정보자산 보호를 위한 최종 방어 "백업 및 복구"

X86 서버 백업 솔루션 소개

2018.04 (Ver 1.0)

세종정보보안 Converter

TANDBERG DATA

정보자산 보호를 위한 최종 방어 "백업 및 복구"

X86 서버 백업 솔루션 소개 | Contents

Chapter I X86 서버 백업 필요 요건

01 APT/랜섬웨어(Ransomware) ?

APT(Advanced Persistent Threat)는 ?

출처 : http://www.bloter.net/archives/221705

01 지능적 (ADVANCED)

▪ 공격자는 코딩 기술, 이전에 알려지지 않은 취약점을 찾아내 이용하는 능력 등 공격 대상의 보안 약점을 악용하는 데 필요한 상당한 기술적 능력을 갖추고 있습니다.

02 지속적 (PERSISTENT)

▪ 일시적인 기회에 한 번 공격하고 마는 단기 해킹과 달리 APT는 수년에 걸쳐 진행되기도 하며 좀더 중요한 여러 정보에 액세스하기 위해 다양한 수단을 활용하여 시간을 두고 여러 가지 보안 위협을 가합니다.

03 위협 (THREAT)

▪ APT 공격을 가하는 개인, 집단 및 조직은 동기(랜섬웨어 감염을 통한 금전적 이익, 사이버 테러 등)를 갖고 있으며, 공격을 성공시키는 데 필요한 능력과 리소스를 보유하고 있습니다.

목표 설정 및 사전 조사 → 메일 이용 악성코드 발송 → 악성코드 최초 감염 → 내부망으로 확대 백도어 및 툴 설치 → 권한 상승 및 탈취 → 내부인프라 장악 → 보안 사고유발

믿을 만한 지인이나 회사 등으로 가장해 '사회공학적(social engineering)기법'의 공격을 감행

01 APT/랜섬웨어(Ransomware) ?

스피어 피싱 이메일을 이용한 APT 공격 방법

출처 : 한국과학기술정보연구원 ReSEAT 스피어 피싱 예방을 위한 국방 사이버 보안관리 대책 연구

악성코드가 삽입된 첨부파일 등을 열어보도록 유도

(스피어 피싱 이메일 중 94%가 악성 코드가 삽입된 첨부파일을 사용하며,
압축된 형태인 .lzh, .rar, .zip 파일 형태로 비밀번호를 걸어 보안솔루션을 우회)

첨부 파일의 위험 요소를 제거하는 방어 기술이 필요

악성코드가 숨겨 있는 URL 링크를 클릭하도록 유도

(악성코드가 위치한 URL 링크(이미지 등으로 위장)를 클릭하면
사용자가 인지하지 못하는 사이에 단말기에 악성코드가 설치)

메일 본문의 링크에 대한 실시간 방어 기술이 필요

목표지향적 공격의 약 91%가 스피어 피싱 이메일 사용
기존의 메일 관련 보안 솔루션은 "수신 단계"에서만 방어
수신 이후에 메일 내용을 열람하는 단계의 대응은 불가

01 APT/랜섬웨어(Ransomware) ?

APT 공격으로 발생 가능한 보안 사고는 ?

정보 유출

회사의 중요 정보(고객 개인정보, 회사 기밀 정보 등)가 외부로 유출되어 오남용(고객 정보의 매매 행위 등)이 발생하는 상황

→ 개인정보보호법 등 법규 위배 및 민사상 소송 등 발생

정보 위변조 (랜섬웨어)

랜섬웨어 등에 의한 회사 중요 정보의 암호화 및 위변조가 발생하여 정상적인 서비스 및 업무 처리가 불가

→ 최악의 경우에는 정보 자산의 손실로 회사 생존의 문제 발생

금전적 손실

스피어 피싱 등을 이용하여 거래 대금 등을 해커의 계좌로 송금하여 금전적인 손해 발생 및 거래 상대방의 신뢰도 저하 발생

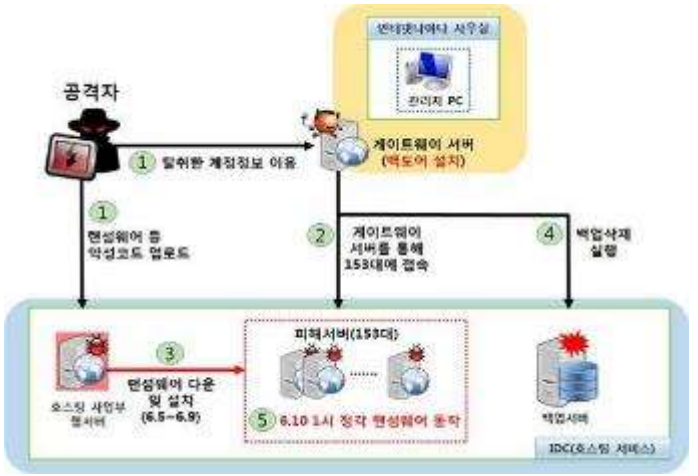
→ 외국 제3의 계좌로 이체를 하거나 인출하여 회수가 불가

인터넷나야나 랜섬웨어 감염 사태

출처 : http://www.ddaily.co.kr/news/article.html?no=157523

"보안은 허술했고 공격은 정교했다"

[디지털데일리 최민지기자] 13억원에 달하는 비트코인을 해커 손에 쥐어주고 5000개 이상의 피해 홈페이지를 발생시킨, 최악의 랜섬웨어 사태에 대한 중간조사 결과가 나왔다. **보안체계는 취약했고, 공격은 정교했다는 평이다.**



미래창조과학부(이하 미래부)는 호스팅 업체 인터넷나야나 침해사고 중간조사 결과, 중소 인터넷기업을 대상으로 한 **지능형지속위협(APT)과 에레버스(Erebus) 랜섬웨어 공격이 결합된 사고**라고 28일 밝혔다.

해커는 사전에 탈취한 계정정보를 활용해 인터넷나야나의 통신용 게이트웨이 서버(고객서버 우회접속 경유지) 및 호스팅 사업부 웹서버(악성코드 유포지)를 해킹해 공격 거점을 마련했다. 최초 계정정보 유출 경위는 현재 조사 중이다.

이후 해커는 고객서버와 백업서버에 대한 우회로 원격 접근하기 위해 통신용 게이트웨이 서버를 경유, 호스팅 웹서버에 [redacted] 어를 설치했다. **동시에 자체 백업파일 2종과 백업서버 파일까지 복구 불가능한 수준으로 삭제했다.**

중요 정보 자산에 대한 물리적으로 분리된 백업 필요

해커는 지난 10일 오전 1시 153대 고객서버에 설치된 랜섬웨어가 동시 실행되도록 설정해 데이터베이스, 이미지, 프로[redacted]

미래부는 유사 사고의 재발방지를 위해 국내 기업들의 기본적인 보안관리 강화를 요청했다. 특히, 네트워크 보안 모니터링 체계 구축, 관리용 단말의 보안강화(전용단말, 일회용 패스워드 사용 등) 및 강화된 백업정책(높은 수준의 접근통제, 오프라인 백업 등)을 강조했다.

아울러, 미래부는 내달부터 150여곳의 호스팅 사업자에 대해 취약점 점검·지원을 실시하는 한편 예상하지 못한 기업의 **랜섬웨어 사고에도 피해를 안전하게 복구할 수 있도록 백업보안 가이드를 제정·보급할 계획**이다.

관련 기사로 분석한 보안 대책의 문제점과 개선 방안

01

에레보스 랜섬웨어는 지난 2월 국내에서 처음 발견

2월 발견 즉시 대응 방안 적용

랜섬웨어 사전 방어

02

원본 파일을 포함한 내부 백업 및 외부 백업 모두 랜섬웨어에 감염

별도의 물리적 소산 백업

백업 복구로 사후 조치

"Zero-Day"나 공격에 대한 분석 및 방어 방법이 없는 "Unknown" 공격이 아니었으므로
발견 즉시 패치를 적용하고, 물리적 소산 백업으로 대응하였으면 피해의 최소화 가능

03 APT/랜섬웨어 대응 방안

APT/랜섬웨어 방어 전략 ?

출처 : 한국랜섬웨어침해대응센터 긴급 랜섬웨어 침해 보고서 (2017. 5. 14)

01 예방이 최선의 방어

랜섬웨어는 악성코드 역사상 최초로 '돈되는 바이러스'이기 때문에 빠른 확산속도로 다양한 형태의 변종으로 진화되어 이번 워너크라이와 같이 글로벌과 우리 사회을 위협하고 있다.
사용자들에게 아무리 주의를 당부해도 날마다 새롭게 진화하는 해커의 기술을 당할 수 없다.
그 이유 중 하나는 해커와 방어자 간'기술정보의 비대칭'문제다.
해커는 시장의 모든 백신엔진과 차단 엔진을 테스트 후 랜섬웨어를 침투시킬 수 있는 기술을 보유하고 있으나 보안회사들은 백신 혹은 차단제품을 공개하기 때문에 랜섬웨어를 100% 차단할 수 없다.

02 사전 백업은 랜섬웨어 방어의 최후의 보루

새로운 공격유형에 대한 방어는 새로운 기술과 정책 대응이 필요하다.
랜섬웨어는 과거의 침투기술을 지능화하고 암호화하여 금전을 요구하는 새로운 형태의 사이버공격이다.
이러한 공격으로부터 중요자료를 보호하기 위해서는 **지능형 침투 차단기술 개발**과 **데이터 백업기술의 멀티레이어 대응방법이 필요**하다.
이럼에도 불구하고 데이터백업에 대한 기술적 표준과 정책이 부재하여 랜섬웨어 대응에 혼란을 겪고 있는 실정이다.
따라서 현재 가장 시급한 것은 보안적 관점에서 데이터백업 기술의 표준을 마련하고 백업을 의무화 시키는 정책수립과 조치다.
그런 이후 해커와의 거래를 불법화시켜 우리나라가 랜섬웨어 해커의 수익성 높은 놀이터가 되는 것을 막아야한다. 막지 못하면 랜섬웨어 공격이 장기화될 것이다.

랜섬웨어 방어를 위한 글로벌 표준

1. 랜섬웨어가 침해하지 못하는 전문 백업제품을 사용하여 사전에 백업 받을 것
2. 랜섬웨어 차단 가능한 백신으로 업데이트할 것
3. 이메일 첨부파일 열람에 주의를 기울일 것
4. 윈도우 업데이트로 보안취약점을 없앨 것
5. 이메일 링크로 접속 말고, 직접 접속할 것

랜섬웨어 등 외부 공격에 대한 복구를 위해
OS 및 중요 데이터에 대한
물리적으로 분리된 소산 백업 필요

03 APT/랜섬웨어 대응 방안

백업 관련 보안 대책의 문제점과 개선 방안

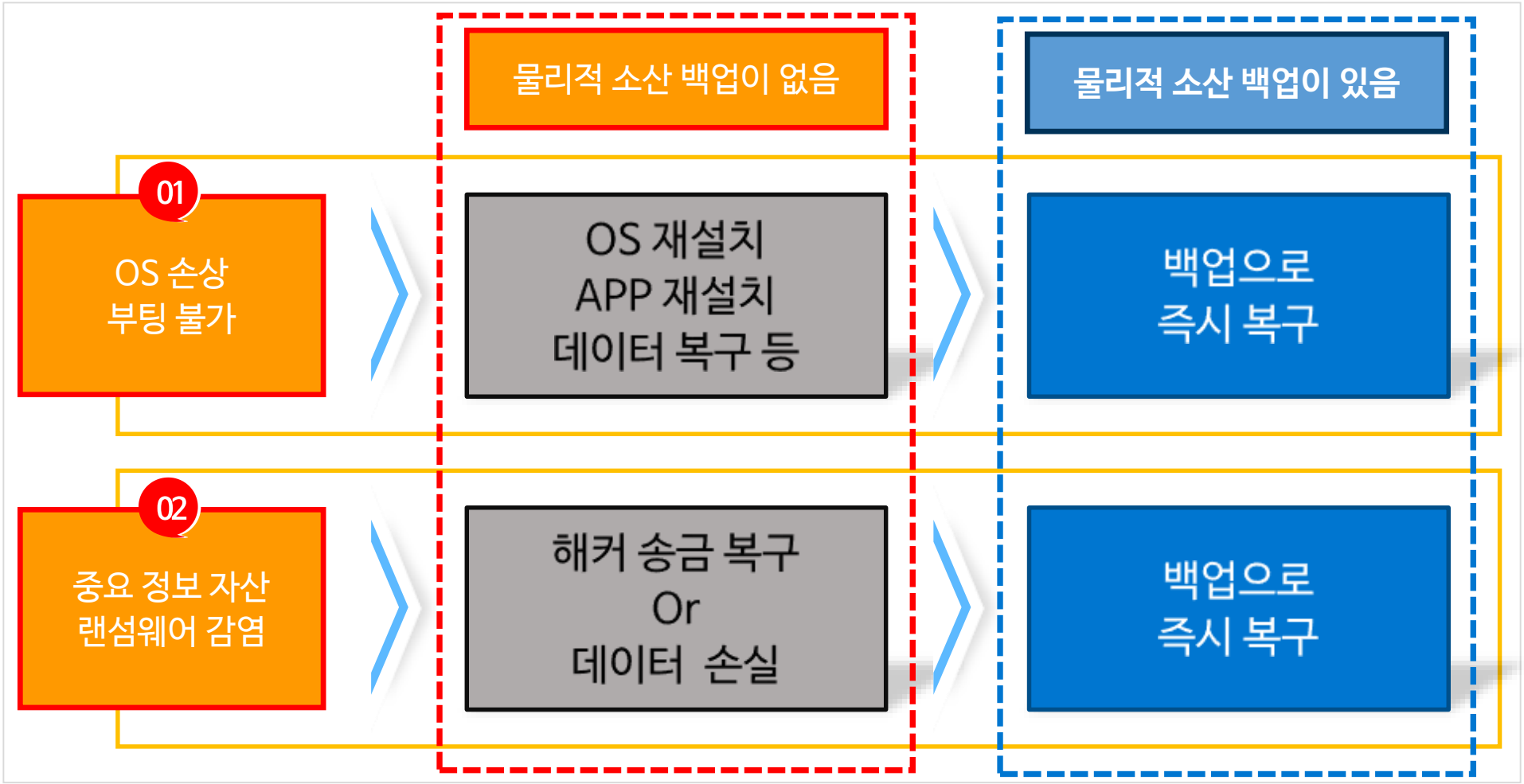
01 PC 및 X86 서버 (Windows/Linux)

- 개인 PC 및 Windows/Linux 서버 OS에 대한 백업이 없는 경우가 많음
- HDD의 물리적 장애나 해킹 등으로 OS 부팅이 불가능한 경우 복구에 많이 시간이 소요됨(OS 및 App 재설치, OS 패치 적용, 데이터 복구 등)
- 특히 APT 공격으로 침해 사고가 발생한 경우에는 추가 보안 사고 예방을 위하여 OS에 대한 신규 설치가 필요함(데이터만 복구하는 경우 숨겨진 해킹 툴에 의한 사고 재발 가능)

02 보안 서버 (Appliance 장비)

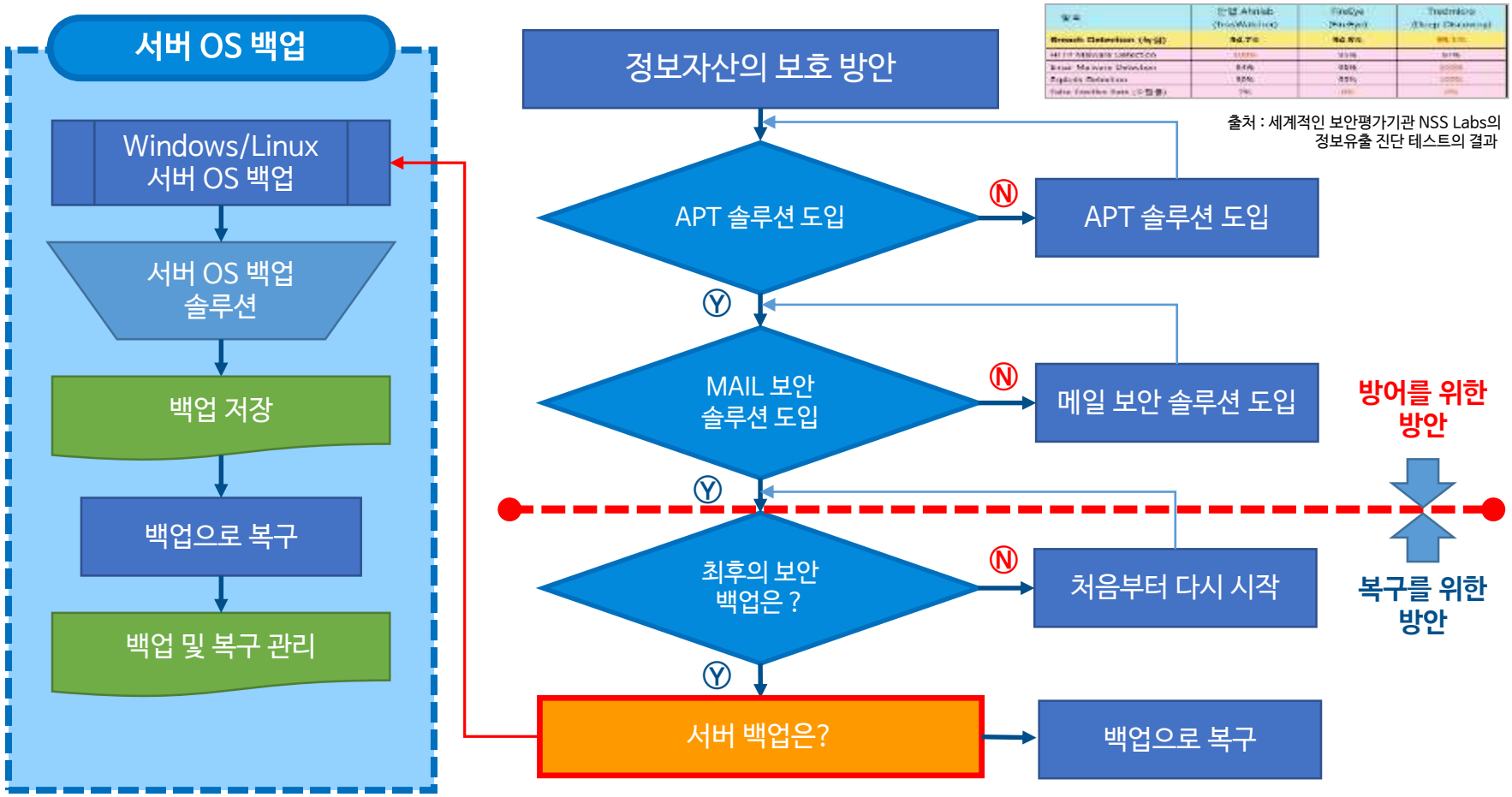
- 대부분의 보안 장비(Appliance)는 비용 절감 및 보안(?)을 위하여 Linux(Cent 등)을 사용하고 있으므로 해커가 OS 구조상의 문제점에 대해서 잘 파악하고 있음
- 보안 장비에는 사용자의 거래 정보, 개인 정보 및 보안 관련 로그 등이 파일이나 Open Source DB(마리아, 몽고 등)에 저장되어 있음
- 해당 로그는 관련 법규(개인정보보호법, 전자금융감독규정 등)에서 위변조가 되지 않도록 일정 기간 보관이 요구되고 있음
- 보안에서 중요한 정보를 저장하고 있음에도 비용이나 보안적인 측면에서 별도의 소산 백업을 수행하지 않고 있어서 물리적인 장애나 해킹 등의 사고가 발생하는 경우 손실이 발생할 수 밖에 없음

