클라이언트/서버 환경에서 유해정보차단을 위한 시스템의 설계 및 구현
(The Design and Implementation of System for Blocking the Harmful Information on Client/Server Environment)

염 태 영(Tae-Young Yum)*

요 약

인터넷 유해정보를 차단하기 위해서는 차단목록에 의한 차단 방안을 기반으로 한 차단 프로그램이 많이 사용되고 있다. 그러나 차단목록에 의한 차단 방안은 클라이언트 PC의 성능 저하와 같은 문제점들을 발생시킨다. 본 논문에서는 차단목록에 의한 차단 방안의 문제점들을 극복할 수 있는 효율적인 방안을 제안한다. 클라이언트/서버 환경에서 차단목록을 차단목록서버에 두고, 웹 사용자의 사이트 재방문 패턴을 이용한 허용목록을 클라이언트 PC에 도입하는 것이다. 본 논문의 실험에서, 제안하는 방안은 클라이언트 PC의 성능 저하를 초래하지 않으면서 차단목록에 의한 차단 방안보다도 상당한 속도 향상을 보여 준다.

ABSTRACT

A intercepting program of Black List Filtering System is widely used for blocking the harmful information in the internet. But The Black List Filtering System give rise to reduce the performance of Client PC. In this thesis the author proposes the good way to solve a problem of the Black List Filtering System. Keep to the point that is puting the black List into The Black List Serve on Client/Server Environment and building Black List into Client PC in use of revisiting pattern of web-user. The best effect that tried to solve the problem in the experiment concerning the thesis is presented not only to maintain the performance of Client PC, but also to improve the speed of performance of Client PC.

* 정회원 : 거창전문대학
컴퓨터정보시스템과 전임강사

논문접수 : 2003. 9. 5.
심사완료 : 2003. 9. 24

1. 서론

최근 네트워크의 발달로 인한 인터넷의 급속한 팽창은 각급 학교에서도 컴퓨터를 이용하여 손쉽게 인터넷과 접속 할 수 있는 환경을 제공하고 있으며, 저가형 PC의 광범위한 보급은 청소년 개개인의 컴퓨터 보유 및 인터넷과의 접속을 가능하게 해주고 있다. 그렇지만, 인터넷은 어린이와 청소년에게 유해한 정보도 방대한 양을 포함하고 있다. 인터넷이 개방화되고 또 자유로운 속성 때문에 심지어 어린이들과 청소년들도 전 세계 도처에 널려 있는 웹 사이트들을 자유롭게 탐험할 수가 있다. 하지만, 어느 누구도 그들이 인터넷을 통해 유해한 정보에 자유롭게 접근하는 것을 바라지 않는다. 인터넷을 통해 전송되는 부적절한 정보로부터 그들은 보호받아야만 한다[1,2].

