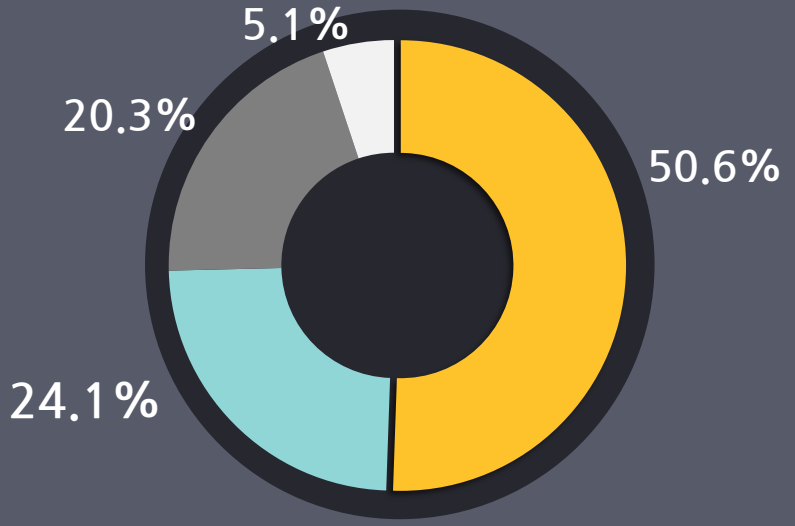
랜섬웨어 대응방안에 대한 오해와 진실

효성인포메이션시스템

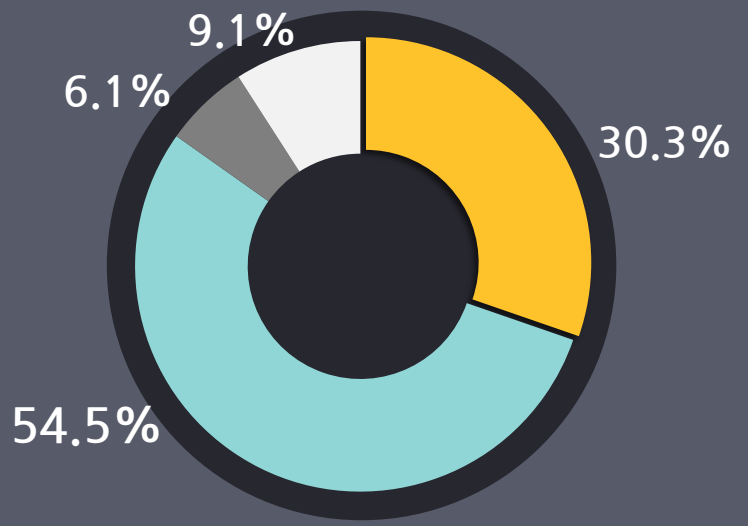
국내 랜섬웨어 피해 현황

랜섬웨어 공격을 당한 경험이 있는가?



- 응답자의 75%가 공격을 당함, 50% 이상이 피해

랜섬웨어 피해를 입은 후 어떻게 조치했나?



- 피해자의 30%는 백업 데이터로, 9%는 돈을 주고 복구했으며, 54%는 데이터를 포기

(출처: 네트워크타임즈 2017년 1월호)

국내 랜섬웨어 피해 현황

[설문조사③] 기업 절반 "랜섬웨어로 피해 입어"

정보보안 담당자 50.6% "랜섬웨어 공격 피해 입었다" … "이메일 이용한 피해 가장 많아"

2016년 12월 29일 09:40:32 김선애 기자 ✉iyamm@da

업무 관련 이메일 피해 가장 많아

2016년 보안 시장을 한해를 뜨겁게 달군 것 중 하나가 랜섬웨어이다. 랜섬웨어 공격이 일반 사용자뿐 [illegible] 기업에까지 막대한 피해를 입혔다. 업무와 연관된 메일로 위장해 유포된 록키 랜섬웨어와 유명 인터넷 커뮤니티의 광고를 통해 유포된 크립트엑스엑스엑스는 국내에 가장 많은 피해를 입힌 공격으로 꼽힌다.

랜섬웨어가 창궐하면서 랜섬웨어 방어 전용 솔루션도 경쟁적으로 쏟아져나왔지만, 응답 기관 중 랜섬웨어 방어 전용 제품을 구입한 곳은 5.3%에 불과했다. 68.4%는 백신과 APT 방어 솔루션으로 대응한다고 답했으며 백업 솔루션 도입, 8.8%는 망분리와 문서중앙화 도입을 들었다.

랜섬웨어 방어를 위한 전용 솔루션이 아니라 APT 방어 솔루션을 선호하는 이유는, 랜섬웨어도 악성코드 진행되기 때문에 악성코드를 탐지·차단하는 제품을 통해 보안 수준을 높이고자 하는 것으로 파악된다. 또한 랜섬웨어가 APT 공격과 마찬가지로 이메일, 웹을 통해 유입되며, 신변종 악성코드를 이용하기 때문에 솔루션이 더 효과적이라고 판단하는 것으로 분석된다.

랜섬웨어 방어를 위해 임직원 보안 교육을 철저히하고, 발견된 공격은 유관기관에 신고하며, 주기적인 데이터를 보호하는 등의 일련의 정보보안 프로세스가 마련돼야 한다는 의견도 다수 제시됐다.

- 이메일
- 인터넷사이트광고
- 랜섬웨어 방어 전용 제품 5.3%
- 백신, APT 방어솔루션 68.4%
- 백업솔루션 7.0%
- 망분리, 문서중앙화 8.8%

(출처: 네트워크타임즈 2017년 1월호)

랜섬웨어는 어떻게 감염되나요?