백업 관련 보안 대책의 문제점과 개선 방안



03 APT/랜섬웨어 대응 방안

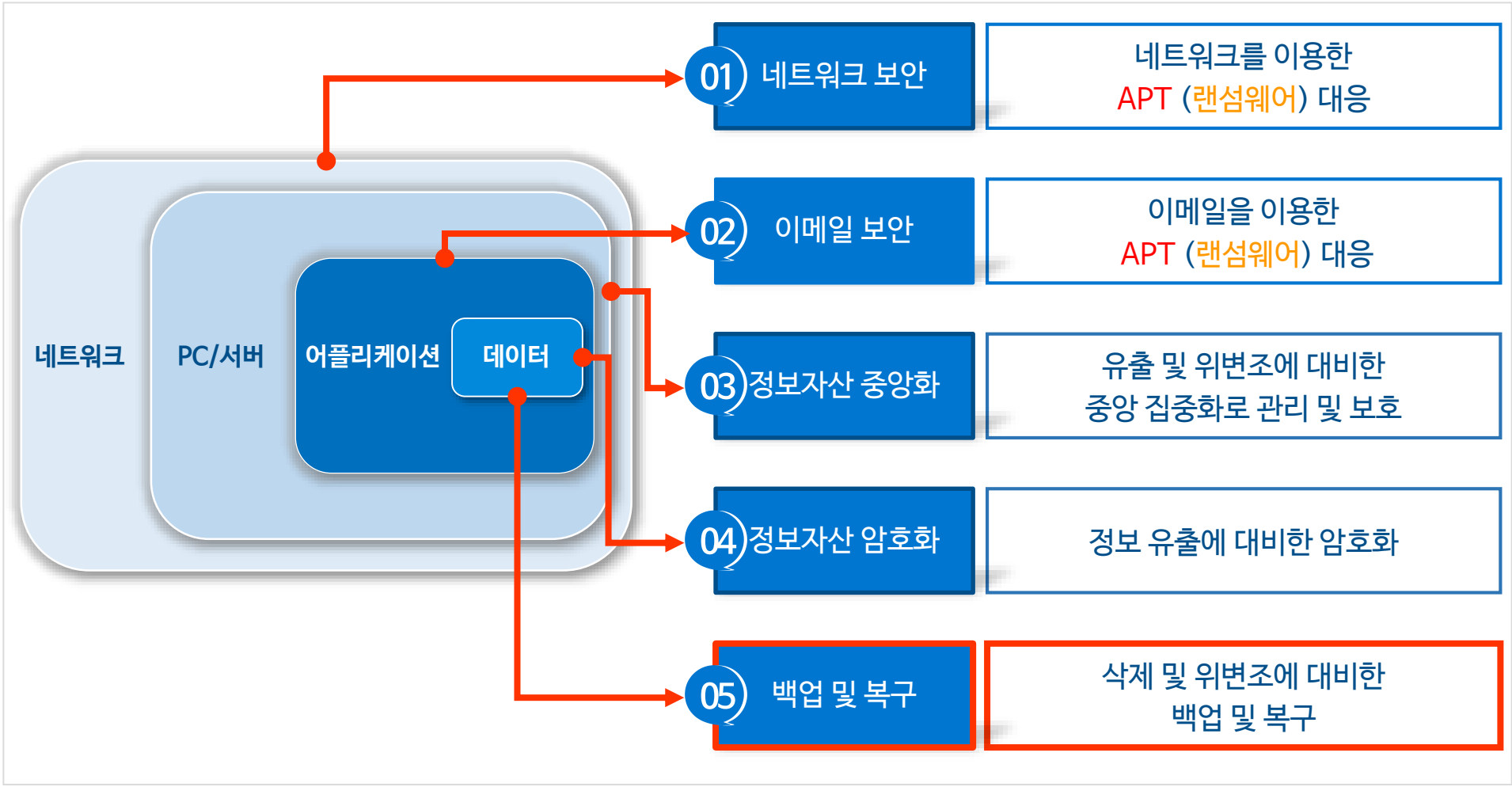
NSS Labs의 테스트의 결과를 보면 어떤 APT솔루션도 100% 탐지가 되지 않음



출처 : 세계적인 보안평가기관 NSS Labs의
정보유출 진단 테스트의 결과

03 APT/랜섬웨어 대응 방안

중요 정보자산 보호를 위한 다단계 정보보안의 구축 및 운영 필요



03 APT/랜섬웨어 대응 방안

APT 공격에 대한 피해를 최소화 하는 방안은 ?

01 보안정책 및 패치 적용

보안 관련 솔루션의 패치 등은 최신 정보로 적용하고,
새로운 형태의 공격(APT 등)에 대비한 **통합 메일 보안 솔루션** 도입

메일 APT 공격에 대한 방어를 실시간으로 적용하여 운영

02 정보자산 파악 및 보호

회사의 중요 정보(고객 개인정보, 회사 기밀 정보 등)가 어디에 어떻게
저장 및 활용이 되고 있는지 확인 필요

PC 및 서버 등에 존재한 개인정보 검색 솔루션 도입

03 정보자산 집중화

PC 및 서버 등에 분산되어 저장 및 활용이 되고 있는 중요 정보를
중앙 집중 관리하고 접근 및 권한 통제하여 유출을 방지

중요 정보 집중 관리 솔루션 도입

04 암호화 및 백업(소산)

회사의 중요 정보는 암호화하여 유출이 되는 경우에도 오남용을 방지하고
랜섬웨어 등의 위변조 발생에 대비한 백업 및 소산을 적용

정형(DB),비정형(파일) 암호화 및 백업(소산) 솔루션 도입

Chapter Ⅱ X86 서버 백업 솔루션
Zconverter

01 X86 서버 백업 솔루션 도입 필요성

☑ 서버의 장애나 해킹이 발생하는 경우 OS와 App을 재설치 하지 않고 신속하게 복구

01 용도	랜섬웨어와 같은 사이버 테러 또는 HDD 장애로 x86서버의 시스템 장애가 발생하는 경우 쉽고 빠르게 복구하는 백업 솔루션
02 도입사유	OS와 데이터 손상이 발생하는 경우 재설치 없이 신속하게 복구
03 적용시점	랜섬웨어와 같은 사이버 공격 등으로 데이터가 정상 사용 불가능한 경우 OS 업데이트 혹은 설치된 S/W들의 충돌 인한 부팅이 안 될 때
04 도입 사례	▪ 경찰청 112시스템 통합 프로젝트 (x86서버 400대,PC 1000대) ▪ 삼성전자 시스템 백업 복구 (200 copy) ▪ 한화생명 전사 x86서버 (x86서버 100대 + VMware 200대) ▪ LG화학 64bit 윈도2008서버 시스템 백업 (300대) ▪ 한국 IBM 송도 데이터센터 (VMware 200대)

서버의 OS 및 데이터를 정상적으로 사용하지 못하는 경우 최후의 대책으로 백업 이용 복구 필요

02 ZConverter Server Backup 주요 기능

Windows , Linux 서버의 OS 디스크 장애 및 랜섬웨어 등에 대비한 백업 및 복구

- X64/ IA64 윈도 서버 2012/2008/2003 시스템 백업 복구 지원
- CentOS/Redhat Linux 시스템 백업 복구 지원
- No Reboot/ No Agent 기술로 신속한 OS백업 환경 구축
- 변경분 복구 (Delta Recovery) 기술로 대용량 데이터를 보유한 서버의 신속한 복구
- AWS 클라우드 가상 서버 백업 복구 지원
- 윈도/리눅스 서버의 라이브 백업 복구 지원
- VMware/Hyper-V/Xen/KVM 가상서버 백업 복구 지원
- 전체 백업/ 증가분 백업/ 변경분 백업/ 업데이트 백업 지원
- 스마트 스케쥴링 백업 지원으로 백업 저장소 공간 절약
- 스마트 이메일 리포트 기능을 통한 백업 상태 관리 지원
- 파일/폴더 선택 백업 복구 지원
- 다중 서버/ 다중 파티션 동시 시스템 백업 지원
- 운영 시스템 자동 검색 및 등록 지원
- 중앙관리 백업 복구 기능 지원

02 ZConverter Server Backup 주요 기능

Windows , Linux 서버의 OS 디스크 장애 및 랜섬웨어 등에 대비한 백업 및 복구

01 다양한 복구 지원

- 이 기종서버 베어메탈 (※주1) 복구 지원
- 운영서버의 하드웨어 장애 발생시 이 기종 복구 가능

03 편리한 백업 및 복구

- Agent 설치 없이 백업 가능(Windows만 해당)
- Production 서버를 재 부팅을 하지 않음

제조사의 개발자 및 엔지니어 레벨 기술지원 제공과 기본적인 Customizing 요청 시 지원가능

02 다양한 보고서 지원

- 스마트 데일리 리포트
- 백업 대상 서버가 많을 경우 백업 상태를 보고서로 제공
- 백업 작업에 대한 이메일 알림 제공

04 가상화 환경 지원

- 다양한 가상화 환경 VM들을 이미지 백업/복원 지원
- Cloud 환경(OpenStack/ AWS, Azure)의 VM 백업/복구 지원

※주1 베어메탈: 운영 체제(OS)를 포함하여 어떤 소프트웨어도 설치되어 있지 않은 하드웨어를 의미한다.

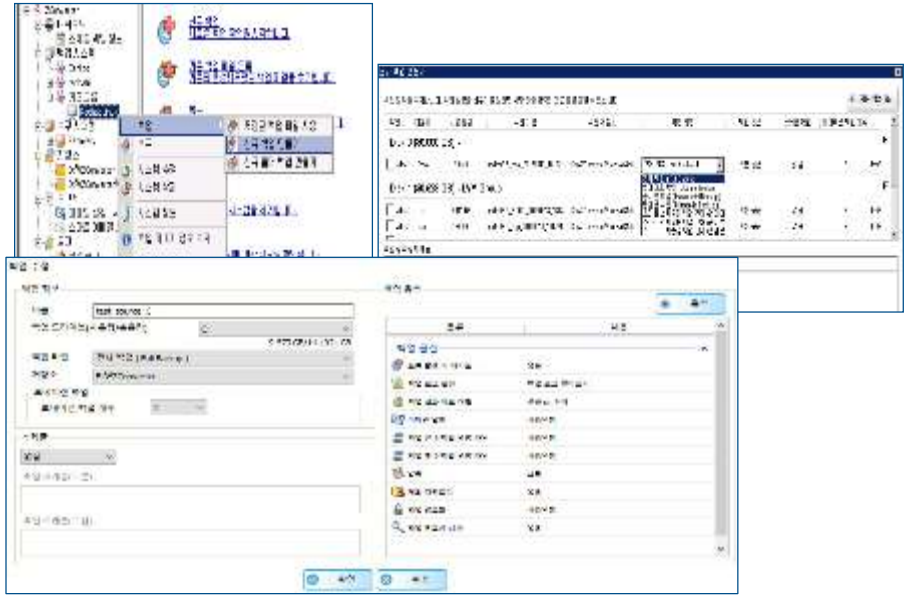
02 ZConverter Server Backup 주요 기능

① 백업 대상 서버 및 백업 정책 관리는 관리서버의 GUI 환경으로 중앙 관리

직관적인 GUI를 통해 백업 수행 및 관리를 쉽게 운영 가능함

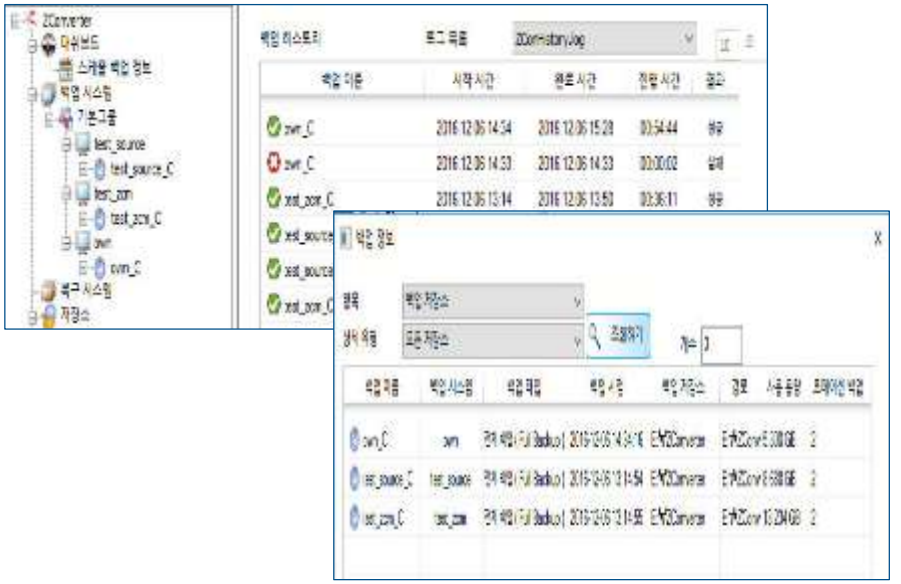
백업 정책 관리

- 손쉬운 Job schedule 설정
- 드라이브 단위 백업 스케줄 확인



백업 히스토리 관리

- 서버별 백업 히스토리 확인
- 한 화면에서 백업 성공, 실패 확인

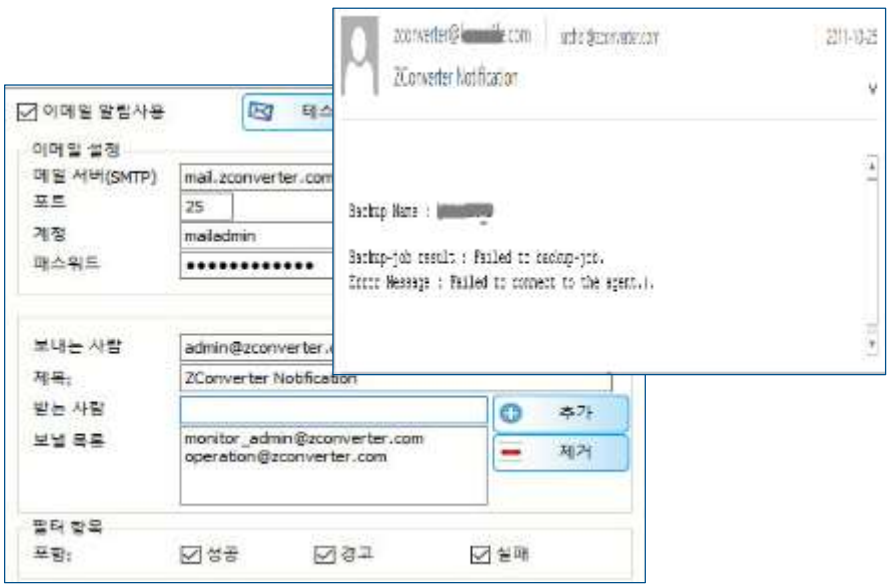


② 백업 결과(성공/실패)에 대해 이메일 알림을 통해 진행 상태에 대해 확인

스마트 이메일 보고서 기능을 통해 전체 백업 상태에 대해 관리자가 빠르게 현황파악이 가능

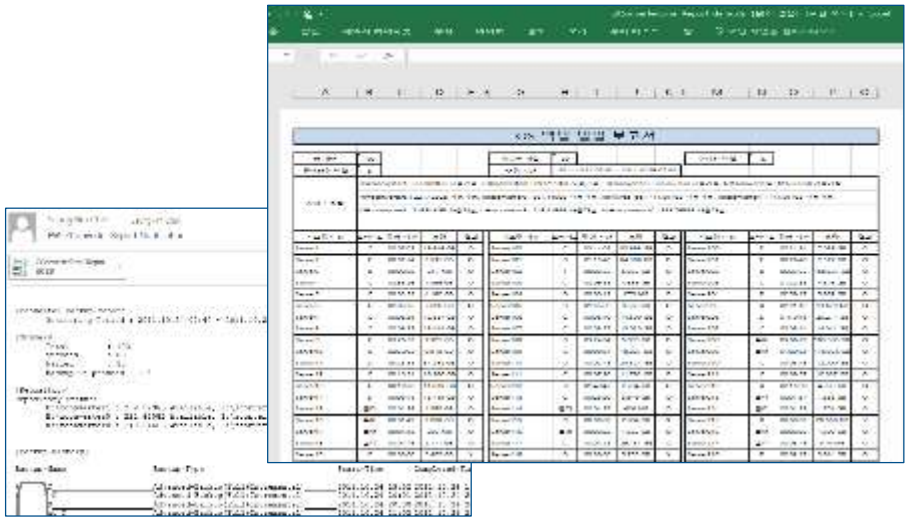
백업 결과 이메일 전송 기능

- 백업 성공/실패 알람
- 알람 확인으로 빠른 대응 조치 가능



통합 이메일 보고서 전송 기능

- Backup job 빠른 현황 파악
- 일, 주, 월 백업 보고서 전송 기능
- 고객사에 맞게 보고서 폼 변경 가능

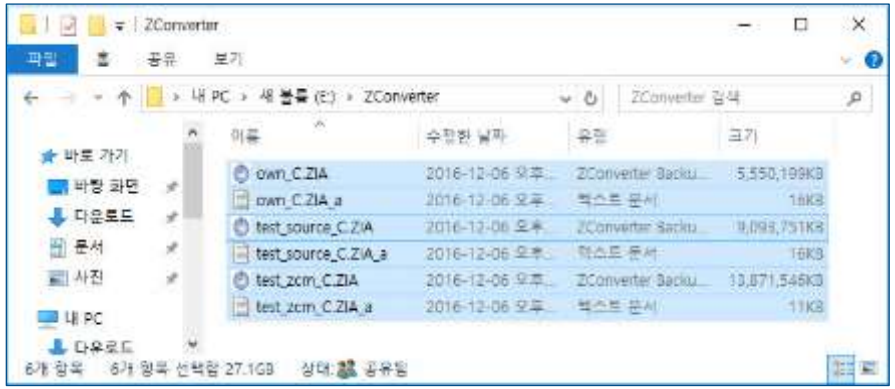


③ 백업 이미지는 기본 압축이 되어 저장 공간을 효율적으로 사용이 가능

추가적인 중복 제거 기능을 통해 이미지 저장 공간을 최적화

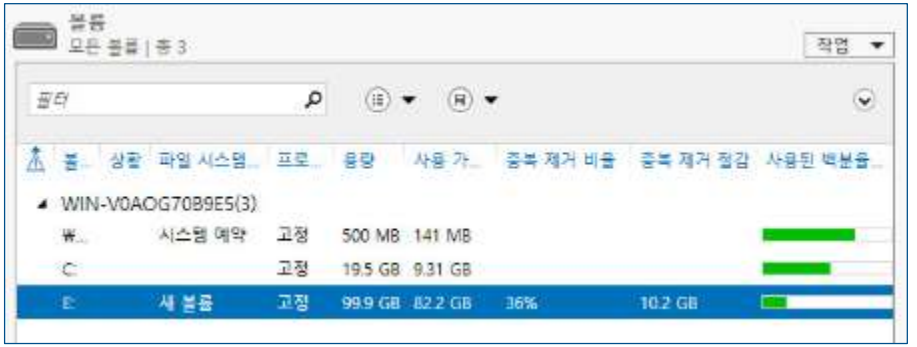
압축으로 인한 이미지 공간 절약

- 압축은 gzip 라이브러리를 통해 압축 수행
- 압축율은 파일 타입에 따라 다르며 일반적으로 50%~80% 압축됨
- 압축된 이미지 파일을 중복제거를 통해 2차적으로 디스크 공간을 절약함



