SPF 기술 설명서

2005. 9.

인터넷침해사고대응지원센터
스팸대응팀

SPF[1] 소개

이메일 헤더는 여러 가지 방법으로 위조될 수 있으나 현재의 SMTP[2]는 반송경로(reverse path) 혹은 전송된 SMTP 명령어에 대하여 아무런 확인을 하지 않고 있다. 이 문서는 SPF 프로토콜 버전1에 대하여 기술하고 있으며 이를 이용하여 각 도메인의 관리자가 자신의 도메인의 적법한 메일발송 호스트를 인가하는 방법과, 메일 수신서버(MTA[3])가 해당도메인의 적법한 메일 발송 호스트를 확인하는 방법을 기술한다.

SPF 설치 및 운영

MAIL FROM 발신자 정보

HELO Identity는SMTP의MAIL FROM 명령어(RFC2821) 에서 유래한다. 이 명령어는 반송경로(reverse path)를 표기하는데 사용된다. RFC2821은 반송경로(reverse path)표기를 의무화 하지 않으므로, 수신서버는 반송경로(reverse path)가 표기되지 않은 메일의 메일박스 주소를 “postmaster”나 “HELO” 발신지 정보를 사용한다. SPF 사용 메일서버(MTA)는 반드시 “MAIL FROM” 혹은 “HELO” 발신자 정보를 사용하여 메일 발신자 확인 정보로 사용하여야 한다.

SPF 레코드 출판

SPF를 사용하는 도메인은 반드시 적법한(오류가 없는) SPF레코드를 출판하여야 하며 발송하지 않는 도메인은 이를 명시하는 레코드를 다음과 같이 “v=spf1 –all” 출판하여야 한다. SPF 사용 중 메일발송 환경에 변화가 생겨 이를 변경하여야 할 경우 이변화를 수용하기 위한 기간이 필요하며 이 기간 중 기존의 레코드와 새롭게 작성된 것 중 어느 것을 사용하는 메일도 수용할 수 있는 레코드를 출판 하여야 한다.

SPF 사용시 정의된 발신자정보	
<IP>	메일발송 시 사용된 SMTP 발송MTU의IP 주소
<domain>	MAIL FROM 혹은 HELO에서 입력된 도메인 정보
<sender>	MAIL FROM 혹은 HELO 입력정보

<표1 SPF 발신자 정보>

수신 메일의 SPF 레코드 확인

이메일 수신 측은 자신의 도메인에 도착한 각각의 메일이 적법한 발송도메인의 발송서버를 통해 발송되었는지 여부를 확인한다. 이는 메일수신부의 MTA혹은 이에 상응하는 어떤 장치(스팸솔루션 등)를 통해서도 확인될 수 있다. 이때 SPF값의 판정여부는 다른 스팸솔루션들과 함께 탄력적으로 사용될 수 있다.

결과값의 해석

SMTP 데이터 전송이 끝난 뒤에는 헤더에서 정확한 발신자 정보를 추출할 수 없으며 또한 발송 중 발생한

[1] Sender Policy Framework
[2] Simple Mail Transfer Protocol
[3] Mail Transfer Agent

에러 값을 발송서버에 직접 리턴 하기 위해서도 SPF확인과정은 반드시 SMTP 데이터전송 중에 이루어 져야 한다. SPF에서 위조가 확실한 메일로 판정 시(fail) 이에 대한 반송메일 전송은 위조메일 발신자에 의한 이메일 자원남용 가능성이 있으므로 위조된 메일에 대한 반송메일은 발송되지 말아야 한다.

- None
  발신 도메인이 SPF 레코드를 설치하지 않았거나 제공된 발신자 정보에서 해당 도메인 정보를 구할 수 없음. SPF 확인 장치가 메일의 위조여부를 판정할 수 없음을 나타낸다.

- Neutral
  메일 발신 도메인에서 자신의 도메인에서 발송되었다고 하는 메일에 대하여 위조여부를 판단하기를 원하지 않음을 나타낸다. “Neutral”로 판정된 메일의 처리는 “None” 판정메일과 동일하게 취급되며 이 옵션은 SPF 시험운영 등의 과정에 사용된다.

