비대면바우처플랫폼 k-voucher.kr

1등급 GOOD Software GS인증

Start 창업기업제품

녹색인증 Green Certification 녹색기술제품

비대면 방식의 온라인원격 디스크영구삭제

제로클솔루션 표준사업제안서

시장상황

진화하는 데이터산업, 전자문서 활성화와 데이터3법개정으로 인한 보안성 중요도가 증가

디스크 완전삭제 관련 지침 획기적변화

제37조(전자정보 저장매체 불용처리) ① 사용자 및 시스템관리자는 하드디스크 등 전자정보저장매체를 불용처리(교체·반납·양여·폐기 등) 하고자 할 경우에는 저장매체에 수록된 자료가 유출되지 않도록 보안조치 하여야 한다.

② 자료의 삭제는 해당 정보가 복구될 수 없도록 저장매체별, 자료별 차별화된 삭제방법을 적용하여야 한다.

③ 연구원 내에서 정보시스템의 사용자가 변경된 경우, 비밀처리용 정보시스템은 완전포맷 3회 이상, 그 외의 정보시스템은 완전포맷 1회 이상으로 저장자료를 삭제하여야 한다.

④ 전자정보 저장매체의 불용처리에 관한 세부적인 사항은 「국가 정보보안 기본지침」에서 정한 바에 따른다.

정보보안지침 개정

제5조(저장매체 불용시 삭제방법) ① 각급기관의 분임정보보안담당관은 저장매체 불용처리시 다음 분류에 따른 기준 이상으로 삭제한다.

저장 매체 \ 저장 자료	공개 자료	비공개 자료	대외비 자료	비밀 자료
자기테이프 플로피디스크	자체 판단	물리적 파괴	물리적 파괴	물리적 파괴
광디스크 (CD·DVD 등)	자체 판단	물리적 파괴	물리적 파괴	물리적 파괴
반도체메모리 (SSD·USB 등)	포맷 또는 삭제	완전삭제 제품	물리적 파괴	물리적 파괴
하드디스크	포맷 또는 삭제	디가우징 또는 완전삭제 제품	물리적 파괴	물리적 파괴

※ 반도체메모리의 경우 최초 사용시부터 디스크 암호화(BitLocker 등)를 사용하고 암호키는 국가 정보보안 기본지침 제76조에 따라 설정하여야 완전삭제 가능

국정원 정보보안지침사항 발췌(2020년 12월20일)

정보보호 VS 데이터 활용, 최적점 찾기 위한 노력 필요

□ 개인정보 보호법

제21조(개인정보의 파기) ① 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.

② 개인정보처리자가 제1항에 따라 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.

③ 개인정보처리자가 제1항 단서에 따라 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장·관리하여야 한다.

④ 개인정보의 파기방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.

데이터 3법 개정

□ 개인정보 보호법 시행령

제16조(개인정보의 파기방법) ① 개인정보처리자는 법 제21조에 따라 개인정보를 파기할 때에는 다음 각 호의 구분에 따른 방법으로 하여야 한다.

1. 전자적 파일 형태인 경우: 복원이 불가능한 방법으로 영구 삭제
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우: 파쇄 또는 소각

② 제1항에 따른 개인정보의 안전한 파기에 관한 세부 사항은 행정자치부장관이 정하여 고시한다.

□ 개인정보의 안전성 확보조치 기준 고시

제13조(개인정보의 파기) ① 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.

1. 완전파괴(소각·파쇄 등)
2. 전용 소자장비를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

② 개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하여야 한다.

1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 천공 등으로 삭제

이데일리 발췌(기사보기)

매체별로 다른 데이터 완전삭제 전격해부

데이터 완전삭제는 하드디스크 기록 원리를 뒤집는 방식이다. 하드디스크는 보호 케이스 안에 있는 플래터(금속 원형판)를 회전시켜 자기 패턴으로 정보를 기록한다. 이때 모든 기록은 PC가 사용하는 이진법을 따라 패턴(010101 등)으로 기록된다. 데이터는 플래터 표면에 코팅된 자성체에 기록되며 회전하는 플래터 위에 부상하는 입출력 헤드가 자기적으로 데이터를 읽고 쓴다.