중복제거를 통한 이미지 공간 절약

- 추가적으로 중복제거 기능과 연동할 수 있어 백그라운드 상태에서 중복제거 수행
- 백업 작업과 별도로 동작이 되기 때문에 백업/복구 속도가 빠름
- 독립적으로 중복제거 기능을 추가/제거가 가능함
  〈중복제거에 대한 성능 이슈 발생 대비〉

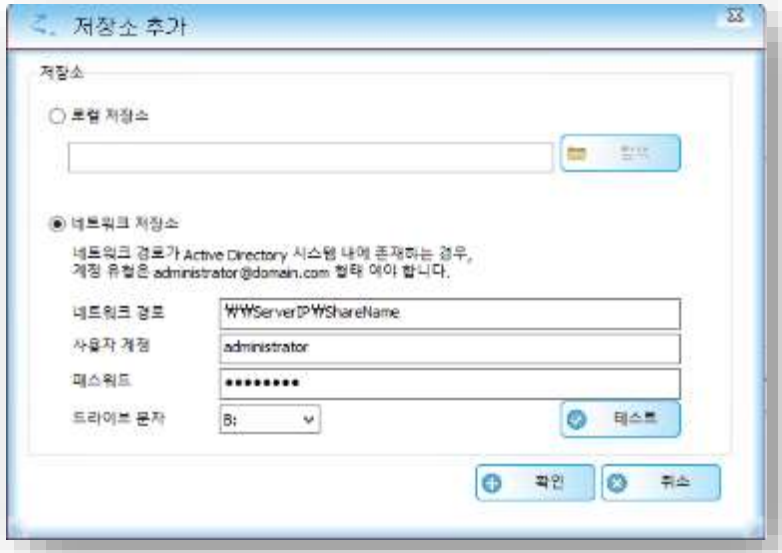


④ 백업 구성을 위한 서버 연결은 Network과 Agentless 방식을 제공

Network과 Agentless 방식 제공으로 운영 환경에 적합한 백업 구성 가능

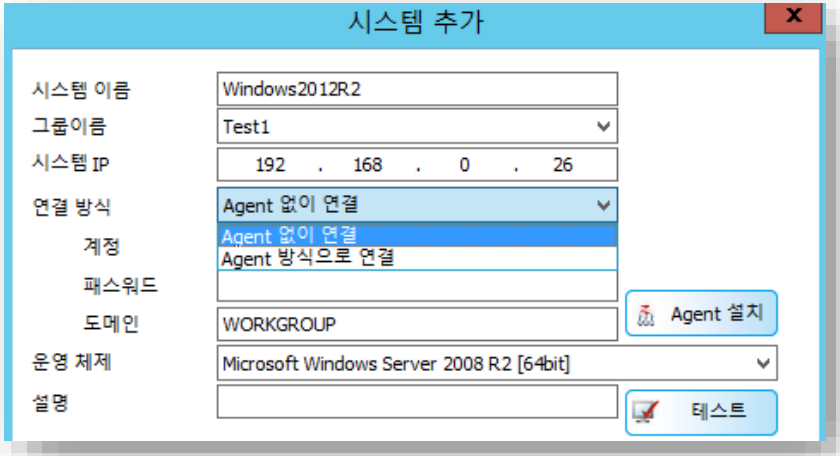
Network 구성

- Network를 이용하여 백업 이미지를 저장이 가능하며 같은 Private 네트워크에서는 쉽게 구성이 가능.



Agentless 구성

- Agentless 방식으로 백업 대상 서버의 부하를 줄여줄 수 있으며 쉽고 간편하게 설치가 구성이 가능
- 고객사 환경(방화벽)에 따라 Agent를 설치 할 수도 있지만 시스템 재부팅 하지 않음.



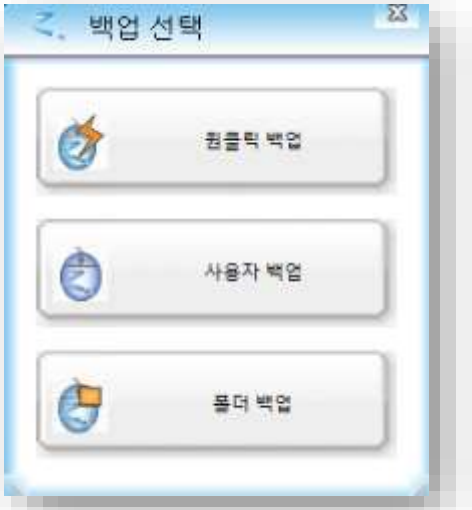
03 ZConverter Server Backup 백업 기능

① One-click Backup 제공으로 쉽고 빠른 백업이 가능

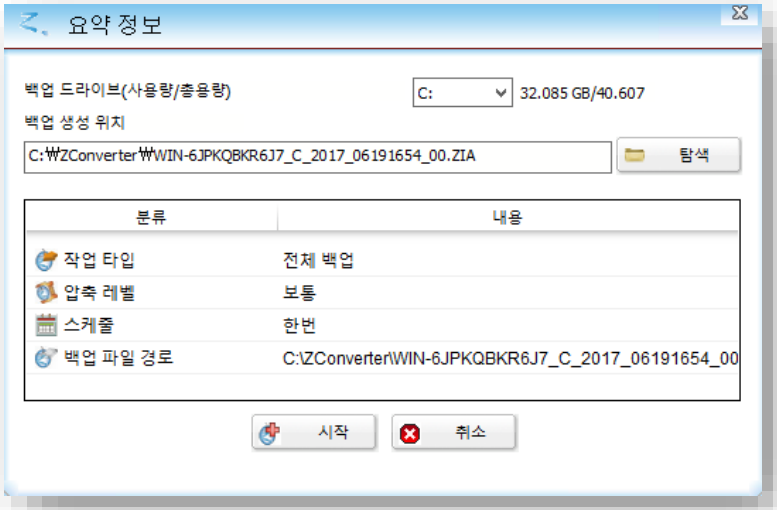
사전에 정의된 내용을 한번의 클릭으로 수행하여 손쉬운 백업이 가능

단순한 백업 과정

01 백업 선택



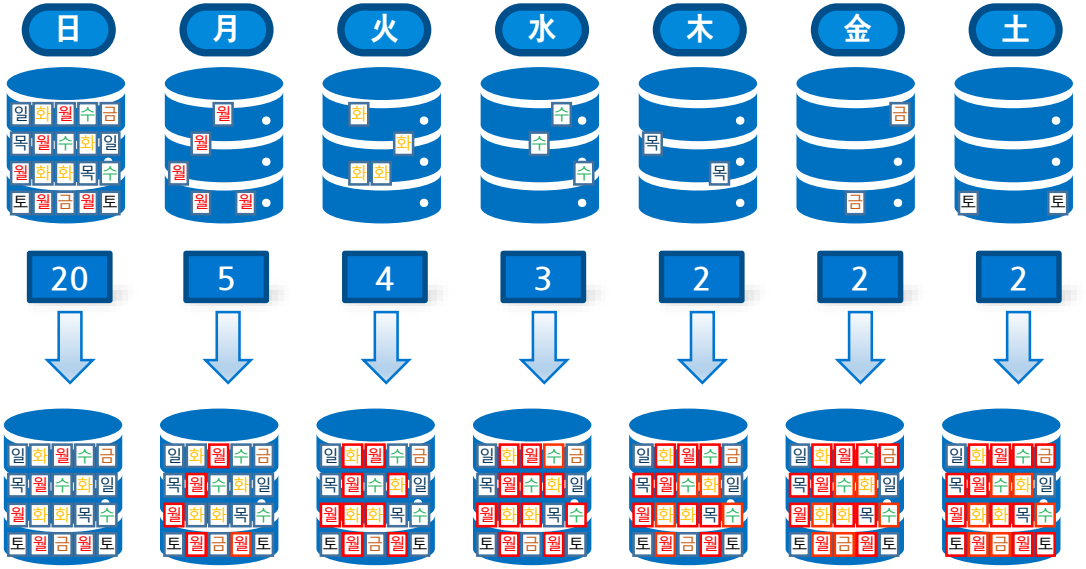
02 백업 완료



② 풀 백업 이후 이전의 파일과 비교하여 변경된 데이터를 보관

증가분(Incremental) 백업

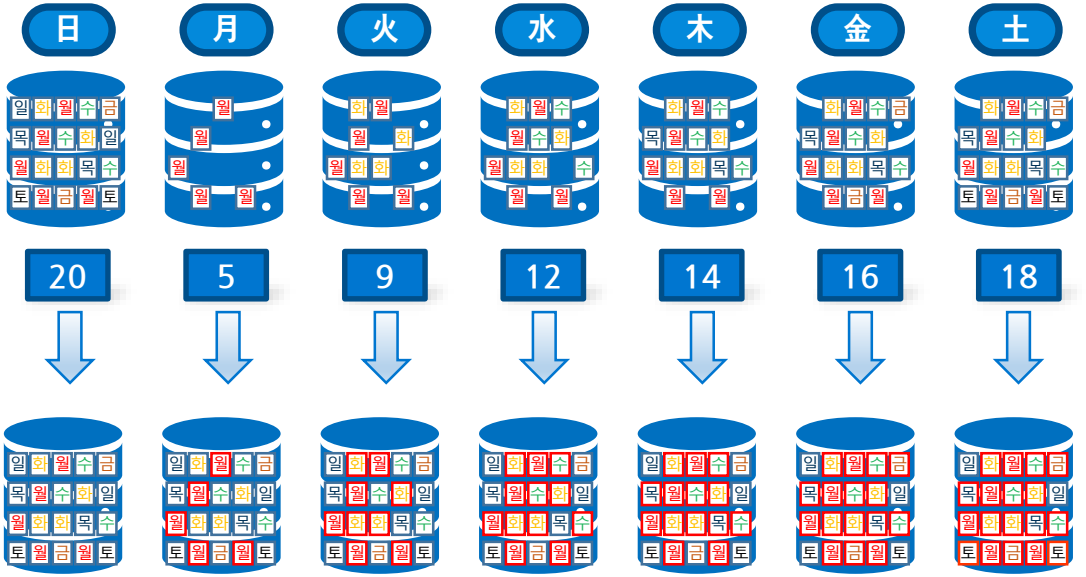
- 풀 백업 이후 이전의 파일과 비교하여 변경된 데이터를 보관 (풀백업 1본, 월~토 백업 6본 저장)
- 중복제거와 결합하여 최적의 디스크 효용성 제공 (풀백업 이후는 변경 부분만 백업)
- 복구 시 날짜별로 복구 가능하지만 모든 순차 파일이 있어야 함



③ 풀 백업 파일과 매번 비교하여 변경된 데이터를 새로운 파일로 생성

변경분(Differential) 백업

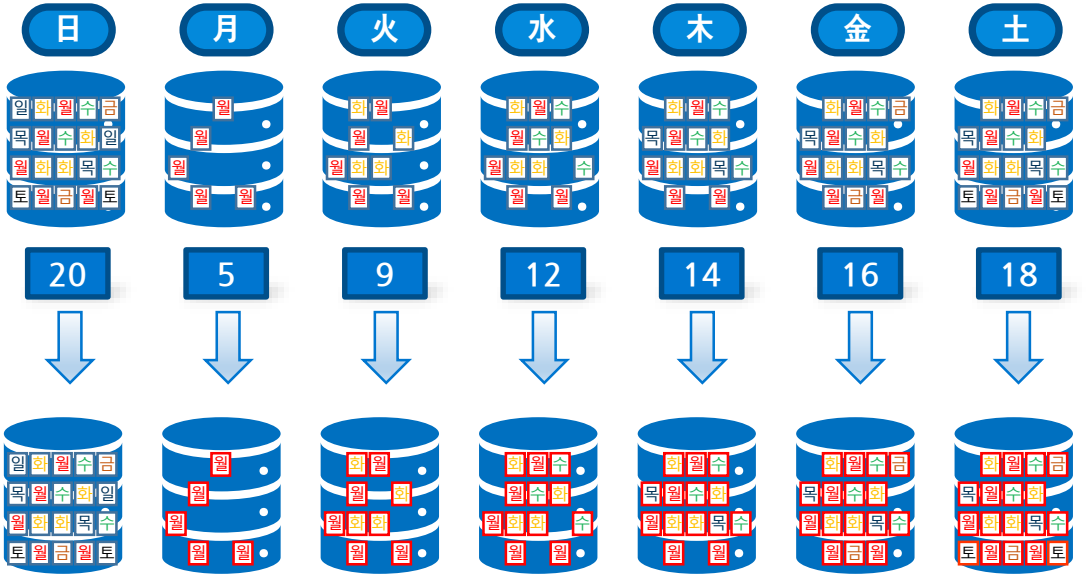
- 풀 백업 파일과 매번 비교하여 변경된 데이터를 새로운 파일로 생성 (풀백업 1본, 월~토 백업 누적 6본 저장)
- 복구 시 풀 백업 파일 + 변경분 백업 파일만 있으면 해당 날짜로 복구 가능 (풀백업 이후는 변경 누적분 백업)
- 변경되는 데이터가 많은 서버는 저장소의 효율성이 떨어질 수 있음



④ 풀 백업 파일과 매번 비교하여 변경된 데이터를 새로운 파일로 Merge

업데이트(Update) 백업

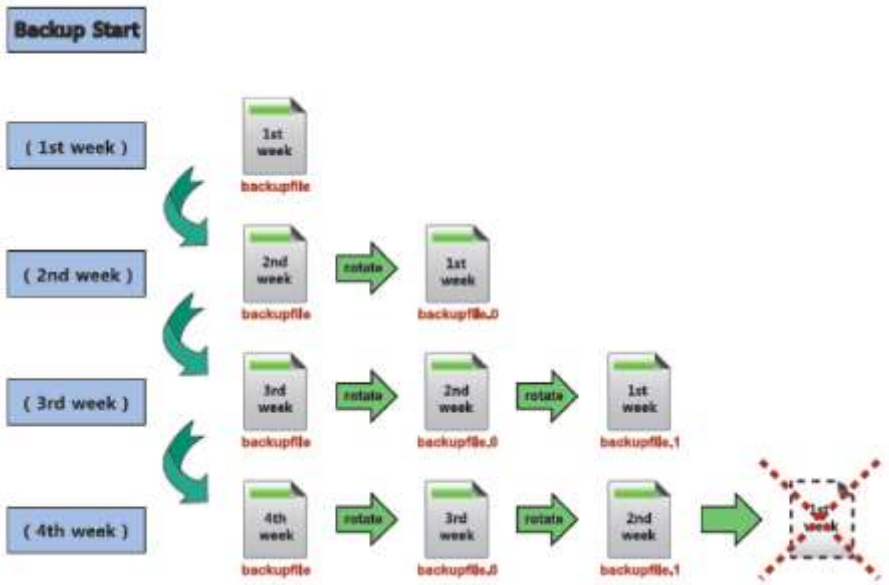
- 풀 백업 파일과 매번 비교하여 변경된 데이터를 새로운 파일로 merge가 됨 (풀백업 1본, 월~토 백업 누적 1본 저장)
- 복구 시 풀 백업 파일 + 업데이트 백업으로 최신 날짜로만 복구 가능 (풀백업 이후는 변경 최종일 누적분 백업)
- 업데이트 백업은 저장공간을 최소화 하지만 지정된 날짜 복구는 지원되지 않음



⑤ 원하는 백업 타입과 주기를 로테이션으로 파일 개수를 설정

Smart 스케줄링 백업

- 고객이 원하는 백업 타입과 주기를 로테이션으로 파일 개수를 설정
- 풀 백업과 변경된 파일을 로테이션 주기 및 파일 개수를 지정
- 증가분 백업, 변경분 백업, 업데이트과 함께 사용하여 저장공간 효율을 높일 수 있음



04 ZConverter Server Backup 복구 기능

① 백업 대상 시스템이 장애 발생 시 빠른 복구를 위해 복구 미디어를 제공

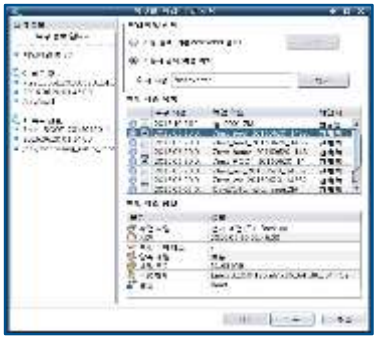
단일 GUI환경으로 제공되기 때문에 쉽고 빠르게 복구가 가능

복구 절차

01 복구 CD 부팅

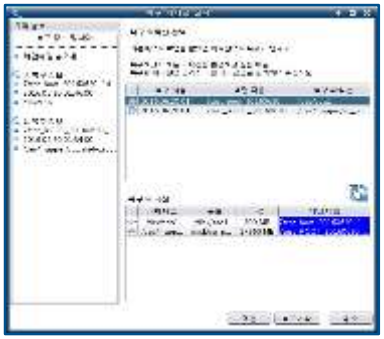
- ZConverter 복구 미디어로 부팅 (CD/PXE/USB 사용이 가능)

