情 報 保 護 學 會 誌
第 14 券 第 2 號, 2004. 4

ISO에서의 정보보호관리 국제 표준화 동향

홍 기 향*, 김 정 덕**

요 약

ISO의 정보보호관리 표준은 ISO/IEC JTC1/SC27 WG1에서 표준화를 진행하고 있으며, 현재까지 제정된 정보보호관리 표준으로는 ISO 13335 MICTS와 ISO 17799 Code of practices for information security management 등이 있다. ISO 13335는 정보보호관리 모델 및 기술에 대한 가이드를 제공하는 표준이고, ISO 17799는 정보보호관리 통제에 대한 가이드를 제공하는 표준이다. 최근 동향으로는 ISMS(Information Security Management Systems)국제표준화 작업이 시작될 것으로 예상되며, WG1에서 작업 중인 정보보호관리 표준 간 유사성을 배제하고 통합된 체제를 만들기 위한 로드맵 작성 작업이 진행 중에 있다.

인터넷의 확산과 정보화의 역기능 증가에 따라 능동적인 정보보호관리체계의 수립을 위하여, 우리나라도 정보보호관리 표준의 제정 과정에 적극적으로 참여할 뿐 아니라 국내 많은 조직에서 정보보호관리 표준이 적용되어 국가적인 정보보호관리 수준이 향상될 수 있도록 할 필요가 있다.

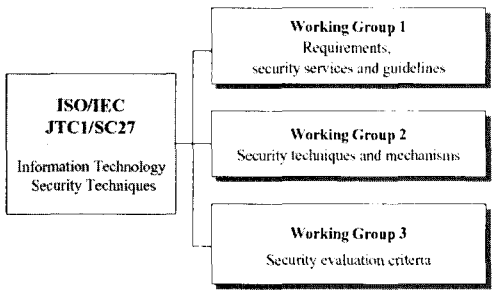
Ⅰ. 서 론

최근 전 세계적으로 정보화 및 인터넷의 확산에 따라 정보화의 역기능 또한 증가하고 있어 사회 각 분야에서 정보보호에 대한 관심이 고조되고 있다. 정보화의 역기능은 해킹 바이러스 등의 피해로부터 심각한 국가, 사회 문제로까지 발전하고 있다. 새로운 보안 위협의 증가에 따라 개별적이고 기술 중심의 정보보호관리에서 종합적인 정보보호관리체계가 요구되고 있으며, 이를 위한 정보보호관리체계의 표준화 또한 국내외적으로 활발히 진행되고 있다. 본 논문에서는 ISO 국제 표준화 기구의 정보보호관리 표준을 살펴봄으로써 정보보호관리 표준의 현황과 전망을 파악해보고자 한다.

Ⅱ. ISO 정보보호관리 표준의 구조

국제적인 정보보호 관련 표준화 기구 중 가장 대표적인 그룹이 ISO/IEC JTC1 SC27이다. SC27은 관련 기술이 복잡해지고, 범위가 넓어지면서 ISO와 IEC의 표준화 활동이 중복되는 경향이 생기게 되어 중복 투자를 줄이고 보다 나은 결과를 도출하기 위해 연합으로 조직된 JTC1에서 안전성 평가 및 감사 기술 분야를 포함하여 정보보호 기술 전반에 대한 표준화를 수행하기 위해 1989년 6월 JTC1 총회에서 새롭게 구성되었다.

현재 JTC1 SC27 (Information Technology, Security Techniques)은 [그림 1]과 같이 3개 작업그룹(WG: Working Group)으로 구성되어 각각



[그림 1] SC27의 구성

* (주)한국전산감리원 책임감리인 (kihyang_hong@daum.net)
** 중앙대학교 정보시스템학과 교수 (jdkim@cau.ac.kr)

정보보호 관리 및 기술 표준화를 담당하고 있으며, 정보보호관리 표준화는 WG1에서 진행 중이다.