실제 데이터가 저장된 하드디스크 플래터 표면을 살펴보면 규칙적인 모양을 찾을 수 있다. 한국캐드컴이 원자력 현미경을 활용해 데이터 삭제 여부를 정밀 촬영한 결과 이레이징, 디가우징을 거친 하드디스크 플래터는 각기 다른 표면을 갖는다. 하드디스크 데이터 규칙성은 이레이징과 디가우징을 거치면서 패턴이 불규칙하게 변하고 데이터가 완전 무결해졌을 때 패턴 자체가 사라진다.

◇데이터 완전삭제…하드웨어(HW), 소프트웨어(SW) 방식으로 구분

하드디스크 데이터 완전삭제는 크게 HW 방식과 SW 방식으로 구분한다. 하드웨어 방식은 디스크 자체 파괴, 디가우저가 있다. SW 방식은 이레이저를 중심으로 각 보안기업마다 다양한 SW솔루션을 제공한다.

정부는 HW 방식 장비에 대해 보안적합성검증을 받도록 한다. 이레이저는 CC인증을 받아야 한다. 디스크 자체 파괴는 하드디스크를 작동하지 못하도록 완전하게 부수는 것이다. 하드디스크는 일반적으로 알루미늄 등 구성체로 쉽게 별도 장비를 이용해 파괴한다. 하드디스크에 구멍을 뚫는 천공, 찌그러뜨리는 만곡, 파쇄기 등이 존재한다.

디가우징은 물리적 자성을 가해 하드디스크를 완전하게 사용 못하게 한다. 현재까지 디가우징을 거친 기기를 복구하는 방법은 없다. 디가우징 장비는 한 번에 강한 자성을 쏘거나 일정 수준 이상 자성을 가하는 방식으로 나뉜다. 천연자석을 활용한 방법도 있다. 플래터에 강한 자성을 주입하면 자력성질이 사라지면서 정보가 지워진다. 승차권, 신용카드에 부착된 자기 테이프 표면에 입혀진 산화철보다 자력이 센 자석이 스치고 지나가면 테이프 입력 자료가 사라지는 것과 마찬가지다.

PC나 주변장치 연결 없이 독립형으로 사용 가능해 폐기를 목적으로 하는 장치에 주로 활용한다. 다만 디가우저, 디스크 파괴 등 방식은 산업 폐기물을 발생시켜 활용도가 점차 감소한다.

데이터 완전삭제

전자신문 발췌(기사보기)

전자문서산업의 활용화로 데이터 정보보호보안 중요성 증가
데이터3법 개정과 안전하게 폐기할 수 있는 영구삭제 관심도 증가!

공공기관 및 금융기관 데이터 완전삭제 관리지침사항

공공기관 부처 데이터 폐기 지침

NIS 대한민국국가정보원

정보시스템 저장매체 불용처리 지침

제 6조 저장자료 삭제방법

비밀자료: 완전 포맷 3회 이상 수행
기타자료: 완전 포맷 1회 이상 수행

불용처리 후 삭제 여부 확인 요구

외부업체에 의뢰할 경우
삭제 절차 확인 및 감독

행정안전부

표준 개인정보 보호지침

개인정보의 파기 및 절차

복원 불가능한 방법, 그리고 현재의
기술수준에서 적절한 비용이 소요되는
방법으로 처리

개인정보 파기에 관한 사항을 기록
관리 및 보관

개인정보 파기 시행 후 파기 결과확인

미래창조과학부
Ministry of Science, ICT and Future Planning

정보보안 기본지침

제 21조 저장매체 불용처리

저장매체를 불용처리 할 경우 자료
유출 방지를 위한 조치

비밀자료:완전 포맷 3회 이상 수행
기타자료: 완전 포맷 1회 이상수행

외부업체에 의뢰할 경우 삭제 절차
확인 및 감독

국정원 보안 적합성 검증을 통과한
제품도입

국가기록원
National Archives of Korea

기록물 평가 , 폐기절차

전자기록물 폐기

전자기록물 폐기는 규정된
방법에 따라 처리

파기,소자,덮어쓰기(3회 이상)
방식 중에서 폐기방법을 선택

폐기 종료 후 폐기 증명서를 제출
받아서 관리 및 보관

데이터 완전삭제 기준은 데이터3법 준수 및 공공기관 정보보안 지침 준수

현재 데이터를 영구삭제 할 수 있는 디가우징 방법은?

