通信情報保護學會誌
第 10 券 第 2 號, 2000. 6

# IETF 정보보호 표준화 동향

윤 혁 중*, 김 학 범*, 이 홍 섭*

요 약

인터넷의 안전한 사용과 전자상거래의 안전·신뢰성 확보에 필요한 핵심 정보보호 기술에 대한 표준화 요구가 급증하면서 정보보호에 관한 표준화 작업이 활발히 진행되고 있다. 이러한 측면의 국제적인 노력으로는 ISO/IEC JTC 1 SC27, ITU-T, IETF의 정보보호 표준화 작업을 들 수 있다. 특히 IETF는 인터넷의 통일성과 표준을 유지하기 위해 설립된 조직으로 인터넷 표준의 개발 및 선정을 목적으로 정부기관, 업계, 학계 등 다양한 분야의 연구개발자들로 구성된 개방된 형태의 국제 단체이다. IETF는 인터넷과 관련하여 다양한 분야의 기술 표준화를 수행하고 있으며 정보보호 기술 표준화에 대해서도 활발한 활동을 수행하고 있다. 본고에서는 IETF의 조직과 표준화 절차를 소개하고 정보보호 분야의 표준화 활동을 소개한다.

## Ⅰ. 서 론

정보통신 분야에서의 표준화는 정보통신 시장의 국제적인 개방화, 다양화, 경쟁화 추세에 의하여 사용자에게 정보통신기기 및 시스템간의 상호연동을 원활하게 하는 것은 물론 국가 사회적으로 불필요한 중복투자를 방지하여 적은 비용으로 고도의 효율을 획득하기 위한 방법이다. 특히, 정보보호 분야에서의 표준화는 정보의 가치가 점차 높아지고 이들 정보에 대한 보호의 필요성이 커짐에 따라 그 중요성이 부각되고 있으며 선진국에서는 자국의 국가 안보 및 국익을 위해서 국제 표준의 선점을 통한 우위확보 경쟁이 매우 치열한 실정이다.

이에 따라 국제적으로 정부 및 민간기관을 중심으로 정보보호 기술에 대한 표준화 요구가 급증하면서 정보보호에 관한 표준화 작업이 활성화되고 있다. 이러한 측면의 대표적인 국제적 노력으로 ISO/IEC JTC 1 SC27, ITU-T, IETF(Internet Engineering Task Force) 등에서 구체적인 정보보호 표준화 작업이 진행되고 있으며 전자상거래, 인터넷 보안을 위한 정보보호 표준화를 활발하게 추진중이다[1]. 특히 IETF는 인터넷의 통일성과 표준을 유지하기 위해 설립된 조직으로 인터넷 표준의 개발 및 선정을 목적으로 정부기관, 업계, 학계 등 다양한 분야의 연구개발자들로 구성된 개방된 형태의 국제단체이다. IETF에서는 정보보호 분야를 포함하여 표준화 분야별로 워킹그룹을 결성하여 표준화 활동을 수행하고 있다[2].

국내에서도 정보화 추진과 더불어 다양한 정보통신망이 상호 연동되고 정보보호 서비스가 구축되어 감에 따라 정보보호기술 표준화에 대한 필요성이 급증하였고 핵심 기술과 응용 기술 분야에 대한 표준화를 추진하고 있다. 정보보호 기술 표준화는 국제 표준 동향을 수용하면서 국내에 적합한 방식으로 이루어져야 한다. 국내에 적합한 표준화 체계 확립과 표준 제정을 위해 국제 표준화 동향 분석은 필수적이라 하겠다.

본고에서는 인터넷 보안 표준화의 핵심 기구인 IETF의 조직구조 및 표준화 절차를 소개하고 정보보호 분야의 워킹그룹에서 수행하고 있는 표준화 활동을 소개한다.

## Ⅱ. IETF의 구조 및 표준화 절차

### 1. IETF의 조직 구조

IETF의 주요한 목표는 인터넷의 운영·기술상의문제점을 해결하기 위하여 프로토콜 및 구조에 대

* 한국정보보호센터(yoonhj@kisa.or.kr, hbkim@kisa.or.kr, hslee@kisa.or.kr)

한 표준을 제안하고 개발하는 데 있다. IETF와 관련된 조직의 구성은 그림 1과 같다.

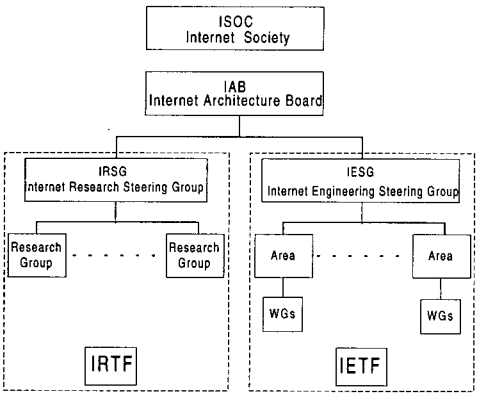


그림 1. IETF의 조직

● **ISOC (Internet Society)**

인터넷의 발전을 위해 결성된 비영리기구로써 기술적인 측면 뿐만 아니라 사회적, 정치적인 분야 등과 같은 광범위한 분야에서 IAB를 비롯한 산하 단체들의 활동을 지원하고 있다[3].

