

Chapter

1

시스템 재난 복구 방안 개요

이 장에서는 윈도우 2000 시스템을 복구하기 위한 준비 방법, 복구 시 주의할 점, 또한 문제 발생을 쉽게 해결할 수 있는 채널을 제시하였다.

1. 시스템 재난 복구 방안 개요

1. 개요

시스템 다운이 일어난 경우 가장 먼저 찾게 되는 해결책은 “어디까지 백업이 되었느냐”는 것이다. 그러나 대부분의 관리자는 “백업을 제대로 받지 않았다”는 답변을 한다. 이러한 점으로 미루어 볼 때 대부분의 관리자는 백업을 매우 귀찮아 하는 것으로 볼 수 있다. 달리 말하면, 백업을 어떻게 받아야 할 지 모르기 때문일 가능성도 높다. 두 말 할 필요 없이 백업은 문제 해결을 위한 가장 중요한 수단이라는 것을 잊지 말아야 한다. 복구 과정에 수행되는 여러 가지 개요를 정리하면 다음과 같다.

첫째, 백업 및 복원

시스템 백업에 대한 복원 방법과 백업 일정은 어떻게 구성 했는지 관리자는 분명히 알고 있어야 하는 부분이며, 이러한 작업은 얼마나 잘 진행되고 있는지가 중요하다.

둘째, 복구 도구 활용

윈도우 2000에서는 윈도우 NT 4.0 보다 향상된 복구 도구가 제공되며, 이 부분에 대해서 잘 알고 있다면 문제가 발생한 경우 빠른 복원을 수행할 수 있다.

예를 들어 윈도우 NT 4.0에서는 유일한 복구 도구가 RDISK(응급복구 디스크)였지만 윈도우 2000에서는 이 도구 외에 복구 콘솔(Recovery Console 이하 복구 콘솔)이라는 도구를 통해서 기존에 복구에 어려움이 있었던 부분을 매우 빠르고 쉽게 복원할 수 있다. 또한 안전 모드 역시 여러 가지 기능이 추가적으로 제공되어 향상된 기능을 볼 수 있으며, 관리자는 이러한 기능들을 모두 익혀 두는 것이 중요하다.

셋째, 레지스터리 활용

레지스터리는 윈도우의 중앙 데이터베이스라고 하며, 시스템에 대한 정보가 보관되어 있다. 따라서 레지스터리에 있는 시스템 정보를 잘 활용하면 효율적인 기능을 활용할 수 있으며, 문제가 발생할 경우 빠른 복원을 도모할 수 있다. 이 내용은 누구나 알고 있는 말일 수 있으며, 레지스터리에 있는 내용도 직접 수정하여 처리할 수 있어야 한다. 따라서 필자는 그에 필요한 정보를 제공하도록 하겠다.

넷째, MS 기술 문서 활용

여러분이 자주 접할 수 있는 대부분의 오류에 관한 정보는 MS 기술 문서에서 찾을 수 있다. 그러나 찾는 방법을 잘 알고 있지 못한 경우도 많으며, 제대로 이해하기 어려운 내용도 많다. (혹은 영어 실력이 부족하기 때문이기도 하다) 이벤트 오류 정보나 블루 스크린에서 나타나는 오퍼랜드 코드(Operand Code) 역시 MS 기술 문서에서 찾아볼 수 있다.

위에서 나열한 시스템 재난 복구에 대한 개요는 필자가 세미나를 통해서, 또는 직접 필드에서 경험한 부분을 토대로 정의했다. 또한 이 책 전반에서 계속 언급될 것이다.

동일한 하드웨어와 소프트웨어를 사용한 시스템의 차이점은 무엇인가?

이 질문에 대해 올바르게 답변할 수 있다면 재난 복구를 어느 정도 이해할 수 있다고 해도 과언이 아니다. 일단 다른 점을 나열해 보기로 하자.

