전사 문서 보호 및 스마트 업무환경 구축을 위한

ECM기반 문서중앙화 솔루션

2020년 2월

|주|애플소프트

CONTENTS

01 제안 배경

02 제안 목적

03 프로세스 및 시스템 구성도

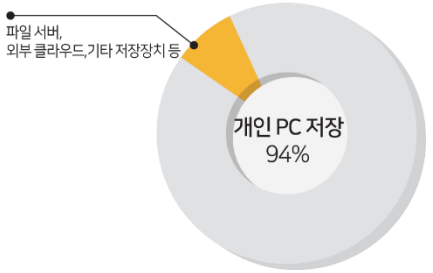
04 문서중앙화 주요 기능

05 개발사 소개

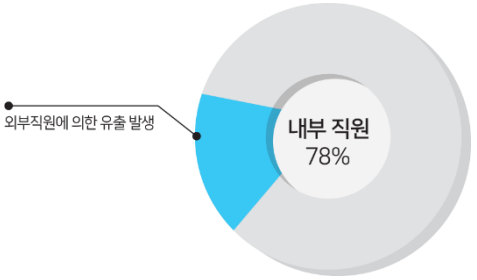
1.제안 배경

제안 배경 - 문서 관리 시스템의 부재로 인한 데이터 유출 발생

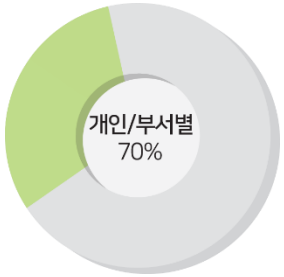
회사내 데이터 자산 관리 시스템 부재



· 회사 기밀문서를 개인 저장 장치에 보관하여 데이터의 유실 및 유출의 위험성이 높아짐



·현직 직원 27.1%
퇴사 직원 51.1% 로
퇴사시 회사 기밀문서를
악의적으로 유출



·전문 조직이나 시스템 없이
방대한 양의 데이터가
관리되고 있지 않고 있어
유출될 위험성이 높아짐

데이터 유출 현황

내부 사용자에 의한 핵심 기술 유출

- 고의적 또는 규정 미 준수에 의한 자료 유출 차단 대책 미흡
- 기업 내부자 소행에 의한 정보유출이 전체의 약78%
- 시스템적 대응을 통한 안정적 기업환경 유지 요구

정보통신기술적 취약 요소

- 고도화/ 지능화된 정보통신 기술 발달에 의한 취약 요소 지속적 증가
- 일반적인 문서보안 대응책 만으로는 유출 차단의 한계 발생 - 랜섬웨어, 악성코드 침입 등

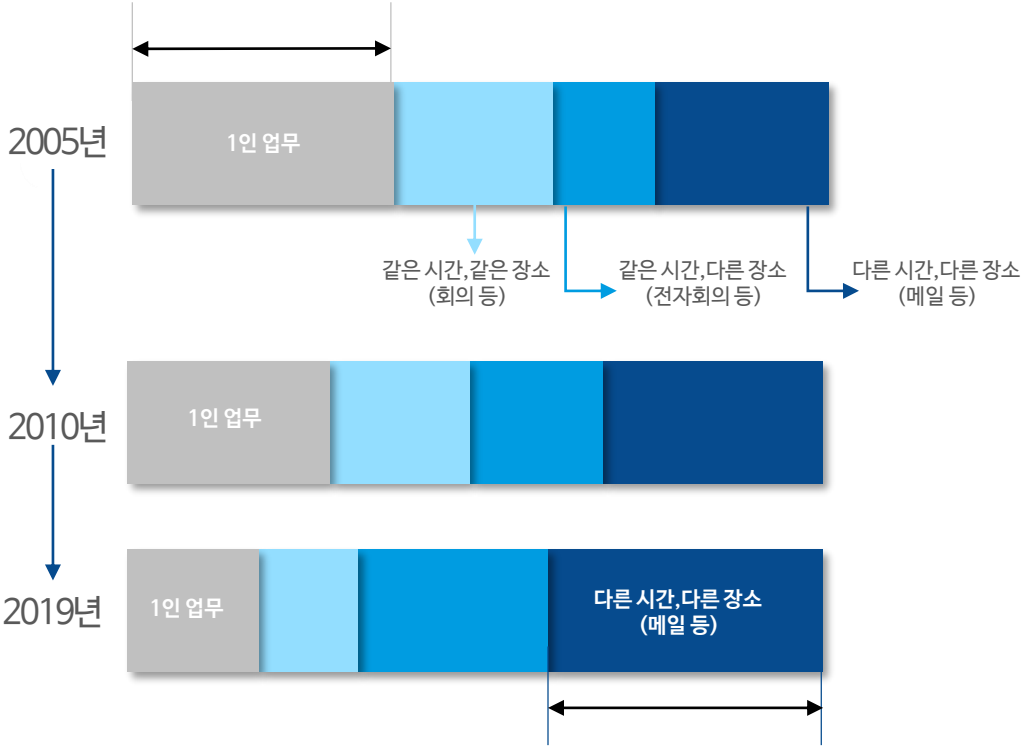
다양한 유출 통로에 의한 중요정보 유출

- E-Mail, 복사 등 다양한 경로에 의한 정보 유출
- 유출 시 피해 사실의 인지 곤란

제안 배경 - 협력사 간 공유 및 협업의 어려움

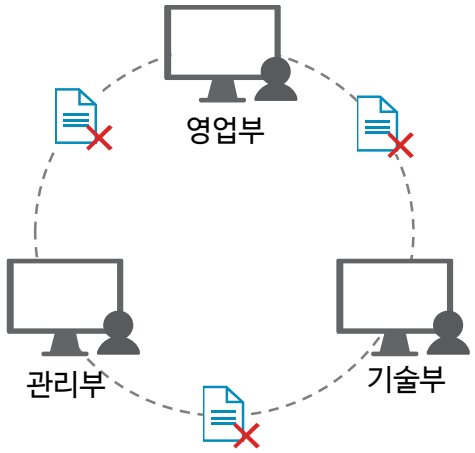
부서간의 장벽과 원활한 커뮤니케이션 부족으로 인한 중요 의사 결정의 지연, 효과적인 고객 서비스 대응 미흡 등의 문제로 조직 경쟁력이 약화됨

공유 & 협업에 의한 업무 추진 증가



시간이 흐를수록 창의적이고 효과적으로
업무를 수행할 수 있는 협업 환경(시스템) 필요

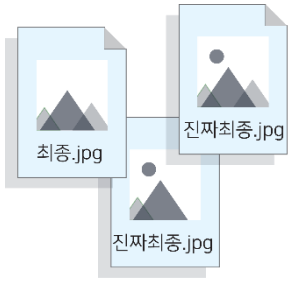
1. 정보 흐름 단절로 인한 부서간 업무 피드백과 대응이 원활하지 않음



〈 정보 흐름의 단절 〉

〈 업무 피드백과 대응 원활하지 않음〉

2. 버전 관리의 부재

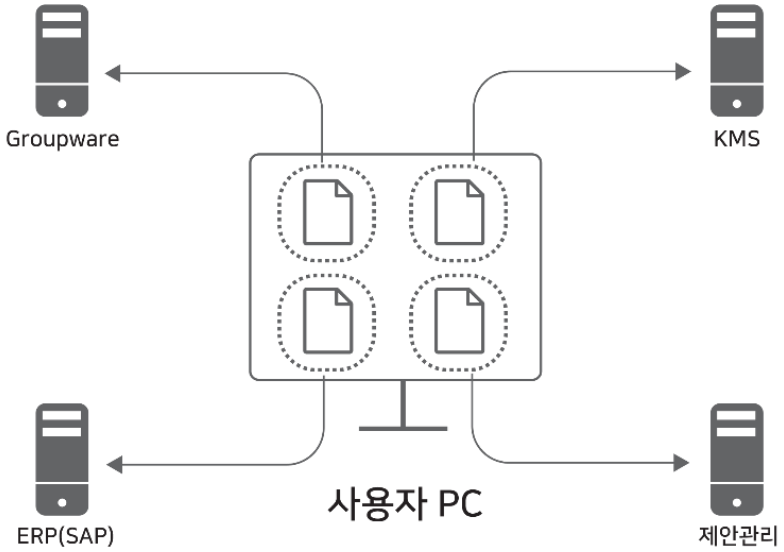


3. 원본 관리의 부재

제안 배경 - 기존 문서관리 시스템의 한계

사용자가 PC에 중요 문서를 저장하는 이유

조직 내 문서 자산 관리 시스템 부재



업무별 별도의 시스템 도입을 통하여, 사내 문서 자료 관리 진행

※문제점

① 업무별로 별도의 시스템 도입으로 인하여, 비용은 증가하고 관리의 어려움 또한 증가하는 현상이 발생한다.

