랜섬웨어 대응을 위한 안전한 정보시스템 백업 가이드(안)

2021. 11.

과학기술정보통신부

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

목 차

<표 차례>

<그림 차례>

정보시스템 백업 가이드
(Guideline for Backup of Information Systems)

1. 개요

과거 랜섬웨어 공격은 불특정 다수를 대상으로 데이터를 암호화하고 이에 대한 몸값을 요구하는 방식이 대부분이었다. 그러나 최근에는 높은 금액을 지불할 수 있는 대규모 엔터프라이즈 환경이 주로 공격 대상이 되고 있고, 암호화 뿐만 아니라 데이터 유출 후 인터넷 공개를 미끼로 협박하는 형태로 공격 방식이 진화되고 있다.

이러한 공격 방식의 진화는 개인 혹은 기업에서 랜섬웨어의 대응 전략으로 데이터 백업을 강화해 더 이상 데이터 암호화만으로 수익을 얻기가 어려워졌기 때문이다. 랜섬웨어 감염을 100% 방어할 수 없다면 데이터 백업이 가장 효과적인 대응 전략이 될 수 있다. 이런 대응 전략으로 인해 최근의 랜섬웨어 공격자는 데이터 백업을 무력화하기 위해 노력하고 있다. 최근 공격자들은 로컬 혹은 공유 드라이브에 백업된 데이터까지 암호화하고 심지어 타겟형 공격과 같이 특정 시스템을 거점으로 백업 데이터의 위치를 찾아 감염시키는 방식으로 백업 체계를 무력화하기도 한다.

랜섬웨어 공격자들이 주로 사용하는 데이터 백업 무력화 기법은 다음과 같다.

▷ **볼륨 섀도 복사본 삭제**

랜섬웨어는 윈도우 시스템의 자체 백업 기능인 볼륨 섀도 복사본(VSC, Volume Shadow Copy)을 삭제해 이전 파일 복원을 차단한다.

▷ **네트워크로 공유된 백업 암호화**

일부 백업 솔루션은 솔루션의 기본 폴더명을 이용하여 네트워크로 공유된 경로에 데이터를 백업한다. 랜섬웨어 공격자는 기업 네트워크에서 이런 백업 폴더를 찾아 함께 암호화한다.

▷ **백업 솔루션 악용**

백업 솔루션은 자체 API를 사용해 기업 내 데이터 백업을 관리한다. 공격자는 탈취한 크리덴셜이나 취약점을 사용해 백업 관리 API에 접근하고 이를 통해 백업을 삭제하거나 암호화한다.

▷ **손상된 데이터 백업 유도**

보통의 랜섬웨어는 최초 침투 후 바로 데이터를 암호화하지만 최근의 일부 랜섬웨어는 타겟형 공격과 같이 내부망을 은밀히 침투해 데이터를 손상시켜 불완전한 데이터가 백업되도록 기다린 후, 원본 데이터를 암호화한다. 이 경우 백업 데이터가

이미 손상되었기 때문에 데이터를 정상적으로 복원할 수 없다.

랜섬웨어는 금전적 이익을 목적으로 나타났고 수익 창출의 가능성이 이미 증명된만큼 앞으로도 지속 발생할 것으로 보이며, 공격 방식도 진화할 것으로 예상된다. 이에 대한 가장 효과적인 대응이 데이터 백업이므로 특히 기업의 경우 실패하지 않은 데이터 백업 전략을 고민해야 한다.

본 가이드에서는 정보시스템 백업 체계 구성을 위한 정보를 제공하고, 백업시스템을 구축 · 운영하기 위한 절차 및 방법에 대해 설명한다. 또한 악성코드와 랜섬웨어 등 외부 환경의 사이버 공격 위협으로부터 백업데이터를 보호하기 위한 보호대책을 제시하고, 중소규모 기업 환경에 적합한 정보시스템 백업 구성을 위한 가이드를 제공한다.

2. 지침의 구성 및 범위

본 가이드는 중소기업 또는 비교적 소규모 서비스를 제공하는 기업에서 필요한 안전한 백업 시스템 구축 방법 및 운영 절차를 제시한다. 먼저 백업 조직 및 역할을 정의하고, 백업 조직이 백업 수행과 보안 관리를 체계적으로 수행할 수 있도록 백업 절차 및 보안 관리 절차를 설명한다. 또한, 악성코드 및 랜섬웨어 감염 시 신속한 대응에 필요한 절차를 제시한다.

백업 시스템 구성은 기업이 일반적으로 사용할 수 있는 백업 시스템 구성 방법과 랜섬웨어 감염 예방을 위한 구성에 대하여 제시한다. 백업 정책은 다양한 백업 방법에 대하여 소산 정책 또는 소규모 기업들이 반영할 수 있는 정책에 대하여 설명한다. 마지막으로 랜섬웨어 피해 등 사이버 공격 예방을 위해 필요한 백업 시스템의 보안 사항에 대하여 설명한다.

3. 백업 용어 정의

▷ **백업**

백업은 정보시스템의 장애, 화재와 같은 재해 또는 해킹으로 인한 정보의 망실에 대비하여 파일 또는 데이터베이스를 복사해 별도의 매체에 저장 및 관리하는 행위를 말하며, 대부분의 기업들이 시스템 장애시 최근 시점으로 복구해 줄 수 있는 중요 업무이다.

▷ **시스템 백업**

정보시스템 OS 영역, 시스템 설정파일, 시스템로그 등에 대한 백업을 의미한다. 데이터 백업과 구별하여 보통 OS(Operating System) 백업이라 한다.

▷ **데이터 백업**

데이터가 손상되거나 유실되는 것을 대비하여 데이터를 복사하고 다른 곳에 저장하는 것을 말한다. 저장 장소는 동일 장비 또는 다른 장비의 하드디스크 공간일

수도 있고 별도의 백업 장치일 수도 있다.
일반적으로 백업대상에는 문서, 소스 코드, DB데이터 관련 파일 등이 있다.

▷ **Cloud 백업**
클라우드 기반 백업 서비스는 흔히들 '온라인 백업'이라고 하며, 보호받아야 할 데이터를 인터넷으로 전송해 사본을 만들고, 필요 시 해당 데이터를 이용해 복원할 수 있는 백업 방식을 말한다.

▷ **백업 장비(장치)**
백업시스템을 구성하기 위해 필요한 매체, 라이브러리, 채널 등의 물리적인 설비를 의미한다. 백업 장비와 백업 장치는 동일한 용어로 정의한다.

▷ **백업 매체(미디어)**
주요 시스템의 OS, 데이터 영역에 대하여 백업하는 저장 장치로 일반적으로 테이프(Tape), 디스크(Disk) 등을 말한다.

▷ **볼팅(Vaulting)**
물리적인 오프사이트 볼트로 보내질 백업의 지정 저장 위치로 작동하는 특정 로봇과 연결된 논리적인 객체이다. "볼트"라는 용어는 오프사이트 테이프 세트의 물리적 저장소 위치와 프로세스를 함께 지칭하는 데 사용한다.

▷ **소산백업**
재난·재해 발생 시 백업된 매체를 일정거리 이상 떨어진 장소에 이격시켜서 보관하는 것으로 지진, 홍수, 화재 등의 재난·재해 발생 시 원본의 손실이 있더라도 백업매체가 원격지에 떨어져 있으므로 손실되는 것을 예방할 수 있다.

▷ **백업센터 · DR(Disaster Recovery)센터**
운영센터 재해 발생 시 즉각적인 서비스 복구를 위한 업무연속성(continuity)을 보장할 수 있는 재해복구를 위한 백업 전산센터를 의미한다.

▷ **백업구성 방식**
백업시스템을 구성하는 형태 및 특징을 의미한다. 백업 솔루션을 구분하기 위해 크게 로컬(다이렉트) 백업, 네트워크 백업, SAN(Storage Area Network) 백업으로 나눠지며 백업 규모, 시간 및 특성에 따라 그 구성 방식이 결정된다.

▷ **디스크 복제**

하드 디스크의 내용물을 다른 디스크나 이미지 파일로 복사하는 과정을 의미한다. 복제의 속도가 빠르고 복구 역시 용이하며, 보통 디스크 제공사의 복제 솔루션을 많이 사용한다.

▷ **미러링**

특정 사이트의 콘텐츠(글, 웹페이지, 이미지 파일, html 소스 등)을 특정 주기를 간격으로 자동으로 복제해 저장해 놓는 기능을 말한다.

미러링은 디스크의 RAID(Redundant Array of Independent Disks) 레벨 중 RAID 1에 해당하는 디스크 구성방법으로써 한 개의 디스크에 물리적 장애가 발생하더라도 미러링 되어 있는 디스크가 자동으로 장애가 발생한 디스크를 대체하여 서비스를 지속할 수 있다.

▷ **전체 백업(full backup)**

지정한 디렉터리 아래의 모든 파일과 디렉터리를 저장소로 복사하는 백업을 말한다. 복구 시에 일부 다른 백업 방식보다 간편하고 시간이 증분 백업에 비해 상대적으로 덜 걸린다는 장점이 있다.

▷ **증분 백업(Incremental backup)**

전체백업과는 달리 최종 전체 백업 혹은 최종 증분 백업 이후에 변경된 파일만을 복사한다. 전체 백업과 비교할 때 증분 백업은 매일 백업해야 하는 파일의 양이 적어 빠른 백업이 가능하다는 점이 장점이다. 그러나 복구 과정에서는 최종 백업된 전체 및 모든 후속 증분 이미지나 복사본까지 복구해야 하기 때문에 복구 작업이 번거로워지고 경우에 따라서는 시간이 훨씬 더 걸릴 수 있다.

▷ **차등 백업(Differential backup)**

마지막 '전체 백업' 이후 변경된 '모든' 데이터를 백업하는 방식이다. 이는 바로 이전의 전체 백업 혹은 증분 백업 이후 '변경된' 데이터만 복사하는 증분 백업과는 다르다. 일단 파일이 변경되면 예정된 다음 전체 백업 시까지 매일 백업한다. 따라서 파일이 변경될 때마다 파일 크기가 증가하게 되며, 다음 전체 백업 때까지 파일크기가 점점 커지게 된다. 하지만, 전체 백업 이미지와 가장 최근의 차등 이미지만 복구하면 되기 때문에 복구 시점에 따라 다르긴 하지만 대개 증분 백업보다 복구 속도가 빠르다.

▷ **자동화 백업(CDP(Continue Data Protection)**

일반적인 파일단위 백업 서비스와는 달리 이미지백업 (Volume Snapshots 방식)이면서 분 단위까지 백업을 받고 필요시 특정 백업 시점으로 복원 할 수 있는 백업 서비스로서 Continuous Data Protection Back-Up 이라는 의미이다.

▷ **SAN(Storage area network)**

블록 레벨 데이터 스토리지로 통합 액세스 할 수 있는 네트워크이다. SAN은 주로 서버가 로컬로 연결된 디바이스에 액세스 할 수 있도록 Disk어레이, 테이프 라이브러리 및 광학 주크 박스와 같은 스토리지 디바이스를 향상시키는 데 주로 사용된다.

▷ **랜섬웨어(Ransomware)**

악성코드의 종류로 사용자의 동의 없이 해당 컴퓨터에 불법으로 설치된다. 불법으로 설치된 랜섬웨어로 해당 컴퓨터에 저장된 파일을 암호화시켜 잠글 수 있다. 그러면 팝업 창이 뜨면서 컴퓨터가 잠겼으니 금액을 지불하지 않으면 컴퓨터에 접속할 수 없다는 경고가 나타난다.

▷ **리던던시(redundancy)**

정상 동작에 필요한 정도 이상의 여분의 장치/기능을 부가하여 안정성을 높인 백업 시스템이다.

▷ **MTTR(Mean Time To Recovery)**

수리 가능한 품목의 유지 보수성을 측정하는 기본 척도이다. 고장난 구성 요소 또는 장치를 수리하는 데 필요한 평균 시간을 의미한다. 수학적으로 표현하면, 실패에 대한 총 교정 유지 보수 시간을 주어진 기간 동안의 실패에 대한 교정 유지 보수 총 횟수로 나눈 값이다.

▷ **시스템 커널(Kernel)**

운영 체제의 핵심 부분으로서, 운영 체제의 다른 부분 및 응용 프로그램수행에 필요한 여러 가지 서비스를 제공한다.

▷ **복구시점목표(RPO: Recovery Point Objective)**

재해 상황에서 수용할 수 있는 최대 허용 데이터 손실을 정의합니다. 예를 들어 재해가 발생했을 때 벙커 노드에 두 시간 분량의 데이터가 있고 한 시간 분량의 데이터만 재생해도 된다면 RPO는 한 시간입니다. 데이터 손실을 수용할 수 없다면 RPO는 0입니다.

▷ **복구시간목표(RTO: Recovery Time Objective)**

복구 시간 목표 데이터를 반드시 복구해야 하는 최대 허용 시간 제한을 정의합니다. 재해가 발생했을 때 시스템을 즉시 사용 가능하게 만들어야 하지만 일부 데이터 손실을 용인할 수 있는 경우 RTO는 0입니다.

4. 백업 조직 및 역할

기업 내 시스템 운영 조직구성과 업무 분장은 기업 내 현황에 적합하도록 구성되어야 한다. 다음의 조직 구성 예시는 일정 규모 이상의 조직의 구성 예시로 조직 구성을 할 수 없는 소규모 기업의 경우 담당업무를 겸직하여 구성한다.

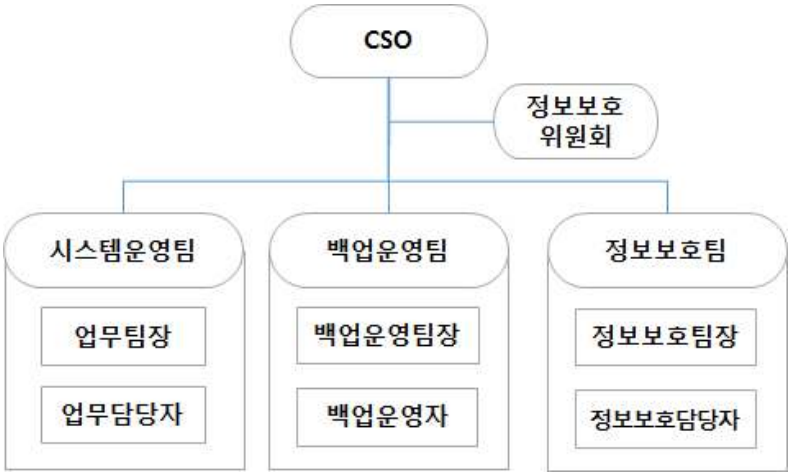
가. 백업 운영 조직도

전사 조직 구성 중 백업시스템 운영과 연관된 조직구성 예시로 중소기업과 중견기업 규모의 조직구성 예시이다.

[그림 1]는 비교적 규모가 작은 중소기업 환경을 고려한 조직구성 예시이다. 중소기업의 경우 인력 및 예산의 한계로 단일 운영팀에 여러 업무영역별 담당자(시스템운영자/백업운영자/정보보호담당자 등)가 존재하거나 구성원이 적은 경우 겸직하여 구성되어 진다.

[그림 1] 중소기업 규모의 백업
유관 조직 구성 예시

[그림 2]는 중견기업 이상 기준 조직구성 예시로 시스템운영팀, 백업운영팀, 정보보호팀, 정보보호위원회 등 운영 영역별 조직이 분리구성 되어 각각의 업무분장을 따르도록 되어 있다.



[그림 2] 중견기업 이상 백업 유관 조직 구성 예시

따라서 기업 내 백업시스템 운영을 위한 조직 구성 시 고려해야하는 부분은 각각의 시스템 운영 특성을 고려하여 업무 분장을 실시해야 하며, 백업 담당업무를 겸직하는 경우 겸직 담당자는 백업시스템에 대한 운영 능력을 보유한 담당자를 지정해야 한다.

나. 역할 분장

1) 업무 담당자

기업의 응용프로그램/서버/데이터베이스 등의 기획, 관리, 운영 업무를 수행하는 현업 담당자로서 백업 정책 설정 시 백업 대상, 유형, 시간 등에 대한 요구사항을 작성하게 된다. 중소기업의 경우 업무 담당자가 백업운영자를 겸직하여 담당할 수 도 있다.

▷ 주요 업무

- 백업 대상 시스템, 백업 유형, 백업 주기, 작업시간 등 요구사항 제시
- 신규 백업대상 시스템의 백업 요청
- 기존 백업 데이터 장애시 복구 요청
- 연간 백업 대상에 대한 백업 세부계획서 작성
- 백업 장애 발생 시 백업 운영자에게 요청

2) 업무 팀장

업무 담당 팀장은 업무 담당자에게 응용시스템/서버/데이터베이스 등에 실질적인 운영에 대하여 이행 지시를 하며, 중소기업의 경우 업무 팀장은 전체 IT인프라에 대한 총괄업무를 담당한다.

▷ 주요 업무

- 담당 시스템에 백업 계획 작성
- 업무 담당자에 시스템 운영 및 복구 지시 등
- 백업 운영부서에 백업 요청
- 백업 데이터의 복구 요청
- 백업 장애 발생 시 백업 운영자에게 요청

3) 백업 운영자

백업 작업 수행, 백업 매체 관리 등의 업무를 수행하는 담당자로서, 현업 업무 담당자로부터 백업 대상시스템 백업 요구 사항을 수렴하여 적용한다. 중소기업의 경우 업무 담당자가 백업 운영업무를 겸직할 수 있다.

▷ 주요 업무

- 신규 백업 대상 시스템 구성 및 추가
- 백업 및 복구 수행

- 모의 백업 및 복구 훈련
- 백업 수행 결과 모니터링
- 백업 장비 및 백업 매체관리
- 백업 장애 발생시 처리
- 침해사고 발생 시 정보보호부서 협조

4) 백업운영팀장

기업의 사내 백업 관련하여 이행을 위해 최종 검토 및 승인 처리업무를 수행하는 것으로 일정규모 이상의 기업은 해당업무를 분리하여 운영하나 중소기업의 경우 업무 팀장이 해당 업무를 수행 한다.

▷ 주요 업무

- 백업 운영자 지정
- 백업 및 복구 요청서를 승인
- 백업 및 복구 Data 검수 결과를 승인
- 적용 업무 Data와 관련된 비정기 백업 사유를 승인
- 백업시스템 장애 및 보안상 이슈 발생 시 정보보호 부서 협조 요청

5) 정보보호담당자

기업 내 정보보호담당자는 전사 정보시스템에 대하여 보안활동을 담당하는 역할을 수행한다. 일정 규모 이상의 기업은 정보보호 주관부서를 별도 분리하여 조직을 구성하고 있으나 중소기업의 경우 전산 부서에 정보보호 담당자를 지정하여 운영할 수도 있다.

