



No Spam! No Virus! No Robot!

Clean Board Institute

게시판 스팸차단 노하우

- 게시판 스팸을 차단하는 11가지 비법 -

게시판 스팸차단 연구소

CBI Networks / bShield 사업본부

목 차

1. 왜? 내 홈페이지 게시판에 스팸을 남기는가?	3
2. 어떻게 남기는가?	4
3. 스팸을 차단하는 11가지 비법	5
A. 필터링 시스템을 이용한 차단	5
B. Referer를 이용한 차단	6
C. IP를 이용한 차단	7
D. Cookie를 이용한 차단	9
E. Session을 이용한 차단	10
F. 주소(URL)변경을 이용한 차단	10
G. 게시판 속성을 이용한 차단	12
H. 이미지 입력을 이용한 차단	13
I. 회원제를 이용한 차단	14
J. Active-X 프로그램을 이용한 차단	14
K. 관련법규 홈페이지 등재하여 차단	15
4. 스팸 로봇 프로그램을 피해가는 방법	16
5. 스팸게시물을 효율적으로 관리하는 노하우	18
6. 맺음말	20

1. 왜? 내 홈페이지 게시판에 스팸을 남기는가?

내 홈페이지 게시판에 스팸을 남기는 가장 큰 이유는 '자신의 사업을 홍보하기 위해서' 다. 오버추어, Naver 파워링크, Daum, Google 애드워즈, Empas, Nate, Yahoo! 등 홍보하기 위한 훌륭한 공간이 있다. 이러한 곳에는 사람들이 많이 찾을 뿐 아니라 접속률도 높아 홍보 효과를 톡톡히 볼 수 있다.

그런데 왜? 홍보를 하기 위해 내 홈페이지까지 찾아오는 이유는 무엇일까?

복잡한 이유가 있는 것은 아니다. 비용을 적게 투자하기 위함 이다.

일례를 들어 보겠다.

네이버 파워링크 시스템에 "홈페이지 제작" 키워드로 클릭 광고를 집행 하려고 한다.

파워링크 1위로, 1명의 방문자를 모집하는데 20,850원의 비용이 든다(CPC). 2위 10,000원, 5위는 9,160원이다. (2007년 11월 현재)

파워링크 5위로 광고를 진행하여 하루에 100명씩 30일간 유입한다면 총 얼마의 광고비가 들겠는가?

$$9,160\text{원} * 100\text{명} * 30\text{일} = 27,480,000\text{원}$$

소기업, 소상공인, 1인 기업 등에서는 광고비에 이만큼 투자할 여력이 되지 않는다.

하지만, 앞서 보았던 홈페이지 게시판에 광고를 하면 얼마가 들겠는가?

프로그램 이용료 또는 광고 의뢰비용 20~50만원이면 수만~수백만 개 홈페이지에 광고 글을 남길 수 있다. 그로 인해 유입되는 방문자 수가 2,700만원의 유료 광고보다 효과가 더 좋다.

두 번째로 비용 문제 외에 게시판으로 광고해야 효과가 좋은 사업이 있다.

최근 등록되는 스팸 광고글의 내용은 성인, 카지노, 도박, 대출이 주를 이루고 있다. 이와 같은 업종은 해외에 서버를 두고 불법 영업을 하는 경우가 많기 때문에 정상적인 방법으로는 광고를 할 수 없는 경우가 허다하다.

따라서 법의 감시망을 피하고, 정상적인 루트를 이용하면서 결제내역 등에 자신의 정보를 노출시키는 것과 정상적인 광고 루트를 기피하고 홈페이지 게시판에 글을 남기는 이유도 있다.

2. 어떻게 남기는가?

홈페이지 게시판에 올라오는 스팸은 시도 때도 없다. 어떤 날은 수십 개의 글이 올라오기도 하고, 어떤 때는 누르자마자 스팸 게시자의 홈페이지로 바로 이동해버려 지을 수도 없는 글이 올라온다.

이러한 스팸글은 적게는 수천 개에서 많게는 수백만 개의 홈페이지 게시판에 남기는데, 하루에도 몇 번씩 올라오는 것은 사람이 직접 남기는 것이 아니라 프로그램이 남기는 것이기 때문에 가능하다.

사람이 게시판에 글을 남기는 과정은 이러하다.



로봇이 게시판에 글을 남기는 과정은 사람이 직접 남기는 것과 다른 점이 있는데, 크게 3가지로 분류할 수 있다.

1. 게시판 DB 입력파일에 직접 데이터를 전송하여 글을 남긴다.
2. 실제 사람이 접속하는 것과 똑같이 홈페이지 게시판에 접속하여 데이터를 작성 후 글을 남긴다.
3. 실제 사람이 글을 남기는 것과 같이 데이터를 생성하여 게시판 DB 입력파일에 데이터를 전송하여 글을 남긴다.

각각의 상황에 대해 자세히 알아보겠다.

1. 게시판 DB 입력파일에 직접 데이터를 전송하여 글을 남긴다.

홈페이지 게시판에 글을 작성하는 부분은 크게 2가지로 나누어진다. 첫째는 글을 입력하는 것이고, 둘째는 데이터를 DB에 입력하는 것이다. 첫 번째 타입의 로봇 프로그램은 둘째 파일에 직접 접속하여 데이터 정보를 바로 전송하여 글을 남긴다.

그렇기 때문에 단어 필터링, IP차단 등의 방지 정책이 효과가 없다. 이렇게 글을 남기는 이유는 단어 필터링, IP 차단을 피해하려는 목적도 있지만 빠른 속도로 여러 개의 게시판에 작업을 할 수 있기 때문이다.

2. 실제 사람이 접속하는 것과 같이 데이터를 생성하여 게시판 DB 입력파일에 데이터를 전송하여 글을 남긴다.

실제 사람은 인터넷 익스플로러(Internet Explorer)를 사용하여 홈페이지 게시판에 접속한 후, 글쓰기를 눌러 글을 남기게 된다. 이 방식을 그대로 본 따 사용하는 방식이다. 때문에 로봇 프로

그럼이지만 실제 사람이 입력하는 것과 거의 동일한 효과를 낼 수 있다. 하지만 단어 필터링, IP 차단 등으로 차단할 경우 글 등록을 막는 것이 가능하다.

3. 실제 사람이 글을 남기는 것과 같이 데이터를 생성하여 게시판 DB 입력파일에 데이터를 전송하여 글을 남긴다.

