정 보 보 호 학 회 지
제25권 제6호, 2015. 12

방산업체 ISMS 인증제도 적용방안 연구

이 재 각*

요 약

방산업체에 대한 해킹사고 및 방산기밀 유출을 예방하기 위한 보안활동은 방산업체뿐만 아니라 국가안보 차원에서도 매우 중요한 문제다. 반면, 방산업체 대상 보안지원활동은 조직 전체가 아닌 시설 및 정보시스템 중심으로 수행되고 있어 조직 전체적인 정보보호수준을 제고하고 사이버위협에 대한 대응능력을 확충하는데는 한계가 있다. 이에 본 논문에서는 방산업체의 보안수준을 근본적으로 향상시키기 위한 방안으로 대내·외에서 널리 활용되고 있는 ISMS 인증제도를 분석하고 이를 토대로 민간 ISMS에 기반한 방산업체 ISMS 적용방안을 제안한다.

Ⅰ. 서 론

방위산업 분야에서의 제 3국발 사이버 테러와 반복되는 해킹사고, 방산기밀 유출사고 발생 등으로 방산 보안에 대한 관심이 고조되고 있다. 특히, 방산업체 및 ADD 해킹사고[1,2] 등 무기체계 원천기술을 목표로 하는 해킹공격의 발생으로 사이버상에서의 위협이 우리가 생각하는 이상으로 심각함을 인식하게 되었으며 사이버위협에 효과적으로 대응하기 위해 방산업체의 보안수준을 체계적으로 관리할 수 있는 방안이 요구되고 있다.

현재 방산업체는 방산보안업무훈령을 근거로 보안감사, 보안측정, 보안사고 조사 등 기무사의 보안지원활동을 받고 있으나 이는 조직 전체적인 수준을 진단하고 대책을 제시하기보다는 보안규정 준수 여부, 위규 적발 및 특정 시설·정보시스템에 대한 보안요건 구비 여부 중심의 단편적인 활동에 국한되어 조직 전체의 정보보호 수준을 향상시키는데는 한계가 있는 실정이다.

따라서 본 논문에서는 조직 전체적인 보안수준을 체계적으로 관리함으로써 방산업체의 해킹사고 및 방산기밀 유출을 예방하기 위한 방안으로 방산업체에 대한 ISMS 인증제도 도입방안을 논의하고자 한다.

KISA의 ISMS 인증제도는 국제표준인 ISO/IEC 27001을 벤치마킹하여 개발한 정보보호관리체계로서 국내 민간분야에 통용되고 있는 체계이다. 방산업체는 기본적으로 민간기업이므로 KISA의 ISMS 평가지표를 적용할 수 있으나 방산업체 특성을 고려하여 특화된 평가지표를 추가하되 평가품질 보장을 위해 방산업체 보안지원을 담당하는 기무사와 KISA 인력이 함께 참여하는 평가팀을 구성하는 방식으로 방산업체에 대한 ISMS 인증제도를 시행할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 정보보호 인증제도 소개 및 도입 효과에 대해 살펴보고 3장에서는 국내외 정보보호 인증제도 현황 및 적용실태를 분석한다. 이를 토대로 4장에서는 방산업체 ISMS 적용 및 발전방향을 제시하고 5장에서는 앞서 논의한 사항들에 대해 시사점을 고찰하고 결론을 맺는다.

Ⅱ. ISMS 인증제도 소개

2.1. ISMS 인증제도

ISMS 인증제도는 정보보호 관리체계라는 도구를 사용하여 전문적이고 객관적인 제3자가 특정 조직의 정보보호수준 전반을 평가하고 인증하는 제도이다[3].

2005년 국제표준화기구에서 정보보호관리체계의 표준화 필요성을 인식하고 영국 표준인 BS7799를 기반으로 ISO/IEC 27001을 국제표준으로 개발하였다. ISO/IEC 27001을 통해 모든 나라가 동일한 기준의 정보보호관리체계 인증을 획득하고 상호 인정함으로써 기업간 국제 거래시 상대방 기업의 정보보호 수준을 객관적으로 평가할 수 있는 기준으로 활용할 수 있게 되었다.