▷ 주요 업무

- 백업 소프트웨어 도입 시 보안성 검토
- 백업 데이터의 (백업, 소산 등)의 선정 시 위험 분석
- 백업 시스템 네트워크 구성 및 시스템 접속 이력 검토
- 백업 시스템 자산에 대한 중요도 산정
- 백업 정책 선정 시 보안성 검토
- 백업 대상 데이터의 무결성 검증 여부 진단
- 연간 정보보호 교육계획 수립 및 이행
- 연간 백업 시스템, 네트워크에 대한 취약점 진단

6) 정보보호위원회

기업의 전사 정보보호 정책의 결의 및 중요 이슈 사항에 대하여 각 현업부서 팀장, 정보보호팀장, 경영진으로 구성된 최고 의결기구를 말한다. 일반적으로 일정규모 이상의 기업에 조직되어 주요한 정책 및 이슈를 협의하나, 중소기업의 경우 업무 환경상 별도 의결기구는 구성되어 있지 않을 수 있다.

▷ 주요 업무

- 위원회는 중요 시스템 백업정책에 대한 의결 및 승인
- 중요 서비스 및 데이터 유실 발생 시 담당자 긴급 소집
- 유실된 데이터 복구 방안 협의 및 이행 지시
- 연간 시스템 운영에 대한 예산안 결의

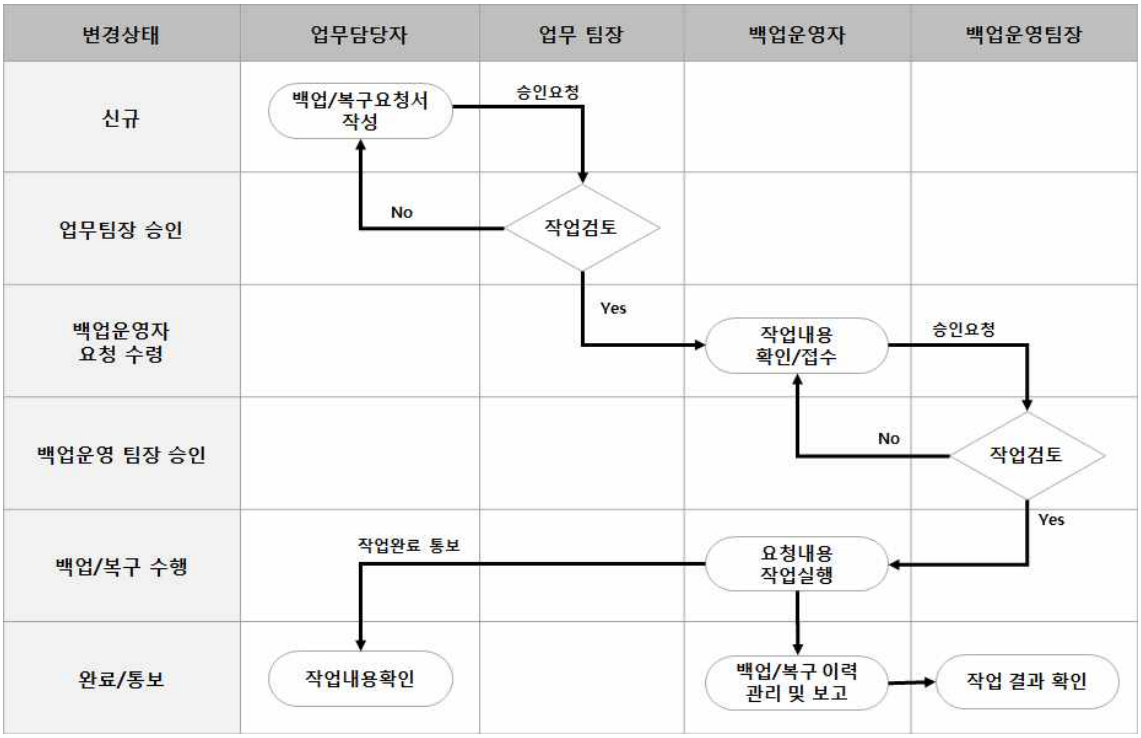
5. 백업 절차 및 보안관리 절차

가. 백업 절차

백업 및 복구 절차는 시스템 종류, 백업 대상 및 백업 방식에 따라 다양하다. 따라서 백업 및 복구 절차를 문서화 하고, 모의훈련을 통해 백업운영담당자들이 숙지하고 있어야 한다.

1) 백업·복구 요청 절차

백업 및 복구 요청시 백업에 대한 작업요청서를 작성하여 검토 승인 후 수행하는 절차를 따라야 한다.



[그림 3] 백업·복구 요청 절차 예시

다음은 백업 및 복구 절차 예시에 대한 세부 설명이다.

수행절차		수행자	양식
1	▶ 신규 요청 ✓ 신규 대상시스템에 대하여 백업요청 ✓ 백업 대상시스템에 대하여 복구요청	업무담당자	백업신청서
2	▶ 백업 요청서 및 복구요청서 검토 및 승인	업무 팀장	
3	▶ 업무부서는 백업요청서(복구요청서)를 백업운영부서에 이행 요청 ▶ 백업운영자는 백업/복구 요청 접수 처리	백업운영자	백업신청서 (백업계획서)

수행절차		수행자	양식
4	▶ 백업/복구 요청 내역에 대한 타당성 분석 및 백업 이행 승인 ▶ 백업운영자에 작업 이행 지시	백업운영팀장	
5	▶ 백업운영자는 작업요청 계획에 따라 작업 이행 ▶ 백업/복구 이력관리 대장 작성 ▶ 작업 결과에 대하여 업무 담당자와 백업운영팀장에 보고	백업운영자	백업이력관리대장, 작업결과 보고

[표 1] 백업 및 복구 세부 수행절차 예시

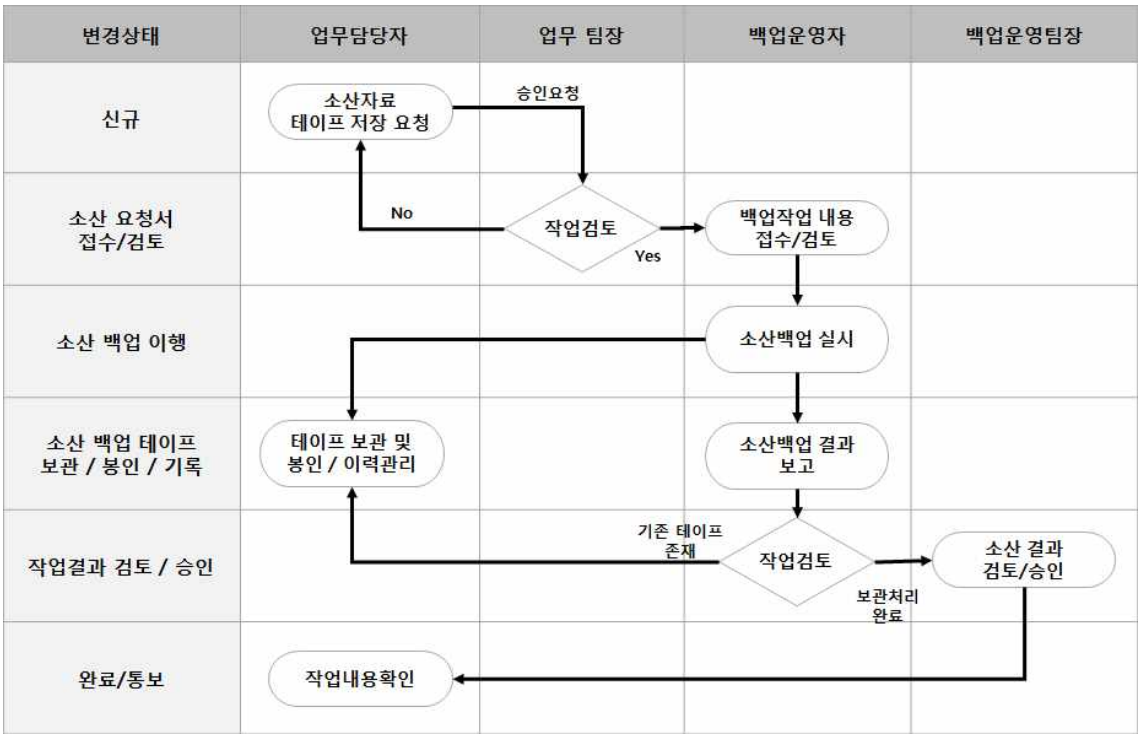
2) 소산백업 절차

백업된 데이터를 천재지변, 비상사태(장애, 외부 해킹 등)에 대비하기 위해 물리적으로 격리된 물리보안 접근통제 구역 또는 일정거리 이상 떨어진 전용 IDC에 보관하여 유사시 복원하여 기업의 사업 연속성을 보장하는 절차이다.

구분	보호대책 내역
데이터 소산	• 전용 IDC 내 소산보관을 위해 물리적으로 보관 및 보호 • 전용 내화금고에 보관하여 화재 시 데이터 파손 방지 및 도난 방지(원격지 소산이 어려운 중소기업 대상 소산관리 적합, 내화금고가 없을 경우 시건 할 수 있는 캐비넷에 보관) • 원격지 소산의 경우 운송 전용 특수 차량(내부 내화금고 설치)을 통한 운반 및 전용 하드케이스 밀봉 • 내부 출입통제 및 감시설비를 통한 모니터링 • 소산 시 담당자 및 운영자 통제를 위한 출입/작업 이력관리

[표 2] 데이터 소산 시 보호대책

다음은 소산백업 업무 처리 절차이다.
소산 백업시 소산 대상에 대하여 소산백업 관리대장을 통해 소산 이력을 관리하여 장애 또는 침해사고 시에 이전 데이터에 대하여 복구할 수 있도록 관리되어야 한다.



[그림 4] 소산 백업 절차 예시

다음은 소산처리 절차 예시에 대한 세부 설명이다.

수행절차		수행자	양식
1	▶ 신규 요청 ✓ 소산자료 디스크 또는 테이프 저장 요청	업무담당자	소산신청서
2	▶ 소산 대상 데이터 내역 검토 및 승인	업무팀장	소산신청서
3	▶ 백업운영 부서에 소산신청서 접수 ▶ 백업운영자 소산 작업 내역 검토 ▶ 소산 백업 이행	백업운영자	
4	▶ 소산 백업 데이터 보관 및 봉인 처리 ▶ 소산 이력 관리대장 작성	업무담당자	소산관리 대장
5	▶ 백업운영팀장에 소산백업 결과 보고	백업운영자	
6	▶ 소산 작업 결과서 검토 및 완료 승인	백업운영팀장	

[표 3] 소산백업 세부 수행절차 예시

3) IT 재해·재난, 해킹 대비 복구 절차

IT 재해·재난 및 해킹 사고 발생시 적시에 복구할 수 있도록 백업 소산 및 복구 절차 조건은 다음과 같다.

(1) 재해·재난 시 복구 절차 조건

① 데이터 무결성 및 정보시스템 가용성 유지를 위한 백업 및 복구 절차를 수립하고 있으며 백업 대상 시스템과 백업대상 데이터를 정하여 정기적인 백업을 수행해야 한다.

② 중요 백업 데이터를 비인가자의 접근으로부터 차단하고 외부 환경적인 위험으로부터 보호하기 위하여 내화금고 등에 안전하게 보관해야 한다.

③ 백업시스템을 이용한 백업 체계를 갖추고 중요 백업본은 동일 장소의 오프라인 보관 또는 일정거리 이상에 소산 백업을 실시하는 것을 권고한다.

④ 백업 데이터를 활용해 연 1회 이상의 재해복구 훈련을 수행한다.

(2) 랜섬웨어 침해 시 대응 및 복구 절차 조건

① 백업 파일 존재 여부를 파악해야 하며, 원본 및 백업 파일의 감염여부 파악은 필수이다.

② 랜섬웨어 복구 도구가 존재하는지 확인하거나 노모어랜섬 홈페이지(https://www.nomoreransom.org/ko/index.html) 등에서 복구 프로그램을 다운받아 복구 시도를 진행할 수 있으며, 복구 시 고려사항을 준수해야 추가 피해를 최소화 할 수 있음

※ [주의사항] 랜섬웨어 복구 시 고려사항

① 복호화 비용을 지불 후에도 암호 해독키를 제공받지 못하는 경우 발생

② 복구 비용을 지불한 후 다시 공격의 대상이 될 수 있으며, 제시한 복호화 비용보다 더 많은 금액을 요구할 수 있음

(3) 랜섬웨어 감염으로 인한 복호화가 불가능한 경우 처리

① 하드디스크 원본을 보존하여 추후 복구 툴이 개발되거나 암호화키가 공개될 경우 복호화 진행

② 복호화가 필요 없을 경우 하드디스크 초기화(포맷) 후 운영체제 및 소프트웨어 등의 최신 보안 업데이트 후 사용

(4) 복구 절차

복구 절차 또한 백업 절차와 마찬가지로 백업 대상 및 방법에 따라 매우 다양하다. 복구절차의 개요는 다음과 같다.

① 장애원인 파악

- 정보시스템에 장애가 발생하면 먼저, 장애 원인, 영향범위 및 장애유형 등을 파악해야 한다.
- 장애 원인 및 범위, 유형에 따라 장애를 복구하기 위해 백업본에 대한 리스토어가 필요한지 여부를 포함한 세부적 장애복구 절차를 결정하고, 이에 따라 장애복구 예상시간 및 사전 준비사항을 마련하여야 한다.

② 복구대상 확인

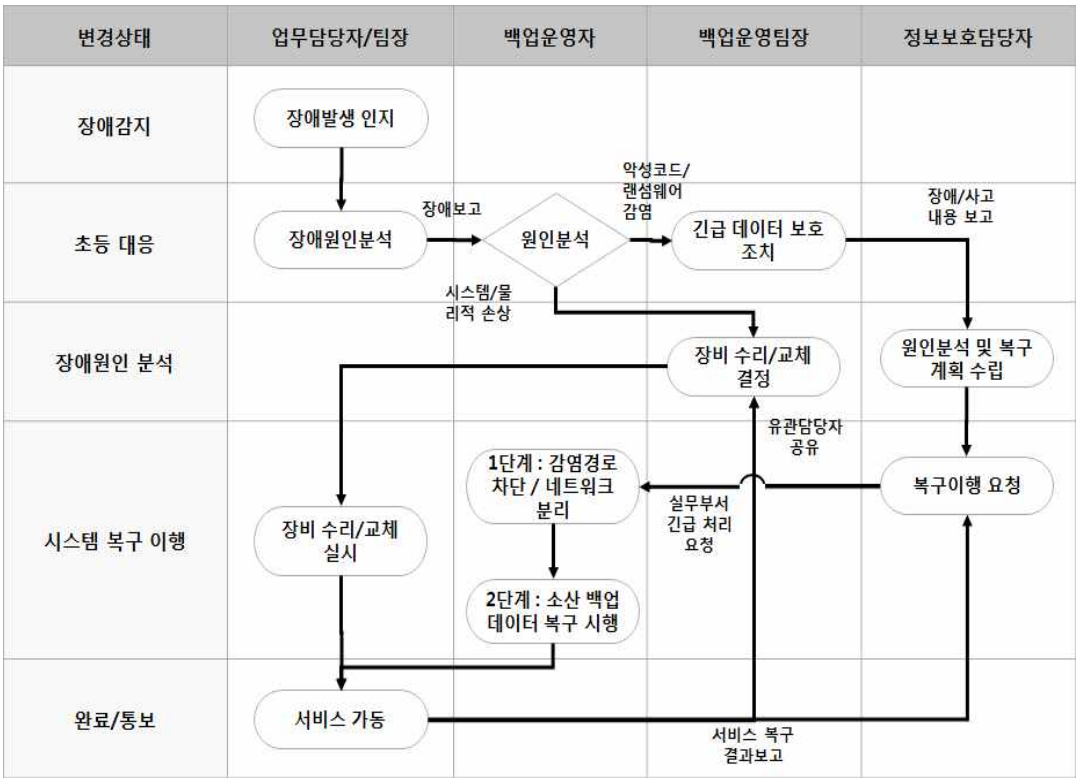
- 시스템 장애 해결책으로 백업본의 리스토어 의사결정이 되면 복구가 요구되는 시점에 유의하여, 백업본을 식별하고 백업 데이터의 랜섬웨어 감염 여부 등 정상 유무를 확인하여 복구 작업을 준비한다.
- 실제로 장애 발생시 백업본을 활용하여 복구를 수행하는 의사결정을 하는 것이 쉽지 않으며 시간도 많이 걸린다. 따라서 장애 유형별 복구 전략을 사전 정의하여 의사결정 시간을 단축하는 것이 장애시간을 최소화하는 데 도움이 된다.

③ 복구 수행

- 복구방법에 대한 의사결정이 나고 복구 대상에 대한 백업본을 식별하여 복구할 준비가 끝나면 실제 복구 작업을 수행한다.

④ 검증

- 복구 작업이 끝나면 업무 담당자 협조 하에 복구 작업의 유효성 및 데이터의 무결성을 검증한다. 검증이 완료된 후에 시스템을 정상적으로 서비스에 투입할 수 있다.
- 복구 작업이 불완전한 상태에서 검증을 거치지 않고 서비스를 투입하면 향후 데이터 정합성에 치명적인 손상을 야기할 수 있으므로 주의한다.
- 장애 복구 완료 후 동일 장애에 대한 방지 대책을 반영한 운영정책을 마련해야 한다.