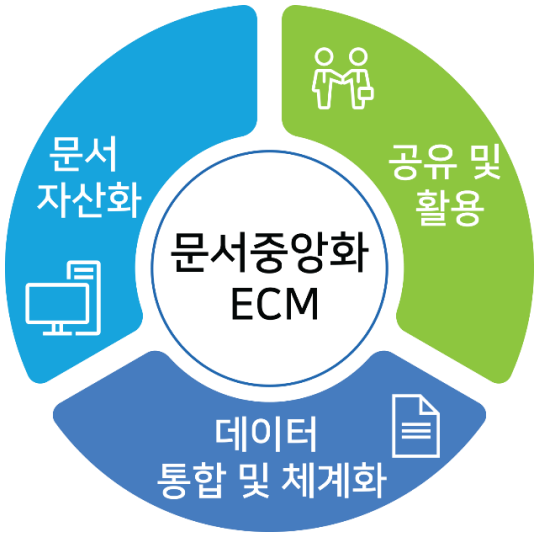
② 좋은 시스템을 도입한다고 하더라도, 사용자들이 사용하지 않아 계속 해서 위협이 존재한다.

2.제안 목적

제안 목적 – 문서 중앙화 구축 목적

사용자별 문서
생애주기 (생성-유통-폐기) 관리

개인 문서함 / 부서 문서함 통합 관리



문서 접근(읽기, 쓰기, 소유권) 권한
및 내용 검색 권한 정책 설정

공유한 파일/폴더 및 공유 받은
파일/폴더 정책 설정

전사 통합 내용 검색 기능으로
업무효율성 제고

로컬 하드드라이브 문서 저장 금지
및 유출방지 기능 제공

제안 목적 - 대내외 환경 분석

정보 자산에 대한 외부 유출 가능성을 원천 차단하여, 내부 사용자의 편의성을 증대한 솔루션의 도입으로 문서 보안 및 업무 편의성을 증대 하는 것이 문서중앙화를 제안하는 목적입니다.

AS-IS

현재 기업시스템의 현황

- 개인 PC내 존재하는 문서로부터 업무 정보 유출
- PC문서의 공유와 협업의 어려움 발생
- 문서 유통, 사용에 대한 관리 및 통제의 부재
- 문서에 허가되지 않은 사용자로 인한 유출 피해 발생

TO-BE

앞으로의 개선 방향

- 중요 문서 ECM등록 관리 및 통합 로그 관리
- 비정형 정보 통합관리를 위한 단일 저장소 구현 신속한 검색 환경 구축
- 생성, 유통, 배포, 폐기에 대한 이력 추적 관리
- 문서에 대한 접근통제 및 권한 부여 가능

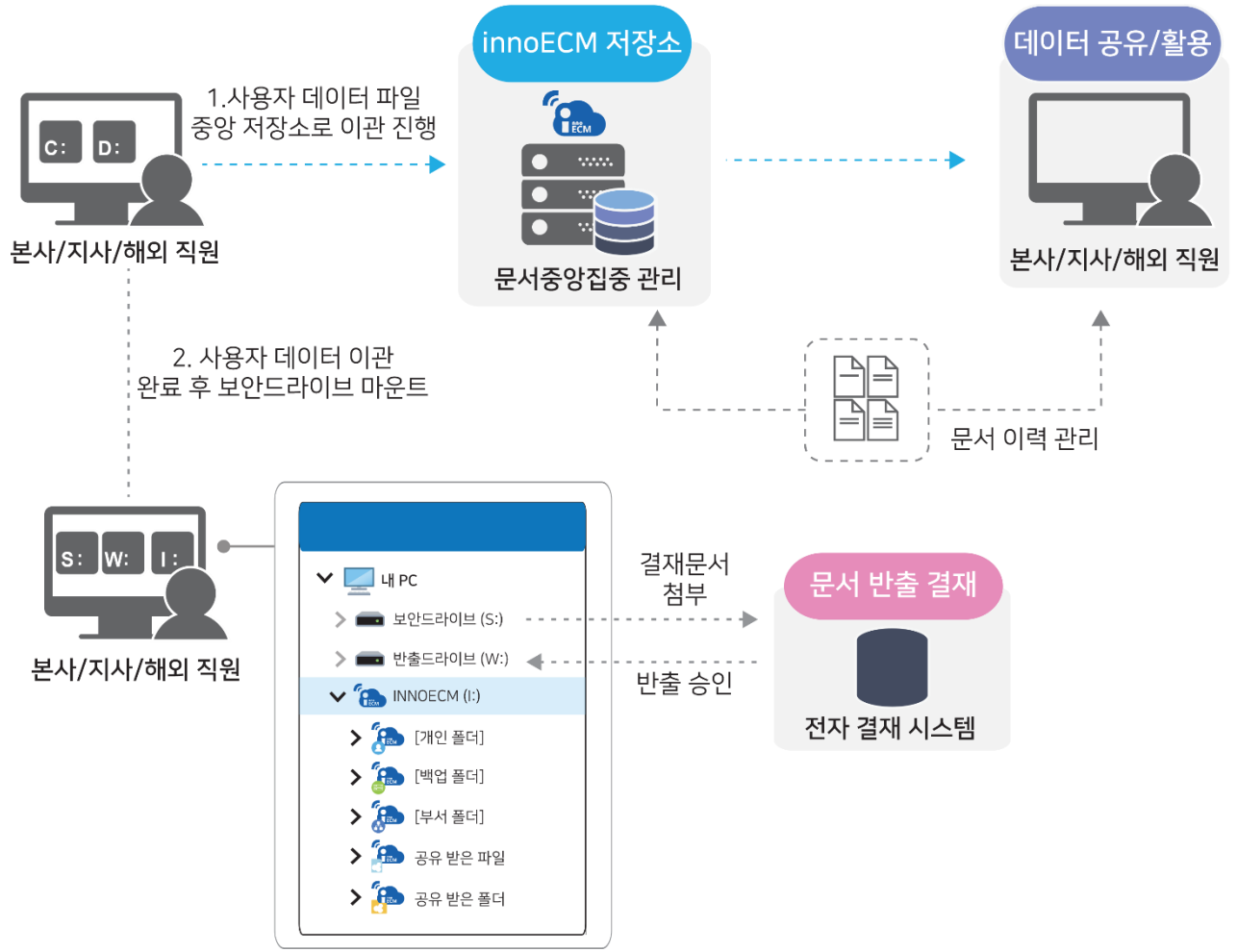
제안 목적 – innoECM 구축 범위

문서 중앙화 시스템을 통해 문서 협업/공유 뿐만 아니라 회사 내 데이터를 통합 관리 함으로써 기밀 데이터의 유실이나 유출을 방지할 수 있고,
체계적인 정책 수립을 통하여 사용자 PC의 데이터를 회사의 데이터로 자산화 할 수 있습니다.

