韓國IT서비스學會誌
第12卷 第4號
2013年 12月, pp.77-90
http://dx.doi.org/10.9716/KITS.2013.12.4.077

국방조직의 정보보호 평가 방법론 개발*

조성림** · 최인수*** · 박지훈*** · 신우창****

Development of the Information Security Methodology for Defense Organization

Sung Rim Cho** · In Soo Choi*** · Ji Hoon Park*** · Woo Chang Shin****

■ Abstract ■

As Cyber threats are rising, the scope of information Security (IS) is extending from technical protection of a single information system to organizational comprehensive IS capability. The ministry of National Defense (MND) has established the IS evaluation for defense organization in 'the Directive for Defense Informatization Affairs.' However, no information about an evaluation method, process and organization is provided.

We surveyed information security management system (ISMS) and related best practices in public sector and other countries, and analysed the military information security affairs. Thus, this paper recommends the IS evaluation method and process. The trial IS evaluation is in progress this year and the MND will expand this IS evaluation to the entire organization.

Keyword : Defense Informatization, Defense Information System, Defense Information Security, Information Security Management System(ISMS), Evaluation Methodology, Information Security Evaluation Model

논문투고일 : 2013년 07월 26일 논문수정완료일 : 2013년 10월 25일 논문게재확정일 : 2013년 11월 01일
* 본 논문은 한국국방연구원이 2012년에 수행한 국방정보보호 표준평가체계 연구를 기반으로 하여 작성되었음.
** 한국국방연구원 국방획득연구센터 선임연구원
*** 한국국방연구원 국방획득연구센터 연구위원
**** 서경대학교 컴퓨터과학과 조교수, 교신저자

1. 서 론

정보화 추진 고도화에 따라 발생한 다양한 정보보호 문제점을 해결하고, 나날이 지능화·악성화되는 사이버위협에 체계적으로 대응하기 위해 조직의 종합적인 정보보호 관리 능력의 중요성이 점점 증대하고 있다. 이에 따라 정부, 민간 및 미국을 비롯한 선진국에서는 정보보호 관리체계(ISMS : Information Security Management System) 인증제도 도입 및 국제표준 ISO 27000 시리즈 제정 등을 통해 조직의 전반적인 정보보호 관리 업무를 체계화하기 위한 노력을 강화하고 있다[5, 8, 9, 10, 12, 14]. 국방부는 국방 정보보호 발전을 위하여 지속적으로 노력하였으나, 주로 정보시스템의 보호 및 기술적 보호수단을 구축하는 것을 중점으로 추진하여서 조직 전반의 체계적이고, 종합적인 정보보호 관리 능력의 발전은 미흡한 실정이다. 평가 측면에서도 보호대책의 검토, 취약점 분석 및 평가, 보안감사 등 다양한 정보보호 평가업무를 수행 중이지만, 대부분 정보시스템을 중심으로 점검, 평가하는 것으로 조직의 정보보호 관리 업무를 위한 제반 요소들을 포괄하지는 않는다[4].

현재 국방부는 국방 조직의 정보보호 관리 업무의 실태를 점검, 평가하기 위해 국방정보화 업무훈령에 '국방 정보보호 기관평가' 업무를 규정하고 있다[2]. 하지만, 구체적인 평가 업무 절차, 평가기준 등은 명확히 정립되지 않아서 정상적으로 시행되지 못하고 있다.

이에 본 연구에서는 국방 조직의 정보보호 수준을 체계적으로 평가하기 위한 국방 정보보호 기관평가 방법론을 제시한다. 본 논문의 구성은 다음과 같다. 제 2장에서는 연구배경과 관련 연구에 대하여 설명하고, 제 3장에서는 국방부에서 수행하고 있는 정보보호 관리 현황에 대하여 기술한다. 제 4장에서는 국방 정보보호 기관평가 방법과 절차에 대하여 설명하고, 제 5장에서 결론에 대하여 살펴보고 마무리를 짓는다.

2. 관련 연구

2.1 전자정부 정보보호 관리체계(G-ISMS)

행정안전부는 급증하는 사이버 침해사고를 효과적으로 대응하기 위하여 기존의 단순 일회성, 단편적 보호대책 중심에서 관리적·기술적 보호대책을 종합한 정보보호 관리체계의 중요성을 인식하게 되었다. 행정안전부는 2009년 12월 ISO 27001 국제표준과 민간 정보보호 관리체계인증 제도(K-ISMS)를 기반으로 전자정부 서비스에 최적화된 전자정부 정보보호 관리체계(G-ISMS : Government Information Security Management System, 이하 G-ISMS) 인증 제도를 마련하였다[6, 11, 13].

G-ISMS 인증 제도는 조직의 정보보호 관리체계 구축/운영과 이의 평가를 위한 기준, 요구사항이 밀접하게 연관되어 있다. G-ISMS 인증심사기준은 이러한 목적에 모두 활용되는데, G-ISMS 인증을 받고자 하는 신청기관은 인증심사기준에 부합하는 조직의 정보보호 관리체계를 구축/운영하고, 인증기관은 인증심사기준에 따라 신청기관에 구축/운영되는 정보보호 관리체계를 평가한다.

G-ISMS 인증심사기준은 행정안전부 훈령 제178호에 제시되어 있는데, 크게 정보보호 관리체계 수명주기(정보보호 관리과정), 문서화 요구사항, 정보보호대책 통제사항으로 구성되며 각각의 내용은 <표 1>과 같다.

〈표 1〉 G-ISMS 인증심사기준

구 분	내용
정보보호 관리과정 (ISMS life cycle)	• ISMS 구축, 운영을 위한 표준 업무/절차 ※ 조직 경영관리 모델인 PDCA 개념 준용 • 위험기반관리를 ISMS의 핵심 업무로 정의
문서화 요구사항	• ISMS 구축, 운영 관련 문서화 • 문서, 기록의 관리/통제
정보보호 대책 통제사항	• ISMS 구축 시 적용되는 세부 통제사항 • 12개 통제분야, 44개 통제목적, 149개 통제항목

2.2 미연방정부 정보보호 관리법(FISMA)

FISMA(Federal Information Security Management Act)는 2002년에 미국에서 제정된 법령인 'E-Government Act, Title Ⅲ'의 별칭으로 일반적으로 미국의 정보보호 관련 제도로 인식된다. 미 정부기관은 FISMA에 따라 조직의 정보 및 정보시스템을 보호하기 위한 전사적 정보보호 프로그램을 개발, 구현한다.