현재, 인터넷의 유해 정보로부터 어린이와 청소년을 보호하기 위해서 차단 프로그램이 가장 보편적으로 사용되고 있다. 차단 프로그램은 각 개인의 컴퓨터에 설치되어 사용자의 인터넷 접근을 감시하고 부적절한 인터넷 정보로의 접근을 차단하는 기능을 제공한다. 이러한 기능을 수행하기 위해서 대부분의 차단 프로그램은 일반적으로 차단목록에 의한 차단(Black List Filtering) 방안을 사용한다[9]. 차단목록에 의한 차단방안은 인터넷상에 존재하는 유해 정보 사이트들의 주소로 구성된 차단목록을 사용한다. 차단목록은 사용자로부터 보안성을 유지하기 위해서 암호화된다. 사용자가 사이트에 접근할 때, 차단 프로그램은 암호화된 차단목록을 검색한다. 사용자 접근 사이트가 차단목록에서 발견되면, 차단 프로그램은 사용자 접근 사이트가 유해한 것으로 간주하고 사용자의 사이트 접근을 차단한다. 그러나, 차단목록에 의한 차단 방안은 사용자의 클라이언트 PC에 암호화되어 저장된 차단목록만을 이용하기 때문에 차단목록에 대한 갱신, 보안 그리고 클라이언트 PC의 성능 저하와 같은 주된 문제들을 발생시킨다. 인터넷의 폭발적으로 성장하는 속성 때문에 날마다 차단목록 서버의 차단목록에는 수백에서 수천 개의 유해 정보 사이트들의 주소가 추가 될 수 있지만, 즉시 클라이언트 PC의 차단목록에는 변경된 내용을 반영하기 어렵다. 또한, 차단목록은 유해 정보 사이트들의 주소로 구성되어 있기 때문에 클라이언트 PC의 사용자에게 차단목록이 유출되는 것을 막아야 한다. 이를 위해 암호화와 같은 방법을 통해 차단목록에 대한 보안이 필요하다. 사용자의 인터넷 응용 프로그램이 사용자가 접근하려는 사이트와 연결을 설립할 때마다, 차단 프로그램은 사용자 접근 사이트의 주소를 클라이언트 PC에 저장된 차단목록에서 매번 검색한다. 그러나, 보안을 위해서 차단목록은 이미 암호화되어 있기 때문에 사용자 접근 사이트의 주소를 암호화해서 검색해야 하며, 차단목록의 크기가 메인 메모리에 적재될 수 없을 만큼 거대하기 때문에 검색 부하가 심한 외부검색을 요구한다. 이와 같이 클라이언트 PC의 차단목록을 기반으로 한 차단목록에 의한 차단 방안은 매우 높은 필터링 비용이 소요됨으로써 클라이언트 PC의 성능을 심각하게 저하시켜 다른 응용 프로그램의 정상적인 운용을 방해한다. 또한, 사용자에게 인터넷 통신 지연뿐만 아니라, 차단 프로그램의 필터링에 따른 지연을 추가로 느끼게 한다. 따라서, 차단목록에 의한 차단방식의 차단 프로그램으로 인한 클라이언트 PC의 성능 저하는 사용자의 큰불만을 초래하게 된다.

본 연구에서는 차단목록에 의한 차단 방안의 문제를 해결하기 위해서 클라이언트/서버 분산환경에서 유해정보를 차단하는 새로운 방안을 제안한다. 제안하는 방안은 차단목록을 클라이언트 PC에서 차단목록 서버로 이동시키고, 웹 사용자들이 한번 방문한 사이트를 재방문하는 허용목록을 도입한다. 허용목록은 개별 사용자가 방문한 사이트들 가운데, 비유해

하다고 판단된 사이트들의 주소로 구성되며, 클라이언트 PC에서 유지 관리된다. 차단목록에 의한 차단 방안은 차단목록을 이용하여 사용자 접근 사이트의 유해성만을 검사한다. 그러나, 제안하는 방안은 허용목록을 이용하여 사용자 접근 사이트의 비 유해성을 먼저 검사하고, 필요한 경우에는 차단목록을 이용하여 사용자 접근 사이트의 유해성을 검사하는 방식이다.

2. 인터넷 유해정보 차단 기술

2.1 구현 방안에 따른 분류

인터넷 필터링은 인터넷에 존재하는 임의의 정보에 대해 접근이나 유입을 차단하는 처리를 말한다. 인터넷 필터링은 주로 다음과 같은 목적으로 사용된다. 첫째, 인터넷을 사용하는 어린이와 청소년들이 그들에게 부적절한 인터넷 정보로 접근하는 것을 차단한다. 둘째, 고용인들의 생산성 향상을 위해, 인터넷을 사용하는 고용인들이 인터넷을 업무 관련 일에만 사용하도록 제한한다. 본 장에서는 인터넷 필터링의 방법과 차단 위치를 기준으로 인터넷 필터링을 분류하고, 각각의 방안에 대해서 기술한다. 인터넷 필터링은 일반적으로 구현하는 방법에 따라서 차단목록에 의한 차단(black list filtering), 허용목록에 의한 차단(white list filtering), 내용등급에 의한 차단(neutral label filtering)으로 구분되어진다[9]. 이들 방안들은 독립적으로 사용되거나, 결합되어진 형태로 사용될 수 있다.

