JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지(J. Korea Inst. Inf. Commun. Eng.) Vol. 18, No. 3 : 761~769 Mar. 2014

# M-ISMS 모델 기반의 군(軍) 보안감사 설계에 관한 연구

김대규[1] · 조희준[2] · 김창수[3*]

# The Design of Military Security Audit based on the M-ISMS Model

**Dae Gyu Kim[1] · Hee Joon Cho[2] · Chang Soo Kim[3*]**

[1]Department of IT Convergence and Application Engineering, Pukyung National University, Busan 608-737, Korea
[2]Department of Digital Management, Korea University, Sejong 339-700, Korea
[3*]Department of IT Convergence and Application Engineering, Pukyung National University, Busan 608-737, Korea

## 요 약

본 논문에서는 군 특수성을 고려한 정보보호 관리체계를 기존 ISMS를 기반으로 개선된 M(Military)-ISMS 모델을 제시한다. 이는 ISMS에서 논의 되지 않은 군 특수성을 고려한 '내부 보안감사'와 '대외활동 관리'부분이 주요 연구대상이다. 내부 보안감사 부분은 민간에서 중요하게 다루는 가용성보다 기밀성이 중요하기 때문에 기밀성과 관련된 보안감사의 6가지 통제항목을 추가하였다. 또한 대외활동 관리부분은 해당 군사자료가 비밀로서 가치가 사라졌을 경우 보안관리 기준 수립과 수준유지에 관한 통제항목 등을 추가하였다. 본 논문에서 제안된 M-ISMS는 기존의 ISMS에서 제공하는 다양한 장점들과 민간 침해사고 사례를 활용하여 군의 특수성을 고려한 신속하고 미래지향적인 보안 침해사고를 사전에 예방할 수 있는 효과가 있다.

## ABSTRACT

We propose an improved M-ISMS(Military-ISMS) model which is based on common ISMS model for regarding military's unique characteristics. Our model focuses on 'Internal Security Audit' and 'Management of external activity' as military circumstances. So, we added the six control new items as internal security audits. Because the confidentiality is more important than availability in military service as compared with private sectors. In addition, we propose some control suggestions for establishing security management standards and keeping level maintenance when it will becomes to lose a value as confidential. The M-ISMS model in this paper has effectiveness which prevents security incidents in advance rapidly throughout a variety of common ISMS's advantages and security incidents of private sectors in consideration of military characteristics.

**키워드** : M-ISMS, ISMS, 군 정보보호관리체계, 정보보호 관리체계, 보안감사

Key word : M-ISMS, ISMS, Military-Information Security Management System, Information Security Management System, security inspection, security audit

접수일자 : 2013. 12. 18 심사완료일자 : 2014. 01. 28 게재확정일자 : 2014. 02. 10

* **Corresponding Author** Chang Soo Kim (E-mail:cskim@pknu.ac.kr, Tel:+82-51-629-6245)
Department of IT Convergence and Application Engineering, Pukyong National University, Busan 608-737, Korea

Open Access http://dx.doi.org/10.6109/jkiice.2014.18.3.761 print ISSN: 2234-4772 online ISSN: 2288-4165

## Ⅰ. 서 론

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 국제표준 정보보호관리체계(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 정보보호관리체계가 반드시 필요하다.

본 연구는 아래 3가지 방향으로 진행된다. 첫째, 국내외 ISMS(정보보호관리체계) 및 지침 등에 관하여 살펴보고, 둘째, 군(軍)보안감사의 현실적 문제점에 대한 선행 연구를 검토하고,셋째, KISA ISMS와 관련된 법률 및 지침 등에서 군용 정보보호관리체계(M-ISMS : Military Information Security Management System) 수립을 위한 요건을 도출하여 군(軍)보안감사에 적용 가능한 정보보호관리체계 모델을 제안한다. 본 논문은 전체 5장으로 구성되어 있다. 2장에서는 국내 정보통신기반 보호법과 ISMS(정보보호관리체계)에 대해 살펴보고, 3장에서는 군 특수성을 고려하여 군(軍)보안감사의 현실적 문제과 IT거버넌스 개념의 ISMS에 대해 분석해 본다. 4장에서는 군 특수성을 고려한 군(軍) 정보보호관리체계(M-ISMS)를 제안하고, 5장에서는 결론으로 구성한다.

