

Chapter

5

응급 복구 디스크

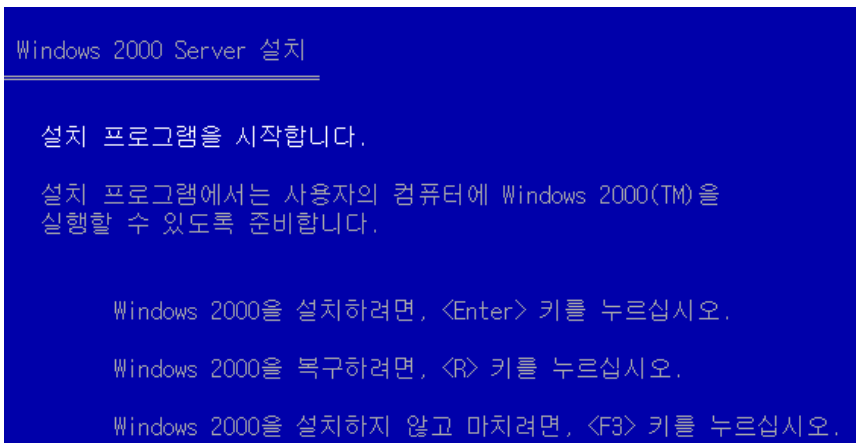
응급 복구 디스크는 레지스터리의 복원을 도와 주는 좋은 유틸리티 중에 하나이다. 기본적으로 제공되는 수동 모드 및 빠른 모드를 잘 이해하고 있다면 응급 복구 디스크를 훌륭한 복원 도구로 활용할 수 있을 것이다.

5. 응급 복구 디스크

1. 응급 복구 디스크 개요

응급 복구 디스크는 아주 곤란한 문제를 잘 해결해 줄 수 있는 유용한 도구 중의 하나이다. 많은 경우 응급 복구 디스크 자체보다 레지스터리의 백업 본을 제작하고 관리하는 것이 더 중요할 수 있다.

윈도우 2000에서 응급 복구 디스크(ERD 이하 응급 복구 디스크)의 활용은 기존 윈도우 NT 4.0과 다소 차이점이 있다. 일단 제작 방법이 다르며, 저장되는 내용 역시 조금 다르다. 물론 용도는 거의 비슷하다.



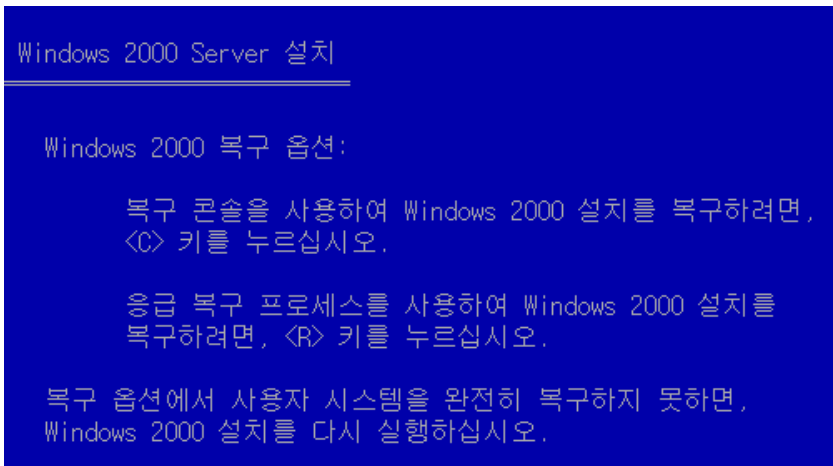
[그림 5-1] 윈도우 2000 부팅 CDRom으로 부팅한 경우 설치 혹은 복구 선택 옵션

윈도우 NT 4.0에서도 그러하였지만, 윈도우 2000 역시 응급 복구 디스크로 부팅이 되는 것이 아니라, 윈도우 2000 원본 CD 혹은 부팅 디스크(다른 말로 설치 디스크 4

장짜리)와 같이 사용하여야 한다. 윈도우 2000 CD으로 부팅하여 복구 작업을 수행하려면 위의 그림에서 제시된 화면에서 “R”을 선택하면 된다.

응급 복구 디스크의 설치 방법과 그 용도를 설명하도록 하겠다. 응급 복구 디스크는 레지스터리 백업 분이 직접 들어 있지 않으며, 다음과 같은 기능만을 제공한다.