차단목록에 의한 차단은 부적절한 정보를 가진 인터넷 사이트들의 주소로 구성된 차단목록을 기반으로 사용자의 사이트 접근을 차단한다[9]. 사용자가 인터넷 사이트에 접근할 때, 차단 프로그램은 차단목록을 검색한다. 사용자 접근 사이트가 차단목록에서 발견되면, 차단 프로그램은 사용자 접근 사이트가 사용자에게 부적절한 것으로 판단하고 사용자의 사이트 접근을 차단한다. 그러나, 사용자 접근 사이트가 차단목록에서 발견되지 않으면, 사용자의 사이트 접근은 허용된다. 따라서, 차단목록은 정확해야 하며, 많은 부적절한 사이트들의 주소를 포함해야 한다. 엄청난 수의 인터넷 사이트들 가운데 부적절한 정보를 가진 사이트들을 선별해서 차단목록을 구축하는 것은 대단히 어려운 일이지만, 차단목록에 의한 차단 방안은 현재의 인터넷 환경에서 가장 효과적이며, 구현이 용이하기 때문에 대부분의 차단 프로그램에 사용되고 있다.

허용목록에 의한 차단은 차단목록에 의한 차단 방안과 정반대의 개념을 사용한다. 차단 프로그램의 관리자는 유용하고 안전한 인터넷 사이트들의 주소로 구성된 허용목록을 구축한다. 허용목록에 의한 차단 방안은 허용목록에 검증되어 포함된 사이트들 이외에 사용자가 접근하는 모든 사이트들에 대해서는 접근을 차단한다. 따라서, 이 방안은 인터넷의 부적절한 정보로의 접근이나 유입에 대해서 매우 안전한 방안이다. 그러나, 허용목록에 의한 차단 방안은 적절함이 검증된 극소수의 사이트들에 대해서만 사용자의 접근을 허용하기 때문에, 사용자의 인터넷 사용을 매우 제한한다. 이와 같은 이유 때문에 일반적으로 허용목록에 의한 차단 방안은 특수한 목적을 위해서 인터넷의 접근을 극도로 제한하는 경우에 사용된다[9].

내용등급에 의한 차단 방안은 차단목록이나 허용목록과 같은 목록을 사용하지 않는다. 이 방안의 주된 아이디어는 인터넷 사이트에 존재하는 정보에 대해서 등급화하는 기능과 필터링하는 기능을 분리한다. 사용자가 인터넷 사이트에 접근시 내용 선택 프로그램은 웹 문서 작성자나 내용 등급 서비스 업체에서 제공하는 해당 사이트의 등급 레이블을 기반으로 사이트 접근 여부를 결정한다. 내용등급에 의

한 차단 방안은 고도의 유연성과 보안성을 제공할 수가 있는 장점을 갖는다. 그러나, 최근까지도 거의 대부분의 인터넷 사이트들은 등급화 되어 있지 않다. 만약 어린이나 청소년이 등급화 되지 않은 사이트에 접근한다면, 차단 프로그램은 불법적이고 유해한 사이트로부터 그들을 보호할 수가 없다. 그래서, 내용등급에 의한 차단 방안은 많은 장점을 가졌지만, 현재의 인터넷 환경에서는 효과적이지 못하다[4].

2.2 사용자 측면에 따른 분류

앞 절에서 설명된 세 가지 인터넷 필터링 방안들은 집이나 학교, 또는 직장내의 클라이언트 PC와 서버 기반의 네트워크 필터링 시스템에 각각 구현되어질 수 있다[10]. 클라이언트 기반의 필터링은 개별적인 클라이언트 PC에서 이루어진다. 클라이언트 기반의 차단 목록에 의한 차단 방안에서는 차단 프로그램과 차단 목록은 사용자의 클라이언트 PC에 저장되어 사용자가 유해 정보 사이트에 접근하는 것을 차단한다. 클라이언트 기반의 필터링은 사용자마다 개별적인 차단 프로그램을 사용하기 때문에 인터넷 사용의 유연성 및 효과적인 필터링을 제공할 수 있지만, 클라이언트 PC의 성능 저하를 야기하며, 차단목록을 유지관리하기 어려운 단점을 가지고 있다. 서버 기반의 필터링은 사용자의 클라이언트 PC가 아니라, 인터넷의 서비스를 제공하는 네트워크 단계에서 사용자들의 접근을 제어한다. 서버 기반의 네트워크 필터링 시스템을 네트워크에 설치하여 운영함으로써 네트워크 내의 전체 워크스테이션에 대한 필터링을 수행할 수 있다. 서버 기반의 필터링은 관리비용의 절감, 차단목록 변경의 용이함, 그리고 향상된 보안성을 제공 하지만, 네트워크 내의 전체 워크스테이션에 대해서 획일적인 필터링을 수행하기 때문에 개별 사용자에게 인터넷 접근의 유연성을 제공하지는 못한다.

