情 報 保 護 學 會 誌
第 11 券 第 6 號, 2001. 12

IETF에서의 인터넷 보안기술 표준화 추세와 동향

이 광 수*

요 약

인터넷 보안기술 관련 프로토콜의 제정과 표준화 작업의 거의 대부분은 IETF에 의해 수행되고 있다. 여기서는 IETF의 조직 구성과 작업 방식, 문서 발간 절차 등을 알아보고, IETF에서 표준화가 진행되고 있는 보안기술 분야와 그 작업 동향을 조사·분석한다. 그리고, IETF의 전반적인 작업에서 보안이 갖는 의미를 살펴보며, 향후 인터넷 보안의 발전 방향을 가늠해 본다.

Ⅰ. 서 론

인터넷 제품들 사이의 상호운용을 위해서는 제품들 사이의 통신을 프로토콜로 규정하고, 또한 이들 프로토콜을 표준화하는 것이 필수적이다. 인터넷 관련 프로토콜의 제정과 표준화에는 웹과 관련된 월드와이드웹 컨소시엄(W3C[1]), 무선 인터넷과 관련된 WAP 포럼[2] 등도 있지만 거의 대부분의 인터넷에 관련된 프로토콜의 개발 작업은 IETF[3](Internet Engineering Task Force)가 수행해 오고 있으며, 인터넷 보안기술에 대한 표준화도 예외는 아니다.

IETF의 인터넷 보안기술에 관한 표준은 주로 보안 영역 산하의 작업반에서 이루어지고 있으며, 네트워크 계층에서의 보안 서비스 제공, 공개키 기반 구조, 전송 계층 보안, 인증 프로토콜 등과 함께 응용 계층에 보안 기능을 제공하기 위한 전자우편 보안, XML 디지털 서명, 침입탐지시스템 메시지 교환, 보안 셸, 안전한 syslog 등의 작업이 진행되어 오고 있다. 그리고, 보안 영역 밖의 작업반에서도 보안과 밀접한 관련을 갖는 프로토콜을 개발하거나 보안이 해당 프로토콜의 중요한 요소인 경우도 많이 있으며, IETF는 근래에 개발되는 모든 프로토콜에서 보안 문제를 고려하도록 규정하고 있다.

본 논문의 남은 부분은 다음과 같이 구성된다. 2절에서는 IETF의 구성과 IETF 문서에 대해 소개한다. 3절에서는 IETF 보안 영역의 작업반 현황과 활동 상황을 살펴보며, 작업반 예비 단계인 BOF 활동들도 함께 알아본다. 4절에서는 IETF 보안 영역 밖에서 이루어지는 보안 관련 활동을 알아보며, 5절에서 결론을 제시한다.

Ⅱ. IETF의 구성과 IETF 문서

여기서는 먼저 IETF를 구성하는 세부 조직들을 살펴보고, 다음에 IETF에서의 표준 문서의 종류와 발간 절차를 알아본다.

1. IETF 조직 구성

1960년대 후반 태동된 인터넷을 위한 프로토콜 표준화를 보다 체계적으로 수행하기 위해 1986년 ISOC[4](Internet Society)에 의해 조직된 기구가 IETF이며, IETF는 회원·비회원의 구분이 없는 개방형 국제기구이다. IETF에는 네트워크 설계자, 운영자, 관련 업체 및 연구원 등의 다양한 인력들이 인터넷 구조의 발전과 순조로운 운영을 위해 활동하고 있다.

IETF의 실제 기술적 작업은 작업반(Working Group)들에서 수행되는데, 이들 작업반은 연관성에 따라 영역으로 묶여 영역 의장단에 의해 관리된다. 2001년 11월 말 현재 IETF에는 표 1에서 보이는 바와 같이 8개 영역에 133개의 작업반이 편재

* 숙명여대 정보과학부 교수 (rhee@sookmyung.ac.kr)
본 연구는 숙명여자대학교 2001년도 교내연구비 지원에 의해 수행되었음

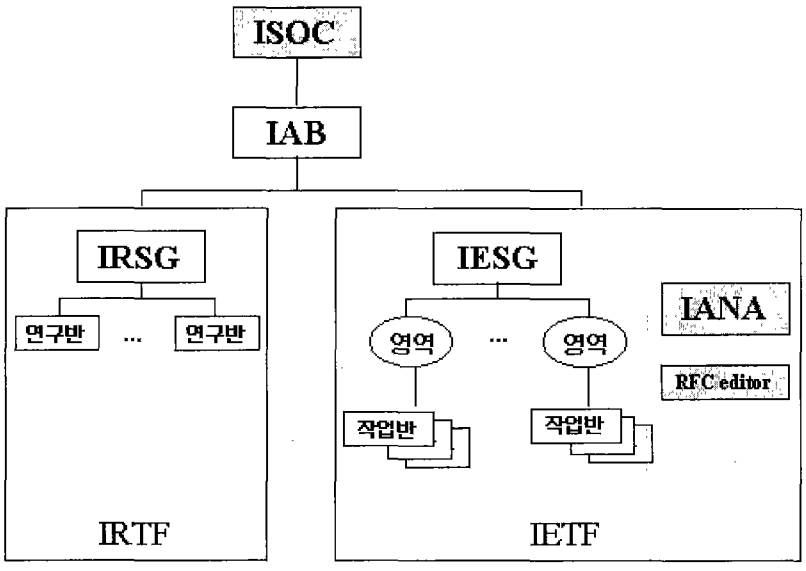
〔표 1〕 IETF 영역 현황

영역	작업반 수
Applications	29
Internet	16
Operations and Management	23
Routing	13
Security	19
Sub-IP	7
Transport	24
User Services	2

되어 있다. 각 작업반에는 한 두 명의 의장이 있으며, 작업반의 임무와 작업 범위를 나타내는 헌장을 갖는다. 작업의 많은 부분은 메일링 리스트를 통해 이루어지며, 연 3회의 총회에서 작업반별 토의를 갖는다. 작업반의 구성을 위해서는 먼저 예비 단계로 총회에서 BOF(Birds-Of-a-Feather)를 열어 많은 사람들이 관심을 갖고 참여할 수 있는지 조사하게 된다. 규정상 BOF는 1-2 회로 제한되어 있으며, 그 안에 많은 사람들의 참여를 구하지 못하면 소멸되도록 되어 있지만, 가끔 3번의 BOF를 갖는 경우도 있다. 여러 해 동안 활동이 없는 작업반은 소멸된다.