- 시작 환경의 검사와 복구
- 윈도우 2000 파일의 조회 및 손상되거나 없어진 파일 대체 정보
- 부트 섹터의 검사와 복구



[그림 5-2] 복구 옵션 메뉴- 복구콘솔과 응급 복구 디스크 선택 메뉴



윈도우 2000에서 응급 복구 디스크를 제작할 때, 레지스터리 복원은 옵션에 속한다. 만들 때 레지스터리를 따로 백업해야 된다.

2. 응급복구 디스크 만드는 방법 및 사용 방법

응급복구 디스크 만드는 방법과 사용 방법은 몇 가지 기준만 준수하면 큰 어려움 없이 진행 할 수 있다. 특별한 기술이 필요한 것이 아니라 시간이 날 때 미리 작업을 해 둔다면 필요할 때 얼마든지 사용할 수 있다. 하지만 응급 복구 디스크를 꼭 사용할 필요가 있는 경우를 제외하면 복구 콘솔을 사용할 것을 권한다.

응급 복구 디스크 만드는 방법

윈도우 2000 백업(ntbackup.exe) 프로그램을 실행하면 기능 중의 하나가 응급 복구 디스크를 만드는 것이다. 윈도우 NT 4.0에서는 커맨드에서 “rdisk” 명령어로 응급 복구 디스크를 제작하였으며, 백업 내용 역시 다소간의 차이가 있다.

윈도우 NT 4.0에서 응급 복구 디스크는 레지스터리 백업의 일부로 간주되었으며, 상당히 많은 정보를 백업할 수 있었기 때문에 복구에 유용한 도구로 사용되었다.(표 5-1 참조)

파일 이름	내용
Autoexec.nt	%systemroot%\system32\autoexec.nt 파일의 복사본 MS-DOS 창을 열었을 때 초기화 파일로 사용된다.
config.nt	%systemroot%\system32\config.nt 파일의 복사본 MS-DOS 창을 열었을 때 초기화 파일로 사용된다.
Default._	HKEY_USERS\DEFAULT 레지스터리 키가 압축된 파일.
Ntuser.DA_	%systemroot%\Profiles\Default User\Ntuser.dat. 의 압축된 버전
Sam._	HKEY_LOCAL_MACHINE\SAM 레지스터리 키가 압축된 파일. 사용자 계정정보와 보안 관련 내용이 삽입되어 있다.
Security._	HKEY_LOCAL_MACHINE\SECURITY 레지스터리 키가 압축된 파일.
Setup.log	설치된 파일에 대한 로그. 복구 중 사용할 CRC 정보를 가지고 있다.
Software._	HKEY_LOCAL_MACHINE\SOFTWARE 레지스터리 키가 압축된 파일.
System._	HKEY_LOCAL_MACHINE\SYSTEM 레지스터리 키가 압축된 파일.

[표 5-1] 윈도우 NT 4.0 응급복구 디스크 제공되는 파일 및 역할 정보

그러나, 윈도우 2000에서는 윈도우 NT 4.0와는 달리 레지스터리 파일 일부만을 백업하며, 나머지 파일의 백업을 위해서는 추가 옵션이 필요하다.

윈도우 2000의 응급 복구 디스크에 삽입되는 파일은 아래와 같다.

- autoexec.nt
- config.nt
- setup.log

setup.log 파일은 컴퓨터에 설치된 파일 정보를 갖고 있으며, 손상되거나 삭제된 파일을 윈도우 2000 원본 CDROM으로부터 복구할 수 있도록 해 준다. 윈도우 2000에서는 autoexec.nt, config.nt 파일은 사용되고 있지 않다.