● **IAB (Internet Architecture Board)**

ISOC의 기술 자문 그룹으로서 인터넷과 관련된 기술적, 구조적, 절차적, 정책적 자문을 ISOC에게 제공한다. 또한 IAB는 Internet Standards를 제정하는 절차를 감시하는 역할을 수행하며 표준화 절차가 부적절하게 시행되는 경우 항의를 할 수도 있다. 또한 RFC(Request For Comments)에 대한 편집 관리와 출판을 감독한다[4].

● **IRTF (Internet Research Task Force)**

표준화 과정에는 직접 참여하지 않으나 추후에 인터넷 표준화의 주제가 될만한 기술에 대한 연구를 진행한다. 연구결과가 성숙되면 IETF의 표준화 과정을 거치게 된다. IRTF는 많은 연구그룹(Research Groups)들로 구성된다. 연구그룹들은 인터넷 프로토콜, 인터넷 응용, 인터넷 구조와 기술에 관련된 주제에 대해 연구를 수행한다. IRTF는 IRSG와의 협조하에 IRTF 의장에 의해 관리된다. IRSG는 IRTF 의장과 다양한 연구그룹 들의 의장 등으로 구성된다[5,6].

● **IESG (Internet Engineering Steering Group)**

IETF의 활동과 표준 제정 과정을 기술적으로 관리하는 조직이다. ISOC의 하위 조직으로써 ISOC 이사회에서 재가된 규칙과 절차에 따라 표준 제정 과정을 관리한다. 인터넷 표준으로의 최종 승인을 포함하여 스탠다드 트랙과 관련된 활동이 이루어진다[7].

● **IETF (Internet Engineering Task Force)**

IETF는 인터넷의 통일성과 표준을 유지하기 위해 네트워크 설계자, 운영자, 인터넷 구조와 효율적인 운영과 관련된 연구개발자들로 구성된 개방된 형태의 국제 단체이다. IETF는 일년에 총 3회의 회의를 개최한다.

IETF의 임무는 다음과 같다[8].

- 인터넷의 운영과 기술과 관련된 문제점을 인식하고 해결책을 제안
- 인터넷에 대한 기술적 문제점들을 해결하기 위한 프로토콜의 개발과 사용, 가까운 장래의 구조를 규정
- IESG에게 인터넷의 프로토콜과 프로토콜 사용 표준화에 대해 권고
- 인터넷 조직내의 업체, 사용자, 연구원, 네트워크 관리자들간의 정보 교환을 위한 장을 제공

IETF의 실제적인 기술적 활동은 다양한 분야(Area)의 워킹그룹(Working Groups) 활동을 통해 이루어지고 있으며, 대부분의 작업은 메일링 리스트를 구성하여 이메일을 통해 이루어진다.

현재 IETF는 인터넷의 각종 응용을 연구하는 응용(Applications) 분야, 인터넷 표준화 절차 및 정책 등을 연구하는 일반(General) 분야, 인터넷(Internet) 분야, 운용관리(Operations and Management) 분야, 대규모 망에서 확장성을 지원하기 위해 기존 라우팅 프로토콜의 진화 및 새로운 라우팅 프로토콜을 개발하는 라우팅(Routing) 분야, 인터넷 정보보호 관련 사항을 연구하는 정보보호(Security) 분야, 인터넷 상에서 오디오/비디오 등 여러 미디어를 사용하는 응용 서비스 제공을 위한 전송 프로토콜 규격 작업 등을 담당하는 트랜스포트(Transport) 분야, 인터넷 상의 사용자 서비스를 포괄하는 사용자 서비스(User Services) 분야의 총 8개 분야로 구성되어 있다[10].

표 1. 분야별 워킹그룹

| 분야 | 워킹 그룹 |
|---|---|
| 응용 | Application Configuration Access Protocol(acap) 등 25개 |
| 일반 | Process for Organization of Internet Standards ONg (poisson) |
| 인터넷 | IPNG (ipngwg) 등 15개 |
| 운용관리 | Authentication, Authorization and Accounting(aaa) 등 22개 |
| 라우팅 | IP Routing for Wireless/Mobile Hosts (mobileip) 등 17개 |
| 정보보호 | IP Security Protocol(ipsec) 등 16개 |
| 트랜스포트 | Audio/Video Transport(avt) 등 24개 |
| 사용자 서비스 | User Services(uswg) 등 4개 |

각 분야는 표 1과 같이 워킹그룹을 가지고 있다. 워킹그룹은 정보 문서의 개발, 프로토콜 명세의 개발, 인터넷의 문제점을 해결하려는 목적을 달성하기 위해 연구하는 그룹이다.

각 분야는 또한 BOF(Birds of a Feather) 회의를 가질 수 있다. BOF는 워킹그룹과 같은 목표를 가지지만 헌장이 없으며 1년에 1~2회의 회의를 가진다[9].

## 2. IETF의 표준화 절차

IETF의 워킹그룹의 작업 결과는 문서로 나타나는데, 이 문서는 크게 Internet-Draft와 RFC (Request For Comments)로 구분할 수 있다. Internet-Draft는 RFC로 선정되기 위해 제출된 문서로 작업이 진행중인 문서라고 할 수 있다. Internet-Draft는 IETF에 의해 발표되어 의견수렴이 이루어지는데, internet-draft 디렉토리에 보관된 후 6개월이 지나도 IESG에 의해 RFC로의 출판이 권고되지 않는다면 디렉토리에서 삭제된다. 언제든지 Internet-Draft는 같은 명세에 대한 최신 버전으로 대체될 수 있으며, 대체된 문서는 다시 6개월의 기한을 가진다.

