Multi-level 보안 아키텍처(MLSA) 구축 방안

최경호* · 이동휘* · 김쿠남**

요 약

보안 평가 체계에서 요구하는 보안 수준은 제시되는 세부지침, 가이드라인 및 우수 구현 사례를 이용하여 달성될 수 있다. 그러나 조직이 2가지 이상의 서로 다른 보안 인증 체계를 요구 받는 경우, 중점 평가 기준, 보안 요구 수준, 평가 항목들이 상이하기 때문에, 보안 아키텍처의 재구축 또는 변경 절차가 요구된다. 따라서 본 연구에서는 ML Analysis를 이용하여 제시되는 다양한 보안 관리 수준을 달성하기 위한 Multi-level 보안 아키텍처(MLSA) 구축 방법론을 제시한다. MLSA는 다양한 보안인증체계의 동시적 달성을 위한 방법론을 제공한다.

A Study on Development of Multi-level Security Architecture(MLSA)

Kyong Ho Choi* · Dong-Hwi Lee* · Kuinam J. Kim**

ABSTRACT

We need development methodology of security architecture which offered various levels of security management in case of the organization required more than two security certifications. In this study, therefore, development methodology of Multi-level Security Architecture(MLSA) proposed. Specifically, we should consider factors of commonness and difference between information security management level evaluation of multiple security architecture. This kinds of endeavor can suggest the direction of the improvement of the evaluating security management and the dynamic plan for the security architecture, and it will make the continuous and systematic security management.

Key words : Security Management, Security Architecture

* 경기대학교 정보보호학과
** 경기대학교 정보보호학과 교수

1. 서 론

개별 조직 및 기관에서는 국내 또는 국제적으로 공신력 있게 제시되는 보안 평가 체계에서 제공하는 세부지침, 가이드라인 및 우수 구현 사례를 이용하여 보안 아키텍처를 구축하고 유지·관리하는 방법을 주로 취하고 있다. 이러한 방법은 보안 평가 체계에서 요구하는 보안 수준을 손쉽게 달성할 수 있고, 표준화된 보안 아키텍처를 구성할 수 있다는 장점이 있으나, 보안 평가 체계의 기준 변경 또는 새로운 항목 신설에 따른 보안 아키텍처 종속화 현상이 나타날 수 있으며, 다른 보안 체계 인증을 위해서는 또 다시 보안 아키텍처를 구축하여야 한다는 단점이 있다. 이와 같은 관점에서 서로 다르게 제시되는 국내외의 보안 인증 체계를 동시적으로 만족시킬 수 있는 보안 아키텍처가 요구되며, 이를 효율적으로 적용하고 지속적인 유지·관리를 위한 구축 방법론이 절실히 요구된다.

따라서 본 연구에서는 국내 기준과 국제 기준의 보안 인증 체계에서 서로 다르게 요구하는 보안 수준의 동시적 달성을 위한 Multi-level 보안 아키텍처(MLSA)의 구축 방법론을 제시하고자 한다. 이어지는 제 2장에서는 보안 아키텍처의 개념 및 구성을 파악하고, 이를 평가하는 국내 기준인 정보보안관리수준 평가, 국제 기준인 ISO 27001에 대하여 살펴본다. 이후의 제 3장에서는 국내외의 보안 평가 기준의 동시적 달성을 위한 MLSA 구축 방법론을 제시하고 제 4장에서는 제시된 보안 아키텍처 모델을 토대로 실제적 구현 사례를 분석하며, 마지막으로 본 연구의 의의 및 향후 연구방향 제시로 결론을 맺고자 한다.