현재 운영되고 있는 시스템에 윈도우 2000 운영 체제가 언제 설치되었는지 알고자 한다면 “%systemroot%\Wrepair” 폴더의 파일 날짜를 참고하면 된다. (초기 설치 시 값임)

이름	크기	종류	수정된 날짜
autoexec.nt	1KB	NT 파일	2000-01-10 오후 9:00
config.nt	3KB	NT 파일	2002-06-26 오전 9:51
default	120KB	파일	2002-06-26 오전 9:57
ntuser.dat	120KB	DAT 파일	2002-06-26 오전 9:51
sam	20KB	파일	2002-06-26 오전 9:58
secsetup.inf	573KB	설치 정보	2002-06-26 오전 9:52
security	28KB	파일	2002-06-26 오전 9:58
setup.log	156KB	텍스트 문서	2002-06-26 오전 9:51
software	6,368KB	파일	2002-06-26 오전 9:57
system	1,072KB	파일	2002-06-26 오전 9:57

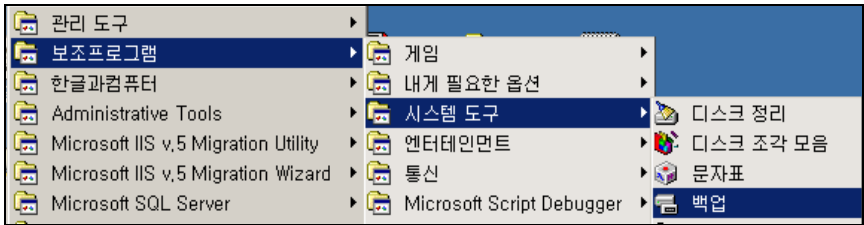
[그림 5-3] %systemroot%\Wrepair 폴더 내용

응급 복구 디스크는 다음과 같은 순서로 제작한다.

1. 실행에서 ntbakup.exe을 실행 한다.

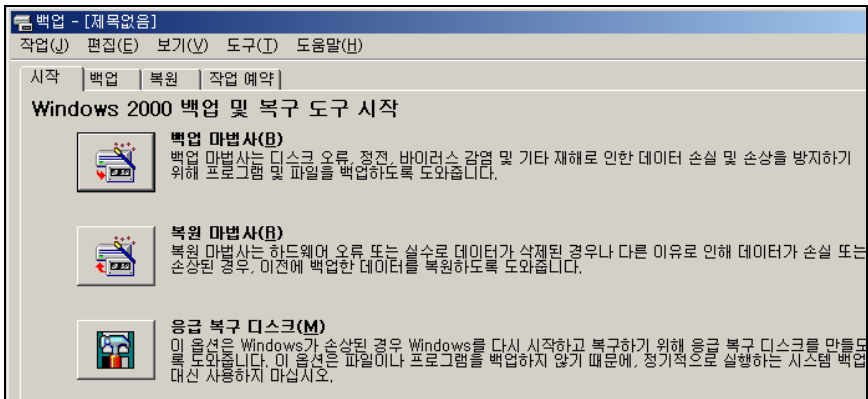
(보조 프로그램/시스템 도구에서도 가능함)

또한 명령 프롬프트에서 ntbakup.exe라고 실행 해도 작업이 가능하다.



[그림 5-4] 백업 실행

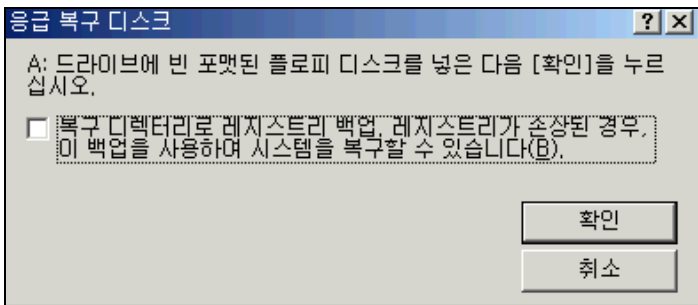
2. 백업 프로그램 실행 화면에서 응급 복구 디스크를 선택한다.



[그림 5-5] 윈도우 2000 백업 프로그램

3. 응급 복구 디스크 아이콘을 클릭한 뒤 플로피 디스크를 삽입하면 된다. 진행하기 전 다음과 같은 메시지가 출력되며 이 메시지를 주목하자.

“ 복구 디렉터리로 레지스터리 백업, 레지스터리가 손상된 경우, 이 백업을 사용하여 시스템을 복구 할 수 있습니다.”



