DOI: 10.3745/KIPSTC.2009.16C.5.543

유해정보 차단 S/W 개선방안 연구

전 웅 렬[†] · 이 현 승[††] · 허 순 행[††] · 김 경 신[†††] · 원 동 호[††††] · 김 승 주[†††††]

요 약

초고속 인터넷망의 활발한 보급과 컴퓨터의 대중화로 인해 인터넷은 이제 일상생활에서 없어서는 안될 필수요소가 되었다. 인터넷을 사용하면 전 세계에 걸쳐 다양한 정보를 손쉽게 획득할 수 있다. 그러나 이와 더불어 유해한 정보 역시 손쉽게 얻을 수 있다는 단점이 있다. 특히 가치관이 아직 명확히 확립되지 않은 청소년들에게 무분별한 유해정보의 유출은 그릇된 가치관의 형성과 더불어 범죄에 영향을 미칠 수 있다. 현재 시중에는 무분별한 유해정보의 확산을 막기 위해 다양한 유해정보 차단 S/W가 출시되어 판매되고 있다. 그러나 현 유해정보 차단 S/W는 기술적 한계로 인해 유해정보의 완벽한 차단을 구현하지 못하고 있으며, 차단기능에 대한 다양한 우회방법 또한 존재한다. 본 논문은 이러한 유해정보 차단 S/W의 차단효과를 분석하고 한계점을 지적한다. 그리고 나아가 기존 유해정보 차단 S/W의 한계점을 극복한 새로운 유해정보 차단 S/W의 요구사항을 도출한다.

키워드 : 유해정보 차단, 유해정보 차단 S/W

Improvement of Internet Content Filtering Software

Woongryul Jeon[†] · Hyunseung Lee[††] · Soonhang Hur[††] · Kyungsin Kim[†††] · Dongho Won[††††] · Seungjoo Kim[†††††]

ABSTRACT

The openness of the Web allows any user to access any type of information easily at any time and anywhere. However, with function of easy access for useful information, internet has dysfunctions of providing users with harmful contents indiscriminately. Some information, such as adult content, is not appropriate for children. To protect children from these harmful contents, many filtering softwares are developed. However, these softwares can not prevent harmful contents, perfectly, because of some limitations. In this paper, we analyze existing eleven filtering softwares and state the limitation of these softwares. Furthermore, we propose requirements for new filtering software which overcomes the limitations, and describe framework of the new software..

Keywords : Filtering Software, Adult Content

1. 서 론

초고속 인터넷망의 활발한 보급과 컴퓨터의 대중화로 인해 인터넷은 이제 일상생활에서 없어서는 안될 필수요소가 되었다. 도서관에 들러 두꺼운 책을 찾아보거나 주위 여러 사람에게 질문을 하며 정보를 얻었던 과거에 비해 지금은 인터넷을 사용하여 전 세계에 걸쳐 다양한 정보를 손쉽게 획득할 수 있다. 그러나 이와 더불어 유해한 정보 역시 손쉽게 얻을 수 있다는 단점 또한 무시할 수 없다. 특히 가치관이 아직 명확히 확립되지 않은 청소년들에게 무분별한 유해정보의 유출은 그릇된 가치관의 형성과 더불어 범죄에 영향을 미칠 수 있다.

실례로 4월말 대구의 한 초등학교에서 음란물에 노출된 학생들이 상당기간 집단 성폭력을 일삼은 사건이 발생하여 사회 전반에 큰 파장을 몰고 왔다. 심지어 가해자인 초등학생들은 지난해 11월부터 동성 아이들 간의 성추행을 시작으로 고학년 학생들이 저학년 학생들을 성적으로 학대하거나 여학생을 집단 성폭행하는 등 학교 폭력과 결합된 성폭력이 5개월 동안 지속되어 왔음이 드러나 충격을 주었다. 조사결과 초등학생들은 쉽게 접할 수 있는 성인사이트를 통해 음란 정보를 습득하였으며, 이러한 행위를 놀이 정도로 생각하고 실천에 옮겼다고 한다. 이처럼 인터넷을 통한 무분별한 정보의 확산은 청소년의 가치관 형성에 지대한 영향을 미칠 수 있으며, 범죄로 이어질 가능성을 내포하고 있다.

현재 시중에는 무분별한 유해정보의 유출을 막기 위해 다양한 유해정보 차단 S/W가 출시되어 판매되고 있다. 그러나 유해정보 차단 S/W의 기술적 한계로 인해 유해정보의 완벽한 차단이 어렵고, 차단기능에 대한 다양한 우회방법 또한 존재한다. 본 논문은 유해정보 차단 S/W의 한계점을

※ 본 연구는 교육과학기술부의 '유해인터넷 차단 S/W 개발관련 사전 기초조사 연구'의 연구결과로 수행되었음
† 준 회 원 : 성균관대학교 전자전기컴퓨터공학과 박사과정
†† 준 회 원 : 성균관대학교 전자전기컴퓨터공학과 석사과정
††† 정 회 원 : 인덕대학교 인터넷 TV 방송과 교수
†††† 종신회원 : 성균관대학교 정보통신공학부 교수
††††† 종신회원 : 성균관대학교 정보통신공학부 교수(교신저자)
논문접수 : 2009년 1월 9일
수 정 일 : 1차 2009년 5월 12일
심사완료 : 2009년 5월 12일

확인하고 이를 개선하기 위해 유해정보 차단 S/W의 차단기능을 분석한다. 그리고 기존 유해정보 차단 S/W의 문제점을 극복한 새로운 유해정보 차단 S/W의 요구사항을 도출한다.

본 논문의 구성은 다음과 같다. 2장에서는 청소년 유해정보를 정의하고 3장에서는 국내 11개 유해정보 차단 S/W를 대상으로 유해정보 차단기능을 분석한다. 그리고 현 유해정보 차단 S/W의 문제점과 우회방법에 대해 설명한다. 4장에서는 3장의 분석결과를 바탕으로 유해정보 차단 S/W를 개선하기 위해 유해정보 차단 S/W의 필수기능을 도출하고 프레임워크를 제안한다. 마지막으로 5장에서 결론을 서술한다.

2. 청소년 인터넷 유해정보[1]

유해정보 차단 S/W는 청소년을 대상으로 유해정보에 대한 접근을 막는 것을 목적으로 한다. 정보의 유무해에 관한 판단기준은 세계 각국이 국내 실정에 맞춰 다양한 기준을 보유하고 있으며, 국내의 경우 현 방송통신심의위원회(구 정보통신윤리위원회)의 인터넷내용등급서비스(SafeNet)를 기반으로 하고 있다. 즉, 국내에 출시되는 유해정보 차단 S/W의 경우 인터넷내용등급서비스를 기반으로 정보의 유무해를 판별하고 차단 여부를 결정한다. 아래 <표 1>은 인터넷내용등급서비스의 등급기준을 나타낸다.

인터넷내용등급서비스는 위와 같은 등급을 바탕으로 각 연령에 적합한 등급을 정의하고 있다. 아래 <표 2>는 인터넷내용등급서비스가 정의하고 있는 연령별 권장사항이다.

즉, 국내 유해정보 차단 S/W가 청소년 유해정보를 분류하는 기준은 인터넷내용등급서비스 기준 18세 이상 정보로 노출과 성행위의 경우 3등급 이상, 폭력과 언어의 경우 4등급으로 분류된 정보를 의미한다.

〈표 1〉 SafeNet 등급 기준

	노출	성행위	폭력	언어	기타
4등급	성기노출	성범죄 또는 노골적인 성행위	잔인한 살해	노골적이고 외설적인 비속어	• 마약사용조장 • 무기사용조장 • 도박 • 음주조장 • 흡연조장
3등급	전신노출	노골적이지 않은 성행위	살해	심한 비속어	
2등급	부분노출	착의 상태의 성적 접촉	상해	거친 비속어	
1등급	노출복장	격렬한 키스	격투	일상 비속어	
0등급	노출없음	성행위 없음	폭력 없음	비속어 없음	

〈표 2〉 SafeNet 등급 기준에 대한 연령별 권장사항

구 분	노출	성행위	폭력	언어
전체가(초등학생 가)	1등급	0등급	1등급	0등급
12세 이상(중학생 가)	2등급	2등급	2등급	1등급
15세 이상(고등학생 가)	2등급	2등급	3등급	2등급
18세 이상(성인 가)	3등급	3등급	4등급	4등급

3. 유해정보 차단 S/W

본 장에서는 유해정보 차단 S/W의 차단기능을 분석하고 현 유해정보 차단 S/W의 한계점을 지적한다. 또 유해정보 차단 S/W의 우회방법에 대해 설명한다.

현재 시중에는 다양한 종류의 유해정보 차단 S/W가 출시되어 판매되고 있다. 본 논문은 유해정보 차단 S/W의 차단기능을 조사하기 위해 총 11개의 S/W를 선정하였다. 11개의 S/W는 인터넷내용등급서비스 홈페이지에서 소개하고 있는 S/W 7개와 국내 주요 포털사이트 등을 통해 선정한 인지도가 높은 4개의 S/W로 구성되었다. 아래 <표 3>은 11개의 유해정보 차단 S/W와 주요 기능을 나타낸다.

선정한 11개의 유해정보 차단 S/W가 구현하고 있는 기능 중 유해정보 차단과 관련이 있는 기능은 크게 유해사이트 차단기능, 유해동영상 차단기능, 그리고 유해파일 검색기능이다. 11개의 S/W는 모두 공통적으로 유해사이트 차단기능을 구현하고 있으며, 일부 S/W의 경우 유해동영상 차단기능과 유해파일 검색기능을 구현하고 있다. 아래 <표 4>는 11개 유해정보 차단 S/W가 구현하고 있는 유해정보 차단기능을 나타낸다.

