情 報 保 護 學 會 誌
第 12 券 第 4 號, 2002. 8

국내 정보보호 표준화 추진 체계

민 준 기*, 진 병 문*

요 약

초고속정보통신망 및 서비스의 발달로 정보통신에서의 정보보호는 점차 그 중요도가 증대되고있다. 본 고에서는 정보보호의 중요성과 국내 정보보호 표준화 추진 현황을 언급하고 정보보호 기술에 대한 표준화 추진 체계와 한국정보통신표준(KICS) 제정 및 향후 정보보호 표준화 추진 방향에 대하여 언급한다.

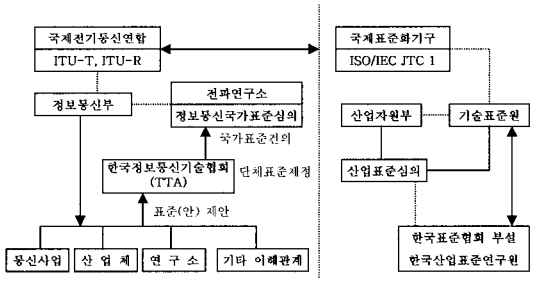
Ⅰ. 서 론

우리나라의 인터넷 보급률은 아시아 1위이며, 우리의 초고속망 인프라 또한 세계적인 수준으로서 우리는 언제, 어디서나 인터넷을 이용하여 필요한 정보를 주고 받을 수 있게 되었다. 우리는 인터넷을 기반으로 하는 정보의 홍수 시대에 살고있으며 이들 정보의 가치가 점차 높아짐에 따라 정보보호의 중요성도 점차 증대되고 있다. 이에 정보통신표준기술의 개발을 주도하는 정보통신부와 한국정보통신기술협회(TTA)에서는 개인 및 국가의 정보를 보호하여 정보의 파손과 유출을 원천적으로 봉쇄할 수 있는 정보보호 기술에 대한 표준 개발에 노력을 경주하고 있다.

II. 국내 정보통신 표준화 추진 체계

1. 국내 표준화 추진체계

정보통신부는 정보통신 표준화 정책 및 정보통신 국가 표준화를 추진하는 최고의 기관으로서 국제표준화기구인 ITU-T, ITU-R의 활동을 주도하고 있으며, 정보통신 분야의 국가표준인 한국정보통신표준(KICS)을 채택하고 고시하는 권한을 가지고 있으며, 정보통신 표준화 정책을 수립하여 추진하고 있다. 이에 따라, 전파연구소는 국가표준화 추진에 대한 기술적, 전문적 뒷받침을 수행하는 기관으로 정보통신국가표준심의회를 운영하고 있다. 한국정보통신기술협회는 통신사업자, 산업체, 연구소, 학교 및 기타 전문가들로 표준화 기술위원회를 구성하여 정보통신기술 관련 표준개발에 역점을 두고있다. 산업자원부, 기술표준원은 산업표준의 집행기관으로 산업표준을 제정하고 이를 보급하기 위하여 한국산업규격(KS)표시 허가제를 운영하고, ISO/IEC JTC1 등 국제표준화기구의 활동에 참여하고있다 (그림 1).



