공 학 석 사 학 위 논 문

M-ISMS 모델 기반의 군(軍) 보안감사 설계에 관한 연구

2014년 2월

부 경 대 학 교 대 학 원

정보시스템 협동과정

김 대 규

공 학 석 사 학 위 논 문

M-ISMS 모델 기반의 군(軍) 보안감사 설계에 관한 연구

지도교수 김 창 수

이 논문을 공학석사 학위논문으로 제출함.

2014년 2월

부 경 대 학 교 대 학 원

정보시스템 협동과정

김 대 규

김대규의 공학석사 학위논문을 인준함.

2014년 2월 21일

주 심 이학박사 박 만 곤 (인)

위 원 공학박사 김 창 수 (인)

위 원 이학박사 이 경 현 (인)

<차 례>

<그림 차례>

<표 차례>

A Study on the Design of Military Security Audit based on the M-ISMS Model

Dae Gyu Kim

Interdisciplinary Program of Information System, The Graduate School,

Pukyong National University

Abstract

In recent, the levels of military information protection has been currently remained through very powerful legal systems such as Military Secret Protection Act and Military security operational defense minister instructions and regular and non-scheduled security inspection by considering the specialization of military.

However, the changes of information speed of military are required because of a relative lower level compared to the developing speed of the private_based ICT(Information Communication Technology). Therefore, the military also needs to adopt management systems of information security based on KISA ISMS(Korea Internet & Security Agency Information Security Management System) following Korean standards for Information Security.

We propose an improved M-ISMS(Military-ISMS) model for the characteristics of the military and management systems of information security based on the existing ISMS model. Our improved model focuses on 'internal security audit' and 'management of

external activity' by considering military characteristics that have not been conducted in ISMS.

Therefore, we added the six control items regarding confidentiality to internal security audits because the confidentiality is more important in militaries than fusibility which is importantly handled in private sectors.

We also recommend some control items regarding standards establishment and level maintain for security management in the external activity management parts because its value for secrecy is disappeared in case militaries reveal information or their external activities such as national defense white papers.

The proposed M-ISMS model in this thesis has an effect on preventing a rapid and future-oriented security intrusion incident in advance by considering a variety of its advantages and case studies of private intrusion incident collected from existing ISMS. However, specific guidelines and technologies of multiple control items in our proposed model will be studied in detail.

1.서 론

1.1 연구배경 및 필요성

우리나라는 1994년 인터넷 도입시기부터 현재까지 급속한 발전을 거듭하면서 인터넷 강국으로서 발돋움하였다. 2012년 발표자료 기준으로 ITU(국제전기통신연합, International Telecommunication Union)의 ICT(Information & Communication Technology) 발전지수 1위를 차지하고, 인터넷 이용자가 3,812만명(인터넷 이용률 78.4%)에 이르고 있다[1].

한편 이처럼 고도화되어가는 정보화 환경에 따른 역기능도 점차 확대되고 있으며, 특히 군과 같이 국가안전보장을 목적으로 하는 조직들의 주요 기밀 유출 가능성이 높아지고 있다.

창과 방패 관계처럼 대응하면 할수록 점점 더 교묘하게 발달하고 있는 정보보안 침해 수법은 국가 안보를 위협하는 커다란 위협으로 다가오고 있다.

국방부는 2010년 제정된 「국방정보화 기반조성 및 정보자원관리에 관한 법률」에 근거한 국방정보화 기본계획을 수립하여 목표지향적인 정보화를 추진하고 있다.

이에 따라 민간의 우수한 IT신기술을 군에 적기에 도입하기 위하여 2007년부터 IT신기술 시범사업을 추진하고 있다. 또한, 사이버 위협 대응 능력 강화를 위하여 2010년 국방부는 국군사이버사령부를 창설하여 군 내부의 기관별 정보보호 임무를 재정립하고 전군 차원의 사이버전 수행 대응센터를 구축·운영하고 있다[2].

이러한 노력과는 별개로 군의 특수성에 따라 보안감사에 대한 체계적 발전을 위한 논의와 제도적 변화는 더디게 움직이고 있다. 민간부문과 공공기관은 국제 표준 정보보호 관리체계(ISO/IEC 27001)을 바탕으로 만들어진 KISA(Korea Internet & Security Agency) ISMS(Information Security Management System)를 도입하여 고객과 대국민 신뢰도 향상을 위해 적극적으로 대응하고 있다.

이와 같은 시대적 요구에 따라 군에서도 형식적인 보안감사를 탈피하고 합리성과 체계성을 바탕으로 한 실질적인 보안감사가 이루어지기 위해서는 군 정보화 시스템에 대한 정보보호 관리실태를 평가 할 수 있는 정보보호 관리체계가 반드시 필요하다.

1.2 연구방법 및 구성

본 연구는 아래 3가지 방향으로 진행된다.

첫째, 국내외 ISMS(정보보호 관리체계) 및 관련 법률, 지침 등에 관하여 살펴보고,

둘째, 군(軍) 보안감사 및 보안규정의 문제점에 대한 선행 연구를 검토하고,

셋째, KISA ISMS와 관련된 법률 및 지침 등에서 군용 정보보호 관리체계(M-ISMS : Military Information Security Management System) 수립을 위한 요건을 도출하여 군(軍)보안감사에 적용 가능한 정보보호 관리체계 모델을 제안한다.

본 논문은 전체 5장으로 구성되어 있다.

2장에서는 국내 정보통신기반 보호법과 ISMS(정보보호 관리체계)에 대해 살펴보고, 3장에서는 군 특수성을 고려하여 ISMS 기반의 군(軍) 보안적용 문제점 분석과 IT기반의 ISMS와 보안규정에 대해 분석해 본다. 4장에서는 군 특수성을 고려한 군(軍) 정보보호 관리체계(M-ISMS)를 제안하고, 5장에서는 결론으로 구성한다.

2. 이론적 배경

2.1 국내 정보통신기반 보호법

정보통신기반 보호법[1]은 전자정부 서비스, VoIP[2] 및 IPTV 서비스, 인터넷 뱅킹, 스마트폰, 태블릿PC 등의 정보화가 진전되면서 방송·통신, 금융, 국방 등 주요사회기반시설의 정보통신 기술 및 서비스에 대한 의존도가 심화되고 있다. 국가 주요 기반시설의 인터넷 연결 확대로 언제 어디서나 인터넷을 통해 편리한 서비스를 제공받을 수 있는 반면 해킹·바이러스·스팸 등의 전자적 침해 행위로 국가의 중요한 정보들이 손쉽게 위협에 노출될 수 있기 때문에 체계적이고 안전한 범정부적 대응체계의 필요성이 강조되고 있다.

특히 최근 분쟁지역에서 적국을 공격하기 위한 수단으로 사이버공간이 공공연히 활용되고 있으며 플레임[3], 스턱스넷[4] 등의 악성코드 출현으로 국가의 주요기반시설을 공격하는 사이버전이 현실화되고 있다. 또한 미국의 상수도 시설 시스템이 해킹 공격을 받아 공공 안전에 위협이 되는 상황이 발생하는 등 국가·사회적으로 중요한 제어시설에 대한 해킹 시도가 빈번해지고 있다.

이에 대한 국가 차원의 대책으로 정부는 2001년 기반시설 중 국

---

1) 법률 제11690호, 2013.3.23, 타법개정. 이 법은 전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립/시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장하는 것을 목적으로 한다.

2) Voice over Internet Protocol, 인터넷 전화 또는 음성 패킷망. 초고속인터네소가 같이 IP망을 기반으로 패킷 데이터를 통해 음성통화를 구현하는 통신기술이다.

3) Flame. 전자메일이나 게시판의 글들 또는 동호회 안에서 맹렬히 논쟁을 하고 서로를 비난할 때 그 참여자들이 서로를 플레임한다고 말한다. 플레이밍은 개인에 대한 맹렬한 인신 공격이다.

4) Stuxnet. 발전소·공항·철도 등 기간시설을 파괴할 목적으로 제작된 컴퓨터바이러스로, 2010년 6월 벨라루스에서 처음으로 발견되었다.

가적으로 중요한 시설을 보호하기 위하여 「정보통신기반 보호법」을 제정하였다. 동 법의 주요 내용은 국가 사회적으로 중요한 정보통신기반시설을 주요정보통신기반시설로 지정하여 중점 관리하고, 지정된 주요정보통신기반시설에 대하여 관리기관이 취약점 분석」평가를 수행하여 취약점에 대한 단기적 및 중·장기적인 보호조치와 시행 사항을 포함하고 있다. 동 법은 전자적 침해행위 수법의 급속한 발전에 대응하여 꾸준히 개정이 이루어졌다.

이를 위해 「정보통신기반 보호법」에서는 [그림 1]와 같이 주요정보통신기반시설의 안정적인 관리 및 운영이 이루어지도록 정보통신기반보호위원회를 운영하여 정보통신기반 보호정책 수립과 시행을 총괄·조정함으로써 관계 중앙행정기관간 침해사고 예방 및 대응 업무가 상호 협력 및 보완될 수 있도록 하고 있다. 주요 임무로는 주요정보통신기반시설 보호정책의 조정, 주요정보통신기반시설 보호계획의 종합·조정 및 추진 실적, 주요정보통신기반시설 보호와 관련된 제도의 개선 및 기반시설의 신규지정·변경과 같은 주요 정책사항 심의 등이다[1].

(출처 : 한국인터넷진흥원)

[그림 1] 주요정보통신 기반시설 보호체계

2.2 국내외 정보보호관리 인증제도

2.2.1 ISMS(정보보호 관리체계)

정보보호(Information Security)란, "정보의 수집·가공·저장·검색·송신·수신 중에서 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적·기술적 수단, 또는 그러한 수단으로 이루어지는 행위"를 말한다.[3]

정보보호의 주요 목표는 전통적으로 다음 3가지로 정리된다.

