중소기업 개인정보보호 핸드북

- 기술적 보호대책 중심으로 -

2007. 4.

정 보 통 신 부

한국정보보호진흥원

주 의 사 항

이 핸드북의 이용에는 어떠한 제한도 없지만 다음과 같은 사항에 주의하여야 합니다.

- 문서 내에 언급된 상표, 제품명 등에 대한 권리는 각 상표 또는 제품을 소유한 해당 기업에 있으며, 설명을 위해 특정 회사 제품명이나 화면이 표시된 경우 “머리말”에 정의된 핸드북의 고유 목적 외에 어떠한 다른 목적도 없으며 그렇게 이용되어서도 안 됩니다.

- 문서 내에 기술된 예시 등은 특정 중소기업에서 구성한 IT 환경과 정보보호 관리체계 및 침해사고 사례로부터 도출된 것이므로, 모든 기업에 적용되지 않을 수 있습니다. 내용의 오류로 인해 발생하는 피해에 대하여 본 핸드북의 발행기관은 책임을 지지 않습니다.

- 또한 본 핸드북에 언급된 취약점은 절대 악용되어서는 안되며, 이로 인하여 발생하는 피해에 대하여 이 핸드북의 발행기관은 책임을 지지 않습니다.

※ 이 핸드북의 내용 중 오류를 발견하였거나 내용에 대한 의견이 있을 때에는 privacytech@kisa.or.kr로 해당 내용을 보내주시기 바랍니다.

중소기업 개인정보보호 핸드북

- 기술적 보호대책 중심으로 -

2007. 4.

정 보 통 신 부

한국정보보호진흥원

머리말

우리나라의 정보화 수준이 높아지면서 많은 중소기업에서 서버 및 PC 장비를 활용하여 개인정보를 비롯한 기업경영 전반에 대한 정보를 처리하고 있으며, 기업의 내외부 네트워크를 통한 다양한 정보의 유통이 가능해졌습니다. 또한 대다수의 중소기업이 홈페이지를 구축 · 운영하고 있고 이 중 상당수가 홈페이지 방문자의 개인정보를 수집하여 텔레마케팅과 같은 상업적 목적으로 활용하고 있습니다.

이는 대기업과 마찬가지로 중소기업에 있어서도 고객관리가 기업의 경쟁력을 갖추기 위한 지식경영의 필수요소이며 기업활동을 위해 개인정보의 수집과 이용이 불가피하게 되었음을 의미합니다. 또한 단 한번의 개인정보 누출로도 기업의 이미지가 상당부분 실추될 수 있고, 기업의 경쟁력 상실과 금전적 손실을 초래할 수 있다는 점에서 기업 경영상의 위협이 되기도 합니다. 뿐만 아니라 개인정보의 오남용과 유출에 따른 불안감은 정보화에 대한 사회적 역기능으로 작용하므로 개인정보는 기업의 주요자산으로 관리되고 보호되어져야 합니다.

따라서, 개인정보 유출에 대한 불안감을 불식시키고 개인정보의 안전한 관리 및 보호가 담보되어야만 중소기업의 활발한 경제활동을 보장할 수 있을 것입니다. 그러나, 중소기업의 경우 정보화 예산과 전문인력의 확보가 부족하여 개인정보 유출방지를 위한 보안대책 마련에 어려움을 겪고 있습니다.

본 핸드북은 이와 같은 열악한 환경에 있는 중소기업 스스로가 개인정보보호를 위해 고려해야 할 보안사항에 대한 기술적 가이드라인을 제시하고 있습니다. 본 핸드북의 활용을 통해 중소기업의 개인정보 침해사례를 줄이고 기업의 보안 강화에도 일조하기를 기대합니다.

2007년 4월

한국정보보호진흥원장

목 차

Information Security

목 차

Information Security

표 차례

그림 차례

목 차

Information Security

제 1 장 총괄편

I

Information Security

1. 중소기업 개요 및 정보화 현황

1.1 중소기업 개요

• 우리나라 전체 기업수의 99.8%, 고용인력의 86.5%를 차지하고 있을 정도로 국가 산업 · 경제의 중요한 역할을 담당하고 있는 중소기업은 『중소기업기본법 제2조및 동법시행령 제3조』에 따라 상시근로자수 · 자본금 또는 매출액의 규모기준에 따라 업종별 유형이 다양하게 분류된다.

[표 1-1] 중소기업의 사업체 및 종사자수(2004년말 기준)

전 체 (A)		중소기업 (B)		비 중 (B/A)	
사업체수	종사자수	사업체수	종사자수	사업체수	종사자수
3,003,180	12,036,330	2,998,223	10,415,383	99.8%	86.5%

※ 출처 : 중소기업청, 2006년 중소기업 관련통계(2006.12)

※ 중소기업기본법 제2조제1항(중소기업자의 범위)

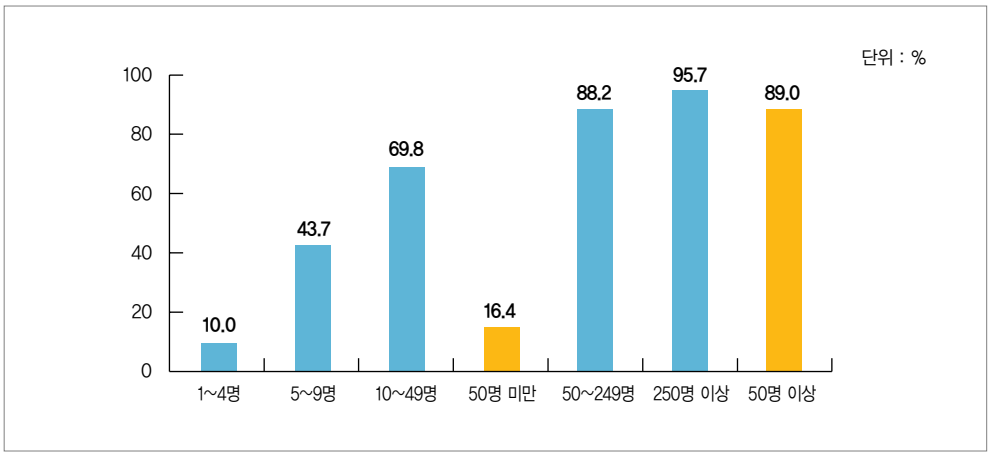
중소기업육성시책의 대상이 되는 중소기업자는 업종의 특성과 상시근로자수, 자산규모, 매출액 등을 참작하여 그 규모가 대통령령이 정하는 기준 이하이고, 그 소유 및 경영의 실질적인 독립성이 대통령령이 정하는 기준에 해당하는 기업을 영위하는 자로 함

1.2 개인정보 측면에서의 정보화 현황 및 문제점

■ 중소기업의 정보화 현황

• 2005년 12월말 기준, 전국의 전체 사업체(315만 5천여 개)중 50명에서 249명 이하인 사업체의 네트워크 구축률은 88.2%로 일정 규모의 사업체는 네트워크 환경을 구축 · 운영하고 있으며, 이에 따라 내외부 네트워크를 통한 개인정보 유통이 가능하다.

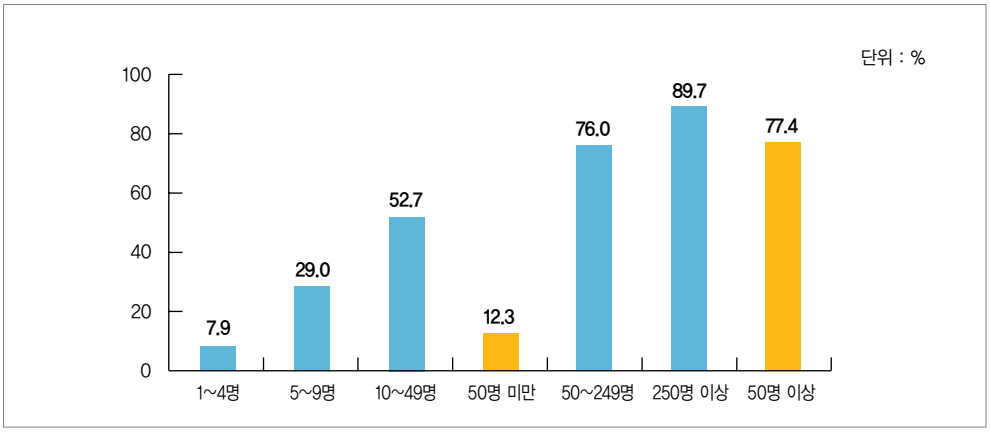
〈그림 1-1〉 규모별 네트워크 구축률



※ 출처 : 한국정보사회진흥원(2006년 정보화 통계조사)

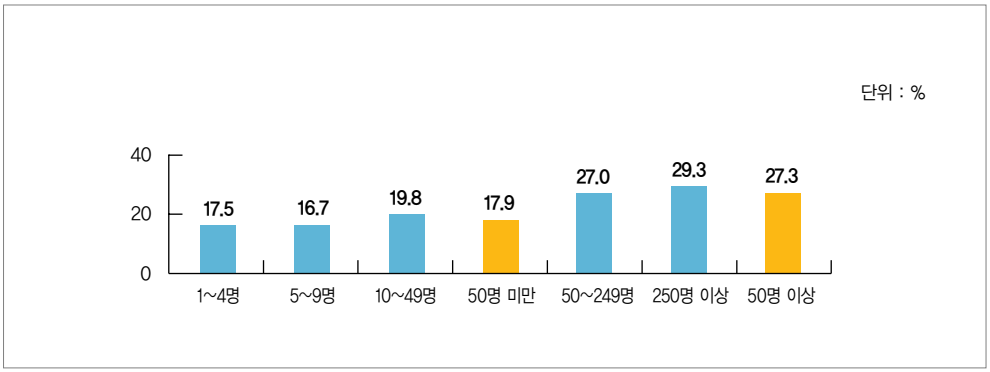
또한, 종사자수 50명에서 249명 이하인 사업체의 76%가 홈페이지를 보유하고 있으며, 이중 상당수가 홈페이지 방문자의 개인정보를 수집하고 있는 것으로 나타났다.

〈그림 1-2〉 규모별 홈페이지 보유율



※ 출처 : 한국정보사회진흥원(2006년 정보화 통계조사)

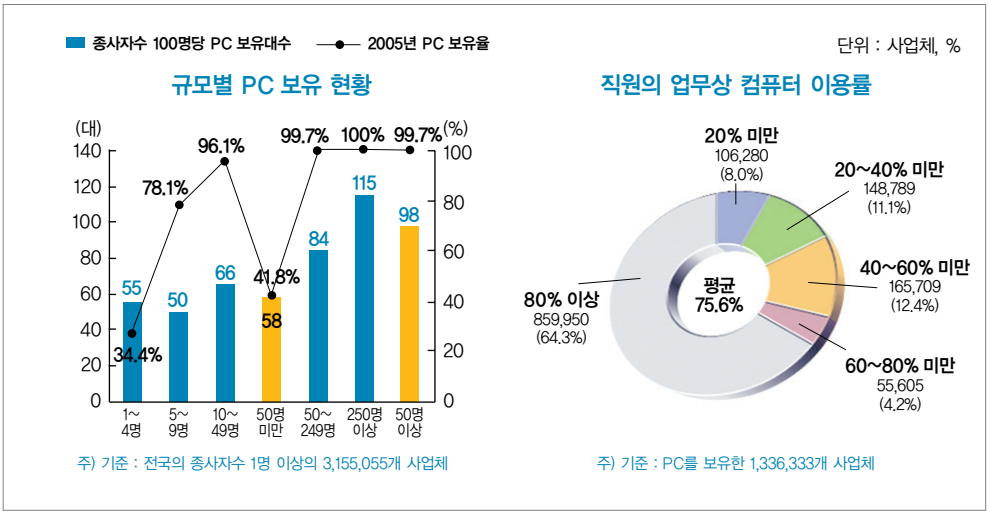
〈그림 1-3〉 규모별 홈페이지 개인정보 수집 현황



※ 출처 : 한국정보사회진흥원(2006년 정보화 통계조사)

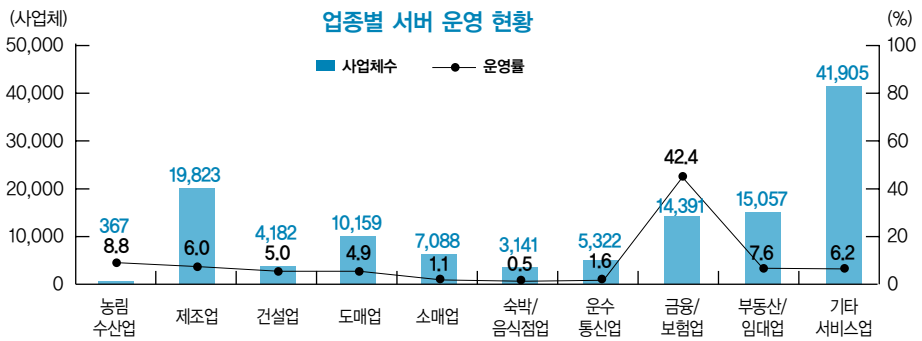
• PC보유율 및 직원의 PC 이용률을 살펴봤을 때, 종사자수 50명에서 249명 이하인 사업체의 PC보유율은 86.1%이며, PC 보유 사업체(133만 6천여 개)중 직원의 평균 PC 이용률은 75.6%였으며, 64.3%가 직원의 80% 이상이 업무상 컴퓨터를 이용하고 있는 것으로 조사되어 PC를 통한 업무수행 및 개인정보처리도 증가하였음을 알 수 있다.

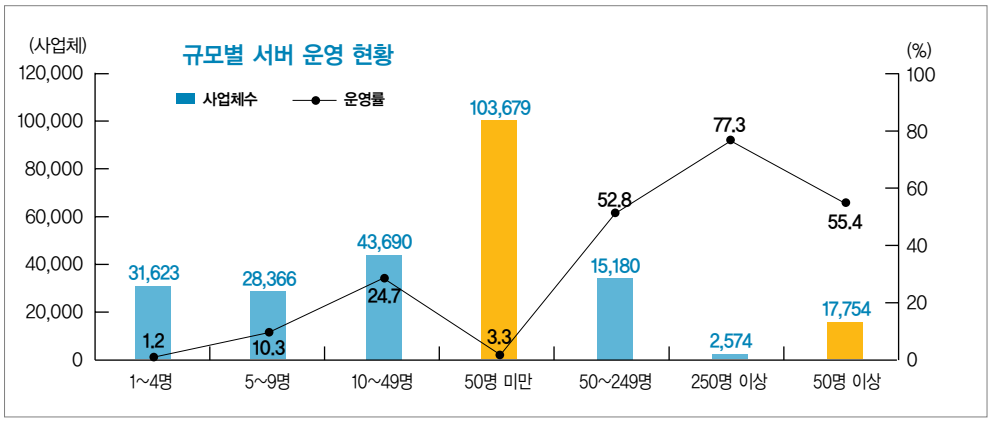
〈그림 1-4〉 규모별 PC 보유 현황 및 직원의 PC 이용률



• 서버를 운영하고 있는 현황을 살펴보면, 종사자수 50명에서 249명 이하인 사업체의 서버 운영률은 52.8%로 나타났으며, 금융 및 보험업의 서버 운영률이 42.4%로 가장 높게 나타났다. 특히 금융 및 보험업의 경우, CRM 등을 도입하여 홈페이지 또는 오프라인으로 수집된 개인정보를 마케팅 등으로 활용하고 있는 것으로 조사됐다.

〈그림 1-5〉 규모별/업종별 서버 운영 현황

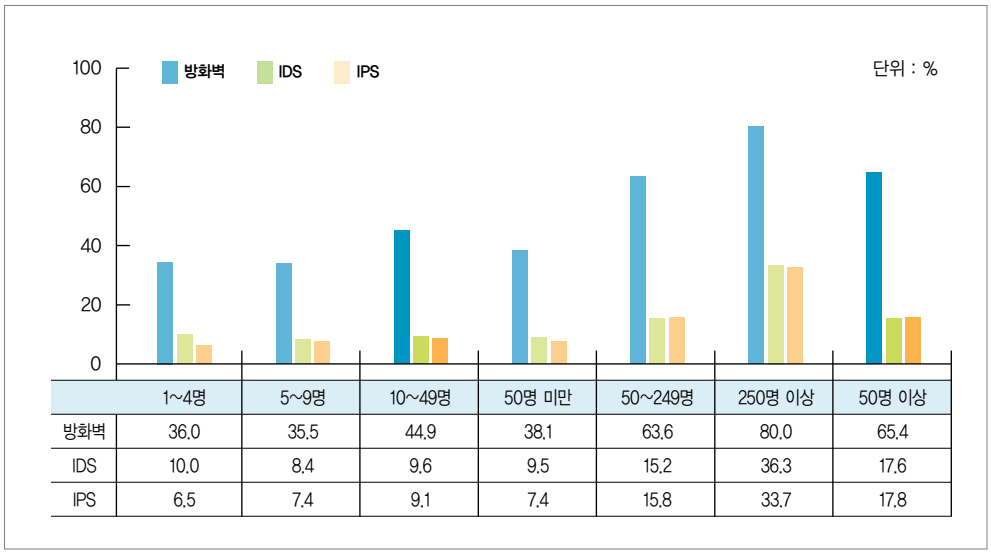




※출처 : 한국정보사회진흥원 (2006년 정보화 통계조사)

• 네트워크를 구축한 사업체(54만여 개)중 침입차단/탐지/방지 등 정보보호시스템을 운영하고 있는 현황을 살펴보면, 종사자수 50명에서 249명 이하인 사업체의 경우, 침입차단시스템은 63.6%, 침입탐지시스템은 15.2%, 침입방지시스템은 15.8%를 도입하여 운영하고 있는 것으로 조사

〈그림 1-6〉 규모별 정보보호시스템 운영 현황



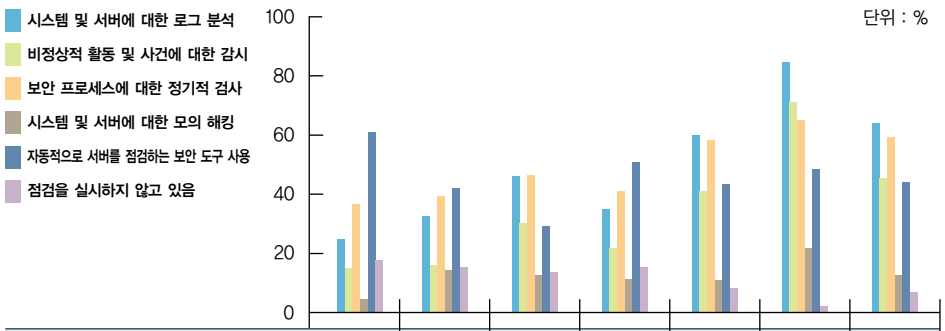
	1~4명	5~9명	10~49명	50명 미만	50~249명	250명 이상	50명 이상
방화벽	36.0	35.5	44.9	38.1	63.6	80.0	65.4
IDS	10.0	8.4	9.6	9.5	15.2	36.3	17.6
IPS	6.5	7.4	9.1	7.4	15.8	33.7	17.8

※출처 : 한국정보사회진흥원 (2006년 정보화 통계조사)

되었다. 특히 중소기업은 정보화 예산의 제약으로 인해 정보보호시스템의 도입률이 저조하며 침입차단시스템도 도입이 안 된 기업이 다수 존재하는 것으로 파악되었다.

- 서버를 운영하는 사업체중 종사자수 50명에서 249명 이하인 사업체의 경우, 서버의 보안성을 확보하기 위한 방법으로 "시스템 및 서버에 대한 로그분석"(60.4%)을 수행하고 있지만, 개인정보 유출방지를 위한 보안관리(보안패치, 권한관리 등)는 잘 이행되지 않는 것으로 나타났다.

〈그림 1-7〉 규모별 서버 보안 활용 현황



	1~4명	5~9명	10~49명	50명 미만	50~249명	250명 이상	50명 이상
시스템 및 서버에 대한 로그 분석	25.4	33.3	46.0	36.2	60.4	84.9	64.0
비정상적 활동 및 사건에 대한 감시	16.0	17.2	30.0	22.2	41.5	72.0	45.9
보안 프로세스에 대한 정기적 검사	37.1	39.6	46.1	41.6	58.2	65.8	59.3
시스템 및 서버에 대한 모의 해킹	5.4	15.5	13.4	12.4	12.1	22.3	13.6
자동적으로 서버를 점검하는 보안 도구 사용	61.0	42.6	49.1	50.9	43.8	47.5	44.3
점검을 실시하지 않고 있음	18.0	16.8	14.6	16.2	9.2	3.8	8.4

※출처 : 한국정보사회진흥원 (2006년 정보화 통계조사)

2. 중소기업 개인정보보호

2.1 개인정보보호의 개요

■ 개인정보의 개념

• "개인정보"라 함은 생존하는 개인에 관한 정보로서 성명 · 주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호 · 문자 · 음성 · 음향 및 영상 등의 정보(정보통신망법 제2조)를 뜻한다.

※ 당해 정보만으로는 특정 개인을 알아볼 수 없는 경우에도 다른 정보와 용이하게 결합하여 알아볼 수 있는 것을 포함

■ 개인정보 관리의 필요성

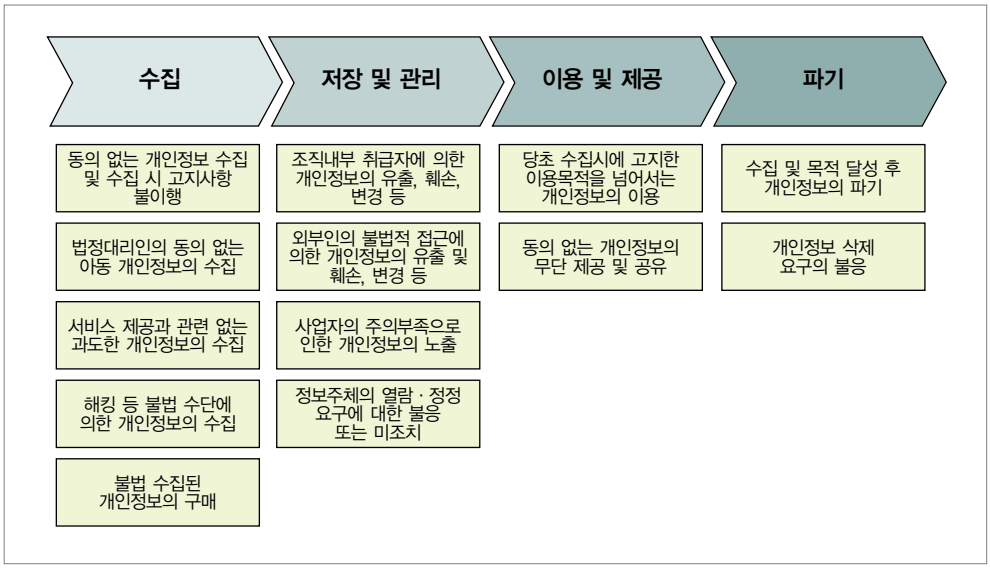
• 기업의 핵심경쟁력 개인정보
  – 중소기업의 고객관리(CRM)는 기업이 경쟁력을 갖추기 위한 지식경영의 필수요소가 되었고,
  – 대기업 뿐만 아니라 중소규모 사업자들도 기업 활동을 위해 개인정보의 수집 및 이용은 불가피하게 되었다.

• 단 한번 누출로 인한 기업경쟁력 상실
  – 개인의 금융정보, 진료정보, 인사정보 등 개인정보는 단 한번의 잘못된 누출만으로 기업의 이미지를 추락시키며,
  – 기업의 경쟁력을 떨어뜨리고 금전적인 손실을 초래함으로써 개인정보 유출이 기업경영상의 중요 요인으로 인식되고 있다.
  (ex : 온라인 게임회사의 개인정보유출로 인한 손해배상청구소송)

2.2 개인정보보호의 침해유형 및 보호대책

• 개인정보 침해유형은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(일부개정 2007.1.26 법률 제8289호)」에 따라 개인정보의 수집, 저장 및 관리, 이용 및 제공, 파기 등의 개인정보 Lifecycle에 따라 발생된다.

〈그림 1-8〉 개인정보의 Lifecycle



• 한국정보보호진흥원에 접수된 개인정보 상담 · 피해 구제접수 현황을 살펴 보면 개인정보의 침해유형별 건수 중 가장 많이 발생한 부문은 "타인정보의 훼손 · 침해 · 도용"이다.

[표 1-2] 개인정보 침해유형 분석

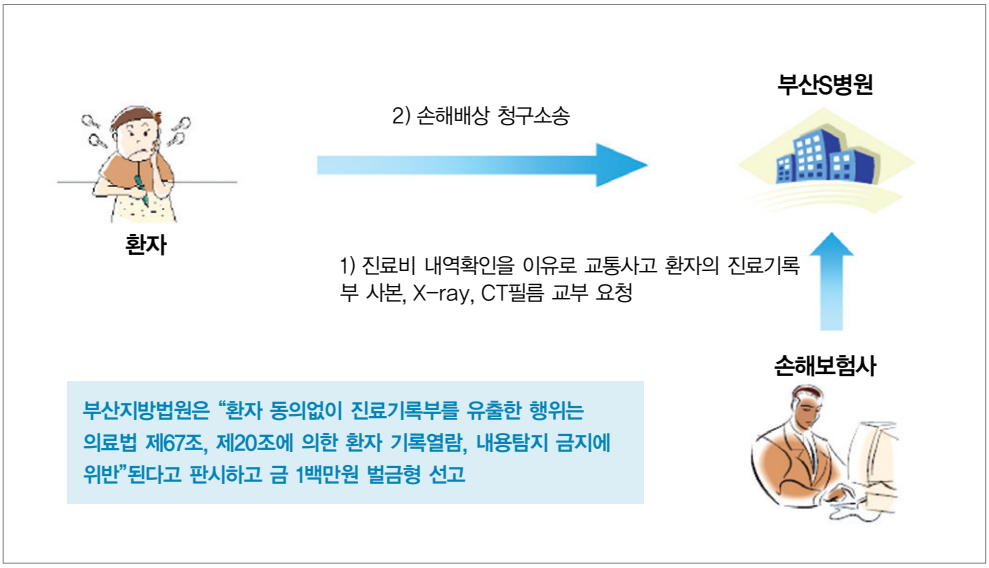
침 해 유 형	2004년	2005년	2006년
이용자의 동의없는 개인정보 수집	564	1,140	2,565
개인정보 수집시 고지 또는 명시 의무 불이행	27	15	27
과도한 개인정보 수집	43	33	61
고지 · 명시한 범위를 넘어선 이용 또는 제3자 제공	784	916	917
개인정보 취급자에 의한 훼손 · 침해 또는 누설	235	186	206
개인정보 처리 위탁시 고지의무 불이행	2	4	5
영업의 양수 등의 통지의무 불이행	5	7	11
개인정보관리책임자 미지정	42	25	23
기술적 · 관리적 조치 미비로 인한 개인정보누출 등	212	390	632
수집 또는 제공받은 목적 달성 후 개인정보 미파기	107	152	266
동의철회 · 열람 또는 정정 요구 불응	2,312	771	923
동의철회, 열람 · 정정을 수집보다 쉽게 해야할 조치 미이행	569	285	484
법정대리인의 동의없는 아동의 개인정보 수집	736	71	23
주민등록번호 등 타인정보의 훼손 · 침해 · 도용	9,163	9,810	10,835
정보통신망법 적용대상 이외의 개인정보침해 (신용정보침해 등)	2,768	4,401	6,355
소 계	**17,569**	**18,206**	**23,333**

■ 개인정보 침해유형

• 고객의 동의 획득 등 정당한 절차없이 제 3자에게 제공하여 본인 모르는 텔레마케팅 수신 등의 정신적 피해를 야기한다.

– 중소기업의 경우, 소비자에게 자사 상품을 홍보 · 판매할 수 있는 적절한 채널이 없어서, 스팸메일 발송 및 텔레마케팅에 이용할 수 있는 개인정보 수집에 주력하고 있다.

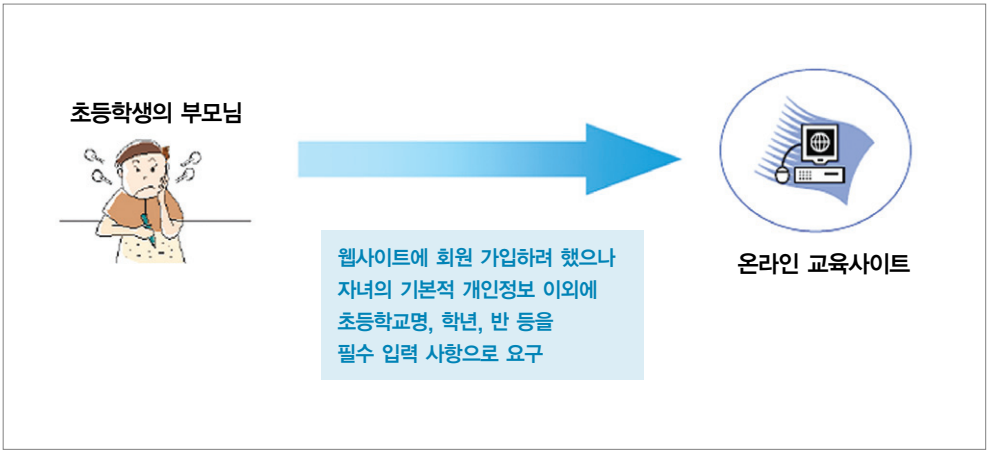
〈그림 1-9〉 환자의 동의 없이 개인정보를 제3자에게 제공



• 필수정보 이외의 과도한 개인정보 수집

– 성명, 연락처 등 서비스 제공에 필수적인 정보 이외의 직접 관계없는 가족관계, 학력, 직업 등 불필요한 부가정보를 수집한다.

〈그림 1-10〉 필수정보 이외에 과도한 개인정보 수집

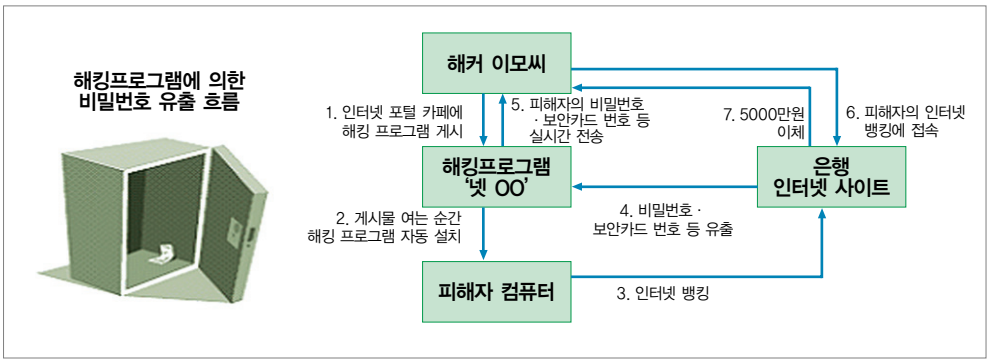


• 내부직원에 의한 개인정보 유출

• 기술적 보호조치 미흡으로 인한 개인정보 유출

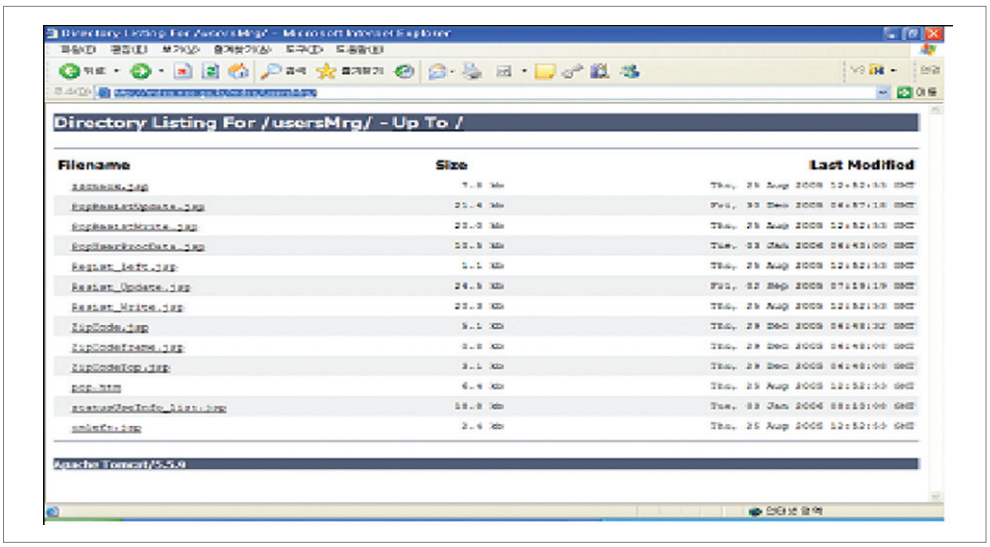
– 키보드 해킹으로 인한 개인정보노출

〈그림 1-11〉 키보드 해킹으로 인한 개인정보 노출



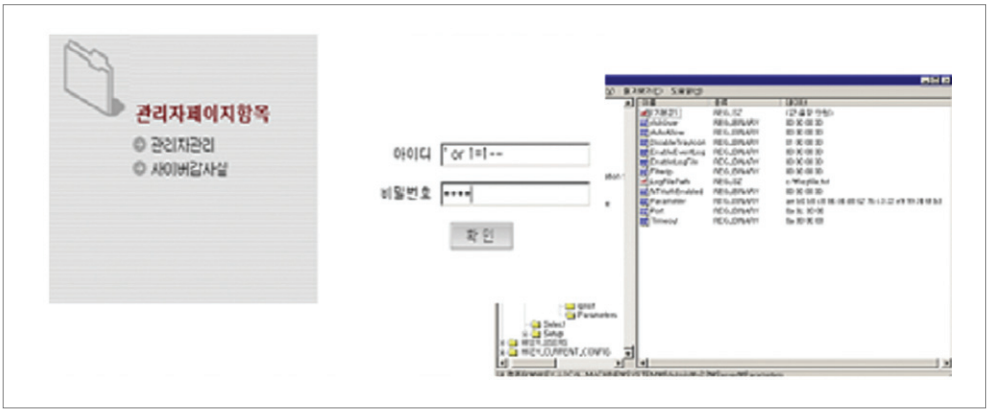
– 웹 취약점으로 인한 개인정보 : 디렉토리 리스팅에 의한 개인정보 유출

〈그림 1-12〉 디렉토리 리스팅에 의한 개인정보 유출

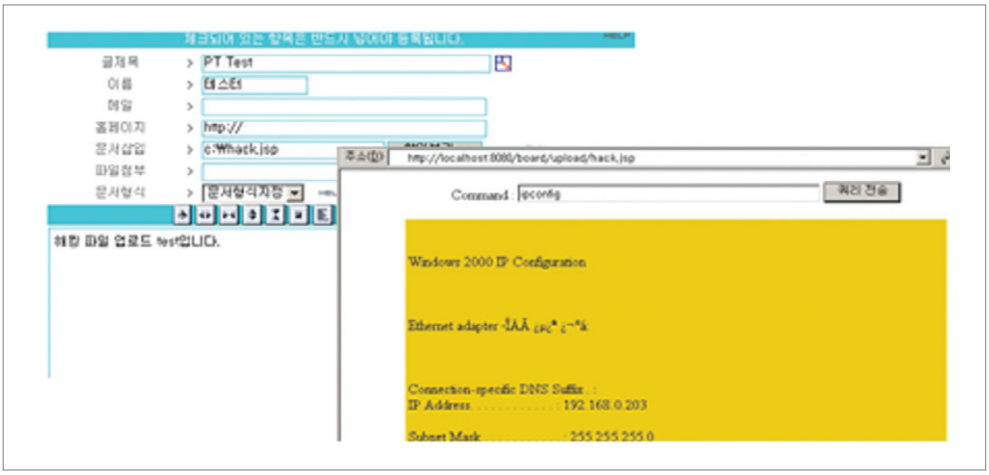


- 웹 취약점으로 인한 개인정보 : SQL Injection에 의한 인증우회

〈그림 1-13〉 SQL Injection에 의한 인증우회(1)

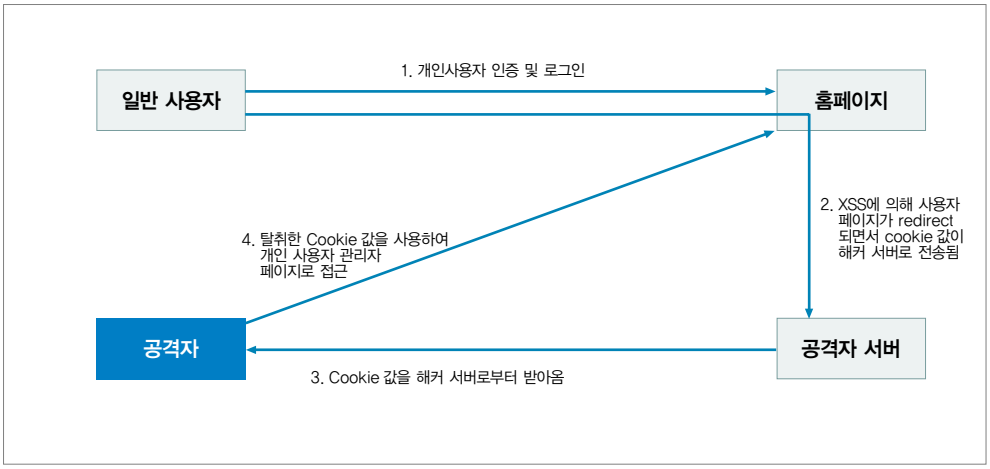


〈그림 1-14〉 SQL Injection에 의한 인증우회(2)



- 웹 취약점으로 인한 개인정보 : XSS를 통한 개인정보 유출

〈그림 1-15〉 XSS를 통한 개인정보 유출



■ 중소기업 개인정보 보호대책

• 개인정보 침해유형별 보호대책은 관리적 · 기술적 대책으로 구분된다.

• 본 핸드북에서는 기술적인 대책에 대한 가이드라인 제공을 목적으로 한다.

구분	침해유형	대책수립시 고려사항
관리적 부문	• 이용자의 동의없는 개인정보 수집 • 개인정보 수집시 고지 또는 명시 의무 불이행 • 과도한 개인정보 수집 • 고지 · 명시한 범위를 넘어선 이용 또는 제3자 제공 • 개인정보 처리 위탁시 고지의무 불이행 • 영업의 양수 등의 통지의무 불이행 • 개인정보관리책임자 미지정 • 수집 또는 제공받은 목적 달성 후 개인정보 미파기 • 동의철회, 열람 또는 정정 요구 불응 • 동의철회, 열람, 정정을 수집보다 쉽게 해야할 조치 미이행 • 법정대리인의 동의없는 아동의 개인정보 수집 • 정보통신망법 적용대상 이외의 개인정보 수집	– 정보통신망 이용촉진 및 정보보호 등에 관한 법률 및 시행령 시행규칙 – 개인정보의 기술적 · 관리적 보호조치 기준 및 해설 – 개인정보보호 가이드
기술적 부문	• 개인정보 취급자에 의한 훼손 · 침해 또는 누설 • 기술적 · 관리적 조치 미비로 인한 개인정보누출 등 • 주민등록번호 등 타인정보의 훼손 · 침해 · 도용	– 본 가이드의 참조

3. 핸드북의 구성 및 활용방안

■ 핸드북의 구성

• 본 핸드북은 중소기업의 일반이용자, 시스템 관리자, 응용서비스 개발자, 개인정보보호 담당자가 개인정보보호를 위해 고려해야 할 기술적 보안사항에 대한 가이드라인 제공을 목적으로 개발하였으며, 총괄편, 일반사용자편, 시스템 관리자편, 응용서비스 개발편, 개인정보보호 피해신고 절차 및 대응 등 총5장으로 구성되어 있다.

※ 개인정보에 대한 관리적 보안 제외함

- 일반 이용자편에서는 일반 이용자 측면에서 개인정보보호를 위해 고려해야 할 PC 보안, 이메일 보안, 전자상거래시 보안 고려사항 등에 대한 가이드라인을 제공한다.

- 시스템 관리자편에서는 『정보통신망 이용촉진 및 정보보호 등에 관한 법률』제28조 (개인정보의 보호조치)와 관련하여 중소기업의 시스템 관리자가 이용자의 개인정보를 취급함에 있어서 개인정보의 안전성 확보에 필요한 기술적 · 관리적 조치의 이행지원을 위한 가이드라인을 제공한다.

- 응용서비스 개발편에서는 중소기업의 웹 어플리케이션 개발시 고려해야 할 보안사항에 대한 가이드라인을 제공한다.

– 개인정보보호 피해신고 절차 및 대응편에서는 중소기업의 개인정보보호 담당자가 고려해야 할 개인정보보호 피해신고 절차 및 대응방법에 대한 가이드라인을 제공한다.

• 본 핸드북은 일반 이용자 및 시스템 관리자의 이해를 돕기 위해 각 항목별로 "정보보호 현안과 예상 피해" 및 "보호대책"으로 나누어 기술하였다.

■ 핸드북의 활용

• 본 핸드북은 중소기업의 일반사용자, 시스템관리자, 어플리케이션 개발자, 개인정보보호 책임자가 각 항목을 적용하여 기업의 보안성을 강화하거나 또는 개인정보보호 교육용 교재로 활용이 가능하다.

구 분	활 용 방 안
일반사용자	– 일반이용자의 개인정보 유출방지를 위한 PC보안, 전자상거래 보안, 바이러스 및 스파이웨어 예방을 위한 기술 습득
시스템 관리자	– 개인정보 유출방지를 위한 서버보안(보안패치, 계정 및 암호관리, 권한관리), DB보안, 웹 보안 방안 기술 습득
응용서비스 개발자	– XSS방지, SQL Injection방지, File Upload/Download 방지 등 개인정보 유출방지를 위한 안전한 웹 개발 기술 습득
개인정보보호 담당자	– 개인정보보호를 위한 PC, 서버, 웹 보안 방법과 개인정보 피해신고 및 대응 절차 습득

• 본 핸드북에서 언급되지 않은 사항이나 기술적으로 자세한 사항은 다음의 참고자료를 참조할 수 있다.