〈표 3〉 포털 사이트 검색을 통해 선정한 유해정보 차단 S/W

유해정보 차단 S/W	S/W 별 주요 기능
엑스키퍼	유해동영상 차단/유해사이트 차단/컴퓨터중독방지
그린웨어	유해사이트 차단/게임 및 음란물 차단
텔레키퍼	유해사이트 차단/게임 및 음란물 차단/휴대폰을 사용한 원격제어
e-클린	인터넷 중독 방지/유해가능 파일 검사/통계보기
웹클린	유해사이트 선별차단/자녀컴퓨터관리
수호천사 i+	인터넷 중독 방지/P2P 차단/임의삭제 방지
지키미	유해사이트 차단/자동설치/사용시간 조절
맘아이	유해 및 음란사이트 접속 차단/게임 사용시간 제한/음란 동영상/P2P 차단
컴사용지킴이	컴퓨터 사용시간 관리/유해인터넷 차단/유해동영상 차단
해피모션	유해사이트 차단/게임 차단/컴퓨터 사용시간 관리
아이컴	유해사이트 차단/게임 차단/컴퓨터 사용시간 관리

〈표 4〉 유해정보 S/W의 유해정보 차단기능

S/W 이름	개발사	유해정보 차단기능		
		유해사이트 차단	유해동영상차단	유해파일 검색
엑스키퍼	㈜지란지교소프트	○	○	○
그린웨어	네티모	○	×	×
e클린	보안연구소	○	×	○
텔레키퍼	로직플렌트	○	×	×
웹클린	넷피아	○	×	×
수호천사i+	플러스기술㈜	○	×	×
지키미	이노비안㈜	○	×	×
맘아이	㈜제이니스	○	○	○
컴사용지킴이	테라정보통신	○	○	○
해피모션	㈜휴모션	○	×	×
아이컴	아이컴소프트	○	×	○

3.1 유해정보 차단 S/W 차단기능

앞서 언급한 바와 같이 유해정보 차단 S/W가 구현하고 있는 유해정보 차단기능은 크게 유해사이트 차단기능, 유해동영상 차단기능, 그리고 유해파일 검색기능이다. 본 절에서는 11개 유해정보 차단 S/W에 대해 세 가지 차단기능의 차단효과를 분석하고 한계점을 설명한다. 차단효과 분석의 신뢰성을 확보하기 위해 본 논문은 통계적 접근방법을 사용하였다. 일반적으로 모집단의 크기가 알려져 있고, 신뢰도와 오차범위를 결정하면 실험에 필요한 표본의 개수를 공식을 통해 구할 수 있다. 본 논문은 신뢰도를 90%, 오차범위를 5%로 결정하고 모집단의 크기를 통해 표본의 개수를 결정하였다. 아래 <표 5>는 신뢰도 90%, 오차범위 5%에서 표본의 크기를 나타낸다.

유해파일 검색기능의 경우 유해사이트 차단기능이나 유해동영상 차단기능과는 달리 컴퓨터에 저장된 전체 유해파일 중 몇 퍼센트를 검색할 수 있는가를 시험하는 것이 목적이기 때문에 표본의 크기 선정에 있어 통계적인 접근방법을 택하지 않았다.

유해사이트는 인터넷 검색을 통해 국내외 유해사이트 270개를 무작위로 선정하였다. 유해동영상은 총 271개를 수집하였으며, 확장자별로 구분하여 실험을 진행하였다. 차단효과 분석 실험은 유해정보 차단 S/W의 데이터베이스를 최신으로 업데이트 한 후 진행하였으며, 상세한 실험환경은 아래 <표 6>과 같다.

〈표 5〉 유해정보 차단효과 시험데이터 수집 방법

분석 대상 기능	시험데이터 수집 방법
유해사이트 차단	• 전 세계 유해사이트 68만개(한겨레신문 2003.04.27) → 모집단의 크기 68만개 • 신뢰도 90%, 오차범위 5% 내에서 표본 270개 필요. → 국내외 유해사이트 270개 수집
유해동영상 차단	• 전 세계 유해동영상 200만개 이상 (대덕이노폴리스벤처협회 2008.06.25) → 모집단의 크기 200만개 • 신뢰도 90%, 오차범위 5% 내에서 표본 270개 필요. → 유해동영상 271개 수집
유해파일 검색	• 유해파일을 텍스트, 이미지, 동영상 형태로 구분하여 수집 • 동영상은 유해동영상 차단을 위해 수집한 데이터를 활용

〈표 6〉 차단기능 분석 시험환경

조사일시	2008년 09월 25일			
조사대상 S/W 버전	엑스키퍼	8092200	지키미	1.65
	그린웨어	1.2.0.5	맘아이	08.09.25일자
	e클린	2.0	컴사용지킴이	2.3.30
	텔레키퍼	1.5 (build 0.72)	해피모션	08.09.25일자
	웹클린	2.6	아이컴	7.95
	수호천사 i+	08.09.25일자		
조사환경	운영체제	Microsoft Windows XP Service Pack 3		
	웹브라우저	Microsoft Explorer 7		

3.1.1 유해정보 차단기능 분석

본 절에서는 유해사이트 차단기능, 유해동영상 차단기능, 그리고 유해파일 검색기능에 대한 실험결과를 기술한다. 아래 <표 7>은 유해정보 차단기능 실험결과를 나타낸다.

유해동영상은 성인 이상 가와 불법 영상으로 구분하여 실험하였다. 성인 이상 가는 인터넷내용등급서비스 기준 18세 이상 가에 해당하는 동영상이고 불법 영상은 인터넷내용등급서비스 기준 성행위와 노출이 4등급에 해당하는 동영상이다. 예를 들어 시중에 합법적으로 유통되는 에로 비디오의 경우 18세 이상 가에 해당하며 불법적으로 유통되는 포르노의 경우 불법 영상에 해당한다. 유해파일은 텍스트파일, 이미지파일, 동영상파일로 구분하여 실험을 진행하였다.

또, 무해사이트의 차단여부를 확인하기 위해 20개의 무해사이트를 대상으로 실험을 진행하였다. 무해사이트 목록은 아래 표와 같다. 차단등급 설정은 18세 이상 가로 두고 하였으며, 실험결과 20개 무해사이트를 차단하는 S/W는 없었다.

〈표 7〉 차단효과 요약

제품명	유해사이트 차단	유해동영상 차단		유해파일 검색		
		성인 이상 가	불법 영상	텍스트 파일	이미지 파일	동영상 파일
엑스키퍼	80.74%	82.7%	97.5%	기능 없음	기능 없음	87.9%
그린웨어	17.41%	기능 없음	기능 없음	기능 없음	기능 없음	기능 없음
e클린	71.48%	기능 없음	기능 없음	0%	5.7%	0.3%
텔레키퍼	66.67%	기능 없음	기능 없음	기능 없음	기능 없음	기능 없음
웹클린	57.41%	기능 없음	기능 없음	기능 없음	기능 없음	기능 없음
수호천사i+	72.96%	기능 없음	기능 없음	기능 없음	기능 없음	기능 없음
지키미	82.96%	기능 없음	기능 없음	기능 없음	기능 없음	기능 없음
맘아이	74.07%	89.9%	76.9%	57.7%	5.7%	36.7%
컴사용지킴이	92.22%	46.7%	44.6%	기능 없음	100%	100%
해피모션	82.96%	기능 없음	기능 없음	기능 없음	기능 없음	기능 없음
아이컴	70.00%	기능 없음	기능 없음	6.0%	0%	0.5%

3.1.2 유해정보 차단기능 한계

유해사이트 차단기능은 11개의 S/W가 모두 제공하는 기능이다. 유해사이트 차단은 유해사이트 데이터베이스를 기반으로 하고 있다. 유해정보 차단 S/W가 서로 다른 데이터베이스에 기반을 두어 유해사이트를 차단하기 때문에 S/W별로 차단되는 유해사이트 목록이 상이하였으며, 데이터베이스 성능에 따라 유해사이트 차단성공률이 현저히 차이가 있다. 데이터베이스를 바탕으로 하는 유해사이트 차단기능은 근본적으로 데이터베이스에 등록되지 않은 유해사이트를 차단하지 못한다는 단점이 있다. 이를 극복하기 위해서는 데이터베이스를 상시 최신의 상태를 유지할 수 있도록 지속적으로 업데이트 해야 한다. 그러나 급격히 증가하는 유해사이트를 모두 데이터베이스에 등록하는 것은 현실적으로 불가능하기 때문에 기존 데이터베이스를 기반으로 하고 있

는 유해사이트 차단기능은 100% 차단을 장담할 수 없다. 그 예로 첫째, 최근 웹 2.0 시대를 맞아 정보생산의 주체로 급부상하고 있는 개인블로그, 카페 등 커뮤니티 사이트를 들 수 있다. 실험결과 자살과 관련한 경험담을 수록하고 있는 개인블록, 개인의 성생활에 관한 노골적인 묘사와 경험담을 포함하고 있는 개인블로그, 폭발물 등 위험물질 제조방법을 상세히 소개하고 있는 카페 등의 웹사이트는 데이터베이스에 등록이 되어 있지 않아 차단되지 않았다. 유해사이트를 제외하고도 수십만개에 달하는 이러한 웹사이트를 일일이 검색하고 데이터베이스에 등록하는 것은 현실적으로 불가능하다. 또 블로그나 카페의 경우 생성과 폐쇄가 기존 웹사이트보다 더 자유롭기 때문에 차단이 어렵다. 둘째, 차단이 되는 유해사이트라해도 다양한 도메인을 통해 접근이 가능하였다. http://sora.net은 대표적인 국내 음란사이트로 대부분의 유해정보 차단 S/W가 접근을 차단하였으나, 다른 도메인, http://tosora.info를 통해 접근이 가능하였다. 이러한 맹점을 활용, 국내 대부분의 유명 유해사이트는 다양한 도메인을 확보하여 차단기능을 회피하고 있다.

