通信情報保護學會誌
第 10 券 第 2 號, 2000. 6

정보기술 보안관리 지침 표준화 동향

김 정 덕*

요 약

인터넷을 중심으로 e-business의 급속한 발전과 정보자산의 보호가 경쟁력을 좌우하는 중요한 수단이라는 인식이 확산됨에 따라 정보보안관리체계 구축에 대한 요구가 급증되고 있다. 효과적 정보보안관리체계를 구축하기 위해서는 정보보안관리에 관한 실질적인 지침이나 표준이 개발되어 상호연계성이 확보되고 이 결과로 시장확대가 이루어져야 한다. 특히 선진 외국에서는 정보보안관리체계에 대한 인증작업이 진행되고 있어 향후, 정보보안관리가 조직의 국제간 거래에서 충족되어야만 하는 요구조건으로 대두될 것으로 예상된다. 따라서 본 고에서는 정보기술 보안관리 지침에 관한 국내외 표준화 동향을 살펴보고 국내 정보보안관리 지침 표준화 작업이 보다 효과적이고 효율적인 방향으로 전개되기 위한 몇 가지 제안을 제시하고자 한다.

Ⅰ. 서 론

정보기술의 급격한 발전과 이에 따른 기업활동의 변화노력에서 정보보호의 중요성이 높아가고 있다. 이에 따라 정보보호 기술의 표준화 작업도 상당히 진전되고 있어 정보보호산업의 발전을 촉진시키고 있다. 특히 보안관리 컨설팅 산업은 높은 부가가치를 지닌 분야로 구미 선진국들이 많은 투자를 하고 있다. 국제 표준화 기구(ISO)에서는 수년동안 보안관리 분야의 표준화 작업을 수행해 왔으며 일부 분야는 이미 표준화가 완료되었다. 특히 보안관리의 핵심분야인 위험관리와 위험분석에 대한 표준화 작업은 상당히 진전을 보여왔다. 그러나 국내에서는 관련 지침 제정이 주로 국제 표준을 번역하는 수준에 그치고 있으며 보안관리 관련 컨설팅 부문도 아직은 체계가 잡혀있지 않은 상태이다[12,14].

뿐만 아니라 공공기관의 정보시스템 구축 및 운영에 필요한 실질적인 보안관리 과정이 사실상 도입되고 있지 않다. 그러나 국제적인 동향을 보면 영국의 보안관리 표준인 BS7799를 기초로 EU 및 BS7799 가입국가는 보안관리 인증작업을 진행하고 있으며 이를 국제 표준화 하고자 노력하고 있다.

이와 같이 정보보안관리 분야에 대한 국제 표준/지침이 제정되어 활용되고 있으나 국내 정보시스템 환경이 외국과 상이하고 국제 표준을 그대로 수용하기에는 어려운 점이 많다. 구미 선진국에서는 국제 표준을 수용하면서 자국내 정보시스템 환경에 맞는 지침을 제정하여 활용하고 있다. 따라서 본 논문에서는 국내외 정보보안관리 지침 표준화 작업을 살펴봄으로써 전반적인 동향을 분석하고 국내 정보보안관리 체계 수립을 위한 방향을 제시하고자 한다.

Ⅱ. 정보보안관리 지침의 국내외 표준화 동향

1. ISO의 정보보안관리 지침 표준화 작업

국제 표준기구인 ISO/IEC JTC1에서 정보보안관리 지침 표준화는 SC27(정보보안기술 표준화 분과위원회) WG1에서 작업하고 있다. 표준문서는 ISO/IEC TR 13335, "Guidelines for the Management of IT Security"로서 5부로 구성되어 있다[5,6,7,8,9]. GMITS의 1부와 2부에서는 보안관리의 개념, 과정모델 및 위험관리와 기획 프로세스에 대한 내용들을 포함하고 있다. 이에 기초하여 3부에서는 보안관리 과정에서의 구체적인 기법들을 제시하고 있다. 4부에서는 보안요구사항과 조직의 특정환경에 따라 보안대책을 어떻게 선정하는 과정을 기술하고 있으며 적절한 보호수준을 달성하기

* 중앙대학교 정보시스템학과 (jdkim@cau.ac.kr)

위한 방법과 기본적 보안대책(baseline security)을 어떻게 적용할 수 있는가를 보여주고 있다. 5부에서는 인터넷과 같은 외부 네트워크와 연결된 상황에서의 보안대책을 선정하는 방법을 기술하고 있다.