3.프로세스 및 시스템 구성도

innoECM 프로세스

innoECM 관리 프로세스는 문서 업로드, 중앙 저장, 공유 & 활용, 반출/반입, 문서이력관리 등 필수적 프로세스를 정리하며 문서에 따라 전자결재 글로벌 공유와 같은 선택적 프로세스 또한 정립합니다.

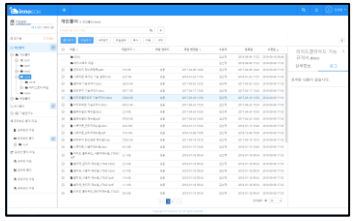


1. 데이터 중앙 저장 및 업로드
   - 개인 PC에서 문서 업로드 진행
   - 데이터 중앙에 강제 저장
2. 데이터 공유/활용
   - 본사/지사/해외 직원 데이터 공유&활용 통합검색 및 문서 이력관리 가능
3. 문서 반출/반입
   - 권한 관리 등 보안 보장 기반 문서 반출
   - 문서 반입 통제
4. 글로벌 공유
   - 국내&해외 등록 문서에 대한 공유 및 협업

innoECM 시스템 구성도

윈도우탐색기

+



WEB 브라우저

중앙화 시스템

개인 폴더

[개인 폴더]
- Junit
- test1
- test2
- test3
- test4

백업 폴더

[백업 폴더]
- sjkim
  - C
  - D
  - dst

부서 폴더

[부서 폴더]
- 기술연구소
  - test

협업 폴더

- 공유 받은 파일
- 공유 받은 폴더

문서자산화

개인문서	부서문서	협업문서	백업문서
• 파일추가 • 파일내려받기 • 파일버전관리 • 파일공유 • 파일분류	• 문서분류 • 파일공유 • 파일권한관리 • 파일버전관리 • 소유자변경	• 공유승인/거절 • 공유삭제 • 공유받은폴더/파일 • 공유한 폴더/파일 • 공유승인폴더	• 파일보안관리 • 파일버전관리 • 파일암호화 • 기간검색 • 결과공유요청

문서활용	권한/보안	통합검색	시스템관리
• 분류조회 • 부서/개인별검색 • 삭제/이동/편집/복사 • 다운로드 • 소유권이전	• 백업문서보안 • 파일소유권한 • 사용자별문서보안	• 부서/개인별검색 • 제목검색 • 내용검색 • 기간검색 • 결과공유요청	• 사용자/부서/역할/저장소관리 • 폴더/파일권한관리 • 휴지통관리 • 로그관리

보안/암호화 | 접근권한통제 | 모니터링(통계) | Repository관리

생성 → 유통 → 보관 → 활용 → 이관 → 폐기

InnoECM Framework

컨텐츠통합저장소

개인문서 | 부서문서 | 백업문서 | 협업/공유자료 | …… | 결재문서

Index DB | Content DB

일반문서 등록 | 백업 대상파일 | 사용자 /조직정보 | 통합검색

연계: PC파일저장 | 보안백업 | 인사조직 | 통합검색

통합검색 → 조회/검색/활용 → 일반사용자

전사함분류/ 문서관리 → 관리/운용 → 시스템관리자, 시스템운영관리

4.innoECM 주요 기능

innoECM 주요기능

부서간 문서 공유 · 협업

- 사용자 중심의 인터페이스 제공
- 웹브라우저와 윈도우 탐색기 기반으로 문서 공유 환경 제공

문서 접근 권한 · 보안 관리

- 폴더/파일 권한 사용자별 접근/검색 통제
- 폴더/파일 권한 그룹별 문서 접근/검색 통제
- 내/외부 반출 통제 및 이력관리
- 외부 반출 승인/결재
- 랜섬웨어 차단

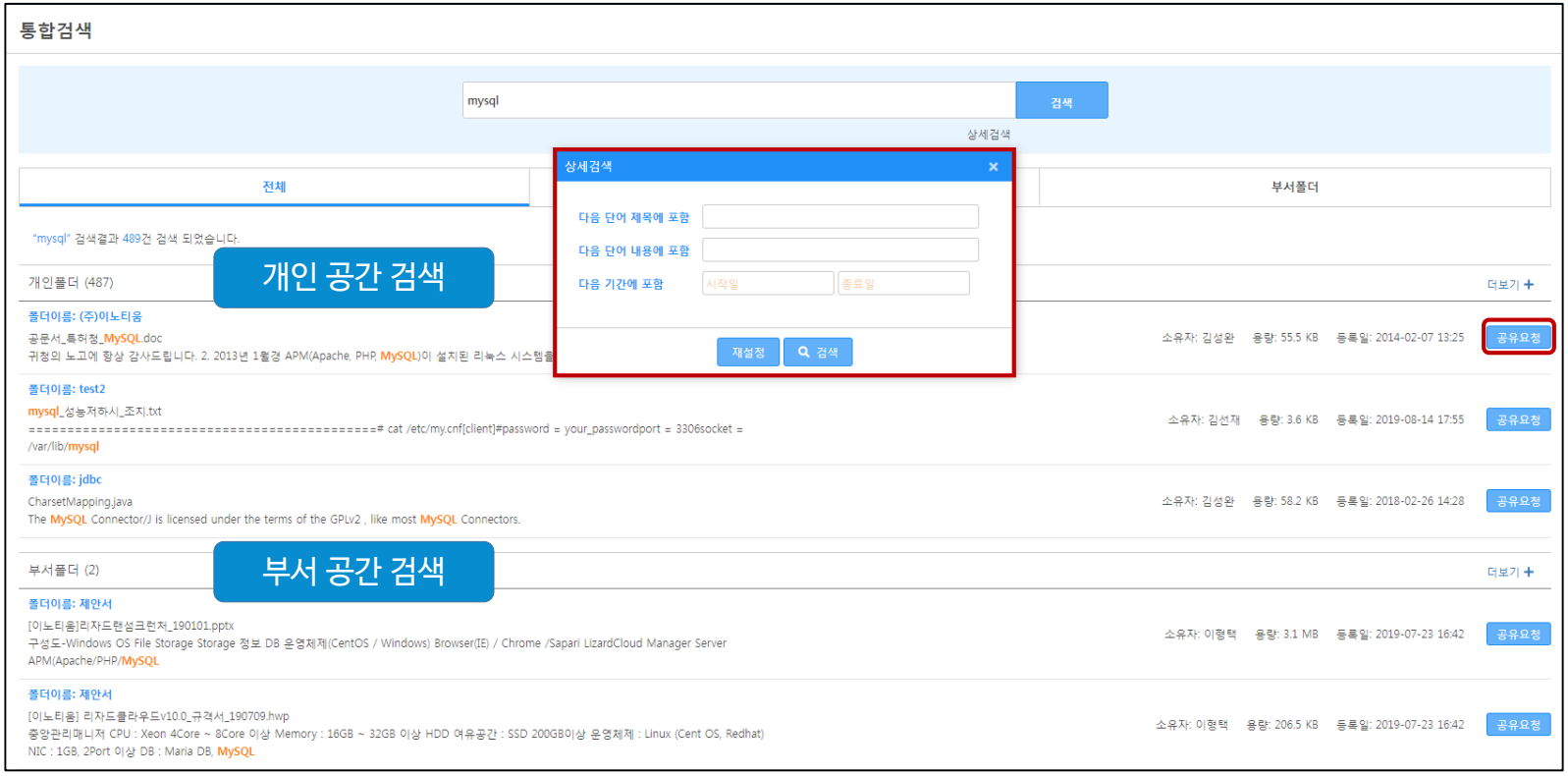
사내 문서 통합 관리

- 표준화된 문서 통합 관리
- 문서 관리 현황 통계
- 문서관리 실시간 모니터링 (부서/개인별 문서 등록/조회 현황)