또 유해정보 차단 S/W의 구현상 문제로 인해 웹브라우저별로 유해사이트 차단기능의 동작여부에 차이가 발생하였다. 본 논문에서 실험은 마이크로소프트사의 인터넷 익스플로러 버전 7을 기준으로 진행하였는데, 익스플로러 버전 7에서 새로 추가된 기능, 새탭으로 열기를 사용하여 웹사이트에 접근할 때, 유해사이트 차단기능이 동작하지 않는 경우가 있었다. 그 외 모질라의 파이어폭스 버전 3.0, 구글 크롬 버전 0.2를 사용하여 웹사이트에 접근할 때에도 11개의 유해정보 차단 S/W 중 유해사이트 차단기능이 동작하지 않는 S/W가 있었다. 아래 <표 8>은 웹브라우저별 유해사이트 차단기능의 동작여부를 나타낸다.

유해동영상 차단기능은 엑스키퍼, 컴사용지킴이, 맘아이 3개의 S/W가 제공하고 있다. 이 중 엑스키퍼와 맘아이는 동영상의 내용을 바탕으로 동영상의 유무해를 판별하고 차단여부를 결정하며, 컴사용지킴이는 동영상의 파일명을 기반으로 유무해를 판별하고 차단하는 차이가 있다. 그러나 내용을 바탕으로 한 유해동영상 차단기능 역시 데이터베이스에 의존하고 있다. 단지 데이터베이스를 구축할 때 유해동영상의 내용을 나타내는 특정값을 사용할 뿐이다. 따라서 현재의 유해동영상 차단기능 역시 유해사이트 차단기능과 동일한 한계점을 나타내었다. 엑스키퍼의 경우 유해동영상 차단기능에서 뛰어난 성능을 나타내었으나 데이터베이스에 등록되지 않은 동영상은 차단하지 못하였다. 이는 유해사이트 차단기능과 마찬가지로 유해동영상 차단기능 역시 차단효과를 높이기 위해서는 지속적으로 데이터베이스를 업데이트 해야하며, 현실적으로 100% 완벽한 차단은 어렵다는 것을 의미한다. 파일명을 기반으로 하는 컴사용지킴이의 경우 차단이 되는 유해동영상의 파일명을 수정하면 간단히 차단기능을 피할 수 있었다. 또 내용을 기반으로 하는 엑스키퍼와 맘아이 역시 차단이 되는 유해동영상의 형식을 인코딩을 통해 변경한 경우 차단효과가 급격히 저하되었다.

〈표 8〉 무해사이트 20개 목록

웹사이트 주소	설명
http://www.amazon.com	인터넷 서점
http://www.aol.com	미국 포털 사이트
http://www.apple.com	미국 제조회사(컴퓨터부문)
http://www.blizzard.com	미국 제조회사(게임부문)
http://www.cnn.com	미국 뉴스사이트
http://www.cyworld.co.kr	국내 커뮤니티 사이트
http://www.daum.net	국내 포털 사이트
http://www.empas.com	국내 포털 사이트
http://www.epost.go.kr	국내 관공서
http://www.harvard.edu	국외 교육기관(하버드 대학교)
http://www.kbs.co.kr/	국내 방송사
http://www.kcc.go.kr	국내 관공서
http://www.korea.com/	국내 포털 사이트
http://www.mest.go.kr	국내 관공서
http://www.naver.com	국내 포털 사이트
http://www.nba.com	국외 스포츠 사이트
http://www.ox.ac.uk	국외 교육기관(옥스퍼드 대학교)
http://www.whitehouse.gov	국외 관공서(백악관)
http://www.yahoo.co.kr	국내 포털 사이트
http://www.microsoft.com	국외 제조회사(컴퓨터부문)

유해파일 검색기능은 엑스키퍼, 맘아이, 아이컴, e클린, 컴사용지킴이 총 5개의 S/W가 제공하고 있다. 유해파일 검색기능은 파일의 내용을 바탕으로 유무해를 결정하고 검출해내는 방법과 파일의 확장자를 기반으로 해당하는 모든 파일을 검색하는 방법으로 구분할 수 있다. 그러나 실험결과 파일의 내용을 바탕으로 유무해를 결정하고 검출해내는 S/W는 성능이 아주 미약하였다. 단, 엑스키퍼는 예외적으로 유해파일 검색기능이 아주 우수하였으나, 동영상 형식의 파일에만 제한되는 단점이 있었다. 컴사용지킴이는 100% 검색효과를 나타내었으나 이는 확장자를 기반으로 한 검색기능으로 사용자가 검색된 파일을 대상으로 일일이 유무해를 직접 확인해야 하는 단점이 있다.

일부 유해정보 차단 S/W는 간단한 시스템 조작이나 프로그램을 사용하여 유해정보 차단 S/W의 차단기능을 우회할 수 있었다. 우회방법은 크게 두 가지로 구분할 수 있다. 아래 <표 9>는 우회방법을 나타낸다.

윈도우 운영체제는 작업관리자를 통해 사용자가 직접 현재 시스템에서 동작중인 프로세스를 관리할 수 있다. 여기에는 프로세스 강제 종료기능도 포함되어 있는데 이를 사용하여 유해정보 차단 S/W를 강제로 종료할 수 있다. 레지스트리 편집을 이용한 유해정보 차단 S/W 우회방법은 유해정보 차단 S/W가 시작프로그램임을 이용한 것이다. 레지스트리는 윈도우 운영체제가 시작과 동시에 실행되어야 하는 프로그램 목록을 포함하고 있는데 시스템 구성 유틸리티나 레지스트리 편집기를 통해 수정이 가능하다. 따라서 레지스트리 편집을 통해 시작 프로그램 목록에서 유해정보 차단 S/W를 삭제하면 시스템이 가동될 때, 유해정보 차단 S/W가 실행되지 않고 유해정보 차단 또한 불가능하게 된다. 시스템 시간정보 변경을 통한 유해정보 차단 S/W는 유료로 제공되는 유해정보 차단 S/W의 경우 시간 단위로 결제가 되며, 결제한 기간 동안만 동작한다는 것을 이용한 방법이다.

〈표 9〉 웹 브라우저 환경 별 유해사이트 차단 기능의 한계점

S/W 이름	웹 브라우저 환경		
	익스플로러 7 새탭	파이어폭스 3.0	구글 크롬 0.2
엑스키퍼	차단	차단	차단
그린웨어	차단	차단 불가	차단 불가
e클린	차단	차단 불가	차단 불가
텔레키퍼	차단 불가	차단 불가	차단 불가
웹클린	차단	차단 불가	차단 불가
수호천사i+	차단	차단	차단
지키미	차단	차단 불가	차단 불가
맘아이	차단	차단	차단
컴사용지킴이	차단	차단	차단
해피모션	차단	차단 불가	차단 불가
아이컴	차단 불가	차단 불가	차단 불가

따라서 시스템 시간을 1970년 등으로 변경하면 결제한 기간이 아니기 때문에 유해정보 차단 S/W가 동작하지 않는다.

우회 프로그램을 사용한 유해정보 차단 S/W 우회방법은 세 가지로 구분할 수 있다. 첫 번째 방법은 앞서 언급한 작업관리자와 비슷한 역할을 하는 컴퓨터 관리 S/W를 사용하는 방법이다. 예를 들어 클릭 투 트윅이라는 프로그램은 악성코드 제거 및 시스템 최적화를 제공하는 프로그램으로 프로그램 제한기능이라는 기능을 포함하고 있다. 본 기능을 사용하여 유해정보 차단 S/W를 제한목록에 등록시켜놓으면 유해정보 차단 S/W가 동작하는 것을 막을 수 있다. 엑스키퍼의 경우 엑스키퍼에 특화된 우회프로그램이 존재한다. X-keeper bypass라는 프로그램은 관리자 패스워드를 무력화하는 프로그램으로 X-keeper bypass라는 프로그램이 실행되고 있을 때에는 관리자 로그인 창에 어떠한 값을 넣어도 비밀번호 인증에 성공을 한다. 이를 통해 엑스키퍼의 우회기능을 관리자가 아닌 사용자가 임의로 차단을 할 수 있다. 마지막으로 키보드 해킹 프로그램을 사용하는 방법이 있다. 현재 다양한 종류의 키보드 해킹 프로그램이 인터넷에 공개되어 있는데 이를 사용하면 사용자의 키보드 입력을 텍스트 파일에 저장할 수 있다. 이를 통해 관리자 비밀번호를 알아내면 역시 유해정보 차단 S/W의 차단기능을 우회할 수 있다. 아래 <표 10>은 언급한 우회방법을 11개 유해정보 차단 S/W를 대상으로 실험한 결과를 나타낸다. 기존 시스템 조작을 통한 유해정보 차단 S/W 우회방법은 현재 대부분의 S/W가 방지하고 있었으나 우회 프로그램을 사용한 우회에는 여전히 취약함을 나타내었다.