[그림 5] 복구 절차 예시

수행절차		수행자	양식
1	▶ 장애감지 ✓ 장애발생 인지 ✓ 장애원인 파악(초등대응)	업무담당자/ 업무 팀장	장애보고서
2	▶ 장애원인 분석 ✓ 악성코드/랜섬웨어 감염 장애 판별 ✓ 시스템/물리적 손상 장애 판별	백업운영자	장애보고서
3	▶ 악성코드/랜섬웨어 감염 장애 ✓ 백업 데이터 감염 여부 확인 ✓ 긴급 데이터 보호 조치 실시 ✓ 정보보호 부서 협조 요청 ▶ 시스템/물리적 손상 장애 ✓ 장비 수리/교체 결정 처리 ✓ 교체 후 서비스 가동	백업운영팀장	장애보고서
4	▶ 악성코드/랜섬웨어 감염 장애 원인 분석 ▶ 세부 복구 계획 수립	정보보호 담당자	복구신청서
5	▶ 시스템 복구 이행 ✓ 1단계 : 감염경로 차단 / 네트워크 분리 실시 ✓ 2단계 : Restore 여부 판단 / 소산 데이터 복구 시행	백업운영자	
6	▶ 서비스 정상 가동 ▶ 복구 결과 유관부서 보고	업무담당자/ 업무 팀장	결과보고

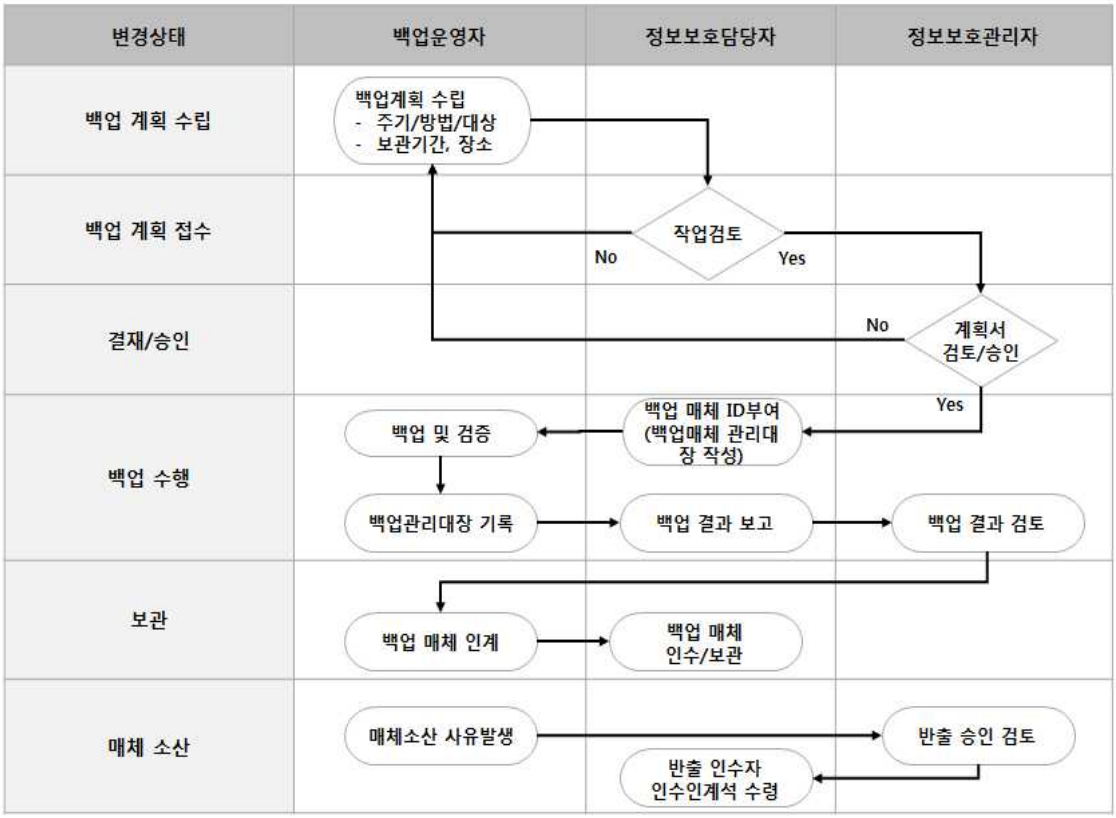
[표 4] 복구 세부 수행절차 예시

나. 백업 보안관리 절차

기업 내 백업 데이터에 대한 관리는 기존 백업담당자 및 관리자를 통해 처리되었으나 현재는 데이터가 외부의 해킹 또는 기타 침해로 인해 망실 될 경우 금전적 피해를 보기 때문에 백업데이터를 처리할 경우 정보보호담당자에 보고하여 처리해야 하며, 백업과 관련된 모든 이력은 관리대장에 기록하여 향후 데이터 외부 유출시 추적성을 고려해야 한다.

1) 업무 통제 절차

안전한 백업보안 관리를 위해서 백업 계획을 수립해야하며, 수립된 계획이 기업 내 현황에 적합한지 백업 담당과 정보보호 담당간 타당성 검토가 선행되어야 한다.



[그림 6] 백업보안관리 절차 예시

다음은 백업업무 보안 절차의 세부 내용을 기술한 것이다.

수행절차		수행자	양식
1	▶ 백업계획 수립 ✓ 매년 말 아래항목에 대한 차년도 백업계획 작성 ✓ 백업주기, 백업매체 분류기준, 백업방법, 적용대상, 보관기간, 보관장소, 매체명명규칙	백업관리자, 백업담당자, 정보보호담당자	백업 계획서
2	▶ 정보보안담당자는 백업계획서의 적절성을 검토 후 승인	정보보호담당자	
3	▶ 백업계획서를 사내 업무시스템을 이용하여 부서원에게 배포	정보보호담당자	
4	▶ 백업 매체 관리를 위해 기준에 따라 매체 ID 부여	백업관리자, 백업담당자, 정보보호담당자	백업매체 관리대장
5	▶ 백업 매체 관리를 위해 백업매체관리대장에 기록	백업관리자, 백업담당자, 정보보호담당자	백업매체 관리대장

수행절차		수행자	양식
6	▶ 백업 수행 ✓ 백업방법 : 백업수행 방법에 따라 자동/수동으로 구분 • 자동백업 : 자동백업 툴 및 장치 활용 • 수동백업(Manual 백업) : 운영체제에서 제공하는 백업 명령 사용 ✓ 정기백업 작업 절차 • 백업계획에 의거 백업 작업 수행 ✓ 비정기 백업 작업 절차 • 해당업무 담당자의 백업작업 의뢰 신청서 작성 후 백업 ▶ 백업 결과 검토 ✓ 백업 후 백업 결과에 대한 검토 실시 • 백업매체 유효성 검증 ✓ 장기 보관 중인 백업 매체에 대한 샘플링 검사(10%)	백업관리자, 백업담당자, 정보보호담당자	백업매체 관리대장
7	▶ 백업 결과를 백업관리대장 기록/자동 로깅	백업관리자, 백업담당자, 정보보호담당자	백업관리 대장
8	▶ 정보보안담당자에게 백업결과 및 백업관리대장 보고	정보보호담당자	
9	▶ 정보보안업무지원 담당자가 보고한 백업 수행 결과를 검토	정보보안담당자	
10	▶ 백업 완료된 백업 매체 인계	정보보호담당자	
11	▶ 백업 완료된 매체 보관 ✓ 백업주기 및 보관기관 • 일일백업 : 2주 보관 (백업장치 상황에 따라 변경됨) • 주간백업 : 2주 보관 (백업장치 상황에 따라 변경됨) • 월간백업 : 2개월 보관 (백업장치 상황에 따라 변경됨)	정보보호담당자	
12	▶ 백업매체 소산 등 반출사유 발생	정보보호담당자	
13	▶ 백업매체 반출에 대해 사유, 수량, 반출처 등을 확인하고 승인	정보보호담당자, 정보보호관리자	

수행절차		수행자	양식
14	▶ 현업 담당자 및 외주 협력/용역 업체는 승인된 건에 대해 매체를 반출하고 매체 인계자로부터 인수인계서를 받는다.	정보보호담당자	사무 인수 인계서

[표 5] 백업 보안관리 절차 예시

2) 시스템 보안 관리 절차

백업 시스템, 인프라에 대한 외부·내부의 불법 침입으로부터 안전하게 보호하기 위해 정기적으로 시스템 취약점 점검을 실시한다.

(1) 점검 시기

① 최소 연 1회 정기 점검하는 것을 원칙으로 한다.

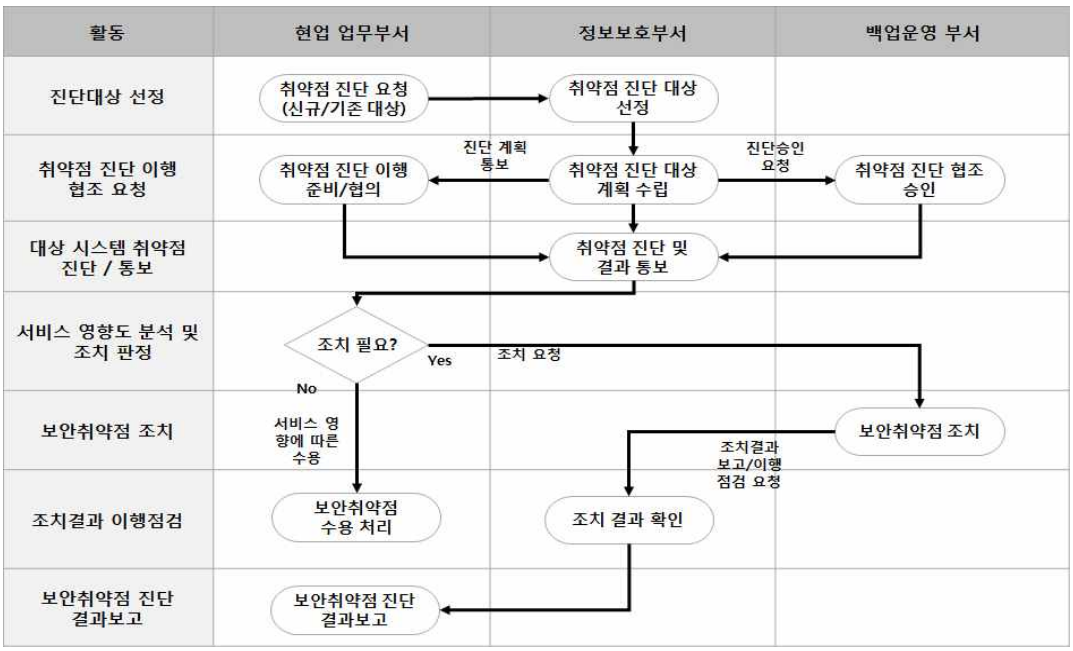
② 필요에 따라 비정기적으로 여러 차례 보안 점검을 실시한다.

③ 보안 담당자나 시스템 운영 담당이 바뀔 경우에 보안 체크리스트의 모든 항목을 점검한다.

(2) 점검 절차

보안취약점 진단은 연간 주기적으로 1회 이상 보안점검 절차에 따라 진단을 실시해야하며, 보안 취약점 점검 계획 수립 시 진단 대상을 정의 후 진단 이행 전 백업 시스템의 경우 반드시 전체 백업을 실시 후 진행해야 한다.

다음은 기업 내 정기적으로 수행되어 지는 정기 취약점 진단 예시이다.



[그림 7] 시스템 취약점 점검 절차 예시

① 정보보호담당자는 보안 점검 대상 및 부분을 관련 부서에 통보한다.
해당 현업 부서에서는 보안 점검에 필요한 자료 및 제반 요청 사항을 준비하여 보안 점검에 대비한다.
② 정보보호담당자는 보안 점검을 실시하여 그 결과를 유관 부서(현업 업무부서, 백업운영 부서)에게 통보한다.
③ 해당 현업 부서는 정보보호담당자 점검 결과에 따른 보안취약점 결과를 보완하고 업무부서 팀장이 정보보호담당자에게 제출 한다.
④ 정보보호담당자는 조치이행 결과에 대하여 조치여부를 점검 후 이행된 결과를 보안취약점 결과보고서를 작성하여 유관부서와 공유 한다.

3) 백업데이터 랜섬웨어 피해 예방 보안 수칙

최근 업무망에서 무분별한 인터넷 사용 및 업무망과 인터넷망 간 접근통제 미흡으로 인해 백업데이터가 랜섬웨어에 감염되어 서비스 중단 및 데이터의 복구 불가가 발생하고 있어 다음과 같이 '랜섬웨어 피해 예방 7대 보안 수칙' 준수를 권장하고 있다.
랜섬웨어에 감염된 원본이 백업 도중 백업데이터를 덮어쓸 수 있어 백업 수행 전 데이터에 대한 무결성 검증 수행 여부를 확인하여 안전한 백업을 수행할 수 있다.
랜섬웨어 감염원인은 광고성 이메일 또는 링크(Link), 이메일 첨부 파일, 취약한 웹사이트와 앱, SNS, USB, 기타 취약한 외부 인터넷 서비스 사용을 통해 감염되어 기업에 심각한 침해가 발생하므로 다음과 같은 수칙을 준수해야 한다.

(1) 백신 소프트웨어를 설치하고 엔진 버전을 최신 버전으로 유지
(2) 운영체제(OS), 브라우저 및 주요 애플리케이션의 최신 보안 업데이트
(3) 발신자가 불분명한 이메일 내 링크 클릭 및 첨부 파일 실행 자제
(4) 보안이 취약한 웹사이트 방문 자제
(5) 업무 및 기밀문서, 각종 이미지 등 주요 파일의 주기적인 백업
(6) 외장하드 등 외부 저장장치를 이용해 중요 파일 주기적으로 백업
(7) 중요 문서에 대해서 '읽기 전용' 설정

6. 백업 시스템 구축

백업은 그 유형에 따라 여러 가지로 분류할 수 있다. 본 지침에서는 크게 디스크나 테이프 등 저장매체에 따른 분류와 OS, 데이터베이스, 사용자 일반파일 및 기타(메일, 이미지 파일)와 같은 백업 대상에 따른 분류로 살펴본다. 최초 백업 시스템을 구축하거나 기존 백업 방식을 변경하기 위해 아래의 내용을 참고한다.

가. 백업 매체 및 장비 선정

백업을 구축하기 위해서 결정해야 할 가장 기본이 되는 것은 적절한 백업 매체와 장비를 선택하는 것이다.

백업의 수행은 일반적으로 테이프를 사용한다. 그 이유는 많은 양의 데이터를 보관하기 위한 매체의 구매 및 유지비용이 저렴하고 또한 시간 차이를 둔 여러 버전의 데이터를 보관 할 수 있기 때문이다.

다음은 매체 특성을 비교한 표이다.

기술의 발달로 디스크와 테이프 속도, 보관용량 및 가격에 많은 변화가 발생하고 있다. 따라서 아래 비교표는 절대적인 것이 아니며, 도입하는 기업의 백업 대상 및 구성 등 필요한 환경에 따라 장단점은 달라질 수 있다.

매체	장점	단점	운영특성
디스크	• 백업 및 복구 속도 빠름	• 구매 및 유지비용이 큼 • 일정시간 차이의 여러 버전의 데이터 보관의 어려움	• 테이프에 비해 오류율이 낮음 • 가상 드라이브 확장의 유연성
테이프	• 여러 주기의 보관 • 소산보관 용이	• 디스크 복제 대비 백업 및 복구 속도가 느림	• 소산의 용이성 • 장기보관에 유리
외장 USB	• 백업 및 복구 속도가 빠름 • 악성코드 감염 시 이전 자료에 복원	• 손상 및 분실 우려	• 물리적인 소산의 용이성 보유
Cloud	• 외부 전문회사에 수탁하여 체계적 관리 • 별도 소산 관리가 필요 없음	• 네트워크 속도에 따라 백업 속도 좌우 • 원격 소산 백업센터 장애시 영향 발생	• 원격 소산 형태 백업용이 • 주기적 관리절차 필요

[표 6] 백업 매체 특징 분류

나. 백업 대상 선정

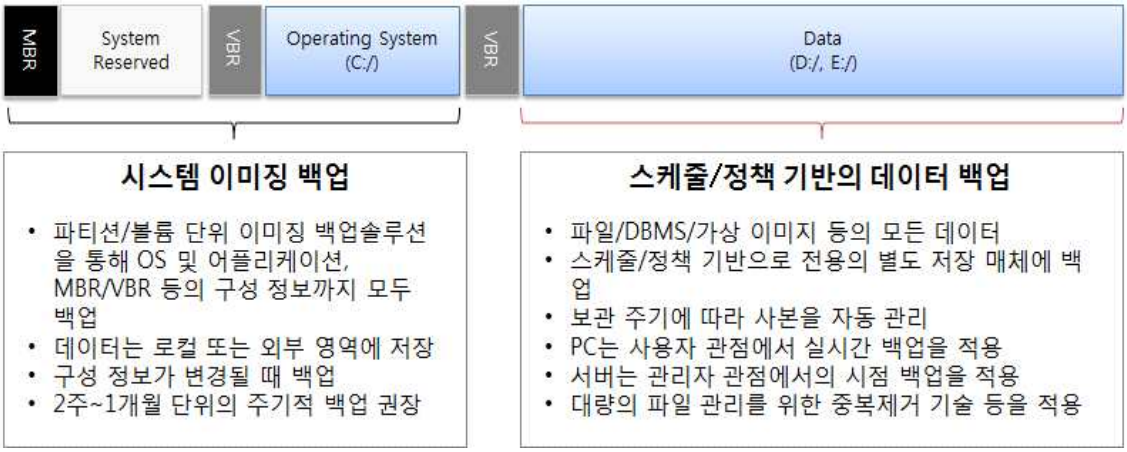
백업은 백업 대상을 기준으로 크게 OS, 데이터베이스, 사용자 일반파일 및 기타파일 등으로 분류할 수 있다. 정보시스템 규모가 큰 기관에서는 모든 시스템을 전산센터에 집중하여 관리하지만 규모가 작은 기관에서는 전산실 내의 시스템 운영파트가 해당 업무를 수행한다. 백업시스템을 관리하는 전산센터 또는 시스템 운영파트에서는 전산실 또는 개발자의 요청을 받아서 주기적인 백업작업을 실시한다.

다음은 백업 대상 분류 사례와 백업 영역별 백업 방법을 설명한 것이다.

구분	백업 관리자(운영자)	백업 요청자(개발, 현업)
OS(시스템 등)	• 월1회 또는 시스템 변경 시 OS 백업 실시 • 시스템 관련 파일 백업	• 정보보호 담당자
DATA	• 일/주 1회 데이터(파일, 데이터베이스) 전체 백업 • 백업요청에 의한 정기 및 비정기 백업 실시 • 원본 백업데이터에 대한 소산 백업정책 반영	• 백업대상, 주기, 방법 결정 후 전산센터에 백업요청 • 사전 실행조건, 필요 디스크, 자동 백업 솔루션 제공여부 고려 적용 • 원본 데이터에 대한 소산 백업 방안 반영 • DBA 관리책임자 승인 후 적용
개발 소스 및 기타 파일(사용자)	• 주/월 1회 전체 백업실시 • 백업 요청에 의한 비정기 백업 실시 • 개발 소스의 경우 운영 별도 분리보관 정책 반영	• 개발 및 기획 등 중요 데이터에 대한 백업은 운영 서비스 데이터와 분리하여 보관 요청

[표 7]백업 대상별 분류

데이터 백업은 PC의 경우엔 실시간 자동화된 백업(CDP(Continue Data Protection) 기반 실시간 백업)이, 항상 켜져 있는 서버(파일서버, DB서버, 웹서버, 그룹웨어 등 업무시스템)의 경우엔 지정된 시간 스케줄·정책 기반 데이터 백업이 수행되어야 한다.