2. 관련 연구

2.1 보안 아키텍처

정보시스템의 효율적 도입 및 운영 등에 관한 법률에서는 보안 아키텍처를 '정보시스템의 무결성, 가용성, 기밀성을 확보하기 위해서 보안요소 및 이들 간의 관계를 식별하고 정의한 구조'라고 정의하고 있다. 이러한 보안 아키텍처는 각국의 다양한 평가/인증 기관에서 요구하는 보안체계 및 규범에 따라 형태와 구성이 복합적으로 표현되고는 있지만, 정보보호의 목표 및 정보보호 요구 수준을 달성하기 위한 정보보호 활동은 일관적인 방향성을 가지고 추진되고 있다.

그러나 엄연히 서로 다른 보안 인증 체계에서 제시하는 중점 평가 기준, 보안 요구 수준, 평가 항목들이 상이하기 때문에 서로 다른 보안 인증이 요구되는 경우, 현재 제시되고 있는 보안 아키텍처 구축 방법론들은 보안 평가 항목 및 보안관리체계의 수정으로 보안 아키텍처를 다시 구축하거나, 재구성해야 하는 단점을 지니고 있다.

그러므로, 2가지 이상의 서로 다른 보안 인증 체계에서 제시하는 다양한 보안 관리 수준을 달성하기 위한 보안 아키텍처 구축 방법론과 이를 통한 다양한 수준의 보안 요구사항의 동시적 만족을 이끌어낼 수 있는 효율적인 접근법이 요구되어 진다.

2.2 국내 기준 : 정보보안관리수준 평가

국내에서 제시된 정보보안관리수준 평가는 국가사이버안전관리규정 제9조 제4항에 의거 사이버안전대책의 강구여부 등 정보통신망에 대한 안전성을 확인하기 위해 각급기관이 정보시스템의 중요도에 따라 소요되는 보안대책을 적절히 강구하고 있는지를 평가하는 것이다[1]. 이는 보안관리 기준을 여러 개의 수준으로 차등 적용함으로써 기존의 획일적인 기준에 의한 과잉, 과소보안을 줄이고 효율적인 보안관리가 이루어지도록 한다[2].

정보보안관리수준 평가에서는 효율적인 보안관리를 위해서 점검항목을 A, B, C 항목으로 분류하고 있으며, 기관분류 결과에 따라 차별화된 점검항목을 적용한다. 적용된 점검항목은 점검분야별 평

가, 점검분야 누적 합산, 종합 평가의 단계를 거쳐 최우수, 우수, 양호, 미흡, 불량과 같이 5개 등급으로 보안관리 수준이 평가된다. 각각의 점검항목은 '평시 안전점검 체크리스트'에 나타나 있다.

2.3 국제 기준 : ISO 27001

ISO 27001은 1995년 영국의 BSI가 개발한 정보보호관리 표준 BS 7799에서 발전된 형태이다. 여기서는 정보를 '사업상 필요한 다른 중요한 자산과 마찬가지로 가치를 가지며, 이에 따라 적절히 보호될 필요가 있는 자산'으로 정의하고 있으며, 이의 비밀성, 무결성, 가용성 유지를 위한 요구사항으로서 보안정책, 보안조직, 자산 분류 및 통제, 인적 보안, 물리적·환경적 보안, 통신 및 운영 관리, 접근통제, 시스템 도입·개발 및 유지보수, 보안사고 관리, 사업 연속성 계획, 준거성 등 11개 분류에 대한 133개 통제항목으로 구성되어 있다.

ISO 27001은 효과적인 정보보호 활동을 위해 PDCA 모델을 적용하고 있다[3]. 이의 목적은 보호해야 할 자산을 식별하고, 이를 누가 어떤 형태로 어디에 보관, 사용하고 있는지를 파악하고, 이 자산에 어떠한 위협과 취약성이 존재하며, 그 가능성은 얼마나 높으냐를 바탕으로 적절한 보안 대책들을 구현하여 이를 실행에 옮기면서, 지속적으로 모니터링하고 있다가, 문제점이 발견되면, 보완·개선해나가는 프로세스를 지속적으로 유지하는 것이다[4].