또한, 이와 관련한 핵심 정보들을 문서화하여 작성, 관리해야 한다. FISMA 제도의 시행을 위해 미 표준기술국(NIST)은 미 정부기관/조직에서 전사적 정보보호 프로그램을 개발, 구현하고 관리하는 데 필요한 표준, 기준, 방법론 등을 개발, 지원한다[17].

FISMA는 ISO/IEC 27000 시리즈, G-ISMS과 같이 조직의 정보보호 관리체계(정보보호 프로그램)에 대한 평가와 직접적으로 연계한 제도는 아니다. 하지만 법 시행의 측면에서 미 정부기관/조직의 FISMA 요구사항 이행 성과 및 결과를 점검, 평가하는 업무를 규정하고 있다[15, 16].

FISMA 이행 점검/평가 체계는 미 정부기관/조직의 자체 성과 보고서와 독립적인 감사 기관/조직의 FISMA 감사보고서로 구분되며, 백악관의 예산관리국(OMB : Office of Management and Budget)이 이를 종합하여 평가한다.

미 정부기관/조직의 자체 성과 보고서는 'FISMA reporting Metric'을 기반으로 하는데, 미 국토안보부에서 운영하는 자동화 도구인 'CyberScope tool'을 이용하여 FISMA 요구사항의 이행 성과 및 결과 정보를 입력한다. FISMA 감사보고서도 'FISMA reporting Metric'을 중심으로 대상 조직의 주요 정보보호 프로그램 구축, 운영 성과를 점검한다.

FISMA 이행 점검/평가의 기반이 되는 'FISMA reporting Metric'은 국토안보부가 매년 발표하는데, 평가 대상, 항목/지표는 FISMA의 정보보호 프로그램 구축, 운영 요구사항 전반이 아니라 FISMA 시행 및 국가 차원의 정보보호 능력 발전과 관련한 핵심적인 정책 추진 목표 및 성과 영역을 중심으로 구성된다. 따라서 평가 대상, 항목/지표는 ISO/IEC 27000 시리즈, G-ISMS 등과 비교하여 간단한데 '12년도 'FISMA Reporting Metrics'에 정의된 평가 대상/항목은 다음과 같다[17].

- 시스템 목록(2)
- 자산 관리(6)
- 보안 설정/구성 관리(3)
- 취약점 관리(3)
- 식별 및 접근 관리(10)
- 데이터 보호(4)
- 경계의 보호(14)
- 침해사고 관리(3)
- 교육 및 훈련(3)
- 원격 접속(1)
- 네트워크 보안 프로토콜(2)

2.3 국가정보원의 정보보안 관리실태 평가

정보보안 관리실태 평가는 국가 보안정책의 이행실태 확인을 위해 국가·공공기관을 대상으로 국가정보원이 시행하는 평가 제도이다[1, 7]. 정보보안 관리실태 평가는 국가 정보보안지침 등에 규정된 주요 보안 요구사항의 이행 여부, 수준을 평가하는 데 초점을 둔다. 이러한 측면에서 이 평가 업무는 군의 보안감사 업무와 유사한 특성이 있다. 정보보안 관리실태 평가는 "기관별 자체평가", "현장실사", "결과분석 및 점수산출", "평가결과심의", "최종 평가 결과통보" 단계로 수행된다. 기관별 자체평가와 현장실사는 평가 목적으로 매년 갱신되는 평가 매뉴얼을 기반으로 수행되는데, 최종 평가 결과에는 매뉴얼 기반의 점수와 함께 사이버위협 대응과 관련한 조직의 실질적인 활동 결과를 추가적으로 고려한다. 평가 매뉴얼은 주로 '국가정보보안지침'의 요구사항을 기반으로 평가분야, 지표, 평가항목을 정의하고 있는데, 조직의 정보보호 관리를 위해 필요한 대부분의 분야/지표들은 포함하고 있지만, 평가항목은 국가·공공기관에서 공통적으로 수행하여야 하는 기본적인 점검요소를 중심으로 구성되어 있다.

2.4 정보보호 관리체계 비교

이들 평가 모델 및 방법론은 모두 조직의 정보보호 관리체계를 구축하고, 운영 및 평가를 수행하는데 적용 가능하지만 접근방법은 다소 차이가 있다. 평가 항목 측면에서 G-ISMS는 조직 차원의 정보보호 관리 업무와 관련한 제반 요소들을 모두 포함하는 반면, FISMA, 정보보안 관리실태 평가는 중요 정보보호 관리 요소를 중심으로 점검, 평가한다. 이는 G-ISMS의 평가가 조직의 정보보호 관리체계를 공적으로 증명하는 인증 제도와 연계되었기 때문으로 분석된다.

평가기준 측면에서 먼저, G-ISMS와 정보보안 관리실태 평가의 평가기준은 모두 군 적용성 측면에서 구체성은 미흡하다. 이는 각 모델/방법론이 다양한 환경, 특성의 조직들에 공통적으로 적용되기 때문으로 특정 조직의 구체적 정보보호 기준, 요구사항을 반영하기 어렵기 때문이다.

FISMA의 경우 평가기준은 주요 정보보호 관리요소의 이행 성과 및 결과를 점거하는 데 중점을 두고 있어 조직의 정보보호 관리체계 평가 측면에서는 활용이 제한된다.

정보보안 관리실태 평가의 경우, 평가항목에 대해 3~4개의 평가기준을 제시하여 현실적인 평가 수검 및 시행의 편의성을 제고할 수 있는 유용한 접근방법을 적용하고 있다.

평가방법 측면에서 G-ISMS와 정보보안 관리실태 평가는 평가자의 현장실사를 주요한 방법으로 적용하고 있으며, FISMA는 자체 및 감사 방식의 독립적인 점검을 사용한다. 평가 결과는 크게 인증과 등급/점수로 구분된다. 이상과 같은 내용을 정리하면 <표 2>와 같다.