[그림 8] 백업 영역별 백업방법

(1) OS(Operating System)

서버의 OS나 시스템 구성(파라미터) 파일 및 시스템 로그 파일이 그 대상이다. 보통 월 1회 혹은 시스템 변경 시 시스템 백업을 실시하여야 하며 백업 및 복구가 간편한 DAT 테이프를 많이 이용한다. 시스템 최초 설치 및 업그레이드, 버그 패치 등의 작업 후에도 이미지 백업을 실시 후 보관한다.

(2) 데이터베이스

데이터베이스의 데이터파일 및 컨트롤 파일, 변경로그 파일 등이 그 대상이다. 이외에도 데이터베이스 엔진(이하 DBMS)이나 구성파일 자체도 주기적으로, 또는 변경작업 전에 백업하여야 한다.

(3) 개발 소스 및 기타 파일(사용자)

사용자 일반파일은 사용자 데이터 , 개발자 소스 파일, 응용 소프트웨어 등이 그 대상이다. 백업 시기로는 일일 주요 파일(개발소스) 백업, 주 1회 전체 백업, 월 1회 전체 백업, 사용자의 요구 시에 발생하는 비정기적인 백업 등이 있다.

다음은 백업작업 유형과 특징을 사례를 통하여 설명하고 있다.

작업 유형	백업특징	백업대상
OS 백업	OS 파일 시스템 백업	OS,파라미터, 로그 파일
데이터베이스 온라인 백업	서비스 가동 중 데이터베이스, 단위 백업	데이터베이스
데이터베이스 오프라인 백업	서비스 중단 후 데이터베이스, 단위 백업	데이터베이스
데이터베이스 변경로그 파일 백업	데이터베이스 변경로그 모드, 운영 시 변경로그 파일을 백업	데이터베이스 변경로그
파일 시스템 백업	특정 파일 시스템 백업(설정 파일 제외)	파일 시스템

[표 8] 백업작업 유형과 특징

다. 백업구성 방식 선택

백업방식은 일반적으로 많이 사용하는 DISK백업, TAPE백업 등 여러 방식이 있는데 최근 백업/복구 기술에 대하여 간단히 소개한다.

백업을 구성하는 방식은 데이터와 해당 데이터가 백업이 되는 테이프 장치와의 연결 방식에 따라 직접(Direct) 백업, 네트워크(Network) 백업, SAN 백업의 세 가지로 크게 나눌 수 있다.

다음은 구성방식별 장점 및 단점을 설명한 표이다.

구성방식	장점	단점	비고
직접연결 백업	• 소기업 환경 적합 • 고속의 백업(LAN 사용 안함) • 소규모 백업 장치 활용(DAT등)	• 시스템별 별도의 백업 장비 필요	• 네트워크 백업과 혼용 • 전통적 방식
네트워크 백업 (원격 백업)	• 네트워크상에 있는 백업 장비 활용 • 구현이 간편하고 비용이 저렴	• 백업 시 네트워크에 부하를 줌 • 온라인 백업에 적합하지 않음	• 소규모 환경 적합 • 백업 윈도가 보장된 환경에 적합
대형 환경 네트워크 백업	• 네트워크상의 백업 장비 활용 • 구현이 간편하고 유연성이 뛰어남	• 별도의 백업 네트워크 구축이 필요 (많은 비용 소용)	• SAN구성이 어려운 대형 백업 환경에 적합 • 전용 백업 네트워크 구성
SAN백업	• SAN상의 장비공유를 통해 백업장비의 활용성이 뛰어남	• 별도의 SAN 네트워크 구축으로 인한 비용 증가 발생	• 백업 관리가 매우 용이함
디스크 복제	• 백업 완료 후 변경 부분에 대한 백업 시간이 짧음	• 구축비용이 높은 단점	
Cloud 백업	• 많은 비용을 절감하고, 복구시간을 단축 • 백업 데이터가 지리적으로 복제된 저장소에 저장되므로 안정적임	• 기업의 기존 백업 방식 사용에 제한적임	

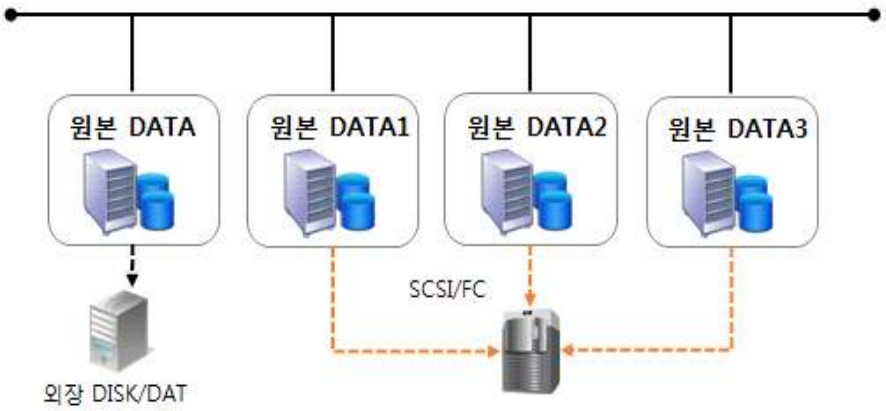
[표 9] 백업방식 및 장단점

(1) 직접 백업

① 데이터 장치와 테이프 장치 간의 연결이 SCSI나 직접 연결된 형태를 의미한다.

② 대개 서버에 DAT와 같은 장치가 직접 연결돼 사용하는 전통적인 방식으로 현재도 TAPE 이용한 소산 방식으로 꾸준한 사용을 하고 있으며, 백업 시 별도 TAPE에 보

관되기 때문에 최근 웜(랜섬웨어 등) 감염으로 인한 피해를 최소화할 수 있는 방안으로 제시되고 있다.



[그림 9] 직접/집중형 백업

(2) 네트워크 백업(Network Backup)

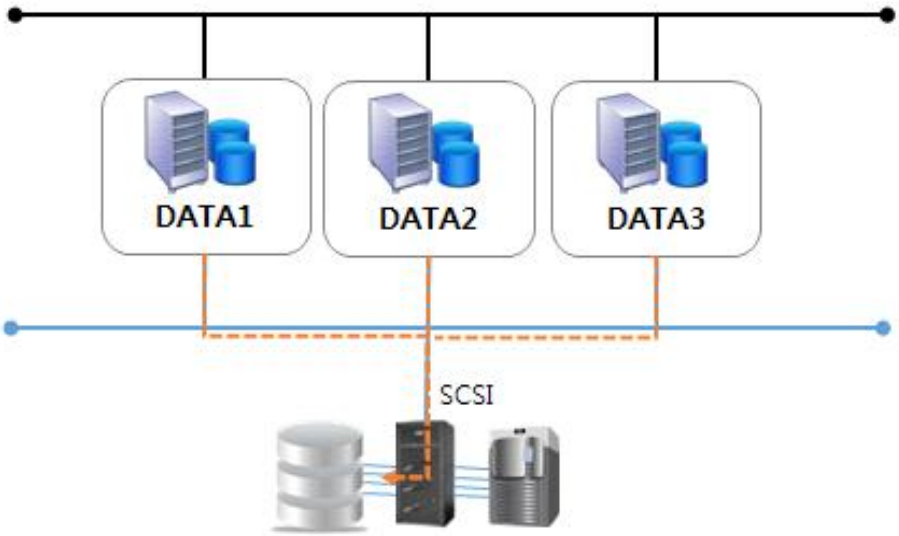
① 현재는 사용이 크게 줄어든 백업 방법으로 데이터 장치와 테이프 장치 간의 연결이 TCP/IP 네트워크로 연결된 형태를 말한다.

② 백업 전용 서버에 백업장비를 모두 연결하고 나머지 서버는 이 백업 전용 서버를 통해 백업을 수행한다.

③ 디스크 구성방식 중 NAS(Network Attached Storage)와 유사한 구성방식이다. 네트워크 백업은 백업 장치를 공유하므로 직접 백업에 비해 백업 장치에 대한 중복 투자를 줄일 수 있다는 장점이 있다.

④ 백업 데이터가 네트워크를 통해 전달되므로 백업 성능이 저하될 수 있다는 점은 단점이 있다.

⑤ **공격자가 네트워크에 연결된 백업 시스템에 침투하여 백업 데이터를 암호화하거나 삭제할 수 있어 백업 스케줄이 없는 시간에는 오프라인으로 설정하는 것이 중요하다.**



[그림 10] 네트워크 백업 구성

(3) SAN 백업

① 직접 백업과 네트워크 백업의 장점만을 이용해 구성한 최적의 백업 구성 방식이다.

② SAN 등장 이후 가장 많이 사용되고 있는 구성 방식으로 직접 백업과 네트워크 백업 방식에 비해 백업 장치 공유 및 관리 측면에서 매우 뛰어난 성능 및 유연성이 있는 백업 방식 이다.

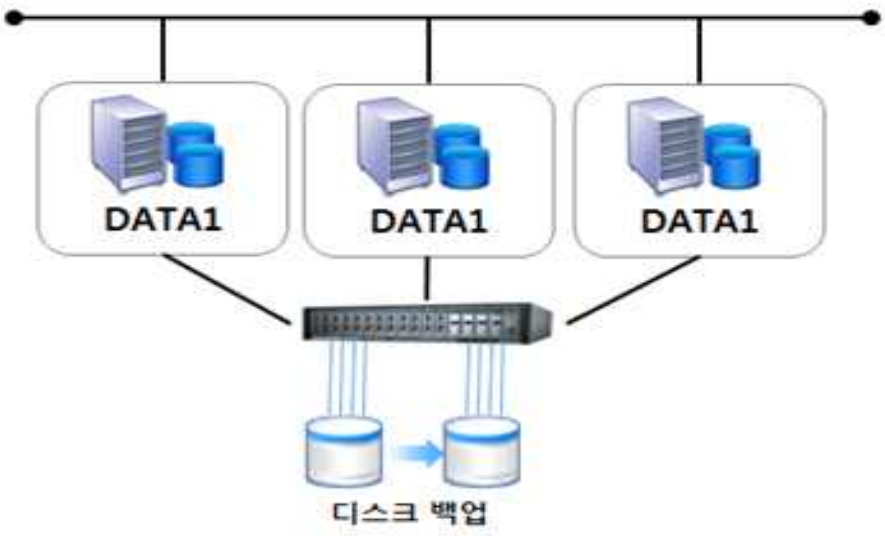
③ 다양한 백업방식(전체백업, 증분백업 등) 적용할 수 있어 현재도 많이 사용 중인 백업 기술이다.

(4) 디스크 복제

① 디스크 복제는 주로 중요하거나 빠른 시간에 백업이 필요한 경우 디스크에서 디스크로 직접 복제하는 백업 방식이다.

② 백업 완료 후 시간이 흘러 데이터의 변경이 있을시 변경된 데이터만을 다시 백업함으로 백업 시간이 타 백업방식에 비해 짧은 장점을 보유한다.

③ 장애 혹은 잘못된 작업으로 데이터 손실 및 변경 시 백업 본을 기준으로 변경된 부분만을 리스토어(restore)함으로 복구 시간을 획기적이나 구성비용이 많다.



[그림 11] 디스크복제 구성

(5) Cloud 백업

① Cloud백업은 최근 도입된 물리적으로 떨어진 외부영역에 백업하는 방식이다.

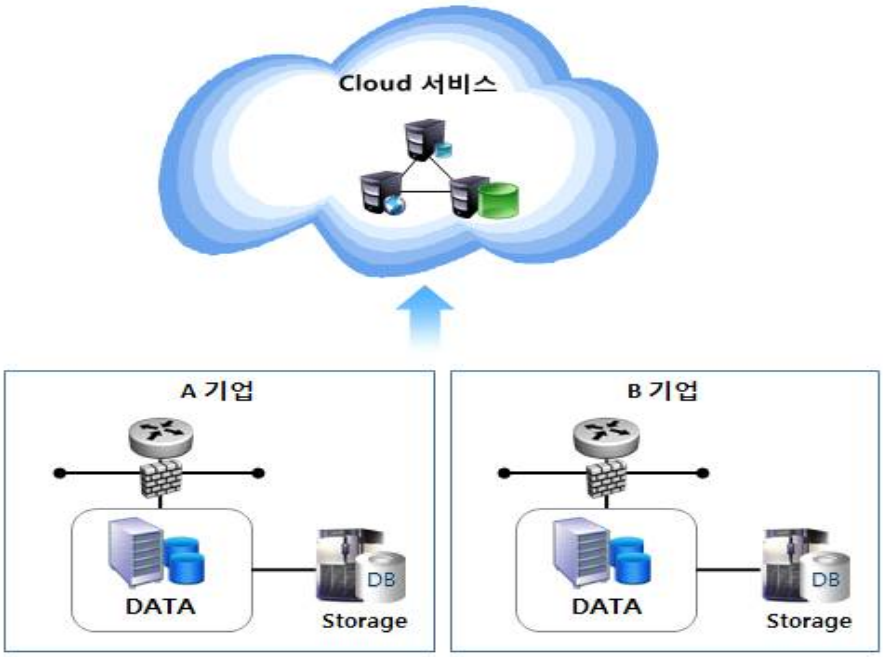
② **일반적으로 로컬 네트워크 내에서 1차 백업 후 외부에 2차 백업으로 소산 개념으로 백업하는 방식**으로 비용을 최소화할 수 있는 방식 중 하나이다.

③ 자체 보안시스템(방화벽, 웹 방화벽, DB암호화시스템, 보안관제시스템 등)으로부터 보호 및 모니터링 되어 개인 및 국내 중소기업에 랜섬웨어 등으로 데이터를 보호하기 위한 방안으로 적합하나 다소 비용이 소요된다.

④ 외부 Cloud 사용 시 이용자(개인)의 경우 웹 계정을 사용하여 백업할 수 있으며, 기업의 경우 Gateway 방식구성으로 Gateway 간 VPN 또는 API연동으로 SSL통신 구성방식으로 구성된다.

⑤ 해당 서비스 제공은 국내 통신사와 해외 IT기업이 서비스를 제공하고 있다.

⑥ 클라우드 서버에 백업데이터가 보관되기 때문에 안전한 클라우드 계정 관리가 중요하다. OTP 등 멀티 인증을 사용하도록 권고한다.



[그림 12] Cloud 백업 구성

라. 랜섬웨어 예방을 위한 백업 구축 방식

지금까지 백업은 대기업을 제외한 비교적 규모가 작은 중소기업의 경우 내부 네트워크에 NAS 또는 외장 디스크, SAN Storage를 구축하여 백업하는 환경으로 외부에 소산 백업으로 데이터 안정성 확보는 비용부담의 요소다.

그러나 **랜섬웨어를 예방하기 위한 백업은 원격장소에 안전하게 보관하거나 오프라인으로 백업 데이터를 보관하는 방법이 안전**하다. 따라서 TAPE, 외장디스크, 외부의 다른 NAS, 혹은 클라우드 서비스를 이용하여 소산 관리 또는 오프라인 상태에서 관리해야 한다.

다음은 악성 웜으로부터 안전하게 데이터를 보존할 수 있는 백업유형이다.

구분	백업 방법
TAPE 백업	• 백업 TAPE은 네트워크를 연결하는 시스템을 통해 백업하는 것이 아닌 각 시스템에 데이터를 백업 TAPE에 복제할 수 있음 • 외부 저장소가 없더라도 자체 소산보관이 용이 • 비교적 저렴하여 중소기업에서 사용이 용이함
Cloud 백업	• 외부 영역에 데이터를 백업하는 방식 • 외부 소산 관리가 용이하며, 보안서비스를 제공받을 수 있는 장점 • 다양한 백업 기능을 사용할 수 있어 유리 • Cloud 서비스 업체에 일부 비용이 발생할 수 있으나 초기 투자비용이 높은 자체 백업 시스템 구축 보다 저렴하여 중소기업에 유리함

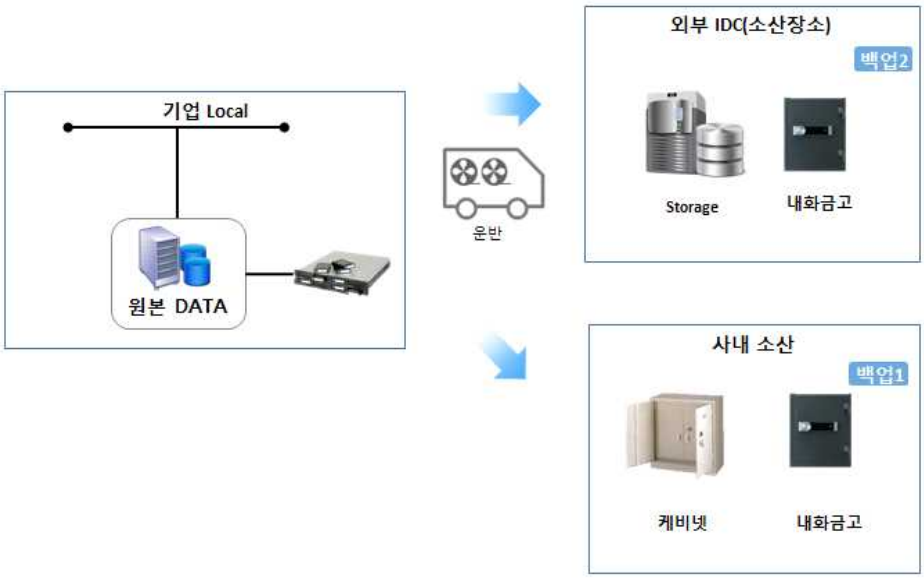
구분	백업 방법
NAS 백업 (NAS 백업)	• 최근 NAS백업 기술의 고도화로 자체 Cloud 백업 구성 및 별도 백업 기능 보유 • 외부 클라우드 시스템에 소산 백업 연계 기능을 보유 • 다양한 백업 기능 제공 • 중소기업이 구성이 용이함 **※ 원격 소산 백업 불가시 백업 방안** • **동일 장소 데이터 백업시 온라인 백업 후 백업 매체 Off-Site 보관(네트워크 분리)** • 백업 전과 백업 후 백업매체 관리 시 접근통제 절차 마련(허가된 사용자만 접근 가능하도록 별도 캐비넷에 보관)
USB 외장디스크	• 데이터 용량이 비교적 작은 경우 적합 • 별도의 백업 소프트웨어 없어 사용자가 직접 백업 계획을 수립하고 수동 백업 수행 • 주기적으로 데이터 백업을 실시한 후 캐비넷 또는 문서고에 보관하는 등 통제 절차 필요 • 백업에 소요비용이 매우 저렴 ※ 원격 소산 백업 불가시 백업 방안 • 동일 장소에 시스템에서 직접 백업 이후 USB 외장 디스크를 시스템에서 분리하여 별도 잠금장치가 있는 케비넷에 보관 • 백업 전과 백업 후 백업매체 관리 시 접근통제 절차 마련(허가된 사용자만 접근 가능하도록 별도 케비넷에 보관)

[표 10] 소산 관리가 용이한 백업 유형

(1) TAPE 백업

① 저렴한 가격 대비 성능, 이동성, 용량 관리의 용이성 등의 특징을 가지고 있다.

