12. 안전한 사이버 환경 구축-I

안동대학교 컴퓨터공학과
차세대 네트워크 연구실

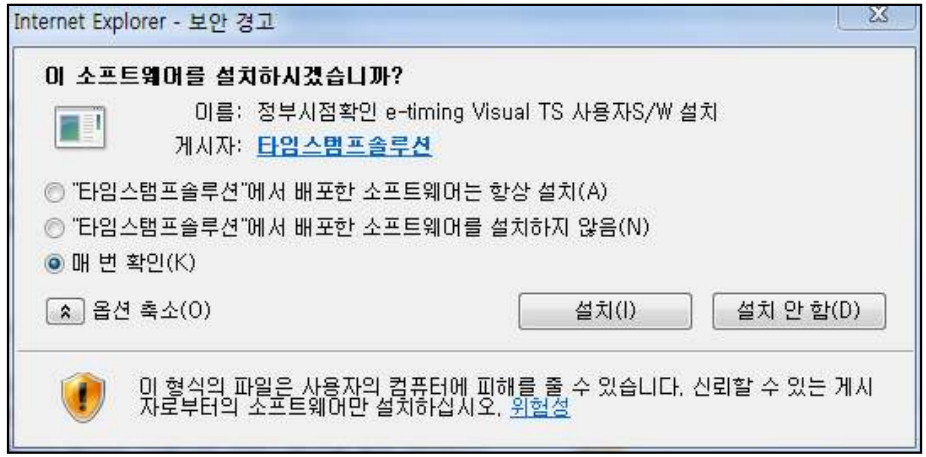
안동대학교
ANDONG NATIONAL UNIVERSITY

목차

- 액티브 콘텐트의 현황과 코드서명용 인증서
- 안전한 쿠키의 사용
- 스팸메일 차단과 안전한 전자메일 사용
- 유해 콘텐트 차단 프로그램

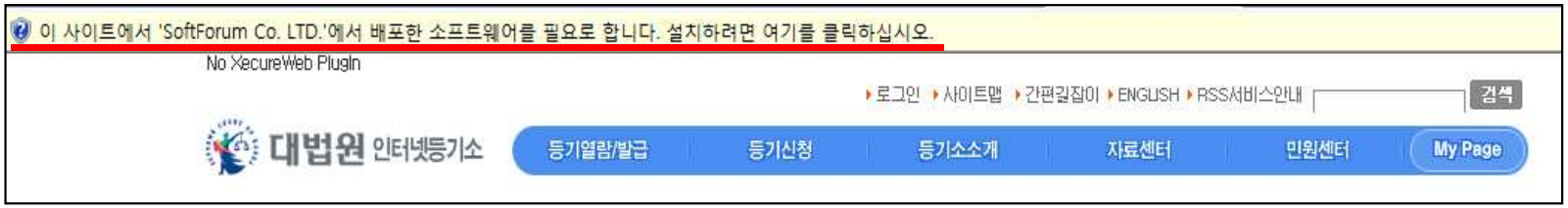
액티브 콘텐트

- 웹 브라우저에서 동작하는 배포용 응용 프로그램을 생성하는데 사용
  - 자바 애플릿은 거의 모든 플랫폼에서 실행되지만 ActiveX는 MS 운영체제와 인터넷 익스플로러에서만 동작
  - 자바 애플릿이나 Fire Fox의 플러그인 프로그램은 웹 브라우저가 할 수 있는 일로 기능이 제한되어 있음
  - ActiveX 컨트롤은 자바 애플릿과 다르게 코드 실행의 제약이 적어 보안에 취약하므로 시스템을 손상시킬 수 있음
  - ActiveX 컨트롤을 통하여 악성코드가 설치될 수 있으므로 ActiveX 컨트롤을 다운로드하기 전에 해당 컨트롤의 안전성(서명, 게시자 등) 확인이 요구됨



국내 액티브 콘텐트 현황

- ActiveX의 천국인 국내에서는 거의 모든 응용 분야에 ActiveX를 설치해야 인터넷 서비스의 이용이 가능
  - 국내 관공서 사이트
  - 각종 금융 및 전자상거래 사이트
- 전자금융거래법에서는 온라인 금융거래를 제공하는 기관은 사용자 PC에 해킹방지 및 키보드 보안 프로그램을 반드시 설치하도록 명시 → ActiveX 사용율의 증가 요인



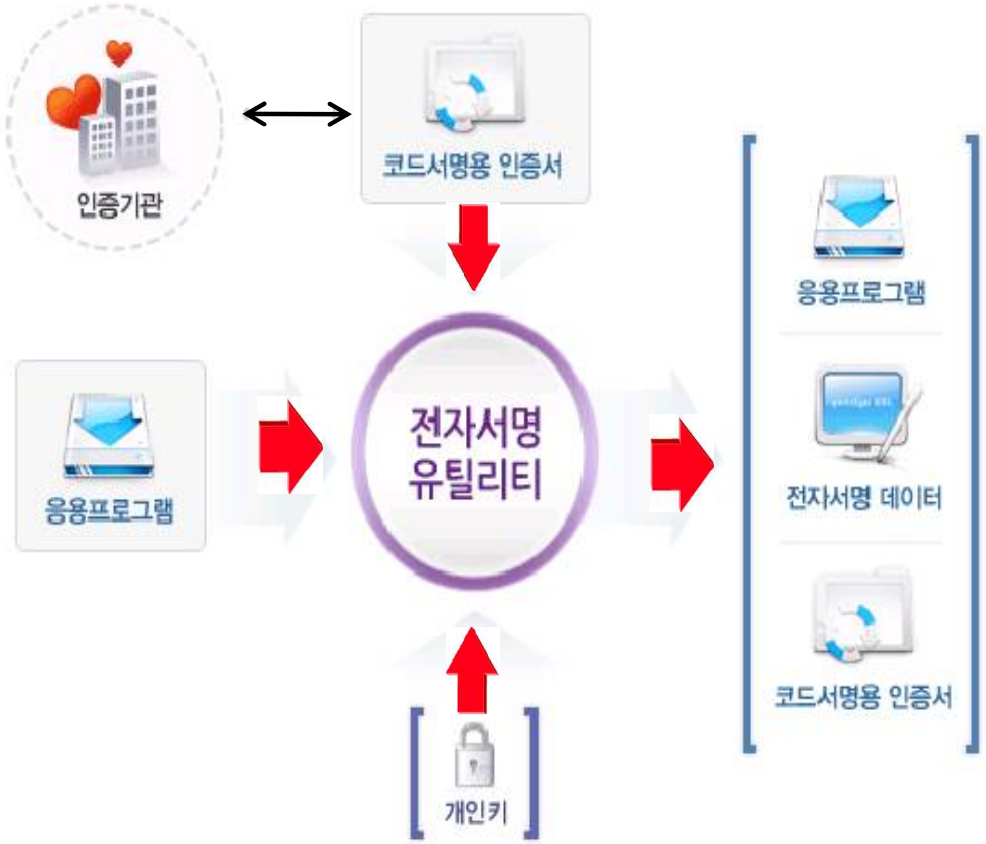
국내 금융기관의 ActiveX 현황

- 인터넷 뱅킹을 위해 은행 사이트를 방문하면 여러 ActiveX가 설치된다.
  - 온라인 경제 메커니즘의 MS 익스플로러 종속
- 2009년 6월 웹 브라우저의 점유율
  - 한국의 인터넷 익스플로러 점유율은 98.5%
  - 유럽의 폭스 점유율은 42.4%, 익스플로러는 42.9%