Internet Standard가 되기 위해 RFC는 standards track이라고 불리는 3단계를 거친다. standards track은 Proposed standard, Draft Standard, Internet Standard로 구성된다[11].

### ● Proposed Standard

Standards track을 위한 진입단계가 "Proposed Standard"이다. 보통, 명세서가 Proposed Standard로 지정되기 위해서 구현이나 운영 경험이 필요하지는 않는다. 그러나, 이러한 경험은 아주 바람직하고, Proposed Standard 지정에 이익이 되도록 강력한 논증을 나타내준다. IESG는 실질적으로 핵심 인터넷 프로토콜과 운영에 중요한 영향을 미치는 명세서를 Proposed Standard 상태로 승인하기에 앞서 구현이나 운영 경험을 요구할 지도 모른다.

Proposed Standard는 이전의 요구사항에 대해서 생략된 기술이 없어야 한다. 그러나, IESG는 기술이 생략되었더라도 이것이 유용하고 필요하다고 생각되면 명세서가 Proposed Standard 상태가 되도록 이러한 요구사항을 보류하기도 한다.

구현자는 Proposed Standard를 미완성 명세서로 여긴다. 경험을 얻고, 명세서를 검증, 시험, 명백하게 설명하기 위해서 이를 구현하는 것이 바람직하다.

### ● Draft Standard

다른 코드 기반의 최소한 2개의 독립적이고 상호운용성을 구현한 명세서가 개발되었고, 충분히 성공적인 운영 경험을 얻었다면, 이는 "Draft Standard" 단계가 된다. Draft Standard로의 승급은 명세서가 완전하고, 유용할 것이라는 강한 신뢰를 나타낸다.

최소한 2개의 독립적이고 상호운용적인 구현의 요구사항은 명세서의 모든 옵션과 특성에 대해 적용된다. 하나 혹은 그 이상의 옵션이나 특성이 최소 둘의 상호운용 구현에서 증명되지 않는 경우에는, 이러한 옵션이나 특징이 제거된 경우에만 Draft Standard 단계로 나아간다.

Draft Standard는 의미와 구현을 개발하기 위한 기초로써 아주 안정적이고 잘 이해되어야 한다. 광범위한 영역에서 이용되어질 때, Draft Standard 명세서에 기초한 구현은 큰 규모에서는 예측하지 못한 반응이 일어날 소지가 있으므로, Draft Standard는 추가적이거나 좀더 광범위한

영역의 경험을 필요로 한다.

Draft Standard는 보통 최종 명세서로 여겨지고, Draft Standard에 대한 변경은 특정 문제들을 해결하기 위한 것이다.

● Internet Standard

의미 있는 구현과 성공적인 운영 경험을 획득한 명세서는 "Internet Standard" 단계로 올라간다. Internet Standard는 Standard로도 불리며 상위 등급의 기술적 완성과 명시된 프로토콜이나 서비스가 인터넷 공동체에 중요한 이익을 제공한다는 일반적 믿음에 의해 특징 지워진다.

Standard 단계에 도달한 명세서는 RFC 번호를 유지한 체, STD시리즈 번호를 부여받는다.

## III. IETF의 정보보호 표준화 동향

IETF의 실제적인 기술적 활동은 다양한 분야(Area)의 워킹그룹(Working Groups) 활동을 통해 이루어지고 있다. 현재 IETF는 8개 분야로 나누어져 있으며 이 중에서 인터넷 정보보호와 관련된 표준화 활동을 하는 분야는 Security 분야, 즉 정보보호 분야이다.

정보보호 분야는 openpgp, aft, cat, ipsp, ipsec, ipsra, idwg, otp, pkix, smime, stime, secsh, spki, tls, wts, xmldsig의 총 16개의 워킹그룹으로 구성된다[12].

정보보호 분야의 워킹그룹을 인터넷의 계층 구조에서 표현해보면 그림 2와 같다.

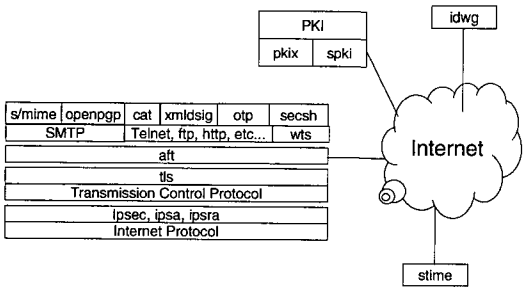


그림 2. 정보보호 분야의 워킹그룹

각 워킹그룹별로 연구 내용은 다음과 같다.

● An Open Specification for Pretty Good Privacy (openpgp)

PGP는 1991년 미국의 Phil Zimmermann에 의해 인터넷에 처음으로 나타났으며 전자우편에 정보보호 기능을 제공하기 위해 사용된다. PGP는 구현이 용이하고 알고리즘의 안전성이 높기 때문에 인터넷 공동체에서 널리 사용되고 있다[13].

PGP는 전자우편과 파일 저장소를 보호하는데 사용되어진다. PGP는 전자서명, 암호화, 압축, radix-64변환을 이용해 메시지와 데이터 파일에 무결성 서비스를 제공한다. PGP는 정보 객체를 전자서명하고 암호화를 하는 방법을 제시하며 어떠한 축적-전송(store and forward) 방식에도 적절하게 사용될 수 있다.

openpgp 워킹그룹의 목적은 MIME 프레임워크의 제공 뿐만 아니라 알고리즘과 PGP가 처리하는 객체들의 포맷에 대한 표준을 제공하는 것이다.

openpgp 워킹그룹에는 현재 OpenPGP Message Format이라는 RFC2440이 있다. RFC 2440은 OpenPGP 포맷에 기반한 상호운용성 있는 응용을 개발하기 위해 필요한 정보로써 암호화, 복호화, 서명과 키관리 기능을 제공하기 위해 OpenPGP에서 사용되는 메시지-교환 패킷에 대한 정보를 제공하고 있다[14].

