

VERITAS PRESENTS:

# RANSOMWARE'S GREATEST FEARS

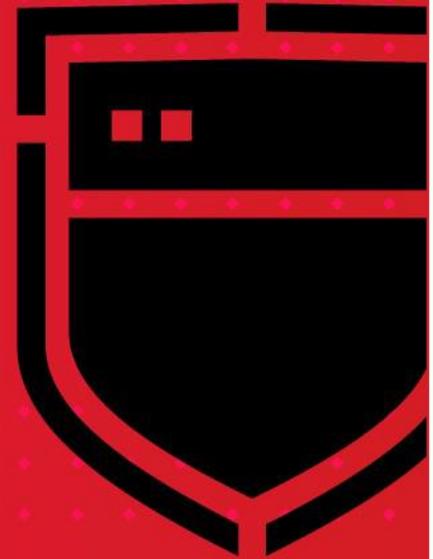
보호, 탐지, 복구를 통한 Best Practices

## 백업을 이기는 랜섬웨어는 없다

이기순 팀장

KTDS Cloud서비스혁신팀

VERITAS™



# 랜섬웨어 공격



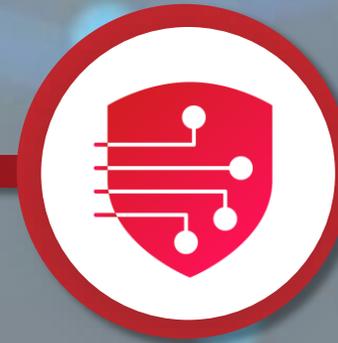
금전요구



내부 Data



복구 불가



암호화

# 랜섬웨어 증상

	Kt ds One backup 행사 기업발표자료.pptx ②	2022-01-11 오후 4:26	Microsoft PowerP...	2,908KB
	Kt ds One backup 행사 기업발표자료_1.pptx ①	2022-01-11 오후 4:26	Microsoft PowerP...	2,905KB
	Kt ds One backup 행사 기업발표자료.pptx	2022-01-11 오후 4:26	Microsoft PowerP...	2,908KB
	Kt ds One backup 행사 기업발표자료_1.pptx	2022-01-11 오후 4:26	Microsoft PowerP...	2,905KB
	Kt ds One backup 행사 기업발표자료_220104_20220111.162...	2022-01-24 오후 1:02	압축(ZIP) 파일	2,906KB
	VSD_One Backu	2022-02-07 오후 12:03	Microsoft PowerP...	5,021KB
	일반문서.png		PNG 파일	18KB

**1**

파일 형식: Microsoft PowerPoint 프레젠테이션(.pptx)  
 연결 프로그램: PowerPoint (데스크톱)  
 위치: D:\wkslee\2022\#02  
 크기: 2.83MB (2,974,542 바이트)  
 디스크 할당 크기: 2.83MB (2,977,792 바이트)  
 만든 날짜: 2022년 2월 3일 목요일, 오전 11:26:57  
 수정한 날짜: 2022년 1월 11일 화요일, 오후 4:26:52  
 액세스한 날짜: 2022년 2월 3일 오늘, 1분 전

이 이미지 출처 : <https://youtu.be/Vkjekr6jacv>

**2**

파일 형식: Microsoft PowerPoint 프레젠테이션(.pptx)  
 연결 프로그램: PowerPoint (데스크톱)  
 위치: D:\wkslee\2022\#02  
 크기: 2.83MB (2,977,710 바이트)  
 디스크 할당 크기: 2.83MB (2,977,792 바이트)  
 만든 날짜: 2022년 2월 3일 목요일, 오전 11:26:57  
 수정한 날짜: 2022년 1월 11일 화요일, 오후 4:26:52  
 액세스한 날짜: 2022년 2월 3일 목요일, 오전 11:26:57