컴퓨터 이름, IP 주소, MAC 주소 등이 달라지는 것은 쉽게 알 수 있지만, 또 다른 것이 무엇이냐고 묻는다면 쉽게 답변하지 못하고 대부분 고개를 숙이고 고민에 빠진다. 그 다음 SID가 서로 다르지 않느냐는 실마리를 주면 이제서야 알겠다는 식으로 대답하는 경우가 많다. SID는 많은 관리자가 알고 있는 부분이며, 인증 부분에서나 파일 시스템에서 학습한 내용이라고 생각된다.

- SID을 어떻게 볼 수 있는가?
- 현재 시스템을 재 설치할 경우 다른 SID을 부여 받게 되는가?

이러한 내용을 이 책 전반적으로 제공하고 있다고 해도 과언이 아니다. 또한, 이러한 과정을 거쳐 어떻게 백업된 내용을 복원할 수 있는지 살펴보게 될 것이다. 궁금하다고

할지라도 천천히 인내를 갖고 따라오기 바란다.

또한 노턴 고스트 같은 디스크 이미지 도구로 작업한 모든 시스템은 동일한 SID을 가지게 된다. 그럼 시스템 백업(다른 말로 시스템 상태 데이터 백업)을 하게 된다면 동일한 SID을 가진다는 뜻인가?

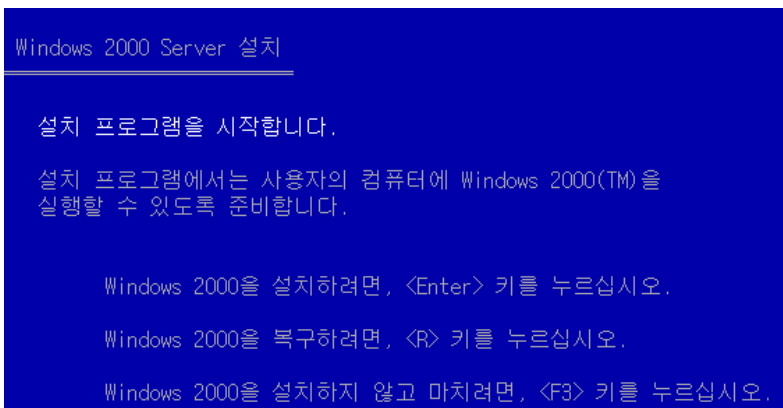
2. 시스템 복구 시 피해야 할 작업들

필자는, 윈도우 2000의 경우 거의 대부분의 재난은 복구가 가능하다고 생각한다. 다만 몇 가지 원칙을 잘 지킬 필요가 있다. 여기서는 그러한 몇 가지 사항에 대하여 알아보기로 한다. 이 내용은 필자의 경험에 따른 것으로 복구에 대한 이론을 훨씬 더 많이 알고 있다면 따르지 않아도 된다.

첫째, 윈도우 2000 원본 CD로 부팅을 하게 되면 복원 설치 부분을 볼 수 있으나 이 작업은 되도록이면 진행하지 말라

복원 설치 작업을 진행할 경우, 설치 작업과 마찬가지로 제품 번호를 입력하게 된다. 이 때, 현재 설치된 윈도우와 동일한 제품 번호를 입력해야만 하며 그렇지 않을 경우는 복원이 불가능해진다. 임의의 제품번호를 입력하게 되면 일단 진행하는 것처럼 보이지만, 그 이후 더 이상에 작업이 진행 불능 상태가 되어 설치 작업 도중 멈추어 버리는 현상이 발생하게 된다.