국제표준화기구에서 개발한 ISO/IEC 27001은 국가별 독자적인 정보보호 수준 인증제도와 상호 보완하며 지속적으로 발전하고 있는데 국제표준은 국가별 정보보

* 국군기무사령부 (jaikag@hanmail.net)

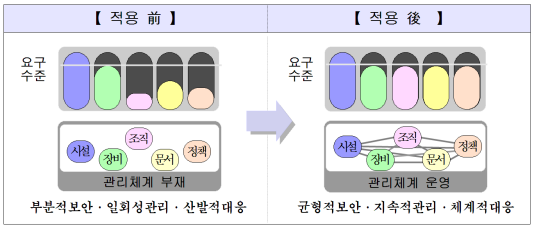
호 수준 인증제도에 영향을 미침으로써 국가별 평가제도의 점검항목은 서로 유사한 형태로 발전하고 있다.

2.2. ISMS 인증제도 적용 효과

ISMS 인증제도는 그림 1에서 보는 바와 같이 정보보호정책, 조직/인력, 정보시스템, 정보통신시설 등 각 분야의 보안수준을 진단하기 위해 개발된 통제항목을 활용하여 조직 전반의 정보보호수준을 점검하고 개선대책을 제시한다.

이러한 ISMS 인증제도는 다양한 장점이 있는데, 대외적으로 기업의 정보보호 관리능력에 대한 보증을 제공함으로써 조직 이미지 제고 및 사업 활성화에 기여할 수 있다. 또한, 인증과정을 통해 관리체계를 재검토하고 보완하는 과정에서 조직 및 인력을 보강하고 정보시스템 취약점을 보완하는 등 관리체계를 강화할 수 있으며 이는 장기적으로 정보보호 수준을 개선하여 조직 목표 달성을 지원한다. 이외에도 정보보호체계를 수립하고 정착시킬 수 있도록 담당조직에 힘을 실어주며 지속적인 관리체계 구축 활동을 통해 직원들로 하여금 정보보호의 중요성 및 필요성을 인식시키고 능동적 정보보호 활동을 가능토록 유도한다[4].

궁극적으로 ISMS 인증체계 도입을 통해 조직내부에 정보의 기밀성, 무결성, 가용성을 지속적으로 유지하는 관리시스템이 정착되며 종합적이고 효과적인 정보보호 대책을 수립토록 함으로써 조직 전반적인 정보보호 관리수준 향상으로 이어지게 된다.



〔그림 1〕 ISMS 적용 前·後 비교

Ⅲ. 국내 · 외 정보보호 인증제도

3.1. 해외 정보보호 인증제도

해외에서는 미국의 FISMA[5], 일본의 JIPDEC ISMS[4,6], 대만의 CNS[4,6] 사례를 참고할 수 있는데 FISMA는 연방기관을 대상으로 정보보호수준을 평가하는데 비해 JIPDEC ISMS는 국가기관 및 민간업체에 동시에 적용하고 있으며 대만 CNS는 주요기반시설에 대해 인증의무를 부여하고 있다는데 차이가 있다.

3.1.1. 미국(FISMA)

FISMA는 2002년 제정된 연방 정보보호 관리법으로 미국 전자정부법 3편(E-Goverment Act, Title III)의 별칭이다. 미국 연방정부의 정보 및 정보시스템에 대한 정보보호를 강화하고 정보보호에 대한 효율성과 적절성을 확보하기 위해 제정되었다.

연방정부기관의 최고정보관리책임자와 정보보호책임자는 관리체계를 매년 검토하여 그 결과를 대통령 직속의 예산관리국에 보고하며 하원정부개혁위원회에서는 보고서를 바탕으로 매년 초 연방기관의 정보보호 수준을 A~F로 평가하여 발표한다.

3.1.2. 일본(JIPDEC ISMS)

JIPDEC(일본정보처리개발협회)에서는 2002년부터 ISMS 관련 독자 기준을 개발하여 사용하고 있으며, 이후 개발된 국제표준인 ISO/IEC 27001의 내용도 일부 수용하였다. 인증유효기간은 3년이고 매년 인증기관 유지요건에 대한 인증심사를 실시한다.

국가기관, 민간업체 등 관리체계 인증 대상에 대한 제한은 없으나, 관리체계 인증활성화를 위해 정부사업 입찰조건으로 관리체계 인증 취득 또는 가산점 부여를 명시하고 있다.