- 비밀성(Confidentiality) : 접근을 허가 받은 사람만이 접근할 수 있는 속성.
- 무결성(Integrity) : 내용 수정의 권한이 없는 사람이 변경을 못하게 하는 속성.
- 가용성(Availability) : 접근권한 및 사용권한 있는 사람이 요구할 경우 적절한 시간 내에 정보나 서비스를 제공하는 속성.

또한 정보전의 분야에서는 "우연히 혹은 의도적으로 허가 받지 않는 정보의 누출, 전송, 수정, 파괴 등으로부터의 보호"로 정의하고 있으며, 국제표준인 ISO/IEC27001[5]에서는 정보보호의 사업 지원 측면을 강조하여 "사업의 지속성을 보장하고 사업 위험을 최소화 하고 투자회수와 사업기회를 최대화하기 위하여 다양한 위협으로부터 정보를

5) 국제표준화기구(ISO : International Oranization for Standardization) 및 국제전기기술위원회(IEC : International Electrotechnical Commission)에서 제정한 정보보호 관리체계 에 대한 국제 표준이자 정보보호 분야에서 가장 권위 있는 국제 인증

보호하는 것"으로 정의 하고 있다.

이러한 정보보호의 목표를 달성하고 모든 위협으로부터 안전하고 효율적으로 관리할 수 있는 정보보호 관리체계를 수립하는 것이 중요하다[4].

여기서 정보보호 관리체계란 정보자산의 비밀성, 무결성, 가용성을 달성하기 위하여, 각종 보안 대책을 관리하고, 위험기반 접근방법에 기초하여 구축·구현·운영·모니터링·검토·개선 등의 주기를 거쳐 정보보호를 관리하고 운영하는 체계를 말한다[5].

2.2.2 BS7799

가. 개 요

BS7799(British Standard 7799)는 영국 BSI[6]에서 정보보호 관리를 위한 표준화된 실무규약으로 1995년 처음 개발되었다. 정보보호 관리를 위한 포괄적인 일련의 관리방법에 대해 섹션별로 해석해놓은 산업체를 위한 규격으로 1998년에는 이 기준에 따른 인증 요건을 개발하여 본래의 표준인 실무 규약은 Part1, 인증요건은 Part2로 만들어졌다. 1999년 10월에는 ISO 표준으로 제안되어 ISO/IEC 17799-1이 되었다. 현재 영국이외에 호주, 브라질, 네덜란드, 뉴질랜드, 노르웨이 등에서 사용되고 있다.

나. 인증 기준 및 절차

6) British Standard Institute, 영국표준협회. 영국 국가규격(BS), 유럽규격(EN) 및 국제규격(ISO) 제정과 제품 시험 및 인증 업무를 수행한다.

BS7799는 2개의 파트로 구성되어 있다. Part 1은 정보보안 관리에 대한 표준적인 실무지침으로 10개의 주요 부문으로 구성되어 있다. 세부지침으로 36개의 통제 목적과 127개의 전체 통제항목을 통한 보호지침을 제공하고 있다 [9].

Part 2는 조직 전체 비즈니스 위험 관리를 위한 관점으로 정보보안관리시스템 문서화 수립실행에 대한 요구사항을 규정하고 있다. 정보보호 관리체계 구축을 위해서는 다음 <표 1>과 같은 6단계의 관리 프레임을 구축해야 한다.

<표 1> BS7799 관리 프레임

프레임 단계	내 용
1단계	정보보호 정책을 정의한다.
2단계	정보보호 관리체계의 범위를 정의한다. 경계는 조직 특성, 위치, 자산 및 기술 등의 용어로서 정의한다.
3단계	적절한 위험성 평가를 실시한다. 위험성 평가는 자산에 대한 위협, 취약점 및 조직에 대한 영향을 식별하고 위험수준을 결정한다.
4단계	관리해야 하는 위험영역은 조직의 정보보호 정책과 요구되는 보증 수준을 토대로 식별해야 한다.
5단계	적절한 통제 목표, 방안을 선정하고 그 선정을 정당화해야 한다.
6단계	보고서를 작성한다.

다. 구축 및 운영사례

BS7799 인증 성공사례로는 영국의 The Co-operative Bank가

있으며, 인터넷 뱅킹부분을 ISMS의 범위로 하여 BS7799 Part2에 의한 인증을 획득하였다. The Co-operative Bank의 인터넷 뱅킹 서비스 'Smile'은 1999년 6월에 BS7799 인증 준비 작업을 시작하여 정보보호 정책 수립, ISMS범위의 설정, 위험평가 등 ISMS 프레임워크 구축과정을 거쳤다. 그리고 BSI를 인증심사 기관으로 선택하였고 BSI의 엄격한 심사절차를 거친 후 2000년 1월에 인증획득에 성공하였다. Smile의 BS7799인증은 단순히 인증획득에 만족하지 않고 이를 적극적으로 마케팅에 도입하여 성공한 사례로 손꼽힌다[7].

2.2.3 ISO/IEC 27001

가. 개 요

국제 표준화 기구 ISO[7]와 IEC[8]는 연합위원회를 구성하여 2005년에 ISMS에 대한 국제 표준인 ISO/IEC 27001과 ISO/IEC 27002를 발표하였다. 이 표준은 원래 BS7799에서 발전한 것으로, 모범사례는 BS7799 Part1, 인증 기준은 BS7799 Part 2로 나뉘어졌으며, BS 7799 Part 1이 ISO/IEC 17799로 먼저 국제 표준이 되었고, BS 7799 Part 2가 뒤이어 국제 표준이 되었다. 개정 작업을 통하여 2005년에는 ISO/IEC 27001과 모범사례의 집합인 ISO/IEC 27002로 바뀌었다.

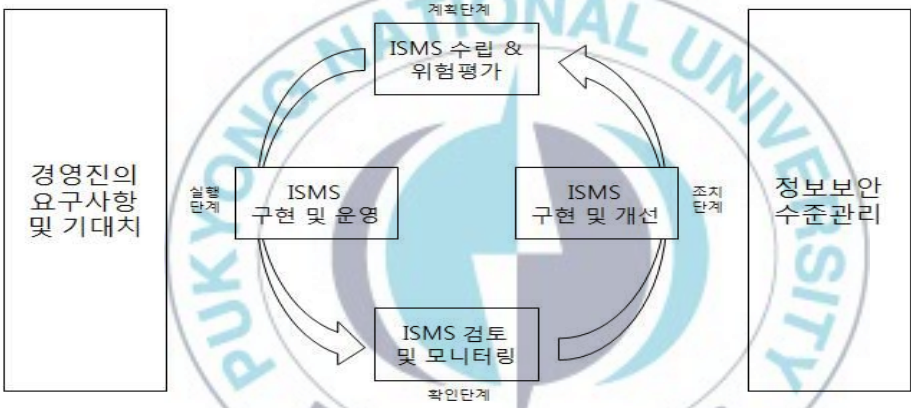
ISO/IEC 27001에 의하면, 정보보호 관리체계를 "전반적인 경영시스템의 일부로, 비즈니스 위험 접근법을 기반으로 하는 정보보호를 수

7) International Organization for Standardization, 국제표준화기구. 지적 활동이나 과학·기술·경제활동 분야에서 세계 상호간의 협력을 위해 1946년 설립한 국제기구.
8) International Electrotechnical Commission, 국제전기표준회의. 각국의 전기기술에 관한 표준에 있어서 각국 간의 조정과 통일을 도모할 목적으로 창설된 국제기관.

립, 구현, 운영, 모니터, 검토, 유지 및 개선하기 위한 시스템"으로 정의하고 있으며, 이러한 관리 시스템은 정보보호 조직 구조, 정책, 계획 활동, 책임, 실무 절차, 프로세스 및 자원을 포함하고 정보보호 활동에 대한 지속적이고 체계적인 경영관리 일부임을 명시하고 있다[8].

나. 인증 기준 및 절차

ISO/IEC 27001은 효과적인 정보보호 활동을 위해 [그림 2]과 같이 PDCA 사이클[9]을 따르고 있다. 이의 목적은 보호해야할 자산을 식별하고, 이를 누가 어떤 형태로 어디에 보관, 사용하고 있는지를 파악하고, 그 자산에 어떠한 위협과 취약성이 존재하며, 그 가능성은 얼마나 높으냐를 바탕으로 적절한 보안 대책들을 구현하는 것이다.



[그림 2] ISO/IEC 27001 관리 프로세스

계획단계는 보안정책, 프로세스, 위험 등을 관리하여 조직의 정책과 목적에 부합하는 결과를 가져오도록 정보보안 관리체계를 수립하며, 실행단계는 수립된 정보보안 관리체계를 실행한다. 확인단계는 실

9) 계획(Plan)단계, 실행(Do)단계, 확인(Check)단계, 조치(Action)단계

행 및 운영되고 있는 정보보안 관리체계에 대해 평가와 측정을 통해 모니터링하며, 조치단계는 정보보안 관리체계의 정보보안 관리 수행 결과들을 기반으로 지속적인 향상을 위한 활동들을 수행한다.

이와 같은 프로세스 안에서 필요한 관리적 · 물리적 · 기술적 정보보호 활동이 적절히 조화를 이루어 운영될 때 효율적인 정보보안 관리체계를 구축할 수 있을 것이다[9].

ISO/IEC 27001은 BS7799 Part 2가 2005년 국제표준으로 채택되었으며, 급증하는 사이버 공격에 대해 보다 효과적으로 대응하기 위해 2013년 9월 25일부로 일부 개정되었다. 개정된 ISO/IEC 27001의 보안통제항목은 다음 <표 2>와 같이 14개 통제 분야, 35개 통제 목적, 114개 통제항목으로 구성되어 있다[10][11].