[그림 5-6] 레지스터리 백업 옵션

이 메시지 체크 박스를 선택하지 않으면 레지스터리는 백업되지 않는다.
(%systemroot%\repair\regback\.* 레지스터리가 백업됨)



응급 복구 디스크 옵션 중, 레지스터리를 백업하는 옵션에서, “%systemroot%\repair” 폴더와 그 하위 폴더를 선택한다. 물론, 레지스터리 백업 옵션을 주지 않았다면 이 옵션을 선택할 수 없다. 레지스터리 초기값은 %systemroot%\repair 폴더에 보관된다. 또한 레지스터리를 백업하면 해당 폴더에 백업 폴더가 추가되는 것을 알 수 있다. (%systemroot%\repair\regback)

4. 플로피 디스크에는 빈 디스크를 삽입하여야 하며, 다음 세 파일이 기록되는 것을 알 수 있다. (autoexec.nt, config.nt, setup.log)

이 과정이 끝나면 레지스터리 파일이 백업되며, 윈도우 NT의 응급 복구 디스크와의 차이점은, 레지스터리 파일이 플로피 디스크에 저장되는지 여부이며, 윈도우 2000은 NT와는 달리 하드 디스크에 레지스터리 백업 본을 저장하게 된다.

실제로 윈도우 2000의 레지스터리 백업 본의 크기는 NT에 비해 훨씬 크며, 백업된 폴더에서 실제 어느 정도의 용량을 갖고 있는지 확인해 보기 바란다.

%systemroot%\system32\config\ 폴더와 그 하위 폴더의 용량을 조사해 보면 된다.

다음은, 윈도우 NT와 윈도우 2000의 응급 복구 디스크 구성의 차이점을 나열해 본 것이다. 약간의 차이점을 제외하고는 거의 유사한 것을 볼 수 있다.

기능	윈도우 NT	윈도우 2000
보안적인 측면	낮음 (SAM 데이터 베이스 유출 우려)	높음 (SAM 데이터 베이스를 포함 되지 않음)
레지스터리 복구	포함	포함 되지 않음(옵션부분)

응급복구 디스크 만드는 방법	커맨드에서 RDISK	NTBACKUP으로 실행
레지스터리 용량(크기)	디스크에 포함 될 수 있도록 크기가 작다.	용량이 최소 15MB 정도가 됨

[표 5-2] 윈도우 NT 와 윈도우 2000 응급 복구 디스크 구성의 차이

응급 복구 디스크의 내용은 실제 시스템 내에 존재하고 있는 복구 디렉터리 (%systemroot%\repair)와 크게 다르지 않다. 즉, 응급 복구 디스크의 내용은 실제 복구 디렉터리에 저장된 내용이 다시 플로피 디스크로 복사된 것으로 보면 된다. 해당 디렉터리의 위와 같은 파일(autoexec.nt, config.nt, setup.log)의 내용을 비교해 보면 된다. 따라서, 응급 복구 디스크를 만들지 않았다고 할지라도, 이 파일을 복사하여 사용할 수도 있는 셈이며, 레지스터리 파일만을 백업할 방안을 마련해 놓으면 된다.

만일, 응급 복구 디스크를 분실한 경우 언급한 3개의 파일을 %systemroot%\repair 폴더에서 플로피 디스크로 복사하고, 레지스터리 파일을 레지스터리 백업 폴더 (%systemroot%\repair\regback)에 복사한다면 응급 복구 디스크를 만든 것과 동일한 효과를 낼 수 있으며, 비슷한 내용이 MS 기술 문서에서도 제공된다.

참고 문헌 “Differences Between Manual and Fast Repair in Windows” 을 참고하면 좋은 정보를 얻을 수 있다.



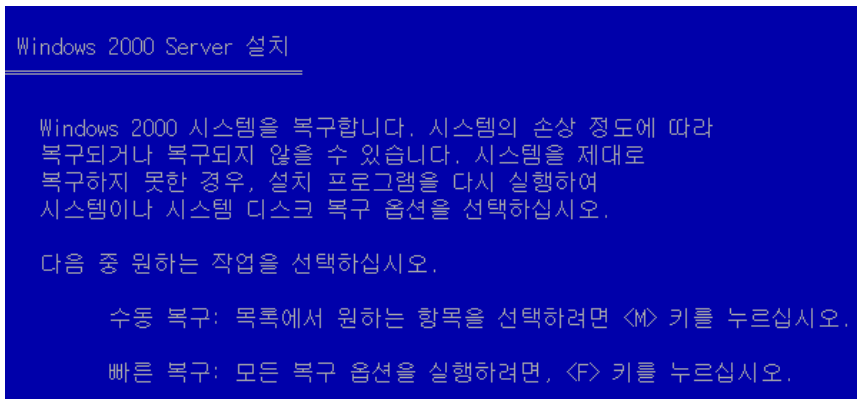
응급 복구 디스크를 수동으로 제작하는 방법은 비교적 간단하다. 응급 복구 디스크에서 제공되는 3개의 파일 (autoexec.nt, config.nt, setup.log 3개의 파일)은 윈도우 2000의 %systemroot%\WrepairW 디렉터리에 존재하고 있으며, 이를 그대로 복사하면 된다. 이 작업만을 거치면 응급 복구 디스크는 제작이 된 셈이다. 추가로, 레지스터리 복원을 위해서는 %systemroot%\WrepairWregback 폴더를 생성하고, 최신 레지스터리 파일을 이 디렉터리에 삽입해 주면 된다. 단, 최신 레지스터리 파일은 갖고 있어야 한다.