3.1.3. 대만(CNS)

CNS(중국국가표준)를 제정하여 총리실 산하 국가정보통신안전회의에서 국가주요기반시설에 대해 관리체계 인증 취득을 의무화하여 시행하고 있다.

〔표 1〕 국외 정보보호 수준 인증제도 비교

평가제도	국 가	시행년도	대 상	방법/결과
FISMA	미 국	2002년	연방기관	현지실사 / 등급 부여 (A~F)
JIPDEC	일 본	2002년	국가기관, 민간업체	현지실사 / 인증
CNS	대 만	2003년	국가기관, 민간업체	현지실사 / 인증

인증대상으로 정부기관, 학술연구기업, 통신・전력・수도・금융・병원 등 산업분야로 구분하고 각 기업을 중요도에 따라 A(중요핵심), B(핵심), C(중요), D(일반) 4등급으로 분류한다. A・B급 기업은 2008년까지 모두 정보보호 관리체계 인증을 취득하였으며 C・D급 기업의 ISMS 인증취득은 권고사항이다.

3.2. 국내 정보보호 인증제도

국내에서 민간영역은 KISA의 ISMS, 국가・공공분야는 국가정보원 정보보안 관리실태 평가, 국방분야는 기무사 정보보호 관리수준평가 제도를 통해 해당 분야 조직에 대한 정보보호수준 평가 및 인증제도를 시행하고 있다.

〔표 2〕 국내 정보보호 수준 인증제도 비교

평가제도	수행기관	시행년도	평가항목	방법/결과
ISMS	미래부	2003년	104개	현지실사 / 인증
정보보안 관리실태 평 가	국정원	2007년	115개	현지실사 + 활동점수 / 점수제
정보보호 관리수준 평 가	국방부 (기무사)	2014년	83개	현지실사 / 점수제

3.2.1. KISA ISMS(민간)

2001년 ‘정보통신망 이용촉진 및 정보보호 등에 관한 법률’ 개정에 따라 정보보호관리체계 인증제도가 탄생하여 2003년부터 인증제도 적용이 시작되었다.

최초인증심사 후 매년 사후심사를 받아야 하며, 인증유효기간 3년 도래시점에 갱신 심사를 통해 인증효력 유지가 가능하다.

KISA ISMS는 ISP, IDC 및 정보통신서비스 제공자 중 연매출 100억원 이상 또는 이용자수 100만명 이상 기업에 의무 적용하고 있으며 의무 대상자가 ISMS 인증을 받지 않을 경우 정보통신망법에 의거 해당업체에 1,000만원 이하의 과태료를 부과하고 있다. 반대로 의무대상자 외 기업이 인증 취득을 희망할 경우에는 자율적인 신청을 통한 인증심사가 가능하다[3,7].

3.2.2. 정보보안 관리실태 평가(국가・공공)

국가정보원에서 2007년부터 전자정부법, 국가정보보안기본지침 등에 의거 국가・공공기관을 대상으로 매년 평가를 수행하며 점수제를 적용하여 우수기관을 선정한다.

정보보안 관리실태 평가는 국가정보보안기본지침 등에 규정된 주요 보안 요구사항의 이행 여부, 수준을 평가하는데 초점을 둔다는 점에서 기무사 정보보호평가와 유사하다.

평가방법은 기관별 자체평가와 국가정보원 현지실사로 구분되며, 매년 갱신되는 평가지표를 기반으로 평가를 수행하는데 최종평가 결과는 평가지표 기반의 점수와 사이버위협 대응활동 결과를 동시에 반영하여 결정된다[8].

3.2.3. 정보보호 관리수준평가(軍)

2011년 제정된 ‘국방정보화법’ 및 ‘국방정보화업무훈령’에 의거 2014년부터 기무사에서 군단급 이상 부대・기관을 대상으로 평가를 수행하고 있다.

정보보호 관리수준평가는 취약점 분석・평가, 보안대책 검토, 보안측정 등 기존 보안지원활동이 정보시스템 위주로 취약점을 진단하던 방식에서 탈피하여 부대단위로 평가대상을 확대하였으며 지휘관 중심의 체계적인 정보보호활동 수행여부 진단에 중점을 두고 있다.