② 최근 랜섬웨어 등으로부터 기업의 중요 데이터를 보호하기 위한 방법 중 하나로 TAPE백업 방식을 채택을 권고하고 있으며, 대부분 저비용으로 구성할 수 있는 장점 때문에 비교적 규모가 작은 기업에 사용하는 것이 유리하다.



[그림 13] TAPE 소산백업 구성

(2) Cloud 백업

① Cloud 백업은 외부 저장소에 백업을 수행하는 것으로 최근 개인, 중소기업 등 다양한 이용자 계층에서 많이 사용하고 있다.

② Cloud 서비스 이용시 구성 방식에 따라 Gateway 구성 방식과 SSL 통신 방식, 웹 접근방식으로 제공된다.

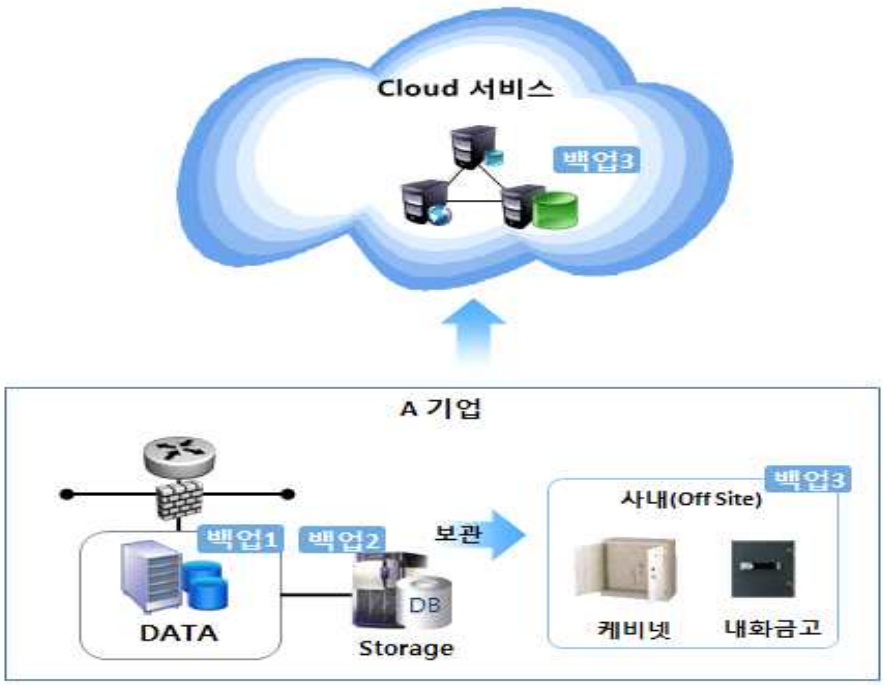
- Gateway 구성 방식은 Cloud 센터의 Gateway와 백업 대상 센터 Gateway간 VPN으로 구성되며, 백업정책은 전체 백업, 소산백업 등 다양한 백업기능이 제공된다.
- SSL통신 방식은 Gateway방식과 유사하지만 구간 통신방식이 SSL방식으로 구성되며, 백업 정책은 Gateway방식 동일한 방식으로 백업 정책을 적용할 수 있다.
- 웹 접근방식은 주로 개인 이용자가 PC백업용으로 사용되는 것으로 접근계정을 생성하여 백업할 수 있다.

③ 백업 방법

- 백업에서 황금률이라는 잘 알려진 규칙(3-2-1)을 기준으로 데이터 복사본 3개를 2개의 형식으로 보관하되 복사본 가운데 1개는 오프사이트에 위치시키는 것을 말한다.
- 3개의 복사본을 유지하면 서로 다른 위치에, 다른 형식으로 존재하므로 리던던시(redundancy)를 확보하게 됩니다. 즉, 주 백업은 로컬 디스크에, 두 번째 백업은 클라우드에 두는 방식으로 오프사이트 데이터 복사본을 클라우드에 보관하여 구조적으로 데이터 소산되어, 랜섬웨어의 공격에서도 최후의 백업본을 지킬 수 있습니다.
- 외부 Cloud 서비스를 사용할 경우 서비스 제공사의 보안서비스(방화벽, 웹방화벽, 접근제어시스템 등)를 받을 수 있는 장점이 있어 비교적 인프라가 열악한 중소

기업에는 장점이라고 할 수 있다.

- 랜섬웨어 등 외부 침해시 데이터 무결성 유지를 위해 반드시 백업 설정에서 "덮어쓰기" 방지 설정을 하여 이미 감염된 데이터가 Cloud 백업 저장소 내의 데이터에 덮어쓰기 되지 않도록 방지해야 한다.
- 또한 클라우드 백업 서비스 사용시 **인증 정보가 탈취되거나 통신구간 암호화 미적용으로 주요 정보가 외부에 노출되지 않도록 주의**해야 한다.



[그림 14] cloud 소산 구성

(3) NAS 백업

① 데이터 복구를 중시하는 일부 소비자와 중소기업은 백업을 위해 전용 NAS(Network Attached Storage) 기기의 사용을 고려할 수 있다.

② 암호화 멀웨어에 대응하기 위해 NAS를 설정하는 방법

- NAS를 데이터 백업을 위한 '전용' 저장소로 이용하도록 구성
- **랜섬웨어 감염 예방을 위해 백업 이후 네트워크를 반드시 분리**
- 기존 백업 데이터에 덮어쓰기가 되지 못하도록 NAS정책에 반영 또는 원본데이터를 단계적으로 복제해야 함
- 전용 백업 소프트웨어가 없는 경우 백업 데이터를 백업시 모두 "읽기 전용으로 설정"하여 추후 데이터 망실이 발생한 경우 복구될 수 있도록 무결성을 유지해야 함

③ 백업 완료 후 백업 매체관리는 별도의 접근통제 절차를 수립하여 운영해야 한다.

- 네트워크를 통해 백업된 NAS디스크 1본을 사내 네트워크가 분리된 장소(Off-Site)에 분리 보관
- 소산백업이 어려운 환경인 동일장소 백업 시 백업 후 네트워크 분리 보관하여

별도의 시건된 장소에 보관

- 백업 매체의 관리는 분리보관 장소에 인가된 담당자만 출입이 가능하도록 출입 통제 절차를 수립(출입 관리대장, 백업 매체 반·출입 대장)

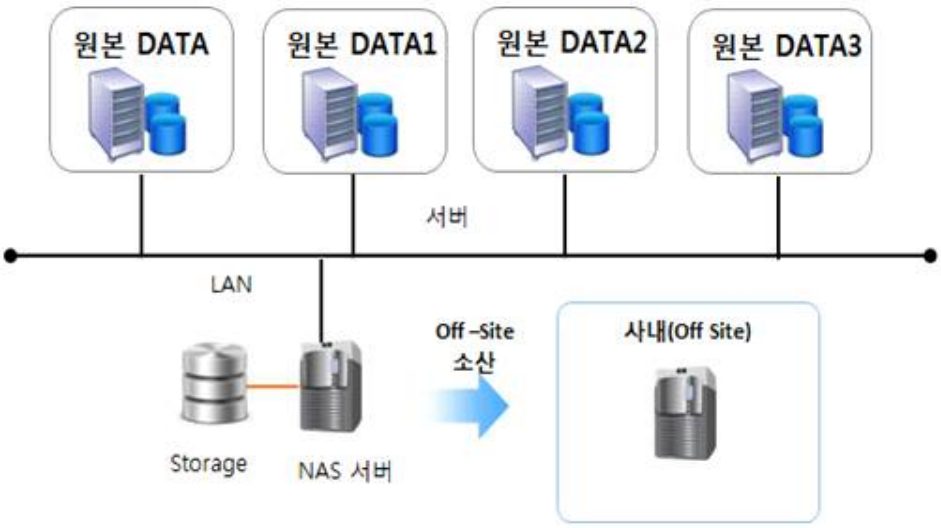
④ 원격 스토리지를 이용한 정기적인 백업 방법

- 기업 전산실 내 NAS 스토리지에 각 원본데이터를 백업 후 백업된 데이터를 원격지 NAS 스토리지에 다시 백업하는 방법
- 내부 NAS 스토리지 백업데이터를 외부 백업센터(IDC) 스토리지에 백업하는 방법

⑤ 원격 스토리지 백업 절차

- NAS는 자체 백업 어플리케이션을 보유하고 있어 PC백업, 파일 공유, 원격지 백업에 대하여 백업 정책을 이행할 수 있다.(NAS 벤더별 기본 백업 프로그램을 포함하고 있음)
- 백업 절차는 타 백업 방법과 마찬가지로 전체백업, 이미지 백업, 실시간백업 기능을 이용하여 정기적인 백업절차를 반영할 수 있다.
- 백업 절차 적용 및 운영 시 비교적 사용방법이 간단하여 일반 사용자도 충분히 백업을 이행 할 수 있다.
- 백업 담당자는 백업 후 원격지 NAS스토리지 또는 IDC 스토리지에 정상적인 백업 상태를 확인해야 한다.

※ NAS 응용프로그램 기능 중 자체 NAS Cloud 기능을 보유하고 있어 외부 지역에 백업을 수행할 수 있고, 타 Cloud 시스템에 백업을 구성할 수도 있다.



[그림 15] NAS 백업 소산 구성

(4) 외장 디스크 백업(USB/DVD 등)

① 외장 디스크(USB/DVD 등) 백업은 개발 소스 및 기업의 중요 파일에 대하여 직접 백업을 받아 별도 시건하여 캐비넷 또는 별도 장소에 보관하는 것을 말한다.

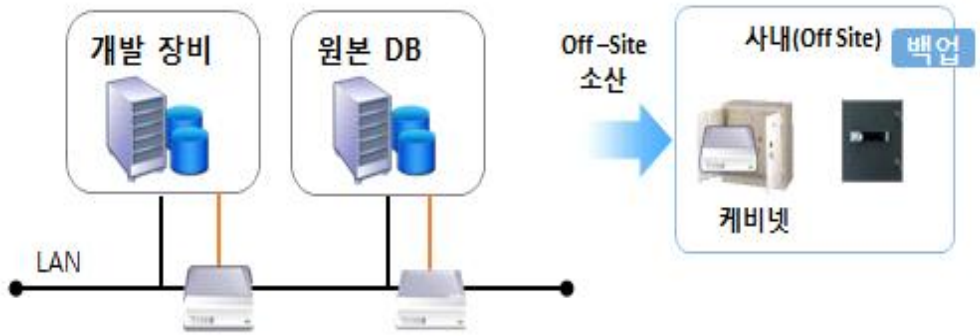
② 본 백업은 주로 사용자 PC 데이터를 백업하는 방식으로 랜섬웨어로부터 데이터를 보호하는 적절한 방법 중 하나이다.

③ 동일 장소 백업 시 효과적이며, 백업 후 백업매체 관리 절차를 수립해야한다.(출입 관리대장, 백업 매체 반·출입 대장)

④ 기업에서 외장 디스크(USB/DVD 등)에 백업을 하는 경우 백업 매체 보관을 위한 충분한 보호 조치가 필요하다. 예를 들자면, 잠김 장치가 된 케비넷, 문서고 등에 보관해야하며, 백업 관리대장을 구비하여 이력을 관리해야 하며, 기존 백업한 데이터에 대하여 삭제가 아닌 보존기간을 정하여 추가 백업하는 방식을 채택해야 한다.

⑤ 외장 디스크(USB/DVD 등) 백업 방법 및 절차

- 백업 방법은 시스템 운영제체 내 작업 스케즐 기능(Window 스케즐관리, Linux/Unix Crontab)을 배치 프로세스로 구성하여 정기적(주간, 월간) 백업 스케줄을 설정하는 방법이다.
- 백업절차는 외장 디스크(USB/DVD 등)이 직접백업과 동일하므로 향후 랜섬웨어 감염에 대비하기 위해서 여러 개의 백업 매체를 사용하여 백업을 수행해야 안전하다.
- 백업 담당자는 백업이 완료된 경우 반드시 백업된 데이터를 검증해야하며, 백업 이력(백업 날짜, 백업데이터 종류, 백업 수행자 등)을 관리해야 한다.



[그림 16] 외장 디스크 소산 백업 구성

(5) 백업 방법 선택 시 고려 사항

중소기업에서는 예산, 백업용량의 크기, 백업의 편의성, 백업 매체의 보관 공간 확보를 고려하여 백업 매체 및 방법을 선택해야 한다.

① 예산

예산이 부족할 경우, 백업 매체가 저렴한 테이프 백업이나 초기 구축 비용이 적게 소요되는 클라우드 백업을 권할 수 있다.

② 백업용량의 크기

대용량(1TB 이상)을 주기적으로 백업해야할 시 테이프 백업이 적당하다.

③ 편의성

백업을 위한 다양한 기능을 제공하고 있는 클라우드 백업 및 NAS 백업을 추천한다. PC 등의 소규모 자료를 수시로 백업하고 보관할 시에는 외장 디스크 백업을 사용할 수 있다.

④ 백업매체의 저장 공간 확보

자료를 백업한 후에는 원격지에 백업매체를 소산을 해야 하는데, 백업 매체의 보관할 수 있는 공간이 필요하다. 공간을 마련하기 힘들 경우에는 따로 저장 공간이 필요 없는 클라우드 백업을 채택할 수 있다.

7. 백업 정책

백업 시스템 구축이 완료되면 백업 정책을 수립하여야 한다. 백업정책은 백업데이터의 무결성과 가용성이 가장 중요하다. 최근 신·변종 랜섬웨어가 지속적으로 등장하고 있는 가운데, 랜섬웨어에 의한 피해를 최소화하기 위해서는 무엇보다 사전 예방이 가장 중요합니다.

다음은 안전한 백업을 위한 정책수립 절차 및 랜섬웨어 예방에 대하여 설명하고자 한다.

가. 오프라인 백업 유지

랜섬웨어 공격자는 감염된 시스템이 접근할 수 있는 모든 경로를 공격할 수 있으므로 데이터의 중요도가 높다면 반드시 오프라인 형태로 백업본이 유지 및 관리될 수 있도록 정책을 마련해야 한다.

나. 변경할 수 없는 저장소 사용

백업이 손상되는 것을 막기 위해 덮어쓰는 것을 막는 WORM(Write Once Read Many) 기술이 적용된 스토리지를 사용할 수 있다. 다만, 이 경우 백업 비용이 증가하기 때문에 증분 백업이나 중복 제거 기술을 사용해 백업되는 데이터를 최소화하거나 데이터의 중요도에 따라 차등 적용하는 것이 좋다.

다. 비즈니스 인프라 백업도 고려

랜섬웨어의 공격 대상은 데이터지만 피해자는 데이터 복원과 함께 시스템을 정상화해야 하기 때문에 관련 소프트웨어, 구성 요소, 네트워크 설정, 종속성 등을 고려해야 한다. 랜섬웨어 공격 후 시스템 혹은 내부 인프라를 재설정해야 한다면 데이터 복원에 걸리는 시간보다 시스템 혹은 인프라 환경을 새롭게 설정하는 시간이 더 많이 걸린다.

예를 들어, 랜섬웨어 공격으로 AD(Active Directory) 환경을 재구축해야 할 경우 기존의 AD 구성 정보의 백업 여부에 따라 비즈니스 정상화에 걸리는 시간은 많은 차이가 날 수 밖에 없으므로 데이터 백업과 함께 비즈니스 환경의 백업도 고려해야 한다.

라. 여러 유형의 백업 유지

백업 대상에 따라 시스템 백업, 데이터 백업, 변경 로그 백업 등 다양한 방식이 있으므로 데이터의 유형과 중요도에 따라 다양한 유형의 백업을 유지해야 한다.

외부의 영향으로부터 백업 데이터의 안전성 확보를 위해 다중 백업을 실시하더라도 최근 악의적 목적의 웜(랜섬웨어 등)으로부터 중요 데이터를 안전하게 보호하기 위해서는

소산백업 이후 네트워크를 분리하여 보관해야 한다.

대상별 종류	백업 대상	백업방식	백업주기	비고
시스템 백업(OS)	OS 파일 시스템 백업 (Boot 영역)	FULL	월간 백업 변경작업 전	
데이터베이스 (On/Off)	DBMS / 구성파일	FULL	격주 / 주 1회	
	DB Archive Log	FULL/INC	매일	
파일 시스템 백업	Application실행 파일 및 소스	FULL/INC	주 1회	
	일반 DATA	FULL/INC	주 1회	
	각종 Log 파일	FULL	주 1회	

[표 11] 백업정책 적용 예시

다음은 백업 대상별 백업방식 및 백업주기 등 정책 사례에 대한 설명이다.

마. 백업방식 결정

백업방식은 일회 백업시 전체를 백업대상으로 하거나 변경분만을 대상으로 하는가에 따라 전체 백업(full backup)과 증분 백업(incremental backup)으로, 백업 시의 업무서비스 제공여부에 따라 온라인 백업(on-line backup)과 오프라인 백업(off-line backup)으로 분류할 수 있다. 또한, 백업 데이터의 형태에 따라 파일단위와 로 디바이스단위로 구분할 수 있다.

다음은 다양한 백업 방식을 결정하기 위한 절차이다.