WG 1(Requirements, security services and guidelines)은 정보기술의 보안성 요구조건, 보안기술의 관리와 지침개발 및 운영방식 등에 대한 표준화 작업을 하고 있다. 즉, 정보기술 분야에서 요구되어지는 보안서비스의 요구조건과 이용지침 그리고 보안기술 프레임워크 구축 등을 여러 가지 측면에서 검토하여 타 분과위원회에서 응용할 수 있도록 작업을 수행하고 있다.

WG1의 정보보호 관리 표준화 활동은 ISO 13335 MICTS(Management of Information and Communication Technology Security), ISO 17799 Code of practices for information security management의 2개 표준을 위주로 이루어지고 있다.

ISO 13335 MICTS은 정보통신기술 보안을 위한 지침으로서 정보보호관리 모델과 기법을 포함한 조직의 정보보호 관리 지침을 제시하고 있다. ISO 13335는 초기에는 GMITS(Guideline for the Management of IT Security)라는 이름 하에 5개 부분으로 구성되어 있었으며 국제표준(International Standard)이 아닌 기술보고서(Technical Report)이었다. 이 문서 중 Part 1 - 3은 TR이 된지 5년이 넘어 개정 작업 중에 있는데 GMITS이 TR로서 되어 있기 때문에 이의 보급을 보다 활성화하기 위해 IS로 바꾸기 위해 문서명을 MICTS로 변경하여 표준화 작업을 진행 중에 있다. 또한 GMITS Part 2가 Part 1, 3과 내용상 상당부분 중복되기 때문에 최근 개정 작업에서는 MICTS Part 1과 2로 재구성되어 재편집 작업 중에 있다. Part 4와 5에 대해서는 아직 개정작업이 진행되고 있지 않기 때문에 새롭게 결정된 사항은 없다.

또한 ISO 17799는 영국 표준인 BS(British Standard) 7799 Part 2가 2000년 ISO 표준으로 채택된 것으로, 정보보호관리체계 수립을 위한 정보보호 통제 목록을 제시하고 있다. 현재 전세계적으로 정보보호관리체계(ISMS)에 대한 요구가 높아지면서 WG1에서도 ISMS justification report에 대한 작업이 2003년도에 이루어졌으며, 2004년도 4월 회의에서부터 본격적인 국제표준화 작업이 진행될 것으로 예상된다.

최근에는 ISO 13335와 17799의 유사성을 고려하여 ISO 내에서 정보보호관리 표준의 일원화된 체계를 수립하고자 정보보호관리 표준의 로드맵 작성이 제안되어 각 국으로부터 의견을 수렴 중에 있다.

Ⅲ. ISO 정보보호관리 표준의 내용

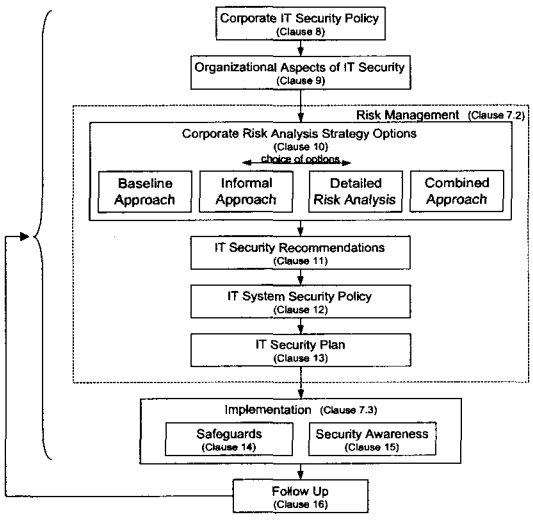
본 장에서는 ISO의 정보보호관리 표준으로 대표적인 ISO 13335 MICTS과 ISO 17799 표준의 내용을 간단히 살펴봄으로써 정보보호관리 국제 표준화 동향을 파악하여 보도록 하겠다.

1. ISO 13335 MICTS

ISO 13335 MICTS는 정보통신기술의 보호 표준으로, 정보보호 관리와 관련된 표준은, Part 1 정보보호관리 모델과 개념, Part 2 정보보호 위험관리 기술 표준이 있다.