## Ⅱ. 국내외 정보보호관리 인증제도

### 2.1. ISMS(정보보호관리체계)

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 비밀성(Confidentiality), 무결성(Integrity), 가용성(Availability) 3가지로 정리된다.

또한 정보전의 분야에서는 "우연히 혹은 의도적으로 허가 받지 않는 정보의 누출, 전송, 수정, 파괴 등으로부터의 보호"로 정의하고 있으며, 국제표준인 ISO/IEC27001에서는 정보보호의 사업 지원 측면을 강조하여 "사업의 지속성을 보장하고 사업 위험을 최소화하고 투자회수와 사업기회를 최대화하기 위하여 다양한 위협으로부터 정보를 보호하는 것"으로 정의 하고 있다.

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

여기서 정보보호관리체계란 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. ISO/IEC 27001

국제 표준화 기구 ISO(International Organization for Standardization)와 IEC(International Electotechinical Commission)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 수립, 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[6].

### 2.3. KISA ISMS

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.

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

정보보호관리과정은 정보보호 관리체계 인증 심사 시 요구되는 필수 항목으로서 5단계, 12개 통제항목으로 구성되어 있으며 그림 1과 같이 조직 내·외부 위협요소의 변화 또는 새로운 취약성 발견 등에 대응하기 위하여 지속적으로 유지 관리되는 순환주기의 형태를 가진다.

**표 1.** KISA ISMS 정보보호 관리체계 인증 기준표
**Table. 1** KISA ISMS Certification Basis

| 분 야 | | 통제 항목 |
|---|---|---|
| 관리과정 | 1. 정보보호정책수립 및 범위설정 | 2 |
| | 2. 경영진 책임 및 조직구성 | 2 |
| | 3. 위험관리 | 3 |
| | 4. 정보보호대책 구현 | 2 |
| | 5. 사후관리 | 3 |
| 정보보호 대책 | 1. 정보보호정책 | 6 |
| | 2. 정보보호조직 | 4 |
| | 3. 외부자 보안 | 3 |
| | 4. 정보자산분류 | 3 |
| | 5. 정보보호교육 | 4 |
| | 6. 인적보안 | 5 |
| | 7. 물리적 보안 | 9 |
| | 8. 시스템 개발보안 | 10 |
| | 9. 암호통제 | 2 |
| | 10. 접근통제 | 14 |
| | 11. 운영보안 | 22 |
| | 12. 침해사고 관리 | 7 |
| | 13. IT재해복구 | 3 |
| 총 계 | | 104 |


**그림 1.** KISA ISMS 정보보호 관리과정 5단계
**Fig. 1** KISA ISMS IS Management Process 5Step

**표 2.** KISA ISMS 정보보호 관리과정 5단계
**Table. 2** KISA ISMS IS Management Process 5Step

| 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 정보보호관리체계 인증 심사시 요구되는 선택 항목으로서 표 2와 같이 총 13개 분야 92개 통제항목으로 구성되어 있으며, 위험평가를 통하여 조직이 수용한 위험수준을 달성할 수 있도록 통제항목을 선택한다.

## Ⅲ. 군 특수성을 고려한 ISMS 분석

### 3.1. 군(軍)보안감사의 현실적 문제

국가안보를 보장하는 군 특수성을 바탕으로 군에서는 보안감사를 위한 별도의 감사팀을 운영하고 있으며 보안감사업무의 전문화가 이루어지고 있다. 군 보안감사는 정기감사(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)[7].