# 랜섬웨어 예방

## 목차

1. 개요
2. 백업
  - 2.1. NAS
  - 2.2. 공 CD/DVD/블루레이
  - 2.3. 클라우드 서비스
  - 2.4. 시스템 복원
  - 2.5. 외장 하드/USB 드라이브
3. 안티 바이러스 및 OS 업데이트, 차단 솔루션 병행 사용
4. 하드웨어 / 소프트웨어적 격리
  - 4.1. 액세스 권한
  - 4.2. 기억 장치 분리
5. 읽기 전용 디스크 설정
6. 문제의 보안 허점 소프트웨어 삭제
7. 브라우저의 광고 차단 플러그인 사용
8. 정품 소프트웨어와 콘텐츠 사용 그리고 정식 프로그램 배포 사이트 확인
9. 수동 대처 방법
10. 그 외의 피해 최소화 방법

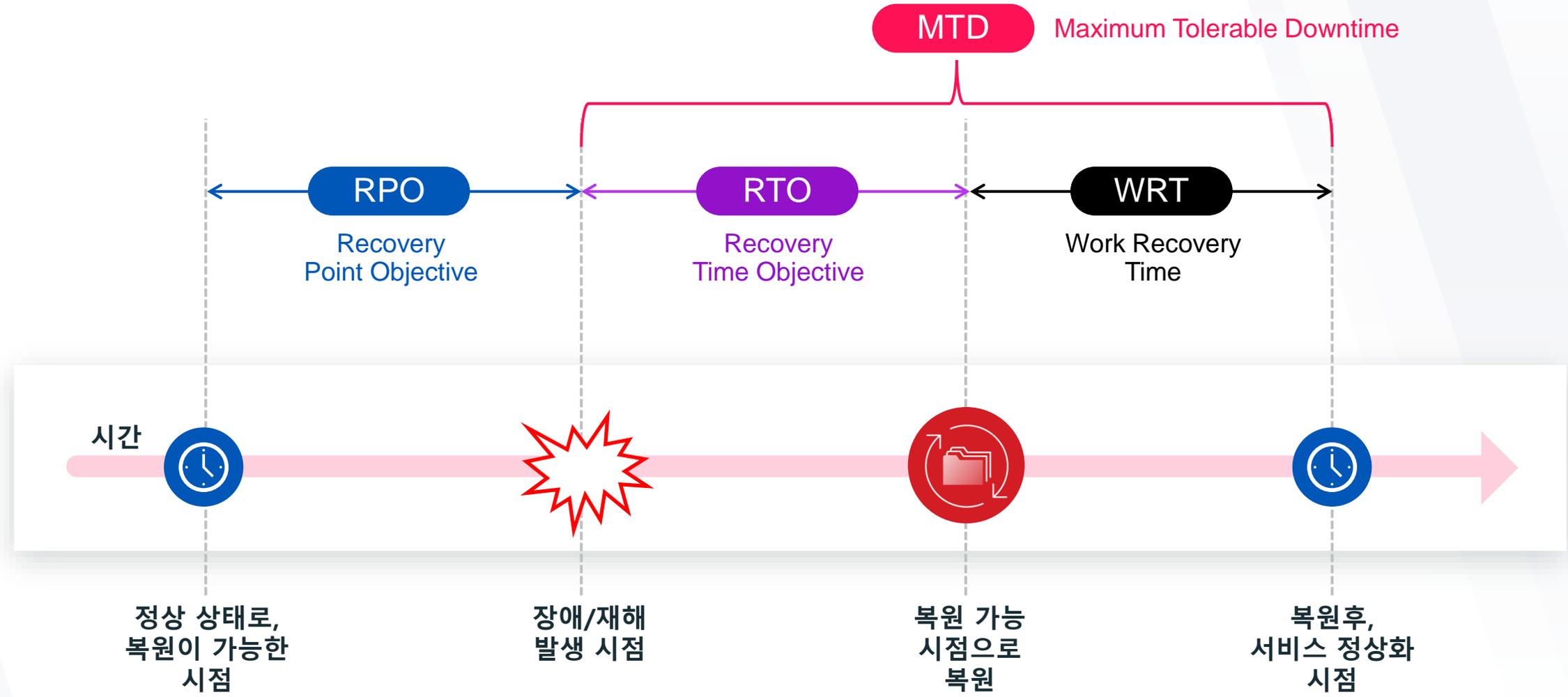
## 2. 백업

[편집]