	우리	외환	하나	신한	국민	동양	우체국
Adobe Flash Player 10 ActiveX	○	○	○	○	○	○	○
Client Keeper KeyPro	○	○					
HanaBank SafeOn			○				
INISafeWeb			○	○			
IssacWebSE 3.3.3.3						○	
K-Defense8 Control							○
LiveCall Suite 2.0s						○	
MeadCo's ScriptX							○
MSXML4							요구
npPCStatus					○		
nProtect KeyCrypt						○	
nProtect Netizen					○		
nProtect Security Center		○					
Personal PC Firewall i-Defense							○
SCSK4			○				
SignGATE EWS Client v3.2							○
SoftCamp Secure KeyStroke				○	○		
VeraPort		○	○				
XecureWeb Control	○	○			○		
	3	5	5	3	5	4	6

코드서명용 인증서(1/2)

- 금융결제원 전자인증센터(https://www.yessign.or.kr/ssl/)의 코드서명용 인증서
  - 악성코드로 인한 전자거래 사고위험의 증가에 따라 배포자가 ActiveX 또는 응용프로그램의 전자서명에 사용하는 인증서 → 응용프로그램의 배포 시에 해당 프로그램의 정보(프로그램명, 회사명, 인증기관)를 확인하여 설치 여부를 판단할 수 있도록 함.



코드서명용 인증서(2/2)

- VeriSign 등의 외국 기관들만 발급을 하였으나, 현재는 국내의 금융결제원에서도 코드서명용 인증서 발급을 개시

- 금융결제원의 yessign 코드서명용 인증서의 주요기능
  - 응용프로그램의 위변조를 확인할 수 있는 무결성 제공
  - 고객에게 프로그램의 정보 제공과 인증기관이 신뢰한 배포자임을 확인시키므로 프로그램의 신뢰성 제공

- 웹에서 배포하는 ActiveX에 공인된 서명이 되어 있지 않으면 브라우저의 보안설정에 따라서 설치 및 실행이 차단된다.

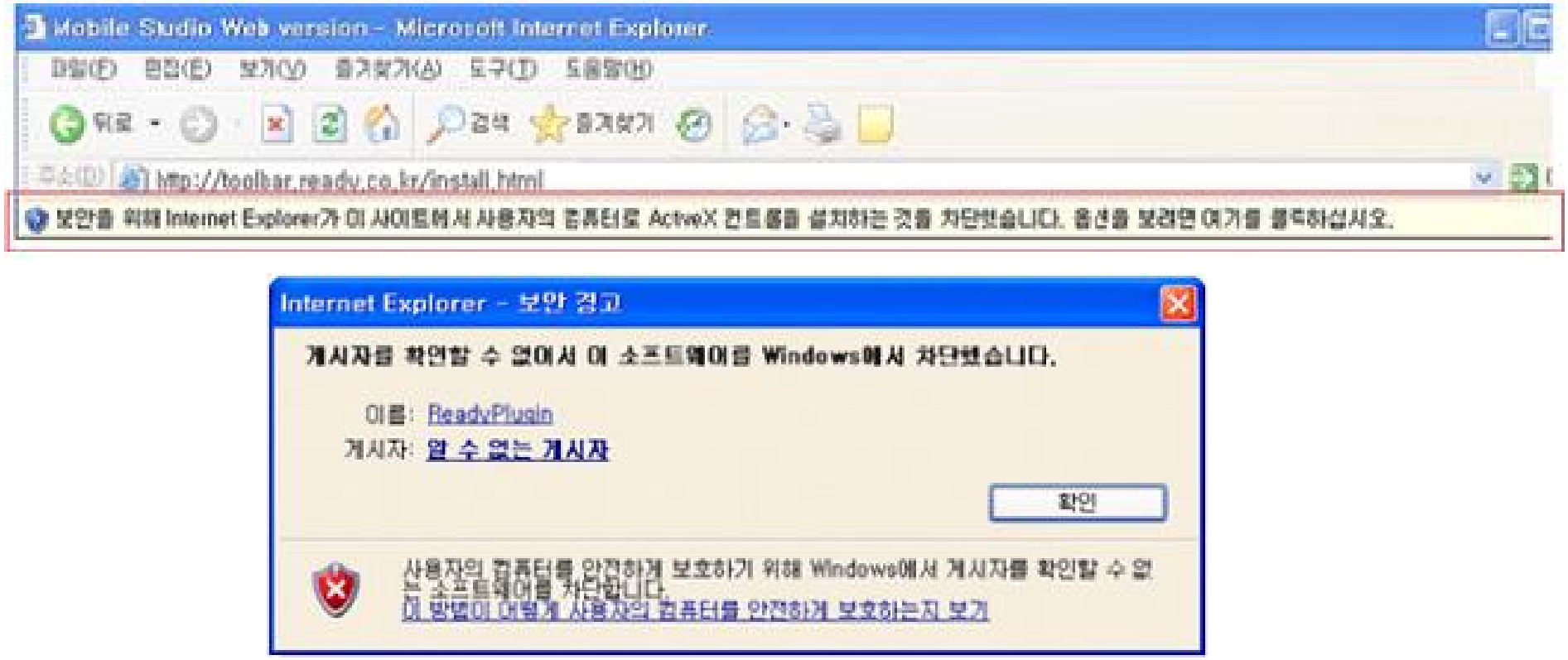
- 코드서명용 인증서는 사이트 단위가 아닌 ActiveX 및 파일 단위로 서명을 하며, 한 번 발급 받으면 유효기간 내에는 계속 사용할 수 있다.