1번과 2번의 장점을 합하여 새로 나타난 방식이다. 실제 사람이 직접 입력하는 것과 같이 모든 정보(Cookie, Session, Referer, ETC ...)를 가상으로 만들어 DB 입력파일에 직접 전송한다. 때문에 이 프로그램으로 남겨지는 스팸글은 단어 필터링, IP 차단도 통하지 않을 뿐 아니라 빠른 속도로 여러 번 올릴 수 있는 기능이 있어 차단하기 어렵다.

3. 스팸을 차단하는 11가지 방법

스팸을 남기는 기술이 갈수록 정교해지고 있기 때문에, 아직까지 스팸 게시물을 100% 구분하여 차단할 수 있는 방법은 존재하지 않는다. 하지만 가능한 모든 방법을 적용하고 새로운 유형의 스팸에 대처 하면서 꾸준히 관리를 하면 대부분 차단할 수 있다.

1. 필터링 시스템을 이용한 차단

가장 기본적으로 취할 수 있는 것이 "필터링 시스템을 이용한 게시판 스팸글 차단" 이다.

자주 올라오는 광고글을 보면서 어떠한 단어가 필수적으로 들어가는지, 또한 어떻게 변형이 되는지 파악하여 기록을 한다.

만약 성인, 포커에 관련된 내용이 자주 올라온다면 다음과 같은 방법으로 단어 필터링을 구성한다.

1차 스팸 단어는 [성인, 포커]

2차 스팸 단어는 [성-인, 성+인, 성☆인, 포-커, 포^커] 등 스팸 단어 사이에 특수문자를 끼워넣어 스팸 게시물로 인식이 안 되도록 변형된 단어를 구성한다.

(게시판 스팸글을 올리는 광고주는 보통 하루에도 몇 번씩 스팸을 올리려고 시도한다. 그리고 필터링 시스템을 가동할 것을 예상하기에 단어를 지속적으로 변형하면서 올린다. 그렇기 때문에 필터링 시스템을 한 번 적용한 것으로는 효과가 없으며, 지속적으로 관리하며 업데이트 해주어야 비로소 효과를 볼 수 있다.)

게시판 스팸 차단을 위한 필터링 시스템을 적용하려면 홈페이지 관리자모드를 살펴보아야 한다. 대부분 특정 단어를 거부할 수 있는 필터링 시스템이 마련되어 있다. 그 곳에 기록한 단어를 넣어주면 게시판 스팸 차단을 위한 필터링 시스템이 가동되는 것이다.

만약, 홈페이지 관리자모드에 해당 내용이 없다면, 프로그래머에게 부탁하여 설치할 수 있다. 비용도 그다지 많이 들지 않는다. 정기적인 유지보수 업체와 계약을 맺고 있다면 무료로 해줄 수

도 있고, 그렇지 않다면 보통 10만원 내외에서 설치가 가능하다.

이런 필터링 시스템으로 완벽히 막을 수는 없지만, 이 시스템에 의해 걸러지는 스팸 프로그램도 있으니, 어느 정도 효과는 볼 수 있다.

게시판 스팸글을 남기는 구 프로그램은 필터링 시스템에 걸리는 것이 많으나, 게시판 스팸글을 남기는 신 프로그램은 필터링 시스템을 무효화 할 수 있는 로직을 가지고 있는 것이 대부분이다. 하지만 이것 마저 안 하게 되면 더욱 많은 스팸에 시달리게 될 것이다.

2. Referer(레퍼러)를 이용한 차단

인터넷에서 발생하는 Referer 정보를 이용하여 게시판 스팸 차단하는 방법 이다.

Referer 정보란? 어디서부터 왔는지 알아보는, 즉 발자취 이다.

홈페이지를 운영해보았다면 방문자 통계 화면을 본 적이 있을 것이다. 통계화면의 주 구성 내용은 보통 다음과 같다.

1. 접속 IP (예: 222.223.224.100)
2. 접속 URL (예: <http://domain.com>)
3. 접속 시간 (예: 2007년 12월 31일 오전 07시 55분 51초)
4. 접속 OS (예: Microsoft Windows XP)
5. 접속 브라우저 (예: MS IE 6.0)

위의 화면에서 **2번, 접속 URL이 바로 Referer 정보다.**

Referer 정보를 이용하여 **게시판 스팸 차단을 하려면 게시판 구조에 대해 알아야 한다.**

홈페이지 게시판 입력 시스템은 2가지로 구분된다.

1. 이름, 제목, 내용 등을 입력하도록 사용자에게 보여주는 화면
 2. 내용을 다 입력하면 Database 시스템에 입력하도록 처리하는 프로그래밍 시스템
- 1번 -> 2번으로 넘어가면서 2번에서는 1번의 주소를 Referer로 인식하게 된다.

스팸 프로그램 중 일부 프로그램은 1번을 거치지 않고 직접 2번 시스템에 접근하여 글을 남기도록 설계되어 있다. 1번을 거치지 않으면 Referer 정보가 존재하지 않는다.

2번 시스템에서 Referer를 체크하여 정보가 존재하지 않을 때, 글쓰기를 차단하는 로직을 작성하면, 위와 같은 설계를 가진 프로그램에서 남기는 게시판 스팸글 차단을 할 수 있다.

PS: 단, 프로그램의 종류가 많고, 각각 로직이 틀려 1번을 거쳐 들어오는 프로그램도 있고, 2번 시스템에 직접 접근하지만 Referer 정보를 임의로 생성하여 보내는 경우도 있다. 그렇기 때문에 모든 스팸을 차단할 수 없지만 위의 시스템을 적용하면 어느 정도 효과를 볼 수 있다.

3. IP를 이용한 차단

대한민국 국민이면 주민등록번호가 있어 사람을 구별할 수 있다. 인터넷을 통해 접속하는 컴퓨터에는 주민등록번호와 비슷하게 해당 컴퓨터를 식별할 수 있는 번호가 있는데 그 것을 바로 IP라 한다.

IP를 분석하여 알아낼 수 있는 정보는 다음과 같다.

- A. IP 사용 기관 명
- B. 기관 주소
- C. IP 네트워크 담당자 전화번호, E-Mail 주소
- D. 국가
- E. 지역

위의 정보를 이용하여 스팸 광고를 차단할 수 있는 방법은 3가지가 있다.

첫째로 IP주소 목록을 만들어 차단하는 방법이다.