〔그림 1〕 국내정보통신표준화 추진체계

2. 정보통신분야 표준 제정절차

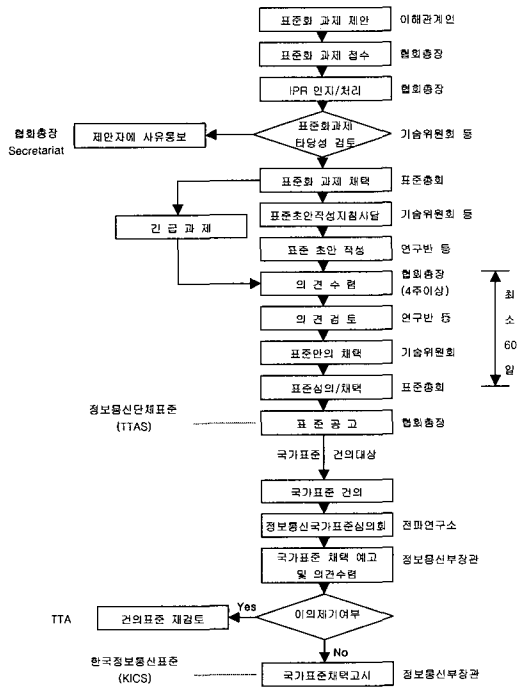
정보통신에 관련된 국가표준은 정보통신부에서 주관하는 한국정보통신표준과 산업자원부에서 주관하는 한국산업표준(KS)중 정보통신분야 표준으로 나뉘어지며, 이들 각각의 제정 절차는 다음과 같다.

2.1 한국정보통신표준 (KICS)

KICS 표준의 제정절차는 다음과 같다. 우선 정보통신분야 표준에 관하여 이해관계를 가진 개인 및

* 한국정보통신기술협회({Jakimin, bmchin}@tta.or.kr)

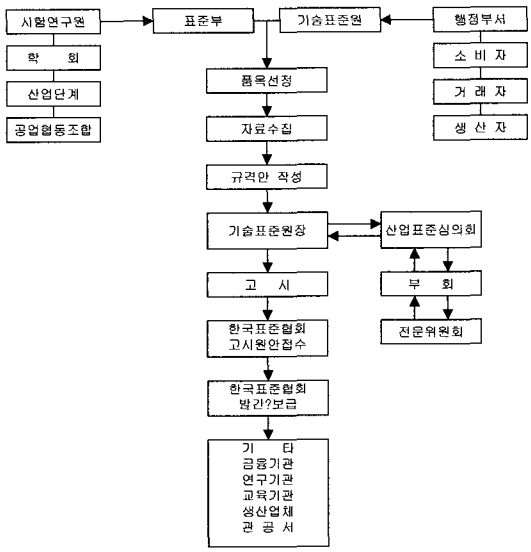
단체는 TTA로 표준제정, 개정등에 관한 과제제안을 한다. 이후, TTA는 제안 접수된 과제에 대하여 표준화의 타당성을 검토하여 표준화 과제 채택 여부를 결정한 후 관련 기술위원회로 표준개발을 의뢰한다. 관련 기술전문가로 구성된 해당 기술위원회는 최적의 품질을 보장할 수 있는 표준의 적용 범위, 표준의 목적 및 기대효과 등의 내용을 포함한 표준 초안을 작성한 후 사업 참가자, 산·학·연 기술 전문가, 관련 기관에 4주간의 의견 수렴을 실시한다. 이후 이해 당사자들의 이의 제기가 없을 경우 표준총회를 개최하여 정보통신단체표준(TTAS)으로 채택한다. 또한 다수의 통신사업자, 산업체간의 호환성 및 상호운용성을 확보하기 위해 국가차원 표준의 제정 등이 필요한 경우이거나 국내 개발 기술로서 국제 표준화 기구에 표준으로 제안된 경우에는 정보통신부장관에게 국가표준으로 건의하여 60일간의 의견수렴을 거쳐 국가 표준인 한국정보통신표준(KICS)으로 채택한다(그림 2).



〔그림 2〕 한국정보통신표준 제정 절차

2.2 한국산업표준 (KS)

한국산업표준(KS)의 제정 및 개정은 산업자원부에서 주관하며 업계, 대학, 연구기관, 관련단체 및 소비자 등 관련 당사자들이 참여하는 표준심의회를 거쳐 표준을 제정한다. 제정된 표준은 5년마다 검토되며 관련기술의 변화는 기술수준의 향상 내용을 반영하여 개정하고, 산업표준심의회는 산업표준화법에 의거하여 한국산업규격의 제정, 개정, 확인 및 기타 산업 표준화 업무의 자문 역할을 수행하고 있으며, 부회, 전문위원회로 구성되어 있다 (그림 3).