● Authenticated Firewall Traversal (aft)

aft 워킹그룹의 목적은 침입차단시스템에 대해 응용계층에서의 프로토콜을 규정하는 것이다. 침입차단시스템의 인증에 대한 일반적인 구조와 함께 TCP와 UDP 응용을 모두 지원하는 프로토콜을 규정한다. 또한 상호운용성을 위한 기본 인증 방법도 제안하고 있다.

현재 aft 워킹그룹에는 3개의 RFC가 있다. RFC 1928에서는 TCP와 UDP 도메인에서 침입차단시스템을 안전하게 사용하기 위해 클라이언트-서버 응용을 위한 프레임워크를 제공하기 위해 설계된 SOCKS Protocol V5에 대해 설명하고 있다. SOCKS Protocol V5 명세에는 초기 socks 연결 확립때 임의의 인증 프로토콜 사용을 위한 일반 구조를 명시하고 있다. RFC 1929와 1961에서는 이러한 프로토콜로써 SOCKS V5를 위한 Username/Password 인증을 기술하며, SOCKS V5 GSS-API 인증 프로토콜에 대한 명세를 제공하고 무결성, 인증과 선택적인 비밀성의 제공을 위해 GSS-API에 기반한 인캡슐레이션을 정의한다[15,16,17]

● Common Authentication Technology (cat)

cat 워킹그룹의 목적은 다양한 프로토콜 호출자에게 호출자를 정보보호 메커니즘의 구체적인 명세에서 격리시키는 방식으로 분산 정보보호 서비스(인증, 무결성, 기밀성, 권한허가)를 제공하는 것이다.

정보보호 데이터 요소들을 호출자 프로토콜로 통합하는 작업으로부터 정보보호 구현 작업을 분리시킴으로써, 이러한 작업들은 다양한 분야의 전문 구현자들에 의해 나누어져 수행되어 질 수 있다. 따라서 프로토콜 구현자에게는 정보보호 메커니즘보다 프로토콜이 제공하는 기능에 중점을 두게 한다. cat 워킹그룹은 정보보호 접근에 통일성과 모듈화를 권장하며, 공통 기술 사용을 지원하며, 내재된 기술의 진화를 수용한다.

이러한 목표를 위해 cat 워킹그룹은 상호관련된 다음과 같은 작업을 추구한다.

cat 워킹그룹은 공통의 서비스 인터페이스로서 GSS-API를 정의했다. GSS-API는 연결 지향 환경에서 호출자로 하여금 채택되는 정보보호 메커니즘을 식별하는 토큰 포맷을 가지고 정보보호 서비스를 제공하게 한다. 지금까지는 GSS-API에 관한 C 언어 바인딩을 제공하고 현재 Java 바인징을 정의하고 있다.

권한허가 인터페이스가 앞으로 수행될 작업의 관련 분야가 될 것이다. 또한 CAT은 정보보호 서비스 제공을 위한 지원 메커니즘을 정의하는데, 현재는 채택과 사용의 용이함을 지원하는 "low infrastructure" 메커니즘의 스펙 정의 활동을 수행하고 있다[18].

● IP Security Policy (ipsp)

인터넷의 급속한 발전과 네트워크 자원(대역폭, 라우터, 호스트 등)에의 접근에 대한 통제의 필요성은 이러한 자원들에 대한 접근을 확장성 있고 안전하게 통제하는 정책의 표현, 발견, 교환, 관리에 대한 필요성을 발생시켰다.

현재의 IP security 프로토콜과 알고리즘은 IKE (Internet Key Exchange)를 이용하여 keying material을 교환할 수 있고 AH와 ESP 프로토콜을 이용하여 데이터 흐름을 보호할 수 있다. IKE의 범위는 프로토콜을 보안 연결(security association)의 양단 간에서 keying material과 관련된 정책 정보들의 인증된 교환으로 제한한다.

그러나, 통신 경로 상에서 보안 게이트웨이와 라우터 필터같은 개체에게 정책 제한을 가할 필요가 있는 관리적인 개체가 있을 수 있다. 또한 보안 연결의 양단간이나 그들 각자의 관리 개체가 엔드 호스트와 통신의 경로 상에서 보안 게이트웨이와 라우터 같은 정책 시행 지점에 대한 접근통제 정보를 안전하게 발견하고 협상할 필요가 있다.