원인

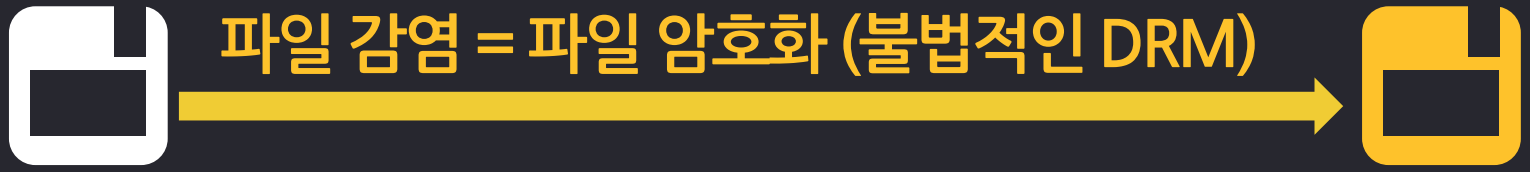
숙주 파일 실행(이메일 첨부 파일, 토랜트 등)

감염코드가 포함된 웹사이트 방문(인터넷 광고 배너 등)

- 인터넷 연결 시 감염(Win SMB 취약점 공격, 랜섬웨어의 진화)

동작

PC에 연결된 파일시스템 구조 파악 → 드라이브, 폴더 리스트와 파일 리스트 확보 → 암호화 시작



오해1

백신 · 방화벽 · APT방어솔루션을 도입/업데이트하면 안전하다?

랜섬웨어 당해보니… 데이터 구출 경험담

저장장치 백업본을 통해 파일들을 복구, 최신 파일들은
안티바이러스 업체의 복구툴을 이용해 복호화
→ 복구에는 총 2시간 정도 소요

매우 짧은 시간 안에 매우 빠르게 확산되고
악성코드 활동을 중단시키거나 봉쇄할 수 있다고
기대해서는 안된다는 것을 깨달았다.

- 한 기업 보안 책임자 -

백신, 방화벽, IDS/IPS, APT방어솔루션

랜섬웨어 패턴을 등록하여 차단

PC에 설치되는 백신프로그램, 또는 방화벽, IDS/IPS, APT방어솔루션 등에 랜섬웨어 패턴 등록

- 모든 패턴의 등록이 가능?
- 지속적 업데이트 가능?

랜섬웨어 감염파일 복호화

백신 프로그램을 이용해 랜섬웨어 감염파일을 치료

- 복호키를 확보하지 못하면?

오해2

랜섬웨어 방어 전용 제품 이어야만 한다?

랜섬웨어 방어 전용 제품

'미끼'를 투척해 랜섬웨어 악성코드가 파일을 암호화하는 것을 찾아내 차단

감염 프로세스 전체를 보고 블랙리스트, 화이트리스트, 임계치 기반 정책의 3단계에 걸쳐 차단

랜섬웨어 프로세스 차단과 백업을 동시에 수행

PC Agent 관리

모든 패턴 등록이 가능?

지속적 업데이트 가능?

프로세스가 바뀐다면?

전세계적 랜섬웨어 공격발생

랜섬웨어는 계속 진화 중

‘동작 프로세스’와 ‘공격 대상 파일’ 계속 변경

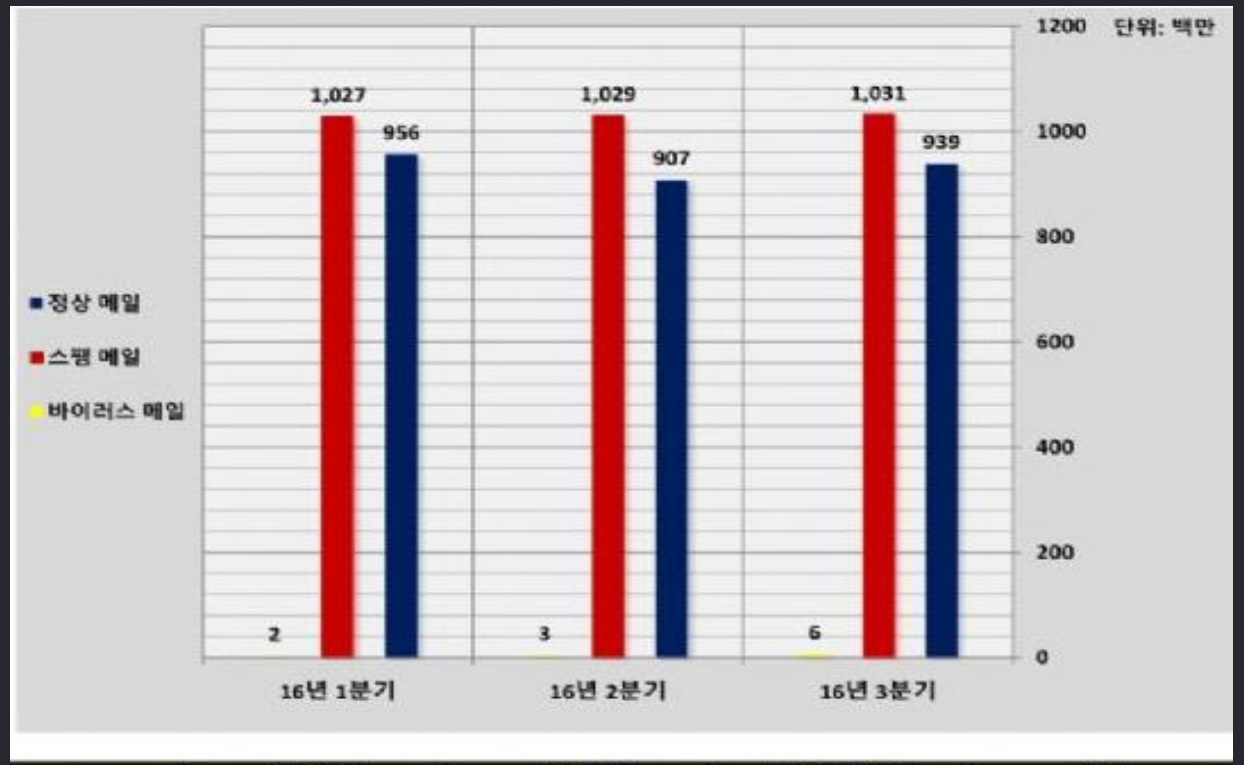
→ 한번의 전용 제품 도입으로는
지속적인 방어 불가능

오해3

이메일 및 광고 차단으로 랜섬웨어를 방지할 수 있다?