<표 2> ISO/IEC 27001:2013 보안통제항목

보안통제항목		주요내용
통제분야	통제 항목	
1. 정보보안정책	2	정보보호에 대한 경영방침과 지원 사항을 제공하기 위함
2. 정보보안조직	7	조치 내에서 보안을 관리하는데 활용
3. 자산관리	10	조직의 자산을 파악하고 이에 대한 적절한 보호책 유지
4. 인적자원보안	6	사람에 의한 실수, 절도, 부정 수단이나 설비의 잘못 사용으로 인한 위험을 감소
5. 물리적·환경적 보안	15	사업장의 비인가된 접근 및 방해요인을 방지
6. 통신 보안	7	데이터 송수신 간에 보안대책을 수립 및 운용
7. 접근통제	14	정보에 대한 접근 통제를 하기 위함
8. 정보시스템 획득, 개발, 유지보수	13	정보시스템 내에 보안이 수립되었음을 보장하기 위함
9. 보안사고 관리	7	보안 사고에 대한 대응 절차의 수립 및 이행을 보장
10. 업무 연속성 관리	4	사업 활동에 방해요소를 완화시키며 중대한 실패 및 재난으로부터 주요 사업 활동을 보호하기 위함
11. 준거성	8	범죄 및 민사상의 법률, 법규, 규정 또는 계약 의무사항 및 보안요구사항의 불일치를 회피하기 위함
12. 공급자 관계	5	공급자에 대한 적절한 보호책 유지
13. 암호 통제	2	인증 및 암호에 대한 대책 수립 및 유지
14. 운영 보안	14	정보처리 설비의 정확하고 안전한 운영을 보장하기 위함
14개	114개	

다. 구축 및 운영사례

ISO survey에 의하면 <표 3>와 같이 ISO/IEC 27001 인증 현황(2012년 12월 기준)은 총 132개국, 19,577개이다[6].

<표 3> ISO/IEC 27001 인증 현황(조직별)

(단위 : 건)

구 분	2010	2011	2012
Total	15,626	17,355	19,577
Africa	46	40	64
Central/South America	117	150	203
North America	329	435	552
Europe	4,800	5,289	6,384
East Asia and Pacific	8,788	9,665	10,373
Central and South Asia	1,328	1,497	1,657
Middle East	218	279	344

(출처 : http://www.iso.org)

ISO/IEC 27001은 세계적으로 널리 알려진 정보보안관리 분야의 국제 표준이며, 오래전부터 지속적으로 개선되고 발전되어온 조직의 정보보호 업무에 관한 지침이다. 따라서 정보보안 관리체계를 구축하고자 하는 기업은 시행착오 단계를 회피하고 효율적인 정보보호 활동의 추진 및 정보보호 분야에서 대외적인 인지도를 확보하려면 ISO/IEC 27001과 같은 표준을 도입하여 사용하는 것이 효과적인 정보보호 접근 방법이 될 것이다[9].

2.2.4 KISA ISMS

가. 개 요

KISA ISMS는 정보보호의 목적인 정보자산의 비밀성, 무결성, 가용성을 실현하기 위한 절차와 과정을 체계적으로 수립 및 문서화 하고 지속적으로 관리 및 운영하는 시스템이다. 즉, 조직에 적합한 정보보호를 위해 정책 및 조직 수립, 위험관리, 대책구현, 사후관리 등의 정보보호 관리과정을 통해 구현된 여러 정보보호대책들이 유기적으로 통합된 체계에 대하여 제3자의 인증기관(KISA)이 객관적이고 독립적으로 평가하여 기준에 대한 적합 여부를 보증해주는 제도이다.

우리나라는 세계 최고 수준의 정보통신 인프라를 기반으로 사회·경제 전반에 걸쳐 인터넷의 이용 및 새로운 융합서비스가 급속히 활성되기 시작함과 더불어 2009년 7.7 DDoS공격, 2012년 통신사 개인정보 대규모 유출사고 등 고도화된 사이버 침해사고 또한 급증하게 되었다. 급변하는 IT서비스 및 사이버 침해 환경에 능동적으로 대처하기에는 현행 정보보호 법제에 한계가 있음을 인지한 정부는 신규 융합서비스 이용환경에 맞는 실질적 정보보호체계 확립 등을 위하여 법 체계를 정비하였다(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」일부개정, 2012.2.17 공포). 또한 기업의 보다 실질적인 정보보호 활동을 유도하고 해킹 등 사이버위협에 대한 사전예방 조치를 강화할 수 있도록 하는 등 정보보호 관련 제도들을 신설·보완하였다.

방송통신위원회는 통신사, 포털, 쇼핑몰 등 주요정보통신서비스 제공자를 인증 의무대상자로 지정하고 인증기준 등을 재정비 하기위해 정보보호 관리체계 인증 등에 관한 고시(2013.1.17 공포) 하였다[1].

나. 인증 기준 및 절차

KISA ISMS 인증 기준은 <표 4>와 같이 정보보호 관리과정(5단계, 12개 통제항목)과 정보보호대책(13개 분야, 92개 통제항목)의 두 가지로 구성되어 있다[1].

<표 4> KISA ISMS 정보보호 관리체계 인증 기준표

분야		통제항목	세부점검항목
관리과정 (구축단계)	1. 정보보호정책수립 및 범위설정	2	5
	2. 경영진 책임 및 조직구성	2	5
	3. 위험관리	3	11
	4. 정보보호대책 구현	2	3
	5. 사후관리	3	8
정보보호 대책	1. 정보보호정책	6	12
	2. 정보보호조직	4	9
	3. 외부자 보안	3	6
	4. 정보자산분류	3	9
	5. 정보보호교육	4	10
	6. 인적보안	5	14
	7. 물리적 보안	9	20
	8. 시스템 개발보안	10	32
	9. 암호통제	2	5
	10. 접근통제	14	19
	11. 운영보안	22	67
	12. 침해사고 관리	7	19
	13. IT재해복구	3	7
총 계		104	261

정보보호 관리과정은 정보보호 관리체계 인증 심사시 요구되는 필수 항목으로서 5단계, 12개 통제항목으로 구성되어 있으며 [그림 3]과 같이 조직 내·외부 위협 요소의 변화 또는 새로운 취약성 발견 등에 대응하기 위하여 지속적으로 유지 관리되는 순환주기의 형태를 가

진다.

[그림 3] KISA ISMS 정보보호 관리과정 5단계

<표 5> KISA ISMS 정보보호 관리과정 5단계

관리과정	세부관리과정
1. 정보보호 정책수립 및 범위 설정	5
2. 경영진 책임 및 조직 구성	5
3. 위험관리	11
4. 정보보호대책 구현	3
5. 사후관리	8
총 계	32

정보보호대책은 정보보호 관리체계 인증 심사시 요구되는 선택 항

목으로서 <표 6>과 같이 총 13개 분야 92개 통제항목으로 구성되어 있으며, 위험평가를 통하여 조직이 수용한 위험수준을 달성할 수 있도록 통제항목을 선택한다.

<표 6> KISA ISMS 통제항목

No	통제분야	통제항목		항목수
1	정보보호 정책	1.1	정책의 승인 및 공표	6
		1.1.1	정책의 승인	
		1.1.2	정책의 공표	
		1.2	정책의 체계	
		1.2.1	상위 정책과의 연계성	
		1.2.2	정책시행 문서수립	
		1.3	정책의 유지관리	
		1.3.1	정책의 검토	
		1.3.2	정책문서 관리	
2	정보보호 조직	2.1	조직 체계	4
		2.1.1	정보보호 최고 책임자 지정	
		2.1.2	실무조직 구성	
		2.1.3	정보보호 위원회	
		2.2	역할 및 책임	
		2.2.1	역할 및 책임	
3	외부자 보안	3.1 보안 요구사항 정의		3
		3.1.1	외부자 계약시 보안요구사항	
		3.2 외부자 보안 이행		
		3.2.1	외부자 보안 이행 관리	
		3.2.2	외부자 계약 만료 시 보안	
4	정보자산 분류	4.1 정보자산 식별 및 책임		3
		4.1.1	정보자산 식별	
		4.1.2	정보자산별 책임할당	
		4.2 정보자산의 분류 및 취급		
		4.2.1	보안등급과 취급	
5	정보보호 교육	5.1 교육 프로그램 수립		4
		5.1.1	교육 계획	
		5.1.2	교육 대상	
		5.1.3	교육내용 및 방법	
		5.2 교육 시행 및 평가		
		5.2.1	교육 시행 및 평가	

No	통제분야	통제항목		항목수
6	인적 보안	6.1 정보보호 책임		5
		6.1.1	주요 직무자 지정 및 감독	
		6.1.2	직무 분리	
		6.1.3	비밀유지서약서	
		6.2 인사규정		
		6.2.1	퇴직 및 직무변경 관리	
		6.2.2	상벌규정	
7	물리적 보안	7.1 물리적 보호구역		9
		7.1.1	보호구역지정	
		7.1.2	보호설비	
		7.1.3	보호구역 내 작업	
		7.1.4	출입통제	
		7.1.5	모바일 기기 반출입	
		7.2 시스템 보호		
		7.2.1	케이블 보안	
		7.2.2	시스템 배치 및 관리	
		7.3 사무실 보안		
		7.3.1	개인업무 환경 보안	
		7.3.2	공용업무 환경 보안	
8	시스템 개발보안	8.1 분석 및 설계 보안관리		10
		8.1.1	보안 요구사항 정의	
		8.1.2	인증 및 암호화 기능	
		8.1.3	보안로그 기능	
		8.1.4	접근권한 기능	
		8.2 구현 및 이관 보안		
		8.2.1	구현 및 시험	
		8.2.2	개발과 운영환경 분리	
		8.2.3	운영환경 이관	
		8.2.4	시험데이터 보안	
		8.2.5	소스 프로그램 보안	
		8.3 외주개발보안		
		8.3.1	외주개발보안	
9	암호통제	9.1 암호 정책		2
		9.1.1	암호 정책 수립	
		9.2 암호키 관리		
		9.2.1	암호키 생성 및 이용	