〔그림 3〕 한국산업표준 제정 절차

III. 국내 정보보호 표준화 현황

정보보호 분야의 표준개발을 위하여 한국정보통신기술협회의 정보통신표준총회 산하에는 약 60명이 참여하는 정보보호기술위원회(TC10)를 두고 있으며, 그 산하에는 정보보호관리연구반, 암호기술연구반, 시스템 및 네트워크보안연구반등이 구성되어 표준개발 활동을 전개중에 있으며, TC10에서의 금년도에 18개의 표준화 과제를 추진하고 있으며 이들 현황은 표 1과 같다. 한편 현재까지 제정된 정보보호 분야의 TTA 단 표준은 총 31건으로 그 내용은 다음 표 2와 같다.

〔표 1〕 2002년도 정보보호기술위원회(TC10) 표준화과제 추진현황

2002년 7월 현재

No.	과 제 명	담당연구반	진행상태	관련국제표준
1	정보보호 전문용어 표준(개정)	정보보호 관리연구반	초안작성중	고유표준
2	공공기관 전산보안정책 수립을 위한 지침서(개정)		과제채택	
3	암호키관리 체계 표준	암호기술 연구반	초안작성중	ISO/IEC 11770-1,-2
4	가변길이 해쉬함수 표준		초안작성중	ISO 10118
5	KCDSA 전자서명 알고리즘 구현 방법론 표준(안)		초안작성중	
6	영지식 기법을 이용한 실체인증 기술 표준(안)		초안작성중	ISO 9798
7	전자서명을 이용한 실체인증 기술 표준(안)		초안작성중	ISO 9798
8	암호 메시지 규격		초안작성중	
9	Diffie-Hellman 키합의 방식		초안작성중	
10	CMS에서 CAST-128 암호화 알고리즘의 사용(안)		초안작성중	
11	S/MIME V3 인증서 운영 규격		초안작성중	
12	전자서명 인증관리체계 인증서 검증 절차 표준(안)	시스템및 네트워크 보안연구반	초안작성중	RFC 2510
13	전자서명 인증관리체계 DN 규격(안)		초안작성중	
14	온라인 인증서 상태 확인 프로토콜 표준		과제채택	
15	시점확인(Time stamp) 프로토콜 표준		과제채택	
16	디렉토리 시스템 인증 프레임워크(개정)		과제채택	
17	S/MIME 메시지 명세서		초안작성중	
18	안전한 전자우편을 위한 보안 서비스 확장		초안작성중	

〔표 2〕 정보보호분야 TTA단체표준 현황

2002년 7월 현재

No.	표준번호	표 준 명	제/개정 년도	표준내용 요약
1	TTAE.IS-15408.1	정보기술 보안성 평가기준-제1부: 소개 및 일반모델	2001	정보 기술 보안성 평가 기준인 ISO/IEC 15408-1의 국내 표준
2	TTAE.IS-15408.2	정보기술 보안성 평가기준-제 2부 : 보안기능 요구사항	2001	정보기술 보안성 평가기준인 ISO/IEC 15408-2의 국내 표준
3	TTAE.IS-15408.3	정보기술 보안성 평가기준-제 3부 : 보안보증 요구사항	2001	정보기술 보안성 평가기준인 ISO/IEC 15408-3의 국내 표준
4	TTAS.IS-10181.4	개방시스템 상호접속 - 개방시스템에서의 보안 골격 - 제4부 : 부인 방지	1999	부인 방지 서비스 규정 관련 표준
5	TTAS.IS-17799	정보보호관리 표준	2002	조직이 체계적이고 효율적으로 정보보호를 관리할 수 있는 공통적인 모델
6	TTAS.IT-X509	디렉토리 기본표준 ; 인증골격	1993	디렉토리의 기능, 디렉토리 모형, 인증 서비스의 제공
7	TTAS.IT-X509/R1	개방시스템상호접속-등록부 표준(1993) : 인증골격(개정)	1995	디렉토리의 기능, 디렉토리 모형, 인증 서비스의 제공
8	TTAS.IT-X509/R2	디렉토리시스템 인증 프레임워크 표준	2000	디렉토리의 기능, 디렉토리 모형, 인증 서비스의 제공
9	TTAS.KO-12.0001	부가형 전자서명 방식 표준 - 제2부 : 확인서 이용 전자서명 알고리즘	1998	부가형 전자서명 알고리즘 (KCSDA : KOREAN CERTIFICATE BASED DIGITAL SIGNATURE ALGORITHM)을 규정