IETF 영역 의장들의 모임을 IESG(Internet Engineering Steering Group)라고 하며, 각종 IETF 활동과 표준화 절차를 관장하며, 특히 작업반에서 제출된 표준 문서의 최종 승인을 담당한다. 표준화 작업을 담당하는 IETF에 병행하여, 미래의 인터넷 발전을 위한 장기적인 연구 과제를 수행하는 연구반들로 구성되는 IRTF[5](Internet Research Task Force)라는 조직이 있으며, 현재 멀티캐스트 보안과 인증/인가/회계 등의 2개의 보안 관련 연구반을 포함하여 12개의 연구반이 활동하고 있으며, 이들 연구반 의장들의 모임은 IRSG (Internet Research Steering Group)라고 불린다. IETF 프로토콜들에서 사용되는 숫자들을 고유하게 지정하는 것은 IANA[6](Internet Assigned Numbers Authority)에서 담당한다. IAB[7](Internet Architecture Board)는 인터넷의 전반적인 구조에 영향을 미치는 문제들을 토의하며, IETF나 IRTF의 그룹들의 구성이나 영역 지정, IESG의 결정에 대한 이의 처리 등의 역할을 수행한다.

좁은 범위의 IETF는 IESG와 그 산하의 작업반, IANA 등 실제 표준화 작업 수행 기구들을 가리키며, 넓은 의미의 IETF는 IAB, IRTF 등을 포함한다. 그림 1은 전체 IETF 조직 구성을 나타낸다.



〔그림 1〕 IETF 구성

2. IETF 문서

IETF 문서는 크게 정식 문서인 RFC(Request For Comments)와 임시 문서인 I-D(Internet Draft)로 나누어진다. RFC 문서의 내용과 형식에 관한 규정은 RFC 2223[8]에 규정되어 있으며, RFC 2026[9]에 규정되어 있는 RFC 발간을 위한 절차는 다음과 같다.

① I-D로 출간
② I-D에 대한 코멘트를 취합
③ 코멘트들에 의거하여 I-D 편집
④ ①~③의 과정을 몇 차례 반복
⑤ 영역 의장에게 드래프트 문서를 IESG에 제출하도록 요청
⑥ IESG가 권고하는 변경 사항 반영
⑦ RFC Editor가 RFC 문서로 편집·출간

위의 과정에서 IESG의 승인 절차를 거치게 하는 것은 한 영역의 작업반에서 개발된 프로토콜에 대해 다른 영역들에서 검토하게 함으로써 보다 종합적인 검토가 가능하도록 하기 위함이다.

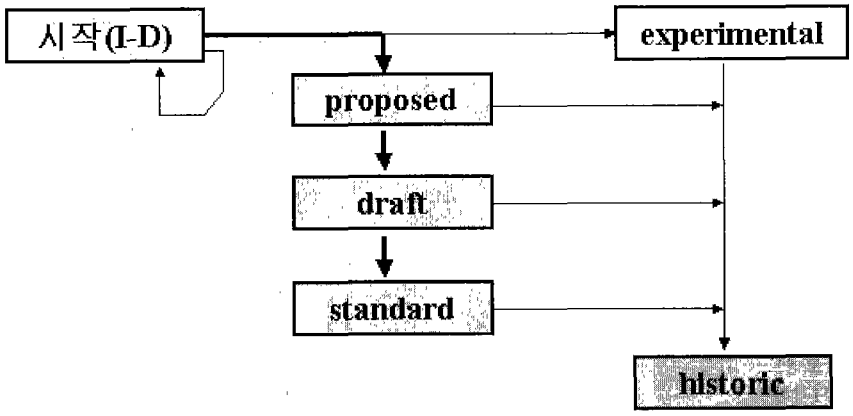
I-D 문서의 명명 방법은 그 작업 근원에 따라 달라지는데, 작업반의 공식 작업 결과일 경우 draft-ietf-작업반명-문서명-버전.txt의 형식을 갖는데, 버전 번호는 00에서 시작되는 두 자리 숫자로 표시된다. 예를 들어 smime 작업반에서 만들어진 인증서 처리와 관련된 문서의 최초 버전이라면 draft-ietf-smime-cert-00.txt와 같은 이름을 가질 수 있을 것이다. 작업반 밖에서도 개인 자격으로 I-D를 작성하여 제출할 수 있는데, 이 경우 문서 이름은 draft-작성자명-문서명-버전.txt의 형식을 갖는데, 예를 들면 draft-hoffman-keying-01.txt와 같다. I-D 문서는 2주 이상의 공개 검토를 거쳐 개정되거나 RFC가 된다. I-D 문서가 개정되면 버전 번호는 1씩 증가한다. I-D가 개정되지 않고 6개월이 지나면 자동적으로 I-D 디렉토리에서 지워지며 소멸되는데, 개정된 I-D는 다시 6개월의 시간을 얻는다. I-D는 RFC 출간을 위한 중간 단계의 임시 문서로 아무런 공식적 지위를 갖지 않으므로, 어떠한 경우에도 표준 문서로 참조되어서는 안 되며, 어떠한 관련 제품도 I-D와 관련하여 표준적합성을 주장하여서는 안 된다.

RFC 문서는 공식 문서로 한 번 발간되면 RFC nnnn과 같이 일련번호를 부여받으며, 이 번호는 1

〔표 2〕 RFC 문서의 분류

표준 문서	Proposed Standard	· IESG의 승인을 요함 · 구현이나 운용을 요구하지 않음
	Draft Standard	· Proposed Standard가 된 후 최소 6개월 경과 · 2개 이상의 상호운용되는 독립적 구현이 존재해야 함
	Internet Standard	· Draft Standard가 된 후 몇 년 경과되어야 함 · 2001년 11월 현재 61편
비표준 문서	Experimental Protocol	· 연구/개발 과정의 일부로 만들어진 문서 · 프로토콜의 중요성이 명확하지 않음
	Informational Documents	· 인터넷 공동체를 위한 일반적 정보 · IETF 밖에서 만들어진 표준 문서인 경우도 많음
	Historic Documents	· 한 때 표준 문서였으나 지금은 다른 문서로 대체되었음

