사이버안보연구, 2집 1호 2025 여름, 045-089

기관 특성을 반영한 사이버보안 실태평가 체계 연구

0201-045089

최명길 | 중앙대학교

논문접수일 2025년 6월 17일 | 논문심사일 2025년 6월 25일 | 게재확정일 2025년 6월 30일

논문 요약

사이버 침해가 증가함에 따라서 기관의 사이버 보안의 중요성이 강조되고 있고, 기관의 보안체계의 보안성을 보증하는 수단으로 사이버 실태평가의 중요성이 주목받고 있다. 본 연구는 국내 공공기관을 대상으로 시행되고 있는 사이버보안 실태평가 체계의 한계를 극복하고, 기관 특성과 보안환경을 반영할 수 있는 자율 기반의 사이버 평가체계를 제안한다. 기존 평가는 일률적 체크리스트 항목 중심으로 구성되어 기관별 보안역량이나 위험요인을 충분히 반영하지 못하는 문제가 있었다. 이에 본 연구는 전 수명주기(Plan-Do-Check-Act, PDCA) 기반의 사이버보안 평가모형을 설계하고, 국내외 보안 평가제도(FISMA, ISMS-P, FedRAMP 등)의 비교 분석을 통해 핵심 요소를 도출하였다. 동 연구는 위험평가와 피드백을 할 수 있는 지표 체계를 제시함으로써, 자율성과 책임성을 동시에 확보할 수 있는 실태평가 체계의 개선 방향을 제안한다.

주제어 사이버안보 실태평가, 위험평가, 정보보호 정책, 자율 기반 보안관리, PDCA 프레임워크

Ⅰ. 머리말

사이버 침해의 급격한 증가에도 불구하고, 사이버보안 실태평가는 기관의 보안성을 확보하는 데 중요한 역할을 수행해왔다. 특히, 이 제도는 우리나라의 특수성을 반영하며 발전해온 제도로 널리 인식되고 있다. 그러나 이러한 긍정적 성과에도 불구하고, 사이버보안 실태평가 제도는 평가자의 관점에서 일률적으로 통제항목을 적용함으로써 기관별 특수성을 충분히 반영하지 못하는 한계를 드러내고 있다. 이에 따라 표준화된 지표를 기반으로 한 평가 결과가 기관의 실제 보안 수준을 명확히 제시하기 어려운 경우가 발생한다. 평가지표는 모든 기관의 상황을 반영할 수 있도록 설계되어 있다. 특히 평가지표가 요구하는 보안 수준이 매우 높아 모든 기관이 보안 대책의 수준을 만족할 수 없는 상황이다. 그럼에도 불구하고 현재 평가체계는 모든 기관이 동일한 보안 대책을 요구할 수밖에 없는 상황이어서 비용 효과적이지 않을 수 있다. 또한, 사이버보안 실태평가에 앞서 기관이 자체 보안 수준을 평가하도록 항목을 제시하고 이를 기반으로 자체 평가를 수행하는 절차가 마련되어 있으나, 일부 기관은 제시된 통제항목에 기반하여 보안 정책을 수립하거나 적절히 대응하지 못해 특정 통제항목에 대해 대책을 수립하지 못하는 사례가 발생하고 있다.

각 기관은 자율적으로 보안 정책을 수립하고 이를 이행해야 할 책임이 있으나, 기관별 특수성을 충분히 반영하면서 정보보안 계획을 효과적으로 수립하기 위해 이를 지원할 수 있는 평가 방법론의 필요성이 제기된다. 이러한 평가 방법론은 기관의 특수성을 고려하여 통제항목을 명확히 제시하고, 각 기관의 고유한 보안 수준을 평가할 수

있어야 한다. 본 연구는 각 기관의 특수성을 반영한 자율적인 보안 활동을 보장할 수 있는 평가 방법론을 제안한다. 동 연구는 국내외 평가 방법론을 분석하고, 국내 실정과 기관의 고유한 특수성에 부합하는 평가 방법론을 제안하고자 한다.

Ⅱ. 사이버보안 실태평가 체계 분석

1. 사이버보안 실태평가 분석

1) 근거 및 평가 대상

사이버보안 실태평가는 「국가정보원법」 제4조 제1항 제4호에서 중앙행정기관 등 기관 대상 사이버공격 및 위협에 대한 예방 및 대응을 위하여 「사이버안보 업무규정」 제13조(사이버보안 실태평가)를 근거로 시행한다 (국가사이버보안센터, 2025).

2) 지표특징

사이버보안 실태평가는 「국가정보원법」 제4조 제1항 제4호에서 중앙행정기관 등 기관 대상 사이버공격 및 위협에 대한 예방 및 대응을 위하여 「사이버안보 업무규정」 제13조(사이버보안 실태평가)를 근거로 한다.

평가지표는 관리적 보안, 기술적 보안, 그리고 위기 대응 역량 등으로 구성되며, 각 분야는 배점은 관리보안 분야 39점, 기술적 보안 분야 37, 5점, 그리고 위기 대응 분야는 23.5점 등이다. 평가점수는 매년

평가지표의 개선에 따라 변경되고 있으며, 전년도에 발생한 보안 위협을 반영하여 추가되고, 중요도에 따라 평가점수의 배점이 달라질 수 있다.

〈표 1〉 평가 항목

분류	항목	질의	설명
관리적 보안 분야	18개	37개	동 분야의 지표는 책무, 인력, 인센티브, 조직, 예산, 정보보안감사, 정보보안교육, 보안성 검토, 용역사업보안, 소프트웨어 개발보안, 보안적합성 검증, 망 분리 정책, 정보자산관리, 보안 위규조치 및 예방대책 마련, 평가 결과에 따른 미비점 개선, 정보보안에 대한 기관장의 관심, 클라우드 정책, 기반 시설 보호 대책 등으로 구성된다.
기술적 보안 분야	13개	37개	동 분야의 지표는 망 분리 운영, 클라우드 보안관리(기술적), 정보보호 시스템 및 네트워크 장비 보안, 인터넷 전화 보안, 서버 보안, 용역사업 보안(기술적), 자료보안, PC 등 단말기 보안, 업무시스템 보안, 전자우편 보안, 비인가 IT 자원 관리, 융합보안, 원격근무시스템 보안 등으로 구성된다.
위기대응역량분야	10개	26개	동 분야의 지표는 자체 사이버위기대응매뉴얼 수립, 클라우드 보안관리(위기 대응), 현황관리, 접속기록 유지, 데이터 암호화, 사이버공격 대응훈련, 시스템 취약점 점검, 보안관제, 정보협력, 위협 동향 공유 등으로 구성된다.

평가지표는 표준화된 통제항목의 정의를 단순히 기반으로 삼는 것이 아니라, 각 기관의 보안환경에 따른 위험 관리를 통해 평가 항목을 도출해야만 기관의 특성을 반영한 평가 방법이 효과적으로 도입될 수 있다. 더불어 기관의 특수성을 반영한 평가 항목을 정량적으로 측정할 수 있는 표준화된 평가 도구의 개발이 필요하며, 더불어 새롭게 등장하는 취약점에 대응하기 위한 표준 적용 절차의 마련이 요구된다.

사이버보안 실태평가는 총 4단계로 구성되며, 각 단계는 다음과 같다. 첫째, 기관별 자체 평가 단계에서는 각급 기관이 국가정보원이 배포한 평가지표에 따라 자체 평가를 실시하고, 이에 대한 증빙자료를 제출한다. 둘째, 현장 실사 단계에서는 국가정보원이 관계 전문가로 구성된 평가반을 파견하여 각 기관을 방문하고, 자체 평가 결과를 검증한다. 셋째, 추가 증빙 및 이의 신청 단계에서는 각급 기관이 현장 실사 종료일로부터 7영업일 이내에 추가 증빙자료를 준비하여 국가정보원에 이의 신청을 할 수 있다. 마지막으로, 평가 결과 통보 단계에서는 국가정보원이 평가 결과를 해당 기관 및 관련 기관에 통보하며, 이를 정부 업무 평가에 반영할 수 있다.

2. 국내 보안 평가체계 분석

동 연구는 국내외 사이버보안 평가체계를 살펴본다. 동 연구에서 살펴보는 사이버보안 평가체계의 내용과 중요한 특징은 다음과 같다. 국내의 대표적인 사이버보안 평가체계는 ISMS-P, 사이버보안 실태평가 등이고, 국외는 FISMA, FedRAMP 등이다. 시행 주체별로 살펴보면, ISMS-P는 민간이 주도하는 형태이고, 사이버보안 실태 평가체계는 국가이다. 국외로 살펴보면 FISMA, FedRAMP의 평가주체는 국가기관이다. 둘째, 평가지표의 관점에서 살펴보면, ISMS-P, FISMA, FedRAMP는 개방형 평가지표로 기관의 특성에 적합한 평가지표를 선택할 수 있지만, 사이버보안 실태평가의 평가지표는 폐쇄형으로 피평가관이 선택할 수 없다.

1) 정보보호 및 개인정보보호 관리체계(ISMS-P, Information Security Management System & Personal Information Management System)

ISMS-P 인증제도는 신청 기관이 정보보호 및 개인정보보호를 위하여 수행하는 일련의 조치와 활동이 인증 기준에 부합함을 검증하는 제도로서, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조, 제47조의2 및 제47조의7과 그 하위 시행령 및 시행규칙, 그리고 「개인정보 보호법」 제32조의2 및 그 하위 시행령 등을 근거로 한다(과학기술정보통신부·개인정보보호위원회. 2023).

