방송통신정책연구

10-진 흥 -라 -08

# 불법유해정보의 우회접속 기술 동향 조사 및 기술 보급

(A Technical Investigation and Supply on the Circuital Connection of Illegal Information)

2010. 11.

연구기관 : (사)한국인터넷진흥협회

방송통신위원회
KOREA COMMUNICATIONS COMMISSION

방송통신정책연구

10-진 흥 -라 -08

# 불법유해정보의 우회접속 기술 동향 조사 및 기술 보급

(A Technical Investigation and Supply on the Circuital Connection of Illegal Information)

2010. 11. 30.

연 구 기 관 : (사)한국인터넷진흥협회

총괄책임자 : 예 영 선 ((사)한국인터넷진흥협회)

# 제 출 문

**방송통신위원회 위원장** 귀하

본 보고서를 **『불법유해정보의 우회접속 기술동향 조사 및 기술 보급』**의 연구결과보고서로 제출합니다.

2010. 12.


연구 기관 : (사)한국인터넷진흥협회

총괄책임자 : 예영선 ((사)한국인터넷진흥협회 차장)

참여연구원 : 안순식 ((사)한국인터넷진흥협회 실장)

최윤경 ((사)한국인터넷진흥협회 대리)

# 요 약 문

## 1. 제 목

불법유해정보의 우회접속 기술 동향 조사 및 기술 보급

## 2. 연구개발의 목적 및 방법

본 연구의 목표는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 정보통신망법)」에 따라 정보통신서비스제공자, 게시판 관리운영자에게 음란, 도박 등 해외 불법사이트 차단에 대한 취급 제한 명령제도의 실효성을 높이기 위한 정책을 수립하는데 필요한 기반 자료를 마련하는데 있다.

본 연구는 해외유입 불법유해사이트의 우회접속기술의 종류 및 차단기술 현황을 조사한다. 또한 해외 불법유해정보의 새로운 우회 접속기술에 대한 기술적인 차단 방법을 연구 및 시험 테스트함으로써, 불법유해정보에 대한 정부의 효율적인 관리감독, 제도 개선 방안을 제시한다.

## 3. 연구개발의 내용 및 범위

연구개발의 내용과 범위는 첫째, 해외유입 불법유해사이트의 우회접속 기술 현황을 조사 및 분석하고 둘째, 우회접속 기술에 대한 차단기술 동향을 조사 및 분석하여 마지막으로 새로운 우회접속에 대한 차단기술 시험 보급해 보는 것에 있다.

## 4. 연구결과

제1장 서 론

인터넷은 21세기 국가 경쟁력을 좌우하는 핵심 인프라이며, 일상생활에서 없어서는 안 될 정도로 큰 역할을 담당하고 있다. 인터넷 환경의 역기능으로 익명성을 악용한 불법·유해정보들이 급증하여 심각한 사회문제로 대두되고 있다.

안전한 인터넷 활용 방안 마련을 위해 인터넷가치사슬을 이용하여 연구를 수행한다. 국내·외 차단 정책과 기술에 대한 문헌조사와 차단기술 테스트 등을 통해 각 기능별로 추진할 수 있는 차단방안을 수립하는 것으로 연구 방향과 범위를 마련하였다.

제2장 인터넷 불법·유해 정보 현황 조사 및 분석

불법정보(illegal information or contents)와 유해정보(legal but harmful information or contents)의 개념을 어떻게 구분하는가에 따라 유형 및 범위, 규제시스템 및 개선방안도 달다진다. 불법정보는 국가가 적극적으로 개입하며, 유해정보는 자율규제시스템을 통한 민간 자율규제 활동이 필요하다.

국내 불법·유해 정보 차단 정책 추진과정은 1994년부터 한국통신(현 KT)이 인터넷상용서비스(KORNET)를 제공하기 시작한 시기로, 해외에서 유입되는 불법·유해정보가 사회적 문제로 제기되었다. 정보통신부(현 방송통신위원회)는 정보통신윤리위원회(현 방송통신심의위원회)를 신설하였다.

그리고 방송통신심의위원회를 주축으로 민간 중심의 자율 규제 제도 도입 시기로 인터넷내용등급서비스 도입과 IP차단과 DNS 변조 방법을 이용하여 해외 한글제공 불법사이트 차단사업을 수행하였으며, IP차단과 DNS 변조 차단기술을 상쇄하는 우회기술이 보급되어 URL기반의 새로운 차단 정책이 필요하게 된 시기로, 정보통신부에서 「해외 불법정보 차단업무 처리지침」을 마련하여 해당 사업자에게 적용하고 있다.

## 제3장 인터넷 불법·유해 정보 차단 기술 현황 및 분석

모든 불법·유해 인터넷 콘텐츠 접속을 차단하는 것이 기술적으로 가능하다 하더라도, 어떠한 인터넷 차단 혹은 필터링 기술도 100% 효과가 있을 수는 없으며, 의도적이고 정보력으로 무장한 공격자를 막아낼 수는 없다.

IP주소를 근거로 한 차단은 일반적으로 매우 신속하지만, 그 성능 영향(performance impact)은 작다. 이러한 차단은 판단되지 않은 콘텐츠의 과잉 차단(over-blocking) 현상을 초래할 수 있으며, 하나 이상의 웹 사이트에 동일한 IP주소를 사용하는 경우에는 무력하다.

DNS 변조(DNS Tampering)는 DNS 탈취(DNS hijacking)라고도 한다. 이는 개별사용자의 컴퓨터에 사용된 DNS 서버가 도메인 차단여부에 대한 질문을 받은 웹사이트의 차단을 요청하는 사용자가 적합한 IP주소에 차단 명령을 내리지 않도록 정보를 변경하는 것을 말한다.

IP주소 차단과 마찬가지로, 이 기술은 차단된 최상위 도메인의 하위도메인에 존재하는 모든 콘텐츠에 영향을 미치기 때문에 과잉차단을 초래할 수 있다.

가장 일반적이고, 효과적인 형태의 출처 기반 필터링은 사람이 읽을 수 있는 웹 페이지 주소인 URL에 근거를 둔 것이다. URL은 전체 컴퓨터 시스템이 아니라 각 웹 페이지의 이름이기 때문에, 이 방식을 사용하면 패킷 필터링보다 좀 더 세밀한 제어가 가능하다.

국내 인터넷서비스사업자들이 사용하는 IP주소 차단, DNS 차단, URL 차단 기술로는 해외유입 한글 불법·유해 정보와 사이트를 100% 차단하기 어렵다.

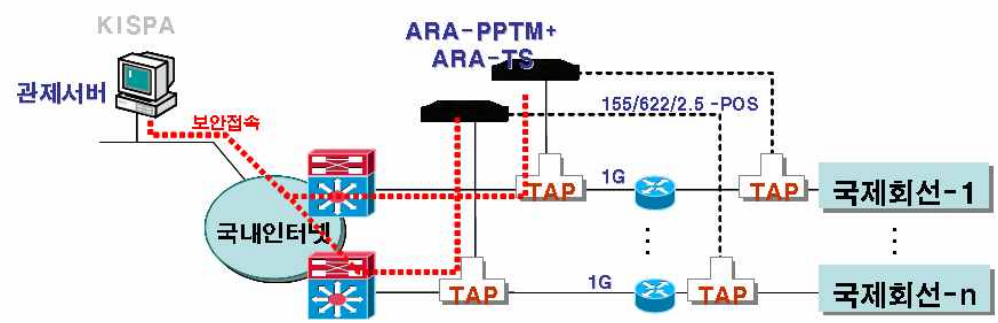
구글 또는 야후 등 해외 검색사이트의 번역 기능을 이용하거나, 프리게이트와 울트라서프 등 우회접속 소프트웨어, SSL를 이용한 VPN접속 서비스 등을 활용하면 우회가 가능하기 때문이다.

제4장 인터넷 불법·유해 정보 차단기술 시험 보급

불법 정보 자동 차단 시스템 지원사업으로 차단 시스템의 효과 검증을 위해 특정 ISP를 선정하여 일정기간 시험 하였다.


차단기술 시험 보급 및 테스트 절차도

기술 보급 기간은 2010년 6월부터 12월까지 시행하였으며, 대상 사업자는 드림라인을 시작으로 하여 8개 차단사업자를 모두 적용하였다.




기술적용은 기존 설치된 차단장비에 새로운 우회기술인 DNS Free Ver 3와 번역사이트, 특수기호 등의 보완사항을 업그레이드하였다.

차단장비의 업그레이드와 관리서버의 패치 등을 통하여 차단장비에 적용하였으며, 이를 통하여 테스트를 통해 시험 적용하였다. 참고로, 차단장비의 테스트는 여러 환경을 할 수 없는 부분이 있기에 장시간을 통하여 테스트를 하였으며, 1개의 사업자를 통하여 테스트를 한 후 전체 차단사업자에게 보급하는 방법으로 진행하였다.

기존에 설치된 차단장비(PPTM Plus) 및 중앙통제서버를 업그레이드를 시행하였고, 장비는 TAP를 통하여 미러방식을 통하여 회선에 최대한 장애를 주지 않는 상태에 네트워크 망을 구성하였다. 또한, 차단장비 및 통제서버는 기존에 설치된 장비 외의 별도의 장비를 이용하여 기존의 차단에 영향을 주지 않는 범위에서 시행하였다.

이때, 환경변수 등을 고려하여 최대한 기존 장비의 설정을 파악하여 고려한 후, 시험테스트 장비를 세팅하고 업그레이드를 통해 테스트할 수 있도록 조치하였다. 여러 가지 환경변수가 발생하였지만, 기존 차단장비에 업그레이드 형태로 진행하여 크게 문제없이 진행할 수 있었다. 다만, 향후 아래의 보완이 필요할 것으로 예측된다.

| 구 분 | 내 용 |
|---|---|
| **절차적 측면** | • 중앙통제서버의 차단목록 등록 방식<br>• 수행서버에서 차단 시작 방식<br>• 로그 분석을 수행할 서버<br>- 1안 : 수행서버에서 분석하여 분석 결과만 중앙통제서버로 전송<br>- 2안 : 수행서버에서는 모든 로그를 모두 중앙통제서버로 전송 한 후 중앙통제서버에서 분석 수행<br>• 로그 분석의 주기 및 범위<br>- 예) 주기 : 일별, 월별, 분기별<br>범위 : 차단 실적(우회 시도 포함), TOP CLIENT&URL |
| **유연성 측면** | • 특정 소스는 특정 URL의 접근을 허용하는 방법<br>• 차단 유형별로 로그를 나누어서 적재하는 방법<br>• 비정상트래픽(예, 127.0.0.1 DoS 공격 등)일경 우 로그 제외 방법<br>• 변칙 URL 문자열 사용시(예, URL 끝에 점(.)을 사용) - 보완 완료 |

이러한 환경설정에도 불구하고 필터 우회 프로그램 등이 발생되고 있고, 장기적인 조사 및 분석, 연구가 필요할 것으로 본다.

## 제5장 결 론

불법·유해정보의 현황을 통한 기술 보급으로 국민들이 보다 건전한 인터넷을 활용할 수 있는 기반을 마련하였으며, 이러한 가치는 건전한 인터넷을 위한 규제 활동이 성공할 가능성은 그만큼 증가한 것으로 볼 수 있다.

인터넷의 불법·유해 정보를 차단하기 위해서는 여러 가지 환경변수를 연계하고 통합 관리해야 한다. 이러한 연계는 어려울 수 있지만, 정부 및 기업 등의 관련된 기관들의 협력과 노력을 통해 실현 가능할 것이다.

## 5. 활용에 대한 건의

본 보고서 크게 3가지 용도로 활용할 수 있을 것이다. 첫째는 차단 정책과 적용 기술에 대한 상세분석 결과를 활용하여 우리나라에 적합한 정책을 도입할 수 있다. 둘째, 국내외 차단기술과 우회기술 분석 결과를 활용하여, 차단 신기술 개발에 응용할 수 있을 것이다. 셋째, 우회접속 기술과 차단기술을 연계하여 종합적인 차단 정책으로 활용할 수 있다.

## 6. 기대효과

국내 불법·유해 정보 차단에 대한 현황 및 기술적으로 차단할 수 있는 여러 가지 정책과 기술을 추진하여 왔다. 본 연구를 통해 불법·유해 정보 차단에 대한 여러 가지 대책을 마련할 수 있게 되었다. 불법·유해 정보 차단 정책과 기술, 보급 등이 총체적으로 정리함으로써 차단정책 추진을 위한 큰 기틀을 마련하였고, 국민들에게 건전한 인터넷 활용을 위해 다각적으로 지원할 수 있는 기틀을 제공하였다.

# 목 차

# 그 림 목 차

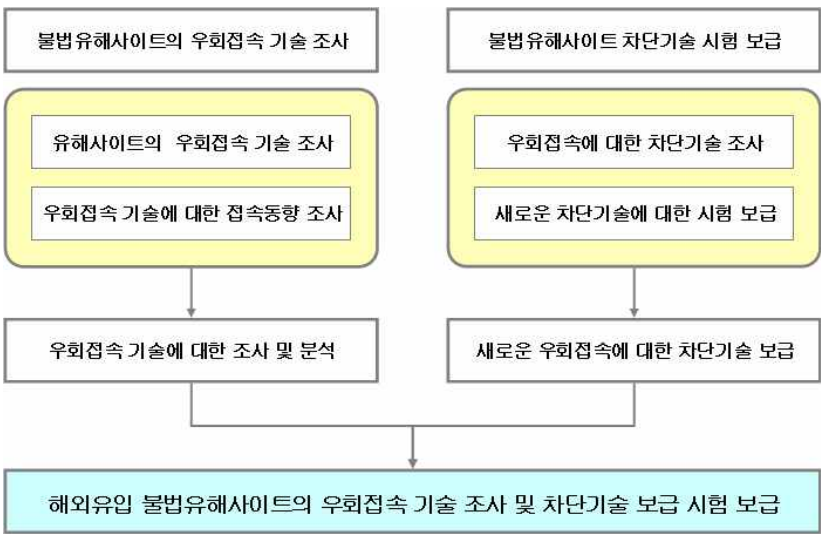
# 표 목 차

# 제1장 서 론

## 1절. 연구의 목적

인터넷은 지구 반대편의 컴퓨터라 할지라도 거리 때문에 접속이 불가능하다는 점이 없어 자신의 도시안의 컴퓨터처럼 쉽게 접속할 수 있다. 개인들은 인터넷서비스사업자를 통해 제공되는 인터넷접속서비스를 제공받아 인터넷에 접속하고 있다. 물론 사업자들도 비슷한 방법으로 인터넷에 접속한다.

인터넷은 일상생활에서 없어서는 안 될 정도로 큰 역할을 담당하고 있다. 이러한 원동력은 우리나라가 세계적인 IT기술을 바탕으로 초고속 정보통신망을 구축하고, 세계 최고의 IT국가로써 인터넷의 이용 빈도 및 수준을 높인 결과이다.




[그림 1] 연구개발 목표

건전한 온라인 정보의 유통을 촉진하고 불법·유해정보의 국내 유입을 효과적으로 차단하기 위한 방안을 마련할 필요가 있다. 차단 방안 수립에 필요한 기초 자료로, 현재 유입되는 해외의 불법·유해정보 현황과 특성을 조사 분석한다.

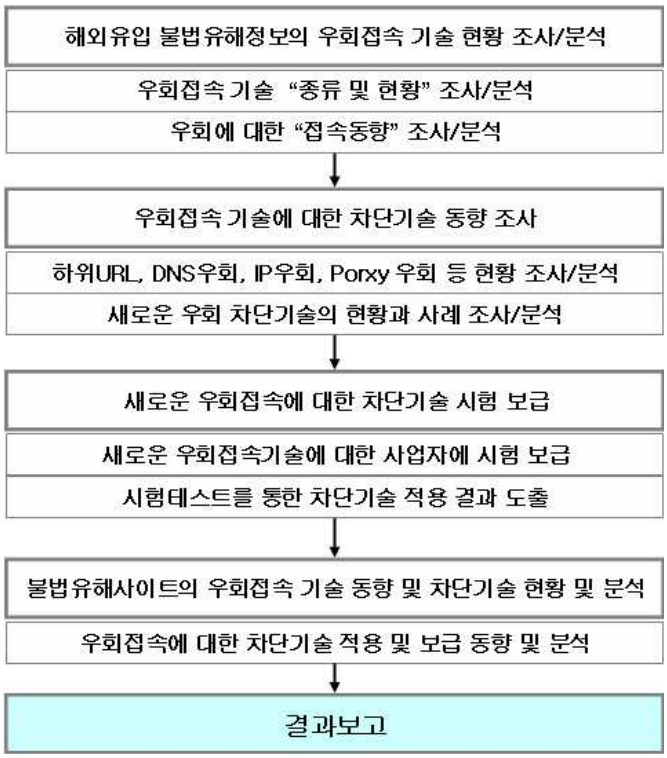
이를 바탕으로, 국내에 인터넷이 도입된 이후의 불법·유해 정보 차단 현황을 살펴본다. 우리나라는 해외에 서버를 둔 도박, 음란 사이트는 DNS 변조방식으로, 친북 사이트는 IP차단 방식으로 차단하였으나, 우회 접속이 가능하여 차단을 완벽하게 수행하지 못했다.

정부는 우회접속을 방지하기 위해 ISP사업자에게 URL 차단을 요청하였고, 2008년 11월부터 8개 기간통신사업자들은 URL 차단 장비를 도입하여 운영 중이다. DNS 변조방식, IP 차단방식, URL 차단방식 등 국내에 적용 중인 차단 기술과 우회 기술을 분석하여 본다.

또한, 국내외 불법·유해정보 동향을 분석하여, 불법·유해정보 우회기술에 대한 신속한 대응을 차단기술을 보급하여 시험 적용을 하여 본다.

## 2절. 연구의 범위

본 연구과제의 목적을 달성하기 위한 연구개발 내용 및 범위를 도식화하고 세부 연구 범위를 기술하면 [그림 2]와 같다.




[그림 2] 연구 내용 및 범위

### 1. 해외유입 불법·유해정보의 종류 및 우회기술 현황 조사

현재 이슈가 되고 있는 해외 유입 불법·유해정보의 종류와 특성을 조사·분석한다. 조사 대상은 불법·유해정보의 정의와 특성, 해외유입 불법·유해정보 현황과 사례 등이다.

해외 유입 불법·유해정보에 사용하는 우회기술의 유형과 특징을 조사하여 분석한다. 조사대상은 DNS 우회, IP Resolving, 등 불법유해정보의 우회기술 유형과 특성, 해외유입 불법·유해정보 우회기술의 사례와 현황, 해외유입 불법·유해정보 우회기술의 문제점 등이다.

## 2. 불법유해정보의 우회기술에 대한 기술적인 차단 방법 연구

해외 유입 불법·유해정보의 우회기술을 차단하는 국내외 기술을 조사·분석한다. 조사대상은 DNS방식, IP방식 등 기존 차단방식과 URL 차단방식 등 최신 해외유입 불법·유해정보 우회기술의 차단 현황과 사례 등이다.

기술 조사 결과를 기반으로 기술적인 차단 방법의 적용방안을 마련한다. 해외유입 불법·유해정보 우회기술 차단의 문제점을 분석하고, 해외유입 불법·유해정보 우회기술 차단방법 적용 방안을 마련한다.

## 3. 불법유해정보의 우회기술에 대한 시험 기술 보급

해외 유입 불법 유해정보의 우회기술을 기소 현황을 바탕으로 새로운 차단 기술을 개발하고, 이를 차단 사업자에게 기술 시험 적용하고, ISP 사업자 등 주요 대상기업을 대상으로, 효율적인 관리 방안을 마련한다.

## 3절. 연구의 방법

### 1. 자료 수집과 분석 활동

국내·외 정부와 공공기관에서 추진하는 최신의 정책과 기술동향 자료를 수집·분석하여 첨단 정보를 제공하고, 국제적인 차단 반대활동 동향 자료를 면밀히 분석하여 기술 방향을 살펴본다.

### 2. 차단기술과 우회기능 성능 분석

최근에 도입하여 운영 중인 URL 차단도구가 효과적으로 활용되는지를 확인하기 위해 다양한 우회 접속 기술을 적용하여, URL 차단 도구를 테스트한다. 이를 통해 불법유해정보의 차단 여부를 파악한다.

# 제2장 인터넷 불법·유해정보 차단 기술 조사

## 1절. 인터넷 불법·유해 정보 현황

불법정보(illegal information or contents)와 유해정보(legal but harmful information or contents)의 개념을 어떻게 구분하는가에 따라 유형 및 범위, 규제시스템 및 개선방안도 달라진다. 일반적으로 불법정보는 유통이 금지되는 정보를 말하며, 유해정보는 유통은 가능하나 특정 계층에 유해한 정보이다.

불법정보와 유해정보의 개념은 이분법적으로 구분할 수밖에 없다. 헌법과 형법 등에서 금지하는 내용의 불법정보와 유해정보를 동일 또는 유사하게 규제하는 경우에는 표현의 자유의 본질적 내용을 침해함으로 헌법 제37조 제2항 과잉금지원칙에 위반할 여지가 있다.

유해정보를 불법정보의 범주에 포함시키면 법의 범위가 너무 확대되어 규율자체가 곤란해지거나, 정보 접근권 및 자기결정권 등이 침해되어 표현의 자유가 침해될 수 있다.

유해정보와 유사한 용어로 불법정보, 불건전정보, 불온통신정보, 불법·청소년유해정보, 비합법적 정보, 유통부적합 정도 등의 용어가 사용되고 있다. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제41조(청소년보호를 위한 시책의 마련 등) 및 제44조의7(불법정보의 유통금지 등)에서는 불법정보 및 청소년유해정보라는 용어를 사용하고 있지만, 불법정보의 대표적인 유형을 열거하거나 단순하게 용어를 풀어 놓은 수준이다.

## ※ 참고 : 실정법의 불법정보 유형

우리나라 실정법은 불법정보와 유해정보를 불법정보와 청소년유해정보로 통칭한다. 유해정보는 청소년유해정보로 표현되어 법 적용범위가 제한적이며, 일부 유해정보는 불법정보와 중복되기도 한다. 본 연구에서는 실정법상에 나타난 불법정보와 청소년유해정보의 유형을 알아본다.

불법정보와 청소년유해정보는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「청소년 보호법」, 「성폭력범죄의 처벌 및 피해자보호등에 관한 법률」, 「정보통신기본법」,「전파법」 등의 실정법과 「방송통신위원회의 설치 및 운영에 관한 법률」에 의한 <정보통신에 관한 심의 규정> 등에서 다루어진다.

'불법정보'를 표현한 실정법은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」제44조의7(불법정보의 유통금지 등)이다. 동법에는 음란, 명예훼손, 스토킹, 해킹, 청소년유해매체물, 사행행위, 국가기밀누설, 국가보안법 금지행위, 범죄 교사나 방조 등 불법정보를 9가지 유형으로 정의한다. 이중 음란, 명예훼손, 스토킹, 해킹, 사행행위 등은 형법에 범죄로 규정되었다.

① 정보통신망 이용촉진 및 정보보호 등에 관한 법률

---

**제44조의7(불법정보의 유통금지 등)**

① 누구든지 정보통신망을 통하여 **다음 각 호의 어느 하나에 해당하는 정보를 유통하여서는 아니 된다.**

1. 음란한 부호·문언·음향·화상 또는 영상을 배포·판매·임대하거나 공공연하게 전시하는 내용의 정보
2. 사람을 비방할 목적으로 공공연하게 사실이나 거짓의 사실을 드러내어 타인의 명예를 훼손하는 내용의 정보

---

3. 공포심이나 불안감을 유발하는 부호·문언·음향·화상 또는 영상을 반복적으로 상대방에게 도달하도록 하는 내용의 정보
4. 정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해하는 내용의 정보
5. 「청소년보호법」에 따른 청소년유해매체물로서 상대방의 연령 확인, 표시의무 등 법령에 따른 의무를 이행하지 아니하고 영리를 목적으로 제공하는 내용의 정보
6. 법령에 따라 금지되는 사행행위에 해당하는 내용의 정보
7. 법령에 따라 분류된 비밀 등 국가기밀을 누설하는 내용의 정보
8. 「국가보안법」에서 금지하는 행위를 수행하는 내용의 정보
9. 그 밖에 범죄를 목적으로 하거나 교사(敎唆) 또는 방조하는 내용의 정보

② 성폭력범죄의 처벌 및 피해자보호등에 관한 법률

**제14조 (통신매체이용음란)**

**자기 또는 다른 사람의 성적 욕망을 유발하거나 만족시킬 목적으로 전화·우편·컴퓨터 기타 통신매체를 통하여 성적 수치심이나 혐오감을 일으키는 말이나 음향, 글이나 도화, 영상 또는 물건**을 상대방에게 도달하게 한 자는 2년 이하의 징역 또는 500만원 이하의 벌금에 처한다.

**제14조의2 (카메라등 이용촬영)**

①**카메라 기타 이와 유사한 기능을 갖춘 기계장치를 이용하여 성적 욕망 또는 수치심을 유발할 수 있는 타인의 신체를 그 의사에 반하여 촬영하거나 그 촬영물**을 반포·판매·임대 또는 공연히 전시·상영한 자는 5년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.

③ 전기통신기본법

**제47조(벌칙)**

①**공익을 해할 목적으로 전기통신설비에 의하여 공연히 허위의 통신**을 한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

②**자기 또는 타인에게 이익을 주거나 타인에게 손해를 가할 목적으로 전기통신설비에 의하여 공연히 허위의 통신**을 한 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.