마이크로소프트의 응용프로그램 배포(1/2)

- Microsoft의 보안수준이 대폭강화(2004년 8월의 XP Service Pack2)되어 응용프로그램의 안전한 배포 지원
- 인증된 응용프로그램의 배포: 주소 창 아래의 상태줄을 클릭하면 설치하는 창이 뜨게 되어 프로그램을 용이하게 배포

마이크로소프트의 응용프로그램 배포(2/2)

- 인증받지 않은 응용프로그램의 배포 → 보안관련 상태줄을 클릭하면 차단되었다는 경고창이 뜨면서 응용프로그램의 배포를 차단



쿠키

- 쿠키는 사용자들의 WWW 이용에 대한 편리성을 목적으로 1994년 넷스케이프에 의해 처음 탄생된 기술
  - 웹 서버에 의해 사용자의 하드 디스크에 저장되는 최대 사이즈가 4K 바이트 정도인 텍스트 파일
  - 넷스케이프 사에서 사용자의 로그인 정보(ID, 패스워드)를 저장하기 위해 고안되었으나, 오늘날은 웹 사이트가 사용자 정보를 수집하는 기술로 널리 이용되고 있음

쿠키의 생성과 저장 및 사용

❑ 쿠키의 생성과 저장

- 생성: 클라이언트로 부터 요청을 받은 웹 서버는 클라이언트의 도메인 이름, 서버가 수집한 클라이언트의 정보인 쿠키(ID, 비밀번호, 이름, 생년월일, e메일 주소 등), 타임스탬프 등의 정보를 파일이나 문자열로 하드디스크에 저장함.
- 전송: 서버는 클라이언트에게 보내는 응답에 쿠키를 포함하여 전달
- 저장: 클라이언트는 응답 메시지에 있는 쿠키를 서버의 도메인 이름으로 정렬되는 쿠키 디렉토리에 저장

❑ 쿠키의 사용

- 클라이언트가 특정 웹 사이트를 재 방문하는 경우 요청 메시지에 저장된 쿠키를 포함하여 전달
- 웹 서버는 요청 메시지의 쿠키를 통해 로그인 및 브라우저 정보 및 그 외의 여러 정보를 습득
- 웹 서버가 쿠키의 정보를 이용하므로 클라이언트는 자신이 과거 입력한 ID나 패스워드와 같은 개인 정보를 또 다시 입력하는 번거로움을 피함

영구 및 세션 쿠키

❑ 영구 쿠키

- 몇 일, 몇 달 또는 몇 년 동안 컴퓨터에 저장되는 쿠키
- 차후 해당 쿠키가 사용되는 웹 사이트에 사용자가 접속 할 경우 속성(ID, Password 등)을 기억하여 로그인하는 번거로움을 제거
- 디스크매체에 저장

❑ 세션 쿠키

- 현재의 웹 탐색을 위한 세션용으로 사용되며 웹 브라우저가 종료되면 사용자의 컴퓨터에서 삭제되는 쿠키
- 사용자가 사이트 접속 시 인증 정보를 유지하거나, 장바구니에 들어 있는 항목과 같은 임시 정보를 저장하기 위하여 사용
- 웹 브라우저가 사용하는 메모리 공간에 저장

쿠키의 동작(1/2)

- 클라이언트 -> 서버
  - 클라이언트에 해당 서버의 영구 쿠키가 저장되어 있는 경우 쿠키의 만료 여부를 확인
  - HTTP 메시지에 쿠키요청 헤더를 포함하여 전달
  - Cookie: name1=value1;name2=value2;…
  - Cookie: PHPSESSID=bb9a6640e8cac4f790689aae94a814d3

쿠키의 동작(2/2)

- 서버 -> 클라이언트
  - 클라이언트가 보낸 Cookie 헤더 정보의 해석
  - 추가적인 변경이 있을 경우 HTTP 응답 메시지에 set-Cookie 헤더로 정보를 전송
  - set-Cookie: name=value;expires=date;path=path;domain=domain;secure
  - set-Cookie: login_id=hosik; expires= Sat, Mar-1-2010 16:50:00 GMT; path=/

- 클라이언트 -> 서버
  - 클라이언트는 서버가 전송한 set-Cookie 정보를 검토하여 규약을 만족한다면 적용
  - 추후 해당 서버로 추가된 쿠키 정보를 포함하여 접속
  - Cookie: PHPSESSID=bb9a6640e8cac4f790689aae94a814d3; login_id=hosik

쿠키의 용도

- 사이트 개인화: 사용자의 취향(예, 비즈니스 웹 페이지에서 주식 정보를 주로 검색)을 쿠키에 저장하여 웹 사이트 방문 시에 반영할 수 있다.
- 장바구니(Shopping Cart) 시스템: 전자상거래를 제공하는 웹 사이트는 쿠키를 이용하여 사용자의 구매 내역을 저장할 수 있으며, 과거 구매 기록이 있는 사용자에게 비슷한 다른 아이템을 추천하는 기능까지 제공할 수 있다.
- 웹 사이트의 이용 방식 추적: 웹 사이트는 쿠키를 통해 특정 페이지에 얼마나 많은 사용자들이 방문했는지 파악하여 사이트의 디자인과 기능을 개선하는데 이용할 수 있다. 그러나 쿠키를 이용한 이런 고객 정보 획득은 불법 감시 카메라와 같다는 의견도 만만치 않다.
- 타깃 마케팅: 온라인 광고대행 업체는 야후 같은 웹 사이트의 광고 공간을 미리 사들여 이것을 제3의 업체들이 광고를 낼 수 있도록 임대한다.
  - 광고대행 업체는 제3의 업체들에 대한 쿠키를 사용자 컴퓨터에 저장하고 사용자들의 이용 정보를 수집하여, 그들의 광고를 얼마나 많은 사람들이 보는지, 고객들이 선호하는 광고는 무엇인지 확인할 수 있다.
  - 쿠키가 개인 정보 유출의 주범으로 지목 받는 것은 바로 이러한 용도 때문이다.

쿠키의 취약성

- 자동으로 수집되는 개인정보에 관여가 거의 불가능함
  - 사용자의 의사와 무관하게 자동으로 이루어지므로 사용자가 허용한 범위 이상의 개인정보 수집이 가능

- 특정 사이트의 접근 불가
  - 쿠키가 깨졌을 경우 쿠키 값을 확인하는 중에 오류가 생겨 접근 불가능한 상황 발생
  - 해당 사이트의 쿠키 값을 삭제함으로 해결

- 쿠키 조작(쿠키 스푸핑)
  - 악의적인 공격자가 서버로 전송되는 쿠키를 습득 및 변조 → 쿠키 값을 신뢰하는 웹 서버는 공격자의 의도대로 동작