이러한 문제점에 대해서 워킹그룹은

- IP 보안 정책들을 지원하기 위해 저장소 독립적인 정보 모델과 저장소에 특정한 데이터 모델을 규정한다. 이 모델들은 운용관리 분야의 Policy Framework 워킹그룹에서 정의된 정보 모델과 데이터 모델로부터 유도한다.
- 확장가능한 정책 명세 언어(policy specification language)를 개발하고 채택한다. 이 언어는 다른 프로토콜 도메인에서 정책을 지원할 수 있도록 범용적이어야 하지만, IPSec에 필수인 정보보호 메커니즘을 제공해야 한다.
- 현재 존재하는 정책분배 프로토콜을 사용하여 IPSec 정책 제공에 대한 지침을 제공한다. 이것은 LDAP, COPS, SNMP, FTP와 같은 프로토콜로 IPSec 정책 분배에 대한 프로파일을 포함한다.
- 정책 서버의 발견, 정보보호 정책의 분배와 협상, intra/inter 도메인 환경에서 정책 충돌을 해결하는 정책 교환 프로토콜과 협상 프로토콜을 개발하고 채택한다. 이 프로토콜은 어떠한 정보보호 프로토콜과 키 관리 프로토콜에도 독립적이어야 한다.

ipsp 워킹그룹의 작업 아이템들은 인터넷 프로토콜을 위한 정보보호 구조(RFC 2401)와 IKE (RFC 2409)에 호환성이 있는 표준들을 산출할 것이며 ipsec 워킹그룹에 의한 표준들을 보충하게 된다[19].

● IP Security Protocol (ipsec)

ipsec 워킹그룹은 클라이언트 IP 프로토콜을 보호하는 메커니즘을 개발하고 있다. 인증, 무결성, 접근통제, 비밀성의 조합들을 유연하게 지원하는 암호화 정보보호 서비스를 제공하기 위해 네트워크 계층에서의 정보보호 프로토콜을 개발한다.

IP Authentication Header(AH)와 IP Encapsulating Payload(ESP)에 대한 프로토콜 포맷은 암호화 알고리즘과 독립적이다. 우선은

host-to-host 보안을 추구하고 다음으로 subnet-to-subnet과 host-to-subnet 위상을 추구할 예정이다.

또한 ipsec 워킹그룹에서는 네트워크 계층에서의 키관리 요구사항을 지원하기 위한 프로토콜과 암호화 기술이 개발될 것이다. IKMP(Internet Key Management Protocol)가 하위 계층의 정보보호 프로토콜에 독립적인 응용 계층 프로토콜로써 명시될 것이며 ISAKMP/Oakley에 기반을 둘 것이다.

ipsec 워킹그룹이 개발하는 문서는 다음의 7가지 종류로 크게 나누어질 수 있다[20].

- 구조(Architecture) : IPSec의 일반적인 개념, 정보보호 요구사항, 정의, 메커니즘
- ESP 프로토콜 : 패킷 암호화와 선택적으로 인증을 위한 ESP의 사용에 대한 일반적인 이슈들과 패킷의 포맷
- AH 프로토콜 : 패킷 인증을 위한 AH의 사용과 관련된 일반적인 이슈들과 패킷의 포맷
- 암호 알고리즘: ESP를 위해 다양한 암호 알고리즘이 어떻게 사용되어지는가를 기술
- 인증 알고리즘 : ESP와 AH를 위한 다양한 인증 알고리즘이 어떻게 사용되어지는가를 기술
- 키 관리 : 키 관리 스킴에 관한 내용
- DOI(Domain of Interpretation) : 승인된 암호와 인증 알고리즘의 식별자 및 키 사용주기와 같은 운용적인 파라미터들과 같이 다른 문서들을 위해 필요한 값들을 포함하고 있음.

### ● IP Security Remote Access (ipsra)

ipsec 워킹 그룹은 원격 접속에 관한 연구를 수행하며 다음과 같은 목적을 가지고 있다.

- 원격 접속 구조를 정의한다. 원격 접속에 참여하는 실체들과 그들 사이의 관계를 정의한다.
- IKE를 운영하는 IPSec 장치에 레거시 인증 메커니즘(legacy authentication mechanism)을 이용하여 사용자 인증을 수행하는 표준 메커니즘을 정의한다.
- 사용자 구성 정보 및 사용자 접근 통제 정보를 사용자의 사설 네트워크로부터 지역 IPSec이 구현된 곳까지 전달하는 표준 메커니즘을 정의

ipsra 워킹그룹은 ipsec 워킹그룹, mobilip 워킹그룹과 협조하여 표준화 활동을 추진한다[21].

### ● Intrusion Detection Exchange Format (idwg)

침입탐지 시스템은 정보 접근, 정보 조작, 시스템 무력화와 같은 불법 침입을 감지하고 대응하는 소프트웨어를 말한다[22].

다양한 사이트에서 다양한 개발자들의 침입탐지 시스템이 사용되고 있다. 보안 사건은 많은 사이트에 분산되어지는 경우가 많기 때문에, 동일한 사건에 대해서도 시스템들에 따라 다양한 측면들이 보여질 것이다. 따라서 다양한 침입탐지 시스템들이 진행중인 공격에 대한 데이터를 공유하는 것은 이익이 될 수 있다.

idwg 워킹 그룹의 목적은 침입탐지와 대응 시스템, 이것들과 상호작용이 필요한 관리 시스템에게 이익이 될 수 있는 정보들을 공유하기 위한 데이터 포맷과 교환 절차들을 정의하는 것이다.

idwg 워킹 그룹은 침입탐지 시스템간의 통신을 위한 기능적 요구사항, 침입탐지 시스템과 관리 시스템간의 통신을 위한 요구사항, 이러한 요구사항에 대한 이론적 근거와 요구사항을 만족하는 데이터 포맷을 기술하는 공통 언어 스펙, 침입탐지 시스템간의 통신을 위해 가장 잘 사용되어지는 현재의 프로토콜과 데이터 포맷을 연관시키는 방법 등에 관한 연구를 수행하고 표준을 제정한다[23].

