보안관리수준 평가 체계에 대한 분석 및 개선안 연구

민병길* · 이도훈*

요 약

정보통신시스템에 대한 기술적 보안만으로는 안전한 정보통신시스템 운영을 보장할 수 없다. 따라서, 안전한 정보통신시스템 운영을 위한 정보보안관리시스템(ISMS)에 대한 연구와 표준화가 활발히 전개되고 있다. 우리나라는 2005년 "국가사이버안전관리규정"을 제정하고, "국가사이버안전매뉴얼"의 "보안관리 기준"에 의하여 국가·공공기관이 자체적으로 "보안관리수준 평가"를 수행토록 함으로써 체계적인 정보보안관리 활동이 이루어지도록 하고 있다. 본 논문은 관련 표준들과 호주, 미국의 보안관리 체계에 대하여 조사하고, "보안관리수준 평가" 체계를 효율적인 보안관리 측면에서 분석하고, 이를 통하여 "보안관리수준 평가"의 개선방향에 대하여 연구하였다. 기존의 체계에 추가항목(A/C ; Additional Control), 선택적 보안관리 기준(Selective Controls) 구성을 도입하고 평가 준비 절차의 개선을 통하여 각 기관에 최적화된 보안관리 기준을 작성할 수 있도록 함으로써, 기관에 적합한 효율적 보안관리의 수행이 가능하고, 급변하는 정보통신 환경에 유연하게 대응할 수 있도록 하였다.

Research of Improvement and System of the Information Security Management Evaluation

Byung-Gil Min* · Do-Hoon Lee*

ABSTRACT

It will not be able to guarantee the secure operation for the information and communication systems with only technical security. So, ISMS(Information Security Management System) research and standardization are active going on. Korea published "The national cyber security management regulation" and "The national cyber security manual" in 2005. According to the regulation and manual, the government organ and public institution must accomplish the security management assessment to itself for systematic management of an information security. We studied related standards and security management systems of the Australia and the USA, and analyzed the security management evaluation system in "The national cyber security manual" in efficient security management focus. We presented the improvement direction of national security evaluation system through the research. We propose the additional control, selective control set and improvement of the evaluation process for efficient security management. Proposed system possible composition of suitable to each organ and flexible adaptation of rapidly changed information environment.

Key words : Information Security Management Evaluation, Information Security Management System

* 국가보안기술연구소

1. 서 론

정보통신시스템이 기업 및 정부기관의 업무 수행에서 차지하는 비중이 점차 증가되고, 정보보안에 대한 인식이 크게 증대되면서, 보안강화를 위한 많은 연구와 기술적 대책들이 제시되었고, 각종 정보보호시스템들이 개발되어 운영되고 있다. 그러나, 이러한 기술적 보안 대책만으로는 안전한 정보통신시스템 운영을 보장할 수 없다. 예를 들어, 내부의 정보시스템을 보호하기 위하여 도입된 침입차단시스템이 제대로 설정되지 않아 많은 포트들이 외부로 허용되어 있으며, 최신의 공격을 탐지하기 위한 룰이 지속적으로 업데이트 되지 않았다면, 침입차단시스템의 도입만으로 안전한 보안이 이루어진다고 할 수 없을 것이다. 즉, 이러한 시스템이 해당 기업과 기관의 보안정책을 정확하게 수행해야 하고, 매일같이 새롭게 등장하는 보안위협으로부터 효과적인 보안대책이 될 수 있도록 지속적인 개선과 운영이 필요하다.

따라서 안전한 정보보안은 정보보호시스템과 같은 기술적, 물리적인 대책 외에 이를 안전하게 운영하기 위한 관리 체계가 필요하며, 이러한 체계를 정보보안관리체계(ISMS ; Information Security Management) 또는 정보보호 경영시스템이라고 한다.

정보보호 경영시스템으로는 BS 7799[1, 2]가 이미 널리 사용되고 있다. 이는 원래 영국 표준이지만 세계 표준처럼 널리 사용되었으며, 이를 기반으로 한 ISO/IEC 17799[3], ISO/IEC 27001[4]이 이미 국제 표준으로 확립되었다. 향후 정보보호 경영시스템의 표준 및 인증과 관련된 제반 사항들이 ISO/IEC 27000대의 시리즈로 계속 표준화가 진행될 예정이다.

우리나라는 2005년 "국가사이버안전관리규정(대통령훈령 제141호)[5]"을 제정하고, 동법 제9조 4항에 의거하여 "국가사이버안전매뉴얼[6]"의 "보안관리 기준"에 의하여 국가·공공기관이 자체적으로 "보안관리수준 평가"를 수행토록 함으로써 체계적인 정보보안관리 활동이 이루어지도록 하고 있다.

본 논문은 정보보안관리를 위한 관련 표준들과 미국의 연방 정보보안 관리법(FISMA ; Federal Information Security Management Act)[7]에 대하여 조사하고, "국가사이버안전매뉴얼"의 "보안관리수준 평가" 체계를 효율적인 보안관리 측면에서 분석하고, 이를 통하여 "보안관리수준 평가"의 개선방향에 대하여 연구하였다.

2. 관련 연구

2.1 ISO/IEC 27001, 17799(BS 7799)

정보보안관리에 대한 필요성이 증가함에 따라 각 국에서는 다양한 정보보안관리 방법론을 독자적으로 개발하고 있으며, 특히 영국에서 개발된 BS7799는 BSI/DISC 위원회 BDD/2의 정보보안관리에 의해 제정된 것으로 정보시스템을 운영하는 조직 전반의 보안상태를 평가하고 인증하기 위한 유용한 정보보안관리시스템으로서, 여러 나라에서 준(準) 국제표준으로 활용되어 왔다.