3. 기존 유해정보차단 시스템

오늘날의 자유롭고 개방적인 인터넷 상황에서 차단목록에 의한 차단 방안은 유해정보 차단에 가장 효과적인 방안으로 알려져 있다[10]. 현재, 대부분의 차단 프로그램에서는 이 방안을 기반으로 한다. 하지만, 차단목록에 의한 차단 방안은 거대한 크기의 차단목록을 클라이언트 PC에서 암호화하여 유지해야 하기 때문에 몇 가지 주된 문제점을 가지고 있다. 본 장에서는 차단목록에 의한 차단 방안의 동작과정을 설명하고, 문제점에 대해서 지적한다.

3.1 동작 과정

차단목록에 의한 차단 방안은 차단목록을 사용하여 사용자가 접근하는 사이트의 유해성 여부를 판단한다. 차단목록은 유해정보를 가진 사이트들의 주소로 구성되며, 불순한 목적의 사용자로부터 차단목록의 유출을 방지하기 위해서 일반적으로 암호화된다. 차단 프로그램은 사용자가 차단목록에 포함된 사이트에 접근할 때는, 유해 정보 사이트에 접근하는 것으로 판단하고 사이트 접근을 차단한다. 그러나, 차단목록에 포함되지 않은 사이트로의 접근은 허용한다. 차단목록에 의한 차단 방안에서 차단 프로그램이 사용자 접근 사이트의 유해성 여부를 정확하게 판단하고 차단하기 위해서는 차단목록이 보유한 유해정보 사이트들의 주소가 정확하며 충분히 많아야 한다. 그러나, 현재 인터넷에는 수 백만 사이트들이 존재하며 계속적으로 폭발적인 증가를 보이고 있기 때문에 사람의 힘만으로는 유해정보 사이트를 분류하고 충분한 양의 차단목록을 구축하는 것은 대단히 어려운 일이다. 대부분의 차단 프로그램에서 사용되는 차단목록은 인터넷에 존재하는 유해정보 사이트를 자동으로 색출하여

차단목록을 구축하는 유해정보 색출 시스템의 서비스에 의해 구축된다. 또한, 보다 정확한 차단목록의 구축을 위해서 많은 인력이 동원되기도 한다.

3.2 문제점

클라이언트 기반의 차단목록에 의한 차단 방안은 대부분의 차단 프로그램에서 폭 넓게 사용되는 방식이지만, 차단 프로그램은 클라이언트 PC 내에 이미 암호화되어 저장된 거대한 차단 목록을 이용하기 때문에 다음과 같은 문제점을 갖는다.

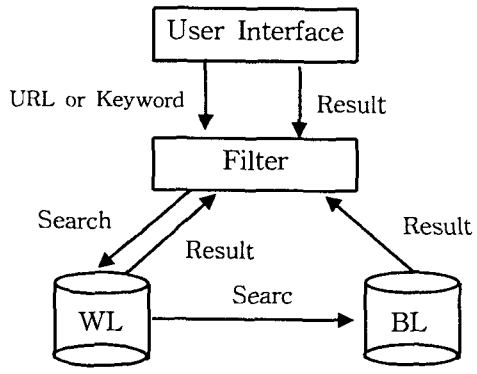
첫 번째 문제는 차단목록 갱신의 문제이다. 유해정보 색출 시스템은 계속적으로 생성되거나 변경되는 인터넷상의 유해정보 사이트를 자동으로 검색하여 차단목록을 변경한다. 변경된 차단목록은 차단목록 서버에 반영되기 때문에 하루에도 수 천 개에 이르는 유해 정보 사이트들이 차단목록에 추가된다. 차단 프로그램이 사용자 접근 사이트가 유해 정보 사이트인지 정확하게 판단하기 위해서는 차단목록 서버의 차단목록에 추가된 내용을 즉시 반영해야 만 한다. 그러나, 클라이언트 기반의 차단 프로그램은 클라이언트 PC 내에 이미 저장된 차단목록을 기반으로 동작하기 때문에 차단목록 서버의 차단목록에 새롭게 변경된 내용을 즉각적으로 반영하기가 어렵다.