전사 문서 내용 검색

- 사내 문서의 활용성 증대
- 문서 파일의 내용 검색 지원
- 열람 요청을 통해 검색된 타 부서의 문서에 대한 자료 공유

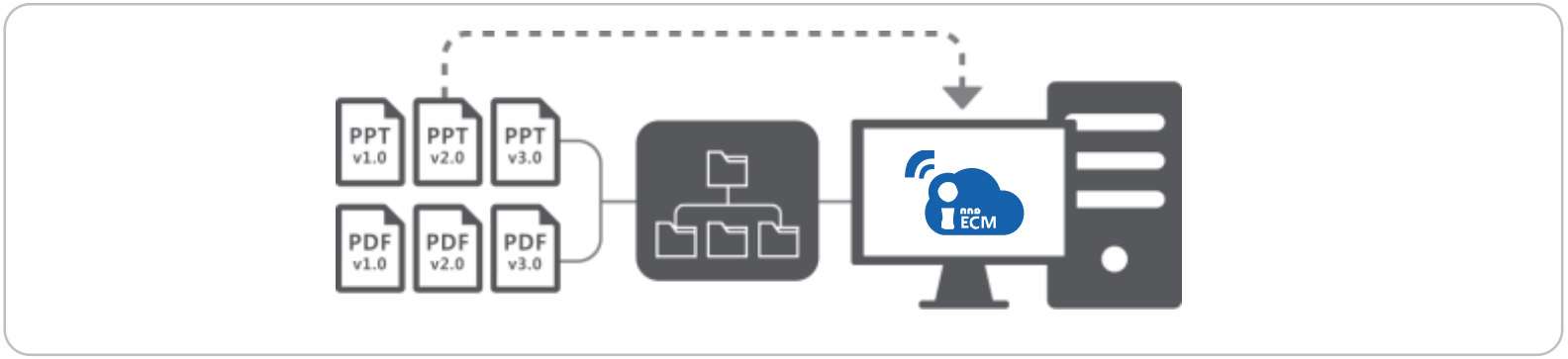
검색기능

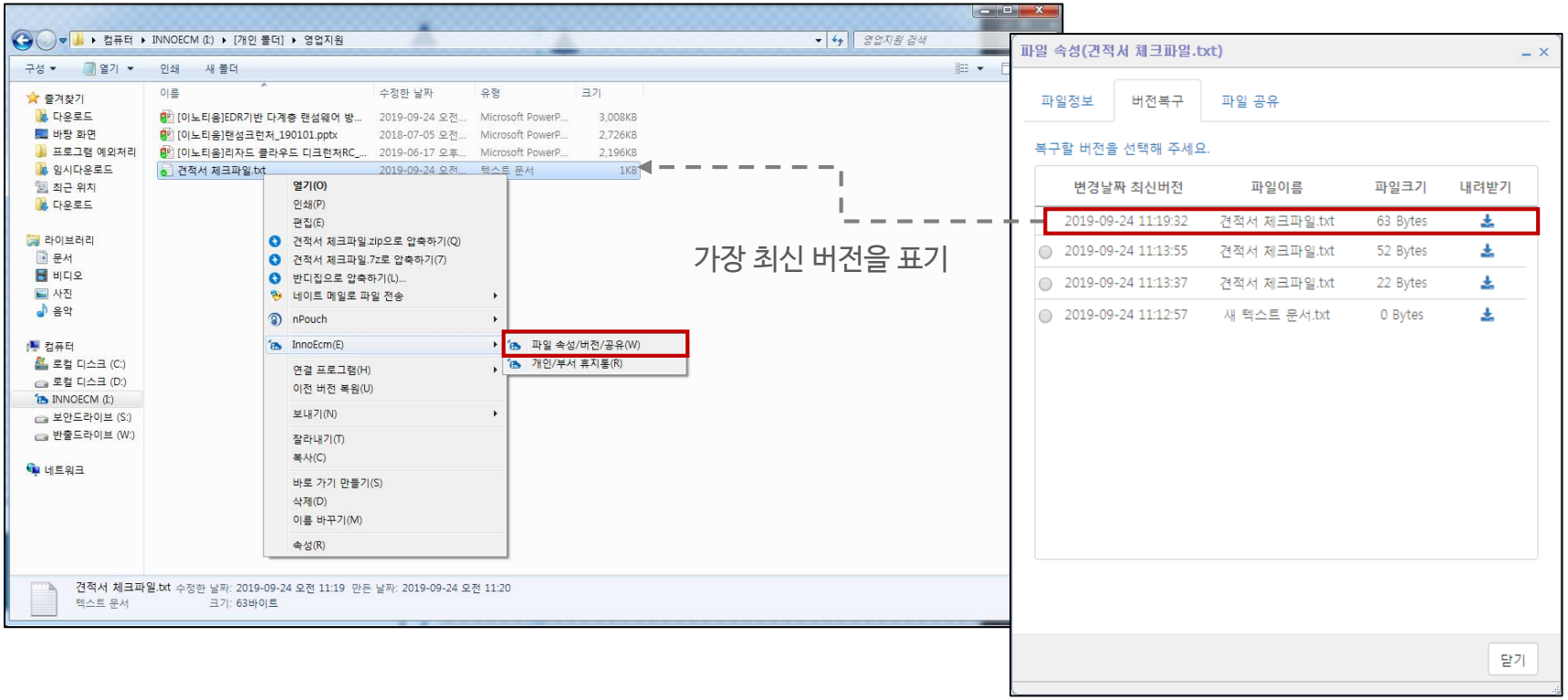


- 키워드 검색 및 문서 정보에 의한 상세검색 기능 제공, 문서의 접근권한에 따라 권한 있는 문서만 검색 결과 노출
- 검색된 파일은 공유 요청을 통해 개인 폴더에 있는 파일이 아니더라도 사용이 가능
- 검색은 개인, 부서, 전사 검색이 가능하나, 기밀문서는 검색에서 제외되고 상세검색을 통해 기간 혹은 제목 내용을 포함 하거나 제외하여 검색할 수 있습니다.
- 검색기능을 통하여 중앙화 문서 빅데이터 분석을 하거나 활용 가능합니다.

문서 버전 관리

innoECM은 문서의 버전관리 기능을 제공하여 협업 진행 시 초기버전에서 현재버전까지의 모든 변경 내용을 이력으로 관리합니다.





문서 접근 권한 관리(1/2)