TR 13335-1(Part 1) : Concepts and Models of IT Security (1996-12-15 TR, 2000 검토)
TR 13335-2(Part 2) : Managing and Planning IT Security (1997-12-15 TR)
TR 13335-3(Part 3) : Techniques for the Management of IT Security (1998-06-15 TR)
TR 13335-4(Part 4) : Selection of Safeguards (DTR)
TR 13335-5(Part 5) : Management Guidance on Network Security (PDTR)

TR 13335 국제표준의 5부문 중 현재 표준으로 확정된 부문은 TR 13335-1, 2, 3이며 나머지 부문도 빠른 시간이내에 모두 표준으로 제정될 예정이다. 본 문서는 기술적 표준이 아니라 TR(Technical Report: 기술 보고서) Type 3로서 명확한 해결책보다는 여러 표준 문서에서 자료를 수집하여 이를 체계적으로 정리한 보고서이므로 표준보다는 지침성격이 강하다. 즉 다른 표준은 국제표준이 된 후 3년내에 재검토를 반드시 해야 하나 TR Type 3 문서는 사용된 자료가 더 이상 적합하지 않거나 유용하지 않으면 재검토할 필요가 없다. 따라서 기술적인 제품 개발에 적용되지는 않으나 전반적인 보안관리 차원의 요구사항을 포함하고 있으므로 국가간의 무역거래나 계약시 본 지침을 적용할 가능성이 있다. 이에 대한 준비로 본 지침에서 제시하는 내용을 정확히 이해하고 국내 환경에 적합하도록 구현해 보는 노력이 요구된다.

1부[5]에서는 정보기술 보안관리에 관한 여러 개념을 기술하고 기본적인 보안 개념과 모델, 과정을 간략히 고위 경영층을 대상으로 소개하기 위한 목적으로 작성되었다. 정보보안관리는 정보와 정보기술 서비스로부터 적절한 수준의 비밀성, 무결성, 가용성을 달성하고 유지하기 위한 하나의 과정으로 정의하고 있다. 즉, 정보보안관리는 조직내 정보보안 환경을 설계, 구축, 운영, 감시하는 활동으로 구성된 생명주기(life cycle)를 기획, 관리하는 과정이라고 할 수 있다. 정보보안 환경은 정보자산과 연관된 원인과 결과의 조합이라고 할 수 있다. 간단히 말하면, 조직내의 정보자산에 대한 여러 긍정적/부정적 영향력을 의미한다고 할 수 있다. 보안관리는 이들 영향력간의 균형을 이루어 건실한 정보보안 환경을 달성하기 위한 활동이다[15]. 특기할 만한 점은 정보보안관리을 위해서 시스템적인 접근방법을 제시하고 있다. 이를 위해서는 우선적으로 조직 상부계층에서 시스템 계층까지 여러 수준에 적합한 보안 목표, 전략, 정책을 개발해야 하며, 주기적인 보안 검토의 결과와 비즈니스 목표의 변화 등을 반영하여 지속적으로 갱신해야 한다. 또한 그림 1.과 같이, 보안 구성요소간의 관계, 보안요소와 위험관리간의 관계를 소개하고 있다.

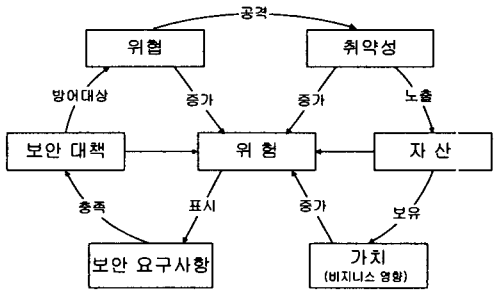


그림 1. 위험관리 요소간의 관계

2부[6]에서는 정보보안관리 기능 및 과정을 소개하고 있으며 정보보안 정책의 계층적 구조와 담당 조직의 역할을 기술하고 있다. 또한 조직내에 비용효과적인 정보보안을 구축하기 위해 정보보안계획수립을 강조하고 있다. 또한 그림 2.와 같이 정보보안관리 과정을 기술하고 있다:

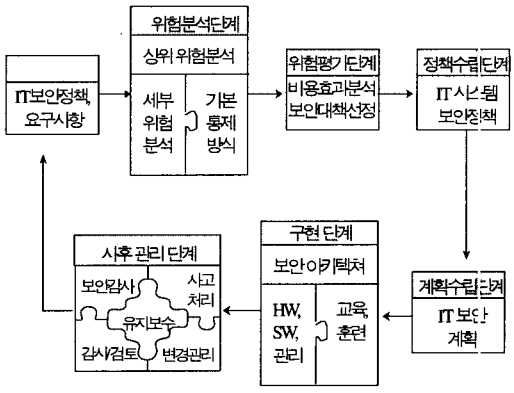


그림 2. 정보보안관리 과정

3부[7]에서는 2부에서 제시한 정보보안관리 과정에서 사용될 수 있는 구체적 기법 및 방법을 제시하여 주고 있다. 특히 정보보안관리 과정에서 중요한 위험관리와 위험분석에 대해 상세하게 기술하고 있다. 위험관리는 시스템의 위험을 평가하고 그 결과에 따라 비용효과적인 대책을 제시하여 시스템 보안정책과 보안대책 계획 수립을 도출하는 일련의 과정이다. 위험관리는 조직의 환경과 능력에 맞추어 대책을 운영하도록 지원하는데 큰 장점이 있다. 위험관리는 조직의 정보시스템을 설계하는 단계에서 고려될 때 가장 큰 효과를 발휘할 수 있다. 시스템이 구축되기 전에 위험관리를 수행함으로써 시스템이 갖추어야할 비용효과적인 대책을 사전에 구현할 수 있다. 뿐만 아니라 위험관리는 시스템이 변경되거나 운영되는 과정에도 적용하면 안정된 시스템 운영에 기여할 수 있다.

본 지침에서는 일반적인 위험관리 과정을 소개하고 있어 구체적인 위험관리 방법론의 개발 또는 선정시 기본적인 틀(framework)로서 활용될 수 있다. 정보보안 위험관리에서 핵심적인 활동은 위험분석과 평가로서, 위험분석은 자료수집과 분석을 하는 단계이며, 위험평가는 분석된 결과물을 기초로 현황을 평가하고 적절한 방법을 사용하여 효과적으로 위험수준을 낮추려는 활동을 하는 단계이다. 즉 위험분석은 위험의 식별과 분석을 하는 단계이고, 위험평가는 위험의 평가와 보안대책을 결정하는 단계이다. 위험분석의 목적은 보호되어야할 대상 정보시스템과 조직의 위험을 측정하는 것이다. 또한 위험분석은 측정된 위험이 통제되어야 할 위험인지 아니면 받아들여질 수 있는 위험인지를 판단할 수 있도록 근거를 제공해야 한다. 위험분석 방법은 여러 가지가 있을 수 있으나 본 지침에서는 상위분석을 통해서 빠르고 적은 노력으로 위험분석 대상 시스템의 위험을 분석한 후, 위험수준이 높지 않은 시스템에 대해서는 기본통제 방법을 적용하고 위험수준이 높거나 핵심업무를 수행하는 시스템에 대해서는 상세한 위험분석을 수행하는 혼합적 방법을 권고하고 있다.

상세 위험분석 과정은 우선 보호 대상인 정보자산의 가치와 상호의존도를 파악하고 자산에 손해를 미칠 수 있는 위협의 유형을 파악하여 이의 강도와 빈도를 측정하는 위협분석을 수행하며 동시에 자산이 보유하고 있는 취약성을 평가하는 과정을 포함하고 있다. 이를 통해 자산의 가치와 위협 및 취약성 평가의 결과를 토대로 위험을 측정, 평가하는 과정으로 구성되어 있다.