이메일 모니터링

’2016년 3분기 스팸메일 동향 분석 리포트



	정상 메일		스팸 메일		바이러스 메일		합계	
16년 3분기	938,683,683	47.50%	1,031,445,569	52.20%	5,955,691	0.30%	1,976,084,943	100.0%
16년 2분기	907,412,173	46.78%	1,029,286,868	53.06%	3,097,895	0.16%	1,939,796,936	100.0%
16년 1분기	956,240,355	48.15%	1,027,404,473	51.74%	2,248,040	0.11%	1,985,892,868	100.0%

※ 분기별 정상/스팸/바이러스 메일 건수는 스팸스나이퍼 고객 중 국내 200여개 회사의 데이터를 집계한 결과임

바이러스 메일

- 전 분기 대비 92% 증가
- 첨부파일 통한 랜섬웨어 多
- 발신자, 제목 수시 변형

스팸 메일

- 주로 영어 → 한국어 발견

(출처: 지란지교소프트)

모니터링 및 차단

특정 패턴을 감지하여
멀웨어/바이러스/랜섬웨어 차단

첨부 파일을 검사하여 문제가
있을 시 차단

외국어로 된 이메일 차단

망분리를 통한 유입 차단

모든 패턴적용 불가

진화 중인 랜섬웨어

업무 효율성 문제

망분리 에서
사고 사례 있음

오해4

랜섬웨어 방지는 개인의 몫이다?

랜섬웨어는 어떻게 확산 되나요?

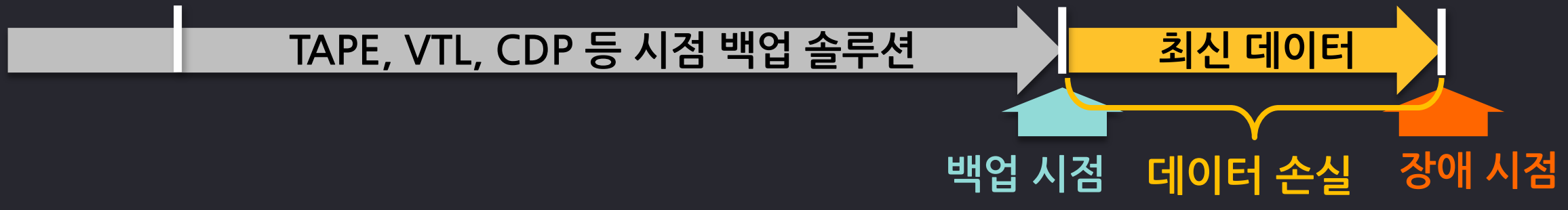
감염 확산 경로 및 영향도

랜섬웨어는 개인의 문제가 아닌
기업 전체의 문제이다.

오해5

랜섬웨어 감염 대응의 유일한 방안은 백업 뿐이다?

백업의 허와 실



✔주요 업무 데이터

스토리지 이중화, 스냅샷,
백업 솔루션을 통한 백업 등

개인 데이터

개인의 관리 영역

개인 데이터도 기업의 자산
- VDI, ECM, 문서 중앙화 -

기존 백업의 한계점

실시간 - 감염도 실시간
주기적 - 데이터 손실 발생(RPO)

✔개인 데이터 백업

개인 데이터 통합 관리 방안
공유 폴더가 랜섬웨어 확산 통로
클라우드 백업 시 보안이슈

랜섬웨어 대응방안에 대한 오해

1. 보안 솔루션

2. 전용 제품

5. 백업

충분한 대응방안이 될수 없다

데이터 보호를 위한 목표

예방	데이터를 보호하기 위한 보안 정책 적용
복구	가장 빠른 시간 내(RTO)에 최신 데이터(RPO)를 복구
업무효율	기존 업무 환경 변화나 영향을 최소화
비용	도입/운영 비용의 최소화, 효율화

랜섬웨어 대응, 발상의 전환

예방

감지, 차단, 예방을 위한
보안 솔루션을 도입한다!

100% 예방과 차단이 가능한가?

VS

파일 변경을 못하게 한다!

복구

백업/복구 솔루션을
도입한다!

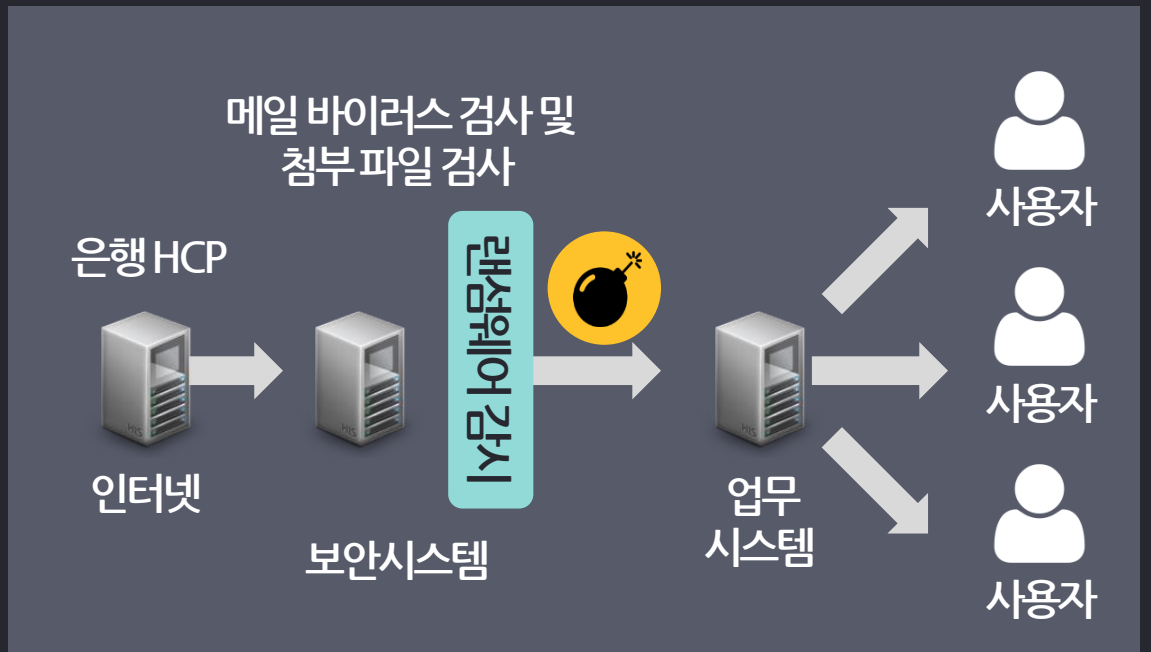
100% 백업과 복구가 가능한가?