기업의 보안 및 업무 지침에 따라 각 문서 단위별로 조직 및 사용자에 따른 접근 권한 체계 수립

사내 보안 지침 및 업무 지침

· 원칙적으로 문서는 공유가 가능하도록 하여 시스템의 정보를 최대한 활용함

· 보안이 필요하거나, 비인가된 수정, 삭제로부터 보호해야할 문서에 대해 권한 설정

문서등급별

- 기밀 문서
- 대외비
- 일반 문서
- 전체 공개
- 그룹 공개

+

문서권한별

- 읽기 권한
- 생성 권한
- 삭제 권한
- 편집 권한
- 편집 취소 권한

문서 접근권한 적용방안

① 접근 권한에 의한 검색 범위 통제

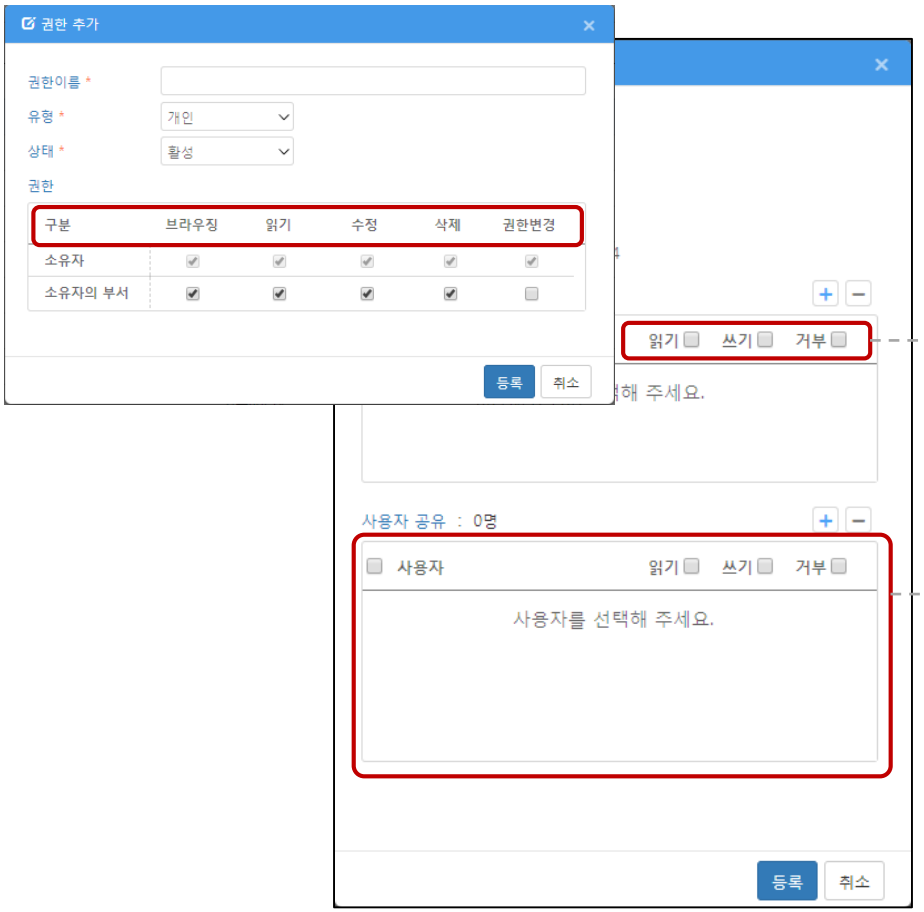
② 사용자/그룹별로 문서의 권한 설정 기능

③ 시스템 관리자 접근 계정 통제

④ 사용자 퇴사 및 부재 시 위임 설정 기능 제공

⑤ 권한이 없을 경우 문서의 소유자 또는 관리자에게 권한 요청 기능 제공

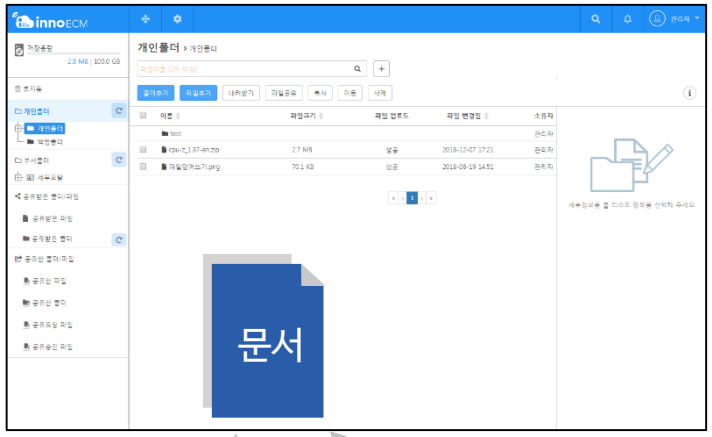
문서 접근 권한 관리(2/2)



읽기 : 파일 다운로드 가능(파일 수정 불가능)
쓰기 : 파일 수정 가능
거부 : 파일 접근 권한 없음

부서에 포함되어 있는 사용자 중
읽기/쓰기 권한을 전부 부여 하지 않을
경우에 사용자를 추가하여 거부 권한을 부여하면
해당 폴더 및 파일에 접근 권한이 없음

문서 접근 권한 적용



① 팀 폴더 생성

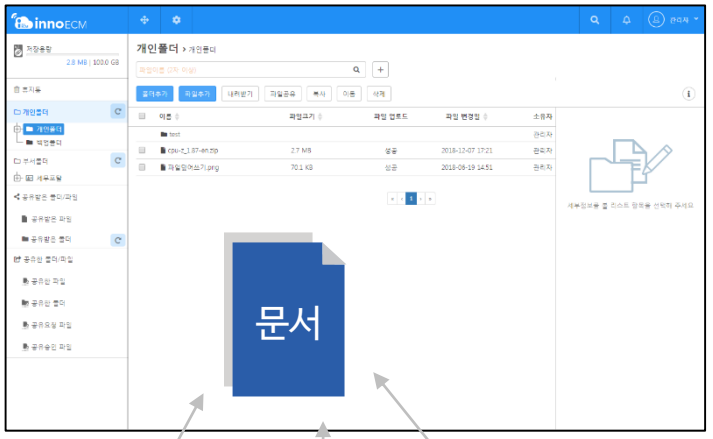
② 팀 폴더에 문서 생성

③ 문서 접근 가능

팀(부서) 기본 권한 설정

< A >

< B >



① 같은 팀원인 C에게

"문서 " 대한 접근 제한

② 접근 권한

미소유로 확인 불가

문서 관리자

문서 접근 가능

< A >

문서 접근 불가능

< C >

문서 라이프 사이클 관리

innoECM은 전자문서의 통합 자산화로써 사용자별 문서의 생애주기(생성 - 유통 - 폐기) 관리 입니다.

▶ 문서 접근 통제

- 역할 범위 통제
  - 계정별 역할에 따른 접근 범위 통제
- 다양한 방식의 접근권한 체계 제공
  - 문서보안등급 및 권한에 따라 문서 접근 및 수정, 삭제 통제

▶ 랜섬웨어 차단 및 암호화

- 화이트리스트 기반 방식 아키텍처
  - 랜섬웨어 등 악성코드 침입 원천 차단
- 저장소 암호화 (AES256)
  - 불특정 하게 생성되는 임의의 폴더에 파일이 암호화되어 저장