스팸 게시물을 올리려면 하나 또는 여러 대의 컴퓨터에서 로봇 프로그램을 가동하여 등록하게 된다. 이 때 가동하는 컴퓨터 IP주소를 홈페이지 게시판에 기록하여 해당 IP를 다시 올리지 못하도록 IP차단을 한다.

IP는 유동IP, 고정IP가 있다. 말 그대로 유동IP는 변하고, 고정IP는 변하지 않는다. 이렇게 되어 있는 이유는 IP범위가 000.000.000.000 ~ 255.255.255.255이기 때문이다. 255씩 4자리를 단순 계산하면 약 42억 개 IP를 사용할 수 있는데, 컴퓨터 숫자가 이보다 많으므로 접속할 때마다 사용하지 않고 비어있는 IP를 부여해 유동적으로 사용할 수 있게 설계해 놓은 것이 유동IP다.

일반 가정 컴퓨터 IP주소는 항상 켜져 있는 서버와 다르게 유동적으로 변하므로, 대부분 유동IP로 운영되고 있다. 유동IP는 보통 다음과 같은 패턴으로 변한다.

예를 들어 지금 사용하고 있는 IP 주소가 250.241.113.17 이라 가정해보자. 이 IP주소를 사용한다. 컴퓨터 전원을 끄고, 다음날 다시 접속을 하면 IP주소 끝자리가 바뀌어 있다.

250.241.113.101, 250.241.113.92 이런 예와 같이 뒷자리가 변하게 된다.

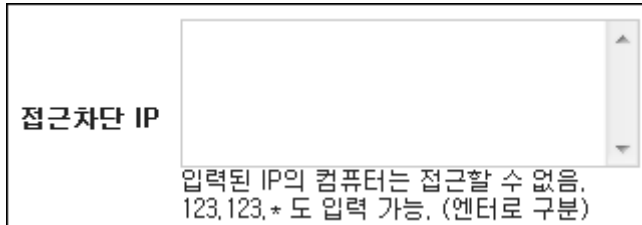
뒷자리가 변하는 이유는 IP주소 배분방식이 A, B, C 클래스가 있는데, 그 중 C 클래스를 대부분 사용하기 때문이다. 클래스에 관련된 사항은 IP주소 배분의 기본 방식이므로 해당 전문 서적을 찾아보길 권한다. 여기서는 C 클래스가 IP주소 가장 뒷자리를 변화시킨다고 이해하면 되겠다.

대부분의 IP가 유동IP기 때문에 IP주소를 차단할 때에 스팸글을 남기는 IP를 직접 차단하면 효과가 크지 않다. 변할 수 있는 IP를 생각하여 뒷자리를 모두 포함하도록 차단해야 한다.

예를 들어, 위와 같이 스팸이 들어왔다면 250.241.113.1 ~ 250.241.113.255 까지 모두 차단한다.

이렇게 차단하면 스팸을 남기는 컴퓨터에서 수시로 IP를 바꾸며 기록을 시도해도 모두 차단되어 있기 때문에 스팸이 차단된다.

IP차단 하는 방법은 홈페이지 관리자 모드에 탑재되어 있는 IP차단 메뉴를 사용하여 스팸글을 등록하는 IP를 차단한다. 지금 운영하고 있는 홈페이지 관리자 모드를 확인해 보면 (그림3-3-1) 과 같이 접근차단 IP를 설정할 수 있는 메뉴가 있다.



(그림3-3-1)

위와 같은 메뉴에 스팸을 등록하는 IP를 설정하면 차단 할 수 있다. 만약, 홈페이지 관리자모드에 해당 내용이 없다면, 프로그래머에게 부탁하여 설치할 수 있다. 비용도 그다지 많이 들지 않는다. 정기적인 유지보수 업체와 계약을 맺고 있다면 무료로 해줄 수도 있고, 그렇지 않다면 보통 10만원 내외에서 설치 할 수 있다.

이 방법으로 스팸을 차단하면 해당 IP에서 등록되는 것을 차단할 수 있다. **하지만 스팸글을 남기는 로봇 프로그램의 종류에 따라 차단되지 못하는 경우가 있는데, 로봇 프로그램이 IP차단을 무마시키는 로직을 개발하여 그 방법으로 글을 남기거나, IP주소 자체를 조작하여 글을 남기는 경우다.**

따라서 위 방법으로 IP차단을 해도 똑 같은 스팸이 100% 차단되지 않는다. 하지만 위 방법으로 차단할 수 있는 스팸이 있으므로 설치하지 않는 것 보다 어느 정도 효과는 볼 수 있다.

둘째로 IP대역폭을 조사하여 해당 국가 전체를 차단한다.

모든 IP는 국제도메인센터에서 관리하여 각 국가별, 지역별로 배분하여, 혼선이 없게 사용하도록 하고 있다. 이 IP의 국가 및 지역 정보를 활용하여 스팸글을 올리는 로봇 프로그램의 국가를 차단하면 스팸 게시물을 어느 정도 차단할 수 있다.

등록되는 스팸글 중 영어로만 이루어진 외국 스팸글이 등록되는 경우를 보았을 것이다. 대부분 외국에서 만든 로봇 프로그램으로, 스팸글이 등록되는 주기가 짧아 자주 올라오며, 때로는 페이지가 자동으로 이동되어 지을 수 없기도 하고, 제목이 없어 클릭 되지 않아 애를 먹기도 한다.

외국 프로그램이 등록되는 곳은 어디일까? 대부분 한국에서 남기지 않는다. 외국에서 남기게 된다. 따라서 IP대역폭을 조사하여 외국 IP 전체를 차단한다면 외국 스팸글을 차단할 수 있다. (IP대역폭 자료는 CBI 자료실에서 다운받아 확인할 수 있다. <http://cleanboard.net>)

이 방법 역시 부작용이 있다. 한국 외의 모든 국가를 차단하였을 경우 외국에서 접속하는 정상적인 사용자 역시 홈페이지 접속이 불가능해 지는 것이므로, 타격을 입을 수 있고, 실제 외국인을 상대로 홈페이지를 운영하면 사용할 수 없다.

하지만 국내 전용으로 운영하고 있는 홈페이지는 이 방법이 어느 정도 효과를 가져올 수 있다. 실제로 어떤 홈페이지에서는 이 방법을 적용하여 매일 30건씩 올라오던 스팸글 대부분을 차단한 예가 있다.