항목 / 방식	제로클솔루션	하드웨어방식 데이터 포맷	디가우저(Degausser)	물리적파쇄
경쟁사 적용방식				
방법개요	소프트웨어 방식 TCG규격의 암호화 삭제기술 기존 Legacy 삭제기능 지원	Overwrite & ATA Security Erase 기반 데이터 삭제 방식	하드웨어적 방법 소자 장비가 발생. 자기장을 활용 HDD내의 기록삭제	드릴/천공/소각/용해 등의 방법 물리적으로 파괴하는 방식
특징	Agent프로그램설치 온라인원격삭제 및 동시삭제	삭제방식이나 하드용량에 따라 소요 시간 변동 / 최소 1시간이상	높은 신뢰, 신속성으로 다양한 매체 적용가능	가장 데이터 복구 불가능 하게하는 완벽한 방법
복구가능성	복구율 0% (*일부가능)	가능	불가 (*일부가능)	불가
디스크재활용여부	가능	가능	불가	불가
단점	서버구축형	영구삭제라고 하지만 실제로는 디지털 포렌식 복구가능	고가의 물리적장비 구입 비용 작업공간의 제안	환경문제 발생 폐기물 처리비용 발생

제로클솔루션의 데이터 영구삭제기술 및 주요기능

TCG 보안규격을 활용한 암호화 방식을 활용한 신기술적용 !!

TPM(*Trusted Platform Module_신뢰 플랫폼 모듈) Clear

- 드라이브 중 파티션(볼륨)의 OS 영역에 BitLocker의 TPM 키보호기가 활성화된 경우 이 옵션을 선택하면 TPM을 초기화

Sanitize Block Erase

- Sanitize 기능을 사용하여 매핑 테이블과 모든 블록에 기록된 데이터를 영구적으로 삭제
- Nand Flash Memory 자체적으로 Erase 기능이 존재하여 memory block에 높은 전압을 인가하여 기존의 데이터 삭제 방식

Sanitize Crypto Scramble

- SSD내부에 저장된 암호화 키를 삭제하여 더 이상 데이터에 접근하지 못하게 하는 방법
- TCG 보안 프로토콜(*Opal v1.00/v2.00/enterprise)을 통해 SSD에 접근하여 기존에 저장된 암호화 키를 삭제함

ATA Security Erase

- ATA 명령에서 지원하는 Legacy 방식으로 SSD 에서 공장 기본 쓰기 상태로 복원.
- 우선적으로 Enhanced 모드를 지원하며, TCG를 지원하면 대부분 Crypto Scramble 및 Block Erase(*Zero Fill)로 초기화

NIST 800-88 Purge / NIST 800-88 Clear

- National Institute for Standards and Technology 규격이며 기존 DoD를 대체하는 방식. 데이터 복구를 불가능하게 만드는 물리적 또는 논리적 삭제.
- 숨겨진 드라이브 (HPA (호스트 보호 영역) 또는 DCO (장치 구성 오버레이)가있는 경우)재설정 후 드라이브 유형에 따라 펌웨어 기반 명령이 실행.

Overwrite(Fill Sectors With 0 > 1 > 0 & 1) / DoD 5220.22-M & 28-STD

- Raw Device (파일 시스템이 설정되지 않은) 상태에서 모든 블록을 아래 옵션 중 선택한 옵션으로 덮어쓰기함.
- 미국 국방부(DoD)에서 권고하는 데이터 보안 및 보호를 위한 표준화 규격.

