I

전자정부서비스의 소프트웨어 안전성 및 신뢰성 강화 정책

중앙대학교 ▌김성근 · 최명길
행정안전부 ▌한근희*

1. 서 론

우리나라의 인터넷 환경은 세계적으로 뛰어나서 '09.5월 기준 초고속 인터넷 보급률 96%로서 1,587만 명이 사용 중이고, '08.12월 기준 인터넷 이용자 수는 3,536만명으로 6세 이상 인구의 77.1%가 사용 중이다.

또한, 우리나라 전자정부 서비스는 UN 전자정부 참여지수 1위, 미국 브루킹스연구소(전 브라운대학) 평가에서 3년 연속 1위를 차지할 정도로 잘 구축되어 있으나, 반면에 세계경제포럼(WEF)에서 2009년 조사한 정보보호 순위는 16위로 2007년 54위에서 대폭 상승된 것 같이 보이나 실제로는 SSL 보안서버 보급률로만 단순 산정한 지수로서, 인터넷 이용자수와 서비스 환경에 비해서 정보보호 분야는 상대적으로 열악한 수준이다[3].

2008년 한 해 동안에만 옥션 정보유출, GS 칼텍스 정보 유출 등 크고 작은 보안 사고들이 끊임없이 발생하여 국민들이 사이버위협에 노출되고 주요 정보들이 유출되고, 2009년에는 국가적으로 중요한 전자정부서비스 및 민간의 주요 정보시스템에 대한 DDoS 공격 등의 사이버공격이 발생하여 점차 정보보안, 개인정보보호의 필요성과 중요성에 눈을 뜨게 되어 정보보호에 대한 요구가 점차 늘어나고 있는 추세이다.

문제는 정보시스템이 취약하기 때문에 조그만 침해시도에도 안전성이 심히 저하되고 피해가 확대된다는 점이다. 이런 정보시스템의 취약성은 정보시스템 개발 초기 단계에서부터 파생되고 있기 때문에, 정보시스템을 기획하고 분석 · 설계하는 단계에서부터 개발 구축, 운영 · 유지보수하는 단계까지 전 과정에서 소프트웨어의 취약점을 사전에 점검하여 제거하는 노력이 필요하다[2].

이런 정보시스템의 취약성을 최대한 억제하고 안정성을 강화하기 위해서는 다양한 노력이 필요하다. 특히 공공 분야에서는 법 · 제도적 기반 마련이 중요한데, 현재 우리의 법 · 제도는 정보시스템 구축의 전 과정에 걸쳐 취약점이 발생할 수 있는 근원적 원인을 사전 제거하고 이를 체계적으로 검증하려는 법 · 제도가 아주 미흡한 실정이다[1].

본고에서는 미국 연방정부의 전자정부 서비스 수준과 정보보호를 위한 법 · 제도 · 정책 등을 살펴보고, 우리나라에서 이를 효율적으로 활용할 수 있는 방안을 찾아서 정보시스템의 안전성을 강화시키기 위한 법체계 및 제도 구현 방안을 제시하여 중앙행정기관 및 지방자치단체에서 제공하고 있는 전자정부 서비스의 안전성과 보안성을 향상시킬 수 있도록 하고자 한다.

2. 미국 연방정부의 법·제도 분석

미국의 정보보호관련 법률과 하위 지침인 FIPS (Federal Information Processing Standards)와 SP(Special Publication) 문서의 목적, 주요 보호대상, 구조, 보안관련 규정 · 법조문을 분석하여 소프트웨어 보안(Secure Coding) 강화 체계 확립에 활용할 수 있는 법 · 제도를 도출하고, 소프트웨어 취약성을 초기 단계부터 찾아서 제거할 수 있는 대안을 마련한다.

연방정보보안관리법(Federal Information Security Management Act; 이하 FISMA)은 2002년도 제정된 전자정부법(e-Government Act) 중 3편(Title III)의 SEC. 301(Information Security)에 포함된 법률이고, 동시에 US Code Title 44(Public printing and documents)의 Chapter 35(Coordination of federal information policy)의 Sub-chapter III(Information security)에 포함된다[4].

FISMA의 목적은 연방 정부의 정보와 자산 및 운영을 보호하기 위한 포괄적인 기본 틀을 만드는 것이다. 2008 회계연도에 연방 기관들은 연방정부가 총 680억 달러나 투자한 전체 IT 포트폴리오의 약 9.2%에 해당되는 62억 달러를 보안 부문에 지출했다. IT 보안에 투입된 기금은 시스템의 전반적인 측면만이

* 종신회원

아니라 시스템의 인증 및 인가(C&A : Certification & Accreditation), 통제 시험, 사용자 보안의식 훈련과 같은 시스템의 구체적인 보안에 사용되었다.

FISMA는 IT 시스템의 보안을 강화하기 위해 국립표준기술원(National Institute of Standards and Technology; 이하 NIST)과 관리예산처(Office of Management and Budget; 이하 OMB)와 같은 연방기관들에 대해 구체적인 책임을 부여하고 있다. 특히 FISMA는 각 기관의 장들이 적은 비용으로 정보보안위험을 허용 가능한 수준까지 낮출 수 있는 정책을 개발하고 또 이를 실행에 옮길 것을 요구하고 있다.

FISMA에 따라 NIST는 전년도에 완료된 활동을 보고하고 FISMA에 따른 책임을 다하기 위해 다음 해의 활동을 상세하게 설명하는 연례보고서를 만들어야 한다. NIST는 NIST 산하 정보기술연구소의 컴퓨터 보안과를 중심으로 법령에 규정된 책임을 다하고 있다.

NIST의 보고서는 홈페이지(http://csrc.nist.gov)에서 볼 수 있다.

