정보보안 기술의 국제표준화

최근 우리나라도 정보화 사회에 접어들면서 컴퓨터와 정보통신기술의 발달에 힘입어 국가 5대 기간전산망을 비롯한 각종 전산망을 이용하여 사회 각분야에서 수많은 정보를 유통시키고 있다. 그리고 최근 정보화 개념의 급속한 확산과 개인용컴퓨터 사용의 폭발적인 증가로 인터넷이나 일반 VAN등을 이용한 정보의 교환이 활발하게 이루어지고 있다.

이 경 석 산업연구원 전산실장

정보보안 기술개요

최근 우리나라도 정보화 사회에 접어들면서 컴퓨터와 정보통신기술의 발달에 힘입어 국가 5대 기간전산망을 비롯한 각종 전산망을 이용하여 사회 각분야에서 수많은 정보를 유통시키고 있다. 그리고 최근 정보화 개념의 급속한 확산과 개인용컴퓨터 사용의 폭발적인 증가로 인터넷이나 일반 VAN등을 이용한 정보의 교환이 활발하게 이루어지고 있다.

이처럼 컴퓨터를 이용하여 각종 정보를 언제 어디서나 손쉽게 이용할 수 있게 됨에 따라 발생되어지는 정보보안에 관련된 문제점들이 점차 증가하고 있는 추세이다. 즉, 컴퓨터 전산망을 통한 주요 정보의 이용도가 점점 높아짐에 따라 보안이 필요한 데이터를 파괴, 변조 및 무단 사용하는 등이 각종 정보보안에 관련된 컴퓨터 역기능들이 증가하고 있는 추세여서 전산망에서의 정보보안이 심각한 사회문제로 대두되고 있다. 현재 정부나 민간 분야에서 다양한 용도로 전산화를 추진하고 각종 전산망을 통하여 막대한 량의 정보를 유통시키고 있다. 이러한 정보화 사회에서의 정보보안이란 비밀 유지가 필요한 주요 정보를 정보관련 제반 사고로부터 정보자산을 보호하는 것이다. 일반적으로 정보보안이란 전산망을 통해 흘러가는 정보나 컴퓨터에 보관되어 있는 정보가 사용자의 과실이나 제3자의 부정행위 및 자연재해등에 의하여 손상되는 것을 방지하기 위한 여러가지 형태의 대책을 의미한다.

이러한 정보보안의 가장 큰 과제로는 정보의 안정성과, 정보 사용자에 대한 신뢰성을 들 수 있다. 그리고 최근 정보전송형태가 복잡 다양화 되어감에 따라 제3자에 의한 침해 행위뿐만 아니라, 통신 당사자간의 여러 형태의 부정행위에 대해서도 정보와 정당한 사용자를 보호할 수 있는 수단이 요구되고 있다.

그리고 정보화사회에서 사용자 상호간의 정보의 유통은 더욱 더 다양해 질 것이며, 안전한 정보전달을 위한 전산망에서의 정보보안 기술은 필수불가결한 요인으로 인식되고 있다. 전산망 이용의 급격한 증가로 최근에는 정보보안이 새로운 이슈로 떠오르고 있으며, 이러한 정보의 역작용에 대한 전산망에서의 주요한 보안기술로 개체인증(Entity Authenticaion), 부인봉쇄(Non-Repudiation), 디지털서명(Digital Signature), 해쉬함수(Hash Functions), 키관리(Key Management), 정보기술 보안관리 지침서(Guidelines For The Management of IT security), 정보기술 보안의 평가기준(Evaluation Criteria For IT Security), … 등이 있다.

본고에서는 국제적인 정보기술의 보안기술 표준화 활동인 ISO/IEC JTC1/SC27에서의 작업을 중심으로 정보보안 기술과 국내의 표준화 동향 및 국내 보안관련 표준화의 효율적인 추진방안에 대하여 서술하였다.

정보보안 기술의 필요성

컴퓨터를 이용한 데이터 통신에서의 정보보호에는 컴퓨터의 하드웨어나 소프트웨어 혹은 컴퓨터 관련시설 및 전산업무에 종사하는 요원등에 의한 정보외적인 위험요소가 있다. 그리고 정보보안은 군에서의 정보 송수신은 물론이고 국가간의 외교문서 교환에도 커다란 비중을 차지하고 있으며, 근래에는 기업에서도 국제경쟁력과 동종 기업간의 경쟁에서 우위를 확보하기 위하여 정보보안 유지가 반드시 필요한 주요 요소중의 하나이다. 그러나 기업내에서 발생하는 정보보안과 관련된 보안범죄는 기업의 대외 신용도에 직접적이고 커다란 영향을 미치기 때문에 대부분이 외부에 공표되지 않는 것이 특징이다.