SaaS기반의 디스크 완전삭제기술

클라우드 기반 원격삭제 / 관리자 통제관리

TCG & BitLocker 지원 SSD

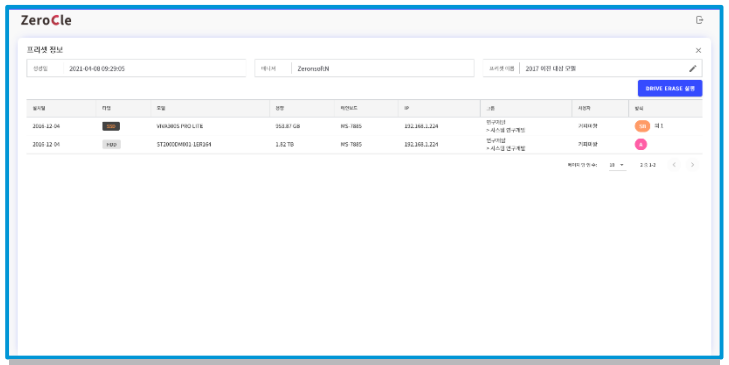
Agent기반 완전삭제 인프라

Sanitize 지원 HDD & SSD

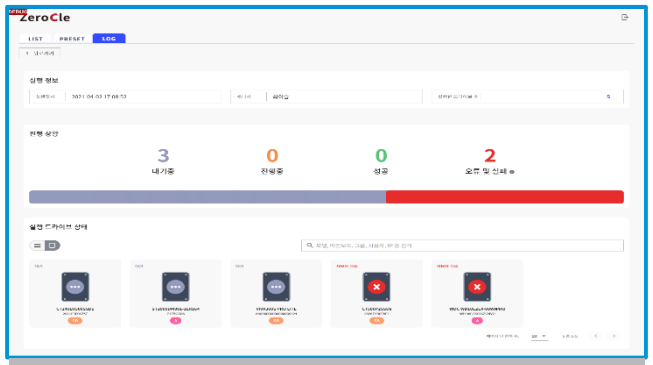
Legacy SATA & SAS HDD

제로클솔루션만의 완벽한 온라인 원격디스크완전삭제 특징

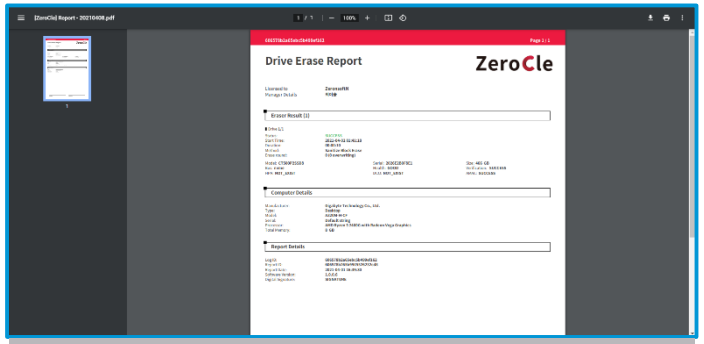
SSD,HDD등의 다양한 드라이버상의 데이터 영구삭제 절차



데이터 삭제 드라이버 선택



데이터삭제 진행상태정보



삭제완료리포트

SSD완전삭제 소요시간 : 5분 미만
(*적용기술 및 용량에 따라 편차 발생할 수 있음)

HDD완전삭제 소요시간 :

HDD기준	3회/국정원기준	5회/미국방성
소요시간	4시간25분	7시간12분

데이터삭제 특징

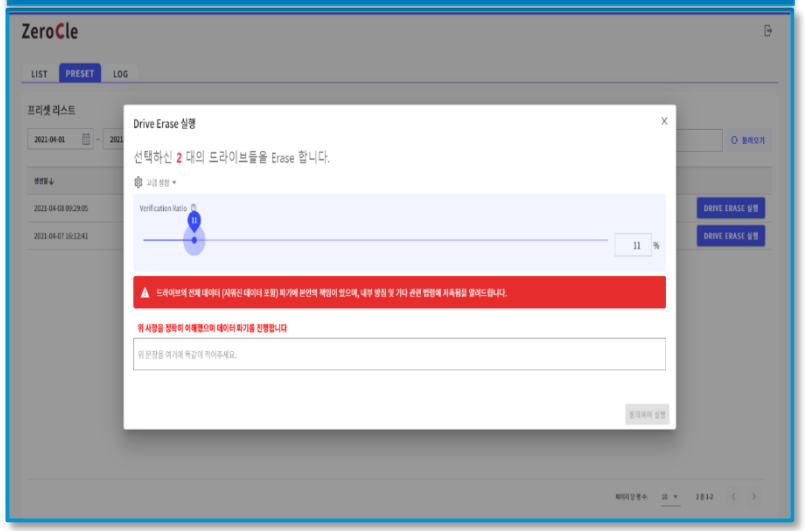
1. 온라인 원격PC에 직접 명령을 통한 데이터 영구삭제 처리
2. SSD & NvME계열에 상관없이 직접 액세스 후 안전하게 삭제
3. 숨겨진 영역(DCO,HPA) 및 재맵핑된 섹터 감지 및 삭제
4. 완전삭제검증율(*Verification ratio)을 통한 삭제된 영역의 재검증 절차방식
5. 암호화 삭제 TCG기능 포함한 드라이버 삭제기능지원
6. Sanitizer기능을 활용한 일반SSD에 삭제 시간 최소화