FISMA는 정부기관이 정보와 정보시스템 보호를 위해 전사적 정보보호 프로그램을 개발, 문서화, 구현을 요구하고 있으며, 연방정부 기관의 정보보안 강화를 위해서 제정되었다. 각 연방 정부기관의 정보시스템의 보안 강화를 위한 프로그램 개발, 문서화, 집행을 의무화하고 있으며, 시행 및 감독은 OMB가 담당하고 있고, 준수 등급에 따라 연방정부기관의 정보화 예산을 지급한다.

FISMA는 감독기관 · 기관장 · 기관담당조직의 역할 및 책임, 보안 프로그램의 적합성 · 구현 · 평가 및 개선, 효과적 수단으로의 표준 및 가이드라인 · 도구 · 기술센터의 활용 등을 모두 명시하고 있다. FISMA가 명시하고 대상은 데이터 수준에서 기반시설을 망라한 정보보호가 필요한 대부분의 관련 대상을 포함하고 있다.

§ 3543(책임자의 권한과 기능)은 OMB 책임자가 각 기관의 시스템 정보보안정책과 실행을 총괄하도록 정의하고 있다. OMB 기관장은 현재 실행 중인 정보보안정책, 원칙, 표준 및 지침 등을 총괄하고 개발해야 하며, 각 기관의 책임자는 매년 3월 1일 이전에 해당 조항(sub-chapter)의 준수사항을 OMB에 보고해야 한다.

§ 3544(연방기관의 책임)은 각 연방기관장은 허가를 받지 않은 접속과 정보의 무단 사용, 공개, 중단, 수정, 파괴 등으로 부터 정보를 보호할 수 있는 방법을 제공해야 함을 명시한다.

§ 3545(독립적인 연간 평가)는 각 기관은 정보보안 프로그램과 기관의 정보보호수행의 효과를 검증하는

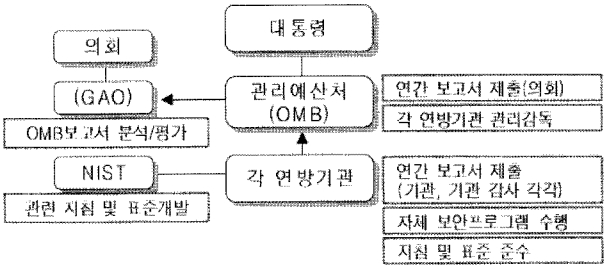

그림 1 미국 연방정보보안 관리체계

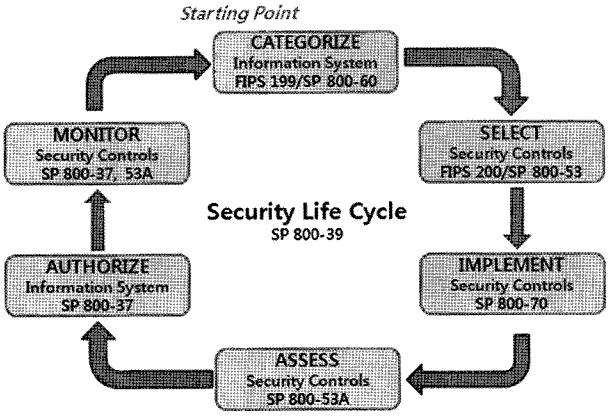

그림 2 FISMA를 위한 정보보안 규격, 표준, 가이드라인

독립적인 평가의 매년 실시를 명시하고 있다.

§ 3546(연방 정보보안사고 센터)는 책임자는 중앙 연방정보보안사고 센터의 운영을 보장해야 한다는 내용으로 정보보안 사고에 대한 확실한 대책을 제시하고 있다.

행정명령(Executive Order 13011)은 연방정보기술도입에 관한 사항을 명시하고 있으며, 문서감축법(PRA)과 정보기술관리개혁법(ITMRA)을 보완하는 행정명령으로 법률을 위반하거나 의회의 입법권을 무력시킬 수 없으며, 정부문서감축, 효율적 정보관리, 정보기술과 조직의 유기적 결합, 연방정부기관의 프로그램의 생산성 향상, 정부기관과 정보기반의 조화, 상호운용성, 안전보장, 정보공유의 촉진 등의 목적을 위하여 제정되었다.

국토안보부의 대통령 명령(HSPD : Homeland Security Presidential Directive 7)은 연방정부 부처와 연방기관이 미국의 주요 기반시설과 핵심 자원을 식별하여 우선순위를 정하고, 동 기반시설과 핵심 자원을 테러리스트의 공격으로부터 보호하는 국가정책을 수립하기 위하여 제정되었다[7].

HSPD-7은 특정 기반시설에 대한 보호책임이 어느 정부기관에 귀속되는지를 식별하고, 핵심 요소는 특정 정부기관이 적절한 민간 기관과 협력하여 임무를 수행할 것을 요구하고 있다.

HSPD-7은 2004년 7월까지, 연방정부 부처 및 기관장은 기관과 부처가 소유 또는 운영 중인 물리적 주요기반시설과 사이버 주요기반시설, 그리고 핵심자원 보호 계획을 식별하고, 우선순위를 선정하고, 보호조치 수립, 비상계획을 수립해야 한다고 규정하고 있으며 매년 기관 활동을 국토안보부 장관에게 보고해야 한다.

국토안보부장관은 주요기반시설과 핵심 자원의 보호를 위하여 연방정부부처 및 연방기관, 지방정부, 그리고 민간부문간의 활동을 조정하는 최고연방책임관으로 역할을 수행한다.

OMB는 기관의 보안프로그램을 감독하는데 필요한 정보를 얻고 연례보고서를 작성하기 위해 매년 각 기관에 보고 지침을 내린다. 과거와 마찬가지로 2008 회계연도의 OMB 보고 지침에는 FISMA의 주요 항목에 대한 정량적이고 정성적인 성과 측정 기준이 포함되어 있다. 인증 및 인가, 보안통제 시험, 비상계획 시험에 대한 주요 성과 측정 기준은 매년 개선되었거나 개선이 필요한 분야를 확인하는데 여전히 유효하다[5,6].