하지만 첫 번째 IP주소로 차단하는 방법과 같이, 프로그램에서 IP주소 체크하는 부분을 무마시키거나, IP주소를 조작하여 글을 등록한다면 이 방법 역시 무용지물이다.

셋째로 IP사용 기관 담당자에게 연락하여 올리지 못하도록 하는 방법이다.

위 3번 항목에서 IP를 분석하여 스팸을 차단하는 정보에 대하여 알아 보았다. 그 중 IP사용 기관 명, 기관 주소, 네트워크 담당자 전화번호, E-Mail 등을 활용해 차단하는 방법이다.

위에서 살펴본 항목 중 유동IP에 대해서 이해하였을 것이다. 그렇다면 고정IP란 무엇일까?

일반 가정과 달리 회사, PC방, 기관 등에서는 컴퓨터를 항상 켜 놓는 경우가 많다. 그런 곳에서는 내부 직원들이 항상 접속 가능해야 하기 때문에 IP가 변하지 않고 고정적으로 쓸 수 있도록 부여해 주는 것이 바로 고정 IP다.

이를 이용해서 스팸글을 등록하는 IP가 기관에 속해있다면 해당 기관 담당자에게 연락을 취하여 올린 스팸글 내용을 확인시키고, 더 이상 올리지 못하도록 당부할 수 있다. 만약 그럼에도 계속 등록을 시도한다면 불법스팸대응센터(<http://www.spamcop.or.kr>)에 신고하면 '정보통신망 이용촉진 및 정보보호 등에 관한 법률' 제 50조 7의 위반으로 처벌받게 된다.

대부분 유동 IP에서 스팸을 올리게 되며, 고정 IP에서 올리는 경우는 드물어 효과가 그리 크지 않다.

4. Cookie(쿠키)를 이용한 차단

Cookie란 인터넷 웹사이트 방문기록을 남겨 사용자와 웹사이트 사이를 매개해 주는 정보이다. 인터넷을 하게 되면 자연스럽게 남는 정보인데, DB에 직접 접속하여 스팸글을 남기는 로봇 프로그램은 Cookie 정보를 만들지 못하기 때문에 Cookie를 이용해 차단할 수 있다.

Cookie를 만들 수 있는 방법은 다양하다. ASP/JSP/PHP 웹 언어 스크립트로 만들 수 있고, JavaScript로 만들 수 있다. 만드는 방법은 계약된 유지보수 업체나 프로그래머에게 부탁하면 알 수 있다.

이를 이용해 실제 스팸차단 하려면 홈페이지 접속 시 Cookie를 생성하고, 글이 등록되는 순간 Cookie 존재여부를 판단하여 생성되지 않는다면 로봇 스팸으로 간주하고 차단 한다. 생성방법과 차단하는 방법은 다양하게 변형할 수 있기 때문에 여기서는 그 세부적인 내용은 다루지 않겠다.

이를 이용해 어느 정도 스팸을 차단할 수 있으나, **요즈음 진화된 스팸 로봇 프로그램은 Cookie를 사람이 직접 접속하는 것과 똑같이 만들어 스팸등록을 시도한다. 따라서 스팸 로봇 프로그램 중 Cookie 정보를 생성하지 못하는 곳에만 차단이 가능하다.**

5. Session(세션)을 이용한 차단

사용자와 컴퓨터 또는 두 대의 컴퓨터간 활성화된 접속을 Session이라 한다. 즉, 인터넷을 하는 일반 컴퓨터와 내용을 보여주는 홈페이지 서버의 연결고리다. Cookie와 비슷하지만 Cookie는 일반 사용자 컴퓨터 파일에 저장되기 때문에 조작이 간단하지만 Session은 홈페이지 서버에 기록 되는 것이기 때문에 조작이 어렵다.

Session은 서버에 기록을 남기기 때문에 ASP/JSP/PHP 등 웹 언어 스크립트로만 만들어 사용할 수 있다. 만드는 방법 및 사용하는 것 모두 Cookie와 비슷하다.

이 방법을 잘 못 사용하면 이미 접속이 끝난 사용자를 계속 접속자로 인식하여 서버의 Session공간이 부족하게 되어 홈페이지 서비스에 장애를 일으키게 된다. 따라서 사용하려 할 때에는 예외상황 대비를 잘 하는 프로그래머에게 부탁 해야한다.

이를 이용해 차단하는 것 또한 취약점이 있다. **본래 세션은 접속자 에게만 생성되는 것이지만, 새로 개발된 스팸 로봇 프로그램은 자신이 접속자로 인식되어 서버에 세션이 생성되도록 하거나, 세션 체크 자체를 무시하고 글을 등록하는 경우가 있다. 하지만 역시 적용하지 않았을 때 보다 차단 확률이 높아지는 것은 사실이다.**

6. 주소(URL) 변경을 이용한 차단

이 방법을 사용하려면 스팸 로봇 프로그램의 구조에 대해 조금 이해하면 된다. 스팸 로봇 프로그램 중 대부분은 홈페이지에 접속하여 게시판을 찾은 뒤 그 주소를 저장하고 글 등록 시 저장된 주소로 접속하여 글을 남기게 된다.

그렇다면 이걸 어떻게? 게시판에 접속할 수 있는 주소를 매번 변경하는 것이다. 주소를 매번 변경하면 스팸 로봇 프로그램에서는 저장된 목록으로 접속을 시도하고 정상적으로 접속을 할 수 없기 때문에 목록에서 삭제해 버린다.

주소를 변경하는 방법은 간단하다. 가장 많이 사용하는 제로보드(ZEROBOARD)를 기준으로 설명하겠다. 제로보드의 게시판관리 화면 (그림 3-6-1)을 보면 게시판 이름을 설정하는 곳이 있다.

게시판 이름	<input type="text"/>
스킨 설정	bbs ▼

(그림 3-6-1)

바로 저 부분을 변경하면 주소가 바뀌게 된다. 예를 들어 board -> boarda 로 변경했다고 하자.
 http://domain.com/board.php?id=board -> http://domain.com/board.php?id=boarda
 뒤에 써진 id 부분이 해당 게시판을 구분하는 주소인데 그 것이 변경되므로 스팸 로봇프로그램
 에서는 인지할 수 없다.

매일 주기적으로 바꾸어 주면 스팸 로봇 프로그램은 당신 홈페이지에 글 남기는 것이 더욱 어
 려워 질 것 이다.