2.4 국내외 기준 분석

앞 절에서 살펴본 국내 기준의 정보보안관리수준 평가와 국제 기준의 ISO 27001은 그 필요성, 정보보호 구조 및 구성에서 차이가 있다. 먼저, 정보보안관리수준 평가의 경우 공공 부문에서의 자체적인 보안관리 활동을 위한 기준안으로 제시되고 있으며, 이의 진행 상황에 대한 보고 및 검토를 요구받고 있다. ISO 27001은 조직의 정보보호 활동에 대한 국제적인 신인도 확보 노력으로 나타나며, 이를 통해 국제적인 활동영역의 기반을 구축할 수 있다.

정보보안관리수준 평가와 ISO 27001의 보안 구조 면에서의 차이는 정보보안관리수준 평가 항목들은 무엇을 하였는지(What to Do)에 초점을 맞추고 있고, ISO 27001은 어떻게 하고 있는지(How to Do)에 중점을 두고 있기 때문에 나타난다.

국내 기준과 국제 기준의 보안 평가 항목 구성 면에서의 형태는 다음의 <표 1>에서 볼 수 있는 바와 같이 나타난다. 국내외의 양 기준은 정보통신환경 하에서 조직이 가진 정보자산 및 정보시스템들에 대한 관리적·물리적·기술적 정보보호 위협 요인을 식별하고, 이에 대한 대응책을 세우고 실행함으로써 정보보호의 주요 과제인 기밀성·무결성·가용성을 달성하고자 하는 목적으로 구성되었다. 이에 따라 정보보호정책, 정보보호 관련 조직, 정보 자산 분류 및 통제, 정보시스템 신규 도입 또는 변경, 개발 및 유지 보수 등과 같이 정보보호 요구사항 식별 영역은 비슷하게 나타나고 있다. 하지만 세부 평가 항목들의 구성은 각각의 영역 별로 교차되어 나타나거나, 또는 양 기준에서 공통적으로 제공되는 항목과 별도로 제공되는 항목으로 표현되고 있다. 즉, 정보보안관리수준 평가에서 평가 기준 항목으로 제공된 항목이 ISO 27001에서는 존재하지 않거나, 다른 영역에서 공통적인 평가 기준 항목으로 나타나고 있는 것이다. 이러한 국내 기준과 국제 기준의 상이성은 각 평가 기준 항목에서 제시하는 세부 기준을 검토할 때 그 차이가 더 많이 나타나고 있다.

이로써 양 기준에서 제시하는 보안 요구 수준의 동시적 달성을 위한 보안 아키텍처를 구축하기 위해서는 보안 아키텍처의 설계 단계부터 이 같은 차이점이 고려되어야 한다는 것을 알 수 있다.

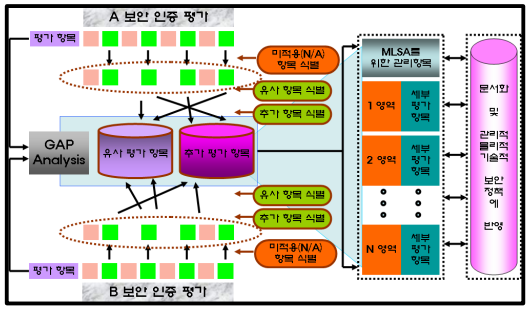
〈표 1〉 정보보안관리수준 평가와 ISO 27001의 구성 비교

정보보안관리수준 평가		ISO 27001	
대분류	항목수	대분류	항목수
1. 정보보안 관리체계	5	5. 보안정책	2
2. 정보보안 계획 및 활동	8	6. 보안조직	11
3. 정보자산통제	7	7. 자산 분류 및 통제	5
4. 인적보안	6	8. 인적보안	9
5. 물리적 보안	10	9. 물리적, 환경적 보안	13
6. 접근 보안대책	17	10. 통신 및 운영 관리	32
7. 운영관리	12	11. 접근통제	25
8. 시스템 개발 및 유지보수	7	12. 시스템 도입, 개발 및 유지보수	16
9. 보안 시스템	9	13. 보안사고관리	5
		14. 사업연속성 계획	5
		15. 준거성	10
합 계	81	합 계	133