평가영역은 지휘관심도, 계획, 운영, 감시, 물리적 보호 5개로 분류되며 총 83개 통제항목 점검 결과를 합산하여 우수부대를 선정한다.

정보보호 관리수준평가는 향후 평가지표 및 평가제도를 지속 개선함으로써 국방분야 ISMS 표준으로서 발전을 도모하고 있다.

Ⅳ. 방산업체 보안수준 향상 위한 방안

IV장에서는 4.1.에서 보안측정, 보안감사, 보안사고 조사 등 방산보안업무훈령에 근거한 방산업체 보안수준 유지 위한 제도[9]를 살펴보고 4.2.에서 방산업체의 조직 전반적인 정보보호수준 제고를 위한 고려사항과 ISMS 인증제도 적용방안을 제시한다.

4.1. 방산업체 보안수준 유지 위한 제도

4.1.1. 보안측정

방산업체와 방산관련업체의 보안요건을 확인하기 위하여 기무사에서 방산업체 및 정보통신시설 등에 대해 보안측정을 실시한다.

방산업체가 최초 방산업체로 지정되거나 소재지 이전 등으로 새로운 보안대책이 요구되는 등의 경우 보안측정 대상이 되며 정보통신시스템의 경우에는 신·증설 또는 이전시, 내·외부 전산망을 연동하는 등의 경우에 보안측정을 실시하며 방산업체는 보안측정 결과에 따라 필요한 보안대책을 수립·시행한다.

4.1.2 보안감사

방산업체는 연 1회 기무사의 보안감사를 받으며 기무사는 필요한 경우에 방산업체에 대한 수시감사를 시행한다. 지역기무부대에서는 방산관련 업체 및 단체에 대해 격년 단위로 보안상태를 확인하는 보안점검을 시행하여 방산업체에 대한 보안수준을 관리한다.

방산업체에 대한 보안감사를 통해 계획·인원·문서·시설·정보통신 및 기업보안 측면에서 방산보안업무훈령 준수여부를 확인하며 특히, 기업보안 분야에서는 방산기술개발 관련 위탁연구 및 기술용역시 방산자료 유출방지 대책, 방산물자 및 기술 수출시 통제 절차, 상주 협력업체 및 외주 하도급 업체에 대한 보안관리 등 방산업체에 특화된 사항을 감사요소에 반영하고 있다.

보안감사 결과는 방위력개선사업 참여업체 선정시 평가에 반영되며 전년도 감사결과 우수업체로 선정될 경우에는 다음연도 보안감사 대상에서 제외될 수 있다.

4.1.3. 보안사고 조사

기무사는 방산보안업무훈령을 미준수한 보안위반사항과 비밀의 분실, 유출, 누설, 방산물자 분실 등의 사항 발생시 방산업체에 대한 보안사고 조사를 실시하며 보안사고가 발생한 방산업체 및 방산관련업체는 필요한 보안조치를 취해야 한다.

4.2. 방산업체 ISMS 적용방안

4.1.에서 방산업체 보안수준 유지 위한 제도 현황을 살펴본 결과 공통적으로 조직 전체적인 정보보호수준을 관리하는데는 한계가 있음을 알 수 있다.

보안측정은 방산업체 및 정보통신시설에 대한 보안요건 충족여부에 중점을 두고 있고 보안감사는 문서·인원·시설·전산보안 분야에 대해 방산보안업무훈령 이행 및 규정 위반실태 점검을 목적으로 한다. 보안사고 조사 역시 규정 위반사항에 대한 사실확인을 목적으로 하는 것이지 조직 전반의 보안수준을 관리하기 위한 보안지원활동은 아니다.

이와 달리 ISMS는 조직의 주요 정보자산을 보호하기 위해 정보보호 관리절차와 과정을 체계적으로 수립하여 지속적으로 관리, 운영하기 위한 종합적인 체계로 기존의 방산업체에 대한 보안지원활동이 단편적 대응, 일회성 관리라는 한계가 있었다면 ISMS는 조직·관리·운영·기술적 통제를 통해 체계적 대응, 지속적 관리, 균형적·전사적 보안을 통해 조직 정보보호 수준 향상 및 개선이 가능하다.