- Pass
  “Pass” 판정값은 메일 헤더가 위·변조 되지 않았으며(제공된 identity가 발신자와 일치함)발신자가 메일에 대해 책임을 가진 도메인임을 나타낸다. 효과적인 스팸차단을 위해서는 발송된 메일의 내용(스팸, 비스팸)분류를 통해 발송도메인의 신용도 확인을 병행하여야 한다

- Fail
  “Fail” 판정값은 메일 헤더가 위·변조 되었음을 나타내며 해당 메일을 발송한 MTU는 자신이 지칭하는 도메인을 사용하도록 허가되어 있지 않음을 나타낸다. 수신 MTU는 “Fail” 판정 메일의 수신을 거부하거나(SMTP reply code 550) 메일헤더에 “fail” 판정 값을 표기할 수 있다.

- Softfail
  “Softfail” 판정값은 “fail” 과 “neutral”의 중간 정도의 값을 나타내며 이는 메일헤더가 위·변조 되었으나 자신의 도메인이 메일포워딩 등의 서비스를 통해 적법하게 위조 될 수 있음을 나타내며 이는 “fail” 정책으로 전환하기 위한 과도기에 사용될 수 있다.

- TempError
  “TempError” 판정값은 메일 수신 서버에서 SPF 결과값 확인 시 문제가 발생하였음을 나타내며 이는 이 메일에 대한 수신여부는 내부 정책에 의해 결정되어 진다.

- PermError
  “PermError” 결과값은 메일 발송 도메인에 출판된 SPF레코드 값이 발송 메일에 있는 “Mail From” 발신자 정보를 확인하는데 사용될 수 없음을 나타낸다. 이러한 경우 수신서버는 이메일을 550 replay 코드를 사용하여 거부하여야 한다.

결과값의 표기

메일 송신 MTA는SPF 판정결과를 메시지 헤더에 ‘Received-SPF’ 키워드를 사용하여 Received 키워드 상단에 SPF 확인에 대한 판정 값을 기록하여야 한다.

SPF 판정값 예

Received-SPF: **pass** (mybox.example.org: domain of myname@example.com designates 192.0.2.1 as permitted sender); receiver=mybox.example.org; client_ip=192.0.2.1; envelope-from=myname@example.com;

Received-SPF: **fail** (mybox.example.org: domain of myname@example.com does not designate 192.0.2.1 as permitted sender)

Received-SPF: **softfail** (mybox.example.org: domain of transitioning myname@example.com does not designate 192.0.2.1 as permitted sender)

Received-SPF: **neutral** (mybox.example.org: 192.0.2.1 is neither permitted nor denied by domain of myname@example.com)

Received-SPF: **none** (mybox.example.org: myname@example.com does not designated permitted sender hosts)

Received-SPF: **unknown** -extension:foo (mybox.example.org: domain of myname@example.com uses mechanism not recognized by this client)

Received-SPF: **error** (mybox.example.org: error in processing during lookup of myname@example.com: DNS timeout)

SPF 레코드

SPF 레코드는 해당 도메인의 도메인 명을 Mail From: 발신자 정보로 사용하도록 인가된 호스트를 정의한다. 이 정보를 이용하여 한 도메인에서 메일발송이 허가된 호스트와 그렇지 않은 호스트를 구별한다. SPF레코드는 한 줄의 텍스트로 구성되어 있다.

SPF 레코드 예

v=spf1 +mx +a:colo.example.com/28 -all

이 레코드는 사용중인 SPF 버전 명을 나타내는 **v=spf1, +mx, +a:colo.example.com/28** 그리고 **-all** 디렉티브로 구성되어있다. **v** 는 SPF 버전명, **mx** 는 수신서버, 그리고 **a** 는 DNS의 A 레코드를 나타내며 all 은 앞에 기술된 세 개의 디렉티브로 명시된 발송서버 이외의 모든 경우를 나타낸다.