02 복구 이미지 선택



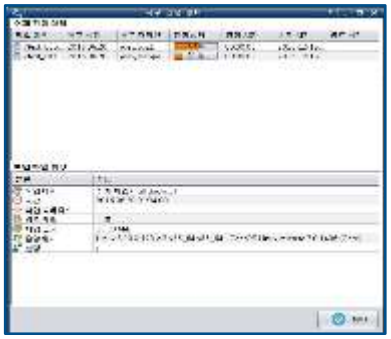
- 백업 이미지가 존재하는 저장소를 연결

03 복구 대상 선택



- 복구 마법사를 통해 백업 이미지를 복구

04 복구 모니터링



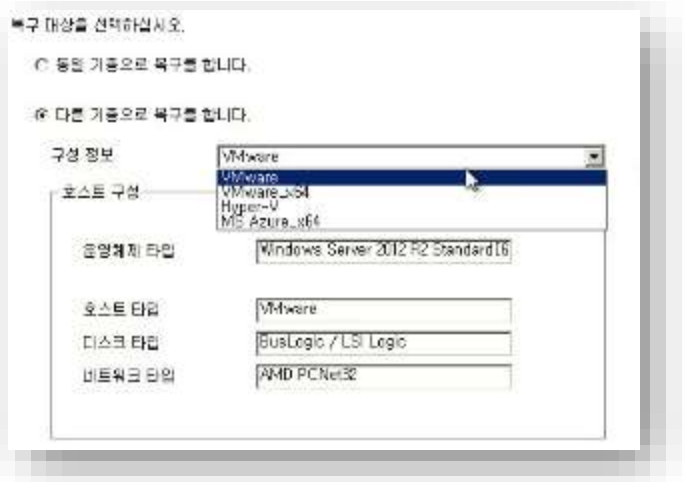
- 복구 진행 사항을 모니터링

② 이 기종서버 베어메탈 복구 지원

운영서버의 하드웨어 장애 발생시 긴급 복구가 필요한 경우 다른 기종 서버에 복구 가능

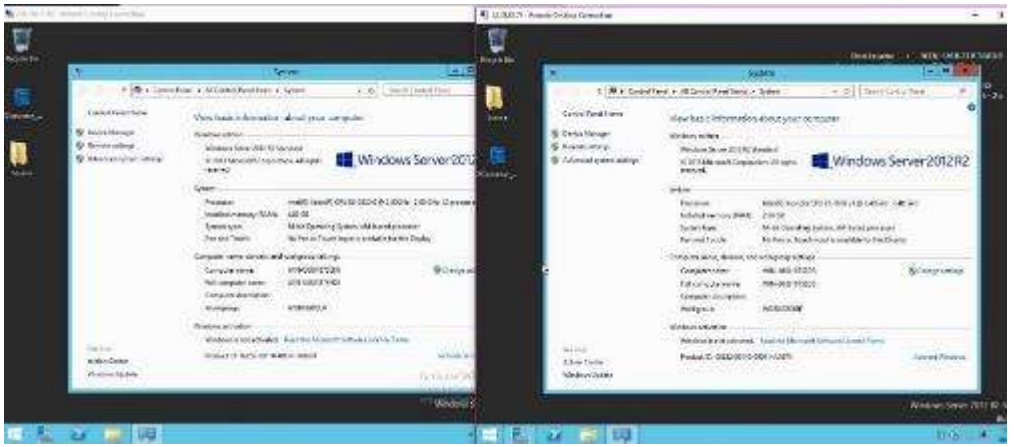
이기종 서버 복구 절차

01 다른 기종 복구 선택



- ZConverter 복구 마법사 진행 시 다른기종 복구를 선택

02 복구 상태 확인



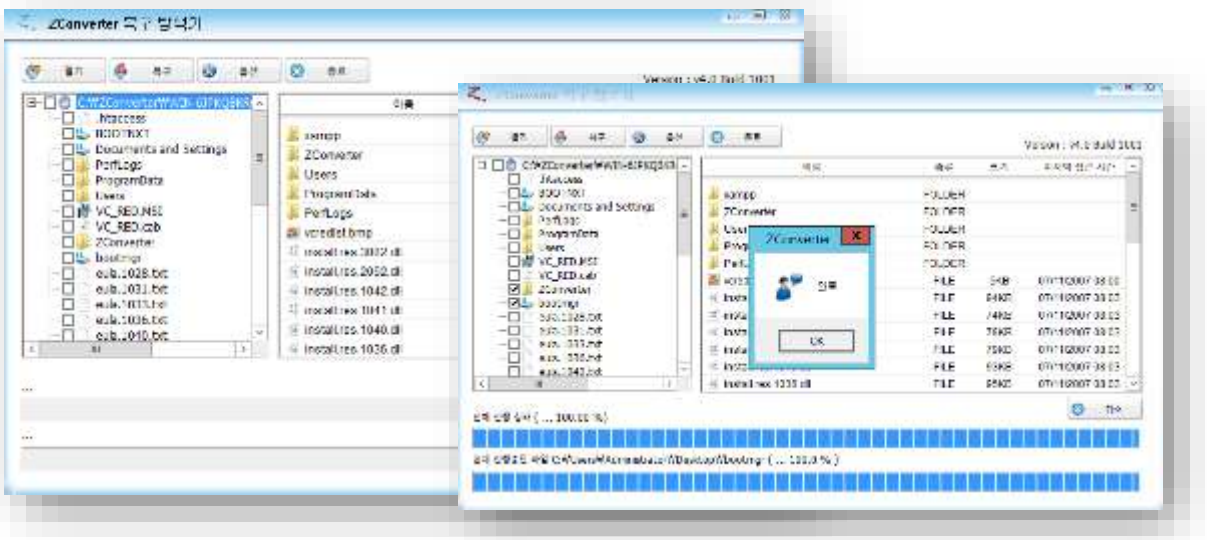
- 복구 완료 후 Source 서버와 비교 및 상태 확인

③ 파일 단위 복구 기능

특정 파일이나 데이터만 복구가 필요한 경우 복구 탐색기를 이용하여 선택적으로 복구 가능

파일복사 / 아카이브

- 복구 탐색기를 이용하여 특정 파일이나 데이터가 있는 폴더만 선택적 복구 가능
- 기존의 데이터와 이름이 같은 때 중복 파일 처리 옵션과 기존 폴더 구조 설정을 변경 복구 선택 가능
- 직관적인 UI로 쉽고 파일 폴더 선택이 가능

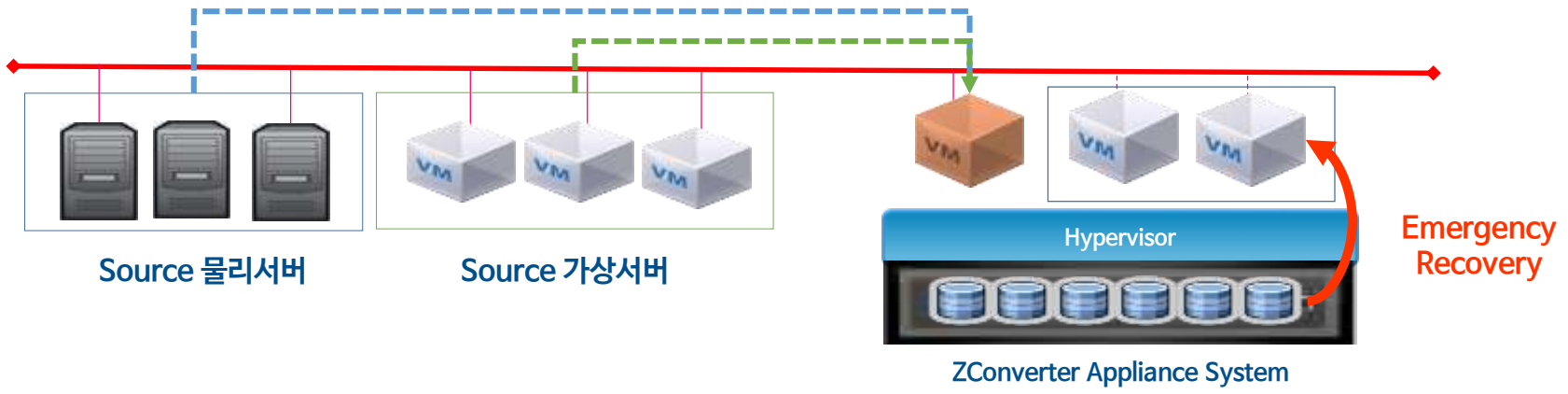


④ 다수의 물리적인 서버(OS)를 가상화 서버로 복구(P2V)가 가능

다수의 물리적, 논리적 서버에 대한 백업을 수행하고 장애가 발생하는 경우 가상화 서버의 VM으로 복구

P2V 복구 방안

- 다수의 물리적, 논리적 서버의 OS에 대한 백업을 수행
- 특정 서버에 장애가 발생하는 경우 Hypervisor 위의 가상머신으로 복구 진행하여 서비스를 재개함
- Hypervisor는 VMware 또는 Hyper-V 를 권장

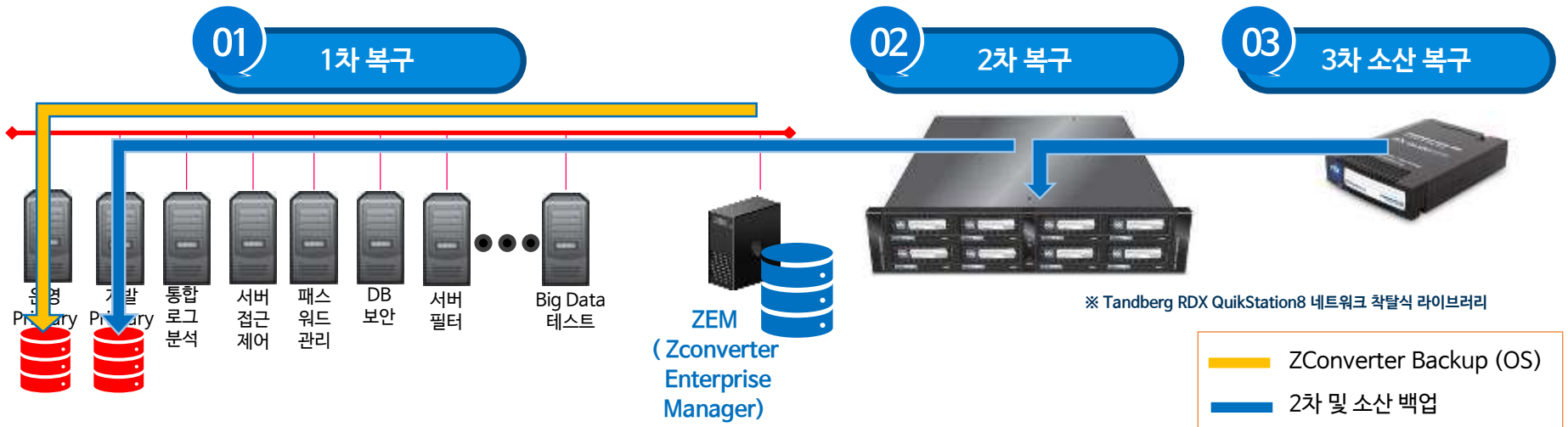


⑤ 백업 디스크 장애 및 랜섬웨어 등에 대비한 다양한 복구 방안을 제공

Hard Disk Drive 최고의 장점과 Tape Drive의 장점만을 하나로 Tandberg Data RDX 이용 복구 방안 제공

소산 복구 구성 안

- 복구 대상 서버의 OS를 ZConverter Appliance의 디스크 백업을 이용하여 1차 복구
- 1차 백업으로 복구가 불가능한 경우 착탈식 백업 장비인 Tandberg Data RDX를 이용하여 2차 복구
- **랜섬웨어 등으로 1차, 2차 백업으로 복구가 불가능한 경우 소산 카드리지를 이용한 3차 복구**



Dell R730xd 기본으로 하며 타벤더 제품과도 호환이 가능

패키지 형태로 Usable 3TB, 5TB, 10TB, 20TB, 30TB 5가지 제품 라인업

구분	제안 사양 (Usable 30TB 기준)
Type	- 2U Form Factor
CPU	- Two Intel Xeon E5-2620v4 2.1Ghz 8Core
Memory	- 64GB RDIMM(16GB*4)
NIC	- Dual 4 x 1GbE Broadcom NIC
OS Disk	- 2 x 300GB SAS 15K RPM RAID 1
Data Disk	- 11 x 4TB NL SAS Hot Swappable drivers RAID 6
운영 체제	- Microsoft Windows Server 2012 Standard R2
전원 구성	- Dual Redundant, Hot Swappable, Auto-ranging, Platinum efficiency 750W
Service	- 3Yr ProSupport & Mission Critical : (7x24) 4-hour Onsite Service

랜섬웨어 등 외부 공격에 대응하기 위한 보안 취약점 대응

ZConverter Appliance 는 Windows 2012 R2 를 사용하며, 보안 취약점에 대한 조치를 적용

구분	조치 사항	비고
계정 및 패스워드 관리	계정 관련 점검(불필요한 계정, admin 권한을 갖는 계정)	
	비밀번호 관련 점검(취약한 비밀번호, 암호화, 비밀번호 오류시 자동 잠금, 비밀번호 최대 사용기간 등)	
접근 제어	접근 설정 점검(공유 폴더, 원격 레지스트리 접근, 화면 자동 잠금 등)	
시스템 보안	권한 설정 점검(시스템 디렉터리 권한, 윈도우 계정 권한, 시스템 사용률 등)	
서비스 보안	서비스 중지(불필요한 서비스, 터미널 서비스, 익명 FTP, SNMP 설정 등)	
모니터링	시스템 감사정책, 로그 기록 설정 등	
기타 보안관리	보안설정, 스케줄링 내용, 백신 사용여부, 최신 패치 점검	
	미래창조과학부고시 주요정보통신기반시설 취약점 분석·평가 기준 Windows 서버 내용 준수	
고객사 보안 준수	Anti-Virus 솔루션 등 고객사의 서버용(Windows 2012) 보안 솔루션 설치	
2차 소산 제공(옵션)	랜섬웨어나 디스크 장애 등에 대비한 Tandberg Data RDX 이용 소산 백업 제공	옵션 기능

06 ZConverter Server Backup 지원 OS

윈도 서버와 리눅스 서버군 모두에 대한 시스템 백업 복구를 지원

01 WINDOWS 서버

- Windows Server 2012
- Windows Server 2008
- Windows Server 2003

02 RedHat LINUX 계열 서버

- RedHat Enterprise Linux 5.x
- RedHat Enterprise Linux 6.x
- RedHat Enterprise Linux 7.x
- CentOS Linux 5.x
- CentOS Linux 6.x
- CentOS Linux 7.x

03 Cloud 플랫폼 환경

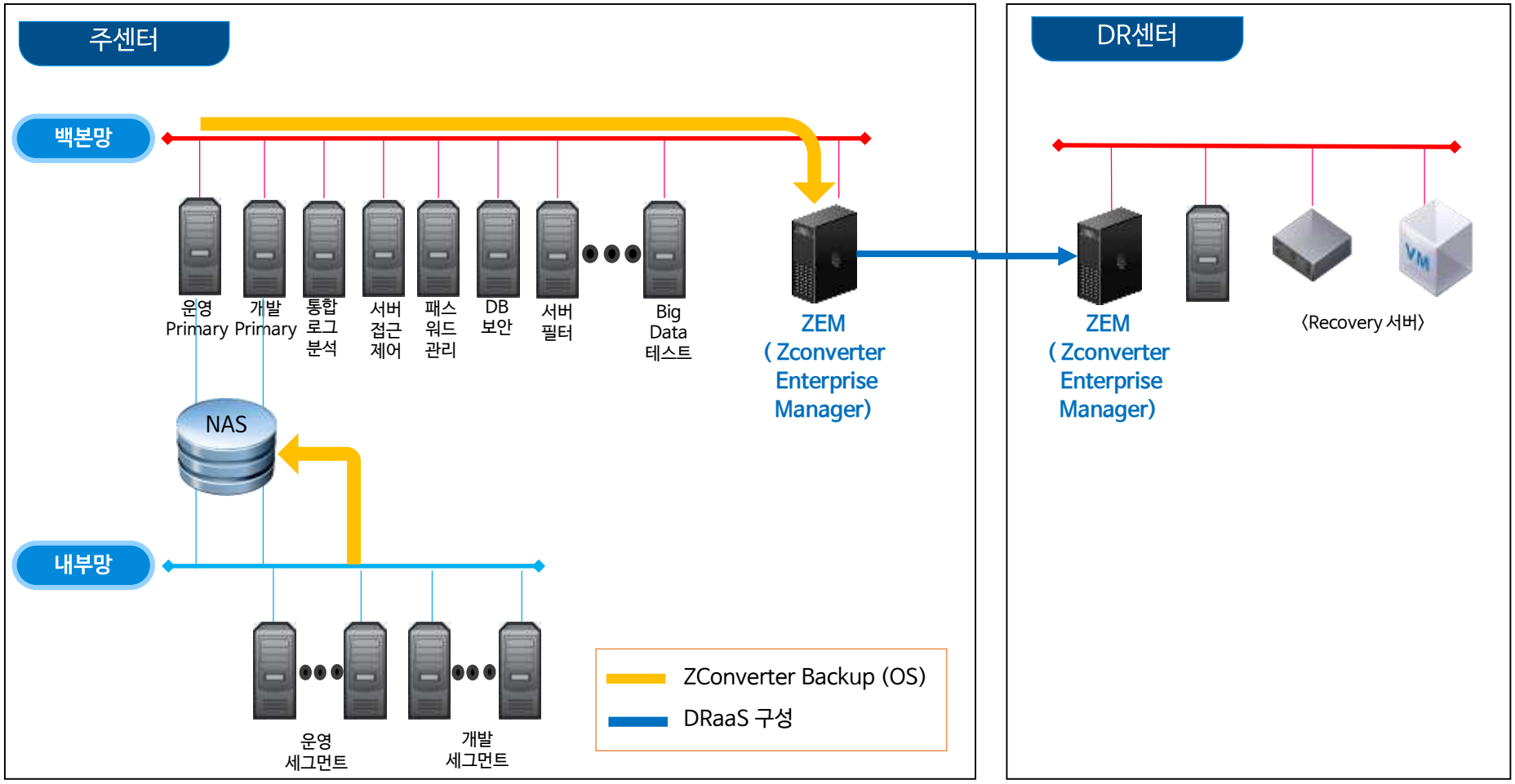
- AWS
- MS Azure
- OpenStack, CloudStack

07 ZConverter Server Backup 구축 사례

ZConverter는 윈도/리눅스 서버 시스템 백업 복구 많은 레퍼런스를 보유

고객명	프로젝트 이름	대수	제품명
삼성전자	시스템 백업 복구	200	ZConverter Server Backup
경찰청	112 콜센터	400	ZConverter Server Backup
동부화재	시스템 백업	100	ZConverter Server Backup
LG화학	시스템 백업 복구 및 재난복구	300	ZConverter Server Backup
한화생명	시스템 백업 복구	300	ZConverter Server Backup
CJ (CJ오쇼핑 포함)	시스템 백업 복구	50	ZConverter Server Backup
한국 IBM (송도데이터센터)	시스템 백업 복구	200	ZConverter Server Backup
LIG 넥스원	시스템 백업 복구	50	ZConverter Server Backup
KB 손해보험	시스템 백업 복구	53	ZConverter Server Backup
만도	시스템 백업 복구	50	ZConverter Server Backup
오뚜기	시스템 백업 복구	50	ZConverter Server Backup

백업 환경 구성 간 운영서버에 대한 시스템 재부팅은 발생하지 않음



08 제조사 ㈜ISA테크 수상 및 인증

시스템 백업 복구 원천기술 및 제품 관련 다수의 수상과 인증을 보유

1. 설　립　: 2004년 11월 01일 (www.zconverter.co.kr)
2. 사업 영역 : 1) 운영 체제 시스템 백업 및 복구
   2) 고 가용성 및 재난 복구 시스템 구축
   3) 가상서버 / 클라우드 마이그레이션
3. 주요 제품 : 1) ZConverter Cloud Migration
   2) ZConverter Server Backup
4. 주요 고객 : 삼성전자 외 800개사
5. 수출 국가 : 미국,일본,대만,싱가폴,말레이시아, 인도네시아 필리핀, 아랍에미레이트

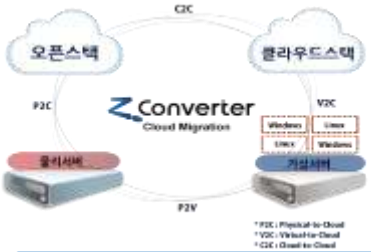
마이크로소프트 공인인증
ZConverter Server Backup

한국IBM 공인인증
ZConverter Server Migration

마이크로소프트 공인인증
ZConverter Windows Backup

Good SoftWare 인증
특허등록
신SW상품 대상
지식경제부 장관상

국내 800여 고객사



클라우드 마이그레이션

openstack
COMPATIBLE

OpenStack Compatible SW

08 제조사 ㈜ISA테크 수상 및 인증

시스템 백업 복구 원천기술 및 제품 관련 다수의 수상과 인증을 보유

ISA테크는 2004년 설립 후 10년 이상 가상화,클라우드, 서버백업,재난복구 전문 기업으로 국내 외 500개 이상의 기업 고객에게 IT 인프라 환경을 효율적이며 안정적으로 운영을 할 수 있는 솔루션과 서비스를 제공하고 있습니다.