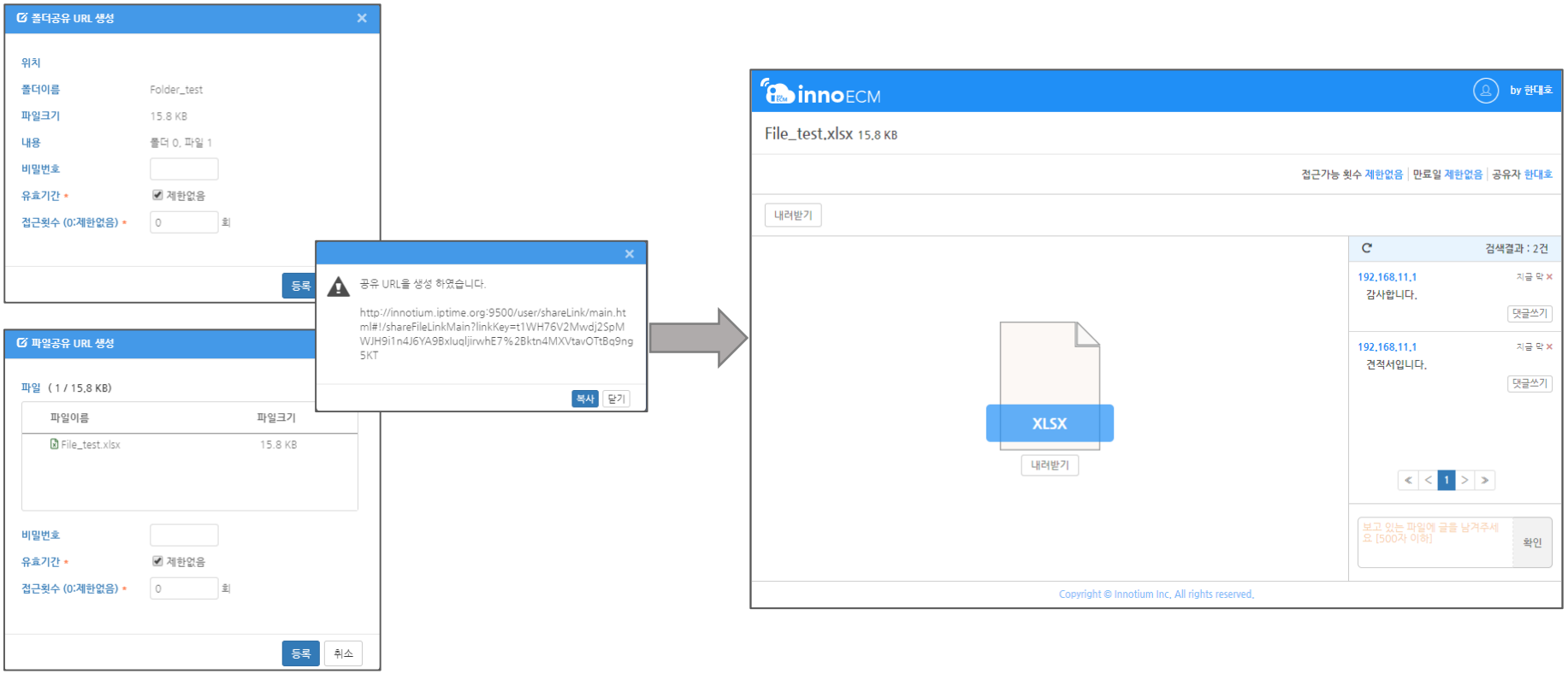
▶ 이력관리 및 백업

- 사용자 행위 감사
  - 문서, 폴더, 권한, 사용자 등 모든 자원에 대해 이력 관리
- 정보 자산에 대한 백업 환경 구축
  - 스토리지 이중화 / 백업 정책 수립

▶ 통합 검색

- 통합 검색 기반 빅데이터 분석 및 활용
  - 키워드 검색 및 문서 정보에 의한 상세 검색 기능 제공, 문서의 접근 권한에 따라 권한 있는 문서만 검색 결과 노출

내/외부 공유 URL

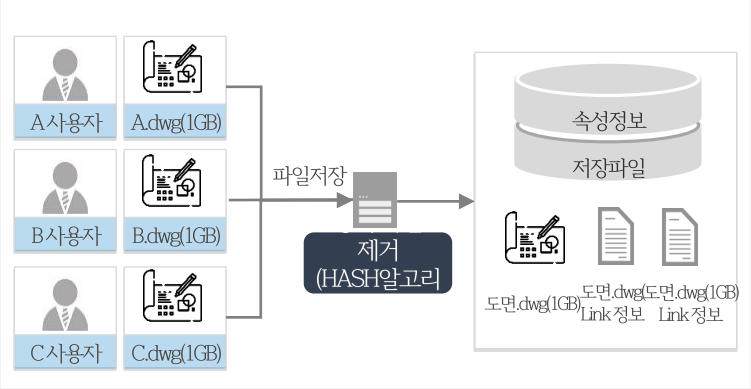


- 내/외부로 공유할 수 있는 URL을 생성하여 파일 및 폴더 공유가 가능합니다.
- 비밀번호/유효기간/접근횟수를 통해 데이터가 유출되는 일을 방지합니다.
- 공유받은 URL로 접속하면 파일에 대한 정보가 나오며 댓글을 통해 효율적인 협업이 가능합니다.
- 생성된 공유 URL에 대한 로그가 남기 때문에 관리가 가능하며, 원클릭으로 해당 파일에 대한 접근 권한을 해제할 수 있습니다.

문서 저장/반출 통제 및 중복 제거

전자문서 생성 및 유통량이 매년 150~200% 증가하고 있기 때문에 보안 파일 서버 스토리지 상에서 문서중복 제거하는 기술은 반드시 필요합니다.

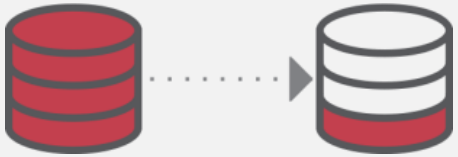
중복제거 프로세스



※실시간 중복 제거

- 동일문서 편집 후 저장 시 중복체크를 통해 서버에서 자체 복제 기능 수행
- 문서중앙화에 저장된 모든 파일 대상으로 중복 파일 모니터링 현황 제공

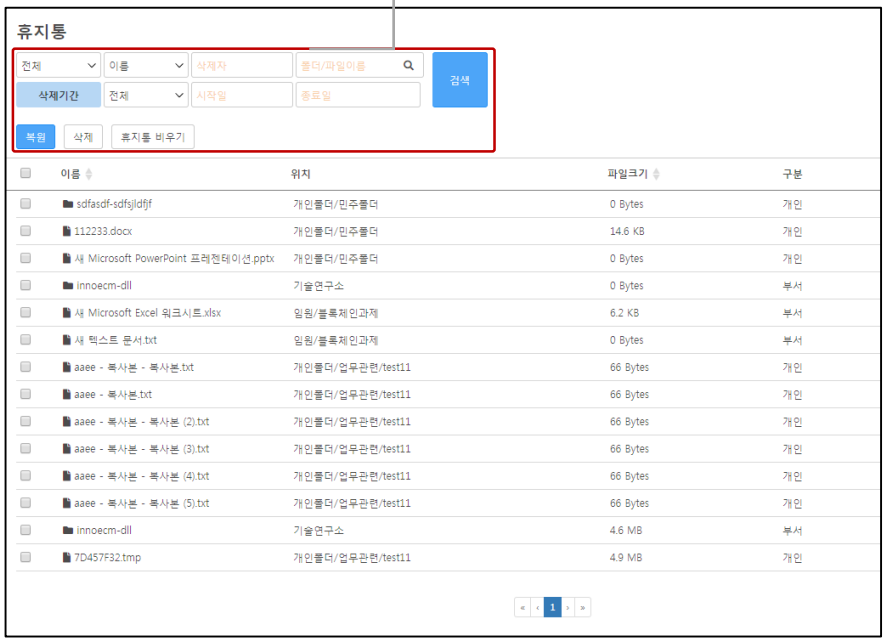
문서 중복제거 효과



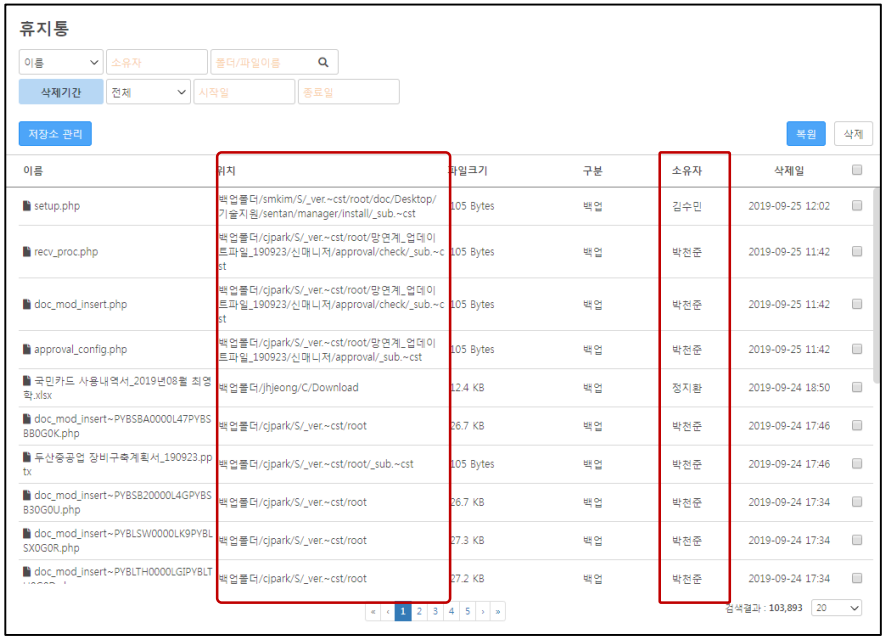
- 디스크 증설비용을 최소화하고 시스템 가용성을 최적화 유지
- SHA256를 이용한 파일 해시값을 사용해서 중복파일은 서버에 저장하지 않음

휴지통 관리

삭제된 폴더 및 파일 중 찾고자 하는 파일의
이름이나 기간을 설정하여 검색할 수 있습니다.



