
4. 감사 저장소: WORM 보관, SIEM 연계 대시보드
5. 접근성/반응형: 스크린리더 라벨, 키보드 내비게이션
6. 성능/안정성: 대용량 업로드·스트리밍, 지연·실패 복구 UX

11. 부록

11.1 캡처 체크리스트(보고용)

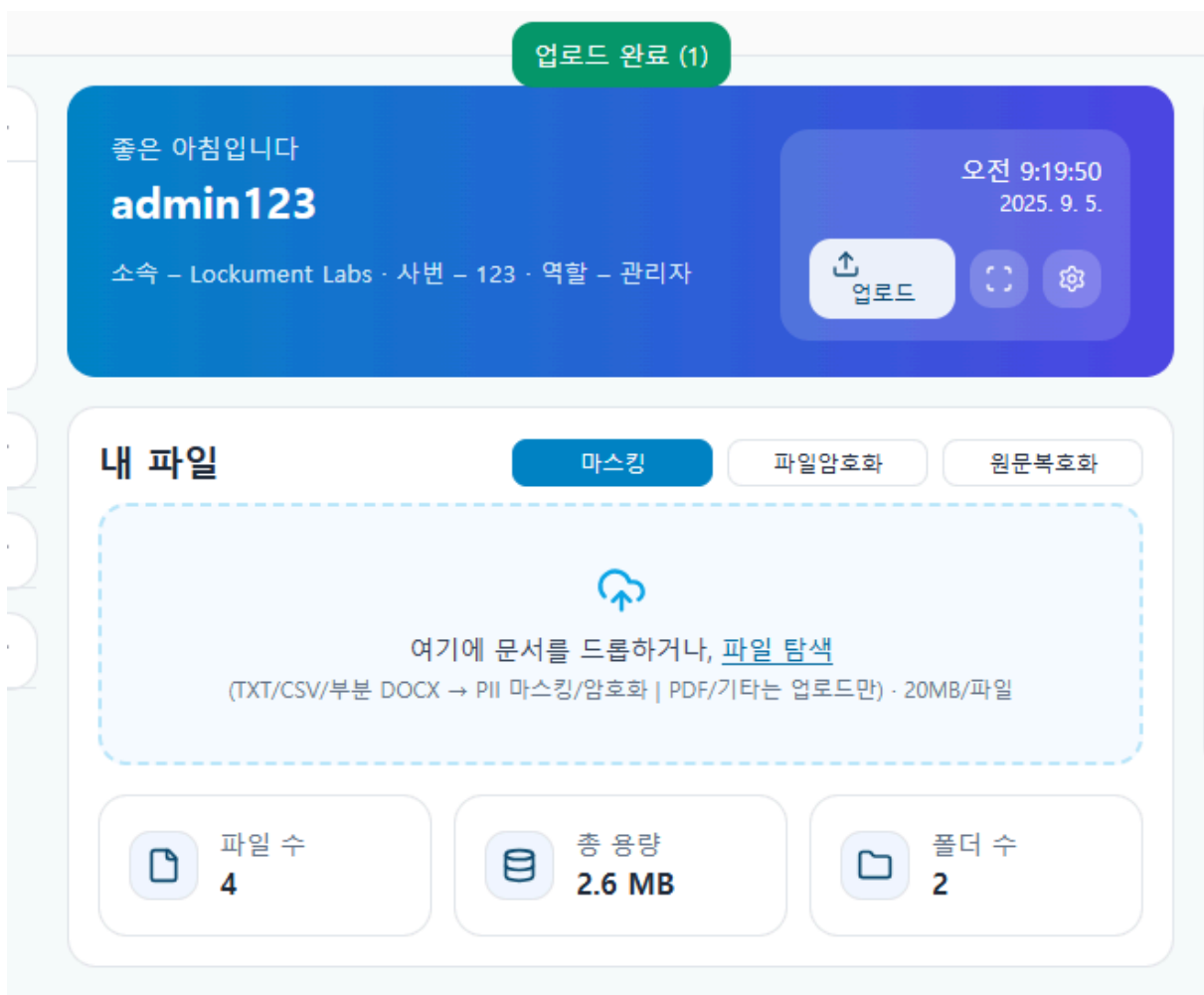
- (캡처) 메인 상단 인사 카드(소속/사번/역할/시간/아이콘)



- (캡처) 업로드 프레임 + 허용 확장자 안내



- (캡처) 알림(Toast) 성공/경고/오류 예시





- (캡처) 최근 문서 테이블(작업 아이콘 3×2 배치)