No.	표준번호	표 준 명	제/개정 년도	표준내용 요약
10	TTAS.KO-12.0001/R1	부가형 전자서명 방식 표준-제 2 부 : 인증서 기반 전자서명 알고리즘	2000	부가형 전자서명 알고리즘(KCSDA : KOREAN CERTIFICATE BASED DIGITAL SIGNATURE ALGORITHM)을 규정
11	TTAS.KO-12.0002	정보보호기술 전문용어 표준	1998	정보보호 기술의 주요 용어 표준
12	TTAS.KO-12.0003	침입차단시스템 선정 지침	1999	외부의 정보통신망 간에 교환되는 데이터를 안전하고 비용 효율적으로 통제하기 위한 지침
13	TTAS.KO-12.0004	128비트 블록 암호 알고리즘 표준	1999	정보처리시스템 및 정보통신망 환경에서 임의의 키(비밀키)를 사용하여 블록단위로 데이터를 변환하는 암호알고리즘
14	TTAS.KO-12.0005	암호학적 확인함수를 이용한 실체인증 기술 표준	1999	다양한 응용의 정당성을 증명하기 위한 암호학적 확인함수를 이용한 실체인증 기술
15	TTAS.KO-12.0006	대칭형 암호화 기법을 이용한 실체인증 기술 표준	1999	대칭형 암호화 기법을 이용한 실체인증 기술
16	TTAS.KO-12.0007	공공정보시스템 보안을 위한 위험분석 표준 - 위험분석 방법론 모델	2000	정보시스템 환경에 맞는 위험관리 및 위험분석
17	TTAS.KO-12.0008	공공기관 정보시스템 구축준비 단계의 보안지침서	2000	정보시스템 구축시 보안 고려 사항
18	TTAS.KO-12.0009	공공기관 정보시스템을 위한 비상계획 및 재해복구에 관한 지침서	2000	정보시스템 관련 업무의 비상계획 및 재해복구에 관한 실무에 응용 가능한 방법론
19	TTAS.KO-12.0010	컴퓨터 바이러스 방지지침	2000	PC 환경에서 일반적인 컴퓨터 사용자나 관리자가 컴퓨터 바이러스 감염 방지를 위한 지침
20	TTAS.KO-12.0011	해쉬함수표준-제2부 : 해쉬함수알고리즘 표준 (HAS-160)	1998	해쉬알고리즘 표준 (HAS-160)
21	TTAS.KO-12.0011/R1	해쉬함수표준-제2부 : 해쉬함수알고리즘 표준(HAS-160)	2000	해쉬알고리즘 개정 표준(HAS-160)
22	TTAS.KO-12.0012	전자서명 인증서 프로파일 표준	2000	전자 서명용 인증서 프로파일에 대한 규격
23	TTAS.KO-12.0013	전자서명 인증서 효력정지 및 폐지 목록 프로파일 표준	2001	전자서명 인증관리체계 내에서의 인증서 효력정지 및 폐지 목록 생성
24	TTAS.KO-12.0014	IP 계층에서의 VPN 보안기술 표준	2001	IP 계층과 응용계층에서 가상 사설망을 구현하기 위한 보안 요소 기술과 프로토콜들
25	TTAS.KO-12.0015	부가형 전자서명 방식 표준-제3부 : 타원곡선을 이용한 인증서 기반 전자서명 알고리즘	2001	부가형 전자서명 알고리즘인 KCDSA (Korean Certificate-based Digital Signature Algorithm)를 타원곡선을 이용한 전자서명 알고리즘으로 변형한 표준
26	TTAS.KO-12.0016	무선 전자서명 인증서 프로파일 표준	2002	무선 전자서명용 인증서 프로파일에 대한 규격
27	TTAS.KO-12.0017	무선 전자서명 인증서 효력정지 및 폐지 목록 프로파일 표준	2002	무선 전자서명용 인증서 효력정지 및 폐지 목록 프로파일.
28	TTAS.KO-12.0018	무선 인증서 요청형식 프로토콜 표준	2002	무선 인증서 요청형식 프로토콜
29	TTAS.KO-12.0019	무선 WTLS 인증서 프로파일 표준	2002	WTLS 인증서 생성 및 인증서 처리
30	TTAS.KO-12.0020	무선 키 분배 알고리즘 표준	2002	무선 키 분배 알고리즘.
31	TTAS.KO-12.0021	무선 전자서명 알고리즘 표준	2002	무선 전자서명용 알고리즘 프로파일