위의 SPF 레코드로 정의된 도메인은

① **mx**: -> DNS 에 명시된 메일수신 서버와

② **a:colo.example.com/28 -> colo.example.com/28** 대역대의 모든 서버

에서 발송된 메일은 적법하며 이외의 모든 all 곳에서 발송된 메일은 부적합 하다고 선언함. 여기서 "+" 는 허가 "-"는 불가를 나타내며 이의 생략 시 "+" 기호가 선행하는 것으로 간주한다.

SPF 레코드 출판

해당 도메인의 SPF레코드는 DNS(네임서버)에 저장된다. 위의 예시 레코드는 다음과 같은 방법으로 도메인의 네임서버에 출판된다.

```
example.com. IN TXT “v=spf1 +mx +a:colo.example.com/28 -all”
```

SPF 레코드는 새롭게 정의된 SPF 레코드 타입으로 정의되거나 기존의 TXT 레코드타입에 정의 될 수 있다. SPF를 출판하는 도메인은 이 두 레코드를 모두 출판하거나 최소한 둘 중 하나의 레코드를 이용하여 SPF를 출판하여야 한다. 이때 발송정책을 명시하는 도메인은 한 개 이상의 레코드를 동시에 출판하여서는 안되며 한 레코드에 대한 추가사항은 _spf 서브도메인을 사용하여 나타낼 수 있다. SPF 레코드는 하나의 UPD 패킷으로 전송될 수 있도록 480byte 이내이어야 하며 레코드 출판 시 와일드카드(*) 사용은 오류의 원인이 됨으로 사용하지 말아야 한다.

SPF 레코드 확인과정

SPF 레코드는 메일 수신 측에서 check_host() 함수를 호출하여 레코드의 적법성 여부를 확인한다. 이때 check_host() 함수는 SPF 레코드를 해당도메인에서 전송 받은 뒤 전송된 스트링을 분석(Parsing)하여 발송된 메일의 발송정책을 확인한다. 이 과정은 수신된 메일이 적법한 발송 서버를 통하여 발송되었는가의 여부와 이에 따르는 발신자 도메인의 정책을 확인 하여 이를 적용하는 과정으로 나누어진다. check_host() 함수의 내부작동 알고리즘은 아래와 같다.

- check_host() 함수는 내부적으로 세 개의 값을 전달 받으며 이 값들은 다음과 같이 정의 되어있다

전달값 (argument)	내 용
<IP>	메일 발송호스트의 IP 주소
<domain>	메일 발송호스트의 도메인 명
<sender>	메일발송자의 메일주소(test@domain.com의 형식)

<표2 check_host() 함수값>

- check_host() 함수 결과값

결과값	코드	내용
Neutral	(?)	출판된 데이터에 근거해 판단을 내릴 수 없음
Pass	(+)	<IP>가 인가되어진 발송서버로 확인됨
Fail	(-)	<IP>가 인가되어지지 않은 발송서버로 확인됨
Softfail	(~)	<IP>는 인가되지 않은 발송서버이나 “Fail” 정책의 적용은 유보함.
TempError		DNS(네임서버) 참조 시 회복 가능한 에러발생
PermError		DNS(네임서버) 참조 시 회복 불가능한 에러발생

<표3 check_host() 함수 결과값>

■ SPF 확인 결과값이 “Fail” 일 경우 이에 대한 이유가 다음 세가지중 하나로 리턴 된다.

1. Not Permitted + [허가되지 않은 이유](허가되지 않음)
2. Malformed Domain(도메인명 오류)
3. Domain Does Not Exist(존재하지 않는 도메인)

check_host() 실행과정

1. 초기 처리과정

   만약 <domain> 값에 오류가 있을 경우(not fully quantified domain name) check_host()는 “fail” 값을 “Malformed Domain” 이유와 함께 리턴한다. 이때 <sender>값이 존재하지 않으면 이는 “postmaster” 값으로 처리된다.

2. DNS 참조 과정

   <domain>의 SPF RR TXT, RR SPF 혹은 두 개의 레코드 값을 로컬 캐시 혹은 해당 도메인 서버에서 구한 뒤 해당 도메인이 존재하지 않을 경우 “fail” 값을 “domain Does Not Exist” 이유와 함께 리턴 한다. 이때 네임서버 장애에러가 발생하면(DNS Server Lookup Failure) check_host() 함수는 “TempError”를 리턴하며 종료 된다.