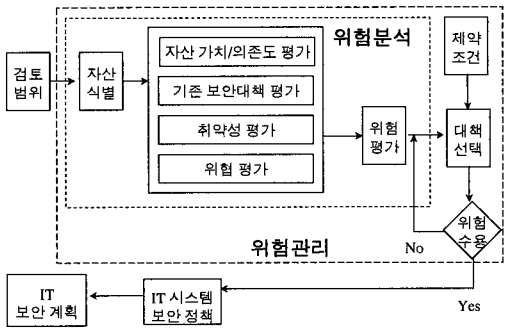


그림 3. 위험관리과정 및 위험분석과의 관계

위험관리 과정을 수행한 뒤 보안대책 수행계획에 따라 대책을 구현해야 한다. 대책은 기술적인 구현 후에도 대책의 특성상 지속적으로 관리, 운영해야 하는 경우가 많다. 따라서 대책 구현이 끝난 뒤 대책이 시스템 보안정책과 대책 수행계획에 맞게 구현되었는지를 검증하고 승인했을 경우에만 대책이 운영에 들어갈 수 있어야 한다.

사후관리는 보안관리 주기에서 가장 중요한 부문이다. 사후관리는 보안정책 수립에서 위험관리에 이르기까지 수행된 보안관리 단계가 조직의 보안성 향상에 실질적으로 도움이 되었는지 점검하고 관리하는 분야이다. 사후관리는 크게 감사(audit), 점검(monitoring), 사고대응(incident respond), 대책의 유지보수 등의 4가지로 나누어 질 수 있다.

4부[8]에서는 보안요구사항과 조직의 특정환경에 따라 보안대책을 어떻게 선정하는 과정을 기술하고 있으며 적절한 보호수준을 달성하기 위한 방법과 기본적 보안대책(baseline security)을 어떻게 적용할 수 있는가를 보여주고 있다. 본래 이 지침은 '96년 런던회의에서 GMITS의 4부로서 "Baseline Approach (SC27/N1354)"라는 이름으로 작성하였다. Baseline Approach는 특정 조직의 최소한의 보안요구사항을 만족시키는 기본통제요소(baseline controls)를 선택하는 것이라고 할 수 있다. 그러나 과제 진행중에 Baseline Approach에 포함되는 기본통제요소 자체를 표준화한다는 것은 국가간의 능력 및 수준 차이로 많은 논란이 있으므로 '97년에는 Baseline Approach를 조직이나 정보시스템을 위한 보안대책 선정시 어떻게 활용할 수 있는가

를 표준화하기로 하고 이를 "Selection of Safeguards(SC2/WD 1527)"로 과제명을 변경하였다.

5부[8]는 4부의 추가 문서의 성격이 강하며, 인터넷과 같은 외부망과 연결하고자 하는 조직에 도움을 주기 위해 작성되었다. 즉 외부망과의 연결과 이로 인해 제공되는 서비스에 대한 보안대책의 제안, 선정 및 사용에 대한 지침을 제공하고 있다. 여기에서는 13가지 보안위험 시나리오과 8가지 외부망 접속 유형에 기초하여 해당되는 보안대책을 제시하고 있다.

2. 선진국의 정보보안관리 표준화 동향

영국에서는 국내 표준인 정보보안관리 지침(BS7799, Code of Practice for Information Security Management)[1,2]을 토대로 조직들이 최소한으로 준수해야 할 보안 대책을 제시하여 정보자산을 보호 할 수 있도록 하고 있다. 영국은 이를 국제 표준(ISO/IEC JTC1 SC27 WG1) 노력에 적극 반영시키고 있으며 유럽연합 국가에서의 유사한 작업(독일의 IT Baseline Protection Manual 등)에 공동 작업을 수행하고 있다. 또한 BS7799에 대한 인증제도(accreditation)를 마련하여 조직의 정보보호 수준을 평가하고 있으며 이러한 인증체계를 타국에도 적용시키려는 노력을 시도 중에 있다. 조직간 또는 국가간 전자적인 거래가 증가함에 따라 정보보안관리에 관련된 공통의 참고자료나 기준을 가지고 이에 대한 적합성을 인증함에 따라 거래 당사자간의 상호 신뢰를 구축하고자 하고 있다. 이 지침에서 제시하는 내용들은 모든 조직에서 최소한으로 준수해야 할 보안 요구사항을 만족시키는 수준의 일종의 기본통제(baseline controls)의 성격이 강하다.