점차 증가하는 방산업체에 대한 해킹위협에 대비하고 사이버상에서의 방산기밀 유출 시도에 능동적으로 대응하기 위해 民·官·軍 공통적으로 활용하고 있는 ISMS 인증제도의 방산업체 적용방안을 모색해보고자 한다. 본 논문에서는 평가기법, 법·제도적 고려사항, 수행조직 측면에서 적용방안을 구체화한다.

4.2.1. 평가기법

방산업체에 대한 정보보호 수준 인증제도 적용을 위해 방산업체에 적합한 ISMS 기반 평가기법 연구가 필요하다.

본 논문에서는 완전히 새로운 평가기법을 개발하기보다는 기본적으로 방산업체가 민간기업이며 방산업체에서 운영하는 정보시스템이 민수·군수영역이 명확하게 분리되어 있지 않음을 감안하여 민간기업에 적용되고 있는 KISA ISMS 인증제도를 방산업체에 적용하는 방안을 제안한다.

KISA 평가지표(104개)를 방산업체에 동일하게 적용하므로 방산업체가 ISMS 인증을 받을 경우 민간 ISMS 인증을 받은 것과 동일한 효력을 발휘한다.

단, 방산업체는 무기체계 개발 및 방산기밀을 취급하기 때문에 일반 기업보다 더욱 엄격한 보안요건이 요구되므로 KISA 평가지표에 방산업체에 특화된 평가지표(+α)를 추가로 적용해야할 것이다. 방산업체 요건에 맞는 평가지표 개발을 위해서는 추가적인 연구가 필요하다.

〔표 3〕 방산업체 현황

분야	주요 방산업체	일반 방산업체
95개	59개	36개
화력(12)	한화테크윈 등 8개	칸워크홀딩 등 4개
탄약(8)	풍산 등 7개	고려화공
기동(15)	현대로템 등 8개	광림 등 7개
항공유도(17)	대한항공 등 8개	성진테크윈 9개
함정(11)	현대중공업 등 8개	두산엔진 등 3개
통신전자(16)	삼성탈레스 등 11개	현대제이콤 등 5개
화생방(3)	삼공물산 등 3개	·
기타(13)	은성사 등 6개	대원강업 등 7개

4.2.2. 법 · 제도

방산업체 ISMS 인증제도 적용을 위해서 우선 법 · 제도적으로 인증제도를 의무화하는 방안 검토가 필요하다.

방산업체 관련 보안지원은 방위사업법, 보안업무규정, 방산보안업무훈령을 근거로 이루어지고 있으며 4.1.2.에서 소개한 바와 같이 해당 법 · 규정을 근거로 기무사에서 방산업체에 대한 보안감사 업무를 수행하고 있다.

법률 개정을 통한 인증제도 적용 방안을 검토할 수도 있으나 방산보안업무훈령에 명시된 기무사의 보안감사 범위를 확대하여 보안감사시 전산분야에 정보보호수준 평가기법을 적용하여 방산업체 정보보호수준을 진단하거나 방산보안업무훈령 개정을 통해 ISMS 인증제도 시행을 구체화하여 반영하는 방안이 합리적인 것으로 판단된다.

또한, 방산업체가 ISMS 인증제도에 적극적으로 참여토록 하기 위해 방사청에서 각종 사업공고시 입찰자격 요건으로 정보보호수준 인증을 의무사항으로 포함하거나 입찰업체 평가시 정보보호 수준 인증업체에 가점을 적용하는 등 인증제도 활성화를 위한 제도를 방산보안업무훈령에 포함할 수 있다.

4.2.3. 수행조직

평가팀 구성은 국방부 인력 또는 KISA 등 민간인력이 방산업체 평가를 전담하거나 국방부 · 민간인력이 T/F를 구성하여 공동 수행하는 방안을 검토할 수 있다. 그러나 방산업체가 국방 주요 무기체계를 연구 · 개발하고 엄격한 보안요건이 적용되는 점을 고려할 때 민간인력만으로 평가팀을 구성하는 것은 바람직하지 않으며 국방부 인력이 전담하거나 국방 · 민간 인력이 함께 참여하는 방안이 타당하다고 판단된다.