플로피 디스크가 존재하지 않는 컴퓨터라면 응급 복구 디스크 작업 도 중 오류가 발생하며 더 이상 진행되지 않는다.

3. 응급복구 디스크 복원 방법

이제 윈도우 2000의 응급 복구 디스크를 사용하여 시스템을 복원하는 방법에 대해 설명하도록 하겠다. 응급 복구 디스크는 수동 모드 혹은 빠른 모드를 사용하여 복원이 가능하며, 각 기능은 문제 해결 방향의 차이가 있다.



[그림 5-7] 응급복구 프로세스 선택 화면

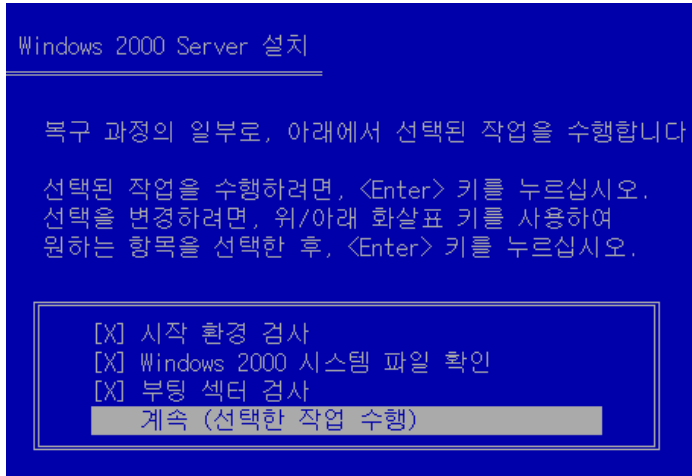
응급복구 디스크에는 레지스터리 파일이 포함 되어 있지 않으며 아래와 같은 기능만 제공한다. (레지스터리 파일은 운영 체제에 백업됨)

- 시작 환경의 검사와 복구
- 윈도우 2000 파일의 조회 및 손상되거나 없어진 파일 대체
- 부트 섹터의 검사와 복구
- 레지스터리에 대한 복원 부분은 응급 복구 디스크를 제작할 때 백업을 받아야 하며 그렇지 않을 경우는 복원을 할 수 없다.

(백업 폴더 위치는 %systemroot%\repair\regback 이다.)

수동 모드(Manual Repair)

수동 모드는 아래 그림과 5-8과 같은 모습으로 세 가지 사항에 대한 문제를 해결하도록 선택할 수 있게 해 준다. 선택한 부분만 복원되기 때문에 필요한 부분만 선택하면 된다.



[그림 5-8]응급 복구 디스크 수동 모드 화면

수동 모드로 선택할 수 있는 세 가지 작업은 다음과 같다.