국방 정보보호 기관평가의 평가항목/기준 개발 측면에서 3개 정보보호 관리체계 사례들은 모두 직접적으로 적용하는 것은 제한이 되지만 부분적으로 벤치마킹할 필요가 있다. 첫째, 조직 차원의 정보보호 평가를 처음 시행하는 측면에서 국방 정보보호 기관평가의 평가항목은 모든 정보보호 관리 업무 요소들을 종합적으로 고려할 필요가 있다. 하지만 실질적인 평가 수행의 효율성, 복잡성을 줄이기 위해 평가항목 및 평가요소들을 중요 요소를 중심으로 구성하는 것이 적합할 것으로 판단된다. 이러한 측면에서 G-ISMS와 정보보안 관리실태 평가의 평가항목들은 기관평가 평가항목 개발의 기반으로 활용할 필요가 있다.

둘째, 평가항목에 대한 평가기준 개발에 있어 정보보안 관리실태 평가의 접근방법은 국방 정보보호 기관평가의 경우에도 유용할 것으로 분석된다.

다만 평가기준의 내용 측면에서는 국방 정보보호 정책/제도 및 특성에 부합하도록 전반적으로 신규 작성 및 구체화가 필요하며, 군 업무 특성 및 기관평가의 목적상 평가 결과는 인증보다 점수/등급 방식이 적합할 것으로 분석된다.

3. 국방 정보보호 관리 현황

국방 정보보호는 국방 정보통신망에 대한 전자적 침해행위의 거부, 예방, 점검, 역추적 및 봉쇄 등

〈표 2〉 G-ISMS, FISMA, 정보보안 관리실태 평가 비교

구 분	평가항목/기준	평가 방법/결과
G-ISMS	• 평가항목은 모든 정보보호 관리 업무 요소를 포괄 • 군 적용성 측면에서 평가기준의 구체성은 미흡	• 방법 : 현장실사(인증심사기준 기반) • 결과 : 인증('Pass' or 'Non-Pass')
FISMA	• 평가항목 : 중요 요소 중심 • 이행 성과/결과 점검	• 방법 : 자체 점검/보고 + 독립 감사 • 결과 : 등급
정보보안 관리실태 평가	• 평가항목 : 중요 요소 평가 • 평가기준 : 3~4단계 선택기준 제시 • 군 적용성 측면에서 평가기준의 구체성은 미흡	• 방법 : 현장실사(매뉴얼 기반) + 활동점수 • 결과 : 점수

군의 작전능력을 높이기 위한 모든 활동을 말한다. 국방부는 국방 정보자원을 보호하기 위하여 국방 정보시스템 보호대책 수립 및 관리, 취약점 분석 및 평가, 주요기반체계 보호계획 수립, 개인 정보보호 등 다양한 정보보호 활동을 수행하고 있다[2-4].

정보시스템은 보호요구수준을 정의하여 보호요구수준에 따른 보호기준 및 보호통제항목이 만족되도록 보호통제 수단을 강구해야 한다. 정보시스템의 보호요구수준은 기밀성을 고려한 정보의 중요도와 정보시스템의 무결성・가용성을 고려한 시스템의 중요도에 따라 결정된다. 국방 정보시스템 보호대책은 보호요구수준에 따라 국방 정보시스템의 전 수명주기 단계에서 지속적으로 적용・관리되어야할 보호통제수단을 포함한다.

취약점 분석 및 평가는 정보시스템의 안전성・보안성을 약화 또는 훼손시키거나 전자적 침해행위에 악용될 수 있는 정보시스템 구성요소(네트워크, 시스템 등)의 허점을 분석하고 평가하는 업무를 말한다. 취약점 분석 및 평가는 위협 분석/평가, 취약성 분석/평가, 위험 분석/평가로 구분되는 관련 정보체계 보호 업무를 포괄한다.

주요 기반체계(정보시스템과 네트워크)는 침해사고 발생 시 미치는 영향도, 군사작전 및 국방운영에 대한 의존도 등을 고려하여 지정한다. 국방부는 주요 기반체계에 대하여 취약점 분석 및 평가를 실시하고, 그 결과를 반영한 보호대책을 종합하여 보호계획을 수립한다. 개인 정보보호는 2011년 9월 개인 정보보호법 시행에 따라 개인정보 노출진단체계 및 개인정보 암호화체계 구축하여 개인정보의 보호를 강화하는 것이다.

원칙적으로 보호대책, 취약점 분석 및 평가, 개인정보보호 등의 정보보호 업무는 단일 정보시스템 단위로 수립하여 관리한다. 또한 정보보호 대책을 종합한 정보 보호 계획을 수립하지만, 이는 조직의 전체 정보시스템을 포괄적으로 포함하는 것이 아니라 주요 기반체계로 한정되고 있다. 그러나 국방 업무를 효율적으로 수행하기 위해서 국방 정보시스템 간 상호운용성 요구가 증대됨에 따라, 이제는 개별 정보시스템을 중심으로 수행되었던 정보보호 업무는 조직 차원에서 관리해야 하는 필요성이 대두되었다.

4. 국방 정보보호 기관평가 방법

4.1 기관평가 수행 모델

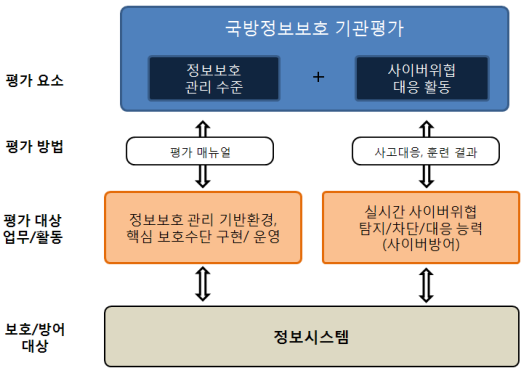
국방 정보보호 기관평가는 조직 측면에서의 정보보호 평가 업무로, 각 군 및 기관의 정보보호 관리 업무와 활동을 수행함에 있어서 적절성과 충분성에 대한 평가를 통해 조직의 정보보호 관리 능력 및 수준을 강화하고 향상시키는 것에 그 목적이 있다.

국방 정보보호 기관평가 요소는 평가중점과 평가방식에 따라 '정보보호 관리수준 평가'와 '사이버위협 대응 활동 평가'로 구분한다.