군내 평가 수행조직으로는 평가의 공정성 · 객관성을 보장할 수 있는 독립성, 평가자료에 대한 보안유지 능력, 방위산업 및 평가 업무에 대한 전문성, 기존 업무와의 연계성 등을 고려시 기무사에서 방산업체 정보보호 평가를 수행하는 것이 가장 적합하며 특히, 기무사의 방산업체에 대한 보안지원활동과 軍 및 軍 관련 기관 대상으로 시행하는 정보보호 관리수준평가 업무 노하우를 방산업체 ISMS 평가시 적용한다면 긍정적인 효과가 클 것으로 기대된다.

4.2.1.에서 논한 바와 같이 KISA ISMS 제도를 방산업체에 도입하기 위해서는 인증품질이 전제되어야 하는데 군 자체 인력만으로 인증품질 보장에 한계가 있으므로 시범운영 기간(최소 2년 이상)에는 KISA 팀장급 인력이 방산업체 ISMS 인증평가팀에 참여하여 인증품질을 보장하고 팀장을 제외한 기타 인력은 ISMS 인증심사원 자격을 갖춘 기무사 인력으로 구성하되 시범기간 종료 후에는 KISA 팀원급 인력이 방산업체 평가팀에 지속 참여하여 인증품질 보장 및 KISA ISMS 제도 정착을 지원한다.

평가팀 규모는 일반 방산업체를 제외한 주요 방산업체(59개)만을 평가대상으로 하고 ISMS 인증 유효기간을 KISA ISMS와 동일하게 3년으로 적용할 경우 1개 팀(3~4명 편성) 편성으로 운영이 가능하다.

Ⅴ. 결 론

지금까지 ISMS 인증제도 소개 및 적용 효과, 국내외 ISMS 인증제도 적용현황 분석을 통해 방산업체에 적합한 ISMS 인증제도 적용방안을 제안하였다.

방산기밀 유출을 목적으로 방산업체에 대한 제 3국발 사이버 공격이 끊임없이 발생하고 있는 시점에서 이에 대한 대응으로 ISMS 인증제도 도입이 최적의 방안으로 평가된다.

본 논문에서 제안한 방산업체 ISMS 적용방안은 KISA ISMS 인증제도라는 큰 틀에서 운영되기 때문에 방산업체가 기무사 ISMS 인증을 받을 경우 민수부문까지 인증효력을 인정받을 수 있어 대외 신인도를 개선하는데 큰 도움이 될 것이다. 또한, 기무사의 평가인력 지원을 통해 민간 ISMS와 달리 인증심사 비용이 소요되지 않으며 무엇보다도 ISMS 인증제도를 통해 조직의 정보보호 수준을 체계적으로 관리할 수 있다는 점에서 긍정적인 효과가 예상된다.

방산업체는 ISMS 인증제도 적용 초기 신규업무 수행에 따른 부담을 호소할 수도 있으나 인증제도 도입에 따른 긍정적인 효과를 고려한다면 방산업체 스스로도 인증제도가 조속한 시일내에 도입될 수 있도록 적극 노력해야 할 것이다.

참 고 문 헌

[1] 동아일보, “이란, 한국 항공-방산업체 2년간 해킹”, 2014.4.

[2] 아시아경제, “ADD 해킹범행자 결국 못 잡았다”, 2014.5.

[3] http://isms.kisa.or.kr

[4] 장상수, “*정보보호 관리체계 구축 및 활용*”, 생능출판사, pp,31-45, 2013.

[5] KIDA, “국방정보보호 표준평가체계 연구 - 정보보호 기관평가체계 구축을 중심으로”, pp.33-38, 2012.

[6] 나관식, “정보보호 관리체계(ISMS)의 국제표준과 국내표준 비교”, 과학과 문화 제8권 제1호, pp. 23-36, 2011.

[7] 한국정보보호진흥원, “정보보호 관리체계 인증제도 소개, p.25. 2008.

[8] 국가정보원, “정보보안 관리실태 평가 해설”, 2015

[9] 국방부, “방위산업보안업무훈령”, pp.96-105, 2015.

〈저 자 소 개〉

이 재 각 (Jai-Kag, Lee)
정회원

1995년 2월 : 광주대학교 경영학과 졸업
2011년 8월 : 수원대학교 경영학과 석사
2014년 3월～현재 : 광운대학교 방위사업학과 박사과정

관심분야 : 방산보안, 정보보호정책, 사이버보안