무상 진단 보고서 Ransomware Database Forensic Diagnosis

랜섬웨어 감염 Oracle 데이터베이스 진단 보고서

LockBit 계열 감염 · Oracle 19c ERP 데이터베이스 · 복구 착수 전 진단

문서 번호	DIAG-SAMPLE-01
발행일	2026-11-21 (판 1.0)
보고서 단계	무상 진단 (복구 착수 전)
진단 대상	ERP 용 Oracle 데이터베이스 1 개 (데이터 파일 6 · 컨트롤 3 · 리두 로그 8 · 임시 1)
의뢰 기관	***** (비식별)
작성 기관	(주)베일리테크 DB 복구팀

공개 샘플

이 문서는 실제 진단 사례를 바탕으로 고객사·데이터베이스·파일·서버 이름과 해시를 모두 가린 홈페이지용 샘플입니다. 수치는 실제 측정값입니다. 실제 고객 보고서에는 받은 파일 목록과 SHA-256 이 부록에 함께 실립니다.

문서 관리

구분	성명	소속	일자	서명
작성		(주)베일리테크 DB 복구팀	2026-11-21	
검토		(주)베일리테크 DB 복구팀		
승인		(주)베일리테크 DB 복구팀		

판	일자	변경 내용
1.0	2026-11-21	무상 진단 결과 발행

목차

1. 진단 결과 요약 3

2. 받은 자료와 증거 보존 4

3. 대상 데이터베이스 4

4. 감염 분석 5

5. 손상 범위 5

6. 복구 가능성 판정 5

7. 복구를 진행하면 6

8. 추가로 필요한 자료 7

9. 즉시 조치 권고 7

10. 진단의 한계 7

부록. 용어 8

1. 진단 결과 요약

복구 가능성 등급	데이터 파일 블록 보존	손상 블록	암호화된 바이트
A 복구 가능	**99.998%**	**102 개**	**0.0017%**
데이터 보존 99% 이상 + 데이터 사전 생존 (6 장 기준표)	5,112,474 / 5,112,576 블록 [계산]	데이터 파일 6 개 전체 블록 중 [측정]	1,126,400 / 64,806,072,320 B [계산]