3. 레코드 선정 과정

   과정2에서 얻어진 레코드 값 중SPF 레코드 타입이 존재 시, TXT 레코드 타입을 이용하여 정의된 값은 처리되지 않는다. 또한 레코드 헤더가 “v=spf1”으로 시작되지 않는 레코드 역시 처리되지 않는다. 과정3을 통해 하나의 레코드만이 레코드 확인과정을 위해 선정되며 이때 아무런 레코드가 남아있지 않는 경우 check_host() 함수는 “None” 을 최종 결과값으로 리턴하며 종료된다. 이때 한 개 이상의 레코드가 남아 있을 시check_host() 함수는 “PermError”을 최종 결과값으로 리턴하며 종료된다.

4. 레코드 확인 과정

   과정3을 통해 하나의 SPF 레코드가 선정된 후check_host() 함수는 레코드의 문법적 오류(Syntax Error)를 확인하며 오류 확인 시 “PermError”를 리턴하며 종료된다.

5. 레코드값 판정과정

   SPF 레코드는 메커니즘(mechanism)과 변형자(modifier)로 구성되며 주어진 메커니즘은 하나의 레코드에 중복되어 나타날 수 있으며 알려지지 않은 메커니즘 사용시 “PermError”값을 리턴하며 종료된다. 하지만 주어진 변형자는 하나의 레코드에 한번만 사용되며 알려지지 않은 변형자는 처리되지 않는다. SPF 레코드에 대한 최종 결과값은 메커니즘과 변형자의 값과 check_host()함수 전달값의 처리를 통해 하나의 결과값으로 구하여 진다. SPF값 판정 시SPF 레코드에 명시된 어느 메커니즘에도 해당하지 않고 “redirect” 변형자 값이 설정되어 있지 않을 시check_host()는 “neutral”을 결과값으로 리턴한다. “redirect” 변형자 값이 설정되어있을 경우에는 Redirected Query를 시행한다.

SPF 레코드 정의어

메커니즘(mechanism)

SPF레코드에서 도메인은 메커니즘을 통해 정의되는데 이 때 메커니즘은 하나도 사용되지 않거나 다수의 메커니즘이 함께 사용될 수 있다. 메커니즘은 적법한 메일발송 호스트를 명시하거나 다른 메일 정책들을 명시하는데 사용된다.

■ prefixes

“+ ”	Pass
“–“	Fail
“~”	SoftFail
“?”	Neutral

<표4 SPF prefix>

■ all (all)

all 메커니즘은 모든 경우에 해당되며 항상 모든 레코드의 마지막에 위치한다.

“v=spf1 -all”

해당 도메인은 메일을 발송하지 않음을 명시함.

■ a (a, a:domain, a:domain/cidr-length, a/cidr-length)

해당 도메인의 모든a레코드 중 하나가 발송 호스트의 IP와 일치 하도록 할 때 이 메커니즘이 적용된다. 도메인 명이 명시되지 않은 경우 현재의 도메인이 사용된다.

“v=spf1 a -all”

현 도메인 명이 사용되며 도메인의 A 레코드가 발송 호스트의 IP와 동일한 서버만 메일을 발송하며 그 이외의 어떤 호스트에서도 메일을 발송하지 않음.

“v=spf1 a:example.com -all”

발송호스트의 IP가example.com의 A 레코드와 동일한 서버만 메일을 발송하며 그 이외의 어떤 호스트에서도 메일을 발송하지 않음.

“v=spf1 a:mailer.example.com -all”

발송호스트의 IP가 mailer.example.com의 A 레코드와 동일한 서버만 메일을 발송하며 그 이외의 어떤 호스트에서도 메일을 발송하지 않음.

.

■ mx (mx, mx:domain, mx:domain/cidr-length, mx/cidr-length)

해당도메인의 모든 mx 레코드의 A 레코드 중 하나가 발송호스트의 IP와 일치 하도록 할 때 이 메커니즘이 적용된다. 도메인이 명시되어 있지 않을 때 현재 도메인 명이 사용된다.