IV. 국내 정보보호기술 표준화 추진 체계

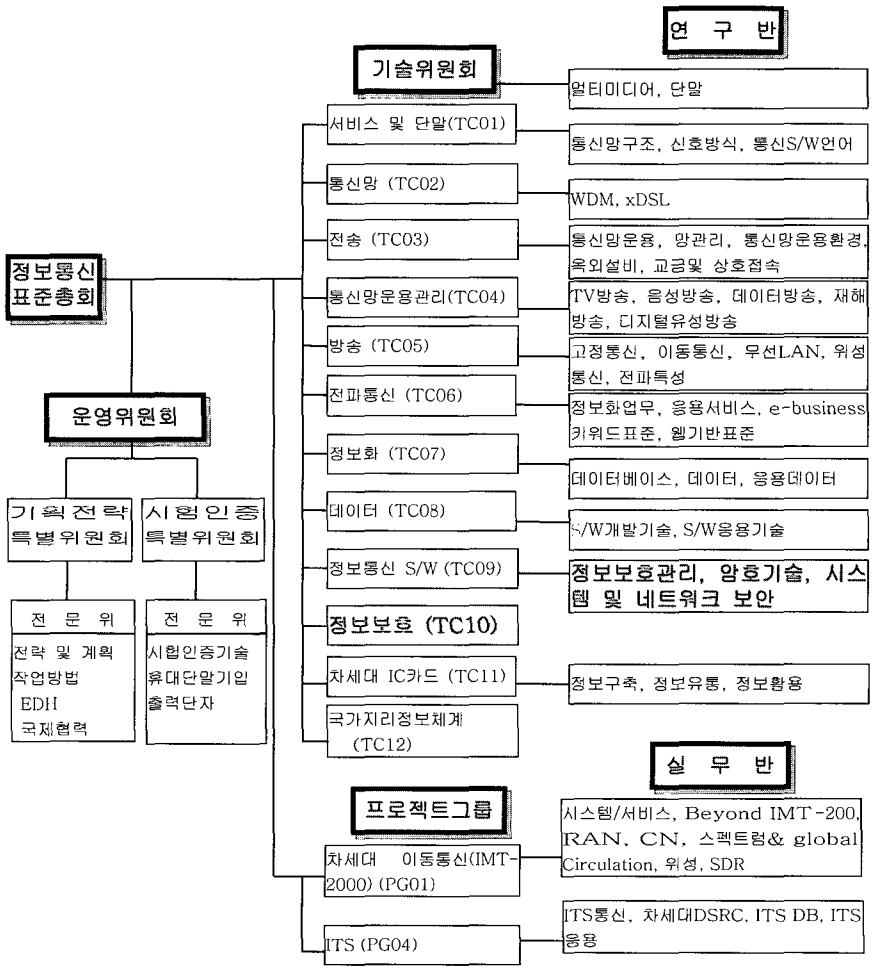
컴퓨터 및 정보통신 기술의 발달, 인터넷 사용 인구의 급증에 따라 이전에 예상하지 못했던 정보보호의 취약성이 급속히 나타나고 있다. 이러한 전자 거래 정보의 유출과 부정한 사용 등은 개별적인 피해뿐만 아니라 민간 및 공공기간, 국가 전체에 커다란 피해를 주고 있다. 이러한 피해는 미래지식정보화 사회의 발전을 지연시키고 국가 경쟁력을 약화시킨다는 점에서 심각한 문제를 야기시키고 있다. 이러한 제반 문제점을 미연에 방지키 위하여 정보보호 표준의 신속한 제정이 필요하다. 이제 정보통신기술협회에서는 정보보호기술위원회와 산하 연구반 조직을 그림 4와 같이 상설화하여 정보보호표준의 개발을 추진하고 있다.

