인터넷보안기술포럼
(www.istf.or.kr)

이홍섭 • TTA 정보보호기술위원회 위원
인터넷보안기술포럼 의장
한국정보보호진흥원 평가인증사업단 단장

1. 소개

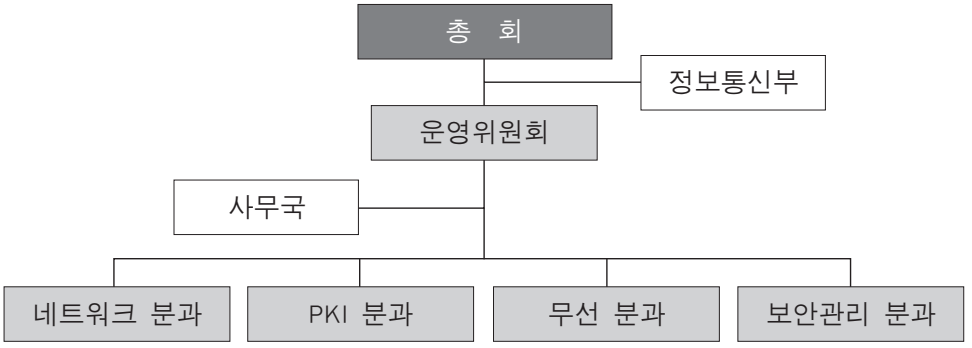
인터넷의 급속한 확산과 더불어 온라인 기반의 개방형 정보통신망에서의 비즈니스 업무처리 비중이 증대됨에 따라 보안면에서도 여러 가지 위험요소가 증가하게 되어, 안전한 인터넷 사용을 위한 인터넷 보안기술과 표준화에 대한 중요성이 그 어느 때보다 부각되고 있다. 인터넷 관련 기술은 발전속도가 매우 빠른 특성으로 이에 대처하는 표준화활동 또한 의사 결정단계나 절차가 복잡한 국제기구나 국가 추진체계보다는, 시장수요에 즉시 대처가 가능한 민간단체가 주도하는 사실표준 활동이 효과적으로서, IETF가 가장 대표적인 사실표준 활동을 수행하고 있다.

이에, 국제적 환경변화에 대응하기 위하여 정보통신부는 2000년부터 인터넷보안기술, IPV6, VoIP, 인터넷정보가전, MPEG 등 30개 정보통신 전략분야를 선정하여, 민간 중심의 포럼을 출범시켜 사실표준에 대한 국제적 동향 대응과 국내실정에 적합한 표준 제정기반을 마련하였다.

인터넷보안기술포럼(Internet Security Technology Forum, ISTF)은 인터넷 보안기술 분야의 솔루션 및 서비스 업체들이 중심이 되어 구성된 민간 포럼으로 인터넷 보안기술 관련 국제 표준화 활동에 공동 대응하고 시장수요를 반영한 사실표준의 개발을 위해 2000년 6월에 창립되었다. 회원사는 정보보호 솔루션, 서비스 업체와 공인인증기관, 그리고 정부출연기관 등 58개사를 중심으로 네트워크, PKI, 무선, 보안관리 등 4개 분과위원회를 구성하여 활동하고 있다.

포럼 조직은 총회, 운영위원회, 분과위원회 그리고 사무국으로 구성된다. 총회는 최고 의결기관으로 모든 회원사가 참여하여 사업 및 예산승인, 의장단 선출 등을 의결하고 운영위원회는 표준안 심의 및 표준제정, 사업 및 예산계획 수립 등을 담당하며, 각 분과위원회는 해당 분야의 사실표준안 개발 및 심의를 담당한다.