통제항목		통제항목		항목수
10	접근통제	10.1 접근통제 정책		14
		10.1.1	접근통제 정책 수립	
		10.2 접근권한 관리		
		10.2.1	사용자 등록 및 권한부여	
		10.2.2	관리자 및 특수 권한 관리	
		10.2.3	접근권한 검토	
		10.3 사용자 인증 및 식별		
		10.3.1	사용자 인증	
		10.3.2	사용자 식별	
		10.3.3	사용자 패스워드 관리	
		10.3.4	이용자 패스워드 관리	
		10.4 접근통제 영역		
		10.4.1	네트워크 접근	
		10.4.2	서버 접근	
		10.4.3	응용 프로그램 접근	
		10.4.4	데이터베이스 접근	
		10.4.5	모바일 기기 접근	
		10.4.6	인터넷 접속	
11	운영보안	11.1 운영절차 및 변경관리		22
		11.1.1	운영절차 수립	
		11.1.2	변경관리	
		11.2 시스템 및 서비스 운영보안		
		11.2.1	정보시스템 인수	
		11.2.2	보안시스템 운영	
		11.2.3	성능 및 용량 관리	
		11.2.4	장애관리	
		11.2.5	원격운영관리	
		11.2.6	스마트워크 보안	
		11.2.7	무선네트워크 보안	
		11.2.8	공개서버 보안	
		11.2.9	백업관리	
		11.2.10	취약점 점검	
		11.3 전자거래 및 정보전송 보안		
		11.3.1	전자거래 보안	
		11.3.2	정보전송 정책 수립 및 협약 체결	
		11.4 매체 보안		
		11.4.1	정보시스템 저장매체 관리	
		11.4.2	휴대용 저장매체 관리	
		11.5 악성코드 관리		
		11.5.1	악성코드 통제	
		11.5.2	패치관리	

통제항목		통제항목		항목수
11	운영보안	11.6 로그관리 및 모니터링		
		11.6.1	시각동기화	
		11.6.2	로그기록 및 보존	
		11.6.3	접근 및 사용 모니터링	
		11.6.4	침해시도 모니터링	
12	침해사고 관리	12.1 절차 및 체계		7
		12.1.1	침해사고대응 절차 수립	
		12.1.2	침해사고 대응체계 구축	
		12.2 대응 및 복구		
		12.2.1	침해사고 훈련	
		12.2.2	침해사고 보고	
		12.2.3	침해사고 처리 및 복구	
		12.3 사후관리		
		12.3.1	침해사고 분석 및 공유	
		12.3.2	재발방지	
13	IT 재해복구	13.1 체계 구축		3
		13.1.1	IT 재해복구 체계 구축	
		13.2 대책 구현		
		13.2.1	영향분석에 따른 복구대책 수립	
		13.2.2	시험 및 유지관리	

KISA ISMS 인증절차는 준비단계, 심사단계, 인증단계, 사후심사 단계로 나누어진다. 인증 소요기간은 내부 준비부터 인증까지 약 6개월 이상이 소요된다. 또한 인증 신청을 위해서는 ISMS 구축 후 최소 2개월 이상 운영을 해야 한다.

단계별 소요시간은 <표 7>과 같이 7~9개월이 소요된다[1].

<표 7> KISA 인증 단계별 소요시간

인증절차내용		소요기간
1. 준비	ISMS 구축	1~3개월
	ISMS 운영	2개월(최소)
	인증신청	5일
2. 심사	심사 준비	30일
	인증심사	5일
	보완조치	30일
	조치확인	5일
	심사 결과보고서 작성	5일
3. 인증	인증위원회 심의 준비	30일
	인증위원회 심의 및 인증서 교부	2일

다. 구축 및 운영사례

KISA ISMS 인증 발급현황은 한국인터넷진흥원 내부 자료에 의하면 다음 <표 8>에서 나타난 바와 같이 총 170개 기관에서 발급받아 운영하고 있다(2013년 10월 31일 기준)[13].

<표 8> KISA ISMS 인증 발급 현황

(단위 : 건)

발급연도	발급현황
총 계	170
2013	19
2012	25
2011	27
2010	22
2009	19
2008	12
2007	8
2006	4
2005	9
2004	18
2003	6
2002	1

(출처 : 한국인터넷진흥원)

KISA ISMS 인증 구축 및 운영사례로는 포털 등 인터넷 서비스 분야 중에 '(주)다음커뮤니케이션[10]' 을 KISA ISMS를 활용한 개인

10) 다음커뮤니케이션(www.daum.net)은 1995년 2월에 설립되었으며, 3,800만 이용자를 확보하고 있는 대한민국의 대표적인 인터넷 포털사이트이다.

정보보호 대응 모범사례로 들 수 있다.

인증범위는 Daum 인터넷 서비스 인프라 운영으로서 2006년 2월에 인증을 취득하였으며, 인터넷 업체 최초로 정보보호 관리체계 인증을 획득하였다.

개인정보를 취급하는 기업에서 내/외부적 환경 변화를 가장 적절하게 대응하기 위해서는 보안장비나 솔루션을 통한 단편적 접근 방식으로는 한계가 있음을 알고 있기에 정보보호 관리체계를 수립하여 운영하고 있다.

개인정보를 취급하는 기업에서 가장 큰 정보보호 이슈는 정통망법[11], 개인정보보호 기술적 · 관리적 보호조치 고시(방송통신위원회 고시 제2009-21호, 2009.8.7)에 대한 대응이라고 해도 과언이 아니다.

각 고시 조항별로 KISA ISMS 통제항목을 통해 대응할 수 있으며, 지속적으로 운영함으로써 서비스 인프라에 대한 취약성과 보완점을 도축하여 보안을 강화할 수 있다. 또한, 전 임직원의 보안에 대한 인식을 내재화 할 수 있도록 지속적으로 교육하고, 개선하는 일련의 사이클을 거치면서 대/내외적인 리스크는 점차 감소하고 이를 통해 회사는 수익극대화에 집중할 수 있는 토대를 만들어 갈 수 있다[14].

11) 정보통신망 이용촉진 및 정보보호 등에 관한 법률(법률 제11690호, 2013.3.23, 타법개정). 이 법의 목적은 정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향사와 공공복리의 증진에 이바지하는 것이다. 간단히 정보통신망법, 정통망법, 망법 등으로 줄여 부르기도 한다.

3. 군 특수성을 고려한 ISMS 분석

3.1 ISMS 기반의 군(軍)보안적용 문제점 분석

3.1.1 군(軍)보안감사의 현실적인 문제

국가안보를 보장하는 군 특수성을 바탕으로 군에서는 보안감사를 위한 별도의 감사팀을 운영하고 있으며 보안감사업무의 전문화가 이루어지고 있다. 군 보안감사는 정기 감사(연 1회)와 불시 보안감사로 구분되고, 사단급 이상부대를 대상으로 기무사령부(격년 1회)와 각 군에서 보안감사(연 1회)를 실시하고 있다.

보안감사는 보안수준이 낮은 부대를 적정한 수준으로 향상시키고, 높은 부대는 계속해서 유지할 수 있도록 지도해야 한다. 하지만 국방부 2012년 보안회보에 따르면, 2012년 후반기 보안감사 결과는 대부분 부대가 '우수' 또는 '보통'의 평가를 받았고 '저조'는 없었다(총 33개 부대 중에 '우수' 28개 부대, '보통' 9개 부대)[15].

이렇게 모든 부대가 후한 평가 받은 원인을 비롯하여 군 보안감사의 문제점을 분석해보았다.

첫째, 아직까지도 정보보안 업무는 보안담당자만 처리하는 일이라는 인식이 쉽게 바뀌지 않고 있다. 그래서 보안사고가 발생하여도 적절한 대응절차와 대응방법을 숙지하지 못해 대응속도가 느리다. 이는 보안 교육이 부족하다기 보다 관심도가 낮아서 발생하는 현상이다.

둘째, 객관적이고 효율적인 보안감사 자료 수집을 하지 못하고 있다. 피감사 부대에서 제출받은 감사 자료를 기초로 일반적으로 3~5일 동안 4~5명으로 편성된 감사관이 문서보안, 인원보안, 정보통신보안, 시설보안 등 정보보안 모든 분야를 감사하기에는 시간적 여유가 부족하다. 특히, 타 조직에 비해 문서보안과 시설보안 비중이 높으므로 물리적인 시간이 많이 소요되며, 보안 위반 사례를 발견했다고 하더라도 감사증적 확보가 신속히 이루어지기 어렵다.

셋째, 감사 주기가 길기 때문에 보안감사 목표 수준을 높게 유지하기가 어렵다. 게다가 감사관 재량범위가 넓어 자체 경감처리에 의한 온정주의 처분도 있어 감사 결과가 질적으로 하락할 가능성도 높다.

넷째, 군 특수성에 따른 폐쇄적인 보안감사 활동 구조가 보안감사 발전을 저해하고 있다. 군 단독적으로 끊임없이 도입되는 각종 신규 정보시스템에 대한 취약점 분석과 침해대응 대책 수립하기에는 국방정보화 속도가 더 빠르기 때문에 구조적인 개선대책이 필요하다.