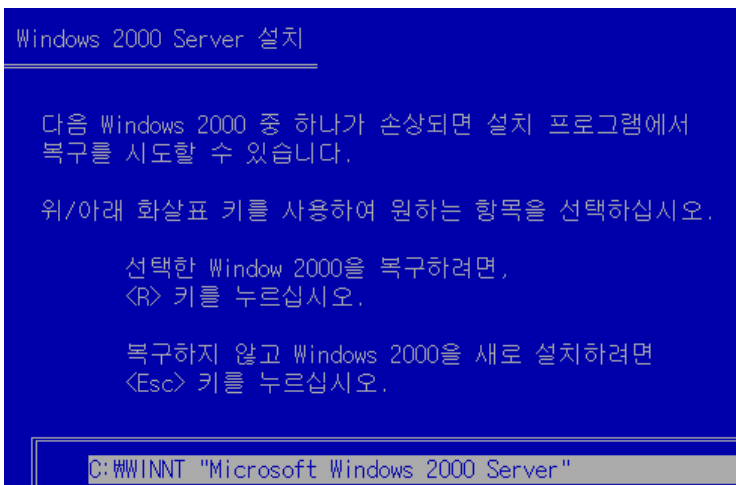
그 결과 다시 부팅을 하더라도 제품번호를 넣는 부분이 계속 나오게 되며 이후 작업을 할 수 없게 된다.



[그림 1-1] 윈도우 2000 원본 CD을 넣고 복원을 선택 할 수 있는 부분

복원 설치를 고려하지 말아야 하는 다른 까닭으로는, 현재 대부분의 윈도우 2000은 SP3(서비스 팩 3)가 설치되어 있으며 복원을 하는 CD는 윈도우 2000 SP(서비스 팩)가 있지 않은 원본 CD라는 점이다. 결국 복원을 하게 되면 원본 CD에 있는 옛 시스템 파일들로 복원이 될 것이다.

이러한 작업을 하고 재부팅을 하게 되면 많은 이벤트 에러를 받을 뿐만 아니라, 여러 프로그램들이 에러를 발생하게 될 것이며 이것은 설치되어 있는 서비스 팩 버전과 다른 파일들이 복원되었기 때문이다.



[그림 1-2] 설치 작업 도중 복원 작업 부분

만일 이렇게 복원을 할 경우 당연히 SP3을 다시 설치해 주어야 한다. 그러나, 이 작업 역시 많은 시스템 파일들의 버전을 혼란스럽게 만들 수 있기 때문에 시스템 파일 상호간 충돌이 발생하게 된다. 따라서, 복원 작업은 다른 여타의 방법으로 복구 작업이 불가능하다고 판단되는 경우 마지막 선택으로 고려하는 것이 좋다.

둘째. 기존에 있는 파일이 최대한 손상이 가지 않도록 복원을 해야 하며, 복원 전 백업을 꼭 받아두기를 바란다.

일반적으로 시스템이 다운되고, 많은 부분들을 복원하기 위해 여러 가지 작업을 진행하게 된다. 그 경우 현재 망가진 시스템의 정도가 “1”이라고 했을 때, 수정 작업을 통해 “2”정도로 망가지다가 결국 “3” 이상으로 망가지는 사태가 벌어진다. 이런 것은 의도한 바는 아니겠지만, 쉽게 볼 수 있는 현상이다. 따라서, 다운된 시스템이라고 할지

라도 복사 등의 방법으로 백업을 받을 수 있다면 백업 작업을 해 두는 것을 권장한다. 이는 시스템뿐만 아니라 데이터 역시 마찬가지다. 다운된 시스템에 대한 복원 방법에 대해서는 이 책에 설명된 자료를 참고하기 바란다.

일반적으로 손상되는 것은 전 부분의 시스템이 아니라, 일부분일 따름이며 그러한 부분의 해결만으로 정상적인 부팅으로 돌아오도록 할 수 있다. 일단 백업을 해 두는 것을 반드시 잊지 않기 바람, 그 이후에는 이 책에서 제공되는 방법을 통해 복원을 시도해 보기 바란다.

3. 문제 발생시 바로 찾아 볼 수 있는 채널

다음 나타낸 표는 시스템에서 문제가 발생할 경우 살펴 볼 수 있는 채널로, 시스템 문제로 어려움에 처할 때 빨리 참조할 수 있는 페이지가 나타나 있다. 또한 책을 이해하기에 좋은 개관이 될 수 있다.