본 인증의 평가 대상은 다음과 같다. 첫째, 정보통신망 서비스 제공자(ISP), 둘째, 집적정보통신시설 사업자(IDC), 셋째, 전년도 매출액 또는 세입이 1,500억 원 이상이거나 정보통신 서비스 부문 전년도 매출액이 100억 원 이상, 또는 일일 평균 이용자 수가 100만 명 이상인 자로서 대통령령에서 정한 기준에 부합하는 자가 포함된다.

ISMS-P 인증 기준은 크게 세 가지 영역으로 구성된다. 첫째, '관리체계 수립 및 운영'(16개 항목) 영역은 전체 관리체계 운영의 중추 역할을 하며 전반적인 운영 라이프사이클을 포괄한다. 둘째, '보호 대책 요구사항'(64개 항목) 영역은 정책, 조직, 자산, 교육 등 관리적 보호 대책과 개발, 접근 통제, 운영 및 보안관리 등 물리적·기술적 보호 대책을 포함한 12개 분야로 구성된다. 셋째, '개인정보 처리단계별 요구사항'(21개 항목) 영역은 개인정보의 수집, 이용, 저장, 파기 등 전 생명 주기에 걸친 보호 조치를 포함한다.

인증 획득에 드는 전체 절차는 약 6개월 이상이며, 인증신청 전에는 위험 관리에 기반한 보호 체계가 구축되어 최소 2개월 이상 운영되어야 한다. 이러한 준비 기간은 객관적인 증가 확보와 제도적 완결성을 담보하며, 실효성 있는 정보보호 및 개인정보보호 수준의 제고

에 이바지한다.

2) 클라우드 보안 인증제도(CSAP, Cloud Security Assurance Program)

클라우드 보안 인증제도(CSAP)는 국가 및 공공기관에 안정성과 신뢰성이 검증된 클라우드 서비스를 제공하기 위한 목적으로 도입되었다. 본 제도는 객관적이고 공정한 보안 인증 체계를 운영함으로써 이용자의 보안 우려를 해소하고, 클라우드 서비스의 전반적인 경쟁력 제고를 도모하고자 마련되었다. CSAP는 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제5조에 근거한 '제1차 클라우드컴퓨팅 기본계획'에 따라 시행되고 있다(과학기술정보통신부. 2023).

본 인증제도의 평가 대상은 동일 법률 제20조에 따라 국가 및 공공기관 등의 업무 수행을 위해 클라우드 서비스를 제공하고자 하는 사업자로 규정된다. 평가 대상에는 해당 클라우드 서비스에 포함되거나 관련된 자산(시스템, 설비, 시설 등), 조직, 지원 서비스 등이 모두 포함된다.

CSAP의 인증 기준은 클라우드 서비스 유형별로 세분되어 있으며, 크게 네 가지 유형으로 구성된다. 첫째, IaaS 인증은 관리적·기술적 보호 조치와 국가기관 전용 추가 보호 조치를 포함하여 총 14개 분야, 116개 통제항목으로 구성된다. 둘째, SaaS 표준등급 인증은 IaaS 위에 구축된 서비스로, 통제항목 수가 약 31% 축소되어 총 13개 분야, 79개 항목으로 구성된다. 이 등급은 서비스 특성과 운영 환경을 고려하여 예비 점검 단계에서 인증 범위와 항목이 일부 조정될 수 있다. 셋째, SaaS 간편 등급 인증은 IaaS 기반 서비스로, 통제항목 수가 약 73% 줄어든 총 11개 분야, 31개 항목으로 구성된다. 해당 등급 역시 예비 점검을 통해 인증 범위와 항목 조정이 가능하다. 넷째, DaaS 인

증은 관리적·물리적·기술적 보호 조치와 국가기관 전용 추가 보호 조치를 포함하여 총 14개 분야, 110개 통제항목으로 구성된다.

클라우드 보안 인증 절차는 시스템 및 서비스 구축 완료 후 신청 접수를 시작하며, 신청일부터 인증서 발급까지 평균 약 2.5개월에서 5개월이 소요된다. 이를 통해 공공 부문의 클라우드 서비스 이용 시 보안 수준의 신뢰성을 확보하고, 클라우드 산업 전반의 품질 향상에 이바지할 수 있다.

3) 주요정보통신기반시설 이행점검

주요정보통신기반시설 이행점검은 전자적 침해행위에 대비하여 해당 시설의 보호 대책을 수립하고 시행함으로써, 시설의 안정적인 운영을 보장하고 궁극적으로 국가 안전과 국민 생활의 안정을 도모하는 것을 목적으로 한다. 본 점검은 「정보통신기반 보호법」에 근거하여 수행된다.

이행점검의 대상은 크게 두 가지로 구분된다. 첫째, 정보통신기반시설은 국가안전보장, 행정, 국방, 치안, 금융, 통신, 운송, 에너지 등 핵심 업무와 관련된 전자적 제어·관리시스템 및 정보통신망을 포함한다. 둘째, 주요 정보통신 기반 시설은 이들 기반 시설 중 전자적 침해행위로부터의 보호가 특히 필요하다고 인정되어 법령에 따라 지정된 시설을 의미한다.

- 실제 이행점검 절차는 다음과 같은 단계로 구성되며, 각 단계는 실효적인 보호 체계 수립과 실행에 중요한 역할을 한다.
- 주요 정보통신 기반 시설 보호 계획의 수립 및 시행
- 보호 대책 수립과 침해사고 예방 및 복구를 위한 체계 정비
- 보호 조치 명령 또는 권고의 이행을 위한 기술적 지원 요청

- 취약점 분석 및 평가 수행, 전담반 구성
- 보호 조치 이행을 위한 명령 또는 권고 실행
- 침해사고 발생 시 관련 기관에 대한 신속한 통지
- 「정보통신기반 보호법」에 명시된 바에 따른 복구 및 보호 조치 수행
- 기타 관련 법령에 따라 정해진 보호 업무의 수행

과학기술정보통신부와 국가정보원 등 관계기관은 관리기관이 수립한 보호 대책의 이행 여부를 직접 점검할 권한을 가지며, 이를 통해 국가 주요 기반 시설의 사이버보안 수준을 지속해서 유지·강화하고 있다.

3. 국외 보안 평가체계 분석

1) 미국

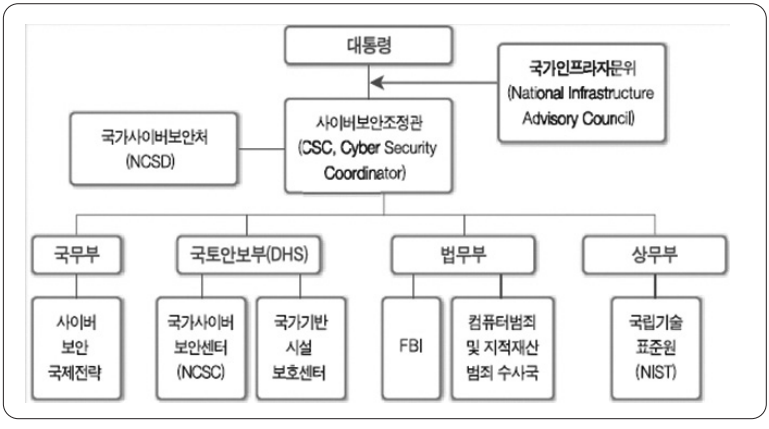
(1) 미 연방정부의 사이버보안 체계

미국 연방정부의 사이버보안 체계는 중앙집중적인 권한 구조를 기반으로 구성되어 있으며, 모든 사이버보안 관련 권한과 책임은 국토안보부(Department of Homeland Security, DHS)에 집중되어 있다. 특히, 대통령 직속 행정관리 예산처(Office of Management and Budget, OMB)는 연방정부 전자정부 운영에 대한 총괄 책임을 지니며, 사이버보안 실무를 담당하는 연방 정보보안 사고센터(Federal Computer Incident Response Center)는 OMB 산하에 운영되고 있다.

미국의 사이버보안 정책은 단일 기관의 지시에 의존하기보다는 다

양한 관계기관 간 수평적 협업 체계를 통해 실행된다. 이러한 협업 체계는 각 기관의 역할과 기능을 명확히 구분하는 동시에 상호 조율을 가능하게 하여, 사이버 위협에 대해 유연하고 효과적인 대응을 도모한다. 관련 조직 간의 정보 공유 및 공동 대응을 강조하여 전반적인 거버넌스의 실효성을 높이고 있다. 미국의 사이버보안 거버넌스 구조는 〈그림 1〉과 같다(NIST 2023, The White house 2016).

〈그림 1〉 연방정부의 사이버보안 체계



(2) FISMA(Federal Information Security Modernization Act)[1)]

미국의 FISMA(Federal Information Security Modernization Act)는 9·11 테러 이후 연방정부 기관의 정보시스템 보호를 목적으로 제정된 법적 장치이다. 동 법은 모든 연방정부 기관이 매년 최소 한 차례 보안

1) PISMA는 2002년에 제정될 때는 Federal Information Security Management Act이었지만, 2024년 Federal Information Security Modernization Act로 명칭이 변경됨.

프로그램의 유효성과 개선계획을 행정관리 예산처(Office of Management and Budget, OMB) 및 미국 의회에 보고하도록 규정하고 있다. FISMA는 정부 정보와 운영 보호를 위한 보안 프레임워크를 제시하며, 연방 차원의 보안 표준 및 가이드라인의 법적 근거로 작용한다(United States Congress. 2014).