– 정보통신망 이용촉진 및 정보보호 등에 관한 법률 및 시행령 · 시행규칙

– 개인정보의 기술적 · 관리적 보호조치 기준 및 해설

- 개인정보보호 핸드북
- 인터넷상의 개인정보보호를 위한 핸드북
- 중소기업 정보보호 가이드라인

제 2 장 일반 이용자편

II

Information Security

1. PC 관리의 기본을 지키자!

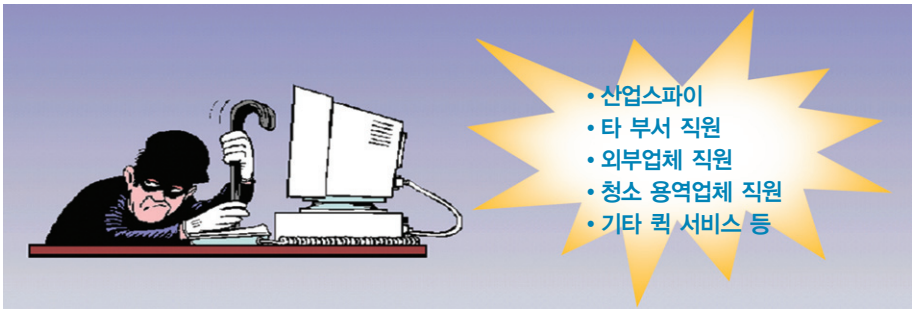
1.1 시스템 패스워드 설정하기

■ 정보보호 현안 및 예상 피해

• PC 접근을 통한 개인정보 유출

– 회사에서 사용하는 PC는 퇴근 또는 장시간 자리를 비울 경우 악의적인 내 · 외부인에 의해서 쉽게 접근할 수 있으며, PC의 시스템 패스워드를 설정하지 않을 경우 PC에 저장된 고객 정보, 급여 정보 등의 개인정보가 유출될 가능성이 높다.

〈그림 2-1〉 PC에 접근하여 개인정보를 유출



- 한 예로, 회사의 급여에 불만을 품은 결혼정보회사의 직원이 야근을 핑계로 모든 직원이 퇴근한 후 고객정보를 담당하는 직원 PC에서 고객정보 파일을 몰래 복사하여 경쟁회사로 팔아넘긴 사례가 있다.

■ 보호대책

• CMOS 패스워드 설정
- PC가 부팅할 때 설정하는 패스워드로 CMOS Setup 화면에서 패스워드를 설정할 수 있다.
- CMOS 패스워드 설정은 PC의 종류에 따라 조금씩 차이가 있을 수 있다.

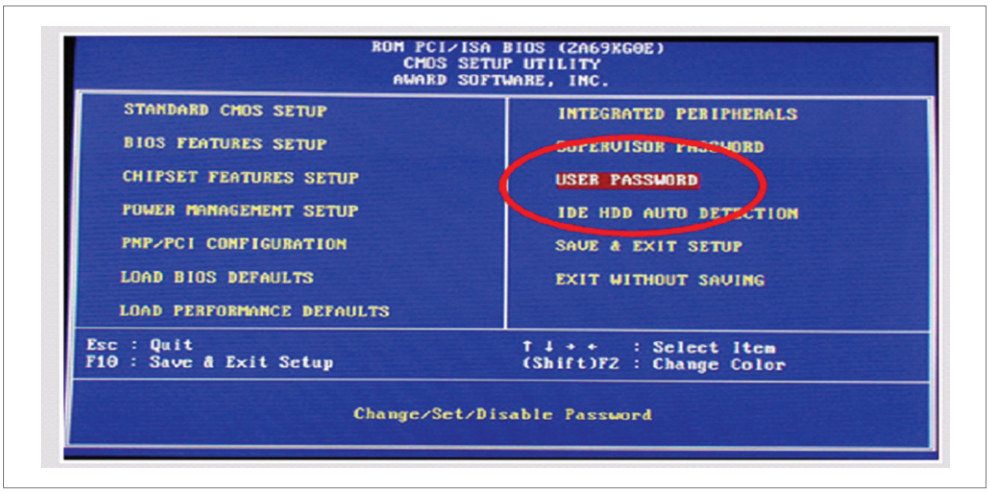
〈그림 2-2〉 PC종류에 따른 패스워드 설정 방법

PC(바이오스) 종류	암호설정법
Award	1. PC 부팅 2. [F2] 또는 [DELETE]키 3. CMOS Setup Utility 화면 4. BIOS Features setup 선택 5. security option설정을 system으로 변환 6. [ESC]키를 누르고 초기 화면으로 복귀 7. 초기화면의 Supervisor Password 항목에서 8.[enter]후 password 입력
Phoenix	1. PC 부팅 2. Phoenix BIOS Setup 화면 3. 메뉴 'Security' 선택 4. Set supervisor Password에 암호 입력 5. password on boot가 'Enabled' 인지 확인 6. EXIT로 이동 저장
Ami	1. PC 부팅 2. System setup 화면 3. Advanced에서 [enter] password check 설정 4. always 선택 [enter] 5. Supervisor Password에 암호 입력 6. [ESC]로 초기 화면으로 복귀

① 부팅시 초기화면에서 제조회사를 확인한 후 [F2] 혹은 [Delete] 키를 눌러 'CMOS' 셋업 화면으로 전환

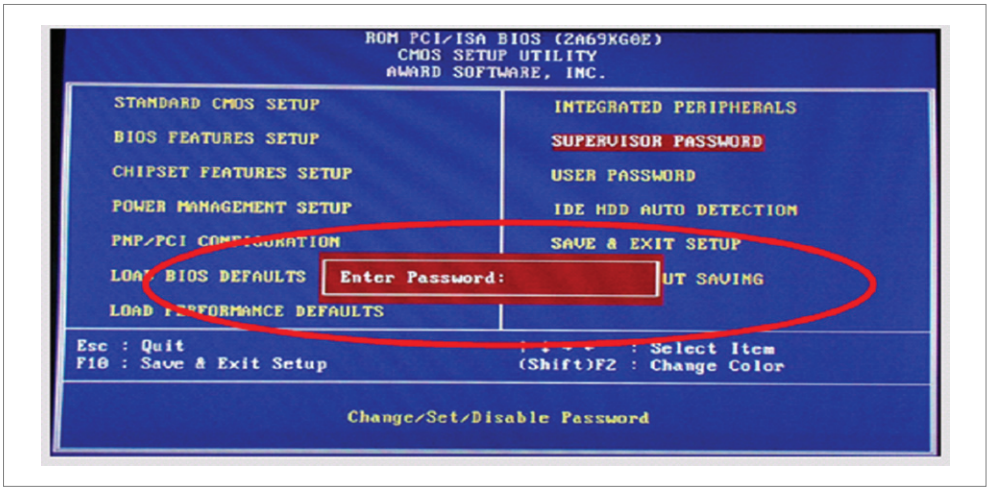
② CMOS 화면에서 [USER PASSWORD]를 선택

〈그림 2-3〉 CMOS 화면에서 패스워드 설정을 위한 메뉴 선택



③ 패스워드를 입력 후 CMOS 셋업을 저장하고 부팅

〈그림 2-4〉 CMOS 화면에서 패스워드 설정



• 로그인 패스워드 설정

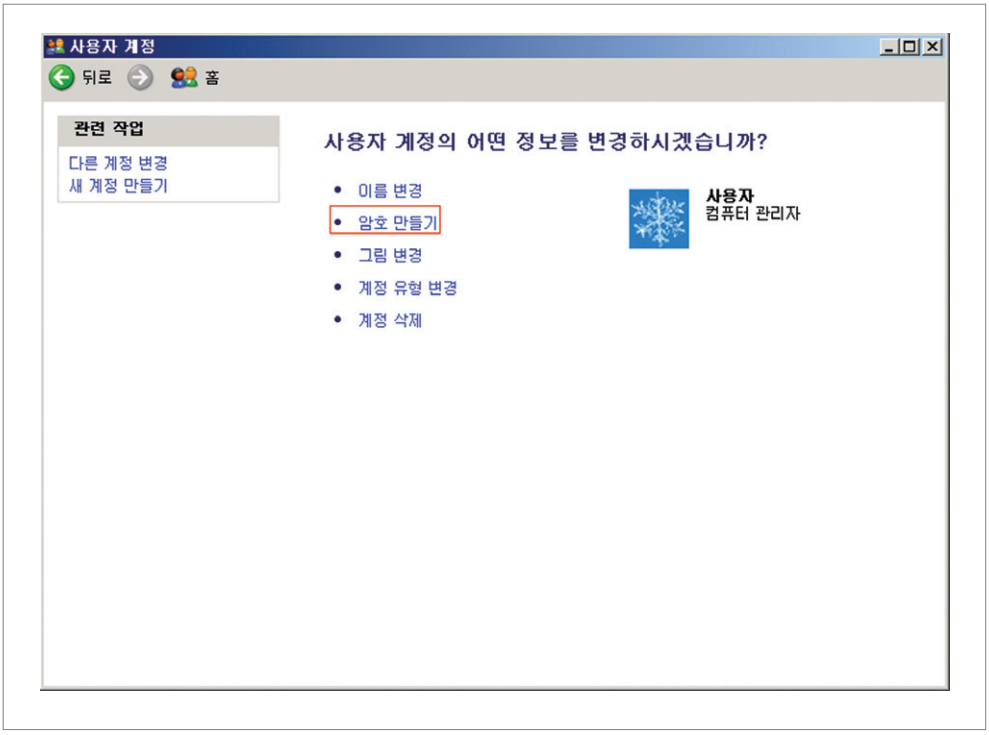
– 로그인 패스워드는 윈도우즈 상에서 사용자 계정에 따라 설정하는 패스워드로 PC에 등록된 사용자별로 패스워드를 설정해야 한다.

① PC화면 하단의 작업표시줄에서 [시작] ⇒ [설정] ⇒ [제어판] ⇒ [사용자계정]을 선택

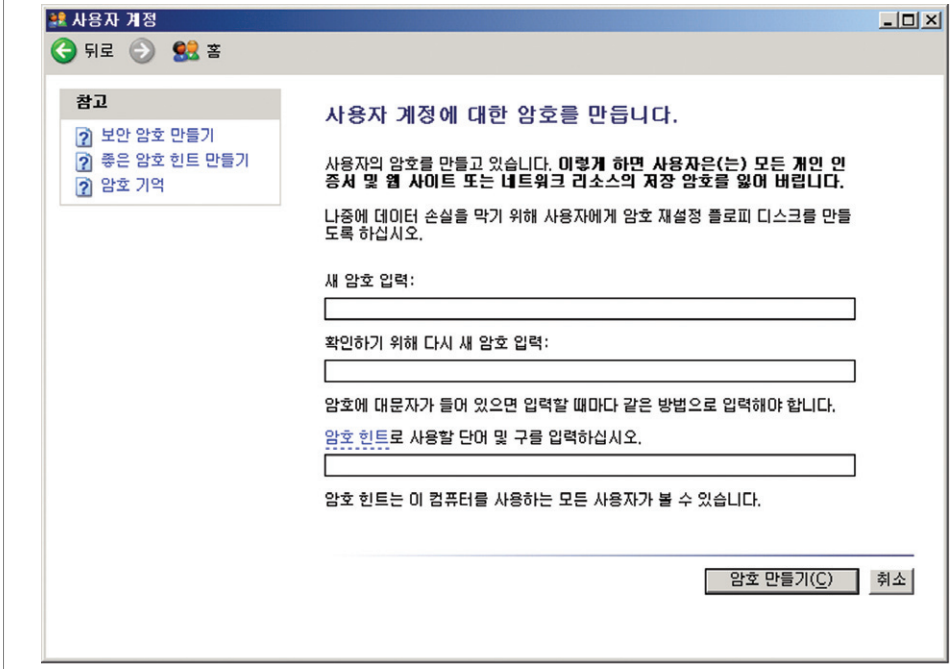
② 사용자계정 화면에서 암호를 설정할 계정을 선택

③ 선택한 계정에 대해서 암호 만들기를 선택한 후 암호를 입력

〈그림 2-5〉 선택한 사용자 계정에 대한 암호 만들기 선택



〈그림 2-6〉 선택한 사용자 계정에 대한 암호 만들기



※ 안전한 암호를 만들기 위해서는 7자리 이상, 특수문자(!@# 등), 숫자 혼합, 계정과 유사한 암호 사용 금지, 사전에 나와 있는 단어 사용 금지 등을 지킴

1.2 화면보호기 설정하기

■ 정보보호 현안 및 예상 피해

• 잠시 자리를 비운 사이에도 정보는 유출될 수 있다.
  – 휴식시간, 점심시간, 회의시간, 외부인 접대 등으로 인해 잠시 자리를 비우는 경우 대부분 컴퓨터를 켜둔 상태에서 자리를 비우게 된다.

이러한 경우 악의적인 내 · 외부인에 의해서 PC의 정보가 유출될 수 있어 주의해야 한다.

- 별도의 접견실이 없어 외부인이 사무실로 출입할 수 있는 환경을 가진 중소기업들의 경우 고객정보가 유출되기 쉬운 환경이다. (특히 물품 배송 업체, 소규모 쇼핑몰, 물품 판매 매장 등의 경우 고객관리 화면을 통해 개인정보가 유출될 가능성이 많음)

〈그림 2-7〉 화면으로 인한 정보 유출

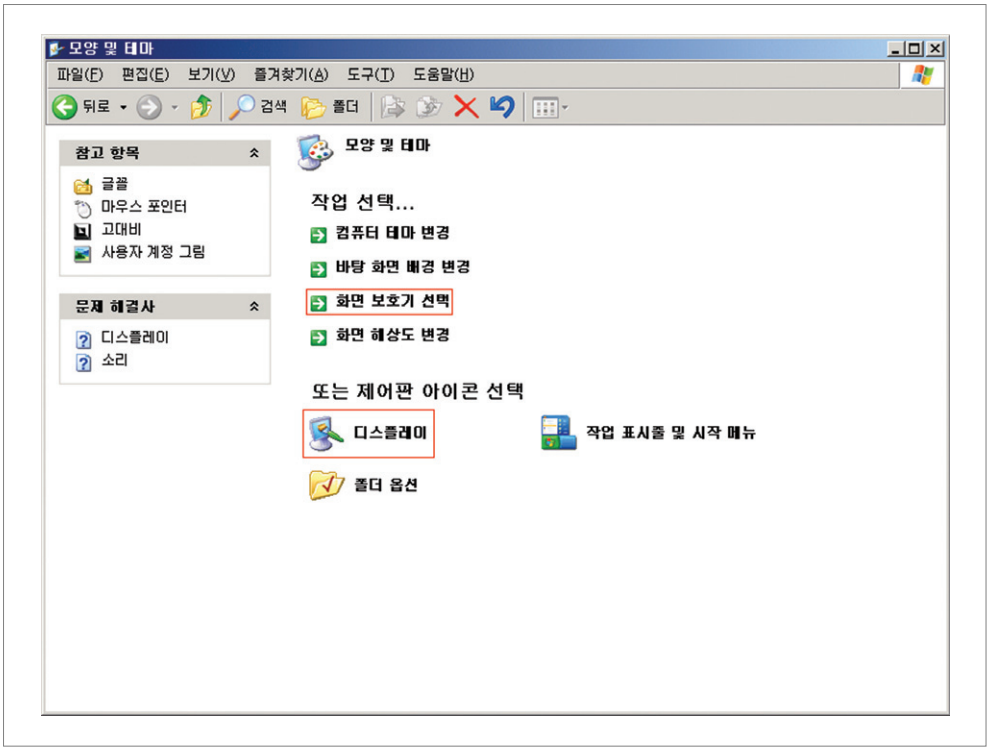
■ 보호대책

• 화면보호기 암호 설정

- PC를 사용하지 않을 경우 자동으로 화면보호기가 작동되게 하고, 화면보호기를 해지할 때 암호를 물어보게 설정하여 악의적인 PC 사용을 막아야 한다.

① PC화면 하단의 작업표시줄에서 [시작] ⇒ [설정] ⇒ [제어판] ⇒ [모양 및 테마] 또는 [디스플레이] ⇒ [화면보호기] 선택

〈그림 2-8〉 화면보호기 선택



② 또는 바탕화면에서 오른쪽 버튼을 누른 후 [속성] ⇒ [화면보호기] 선택

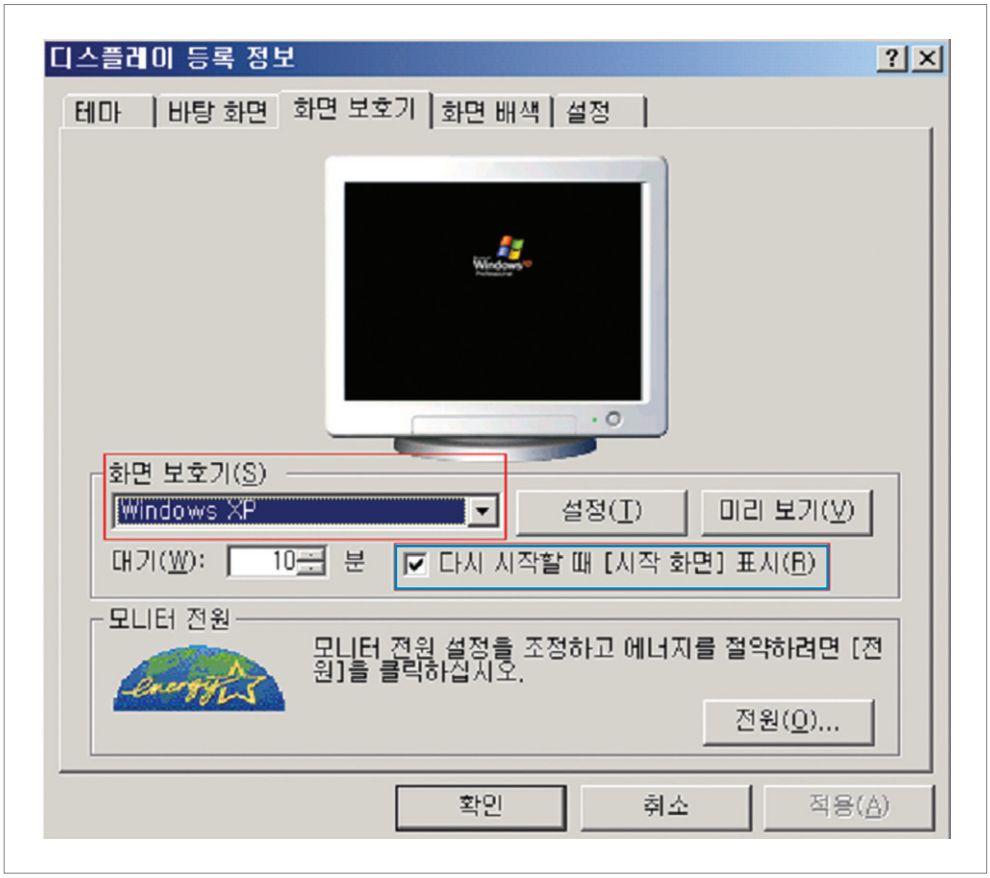
③ 화면보호기 설정 화면에서 원하는 화면보호기 선택

④ "다시 시작할 때[시작 화면] 표시"의 체크박스에 체크

⑤ "대기" 부분의 대기시간 설정은 너무 길지 않게 설정(5분 이내로 설정하는 것이 안전함)

⑥ [적용] ⇒ [확인] 버튼을 누름

〈그림 2-9〉 화면보호기 암호 설정



1.3 바이러스 엔진 업그레이드 및 검사 의무화하기

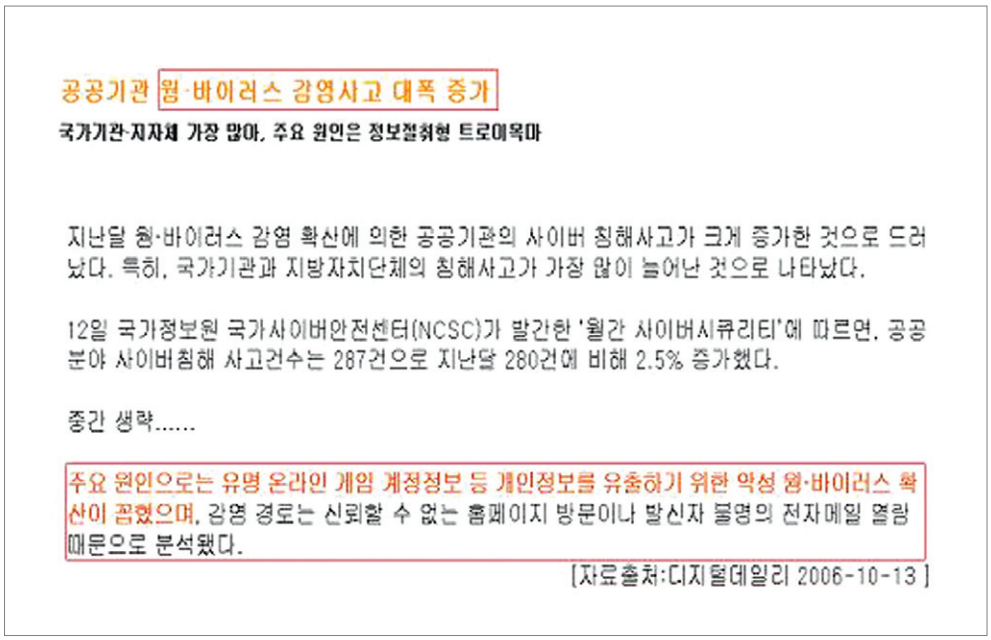
■ 정보보호 현안 및 예상 피해

• 바이러스에 의한 개인정보 유출

– 바이러스, 악성코드 등에 의해서 PC가 해킹을 당할 수 있을 뿐만 아니라

PC에 저장된 파일, 쿠키정보 등이 자신도 모르게 유출될 수 있다.

- 근래에는 PC에 장애를 주는 바이러스나, 악성코드 보다는 PC에 저장된 정보를 수집하기 위해 무작위로 바이러스를 배포하고 이를 통해 개인 정보를 수집하여 금전적인 이득을 취하려는 경향이 부쩍 늘어나고 있는 추세이다.



공공기관 웜·바이러스 감염사고 대폭 증가

국가기관·지자체 가장 많아, 주요 원인은 정보절취형 트로이목마

지난달 웜·바이러스 감염 확산에 의한 공공기관의 사이버 침해사고가 크게 증가한 것으로 드러났다. 특히, 국가기관과 지방자치단체의 침해사고가 가장 많이 늘어난 것으로 나타났다.

12일 국가정보원 국가사이버안전센터(NCSC)가 발간한 '월간 사이버시큐리티'에 따르면, 공공분야 사이버침해 사고건수는 287건으로 지난달 280건에 비해 2.5% 증가했다.

중간 생략.....

주요 원인으로는 유명 온라인 게임 계정정보 등 개인정보를 유출하기 위한 악성 웜·바이러스 확산이 꼽혔으며, 감염 경로는 신뢰할 수 없는 홈페이지 방문이나 발신자 불명의 전자메일 열람 때문으로 분석됐다.

[자료출처:디지털데일리 2006-10-13]

■ 보호대책

※ 본 대책에서는 V3, 바이로봇을 예로 설명함

• 바이러스 엔진 업그레이드 및 검사 의무화

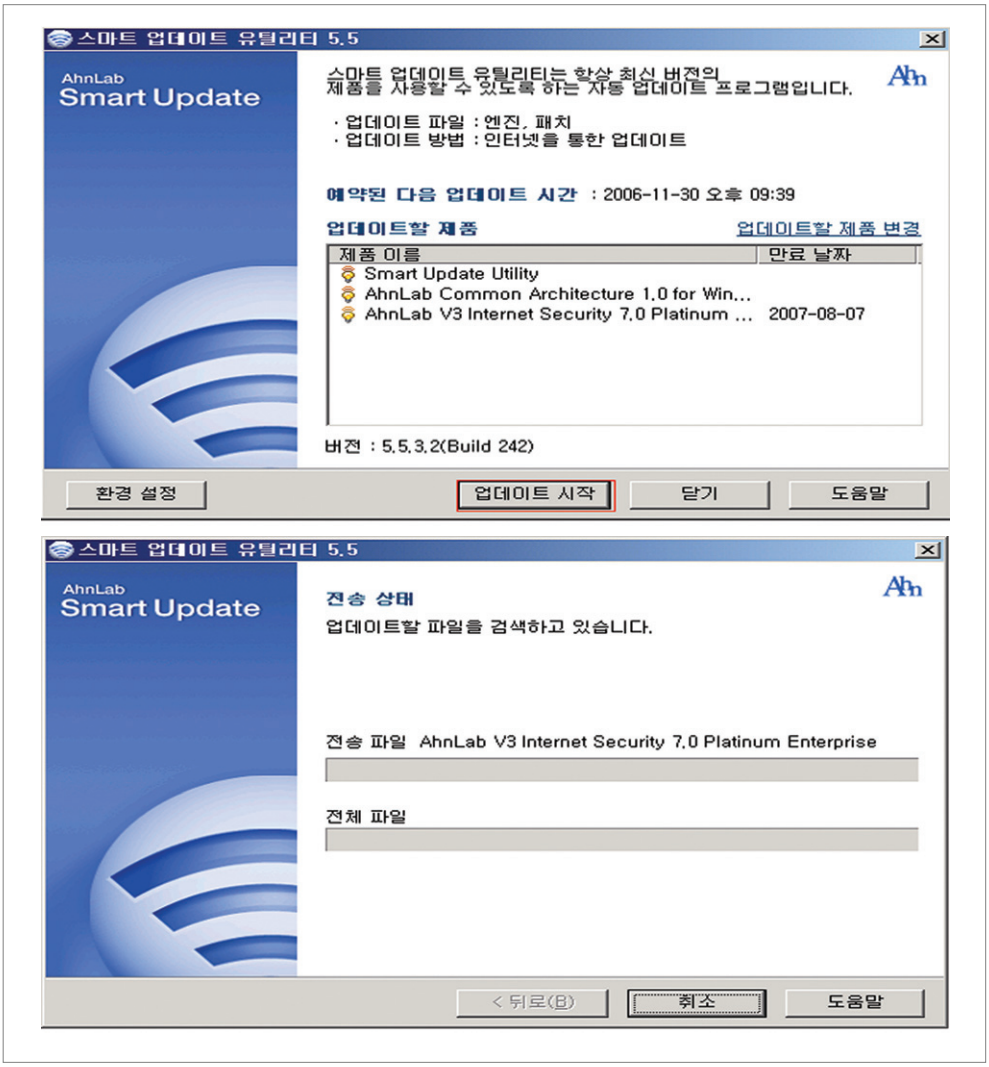
- PC 사용에 있어서 바이러스 백신을 반드시 설치하고 이에 따른 엔진을 최신 버전으로 업그레이드해야 한다.
- 대부분의 PC 사용자들은 바이러스 백신만 설치하면 해킹 피해를 막을 수 있다고 생각하고 바이러스 엔진 업그레이드를 소홀히 하는 경향이 있으나

급속도로 진화하는 바이러스 및 악성 코드를 방지하기 위해서는 신속한 바이러스 엔진 업그레이드 및 정기적인 검사를 해야 한다.

• 백신 프로그램별 업데이트 방법

– V3

〈그림 2-10〉 V3 엔진 업데이트



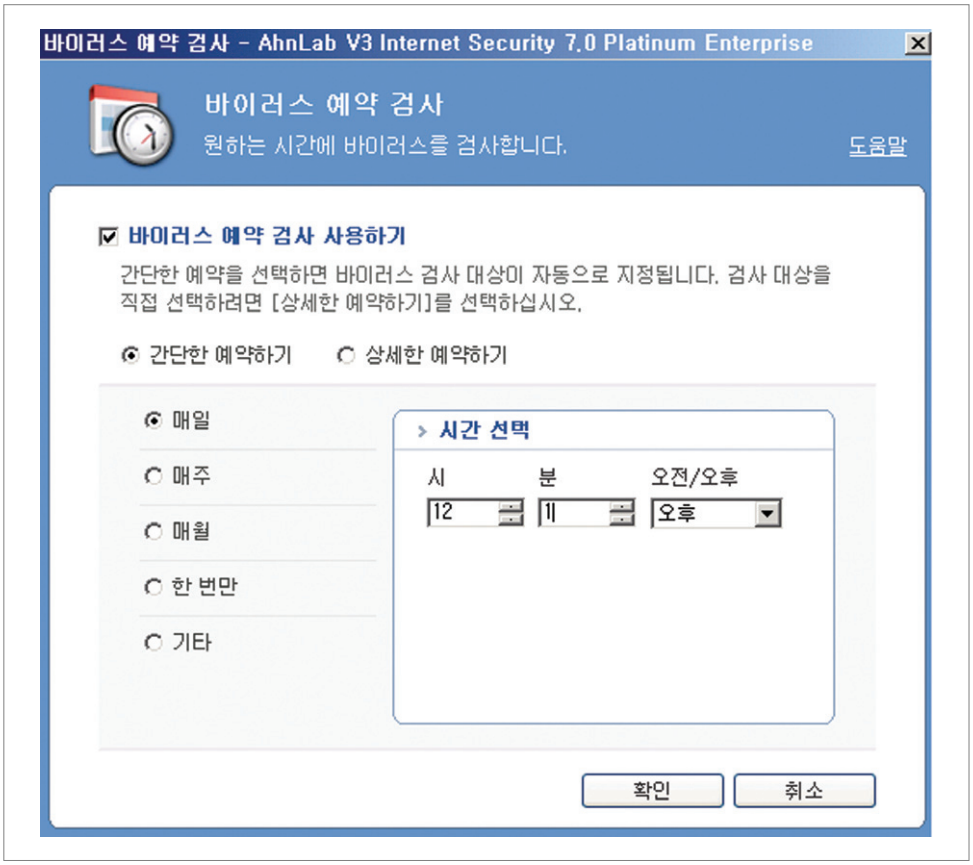
① V3 백신을 실행하여 [업데이트] 부분을 클릭하여 스마트 업데이트 유틸리티 실행

② 스마트 업데이트 유틸리티에서 [업데이트 시작] 버튼을 클릭하여 업데이트 실행

※ 지속적인 업데이트를 위해서는 스마트 업데이트 유틸리티에서 [환경설정] ⇒ [예약 설정]에서 자동으로 매일 일정한 시간에 업데이트를 수행하도록 설정함

③ V3에서 [바이러스 검사] ⇒ [예약 검사] 선택 후 예약된 시간에 자동으로 바이러스 검사를 수행하도록 설정

〈그림 2-11〉 자동으로 바이러스 검사 수행(V3)

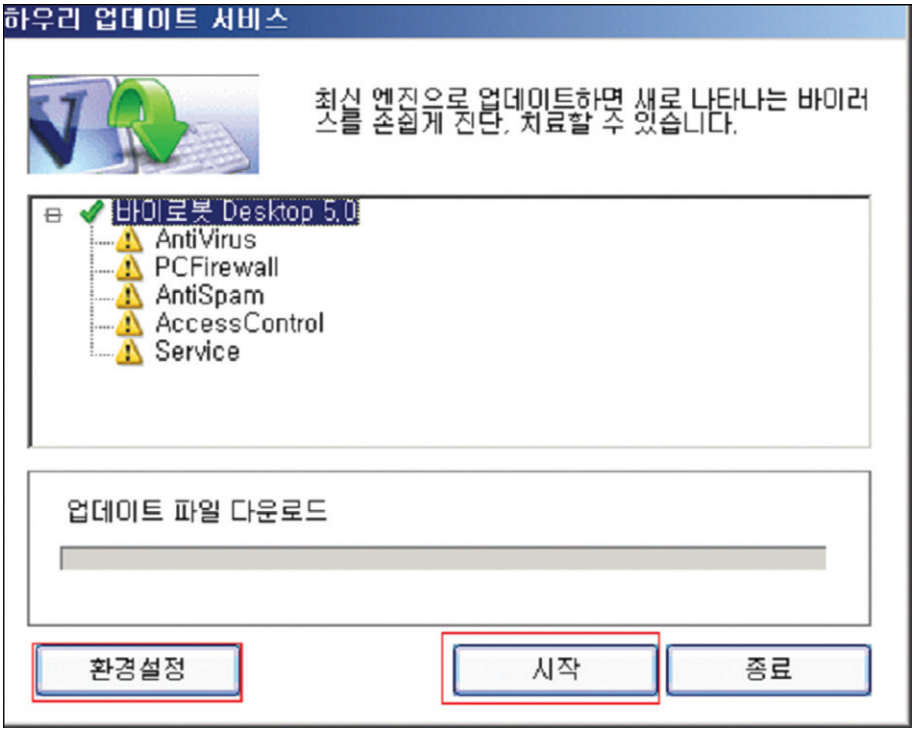


– 바이로봇

① 바이로봇 백신을 실행하여 [업데이트] 부분을 클릭하여 하우리 업데이트 서비스를 실행

② 하우리 업데이트 서비스 화면에서 [시작] 부분을 클릭하여 업데이트 실행

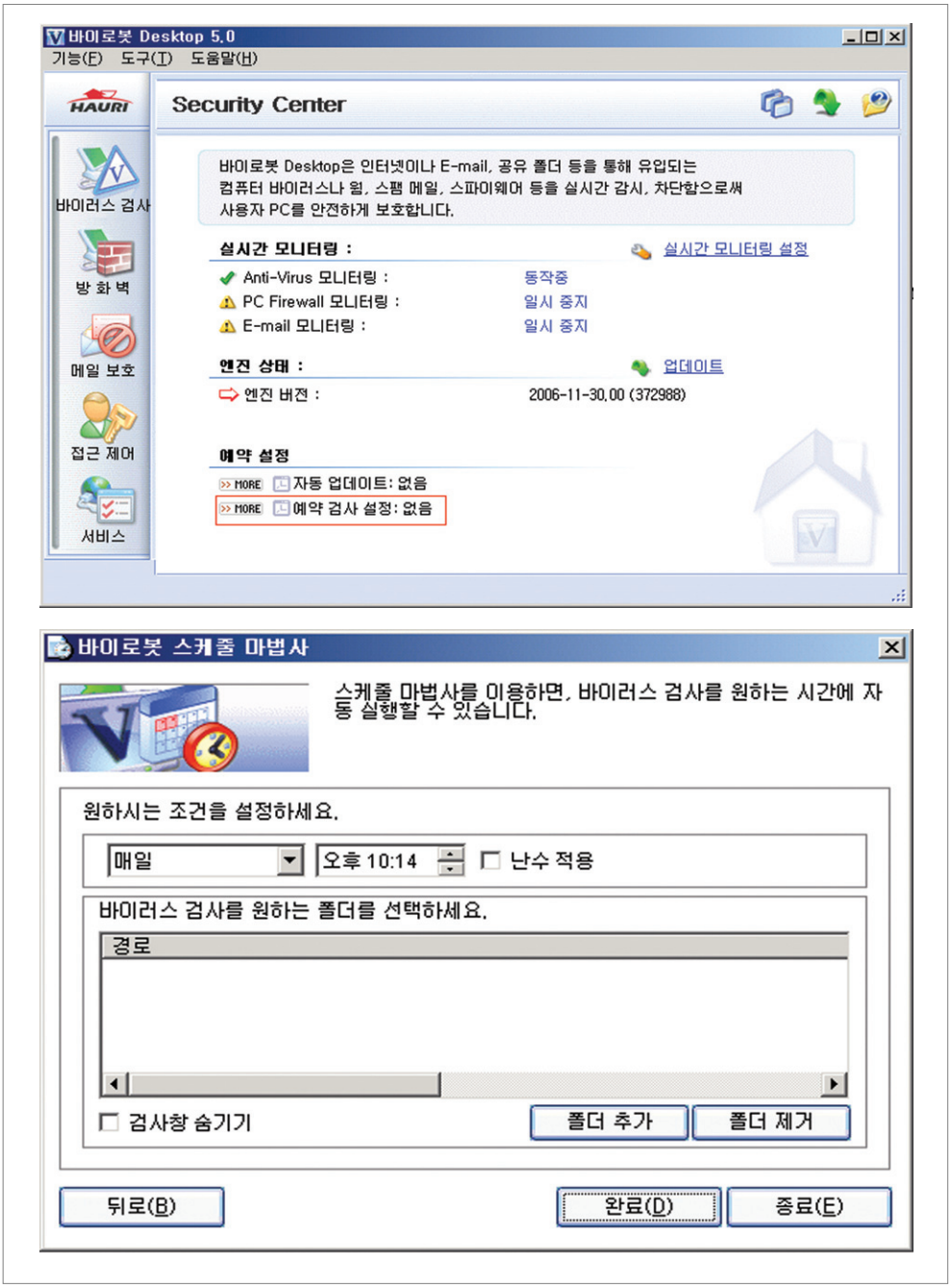
〈그림 2-12〉 바이로봇 엔진 업데이트



※ 지속적인 업데이트를 위해서는 하우리 업데이트 서비스에서 [환경설정]에서 [자동 업데이트 설정]을 체크하고 일정한 시간 마다 업데이트를 수행하도록 설정함

③ 바이로봇에서 [예약검사 설정] ⇒ [추가] 버튼을 클릭한 후 예약된 시간에 자동으로 바이러스 검사를 수행하도록 설정

〈그림 2-13〉 자동으로 바이러스 검사 수행(바이로봇)



2. 공유폴더는 최소한으로 하자!

■ 정보보호 현안 및 예상 피해

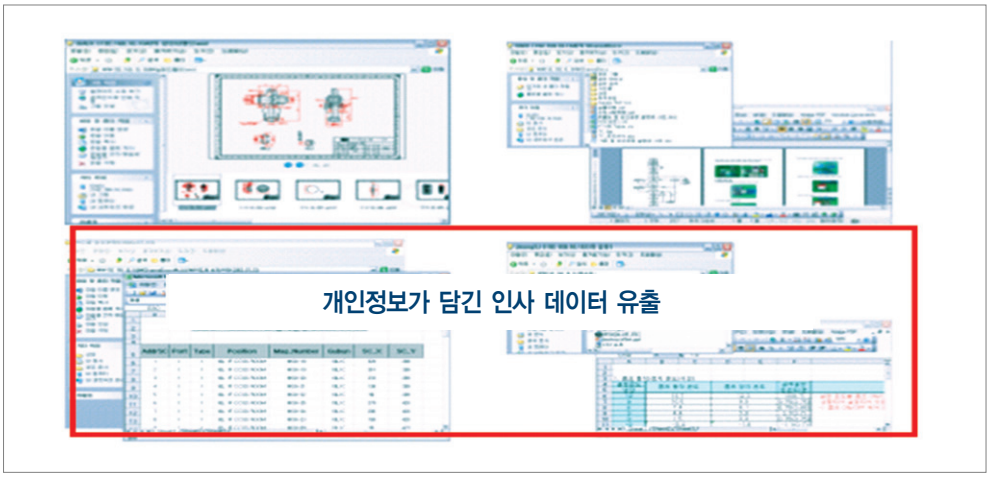
• 공유폴더를 이용한 정보 유출

– 업무의 효과적 수행을 위하여 정보를 공유할 필요성은 매우 크나, 안전한 정보 공유가 이루어지지 않는다면 막대한 피해가 발생할 수 있다.

– 내부 직원 및 외부 직원들도 대부분 PC를 사용하고 있으며, 이러한 사용자들이 별도의 해킹 지식 없이도 손쉽게 중요 정보에 접근할 수 있는 방법이 바로 암호가 설정되지 않은 공유 폴더에 접근하는 것이다.

– A컨설팅 업체에서 중소기업 약 30곳을 대상으로 PC에 대한 공유 폴더 취약점을 점검한 결과 50% 이상이 암호를 설정하지 않고 사용하는 것으로 조사되었으며, 중요기술정보 뿐만 아니라 인사정보 등 개인정보가 담긴 문서들이 공유 폴더에서 발견되었다.

〈그림 2-14〉 공유폴더를 통한 중요정보 유출

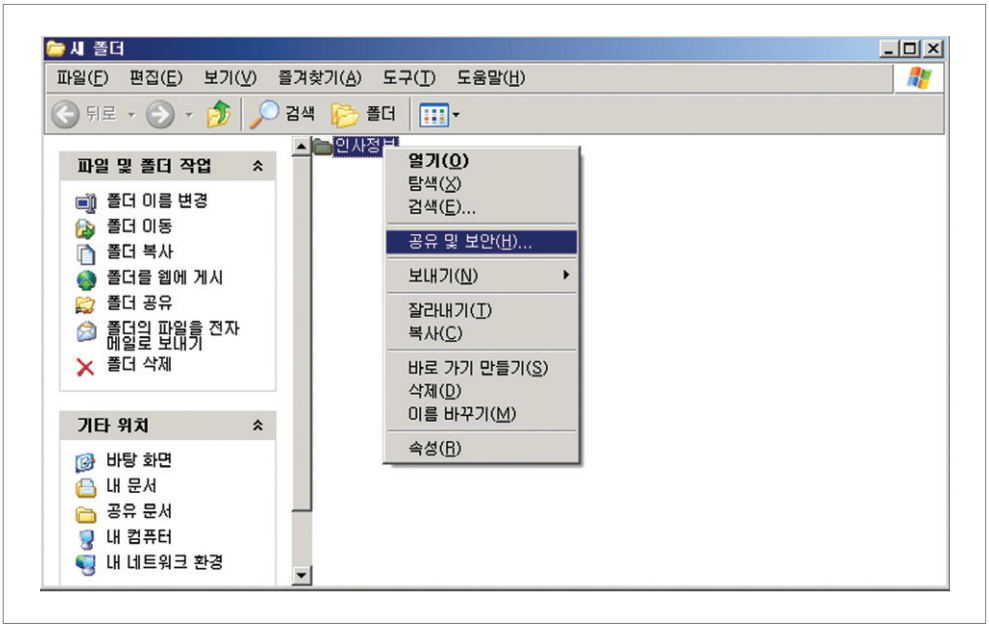


■ 보호대책

• 공유폴더는 최소한으로 하고 필요시 반드시 암호설정
  – 공유폴더는 정보의 공유가 필요한 때에만 사용하고 사용이 끝나면 공유를 해제해야 한다.
  – 공유폴더를 사용할 경우에는 반드시 암호를 설정하여 허가된 인원만이 접근할 수 있도록 조치해야 한다.

