정보보안경영실무지침 규격(KS X17799) 개발배경 및 주요내용

전자거래표준과 공업연구사 차재현
02) 509-7338 chajh@ats.go.kr

1. 정보보안의 필요성

정보는 기업 또는 기관 등 당해 조직의 다양한 가치를 지니는 자료로써 그 내용에 따라 적절히 보호되어야 할 자산이다. 정보는 많은 형태로 존재할 수 있으며 종이로 인쇄되거나 쓰여질 수 있고, 전자적으로 저장될 수 있고, 우편이나 전자매체를 통하여 전달될 수 있으며, 필름으로 보여지거나 대화로 말해질 수도 있다.

정보보안은 외부의 광범위한 위협으로부터 자신의 정보를 보호하기 위한 행동과 절차로서, 대상정보의 형태 또는 정보의 공유 및 저장수단이 무엇이든 간에 항상 적절한 보호시스템에 의하여 관리되어야 한다.

정보보안은 기밀성(confidentiality), 무결성(integrity), 가용성(availability)의 특징을 유지하는 것으로서, 기밀성이란 인증되지 않은 폭로 또는 지적 침해로부터 자신의 정보를 보호하는 것을 말하고, 무결성은 정보와 소프트웨어의 정확성 및 완전성에 의하여 명확하게 보호된다는 보장을 말하며, 가용성은 사용자의 정보요구에 대하여 대상정보와 서비스를 명확하게 제공할 수 있음을 보장하는 것으로 정보보안 시스템의 기본적인 구성요소이다.

오늘날의 정보시스템 및 네트워크는 컴퓨터를 이용한 사기, 스파이 활동, 방해공작, 파괴행위, 화재 또는 홍수를 포함한 광범위하고 다양한 원인들로부터 충분한 보호장치없이 더욱 빈번하고, 더욱 대규모적이며, 더욱 정교해지고 있는 컴퓨터 바이러스와 컴퓨터 해킹 등으로부터 심각한 도전을 받고 있는 실정이다. 일반조직에 있어서 정보시스템과 서비스에 의존하고 있다는 것은 그만큼 조직이 보안위협에 더욱 취약해진다는 것을 의미하며, 공공 및 개인 네트워크의 상호접속과 정보자원의 공유는 점점 보안관리의 어려움을 증가시키고 있다. 또한 네트워킹 기반의 정보시스템 확산은 여러 가지 편리성을 제공하고 있으나 반대로 심각한 보안의 취약성을 그대로 노출시키고 있기도 하다. 우리가 사용하고 있는 대부분의 정보시스템은 업무처리를 위한 관점에서만 집중적으로 고려되고 설계되며 안전성에 대해서는 설계시 심각하게 고려되지 않기 때문에, 기술적 수단만으로 보안목표를 달성할 수 있는 것은 한계가 있으며 조직의 구성원 및 보안절차 등

조직의 전반적인 대응여부가 성공적인 정보보안을 결정짓게 된다. 이번에 KS로 제정된 정보보안경영 실무지침은 조직적인 정보보안을 준비하는 많은 기업들에게 많은 도움이 될 것으로 기대된다.

2. 정보보안경영

기업경영에 있어 기밀정보와 고객정보 등을 체계적으로 보호하면서 기업의 정보보안능력을 평가할 수 있는 요구가 증가하고 있다. 인터넷의 급속한 보급과 기업들의 e-비즈니스 활성화와 비례해 보안사고가 급증함에 따라 지능적인 정보유출과 해킹 등에 대한 완벽한 정보보안대책이 시급히 요구되고 있으며 기업이 자체적으로 보안규정을 제정하고자 하여도 참고할만한 규격도 없고 어떤 방법에 의하여 관리하는지도 모르고 있다.

또한 인터넷망을 이용해 전자상거래를 하거나 은행거래를 하는 고객들은 개인정보가 유출되거나 해킹당할 수 있다는 점 때문에 매우 불안해하고 있다.

이런 우려를 씻어주고 특정기업에 안정된 정보보안시스템을 구축하기 위한 정보를 필요로 하므로 이번 KS규격 제정에 안전한 정보보안시스템 구축과 보안관리에 관한 전반적인 표준 가이드라인을 명시한 정보보안경영실무지침을 제정하였다.