번부터 시작해서 2001년 11월말 현재 RFC 3198까지 발간되어 있다. RFC는 비록 오류를 포함하고 있더라도 그 내용을 고칠 수 없으며, 다만 그 개정판에 의해 그 효력을 없앨 수 있다. RFC 문서는 표준 트랙 문서와 비-표준 문서로 분류할 수 있으며, 이들은 표 2에서와 같이 그 수준과 성격과 따라 세분된다. I-D는 표준 트랙을 밟을 것인지 말지를 미리 결정하는데, 경우에 따라서는 중간에 방향을 변경할 수도 있다. 표준 트랙 I-D가 IESG의 승인을 거쳐 처음 표준 RFC가 될 때는 Proposed Standard의 지위를 얻는다. 표준 트랙 I-D가 많은 참여자들의 관심을 얻지 못할 경우에는 그 프로토콜의 채택 제품이 한정될 것으로 판단하여 Experimental Protocol로 분류되기도 한다. Proposed Standard는 최소 6개월 이상의 기간이 경과하고, 서로 상호운용 되는 독립적인 소스로부터의 둘 이상의 구현이 존재할 경우 Draft Standard가 될 수 있는데, 이 경우 대체로 그 간의 운용 및 개발 경험을 토대로 개정된 문서를 만들게 된다. Draft Standard가 되기 위한 또 하나의 조건은 그 표준이 의존하고 있는 다른 표준들도 모두 Draft Standard 이상의 지위를 갖고 있어야 한다는 점인데, 여러 개의 다른 표준들에 의존하는 문서의 경우 이 요건을 충족하는 것은 쉽지 않으며, 따라서 많은 표준들이 Draft Standard 단계로 진행되지 않고 남아 있으며, 현장에서의 중요성도 꼭 그 표준 성숙 정도와 일치하



〔그림 2〕 표준 트랙 RFC 문서 진행 과정

는 것은 아니다. Draft Standard가 몇 년간의 운용을 통해 안정성과 그 중요성이 충분히 인식될 경우 Full Standard라고도 불리는 Internet Standard가 되는데, 이 경우 RFC 번호와는 별도의 표준 번호를 부여받게 되는데, 2001년 11월 말 현재 61개의 Internet Standard 문서가 승인되어 있다. 표준 트랙 프로토콜이 새로운 프로토콜로 대체될 경우 Historic RFC의 지위를 갖게 되며, 더 이상 표준으로서의 의미를 갖지 않는다. 표준 트랙 RFC의 진행 과정을 도식화하면 그림 2와 같다. Informational RFC는 IETF 밖에서 작업된 표준 문서를 인터넷 공동체에 제공할 필요가 있을 경우, 또는 프로토콜 개발 작업을 위한 요구사항 정의 문서나 기타 지침서 등의 문서를 배포할 필요가 있을 경우 제정한다.

Ⅲ. IETF 보안 영역 작업 현황

현재 IETF 보안 영역에 소속되어 있는 작업반을 현황을 먼저 살펴본 후, 최근 4년간의 총회 활동을 통해 작업반과 BOF들의 활동 상황을 요약해 본다. 또한 보안 영역에서 소멸된 작업반들을 통해 과거에 진행되었던 활동들을 알아보며, 가장 최근에 있었던 제51차 IETF 총회의 회의 내용을 요약하며 제52차 총회에 토의 방향을 전망해 본다.

1. IETF 보안 영역 작업반

2001년 11월 현재 IETF 보안 영역에는 표 3과 같이 19개의 작업반이 소속되어 있다. 이들 중 aft, cat, krb-wg, ipsra, otp, secsh 등은 주로 인증 관련 프로토콜을 개발하고 있다. ipsec, ipsra, secsh, pkix, tls 등의 작업반은 인증과 암호화 기술을 사용한 정보의 안전한 전송을 위한 프로토콜의 개발에 주력하고 있으며, ipsec, kink, msec, pkix, krb-wg 등의 작업반은 키 관리 프로토콜 개발을 담당한다. smime, openpgp, xmldsig, idwg, syslog 등은 응용 계층 보안을 위한 기술을

〔표 3〕 IETF 보안 영역 작업반

약 어	이 름
aft	Authenticated Firewall Traversal
cat	Common Authentication Technology
idwg	Intrusion Detection Exchange Format
ipsec	IP Security Protocol
ipsp	IP Security Policy
ipsra	IP Security Remote Access
kink	Kerberized Internet Negotiation of Keys
krb-wg	Kerberos WG
msec	Multicast Security
openpgp	An Open Specification for PGP
otp	One Time Password Authentication
pkix	Public Key Infrastructure (X.509)
sacred	Securely Available Credentials
smime	S/MIME Mail Security
stime	Secure Network Time Protocol
syslog	Security Issues in Network Event Logging
tls	Transport Layer Security
xmldsig	XML Digital Signatures

개발하고 있으며, 기타 ipsec 관련 정책 관리를 위한 ipsp, 신뢰 정보의 안전한 전달을 위한 sacred, 네트워크 시간의 안전한 전달을 목표로 하는 stime 등의 작업반이 있으며, 일부 작업반은 여러 유형의 작업에 걸쳐 있다.

aft 작업반은 1994년도에 구성되어, David Koblas가 개발한 SOCKS 시스템에 기초한 방화벽 통과 인증 구조를 갖는 통과 프로토콜에 대한 작업을 수행해 왔고, 최근까지 V5 개정판 및 V6에 대한 작업이 진행되어 왔으나 현재 작업들이 소강 상태이다. 3편의 RFC가 있으며, I-D 문서는 없다.

cat 작업반은 분산 시스템에서의 인증, 무결성, 기밀성, 권한 부여 등의 보안 서비스 제공을 위한 프로토콜을 개발해 왔으며, 보안 서비스와 하부 보안 메커니즘의 분리를 강조하고 있다. 지원하고 있는 기존 보안 메커니즘으로는 공개키 기반의 DEC사의 DASS와 공유 비밀키 기반의 MIT의 Kerberos인데, 대부분의 작업은 Kerberos에 치중되어 있다. 최근 몇 년간은 작업이 소강 상태이며, 특별한 수요가 새로 발생하지 않는 한 이 작업반은 조만간 소멸될 것으로 판단된다. 13편의 RFC는 분산 환경에서의 보안 서비스와 인증 서비스, Kerberos V5, GSS-API, 키 교환 방식과 SKIPJACK 블록 암호 알고리즘에 의한 암호화 등을 규정하고 있다. I-D 문서는 1편만 있다.

