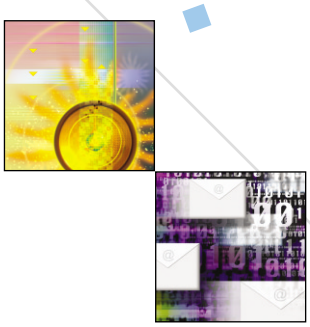
2006 스팸메일 차단 솔루션 활용 가@이드

– 스팸메일, 줄이는 것이 경쟁력 –



2005. 12

정보통신부

KISA 한국정보보호진흥원
Korea Information Security Agency

2006 스팸메일 차단 솔루션 활용 가이드

- 스팸메일, 줄이는 것이 경쟁력 -

2005. 12.

정 보 통 신 부

한국정보보호진흥원
Korea Information Security Agency

Contents

목차

1 스팸메일이란?

◉ 이메일이나 휴대폰 등 정보통신서비스를 이용하는 이용자의 단말기로 본인이 원치 않음에도 불구하고 일방적으로 전송되는 영리목적의 광고성 정보를 말합니다.

◉ 스팸메일은 대량으로 반복 전송되기 때문에 이를 받는 이용자의 짜증을 유발하고 필요한 정보 수신을 방해하며 메일서버의 과부하를 초래하는 등 많은 문제점을 야기하는 대표적인 정보화역기능 중 하나입니다.

2 스팸메일 차단 솔루션이란?

◉ 스팸문제가 심각한 사회문제로 대두됨에 따라 스팸메일을 방지 또는 차단하기 위한 기술적 대응이 매우 중요하게 부각되고 있습니다.

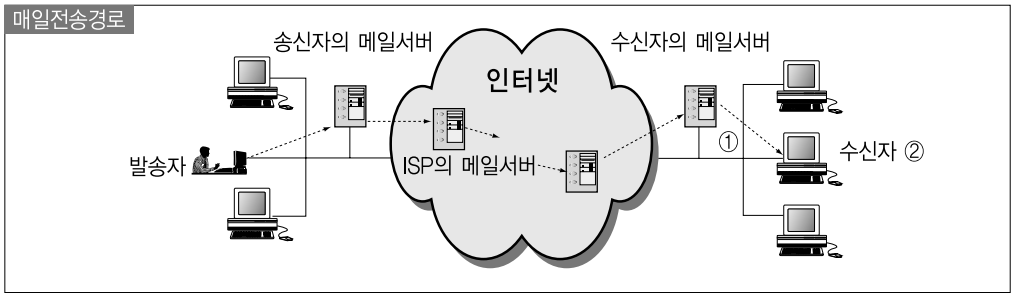
◉ 메일서버를 운영하는 관리자나 개인 이용자가 가장 대중적으로 활용할 수 있는 기술적 대응방안이 '필터링(filtering)'과 '인증(authentication)' 기능입니다.

※ 동 기술에 대한 자세한 설명은 [부록1] 참조

◉ 스팸메일 필터링 또는 정상메일 인증 기능 등을 제공함으로써 정상메일과 스팸메일을 구별하도록 도와주는 프로그램이 바로 **"스팸메일 차단 솔루션"**입니다.

◉ 메일전송경로 중 스팸대응기술을 어느 단계에서 사용하는가에 따라 솔루션은 '서버용'과 '클라이언트용'으로 나뉩니다.

- 다음, 네이버 등 웹메일서비스 이용자의 경우, 개인 선호에 따라 해당 웹메일서비스 업체가 제공하는 다양한 스팸 필터링(서버 단계/이용자 단계) 및 인증 서비스를 받을 수 있으며,
- 회사 등에서 메일전용 프로그램을 이용할 경우에는, 회사 차원에서 메일서버에 '서버용' 스팸메일 차단 솔루션을 설치하거나 이용자가 직접 '클라이언트용' 솔루션을 구입하여 활용할 수 있습니다.



• **"서버용"** : ①단계에 설치 • **"클라이언트용"** : ②단계에 설치

※ 메일전용 프로그램 이용자 중 별도의 솔루션 구입이 어려운 경우에는, 프로그램에 내장된 기본적인 스팸차단 기능을 본인이 직접 설정함으로써 일정 정도 스팸 차단효과를 거둘 수 있음. 다만, 날로 지능화하는 스팸에 적절히 대처하기에는 한계가 있음

3 스팸메일 차단 솔루션 왜 필요할까요?

◉ 스팸으로 인해 발생하는 가장 큰 문제는 수신자를 성가시고 짜증나게 한다는 정신적인 피해도 있지만 그로 인해 실제 엄청난 경제적 손실이 초래된다는 점입니다.

– 미국의 전문 시장조사 기관인 Ferris Research사에 의하면, 생산성 손실 비용 등 2005년 스팸으로 인한 전 세계의 피해액을 약 5억 달러 이상으로 추정하였는데,

– 스팸으로 인한 가장 큰 피해는 스팸을 필터링하는데 근무시간을 낭비하고, 스팸으로 발생한 각종 문제를 해결하기 위해 추가적인 자원을 투여하는 기업이나 기관에서 주로 발생하고 있습니다.

• 웹메일서비스업체는 다양한 인증 및 필터링 기능을 활용함으로써 이용자에게 최종 수신되는 스팸메일의 양을 감소시키고 있는 반면,

• 자체 메일계정을 발급 · 관리하는 기업이나 기관에서는 상대적으로 스팸메일의 피해에 대한 문제 인식이 부족하여 스팸메일 차단 솔루션 활용률이 저조하고, 결과적으로 해당 메일계정 이용자에게 수신되는 스팸수신량이 높기 때문입니다.

〈웹메일 및 메일전용프로그램의 1계정당 스팸메일 수신량 비교〉

구 분	1일 평균 스팸수신량
웹메일	1.6통/일
메일전용프로그램	13.1통/일

출처 : 한국정보보호진흥원, 2005.11

◉ 이에 관공서, 학교, 기업 등 메일서버를 구축하거나 임대하여 자체 메일계정을 발급·관리하고 있는 기업 및 기관 대상으로 서버용 스팸메일 차단 솔루션 설치를 권장함으로써 보다 효율적으로 최종 이용자에게 수신되는 스팸의 양을 감소시키는 것이 필요합니다.

◉ 또한, 서버용 스팸메일 차단 솔루션이 설치되지 않은 기업 및 기관 메일전용 프로그램 이용자에게 가격이 저렴한 클라이언트용 솔루션을 활용토록 권장하는 것도 필요합니다.

4 스팸메일 차단 솔루션 효과 얼마나 될까요?

◉ 현재 국내에서 판매되고 있는 대부분의 서버용 스팸메일 차단 솔루션의 스팸감축 효과는 80~90% 이상이라고 합니다.

▶사례 ※ 1통당 20원의 경제적 손실이 발생한다고 가정한 경우

- **A 도청 (이용자 수 : 30만 명)**
  - 1개월 평균 3,700,000 여통 스팸메일 수신 차단
  - 연간 9억 2천만원의 비용 절감 효과
- **B 기업 (이용자 수 : 2만 명)**
  - 1개월 평균 600,000 여통 스팸메일 수신 차단
  - 연간 1억 5천만원 비용 절감 효과

◉ 스팸메일 차단 솔루션은 직원의 생산성 손실을 막아주고, 대량 또는 악성 스팸으로 인한 서버 다운 등의 시스템 장애를 미리 예방함으로써 기업이나 기관의 경제적 손실을 최소화합니다.

▶ 스팸메일 차단 솔루션의 효과

가. 불필요한 메일로 인한 메일서버 증설 비용 등 직접 투자비용 절감
나. 바이러스메일 원천 차단으로 인한 시스템 보호 및 생산성 제고
다. 메일서버 도용 분쟁 제거로 인한 기업이미지 제고
라. 메일서버 공격에 대한 효과적인 방어라인 구축

5 필요에 따라 골라쓰는 스팸메일 차단 솔루션

◉ 기업이나 기관 메일 이용자 규모에 따라 솔루션을 Package로 구입하는 방법과 월 단위로 임대서비스를 받는 방법(ASP)이 있습니다.

- Package 구입 : 이용자 수가 비교적 많은 큰 규모의 기업, 기관, 학교 등에 적합
- ASP 서비스 이용 : 이용자 수가 적은 중소기업 등에 적합

※ ASP(Application Service Provider) 서비스 : 기업 운영에 필요한 각종 소프트웨어를 인터넷을 통하여 임대하는 새로운 방식의 비즈니스

▶ 이 장에서 소개되는 스팸메일 차단 솔루션 제품에 대한 내용은 해당 업체로부터 자료를 제공받아 작성된 것으로 한국정보보호진흥원의 입장이나 의견과는 무관한 것이라는 점을 알려드립니다.

▶ 제품에 대한 보다 자세한 문의는 자료에 소개되어 있는 해당업체 담당자에게 직접 하시기 바랍니다.

Local Business Solution

국내 상용 솔루션

특징 | 스팸차단 기능이 우수하고 서비스 지원이 용이함

※ 이 장의 용어해설은 PP.51 ~ 53 참조

클린스팸

Clean Spam

- *(주)컴트루테크놀로지*
- *홈페이지 : http://www.cleanspam.co.kr*
- *영업부 조학인 (02-396-7005, hicho@comtrue.com)*

① **제품명 :** 클린스팸 엔터프라이즈 2.0 (패키지 / ASP)

② **사용환경 :** Linux / Solaris / HP-UX

③ **타겟고객층 : 서버용**

※ 판매처 : 전경련 외 400여개 기관, 학교, 업체

④ **표창이나 마크 등**

- 2002 신소프트웨어 대상(스팸차단분야 최초)
- 행망용 조달제품 등록 (2002, 2003, 2004, 2005)

⑤ **기능**

아래 표는 기능의 우열을 나타내는 것이 아니며 단순히 해당 제품의 기술적 특징을 나타내는 것임

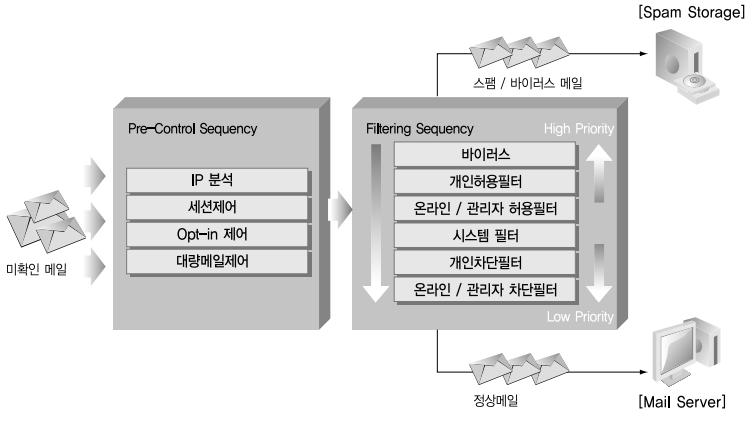
구 분	기 술		구현여부
발송 단계	오픈 렐레이 및 프록시 차단		O
	발송 총량 제한		O
	발송 비용 부담	Challenge & response 또는 bouncing back	O
		Online Stamp	-
		Hash Cash	-
		Graylist	△
	유동 IP이용자의 25번 포트 차단		△
수신 단계	필터링 기술	단어 / 전송자정보 / 이미지 / 패턴학습	O
		신뢰도 평가시스템 (reputation system)	O
	발송자 인증 기술	Reverse DNS / HELLO Check	O
		SPF	O
		Sender ID	△

구 분	기 술		구현여부
수신 단계	발송자 인증 기술	DKIM	△
		White IP 등록	O
정부권장기술	SPF (발송자 인증)		O
	RBL (필터링)		O

[기타 기능 및 특징]

- 고객사 환경별 설치방식 (DNS, 브릿지) 제공, 자동화 설치패키지 제공
- 효과적인 온라인차단 필터와 바이러스 필터를 주기적으로 제공
- SMTP 공격으로부터 메일서버 보호기능 (대량메일공격방어)
- Opt-in방식의 차단기능 제공(옵션)
- 메일 traffic 감시 (내부, 외부로 대량으로 발송되는 Traffic관리 및 reporting)
- 고객사의 조직도 구조에 기반한 부서별 필터링 기능 적용/ alias 메일계정 관리
- 외부로 발송되는 메일에 대해서 정보유출이 의심되는 메일 사전 차단 및 관리 기능 제공 (메일암호화 및 백업기능 제공)
- 스팸메일로 처리된 메일에 대하여 IP, 메일서버, 검사한 메일 수, 스팸 처리된 메일 수 등 1일 reporting 기능을 제공
- 관리자용 페이지뿐만 아니라 사용자가 스팸을 관리할 수 있는 개인용 웹페이지 제공 (개인설정필터는 개인메일에 대해서만 적용)
- 세계적인 안티 바이러스 업체 소포스(Sophos)의 바이러스 백신 기능 제공

⑥ 구현원리



⑦ **구매비용 :**

- Package : 가격은 메일 사용자 수에 따라 달라짐
  (100, 200, 500,1000, 3000, 5000, 10000, unlimited)
- ASP : 메일 사용자 수별 월 2,500원(스팸차단 + 바이러스 백신)

크레디쉴드 *Credishield*

- *(주)모비젠*
- *홈페이지 : http ://www.mobigen.com*
- *일반기업 : 이세연 부장 (sylee@mobigen.com)*
  김형준 대리 (skid123@mobigen.com)
- *관 공 서 : 이동재 차장 (djlee20@mobigen.com)*
- *교육기관 : 서 영 대리 (seo0@mobigen.com*

① **제품명 :** 크레디쉴드 엔터프라이즈 3.0 (Package/ ASP)

② **사용환경**

- OS : Linux, Unix
- H/W 사양 : 메일의 유통량에 따라 상이

③ **타겟고객층 : 서버용**

※ 판매처 : KT-IDC 외 200여개 업체, 기관, 학교

④ **표창이나 마크 등**

- 2001년 정보통신부 신기술 선정(국내최초)
- 2004년 조달청 우수제품 선정(국내최초)
- 2005년 행정업무용 소프트웨어 선정
- 2005년 ISO 9001 품질경영시스템 인증기업