특히 근래에는 컴퓨터와 각종 통신매체가 발달하고 전국적인 전산망이 구축되어 정보의 이용이 점차 대중화·다양화되면서 컴퓨터를 이용한 범죄의 실행기회가 증가하고 있다. 그러나 컴퓨터와 정보통신망의 확산으로 발생되고 있는 불법적인 정보의 이용, 유출, 파괴…등의 정보보안 관련범죄를 억제하기 위한 노력이 매우 미약한 실정이다. 한편, 개인의 각종 데이터가 저장되어 그 정보의 이용도가 점점 높아짐에 따라 사기, 절도, 개인의 프라이버시 침해등의 각종 컴퓨터 역기능들이 증가하고 있는 추세여서 정보보안이 심각한 사회문제로 대두되고 있다.

그리고 컴퓨터와 통신망의 부정사용으로 인한 정보보안 문제의 심각성을 살펴보면 전국 규모의 각종 선거에서 개표조작 가능성과 각종 컴퓨터 바이러스에 의한 정보통신망의 파괴 행위 및 각종 대형 금융사고 등으로서 경제적이나 사회적으로 파급효과 매우 큰 사안들이다. 정보보안의 문제는 정보가 기억매체에 보관중인 경우와 정보가 장소이동을 위하여 전송중인 2가지 경우로 나누어 생각할 수 있다. 여기서 어느 경우든 정보보호를 위하여는 우선 정보에 물리적으로 접근하는 것을 차단하는 것이 가장 중요하며, 만일 완벽하게 정보에의 접근을 차단할 수 있다면 정보보호 문제는 해결되었다고 할 수 있다. 그러나 정보가 장소이동이라는 요소를 포함하게 되면 문제가 훨씬 복잡하고 다양해지며, 이런 경우에는 물리적 접근제어가 거의 불가능해지므로 암호화 기법을 정보보안 수단으로 사용하여야 한다.

국제보안기술 표준화 작업

불법적인 사용자가 패스워드를 도용하거나 액세스 제어시스템의 통제를 피하여 주요 데이터를 탈취하였을 경우, 불법적으로 탈취된 그 데이터에 대한 보안을 유지시킬 수 있는 마지막 방안은 데이터 자체에 대하여 암호화시키는 것이다. 이러한 암호기법은 특히 컴퓨터 통신망을 통한 주요 정보의 송수신시에 발생하는 범죄의 예방을 위하여 반드시 필요한 기법이며, 컴퓨터 통신망을 이용한 정보의 송수신 과정에서의 보안문제는 정보 외적인 위험 요소와 정보자체에서 발생되는 위험요소로 구분할 수 있다.

컴퓨터와 통신기술의 발달로 정보화사회로 진입을 앞당겼으며, 각종 데이터의 공유와 전산망의 효율을 높이기 위하여는 망간의 상호연동이 필요한 실정이다. 이러한 전산망의 상호접속에서 반드시 갖추어야 할 요소가 보안시스템의 구축이며, 이를 위한 주요 선진국 및 보안관련 국제표준화 동향 분석이 선행되어야 한다. 본 장에서는 현재 진행중인 국제적인 보안기술의 표준화 작업 내용을 파악하기 위하여 ISO/IEC JTC1/SC27의 표준화 진척현황을 조사 분석하였다. JTC1/SC27은 국제표준화 기구인 ISO (International Organization for Standardization)와 국제전기기술위원회인 IEC(International Electrotechnical Commission) 산하에서 가장 대표적으로 보안에 관련된 표준화 활동을 공동으로 수행하고 있는 소위원회이다.

국제표준화기구(ISO)

1942년에 발족된 ISO는 스위스 제네바에 본부가 있으며, 각국의 제품과 각종서비스의 용이한 국제교류 및 각 분야에서의 국제간 협력증진을 위하여 여러가지 표준화와 관련된 활동을 하고 있다. ISO의 주

요 활동에는 국제표준(IS ; International Standard)의 제정, 배포, 관련업무의 정보교환 그리고 기타 표준화와 연관된 국제기구와의 협의 및 조정 등이다. 현재 ISO는 이사회와 179개의 기술위원회(TC ; Technical Committee) 및 620개의 분과위원회(SC ; Sub Committee) 등으로 나뉘어 활동중이다.