3. Multi-level 보안 아키텍처(MLSA) 설계

국내의 정보보안관리수준 평가와 국제적 기준인 ISO 27001의 평가 항목들이 요구하는 정보보호 수준을 달성하기 위해, 보안 아키텍처를 준비하고 계획하는 단계에서부터 각각의 요구사항을 달성할 수 있도록 고려되어야 한다. 이에 따라 보안 아키텍처의 계획 단계에서 각각의 기준이 요구하는 평가 항목 및 이의 세부 기준에 대한 비교·검토가 이루어져야 하며, 이러한 방법은 (그림 1)에서 제시된 바와 같이 나타낼 수 있다.

MLSA를 구축하기 위한 세부 기준 추출 프레임워크의 각 단계별 국면에서의 추진 내용은 다음과 같다. 먼저, 국내 기준과 국제 기준에서 제시하는



(그림 1) MLSA 세부 기준 추출 프레임워크

영역별 보안 평가 항목과 여기에 귀속되어 있는 세부 기준들을 파악한다. 이를 토대로 먼저 미적용 항목의 추출을 통해 실제적으로 달성하고자 하는 각각의 보안 평가 항목을 설정한다. 다음으로 양 기준에서 충족시켜야 하는 보안 평가 항목들을 비교하여 유사 기준과 추가적으로 달성되어야 할 기준을 구분하여야 한다. 유사 기준은 국내 기준에 부합한 정보보호대책을 실행하면서 함께 달성할 수 있는 보안 요구 수준이며, 부가적인 보완 조치를 통해 보안정책의 일관성을 유지하면서 획득될 수 있는 보안 요구 수준을 의미한다. 추가 기준은 국내 기준과 국제 기준에서 공통적으로 적용되지 않는 부분으로써 양 기준의 동시적 적용을 위해 추가적으로 관리되어야 하는 보안 평가 항목을 의미한다.

그런데, 보안 평가 항목에서 제시하는 각각의 세부 기준들에 대하여 공통적인 또는 비공통적인 요소를 구분하여 이를 보완·개선하기 위한 정보보호대책을 수립하기에는 명확한 구분 기준이 필요하다. 이는 각각의 기준이 서로 다른 영역 구성 및 보안 구조를 가지고 있기 때문에, 각각의 기준이 가진 세부 기준들에 대한 연관성을 이해하고 파악할 수 있어야만 가능하다. 마찬가지로, 이러한 이해도는 각 기준에 대한 교차적인 수준까지 확보되어야 하며, 이를 위한 세부 기준 추출 설문서(ML Analysis)로 구체적인 검토 결과가 제시되어야 하고, 이에 대한 문서화 작업이 요구된다.

상기 내용으로 추진된 두 번째 단계에서의 실행 결과를 이용하여 유사 항목과 추가 항목으로 구분된 국내 기준과 국제 기준에서의 세부 보안 평가 항목들에 대해 MLSA에 반영해야 할 요소들을 식별하고 이의 추진 전략을 구체적으로 수립할 수 있다.

4. MLSA 분석

4.1 연구 수행 환경

본 연구에서 제안한 MLSA의 분석을 위해 동일한 규모로 평가되는 조직들에서 보안 아키텍처 구축 방법을 달리하였을 경우에 어떠한 평가 결과를 얻게 되는지를 살펴보고자 하였다. 이를 위해 보안 아키텍처를 필요로 하는 조직들 중 500인 이상의 인력, 정보시스템을 활용하여 조직의 주요 업무를 추진, 업무 개시 후 2년 이상 경과 등의 기준을 적용하여 선정하고, 이중 서로 다른 산업 분야에 속해 있는 D조직(IT 컨설팅 업체), T조직(서비스업), K조직(교육 기관)을 대상으로 국내 기준의 기관분류 기준에 의거하여 동일한 규모인지의 여부를 판별하였다.