NO	내용	페이지
1	윈도우 2000 부팅 시 필요한 파일들은 어떤 것이 있는가?	24
2	boot.ini 파일은 일반적으로 C:\Wboot.ini에서 볼 수 있다고 하는데 살펴 보니 없다. 왜 그런가?	27
3	MULTI(xx)와 SCSI(xx)라는 ARC 규칙 사용 하는 방안은? 또한 SCSI BIOS 에 활성화와 비 활성화 시 차이점은?	28,29
4	시동디스크(StartUp) 디스크는 어떻게 만드는가?	30,31
5	Ntbootdd.sys에러가 발생했다, 해결 방법과 역할은?	31
6	시스템 파티션과 부팅 파티션에 대한 차이점은 무엇인가?	32
7	MBR 에러 또는 부트 섹터 문제가 발생 시 해결 방안 Invalid partition table. Error loading operating system. Missing operating system.	35, 72
8	하드웨어 프로파일은 어떻게 구성 하고 무엇을 저장 하는가?	41,42
9	부팅 시 ntoskrnl.exe에 관한 에러 메시지가 나타난다. 동일한 에러 메시지가 계속 반복된다. 그 이유는?	44,45,70

10	멀티 부팅을 하는 환경에서 C 드라이브를 포맷하였다. D 드라이브는 윈도우 2000 운영체제가 설치되어 있지만, C 을 포맷한 관계로 부팅을 할 수 없다. 해결방안은?	47,48
11	윈도우 2000 진행 상태 바에 대한 자세한 자료를 얻고자 한다, 실제 문제 상황을 제공 받고자 한다.	49,50,51
12	복구 콘솔로 로그인 하게 될 경우 접근 할 수 있는 폴더 위치는?	57
13	NTLDR is compressed Press Ctrl+Alt+Del to restart 에러 메시지가 발생	60
14	블루 스크린을 통해서 chkdsk 실행 하라고 메시지가 나온 다 해결 방안은?	61
15	복구 콘솔에서 서비스를 시작 또는 중지 하는 방법은?	61,63
16	ntldr 이라는 메시지가 발생 시 해결 방안은? FAT 일 경우 - "Boot: Couldn't find NTLDR " NTFS 일 경우 -"NTLDR is missing"	66
17	"Ntdetect.com을 찾을 수 없습니다."라는 에러 메시지를 받았다. 이에 대한 해결 방법은 무엇인가?	68
18	부팅 시 ntoskrnl.exe에 관한 에러 메시지를 받았을 때의 해결 방법은 무엇인가?	69
19	boot.ini 규칙이 문제가 되었거나, 파일이 없어서 에러가 발생 할 때 해결 방법은 무엇인가?	71
20	MBR을 해결 방안 및 제거 하는 방법은 어떻게 되는가?	72,73
21	DOS 용 Floppy 이미지 만드는 방법 소개	75
22	복구 콘솔 : 모든 드라이브 및 폴더에 플로피 복사 및 액세스 허용 부분을 가능하도록 하려면 어떻게 해야 하는가?	83,84
23	복구 콘솔로 부팅을 한 경우, 접근 할 수 있는 부분이 제한이 되어 있다. 또한 내부에 있는 데이터를 A 드라이브로 복사할 수 없다.	82
24	페이지 파일 에러로 부팅이 되지 않을 때 페이지 파일을 지우고자 한다 어떻게 지울까?	77
25	페이지 파일을 4GB로 설정하고 싶다 방법은?	77