BS 7799 Part 1[1], Part 2[2]는 각각 ISO/IEC 17799, 27001의 국제표준으로 채택되었다. ISO/IEC 17799는 "정보보안관리 실무 규범(A Code of Practice for Information Security Management)"이라는 제목 하에 조직의 정보보안을 구현하고 유지하는 책임을 지는 관리자들이 참조할 수 있는 보편적인 문서로 사용하도록 개발되었으며, 조직 보안표준의 기반이 되도록 고안되었다. ISO/IEC 27001은 정보보안관리시스템에 대한 인증 규격을 기술하고 있다. 이 표준에서 제시하고 있는 통제항목들(Controls) 모두가 모든 상황에 적용될 수 있는 것은 아니며, 개별적인 환경적 또는 기술적 제약조건을 고려하여 선택하여야 한다.

ISO/IEC 27001과 BS 7799의 인증을 위해서는 반드시 위험분석이 선행되어야 하며, 분석된 정보보안 위험을 어느 수준으로 낮출 것인가와 수행하고자 하는 통제항목(Controls)의 구성은 기관(또는 기업)이 자율적으로 결정하도록 하고 있다.

2.2 GMITS (ISO/IEC TR 13335)

ISO/IEC TR 13335, "Guidelines for the Management of IT Security(GMITS)"는 정보보호 관리를 위한 표준으로 5부로 구성되어 있으며, 기술보고서로서 IT 보호 관점에서의 가이드라인을 제시하고 있다. GMITS은 조직이 보유하고 있는 정보자산이 주요 대상이라고 할 수 있다. ISO/IEC TR 13335-1(Concepts and Models of IT Security)[8]은 정보기술 정보보호 관리를 설명하기 위한 기본적인 개념과 모델을 다루며, 조직의 전반적인 보안을 책임지고 있는 관리자나 정보보호 관리자들에게 도움이 된다. ISO/IEC TR 13335-2 (Managing and Planning IT Security)[9]는 관리와 계획의 측면을 다루고 있으며, 조직의 정보시스템 설계, 구현, 시험, 조달, 운영 및 사용에 관련된 담당자들에게 도움이 된다. ISO/IEC TR 13335-3 (Techniques for the Management of IT Security)[10]은 계획, 설계, 구현, 시험, 획득, 운영 프로젝트 Life-Cycle의 관리와 관련된 보안기술을 다루고 있다. ISO/IEC TR 13335-4(Selection of Safeguards)[11]은 대응책 선택을 위한 가이드를 제시하고, ISO/IEC TR 13335-3의 보안기술과의 연관성 및 대응책 선택 시 평가 방법 등에 관해 다루고 있다. ISO/IEC TR 13335-5(Management Guidance on Network Security)[12]는 외부 네트워크 및 인터넷과 연결된 사이트의 정보보호 관리와 유지보수에 대한 가이드를 제시, 대응책 선택과 사용, 대응책 구현 시 이용될 메커니즘과 표준 내용 포함한다.

2.3 ACSI33(Australian Government Information and Communication Technology Security Manual)

ACSI 33(Australian Government Information and Communication Technology Security Manual)[13]은 국방신호국(DSD ; Defence Signals Directorate)에서 호주 정부기관의 정보통신시스템(ICT Systems ; Information and Communications Technology Systems)의 보안정책과 지침(Guidance)을 제공하기 위하여 발행하고 있다.

ACSI33은 호주 정부기관 보안매뉴얼(PSM ; Protective Security Manual)[14]을 정보통신보안에 적용하기 위한 정보보안 관리 체계를 위한 매뉴얼로서, 호주 정부기관이 보안을 위하여 따라야 하는 보안정책, 기준 및 표준, 절차에 관한 내용을 정리하여 호주 정부기관들이 공통적으로 따라야 하는 최소한의 기준을 제시하고 있다. 호주 정부기관은 보안 매뉴얼에 의해서 정보시스템의 보호를 위한 적절한 보안정책과 대책, 계획을 수립하여 시행해야 한다.

〈표 1〉 ACSI33 ICT Security Process

단 계
1. 정책수립(Policy development)
2. 위험관리(Conduct risk management)
3. 계획수립(Plan development)
4. 실행(Implementation)
5. 인증(Certification)
6. 인정(Accreditation)
7. 유지(Maintenance)
8. 검토(Review)

ACSI33의 각 지침은 정보보 안관리를 위해서 필요한 사항에 따라 MUST, MUST NOT, SHOULD, SHOULD NOT, RECOMMENDS(or RECOM MENDED)로 표시하고 있다.

ACSI33의 ICT Security Process는 정보보안관리체계(ISMS)의 PDCA(Plan-Do-Cechk-Act) 모델을 충실히 반영하고 있다. 즉 정책수립 - 실행 - 검토 - 개선들로 이뤄진 절차를 정기적으로 수행하여 지속적인 보안강화가 이루어질 수 있도록 하고 있다.

2.4 FISMA(Federal Information Security Management Act)

FISMA(Federal Information Security Management Act)는 미국 연방정부 정보 및 정보시스템에 대한 정보보안을 강화하고 그 정보보안에 대한 효율성과 적절성을 확보하기 위하여 제정된 연방 정보보안 관리법이다. NIST(National Institute of Standards and Technology)[15]는 FISMA에 의거하여 연방 정부의 정보보안과 관련하여 SP(Special Publication) 시리즈를 발표하고 있으며, 컴퓨터 보안과 관련하여 FIPS(Federal Information Processing Standards Publications)를 발표하고 있다.