〈 사용자 〉



〈 관리자 〉

- 폴더 및 파일에 대해서 삭제한 항목은 개인 휴지통으로 이동됨
- 휴지통에서 삭제한 폴더 및 파일을 다시 복원할 수 있으며, 휴지통 비우기 및 삭제를 통해 휴지통의 내용을 관리자 휴지통으로 이동하기 기능 제공
- 사용자 휴지통에서 파일이 삭제되었다고 하더라도, 최종적으로 관리자 휴지통으로 이동하기 때문에 파일이 필요한 경우에는 관리자 휴지통에서 복원 가능

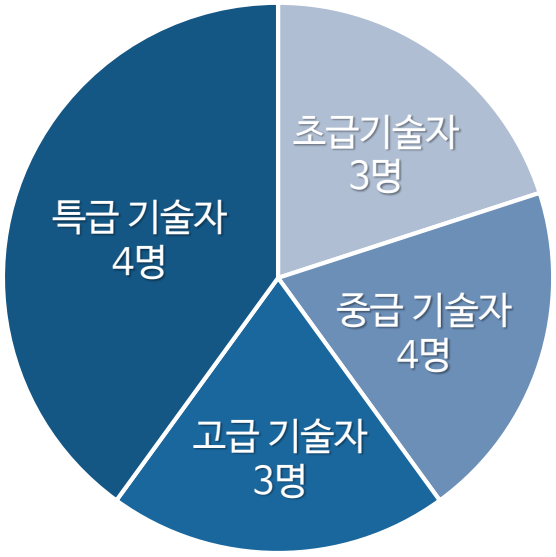
5.개발사 소개

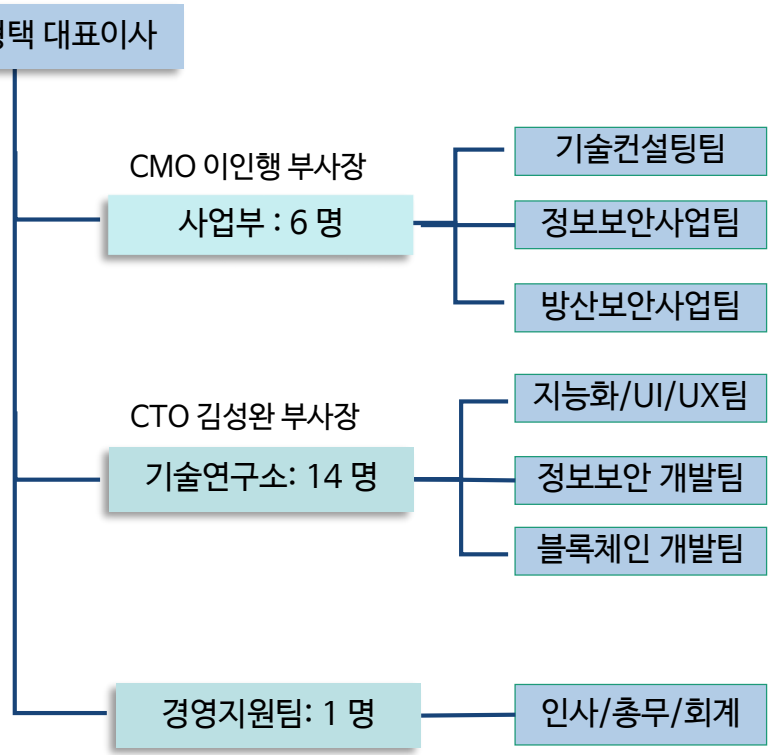
이노티움 개황

회사명	(주)이노티움 / Innotium Inc.
대표자	이형택 (010-6239-2764, htlee@innotium.com)
홈페이지	T: 02-3283-2021 F: 02-3283-2015 A:서울시 구로구 디지털31길 20, 301호
설립일	2010년 1월 7일
영위사업	-랜섬웨어 방어 사전차단/보안백업SW, 문서보안관리 SW, 반출문서 유출방지/추적관리 SW, 블록체인 플랫폼SW -한국랜섬웨어침해대응센터 운영 -리자드방산보안지원센터 운영

개발자 보유 현황

(2020년 2월 기준, 단위: 21명)