VS

감염 직전 버전으로 되돌릴 수
있는 효율적 방법을 찾는다!

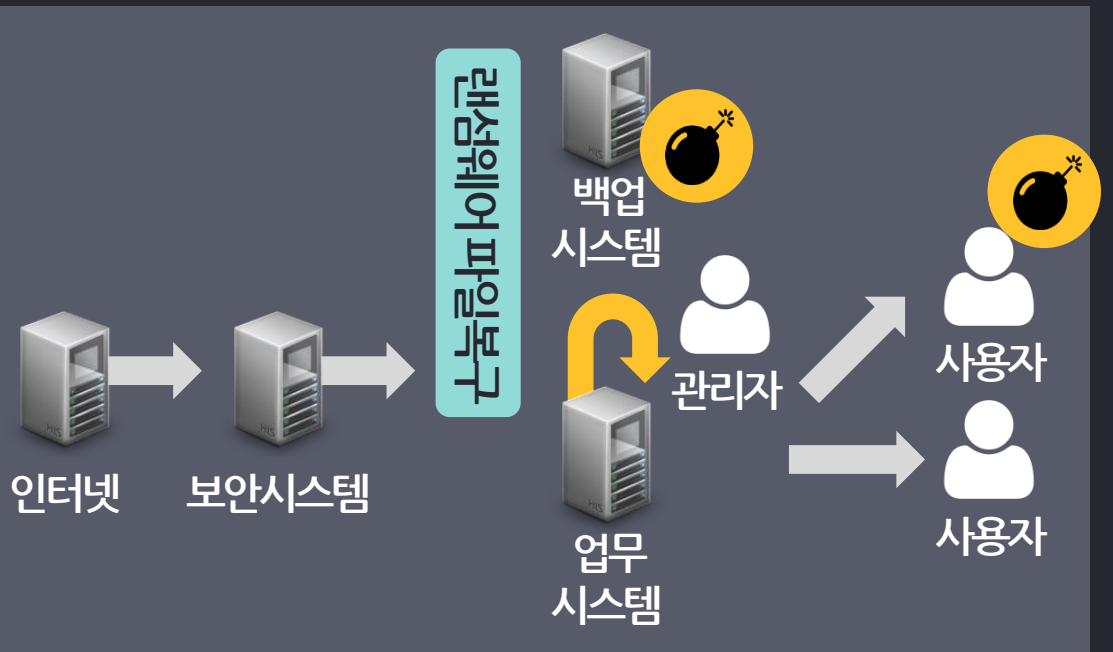
기존의 랜섬웨어 대응 방안

보안 시스템에서 이메일, 광고에 대한 바이러스 검사 및 첨부 파일 검사 방식



다양한 방식의 랜섬웨어 탄생하여
기존방식으로 100% 감시 불가능

백업 시스템으로 데이터 백업을 수행, 백업으로부터 데이터를 복구하는 방식



- 긴 복구 시간, 데이터 손실 발생
- 개별 PC 사용자에 대한 대응은 미비

제언1

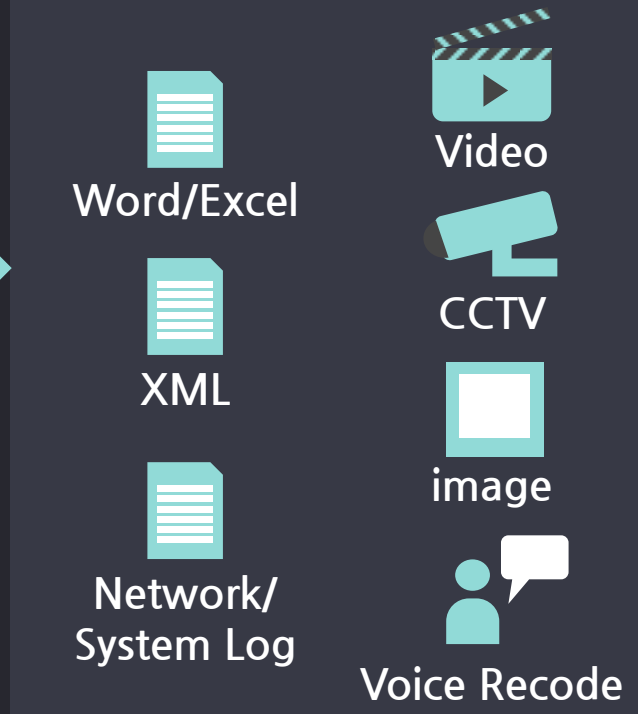
신개념 스토리지를 통해 예방하고 복구하라

컨텐츠 보호 전용 신개념 스토리지

데이터 보호 특화 설계

- 파일시스템으로 마운트 되어 있지 않아 파일의 감염 확산 방지
- 파일 수정 방지 : 파일의 훼손/손상/감염 자체 방지
- WORM 기능 : 스토리지 레벨에서 파일의 이름 변경 및 내용 변경 기능 자체 방지
- 파일 버저닝 : 파일 변경/삭제시 이전 버전 파일 보관