연방 정부 부처들은 FIPS 200(Minimum Security Requirements for Federal Information and Information Systems)[16]을 반영하여 FIPS 199 (Standards for Security Categorization of Federal Information and Informaton Systems)[17]와 NIST SP 800-53(Recommended Security Controls for Federal Information Systems)[18]를 활용한 표준화된 보안 통제항목(Control)을 선택하고, NIST SP 800-18(Guide for Developing Security Plans for Federal Information Systems)[19]에 의하여 정책 수립과 정보보안 관리에 대한 문서화를 수행해야 한다.

또한, NIST SP 800-53A(Guide for Assessing the Security Controls in Federal Information Systms)[20], NIST SP 800-26(Security Self-Assessment Guide for Information Technology Systems)[21]에 의한 평가를 수행하고, NIST SP 800-37(Guide for the Security Certification and Accreditation of Federal Information System)[22]에 의한 인증 및 인정(Accreditation)을 받는다.

각 연방 정부 부처는 자체 보안 프로그램 수행과 지침 및 표준 준수에 대한 평가 결과를 관리예산처(OMB ; Office of Management and Budget)에 보고하고, 관리예산처와 회계감사원(GAO ; General Accounting Office)은 평가 및 분석결과를 의회와 국민에게 공표하고, 그 성과를 측정하여 정보화 예산 편성시 반영하도록 하고 있다.

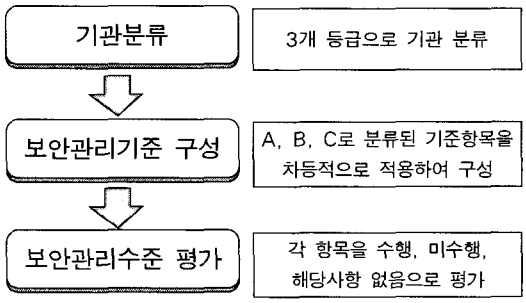
FISMA 정보보안 관리 체계는 ISO/IEC 27001의 기본적인 체계를 따르고 있으며, 통제항목의 구성과 문서화, 정부 조직 차원에서의 체계적인 구성이 이루어져 있다. 또한 관리예산처와 회계감사원을 통한 예산 편성 반영으로 정보보안 관리 체계에 대한 실효성을 크게 강화하였다.

ISO/IEC 27001과 BS 7799는 보편적인 정보보안관리 체계로서 통제항목의 구성을 수행 기관의 자율성에 전적으로 의지 하는데 반해서, FISMA는 최소 보안 통제항목(minimum security controls)을 두어 연방 정부 부처가 수행해야 하는 최소한의 필수 보안관리 사항을 강제하고 있다.

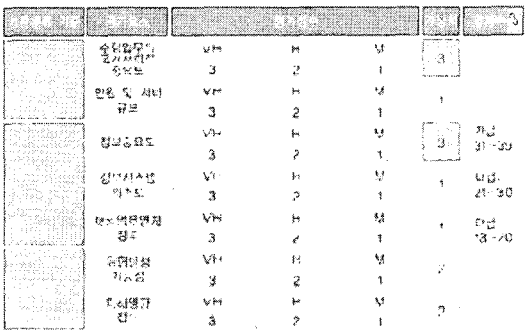
3. 보안관리수준 평가

"국가사이버안전매뉴얼"의 "보안관리수준 평가" 체계를 간략히 살펴보면 (그림 1)과 같다.

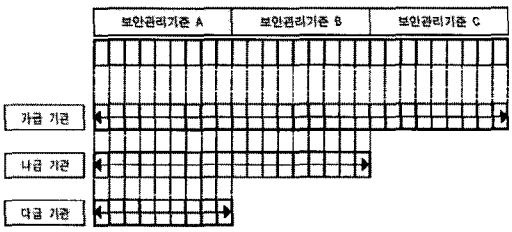
국가·공공기관은 3개 분류기준, 7개의 평가요소로 구성된 (그림 2)의 기관분류 기준을 자체적으로 평가하여 '가', '나', '다'의 3개 등급으로 해당 기관을 분류하게 된다. '가'급으로 분류된 기관은 가장 높은 보안관리 기준을 적용받게 된다.



(그림 1) 보안관리수준 평가 체계



(그림 2) 기관분류 기준



(그림 3) 기관등급별 보안관리 기준 적용

보안관리 기준은 각 항목을 A, B, C로 구분하여 놓았는데, A항목은 보안관리를 위한 필수적인 기준으로 모든 기관들이 필히 수행해야 하는 항목이며, B항목은 중요 정보통신시스템 운영기관이 수행해야 하는 항목이며, C항목은 매우 중요한 정보시스템을 운용하는 기관이 추가적으로 수행해야 하는 항목이다. 따라서 각 항목은 앞서 분류된 기관등급에 따라 (그림 3)과 같이 차등적으로 적용된다. 이에 따라서 '가'급 기관은 총 253개의 보안관리 기준을, '나'급 기관은 222개, '다'급 기관은 139개의 보안관리 기준을 적용받게 된다.

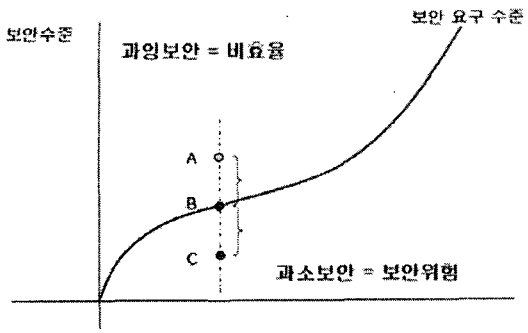
4. 보안관리수준 평가 체계 분석

앞서 살펴본 바와 같이 "보안관리수준 평가" 체계는 기관을 분류하고, 그 분류에 따라서 통제항목(Controls)인 보안관리 기준을 차등적으로 적용하고 있다. 이는 기관의 중요도에 따라 최소한의 필수적 수행이 필요한 보안관리 기준을 강제하는 것에서 FISMA와 유사하지만, FISMA가 최소 보안 통제항목(minimum security controls)을 두고 그 외의 통제항목은 표준 통제항목에서 선택하도록 하는 것에 비해서는 보다 유연성이 떨어지는 구조라고 할 수 있다.