FISMA의 실행을 지원하기 위해 국립표준기술연구소(National Institute of Standards and Technology, NIST)는 정보 및 정보시스템의 민감도와 위험 수준에 따라 분류하기 위한 통일된 기준을 마련하고, 기관의 분류 작업을 지원하기 위해 각 분류 범주에 포함될 수 있는 정보 및 시스템 유형을 구체적으로 제시한다. 또한 각 분류 범주에 해당하는 정보 및 시스템에 적용될 최소한의 보안 요구사항을 규정하며, 이는 관리적, 운영적, 기술적 통제를 포함한다. FISMA 준수를 위한 핵심 요건에는 정보시스템 목록 작성, 위험 분류, 시스템 보안 계획 수립, 보안 통제의 구현, 위험평가, 그리고 인증 및 증명(authentication and certification) 절차가 포함된다.

〈표 2〉 FISMA의 규정 준수 요구사항

요구사항	설명
정보시스템 목록 작성 (Information systems Inventory)	기관은 규정을 준수하면서 모든 시스템의 인벤토리와 기관의 업무 간의 연결성을 파악해야 한다.
위험 분류 (Risk Classification	기관은 보안 및 위험 요구사항을 FIPS-199에 따라서 위험 평가를 수행해야 한다.
시스템 보안 프로세스 (System Security Path	각 기관은 규정을 준수하기 위해 보안 계획과 정기적으로 업데이트되는 프로세스를 개발해야 한다.
보안 통제 (Security Controls	NIST 800-53에 수록된 보안 통제를 기반으로 모든 기관은 규정을 준수하고 보안 통제를 구현해야 한다.

요구사항	설명
위험평가 (Risk Assessment	기관은 위험 관리 프레임워크(RMF)에 따라서 위험을 재평가해야 한다.
식별 및 인증 (Authentication and Certification	FISMA를 준수하기 위해 모든 기관은 최소 1년에 한 번 보안 검토를 수행해야 한다. 보안 검토를 기반으로 기관은 보완 조치하고, 관련 시스템을 관찰해야 한다.

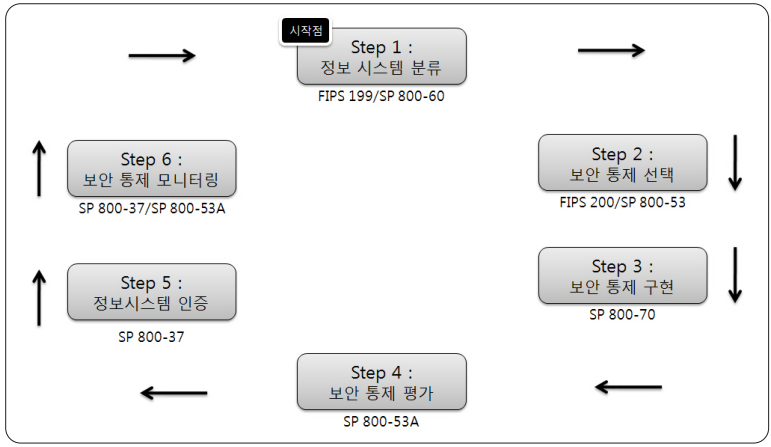
이러한 요건은 NIST에서 발간한 일련의 문서를 통해 구체화하며, 해당 문서는 미국 사이버보안 평가체계의 근간인 가이드라인으로 활용된다(〈표 3〉).

〈표 3〉 미국 사이버보안 가이드라인 문서

문서번호	설명
FIPS 199	연방정부의 정보와 정보시스템 보안에 대한 분류를 위한 표준
FIPS 200	연방정부의 정보와 정보시스템의 최소 보안 요구사항
NIST SP 800-30	정보기술 시스템을 위한 위험 관리 지침
NIST SP 800-37	연방 정보시스템 보안 허가를 위한 지침
NIST SP-800-29	NIST의 위함 관리체계(RMF)에 대한 지침
NIST SP-800 53A	연방 정보시스템의 보안 통제 평가 지침
NIST SP-800-59	정보시스템을 국가 보안 시스템으로 식별하기 위한 분류 지침

FISMA는 이러한 표준과 지침을 효과적으로 통합·운영하기 위해 위험관리체계(Risk Management Framework, RMF)를 도입한다. RMF는 보안 요구사항을 체계적으로 반영하는 주기적 관리 절차를 통해 각 기관의 정보시스템에 대해 지속적인 보안 수준 확보를 가능하게 한다. RMF의 절차적 흐름은 〈그림 2〉와 같다.

〈그림 2〉 위험 관리 체계 보안 생명 주기



FISMA의 RMF 체계는 본 연구가 제안하는 중요 프로세스에 반영된다. 반영된 프로세스는 위험분석과 위험분석에 정보시스템의 중요도 분류 절차이다.

(3) FedRAMP (Federal Risk and Authorization Management Program)

미국 FedRAMP(Federal Risk and Authorization Management Program)는 2011년 미국 연방정부가 클라우드 서비스 도입을 촉진하고 정보보안 수준을 강화하기 위해 수립한 통합 보안 인증 프레임워크다(GSA, 2024). 클라우드 서비스의 확산과 함께 보안 평가 및 승인 절차의 표준화 필요성이 대두되었으며, 중복된 보안 평가로 인한 비용 및 시간 낭비를 줄이기 위한 제도적 기반으로 마련되었다. 이 제도는 미국 대통령 행정명령 13571(2011년)에 따라 설립되었으며, NIST(National Institute of Standards and Technology)의 보안 통제 기준인 SP 800-53을 기반으로 개발된다.

FedRAMP는 13개 보안 통제 분야를 중심으로 세부 통제항목을 제시하며, 주요 통제 분야는 〈표 4〉와 같다.

〈표 4〉 FedRAMP의 보안 통제항목

영역	코드	설명
접근 통제	AC	권한 있는 사용자만 시스템과 데이터에 접근할 수 있도록 보장. 역할 기반 접근 제어(RBAC) 등을 서술
인식 및 훈련	AT	시스템 사용자나 관리자에게 보안 정책 및 절차를 훈련.
감사와 책임	AU	보안 이벤트를 기록하고 관찰하며 책임성을 보장. 로그 관리와 감사 준비
보안 평가 및 승인	CA	시스템 보안 평가 및 인증, 승인 절차
구성 관리	CM	시스템 구성 변경에 대한 관리 및 승인 절차
비상 계획	CP	비상시 시스템 복구와 업무 연속성을 보장
식별 및 인증	IA	시스템 사용자와 장치에 대한 인증 및 식별 절차
사고 대응	IR	보안 사고 발생 시 대응 계획과 절차
유지 보수	MA	시스템 유지 보수 절차와 보안관리
미디어 보호	MP	데이터 저장 매체의 보호 및 폐기 절차
물리적 보호	PE	시설과 시스템 하드웨어에 대한 물리적 접근 통제
시스템 및 통신 보호	SC	네트워크 보안, 암호화, 데이터 보호
시스템 및 정보 무결성	SI	보안 위협 탐지, 취약점 관리, 정보 무결성 보장

- 접근 통제(AC, Access Control): 사용자와 시스템에 대한 접근을 통제하여 무단 접근을 방지함
- 인식 및 훈련(AT, Awareness and Training): 사용자와 관리자에게 보안 정책과 절차에 대한 이해를 제고하고 교육을 제공함
- 감사 및 책임(AU, Audit and Accountability): 보안 이벤트 기록 및 모

니터링을 통해 책임성을 확보함

- 보안 평가 및 승인(CA, Security Assessment and Authorization): 시스템 보안 상태를 평가하고 운영 승인 여부를 결정함
- 구성 관리(CM, Configuration Management): 시스템 및 네트워크의 구성을 안전하게 관리함
- 비상 계획(CP, Contingency Planning): 비상 상황 발생 시 시스템 복구 및 업무 연속성 확보를 목적으로 함
- 식별 및 인증(IA, Identification and Authentication): 사용자와 시스템의 신원을 식별하고 인증함
- 사고 대응(IR, Incident Response): 보안 사고 발생 시 신속히 대응하여 피해를 최소화함
- 유지 보수(MA, Maintenance): 시스템 유지 보수 과정에서 보안을 지속해서 확보함

이러한 FedRAMP의 보안 통제항목은 미국 연방 기관이 클라우드 서비스를 도입할 때 통합적으로 적용하는 기준으로, 사이버보안 체계의 표준화와 신뢰성 확보에 이바지한다. 동 연구는 FedRAMP의 프로세스 중 위험평가와 중요도에 따른 시스템 분류에 반영하고 있다.

2) EU

EU는 사이버보안 강화를 위해 「네트워크 및 정보보안 지침(Network and Information Security Directive, 이하 NIS 지침)」을 제정하였으며, 이는 현재 「NIS2 지침」으로 개정되어 시행 중이다(European Parliament & Council. 2022). NIS2는 EU 전역을 대상으로 통일된 사이버보안 법제 체계를 제공하고 있으며, 증가하는 랜섬웨어 공격과 정보 유

출 등 다양한 사이버 위협에 능동적으로 대응하기 위한 제도적 기반을 마련하고자 하였다.

NIS2 지침은 2023년 1월 16일 발효되었으며, 각 EU 회원국은 2024년 10월 17일까지 이를 국내법으로 전환해야 한다. 동 지침은 유럽 사이버보안 기구(ENISA, European Union Agency for Cybersecurity)의 위협 환경 보고서를 기반으로, EU 역내 중요 기관의 사이버보안 수준을 높이는 데 그 목적이 있다.

NIS2 지침 제21조는 대상 기관이 '적절하고 비례적인 기술적 및 조직적 조치'를 통해 사이버 위험을 관리해야 함을 명시하고 있으며, 주요 요구사항은 다음과 같다.