정보보호 관리수준 평가는 일반적인 정보보호 관리체계 모델/프레임워크에 대응하는 업무로 각 군 및 기관에서 수행하는 기본적・공통적인 정보보호 관리 업무/활동에 대해 점검, 평가한다. 평가대상 업무/활동에는 정보보호 제도/규정, 조직 등 기반 환경과 함께 조직 차원의 점검, 평가가 필요한 공통・핵심 보호통제항목들의 구현 및 운영 여부 등이 포함된다. 정보보호 관리 수준 평가는 평가 매뉴얼을 기반으로 수행한다.

사이버위협 대응 활동 평가는 사이버위협・공격에 대한 조직의 방어, 대응 능력을 평가한다. 정보보호 관리 수준 평가가 조직의 정보시스템 보호, 방어를 위한 일상적인 정보보호 관리 업무/활동에 초점을 둔다면 사이버위협 대응 활동 평가는 정보시스템에 대한 사이버위협・공격이 발생하였을 때 이에 대한 실질적인 방어 능력에 초점을 둔다. 기관평가는 사이버위협 대응 활동 평가를 위해 별도의 업무/활동을 수행하지 않으며, 국방 사이버안전 위기관리체계에 따른 각 군 및 기관의 사이버침해사고 탐지/차단/대응 활동 정보, 사이버전 관련 훈련 및 모의침투시험(penetration test) 결과 등을

활용한다. 이상과 같은 내용을 정리한 국방 정보보호 기관평가 수행 모델은 [그림 1]과 같다.



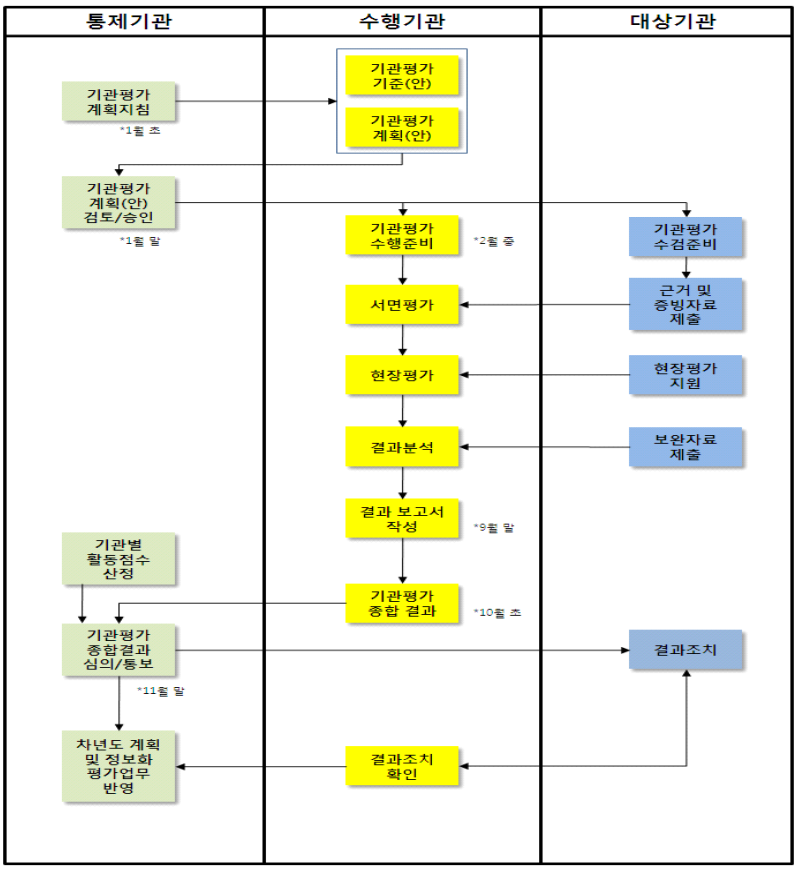
[그림 1] 국방 정보보호 기관평가 수행 모델

4.2 기관평가 업무 및 절차

국방 정보보호 기관평가 업무/절차는 통제기관, 수행기관, 대상기관의 구분에 따라서 매년 주기로 계획의 수립, 기관평가 수행 및 최종 점수 산정의 순기를 가지며 수행되는데 세부적인 절차는 [그림 2]와 같다.

4.2.1 기관평가계획 수립

통제기관은 국방정보화기본계획 등 국방 기획문서, 정보화환경 변화를 반영하여 '국방 정보보호 기관평가계획'(이하 '기관평가계획') 지침을 수행기관에 시달한다. '기관평가계획' 지침은 다음의 사항을 포함한다.



[그림 2] 기관평가 수행 절차도

- 전년도 기관평가 종합분석 결과
- 기관평가 중점사항
- 기관평가 대상기관
- 기관평가 계획 작성 시 고려사항
- 기관평가 일정

수행기관은 '기관평가계획' 지침에 따라 당해 연도 기관평가 계획 및 기준(안)을 작성하고 통제기관에 보고한다. 통제기관은 기관평가 계획 및 기준을 검토하고 국방 정보화책임관 실무협의회의 의결을 거쳐 매년 초에 수행기관과 대상기관에 시달한다.

4.2.2 기관평가 준비 및 수행

대상기관은 '기관평가기준', '세부기관평가 계획'에 따라 기관의 기관평가를 수검하기 위해 필요한 정보자산을 식별한다. 또한 대상기관은 '기관평가 기준'에 따라 평가항목별 관련근거 및 증빙자료를 포함한 자료를 준비하고 현장평가 시 제출하도록 한다.

수행기관은 '기관평가 계획'의 일정에 따라 대상기관에 대한 기관평가를 수행하며, 기관평가 기준에 명시된 항목의 요구수준을 만족하는지 여부에 대해 평가한다. 수행기관은 대상기관에서 제출한 관련근거와 증빙자료를 바탕으로 먼저 서면평가를 실시하고 현장평가가 필요한 항목을 식별하고 현장평가가 식별된 항목에 대해서 적절한 샘플링을 통해서 기준 적합성을 현장에서 검증한다.

4.2.3 기관평가 결과분석 및 산출

수행기관은 기관평가가 종료됨과 동시에 기관별 서면평가와 현장평가 결과를 기초로 결과를 분석하고 결과보고서를 작성한다. 기관평가 점수 산출은 다음의 사항에 따른다.

- 수행기관은 '기관평가 기준'을 바탕으로 분석·평가 결과를 작성한다.
- 기관평가 점수는 정보보호 관리 실태와 사이버 방호태세로 구분하여 산출한다.