두 번째 문제는 차단목록 보안의 문제이다. 차단목록에 의한 차단 방안에서는 유해 정보 사이트들의 주소로만 구성된 차단목록이 사용자의 클라이언트 PC에 저장되어 유지된다. 만약 불순한 목적의 사용자에 의해 차단목록이 외부로 노출되면, 차단목록의 의도된 목적과 다르게 사용되는 심각한 문제가 발생될 수 있다. 따라서 클라이언트 PC 내에 저장된 차단목록이 사용자에게 그대로 노출되는 것을 막기 위해서 암호와 같은 보안 방안이 필요하다.

세 번째 문제는 차단 프로그램의 필터링 부하로 인해 발생되는 클라이언트 PC의 성능저하이다. 차단목록은 보통 수십 만개의 유해 정보 사이트들의 주소를 암호화하여 구성된 거대한 크기의 목록이다. 차단 프로그램은 차단목록의 크기가 너무 커서 메인 메모리에 적재할 수 없기 때문에, 높은 검색 부하를 가진 외부 검색을 통해서 사용자 접근 사이트의 유해성 검사를 시도한다. 이러한 작업들은 큰 부하와 시간을 요구하기 때문에 클라이언트 PC의 전체적인 성능을 저하시키게 된다. 차단 프로그램이 사용자의 인터넷 접근을 감시, 필터링 및 차단하는 과정은 사용자에게 성능의 투명성을 제공하는 가운데 이루어져야 한다. 차단 프로그램으로 인한 다른 응용 프로그램의 성능저하를 초래하거나, 인터넷 사용에 심각한 지연을 초래한다면 사용자가 차단 프로그램의 사용을 기피할 수도 있기 때문이다.

4. 유해정보 차단 도구의 구현

4.1 컨텐츠의 설계



[그림 1] 유해정보 차단 도구의 모형
[Fig. 1] The model of tool for blocking the harmful information

4.2 컨텐츠의 구성

4.2.1 차단필터

차단필터는 웹 브라우저 등의 인터넷 접속 프로그램과 한글 윈도우 98사이에서 동작하면서 기본 차단주소목록과 관리자가 관리도구를 통해 설정한 유입방지정보에 따라 유입방지 기능을 수행하게 된다. 유해정보를 제공하는 사이트의 주소를 주소목록에 미리 등록해 놓고, 사용자가 특정 사이트에 접속을 시도할 때 차단목록에 등록된 사이트일 경우는 접속을 불허하고 그렇지 않을 경우 접속을 허용한다. 만약 접속이 허용되었다 하더라도 인터넷 내용물이 사용자목록에 등록된 음란, 폭력 등 유해단어를 포함하고 있다면 최종적으로 어린이에게 보여지지 않는다. 그리고 관리자가 설정해놓은 요일별 인터넷 사용 가능 시간대 및 최대 인터넷 사용시간에 따라 어린이의 인터넷 사용시간을 제어한다. 또한 어린이가 인터넷에 접속한 내역을 기록하여 관리자가 효과적으로 관리하도록 함으로써 어린이의 건전한 인터넷 사용을 유도할 수 있다.

4.2.2 관리도구

관리도구 실행시 항상 사용자인증 과정을 거치게 하여 관리자만이 관리도구를 이용하여 유입방지 정보를 설정할 수 있도록 한다. 관리도구를 이용해 관리자는 요일별 인터넷 접속 시간대와 최대 사용시간을 설정할 수 있으며, 유해사이트 주소 및 유해단어를 추가 및 삭제할 수 있다. 그리고 인터넷 사용내역 보기 등을 통해 관리자가 인터넷 사용관리 및 소프트웨어 관리를 손쉽게 할 수 있도록 해 준다. 또한 관리자가 필요시 차단기능을 해제시켜 인터넷을 아무런 제약 없이 사용할 수도 있다.

4.2.3 허용목록

차단 프로그램의 관리자는 유용하고 안전한 인터넷 사이트들의 주소로 구성된 허용목록을 구축한다. 허용목록에 검증되어 포함된 사이트들 이외에 사용자가 접근하는 모든 사이트들에 대해서는 접근을 차단한다. 따라서, 이 방안은 인터넷의 부적절한 정보로의 접근이나 유입에 대해서 매우 안전한 방안이다.