④ 전파법

제80조(벌칙)

① 무선설비나 전선로에 주파수가 9킬로헤르츠 이상인 전류가 흐르는 통신설비(케이블반송설비 및 평형2선식 나선반송설비를 제외한 통신설비를 말한다)를 이용하여 「대한민국헌법」 또는 「대한민국헌법」에 따라 설치된 국가기관을 폭력으로 파괴할 것을 주장하는 통신을 한 자는 3년 이상의 유기징역 또는 금고에 처한다.

제83조(벌칙) ① 자기 또는 타인의 이익을 위하거나 타인에게 손해를 줄 목적으로 무선설비 또는 전선로에 주파수가 9킬로헤르츠 이상인 전류가 흐르는 통신설비(케이블반송설비 및 평형2선식 나선반송설비를 제외한 통신설비를 말한다)에 의하여 거짓으로 통신을 한 자는 3년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.

제85조(벌칙) 무선설비 또는 전선로에 주파수가 9킬로헤르츠 이상인 전류가 흐르는 통신설비(케이블반송설비 및 평형2선식 나선반송설비를 제외한 통신설비를 말한다)로 음란한 통신을 한 자는 2년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.

⑤ 게임산업진흥에 관한 법률

제32조(불법게임물 등의 유통금지 등)

②누구든지 다음 각 호에 해당하는 게임물을 제작 또는 반입하여서는 아니 된다.

1. 반국가적인 행동을 묘사하거나 역사적 사실을 왜곡함으로써 국가의 정체성을 현저히 손상시킬 우려가 있는 것
2. 존비속에 대한 폭행·살인 등 가족윤리의 훼손 등으로 미풍양속을 해칠 우려가 있는 것
3. 범죄·폭력·음란 등을 지나치게 묘사하여 범죄심리 또는 모방심리를 부추기는 등 사회질서를 문란하게 할 우려가 있는 것

⑥ 형법

제243조 (음화반포등) 음란한 문서, 도화, 필름 기타 물건을 반포, 판매 또는 임대하거나 공연히 전시 또는 상영한 자는 1년 이하의 징역 또는 500만원 이하의 벌금에 처한다.

**제244조 (음화제조등)** 제243조의 행위에 공할 목적으로 음란한 물건을 제조, 소지, 수입 또는 수출한 자는 1년 이하의 징역 또는 500만원 이하의 벌금에 처한다.

**제246조 (도박, 상습도박)** ①재물로써 도박한 자는 500만원 이하의 벌금 또는 과료에 처한다. 단, 일시오락정도에 불과한 때에는 예외로 한다.

**제247조 (도박개장)** 영리의 목적으로 도박을 개장한 자는 3년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.

**제248조 (복표의 발매등)** ①법령에 의하지 아니한 복표를 발매한 자는 3년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.<개정 1995.12.29>

---

**제283조 (협박, 존속협박)** ①사람을 협박한 자는 3년 이하의 징역, 500만원 이하의 벌금, 구류 또는 과료에 처한다.<개정 1995.12.29>

②자기 또는 배우자의 직계존속에 대하여 제1항의 죄를 범한 때에는 5년 이하의 징역 또는 700만원 이하의 벌금에 처한다.<개정 1995.12.29>

③제1항 및 제2항의 죄는 피해자의 명시한 의사에 반하여 공소를 제기할 수 없다. <개정 1995.12.29>

**제284조 (특수협박)** 단체 또는 다중의 위력을 보이거나 위험한 물건을 휴대하여 전조제1항, 제2항의 죄를 범한 때에는 7년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.<개정 1995.12.29>

**제307조 (명예훼손)** ①공연히 사실을 적시하여 사람의 명예를 훼손한 자는 2년 이하의 징역이나 금고 또는 500만원 이하의 벌금에 처한다.<개정 1995.12.29>

②공연히 허위의 사실을 적시하여 사람의 명예를 훼손한 자는 5년 이하의 징역, 10년 이하의 자격정지 또는 1천만원 이하의 벌금에 처한다.<개정 1995.12.29>

**제308조 (사자의 명예훼손)** 공연히 허위의 사실을 적시하여 사자의 명예를 훼손한 자는 2년 이하의 징역이나 금고 또는 500만원 이하의 벌금에 처한다. <개정 1995.12.29>

**제309조 (출판물등에 의한 명예훼손)** ①사람을 비방할 목적으로 신문, 잡지 또는 라디오 기타 출판물에 의하여 제307조제1항의 죄를 범한 자는 3년 이하의 징역이나 금고 또는 700만원 이하의 벌금에 처한다.<개정 1995.12.29>

②제1항의 방법으로 제307조제2항의 죄를 범한 자는 7년 이하의 징역, 10년 이하의 자격정지 또는 1천500만원 이하의 벌금에 처한다.<개정 1995.12.29>

**제311조 (모욕)** 공연히 사람을 모욕한 자는 1년 이하의 징역이나 금고 또는 200만원 이하의 벌금에 처한다.<개정 1995.12.29>

**제313조 (신용훼손)** 허위의 사실을 유포하거나 기타 위계로써 사람의 신용을 훼손한 자는 5년 이하의 징역 또는 1천500만원 이하의 벌금에 처한다.<개정 1995.12.29>

**제314조 (업무방해)** ①제313조의 방법 또는 위력으로써 사람의 업무를 방해한 자는 5년 이하의 징역 또는 1천500만원 이하의 벌금에 처한다.<개정 1995.12.29>

②컴퓨터 등 정보처리장치 또는 전자기록등 특수매체기록을 손괴하거나 정보처리장치에 허위의 정보 또는 부정한 명령을 입력하거나 기타 방법으로 정보처리에 장애를 발생하게 하여 사람의 업무를 방해한 자도 제1항의 형과 같다.<신설 1995.12.29>

**제316조 (비밀침해)** ①봉함 기타 비밀장치한 사람의 편지, 문서 또는 도화를 개봉한 자는 3년 이하의 징역이나 금고 또는 500만원 이하의 벌금에 처한다. <개정 1995.12.29>

②봉함 기타 비밀장치한 사람의 편지, 문서, 도화 또는 전자기록등 특수매체기록을 기술적 수단을 이용하여 그 내용을 알아낸 자도 제1항의 형과 같다.<신설 1995.12.29>

⑦ 풍속영업의규제에관한법률

**제3조(준수사항)** 풍속영업을 영위하는 자(허가 또는 인가를 받지 아니하거나 등록 또는 신고를 하지 아니하고 풍속영업을 영위하는 자를 포함하며, 이하 "풍속영업자"라 한다) 및 대통령령으로 정하는 종사자는 다음 각호의 사항을 지켜야 한다.

2.**풍속영업소에서 음란한 문서·도화·영화·음반·비디오물 기타 물건(이하 "음란한 물건"이라 한다)을 반포·판매·대여하거나 이를 하게 하는 행위와 음란한 물건을 관람·열람하게 하는 행위 및 반포·판매·대여·관람·열람의 목적으로 음란한 물건을 진열 또는 보관**하여서는 아니된다.

**제10조(벌칙)**

②제3조제1호의2·제2호 및 제3호의 규정을 위반한 자는 3년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.

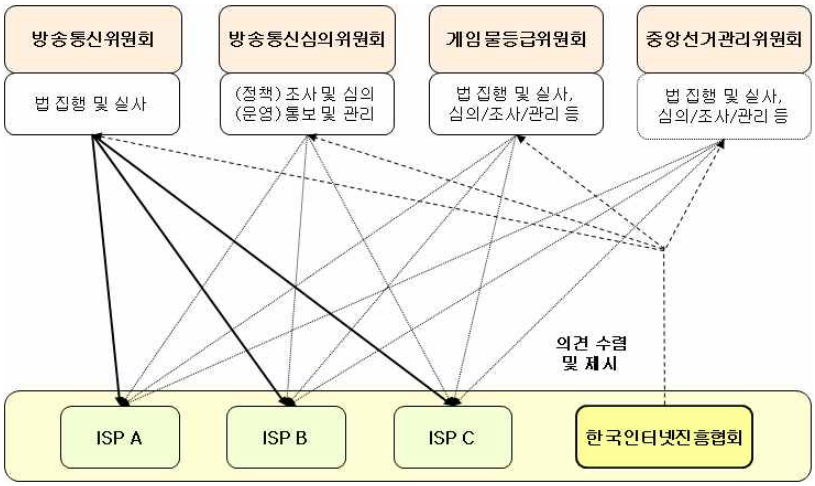
## 2절. 국내 불법 · 유해 정보 차단 정책

1985년 데이콤이 국내 최초로 PC통신을 이용한 온라인 서비스를 제공하였다. 1992년 하이텔이 유료 PC통신 서비스를 제공하면서부터 외설 및 음란물 유통에 대한 범정부차원에서 대책을 추진하였다. 정보통신부는 1992년 PC통신상의 외설 및 음란물 확산을 방지하기 위한 대책으로 정보윤리위원회와 불건전정보신고센터를 설치하였다.

1994년부터 한국통신이 인터넷상용서비스(KORNET)를 제공하기 시작했고, 이를 계기로 해외에서 유입되는 불법·유해정보가 사회적 문제로 대두되었다. 정보통신부는 불법·유해정보 차단정책을 추진하기 위해 정보통신윤리위원회를 설립하였다. 정보통신부는 1998년부터 2년간 한국전산원과 정보통신윤리위원회 공동으로 서버용 유해정보 차단도구를 개발하는 등 다양한 정책과 기술개발을 추진하였다.

정보통신윤리위원회(현, 방송통신심의위원회)와 한국ISP협회(현, 한국인터넷진흥협회) 등 민간 중심의 자율적 규제 제도가 도입된 시기다. 인터넷내용등급서비스 제도를 도입하였고, IP 차단과 DNS 변조 방법을 이용하여 해외 한글제공 불법·유해사이트 차단사업을 수행하였다.

IP차단과 DNS 변조 차단기술을 상쇄하는 우회 접속기술 방법이 보급되어 URL 기반의 새로운 차단 정책이 필요하게 된 시기로, 정부부처(방송통신위원회, 문화체육관광부, 경찰청, 국가청소년위원회, 게임물등급위원회, 방송통신심의위원회 등) 및 관련 기관(포털사업자, 민간단체, ISP기관 등)의 협의체 구성을 통한 공조활동을 수행하고 있다.




[그림 3] 우리나라 인터넷 불법·유해 정보 규제 체계

우리나라에서 음란 정보에 대한 규제 및 단속 업무를 담당하는 기관은 방송통신심의위원회(이하 심의위), 청소년보호위원회(이하 보호위), 그리고 경찰청 등 3개 기관이다. 이외 방송통신위원회, 보건복지가족부 등이 음란 정보 관련 유관 기관이다.

심의위는 불법·청소년유해정보신고센터, 온라인 모니터 단을 운영하고 있다. 모니터를 통한 정보수집과 분석을 통해, 불법사항을 적발하면 증거자료를 수집하여 불법·유해 정보에 대한 심의과정을 거친다. 필요에 따라 유관기관에 협조를 요청, 수사의뢰 및 사이트 접속 차단 등 행정 및 사법적인 조치가 이루어지도록 한다. 「방송통신위원회의 설치 및 운영에 관한 법률 시행령」은 심의위로 하여금 '해당 정보의 삭제 또는 접속차단' 시정요구를 할 수 있게 했다.

보호위는 불법·청소년유해 매체물에 대한 신고가 접수되거나 자체적으로 매체물에 대한 심의가 필요한 경우, 불법·청소년유해 매체물 심의를

심의위에 요청한다. 불법·청소년유해 매체물로 심의위의 통보를 받으면, 장관명의로 고시를 한다.

경찰청은 이러한 심의위나 보호위의 수사의뢰에 따라 보내진 증거자료 및 자체 수사를 통해 불법사항을 확인하고 범인 검거를 위한 조치를 취한다. 심의위의 수사의뢰 외에도 경찰청 사이버테러대응센터 내 콜센터에서 접수받는 각종 신고를 처리한다.

방송통신위원회의 불법·유해정보 유통행위에 대한 취급거부·정지·제한명령제도는 인터넷상의 음란, 폭력, 자살 등 각종 불법·유해정보에 대한 매우 강력한 규제수단이다. 방송통신위원회는 취급거부·정지·제한명령의 대상이 되는 불법정보를 구체적으로 개별화하여, 내용상 명백한 불법정보만 규제함으로서 과도한 규제 소지를 해소하였다.

'접속차단'에 대한 명확한 근거는 「방송통신위원회의 설치 및 운영에 관한 법률」시행령 제8조 제2항 제1호 '해당 정보의 삭제 또는 접속차단'이다. 방송통신심의위원회는 심의를 통해 시정 요청할 수 있으며, 이를 거부할 경우 방송통신위원회는 해당 정보의 취급을 거부·정지 또는 제한하도록 명할 수 있다.

## 3절. 인터넷 불법·유해정보 차단 기술

불법 유해정보는 기존의 IP접속, 단순 DNS변경(DNS Free ver 2)과 Port 변경, Proxy 등의 여러 가지 방법의 차단이 이루어져 왔으며, 차단사업자는 URL 차단장비를 도입하여 2009년 12월부터 차단을 시행하였다.

하지만, 이러한 차단에 따른 반발로 또다른 우회방법이 나타나고 있다. 이러한 우회 접속방법의 대표적인 기술이 DNS변경이다.

DNS변경은 단순하면서 접속하기 간단하고, 설치가 쉬워 누구나 쉽게 이용이 가능한 장점을 지니고 있다. 이러한 DNS변경 대표 프로그램이 바로 DNS Free이다. 현재 DNS Free ver 3까지 개발되어 유포되고 있다.


[그림 4] DNS Free Ver 3 실행화면

DNS Free ver 3의 특징으로는 별도의 DNS 프로그램을 통한 우회접속 가능하며, 기존 "DNS Free ver 2.0"과 달리 멀티 도메인을 사용하게 되며 차단 URL을 접속 가능한 URL로 수시로 변경하여 접속케 하여 서비스 하는 프로그램이다. 접속방법은 패킷의 IP헤더의 목적지 주소는 과거 사용했던 DNS주소를 이용하여 접속하여, HTTP 헤더와 Host 필드 값은 사용자가 입력한 URL과 무관하게 랜덤 생성하여 대체도메인(예: sex.com → hixava.com)으로 바꾸어 서버에 요청하는 방법을 취하고 있다.

또한, DNS Free와 다른게 기존에 제공하고 있는 인터넷 서비스를 통하여 접속하는 방법으로 번역사이트를 들 수 있다.

구글 등의 번역사이트를 통하여 해당 차단대상 URL를 번역할 경우 영어 등의 외국어뿐 아니라 국내의 한글로 된 사이트까지 그대로 나타나고 이러한 사이트는 무방비라 할 수 있다. 번역사이트는 2010년 초에 조사에서 새롭게 발견한 접속 방법으로 단순하면서 사용자가 쉽게 접속할 수 있는 장점을 지니고 있다.

[표 1]에서 보는 바와 같이, 2009년 12월까지 차단기술을 개발 및 차단사업자가 장비를 도입하여 차단기술을 적용하여 왔다.

기존의 DNS변경(DNS Free Ver 2) 및 IP접속, Port 변경, Proxy서버 사용 등의 여러 가지 방법으로 우회하는 기술을 차단하였으나, 차단기술 장비도입의 시점과 맞추어 새로운 우회접속 기술방법은 여러 가지로 개발될 것으로 예측된다.

[표 1] 불법 유해사이트 우회접속 기술 현황

| 우회접속기술 | 예 시 | ~ 2009년 12월 |
|---|---|---|
| DNS 변경 | DNS Free | DNS프리2 프로그램 차단,<br>DNS프리3 프로그램 등장(2010년) |
| IP Resolving | 10.10.10.5 | 차단 |
| Port 변경 | 80포트 외 | 차단 |
| Proxy 설정 | proxy server | 차단 |
| Proxy프로그램 | burp proxy | 차단 |
| Anonymizer | proxyguy.com 등 | 차단 |
| URL 단축 | sfider.com | 차단 |
| SSL 이용 | 프리게이트 등 | 차단 불가(암호화 해독 불가능) |
| 번역사이트 이용 | Yahoo 등 | 2010년 새롭게 발견된 접속방법 |
| 기타 | 특수기호 등 | 2010년 새롭게 발견된 접속방법 |

# 제3장 인터넷 불법·유해정보 차단 기술 분석

## 1절. 인터넷 차단과 필터링

인터넷은 지리적·정치적 경계와 상관없이 전 세계의 컴퓨터를 단일하고 경계가 없는 네트워크로 연결해 준다. 지구 반대편의 컴퓨터라 할지라도 거리 때문에 약간 반응이 느릴 뿐 같은 도시 안의 컴퓨터처럼 쉽게 접속할 수 있다. 인터넷은 단일한 네트워크이지만, 사실 많은 수의 더 작고, 자율적인 네트워크들의 상호 연결로 이루어져 있다. 인터넷은 어떤 단일한 조직이나 정부가 소유, 제어 혹은 관리하는 것이 아니다.

보통 개인들은 ISP를 통해 제공되는 서비스에 가입하여 인터넷에 접속한다. 이 서비스는 보통 적어도 다음 두 가지를 포함한다.

- o 개인 컴퓨터로부터의 인터넷 접속 : 사용자가 먼저 서비스를 제공받는 ISP에 전화 모뎀이나 전용회선을 이용하여 접속하면, 컴퓨터가 인터넷에 'on' 상태가 되어, 인터넷이 제공하는 모든 것에 접속할 수 있게 된다.
- o 선택적 웹 사이트 호스팅 : 가입자가 자신만의 웹 페이지를 만들고 서비스를 제공받는 ISP 서버에 호스트 시킨다. 이 페이지는 누구나, 전 세계 어디에서, 언제나 이용 가능하다.

사업자들도 비슷한 방법으로 인터넷에 접속하는데, 내부 네트워크와 서버를 인터넷에 연결해 주는 영구적인 ISP 접속을 주로 사용한다. 대형 사업자들은 자체 이메일 혹은 웹 서버를 운영하며, ISP는 인터넷에 접속하는 경로로만 사용한다.

인터넷 출판은 신문, 서적, 텔레비전과 같은 보다 전통적인 매체들에 비해 훨씬 사용하기 쉽고 저렴하다. 인쇄는 비교적 비싸며, 출판된 자료는 물리적으로 배포되어야 하므로 통제하거나 규제하기가 쉽다.

라디오와 텔레비전은 배포 비용이 저렴한 방송 매체이지만 고가의 장비와 넉넉하지 않은 (그리고 강한 규제를 받는) 전파 스펙트럼 공간을 필요로 한다. 반면, 웹 출판은 비용이 거의 들지 않으며, ISP에 의해 최종 사용자에게 제공되는 패키지의 일부로서 무료 서비스인 경우가 많다.

정부가 전통적인 매체를 규제하고 통제하는 것은 쉬운 일일지 모르나, 인터넷은 그 규모와 국제적인 속성 때문에 통제하기가 훨씬 어렵다. 세계 대부분의 지역에서는 누구나 자료의 검사나 승인 없이 쉽게 웹상에서 출판할 수 있다. 출판은 그저 파일을 웹 서버에 복사해 넣는 정도의 일에 불과하며, 이 간단한 행위만으로도 전세계 사람들이 이용할 수 있게 만들 수 있다.

인터넷은 단지 컴퓨터의 네트워크이며, 텍스트, 그림, 소리, 영상을 포함하여 디지털 형식으로 변환될 수 있고 컴퓨터 간에 전달될 수 있는 것은 무엇이든지 이동시킬 수 있다. 이러한 콘텐츠는 웹사이트에 출판하거나, 이메일을 통해서 전송하거나, 뉴스 그룹에 게시하거나, 대화방에서 토의하거나, 파일로 전송될 수 있다.

ISP나 인터넷 백본을 운영하는 전달자가 볼 수 있는 것은 단지 데이터의 패킷 및 그 출처와 목적지 주소뿐이다. 영상이든 텍스트이든, 웹 페이지이든 이메일이든, 패킷을 최종 목적지까지 갈 길로 보내는 역할을 하는 라우

터에는 모두 똑같은 것이다. 데이터 패킷은 최종 목적지에 도착하고 나서야 영상 스트림이나 사진으로 재조립되고 해석되는 것이다.

인터넷은 웹 이상의 것으로서, 필터링 제품이 정말 효과가 있으려면, 가능성 있는 콘텐츠 출처들의 주소를 많이 지정해야 한다. 이러한 출처에는 다음과 같은 것들이 있다.

## 1. IP주소와 URL

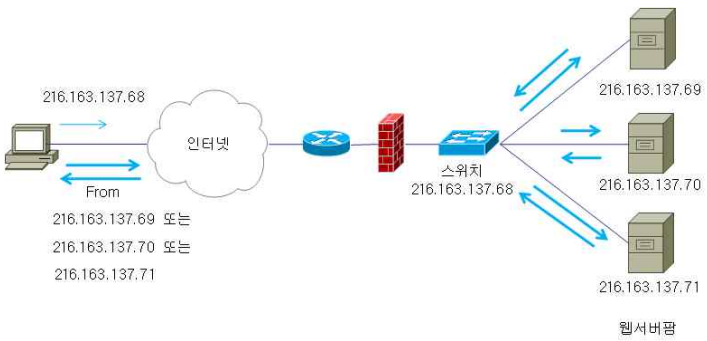
인터넷은 IP주소를 사용하여 작동한다. www.playboy.com과 같은 도메인 이름은 사람들이 숫자들을 잘 기억하지 못하기 때문에 존재하는 것이며, 사실, URL에 들어 있는 친숙한 '도메인 이름'은 실제로는 콘텐츠에 접속하기 전에 숫자로 된 IP 주소로 번역된다.

사용자도 항상 URL의 숫자 형태만을 사용할 수도 있으며, 그렇게 해서 친숙한 도메인 이름 형식만 검사하는 필터링 제품을 속일 수 있다. 예를 들어, http://www.playboy.com/과 http://216.163.137.68/이라는 두 개의 URL은 완전히 동등하며 상호전환 가능한 것이어서, 필터링 제품은 이 두 형식을 모두 차단할 수 있어야 한다.

인터넷 상의 컴퓨터 시스템은 도메인 이름을 가질 필요가 전혀 없지만, 큰 용량의 웹사이트를 더 작지만 크기가 같은 서버들 여럿으로 구성할 경우에 일반적으로 그렇게 한다. [그림 4-1]에 나오는 것처럼, 사용자가 하나의 컴퓨터 시스템처럼 보이는 곳에 검색 요청을 보내면 그 요청은 실제로는 그 사이트를 지원하는 다수의 컴퓨터 중 하나로 전달된다.

이 각각의 컴퓨터는 각기 고유의 IP 주소가 있으며, 인터넷에서 직접 접속할 수 있고, 요청한 콘텐츠를 보낼 줄 수 있다. 필터링 제품이 대표 IP 주소로의 접속은 차단할 수 있을지 몰라도, 사용자는 실제 서버들 중 하나로 직접 접근함으로써 동일한 콘텐츠로 접속할 수 있다.

필터링 제품이 이러한 사이트에서 나오는 콘텐츠로의 접속을 효과적으로 차단하려면 각각의 가능한 IP주소를 차단해야 하는데, 이것은 어려운 작업이며, 그 대상도 계속 움직이는 것이다. 이러한 상황은 웹 사이트의 소유자가 자신들의 콘텐츠가 필터링 되지 않게 하기 위해 애쓰고 있는 것은 아니며, 단지 그들의 방대한 수의 검색 요청을 다루기 위해 사용하는 기술의 결과일 뿐이다.




[그림 5] 대용량 웹 서버

웹 페이지는 인쇄한 페이지와는 달리 한 덩어리로 된 실체가 아니며, 대신 각각 고유의 URL이 있으며, 분리된 상태로 독립적으로 브라우저에 의해 호출되는 독립적인 요소들 여럿으로 구성되어 있다. 이 각각의 구성 요소들은 URL을 통해서 직접 접속할 수 있으며 따라서 필터링의 대상 후보가 될 수 있다. 예를 들어, 필터링 제품은 http://www.playboy.com/으로

의 접속을 차단할지 모르지만, 하위 URL인 http://www.playboy.com/girls/에 사용된 그림들로의 접속은 막지 않을 수도 있다.

이 문제에 대한 보통의 접근 방식은 www.playboy.com과 같이 도메인 이름이나 URL 내에 들어 있는 URL의 일부분을 이용해 차단하는 것이다. 이러한 도메인 이름은 매우 역동적이어서 한 사이트가 여러 개의 도메인 이름을 가질 수도 있고, 새 명칭을 재빨리 할당할 수도 있다.

Playboy와 같은 사이트라면, www.playboy.com 라는 이름은 서버를 가리키는데 사용할 수 있지만 ww2.playboy.com이나 ww3.playboy.com과 같이 고유한 도메인 이름을 가진 추가적인 서버들도 사용하여 실제 콘텐츠의 대부분을 공급할 수도 있다. 이렇게 다수의 서버를 사용하는 것은 필터링을 피하기 위함이 아니라 용량을 증설하기 위한 것이지만, 차단이 효과가 있으려면 이러한 잠재적인 이름들이 모두 필터링 목록에 올라 있어야 한다.

## 2절. 불법 · 유해 정보 차단 기술 동향

### 1. 차단(blocking)과 필터링(filtering)의 이해

‘차단’과 ‘필터링’이라는 용어는 종종 동의어로 사용되는데, 인터넷에서 이용 가능한 특정 형식이나 특정 부분의 콘텐츠로의 접속을 막는 기술을 가리킨다. 이 보고서에서 ‘차단’은 라우터[1] 수준에서 인터넷 트래픽을 주소에 기반하여 정지시키는 기술을, ‘필터링’은 내용에 근거하여 그 콘텐츠로의 접속을 막는 기술을 가리킬 때 사용할 것이다. ‘필터링’이라는 용어는 또한 차단과 필터링 둘 다를 가리키는 일반적인 용어로도 사용할 것이다.