⑤ **기능**

다음 표는 기능의 우열을 나타내는 것이 아니며 단순히 해당 제품의 기술적 특징을 나타내는 것임

구 분	기 술		구현여부
발송 단계	오픈 렐레이 및 프록시 차단		O
	발송 총량 제한		O
	발송 비용 부담	Challenge & response 또는 bouncing back	-
		Online Stamp	-
		Hash Cash	-
		Graylist	-
	유동 IP이용자의 25번 포트 차단		O
수신 단계	필터링 기술	단어 / 전송자정보 / 이미지 / 패턴학습	O
		신뢰도 평가시스템 (reputation system)	O
	발송자 인증 기술	Reverse DNS / HELLO Check	O
		SPF	O
		Sender ID	O
		DKIM	-
		White IP 등록	O
정부권장기술	SPF (발송자 인증)		O
	RBL (필터링)		O

⑥ 구현원리

▶ 스팸정보센터 운영

- 스팸관련 특허기술과 스팸센터 운용을 통한 지속적인 신종스팸차단 룰 서비스 제공
- 실시간 스팸 엔진 업데이트 서비스 지원
- 중앙집중식 스팸 정보 공유(특허출원)

▶ 동적차단

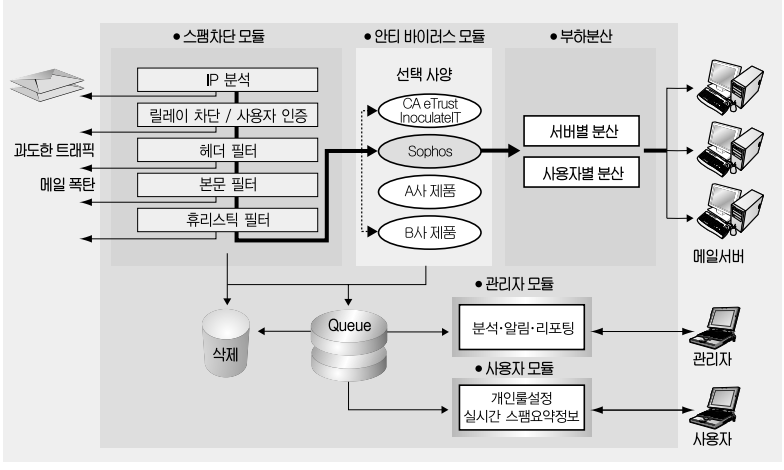
- 유인메일 주소 활용(특허)
- 동일/유사 본문 검출(특허)
- 동적 IP제어를 통한 스팸메일 차단

▶ 필터링 기법

- 메시지 제목 및 본문키워드 검색에 의한 차단
- 동보전송수 제한[RCPT TO(수신자)의 수 제한 기능]
- 메일 패턴 및 규격에 의한 차단
  - ➡ 날짜, 제목, 메일계정의 유효성, 위 · 변조 등에 의한 차단

➡ 규약위반 여부(표준권고안 준수 여부)검사, 메일용량(최대,최소)등에 의한 차단

- 허용 IP, 차단 IP 관리 및 설정을 통한 필터링
- Domain Reverse Lookup 에 의한 차단
- 각 시스템, 그룹, 개인별로 특성을 감안한 룰 설정 제공으로 고객맞춤 형 차단 환경 제공
- 다국어 및 특수문자 필터링
- 바이러스 차단 기능
  - ➡ 패턴 및 엔진 자동업데이트 지원으로 바이러스 감염을 사전에 방지
  - ➡ 다양한 압축파일(zip, tar, ljh 등) 지원 및 스크립트형태의 바이러스 검색, 치료, 제거
  - ➡ 악성 스크립트 코드 검색 및 트로이 목마 형태의 바이러스 유포 원천 차단



[스팸메일차단 시스템 구성도]

⑦ 구매비용

▶ 사용자 수 구분에 의한 가격 산정

한월프로

HanWall-Pro

- *(주)한인터네트웍스*
- *홈페이지 : www.hanwall.com*
- *기술영업본부 (02-860-8003, sales@haninternet.co.kr)*

① **제품명 :** HanWall-Pro

② **사용환경 :** 사용자 수에 따라 제품 구분(50 user, 200 user, 200 user 이상),
임베디드 리눅스 어플라이언스(Embedded Linux Appliance) 장비

③ **타겟고객층 : 서버용**

※ 판매처 : 동양생명 등 90여개 업체, 병원, 기관

④ **기능**

아래 표는 기능의 우열을 나타내는 것이 아니며 단순히 해당 제품의 기술적 특징을 나타내는 것임

구 분	기 술		구현여부
발송 단계	오픈 렐레이 및 프록시 차단		O
	발송 총량 제한		O
	발송 비용 부담	Challenge & response 또는 bouncing back	O
		Online Stamp	-
		Hash Cash	-
		Graylist	-
	유동 IP이용자의 25번 포트 차단		-
수신 단계	필터링 기술	단어 / 전송자정보 / 이미지 / 패턴학습	O
		신뢰도 평가시스템 (reputation system)	O
	발송자 인증 기술	Reverse DNS / HELLO Check	O
		SPF	O
		Sender ID	-
		DKIM	-
		White IP 등록	-
정부권장기술	SPF (발송자 인증)		O
	RBL (필터링)		O

[기타 기능 및 특징]

- ALL-In-One Spam Filter (FW/VPN/IPS)
- Application GateWay 기반의 SpamFilter
- Virus Filter, Pattern Matching, Bayesian Filter
- E-Mail 주소별 규칙적용기능
- 다국어 필터링
- Virus DB, Filter DB 자동업데이트 및 Center 운영
- 사용자별 메일 복구기능
- 필터링 엔진 추가 및 Adaptable한 엔진 적용가능
  - ➡IP Filter, Key Word Filter, RBL, Bayesian, White IP 엔진 등

⑤ 구현원리

▶ FireWall + SMTP Application GateWay

⑥ 구매비용

▶ 별도상담요망

메일와쳐 Mail Watcher

- *(주)테라스테크놀로지*
- *홈페이지 : http://www.terracetech.com*
- *영업팀 김재석 부장(02-2082-0339),*
  부완혁 과장(02-2082-0340)

① **제품명 :** Terrace MailWatcher (S/W 제품 및 장비일체형 2가지)

② **사용환경 :** Unix, Linux

③ **타겟고객층 :** 서버용

④ **표창이나 마크 등**

- KT 마크 인증
- GS 인증

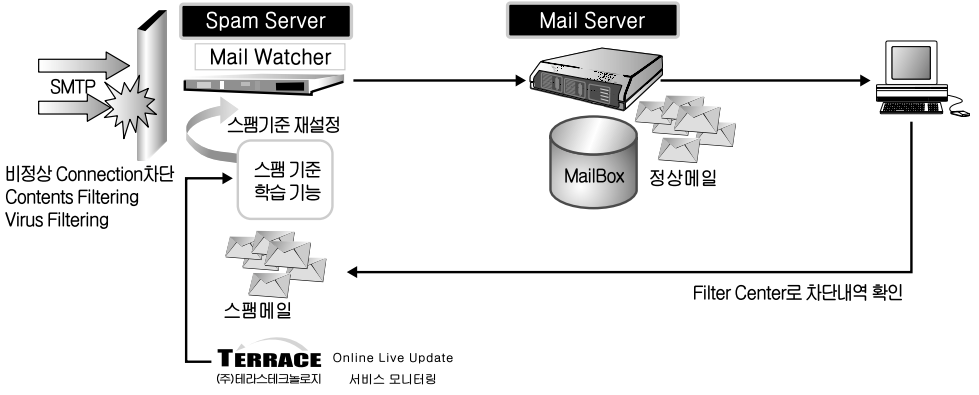
⑤ **기능**

아래 표는 기능의 우열을 나타내는 것이 아니며 단순히 해당 제품의 기술적 특징을 나타내는 것임

구 분	기 술		구현여부
발송 단계	오픈 렐레이 및 프록시 차단		O
	발송 총량 제한		O
	발송 비용 부담	Challenge & response 또는 bouncing back	-
		Online Stamp	-
		Hash Cash	-
		Graylist	-
	유동 IP이용자의 25번 포트 차단		O
수신 단계	필터링 기술	단어 / 전송자정보 / 이미지 / 패턴학습	O
		신뢰도 평가시스템 (reputation system)	-
	발송자 인증 기술	Reverse DNS / HELLO Check	O
		SPF	O
		Sender ID	-

구 분	기 술		구현여부
수신 단계	발송자 인증 기술	DKIM	–
		White IP 등록	O
정부권장기술	SPF (발송자 인증)		O
	RBL (필터링)		O

⑥ 구현원리



[4단계 다중차단엔진 동작 원리]

⑦ 구매비용

▶ 사용자 수에 따른 적정 가격

마음메일

MAUMMAIL

- *(주)누리비전*
- *홈페이지 : http://www.maummail.com*
- *02-959-6438, nurivision@nurivision.com*

① 제품명(2가지)

- 마음메일 스팸차단 게이트웨이(모델명 : MMP-GW)
- 마음메일 스팸차단 ASP(모델명 : MMAS-ASP)

② 사용환경

제 품	MMP-GW		MMAS-ASP
구 분	사용자수 500명 이하	사용자수 500명 이상	1~250명까지 사용자수별 구분
하드웨어	· CPU : P4 3.0 · HDD : 80 GB · RAM : 512 MB	· CPU : P4 2.4Dual · HDD : 80 GB · RAM : 1 G	ASP 서비스 전용 게이트웨어
OS	리눅스 슬랙웨어		리눅스 슬랙웨어

③ 타겟고객층 : 서버용, ASP용

※ 판매처 : LG텔레콤 외 100개 업체, 기관, 학교

④ 표창이나 마크 등

- 2005. 10. '대한민국창업대전'에서 '벤처기업협회장상' 수상(중소기업청 주관)
- 2005. 9. '홍릉지역혁신특성화사업(RIS)'에서 '선도육성기업'으로 선정(산업자원부 주관)
- 2004. 6 '04년도 'IT마크' 획득 (정보통신부 주관)
- 2005. 7. '05년도 상반기 행정업무용 소프트웨어 선정(행정자치부 주관)
- 2005. 5. 한국특허 획득
- 2005. 1. '05년도 공공기관 우선 구매 대상 제품 선정(산업자원부)
- 2004. 7 '04년도 상반기 행정업무용 소프트웨어 선정(행정자치부 주관)
- 2004. 6 '04년도 '정보통신우수신기술'로 지정 (정보통신부 주관)

- 2004. 1 대만특허 획득
- 2003. 12 '2003 올해의 인터넷기업대상' 신생기업부분(우수상) 선정
  (한국인터넷기업협회 주관, 정보통신부 후원)

⑤ 기능

아래 표는 기능의 우열을 나타내는 것이 아니며 단순히 해당 제품의 기술적 특징을 나타내는 것임

구 분	기 술		구현여부
발송 단계	오픈 렐레이 및 프록시 차단		O
	발송 총량 제한		-
	발송 비용 부담	Challenge & response 또는 bouncing back	O
		Online Stamp	-
		Hash Cash	-
		Graylist	-
	유동 IP이용자의 25번 포트 차단		-
수신 단계	필터링 기술	단어 / 전송자정보 / 이미지 / 패턴학습	O
		신뢰도 평가시스템 (reputation system)	-
	발송자 인증 기술	Reverse DNS / HELLO Check	O
		SPF	O
		Sender ID	-
		DKIM	-
		White IP 등록	O
정부권장기술	SPF (발송자 인증)		O
	RBL (필터링)		O
기 타	4단계 다중차단엔진탑재, 허위계정차단, 바이러스엔진탑재, SPR엔진, 바운싱백엔진		O

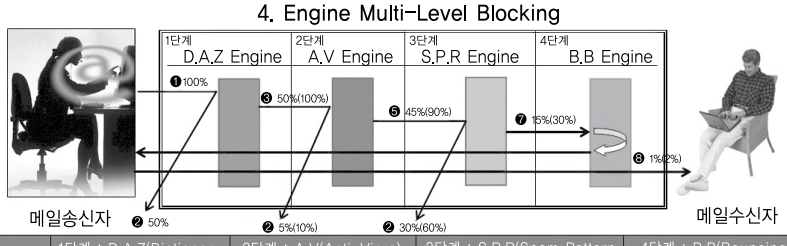
[기타 기능 및 특징]

- 기존 솔루션들이 거의 대부분 필터링(Filtering)방식을 사용하고 있는 반면에 '마음메일 스팸차단 게이트웨이'는 '송신자 자가인증'형의 신 기술인 '옵트플러스'(Opt-Plus) 방식을 이용하고 있음
- 옵트플러스는 메일 송신자가 인증을 통해 스패머가 아님을 입증하는 개념으로서 스팸 차단율이 거의 100%에 가까운 차단 효과를 나타내고 있음

⑥ 구현원리

▶ 4단계의 복합적이고 입체적인 차단 엔진을 통해 스팸 뿐만아니라 바이러스까지 차단 가능

- **1단계** : 허위공격차단엔진(Dictionary Attack Zero Engine) 사용
- **2단계** : 안티바이러스 엔진(Anti-Virus Engine) 사용
- **3단계** : 스팸패턴랭킹 엔진(Spam Pattern Ranking Engine) 사용
- **4단계** : 바운싱백 엔진(Bouncing Back Engine)에서 옵트플러스방식을 통해 스팸 메일 차단



단 계	1단계 : D.A.Z(Dictionary Attack Zero) Engine	2단계 : A.V(Anti-Virus) Engine	3단계 : S.P.R(Spam Pattern Ranking-Filtering) Engine	4단계 : B.B(Bouncing Back) Engine
세부 단계	❶ ❷	❸ ❹	❺ ❻	❼ ❽
단계별 주요 기능	• 허위계정공격(Dictionary Attack) 차단 • 사용자 및 관리자 설정 블랙리스트 차단	• Virus Engine for SMTP • 피싱(Phishing) 등 최신 바이러스 및 악성코드 차단	• 스팸의 패턴유형 분석 • 스팸가능성(Ranking)으로 차단 • 이메일 규칙 준수여부로 차단	• 송신자 자가인증기법 사용 • 사용자별 선택적 사용 가능 • 가장 강력한 스팸차단 엔진
차단 내용	• 허위로 작성된 이메일 계정으로 들어오는 허위계정공격을 서버 교신만으로 차단 • 도메인, 아이피, 이메일주소로 블랙리스트를 설정 차단	• 허위계정차단 엔진을 통과한 메일들(약 50%)중에서 바이러스 메일로 확인되는 메일들을 차단 • 50%의 메일들 중에에 바이러스 메일은 약 5%정도 차지	• 엔진으로 유입되는 메일(45%)중 스팸메일로 확실히 확인되는 메일(약 30%) 차단 • 일정기간 저장 및 삭제 • 관리자 검색 및 메일 구제	• 1, 2, 3단계 엔진을 통과한 약 15%의 메일들의 송신자에게 인증메일 발송 • 약 1%의 메일만이 인증과정을 완료한 정상메일로 수신자에게 전달됨