다섯째, 지난 천안함 피격사건과 연평도 포격사건 등 주요 군사 작전 시 정보통제가 적절하게 이루어지지 않았던 점에서 대군 신뢰도를 크게 하락되었었다. 언론의 자유와 국민의 알 권리도 중요하지만 국가 존속여부를 결정하는 국가기밀에 대한 보도는 적절하게 통제되어야 한다. 따라서 군사기밀 보호를 위한 군 대외 활동에 대한 체계적인 관리가 필요하다.

3.2 IT기반의 ISMS와 보안규정

3.2.1 거버넌스 개념의 ISMS 검토

최근 IT 융·복합 환경의 급속한 변화로 인해 개인정보 및 기업정보 등 정보자산에 대한 위협 및 취약성을 어느 때보다 매우 심각하게 인식하게 되었으며, 이에 대한 적절한 위험관리 활동이 필요하게 되었다. 이를 위해 조직에서 정보자산을 보호하고 조직경쟁력을 강화하기 위한 수단으로 정보보호 관리체계 개선활동의 하나로 강화된 정보보호 관리체계 구축 및 운용에 대한 연구들이 진행되고 있다[16].

이러한 배경과 더불어 국가경영 또는 공공경영의 개념으로 IT 거버넌스(governance)라는 용어가 생겨났고, IT의 도움과 효율적인 활용을 전제로 하지 않으면 국가나 군 그리고 공공기업의 전략적 목표 달성이 어려운 상황에 도달할 수 있다. 군의 관계에서 보면 IT 거버넌스의 구조와 원리는 지휘부와 보안담당자들이 조직의 보안 목적 달성을 위해 상호 연관된 구조와 프로세스들이 융합되어야 한다. 이러한 구조와 논리는 [그림 4]에서처럼 지휘와 통제, 책임감, 책임 추적성의 요소가 서로 균형을 이루는 관리체계가 필요하다. 군 경영의 관점에서 IT 거버넌스는 각 주체가 상호 균형을 이루면서 자신의 분야에 책임감을 가질 수 있는 관리체계를 구축하는 과정이 필요할 것이다.

[그림 4] IT 거버넌스의 구조와 원리

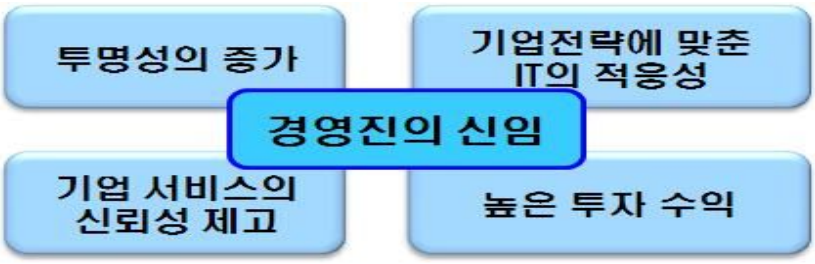
이러한 IT 거버넌스의 구조와 원리의 내용을 <표 9>에 정리하였다.

<표 9> IT 거버넌스의 구조와 원리

IT 거버넌스의 구조와 원리	내용
지휘와 통제	·고위 경영진은 조직의 목적을 수립하고 IT 수행활동을 위임함으로써 지휘와 통제를 한다. ·고위경영진은 방향 설정과 지휘와 통제를 위한 조직이나 기업의 문화를 조성한다.
책임감	·경영진은 내부통제에 대해 궁극적인 책임을 갖는다. ·IT 관리자는 내부통제의 정책과 절차를 수립하고 이를 위한 권한부여의 책임을 갖는다. 내부통제라 함은 기업이나 조직 내에서 수립해 놓은 절차 등을 미리 사전적인 의미에서 제어하는 장치를 말하며, 기업과 조직에서 상시 진행되는 일련의 장치이다.
책임추적성	·책임추적성은 책임과 권한을 가지고 구체적으로 내용을 수행하는 것을 의미한다. ·이사진은 IT를 감독하며 거버넌스를 제공한다. ·책임 추적성은 투명성을 기준으로 한다.

군의 관점에서 IT 거버넌스의 구조와 원리는 지휘와 통제, 책임감, 책임 추적성 중 가장 중요시 되는 내용은 책임 추적성이다. 책임감과 책임 추적성을 분리시킨 이유는 담당자가 책임져야 할 내용에 대해 책임감을 강조한 것이며, 책임 추적성은 그 내용을 구체적으로 실천하는 실천 강령을 강조한 것으로 볼 수 있다.

[그림 5]은 국가경영 혹은 기업경영 관점에서 경영진의 신임, 기업전략에 맞춘 IT의 적응성, 높은 투자수익률, 기업 서비스의 신뢰성 제고, 투명성의 증가와 관련하여 상호연관성을 나타낸 것이다[17].



[그림 5] IT 거버넌스의 효과

<표 10> IT 거버넌스의 효과의 내용

IT 거버넌스의 효과	내용
경영진의 신임	·경영진의 IT에 대한 이해도가 증가한다. ·IT 부서의 경영 언어 사용으로 타 부서와의 의사소통이 원활하게 된다.
기업전략에 맞춘 IT의 적응성	·기업의 전략과 요구사항이 IT에 의해 신속하고 유연성 있는 대처를 한다.
높은 투자수익률	·프로젝트의 실패, 비효율적인 IT 설비투자 및 기준에 의한 업무 프로세스로 인해 발생하는 비용을 줄인다. ·고객만족과 직결되는 핵심기능을 IT의 성과로 지원하므로 기업의 투자 유치가 높아진다.
기업서비스의 신뢰성 제고	·IT의 기업 핵심프로세스에 대한 지원 향상으로 기업의 위상이 제고된다. ·핵심 프로세스를 지원하는 IT 프로세스는 항상 성과가 감시되고 측정되어짐으로 인해서 신뢰성이 제고된다.
투명성의 증가	·프로젝트 혹은 IT 서비스 비용에 대해 정확하고 신뢰할만한 정보를 경영진에게 제공한다. ·경영진은 이해관계자에게 투명성 있는 자료를 제공한다. ·투명성 있는 정보로 의사결정자의 의사결정에 기여한다.

조직의 비즈니스 연속성 확보뿐만 아니라 2009년 7.7 DDoS 공격[12]과 같이 매우 지능화되고 있는 침해사고에 효율적으로 대응하기 위해서는 제품중심의 기술적 대응에 한계가 있다는 것을 국가나 조직의 정보보호 담당자 모두가 이를 인식하고 정보보호 관리체계 구축에 관심이 고조되고 있다. 또한, 이런 사이버 공격에 능동적이고 선제적으로 대응하고 침해사고에 대해 사전적 예방을 위해서 국내외적으로 정보보호 관리체계 도입을 제도화하고 있다[16].

3.2.2 효율적인 ISMS의 성과 및 영향

정보보호 관리체계의 관리과정이 정보보호 성과에 미치는 영향에 관한 실증연구 자료를 살펴보면, 효과적인 정보보호 투자와 비즈니스와 연계한 조직의 경영활동의 일환으로 정보보호활동이 존재한다는 것이 입증되었다[8].

정보보호 관리체계 인증 제도를 도입하게 되면 조직은 광범위하고 효율적인 정보보호 대책을 개발할 수 있을 뿐만 아니라 자신의 정보보호 수준에 관하여 객관적인 심사를 통해 더 높은 신뢰를 가질 수 있다. 또한 위험 관리체계를 유지하고 적절한 통제를 구현함으로써 정보보호 사고와 피해 발생이 예상될 때 이를 감소시킬 수 있다. 이것은 사고로부터 조직의 가치를 보호하게 된다[18].

게다가 처음 인증 받을 당시의 정보보호 체계를 지속적으로 유지할 수 있는지 살펴보고, 정기적으로 재인증을 수행하기 때문에 조직의 정보보호 체계를 일정한 수준으로 유지할 수 있다는 점이 큰 강점이다.

12) Distributed Denial of Service. 해킹 방식의 하나로서 여러 대의 공격자를 분산 배치하여 동시에 '서비스 거부공격(Denial of Service attack; DoS)'을 함으로써 시스템이 더 이상 정상적 서비스를 제공할 수 없도록 만드는 것을 말한다.

3.3 선행 연구 검토결과

‘ISMS 기반의 군(軍)보안적용 문제점 분석’과 ‘ IT기반의 ISMS와 보안규정’에 대한 선행연구를 통해서 군 정보보호 관리체계 도입의 필요성을 확인할 수 있었다. 물론 국가기밀보호법에 기반한 군사보안훈령과 각 군에서 규정한 보안규정을 토대로 정기·수시 보안감사를 실시하여 연중 균형된 보안수준을 유지하고 있지만, 점차 빨라지는 국방 정보화 속도에 발맞추어 안정적인 보안수준을 유지하기 위한 방안이 필요하다. 따라서 국내 정보보호 관리체계(KISA ISMS)를 기반으로 하여 기존 보안감사 기법을 적절하게 조합한다면, 새롭게 증가하는 보안위협들에 대해 신속하고 능동적으로 대처하고 높은 수준의 보안태세를 항시 유지할 수 있는 좋은 시스템이 될 것이다.

이에 본 논문에서는 군에 적합한 군 정보보호 관리체계(M-ISMS)를 제안한다.

4. 군 특수성을 고려한 M-ISMS 모델 제안

4.1 M-ISMS 모델 제안

4.1.1 M-ISMS 개념

본 연구에서는 군의 특수성을 고려한 군(軍) 정보보호 관리체계(M-ISMS: Military-Information Security Management System) 모델을 제안한다. 이는 군(軍)내 정보시스템을 포함한 정보보호 분야 보안에 관한 지침과 기준을 제공하고, 정보자산의 비밀성, 무결성, 가용성을 실행하기 위한 절차와 과정을 체계적으로 수립하고, 지속적으로 관리하는 시스템을 의미한다. 제안된 M-ISMS는 첨단화 되어가고 있는 군 정보시스템 환경에 대한 정보보호 관리체계를 수립하고, 지속적인 운영이 가능하도록 하여 전반적인 군 보안감사 수준을 향상하는데 초점을 두고 있다.