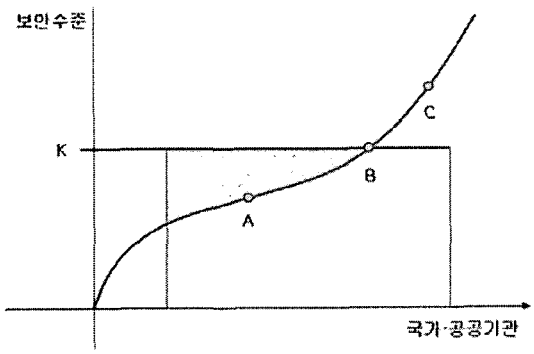
따라서 본 논문에서는 "보안관리수준 평가" 체계를 보안관리의 효율성과 적합성 측면에서 시각화 분석(Visualization analysis)해 보고, 그 근본적인 체계의 수정없이 효율성과 유연성을 향상 시킬 수 있는 개선 방안을 제시하였다.

4.1 단일 수준 보안관리 기준

(그림 4)와 같이 각 기관이 필요로 하는 보안요구 수준이 그래프의 곡선과 같다고 할 때, 해당 조직에 가장 적합한 보안관리 기준(또는 통제항목)의 수준은 기관의 보안요구 수준과 일치하는 B점이라고 할 수 있다. A점에서 보안관리 기준이 수립되어 적용되는 경우에는 과잉 보안이 이루어지는 점으로, 필요한 보안요구 수준을 만족하지만, 추가적인 비용과 시간의 투자와 필요 이상의 사용자 편의성, 업무 효율성 저해가 일어나는 점이 된다. 반면 C점은 과소 보안이 이루어지는 점으로, 조직에서 요구되는 보안요구 수준을 만족하지 못함으로 인해 보안위험이 여전히 존재하는 점이 된다.



(그림 4) 보안요구 수준과 과잉, 과소 보안

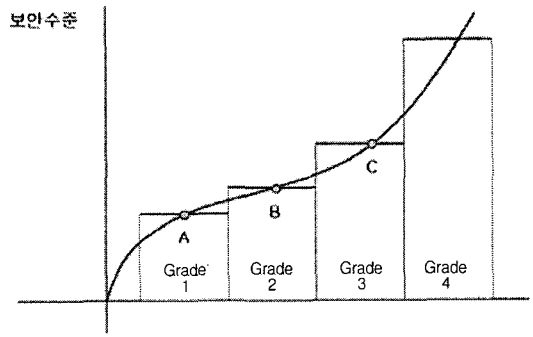


(그림 5) 단일 수준 보안관리 기준

이렇게 서로 다른 정보보안 요구 수준을 가지는 다양한 기관들에 대해서 획일화된 보안관리 수준을 적용하는 것은 지나친 보안으로 인한 효율성의 저해나, 미비한 보안으로 인한 보안 문제점을 노출하게 된다. (그림 5)와 같이 서로 다른 보안관리 수준이 필요한 국가 · 공공기관이 X축에 정렬되어 있다고 가정하는 경우(원점에서 멀어질수록 보다 높은 보안관리 수준이 요구됨), 보안관리 기준이 K 수준에서 단일하게 정의되는 경우, B점에 위치하는 기관은 적합한 보안관리가 이루어지겠지만, B점보다 원점에 가까운 기관들은 불필요한 과잉 보안에 의한 비용과 시간의 낭비를 가지게 되며, B점보다 원점에서 멀리 떨어진 C점에 위치한 기관은 실제로 필요한 보안관리 수준보다 낮은 과소 보안이 이루어지게 되어 보안위험을 가지게 된다.

4.2 다수준 보안관리 기준

기관의 서로 다른 보안수준 요구를 만족하도록 보안관리 기준을 차등적으로 구분하여 적용하는 것은 앞서의 과잉 및 과소보안을 최소화할 수 있도록 한다. (그림 6)은 4개의 서로 다른 수준을 가지는 보안관리 기준 체계를 각 조직 A, B, C에 차별적으로 적용한 예를 보여주고 있다. A, B, C에 각각 Grade 1, 2, 3를 적합하게 적용함으로서, 앞서 (그림 5)에서 나타났던 과잉, 과소 보안이 없이 해당 조직의 보안 요구 수준을 만족할 수 있음을 알 수 있다.

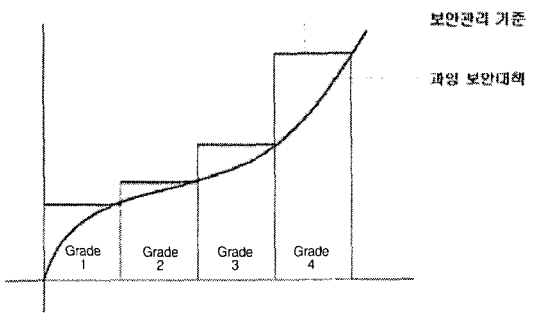


(그림 10) 다수준 보안관리 기준

"국가사이버안전매뉴얼"에 의한 "보안관리수준 평가"는 이렇게 보안관리 기준을 여러개의 수준으로 차등 적용함으로써 기존의 획일적인 기준에 의한 과잉, 과소보안을 줄이고 효율적인 보안관리가 이루어지도록 하고 있다.