- 위험 분석 및 정보보호 정책
- 철저한 사고 처리
- 비즈니스 연속성 및 위기관리
- 강력한 공급망 보안
- 광범위한 네트워크 보안
- 취약점 처리 및 공개
- 사이버보안 위기관리의 효과성을 평가하는 정책 및 절차
- 암호 및 암호화 사용
- 다단계 인증 사용

3) 영국

영국은 정부와 공공기관의 사이버보안 역량 강화를 목적으로 「Government Functional Standard GovS 007: Security」(이하 GovS 007)을 도입하여 운영하고 있으며, 이는 영국 내 모든 정부 부처와 공공기관이 준수해야 하는 기능 표준으로 자리 잡고 있다(Cabinet Office

Government Security Group. 2021). GovS 007은 「사이버보안 표준(Cyber Security Standard)」을 통해 구체화하며, 각 조직이 달성해야 할 보안 성과와 이를 검증하기 위한 절차를 명확히 규정한다.

이 표준의 핵심 요구사항은 「사이버 평가 프레임워크(Cyber Assessment Framework, CAF)」를 기반으로 하며, 주요 구성 항목은 다음과 같다.

① 보안 위험 관리: 조직의 거버넌스 체계, 위험평가 및 관리, 자산의 식별 및 보호, 공급망 보안을 포함한다.

② 사이버공격 방지: 서비스 보호를 위한 정책을 수립하고, 접근 제어 메커니즘을 적용하며, 데이터 보호 조치를 시행하고 시스템 보안을 강화한다. 네트워크와 시스템의 복원력을 확보하고, 관련 직원에 대한 정기적인 교육을 요구한다.

③ 사이버보안 이벤트 탐지: 보안 모니터링 체계를 구축하여 이상 행위를 탐지하고, 이를 통해 공격 징후를 조기에 식별한다.

④ 사이버보안 사고 영향 최소화: 사고 발생 시 신속히 대응하고 복구 계획을 수립하며, 사후 분석을 통해 보안 개선 사항을 도출한다.

영국의 사이버보안 정책은 국가 사이버보안센터(NCSC, National Cyber Security Centre)를 중심으로 추진되며, 정부 지침, 인증제도, 법률 및 규정, 산업별 권고사항 등을 통합하여 체계적인 보안 거버넌스를 실현한다. 이 정책은 국가 핵심 인프라의 보호, 기업 정보보안 강화, 개인 데이터 보호 등을 목표로 하며, 정부, 규제기관, 산업계 간의 협력을 바탕으로 마련된다.

〈표 5〉 영국 정보보안 가이드라인

가이드라인	적용 대상	내용	의무 여부
GovS 007	모든 정부 기관	공공기관 보안 기본 규정	의무
Cyber Security Strategy	정부 전체	2030년까지 사이버 회복력 강화	전략적 로드맵
CAF	중요 공공서비스 운영기관	보안 성숙도 자기진단 또는 감사	권고/평가 기반
MCSS	공공 IT 시스템 운영기관	최소 보안 기술 요건	의무
SPF	모든 공공기관	정보보호 정책 프레임워크	준수 필요
NCSC Cloud Security Principles	전체조직	NCSC Cloud Security Principles	권고

4) 독일

독일 정부는 연방 정보보안청(BSI, Bundesamt fur Sicherheit in der Informationstechnik)을 중심으로 정보보안 표준 지침을 수립하고 이를 체계적으로 운영한다. 이러한 지침은 공공 및 민간 부문의 정보보안 수준을 향상하기 위한 기반으로 기능한다. BSI는 정보보안 관리체계(Information Security Management System, ISMS)의 구축과 운영을 지원하기 위해 종합적인 프레임워크인 「IT-Grundschutz」를 개발한다. 이 체계는 기술적, 조직적, 인프라적, 인적 요소를 모두 포괄함으로써 ISO/IEC 27001 국제표준과의 높은 호환성을 확보하고 있다(National Office for Information Security (BSI). 2023).

IT-Grundschutz는 다음과 같은 주요 표준들로 구성된다.

BSI 표준 200-1은 정보보안 관리체계(Information Security Management System, ISMS)의 일반적인 요구사항을 정의하고, 조직이 효과적

인 보안관리 체계를 수립하고 운영하는 데 필요한 기본 지침을 제공한다.

BSI 표준 200-2는 조직의 정보보안 수준과 요구사항에 따라 정보보안 관리체계(ISMS)를 구축할 수 있도록 세 가지 접근 방식을 제시하며, 이를 통해 조직 맞춤형 보안 구현을 가능하게 한다. BSI 표준 200-2는 조직의 정보보안 수준과 요구사항에 따라 정보보안 관리체계(ISMS)를 구축할 수 있도록 다음의 세 가지 접근 방식을 제시하며, 이를 통해 조직 맞춤형 보안 구현을 가능하게 한다. 기본 보호(Basisschutz, Basic Protection)는 비교적 일반적인 보안 요구사항을 충족시키기 위한 접근 방식으로, 표준화된 보안 조치를 통해 대부분 조직이 쉽게 도입할 수 있도록 구성되어 있다. 중소규모 조직이나 정보보안이 비교적 단순한 환경에 적합하다. 표준 보호(Standardschutz, Standard Protection)는 보다 구체적이고 체계적인 위험 분석을 기반으로 보안 조치를 수립하는 방식으로, 조직의 운영 환경과 정보자산의 특성에 맞춘 맞춤형 보안 구현이 가능하다. 보안 수준의 균형을 중시하는 조직에 적합하다. 코어 보호(Kernschutz, Core Protection)는 핵심 자산에 대해 높은 수준의 보안 통제를 적용하는 접근 방식으로, 고도의 위험 분석과 맞춤형 보안 설계가 요구된다. 국가 기반 시설이나 고도화된 사이버 위협에 노출된 조직에 적합하다.

BSI 표준 200-3은 정보보안 위험에 대한 분석 및 평가 절차를 포함하며, 조직이 위험 기반의 보안 조치를 체계적으로 수행할 수 있도록 지원한다.

BSI 표준 100-4는 비즈니스 연속성 관리(Business Continuity Management, BCM)를 다루며, 재난이나 시스템 장애 등 비상 상황에서도 조직의 핵심 업무 기능을 지속할 수 있도록 계획을 수립하는 것을 주

요 목적으로 한다.

독일의 정보보안 체계는 표준화된 정보보안 관리체계의 운영을 통해 각 공공기관과 민간 기업이 정보보안 위험에 능동적으로 대응할 수 있도록 지원하며, 국제적 기준에 부합하는 수준 높은 보안 거버넌스를 실현한다.

〈표 6〉 독일 정보보안 가이드라인

가이드라인	적용 대상	내용	의무 여부
IT-Grundschutz	모든 조직	보안 프레임워크 (ISO 27001 기반)	선택적
C5 (Cloud Computing Compliance Criteria Catalogue)	클라우드 서비스 제공자	클라우드 보안 인증 기준	반의무
Mindeststandards (BSI 최소보안 기준)	연방 기관	정부 기관 보안 최소 기준	의무
DIN SPEC 27076 (중소기업 사이버 위험 체크)	KMU	중소기업을 위한 보안 체크	권고

5) 일본

(1) 정보보안 표준 지침

일본 정부는 정보보안 표준 지침의 수립과 보안성 평가체계의 구축을 통해 국가 차원의 사이버 위협에 대응한다. 이를 위해 일본 정보기술 보안 평가·인증 제도(Japan Information Technology Security Evaluation and Certification Scheme, JISEC)를 운영하며, 이를 통해 IT 제품의

보안성을 평가하고 인증하는 제도를 시행하고 있다. 이러한 정보보안 지침은 국가 법률, 정부 기관의 기술 가이드라인, 산업별 기준, 그리고 국제표준과의 연계를 기반으로 구성된다.

일본의 주요 정보보안 관련 법·제도 및 정책은 다음과 같다.

일본의 「사이버보안 기본법(Basic Act on Cybersecurity)」은 2015년에 시행되었으며, 국가 사이버보안 정책의 기본 원칙과 함께 정부, 민간 부문, 시민의 책임을 명확히 규정한다. 이 법은 사이버보안 전략의 수립과 사이버보안 전략 본부의 설립 등 정책 추진 체계를 제도화함으로써, 국가 차원의 사이버보안 거버넌스를 체계적으로 정립한다(Government of Japan. 2014).

〈표 7〉 JISEC 관련 지침 분류

분야	지침서	
일본 IT 보안 평가 및 인증제도	CCS-01	IT 보안 평가 및 인증제도의 기본 지침
인증신청	CCM-02	IT 보안 인증 신청 절차 등에 관한 지침
평가 기관	CCM-03	IT 보안 평가 기관 승인 신청 절차 등에 관한 지침
인증기관 운영	CCM-01	IT 보안 인증기관 조직 및 업무 운영에 관한 지침
	CCM-01-A	IT 보안 인증 업무 취급 순서
	CCM-01-B	IT 보안 평가 기관 승인 업무 취급 순서
	CCM-01-C	IT 보안 인증기관 인원 관리 순서

일본 정부는 2021년에 최신 「국가 사이버보안 전략(Cybersecurity Strategy)」을 발표하였으며, 이를 통해 향후 3년간의 사이버보안 정책 방향을 다음과 같이 제시한다.

- 자유롭고 공정하며 안전한 사이버 공간 실현

- 디지털 사회에서 국민이 안심하고 생활할 수 있는 환경 조성
- 국제 협력과 연계를 통한 사이버보안 강화

일본 내각 사이버보안센터(National center of Incident readiness and Strategy for Cybersecurity, NISC)는 정부 기관 및 관련 기관의 정보보안 수준을 향상하기 위해 「사이버보안 대책 공통 기준」을 수립한다. 이 기준은 정보자산의 분류, 접근 제어, 로그 관리, 사고 대응 등 다양한 보안 조치를 포함하며, 클라우드 서비스 이용 시 적용해야 할 보안 요구사항도 명시한다.

