

정보시스템 긴급 재난복구 절차서

2020. 6.

정보시스템 긴급 재난복구 절차서

제1장 총칙

제1조 (목적) 이 절차서는 KEI 정보시스템 긴급재난복구에 관한 기준을 정함을 목적으로 한다.

제2조 (적용범위) 적용범위는 다음 각 호와 같다.

1. 서버시스템의 재난복구
2. 네트워크 시스템의 재난복구
3. 데이터, 어플리케이션 등 정보서비스 재난복구

제2장 서버시스템의 재난복구

제3조 (시스템SW백업) ①시스템SW 장애를 대비하기 위해 시스템SW 백업을 실시하여 물리적 접근통제와 화재 등의 위험 요소로부터 보호되는 장소에 보관한다.

②시스템SW백업은 다음 각 호에 따라 실시한다.

1. 백업대상 : 정보서비스를 제공하는 서버로 전자결재시스템, 행정정보시스템, DBMS 시스템, e-mail 시스템 등 주요 정보시스템의 시스템 파티션을 파일단위로 전체 백업한다.
2. 백업주기 : 매주 1회 전체 백업 및 매일 증분 백업을 실시한다.
3. 백업방법 : 백업시스템(VTL기반 - VERITAS NETBACKUP)을 이용하여 1차 백업 후 Tape 드라이브를 이용하여 2차 백업을 실시한다.

제4조(하드웨어 백업) 유지보수 계약을 통해 장애발생 가능성이 있는 파트에 대한 예비 부품을 확보한다.

제5조(시스템SW복구) ①전산서버실과 독립된 별도의 통제된 안전한 공간에 보관된 백업 데이터를 사용하여 복구한다.

②시스템SW 복구는 다음 각 호의 순으로 실시한다.

1. 시스템SW 장애가 발생한 서버의 시스템SW를 재설치 한다.
2. VTL 백업시스템에 백업된 데이터를 이용하여 시스템SW 파일을 재설치한 서버에 복구(recovery)한다.
3. 복구가 완료되면 시스템의 이상 유무를 확인한 후 서비스를 구동한다.

제6조(하드웨어 복구) 서버 시스템의 하드웨어 장애가 발생했을 경우 유지보수 계약업체는 대체 하드웨어를 조달하여 신속히 교체 복구한다.

제3장 네트워크 시스템의 재난복구

제7조(소프트웨어 백업) ①백업 대상은 인터넷 라우터, 백본 스위치, 방화벽, 웹방화벽 IPS, UTM, DDoS시스템 및 네트워크를 위한 L2 ~ L4 스위치의 설정파일로 한다.

①정보시스템 유지보수 시 정기백업(월/분기), 설정 변경 시 (수시백업) 실시한다.

②tftp를 통한 백업 또는 자체파일 내려받기를 이용하여 백업한다.

③전산서버실에 위치한 별도의 파일서버에 보관한다.

제8조(하드웨어 백업) 유지보수 계약을 통해 장애발생 가능성이 있는 파트에 대한 예비 부품을 확보한다.

제9조(소프트웨어 복구) 서버실 파일서버에 백업된 파일을 사용하여 복구하며, 복구절차는 다음 각 호와 같다.

1. 펌웨어 장애 발생 시스템을 대체 장비로 교체한다.
(설정 또는 정책파일만 장애시 생략한다.)
2. 백업 받아 두었던 설정파일을 준비한다.
2. 시스템에 적용하고 재부팅 한다.
3. 부팅 후 백업된 설정파일을 적용하여 시스템의 설정을 복구한다.
4. 복구가 완료되면 시스템의 이상 유무를 확인 및 통신상태를 점검한다.
5. 펌웨어 장애 발생 시스템의 펌웨어 작업은 각 유지보수 업체에서 별도로 실시한다.
6. 펌웨어 작업이 완료된 시스템에 설정파일을 적용한다.
7. 설정파일이 적용된 시스템을 테스트한다.
8. 테스트가 완료된 시스템을 대체장비와 서로 교체한다.
9. 장비 장애시점 전과 후를 비교하며, 정상 유무를 판단한다.

제10조(하드웨어 복구) 네트워크 시스템의 하드웨어 장애가 발생했을 경우 유지보수 계약에 의거 계약업체의 대체 하드웨어를 조달하여 신속히 교체 복구한다.