BS7799는 2부로 구성되어 있으며 1부[1]는 정보보안관리 지침으로 10개 분야에 127개의 통제대책(실제로는 약 2000 여개의 통제대책 포함)을 제시하고 있다. 10개 분야는 다음과 같다: 1) 보안 정책, 2) 보안 조직, 3) 자산의 분류와 통제, 4) 인사보안, 5) 물리적, 환경적 보안, 6) 컴퓨터 및 네트워크 관리, 7) 시스템 접근제어, 8) 시스템 개발 및 유지보수, 9) 업무지속성계획, 10) 준거. 2부는 인증을 위해 작성되었으며 특기할 만한 것은 보안관리에서 위험분석 수행을 요구하고 있다는 점이다. 2부에서는 BS7799 인증에 관한 것으로 인증은 신뢰된 제3자인 인증기관(certification body)을 통해 획득되며, 인증기관은 인증수여 후에도 BS7799 준수 여부에 관하여 지속적인 감사를 수행하게 된다. 이러한 인증기관은 영국 DTI(Department of Trade and Industry)산하의 UKAS에 의해 인가(accreditation)되며 인증활동에 대해서 지속적인 감시 및 평가를 받게 된다.

BS7799의 관련 문서는 다음과 같다:

DISC PD 3001 : Preparing for BS7799 certification

DISC PD 3002 : Guide to Risk Assessment and Risk Management

DISC PD 3003 : A pre-certification assessment workbook

DISC PD 3004 : Guide to BS7799 Auditing

DISC PD 3005 : Guide on the Selection of BS7799 Controls

미국이 정보시스템 개발·구입시 국방부 표준인 TCSEC(Trusted Computer System Evaluation Criteria)을 적용하여 일정 등급이상의 제품을 개발·구입토록함으로써 무역거래시 새로운 장벽의 효과를 거두었듯이, 영국도 BS7799 인증제도를 자국 내 조직뿐만 아니라 타국에도 적용함으로써 조직간 또는 국가간 정보보호 관리에 적합성을 인증하여 거래 당사자간의 상호 신뢰를 구축하는 것은 물론 무역 파트너를 선별하고자 하고 있다. 국제 표준기구인 ISO에도 적극적으로 BS7799를 반영시키려는 영국의 움직임을 볼 때, 영국뿐만 아니라 유럽, 나아가 전세계와의 무역 거래시 ISO 9000 시리즈 인증제도와 같이 BS7799가 새로운 무역장벽으로 대두될 것으로 예상된다.

이외에도 미국을 비롯한 선진국에서는 다음과 같은 정보보안관리 관련 지침[3,4,10,11]들을 수립하여 수행하고 있다:

NIST FIBS PUB 65, Guidelines for Risk Management

NIST FIBS PUB 73, Guidelines for Security of Computer Application,

NIST FIBS PUB 191, Guidelines for the Analysis of LAN Security

NISTIR 4387, DOE Risk Assessment Methodology

NISTIR 4325, DOJ SRAG(Simplified Risk Analysis Guidelines)

3. 국내 정보보안관리 지침 표준화 작업

정보보호 관련 표준안의 추진체계는 그림 4.와 같이 한국통신기술협회(TTA)의 정보보호분과위원회인 SC10과 정보통신부를 통하여 제정되는 한국정보통신인 KICS 형태가 있으며, 산업표준연구원과 산업자원부를 거쳐서 제정되는 KS 형태등 2가지로 분류가 된다[12].

국내의 정보보안관리 관련 표준화 활동은 1992년 SC27의 국내위원회가 기술표준원 산하에 구성되면서 활발하게 진행되고 있다. 그리고 1993년부터 개방형컴퓨터통신연구회의 보안기술위원회, 1994년에는 한국통신기술협회의 정보보호분과위원회(TTA-SC10) 산하의 정보보호관리 연구위원회 및 1996년에 한국통신정보보호학회의 정보보호 표준연구회(KIISC/SIS)등이 구성되어 정보보안기술의 국내 표준화 작업이 진행되고 있다. 한편, 1995년부터 한국전산원의 '전산망보안표준협의회'와 1996년부터 개방형컴퓨터통신연구회의 '인터넷 보안그룹(OSIA/

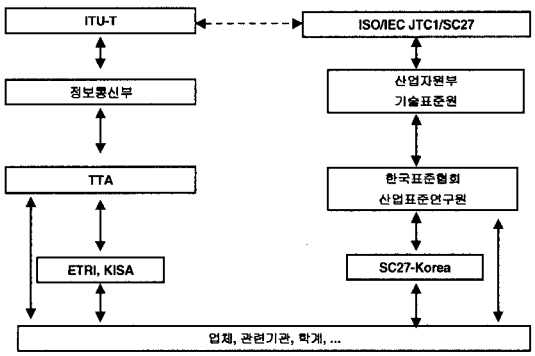


그림 4. 국내 정보보호 추진체계

Internet KIG-SEC)' 등도 보안표준 작업을 수행하였으나, 2개의 기능 모두가 현재는 폐지되었다.