가장 강력하고 가장 확실하며 수많은 실전 경험이 축적되고 검증된 대처법이다. 백업을 이기는 랜섬웨어는 없다. 아래 설명된 모든 방법을 시도하기 전에 백업부터 먼저 챙겨야 한다. 아래 설명된 방법들을 다 지켜서 철통방어를 한다고 해도 **창은 언제나 방패를 이겨왔다.** 백업이야말로 그 무엇보다 **최고의 보험**이다. 단 랜섬웨어 감염 **이전에** 미리 챙겨야 한다. **백업 항목을** 가서 보면 알겠지만 백업은 랜섬웨어 외에도 파일의 손상과 유실을 야기하는 수많은 재난 상황에서 가장 신뢰할 수 있는 복구 수단이다.

출처 : 나무위키 "랜섬웨어/예방법"

# 랜섬웨어 예방



# One Backup 서비스의 필요성

## 기존 백업 시스템



### 확장성

데이터 증가에 따른  
인프라 확장이 어려움



### 비용

인프라/시설/운영 및  
관리비용 발생



### 민첩성

데이터 활용 및 복구지연

## One Backup

(Backup as a Service)

### 핵심 업무에 집중

(자동화된 백업)

### 비용 절감 및 확장성

(사용한 만큼 지불)

### 품질 및 보안성 확보

(SLA 기반 품질보호)

### 신속한 재해복구

### 실패 비용 제거

(Best Practices 활용)

**RANSOMWARE'S  
GREATEST  
FEARS**

# One Backup 서비스



## One Backup

kt ds Backup as a Service

**VERITAS™**

# One Backup 서비스

국내 최대 Data Center/Network  
인프라를 갖춘 사업자

시장 점유율 1위 검증된  
백업 솔루션 사업자

대규모ITO/클라우드 사업  
역량 보유한 사업자



### 국내 최대 Data Center 보유

목동IDC1, 목동IDC2, 분당IDC, 제주IDC, 광주IDC, 여의도, 용산IDC, 강남IDC, 대구IDC, 부산IDC, 김해GDC

### 백업 솔루션 시장 점유율 1위

Ranked #1 in Backup and Recovery Software Market Share Revenue, Worldwide for 2020\*

Ranked #1 in Integrated PBBA Market Share Vendor Revenue, Worldwide 2020\*

Vendor	Market Share
Veritas	23%
Others	22%
Veeam	19%
Dell EMC	17%
CommVault	9%
IBM	14%

Vendor	Market Share
Veritas	40%
Others	30%
Oracle	5%
Barracuda	3%
Dell	23%

### 대규모ITO 사업의 안정적 운영 역량 보유

해결방안 및 재발 방지 대책 제시 (Knowledge Base)   
 OS, NW, 보안 등 각 분야 전문 기술지원

kt ds PM   
 kt ds 기술지원팀

사업의 안정적 운영 강화

### 높은 Network 대역폭 제공

kt Cloud

국내 업계 1위 자체 CDC 회선 사업자 (ISP)