일본의 「능동 사이버 방어법(Active Cyber Defense Law)」은 2025년 5월에 제정된 법률로, 국가의 사이버보안 대응 역량 강화를 목표로 한다. 이 법은 다음과 같은 주요 내용을 포함한다.

정부가 외국과의 통신에서 발생하는 사이버공격을 사전에 탐지하고 대응할 수 있는 권한 부여

경찰과 자위대가 사이버 공격자에 대한 적극적인 방어 조치를 수행할 수 있도록 허용

중요 인프라 운영자에게 사이버보안 사고 보고 의무 부과

(2) JISMS 적합성 평가 제도

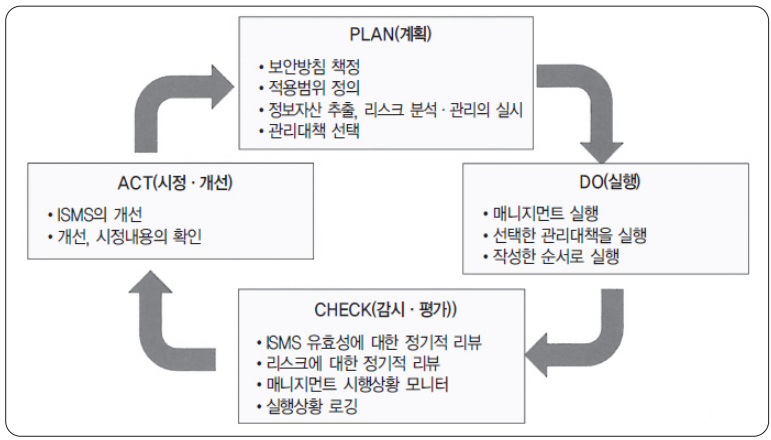
JISMS(Japan Information Security Management System) 적합성 평가 제도는 일본정보처리개발협회(JIPDEC, Japan Information Processing Development Corporation)가 운영하는 제삼자 적합성 인증 제도로, 국제표준인 ISO/IEC 27001에 기반한다. 이 제도는 국제적 정합성을 반영함으로써 일본 내 정보보안 관리 수준을 향상하는 데 이바지하며, 글로벌 신뢰도 확보를 위한 제도적 기반을 제공한다(Japan Information Pro-

cessing Development Corporation. 2023).

JISMS 적합성 평가 프로세스는 ISO/IEC 27001의 'Plan-Do-Check-Act (PDCA)' 모델을 채택하고 있으며, 조직의 정보보안 관리체계가 지속해서 개선될 수 있도록 설계되어 있다. 이 프로세스는 정보보안 운영의 계획(Plan), 실행(Do), 점검(Check), 개선(Act)이라는 순환적 구조를 통해 정보보호 관리 역량을 체계적으로 발전시키는 것을 목표로 한다.

동 연구는 JISMS의 Plan-Do-Check-Act (PDCA) 모델을 프로세스의 중요 기반으로 수용하고 있다.

〈그림 3〉 ISO/IEC 27001의 PDCA 모델



6) 국제표준

(1) 정보보안 표준 지침

ISO/IEC 27001은 정보보안 관리체계(ISMS, Information Security

Management System)에 관한 국제표준으로, 조직이 정보자산의 기밀성, 무결성, 가용성을 보호하기 위해 위험 기반의 보안관리 체계를 수립하고, 이를 운영·유지·지속해서 개선할 수 있도록 지원한다(ISO 2022).

이 표준의 주요 목적은 다음과 같다.

- 정보보안 위험 관리 체계의 구축
- 정보보안 정책, 절차, 책임, 기술적 통제의 수립,
- 사이버공격, 데이터 유출, 비즈니스 중단 등 다양한 위협에 대한 효과적 대응,
- 내부 및 외부 감사와 인증을 통한 신뢰성 확보.

이 표준은 다음과 같은 '관리 요구사항(Clauses 4~10)'과 'Annex A 통제(Controls)'로 구성된다.

가. 관리 요구사항 (Clauses 4~10)

- Clause 4: 조직 상황(Context) – 이해관계자, 내·외부 이슈 분석
- Clause 5: 리더십 – 경영진의 약속, 보안 정책 수립
- Clause 6: 계획(Planning) – 정보보안 리스크 식별 및 처리 계획
- Clause 7: 지원(Support) – 자원, 역량, 인식, 커뮤니케이션, 문서화
- Clause 8: 운영(Operation) – 위험 대응 실행
- Clause 9: 성과 평가(Performance Evaluation) – 내부 감사, 경영 검토
- Clause 10: 개선(Improvement) – 시정 조치, 지속적 개선

나. Annex A 통제 (Controls)

- Organizational Controls (37개): 정책, 책임, 공급망 관리 등

- People Controls (8개): 인적 보안, 보안 교육 등
- Physical Controls (14개): 출입 통제, 장비 보호 등
- Technological Controls (34개): 암호화, 백업, 로그, 접근 제어 등

동 연구는 ISO/IEC 27001의 Plan-Do-Check-Act (PDCA) 모델을 프로세스의 중요 기반으로 수용하고 있다.

4. 국가 공공기관 사이버보안 실태 평가체계 분석

1) 국가 공공기관 사이버보안 실태평가의 목적과 근거

국가 공공기관을 대상으로 한 사이버보안 실태평가는 「국가정보원법」 및 「사이버안보업무규정」에 근거하여 수행되며, 중앙행정기관과 지방자치단체 등 공공기관의 사이버공격 위협에 대한 예방 및 대응 체계를 체계적으로 진단하는 것을 목적으로 한다(국가사이버보안센터, 2025).

「국가정보원법」 제4조 제1항 제4호는 국가정보원이 중앙행정기관 등을 포함한 국가 공공기관의 사이버 위협에 대한 예방 및 대응을 담당할 권한을 가짐을 명시하고 있으며, 「사이버안보업무규정」 제13조는 사이버보안 실태평가의 수행 절차와 대상 기관의 협조 의무를 구체적으로 규정하고 있다.

2) 국가 공공기관 사이버보안 실태 평가 대상 및 절차

사이버보안 실태평가는 중앙행정기관(대통령과 국무총리 소속기관 포함), 그 산하기관, 국가인권위원회, 고위공직자 범죄수사처, 「행정기관 소속 위원회의 설치·운영에 관한 법률」에 따라 설립된 위원회, 지방

자치단체와 그 소속기관, 그리고 대통령령으로 정한 기타 공공기관을 대상으로 실시된다.

국가정보원은 매년 평가 대상 기관과 일정을 확정하여 이를 각 기관에 통보한 후, 사이버보안 환경 변화와 위협 실태를 반영하여 평가기준을 보완하고 실태평가를 수행한다. 본 평가는 ① 기관별 자체 평가, ② 현장 실사, ③ 추가 증빙 및 이의 신청, ④ 평가 결과 통보의 네 단계로 구성된다.

기관은 국가정보원이 배포한 평가지표에 따라 자체 평가를 실시하고, 이에 대한 관련 증빙자료를 제출한다. 이후, 국가정보원은 관계 전문가로 구성된 평가반을 통해 현장 실사를 수행하며, 필요시 서면 또는 원격 실사를 병행할 수 있다. 실사 이후 기관은 7일 이내에 추가 증빙자료를 제출하거나 이의를 제기할 수 있으며, 국가정보원은 최종 평가 결과를 각 기관 및 관계기관에 통보하고, 해당 결과를 정부 업무 평가에 반영할 수 있다.

3) 평가 방법

사이버보안 실태평가는 세 가지 주요 분야로 구성된 평가지표를 기준으로 수행된다.

첫째, 관리적 보안 분야는 총 18개 항목, 37개 질의, 배점 39점으로 구성되며, 조직 구성, 인력 운영, 예산 편성, 내부 감사, 보안 교육, 클라우드 정책 등 조직의 전반적인 관리체계를 포괄한다.

둘째, 기술적 보안 분야는 13개 항목, 37개 질의, 배점 37.5점으로 구성되어 있으며, 망 분리 운영, 시스템과 단말기 보안, 전자우편 보안, 원격근무 시스템 보호 등 기술 기반의 보안 통제항목을 포함한다.

셋째, 위기 대응 역량 분야는 10개 항목, 26개 질의, 배점 23.5점으

로, 사이버 위기 대응 매뉴얼 수립, 재난 대응 체계, 보안관제 운용, 위협 정보 공유 등 대응 역량과 관련된 요소들을 평가한다.

최종 평가는 분야별 현장 실사 점수, 자체 평가 부실도 감점, 추가 정보보안 활동에 대한 가점을 합산하여 산정되며, 총점은 최대 100점을 초과할 수 없다. 기관은 중대한 보안 취약점에 대한 공유, 국가정보원의 측정 결과에 따른 개선 활동, 자체 수행한 추가 정보보안 활동에 대해 관련 증빙자료를 제출할 경우, 가산점을 부여받을 수 있다.

4) 평가지표의 특성과 한계

현재 운용 중인 사이버보안 실태 평가지표는 모든 공공기관에 공통으로 적용되는 체크리스트 기반의 평가 방식으로, 특히 망 분리 환경에서의 보안관리 상태를 중점적으로 점검하도록 설계되어 있다. 이 평가 방식은 명확한 질의 항목과 배점 기준에 근거하여 평가자의 주관적 판단 오류를 최소화하고, 단기간 내 실효성 있는 현장 평가를 수행할 수 있다는 장점을 지닌다.