4.2.4 기관평가 결과 심의

통제기관은 수행기관이 결과보고서를 기초로 평가내용의 적절성과 결과점수의 적합성을 확인하며 당해 연도 기관평가 종합결과와 기관의 사이버 방호태세 점수를 일정비율로 합산하여 최종 평가점수를 산정한다. 대상기관의 사이버 방호태세 점수는 다음 사항을 포함하며, 기관평가 대상 전 연도 10월부터 대상 연도 10월까지로 한정한다.

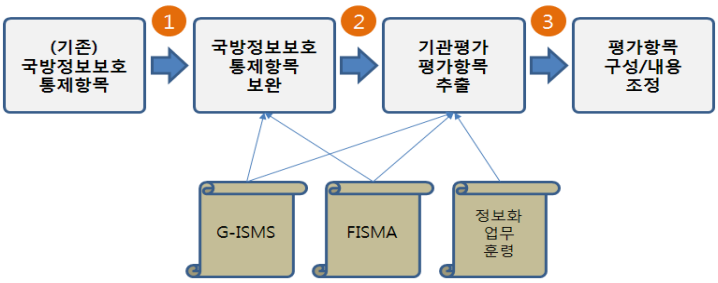
- 사이버침해사고 및 대응 건수
- 사이버 훈련 평가 점수
- 전산보안 사고 및 정보보호 우수사례

4.2.5 기관평가 최종결과 통보 및 조치

통제기관은 기관별 정보보호 관리실태 최종 평가 결과를 수행기관과 대상기관에 통보하며, 대상기관은 통보받은 평가 결과를 자체 정보보호 대책 등에 반영, 미흡점을 개선/보완하여 정보보안 수준을 제고한다. 통제기관은 평가 결과 공통적으로 드러난 보안 취약요소에 대해 국방 정보보호 정책에 반영하는 한편, 다음 년도 정보보호 기관평가 계획 수립에 반영하고 평가 시 이를 집중 점검하도록 한다.

4.3 평가항목 및 기준

실질적인 국방 조직의 정보보호 관리 업무 점검, 평가를 위해서는 국방 정책 및 기준, 요구사항에 기반을 둔 평가항목 및 기준이 필요하다. 이러한 측면에서 기관평가 평가항목은 현재 국방 정보시스템 구축, 운영에 공통적으로 적용되는 기준인 국방 정보보호통제항목을 국내외 모범사례를 반영하여 보완하고, 이에 대응하는 평가항목을 추출, 조정하는 방식으로 수행하였다. 국방 정보보호 기관평가의 평가항목 및 기준 개발을 위한 절차는 [그림 3]과 같다.



[그림 3] 평가항목 및 기준 개발 절차

기존의 국방 정보보호 관련 규정/제도들은 국내외 정보보호 관리체계 모범사례들에서 제시하는 대부분의 정보보호대책 통제사항들을 포함하고 있다. 하지만, 국방 정보보호 정책/제도들의 기준과 요구사항들을 구조화, 체계화하여 정리한 현 국방 정보시스템 보호통제항목들은 조직 차원의 종합적인 정보보호 관리를 위한 내용이 미흡하다. 기관평가를 위한 평가항목 및 기준들은 국방정보시스템 보호통제항목들과 독립적으로 작성될 수 있지만, 업무 요구사항과 평가와의 연계 및 국방 조직의 정보보호 업무 체계화를 위해 제반 정보보호 관리 업무 요소들을 포괄한 국방 정보시스템 보호통제 항목의 개선, 보완이 필요하다.

이와 같은 측면에서 조직 차원의 정보보호 관리 업무와 좀 더 밀접하게 관련되는 요소들을 '정보보호 정책 및 관리', '공통/기반 및 지원' 분야로 추가하여 국방 정보보호 통제항목을 보완하였으며, 이를 기반으로 조직 차원의 정보보호 관리 업무 점검, 평가 목적에 부합하는 평가 요소들을 추출하고 평가 요소들의 구성 및 내용을 조정하는 방식으로 작성하였다. 최종 개발된 평가항목은 <표 3>과 같다.

<표 3>의 국방 정보보호 기관평가 평가항목 분류와 함께 세부 평가항목, 평가기준 및 평가항목별 가중치는 연구 중간 결과를 기반으로 각 군 및 기관의 정보보호 전문가들의 검토 및 자문을 기반으로 개발되었다.

평가항목의 구성 및 내용, 평가기준의 적절성, 적용 타당성 등을 검토하기 위하여 국방부, 합참, 육 · 해 · 공군, 국방 전산정보원, 국군지휘통신사령부, 기타 정보보호 관련 국직부대 등과 2차례의 공식 회의와 수시 검토/자문을 통해 검토하였다. 그리고 AHP 방법론을 활용한 평가항목별 가중치 산정은 2012년 00월 00일에 국방부, 합참, 육 · 해 · 공군, 국군지휘통신사령부 등 관련기관의 정보보호 업무 실무자 8명을 대상으로 실시하였다. 이상과 같은 과정을 통해 개발된 국방 정보보호 기관평가 평가항목 및 평가항목별 가중치의 일부를 <표 4>에 보인다.

〈표 3〉 국방 정보보호 기관평가 평가항목 분류

기관평가 평가항목 분류	
1. 정보보호 정책/관리	1.1 정보보호 규정/계획
	1.2 정보시스템 보호대책
	1.3 정보보호 조직/인력
	1.4 위험관리
2. 정보시스템 보호	2.1 네트워크 보호
	2.2 식별/인증
	2.3 접근통제
	2.4 로그 및 백업
	2.5 기반 S/W 및 S/W 보호관리
	2.6 응용체계 보호
3. 공통/기반 및 지원	3.1 사이버위협 대응
	3.2 암호기술
	3.3 개발 및 유지보수 보안
	3.4 형상관리
	3.5 물리적/관리적 보호
	3.6 인적 보호
	3.7 개인정보 보호