Tbps급

1~2 TB

A사 1000배, N사 50배

### 다양한 백업 기능 보유 (ex. 온라인 소산, 중복제거)

중복 제거된 데이터만 전송함으로 최소한의 저장소 요구

### 통합 백업 시스템 구축 방법론 보유

계획 수립	인프라 구축	시스템 적용	인프라운영 테스트	운영 지원
<ul style="list-style-type: none"> <li>Project Management Plan 수립</li> <li>통합 백업 시스템 개선안 구축 계획</li> </ul>	<ul style="list-style-type: none"> <li>운영 백업시스템 구축</li> <li>재해복구 백업 시스템 구축</li> <li>하드웨어 인프라 구축</li> </ul>	<ul style="list-style-type: none"> <li>운영 백업시스템 백업정책 적용</li> <li>재해복구 백업 시스템 정책 적용</li> <li>백업 성능관리 시스템 구축</li> <li>마이그레이션 작업 수행</li> </ul>	<ul style="list-style-type: none"> <li>운영 백업 기능 테스트</li> <li>재해복구 백업 기능 모의 훈련</li> <li>백업 성능 관리기능 테스트</li> </ul>	<ul style="list-style-type: none"> <li>통합 백업 시스템 운영 관리 방안 수립</li> <li>운영 이관</li> </ul>

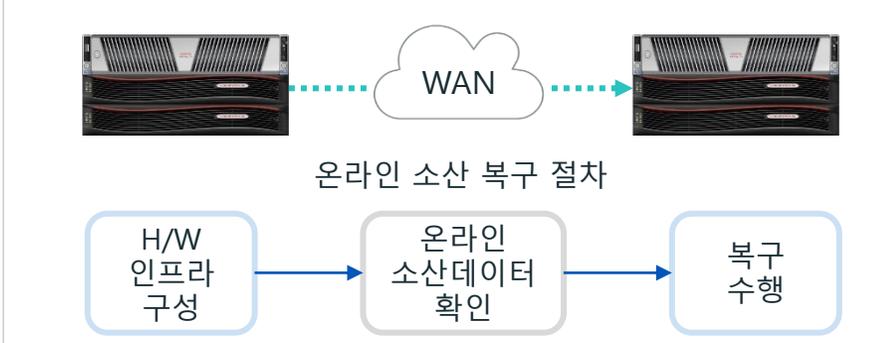
# One Backup 주요 기능(By VERITAS)

## 1. 중복제거



✓ Source, Target 중복제거로 유연한 백업 구성 가능

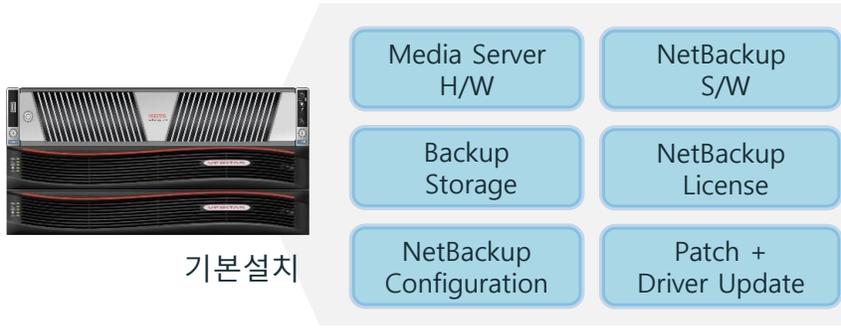
## 2. A.I.R(Auto Image Replication)



✓ WAN 최적화된 복제 수행, 사전준비 절차 없이 즉시 복구 시작



## 3. 어플라이언스



✓ 백업 마스터와 데이터 전용 처리 서버가 필요 없음

## 4. 데이터 보호

blackhat USA  
PASSED  
Canadian Common Criteria Evaluation and Certification Scheme (CCS) 인증  
Certification Report: Symantec™ Critical System Protection v5.0.5

✓ 랜섬웨어 등의 보안 위협으로부터 데이터를 안전하게 보호

# One Backup 주요 기능 (By VERITAS)

## 1. 네트워크 대역폭 조절

The image shows a 'Master Server Properties for smb' window with a 'Bandwidth' tab. A red circle highlights the 'Add' button. Next to it is the 'Add Bandwidth Settings' dialog box where 'From IP address' is set to '10.196.63.23' and 'To IP address' is '10.196.63.11' with a bandwidth of '100 KB/Sec'. Below this is a network diagram showing a '백업 서버' (Backup Server) connected to '백업장비' (Backup Appliances) and '네트워크 대역폭' (Network Bandwidth). A red box highlights the network bandwidth control area, with labels for '전체 네트워크 대역폭' (Total Network Bandwidth), '네트워크 대역폭 조절' (Network Bandwidth Control), and '활당된 네트워크 대역폭' (Active Network Bandwidth). A separate box shows '네트워크 백업 대상 서버' (Network Backup Target Servers).