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. 피감사부대에서 제출받은 감사자료를 기초로 일반적으로 3~5일 동안 4~5명으로 편성된 감사관이 문서보안, 인원보안, 정보통신보안, 시설보안 등 정보보안 모든 분야를 감사하기에는 시간적 여유가 부족하다.

셋째, 감사 주기가 길기 때문에 보안감사 목표 수준을 높게 유지하기가 어렵다. 게다가 감사관 재량범위가 넓어 자체 경감처리에 의한 온정주의 처분도 있어 감사결과가 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 국방 정보화 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. IT거버넌스 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[8].

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 군 경영의 관점에서 주체가 상호 균형을 이루면서 자신의 분야에 책임감을 가질 수 있는 관리체계를 구축하는 과정이 필요할 것이다.

군의 관점에서 가장 중요시 되는 것은 바로 책임 추적성이다. 그리고 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[9].

### 3.3. 선행 연구 검토결과

'군(軍)보안감사의 현실적 문제'와 'IT거버넌스 개념의 ISMS 검토'에 대한 선행연구를 통해서 군 정보보호

관리체계 도입의 필요성을 확인할 수 있었다. 물론 국가기밀보호법에 기반한 군사보안훈령을 토대로 정기·수시 보안감사를 실시하여 연중 균형된 보안수준을 유지하고 있지만, 점차 빨라지는 국방 정보화 속도에 발맞추어 안정적인 보안수준을 유지하기 위한 방안이 필요하다. 한편, 정보보호 거버넌스의 역할은 문서화된 정책에 기반을 두어 수행되는 정보보호 활동을 보다 굳건히 만드는 것에 있다. 기업으로 비유하자면, 기업에서 수행되는 수많은 정보보호 활동들이 기업의 목표와 방향에서 벗어나지 않도록 책임성, 비즈니스 연계성, 준거성 원칙에 따라 중심을 잡는 역할을 수행함을 의미한다. 정보보호 거버넌스의 목표와 원칙을 정보보호 관리체계에 적용하기 위해서는 정보보호 관리체계 기반이 정보보호 활동과 정보보호 거버넌스의 목표인 책임성, 비즈니스 연계성, 준거성을 연계하는 연결 고리가 반드시 결정되어야 한다[10]. 따라서 국내 정보보호관리체계(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 정보보호관리체계(M-ISMS)를 제안한다.

## Ⅳ. 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) 정보보호관리체계(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 ISMS정보보호 관리과정과 크게 다른 점이 없으며, M-ISMS에서는 그림 2과 같이 5단계 순환구조로 되어있고 현 보안감사 시스템 개선의 핵심 2가지는 바로 2단계(지휘관 책임 및 조직 구성)와 5단계(사후관리)이다.


**그림 2.** M-ISMS 정보보호 관리과정 5단계
**Fig. 2** M-ISMS IS Management Process 5Step

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 정보보호 조직이 구성되도록 해야 한다. 그림 3는 사단급 정보보호 조직 구성에 대한 예시이다.

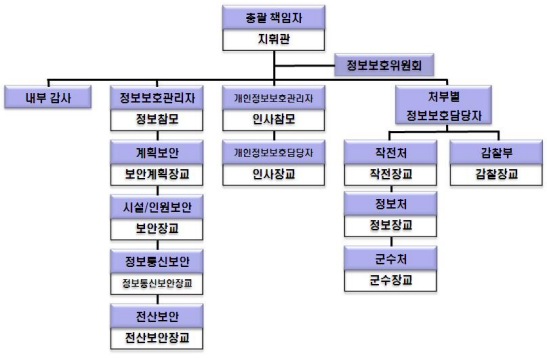


**그림 3.** M-ISMS 정보보호 조직 구성(예시)
**Fig. 3** M-ISMS Information Security Organization(example)

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. 그리고 내부감사 조직을 구성하여 연 2회(반기 1회) 이상 내부감사를 수행하고 감사결과를 지휘관에게 보고해야 한다.