〈표 4〉 정보보호 기관평가 평가항목과 가중치 일부

분야(분야별 가중치)		평가항목	가중치
1. 정보보호 정책/관리(40)	1.1 정보보호 규정/계획(15)	1.1.1 정보보호 규정 수립, 관리	30
		1.1.2 정보보호계획 수립, 시행	30
		1.1.3 정보시스템 비상계획 수립	20
		1.1.4 정보시스템 비상계획 교육/훈련 시행	20
	1.2 정보시스템 보호대책(35)	1.2.1 정보시스템 보호대책서 수립, 관리	60
		1.2.2 정보시스템 보호대책 이행점검	40
	1.3 정보보호 조직/인력(25)	1.3.1 정보보호 책임자/담당자 지정	10
		1.3.2 정보시스템 운영관리/정보보호 부서 임무분장	15
		1.3.3 정보보호 인력의 전문성	45
		1.3.4 정보보호 동향 파악	15
		1.3.5 정보보호·사이버위협 정보의 공지	15
	1.4. 위험관리(25)	1.4.1 정보시스템 현황 정보 관리	30
		1.4.2 H/W 정보자원 식별, 관리	15
		1.4.3 S/W 정보자원 식별, 관리	25
		1.4.4 정보보호 위험관리	30

각 평가항목에 대한 평가기준은 <표 5>의 예시와 같은 구성으로 작성된다. 예시의 '평가항목'은 기관평가 평가항목에 대한 구체적인 질의와 함께 평가 결과를 판단하는 기준을 포함하며, 수준/등급 개념의 기관평가 수행을 위해 해당 정보보호 관리 업무가 조직 차원에서 시행되는 수준을 4단계로 구분하여 정의한다.

'증빙 자료'와 '관련 규정'은 기관평가 준비 및 시행의 편의성을 위해 해당 평가항목의 점검 및 평가와 관련한 주요 정보들을 포함한다.

'평가 기준 및 해설'은 평가 수행을 위한 추가적인 정보로 '평가항목'에 포함된 4단계 구분을 중심으로 조직의 정보보호 업무가 각 단계를 충족하는 기준을 보다 구체적으로 기술한다.

4.4 기관평가 점수 산정

기관평가 점수는 '정보보호 관리수준 평가' 결과와 '사이버위협 대응활동 평가' 결과를 일정 비율로 합산한다.

'정보보호 관리수준 평가' 점수는 기관평가 평가항목 및 기준에 따른 각 항목별 평가 점수(1점~4점)를 기반으로 각 항목 및 분야별 가중치를 반영하여 점수를 산정한다. '정보보호 관리수준 평가'를 위한 기관평가 평가항목의 수준 구분은 <표 6>과 같다.

〈표 5〉 정보보호 기관평가 평가기준 구성 및 내용 예시

분류	1.2.1 정보시스템 보호대책서 수립, 관리
평가항목	정보시스템 보호대책서를 수립, 관리하는가? ① 보호대책서를 주기적으로 검토, 갱신 ② 모든 정보시스템에 대해 보호대책서 수립, 관리 ③ 일부 정보시스템에 대해 보호대책서 수립, 관리 ④ 수립, 관리되지 않음
증빙자료	◦ 정보시스템 목록 및 정보시스템 보호대책서 ◦ 정보시스템 형상변경 이력자료(수정/변경, 성능개량 등) ◦ 정보시스템 취약점 분석·평가 실시 결과(이전 2년) ◦ 보호대책서 검토 관련 입증자료(메일, 공문, 회의기록 등)
관련 규정	◦ 국방 정보화업무훈령 제261조(정보시스템 수명주기 보호대책 수립 및 관리)~제268조(운영 및 유지보수 단계) ◦ 군사보안업무훈령 제94조(정보통신보안 관련규정)
평가기준 및 해설	생략

〈표 6〉 기관평가 평가항목의 수준 구분

수준 1	수준 2	수준 3
1. 정보보호 정책/관리	1.1 정보보호 규정/계획	4개 항목
	1.2 정보시스템 보호대책	2개 항목
	1.3. 정보보호 조직/인력	5개 항목
	1.4. 자산관리/위험관리	4개 항목
2. 정보시스템 보호	2.1 네트워크 보호	7개 항목
	2.2 식별/인증	2개 항목
	2.3 접근통제	4개 항목
	2.4 로그 및 백업	5개 항목
	2.5 기반 S/W 보호	4개 항목
	2.6 응용체계 보호	6개 항목
3. 공통/기반 및 지원	3.1 사이버위협 대응	3개 항목
	3.2 암호기술	2개 항목
	3.3 개발 및 유지보수	3개 항목
	3.4 형상관리	2개 항목
	3.5 물리적/관리적 보호	3개 항목
	3.6 인적 보호	2개 항목
	3.7 개인정보 보호	4개 항목

기관평가 항목 중 수준 3에 대한 점수 산정은 다음 수식과 같다.

$$L3P_X = \sum_{l3i=1}^{N} P_{l3i} \times W_{l3i}$$

- $L3P_X$: 수준 3 분야 점수
- P_{l3i} : 수준 3 항목별 평가 점수
- W_{l3i} : 수준 3 항목별 가중치

기관평가 항목 중 수준 2에 대한 점수 산정은 아래의 수식과 같다.

$$L2P_X = \sum_{l2i=1}^{N} L3P_{l2i} \times W_{l2i}$$

- $L2P_X$: 수준 2 점수
- $L3P_{l2i}$: 수준 3 분야 점수
- W_{l2i} : 수준 2 분야별 가중치

기관평가 항목 중 수준 1에 대한 점수 산정은 다음 수식과 같다.

$$L1P_X = \sum_{l1i=1}^{N} L2P_{l1i} \times W_{l1i}$$

- $L1P_X$: 수준 1 점수
- $L2P_{l1i}$: 수준 2 분야 점수
- W_{l1i} : 수준 1 분야별 가중치

'정보보호 관리수준 평가' 점수는 모든 항목의 최대점수에 대한 대상기관의 평가점수를 백분율로 산정하며, 그 수식은 다음과 같다.

$$SMTP_X = \frac{\sum_{l1i}^{N}(\sum_{l2i}^{N}(\sum_{l3i=1}^{N} P_{l3i} \times W_{l3i}) \times W_{l2i}) \times W_{l1i}}{\sum_{l1i}^{N}(\sum_{l2i}^{N}(\sum_{l3i=1}^{N} MP_{l3i} \times W_{l3i}) \times W_{l2i}) \times W_{l1i}} \times 100$$

- $SMTP_X$: 정보보호 관리수준 평가 결과
- MP_{l3i} : 수준 3 항목 최대 점수

사이버위협 대응활동 평가 점수는 사이버 침해대응(IR)과 사이버 침해사고 대응 훈련 점수(CE)를 일정 비율로 합산하여 산정한다.