- 네트워크 분과 : VPN, IDS, 이메일 보안 등 인터넷 기반 표준 제정
- PKI 분과 : 전자서명 인증서 사용, 관리, 검증 등 PKI 관련 표준 제정
- 무선 분과 : WAP, WTLS 등 무선 보안기반 표준 제정
- 보안관리 분과 : 정보보호 위험분석 및 관리지침, 보안관리 및 대책 등 지침 제정



(그림) 인터넷보안기술포럼 조직도

2. 인터넷보안기술포럼 주요실적

정보보호 제품개발 및 서비스 제공 등 산업부분과 효율적인 시스템 운영 및 관리부분에서 필요한 사실표준 제정을 비롯하여 국내외 인터넷 보안기술 관련 표준 기술정보 제공, 국제표준화 회의 · 포럼 활동 공동대응, 정보보호 제품 상호운용성 연구, 인터넷 보안기술 관련 워크숍외 행사개최 등 여러 부문의 사업을 다각도로 수행하고 있다. 특히 2001년부터 정보통신부가 지원하는 국제표준전문가에 본 포럼 운영위원과 자문교수 등 6명이 선정되어, 포럼의 전문성을 인정받아 지속적으로 IETF Security Area를 중심으로 활동하고 있다.

ㅇ 인터넷 보안기술 관련 사실표준 개발

ISTF는 2000년도에 전자서명 관련 2건의 PKI 표준을 제정하여 공인인증 기관간의 인증서 호환 및 상호 연동을 가능토록 해 공인인증 서비스 활성화에 적지않게 기여하였으며, 2001년도에는 인터넷을 전용선처럼 사용하는 'VPN 표준'과 침입탐지 및 침입차단시스템에 이용되는 'ESM 표준'을 제정하였다. 또한, 올해에는 취약한 전자우편의 보안성을 높이기 위해 '전자우편 보안 국내표준'과 안전한 무선인터넷 서비스 제공을 위해 필요한 '무선 PKI 표준'을 제정하여 공인인증기관, 이동통신사업자, PKI 솔루션업체가 구축한 무선 PKI 시스템에 적용된 상태이다. 최근 전자서명 인증서비스 활성화의 저해 요인으로 조직 및 국가단위로 구축된 PKI 서비스간 상호연동 문제를 시급히 해결하기 위해 마련된 '공인인증 기관간 상호연동 표준'은 국내 공인인증 기관들에서 이 표준에 따라 상호연동을 준비하고 있다.

ㅇ 세미나, 워크숍 등 행사 개최

- 창립총회 및 기술세미나(2000. 6. 30, 상공회의소)
- 제1회 인터넷보안 기술표준 워크숍(2000. 12. 8, 상공회의소)
- 러시아 IT 보안전문가 초청 세미나(2001. 2. 2, 상공회의소)
- IT Forum Korea 2001(2001. 5. 9 ~ 11, COEX)
- 정기총회 개최(2001. 6. 28, 그랜드 인터콘티넨탈 호텔)
- 제2회 인터넷보안기술 표준 워크숍(2001. 12. 4, COEX)
- IT Forum Korea 2002(2002. 4. 23 ~ 25, 르네상스 서울호텔)
- 2002 정기총회(2002. 6. 27, 그랜드 인터컨

〈인터넷보안기술포럼 사실표준 제정현황〉

번호	표준번호	제목	제정날짜	TTA 단체표준
1	ISTF-001	전자서명 인증서 프로파일 표준	2000. 9	TTAS.KO-12.0012
2	ISTF-002	전자서명 인증서 효력정지 및 폐지 목록 프로파일 표준	2000. 10	TTAS.KO-12.0013
3	ISTF-003	IP 계층에서의 VPN 보안기술 표준	2001. 5	TTAS.KO-12.0014
4	ISTF-004	침입차단시스템 로그형식 표준	2001. 5	
5	ISTF-005	침입탐지시스템 로그형식 표준	2001. 5	
6	ISTF-006	암호 메시지 규격 표준	2002. 2	
7	ISTF-007	Diffie-Hellman 키합의 방식 표준	2002. 2	
8	ISTF-008	S/MIME V3 인증서 운영규격 표준	2002. 2	
9	ISTF-009	S/MIME 메시지 명세서 표준	2002. 2	
10	ISTF-010	안전한 전자우편을 위한 보안 서비스 확장 표준	2002. 2	
11	ISTF-011	CMS에서 CAST-128 암호화 알고리즘의 사용 표준	2002. 2	
12	ISTF-012	무선 전자서명 인증서 프로파일 표준	2002. 4	TTAS.KO-12.0016
13	ISTF-013	무선 전자서명 인증서 효력정지 및 폐지목록 프로파일 표준	2002. 4	TTAS.KO-12.0017
14	ISTF-014	무선 WTLS 인증서 프로파일 표준	2002. 4	TTAS.KO-12.0019
15	ISTF-015	무선 전자서명 알고리즘 표준	2002. 4	TTAS.KO-12.0020
16	ISTF-016	무선 키분배 알고리즘 표준	2002. 4	TTAS.KO-12.0021
17	ISTF-017	무선 인증서 요청형식 프로토콜 표준	2002. 4	TTAS.KO-12.0018
18	ISTF-018	공인인증기관간 상호연동을 위한 PKI 표준	2002. 10	