4.2.4 차단목록

차단필터가 차단동작을 수행하는데 기초가 되는 유해사이트의 주소목록이다. 만약 차단될 리스트에 등록이 되어 있다면 다음 단계로 넘어 가고 차단될 리스트에서 가져온 URL과 일치하는 URL를 찾지 못했다면 다음단계로 단어 검색을 한다. 일단 가져온 URL로 접속하여 HTML 소스를 다운받는다. 소스만 받는 것이므로 인터넷 속도에는 별 영향을 미치지 않는다. 이 소스를 차단될 단어 리스트와 검색한다. 만약 차단될 단어 리스트와 같은 것이 있다면 차단될 주소 리스트에 추가하고 설정된 것을 차단하게 된다. 그리고 차단필터 수행시 주소목록에의 접근속도가 빨라야 한다. 오용방지를 위해 암호화되어 있다.

4.2.5 안전장치

유해정보 유입방지도구가 설치된 이후에 도구의 차단필터를 수행시키지 않았거나 도구를 비정상적으로 삭제하였을 경우에는 인터넷 접속 자체를 불가능하도록 함으로써 차단필터의 동작을 보장시키기 위한 기능이다.

4.2.6 설치 및 삭제 프로그램

설치 및 삭제를 용이하게 하기 위해 만들어진 프로그램이다.

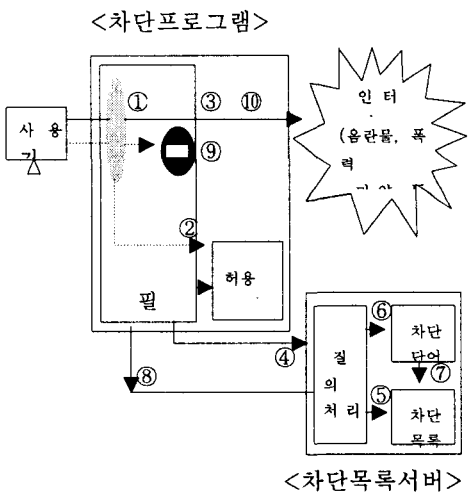
4.3 컨텐츠의 개발

4.3.1 개발환경 및 구현

본 연구에서 개발할 시스템을 운영하기 위

하여 Windows 2000 서버를 채택하였으며, 웹 서버는 차단목록을 저장하기 위해 윈도우용 웹서버인 IIS(Internet Information Server) 5.0을 포함하고 있다. 그리고 웹 응용프로그램의 구성 요소로서 HTML파일, 데이터의 조작을 위하여 ASP를 이용하여 시스템을 구축하였고 차단 목록 내용 등을 저장한 데이터베이스 서버로 MS
-Access 2000을 이용하였다.

4.3.2 컨텐츠 모델

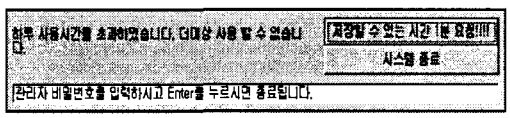


[그림 2] 유해정보 차단 도구의 동작과정
[Fig. 2] The process of performance of tool for blocking the harmful information

단계①) 차단 프로그램은 사용자의 인터넷 사이트 접근을 감시한다.
단계②) 사용자가 인터넷 사이트로 접근을 시도하면, 차단 프로그램은 사용자 접근 사이트의 주소를 접근목록에서 내부 검색한다.
단계③) 사용자 접근 사이트의 주소가 허용목록에서 발견되면 사용자의 사이트 접근을 허용하고 단계①로 이동한다.
단계④) 허용목록에서 사용자 접근 사이트가 발견되지 않으면, 차단목록 서버에 사용자 접근 사이트의 주소를 질의한다.
단계⑤) 차단목록 서버는 사용자 접근 사이트가 차단목록에서 발견되면, '접근 차단'을, 그렇지 않은 경우는 '접근 허가'를 차단 프로그램에 응답한다.
단계⑥) 차단될 리스트에서 가져온 URL과 일치하는 URL를 찾지 못했다면 다음단계로 단어 검색을 한다. 일단 가져온 URL로 접속하여 HTML 소스를 다운 받아 차단될 단어 리스트와 검색한다. 만약 차단될 단어 리스트와 같은 것이 있다면 차단될 주소 리스트에 추가하고 설정 된 것을 차단하게 된다.
단계⑦) 차단될 주소 리스트에 추가한다.
단계⑧) 차단 프로그램은 차단목록 서버의 응답이 '접근차단'인 경우 사용자의 사이트 접근을 차단하고 단계①로 이동한다.
단계⑨) 차단 프로그램은 차단목록 서버의 응답이 '접근허가'인 경우 사용자의 사이트 접근을 허용한다.
단계⑩) 차단 프로그램은 접근 허가된 사이트 주소를 허용목록에 추가하고 단계①로 이동한다.