제11조(복구 우선순위) 재난에 의거 다수 지역에서 장애가 동시 발생했을 경우는 다음 각 호의 순에 의거 복구를 시행한다.

1. 인터넷 관문
2. 백본 L2스위치
3. 네트워크 연결을 위한 L2/L3/L4 스위치

제4장 데이터, 어플리케이션 등 정보서비스 재난 복구

제12조(백업시스템을 이용한 백업) ①각 주요서버에 대해서 일별 Online 백업, 월별 소산백업을 진행한다.

②중요데이터, 어플리케이션 등 정보서비스는 백업시스템을 이용하여 다음 각 호와 같이 일별 Online 백업을 실시한다.

1. 백업대상은 정보서비스를 제공하는 서버로 별표1과 같으며, 대상은 변경될 수 있다.
2. 백업방법은 백업시스템의 운영환경 및 백업 대상장치 및 백업용량에 따라 설정된 백업 정책에 의해 일별 증분백업 및 주별 일괄백업을 수행한다.
3. 백업주기는 별표1과 같다.

③월1회 주기로 백업시스템을 이용하여 백업된 데이터들에 대해서 다음 각 호와 같이 소산 백업을 실시한다.

1. 백업 대상 데이터는 백업시스템에 보관중인 모든 백업데이터로 한다.
2. 소산 백업방법은 백업시스템의 백업 데이터복사기능을 이용하여 소산용 Tape 드라이브의 미디어에 백업데이터 복사한다.
3. 백업 데이터를 재 백업(이중 백업)한 Tape 드라이브의 미디어는 독립된 별도의 통제된 안전한 공간에 보관한다.

④소산 백업한 백업데이터 복사본은 전산서버실과 백업서버실에 격월로 보관하며 다음 각 호와 같이 처리한다.

- 1.보관방법은 전산서버실과 백업서버실에 이중 보관한다.
- 2.보관주기는 1개월로 한다.

제13조 (재난·재해 시 백업시스템을 이용한 복구)

- ①백업시스템(VERITAS NETBACKUP) 솔루션은 데이터 복사가 가능한 솔루션으로 데이터를 독립된 별도의 통제된 안전한 공간에 독립된 Tape 드라이브에 이중 복사하여 보관한다.
- ②백업대상서버는 전자결재시스템, 행정정보시스템, DBMS 시스템, e-mail 시스템, KEI 대표 홈페이지 등 KEI에서 운영하고 있는 정보시스템 서버들이다.
- ③백업대상파일은 별표1과 같다.
- ④백업방법은 전산서버실과 백업서버실 스케줄에 의한 데이터를 복사 및 보관한다.

제14조(사용자실수에 의한 데이터 손실복구) 백업시스템에 의해 백업된 데이터를 사용하여 다음 각 호와 같이 복구를 실시한다.

1. 주기적인 백업을 수행한 백업 데이터를 이용하여 데이터 복구를 수행한다.
2. 데이터가 소실된 대상 서버에서 백업시스템 복구명령 또는 GUI 매니저를 이용하여 손실된 데이터(파일 또는 파일 시스템)를 복구한다.
3. 복구된 데이터에 대한 정합성 및 활용성 테스트를 진행한다.

제15조(재난에 의한 데이터 손실 복구) ①백업시스템과 Tape 드라이브에 저장된 백업데이터를 사용하여 복구한다.

- ②시스템 하드웨어와 데이터의 완전 파손 시 백업시스템에 백업된 데이터를 사용하여 다음의 순서로 복구를 진행한다.
 1. 유지보수 계약업체를 통해 파손된 하드웨어의 대체 하드웨어를 신속하게 준비한다.
 2. 시스템 OS 복구는 서버 시스템의 재난복구계획을 참조한다.
 3. 데이터, 어플리케이션의 복구는 준비된 시스템에 백업시스템을 사용하여 백업데이터를 순서에 따라 복구한다.
 4. 데이터 복구 완료 시 해당 시스템에 대한 어플리케이션 서비스를 재개한다.

부 칙

- ①(시행일) 이 절차서는 2014년 4월 18일부터 시행한다.

부 칙

- ①(시행일) 이 절차서는 2017년 12월부터 시행한다.