이 방법을 사용함으로써 적용할 업무가 더 늘어나게 되는데, 게시판 주소는 id로 관리가 되기
 때문에 바로 변경할 수 없고 삭제 후 다시 생성하여야 한다. 즉, 기존 게시板的 데이터를 백업
 한 후 삭제하고 새로운 게시판을 만들어 그 게시판에 백업해둔 데이터를 삽입하는 것이다.

게시판 주소가 변경되면 홈페이지 서버도 인식을 할 수 없게 되므로 서버내의 파일도 수정된 id
 에 맞게 변경해 주어야 정상적으로 작동할 수 있다.

이 방법을 사용함으로써 얻을 수 있는 효과는 상당히 크다. 실 예로 어떤 홈페이지에 적용한 결
 과 90% 이상의 차단률을 보였다. 대부분의 스팸 로봇 프로그램이 위와 같이 주소를 변경하게
 되면 속수무책으로 당한다.

하지만 외부에 링크를 사용하는 홈페이지의 경우 게시판 주소가 매번 변경되면 기존 주소로는
 접속을 할 수 없기 때문에 다른 조치가 필요하거나 사용을 피해야 한다. 또한 주소 변경 당시
 글을 쓰던 사용자가 있는 경우 작업을 완료했을 때에 오류가 나게 되므로 이에 대한 대책도 필
 요하다.

위는 제로보드로 예를 들었지만, 그 외 모든 게시판도 적용이 가능하다.

7. 게시판 속성을 이용한 차단

일반적으로 게시판의 글쓰기 화면은 다음과 같이 구성되어 있다.

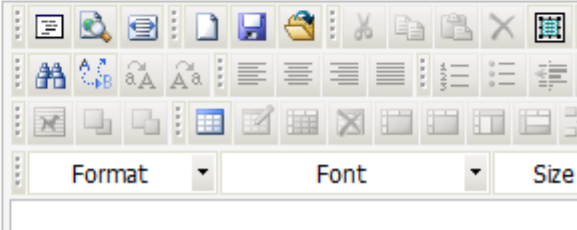
성함

전자메일

홈페이지

설정 태그사용 답변메일 받기

제목

문의내용 

이 중 게시판에 글을 남기기 위해 필수적으로 입력해야 하는 항목이 있다.

- 이름
- 비밀번호
- 제목
- 내용

보통 위 4가지 항목이 필수고 그 외에 선택적으로 늘어나거나 줄어든다.

스팸 로봇 프로그램은 필수로 입력되는 내용의 게시판 필드 이름을 기억하고 있다. 예를 들어 게시판 등록 폼에서 다음과 같이 설정되어 있다고 가정해보자.

- 이름: name
- 비밀번호: password
- 제목: subject
- 내용: content

스팸 로봇 프로그램은 게시판 주소와 위의 정보를 함께 저장해두고 글 등록할 때 DB입력파일에 직접 데이터를 전송해 글을 남기게 된다. 따라서 위의 이름, 비밀번호등의 사용자 정의 이름을 수시로 변경하여 주면 6번의 방법과 동일한 효과를 볼 수 있다.

이 방법으로 차단하면 6번 주소(URL)변경을 이용한 차단의 단점인 외부 링크 문제를 해결할 수 있다. 차단방법은 게시판 소스 내의 글쓰기폼의 이름, 비밀번호등의 필드 이름을 직접 수정하고 글쓰기 완료폼에서 바꾼 이름으로 체크한 필드 데이터를 받아 처리하면 된다.

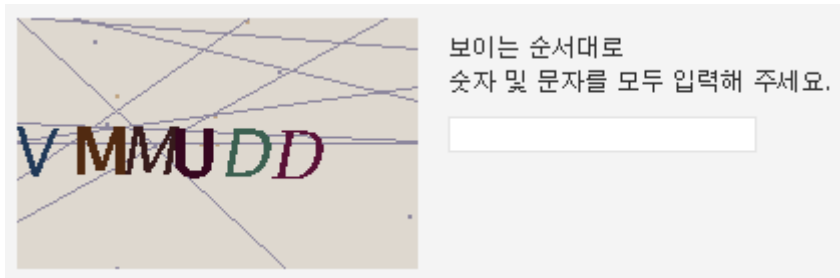
이 방법은 들어가는 노력에 비해 차단효과가 크지 않다. 매일 일정한 주기로 수시 변경해주어야

하는데 비해 스팸 로봇프로그램은 단지 필드명 뿐만 아니라 필드의 속성까지 체크하도록 진화하였기 때문이다. 비밀번호를 입력하는 필드는 PassWord 속성, 내용을 입력하는 필드는 TextArea속성 등 일정한 패턴이 있고 이 것을 읽도록 한다.

하지만 아직도 예전 방식으로 작동되고 있는 스팸 로봇 프로그램이 많기 때문에 어느 정도 효과는 볼 수 있고, 부작용도 적은 편이다.

8. 이미지 입력을 이용한 차단

게시판 글 등록 시 숫자가 포함된 이미지 파일을 보여주고(그림 3-8-1) 그 숫자와 동일하게 입력한 경우에만 정상적으로 인식하여 등록하는 차단 방식이다.



(그림 3-8-1)

이 방법은 로봇이 등록하지 못하는 강력한 수단이 되어, 많은 홈페이지에서 도입하고 있다. 이미지 입력 방식을 사용하면 실제로 90% 이상의 스팸 로봇 프로그램이 걸러지게 된다. 이미지를 인식하여 존재하는 숫자, 문자를 인식하여 입력하고 스팸을 등록시키는 로봇 프로그램은 개발되는 단계라 그 수가 적어 많은 차단 효과를 볼 수 있다는 장점이 있다.

이미지 입력 솔루션을 설치하는 과정도 큰 비용이 들어가지 않는다. 프로그래머에게 부탁하거나 홈페이지 유지보수 업체에게 의뢰하면 10만원 내외에 설치가 가능하다.

단, 강력한 만큼 단점이 있는데, 일반 사용자까지 불편을 겪는다는 점이다. 상품문의, 자유토론 등 활성화를 위해 게시판을 운영하는데 이미지의 숫자, 문자를 한 번 더 치는 과정은 불편을 주어 참여율을 떨어뜨리게 된다. 특히 나이 지긋한 분들의 경우 시스템을 제대로 이해하지 못하고 글을 못 남기는 경우가 많다. 회원가입 등 간헐적으로 사용되는 메뉴에나 어울리는 차단방법인 것이다.