4.1.3. M-ISMS 통제항목

본 연구에서는 KISA ISMS 통제분야를 기반으로 하여 군의 특수성을 고려한 M-ISMS 통제분야 및 통제항목을 확장한 유형을 제시한다. 군의 특성상 기밀성이 강조된 내부 보안감사와 대외활동 부분이 추가되었다.

4.1.4. KISA ISMS와 M-ISMS 비교 분석

M-ISMS 구축을 위한 통제분야 및 통제항목들은 그림 4과 같이 KISA ISMS와 비교하여 2개분야, 15개 통제항목이 추가, 수정(3개) 및 삭제(3개)되었다.


**그림 4.** KISA ISMS와 M-ISMS 통제항목 비교
**Fig. 4** The comparison of KISA ISMS and M-ISMS control items

내부 보안감사는 정보보호 관리체계를 지속유지 하는 핵심 통제분야이며, 연 2회(반기 1회) 정기 내부 보안감사를 수행하고 지휘관에게 정보보호 관리수준을 모니터링 할 수 있도록 도움을 주는 자체 보안시스템이다. 그리고 대외 활동 관리는 국민의 알 권리를 충족시키기 위하여 필수불가결하게 수행되는 대외 활동에 대한 적절한 통제도구로서 역할을 수행한다. 핵심 통제분야에 대한 세부내용은 표 4에 정리하였다.

**표 3.** M-ISMS 모델 핵심 통제분야
**Table. 3** Key control area of M-ISMS model

| 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 |

**표 4.** 핵심 통제분야 세부내용
**Table. 4** Detailed contents of Key control area

| 통제항목 | 세부내용 |
|---|---|
| 14.1 법적 준수검토 | |
| 최신 법령 준수검토 | 감사 실시 전, 반드시 관련 정보보호 관련 최신 법령을 확인한다. |
| 14.2 점검 | |
| 사전 점검 | 연간 정보보안 계획수립 적절성에 대해 사전 점검을 실시한다. |
| 기술적 점검 | 감사증적을 제거하기위한 행위를 점검할 수 있는 최신 감사도구를 활용하여 책임추적성을 향상시킨다. |
| 접근 및 사용모니터링 | 감사 실시 1주일 전에 네트워크 관제팀으로부터 주요 시스템 접근 현황을 보고받고 이상여부를 분석한다. |
| 14.3 보안감사 실시 | |
| 보안 감사 계획 및 이행 | 연 2회(반기 1회) 내부 내부 보안감사 계획을 수립하고 지휘관으로부 승인받은 계획대로 감사임무를 수행한다. |
| 14.4 보안감사 종료 | |
| 감사결과 및 사후관리 | 감사결과는 지휘관에게 보고하고 감사성과가 지속유지 될 수 있도록 사후관리를 실시한다. |
| 15.1 대외 자료 공개 | |
| 일반 군사자료 공개 | '공공기관의 정보 공개에 관한 법률'에 정한 절차에 의한다. |

| | |
|---|---|
| 보안성 검토 | 모든 군사정보는 정보보호 정책에 따라 각 분야별로 사전에 보안성 검토를 받아야 한다. |
| 대외홍보자료 제작 및 배포 | 보안성 검토를 받은 자료에 대해서만 제작 및 배포가 가능하다. |
| 보안조치 대상 및 시기 | 군 관련 사항을 공식적으로 대외 발표해야 할 때 정보보호 정책에 따른 보안조치를 실시해야 한다. |

### 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 대군 신뢰도 향상의 효과를 얻을 수 있다.

M-ISMS가 도입되면 그림 5와 같은 5가지 긍정적인 효과가 발생할 것이다.