모든 불법·유해 인터넷 콘텐츠 접속을 차단하는 것이 기술적으로 가능하다 하더라도, 어떠한 인터넷 차단 혹은 필터링 기술도 100% 효과가 있을 수는 없다. 의도적이고 정보력으로 무장한 공격자를 막아낼 수는 없지만 차단 기술의 대부분은 일반적인 불법·유해 정보의 차단 용도로 사용하는 데 문제가 없다.

인터넷 차단과 필터링 기술이 진정으로 효과가 있으려면 인터넷 콘텐츠가 배포되는 가능한 모든 경로를 다루어야 한다. 필터링 된 인터넷 서비스는 알려져 있는 불법·유해 웹 사이트뿐만 아니라 FTP, 대화방으로의 접속 또한 차단해야 한다. 완벽하게 ‘안전한’ 인터넷이 있다면 그것은 굉장히 제한적인 인터넷일 것인데, 신형 콘텐츠와 새로운 배포 기술이 새롭게 등장하는 경우에는 특히 그러하다.

---

1) 데이터 전송 시 최적경로를 선택하는 장치

비록 필터링 기술의 성능이 음란물이나 다른 불법·유해 콘텐츠로의 접속을 얼마나 잘 차단 하냐에 초점이 맞추어져 있기 하지만, 일부 제품들은 스포츠나 다른 취미와 같은 광범위한 콘텐츠의 차단 기능을 제공하기도 한다. 이러한 제품들은 업무 환경에서 사용하기 위한 의도로 만드는 것인데, 직원들이 업무와 관련 없는 활동을 위해 인터넷에 접속하는 것을 관리자들이 원치 않을 경우 그러하다. 그런 제품은 관리자들이 차단할 콘텐츠의 카테고리를 선택할 수 있는 기능을 제공한다.

## 2. 필터링 작동 방식

### 가. 식별 기술(Identification Techniques)

필터 제품들은 인터넷 사용자의 콘텐츠 접근을 제한하기 위해 두 가지 기본 기능을 수행한다. 이들은 차단(또는 허용)할 콘텐츠를 식별하고 해당 내용물로의 접속을 차단(또는 허용)한다. 콘텐츠 식별 방법은 필터 제품을 이용하는 것이 가장 일반적이지만, 이러한 차단 방법은 필터가 설치된 장치, 예를 들어 가정용 컴퓨터, ISP 서버 또는 휴대전화 네트워크 유형 등에 따라 차이를 보인다.

차단할 콘텐츠를 식별하는 방법은 인덱스 필터링과 분석 필터링 2가지다.

① 인덱스 필터링(Index Filtering) 기술 - 내용물을 '적합(good)' 또는'부적합(bad)' 콘텐츠 목록 중 하나에 포함시키는 기술이다.

② 분석 필터링(Analysis Filtering) 기술 - 콘텐츠 검사를 통해, 그 적용가

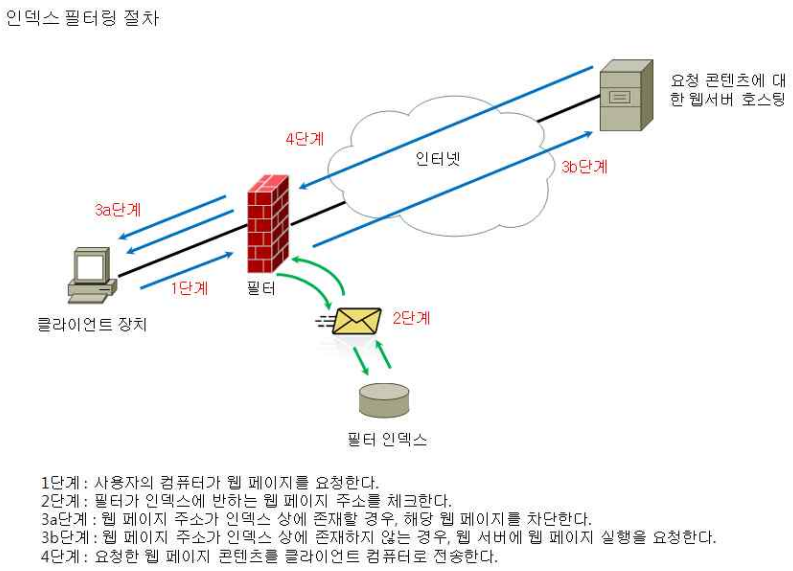
능성을 결정하는 기준을 얼마나 만족하는지 알아내는 기술이다.

위와 같은 식별 기술을 아래에서 더 자세히 검토해보자.

## 나. 인덱스 기반 필터링(Index-based Filtering)

인덱스 기반 필터링(Index-based Filtering) 기술은 웹 자원 인덱스(또는 리스트) 상에 포함된 사항을 근거로 웹 페이지 접속을 허용하거나 차단하는 기술이다 [그림4-2].

이 기술은 '허용리스트(whitelist)'와 '차단리스트(blacklist)'에 바탕을 둘 수 있다. 인덱스는 휴먼 검색(Human Search)과 콘텐츠 분석을 통해 수동적으로 개발할 수도 있고, 아래에서 논의한 바와 같이 분석을 기반으로 한 필터링 기술을 통해 자동적으로 개발할 수도 있다.




[그림 6] 인덱스 필터링 절차(Index Filtering Process)

**① 허용리스트 인덱스(Whitelist Indexes)**

허용리스트 기반의 인덱스 필터링 기술은 사전에 승인된 리스트에 존재하는 웹 자원에만 접속을 허용한다. 유아들이 다수의 인터넷 콘텐츠와 어플리케이션 접속에 방해가 되기 때문에 일반적으로 허용리스트는 유아용 필터 설치에 대한 기준으로 사용된다.

**② 차단리스트 인덱스(Blacklist Indexes)**

차단리스트 기반의 인덱스 필터링 기술은 사전에 차단리스트 컴퓨터가 정해진 사용자에게 부적당하다고 식별한 웹 콘텐츠를 제외한 모든웹 콘텐츠의 접속을 허용하는 기술이다.

**③ 카테고리 인덱스(Category Indexes)**

대부분의 상업용 필터 판매업자들은 폭력물, 포르노, 사교성 네트워크 사이트, 도박 또는 인종차별 내용물 등과 같이 부모(또는 기업용 필터의 경우, 기업주)가 차단하고자 하는 콘텐츠 유형과 일치하는 광범위한 주제별 범주에 따라 콘텐츠를 분류한다. [그림 4-3]에 카테고리 리스트의 예가 있다.

가정용 필터의 경우, 카테고리 리스트를 바탕으로 일반적으로 부모들이 필터 관리자가 해당 콘텐츠의 범주가 개별 사용자에게 적합한지 부적합한지를 선택할 수 있다. 선택한 카테고리에 포함된 것으로 분류된 필터 인덱스 상의 웹 자원은 해당 사용자의 목적에 따라 허용할 콘텐츠인 허용리스트(whitelist) 또는 차단할 콘텐츠인 차단리스트(blacklist)를 구성한다. 이에 더하여 몇몇 필터 제품들은 현재 시각 및 총 인터넷 접속 시간과 같은 부수적인 기준을 바탕으로 카테고리 차단을 허용한다.

특수 목적에 따라 설계된 필터는 더욱 제한된 인덱스를 만들 수 있다. 예를 들어, 영국의 IWF(Internet Watch Foundation)이 편성한 리스트와 같이, 주어진 구역내에 불법으로 판단된 내용물로 구성된 차단리스트에는 영국의 인터넷 사용자들이 아동 포르노 콘텐츠에 접속하지 못하도록 하는 인덱스를 사용하고 있다.

웹 콘텐츠 인덱스는 **IP 주소**[2]와 **URL**[3] 을 기반으로 내용물을 식별할 수 있다. 인덱스에 사용하는 주소 유형의 선택은 차단 행위에 포함되는 내용물의 범주에 중대한 영향을 미칠 수 있다. 본 장에서는 차단 기술에 입각하여 이를 보다 더 자세히 검토하고자 한다.

## 다. 분석 기반 필터링(Analysis-based Filtering)

분석기반 필터링 기술은 컴퓨터 소프트웨어를 사용하는 콘텐츠의 동적 분류방법을 말하며, 이는 인덱스 기반 필터링 기술의 단점을 보완하기 위해 등장했다. 다시 말해, 인덱스 기반 필터링 기술만이 사전에 등급제한 웹 페이지에 적용할 수 있다.

다음 사항을 포함하여 필터링 관리를 위해 도입된 여러 분석기술들에 대해 살펴본다.

---

2) IP주소(IP address)는 필수 네트워크 주소를 말한다. 이는 컴퓨터, 라우터, 프린터와 같은 전자장치가 인터넷 프로토콜을 사용하는 컴퓨터 네트워크 상에서 서로 식별하고 통신하는데 사용되는 유일한 식별자이다.

3) URL은 인터넷 자원을 식별하거나 명명하는데 사용하는 특수문자열(string)이며, 이는 URL의 위치를 통해 인터넷 사용자에게 (웹사이트, 그림, 기타 웹사이트 내 요소와 같은) 자원에 접속하는 방법을 제공해 준다.

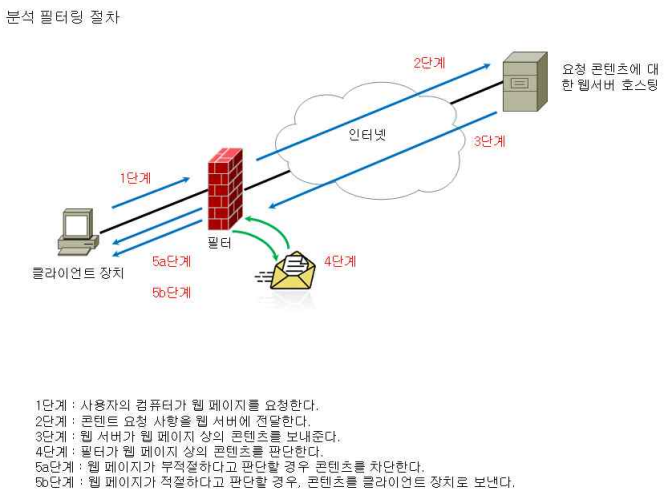
① ‘키워드 필터링’은 해당 사이트 상에 문제적 성격을 갖고 있는 단어들을 찾는다는 것이다. 이러한 단어들은 URL, 제목 또는 웹사이트 상의 텍스트 또는 이메일이나 채팅과 같은 통신 텍스트 상에서 발견할 수 있다. 이는 식별 단어를 포함하는 부적절한 사이트나 통신 유형과도 관계가 있고, 또한 부적절한 단어를 텍스트에 인용할 수 있는지의 여부를 결정하기 위한 복잡한 관용어구의 분석과 관계가 있을 수도 있다. 필터링은 가장 기본적인 형태로 단일 언어로 작업할 수 있지만, 또한 **과잉차단**을 야기할 수도 있다. 과잉차단이란 채택한 필터링 기술의 결과로서 의도치 않게 허용 가능한 콘텐츠까지 차단하는 것을 말하며, 키워드 필터링 기술이 안고 있는 문제점들은 다음과 같다.

o 키워드 필터링 제품은 단지 텍스트만 점검하며, 거절해야 할 만한 그림이 (부)적절한 텍스트를 동반하지 않는 경우에는 차단하지 못한다. 이것은 특히 음란물 콘텐츠의 경우에 특히 문제가 되는데, 일본이나 미국에서 나오는 성적으로 노골적인 사진은 우리나라의 음란물과 거의 비슷해 보이지만, 차단하는데 도움이 될만한 한글 키워드를 동반하지 않는 경우가 있다.

o ‘수용가능성’을 문맥 가운데서 분별해 낼 수 있어야 한다. 초기 키워드 스캐닝 제품은 ‘단순 무식하다’는 평가를 받았는데, 단어가 어떻게 사용되는지 관계 없이 무조건 차단했기 때문에 바람직한 콘텐츠로의 접속도 불필요하게 차단했기 때문이다. 고전적인 예로는 ‘유방암(breast cancer)’이라는 용어가 있는데, ‘유방(breast)’이라는 단어를 찾는 키워드 필터링 제품이 이 용어를 골라내어 결국 전체 사이트가 차단되는 결과를 낳았다. 또 다른 문제는 블랙리스트에 올라 있는 단어가 다른 단어에 포함되어 있을 경우에 발생하는데, 예를 들면, ‘sex’를 블랙리스

트에 올려놓은 키워드 필터링 제품은 'Middlesex(잉글랜드 남동부의 옛 주; 1965년 Greater London에 편입)'라는 단어가 포함된 문서들을 차단시켜 버릴지 모른다. 이러한 문제들을 해결하기 위한 시도로, 예를 들어, 한 페이지 안에 유인하는 단어가 특정한 개수 이상 있는 경우에만 차단한다든지 하는 방식으로 이러한 문제를 부분적으로 극복할 수 있을지 모르지만, 그 개수를 몇 개로 정할 것인지도 어려운 일이다.

키워드 필터링에 대한 지금까지의 논의는 주로 음란물 콘텐츠를 분류하는 문제에 집중되어 왔지만, 카테고리가 확장되면 될수록 이 분야는 문제가 가장 적은 카테고리일지 모른다. 많은 필터링 제품들은 사용자가 사실 차단되어야 하는 여러 카테고리를 선택하는 것을 허용하고 있으며, 성교육이나 도박이나 마약(drugs)과 같은 사이트를 키워드에만 의존하여 분류하려고 하는 것은 음란물을 분류하는 것보다 훨씬 문제가 복잡하다. 왜냐하면 이러한 사이트에 나오는 단어들은 거부할 이유가 없는 일반적인 용어에 훨씬 가까워 보이기 때문이다.




[그림 7] 분석기반 필터링 절차(Analysis Filtering Process)

② 프레이즈 필터링(구절) 필터링은 키워드 필터링을 좀더 정교하게 확장한 것이다. 프레이즈 필터링은 단어를 따로따로 보지 않고, 프레이즈의 부분으로 본다. 이렇게 하면 좀더 세밀한 분류가 가능하게 되며, '거대 유방'(hugebreasts)과 '유방암'(breastcancer)과 같은 프레이즈를 각각의 문맥 속에서 고려할 수 있게 된다. 이러한 접근 방식은 키워드 필터링만 사용했을 때보다는 좀 더 낫겠지만, 한 페이지를 차단하기 전에 거부할 프레이즈가 얼마나 많아야 하는가를 결정해야 한다든지, 영어 외 다른 언어로 된 사이트에는 쓸모가 없다는 것 등 여전히 관련된 문제들이 많이 있으며, 게다가 거부해야 하는 것으로 간주되는 모든 상이한 프레이즈를 열거해야 한다는 어려움까지 추가된다.

③ 프로파일 필터링(profile filtering)은 (형식, 관용구 또는 기술적 특징과 같은) 콘텐츠의 특성을 문제적 성격이 있는 것으로 판단한 다른 콘텐츠와 비교함으로써 요청한 콘텐츠의 범주를 분류하는 것이다.

예를 들어 성(性)적 이미지나 기타 성적 특징을 포함한 페이지 비율을 근거로 해당사이트가 상업적인 성인물 사이트일 가능성을 등급제하기 위해 웹 페이지 콘텐츠를 분석할 수 있다. 프로파일 필터링은 전산 자원 활용을 집약적으로 수행해야 한다. 인터넷 사용자가 요구한 대로 내용물의 실시간 분석보다는 리스트 편성을 목적으로 한 웹 자원의 오프라인 분석에 주로 사용할 수 있다.

④ 이미지 분석 필터링(Image Analysis Filtering)은 해당 이미지가 노출을 포함하는 여부를 결정하기 위해 다량의 표면 색상(Skin Tone)에 대한 이미지 검사를 포함한다. 이 필터링 방법 역시 전산 자원을 집약적으로

사용해야 한다. 허용가능 또는 불가능한(예를 들어 아동을 위한 수영강습 이미지를 생각해보라)노출이나 반라(半裸) 이미지를 잘 구별할 수 없다. 이 기술은 인종차별이나 폭력 관련 콘텐츠와 같이 노출과 다른 이미지가 아닌 성인 콘텐츠를 식별하는 용도로만 적용할 수 있다.

⑤ 파일 타입의 필터링(File type filtering)은 파일 확장자(file extension)를 근거로 주로 영화나 사진 파일과 같은 일정한 파일이나 매체 유형을 차단한다. 주로 악성 유료 콘텐츠를 전달하거나 과도한 대역폭을 이용하는 대용량 이메일 첨부파일에 주의를 기울이는 기업들이 이 기술을 사용한다.

⑥ 링크 필터링(Link Filtering) 기술은 요청한 웹 페이지의 성격을 검사하고 결정하기 위해 웹 페이지에 포함된 링크를 분석한다. 이 기술은 웹 페이지가 성인 콘텐츠와 같은 명백한 부적합한 콘텐츠로 알려진 다른 웹 페이지와 링크되어 있는 경우, 부적합한 내용물을 포함하기 쉽다는 전제하에 이용된다. 필터 판매업자들은 다른 기술을 사용하는 더욱 정밀한 조사를 보장할 수 있는 웹 페이지 식별에 가장 많이 사용된다.

⑦ 레퓨테이션 필터링(Reputation filtering)은 악성행위(malicious behaviors)에 대한 과거 및 현재 콘텐츠를 근거로 통신소스를 등급화하고 유해하거나 부적절한 통신소스에서 악성 콘텐츠가 발생할 가능성을 검토한다. 이 기술은 가장 보편적으로 스패머(spammer)가 보낸 스팸 메일을 여과하는데 사용한다. 하지만, 전자보안상의 위험과 온라인 사기를 공개하기 위한 콘텐츠에도 점차적으로 적용하고 있다.

많은 필터 제조업자들이 인덱스 기반 및 분석 기반 식별 기술 모두를 자

신의 제품에 시험하여 수익을 극대화 하고 두 식별 기술의 한계를 최소화 하고자 노력하고 있다. 인덱스 기반 필터링 기술은 주로 식별을 완료할 수 있는 속도 때문에 콘텐츠를 여과하는 1차적 수단으로 사용되고 있다. 분석 기반필터링은 일반적으로 전산상 훨씬 더 집약적이지만 신규 콘텐츠를 즉시 공개할 수 있다. 이런 점에서 필터 판매업자는 부적합 내용물에 대한 인덱스를 개발하기 위해 오프라인 상에서 종종 이 기술을 사용하고 있다. 그러나 경우에 따라 분석 기반 필터링 기술은 사용자가 활성 또는 비활성을 선택할 수 있는 옵션 기능을 갖고 있기도 하다.

## 3. 차단 기술(Blocking Techniques)

사용자가 콘텐츠를 식별하게 되면, 필터는 해당 콘텐츠의 접속을 차단해야 한다. 사용자가 콘텐츠에 접속하지 못하도록 하기 위해 채택한 차단 기술은 어느 정도 까지는 기존에 사용된 식별 기술에 의존할 것이다. 예를 들어, 차단할 콘텐츠를 식별하기 위해 인덱스 필터링 기술을 사용하는 경우에서는 콘텐츠에 대한 요청을 요청된 콘텐츠의 웹 서버 호스팅(web server hosting)으로 전달하지 않는다. 이에 비해, 분석 필터링 기술은 분석을 실행하기 위해 콘텐츠의 전달을 필요로 한다.

본 장에서는 패킷 필터링, 도메인 네임 서버(DNS) 변조, 포트 차단(port blocking), URL 필터링, 웹 프락시 캐싱(web proxy caching) 등을 포함한 콘텐츠의 접속을 차단하는 여러 기술들을 살펴본다.

### 가. 패킷 필터링(Packet Filtering)

패킷 필터링(Packet Filtering)은 IP 주소 차단(IP address blocking)에 활용하는 기술이다. 이 기술은 모든 네트워크 등급제에 이용할 수 있는 차단 기술로, 이를 통해 라우터나 다른 장치들이 패킷[4]이 지나간 헤더[5]를 검사하여 콘텐츠에 대한 요청의 허용 또는 거부를 결정한다.

헤더 내의 목적 IP주소(destination IP address)를 검사하여 인덱스에 따른 해당 IP주소의 차단 여부도 결정한다. IP주소를 차단하는 경우에서는 라우터가 데이터 요청사항을 콘텐츠 호스트로 전송하지 않는다. 그렇기 때문에 호스트 컴퓨터와는 관계가 없다. 이는 IP주소가 차단된 경우의 웹 콘텐츠 뿐만 아니라 채팅 및 전자메일을 포함하는 기타 모든 인터넷 어플리케이션과도 관계가 없다는 것을 의미한다.

IP 주소 차단은 일반적으로 매우 신속하지만, 그 성능 영향(performance impact)은 작다. 이러한 차단은 판단되지 않은 콘텐츠의 과잉차단(over-blocking) 현상을 초래할 수 있으며, 하나 이상의 웹 사이트에 동일한 IP주소를 사용하는 경우에도 무력하다.

동일한 IP주소를 사용하는 여러 웹사이트 중 하나가 차단리스트에 포함되는 경우, 이 기술은 동일 IP주소를 사용하는 모든 웹사이트에의 접속을 차단할 것이다. 게다가 그 웹 페이지들 중에 하나만이 부적합한 내용물을 포함한 것일 수도 있지만, IP 주소를 근거로 여러 사이트 전체의 차단을 야기할 것이다.

---

4) 패킷(Packet)은 네트워크로 전송할 수 있는 데이터로 포맷으로 구획된 전송 데이터를 말한다. 이는 헤더 데이터와 전송할 콘텐츠 모두를 포함한다.

5) 헤더(Header)란 패킷 초기에 포함된 정보를 말하며, 이는 패킷 처리에 대한 정보를 포함하고 있다. 편지봉투와 유사한 모양을 가진 헤더 정보는 무엇보다도 목적 및 소스 IP 주소를 포함한다.

## 나. DNS 변조(DNS Tampering)

DNS 변조(DNS Tampering)는 DNS 탈취(DNS hijacking)라고도 한다. 이는 개별사용자의 컴퓨터에 사용된 DNS 서버[6]가 도메인 차단여부에 대한 질문을 받은 후 웹사이트의 차단을 요청하는 사용자가 적합한 IP주소에 차단 명령을 내리지 않도록 정보를 변경하는 것을 말한다. IP주소 차단과 마찬가지로, 이 기술은 차단된 최상위 도메인의 하위도메인에 존재하는 모든 콘텐츠에 영향을 미치기 때문에 과잉차단을 초래할 수 있다.

## 다. 포트 차단(Port Blocking)

몇몇 필터들은 데이터를 전송할 수 있는 개별 포트[7]를 차단한다. 컴퓨터 상 서로 다른 종류의 프로그램이나 서비스는 데이터를 전송하고 수신하는데 서로 다른 포트를 이용한다.

예를 들어, 어떤 전자메일 프로그램은 110 포트(port 110)을 사용하는 반면, 웹 트래픽(web traffic)은 디폴트(default)를 통해 80 포트(port 80)를 거쳐 수신한다. 필터는 여러 프로그램들이 인터넷 접속을 위해 이용하는 포

---

6) 도메인명 시스템은 IP 주소 내에 'www.kcc.go.kr'과 같은 인터넷 도메인 명을 번역하는 시스템이다. DNS 서버란 이와 같은 종류의 번역을 수행하는 서버이며, ISP는 일반적으로 DNS 서버를 보유하고 있다.

7) 포트번호는 인터넷이나 기타 다른 네트워크 메시지가 서버에 도착하였을 때, 전달되어야 할 특정 프로세스를 인식하기 위한 방법이다. TCP와 UDP에서, 포트번호는 단위 메시지에 추가되는 헤더 내에 넣어지는 16 비트 정수의 형태를 갖는다. 예를 들면, 클라이언트가 인터넷 서버에 하는 요청은, 호스트의 FTP 서버에 의해 제공되는 파일을 요청하는 것일 수 있다. 원격지의 서버 내에 있는 FTP 프로세스에 사용자의 요청을 전달하기 위해, 사용자 컴퓨터에 있는 TCP 소프트웨어 계층은 요청에 부가되어지는 21 (FTP 요청과 관련하여 통상 사용되는 번호이다) 이라는 포트번호를 확인한다. 서버에서, TCP 계층은 21이라는 포트번호를 읽고, 사용자의 요청을 서버에 있는 FTP 프로그램에 전달할 것이다.

트를 차단하여 인터넷 콘텐츠에 접근하는 프로그램 이용의 차단을 목표로 하고 있다.

[표 2] 주요 포트 번호

| Port | Service | 설 명 |
|---|---|---|
| 20 | FTP | File Transefer Protocol - Datagram<br>- FTP 연결시 실제로 데이타가 전송되는 포트 |
| 21 | FTP | File Transefer Protocol - Control<br>- FTP 연결 시 인증과 컨트롤을 위한 포트 |
| 23 | Telnet | 텔넷 서비스로서 원격지의 서버의 실행 창을 얻어낸다. |
| 25 | SMTP | Simple Mail Transfer Protocol<br>- 메일을 보낼 때 사용하는 서비스 |
| 53 | DNS | Domain Name Service<br>- 이름을 해석하는 데 사용하는 서비스 |
| 69 | TFTP | Trivial File Transfer Protocol<br>- 인증이 존재하지 않는 단순한 파일 전송에 사용하는 서비스 |
| 80 | HTTP | Hyper Text Transfer Protocol - 웹 서비스 |
| 110 | POP3 | Post Office Protocol<br>- 메일 서버로 전송된 메일을 읽을 때 사용하는 서비스 |
| 111 | RPC | Sun의 Remote Procedure Call<br>- 원격에서 서버의 프로세스를 실행할 수 있게 한 서비스 |
| 138 | NetBIOS | Network Basic Input Output Service<br>- 윈도우에서 파일을 공유하기 위한 서비스 |
| 143 | IMAP | Internet Message Access Protocol<br>- POP3와 기본적으로 같으나, 메일을 읽고 난 후에도 메일은 서버에 남는 것이 다름 |
| 161 | SNMP | Simple Network Management Protocol<br>- 네트워크 관리와 모니터링을 위한 서비스 |

### 라. URL 필터링

가장 일반적이고, 효과적인 형태의 출처 기반 필터링은 사람이 읽을 수 있는 웹 페이지 주소인 URL에 근거를 둔 것이다. URL은 전체 컴퓨터 시스템이 아니라 각 웹 페이지의 이름이기 때문에, 이 방식을 사용하면 패킷 필터링보다 좀 더 세밀한 제어가 가능하다. URL 필터링은 화이트리스트와 블랙리스트 기법으로 모두 사용할 수 있다.