데이터삭제처리기술

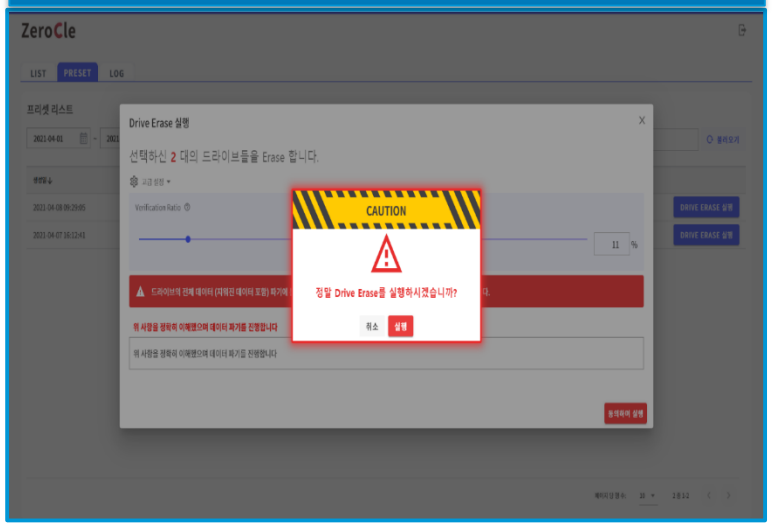
1. 국정원 기준 Overwrite 3회, 미국국방성 기준 5회 성능 준수.
2. 덮어쓰기 패턴을 자동으로 검사하는 방식의 알고리즘.
3. Linux Agent기반의 사용자프로그램 설치 후 동의실행
4. 제로클 관제센터를 통한 드라이버 간의 원격통제방식 수행.
5. 삭제보고서 및 결과 레포트 제공
6. HDD & SSD 모든 타입지원(IDE,ATA,SATA,SAS,NvME등)