쿠키에 관한 오해

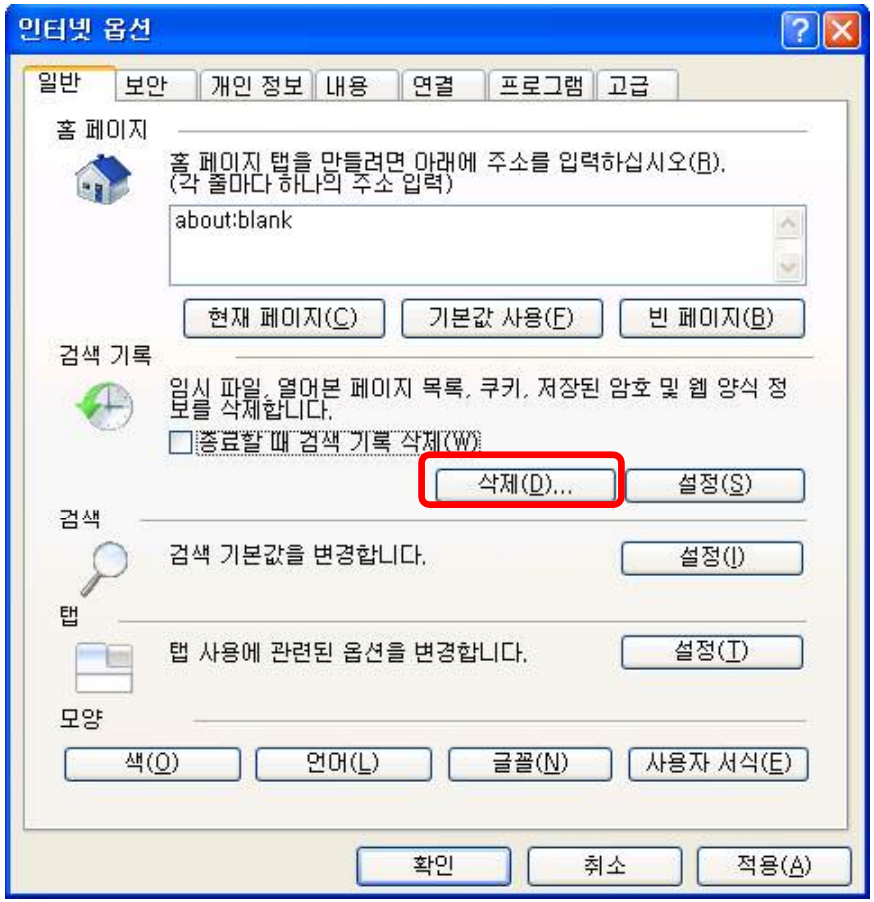
- 쿠키는 실행 파일이 아닌 텍스트 파일이며, 데이터를 저장하는 기능 밖에 없다.
  - 쿠키는 사용자의 하드 디스크를 스캔하거나 디렉터리를 읽거나, 파일을 지우거나, 바이러스를 옮기는 등의 기능은 수행할 수 없다.

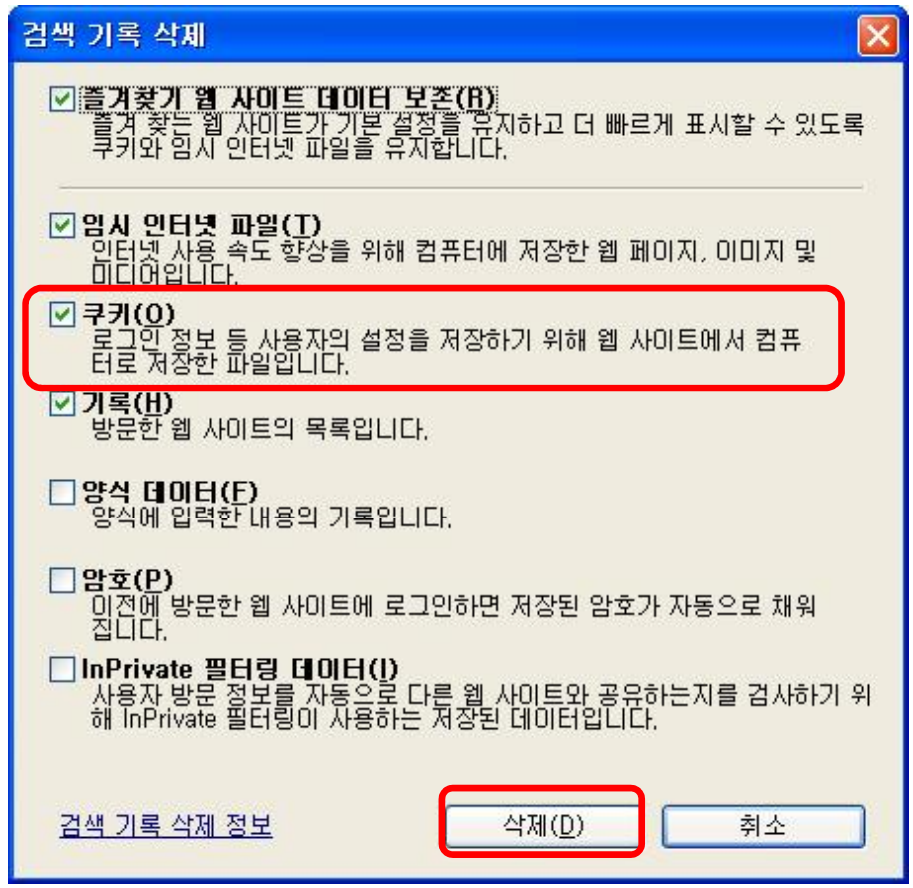
- 쿠키는 자신에게 저장된 도메인 네임을 갖고 있는 사이트만 액세스가 가능하므로 특정 웹 사이트가 저장한 쿠키를 다른 웹 사이트에서 읽어 들일 수 없다.

- 사용자가 특정 웹 사이트에서 자신의 e메일 주소를 입력한 경우에 e메일 주소가 쿠키에 저장된다.
  - 저장된 쿠키는 특정 웹 사이트에서만 액세스가 가능하기 때문에 e메일 주소가 쿠키를 통해 불법 유출되는 일은 없다.

안전한 쿠키의 사용

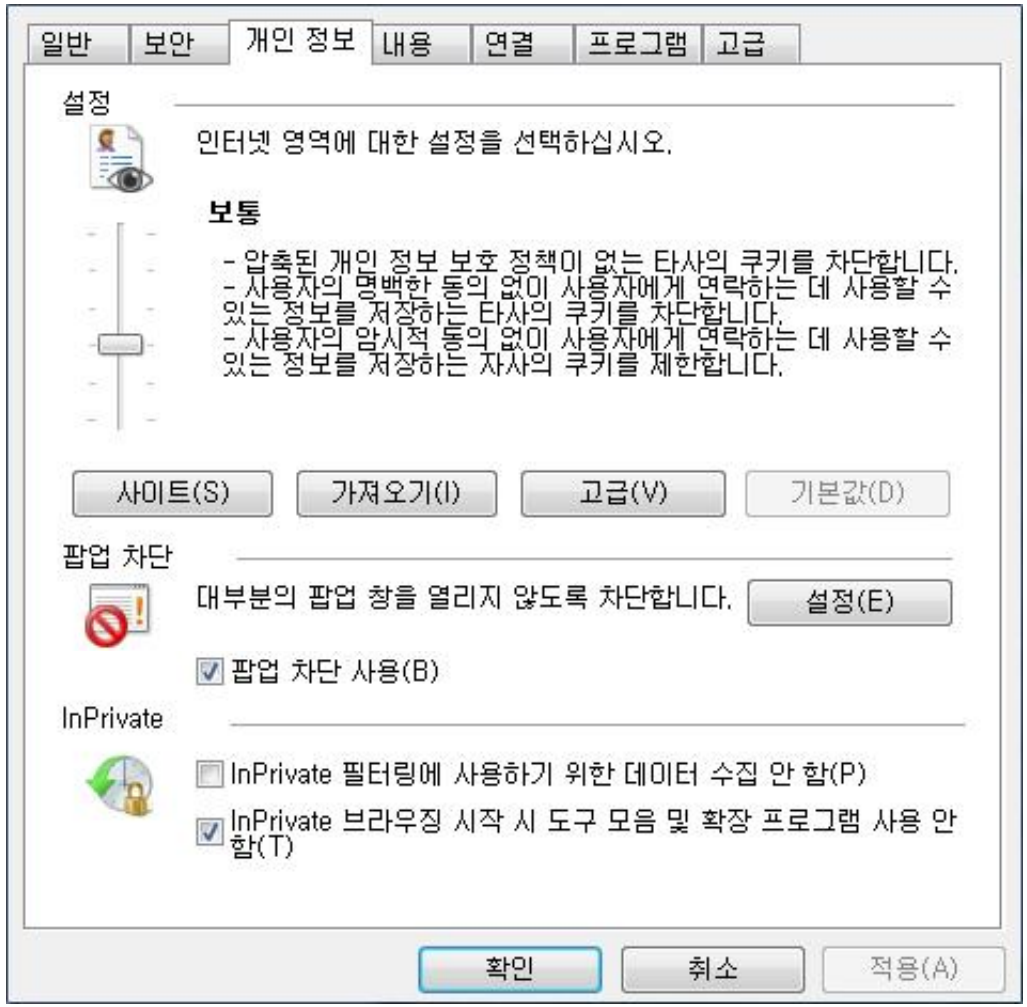
- PC방이나 도서관 등에서 컴퓨터를 사용 후에는 쿠키 파일을 삭제하여 아이디와 비밀번호의 노출을 방지
- 인터넷 익스플로러의 [도구]-[인터넷 옵션]