〈표 10〉 유해정보 차단 S/W 우회방법

유해정보 차단 S/W 우회방법		설명
시스템 조작	작업관리자 이용	작업관리자를 이용하여 유해정보 차단 S/W의 프로세스를 종료시킴
	레지스트리 편집	레지스트리를 편집하여 시스템 부팅 시 유해정보 차단 S/W가 실행되지 않도록 함
	시스템 시간 변경	시스템의 시간정보를 변경하여 유해정보 차단 S/W가 동작하지 않도록 함
우회 프로그램 사용	일반 우회 프로그램 사용	클릭 투 트윅"이라는 컴퓨터 관리 프로그램을 사용하여 유해정보 차단 S/W를 종료시킴
	특정 우회 프로그램 사용	엑스키퍼의 패스워드를 무시하는 "X-keeper Bypass"를 사용하여 관리자 패스워드를 무시하고 로그인
	키보드 해킹 프로그램 사용	인터넷에 공개되어있는 키보드 해킹 프로그램을 사용하여 관리자가 비밀번호를 입력할 때 관리자 비밀번호를 알아냄

〈표 11〉 유해정보 차단 S/W 우회방법

S/W 명	시스템 조작			우회 프로그램 사용		
	작업관리자 사용	레지스트리 편집	시스템 시간 변경	일반 우회프로그램	키보드 해킹 프로그램	특정 우회프로그램
엑스키퍼	불가능	불가능	불가능	불가능	가능	가능
그린웨어	가능	가능	해당사항없음 (무료 S/W)	가능	가능	해당사항 없음
e클린	불가능	불가능	불가능	가능	가능	해당사항 없음
텔레키퍼	불가능	불가능	불가능	불가능	불가능	해당사항 없음
웹클린	불가능	불가능	해당사항없음 (무료 S/W)	불가능	가능	해당사항 없음
수호천사 i+	불가능	불가능	불가능	가능	가능	해당사항 없음
지키미	불가능	불가능	불가능	가능	가능	해당사항 없음
맘아이	불가능	불가능	불가능	불가능	불가능	해당사항 없음
컴사용지킴이	불가능	불가능	불가능	불가능	가능	해당사항 없음
해피모션	불가능	불가능	불가능	불가능	가능	해당사항 없음
아이컴	불가능	불가능	불가능	불가능	가능	해당사항 없음

4. 유해정보 차단 S/W 필요기능 도출

본 장에서는 3장에서 분석한 유해정보 차단 S/W의 한계를 바탕으로 새로운 유해정보 차단 S/W가 지녀야 할 필요기능을 도출한다. 필요기능 도출에 앞서 3장에서 분석한 기존 유해정보 차단 S/W의 한계점을 요약하면 아래와 같다.

유해사이트 차단기능의 경우 데이터베이스에 등록되어 있지 않은 사이트는 차단할 수 없었다. 이는 어떤 유해사이트가 여러 도메인을 확보하고 있는 경우, 데이터베이스에 모든 도메인이 등록되어 있지 않으면 해당 유해사이트를 차단할 수 없다는 뜻이다. 국내 주요 유해사이트가 여러 도메인을 확보하고 있다는 점을 감안할 때 이는 효과적인 유해사이트 차단 방식이 될 수 없다. 실례로 앞서 언급한 바와 같이 http://sora.net/와 http://tosora..info/는 동일한 사이트임에도 불구하고 널리 알려진 도메인 http://sora.net/만 차단이 되는 경우가 있다. 또, 하루에도 엄청난 개수로 증가하는 유해사이트 생성 속도를 데이터베이스 업데이트로는 만회하기가 어렵기 때문에 데이터베이스를 사용한 유해사이트 차단 기능은 사후약방문격이 될 수밖에 없다. 그 외에도 최근 정

〈표 12〉 기존 S/W 차단기능의 한계

기 능	한 계
유해사이트 차단	• 11개 S/W 모두 유해사이트 차단기능 제공 • 데이터베이스 업데이트의 한계로 인해 다양한 경로를 가지는 유해사이트의 경우 일부 경로만 차단 • 개인블로그, 카페 등 커뮤니티 사이트에 대한 차단효과 미비 • 웹브라우저 종류에 따라 차단기능이 동작하지 않을 수 있음
유해동영상 차단	• 11개 S/W 중 3개만 유해동영상 차단기능을 제공 • 파일명을 기반으로 유해동영상을 차단하는 경우 유해동영상의 파일명 변경으로 차단을 피할 수 있기 때문에 사실상 차단효과가 없음 • 내용을 기반으로 유해동영상을 차단하는 기능 역시 유해사이트 차단기능과 마찬가지로 데이터베이스에 의존하는 차단방식이기 때문에 유해동영상의 형식을 변경함으로써 차단기능을 우회할 수 있음
유해파일 검색	• 11개 S/W중 5개가 유해파일 차단기능을 제공 • 유해파일을 텍스트, 이미지, 동영상으로 구분했을 때, 세 가지 유형의 검색을 모두 지원하는 S/W는 3개에 불과 • 검색기능은 S/W가 자체적으로 유무해를 판별하고 검색을 하는 경우와 모든 파일을 검색하는 경우로 구분 • S/W가 자체적으로 유무해를 판별하는 경우 조사결과 검색능력이 미약함(엑스키퍼의 경우 동영상 검색만 제공하지만 검색성능은 우수) • S/W가 확장자를 기반으로 모든 파일을 찾아주는 경우 사용자가 파일을 하나하나 일일이 확인하며 유해여부를 결정해야 하는 불편함

보의 생산지로 급부상하고 있는 개인블로그, 카페 등 커뮤니티 사이트의 경우 안전한 도메인으로 판단하기 때문에 기존 유해정보 차단 S/W는 적절한 차단효과를 나타내지 못했다.

유해동영상 차단기능은 11개의 S/W중 3개의 S/W만 구현하고 있었으며 그나마 차단효과가 뛰어난 제품은 1개에 불과하였다. 3개 중 하나의 제품은 파일명을 기반으로 유해사이트를 차단하기 때문에 파일명의 변경을 통해 손쉽게 차단기능을 우회할 수 있었고, 나머지 2개의 S/W는 유해동영상에서 해쉬값 등을 추출하여 데이터베이스를 구축하고 이를 바탕으로 차단여부를 결정하였는데, 이 역시 유해동영상의 형식을 변경함으로써 우회가 가능하였다. 그리고 유해이미지나 유해텍스트에 관해서는 차단기능이 현재로선 전무함을 확인하였다.

P2P나 웹하드를 통해 전송되는 파일형태의 유해정보는 웹사이트에 비해 높은 품질을 지닌다. 왜냐하면 웹사이트의 경우 외부 제약사항으로 인해 한정적인 서비스를 제공해야 하는 반면, P2P나 웹하드의 경우 초고속 인터넷의 발달과 컴퓨터 성능의 향상으로 대용량의 데이터를 빠르게 제공할 수 있기 때문이다. 또, 수많은 사람들이 참여할 수 있기 때문에 여러 유해사이트에서 나누어 얻을 수 있는 유해정보를 한곳에서 쉽게 얻을 수 있다는 특징이 있다. 2007년 조사결과에 의하면 P2P나 웹하드를 통한 유해정보의 접촉이 22.6%에 지나지 않지만 점차적으로 P2P나 웹하드의 사용이 빈번해질 것으로 추측되는 바, 이에 대비하여 유해동영상, 유해이미지, 유해텍스트에 대한 차단기능이 추가될 필요가 있다.

유해파일 검색기능은 유해정보 차단 S/W를 사용하는 부모에게 자녀가 어떠한 유해정보를 현재 컴퓨터에 저장하고 있는지 확인할 수 있는 도구가 된다. 그러나 현재 실험을 통해 확인된 사항을 요약하면 모든 파일을 검색하거나, 혹은 거의 검색하지 못하거나 둘 중의 하나이다. 모든 파일을 검색해내는 것은 운영체제가 지원하는 파일 검색기능을 사용하는 것과 다를 것이 없다. 이는 결국 부모가 하나하나 대상 파일을 확인하고 유무해를 결정해야 한다는 점에서 유해파일 검색 기능이라 부르기 어렵다. 반면 유해여부를 유해정보 차단 S/W가 결정하고 검색을 하는 방식은 유해동영상 차단 및 검출에 특화된 1개의 S/W를 제외하면 검색성능이 너무 미약한 것으로 드러났다.

4.1 유해정보 차단 S/W 요구사항 도출

지금까지 11개의 S/W를 대상으로 유해정보 차단효과 조사 결과와 그 한계점에 대해 지적하였다. 살펴본 바와 같이 현재의 유해정보 차단 S/W는 정보의 내용을 바탕으로 유해정보를 차단하는 것이 아니라, 정보의 메타데이터를 사용하여 데이터베이스를 구축하고 이를 바탕으로 유해정보를 차단하기 때문에 근본적으로 유해정보를 차단할 수 없는 한계점이 있었다. 이로 인해 3장에서 언급한 바와 같이 다수의 도메인을 소유하고 있는 유해사이트의 경우 완벽한 차단이 되지 않음을 확인하였다. 이에 본 절에서는 앞서 분석한 내용을 바탕으로 내용을 기반으로 유해정보를 차단할 수 있는 유해정보 차단 S/W의 기능 요구사항을 도출한다. 요구사항의 도출은 위협 도출, 위협을 제거하기 위한 요구사항 정립, 그리고 요구사항을 구현하기 위한 필요기능 도출의 3단계로 구성된다.

4.1.1 위협 도출

위협은 유해정보 차단 S/W 차단기능의 범위와 역할을 구분하고 결정하기 위한 첫 번째 단계이다. 위협은 사용자가 접촉할 수 있는 유해정보의 유형과 사용자가 유해정보를 접촉하는 경로에 따라 구분할 수 있다. 우선 사용자가 인터넷을 통해 접촉할 수 있는 유해정보는 아래 표와 같다.

사용자가 유해정보를 접촉할 수 있는 경로는 크게 온라인을 통한 접촉과 오프라인을 통한 접촉, 두 가지로 구분할 수 있다. 온라인을 통한 접촉은 유해사이트 방문을 통해 유해사이트에 포함된 유해정보를 접촉하는 형태와, P2P, 웹하드 등의 웹사이트나 메신저, 이메일 등을 통해 파일 형태의 유해정보를 다운로드 받는 형태로 구분할 수 있다. 오프라인을 통한 접촉은 2차 확산으로 주변 사람들을 통해 파일 형태의 유해정보를 접촉하는 것이다. 이를 바탕으로 사용자의 유해정보 접촉 경로를 정의한다.