제로클솔루션의 데이터 영구삭제 착오방지 시스템

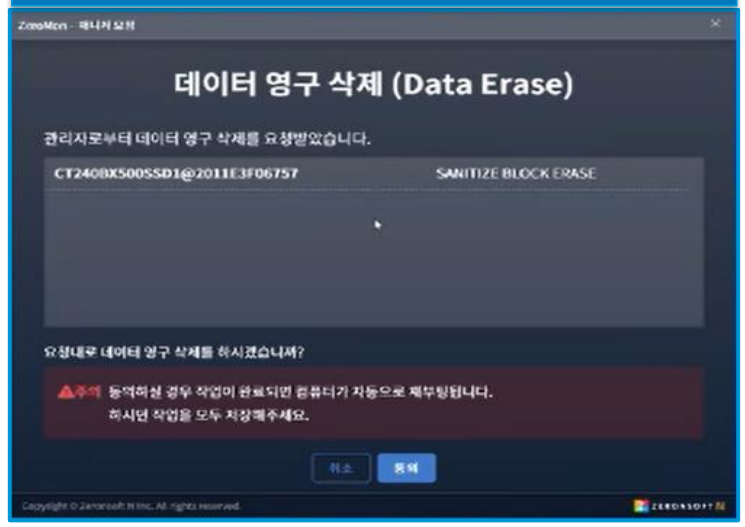
관리자 데이터 영구삭제동의 서명



관리자 데이터 파기 동의



사용자 데이터영구삭제 동의



완벽한 데이터 삭제위한 안전한 단계별 동의절차

관리자 동의

- 다수의 PC에 일괄적용시 데이터 오삭제 명령 재확인 과정
- 관리자 완전삭제 서명으로 위험방지 각인

데이터 파기 동의

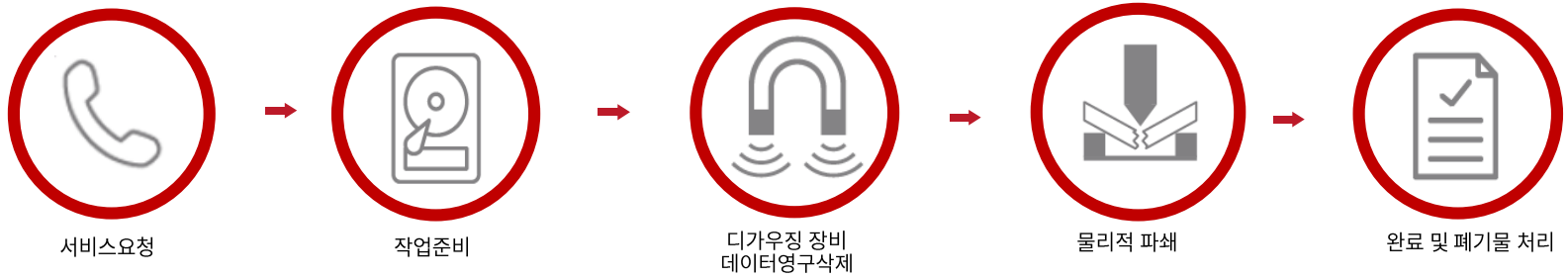
- 파기 명령시에 삭제프로세스 과정전에 재확인 및 오작동 방지
- 완전삭제시 원복불가사항 사용자에게 전달

사용자 동의

- 관리자의 완전삭제 명령시에 사용자 데이터 백업여부 재확인
- 사용자 동의 후 완전삭제 즉각 실행 진행

경쟁사 데이터영구삭제 방식 비교

타사 데이터 영구삭제 절차



- ✓ 관리자 직접 PC에서 디스크 분리 작업 필수
- ✓ 관리자 직접 디가우징 및 영구삭제 작업
- ✓ 관리자 직접 레포트 출력>스캔>메일발송
- ✓ 관리자 직접 파쇄 후 폐기물 처리작업
- ✓ 관리비용 발생 및 관행적 방식

제로클솔루션의 데이터 영구삭제 절차

- ✓ 사용자 PC에서 프로그램설치
- ✓ 사용자 동의 후 온라인 원격 영구삭제 실행
- ✓ 사용자 삭제레포트 메일 자동발송
- ✓ 폐기물 미발생 및 디스크 재활용
- ✓ 관리비용 개선 및 비용절감 및 업무경감

경쟁사제품과 비교분석

프로그램 비교	삭제방식	프로그램동작방식	데이터영구삭제방법	삭제시간	재활용여부	적용삭제범위
제로클솔루션	Linux	소프트웨어 SaaS구축형	온라인원격 영구삭제	***SSD-SED 1회기준 5분이내**	가능	원격 멀티삭제
타사프로그램	디가우징 장비 & Windows installer	물리적장비, 사용자 개별설치	물리적파괴 영구삭제	수십분~수시간	불가능	사용자 직접 삭제

경쟁사프로그램과 솔루션 소요시간 비교

데이터삭제 시 소요시간 비교

GS 인증 시험 결과, 영구 삭제 기능 실행 시 평균 약 8분 소요

(*적용기술 및 용량에 따라 편차 발생할 수 있음)

<응답시간 시험 결과 : GS 인증>

용량	응답시간					
	1회	2회	3회	4회	5회	평균
50GB	480	479	481	480	484	481
100GB	488	486	483	487	488	486
200GB	497	498	497	496	493	496

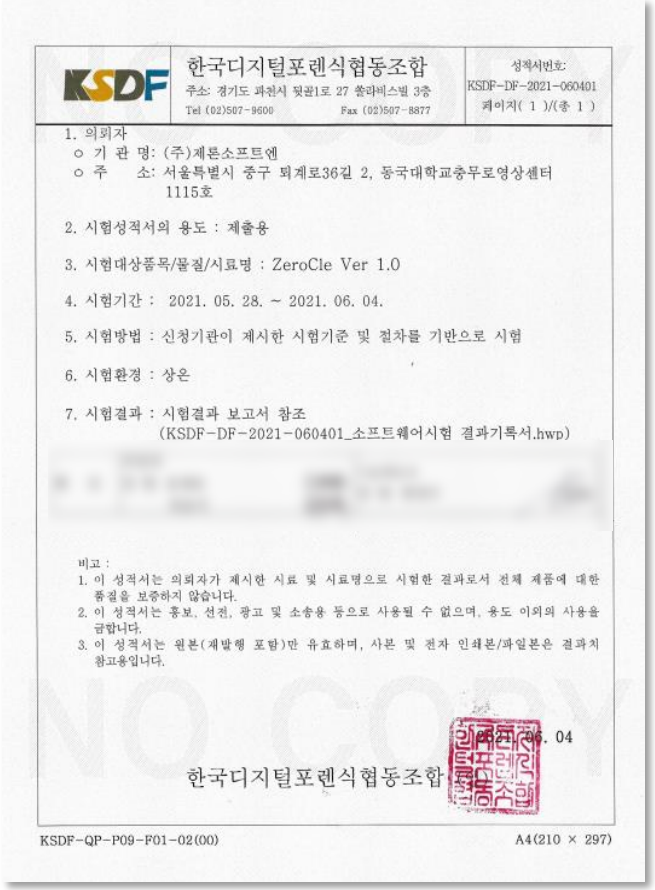
HDD 타입별 삭제 시간 시험 결과, 경쟁사 대비 신속한 영구 삭제 시간 기록