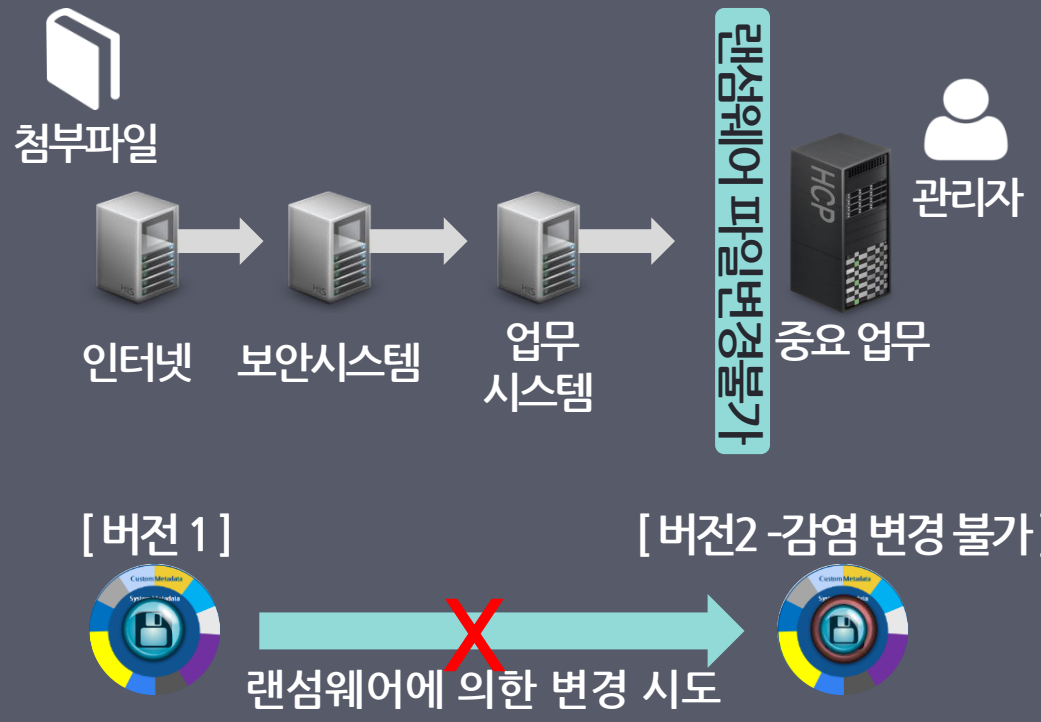
HCP (오브젝트 스토리지)



효율적인 컨텐츠 관리

- 단일 스토리지 플랫폼 내에서 데이터 가치에 따라 저장 매체와 보호 정책 차등 적용
- 빠른 파일 검색
- 중복파일제거, 압축
- 프로비저닝, 유연한 할당과 회수
- 백업리스 (백업비용 감소)
- 파일에 메타데이터

파일 변경 원천 방지를 통한 업무 시스템 예방



- 중요한 업무 파일에 대한 랜섬웨어 감염에도 파일변경 원천 방지

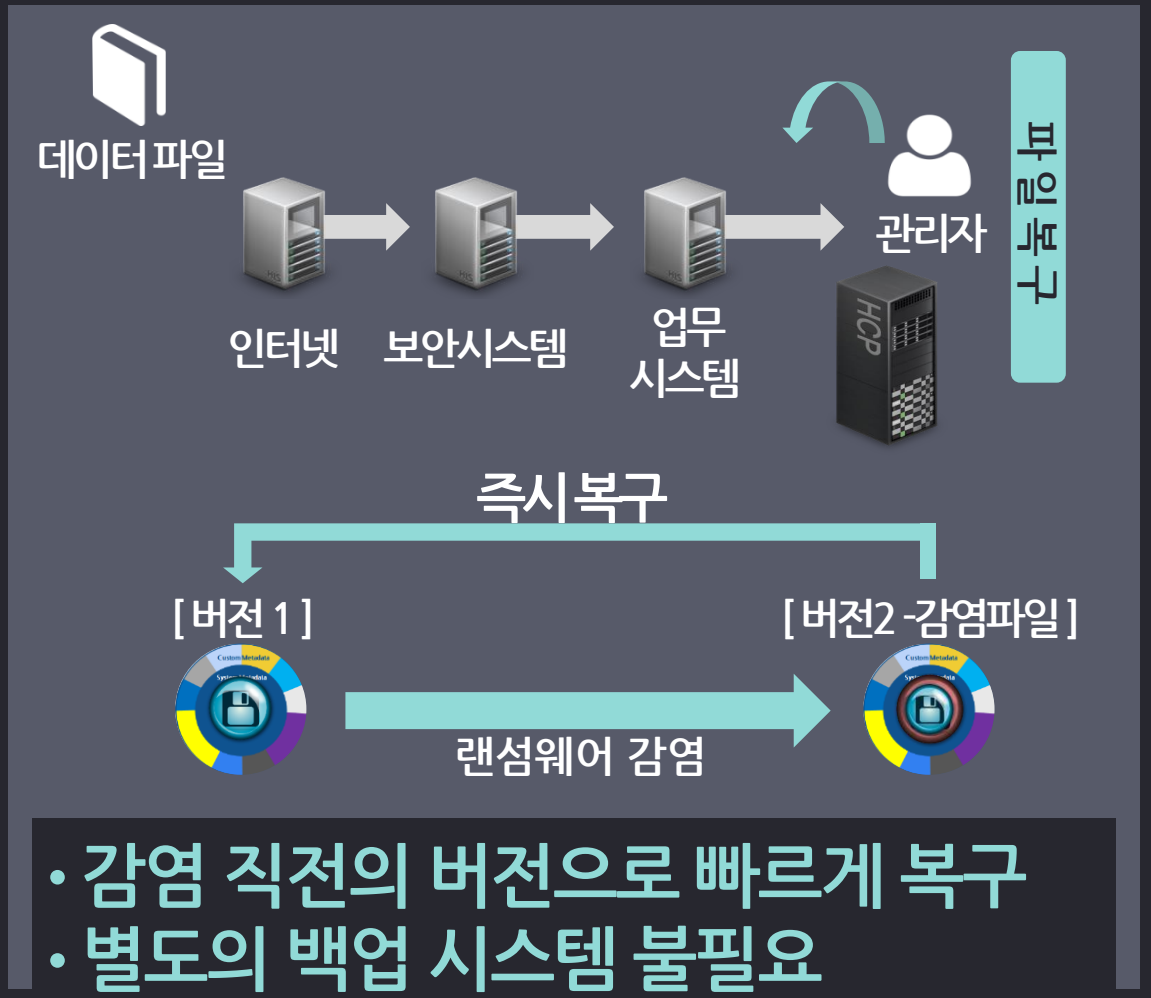
중요 파일 시스템 파일 변경 방지

- 장기 보관용 파일 또는 원본 파일 감염 리스크
- 컴플라이언스 제도상 보관 및 관리 의무가 있는 파일 감염 리스크

HCP(Hitachi Content Platform)

- 외부 침입 또는 내부의 실수에 의한 어떠한 시도에서도 파일 훼손 불가

파일 버저닝을 통한 업무 시스템 복구



- 감염 직전의 버전으로 빠르게 복구
- 별도의 백업 시스템 불필요

시스템 복구 방식

- 관리자 단위에 의해서만 파일 복원 가능
- 개별 사용자별 복원 불가능
- 복원 시점에 따른 최신 파일 복원이 어려움 있음

HCP(Hitachi Content Platform)

- 관리자에 의한 복원
- 파일 단위의 복원 지원
- 랜섬웨어의 패턴에 관계 없이 이전 버전으로 바로 복원 가능

신개념 스토리지 파일 보호 기능

삭제가 안되는 파일이 계속 늘어 난다면?