idwg는 1999년 출범하였으며, IDS 구성 요소들, 대응 시스템, 관리 시스템 사이의 정보 공유를 위한 데이터 포맷과 교환 절차를 정의하고 있다. 아직 RFC는 없으며, 현재 3편의 I-D 문서가 있다.

ipsec 작업반은 1992년 구성된 이래 응용 계층과 무관하게 IP 계층에서 암호화와 인증 등의 보안 서비스를 제공하기 위한 프로토콜과 관련 키 관리 프로토콜에 대한 작업을 수행하고 있으며, 18개 문서에 대한 작업이 완료되어 있고 현재 토의되고 있는 I-D 문서는 29개에 이르고 있다. ipsec 작업반의 주요 RFC는 IPsec 구조 문서, 인증 메커니즘 문서, 암호화/인증 메커니즘 문서, 키 관리 관련 문서, 인증 알고리즘 문서, 암호화 알고리즘 문서 등으로 분류된다. IPsec은 차세대 IPv6에서는 필수적으로 구현되도록 규정되어 있으나 현재의 IPv4에서는 선택 사항이며, 가상사설망(VPN)의 주요 프로토콜로 사용되고 있다.

ipsp 작업반은 2000년도에 구성되어 보안 정책의 표현, 발견, 교환, 관리 등을 위한 구조 정의를 임무로 하고 있다. 구체적으로는 IP 보안 정책을 지원하기 위한 저장소 독립적 정보 모델과 저장소 종류별 데이터 모델 명세, 확장 가능한 정책 표현 언어 개발, 정책의 교환과 협상 프로토콜 개발 등을 수행하고 있으며, 현재 RFC는 없으며 토의 중인 I-D는 5편이 있다.

ipsra 작업반은 2000년도에 구성되어 IPsec 게이트웨이 바깥에서 이동식 장비를 이용하는 원격 사용자를 위한 IPsec 지원을 위한 프로토콜을 개발하고 있으며, 고려되는 원격 사용자들의 인터넷 접속 형태는 지역 ISP에의 모뎀 접속 사용자와 컨퍼런스 등 객지에서의 유선/무선 LAN 접속 등이다. 일반적인 IPsec과의 차이점은 인증 실체가 사람이라는 점, 여러 사람이 동일한 장비를 공유하는 상황을 고려해야 한다는 점, 엔트리 지점에서 접근 실체에 대한 정보를 갖고 있지 않을 수도 있다는 점, 원격 접근 실체가 설정 정보를 갖고 있지 않을 수도 있다는 점 등이다. 현재 RFC는 없으며 토의 중인 I-D는 3편이 있다.

krb-wg는 2000년 출범하였으며, MIT에서 개발된 인증 서비스 Kerberos의 보안성 강화와 Kerberos 구현 시스템 사이의 상호운용성을 목표로 작업하고 있다. Kerberos는 개방된 분산 환경에서의 강한 인증 방법 제공을 목적으로 하고 있다. 현재 RFC는 없으며, 10편의 I-D 문서가 있다.

kink 작업반은 2000년도에 구성되어 Kerberos 기반 중앙 집중형 IPsec 키 관리 메커니즘 개발을 수행하고 있다. 현재 RFC는 없으며, 2편의 I-D 문서가 있다.

msec 작업반은 2001년도에 구성되어, 인터넷에서의 그룹 통신 보호를 위한 IRTF의 보안 멀티캐스트 연구반의 작업에 기반한 프로토콜에 대한 표준화 작업을 수행하고 있다. 프로토콜의 주된 구성 요소는 데이터 보호 변환 (당사자 인증과 기밀성), 그룹 키 및 SA 관리, 그룹 정책 관리 등이며, IRTF의 gsec과 RMRG, IETF의 ipsec, ipsp, policy, rmt 작업반과 긴밀하게 협조하고 있다. 현재 RFC는 없으며, 6편의 I-D 문서가 있다.

openpgp 작업반은 1997년 구성되어, 전자 우편 보안 소프트웨어인 PGP 프로그램에 의해 처리되는 객체를 위한 알고리즘과 메시지 양식 규정, PGP 객체에 대한 MIME 프레임워크에 대한 표준화를 목표로 하고 있다. 2편의 RFC 문서는 OpenPGP 메시지 양식과 MIME 보안 등을 규정하고 있으며,

OpenPGP 메시지 양식에 대한 개정 작업 I-D가 토의되고 있다.

otp 작업반은 1995년 구성되어, 벨코어에서 개발한 일회용 패스워드 시스템인 S/Key의 표준화를 수행해 왔으며, 3개의 RFC 문서는 확장된 질의와 응답에 관한 규정, 일회용 패스워드 시스템 개요, SASL 메커니즘에의 적용 등을 규정하고 있다. 지난 3년 동안 거의 활동이 없는 상태이며, 현재 작업 중인 I-D 문서는 없다.

pkix 작업반은 1995년도에 구성되어, X.509 기반의 PKI 지원을 위한 인터넷 표준 개발을 수행하고 있다. 15편의 RFC 문서는 X.509 V3에 대한 규정, 공개키 확인서의 관리와 요청과 상태 표시 등을 위한 프로토콜, LDAP/FTP/HTTP 등에 의한 PKI 작업, Diffie-Hellman 소유 증명 알고리즘, 적격인증서 프로파일, 데이터 검증/인증 서버 프로토콜, 타임스탬프 프로토콜 등을 규정하고 있다. 현재의 주요 활동은 PKIX 인증서 및 CRL 프로파일 개정 작업 (경로 검증, CRL 검증 보완), CRMF, OCSP, CMC 등에 대한 개정 작업, 영구 식별자, 대리 인증서, SCVP, 그룹 이름, LDAPv3, NR, TSA, DPV/DPD, OCSPv2, TSP에 대한 개발 등이다. 25편의 I-D 문서에 대한 토의가 진행되고 있다.

sacred 작업반은 2000년도에 구성되어, 신뢰성 확보와 관련된 개인 정보 (공개키/개인키 쌍, 인증서, 인증서 체인, 신뢰 정보, 루트 인증 기관 정보 등등)의 안전한 export/import를 위한 메커니즘 개발을 목표로 작업을 수행 중이며, 정보의 이동은 credential 서버로부터의 전송 방법과 동격 장비 사이의 전송 방법으로 분류된다. 요구사항을 규정하는 1편의 RFC와 3편의 I-D 문서가 있다.