효율적인 보안관리를 위해서는 과잉, 과소 보안이 일어나지 않도록 해야 하며, 특히 안전한 정보통신시스템 운영을 위해서는 과소보안이 이뤄지지 않아야 한다. 따라서 적용되는 보안관리 수준은 한 조직에서 요구되는 보안수준을 모두 만족하는 최소 보안관리수준을 적용하여야 한다. 예를 들면, (그림 6)에서 Grade 3, 4는 모두 C점의 보안수준을 만족하지만 과잉보안이 최소화되는 최소 보안관리수준 Grade 3을 적용하는 것이 가장 효율적이

다. 즉, 과소보안이 일어나지 않으면서 과잉 보안이 최소화되는 정보 보안관리수준을 적용해야 하는 것이다. 이를 그래프로 살펴보면 (그림 7)과 같이 각 보안관리 기준은 그 보안수준을 적용받는 기관의 보안요구 수준보다 항상 높아야 한다.

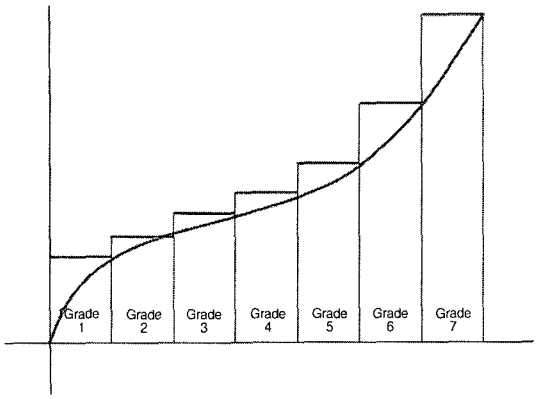


(그림 15) 과소보안이 없는 다수준 보안관리 기준 적용

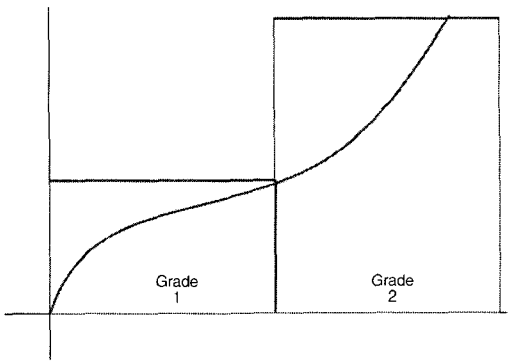
안전한 보안관리가 이뤄지도록 하기 위하여 보안관리 기준이 항상 기관의 보안관리 요구 수준보다 높게 구성되는 것은 보안을 위해서는 바람직하지만, 과잉보안에 의한 비효율성이 일정부분 존재하게 된다.

즉, 다수준 보안관리 기준을 도입하는 경우에도 (그림 7)과 같이 항상 일정부분의 과잉보안이 존재하게 된다. 과잉보안에 의한 비효율성을 줄이는 방법으로는 각 보안관리 기준의 단계를 좀 더 미세하게 구성함으로서 각 기관이 요구하는 보안수준과 보안관리 기준과의 차이를 줄이는 방법이 있을 수 있다. (그림 8)과 같이 보안관리 기준의 단계를 세부적으로 구성하게 되면 (그림 9)와 같이 단계를 적게 구성한 것에 비해서 과잉보안 영역(각 단계에서 보안요구 수준 그래프에 의해 나누어진 윗부분의 면적)이 크게 감소하는 것을 알 수 있다.

따라서 과잉 보안을 최소화하기 위해서는 많은 단계로 미세하게 구성된 보안관리 기준을 구성하는 것이 해결책이 될 수 있다. 하지만 많은 단계로 이루어진 보안관리 기준을 구축하는데는 그렇지



(그림 23) Fine grade(미세 단계) 보안관리 기준 구성



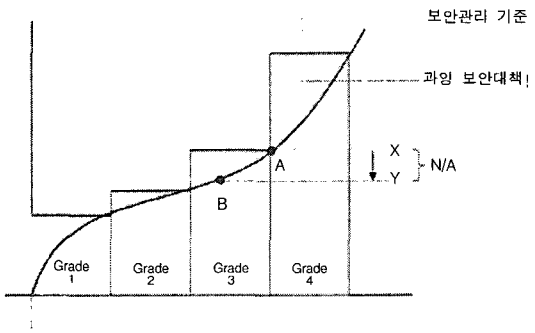
(그림 26) Coarse grade(성긴 단계) 보안관리 기준 구성

않은 경우에 비해서 더 많은 복잡성과 비용이 요구되며, 이를 적용하여 운영하는데 있어서도 이에 따른 비효율성이 증가하게 된다. 보안관리 기준을 여러 수준으로 구성하고 차별화된 기준을 적용하는 것은 정보보안활동의 효율성을 증대시키기 위한 것이므로, 과잉 보안을 제거하기 위하여 무조건적으로 많은 단계의 보안관리 기준을 구성하는 것은 바람직하지 못 하다. 따라서 이러한 점을 고려하여 적절한 단계의 보안관리 기준을 구성하여야 한다. 즉, 단계 구성에 따른 과잉보안과 단계 구축 및 운영비용의 합이 최소화되는 점에서 보안관리 기준을 구성하여야 하는 것이다.

4.3 미적용(N/A : Not Applicable) 항목 적용

"보안관리수준 평가"는 보안관리 기준의 단계를 '가', '나', '다'의 3등급으로 구분하여 구성하였다. 이는 이보다 더 세밀하게 단계가 구성된 것에 비하여 과잉보안에 의한 비효율성이 일정부분 존재하는 것을 의미하기도 한다.