4.1.2 M-ISMS 정보보호 관리과정(5단계)

정보보호 관리과정은 ISMS의 기본 흐름이기 때문에 KISA ISMS 정보보호 관리과정과 크게 다른 점이 없으며 M-ISMS에서는 [그림 6]와 같이 정보보호 정책수립 및 범위설정을 시작으로 사후관리까지 5단계 순환구조로 되어있고 보안감사 시스템 개선에 가장 핵심이 되는 2가지는 바로 2단계(지휘관 책임 및 조직 구성)와 5단계(사후관리)이다.

[그림 6] M-ISMS 정보보호 관리과정 5단계

<표 11> M-ISMS 정보보호 관리과정 5단계

관리과정	세부관리과정
1. 정보보호 정책수립 및 범위 설정	5
2. 지휘관 책임 및 조직 구성	5
3. 위험관리	11
4. 정보보호대책 구현	3
5. 사후관리	8
총 계	32

2단계에서는 정보보호 거버넌스 개념을 바탕으로 한 지휘관 중심의 정보보호 의사결정 체계를 구축해야 하고, 지휘관은 부대의 규모와 임무 중요도 분석을 통해 정보보호 관리체계의 지속적인 운영이 가능하도록 정보보호 조직을 구성하고 필요한 자원을 확보해야 한다.

정보보호 전담 조직은 기존에 임무를 수행하던 정보부서에서 담당하되 정보통신 및 전산분야는 전담 인원을 추가 할당하여 완전한 정보

보호 조직이 구성되도록 해야 한다. 이에 대한 사단급 정보보호 조직 구성에 대한 예시는 [그림 7]과 같다.

[그림 7] M-ISMS 정보보호 조직 구성(예시)

5단계에서는 지속적인 정보보호 수준 유지 및 관리를 위해 조직이 준수해야할 정보보호 관련 법적 요구사항에 대한 최신화를 유지하고, 정보보호 관리체계 범위 내에서 수행해야 하는 활동을 문서화하여 관리한다. 가장 중요한 업무는 내부감사 조직을 구성하여 연 2회(반기 1회) 이상 내부감사를 수행하고 감사결과를 지휘관에게 보고해야한다.

4.1.3 M-ISMS 통제항목

본 연구에서는 KISA ISMS 통제분야를 기반으로 하여 군의 특수성을 고려한 M-ISMS 통제분야 및 통제항목을 다음 <표 12>와 같이 확장된 유형을 제시한다. 전체적으로는 KISA ISMS를 기반으로 하지만 내부 보안감사와 대외활동 부분이 추가되어 있다. 앞에서도 설명하였듯이 보안감사 부분은 군의 특수성으로 기밀성이 보장되어야 하므로 기존의 관리체계에 추가적인 통제항목으로 포함하였다. 대외활동 관리

분야도 대외자료 공개 통제항목을 추가하였다.

<표 12> M-ISMS 통제항목

No	통제분야		통제항목	항목수
1	정보보호 정책	1.1	정책의 승인 및 공표	6
		1.1.1	정책의 승인	
		1.1.2	정책의 공표	
		1.2	정책의 체계	
		1.2.1	상위 정책과의 연계성	
		1.2.2	정책시행 문서수립	
		1.3	정책의 유지관리	
		1.3.1	정책의 검토	
		1.3.2	정책문서 관리	
2	정보보호 조직	2.1	조직 체계	4
		2.1.1	정보보호 최고 책임자 지정	
		2.1.2	실무조직 구성	
		2.1.3	정보보호 위원회	
		2.2	역할 및 책임	
		2.2.1	역할 및 책임	
3	외부자 보안	3.1 보안 요구사항 정의		4
		3.1.1	외부자 계약시 보안요구사항	
		3.2 외부자 보안 이행		
		3.2.1	외부자 보안 이행 관리	
		3.2.2	외부자 계약 만료 시 보안	
		3.2.3	외국인 고용 및 접촉관리	
4	정보자산 분류	4.1 정보자산 식별 및 책임		3
		4.1.1	정보자산 식별	
		4.1.2	정보자산별 책임할당	
		4.2 정보자산의 분류 및 취급		
		4.2.1	보안등급과 취급	
5	정보보호 교육	5.1 교육 프로그램 수립		4
		5.1.1	교육계획	
		5.1.2	교육대상	
		5.1.3	교육내용 및 방법	
		5.2 교육 시행 및 평가		
		5.2.1	교육 시행 및 평가	

No	통제분야	통제항목		항목수
6	인적 보안	6.1 정보보호 책임		8
		6.1.1	주요 직무자 지정 및 감독	
		6.1.2	직무 분리	
		6.1.3	비밀유지서약서	
		6.2 인사규정		
		6.2.1	퇴직 및 직무변경 관리	
		6.2.2	상벌규정	
		6.3 비밀취급 관리		
		6.3.1	비밀취급 인가관리	
		6.3.2	신원조사 처리	
		6.3.3	암호취급자 관리	
7	물리적 보안	7.1 물리적 보호구역		9
		7.1.1	군사보호구역 지정	
		7.1.2	군사보호구역 설비	
		7.1.3	군사보호구역 내 작업	
		7.1.4	출입통제	
		7.1.5	모바일기기 반출입	
		7.2 시스템 보호		
		7.2.1	케이블 보안	
		7.2.2	시스템 배치 및 관리	
		7.3 사무실 보안		
		7.3.1	개인업무 환경 보안	
		7.3.2	공용업무 환경 보안	
8	시스템 개발보안	8.1 분석 및 설계 보안관리		10
		8.1.1	보안 요구사항 정의	
		8.1.2	인증 및 암호화 기능	
		8.1.3	보안로그 기능	
		8.1.4	접근권한 기능	
		8.2 구현 및 이관 보안		
		8.2.1	구현 및 시험	
		8.2.2	개발과 운영환경 분리	
		8.2.3	운영환경 이관	
		8.2.4	시험데이터 보안	
		8.2.5	소스 프로그램 보안	
		8.3 외주개발보안		
		8.3.1	외주개발보안	
9	암호통제	9.1 암호 정책		3
		9.1.1	암호 정책 수립	
		9.2 암호키 관리		
		9.2.1	암호키 생성 및 이용	
		9.3 암호프로그램 관리		
		9.3.1	암호프로그램 보호관리	

No	통제분야	통제항목		항목수
10	접근통제	10.1 접근통제 정책		14
		10.1.1	접근통제 정책 수립	
		10.2 접근권한 관리		
		10.2.1	사용자 등록 및 권한부여	
		10.2.2	관리자 및 특수 권한 관리	
		10.2.3	접근권한 검토	
		10.3 사용자 인증 및 식별		
		10.3.1	사용자 인증	
		10.3.2	사용자 식별	
		10.3.3	사용자 패스워드 관리	
		10.3.4	이용자 패스워드 관리	
		10.4 접근통제 영역		
		10.4.1	네트워크 접근	
		10.4.2	서버 접근	
		10.4.3	응용 프로그램 접근	
		10.4.4	데이터베이스 접근	
		10.4.5	모바일 기기 접근	
		10.4.6	인터넷 접속	
11	운영보안	11.1 운영절차 및 변경관리		19
		11.1.1	운영절차 수립	
		11.1.2	변경관리	
		11.2 시스템 및 서비스 운영보안		
		11.2.1	정보시스템 인수	
		11.2.2	보안시스템 운영	
		11.2.3	성능 및 용량 관리	
		11.2.4	장애관리	
		11.2.5	원격운영관리	
		11.2.6	무선네트워크 보안	
		11.2.7	공개서버 보안	
		11.2.8	백업관리	
		11.2.9	취약점 점검	
		11.3 매체 보안		
		11.3.1	정보시스템 저장매체 관리	
		11.3.2	휴대용 저장매체 관리	
		11.4 악성코드 관리		
		11.4.1	악성코드 통제	
		11.4.2	패치관리	
		11.5 로그관리 및 모니터링		
		11.5.1	시각동기화	
		11.5.2	로그기록 및 보존	
		11.5.3	접근 및 사용 모니터링	
		11.5.4	침해시도 모니터링	

No	통제분야	통제항목		항목수
12	침해사고 관리	12.1 절차 및 체계		7
		12.1.1	침해사고대응 절차 수립	
		12.1.2	침해사고 대응체계 구축	
		12.2 대응 및 복구		
		12.2.1	침해사고 훈련	
		12.2.2	침해사고 보고	
		12.2.3	침해사고 처리 및 복구	
		12.3 사후관리		
		12.3.1	침해사고 분석 및 공유	
		12.3.2	재발방지	
13	IT 재해복구	13.1 체계 구축		3
		13.1.1	IT 재해복구 체계 구축	
		13.2 대책 구현		
		13.2.1	영향분석에 따른 복구대책 수립	
		13.2.2	시험 및 유지관리	
14	내부 보안감사	14.1 법적 준수검토		6
		14.1.1	최신 법령 준수검토	
		14.2 점검		
		14.2.1	사전 점검	
		14.2.2	기술적 점검	
		14.2.3	접근 및 사용모니터링	
		14.3 보안감사 실시		
		14.3.1	보안 감사 계획 및 이행	
		14.4 보안감사 종료		
		14.4.1	감사결과 및 사후관리	
15	대외활동 관리	15.1 대외 자료 공개		4
		15.1.1	일반 군사자료 공개	
		15.1.2	보안성 검토	
		15.1.3	대외홍보자료 제작 및 배포	
		15.1.4	보안조치 대상 및 시기	

4.1.4 KISA ISMS와 M-ISMS 비교 분석

M-ISMS 구축을 위한 통제분야 및 통제항목들은 다음 [그림 8]와 같이 KISA ISMS와 비교하여 2개 분야, 15개 통제항목이 추가되었고, 수정(3개) 및 삭제(3개)되었다.