용량 관리를 위한 다양한 옵션 지원

- 파일 수정 영구 금지
- 금지 기간 옵션 지원
- 금지 기간 이후 삭제를 통한 용량 회수 재사용 가능

변경 금지 기간 이후의 대응책은 ?

파일 보호 기능 재적용

- 파일 수정 금지 기간 이후에는 버저닝 기능을 적용하거나 또는 파일 수정 금지 기간 연장

제언2

개인 및 공유 파일을 보호하고 복구하라

HCP Anywhere: 개인 파일 보호/복구 솔루션

자동백업

- 개인 - 백업 폴더 지정
  - HCP Anywhere 폴더에 파일 업로드
- 관리자 - 백업 폴더, 파일 지정
- 파일 버저닝 기능 : 감염 직전 버전 복구

보호/복구

협업

- 팀폴더, 공유폴더
- 통제와 접근제어 가능
- 파일 사용 이력 추적 가능

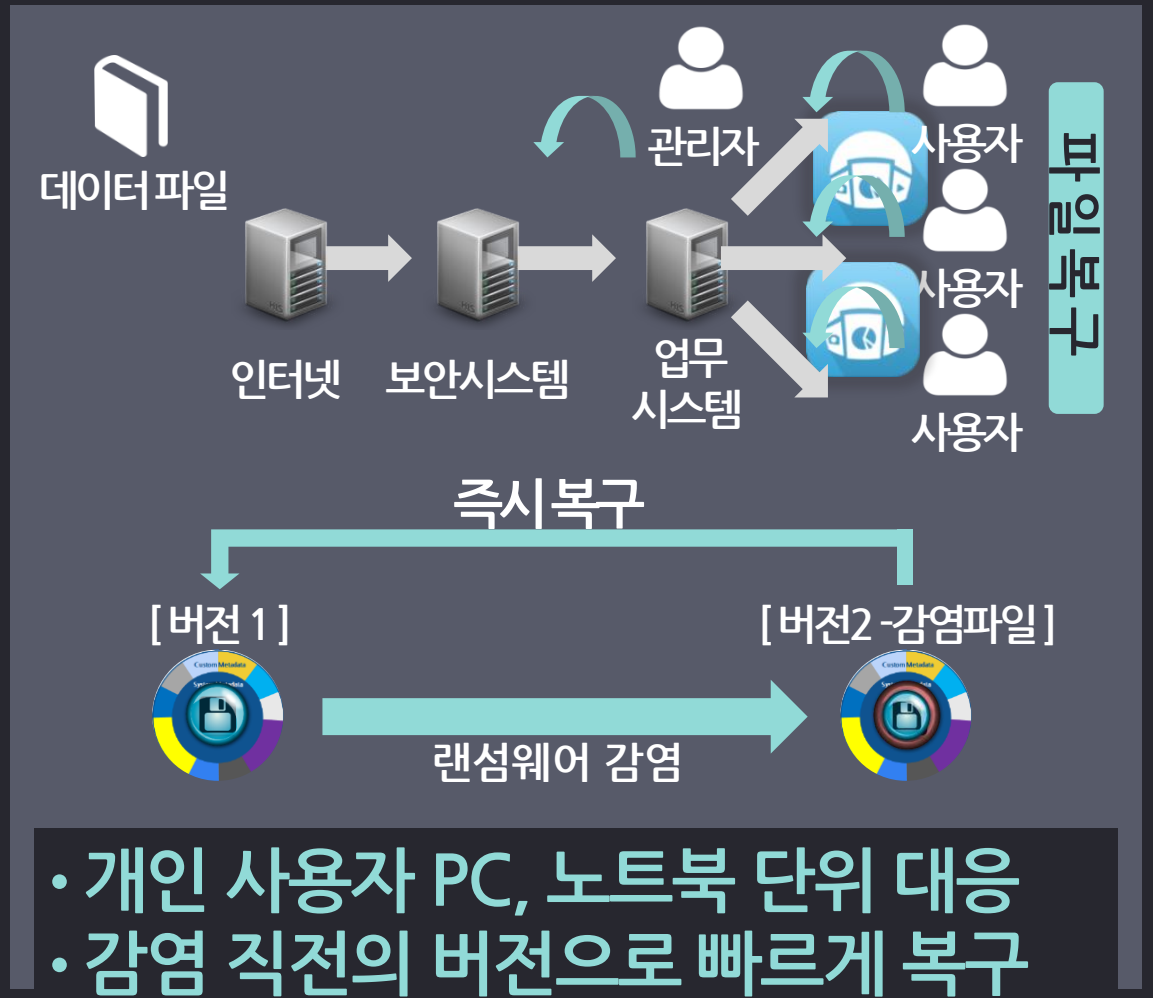
공유

클라우드홈

- HCP Anywhere 동기화 서비스
- 사내 NAS/파일공유서버를 HCP Anywhere를 통해 Access

액세스

개인 PC 백업 및 파일 복구



- 개인 사용자 PC, 노트북 단위 대응
- 감염 직전의 버전으로 빠르게 복구

개인용 파일 별 복구 방식

- 개별 사용자 별 복원 불가능
- 복원 시점에 따른 최신 데이터 복원이 어려움
- 클라우드 백업 데이터 보안 이슈

HCP Anywhere

- 개별 사용자가 원하는 시점으로 전체 또는 파일 단위 복원 가능
- 특정 날짜 복원 지원
- 온-프레미스 클라우드 백업 시스템

개인 / 공유 파일 보호 기능

파일 변경 지원 숫자와 용량 필요 정도는?