“v=spf1 mx mx:deferrals.example.com -all”

발송호스트 IP가 발송도메인의 mx 레코드 중 하나의 IP와 일치하거나 deferrals.domain.com의

mx 레코드 중 하나의 IP와 동일한 서버만 메일을 발송하며 그 이외의 어떤 호스트에서도 메일을 발송하지 않음.

“v=spf1 mx/24 mx:offsite.domain.com/24 -all”

발송호스트의 IP가 발송도메인의 mx 레코드 의 C-클래스 네트워크 주소중의 하나가 발송지의 IP와 일치하거나 외부도메인(offsite.domain.com)의 mx 레코드의 C-클래스 주소중의 하나가 발송호스트의 IP와 동일한 서버만 메일을 발송하며 그 이외의 어떤 호스트에서도 메일을 발송하지 않음.

■ ptr(ptr, ptr:domain)

발송 호스트의 PTR 쿼리를 통해 얻어진 호스트 명의 A레코드가 발송 IP와 일치 할 때 이 메커니즘이 적용된다. 도메인이 명시되어 있지 않을 때 현재 도메인 명이 사용된다.

“v=spf1 ptr -all”

발송호스트의 IP의 ptr 쿼리가 현재 도메인 이름과 일치하는 호스트만 메일을 발송하며 그 이외의 어떤 호스트에서도 메일을 발송하지 않음.

“v=spf1 ptr:otherdomain.com -all”

발송호스트의 IP의 ptr 쿼리가 “otherdomain.com”과 일치할 경우 메일발송을 허가하며 그 이외의 어떤 호스트에서도 메일을 발송하지 않음.

■ ip4

발송호스트의 IP를CIDR로 정의된 네트워크의 IP 범위 내에 위치시킬 때 이 메커니즘이 적용된다. CIDR의 범위를 한정하는 “/xx” 이 명시되지 않을 경우에 이는 /32가 생략된 것으로 정의된다.

“v=spf1 ip4:192.168.0.1/16 -all”

발송호스트의 IP가 192.168.0.1/16 범위에 있는 호스트만 메일을 발송하며 그 이외의 어떤 호스트에서도 메일을 발송하지 않음.

■ ip6

IPv6의 발송대역을 정의

■ exists

exit로 정의된 도메인에 대해 쿼리를 실시한 뒤 이에 대한 A레코드가 리턴 된 경우에 적용 되도록 할 때 이 메커니즘이 사용된다. 이 메커니즘은 매크로와 함께 쓰여져 블랙리스트/화이트리스트를 이용한 스팸차단 기법에 응용될 수 있다.

“v=spf1 exist:example.net –all”

example.net의 A레코드가 존재할 때 발송된 메일을 적법하게 취급되어야 함

■ include

발송호스트의 IP가 해당도메인의 외부에 위치할 때include를 사용하여 외부 발송도메인을 정의함. 만일 정의된 도메인이 적법한 레코드를 사용하고 있지 않을 시에는 “PermError”를 결과값으로 리턴함.

“v=spf1 include:example.net -all”

example.net.의 SPF레코드를 검색하여 SPF레코드가 출판되어있지 않을 시에는 “PermError”를 리턴함

변형자(modifier)

변형자는 옵션으로 사용되며 하나의 SPF 레코드(directive set)에 한번만 사용될 수 있다. 정의되지 않은 변형자는 처리되지 않고 생략 된다.

■ redirect

리디랙트(redirect)는 SPF 레코드를 명시된 값으로 대치한다.

“v=spf1 redirect=example.net”

example.net의SPF레코드를 사용하여 결과값을 판정하고 해당도메인에 SPF레코드가 정의되어 있지 않을 시unknown값을 리턴한다. 이때 단순하지 않은 리디렉트(redirect) 도메인을 명기할 경우 SPF에서 제공하는 매크로기능을 이용할 수 있다.