### ● One Time Password Authentication (otp)

사용자가 시스템에 로그인하기 위해 동일한 패스워드를 매번 사용하는 기존 패스워드 인증 시스템은 네트워크 상에서 재사용공격에 대한 위협에 취약하다. 이러한 문제점을 해결하기 위해 Bellcore의 S/Key을 토대로 패스워드를 매번 바꾸어 사용할 수 있는 일회용 패스워드 기술에 대한 표준화 작업을 수행하고 있다[24].

### ● Public-Key Infrastructure (X.509)(pkix)

pkix 워킹그룹은 X.509에 기반한 공개키기반구조를 지원하기 위해 필요한 표준 개발을 목적으로 설립되었다.

X.509 V3 인증서와 V2 인증서 폐지목록, 인증서 생성과 관리를 위한 메시지들을 정의하는 인증서 관리 프로토콜, 인증서 폐지목록을 요청하지 않고도 인증서의 현재 상태를 결정하는데 유용한 프로토콜인 OCSP(Online Certificate Status Protocol), X.509 인증서의 생성을 위해 인증기관에 인증서 요

청을 전송하기 위해 사용되는 인증서 요청 메시지 포맷(CRMF :Certificate Request Message Format) 등이 RFC로 승인되었다.

또한 PKIX를 지원하기 위한 최소의 스키마가 정의된 인증서와 인증서 폐지목록 저장소에 LDAP V2의 사용에 관한 프로파일과 PKI 운영에 관한 전송을 위한 FTP와 HTTP의 사용, 인증 정책과 업무에 관한 지침, KEA의 사용에 관한 RFC가 승인되어 졌고, ECDSA에 관한 RFC도 승인될 예정이다. 두번째의 인증서 관리 프로토콜인 CMC (Certificatie Management Protocol using CMS) 에 관한 작업도 PKCS와 S/MIME을 위해 개발된 CMS(Cryptographic Message Syntax)와 보조를 맞추어 추진되어 왔으며 최근에 RFC로 승인되었다. 또한 PKIX 문서에 관한 가이드를 제공해줄 로드맵도 informational RFC로 추진되고 있다[25-32].

pkix 워킹그룹은 PKI 관리에 통합적인 프로토콜과 PKI 사용과 밀접히 관련을 가지는 프로토콜의 개발에 착수하고 있다. 인증서 폐지 방법의 대안에 관한 작업이 이루어지고 있으며 인증서 명명 형태와 부인방지 문맥(context)에 사용되기 위해 설계된 인증서인 "qualified certificates"에 대해 확장 사용(extension usage)을 정의하고 있으며, 시점확인과 데이터 인증에 관한 프로토콜도 작업중이다.

X.509 속성(attribute) 인증서 프로파일 작업이 수행될 것이고 공개키 인증서와 속성 인증서 사이의 차이점을 수용하기 위해 현재의 인증서 관리 표준에 확장을 가져올 것이다.

### ● S/MIME Mail Security (smime)

smime 워킹그룹은 전자우편의 보안 문제를 해결하기 위한 워킹그룹으로서 MIME 데이터에 암호학적 서명과 암호화 서비스를 추가하는 프로토콜을 기술한 S/MIME Version 3 메시지 스펙, Diffie-Hellman 키 협상 방식을 사용할 경우 small-subgroup 공격을 방지하기 위한 방법, CMS (Cryptographic Message Syntax), S/MIME을 위한 선택적인 보안 서비스 확장과 인증서 처리에 관한 RFC를 제정하였다[33].

### ● Secure Network Time Protocol (stime)

인증된 원천으로부터 안전하게 시간을 얻는 방법이 정보보호와 부인방지를 위한 주요 요소가 되고 있다.

시간을 분배하는 현재의 방법은 공개키기반구조나 암호학적 방법을 사용하지 않고 있기 때문에 외부의 공격과 변형에 취약하다. 이러한 취약점을 극복하기 위해 공개키기반구조를 사용하여 시간 분배를 안전하게 하며 위험을 감소시킬 수 있다.

stime 워킹그룹은 현재의 Network Time Protocol(NTP)에 대한 수정을 통해 인터넷에 대해서 인증된 시간의 분배를 지원하기 위해 필요한 메시지 포맷과 프로토콜을 정의한다[34].

### ● Secure Shell (secsh)

telnet 혹은 rlogin 등은 보안 측면에서 매우 취약한 응용 시스템으로 강력한 보안 서비스를 요구하고 있다. 이에 따라 SSH, Secure-Telnet, SSL-telnet등과 같이 telnet 세션 전체를 암호화하여 동작하는 프로토콜이 제안되어 사용되고 있다.

이 가운데 SSH는 가장 널리 보급된 제품으로 사용자 인증에 사용되는 로그인 명과 패스워드만을 보호하는 것이 아니라, 로그인 한 후 모든 세션을 암호화하여 비밀성을 제공하는 역할을 하므로 안전하게 telnet을 이용할 수 있게 한다.

secsh 워킹그룹에서는 SSH가 암호 해독과 프로토콜 공격에 대해 강력한 보안을 제공하고, 글로벌한 키관리와 인증서 기반구조 없이도 작동되며, 현존하는 인증서기반구조를 사용할 수 있고, 채택과 사용이 쉽고, 사용자로부터 수동의 상호작용을 최소로 하거나 없도록 하며, 구현의 용이성 보증에 대해 연구하고 있다[35].