[4단계 다중차단엔진 동작 원리]

⑦ 구매비용

▶ 마음메일 스팸차단 게이트웨이

- 일괄구매(턴키 구매, VAT별도) 및 년라이센스 구매(VAT별도) : 별도 문의

※ 공공기관은 50% 할인가 적용

▶ 마음메일 스팸차단 ASP

- 가격 : 월 3,000 원 / 계정(VAT별도)
- 사용자수에 따라 소정의 할인율 적용
- 사용자수에 따른 정확한 가격은 별도 문의 바람

스팸블러커 *Spam Blocker*

- *(주)엑티브메일코리아*
- *홈페이지 : http://www.spamblocker.co.kr*
- *02-3443-8120, sales@icoit.com*

① **제품명 :** 스팸블러커(SpamBlocker)

② **사용환경**

- OS: Unix 및 Linux
- Mailserver: Send mail, Qmail, Postfix, Ms-Exchange, Domino Notes 등
- DB: MySQL, PostgreSQL, Oracle, MS-SQL

③ **타겟고객층 : 서버용**

④ **표창이나 마크 등**

- TTA 소프트웨어품질인증서 획득(GS인증)
- 행정업무용 S/W 적합성 통과
- 신 S/W대상 우수 소프트웨어
- 디지털타임즈 HIT상품 선정

⑤ **기능**

아래 표는 기능의 우열을 나타내는 것이 아니며 단순히 해당 제품의 기술적 특징을 나타내는 것임

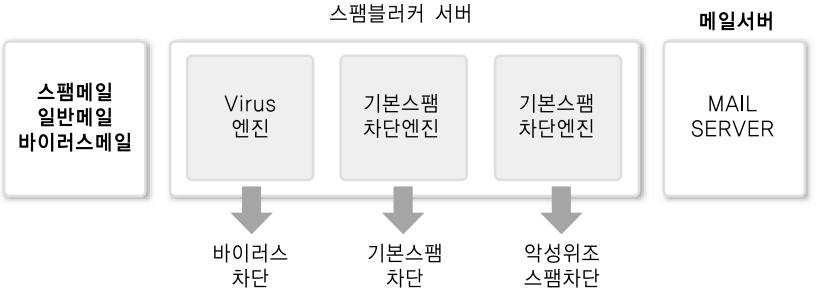
구 분	기 술		구현여부
발송 단계	오픈 렐레이 및 프록시 차단		O
	발송 총량 제한		O
	발송 비용 부담	Challenge & response 또는 bouncing back	-
		Online Stamp	-
		Hash Cash	-
		Graylist	△
	유동 IP이용자의 25번 포트 차단		O

구 분	기 술		구현여부
수신 단계	필터링 기술	단어 / 전송자정보 / 이미지 / 패턴학습	O
		신뢰도 평가시스템 (reputation system)	O
	발송자 인증 기술	Reverse DNS / HELLO Check	O
		SPF	–
		Sender ID	–
		DKIM	–
		White IP 등록	O
정부권장기술	SPF (발송자 인증)		–
	RBL (필터링)		O

[기타 기능 및 특징]

- **자체 메일 큐(Mail Queue) 관리**
  - ➡ 메일 유실율 0% (Queue로그 기능 구현)
  - ➡ 메일 큐는 기존 판매된 메일서버의 가장 취약점
- **웹메일 서버연동 활용성**
  - ➡ No User처리 연동: 기존 메일 서버 인증통합
  - ➡ 운영중인 모든 메일 서버와 통합 가능한 구조설계
- **스팸차단 보안성**
  - ➡ IP Blocking 을 이용한 대용량 메일 공격 차단
  - ➡ 바이러스 방역기능
  - ➡ 기타 보안 정책 : 버퍼 오버플로우, 스트링 포맷공격 원천차단

⑥ 구현원리



Anti-Virus엔진

- SMTP용 차단방식 채용
- Virus Mail 차단
- 웜 바이러스 자동삭제

기본스팸차단엔진

- 자체 개발 MTA탑재
- RFC822/RFC2505적용
- 대용량메일에 탁월한 성능
- GS인증획득

인공지능학습

- SVM알고리즘
- 최신 인공지능기법 수용
- 스팸메일 자동학습

▶ Inbound / Outbound 동시 처리
▶ 개인별 스팸필터
▶ 스팸메일 인공지능 자동학습
▶ 웜바이러스 자동 차단

⑦ 구매비용 : 라이센스별 가격정책

- Small Business License
- Enterprise License
- 다중서버 및 호스팅용 License

스팸브레이커 Spam Breaker

- *(주)쓰리알소프트*
- *홈페이지 : http://www.3rsoft.com*
- *시큐리티팀 윤석주 팀장 02-573-0030 (내선번호 205), neo@3rsoft.com*

① **제품명 :** SpamBreaker 스팸브레이커

② **사용환경**

- **OS** : Linux, Unix
- **DB** : Oracle, MS-SQL, DB2

③ **타겟고객층 : 서버용**

④ **표창이나 마크 등**

- GS 인증 획득
- 디지털타임즈 히트상품
- 대한민국 이머징 우수 기술상

⑤ **기능**

아래 표는 기능의 우열을 나타내는 것이 아니며 단순히 해당 제품의 기술적 특징을 나타내는 것임

구 분	기 술		구현여부
발송 단계	오픈 렐레이 및 프록시 차단		O
	발송 총량 제한		O
	발송 비용 부담	Challenge & response 또는 bouncing back	-
		Online Stamp	-
		Hash Cash	-
		Graylist	-
	유동 IP이용자의 25번 포트 차단		O
수신 단계	필터링 기술	단어 / 전송자정보 / 이미지 / 패턴학습	O
		신뢰도 평가시스템 (reputation system)	-
	발송자 인증 기술	Reverse DNS / HELLO Check	-
		SPF	O
		Sender ID	-

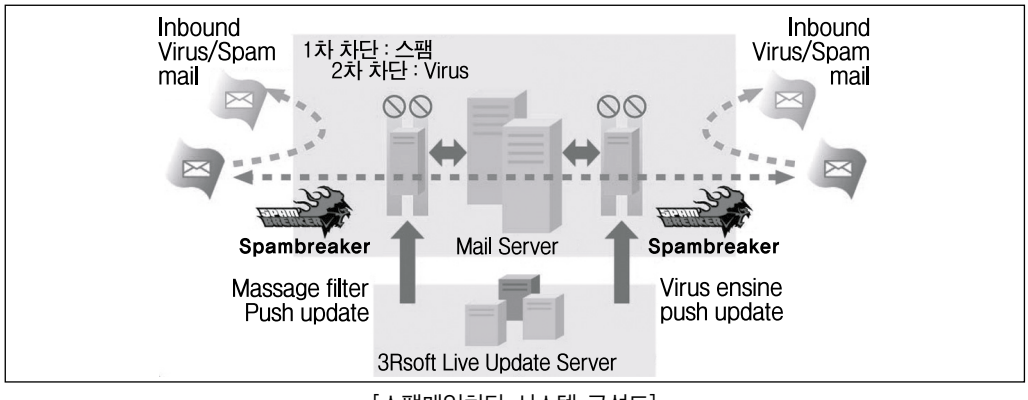
구 분	기 술		구현여부
수신 단계	발송자 인증 기술	DKIM	–
		White IP 등록	O
정부권장기술	SPF (발송자 인증)		O
	RBL (필터링)		O
기 타	PRBL(Phantom RBL)–기존 RBL 확장 개선		O
	팬텀유저필터링 – 도메인필터 적용전 차단		O
	Online Filtering – 실시간 스팸유형차단지원		O
	바이러스메일 필터링 – 1일 24회 업데이트		O

[기타 기능 및 특징]

- 자기학습 기능을 통한 높은 스팸메일 차단율 제공
- Bypass FOD 기능을 통한 365X24 무정지 메일 송 · 수신
- 메일서버 연동을 통한 개인별 스팸설정이 가능
- 국내 유일의 Pure Java 기반으로 설계되어 네트워크 및 인터넷 환경에 매우 적합하며 이기종 하드웨어 및 운영 체제로 인한 호환성 문제가 발생하지 않음

⑥ 구현원리

- 기존의 운영 중인 메일서버 앞단에 위치하여 스팸메일과 바이러스 메일을 차단
- 기존 메일서버 네트웍 설정, DNS설정, Outlook 사용자의 송 · 수신 서버 설정사항 변경 없이 사용 가능



[스팸메일차단 시스템 구성도]

⑦ 구매비

- 별도 협의

스팸아웃 Spam Out

- *(주)바네트*
- *홈페이지 : http://www.spamout.co.kr, http://www.vanet.co.kr*
- *02-2108-1490~3, sales@vanet.co.kr*

① **제품명** : SpamOut(서버형, 네트워크 장비형)

② **사용환경** : Linux, Windows, Unix계열 모든 메일 엔진과 호환

③ **타겟고객층** : 서버용

※ 판매처 : 공정거래위원회 등 60여개 기관, 업체, 학교

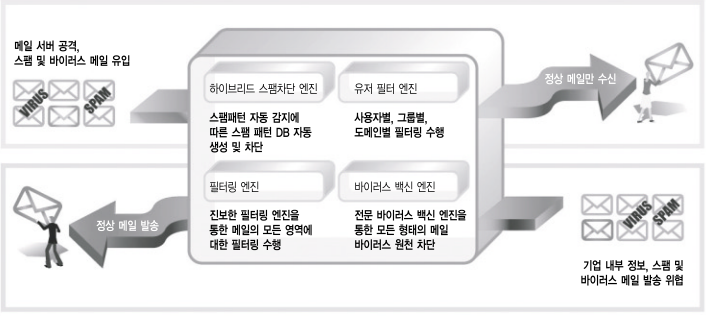
④ **기능**

아래 표는 기능의 우열을 나타내는 것이 아니며 단순히 해당 제품의 기술적 특징을 나타내는 것임

구 분	기 술		구현여부
발송 단계	오픈 렐레이 및 프록시 차단		○
	발송 총량 제한		○
	발송 비용 부담	Challenge & response 또는 bouncing back	-
		Online Stamp	-
		Hash Cash	△
		Graylist	○
	유동 IP이용자의 25번 포트 차단		○
수신 단계	필터링 기술	단어 / 전송자정보 / 이미지 / 패턴학습	○
		신뢰도 평가시스템 (reputation system)	△
	발송자 인증 기술	Reverse DNS / HELLO Check	○
		SPF	○
		Sender ID	-
		DKIM	○
		White IP 등록	○
정부권장기술	SPF (발송자 인증)		○
	RBL (필터링)		○

⑤ 구현원리

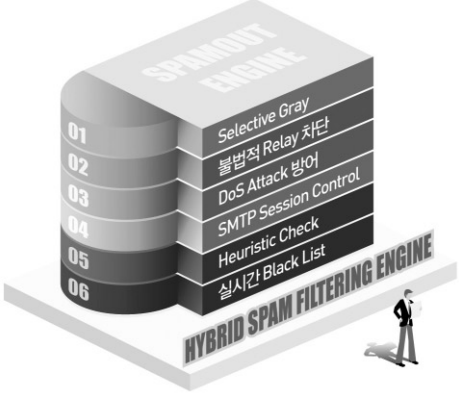
▶ 획기적인 하이브리드 스팸차단 엔진을 통해 기업 고유의 패턴 유형에 빠르게 적응



[하이브리드 엔진 구성 및 개요]

▶ Non-Contents Filtering
- Selective Gray-List antispam
- 불법적 Relay 차단 및 RBL
- DoS Attack 방어
- SMTP Session 제어
- Heuristic Scanning

▶ Contents Filtering
- URL Filtering / URL 추적 기능
- 정규식 Filtering
- Heuristic Scanning



[하이브리드 엔진 기능 구성]

⑥ 구매비용

▶ 별도 문의

스팸스나이퍼 SpamSniper

- *(주)지란지교소프트*
- *홈페이지 : http://www.jiran.com*
- *영업팀장 황성택 (02-2006-6999)*
- *대리 손미주 (02-2006-6998)*

① **제품명 :** 스팸스나이퍼(SpamSniper)

② **사용환경 :** Linux 계열, Unix 계열, 모든 메일 엔진과 호환

③ **타겟고객층 :** 서버용/개인용

※ 판매처 : 행정자치부 외 700여개 기관, 학교, 업체 등

④ **표창이나 마크 등**

- 행정용 소프트웨어 (2003)
- GS인증 (2005)
- 대한민국소프트웨어 대상 "보안부문 우수상" (2005)
- 디지털타임스 2005상반기 히트상품 (2005)

⑤ **기능**

아래 표는 기능의 우열을 나타내는 것이 아니며 단순히 해당 제품의 기술적 특징을 나타내는 것임

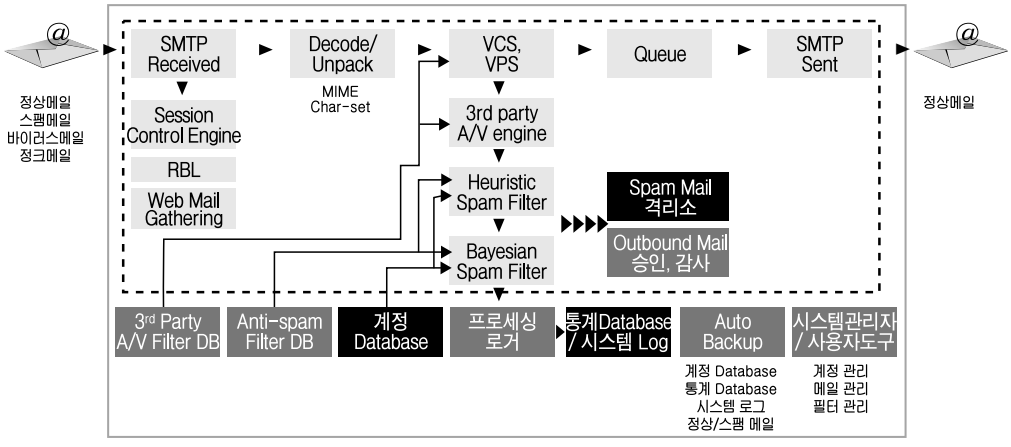
구 분	기 술		구현여부
발송 단계	오픈 렐레이 및 프록시 차단		O
	발송 총량 제한		O
	발송 비용 부담	Challenge & response 또는 bouncing back	O
		Online Stamp	-
		Hash Cash	-
		Graylist	Beta
	유동 IP이용자의 25번 포트 차단		O