▷ **1단계 : 백업대상서버 식별**

- 전체 서버 중 백업이 필요한 서버를 식별하고 서버별 중요도 식별

▷ **2단계 : 백업대상서버 백업대상 데이터 식별**

- 백업 대상 서버에서 백업 대상 File 혹은 DB를 식별
- 백업 대상 데이터의 용량 파악

▷ **3단계 : 백업대상 데이터별 백업시스템 식별**

- 백업 대상 서버의 서비스에 따른 백업이 가능한 시간 식별

▷ **4 단계 : 백업대상 데이터별 백업주기 식별**

- 백업 시스템 및 백업 데이터 용량을 고려한 백업 주기 및 백업 Level(Full, Incremental 등) 식별

▷ **5단계 : 백업대상 보관기관 식별**

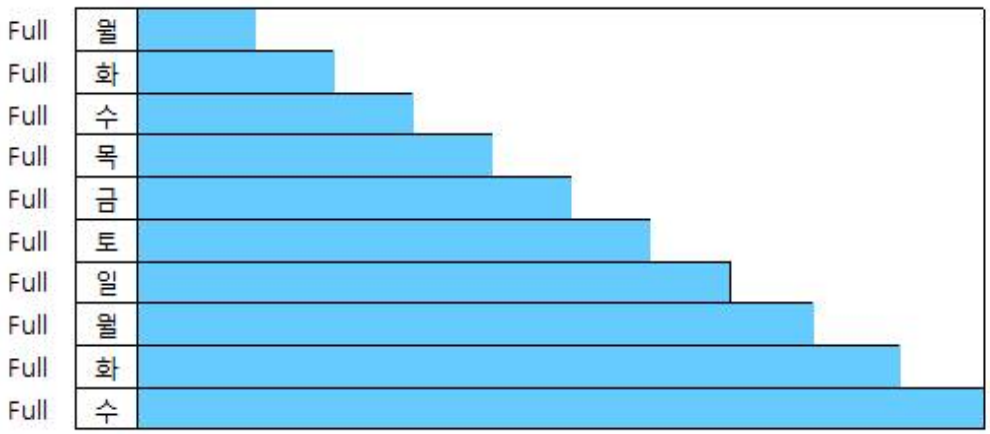
- 데이터의 중요도 및 과거 데이터 필요성을 고려한 보관기간 식별(1주, 1개월, 1년, 영구 등)

▷ **6단계 : 백업정책 수립 및 정책 적용**

1) 전체 백업과 증분백업

(가) 전체 백업(Full backup)

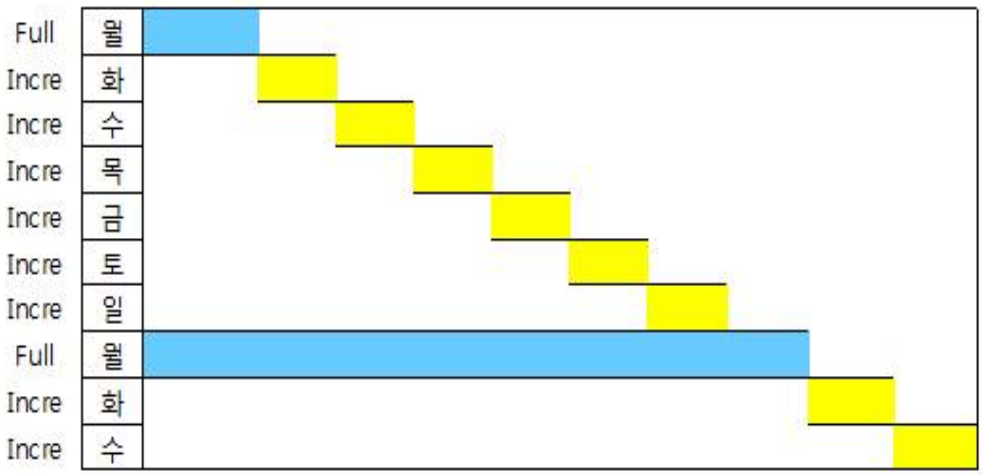
'변경(changed)' 데이터나 '고유(unique)' 데이터를 전혀 구분하지 않고 백업할 때마다 모든 데이터의 복사본을 만드는 백업 방식이다. 전체 백업은, 복구 시에 일부 다른 백업 방식보다 간편하고 시간이 증분 백업에 비해 상대적으로 덜 걸린다는 장점이 있다.



[그림 17] Full 백업 방식 예시

(나) 증분 백업(Incremental backup)

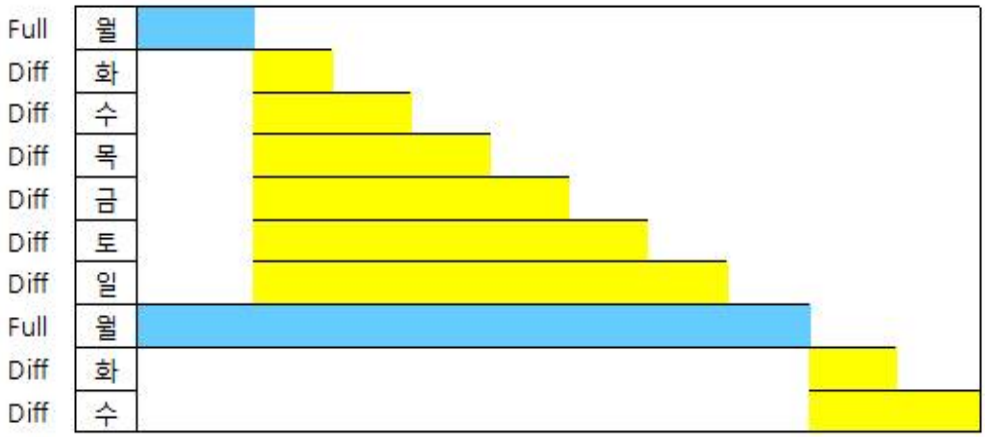
전체백업과는 달리 최종 전체 백업 혹은 최종 증분 백업 이후에 변경된 파일만을 복사한다. 전체 백업과 비교할 때 증분 백업은 매일 백업해야 하는 파일의 양이 적어 빠른 백업 윈도가 가능하다는 점이 장점이다. 그러나 복구 과정에서는 최종 백업된 전체 및 모든 후속 증분 이미지나 복사본까지 복구해야하기 때문에 복구 작업이 번거로워지고 경우에 따라서는 시간이 훨씬 더 걸릴 수 있다.



[그림 18] 증분백업 방식 예시

(다) 차등 백업(Differential backup)

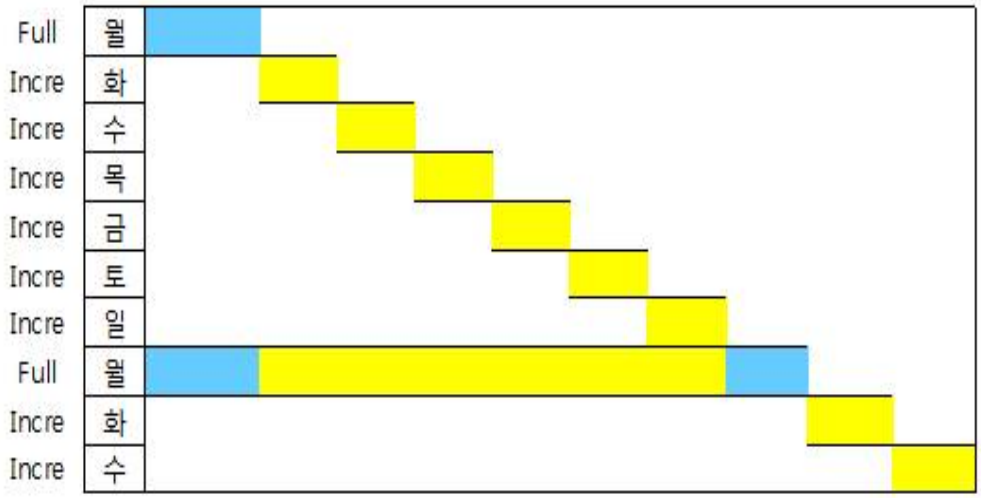
'전체 백업' 이후 변경된 '모든' 데이터를 백업하는 방식이다. 이는 바로 이전의 전체 백업 혹은 증분 백업 이후 '변경된' 데이터만 복사하는 증분 백업과는 다르다. 일단 파일이 변경되면 예정된 다음 전체 백업 시까지 매일 백업한다. 따라서 파일이 변경될 때마다 파일 크기가 증가하게 되며, 다음 전체 백업 때까지 파일크기가 점점 커지게 된다. 하지만, 전체 백업 이미지와 가장 최근의 차등 이미지만 복구하면 되기 때문에 복구 시점에 따라 다르긴 하지만 대개 증분 백업보다 복구 속도가 빠르다.



[그림 19] 차등백업 방식 예시

(라) 신세틱(Synthetic Backup) 백업

기본 백업과 후속 증분 백업으로부터 전체 백업을 구성하거나 통합하는 방식의 백업을 말한다. 선택된 폴더의 Full 백업 이후 변경, 추가된 Data를 Incremental Backup 형식으로 저장 후 두번째 Full 백업 작업시 중간에 모아 둔 Incremental backup을 이용하여 Full Backup으로 재생성 하는 방식으로 Synthetic 백업을 이용하면 백업 서버에서 이미 저장되어 있는 Incremental Data를 이용해 Full Backup을 새로 만들기 때문에 Network 사용량을 줄일 수가 있습니다.



[그림 20] 신세틱(Synthetic) 백업 방식 예시

(마) 중복제거(Deduplication Backup) 백업

한개의 파일 혹은 여러 개의 파일에서 동일한 부분은 하나만 저장하고 나머지 파일 구조는 메타 데이터로 따로 저장하여 백업 저장소와 백업 DATA를 줄일 수 있습니다.

증분/차등 백업 그리고 중복제거 변경된 파일을 가져 온다는 의미에는 큰 차이점이 없습니다. 그러나 실제로 백업 소프트웨어에서 동작할 때 차이점이 발생 한다.

[그림 21] 중복제거 백업 방식 예시

백업 소프트 위에는 파일단위 백업이 기본이기 때문에 파일의 사이즈에 관계없이 변경되면 변경된 파일을 모두 백업하도록 동작 한다.

중복제거 기술은 섹터 단위로 파일을 검사하기 때문에 변경된 섹터의 값만 다시 백업한다.

2) 백업 시의 업무서비스 제공 여부에 따른 방식

(1) 온라인 백업

백업 시 데이터베이스의 다운타임을 가지지 않고 해당 데이터를 백업하는 방식이다. 보통 백업 소프트웨어에서 제공하는 데이터베이스 옵션을 사용하여 백업하기도 하

지만 표준 쉘(Shell) 스크립트를 이용하여 특정시간에 자동으로 실행하는 경우가 더 일반적이다.

(2) 오프라인 백업

백업 시 데이터베이스를 다운시키고 백업을 받는 방식이다. 업무상 다운 시간을 확보할 수 있는 경우에 사용되며 가장 확실한 데이터베이스 백업방식이다. 주간, 월간, 연간, 또는 수시 백업시 수행하는 경우가 보통이다. 데이터베이스 데이터 구성방식은 파일 단위와 로디바이스 단위 구성방식이 있다.

(가) 소산백업

백업 실시 후 재난 및 재해에 대비하여 백업 테이프를 외부에 보관하는 경우가 많은 데 이를 소산 백업 또는 볼팅(Vaulting)이라 한다.

소산 백업의 주기는 보통 월별, 분기별 등 백업 주기와 같이 정기적으로 실시하며, 동일 건물 내 또는 너무 멀리 있는 원격지에 보관하는 경우는 좋지 않다. 동일 건물 내 보관하는 경우, 건물 재난 발생시에 백업시스템과 동시에 망실이 일어 날 수 있기 때문이다. 너무 멀리 있는 원격지에 보관하는 경우는 테이프 운송시간이 과다하게 발생하여 전체 복구 시간이 길어 질 수 있다.

① 소산 백업 방법

- 소산 백업은 정기적인 스케줄로 운영하며 원격지에 테이프를 보관하는 것이므로 소산용 테이프도 별도로 두어야 한다.
- 백업 소프트웨어에서 소산 백업만을 위해별도 백업을 수행하기도 하지만 정기 백업 시 두 벌씩 데이터를 백업하거나, 백업 완료 후 매체 복사를 통해 한 벌을 소산하여 다른 장소(내화 금고, 원격지 등)에 보관하여 안정성을 확보해야 한다.
- 외부로 소산되는 테이프들은 매체 관리대장을 만들고 매체에 라벨 링을 해서 쉽게 식별가능 하도록 한다.

② 내화 금고 및 기타

소산용으로 백업된 테이프는 테이프 공급자들이 권장하는 온도와 습도 하에서 내화 금고에 보관되는 것이 가장 이상적이다. 그러나 내화 금고는 별도 공간 및 관리 비용을 고려해야 하므로 중소기업의 경우별도 시건된 케비넷 또는 네트워크를 절체한 특정된 NAS 시스템에 보관이 효율적이다.

바. 백업 수행 점검 및 복구훈련

1) 백업대상 확인

백업대상 시스템에 대해 적절한 소프트웨어 모듈이 설치되었는지 확인하고 백업대상 파일들이 모두 포함되어 있는지 확인한다. 네트워크 백업대상들의 경우 중계 할 서버(주로

백업 전용 서버)들이 정의되어야 한다.

2) 복구 훈련

비상시 복구 훈련은 백업시스템 설치 직후 또는 정기적으로 실시하여 데이터의 무결성을 확인을 목적으로 데이터를 리스토어 가용성을 확인해야한다.
복구 훈련을 통해 복구시간을 산정하여야 하는데 일반 파일의 경우에는 복구시간이 리스토어 시간과 동일하지만, 데이터베이스의 경우 리스토어 시간과 리커버리(Recovery) 시간을 합친 시간 이 복구시간이 된다.

복구시간 = 리스토어 시간 + 리커버리 시간

(가) 리스토어 시간
테이프로 백업받은 데이터를 다시 디스크로 복사하는 시간으로서 백업 장비의 성능과 디스크 성능에 따라 좌우된다.

(나) 리커버리 시간
리스토어 이후에 데이터베이스를 장애가 난 시점으로 복구하는 시간으로서, 데이터베이스가 변경로그 모드인 경우 백업 후 장애시점까지 발생한 변경로그를 데이터베이스에 적용하는 시간이다.
시스템 및 데이터베이스 운영자는 데이터베이스의 각종 장애 시 시스템별 복구시간을 예측할 수 있어야 하는데 데이터베이스 복구 예측시간을 MTTR(Mean Time To Recovery)이라고 한다.

3) 백업 관리 유의 사항

(가) 백업 저장 매체에 대한 물리적 접근통제
물리적인 백업 테이프 접근은 원본 파일시스템이 또는 데이터베이스가 있는 디스크에 루트 권한으로 접근하는 것과 동일하다. 테이프를 무방비로 노출시킨다면 어느 곳에서나 테이프를 읽을 수 있다.
따라서 별도의 접근통제 절차를 수립해야 한다.

※ 백업 후 백업 매체에 대한 접근통제
- 허용된 사용자(백업 운영자)만 접근 가능
- 출입 시 반드시 출입관리대장을 기록
- 백업 매체 반출·입 시 반출·입 대장관리

(나) 백업 매체는 재난 및 재해로부터 안전한 장소에 보관
적정한 습도와 온도를 유지할 수 있는 안전한 장소(예로 내화금고)에 백업 매체를 보관하여, 재해로부터 보호될 수 있도록 해야 한다.

(다) 비인가자의 데이터 복구 통제
데이터 복구 시는 반드시 복구신청서를 수령하되 신청자의 부서장 허가와 백업담당 부서장의 허가를 받아 복구하여야 한다.

(라) 백업 매체(데이터)는 원격/소산 보관
동일 네트워크 구간 또는 물리적으로 동일한 장소에 보관은 재해발생 시 데이터가 망실 가능하며, 랜섬웨어 감염 시 백업데이터가 동일 네트워크에 위치한 경우 데이터의 복구가 불가능할 수 있으므로 가까운 IDC에 소산하거나 Cloud 백업 소산 방법을 사용하는 것이 안전하다.

(마) 백업 테스트를 통한 백업 및 복원 정기적 적정성 확인
주기적인 백업을 수행해야하며, 다양한 환경에서 테스트를 연 1회 이상 실시하여 데이터의 무결성을 유지해야 한다.

① 실제 환경을 반영해 하드웨어, 소프트웨어, 서비스 장애 상황 테스트
② 사용할 수 있는 모든 복원 옵션을 테스트
③ 변경관리가 필요한 변화가 발생한 경우 테스트
④ 테이프 같은 기존 백업 미디어가 새로운 백업 하드웨어 및 소프트웨어에서 정상 기능 확인

(바) 백업 담당자 및 운영자 PC의 외부 네트워크 접근 통제

① 일반 중소기업의 시스템 담당자(백업 담당자 겸직), 백업 운영자들의 업무용 PC외 허가되지 않은 PC에 대하여 사내 반입하여 네트워크 접근을 통제해야 한다.
② 업무용 PC의 경우 최신 패치 및 백신업데이트를 실시간으로 설정해야하고 외부 인터넷을 차단 또는 망분리 해야 한다.

(사) 백업 환경 점검
백업 관련 담당자 및 운영자 PC를 대상으로 악성코드 감염, 백신 업데이트, 패치, 공유폴더 사용, 외부 인터넷 사용 여부 등에 대한 보안성을 점검해야 한다.

8. 백업시스템 보호대책

가. 시스템 보안

1) 계정 관리

(가) 계정 등록, 변경, 삭제에 대한 절차를 수립하고 처리결과를 기록하여 보관한다.

(나) 모든 사용자 계정은 최초 생성에서 삭제까지 이력이 관리되어야 하며 최신의 상태를 유지해야 한다.

(다) 모든 계정에 생성 및 변경 이력에 대하여 분기 1회 이상 비정상 여부를 점검해야 한다.

(라) 퇴사나 전환배치 등 인사 변경이 발생한 경우 정해진 절차에 따라 삭제 또는 권한을 변경해야 한다.

(마) 모든 사용자는 유일한 1개의 계정을 사용해야 하며, 공용 계정 사용을 금한다. 단, 공용 계정이 필요한 경우 정보보호 책임자 및 해당 관리자의 승인을 득한 후 부여한다.

(바) 일정기간(90일) 이상 사용되지 않은 계정은 일시 중지시키거나 삭제한다.

(사) 일반 사용자에게 슈퍼유저의 권한을 부여하지 않으며, 콘솔 이외의 단말기에서는 슈퍼 유저로 직접 로그인하는 것을 금한다. 단, 업무상 필요시에는 SSH 등과 같이 보안이 강화된 툴을 사용하여야 한다.

(아) 계정에 사용자 신분과 관련된 정보가 포함되지 않도록 한다.

2) 패스워드 관리

(가) 사용자는 패스워드에 대하여 비밀을 유지해야 하며, 타인에게 가르쳐주거나 노출시켜서는 안 된다.

(나) 패스워드는 영문 대·소문자와 숫자, 그리고 특수문자 중 최소 3가지 이상을 혼합하여 최소 8자 또는 2종류 10자리 이상으로 하며, 연속 4자리 동일 문자의 사용을 금지하고 ID와 동일한 패스워드 사용을 금지한다.

(다) 패스워드는 3개월 주기로 변경하여 사용해야 한다. 유출된 경우, 즉시 변경한다.

(라) 임시 패스워드는 최초 로그인 시 새로운 패스워드로 변경하여야 한다.

(마) 계정 및 사용자 정보(생일, 전화번호 등)가 포함된 패스워드를 사용하지 않는다.