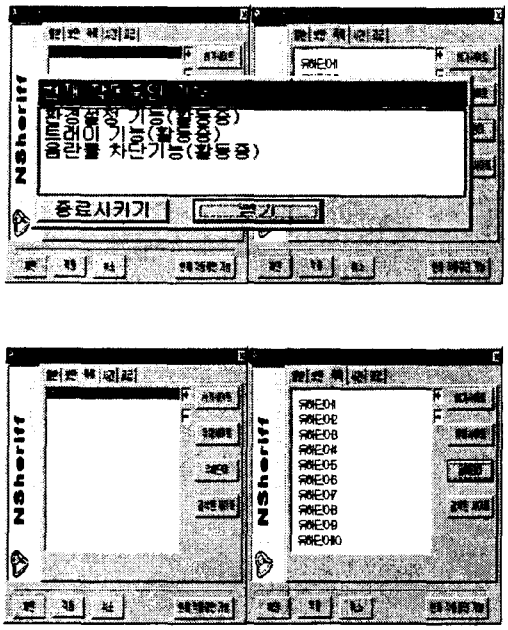
4.4 컨텐츠의 실행

4.4.1 설정(일반)



[그림 3] 환경설정도구 실행화면
[Fig. 3] A Execution-Scene for Setting tool of environment

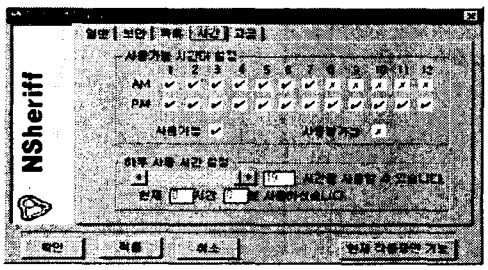
4.4.2 목록설정(허용목록/차단목록)



[그림 4] 허용목록/차단목록/차단단어 실행화면

[Fig. 4] A Execution-Scene for index of permission/index of blocking/word of blocking

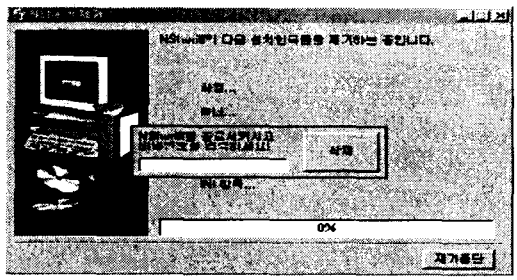
4.4.3 사용시간 설정 및 제한도구



[그림 5] 사용시간 설정 및 제한도구 실행화면

[Fig. 5] A Execution-Scene for Install of the useful time and Limit of tool

4.4.4 무단삭제 방지 도구



[그림 6] 무단삭제 방지 실행화면

[Fig. 6] A Execution-Scene for blocking an illicit remove

4.4.5 목록 암호화

[그림 7] 목록 암호화 저장 화면

[Fig. 7] A Scene of preservation of an index' code

4.5 실행 결과 분석

본 장에서는 차단목록에 의한 차단 방안과 클라이언트/서버 분산환경에서 차단목록을 서버에 두고 유해 정보를 차단하는 방안의 성능 비교를 위해 상업용 웹브라우저를 사용하는 10명의 웹 사용자들로부터 4주간의 웹 사용에 대한 데이터를 수집하여 웹 사용자의 사이트 재방문 패턴을 분석한 결과 웹 사용자들은 한 번 방문한 사이트를 대부분 다시 방문하며, 소수의 몇몇 사이트들을 빈번하게 재방문하는 패턴을 발견하였다. 이와 같은 웹사용자의 사이트 재방문 패턴을 이용한 허용목록을 클라이언트 PC와 차단 목록을 서버에 도입하므로

써 상당한 필터링 성능의 향상을 얻을 수가 있었다.