OMB 지침에는 다음과 같은 주제를 비롯해 개별적인 FISMA 요건에 대한 구체적인 문항이 들어 있다.

- o 본래 문서감축법(Paperwork Reduction Act: 44 U.S.C. § 101 note)이 요구하는 대로, 기관에 의해서 또는 기관의 통제 하에 운영되는 주요 정보시스템 목록의 개발 및 유지. 정보보안통제의 감독, 시험 평가를 지원하기 위해 이 목록이 이용되어야 한다.
- o 다른 기관이나 하도급업체, 또는 그 기관을 대신한 다른 조직이 제공 또는 관리하는 것을 포함하여 기관의 운영과 자산을 지원하는 정보 및 정보시스템에 대한 정보보안 제공. 외부 제공자들을 이용하는 기관은 그 기관에 대한 위험이 허용 가능한 수준인지를 판단해야 한다.
- o 최소한으로 수용 가능한 시스템 설정 요건을 정하고 그에 부합하도록 보장. 아울러 기관들은 어느 정도까지 보안 설정(security configurations)을 해야 하는지를 설명해야 한다.
- o 기관의 정보보안 정책과 절차, 관행상의 모든 부족한 부분을 다루기 위한 개선책을 마련해서 이행하고 이를 평가하고 문서화하기 위한 실행계획 및 공정표(POA&M : Plan of Action & Milestones)의 개발. 공정표는 구체적인 프로그램과 시스템 차원의 보안 취약점, 개선 요구, 계획을 이행하는데 필요한 자원, 그리고 계획된 완수 일정을 구체적으로 적시하기 위해 기관이 사용하는 믿을만한 관리 도구이다.

개인정보보호 보고 지침에는 개인식별정보(PII)를 비롯한 민감한 정보에 대한 기관의 취급방식을 평가하기 위한 성과 측정 기준들이 포함되어 있다. 이 성과 측정 기준들은 전자정부법, 개인정보보호법, 그리고 관련 OMB 지침의 요구사항을 반영하고 있다. 이와 함께 각 기관은 개인정보영향평가(PIA)와 기록물 공지시스템(SORN)의 운용 링크가 나열된 기관 웹사이트 상의 중심 페이지의 URL을 제공해야 한다.

OMB Circular(회람) A-130은 연방정부의 문서감축법 구현을 명시한 행정명령으로, 모든 행정기관에 적용되는 정보자원관리정책을 규정하기 위하여 제정되었다[8].

동 회람의 주요 정책은 정보관리, 정보시스템 및 정보기술로 구성되어 있고. 정보관리는 생명주기에 따라 정보관리계획, 정보수집 가이드라인, 전자정보수집 가이드라인, 기록관리방안, 기관의 정보제공의무, 보안규칙수행 등을 명시하고 있다. 정보시스템 및 정보기술은 정보기술의 획득 및 활용을 위한 전략계획수립, 정보체계와 조직의 정보수요와의 연계, 연방정보처리 및 통신의 표준 사용, 정보기술 비용분석 등을 규정한다. 정보시스템 및 정보기술은 4 파트이며, 예산과 직접적 관련된 자본계획 및 투자통제를 자세하게 규정한다.

OMB A-130의 8b(3)은 정보보호와 관련하여 정부기관의 정보시스템의 보안을 보장하는 방법을 규정하고 있다. 정부기관은 반드시 정보와 시스템의 아키텍처에 사업 운영 전반을 지원할 수 있도록 보안대책을 수립하고, 예산계획 및 보안관리 생명주기와 정보시스템을 일치시켜야 하며, 정부기관은 NIST지침과 OMB정책을 준수하는 보안제도를 수립하고, 구현해야 한다.

OMB A-130 부록3은 연방 정보보안제도에 포함된 보안대책을 설명하고, 정보보안과 관련된 개별 연방정부기관의 책임을 명시한다.

OMB A-123은 정보보안 프로그램과 기관관리 통제 시스템과 관련이 있으며, [조항 3]에서 정보보안을 위하여 기관에서 보안이 보장된 프로그램의 유지·관리를 수행해야 한다.

NIST는 FISMA를 위한 정보보안 규격, 표준, 가이드라인을 개발하였다. 가이드라인은 각 연방정부가 활용하기 위한 정보자산 등급, 보안대책 선택, 문서화, 감시, 평가 및 인증(C&A)과정 등을 담고 있다. 가이드라인은 FIPS 및 SP 800 시리즈 등이다.

FIPS 199는 정보와 정보 시스템을 분류하는 표준을 개발하는 프로세스 등을 서술한다[9]. FIPS 199는

정보, 정보시스템의 보안분류 표준에 따라 공통의 프레임워크와 보안표준기준을 제공한다.

FIPS 199는 NIST 가이드라인 중 첫 번째로서, NIST의 개발 수명주기 중에서 최초 단계인 시작단계에 속한다. 시작단계에서 산출되는 문서는 최초의 업무내용을 정의하고, 보안 분류를 설명한다. 동 가이드라인은 손실의 잠재적인 영향에 따른 정보시스템의 그룹을 정의하고, FIPS 200, SP 800-53의 보안대책을 선택하는 가이드라인과 연결된다[11,12].

FIPS 200은 연방기관 정보와 정보시스템에 대한 최소 보안요구사항(Minimum Security Requirements for Federal Information and Information Systems)을 충족시키기 위해 필요한 보안통제를 위험에 따라 선택하는 과정을 규정하며, 정보보안을 위해 시스템에 필요한 시스템 등급기준을 제공하고, 연방기관내에 안전한 정보 시스템을 개발하여 도입 및 운용을 촉진시키는데 목적이 있다.

FIPS 200은 FISMA를 기초로 하고 있으며 SP 800-53을 통해 연방기관의 시스템에 필요한 보안대책 선택 기준을 제시하며, 최소 보안요구사항 항목은 다음과 같다[10].