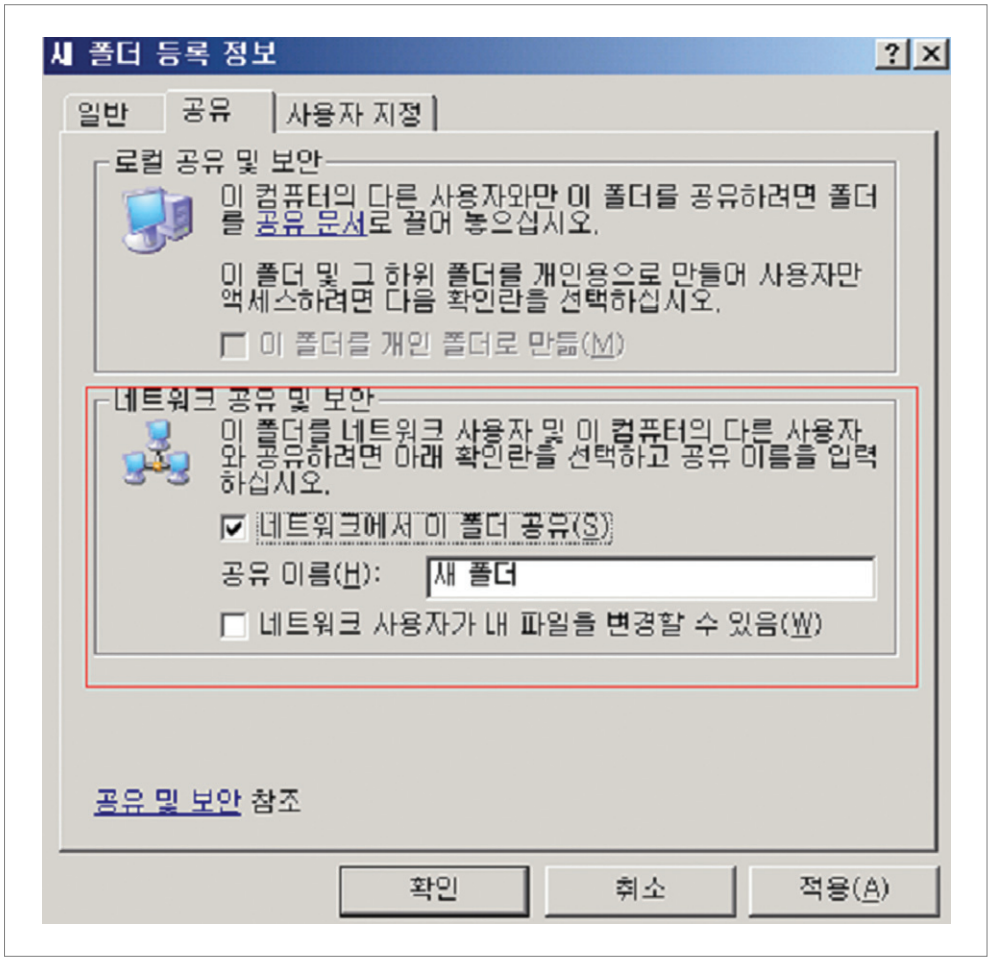
• 공유폴더의 암호설정 방법은 다음과 같다. (WindowsXP Home Edition 기준으로 작성됨)
  ① 공유할 폴더를 선택하고 오른쪽 마우스 클릭

〈그림 2-15〉 폴더 공유 설정



② [폴더 등록정보]의 공유 탭에서 [네트워크 공유 및 보안]
⇒ [네트워크에서 이 폴더 공유] 체크 후 [적용] 버튼을 누름

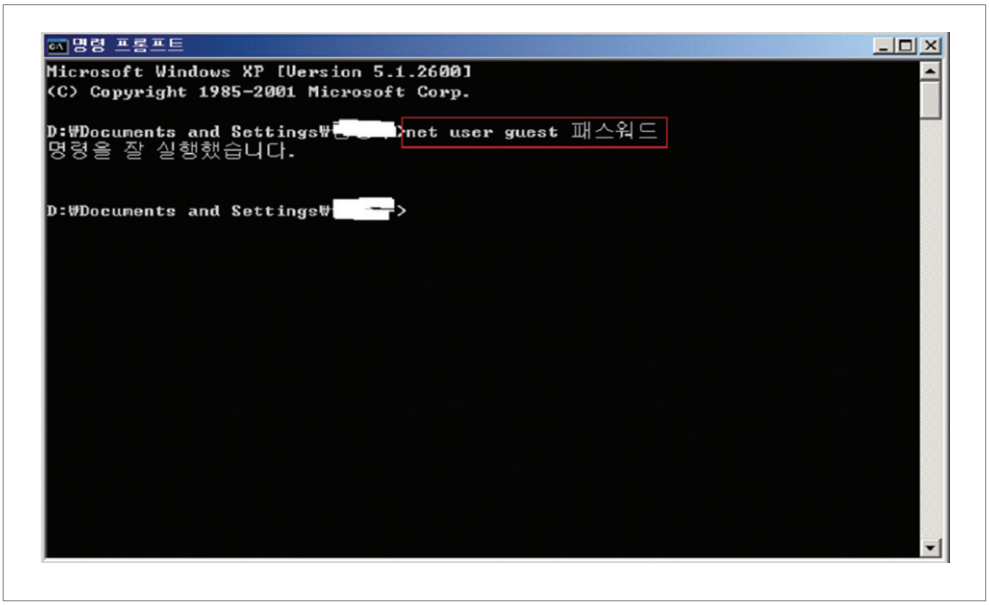
〈그림 2-16〉 폴더 공유



③ 공유된 폴더는 누구나 접근할 수 있으므로 guest 계정에 암호를 설정하여 공유폴더 접근을 제한. PC화면 하단의 작업표시줄에서 [시작] ⇒ [프로그램] ⇒ [보조 프로그램] ⇒ [명령 프롬프트] 선택

④ [명령 프롬프트]에서 “net user guest 패스워드”를 입력하고 Enter 키를 누름

〈그림 2-17〉 공유 폴더에 접근 가능한 guest 계정 패스워드 설정



※ 패스워드 부분에 원하는 암호를 입력함

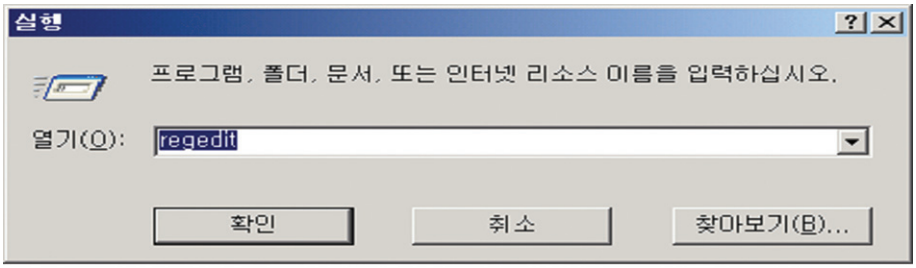
• 숨은 공유 폴더 해제

– Windows 설치시 자동으로 숨은 공유 폴더가 생성된다. 따라서 사용자 계정에 대한 암호 유출시 이렇게 생성된 폴더는 PC 전체에 대해 접근이 가능한 경로를 제공한다.

• 숨은 공유 폴더의 해제 방법은 다음과 같다. (WindowsXP Home Edition 기준으로 작성됨)

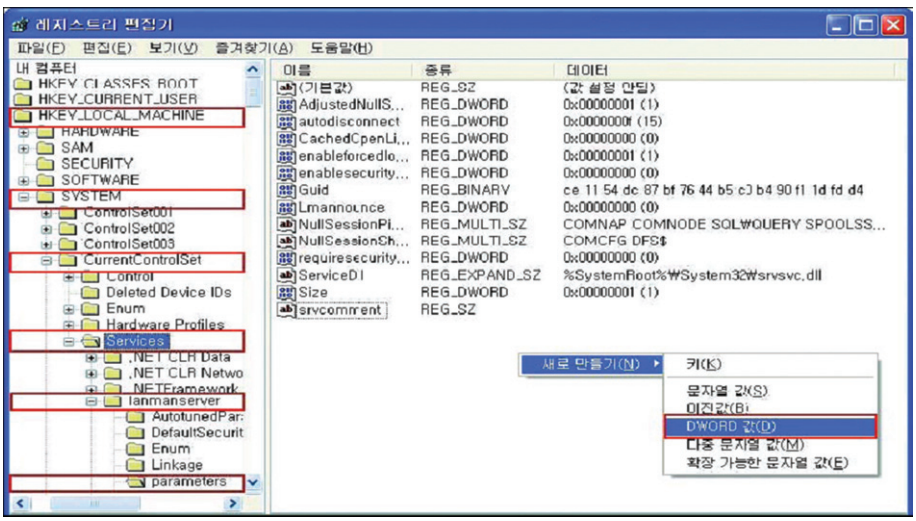
① PC화면 하단의 작업표시줄에서 [시작] ⇒ [실행] 선택 후 실행 화면에서 regedit 입력 후 [확인] 버튼을 누름

〈그림 2-18〉 regedit 실행



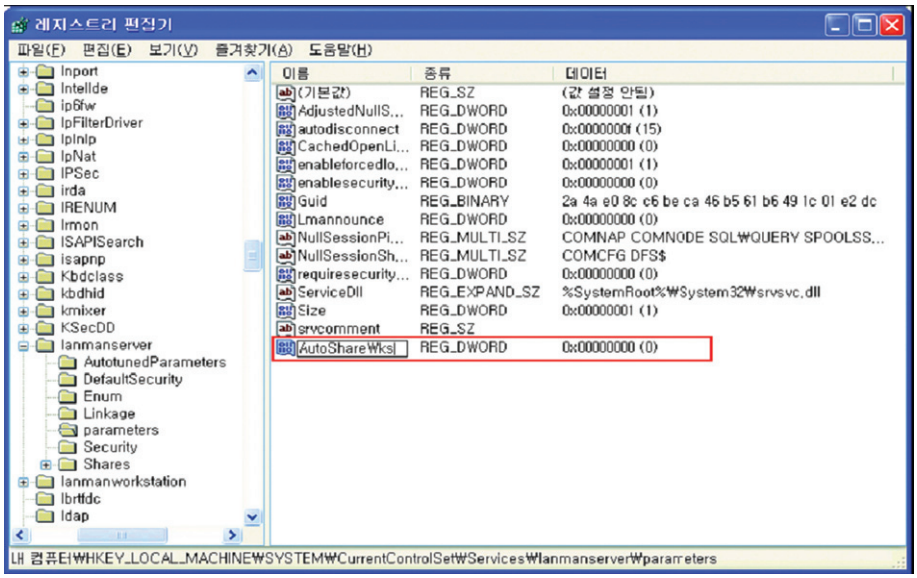
② 레지스트리 편집기에서 [HKEY_LOCAL_MACHIN\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters] 선택 후 오른쪽 마우스 버튼을 클릭하여 [새로 만들기] ⇒ [DWORD 값] 선택

〈그림 2-19〉 레지스트리 값 입력



③ 입력 값 설정 화면에서 [이름] 필드에 [AutoShareWks]를 입력하고 Enter 키를 누름

〈그림 2-20〉 레지스트리 값 추가



④ 숨겨진 공유 폴더를 제거하기 위해 PC화면 하단의 작업표시줄에서 [시작] ⇒ [프로그램] ⇒ [보조 프로그램] ⇒ [명령 프롬프트] 선택 후 다음 명령어를 실행

```
C: net share C$ /delete
C: net share D$ /delete
C: net share Admin$ /delete
```

3. 전자거래시, 개인정보보호는 이렇게~

3.1 피싱 주의

■ 정보보호 현안 및 예상 피해

• 피싱으로 인한 개인정보 유출 무방비

– 피싱이란 개인정보(Private data)와 낚시(Fishing)의 합성어로 인터넷 이용자들에게 유명 회사를 사칭하는 이메일을 보내고, 위장된 홈페이지에 접속하여 계좌번호, 주민등록번호 등의 개인정보를 입력하도록 유도하여 이들 정보를 이용해 금융사기를 일으키는 신종 사기 수법이다.

〈그림 2-21〉 피싱 사례

〈C게임사 홈페이지 사칭화면〉

■ 보호대책

• 신뢰된 경우에만 개인정보를 제공해야 한다.
  – 개인정보의 제공은 최소로 하고 제공이 필요한 경우 신뢰된 사이트인지를 먼저 확인해야 하며, 메일 링크를 사용하지 말고 직접 사이트에 접속하여 제공한다.
    ① 은행, 카드사 등에 직접 전화를 걸어 이메일이 안내하는 사항이 사실인지를 확인
    ② 이메일에 링크된 주소를 바로 클릭하지 말고, 해당 은행, 카드사 등의 홈페이지 주소를 인터넷 주소창에 직접 입력하여 접속
    ③ 출처가 의심스러운 사이트에서 경품이 당첨되었음을 알리는 경우 직접 전화를 걸어 사실인지를 확인하고, 사실인 경우에도 가급적이면 중요한 개인정보를 제공하지 않음
    ④ 피싱이라고 의심되는 메일을 받았을 경우 해당 은행, 카드사, 쇼핑몰 및 아래 기관에 신고

      – 한국정보보호진흥원 전화 118 또는 1336
        E-mail:phishing@certcc.or.kr
      – 경찰청 사이버테러대응센터 (02) 3939-112
      – 피싱 신고 접수 사이트 : http://www.krcert.or.kr

    ⑤ 은행, 신용카드, 현금카드 등의 내역이 정확한지 정기적으로 확인

3.2 공인인증서(또는 ISP) 사용하기

■ 정보보호 현안 및 예상 피해

• 전자거래시 개인정보의 노출 위험

– 인터넷을 통한 전자거래시 다량의 개인정보가 노출될 가능성이 있으며, 특히 대금 등의 결제를 수행할 경우 카드번호, 주민등록번호, 계좌번호 등 매우 민감한 개인정보가 노출될 수 있다.

올해로 10주년을 맞는 국내 전자상거래 시장은 90년대 1조원 미만에서 현재 약 13조원으로 급성장했다. 사용자 수도 지난해 3300만 명으로 증가한 인터넷 사용자 중 51.2%가 인터넷에서 물건을 구매할 정도로 늘어났다.

이처럼 전자상거래를 통해 오가는 물품과 정보의 규모가 커짐에 따라 금전적인 이득을 보려 하는 해커들의 시도 또한 갈수록 증가하고 있다. 한국정보보호진흥원의 통계에 따르면 2006년 5월 국내 웹사이트가 피싱 경유지로 악용된 사례가 130건으로 전년 동월 대비 34%,2006년 4월 대비 8.3% 증가했다. 또한 온라인 뱅킹에서도 은행 온라인 사이트에 해킹 프로그램을 설치해 개인 금융 정보를 빼내는 범죄가 지속적으로 발생하고 있는 것으로 밝혀졌다.

[자료출처:매일경제]

■ 보호대책

• 공인인증서를 사용하자.

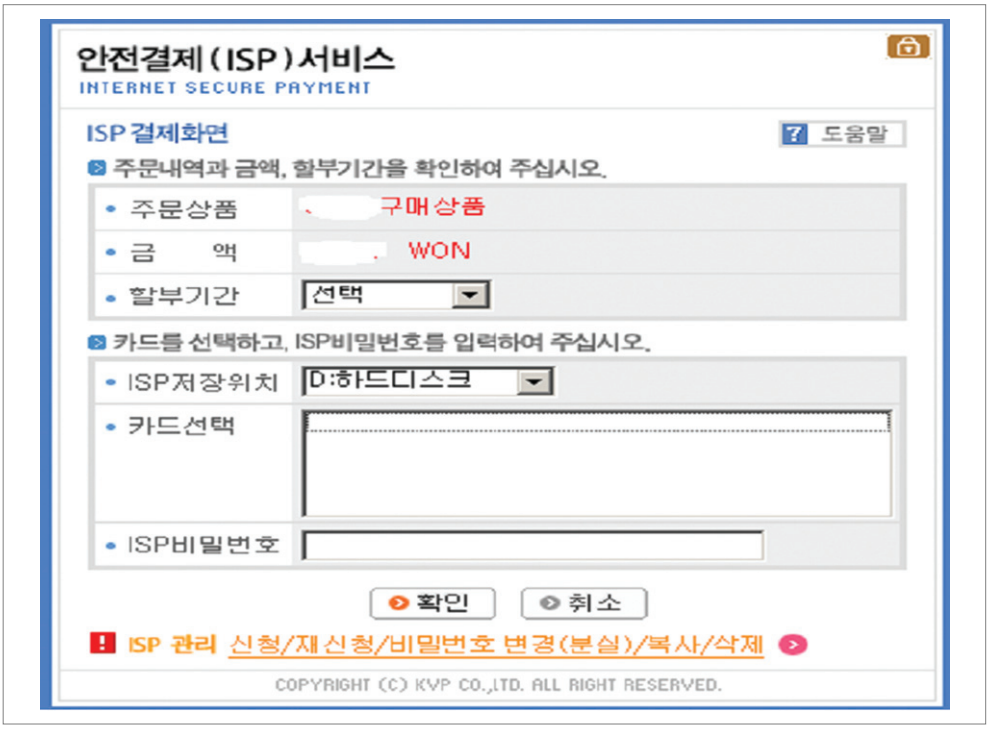
– 공인인증서란 개인이 현실세계에서 중요한 거래시 계약서에 날인 후 인감증명서를 첨부하듯이, 네트워크 통신의 경우도 컴퓨터나 개인에 상관없이 자기 자신임을 증명하기 위하여 각자 인감에 해당하는 개인키와 이에 대응하는 공개키를 인증기관에게 등록하는 것으로써, 인감증명서와 마찬가지로 인증기관(CA)이 등록요청된 정보에 대하여

〈그림 2-22〉 인증서의 개념

가입자 본인에 대한 신원확인 후 발행함으로써 컴퓨터 또는 개인 신분 증명시에 사용하는 증명서를 뜻한다.

- ISP(Internet Secure Paymont)란 인터넷 전자상거래시 개인신용정보 유출을 차단하는 신용카드 결제서비스로서 안전결제(ISP)서비스 비밀번호만 입력하여 결제하도록 함으로써 신용카드번호 등이 유출되는 것을 사전에 방지하는 방법이다.

〈그림 2-23〉 ISP를 이용한 결재



3.3 키로깅 방지하기

■ 정보보호 현안 및 예상 피해

• 키로깅에 주의하자

– 키로깅이란 PC에 해킹 프로그램을 몰래 숨겨 놓아 PC를 사용하는 사람이 키보드로 입력한 내용을 저장하였다가 유출하는 행위를 말한다.

– 인증서 등의 강력한 인증 수단을 사용하더라도 키로깅에 의해서 인증서 암호가 노출될 수 있으며, 특히 게임방, 휴게실 등에서 사용하는 공용 PC의 경우 이러한 위험에 쉽게 노출될 수 있다.

– 최근 바이러스나 악성코드도 키로깅 기능을 가지고 있는 것이 많으며, 수집한 개인정보를 자동으로 해커에게 전송하는 기능을 가지고 있다.

21일 정통부와 관련 업체에 따르면 최근 국내 온라인 게임 업체 및 이용자를 대상으로 해킹 피해가 급증해 피해사례를 분석하고 방지 대책을 수립하는 민관 협조 체계가 만들어진다. 이번 협조 체계 구축은 최근 끝난 국제게임산업전시회 'G스타'에서 게임업체 CEO들이 진대제 장관의 간담회시 중국발 해킹에 대한 해결방안 모색을 건의, 이에 대한 후속 조치다.

중략…

안철수연구소에 따르면 올 한해 동안 키로깅 방식으로 인기 온라인 게임 계정을 훔쳐내 이메일 주소나 FTP(파일전송규약)에 이를 전송하는 트로이목마가 다수 등장했다. 이 가운데 리니지핵 트로이목마는 신고 순위 상위에 오를 만큼 맹위를 떨쳤다. 특정 웹사이트를 해킹해 트로이목마를 심어놓고 취약점이 있는 PC에서 웹사이트에 접속했을 때 자동 설치되게 한 일이 발생하는 등 온라인 게임이 해킹의 주된 표적으로 자리 잡았다

[자료출처: 전자신문]

■ 보호대책

• 키로깅 방지 프로그램 사용

– 키로깅 프로그램은 대부분 악성코드 제거 프로그램이나, 바이러스 백신에 의해서 탐지되고 제거될 수 있으므로 이러한 프로그램을 설치하고 실시간 감시 기능을 활성화한다.

– 키보드 보안 프로그램을 설치하여 키보드에서 입력하는 값을 실시간으로 암호화하여 PC로 전달하는 개인정보를 해킹 툴로부터 보호해야 한다.

4. email을 통한 바이러스 감염을 막자!

4.1 Outlook Express 바이러스 방지 기능 설정하기

■ 정보보호 현안 및 예상 피해

• 메일을 통한 바이러스 감염 및 전파

– 사용자가 수신하는 메일중에는 단순한 광고성 메일도 있지만 바이러스나 악성 코드가 첨부된 메일도 수신된다. 따라서 보안 솔루션을 설치하지 않은 중소기업의 경우 상당히 많은 바이러스에 감염되고 있다.

○ 10월의 신종 웜·바이러스는 지난달에 비해 감소하였으며, 주요 변종으로는 전월과 같이 메일의 첨부파일 실행으로 전파되며 감염될 경우 백도어를 생성하고 트로이목마, 스파이웨어를 다운로드하여 개인정보를 유출하는 특징을 가지는 Win32/Stration.worm 변종이 계속적으로 발생하고 있다.

○ 10월 전체 웜·바이러스 신고는 892건으로 전월에 비하여 3.1% 증가하였다. 이번 달에는 특정 게임 아이디/비밀번호을 유출하는 LineageHack에 의한 피해신고가 1위를 차지하였으며 이메일로 감염되는 Bagle변종웜에 의한 피해가 2위를 차지하였다.

※ 자료출처 : KISA

■ 보호대책

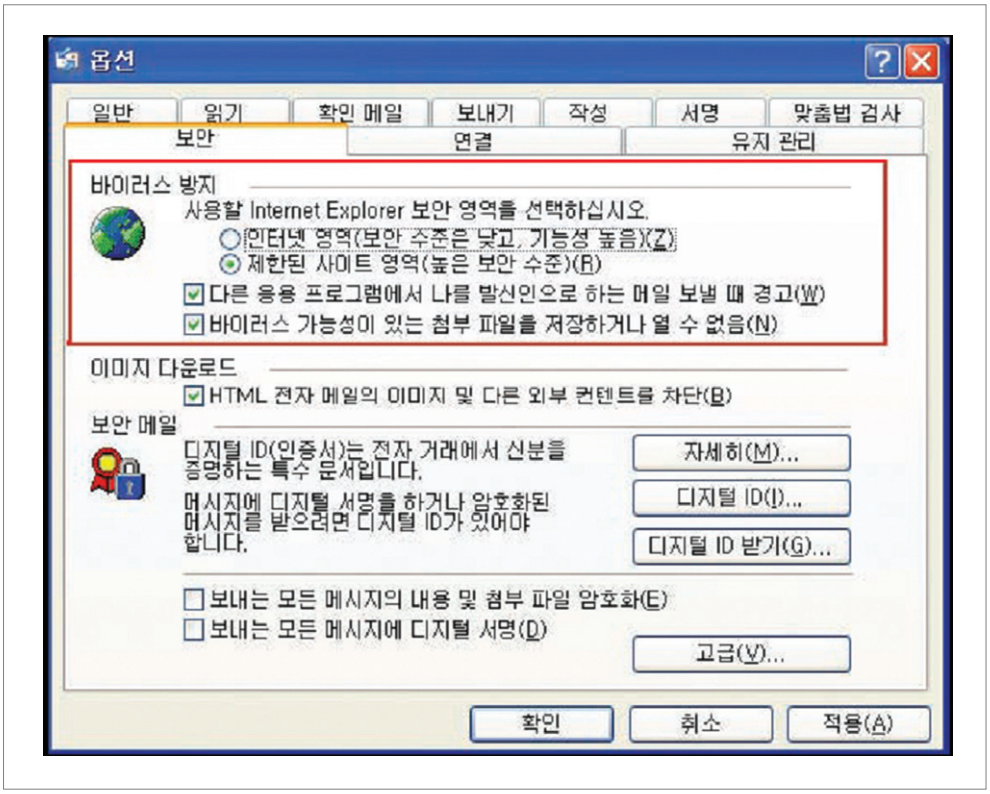
• Outlook Express 바이러스 방지 기능 설정하기

– 바이러스에 감염된 메일을 수신하였을 경우 바이러스가 실행되지 않도록 Outlook Express에 보안 설정을 해야 한다.

① Outlook Express의 [도구] ⇒ [옵션] ⇒ [보안] 탭 선택

② [보안] 탭 화면에서 바이러스 방지 영역을 다음과 같이 선택

〈그림 2-24〉 Outlook Express 보안설정



※ 바이러스 백신의 메일보안 기능을 병행해서 사용하고, 의심스러운 메일은 반드시 바이러스 백신 등을 통해 검사를 해야 함

4.2 메일 미리보기 방지하기

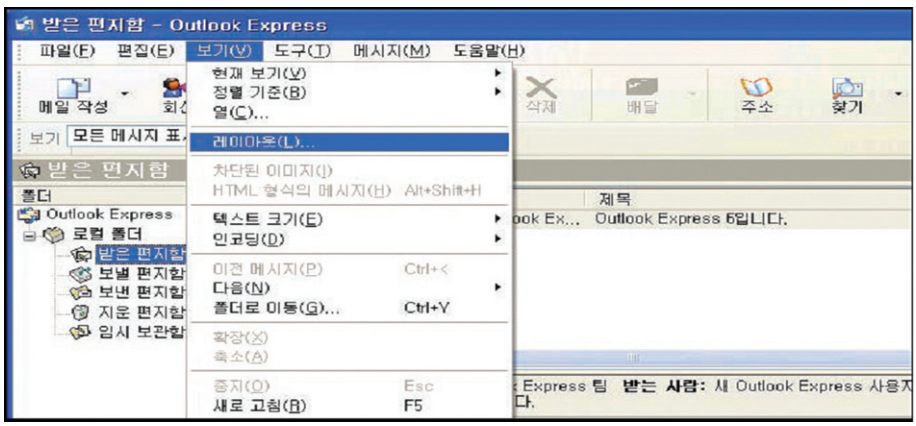
■ 정보보호 현안 및 예상 피해

• 메일을 읽는 것만으로도 개인정보는 유출될 수 있다.
  – 악성코드나 바이러스에 감염된 메일은 사용자가 읽는 것으로도 실행되고 이를 통해 개인정보의 유출이 가능하다.
  – Outlook Express에서 메일 미리보기가 설정 되어 있으면 의심되는 메일을 삭제하기 위해 선택만 하여도 메일 읽기가 되므로 위험하다.

■ 보호대책

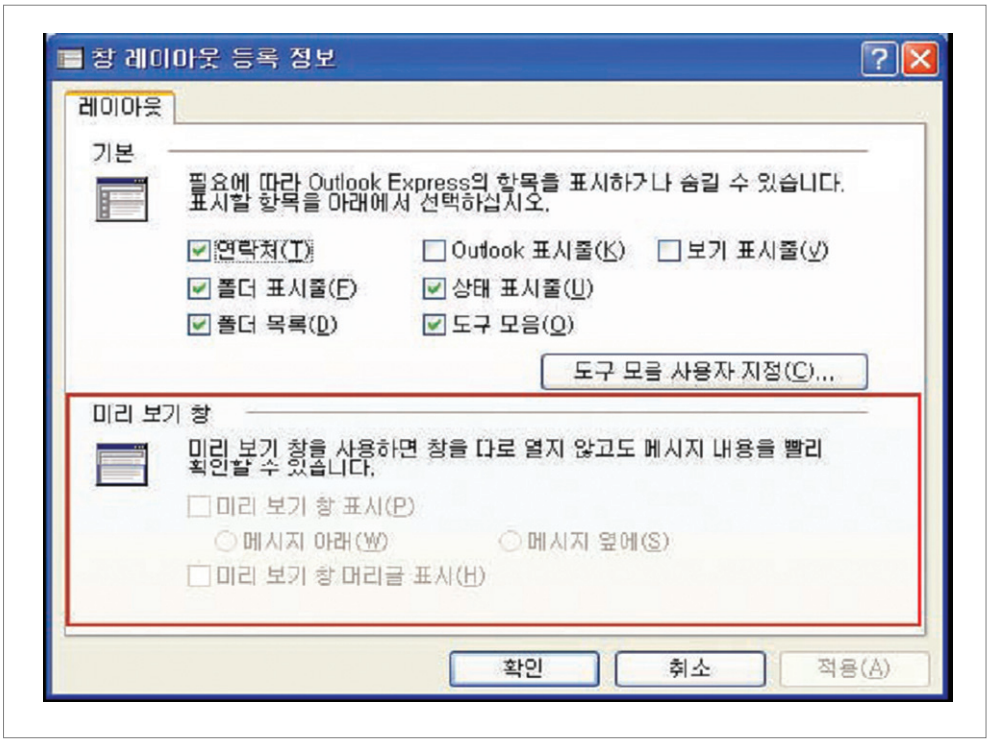
• Outlook Express에서 메일 미리보기 해제
  – 메일 미리보기 기능을 해제함으로써 바이러스나 악성코드에 의해서 개인정보가 유출될 가능성을 줄일 수 있다.
  ① Outlook Express의 [보기] ⇒ [레이아웃] 선택

〈그림 2-25〉 Outlook Express의 레이아웃



② [미리 보기 창] 영역에서 [미리 보기창 표시] 체크박스를 선택해제함

〈그림 2-26〉 Outlook Express의 미리보기 방지



5. 스파이웨어 등 악성 프로그램을 제거하자!

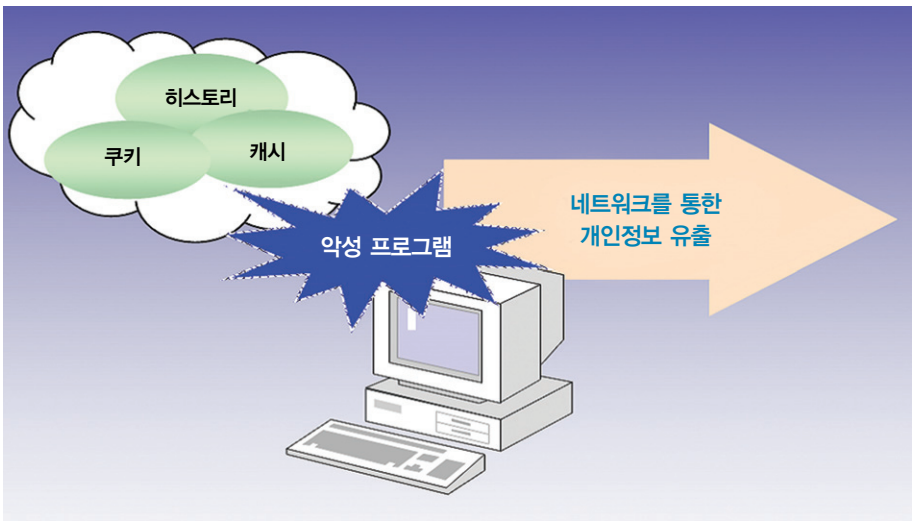
5.1 PC 방화벽 설정하기

■ 정보보호 현안 및 예상 피해

• 악성 프로그램을 통한 개인정보 유출

– 악성 프로그램은 신뢰성이 없는 프로그램이나 Active-X 프로그램 등을 다운 받을 때 설치되며, 악성 코드에 감염된 웹 사이트를 방문하는 것만으로도 감염될 수 있다. 이러한 악성 코드에 감염된다면 PC에 있는 개인정보가 유출될 수 있으며, 회사 내의 다른 PC를 감염시켜서 다량의 정보가 유출될 수 있다.

〈그림 2-27〉 악성 프로그램을 통한 개인정보 유출



■ 보호대책

• PC 방화벽 설정을 통한 네트워크 통제

– PC 방화벽 프로그램을 설치해두면 오픈된 포트로 전송되는 패킷을 막아주어 새로운 악성프로그램을 통해 개인정보가 유출되는 것을 예방할 수 있다.

– Windows XP에서 방화벽 기능을 사용하려면 서비스팩2가 설치되어 있어야 한다.

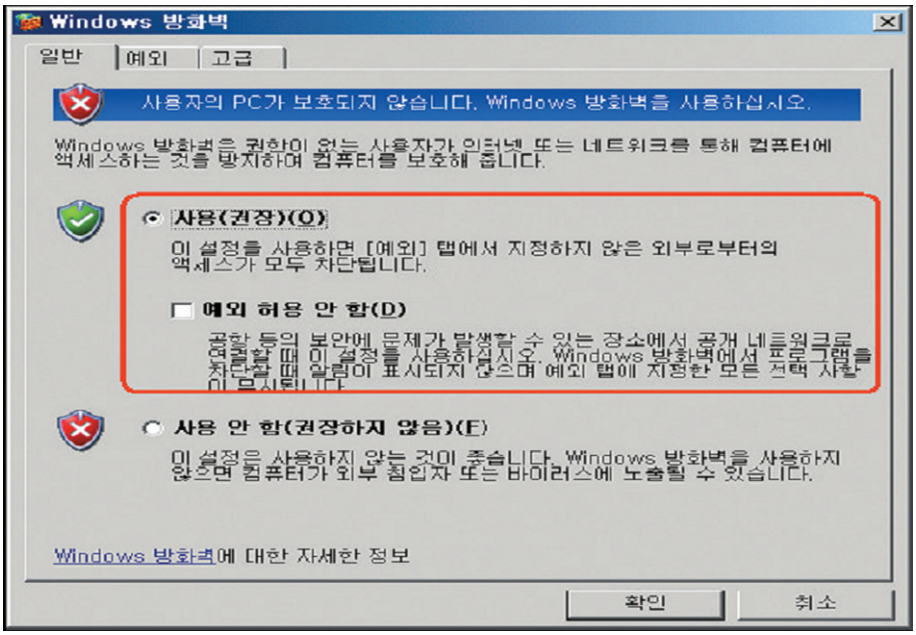
① PC화면 하단의 작업표시줄에서 [시작] ⇒ [제어판] ⇒ [보안센터] 선택

② [보안센터] 화면에서 Windows 방화벽 선택

〈그림 2-28〉 Windows 보안 센터

③ [Windows 방화벽] 화면에서 [일반]탭 선택 후 [사용권장] 체크

〈그림 2-29〉 Windows 방화벽 사용



5.2 스파이웨어 제거기 사용

■ 정보보호 현안 및 예상 피해

• 스파이웨어를 통한 개인정보 유출

– 내가 어떤 소프트웨어를 설치했고, 쇼핑몰에서 어떤 상품을 사는지

이 모든 것들을 누군가 알고 있다면?

- 트로이 목마 등 악의적인 해킹이나 컴퓨터를 훔쳐야만 가능한 일이 아니다. 소프트웨어에 끼워져 제작사에 사용자 정보를 낱낱이 보고하는 '스파이웨어' 나 온라인 컴퓨터 애프터서비스, 온라인 백신 등이 일반화 되면서 사용자들은 인터넷에 연결하는 것만으로도 일거수 일투족을 감시 당하고 있는 상태이다.
- 이러한 스파이웨어가 해킹 수단으로 이용될 경우 사용자 ID, 비밀번호, 주민등록번호 등 개인정보까지 빼낼 수 있다는 점에서 위험성이 매우 높다.

스파이웨어, 지워야 되나 말아야 되나

개인정보 침해사례가 급증하는 가운데 PC에 설치돼 있는 이른바 '스파이웨어(Spyware)'가 네티즌들 사이에서 개인정보 유출의 불안요인으로 떠오르고 있다.

스파이웨어는 트로이목마나 백도어 등의 악의적인 해킹도구와 달리 정품 소프트웨어나 공개 소프트웨어에 포함돼 있는 개인정보 유출 기능을 가진 파일로서 사용자가 임의로 이를 지울 경우 해당 소프트웨어를 사용할 수 없게 된다. 일종의 공인된 정보유출 도구인 셈이다. 따라서 사용자들은 스파이웨어를 통해 자신도 모르게 유출되는 자신의 개인정보가 악용되지 않을까 하는 불안감 또한 배제할 수 없는 실정이다.

스파이웨어는 시스템 레지스트리에 있는 이용자 이름, 이용자의 IP 주소, 이용자의 PC에 설치된 소프트웨어 리스트, 이용자가 찾아간 URL 리스트, 마우스로 클릭한 배너 광고, 여러 사이트에서 내려받은 파일 정보, 브라우저를 이용할 때에 나타나는 동작 정보 등을 통해 개인정보를 유출시킬 수 있다.

스파이웨어는 일반적으로 기존 쿠키 파일보다는 강력한 기능을 가지고 있지만, 사용자의 동의없이 PC에 침입해 개인정보를 무단 유출·악용하는 백오리피스·스쿨버스 등의 해킹도구와는 성격이 다르다.

그러나 스파이웨어는 악의적인 해커를 통해 특정인의 ID와 패스워드를 유출시킬 수 있는 가능성이 아주 높은 것으로 알려져 있다.이에 따라 전문가들 사이에서는 스파이웨어에 대한 법적 규제가 필요하다는 의견도 나오고 있다.

스파이웨어는 소프트웨어회사들이 정품 프로그램을 무료로 배포하기 위한 재원마련용 마케팅 수단으로 설치하는 경우가 대부분인 것으로 알려지고 있다. 특히 리얼플레이어 등 유명 프로그램을 비롯, 이용자가 많은 공개프로그램 등에 내장돼 있다는 것이다. 따라서 네티즌들은 자신도 모르게 개인정보가 외부로 알려지거나 악의적인 해커에 의해 피해를 볼 수도 있고, 귀찮은 스팸메일에 시달리게 된다는 것이다.

스파이웨어의 설치 여부나 프로그램을 제거하기 위해서는 정보보안업체들이 제공하는 스파이웨어 전문검색기나 PC방화벽을 이용하면 된다. 그러나 스파이웨어를 제거하면 해당 소프트웨어를 더이상 사용할 수 없게 돼 네티즌들은 이러지도 저러지도 못하고 있는 실정이다.

※ 자료출처 : 디지털타임스

■ 보호대책

• 스파이웨어 설치 예방 및 제거기를 통한 제거
  – 무료 소프트웨어는 함부로 설치하지 말고, 사용자 동의서에 '정보수집' 항목이 있을 경우 정보가 유출될 수 있으니 주의해야 한다.
  – 특정 사이트에서 '보안경고창'이 뜰 때 무조건 '예(Y)' 버튼을 누르지 않고, 경고문을 자세히 읽어본 후 실행여부를 결정한다.
  – 스파이웨어 제거기를 사용하여 정기적으로 점검하도록 하며, 스파이웨어 제거기는 아래 웹사이트에서 참조할 수 있다.

■보호나라

http://www.boho.or.kr

상용스파이웨어 제거기 : 사이버방역 · 온라인 검사 · 온라인 스파이웨어 제거 사이트

제 3 장 시스템 관리자편

III

1. 서버 관리의 기본을 지키자!

1.1 운영체제 업데이트 및 패치하기

■ 정보보호 현안 및 예상 피해

• 보안패치는 시스템 관리의 기본
  – 운영체제의 서비스 팩과 보안패치를 최신버전으로 유지하는 것은 보안 사고를 예방하기 위한 기본 과제이다.
  – 운영체제의 서비스 팩과 보안패치를 최신버전으로 설치하지 않았을 경우 해킹프로그램(exploit) 등에 의해 시스템이 침해당해 개인정보를 비롯한 중요 정보가 유출될 수 있다.

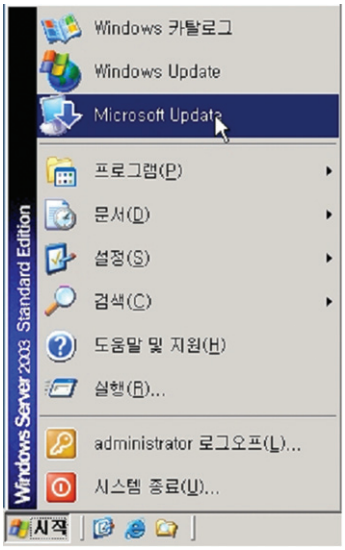
• 타 시스템 해킹의 전초기지 제공
  – 아무리 중요하지 않은 시스템이라도 침해사고가 발생하면 악의적인 공격자(해커)는 그 서버를 전초기지로 삼아 타 시스템을 공격하여 관리자 권한을 획득하거나 공유폴더 등을 이용하여 개인정보 등 중요 정보를 유출하게 된다.

■ 보호대책

• 보안패치 절차 수립
  – Windows등 운영체제는 지속적으로 보안패치가 나오고 있으므로 이를 반영하는 것이 필요하다.
  – 사용 중인 시스템을 중요도에 따라 상/중/하로 분리하고 중요도가 "하"인 시스템부터 차례로 보안패치를 수행하여 장애 여부를 확인한 후 중요도가 높은 시스템에 적용하는 것이 필요하며, 중요도가 "상"인 시스템은 충분한 검증을 거친 후 보안패치를 적용해야 한다.
  – 이러한 절차를 기록한 "보안패치 적용 절차서"를 마련하는 것도 바람직하다.