파일 수
7



총 용량
5.5 MB



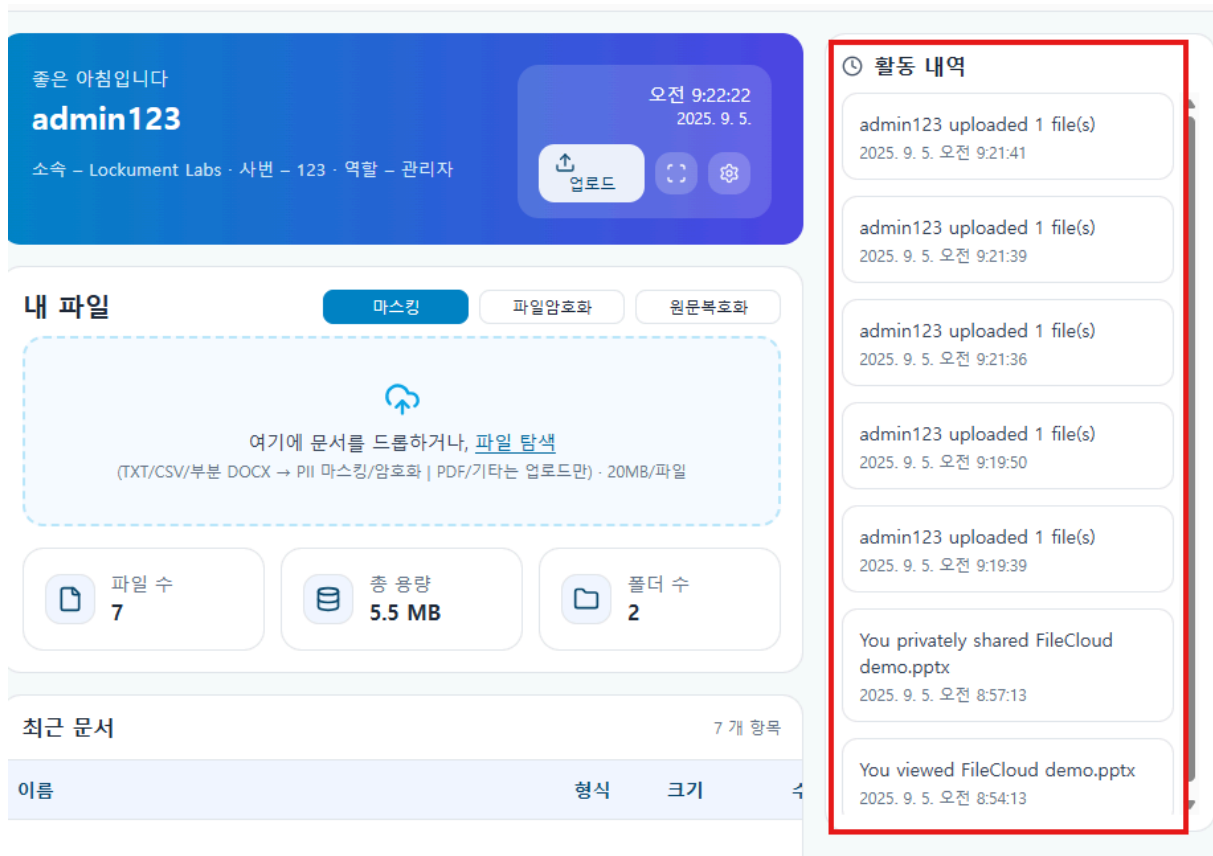
폴더 수
2

최근 문서

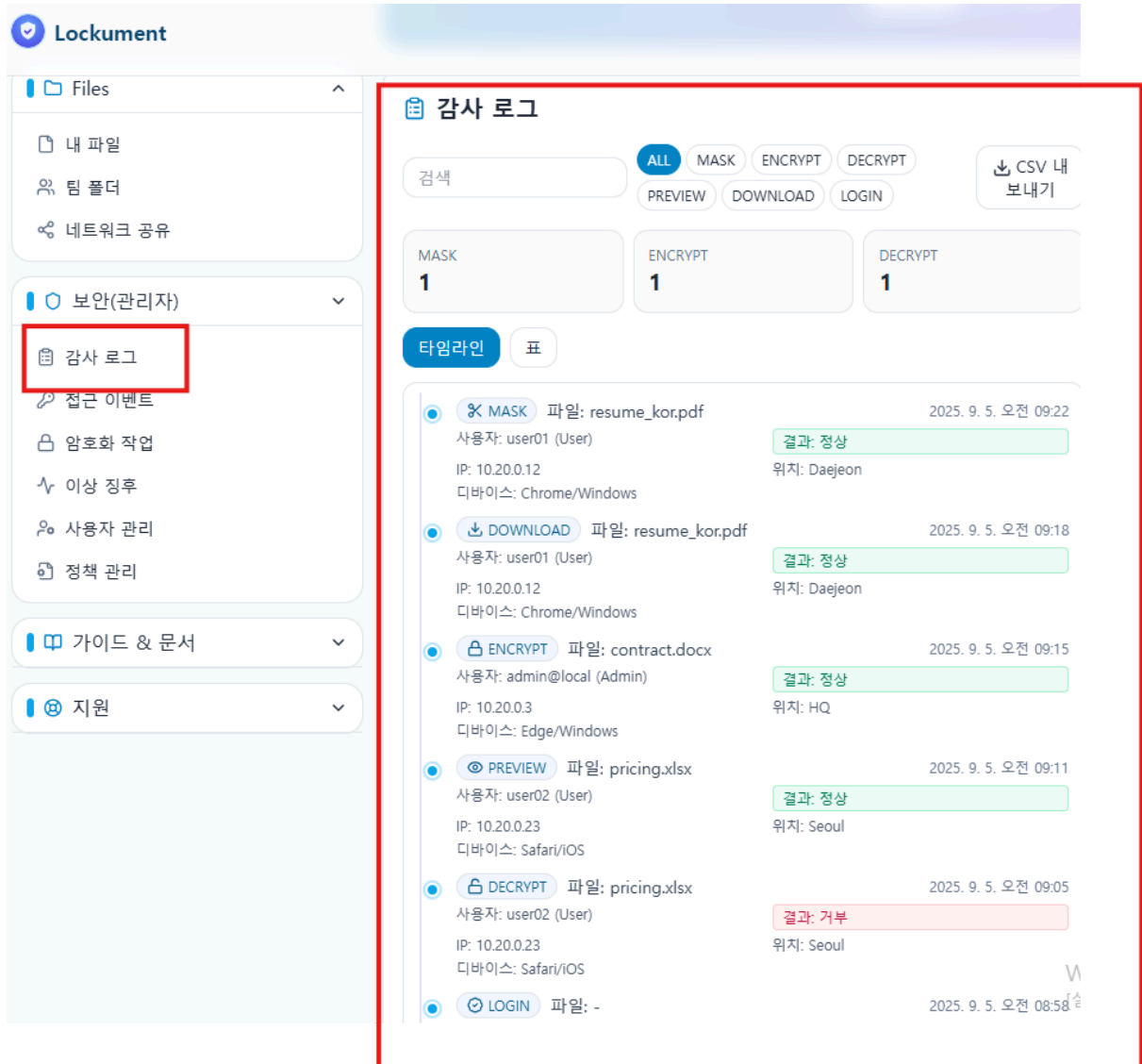
7 개 항목

이름	형식	크기	수
02_DB_구축_보고서.pdf	PDF	907 KB	9/5/202
01-1 부록_NIST Guide.pdf	PDF	808 KB	9/5/202
01 PII 구분_개인정보 유출사례 및 주요 PII 구분 조사_ver03.pdf	PDF	1.2 MB	9/5/202
To do list.txt	TXT	591 B	9/5/202

- (캡처) 활동 내역(스크롤)



- (캡처) 관리자: 감사 로그·접근 이벤트(IP/MAC)·암호화 작업·이상 징후·사용자/정책 화면



11.2 역할 정의(요약)

- **Guest:** 열람 제한, 업로드 불가(로그인 유도)
- **User:** 업로드(마스킹/암호화), **자신이 수행한 보호**에 한해 복원
- **Admin:** User 기능 + 감사·접근·암호화·이상징후·사용자·정책

11.3 참고 출처(문장 옆 이탤릭·대표 5건 이상)

- 개인정보위·KISA, 2024년 개인정보 유출 신고 동향(해킹 56%, 과실 30% 등) www.pipc.go.kr경향신문
- 개인정보위, LGU+ 유출 과징금 68억·과태료 2,700만 원(보도자료) www.pipc.go.kr
- LH, 이메일 오발송으로 개인정보 유출(언론 보도) MunhwaDaum
- 2014 카드 3사 대형 유출—판결/사후 정리(언론) Donga

- 개인정보위, 2024 '업무과실편' 카드뉴스(게시/오발송/오첨부 세부 유형)
www.pipc.go.kr
-

12. 결론

Lockument 포털 데모는 "업로드 시점 보호", "권한 기반 복원", "**"가시성/감사"**를 한 화면에 결합해 **현실적인 문서 보안 UX**를 제시합니다.

본 GUI 프로토타입을 기반으로 PII 엔진·암복호·KMS·SSO 등 백엔드를 단계적으로 연계하면, **실사용 가능한 보안 문서 포털**로 발전 가능합니다.