실제로 이미지 입력 방식 사용 후 게시판 참여율을 조사해본 결과 도입하기 전에 비해 평균 30% 정도 줄어든 것으로 통계결과가 나타났다. (CBI 자체시행, 커뮤니티 운영자 7명 대상)

인터넷 대형 포털 Daum의 경우 카페가입을 할 때에 위와 같은 이미지 보안코드를 입력하도록 하였으나 그 이용 불편도가 높아지자 폐지하여 버렸다. 따라서 커뮤니티 활성화 차원에서는 추천하지 않는 방법이다.

9. 회원제를 이용한 차단.

스팸을 차단하는 가장 빠르고 확실한 방법은 모든 커뮤니티 공간을 회원만 입력 가능하도록 변경하는 것이다. 제 아무리 스팸 로봇 프로그램이라도 회원가입을 하여 로그인한 대상만 글을 남길 수 있는 곳에 등록하기란 쉽지 않다.

설치방법도 간단하다. 홈페이지에서 사용하는 게시판이 제로보드 등 유명한 게시판이거나 회사의 정형화된 솔루션일 경우 대부분 회원제 기능을 지원한다. 관리자모드에서 회원만 글을 남길 수 있도록 설정만 해주면 곧바로 적용되어 스팸글에서 해방될 수 있다.

만약 이러한 기능이 지원되지 않는 게시판을 사용하고 있다면, 유지보수 업체 또는 프로그래머에게 부탁하면 5만원 내외의 금액만으로 회원제를 운용할 수 있다.

스팸을 차단하는 가장 강력하고 확실한 방법이지만 그만큼 부작용이 크다. 위의 8번과 같이 커뮤니티 활성화에 크게 방해가 된다. 단순 커뮤니티 활성화뿐만 아니라 쇼핑몰 또는 기업의 경우 **일반 문의, 상담을 회원가입까지 하면서 남기는 경우는 드물기 때문이다.**

따라서 이 결정을 할 때에는 홈페이지의 사황이 바뀔 수도 있으므로 신중하게 고려하여 결정하여야 한다. 인터넷과 같이 오픈된 공간에서는 폐쇄적인 회원제 운영방식이 통용되기 힘들기 때문이다.

그리고 또한 위 방법도 문제가 있다. 최근 새로 개발되고 있는 스팸 로봇 프로그램은 홈페이지의 회원가입 및 로그인 시스템을 분석하여 회원가입을 하고 스스로 글을 남기는 지능형으로 변하고 있기 때문이다. 아직은 그 수가 적으나 지능형 스팸 로봇 프로그램은 더욱 확산될 전망이다.

하지만 **회원제를 사용할 경우 99%의 스팸을 차단할 수 있으므로, 자유로운 참여를 제한시켜도 되는 홈페이지에는 적용시켜 사용할 경우 큰 효과를 볼 수 있다.**

10. Active-X를 이용한 차단.

윈도우 응용프로그램을 인터넷과 결합시켜, 인터넷 익스플로러에서 사용 가능하도록 설계된 것이 Active-X 다. Active-X는 일련의 설치과정을 거쳐 사용자의 컴퓨터 상에서 수행하게 된다. 보통 Active-X는 실제 작동하는 과정은 응용프로그램과 비슷하고 인터넷상에서 쉽게 설치가 가능하기 때문에 악용하는 사례가 많으나 은행, 카드사 등 금융기관과 공공기관에서도 많이 사용하고 있다.

Active-X로 프로그램을 작성하게 되면 게시판 스팸이 절대 올라오지 못하도록 스팸 필터링 및 로봇 차단을 할 수 있다. 하지만 이 것은 전문프로그래머가 아니면 설치하기 힘들다. 당신이 계약을 맺고 있는 유지보수 업체에서도 적용하지 못할 수 있다. 따라서 이 것을 설치하려면 적지 않은 금액을 투자하여야 한다.

그런데 투자하는 비용만큼 많은 효과를 얻을 수 있는 것도 아니다. Active-X는 악용되는 곳(특히 바이러스, 악성코드 등의 설치)이 많아서 인터넷 사용자들은 신뢰할 수 있는 홈페이지가 아닌 곳에서 제공하는 Active-X 컨트롤은 설치하지 않는다.

오히려 설치하라는 경고창이 뜬다면 그 즉시 창을 꺼버리고 홈페이지를 닫는 경우가 부지기수이다. 회원가입보다 Active-X 설치를 더 꺼려하는 사용자가 있을 정도다. Active-X를 적용하려면 그만큼 홈페이지 신뢰도가 받쳐주어야 한다.

홈페이지 신뢰도가 받쳐주고, 얼마만큼의 비용을 투자할 준비가 되었다면 Active-X를 이용한 스팸 차단 방법을 적용하는 것이 큰 도움이 될 것이다. 하지만 그 반대로 아직 신뢰도가 높지 않고 간헐적으로 문의 글을 받는 입장이라면 오히려 Active-X를 적용함으로써 손해를 보게 된다.

11. 관련법규 홈페이지 등록하여 차단

불법스팸대응센터(<http://www.spamcop.or.kr>)에서는 '정보통신망 이용촉진 및 정보보호 등에 관한 법률' 제 50조 7항을 위반하여 스팸글을 등록하는 업자들을 조사하고 처벌하는 기관이다. 주요 내용은 다음과 같다.

“홈페이지 운영자가 스팸글에 대한 거부를 명시하고 1회 이상 서면 또는 이메일로 거부의를 표명하였음에도 스팸글을 올리면 법률 위반으로 처벌한다”

이를 이용하여 홈페이지 약관, 게시판에 위의 내용을 명시하여 놓고 글을 올리는 업자들에게 거부의를 밝힌 후 계속 올리는 사용자가 있다면 증거물을 수집하여 불법스팸대응센터에 신고한다.

이 방법은 당장 효과를 보지 못하고 시간이 오래 걸리지만, 계속적으로 신고하여 스팸게시물을 등록하는 업체가 점점 줄어들면 어느 정도 스팸글에서 해방될 수 있다.

이 방법을 사용하면 인력이 많이 소요된다. 스팸글을 등록하는 업자에게 이메일 등으로 거부의를 표명하고, 스팸글에 대한 증거물을 정리하고, 센터에 신고하는 일련의 과정이 모두 인력이 소요되는 부분이다.