**그림 5.** M-ISMS 도입 효과
**Fig. 5** The effect of M-ISMS model

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 544억원이라고 한다[11]. 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 보안감사에 투입되는 자원(인력, 시간, 예산 등) 낭비를 줄이게 되며, 보안감사관의 독립성이 강화되어 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 모니터링함으로써 지속적인 보안 수준 유지가 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 향상되는 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 대책이 조직적이고 종합적인 정보보호 대책으로 체계적으로 구현된 것을 운용함으로써 군 정보보호 관리 수준을 한층 더 향상시킬 수 있다.


**그림 6.** M-ISMS 목표
**Fig. 6** The aim of M-ISMS model

## Ⅴ. 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.

최고 지휘관이 중심이 되어 보안 분야에 대한 균형적인 조직관리가 이루어짐으로써 필요한 조직을 구성하고 제도를 재정립하고, 예산 및 자원을 확보하는 거버넌스 실행체계를 운영함으로써 군사기밀 유출사고를 사전에 방지하고 신속하게 대응책을 마련할 수 있다.

끝으로 M-ISMS 모델은 다양한 영역을 운영하고 통제하는 군의 특성을 고려할 경우 현장 특성에 부합되는 세분화된 실행모델에 대한 연구가 필요하다.

## REFERENCES

[1] KISA, *2013 National Information Security Whitepaper*, 2013.
[2] Ministry of National Defense, *2012 Military Whitepaper*, ch. 6, pp. 136-140, 2013.
[3] Telecommunications Technology Association. [Internet]. Available: http://word.tta.or.kr.
[4] Kyoung-yun Ahn, "Design of Digital Forensics Control System based on ISMS Control Item," M.S. dissertation, Dongguk University, Seoul, 2011.
[5] KISA, *ISMS certification system guidebook v0.8*, ch. 1, pp. 5, 2013.
[6] Sang-soo Jang, "The effects of the operation of an information security management system on the performance of information security," Ph.D. dissertation, Chonnam University, Gwangju, 2011.
[7] Dong-hee Park, "Probems of the Security Regulation and Improvement Measures," M.S. dissertation, Kyonggi University, Suwon, 2011.
[8] S. S. Jang, B. N. Noh, and S. J. Lee, "The Effects of the Operation of an Information Security Management System on the Performance of Information Security," *Journal of Korean Institue of Information Scientists and Engineers*, vol. 40, no. 1, pp. 58-69, Feb. 2013.
[9] Hee-joon Cho, *IT Governance Framework COBIT*, ch. 2, pp. 41-46, 2010.
[10] Seung-Han Ryu and Dae-Ryeong Jeong and Hoe-Kyung Jun, "Ways to establish public authorities information security governance utilizing E-government information security management system(G-ISMS)," *Journal of KIICE*, vol.17, no.4, pp.769-774, April 2013.
[11] Jang-gyun Lee, "Let's build a system for monitoring of cyber terrorism" Hyundai Research Institute, Pending issue Reference, 2009.

김대규(Dae-Gyu Kim)

2007년 부경대학교 컴퓨터멀티미디어공학과 공학학사
2014년 부경대학교 정보시스템협동과정 공학석사
※관심분야 : 해양안보 및 군사/국방과학, 컴퓨터시스템 및 정보보안, 정보통신행정 및 정책

조희준(Hee-Joon Cho)

2012년 고려대학교 정책대학원 감사행정학 석사
2012년~현재 고려대학교 일반대학원 디지털경영학과 박사 수료
2010년 6월~현재 (주)씨에이에스 컨설팅 이사
※관심분야 : IT/정보보호 거버넌스, IT/정보보호 감사 및 감리

김창수(Chang-Soo Kim)

1991년 중앙대학교 컴퓨터공학과 공학박사
2006년~현재 유비쿼터스 부산도시협회 부회장
2006년~현재 (사)그레고리장학회 이사
2013년~현재 한국정보통신학회 이사
1992년~현재 부경대학교 IT융합응용공학과 교수
※관심분야 : 운영체제, 방재IT, 지리정보, 도시방재, u-헬스, 바이오엔지니어링, 지식재산 등