실제 URL 필터링은 개개의 페이지의 목록이 아니라 수용가능 혹은 수용불가 사이트 혹은 사이트 일부분의 목록에 근거해 있다. www.playboy.com과 같은 단일 웹 페이지도 수백 혹은 수천 개의 별개 페이지를 포함하고 있을 것이며, 각 페이지는 고유의 URL이 있다. 웹 페이지 이름의 계층적(왼쪽에서 오른쪽으로) 구조 때문에 필터링 제품 판매자는 전체 사이트 접속을 차단하거나, 특정 부분 URL을 사용하여 사이트의 일부만을 차단할 수도 있다.

플레이보이 사이트에 호스팅 되어 있는 모든 페이지 주소는 보통 www.playboy.com으로 시작하며, 이것만으로도 http://www.playboy.com/girls/index.html 와 http://www.playboy.com/girls/coeds/index.html 를 포함하고 있는 전체 사이트로의 접속을 차단하도록 필터링 리스트에 구체적으로 표시할 수 있다.

이러한 부분 이름은 어떤 수준에서도 구체화될 수 있어서 한 사이트의 일부분으로의 접속은 허용하면서도 다른 부분으로의 접속은 차단할 수 있다. 예를 들어, 판매자는 http://www.big.or.jp의 Web 서버에 호스팅 되어 있는 다른 사용자의 개인 홈페이지로의 접속은 차단하지 않으면서도 http://www.big.or.jp/~jrldr/index.html로의 접속은 차단할 수 있다.

부분 URL이름을 매칭시키는 것은 http://www.playboy.com과 같은 인식 가능한 '도메인 이름'을 URL 내에 사용하느냐에 달려 있다. 이러한 도메인 이름은 매우 역동적이어서 한 사이트가 여러 개의 도메인 이름을 가질 수도 있고, 새 명칭을 재빨리 할당할 수도 있다.

Playboy와 같은 사이트라면, http://www.playboy.com 라는 이름을 서버를 가리키는 데 사용할 수 있지만 http://ww2.playboy.com이나 http://ww3.playboy.com과 같이 고유한 도메인 이름을 가진 추가적인 서버들도 사용하여 실제 콘텐츠의 대부분을 공급할 수도 있다. naver, daum, HotMail, EBay와 같은 일부 대형 웹사이트들은 한 개의 도메인 이름 뒤에 수백 내지 수천 개 이상의 서버가 있다. 이렇게 다수의 서버를 사용하는 것은 필터링을 피하기 위함이 아니라 용량을 증설하기 위한 목적이지만, 차단이 효과가 있으려면 이러한 잠재적인 이름 혹은 IP주소가 모두 필터링 목록에 올라 있어야 한다.

http://www.playboy.com과 같은 도메인 이름은 단지 사람들의 편의를 위해 존재하는 것으로 그런 이름을 사용할 것인가의 여부는 선택할 수 있는 것이다. 인터넷으로 연결되는 각 컴퓨터 시스템은 실제로는 216.163.137.68 처럼 일반적으로 '점 표기 방식'으로 표현되는 32비트 IP주소로 구분된다. 예를 들어, http://www.playboy.com/과 http://216.163.137.68/이라는 두 URL은 완전히 동등한 것이며 상호 변환 가능하다. 결국, 필터링 제품은 두 가지 형태의 URL을 모두 차단할 수 있어야 하며, 도메인 이름을 점검하기 전에 IP 주소로 번역해야 한다면 블랙 리스트의 크기가 추가되거나 필터링 지연이 늘어나야 된다. 인터넷 상의 컴퓨터 시스템은 도메인 이름을 가질 필요가 전혀 없지만, 큰 용량의 웹사이트를 더 작지만 크기가 같은 서버들 여럿으로 구성할 경우에는 일반적으로 그렇게 한다.

이 각각의 웹 서버들은 보통 개별적으로 접속할 수 있기 때문에 필터링 제품에는 문제가 된다.

### 마. 서버 기반 콘텐츠 필터링

콘텐츠 필터링은 ISP나 조직들이 몇몇의 서버 기반 기술을 사용하여 수행할 수도 있는데, 이렇게 하면 비용과 효과 뿐 아니라, 인터넷 사용자의 경험에 따라 잠재적 손실에 차이가 있다. 서버 기반 필터링은 가장 안정적이며 우회하기 어렵다는 장점이 있다. 사용자는 특별한 소프트웨어를 가정의 컴퓨터에 설치할 필요가 없으며, 모든 인터넷 접속이 필터링을 통과해야 한다.

서버 기반 필터링의 일차적인 단점은 직면하게 되는 작업의 규모에서 기인한다. 가정용 필터링 제품은 한 명의 사용자를 위해서만 작동하므로 상당한 (기술적 의미의) 시간을 검색 요청과 웹 콘텐츠를 점검하는데 사용할 여유가 있다.

콘텐츠가 필터링 제품을 통과하여 검사를 받는 0.1초의 시간으로는 사용자 반응 시간에 부정적인 영향은 거의 없다. 프로세스 사용 시간이 동일한 0.1초라고 해도 동시에 수십만의 병렬 사용자를 위해 작동하는 ISP에는 적용할 수 없는 것이다.

#### ① 프락시서버

가장 일반적인 서버 기반 필터링 기술은 프락시 서버에 기반한 것이다. 프락시 서버는 사용자와 인터넷 사이의 경로에 자리하고서 지나가는 모든 검색 요청과 돌아오는 콘텐츠를 검사할 수 있다. 모든 클라이언트는 이 프

락시 서버를 통과해야 합당하게 인터넷에 접속할 수 있다.

웹 페이지나 ftp 파일에 접속하기 위해서 소프트웨어가 이 프락시서버를 설정할 것을 클라이언트에게 요구하는데, 최근에 나온 투명 프락시서버를 사용하면, 이용 가능성이 떨어지고 성능이 저하되기는 하지만, 이런 귀찮은 작업을 피할 수도 있다.

프락시 서버는 인터넷의 다른 위치에서 실제 서버의 '대리인' 노릇을 하는 범용 컴퓨터를 말한다. 주요 역할은 출입하는 트래픽을 점검하여 보안용 대문처럼 작동하고, 자주 접속하는 정보의 사본을 보관함으로써(캐싱, caching) 인터넷 접속 시간을 개선하는 것이다.

프락시서버는 캐싱 작업에 이용하는 것과 기본적으로 동일하고, 효율적인 메커니즘을 사용하여 필터처럼 작용할 수도 있다. 프락시 서버는 웹 검색 요청을 받고 나서, 사이트나 페이지의 허용 혹은 차단 목록에 있는 URL을 재빨리 살펴볼 수 있다.

프락시서버는 무엇을 차단할 것인지 선택할 수 있으며 단지 웹 페이지만이 아니라 특정 범위의 인터넷 기반 서비스로의 접속을 차단하거나 허용하도록 설정할 수도 있다. 원래 프락시서버는 콘텐츠를 필터링 하기 위해서가 아니라 보안이나 접속 시간을 개선하기 위해 설계한 것이다. 특히, 웹 사이트에 접속하기 위해 비표준적인 '포트' 번호를 사용하는 식의 단순한 대응 방법도 방어해 내지 못할 수 있다.

프락시 서버가 범용이고, 어떤 필터링 기법도 지원하도록 사용할 수 있지만, 실제적으로는 부분 URL에 기반한 블랙리스트 필터링과 같이 효율이

높은 기법으로 그 적용이 제한되어 있다. 프락시 서버는 매초 많은 수의 검색 요청을 다루어야하며, 일반적으로 속도가 느리고, 콘텐츠에기반한 필터링 도구를 운영할 수 있을 만큼 충분한 프로세스 시간이 없다.

ISP는 인터넷 접속을 필터링 하기 위해 특수한 캐싱 장비를 사용할 수도 있다. 이 특별히 고안된 장비란, 캐싱을 통해서 성능을 향상시키고 네트워크 비용을 저감하도록 최적화된 프락시 서버이다. 이 장비들은 범용 프락시 서버보다 빠르지만 필터링 능력은 훨씬 제한되어있다.

### ② 분석기반 필터링의 차단 방법(Blocking modes for analysis filtering)

분석 필터링 기술을 사용하는 경우는 요청된 정보를 회수하여 분석하며, 해당 사용자에게 부적합하다고 판단한 정보를 사용자에게 전송하지 않고 폐기한다. 이러한 분석 및 차단에는 두 가지 방식이 있다.

- 통과 필터링 방식(Pass-by Filtering)은 요청된 페이지를 웹상에 올리도록 허용하며 이를 사후 분석(later analysis)으로 표시한다. 해당 페이지가 필터 소프트웨어 사용자에게 적합할 경우, 추후에 이를 필터 판매업자의 분류 콘텐츠 인덱스에 추가시키고 이어서 이를 차단한다. 요청한 내용물에 접근시 지연되지는 않지만 사용자는 적어도 한 번 정도는 그러한 부적절한 콘텐츠를 검사해야 한다.

- 통과지점 필터링 방식(Pass-through Filtering)은 종종 '프록싱(proxying)'으로도 불린다. 필터 소프트웨어를 설치한 하드웨어의 처리능력에 의존하는 확실한 지연 분량을 알려줌으로써 해당 콘텐츠에 대한 분석을 완료할 때까지 요청된 웹사이트의 전송을 허용하지 않는다.

## 4. 차단 도구 설치 방법

이번 절은 가정용 컴퓨터, 이동전화, ISP 서버, 기업 및 검색 엔진(search engines) 등을 포함한 서로 다른 네트워크 위치에서의 필터링 기술 이행방식에 대해 살펴본다.

### 가. 가정용 컴퓨터 및 최종사용자용 필터

가정용 컴퓨터를 위해 설계한 필터는 가정용 컴퓨터(또는 컴퓨터)에 바로 설치할 수 있으며, 사용자의 유형에 따라 서로 다른 레벨의 필터링 기능을 제공하도록 제작되었다. 가정용 컴퓨터에 사용하는 필터는 '아동보호 소프트웨어(Parental control software)'와 '컴퓨터 보안 소프트웨어'로서의 기타 특징과 함께 하나의 제품으로 점차 일괄 포장하는 추세이다. 가정용 컴퓨터 필터의 범위는 단순 '추가장치'에서 인터넷 사용자가 접속할 수 있는 웹사이트를 제한하는 웹 브라우저, 특수 콘텐츠 및 어플리케이션에의 접속 차단, 감시(모니터링), 보고 및 시간 관리 기능 등을 포함한 포괄적인 아동보호기능에 이르기까지 매우 다양하다.

가정용 컴퓨터에 대한 하이브리드모델(Hybrid Models)[8] 필터가 존재하기는 하나, 가정용 필터링 소프트웨어의 대부분은 원격 컴퓨터(remote computer)와 연결되지 않아도 가정용 컴퓨터에 거의 독점적으로 작용하고 있다. 몇몇 필터 제품들은 소프트웨어 요소(software element) 뿐만 아니라 하드웨어 요소(hardware element)도 포함하고 있다.

---

8) 하이브리드 모델(Hybrid models)은 사용자 컴퓨터에 설치한 소프트웨어뿐만 아니라 (모바일 ISP 포함) ISP용 필터 섹션에서 기술한 바와 같이 원격 장치의 여러 기능도 포함하고 있다.

기업 환경에서 보다 더 일반적이긴 하지만, 가능성 있는 새로운 추세는 여러 컴퓨터의 홈 네트워크와 플러그로 연결한 장치에 필터링 소프트웨어를 공급하는 것이며, 이로써 가정용 컴퓨터와 모뎀 사이에 필터를 공급한다.

## 나. 이동전화용 필터(Mobile Phone Filters)

새로이 등장하고 있는 필터 제품은 (이동전화를 포함한) 휴대용 장치(mobile devices)에 사용하는 필터이며, 인터넷을 검색하고 음악, 게임 및 비디오 등을 다운받기 위한 용도로 사용하고 있다. 이동전화는 휴대용 장치의 성능에 따라 필터의 설치여부가 결정되는 한계를 갖고 있다.

이동전화는 일반적으로 다음과 같은 한계점을 지니고 있다.

- o 필터링 소프트웨어를 실행하기 위한 전산 능력(computational power) 및 배터리 전력(battery power)
- o 콘텐츠 인덱스를 보유할 만큼의 저장 용량(storage capacity)
- o 사용자가 필터를 손상시키지 못하도록 하는 보안 제어(security controls)

휴대용 장치 전용 필터 소프트웨어는 여전히 개발 중에 있다. 보다 강력한 기능과 보다 큰 저장용량의 휴대용 장치들이 출시되고 있기 때문에 휴대용장치 상의 필터를 사용하는 것이 더욱 용이해지고 있다.

## 다. ISP용(휴대용 ISP포함) 필터

필터링 솔루션은 ISP 레벨에서 실행할 수 있다. ISP 네트워크 내부에 있는

서버 상에 필터 소프트웨어를 설치하며 필터링은 사용자의 업스트림[9] (Upstream) 현상을 발생시킨다. 사용자는 필터링 기법을 실행하는 시스템에 물리적으로 접촉하지 않기 때문에 이러한 필터링 기법은 가정용 컴퓨터에 대한 필터링 기법 보다 안전하다고 할 수 있다.

ISP 담당 직원이나 사용자가 필터를 제어하기 위한 접근 방법을 관리하는지의 여부와 같이 해당 ISP가 필터의 설치 여부를 선택하는 방법에 의존함으로써 부모들은 자신이 가정용 컴퓨터에 아동보호기능 패키지를 설치하는 것보다는 차단된 콘텐츠 유형의 통제를 결정하는데 대한 관여를 줄일 수 있다.

역사상으로 볼 때, 인터넷 서버는 수많은 동시 사용자를 위한 콘텐츠의 동적 분석(dynamic analysis)에 필요한 추가적인 정보 처리량을(computational load)을 감당할 수 없기 때문에, 서버 레벨 필터링 기법(server level filtering)은 인덱스 기반 필터링 기법을 사용해야만 실행이 용이하다고 여겨져 왔다. 하지만 네트워크 상의 정보 처리 능력(computing power)이 개선됨에 따라, 몇몇 ISP는 분석기반 요소를 포함하는 필터링 기법을 사용하기 시작했다.

소비자에게 인터넷 접속 서비스(internet access)를 제공하고 있는 세계 여러 나라의 모바일 서비스 공급업자들 역시 모바일 서비스가 사용자의 이동전화에 도달하기 전에 인터넷 콘텐츠를 여과시켜 공급업자들의 이동 플랫폼(mobile platform) 상에 있는 ISP 레벨에 필터 제품을 설치하고 있다. 이 솔루션은 아동용 계정(children's accounts)에 대한 서비스 옵션으로, 일반적으로 부모들이 구입하고 있다.

9) 사용자의 컴퓨터가 해당 자료를 받았다는 신호를 서버에 보내는 활동

### 라. 기업용 솔루션(Enterprise solutions)

소기업, 학교 및 도서관 등의 비교적 작은 기업은 인터넷 접속에 사용하는 컴퓨터 상에 직접적으로 설치하도록 설계된 네트워크 솔루션 또는 소프트웨어 둘 중 하나를 선택하여 이용할 수 있지만, 반면 대기업의 경우는 전형적으로 네트워크 솔루션을 사용한다.

사용자 장치(user's device)에 설치한 소프트웨어 솔루션은 가정용 컴퓨터에 사용하는 필터와 유사한 방식으로 작동하는 반면, 네트워크 솔루션은 ISP용 필터링 기법과 유사하다.

기업 네트워크용 필터 제품은 중소기업, 대기업, 학교 및 도서관 등을 포함하는 모든 네트워크에 적용할 수 있다. 주로 하드웨어와 소프트웨어 모두로 구성된 솔루션으로 설치된 필터링 장치(filtering device)는 기업 네트워크, 전형적으로는 서버 상에 부착한다. 필터 제품 내부에서 사용되는 하드웨어는 복잡한 필터링 소프트웨어와 관련하여 민감한 요구사항을 제시하기도 한다.

### 마. 제3자용 필터(Third Party Filters)

필터링과 차단(blocking)은 제3자가 호스팅한 서버나 라우터(router) 상에서 수행할 수 있다. 이 솔루션은 사용자가 시작한 웹 리퀘스트(web requested) 또는 리퀘스트(request)에 답하는 콘텐츠의 전송 사이에 위치한 제3자 서버(third party server)를 필요로 한다. 이러한 트래픽 라우팅(routing of traffic)은 사용자의 웹 브라우저 또는 로컬 ISP 네트워크 라우팅 정책(network routing policies)의 형성과 같은 여러 가지 방법으로 진행할 수 있다.

제3자 필터링 기법은 때때로 기업의 고용주가 사무실을 비우는 경우 종업원에게 인터넷 트래픽을 여과할 수 있는 자격을 부여 할 때 사용한다. 고객을 위해 콘텐츠 필터링 기법을 외부에 의뢰하여 제작하고자 하는 ISP 또한 이 기법을 사용할 수 있다. 이 솔루션은 전 세계 어느 곳에서든지 사용할 수 있는 잠재적 이점이 있는 반면, 성능 저하를 피하기 위해 고객과 비교적 근접한 곳에 제3자 서버를 설치해야 하는 등의 단점도 있다.

**제3자 필터 프로세스(Third party filter process)**

1단계(Step 1) : 사용자가 콘텐츠를 요청한다.
2단계(Step 2) : 3자 필터에 콘텐츠 전송을 요청
3단계(Step 3) : 3자 필터(Third Party Filter) 전송을 웹 서버에 요청한다.
4단계(Step 4) : 3자 필터가 웹 서버에서 콘텐츠를 수신한다.
5단계(Step 5) : 3자 필터가 콘텐츠를 전달할 지에 대해 결정한다.
6단계(Step 6) : 사용자는 '접속 불가(ACCESS DENIED)' 메시지를 받거나 콘텐츠를 요구한다.

## 바. 검색 엔진용 필터(Search Engine Filters)

대부분의 주요 검색 엔진들은 고객 자신이 콘텐츠에 접속할 자격을 부여할 수 있도록 여과된 검색성능(search capabilities)을 제공한다. 비록 검색 엔진 공급자들이 필터가 100%의 효과를 내지 못한다고 강조하고 있음에도 불구하고, 주어진 검색 구역 내의 불법 콘텐츠 또는 검색 결과 아이들에게 부적절하다고 판단된 콘텐츠를 제거하기 위해 이 필터를 설계하였다.

몇몇 검색 엔진은 이미지나 기타 매체를 여과하거나 또는 웹 검색 결과 모두를 여과하는 옵션에 따라 주요검색 사이트 내에서  사용자가 필터링 프로그램(filtering preferences)을 우선적으로 설치할 수 있도록 허용하고 있고, 다른 검색 엔진들은 특히 아이들을 대상으로 설계한 개별 검색 페이지(separate search page)를 제공한다.

필터 판매업자들은 종종 자신의 제품에 이와 같은 안전 검색 필터(safe searches)를 통합시킨다. 여러 아동보호기능은 필터링 프로그램을 진행하는 동안 아이들이 이를 중단할 수 없도록 부모에게 안전 검색 필터를 사용할 수 있는 방법을 제공한다.

인터넷 서비스 제공자(ISP)는 고객이 콘텐츠 차단을 외주에서 수행하기를 희망한다. 이 해결책은 세계 어느 곳에서나 이용할 가능성이 있는 혜택인 반면, 수행 저하를 피하기 위해 제3의 서버가 고객에 아주 근접하여 배치하는 것이 바람직하다.

### 사. 차단 필터의 장점 및 제약 사항

차단 필터는 여러 콘텐츠의 위험을 나타낸다. 이 장에서는 수행 효과, 정확도, 우회와 관련하여 차단 필터의 장점 및 제약 사항을 논의한다. 차단 필터는 사용자가 부적절한 콘텐츠에 접근하는 것을 통제하는데 효과적일 수 있다. 그러나 일반적으로 차단 필터의 사용과 관련하여 여러 가지 제한 사항이 있다.

o 수행 효과 - 차단 필터는 인터넷 접속을 느리게 할 수 있다.
o 부정확성 - 차단 필터는 무해한 콘텐츠를 차단할 수 있다. (과잉 차단)

혹은 불필요한 콘텐츠를 차단하지 못할 수 있다. (차단 저하)

o 우회 - 사용자가 제약 없이 인터넷에 접속하기 위해 차단 필터를 우회할 수 있다.

o 방해 - 차단 필터는 보안 소프트웨어와 같이 다른 소프트웨어의 운영을 방해할 수 있다.

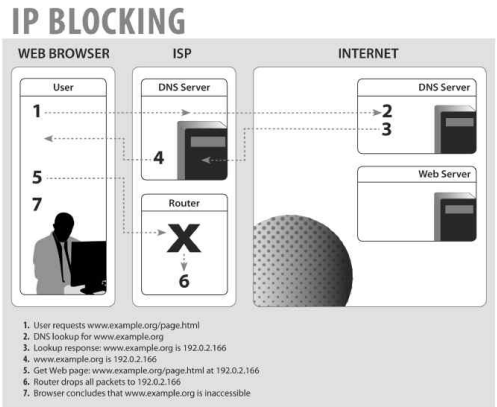
## 5. 국내 적용 차단 기술

### 가. IP 차단 방식

현재 친북 사이트는 IP방식으로 차단한다. IP방식은 중계(Proxy)서버를 이용하여 우회 접속이 가능하고 라우터에 별도의 부하를 주어 전체 인터넷 처리 속도 저하를 초래하기도 한다.

※ IP 방식 : 해외관문국의 인터넷 연결 장비인 라우터에서 해당 IP주소를 직접 차단하는 방식으로 프락시 등 중계 서버를 이용하여 우회 시 차단불가

※ Proxy서버 관련 목록은 P2P, 포털 등을 통해 쉽게 입수 가능



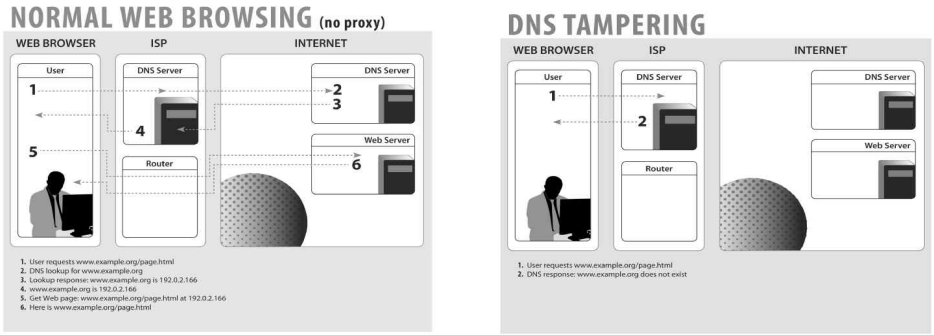

[그림 8] IP 차단 방법

## 나. DNS 변조 방식

도박, 음란 사이트는 대부분 DNS 변조 방식을 적용하여 차단한다. DNS 변조 방식은 이용자가 별도의 DNS 서버를 설정하거나 별도 소프트웨어(DNS Free 등) 이용하는 경우 쉽게 우회 가능하여, 차단을 효율적으로 수행하지 못한다.

※ DNS Free(DNS 자동변경 프로그램)는 포털 등에서 손쉽게 입수가능

※ DNS(Domain Name Sever)방식 : 인터넷주소를 IP주소로 변환하는 DNS서버에서 차단하는 기술로 Domain Name을 변경하거나 별도 DNS 사용시 차단불가




[그림 9] 정상적인 웹 접근 및 DNS 변조 방법

## 다. URL 차단 방식

IP 차단 방식과 DNS변조 차단 방식의 취약점을 보완하기 위해, 2008년 이후 ISP(기간통신사업자)들은 URL 차단 방식 필터링 장비를 도입하였다. 해외 관문국에 URL 차단 전용장비를 설치하여 불법 유해사이트를 필터링 하는 방법으로 다음과 같은 장점이 있다.

① Domain과 IP 단위의 차단뿐만 아니라 하위 디텍토리 및 페이지단위로 차단이 가능하다. (예 : www.big.or.jp/~jrldr/index.html)까지 차단 가능

※ 친북사이트 중 선군정치연구소 등 2곳은 각각 geocities.com과 yahoo.com의 하위 디렉토리로 구성되어 해당 메뉴를 차단할 경우 yahoo 등 전체 사이트가 차단되는 문제가 있다.

② URL 차단은 국제 게이트웨이에서 특정 IP 패킷에 목적지 IP 주소, 프락시서버 주소 등 관련 내용을 함께 보고 차단여부를 결정할 수 있어 DNS우회, 프락시 서버 등의 우회 접속도 차단가능하다.

※ 프락시서버를 이용할 경우 IP 패킷에 프락시서버와 목적지 주소가 함께 포함되어 있어 URL 차단장비에서 차단가능

③ 도메인 네임서버나 라우터에 별도의 부하를 주지 않기 때문에 인터넷 속도에 영향이 없어 ISP 입장에서도 IP 차단시 우려되는 속도 저하 문제와 전국에 산재된 DNS 서버에 대하여 수작업 입력에 따른 관리상의 부담을 줄일 수 있다.