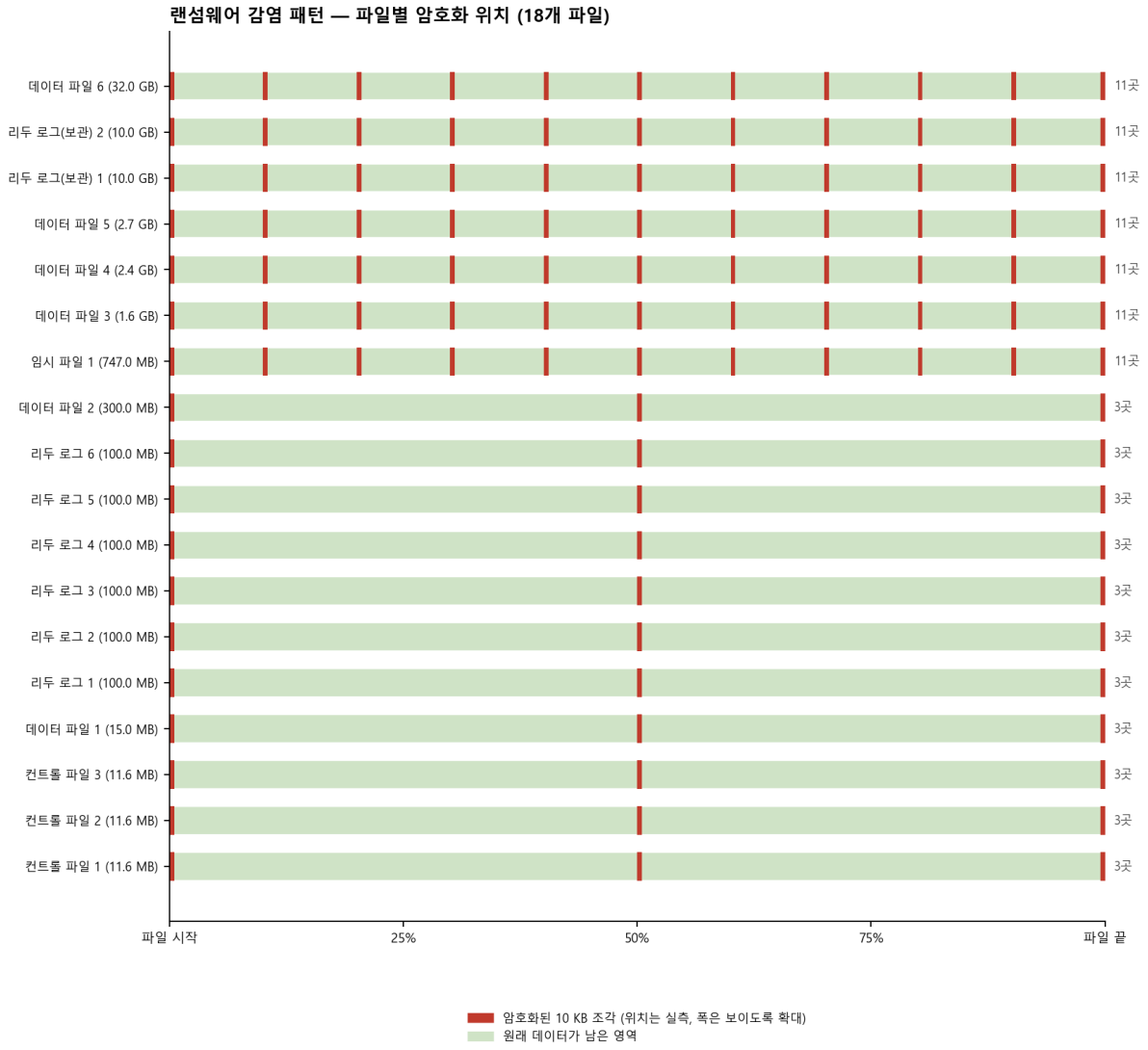


그림 1. 파일별 암호화 위치 — 18 개 파일 모두 같은 규칙(작은 파일 3 곳: 시작·가운데·끝 / 큰 파일 11 곳: 시작·10% 간격·끝)

빨간 조각만 암호화되고 나머지(초록)는 원래 데이터가 그대로 남아 있습니다. 조각 하나는 10 KB 로, 가장 큰 데이터 파일(32 GB)에서도 11 곳 110 KB 만 암호화된 것입니다 [측정]. 이런 간헐 암호화는 복호 키 없이도 대부분의 데이터를 되살릴 수 있는 근거입니다.

1. LockBit 계열 랜섬웨어가 파일마다 10 KiB 조각 몇 곳만 암호화했습니다. 데이터 파일 블록의 99.998%는 원래 상태 그대로입니다 [측정].
2. 데이터 파일 머리가 손상돼 Oracle 로 바로 열 수는 없지만, 표 구조를 기록한 데이터 사전이 살아 있어 표·열 이름과 자료형, 인덱스·제약·시퀀스 정의까지 원래대로 복원할 수 있습니다 [측정].
3. 행 손실은 손상 블록 102 개 안의 행으로 한정될 것으로 예측합니다. 데이터 파일 백업이나 export 덤프가 있으면 이 행도 보충할 수 있습니다 [예측].

고객이 결정할 일 ① 복구 의뢰 여부 ② 데이터 파일 백업·export 덤프 보유 여부 확인(8 장) ③ 운영 Oracle 버전·문자셋 확인 — 복구 DB 를 같은 환경으로 맞추기 위해.

2. 받은 자료와 증거 보존

항목	내용
받은 파일	18 개 (데이터 파일 6 · 임시 파일 1 · 컨트롤 파일 3 · 리두 로그 6 · 별도 폴더 리두 로그 2) + 랜섬 노트 2, 총 약 64.8 GB
증거 보존	원본은 읽기 전용으로만 열고, 진단은 작업 사본에서 했습니다. 작업 전후 SHA-256 이 18 / 18 일치합니다 [측정].
파일 특징	모든 파일 이름 뒤에 .lockbit 가 붙었고, 파일 크기는 원래 크기 + 272 B 입니다 [측정].

3. 대상 데이터베이스

항목	값	근거
제품·버전	Oracle Database 19c 계열	데이터 사전의 버전 문자열 [측정]
플랫폼	Windows x64 (리틀 엔디언), 블록 8 KB	블록 머리 [측정]
문자셋	KO16MSWIN949 / 국가 문자셋 AL16UTF16	데이터 사전 [측정]
업무 스키마	4 개 (가장 큰 스키마 세그먼트 1,290 개)	데이터 사전 [측정]

4. 감염 분석

항목	결과	근거
랜섬웨어 계열	LockBit 계열	확장자 .lockbit · 파일 끝 272 B 추가 · 간헐 암호화 [예측] — 악성 실행 파일 미대조
암호화 방식	파일 전체가 아니라 10,240 B 조각 3 개(작은 파일) 또는 11 개(큰 파일)만 암호화	18 개 파일 모두 같은 위치 공식에 맞음 [측정]
복호 가능성	복호 키 없음	키 없이 암호화되지 않은 블록으로 복구

파일별 암호화 위치는 1 장 그림 1 과 같습니다.

5. 손상 범위

항목	값	분자 / 분모
암호화된 바이트 (전체 파일)	0.0017%	1,126,400 / 64,806,072,320 [계산]
암호화된 바이트 (데이터 파일 6 개)	0.0012%	512,000 / 41,882,271,744 [계산]
손상 블록 (데이터 파일 6 개)	0.0020%	102 / 5,112,576 [측정]
데이터 파일 머리	6 개 모두 손상	그대로 열 수 없음 [측정]
데이터 사전	생존	표·열·사용자 정의 해석 가능 [측정]

※ 손상 블록 102 개는 암호화 위치 공식으로 계산한 블록과 정확히 같고, 서로 독립된 두 분석 절차의 블록 검사 결과와도 같습니다.