첫 번째, 사용자는 온라인으로 유해사이트를 방문하여 유해사이트에 포함된 유해정보를 접촉할 수 있다. 이러한 정보의 유형에는 텍스트, 이미지, 동영상, 게임, 기타를 모두 포함한다. 그러나 유해사이트에 포함된 정보는 서버 용량의 한계로 인해 동영상이나 게임의 경우 데이터의 품질이 제한적이라는 특징을 지닌다.

〈표 13〉 인터넷 유해정보의 유형

구 분	종 류	사 례
텍스트	• 유해게시물 • 유해소설	• 인터넷게시판, 성인사이트 등에 게시된 성행위를 노골적으로 묘사한 소설 및 게시물 • 자살을 조장하는 사이트에 게시된 자살 경험담 • 폭발물 제조 방법
이미지	• 유해사진, 그림, 만화, 애플릿(움직이는 그림)	• 노골적인 노출 및 성행위를 묘사하고 있는 사진 • 잔혹한 살해 및 폭력성을 묘사하고 있는 사진 • 근친상간 등 음란하고 비정상적인 내용을 포함하고 있는 일본만화
동영상	• 실시간 동영상물 • 파일형 동영상물	• 노골적인 성행위 묘사 및 폭력성을 포함하고 있는 동영상
게 임	• 음란게임 • 폭력게임 • 사행성게임	• 퇴폐적인 내용의 일본 게임물 • 잔혹한 장면을 묘사하고 있는 게임물 • 실제 현금을 사용하는 사행성 온라인게임
기 타	• 음란대화 • 음란사이트 배너광고 • 음란물 판매 광고	• 채팅사이트를 사용한 음란채팅 • 캠을 이용한 성인채팅 • 성인웹사이트 배너광고

두 번째, 사용자는 온라인으로 파일 형태의 유해정보를 다운로드 받을 수 있다. 파일 형태의 유해정보 유형에는 텍스트, 이미지, 동영상, 게임이 있으며, P2P나 웹하드 등 면식이 없는 여러 명의 사용자가 자료를 공유하는 웹사이트를 방문하여 유해정보를 다운로드를 받는 경우와 메신저, 이메일 등 주변 사람들과의 일대일 접촉을 통해 유해정보를 다운로드 받는 경우로 구분할 수 있다.

세 번째, 사용자는 오프라인으로 파일 형태의 유해정보를 획득할 수 있다. 이는 USB, DVD 등 이동저장장치의 용량이 커지고 속도가 빨라지면서 가능해졌다. 유통될 수 있는 정보는 파일 형태의 텍스트, 이미지, 동영상, 게임이 있다. 오프라인을 통한 파일 형태의 유해정보 접촉은 이미 인터넷을 통해 획득한 유해정보의 2차적 확산으로 직접 인터넷을 통한 유해정보의 확산은 아니지만, 실제 현실에서 널리 이용되는 유해정보 확산 경로 중 하나이기 때문에 유해정보 차단 S/W가 간과해서는 안될 경로이다. 언급한 유해정보의 유형과 사용자가 유해정보를 접촉할 수 있는 경로를 바탕으로 위협을 정의하면 <표 14>와 같다.

〈표 14〉 인터넷 유해정보 접촉 위협

위 협		설 명
온라인	T1. 유해사이트 방문	• 사용자의 유해정보를 포함하고 있는 유해사이트를 방문하여 유해한 정보를 습득할 수 있다. • 유해사이트는 일반적으로 일컫는 유해사이트 외에도 개인블로그, 카페, 채팅사이트, 화상채팅 사이트 등 커뮤니티 사이트를 모두 포함한다. • 본 위협에서 습득할 수 있는 유해정보는 텍스트 형태, 이미지 형태, 동영상 형태, 게임 형태, 기타 배너 형태를 모두 포함하나 서버 용량에 따라 퀄리티가 제한적이다.
	T2. 유해정보다운로드	• 사용자는 P2P, 웹하드, 메신저, 이메일 등을 통해 파일 형태의 유해정보를 다운로드 받아 사용자 PC에서 실행할 수 있다. • 파일 형태의 유해정보는 텍스트, 이미지, 동영상, 게임의 형태를 포함하며 퀄리티가 우수한 대용량 유해정보 확산이 가능하다는 특징이 있다.
오프라인	T3.오프라인	• 사용자는 대용량 이동저장장치를 사용하여 파일 형태의 유해정보를 주변 지인으로부터 획득할 수 있다.
기타	T4.알려지지 않은경로	• 사용자는 알려지지 않은 경로를 통해 유해정보에 접촉할 수 있다.

4.1.2 요구사항 도출

위협을 바탕으로 유해정보 차단 S/W에 대한 기능 요구사항을 도출하면 다음과 같다.

첫째, 유해정보 차단 S/W는 유해사이트를 차단할 수 있어야 한다. 특히 유해사이트 차단기능은 웹브라우저의 종류에 관계없이 동작해야 한다. 또, 기존 데이터베이스 방식의 유해사이트 차단기능의 한계를 극복하기 위해 웹사이트의 내용을 기반으로 유해여부를 판별하는 기능도 함께 적용해야 한다. 내용을 기반으로 유해사이트의 유해여부를 판별할 때에는 웹사이트에 포함된 텍스트, 이미지, 동영상, 게임, 배너 등 모든 항목을 고려해야 한다.

둘째, 유해정보 차단 S/W는 유해파일을 차단할 수 있어야 한다. 유해파일은 텍스트, 이미지, 동영상 형태로 분류할 수 있으며 유해정보 차단 S/W는 각 형식별로 내용 기반 유해여부 판별 기능을 보유하고 있어야 한다. 파일 형태의 유해정보는 유해사이트에 포함되어 제공되는 유해정보와 달리 유해정보의 재사용, 재생산, 확산이 용이하기 때문에 반드시 추가되어야 한다.

셋째, 유해정보 차단 S/W는 프로그램 차단 기능을 제공해야 한다. 이는 게임 형태의 유해정보를 차단하고 메신저, 이메일 등을 통해 유해정보가 확산되는 것을 막기 위함이다. 여기서 지칭하는 게임은 온라인게임과 오프라인 게임을 모두 포함한다.

넷째, 유해정보 차단 S/W는 알려지지 않은 경로를 통한 유해정보 접촉을 차단하기 위해 감사기록을 생성해야 한다. 감사기록은 웹사이트 접근 기록, 파일 열람 기록, 프로그램 실행기록을 포함해야 한다. 특히 프로그램을 통한 유해정보 접촉 여부를 확인하기 위해 컴퓨터 화면을 주기적으로 저장하는 기능을 포함해야 한다. 왜냐하면 사용자 PC에서 실행하는 게임은 접근을 원천적으로 막기가 상당히 어렵기 때문이다. 온라인 게임은 기본적으로 웹사이트를 통해 접근해야 하기 때문에 해당 웹사이트를 차단하면 접근을 막을 수 있고, 또 웹사이트를 통해 접근하지 않는 게임이라 해도 프로그램이 컴퓨터에 설치되면 그 여부를 확인할 수 있다. 그러나 오프라인 게임의 경우 설치과정이 있는 게임과 설치과정이 없는 게임으로 구분할 수 있는데 설치과정이 있는 게임은 운영체제가 제공하는 프로그램 목록에서 존재여부를 확인할 수 있지만, 설치과정이 없는 게임은 운영체제에 등록되지 않기 때문에 존재여부를 파악하기가 힘들기 때문이다. 대표적

예로는 플래시로 제작한 게임을 들 수 있다. 플래시로 제작한 게임은 설치과정이 없고 실행파일을 통해 바로 동작하기 때문에 숨겨놓는 경우 확인하기가 어렵다. 따라서 이러한 프로그램의 실행을 확인하고 차단하기 위해서는 감사기록 생성 시 컴퓨터 화면도 저장하는 기능을 포함해야 한다.

다섯째, 유해정보 차단 S/W는 컴퓨터의 사용시간을 제한하는 기능을 제공해야 한다. 컴퓨터 사용 시간의 제한은 유해정보 접촉 확률을 낮출 수 있고, 청소년의 잠재적인 컴퓨터 중독 현상을 막기 위해 필요하다. 컴퓨터의 장시간 사용은 유해정보 접촉의 기회 증가를 초래할 수 있으며, 컴퓨터 중독은 일상생활에 영향을 미칠 수 있기 때문에 유해정보 차단 S/W는 컴퓨터 사용시간을 제한하는 기능을 제공해야 한다.

여섯째, 유해정보 차단 S/W는 유해정보 차단 우회를 방지하는 기능을 제공해야 한다. 시스템 조작이나 우회 프로그램 사용으로 유해정보 차단 S/W의 차단기능을 우회할 수 있기 때문에 이에 대한 대응책이 필요하다.

아래는 언급한 요구사항을 <표 15>로 정리한 것이다.

도출한 요구사항에 대한 근거는 <표 16>과 같다.

R1.유해사이트 차단 요구사항은 유해사이트에 대한 접근을 방지하기 위해 필요한 요구사항이다. R2.유해파일 차단과 R3.프로그램 실행차단은 텍스트, 이미지, 동영상 파일 형태의 유해콘텐츠와 유해게임을 차단하기 위한 요구사항이다. R4.감사기록 생성 요구사항은 알려지지 않은 경로를 통해 유해정보를 접촉했는지 여부를 확인하기 위해 필요하다. 특히 채팅사이트의 경우 대화내용의 실시간 감시가 어렵기 때문에 감사기록을 통해 내용을 확인하는 과정이 필요하다. R5.사용시간 제한 요구사항은 장시간 컴퓨터 사용을 방지하고 알려지지 않은 경로를 통한 유해정보 습득 여부를 차단하기 위해 필요하다. 또 잠재적으로 컴퓨터 사용시간을 억제함으로써 유해정보 접근 가능성을 낮추는 효과를 기대할 수 있다. R6.S/W 우회방지 요구사항은 우회 프로그램을 사용하여 유해정보 차단 S/W를 우회하려는 시도를 차단하기 위해 필요하다.