쿠키 보안 관리

- [도구] -> [인터넷 옵션] -> [개인정보]를 통해 인터넷 익스플로러의 쿠키 보안 설정
  - 모든 쿠키 차단
  - 높음
  - 보통 높음
  - 보통
  - 낮음
  - 모든 쿠키 허용



전용메일 프로그램

- Outlook Express나 Netscape Messenger와 같은 전용메일 프로그램을 이용하여 전자 우편을 송수신 하는 프로그램
  - PC에서 메일을 관리하므로 웹 메일에 비해 저장공간의 제약이 적음
  - 수신 확인을 위한 서버 방문이 필요 없음
- 통신 프로토콜
  - POP3: Post Office Protocol
  - SMTP: Simple Mail Transfer Protocol

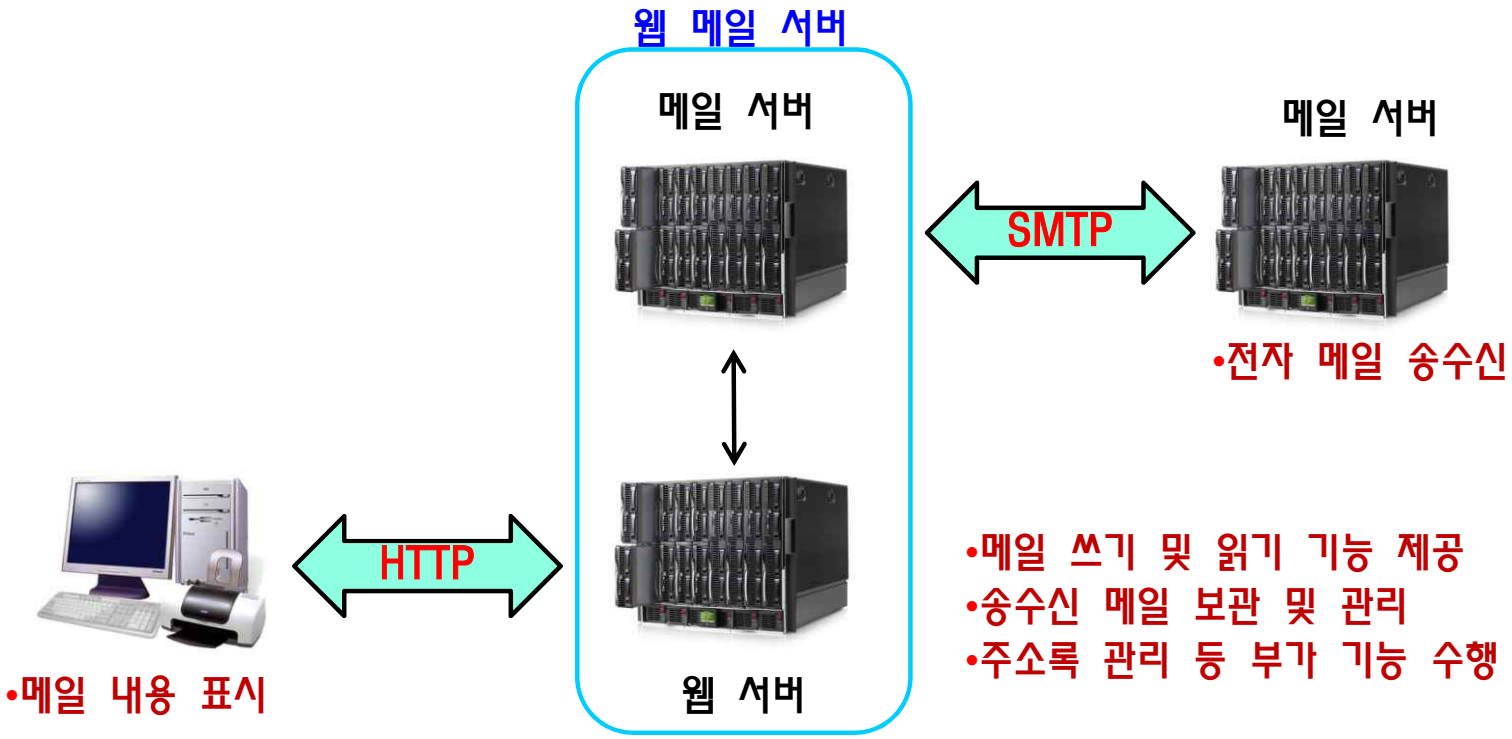
- 메일 쓰기 및 읽기 기능 제공
- 송수신 메일 보관 및 관리
- 주소록 관리 등 부가 기능 수행

- 전자 메일 송수신
- PC에서 작성된 메일을 목적지 메일 서버로 전달

- 전자 메일 송수신

웹 메일

- 웹 브라우저를 이용하여 메일 서비스를 제공하는 웹 서버에 접속
  - 발신 및 수신된 메일은 웹 서버의 사용자 계정에 저장
  - PC에서 관리하는 전용 메일프로그램 방식에 비해 저장 공간의 한계를 지님



스팸 메일

- 수신자의 의사와 무관하게 전송되는 영리/비영리 목적의 광고성/비광고성 전자 우편
  - 스팸: 2차 세계대전 당시 미군에 보급됐던 호멜 사의 고기 통조림 상표
  - 스팸메일: 회사가 통조림을 팔기 위해 불특정 다수에게 스팸을 광고하는 전단지를 무차별적으로 뿌린 것에서 유래
  - 정크메일(Junk Mail), 벌크메일(Bulk Mail)이라고도 부름