26	노턴 고스트로 타 시스템 복원 시 화면이 나타나지 않거나 여타 문제가 발생한 경우, 해결 방법은 무엇인가? 혹은 서버 시스템을 데스크 탑에 복원하고자 한다. 방법은?	79
27	탐색기 문제로 인해 재부팅을 했지만 데스크탑 환경이 나타나지 않는다. 해결 방법은?	80
28	시스템이 어느 날 갑자기 "Missing Operating System" 에러가 나타났다. 해결책은 무엇인가?	86
29	"The SET command is currently disabled. The SET command is an optional Recovery Console command that can only be enabled by using the Security Configuration and Analysis snap-in." 이라는 에러가 발생하였다. 그 이유는 무엇인가?	85
30	윈도우 XP 설치 후 윈도우 2000을 설치하면 부팅에서 에러가 발생을 한다. 그 까닭은 무엇이며 해결 방안은?	87
31	모니터 설정 화면에서 재생 빈도를 변경한 뒤 시스템을 제어되지 않는다. 화면이 검은 색으로 변하거나 심하게 회전하는 모습으로 나타난다. 해결 방법은?	97
32	레지스터리 또는 잘못된 제어기로 인해 야기된 문제의 해결 방안은?	98
33	"마지막으로 성공한 구성"은 언제 사용할 수 있는가?	99,100
34	디렉터리 서비스 복원 모드 사용 방법은?	104
35	응급복구 디스크 만드는 방법은 어떻게 되는가?	112,113
36	윈도우 NT 4.0 rdisk는 어떠한 내용이 첨부되어 있는가?	112
37	Repair 디렉터리 밑에 Regback라는 디렉터리는 왜 생기는가? 또는 어떻게 만들 수 있는가?	115
38	응급복구 디스크에 수동 모드와 빠른 모드가 있다. 차이점은 무엇인가?	118,119
39	응급복구 디스크의 내용으로 레지스터리를 복원 시키고자 한다. 어떻게 진행하고 어떤 상태에서 쓰이는가?	120
40	응급복구 디스크를 자동으로 백업 하는 방안은 없는가?	121

41	HKEY_CURRENT_USER 에는 어떠한 내용이 있는가?	132
42	레지스터리 백업 방법은 어떻게 되는가?	133
43	병합 기술을 통해서 자동 로그인 설정하기	139
44	응용프로그램 제거 방법은 어떻게 되는가?	141
45	서비스 목록 제거 방법은?	142
46	관리자 계정 암호를 분실했다. 해결 방안은 없는가?	143
47	하이브 로드와 하이브 언 로드는 무슨 뜻인가?	144
48	SAM 하이브를 보면 실제 사용자 리스트를 볼 수 있다. 실제 SAM 파일과 연관성은 있는가?	147
49	“복구 콘솔 : 모든 드라이브 및 폴더에 플로피 복사 및 액세스 허용” 을 레지스터리에서 수정 하고 싶다. 또한 다운된 시스템에서 이 부분을 수정 할 수 있을까?	145,146
50	백업에도 여러 정책이 있는데 활용 방안은 어떻게 되는가?	155,156
51	백업 프로그램에서 일정을 추가 해서 백업을 하고 싶을 때 방법은 없는가?	158,159
52	백업 일정을 명령 라인에서 실행 하고 싶는데 좋은 방법이 없는가?	161
53	윈도우 2000 운영체제가 두 개의 동일한 하드웨어에 설치되었더라도 서로 다른 부분이 있다. 어떠한 것이 있는가?	167
54	기존 시스템 백업 후 새로운 시스템 복원 작업 진행 결과는 어떻게 되는가?	168
55	SID(보안 식별자)란?	169
56	기존 시스템 상태 데이터 백업 후 새로운 시스템에 복원 결과는 어떻게 되는가?	169
57	실제 운영되고 있는 레지스터리 파일만 백업해서 새로운 시스템에 복원을 하게 될 경우 어떻게 되는가?	170
58	자신의 시스템에서 응급복구 디스크로 백업 해 둔 레지스터리를 복원하였다면 그 결과는 어떠한가?	171
59	ADDUSERS 유틸리티 사용 사용자 백업 방법 및 복원은 어떻게 되는가?(독립형 서버)	173