티넨탈 호텔)

- 제3회 인터넷보안 기술표준 워크숍(2002. 12. 3, 잠실 롯데호텔)

○ 관련 국제표준화 회의참석 및 기고문 발표

- IETF 회의참가 및 기고문 발표
  - 무선 인증서 요청형식 프로토콜 규격발표 (2001. 12, 2002. 6)
  - 식별번호를 이용한 본인확인 기술규격 (2002. 11)
- ASTAP 포럼 회의참석 및 표준(안) 기고
  - 전자서명 인증서 및 CRL 프로파일 표준 등 4건(2001. 10)
  - ESM 로그 포맷(2002. 6)

○ 인터넷 보안기술 관련 최신 기술정보의 수집, 분석, 보급 및 활용촉진

3. 활동 계획

향후 분과별 주요사업을 살펴보면, 네트워크 분과에서는 다양한 단일 보안제품 및 솔루션들의 제공 및 구매 추세에서 통합 보안 솔루션을 요구하고 개발하는 추세로 변화됨에 따라, 현재 이미 보유하고 있는 네트워크 보안 표준 규격의 확장을 통한 'ESM 통합 API 표준(안)'을 실무작업반을 구성하여 개발하고 있어, 사용자와 개발자의 편의성을 도모하고자 한다.

PKI, 무선 분과에서는 무선 인증서의 재발급, 폐지, 갱신 등에 관한 무선 인증서 관리 프로토콜 표준과 응용계층 소프트웨어간 단대단 보안프로토콜에 사용될 무선 인증서 응용계층 보안 프로토콜 표준을 심의하고, 지난 4월 제정된(ISTF-017) 무선 인증서 요청형식 프로토콜 표준에 본인확인 기술을 추가하여 개정할 예정이다.

보안관리 분과에서는 관리기관들이 취약점 점검 도구 및 위험분석 도구선정시 활용할 수 있도록 하는 위험 분석도구 선정지침, 네트워크 취약점 점검 도구 선정 지침, 시스템 취약점 점검도구 선정지침을 내년 상반기중 제정을 목표로 추진하고 있다.

4. 결론

정보보호에 대한 표준화는 인터넷의 발전과 더불어 개방적이고 분산된 환경에서 가치있는 정보의 안전한 활용과 정보통신의 신뢰성을 확보하기 위해 어떠한 요소보다도 그 중요성이 강조되어야 할 부분이다. 또한, 글로벌 시대에 살고있는 우리가 보다 집중해야 할 방향은 당연히 국제표준으로, 많은 국내 관계자들이 IETF 등 국제표준화 기구에 지속적으로 참여함으로써, 관련 동향을 분석하고 기고문 발표 등을 통해 적극적으로 대응해야 한다.

이에 따라, 포럼의 운영방향은 국제표준을 고려한 실용적인 사실표준을 지속적으로 제정하고, 제정된 표준의 적극 활용을 위한 관련 기관의 제도적 강구 및 협조요청, 그리고 매체를 통한 홍보를 강화할 예정이다. 더 나아가, 국내에서도 높은 기술력과 많은 업체를 보유하고 있는 PKI와 SMIME 등의 분야에서 국제적으로 경쟁력있는 표준을 개발해 나가는 한편, 적합성 및 제품간 상호운용성 관련 기반구축을 통해 정보보호 표준 준용제품의 상호운용성 확보에 주력할 것이다.

또한 표준 제정활동을 통한 회원사간의 친목을 강화하여 상호협력 도모 등 적극적인 포럼활동을 통해, 궁극적으로는 회원사의 경쟁력 강화와 국내 인터넷 보안 산업활성화, 그리고 국내 정보보호 제품의 국제경쟁력 제고에 일익이 되도록 노력할 것이다.