- 스팸메일 전송 방식
  - 직접 스팸: 스패머가 자신이 사용하는 메일서버를 통해 불특정 다수의 수신자에게 직접 배포
  - 중계 스팸: 스패머가 자신이 사용하는 메일 서버 대신 임의의 ISP나 기업의 메일서버를 중계서버로 이용 →마치 중계서버의 사용자가 유포하는 것처럼 위장하여 배포하므로 각종 필터링 차단방식을 우회

스팸메일의 현황

- 스팸메일 차단 전문업체 지란지교소프트의 안티스팸연구소에 의한 2007년 상반기의 상위 10개 고객사에 대한 메일 유통량 분석
  - 유통된 이메일 총 2억8천7백 만 통 중 단지 8.8%만이 정상메일이고 나머지는 스팸메일(90.8%)과 바이러스메일(0.4%)
  - 2006년 하반기와 비교해 정상메일은 5.6% 줄고 스팸메일은 6.9%가 증가
  - 스팸메일의 순위
    - 대출광고(34%), 성인사이트와 성인용품 판매 메일(28%)
    - 각종 부동산 및 컴퓨터 자격증 광고(17%)
    - 제품광고(16%) 그리고 기타(5%)

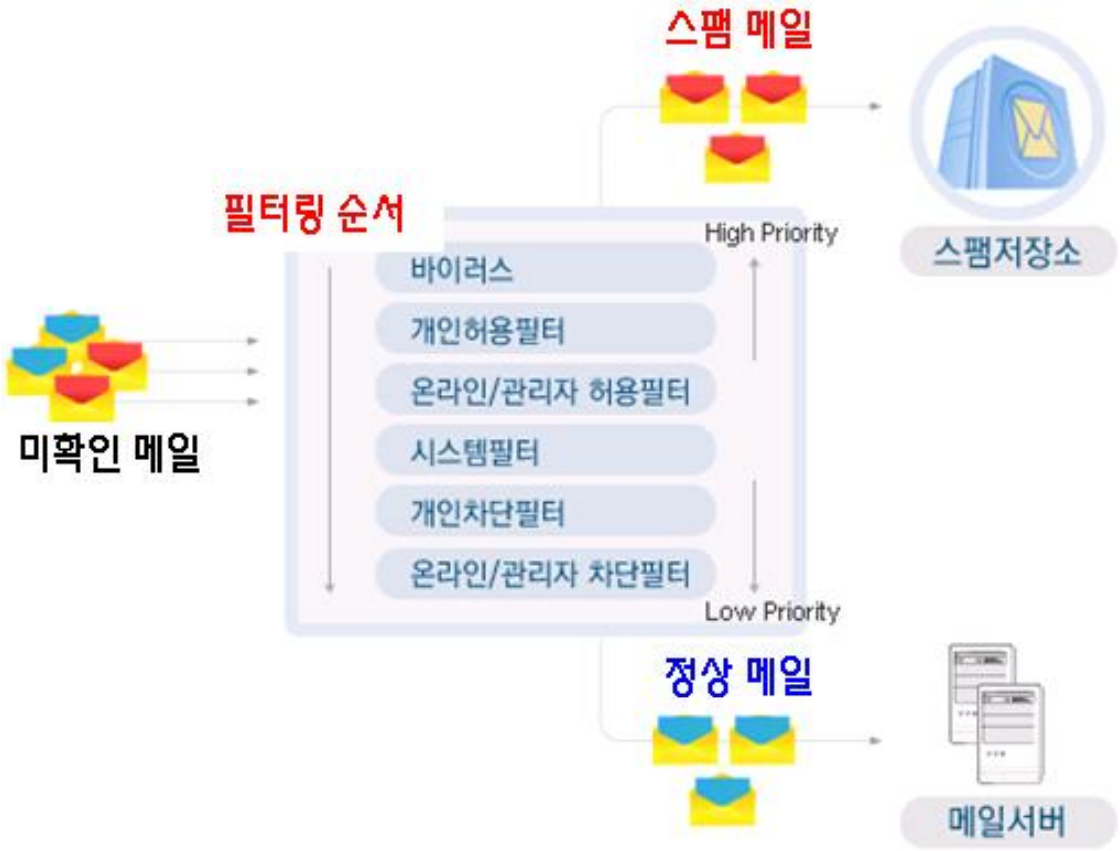
스팸메일 방지 수칙

- 이메일 서비스나 프로그램 자체에서 제공하는 스팸차단 기능 활용
  - 네이버, 다음, 네이트 등의 웹메일: 개인 설정에 들어가 스팸메일 차단 여부를 묻는 체크박스의 체크
  - 아웃룩 사용자: 프로그램 안의 [도구]-[메시지규칙] 기능에서 스팸메일이라고 생각하는 특정 단어 혹은 발송자 이메일 등을 설정하여 스팸메일 차단
- 스팸메일차단 솔루션 활용
  - 지란지교소프트의 스팸스나이퍼, 안철수연구소의 트러스가드, …
- 개인 메일주소 관리
  - 각종 사이트의 회원가입 시에 필수적으로 정보를 수신하여야 할 사이트가 아니라면 별로 사용하지 않는 여분의 메일 주소를 입력
  - 불필요한 광고메일 수신에 동의 않으며, 웹사이트, 게시판 등에 이메일 주소를 남기지 않음
- 수신된 메일 하단의 수신거부 링크를 눌러 수신거부 의사를 전달
  - 이후에도 동일한 곳에서 스팸메일이 온다면 불법스팸대응센터(http://www.spamcop.or.kr)에 신고

스팸 메일 차단 기술

- **콘텐트 필터링:** 메일의 헤더 정보, 본문, 첨부파일의 정보를 읽어서 **차단 솔루션에서 제공하는 필터를** 적용하여 매칭 여부를 판단

- **자동차단 기술:** 스팸 메일의 콘텐트가 아니라 발송형태와 전송방식을 판단해 검출하는 방법으로 대량메일을 차단하기 위해 주로 사용
  - 스팸메일 발송기에서 전송되는 자동생성 메일의 차단
  - 같은 형태의 메일이 단위 시간당 일정량 이상으로 발송될 경우에 차단



전자우편을 통한 악성코드 유포

❑ 전자우편을 통한 악성코드(예, 멜리사 바이러스)의 유포 시에 수신자의 경계심을 감소시키는 유형

- 보안업데이트 공지메일로 위장한 형태, 운송장이나 주문서 메일로 위장한 형태
- 금융거래나 세금고지 메일로 위장한 형태, 서비스 관리자 공지메일로 위장한 형태
- 사회적 이슈를 담은 형태, 기념일을 담은 형태, 소셜 네트워크 서비스를 담은 형태, …


[3보] 카드 **이메일** 명세서 위장 **악성코드**, 목적은 - **보안뉴스**_뉴스
2010년 6월 26일 … 최근 '비씨카드 이용대금 명세서'로 위장한 **악성코드**가 **이메일**로 국내에서 확산되고 … 현재 **보안**업계에서 분석한 **정보**에 따르면, 이번 명세서 **이메일 악성코드**는 … **개인정보 유출**을 막기 위해 가장 필요한 **보안**시스템은 무엇이라고 생각하 시나요? … 웹**보안** 서비스 및 장비. DB**보안** 솔루션. **보안**USB. **보안관제** 서비스 …
www.boannews.com/media/view.asp?idx=21675&kind=1