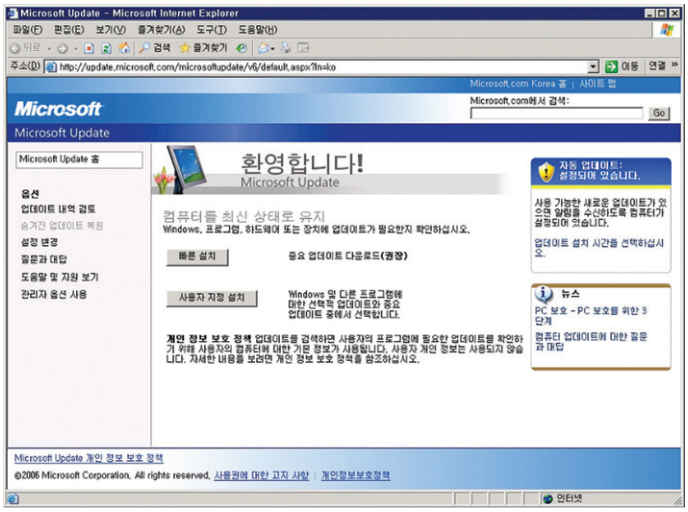
• 수동 보안패치 수행 절차(Windows Server 2003)
  – 시스템은 자동 보안패치를 권장하지 않는다.
  – Microsoft에서 제공하는 최신패치를 수행하기 전에 반드시 아래 사이트의 내용을 참고하여야 한다.
    http://www.microsoft.com/korea/technet/serucity/current.asp
  – 인터넷과 연결된 상태에서 http://update.microsoft.com 사이트를 직접 방문하거나, 아래 그림처럼 "시작 → Microsoft Update" 메뉴를 선택할 수 있다.

〈그림 3-1〉 Windows Update 선택



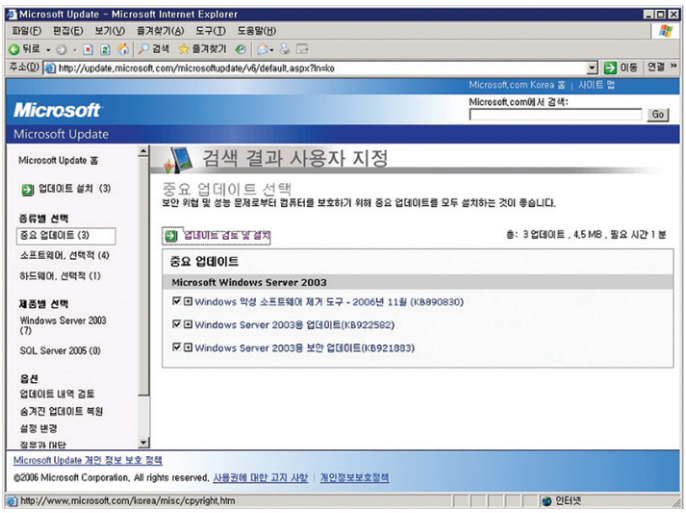
– 사용자 지정 설치를 클릭

〈그림 3-2〉 사용자 지정 설치 선택



– 사전에 확인한 필요한 업데이트만 선택하여 설치

〈그림 3-3〉 필요한 업데이트 선택

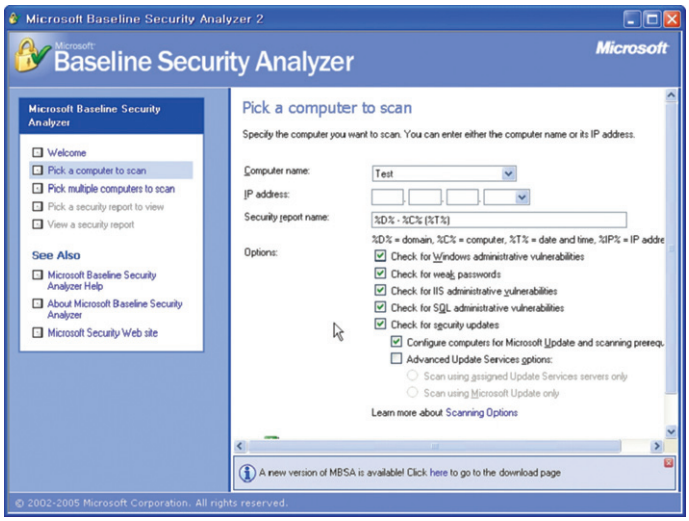


• Windows MBSA 활용하여 보안패치 미설치 확인하기

– Windows 시스템의 경우 Microsoft사에서 제공하는 MBSA (Microsoft Baseline Security Analysis)를 통해 쉽게 서버의 패치 현황 및 보안 취약점을 점검할 수 있다.

– [시작] ⇒ [프로그램] ⇒ Microsoft Baseline Security Analyzer 2.0 실행

〈그림 3-4〉 Microsoft Baseline Security Analyzer 2.0 실행



• Unix 및 Linux

– Unix 및 Linux의 경우 운영체제별로 각 제조사의 사이트에서 보안 패치가 제공되므로 이를 참조할 수 있다.

1.2 시스템 계정 및 암호 설정하기

■ 정보보호 현안 및 예상 피해

• 관리자 계정 노출 시 피해

– 시스템 관리자 계정을 잘못 관리하여 악의적인 공격자가 시스템 관리자 계정을 획득할 경우 임의의 명령어를 실행할 수 있으며, 임의의 파일을 수정하고 시스템 관리자 권한을 획득하여 개인정보를 유출할 수 있다.

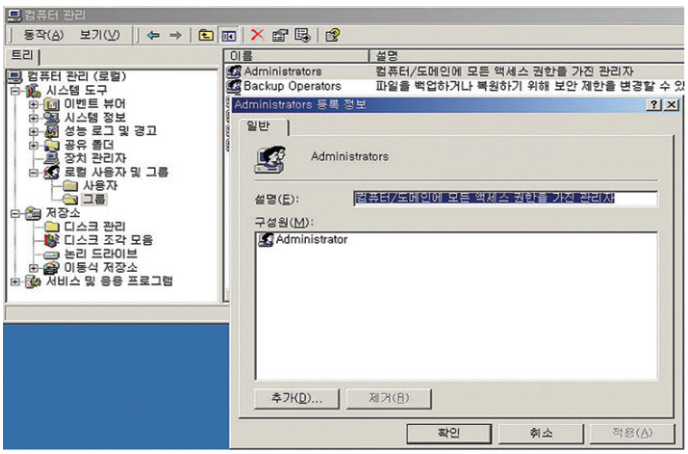
– 한 시스템의 시스템 관리자 권한을 획득할 경우 이를 전초기지로 삼아 DB 등 핵심 시스템에 접근할 수 있으므로 모든 시스템의 관리자 계정은 동일한 중요성을 가지고 보호해야 한다.

■ 보호대책

• 관리자도 평상시에는 일반 사용자 계정으로 접속하기
  – 일반적으로 관리자는 관리자 계정과 일반 사용자를 위한 계정을 분리하여 사용하는 것이 바람직하다. 하나는 관리업무를 위한 것이고, 다른 하나는 일반적인 일을 하기 위한 것이며, 이는 관리자 계정으로 접속하여 업무를 수행하다 발생하는 피해를 방지할 수 있다.

• 시스템 관리자 계정 하나만 사용하기
  – 시스템 계정 중 관리자 그룹으로 설정되어 있는 계정 중 administrator 계정을 제외한 모든 불필요한 관리자 계정을 삭제하거나 다른 그룹으로 권한을 변경해야 한다.

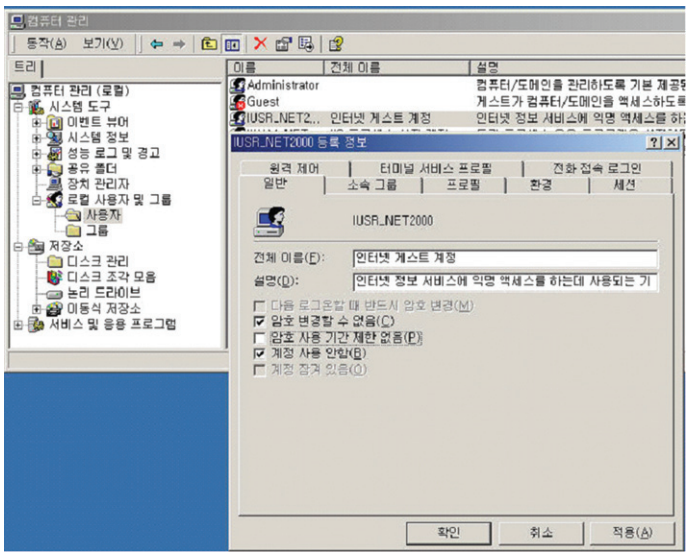
〈그림 3-5〉 시스템 관리자 계정 관리



• 불필요한 계정 삭제하기

– 퇴직, 전직, 또는 휴직 등의 이유로 더 이상 사용하지 않는 관리자의 계정과 불필요한 계정 그리고 의심스러운 계정이 있는지 점검하고 삭제해야 한다.

〈그림 3-6〉 불필요한 계정 삭제

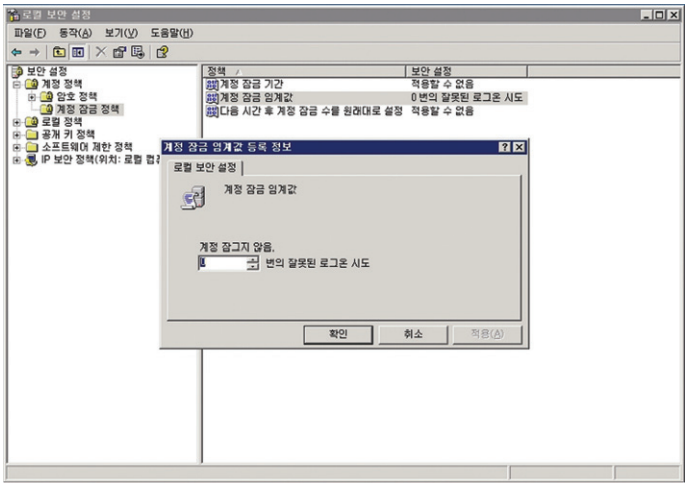


• 계정 잠금 정책 설정하기

– Administrator 계정은 로그온 시 몇 번이고 실패해도 절대 접속을 차단하지 않기 때문에 시스템을 공격하려는 사람들은 이 계정의 패스워드 유추를 계속 시도할 수 있으므로 로그온 시도를 제한해야 한다.

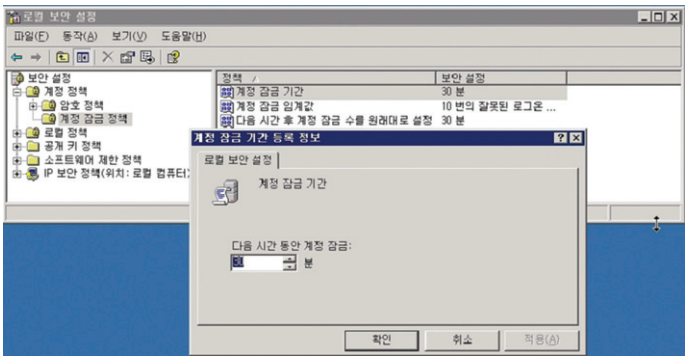
– [시작] ⇒ [프로그램] ⇒ [관리도구] ⇒ [로컬보안정책] ⇒ [계정정책] ⇒ [계정잠금정책] ⇒ [계정 잠금 임계값] 선택 후 로그인 시도 횟수를 설정

〈그림 3-7〉 계정 잠금 정책 설정



– [시작] ⇒ [프로그램] ⇒ [관리도구] ⇒ [로컬보안정책] ⇒ [계정정책] ⇒ [계정잠금정책] ⇒ [계정 잠금 기간] 선택 후 잠금 기간 설정

〈그림 3-8〉 계정 잠금 시간 설정

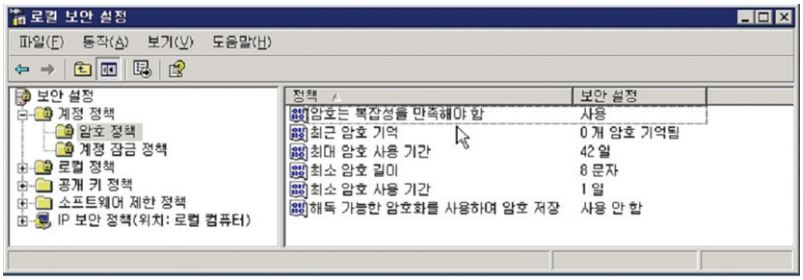


• 암호 정책 설정하기

– 패스워드 추측공격을 피하기 위하여 패스워드 최소 길이를 설정하고, 암호의 복잡성을 만족시켜야 하며 주기적으로 암호를 변경해야 한다.

– [시작] ⇒ [프로그램] ⇒ [관리도구] ⇒ [로컬보안정책] ⇒ [계정정책] ⇒ [암호 정책] ⇒ [암호는 복잡성을 만족해야 함], [최대 암호 사용 기간] 그리고 [최소 암호 길이] 등을 정책에 맞게 설정해야 한다.

〈그림 3-9〉 로컬 보안정책 설정



1.3 파일 시스템 관리하기

■ 정보보호 현안 및 예상 피해

• 파일 시스템 보안

– 파일시스템은 사용자 및 운영체제 데이터가 저장되는 운영체제의 자료구조이므로, FAT32 등 모든 파일과 폴더에 접근권한을 설정할 수 없는 파일 포맷으로 설정될 경우 불법적인 로컬 및 원격사용자로부터 손상, 삭제, 특정 명령어의 실행이 가능하여 침해사고를 유발할 수 있으며, 피해를 확장시킬 수 있다.

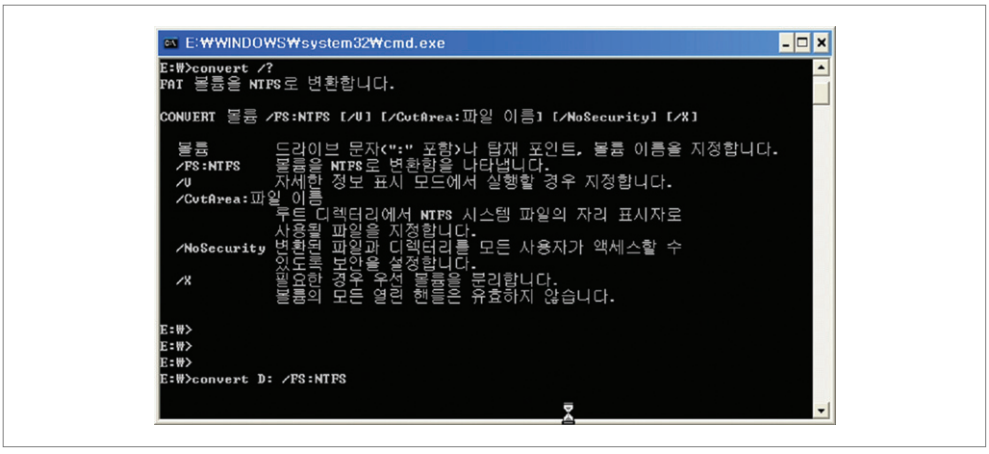
– 또한 시스템의 기본 공유폴더를 해제하지 않을 경우 웜 등의 감염으로도

개인정보 등 중요 데이터가 유출될 수 있다. 실제로 Nimda 바이러스도 여러가지 방법 중에서 이러한 공유기능을 침투의 한 경로로 이용한 예가 있다.

■ 보호대책

• NTFS 파일시스템 사용하기
  - 파일 시스템으로 NTFS를 사용하는 방법에는 3가지가 있으나 처음 운영체제를 설치할 때 NTFS로 포맷하는 것이 바람직하다.
  - 운영체제를 처음 설치하는 과정에서 파일시스템을 NTFS로 설정한다.
  - 운영체제가 이미 설치되어 있는 경우에는 Convert 유틸리티를 사용하여 FAT 파일시스템을 NTFS 파일시스템으로 변환한다.
    (C:\convert D: /FS:NTFS 실행)

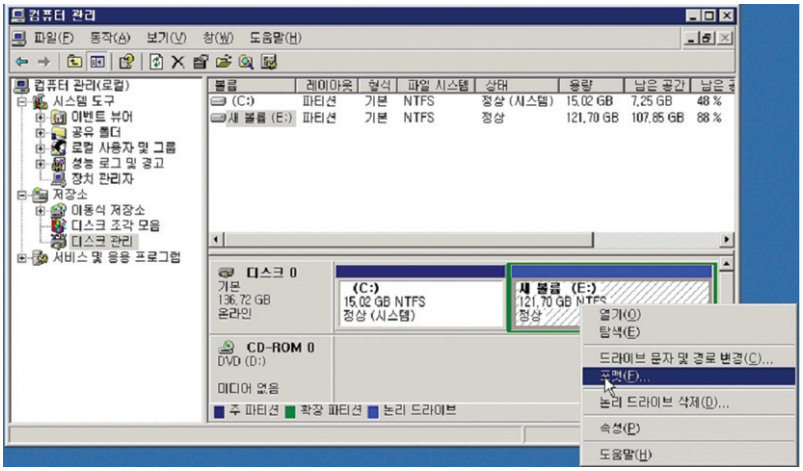
〈그림 3-10〉 NTFS 파일시스템 변환



  - 데이터가 없는 파티션의 파일시스템을 변환하는 경우, [시작] ⇒ [프로그램] ⇒ [관리도구] ⇒ [컴퓨터관리] ⇒ 디스크 관리]를 선택하여

해당 드라이브에 대해 마우스 오른쪽 버튼을 클릭한 후 [포맷]을 선택하여 파티션을 NTFS로 재포맷한다.

〈그림 3-11〉 NTFS 파일시스템 포맷 실행



• 공유폴더 관리

– 공유폴더 관리는 "제 2 장 일반사용자 편"의 "2. 공유폴더는 최소한으로 하자"의 내용과 동일하므로 이를 참고할 수 있다.

2. 개인정보는 반드시 암호화 하자!

■ 정보보호 현안 및 예상 피해

• 패스워드, 바이오정보 암호화하기

- 패스워드 및 바이오정보 등과 같은 개인정보가 암호화되지 않고 저장 및 전송되는 경우, 패스워드 및 개인정보가 노출되거나 위 · 변조될 위험이 있다.
- 실례로, 2006년 3월 A은행은 고객 3,000여명에게 홍보메일을 발송하면서 실수로 주민번호 등 30,000여명의 개인정보가 들어있는 엑셀 파일을 첨부하여 보내는 사고가 발생하였다. A은행은 즉각 사과하고 재발방지를 약속하였으나 개인정보가 유출된 고객 중 1,026명은 30억의 집단소송을 벌이고 있다.
- 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제28조에 근거한 "개인정보의 기술적/관리적 보호조치 기준(정통부 고시)" 제5조(개인정보의 암호화)에는 개인정보 및 인증정보에 대한 암호화 저장 및 전송에 관한 사항이 규정되어 있다.

〈 개인정보의 기술적/관리적 보호조치 기준 〉
제5조(개인정보의 암호화) ① 정보통신서비스제공자등은 패스워드, 생체정보 등 본인임을 인증하는 정보에 대해서는 복호되지 아니하도록 일방향 암호화하여 저장한다.
② 정보통신서비스제공자등은 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송 · 수신할 때에는 보안서버 구축 등의 조치를 통해 이를

암호화하여야 한다. 보안서버는 다음 각 호의 어느 하나의 기능을 갖추어야 한다.

1. 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하여 개인정보를 암호화하여 송 · 수신하는 기능
2. 웹서버에 암호화 응용프로그램을 설치하여 개인정보를 암호화하여 송 · 수신하는 기능

③ 정보통신서비스제공자등은 이용자의 개인정보를 PC에 저장할 때에는 이를 암호화하여야 한다.

■ 보호대책

• DB 암호화하기

– Oracle7i 이상 버전 및 MS-SQL Server 2005에서는 기본적으로 암호화 모듈을 제공하고 있으며 암호화 모듈 패키지를 활용하여 주민

[표 3-1] 국내외 상용 암호화 솔루션

제품명	제조사	구성방식	비고
D'amo (디아모)	펜타시큐리티	DB agent 방식 Oracle/MSSQL 지원	국산
SafeDB	이니텍	DB agent, application agent 방식 지원 Oracle/MSSQL 지원	국산
XecureDB	소프트포럼	DB agent, application agent 방식 지원 Oracle/MSSQL 지원	국산
Cubeone	이글로벌시스템	application agent 방식 oracle 만 지원	국산
Secure .data	Protegrity (국내 위즈메카 총판)	DB agent 방식 Oracle/MSSQL 지원	외산
Datasecure	Ingrian (국내 한국전자 증명원 총판)	Hardware 일체형 장비	외산

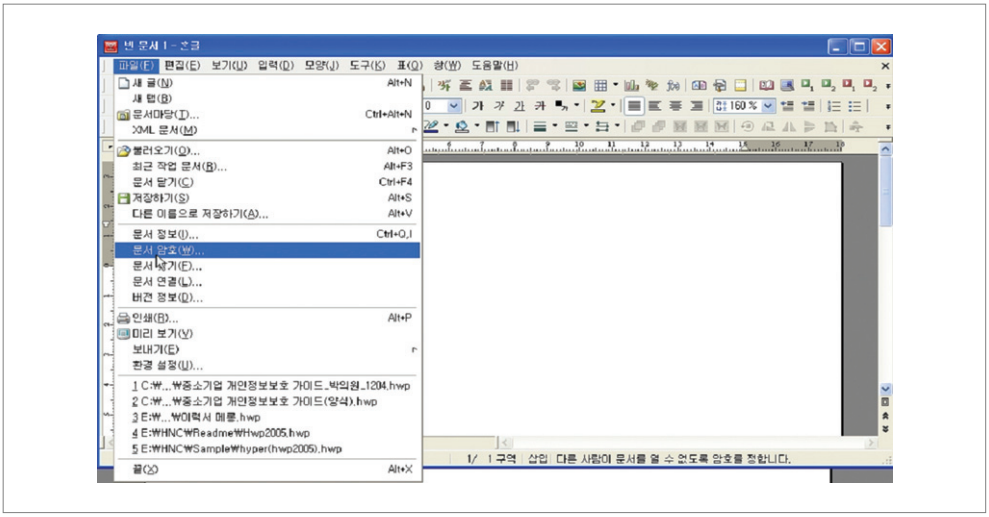
번호 및 개인정보를 암호화할 수 있다.

- MS-SQL Server 2000에서는 암호화 모듈을 지원하지 않으므로 기본적으로 주민번호와 개인정보를 암호화할 수 없고, 상용 암호화 솔루션을 구입하여 사용할 수 있다.
- 국내외 상용 암호화 솔루션은 위와 같으며, 각기 장단점이 있으므로 업체의 특성에 맞게 선택하여야 한다.

• 개인정보가 저장된 문서 암호 설정하기

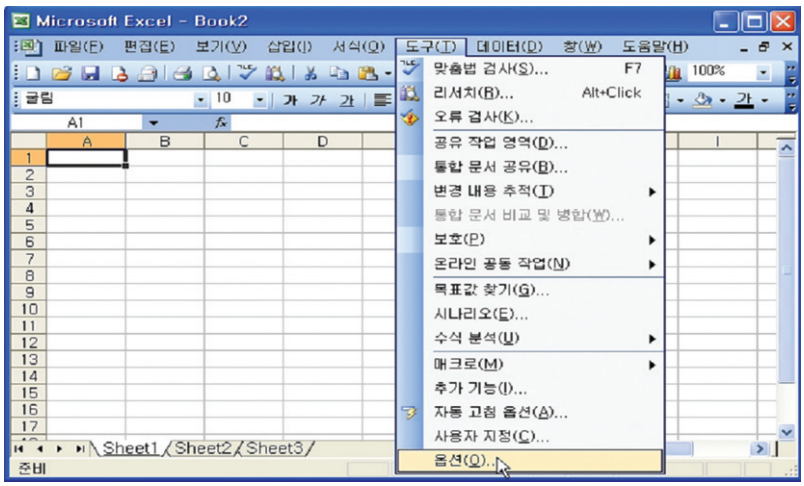
- 한글 파일(HWP)에 암호를 설정하기 위해 [파일] ⇒ [문서 암호]를 클릭한 후 암호를 설정

〈그림 3-12〉 한글파일 문서 암호화 설정

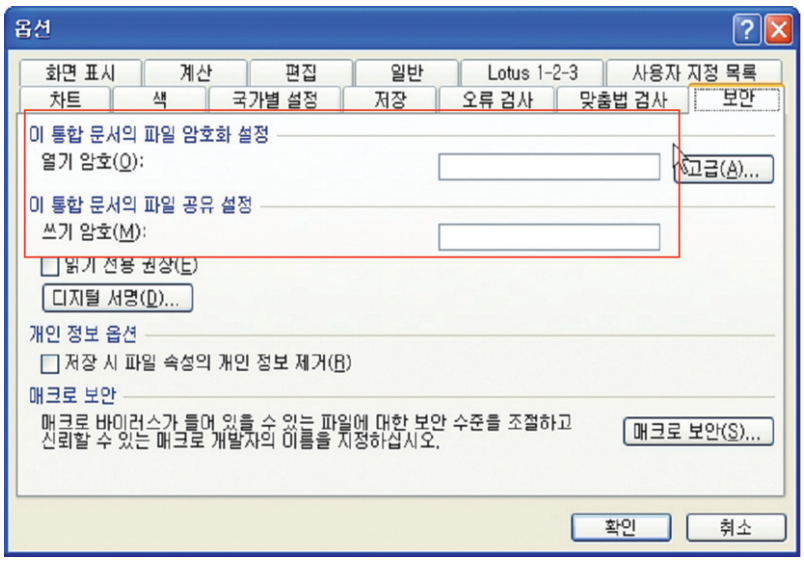


- Microsoft사의 엑셀(excel)과 워드(word) 문서는 암호를 설정하기 위해 [도구] ⇒ [옵션] ⇒ [보안 탭]을 클릭한 후 파일 열기, 쓰기 암호를 설정

〈그림 3-13〉 엑셀파일 암호화 설정옵션 선택



〈그림 3-14〉 엑셀파일 암호화 및 공유 설정



3. 사용자 및 기기 인증 체계를 강화하자!

3.1 서버 사용자의 계정 및 암호 관리하기

■ 정보보호 현안 및 예상 피해

• 퇴사자 계정 관리하기

- 개인정보를 비롯한 중요정보 유출의 70~80%는 내부 직원의 소행이며, 이중 대부분이 퇴사자나 퇴사를 예정한 내부직원으로 인해 발생하였다.
- 2006년 5월 경기경찰청은 초고속인터넷 가입자 88만명의 정보를 유출한 통신업체의 전현직 직원 4명을 구속하고 4명을 불구속 기소하였다.

• 계정별 권한 부여하기

- 서버의 사용자는 그 업무에 맞는 권한만 부여하여야 하며, 권한별로 접근통제를 실시하여야 한다. 그러나 대부분의 기업에서 모든 사용자에게 모든 권한을 부여하고 있으며, 이는 매우 위험한 일로 고객의 개인정보를 비롯하여 회사의 중요 정보가 유출될 수 있다.
- 2006년 4월 인천 남동경찰서는 인터넷서비스가입자의 개인정보를 불법 유출시킨 혐의로 인터넷 서비스 업체 직원을 불구속입건하였다. 이 직원은 자신의 계정으로 모든 인터넷 서비스 가입자의 정보를 조회할 수 있다는 것을 알고 본인의 계정과 비밀번호를 마케팅업체 직원에게 알려주어 50만 명의 개인정보를 유출하게 한 혐의를 받고 있다.
- 국내 모 회사의 경우 임시직의 계정에 인사시스템의 정보를 검색할 수 있는 권한이 부여되어 있어 이를 통해 임직원의 개인정보가 유출된 사례도 있다.

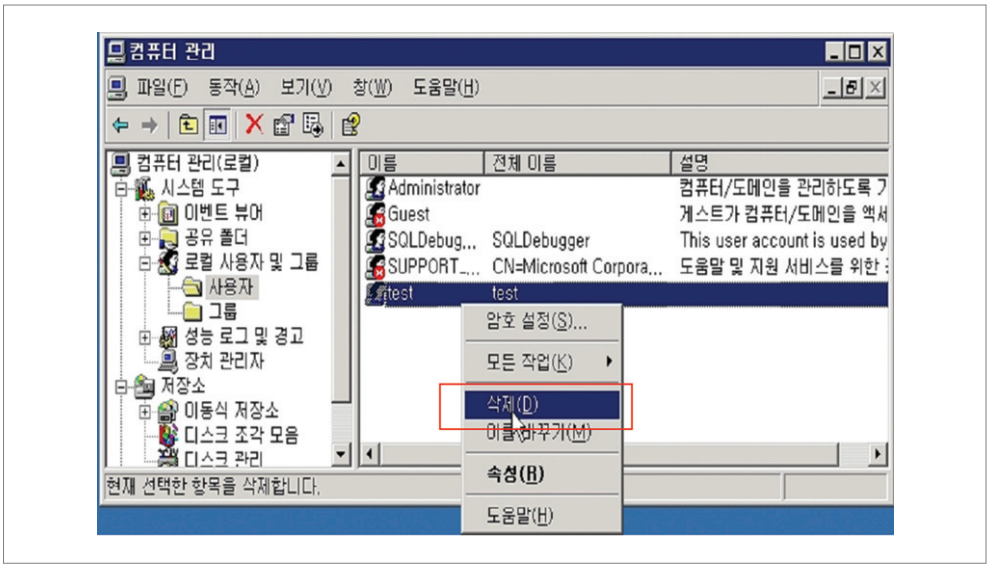
■ 보호대책

• 퇴사자 계정 삭제하기

– 퇴직, 전직, 또는 휴직 등의 이유로 더 이상 사용하지 않는 사용자의 계정을 인사발령 후 즉시 잠금 또는 삭제해야 한다.

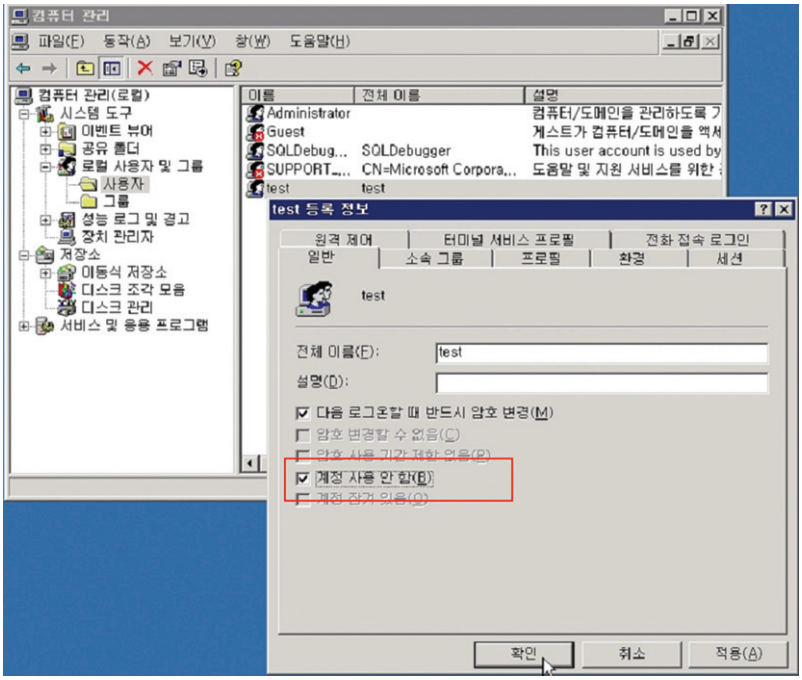
– [시작] ⇒ [프로그램] ⇒ [관리도구] ⇒ [컴퓨터 관리] ⇒ [로컬사용자 및 그룹]에서 삭제 대상 계정을 지정한 후 마우스 오른쪽 버튼을 클릭하여 “삭제” 메뉴를 클릭

〈그림 3-15〉 퇴사자 계정 삭제



– 해당 계정을 삭제하지 않고 사용을 중지시키고자 할 경우 해당 계정에서 마우스 오른쪽 버튼을 클릭한 후 [속성]을 클릭하여 “계정 사용 안함“을 설정

〈그림 3-16〉 계정 사용 중지 설정

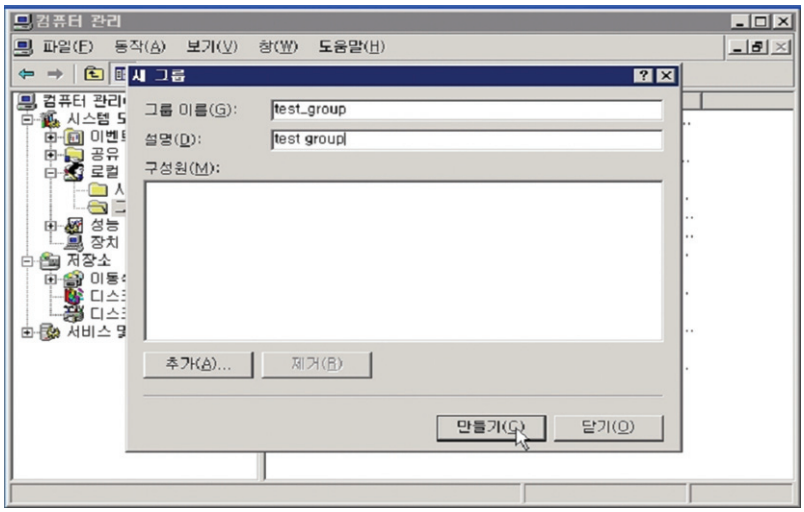


– 사용자 계정에 대한 암호 설정 방법은 "1.2 서버 계정 및 암호 설정하기"를 참조

• 계정별 권한 부여하기

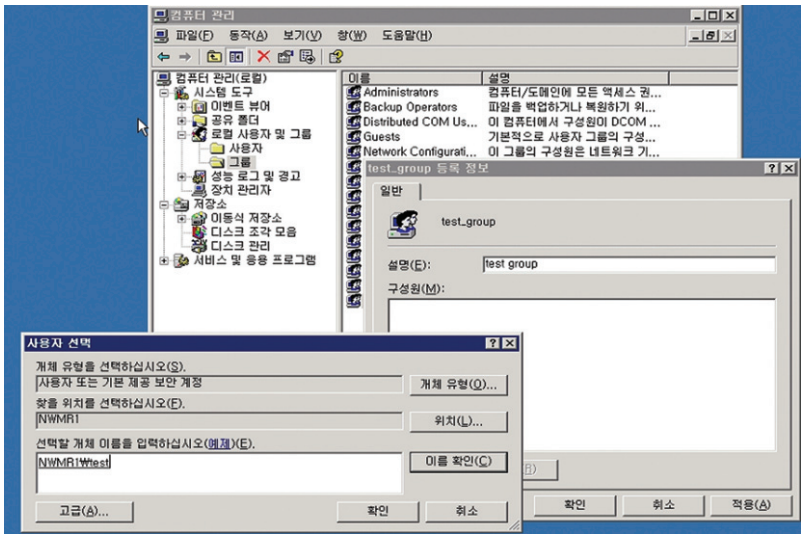
– [시작] ⇒ [프로그램] ⇒ [관리도구] ⇒ [컴퓨터 관리] ⇒ [로컬사용자 및 그룹]에서 그룹을 지정한 후 마우스 오른쪽 버튼을 클릭하여 "새 그룹"을 선택. 그룹 이름에 원하는 명칭을 쓰고 "만들기" 버튼을 클릭

〈그림 3-17〉 로컬사용자 및 그룹 만들기



– 생성된 그룹에서 마우스 오른쪽 버튼을 클릭하여 사용자 계정을 추가

〈그림 3-18〉 계정별 권한 부여 설정



3.2 관리자는 등록된 단말기만 사용하기

■ 정보보호 현안 및 예상 피해

• 관리자 계정 정보 유출 주의

- 시스템의 관리자 계정(administrator 또는 root등)은 막강한 권한을 가지고 있어 그 어떤 계정보다 철저히 관리하여야 한다.
- 관리자가 등록된 관리자 컴퓨터 외에 게임방 컴퓨터 또는 공공장소에 노출된 컴퓨터 등에서 시스템에 접근할 경우 계정 및 패스워드가 노출될 수 있으며, 타 직원의 컴퓨터에서 접속하면서 패스워드가 노출되어 피해를 유발할 수 있다.
- 실례로, 2004년 6월 미국 AOL(America Online)의 직원 중 고객 데이터베이스에 접근 권한이 없는 직원이 본인 컴퓨터에서 다른 직원이 고객DB에 로그인할 때 계정 및 비밀번호를 획득하여 불법으로 데이터베이스에 접근함으로써 9,200만 명의 고객 정보를 유출하였다.

■ 보호대책

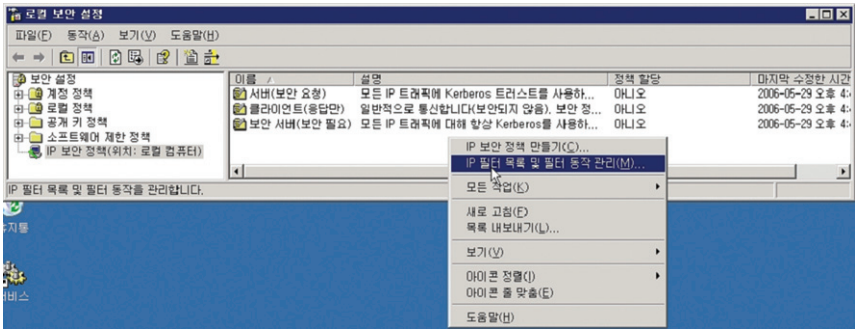
• 관리자는 등록된 단말기만 사용하여 접속

- 시스템 관리자는 허가된 컴퓨터에서만 시스템에 접속하여야 하며, 그 외 타인의 컴퓨터 또는 공공장소의 컴퓨터에서는 접속을 금하여야 한다.
- 방화벽 또는 시스템의 접근통제를 활용하여 관리자 등 접근권한이 있는 사람에 대해서만 시스템에 접근할 수 있도록 강제하여야 한다.
- 상용 침해차단시스템(이하 방화벽)이 있는 경우는 방화벽에서 접근통제정책(ACL)을 적용하여야 하며, 상용 방화벽이 없는 경우 운영체제에서 기본적으로 제공하는 프로그램을 사용하여 관리자 등에 대해서만 시스템 접근을 허용해 줄 수 있다.