정보보안경영실무지침에는 인사보안, 자산관리, 외부침입에 대한 물리적 경비, 내부자료 유출방지를 위한 환경적 관리, 네트워크에 대한 관리, 정보시스템에 대한 접근관리 등의 정보보안시스템 구축을 위한 기술표준을 체계적으로 제시하여 우리기업이 정보보안경영이라는 신개념을 쉽게 이해하고 안전하고 신뢰할 만한 정보보안경영시스템을 글로벌 스탠다드에 적합하게 구축할 수 있는 핵심가이드라인 역할을 하게 될 전망이다.

정보보안 시스템 구축을 찾는 이유는 전자상거래 시장의 규모가 커지면서 사이버 범죄가 급증하고 있기 때문이다. 사이버 범죄로 인한 기업의 손실은 기업의 이윤보다 클 수 있다. 그리고 사이버 범죄 이외에도 회사직원들의 실수와 네트워크 장애 등 내부적인 손실 요인을 감안하면 기업들의 피해 규모는 추정이 불가능할 정도로 크다.

그러므로 정보보안경영 실무지침에는 기업의 사고 예방과 위험의 조기발견에 초점을 맞추고 있으며 시스템 구축에 대한 전반적인 가이드라인을 제시하고 있다.

3. 정보보안경영 실무지침(KS X 17799)의 제정배경

정보보안경영시스템 규격은 2000년 전세계 각국의 주요기관의 홈페이지 해킹소동과 전자상거래 확산에 따른 사이버 범죄가 급증함에 따라 더욱 요구되고 있으며 또한, 정보시스템을 포함한 기업의 보안경영이 국제적으로 급속히 부각되어 각국의 요청에 따라 정보보안국제표준을 담당하고 있는 국제표준화기구(ISO) 정보기술위원회 산하의 정보보안분과위원회(JTC1 SC27)에서 2000년 12월 ISO 17799를 제정하였다.

ISO 17799(Information technology-Code of practice for information security management)는 1998년에 영국에서 정보보안경영인증이 필요한 조직의 요청에 의하여 제정된 BS7799를 기본으로 하여 신속제정 프로그램(Fast Track)에 따라 제정

된 국제표준규격이다.

정보보안 표준 규격을 제정하고 있는 JTC1 SC27에서 한국 대표(NB)로서 활동하고 있는 기술표준원은 정보보안분야의 표준을 주도적으로 이끌고 있으며 작년(2001년) 10월에는 서울에서 SC27 총회를 개최한 바 있다. JTC1 SC27의 총회원국은 우리나라를 포함하여 37개국(정회원 26개국, 부회원 11개국)이며, 담당하고 있는 국제표준분야는

- 개인정보보호 및 보안경영, 전자지불보안 등에 관련된 암호기술
- 전자상거래 활성화에 따른 디지털서명, 전자서명기술
- 정보보안제품 평가 및 국가별 인증서비스 기술

등이다.

기술표준원은 점차 외국의 바이어들이 정보보안경영시스템이 인증된 기업에서 나온 제품의 요구가 증가하고 있고 우리나라 기업이 정보보안경영시스템 구축이 필요한 시점에서 ISO 17799를 한국산업규격(KS)으로 도입하였으며, 국제적으로도 정보보안관리에 대한 논의가 매우 크게 확대되고 있어 적절한 시기에 도입되었다고 할 수 있다. 정보보안경영을 국내 도입으로 국내기업의 신뢰성 확보와 경쟁력 향상을 기할 수 있으며 우리기업의 정보보안 수준을 한단계 높이는 계기가 되었다.

4. 정보보안경영 실무지침(KS X 17799) 주요 내용

정보보안경영실무지침 규격에는 인사, 조직, 경비 대책 등 일반적인 보안 대책과 패스워드와 네트워크 관리 등 정보시스템의 보안 대책으로 구성되어 있으며 10개 항목에 걸쳐 36개의 관리목표와 127개의 세부관리방안에 대하여 구체적으로 설명되어있다.