세 개의 조직들은 모두 부분적 또는 IT 관점에서의 정보보안 업무가 진행되고 있었으나, 보안 아키텍처를 구축하기 위해 별도의 보안 TFT를 구성하여 이들이 전담으로 배치되어 활동하였다. D조직은 MLSA를 적용하여 국내 기준에서의 보안 평가 항목들에 대한 요구 수준 달성과 국제 기준인 ISO 2700의 인증 획득을 동시에 진행하고자 하였다. 그리고 T조직은 국제 기준인 ISO 27001의 인증을 목적으로 보안 아키텍처를 구축, 마지막으로 K조직은 국내 기준인 정보보안 관리수준 평가를 기준으로 보안 아키텍처를 구축하였다.

4.2 MLSA 실행

MLSA를 적용하기 위해 국내 기준인 정보보안 관리수준 평가와 국제 기준인 ISO 27001에 대한 ML Analysis 를 실행하여, 이 결과를 MLSA에 적용시키기 위한 추진 전략을 도출하고자 하였다. 도출된 추진 전략은 <표 2>와 같이 나타나며, 이의 기초 자료로 사용된 ML Analysis의 예는 <표 3>과 같이 볼 수 있다. 따라서 ML Analysis 결과 추가된 ISO 27001의 보안 평가 항목을 토대로 ISO 27001의 변화되는 구성을 살펴보면 다음 <표 4>와 같이 나타난다.

〈표 2〉 ML Analysis 결과 추가된 ISO 27001의 보안 평가 항목(예시)

ML Analysis 결과 추가된 ISO 27001 설문 내용	Y,P,N, N/A	비고
8.2.2 정보보호 교육 및 훈련		
정보보호 교육은 보안요구사항, 법적 책임, 보안 통제사항과 정보시스템의 올바른 사용을 포함하고 있는가 (이용수단 : 소집교육, 유인물 배포, 정보통신망 게재 등)		수정
연간 정보보안교육계획을 수립하여 시행하는가		추가
정보보안담당자 및 시스템관리자의 역량강화를 위한 전문 보안교육을 수행하는가		추가

〈표 3〉 MLSA 세부 기준 검토 결과표(예시)

07-04-01-04	평가 결과
	추가 (개선)

정보보안관리수준 평가
4. 인적보안
4.1. 인원보안
4.1.4 보안규정 준수

ISO 27001
8. 인적 보안
8.2 고용기간 중
8.2.3 징계 절차

<평가 근거> 정보보안관리수준 평가의 4.1.4의 2 세부 기준과 ISO 27001의 8.2.3의 1 세부 기준은 동일한 내용을 점검하는 보안 평가 항목임, 그러나 ISO 27001의 8.2.3의 2 세부 기준에 대한 추가적인 평가 항목으로 보안 평가 인증을 위한 보완 요소가 필요함

15. 준거성 15.2 보안정책 및 기술적 부합성 검토 15.2.1 정보보호 정책과의 부합
<평가 근거> 정보보호 규정 준수 여부에 대한 점검을 수행하였는지, 이는 주기적으로 행하여지고 있는지에 초점이 맞추어져 있음, 따라서, 내부 직원의 보안정책과 지침/절차 위배 여부와 규정 준수에 대한 감사가 직접적으로 직원평가에 반영할 수 있는 절차적 수단이 요구됨

<추진 전략> 15.2.1 정보보호 정책과의 부합에 내부자로부터 이행되는 평시 정보보호 활동 성과를 각종 직원 평가 제도에 반영하여 일정 기준을 충족시키도록 요구함, 직원 평가 제도는 인사고과, 성과급 지급 평가, 부서 활동비 지원 등 직접적인 인센티브에 반영하여, 보안 규정 준수에 대한 홍보 활동도 시행함