구 분	기 술		구현여부
수신 단계	필터링 기술	단어 / 전송자정보 / 이미지 / 패턴학습	O
		신뢰도 평가시스템 (reputation system)	O
	발송자 인증 기술	Reverse DNS / HELLO Check	O
		SPF	O
		Sender ID	Beta
		DKIM	Beta
		White IP 등록	O
정부권장기술	SPF (발송자 인증)		O
	RBL (필터링)		O
기 타	URL/Heuristic/Bayesian/VPS/VCS/AIBlocking/Collaborative Spam Filtering		O

[기타 기능 및 특징]

- SMTP : Real Time Blacklist, 세션컨트롤링, 도메인 인증, AI Blocking, 내부 사용자의 외부 메일 및 웹 메일도 스팸 수집 및 차단
- Contents Filtering
  - URL/Heuristic/Bayesian 필터링
  - 최대/최단 주기의 필터 업데이트 지원 (패턴별 매분/매시간/매일 업데이트)
  - Collaborative Spam Filtering : Jiran 협업 시스템의 조합을 이용한 스팸, 바이러스 메일의 확률 계산
- 빠른 바이러스 차단 : 소포스(Sophos)등 3rd party 엔진, 독자 기술인 VPS/VCS로 실시간 웜 차단 기능 지원
- 내부정보 유출방지 : 회사 기밀정보에 대한 감사 및 승인, DRM기술 연동을 통한 내부 자료 유출 차단 기능 (옵션)

⑥ 구현원리



⑦ 구매비용

▶ 사용자 수에 따른 단가 별도 책정

(구분 : 50/ 100/ 150/ 250/ 500/ 1,000/ 2,500/ 5,000/ 10,000/ 30,000/ unlimited)

더블블럭

WBlock

- *(주)디프소프트*
- *홈페이지 : http://www.deepsoft.co.kr*
- *기술지원팀 (02-562-9051/8906, support@deepsoft.co.kr)*
  영업팀 (02-562-8545/9061, taehoon@deepsoft.co.kr)

① **제품명 :** WBlock 4

② **사용환경**

- 지원OS
  - Windows 2000/2003 server 이상, Linux Redhat계열 7.3 이상, Solaris 6 이상
- 권장 H/W
  - CPU PentiumIII 500 이상, Memory 512Mb 이상, HDD 36Gb 이상

③ **타겟고객층 : 서버용**

- KT 등 600여 개 업체, 학교, 기관

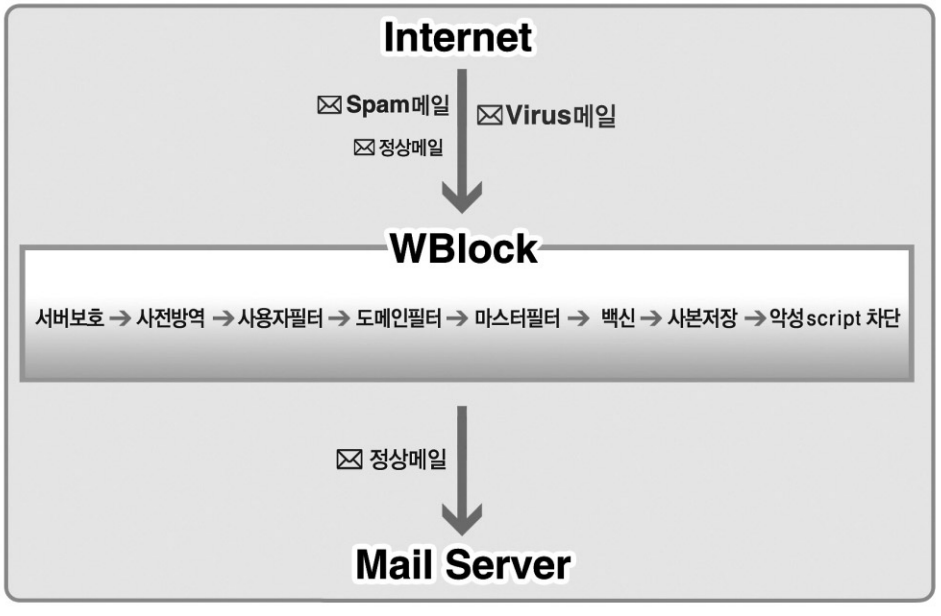
④ **기능**

아래 표는 기능의 우열을 나타내는 것이 아니며 단순히 해당 제품의 기술적 특징을 나타내는 것임

구 분	기 술		구현여부
발송 단계	오픈 렐레이 및 프록시 차단		O
	발송 총량 제한		O
	발송 비용 부담	Challenge & response 또는 bouncing back	△
		Online Stamp	△
		Hash Cash	△
		Graylist	△
	유동 IP이용자의 25번 포트 차단		O
수신 단계	필터링 기술	단어 / 전송자정보 / 이미지 / 패턴학습	O
		신뢰도 평가시스템 (reputation system)	O
	발송자 인증 기술	Reverse DNS / HELLO Check	O
		SPF	O
		Sender ID	△

구 분	기 술		구현여부
수신 단계	발송자 인증 기술	DKIM	△
		White IP 등록	○
정부권장기술	SPF (발송자 인증)		○
	RBL (필터링)		○
기 타	악성 script 차단		○
	Traffic Control		○
	사전방역		○

⑤ 구현원리



⑥ 구매비용

▶ Package : 사용자 수 300 이상 (최소 사용자 수 100)

• 별도 문의

▶ ASP : 사용자 수 300 이하 권장

• 이메일 계정당 월평균 2,000원 ~ 3,000원 / 연평균 22,000원 ~ 34,000원

Local & Overseas
Service Solution

국내 · 외 무료 솔루션

특징 구입비용이 들지 않으나 설치 및 이용 측면에서 사용자의 추가노력이 상용제품에 비해 더 필요할 수 있음

※ 이 장의 용어해설은 PP.51 ~ 53 참조

스팸어쌔신 Spam Assassin

▸ *홈페이지 : http://spamassassin.apache.org*

① **제품명** : SpamAssassin

※ 아직 한글화 버전은 출시되어있지 않으나 ok_locales 기능을 사용하여 non-ISO-8859 언어 (한글, 일본어 중국어 등)의 메시지 처리 가능

② **사용환경** : Unix, Linux

③ **타겟고객층** : 서버용

④ **기능**

아래 표는 기능의 우열을 나타내는 것이 아니며 단순히 해당 제품의 기술적 특징을 나타내는 것임

구 분	기 술		구현여부
발송 단계	오픈 렐레이 및 프록시 차단		-
	발송 총량 제한		-
	발송 비용 부담	Challenge & response 또는 bouncing back	-
		Online Stamp	-
		Hash Cash	O
		Graylist	-
	유동 IP이용자의 25번 포트 차단		-
수신 단계	필터링 기술	단어 / 전송자정보 / 이미지 / 패턴학습	O
		신뢰도 평가시스템 (reputation system)	-
	발송자 인증 기술	Reverse DNS / HELLO Check	-
		SPF	O
		Sender ID	-
		DKIM	-
		White IP 등록	O
정부권장기술	SPF (발송자 인증)		O
	RBL (필터링)		O

- 아파치 라이센스 2.0(Apache License 2.0)에 의거하여 무료로 배포되는 스팸메일 차단 솔루션으로 content, rule, 네임서버(DNS) 기반의 필터링, 통계적 방법 등 사용

⑤ **구현원리**

- 다수의 스팸판별기준을 수신된 메일의 헤더나 내용에 적용하여 적용된 값의 총 합이 일정 수치를 넘어서게 되면 해당 메시지를 스팸으로 분류, 이를 삭제하거나 특정 폴더로 분리 저장
- SpamAssassin의 사용자는 SpamAssassin에서 제공하는 다양한 각각의 값들을 조절하여 자신의 환경에 알맞은 스팸대응수위를 결정하며 그에 따른 메시지 처리방법 등을 다양하게 적용할 수 있음

⑥ **구매비용** : 무료 (기능 제한 없음)

스팸닥터

Spam Doctor

- *(주)데이타웨이브시스템 (02-3413-2050)*
- *홈페이지 : http://www.dataware.co.kr*

① **제품명 :** 스팸닥터 (SpamDoctor)

② **사용환경 :** MS Outlook (Win9x, Win2k, WinXp)

③ **타겟고객층 :** MS Outlook 개인 이용자

④ **기능**

아래 표는 기능의 우열을 나타내는 것이 아니며 단순히 해당 제품의 기술적 특징을 나타내는 것임

구 분	기 술		구현여부
발송 단계	오픈 렐레이 및 프록시 차단		-
	발송 총량 제한		-
	발송 비용 부담	Challenge & response 또는 bouncing back	-
		Online Stamp	-
		Hash Cash	-
		Graylist	-
	유동 IP이용자의 25번 포트 차단		-
수신 단계	필터링 기술	단어 / 전송자정보 / 이미지 / 패턴학습	O
		신뢰도 평가시스템 (reputation system)	-
	발송자 인증 기술	Reverse DNS / HELLO Check	-
		SPF	-
		Sender ID	-
		DKIM	-
		White IP 등록	-
정부권장기술	SPF (발송자 인증)		-
	RBL (필터링)		-

⑤ **구현원리**

- 사용자의 PC에서 구동되는 프로그램으로 모든 메일 서버에 대한 스팸 메일 필터링을 제공하며 기본 필터 없이 통계적 학습으로 스팸 메일을 익혀 차단하는 '인공 지능 방식'의 강력한 스팸 메일 차단 프로그램

⑥ **구매비용 :** 무료 (기능 제한 없음)

Government Promotion

정부권장 기술

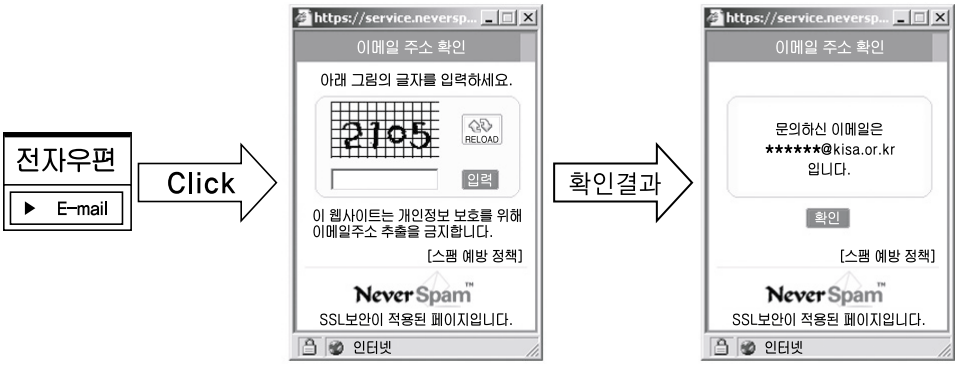
특징 | 스팸을 감축하는 환경을 구축하기 위한 기반기술

가. 이메일주소 추출방지 프로그램 "NeverSpam"

▶ 2002. 12월 개발하여 현재까지 불법스팸대응센터 홈페이지(www.spamcop.or.kr)를 통해 무료 보급 중

▶ **기술 개요** : 이미지 파일 생성 방식에 HIP(Human Interactive Proof) 기술을 결합하여 웹상에 표기된 이메일주소를 이메일주소 추출 프로그램이 가져가지 못하도록 보호

▶ **보호 원리** : 아래의 예처럼, 이메일주소를 웹상에 그대로 공개하지 않고 한글이나 기타 아이콘으로 숨겨놓은 후, 이를 클릭했을 때에만 사람 여부를 판단할 수 있는 간단한 퀴즈를 통해 이메일주소를 보여주게 됨



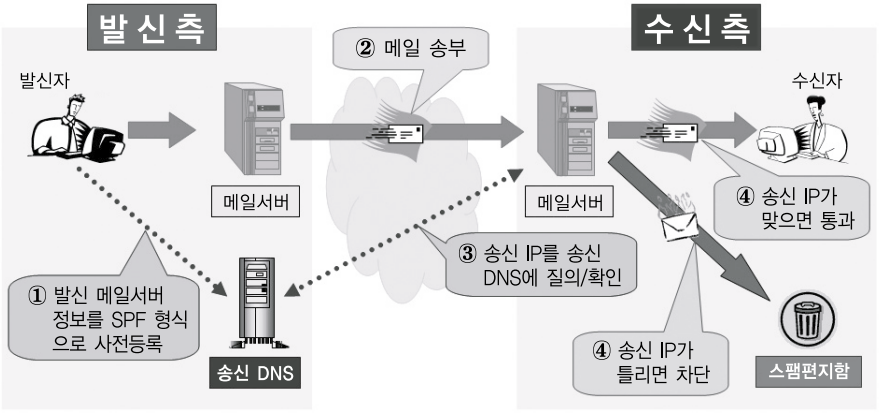
나. 메일서버 등록제 "SPF"

▶ 2005. 11월부터 국내 주요 10개 포탈을 중심으로 메일서버등록제(SPF: Sender Policy Framework) 도입 및 활용 추진 중

▶ **기술개요** : SPF를 통해 발송자 정보가 위 · 변작된 스팸을 식별함으로써 이메일 전송 체계의 구조적 취약점 보완

▶ **SPF 작동원리**

- 발송자 도메인 : 발송 메일서버를 공개하기 위하여 해당 DNS에 SPF 레코드를 등록
- 수신자 도메인 : 발송자 DNS에 등록된 SPF 레코드를 확인하고 결과값에 따라 이메일 수신여부 결정



[SPF 인증경로]

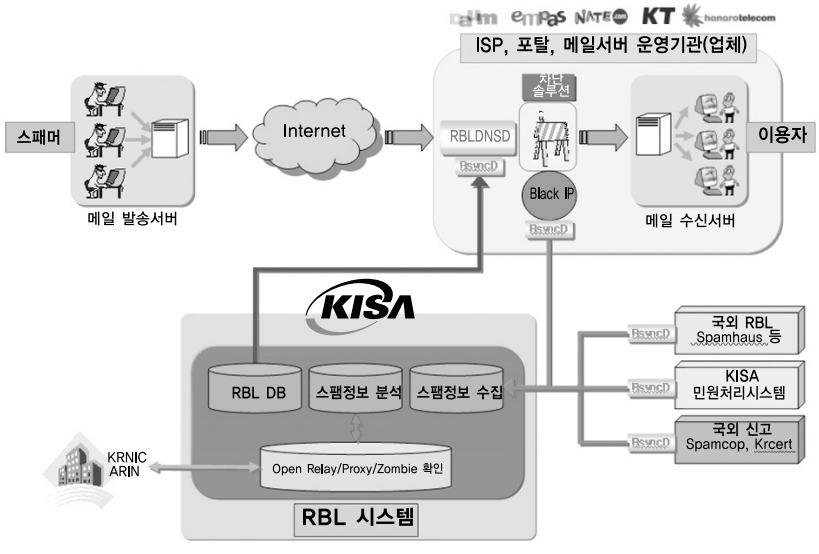
다. 실시간스팸차단리스트 "RBL"

▶ 2005. 11월부터 국내 · 외 스팸 정보를 수집하여 구축한 실시간 스팸차단리스트(RBL : Real-time Blocking List)를 국내 ISP, 포탈 및 일반 메일서버 운영기관 등에 보급하여 자율적인 스팸차단에 활용토록 유도

▶ **기술 개요** : 국내 · 외의 다양한 스팸정보를 실시간으로 통합 · 분석하여 IP 기반의 등급별 스팸차단리스트 생성

▶ RBL 구현과정

- 국내 · 외 스팸 정보를 정해진 주기에 따라 수집
  - 국내 주요 ISP, 포탈, 스팸차단솔루션 업체 등의 스팸차단 정보
  - 국외 주요 SBL 및 스팸신고(Spamcop, KrCERT) 정보
  - KISA 불법스팸대응센터 신고접수 민원
- 정보제공기관의 신뢰도, 차단사유, 빈도, 과거 SBL 등재기록 등을 종합적으로 분석하여 단계별 Blocking List 생성
- RBL에 등재되는 IP에 대해서는 자체적으로 Open Relay/Proxy 여부 등을 검사하고 DNS에 등록된 해당 ISP 정보 확인



[RBL 시스템 개념도]

※ RsyncD : Rsync Daemon / RBLDNSD : RBL DNS Daemon

스팸메일, 줄이는 것이 경쟁력

1. 스팸기술과 대응기술은 창과 방패의 대결!