이러한 과잉보안 요소를 제거하고 효율적인 보안관리가 수행될 수 있도록 하기 위하여 미적용(N/A ; Not Applicable) 항목을 도입하였다.

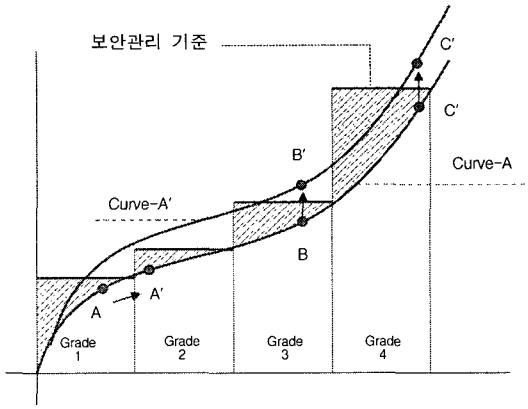


(그림 37) 미적용(N/A ; Not Applicable) 항목에 의한 과잉보안 제거

(그림 10)의 A기관은 X 수준의 보안관리 기준에 의해서 적합한 보안관리가 이뤄지지만, B기관은 X-Y만큼의 과잉보안에 의한 비효율성이 존재하게 된다. 따라서 적용되는 X 수준의 보안관리 기준에서 불필요한 기준 항목을 미적용(N/A)으로 지정하여 제거함으로써 B기관은 과잉보안을 제거하고 효율적인 보안관리를 수행할 수 있다.

4.4 보안관리 요구 수준의 변화

지금까지 "보안관리수준 평가" 체계가 어떻게 기관에 적합한 효율적 보안관리를 수행할 수 있는지를 분석해 보았다. 이 절에서는 기관의 보안관리 요구 수준이 변화되는 경우에 "보안관리수준 평가" 체계의 효율성에 대해서 분석해 보고자 한다.



(그림 52) 보안관리 요구 수준의 변화

(그림 11)은 기관의 보안관리 요구 수준이 변화되는 몇 가지 경우를 보여주고 있다. 먼저 A기관이 A'으로 보안관리 요구 수준이 변화되는 경우에는 Grade 2로 기관분류를 상향 조정함으로써 적합한 보안관리를 수행할 수 있다.

만일 정보통신 환경의 변화 등으로 전체 기관들의 보안관리 요구 수준 분포가 Curve-A에서 Curve-A'으로 이동되는 경우에 B기관은 B'으로 상향 이동된다. 이때에는 Grade 4로 기관분류를 상향 조정함으로써 적합한 보안관리를 수행할 수 있다. 그러나 C기관의 경우는 C'을 만족하는 보안관리 수준이 없기 때문에 과소보안이 이루어지게 된다.

이러한 문제를 해결하기 위해서는 전체적인 보안관리 수준 체계를 재조정함으로써 가능하다. 즉, 새롭게 Grade 5를 구성하거나, Grade 4가 C'을 만족할 수 있도록 확장되어야 한다.

이러한 전체 체계에 대한 조정은 지속적으로 급변하는 정보보안 환경에 대하여 신속한 변화 대응이 어렵고, 많은 시간과 비용이 소모되어 유연성과 효율성이 크게 떨어진다.

ISO/IEC 27001, BS 7799는 통제항목(Controls)에 대하여 선택과 구성을 기관(기업)의 자율에 전적으로 맡기고 있으며, FISMA는 필수 통제항목을 제외한 통제항목의 추가, 구성을 자율에 맡기고 있어 앞서와 같은 문제로부터 유연하게 대응할 수 있다. 하지만, "보안관리수준 평가"는 정해진 보안관리 기준 집합(Control set)에서 미적용 항목의 선택만 가능하므로 이러한 환경의 변화, 또는 기관에 특화되어 필요한 보안관리 요구에 대하여 유연성이 크게 떨어진다.

4.5 보안관리수준 평가의 장단점

"보안관리수준 평가"는 기관분류에 의한 3단계 보안관리 기준(통제항목)의 차등적용과 미적용 항목 도입으로 획일화된 보안관리 기준에 의한 과잉, 과소보안 활동의 비효율성을 제거하여 효율적인 보안관리가 이루어질 수 있도록 하고 있다. 또한 기관 자체적으로 모든 통제항목을 구성하지 않고 기관분류에 따라 정의된 보안관리 기준을 적용하므로 FISMA에 비해서 보다 간결하고 편리하다고 할 수 있다.

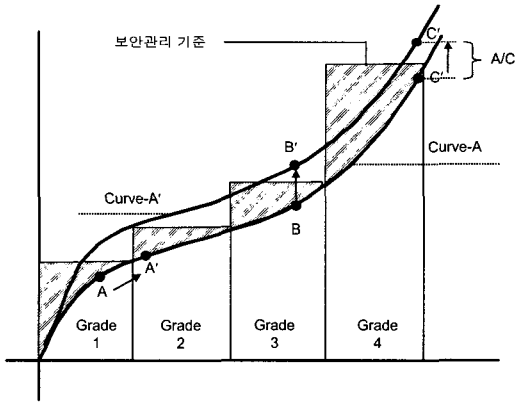
그러나 한편으로는 각 기관분류에 통제항목이 고정적으로 구성되어 각 기관의 자율성이 미적용 항목의 선택만으로 제한되며, 각 기관의 특성에 맞는 적합한 통제항목을 추가적으로 구성할 수 없으며, 급변하는 정보통신 환경에 맞춰 기관 스스로가 보안관리 통제항목을 구성하는 유연성이 크게 떨어지게 된다.