- o 접근 통제(Access Control)
- o 식별 및 인증(Identification and Authentication)
- o 유지 보수(Maintenance)
- o 기록매체 보호(Media Protection)
- o 물리적 · 환경적인 보호(Physical and Environmental Protection)
- o 계획(Planning)
- o 인적 보안(Personnel Security)
- o 위험 평가(Risk Assessment)

SP 800-37 연방기관 정보 시스템의 보안 인증 및 승인 지침(Guide for the Security Certification and Accreditation of Federal Information Systems)은 연방기관 내의 정보시스템에 대한 보안 인증 및 승인을 위한 지침이다[13]. 동 지침은 연방기관이 안전한 정보시스템 구축을 위해 제정되었으며 지침의 목적은 아래 3가지이다.

- o 연방기관의 정보시스템에 대한 지속적인 평가
- o 정보시스템의 운영과 관련된 기관 업무의 위험성 이해
- o 의사결정자에게 보안승인에 필요한 신뢰할 수 있는 정보 제공

SP 800-53 연방기관 정보시스템의 보안대책(Recommended Security Controls for Federal Information Systems)의 목적은 연방기관 정보시스템의 보안대책 선택 지침을 제공한다[14,15]. 동 지침은 연방기관의 정보를 처리, 저장, 전송, 수신하는 정보시스템의 모든 구성요소에 적용된다.

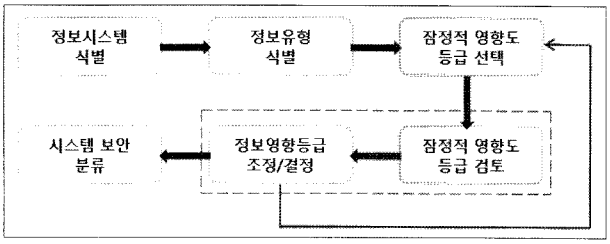

그림 3 SP 800-60의 보안분류 프로세스

SP 800-53은 FIPS 199와 SP 800-60에서 지정된 보안 분류를 통해 적절한 보안 대책의 선택을 서술한다.

SP 800-60 정보 및 정보시스템의 유형과 보안 분류의 적용 지침(Volume 1 : Guide for Mapping Types of Information and Information Systems to Security Categories)은 정보 · 정보 시스템 유형을 잠재적인 보안 영향에 따라 분류한 지침이다[16]. 동 지침은 연방기관이 보안영향등급을 정보 · 정보시스템에 일관성 있게 적용하기 위해 개발되었다. 정보의 유형은 각 정부 위원회 활동정보 및 연방기관의 일반적인 운영, 관리 및 지원 활동과 관련된 정보로 나뉜다. SP 800 - 60은 운영, 관리 및 지원정보를 관리지원정보라고 명명하고 있다. 임무 및 활동과 관련된 정보의 보안 특성은 연방기관에 따라 달라질 수 있고, 기관 내 조직에 따라 달라질 수 있다.

SP 800-60은 FISMA를 기초로 하고 있으며 FIPS 199의 보안 목표 및 영향 등급의 개요에 대한 세부적 지침을 제공하고 있다. SP 800-60은 FIPS 199의 세부 지침이므로 정보화 사업의 계획 수립 단계를 정의하고 있는 지침이다.

SP 800-64 보안을 고려한 시스템 개발 생명주기(Security Considerations in the SDLC : System Development Life Cycle)는 SDLC 단계상에서 검토해야 할 제어 관문(Control Gate)을 포함하고 있으며, SDLC를 다시 세부 항목으로 나누어 각 항목별로 고려해야 할 정보보안 사항을 제시하기 위하여 개발되었다[17].

SP 800-64는 FISMA를 기초로 하고 있으며, SDLC 단계별로 보안과 관련된 내용과 관련된 지침을 제공하고 있다. SP 800-64은 정보화 사업의 전 단계와 시스템의 종료 및 폐기에 이르기까지 보안을 고려하여 프로세스를 시행해야 한다고 제시하고 있다.

SP 800-70 IT 제품을 위한 보안 구성 점검표 프로그램 - 점검표 사용자와 개발자를 위한 지침(Security

Configuration Checklists Program for It Products – Guidance for Checklists Users and Developers)은 미리 정의된 환경에 맞는 제품을 구성하는 일련의 지침을 간단한 형식으로 문서화한 보안점검표의 사용자에게 보안 구성 점검표와 그 이점을 설명하고, NIST 점검표 프로그램을 사용해서 점검표를 검색 및 취득하는 방법의 설명을 제공하고, 개발자에 대해서는 NIST 점검표 프로그램 참여 정책, 절차, 일반적인 요구 사항을 본문과 부록에서 설명한다[18].

SP 800-70는 FISMA를 기초로 하고 있으며 점검표 프로그램의 요구사항은 FIPS 199, SP 800-53의 요구사항을 참조하여 개발되었다. SP 800-70은 앞서 정의된 보안 대책을 바탕으로 하여 보안 대책을 구현하는 단계로써, 그 도구로 점검표 프로그램을 사용하고 있다.