현재 정보보안관리 측면에서의 표준화 작업은 ISO TR 13335의 1부가 1998년에 KS 표준으로 제정되었으며, 2부, 3부는 1999년부터 표준화 작업이 진행 중에 있다. 이외 KICS는 아래 표와 같이 표준화 작업이 진행되고 있다.

표 1. 국내 정보보안관리 지침 표준화 현황

과제번호	과제명	검토사항
KICS.KO-10.0005	전산망 보안관리를 위한 기술지원서(총론)	1993년 제정
KICS.KO-10.0006	전산망 보안관리를 위한 기술지원서(전산센터의 물리적 보안)	1993년 제정
KICS.KO-10.0047	전산망 보안관리를 위한 위험관리 지침서	1995년 12월 6일 제정
KICS.KO-10.0072	네트워크 보안관리 지침서	1996년 12월 14일 제정
KICS.KO-10.0073	소프트웨어 보안관리 지침서	1996년 12월 14일 제정
KICS.KO-10.0074	자료 보안관리 지침서	1996년 12월 14일 제정
KICS.KO-10.0075	S/W 개발 및 변경에 대한 보안관리 지침서	1996년 12월 14일 제정
97-145	인터넷 보안관리 지침표준(안)	
99-142	공공정보시스템 보안을 위한 위험분석 표준	해당 과제는 이미 초안이 전산원으로부터 제출되어 있으며, '99. 8월부터 의견수렴 중
99-143	정보시스템 구축 준비 단계의 보안관리 지침	
99-144	공공정보시스템 비상계획 및 재해복구 지침	
99-145	정보시스템 보안 감리 지침	KISA로부터 과제폐지가 요청된 상태이며, 논의 후 분과위원회의 결정수용
99-147	공공기관 전산보안정책 수립을 위한 지침서	의견수렴 중

III. 맺는 말

현재의 국내 정보보안 관련 표준화 활동의 대표적 특징은 아직도 표준화 주도 주체가 정부 및 정부에서 지원하는 연구기관이나 표준화 기구와 학계를 중심으로 이루어지고 있다는 점이다. 이는 우리 나라의 정보보호 관련 기술의 수준과 표준화 관련 역사의 짧음을 단적으로 나타내는 증표라 여겨진다. 즉, 표준화의 중요성이 기업체의 관리자에게 아직 확고하게 인식되거나 자리잡지 못한 채 소수의 전문가나 교수들에 의하여 그 중요성이 강조되면서 조금씩 확산되어 가는 단계라 할 수 있다[15].

따라서 국내 정보보안관리 표준화 활동은 아직도 선진국 또는 국제 표준화 기구에서 만들어지는 권고 또는 각종 표준 지침들을 이해해서 이를 국내 표준이나 지침으로 작성하고 있는 수준이라고 할 수 있다.

국내 현실에 적합한 정보보안관리 지침 작성에 대한 노력이 있었으나 실제적인 결과를 맺지 못한 채 국제 표준에 대한 번역 수준에서 크게 벗어나지 못했다는 사실을 인정하지 않을 수 없다. 즉, 조직 차원의 정보보호관리를 위해 개별 조직에 적합한 보안정책 및 보안지침을 수립하였으며, 공공기관의 경우 1997년 "국가전산보안업무기본지침"이 제정되었으나, BS7799 및 GMITS 등과의 호환성 특히 BS7799 인증제도에 대한 대응방안에 관한 연구는 미흡한 실정이다.