2. RBL 설치 및 운영 지침서

3. SPF 레코드 설치 및 운영 지침서

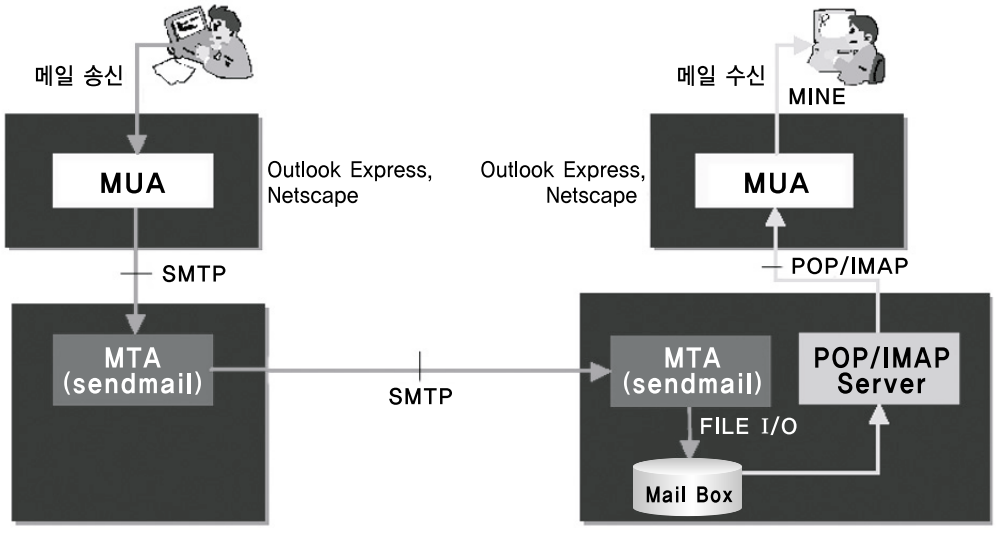
1 스팸기술과 대응기술은 창과 방패의 대결!

1. 이메일 전송 체계

이메일은 인터넷의 등장과 함께 인터넷을 이용하는 네티즌들에게 가장 광범위하게 이용되고 있는 통신수단이다. 또한 모든 비즈니스에서 빠르고 정확하게 자료를 전달할 수 있는 수단으로써 인터넷을 대중화시키는 결정적인 역할을 하였다.

이메일은 컴퓨터 통신망에서 신뢰를 기반으로 만들어진 SMTP(Simple Mail Transfer Protocol)을 이용하여 정보 또는 자료를 전달한다. 즉, 이메일 수신자는 발송자가 전달한 메시지를 아무런 의심 없이 자신에게 도착한 메일이면 무조건 수신하도록 만들어졌다.

이메일 전송 체계는 다음과 같다.



용어 해설

- **MUA** (Mail User Agent) : 사용자가 이메일을 송 · 수신할 때 사용하는 클라이언트 프로그램으로 아웃룩/아웃룩 익스프레스 등이 대표적인 예임
- **MTA** (Mail Transfer Agent) : 인터넷 상에 있는 하나의 컴퓨터로부터 다른 컴퓨터(메일 서버)로 전자 메일을 전송하는 서버 프로그램. sendmail, qmail, postfix 등이 대표적인 예이며, 메일서버 관리자가 운영하게 됨
- **SMTP** (Simple Mail Transfer Protocol) : 이메일 서버 간에 메시지를 전송하기 위해서 사용되는 인터넷 프로토콜
- **MIME** (Multi-Purpose Internet Mail Extensions) : 원래의 인터넷 이메일 프로토콜, 즉 SMTP를 확장하여 오디오, 비디오, 이미지, 응용프로그램, 기타 여러 가지 종류의 데이터 파일들을 주고받을 수 있도록 기능이 확장된 프로토콜임
- **POP3/IMAP**(Post Office Protocol 3/Internet Message Access Protocol) : 이메일을 수신하고 보관하는 표준 프로토콜로써, 사용자가 이메일 서버로 하여금 본인의 이메일을 확인할 수 있도록 정보를 제공하는 기능을 수행

① **송신자** : 본인의 컴퓨터에서 아웃룩 익스프레스 등의 MUA를 통하여 이메일을 작성

② **MUA** : 작성이 끝난 이메일은 MUA의 요청으로 사용자의 이메일 계정을 운용하고 있는 이메일 서버의 MTA로 전송됨

③ **MTA** : 이를 다시 수신자의 이메일 계정이 위치한 이메일 서버의 또 다른 MTA로 전송함. 전송된 이메일은 수신자의 이메일 계정(Mail Box)에 쌓이게 됨

④ **Mail Box** : 수신자의 Mail Box에 쌓인 이메일은 메일을 보내기 위하여 POP3/IMAP 서버에 전송됨

⑤ **수신자** : POP3/IMAP서버로부터 이메일을 수신하도록 자신의 MUA에 요청하여 이메일을 수신하게 됨

2. 스팸발생 원인

1) 기술적 원인 : 메일전송 프로토콜(SMTP)의 익명성 악용[1)]

① HELO : host name 입력
② MAIL FROM : sender 입력
③ RCPT TO : receiver 입력
④ DATA : 사용자가 실제로 보는 메시지 내용
(header, subject, body, attached file 등) 입력
⑤ QUIT

[메일 전송을 위한 단계별 SMTP 명령어]

- HELO 뒤의 host name에서 FQDN(Fully Qualified Domain Name)을 확인하지 않음으로써 송신자가 실제하는 Domain 또는 Host Name으로부터 메일을 송신하는지 알 수 없음
- MAIL FROM뒤의 sender를 확인하지 않고 단지 sender@a.b.c.d와 같이 syntax check만을 함으로써, 송신자의 메일주소가 실제 존재하는 메일주소인지 확인할 수 없음
- SMTP의 MAIL FROM과 메일헤더의 From과는 같을 필요가 없고, SMTP의 RCPT TO와 메일헤더의 To가 같을 필요가 없기 때문에 스팸 전송자는 자신의 존재를 숨기며 안전하게 스팸메일을 수신자에게 전송할 수 있음
- 즉, SMTP의 RCPT TO에만 실제 수신자의 이메일 주소를 쓰고, 나머지 SMTP와 메일헤더의 송신자/수신자 란에 가상의 주소를 기재하여도 원하는 수신자에게 메일이 전송됨

이러한 SMTP의 취약점을 악용하여 스팸메일 발송자들은 스푸핑(spoofing), 오픈 릴레이, 오픈 프록시 및 좀비 감염 등의 방법으로 신원을 감춘다. 이러한 각 기법들은 이메일 헤더를 통해 스팸메일 발송자들을 식별하기가 매우 어렵게 만들기 때문에 법을 집행하는 정부 입장에서는 큰 문제로 인식하고 있다.

1) 미 FTC 보고서, "National Do Not E-mail Registry"(2004. 6.) pp. 8 - 13 참조

2) 경제적 원인 : 저비용 고효율

기본적으로 스팸발송비용은 디지털 매체의 특성상 한통당 소요되는 한계비용이 0원에 가깝다. 더구나 정액제로 빠른 속도의 인터넷서비스를 무한 사용할 수 있으며 저렴한 값에 이메일주소 목록이나 스팸메일 발송기를 손쉽게 구입할 수 있는 국내 환경에서는 외국에 비해 더욱 스팸메일 발송비용이 저렴하다.

발송비용이 이같이 저렴한 데 비해 스팸으로 인한 마케팅 효과는 상당히 높다. 2002. 11. 13일 월스트리트 저널에 실린 기사 "For Bulk E-Mailer, Pestering Millions Offers Path to Profit"에 의하면, 발송된 전체 스팸 중 0.001%만 반응을 보여도 발송자는 손해를 보지 않는다고 한다. 이러한 스팸의 저비용 고효율의 특성이야말로 스팸이 근절되지 않는 가장 큰 이유이다.

3. 스팸 대응기술 현황

스팸에 대한 기술적, 법적 규제가 강화됨에 따라 이를 회피하고자 하는 스패밍 기술 또한 날로 지능화하고 있다. 국외 포탈(Hotmail, Yahoo 등)에 무단으로 계정을 생성하거나 외국을 경유하여 스팸을 발송하는 사례가 늘고 있는 추세이며, 향후 무선망의 본격 개방, 유비쿼터스 환경의 대중화 등 정보통신 환경변화에 따라 발송자를 추적하기 어려운 신종 스팸의 등장이 예상된다. 이에 대응하는 기술을 스팸 발송 단계에 따라 아래와 같이 정리한다.

1) 발송전

① 수신자 이메일주소 수집 차단 기술

메일주소를 웹브라우저에 출력되기 전에 여러 형태로 변형함으로써 이메일주소를 숨겨놓는 아래의 다양한 이메일 마스킹 기술들을 적용하여 자동 프로그램이 이메일주소를 수집해내지 못하도록 조치한다. 이러한 조치는 Java Script 변환, ASCII Code 변환, CGI SSI 변환, 이메일 주소 이미지 파일 생성 기술 등을 통해 이루어진다. 한국정보보호진흥원(KISA)에서는 이메일 주소 추출을 방지할 수 있는 프로그램인 NeverSpam (http://www.neverspam.or.kr/ download_spamcop2.html)을 무료로 배포하고 있다.

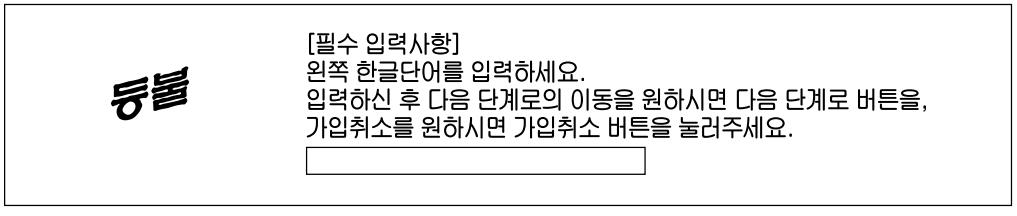
② 이메일주소 생성 대응 기술

스패머가 이메일주소를 임의로 생성하여 메일을 발송할 때, 존재하지 않는 이메일주소에 대해 '수신자 없음' 확인메일을 회신해주지 않도록 설정할 수 있는데 이것을 이메일주소 생성 대응 기술로 볼 수 있다.

③ 웹메일 자동생성 차단 기술

회원가입단계에서 인간의 육안으로만 식별이 가능한 왜곡된 이미지를 무작위로 제시하여 제한시간 내 입력토록 하는 등의 HIP(Human Interactive Proof) 기술을 적용함으로써 자동 프로그램에 의한 무차별적인 계정생성을 제한한다. 사람은 풀 수 있지만 기계적인 프로그램은 쉽게 풀지 못하는 인지적 단계의 퍼즐을 제공하는 방식으로, 아주 단순한 단어를 무작위로 골라 글자를 약간 훼손시킨 뒤 복잡한 배경 화면 위에 표시하는 CAPTCHA(Completely Automated Public Turing test to tell Computers and Humans Apart) 기술이 가장 대표적이다.

〈CAPTCHA 예시〉



2) 발송 단계

① 오픈 릴레이 및 프록시 차단

이메일은 메일발송지에서 수신지까지 직접 전달되는 경우와 전달과정 중 중계서버를 거쳐 전달이 되는 경우가 있다. 이때 오픈 릴레이 중계서버를 거쳐 전달되는 경우 최초 전달자를 식별하기 어렵기에 이러한 기능이 스팸메일의 발신지를 속이기 위해 주로 사용되고 있다. 오픈 프락시 기능은 최초 발신지의 IP 정보가 유실된다는 점은 오픈 릴레이 기능과 매우 유사하나 기능적으로는 발신지의 IP 패킷 정보를 최종 수신지에 전달한다는 것이 다르다. 이러한 경유지를 차단함으로써 스패머가 자신의 발신지를 위조하여 메일을 발송하는 것을 막을 수 있다.

② 발송량 제한

발송량 제한방식은 특정 IP에 대하여 일정시간당 전송할 수 있는 메시지의 수를 제한함으로써 한 IP에서 대량으로 메일을 발송할 수 없도록 하는 방법이다.

③ 발송비용 부담

- **Online Stamp** : 온라인 우표제 방식의 이메일 시스템은 스패머에게 금전적인 비용을 발생시켜 스팸을 전송하지 못하게 하는 방법으로 대량 메일발송자에게 일정량의 비용을 부과하여 스팸발송을 억제하는 방법이다.