- Part 1: Concepts and models for information and communications technology security management
- Part 2: Techniques for information and communications technology security risk management

Part 1은 [그림 2]와 같이 정보보호관리 프로세스를 정의하고, 각 프로세스별 활동과 위험을 구성하는 각 개념을 정의함으로써 정보보호관리 모델을 제시하고 있다.



[그림 2] ISO 13335 -1 정보보호관리 프로세스

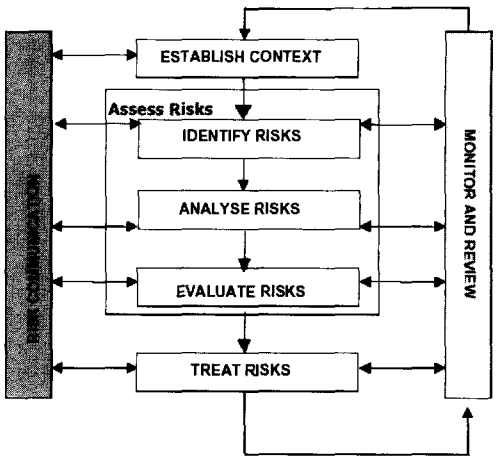
정보보호관리 프로세스는 기업 수준 및 IT 수준의 정보보호 정책을 수립한 후 위험관리 활동을 수행하고, 이에 따라 적절한 정보보호 대책 및 교육 훈련을 실시하고, 지속적으로 사후 관리하는 활동으로 이루어져 있다. 위험관리 활동은 조직의 위험 수준을 정의하기 위한 것으로 위험 분석과 가능한 정보보호 대책의 권고 및 IT 보안 계획을 수립하는 활동을 포함한다. 또한 정보보호관리 프로세스는 사후 관리 활동의 결과가 정책 수립, 위험관리, 정보보호 대책 구현 등 활동에 반영되는 순환적인 구조를 가지고 있다.

Part 1 정보보호관리 프로세스의 특징은 위험분석 전략을 4가지로 제시하고, 조직이 처한 환경과 목적에 따라 적절한 위험분석 전략을 선택하도록 한 것이다. 비공식적 접근방법(Informal Approach)은 전문가가 주관에 따라 위험분석을 수행하는 것으로 간단하지만 결과를 객관화하기 어려운 단점이 있고, 기준선 접근방법(Baseline Approach)은 위험분석을 수행하지 않고 기본적으로 제공되는 정보보호 통제를 사용하는 방법으로 규모가 적은 조직이나 핵심 업무가 아닌 경우에만 사용하며, 상세 위험분석(Detailed Risk Analysis)은 자산별 위협, 취약점, 가치를 모두 고려하여 위험분석을 수행하는 것으로 시간과 노력이 많이 들지만 중요 위험을 식별하고 적절한 정보보호 대책을 수립할 있도록 하는 장점이 있다. 혼합 접근방법(Combined Approach)는 중요하지 않은 업무는 기준선 접근 방법을 사용하고, 중요 업무 또는 자산에 대해서는 상세 위험분석을 수행하는 방법으로 각 위험분석 방법의 장단점을 고려한 비용효과적인 위험분석 방법이다.

Part 1의 또 다른 특징은 모니터링, 유지보수, 변화관리, 사고처리 및 준거성 확인 등 사후관리(Follow-Up)활동을 강조하고, 사후관리 활동의 결과가 다른 정보보호관리 활동에 반영되는 순환적 구조로 정보보호관리 프로세스를 정의한다는 점이다. 이는 정보보호관리가 위험분석과 이에 따른 정보보호 대책의 구현에서 끝나는 일회성 활동이 아니라 사후관리를 통하여 위험의 변화에 능동적으로 대처하는 지속적 활동임을 나타낸다.

Part 2는 정보보호 위험분석 기술에 대한 표준으로, [그림 3]과 같이 위험분석 환경의 정의, 위험 평가 및 위험 처리를 포함하는 일련의 위험 관리 활동을 기술적 측면에서 정의하고 있다.