〈표 4〉 추가된 ISO 27001의 보안 평가 항목 구성

ISO 27001 설문 내용			추가 항목	추가적 ISO 27001 세부 기준 항목
대분류	항목 수	세부 기준		
보안정책	2	11	4	15
보안조직	11	41	2	43(1)
자산 분류 및 통제	5	9	·	9
인적보안	9	19	2	21(1)
물리적, 환경적 보안	13	40	4	44
통신 및 운영관리	32	207	12	219(2)
접근통제	25	130	10	140(3)
시스템 개발 및 유지보수	16	128	4	132
보안사고관리	5	23	1	24
사업연속성 계획	5	33	1	34
준거성	10	41	2	43
합 계	133	682	42	724(7)

주) ( ) 안의 항목은 세부 기준이 수정된 보안 평가 항목 수.

4.3 분석 결과

MLSA를 평가하기 위해 각기 다른 기준을 적용하여 보안 아키텍처를 구축한 세 조직에 대해 정보보안 관리수준 평가의 점검분야별 평가와 ISO 27001에서 제시되는 보안 항목 평가를 기준으로 현황 평가를 시행하였다. 단, 세 조직의 항목 구성의 차이에 따른 평가 결과 차이 발생을 방지하기 위해, 미적용(N/A) 항목은 전년도 정보보안활동과 관련된 내용인 1 세부 기준으로 한정하였다. 여기서는 제시된 평가 항목에 대해 수행한 항목 즉, 적정보안관리 수준을 달성한 항목들에 대한 백분율을 비교하여 살펴보고자 하였으며, 이는 제시된 보안 평가 항목들 중 수행된 비중을 확인하기 위함이다. 각각의 조직에서 적용된 보안 아키텍처의 국내 기준 평가 결과, 국제 기준 평가 결과는 다음과 같다.

〈표 5〉 세 조직의 SA 국내 기준 평가 결과

정보보안관리수준 평가					
대분류	항목 수	세부 기준 수	MLSA 수행 비중 (%)	국제 기준 SA수행 비중(%)	국내 기준 SA수행 비중(%)
정보보안 관리 체계	5	13	100	100	100
정보보안 계획 및 활동	8	22	100	77	100
정보자산통제	7	16	100	94	100
인적보안	6	17	100	76	94
물리적 보안	10	25	72	72	72
접근 보안대책	17	43	98	86	98
운영관리	12	41	98	93	95
시스템 개발 및 유지보수	7	18	100	83	100
보안 시스템	9	26	100	85	100
합 계	81	221	96	85	95

상기 결과에서 볼 수 있는 것은 국내 기준과 국제 기준에서 요구하는 보안 평가 항목들을 통합하여 제시된 MLSA 평가 기준을 사용한 D조직, 국

제 기준을 적용한 T조직, 그리고 국내 기준을 적용한 K조직을 국내 기준과 국제 기준에 따라 평가하였을 때, MLSA를 사용한 D조직이 어느 하나의 기준을 이용한 조직들보다 전반적으로 좀 더 강건한 정보보호체계를 달성할 수 있었다는 것이다. 이는 보안 평가 항목 기준 상에서는 중점 사항이었으나, 국내 기준 평가 또는 국제 기준 평가에서는 실질적인 영향을 미치지 않는 항목이 있기 때문이었다. 이러한 부분은 보안 아키텍처가 잘못되었다는 사실이 아닌 관리적 측면의 개선 요소라고 볼 수 있다.