〈표 15〉 유해정보 차단 S/W 기능요구사항

요구사항	내 용
R1.유해사이트 차단	• 웹브라우저와 독립적인 유해사이트 차단 • 웹사이트 내용 기반 유해여부 결정기능 지원
R2.유해파일 차단	• 텍스트, 이미지, 동영상 형태의 유해콘텐츠 차단
R3.프로그램 실행차단	• 특정 프로그램의 실행 차단
R4.감사기록 생성	• 유해정보 접촉여부를 확인하기 위한 감사기록 생성 • 접근한 웹사이트, 접근한 파일, 실행한 프로그램 목록 그리고 컴퓨터 화면의 주기적인 저장기능 포함
R5.사용시간 제한	• 컴퓨터 사용시간 제한 기능
R6.S/W 우회방지	• 유해정보 차단 S/W 우회방지 기능

〈표 16〉 유해정보 차단 S/W 요구사항의 근거

	T1. 유해사이트 방문	T2. 유해파일 다운로드	T3. 오프라인	T4. 알려지지 않은경로
R1.유해사이트 차단	O	-	-	-
R2.유해파일 차단	-	O	O	-
R3.프로그램 실행차단	-	O	O	-
R4.감사기록 생성	-	-	-	O
R5.사용시간 제한	-	-	-	O
R6.S/W 우회방지	O	O	O	O

4.1.3 유해정보 차단 S/W 필요기능

앞선 절에서는 유해정보 차단 S/W가 갖추어야 할 요구사항을 도출하고 그 근거를 명시하였다. 본 절에서는 이를 바탕으로 유해정보 차단 S/W의 필요기능을 도출하고 그 근거를 설명한다.

<표 17>은 유해정보 차단 S/W가 갖추어야 할 필요기능과 기능에 대한 설명이다.

필요기능에 대한 근거와 설명은 아래와 같다.

원격제어 기능은 유해정보 차단 S/W의 관리자가 일반적으로 부모이며, 맞벌이 부부의 경우 관리자가 컴퓨터에 대한 물리적인 접근을 24시간 유지하기 어렵기 때문에 추가한 기능이다. 원격제어 기능을 통해 컴퓨터 사용시간 설정을

〈표 17〉 유해정보 차단 S/W 필요기능

기능	요구사항
유해사이트 차단기능	• 웹브라우저와 독립적으로 유해사이트 차단 • 유해사이트 목록 데이터베이스 기반 차단 및 유해사이트 내용 기반 차단 • 사용자가 지정한 유해사이트 차단 • 사용자가 지정한 단어 포함 사이트 차단
유해파일 차단기능	• 유해텍스트, 유해이미지, 유해동영상 차단기능 • 콘텐츠의 내용을 기반으로 유해여부 결정 및 차단
프로그램 차단기능	• 현재 컴퓨터에 설치된 프로그램 목록 제공 • 사용자가 프로그램 차단 여부 결정
감사기록 생성기능	• 월별, 주간별, 일별 감사기록 제공 • 접근한 웹사이트 기록 제공 • 접근한 파일 목록 제공 • 실행한 프로그램 목록 제공 • 주기적으로 컴퓨터 화면을 저장
관리자 알림기능	• 유해정보 접촉 시 SMS, 이메일 등을 통해 관리자에게 알림기능
사용시간 제한설정 기능	• 시간대별 컴퓨터 사용시간 설정 기능 • 하루 컴퓨터 사용 가능시간 설정 기능
유해정보 차단 S/W 보호	• 관리자 허가 없이 프로그램 삭제 불가 • 관리자 외 다른 사용자의 차단기능 설정 변경 불가
원격제어 기능	• 프로그램 사용 시간의 원격설정 기능 • 컴퓨터 잠금 기능의 원격설정 기능
유해정보 차단 S/W 우회방지 기능	• 키보드 해킹 방지 기능 • 작업관리자 사용, 레지스트리 편집, 시스템 시간 변경, DNS 변경 제한 기능 • 우회 프로그램 사용 제한 기능

〈표 18〉 유해정보 차단 S/W 필요기능의 근거

기능	R1	R2	R3	R4	R5	R6
유해사이트 차단기능	O	-	-	-	-	-
유해파일 차단기능	-	O	-	-	-	-
프로그램 차단기능	-	-	O	-	-	-
감사기록 생성기능	-	-	-	O	-	-
관리자 알림기능	-	-	-	O	-	-
사용시간 제한설정 기능	-	-	-	-	O	-
S/W 우회방지 기능	-	-	-	-	-	O
유해정보 차단 S/W 보호	-	-	-	-	-	O
원격제어 기능	-	-	-	-	O	-

변경할 수 있으며, 관리자 알림기능을 통해 유해정보 접촉이 확인된 경우 컴퓨터의 모니터를 잠그거나, 전원을 차단하는 등 즉각적인 조치가 가능하도록 한다.

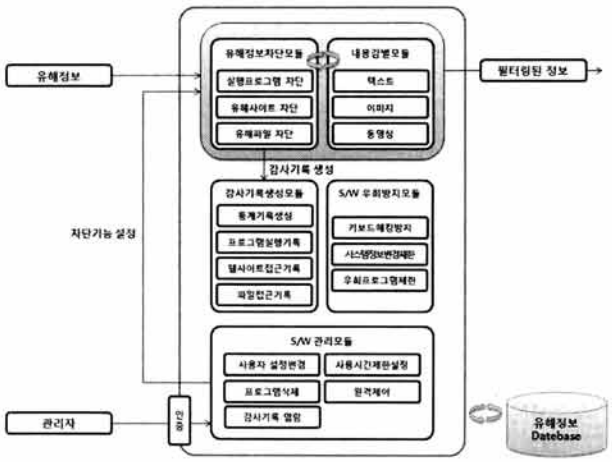
4.2 새로운 유해정보 차단 S/W 프레임워크

새로운 유해정보 차단 S/W는 기존 유해정보 차단 S/W와는 달리 내용 기반 유해정보 차단 기능을 제공한다. 내용기반 유해정보 차단기능은 텍스트 형태, 이미지 형태, 동영상 형태의 유해정보를 획득한 후 내용을 기반으로 유해여부를 판별한다. 아래 그림은 새로운 유해정보 차단 S/W의 프레임워크를 나타낸다.

유해정보 차단 S/W는 청소년으로부터 유해정보를 차단하는 것이 목적이다. 따라서 유해정보 차단 S/W는 일반적인 데스크탑을 사용하는 청소년을 공격자로 가정한다. 공격의 목적은 유해정보 차단기능을 우회하는 것이다. 유해정보 차단 S/W의 우회기능 활성화/비활성화는 관리자 인증을 통해 설정이 가능하다. 이 때 관리자 인증은 패스워드를 사용한 인증방법을 사용하며, 관리자 패스워드는 유해정보 차단 S/W가 보호해야 할 자산이다.

유해정보 차단 S/W는 PC의 부팅이 완료되면 차단기능이 활성화되어 자동으로 실행된다. 차단기능의 비활성화는 관리자만 가능하다. 관리자는 유해정보 차단 S/W의 S/W 설정 변경, 감사기록 열람 등이 가능하다. 관리자가 아닌 사용자는 유해정보 차단 S/W의 종료, 설정 변경이나 감사기록 확인 등이 불가능하며, 지정된 환경설정을 바탕으로 필터링된 정보만 습득할 수 있다.

새로운 유해정보 차단 S/W는 기존 데이터베이스 유해정보 차단기능과 내용 기반 유해정보 차단 기능을 함께 보유하고 있다. 만약 데이터베이스에 등록되지 않은 유해정보를 접촉하는 경우 내용 기반 유해정보 차단 기능을 바탕으로 정보의 유해여부를 결정하고 업데이트하여 추후 차단기능에 반영할 수 있다. (그림 1)에서 가장 핵심이 되는 모듈은 내용감별 모듈로 텍스트 분석 모듈과 이미지 분석 모듈 그리



(그림 1) 유해정보 차단 S/W 프레임워크

고 동영상 분석 모듈로 구성되어 있다. 내용감별 모듈이 식별하는 대상이 되는 형태는 웹사이트에 포함된 텍스트, 이미지, 동영상과 파일 형태의 텍스트, 이미지, 동영상을 모두 포함한다. 각 모듈에 대한 상세한 설명은 다음과 같다.

4.2.1 내용감별 모듈

내용감별 모듈은 내용을 기반으로 유해정보를 차단한다. 차단의 대상이 되는 유해정보는 웹사이트에 포함된 텍스트, 이미지, 동영상은 물론 파일 형태의 텍스트, 이미지, 동영상을 모두 포함한다. 내용을 기반으로 유해정보를 차단하기 위해서는 학습모듈을 적용해야 한다. 일반적으로 분류에 가장 널리 사용되는 학습모델은 90년대 중반에 등장한 SVM(Support Vector Machine) 모델이다. SVM 모델은 첫째, 명백한 이론적 근거에 기반하므로 결과 해석이 용이하고, 둘째, 실제 응용에 있어서 다른 모델에 비해 우수한 성능을 나타내며, 셋째, 적은 학습자료만으로도 신속하고 정확한 분별학습이 가능하다는 장점이 있다[5].