효율적 용량 관리

- 버저닝을 통한 용량 증가는 일정 기간 경과 후 자동으로 정리
- 파일 압축 기능과 중복 제거 기능으로 인한 용량 절감 효과가 보다 큼

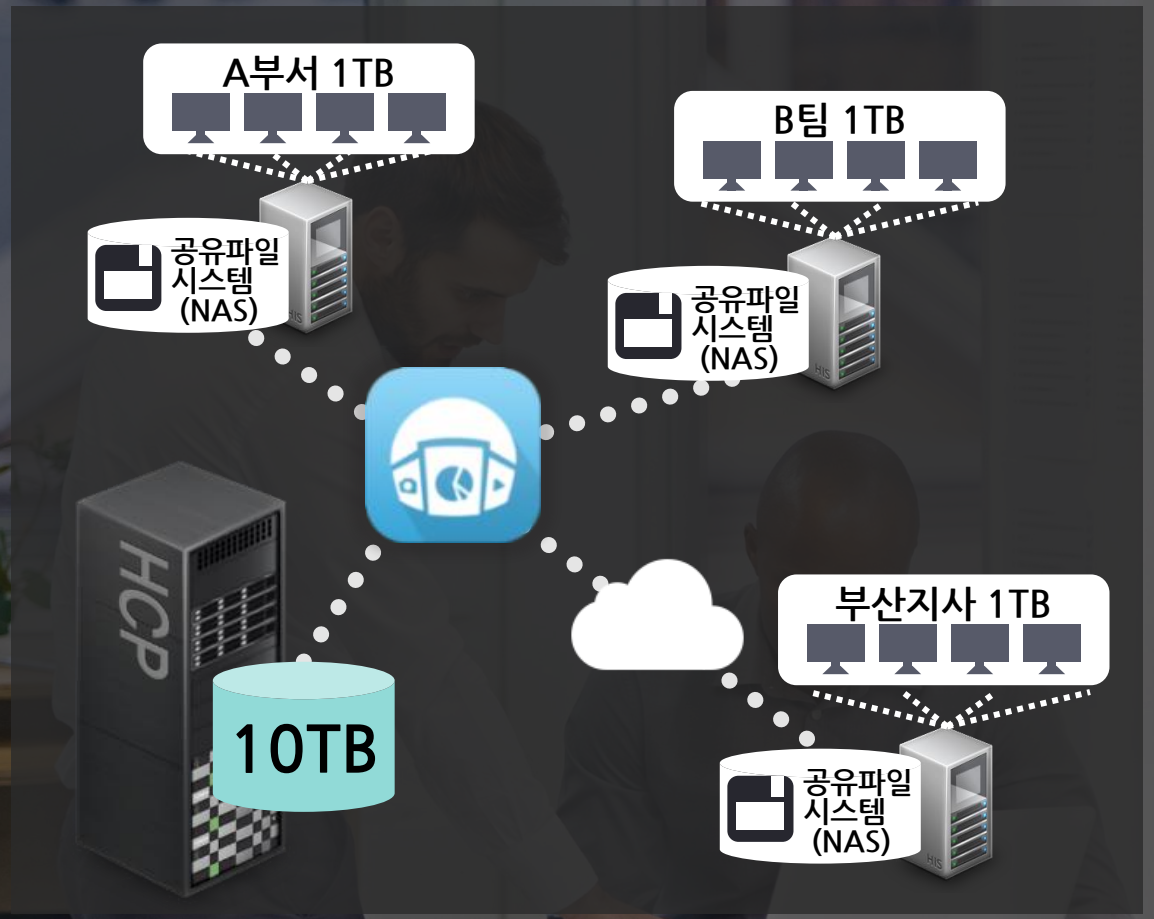
랜섬웨어 뿐 아니라 다른 훼손 시에도 복구 가능?