### ● Simple Public Key Infrastructure (spki)

spki 워킹그룹은 쉽고, 간단하고, 확장 가능한 인증서 구조와 운영 절차를 만드는 작업을 하고 있다. spki 워킹그룹에서는 키 인증서 형식, 서명 형식 및 키 획득 프로토콜 등에 관한 표준 개발 작업이 진행 중이며 이러한 키 인증서 형식과 관련 프로토콜은 이해, 구현 그리고 사용이 간단해야 한다.

현재 제정된 RFC에서는 SPKI의 요구사항과 SPKI 인증서 및 인증서 폐지 목록에 관한 이론을 제시하고 있다[36,37].

### ● Transport Layer Security (tls)

현재까지 인터넷의 양 단간 전송 계층에서 안전하고 인증된 채널을 제공하는 몇 가지 방법들이 제시

되어졌다.

그중에서 TLS는 IETF가 표준화하기 위해 제안한 보안 프로토콜로 넷스케이프사의 SSL(Secure Socket Layer)과 유사한 메커니즘으로 전송 계층에서 보안 서비스를 제공한다.

tls 워킹그룹은 일반적인 목적의 보안과 키관리 메커니즘 보다는 전송 계층에서의 보안 특성을 제공하는데 초점을 맞추고 있으며, 전송 계층에서 인증, 무결성, 프라이버시를 구현하기 위한 방법을 제공하기 위한 방법을 제공하다[38].

현재까지 제정된 RFC에서는 TLS V1.0과 Kerberos에 기반한 인증을 지원하기 위해 TLS 프로토콜에 새로운 cipher suites를 제안하였다. 또한 현재의 TCP 연결에서 TLS를 개시하기 위해 HTTP/1.1에서 Upgrade 메커니즘을 사용하는 방법, HTTP 연결을 안전하게 하기 위해 TLS를 사용하는 방법 등도 포함되어 있다.

● **Web Transaction Security (wts)**

wts 워킹그룹에서는 HTTP를 이용하는 웹 트랜잭션에 정보보호 서비스를 제공하기 위한 요구사항과 명세를 개발하는 것을 목표로 하고 있으며 HTTP에 정보보호 기능을 추가한 S-HTTP (Secure HTTP)를 근간으로 작업하고 있다. S-HTTP는 트랜잭션 비밀성과 무결성, 발신처 부인방지 등의 서비스를 제공한다. S-HTTP는 각 트랜잭션에 대해 협상을 지원하여 키 관리 메커니즘, 정보보호 정책, 암호 알고리즘의 선택에 있어 유연성을 강조한다[39].

현재까지 제정된 RFC에서는 HTTP에 정보보호 서비스를 제공하기 위한 비밀성, 무결성, 사용자 인증, 서버/서비스 인증 요구사항을 명시하고 있고, S-HTTP 협상 매개변수에 대한 문법을 기술하고 있다.

● **XML Digital Signatures (xmldsig)**

XML은 SGML의 간략화된 버전으로 SGML의 확장성, 구조, 검증 등 장점을 그대로 상속받고, 이를 조금 더 배우기 쉽고, 표현하기 쉽고, 응용하기 쉽도록 제작된 언어이다. XML 문서에 대한 전자서명은 웹 데이터에 대해 무결성, 서명 보증, 부인방지를 제공할 수 있다. 이러한 특성은 특히 계약, 가격 목록 등을 나타내는 문서에 특히 중요하다.

xmldsig 워킹 그룹은 웹 자원의 서명을 표현하기 위해 사용되어 지는 XML 문법과 프로토콜 메시지, 서명을 계산하고 검증하기 위한 절차의 개발을 목표로 하고 있다[40].

xmldsig 워킹 그룹의 활동의 핵심 범위는 데이터 모델, 문법, 암호학적 서명을 XML 자원에 바인드하기 위한 처리 등을 규정하는 것이다. 이를 위해 XML-DSig가 메타데이터와 객체모델기술 개발의 구성요소가 되도록 하는 데이터 모델 정의, 확장가능한 규범 프레임워크의 정의, XML 서명에 대한 문법과 처리 절차 등에 초점을 맞출 것이다.

xmldsig 워킹그룹의 요구사항은 다음과 같다.

- 확장성이 높은 단순한 XML 서명 문법을 정의
- 응용으로 하여금 분리된 서명블록에 대한 처리뿐 아니라, XML과 non-XML로 이루어진 복합적인 문서의 생성과 처리를 하게 한다.
- XML-DSig는 다른 XML 기술과 함께 통합되어질 수 있어야 한다.

## Ⅳ. 결 론

본고에서는 IETF의 조직구조 및 표준화 절차를 소개하였고 연구 내용별로 분류되는 분야와 정보보호 분야의 워킹그룹 구성, 정보보호 분야 워킹그룹의 목적 및 연구 내용, 표준화 동향을 소개하였다.

IETF는 인터넷에 대한 통일성과 표준 제정을 위해 조직된 개방된 형태의 표준화 단체로서 인터넷 구조의 발전과 원활한 운영을 위해 분야별로 표준화 활동을 수행하고 있으며 인터넷과 관련하여 개방성을 바탕으로 가장 활발한 활동을 하고 있다.

국내의 정보보호 표준 제정을 위해서는 국제 정보보호 표준화 동향을 분석하고 국내에 적합한 표준을 제정하는 것이 필수적이라 하겠다. 따라서 IETF의 표준화 활동의 계속적인 주시와 지속적인 참여를 통해 국제 표준화 동향의 흐름에 동참하여야겠다.