사이버 침해대응(IR) 점수는 대상기관의 총 침해사고 건수에 대한 대응 건수를 백분율로 산정한다. 대상기관의 총 침해사고 건수는 '정보작전방호태세규정' 제10조에 따라 국방 사이버지휘통제 센터에 보고하는 '정보체계 위협/손상 보고(제3호 서식)' 건수를 기준으로 하며[3], 침해 대응 건수는 국방 사이버지휘통제센터에서 위협 및 손상을 분석하여 사이버사령부에서 대상기관이 적절하게 조치를 취했다고 판단한 건수를 기준으로 하며 점수 산정은 아래의 수식과 같다.

$$IR = \frac{ID}{TI} \times 100$$

- IR : 사이버 침해대응 점수
- TI : 대상기관 총 침해사고 건수
- ID : 자체 침해탐지 및 대응 건수

사이버 침해사고 대응 훈련 점수(CE)는 기관평가 해당 연도(격년 평가 대상 기관의 경우 전년도

포함)에 대상기관에 대한 전군 차원의 사이버전 대응 훈련 결과를 반영하여 점수를 산정한다.

사이버위협 대응활동 평가 점수의 산정은 위의 계산식에 따라서 산정된 사이버 침해대응 점수와 사이버 침해사고 대응 훈련 점수를 일정 비율의 가중치를 곱하여 산정하며 세부적인 수식은 아래와 같다.

$$CDTP_X = IR \times \text{가중치} + CE \times \text{가중치}$$

- $CMTP_X$: 방호태세 최종평가 점수
- IR : 사이버 침해대응 점수
- CE : 사이버 훈련 점수

기관평가 최종 점수는 정보보호 관리수준 평가 점수와 사이버위협 대응활동 평가 점수를 가중치를 고려하여 산정하는데, 기관평가의 우선적인 목적이 각 군 및 기관의 정보보호 관리수준 제고에 있다는 측면에서 단기적으로 정보보호 관리수준 평가와 사이버위협 대응활동 평가의 가중치를 9 : 1 수준으로 시행하는 것이 적절하다고 판단된다. 기관평가 최종 점수 산정을 위한 산식은 다음과 같다.

$$\begin{aligned} \text{최종점수} &= SMTP \times 0.9 + CDTP \times 0.1 \\ &= (\text{관리실태 최종점수} \times 0.9) + \\ &\quad (\text{사이버방호태세 최종점 수} \times 0.1) \end{aligned}$$

대상기관의 기관평가 최종 결과는 기관평가 최종점수를 기반으로 <표 7>에 보이는 기준에 따라 등급을 판정한다.

〈표 7〉 국방 정보보호 기관평가 점수 및 등급

기관평가 결과	기관평가 최종점수
최우수	90점 이상
우수	80점~89점
보통	70점~79점
미흡	60점~69점
저조	60점 미만

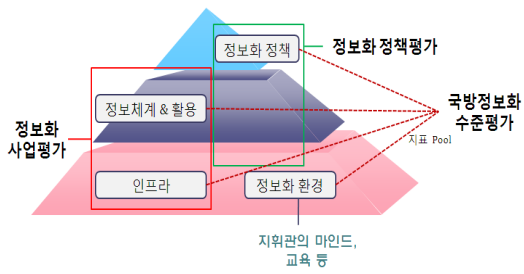
최우수 등급은 조직에서 정보보호 평가항목에 대한 활동이 수행되며 주기적으로 관리되는 수준을 나타낸다. 우수 등급은 정보보호 평가항목에 대한 활동들이 수행은 되지만 주기적인 점검은 이루어지지 않는 수준이다. 보통 등급은 정보보호 평가 항목에 대한 활동들이 부분적으로 수행되거나, 관리되는 수준이다. 미흡 등급은 정보보호 평가항목에 대한 활동들이 정의는 되어 있으나, 수행되지 않는 수준이다. 마지막으로 저조 등급은 정보보호 평가항목에 대한 활동들이 정의되어 있지 않는 수준을 의미한다.

4.5 기관평가 결과 활용

국방 정보보호 기관평가의 체계적인 시행 및 관리를 위해서는 국방정보화 평가 업무와의 연계 및 결과 활용 방안의 다양화가 필요하다.

국방정보화 평가 프레임워크는 [그림 4]에 보이는바와 같이 국방정보화 정책평가, 수준평가, 사업평가로 구분되는데, 국방정보보호 기관평가는 국방정보화 정책평가, 수준평가와 직·간접적으로 연관된다.

국방정보화 정책평가는 국방정보화 정책에 대한 기관별 정책 이행 여부를 평가하는 개념인데, 국방정보화 정책에 포함되는 정보보호 정책의 이행평가를 위해 국방 정보보호 기관평가 결과를 활용할 수 있다. 또한, 국방정보화 정책평가의 목적에 따라 기관평가 평가항목을 수정, 보완하는 방식으로 연계를 고려할 수도 있다.



[그림 4] 국방정보화 통합 평가프레임워크

국방정보화 수준평가는 국방 조직을 대상으로 정보화 수준을 평가하는 업무로 국방 정보보호 기관평가의 목적 및 결과와 직접적으로 대응된다. 따라서 국방정보화 수준평가 요소에 정보보호 분야가 포함될 경우, 이를 국방 정보보호 기관평가 결과로 대체하거나 활용하는 방식으로의 연계가 가능하다.

국방 정보보호 기관평가 업무가 국방 정보보호 능력 발전에 체계적으로 연계되기 위해서는 각 군 및 기관의 정보보호 계획 수립 시 기관평가 결과가 직접적으로 연계될 수 있도록 업무/절차의 개선이 필요하다.

5. 결 론

사이버위협의 증대에 따라 오늘날 정보보호는 정보시스템에 대한 기술적 보호, 방어 수단의 확충과 함께 조직의 종합적인 정보보호 관리 능력의 확보가 중요해지고 있으며 이를 점검, 평가하는 노력도 확대되고 있다. 이와 관련하여 현 국방정보화업무훈령에는 국방 조직의 정보보호 관리 업무 실태 점검 및 평가를 위한 목적으로 '국방 정보보호 기관평가' 업무를 규정하고 있지만, 구체적인 수행 체계, 평가 방법론 등은 정립되지 않은 실정이다.