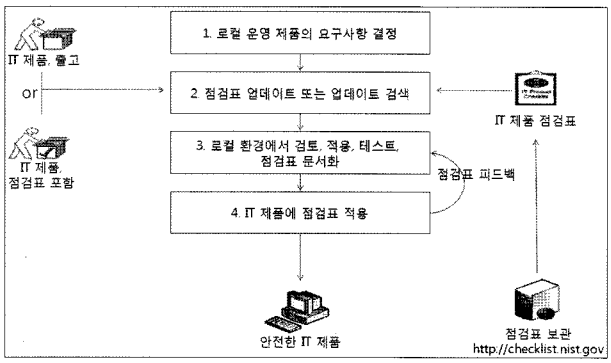

그림 4 점검표 사용자의 사용과정 개요

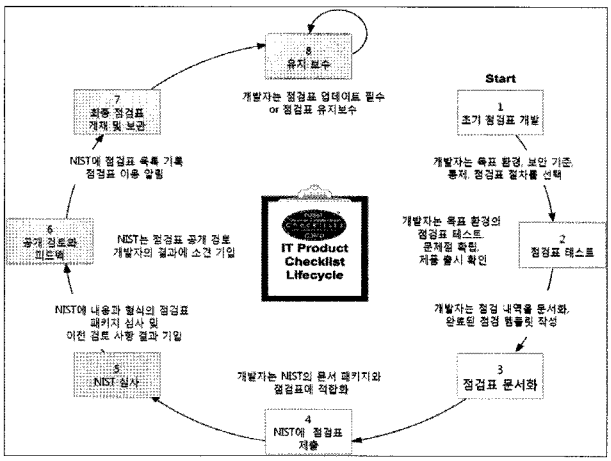

그림 5 NIST 점검표 프로그램의 개발 8 단계

3. 국내 법·제도 분석

정보보호 관련 국내의 법령, 제도 등을 정보시스템/정보자원, 정보보호솔루션, 프로그램(기준/수단), 역할/책임 등의 관점에서 분석하여 소프트웨어 보안강화 체계 확립에 활용할 수 있는 법·제도를 도출하고, 소프트웨어 보안강화를 위한 대안을 마련한다[1,2].

소프트웨어산업진흥법은 총 4장 36조로 구성되어 있으며, 주로 소프트웨어산업을 육성하기 위한 사항들을 정하고 있다. 특정 산업과 관련된 법률이기 때문에 정보보호와 관련하여 명확하게 언급되어 있는 조문은 없으나 제13조(품질인증), 동법 시행령 제9조(인증기관의 지정 등), 제9조의2(품질인증기준), 제10조(품질인증의 실시), 동법 시행규칙 제3조의3(소프트웨어 품질인증기관의 지정절차 등), 그리고 지식경제부 고시인 '소프트웨어 품질인증의 세부기준 및 절차'와 연결되어 있다. 다만, 본 조항들은 사전 점검이 아닌 사후 인증의 개념이라는 특징을 가지고 있다.

소프트웨어 품질인증 차원에서 접근하여 취약점을 제거하도록 유도할 수 있을 것이나, 이를 위한 지침이나 규정이 뒷받침되지 않아서 현장에 적용하지 못하고 있는 실정이다.

전자정부법은 총 7장 54조로 구성되어 있다. 정보보호와 관련하여 제12조(개인정보보호의 원칙), 제18조(전자문서의 송·수신), 제27조(정보통신망 등의 보안대책 수립·시행), 제39조의2(전자적 대민서비스 보안대책)과 시행령 제35조(전자문서의 보관·유통 관련보안조치), 제36조(이행여부의 확인), 제49조(전자적 대민서비스 보안대책의 범위)가 연결된 것밖에 없다. 하위 지침으로는 '행정기관 정보시스템 접근권한 관리규정', '전자정부사업 제안요청 지침', '전자정부지원사업 관리지침'이 있다. 하지만 이들 조항, 지침에서는 정보시스템 소스코드 보안취약성 사전진단 및 제거를 위한 사항에 대해서는 구체적인 언급이 되어있지 않다.

정보시스템의 효율적 도입 및 운영 등에 관한 법률은 정보기술아키텍처의 활용 촉진과 정보시스템 감리제도 확립을 위한 사항을 정하고 있다. 주요 대상으로는 정보기술아키텍처, 응용체계 소프트웨어, 시스템 소프트웨어, 서버 및 하드웨어, 네트워크가 있다.

본 법률은 총 23조로 구성되어 있으며 제7조(정보기술아키텍처의 도입·운영 지침 등)과 시행령 제9조(기술평가의 내용), 법령 제11조(공공기관의 정보시스템 감리)와 시행령 제11조(정보시스템 감리의 대상), 제12조(감리법인의 업무 범위 등)가 있다. 하위 지침으로는 '정보시스템의 구축·운영 기술 지침'이 있으나 정보보호와 관련하여 명확하게 언급되어 있는 조문은 없다.

정보통신망 이용촉진 및 정보보호 등에 관한 법률은 총 7장 76조로 구성되어 있다. 주로 정보통신망을 제공하는 사업자와 관련성이 있는 내용을 다루고 있

다. 정보보호와 관련하여 제4조(정보통신망 이용촉진 및 정보보호 등에 관한 시책의 마련), 제28조(개인정보의 보호조치), 제45조(정보통신망의 안정성 확보 등), 제46조(집적된 정보통신시설의 보호), 제46조의3(정보보호 안전진단), 제47조의3(이용자의 정보보호), 제48조의2(침해사고의 대응 등), 시행령 제3조(개인정보보호지침), 시행령 제15조(개인정보의 보호조치), 시행령 제37조(집적정보통신시설사업자의 보호조치), 시행령 제39조(정보보호 안전진단의 방법 및 절차 등)에서 언급하고 있다.

본 법률에서는 주로 네트워크, 정보시스템, 정보통신시설, 이용자의 보호를 위한 사항을 규정하고 있지만 정보시스템 소스코드 보안취약성 사전진단 및 제거를 위한 사항에 대해서는 언급되어 있지 않다.

국가정보화기본법은 국가정보화의 기본 방향, 국가정보화와 관련 정책의 수립·추진에 필요한 사항, 국가정보화의 역기능을 방지하기 위한 사항의 규정을 정하고 있으며, 주요 대상은 정보화를 추진하는 국가기관·지방자치단체, 지식정보자원, 정보통신망, 정보보호시스템 등이다.