한편, 국제규격인 IS는 분과위원회 산하의 작업그룹(WG ; Working Group)이나 SC를 거쳐 TC등에서 작성된 국제규격안(DIS ; Draft International Standard)을 이사회의 최종심의를 거쳐 IS로 확정되며, IS의 일반적인 제정절차는 다음과 같다.

1) NP 결정 : 기술위원회(TC) 간사국에서 IS 심의항목을 제안하고, 연구기간(SP ; Study Period)을 거쳐 심의하여 새로운 과제(NP ; New Project)로 설정여부를 결정한다.
2) WD 작성 : NP로 결정되면 과제번호가 주어지고, 관련 WG에 배당되어 편집자의 책임하에 작업초안(WD ; Working Draft)을 작성한다. 한편, NP로 결정되지 않고 SP가 연장되는 '진행중인 작업'(OW ; Ongoing Work) 형태도 있다.
3) CD 작성 : WD의 내용을 분과위원회에서 여러번의 수정과 보완작업을 거쳐 위원회초안(CD ; Committee Draft)을 만든다.
4) DIS 작성 : CD 상태의 문서를 회원국들에 회람시켜 수정과 보완작업을 통해 국제표준초안(DIS)을 작성하여 회원국들의 투표에 붙인다.
5) IS 채택 : DIS의 내용을 회원국 75% 이상의 동의를 얻으면 국제표준(IS)으로 확정된다.

국제전기기술위원회(IEC)

IEC는 전기 및 전자분야의 표준화에 관련된 업무를 수행하기 위하여 1908년 10월에 발족된 국제전기기술위원회로서 본부는 스위스 제네바에 있다. IEC는 이사회 산하에 81개의 전문위원회(TC)와 128개의 분과위원회(SC)가 구성되어 있으며, IEC의 규격은 SC나 TC의 회의를 거쳐 편집위원회(EC)에서 작성된 최종규격안(Final Draft)이 투표에서 20% 이상의 반대가 없으면 IEC 규격으로 채택된다.

최근 ISO와 IEC의 표준화 업무중에서 관련기술의 중복분야가 발생하기 시가하였으며, 이러한 문제를 해결하기 위한 공동위원회(ISO/IEC JTC1)가 1987년 11월에 구성되었다.

즉, ISO의 정보처리시스템 기술위원회(TC97 ; Information Processing Systems)와 IEC의 정보기술장비 기술위원회(TC83 ; Information Technology Equipment) 소속 마이크로프로세서시스템 분과위원회(SC47B ; Microprocessor Systems) 업무를 통합한 공동위원회(JTC1 ; Joint Technical Committee 1)가 만들어졌다.

ISO/IEC JTC1/SC27

정보기술(Information Technology)의 전세계적인 표준화를 위하여 1987년 11월 ISO와 IEC는 첫번째의 공동기술위원회(JTC1)를 구성하였으며, 1989년의 ISO/IEC JTC1 총회에서 암호학 기술(Cryptographic Techniques)을 다루는 JTC1/SC27이 탄생되었다.

그리고 현재 JTC1 산하에는 19개의 소위원회(SC)들이 활동중이다. 그리고 SC27은 1990년 4월에 스웨덴에서 제1차 SC27 총회를 열었으며 우리나라도 1992년에 가입하여 1993년부터 "P"회원으로 활동중이고, 1995년 11월에 총회와 작업그룹(Working Group) 회의는 서울에서 개최되었었다. SC27은 정보기술의 보안사항중 보안관련 서비스와 지침 및 일반적인 요구사항, 보안기술과 기법, 그리고 보안평가 기준등의 연구분석과 표준화 작업을 수행한다. 현재 JTC1/SC27에서 운영하고 있는 3개 작업그룹(WG)의 표준화 담당분야(Project 번호)는 다음과 같다.