[긴급] **보안** 파일 발송처럼 위장한 트위터 위장 **메일** - **보안뉴스**_뉴스
2010년 6월 7일 … [**보안뉴스** 김정완] 6월7일 현재, 트위터에서 발송한 **메일**처럼 위장하고, 특정 링크를 클릭하게 만들어 **악성코드**에 감염되도록 하는 트위터 위장 **메일** …
www.boannews.com/media/view.asp?idx=21388&kind=1

❑ 안전한 전자우편 사용

- 신원 불명의 사람이 보낸 전자우편의 첨부 파일을 열 때는 항상 경계해야 함
- 하이퍼링크는 피싱 및 악성코드, 바이러스의 감염 등의 위험에 노출되어 있으므로 전자 우편 메시지의 하이퍼링크를 실행할 경우 항상 주의

유해 콘텐트와 사이트

❑ 유해 콘텐트

- 인터넷 이용자에게 정신적, 시간적, 경제적으로 피해를 가져오는 정보
- 법과 국가질서의 존엄성 유지를 위해 현행법이 생산, 저장, 유통을 금지한 불법 정보
- 미풍양속 등의 문제를 야기시키는 불건전 정보로 음란정보와 폭력정보가 대표적

❑ 유해 사이트

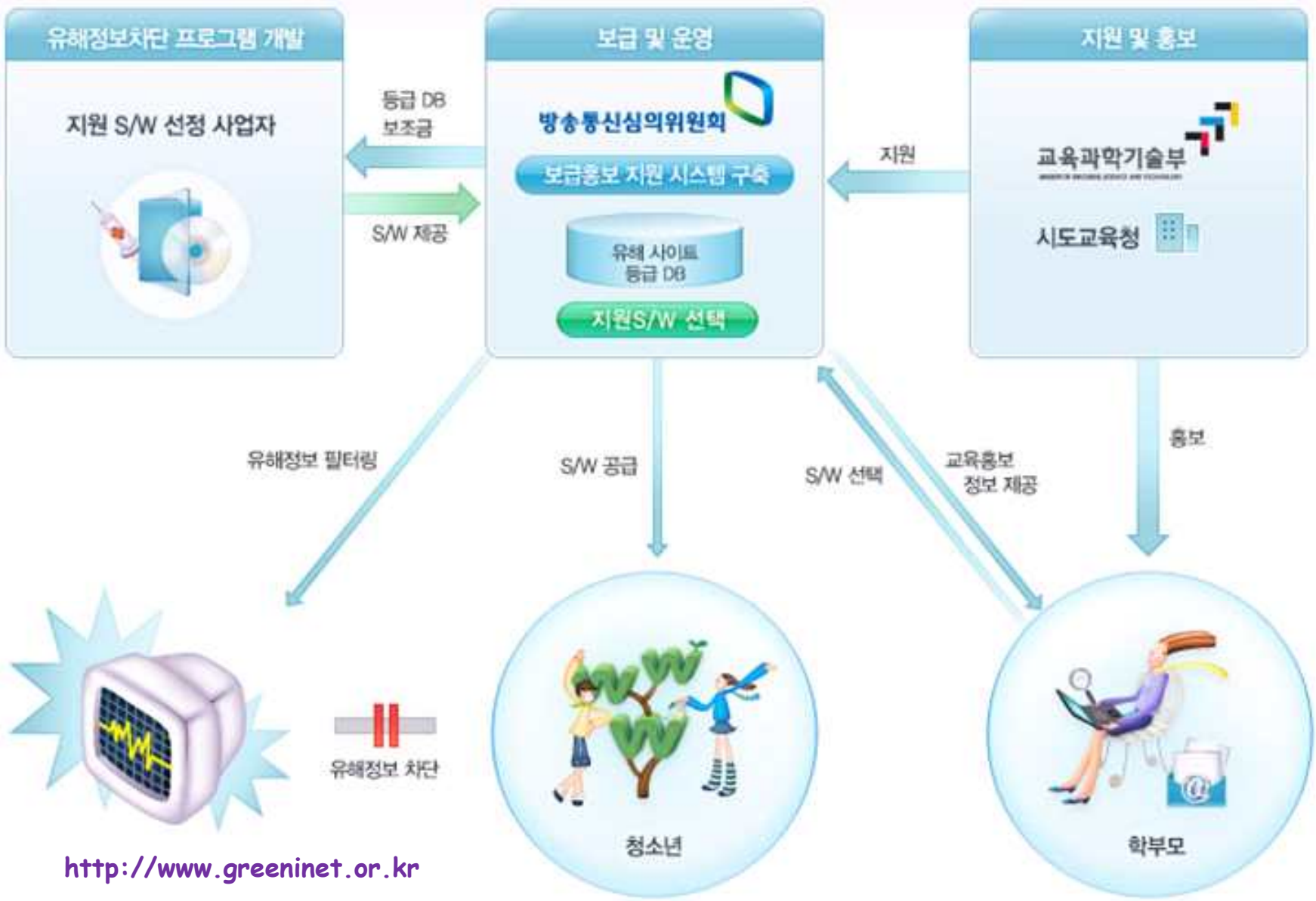
- 음란물 사이트
- 범죄 모의사이트
- 자살 조장사이트
- 폭탄 제조사이트
- 도박 사이트
- 마약 거래사이트, …

청소년 인터넷 안전망(그린 i-Net)

그린 Green + i 아이 + Net 안전망

http://www.greeninet.or.kr

그린 i-Net의 유해정보차단 프로그램 지원체계



유해정보차단 프로그램 기능 비교(1/3)

기능 목록 \ 소프트웨어 종류	맘이on mom	안심	수호천사	키즈	JIKIMI	SG 자녀사랑	아이넷	엑스키퍼 FREE	home 그린윙	iSafe II	SAFER	컴맹지킴이	모하니 3.0
	다운로드	다운로드	다운로드	다운로드	다운로드	다운로드	다운로드	다운로드	다운로드	다운로드	다운로드	다운로드	다운로드
유해사이트 차단													
내용등급 반영	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
허용/차단 예외 적용	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
기타 차단													
유해동영상 차단	✓	✓		✓				✓			✓	✓	✓
P2P (파일공유 프로그램) 차단	✓	✓	✓	✓	✓	✓		✓	✓		✓	✓	
메신저 차단	✓		✓	✓	✓	✓		✓	✓		✓	✓	
특정 프로그램 직접 차단	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

유해정보차단 프로그램 기능 비교(2/3)