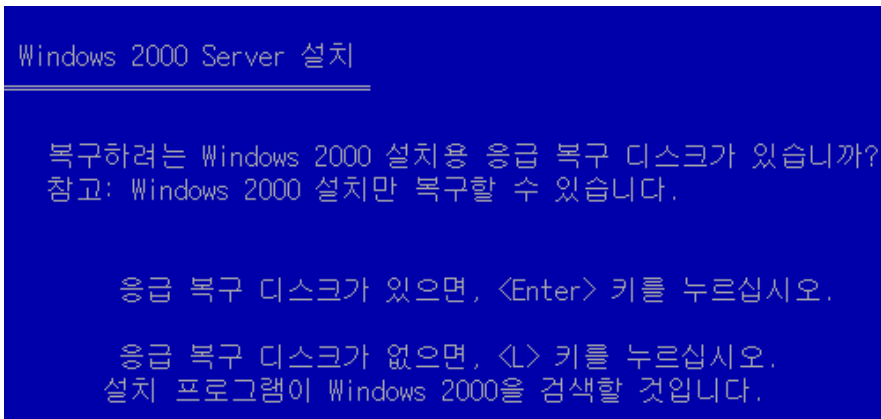
- 시작 환경 검사(Inspect startup environment) – 부팅 파티션과 시스템 파티션에 대한 문제 시 복원 작업을 한다. 일반적으로 Setup.log을 사용하여 복원 작업을 한다. boot.ini 에러 등을 복원 작업을 수행한다.
- 윈도우 2000 시스템 파일 확인(Verify Windows system files) – 부팅할 때 필요한 파일들에 대해서 검사한 뒤 수정한다. Ntldr, Ntdetect.com, Arcsetup.exe, Arcldr.exe, 또한 Ntbootdd.sys등의 파일이 문제가 되었을 때 복원에 사용되며, 윈도우 2000 원본 CD에서 파일을 복사하고 Setup.log 파일을 참조한다.
- 부팅 환경 검사(Inspect Boot Sector) – 일반적으로 부트 섹터 및 파티션 테이블 등을 복원할 수 있다. 또한, 윈도우 95/98등과 듀얼 부팅이 이루어질 경우 그에 필요한 여러 지원을 하게 된다. 듀얼 부팅일 경우에는 당연히 파일 시스템이 FAT 16/32 이어야 한다. (Bootsect.dos 와 Boot.ini 파일에 C:\="Microsoft Windows" 등과 같은 정보를 추가 한다.)

수동 모드로 복원하면 레지스터리 값의 복원은 이루어지지 않는다.

빠른 모드(Fast Repair)

빠른 모드는 수동 모드에서 사용된 모든 기능과 레지스터리 파일을 (SAM, SECURITY, SYSTEM, SOFTWARE 등) 복원한다. 레지스터리 파일이 손상되거나 읽히지 않을 경우 이 방법으로 수정하며 복원 폴더의 위치는 %systemroot%\Repair 이다.

빠른 모드에서는 응급 복구 디스크 유무를 질문 받게 되며, 응급 복구 디스크의 존재 유무에 따라 레지스터리 파일의 복원 방법에는 차이가 있다. 따라서, 응급 복구 디스크의 사용 여부를 잘 판단해 보아야 한다.



[그림 5-9] 응급 복구 디스크 유무 질문

복원할 레지스터리 파일은 SAM, SECURITY, SYSTEM, SOFTWARE 등이다.

- 응급 복구 디스크가 있다면 - %systemroot%\Repair\Regback 있는 레지스터리의 내용을 사용하여 복원 작업을 진행한다.
- 응급 복구 디스크가 없다면 - %systemroot%\Repair 있는 레지스터리의 내용을 사용하여 복원 작업을 진행한다.

%systemroot%\Repair 디렉터리는 시스템이 처음 설치될 때의 레지스터리 내용이 들어 있으므로, 만약 이 파일을 기준으로 복원하면 시스템 전체가 초기화되어 버린다.

%systemroot%\Repair\Regback는 응급복구 디스크를 작성하면서 생성한 가장 최신의 레지스터리 백업 본이다.

만일 응급 복구 디스크를 만들지 않았지만, 시스템 상태 백업 혹은 수동 레지스터리 백업을 사용하였다면 레지스터리 파일을 %systemroot%\Repair\Regback 디렉터리

로 복사한 뒤 응급 복구 디스크를 수동으로 생성해도 된다.

그 외 레지스터리에 대한 세부적인 복원과 관계된 내용은 “6장 레지스터리 이해와 활용”을 참고 하기를 바란다.

다음 제시되는 사례는 주로 윈도우 2000 CD으로부터 시스템이 복원될 때 나타나며, 간혹 응급 복구 디스크를 사용하더라도 받을 수 있는 문제이다. 이는 시스템에 있는 파일이 교체되면서 버전 충돌의 문제 등을 발생시키는 경우가 많다.