<SATA 타입 HDD 대상 영구 삭제 시간 비교>

용량	ZERONSOFT N (단위 : 분)		경쟁사 (단위 : 분)	
	Overwrite 1회	Overwrite 3회	Overwrite 1회	Overwrite 3회
250GB	**42분**	**2시간 15분**	55분	3시간 10분
500GB	**1시간 20분**	**2시간 25분**	1시간 45분	4시간 17분
1TB	**2시간 43분**	**3시간 38분**	3시간 5분	4시간 38분

국내 최고기술 포렌식업체 시험성적보고서_복구율 0%!!

한국디지털포렌식 협동조합



KSDF 한국디지털포렌식협동조합
주소: 경기도 파천시 탯골1로 27 쏠라비스빌 3층
Tel (02)507-9600 Fax (02)507-8877
성적서번호: KSDF-DF-2021-060401
페이지(1)/(총 1)

1. 의뢰자
○ 기 관 명: (주)제론소프트엔
○ 주 소: 서울특별시 중구 퇴계로36길 2, 동국대학교충무로영상센터 1115호
2. 시험성적서의 용도 : 제출용
3. 시험대상품목/물질/시료명 : ZeroCle Ver 1.0
4. 시험기간 : 2021. 05. 28. ~ 2021. 06. 04.
5. 시험방법 : 신청기관이 제시한 시험기준 및 절차를 기반으로 시험
6. 시험환경 : 상온
7. 시험결과 : 시험결과 보고서 참조
(KSDF-DF-2021-060401_소프트웨어시험 결과기록서.hwp)

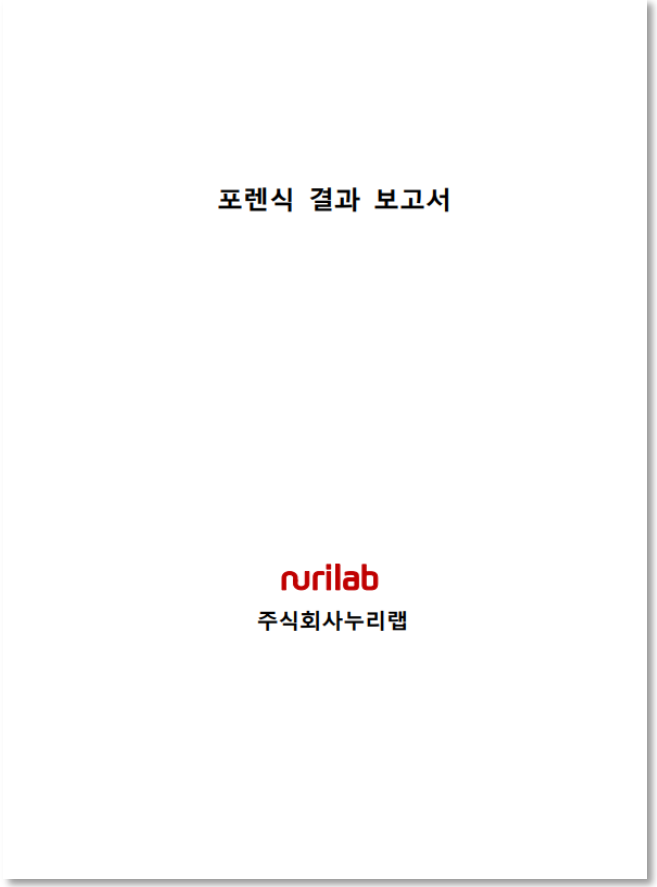
비고 :
1. 이 성적서는 의뢰자가 제시한 시료 및 시료명으로 시험한 결과로서 전체 제품에 대한 품질을 보증하지 않습니다.
2. 이 성적서는 홍보, 선전, 광고 및 소송용 등으로 사용될 수 없으며, 용도 이외의 사용을 금합니다.
3. 이 성적서는 원본(재발행 포함)만 유효하며, 사본 및 전자 인쇄본/파일본은 결과치 참고용입니다.