• Windows server 2003에서 접근제어 설정하기

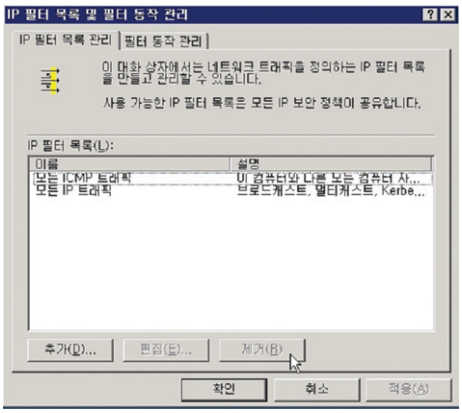
– [시작] ⇒ [프로그램] ⇒ [관리도구] ⇒ [로컬 보안 정책]을 선택하여 나타난 로컬 보안정책 화면의 왼쪽 맨 아래 "IP 보안 정책" 메뉴를 선택하면 오른쪽에 3가지의 설명이 보일 것이며, 빈 공간에서 마우스 오른쪽 버튼을 클릭하여 "IP 필터 목록 및 필터 동작관리"를 선택

〈그림 3-19〉 IP 필터 목록 및 필터 동작 관리 설정



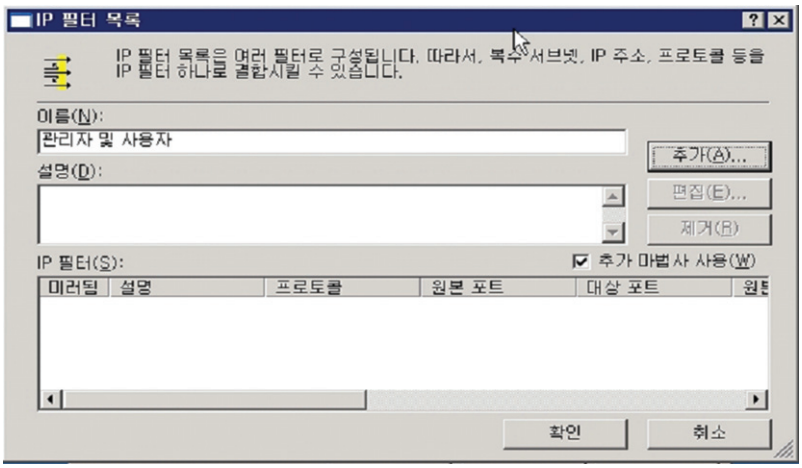
– 아래 화면이 나타나면 "IP 필터 목록 관리" 탭에서 추가 버튼을 선택

〈그림 3-20〉 IP 필터 목록 관리 설정



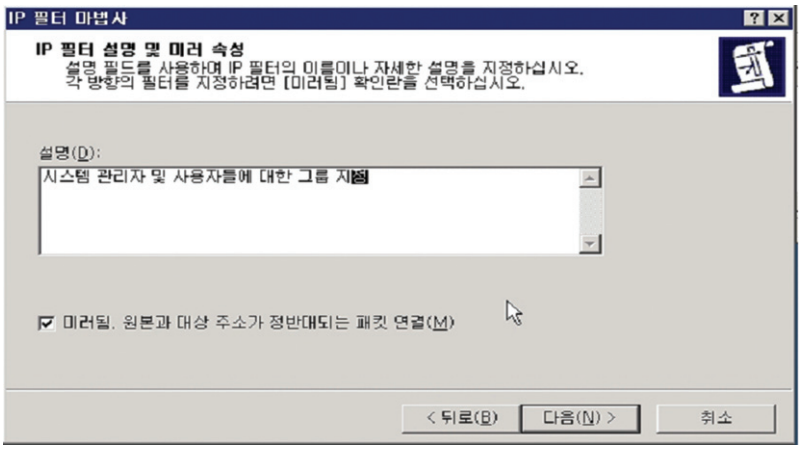
– 이름(N)에 적절한 명칭을 기입하고 확인하면 새로운 창이 나올 것이며 이 때 다음 버튼을 선택

〈그림 3-21〉 IP 필터 목록 이름 지정



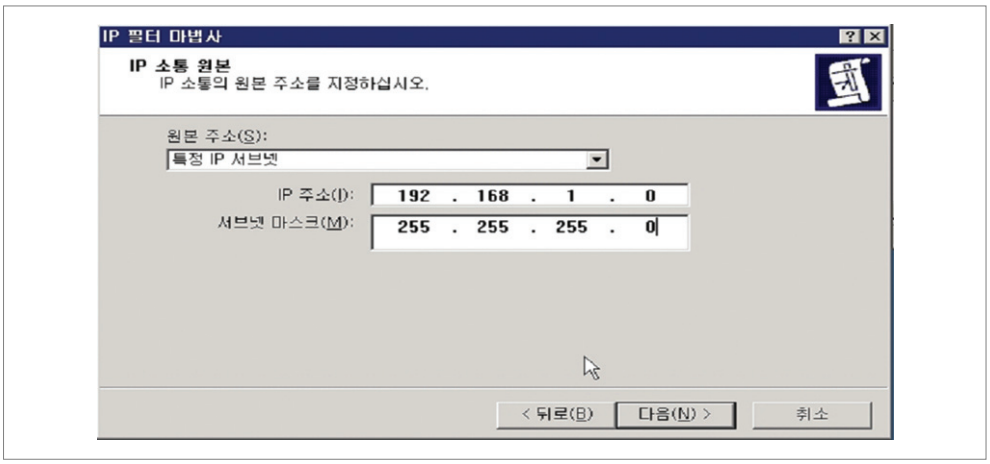
– 설명 부분에 적절히 기입한 후 다음을 선택

그림 3-22〉 IP 필터 목록 설명 기입



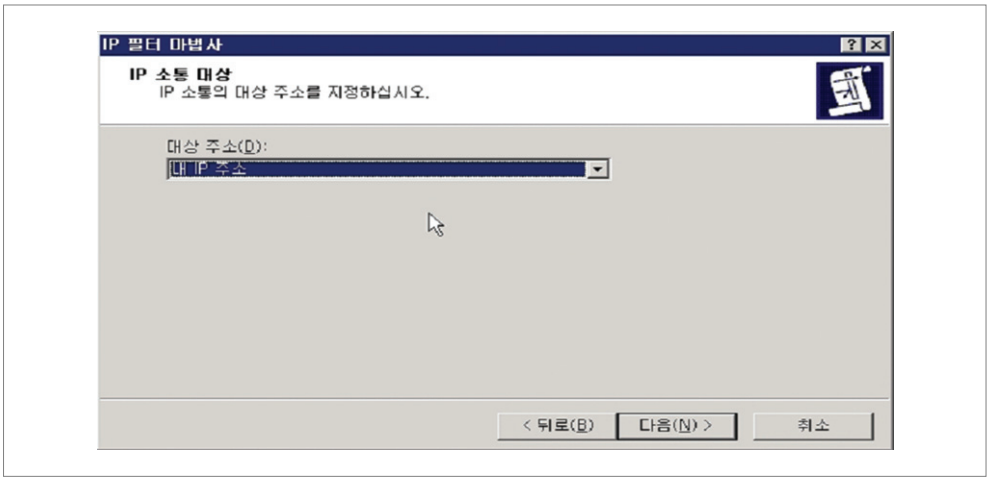
– "IP 필터 마법사"에서 원본 주소(Source IP)에는 특정 IP, 특정 IP 서브넷 등 여러 메뉴 중 적절한 메뉴를 선택하여 설정

〈그림 3-23〉 IP 소통 원본 주소 설정



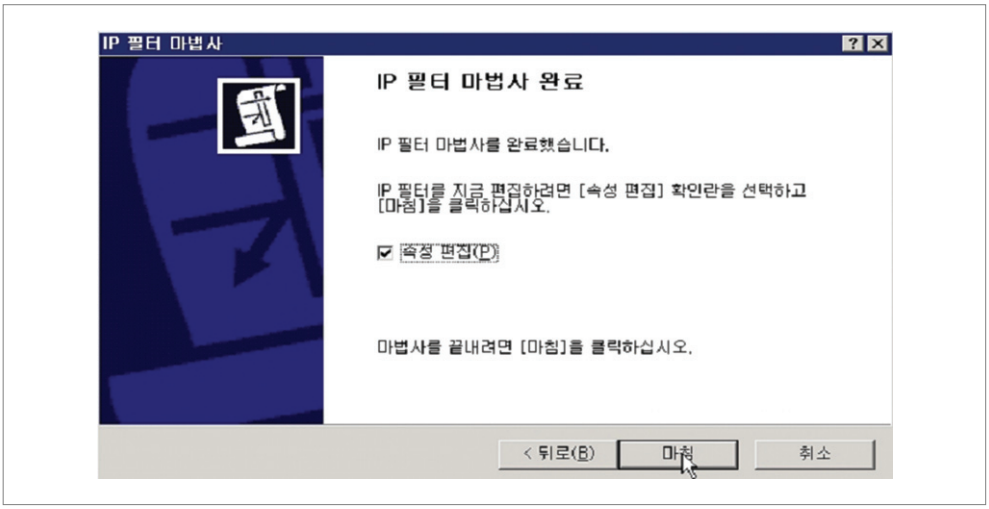
– 대상 주소(Destination IP)는 시스템이므로 "내 IP 주소"를 선택하고 다음 프로토콜 역시 정책에 따라 선택

〈그림 3-24〉 IP 소통 대상 주소 설정



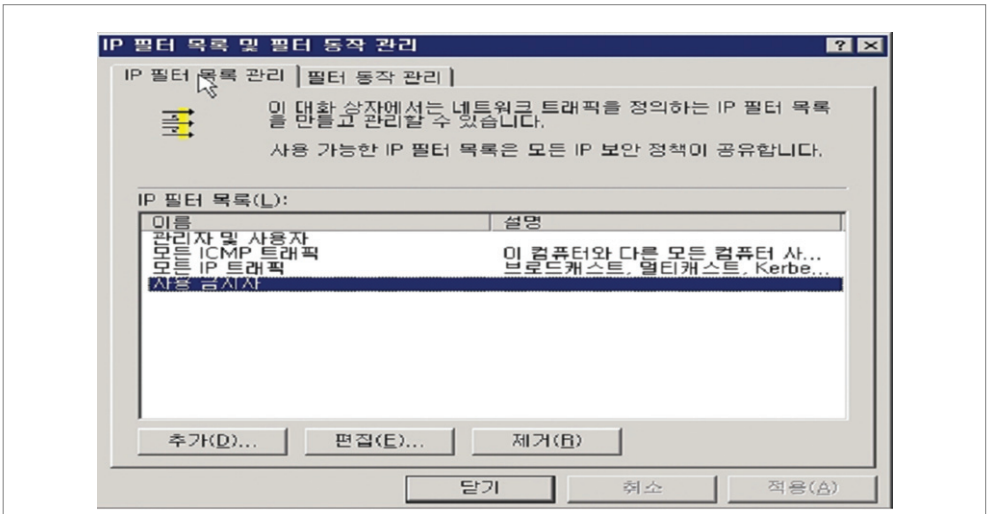
– 선택이 완료되면 “속성편집“ 체크한 후 마치며, 이후 속성을 다시 확인

〈그림 3-25〉 IP 필터 속성편집 선택



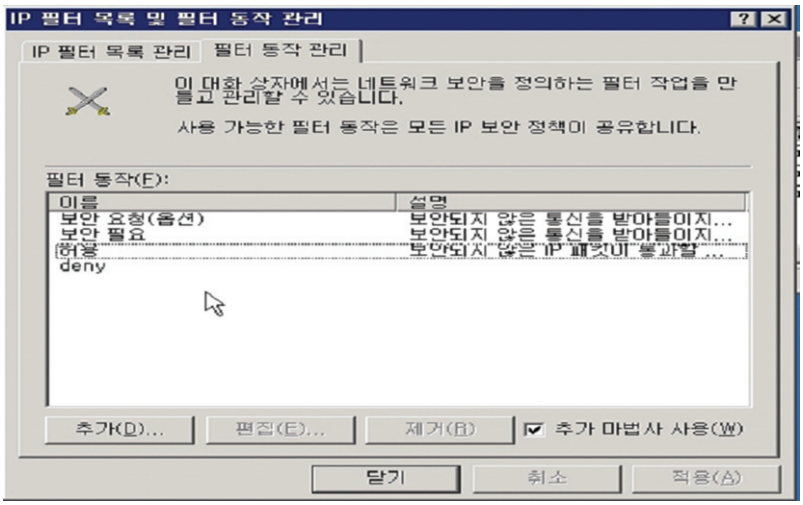
– 같은 방법으로 “사용 금지자” 등 새로운 객체를 생성

〈그림 3-26〉 IP 필터 목록 사용금지자 설정



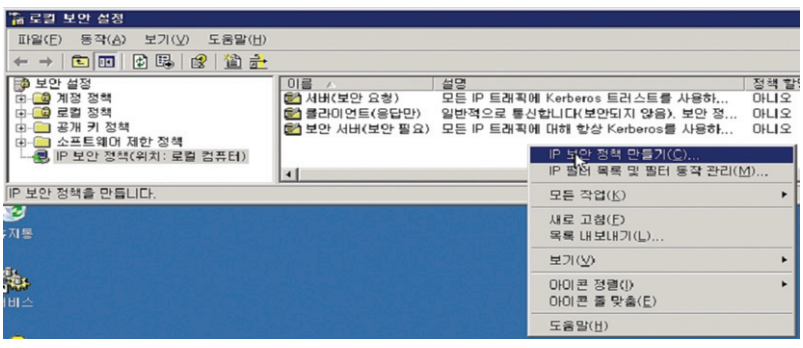
– 다음으로 “필터 동작 관리”탭을 선택하여 허용과 차단 정책을 추가 (아래는 추가가 완료된 그림임)

〈그림 3-27〉 필터 동작 관리 설정



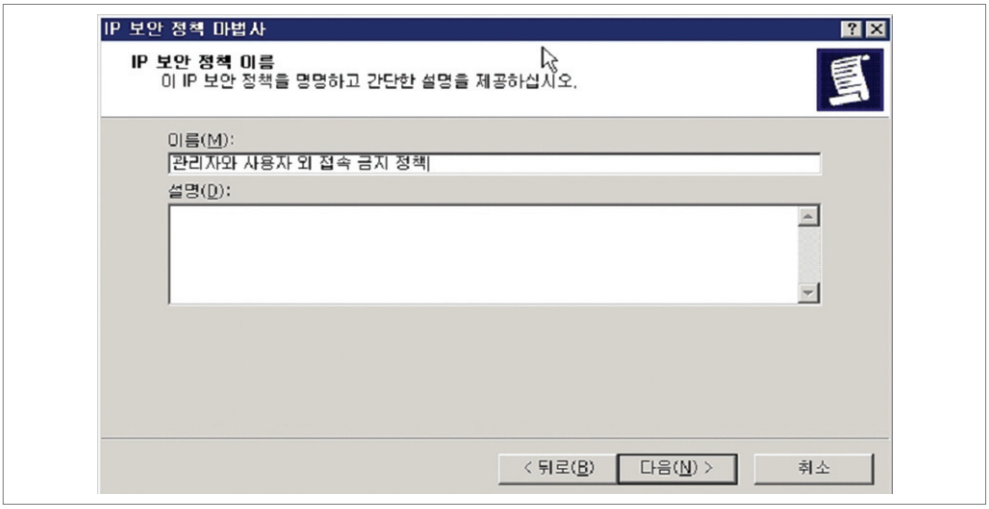
– 이제 관리자 컴퓨터 외에 타인의 접속을 차단할 준비가 완료됨. 빈 공간에서 마우스 오른쪽 버튼을 클릭하여 “IP 보안정책 만들기”를 선택

〈그림 3-28〉 IP 보안정책 만들기 선택



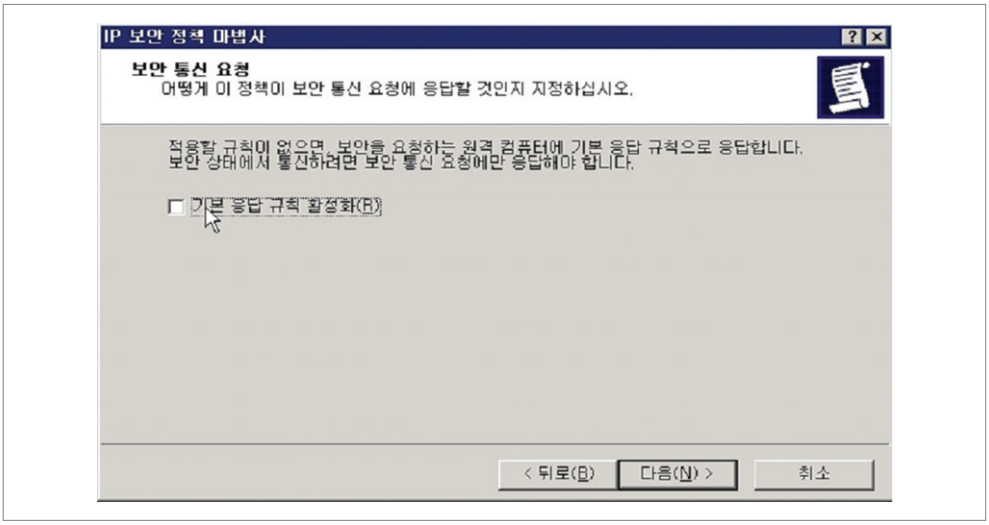
– 적절한 보안정책 명을 지정

〈그림 3-29〉 IP 보안정책 이름 설정



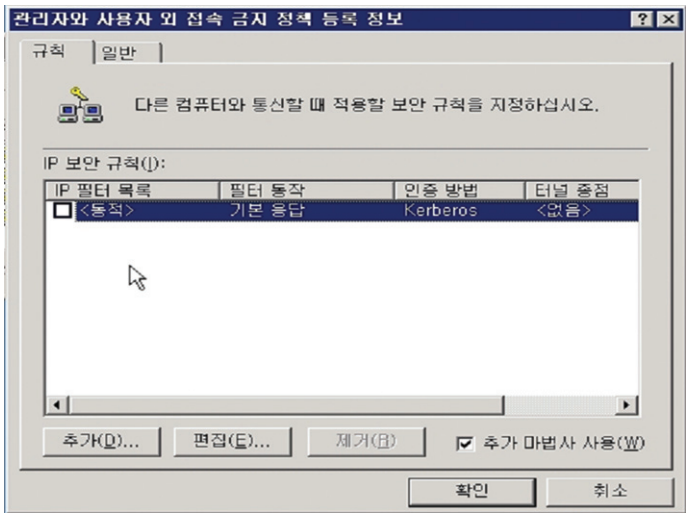
– "기본 응답 규칙 활성화(R)"를 선택하지 않고 다음으로 넘어감

〈그림 3-30〉 IP 보안통신 정책 설정



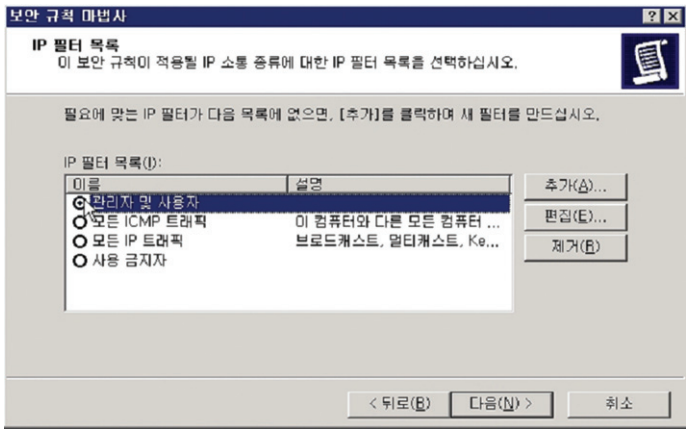
– 규칙 등록 화면에서 추가 버튼을 클릭하여 새로운 규칙을 등록

〈그림 3-31〉 관리자와 사용자 외 접속 금지 정책 등록 설정



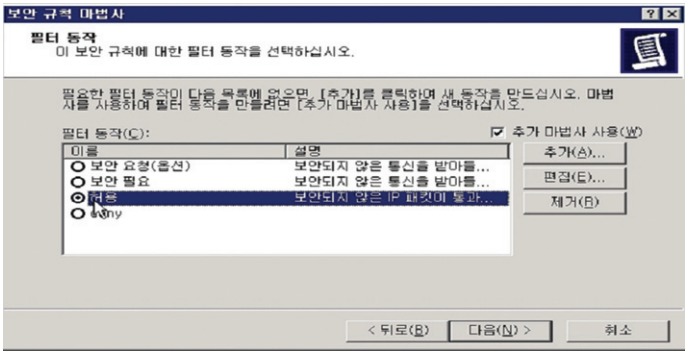
– 앞에서 등록된 “관리자 및 사용자“를 선택

〈그림 3-32〉 IP 필터목록 관리자 및 사용자 선택



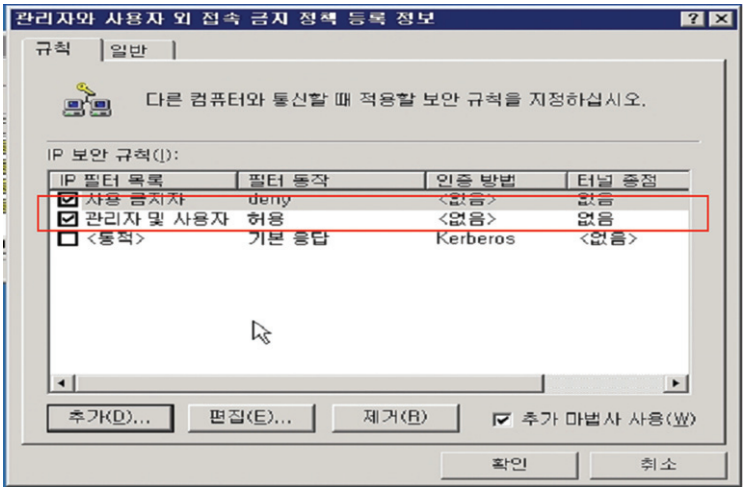
– 필터 동작으로 허용을 선택하여 관리자 및 사용자의 접속을 허가

〈그림 3-33〉 관리자 및 사용자의 접속 허가 설정



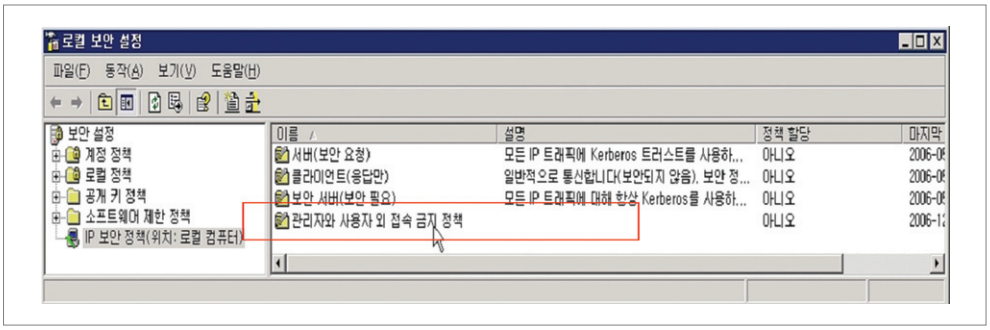
– 필터 정책을 완료하면 아래와 같이 관리자 및 사용자는 접속이 허용되는 규칙이 생겼음을 확인할 수 있다. 또한 사용 금지자에게는 차단 정책을 적용하면 시스템 관리자 및 사용자를 제외한 곳에서 접근을 차단할 수 있다. 이를 응용하여 여러 정책을 설정하는 것이 바람직하다.

〈그림 3-34〉 관리자와 사용자의 접속 허용 규칙 확인



– 정책이 완료되면 “IP 보안 정책”에 새로운 정책이 생성됨을 확인가능

〈그림 3-35〉 IP 보안 정책 생성 확인



4. 개인정보 유출 항상 모니터링하자!

■ 정보보호 현안 및 예상 피해

• 웹 게시판을 통한 개인정보 유출 현황

- 관리자의 부주의와 임직원의 안이한 행동이 웹 게시판을 통한 개인정보 유출의 가장 근본적이며 치명적인 원인이다. 정부기관은 물론이고 중소기업 뿐 아니라 대기업까지도 상당히 별로 다르지 않다.
- 2006년 9월 A전자 채용사이트를 통해 입사지원을 한 대학원생이 URL의 간단한 조작을 통해 다른 사람의 지원 내역을 확인한후 그 방법을 인터넷 카페에 게시하여 이 대학원생을 통해 유출된 개인정보는 B그룹 1만 여명, A전자 3,600여명 등 총 14,000명에 이르렀다.
- 2006년 7월 명문대학교 휴학생이 060 콘텐츠 제공업체의 홈페이지 관리자 모드의 허점을 이용하여 개인정보 230만 건을 유출한 혐의로 강원지방경찰청에 긴급 체포되었다.

■ 보호대책

• 예제 응용 프로그램 삭제하기

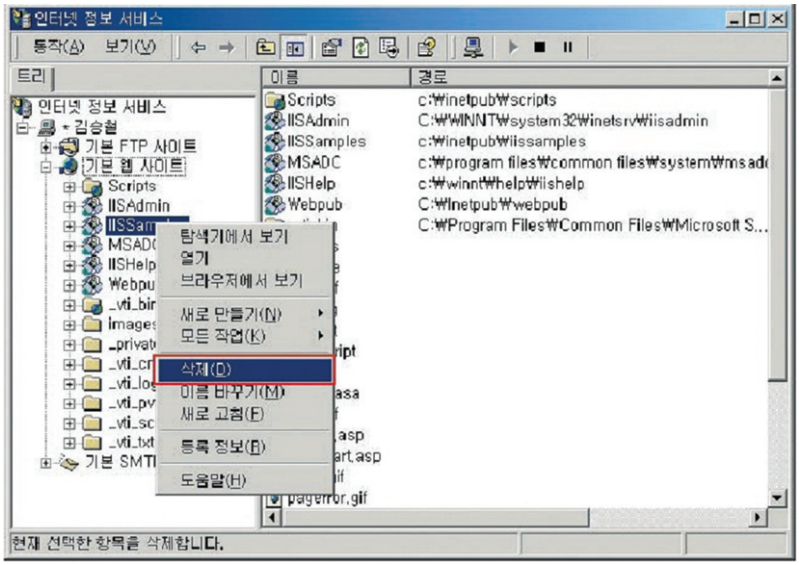
- IIS를 설치하면 기본적으로 예제와 설명서 등이 같이 설치되는데,

예제	가상 디렉토리	위치
IIS 예제	\IISSamples	c:\inetpub\iissamples
IIS 설명서	\IISHelp	c:\winnt\help\iishelp
데이터 액세스	\MSADC	c:\program files\common files\system\msadc

이 폴더들은 해킹에 이용되거나 백도어가 심어질 위험이 있으므로 제거하여야 한다.

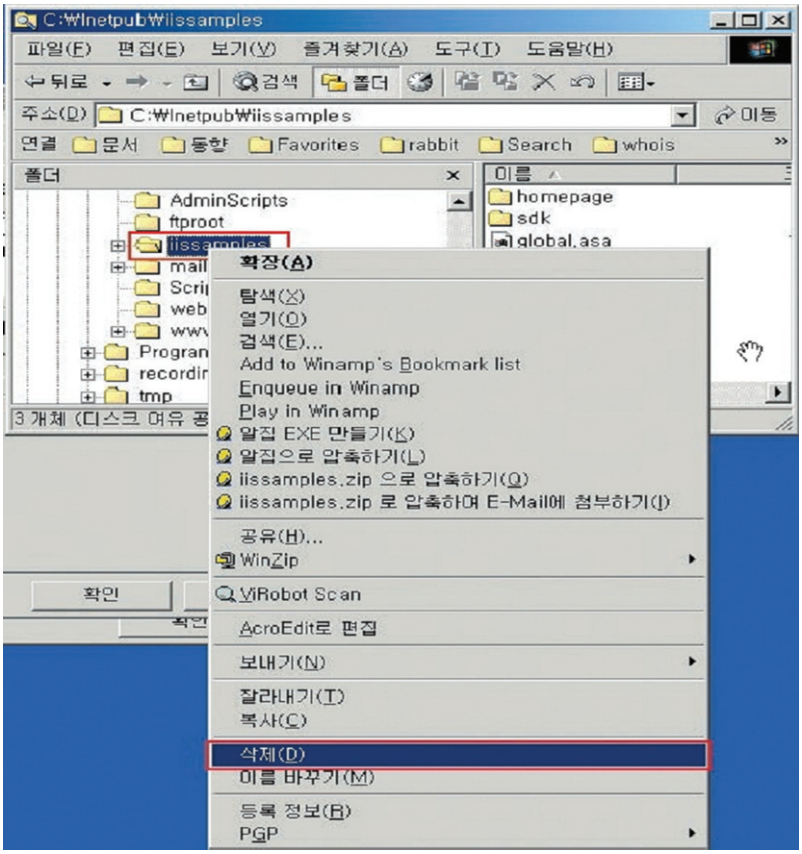
- [시작] ⇒ [프로그램] ⇒ [관리 도구] ⇒ [인터넷 서비스 관리자]에서 삭제하려는 가상 디렉토리를 선택하고 마우스 오른쪽 버튼을 클릭한 후 "삭제"를 선택

〈그림 3-36〉 삭제대상 가상디렉토리 선택



- 내컴퓨터에서 [c:\inetpub\iissamples]를 삭제

〈그림 3-37〉 가상디렉토리 삭제

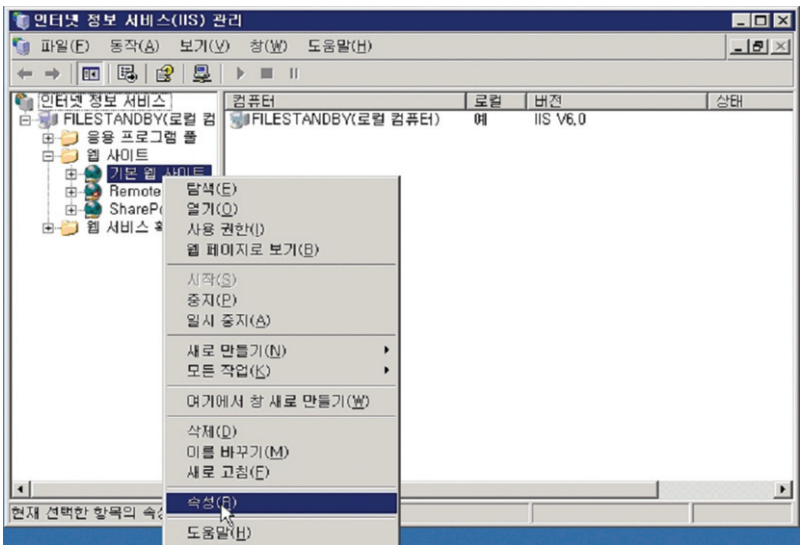


• 디렉토리 목록 검색 방지

– 웹서버에 저장된 임의의 HTML 파일을 공격자가 검색하여 해킹에 이용할 수 있으므로, 이를 방지하기 위해서는 디렉토리가 검색되지 않도록 설정해야 한다.

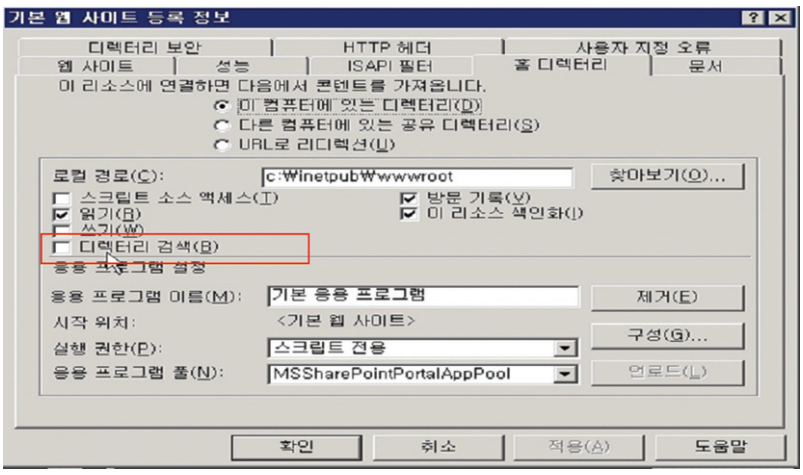
– [시작] ⇒ [프로그램] ⇒ [관리 도구] ⇒ [인터넷 정보 서비스]를 실행시킨 후 [기본 웹 사이트]에 대해 마우스 오른쪽 버튼을 클릭한 후 [속성]을 선택

〈그림 3-38〉 기본 웹사이트 속성 선택



– [디렉토리] 탭에서 [디렉토리 검색]을 다음 그림과 같이 체크되지 않은 상태로 유지

〈그림 3-39〉 디렉토리 검색 기능 해제



5. 메일 서버를 안전하게!

5.1 메일서버 환경 설정하기

■ 정보보호 현안 및 예상 피해

• MS Exchange Server 환경 설정

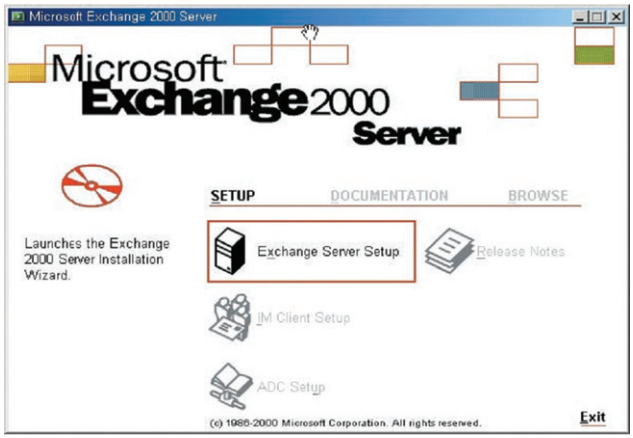
- MS Exchange Server는 Windows server 사용자가 손쉽게 MS IIS Server와 함께 메일서버를 구축할 수 있는 방법이다. 기본적으로 Exchange 2000을 설치하기 위해서는 Windows 2000 server 이상의 운영체제와 서비스팩 1 이상 설치 및 AD, IIS(SMTP 포함), NNTP가 설치되어 있는 시스템이 필요하다.

■ 보호대책

• MS Exchange Server 설치하기

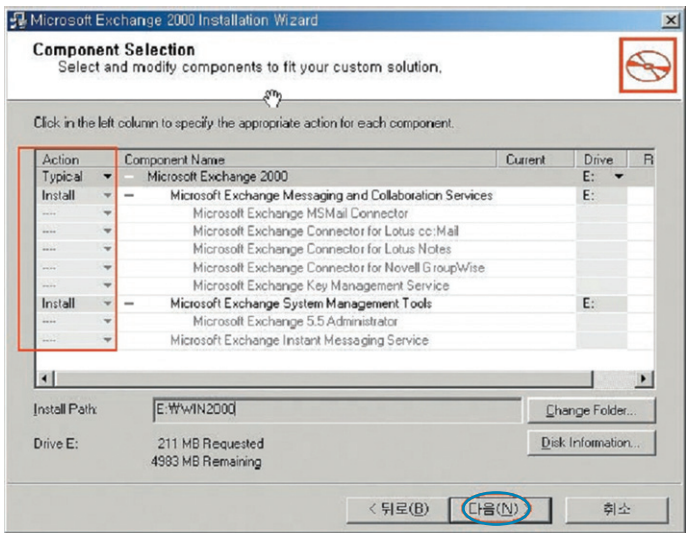
- 컴퓨터에 Exchange CD-ROM을 넣고 자동실행 화면이 나타나면 [Exchange Server Setup]을 선택

〈그림 3-40〉 Microsoft Exchange Server Setup 화면



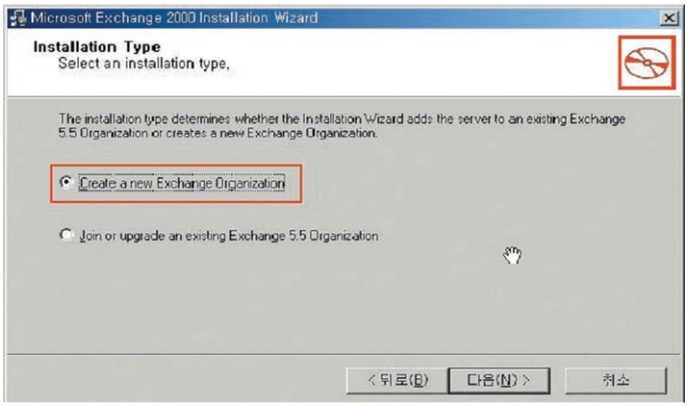
– 라이센스 화면 및 CD-Key 값을 입력한 후 설치 구성요소를 선택하기 위한 설치방법 선택 화면이 나타나면 설치방법을 선택하며, 일반적으로 Typical 설치를 권장

〈그림 3-41〉 Typical 설치 선택



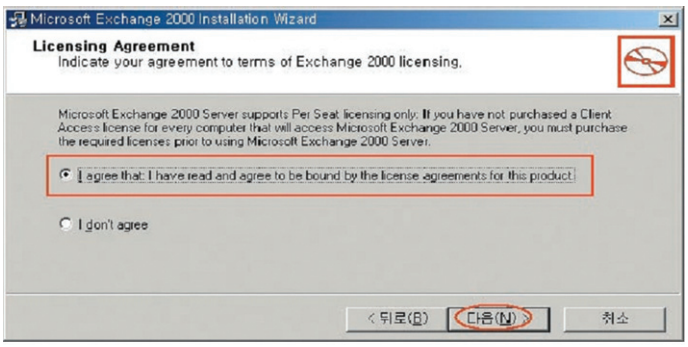
- [Install Type]를 선택하는 화면에서는 신규 설치 또는 기존 Exchange를 2000으로 업그레이드하는 것을 선택할 수 있음

〈그림 3-42〉 신규 설치 또는 업그레이드 선택



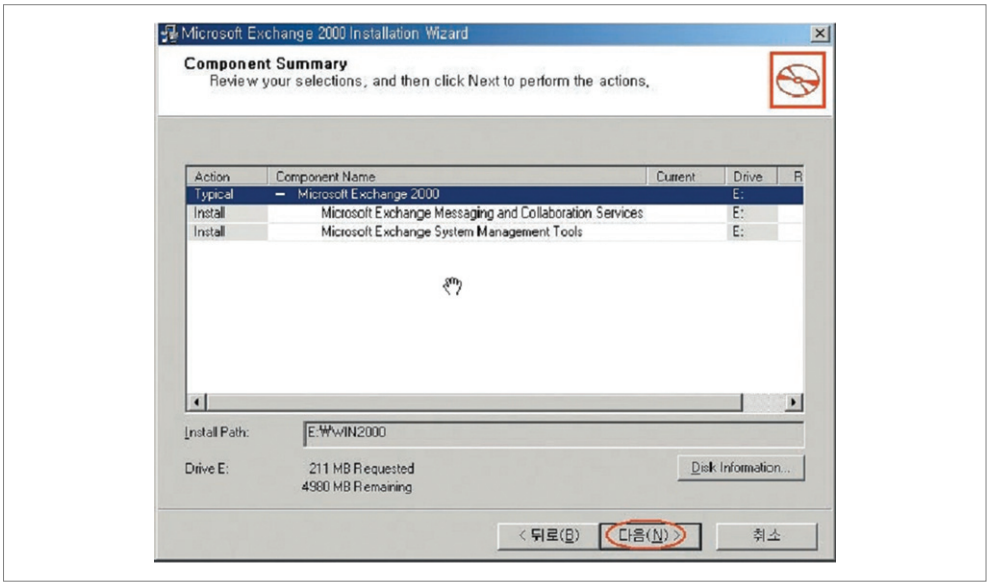
- [Organization Name]를 설정한 후 [Licensing Agreement] 화면이 나타나면, Exchange 2000은 클라이언트 라이센스에 사용자 단위 라이센스만을 허용하며, 사용자 수에 맞는 라이센스를 구입하여야 한다는 내용에 동의

〈그림 3-43〉 라이센스 동의 화면



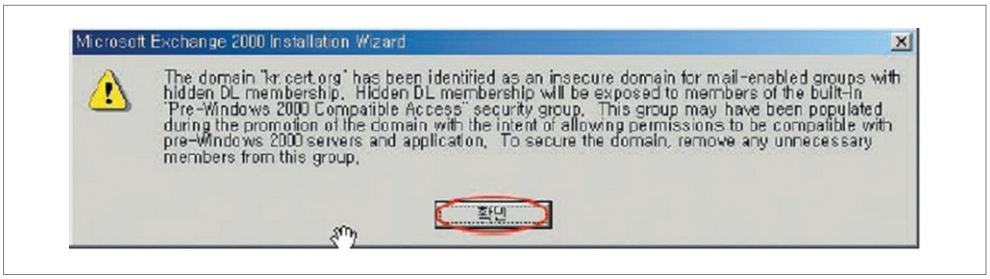
– 설치과정에서 선택한 모든 설치 구성요소가 적절히 표시되었는지 최종적으로 확인

〈그림 3-44〉 설치 구성요소 표시 확인



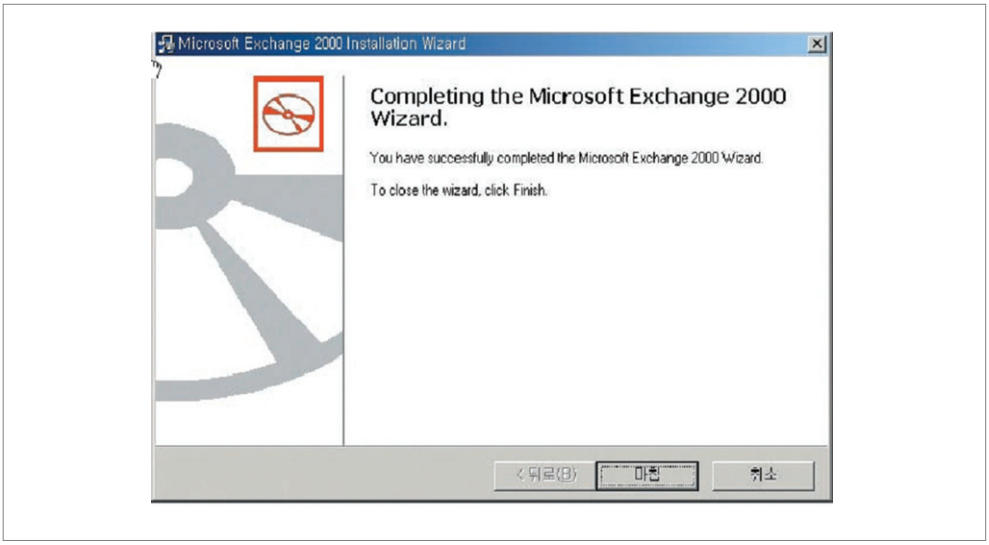
– 아래 그림에서 [확인]을 클릭하여 마법사를 실행

〈그림 3-45〉 설치 마법사 실행



– 설치 과정을 거쳐 아래와 같이 설치가 완료됨

〈그림 3-46〉 Microsoft Exchange 설치 완료



5.2 스팸 릴레이 방지하기

■ 정보보호 현안 및 예상 피해

• 스팸 발송 및 메일 서버 비정상 동작 발생

– 스팸릴레이 방지 설정을 하지 않고 운영되는 메일 서버가 스팸 메일 발송 서버로 악용되는 사례가 많다.

– 메일 서버의 관리 소홀로 인해 스팸 메일이 발송될 경우 회사와 담당자에게 직 · 간접적으로 피해가 발생할 수 있을 뿐만 아니라 메일 서버가 다량의 메일을 발송하게 됨에 따라 서버자체의 부하가 증가되어 정상

적인 동작을 방해받는다.