V. 정보보호관련 국가표준화 추진방안

각 국가는 국가 사회의 모든 분야에서 국가적 차원에서 준용하여야 할 과학적·기술적 공공기준을 만들어 국가표준으로 채택하고있다. 국가표준 중에서도 정보보호 분야의 국가표준은 그 역할이 매우 중요하다.

앞에서도 언급한 바와 같이 우리나라의 국가표준으로는 정보통신부의 한국정보통신 표준(KICS)과 산업자원부의 한국산업표준 (KS)이 존재한다.

최근 정보보호진흥원에서 개발된 "128비트 블록 암호 알고리즘(SEED) 표준 (안)"을 대상으로 상기 2개 부처가 국가 표준으로 제정하는 방향에 대하여 서로 다른 입장을 보이고 있다. 본 SEED 표준은 ISO/IEC JTC1/SC27/WG2에서 국제 표준의 채



〔그림 4〕 한국정보통신기술협회 표준 개발 조직

택여부를 검토 중에 있으나 아직도 우리나라에는 이에 해당되는 국가 표준은 없는 실정이다.

산업자원부에서는 ISO의 National Body로서 해당 표준이 국제 표준으로 채택된 후에 산업표준 규격(KS)으로 제정해야 한다는 입장이며, 정보통신부에서는 해당표준의 제정이 시급하므로 우선 KICS로 제정한 후에 해당되는 표준이 국제표준으로 채택되면 그 후에 KS화 여부를 검토하겠다는 입장을 보이고 있다.

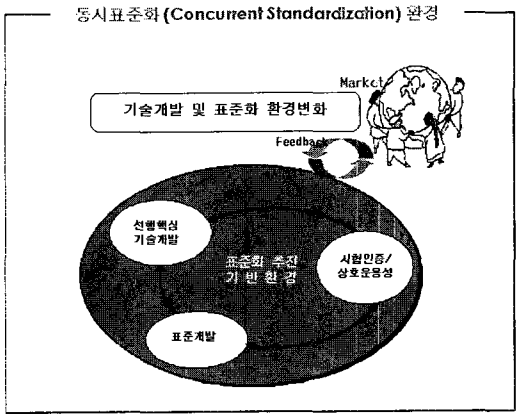
이러한 부분적 입장 차이는 기본적으로 2 부처간의 원만한 협의를 통하여 해결되어야 할 문제이지만, 산업자원부가 단지 ISO의 창구라는 입장에서 정보통신에 관련된 분야의 표준화까지도 모두 주도하려는 것은 근본적으로 여러 문제를 야기시킬 소지가 있다. 산업자원부로서는 ISO와 관련된 농업, 건축, 환경 등 전 분야의 표준을 모두 직접 다룰 수 없듯이 정보통신분야의 표준화는 정보통신부에 위임하고 ISO와의 창구 역할 및 각 부처에서 제정되는 표준들간의 조정에 노력을 집중하는 것이 바람직할 것이다.