- **challenge & response 또는 Bouncing back** : 이는 기존의 필터링방식의 스팸처리방식이 수신서버에 부과하는 부하를 스팸메일 발송자에게 부담시키기 위해 고안된 방법이다. 내부적으로 화이트 리스트와 블랙리스트를 관리하며 화이트 리스트에 등재되어 있지 않은 사용자가 발신한 메일은 발신자에게 확인메일을 발송하여 이에 응답 메일이 수신되면 해당 발신자의 메일주소를 화이트리스트에 보관, 추후에는 이러한 과정 없이 메일을 사용할 수 있게 하는 방법이다.

- **Hash-Cash** : Hash-Cash는 메일발송비용과 메일처리비용의 비대칭성을 해결하기 위해 고안된 방법으로 메일발송시 수신자의 이메일주소를 사용한 계산값을 첨가하여 이 값이 정상적으로 첨가된 메일만 수신 처리하는 방법이다. 해쉬캐쉬 사용 시 스팸발송자는 다량의 메일을 짧은 시간에 발송할 수 없어 경제성을 상실하게 되는 반면, 소량의

메일을 발송하는 정상 사용자는 그 차이를 느낄 수 없게 하는 방법이다.

▶ **Greylist** : 그레이리스트는 시스템에 처음 접속한 사용자에 대하여 한시적 접속제한을 하며 일정기간이 지난 뒤 재 접속 시도자에 한하여 메일전송을 허용함으로써 한번 전송이 일어난 사용자에 대해서는 지연 없는 메일전송을 허용해 주는 방법이다. 이는 대부분의 스팸이 메일발송시 발생하는 접속지연을 처리하지 못하는 점에 착안한 것으로 소량 고품질의 메일을 정기적으로 사용하는 메일환경에 적합한 장치이다.

④ 유동IP 이용자의 25번 포트 차단

정상적인 메일발송의 경우 발신자가 직접 수신지의 메일포트(25번)를 접속하지 않고 자신의 도메인 메일서버를 통하여 발송하며 대부분의 정상메일서버는 유동 IP대역에 설치되어 있지 않는다는 점에 착안한 스팸대응기술로서 유동IP 사용자의 수신서버 직접접속을 기술적으로 제한하여 유동대역에서 발송기 등을 이용한 스팸행위를 효과적으로 막을 수 있는 방법이다.

3) 수신 단계

① 사후 필터링 기술

▶ **단어/전송자정보/이미지/패턴학습** : 수신도메인에 전송되어진 이메일 메시지의 내용, 발신자 정보, 포함된 이미지 혹은 메시지 패턴을 이용하여 스팸성이 높다고 판단되어진 메시지는 최종수신자에게 전달하지 않거나 주제어 란에 특정어구를 삽입하여 최종수신자가 편의에 따라 필터링 처리할 수 있도록 하는 기술이다.

▶ **신뢰도 평가시스템 (reputation system)** : 신뢰도 평가시스템은 이메일 발송자의 IP 혹은 도메인별 메일사용 이력을 기록함으로써 각 IP 및 도메인별 신뢰도를 평가, 스팸발송 등에 악용되는 IP나 도메인으로부터 전송되는 메일은 수신하지 않을 수 있도록 정보를 주는 시스템이다.

② 발송자 인증 기술

▶ **SPF(Sender Policy Framework)** : 이메일 발송시 현 SMTP의 특성인 발송자 정보를 감출 수 있다는 취약점을 악용하여 스팸, 피싱 등의 악성행위가 가능하였으므로 메일의 발송경로를 인증함으로써 이를 원천차단하는 기술이다. SPF는 발송 도메인의 메일

발송정책을 해당 도메인의 DNS 서버에 설치하는 메일정책표기 단계와 메일정책확인 단계로 나뉜다. 메일정책표기 단계는 자사 도메인의 발송호스트를 SPF 레코드 형태로 DNS 서버에 설치하는 단계이며, 메일정책확인 단계는 수신된 메일이 적법한 발송서버를 통해 발송되었는지를 판단하고 판단결과에 따라 해당메일의 수신여부를 결정하는 단계다. SPF는 추후 도메인 신뢰도 평가시스템(Reputation System)과 연동하여 보다 효과적으로 사용될 수 있다.

- **Sender ID** : Sender ID는 Microsoft사에 의해 제안된 확장된 형태의 SPF로 발송 도메인 인증기능에 발송자 인증기능인 PRA(Purported Responsible Address)기능을 추가한 인증기술이다. Sender ID를 이용한 메일경유지 확인 시 메일발송 도메인에 별도의 PRA(Purported Responsible Address)레코드가 설치되어있지 않더라도 SPF 레코드가 설치되어있는 경우 이와 완벽하게 호환된다.

- **DKIM(DomainKeys Identified Mail)** : DKIM은 야후(Yahoo)사와 CISCO사에 의해 공동 제안된 이메일 메시지 인증방법으로 발송도메인은 자신의 메일서버를 통해 발송되는 메일을 공개키 방식으로 서명하고 이를 수신도메인에서 확인함으로써 메시지 발송과정의 위 · 변조를 원천적으로 방지할 수 있는 기술이다.

- **PKI 또는 PGP를 통한 인증** : PKI(Public Key Infrastructure) 및 PGP(Pretty Good Privacy)는 공개키 방식의 이메일 암호화 및 전자서명 방법이다. PKI는 중앙화된 인증서 관리를 통해 메시지의 전송과정 및 발송과정의 위?변조를 방지 할 수 있는 기술이며, PGP는 메일사용자간의 공개키 교환을 통해 동일한 효과를 얻을 수 있는 기술이다. 이 두 기술은 현재의 SMTP 환경에서 메시지의 암호화 혹은 서명을 통한 메시지 암호와 완결성 보장 등을 위한 방법으로 사용되고 있다.

- **White IP 등록 (Bonded Sender 등)** : 스팸메일의 양이 급격히 증가하고 이에 따른 과도한 스팸차단으로 정상사용자의 메일이 과, 오 차단됨을 방지하기위해 정상적 메일 사용자의 IP를 등록하고 등록된 IP에 대해서는 전송을 보장해 주는 방법이다.

2 RBL 설치 및 운영 지침서

1 배경 및 목적

KISA RBL1)은 한국정보보호진흥원(이하 "KISA")이 개발한 IP 기반의 실시간 스팸차단 리스트이다. 국내의 주요 메일 수신 사이트에 설치된 스팸차단 소프트웨어가 스팸을 차단한 결과로 어떤 IP가 스팸을 발송하는 IP인지를 실시간으로 분석하여 그 결과를 배포함으로써, 스팸 발송 IP를 차단하는 역할을 한다.

KISA RBL은 두 가지 형태로 배포가 되며, 이 문서는 중소규모의 사이트에서 활용하는 방법을 설명한다.

RBL 차단기능이 포함되어 있는 스팸차단 솔루션이 사용되고 있는 경우, 이 문서에서 설명하는 RBL 베이스 주소2)만 입력하면 스팸차단 솔루션에서 차단을 수행한다. 본 문서는 RBL 차단기능이 포함된 스팸차단 솔루션이 없는 경우를 가정하고 작성되었다. 스팸차단 솔루션을 사용하고 있는 경우에는, 스팸차단 솔루션 공급자에게 RBL 기능에 대해서 문의하면 된다.

2 동작이해

기본적으로 차단 IP는 표준적인 DNS 형태로 공개된다. 특정 IP 주소(예를 들어 1.2.3.4)가 차단 IP에 들어 있는지 없는지를 확인하기 위해서는 다음과 같은 DNS LOOKUP을 통해서 조회할 수 있다.

% nslookup 4.3.2.1.krrbl.or.kr
(IP 주소를 맨 끝자리부터 역순으로 뒤집어서 배열하고, 그 뒤에 krrbl.or.kr 이라는 베이스 주소를 덧붙인 후에 nslookup 수행)

1) RBL (Real-time Blocking List) 실시간으로 스팸의 진원지가 되는 IP주소를 파악하여 공개하는 데이터 베이스
2) RBL 베이스 주소란 IP에 대한 RBL DNS 조회시 postfix로 덧붙여서 사용할 도메인 명을 의미함. 예를 들어, RBL 베이스 주소가 krrbl.or.kr 이고 IP 주소가 1.2.3.4일 경우, 4.3.2.1.krrbl.or.kr로 DNS조회를 하면 RBL에 등록되어 있는지를 확인할 수 있음.

만약 이렇게 Lookup한 후에 그 결과가 127.0.0.x 형태로 나오게 되면, 그 해당 IP는 차단으로 등록된 IP이며 그렇지 않고 "찾을 수 없음"으로 나오면, 차단이 아닌 IP이다.

2.1 차단리스트 레벨

KISA RBL에서는 3가지의 차단리스트를 제공한다.
레벨1은 스팸확률이 가장 높은 것으로써, 확인된 Open Relay, Open Proxy 서버의 IP주소가 포함된다.
레벨2은 스팸확률이 비교적 높은 IP를 막고자 할 때 사용한다.
레벨3은 스팸확률이 상대적으로 낮지만 커버리지가 가장 높다. 해외에서 리포트된 해외IP, 국내 유동IP 등 스팸가능성이 있는 IP가 포함된다.
어떤 레벨까지를 스팸차단에 사용할 것인가는 사용하는 측에서 결정하면 된다.

3 . rsync/rbldnsd를 이용한 연동

KISA RBL 사이트에서 차단 IP를 모두 다운로드 받은 후에 다운로드 받은 데이터 내에서 직접 Lookup 하는 방식을 취하게 된다.
이런 방식으로 사용하려면, 해당 사이트/머신이 KISA RBL사이트에 등록되어서 다운로드 권한을 부여 받아야 하며, 다운로드 권한을 부여 받은 다음에는 rsync 프로그램으로 주기적인 차단리스트 다운로드를 수행하게 되고, 다운로드 받은 차단리스트를 참조하는 것은 해당 사이트의 머신에 설치되는 rbldnsd 라는 프로그램을 통해서 조회하게 된다.
rbldnsd 라는 프로그램이 다운로드 된 차단리스트를 참조하게 되므로 머신 밖으로 DNS 조회가 나가지 않게 되어 사이트의 DNS 서버에 과부하를 야기하지 않는다. (rbldnsd는 로컬로 동작할 경우, 중소규모의 메일 서버에서 초당 3,000회 정도의 RBL DNS Lookup을 처리할 수 있다.)

3.1 rsync 다운로드 권한 신청 – 웹사이트

KISA RBL 사이트에 접속하여 계정신청을 하면 된다. 계정신청 시 사업자 등록증 사본이 필요하다.

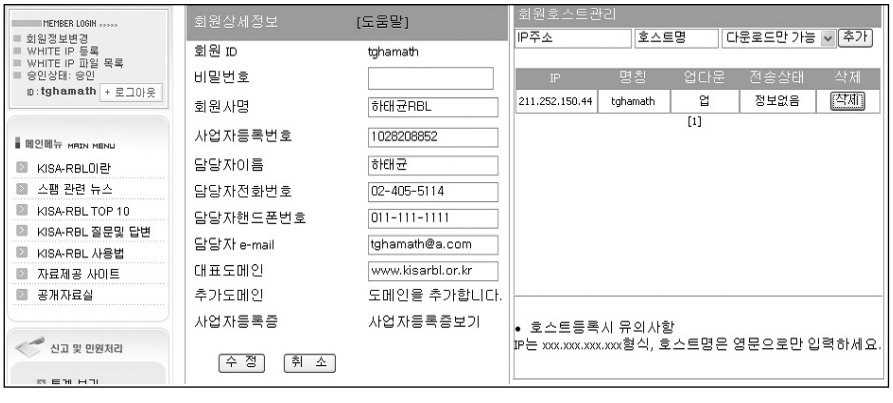
〈KISA RBL 사이트: www.kisarbl.or.kr〉

계정을 신청하면, KISA RBL 운영자가 검토한 후에 계정을 활성화시키고 확인메일을 보내 준다.

확인메일

KISA RBL에 등록하셨습니다.
다음 링크를 클릭하시면 로그인 하실 수 있습니다.
http://www.kisarbl.or.kr/web/confirm_email.jsp?your@mail.com
감사합니다.

확인 메일을 받은 후, KISA RBL 사이트에 접속하여 로그인하면 머신등록 메뉴가 나온다.



회원으로 로그인한 후 회원호스트관리에서 접속할 머신의 IP주소와 명칭(구별자)을 넣고 추가버튼을 누르면 화면과 같은 라인이 생기며, 그 머신은 데이터 다운로드가 허락된다.

3.2 rsync 다운로드 시험

머신의 IP가 다운로드 가능하도록 설정되었으면, rsync 명령어를 통해서 데이터를 다운로드 할 수 있다. 다음과 같은 명령어를 통해서 다운로드가 되는지를 확인한다.

```
% rsync -avz www.kisarbl.or.kr::spamlist1.txt /KISARBL/zone
(rsync패스)/rsync -avz kisarbl.or.kr::krrbl 받고자하는 디렉토리
```

이 명령어가 끝나면 /KISARBL/zone 디렉토리에 spamlist1.txt, spamlist2.txt, spamlist3.txt 파일이 생성된다. Spamlist1.txt 는 차단리스트 레벨 1, Spamlist2.txt은 레벨2, Spamlist3.txt은 레벨3의 경우이다.

Spamlist1.txt에는 레벨1인 차단 IP만 들어 있고, Spamlist2.txt에는 레벨 1, 2인 차단 IP가 들어있으며, Spamlist3.txt는 레벨 1, 2, 3 전체를 포함하고 있다.

3.2.1 주기적인 다운로드 설정

주기적으로 데이터를 다운로드 하려면, 다음과 같이 크론탭에 설정하면 된다. Rbl 데이터의 절대 위치가 /KISARBL/zone라고 했을 때,

```
# RBL download
0 * * * * rsync -avz www.kisarbl.or.kr::krrbl /KISARBL/zone
>/dev/null 2>/dev/null
```

(0 * * * * 은 매시 0분에 동작시킨다는 뜻이다. 0분 대신 5 또는 10으로 해도 된다.
수행하는 명령어는 rsync -avz www.kisarbl.or.kr::krrbl /KISARBL/zone 이다.
이 명령어가 수행되려면 rsync라는 명령어가 해당 서버에 설치되어 있어야 한다.
>/dev/null 2>/dev/null 은 rsync가 실행되면서 생기는 에러가 메일로 발송되지 않고 무시되도록 하는 것이다.)