60	ADDUSERS 유틸리티로 한글 사용자도 백업 및 복원이 가능한가?	174
61	레지스터리로 DNS 정보를 내보내기 한 파일 내에는 어떠한 정보가 저장되고, 또한 복원은 어떻게 하는가?	183
62	DNS 서비스 시스템이 다운되었을 경우 백업과 복원 방법은 어떻게 되는가?	187
63	DNS 서비스 시작 시 부팅 방법을 선택 할 수 있도록 하려면 어떻게 하는가?	189
64	DNS 서비스를 부트 파일을 이용하여 시작할 수 있는 방법과 부트 파일의 백업 및 복원 방법은 어떻게 되는가?	191
65	유닉스 DNS named.boot 파일을 윈도우에서 바로 사용할 수 있는 방법은 무엇인가?	192
66	다운되어 복구가 불가능한 경우가 아니라면 IIS만을 다시 설치하여 문제를 해결할 수 있다. 이 경우 미리 백업된 IIS 정보를 통해 복원을 할 수 있는가?	197
67	웹 서비스가 설치된 윈도우 2000 서버를 그대로 다른 서버로 이동할 경우나, 현재의 윈도우 2000 서버를 재설치하려면 어떻게 할 수 있는가?	203
68	웹사이트 및 FTP에 대한 설정 정보를 백업 받고자 한다. 어떻게 작업하는가?	206
69	MetaEdit 2.2을 통해 웹과 FTP 서비스 대한 설정 정보를 백업 및 복원 방법은?	207,208
70	SMTP 폴더를 다른 디렉터리로 변경 하고자 할 때 작업 방법은 어떻게 되는가?	209
71	시스템 상태 데이터 백업 시 웹 서비스는 백업이 되는가?	164,201
72	단일 프로세서에서 다중 프로세서로 업그레이드 방법(윈도우 NT/2000)	214
73	윈도우 2000에서 노턴 고스트 사용 방법은?	224
74	유용한 플로피 디스크 제작 방법들을 알고 싶다면?	226
75	가상 메모리란 무엇이며 무슨 작업을 하는가?	228

76	블루 스크린 왜 나타나며 해결 방안은 없는가?	230
77	윈도우 PE 라는 것이 있다고 하는데 무엇인가?	235




[표 1-1] 시스템 문제 해결 채널(북 마크)

4. 이 책의 활용 방법

필자는 많은 시스템의 재난 복구의 경험을 바탕으로 이 책을 발행하였다. 또한 그 외 여러 번의 세미나를 통해 실제로 경험한 이야기와 내용을 접하면서 시스템 복구에 대한 긍정적인 내용들을 많이 얻게 되었으며 그러한 것들을 토대로 하여 책을 펴내게 되었다. 필자도 또한 재난 복구 도중 많은 서버를 망가뜨려 상당한 어려움을 겪은 적이 있으나, 이러한 사항들이 모두 필자에게는 좋은 경험이 되었으며, 시스템을 확실하게 이해할 수 있는 도움을 주게 되었다. 이러한 과정을 통해 알게 된 정보와 자료들은 이 책을 통해 풀어 나갈 것이며, 이 책이 여러분들에게 좋은 안내서가 되기를 바란다.

마지막으로 이 책을 잘 활용하기 위해 최소한 한 대의 실습용 장비를 준비하여 시스템을 망가뜨리는 것에 대한 공포가 없어야 할 것이다. 망가뜨린 시스템을 원상 회복시키는 방법은 이 책에서 잘 소개 되어 있으니 하나씩 따라 한다면 복구에는 무리가 없을 것이다. 또한 그런 경험들이 실무에도 많은 도움을 줄 것이다.

아래 내용은 책 속에서 제공되는 문서에 대한 보충 설명이나 위험들을 알려 주는 아이콘 자료이다.

아이콘	내용
	경고 또는 주의, 실제 작업을 하면서 어려움을 겪게 될 때 주의해서 작업하는 것이 필요할 때
	정보나 참고의 의미, 현재의 내용을 좀 더 보완을 하고자 정리한 문서
	메모나 노트의 의미. 주요 상식이나 아주 짧게 문서를 제공 하는 글

[표 1-2] 책에 사용되는 아이콘 설명