1) WG1(Requirements, Security Services and Guidelines) ; 정보기술 보안서비스의 요구조건, 보안기술의 관리와 이용지침 개발 및 운영방식등에 대한 표준화 작업을 수행하고 있다.
   - 개체인증 메카니즘, 제1부 : 일반모델(27.03.01)
   - 암호 알골리즘의 등록을 위한 절차(27.10)
   - 보안 정보 객체(27.13)
   - 정보기술(IT) 보안의 관리 지침, 제1부 : IT 보안의 개념과 모델(27.14.01)

제2부 : IT 보안의 관리 및 계획(27.14.02)
제3부 : IT 보안의 관리기술(27.14.03)
제4부 : 최소의 보안 요구사항(27.14.04)
제5부 : IT 보안 서비스와 메카니즘 응용 관련사항(27.14.05)
- 키 관리, 제1부 : 골격(27.18.01)
- 믿을 수 있는 제3자 서비스의 사용과 관리 지침
제1부 : 일반 개요(27.19.01)
제2부 : 기술적 측면(27.19.02)

2) WG 2(Security Techniques And Mechanisms) ; SC20의 '암호화 기술'의 업무중에서 암호 알리고즘 자체의 표준화를 제외한 부분을 인계 받아 보안기술 자체의 표준화 작업을 수행하고 있다. 즉, WG1의 보안서비스 구현을 위한 다양한 보안기술과 관련된 여러 메커니즘의 표준화 작업과 비암호 방식의 보안기술도 취급하고 있다.
- 64 비트 블록암호 알고리즘 운영모드(27.01)
- n 비트 블록암호 알고리즘 운영모드(27.02)
- 개체인증
제2부 : 대칭형 암호기술을 이용함 메카니즘(27.03.02)
제3부 : 공개키 알고리즘을 이용한 개인인증(27.03.03)
제4주 : 암호학적 검산함수를 이용한 메카니즘(27.03.04)
제5부 : 영지식 기술을 이용한 메카니즘(27.03.05)
- 블록암호 알고리즘을 사용하는 검사함수를 이용한 데이터 무결성 기법(27.04)
- 부인봉쇄 기법
제1부 : 일반모델(27.06.01)
제2부 : 대칭형 기술사용(27.06.02)
제3부 : 비대칭형 기술사용(27.06.03)
- 메시지 복원형 디지털 서명 방식
제1부 : 잉여치를 이용한 메카니즘(27.07.01)
제2부 : 해쉬함수를 이용한 메카니즘(27.07.02)
- 부가형 디지털 서명
제1부 : 일반(27.08.01)
제2부 : 식별자(ID)를 근거한 메카니즘(27.08.02)
제3부 : 확인서를 근거한 기술(27.08.03)
- 해쉬함수
제1부 : 일반(27.09.01)
제2부 : n 비트 블록암호 알고리즘을 사용한 해쉬함수(27.09.02)
제3부 : 전용 해쉬함수(27.09.03)
제4부 : 모듈라 연산을 이용한 해쉬함수(27.09.04)
- 키 관리
제2부 : 대칭형 기술을 사용한 방식(27.18.02)
제3부 : 비대칭형 기술을 사용한 방식(27.18.03)
제4부 : 암호학적 분리(27.18.04)

3) WG 3(Security Evaluation Criteria) ; 정보기술(IT) 시스팀 혹은 관련제품 등의 보안평가에 대한 기준이나 그 기준의 적용방법과 보안평가와 검증에 관련된 처리절차등을 표준화를 하고 있다.
- 정보기술 보안의 평가기준
제1부 : 보안평가 일반모델(27.16.01)
제2부 : 정보기술시스팀의 기능 … 등(27.16.02)
제3부 : 정보시술시스팀의 보증 … 등(27.16.03)

그리고 JTC1/SC27 이외에 ISO 산하에서 정보보안 관련 표준화 활동을 하고 있는 주요 위원회와 내용들은 다음과 같다.
- JTC1/SC1 : 보안 관련되 용어
- JTC1/SC6 : OSI 하위계층 안전모델과 안전지침 및 통신보안
- JTC1/SC17 : IC Card의 개인식별과 보안응용
- JTC1/SC18 : '사무시스템의 안전 요구조건 및 보안관리', 'MHS 보안'
- JTC1/SC21 : 'OSI 보안구조 및 보안기본골격', 'OSI 디렉토리와 보안관리', 'OSI 상위계층 보안부분'

- JTC1/SC22 : POSIX상에서의 보안
- JTC1/SC30 : E야 관련 보안
- ISO TC68 : 은행시스팀 보안('Wholesale Banking', 'Retail Banking 보안', 'Banking 시스팀 보안구조')

국내 보안기술 표준화 작업

국내의 보안기술 표준화를 위한 연구회로는 1992년 보안기술 분야의 한국표준(KS) 작업을 위한 보안기술전문위원회(JTC1/SC27-Korea)등 다음과 같이 5개의 표준화 연구회가 구성되어 활발하게 작업을 진행하고 있다.