본 고에서 살펴보았듯이 정보보안관리의 중요성이 대두되고 정보보안이 조직간 거래에 기본적으로 구축되어야할 기반구조로서의 역할을 수행함에 따라 국내 현실에 적합하면서 국제표준과의 호환성을 보장할 수 있는 지침 개발 및 인증제도 개발에 관한 연구가 절실히 요구된다. 최근의 정보보호 컨설팅 업체가 주축이 되고 정통부가 후원이 되어 이루어진 "정보보호컨설팅포럼(FISC)"이 정보보안관리 지침 개발 및 인증 작업을 위해 작업을 시작한 것은 매우 바람직한 일이라고 사료된다. 이러한 노력이 결실을 맺고 표준화 작업으로 이어져 국내 정보보안관리 체계가 조기에 정착될 수 있어야 한다. 이를 위해서는 업계의 현실적인 전문성을 반영할 수 있도록 보다 적극적인 산업체의 참여가 필요하고 국제적 표준/지침이나 인증작업과의 호환성을 유지할 수 있는 체계 구축이 요구된다.

또한, 보안관리 활동을 위한 구체적인 지침 작성이 요구된다. 이제는 보안관리 전반적인 활동에 관한 지침에 기초하여 구체적이며 현실적인 개별적 보안관리 활동을 위한 지침 작성이 필요한 때이다. 즉, 정보보안 정책 개발 지침, 정보보안 계획 수립을 위한 지침, 보안대책 선정을 위한 지침 등 정보보안관리 활동중 중요하고 시급한 활동을 수행하기에 필요한 지침이 개발되어야 한다. 이를 위해 산학연의 유기적인 협조체제가 필요하며, 표준(안)개발에 대한 평가제도를 통한 고품질화와 표준화 관련 기관의 역할 재정립 및 협력을 통해 보다 효과적이며 효율적인 표준화 과정이 필요하다.

참 고 문 헌

[1] BSI 7799-1: Information Security Management - Part 1: Code of Practice for Information Security Management, BSI, 1999.

[2] BSI 7799-2: Information Security Management - Part 2: Specification for Information Security Management Systems, BSI, 1999.

[3] FIPS PUB 65, Guidelines for Automatic Data Processing Risk Analysis, U.S. Department of Commerce/National Bureau of Standards, Aug. 1979.

[4] FIPS PUB 73, Guidelines for Security of Computer Applications, U.S. Department of Commerce/National Bureau of Standards, Jun. 1980.

[5] ISO/IEC JTC1/SC27 TR 13335-1, Guidelines for the Management of IT System Security: Part1-Concepts and Models for IT Security, ISO, 1996.

[6] ISO/IEC JTC1/SC27 TR 13335-2, Guidelines for the Management of IT System Security: Part2-Managing and Planning IT Security, ISO, 1997.

[7] ISO/IEC JTC1/SC27 TR 13335-3, Guidelines for the Management of IT System Security: Part3-Techniques for the Management of IT Security, ISO, 1998.

[8] ISO/IEC JTC1/SC27 DTR 13335-4, Guidelines for the Management of IT System Security: Part4-Selection of Safeguards, ISO, 1999.

[9] ISO/IEC JTC1/SC27 TR 13335-5, Guidelines for the Management of IT System Security: Part5-Management Guidance on Network Security, ISO, 1999.

[10] NIST, U.S. Department of Justice Simplified Risk Analysis Guidelines, NISTIR 4387, Aug. 1990.

[11] Robak, Edward. & Security and Emergency Planning Staff, U.S. Department of Justice Simplified Risk Analysis Guidelines(SRAG), National Institute of Standards and Technology, 1990.

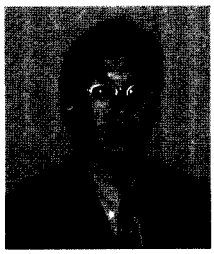
[12] 이홍섭, "정보보호와 표준화 추진전략, TTA 저널, 61호, 1999. 2.

[13] 한국정보보호센터, '97 정보보호기술 표준화 현황, 1997. 12.

[14] 한국정보보호센터, "국내·외 정보보호산업 현황", 1999. 5.

[15] 한국정보보호센터, "정보보호산업 표준화 수요 분석 연구", 1999. 11.

〈著者紹介〉



김 정 덕
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, 전자상거래, 정보시스템의 전략적 응용
E-mail: jdkim@cau.ac.kr