6. 복구 가능성 판정

영역	판정	근거
업무 데이터(행)	복구 가능	블록 보존 99.998% [계산] · 손상 블록 102 개 안의 행만 손실 예상 [예측]
표 구조(표·열·자료형)	복구 가능	데이터 사전 생존 [측정]

인덱스·제약	복구 가능	인덱스 3,269 개 · 제약 2,888 개 정의 해석 [측정]
시퀀스·열 기본값	복구 가능	시퀀스 62 개 · 기본값 15,477 개 [측정]
뷰·시노님·프로시저 등 코드	복구 가능	뷰 317 · 시노님 209 · 프로시저 16,424 · 함수 298 · 트리거 524 [측정]
원래 행 수 대비 복구율	복구 후 확정	원래 행 수 기준 자료 필요 [확인 필요]

※ 판정 등급 A(복구 가능): 데이터 보존 99% 이상 + 구조 정보 생존. 수치는 서로 독립된 두 분석 절차가 같은 결과를 낸 값만 실었습니다. 예상 범위는 진단 시점의 판단이며 보증이 아닙니다.

복구 가능성 등급 기준 (모든 고객 공통)

등급	이름	기준
A	복구 가능	데이터 영역 보존 99% 이상, 구조 정보(데이터 사전·카탈로그) 생존 또는 같은 DB 정상 백업 있음
B	조건부 복구	데이터 영역 보존 90% 이상, 구조 정보 일부 손실 — 추가 자료에 따라 범위가 달라짐
C	부분 복구	데이터 영역 보존 90% 미만 또는 구조 정보 대부분 손실 — 남은 데이터 조회용 추출
D	복호 키 필요	파일 전체 암호화 — 키 없이는 복구 불가

7. 복구를 진행하면

항목	내용
복구 방식	손상되지 않은 블록에서 데이터를 읽고, 데이터 사전으로 원래 표 구조를 되살려 새 Oracle 데이터베이스에 적재합니다. 서로 독립된 두 분석 절차가 같은 값을 낸 데이터만 넣습니다.
받게 되는 결과물	① 복구된 데이터베이스(Oracle Data Pump 덤프) ② 표마다 앞 100 행을 보여 주는 미리보기 엑셀 ③ 가져오기 순서와 표별 복구 내역을 담은 복원 안내서 ④ 축별 복구 결과를 담은 최종 보고서
납품 전 검증	빈 Oracle 데이터베이스에 가져오기 시험 · 응용프로그램이 쓰는 질의 유형(키 조회·조인·시퀀스·쓰기·한글)을 흉내 낸 사용 가능성 시험

진행 단계	의뢰 → 정밀 추출 → 적재·구조 복원 → 가져오기·사용 가능성 시험 → 납품
예상 기간	24 시간 [예측] — 받은 자료 약 64.8 GB(100 GB 미만) 기준

※ 예상 기간 기준(받은 자료 전체 크기): 50 GB 미만 12 시간 · 100 GB 미만 24 시간 · 300 GB 미만 36 시간 · 300 GB 이상은 별도 안내. 의뢰·자료 수령 후부터 계산합니다.

8. 추가로 필요한 자료

자료	있으면 좋아지는 것
데이터 파일 백업(RMAN 등) 또는 export·Data Pump 덤프	손상 블록 102 개 안의 행 보충
운영 Oracle 버전·패치 수준·문자셋	복구 DB 를 운영 환경과 같은 버전으로 납품
업무 기준 행 수·합계(전표·원장 등)	원래 행 수 대비 복구율 확정
감염 발견 시각·서버 정보	감염 범위 확정

9. 즉시 조치 권고

1. 감염 파일을 지우거나 덮어쓰지 마십시오. 이름 변경·복사도 원본은 그대로 두고 사본으로 하십시오.
2. 감염 서버는 네트워크에서 분리한 상태를 유지하십시오.
3. 복호 협상 전에 진단 결과를 먼저 확인하십시오. 이 사례처럼 간헐 암호화라면 키 없이도 대부분 복구됩니다.
4. 재발 방지: 백업을 운영 저장소와 분리된 쓰기 금지 저장소 또는 오프라인 매체에 보관하고, 가상화 관리 계정에 다중 인증을 적용하며, 분기마다 복원 시험을 하십시오.

10. 진단의 한계

- 무상 진단은 파일을 읽기만 한 결과입니다. 행 단위 복구 수치는 복구 작업 후 최종 보고서에서 확정합니다.
- [예측] 표시는 진단 시점의 판단이며 결과를 보증하지 않습니다.
- 랜섬웨어 계열은 파일 특징에 근거한 판단이며, 악성 실행 파일 분석은 진단 범위에 들지 않습니다.

부록. 용어

용어	뜻
블록	Oracle 이 데이터를 저장하는 단위(이 DB 는 8 KB)
데이터 사전	표·열·인덱스·사용자 등 데이터베이스 구조 정보를 담은 내부 표
간헐 암호화	파일 전체가 아니라 일부 구간만 암호화하는 방식 — 나머지는 원래 데이터가 남음
Data Pump 덤프	Oracle 표준 내보내기 파일. 고객 서버에서 가져오기(impdp)로 복원
SHA-256	파일 내용이 바뀌지 않았음을 확인하는 지문 값