secsh 작업반은 1997년도에 구성되어, 원격 로그인, 파일 전송, X11 세션, 기타 TCP/IP 세션을 안전하게 지원하기 위한 보안 셸인 SSH 프로토콜을 개량하고 표준화하는 것을 목표로 작업해 왔다. 보안 셸은 rsh, rlogin, rcp, telnet, rexec, rcp, ftp 등을 대치하며, 모든 트래픽을 암호화하고 다양한 수준의 사용자 인증 제공을 제공한다. 현재는 SSH 버전 2 프로토콜에 대해 강한 보안성 제공과 확장성(scalability) 향상, 기존 인증서 구조 활용, 명료하고 구현하기 쉬운 명세서 개발, TCP/IP나 다른 전송 프로토콜 상에서도 작동 등을 목표로 작업 중이다. RFC는 없으며, 10편의 I-D 문서가 있다.

smime 작업반은 1997년도에 구성되어, RSA사의 주도로 만들어진 인터넷 전자우편 보안 표준인 S/MIME 버전 2를 수용하여 RFC로 발표하고, 바로 이어 메시지 양식, 처리 절차, 보안성 등을 개선하고 새로운 기능을 추가하기 위한 버전 3 개발 작업에 착수한 이래 현재 14편의 RFC를 공식 문서로 지정하고 있으며, 15편의 I-D 문서가 있다. RFC 문서는 S/MIME 메시지 형식과 처리, 인증서 처리, 추가로 도입되는 암호 알고리즘들(IDEA, SKIPJACK, PBE, CAST-128), Diffie-Hellman 알고리즘 관련 사항, 강화된 보안 서비스, 전자서명 정책, 도메인 보안 서비스 등을 규정하고 있다.

stime은 1999년 구성되어, 인터넷에서의 시간의 인증된 분배를 위해 필요한 메시지 양식과 프로토콜을 정의한다는 목표 아래, 기존의 인터넷 기반 시간 분배 프로토콜인 NTP (Network Time Protocol, RFC 1305)에 공개키 기반 인증과 보안 기능 강화에 주력하고 있다. RFC는 없으며, 1편의 I-D 문서가 있다.

syslog는 2000년 구성되어, 시스템/네트워크 이벤트의 네트워크 로깅을 위한 사실상의 표준인 기존 BSD syslog를 informational RFC로 기술하였으며, 여러 수준의 보안 메커니즘 권고안을 개발하고 있다. 1편의 RFC와 3편의 I-D가 있다.

tls 작업반은 1996년도에 구성되어, 트랜스포트 계층 상위에서의 기밀성, 인증, 무결성 구현 방법 제공을 목표로 표준화 작업을 수행하고 있으며, 넷스케이프 SSL을 기초로 하고 있다. 4편의 RFC와 12편의 I-D 문서가 있다.

xmldsig는 1999년 구성되어, 웹자원/XML문서에 대한 서명을 표현하는 XML 구문 개발과 XML 서명의 계산과 확인을 위한 절차를 개발하였다. 특히 XML 문서에 대한 서명의 경우 정규화와 부분 서명을 고려하였다. XML 서명 표준화 작업은 IETF와 W3C의 연합 작업으로 진행되고 있으며, W3C는 XML에 대한 전문성과 XML 관련 표준 작업반들에 대한 조정을 담당하며, IETF는 인터넷 보안기술에 대한 전문성과 IETF 관련 작업반들에 대한 조정을 담당한다. 3편의 RFC는 XML 서명 요구사항, XML 서명 구문과 처리, XML 정규화 등을 규정하고 있다. 현재 Proposed Standard인 XML 서명 구문과 처리 문서를 Draft Standard로 격상시키기 위한 작업의 일환으로 관련 문서에

대한 개정판인 I-D가 토의되고 있다.

2. 최근 IETF 총회에서의 작업반 및 BOF 현황

1998년에서 2001년까지의 연 3회 개최되는 IETF 총회에서의 작업반별 토의를 위한 모임 현황은 표 4와 같다. 표에서 B는 BOF 모임을, O는 작업반 모임을, 음영 처리된 부분은 그 기간 중 해당 작업반이 존재하지 않는 시기임을 나타낸다. 표 하단의 숫자는 해당 문서의 총계 또는 해당 기간 중 존재한 작업반 총수를 나타낸다.

표의 결과를 요약해 보면 가장 활동이 왕성한 작업반은 ipsec, pkix, smime임을 짐작할 수 있으며, 문서의 수도 이를 뒷받침한다. 반면 활동이 미약한 작업반은 이미 소멸된 작업반들인 dnssec, spki, wts와 otp이다. 그리고, aft, cat, openpgp, syslog, xmldsig 등도 추가 작업이 없거나 현재 진행 중인 I-D 문서의 정리 정도에 그칠 것으로 예상된다.

wts는 작업 기반인 S-HTTP(Secure HTTP)가 사장되면서 함께 의미를 잃고 그 활동이 소멸되었다. spki는 pkix의 진행이 부진하던 1997년 그 대안으로 태동되었으나 1999년 이후 pkix의 사용이 활성화됨에 그 의미를 잃게 되었다. dns 보안을 강화하기 위한 dnssec는 인터넷 영역의 dnsind와 합하여 인터넷 영역 소속의 dnsext(DNS Extension)이라는 새로운 작업반을 형성하여 그 작업을 계승하게 하였다.

최근 4년간 작업반을 형성하지 못한 채 BOF만으로 끝난 모임 현황은 표 5와 같으며, 2001년 개최된 BOF의 경우 작업반으로 승인될 가능성은 남아 있다.

1986년 IETF 창설 이래로 보안 영역 작업반들 중 활동이 중지되어 이미 소멸된 작업반 현황은 표 6과 같다.