■ exp

SMTP 수신자가 SPF 판정 값에 따라 메시지를 거부할 경우 메시지 거부이유를 명시하는데 사용된다. 위의 경우와 같이 다양한 내용의 설명문이 SPF에서 제공하는 매크로 기능을 이용하여 정의될 수 있다.

“v=spf1 mx –all exp=explain._spf.%{d}”

발송도메인의 메일수신서버의 IP와 일치하는 호스트만 메일을 발송할 수 있으며 그 이외의 어떤 호스트에서 발송된 메일 수신 시 메일 수신을 거부하며 explain.spf.<domainname> 에 명시된 안내문을 리턴한다.

마크로

많은 메커니즘과 변형자는 마크로 확장을 사용하여 간결하게 표현될 수 있다.

마크로	설 명
s	<sender>
l	local-part of <sender>
o	Domain of <sender>
d	<domain>
i	<ip>
t	Current time stamp
p	The validated domain name of <ip>
v	The string “in-addr”
h	HELO/EHLO domain
c	SMTP client IP
r	Domain name of host performing the check

<표5 SPF 마크로>

서비스 별SPF 설치요건

SPF를 성공적으로 설치 운영하기 위해서는 이메일발송에 관련된 발송, 메일링리스트, 포워딩서비스 도메인이 아래에 기술된 적절한 조치를 취하여야 한다.

메일발송 도메인

SPF를 설치하고자 하는 도메인은 우선 메일발송 호스트의 리스트를 작성하여야 한다. 기술적으로 이러한 리스트를 작성하는 것은 쉽게 이루어질 수 있으나 자신의 도메인의 메일정책을 수립하는 과정에서는 기술적인 요인뿐 아니라 관리자적인 요인도 함께 고려되어야 한다.

메일링리스트

메일링리스트 운영자는 메일 발송 시 반송주소가 어떻게 표기되는지를 확인하여 반송주소의 표기가 [RFC1123] 섹션5.3.6에 명시된 것과 같이 메일의 반송주소는 발송의뢰인의 주소가 아닌 실재 발송자의 주소로 표기하여야 한다.

메일포워딩 서비스

메일포워딩 서비스는 자신의 도메인에 전송된 메일을 외부의 도메인으로 재 전송함을 말한다. 일반적 메일포워딩 서비스는 메일 재전송 시 반송주소를 자신의 도메인이 아닌 전송 의뢰인의 주소로 표기하는데 이는 SPF의 적법성검사에서 "fail" 판정을 받게 된다. 이러한 문제점을 해결하기 위해 아래와 같은 세 가지의 순차적인 방법을 적용할 수 있다.

A. 포워딩메일 전송도메인

① 포워딩 도메인에 RBL[4]를 사용하여 'fail"대신 "neutral" 결과값 제공

예) "v=spf1 mx –exists:%{ir}.sbl.spamhaus.example.org ?all"

② MAIL FROM 발신자 정보에 대한 추가적인 확인

예) "v=spf1 mx exists:%{l}._spf_verify.%{d} -all"

③ 특화된 도메인 서버를 이용한 발송 건수 제한

예) "v=spf1 mx exists:%{ir}._spf_rate.%{d} -all"

④ 개별 사용자 별 정책 수립 및 적용

예) "v=spf1 mx redirect=%{l1r+}._at_.%{o}._spf.%d{d}"

B. 포워딩 도메인

① 메일을 포워딩하는 도메인은 MAIL FROM[5] 발신자 정보에 자신의 도메인 정보를 제공

C. 포워딩메일 수신도메인

① 확인되어진 포워딩 서비스 도메인에 대하여 SPF 확인을 면제한다

② HELO 발신자 정보를 이용하여 SPF검사를 시행한다

③ 포워딩 서비스를 주로 이용하는 대형 도메인일 경우 화이트 리스트를 이용한다.

메일발송대행업체

타 도메인의 메일발송을 대행하고 있는 경우 MAIL FROM 발신자정보를 자신의 도메인 명을 사용하고 적절한 SPF레코드를 출판한다. MAIL FROM 발신자정보를 사용하지 않을 경우 제공된 메커니즘과 변형자를 사용하여 적절한 SPF레코드를 작성한다.