5. 보안관리수준 평가 체계 개선안

"보안관리수준 평가" 체계의 간결성과 편리성을 살리면서도 ISO/IEC 27001, BS 7799와 같은 유연성을 확보하고, FISMA와 같이 정부 부처가 필수적으로 수행해야 하는 필수 통제항목 강제의 장점을 살릴 수 있도록 하기위하여, 본 논문에서는 추가항목(A/C ; Additional Control)의 도입, 선택적 보안관리 기준 구성, 평가 준비 절차의 개선을 제안하고 있다.

5.1 추가항목의 도입

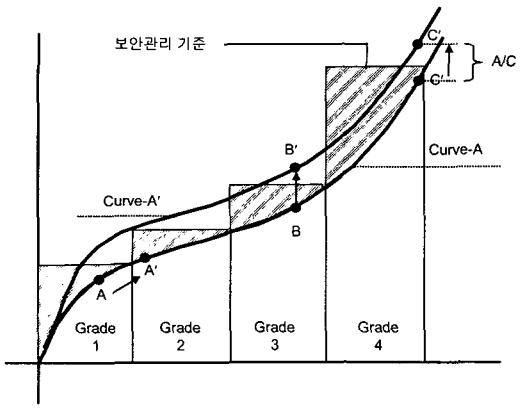
미적용 항목만으로도 각 기관의 보안 요구 수준에 적합한 효율적 보안관리가 가능하지만, 추가항목(A/C; Additional Control)의 도입이 필요하다. 추가항목의 도입은 미적용 항목보다 편리하게 효율적인 보안관리 기준 조정이 가능하며, 새로운 정보통신 환경과 보안 요구 사항에 유연하게 대응할 수 있는 이점을 준다.



(그림 53) 미적용(N/A ; Not Applicable) 및 추가항목(A/C ; Additional Control)의 적용

(그림 12)와 같은 경우, 미적용 항목만 적용되는 경우에는 Grade 4를 적용하고 X-Y만큼의 미적용 처리가 필요하다. 하지만 추가항목을 적용할 수 있는 경우에는 Grade 3을 적용하고 Y-Z만큼의 추가항목(A/C)만으로 쉽게 적합한 보안 요구 수준을 달성할 수 있다. 또한 구성된 각 보안관리 기준외에 각 기관에 특화되어 필요한 보안관리 항목이 있거나, 새로운 보안관리 요구 사항이 생기는 경우

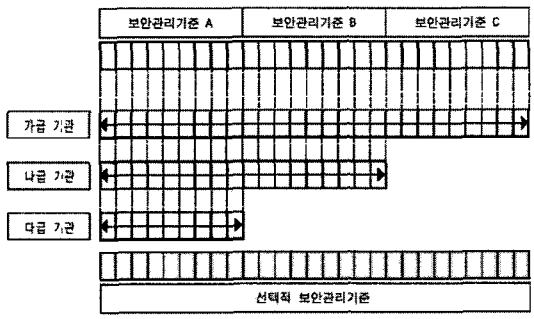
에도 전체 구성의 변경없이 쉽게 추가항목을 도입함으로써 유연하게 대처할 수 있게 된다. (그림 13)은 정보환경의 변화로 인하여 C'에서 과소보안이 생기는 경우에도 추가항목을 통하여 적합하게 수행될 수 있음을 보여주고 있다.



(그림 54) 추가항목(A/C : Additional Control)의 적용에 의한 유연성 확보

5.2 선택적 보안관리 기준의 도입

추가항목은 기관이 필요에 의해서 스스로 구성할 수도 있으나, 이와 더불어서 FISMA의 NIST SP 800-53(Recommended Security Controls for Federal Information Systems)과 같은 표준화된 통제항목들을 사전에 정의하여 놓고, 이러한 통제항목에 대해서는 기관분류에 관계없이 기관의 필요에 의해서 자율적인 선택이 가능하도록 병행하면 추가항목 구성의 편리성과 통제항목의 일관성을 동시에 확보할 수 있다.

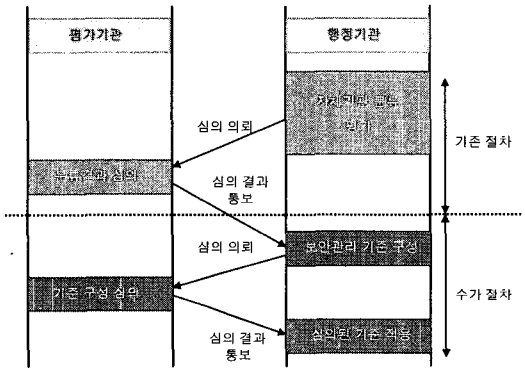


(그림 55) 선택적 보안관리 기준(Selective Controls)

따라서, 보안관리 기준의 구성은 (그림 14)과 같이 선택적 보안관리 기준(Selective Controls)을 추가적으로 구성하여 기관이 자율적으로 선택할 수 있도록 개선하는 것이 필요하다.

5.3 보안관리수준 평가 준비 절차 개선

추가항목과 선택적 보안관리 기준의 도입으로 각 기관에 가장 적합하게 보안관리 기준이 구성될 수 있는 유연성과 자율성이 크게 확보되지만, 기존과 달리 같은 등급의 기관이라도 서로 다른 보안관리 기준 집합(Control set)을 가지게 된다. 따라서, 기관이 자율적인 기관분류와 미적용, 추가항목 적용으로 구성한 보안관리 기준에 대하여 적절성을 심의하고 보안관리 기준을 확정하는 (그림 15)와 같은 절차가 추가적으로 필요하다.