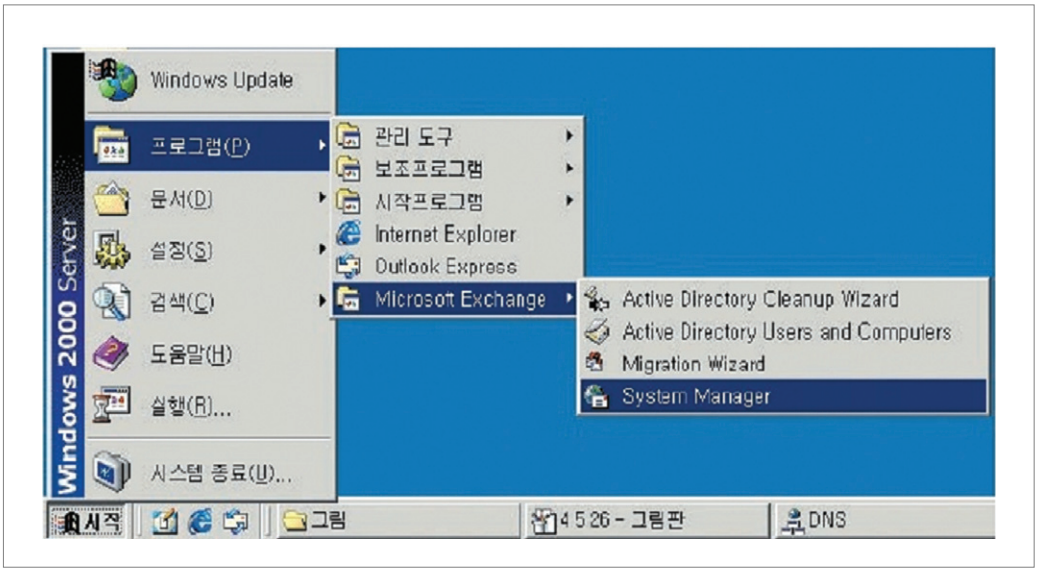
■ 보호대책

• MS Exchange Server 스팸 메일 릴레이 방지하기

– 스팸 메일 릴레이를 방지하기 위해서는 메일 릴레이를 허용하는 IP대역을 지정함으로써 그 외 모든 대역에서의 메일 릴레이를 차단

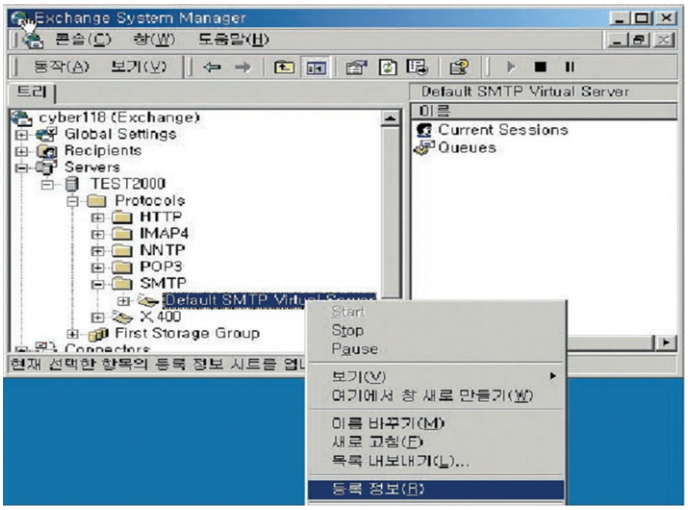
– [시작] ⇒ [프로그램] ⇒ [Microsoft Exchange] ⇒ [System Manager] 선택

〈그림 3-47〉 Microsoft Exchange System Manager 선택



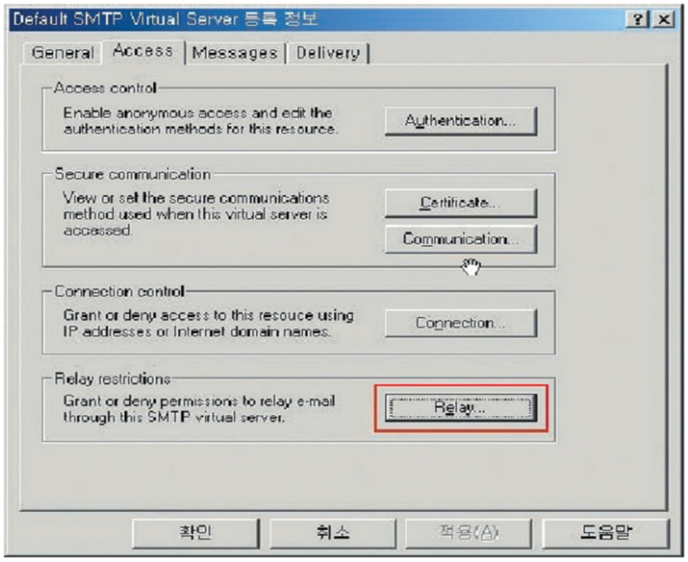
– [Servers] ⇒ [서버명] ⇒ [Protocol] ⇒ [SMTP] ⇒ [Default SMTP Virtual Server]에서 마우스 오른쪽 버튼을 클릭하여 [등록정보]를 선택

〈그림 3-48〉 Default SMTP Virtual Server 등록정보 선택



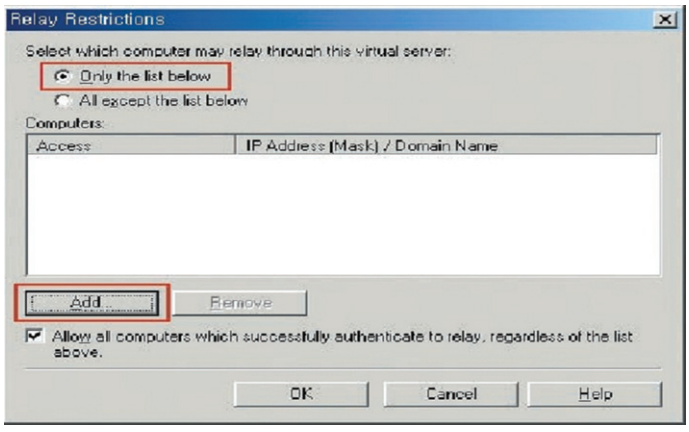
- [Access] 탭을 선택한 후 [Relay] 버튼을 클릭

〈그림 3-49〉 Access 탭의 Relay 선택



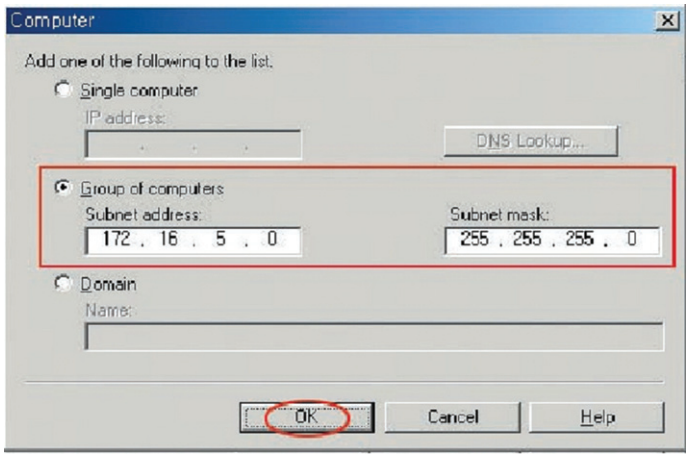
- [Only the list below]를 체크한 후 아래 부분에 있는 [Add] 버튼 클릭하여 릴레이를 허용할 IP 주소를 입력

〈그림 3-50〉 릴레이를 허용할 IP 주소 추가



- 중간에 있는 [Group of computers]를 체크한 후 릴레이를 허용할 [Subnet address]와 [Subnet mask]를 입력한 후 [OK]버튼을 클릭

〈그림 3-51〉 릴레이를 허용할 Subnet 주소와 Subnet mask 입력



제 4 장 응용서비스 개발편

Ⅳ

1. 웹 페이지 개발시, 이렇게!

1.1 XSS 방지를 위한 프로그램 작성 방법

■ 정보보호 현안 및 예상 피해

- XSS(Cross Site Script)는 불법적인 의도를 가진 공격자가 웹 어플리케이션을 이용하여 다른 일반 사용자에게 악성 코드를 보내는데 사용할 수 있는 취약점이다.

- 이런 악성 코드는 일반적으로 스크립트 형태로 이루어져 있고, 매우 보편적으로 나타나는 문제이며, 사용자의 입력을 받아들여서 별도의 입력값 검증 없이 반환하는 웹 어플리케이션의 경우 찾아볼 수 있는 취약점이다.

- 웹 브라우저는 이 스크립트가 신뢰할 수 있는 사이트로부터 전송되었다고 생각하기 때문에, 악성 스크립트는 해당 사이트에서 사용하는 브라우저 쿠키, 세션 토큰 혹은 다른 민감한 정보에 접근할 수 있고, 이 스크립트는 심지어 HTML 페이지의 내용을 조작하여 변경할 수도 있다.

〈그림 4-1〉 XSS 피해 사례

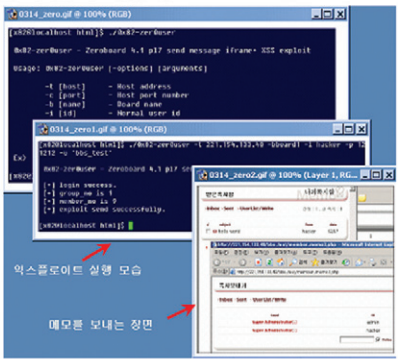
[CNet 월드뉴스]날뛰는 변종 피싱 혹 집어낼수 없나

[디지털타임스 2005-04-12 10:56]

XSS · 브라우저 취약점 이용하는 등

전문범죄 · 기술 합작사례 확산 추세

기관 · 고객`온라인 범죄'일전 벌여야



최근 들어 피싱 공격의 발생 빈도가 줄어들고 있다는 좋은 소식이 들려오고 있다. 온라인 사기를 감시하는 피싱방지실무그룹(APWG)은 올 1월과 2월 사이에 발견된 피싱(phishing) 사기 이메일이 2% 증가하는 수준에 그쳤다고 지난 주 발표했다.

이러한 수치는 지난해 7월 이후 매달 평균 26%씩 증가한 것을 감안하면 상당히 감소한 것이다. 그러나 전문가들은 1월과 2월 사이에 피싱 공격 수법이 훨씬 더 복잡해졌다고 말한다.

피싱 사기 공격이 어떤 형태를 취하든 피싱 사기 수법, 예를 들면 파밍 · 크로스 사이트스크립팅(cross-site scripting) · DNS 포이즈닝 등은 날이 갈수록 지능화되고 있다.

마이크로소프트(MS)는 최근 피싱 웹사이트를 운영한 혐의자들을 대상으로 117개의 소장을 제출하면서 온라인 범죄와의 전쟁을 선포했다.

MS의 변호사인 아론 콘블럼은 "피싱 사기꾼들은 도둑이다. 이 신종 도둑들은 실제 세계에서와 마찬가지로 온라인에서도 피해자의 개인 금융 정보와 여타 데이터를 빼내려고 갖은 방법을 다 쓰고 있다"라고 말했다.

• XSS 공격의 종류는 두 가지가 있다.

구분	내역
저장식 공격	– 공격자에 의해 삽입된 코드가 데이터베이스나 게시판, 접속자 로그 정보, 주석 등 대상 서버 상에 영구적으로 저장 – 피해자는 서버에 저장된 정보를 요청하는 과정에서 악성 스크립트를 내려받음
반향식 공격	– 공격자에 의해 삽입된 코드가 웹 서버를 통해 반향되는 것으로, 웹 서버의 에러 메시지, 검색 결과 또는 서버에 대한 요청의 결과로 요청시 입력한 값들을 전부 혹은 일부를 응답으로 보낼 때 발생 – 피해자에게 전자 메일 메시지나 다른 웹 서버와 같이 해당 웹 서버가 아닌 다른 경로를 통해 전달

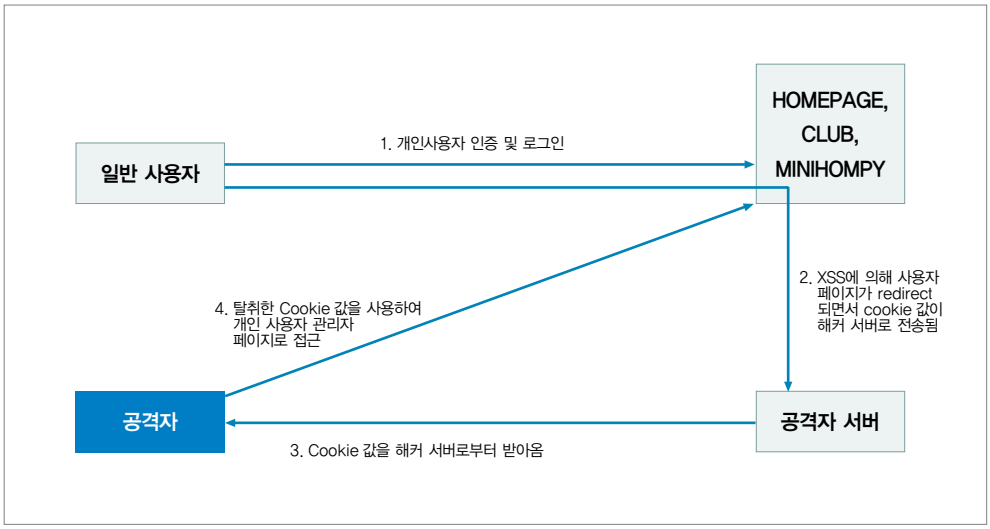
• XSS의 문제점에 대한 원인은 다음과 같다.

① HTTP 프로토콜의 비 연결 지향성으로 인한 Cookie의 사용

② 게시판 등에 글을 올릴 경우 HTML 태그 문자 혹은 JavaScript의 허용

③ 사용자 입력 값의 필터링(filtering) 부재

〈그림 4-2〉 XSS 공격의 개념도



■ 보호대책

• XSS 취약점 존재 가능 점검

– 사용자의 홈페이지 및 사용자의 브라우저에 아래와 같이 〈Script〉 태그가 포함된 URL을 입력하여 팝업창이 뜨면 취약점이 존재한다.

〈그림 4-3〉 쿠키 정보 불법 수집 가능 점검

http://test.site.com/default.asp · 〉〈script〉alert('test')〈/script〉

// 테스트라는 경고창이 뜨면 쿠키 정보를 불법적으로 획득 가능함

• 문자열 치환을 통한 XSS 취약점 방지

– XSS 공격으로부터 웹 어플리케이션을 방어하는 최선의 방법은 어플리케이션 차원에서 HTTP 헤더, 쿠키, 쿼리 스트링, 폼 필드, 히든 필드 등의 모든 인자들에 대해 허용된 유형의 데이터만을 받아들이도록 입력값 검증을 실시하는 것이다.

– 아래와 같은 문자들을 사용자에게 반환할 때는 적절한 HTML 엔티티 인코딩으로 변환하면 스크립트 기반의 공격에 대해 방어가 가능하다.

[표 4-1] 문자열 치환표

From	To	From	To	From	To
〈	&lt;	〉	&gt;	(	&#40;
)	&#41;	#	&#35;	&	&#38;

• 스크립트 별 XSS 방지 예

– ASP 안전한 프로그램 방식 예

```
If use_html Then' HTML tag를 사용하게 할 경우 부분 허용
memo = Server.HTMLEncode(memo) 'HTML tag를 모두 제거

' 허용할 HTML tag만 변경
memo = replace(memo, "&lt;p&gt;", "<p>")
memo = replace(memo, "&lt;P&gt;", "<P>")
memo = replace(memo, "&lt;br&gt;", "<br>")
memo = replace(memo, "&lt;BR&gt;", "<BR>")

Else' HTML tag를 사용하지 못하게 할 경우
memo = Server.HTMLEncode(memo)' HTML encoding 수행
memo = replace(memo, "<", "&lt;")
memo = replace(memo, ">", "&gt;")
End If

Response.write "게시물 내용-" & memo & "<BR>"
```

– PHP 안전한 프로그램 방식 예

```
if(use_html) // HTML tag를 사용하게 할 경우 부분 허용
memo = memo.replaceAll("<","&lt;");//HTML tag를 모두 제거
memo = memo.replaceAll(">","&gt;");

// 허용할 HTML tag만 변경
memo = memo.replaceAll("&lt;p&gt;", "<p>");
memo = memo.replaceAll("&lt;P&gt;", "<P>");
memo = memo.replaceAll("&lt;br&gt;", "<br>");
memo = memo.replaceAll("&lt;BR&gt;", "<BR>");

else // HTML tag를 사용하지 못하게 할 경우
memo = memo.replaceAll("<","&lt;");
memo = memo.replaceAll(">","&gt;");

out.print("게시물 내용-" + memo + "<BR>");
```

– JSP 안전한 프로그램 방식 예

```
$use_tag = "img,font,p,br";// 허용할 HTML tag

if($use_html == 1) // HTML tag를 사용하게 할 경우 부분 허용
$memo = str_replace("<", "&lt;", $memo);// HTML TAG를 모두 제거

$tag = explode(",", $use_tag);
for($i=0; $i<count($tag); $i++) // 허용할 TAG만 사용 가능하게 변경
$memo = eregi_replace("&lt;".$tag[$i]." ", "<".$tag[$i]." ", $memo);
$memo = eregi_replace("&lt;".$tag[$i].">", "<".$tag[$i].">", $memo);
$memo = eregi_replace("&lt;/".$tag[$i], "</".$tag[$i], $memo);

else // HTML tag를 사용하지 못하게 할 경우

// $memo = htmlspecialchars($memo);
// htmlspecialchars() 사용시 일부 한글이 깨어지는 현상이 발생 할 수 있음

$memo = str_replace("<", "&lt;", $memo);
$memo = str_replace(">", "&gt;", $memo);


echo "게시물 내용-" . $memo . "<BR>\n";
```

1.2 SQL Injection 방지를 위한 검색문 검증

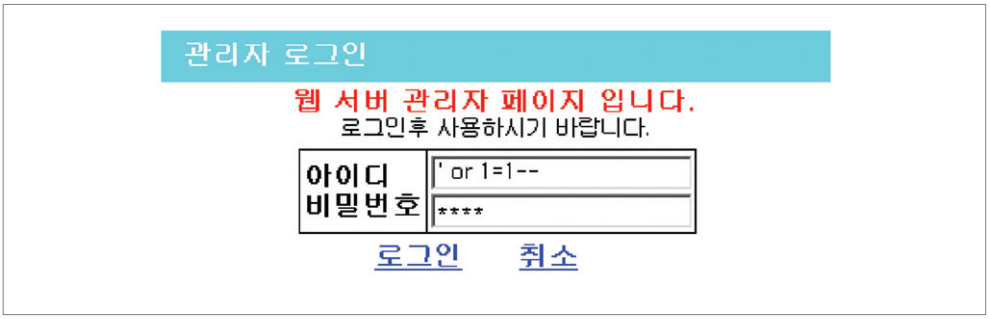
■ 정보보호 현안 및 예상 피해

- SQL Injection은 DB서버에 전달되는 SQL쿼리를 변조하여 의도되지 않은 동작을 실행함으로써 불법적으로 관리자 페이지 및 DB에 접속을 시도하여 중요 정보를 열람하거나 빼내갈 수 있다.

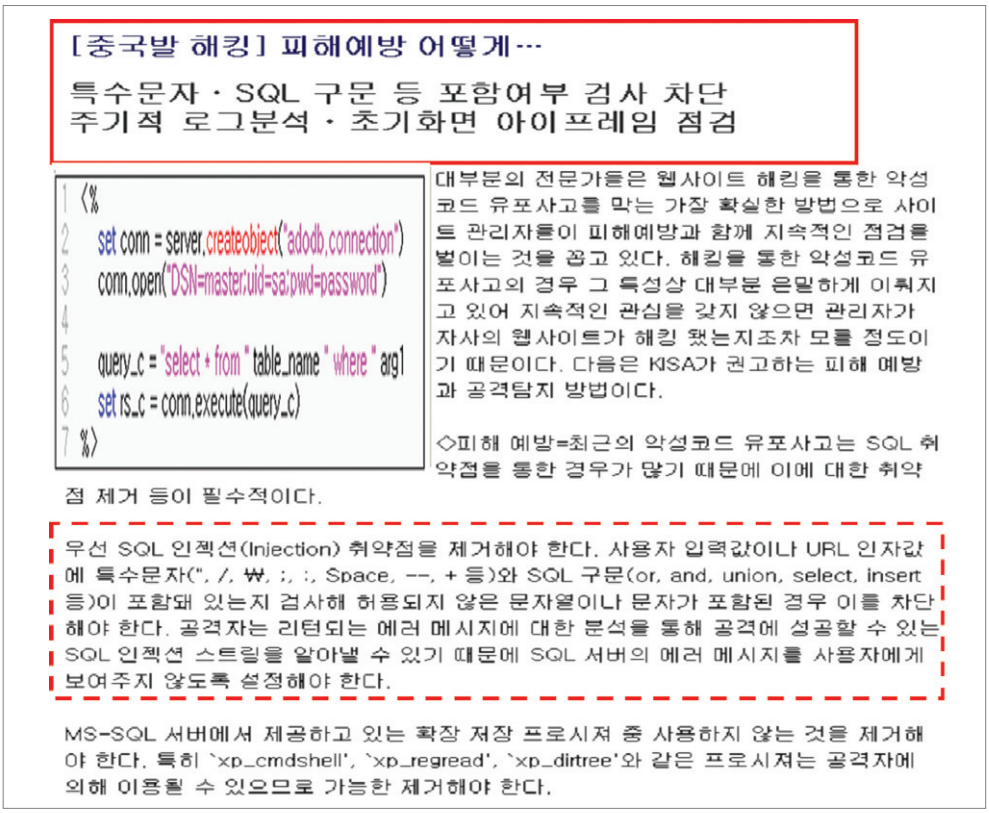
- 웹 응용 프로그램에서 사용하는 변수명에 SQL문이 삽입되어 데이터베이스에 악의적 영향을 미치는 취약점으로 사용자/관리자 인증 우회, DB 파괴, 정보 노출, 서버 내부의 명령 실행이 가능하다.

• 공격자가 특별히 고안된 script를 웹 페이지에 삽입해서 일반 사용자의 세션 및 쿠키 정보를 불법으로 획득할 수 있다.

〈그림 4-4〉 SQL Inject을 이용한 관리자 페이지 로그인 예



〈그림 4-5〉 SQL Injection 피해 사례



■ 보호대책

• 취약점 점검
  – 검색어 필드 및 ID/Passwd 필드에 큰따옴표(“), 작은따옴표(‘), 세미콜론(;) 등을 입력한 후, DB error가 일어나는지 반드시 확인해야 한다.
  – MS SQL인 경우 ID 필드에 [‘or 1=1 ;--], 비밀번호 필드에는 아무 값이나 입력한 후 로그인을 시도하여 점검해야 한다.
  – Oracle인 경우 ID 필드에 [‘or 1=1 ;--], 비밀번호 필드에는 아무 값이나 입력한 후 로그인을 시도하여 점검해야 한다.

• 입력값 검증을 통한 SQL Injection 방지
  – 웹 상에서 입력된 데이터에 대해 주의 깊게 입력값 검증을 수행하며, SQL Injection을 발생시킬 수 있는 특수문자가 삽입되지 않도록 replace 함수를 이용하여 특수 문자열을 일반 문자열로 아래 표와 같이 치환하도록 한다.

[표 4-2] 치환 문자표

From	To	From	To	From	To
‘	\’	–	\–	“	\”

• 스크립트 별 SQL Injection 방지 예

– ASP 안전한 프로그래밍 예

```
prodId = Request.QueryString("productId")
prodId = replace(prodId, "'", "''")' 특수문자 제거
prodId = replace(prodId, ";", "")
set conn = server.createObject("ADODB.Connection")
set rs = server.createObject("ADODB.Recordset")
query = "select prodName from products where id = " & prodId
conn.Open "Provider=SQLOLEDB; Data Source=(local);
Initial Catalog=productDB; User Id=dbid; Password="
rs.activeConnection = conn
rs.open query
If not rs.eof Then
response.write "제품명" & rs.fields("prodName").value
Else
response.write "제품이 없습니다"
End If
```

– PHP 안전한 프로그래밍 예

```
$query = sprintf("SELECT id,password,username FROM user_table WHERE
id='%s';",addslashes($id));
// id변수를 문자형으로 받고, id변수의 특수문자를 일반문자로 변환한다.

// @ 로 php 에러 메시지를 막는다.
$result = @OCIParse($conn, $query);
if (!@OCIExecute($result))
error("SQL 구문 에러");
exit;

@OCIFetchInto($result,&$rows);
... 중략 ...
```

– JSP 안전한 프로그래밍 예

```
String sql = "SELECT * FROM user_table" + " WHERE id = ?" + " AND password = ?";
ResultSet rs = null;
PreparedStatement pstmt = null;
try
conn = DBManager.getConnection();
pstmt = conn.prepareStatement(sql);

pstmt.setString(1, request.getParameter("id"));
pstmt.setString(2, request.getParameter("password"));

rs = pstmt.executeQuery();
```

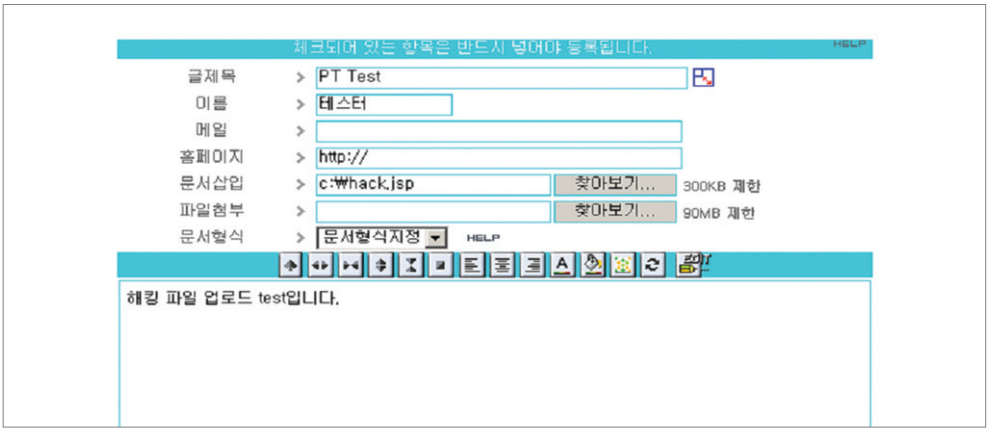
1.3 File Upload 방지하기

■ 정보보호 현안 및 예상 피해

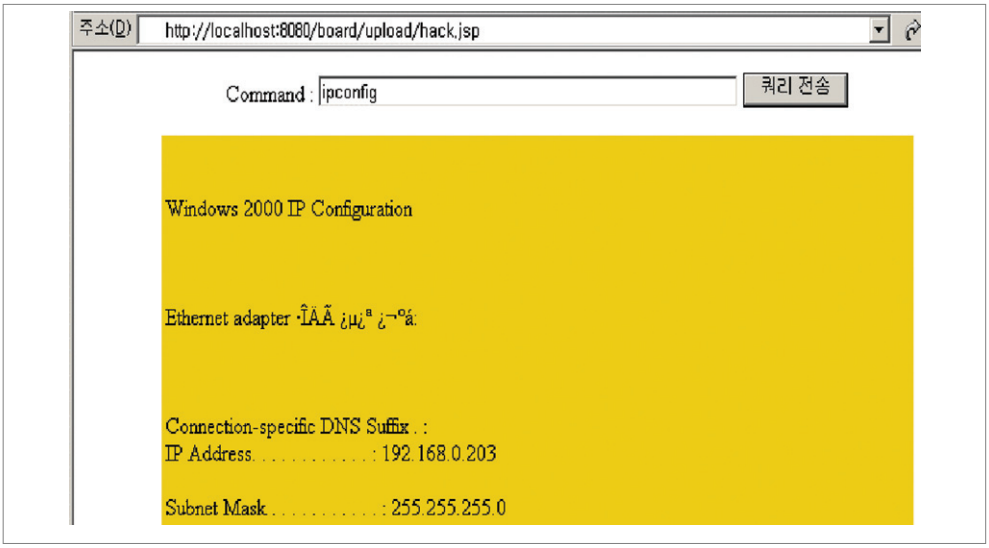
• 게시판, 자료실 등에 파일 첨부 기능이 있는 경우 발생할 수 있는 취약점으로 웹 서버에 스크립트 파일을 첨부하여 올릴 수 있고, 파일이 저장되는 디렉토리가 스크립트의 실행을 제한하지 않는 경우 발생할 수 있다.

• 해킹 스크립트의 업로드가 성공하게 되면 웹 브라우저 상에서 시스템에 명령을 내리고 그 결과를 얻는 것이 가능해진다.

〈그림 4-6〉 File Upload 기능이 있는 게시판



〈그림 4-7〉 FileUpload 취약점 실행 결과 화면



■ 보호대책

• 취약점 점검

– 사용자 게시판에 파일 첨부 기능이 있는지 조사해야 한다. (게시판,

공개 자료실, 관리자 자료실, 이미지 자료실 등)

- 첨부기능이 존재하는 경우, 파일 확장자가 jsp, php, asp, cgi 등으로 된 Server Side Script 프로그램의 업로드 가능 여부에 대해 조사해야 한다.
- javaScript, VBscript 등의 스크립트로 파일첨부를 차단하는 경우 아래와 같이 파일명을 수정하여 파일 첨부가능 여부를 점검해야 한다.

```
// 이중 확장자를 적용하여 업로드 점검
예제) hack.txt.asp
// 확장자를 대문자로 적용하여 업로드 점검
예제) hack.ASP
//체크하지 않은 확장자를 선택하여 점검
예제) hack.asa
```

• 웹서버의 디렉토리 권한 조정

- 업로드 된 파일이 저장되는 디렉토리의 권한을 조정해야 하고 서버에서 파일이 저장되는 디렉토리는 스크립트가 실행되지 않도록 한다.
- 파일이 서버에 저장될 때 파일명 및 확장자를 변경하여 파일로 저장하고, 원래의 이름은 DB의 테이블에 저장하도록 한다.
- 파일을 upload 스크립트에서 확장자 필터링을 하도록 한다. 이 때, 실제 filtering을 수행하는 부분은 서버 측에서 동작하도록 코딩한다.

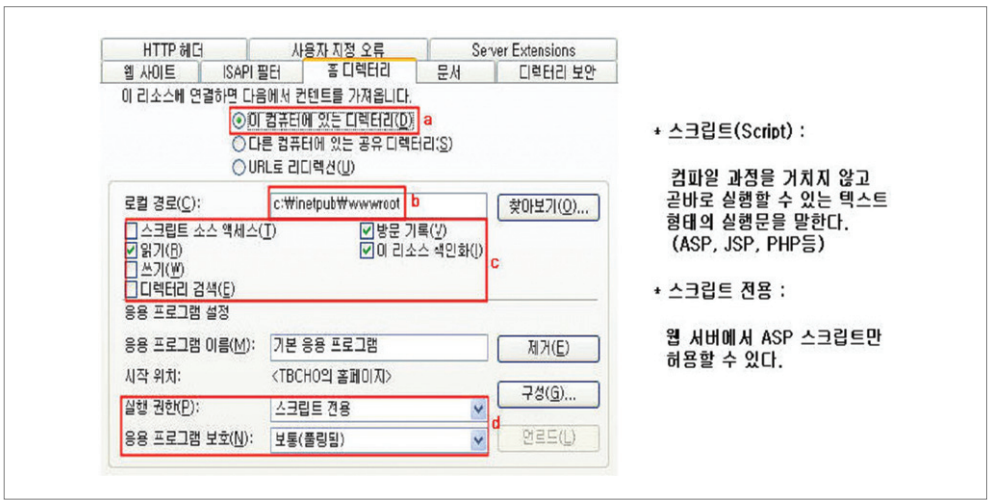
```
CGI, PL, HTML, HTM, PHP, PHP3, INC, ASP, ASA, JSP
```

• IIS 웹 서버의 디렉토리 실행 권한 제어

- IIS 서버 보안 설정 : 설정 ⇒ 제어판 ⇒ 관리도구 ⇒ 인터넷 서비스

관리자 선택. 해당 업로드 폴더에 오른쪽 클릭을 하고 등록정보 ⇒ 디렉토리 ⇒ 실행권한을 "없음"으로 설정한다.

〈그림 4-8〉 IIS 웹서버 디렉토리 실행권한 비 활성화



• Apache 웹 서버의 디렉토리 실행 권한 제어

– Apache 서버는 "httpd.conf" 파일에서 해당 디렉토리에 대한 문서 입력을 컨트롤하기 위해 Directory 섹션의 AllowOverride option에서 fileInfo 또는 All 추가

```
〈Directory "/user/local/apache"〉
AllowOverride FileInfo (또는 All) ...
....,
....,
〈/Directory〉
```

– 파일 업로드 디렉토리에 .htaccess 파일을 만들고 AddType 지시자를

이용, 웹 서버에서 운영되는 Server Side Script 확장자를 text/html로 MIME Type를 재조정하여 업로드된 Server Side Script가 실행되지 않도록 설정

```
<.htaccess>
<FilesMatch "\.(ph|inc|lib)">
  Order allow, deny
  Deny from all
</FilesMatch>
AddType text/html .html .htm .php .php3 .php4 .phtml .phps .in .cgi .pl .shtml .jsp
```

• 스크립트 별 파일 업로드 방지 예

– ASP 안전한 프로그래밍 예

```
<%
Set Up = Server.CreateObject("SiteGalaxyUpload.Form")
Path1 = server.mappath(".") & "\upload\"

Fname = Up("file1")

if Fname <> "" then'파일 첨부가 되었으면

if Up("file1").Size > 10240 then' 용량 제한
Response.Write "용량 초과"
Response.End
end if

if Up("file1").MimeType <> "image" then' 이미지만 업로드 허용
Response.Write "이미지 파일이 아닙니다."
Response.End
end if

Filename=Mid(Fname,InstrRev(Fname,"\")+1)'파일이름부분 추출

' 중복시에 파일이름부분을 변경하기 위해 분리를 한다
Farry=split(Filename,".")'.을 기준으로 분리
preFname=Farry(0)'파일이름 앞부분
extFname=Farry(1)'파일의 확장자

' 저장할 전체 path를 만든다, 파일이름을 구한다
Path2 = Path1 & Filename
```

```
saveFname=preFname & "." & extFname


Set fso = CreateObject("Scripting.FileSystemObject")
countNo = 0' 파일 중복될경우 셋팅 값
fExist=0' 같은 이름의 파일 존재 체크
Do until fExist = 1
If(fso.FileExists(Path2)) Then
countNo = countNo + 1
Path2 = Path1 & preFname & countNo & "." & extFname
saveFname=preFname & countNo & "." & extFname
else
fExist=1
End If
Loop

Up("file1").SaveAs(Path2)
response.write(saveFname & " 저장완료")
else
response.write("Error")
end if

Set Up = nothing
%>
```

– PHP 안전한 프로그래밍 예

```
<?php
$uploaddir = '/var/www/uploads/';

//파일 사이즈가 0byte 보다 작거나 최대 업로드 사이즈보다 크면 업로드를 금지 시킨다.
if($_FILES['userfile']['name'])
if($_FILES['userfile']['size'] <= 0)  // 최대 업로드 사이즈 체크 삽입
print "파일 업로드 에러";
exit;

//파일 이름의 특수문자가 있을 경우 업로드를 금지 시킨다.
if (eregi("[^a-z0-9\._\-]",$_FILES['userfile']['name']))
print "파일 이름의 특수문자 체크";
exit;

//파일 확장자중 업로드를 허용할 확장자를 정의한다.
$full_filename = explode(".", $_FILES['userfile']['name']);
$extension = $full_filename[sizeof($full_filename)-1];
```

```
/* PHP의 경우 확장자 체크를 할 때 strcmp(확장자,"php3"); 로 체크를 하게 되면 pHp3
이나 phP3는 구별을 하지 못하게 되므로 strcasecmp처럼 대소문자 구별을 하지 않고
비교하는 함수를 사용한다. 또한 .를 기준으로 하여 확장자가 하나로 간주하고
프로그램을 할 경우 file.zip.php3 이라고 올린다면 zip파일로 인식하고 그냥 첨부가
되므로 아래와 같이 제일 끝에 존재하는 확장자를 기준으로 점검하도록 한다. */

$extension= strtolower($extension);
if (!( ereg($extension","hwp") || ereg($extension","pdf") || ereg($extension","jpg")) )
print "업로드 금지 파일 입니다";
exit;


$uploadfile = $uploaddir. $_FILES['userfile']['name'];
if (move_uploaded_file($_FILES['userfile']['tmp_name'], $uploadfile))
print "파일이 존재하고, 성공적으로 업로드 되었습니다.";
print_r($_FILES);
else
print "파일 업로드 공격의 가능성이 있습니다! 디버깅 정보입니다:\n";
print_r($_FILES);

?>
```

- JSP 안전한 프로그래밍 예

```
<%@ page contentType="text/html;charset=euc-kr" %>
<%@ page import="com.oreilly.servlet.MultipartRequest,com.oreilly.servlet.multipart.
DefaultFileRenamePolicy, java.util.*"%>
<%
String savePath="/var/www/uploads";// 업로드 디렉토리
int sizeLimit = 5 * 1024 * 1024 ; // 업로드 파일 사이즈 제한

try
MultipartRequest multi=new MultipartRequest(request, savePath, sizeLimit, "euc-kr", new
DefaultFileRenamePolicy());
Enumeration formNames=multi.getFileNames();  // 폼의 이름 반환
String formName=(String)formNames.nextElement();
String fileName=multi.getFilesystemName(formName); // 파일의 이름 얻기

String file_ext = fileName.substring(fileName.lastIndexOf('.') + 1);
if(!( file_ext.equalsIgnoreCase("hwp") || file_ext.equalsIgnoreCase("pdf") ||
file_ext.equalsIgnoreCase("jpg")) )
out.print("업로드 금지 파일");
```

```
if(fileName == null)
out.print("파일 업로드 실패");
 else
fileName=new String(fileName.getBytes("8859_1"),"euc-kr"); // 한글인코딩
out.print("File Name  : " + fileName);

 catch(Exception e)
```

1.4 File Download 방지하기

■ 정보보호 현안 및 예상 피해

• 웹 서버에서 파일을 다운로드 하는 경우 스크립트에서 해당 파일을 열어서 전송하도록 작성을 할 수 있다.

• 이 때, URL의 다운로드 스크립트의 인수 값에 "../" 문자열 등을 입력하게 되면 웹 서버에 저장된 모든 파일을 다운로드할 수 있게 되어 중요 자료나 개발 소스 등을 불법적으로 획득할 수 있다.

• 웹 페이지에서 cgi, jsp, php, php3 등의 프로그램에서 입력되는 경로를 체크하지 않는 경우, 임의의 문자(../.. 등)나 주요 파일명의 입력을 통해 웹 서버의 홈 디렉토리를 벗어나서 임의의 위치에 있는 파일을 열람하거나 다운받을 수 있다.

• 인수 조작을 이용하여 다운로드 수행

```
1) download.jsp · filename=../../../../../../../boot.ini
2) download.jsp · filename=..%2F..%2F..%2F..%2F..%2F..%2F..%2F
   boot.ini
```

〈그림 4-9〉 인수조작을 통한 불법 파일 다운로드

■ 보호대책

• 파일다운로드 스크립트를 사용하지 않고 직접 링크를 걸어 사용한다.

• 서버 측에서 동작하는 스크립트에 경로(../..\\)검사를 하는 함수를 작성하여 사용한다.

• 게시판에서 첨부파일 저장 시 첨부 파일의 저장 위치를 웹에서 접근할 수 없는 디렉토리로 설정한다.

• Chroot()함수를 사용하여 웹 상에서 접근할 수 있는 디렉토리의 경로 이동을 제한시킨다.

• 특정 디렉토리에서만 파일을 다운로드 받을 수 있도록 하여, 파일명 및 디렉토리에 대한 조작이 있더라도 특정 디렉토리를 벗어날 수 없도록 한다.

※ 다운로드 스크립트 Filtering 수행 코드 작성사례

– 다운로드 기능을 구현한 Script의 경우, 다운로드 하려는 파일명을 먼저 체크한 후에 다운로드를 시도해야 함

– 비인가자가 ../../../../../ 과 같이 ../과 ./을 불규칙하게 사용할 수 있기 때문에 파일명전체에 걸쳐 ../의 치환이 이루어져야 함

```
// ASP 경우
'ASP Script
string userInput = UserInput.Text;
userInput = userInput.Replace("../", ""); '../ 스트링을 치환

// JSP 경우
String userInput = request.getParameter("filename");
/% userInput에 대해서 ../ 스트링을 치환. %/
userInput.replaceALL("../", "")

// PHP 경우
$userInput = $_GET( 'filename' )
str_replace("\.\.\/", "", $userINPUT);
```

※다운로드 경로 체크 코드 사례

– 파일 다운로드 스크립트를 사용할 경우 아래 예와 같은 함수를 서버 측에서 동작하는 다운로드 스크립트에 작성하여 경로를 이탈하지 못하도록 함

```
try {
    filename =  request.getParameter("filename");
    path = request.getParameter("path");
    dir = request.getParameter("dir");

    String fileRoot = "";

    if((filename.indexOf("../") != -1) || (filename.indexOf("../")
        != -1)){
            throw  new Exception("경로가 잘못되었습니다.");
                                    }

    if ( path == null || path == "" ) {
        fullFilePath = filename;
} else {
        try  {
          LConfiguration conf = LConfiguration.getInstance();
          fileRoot = conf.get( "/download/path/" + path);
                fullFilePath = fileRoot + "/"  + filename;
       } catch ( Exception e ) {
          fullFilePath = filename;
       }
      }
```

1.5 관리자 페이지 인증 강화

■ 정보보호 현안 및 예상 피해

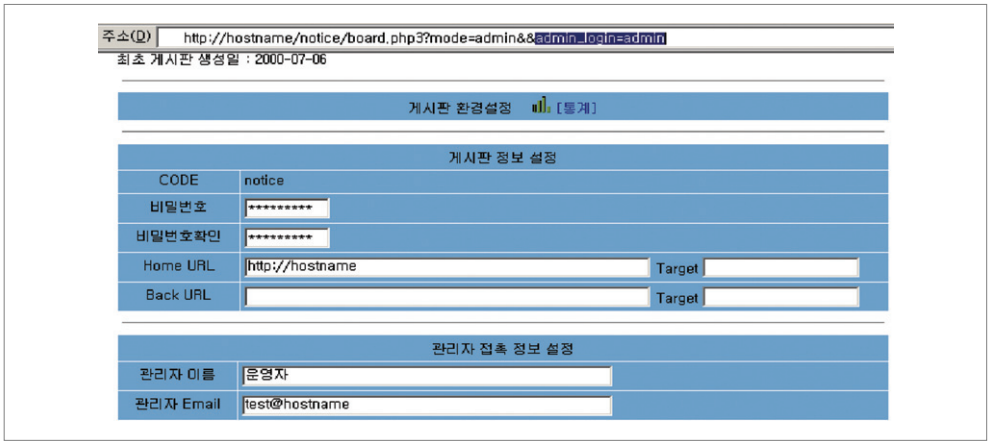
• 관리자 페이지는 웹 서비스의 사용자나 데이터, 콘텐츠를 손쉽게 관리하기 위한 목적으로 다양한 기능과 권한을 갖고 있다.

• 따라서 일반적으로 추측하기 쉬운 URL(예 : /admin, /manager)을 사용하고 있어, ID/Password 만 알고 있다면 일반사용자도 관리자 페이지에 접속이 가능하다.

• 이에 따라 웹 관리자의 권한이 노출될 경우 홈페이지의 변조뿐만 아니라 취약성 정도에 따라서 웹 서버의 권한까지 노출될 수 있다.

• 스크립트(예: PHP, ASP, JSP 등) 내부 변수 조작을 통한 관리자 페이지 접속으로 내부 변수인 admin_login 변수를 입력하여 패스워드가 없어도 관리자 페이지에 접근이 가능하다.

〈그림 4-10〉 내부 변수를 이용한 관리자 페이지 접근 가능 예



■ 보호대책

• 관리자가 사용하는 모든 웹 어플리케이션의 경우 소스의 상단에 관리자 인증 모듈을 추가하여 인가된 관리자만 접근이 가능하도록 수정해야 한다.