모든 파일 복구 지원

- 삭제된 파일도 버저닝 복구 지원
- 삭제 파일 보존 기간 별도 설정 지원

효성인포메이션시스템이 제안하는
데이터 보호 정책 단계별 적용

1단계 개인 데이터 백업

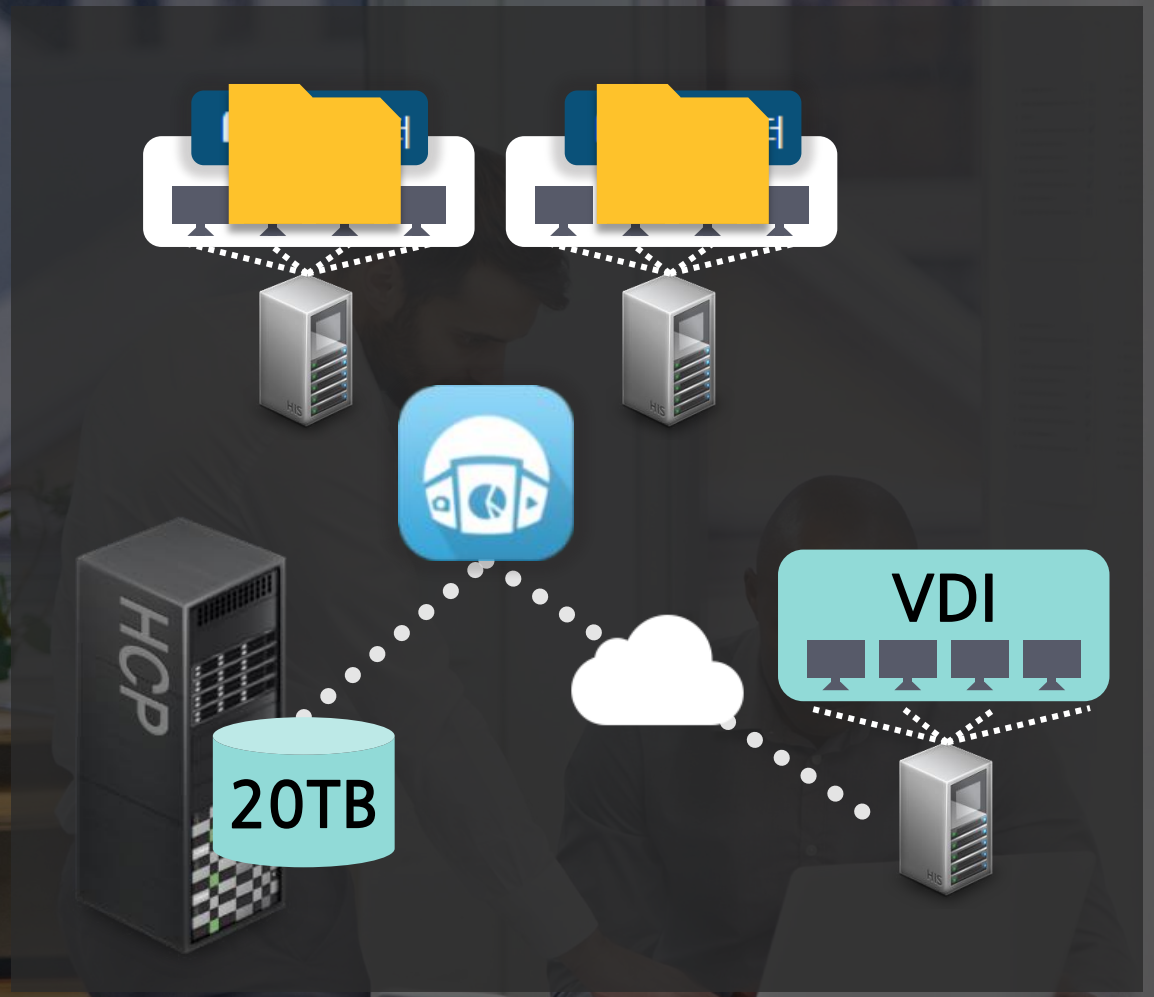


개인용으로 클라우드 백업 서비스 구축

- 개인당 10GB 제공
- 파일 Sync/share 및 협업
- 온프레미스 “BOX” 어플라이언스 솔루션

최소의 비용과 변경으로
기업 내 개인들이 보유하고 있는 데이터를
보호할 수 있음

2단계 클라우드 홈 구현



파일 공유 서버 통합

- 팀/부서 파일 서버 통합
  - HCP AW 팀/부서용 협업 폴더
- 개별적으로 운영되던 공유서버 통합
- 원격지에서도 VDI 환경 운영 가능

팀이나 부서에서 개별적으로 운영되는 파일 서버를 HCP AW로 통합하여 효율적 관리

VDI를 NAS로 사용하는 경우
NAS를 개인 네트워크 드라이브로 사용하는 대신 HCP AW 로 할당

3단계 업무 서비스에의 적용

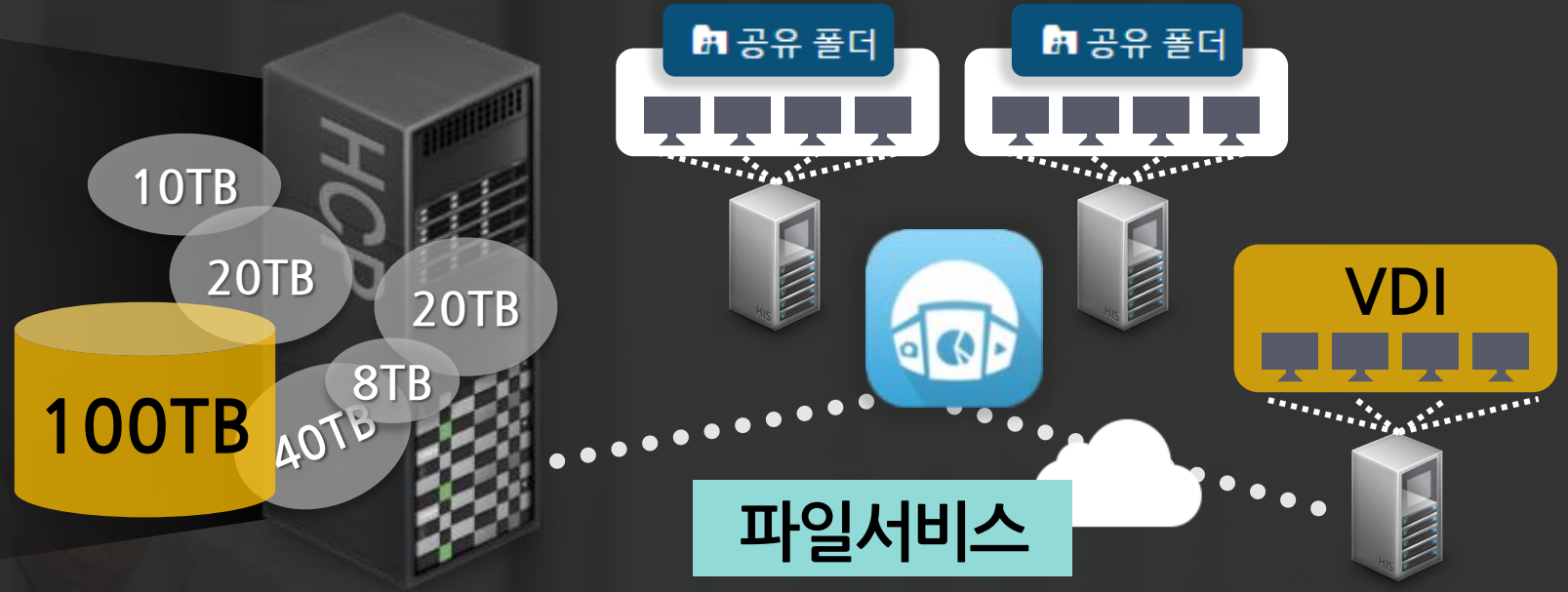
콜센터/녹취

이미지/도면

PACS 시스템

ECM/EDMS

기록물 보관



업무 서비스 통합 스토리지

- 파일 서비스가 필요한 업무 시스템의 주요 통합 저장 장치
- VDI, ECM 등의 솔루션의 통합 스토리지로 기업 내 주요 파일의 통합 저장소


RANSOMWARE
웨비나 보러가기
CLICK
효성인포메이션시스템