그러나 전산 자원이 상대적으로 적은 기관이 오히려 높은 기술 점수를 획득하는 역설적인 상황이 발생할 수 있으며, 기관별 기능적 특수성이나 자율적인 정보보안 활동의 다양성이 평가에 충분히 반영되지 않는다는 한계가 존재한다.

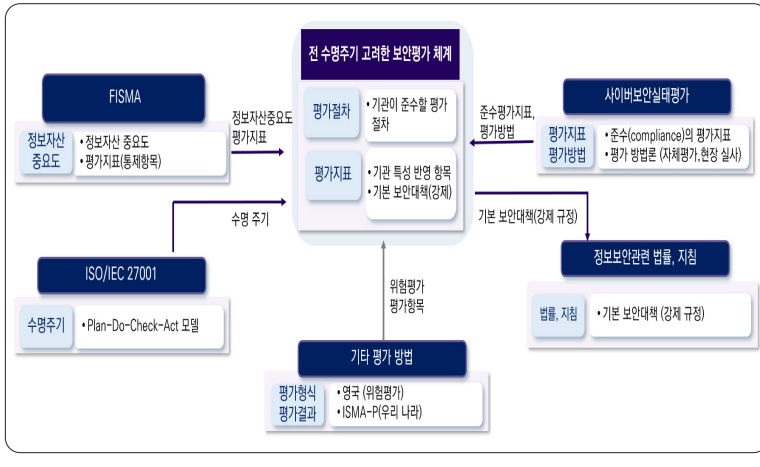
특히 최근에는 클라우드 서비스 및 생성형 AI 도입의 확산 등 국가망 보안환경이 급변하고 있으며, 이에 따라 기관별 정보자산의 중요도와 위험 수준을 반영한 자율 보안계획의 수립과 이에 대한 평가가 가능한 체계적 접근이 요구된다. 이러한 배경에서, 자율적 평가체계 기반의 표준모델 마련이 향후 사이버보안 실태평가의 방향으로 제시되고 있다.

Ⅲ. 기관 특수성을 반영한 사이버 실태평가 체계 개발

1. 개발 방향

기관의 특성을 반영한 사이버보안 실태평가 체계(안)는 현행 사이버보안 실태평가 제도의 한계를 보완하고자, 국내외 정보보안 관련 제도와 평가 프레임워크의 핵심 개념을 통합하여 개발된다. 이 체계는 국내 정보보안 관련 법령 및 지침, 미국의 「연방 정보보안 현대화법(Federal Information Security Modernization Act, FISMA)」, 국제표준인 ISO/IEC 27001, 그리고 주요 평가 기법의 개념을 기반으로 하며, 현행 평가체계와의 정합성을 확보하도록 설계된다.

〈그림 4〉 기관의 특성을 반영한 사이버보안평가 체계 개발 개념(안)



사이버보안 실태평가에 대한 개선 요구사항 중 기관에 적합한 보안 대책의 선정, 기관의 보안환경을 고려한 보안 수준의 설정 등이 있다. 따라서 사이버보안 실태평가의 개선 방향은 기관이 처한 보안환경을 반드시 분석하고, 이를 기반으로 보안 대책을 수립하는 절차를 포함할 필요가 있다.

사이버보안 실태평가는 국가기관이 반드시 준수해야 하는 기본 대책으로서, 평가지표, 자체 평가 및 현장 실사 등의 평가 절차, 그리고 평가 결과의 처리 방식 등 핵심 요소를 포함한다. 이러한 구성 요소는 기관의 특성을 반영한 사이버보안 실태평가 체계에서 보안관리 수명주기 관점을 반영한 핵심 틀로 수용된다.

국내 법령과 지침에서 제시하는 보안 책임 및 의무 사항은 해당 평가체계 내에서 국가기관이 반드시 이행해야 할 필수 보안 대책으로 수렴된다는 점에서 기존 정보보안 관련 규정 등을 포함할 수 있는 제도적 정합성을 확보할 수 있다.

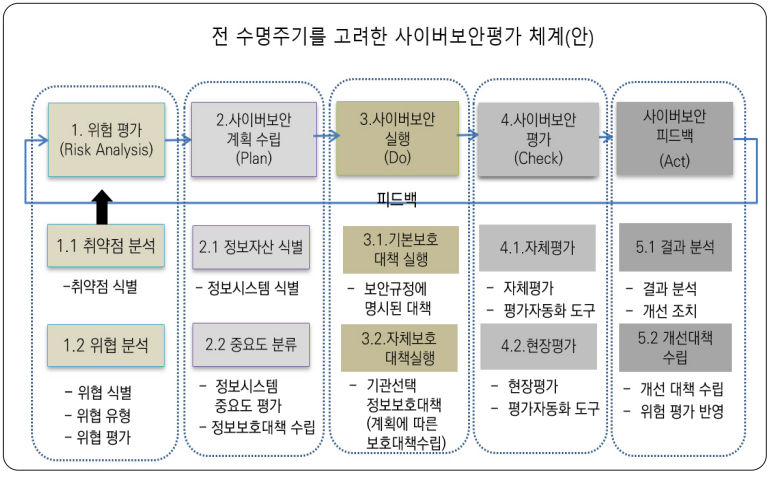
FISMA가 강조하는 위험 기반 평가 방식과 정보자산의 중요도에 따른 보호 대책 수립 개념은, 기관별 운영 환경과 특성을 실태평가에 반영할 수 있는 주요 요소로 작용하며, 본 평가체계는 이러한 개념을 적극적으로 수용한다.

국제표준 ISO/IEC 27001은 계획(Plan), 실행(Do), 점검(Check)으로 구성된 정보보안 관리 절차를 기반으로 한다. 본 평가체계는 여기에 개선(Act) 단계를 추가하여 PDCA(Plan-Do-Check-Act) 사이클을 완성함으로써, 지속적인 보안관리의 고도화를 유도한다. 제안된 평가체계는 영국의 위험평가 절차와 국내 ISMS-P(Information Security Management System-Privacy)의 구조적 특성도 일부 반영함으로써, 국내 현실에 적합하면서도 국제적 정합성을 갖춘 평가체계로 구성된다.

2. 위험평가와 수명주기(PDCA)로 구성된 평가체계

1) 평가 체계(안) 개념

〈그림 5〉 보안관리 수명주기를 고려한 평가체계(안)



본 연구가 제안하는 기관의 특성이 반영된 사이버보안 평가체계는 위험평가(Risk Analysis)와 PDCA(Plan-Do-Check-Act) 수명주기 절차 등을 결합한 통합적 구조로 설계된다. 이 체계는 기관별 환경 및 특성에 따라 보안 위협을 사전에 분석하고, 이에 기반한 계획 수립, 실행, 평가, 개선의 절차를 순환적으로 수행함으로써, 보안관리의 체계적 운영을 가능하게 한다. 특히, 본 평가체계는 사이버보안 관리 활동 전반에 걸쳐 단계별 역할을 명확히 규정하며, 조직의 상황에 부합하는 보안 대책 수립을 가능하게 하는 위험평가 방법론과 PDCA 구조를 통합하여 자율적이고 반복적인 보안관리 프로세스를 실현할 수 있다.

2) 제안된 평가체계의 특성

제안된 평가체계는 기관이 자체적 특성과 보안환경을 고려하여 계획-실행-평가-개선(Plan-Do-Check-Act)이라는 일련의 절차를 자율적으로 수행할 수 있도록 구성된다. 동 평가체계는 개별 절차의 이행 여부와 적정성을 평가할 수 있는 구조를 가질 수 있도록 지표가 설계된다. 모든 사이버보안 활동은 〈표 8〉과 같이 PDCA의 특정 절차와 연계되어 있으며, 해당 활동을 평가하기 위한 지표는 반드시 절차별 성취 목표와 함께 설정되어야 한다. 이러한 분류 방식은 평가지표 개발 시 기준의 명확성을 제공한다는 점에서 의의가 있다.

본 평가체계는 단순한 보안 현황 진단을 넘어, 위험평가에서부터 개선 활동에 이르는 전 과정을 체계화함으로써 정보보안 수준의 실질적 향상을 도모한다. 이 체계는 기관의 자율성과 책임성을 동시에 강화하는 방향으로 설계되며, 결과적으로 평가의 객관성과 신뢰성을 제고하고, 규정 준수 여부 및 절차의 완결성을 종합적으로 검토할 수 있는 평가 기준을 제시한다.

〈표 8〉 사이버보안 평가지표의 PDA 분석과 지표 목표 분석

문항 번호	계획 (plan)	실행 (do)	평가 (check)	개선 (Act)	현수준(As-Is)					목표 수준(To Be)				
					정책 수준	절차 수준	기술 수준	검증 수준	제도 수준	정책 수준	절차 수준	기술 수준	검증 수준	제도 수준
1.2.1	O	O			O	O	O			O	O	O	O	
1.2.2	O	O			O	O	O	O	O	O	O	O	O	O
2.1.4	O	O	O		O	O	O			O	O	O	O	
2.2.9	O	O				O	O			O	O	O	O	
3.2.4	O	O	O	O		O				O	O	O	O	
4.2.7	O	O			O	O	O	O		O	O	O	O	
5.4.1	O	O	O	O	O		O			O	O	O	O	

문항 번호	계획 (plan)	실행 (do)	평가 (check)	개선 (Act)	현수준(As-Is)					목표 수준(To Be)				
					정책 수준	절차 수준	기술 수준	검증 수준	제도 수준	정책 수준	절차 수준	기술 수준	검증 수준	제도 수준
5.4.2	O	O	O	O	O		O			O	O	O	O	
5.5.1	O	O			O		O			O	O	O	O	
6.4.1	O	O	O	O	O	O	O	O		O	O	O	O	
6.4.5	O	O	O	O	O	O	O	O		O	O	O	O	
6.5.1	O	O	O		O					O	O	O	O	
6.5.5	O	O	O		O					O	O	O	O	
6.6.4	O	O	O		O	O				O	O	O	O	
신항목1	O	O				O				O	O	O	O	
신항목2	O				O					O				
신항목3	O	O		O	O					O	O	O	O	O
신항목4	O	O		O	O					O	O	O	O	O
신항목5	O	O		O	O					O	O	O	O	O
신항목6			O		O					O	O	O	O	O
신항목7	O	O			O	O				O	O	O	O	O
신항목8	O			O	O					O	O	O	O	O

3. 기관의 특성을 반영한 사이버보안 평가체계

〈그림 5〉와 같이 제안된 사이버보안 평가체계는 위험평가, 사이버보안 계획 수립, 사이버보안 실행, 사이버보안 평가, 사이버보안 개선 등의 절차로 구성된다. 개별 절차의 구체적인 내용은 다음과 같다.