※ 인터넷접속 기간통신 사업자의 URL 차단장비 도입 현황

[표 3] URL 차단장비 도입 현황

| 사업자명 | 회선용량 | 회선수 | 장비수량 | 장비 제조사 | 비 고 |
|---|---|---|---|---|---|
| KT | 10G | 24 | 6 | 아라기술 | |
| | 2.5G | 16 | 2 | 아라기술 | |
| | 1G | - | - | | |
| LG데이콤 | 10G | 6 | 6 | 아라기술 | |
| | 2.5G | - | - | | |
| | 1G | - | - | | |
| SK브로드밴드 | 10G | - | 5 | 아라기술(3대)<br>시큐아이닷컴(2대) | 10G S/W 접선 |
| | 2.5G | | | | |
| | 1G | 42 | | | |
| 온세텔레콤 | 10G | | | | |
| | 2.5G | | | | |
| | 1G | 4 | 2 | 아라기술 | 1G S/W 접선 |
| 세종텔레콤 | 10G | | | | |
| | 2.5G | | | | |
| | 1G | 8 | 4 | 아라기술 | |
| SK네트웍스 | 10G | | | | |
| | 2.5G | | | | |
| | 1G | 8 | 4 | 아라기술 | |
| 삼성네트웍스 | 10G | | | | |
| | 2.5G | | | | |
| | 1G | 8 | 2 | 시큐아이닷컴 | |
| 드림라인 | 10G | | | | |
| | 2.5G | | | | |
| | 1G | 2 | 3 | 아라기술 | |

## 3절. 불법 · 유해 정보 차단 우회 기술 동향

### 1. 차단 우회 기술 종류

필터링 우회의 용이함은 사용자의 기술지식에 따라 달라진다. 우회가 가능한 방법은 필터링을 배치하는 위치에 따라 달라진다. 예를 들어, 가정용 컴퓨터에 설치한 아동보호소프트웨어를 우회하는 방법은 ISP 서버에 위치한 필터링 소프트웨어를 우회하는 방법과 다를 수 있다. 필터링 환경에서 작업 방식을 우회할 수 있는 방법은 여러 요소 중에서도 배치된 필터링의 성질과 설치방식에 따라 달라질 것이다. 필터링 판매자는 이러한 모든 우회 방법을 인지하고 있다. 우회 방법이 변경되거나 그 응용 방법이 확대되면서, 필터링 판매자는 방지를 우회하기 위한 시도를 제한하는 인덱스나 분석 기술을 업데이트한다. 어떤 우회방법은 컴퓨터를 통제하거나 필터링 소프트웨어를 피하여 사용자의 컴퓨터에 설치한 필터링을 우회하도록 설계된다. 예를 들면 다음과 같다.

#### 가. 사용자 컴퓨터 필터링 우회 방법

관리자 비밀번호 - 필터링 소프트웨어를 원격 서버가 아닌 컴퓨터에 설치하는 경우에, 사용자가 필터링 소프트웨어를 통제하여 필터링을 우회할 수 있다. 이것은 사용자가 아닌 컴퓨터 관리자로서 로그인하여 달성할 수 있다. 이는 일반적으로 사용자에게 컴퓨터와 필터링 관리자의 사용자 이름과 비밀 번호를 요구한다.

부팅 디스크 - 필터링 소프트웨어를 원격 서버가 아닌 컴퓨터에 설치하

는 경우에서, '부팅 디스크'의 사용으로 소프트웨어의 완벽한 우회가 가능하다. 사용자는 CD나 운영 시스템과 인터넷브라우징 소프트웨어에 포함된 제거 가능한 저장장치에서 컴퓨터를 부팅할 수 있다. 컴퓨터 하드웨어에 설치된 운영 시스템과 필터링소프트웨어는 적재(load)되지 않을 것이고 인터넷 접속에 제한을 받지 않을 것이다.

## 나. 인덱스 기반 필터링 우회 방법

어떤 우회 방법은 분석기반이 아니라 인덱스 기반 필터링 기술로 작동된다. 이경우는 보통 요청한 콘텐츠의 IP 주소나 URL을 숨겨서 작동한다.

익명자(아노마이저)는 인덱스 필터링 기술을 우회하고 사용자 요구의 콘텐츠 게이트웨이로서 작용하는 프락시 서버의 한 형태이다. 필터링 네트워크에 있는 사용자는 브라우저가 사이트에 직접 접속하지 않고 사이트에 접속하는 프락시 서버를 통해 웹 통신(traffic)의 루트를 정하도록 설정한다. 필터링 소프트웨어는 요청하는 웹사이트가 아닌 익명자의 URL이나 IP 주소만을 본다. 그래서 익명자를 차단하지 않을 경우 콘텐츠 필터링을 수행할 수 없다.

번역 소프트웨어 사이트는 텍스트 웹 콘텐츠를 한 언어에서 다른 언어로 번역하기 위해 사용한다. 사용자가 번역되는 웹사이트의 URL에 들어간다. 그리고 번역 소프트웨어는 자신의 페이지 내에서 번역된 정보를 제시한다. 이 기능은 익명자의 방법과 유사하게 사용된다. 번역 사이트의 URL만을 보고 필터링에서 웹사이트의 자원 URL을 숨긴다.

검색 엔진 캐싱(caching) - 어떤 검색 엔진은 '캐싱' 버전이라고 알려진

웹사이트의 저장된(archived)사본에 접속하도록 제공된다. 프락시와 번역기처럼, 어떤 검색 엔진 제공업체는 숨겨진 콘텐츠의 접속을 허용하고 자신의 페이지 내에서 나타낸다. 이와 유사하게 인덱스 필터링에서 차단된 콘텐츠의 자원을 숨길 수도 있다.

거울(mirror)은 이중 웹사이트로 보통 접속한 웹사이트를 자주 관리하여 서버에 있는 통신 로드를 줄이기 위해 만들어졌다. 차단된 콘텐츠에 접속하고자 하는 사용자는 차단된 사이트의 거울에 접속할 수 있다. 이는 거울 사이트의 특정 콘텐츠가 최우선 사이트에 추가된 인덱스의 목록에 없을 경우 인덱스 필터링을 우회한다.

추가 도메인 이름 - 콘텐츠 운영자는 콘텐츠를 운영하는 동일한 IP 주소를 지정하는 복합 URL을 사용하여 필터링을 피할 수 있다. 이것은 IP 주소에 기반을 둔 필터링 기술에 영향을 미치지 않는다. 특정 콘텐츠의 대안이 되는 주소가 필터링 인덱스의 목록에 없을 경우에는 URL이나 도메인 이름에 기반을 둔 필터링을 우회한다.

### 다. 소프트웨어를 이용한 우회 방법

Freenet은 1999년 이안 클라크가 창안한 것이다. Freenet은 인터넷의 최상층 부에서 탈 중심화된, P2P(Peer-to-peer) 네트워크로 만들기 위해서, 온전히 익명화된 정보의 출판, 저장 및 검색을 지원하기 위한 의도로 설계되었다. Freenet은 그 때 이후로 계속 개발이 진행 중이며, 수많은 개정을 거쳐 왔다. 현재 버전은 Freenet 0.7.5이다.

Freenet은 다른 P2P 시스템 중에서 잠재적인 차단 반대 시스템으로 두드

러지는데, 중앙 통제가 없다는 면에서 여타 P2P 네트워크와는 확연한 차이를 보인다. 대부분의 P2P 시스템들, 특히 Nepster나 Gnutella와 같은 인기 있는 파일 공유 네트워크들은 동등 계층 컴퓨터(peer)들이 다른 동등 계층 컴퓨터에 고지하거나 위치를 알아 낼 수 있는 중앙 디렉토리 서비스에 의존한다.

Freenet 구조는 차단 공격에 약한데 중앙 디렉토리 서버가 쉽게 차단되어 전체 시스템이 못쓰게 될 수 있기 때문이다. Freenet은 네트워크 간의 문서를 찾아내는 데 내부 간 노드 통신과 참조를 사용한다. Freenet 상의 정보는 고정된 컴퓨터들에 저장되지 않는다. 정보는 사용 경향에 따라 네트워크 내에서 이동할 수 있다. 콘텐츠 출판자와 독자 모두의 익명성을 달성할 수 있으며, Freenet 노드 수가 많을 때 탈중심화된 P2P 구조를 통해 차단을 좌절시킨다.

초기 단계에는 차단 반대 공동체의 많은 단체들이 Freenet이 인터넷 차단에 대해 승리를 거둘 수 있는 궁극적인 무기가 될 것이라는 희망을 품었었다. 어떤 단체는 Freenet을 홍보하는 중국어 웹사이트를 만들기까지 했다. 하지만, 현재까지 Freenet의 유용성과 성능은 만족스럽지 못하며, 사용자 기반에 있어서도 폭발적인 증가를 달성하지 못했다.

Freenet은 월드 와이드 웹의 풍부한 콘텐츠와 동시에 사용할 수 없다. 사용자는 네트워크에 콘텐츠를 올리기 위해서 반드시 Freenet의 출판 시스템을 이용해야 한다. 이러한 제한들 때문에, Freenet이 당장은 차단과의 대결에서 중요한 역할을 수행할 것이라고 기대하기 어렵다. 적극적으로 홍보하거나 사용자를 지원하지 않는 이상, 시장에서 Freenet이 차지하는 비율은 크게 증가하지 않을 것으로 예상된다.

Triangle Boy는 원래 세이프웹(Safeweb, http://www.safeweb.com)에 의해 개발되어 2000년 10월에 시장에 나온 Triangle Boy는 2001년 초에 CIA의 벤처 자금 회사인 In-Q-Tel이 이 기술에 투자하기로 결정했을 때 언론의 집중적인 조명을 받았다. Triangle Boy는 사우디아라비아와 중국에서 제한된 규모로 설치되어 사용되었다. 중국은 2001년 3월 세이프웹을 차단하는 데 성공했다.

아마도 운영에 헌신적인 노력을 기울이지 않았기 때문에, Triangle Boy는 인기를 얻지 못했고 2003년 시멘텍(Symantec)社에 인수되었으며, 이 회사는 Triangle Boy나 차단 우회 기능을 지원하는 데 별다른 관심이 없어 보였다.

수명이 짧았음에도 불구하고 Triangle Boy는 차단 반대 기술계에 오래 가는 자취를 남겼다. 기본적인 발상은 이렇다. 세이프웹은 사용자에게 웹페이지를 따오기 위해 웹 프락시와 유사한 기능을 가진 서버들을 제공한다. 사용자는 일반적인 웹 프락시처럼 차단을 당하기 쉽도록 세이프웹의 프락시 서버로 직접 접속하지는 않는다.

사용자는 일단 노드라고 부르는 제3자 컴퓨터에 접속하는데, 컴퓨터들은 Triangle Boy 소프트웨어를 실행하고 사용자의 요청을 세이프웹의 프락시 서버들로 전달한다. 세이프웹의 서버들은 트래픽을 사용자에게 직접 돌려주는데, 트래픽이 노드에서 돌아오는 것처럼 가장하면서 그렇게 한다. 차단의 관점에서, 사용자들이 단지 노드와 상호작용하는 것처럼 보인다. 세이프 웹의 서버들은 차단도구에 보이지 않는다.

이론적으로, 동적인 IP 주소를 가진 노드를 많이 실행할 수 있는 충분한

수의 자원자가 있다면, 차단도구가 이 모든 노드를 차단하기란 극히 어려운 일이다. 하지만 운영에 있어서, 이 기술을 개발하는 것보다 충분한 노드를 지원할 자원자를 찾는 것이 더 어려운 일이며, 이것이 Triangle Boy가 임계 사용자 수에 도달하지 못한 주요 이유들 중의 하나이다.

Triangle Boy가 처음 등장했을 때에는 차단 기술이 충분히 정교한 수준에 이르지 못했다. Triangle Boy의 설계 목표는 단지 IP 차단에 대항하기 위한 것이었다. 이것은 DNS 납치나 콘텐츠 필터링이 등장한 후기에는 효과가 별로 없었을 것이다. 그렇지만 Triangle Boy는 인터넷 트래픽을 비껴가고 IP 차단에 대항한 첫 번째 효과 있는 사례라고 할 수 있다.

GTunnel은 가장 초기의 스마트 프락시 시스템 중의 하나로, 2001년 Garden Networks (http://www.gardennetworks.org)가 발표했다. 이것은 UltraSurf와 DynaWeb과 더불어 전 세계에서 가장 인기 있는 차단 반대 시스템 중의 하나다.

많은 인터넷 사용자들이 애정을 가지고 있으며, 이 세 가지 차단 반대 프로그램을 '무사'라고 부른다. 한 자발적인 자원자 팀이 적극적으로 이 소프트웨어를 개선하고 지원해 왔다. 초기 소프트웨어는 Garden 3.5 버전까지 개발되었으며, 현재 소프트웨어는 GTunnel이라 부른다.

GTunnel은 단순한 웹 프락시의 개념에 기초하여 사용자의 컴퓨터에서 실행되는 약간의 클라이언트 소프트웨어로 구성되어 있다. 이 클라이언트 소프트웨어는 똑똑하게 작용하여 검열 반대 기능의 보안과 유용성을 개선한다. 이것은 능동적으로 해외의 GTunnel 프락시 서버의 위치를 파악하여 IP 차단을 피하고, 콘텐츠 필터링을 피할 수 있도록 사용자의 트래픽을 암

호화하고, DNS 납치에 대항할 수 있도록 URL 재작성 기술을 사용한다.

GTunnel 소프트웨어는 보안을 증대시키기 위해 사용자 PC의 검색 기록을 깨끗이 삭제할 수 있다. 이러한 기능은 사용자를 방해하지 않고 자동적으로 실행되며, 기술을 잘 모르는 사용자들에게 적합하다. GTunnel은 잘 관리되는 프락시 서버를 콘텐츠 캐싱 없이 해외에 여럿 보유하고 있는 것 같으며, 이는 사용자 경험을 크게 개선할 수 있는 요소이다.

GTunnel의 기술은 방화벽 차단에 대해 승리를 거두어 왔다. GTunnel이 방화벽의 목표물 목록 맨 위에 있고, 많은 수의 사용자를 매혹시켜 왔지만, 차단 국가들(예를 들면, 중국) GTunnel의 파이프를 통해 방화벽을 통과하여 정보가 흘러가는 것을 중단시킬 수 없었다.

GTunnel이 성공한 것은, 특히 중국의 경우에 주로 유용성과 운영 지원 덕택이다. 초기 단계에서부터 중국어를 지원했으며, 헌신적인 지원 팀이 이 소프트웨어의 존재를 차단 반대 통신 플랫폼(www.qxbbs.org)에 알렸다. GTunnel의 기술과 소프트웨어는 성숙 단계에 이르고 안정화 되었다. GTunnel을 더 강하게 만들 수 있도록 더 많이 운영을 지원하고 자원을 확장하기를 권한다.

UltraSurf는 실리콘밸리 기술자 단체에 의해 설립된 인터넷 기술 회사인 UltraReach의 중요한 차단 반대 제품이다. 2002년 이래로, UltraReach는 핵심 사업의 초점을 차단 반대 기술을 개발하는데 맞추어 왔으며, 현재 내놓은 차단 반대 소프트웨어는 UltraSurf 9.91이다.

UltraReach는 글로벌 인터넷 자유 기술(GIFT, Global Internet Freedom Technology) 플랫폼에 기반하여 매출을 확대해 왔으며, 최근에는 UltraMail이라 부르는 보안이 되는 이메일 서비스와 중국 사용자를 위한 보호된 웹 포탈(http://www.UltraReach.net, 혹은 http://www.wujie.net)을 제공한다. UltraSurf의 중국어 명칭인, Wujie(無界)는 경계가 없음을 뜻하는데, 중국 인터넷 사용자 사이에는 흔히 사용되는 단어가 되었다. UltraSurf는 '삼무사' 중 하나인데, 부분적으로 이는 사용자 친숙성과 사용자 중국어 지원 덕분이다.

UltraSurf는 중국의 차단기술과 UltraReach 사이의 계속 되는 전투에 의해 발전하게 된 강력한 차단 반대 시스템이다. UltraSurf는 걸음마 단계부터 중국 공산당이 제일 좋아하는 목표물이 되었다.

무료로 사용할 수 있는 이 소프트웨어는 분석되고, 망가뜨려지고, 속임수를 당했으며, 지원 네트워크 인프라는 계속해서 공격을 받아왔다. 이러한 요인들이 UltraSurf가 지금의 높은 수준의 정교함과 명성에 이르도록 촉진시켰다.

현재 나와 있는 버전인 UltraSurf 9.91은 완전히 투명한 복합 프락시 시스템과 마이크로소프트 인터넷 익스플로러 플랫폼의 높은 암호와 수준을 시행한다. UltraSurf 9.91을 이용하면, 이 소프트웨어가 보이지 않게 가장 빠른 프락시 서버를 자동적으로 찾아 주는 동안, 사용자는 일반적인 인터넷 익스플로러를 사용하듯이 어떤 웹사이트든지 자유롭게 검색할 수 있다.

이것은 강력한 부하 조절 기능(병렬처리 컴퓨터에서 프로세서들 간에 작업들을 고루 분배하는데 기능)과 무정지 기능(어떤 한 부품에 장애가 생겼

을 때 예비 부품이나 절차가 즉시 그 역할을 대체 수행함으로써 서비스의 중단이 없도록 하는 기능)을 지원하며, 심지어 인프라 구조와의 통신을 추적하려는 어떠한 시도도 좌절시킬 수 있는 유인 메커니즘도 사용한다.

DynaWeb은 Dynamic Internet Technology(DIT, http://www.dit-inc.us/)에 의해 제공되는 차단 반대 서비스 도구이다. DIT는 원래 2001년 미국 정보기관이나 비정부기구들이 중국으로 이메일을 전달할 수 있게 하는 서비스를 제공하기 위해 설립되었다.

2002년에, DIT는 DynaWeb의 구조를 이용하여 차단 반대 서비스를 제공하기 시작했으며, UltraSurf처럼 DynaWeb도 중국의 차단기술을 관통하는 노력에 있어서 최고 경쟁자 중 하나가 되었다. DynaWeb과 중국 차단기술 사이의 전쟁은, 비록 일반 대중에게 거의 보이지는 않지만, 흥미진진하고, 역동적이며 극적이었다. 요즈음 DynaWeb은 사용자가 인터넷을 자유롭게 접속할 수 있도록 가장 넓은 범위의 옵션을 제공하며, 중국 사용자에 의한 것만 해도 매일 평균 5천만번의 조회수를 지원한다.

DynaWeb은 웹 기반 차단 반대 포털이다. 사용자가 웹 브라우저를 DynaWeb의 URL 중 하나로 지정하면, 링크로서 차단이 가장 많이 되는 웹사이트인 http://www.dongtaiwang.com에 있는 것과 비슷한 페이지가 나타난다.

사용자는 이 페이지의 네모 안에 어떤 URL이든지 입력하면, DynaWeb은 그 페이지를 따와서 즉시 사용자에게 보여준다. 아무 소프트웨어도 필요 없고, 사용자 컴퓨터의 설정을 약간이라도 바꿀 필요도 없다. 중국 네트워크 경찰이 DynaWeb의 포털 웹사이트를 면밀히 감시하면서 찾아내는 즉시 차

단해 버리기 때문에, DynaWeb은 매우 동적이어야 한다.

언제나 IP 차단과 DNS 납치에 대항하기 위해 IP와 DNS 도메인 이름이 각기 다른 수백 개의 미러 사이트[10]가 있다. DynaWeb은 미리 대비할 수 있게 각각의 미러 사이트의 차단 상황을 모니터링하는 메커니즘이 있으며, 차단이 발견되면 즉시 IP와 DNS 도메인 이름을 바꾸어 버린다.

사용자가 이처럼 동적인 인프라구조에 계속해서 접속할 수 있도록, DynaWeb은 사용자를 업데이트를 위한 다양한 방법을 보유하고 있다. 예를 들어, 사용자는 DynaWeb의 메신저 계정으로 메시지를 보낼 수 있으며, 즉시 DynaWeb 포털의 새 주소를 받을 수 있다. 이메일로도 비슷하게 할 수 있다.

이러한 다양하고 동적인 방법을 통해 DynaWeb은 DynaWeb의 주소를 수집하려는 차단도구의 시도보다 더 똑똑하게 작동하는데, 이는 각각의 사용자가 DynaWeb 주소의 (상이한) 부분 집합만을 받게 되기 때문이다. 자동 차단 탐색 기능과 빠른 반응 속도와 덕택에 중국 측에서 차단하려는 시도를 좌절시키고 있는 것으로 보인다.

DynaWeb도 FreeGate(현재 버전, 6.80)라는 아주 작은 크기의 소프트웨어를 제공하는데, 이것은 DynaWeb의 구조에 직접 붙어 있으며 사용자가 동적인 채널에 자동적으로 접속 되어 있을 수 있도록 해준다. FreeGate 안에 제로데이 공격 취약성을 이용하는 기능이 내장되어 있음을 암시하는 증거들도 있다. DynaWeb 서비스에 더해, DIT는 변화하는 인터넷 검열 작동에 관련된 조언과 기술 분석을 제공한다.

---

10) 다른 컴퓨터 서버를 복사해 놓은 웹사이트 또는 컴퓨터 파일서버

최근 GPass와 FirePhoenix 라는 두 개의 새로운 소프트웨어가 등장했다. 둘 다 윌드게이트 사에 의해 2006년 여름에 발표된 것이다. 윌드게이트는 새로 떠오르는 조직으로 특히 억압정권 하의 사용자들을 위한 광범위하고 신뢰할 만한 인터넷 플랫폼인 Edoors(http://www.edoors.com)을 구축하는 데 초점을 맞추고 있다.

대중적인 서비스인 이메일과, 블로그, 포럼 및 사회 네트워크를 지원함으로써 자유롭고 안전하게 접속하고 정보를 출판할 수 있게 하는 것이 목표이다. 이의 일환이라고 할 수 있는 GPass와 FirePhoenix는 둘 다 Edoors와 다른 인터넷 서비스로의 접속을 원활하게 해주는 차단 반대 시스템이다.

GPass와 FirePhoenix는 멀티 프로토콜 보호라는 경향을 세웠다. 현재 대부분의 차단 반대 도구들은 웹 트래픽에 대한 보호만을 제공하는데, 이것은 사용자가 특정 웹사이트를 방문할 경우에만 사용자 프라이버시나 안전성이 보호된다는 뜻이며, 이메일, 메신저, 오디오/비디오 스트리밍 등 웹 프로토콜이 아닌 다른 응용의 경우 여전히 검열을 받고 있음을 의미한다.

GPass는 웹 서핑(예, HTTP) 뿐만 아니라 멀티미디어 스트리밍(예, MMS 프로토콜), 파일 전송(예, FTP), 메신저 등의 많은 응용 프로토콜을 지원한다. GPass 소프트웨어는 직관적인 인터페이스를 사용자에게 제공하기 때문에 어떤 응용 프로그램을 보호받을 것인지 선택 할 수 있다. GPass는 사용자를 방해하지 않으면서도 서버를 찾고 연결해 주는 일과 트래픽을 암호화하고 차단도구를 피해가는 일을 해준다. GPass는 GTunnel, UltraSurf 및 DynaWeb의 경험을 바탕으로 만들어진 것 같다.

FirePhoenix가 검열을 피하는 방식은 현존하는 다른 도구들과 훨씬 더 큰 차이를 보인다. 이것은 가상 사설망(Vitual Private Network, VPN)에 기반한 최초의 차단 반대 도구이다. FirePhoenix는 이제까지 차단 하에 있는 사용자에게 제공된 것 중 가장 강력한 보호를 제공한다. 설치 후, 사용자 컴퓨터의 FirePhoenix 소프트웨어는 가상 네트워크 카드를 발생시키며, FirePhoenix 소프트웨어가 차단도구 바깥쪽에 있는 수많은 FirePhoenix 서버들 중 하나에 접속하기만 하면, 가상 네트워크 카드가 실제 네트워크 카드와 동일하게 기능하게 되지만, 네트워크 케이블은 FirePhoenix 서버의 지역 네트워크에 꽂혀 있는 상태로 있다. 사용자에게 사용자 컴퓨터가 해외의 널리 공개된 네트워크에 직접 접속되어 있는 것과 같으며, 차단 도구는 없는 것과 마찬가지이다.

최종 결과는 웹 서핑, 채팅, 메신저, 오디오/비디오 스트리밍, 양방향 게임, 다른 어떤 형태의 트래픽이나 프로토콜에 관계없이 사용자의 모든 인터넷 트래픽이 자동적으로 보호를 받는 것이다. 악의적인 고발 소프트웨어가 사용자 컴퓨터에 심어져 있는 경우라도, 그 고발은 해외의 컴퓨터에서 오는 것으로 나타날 것이다.

GPass와 FirePhoenix는 둘 다 서버를 찾는 기술에 대해 저작권을 가지고 있다. 이 기술을 가지고 차단 도구의 알려지지 않은 약점을 효과적으로 이용할 수 있다는 증거들이 있다. 이렇게 약점을 이용하기 때문에 서버를 찾는 과정이 단순하고 직접적이 되며, Freenet과 같은 다른 도구들이 직면해야 하는 문제들을 피할 수 있다.

GPass와 FirePhoenix는 나온 지 얼마 되지 않았음에도 불구하고 재빨리 사용자의 신뢰를 얻었으며 사용자 기반이 계속 증가하고 있다. 글로벌 인

터넷 자유 콘소시엄(GIFC: http://www.internetfreedom.org)에 상위 세 개의 차단 반대 도구인 GTunnel, UltraSurf 및 DynaWeb과 함께, 상호 보완하고 기술을 공유하고 사용자들에게 좀 더 신뢰할 수 있는 서비스를 제공할 수 있게 되었다.