2021. 06. 04
한국디지털포렌식협동조합

KSDF-QP-P09-F01-02(00) A4(210 × 297)

주요고객사 :
대검찰청,경찰청,과기정통부,
산업통상자원부,행정안전부

주식회사 누리랩



포렌식 결과 보고서

nurilab
주식회사누리랩

주요고객사 :
국*원,대검찰청,국가정보기록원

포렌식 시험 분석도구(데이터복구율)

분석도구	분석용도	한국디지털포렌식 협동조합	주식회사 누리랩
Ndfinder	문서파일 내 키워드검색	-	0%
Autopsy	증거자료 포렌식툴	-	0%
AccessData_FTK_Imager	증거자료 이미지	0%	0%
TortoiseSVN	SVN사용툴	-	0%
KFOLT	증거자료 포렌식툴	-	0%
Search Everything	파일이름검색	-	0%
EnCase	미디어의 포렌식생성기툴	0%	-
R_Studio	복구 소프트웨어 및 하드 드라이브 데이터 복구 도구	0%	-
DFL-DDP Data Recovery Equipment	USB3.0 물리적 데이터 복구 장비	0%	-

✓ 시험성적보고서 별도 제공가능 함.
✓ 국세청 포렌식장비 “천둥”에서 포렌식 결과 0% 성능인증.

솔루션 도입 후 개선효과

제로클솔루션 정성적 도입효과

업무 개선 효과

데이터 정보유출에 대한 엔드포인트 보안	디스크 재활용에 따른 환경문제개선
원격시스템데이터관리로 유출우려 개선	체계적인 디가우징으로 SW관리 제품내구연한 개선
삭제레포트 폐기시스템정보 확인	관행적인 방식에서 탈피 삭제업무경감

참고_경쟁사 제품비교(*국내 및 해외)

번호	기능	제론소프트엔 (ZeroCle Solution/한국)	Blancco (Data Erasure/미국)	데이터텍 (EDE for Desktop v3.0/한국)
1	모든종류의 하드디스크지원 (SSD, SAS, SCSI, SATA 각종 저장매체)	O	O	O
2	데이터영구삭제 시 재사용 가능여부	O	O	O
3	국정원 규정 준수 알고리즘	O	O	O
4	영구삭제 착오방지 프로세스	O	X	X
5	서버/클라이언트 동시 디스크 모니터링	O	O	O
6	원격 디스크 삭제	O	X (Standard Alone제품)	X (Standard Alone제품)
7	BitLocker(*TPM폐기방식)	O	O	X
8	SED(*PSID폐기방식)	O	X	X
9	한 디스크 동시 영구삭제	O	O	X
10	로그 레포트 위변조 방지	O	O	O
11	로그 데이터베이스 관리	O	O	O
12	삭제 레포트 제공	O	O	O
13	데이터백업 원격지원	제로업솔루션백업 권장	X	백업 원격지원
14	글로벌보안표준규격(TCG1.2) 준수여부	O	O	X
15	Linux기반 디스크 지원	O	X	O
16	GS인증	O	글로벌CC인증 보유	O
17	포렌식복구방식 재검증	O	X	X

(*상기 성능비교는 자사 기능을 토대로 분류함으로 다소 이견이 있을수 있음.)

Thank you

산업폐기물 절감으로 지구온난화로 어려움에 처한 **북극곰**을 구할 수 있습니다.

ZERONSOFT N

Hewlett Packard Enterprise OEM

(주)제론소프트엔

송창민 이사 | 기술영업팀

Phone 010-7323-9153 | **Office** 070-7764-0100

E-mail zerobacknet@gmail.com | **Fax** 050-7331-9153

Address 서울시 중구 퇴계로 36길 2, 1115호

Homepage www.zeronsoftn.com