3.2.2 rsync 다운로드 데이터 설명

다운로드 된 데이터는 다음과 같은 텍스트 데이터 이다. 레벨별로 텍스트 파일의 길이가 다르며, 레벨 3의 spamlist3.txt의 경우 다음과 같이 3개의 섹션으로 나눠진다.

```
:127.0.0.1:Blocked
211.37.48.243 "Krrbl"
211.217.38.129 "Krrbl"
80.51.255.213 "Krrbl"
211.233.80.31 "Krrbl"
201.144.13.99 "Krrbl"
203.254.120.15 "Krrbl"
211.233.80.33 "Krrbl"
211.117.163.69 "Krrbl"
```

단순한 IP 주소의 리스트로서, 레벨에 따라서 적게는 20만 많게는 200만 라인 정도의 텍스트 파일이다.

3.3 로컬 머신에 rbldnsd 설치하기

중대형 사이트에는 해당 머신 별로 별도의 RBL 전용 DNS 데몬이 설치되어야 하는데, 이는 rbldnsd 라는 오픈소스 프로그램을 사용하면 된다. 해당 프로그램을 다운로드 하여 설치하면 된다. (원본위치: http://www.corpit.ru/mjt/rbldnsd.html)

rbldnsd 프로그램의 사본은 KISA RBL 사이트의 다운로드 자료실에서 구할 수 있다.

3.3.1 rbldnsd 다운로드 받기 -> 웹사이트 다운로드 게시판

KISA RBL 사이트에 접속하여 "다운로드" 링크를 클릭하면 각 소프트웨어의 최신 버전이 공개 되어 있다.

3.3.2 rbldnsd 실행시키기

시스템의 이름을 확인한다.

```
% vi /etc/hosts
# Internet host table
#
127.0.0.1       localhost
203.233.240.204 a.com   a.com.  loghost
```

다운로드 한 프로그램을 압축을 푼 후에 압축을 푼 서브디렉토리에서

```
% ./configure
% make
```

하면 rbldnsd 프로그램이 생성된다. 생성된 프로그램을 임의의 위치에 복사하면 설치가 완료된다. rbldnsd가 설치된 다음에는 다음과 같은 명령어로 실행시키면 된다.

```
% cd 해서 rbldnsd가 설치된 디렉토리로 간다.
% ./rbldnsd -b -p 127.0.0.1/5353 a.com:ip4set:/KISARBL/zone
/spamlist1.txt  /tmp/rbldnsd.pid
```

(이렇게 설정할 경우, 로컬 머신의 5353번 포트로 DNS lookup을 할 수 있으며, 외부 머신에서는 이 포트에 접근할 수 없다.)

./Rbldnsd 실행,
-b (백그라운드),
-p(rbldnsd process id),
127.0.0.1(응답값),
5353(rbldnsd 사용포트),
a.com(호스트네임-hosts에 등록된 이름),
ip4set(ipv4사용),
/KISARBL/zone/spamlist3.txt(사용할 rbl파일),
/tmp/rbldnsd.pid(pid 이름 저장 파일)

3.3.3 rbldnsd 실행 확인하기

이렇게 수행시키면, rbldnsd 가 수행되고 nslookup 또는 dig명령을 수행할 수 있게 된다.

```
% nslookup
>server 127.0.0.1
```

이 상태에서 임의의 IP(예를 들어 1.2.3.4)일 경우, 베이스 주소가 krrbl.or.kr 일 경우,

```
>4.3.2.1.a.com
```

또는

```
% dig @localhost -p5353 4.3.2.1.a.com
```

로 Lookup을 시도하여 127.0.0.1 이 나오면 차단 IP이고 그렇지 않으면 정상 IP이다.

3.3.4 주기적인 데이터 반영 처리

크론 테이블에 다음과 같은 항목을 추가해 두면, 주기적인 다운로드가 이뤄진 후에 rbldnsd에 그 결과가 반영된다.

```
10 * * * * kill -HUP cat /tmp/rbldnsd.pid >/dev/null 2>/dev/null&
```

3.4 기존 메일 서버와의 연동

메일 서버와의 연동은 2장에서 설명한 바와 동일하다. 다만, 대량의 DNS 쿼리를 로컬머신에 설치된 rbldnsd로 전달하기 위해서 DNS설정이 별도로 요구 된다.

3.4.1 센드메일(Sendmail)과 연동방법

3.1에서 언급한 바와 같이 sendmail의 dnsbl이라고 부르는 FEATURE를 사용하여, 차단한다. 다만, 차단리스트에 대한 DNS 쿼리가 로컬머신으로 전달 되어야 하기 때문에 다음과 같이 DNS 서버에 존 포워딩 설정을 해야 한다. 이 설정은 DNS 담당자에게 도움을 청해야 한다.

```
존 포워딩 설정의 예
zone "a.com" IN {
        type forward;
        forward first;
        forwarders {
                127.0.0.1 port 5353;
        };
};
```

3.4.2 큐메일(Qmail)과 연동방법

qmail에서 제공되는 ucspi-tcp 패키지를 이용한다. 마찬가지로, 대량의 DNS 쿼리를 로컬로 소화하기 위해서 앞에서 언급한 존 포워딩 설정을 별도로 DNS 서버에 적용해야 한다.

3 SPF 레코드 설치 및 운영 지침서

1. SPF 레코드 작성

SPF 레코드는 DNS 서버의 존(Zone) 파일 TXT RR(Resource Record)에 설치되어 자사의 메일정책을 외부에 알리는 역할을 한다. 발신 도메인의 메일정책을 나타내는 이 레코드는 메일수신 초기단계에서 DNS 쿼리를 통해 얻어지며 이때 얻어진 발신도메인의 메일정책에 의거하여 처리된다. 이때 발신지 도메인에서 자신의 도메인에서 발송되지 않은 메일의 거부정책을 표명하였다면 발송도메인 이외의 장소에서 발송된 위조된 메일은 수신도메인에 전송되지 않고 수신이 거부된다.

2. SPF 레코드 설치(Publishing SPF 레코드)

자사 도메인의 메일정책을 나타내는 SPF 정보는 자사 DNS 존(Zone) 파일의 TXT RR(Resources Record)에 자신의 도메인의 메일정책을 SPF RFC에 정의된 레코드작성 규칙에 따라 작성하여 공표한다. SPF 레코드의 출판은 한국정보보호진흥원 스팸대응팀에서 작성한 SPF 기술설명서 혹은 SPF RFC(DRAFT-SCHLITT-SPF-CLASSIC-02)를 참고하여 작성하거나 SPF 레코드 출판을 도와주는 사이트 등을 참조하여 작성 할 수 있다.

SPF 레코드 출판 도우미 사이트
http://spf.pobox.com/wizard.html http://www.anti-spamtools.org/SenderIDEmailPolicyTool/Default.aspx

〈표 1 SPF 레코드 출판도우미 사이트〉

이때 잘못 작성된 SPF 레코드는 자사의 도메인 서버에 불필요한 부하를 부과 하거나 자사에서 발송된 메일의 정확한 전달을 저해할 수 있으므로 자신의 도메인에서 발송된 메일의

정상 수신여부를 반드시 확인하여야 한다. 이는 출판된 레코드의 정상작동여부를 알려주는 이메일주소를 이용하여 확인할 수 있다.

SPF레코드 설정 이메일주소
check-auth@verifier.port25.com 〈사용방법〉 만약 자신의 사이트 명이 domain.com, 자신의 id 가 admin이면 admin@domain.com의 주소를 사용하여 check-auth@verifier.port25.com으로 메일을 전송하면 설치된 SPF 레코드의 테스트 값을 전송하여 준다. 이때 자신의 도메인의 판정 값이 "pass"로 확인되면 SPF가 정상적으로 설정된 것으로 간주할 수 있다.

〈표 2 SPF레코드 설정 확인 이메일주소〉

2.1 Bind DNS 서버에서 SPF 레코드 등록방법 (UNIX, LINUX)

① 유닉스 계열의 네임서버인 BIND를 사용할 경우 /var/named 혹은 상응하는 BIND ZONE 파일 정의 패스에 존재하는 자신의 도메인 ZONE 파일에 자사의 메일정책을 나타내는 SPF 레코드를 추가한다.

② Name 서버를 재 시작한다.

ex) 레드햇 계열의 리눅스일 경우/etc/init.d/named restart

③ SPF레코드 정상작동여부를 확인한다.

ex) check-auth@verifier.port25.com로 메일발송 후 결과값 확인

```
#존 파일 예
$TTL 86400
@               IN      SOA     ns.example.com
root.example.com(
                        2005081200      ; serial
                        10800           ; refresh
                        3600            ; retry
                        604800          ; expire
                        86400 )                 ; ttl
                        IN      NS      ns.example.com.
                        IN      MX      mx1.example.com
        www             IN      A       192.168.1.100
        mail            IN      A       192.168.1.101
        example.com.    IN      TXT     v=spf1 a:mail.example.com -all"
```

※ 밑줄로 표시된 마지막 열이 추가된 SPF레코드임

〈표 3 SPF 설치 존-파일(예)〉

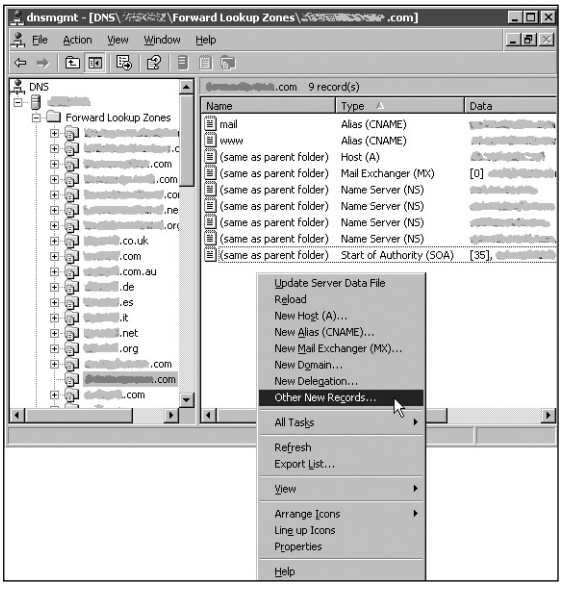
2.2 WINDOWS 2000/2003 DNS 서버에서 SFP레코드 등록방법

마이크로소프트사의 MMC(Microsoft Management Console)를 사용하여 DNS 존 파일을 편집할 수 있다.

① 시작버튼 -〉 프로그램 -〉 관리자 도구 -〉 DNS

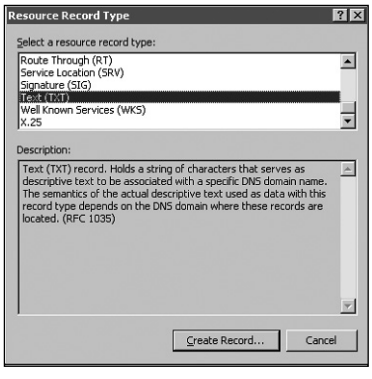
② Forward lookup zones을 마우스 오른쪽 버튼을 사용 하여 선택한 뒤 SPF 레코드를 출판할 도메인(도메인 존 파일)을 선택한다.

③ 레코드 리스트를 마우스 오른쪽 버튼으로 선택한 뒤 메뉴에서 "Other New Record"를 클릭한다.



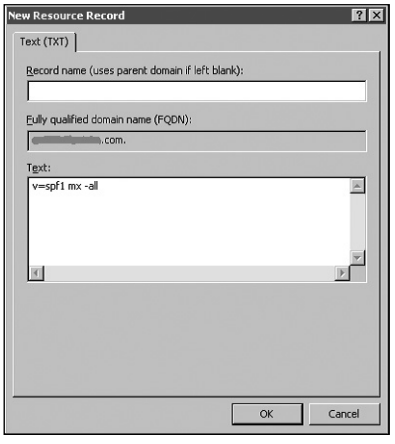
〈그림 1 SPF 출판법 1〉

④ TXT 레코드 타입을 선택한 뒤 "Create Record"를 클릭한다.



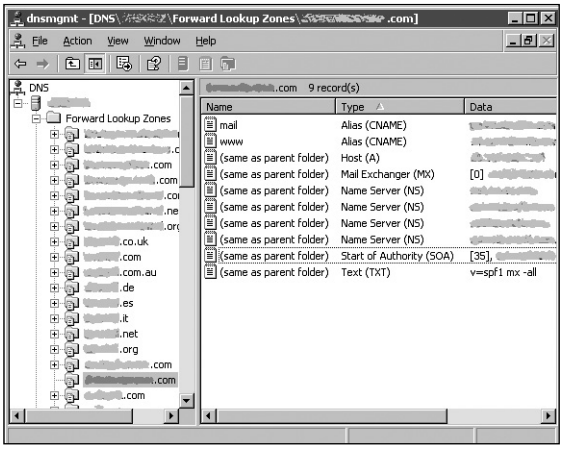
〈그림 2 SPF 출판법 2〉

⑤ 위에서 작성된 SPF 레코드를 Text 창에 추가한다.
(이때 아래그림의 "v=spf1 mx –all"은 자사의 레코드로 대치 한다)



〈그림 3 SPF 출판법 3〉

⑥ Ok를 선택한 뒤 출판된 레코드를 확인한다.(점선 안의 내용)



〈그림 4 SPF 출판법 4〉

3. SPF 레코드 동작확인

자신의 도메인에 SPF레코드 설치 시 설치된 SPF가 자신의 도메인의 메일정책을 정확하게 반영하는지 여부를 반드시 확인하여야 한다. 잘 알려진 확인방법은 다음과 같다.