5. 결론 및 향후 연구과제

본 연구에서는 인터넷상에서 해당 사이트의 유효 여부를 먼저 판단하여 유효하지 않는 사이트는 불필요한 접근 시도를 방지하고 유효한 사이트인 경우 유해 여부를 판단, 유해 사이트를 차단하는 새로운 방안인 클라이언트/서버 분산환경에서 차단목록을 서버에 두고 유해 정보를 차단하는 시스템을 설계 및 구현하였다. 이 방안은 기존의 차단목록에 의한 차단 방안이 가졌던 차단목록 갱신, 보안 및 클라이언트 PC의 성능 저하와 같은 주된 문제점들을 해결할 수가 있다. 본 연구의 실험에서는 수백 개의 사이트 주소를 포함한 허용목록을 사용하는 클라이언트/서버 분산환경에서 차단목록을 서버에 두고 유해 정보를 차단하는 방안이 LAN 환경과 WAN 환경에서도 차단목록에 의한 차단 방안보다도 향상된 속도를 얻었다. 허용목록의 사용율이 증가되면, 차단목록의 외부 검색 시간이 감소한다. 클라이언트/서버 분산환경에서 차단목록을 서버에 두고 유해 정보를 차단하는 방안은 클라이언트 PC의 성능 저하를 초래하지 않으면서 인터넷상의 불법적이고 유해한 사이트로의 접근을 차단할 수 있도록 지원하는 효율적인 방안이다.

현 컨텐츠에서는 단어만을 대상으로 자료를 분석하여 유해 정보를 차단하는데 보다 정확한 차단을 위해서는 단어에 대한 분석보다는 문맥에 대한 분석이 보다 효과적이라 할 수 있다. 뿐만 아니라 본 검색 시스템에서 유해 사이트의 검색은 텍스트로만 검색할 수 있게 되어 있다. 그러나 실제 유해 사이트들은 텍스트뿐만 아니라 유해 이미지들을 동시에 가지고 있어 텍스트만을 가지고 검색을 시도하다 보면 많은 이미지로 구성된 유해 사이트는 검색되지 않을 경우도 있다. 따라서 텍스트와 이미지를 같이 검색할 수 있다면 더 많은 유해 사이트를 효과적으로 차단할 수 있을 것이다. 향후 연구 과제는 보다 효과적인 분석을 위해 문맥에 대한 분석이 가능하도록 검색 시스템을 설계하는 것과 텍스트와 이미지를 같이 검색할 수 있도록 확장하는 것이다.

참고 문헌

[1] YWCA 청소년유해감시단, "컴퓨터 통신 음란물 모니터 보고서", URL:http://myhome. netsgo.com/pywca/보고서.htm

[2] 김성운, 김인홍, 강현석, "유해 정보 차단을위한 데어터 관리 에이전트들의 설계 및 구현", 한국정보처리학회 추계학술발표논문집 제6권 제2호, pp DB62-67, 1999

[3] 김성운, 김성진, 강현석, "웹 문서 분석/검색 시스템의 설계 및 구현", 한국정보처리학회 춘계학술발표논문집 제6권 제1호, pp235-238, 1999 [4] 유병전, "웹 사용자의 사이트 재방문 패턴을 이용한 인터넷 유해 정보 차단 방안", 1999

[5] 정회, "유해 정보 차단을 위한 검색 시스템의 설계와 구현", 1999

[6] 이민구, "인터넷 유해정보 유입방지 방안에 관한 연구", 1998

[7] 김효남, "인터넷에서 청소년 보호를 위한 음란물 접속차단 방안 연구", 1999

[8] 김민중, "네트워크 모니터링에 의한 유해정보 차단", 2001

[9] European Union Communication on illegal and harmful content on the internet.

Online document can be found at
URL
http://europa.eu.int/en/record/legal/index.htm
[10] P. McCrea, B. Smart and M. Andrews 1998, Blocking content on the internet. Online document can be found at
URL:
http://www.cmis.csiro.au/pubs.html

염태영

2000~ 경일대학교 컴퓨터공학과 박사과정 수료
2002~현재: 거창전문대학 컴퓨터 정보시스템과 전임강사
관심분야: 웹데이터베이스, XML응용