특히, 최근 우리나라가 IT정보 강국 위치에 오를 수 있게 된 것은 최근 수년간 정보통신부에서 정보통신기술의 연구개발에 집중적으로 많은 투자를 한 결과와 무관치 않을 것이다. 정보기술의 한 부분인 정보 보호도 통신망을 근간으로 하여 정보의 보호관리, 정보의 암호화, 시스템 및 네트워크 보안이 주축이 되는 것이기 때문에 정보통신부 주도로 원천기술을 연구 개발함과 아울러 해당되는 표준도 한국정보통신표준(KICS)으로 신속히 제정하여 정보보호와 관련하여 발생 가능한 문제점들을 국가적 차원에서 사전에 예방하고 방지 할 수 있는 기반을 마련하여야 할 것이다.

VI. 결 론

우리가 표준화를 추진하는 궁극적인 목적은 우리 원천기술의 표준화를 통하여 해당 원천기술과 관련하여 우리가 확보한 지적재산권을 표준과 연계시킴으로써 해당 분야의 세계시장을 선점하는 것이다.

정보통신부에서는 사이버 테러 대응방안, 전자서명 인증 및 암호이용 활성화 방안, 개인정보보호 방안, 정보통신윤리 확립 방안, 정보보호 산업육성 등의 정보보호 관련 방안 등을 마련하였고, 정보보호 기반 기술의 연구개발 및 표준화를 강력히 추진하고 있다. 한편, 정보보호 관련 선행 핵심 기술의 개발과 표준 개발, 개발된 표준에 대한 시험인증 활동이 유기적으로 결합되는 동시 표준화 환경을 그림 5와 같이 조성하여 적시에 적용 가능한 정보보호 관련 표준을 한국정보통신표준(KICS)으로 조기에 제정해야 할 것이다. 정보 기술의 국제 표준화도 UN산하의 ITU(국제전기통신연합)와 민간 국제기구인 ISO(JTC1)가 상호 협력하여 긴밀하게 표준화가 추진되고 있으며, 양 기관에서는 정보기술 표준 제정시 공동 표준안을 작성하여 양 기관의 번호체계만 달리한 공동 표준으로 제정하고 있는 상황이다. 지금 지식정보화사회로 이행되어 가는 과정에서 총성 없는 전쟁터인 IT 분야에서 세계 대전이 벌어지고 있다. 미래의 지식 정보화 사회는 어느 누구도 아직 가보지 못한 미지 의 세계이다. 우리 내부의 다툼을 멈추고 바깥을 보며 부처간에 힘을 합쳐 나아간 다면 정보화 사회에서의 우리나라의 미래는 매우 밝다고 하겠다.



〔그림 5〕 동시 표준화 환경

참고문헌

〔1〕 TTA, "2001년도 정보통신표준화 백서," 2001
〔2〕 한국정보보호센터편, "정보보호 개론," 교우사, 2000
〔3〕 디지털 타임즈 2002. 6.
〔4〕 http://www.tta.or.kr
〔5〕 http://www.etri.re.kr
〔6〕 http://www.kisa.or.kr

〈著者紹介〉

민 준 기 (Jun-Ki Min)

1991년 2월 : 한남대학교 대학원 전자계산공학과 석사
1980년 8월~1999년 6월 : 한국전자통신연구원 근무
1999년 7월~2001년 5월 : 로커스 정보통신연구소 근무
1993년~1999년 : 대덕대학, 혜천대학, 우송대학(정보통신이론, 객체지향언어, 사무자동화 관련) 강의
2001년 7월~현재 : 한국정보통신기술협회 정보기술팀 팀장

진 병 문 (Byoung-Mun Chin)

본호의 "ITU SPU 정보보호 워크샵 보고" 저자 소개 참조.