1) 보안기술전문위원회(JTC1/SC27-Korea) ; 공업진흥청(구 국립기술품질원) 산하 한국산업표준원 소속으로 1992년에 구성되어 보안분야 국제표준(IS) 연구 및 한국표준(KS) 연구 등 보안표준 관련작업등을 수행하고 있다.
2) 보안기술위원회(OSIA/TG-SEC) ; 정보통신부 산하 개방형컴퓨터통신연구회 소속으로 1993년에 구성되어 한구전기통신표준(KCS) 및 국전산망표준(KIS)등의 연구등을 수행하고 있다.
3) 보안기술연구 실무작업반(TTA/JSC27) ; 1994년 한국통신기술협회 산하에 구성되어 한국전기통신표준(KCS) 및 보안표준 관련작업 등을 수행하고 있다.
4) 정보보호표준연구회(KIISC/SIS) ; 한국통신정보보호학회 산하에 1996년 구성되어 한국전기통신표준(KCS)과 한국전산망표준(KIS) 연구등 보안표준 관련작업등을 수행하고 있다.
5) 인터넷 보안그룹(OSIA/Intemet KIG-SEC) ; 1996년 개방형컴퓨터통신연구회 산하에 구성되어 인터넷 보안연구 및 보안표준 관련 작업 등을 수행하고 있다.

한국표준(KS) 작업 현황

현재까지 JTC1/SC27 분야에서 제정한 12건의 국제표준(IS)과 통산부 국립기술품질원과 한국산업표준원에서 KS로 제정한 6건의 표준안(KS번호)은 다음과 같다.

- 64비트 블록부호 알고리즘 운영모드
- 물리층에서의 데이터 암호화(KSC 5884)
- n 비트 블록부호 알고리즘의 운영모드(KSC 5767)
- 개체인증 기법-제1부 ; 일반모델(KSC 5794)
- 블록암호 알고리즘을 사용하는 검사함수를 이용한 데이터 무결성 기법(KSC 5792)
- 메시지 복원형 디지털 서명방식(KSC 5791)

그리고 정보보안 표준화 작업중 정통부와 한국전산원에서의 제정한 4건의 한국전산망표준(KIS) 및 정통부와 한국통신기술협회에서 제정한 2건의 한국전기통신표준(KCS)의 표준안은 다음과 같다.

- 국가기간전산망 패스워드 활용 표준(KIS 4)
- 전산망 보안관리를 위한 기술지원서(총론)(KIS 6)
- 전산망 보안관리를 위한 기술지원서(전산센터의 물리적 보안)(KIS 7)
- 전산망 보안관리를 위한 위험관리 지침서(KIS 74)
- 디렉토리 기본표준 ; 인증골격(KCS 88)
- 부가형 디지털 서명방식 표준(KCS 221)

결론

정보보안 기술에 대한 연구는 1990년 한국통신정보보호학회가 발족되면서 활성화되었고, 보안기술의 표준화를 위한 작업은 ISO/IEC JTC1/SC27의 표준화 작업을 위한 국내 보안기술전문위원회(JTC1/SC27-Korea)가 1992년 공업진흥청(현 국립기술품질원) 산하에 구성되면서 본격화되었다.

보안제품에 대한 국내 기업의 경쟁력을 향상시키기 위하여는 국제적인 표준화 동향을 신속히 파악하고, 보안기술의 개발과 표준화 양면에서의 연구와 실용화 작업이 정책적으로 지원되어야 할 필요성이 있으며 종합적인 보안기술 표준화에 대한 대책이 마련되어야 할 것이다. 즉, 보안기술에 대한 표준화 연구의 투자를 확대하여 우리 환경에 적합한 보안기술 표준을 개발하고 국제표준화를 적극 유도하며, 보안상품을 실용화하고 보안제품 이용을 활성화시켜야 할 것이다.