(바) 패스워드는 모니터, 책상서랍 등 타인의 눈에 쉽게 띄거나 위치를 유추할 수 있는 곳에 기록하여서는 안 된다

(사) 서버 담당자가 패스워드를 전달할 경우, 사용자를 확인하는 절차를 거쳐야 하며 팩스나 전화로 전달하여서는 안 된다

(아) 패스워드가 타인에게 노출되었거나 노출이 의심될 경우 즉시 변경하여야 한다.

(자) 패스워드는 암호화하여 관리하여야 한다.

(차) 패스워드나 세션 정보가 자동 저장되도록 설정해서는 안 된다.

3) 로그인

(가) 중요정보가 저장된 서버는 보안 로그인을 지원하는 툴을 이용해서 접속하며 강화된 인증(인증서, 토큰, 생체인식 등)을 적용할 수 있다.

(나) 1차 인증 정보가 노출되더라도 접근할 수 없도록 가능한 다단계 인증(MFA, Multi-Factor Authentication)을 적용해야 하고, 2차 인증 정보는 OTP(One Time Password)와 같이 일회성 정보를 사용해야 한다.

(다) 사용자가 응용시스템에 로그인하기 전에 보안경고 문구를 표시하고 로그인 시에는 서버에 대한 어떠한 정보도 노출되지 않도록 설정하여야 한다.

(라) 일정횟수 이상으로 패스워드를 잘못 입력할 경우 세션을 차단시켜야 한다.

(마) 서버에 접속한 후 일정시간 동안 어떤 입력도 일어나지 않으면 자동적으로 로그오프 시키거나 세션을 중단시켜야 한다. 서버의 사용은 업무의 효율성을 고려하여 필요한 경우 업무시간 외에도 사용할 수 있도록 한다.

4) 권한 관리

백업 담당자는 서버 또는 DB 내에 보관된 정보에 대한 접근 권한 및 서버 사용상의 권한을 사용자에게 부여 시 다음의 사항을 준수한다.

(가) 서버 접근에 필요한 권한의 요청 및 변경, 삭제는 공식적인 절차를 통해 이루어져야 하고, 처리 결과는 향후 감사나 문제 발생 시의 자료로 사용할 수 있도록 보관해야 한다.

(나) 서버 담당자는 사용자 별 접근 가능한 정보를 기술한 접근 권한 관리 목록을 만들어 유지, 관리한다.

(다) 서버 담당자 및 해당 서버 소유자는 주기적으로 사용자에게 부여된 권한을 점검해야 한다.

(라) 서버 담당자는 서버의 정상적인 운영을 방해하거나, 다른 사용자의 사용을 저해하는 등의 행위가 발견되거나 의심이 될 때, 공식적인 절차에 따라 해당 사용자의 권한을 제한 또는 취소할 수 있다.

(마) 특정 수준의 정보에 대한 접근 권한을 부여 받은 사용자는 해당 수준 또는 그 이하의 정보에만 접근 가능하도록 해야 하며, 그 이상의 권한이 필요한 정보에 대해서는 접근을 제한한다.

5) 접근 통제

(가) 기업 내 IT인프라에 대한 접근통제

- 네트워크를 통한 시스템 접근 권한은 원격 로그온이 반드시 필요한 계정에만 설정하도록 한다.
- 보안로그와 감사는 관리자 그룹만이 관리하여야 한다.
- 공유 폴더의 필요성을 검토하여 불필요한 공유 기능을 제거하여야 한다.

- 시스템에 설치된 서비스를 조사하여 불필요한 서비스는 제거하여야 한다.
- 사용자는 서버 담당자 및 정보보호 담당자의 사전 승인이 없는 한 운영체제의 접근 통제 기능 또는 접근 통제 도구를 우회할 수 있는 프로그램을 사용해서는 안 된다.
- 서버 담당자는 시스템 파일과 일반 데이터 파일을 논리적 또는 물리적 분리 구성하고 접근통제를 적용한다.
- 시스템 유틸리티 및 데이터, 라이브러리(library) 등의 중요 시스템파일에 대한 사용자의 접근을 엄격히 통제해야 한다.
- 서버 담당자는 서버가 정상적으로 동작하지 않을 경우 정상적으로 동작될 때까지 사용자의 접근을 제한할 수 있다.
- 서버 담당자는 일관성 있는 접근 제어를 위하여 사용자 ID, 파일 이름, 서버 명 등에 대한 명명규칙을 표준화하여 관리한다.
- 모든 접근 권한은 RBAC(Role-Based Access Control)를 사용해 사용자의 역할에 따라 최소 권한이 부여될 수 있도록 관리한다.

(나) 백업관점의 통제

① 백업본 소산

- 랜섬웨어 피해의 가장 큰 원인 중 하나는 원본서버와 백업서버가 동일 네트워크상에 운영되는 경우 많은 피해를 볼 수 있다.
- 피해를 최소화하고 신속한 복구를 위해서는 최소 1개 이상의 백업본은 네트워크의 외부나 클라우드에 저장해야 한다.

② 백업시스템 접근 제한

- 백업시스템에 접근은 외부 네트워크로부터 접근을 차단해야 하며, 운영자는 백업시스템이 위치한 곳에서 접속해야한다.
- 일반 사용자의 원격접속은 불가능하게 차단하거나 원격접속을 최소화해야 한다. 가급적 물리서버에 직접 콘솔을 연결하거나 인터넷망과 분리된 격리 영역에서 시스템에 접속하도록 통제해야 한다.

③ 접근이 어려운 백업시스템

백업시스템이 범용적일수록 램섬웨어 공격에 취약하므로 독자적인 OS를 사용하고, 독자 전송 프로토콜을 사용하면 상대적으로 안전하다.

④ 안전한 스토리지

윈도우에서는 랜섬웨어가 시스템에 로딩 되면 접근 가능한 모든 파일을 감염 시킨다. 따라서 스토리지 내에서 파일이 실행될 수 없는 구조라면 백업시스템 내에서도 데이터의 무결성을 보장 받을 수 있다.

- 백업 시스템 소프트웨어 데이터 백업 옵션 기능 중 읽기 전용, 덮어쓰기 금지, 포맷 금지 등 옵션을 활용

- 별도 옵션이 없을 경우 백업 이후 별도 영역(별도 DISK, TAPE, NAS 등)에 격리

6) 보안패치

최근 기업의 중요 정보에 대한 침해사고가 빈번히 발생하는 원인 중 하나가 시스템에 대한 패치 적용 미흡으로 기업의 사내 서비스 IT 인프라에 악성코드 또는 웜(랜섬웨어 등) 감염으로 인해 데이터의 망실과 금전적인 손실이 발생하고 있다.
다음은 기업의 사내 시스템 및 운영 담당자 PC에 대한 패치 요령 및 관리에 대하여 기술한 것이다.

(가) 보안패치는 각종 소프트웨어, 운영체제 등에서 발견되는 보안상의 취약성을 보완해주는 프로그램으로 새로운 취약성에 대한 보안패치가 발표되는 즉시 시스템에 적용하여 보안조치를 취함으로써 보안사고를 사전에 예방할 수 있도록 한다.
- 보안패치 정보를 주기적으로 입수하고 적용
- 주요 보안패치에 대해서는 적용일 등 패치정보를 기록·관리

(나) 조직 내의 패치 적용 대상 시스템, 소프트웨어 별로 보안패치 방법 및 절차를 정리하여 패치 적용 정보를 기록·관리하도록 하고 다음 사항을 포함하도록 한다.
- 시스템 성능 및 환경의 문제로 패치를 하지 못하는 경우에는 해당 사유와 이를 보완하기 위해 적용한 대체수단이나 방법을 기록
- 각 서버에서 사용되는 소프트웨어 목록 및 버전 정보 목록 관리
- 각 소프트웨어 또는 시스템 제공업체의 홈페이지를 확인하여 최신버전의 보안패치 목록 및 패치 방법 확인
- 패치 설치 후 서버의 정상적인 운영상태 확인

(다) 기타 보안패치 관리 작업을 자동화 해주는 소프트웨어를 사용할 경우, 위 사항들을 만족하고 있는지 주기적으로 검토한다.

7) 백업 관리

(가) 서버장애나 저장매체의 불량으로부터 중요정보와 소프트웨어를 보호하기 위해 월간 백업을 시행하고 정보소유자와 협의 하에 적정한 기간 동안 보관되어야 한다.

(나) 기밀정보의 백업내용은 필요에 따라 암호화해 보관해야 한다.

(다) 백업할 데이터에 대해 백업의 방법 즉 전체 파일을 대상으로 할 것인지 아니면 변경된 파일만 대상으로 할 것인지에 대해 결정을 해야 하며 또한 백업 수행시간 및 백업 수행 담당자를 지정해 놓아야 한다.

(라) 테이프 드라이브와 백업 테이프는 권한이 없는 사용자가 접근할 수 없는 격리된 곳에 보관한다. 권한이 없는 사용자에 미디어가 노출되면 자신들이 관리하는 시스템에 복구하여 미디어 내용물에 접근을 할 수 있으므로 안전하게 관리해야 한다.

(마) 저장매체 관리 부주의로 인한 정보유출을 최소화하기 위하여 기밀정보를 포함한

저장매체의 안전한 처리를 위한 절차가 수립되어야 한다.

(바) 서비스 제공 및 업무 수행과 직접적인 관계가 있는 주요정보는 물리적 재난이나 정보통신설비의 오류 발생으로 긴급상황이 발생할 경우, 즉각적으로 복구할 수 있도록 주기적으로 백업을 수행하고 백업 매체를 안전한 곳에 보관하도록 한다.

(사) 위험분석 등의 방법을 통하여 자체적으로 중요도에 따라 관리가 필요한 주요정보를 식별하고 주요정보에 대한 백업 계획을 마련한다. 정보의 중요성 및 특성을 고려하여 백업의 방법 및 횟수 등의 백업 계획을 마련한다.

(아) 백업은 백업될 데이터의 성격에 따라 백업 시기, 백업주기, 백업방법, 백업데이터의 보관방식 및 보존기간 등을 포함하여 백업 담당자, 백업 및 복구 방법.절차.주기 등을 기록/관리 한다.

8) 복구

(가) 수립한 백업 및 복구 방법.절차는 다음과 같은 단계에 따라 수행되도록 한다.

- 장애발생 상황인지 및 보고
- 복구 우선순위의 결정
- 사후 점검 및 원인분석
- 장애 및 복구기록 유지관리 등

(나) 복구는 가장 믿을만한 백업매체를 사용해야 한다. 피해 시점 또는 문제발생 시점 이전의 백업 본을 사용하도록 한다. 백업·복구의 관리를 위해 관리대장을 만들고 기록할 수 있도록 한다.

(다) 다음은 복구 절차 사례에 대하여 설명한 것이다.

단계	업무	세부 내용
1	재난상황 접수집합	▪ 재해를 통보 받으면, 요원들은 지시되는 대로 긴급 대기 또는 소집 ▪ 요원들은 소집 시 시간/장소를 확인하고 미리 발행된 계획서사본 지참
2	복구팀 구성	▪ 재해복구팀장을 지원하여 재해 상황을 유지하며, 복구를 위한 팀 구성
3	대응조치통보	▪ 재해복구를 위한 재해복구계획을 재해복구팀과 수립하고 재해복구조직에 재해복구 방안을 설명
4	대응조치 문서화	▪ 대응조치를 위한 재해복구계획을 문서화하여 전 임직원이 공유토록 지원
5	업무복귀시간 및 장소통보	▪ 업무복귀 시간 및 장소에 대해 재해복구팀장과 결정하고, 관련 직원 및 재해복구조직에게 통보

6	복구 및 업무 재가동 현황	▪ 복구 현황 및 업무 재가동 현황을 파악하여 관련 임직원 공유
7	요원가동현황 관리	▪ 직원의 가용현황을 수시로 파악/검토 ▪ 안내정보를 제공, 임무를 부여 ▪ 업무 보고 요건을 규정
8	재해복구팀장 지원	▪ 재해복구팀장이 원활히 복구업무를 수행할 수 있도록 지원부서, 상황유지부문과의 원활한 업무협조 지원
9	재해종료	▪ 재해복구완료 후 결과를 문서화하여 관리

[표 12] 백업 복구 절차 예시

9) 보안관리

(가) DB서버의 취약성과 관련된 정보는 허용된 사용자만 접근할 수 있도록 엄격히 제한해야 한다.

(나) 정보보호 담당자는 취약성 점검을 위해 정기 혹은 수시로 서버에 대한 보안 취약성 스캐닝 작업을 수행하고 취약성을 시정 조치한다.

(다) 업무적으로 불필요하거나, 침해의 위협이 있는 네트워크 서비스를 제공하지 않도록 한다.

(라) 서버의 하드웨어 및 소프트웨어는 지속적인 가용성과 무결성 확보를 위해 주기적으로 예방점검을 해야 한다.

10) 바이러스 관리

(가) 악성코드 및 바이러스 감염을 방지하기 위해 서버에 바이러스 검색 프로그램을 설치하고 주기적으로 바이러스를 점검해야 한다.

(나) 서버 담당자는 바이러스 패턴이 최신으로 유지되도록 관리한다.

(다) 서버 담당자는 서버에 파일을 업로드하기 전에 바이러스 감염 여부를 검사한다.

11) 변경 이력 관리

(가) 데이터 백업의 신청, 변경, 소산 등에 대하여 백업관리 대장을 구비하여 변경 이력에 대하여 관리해야한다.

(나) 기업 내 시스템 백업과 데이터 백업에 대하여 구분하여 관리되어야 한다.

(다) 백업 보관 주기 및 백업 주기, 백업 방식에 대하여 백업 정책 이력을 관리해야 한다.

(라) 백업 데이터의 주요한 변화에 대하여 반드시 정보보호부서와 협의하여 보안성을 검토하여 해당 이력을 공유해야 한다.

12) 로그 기록

백업 운영자는 정보보호 사고 발생시 추적성을 확보하기 위해 다음 각 항과 같은 로그를 기록하도록 설정해야 한다.

(가) 기밀정보를 취급하는 서버의 경우 기밀정보의 추자·수정·삭제 및 보안 위반사항들에 대해여 로그를 기록하여야 한다.
(나) 사용자 책임성을 확보하기 위해 사용자의 모든 보안관련 활동은 로그에 기록되어야 한다.
(다) 로그는 보안대책의 효과성 또는 준수성을 종합적으로 점검하기 위한 내용을 포함하여야 한다.
(라) 장애 및 시스템 운영자에 의해 발행되는 시스템 관련 명령어는 로그를 통해 추적할 수 있도록 해야 한다.
(마) 시스템 커널(Kernel)이나 중요파일에 접근할 수 있는 시스템 프로그래머의 활동은 로그가 기록되어야 한다.
(바) 백업 운영자는 정보보호 담당자와 협의하여 시스템의 성능 및 디스크 용량 등을 고려하여 로그기록 대상을 선정한다.
(사) 시스템 침해가 발생했다고 의심될 때 증거확보를 위해 관련정보를 사고처리 절차에 따라 확보해야 한다.

13) 로그 위변조 방지 및 검토

백업업무 운영자는 로그기록 시 다음의 각호를 준수하여 관리해야 한다.

(가) 백업업무 운영자는 로그의 정확한 기록을 위해 네트워크에 연결된 모든 서버의 내부 시각을 일치시키도록 한다.
(나) 중요 서버의 로그 파일들은 별도의 로그서버를 지정하여 통합 저장하여 운영할 수 있으며, 로그에 대한 정기적인 백업을 실시하여 로그 변조 행위에 대응한다.
(다) 로컬 서버에 로그가 저장될 경우 접근통제, 로그 파일 복사 등을 통해 로그 위·변조를 방지한다.
(라) 시스템 접속내역을 기록한 로그는 정보보호 책임자, 전사 정보보호 담당부서의 요청, 사용자의 서면동의나 법률에 의한 사직당국의 협조요청에 의하지 않고는 타인에게 공개하지 않는다.
(마) 백업업무 운영자는 주기적으로 정보보호에 관련된 로그 기록을 검토하여야 한다.
(바) DB 서버의 정보보호 관련 로그 및 접근권한에 관한 기록은 비인가자로부터 로그의 누설이나 수정을 할 수 없는 곳에 안전하게 보관한다.

14) 모니터링

(가) 백업업무 운영자는 정기·비정기적으로 로그를 분석 모니터링 한다.

(나) 백업업무 운영자는 다음 각 호에 대해 모니터링 한다.

- 시스템 사용량 부하
- 파일시스템 용량초과
- 프로세스 루핑(looping)
- 사용자 접속현황
- 비인가자의 접근

(다) 이상 상황 발생 시 신속히 조치한 후 정보보호 담당자 또는 책임자에게 보고한다.

15) 장애 관리

(가) 장애 시 백업 운영자는 다음과 같은 사항을 고려하여 장애보고서를 작성하여 시스템 운영관리자에게 보고하고 보안과 관련된 장애사항이 발생할 경우 정보보호 담당자에게 통보하여야 한다.

- 소속 및 장애 명
- 담당자, 장애발생일, 장애발생시간
- 장애현황 및 장애원인
- 조치결과 및 향후 계획
- 서비스 영향도.

(나) 백업 운영자는 장애 보고서 작성 시 정보보호 이슈에 대해 정보보호담당자에게 지원을 요청할 수 있다.

(다) 백업 운영자는 장애 처리 관련 정보를 안전하게 보관하여야 하며, 장애 예방자료 및 장애 발생시 참고자료로 이용 가능하도록 하여야 한다.

(라) 백업 운영자는 정보보호 관리 업무의 일환으로 이루어지는 장애 처리의 기록, 보관, 활용에 대한 정보보호담당자의 확인 요청에 협조하여야 한다.

나. 네트워크 보안

1) 네트워크 IP통제

(가) 백업 시스템에 대한 네트워크 IP통제를 위해 백업운영자는 백업시스템에 지정 IP를 신청하고 IP 할당 이후 지정된 접근통제 영역에서만 백업시스템 및 기타 인프라에 접근하도록 한다.

(나) 기업 내 네트워크 구성은 인터넷이 가능한 업무망과 주요 시설을 관리하는 내부 IT 인프라가 위치한 내부망으로 구분하여 IP통제 정책을 반영해야 한다.