Tor 역시 비교적 최근에 개발된 차단 반대 도구이다. 이 프로젝트(https://www.torproject.org/)는 원래 미 해군 연구소의 지원을 받았으며 그 후 2004년에 EFF(Electronic Frontier Foundation)이 이어 받았다. Tor의 개발은 주로 공동체와 자원자들이 추진하고 있다. 2008년 5월 25일부터 Tor는 NLnet 재단(http://nlnet.nl/)의 지원으로 새로운 프로젝트를 진행 중이며, 현재 버전은 Tor 0.2.0.26-rc 이다.

Tor는 프락시 서버의 사슬이다. Tor 프락시 (프락시 서버)를 컴퓨터에서 실행하는 자원자들에 의존해 있다. Tor 사용자는 Tor 클라이언트를 설치하는데 사용자의 트래픽을 일련의 Tor 서버를 통해 라우팅 한다. TCP기반 응용 프로그램을 지원하지만, 사용자가 Tor 프락시 서비스를 사용하기 위해 각 응용 프로그램을 설정하는 것이 요구된다.

Tor는 공개 소스 소프트웨어로 나왔기 때문에, 엿보고 다니는 차단도구의 눈을 피하면서 동시에 사람들이 Tor가 어떻게 작동하는지 속속들이 알려 줄 것인가 하는 딜레마를 직면해야 한다. Tor는 철저하게 감시를 당하는 상황에서 어떻게 사용자들이 부트스트랩을 할 수 있게 하느냐 하는 도전에 직면한다.

Tor는 중국의 차단도구에 의해 쉽게 차단될 수 있는데 몇 개 있는 부트스트랩 Tor 서버의 주소가 소스 코드에 숨김없이 드러나 있기 때문이다. 개발자들은 차단 감지하는 데 노력을 낭비하고 있는 것 같은데, 이것은 이미

UltraSurf와 DynaWeb과 같은 다른 많은 서비스에 의해 이미 해결되어 일상적으로 작동하고 있는 것이다. Tor의 다중 홉[11] 트래픽 방식 역시 단일-홉 프락시 시스템보다 대기 시간이 길기는 하지만 차단 하의 사용자들은 일반적으로 잘 활용하고 있다.

## 2. 국내 차단 우회 기술 분석 결과

### 가. 국내 우회 기술 분석 결과

국내 인터넷서비스사업자들은 IP주소 차단 방식, DNS 변조 방식, URL 차단 방식 등을 적용하여 해외 한글 불법·유해 정보와 사이트를 차단하고 있다. [표4-5]와 같이 국내 차단 우회기술 지원 기관에서 제공하는 기술과 소프트웨어를 분석결과는 다음과 같다.

국내 단체에서 제공하는 DNS Free와 같은 우회접속 가능한 프로그램을 이용하여 불법·유해 사이트를 우회 접속하는 경우 차단이 불가능하다. 분석결과 해당 프로그램과의 통신에서 먼저 SSL 통신을 연후에 접속이 진행이 되고 있어, SSL 통신임으로 암호화가 되어서 불법·유해 사이트 접속에 대한 통제가 불가능하다. https 등의 암호화의 경우 차단은 현재 기술로는 불가능하며, 추가적인 기술분석과 개발이 요구된다.

엔트로링크(주), (주)엔블링크 등 SSL를 이용한 VPN접속 서비스를 제공하는 업체의 서비스는 2가지 점에서 차단이 거의 불가능하다. 첫째, SSL과 VPN접속 자체는 불법이 아니기 때문에 이러한 기술을 적용하여 어떠한

11) 패킷 교환방식의 네트워크에서 데이터 패킷이 하나의 라우터로부터 네트워크 상의 다른 라우터로 보내어지는 과정

행위를 하는지 파악하기 힘들어, 해당 서비스가 불법 서비스인가에 대한 해석과 규제가 어렵다. 둘째, 해당 서비스 자체에 대한 분석이 어렵다. VPN 통신의 구간이 어디서 어디까지 인지 파악하기 위해서는 해당업체의 VPN 서버의 위치 및 서비스 형태 등에 대한 자세한 정보가 있어야 분석이 가능한데, 이러한 개별 기업 정보를 수집하기 어려운 상황이다.

[표 4] 국내 차단 우회기술 제공 단체

| 단체 및 기업명 | 사이트 | 주요활동 | 사용료 |
|---|---|---|---|
| 성의 자유와 평등을 위한 시민연대 | http://kofree.net<br>http://kofree.wordpress.com/ | DNS Free 제작 무료 배포 | 무료 |
| | | KT 메가패스 불매운동 | |
| 세계 아고라 정의 포럼 | http://cafe.daum.net/naneoneonaism | IP 추적/차단 방지법 제공<br>1) DNS 서버 변경하기<br>2) 프락시 서버 이용하기<br>3) Tor 사용하기 | 무료 |
| 대한민국네티즌망명지 | https://www.exilekorea.net/ | '세계 아고라 정의 포럼' 차단에 대비한 사이트로 아고라 글들을 많이 연결함. | 무료 |
| 엔트로링크 주식회사 | http://www.anyvpn.net/ | SSL을 이용한 VPN접속 서비스 제공 | 유료 |
| (주)엔블링크 | http://www.mivpn.com | SSL을 이용한 VPN접속 서비스 제공 | 유료 |
| 아름다운 세상만들기 | http://www.wego.6-sys.com/main/ | 차단 우회용 브라우저(six 브라우저) 제공 | 무료 |

## 3. 차단 우회 접속기술 테스트

### 가. 해외 검색 사이트 테스트

구글 또는 야후 등 해외 검색사이트의 번역 기능에 불법·유해 사이트의 URL을 입력하면, 차단 장치를 우회하여 해당 사이트에 접속이 가능하다. 번역 사이트에 차단 대상 URL을 입력하는 경우 해당 사이트 (구글 등)에서 직접 차단 사이트에 대해 분석 하는 방법 (해외 서버에서 해외에 있는 차단 서버의 Contents 를 번역함)을 적용하기 때문이다.

해당 번역 사이트 주소를 차단 목록에 넣어 URL 주소를 차단하는 방법은 너무 많은 경우의 수가 발생하기 때문에 현재의 URL 차단 장비로는 차단이 불가능하다. 그러나, 국가별 해당사이트와 언어별 그리고 Yahoo 등 번역 사이트의 서비스 패턴을 분석하여 차단 기술을 개발하면 번역 사이트를 이용한 우회는 차단할 수 있을 것으로 판단된다.

## 나. 해외 차단 우회 소프트웨어 테스트 결과

해외 차단 반대 단체에서 제작하여 배포하는 GTunnel, UltraSurf, DynaWeb 등의 소프트웨어를 사용하면, 인터넷서비스사업자들이 적용한 차단 기술을 쉽게 우회할 수 있다.

해당 소프트웨어는 IP 차단과 DNS 납치, URL 차단을 우회하기 위해 IP와 DNS 도메인 이름이 각기 다른 수백 개의 미러 사이트가 있다. 각각의 미러 사이트의 차단 상황을 모니터링하는 메커니즘이 있으며, 차단이 발견되면 즉시 IP와 DNS 도메인 이름을 바꾸어 버린다. 현재 기술로는 차단이 불가능하다.

# 제4장 인터넷 불법·유해정보 차단기술 시험 보급

각 국가들은 인터넷에서의 불법·유해 정보를 감소시키기 위한 새로운 기술과 정책 방안을 개발하고 있다. 이에 국내에 적용되어 있는 차단기술의 적용 현황과 새로운 차단기술을 시험 적용해 본다.

## 1절. 차단기술 적용 현황 및 시험보급 방법

### 1. 차단기술 적용 현황


[그림 10] 차단 기반기술의 개념도

차단장비가 도입되기 전, ISP사업자는 대부분 네트워크 라우터에서 L3방식으로 IP를 차단하거나 DNS 등에서 URL로 차단하는 방법을 사용하고 있었다. 이는 L3 IP차단은 장비성능에 영향을 주고 차단에 한계가 있으며 URL 차단은 장비 성능에 따라 실패율이 발생했다.

[표 5] 차단장비 도입 전, ISP사업자의 차단방법

| ISPs | 차단장비 | 차단방법 |
|---|---|---|
| KT | Cisco 7513 1대 | |
| LGU+ | Cisco GSR 12008 | 라우터에서 IP주소를 L3방식으로 차단 |
| SK브로드밴드 | GSR 라우터 | |
| SK텔레콤 | T320 2대,M20 1대,T320 1대 | 라우터에서 IP주소를 L3방식으로 차단 |
| 세종텔레콤 | Juniper M20 2대 | |
| 온세텔레콤 | DNS서버 6대<br>Cisco GSR 12016 | 블랙홀라우터에서 L3방식 차단 |
| 드림라인 | Cisco GSR 12008 | 국제망 라우터 및 방화벽에서 IP주소를 L3 방식으로 차단 |
| 삼성SDS | Cisco 3640 | 불법 사이트 차단용 전용 라우터(블랙홀라우터)에서 L3방식 차단 |

기존 차단방법은 [표 5]에 나타나 있듯이 국제 라우터 또는 스위치에서 IP주소를 L3방식으로 차단 방법으로 ACL(Access List)을 이용하였으며, URL만 제공될 때는 직접 입력이 불가능하여 차단이 불가능해 진다.

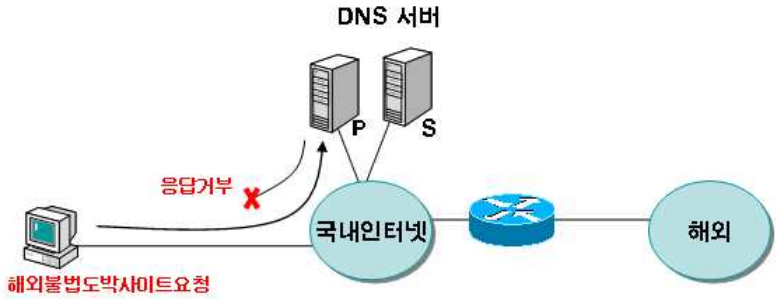
또한, IP주소를 차단할 경우 다른 서비스에 영향을 줄 수 있어, 이를 피하기 위해 HTTP 프로토콜(TCP-80)을 차단하기 위해 확장 ACL(Extended ACL)을 사용하여야 하므로 차단 목록의 수가 증가할수록 많은 메모리 사용으로 성능이 떨어진다. 그리고, ACL의 추가, 삭제, 편집이 복잡하고, 국제 라우터가 여러 대 일 경우 관리가 복잡해 질 수 있다. Proxy를 설정하여 우회 시 차단 불가능하고, ACL 조작 실수로 대형 인터넷 장애 발생 가능성이 나타날 수 있다.

하지만, 블랙홀 라우터를 이용한 방식은 시스코 라우터의 AD(Administrative Distance)값 조작 또는 Longest Match 기법을 이용한 기법으로 자가망 내 iBGP peer 라우터를 만든 후 차단 리스트를 라우팅리스트에 추가하여 전파(Redistribution)하거나 loop인터페이스 생성-하면, 라우팅의 Longest Match에 의해 해당 사이트의 모든 경로는 이 iBGP peer 라우터로 흘러가게 되어 이후 Null로 처리한다.

이러한 블랙홀 라우터를 이용한 방법은 ACL 방식보다는 관리가 쉬우나, 별도의 블랙홀 라우터를 운영하여야 하며, IP주소를 기본으로 하여 네트워크 망에 라우팅테이블이 증가하며, 수시로 갱신되므로 오버헤드 트래픽 발생할 수 있다.

eBGP peer로 전파될 때 국내 AS 또는 인접한 AS에 영향을 줄 수 있으며(AD값이 iBGP보다 작기 때문), 이를 막기 위해 별도의 BGP policy를 설정하여야 함으로 관리가 복잡해 질 수 있다. 이 방법 또한 Proxy를 설정하여 우회 시 차단 불가능하며, 조작 및 관리 실수로 대형장애 발생할 수 있으므로 차단사업자에게는 부담이 아닐 수 없을 것이다.

그리고, 두 번째로 소개할 방법이 DNS를 이용한 방식이다. 이 방법은 해당 URL에 대하여 DNS에서 쿼리에 대한 응답을 하지 않는 방법으로 운영되며, 만약 타 ISP(해외 ISP 포함) DNS로 우회 시 차단 할 수 없는 단점이 있고, URL이 아닌 IP로 접속 시 차단 할 수 없다.



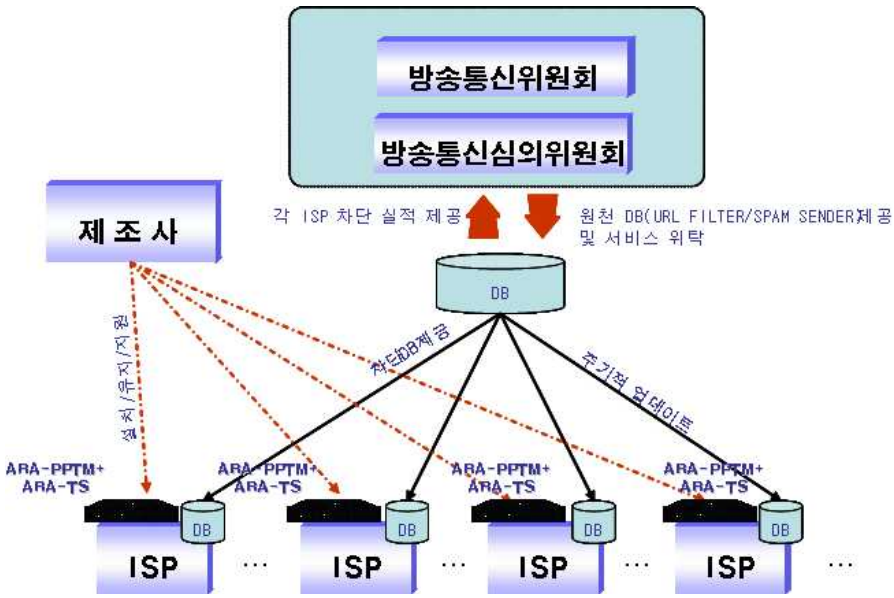

[그림 11] DNS 서버를 이용한 사이트 차단 방법

이러한 문제점 및 애로사항을 해결하고, IP주소 및 DNS 차단, 그리고 URL 차단까지 가능한 차단장비를 도입하게 되었다.

차단장비는 고성능 대역폭 처리 보장해야 하며, 다양한 인터페이스 처리 속도-155M, 622M, 1G, 2.5G-를 지원해야 하고 망 성능에 영향을 주지 않으면서 효과적으로 차단 할 수 있어야 한다.

또한, 네트워크 망의 안정성 보장하기 위하여 TAP 방식으로 차단 할 수 있어야 하며, Redundancy 구현이 가능해야 한다. 그리고, 중앙 관제가 가능해야 하므로, 중앙에서 단일의 콘솔로 관리가 가능하고, 보안 접속이 가능해야 한다.

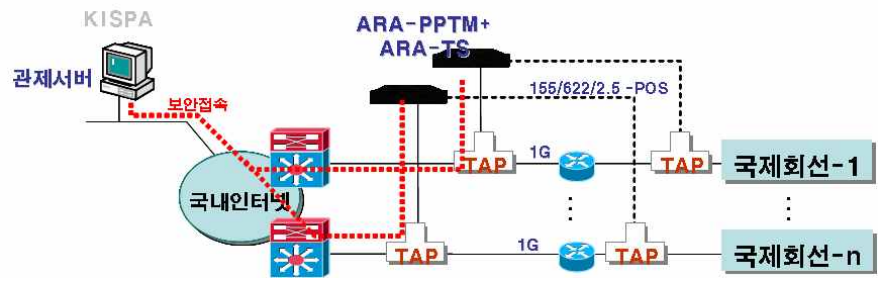
마지막으로 다양한 환경에서 도입 한 사례가 있는지 여부와 다양한 분석 형태로 분석이 가능하고 요구사항에 따라 개발 가능한 지 여부와 기술변화에 따라 신속히 추가 개발 가능한지 여부도 중요한 변수가 될 수 있다.




[그림 12] URL 차단장비 도입에 따른 관리 현황

이러한 전체적인 환경변수를 고려하여 URL 차단장비를 개발하였고, [그림 12]과 같이 ISP사업자에게 차단장비를 설치하게 되었다.

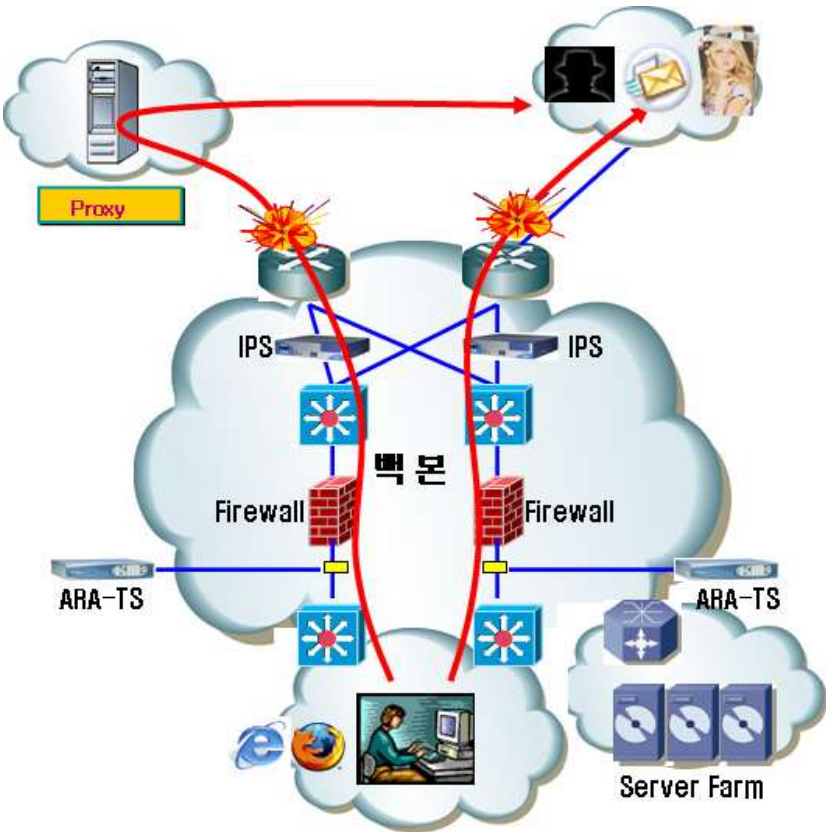
ISP사업자는 이러한 환경변수를 고려하여 국제회선에 차단장비를 시험 적용하였고, [그림 13] 같이 차단장비를 국제회선에 영향을 주지 않는 범위 내에서 설치하게 되었다.




[그림 13] ISP사업자의 차단장비 도입 방법

이러한 URL기반 차단 장비는 SPAM Sender Block-스팸 전송자 그룹 식별하고, 포트/IP/Proxy 우회접속 차단 및 요일/시간대별 차단 - 지능적/효율적 차단방안 제공, 트래픽 모니터링, 실시간 양방향 최대 4.5Gbps을 지원한다.

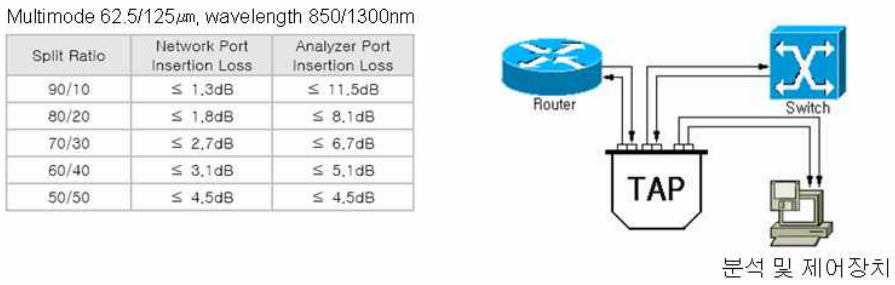
또한, Total/IP/TCP/Port/Protocol별 리포트, 분/일/월/년간 별 리포트 비정상 트래픽 감지/차단, 로그 분석 및 실시간 로그 분석/검색 제공을 제공하여 차단사업자가 보다 편리하게 이용할 수 있을 것으로 본다.




[그림 14] ISP사업자의 차단장비 적용 개괄도

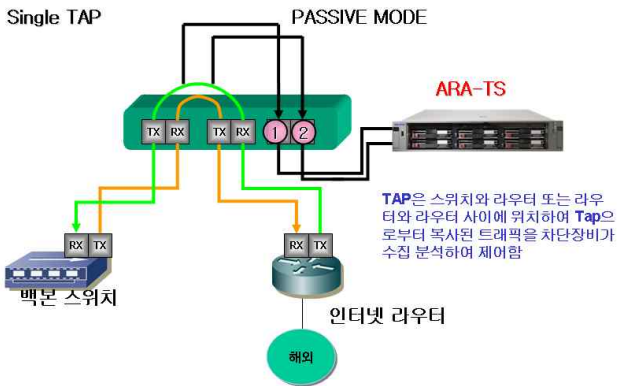
## 2. 차단장비 적용 방법

차단장비의 가장 큰 특징은 TAP 방식으로 다른 회선이나 장비에 영향을 주지 않는다는 것이다. 이 TAP 방식의 특징으로는 무정전, 무중단으로 네트웍 모니터링이 가능하며, Full Duplex로 TX, RX 동시 모니터링하고, 투명모드(Transparent Mode) 동작하고, 광 손실 최소화하였다는 것이다.

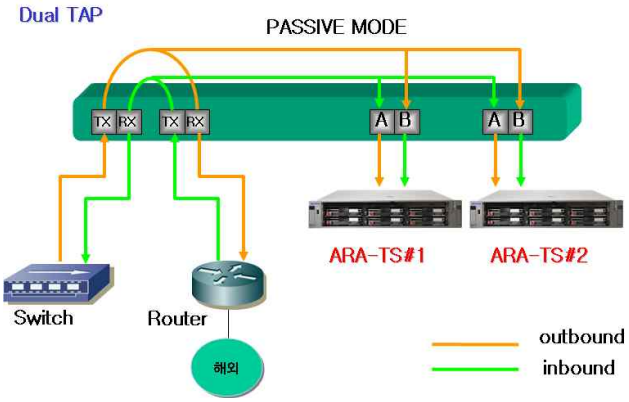



[그림 15] 차단장비의 TAP방식의 연동 방법

TAP의 종류에는 Cooper Tap(10/100M UTP), Gigabit Fiber Tap(멀티/싱글모드, LX, SX), T1/E1, DS3/E3, 10Giga Fiber 등이 있다.




[그림 16] Single TAP방식의 결선 및 동작 방법



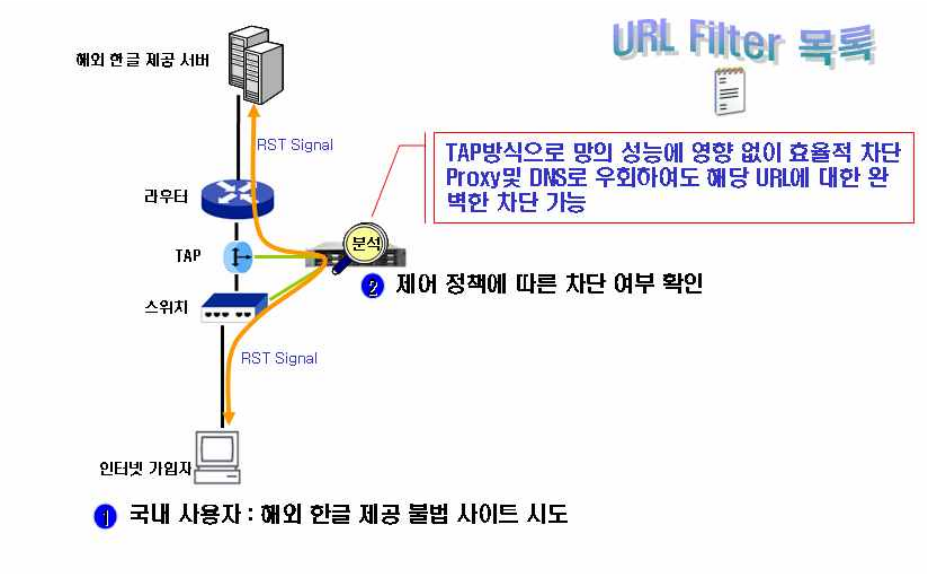

[그림 17] Dual TAP방식의 결선 및 동작 방법

상기와 같이 TAP방식은 Single과 Dual 2가지 결선 방식이 존재한다. 2가지에 따라 이용할 수 있는 차단회선 및 장비가 달라지며, 가능한 회선을 수용하기 위해 Dual로 사용할 수 있게 고려했다고 할 수 있다.

## 3. 차단기술 동작 방법

차단기술은 동작은 먼저 사용자가 해당 차단대상 사이트를 접속하게 되면, 제어 장비인 차단장비를 통하여 해당 사이트인지 확인하고 이에 대상 사이트가 되면, 차단통보를 사용자에게 전달하는 방식을 취한다.