SPF에 관련된 보안사항

다른 많은 인터넷프로토콜과 같이 SPF역시 악성 사용자들에 의해 오·남용 될 수 있다. 이러한 공격의 결과는 대부분 시스템자원을 소진시켜 정상적인 서비스를 수행할 수 없게 만드는 DoS 공격으로 귀착된다. 이러한 공격의 유형에는

- 공격대상의 도메인을 참조하는 악성 SPF레코드를 출판하여 공격대상 도메인에 대한 DoS공격.
- 공격대상 도메인에 대하여 다량의 DNS 참조를 시행하는 악성 SPF 레코드를 출판하여

[4] Realtime Blocking List: IP를 기준으로 메일접속을 차단하는 리스트
[5] SMTP 반송메일주소 입력명령어

공격대상 도메인의 CPU, 메모리 사용량을 증가시키는 DoS[6]공격.

- 공격대상 도메인에 대하여 출발지를 달리하는 다량의 메일을 발송하여 해당도메인의 DNS 서버의 무력화를 시도하는 공격이 있을 수 있다.

이러한 다양한 공격의 유형에 대응하기 위해 대부분의 SPF 모듈은 DNS 룩업을 "include", "redirect"를 포함하여 메일 하나당 최대 10개 까지만 질의 하도록 설정되어 있다. 만약 질의가 정하여진 한계를 넘으면 "PermError" 에러코드를 리턴 하도록 되어있다. SPF의 디렉티브 중 "all", "ipv4" 그리고 "ipv6" 는DNS 룩업을 요하지 않는다. DNS 부하를 최소화 하는 SPF 레코드를 출판하기 위해서는 레코드 설정 시 신중한 고려가 필요하다. 예를 들어 다음과 같은 경우에

example.com.	IN MX	10 mx.example.com
mx.example.com.	IN A	192.0.2.1
a.example.com.	IN TXT	"v=spf1 mx:example.com –all"
b.example.com	IN TXT	"v=spf1 a:mx.example.com –all"
c.example.com	IN TXT	"v=spf1 ip4:192.0.2.1 –all"

<표6 SPF 레코드 예>

a. a.example.com의 SPF 레코드 처리시
   - example.com의 mx 레코드를 구하여야 하며
   - 각각의 mx 서버에 대하여 A레코드를 구하기 위해 여러 번의 룩업이 필요함

b. b.example.com의 SPF 레코드 처리시
   - mx.example.com의 A레코드를 구하기 위한 한번의 룩업이 필요하다

c. c.example.com의 SPF 레코드 처리시
   - 레코드 처리를 위한 DNS 질의가 필요치 않다

메일 발송서버의 IP의 변동이 많아 효율적인 서버관리를 위해서 불가피하게 "a" 혹은 "mx" 레코드가 사용되어야 하는 경우를 제외하고는 질의수가 최소화된 SPF레코드를 출판함이 바람직하다.

맺음말

SPF의 구현(implementation)은 기본적으로 SPF RFC에 의거하여 이루어졌으나 각각의 프로그램에 약간의 차이가 있다. 예를 들어 2005년 9월 현재 Meng Weng Wong이 작성한 perl을 기반으로 한 spf 확인모듈이 가장 많은 기능을 제공하고 있으며 Jef Poskanzer의 C 기반의 spfmilter는 보다 안정적인 실행환경을 제공한다. 위의 두 개의 예 이외에도 다른 많은 프로그램들이 있으며 각각의 장 단점이 존재한다. 사용자는 자신에 환경에 가장 적합한 프로그램을 선택하여 사용할 때 최적의 효과를 얻을 수 있다.

[6] Denial of Service 공격

참고문헌

- M. Wong and W. Schlitt “SPF Draft-schlitt-spf-classic-02”IETF RFC[pending], June 2005
- Paul Albitz & Cricket Liu “DNS and BIND” 3rd Ed O’reilly & Association, September 1998
- Meng Weng Wong “SPF: Sender Policy Framework” http://spf.pobox.com, August 2005