ZConverter Server Backup

- ➲ 윈도 서버/ 리눅스 서버 OS 백업 복구 지원
  - 국내 최초 원천기술 보유
  - MS 공식 호환 OS백업 복구 SW
    AWS 클라우드 가상서버 백업 복구
  - 삼성전자, 한화생명, 경찰청, 한국IBM, LIG넥스원 외
- ➲ 재난 복구 서비스 제공
  - LG화학, 현대자동차(미주법인) ,미쓰비시, 신항만 외

ZConverter Cloud Migration

- ➲ VMware/ Hyper-V/ Xen/ KVM P2V 지원
  - 자체 원천기술 보유
  - 지식경제부 장관상, 신SW상품 대상 수상
- ➲ Cloud Migration P2C, V2C, C2C 지원
  - 국내 최초 클라우드 마이그레이션 원천기술 보유
  - OpenStack Compatible 마이그레이션 지원

가상서버 통합 (VMware/Xen/KVM)

- ➲ VMware Tier1 Enterprise Partner (2004년)
  - 국내 최초 Linux P2V 마이그레이션 지원
- ➲ Hyper-V, Xen, KVM 서버 통합 지원
  - 국내 최초 Xen / KVM 마이그레이션 툴 개발

Professional Services

- ➲ P2V 마이그레이션 서비스
- ➲ Xen/ KVM / Hyper-V / VMware 지원
- ➲ 클라우드 마이그레이션 서비스 제공
- ➲ 서버통합 진단 컨설팅 제공
- ➲ 재난, 백업 복구 구축 서비스 제공

08 제조사 ㈜ISA테크 수상 및 인증

시스템 백업 복구 원천기술 및 제품 관련 다수의 수상과 인증을 보유

지식경제부 장관상

Good Software 인증

신SW 상품 대상

Microsoft 공인 인증

한국 IBM 공인 인증

특허

Chapter III 물리 소산 백업 장비

Tandberg Data RDX

01 Tandberg Data RDX ?

텐드버그 데이터는 RDX 원천 기술 라이센스를 유일하게 보유한 기업입니다.

RDX는 디스크 기반의 카트리지 솔루션으로 유일하게 테이프를 대체할 수 있는 안정성과 국제 규격화에 성공 하였으며,
텐드버그 데이터는 RDX 원청 기술 라이센스를 유일하게 보유한 기업으로 RDX 스토리지 연합의 공식 후원 사입니다.

OEM 파트너

Apple, HITACHI Inspire the Next, IBM, TOSHIBA Leading Innovation, FUJITSU, hp, NEC, lenovo

01 Tandberg Data RDX ?

Hard Disk Drive 최고의 장점과 Tape Drive의 장점만을 하나로

Hard Disk Drive 최고의 장점과 Tape Drive의 장점만을
하나로 통합시킨 전문가 수준의 최첨단 백업 장비

- Tandberg Data의 RDX 솔루션은 백업과 아카이빙, 그리고 재난 시의 복구를 위한 탈착식 디스크 카트리지 솔루션.
- RDX 카트리지는 테이프 카트리지의 장점과 디스크의 장점만을 포함하여 견고 하면서도, 높은 신뢰성과 편리함을 동시에 제공하는 장기 보관을 위한 최적의 솔루션.

01 Tandberg Data RDX ?

Hard Disk Drive 최고의 장점과 Tape Drive의 장점만을 하나로

- Tandberg Data의 RDX 솔루션은 HDD의 문제점인 진동,충격,정전기 문제와 장기간 전원이 연결되지 않아도 데이터 유실 문제를 완벽하게 해결하도록 설계
- 데이터 장기 보관을 위한 어떠한 매체 보다 빠르고 안전하며 보관이 용이. RDX는 최대 3TB의 대용량을 지원하며, 중요 데이터를 장기 보존하고 관리가 용이

HDD

- 자기 기록 방식으로 장기간 전원 연결이 없으면 데이터 유실 위험 높음
- 진동, 충격, 정전기에 취약함

CD/ DVD/ BD

- 읽기 ,쓰기 속도 느림
- 빛.온도에 취약함
- 저장 용량 매우 작음

TAPE

- 고온, 고습에 취약함
- 랜덤 액세스가 느림

Tandberg Data RDX

- 진동,충격, 정전기로 부터 보호
- 10년이 장기 보관 가능
- 읽기,쓰기 속도 빠름
- 랜덤 액세스 빠름
- 빛, 온도, 습도에 타 매체 보다 민감하지 않음
- 4TB 단일 카트리지 용량

01 Tandberg Data RDX ?

Hard Disk Drive 최고의 장점과 Tape Drive의 장점만을 하나로

- **고성능 및 고용량**
  - 1TB ~ 4TB 저장 용량
  - 초당 180 MB(USB3.0)에 이르는 Hard Disk 성능 이용
- **내구성이 강한 미디어**
  - 뛰어난 충격흡수 능력 Cartridge 설계
  - 방전방지 Cartridge 설계 (충격으로부터의 보호)
- **전문성을 갖춘 신뢰성**
  - 최소 5,000번 이상의 넣기-빼기 가능 및 보증
  - 주요 Backup Application과의 호환성
- **비용 절감**
  - 저렴한 Drive 메커니즘
  - 보다 긴 미디어 수명: 초급단계의 Tape 대비
- **미래에 대한 호환성 제고**
  - HDD Roadmap에 따른 제품 용량의 Roadmap 계획
  - 미래 호환성: 미래의 새로운 고용량 미디어도 수용
- **손쉬운 사용**
  - Cartridge 미디어에 Drag & Drop 가능
  - Plug & Play 장비

01 Tandberg Data RDX ?

백업 관련 규정 준수를 위한 WORM 아카이빙 rdxLOCK WORM (※ 주1)

랜섬웨어 감염이나 관련 법규 준수를 위한 WORM 기능의 제공으로 안전한 백업 구축이 가능

- rdxLOCK WORM 미디어는 규정 준수 요구 사항을 충족하며, 데이터를 삭제하거나 덮어 쓰지 않아야 하는 엔터프라이즈 콘텐트 관리 및 문서 관리 시스템과 같은 많은 보관 응용 프로그램에 이상적 솔루션임
- 백업을 삭제 불가능한 방식으로 저장 및 보관할 수 있으며, RDX WORM 미디어를 통한 랜섬웨어와 같은 바이러스 공격으로부터 보호 할 수 있음

- RDX 미디어에서 WORM 데이터 보호 제공
- 투명한 아카이브 애플리케이션 통합

Enable WORM with rdx LOCK

- 정의 가능한 WORM 보유 시간
- 향상된 보호 모드를 위한 향상된 보안 모드
- RDX 미디어에서 WORM 데이터 보존 시간을 보호하는 검증 된 보존 클럭
- Tandberg Data RDX QuikStor 드라이브 및 RDX QuikStation 디스크 배열과의 호환성
- **Windows 운영 체제의 경우 Windows 7, 8, 8.1, Windows Server 2008, 2008 R2, 2012, 2012 R2**

※ 주1 : 별도의 WORM 카트리지, 솔루션(rdxLock) 라이선스 필요, Windows OS 지원

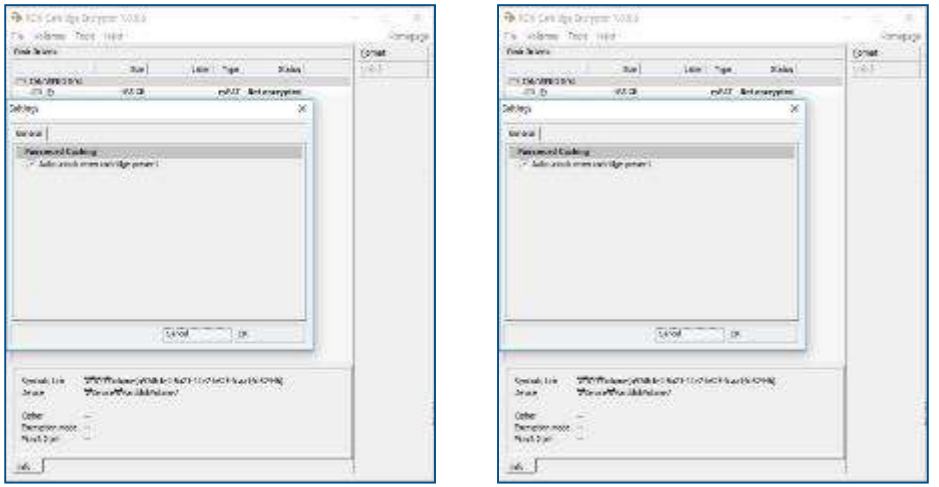
랜섬웨어 감염 등에 대비한 백업 테이프에 대한 쓰기 방지 기능과 카트리지 암호화 지원

랜섬웨어 감염이나 백업 손상 방지를 위하여 카트리지 잠금으로 읽기 전용으로 사용 가능하고, 암호화 기능도 지원

- 쓰기방지의 경우 강제로 쓰기 권한에 락을 걸게 되며 읽기만 가능하고 쓰기작업은 불가능
- 수동으로 카트리지 잠금을 설정하면 랜섬웨어 방지 및 백업 이미지에 대한 보호가 가능
- 카트리지안의 데이터를 AES-256Bit 암호화 지원하며, 이 기능은 전원이 해제된 후 다른 장비와 연결하게 되거나 강제로 락을 설정한 후 암호화 키를 입력하지 않으면, 카트리지안의 데이터 확인이 불가능

쓰기 방지 기능 적용

암호화 기능 적용



01 Tandberg Data RDX ?

다양한 OS 및 백업 솔루션에 대한 호환성을 제공

Operating Systems

- Fedora
- Mac OS X
- Redhat EL 3, 4, 5
- SuSE ES 9, 10, 11
- Windows Storage Server
- Windows XP, Vista, 7, 8
- Windows sever 2003, 2008, 2012

Backup Software Applications

- Zconverter
- Barracuda Yosemite Backup
- CA ARCserve
- EMC Retrospect
- Microsoft NT Backup
- Symantec Backup Exec & System Recovery

Hard Disk Drive 최고의 장점과 Tape Drive의 장점만을 하나로

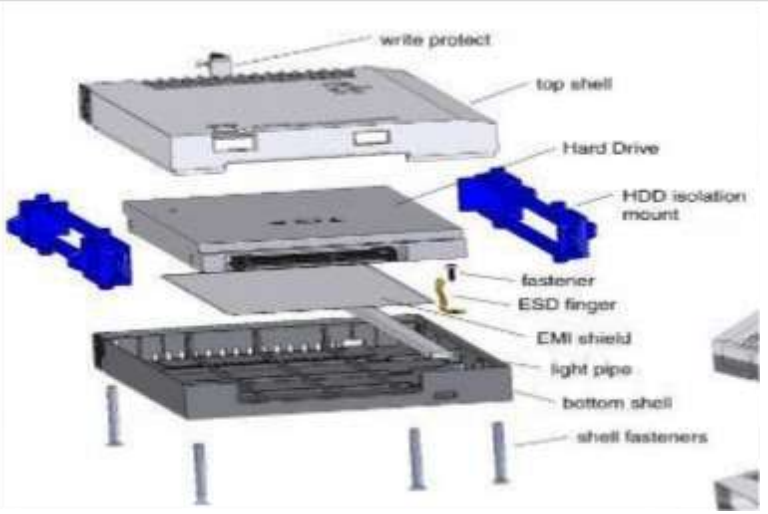
“세계 최초의 전원 케이블 없는 RDX 드라이브”

- 전원 케이블의 불필요
- USB3.0 케이블 연결로 필요할 때만 전원이 ON
- 이동성과 휴대성 강화

“RDX 랙 마운트 솔루션”

- 19인치 표준랙에 설치 가능
- 용량 및 성능향상을 위해 4개까지 RDX 장착 가능
- 전면으로 나사 없이 드라이브 마운트

Hard Disk Drive 최고의 장점과 Tape Drive의 장점만을 하나로



- 내구성을 강화시킨 설계
- 자동-제어 설계
- 사용자 친화적인 외양
- 5,000번 이상의 착탈 순환
- SATA Cartridge 인터페이스
- 1TB, 2TB, 3TB, 4TB

- 특별 분리 층으로 설계하여 충격흡수 및 내구성이 뛰어나고 진동에 강함
- 전도성이 있는 외형 덮개를 사용하여 전기적인 인터페이스가 일어나기 전에 정전기의 배출을 용이하게 하였음
- HDD “지문” 과 전자 Bar-code

03 RDX QuikStation8

Hard Disk Drive 최고의 장점과 Tape Drive의 장점만을 하나로

- RDX QuikStation8은 네트워크 착탈식 라이브러리로, 데이터 보호와 오프사이트 재해 복구를 위한 다중 카트리지 플랫폼을 제공
- Tandberg Data의 4TB RDX 카트리지를 통하여 최대 32TB의 온라인 백업과 무제한의 오프라인 용량을 제공하며, 주요 백업 솔루션 벤더의 백업 소프트웨어와 완벽한 호환성 및 다양한 백업 시스템 구성을 제공

- 2U에 최대 8개의 RDX카트리지를 사용 가능
- 10GbE 포트X41 1GbE 포트X4(iSCSI)
- 가상 테이프 드라이브 수 : 1대 또는 2대
- 가상 테이프 슬롯 수 : 8슬롯
- RAID5,6 지원

Hard Disk Drive 최고의 장점과 Tape Drive의 장점만을 하나로

▪ 높은 성능

- QuikStation4와 같은 패스-스루 드라이브 구조
  (1드라이브 당 성능이 향상)
- 1G Ether x 4 또는 10G x1 + 1G x4
- Bonding Option 추가(Dynamic Link Aggregation 지원)
- 그 외: CPU, Memory 등의 스펙 향상

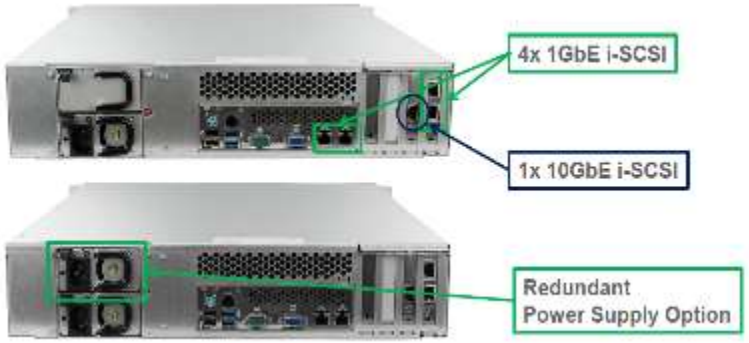
▪ 신뢰성 향상

- 확장 전원 지원 (옵션)
- 내부 시스템 디스크를 USB DOM에 SATA DOM으로 변경

▪ 논리 볼륨/보호 볼륨 모드 추가

- 복수의 카트리지를 결합하는 논리 볼륨 모드를 추가
- RAID 5 또는 RAID 6의 보호 볼륨 모드 추가

1	RDX 드라이브(8개소)
2	긴급 이젝트 용 키 삽입 구멍 (8개소) 액세서리 키트에 포함되어 있는 이젝트 키트를 사용하거나, 클립 등을 이용하여 카트리지의 강제 이젝트를 실시합니다.
3	RDX 카트리지 이젝트 버튼(8개소)
4	전원 버튼
5	USB3.0 포트



Tandberg Data RDX 고객 레퍼런스

Meritz Fire & Marine Insurance 고객 사례

- 메리츠 화재 보험은 8대의 서버에서 발생되는 각종 로그파일을 백업 및 소산 보관 하기 위하여 Tandberg Data QuikStation와 NAS의 2차 백업으로 RDX 1U RackMount를 도입

- QNAP NAS는 USB3.0 포트를 기본 지원하여 RDX 1U RackMount와 손쉽게 연결되며, QNAP NAS의 기본 기능인 RDX 백업 기능을 이용하여 NAS의 데이터를 소산 백업하여 사내 주요 데이터를 안전 하게 보호