〈표 6〉 세 조직의 SA 국제 기준 평가 결과

ISO 27001					
대분류	항목수	세부기준수	MLSA 수행 비중 (%)	국제 기준 SA수행 비중(%)	국내 기준 SA수행 비중(%)
보안정책	2	11	100	100	91
보안조직	11	41	100	100	95
자산 분류 및 통제	5	9	100	100	89
인적보안	9	19	100	95	95
물리적, 환경적 보안	13	40	95	95	88
통신 및 운영 관리	32	207	88	88	86
접근통제	25	130	99	99	76
시스템 도입, 개발 및 유지 보수	16	128	99	99	97
보안사고 관리	5	23	100	100	91
사업연속성 계획	5	33	100	100	88
준거성	10	41	100	100	90
합 계	133	682	96	96	88

전술한 바와 같이, 국내 기준과 국제 기준은 평가 항목의 세부 기준이 다르기 때문에 관리적·물리적·기술적 보안 대책 상에서 요구되는 세세한 단계별 점검 사항에서 평가 점수의 하락 요인이 발생하고 있는 것이다. 따라서 2가지 이상의 보안 인증 체계를 동시적으로 요구 받고 있는 조직들은 본 연구에서 제시한 MLSA와 같은 방법론을 필요로 하게 된다.

그러므로 MLSA의 분석 결과는 정보보호정책의 수립 단계에서 요구되는 보안 정책 계획에 대한 일정이 국내 기준과 국제 기준을 함께 고려해야 하므로 조금 더 필요하게 되기는 하지만, 보안 아키텍처를 위한 관리적·물리적·기술적 정보보호 대책의 설계와 구현 면에서 국내의 정보보안관리수준 평가와 국제적으로 요구되는 ISO 27001의 동시적 달성이 가능하고, 보다 더 강건한 보안 아키텍처의 정보보호 수준을 확보할 수 있음을 보여주었다.

5. 결 론

본 연구에서는 MLSA를 제안하여 최근의 조직들이 보안 아키텍처를 구축 때 요구 받고 있는 2가지 이상의 서로 다른 보안 평가 기준의 동시적 충족을 위해서 수행해야 하는 정보보호정책 수립과 관리적·물리적·기술적 정보보호대책의 설계 및 구현에 관한 구체적인 방법론을 제시하고 이를 직접적으로 적용시켜 정보보호체계를 구축하고 결과적으로는 전체적인 정보보호 수준을 향상시키고자 하였다. MLSA는 다음과 같은 장점을 갖는다. 첫째, 타 인증 체계 또는 타 보안 아키텍처와의 호환성·상호운용성을 가지고 있어 복합적인 보안 아키텍처를 설계할 수 있었다. 둘째, 조직의 보안 아키텍처 구축 시 참고할 수 있도록 정보보호대책간의 연관성을 보여주었다.

향후에는 조직의 고유의 특성에 따른 보안 아키텍처에 대한 요구 사항 및 각각의 보안 평가 기준들에서 중요시하는 세부 평가 항목들을 고려하여, 이에 따른 실질적이고 효율적인 추진 전략들을 도출하여 이행할 수 있어야 할 것이다.

참 고 문 헌

[1] 국가사이버안전센터, 국가사이버안전매뉴얼,

2005.
[2] 민병길, 이도훈, 보안관리수준 평가 체계에 대한 분석 및 개선안 연구, 정보·보안 논문지, Vol. 6, No. 4, December, 2006.
[3] Robert Whitcher, ISO 17799 and SEC 27001 -how to use ISO 27001 (Governance, SoX) and how to implement, ISSA e-Symposium, 2007 Series.
[4] 박태완, ISO 27001 인증의 동향과 중요성, 인증포커스, 제6권, 봄호, 한국인정원.

최 경 호

2003년 경기대학교 경제학과 (경제학 학사)
2005년 경기대학교 경제학과 (경제학 석사)
2005년~현재 경기대학교 정보보호학과 박사과정

이 동 휘

2000년 경기대학교 전자계산학과 (이학사)
2003년 경기대학교 정보보호기술 공학과 (공학석사)
2006년 경기대학교 정보보호학과 박사

김 귀 남

미국 캔자스대학 수학과 (응용수학사)
미국 콜로라도주립대학 통계학과 (통계학석사)
미국 콜로라도주립대학 기계산업공학과 (기계·산업공학 박사)
현재 경기대학교 정보보호학과 주임교수