이노티움 연혁

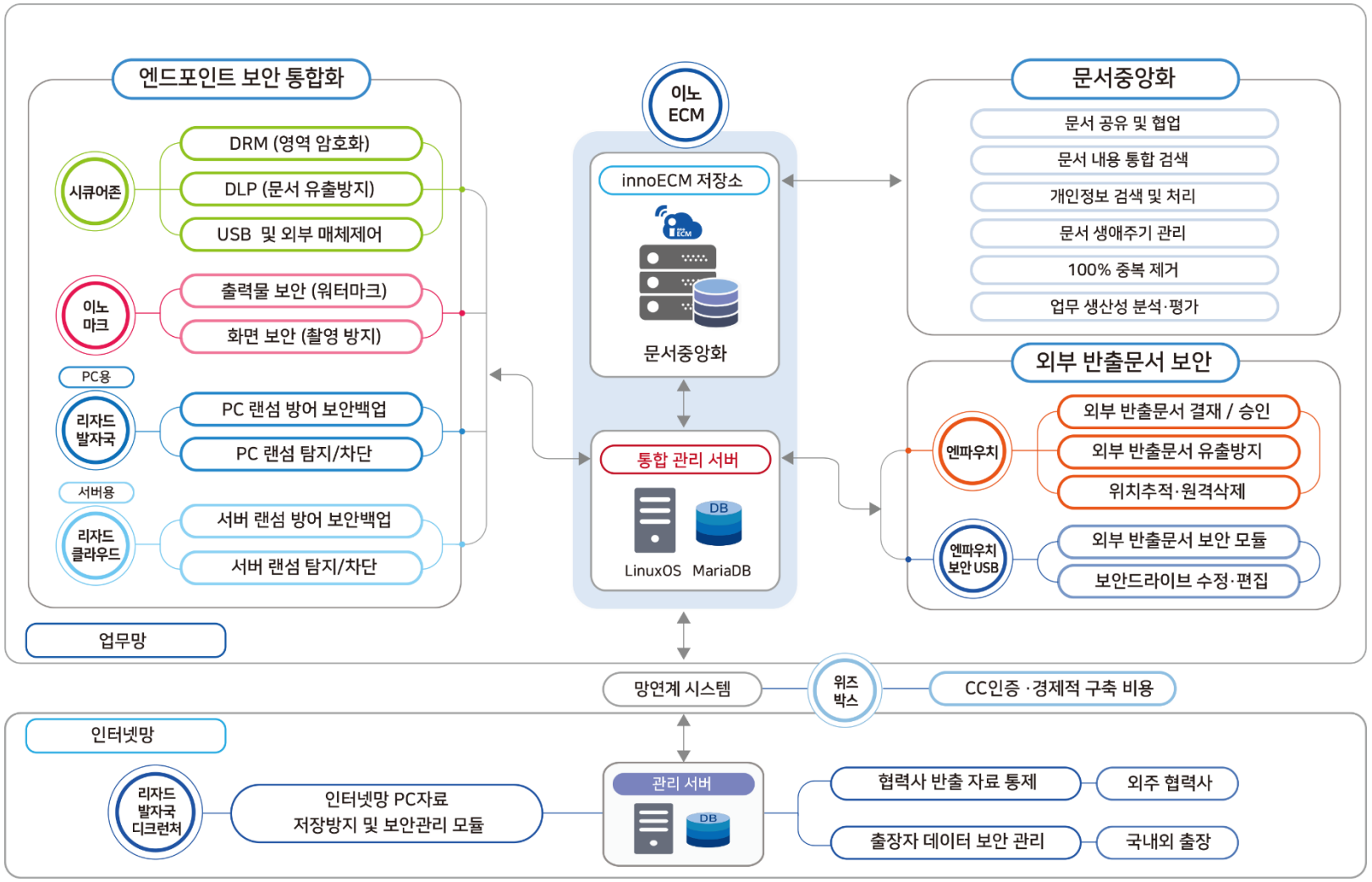
HISTORY

연도	내용
2019	-잊혀질 권리 구현 블록체인 플랫폼 개발 InnoBlock Chain Platform -국가핵심기술 데이터 위치추적 서비스 개발 -사내 데이터 공유 및 협업을 위한 innoECM 개발 -엔드포인트 보안기술 통합화-지능화-시각화 프로젝트 개시
2018	-100대 방산업체 망분리 사업 15개 사이트(한화 에어로스페이스, 두산중공업 등) 수주 및 공급 -시험지 유출방지용 스마트 시험관리 통합 보안관제 플랫폼 개발 -2018 랜섬웨어 디펜더 컨퍼런스 개최: 2.6
2017	-한화그룹 외 방산부문 데이터 보안 사업 수주 및 공급 -에스원과 방산업체 망분리사업 협약 체결 -미래부 주관 랜섬웨어 민관 대응 핫라인 구성
2016	-2016 차세대 데이터 보호 컨퍼런스 개최 -에스원과 '대국민 랜섬웨어 대응서비스 ' 협약
2015	-한국랜섬웨어침해대응센터 오픈 -ID 패스워드 보안인증 핀테크 솔루션 "아이오써티" 출시 -리자드클라우드 엔파우치 v10 GS인증 획득
2014	-발자국 조달등록 -일본 서버백업용 클라우드백업 서버 수출 -중소기업청 "수출역량강화사업자" 선정 -삼성디스플레이 DB백업사업 수주 (100 Unit)
2013	-DB백업용 클라우드백업 일본 수출 -SW산업원천기술개발사업 "클라우드 환경의 DRaaS"개발 컨소시움 참여 -엔파우치 특허등록 및 프로그램 등록
2012	-세무사협회 한길 TIS와 세무회계 데이터 온라인 백업서비스 개시 -특허청 VDI 클라우드 데이터 백업 솔루션 2,000유저 납품
2011	-일본KCS사와 클라우드백업v7 공급계약 체결 -사내 구축형 프라이빗 클라우드 "리자드 클라우드"출시
2010	-(주)이노티움 설립

이노티움 기술개발 도메인

개발사인 ㈜이노티움은 다수의 특허와 인증서를 기반으로 실시간 PC(엔드포인트) 개인정보 백업 및 랜섬웨어 예방 보안 백업, 문서보안, 외부반출문서보안 등 정형/비정형 전자문서의 관리와 정보보호 관련 솔루션 사업에 주력하고 있습니다.

이노티움 지능형 보안파일서버 기반 통합 문서보안 플랫폼



특허증 및 인증서

특 허 증

CERTIFICATE OF PATENT

특 허 제 10-1346284 호 (PATENT NUMBER)

출원번호 (APPLICATION NUMBER) 제 2012-0058844 호

출원일 (FILING DATE:YY/MM/DD) 2012년 05월 31일

등록일 (REGISTRATION DATE:YY/MM/DD) 2013년 12월 23일

발명의명칭 (TITLE OF THE INVENTION)

암호화 파일의 생성 방법 및 해독 방법과 이 방법을 실행시키기 위한 프로그램을 기록한 컴퓨터로 판독 가능한 기록 매체

특허권자 (PATENTEE)

주식회사 이노티움(110111-4******)

서울특별시 구로구 디지털로 285 , 902호(구로동, 에이스원타워1차)

발명자 (INVENTOR)

등록사항란에 기재

위의 발명은 「특허법」에 따라 특허등록원부에 등록되었음을 증명합니다.

(THIS IS TO CERTIFY THAT THE PATENT IS REGISTERED ON THE REGISTER OF THE KOREAN INTELLECTUAL PROPERTY OFFICE.)

2013년 12월 23일

특허청장 김 영

COMMISSIONER, THE KOREAN INTELLECTUAL PROPERTY OFFICE

엔파우치 특허증

특허 / 인증

백업방법 특허증

이중파일백업 방법 특허증

원상복구 보증서

Certificate of Assurance

(주)이노티움은 아래 대상 제품을 구입한 고객의 데이터가 랜섬웨어 공격으로부터 암호화될 경우 원상복구할 것을 보증합니다.

대상제품 1. 리자드백업 v10 DB서버 랜섬크린저
2. 리자드클라우드 v10 랜섬크린저
3. 발자국 v3.0

2017년 12월 2일

주식회사 이노티움 대표이사

악성코드 탐지 방법 특허증

웹접속 정보 실행 특허증

소프트웨어품질인증서

Certificate of Software Quality

리자드클라우드 엔파우치 v10 GS인증

저작권 등록증

발자국 v3.0 GS인증

상표등록증

LIZARD

리자드클라우드 상표등록증

상표등록증

NPOUCH

엔파우치 상표등록증

행정업무용 소프트웨어 선정확인서

발자국 행정업무용 소프트웨어 선정확인서

주요 레퍼런스

경상남도청, 문화체육관광부, 특허청, KISA, 삼성전자, 현대자동차을 비롯하여 다양한 산업의 고객들에게
PC(엔드포인트) 랜섬웨어 탐지 및 개인정보 백업 사업을 수행하였으며 제품의 안정성과 신뢰성을 인정받고 있습니다.

경상남도 GYEONGNAM | 문화체육관광부 | 특허청 KOREAN INTELLECTUAL PROPERTY OFFICE | SAMSUNG ELECTRONICS | 한화시스템 | KORAIL 한국철도공사

공공

경상남도청 | 양산시청 | 통영시청 | 광명시청 | 강동구청 | 은평구청 | 강화군청 | 울주군청 | 문화체육관광부 | 한국전력거래소 | 우정사업본부 | 여성가족부 | 특허청 | 한국인터넷진흥원 | 한국전자통신연구원 | 한국수자원공사 | 대한석탄공사 | 한국전력기술

외 100여 기관

금융

KB카드 | 동부증권 | 신영증권 | KDB인프라자산운용 | 한화저축은행 | 스마트저축은행 | 골든브릿지저축은행

외 50여 업체

기업

삼성전자 | 현대자동차 | 두산중공업 | LS전선 | 대명 | 효성 | 유한화학 | 동국제약 | 이연제약 | 서울제약 | 미림화학 | 유한화학 | 국방일보 | 전남일보 | 국제신문 | 동아일렉콤 | 두산중공업 | 한화시스템 | 한진중공업 | 한화에어로스페이스

외 300여 업체

의료

국립암센터 | 충북대학교병원 | 국립정신건강센터 | 부산대학교병원 | 효성병원 | 효성세종병원

외 20여 업체

교육 및 협회

계명문화대학교 | 창원대학교 | 울산대학교 | 전북대학교 | 한국건설자원공제조합 | 벤처기업협회 | 한국전기기술인협회 | 한국전기공사협회

외 10여 기관

한국랜섬웨어침해대응센터

rancert 한국랜섬웨어침해대응센터

렌섬웨어 예방을 위한 개인사용자 무료 다운로드 200,000여명
www.rancert.com

유비무환

有備無患

㈜애플소프트 www.applesoft.co.kr
T. 02)836-4024 | E.yjyeung@applesoft.co.kr