제안 구성

RDX QuikStation

QNAP NAS

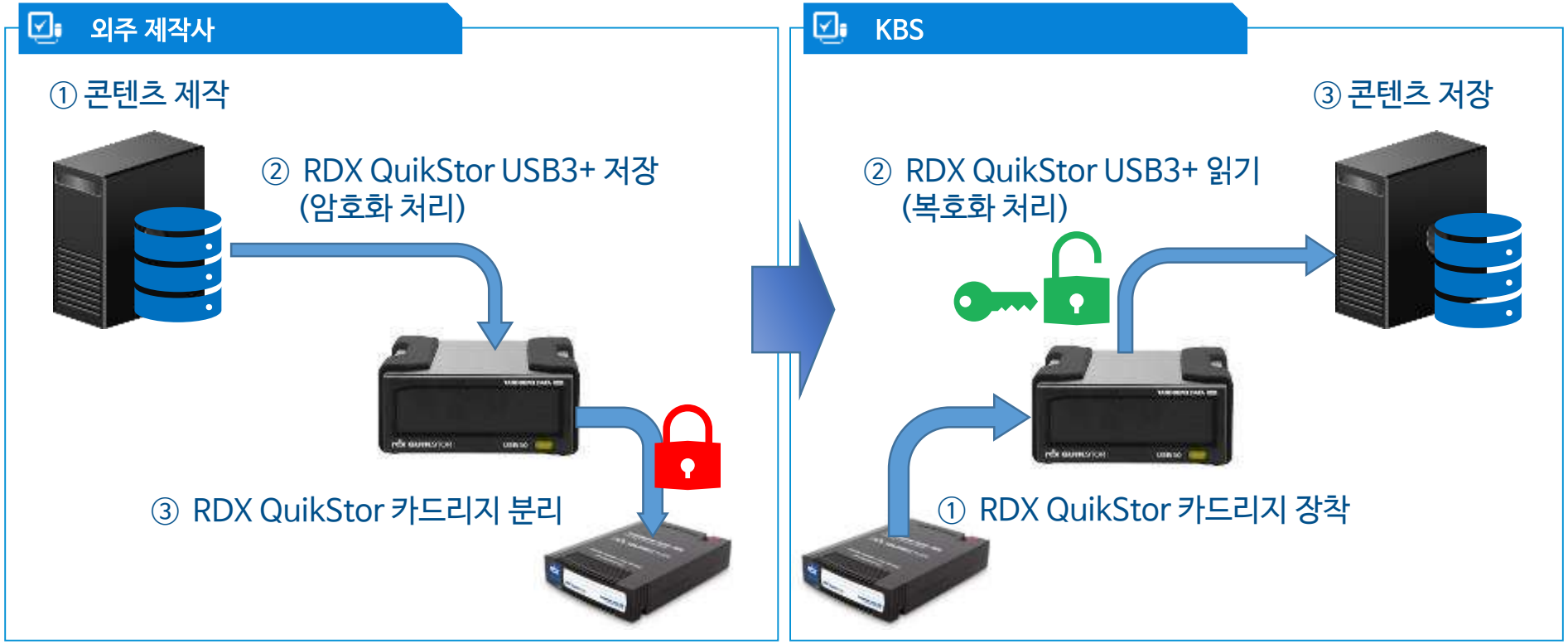
RDX 1U RackMount

대검찰청 디지털 송치체계 사업

- 대검찰청은 2014년부터는 D-NET 사업을 확장한 KD-NET(국가 디지털 송치체계 사업 :2014년- 2016년) 사업의 일부로 디지털 증거자료(CCTV,블랙박스,스마트폰, PC내 파일 등등..)의 수집,보존, 송치를 위한 표준 저장매체로 RDX를 도입, 디지털 증거팩(DEP-Digital Evidence Pack)으로 사용
- 디지털 증거팩(RDX)은 피압수자의 모든 디지털 데이터를 수집,추출,분석하여 증거로 활용하고, 이 증거물이 송치되고 재판의 증거로 사용

KBS 외주 제작사 콘텐츠 관리

- 외주 콘텐츠 제작사에서는 제작이 완료된 콘텐츠를 RDX 카드리지에 암호화하여 저장
- KBS에서는 PC별로 1대의 드라이브를 장착하여 RDX 카드리지의 데이터를 복호화하여 저장
- RDX 카드리지의 데이터는 암호화되어 카트리지를 분실해도 암호키가 없으면 복호화가 불가능함



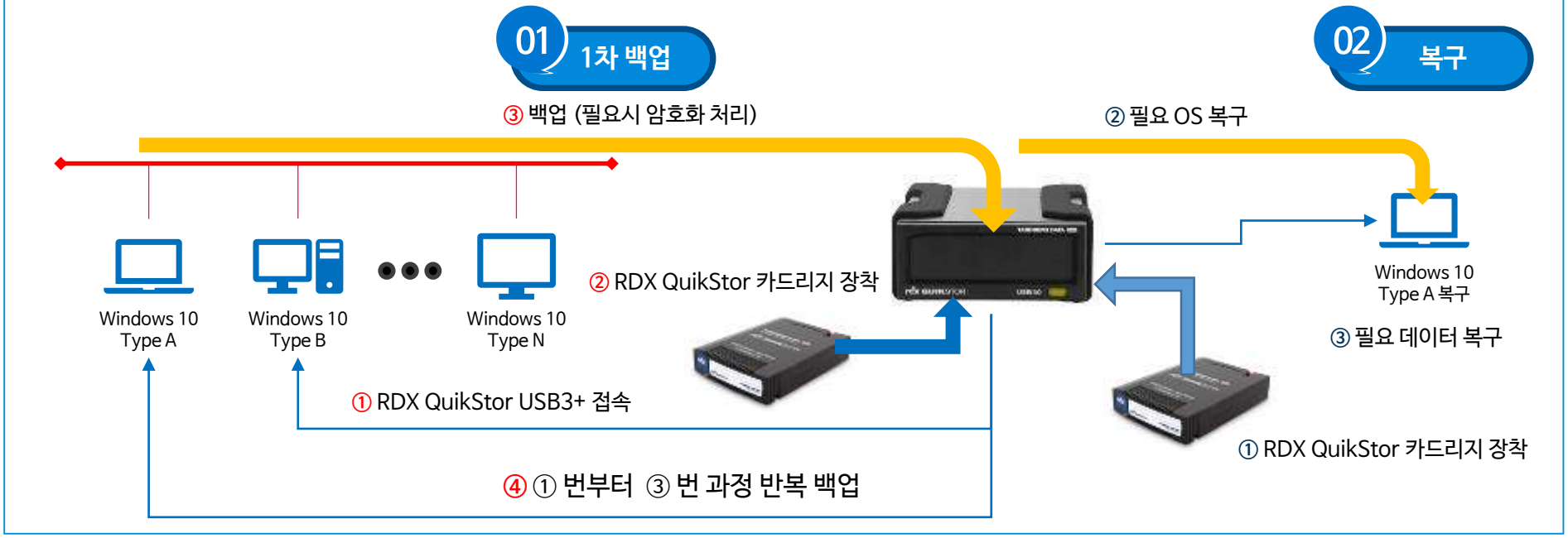
Chapter Ⅳ X86 서버 백업 구성 방안

01 RDX QuikStor USB3+ 표준 PC 백업

1대의 RDX QuikStor USB3+ 이용 표준 PC의 OS 백업 및 복구

- PC 설치 유형(OS, Application 설치 등)에 따라서 표준 PC 환경을 구축하고, 정기적인 패치 및 관리로 표준 PC로 운영
- 1대의 RDX QuikStor USB3+와 표준 PC 수량 만큼의 Tandberg RDX Cartridge 를 도입
- 백업 대상 PC의 수량에 해당하는 PC 백업 솔루션(ZConverter Windows Backup Professional Edition) 도입
- **특정 PC에 문제가 발생하는 경우 RDX QuikStor USB3+와 백업 이미지를 이용하여 OS 복구 후 개별 데이터 복구**

표준 PC OS 백업 수행 방안

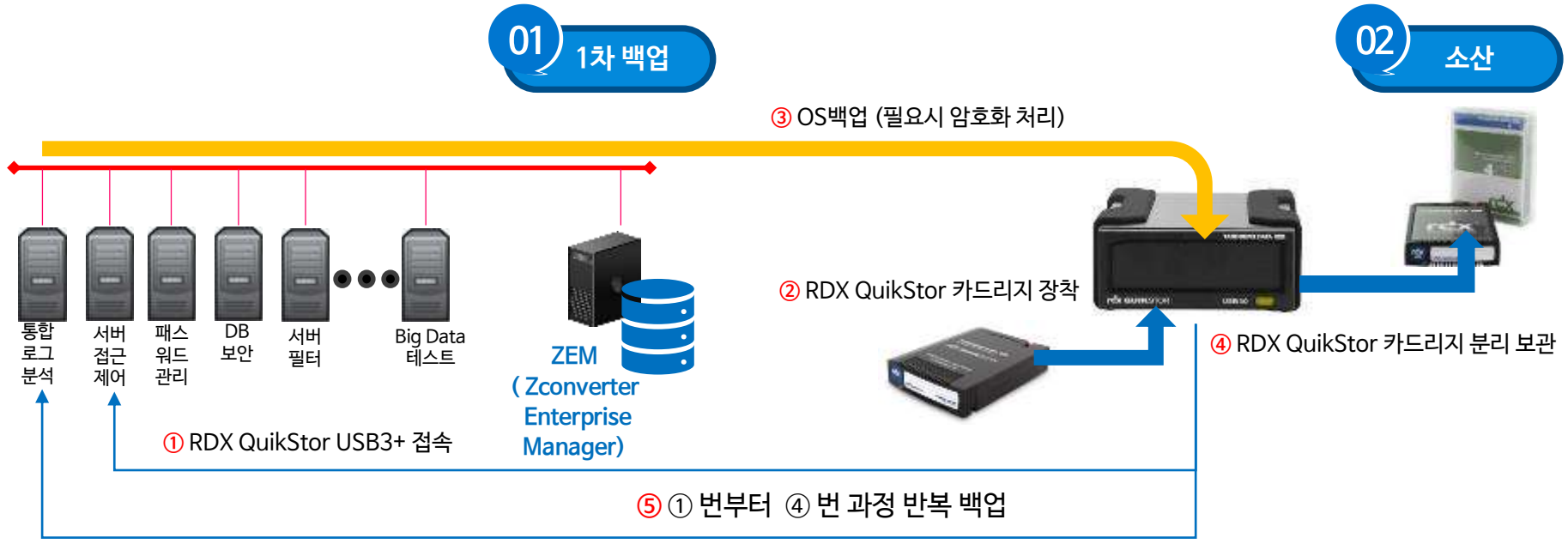


02 RDX QuikStor USB3+ 개별 백업

1대의 RDX QuikStor USB3+ 이용 다수 서버 직접 접속 OS 백업

- 1대의 RDX QuikStor USB3+와 대상 서버 수량 만큼의 Tandberg RDX Cartridge 를 도입
- 백업 대상 서버의 수량에 해당하는 백업 솔루션(ZConverter Server Backup ENT Server Access License) 도입
- 신규 설치, OS 버전업, 패치 적용 전후 등 백업이 필요한 서버에 RDX QuikStor 를 연결하고 백업 및 소산
- **가장 간단한 구성과 저렴한 비용으로 가장 안전한 소산 백업을 수행하여 문제 발생시 신속한 복구가 가능함**

OS 백업 개별 수행 방안

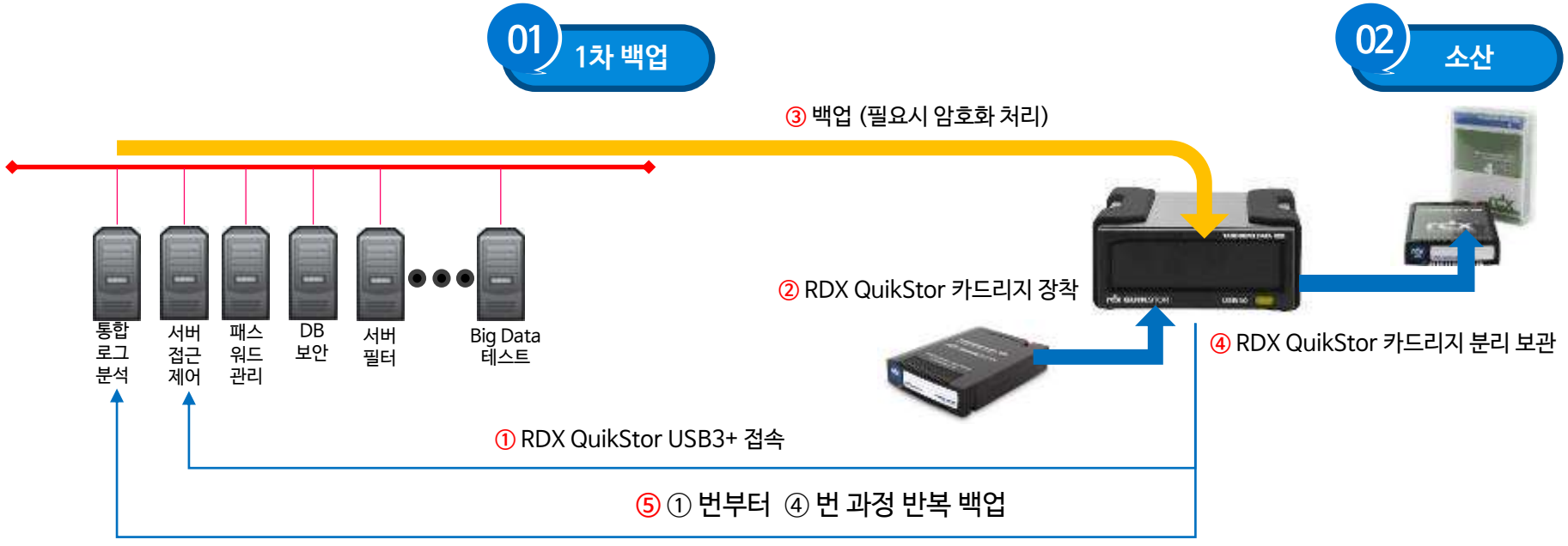


03 RDX QuikStor USB3+ 추가 소산 백업

1대의 RDX QuikStor USB3+ 이용 다수 보안 장비(어플라이언스) 소산 백업

- 1대의 RDX QuikStor USB3+와 대상 장비 수량 만큼의 Tandberg RDX Cartridge 를 도입
- 신규 설치, OS 버전업, 패치 적용 전후 등 백업이 필요한 보안 장비(서버 등)에 RDX QuikStor 를 연결
- OS의 명령어(cp, tar 등)을 이용하여 **보안 장비의 하드 디스크 등에 저장되어 있는 로그 및 정책 정보를 백업 및 소산**
- **서버의 디스크를 이용하여 로그 및 백업을 저장한 경우 간단한 구성으로 물리적인 소산을 적용 가능**

보안 장비 소산 백업 방안

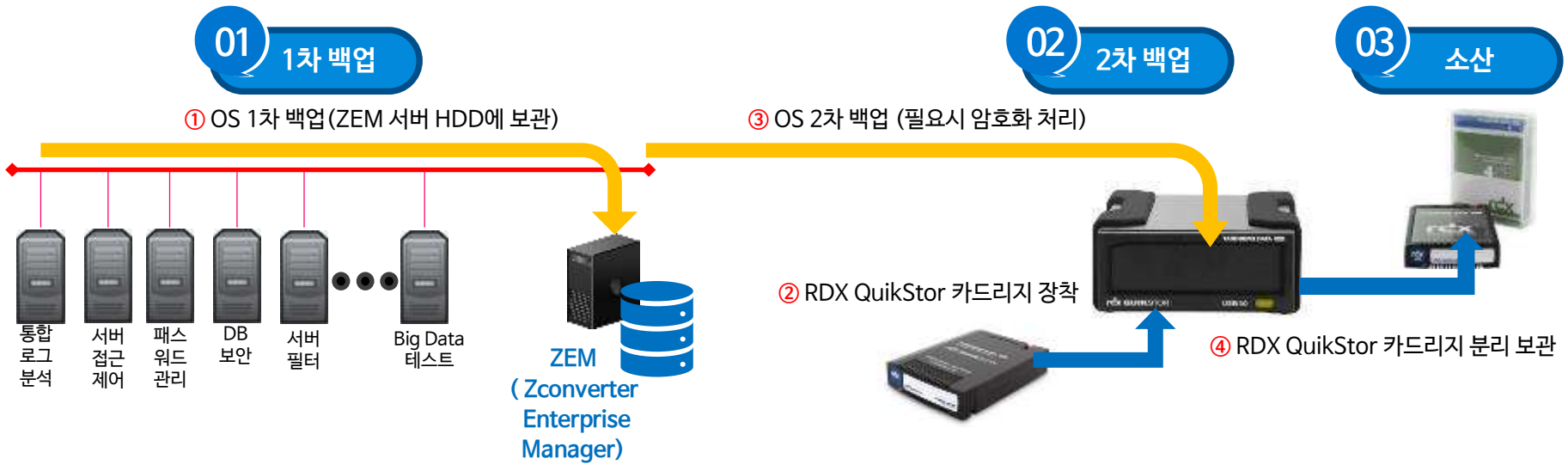


04 RDX QuikStor USB3+ 통합 백업

1대의 RDX QuikStor USB3+ 이용 다수 서버 통합 OS 백업

- 1대의 RDX QuikStor USB3+와 대상 서버 수량 만큼의 Tandberg RDX Cartridge 를 도입
- 백업 대상 서버의 수량에 해당하는 백업 솔루션(ZConverter Server Backup ENT Server Access License) 도입
- 신규 설치, OS 버전업, 패치 적용 전후 등 백업이 필요한 경우 백업 메니저에서 1-2차 백업 및 소산
- **간단한 구성과 저렴한 비용으로 통합 백업 및 안전한 소산 백업을 수행하여 문제 발생시 신속한 복구가 가능함**