① 업무망과 인터넷망의 IP설계 시 다른 Subnet을 분리 구성하거나 별도 방화벽에 네트워크 영역을 분리하여 반영

② 백업담당자 PC에서 백업시스템 또는 DB에 접속 시 접속 IP를 특정하여 해당 IP로만 접속할 수 있도록 접근통제 정책 적용

2) 접근통제

(가) 백업업무 담당자는 DB 및 백업 시스템에 대한 접근시 지정된 PC 및 콘솔에서 수행하는 것을 원칙으로 한다. 단. 시스템 유지보수를 위한 접근 시는 예외로 하며, 전산실 내 지정된 PC로 접속할 수 있도록 통제해야 한다.(외부 유지보수 업체 PC의 경우 외부 인터넷에 접속하여 취약할 수 있으므로 반드시 충분한 방역처리를 해야 함)

(나) 백업업무 담당자는 DB 및 백업 시스템에 대한 접근 권한 부여 시 다음 사항을 준수한다.

① 다음 사항을 준수하여 권한 오남용을 방지한다.

- ✓ 시스템 접근 권한은 백업관리자(팀장)과 정보보호 주관부서의 승인을 받아야 한다.(유지보수, 장애처리 등 업무적인 필요성에 의하여 협력직원에게 접근 권한을 부여시도 동일하며, 이러한 권한은 업무 종료 시 삭제)

② 정보보호담당자는 주기적으로 권한이 적절히 설정되어 있는지 검토한다.

- ✓ 시스템에 접속할 경우 계정 및 패스워드 등의 인증체계를 사용하여 접근한다.
- ✓ 로그인 화면에서는 로그인 관련 정보만 표시한다. 조직이나 운영체제, 네트워크 환경, 내부적인 사항과 같은 정보는 로그인이 성공적으로 이루어진 후에 표시되도록 한다.
- ✓ 연속적 3회 이상 패스워드 오류 발생에 대하여 로그내역을 검토한다.
- ✓ 업무상 접속할 필요가 있는 중요 통신 장비는 사용자의 IP를 파악한 후 IP주소 기반의 접근 통제를 한다.

(나) 백업업무 담당자는 비인가자의 불법적인 접근 및 서비스 중지 등을 예방하기 위해 보안설정을 강화하고 업무적으로 불필요하거나, 침해의 위험이 있는 서비스를 제한할 수 있다.

3) 백업망과 인터넷망 분리 시 고려사항

(가) 기업 내 임직원과 IT인프라를 운영하는 사용자(시스템 담당자, DB/백업 담당자 등)에 대하여 업무망은 분리되어야 한다.

(나) 기업에 중요 데이터를 저장 관리하는 전산 시설 및 주요 IT인프라에 대하여 외부 인터넷과 격리된 영역에 구성해야 한다.

(다) 일반 임직원이 접근이 통제된 네트워크에 접속을 차단해야하며, 내부 망에서 사용자가 외부 인터넷을 사용하는 행위를 통제해야 한다.

(라) 기업의 사내 네트워크에 대하여 내·외부 망으로 분리는 가상화 솔루션을 사용하여 논리적으로 망을 분리하거나 물리적으로 네트워크를 분리하여 접근통제를 구성할 수 있다.

(마) 무선 네트워크에 대하여 주요시설 사용을 금지해야한다.

(바) 그러나 중소기업의 경우 구성비용 등의 이슈로 구성이 어려운 경우 네트워크 스위치 또는 대상 기업에 적합한 방화벽 등을 사용하여 접근제어 정책으로도 최소한의 네트워크 분리가 가능하므로 가능하면 인터넷망과 내부 시스템 망은 분리해야 할 것이다.

4) 백업 시스템 네트워크 분리 시 접근통제 방식

백업시스템 보호를 위한 네트워크 분리방안으로 망분리 시 자료 전송 연계 기법 사용과 방화벽 사용을 통해 분리하여 구성할 수 있다.

항목	스토리지 방식	방화벽 방식
특징	• 내/외부 망연계 서버 사이에 스토리지를 이용하여 데이터를 중계하는 방식	• 내/외부 망연계 서버 사이에 방화벽을 두고 제어하는 방식
전송 매체	• FC케이블을 이용한 방식 • 스토리지 내 파일시스템의 Read / Write만 허용	• 방화벽에 백업시스템 네트워크 영역을 구성하는 방식 • 백업 담당자만 접근허용(IP통제) • 백업시스템과 스토리지간 통신시 일방향 통신만 가능하도록 허용
보안성	• 보안 정책설정 외에 기타 설정은 불필요 • 외부망 연계서버 해킹 시에도 내부 방으로 진입 불가	• 포트스캔을 통해 방화벽 존재유무 파악 가능 • 일방향 통신으로 정보 유출 및 침입 불가
유지 관리	• 보안정책 및 필수 항목 외에 지속적 유지보수 필요는 없음	• 취약점 발견시 마다 업데이트 필수, 지속적 유지관리 필요
기타	• 악성코드 및 웜 감염 방지를 위한 별도 백업 정책 필요 • 백업 수행 시 기존 데이터에 대하여 읽기전용 설정 필요	• 악성코드 및 웜 감염 방지를 위한 별도 백업정책 필요 • 필요에 따라 웹방화벽 등 보호시스템 추가구성 필요 • 백업 수행 시 기존 데이터에 대하여 읽기전용 설정 필요

[표 13] 백업망 분리 구성 방안

다. 소프트웨어 보안

백업 소프트웨어 도입에 앞서 백업 솔루션에 대한 기능 및 보안성을 점검 후 백업 소프트웨어를 도입해야 한다.

다음은 백업 소프트웨어 도입 및 운영시 검토해야할 점검항목이다.

NO	검토항목	비고
1	백업 데이터에 대한 보호	데이터 보호는 새로운 백업 솔루션의 도입을 주도한 기능 중 하나다. CDP 기능은 서버에 미치는 영향을 최소화 해준다. 스케쥴링 매커니즘을 지원하는 백업복구 솔루션을 선택
2	신속한 복구 시간 목표(RTO)와 복구 시점 목표(RPO) 달성	재해가 발생했을 때 가장 신속하게 복구시점목표(RPO: Recovery Point Objective)와 복구시간목표(RTO: Recovery Time Objective)를 달성할 수 있어야 함
3	타 백업 소프트웨어와 호환 여부	솔루션 도입시 타 벤더 소프트웨어와 적절한 연동 가능여부를 확인해야 함
4	불필요한 서비스 또는 프로그램 제거	백업 서비스와 관계없는 서비스에 대하여 삭제하여 외부 위협요소를 최소화해야 함
5	설치와 사용이 용이	너무 많은 옵션이 있는 가상화 백업 솔루션은 관리상의 불편함을 가져온다. 몇 번의 클릭만으로 백업 솔루션을 어플라이언스로 배포할 수 있는 기능이 필요
6	백업의 유효성과 보안 기능을 확인	백업 솔루션에는 자동 백업 유효성 검사 기능이 반드시 포함되어야 한다. 이것은 백업을 성공적으로 완료시킨 후에도 혹시 모를 복원 실패를 대비한 안전장치 역할을 함
7	백업 스토리지 옵션의 유연성을 점검	LAN-free SAN 백업은 백업 시간을 줄여주며 네트워크의 전체 부하를 감소 시켜준다. 이런 유연성은 클라우드 기반 백업과 스토리지 유연성을 위한 필수 조건
8	스토리지의 효율적 사용을 위해 중복 제거 기능 제공 여부를 확인	데이터 중복 제거 기능은 비용을 줄이고 스토리지를 효율적으로 사용하고 싶다면 중복 제거 기능을 백업 솔루션의 필수 조건
9	가상화 및 물리적 시스템으로의 원활한 마이그레이션 지원 여부를 확인	가상 서버 백업 솔루션에서 실제 서버를 가상 인프라로 편리하게 이전시키는 기능을 제공
10	백업복구 시스템 도입과 관리 측면에서 비용 효율성을 점검	고도로 통합된 인프라 구조에서만 비즈니스는 최상의 ROI를 얻을 수 있으며 사용량당 라이센스 비용을 요구하는 솔루션은 지속적인 비용발생의 요소를 확인해야 함

[표 14] 백업 소프트웨어 구성시 고려사항

라. 운영자 교육

구축 및 테스트가 완료된 백업시스템을 운영조직으로 이관하기 위한 운영자 교육이 필요하다. 운영자 교육은 구축된 백업시스템에 대한 이해도를 높이고 운영능력 향상 및 체계적인 보안유지를 목적으로 연 1회 이상 교육해야 한다.

▷ 운영자 교육
- 교육 유형 : 전문 교육(DB 및 백업 시스템 관련)
- 교육 회수 : 연간 1회
- 교육 내용 : 백업 담당자 및 운영자에 대하여 주기적인 DB 및 백업시스템에 대한 최신 기술 및 심화교육

▷ 정보보호 교육
- 교육 유형 : 정보보호 인식 교육
- 교육 회수 : 연간 1회
- 교육 내용 : 기업 내 정보보호 강화를 위한 인식 교육 등

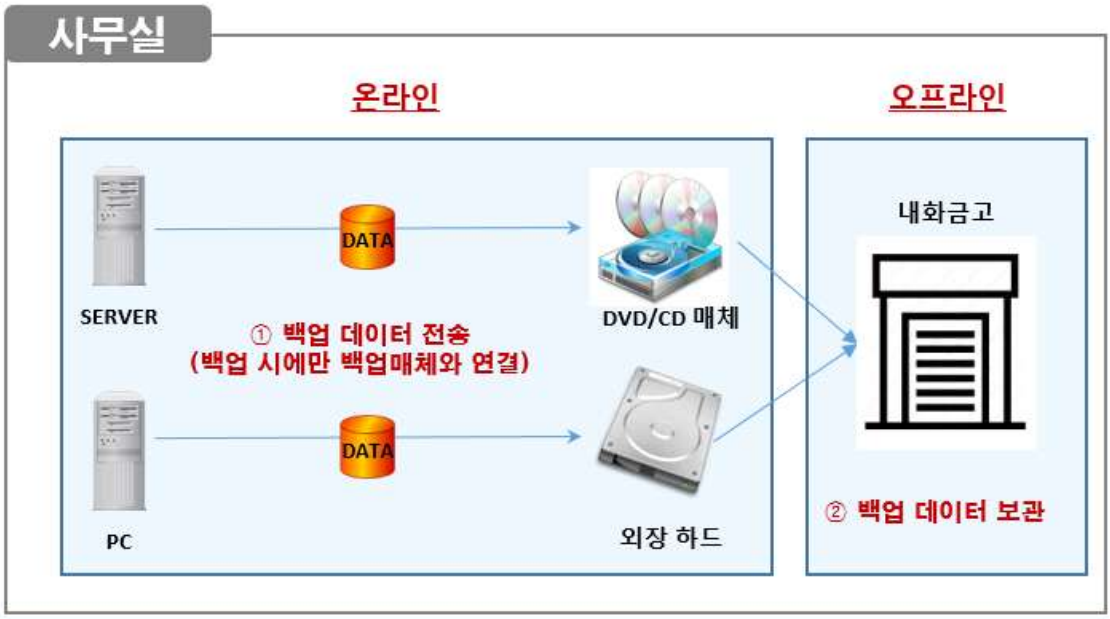
1) 운영 매뉴얼 작성

운영 매뉴얼은 시스템운영자가 언제든 매뉴얼을 사용하여 시스템을 구동할 수 있도록 절차화 되어 작성되어야 하고, 연 1회 최신성을 검토하여야 한다.

(가) 운영이관을 위해서는 운영자 교육과 함께 운영 매뉴얼이 반드시 제공되어야 한다.
(나) 운영 매뉴얼에는 백업시스템 구성현황, 백업스케줄 현황 등이 명시되어야 한다.
(다) 백업 정책 등 운영에 필요한 기본 지침이 마련되어야 한다.
(라) 운영 매뉴얼에는 백업 수행자가 백업을 원활히 수행할 수 있도록, 각 시스템별 가동 및 정지 절차가 상세하게 기술되어야 한다.

9. 붙임. 백업 시스템 구성도

< DVD/외장하드를 이용한 수동 백업 구성도>

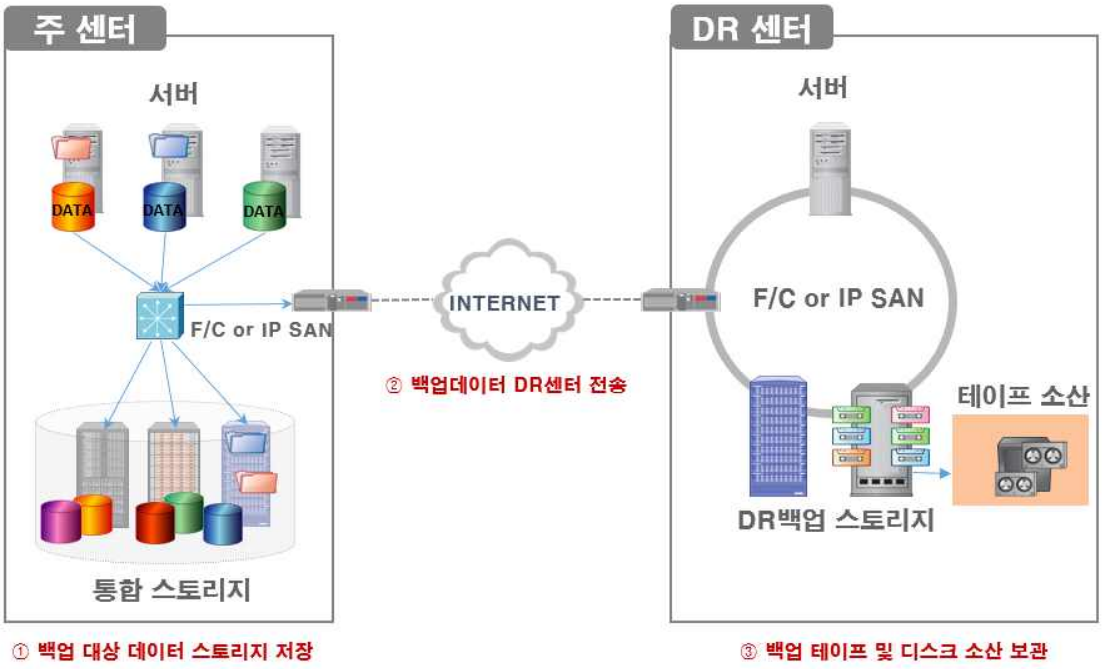


① 서버 및 PC 등 백업 대상 데이터의 무결성을 확인한 후 DVD/CD 매체, 외장하드 등에 전송
② 백업 데이터를 보호하기 위해 내화 금고 등 안전한 장소에 보관
③ 개인 PC 및 소규모 서버를 운영하는 기업에 적합

< 백업 서버를 이용한 자동 백업 구성도>

① 백업 에이전트에서 백업 대상 데이터를 정해진 정책에 따라 백업 마스터 서버로 전송
② 백업 데이터가 랜섬웨어 등에 오염되었는지 확인
③ 백업 데이터를 보호하기 위해 백업 마스터 서버에서 테이프 라이브러리로 소산하여 오프라인 관리
④ 다수의 서버 및 PC의 시스템을 운영하는 중소기업에 적합

< 재해복구(DR) 센터를 이용한 백업 구성도>



① 정해진 백업 정책을 참조하여 백업 대상 데이터를 주 IDC 센터의 통합 스토리지에 저장
② 백업 데이터를 물리적으로 독립된 재해복구(DR) 센터의 백업 스토리지로 전송
③ DR 백업 스토리지에 저장된 백업 데이터를 테이프 또는 디스크 등의 매체를 이용하여 소산
④ 대규모 서버 및 예산이 충분한 중견 기업 이상에 적합

10. 별지. 백업관리 양식

[별지.1] 백업관리대장

백업관리대장

대상	백업매체 (매체 ID)	백업스케줄	경과 시간	백업 보관주기	업무 담당자	확인

[별지.2] 소산관리대장

소산관리대장

No.	소산일자	백업매체 (매체 ID)	보관장소	보존기간	이상 유무	업무 담당자	확인

[별지.3] 테이프관리대장

테이프관리대장

작업일자	테이프 명	시리얼번호	용도	업무담당자	확인

[별지.4] 백업매체관리대장

백업매체관리대장

시스템 명 :
작업일자 :
작업자 명 :

매체-ID	구입 일자	용 도	사용 주기	내 용	보관 장소	담당자	폐기 일자

[별지.5] 백업매체 반입/출 관리대장

백업매체 반입/출 관리대장

일시	매체ID	요청자	반입/출 사유	수량	반입/출 처	반입자	재반출 여부	확인

[별지.6] 인수인계서

인수인계서

결재	기안	심사	승인
	/	/	/

위와 같이 인수인계 하였음을 확인합니다.

1.인수인계 사유

2.인수인계 내역

번호	인수인계 내역	인수	비고

1. 특이사항
-

위와 같이 인수인계 하였음을 확인합니다.

년 월 일

인계자: (인)

인수자: (인)

ABC 주식회사 귀중

[별지.7] 백업 신청서

백업·소산 신청서

신 청 부 서	
담당	검토

1. 일반 사항

신청일자					
신청자 성명		**전 화**		**부서명**	

2. 백업 정보

구 분	**내 용**			
서 버 명(IP주소 명기)				
백업/소산 대상 (해당항목 'Y')	**OS ( ) 데이터베이스 ( ) 사용자 일반파일 ( ) 기타 ( )**			
백업 주기 (해당항목 'Y')	**일간 ( ) 주간 ( ) 월간 ( ) 연간 ( ) 수시 ( )**			
백업/소산 본 보관기간				
백업/소산 대상 위치				
백업/소산 전체 용량				
희망시간	**시작시간**		**완료시간**	
소산보관 위치				

※ 신청서 접수정보

접수일시		**접수자 성명**	
백업/소산 적용일자			
백업/소산 장치		**백업 소프트웨어**	
특기사항	※ 백업적용 후 신청자에게 회신할 것		

※ 검토란은 승인자의 성명을 기입하여 결재가 가능함.

[별지.8] 복구 신청서

복구 신청서

신 청 부 서	
담당	검토

1. 일반 사항

신청일자					
신청자 성명		**전 화**		**부서명**	

2. 복구 정보

구 분	**내 용**
서 버 명	
복구 목적	
복구 파일명	
전체 파일크기	
대상파일 백업일자	
※ 복구 불가시 대체백업일자	
복구 위치	
복구 완료 희망시간	
특기사항	

※ 작업 완료정보

접수일시			
작업자성명		**작업소요시간**	
복구 결과			

※ 검토란은 승인자의 성명을 기입하여 결재가 가능함.

[별지.9] 백업 변경 작업 내역서

백업 변경 작업내역서

작업 일시		작업자	
대상 시스템			
작업 형태	장애처리 ( ) 백업정책 변경 ( ) 설치 및 업그레이드 ( ) 기타 ( )		

문제점 / 요청사항

작업 내용

작업 시간			작업자 확인	
시작시간	종료시간	경과시간	이름	서명