Part 2에서는 Part 1에서 제시된 여러 가지 위험분석 방법의 선택을 위한 상위 수준의 위험분석



[그림 3] ISO 13335-2 위험관리 프로세스

(High Level Risk Analysis)을 소개하고, 상세 위험분석을 자세히 소개한다. 또한 Part 1과 일관성을 유지하기 위하여 위험처리(Risk Treatment)를 정보보호 대책의 선택으로, 모니터링과 검토를 사후관리 활동으로 상세히 소개하고 있다.

Part 1과 Part 2는 위험분석과 처리를 포함하며, 일련의 순차적 또는 순환적 활동으로 정보보호관리를 정의하는 유사성을 가지고 있으나 Part 1이 조직 측면에서 정보보호관리에 접근한 반면, Part 2는 위험 측면에서 정보보호에 접근한 차이점이 있다.

2. ISO 17799 Code of practices for information security management

ISO 17799는 영국의 정보보호 표준인 BS 7799 Part 1의 정보보호관리 실무 규격을 2000년 ISO에서 국제표준으로 채택한 것으로, 전 세계 유수 기업으로부터 정보보호관리의 최선 사례(Best Practice)를 수집하여 다음과 같이, 11개 분야, 127개 통제 항목을 정보보호관리 표준으로 제시한 것이다.

- Security Policy
- Organizing Information Security
- Asset Management
- Personal Security
- Physical and Environmental Security
- Communication and Operations Management
- Access Control

- Information Systems Development and Maintenance
- Business Continuity Management
- Compliance
- Security Incident Management

ISO 17799는 위험분석 결과와 별도로 선진 조직에서 효과적인 통제수단이라고 입증된 127개 통제 항목 중 선택적으로 통제를 구현하도록 한 것으로, ISO 13335의 기준선 접근방법(Baseline approach)에 해당한다고 할 수 있다. ISO 17799는 정보보호관리의 경험이 없거나 정보보호에 대한 투자가 미미한 조직에 적용하기 용이한 정보보호관리 방법이나 주요 위험을 식별하지 못하고, 비용효과적인 정보보호관리 방법이 되지 못하는 등의 단점이 발생할 가능성이 있다.

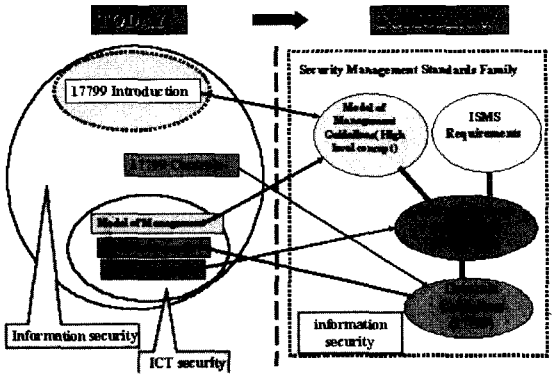
ISO 17799는 BS 7799의 Part 1만 표준화된 것으로 정보보호관리 프로세스를 제시하고 있지 않으나 표준화 작업 중에 있는 ISMS 작업에는 BS 7799 Part 2 (Specification for Information Security Management Systems)의 내용이 상당부분 포함될 것으로 예상되며 위험분석을 포함하는 정보보호 통제의 선택, 구현 및 사후관리 등 일련의 정보보호관리 활동이 제시될 예정이다. 이 작업은 현재 2008년도에 국제표준화를 목표로 작업 중에 있다.

현재 세계적으로 BS 7799 정보보호관리체계 인증을 수용하거나 진행하고 있는 많은 국가가 있으며, 국내에서도 BS 7799 인증을 받은 조직의 수가 점차 증가하고 있다. 일본의 경우, JIPDEC(Japan Information Processing Development Corporation)에서 제공하는 ISMS 인증체계를 BS 7799 인증체계와 동일화함으로써 한 번의 심사로 2개의 인증서(JIPDEC와 BS 7799)를 부여하는 등 방법으로 2003년 10월 약 221개의 일본 기업이 BS 7799를 획득하였다고 한다.