정보보호와 관련하여 제37조(정보보호 시책의 마련), 제38조(정보보호시스템에 관한 기준 고시 등), 제39조(개인정보 보호 시책의 마련), 시행령 제35조(정보보호시스템의 보완 등)에서 언급하고 있지만 정보시스템 소프트웨어 보안이 아닌 솔루션 측면의 정보보호시스템을 강조하고 있다.

정보통신기반보호법은 주요정보통신기반시설의 전자적 침해행위에 대비하기 위한 방안을 규정하고 있으며, 주요 대상은 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등 정보통신기반시설의 업무와 관련된 전자적 제어·관리시스템 및 정보통신망이다.

본 법률은 총 7장 30조로 구성되어 있으나 주로 기반시설의 보호를 위한 내용을 정하고 있기 때문에 정보보호와 관련하여 제5조(주요정보통신기반시설보호대책의 수립 등), 제5조의2(주요정보통신기반시설보호대책 이행 여부의 확인), 제6조(주요정보통신기반시설보호계획의 수립 등), 제7조(주요정보통신기반시설의 보호지원), 제9조(취약점의 분석·평가), 제10조(보호지침), 제12조(주요정보통신기반시설 침해행위 등의 금지), 제16조(정보공유·분석센터), 시행령 제8조(주요정보통신기반시설보호대책의 수립), 시행령 제10조(주요정보통신기반시설보호계획의 수립), 시행령 제12조(주요정보통신기반시설 보호지원기관의 범위), 시행령 제18조(취약점 분석·평가 방법 및 절차), 제19조(정보공유·분석센터의 취약점 분석·평가), 시행령 제24조(정보공유·분석센터 구축의 통지) 등과 같이 다양하게 언급하고 있다.

본 법률에서의 정보통신기반시설은 물리적인 시설만을 의미하는 것이 아니라 전자적 제어·관리시스템과 정보통신망을 포함하지만 정보시스템 소스코드 보안취약성 사전진단 및 제거와 관련된 내용은 없다.

정보보호 관련 지침·훈령 등은 다음과 같은 것들이 있으나 모두 정보시스템 소스코드 보안취약성 사전진단 및 제거와 관련된 내용은 없다.

정보통신보안업무규정은 행정안전부 훈령으로 정보보호와 관련된 사후관리에 대한 업무 내용을 정의하고 있으며, 행정안전부와 그 소속기관, 특별시·광역시·도·특별자치도 및 시·군·구에 적용하고 있다.

행정기관 정보시스템 접근권한 관리 규정은 국무총리 훈령으로 정보시스템의 접근 시 사용자 규칙 및 운영 사항 등을 명시하고 있으며, 적용대상은 중앙행정기관(대통령실과 국무총리실을 포함한다) 및 그 소속기관과 지방자치단체이다.

전자정부 정보보호관리체계 인증지침은 행정안전부 훈령으로 정부·공공기관을 대상으로 체계적이고 효율적으로 정보보호관리체계를 구축할 수 있도록 정보보호 관리 과정과 활동 사항 등을 공통적으로 적용할 수 있는 표준 모델을 제시하고 있다.

정보시스템의 구축·운영 기술지침은 행정안전부의 지침으로 공공기관에서 정보시스템을 구축·운영함에 있어서 준수해야 할 기술과 표준을 정하고, 정보시스템의 상호운용성, 정보의 공동 활용, 정보시스템의 효율성 및 정보접근을 위한 기술적 편의성 등을 위한 기술평가에 필요한 사항을 정하고 있다.

전자정부사업 제안요청 지침은 행정안전부의 지침으로 전자정부사업 발주 시에 필요한 절차 및 내용을 제시하고 있다.

전자정부지원사업 관리지침은 행정안전부의 지침으로 전자정부지원사업의 선정·관리 등에 관한 사항과 그 시행에 필요한 세부사항을 제시하고 있다.

4. 국내·외 법·제도 비교분석

한국과 미국의 법제도 체계를 비교분석하여 우리나라 전자정부 환경에 맞는 적합한 방안을 도출하고자 한다.

미국은 법률이 US Code체계로 되어 있기 때문에 법률간 중복이 적고, 체계적으로 정비되어 있다. 국토안보와 관련된 사항은 국토안보부와 CIA에서 관리를 하고, 정보보호와 관련된 사항은 FISMA법을 통하여

OMB에서 관리하는 특징이 있다.

FISMA법을 통하여 기관의 역할, 보안프로그램, 지침·가이드라인의 활용, 솔루션 활용, 기술센터의 활용 등 정보보호를 위한 노력 전반에 걸쳐 의무화하고 있으며, NIST의 가이드라인인 FIPS, SP문서를 통하여 보안대책의 프로세스별 필요활동을 보여주고 있다.

한국의 정보보호 관련 법률은 개별 목적이 따라 제정되었고, 법률의 대상도 다르게 되어있다. 그 결과 미국의 FISMA법과 같은 정보보호 전반을 관리하는 법률이 없는 상황이다.

또한, 국내 법률 제·개정 시에 발생하는 부처 간 이해관계와 절차로 인하여 정보보호 전반을 관리하는 법률의 제·개정은 현실적으로 많은 어려움이 발생하고 있는 상황이다.

국내 정보보호 관련 체계는 미국의 ISMA와 다르게 여러 법률에서 개별적으로 담고 있다. 이는 여러 가지의 현상적 이슈를 초래할 수 있다.

첫째, 정보보호에 대한 총체적 대책 마련을 어렵게 하고 있다. 정보보호에 관한 역할과 책임이 여러 법에 흩어져 있다 보니, 이 전체를 아우르는 역할과 책임의 소재에 대한 많은 의문이 제기되고 있다. 이는 보안사고가 일어날 때 마다 언론에서 제기되고 있는 정보보호 컨트롤 타워의 부재와 일맥상통한다고 하겠다.