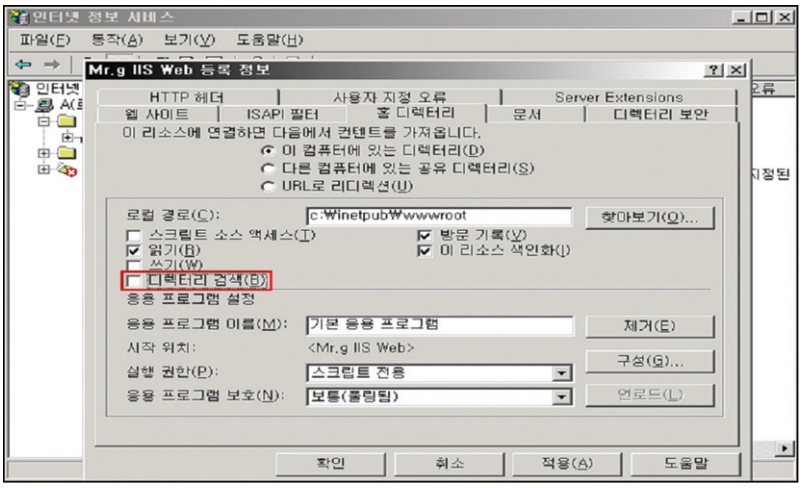
• 관리자 인증 모듈이 빠져있는 채로 운영되는 웹 어플리케이션이 존재할 수 있으므로 관리자의 모든 파일을 주기적으로 점검한다.

• 웹 서버의 디렉토리 인덱싱 서비스 정지

```
// 아파치 웹서버의 디렉토리 인덱싱 방지
   // httpd.conf 파일에 아래 항목으로 변경
(중간생략)
    〈Directory "/etc/httpd/htdocs/manual"〉
            Options FollowSymlinks MultiViews
            AllowOverride None
            Order allow,deny
            Allow from all
       〈/Directory〉
(중간생략)
```

• IIS Web 서버의 디렉토리 리스팅 기능 비활성화 적용

〈그림 4-11〉 IIS 서버 디렉토리 인덱싱 방지



• 관리자 페이지 인증 시, 계정 / 패스워드 방식으로 로그인 할 수 있도록 인증 모듈로 구성하고, 특정 관리자 페이지는 공인인증서 방식을 사용하여 인증을 수행해야 한다.

• 스크립트 별 안전한 프로그램 예
  - 인증 과정을 처리하는 부분에 Client Side Script을 사용하면 사용자가 임의로 수정할 수 있으므로 Server Side Script(PHP, ASP, JSP 등)를 통하여 인증 필터링 수행
  - ASP의 안전한 프로그래밍 예

```
<%
If myfunc_userauth(userid, userpw) <> 1 Then 'DB에서 사용자 인증을 처리
Response.write "인증 실패"
Else
If Request.ServerVariables("REMOTE_ADDR") <> "10.10.1.1" Then' 관리자 IP 확인
Response.write "관리자 IP가 아닙니다."
Response.write "인증실패"
LogSave(userid, user_ip, 0)'접속에 실패한 ID 및 IP 기록
Else
Session("logged_in") = 1'인증에 성공했을경우 logged_in 에 1의 값을 셋팅
Session("userid") = userid
Session("user_ip") = Request.ServerVariables("REMOTE_ADDR")

LogSave($userid, $user_ip)'접속에 사용한 ID 및 IP 기록

... 중략 ...
End If
End If
%>
```

– PHP의 안전한 프로그래밍 예

```
<?PHP
@session_start(); //세션 데이터를 초기화
if(!myfunc_userauth($userid, $userpw) || $_SERVER["REMOTE_ADDR"] != "10.10.1.1")
//DB 에서 사용자 인증을 처리, 관리자 IP인지 확인
print "인증 실패";
LogSave(userid, user_ip, 0)'접속에 실패한 ID 및 IP 기록
exit;//인증 실패시 종료

//인증에 성공한 경우 처리 해야 되는 부분
if (!session_is_registered("logged_in"))

$logged_in = 1;//인증에 성공했을경우 logged_in 에 1의 값을 셋팅
$user_ip = $_SERVER["REMOTE_ADDR"];
session_register("logged_in");//인증 결과 저장
session_register("userid");//사용자 ID를 저장
session_register("user_ip");//사용자 IP를 저장

LogSave($userid, $user_ip);// 접속한 사용자 ID 및 IP 기록
... 중략 ...
```

– JSP의 안전한 프로그래밍 예

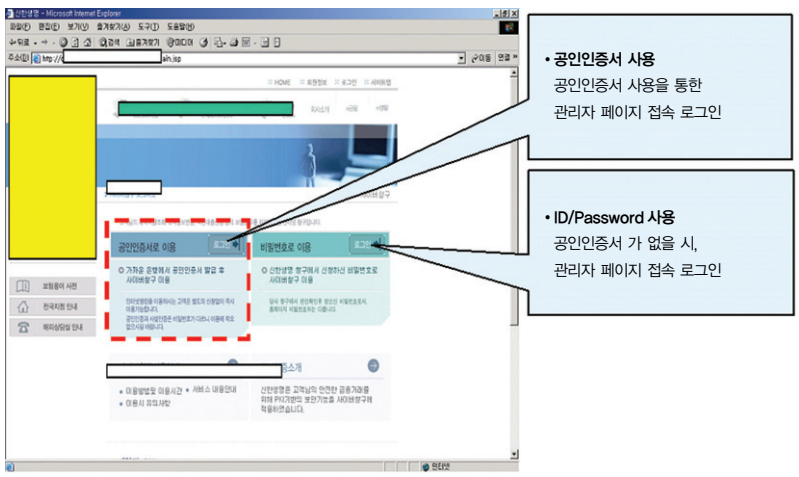
```
<%@ page contentType="text/html;charset=euc-kr" %>
<%@ page import="java.util.* " %>
<%@ page import="java.sql.* " %>
<%
//HttpSession session = request.getSession(true);
String user_ip = request.getRemoteAddr();

// form 에서 사용자 id와 사용자 password를 아래 변수로 전달
if(!myfunc_userauth(userid, userpw) || !user_ip.equals("10.10.1.1"))
//DB 에서 사용자 인증을 처리, 관리자 IP인지 확인
out.println "인증 실패";
LogSave(userid, user_ip, 0)'접속에 실패한 ID 및 IP 기록
else
//인증에 성공한 경우 처리 해야 되는 부분
session.putValue("logged_in","logok");
session.putValue("userid",userid);
session.putValue("user_ip", user_ip);

LogSave(userid, user_ip);// 접속한 사용자 ID 및 IP기록
...
```

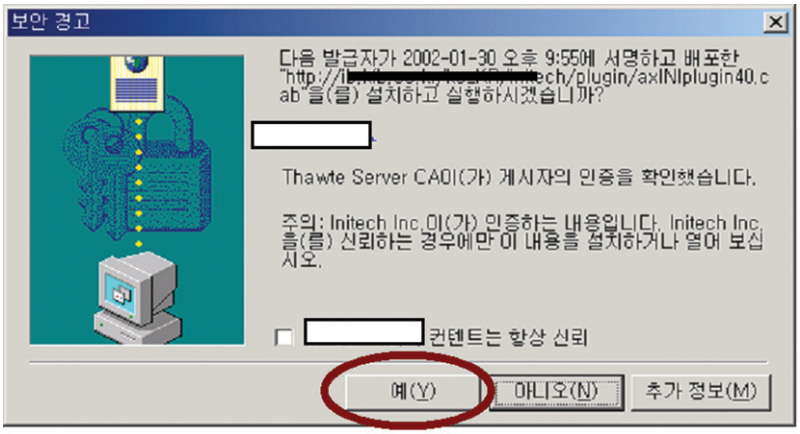
- 공인인증서를 이용한 관리자 페이지 접속
  - 공인인증서를 통한 관리자 페이지 인증 강화

〈그림 4-12〉 관리자 페이지 공인인증서 로그인



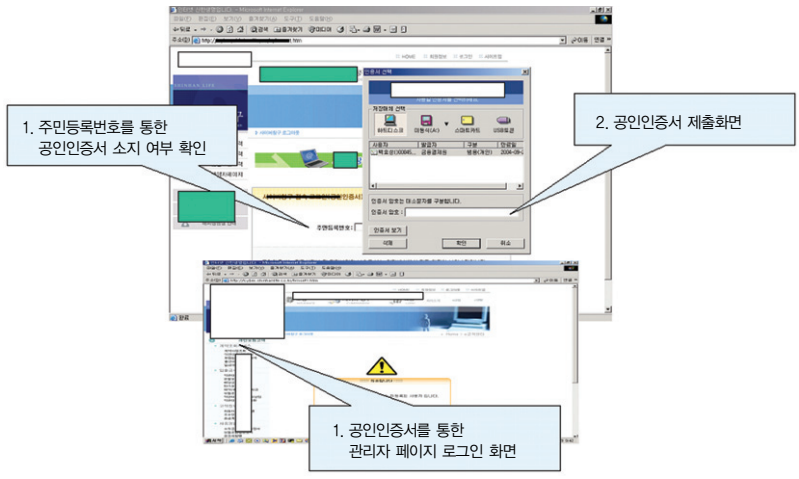
– 공인인증서 및 암호화 프로그램 설치 화면

〈그림 4-13〉 공인인증서 및 암호화프로그램 설치 화면



– 공인인증서를 통한 로그인

〈그림 4-14〉 공인인증서를 통한 로그인



2. 인터넷상 개인식별번호(*i*-PIN)를 사용해 보자!

■ 정보보호 현안 및 예상 피해

• 개인정보 보호 인식 수준 최하위
  – 국내 신용카드 가맹점들의 고객정보 보안 인식이 아시아 · 태평양 지역 국가 중 가장 낮은 수준인 것으로 나타났다.
  – 아 · 태 지역 11개 국가의 가맹점 및 결제대행업체 인지도 조사 결과 조사 대상자 중 78%가 리스크 관리에서 고객정보 보호를 가장 중요한 사안이라고 응답했다.

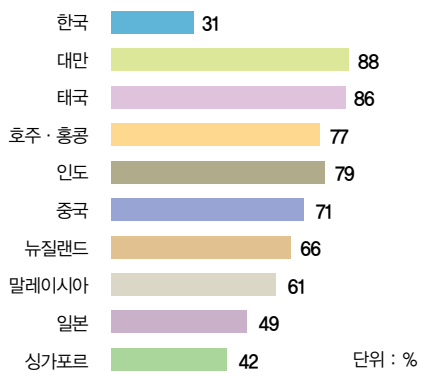
〈그림 4-15〉 개인정보 보호 인식 수준

보도자료 (2006. 7. 5. 디지털 타임즈)

국내 신용카드 가맹점들의 고객정보 보안 인식이 아시아 · 태평양 지역 국가 중 가장 낮은 수준

비자카드는 4일 리서치 전문 기관인 해리스 인터렉티브에 의뢰한 아 · 태 지역 11개 국가의 279개 가맹점 및 49개 결제 대행업체 인지도 조사 결과 국가별로는 한국이 31%로 11개 국가중 가장 낮아 고객 정보 보안 인식이 아직 걸음마 수준인 것으로 조사 됐음. 반면 대만이 88%로 가장 높았으며 태국(86%), 호주 · 홍콩(77%), 인도(79%)도 고객정보 보호 인식이 높은 수준인 것으로 조사됐음.
비자카드는 이에 대해 국내 가맹점들의 자체적인 정보 보호 체계 관리 및 인식이 부족해 고객 정보 보호에 대한 인지도가 낮은 수준이라고 분석했음.(이하 생략)

아 · 태 11개국 고객정보 보호 인지도



• 공공기관 홈페이지 114개 중 41개 주민번호 노출
  – 공공기관 114곳과 대학 35곳, 민간기업 150곳 등 299곳 홈페이지 조사

결과 주민번호 1만7626건을 아무런 보호 조치없이 노출하고 있는 것으로 확인되었다.

- 공공기관 114곳 가운데 36%인 41개 홈페이지에서 1만 1035건, 대학 35곳 중에서는 17개(49%)의 홈페이지에서 1417건, 민간기업 150곳 가운데 26개(17%)의 홈페이지에서 5174건의 주민등록번호가 검색 되었다.

〈그림 4-16〉 주민번호 유출 실태

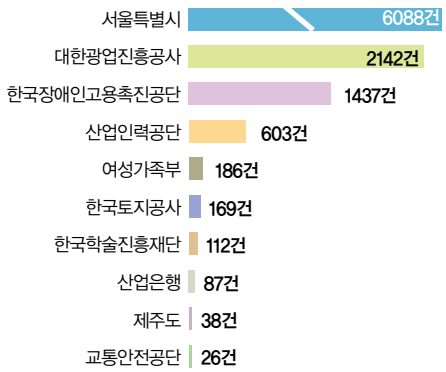
보도자료 (2006. 4. 6. 동아일보)

당신의 신상저보가 이렇게 새고 있습니다.

인터넷 홈페이지 품질진단업체의 도움을 받아 2월1일부터 3월17일까지 공공기관 114곳과 대학 35곳, 민간기업 150곳 등 299곳 홈페이지 조사 결과 주민번호 1만7626건을 아무런 보호 조치없이 노출하고 있는 것으로 확인됐다.

이들기관의 홈페이지는 입력한 주민등록번호 장기간 방치, 시스템 설계 미비로 인한 보안허술, 관리자 화면으로 검색 로봇 진입허용, 검색 로봇에 대한 방어 장치 미흡 등의 문제가 있우ㅆ다. 실제 주민등록번호를 대규모로 노출한 홈페이지는 게시판 등에 사용자가 입력한 개인정보를 방치하고 있었다.(이하 생략)

공공기관 홈페이지 주민번호 노출 상위 10위

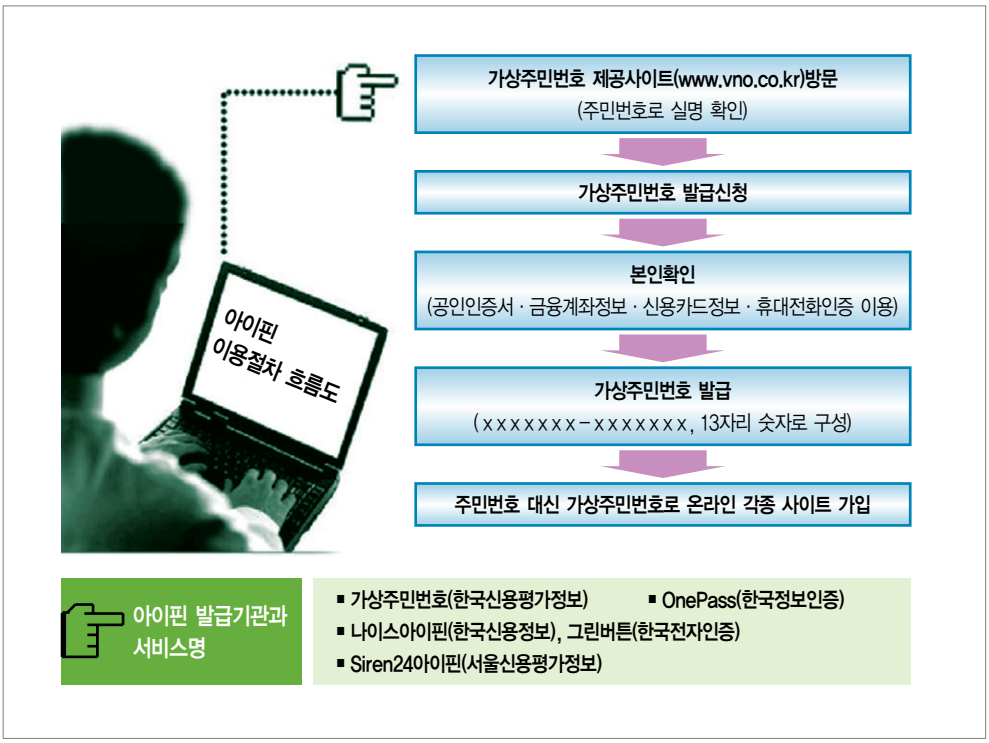


■ 보호 대책

- '아이핀' 서비스를 이용
  - 개인정보 침해 또는 명의도용 등 주민번호의 오/남용 문제를 해결하기 위한 방안으로 주민번호를 대신해서 사용할 수 있는 것이 아이핀(*i*-PIN : Internet Personal Identification Number) 서비스이다.
  - 정보통신부는 온라인 사이트 회원 가입을 받을 때 주민번호와 이름을 입력하는 대신 본인확인 기관이 제공하는 개인 식별 코드를 이용하도록 하는 아이핀 제도를 도입하였다.(2006년 10월)

– 아이핀은 5개 공인기관이 본인 확인을 거쳐 발급하는 개인식별 코드로, 13자리 이상의 숫자나 영문자로 구성되며, 주민번호와 달리 생년월일, 출생지, 성별 등의 개인정보를 포함하지 않는다.

〈그림 4-17〉 아이핀 이용절차 및 종류



– 본인확인 기관들은 개인이 아이핀 발급을 신청하면 공인인증서(용도 제한용도 가능), 신용카드 정보, 금융계좌 정보, 휴대전화 인증, 대면 확인 등을 거쳐 개인식별 번호를 발급한다.

• 아이핀 서비스 신청과 이용(사례 : 한국전자인증 그린버튼서비스)

– 인터넷사이트 회원가입을 신청 ⇒ 주민번호 입력 대신 그린버튼서비스 신청

– 그린버튼서비스를 선택한 고객에 대해 본인확인을 요청

– 이용자는 본인확인시스템을통해 신원정보를 입력

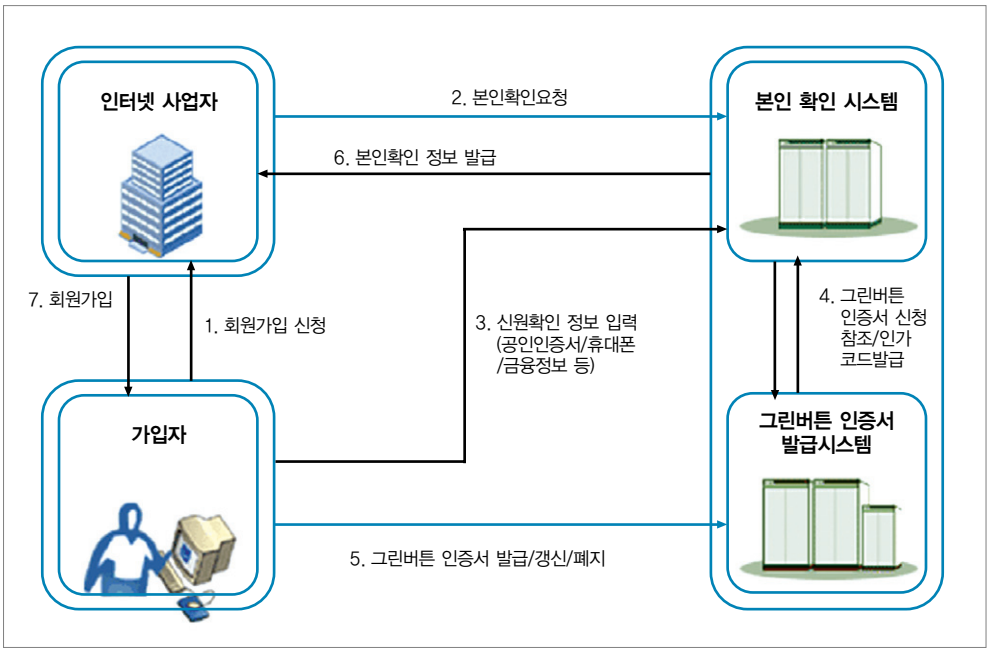
– 공인인증기관에 그린버튼 인증서를 발급

– 그린버튼 인증서는 이용자가 발급/ 갱신/폐지 모두 가능

– 인터넷사업자가 인증서를 통해 이용자 정보 확인

– 주민번호를 입력하지 않고 회원가입 완료

〈그림 4-18〉 그린버튼 서비스 신청과 이용 절차



• 서비스 이용 절차

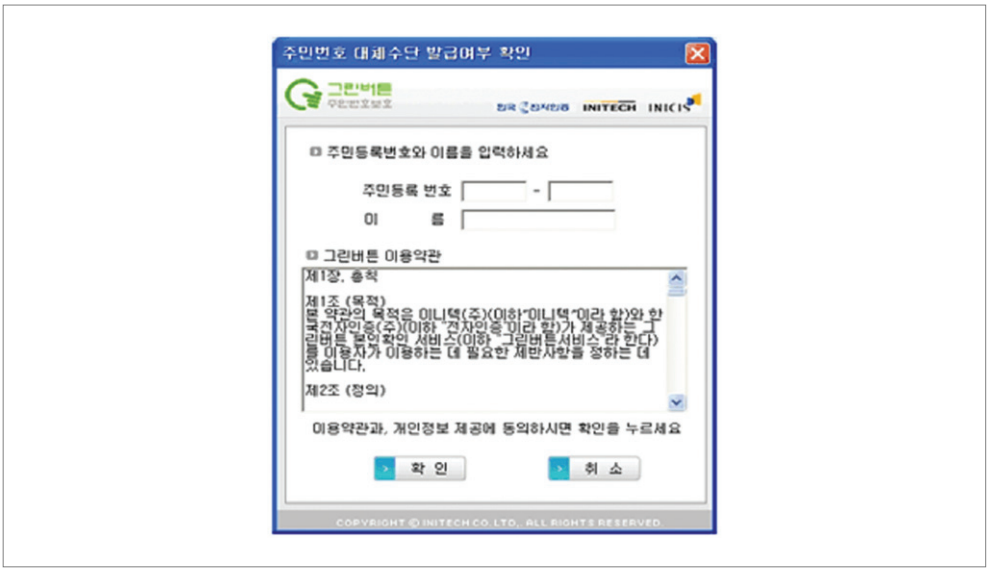
– 서비스 제공기관의 홈페이지에서 회원가입 및 아이디, 비밀번호 분실

페이지에서 그린버튼 선택

〈그림 4-19〉 그린버튼 서비스 신청 버튼

- 대체수단으로 보호할 주민번호와 이름 입력 및 약관동의

〈그림 4-20〉 약관동의 메뉴

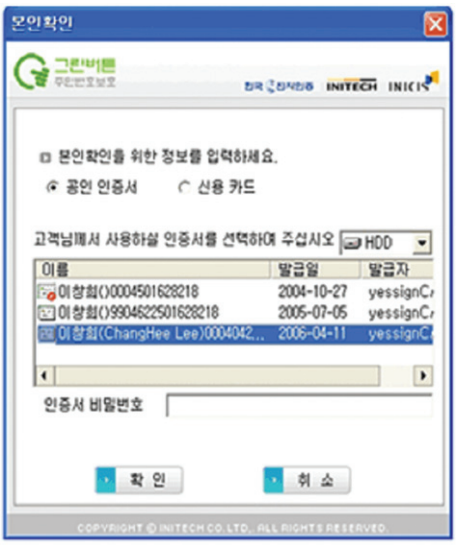


- 정보입력(이메일 주소와 패스워드가 대체수단으로 사용됨)

〈그림 4-21〉 아이핀 설정

– 공인인증서 또는 신용카드로 신원확인 하면 발급완료

〈그림 4-22〉 아이핀 발급완료



3. 보안서버로 개인정보 유출 방지하자

■ 정보보호 현안 및 예상 피해

• 스니핑(sniffing)에 따른 개인정보 유출

– 학교, PC방, 회사 등의 공용 네트워크를 사용하는 PC에서 보안서버가 구축되지 않은 사이트로 접속할 경우, 스니핑 툴(sniffing tool)을 사용하여 다른 사람의 개인정보(ID/패스워드/이메일/주민번호/주소/전화번호 등)를 손쉽게 얻을 수 있다.

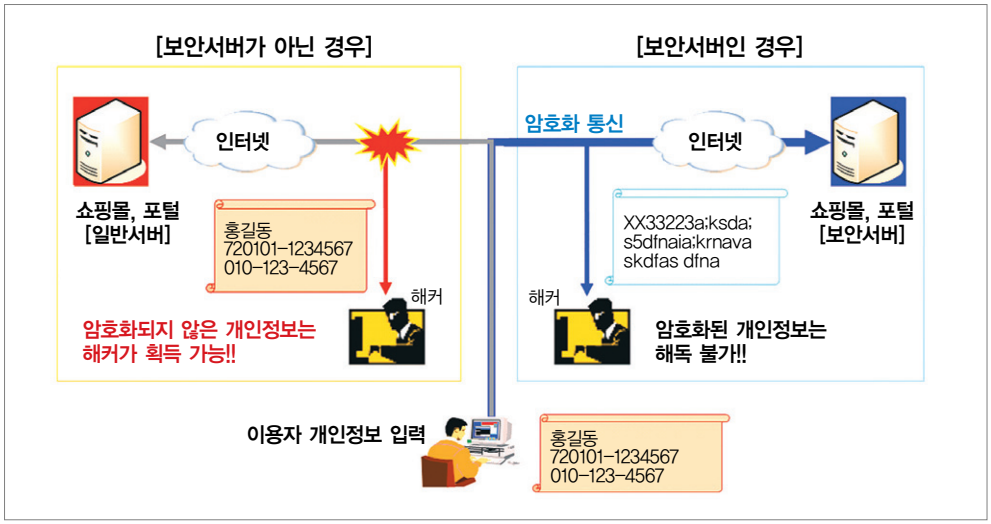
• 피싱(phising)에 따른 개인정보 유출

– 보안서버가 구축되지 않으면 정상사이트를 위조한 피싱사이트를 통해 계좌번호, 비밀번호 등 개인정보가 유출되어 고객의 신뢰가 저하될 수 있다.

• 암호화 미비에 따른 개인정보 유출

– 인터넷상의 암호화되지 않은 개인정보는 가로채기 등의 해킹을 통해 해커에게 쉽게 유출될 수 있는 반면 암호화된 개인정보는 해킹을 당해도 보호받을 수 있다.

〈그림 4-23〉 암호화 미비에 따른 개인정보 유출



■ 보호대책

• 보안서버란?

– 인터넷상에서 사용자 PC와 웹 서버 사이에 송수신되는 개인정보를 암호화하여 전송하는 서버이다. 보안서버는 정보통신서비스 제공업체의 실존을 증명하여 고객과 기업간 신뢰를 형성하고, 브라우저와 서버간 전송되는 데이터의 암복호화를 통하여 개인정보의 보호를 위한 보안 채널을 형성한다.

• 보안서버의 종류

– 보안서버는 구축 방식에 따라 크게 「SSL 방식」과 「응용프로그램 방식」 2가지로 구분할 수 있다.

– SSL 방식 보안서버는 「SSL 인증서」를 이용하여 사용자 컴퓨터에 별도 보안 프로그램 설치가 필요 없다. 로그인 페이지 등 보안이 필요한 웹페이지에서 자물쇠 모양의 마크로 확인할 수 있다.

〈그림 4-24〉 SSL 방식의 보안서버 실행 확인

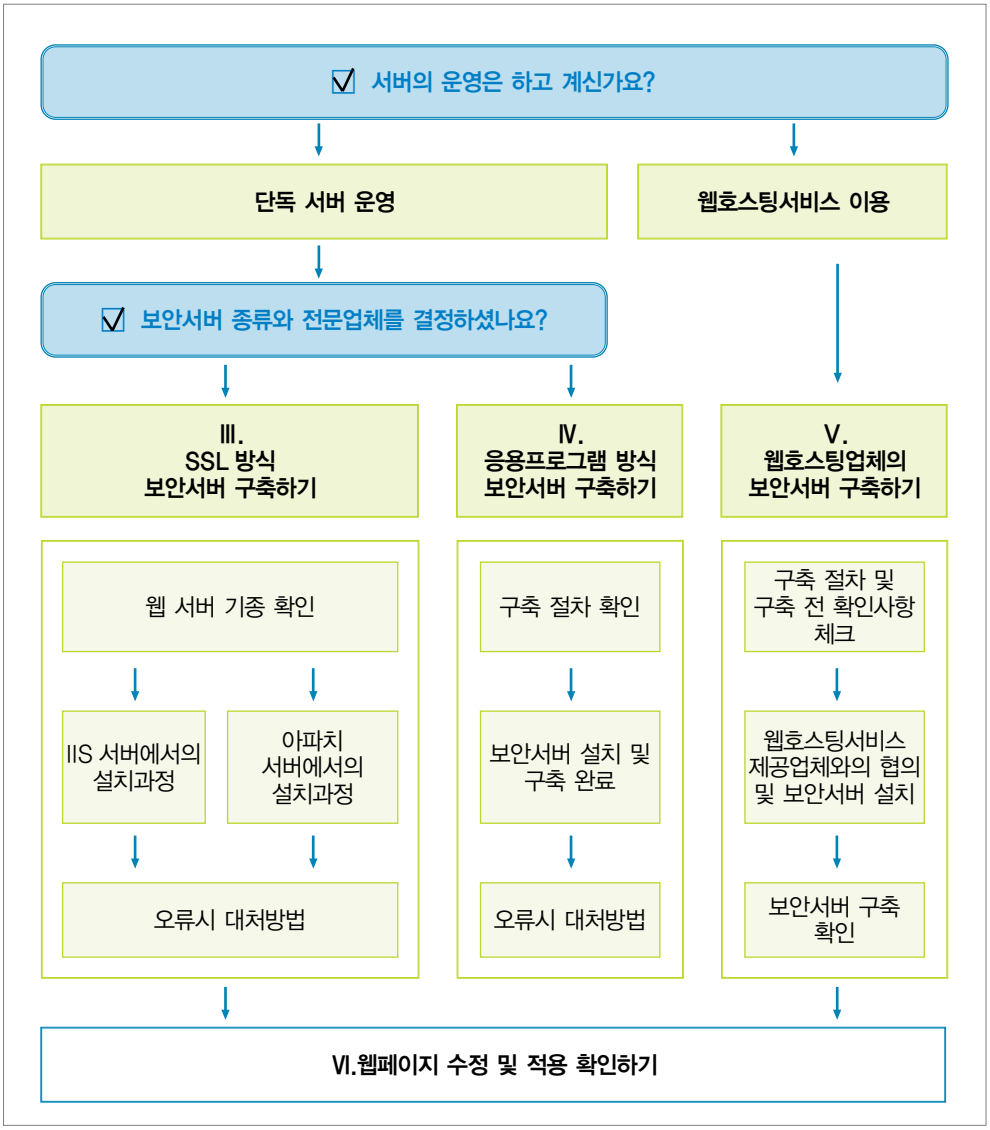
- 응용프로그램 방식 보안서버는 사용자가 웹 서버에 접속하면 사용자 컴퓨터에 자동으로 보안 프로그램이 설치되어 로그인 후 윈도우 작업 표시줄에 암호화 프로그램 실행여부를 확인할 수 있다.

〈그림 4-25〉 응용프로그램 방식의 보안서버 실행 확인

• 보안서버 구축 절차

– 보안서버 구축을 위해서는 먼저 서버 운영 형태, 보안서버 종류 등을 각 기업의 현황에 따라 설정한 후 필요한 절차를 따르면 된다.

〈그림 4-26〉 보안서버 구축 절차 흐름도



보안서버 구축 절차는 「보안서버 구축 핸드북」을 참조하고(www.kisa.or.kr), 아래 「보안서버전문협의회」회원사나 기타 보안서버 구축 전문업체를 통하여 자세한 설명을 받을 수 있다.

회사명	홈페이지	연락처
SSL 방식 솔루션 공급 업체		
한국전자인증(주)	www.crosscert.com	1588-1314
한국정보인증(주)	www.kica.net	(02) 360-3065
이모션	www.trust1.co.kr	(02) 542-1987
(주)한국무역정보통신	www.tradesign.co.kr	(02) 6000-2162
(주) 한비로	comodossl.co.kr	1544-4755
(주)닷네임코리아	www.anycert.co.kr	080-456-7770
나인포유	www.certkorea.co.kr	(02) 3444-2750
(주)아이네임즈	cert.inames.co.kr	(02) 559-1006
응용 프로그램 방식 솔루션 공급 업체		
한국전자인증(주)	www.crosscert.com	1588-1314
이니텍(주)	www.initech.com	(02) 2140-3553
한국정보인증(주)	www.signgate.com	(02) 360-3065
(주)케이사인	www.ksign.com	(02) 564-0182
드림시큐리티	www.dreamsecurity.com	(02) 2233-5533
시큐리티 테크놀로지(STI)	www.stitec.com	(02) 558-7391
펜타시큐리티시스템(주)	www.pentasecurity.com	(02) 780-7728
소프트포럼	www.softforum.co.kr	(02) 526-8423
(주)코스콤	www.signkorea.co.kr	(02) 767-7224
엠큐릭스(주)	www.mcurix.com	(02) 2253-8882
유넷시스템(주)	www.unetsystem.co.kr	(02) 390-8000

• 보안서버 관련 규정

– 개인정보의 보호조치는 법 규정을 통하여 의무화되어 있는 사항으로 개인정보를 취급하는 정보통신서비스제공자는 보안서버를 통하여 이용자의 개인정보를 암호화해야 한다.

1. 정보통신망 이용촉진 및 정보보호 등에 관한 법률

▶ 제28조(개인정보의 보호조치) 정보통신서비스제공자등은 이용자의 개인정보를 취급함에 있어서 개인정보가 분실 · 도난 · 누출 · 변조 또는 훼손되지 아니하도록 정보통신부령이 정하는 바에 따라 안전성 확보에 필요한 기술적 · 관리적 조치를 하여야 한다. 〈개정 2004.1.29〉

▶ 제67조 (과태료) ②다음 각 호의 어느 하나에 해당하는 자는 1천만원 이하의 과태료에 처한다. 〈개정 2004.1.29〉
8의2. 제28조의 규정을 위반하여 기술적 · 관리적 조치를 하지 아니한 자

2. 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행규칙

▶ 제3조의2(개인정보의 보호조치) ①법 제28조의 규정에 의한 개인정보의 안전성 확보에 필요한 기술적 · 관리적 조치는 다음 각호와 같다.(중간 생략)
4. 개인정보를 안전하게 저장 · 전송할 수 있는 암호화기술 등을 이용한 보안조치(이하생략)

3. 개인정보의 기술적 · 관리적 보호조치 기준

▶ 5조(개인정보의 암호화) ②정보통신서비스제공자등은 정보통신망을 통해 이용자의 개인정보 및 인증정보를 송 · 수신할 때에는 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다. 보안서버는 다음 각호의 어느 하나의 기능을 갖추어야 한다. 〈개정 2007.1.29〉
1. 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하여 개인정보를 암호화하여 송 · 수신하는 기능
2. 웹서버에 암호화 응용프로그램을 설치하여 개인정보를 암호화하여 송 · 수신하는 기능
③정보통신서비스제공자등은 이용자의 개인정보를 PC에 저장할 때에는 이를 암호화해야 한다.

제 5 장 개인정보보호 피해신고 절차 및 대응

V

1. 개인정보 피해신고센터

1.1 개인정보 침해유형

■ 개인정보의 구체적인 예

• "개인정보"란 개인의 신체, 재산, 사회적 지위, 신분 등에 관한 사실, 판단, 평가 등을 나타내는 일체의 모든 정보를 말한다.
  – 신분관계 : 성명, 주민등록번호, 주소, 본적, 가족관계, 본관 등
  – 내면의 비밀 : 사상, 신조, 종교, 가치관, 정치적 성향 등
  – 심신의 상태 : 건강상태, 신체적 특징, 병력, 장애정도 등
  – 사회경력 : 학력, 직업, 자격, 전과 여부 등
  – 경제관계 : 소득규모, 재산보유상황, 신용정보, 채권채무관계 등
  – 기타 새로운 유형 : 바이오인식정보(지문, 홍채, DNA 등), 위치정보 등

• 우리나라의 민간분야 개인정보보호를 규율하고 있는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제2조에서는
  – 개인정보를 "생존하는 개인에 관한 정보로서 성명, 주민등록번호 등에 의하여 당해 개인을 알아볼 수 있는 부호, 문자, 음성, 음향 및 영상

등의 정보를 말한다" 라고 규정하고 있다.

■ 개인정보 침해 사례

• 본인의 동의 없는 개인정보 수집, 정정 요구 불응
  – 관리자의 허가를 받지 않고 공공기관이나 기업 등의 컴퓨터에 침입하여 개인정보를 수집하거나 변경하는 행위
  – 인터넷에 연결된 개인컴퓨터에 은밀하게 침입하여 개인정보를 수집하는 행위
    • 은행이나 백화점의 데이터베이스에 침입하여 개인의 신용정보를 빼내거나, 개인컴퓨터에 침입하여 사용자의 전자우편주소, 사용하는 소프트웨어 유형, 웹 접근기록, 개인적인 데이터베이스를 수집하는 등의 침해행위
  – 정보주체의 동의가 없는 개인정보 수집
    • 인터넷마케팅 업체들이 쿠키를 사용해서 소비자들이 어느 웹사이트를 접속해 얼마나 머무르고 어떤 거래를 하는지 등 소비자들에게 알리지 않고 인터넷 활동을 모니터링 하는 행위
    • 호텔의 침실에 몰래카메라를 설치하여 투숙객들의 행동을 촬영하여 팔아 넘기고 공장이나 백화점과 같은 일터에 CCTV를 설치하여 근로자들의 행동을 감시하는 행위
  – 개인정보 수집시 고지 또는 명시의무를 이행하지 않는 행위
  – 과도한 개인정보 수집
  – 정보주체의 동의 철회(회원탈퇴), 열람 또는 정정요구에 불응
  – 정보주체의 동의 철회(회원탈퇴), 열람 또는 정정을 수집보다 쉽게 해야 할 조치를 이행하지 않는 행위
  – 개인정보 등 원치않는 정보 수신

• 개인정보의 훼손, 침해, 도용
  – 개인정보를 안전하지 못한 방식으로 보관하여 저장된 정보의 신뢰성을 떨어뜨리고 정보접근에 대한 인증을 수행하지 못하는 행위
    • 데이터베이스 시스템 관리를 잘못하여 개인사용자가 다른 사용자의 정보를 훔쳐볼 수 있게 한 행위, 개인정보취급자에 의한 훼손이나 침해, 그리고 수집 또는 제공받은 목적 달성 후 개인정보를 파기하지 않은 행위
  – 명의 도용으로 인한 금전적 피해를 끼치는 행위
    • 타인 명의로 계좌 개설거래, 유료 통신서비스 개설 및 부당 요금 부과 주민등록번호를 도용하여 사이트에 무단으로 회원 가입하는 행위

• 개인정보의 유출 및 제 3자 제공
  – 고객에게 알리지 않고 고객의 개인정보를 다른 기업들에게 넘겨주는 행위
  – 고지명시한 범위를 넘어선 이용 또는 제3자 제공, 영업의 양수 등의 통지의무 불이행
  – 개인정보취급자에 의한 누설, 기술적 · 관리적 조치미비로 인한 개인정보 누출

1.2 개인정보 침해신고센터 주요업무

■ 개인정보침해신고센터

• 개인정보침해신고센터는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」상의 개인정보 보호규정이 이행되는지 여부를 감시하는 임무를 수행하며, 정보통신부 산하 한국정보보호진흥원 내에 설치되었다.
  – 온라인 또는 전화 등의 방법을 통하여 개인정보와 관련한 일반적 문의

사항, 또는 법령질의, 개인정보침해신고 등 개인정보와 관련된 것이라면 무엇이든지 문의할 수 있다.

- 누구든지 개인정보에 관한 문의사항이 있거나, 개인정보를 침해당한 경우 개인정보침해신고센터에 상담 또는 피해구제를 신청할 수 있다.
- 개인정보보호와 관련된 내용과 자신의 권익내용에 관한 사항을 상담할 수 있다.
- 개인정보보호에 관한 국민 인식제고를 위하여 각종 국내외 자료, 법률 및 연구보고서 등을 무료로 제공한다.
- 사이버포럼, 정보보호감시단 활동지원, 개인정보보호 관련 수기 및 법제도 개선방안 공모 등 다양한 행사를 개최한다.

■ 개인정보분쟁조정위원회

• 개인정보분쟁조정위원회는 2001년 12월 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제33조에 의거하여 설립된 분쟁해결 전문기관이다.
  - 이용자와 사업자 사이의 개인정보분쟁조정
  - 교육과 홍보를 통한 피해예방 활동, 법제도 개선 건의, 기업의 거래행태나 약관의 시정권고, 위법사실 처리 등의 각종 재발방지조치를 통해 국민의 권리 보호를 목적으로 한다.

■ 사업자 지원창구

• 사업자 지원창구는 고객의 개인정보를 수집 · 취급하고 있는 기업에게 개인정보 관련 문의에 도움이 되고자 운영하는 민원 창구이다.
  - 기업이 질의한 개인정보보호 관련 문의에 대해서는 개인정보침해신고센터 소속 전문연구원들의 검토 및 필요시 외부 전문가들의 자문을 거쳐, 원칙적으로 14일 이내에 답변한다.