또한, 국내가 아닌 외국광고프로그램에는 국내법 영향을 받지 않으니 효과가 없다. 따라서, 이 방법을 사용하려면 인력과 시간이 충분한 상태에서 진행해야 한다.

4. 스팸로봇을 피해가는 방법

검색로봇은 홈페이지를 방문하여 내용을 수집하고, 자신의 DB에 기록하여 인터넷 사용자들이 필요한 자료를 검색할 시 수집한 자료 중 일치하는 자료를 보여준다. 스팸로봇도 비슷한 일련의 과정을 거쳐 홈페이지를 접속하여 게시판 주소를 수집한다.

스팸로봇이 어떠한 방식으로 홈페이지 게시판을 찾아내는지, 그를 피해가려면 어떻게 해야 하는지 살펴보겠다.

스팸로봇이 당신의 홈페이지를 찾아내는 방법은 크게 3가지다.

첫째, 검색엔진에서 하나의 키워드로 검색 후 결과를 수집한다.

둘째, 국제도메인센터에 등록된 홈페이지 주소에 무차별 접속하여 수집한다.

셋째, 하나의 홈페이지에 접속 후 모든 링크를 따라다니며 무차별 수집한다.

위의 세가지 방법을 차단하는 방법은 다음과 같다.

첫째, 스팸머들이 좋아하는 키워드로 검색엔진에 노출되는 것을 피해야 한다.

스팸머들은 인기 키워드로 인해 검색되는 인기 있는 홈페이지에 광고 글을 올리고, 키워드로 인한 연관성으로 타겟 광고를 하기 위해 검색 키워드 선별을 한다. 따라서 이를 피하려면 키워드 검색 결과를 주시해야 한다.

홈페이지와 상관 없는 키워드에 노출이 되는 것을 피해야 하는 것이다. 예를 들어 의류 쇼핑몰을 하고 있는데 철판 이라는 키워드에 노출이 된다면 전혀 소용이 없을 뿐 더러 철판으로 검색하여 DB를 수집하는 스팸 로봇 프로그램의 타겟이 되고 만다.

키워드를 숨기는 방법은, 홈페이지 내의 콘텐츠를 올릴 때 주의해야 한다. 검색엔진의 로봇은 홈페이지에 접속하여 홈페이지의 텍스트 부분에서 주요키워드를 수집하여 간다. 따라서 게시판이나 홈페이지 내용에 글을 올릴 때 홈페이지 성격과 다른 키워드가 노출되지 않도록 주의해야 한다.

수시로 검색엔진(네이버, 다음 등) 에서 검색을 하며 자신의 홈페이지가 다른 키워드에서 노출이 되고 있는지 확인하여, 노출되고 있다면 해당 내용을 수정하여 노출이 되지 않도록 하면 스팸 로봇 프로그램의 추적을 어느 정도 막을 수 있다.

홈페이지를 알리기 위해서는 많은 사람들에게 노출이 되고 알려지는 것이 필수이다. 따라서 대형 포털, 커뮤니티, 쇼핑몰 보다는 알려진 사람들에게만 운영되는 홈페이지(교회, 공공기관 등)에 적용하는 것이 더욱 효율적이다.

둘째, 국제도메인센터에 등록된 홈페이지 주소에 무차별 접속하여 수집한다.

호스팅 업체에서 도메인을 구입하면 국제도메인센터에 등록이 된다. 스팸 로봇 프로그램은 이를 이용하여 국제도메인센터에 등록된 모든 홈페이지에 무차별 접속하여 스팸광고를 할 수 있는지 여부를 체크하여 데이터베이스에 저장하고 스팸등록에 사용한다.

이를 피하려면 어떻게 해야 할까? 가장 좋은 방법은 도메인을 구입하지 않는 것이다. 하지만 홈페이지로 사업을 하는 대부분의 사업장은 도메인 주소가 없으면 안되기 때문에 실제 이 방법을 피할 수는 없다. 비영리단체, 사내 그룹웨어 등으로 사용되는 곳에서 서브도메인을 활용하여 도메인 주소를 얻은 후 그리로 접속하는 방법만이 없는 것이다.

서브도메인이란 주 도메인에 의미 있는 단어를 추가시켜서 사용되는 것을 말한다. 예를 들어 hosting.com 이라는 주소에서 test라는 이름으로 웹호스팅을 신청했다고 하자. 그러면 test.hosting.com 이라는 주소를 받을 수 있을 것이다. hosting.com이 주 도메인이고, test.hosting.com이 서브도메인이다.

도메인을 등록하면서 스팸로봇을 피해가려면 홈페이지 내부를 스팸에 당하지 않는 구조로 변경하는 수 밖에 없다. 그 내용은 방대하여 이 지면에 다 실을 수 없고, 주요한 몇 가지 내용을 요약해 보면 다음과 같다.

- Frame 구조를 최대한 활용한다.
- 단순링크 보다는 Java Script를 활용한다.
- 의미 없이 숨겨진 링크, Form을 많이 배치한다.

셋째, 하나의 홈페이지에 접속 후 모든 링크를 따라다니며 무차별 수집한다.

홈페이지에는 내부링크와 외부링크가 있다. 내부링크는 홈페이지 내부의 각 메뉴를 연결시켜주는 것이고, 외부링크는 배너, 신문기사 등과 같이 클릭 시 다른 홈페이지로 연결되는 링크이다. 이 링크를 활용하여 스팸로봇 프로그램은 당신의 홈페이지를 수집한다.

수집된 홈페이지를 게시판 스팸글 등록에 사용하는 과정은 동일하다. 이를 피하려면 내부링크의 구조를 변경하여야 한다. 링크를 정의하는 태그는 <a> 이다. 이 코드를 변형하여 Javascript를 사용하는 코드로 변경하면 링크를 따라 검색하는 스팸 로봇 프로그램을 어느 정도 피할 수 있다.

또한 Frame을 사용하여 게시판을 출력할 경우 링크 태그만을 따라다니는 스팸 프로그램을 피할 수 있는 확률이 높아진다.

완벽하게 피할 수는 없지만, 적용하지 않았을 때 보다는 더 큰 효과를 볼 수 있다.

5. 스팸게시물을 효율적으로 관리하는 노하우

모든 스팸글을 100% 차단하는 것은 사실상 불가능하다. 위에서 본 것과 같이 스팸글을 남기려는 자와 차단하려는 자의 치열한 공방전이 일어나고 있고, 프로그램의 지능과 패턴이 갈수록 정교해지고 있다.