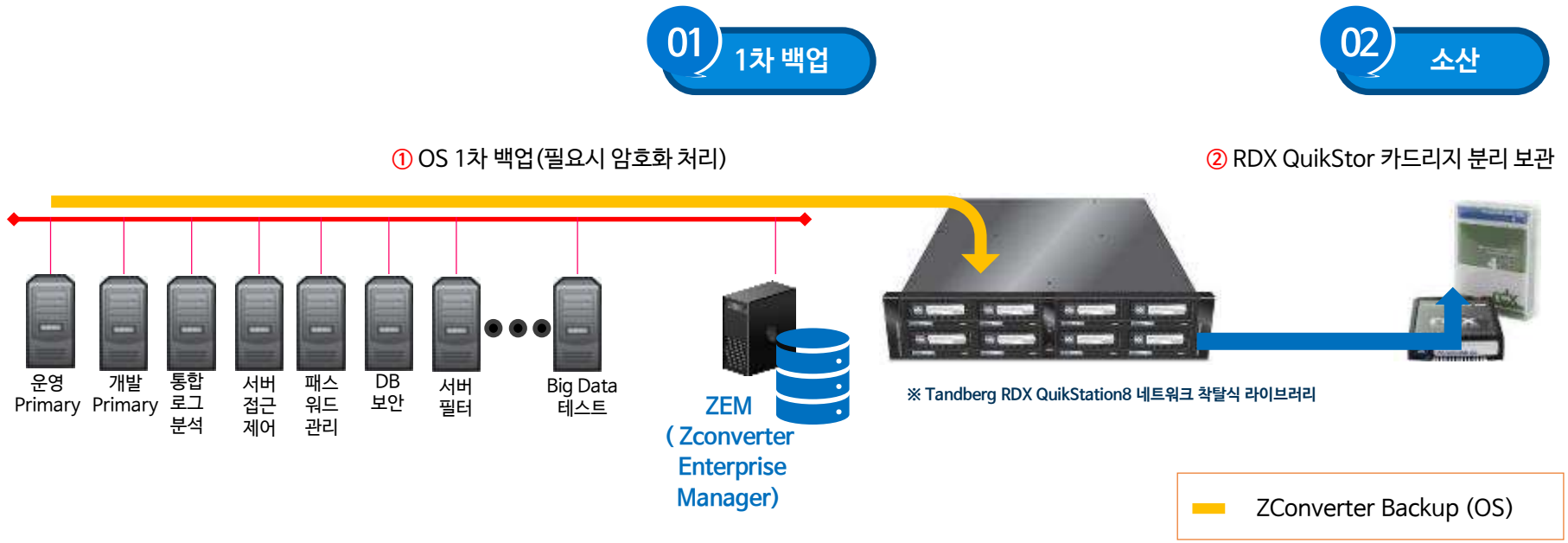
OS 통합 백업 수행 방안



RDX QuikStation8 이용 다수 서버 통합 OS 백업

- 백업 대상 서버의 OS를 착탈식 백업 장비인 Tandberg RDX QuikStation8 를 이용하여 1차 백업
- 소산이 필요한 경우 백업 카드리지를 물리적으로 분리하여 별도 보관 (랜섬웨어 등 복구용으로 사용)
- **Tandberg RDX QuikStation8은 온라인으로 32TB를 구성 가능하며, 32TB 이상의 용량은 카드리지의 교체로 무제한으로 구성 가능함**

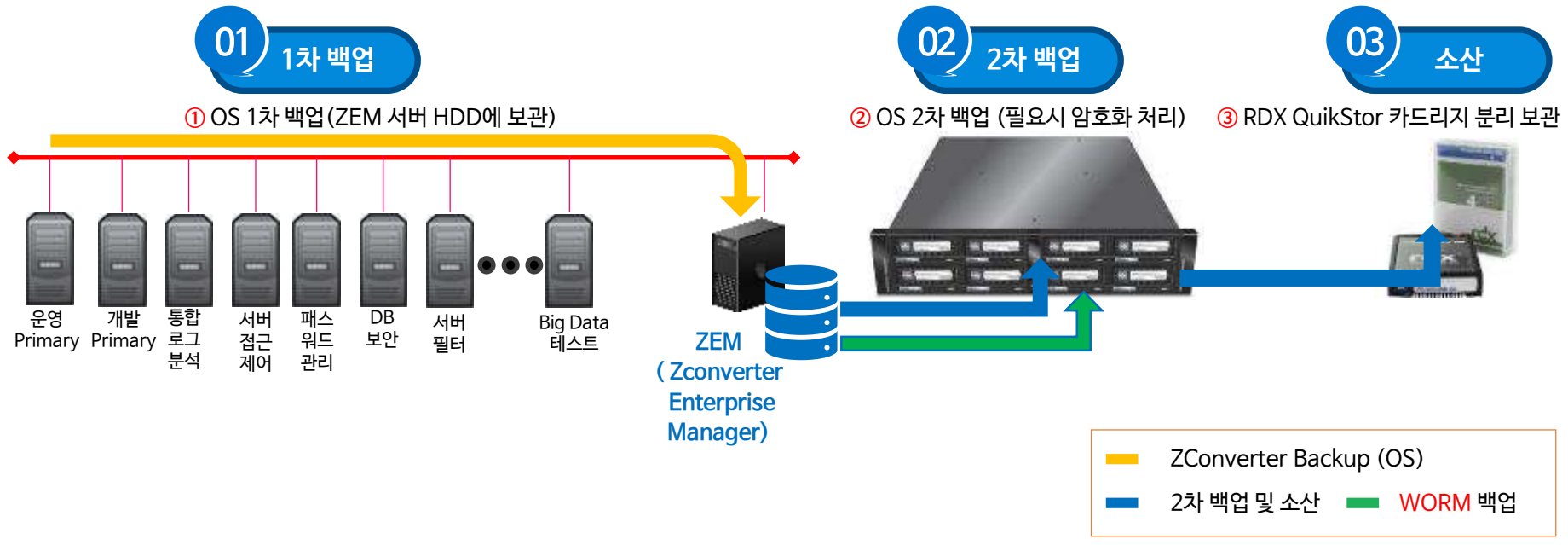
OS 통합 백업 수행 방안



RDX QuikStation8 이용 다수 서버 통합 OS 백업

- 백업 대상 서버의 OS를 ZConverter Appliance의 백업용 디스크를 이용하여 1차 백업
- 1차로 백업한 이미지를 착탈식 백업 장비인 Tandberg RDX QuikStation8 를 이용하여 2차 백업
- 소산이 필요한 경우 백업 카드리지를 물리적으로 분리하여 별도 보관(랜섬웨어 등 복구용으로 사용)
- **랜섬웨어 감염이나 위변조 방지를 위한 대비로 Tandberg Data RDX의 WORM 기능을 이용 백업 가능**

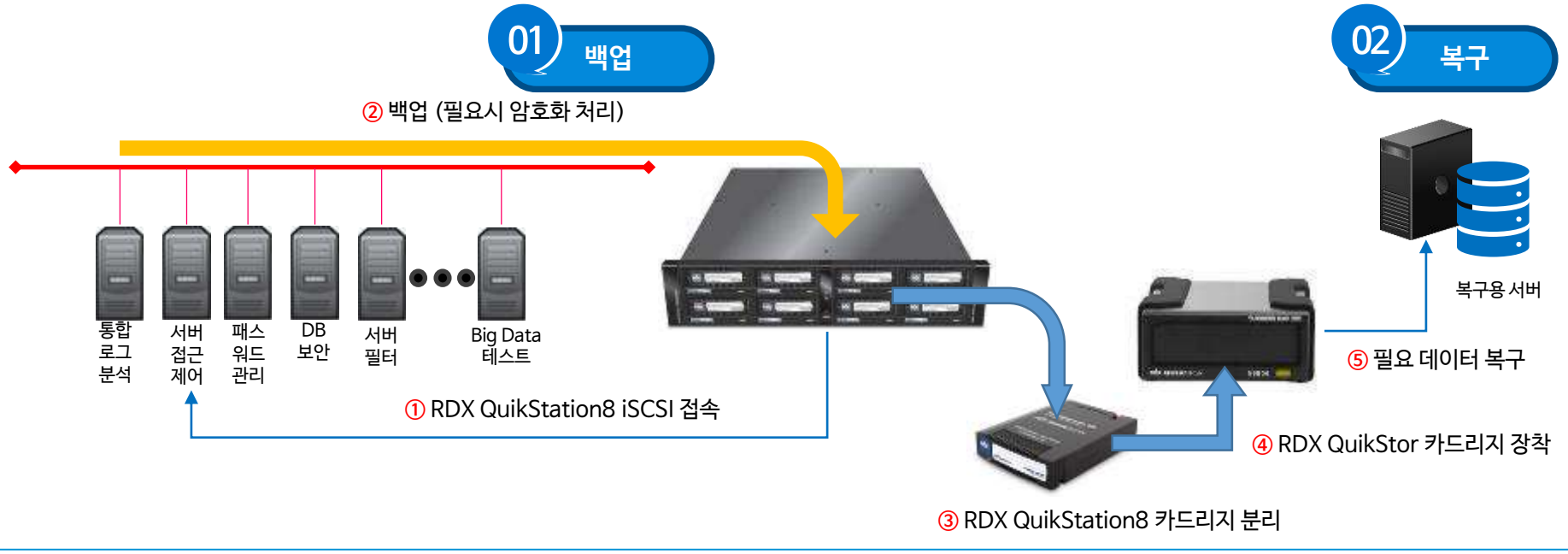
OS 통합 백업 수행 방안



RDX QuikStation8 이용 다수 서버 통합 데이터 백업 및 RDX QuikStor 이용 복구

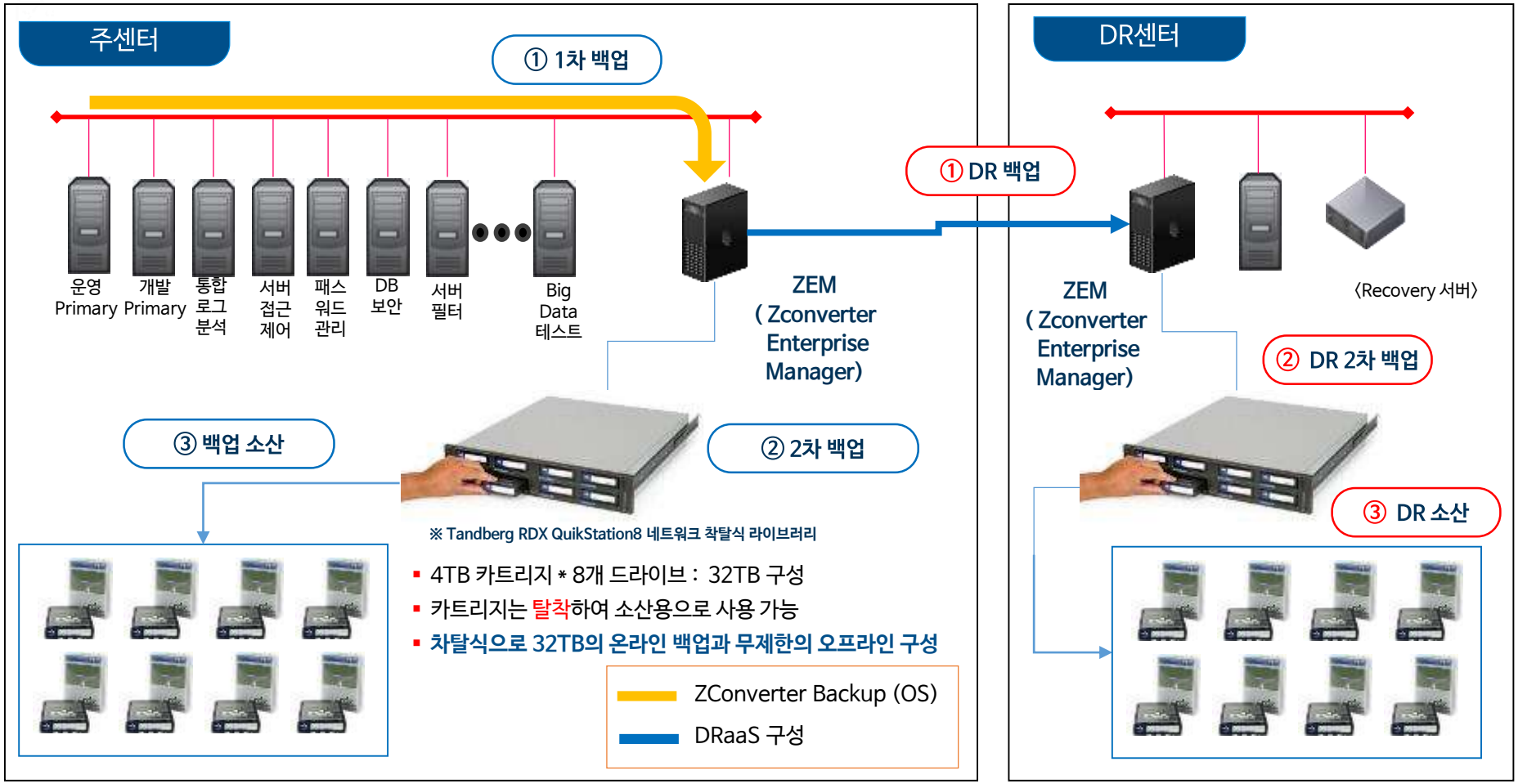
- 백업 대상 서버와 Tandberg RDX QuikStation8 를 iSCSI로 연결하여 볼륨을 할당
- 백업 솔루션(ZConverter Appliance)이나 OS명령어 등을 이용하여 할당된 볼륨 이용하여 백업
- 소산이 필요한 경우 백업 카드리지를 물리적으로 분리하여 별도 보관(랜섬웨어 등 복구용으로 사용)
- 특정 서버의 데이터에 대한 복구가 필요한 경우 카드리지를 RDX QuikStor USB3+ 에 장착하여 확인

데이터 통합 백업 수행 방안



08 RDX QuikStation8 다중(DR) 백업

IDC와 DRC의 이중화된 백업 및 소산 구성이 가능하여 다양한 복구



Chapter V X86 서버 백업 필요 근거

정보자산에 대한 정의 및 보호체계를 수립하고 활용 상태를 감사하여 보호대책을 적용

정보자산 처리현황은 ?

- 사용자(현업, 운영)
- PC (개인), 서버
- 보안 장비 등 솔루션
- 백업 및 소산
- 기타 전자적 처리 정보자산

우리 회사의 정보자산은 ?

- 관련 법규 요구 사항
  고유식별정보, 정보자산 등
- 내부 중요 기밀 정보
- 기타 중요 정보자산

정보자산 보호대책은 ?

- 암호화 및 접근 통제
- APT, 랜섬웨어 공격 대응
- 중앙 집중화
- 백업 및 복구
- 삭제 및 폐기

개인정보보호법 “고유식별정보“ 등 법규 요구 및 고객정보와 내부 기밀 정보 등을 포함

01 개인정보보호법 “고유식별정보“, 신용정보법 ”개인신용정보” 등 관련 법규에서 정의하는 정보

02 성명, 전화번호, E-Mail, 카드번호, 계좌번호 등 불법 유출되면 오용 가능한 개인의 민감정보

03 회계, 인사, 마케팅, 기획, 대외비 문서 등 외부 유출이 금지되는 내부 기밀 정보

비밀 분류(등급) 예시

1급 비밀 (Top Secret)

- 누설(unauthorized disclosure)되는 경우, 국가 안전에 상당히 심각한 위해(exceptionally grave damage)를 끼칠 것이 합리적으로 기대되는 정보
- 국가방위 및 외교에 결정적인 영향을 주는 사항

2급 비밀 (Secret)

- 누설되는 경우, 국가 안보에 심각한 위해(serious damage)를 끼칠 수 있는 정보
- 국가방위에 중요한 손해를 초래할 우려가 있는 것으로서 조약, 회의 등의 부분적인 사항 등 국제 관계에 중대한 영향을 미치는 비밀활동

3급 비밀 (Confidential)

- 누설되는 경우, 국가 안보에 위해(damage)를 끼칠 수 있는 정보
- 국가외교 상황 중 공개됨으로써 적 또는 가상의 적국에게 유리하게 악용될 우려가 있는 사항

02 정보자산 ?

DB, 로그, 녹취 및 영상, 어플리케이션 및 솔루션 로그 등 모든 형태의 "정보자산"

DBMS 등	▪ ORACLE, MS SQL 등 운영하고 있는 DBMS에 저장되어 있는 개인정보 ▪ IBM DB2 , Teradata, 보안 솔루션의 DB 등 자사에서 운영하고 있는 모든 DBMS 포함
데이터 파일	▪ 배치나 대외계(금결원, 심평원, 손보협회 등)에서 업무 처리를 위하여 SAM 파일 형태로 저장되는 파일 ▪ 기타 업무 처리를 위하여 개인정보를 포함하여 저장되는 파일(임시 파일, 데이터 파일 등) ▪ **백업이나 소산을 위하여 LTO, DAT 등의 백업 매체에 저장되어 있는 백업 파일**
로그 파일	▪ WEB, WAS(AP), DB 서버 등에서 운영되는 어플리케이션에서 파일 형태로 저장되는 로그 파일 ▪ **보안 관련 장비(서버, DB 접근 통제 등) 등 기타 서버에서 개인정보를 포함하는 로그 파일**
이미지 파일	▪ 스캐너 등을 이용하여 이미지 형태로 저장되는 파일(신분증, 각종 장표, 기타 이미지 파일) ▪ 그룹웨어나 전자 결재 등에서 첨부 파일로 저장되는 이미지 파일이나 문서 파일 ▪ 공인인증서를 대체하는 바이오 정보(홍채, 정맥, 지문 등)의 이미지 파일
동영상 파일	▪ CCTV 등 개인를 식별할 수 있는 형태로 저장된 동영상과 개인정보가 포함되어 있는 동영상 파일
음성(녹취) 파일	▪ 콜센터 등에서 개인정보를 포함하는 녹취 파일 및 음성 파일(소산용 백업도 포함)
빅데이터 파일	▪ 하둡, 스플렁크 등 빅데이터 처리 시스템에서 저장된 데이터(개인정보 비식별 조치 적용 데이터 제외)
기타 파일	▪ E-Mail 서버 , PC 백업 , 외장 저장 매체(USB, HDD 등)에 저장된 데이터 ▪ 인쇄 및 FAX 서버 등 비정형으로 저장되는 전자 파일에서 개인정보를 포함한 파일

02 정보자산 ?