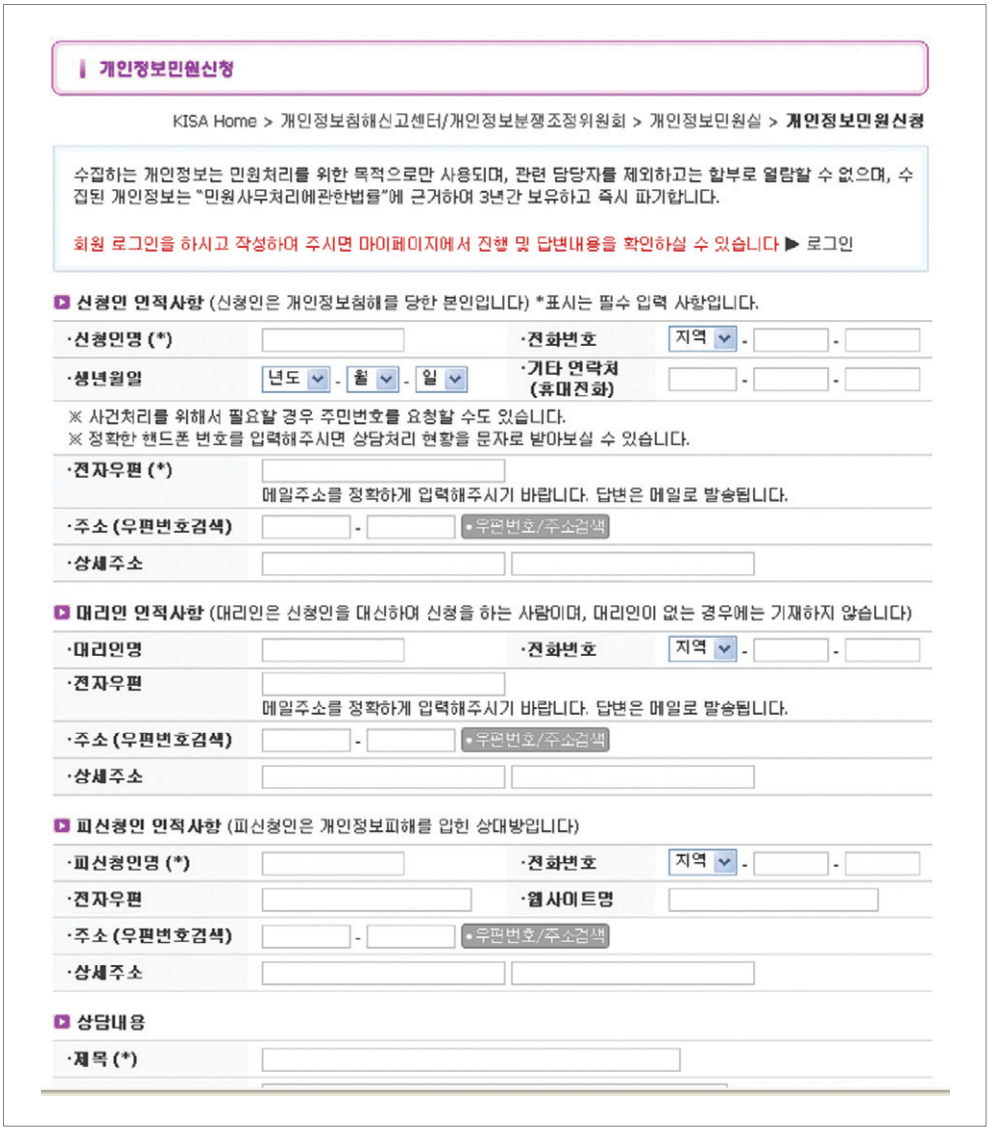
〈그림 5-1〉 기업 개인정보보호 관련 문의 처리 절차

2. 개인정보 민원신청 및 분쟁조정

■ 민원신청 절차

• 개인정보피해로 인한 민원신청은 웹사이트, 우편, 팩스, 방문 등을 통해 신청인이 직접 또는 대리로 신청할 수 있다.
  - 인터넷 접수 : www.1336.or.kr
  - 전자우편 : privacy@kisa.or.kr
  - 전화 : 국번없이 1336(ARS 내선 2번)
  - 팩스 : 02) 405-4729
  - 우편 및 방문 : 서울시 송파구 가락동 78번지 IT벤처타워
  - 팩스, 우편, 방문을 통하여 민원을 접수하시는 경우 별첨된 신청서 양식을 이용

〈그림 5-2〉 인터넷 접수 화면



• 접수된 민원신청 처리절차는 다음과 같다.

– 민원신청이 접수되면 상담원들이 1차적으로 검토하여 내용에 따라, 분류하여 답변

- 간략하게 상담답변으로 종결할 수 있는 내용은 원칙적으로 7일(법령 질의는 14일) 이내에 온라인으로 답변
- 좀더 자세하게 사실조사가 필요하거나 법률검토가 필요한 부분에 대해서는 우선 신청인에게 민원접수사실을 통보
- 민원처리담당자는 양 당사자의 의견청취, 증거수집, 전문가 자문 등 필요한 사실조사를 실시
- 개인정보에 관한 분쟁의 경우 개인정보분쟁조정위원회의 분쟁조정 절차에 의하여 해결되며, 사업자의 위법사실에 대한 법적조치 건의에 대해서는 사실조사 후 관계기관에 위법사실을 통보
- 다만, 법적조치 건의는 정보통신망 이용촉진 및 정보보호 등에 관한 법률의 적용을 받는 「정보통신서비스제공자」에 한함
- 피해구제신청으로 접수된 경우 원칙적으로 60일 이내에 사건처리종료
- 다만, 사실조사에 시간이 많이 소요되는 등 부득이한 사정이 있는 경우에는 그 기간을 연장

■ 분쟁조정 절차

• 개인정보피해로 인한 분쟁조정은 웹사이트, 우편, 팩스, 방문 등을 통해 신청인이 직접 또는 대리로 신청할 수 있다.
- 개인정보침해 관련 상담 또는 신고사건 처리과정에서 신청 가능
- 분쟁조정 신청사건이 접수되면, 신청자와 상대방에게 접수사실 통보

• 접수된 분쟁조정 신청사건의 처리절차는 다음과 같다.
① 사실확인 및 당사자 의견청취
- 사건담당자는 전화, 우편, 전자우편, 팩스 등 다양한 수단을 이용해 자료 수집을 통한 분쟁조정 사건에 대한 사실조사를 실시
- 사실조사가 완료되면 이를 토대로 사실조사보고서를 작성하여 본

사건을 위원회에 회부

② 조정전 합의를 권고

- 개인정보분쟁조정위원회는 조정에 들어가기 앞서 당사자간의 자율적인 노력에 의해 원만히 분쟁이 해결될 수 있도록 합의를 권고
- 합의권고에 의해 당사자간 합의가 성립하면 사건이 종결

③ 위원회의 조정절차 개시

- 조정 전 합의가 이루어지지 않으면 위원회를 통해 조정절차 개시
- 조정절차가 진행되면 당사자의 의견청취, 증거수집, 전문가의 자문 등 필요한 절차를 거쳐 쌍방에게 합당한 조정안을 제시하고 이를 받아들일 것을 권고
- 이 경우 사건의 신청자나 상대방은 위원회의 회의에 참석하여 자신의 의견을 개진할 수 있음
- 조정절차가 진행되는 중에 원만한 합의가 이루어지는 등의 사유로 인해 더 이상 조정을 원하지 않을 경우 신청인은 조정신청을 철회할 수 있음

④ 조정의 성립

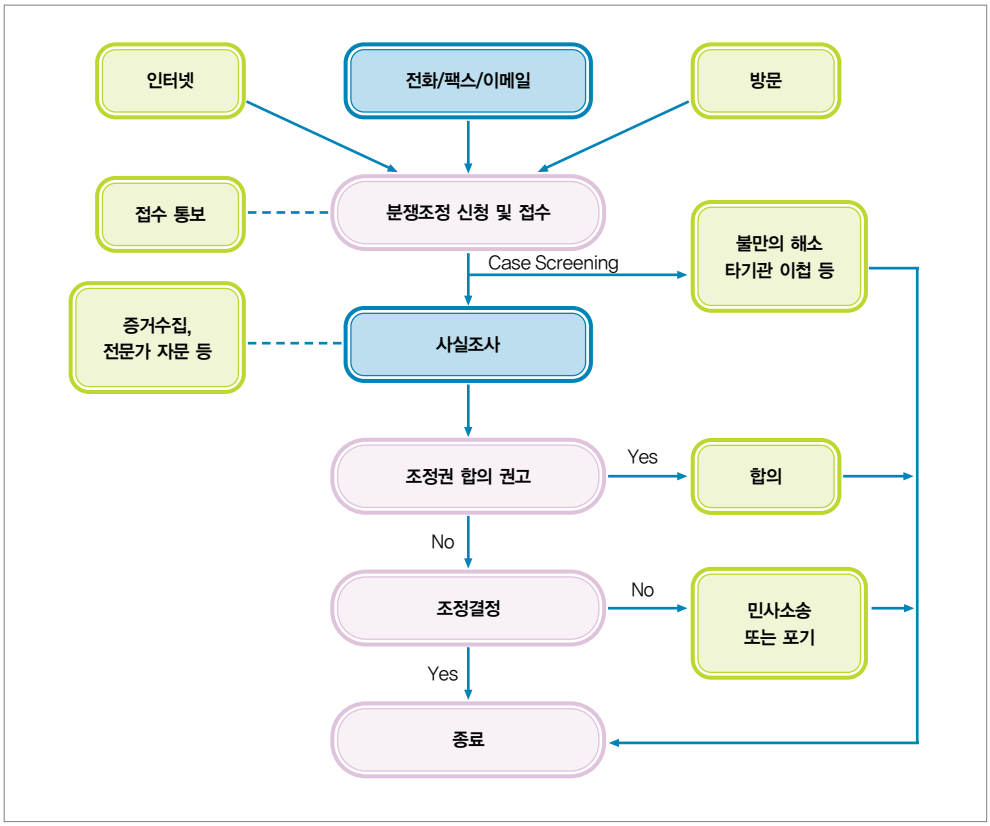
- 개인정보분쟁조정위원회의 조정을 통하여 내려진 결정에 대하여 조정결정일부터 15일 이내에 신청인과 상대방이 이를 수락한 경우에는 조정이 성립
- 당사자가 위원회의 조정안을 수락하고자 하는 경우 위원회가 송부한 조정서에 기명날인하여 위원회에 제출
- 양 당사자가 모두 조정안을 수락하면 조정이 성립되어 조정서가 작성되고 조정절차가 종료
- 당사자중 일방이 조정안을 수락하지 않을 경우 민사소송을 제기하거나

포기할 수 있음

⑤ 효력발생

– 개인정보분쟁조정위원회의 조정 결정에 대해 신청인과 상대방이 이를 수락하여 조정이 성립된 경우 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제38조제4항의 규정에 따라 양 당사자간에는 조정서와 동일한 내용의 합의(민사상의 화해계약)가 성립한 것으로 간주함

〈그림 5-3〉 분쟁조정위원회 조정 절차



부록 A 개인정보침해 관련 법률 및 규정

A-a. 정보통신망이용촉진및정보보호등에관한법률

[일부개정 2007.1.26 법률 제8289호]

제4장 개인정보의 보호

제1절 개인정보의 수집 이용 및 제공 등

제22조 (개인정보의 수집·이용 동의 등) ① 정보통신서비스제공자는 이용자의 개인정보를 이용하려고 수집하는 때에는 다음 각 호의 모든 사항에 대하여 이용자에게 알리고 동의를 얻어야 한다. 다음 각 호의 어느 하나의 사항을 변경하려는 때에도 또한 같다.

1. 개인정보의 수집 · 이용 목적
2. 수집하는 개인정보의 항목
3. 개인정보의 보유 및 이용 기간

② 정보통신서비스제공자는 다음 각 호의 어느 하나에 해당하는 경우에는 제1항의 규정에 따른 동의 없이 이용자의 개인정보를 수집 · 이용할 수 있다.

1. 정보통신서비스의 제공에 관한 계약의 이행을 위하여 필요한 개인정보로서 경제적 · 기술적인 사유로 통상의 동의를 받는 것이 현저히 곤란한 경우

2. 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우
3. 이 법 또는 다른 법률에 특별한 규정이 있는 경우

[전문개정 2007.1.26]

제23조 (개인정보의 수집의 제한 등) ① 정보통신서비스제공자는 사상·신념·과거의 병력 등 개인의 권리·이익이나 사생활을 현저하게 침해할 우려가 있는 개인정보를 수집하여서는 아니된다. 다만, 제22조제1항의 규정에 따른 이용자의 동의를 얻거나 다른 법률에 따라 특별히 수집대상 개인정보로 허용된 경우에는 그러하지 아니하다. 〈개정 2007.1.26〉

② 정보통신서비스제공자는 이용자의 개인정보를 수집하는 경우 정보통신서비스의 제공을 위하여 필요한 최소한의 정보를 수집하여야 하며, 필요한 최소한의 정보외의 개인정보를 제공하지 아니한다는 이유로 그 서비스의 제공을 거부하여서는 아니된다. 〈개정 2007.1.26〉

제2절 삭제 〈2007.1.26〉

제24조 (개인정보의 이용 제한) 정보통신서비스제공자는 제22조 및 제23조 제1항 단서의 규정에 따라 수집한 개인정보를 이용자로부터 동의받은 목적 또는 제22조제2항 각 호에서 정한 목적과 다른 목적으로 이용하여서는 아니 된다.

[전문개정 2007.1.26]

제24조의2 (개인정보의 제공 동의 등) ① 정보통신서비스제공자는 이용자의 개인정보를 제3자에게 제공하려는 경우 제22조제2항제2호 및 제3호의 규정에 해당하는 경우를 제외하고는 다음 각 호의 모든 사항에 대하여 이용자에게 알리고 동의를 얻어야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다.

1. 개인정보를 제공받는 자
2. 개인정보를 제공받는 자의 개인정보 이용 목적
3. 제공하는 개인정보의 항목
4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간

② 제1항의 규정에 따라 정보통신서비스제공자로부터 이용자의 개인정보를 제공받은 자는 그 이용자의 동의가 있거나 다른 법률에 특별한 규정이 있는 경우를 제외하고는 개인정보를 제3자에게 제공하거나 제공받은 목적 외의 용도로 이용하여서는 아니 된다.

[본조신설 2007.1.26]

제25조 (개인정보의 취급위탁〈개정 2007.1.26〉) ① 정보통신서비스제공자와 그로부터 제24조의2제1항의 규정에 따라 이용자의 개인정보를 제공받은 자(이하 "정보통신서비스제공자등"이라 한다)는 제3자에게 이용자의 개인정보를 수집 · 보관 · 처리 · 이용 · 제공 · 관리 · 파기 등(이하 "취급"이라 한다)을 할 수 있도록 업무를 위탁(이하 "개인정보취급위탁"이라 한다)하는 경우에는 다음 각 호의 사항 모두에 대하여 이용자에게 알리고 동의를 얻어야 한다. 다음 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다. 〈개정 2007.1.26〉

1. 개인정보취급위탁을 받는 자(이하 "수탁자"라 한다)
2. 개인정보취급위탁을 하는 업무의 내용

② 정보통신서비스제공자등은 정보통신서비스의 제공에 관한 계약의 이행을 위하여 필요한 경우로서 제1항 각 호의 사항 모두를 제27조의2제1항의 규정에 따라 공개하거나 전자우편 등 대통령령이 정하는 방법에 따라 이용자에게 통지한 경우에는 개인정보취급위탁에 따른 제1항의 고지 및 동의절차를 거치지 아니할 수 있다. 제1항 각 호의 어느 하나의 사항이 변경되는 경우에도 또한 같다. 〈신설 2007.1.26〉

③ 정보통신서비스제공자등은 개인정보취급위탁을 하는 경우에는 수탁자가 이용자의 개인정보를 취급할 수 있는 목적을 미리 정하여야 하며, 수탁자는

이 목적을 벗어나서 이용자의 개인정보를 취급하여서는 아니 된다.
〈신설 2007.1.26〉
④ 정보통신서비스제공자등은 수탁자에 대하여 이 장의 규정을 위반하지 아니하도록 관리 · 감독하여야 한다. 〈신설 2004.1.29, 2007.1.26〉
⑤ 수탁자가 개인정보취급위탁을 받은 업무와 관련하여 이 장의 규정을 위반하여 이용자에게 손해를 발생시킨 경우에는 그 수탁자를 손해배상책임에 있어서 정보통신서비스제공자등의 소속직원으로 본다.
〈개정 2004.1.29, 2007.1.26〉

제26조 (영업의 양수 등에 따른 개인정보의 이전 〈개정 2007.1.26〉) ① 정보통신서비스제공자등이 영업의 전부 또는 일부의 양도 · 합병 등으로 그 이용자의 개인정보를 타인에게 이전하는 경우에는 미리 다음 각 호의 사항 모두를 인터넷 홈페이지 게시, 전자우편 등 대통령령이 정하는 방법에 따라 이용자에게 통지하여야 한다. 〈개정 2007.1.26〉

1. 개인정보를 이전하려는 사실
2. 개인정보의 이전을 받는 자(이하 "영업양수자등"이라 한다)의 성명(법인의 경우에는 법인의 명칭을 말한다. 이하 이 조에서 같다) · 주소 · 전화번호 그 밖의 연락처
3. 이용자가 개인정보의 이전을 원하지 아니하는 경우 그 동의를 철회할 수 있는 방법 및 절차

② 영업양수자등은 개인정보의 이전을 받은 경우에는 지체 없이 그 사실을 인터넷 홈페이지 게시, 전자우편 등 대통령령이 정하는 방법에 따라 이용자에게 통지하여야 한다. 다만, 정보통신서비스제공자등이 제1항의 규정에 따라 그 이전사실을 이미 통지한 경우에는 그러하지 아니하다.
〈개정 2007.1.26〉
③ 영업양수자등은 정보통신서비스제공자등이 이용자의 개인정보를 이용하거나 제공할 수 있는 당초의 목적 범위 안에서만 개인정보를

이용하거나 제공할 수 있다. 다만, 이용자의 별도의 동의를 얻은 경우에는 그러하지 아니하다. 〈신설 2007.1.26〉

제26조의2 (동의획득방법) 제22조제1항 · 제23조제1항 단서 · 제24조의2 제1항 및 제2항 · 제25조제1항 · 제26조제3항 단서 또는 제54조제2항의 규정에 따른 동의(이하 "개인정보수집 · 이용 · 제공 등의 동의"라 한다)를 얻는 방법은 개인정보의 수집매체, 업종의 특성 및 이용자의 수 등을 참작하여 대통령령으로 정한다.
[본조신설 2007.1.26]

제2절 개인정보의 관리 및 파기 등 〈신설 2007.1.26〉

제27조 (개인정보관리책임자의 지정) ① 정보통신서비스제공자등은 이용자의 개인정보를 보호하고 개인정보와 관련한 이용자의 고충을 처리하기 위하여 개인정보관리책임자를 지정하여야 한다. 다만, 종업원 수 · 이용자 수 등이 정보통신부령이 정하는 기준에 해당하는 정보통신서비스제공자등의 경우에는 지정하지 아니할 수 있다. 〈개정 2004.1.29, 2006.10.4〉
② 제1항 단서의 규정에 따른 정보통신서비스제공자등이 개인정보관리책임자를 지정하지 아니하는 경우에는 그 사업주 또는 대표자가 개인정보관리책임자가 된다. 〈신설 2006.10.4〉
③ 개인정보관리책임자의 자격요건 그 밖의 지정에 관하여 필요한 사항은 정보통신부령으로 정한다. 〈개정 2006.10.4〉

제27조의2 (개인정보취급방침의 공개) ① 정보통신서비스제공자등은 이용자의 개인정보를 취급하는 경우에는 개인정보취급방침을 정하여 이를 이용자가 언제든지 쉽게 확인할 수 있도록 정보통신부령이 정하는 방법에 따라 공개하여야 한다.

② 제1항의 규정에 따른 개인정보취급방침에는 다음 각 호의 사항이 모두 포함되어야 한다.

1. 개인정보의 수집 · 이용 목적, 수집하는 개인정보의 항목 및 수집방법
2. 개인정보를 제3자에게 제공하는 경우 제공받는 자의 성명(법인의 경우에는 법인의 명칭을 말한다), 제공받는 자의 이용 목적 및 제공하는 개인정보의 항목
3. 개인정보의 보유 및 이용 기간, 개인정보의 파기절차 및 방법(제29조 단서의 규정에 따라 개인정보를 보존하려는 경우에는 그 보존근거 및 보존하는 개인정보 항목을 포함한다)
4. 개인정보취급위탁을 하는 업무의 내용 및 수탁자(해당되는 경우에 한한다)
5. 이용자 및 법정대리인의 권리와 그 행사방법
6. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치 · 운영 및 그 거부에 관한 사항
7. 개인정보관리책임자의 성명 또는 개인정보보호 업무 및 관련 고충사항을 처리하는 부서의 명칭과 그 전화번호 등 연락처

③ 정보통신서비스제공자등은 제1항의 규정에 따른 개인정보취급방침을 변경하는 경우에는 그 이유 및 변경 내용을 정보통신부령이 정하는 방법에 따라 지체 없이 공지하고, 이용자가 언제든지 변경된 사항을 쉽게 알아볼 수 있도록 조치하여야 한다.

[본조신설 2007.1.26]

제28조 (개인정보의 보호조치) ① 정보통신서비스제공자등은 이용자의 개인정보를 취급함에 있어서 개인정보가 분실 · 도난 · 누출 · 변조 또는 훼손되지 아니하도록 정보통신부령이 정하는 바에 따라 안전성 확보에 필요한 기술적 · 관리적 조치를 하여야 한다.

② 정보통신서비스제공자등은 이용자의 개인정보를 취급하는 자를 최소한으로 제한하여야 한다.
[전문개정 2007.1.26]

제28조의2 (개인정보의 누설 금지) 이용자의 개인정보를 취급하거나 취급하였던 자는 직무상 알게 된 개인정보를 훼손·침해 또는 누설하여서는 아니 된다.
[본조신설 2007.1.26]

제29조 (개인정보의 파기) 정보통신서비스제공자등은 다음 각 호의 어느 하나에 해당하는 경우에는 당해 개인정보를 지체 없이 파기하여야 한다. 다만, 다른 법률에 따라 개인정보를 보존하여야 하는 경우에는 그러하지 아니하다.

1. 제22조제1항·제23조제1항 단서 또는 제24조의2제1항 및 제2항의 규정에 따라 동의를 얻은 개인정보의 수집·이용 목적 또는 제22조제2항 각 호에서 정한 해당 목적을 달성한 경우
2. 제22조제1항·제23조제1항 단서 또는 제24조의2제1항 및 제2항의 규정에 따라 동의를 얻은 개인정보의 보유 및 이용 기간이 종료한 경우
3. 제22조제2항의 규정에 따라 이용자의 동의를 얻지 않고 수집·이용한 때에는 제27조의2제2항제3호의 규정에 따른 개인정보의 보유 및 이용 기간이 종료한 경우
4. 사업을 폐지하는 경우

[전문개정 2007.1.26]

제3절 이용자의 권리

제30조 (이용자의 권리 등) ① 이용자는 정보통신서비스제공자등에 대하여

언제든지 개인정보수집 · 이용 · 제공 등의 동의를 철회할 수 있다.
〈개정 2007.1.26〉
② 이용자는 정보통신서비스제공자등에 대하여 본인에 관한 다음 각 호의 어느 하나의 사항에 대한 열람 또는 제공을 요구할 수 있고 오류가 있는 경우에는 그 정정을 요구할 수 있다. 〈개정 2007.1.26〉

1. 정보통신서비스제공자등이 보유하고 있는 이용자의 개인정보
2. 정보통신서비스제공자등이 이용자의 개인정보를 이용하거나 제3자에게 제공한 내역
3. 정보통신서비스제공자등에게 개인정보수집 · 이용 · 제공 등의 동의를 한 내역

③ 정보통신서비스제공자등은 이용자가 제1항의 규정에 의하여 동의를 철회한 경우에는 지체없이 수집된 개인정보를 파기하는 등 필요한 조치를 취하여야 한다.
④ 정보통신서비스제공자등은 제2항의 규정에 따라 열람 또는 제공을 요구받은 경우에는 지체없이 필요한 조치를 취하여야 한다. 〈개정 2004.1.29, 2007.1.26〉
⑤ 정보통신서비스제공자등은 제2항의 규정에 따라 오류의 정정을 요구받은 경우에는 지체 없이 그 오류를 정정하거나 정정하지 못하는 사유를 이용자에게 통지하는 등 필요한 조치를 취하여야 하고, 필요한 조치를 취할 때까지는 당해 개인정보를 제공 또는 이용하여서는 아니 된다. 다만, 다른 법률에 따라 개인정보의 제공을 요청받은 경우에는 그러하지 아니하다. 〈개정 2007.1.26〉
⑥ 정보통신서비스제공자등은 제1항의 규정에 따른 동의의 철회 또는 제2항의 규정에 따른 개인정보의 열람 · 제공 또는 오류의 정정을 요구하는 방법을 개인정보의 수집 방법보다 쉽게 하여야 한다. 〈개정 2007.1.26〉
⑦ 제1항 내지 제6항의 규정은 영업양수자등에 이를 준용한다. 이 경우 "정보통신서비스제공자등"은 "영업양수자등"으로 본다.

제31조 (법정대리인의 권리) ① 정보통신서비스제공자등이 만 14세 미만의 아동으로부터 개인정보수집 · 이용 · 제공 등의 동의를 얻고자 하는 경우에는 그 법정대리인의 동의를 얻어야 한다. 이 경우 정보통신서비스제공자는 그 아동에게 법정대리인의 동의를 얻기 위하여 필요한 법정대리인의 성명 등 최소한의 정보를 요구할 수 있다. 〈개정 2007.1.26〉
② 법정대리인은 당해 아동의 개인정보에 대하여 제30조제1항 및 제2항의 규정에 따른 이용자의 권리를 행사할 수 있다. 〈개정 2007.1.26〉
③ 제30조제3항 내지 제5항의 규정은 제2항의 규정에 의하여 법정대리인이 동의를 철회하거나 열람 또는 오류정정의 요구에 관하여 이를 준용한다.

제32조 (손해배상) 이용자는 정보통신서비스제공자등이 이 장의 규정을 위반한 행위로 손해를 입은 경우에는 그 정보통신서비스제공자등에 대하여 손해배상을 청구할 수 있다. 이 경우 당해 정보통신서비스제공자등은 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.

제4절 개인정보분쟁조정위원회

제33조 (개인정보분쟁조정위원회의 설치 및 구성) ① 개인정보에 관한 분쟁을 조정하기 위하여 개인정보분쟁조정위원회(이하 "분쟁조정위원회"라 한다)를 둔다.
② 분쟁조정위원회는 위원장 1인을 포함한 15인 이내의 위원으로 구성하며, 그 중 1인은 상임으로 한다.
③ 위원은 다음 각호의 1의 자 중에서 대통령령이 정하는 바에 의하여 정보통신부장관이 임명 또는 위촉한다. 이 경우 다음 각호의 1의 자가 1인 이상 포함되어야 한다. 〈개정 2005.12.29〉

1. 대학이나 공인된 연구기관에서 부교수급 이상 또는 이에 상당하는 직에 있거나 있었던 자로서 개인정보보호관련 분야를 전공한 자

2. 4급 이상 공무원(고위공무원단에 속하는 일반직공무원을 포함한다) 또는 이에 상당하는 공공기관의 직에 있거나 있었던 자로서 개인정보보호업무에 관한 경험이 있는 자
3. 판사 · 검사 또는 변호사의 자격이 있는 자
4. 정보통신서비스이용자단체의 임원의 직에 있거나 있었던 자
5. 정보통신서비스제공자 또는 정보통신서비스제공자단체의 임원의 직에 있거나 있었던 자
6. 비영리민간단체지원법 제2조의 규정에 의한 비영리민간단체에서 추천한 자

④ 위원의 임기는 3년으로 하고, 연임할 수 있다.
⑤ 위원장은 위원중에서 정보통신부장관이 임명한다.
⑥ 분쟁조정위원회의 업무를 지원하기 위하여 제52조의 규정에 의한 한국정보보호진흥원(이하 제46조의2 · 제47조 · 제47조의2 · 제48조의2 및 제48조의3, 제49조의2에서 "보호진흥원"이라 한다)에 사무국을 둔다.
〈개정 2004.1.29, 2005.12.30〉

제33조의2 (조정부) ① 분쟁의 조정업무를 효율적으로 수행하기 위하여 분쟁조정위원회에 5인 이하의 위원으로 구성되는 조정부를 두되, 그 중 1인은 변호사의 자격이 있는 자로 한다.
② 분쟁조정위원회는 필요한 경우 일부 분쟁에 대하여 제1항의 규정에 의한 조정부에 일임하여 조정하게 할 수 있다.
③ 제1항의 규정에 의한 조정부의 구성 및 운영에 관하여 필요한 사항은 정보통신부령으로 정한다.
[본조신설 2004.1.29]
제34조 (위원의 신분보장) 위원은 자격정지 이상의 형의 선고를 받거나 심신상의 장애로 직무를 수행할 수 없는 경우를 제외하고는 그의 의사에 반하여 면직 또는 해촉되지 아니한다.

제35조 (위원의 제척 · 기피 · 회피) ① 위원은 다음 각호의 1에 해당하는 경우에는 당해 분쟁조정청구사건(이하 이 조에서 "사건"이라 한다)의 심의 · 의결에서 제척된다.

1. 위원 또는 그 배우자나 배우자이었던 자가 당해 사건의 당사자가 되거나 당해 사건에 관하여 공동권리자 또는 의무자의 관계에 있는 경우
2. 위원이 당해 사건의 당사자와 친족관계에 있거나 있었던 경우
3. 위원이 당해 사건에 관하여 증언이나 감정을 한 경우
4. 위원이 당해 사건에 관하여 당사자의 대리인 또는 임직원으로서 관여하거나 관여하였던 경우

② 당사자는 위원에게 심의 · 의결의 공정을 기대하기 어려운 사정이 있는 경우에는 분쟁조정위원회에 기피신청을 할 수 있다. 이 경우 분쟁조정위원회는 기피신청이 타당하다고 인정하는 때에는 기피의 결정을 한다.

③ 위원이 제1항 또는 제2항의 사유에 해당하는 경우에는 스스로 그 사건의 심의 · 의결에서 회피할 수 있다.

제36조 (분쟁의 조정) ① 개인정보와 관련한 분쟁의 조정을 원하는 자는 분쟁조정위원회에 분쟁의 조정을 신청할 수 있다.

② 제1항의 규정에 의한 분쟁의 조정신청을 받은 분쟁조정위원회는 신청을 받은 날부터 60일 이내에 이를 심사하여 조정안을 작성하여야 한다. 다만, 부득이한 사정이 있는 경우에는 분쟁조정위원회의 의결로 그 기간을 연장할 수 있다.

③ 제2항 단서의 규정에 의하여 기간을 연장한 경우에는 기간연장의 사유 그 밖의 기간연장에 대한 사항을 신청인에게 통보하여야 한다.

제37조 (자료요청 등) ① 분쟁조정위원회는 분쟁조정을 위하여 필요한 자료의 제공을 분쟁당사자에게 요청할 수 있다. 이 경우 당해 분쟁당사자는 정당한 사유가 없는 한 이에 응하여야 한다.

② 분쟁조정위원회는 필요하다고 인정하는 경우에는 분쟁당사자 또는 참고인으로 하여금 분쟁조정위원회에 출석하게 하여 그 의견을 들을 수 있다.

제38조 (조정의 효력) ① 분쟁조정위원회는 제36조제2항의 규정에 의하여 조정안을 작성한 때에는 지체없이 이를 각 당사자에게 제시하여야 한다.
② 제1항의 규정에 의하여 조정안을 제시받은 당사자는 그 제시를 받은 날부터 15일 이내에 그 수락여부를 분쟁조정위원회에 통보하여야 한다.
③ 당사자가 조정안을 수락한 때에는 분쟁조정위원회는 즉시 조정서를 작성하여야 하며, 위원장 및 각 당사자는 이에 기명날인하여야 한다.
④ 당사자가 제3항의 규정에 의하여 조정안을 수락하고 조정서에 기명날인한 때에는 당사자간에 조정서와 동일한 내용의 합의가 성립된 것으로 본다.
제39조 (조정의 거부 및 중지) ①분쟁조정위원회는 분쟁의 성질상 분쟁조정위원회에서 조정함이 적합하지 아니하다고 인정하거나 부정한 목적으로 신청되었다고 인정하는 경우에는 당해 조정을 거부할 수 있다. 이 경우 조정거부의 사유 등을 신청인에게 통보하여야 한다.
② 분쟁조정위원회는 신청된 조정사건에 대한 처리절차를 진행중에 일방 당사자가 소를 제기한 때에는 그 조정의 처리를 중지하고 이를 당사자에게 통보하여야 한다.

제40조 (조정절차 등) 제36조 내지 제39조에서 정한 것외에 분쟁의 조정방법 · 조정절차 및 조정업무의 처리 등에 관하여 필요한 사항은 대통령령으로 정한다.

A-b. 정보통신망이용촉진및정보보호등에관한법률시행령

[일부개정 2006.10.27 대통령령 제19719호]

제4장 개인정보의 보호

제10조 삭제 〈2005.3.30〉

제11조 (영업의 양수 등의 통지) ① 법 제26조제1항의 규정에 의하여 정보통신서비스제공자와 그로부터 이용자의 개인정보를 제공받은 자(이하 "정보통신서비스제공자등"이라 한다)가 권리 · 의무를 이전하는 경우 그 사실을 통지하는 방법은 다음 각호와 같다.

1. 인터넷홈페이지에 최소 30일 이상 게시
2. 서면 · 전자우편 그 밖의 방법으로 이용자에게 통지

② 제1항제2호의 규정에 의한 통지는 정보통신서비스제공자등이 과실 없이 이용자의 연락처를 알지 못하거나 천재 · 지변 그 밖에 통지할 수 없는 정당한 사유가 있는 경우에는 2 이상의 중앙일간지(이용자의 대부분이 특정지역에 거주하는 경우에는 그 지역을 보급구역으로 하는 일간지로 할 수 있다)에 1회 이상 공고하는 것으로 갈음할 수 있다.

③ 법 제26조제2항의 규정에 의하여 권리 · 의무를 승계한 정보통신서비스제공자등의 이용자에 대한 통지에 관하여는 제1항 및 제2항의 규정을 준용한다.

④ 법 제26조제2항제5호에서 "대통령령으로 정하는 사항"이라 함은 다음 각호의 사항을 말한다.

1. 개인정보 항목

2. 개인정보의 보유기간 및 이용기간

제12조 (개인정보분쟁조정위원회 위원장의 직무) ① 법 제33조의 규정에 의한 개인정보분쟁조정위원회(이하 "분쟁조정위원회"라 한다)의 위원장(이하 "위원장"이라 한다)은 분쟁조정위원회를 대표하고, 그 직무를 통할한다.
② 위원장이 부득이한 사유로 직무를 수행할 수 없는 때에는 위원장이 지명한 위원이 그 직무를 대행한다.

제13조 삭제 〈2004.7.30〉

제14조 (분쟁조정위원회 등의 운영) ① 위원장은 분쟁조정위원회의 회의를 소집하며, 그 의장이 된다.
② 위원장이 분쟁조정위원회의 회의를 소집하고자 하는 때에는 회의개최 5일전까지 회의의 일시 · 장소 및 심사안건을 각 위원에게 통지하여야 한다. 다만, 긴급을 요하는 경우에는 회의개최 5일전까지 통지하지 아니할 수 있다.
③ 분쟁조정위원회는 위원장을 포함한 재적위원 과반수의 출석으로 개의하며 출석위원 과반수의 찬성으로 의결한다.
④ 분쟁조정위원회 및 법 제33조의2의 규정에 의한 조정부(이하 "조정부"라 한다)의 회의는 공개하지 아니한다. 다만, 필요하다고 인정될 때에는 분쟁조정위원회의 의결로 당사자 또는 이해관계인에게 방청을 하게 할 수 있다. 〈개정 2004.7.30〉

제15조 (사무국) 법 제33조제6항의 규정에 의한 사무국은 위원장의 명을 받아 분쟁조정신청사건에 대한 사실확인 및 그 밖의 사무 등을 처리한다.

제16조 (조정전 합의권고) 분쟁조정위원회는 법 제36조제1항의 규정에

의한 분쟁조정의 신청을 받은 때에는 당사자에게 그 내용을 통지하고 조정전 합의를 권고할 수 있다.

제17조 (의견청취) 분쟁조정위원회는 법 제37조제2항의 규정에 의하여 의견을 듣고자 하는 때에는 일시 및 장소를 정하여 의견청취 5일전까지 당사자 또는 참고인에게 통지하여야 한다. 다만, 긴급을 요하는 경우에는 그러하지 아니하다.

제18조 (수당과 여비) 분쟁조정위원회 및 조정부의 회의에 출석한 위원 등에 대하여는 예산의 범위안에서 수당과 여비를 지급할 수 있다. 다만, 공무원인 위원이 그 소관업무와 직접적으로 관련되어 출석하는 경우에는 그러하지 아니하다. 〈개정 2004.7.30〉

제19조 (분쟁조정세칙) 이 영에서 규정한 것 외에 분쟁조정위원회의 운영 그 밖에 분쟁조정에 관하여 필요한 사항은 분쟁조정위원회의 의결을 거쳐 위원장이 정한다.

A-c. 정보통신망이용촉진및정보보호등에관한법률시행규칙

[일부개정 2006.7.14 정보통신부령 제199호]

제4장 개인정보의 보호

제3조 (개인정보관리책임자의 자격요건 등) ①정보통신서비스제공자와 그로부터 이용자의 개인정보를 제공받은 자(이하 "정보통신서비스제공자등"이라 한다)가 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 "법"이라 한다) 제27조제1항 본문에 따라 지정하는 개인정보관리책임자는 다음 각 호의 어느 하나에 해당하는 지위에 있는 자로 하여야 한다.

1. 임원
2. 개인정보와 관련하여 이용자의 고충처리를 담당하는 부서의 장

② 법 제27조제1항 단서에서 "정보통신부령이 정하는 기준에 해당하는 정보통신서비스제공자등"이라 함은 상시 종업원 수가 5인 미만인 정보통신서비스제공자등을 말한다. 다만, 인터넷으로 정보통신서비스를 제공하는 것을 주된 업으로 하는 정보통신서비스제공자등의 경우에는 상시 종업원 수가 5인 미만으로서 전년도말 기준으로 직전 3개월간의 일일평균이용자가 1,000명 이하인 자를 말한다.

[전문개정 2007.3.16]

제3조의2 (개인정보의 보호조치) ① 법 제28조의 규정에 의한 개인정보의 안전성 확보에 필요한 기술적 · 관리적 조치는 다음 각호와 같다.

1. 개인정보의 안전한 취급을 위한 내부관리계획의 수립 및 시행
2. 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등

접근통제장치의 설치 · 운영

3. 접속기록의 위조 · 변조 방지를 위한 조치

4. 개인정보를 안전하게 저장 · 전송할 수 있는 암호화기술 등을 이용한 보안조치

5. 백신소프트웨어의 설치 · 운영 등 컴퓨터바이러스 방지 조치

6. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치

② 정보통신부장관은 제1항 각호의 규정에 의한 보호조치의 구체적인 기준을 정하여 고시하여야 한다.

[본조신설 2004.7.30]

제3조의3 (조정부의 구성 및 운영) ① 법 제33조의2의 규정에 의한 조정부는 개인정보분쟁조정위원회의 위원장(이하 "위원장"이라 한다)이 지명하는 5인 이내의 위원으로 구성한다.

② 조정부의 회의는 위원장이 소집한다.

③ 위원장이 조정부의 회의를 개최하고자 하는 때에는 회의 일시 · 장소 및 심사안건을 정하여 부득이한 사유가 있는 경우를 제외하고는 회의개시 7일 전까지 각 위원에게 통지하여야 한다.

④ 조정부의 회의는 위원 과반수의 출석으로 개의하며 출석위원 과반수의 찬성으로 의결한다.

⑤ 조정부의 장은 위원중에서 호선한다.

[본조신설 2004.7.30]

제3조의4 (분쟁조정세칙) 이 규칙에서 정한 것외에 조정부의 구성 및 운영에 관하여 필요한 사항은 개인정보분쟁조정위원회의 의결로 정한다.

[본조신설 2004.7.30]

제11조의3 (개인정보 국외이전시 보호조치) ① 법 제54조제3항에서 "이전목적

등 정보통신부령이 정하는 사항"이라 함은 다음 각호의 사항을 말한다.

1. 이전되는 개인정보 항목
2. 개인정보가 이전되는 국가, 이전일시 및 이용기간
3. 개인정보를 이전받는 자의 성명(법인의 경우에는 명칭) 및 정보관리 책임자의 연락처
4. 개인정보의 이전목적 및 이전방법

② 법 제54조제4항의 규정에 의하여 개인정보의 국외이전시 취하여야 하는 보호조치는 다음 각호와 같다.

1. 제3조의2의 규정에 의한 개인정보보호를 위한 기술적 · 관리적 조치
2. 개인정보침해에 대한 고충처리 및 분쟁해결에 관한 사항
3. 그 밖에 이용자의 개인정보보호를 위하여 필요한 조치

③ 정보통신서비스제공자등은 제2항 각호의 사항을 당해 개인정보를 국외에서 이전받는 자와 사전에 협의하고, 이를 계약내용 등에 반영하여야 한다.

[본조신설 2004.7.30]

이 핸드북의 작성을 위하여 다음과 같은 분들께서 수고 하셨습니다.

2007년 4월

총괄책임자	정보통신부	개인정보보호팀	팀 장	정 현 철
기획 및 집필	한국정보보호진흥원	개인정보보호지원센터	단 장	박 광 진
	정보통신부	개인정보보호팀	서 기 관	박 형 민
	한국정보보호진흥원	기술지원TFT	팀 장	이 강 신
	한국정보보호진흥원	기술지원TFT	선 임	홍 기 향
	한국정보보호진흥원	기술지원TFT	주 임	이 진 태
	한국정보보호진흥원	기술지원TFT	주 임	김 정 희
감 수	GMARKET	보 안 팀	팀 장	박 의 원
	이니텍	컨설팅사업부	과 장	김 동 우
	이니텍	컨설팅사업부	차 장	정 찬 석
	SM시큐리티컨설팅	컨설팅사업부	책 임	오 영 수

중소기업 개인정보보호 핸드북

2007년 4월 인쇄
2007년 4월 발행

발행처 : **정보통신부 · 한국정보보호진흥원**
서울특별시 종로구 세종로 100번지
정보통신부
서울특별시 송파구 가락동 78번지
한국정보보호진흥원
Tel : (02) 405-5114
인쇄처 : 한올
Tel : (02) 2279-8494

Information Security

정 보 통 신 부

110-777 서울특별시 종로구 세종로 100번지
정보통신부
대표전화 : 02-750-2114
www.mic.go.kr

한국정보보호진흥원

138-803 서울특별시 송파구 가락동 78번지
한국정보보호진흥원
대표전화 : 02-405-5114
www.kisa.or.kr