이에 본 논문에서는 조직 차원의 정보보호 평가와 관련된 국내 · 외 모범사례와 군 정보보호 업무 현황에 대한 분석을 기반으로 국방 정보보호 기관평가 방법과 절차를 제시하였다.

국방 정보보호 기관평가 방법은 기관평가의 목적 및 범위, 업무/절차, 평가항목/기준 등을 포함한다. 기관평가는 각 군 및 기관의 정보보호 수준 제고를 목적으로 조직의 주요 정보보호 관리 업무와 핵심적이고 공통적인 정보시스템 보호 요소를 중심으로 평가한다. 업무/절차에서는 평가 계획 수립에서 결과 조치까지 일련의 업무/절차를 정의하였다. 평가항목/기준은 현 국방 정보보호 관련 기준 및 요구사항을 기반으로 국내 · 외 모범사례와 군 정보보호 업무 개선방향을 고려하여 구체성 있게 작성하였다.

국방부는 본 연구에서 제안하고 있는 국방 정보보호 기관평가 방법에 따라 국방 조직에 시범 적용하여 문제점을 사전에 식별하기 위한 '국방 정보보호 기관평가 시범적용 계획'을 수립하여 추진하고 있으며, 시범적용 결과를 반영하여 2014년에는 전군차원의 국방 정보보호 기관평가를 추진할 계획이다.

향후에는 국방 정보보호 기관평가를 지속적으로 수행하여 평가모델과 평가항목을 개선하고, 다년간 축적된 평가결과를 바탕으로 국방 정보보호 수준을 향상시키는 작업이 필요하다.

참 고 문 헌

[1] 국가사이버안전센터, 「정보보안 관리실태 평가 해설」, 2011.

[2] 국방부, 「국방부 훈령 제1304호 국방정보화업무훈령」, 2011.

[3] 국방부, 「국방부 훈령 제1525호 군사보안업무훈령」, 2013.

[4] 국방부, 「국방정보체계 취약점 분석 · 평가 실무지침」, 2011.

[5] 김기철, 김승주, "K-ISMS 기반의 한국형 스마트 그리드 정보보호 관리체계 평가 기준제안", 「정보보호학회논문지」, 제22권, 제6호(2012), pp.1375-1391.

[6] 김지숙, 임종인, "스마트폰 이용 환경에서 국가기관 정보보호 관리방안", 「정보보호학회논문지」, 제20권, 제6호(2010), pp.83-96.

[7] 김지숙, 이수연, 임종인, "민간기업 공공기관의 정보보호 관리체계 차이 비교", 「정보보호학회논문지」, 제20권, 제2호(2010), pp.117-129.

[8] 김지숙, 최명길, "국가기관의 정보보호 수준평가에 관한 연구", 「정보보호학회논문지」, 제18권, 제6호(2008), pp.6-10.

[9] 오남석, 한영순, 엄찬왕, 오경석, 이봉규, "정보

보호 수준평가 방법 개선에 관한 연구", 「한국전자거래학회지」, 제16권, 제2호(2011), pp. 159-169.

[10] 이동희, 여돈구, 염흥열, "국내·외 정보보호 수준 평가 체계 및 지표 동향", 「정보보호학회지」, 제20권, 제5호(2010), pp.74-85.

[11] 한국인터넷진흥원, 「전자정부 정보보호 관리체계(G-ISMS) 심사원 교육」, 2010.

[12] 한국인터넷진흥원, 「정보보호 관리체계(ISMS) 인증제도 소개」, 2010.

[13] 한근희, "전자정부 정보보호 관리체계(G-ISMS) 적용 정책", 「정보보호학회논문지」, 제19권, 제5호(2009), pp.119-130.

[14] 허순행, 이광우, 조혜숙, 정한재, 전웅렬, 원동호, 김승주, "정보보호 수준평가 적정화 방안 연구", 「정보처리학회논문지」, 제15-C권, 제3호(2008), pp.173-190.

[15] Jo, H. S., "Advanced Information Security Management Evaluation System", *KSII TRANSACTIONS AND INFORMATION SYSTEMS*, Vol.5, No.6(2011), pp.1192-1213.

[16] NIST, *Federal Information Security Management Act (FISMA) Implementation Project,* Title Ⅲ of the E-Government Act, 2002.

[17] NIST, *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Publication 800-53, Rev., Vol.4(2012).

[18] US Department of Homeland Security, *FY-2012 Chief Information Office Federal Information Security Management Act Reporting Metrics*, 2012.

◈ 저 자 소 개 ◈

조 성 림 (srcho@kida.re.kr)

현재 한국국방연구원에서 선임연구원으로 재직 중이며, 숙명여자대학교에서 컴퓨터과학과를 졸업하고, 서울대학교에서 전기 · 컴퓨터공학부에서 석사학위를 취득하였다. 주요 관심분야로 국방정보화 정책, 정보화 평가, 소프트웨어 프로세스 개선 등이며, 한국정보과학회, 경영정보학회, IT서비스 학회 등에 논문을 게재하였다. 주요 저서로는 "국방 정보화 수준평가 방법론"과 "정보시스템 품질평가 방법론"이 있다.

최 인 수 (ischoi@kida.re.kr)

현재 한국국방연구원에서 연구위원으로 재직 중이며, 고려대학교 수학과에서 석사 학위를 취득하였다. 주요 관심분야는 정보보증, C4ISR, 취약점 분석 등이며, 주요 저서로는 "통합정보보호 구조설계 및 종합발전계획 연구"(공저), "국방인증체계구축을 위한 세부개념연구"(공저) 등이 있다.

박 지 훈 (jihunprk@gmail.com)

현재 한국국방연구원 획득연구센터에서 연구위원으로 재직 중이며, 한국외국어대학교 경영정보학과에서 석사학위를 취득하였다. 주요 관심분야는 정보기술 정책, IT 거버넌스, 정보보호 등이다.

신 우 창 (wcshin@skuniv.ac.kr)

서울대학교에서 전산학 학사 · 석사를 하고 동 대학에서 컴퓨터공학 박사를 받았다. 현재 서경대학교 컴퓨터과학과 교수로 재직 중이며 주요 연구관심분야는 소프트웨어 평가, 설계패턴, 컴포넌트기반 개발, 소프트웨어 재구조화, 소프트웨어 아키텍처 등이다.