1) 위험평가

위험평가는 기관이 보유한 정보시스템 자산에 내재한 취약점과 이를 둘러싼 내·외부 위협을 식별하고 분석하는 절차로 구성된다. 기관은 이 절차를 통해 자산의 취약성과 위협 요소를 체계적으로 분석하

고, 이를 기반으로 관리 대상이 되는 주요 위험 항목을 도출한다.

도출된 위험 항목은 기관의 정보시스템 특성, 보안환경, 업무 성격 등을 반영하여 작성되며, 이후 보안계획 수립의 기초 자료로 활용된다. 또한, 위험평가 결과는 객관적인 평가의 신뢰성을 확보하기 위해 정량화된 지표 형태로 도출되어야 하며, 해당 지표는 현행 세부 지표와 유사한 수준의 구체성을 가지면서도 기관 활동 전반을 측정할 수 있는 구성으로 설계되어야 한다.

2) 사이버보안 계획 수립(Plan)

사이버보안 계획 수립 단계는 기관이 수행해야 할 보안관리 활동, 정보보호 대책, 평가 시기 및 절차, 평가 결과의 반영 방안을 포괄적으로 계획하는 과정으로 구성된다.

계획 수립은 크게 정보시스템 식별과 중요도 분류의 두 단계로 구분된다. 먼저, 정보시스템 식별은 기관이 보유한 모든 정보자산을 정보시스템 단위로 식별하는 절차이며, 중요도 분류는 각 시스템의 중요도에 따라 관리적, 기술적, 위기 대응 보안관리 영역으로 세분된 보안 대책을 차등적으로 수립하는 과정을 의미한다.

3) 사이버보안 실행(Do)

사이버보안 실행 단계는 수립된 보안계획에 따라 정보시스템 보호를 위한 구체적인 대책을 실행하는 과정으로, 기본 보호 대책 실행과 자체 보호 대책 실행으로 구성된다.

기본 보호 대책 실행은 관련 법령이나 국가 지침에 명시된 필수 보안 조치를 기관이 도입하고 운영하는 절차로, 모든 기관에 공통 적용된다. 반면, 자체 보호 대책 실행은 기관별 위험평가 결과를 기반으

로, 기존 대책을 보완하거나 삭제하는 등 기관의 자율성을 반영한 보안 대응 활동을 의미한다.

따라서, 본 연구에서 제안하는 실행 체계는 법적 의무를 충실히 이행함과 동시에, 기관의 환경과 특성에 적합한 자율적 보안 대책의 수립과 운영을 가능하게 하는 이중적 구조를 특징으로 한다.

4) 사이버보안 평가(Check)

사이버보안 평가는 기관이 앞서 수행한 위험평가, 보안계획 수립, 보호 대책 실행의 적절성을 검토하는 단계이다. 본 평가는 위험평가의 정확성, PDCA 체계 반영 여부, 그리고 수립된 보안 대책의 적정성 등을 중심으로 이루어진다.

자체 평가는 기관이 스스로 전 단계의 연계성과 이행의 충실성을 점검하는 활동이며, 현장 평가는 외부 평가 기관이 해당 기관의 사이버 보안관리 수명 주기별 활동과 보호 대책 이행 여부를 종합적으로 검토하는 절차이다.

이때, 기본 보호 대책은 항목별 준수 여부를 중심으로 평가하며, 수명주기 기반 활동은 각 단계 간의 유기적 연계성을 기준으로 평가가 이루어진다.

5) 사이버보안 피드백(Act)

사이버보안 피드백 단계는 평가 결과를 분석하고, 발견된 문제점에 대한 개선대책을 수립한 뒤 이를 다시 위험평가에 반영하는 활동으로 구성된다. 이 단계는 기관의 보안 수준을 실질적으로 향상하기 위한 절차로서, 결과 분석과 개선 조치 수립의 두 과정으로 이루어진다.

분석 결과는 미비한 보안 활동을 보완하기 위한 근거 자료로 활용되며, 도출된 개선대책은 정보보호 대책의 보완 또는 위험평가 항목의 재설계 등의 방식으로 체계 내에 반영된다. 이와 같은 순환 구조는 지속적인 보안관리 고도화와 PDCA 사이클의 완결성 확보에 이바지한다.

4. 제안된 체계의 특성 분석

1) 선결 사항

기관의 특성을 반영한 사이버보안 실태평가 체계의 도입을 위해서는 몇 가지 선결 과제가 존재한다. 첫째, 법적·제도적 기반의 정비가 필요하다. 본 체계가 현행 「국가정보원법」 및 「사이버안보업무규정」과의 정합성을 유지하면서도 실질적인 평가 기준으로 기능하기 위해서는, 관련 법령의 개정 또는 하위 지침의 보완이 요구된다. 또한 새로운 평가체계에 대한 법적 구속력 확보가 병행되어야 한다.

둘째, 평가지표의 정량화와 표준화가 필요하다. PDCA 단계별 성취 목표에 대응하는 정량화된 평가지표를 설계함으로써, 기관의 활동을 객관적으로 측정할 수 있어야 한다. 동시에 기관별 특수성을 반영할 수 있도록, 공통 지표와 선택적 지표가 유연하게 병행될 수 있는 설계 구조가 필요하다.

셋째, 체계 운영을 위한 전문 인력과 평가 기관의 역량 강화가 필요하다. 특히 외부 평가 기관은 위험 기반 평가와 수명주기 기반 관리를 수행할 수 있는 전문성을 갖춘 인력을 확보해야 하며, 이를 위한 지속적인 교육과 훈련 체계가 뒷받침되어야 한다.

넷째, 정보시스템 식별 및 중요도 분류 기준의 정립이 요구된다. 정

보자산을 정보시스템 단위로 통합적으로 식별하고, 그 중요도에 따라 관리적·기술적·위기 대응 영역별로 보안 대책을 차등 적용할 수 있는 분류 체계의 정교화가 필요하다.

마지막으로, 기관의 자율성을 전제로 한 체계의 성공적 도입을 위해, 참여 유도 방안이 함께 마련되어야 한다. 기관의 자발적인 보안관리 역량 강화를 장려하기 위한 인센티브 제공, 성과 기반 피드백 체계 등의 정책적 설계가 요구된다.

〈표 9〉 제안된 체계의 선결 사항

구분	선결 과제	내용
법적·제도적 기반 확보	현행 제도와의 정합성 검토	「국가정보원법」 및 사이버안보업무규정 등 관련 법령과의 조율 필요
	법적 구속력 확보	새로운 평가체계의 적용 강제력을 위한 법·지침 개정 필요
평가지표 설계 표준화	정량 지표 개발	PDCA 단계별 성취 목표 및 측정 가능 지표의 구체화 필요
	공통성과 유연성 확보	기관별 특성을 반영하면서도 공통 적용할 수 있는 표준 지표 구성
운영기관 및 인력 역량 강화	평가 인력의 전문성 강화	평가 기관의 평가 역량 및 전문성 강화 필요
	교육 및 훈련	위험 기반 평가 및 수명주기 관리 관련 교육체계 마련
정보시스템 분류 기준 정립	시스템 식별 및 중요도 분류	정보자산 식별 및 중요도 분류를 위한 기준 체계 수립 필요
기관 참여 유도	자율성과 책임 기반 평가 설계	기관 참여를 촉진하기 위한 인센티브 구조 및 가이드라인 필요

2) 장단점 분석

제안된 사이버보안 실태평가 체계는 다음과 같은 장점을 지닌다. 첫째, PDCA(Plan-Do-Check-Act) 기반의 수명주기 구조를 채택함으로써, 보안관리의 일회성 점검을 넘어 지속적 개선과 순환적 관리를 가능하게 한다. 현재 사이버보안 실태평가도 일부 지표의 경우 개선 사항을 점검하고 있으나, 관련된 지표의 숫자가 매우 적고 개선 사항이 계획과 연결된 부분도 미비한 실정이다. 둘째, 정보시스템의 중요도 및 기관별 운영 환경을 반영할 수 있어, 자율성과 상황 적합성이 강화된다. 현재 평가체계는 정보시스템의 중요도는 고려하지 않고 있어 자원의 효과적인 투입을 고려할 수 없다. 중요한 정보시스템에 투입되는 보안 자원과 덜 중요한 정보시스템에 투입되는 보안 자원의 양과 질이 거의 동일하다. 셋째, 평가지표의 정량화 설계를 통해 객관성과 신뢰성이 제고될 수 있다. 현재 평가체계는 정성적 평가 체계 구조로 되어 있어 평가자와 피평가자 간에 신뢰성이 저하되는 경우가 존재한다. 위험 분석을 기반으로 지표를 설계하면 정량적 지표 설계가 가능하다. 넷째로 본 체계는 FISMA, ISO/IEC 27001, ISMS-P 등 국내외 제도와의 정합성을 갖춘 구조로 설계되어 국제 기준에 부합하는 평가를 수행할 수 있다. 본 연구가 제안하는 평가 프로세스는 국제적인 표준이 제안하는 프로세스와 동일하다. 마지막으로, 평가 이후 개선까지 반영하는 피드백 절차를 포함함으로써, 단순 진단을 넘어 보안 수준의 실질적 향상을 도모할 수 있다.