특히, 군 특수성을 반영하여 내부 보안감사와 대외활동 관리 통제분야를 추가하고 세분화시켰다.

[그림 8] KISA ISMS와 M-ISMS 통제항목 비교

M-ISMS 구축을 위한 신규 통제항목들을 KISA ISMS에 반영하

기 위하여 KISA ISMS 통제 분야를 기준으로 수정 및 추가로 구분하여 나타내었다. 또한 기존 KISA ISMS 통제항목 중 M-ISMS 구축시 불필요한 항목들은 삭제로 표기하여 <표 13>과 같이 나타내었다.

<표 13> KISA ISMS와 M-ISMS 통제항목 비교

No	통제분야	추 가	수 정	삭 제
1	정보보호 정책	-	-	-
2	조직의 체계	-	-	-
3	외부자 보안	3.2.3	-	-
4	정보자산 분류	-	-	-
5	정보보호 교육	-	-	-
6	인적보안	6.3.1 6.3.2 6.3.3	-	-
7	물리적 보안	-	7.1.1 7.1.2 7.1.3	-
8	시스템 개발 보안	-	-	-
9	암호통제	9.3.1	-	-
10	접근통제	-	-	
11	운영보안	-	-	11.2.6 11.3.1 11.3.2
12	침해사고 관리	-	-	-
13	IT 재해복구	-	-	-
14	내부 보안감사	14.1.1 14.2.1 14.2.2 14.2.3 14.3.1 14.4.1	-	-
15	대외활동 관리	15.1.1 15.1.2 15.1.3 15.1.4	-	-

먼저 추가된 통제항목의 목적을 살펴보면, ‘3.2.3 외국인 접촉 및 고용관리’ 는 군내 정보가 타국으로 유출될 경우 자국의 군사력에 심

각한 영향을 미칠 수 있기 때문에 외국인을 고용하거나 접촉할 때 사전에 군사기밀 누설을 방지하기 위한 별도의 통제가 필요하다. ‘6.3 비밀취급 관리(3개 세부통제항목 포함)’는 관리자 직급을 가진 현역 간부와 군사 작전분야에서 임무를 수행하는 대부분의 장병들이 비밀을 취급하기 때문에 많은 인원에 대한 비밀취급 인가관리가 체계적으로 이루어져야하고 신원조사도 병행되어야 한다. 특히, 암호장비와 보안자재를 관리하는 암호실을 출입하는 인원은 별도로 취급인가를 발급하고 직무가 끝나는 순간까지 철저히 관리되어야 한다. ‘9.3.1 암호프로그램 보호관리’도 군사 암호알고리즘이 비인가자가 열람·획득하지 못하도록 별도의 통제 프로세스로 관리가 되어야 한다.

다음으로 추가된 통제항목 중에 가장 중요한 2가지 통제항목인 ‘내부 보안감사’와 ‘대외활동 관리’ 통제분야는 <표 14>에서 알 수 있듯이 군 특수성을 가장 잘 고려한 통제분야이다.

<표 14> M-ISMS 모델 핵심 통제분야

No	통제분야	통제항목	
14	내부 보안감사	14.1 법적 준수검토	
		14.1.1	최신 법령 준수검토
		14.2 점검	
		14.2.1	사전 점검
		14.2.2	기술적 점검
		14.2.3	접근 및 사용모니터링
		14.3 보안감사 실시	
		14.3.1	보안 감사 계획 및 이행
		14.4 보안감사 종료	
		14.4.1	감사결과 및 사후관리
15	대외활동 관리	15.1 대외 자료 공개	
		15.1.1	일반 군사자료 공개
		15.1.2	대외홍보자료 제작 및 배포
		15.1.3	보안성 검토
		15.1.4	보안조치 대상 및 시기

내부 보안감사는 정보보호 관리체계를 지속유지 하는데 핵심 통제

분야이며, 연 2회(반기 1회) 정기 내부 보안감사를 수행하고 지휘관에게 정보보호 관리수준을 모니터링 할 수 있도록 도움을 주는 자체 보안 시스템이다. 그리고 대외 활동 관리는 국민의 알 권리를 충족시키기 위하여 필수불가결하게 수행되는 대외 활동에 대한 적절한 통제도구로서 역할을 수행한다. 핵심 통제분야에 대한 세부내용은 <표 15>에 정리하였다.

<표 15> 핵심 통제분야 세부내용

통제항목		세부내용
14.1 법적 준수검토		
14.1.1	최신 법령 준수검토	감사 실시 전, 반드시 관련 정보보호 관련 최신 법령을 확인한다.
14.2 점검		
14.2.1	사전 점검	연간 정보보안 계획수립 적절성에 대해 사전 점검을 실시한다.
14.2.2	기술적 점검	감사증적을 제거하기위한 행위를 점검할 수 있는 최신 감사도구를 활용하여 책임추적성을 향상시킨다.
14.2.3	접근 및 사용모니터링	감사 실시 1주일 전에 네트워크 관제팀으로부터 주요 시스템 접근 현황을 보고받고 이상여부를 분석한다.
14.3 보안감사 실시		
14.3.1	보안 감사 계획 및 이행	연 2회(반기 1회) 내부 보안감사 계획을 수립하고 지휘관으로부터 승인받은 계획대로 감사임무를 수행한다.
14.4 보안감사 종료		
14.4.1	감사결과 및 사후관리	감사결과는 지휘관에게 보고하고 감사 성과가 지속유지 될 수 있도록 사후관리를 실시한다.
15.1 대외 자료 공개		
15.1.1	일반 군사자료 공개	'공공기관의 정보 공개에 관한 법률'에 정한 절차에 의한다.
15.1.2	보안성 검토	모든 군사정보는 정보보호 정책에 따라 각 분야별로 사전에 보안성 검토를 받아야 한다.
15.1.3	대외홍보자료 제작 및 배포	보안성 검토를 받은 자료에 대해서만 제작 및 배포가 가능하다.
15.1.4	보안조치 대상 및 시기	군 관련 사항을 공식적으로 대외 발표해야 할 때 정보보호 정책에 따른 보안조치를 실시해야 한다.

이어서 수정된 통제항목의 목적에 대해 살펴보면, ‘7.1 물리적 보호구역(3개 세부통제항목)’은 주요 정보시스템뿐만 아니라 군사보호구역으로 설정된 모든 군사시설에 대한 통제가 필요하므로 개념을 확장하여 수정하였다.

끝으로 삭제된 통제항목인 ‘11.2.6 스마트워크 보안’, ‘11.3.1 전자(상)거래 보안’, ‘11.3.2 정보전송 정책 수립 및 협약 체결’은 군내 정보시스템과는 상관없기에 통제항목에서 제외하였다.

4.2 M-ISMS 효과성

군 보안감사의 목적은 보안 제 규정에 의해 이행되는지 여부와 각 분야별로 수립된 보안대책에 대한 준수상태를 평가 및 점검하고, 보안 취약점 및 문제점에 시정을 촉구하는 데에 있다.

그리고 국민의 알 권리를 충족시킴과 동시에 군사기밀을 보호하고 적으로부터 정보우위를 지켜야 하는 군의 입장에서 본 논문에서 제안하는 포함되어 있는 대외활동 관리를 통해 효과를 얻을 수 있다. 이를 통해 국민들로부터 대군 신뢰도 향상과 향후 군사작전 계획 및 추진에 있어 큰 도움이 될 것이다.

M-ISMS가 도입되면 [그림 9]과 같은 5가지 긍정적인 효과가 발생할 것이다.

[그림 9] M-ISMS 도입 효과

첫째, 정보보호 거버넌스 개념 도입으로 인한 지휘관 중심의 정보보호 활동이 가능하다. 현대경제연구원 보고서에 따르면 지난 2009년 7·7DDoS 공격으로 인한 금전적 손실은 최소 363억원에서 최대 544

억원이라고 한다[19]. 이처럼 명확한 출처를 알 수 없는 사이버공격에 대응하기 위해서는 지휘관의 적극적인 정보보호 활동이 바탕이 되어야 정보보호 전담 조직 구성 및 정보보호 자산 확보가 가능하고 정보보호 인식과 수준 또한 향상될 수 있다. 군(軍)에서 유사한 보안사고 발생할 경우에는 민간에서 피해액을 산정하는 것과는 비교할 수도 없을 만큼 심각한 국가위기 사태에 빠질 우려도 있다. 이에 따라 사전 예방활동을 위한 전담 정보보호 조직이 구성되면 일원화 된 대응체계가 구축되어 침해사고에 따른 신속한 대응이 가능하다.

둘째, 책임추적성이 강화되어 보안감사 성과의 질적 향상 효과가 있다. 객관적이고 투명한 감사증적을 통한 정량적 평가가 가능하게 됨으로써 보안감사관의 독립성이 강화되고 인간관계에 따른 온정주의적 처분이 줄어든다.

셋째, 정보보호 관리단계에 따른 사후관리를 통해 지속적이고 균형적인 보안활동이 가능하여 평균적인 보안수준이 향상된다. 지휘관이 직접 해부대 정보보호 수준을 정기적(연간 2회)으로 모니터링 함으로써 지속적인 보안 수준 유지가 가능하며 필요시에는 지휘권을 활용하여 부대별 특성에 따른 탄력적인 정보보호 조직 개편이 가능하다.