✓ 고객별 NW QoS 관리로 안정적인 서비스 제공

## 2. Accelerator

The diagram illustrates the Accelerator feature. On the left, it lists '클라이언트' (Client) settings: '낮은 CPU 사용률' (Low CPU usage), '낮은 디스크 I/O' (Low disk I/O), and '낮은 LAN 사용률' (Low LAN usage). It also shows '클라이언트 파일 시스템' (Client File System) and 'Accelerator Track Log'. The main part shows '고속 백업 (변경된 블록만 처리)' (High-speed backup (process only changed blocks)). It compares '이전의 full 백업 이미지' (Previous full backup image) with 'Optimized Synthetic full (새로운 full 백업 이미지)' (Optimized Synthetic full (new full backup image)). The process is labeled 'Accelerator incremental'. Three steps are listed: 1. Track log를 통한 변경 블록 식별 (Block identification via track log), 2. 변경된 블록은 인라인으로 처리 (Changed blocks are processed inline), and 3. Synthetic full 백업 생성 (Synthetic full backup creation).

✓ 변경된 데이터 블록만 백업, 빠르게 새로운 전체 백업본 생성

## 3. Intelligent Garbage Collection

**시점:** 보관주기 만료 이후 즉시      **대상:** 백업 이미지 단위

**절차:**

DATA → BACKUP → DEDUPE → STORAGE → EXPIRATION → 공간회수

- 1 백업 만료 & 삭제카탈로그
- 2 중복 제거된 카탈로그 업데이트
- 3 DEDUPE 데이터 삭제 & 공간확보

✓ GC로 인한 백업, 복구 성능의 저하가 없음



## 4. Hybrid Cloud 통합 솔루션

The diagram shows a 'Hybrid Cloud' solution. On the left, there are screenshots of a dashboard with charts and tables. On the right, there are six boxes listing benefits: '복잡성 해소' (Complexity reduction), '손쉬운 관리' (Easy management), '성능 최적화' (Performance optimization), '이벤트 식별' (Event identification), '백업실패 여부 파악' (Backup failure identification), and '비용 최적화' (Cost optimization).

✓ Hybrid Cloud 이기종 IT환경에서 통합 인사이트를 제공

# One Backup 서비스 대상 고객

## 소규모 백업이 필요한 기업

- ~ 10TB 미만의 소규모 백업
- 자체 백업 시스템 구축/투자 부담
- 백업 시스템 운영 어려움
- 사업 초기 단계

## 2 차(소산) 백업을 고려 중인 기업

- 기존 백업 시스템 운영 중
- Tape 기반 소산 백업 전환 검토
- 원격 소산 필수 사업장
- 2차백업의 효율적 운영

OneBackup  
kt ds Backup as a Service

## KT Cloud 이용 고객

- 기존 KT Cloud 이용 고객
- 고성능 대용량 백업 필요
- On-premise & KT Cloud 통합 백업

## KT Cloud 포함 다수 Cloud 이용 고객

- 기존 백업 시스템 운영 중
- 자체 백업시스템 구축/투자 어려움
- Multi/Hybrid Cloud에 따른 백업운영 어려움
- 고성능 백업시스템 필요

# One Backup 구축 사례

## ETOOS

- 세계최초 메타버스 교육 플랫폼
- 온·오프라인 교육 플랫폼 기업  
'이투스교육'의 고등 온라인 강의 사이트
- 'Easy To Study'의 줄임말



### 프로젝트 개요

프로젝트 명 : 이투스 메타버스 플랫폼 구축사업

프로젝트 기간 : '21년 02월~22년 06월

VM 49대(컨테이너 15대 포함)