그러나 이 체계는 몇 가지 한계점도 함께 내포한다. 첫째, 수명주기 기반의 평가 구조는 중소규모 기관에 과도한 행정적·운영적 부담으로 작용할 수 있다. 둘째, 기관의 자율성에 기반한 평가 구조는 편차를 유발할 가능성이 있으며, 결과의 일관성 확보를 위한 최소 기준 마

련이 요구된다. 셋째, 기관의 고유 특성을 반영한 정량 지표의 개발은 기술적으로 복잡하며, 표준화에도 시간이 소요된다. 넷째, 기존 체크리스트 중심의 단순 평가에 익숙한 기관은 체계 도입 초기 저항감을 보일 수 있으며, 마지막으로 평가자의 전문성 부족은 체계 전반의 실효성을 저해할 수 있다.

5. 기대 효과

1) 기관 특성을 반영한 보안관리 체계 도입

기존의 사이버보안 관리는 규정 중심의 일률적 방식으로 운영되어, 기관별 환경과 특성을 충분히 반영하지 못하는 한계가 존재한다. 그러나 본 연구에서 제안하는 사이버보안 평가체계의 도입을 통해, 기관의 고유한 특성과 상황을 평가에 적극적으로 반영할 수 있다.

제안된 체계는 위험평가(Risk Analysis)를 사이버보안 관리체계에 통합함으로써, 기관의 규모, 보유한 정보시스템의 보호 수준, 운영 중인 보안환경 등을 고려하여 정보보호 대책 수립의 실질적 근거를 제공한다. 이를 통해, 각 기관은 규정 준수에 그치지 않고 상황 기반의 자율적 보안관리 전략을 수립·운영할 수 있게 된다.

2) 보안관리 수명주기를 기관의 보안 관리체계와 보안 평가에 반영

현행 사이버보안 관리는 형식적으로는 보안관리 수명주기를 대상으로 하나, 실제로는 수명주기 각 단계 간의 체계성 및 연계성 확보에 미흡하여, 보안 관리체계가 느슨하게 작동하거나 분절적으로 운영되는 한계를 보인다. 이러한 운영 방식은 보안 활동 간의 일관성을 저해하고, 위협 대응의 실효성을 저하할 수 있다.

반면, 본 연구에서 제안하는 보안관리 수명주기 기반 사이버보안 평가체계는, 위험평가에서부터 개선대책 수립에 이르는 전 과정을 통합적으로 포괄하며, 수명주기 각 단계 간의 연계성과 구조적 일관성을 강화한다. 이를 통해 사이버보안 관리는 단순한 규정 이행을 넘어서, 자율적이고 효율적인 방식으로 수행될 수 있을 것으로 기대된다.

3) 효율적인 보안관리 수준 도입

현행 사이버보안 관리는 법령이나 지침에서 명확하게 규정하지 않은 영역에 대해 기관이 임의로 보호 대책을 수립하는 방식으로 운영되는 경우가 많아, 보안관리의 효율성을 저해하는 문제가 발생하고 있다. 이에 따라 일부 기관은 과도하게 보수적인 대책을 수립하거나, 반대로 위험 수준에 비해 지나치게 낮은 수준의 대응 등 일관성 없는 보호 수준을 보일 수 있다.

본 연구가 제안하는 평가체계는, 사이버보안 관련 법령이나 지침에서 명시하지 않은 영역에 대해서도 기관이 적정 수준의 보호 대책을 수립할 수 있도록 유도하는 구조를 갖춘다. 이를 통해 보호 대책의 과소 또는 과잉 설정을 방지하고, 기관의 특성과 위험 수준에 부합하는 합리적 대응이 가능하게 한다.

Ⅳ. 시사점 및 결론

본 연구는 국가 공공기관의 사이버보안 수준을 높이기 위한 평가체계의 개선 방향으로, 보안관리 수명주기를 고려한 사이버보안 평가체계를 제안하였다. 기존 평가체계는 규정 중심의 일률적 접근에 머물러 있어 기관별 특성과 환경을 충분히 반영하지 못하며, 위험평가보호대책 실행 피드백 간 연계성이 부족한 구조적 한계를 내포하고 있다.

이에 본 연구는 위험 기반 접근 방식을 도입하여 기관별 정보시스템의 특성과 업무 환경을 반영할 수 있는 평가 틀을 마련하였으며, 계획(Plan)-실행(Do)-평가(Check)-개선(Act)으로 구성된 PDCA 수명주기 기반 체계를 적용함으로써 평가의 연속성과 체계성을 강화하였다. 특히, 단계별로 구성된 구체적 평가지표와 절차 기반 평가 방식은 기관의 자율성과 보안 수준 간의 균형을 도모하는 데 이바지한다.

이러한 체계를 통해 다음과 같은 기대 효과를 도출할 수 있다.

첫째, 기관 특성을 반영한 맞춤형 보안 관리체계 구축이 가능하다. 둘째, 보안관리 전 과정의 연속성과 일관성 확보를 통해 실질적인 보안 수준 향상이 기대된다. 셋째, 법령이나 지침에서 명확히 규정하지 않은 영역에 대해서도 효율적이고 적정 수준의 보호 대책 수립이 가능하여, 평가의 전체적인 실효성과 효율성이 제고된다.

동 평가체계의 도입을 위해서는 점진적인 평가 프로체계의 변경이 필요하다. 먼저 평가 프로세스를 기관의 실정에 맞게 변경할 수 있는 자율적인 프로세스로 변경하고, 둘째, 프로세스의 변경에 따라 평가지표를 자율적인 체계로 변경할 필요가 있다. 다만, 이 과정에서 기관

의 평가 실행의 완전성과 신뢰성에 대한 평가가 이루어져야 한다.

향후 연구에서는 제안된 평가체계의 시범 적용을 통한 실효성 검증이 필요하며, 다양한 기관 유형을 대상으로 한 사례 연구를 통해 모델을 정교화해 나가야 한다. 아울러 본 체계가 정책적·제도적으로 안착하기 위해서는 관련 법령 및 가이드라인의 정비, 전문 평가 인력의 양성, 현장 적용을 위한 운영지침 마련 등이 병행되어야 할 것이다. 동 평가체계가 도입되는 과정에서 우려스러운 지점은 기관의 정보보호인력의 전문성 확보와 자원의 확보가 절실히 필요하다는 점이다.

〈참고문헌〉

국가사이버보안센터, 2025,『국가사이버보안평가 해설집』. 서울: 두리사.

과학기술정보통신부·개인정보보호위원회. 2023.『정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시』(과기정통부 고시 제2023-22호)

과학기술정보통신부. 2023.『클라우드 서비스 보안 인증제도 운영지침 (제5판)』.

과학기술정보통신부. 2023.『주요정보통신기반시설 보호계획 이행점검 종합결과 보고서』.

Cabinet Office Government Security Group. 2021.『Government Functional Standard GovS:007: Security (Version 2.0)』.

European Parliament & Council. 2022.『Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)』. Official Journal of the European Union, L 333, 80–15

General Services Administration. 2024.『FedRAMP Agency Authorization Playbook』.

Government of Japan. 2014.『Basic Act on Cybersecurity (Act No.104). Retrieved from Japanese Law Translation』

International Organization for Standardization & International Electrotechnical Commission. 2022. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection Information security management systems Requirements. Geneva, Switzerland: ISO.

Japan Information Processing Development Corporation. 2023.『Overview of the Japan ISMS Certification Program (JISMS)』. Tokyo: JIPDEC.

National Institute of Standards and Technology. 2023.『Cybersecurity Framework 2.0. NIST Special Publication』.

National Office for Information Security (BSI). 2023. IT-Grundschutz-Kompendium (Edition 2023). Bundesamt fur Sicherheit in der Informationstechnik.

United States Congress. 2014, 『Federal Information Security Modernization Act of 2014』 (Pub. L. No. 113-283, 128 Stat. 3073). Retrieved from https://www.govinfo.gov

The White House. 2016, 『Presidential Policy Directive 41: United States Cyber Incident Coordination』.

A Study on Security Assessment Methodology Influencing the Characters of the Institutions Security Management

Myeonggil Choi | Dept.of Business Administration, Chung-Ang University

With the growing number of cyber intrusions, the importance of cybersecurity in public institutions has become increasingly emphasized. As a result, cybersecurity readiness assessments are gaining attention as a means to verify the robustness of institutional security systems. This study proposes a self-directed cybersecurity evaluation framework that reflects organizational characteristics and security environments, aiming to overcome the limitations of the current cybersecurity assessment system applied to public institutions in South Korea. Existing assessments rely heavily on uniform checklist-based items, which fail to adequately account for agency-specific security capabilities and risk factors. To address this issue, this study designs a cybersecurity evaluation model based on the full life-cycle Plan-Do-Check-Act (PDCA) framework and identifies its core components through a comparative analysis of international security evaluation systems such as FISMA, ISMS-P, and FedRAMP. By presenting a measurable indicator system that incorporates both risk assessment and feedback mechanisms, this research offers an improved direction for cybersecurity readiness evaluations that ensures both autonomy and accountability.

Keyword Cybersecurity Status Assessment, Risk Assessment, Information Security Policy, Autonomy-Based Security Management, PDCA Framework