정보보안경영을 위한 10개 주요 관리항목으로는

1) 보안정책(Security Policy) : 정보보안경영시스템의 구축을 위한 경영정책 수립에 관한 방법에 대하여 규정하고 있으며
2) 조직보안(Organizational Security) : 조직 전체의 보안업무의 총괄 및 보안지침 등을 제정하기 위한 전담조직의 설치 등에 관한 규정으로 정보유출 방지를 위한 제3자 접근 및 아웃소싱에 대한 보안관리방안도 포함되어 있다.
3) 자산분류 및 관리(Asset Classification and Control) : 효율적인 보안관리가 유지될 수 있도록 핵심보호자산을 식별, 분류하고, 각 자산별로 보안책임자를 임명하여 관리하도록 하며
4) 인사보안(Personnel Security) : 내부직원에 대한 보안책임을 규정하여 실수, 절도 또는 남용에 의한 보안위험을 줄이는 방안규정으로 보안 상태를 유지하기 위한 교육훈련방안이 포함되어 있다.
5) 물리적 및 환경적 보안(Physical and Environmental Security) : 정보 및 사업장에 대한 비인가자의 접근, 손상 및 방해를 예방하기 위한 경비방안으로서 경비 및 보안구역, 장비에 물리적 및 환경적 보안 유지방안을 수

립하는 규정을 하도록 하며

6) 통신 및 운영관리 (Communications and Operations Management) : 정보보안경영시스템의 원활한 운영을 위한 통신보안의 최적화로서 정보처리설비의 관리 및 운영에 관한 책임과 절차를 구분하며 바이러스 등 악성 소프트웨어로부터의 보호방안을 수립하도록 하며, 데이터의 백업 및 복구방안을 규정하고 네트워크에서의 보안에 관한 운영절차 수립과 조직간에 교환되는 정보의 손실, 변조를 예방하기 위한 관리방안 등을 포함한 규정을 담고 있으며
7) 접근관리(Access Control) : 네트워크정보의 보호를 위하여 네트워크 사용자의 관리와 책임에 대하여 규정하는 네트워크 관리방안이 있어야 하며
8) 시스템 개발 및 유지보수(System Development and Maintenance) : 위험(Risk)에 대비한 정보를 보호하기 위한 암호기술의 적용 등 정보처리시스템에 대한 보호방안을 수립하여야 하고
9) 업무의 연속성 관리(Business Continuity Management) : 자연재해나 대형사고 발생 시 주요업무처리를 중단없이 수행할 수 있도록 관리하는 방법에 대해 규정하고
10) 준거성(Compliance) : 각종 법규 및 규정 또는 고객과의 계약에 따른 보안의무에 대한 관리방안 등이 기술되어 있다.

이러한 모든 경영에 필요한 관리, 절차 등 세부적인 보안사항을 정보보안경영이라 하며 이것은 경영자 및 관리자만 하는 것이 아니라 최소한 조직내의 모든 종업원이 참여하여야 한다. 그리고 공급자, 고객 또는 이해관계자의 참여를 요구할 수도 있고 외부 조직으로부터의 전문가 조언도 필요할 수가 있다.

정보보안경영은 최초 시스템설계단계에서부터 필요한 요구사항 명세서를 포함하여 설계된다면, 상당히 경제적이며 더욱 효과적이다. 그러므로 시스템에 필요한 보안 요구사항을 파악하는 것이 필수적인데 이를 위해 다음과 같이 세 가지의 중요한 분야로 분류되어 설계되어야 한다.

- 보안성이 약한 조직은 위험평가에서 모든 것이 노출된다. 그러므로 수시로 위험평가를 시행하면 자산에 대한 위협이 파악되고, 보안유출사항이 발생하기 쉬운 취약성 및 가능성이 평가되며 잠재적 영향이 예측된다.
- 우리 조직과 조직의 교역 파트너, 계약자 및 서비스 제공자가 만족해야 하는 법률적, 규제적 및 계약상의 요구사항이다.
- 조직이 자체적인 운영을 지원하기 위해 개발해 온 정보처리에 대한 조직 특유의 원칙, 목적 및 요구사항이다.

보안요구사항은 보안위험에 대한 철저한 위험평가에 의해서 파악될 수 있다. 위험평가기법은 위험요소를 가지고 있는 개인 정보시스템과 특정 시스템의 요소 또는 서비스에 적용될 뿐만 아니라, 전체 조직 또는 조직의 일부분에 대해서만 적용될 수도 있다.