(그림 56) 보안관리수준 평가 준비 절차 개선

각 기관은 자체적으로 기관을 분류하고, 기관분류에 따라 차등적인 보안관리 기준을 적용받으며, 필요에 의해서 미적용, 추가항목을 적용하여 보안관리 기준 집합(Control set)을 자유롭게 구성한다. 이렇게 구성된 보안관리 기준은 기관에 최적화된

보안관리 기준 프로파일이라고 할 수 있다. 이러한 보안관리 기준 프로파일은 평가기관에 의해서 그 타당성과 적합성을 심의받고 최종 확정되어 수행되게 된다. 이렇게 함으로써 기존의 "보안관리수준 평가"에 비해서 보다 유연하고, 각 기관에 특화된 보안관리 기준을 적용할 수 있도록 개선될 수 있다.

6. 결 론

본 논문은 ISO/IEC 27001, BS 7799의 국제 표준과 ACSI33에 의한 호주 정부부처 보안관리 체계, FISMA에 의한 미연방 정부부처 보안관리 체계를 살펴보고, "국가사이버안전매뉴얼"의 "보안관리 수준 평가" 체계를 분석하였다. 이를 통하여 "보안관리 수준 평가" 체계가 효율적인 보안관리를 어떻게 수행할 수 있는지 고찰하고, 관련 체계와 비교하여 장, 단점을 분석하였다.

이러한 분석을 통하여 현행 "보안관리수준 평가" 체계는 각 기관의 특성에 맞는 적합한 통제항목을 추가적으로 구성할 수 없으며, 급변하는 정보통신 환경에 맞춰 기관 스스로가 보안관리 통제항목을 구성하는 유연성이 크게 떨어짐을 알 수 있었다.

따라서, 본 논문에서는 이러한 단점을 극복하여 ISO/IEC 27001 및 FISMA의 효율성과 유연성을 확보하면서, 현행 "보안관리수준 평가" 체계의 장점을 유지할 수 있는 개선안을 제시하였다.
기존의 체계에 추가항목(A/C ; Additional Control), 선택적 보안관리 기준(Selective Controls) 구성을 도입하고 평가 준비 절차의 개선을 통하여 각 기관에 최적화된 보안관리 기준 프로파일을 작성할 수 있도록 함으로써, 기관에 적합한 효율적 보안관리의 수행이 가능하고 급변하는 정보통신 환경에 유연하게 대응할 수 있도록 하였다.

참 고 문 헌

[1] "BS 7799 Part 1 : The Code of Practice for Information Security Management(BS 7799-1 : 2005)", British Standards Institution, UK, 2005.

[2] "BS 7799 Part 2 : The Specification for Information Security Management Systems (BS 7799-2 : 2002)", British Standards Institution, UK, 2002.

[3] "The Code of Practice for Information Security Management(ISO/IEC 17799 : 2005)", International Standards Organization, 2005.

[4] "The Specification for Information Security Management Systems(ISO/IEC 27001 : 2005)", International Standards Organization, 2005.

[5] "국가사이버안전관리규정(대통령훈령 제141호)", 2005.

[6] "국가사이버안전매뉴얼", 국가사이버안전센터, 2005.

[7] "Federal Information Security Management Act of 2002", US federal law : E-Government Act of 2002. USA, 2002.

[8] "Information technology - Guidelines for the management of IT Security (GMITS) Part 1 : Concepts and models for IT Security (ISO/IEC TR 13335-1)", International Standards Organization, 1996.

[9] "Information technology - GMITS Part 2 : Managing and planning IT Security(ISO/IEC TR 13335-2)", International Standards Organization, 1997.

[10] "Information technology - Security techniques - GMITS Part 3 : Techniques for the management of IT Security(ISO/IEC TR 13335-3)", International Standards Organization, 1998.

[11] "Information technology - GMITS - Part 4: Selection of safeguards(ISO/IEC TR 13335-4)", International Standards Organization, 2000.

[12] "Information technology - GMITS - Part 5: Management guidance on network security(ISO/IEC TR 13335-5)", International Standards Organization, 2000.

[13] "Australian Government Information and Communications Technology Security Manual", Defence Signals Directorate, Aus, 2005.

[14] "Protective Security Manual(PSM 2005)", Attorney General's Department, Aus, 2005.

[15] National Institute of Standards and Technology, http://www.nist.gov

[16] "Minimum Security Requirement for Federal Information and Information Systems(FIPS 200), National Institute of Standards and Technology, USA, 2006.

[17] "Standards for Security Categorization of Federal Information and Information Systems(FIPS 199)", National Institute of Standards and Technology, USA, 2004.

[18] "Recommended Security Controls for Federal Information Systems(NIST SP 800-53, Rev. 1)", National Institute of Standards and Technology, USA, 2006.

[19] "Guide for Developing Security Plans for Federal Information Systems(NIST SP 800-18, Rev. 1)", National Institute of Standards and Technology, USA, 2006.

[20] "Guide for Assessing the Security Controls in Federal Information Systems(NIST SP 800-53A)", National Institute of Standards and Technology, USA, 2006.

[21] "Security Self-Assessment Guide for Information Technology Systems(NIST SP 800-26, Rev. 1)", National Institute of Standards and Technology, USA, 2005.

[22] "Guide for the Security Certification and Accreditation of Federal Information Systems(NIST SP 800-37), National Institute of Standards and Technology, USA, 2004.

민 병 길

2002년 충북대학교 컴퓨터공학과(공학사)

2004년 포항공과대학교 대학원 컴퓨터공학과(공학석사)

2004년~현재 국가보안기술연구소 연구원

이 도 훈

1989년 한양대학교 전산학과(공학사)

1991년 한양대학교 대학원 전산학과(공학석사)

1991년~2000년 국방과학연구소

2000년~현재 국가보안기술연구소