넷째, 민간 정보보호 우수 사례를 개선하여 도입하기가 쉽다. 신규 도입된 정보시스템에 대한 취약점 분석 및 침해사고 대응방안 수립 시에 민간으로부터 다양한 사례를 미리 입수할 수 있기 때문에 정보보호 대책 수립에 많은 도움이 된다. 예를 들어, 2011년 7월에 S사에서 3,500만명 고객의 개인 정보가 유출되는 침해사고가 발생하였는데 공격은 무료 소프트웨어 업데이트 서버를 해킹하여 정상 파일을 악성코드로 변경해서 유포하는 방법을 사용했었다. 군에서도 공격자가 외부 공개서버나 사회공학 기법을 이용한 악성코드 유포를 통해 외부로 군사정보를 유출시킬 수 있을 가능성이 존재하므로 민간에서 개발한 대응책을 응용하여 군 특수성에 알맞게 적용할 수 있을 것이다.

다섯째, 안정적인 정보보호 활동으로 인해 대군 신뢰도가 향상된다. 군 특성상 폐쇄적인 정보유통 구조로 인해 국민으로부터 제대로 된 보안활동 수행여부를 밝히기 어려우나, 표준화 된 정보보호 관리체계를 도입하고 운영함으로써 보다 신뢰성 있고 안정적인 프레임워크로 관리하고 있는 모습을 통해 대군 이미지가 좋아지는 효과가 있다. 특히, 대외 홍보 활동에 대한 체계적이고 지속적인 보안활동으로 군사정보 유출을 막음으로써 그 효과를 손쉽게 증명할 수가 있다.

요약하면, 현재 단편적이고 단순 일회성으로 관리하던 정보보호 대책을 지휘관을 중심으로 한 종합적인 정보보호 대책으로 운용함으로써 군 정보보호 관리 수준을 한층 더 향상시킬 수 있다.

특히, 지휘관이 직접적으로 정보보호 활동에 개입하게 되므로 통합적이고 균형적인 보안이 가능하다. 나아가 정보보호 거버넌스 및 컴플라이언스와 연계되어 지속적이고 체계적인 정보보호 관리가 이루어질 것이다. 게다가 민간과 유사한 관리체계를 운영함으로써 침해사고 발생시에 대응방안도 유사하게 도출 할 수 있게 되므로 민-군 연계 대응이 가능한 장점이 있다.

또한, M-ISMS에서 요구하는 통제항목을 시행하게 되면 정보관리에 대한 책임추적성이 강화되어 군 보안감사에 결정적인 도움이 될 것이다.

[그림 10] M-ISMS 목표

5. 결론 및 향후 연구 방향

5.1 결 론

본 논문에서는 국내외 정보보호 관리체계에 대한 이론적 배경과 기존 선행 연구를 토대로 군(軍)정보보호 관리체계를 제안하고, KISA ISMS를 적용한 M-ISMS가 군 보안감사 개선에 주는 효과성에 대해 연구하였다.

현재 군 보안감사는 규정에 입각하여 감사 임무를 수행하되, 감사관의 주관적 판단이 많이 개입될 소지가 많으므로 보다 객관적이고 체계적인 관리 방법론의 필요성이 대두되고 있다. 또한, 민감한 군사정보 취급과 대국민 홍보를 함께 해야 하는 두가지 입장에서 효과적인 대외활동을 위해서 보다 안전한 정보보호 관리방법이 필요한 상태이다.

이에 본 논문에서는 일반 조직과 다른 특수한 환경적 특성을 고려하여 기존 KISA ISMS를 바탕으로 군에 최적화된 통제항목(15개 통제분야 104개 통제항목)을 개발하여 새로운 정보보호 관리체계 모델(M-ISMS)을 제시하였다.

본 논문에서 제안한 M-ISMS는 군내 정보시스템을 포함한 전반적인 보안에 관한 지침과 기준을 제공하고, 정보자산의 비밀성, 무결성, 가용성을 실행하기 위한 절차와 과정을 체계적으로 수립하고 지속적으로 관리할 수 있는 시스템으로써 정보보호 거버넌스 개념을 바탕으로 설계되어있다.

정보보호 거버넌스는 보안담당자만 정보보호 임무를 수행하는 것이 아니라 모든 임무수행에 사용되는 유용한 도구인 정보시스템을 포함한 전반적인 정보보호 분야를 정보보호 관리체계를 통하여 최고 지

휘관이 중심이 되어 보안 분야에 대해 균형적으로 조직을 관리하는 것을 말한다. 이는 간략히 관리책임성(Accountablility), 임무 연계성(Mission Alignment), 준거성(Compliance) 3가지 명제로 표현할 수 있으며, 이 명제들을 확보하기 위한 조직의 노력이 곧 정보보호 거버넌스라 할 수 있다. 이 목표를 달성하기 위해 필요한 조직을 구성하고 제도를 재정립하고, 예산 및 자원 확보를 하는 거버넌스 실행체계를 운영함으로써 사전에 군사기밀 유출사고를 방지하고 신속하게 대응책을 마련할 수 있다.

지금까지 군 자체 단독 대응책으로 정보보호를 수행하고 있는데 반해 표준화 된 정보보호 관리체계 도입은 민간 운영사례와 사고 사례를 통해 향후 대책을 보다 손쉽게 수립할 수 있다. 특히, 운영보안, 침해사고 관리, IT재해복구 분야에 대해서는 최근 발생한 2009년 7.7 DDoS 공격, 2013년 3.20 사이버테러, 6.25 사이버테러 등 다수의 침해사고 사례에 대한 다양한 대응책이 수립되어 있으며, 홈페이지 변조나 DDoS 공격, 신상정보 탈취 공격 등에 대한 세부 대응책들을 큰 어려움 없이 군 정보보호 체계와 연계해서 더욱 발전된 형태로 계획을 수립하여 추진할 수 있다.

끝으로 M-ISMS 도입에 따른 가장 큰 효과는 지휘관 중심의 정보보호 관리체계가 구축되어 보안감사 수준이 지속적으로 향상되는 결과를 가져오게 되므로 현재 군 보안감사 개선에 큰 도움이 될 것이라 기대된다.

5.2 향후 연구방향

본 논문에서 제안한 바와 같이 정보보호 관리체계의 도입과 운영은 현재의 군 정보보호 수준을 전반적으로 향상시키고 지속유지 시켜주는 좋은 도구가 될 것이다. 이를 통해 군 보안감사 기법과 혁신적인 모델을 만들어 나간다면 급속도로 발전해나가는 ICT 수준과 발맞춰 선진화 된 국방 정보시스템 도입에도 큰 역할을 할 것으로 생각된다.

따라서, 앞으로 국·내외 위탁교육생들의 활발한 연구활동을 통해 현역 보안감사관을 비롯한 IT거버넌스에 포함되는 관계자들에게 실질적 필요성과 효과성을 검증하기 위한 설문 조사를 비롯한 각 제대별 모델 제시 및 실증테스트 검증이 이루어져야 할 것이며, 이를 정책적으로 발전시켜 나가는 개선된 연구모델 개발이 필요하다.

참고문헌

[1] 국가정보원·미래창조과학부·방송통신위원회·안전행정부, "2013 국가정보보호백서", 한국인터넷진흥원, pp.5, 96, 97, 275, 283, 286, 2013.

[2] 국방부 정책기획관실 기본정책과, "2012년 국방백서", 국방부, pp.140 2013.

[3] 한국정보통신기술협회(정보통신용어사전), http://word.tta.or.kr

[4] 안경윤, "정보보호 관리체계 통제항목기반 디지털 포렌식 통제체계 설계", 동국대 국제정보대학원 정보보호학과, pp.5-6, 2011.

[5] 미래창조과학부·한국인터넷진흥원, "정보보호 관리체계(ISMS) 인증 제도 안내서 v0.8", pp.5, 2013.

[6] ISO Survey 2012, Retrieved on 10th November 2013 from http://www.iso.org/iso/home/standards/certification/iso-survey.htm

[7] Smile:it's BS7799, Retrieved on 2nd November 2013 from http://archive.bcs.org/bulletin/may01/article4.htm

[8] 장상수, 정보보호 관리체계 운용이 정보보호 성과에 미치는 영향에 관한 실증 연구, 전남대 정보보호 협동과정 박사, pp.6, 2011.

[9] 이동녁, 개인정보보호를 위한 정보시스템 보안감사 방법에 관한 연구, 명지대 산업경영공학과 석사, pp.17, 21-23, 2010.

[10] 산업통상자원부, 정보보안관리체계(ISMS) 국제표준 2.0 시대 예고, pp.3-4, 2013.

[11] Introducing the 2013 revision of ISO/IEC 27001, Retrieved on 15th November 2013 from http://www.bsigroup.ae

[12] 한국인터넷진흥원, http://isms.kisa.or.kr/kor/intro/intro01.jsp

[13] ISMS 연도별 인증서 발급현황, Retrieved on 31th October 2013 from http://isms.kisa.or.kr/kor/issue/issue01.jsp?certType=ISMS

[14] 방송통신위원회/한국인터넷진흥원, "ISMS 인증 모범사례집", pp.20-25, 2010.

[15] 박동희, 군 보안규정의 문제점과 발전방향 모색, 경기대학교, pp.45, 2013
[16] 정보과학회논문지, 정보보호 관리체계 운용이 정보보호 성과에 미치는 영향, pp.2, 2013.
[17] 조희준, "IT 거버넌스 프레임워크 코빗 – COBIT 4.1을 중심으로", pp.41-46, 2010.
[18] KISA, "정보보호 관리체계인증 ISMS, pp.18, 2007.
[19] 현대경제연구원 “사이버 테러의 상시 감시 체제를 구축하자! – 디도스 사이버 테러의 피해와 대책 –”, pp.2, 2009.