〔표 4〕 보안 영역 작업반 총회 활동 현황

작업반	#RFC	#I-D	1998			1999			2000			2001		
aft	3	0		O			O			O			O	
cat	13	1	O	O	O	O	O	O	O					
dnssec											소멸 (dnsext에 흡수)			
idwg	0	3	cidf		O	O	O	O	O	O	O	O		O
ipsec	18	29	O	O	O	O	O	O	O	O	O	O	O	O
ipsp	0	5				B	B	B	O	O	O	O	O	O
ipsra	0	3				B		B	O	O	O	O	O	
kink	0	2								B	O	O	O	O
krb-wg	0	10								B	O	O	O	O
msec	0	6									B	O	O	O
openpgp	2	1	O	O	O		O					O		
otp	3	0												
pkix	15	25	O	O	O	O	O	O	O	O	O	O	O	O
sacred	1	3								B	O	O	O	O
secsh	0	10								O	O	O	O	O
smime	14	15	O	O	O	O	O	O	O	O	O	O	O	O
spki			O										소멸	
stime	0	1			B	B	B			O		O		
syslog	1	3						B	B		O			
tls	4	12	O	O				O		O	O		O	
wts														소멸
xmldsig	3	1				B	O	O	O	O				
#doc/#WG	77	130	12	12	13	13	14	14	15	16	20	20	19	19

3. 51차 런던 회의 결과

2001년 8월 5일부터 10일까지 영국 런던에서 개최된 51차 IETF 회의의 경우, 45개국에서 2,500명 정도의 인터넷 전문가들이 모였으며, 보안 영역에서는 ipsec, ipsra, ipsp, smime, aft, secsh, krb-wg, kink, tls, msec, sacred, pkix 등의 12개 작업반과 sasl BOF가 진행되었다. sasl 예비 모임은 SASL(Simple Authentication and Security Layer) 문서인 RFC 2222를 드래프트 표준으로 승격시키기 위한 작업반의 구성을 토의하기 위한 것으로, 이 프로토콜은 인증과 기밀성을 BEEP, IMAP, LDAP, POP, SMTP 등의 상위 어플리케이션 프로토콜에 손쉽게 제공하기 위한 것이다. 작업 방향은 RFC 2222에 대한 개정, SASL 메커니즘 문서들의 개정 등이며, 특히 SASL 메커니즘의 개정은 현재 RFC 2195, 2222, 2831 등에 지정되어 있는 CRAM-MD5, DIGEST-MD5, EXTERNAL 등에 기초한다. 주요 토의 사항은 AES 알고리즘의 도입, 인증 식별자의 표현, SM2 인증 프로토콜의 도입 등에 관한 것이었다.

ipsec에서 주로 토의된 사항은 AES 알고리즘 관련 사항, NAT 및 방화벽 통과 문제, 그리고 IKE 개정에 관한 문제이었으며, 특히 IKE 개정이 주 쟁점 사항이었다. 그리고, 회의 시작 직전 보안 영역 전·현임 의장단 공동 명의로 발표된 IKE 관련 성명이 있었는데, 이 내용은 IKE 개정이 임박해 있고 IKE의 주된 문제가 너무 많은 인증 방식 및 메시지 교환 방식이 포함되어 있어 프로토콜이 복잡해져 있고 많은 보안 문제가 프로토콜 자체의 결함보다는 구현상의 결함으로 인한 것이며 프로토콜의 복잡성은 취약한 구현의 가능성을 높일 뿐이라는 점에서 IKE의 명백한 결함을 보완하기 위한 I-D 문서 외에는 IKE 관련 작업의 보류를 요청하는 것이었다. 이번 회의에서는 이 성명과 관련하여 현재의 IKE에 명백한 취약점이나 알려진 공격 방법이 존재

〔표 5〕 BOF 현황

약어	이름	모임 시기	비고
stp	Secure Transport Proxy	08/1998	aft로 흡수
trustmgt	Trust Management	08/1998	
eap	Extensible Authentication Protocol	12/1998	
micropay	Micro Payments	11/1999	
telsec	Telnet Security	12/2000	
sasl	Simple Authentication and Security Layer	08/2001	1996년부터 활동
inch	Extended Incident Handling	12/2001	
nmsec	Security Requirements for Management Protocols	12/2001	

〔표 6〕 소멸 보안 영역 작업반

이름	소멸 년도	#RFC
IP Authentication	1991	0
Internet Security Policy	1991	1
TCP Client Identity Protocol	1993	2
SNMP Security	1993	6
Authorization and Access Control	1995	0
Commercial Internet Protocol Security Option	1995	0
Privacy-Enhanced Electronic Mail	1996	9
Trusted Network File Systems	1996	0
Internet Secure Payments Protocol	1997	0
Domain Name System Security	1999	9
Simple Public Key Infrastructure	2001	2
Web Transaction Security	2001	3

하는 것은 아니라는 부연 설명이 있었다.

ipsra 회의에서의 주요 토의 사항은 원격 접속자 인증 프로토콜에 관한 것으로 PIC(Pre-IKE Credential 제공 프로토콜)가 다른 경합 프로토콜을 제치고 우위를 차지한 것으로 판단된다.

ipsp 회의에서는 I-D 문서들에 대한 발표가 있었으며, 장차 작업이 필요한 분야로 정책 프레임워크 정책, 보안 게이트웨이 발견 프로토콜, 정책 명세와 합치성 검사에서의 루프 종결 문제, 멀티캐스트 보안에 대한 지원 문제 등이 될 것으로 예상하고 있다.

krb-wg 회의에서 주로 토의된 것은 Kerberos 개정에 관한 문서였으며, 특히 ID 표현에 있어서 GeneralString과 UTF8의 사용에 관한 문제점에 관한 것이었으며, 해결 방안이 모색되어야 하지만 UTF8의 도입으로 인해 Kerberos 표준화가 지연되는 것보다는 현재의 방식으로 표준화한 후 개정판에서 UTF8의 도입을 반영하자는 것으로 결론지어졌다. 그외에도 AP_REP의 안전성, NAT나 VPN과 관련된 주소 지정 문제 등이 토의되었다.

aft 회의는 프로토콜에 대한 토의를 위한 것이라기보다는 작업반의 존속 여부를 결정하기 위한 여론조사의 성격이었으며, 모임 참여자의 상당수가 작업반의 존속을 희망한다고는 했지만 실질적인 기여에 대해서는 대체로 부정적이었던 것으로 판단된다. 작업반이 존속된다고 해도 실질적인 작업이 이루어지기는 어려울 것으로 평가되며, SOCKS는 응용 프로그램으로 남겠지만 이에 대한 표준화는 이루어지지 않을 것으로 판단된다.

smime 회의에서의 주된 토의 사항은 AES 알고리즘의 도입 문제, 필수 공개키 알고리즘을 DH/DSA에서 RSA로 변경하는 문제, S/MIME 버전 3 주요 문서들에 대한 개정 드래프트, NIST에서 발표한 S/MIME 버전 3에 대한 구현 프로파일 등이었다.