텍스트의 경우 전처리부에서는 유해어 판별과 관련없는 단어들을 제거하는 작업을 수행한다. 이때 문장부호, 조사, 등이 삭제된다. 또 자주 등장하는 단어지만 유해어가 아닌 단어들 역시 제거하면 추후 판별과정에서 성능 향상을 기대할 수 있다.

이미지의 경우 전처리부에서는 판별을 위해 이미지의 특징을 추출하는 과정을 거친다. 유해이미지를 판별하기 위해서는 우선 유해이미지와 무해이미지를 구분할 수 있는 특징을 선택하고 이를 추출하는 기술이 필요하다. 이러한 기술을 유해이미지 특징 추출 기술이라고 한다. 유해이미지 특징 추출 기술은 특징을 이미지의 정보에 따라 1세대, 2세대, 3세대로 구분할 수 있다. 1세대 유해이미지 특징 추출 기술은 이미지에서 피부색 영역을 찾은 후 피부색 영역의 크기와 전체 이미지에 대한 피부색 영역의 비율, 피부색 영역의 개수 등 피부색에 관한 정보만을 바탕으로 특징을 추출하는 기술을 의미한다. 2세대 유해이미지 특징 추출 기술은 이미지에서 피부색 영역 관련 정보뿐만 아니라, 이미지의 컬러, 형태, 질감 등 여러 가지 저수준 특징들을 함께 추출하는

〈표 19〉 내용 기반 유해정보 판별 과정

단 계	설 명	
전처리 단계	텍스트	· 입력된 문장을 분석하여 조사 등 유해어 판별과 관계없는 단어들을 분리 · "내가", "이제" 등 빈번하게 출현하는 유해어가 아닌 단어들을 따로 모아 데이터베이스화 함으로써 전처리과정의 속도를 높일 수 있음
	이미지	· 그래픽 이미지 분류, 프레임 제거, 얼굴 검출, 다중 영상 분리 방법 등 다양한 이미지 전처리 과정을 통해 이미지의 특징을 추출하기 위한 전처리 과정을 수행 · 전처리 과정을 거친 이미지를 대상으로 특징을 추출 · 특징 추출 방법에는 1세대, 2세대, 3세대로 구분할 수 있음
	동영상	· 동영상의 프레임만 바탕으로 유해여부를 결정하는 것은 신뢰도가 떨어지므로 동영상에서 일부 구간의 프레임을 추출 · 프레임 집합의 특징값 추출
판별 단계	텍스트	· 추출한 단어를 바탕으로 기계 학습 모델을 적용, 텍스트의 유해여부를 판별
	이미지	· 추출한 이미지의 특징을 바탕으로 기계 학습 모델을 적용, 이미지의 유해여부를 판별
	동영상	· 추출한 프레임 집합의 특징값을 바탕으로 프레임 집합의 유해여부를 판별
학습 단계	· 유해로 판정된 텍스트, 이미지, 동영상에 대해 학습 모델을 업데이트	

기술을 의미한다. 3세대 유해이미지 특징 추출 기술은 이미지의 컬러, 형태, 질감 등 저수준 특징들을 바탕으로 고수준 특징을 추출하는 기능을 의미한다. 고수준 특징은 이미지에 존재하는 객체의 자세 등이 있으며 객체의 자세가 어떤 의미를 지니는지 추론하여 유해여부를 판별하는 방식이다.

동영상의 경우 유해여부를 판별하기 위해선 동영상의 특징을 추출해야 한다. 동영상의 특징을 추출하는 방법에는 두 가지가 있다. 하나는 동영상의 정지영상, 즉 이미지를 사용하여 동영상의 특징을 추출하고 유해여부를 판별하는 방식이고 다른 하나는 동영상의 일부, 프레임 집합에 대해 특징을 추출하고 동영상의 유해여부를 판별하는 방식이다. 전처리부는 동영상의 일부분을 통해 특징을 추출하는 기능을 수행한다.

4.2.2 유해정보차단 모듈

유해정보차단 모듈은 웹사이트 프로그램, 그리고 파일에 대한 직접적인 차단기능 수행을 담당한다. 유해정보차단 모듈은 유해사이트 차단 모듈, 실행프로그램 차단 모듈, 유해파일 차단 모듈로 구성된다. 유해사이트 차단 모듈은 데이터베이스에 등록된 URL을 바탕으로 사이트를 차단하며, 데이터베이스에 등록되지 않은 웹사이트는 내용감별 모듈을 통해 유해여부를 판단한다. 만약 데이터베이스에 등록되지 않은 웹사이트가 내용감별 모듈에 의해 유해사이트로 판정되면 유해사이트 차단 모듈은 해당 웹사이트 열람을 즉시 차단하고 URL을 데이터베이스에 등록하여 업데이트한다. 유해사이트를 차단하는 기능은 웹브라우저에 독립적으로 동작해야 하며, 이를 위해서는 구현 시 URL 추출방법을 웹브라우저에 독립적인, 패킷에서 URL을 추출하는 방법을 사용해야 한다. 실행프로그램 차단 모듈은 운영체제를 통해 현재 실행 가능한 프로그램 목록을 사용자에게 제공하며, 사용자는 이를 바탕으로 프로그램의 실행여부를 결정할 수 있다. 유해파일 차단 모듈은 내용감별 모듈을 통해 실행하려는 파일의 유무해 여부를 판별하고 차단기능을 수행한다. 이 때 널리 사용되는 파일의 확장자 등을 통해 내용감별 모듈을 적용할 파일의 범위를 한정할 수 있다. 유해로 판별된 파일은 데이터베이스 특징값을 저장하여 추후 실행 시 차단 여부를 바로 결정할 수 있게 한다.

4.2.3 감사기록생성 모듈

감사기록생성 모듈은 차단범위에서 제외될 수 있는 유해정보를 추후 차단하기 위해 감사기록을 생성한다. 감사기록은 실행한 프로그램 목록, 접근한 웹사이트 목록, 그리고 실행한 파일 목록을 포함하며, 덧붙여 일정 시간 단위로 모니터 화면을 캡쳐하여 저장하는 기능을 보유하고 있다. 이는 차단기능이 감지하기 어려운 유해정보를 추후 차단하기 위해 필요한 기능이다. 실행프로그램의 경우 플래시로 제작된 성인게임은 설치과정이 없이 바로 실행되기 때문에 실행프로그램 차단 모듈이 감지할 수 없다. 따라서 이러한 프로그램은 사용자가 고의로 숨겨놓고 실행하는 경우 쉽게 감지할 수 없기 때문에 차단이 어렵다. 또, 웹사이트의 경우 채팅방에서 이루어지는 음란한 대화 등을 통한 유해정보 간접노출은 유해사이트 차단 모듈이 감지하고 차단하기가 어렵다. 유해파일 역시 성인만화책을 스캔한 그림파일의 경우 이미지가 단순한 흑백으로 구성되어 있고, 하나의 그림파일에 여러 컷이 등장하기 때문에 기존 이미지 특징추출 기술로는 유해여부를 판별하기가 어렵다. 감사기록생성 모듈은 이러한 유형의 유해정보를 차단하기 위해 실행한 프로그램 목록, 접근한 웹사이트 목록, 그리고 실행한 파일 목록과 함께 모니터 화면 캡쳐기능을 제공한다. 감사기록생성 모듈은 이와 같은 기능을 통해 알려지지 않은 경로를 통한 유해정보의 접촉을 차단할 수 있다.

4.2.4 S/W 관리모듈

유해정보 차단 S/W는 관리자 외에는 프로그램 삭제, 차단기능 설정 변경, 차단기능 활성화/비활성화 등이 불가능해야 한다. 이를 위해 S/W 관리모듈은 사용자 인증기능을 포함하고 있다. S/W 관리 모듈에 접근하기 위해서는 반드시 관리자 인증과정을 거쳐야 한다. 관리자 인증을 거친 사용자는 S/W 관리 모듈을 통해 유해정보 차단기능의 활성화/비활성화를 설정할 수 있다. 유해사이트 차단기능의 경우 사용자는 URL 뿐만 아니라 금칙어가 포함된 웹사이트 차단, 국가별 도메인 차단, 허용사이트만 접속가능 등을 설정할 수 있다. 실행 프로그램 차단기능의 경우 사용자는 운영체제로부터 제공받은 설치된 실행 프로그램 목록 외, 수동으로 실행파일을 검색하여 직접 실행되는 프로그램의 실행 역시 차단할 수 있다. 유해파일 차단기능의 경우 사용자는 특정 확장자, 금칙어 포함 파일명 등의 설정을 통해 다양한

〈표 20〉 내용 기반 유해정보 판별 과정

차단기능	기존 유해정보 차단 S/W의 한계점	새로운 유해정보 차단 S/W의 강점
유해사이트 차단기능	- 다수의 도메인을 가지는 유해사이트의 경우 데이터베이스에 등록되지 않은 도메인은 차단되지 않기 때문에 유해사이트에 대한 접근이 원천적으로 차단되지 않음	- 유해사이트 도메인이 아니라 유해사이트에 포함된 콘텐츠의 내용을 바탕으로 유해사이트를 차단하기 때문에 데이터베이스에 등록되지 않은 도메인이라 하더라도 차단이 가능함
	- 기존 유해사이트 차단 S/W의 경우 익스플로러에 초점을 맞추고 있기 때문에 파이어폭스, 크롬 등 기타 웹브라우저를 사용하여 유해사이트에 접근하는 경우 차단이 되지 않음	- 새로운 유해정보 차단 S/W는 웹브라우저에 독립적인 차단모듈 구현을 원칙으로 하고 있기 때문에 웹브라우저에 관계없이 유해사이트 차단이 가능함
유해동영상 차단기능	- 유해동영상의 동영상 형식을 변경하는 경우 동영상 차단이 되지 않음	- 유해동영상을 변경한다 하더라도 동영상의 프레임을 분석하고 내용을 바탕으로 유해여부를 판별하기 때문에 새로운 유해정보 차단 S/W는 형식을 변경한 유해동영상 역시 차단 가능

범주의 파일을 차단할 수 있다. S/W 관리모듈은 이밖에도 사용시간 제한 설정, 원격 제어 등을 통해 사용자 PC의 사용가능 시간대와 원격에서의 관리자 설정 변경을 지원한다. 사용시간 제한 설정은 컴퓨터 사용가능 시간, 인터넷 사용가능 시간으로 구분하여 제공하며, 하루 사용 가능량 또는 하루 사용가능 시간대를 설정할 수 있다. 원격제어 모듈은 원거리에서 컴퓨터 사용가능 여부와 사용가능 시간을 변경하는 기능을 제공하는데 이 때 반드시 관리자 인증을 거쳐야 한다. 관리자 인증은 패스워드를 사용하여 구현할 수 있다.