기능 목록 \ 소프트웨어 종류	맘아이mom	엄마	수호천사	O2 키즈	JiKIMI	SG 자녀사랑	아이눈	엑스키퍼 FREE	home 그린웨어 홈	iSafe	iSAFER	컴사용지킴이	[illegible] 3.0
	다운로드	다운로드	다운로드	다운로드	다운로드	다운로드	다운로드	다운로드	다운로드	다운로드	다운로드	다운로드	다운로드
관리기능													
PC 사용시간 조회	✓	✓		✓		✓		✓	✓		✓	✓	✓
게임 사용시간 조회	✓			✓		✓			✓		✓	✓	
인터넷 접속내역 조회	✓		✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
인터넷/휴대폰 원격관리	✓		✓		✓	✓		✓		✓		✓	
사용통계내역 이메일서비스	✓	✓				✓		✓	✓			✓	

유해정보차단 프로그램 기능 비교(3/3)

기능 목록 / 소프트웨어 종류	맘아이mom	안심	두손천사	O2 키즈	JiKIMI	SG 자녀사랑	아이넌	엑스키퍼 FREE	home 그린웨어 홈	iSafe II	iSAFER	컴사용지킴이	모하니 3.0
	다운로드	다운로드	다운로드	다운로드	다운로드	다운로드	다운로드	다운로드	다운로드	다운로드	다운로드	다운로드	다운로드
사용시간 관리													
PC 사용시간 제한	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
게임 사용시간 제한	✓	✓		✓		✓			✓		✓	✓	
인터넷 사용시간 제한					✓	✓			✓		✓	✓	
기타 기능													
사용내역 SMS 전송	✓	✓		✓				✓				✓	

컴사용지킴이 사용방법(1/3)

① 사용자 변경
② 부모님 사용모드 전환
③ PC 이용현황
④ 사용시간 설정
⑤ 원격제어 요청
⑥ 인증번호
⑦ 부모님 로그인
⑧ 환경설정

http://www.toxicfree.co.kr/

컴사용지킴이 사용방법(2/3)

1 사용자변경

자녀모드는 부모님이 설정한 시간과 등급으로 게임&인터넷시간을 활용할 수 있습니다.

2 부모님사용모드전환

컴사용지킴이의 유해정보차단 기능을 일시적으로 멈추게 하는 메뉴입니다
부모님사용모드전환에서는 사용시간 및 사이트 제한 없이 사용가능 합니다.

3 PC 이용현황 / 현재 사용자 표시

자녀의 오늘 사용시간(잔여시간)을 즉시 확인 할 수 있는 메뉴입니다.

4 사용시간 설정 / 오늘시간변경 / 이용가이드

요일별 사용시간(게임,인터넷) 변경 / 사용금지 시간설정 / 오늘 사용시간 추가 / 이용가이드

컴사용지킴이 사용방법(3/3)

5 원격제어 요청

원격지원 사이트로 전문상담원과 1:1로 연결되는 메뉴입니다.
원격제어요청은 상담원이 고객의 컴퓨터를 보면서 장애(기술지원)를 해결하는 메뉴입니다.

6 인증번호

고객님의 비밀번호를 분실 하셨을 시 컴사용지킴이 홈페이지를 통하여 확인 할 수 있습니다.
1544-1443 고객센터로 인증번호를 알려주시면 인증절차를 거쳐 확인가능.

7 부모님로그인

자녀의 컴퓨터 환경(시간,등급설정, 사용(게임,인터넷)내역확인)을 관리하는 메뉴입니다.

8 환경설정

시간설정 / 고급설정 / 차단사이트 설정 / (허용,차단)프로세서 설정 /
프로그램 제거 / 문자메세지설정 / E-메일설정 / 사용내역확인

공부방모드

인터넷 강의사이트 및 학습 집중모드 모드 (별도 설정 가능),
학교 숙제 등을 위한 한글 워드 엑셀 프린터등의 제한된 프로그램만 사용이 가능합니다.

유해 콘텐트 차단 프로그램의 한계

- 자살이나 성생활과 관련한 경험담을 포함하고 있는 개인 블로그, 폭발물과 같은 위험 물질 제조방법을 소개하고 있는 카페 등의 웹사이트는 데이터베이스에 등록이 되어 있지 않아 차단이 어려움
- 차단되는 유해사이트라 해도 다양한 도메인을 통해 접근이 가능 → 이러한 맹점을 활용하여 국내 대부분의 유명 유해사이트는 다양한 도메인을 확보하여 차단기능을 회피하고 있음
- 유해정보 차단 S/W의 구현상 문제로 인해 웹브라우저 별로 유해사이트 차단기능의 동작 여부에 차이가 발생
- 유해동영상 차단기능의 경우 동영상의 내용 및 파일명을 기반으로 유무해를 판별하고 차단 → 이는 DB등록 상황과 파일명의 조작, 인코딩 형식의 변화에 따라 차단율이 대폭 하락할 수 있음

요점정리(1/2)

- ActiveX 컨트롤: 웹 브라우저에서 동작하는 배포용 응용 프로그램을 생성하는데 사용되며
  - 코드 실행의 제약이 적어 보안에 취약하므로 시스템을 손상시킬 수 있음
  - ActiveX 컨트롤을 통하여 악성코드가 설치될 수 있으므로 ActiveX 컨트롤을 다운로드하기 전에 해당 컨트롤의 안전성(서명, 게시자 등) 확인이 요구됨
- 금융결제원 전자인증센터의 코드서명용 인증서: 악성코드로 인한 전자거래 사고위험의 증가에 따라 배포자가 ActiveX 또는 응용프로그램의 전자서명에 사용하는 인증서

- 쿠키: 넷스케이프 사에서 사용자의 로그인 정보(ID, 패스워드)를 저장하기 위해 고안되었으나, 오늘날은 웹 사이트가 사용자 정보를 수집하는 기술로 널리 이용되고 있음
  - 사이트 개인화
  - 장바구니(Shopping Cart) 시스템
  - 웹 사이트의 이용 방식 추적
  - 타깃 마케팅
- PC방이나 도서관 등에서 컴퓨터를 사용 후에는 쿠키 파일을 삭제하여 아이디와 비밀번호의 노출을 방지

요점정리(2/2)

❑ 스팸메일 방지 수칙

- 이메일 서비스나 프로그램 자체에서 제공하는 스팸차단 기능 활용
- 스팸스나이퍼, 트러스가드와 같은 스팸메일 차단 솔루션 활용
- 개인 메일주소 관리: 각종 사이트의 회원가입 시에 여분의 메일 주소를 입력하거나, 불필요한 광고메일 수신에 동의하지 않고, 웹사이트, 게시판 등에 이메일 주소를 남기지 않기
- 수신된 메일 하단의 수신거부 링크를 눌러 수신거부 의사를 전달

❑ 안전한 전자우편 사용

- 신원 불명의 사람이 보낸 전자우편의 첨부 파일을 열 때는 항상 경계해야 함
- 하이퍼링크는 피싱 및 악성코드, 바이러스의 감염 등의 위험에 노출되어 있으므로 전자 우편 메시지의 하이퍼링크를 실행할 경우 항상 주의

❑ 유해 콘텐트: 이용자에게 정신적, 시간적, 경제적으로 피해를 가져오는 정보

- 청소년 인터넷 안전망의 유해정보차단 프로그램 (http://www.greeninet.or.kr)