각종 서버, 보안 장비, 스토리지, 백업 등 모든 형태의 “정보자산”을 저장하는 장비

WEB/WAS/AP FEP 서버 등	▪ 각 서버에서 운영하는 어플리케이션에서 저장하는 각종 파일(로그, 임시 파일, 데이터 파일 등) ▪ **디버깅 용으로 저장하거나 외부 기관과의 전문 송수신을 위하여 저장되는 내용은 평문 형태로 저장되어 있어 보안상 매우 취약함**
DB 서버	▪ DBMS 내에 저장되는 개인정보(암호화 적용 및 미적용 구분 확인 필요) ▪ DBMS 가 저장하는 접속 기록 등 로그에서 저장하는 각종 파일 ▪ DB서버에서 운영되는 배치 등 어플리케이션에서 저장하는 각종 파일(로그, 임시 파일, 데이터 파일 등)
이미지 처리 서버	▪ BPR(PI)에서 스캐너 등을 이용하여 이미지 형태로 저장되는 개인정보가 포함된 파일 ▪ 그룹웨어나 전자 결재 등에서 첨부 파일로 저장되는 이미지 파일이나 문서 파일
녹취(음성) 처리 서버	▪ 콜센터에서 고객의 업무 처리를 위하여 개인정보를 포함하는 녹취 파일
빅 데이터 서버	▪ 하둡, 스플렁크 등 빅데이터 처리 시스템 및 클라우드, IoT 장비 등에 저장된 데이터
보안 관련 서버	▪ **서버 접근 통제나 DB 접근 통제 솔루션에서 모니터링을 위하여 저장하는 로그** ▪ 기타 보안 장비에서 모니터링을 위하여 저장하는 로그(보안 어플라이언스 장비의 로그 등)
기타 서버	▪ CCTV, 인쇄 및 FAX 서버 등 비정형으로 저장되는 전자 파일에서 개인정보를 포함한 파일
백업 장비 및 소산 Tape	▪ 각종 개인정보를 처리하는 서버의 데이터를 보관하는 백업 장비에 포함되어 있는 개인정보 ▪ **소산용으로 별도로 저장하고 있는 백업(LTO, DAT, DVD 등)에 저장되어 있는 개인정보**

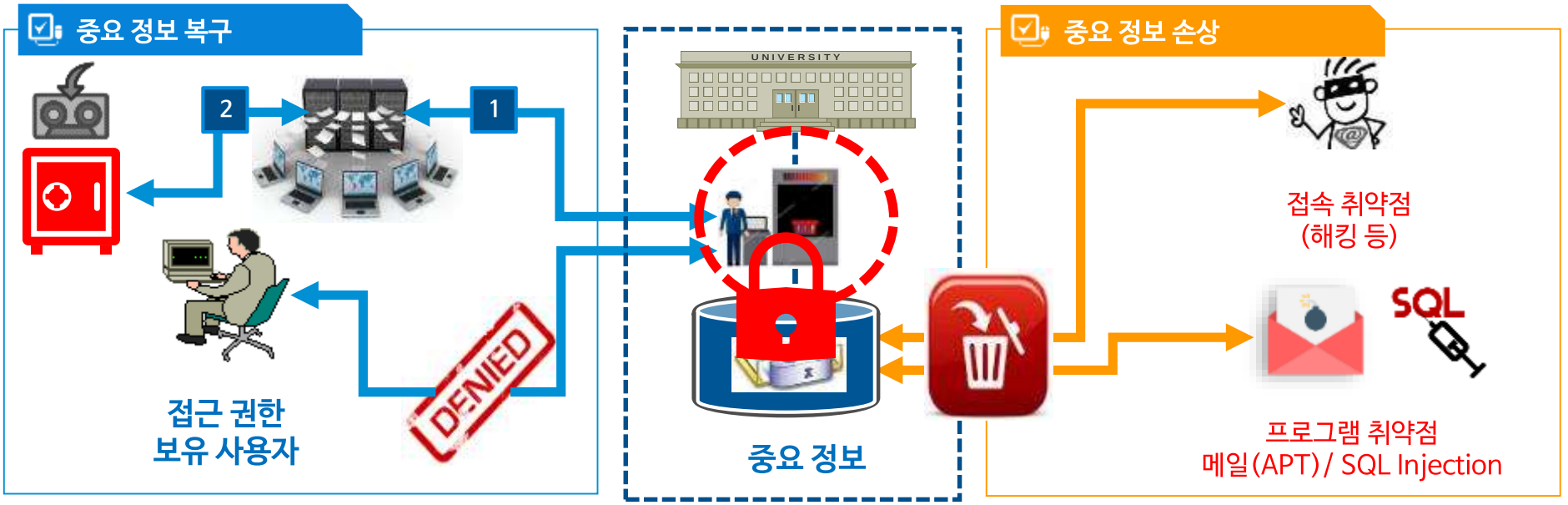
03 정보자산 보호 ?

랜섬웨어 및 해커 등에 의한 중요 정보 손실 대응 위한 안전한 백업 및 복구

01 메일을 이용한 APT (피싱, 스피어피싱)공격 등 정보 위변조가 발생한 경우 백업을 이용한 복구

02 랜섬웨어에 의한 주요 데이터 암호화 발생시 해커 협상이 아닌 백업을 이용한 복구

03 최후의 보호 조치는 백업한 정보로 복구를 하는 것이므로 별도의 안전한 상태(소산)로 보관

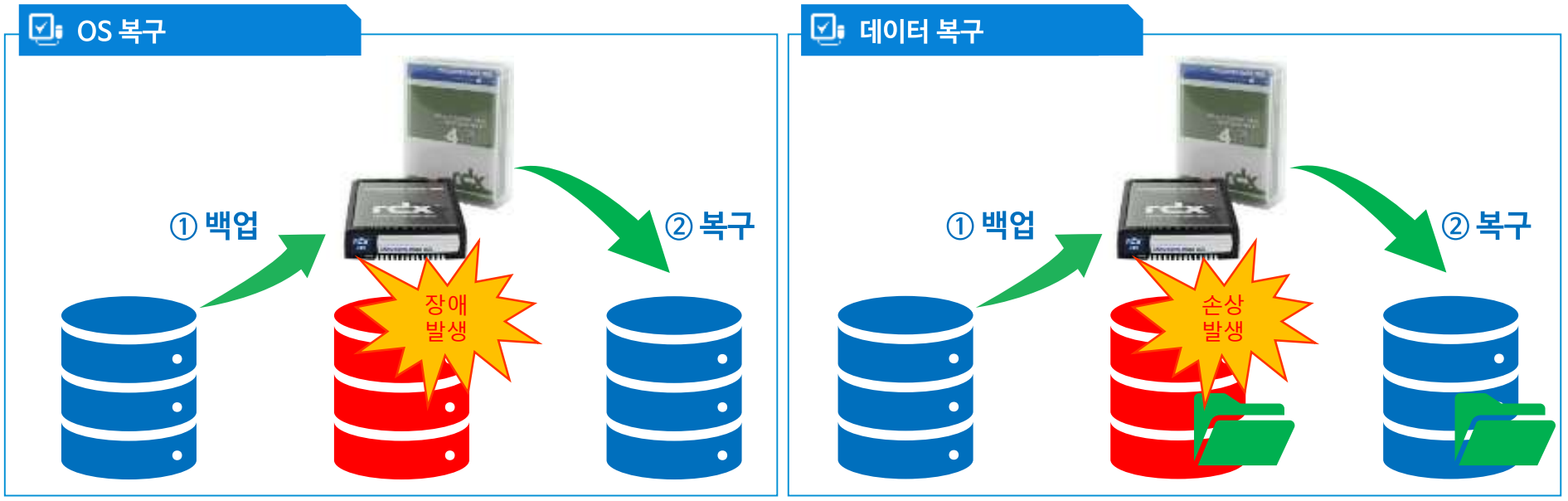


HDD의 물리적 장애 및 OS, 데이터, App 이상에 대한 신속한 복구

01 HDD의 물리적 장애가 발생하는 경우 OS, App 재설치 없이 신속한 복구

02 개인 PC는 OS 및 데이터 백업, 중요 정보는 중앙 집중화하여 정기적으로 백업

03 최후의 보호 조치는 백업한 정보로 복구를 하는 것이므로 별도의 안전한 상태(소산)로 보관



개인정보보호법의 개인정보 보호를 위한 관리적인 보호 조치 조항

출처 : 개인정보의 안전성 확보조치 기준 [행정자치부고시 제2016-35호, 2016.9.1, 전부개정])

정보자산의 안전성 확보조치 기준

구분	내용
제4조 (내부 관리계획의 수립·시행)	① 개인정보처리자는 개인정보의 분실·도난·유출·**위조·변조 또는 훼손되지 아니하도록** 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립·시행하여야 한다. **7. 접속기록 보관 및 점검에 관한 사항**
제8조 (접속기록의 보관 및 점검)	① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 **접속한 기록을 6개월 이상 보관·관리**하여야 한다. ② 개인정보처리자는 **개인정보의 분실·도난·유출·위조·변조 또는 훼손 등에 대응**하기 위하여 개인정보처리시스템의 접속기록 등을 반기별로 1회 이상 점검하여야 한다.
제12조 (재해·재난 대비 안전조치)	① 개인정보처리자는 화재, 홍수, 단전 등의 재해·**재난 발생 시 개인정보처리시스템 보호**를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다. ② 개인정보처리자는 재해·재난 발생 시 **개인정보처리시스템 백업 및 복구를 위한 계획을 마련**하여야 한다.

04 관련 법규 : 신용정보법

금융회사에 적용되는 정보보호 관련규제를 "신용정보법"으로 일원화

신용정보법 관련 항목

구분	내용	비고
안전 보호	▪ 신용정보법 제19조(신용정보전산시스템의 안전보호) ① 신용정보회사등은 신용정보전산시스템(제25조제6항에 따른 신용정보공동전산망을 포함한다. 이하 같다)에 대한 **제3자의 불법적인 접근, 입력된 정보의 변경 · 훼손 및 파괴, 그 밖의 위험**에 대하여 대통령령으로 정하는 바에 따라 **기술적 · 물리적 · 관리적 보안대책을 수립 · 시행**하여야 한다.	신용정보회사 등에게 대통령령으로 정하는 위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다. 다만, 제1호에 해당하는 행위가 있는 경우에는 50억원 이하의 과징금을 부과할 수 있음
처벌 내용	**신용정보법 제42조의2(과징금의 부과 등)** **1. 개인비밀을 분실 · 도난 · 누출 · 변조 또는 훼손당한 경우** 2. 개인비밀을 업무 목적 외에 누설하거나 이용한 경우 3. 불법 누설된 개인비밀임을 알고 있음에도 그 개인비밀을 타인에게 제공하거나 이용한 경우	
보호 방법	**신용정보업감독규정 [별표 3] 기술적. 물리적. 관리적 보안대책 마련 기준(제20조 관련)** ▪ Ⅱ. 기술적. 물리적 보안대책 2. 접속기록의 위·변조방지 ① 신용정보회사등은 개인신용정보취급자가 개인신용정보처리시스템에 접속하여 개인신용정보를 처리한 경우에는 **처리일시, 처리내역 등 접속기록을 저장**하고 이를 월 1회 이상 정기적으로 확인·감독한다. ② 신용정보회사등은 개인신용정보처리시스템의 **접속기록을 1년 이상 저장**하고, **위·변조되지 않도록 별도 저장장치에 백업 보관**한다.	

해킹 등 전자적 침해행위로 인한 사고를 방지하기 위한 정보보호시스템 설치 및 운영

전자금융감독규정 관련 항목

항목	내용	비고
제13조 (전산자료 보호대책)	① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다. **8. 중요도에 따라 전산자료를 정기적으로 백업하여 원격 안전지역에 소산하고 백업내역을 기록·관리할 것** **9. 주요 백업 전산자료에 대하여 정기적으로 검증할 것**	
제14조 (정보처리시스템 보호대책)	금융회사 또는 전자금융업자는 정보처리시스템의 안전한 운영을 위하여 다음 각 호를 포함한 보호대책을 수립·운용하여야 한다. **8. 중요도에 따라 정보처리시스템의 운영체제 및 설정내용 등을 정기 백업 및 원격 안전지역에 소산하고 백업자료는 1년 이상 기록·관리할 것**	
제15조 (해킹 등 방지대책)	② 제1항제1호의 규정에 따른 정보보호시스템을 설치·운영하는 경우에는 다음 각 호의 사항을 준수하여야 한다. **6. 시스템 장애, 가동중지 등 긴급사태에 대비하여 백업 및 복구 절차 등을 수립·시행할 것** ④ 금융회사 또는 전자금융업자는 **해킹 등 전자적 침해행위로 인한 피해 발생시 즉시 대처할 수 있도록 적절한 대책을 마련**하여야 한다.	

04 관련 법규 : 금감원 IT 검사업무 안내서

IT보안 및 정보보호 부문, 대형은행 기준 체크리스트

출처 : 금융감독원 IT 검사업무 안내서 2016. 12.

IT서비스 제공 및 지원 부문

세부평가항목	점검 내용	비고
재해복구 및 비상대책	o 최종사용자 컴퓨팅 관련 비상대책이 적정한지 다음과 같이 점검한다 - 최종사용자컴퓨팅 관련 비상대책이 수립되어 있는지 - 최종사용자컴퓨팅 관련 주요 소프트웨어, 데이터를 백업하고 있는지 - 최종사용자컴퓨팅 관련 비상대책에 따른 주기적 훈련이 적절한지	
전자금융거래 고객 보호	o 전자금융 거래내역 기록 및 보관이 적정한지 다음과 같이 점검한다 - 전자금융거래 관련 로깅 대상, 백업대상, 소산대상 및 절차, 보존기한 등이 내규화되어 있는지 - 전자금융거래 관련 로깅 대상, 백업대상, 소산대상 및 절차, 보존기한 등이 내규대로 실제로 이행되고 있는지	

IT보안 및 정보보호 전략

세부평가항목	점검 내용	비고
정보보안 정책과 규정	o 정보보호시스템이 아래 각 사항을 준수하는지 1) 최소한의 서비스번호(port)와 기능만을 적용하고 업무목적 이외의 기능 및 프로그램을 제거할 것 **4) 시스템 장애, 가동중지 등 긴급사태에 대비하여 백업 및 복구 절차 등을 수립·시행할 것** o 이메일 등의 관리절차가 적정한지 다음과 같이 점검한다 **- 이메일, 메신저 등을 이용하여 송수신한 회사업무 자료나 정보 등을 백업하여 일정 기간 보관하고 있는지**	

IT보안 및 정보보호 부문, 대형은행 기준 체크리스트

출처 : 금융감독원 IT 검사업무 안내서 2016. 12.

IT부문 실태평가용 체크리스트

평가항목	세부 평가항목	세부평가항목에 대한 점검사항	선택(옵션) 표시							
			은행		비은행		보험		증권	
			시중. 특수	지방은행	카드사	종금사	대형	중소형	대형	중소형
4.비상계획	하드웨어 백업 및 복구	- IT센터 기능 마비시의 하드웨어 대체처리 대책								
		- 자체 백업장비의 수용 능력								
		- 외부기관 IT장비 수용 능력								
		- 백업시설 변동정보 확보								
		- 비상시 복구설비의 물리적 보안대책								
	소프트웨어/데이터 백업 및 복구	- 백업 및 소산의 적정성								
		- 복구절차의 적정성								

구분	대상업무	호스트명	도입년도	회사명	모델명	OS(버전)	설치장소	이중화 구성	백업 방식	보관 주기	소산 주기	소산 장소	백업 대상	저장 매체	백업 정책	백업 시작 시간	백업 종료 시간	비고
계정계																		
정보계																		
개발																		
...																		

정보보호 솔루션 전문가 집단

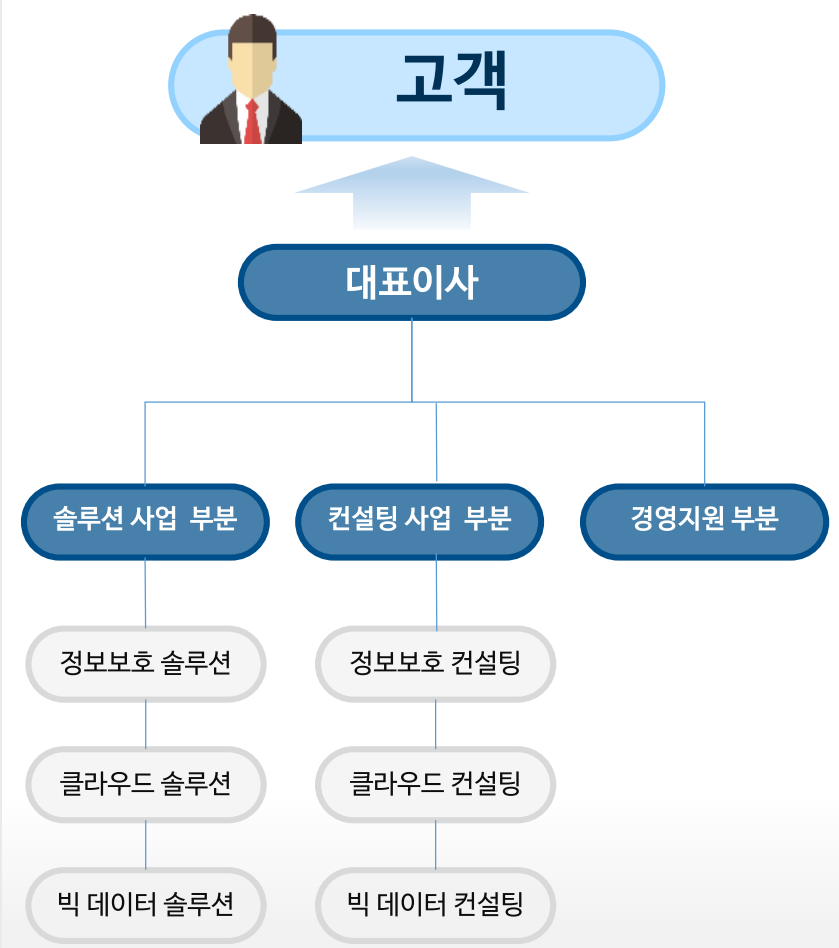
Chapter VI 세종정보보안(주)

01 세종정보보안(주)

세종정보보안은 개인정보보호 솔루션 및 클라우드/빅 데이터 솔루션 전문 IT기업입니다.

세종정보보안㈜

대 표 자	이 국 연
설 립 일	2016년 6월
주 소 (본 사)	서울시 금천구 가산디지털1로 30 에이스하이엔드 10차 607호
자 본 금	5천만원
신 용 등 급	B0
사 업 분 야	▪ 개인(신용)정보 보호 솔루션 ▪ 클라우드 솔루션 ▪ 빅데이터 솔루션 ▪ 개인정보보호, 가상화, 클라우드 컨설팅
주 요 연 혁	▪ 2016년 : 세종정보보안 설립 ▪ 2016년 : NHN엔터테인먼트 클라우드 솔루션 파트너 ▪ 2016년 : DB보안전문 솔루션 피앤피시큐어 파트너 ▪ 2016년 : DB암호화 솔루션 이글로벌시스템 파트너 ▪ 2016년 : 망연계 솔루션 한싹시스템 파트너 ▪ 2016년 : 퓨어스토리지 파트너 ▪ **2016년 : 메일 보안 솔루션 리투인소프트웨어 기술 총판**



정보자산 보호를 위한 최종 방어 "백업 및 복구" 솔루션 : Zconverter, Tandberg Data RDX

정보자산 보호를 위한 X86 서버 백업 솔루션 소개

감사합니다
Thank you

세종정보보안㈜
강 윤 채 / 부대표
T : 010-2047-5543
E : yckang@sejonginfo.co.kr