- check-auth@verifier.port25.com에 자신의 도메인명의 메일 전송 후 반송메일의 결과값 확인

반송메일 결과값의 예

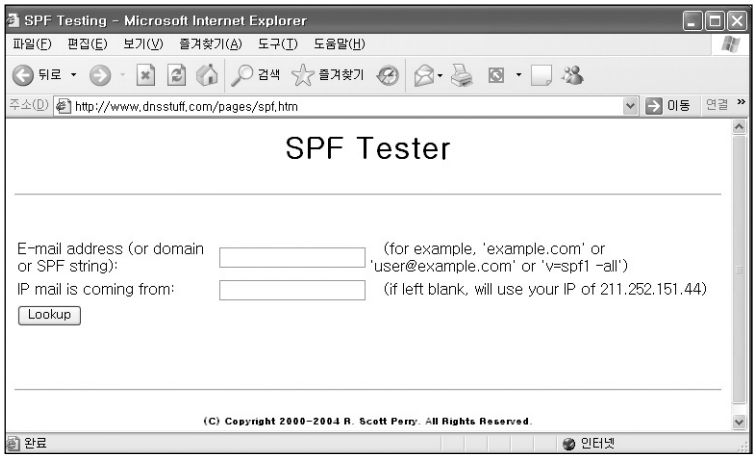
```
==========================================================
Summary of Results
==========================================================
mail-from check: pass
PRA check: pass
DomainKeys check: neutral (message not signed)
==========================================================
Details:
==========================================================
HELO hostname: sniper.kisa.or.kr
Source IP: 211.252.150.22
mail-from: joonkim@kisa.or.kr
PRA Header: from
PRA: joonkim@kisa.or.kr

SPF TXT record/s:
v=spf1 a:sniper.kisa.or.kr ~all

PRA TXT record/s:
v=spf1 a:sniper.kisa.or.kr ~all

Domain Key TXT record:
None
```

• http://www.dnsstuff.com/pages/spf.htm를 통한 직접확인



〈그림 5 SPF 확인 사이트〉

4. SPF 확인장치 설치

SPF 레코드가 자사의 메일정책을 외부에 알리는 역할을 하는데 반하여 SPF 확인 장치는 메일 수신부의 MTA[1](Mail Transfer Agent)에 설치되어 자신의 도메인에 수신된 메일에 대하여 송신도메인의 정책에 의거하여 처리한다. 이때 SPF 레코드의 처리는 내용분석(Content Filtering) 전 단계에서 실시하여 메일정책에 위배되는 메일을 SMTP[2] data가 전송되기 전 커넥션 단계에서 차단함이 가장 경제적인 방법이다. SPF[3]를 적용하기 위해서는 Sendmail의 경우 버전 8.12이상이며 밀터(milter) 기능이 컴파일(compile) 되어있어야 한다. 참고로 Sendmail 버전 8.13이상은 밀터 기능이 기본으로 컴파일 되도록 되어있다. Postfix의 버전 2.1 이상일 경우 SPF 패치를 설치하거나 공식 SPF 사이트인 spf.pobox.com에서 제공하는 Policy Daemon을 설치하여 SPF 기능을 사용할 수 있다. 이들 중 자사의 메일서버의 생산성에 가장 적은 영향을 미치는 방법은 메일서버 앞에 위치한 스팸솔루션에서 SPF 테스트를 실시하는 것이나 이는 해당 도메인에서 사용하는 스팸솔루션에 SPF 확인기능이 있어야 한다.

1) Mail Transfer Agent
2) Simple Mail Transfer Protocol
3) Sender Policy Framework

4.1 SpamAssassin

스팸어쌔신 버전 3.0이상에서는 SPF기능을 기본적(default)으로 지원해 주며 이를 사용하여 발신도메인의 메일정책(SPF) 확인 시 MTA/수신서버의 사용환경을 변경하지 않는 장점이 있다. 또한 각각의 SPF 판정결과를 자신의 도메인의 메일정책에 따라 선택적으로 스팸가중치를 부과할 수 있다. 하지만 SPF의 장점의 하나인 선택적 데이터 수신이 지원되지 않아 위조가 확실한 메일이라 하더라도 일단 모든 데이터를 수신한 뒤 처리하는 단점이 있다. 아래는 스팸어쌔신의 SPF 환경설정 파일이며 각 SPF 판정결과에 따른 스팸성 가중치 값이 나열되어 있다(굵게 표시된 폰트). 스팸어쌔신과 MTA(Sendmail, Postfix, Qmail 등)의 연동은 각 MTA에서 기본적으로 지원하는 메시지 필터 기능을 사용한다.

스팸어쌔신 SPF 환경설정(/usr/share/Spamassassin/50_scores.cf)
SPF # PATH /usr/share/spamassassin/ ifplugin Mail::SpamAssassin::Plugin::SPF **score SPF_PASS -0.001 # SPF** 통과 시 스팸성이 **0.001** 만큼 적어짐 . . endif # Mail::SpamAssassin::Plugin::SPF

〈표 4 스팸어쌔신 SPF 환경설정〉

4.2 MTA(Mail Transfer Agent)

위[4]에서 언급한 것처럼 SPF 기능을 사용하기 위해서는 milter 기능이 있는 Sendmail을 사용하여야 하며 Perl을 기반으로 Mark Kramer에 의해 개발된 spf-milter와 C를 기반으로 Jef Poskanzer에 의해 개발된 spfmilter가 있다. 기능적으로는 Perl 기반의 SPF

4) SPF 확인장치 설치

밀터가 보다 오랜 기간 동안 개발되어 다양한 기능을 제공한다. C 기반의 밀터는 libspf2 라이브러리를 사용하며 상대적으로 적은 기능을 제공하는 반면 상대적으로 안정적이며 속도가 빠른 장점이 있다.

- *Sendmail*
  - ▶ Perl based spf-milter

A. 밀터 설치에 앞서 설치하여야 할 펄 모듈 다운로드

POSIX
Sendmail::Milter
Socket
Net::CIDR
Mail::SPF::Query
Mail::SRS
Getopt
Errno

〈표 5 spf-milter Perl 모듈〉

B. Sendmail.mc 파일 편집 (다운로드 사이트 http://www.cpan.org/)

```
#다음의 내용을 Sendmail.mc 파일에 추가한다.
define(confMILTER_LOG_LEVEL', 9')dnl
define(confMILTER_MACROS_HELO', confMILTER_MACROS_HELO, {verify}')dnl
INPUT_MAIL_FILTER(spf-milter', S=local:/var/spf-milter/spf-milter.sock,
F=T,T=C:4m;S:4m;R:8m;E:10m')dnl
```

〈표 6 spf-milter 사용시 Semdmail.mc 편집〉

C. Sendmail.cf 파일 생성

Sendmail.cf 파일을 생성한다.

예) 〉 m4 〈 sendmail.mc 〉 sendmail.cf

D. spf-milter 시작

예) 〉 /usr/local/perl-threaded/bin/perl /usr/local/spf/sendmail-milter.pl milter

E. Sendmail 재 시작

예) /etc/init.d/Sendmail restart

▶ C based spfmilter

A. sendmail 이 밀터기능을 사용하도록 컴파일 되어있는지 확인한다

〉sendmail -d0.1 -bt 〈 /dev/null | grep MILTER

이때 "MILTER"스트링이 발견되면 밀터기능이 설치 되어있음

B. libspf2를 설치한다.

www.libspf2.org/download.html

libspf2-1.2.5.tar.gz를 위의 사이트에서 다운로드 후 일반적 설치 절차에 따라 설치함

예)./configure -enable-pthreads; make; make install

C. spfmilter 를 설치한다.

http://www.acme.com/software/spfmilter/

spfmilter-x.xx.tar.gz를 위의 사이트에서 다운로드 후 설치함

예)./configure; make; make install

D. sendmail.mc 파일을 편집한다.

아래의 내용 추가

```
INPUT_MAIL_FILTER(spfmilter', S=unix:/var/run/spfmilter.sock, T=S:8m;R:8m')
```

〈표 7 spf-milter 사용시 Semdmail.mc 설정〉

E. sendmail.cf를 생성.

예) 〉**m4 〈 sendmail.mc 〉 sendmail.cf**

F. SPF 레코드가 설정되지 않은 주요 사이트에 fallback 파일을 작성

/etc/mail/spfmilter-fallback 파일의 예

yahoo.* ptr:yahoo.com -all

.yahoo. ptr:yahoo.com -all

※ fallback파일은 SPF 레코드가 설정되어 있지 않은 야후 등의 주요사이트의 SPF레코드를 적용도메인에서 자신의 메일수신정책에 맞게 설정하는 옵션으로 발송서버의 주소가 명확한 경우 이를 사용하면 큰 효과를 얻을 수 있다.

G. SPF 레코드 확인이 필요치 않은 화이트 리스트를 작성

/etc/mail/spfmilter-whitelist 파일의 예

127.0.0.1 # 로컬 루프백 (local loopback interface)

192.168.64.0/24 # 내부 사설망

10.0.0.0/8

192.68.1.0-192.68.1.255

192.68.0.0/16

H. spfmilter를 실행

예) # spfmilter unix:/var/run/spfmilter.sock

I. sendmail을 재실행

예) /etc/init.d/sendmail restart

J. SPF 작동확인 후 부팅 시 자동실행 스크립트 작성한다.

SPF 작동시험을 한 뒤 이상이 없을 시 시스템에 따른 자동 시작스크립트를 작성한다.
이때 spfmilter는 반드시 sendmail 보다 먼저 실행되어야 한다.

4.3 P●stfix

A. 파일 설치

http://spf.pobox.com/download에서 smtpd-policy.pl 파일을 다운로드 받는다.
Sendmail Perl-based-filter에 필요한 모듈을 설치한다.
(Sendmail perl-based 참조)

B. Postfix 환경변수 설정

* /etc/postfix/master.cf 및 /etc/postfix/main.cf 편집

```
policy unix -   n       n       -       -       spawn
user=nobody argv=/usr/bin/perl /usr/libexec/postfix/smtpd-policy.pl
```

〈표 8 postfix master.cf 편집〉

```
smtpd_recipient_restrictions =
...#기존의 환경변수
reject_unknown_sender_domain
reject_unauth_destination
check_policy_service unix:private/policy
...#기존의 환경변수
```

〈표 9 postfix main.cf 편집〉

C. Postfix 재 시작

예) /etc/init.d/postfix restart

4.4 Qmail

A. 다운로드 qmail SPF 패치

http://spf.pobox.com/download에서 qmail 패치파일을 다운로드 받는다.

B. 설치

다운받은 패치파일을 설치한다.

예) > patch -p1 < /path/to/qmail-spf-<version>.patch

이때 <version>은 현재 설치하는 패치의 버전을 의미한다. 만약 버전이 1.02 라면 qmail-spf-1.02.patch 파일이 패치된다.

C. SPF 변수설정

/var/qmail/control에 위치한 환경변수를 설정한다.

• spfbehavior 변수

0: SPF확인 하지 않음 , SPF-Received 헤더 추가하지 않음 1: SPF-Received 헤더만 추가, 메일거부기능 사용하지 않음 2: DNS 참조에러발생시 Temperr 사용 3: "fail" 판정메일거부 4: "Softfail" 판정메일거부 5: "neutral" 판정메일거부 6: "pass"이외의 모든 판정값거부

<표 10 qmail SPF 환경설정>

4.5 MS Exchange

MS Exchange 서버 SPF 확인장치 설치는 GFI사의(www.gfi.com) MailEssential 10.1에 내장된 SPF모듈을 사용할 수 있다.

A. 시스템 사양조건

- Windows 2000/2003 Sever 혹은 Advanced/Enterprise Server
- Microsoft Exchange 2000/2003

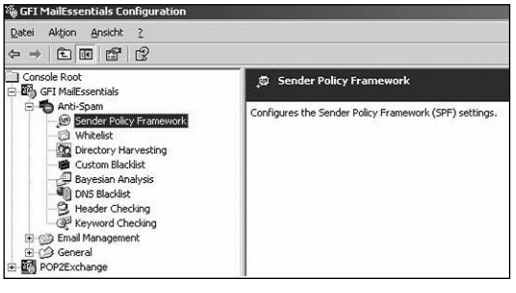
B. 설치

- GFI MailEssentials를 Exchange Server 2000/2003이 동작하는 컴퓨터에 설치한다

〈그림 6 GFI 설치 1〉

C. SPF설정

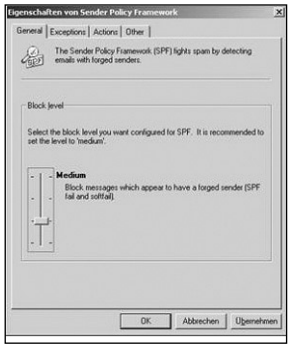
- GFI MailEssentials을 시작한다
- Configuration메뉴의 "Sender Policy Framework"을 마우스 오른쪽 버튼으로 클릭한다



〈그림 7 GFI 설치 2〉

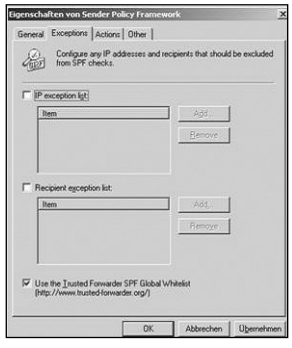
- 위의 과정에서 열린 메뉴 중 "Properties"를 선택한다.

• Never, Low Medium High중 자신의 도메인정책에 상응하는 옵션을 선택한다.



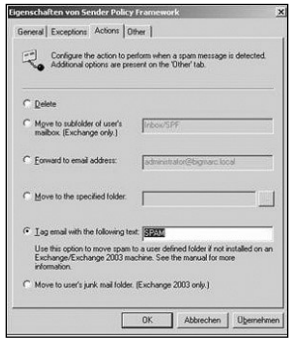
〈그림 8 GFI 설치 3〉

• 화이트 리스트 작성



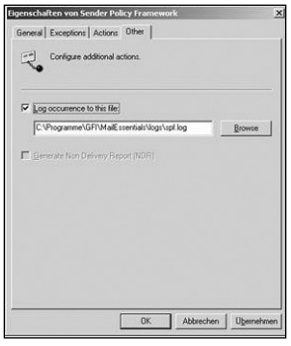
〈그림 9 GFI 설치 4〉

• 스팸판정메일 처리방법 설정



〈그림 10 GFI 설치 5〉

• SPF로그기능 설정



〈그림 11 GFI 설치 6〉

5. 맺음말

SPF는 기존 SMTP기반의 취약한 메일인증구조를 보완하는 SMTP 프로토콜의 확장판으로 책임 있는 메일발송 환경을 만들기 위한 기술적인 대안이다. SPF는 다른 인증기술들과 비교하여 기술적으로 완성도가 높고 많은 변수가 작용하는 인터넷 메일환경을 최대한 수용하도록 설계되어있다. 이 기술문서는 SPF의 보급을 원활하게 하기 위해 작성되었으며 많은 메일환경 중 대표적인 몇몇 환경을 선택하여 작성되었다. 이 문서에 기술되지 않은 환경에 설정 시 SPF공식 사이트인 spf.pobox.com 및 참고문헌에 소개된 자료를 참조하면 많은 자료를 얻을 수 있다.

2006 스팸메일 차단 솔루션 활용 가이드

- 스팸메일, 줄이는 것이 경쟁력 -

2005년 12월 인쇄

2005년 12월 발행

발 행 인 이 홍 섭

발 행 처 **한국정보보호진흥원**

138-803 서울시 송파구 가락동 78번지

TEL:(02)4055-114 FAX:(02)4055-619

URL http://www.kisa.or.kr

인 쇄 처 호정씨앤피(Tel 02-2277-4718)

〈 비 매 품 〉