평가결과는 정보보안위험을 관리하고 이러한 위

험으로부터 보호하기 위하여 선택한 관리를 구현하기 위한 적절한 경영조치 및 우선 조치사항을 결정하는데 도움을 줄 것이다. 위험평가와 관리선택 프로세스는 조직 또는 개개 정보시스템의 상이한 부분을 포함하기 위해 수 차례 수행될 수도 있다.

일단, 보안요구사항이 파악되면, 위험이 축소 가능한 수준까지 감소된다는 것이 보장되는 관리시스템이 설정되고 실행되어야 할 것이다. 이러한 관리시스템은 어떤 방법으로 전 분야에서 실행될 수 있으며 적절한 경우 특정 요구사항을 충족시키기 위해 새로운 관리시스템이 계획될 수도 있다.

그러나, 어떤 방법이든 모든 정보시스템이나 환경에 적용될 수 있는 것이 아니며 모든 조직에 대하여 실용 가능하지 않을 수도 있다는 것을 명심하여야 할 것이다.

법률요구사항은 정보보안을 유지하기 위한 필수적인 법률적 사항에 근거를 두거나 조직의 정보보안을 위한 일반적인 원칙을 세워야 한다.

법률적인 관점에서 보면 조직에 필수적인 것으로는

- 개인정보의 데이터 보호 및 프라이버시
- 조직의 기록보호
- 지적재산권을 말할 수 있으며

정보보안을 위한 일반적인 원칙으로는

- 정보보안 정책 문서
- 정보보안 책임의 할당
- 정보보안 교육 및 교육훈련
- 보안사고 보고
- 업무연속성 관리가 있다.

이러한 모든 관리는 제한되지 않는 환경에서 모든 조직에 적용될 수 있다. 비록 모든 관리시스템이 중요할지라도, 그것의 적절성은 조직이 당면한 특정 위험을 고려하여 결정되어야 할 것이다. 따라서, 비록 상기 접근방식이 좋은 출발점으로 간주될지라도, 위험평가에 근거한 관리를 선택하는 것을 대신하지는 않는다.

많은 경험에 의한 결과로 다음 요인들이 포함되어야 보통 조직 내 정보보안의 성공적인 구현을 위한 구성이라고 볼 수 있다.

- 사업목적을 반영하는 보안정책, 목적 및 활동
- 조직문화에 일치하는 보안 이행의 접근방식
- 경영자로부터의 가시적인 지원 및 책임
- 보안요구사항, 위험평가 및 위험경영관리에 대한 충분한 이해
- 모든 관리자와 종업원에 대해 보안의 효과적인 홍보
- 모든 종업원과 계약자에게 정보보안정책 및 규격에 대한 지침의 배포
- 적절한 교육훈련 및 교육의 제공
- 정보보안경영의 성과를 평가하고 개선을 위한 피드백 제안을 위해 사용되는 포괄적이며 균형된 측정시스템

이와 같은 모든 분야에서의 정보보안이 구현되어야만 보안성이 높은 정보보안경영시스템을 구축하였다고 볼 수 있다.

그러므로 기업에서 인증을 받기 위한 기본적인 준비로는 인증을 받기 위한 체계적인 시스템을 다음과 같이 준비하여야 하며 이것은 ISO 9000 시스템의 문서체계와 유사하다.