스팸차단 정책을 최대한 적용해도 어느 정도 스팸글이 올라올 수 밖에 없는데, 이를 전략적으로 관리하지 않고, 보이는 대로 삭제하면 인력 및 시간낭비가 클 뿐만 아니라, 홈페이지에 방문하는 고객, 이용자들에게도 악영향을 끼쳐 결국 신뢰도 없는 죽은 홈페이지가 될 수 있다.

스팸게시물을 효율적으로 관리하는 노하우는 크게 세가지가 있다.

첫째, 게시판에 새로운 글 등록시 무조건 확인하여 스팸여부를 확인한다.

둘째, 게시판에 새로운 글을 등록하면 관리자 확인 후 게재되도록 시스템을 구축한다.

셋째, 게시판에 스팸 신고 기능을 넣어 일정 횟수 이상 클릭 시 삭제되도록 한다.

첫째, 게시판에 새로운 글 등록 시 무조건 확인하여 스팸여부를 확인한다.

게시판에 등록되는 모든 글을 관리자의 이메일, 핸드폰 또는 알람창 등으로 실시간 알려 즉시 확인하고 실시간으로 바로 삭제하는 방법이다. 언제 새로운 스팸글이 등록될 지 몰라 매 시간마다 홈페이지에 접속하여 새로고침을 하며 확인하는 것 보다 훨씬 효율적으로 관리할 수 있다.

이메일, 핸드폰 등으로 알림이 오게 되므로 새로운 글이 등록될 때 마다 확인할 수 있다. 수신할 때 게시물의 제목, 내용들을 같이 받도록 설정하면 홈페이지에 접속하지 않고도 등록된 게시물의 내용을 확인할 수 있다.

이러한 시스템 변경은 추가적인 비용이 들어가게 되는데, 특히 핸드폰 알람 기능을 사용할 때에는 건당 일정의 수수료가 들어가게 되므로 일일 등록 게시물 건수가 많은 경우 생각지 못한 비용이 소요될 수 있고, 수많은 문자로 인해 업무에 방해가 될 수 있으므로 주의해야 한다.

새로운 글 등록 알람 시스템을 구축하기 힘든 상황이라면 다음과 같은 프로그램을 사용하는 것도 좋은 방법이다. 인터넷에서 검색을 하면 "홈페이지 변동내역 확인 프로그램"을 다운받을 수 있다. 홈페이지 변동내역 확인 프로그램이란 홈페이지 주소를 입력해두면 일정간격으로 접속하여 홈페이지의 내용이 새로운 정보로 바뀌었다면 바뀐 내용을 표시해주는 프로그램이다.

위 프로그램을 이용하여 홈페이지 게시판 주소를 입력해두면 게시판에 새로운 글이 등록될 때 마다 프로그램에서 감지해 알려주므로, 새로운 글 등록 여부를 간단하게 알 수 있다.

둘째, 게시판에 새로운 글을 등록하면 관리자 확인 후 게재되도록 시스템을 구축한다.

이 방법은 스팸 게시물을 100% 차단하면서 원하는 글만 게재할 수 있는 시스템이다. 홈페이지 게시판에 새로운 글이 등록되면 곧바로 열람할 수 있는 것이 아니라 관리자의 승인을 거쳐야만 이 등록되도록 하는 시스템이다.

폐쇄형 커뮤니티이기 때문에 고객의 참여율에 어느 정도 영향은 미치지만, 겉으로 보는 것과 글을 남기는 일련의 과정이 일반 게시판과 동일하므로 비회원제로 게시판을 운영하는 것과 거의 동일한 수준의 초기참여율을 이끌어 낼 수 있는 장점이 있다.

하지만 바로 즉시 열람이 되지 않기 때문에 회원 상호간의 댓글, 답글을 통한 커뮤니티공간인 경우에는 참여율을 떨어뜨려 저조하게 만들 염려가 있으니 주의해서 사용해야 한다.

이 방법을 도입하여 스팸게시물을 관리하면 글이 많이 등록되는 홈페이지는 전담 직원이 있어 수시로 글을 확인하는 체계를 구축해두면 탄력 있는 관리가 가능해진다. 첫째 관리방법과 겸하여 사용하면 더욱 큰 효과를 볼 수 있다.

셋째, 게시판에 스팸 신고 기능을 넣어 일정 횟수 이상 클릭 시 삭제되도록 한다.

일방적인 상품 판매, 회사소개 홈페이지가 아닌 회원들이 활동하는 교회, 카페와 비슷한 성격을 지닌 홈페이지에서 사용하면 효과가 좋은 관리 방법이다. 게시판에 스팸신고 버튼을 만들어 놓고 일정 횟수 이상 클릭되면 해당 게시물을 삭제하여 다른 이들이 볼 수 없도록 한다.

회원제 커뮤니티의 경우 다른 회원 글을 임의로 삭제시키는 것으로 악이용 될 수도 있는 방법이지만, 이런 부분을 제외한다면 관리자의 노고를 들이지 않고 회원 스스로 스팸 차단을 하는 것이니 최선의 방법이라 할 수 있다.

이상 스팸글이 등록되는 원인과 차단하는 방법, 피해가는 방법, 등록되는 스팸을 효율적으로 관리하는 방법에 대해 알아보았습니다. 이 내용이 홈페이지 게시판에 스팸을 당하고 있는 분들에게 조금이나마 도움이 되었으면 하는 바람으로 한 단락 한 단락 모두 정성스럽게 내용을 작성하였습니다.

스팸글의 파급력은 마치 바퀴벌레와도 같아서, 지금 홈페이지 게시판에 한두개의 스팸글이 간헐적으로 등록되고 있다면, 곧 수많은 스팸글이 등록될 것임을 예고하므로 발 빠른 대응을 하지 않으면 스팸 폭탄을 맞게 될 것입니다. 위의 노하우를 참고하여 스팸글 차단에 도움 되기를 바랍니다.

내용을 읽으면서 해결되지 않는 궁금한 점이나, 구체적인 방법에 대한 궁금증 또는 새로운 아이디어가 있으시다면, 저의 이 메일은 언제든지 열려있습니다.

게시판 스팸차단 연구소 차단설계사 김기용 올림

차단설계사 김기용
kykim@cleanboard.net

게시판 스팸차단 연구소
CBI Networks / bShield 사업본부
02) 2631-3757

<http://cleanboard.net>