응급복구 디스크로 해결 할 수 있는 사항 및 문제점을 정리하면 다음과 같다.

- 응급복구 디스크는 시스템 시작과 관계되어 일어나는 문제를 쉽게 해결할 수 있다. 하지만, 엉뚱한 문제를 야기할 가능성도 있다는 것이 필자의 생각이다. 수동 모드로 작업을 하는 경우에도 물론 상당 부분의 복원을 수행할 수는 있지만, 레지스터리와 관계된 작업은 수행할 수 없다.
- 수동 모드로 복원을 하더라도 복원 후 많은 오류 메시지를 볼 수 있다. 이것은 서비스 팩 등을 설치하여 업그레이드 된 버전의 시스템 파일들을 원래 윈도우 2000 CD으로부터 복구한 까닭에 예전 버전으로 회귀한 까닭이다. 따라서, 최종적으로 서비스 팩을 재 설치해야 완벽한 복원이 이루어진다. 이 문제를 원천적으로 해결하는 방법으로는 윈도우가 현재 설치된 서비스 팩 내용을 담고 있는 CDROM을 제작하는 것이지만, 아직 이 CDROM 제작 방법은 공개되지 않았다. 또한, 파일 복구는 전체 파일을 모두 복구하고 난 뒤, 서비스 팩을 설치하여 버전을 맞추는 방법이 더 현실적이다.

손상된 부트 섹터, 손상된 MBR, 지워 졌거나 손상된 NTLDR과 ntdetect.com을 복구 하려고 한다. 이 경우 응급 복구 디스크를 사용할 수 있는가? 또한 바이러스에 감염된 시스템 디스크 역시 복구가 가능한가?

이러한 문제점은 일반적으로 응급 복구 디스크로 복원이 가능하다. 응급복구 디스크에서 복원 방법은 수동으로 작업하여 부팅과 관계된 파일만을 복구하면 작업이 쉽게 이루어진다. 따라서, 이런 문제들이 발생했을 경우 수동 모드로 들어가서 필요한 부분만을 선택하여 작업할 것을 권한다. 또한 복구 콘솔의 기능도 이러한 작업들을 가능하게 하므로, 여러 도구 중 적절한 도구를 선택하여 사용하면 된다. 그 외 블루 스크린으로 문제를 어렵게 만들어진다고 하여도 응급복구 디스크는 좋은 해결 방안을 만들어 줄 수 있다. 그럴 때는 응급복구 디스크에서 빠른 모드로 진행을 고려 해야 한다.

4. 응급복구 디스크를 자동으로 백업 하게 하는 방안

응급복구 디스크 작업을 자동으로 백업 받고자 하려면 윈도우 2000 리소스 키에 존재하는 Regback이라는 툴을 활용 한다면 아주 좋을 것이다. Regback 툴은 레지스터리를 백업 할 수 있는 툴을 말하며 운영 중 일 때도 동작을 하게 된다.

작업은 윈도우 2000 리소스 키 툴이 설치가 되어 있는 곳에서 커맨드에서 작업 해야만 하며, Regback.exe 툴만 있어도 가능하다.

1. Regback.exe있는 커맨드에서 아래와 같이 실행 한다.

사용 예 :

```
# regback -m \\home(컴퓨터 이름) c:\rdisk(저장할 디렉터리)
```

2. 아래 그림과 같이 작업 진행을 살펴 볼 수 있다.

(아래 그림 외 다른 것을 볼 수 있는데 그것 또한 받고자 한다면 수동으로 백업을 해야 된다는 것을 볼 수 있을 것이다. 실제적으로 레지스터리를 복원 시에는 아래와 같은 파일만 필요함

예: regback <filename you choose> users SID 처럼 해야 함)

```
C:\Rdisk>regback -m W\home c:\rdisk
saving SECURITY to c:\rdisk\SECURITY
saving SOFTWARE to c:\rdisk\software
saving SYSTEM to c:\rdisk\system
saving .DEFAULT to c:\rdisk\default
saving SAM to c:\rdisk\SAM
```

[그림 5-10] regback 커맨드에서 작업 화면

3. 아래와 같은 파일들이 백업이 될 것이다.

c:\rdisk 디렉터리를 살펴 보면 레지스터리가 백업 되어 있다.