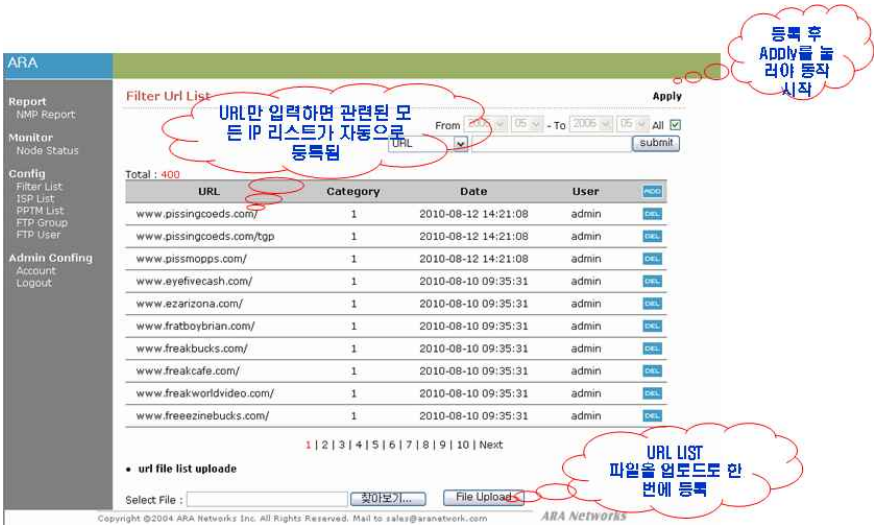
이러한 방식은 회선이나 다른 라우터 장비에 영향을 주지 않기 위해 미러방식은 TAP를 사용하기 때문에 영향을 최소화할 수 있다.




[그림 18] 차단기술 적용 및 분석 방법

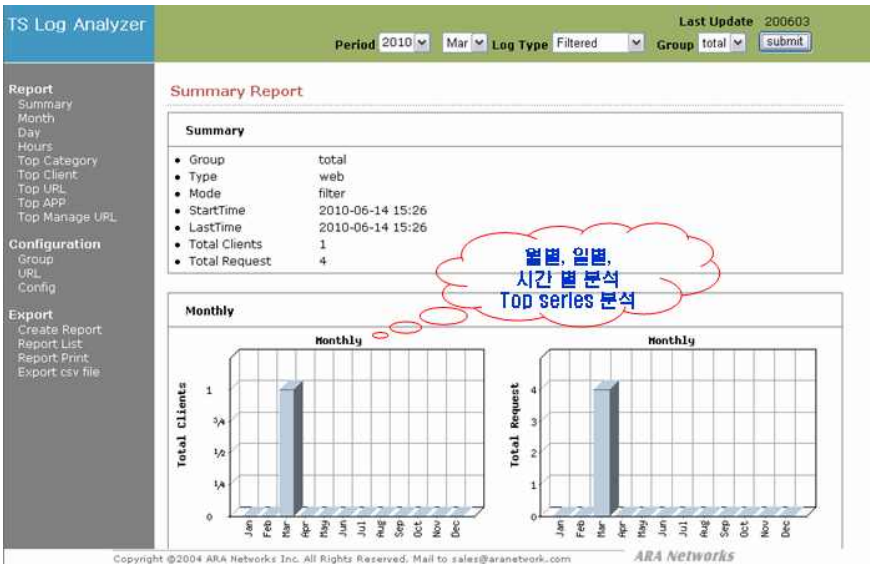
## 4. 차단기술 분석 현황

이렇게 설치된 차단장비는 [그림 19]에 보이는 차단목록을 등록하고 관리하는 서버를 두어 관리하게 된다. 그리고 차단 목록뿐 아니라, 차단관리 현황까지 파악할 수 있으므로 효율성은 뛰어나다 하겠다.




[그림 19] 차단장비 도입에 따른 차단목록 등록 화면

차단장비는 월별, 일별, 시간별로 차단분석이 가능하며, 전체적인 통합 통계도 가능하다.




[그림 20] 차단장비의 차단분석 화면

## 2절. 차단기술 시험보급

### 1. 시험보급 개요

불법 정보 자동 차단 시스템 지원사업으로 차단 시스템의 효과 검증을 위해 특정 ISP를 선정하여 일정기간 시험 하였다.


[그림 21] 차단기술 시험 보급 및 테스트 절차도

기술 보급 기간은 2010년 6월부터 12월까지 시행하였으며, 대상 사업자는 드림라인을 시작으로 하여 8개 차단사업자를 모두 적용하였다.

[표 6] 차단기술 시험보급을 위한 작업 일정표(샘플)

| 일자 | 작업구분 | 세부작업내용 | 작동시간 | 비고 |
|---|---|---|---|---|
| 9/28 | 설치<br>제어시작 | 통제서버 및 수행서버 설치<br>우회코드(P,N,A등) 입력 | 15:00<br>22:40 | 우회방법구분(패치) |
| 9/29 | 제어 | | | |
| 9/30 | 제어 | | | |
| 10/1 | 제어 | | | |
| 10/2 | 제어 | - DNS 변경 | 19:00 | DNS차단과 병행 |
| 10/3 | 제어 | | | |
| 10/4 | 제어 종료 | | 10:45 | |

기술적용은 기존 설치된 차단장비에 새로운 우회기술인 DNS Free Ver 3와 번역사이트, 특수기호 등의 보완사항을 업그레이드하였다.

차단장비의 업그레이드와 관리서버의 패치 등을 통하여 차단장비에 적용하였으며, 이를 통하여 테스트를 통해 시험 적용하였다.

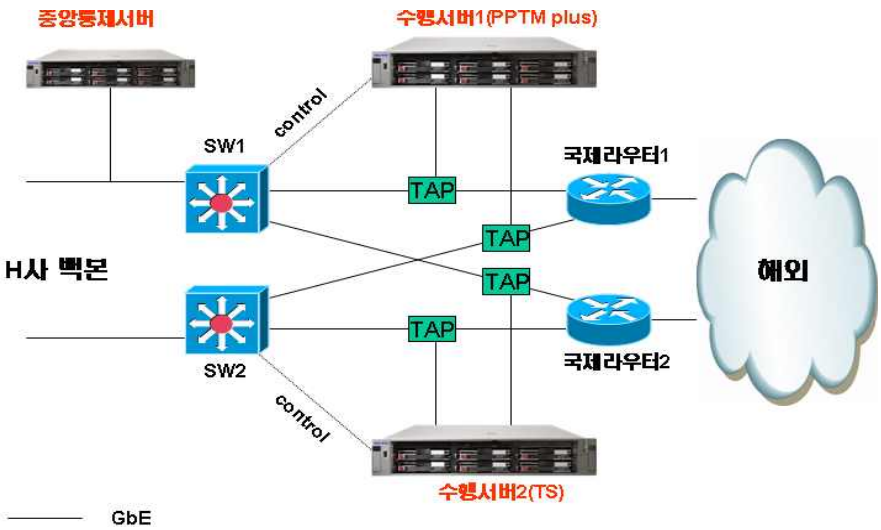
참고로, 차단장비의 테스트는 여러 환경을 할 수 없는 부분이 있기에 장시간을 통하여 테스트를 하였으며, 1개의 사업자를 통하여 테스트를 한 후 전체 차단사업자에게 보급하는 방법으로 진행하였다.

## 2. 시험보급 구성도

기존에 설치된 차단장비(PPTM Plus) 및 중앙통제서버를 업그레이드를 시행하였고, 장비는 TAP를 통하여 미러방식을 통하여 회선에 최대한 장애를 주지 않는 상태에 네트워크 망을 구성하였다.

또한, 차단장비 및 통제서버는 기존에 설치된 장비 외의 별도의 장비를 이용하여 기존의 차단에 영향을 주지 않는 범위에서 시행하였다.

이때, 환경변수 등을 고려하여 최대한 기존 장비의 설정을 파악하여 고려한 후, 시험테스트 장비를 세팅하고 업그레이드를 통해 테스트할 수 있도록 조치하였다.




[그림 22] 차단기술 보급을 위한 시험망 구성도

## 3. 차단 성능

차단장비의 성능은 여러 가지가 있지만, 최소한의 측정방법 및 기준을 통하여 성능을 고려하였다. 이는 여러 가지 요소가 있지만 주요 핵심요소만을 선정하여 고려하였으며 이외의 사항은 기존의 차단장비의 환경변수에 고려되어 있는 것을 기준으로 하였다.

[표 7] 차단 성능의 측정 방법

| 구분자 | 제 목 | 설 명 |
|---|---|---|
| f | 차단실패 | HTTP 요청이 차단목록의 데이터와 일치하나 차단이 안된 것, 명백한 **차단 실패로 간주**, 예) 다음장 참조 |
| c | Counter어플리케이션 (redirect의심) | 음란사이트 등의 객체에 counter application이 연동되어 참조되는 경우, redirect요청일수도 있음, url 문자열에 차단목록 데이터가 포함됨, **차단하면 안됨**. 예) 다음장 참조 |
| a | 신생anonymizer의심 | 알려지지 않은 anonymizer에 의한 HTTP 요청임, **차단 실패로 간주**, 예) 다음장 참조<br><br>주)실제 anonymizer를 경유하면 속도가 매우 느리기 때문에 실효성이 떨어짐 |
| t | 번역사이트 | 영문번역 포털을 이용하는 경우, 예) 다음장 참조 |
| r | redirect 또는 refer | UCC, 성인사이트, 국내외 포털에 의한 이미지 검색 등으로 redirect되거나 참조태그로 처리된 요청, 다음 단계에서 독립적인 HTTP 요청을 맺으므로 수행서버의 의해 차단됨 |
| xx | 총계 | 나열된 HTTP 요청수, 위의 f+c+a+t+r과 차이가 있을 수 있음, 차단하면 안 되는 것으로 차단목록 데이터와 패턴만 일치하기 때문에 발생, 예) 다음장 참조 |
| 65,535 | 전체요청수 | 전체요청수는 항상 65,535로 고정됨(8:1 표본추출) |

[표 8] 차단 성능의 구분자 사용 예

| 구분자 | 사용 예 |
|---|---|
| f | http://www.dabogy.com./x/ |
| | • 사이트문자열 끝에 점(.)을 사용하는 예<br>• 패치 완료함 |
| c | http://image.masterstats.com/cnt?id=16789&ex=http%3A//www.omadam.net/&pg=http%3A//www.omadam.net/intro.htm&r=0.030169738862406814 |
| | • counter applicaqtion |
| a | http://11.on.arena.ne.jp/cgi/nph-proxy.cgi/000000A/http/www.ya-moon.com<br>http://61.14.172.254:5000/proxy.cgi/000000A/http/www.sora.net/ |
| | • 신규 anonymizer |
| t | http://64.233.179.104/translate_c?hl=ko&ie=UTF-8&oe=UTF-8&langpair=en%7Cko&u=http://www.ya-moon.com/&prev=/language_tools |
| | • 64.233.179.104는 google korea 번역 사이트임 |
| xx | www.www.omadam.net.net<br>wwww.sora.net<br>www.sora.net.net<br>www.hojoomall.com.au |

상기 표는 차단장비의 성능 구분자를 샘플로 구성해 놓은 것이며, 해당 구분자는 새로운 차단기술 등을 고려하여 진행하였다. 그리고 새로운 차단기술 적용의 구분자 선정은 차단 목록의 테스트를 통하여 구분하였다.

[표 9] 여러 가지 차단 통계 현황(샘플)

| 구분 | ① 차단 실패 | ② 신생 anonymizer 의심 | ③ counter 어플리케이션 (redirect의심) | ④ 번역 사이트 | ⑤ redirect 또는 refer | ⑥ 기타 | 총계 | 차단 실패수 ①+② | 차단 실패율 (%) ①+② |
|---|---|---|---|---|---|---|---|---|---|
| 구분자 | f | a | c | t | r | xx | | | |
| 전체 | 55 | 490 | 3299 | 30 | 619 | 11 | 4504 | 545 | 0.83162% |
| 평균 | 0.243 | 2.168 | 14.597 | 0.133 | 2.739 | 0.049 | 19.929 | 2.412 | **0.00368%** |

## 4. 새로운 차단기술 적용 결과

[표 10] 차단 설정

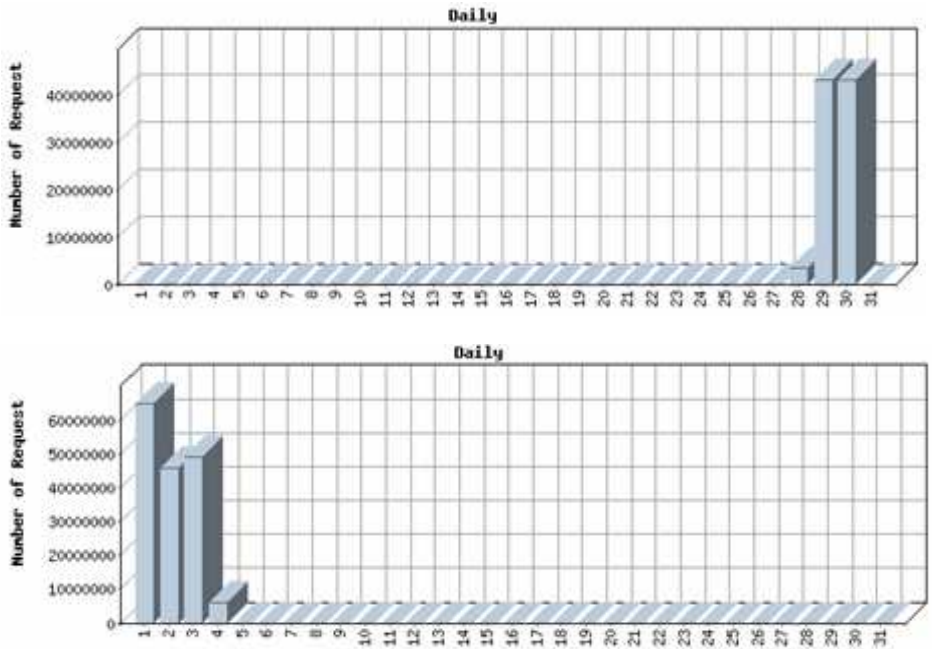
| 로그 | 설 명 |
|---|---|
| 전체요청수 | 인터넷으로 HTTP 요청된 수, access+filter=전체요청수 |
| access | 차단되지 않은 요청수 |
| filter | 차단된 요청수 |

[표 11] 차단 결과

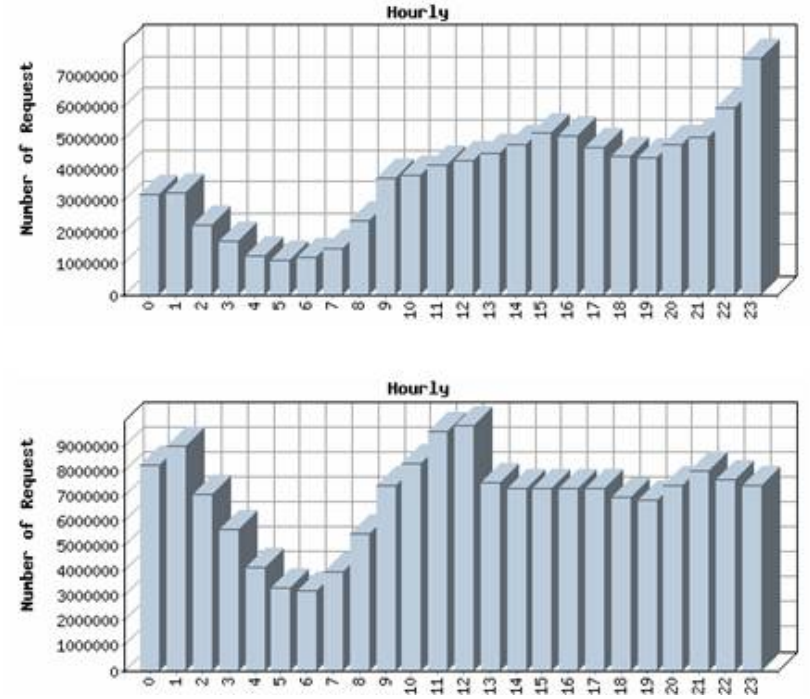
| 일자 | access | filter | 전체요청수 | 차단 율 | 비고 |
|---|---|---|---|---|---|
| 09월 28일 | 3,298,581 | 3,530,520 | 6,829,101 | 51.70% | 주1 |
| 09월 29일 | 43,449,660 | 6,851,240 | 50,300,900 | 13.62% | |
| 09월 30일 | 43,425,584 | 1,450,006 | 44,875,590 | 3.23% | |
| 10월 01일 | 64,785,102 | 2,442,174 | 67,227,276 | 3.63% | |
| 10월 02일 | 45,630,519 | 1,502,294 | 47,132,813 | 3.19% | |
| 10월 03일 | 49,251,353 | 1,462,429 | 50,713,782 | 2.88% | |
| 계 | 249,840,799 | 17,238,663 | 267,079,462 | 6.45% | |

[표 12] Access 로그 분석

| 9월 | 10월 |
|---|---|
| **Summary** | **Summary** |
| • Group total<br>• Type web<br>• Mode access<br>• StartTime 2006-09-28 22:39<br>• LastTime 2006-09-30 23:59<br>• Total Clients 879,395<br>• Total Request 90,173,825 | • Group total<br>• Type web<br>• Mode access<br>• StartTime 2006-10-01 00:00<br>• LastTime 2006-10-04 04:51<br>• Total Clients 951,393<br>• Total Request 165,772,392 |




[그림 23] 차단시험에 따른 결과(일별)




[그림 24] 차단시험에 따른 결과(시간별)


| Time | Number of Request | Time | Number of Request |
|---|---|---|---|
| 0 | 3,186,754 | 12 | 4,268,282 |
| 1 | 3,258,261 | 13 | 4,531,966 |
| 2 | 2,231,953 | 14 | 4,789,991 |
| 3 | 1,705,231 | 15 | 5,190,991 |
| 4 | 1,258,814 | 16 | 5,085,849 |
| 5 | 1,120,176 | 17 | 4,679,070 |
| 6 | 1,199,118 | 18 | 4,425,232 |
| 7 | 1,495,880 | 19 | 4,374,512 |
| 8 | 2,353,905 | 20 | 4,776,706 |
| 9 | 3,736,730 | 21 | 5,012,568 |
| 10 | 3,801,566 | 22 | 5,978,787 |
| 11 | 4,134,195 | 23 | 7,577,288 |


| Time | Number of Request | Time | Number of Request |
|---|---|---|---|
| 0 | 8,211,174 | 12 | 9,800,887 |
| 1 | 8,999,262 | 13 | 7,528,864 |
| 2 | 7,026,254 | 14 | 7,300,750 |
| 3 | 5,653,953 | 15 | 7,295,374 |
| 4 | 4,117,686 | 16 | 7,253,742 |
| 5 | 3,295,178 | 17 | 7,296,370 |
| 6 | 3,177,614 | 18 | 6,913,536 |
| 7 | 3,965,407 | 19 | 6,818,917 |
| 8 | 5,446,256 | 20 | 7,402,191 |
| 9 | 7,396,191 | 21 | 7,977,301 |
| 10 | 8,292,088 | 22 | 7,613,517 |
| 11 | 9,586,115 | 23 | 7,403,765 |

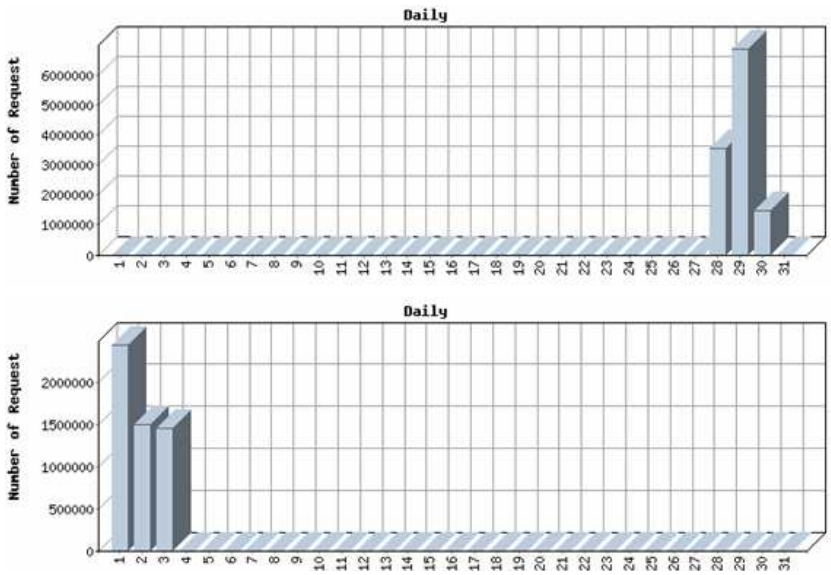
[그림 25] 차단시험에 따른 결과(건수)

| Summary | |
|---|---|
| • Group | total |
| • Type | web |
| • Mode | filter |
| • StartTime | 2006-09-28 22:39 |
| • LastTime | 2006-09-30 23:59 |
| • Total Clients | 45,925 |
| • Total Request | 11,831,766 |

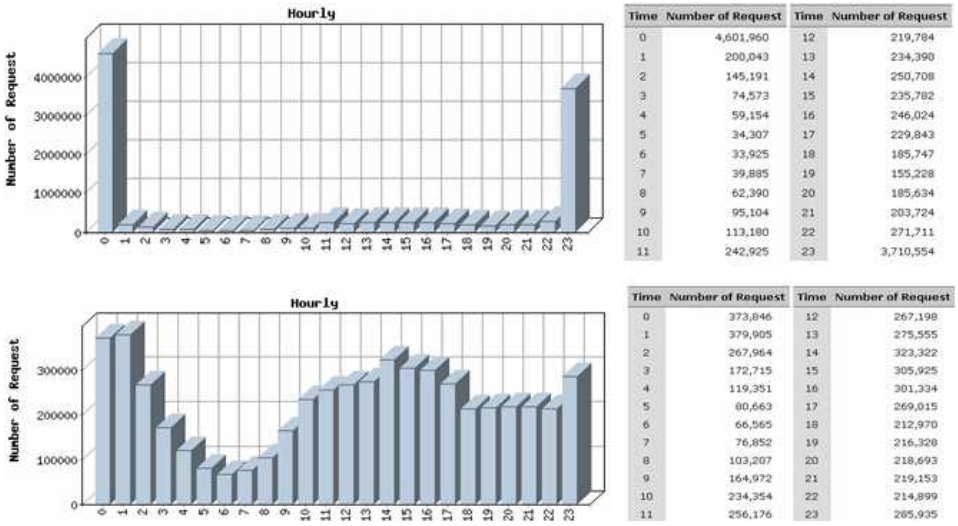
| Summary | |
|---|---|
| • Group | total |
| • Type | web |
| • Mode | filter |
| • StartTime | 2006-10-01 00:00 |
| • LastTime | 2006-10-03 23:59 |
| • Total Clients | 56,211 |
| • Total Request | 5,406,897 |

[그림 26] 필터로그 분석 결과

로그가 적재되고 약 24시간이 지나야 분석프로세서가 실행되었으며, 9월 차단이 월등히 많은 이유는 특정 URL을 DNS가 127.0.0.1로 resolving하였고(예, www.xbdvd.com), 특정단말(프로그램으로 추정)이 특정 시간대에(주로 밤시간) URL을 "127.0.0.1"로 하는 비정상 트래픽을 유발되었다.




[그림 27] 필터로그 분석 결과(일별)




| Time | Number of Request | Time | Number of Request |
|---|---|---|---|
| 0 | 4,601,960 | 12 | 219,784 |
| 1 | 200,043 | 13 | 234,390 |
| 2 | 145,191 | 14 | 250,708 |
| 3 | 74,573 | 15 | 235,782 |
| 4 | 59,154 | 16 | 246,024 |
| 5 | 34,307 | 17 | 229,843 |
| 6 | 33,925 | 18 | 185,747 |
| 7 | 39,885 | 19 | 155,228 |
| 8 | 62,390 | 20 | 185,634 |
| 9 | 95,104 | 21 | 203,724 |
| 10 | 113,180 | 22 | 271,711 |
| 11 | 242,925 | 23 | 3,710,554 |

| Time | Number of Request | Time | Number of Request |
|---|---|---|---|
| 0 | 373,846 | 12 | 267,198 |
| 1 | 379,905 | 13 | 275,555 |
| 2 | 267,964 | 14 | 323,322 |
| 3 | 172,715 | 15 | 305,925 |
| 4 | 119,351 | 16 | 301,334 |
| 5 | 80,663 | 17 | 269,015 |
| 6 | 66,565 | 18 | 212,970 |
| 7 | 76,852 | 19 | 216,328 |
| 8 | 103,207 | 20 | 218,693 |
| 9 | 164,972 | 21 | 219,153 |
| 10 | 234,354 | 22 | 214,899 |
| 11 | 256,176 | 23 | 265,935 |

[그림 28] 필터로그 분석 결과(시간별)

[표 13] 필터로그 분석 결과

| 구분 | 우회 유형 | 9월 | | 10월 | |
|---|---|---|---|---|---|
| URL | WEB(정통윤 목록) | 3,621,628 | 30.61% | 4,652,197 | 86.04% |
| | 포트 | 0 | 0.00% | 0 | 0.00% |
| | 프록시 | 3,032 | 0.03% | 5,356 | 0.10% |
| | Anonymizer | 48 | 0.00% | 503 | 0.01% |
| | 포트+프록시 | 942 | 0.01% | 2,515 | 0.05% |
| | 포트+Anonymizer | 0 | 0.00% | 0 | 0.00% |
| | 프록시+Anonymizer | 0 | 0.00% | 0 | 0.00% |
| | 포트+프록시+Anonymizer | 0 | 0.00% | 0 | 0.00% |
| IP | IP(resolving) | 410,299 | 3.47% | 588,385 | 10.88% |
| | 포트 | 7,657,480 | 64.72% | 63 | 0.00% |
| | 프록시 | 120,143 | 1.02% | 132,232 | 2.45% |
| | Anonymizer | 0 | 0.00% | 0 | 0.00% |
| | 포트+프록시 | 18,194 | 0.15% | 25,646 | 0.47% |
| | 포트+Anonymizer | 0 | 0.00% | 0 | 0.00% |
| | 프록시+Anonymizer | 0 | 0.00% | 0 | 0.00% |
| | 포트+프록시+Anonymizer | 0 | 0.00% | 0 | 0.00% |
| TOTAL | | 11,831,766 | 100.00% | 5,406,897 | 100.00% |

Top URL

| IP/URL | Request Count | |
|---|---|---|
| 127.0.0.1 | 7,660,868 | 64.75 % |
| omadam.net | 269,492 | 2.28 % |
| 216.17.111.122 | 165,208 | 1.4 % |
| club-chaos.com | 140,063 | 1.18 % |
| 211.253.9.250 | 138,318 | 1.17 % |
| sexnight.bz | 126,399 | 1.07 % |
| www.sexpq.com | 124,093 | 1.05 % |
| dabogy.com | 121,861 | 1.03 % |
| www.sora.net | 118,700 | 1 % |
| www.sexwal.com | 110,311 | 0.93 % |
| erozn.net | 103,071 | 0.87 % |
| board.erozn.net | 96,501 | 0.82 % |

[그림 29] 필터로그 분석 결과(종합1)

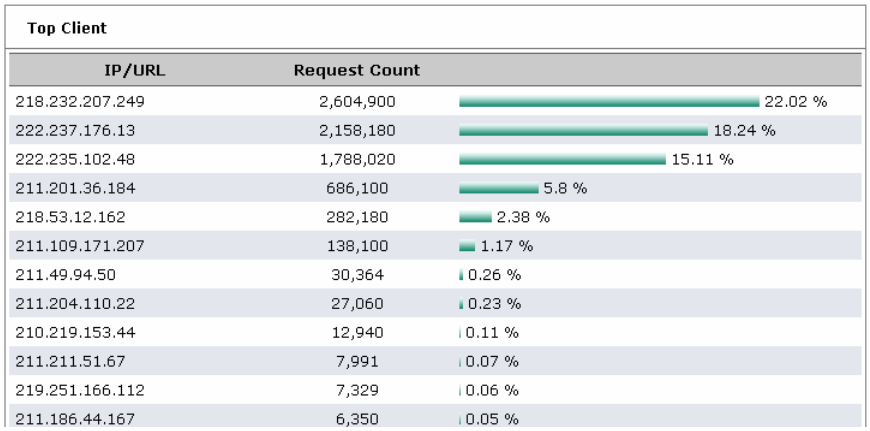
상기 차단 로그 분석에서는 127.0.0.1은 특정 가입자의 공격 시도로 보이며, IP주소 216.17.111.122고 mybozi.net으로, IP주소 211.253.9.250는 방송통신윤리위원회 불법정보 차단 안내페이지가 나타난다. 차단기술 장비는 타 DNS로 변경하여 시행한 것이다.