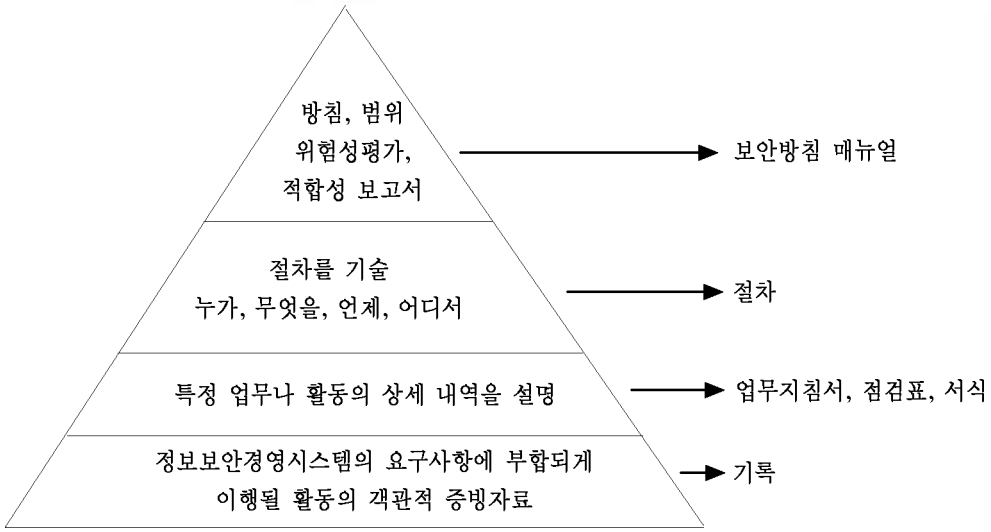

그림. 정보보안경영시스템의 문서화 체계도

정보보안경영시스템 문서에 관한 내용이 준비되면 다음과 같은 절차를 거쳐서 인증 준비를 확인한다. 이것은 인증을 받기 위한 준비라기보다 평소 기업의 보안상태를 점검할 수 있는 장치로 활용하면 좋은 효과를 낼 수 있다.

- 1단계 : 정보보호정책을 정의한다
- 2단계 : 정보보호 관리시스템의 범위를 정의한다. 경계는 조직특성, 위치, 자산 및 기술 등의 요소로서 정의한다.
- 3단계 : 정보자산의 파악 및 적절한 위험평가를 실시한다. 위험평가는 자산에 대한 위협, 취약점 및 조작에 대한 영향을 식별하고 위험수준을 결정한다
- 4단계 : 관리하여야 하는 위험영역은 조직의 정보보안정책과 요구되는 보장수준을 토대로 식별하여야 한다.
- 5단계 : 적절한 관리목표 및 방안을 실무지침의 세부항을 토대로 선정하고, 그 선정을 정당화한다.
- 6단계 : 적용성 보고서를 작성한다. 설정한 관리목표 및 방안과 그것의 설정사유는 적용성 보고서로 문서화한다. 이 보고서는 세부항에 정의한 관리방안 중 제외된 것을 전부 기록하여야 한다.

5. 맺음말

앞으로 정보보안경영 실무지침에 따라 구축되는 우리기업의 정보보안경영시스템은 국내외 공인인증기관으로부터 인증을 받을 수 있게 된다.

이것은 제3자가 인정해주는 인증이므로 관련된 인증기관으로부터 인증을 받을 수 있다. 인증받은 우리기업은 지식정보화사회에서 가장 중요한 자산

인 정보의 관리능력을 공인받게 되는 것이다.

인증결과에서 보면 정보보안경영시스템의 독립적인 검토로 취약한 부분을 식별하여 개선할 기회로 삼고 사업에 필수적인 정보자산의 보호와 내부조직의 위험을 줄이고 취약부분을 보완하여 경쟁력을 높일 수 있으며 나아가서 상업적인 이미지를 높여 요구기관 및 바이어에 신뢰도를 높일 수 있는 방법으로 이어져야 한다.

그러므로 이번에 제정된 정보보안경영 실무지침에 이어 우리기업이 국내에서도 국제적 수준의 정보보안경영시스템 인증을 받을 수 있도록 국제표준을 KS규격으로 도입할 계획이다. 인증규격이 도입되면 외국 바이어들이 정보보안경영시스템이 인증된 국내기업에서 나온 제품을 선택하는 요구사항을 충족하고 수출에 대한 박차를 가할 수 있을 것이다.

현재, 기업의 품질 및 환경경영을 보증하는 것으로 널리 알려진 ISO 9000(품질경영시스템), ISO 14000(환경경영시스템)의 양대 경영시스템 인증과 함께, ISO 17799(ISMS, Information Security Management System; 정보보안경영시스템)에 의한 인증은 앞으로 지식정보화 사회의 진전과 함께 가장 중요한 경영시스템 인증의 하나로 부상할 것으로 전망되고 있다.