kink 회의에서의 주된 쟁점은 접속 요청자의 제안에서 응답자가 첫 번째 이외의 제안을 선택하여 응답한 경우 요청자가 응답자에게 보내게 되는 확인 메시지인 ACK의 신뢰성에 관한 문제이었으며, 토의 끝에 재전송이 가장 유력한 방안으로 수렴되었다.

tls 회의에서는 큰 쟁점 없이 주로 무선 인터넷을 위한 TLS 확장 문서에 대한 발표와 토의가 진행되었다.

msec 회의에서의 주된 토의 사항은 키 변경 문제, GSAKMP의 경량화 버전, GDOI의 갱신 등이었다.

sacred 회의에서는 요구사항 문서가 RFC로 승인되었음을 공지하고, 프로토콜 문서, 프레임워크 문서, PKI 등록 정보 문서 등을 발표하고 토의하였다. 의장단은 작업반의 전체적인 활동과 문서에 대한 일반의 관심이 적음을 우려하고, 이 경우 프로토콜에 대한 작업이 완료되더라도 표준 문서가 되기보다는 실험적 문서의 지위로 격하될 것임을 경고하였다.

pkix 회의에서는 현재 진행 중인 문서들에 대한 간략한 발표들이 있었으며, 특히 로고 유형이라 불리는 X.509 경로 검증 결과를 사람이 이해하기 쉬운 형태로 표현하는 방법에 관한 문서가 발표되어 주목을 받았다.

4. 52차 솔트레이크시티 회의 전망

제 52차 IETF 총회는 2001년 12월 9일부터 15일까지 미국 솔트레이크시티에서 개최된다. 현재 예정되어 있는 보안 영역 회의는 idwg, ipsec, ipsp, kink, krb-wg, msec, pkix, sacred, secsh, smime 등의 10개 작업반 모임과 inch, nmsec 등 2개의 BOF 모임이다.

inch BOF는 2001년 3월 미국 미니애폴리스에서 개최되었던 제 50차 총회의 idwg 회의에서 제기되어 많은 참석자의 호응을 받은 컴퓨터 보안 사건의 표현 양식에 대한 표준화 작업을 위한 것으로 IODEF(Incident Object Description and Exchange Format)를 기초로 작업을 계획하고 있다. 원래 8월의 런던 회의에서 모임을 갖기로 계획되었으나 핵심 구성원들이 참석하지 못하게 되어 52차 회의로 연기되었다.

nmsec BOF는 SNMP와 COPS 등의 기존 네트워크 관리 프로토콜에서 발생하는 보안 요구사항을 다루게 되며, 장차 네트워크 관리 프로토콜을 위한 새로운 보안 구조 개발을 목표로 하고 있다.

최근 IESG는 새로 개발되는 프로토콜들이 국제적으로 적용될 수 있도록 해야 하며, 특히 식별자의 표현에서 UTF8String을 지원해야 한다는 권고사항을 천명하였다. 이는 보안 관련 프로토콜에도 적용되며, 특히 인증에서 사용되는 ID들이 이와 관련되어 있고, 51차 회의에서도 krb-wg와 sasl에서 이 문제가 제기된 바 있다. 기존의 대부분 ID들은 US-ASCII만 지원하고 있으며, 이러한 변화는 기

존 코드들을 상당 부분 변경하여야 하는 부담을 갖고 있어, 많은 프로토콜에서 기존 상태로 우선 표준화한 후 차기 개정 버전에서나 IESG 권고를 반영하려는 계획을 갖고 있다. 52차 회의에서 응용 영역 소속의 intloc(Internationalization and Localization of In ternet protocols) BOF는 이 문제를 토의하기 위한 모임으로 보안 영역 참석자를 비롯한 많은 참석자들의 관심을 모을 것으로 예상된다.

52차 회의에서 보안 영역에서 가장 관심을 모으게 될 사항은 흔히 son-of-ike로 알려진 IKE 문서에 대한 개정 작업에 관한 ipsec 모임에서의 토의로 예상된다. 지난 2년간 계속 이 문제를 논의해 오며, IKE 프로토콜에 관한 부분적 보완 사항을 담은 I-D 문서들만 여럿 발표되어 왔었는데, 최근에 son-of-ike 요구사항 문서[10]와 3개의 경쟁적인 IKE 개정판 문서가 제안되었다. 이들 중 가장 완전한 형식을 갖춘 것은 Dan Harkins 등이 제안한 IKE 버전 2 문서[11]이지만, C. Madson이 제안한 JFK(Just Fast Keying)[12]이나 H. Krawczyk이 제안한 IKE-SIGMA[13]도 프로토콜 자체만으로는 오히려 IKE 버전 2에 비해 우수한 것으로 평가받고 있어 그 귀추가 주목된다. 바람직한 방향은 IKE 버전 2에서 JFK와 IKE-SIGMA의 내용을 수용하는 것으로 생각될 수도 있지만 이 경우 복잡한 프로토콜로 알려진 IKE 초안의 전철을 밟게 될 것이다.

Ⅳ. 보안 영역 밖에서의 보안 관련 활동

보안 영역에 소속되어 있지는 않지만 보안과의 관련성이 밀접한 작업반으로는 인터넷 영역에 속하는 dnsext(DNS Extensions), 운용 및 관리 영역 소속의 aaa(Authentication, Authorization, and Accounting)와 grip(Guidelines and Recommendations for Security Incident Processing), Sub-IP 영역 소속의 ppvpn (Provider Provisioned Virtual Private Networks) 등이 있다.

dnsext는 2000년 구성되어, dnssec의 작업을 계승하여 DNS 보안 작업을 계속 수행하고 있다.

aaa는 1999년 구성되어, 동격 실체 사이의 기능 협상과 메시지 전송을 위한 Diameter 프로토콜에 기초하여 네트워크 접근에 대한 인증, 인가, 그리고 과금 관련 프로토콜 개발을 목적으로 하고 있다.

grip는 1995년 구성되어, 인터넷에서의 보안 사고의 일관성 있는 처리를 용이하게 하기 위한 지침과 권고 사항을 개발하는 것을 목표로 하고 있으며, 이들은 보안사고 발생 시에 기술 제공 업체, 네트워크 서비스 제공자와 보안사고 대응팀에게 보안사고 처리와 관련하여 그 역할을 규정하고 있다. 현재 이 작업반의 활동은 극히 미약한 실정이다.

ppvpn은 2001년 구성되어, 인터넷 서비스 제공자가 VPN 서비스를 지원하기 위한 프레임워크, 서비스 요구사항, 개별 프로토콜에 대한 프로파일 문서들의 개발을 작업 목표로 하고 있다.