둘째, 해킹 등과 같은 보안 침해 기술이 날로 증대하고 있는 현실에서 신속한 대응을 어렵게 한다. 우리 정보보호 법률 체계는 대상별로 정보보호 내용을 포함하고 있다 보니, 새로운 보안 대책 또는 기법이 필요하다 하더라도 이를 여러 법에 정확하게 녹여 넣는 게 매우 어려운 작업일 수 있다.

이런 문제점의 극복을 위해서는 정보보호 관련 법체계의 전면적 수정 및 보완이 필요하다고 하겠다. 그러나 우리의 법체계적 특성과 관련 정부부처간의 이해관계 충돌 등으로 인해 단시일 내에 이의 전면적 수정보완은 쉽지 않은 상황이다.

5. 소프트웨어 안전성 및 신뢰성 향상을 위한 법·제도적 접근

가장 효과적 방안으로는 미국의 FISMA와 같은 정보보호와 관련된 총괄 법안을 제정하는 것이나, 현실적인 접근 방법으로 관련 법률의 전면 수정 및 보완이라는 원칙 하에 가능한 수준에서 기존 법률의 개정 및 보완을 꾀하고, 아울러 구체성이 부족한 부분은 「전자정부지원사업 관리지침」, 「정보시스템의 구축·운영 기술 지침」, 「전자정부법 및 동법 시행령을 근거로 하는 새로운 지침의 제정」 등을 통하여 보완해나가는 방법을 택하는 것이라 하겠다.

5.1 전자정부법을 활용한 방안

제27조(정보통신망 등의 보안대책 수립·시행)을 활용한 적용 방안으로 보안대책 수립·시행의 요소로서 정보시스템을 기획하는 단계부터 운영·유지보수하는 전체 과정에서 소프트웨어에 대한 오류·결함·결점·보안취약성 등을 사전에 점검·진단하여 제거하는 '소프트웨어 견고화(Secure Coding)' 기술을 적용하는 것이다.

제39조2(전자적 대민서비스 보안대책) 활용한 방안으로 행정기관에서 하는 업무는 궁극적으로 국민을 위한 것이다. 전자정부법 시행령 제49조(전자적 대민서비스 보안대책의 범위) 4호에서는 '전자적 대민서비스 제공 시스템에 대한 보안'이 포함되어 있다. 이에 전자적 대민서비스 시스템의 보안을 위하여 전자정부법 제39조의2(전자적 대민서비스 보안대책)의 일환으로 '소프트웨어 견고화(Secure Coding)'를 적용하여 세부지침을 제정하는 것이다.

'전자정부법'에서 언급하고 있는 정보통신망에는 네트워크뿐만 아니라 응용시스템도 포함된다고 정의된다. 또한 '전자정부법'이라는 법률을 근거로 하기 때문에 실행력이 담보될 수 있다. 따라서 '전자정부법'에 '소프트웨어 견고화'를 적용하는 것이 가장 적절하다고 판단된다. 하지만 '전자정부법'을 통하여 적용할 경우에는 관계 기관과의 협의가 필요하기 때문에 상호간 의견조율이 중요하다.

5.2 정보시스템의 효율적 도입 및 운영 등에 관한 법률을 활용한 방안

정보시스템의 효율적 도입 및 운영 등에 관한 법률은 정부의 정보화투자의 효율성을 높이기 위해 정보시스템을 도입하고, 이를 위하여 정보기술아키텍처를 활용하고 있다.

정보기술아키텍처는 업무, 응용, 데이터, 기술, 보안 등 조직 전체의 정보화 구성요소의 구조적으로 정리한 체계와 정보시스템을 효율적으로 구성하기 위한 방법으로 구성되어 있다. 본 법령의 정보기술아키텍처의 도입·운영을 분석하면 정보기술아키텍처의 체계는 도입과 관련성이 있고, 방법은 정보기술아키텍처의 운영과 관련성이 있다. '소프트웨어 견고화'는 취약성 검토를 하기 위한 방법 중의 하나이기 때문에 본 조항의 정보기술아키텍처의 도입·운영 지침을

근거로 삼을 수 있다고 판단된다.

또한, 감리요소에 '소프트웨어 견고화'를 포함하여 수행할 수 있는데, 감리란 갑과 을이 아닌 제3자가 시스템 개발이 시행되는 과정에서 계약서, 시행계획서에 따라 개발되고 있는지 여부를 감독하는 것이기 때문에 '소프트웨어 견고화'가 감리의 일부 요소로 볼 수 있다고 판단된다.

5.3 국가정보화기본법을 활용한 방안

국가정보화 기본법은 정보를 처리·유통하는 과정에서 안전성 확보와 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적·기술적 수단인 정보보호시스템, 개인정보의 보호시책을 마련하여야 한다고 정하고 있다.

따라서, '소프트웨어 견고화'는 시스템의 취약성을 분석하여 안전성을 높이기 위한 방법이므로 정보보호 시책의 일환으로 포함된다고 볼 수 있다. 그렇기 때문에 국가정보화 기본법의 제37조를 '소프트웨어 견고화' 적용의 근거로 삼을 수 있다고 판단된다.

'소프트웨어 견고화'는 취약성 진단을 통해 보유하고 있는 정보를 보호하기 위한 방법이기 때문에 정보보호시스템의 일환으로 포함될 수 있다. 하지만 정보보호시스템은 솔루션의 개념이 크기 때문에 '소프트웨어 견고화' 적용의 근거로 정보보호시스템에 관한 기준으로 삼기에는 무리가 있다고 판단된다.

5.4 정보통신기반보호법을 활용한 방안

'정보통신기반 보호법'에서 말하는 정보통신기반시설은 일반적으로 말하는 기반시설이 아니라 전자적 제어·관리시스템 및 정보통신망을 의미하며, 정보통신기반시설에 대한 보안대책을 마련하여야 한다고 정하고 있다.