또한 국가적인 차원에서 인터넷 서비스의 활성화 및 인터넷 기술의 국가 경쟁력을 확보하기 위해 각 분야별로 표준화 동향 파악과 적극적인 표준 개발의 노력이 이루어져야만 선진국에 뒤지지 않는 기술 개발이 가능하리라 생각된다.

## 참 고 문 헌

[1] 정보보호 기술표준 연구 제1차년도 연구개발

결과보고서, 한국정보보호센터, 1998
[2] http://www.ietf.cnri.reston.va.us/overview.html
[3] http://www.isoc.org
[4] http://www.iba.org/overview.html
[5] http://www.irtf.org
[6] RFC 2014, IRTF Research Group Guidelines and Procedures, Oct. 1996.
[7] http://www.ietf.cnri.reston.va.us/glossary.html
[8] http://www.ietf.cnri.reston.va.us/tao.html
[9] RFC 1603, IETF Working Group Guide-lines and Procedures, Sep. 1998.
[10] 1999년도 정보통신표준화백서, 한국정보통신기술협회, 1999
[11] RFC 2026, The Internet Standards Process, Oct. 1996.
[12] http://www.ietf.org/html.charters/wg-dir.html
[13] 이만영, 김지홍, 류재철, 송유진, 염흥열, 이임영, 전자상거래 보안 기술, 1999.
[14] RFC 2440, OpenPGP Message Format, Nov. 1998.
[15] RFC 1928, SOCKS Protocol Version 5, Mar. 1996.
[16] RFC 1929, Username/Password Authentication for SOCKS V5
[17] RFC 1961, GSS-API Authentication Method for SOCKS Version 5
[18] http://www.ietf.org/html.charters/cat-charter.html
[19] http://www.ietf.org/html.charters/ipsp-charter.html
[20] RFC 2411, IP Security Document Roadmap, Nov. 1998.
[21] http://www.ietf.org/html.charters/ipsra-charter.html
[22] 김병구, 정태명, "침입탐지 기술의 현황과 전망", 정보과학회지 제 18권 제 1호, Jan. 2000.
[23] http://www.ietf.org/html.charters/idwg-charter.html
[24] http://www.ietf.org/html.charters/otp-charter.html
[25] RFC 2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile, Jan. 1999.
[26] RFC 2510, Internet X.509 Public Key Infrastructure Certificate manegement Protocols, Mar. 1999.
[27] RFC 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP, Jun. 1999.
[28] RFC 2511, Internet X.509 Certificate Request Message Format, Mar. 1999.
[29] RFC 2587, Internet X.509 Public Key Infrastructure LDAPv2 Schema, Jun. 1999.
[30] RFC 2585, Internet X.509 Public Key Infrastructure Oprational Protocols: FTP and HTTP, May 1999.
[31] RFC 2527, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Mar. 1999.
[32] RFC 228, Internet X.509 Public Key Infrastructure Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates, Mar. 1999.
[33] http://www.ietf.org/html.charters/smime-charter.html
[34] http://www.ietf.org/html.charters/stime-charter.html
[35] http://www.ietf.org/html.charters/secsh-charter.html
[36] RFC 2692, SPKI Requirements, Sep. 1999.
[37] RFC 2693, SPKI Certificate Theory, Sep. 1999.
[38] http://www.ietf.org/html.charters/tls-charter.html
[39] http://www.ietf.org/html.charters/wts-charter.html
[40] http://www.ietf.org/html.charters/xmldsig-charter.html

## 〈著者紹介〉

**윤 혁 중 (Hyukjoong Yoon)**
1998년 2월 : 아주대학교 컴퓨터공학과 졸업(학사)
2000년 2월 : 아주대학교 대학원 컴퓨터공학과 졸업(석사)
1999년 12월 ~ 현재 : 한국정보보호센터 연구원
※ 관심분야 : 정보보호 표준화, 네트워크 정보보호

**김 학 범 (Hakbeom Kim)**
1990년 8월 : 중앙대학교 전자계산학과 졸업(석사)
1996년 3월 ~ 1999년 2월 : 아주대학교 컴퓨터공학과 박사과정 수료
1991년 10월 ~ 1996년 6월 : 한국전산원 주임연구원
1997년 4월 ~ 1998년 12월 : TTA/SC10/SG3(시스템보안 연구위원회) 간사
2000년 1월 ~ 현재 TTA/TC10(정보보호 기술위원회) 간사, TTA/SC10/SG3 의장
1996년 7월 ~ 현재 한국정보보호센터 선임연구원, 표준과제책임자
※ 관심분야 : 컴퓨터·네트워크 보안, 접근통제, 정보보호 표준화

**이 홍 섭 (Hongsub Lee)**
한양대학교 전자공학과 학사
한양대학교 전자공학과 석사
대전대학교 컴퓨터공학과 박사
1980년 ~ 1996년 : 한국전자통신연구원 실장
1996년 ~ 현재 : 한국정보보호센터 개발부장, 정보통신기술협회 정보보호기술위 의장, 정보통신기술협회 정보기술표준용어 의장, 한국통신정보보호학회 상임이사, 전자거래분쟁조정위원회 위원(산자부), 개인정보분쟁조정위원회 위원(정통부), 이커머스 클럽 운영위원
※ 관심분야 : 시스템 및 네트워크 정보보호, 전자서명 인증관리체계, 정보보호기술 표준화