4.2.5 S/W 우회방지 모듈

앞서 3장에서 언급한 바와 같이 기존 유해정보 차단 S/W는 작업관리자를 통한 유해정보 차단 S/W 강제종료, 윈도우의 경우 레지스트리 편집을 통한 유해정보 차단 S/W 초기 실행 방지, 키보드 해킹을 사용한 유해정보 차단 S/W 관리자 비밀번호 획득 등 다양한 유해정보 차단 S/W 우회 경로를 포함하고 있었다. 이는 유해정보 차단 S/W의 활용 가능성을 심각하게 저하시키는 요인으로 새로운 유해정보 차단 S/W는 이러한 우회를 방지하기 위해 우회방지 모듈을 포함하고 있다. 우회방지 모듈은 키보드 해킹 방지, 시스템 정보 변경 제한, 그리고 우회 프로그램 사용 제한 모듈로 구성된다. 키보드 해킹을 근본적으로 막기 위해서는 드라이버 레벨에서 키보드 입력을 암호화하여 전달하는 방법을 사용해야 한다. 현재 주로 사용되는 키보드 해킹 프로그램은 응용 프로그램 레벨에서 키보드 입력을 암호화하는 방법을 주로 택하고 있기 때문에 응용 프로그램과 운영체제 사이에서 키보드 입력을 가로채면 암호화 이전의 입력내용을 확인할 수 있다. 시스템 정보 변경 제한 모듈을 구현하기 위해서는 윈도우의 경우 레지스트리 조작을 통해 관리자 이외의 사용자 접근을 방지할 수 있다. 우회 프로그램 실행 제한은 실행 프로그램 차단 기능과 그 구조가 동일하다. 그러나 사용자가 우회 프로그램 목록을 모두 확인할 수는 없기 때문에 유해정보 차단 S/W 개발 시 우회 프로그램 목록을 확보하여 이를 지속적으로 프로그램 업데이트 시 반영할 필요가 있다.

4.3 기존 유해정보 차단 S/W와 비교

새로운 유해정보 차단 S/W는 기존 유해정보 차단 S/W와는 달리 내용을 바탕으로 유해정보를 차단한다. 아래 <표 20>은 차단기능에 있어 기존 유해정보 차단 S/W의 한계점과 새로운 유해정보 차단 S/W이 지니는 강점을 나타낸다.

5. 결 론

인터넷의 확산과 컴퓨터의 대중화는 정보에 대한 접근성을 급진적으로 향상시켜 정보의 공유 및 확산이 활성화되었다. 인터넷 사용자는 누구나 컴퓨터를 사용하여 전세계에 걸쳐 필요한 정보를 검색할 수 있으며, 스스로의 정보를 웹에 게시하여 공유할 수 있다. 그러나 이와 같은 순기능에도 불구하고 역기능 역시 대두되고 있으나 바로 유해정보의 확산이다. 청소년에게 유해한 정보 역시 접근성이 향상되면서 그릇된 가치관 형성 및 청소년 범죄에 영향을 미치면서 사회적은 문제로 대두되고 있다. 2008년 4월 대구의 한 초등학교에서 일어난 집단 성폭력 사건은 인터넷의 유해정보 확산을 더 이상 방치할 수 없음을 의미한다. 조사결과 가해자인 고학년 학생들은 인터넷을 통해 접한 음란물로 인해 그릇된 성가치관을 형성하였으며 범죄로 이어졌음을 확인하였다.

이처럼 무분별한 유해정보의 확산을 막기 위해 현재 시중에는 무분별한 유해정보의 유출을 막기 위해 다양한 유해정보 차단 S/W가 출시되어 판매되고 있다. 그러나 3장에서 언급한 바와 같이 유해정보 차단 S/W의 기술적 한계로 인해 유해정보의 완벽한 차단이 어렵고, 차단기능에 대한 다양한 우회방법 또한 존재한다. 이에 본 논문은 유해정보 차단기능을 분석하고 기존 유해정보 차단 S/W의 한계점을 확인하였다. 그리고 기존 유해정보 차단 S/W의 문제점을 극복한 새로운 유해정보 차단 S/W의 요구사항을 도출하였다.

참 고 문 헌

[1] SafeNet, http://www.safenet.ne.kr

[2] PC 통신과 인터넷상의 불건전 정보유통 및 윤리의식 실태조사와 대응방안에 관한 연구, 정보통신윤리위원회 연구보고서, Jan., 1999.

[3] 2006년 불법·청소년 유해정보 실태 조사, 정보통신윤리위원회 연구보고서, July, 2006.

[4] 2007년 불법·청소년 유해정보 이용실태 조사, 정보통신윤리위원회 연구보고서, July, 2007.

[5] 장병탁, "차세대 기계학습 기술", 정보과학회지 제25권 제3호, Mar., 2007.

[6] 박성배, 태윤식, "기계학습과 정보검색", 정보과학회지 제25권 제3호, Mar., 2007.
[7] 김영수, 남택용, 원동호, "등급에 따른 웹 유해 문서 분류 기술", 정보처리학회논문지 C 제13-Crnjs 제7호, Dec., 2006.
[8] 남택용, 정치윤, 한치문, "인터넷에서의 유해 이미지 컨텐츠 등급 분류 기법", 정보과학회 논문지 정보통신 제32권 제3호, June, 2005.
[9] 동영상의 비주얼 특징을 이용한 유해 동영상 판별함수 생성 및 판별 방법 그리고 그 장치, 대한민국특허청 공개특허공보, May, 2007.
[10] 이재선, 전용희, 장정숙, "유해 인터넷 정보 차단을 위한 내용 등급 서비스 기반 사용자 인터페이스 설계 및 구현", 한국통신학회논문지, Vol.28, No.10B, Oct., 2003.

전 웅 렬

e-mail : wrjeon@security.re.kr
2006년 성균관대학교 정보통신공학부(학사)
2008년 성균관대학교 전자전기컴퓨터공학과(공학석사)
2008년~현 재 성균관대학교 전자전기컴퓨터공학과 박사과정
관심분야 : 보안성평가, 데이터베이스 보안

이 현 승

e-mail : hsrhee@security.re.kr
2008년 성균관대학교 정보통신공학부 컴퓨터공학과(학사)
2008년~현 재 성균관대학교 전자전기컴퓨터공학과 석사과정
관심분야 : 암호이론, 네트워크 보안, 금융보안

허 순 행

e-mail : shhur@security.re.kr
2007년 성균관대학교 정보통신공학부(학사)
2007년~현 재 성균관대학교 전자전기컴퓨터공학과 석사과정
관심분야 : 정보보호, 보안성 평가 등

김 경 신

e-mail : kskim@mail.induk.ac.kr
1983년 성균관대학교 전자공학과 학사
1985년 성균관대학교 전자공학과(석사)
1997년 성균관대학교 정보공학과(박사)
1984년~1991년 삼성전자(주) 컴퓨터부문 선임연구원
1995년~현 재 인덕대학교 인터넷 TV 방송과 교수
2001년~2002년 California State University, Northredge 객원연구원
관심분야 : 정보보호, 암호이론

원 동 호

e-mail : dhwon@security.re.kr
1976년~1988년 성균관대학교 전자공학과 (학사, 석사, 박사)
1978년~1980년 한국전자통신연구원 전임연구원
1985년~1986년 일본 동경공업대 객원연구원
1988년~2003년 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장, 연구처장
1996년~1998년 국무총리실 정보화추진위원회 자문위원
2002년~2003년 한국정보보호학회장
2002년~현 재 대검찰청 컴퓨터범죄수사 자문위원, 감사원 IT 감사 자문위원
2007년~현 재 성균관대학교 정보통신공학부 교수, 한국정보보호학회 명예회장, 정보통신부지정 정보보호인증기술연구센터 센터장, 정보통신대학원장
관심분야 : 암호이론, 정보이론, 정보보호

김 승 주

e-mail : skim@security.re.kr
1994년~1999년 성균관대학교 정보공학과 (학사, 석사, 박사)
1998년~2004년 한국정보보호진흥원(KISA) 팀장
2004년~현 재 성균관대학교 정보통신공학부 교수
2001년~현 재 한국정보보호학회, 한국인터넷정보학회, 한국정보과학회, 한국정보처리학회 논문지 및 학회지 편집위원
2002년~현 재 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2005년~현 재 교육인적자원부 유해정보차단 자문위원, 디지털콘텐츠유통협의체 보호기술워킹그룹 그룹장
2007년~현 재 대검찰청 디지털수사 자문위원, KISA VoIP 보안기술 자문위원, 기술보증기금 외부 자문위원, 전자정부서비스보안위원회 사이버침해사고대응 실무위원회 위원
관심분야 : 암호이론, 정보보호표준, 정보보호제품 및 스마트카드 보안성 평가, PET