일반 작업반에서 개발되는 프로토콜에서도 보안 관련 부분이 별도의 문서로 작성되는 작업반이 다수 존재한다. 예를 들면, 전송 영역 소속의 sip 작업반 관련 I-D 문서로 SIP 보안 구조[14], SIP 다이제스트 접근 인증[15], 다이제스트 인증을 위한 RADIUS 확장[16] 등이 SIP 프로토콜에서의 보안 관련 문서들이다. 그리고, 라우팅 영역 소속의 mobileip 작업반 관련 I-D 문서로 모바일 IP를 위한 일반화된 키 분배 확장[17], 모바일 IPv6로 인한 위협 모델과 모바일 IPv6에서의 보안 요구사항[18], 모바일 IP를 위한 동적 Diffie-Hellman 기반 키 분배[19] 등도 보안 관련 문서들이다.

1980년대 종반부터는 RFC들에 보안 고려사항 절들이 나타나기 시작하며, 1993년에 제정된 RFC 저자들을 위한 지침서인 RFC 1543[20]에 따르면 모든 RFC는 보안 고려사항 절을 반드시 두고 보안성 관련 사항을 기술하도록 의무화하고 있다.

IESG는 RFC 문서의 최종 승인 절차를 담당하고 있는데, 여기에는 보안 영역 의장단도 참여하고 있으며, 새로운 프로토콜로 인해 인터넷이 현재 상태보다 보안이 취약해질 우려가 있는 경우 RFC의 승인을 보류한다는 방침을 적용하고 있다. 모바일 IPv6의 경우 좋은 사례이며 2001년 3월 IESG에서 IPv6에서의 모바일 기능 지원을 위한 문서가 보안 영역 의장단의 거부에 의해 표준화가 지연되고 있다.

Ⅴ. 결 론

IETF에서의 보안기술 표준화와 관련된 활동은 여러 부분에서 수행되고 있다. 인터넷 보안 제품 또는 인터넷 보안 전체에 영향을 미치는 프로토콜 표준화 작업은 IETF 보안 영역 소속의 작업반에서 수행되고 있다. 그리고, 보안 영역 밖의 일부 작업

반은 보안과 밀접한 관련을 갖는 활동을 수행하고 있다. 일반 통신 서비스를 위한 프로토콜 개발에 있어서도 인가된 사용자에게만 서비스를 제공해야 할 경우 또는 부가 보안 서비스를 제공할 필요가 있을 경우 자체적으로 보안기술에 관련된 작업을 수행한다. 그리고, IESG에서도 새로 개발되는 프로토콜의 보안성을 검토하여 RFC 승인 여부를 결정한다.

오늘날 인터넷의 모든 서비스는 직접 또는 간접적으로 보안 관련성을 갖고 있다. 현재와 같은 각종 인터넷 침해 행위가 급격히 증가하고 있는 상황에서 새로운 서비스를 통한 인터넷 영역의 확장 못지 않게 보안에 대한 인식과 대비가 중요하며, IETF의 작업과 표준화 절차는 이를 반영하고 있으며, 프로토콜 개발자들의 보안에 대한 이해와 보안 전문가와의 협력이 긴요함을 알 수 있다.

참 고 문 헌

[1] http://www.w3c.org/
[2] http://www.wapforum.org/
[3] http://www.ietf.org/
[4] http://www.isoc.org/
[5] http://www.irtf.org/
[6] http://www.iana.org/
[7] http://www.iab.org/
[8] J. Postel, J. Reynolds, "Instructions to RFC Authors," RFC 2223, 1997. 10
[9] S. Bradner, "The Internet Standards Process — Revision 3," RFC 2026, 1996. 10
[10] C. Madson, "Protocol Requirements for Son-of-IKE," IETF I-D, draft-ietf-ipsec-son-of-ike-protocol-reqts-00.txt, 2001. 11
[11] Dan Harkins, Charlie Kaufman, and Radia Perlman, "The Internet Key Exchange (IKE) Protocol," IETF I-D, draft-ietf-ipsec-ikev2-00.txt, 2001.11
[12] W. Aiello et al., "Just Fast Keying (JFK)," IETF I-D, draft-ietf-ipsec-jfk-00.txt, 2001. 11
[13] H. Krawczyk, "The IKE-SIGMA Protocol," IETF I-D, draft-krawczyk-ipsec-ike-sigma- 00.txt, 2001. 11
[14] Michael Thomas, "SIP Security Framework," IETF I-D, draft-thomas-sip-sec-framework-00.txt, 2001. 7
[15] J. Undery, "SIP Authentication: SIP Digest Access Authentication," IETF I-D, draft-undery-sip-digest-00.txt, 2001. 7
[16] B. Sterman et al., "RADIUS Extension for Digest Authentication," IETF I-D, draft-sterman-aaa-sip-00.txt, 2001. 11
[17] Charles E. Perkins and Pat R. Calhoun, "Generalized Key Distribution Extensions for Mobile IP," IETF I-D, draft-ietf-mobileip-gen-key-00.txt, 2001. 7
[18] Allison Mankin et al., "Threat Models introduced by Mobile IPv6 and Requirements for Security in Mobile IPv6," IETF I-D, draft-ietf-mobileip-mipv6-scrty-reqts-02.txt, 2001. 5
[19] Franck Le and Stefano M. Faccin, "Dynamic Diffie Hellman based Key Distribution for Mobile IPv6," IETF I-D, draft-le-mobileip-dh-00.txt, 2001. 4
[20] J. Postel, "Instructions to RFC Authors," RFC 1543, 1993. 10

〈著 者 紹 介〉

이 광 수(Gwangsoo Rhee)
종신회원

1981년 2월 : 서울대학교 계산통계학과 졸업
1986년 12월 : 워싱톤대학교 컴퓨터과학과 석사
1990년 5월 : 워싱톤대학교 컴퓨터과학과 박사
1990년 9월 ~ 현재 : 숙명여자대학교 정보과학부 교수
2000년 1월 ~ 현재: OSIA TG-SEC 의장
관심분야 : 네트워크 보안, 알고리즘, 암호학