이름 ▲	크기	종류
default	148KB	파일
SAM	28KB	파일
SECURITY	36KB	파일
software	18,200KB	파일
system	2,680KB	파일

[그림 5-11] regback으로 레지스터리 백업 받은 파일

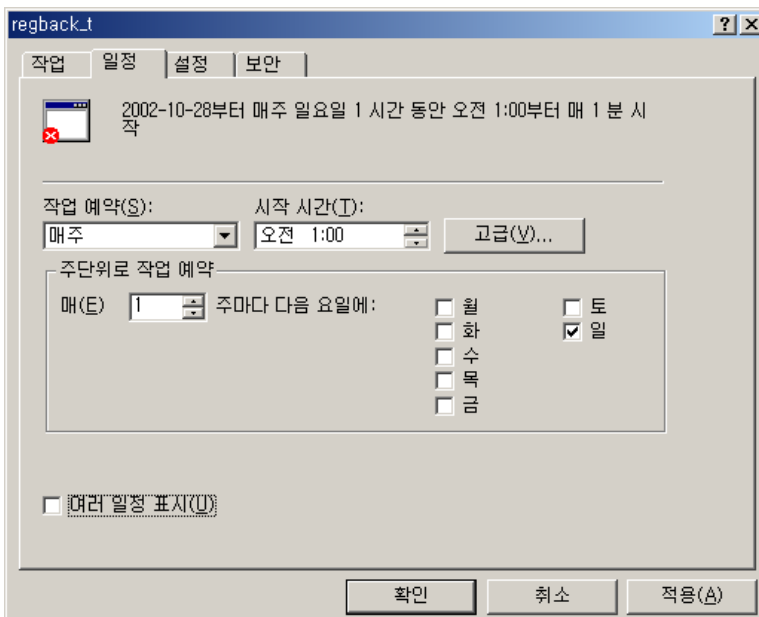
이러한 작업을 시스템 환경이 변경 시 마다 적용 하고자 하는 것은 번거롭다는 것을 알 수 있을 것이며 좀 더 편한 작업을 고려 한다면 아래와 같은 방법으로 적용 해 보기를 바란다.

Regback.bat 파일을 만들어서 아래 두 줄을 넣어서 스케줄 작업을 진행을 한다.

```
del c:\rdisk\*. * /q - 먼저 제공된 것을 지워야 regback 작업이 진행 됨
regback -m \\home c:\rdisk
```

위 작업에서 먼저 제공 된 것을 지운 후에 작업이 가능하다는 점 알고 있어야 하며, 이 작업을 날짜 별로 디렉터리를 만들어서 백업을 하고자 한다면 WSH등을 활용 하기를 바란다.

예약은 제어판에서 아래와 같이 작업 일정을 추가 해 주기를 바란다. 일정 주기는 관리자가 직접 정하기를 바라며, 큰 부하는 주지 않기 때문에 일주일에 한번 정도로 진행을 하는 것도 좋은 방안이다.(스케줄 서비스가 시작 되어야 함)



[그림 5-12] 응급복구 디스크를 일주일에 한번 단위로 예약 화면

5. 마무리

응급복구 디스크는 현재 운영하는 윈도우 2000 시스템에 문제가 발생한 경우 원래대로 복구하는 수단으로 이용된다. 하지만, 레지스터리를 백업하고 복원하는 수단 외의 응급 복구 디스크 자체의 활용 범위는 매우 한정적인 부분을 가지고 있다. 이 말은 따로 관리자가 추가로 작업 해야 하는 것 보다는 간단하게 응급복구 디스크가 존재 여부로 문제 해결을 결정 짓기 때문이다. 결과적으로 응급 복구 디스크로 제공되는 두 가지 모드에 대한 내용을 잘 숙지 한다면 쉽게 해결 방법을 찾을 수 있으며 응급복구 디스크에 중요성 또한 잊지 않고 사용을 하기를 바란다.

참고 문헌

- Differences Between Manual and Fast Repair in Windows
<http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q238359>
- Using System.alt to Recover the System Hive
<http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q151247>
- How to Create an Emergency Repair Disk in Windows 2000
<http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q231777>
- Recovering from Failed System Drive with Non-Default %SystemRoot% Folder
<http://support.microsoft.com/default.aspx?scid=kb;en-us;Q235478>
- Emergency Repair Disk Information Requires 1.44-MB Floppy Disk
<http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q156052>