### 이용 현황

메타버스 플랫폼 100G, 일 증분백업, 주 Full 백업

### 도입 기대 효과

- ❖ One Backup 서비스 이용으로 장비 구축에 필요한 초기 비용 절감
- ❖ 이용량에 따른 과금으로 사용자가 불필요한 백업에 대한 관리 가능
- ❖ 백업 증가량 변동에 따른 과금  
→ 기존 타 백업 시스템 대비 사용량 기반 과금으로 비용 효율 우수
- ❖ 백업 서비스 운영 전문가의 지원
- ❖ 백업량 변동에 따른 백업 실패 원인 제거

# 랜섬웨어 예방

## 목차

1. 개요
2. 백업
  - 2.1. NAS
  - 2.2. 공 CD/DVD/블루레이
  - 2.3. 클라우드 서비스
  - 2.4. 시스템 복원
  - 2.5. 외장 하드/USB 드라이브
3. 안티 바이러스 및 OS 업데이트, 차단 솔루션 병행 사용
4. 하드웨어 / 소프트웨어적 격리
  - 4.1. 액세스 권한
  - 4.2. 기억 장치 분리
5. 읽기 전용 디스크 설정
6. 문제의 보안 허점 소프트웨어 삭제
7. 브라우저의 광고 차단 플러그인 사용
8. 정품 소프트웨어와 콘텐츠 사용 그리고 정식 프로그램 배포 사이트 확인
9. 수동 대처 방법
10. 그 외의 피해 최소화 방법

## 2. 백업

[편집]

가장 강력하고 가장 확실하며 수많은 실전 경험이 축적되고 검증된 대처법이다. 백업을 이기는 랜섬웨어는 없다. 아래 설명된 모든 방법을 시도하기 전에 백업부터 먼저 챙겨야 한다. 아래 설명된 방법들을 다 지켜서 철통방어를 한다고 해도 창은 언제나 방패를 이겨왔다. 백업이야말로 그 무엇보다 최고의 보험이다. 단 랜섬웨어 감염 이전에 미리 챙겨야 한다. 백업 항목을 가서 보면 알겠지만 백업은 랜섬웨어 외에도 파일의 손상과 유실을 야기하는 수많은 재난 상황에서 가장 신뢰할 수 있는 복구 수단이다.

백업을 이기는 랜섬웨어는 없다.

출처 : 나무위키 "랜섬웨어/예방법"

# “데이터 금고” 백업관리 지원사업

## 랜섬웨어 범정부 대응...기반시설·중소기업 보안 강화

중소기업 '데이터금고'로 백업-암호화-복구 체계적 지원

2021.08.05 | 과학기술정보통신부

갈수록 더 교묘해지고 악랄해지는 랜섬웨어 공격에 대응하기 위해 정부 관련부처가 팔을 걷고 나서 방안을 마련했다.

국가중요시설의 기반시설 지정 확대 및 정부출연연구원 등 보안을 강화하고, 'SW 개발보안 허브' 구축 등 SW 공급망 보안을 높이기로 했다.

또 대처 여력이 부족한 중소기업은 '데이터금고'를 통해 '데이터 백업'뿐만 아니라 '데이터 암호화', '데이터 복구' 까지 체계적으로 지원하고 랜섬웨어 대응 3중 패키지를 제공한다.

아울러 일반국민은 '내 PC 돌보미 서비스'를 통해 사용하는 PC와 IoT 기기가 랜섬웨어에 취약한지 여부를 원격으로 점검하고 개선까지 지원하기로 했다.

랜섬웨어에 안심할 수 있는  
디지털 환경을 구축하겠습니다!

01 예방 국가중요시설 - 기업 - 국민 수요자별로 선제적 지원하겠습니다

특정한 국가중요시설 관리 체계 구축

중소기업 보안역량 지원 강화

대국민 랜섬웨어 면역력 향상

# THANK YOU

VERITAS™

Copyright © 2022 Veritas Technologies, LLC. All rights reserved. This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.