이와 같이 정보보호관리체계 인증에 대한 공공 및 민간기업의 요구가 높아지고, 영국 표준을 기준으로 한 정보보호관리체계 인증에 대한 반작용이 커짐에 따라, 현재 진행 중인 ISMS 국제표준화 노력이 더욱 빠르게 진행될 가능성도 있다.

Ⅳ. ISO의 정보보호관리 표준의 전망

ISO의 정보보호관리 표준으로 채택된 ISO 17799와 ISO 13335는 정보보호관리 프로세스의 유사성이



〔그림 4〕 SC27 정보보호관리 표준 로드맵

많아 2003년 10월 SC 27 회의에서 정보보호관리 표준 간 유사성을 배제하고 통일된 체제를 유지하기 위한 로드맵 작업이 제의되어, 〔그림 4〕와 같은 아이디어에 따라 진행 중에 있다.

〔그림 4〕에 따르면 현재 ISO의 정보보호관리 표준은 ISO 17799와 13335가 혼재되어 있으나 이를 핵심 기능에 따라 통합 및 분류하여 정보보호관리 모델, 정보보호관리체계 요구사항, 위험관리 방법 및 통제 가이드의 4 부분으로 구성하고, 표준 간의 관계도 명확히 하자는 내용이다.

Ⅴ. 결 론

이상 ISO의 정보보호관리 표준화 현황 및 전망을 간략히 살펴보았다. ISO의 정보보호관리 표준은 ISO 13335 MICTS와 ISO 17799 Code of practices for information security management가 대표적으로 각각 정보보호 관리 모델과 기술 통제 등 내용을 포함하고 있으나 각 표준 간 유사성이 있기 때문에 이를 통일된 체제로 만들려는 작업 일정의 로드맵이 작성 중이다.

정보보호관리는 증가하는 정보보호 역기능에 능동적으로 대처하고, 기업간 거래의 신뢰성을 확보하기 위한 기반으로 그 중요성이 날로 증가하고 있으며, 이러한 시대적 필요성에 따라 ISO 국제표준화기구에서도 정보보호관리 표준의 제정에 박차를 가하고 있다.

따라서 우리나라도 정보보호관리 표준의 제정 과정에 적극적으로 참여할 뿐 아니라 국내 많은 조직에서 정보보호관리 표준이 적용되어 국가적인 정보보호관리 수준이 향상될 수 있도록 할 필요가 있다.

참 고 문 헌

[1] ISO, "From Common Criteria to Eliptic Curves-ISO/IEC JTC 1/SC 27, IT Security Techniques", ISO Bulletin June 2000.

[2] ISO, "ISO/IEC 17799:2000 Code of Parctice for Information Security Management", May 2003.

[3] ISO, "ISO/IEC 13335 - Management of information and communications technology security (MICTS)", Nov. 2003.

[4] 장상수, "정보보호관리 국제표준화 동향", 정보보호뉴스, 2000년 11월.

〈著 者 紹 介〉

홍 기 향 (Kihyang Hong)
정회원

1992년 : 이화여자대학교 전산학과 학사
1997년 : 국민대학교 정보과학대학원 정보통신 석사
2004년 : 국민대학교 정보관리학과 박사
〈관심분야〉 정보보호관리, 정보보호성과, 정보시스템 감사 및 통제

김 정 덕 (Jungduk Kim)
정회원

1979년 : 연세대학교 정치외교학과, 학사
1981년 : 연세대학교 경제학과 대학원, 석사
1986년 : University of S. Carolina, MBA
1990년 : Texas A&M University, Ph. D. in MIS
1991년~1993년 : 한국전산원, 선임연구원
1993년~1995년 : 원광대학교, 조교수
1995년~현재 : 중앙대학교, 부교수
〈관심분야〉 정보보호관리, 시스템감사, 전자정부, 정보시스템의 전략적 응용