Top URL

| IP/URL | Request Count | |
|---|---|---|
| omadam.net | 320,311 | 5.92 % |
| 216.17.111.122 | 233,473 | 4.32 % |
| sexnight.bz | 232,904 | 4.31 % |
| club-chaos.com | 166,399 | 3.08 % |
| dabogy.com | 158,508 | 2.93 % |
| 211.253.9.250 | 157,878 | 2.92 % |
| www.sexpq.com | 153,534 | 2.84 % |
| sexwal.com | 131,327 | 2.43 % |
| erozn.net | 130,010 | 2.4 % |
| www.sexwal.com | 126,045 | 2.33 % |
| board.erozn.net | 124,443 | 2.3 % |
| www.cosex.net | 118,688 | 2.2 % |
| www.sora.net | 110,894 | 2.05 % |

[그림 30] 필터로그 분석 결과(종합2)

상기 그림에서 IP주소 216.17.111.122는 mybozi.net 이고, IP주소 211.253.9.250는 앞서와 마찬가지로 방송통신심의위원회 불법정보 차단 안내페이지가 나타난다. 이 환경에서도 차단장비의 DNS를 타 DNS로 변경하여 실행하였다.

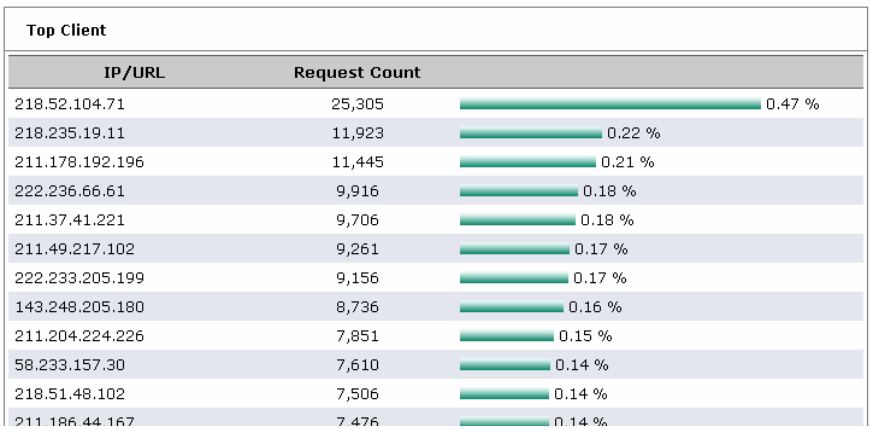


Top Client

| IP/URL | Request Count | |
|---|---|---|
| 218.232.207.249 | 2,604,900 | 22.02 % |
| 222.237.176.13 | 2,158,180 | 18.24 % |
| 222.235.102.48 | 1,788,020 | 15.11 % |
| 211.201.36.184 | 686,100 | 5.8 % |
| 218.53.12.162 | 282,180 | 2.38 % |
| 211.109.171.207 | 138,100 | 1.17 % |
| 211.49.94.50 | 30,364 | 0.26 % |
| 211.204.110.22 | 27,060 | 0.23 % |
| 210.219.153.44 | 12,940 | 0.11 % |
| 211.211.51.67 | 7,991 | 0.07 % |
| 219.251.166.112 | 7,329 | 0.06 % |
| 211.186.44.167 | 6,350 | 0.05 % |

[그림 31] 필터로그 분석 결과(공격 의심 로그1)

상위 4개 클라이언트는 DoS(127.0.0.1)공격자로 의심된다.



Top Client

| IP/URL | Request Count | |
|---|---|---|
| 218.52.104.71 | 25,305 | 0.47 % |
| 218.235.19.11 | 11,923 | 0.22 % |
| 211.178.192.196 | 11,445 | 0.21 % |
| 222.236.66.61 | 9,916 | 0.18 % |
| 211.37.41.221 | 9,706 | 0.18 % |
| 211.49.217.102 | 9,261 | 0.17 % |
| 222.233.205.199 | 9,156 | 0.17 % |
| 143.248.205.180 | 8,736 | 0.16 % |
| 211.204.224.226 | 7,851 | 0.15 % |
| 58.233.157.30 | 7,610 | 0.14 % |
| 218.51.48.102 | 7,506 | 0.14 % |
| 211.186.44.167 | 7,476 | 0.14 % |

[그림 32] 필터로그 분석 결과(공격 의심 로그2)

## 5. 보완사항

차단장비와 관리서버로 이루어진 시험보급 과정에서는 URL이 일치하여야만 차단 수행을 수행하게 된다. 따라서 소라넷의 경우 www.sora.net은 차단하지만, photo1.sora.net은 차단하지 않게 된다. 참고로 이러한 환경설정에도 불구하고 필터 우회 프로그램 등이 발생되고 있고, 장기적인 조사 및 분석, 연구가 필요할 것으로 본다.

[표 14] 필터 우회 프로그램

| 개발사 | 프로그램 | 특징 |
|---|---|---|
| **에로스아시아 (erosasia.com)** | • XBroswer | • 프록시 자동 헌팅 및 업데이트<br>• 2002년도 출시 프로그램 관리가 안되어 거의 사용 안함 |
| **성자평련 (www.kofree.net)** | • DNSFree | • 클릭시 DNS를 자동으로 변경<br>• 2006년 출시<br>• 대부분의 사용자가 이용 |

[표 15] 차단기술 시험적용 보완사항

| 구 분 | 내 용 |
|---|---|
| **절차적 측면** | • 중앙통제서버의 차단목록 등록 방식<br>• 수행서버에서 차단 시작 방식<br>• 로그 분석을 수행할 서버<br>- 1안 : 수행서버에서 분석하여 분석 결과만 중앙통제서버로 전송<br>- 2안 : 수행서버에서는 모든 로그를 모두 중앙통제서버로 전송 한 후 중앙통제서버에서 분석 수행<br>• 로그 분석의 주기 및 범위<br>- 예) 주기 : 일별, 월별, 분기별<br>범위 : 차단 실적(우회 시도 포함), TOP CLIENT&URL |
| **유연성 측면** | • 특정 소스는 특정 URL의 접근을 허용하는 방법<br>• 차단 유형별로 로그를 나누어서 적재하는 방법<br>• 비정상트래픽(예, 127.0.0.1 DoS 공격 등)일경 우 로그 제외 방법<br>• 변칙 URL 문자열 사용시(예, URL 끝에 점(.)을 사용) - 보완 완료 |

[표 16] 차단 방식과의 비교(URL 방식)

| 우회방식 | 차단서버를 이용한 방식 (TS&PLUS) | 라우터 컨피규를 이용한 방식(ACL) | REROUTING을 이용한 방식 (BLACK HOLE) | DNS를 이용한 방식 (DENY) |
|---|---|---|---|---|
| URL | **YES** | NO | NO | **YES** |
| 포트 | **YES** | **YES** | NO | NO |
| 프록시 | **YES** | NO | NO | NO |
| Anonymizer | **YES** | NO | NO | NO |
| 포트+프록시 | **YES** | NO | NO | NO |
| 포트+Anonymizer | **YES** | NO | NO | NO |
| 프록시+Anonymizer | **YES** | NO | NO | NO |
| 포트+프록시 +Anonymizer | **YES** | NO | NO | NO |
| 장단점 | 네트워크에 무영향 차단의 일관성 및 정확성으로 실효성 확보 | 라우터성능 저하우려,관리복잡, 실효성 낮음 | 간단한 구성, 관리복잡, 실효성 낮음 | 관리복잡, 실효성 낮음 |

[표 17] 차단 방식과의 비교(IP 방식)

| 우회방식 | 차단서버를 이용한 방식 (TS&PLUS) | 라우터 컨피규를 이용한 방식(ACL) | REROUTING을 이용한 방식 (BLACK HOLE) | DNS를 이용한 방식 (DENY) |
|---|---|---|---|---|
| IP | **YES** | **YES** | **YES** | NO |
| 포트 | **YES** | **YES** | NO | NO |
| 프록시 | **YES** | NO | NO | NO |
| Anonymizer | **YES** | NO | NO | NO |
| 포트+프록시 | **YES** | NO | NO | NO |
| 포트+Anonymizer | **YES** | NO | NO | NO |
| 프록시+Anonymizer | **YES** | NO | NO | NO |
| 포트+프록시 +Anonymizer | **YES** | NO | NO | NO |
| 장단점 | 네트워크에 무영향 차단의 일관성 및 정확성으로 실효성 확보 | 라우터성능 저하우려,관리복잡, 대형사고우려 | 간단한 구성, 관리복잡, 대형사고우려 | 관리복잡, 실효성 낮음 |

# 제5장 결 론

디지털경제는 급속히 성장하여 세계경제에서 중요한 부분을 차지하게 되었고, 오늘날의 온라인 커뮤니티는 전 세계 대다수의 사람들이 사용하는 가장 일반적이면서도 주요한 소통수단이 되었다.

인터넷에서 통용되는 광범위한 콘텐츠와 온라인에서 일어나는 수많은 활동들은 대개는 긍정적이고 건설적인 변화들로 간주 되지만, 동시에 상당수의 불법·유해 행위들 역시 인터넷상에서 만연하고 있는 것이 사실이다.

오프라인(즉, 인터넷의 대치되는 의미에서의 현실사회)을 통제하는 형사법 및 치안활동을 인터넷 상에 어떻게 적용하는가 하는 것은 중요한 문제지만, 인터넷 상의 대다수 불법·유해 행위의 파생 및 피해 발생 과정은 특정 국가 및 지역에 국한되지 않는다는 특성을 보인다는 점에서 오프라인 상의 범죄행위와 상이하며, 이러한 온라인 불법행위의 범국가적 특성은 발생 양상과 해결방법에서도 오프라인의 그것과 차이를 만들어 그 나름의 고유한 특성을 갖게 한다.

개별 국가가 단독으로 추진하거나 국제기구가 함께 참여하는, 온라인상 불법·유해정보 차단 정책은 다양하게 추진하여 왔으나, 완벽한 실효를 거두고 있는 정책은 없다. 이는, 인터넷상의 불법·유해정보를 차단하는데 다음과 같은 기술적·제도적 한계가 있기 때문이다.

첫째, 인터넷 기술의 급속한 발전은 전 세계 누구나, 어디서든지, 즉각적으로, 손쉽게 불법·유해 콘텐츠와 사이트의 생산과 유통을 가능하게 한다.

또한, 트위터 등 새로운 형태의 인터넷 서비스가 지속적으로 개발되고, 순환 주기가 매우 짧은 기술적 특성으로 인해, 불법·유해 콘텐츠의 생산과 유통을 차단하는 기술 개발과 제도 마련이 쉽지 않고, 정책실효성도 낮은 편이다.

둘째, 해외 불법·유해 사이트를 차단하는 방안을 마련하더라도, 국경 없이 유통되는 인터넷의 특성으로 인해 실질적인 효과를 발휘하기 어렵다. 특히, 해외에서 유입되는 불법·유해 콘텐츠의 생산과 유통을 차단하기 위해서는 관련 국가들과의 긴밀한 공조체계 마련이 필요한데, 각국의 문화적·법률적 특성에 따라 동일 콘텐츠에 대해 동일한 규제와 차단 정책을 적용하기 어려운 실정이다.

셋째, 불법·유해사이트의 규제는 '표현의 자유'와 관련되어 국가의 직접 개입보다는, 관련단체나 생산과 유통에 참여하는 사업자와 사용자 중심의 자율규제가 중심이 되어야 하는데, 이러한 과정에서 이해당사자간의 주장이 상충되는 어려움이 있다.

기술적 한계가 있음에도 불구하고, 인터넷 가치사슬이 길수록 불법·유해 행위의 발생과 유통 지점(또는 불법·유해행위와 공급채널의 접촉점)이 증가하므로 인터넷 가치사슬 과정에 개입할 수 있는 여지 또한 많아져 온라인 불법·유해 행위를 감소시키기 위한 인터넷 가치사슬에서의 규제 활동이 성공할 가능성은 그만큼 증가한다.

첫째, 인터넷 가치사슬에서 불법·유해 정보 생산 축소 전략을 추진해야 한다. 콘텐츠 생산자, 콘텐츠 수집자, 웹 호스트의 불법·유해 콘텐츠의 생

산 활동을 제약함으로써, 국내에 유입되는 불법·유해 콘텐츠의 양을 감소시켜야 한다.

둘째, 인터넷 가치사슬에서 불법·유해 정보 접근 제한 전략을 추진해야 한다. 인터넷서비스사업자, 검색과 내비게이션, 사용자 장치에 대한 규제를 통해 불법·유해 정보에 접근을 제한하는 다양한 규제 정책과 기술을 도입해야 한다.

인터넷서비스사업자들에 대한 공적 규제와 자율 규제가 공존하는 협력공간이 필요하다. 인터넷서비스사업자들에게 법률적 책임을 강화함과 동시에 사업자를 대표하는 민간자율기구의 역할과 기능을 확대하여 자율적으로 이해관계를 해결하고 조정하도록 해야 한다.

인터넷서비스사업자는 불법·유해 정보 차단을 위한 기술개발과 장비도입 비용을 사회적 책임(ISO 26000)에 참여하는 사회적 투자로 인식해야 한다. ISO 26000의 소비자 이슈인 '소비자의 건강 및 안전보호' 차원에서 불법·유해 정보에 대한 접근 규제에 자발적으로 참여해야 한다.

해외인터넷접속서비스를 제공하는 모든 사업자들이 차단 장비를 설치하게끔 하여, 우회 접속에 대한 가능성을 줄여야 한다. 차단 우회기술의 발전함에 따라, 정부차원에서 지속적으로 새로운 차단기술 발전 추세를 분석하고, 우회 대응 기술을 개발·보급함으로서 효과적으로 해외 불법·유해 정보를 차단시킬 필요가 있다.

다양한 정부 기관이 차단대상사업자에게 차단요청을 의뢰하는 경우, 업무의 중복성과 복잡성이 증가하여 차단 업무 효율성과 생산성이 낮아질 가

능성이 많다.

이를 개선하기 위해, 차단통합지원센터를 구축하여 업무 효율성을 높일 필요가 있다. 청소년이 성인인증을 쉽게 받지 못하도록 하는 다양한 조치들이 추진되어야 한다. '그린 I-Net'에서 제공하는 14개 소프트웨어의 성능 평가 기준을 개발하고, 성능시험을 통해 개별 소프트웨어의 성능 정보를 학부모와 사용자들에게 제공해야 한다.

셋째, 인터넷 가치사슬에서 불법·유해 정보 접근에 대한 자율성 확대를 통한 접근 감소 전략을 추진해야 한다. 우리나라 청소년들은 주로 가정에서 인터넷 검색을 통한 불법·유해 정보 접속 비율이 가장 높다는 점에서, 개인의 자율성과 자정 능력 향상을 위한 다양한 인터넷 윤리 교육과 안전성 교육을 실시해야 한다. 이러한 운동은 범국민적 생활운동으로 확산시켜야 한다.

다양한 한계를 극복하고 인터넷의 불법·유해 정보를 차단하기 위해서는 인터넷 가치 사슬의 8개 기능을 효과적으로 연계하고 통합 관리해야 한다. 8개 기능의 연계와 통합관리는 매우 어려운 도전이지만, 관계 기관들의 협력과 노력을 통해 실현 가능하다. 8개 기능별로 실효성 있는 정책과 기술을 적용하기 위한 정부의 지속적인 노력, 민간 사업자의 자발적 참여, 사용자의 자율성 확대가 필요한 시점이다.

# 참고문헌

**<국내문헌>**


1. 김성천,「ISO26000(사회적 책임)제정 움직임과 소비자 정책의 과제」, 소비자정책동향 (제5호), 2008.7.20
2. 노미숙, 「인터넷상의 청소년 유해정보의 실태와 차단 방안 연구」, 부산대학교 교육대학원, 2004
3. 박형민, 「인터넷 유해사이트의 실태와 대책에 관한 연구」, 한국형사정책연구원, 2005
4. 백욱인, 「인터넷에서의 표현의 자유 보호를 위한 정책 연구 보고서」, 국가인권위원회, 2004
5. 송금연, 「인터넷상 음란물 규제에 대한 형사법적 고찰」, 전남대학교 대학원, 2003
6. 양훈석, 「사이버스페이스에서 청소년유해정보의 차단기술」, 단국대학교 정보통신대학원, 2004
7. 유승화・김성조・김희동・염현영・이준원, 「인터넷음란물 차단을 위한 기술방안 연구」, 청소년보호위원회, 2000
8. 이원태, 「인터넷 참여문화의 성숙을 위한 정책방향」, 정보통신정책연구원, 2009한국인터넷문화의 특성과 발전방안 심포지엄 발표자료, 2009.11.26
9. 장우영・안명규, 「세계의 인터넷 자율규제시스템 비교 고찰을 통한 한국 인터넷 언론의 자율규제 제도화 방안 연구 : EU・미국의 현황과 한국의 과제」, 신문발전위원회, 2007
10. 정보통신윤리위원회, 「U-사회에서의 정보이용 건전성 확보방안」, 정보통신윤리위원회, 2006

11. 정재봉, 「사이버 범죄의 실태와 대책에 관한 연구」, 원광대학교 행정대학원, 2007
12. 정 완, 사이버공간상 불법·유해정보의 합리적 규제방안, 한국형사정책연구원, 2003
13. 한명호・서경원・최정윤・김상욱, 「불법・유해정보의 유통방지를 위한 형사규제의 실효적 확보방안」한국형사정책연구원, 2007
14. 한국정보사회진흥원, 「해외 주요국 인터넷 규제현황과 시사점」, 한국정보사회진흥원, 2008
15. 한국정보사회진흥원, 「인터넷 자율규제 확산을 위한 정채 이슈 도출 및 개선방안 수립에 관한 연구」, 한국정보사회진흥원, 2007
16. 현대경제연구원, 「'SR26000'의 도입과 사회적 자본」, 09-49(통권 378호), 2009.12.11

**<외국문헌>**

1. ACMA, 「Closed Environment Testing of ISP-Level Internet Content Filtering」, 2008.6
2. ACMA, 「Developments in Internet Filtering Technologies and Other Measures For Promoting Online Safety, First Annual Report to the Minister for Broadband, Communications and the Digital Economy, Australian Communications and Media Authority」, Feb. 2008.
3. ACMA, 「Developments in internet filtering technologies and other measures for promotion online safety, Second annual report to the Minister for Broadband, Communication and the Digital Economy, Australian Communications and Media Authority」, April. 2009.
4. Paul Greenfield, Peter Rickwood, Huu Cuong Tran., 「Effectiveness of

Internet Filtering Software Product」, CSIRO, Sep. 2001.
5. GIFC, 「Defeat Internet Censorship: Overview of Advanced Technologies and Products」, Global Internet Freedom Consortium, White Paper, 2007
6. Ofcom, 「Online Protection」, June. 2006.
7. Ofcom, 「Ofcom's Response to the Byron Review」, 2008.3.
8. Ronald Deibert, John Palfrey, Rafal Rohozinski, Jonathan Zittrain, eds., 「Access Denied: The Practice and Policy of Global Internet Filtering」, Cambridge: MIT Press, 2008.

**<국내 웹사이트>**

1. 경찰청 사이버테러대응센터
2. 국회 전자도서관
3. 방송통신위원회
4. 방송통신심의위원회
5. 보건복지가족부
6. 사행산업감독위원회
7. 한국인터넷진흥원
8. 한국인터넷진흥협회
9. 한국정보화진흥원
10. 형사정책연구원

<해외 웹사이트>


1. http://cafe.daum.net/naneoneonaism
2. http://circamp.eu/index.php?option=com_weblinks&view=category&id=3&Itemid=3
3. http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG
4. http://firephoenix.edoors.com/
5. http://gpass1.com/gpass/
6. http://groups.yahoo.com/group/Songun2
7. http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html#time
8. http://internet.watch.impress.co.jp
9. http://kofree.net
10. http://kofree.wordpress.com/
11. http://nlnet.nl/
12. http://soraro.info
13. http://www.acma.gov.au
14. http://www.anyvpn.net/
15. http://www.big.or.jp
16. http://www.big.or.jp/~jrldr/index.html
17. http://www.childnet-int.org/
18. http://www.connectsafely.org/
19. http://www.crn.com/security/212002220
20. http://www.dit-inc.us/
21. http://www.edoors.com
22. http://www.engagelive.net/
23. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+AGENDA+20081020+SIT+DOC+XML+V0//EN

24. http://www.europol.europa.eu/index.asp?page=InternetRelatedChildAbusiveMaterialProject
25. http://www.fsm.de/en/SubCoC_Search_Engines
26. http://www.gardennetworks.org
27. http://www.geocities.com/songunpoliticsstudygroup
28. http://www.GetNetWise.org/
29. http://www.homeoffice.gov.uk/
30. http://www.iia.net.au/
31. http://www.ikeepsafe.org/
32. http://www.internetfreedom.org
33. http://www.isafe.org
34. http://www.ispa.org.uk/
35. http://www.iwf.org.uk
36. http://www.kaisernetwork.org
37. http://www.lunastorm.se
38. http://www.missingchildreneurope.eu/index.php?option=com_content&view=article &id=70& Itemid=57
39. http://www.missingkids.com
40. http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId= 3703
41. http://www.mivpn.com
42. http://www.ncsl.org/programs/lis/cip/filterlaws.htm
43. http://www.ofcom.org.uk/
44. http://www.opennetinitiative.org
45. http://www.playahead.se
46. http://www.playboy.com
47. http://www.safeweb.com

48. http://www.spotspam.net/goals.html
49. https://www.torproject.org/
50. http://www.UltraReach.net
51. http://www.wego.6-sys.com/main/
52. http://www22.verizon.com/ResidentialHelp/HighSpeed/Email/Blocked+Email/QuestionsOne/123706.htm
53. https://www.exilekorea.net/

**<법률 및 지침>**

1. 게임산업진흥에관한법률
2. 국가정보화기본법
3. 문화산업진흥기본법
4. 방송통신위원회의설치및운영에관한법률
5. 방송통신위원회의 설치 및 운영에 관한 법률 시행령
6. 방송통신심의위원회 기본규칙
7. 성폭력범죄의 처벌 및 피해자보호 등에 관한 법률
8. 성폭력범죄의 처벌 및 피해자보호 등에 관한 법률 시행령
9. 온라인디지털콘텐츠산업발전법
10. 전기통신기본법
11. 전기통신사업법
12. 전기통신사업법 시행령
13. 전파법
14. 정보통신망 이용촉진 및 정보보호 등에 관한 법률
15. 정보통신망 이용촉진 및 정보보호 등에 관한 법률시행령

16. 정보통신에 관한 심의규정
17. 청소년보호법
18. 청소년보호법 시행령
19. 청소년의 성보호에 관한 법률
20. 청소년의 성보호에 관한 법률 시행령
21. 풍속영업의규제에관한법률
22. 형법
23. 해외 불법정보 차단업무 처리지침

1. 본 연구보고서는 방송통신위원회의 출연금 등으로 수행한 방송통신정책연구용역사업의 연구결과입니다.
2. 본 연구보고서의 내용을 발표할 때에는 반드시 방송통신위원회 방송통신정책연구용역사업의 연구결과임을 밝혀야 합니다.