주요정보통신기반시설 보호대책은 주요정보통신기반시설을 안전하게 보호하기 위한 물리적·기술적 대책을 포함한 관리대책을 말한다. '소프트웨어 견고화'는 취약점을 분석하는 기술적인 방법으로 볼 수 있기 때문에 주요정보통신기반시설의 기술적 보호대책을 근거로 삼아 '소프트웨어 견고화'를 적용할 수 있다고 판단된다.

5.5 법률 종합분석

'정보통신기반 보호법'은 '소프트웨어 견고화'를 적용하는데 있어서 적용대상 측면에서 적절한 법률로 판단된다. 하지만 '정보통신기반 보호법'은 2008년 정부의 조직개편으로 이후 여러 부처 간 이해관계가 얽혀있는 상태이다. 따라서 '정보통신기반 보호법'을 통하여 '소프트웨어 견고화'를 적용하는 것은 쉽지 않을 것으로 생각된다.

'국가정보화 기본법'은 국내 정보화 관련 법률이나 하위 지침들의 모법으로 범용 용도로는 최적화된 법률로 판단된다. 하지만 법 조문의 성격 상 주로 정보보호시스템에 대한 내용측면에 치우쳐있고, '소프트웨어 견고화'를 위한 응용시스템은 포함되고 있지 않다. 따라서 '국가정보화 기본법'을 통하여 '소프트웨어 견고화'를 적용하는 것은 적절하지 않다고 보인다.

'정보시스템의 효율적 도입 및 운영 등에 관한 법률'의 감리의 일부분으로 '소프트웨어 견고화'를 적용하는 것이 가능하다고 판단된다. 하지만 감리는 감리기관의 준비가 필요하기 때문에 시간이 오래 걸릴 수 있다. 그리고 본 법률은 '전자정부법'에 흡수·통합되는 새로운 '전자정부법'으로 탄생하게 되었기에 '소프트웨어 견고화'를 적용하는 것이 적절하지 않다고 보인다.

'전자정부법'에서 언급하고 있는 정보통신망에는 네트워크뿐만 아니라 응용시스템도 포함된다고 보여진다. 또한 법률을 근거로 하기 때문에 실행력이 담보될 수 있기 때문에 '전자정부법' 및 시행령을 통해 '소프트웨어 견고화'를 적용하는 것이 가장 적절하다고 판단된다.

기존 법률을 통하여 '소프트웨어 견고화'를 담는 것은 내용의 구체성이 떨어지기 때문에 온전하게 적용하기 힘들어 보인다. 법률의 변화가 필요한 실정이다. 하지만 법제도의 제·개정은 절차상의 어려움과 타 부처와의 의견충돌로 인하여 시간이 많이 걸리고, '소프트웨어 견고화'의 내용을 담을 수 있다고 담보할 수 없다.

법률 개정에 오랜 시간이 소요될 것으로 보이기 때문에 과도기적인 방안으로 법률 하위 지침에 포함하여 적용하는 방안이 현실적으로 바로 적용할 수 있을 것으로 본다.

'소프트웨어 견고화'를 효과적으로 적용할 수 있는 지침으로 전자정부법을 기초로 하는 '전자정부지원사업 관리지침'과 '정보시스템의 구축·운영 기술 지침'을 살펴본다.

전자정부지원사업 관리지침 제23조(표준화 및 보안)에서는 보안과 관련된 사항이 구체적으로 언급되고 있지 않다. 이에 보안부분의 내용에 '소프트웨어 견고화' 관련 내용을 삽입하는 조문 개정을 통하여 '소프트웨어 견고화'를 적용하는 것이다. 본 지침은 행안부 예규이고 전자정부지원사업을 대상으로 하고 있기 때문에 모든 공공기관에의 적용가능성에 대한 전문가 의견수렴이 필요하다.

정보시스템의 구축·운영 기술 지침은 행정기관이 정보시스템을 구축·운영함에 있어서 준수해야 할 기술·표준과 기술평가에 필요한 사항을 규정하고 있다. 그렇기 때문에 모든 공공기관에의 적용가능성이 높다고 보여진다. 또한 가이드라인 제정의 형태로 되어 있기 때문에 내용의 구체성도 높다고 보인다. 또한 지침의 개정이기 때문에 법령을 활용하는 것에 비하여 추진의 적합성은 높다고 판단된다.

'소프트웨어 견고화'란 보안상의 허점 및 취약점을 최대한 배제하여, 외부 공격으로부터 충분히 견뎌낼 수 있는 소프트웨어를 개발하기 위한 일련의 노력을 의미하기 때문에 '응용시스템 보안'영역으로 정의하는 것이 적절하다고 볼 수 있다.

추가로 고려해 볼 수 있는 사항으로 전자정부법 및 동법 시행령을 근거로 '소프트웨어 견고화'를 목적으로 한 새로운 지침을 제정하여 정부·공공기관에 적용시키는 것도 좋은 방안으로 본다.

6. 결 론

본 연구는 정부·공공기관에서 개발·구축되는 정보시스템의 소프트웨어 취약성을 사전에 자동 진단하여 제거하도록 하여 시스템의 안전성과 신뢰성을 확보하기 위한 것으로, '소프트웨어 견고화' 적용을 위하여 '법령 및 시행령의 개정', '지침의 개정', '새로운 지침의 제정' 등의 3가지 노력의 병행이 필요함을 도출하였다. 여러 가지 방안은 정보시스템 보안강화체계를 위한 '소프트웨어 견고화'를 할 수 있는 가능성을 담고 있다. 그러나 위에서 제시된 방안을 실제로 적용할 때 법적 해석의 어려움 및 타 기관과의 이해관계가 얽혀있어서 실제로 현장에 적용하고자 할 때 과정이 복잡하고 장시간이 소요될 수 있을 것으로 본다. 따라서 법률 자문을 통해 위와 같은 한계점을 최대한 빨리 극복하고 보다 구체적으로 적용 방안을 강구할 필요가 있다.

정보시스템 소프트웨어 안전성 확보의 제도화를 통하여 국내 행정기관 정보화 사업 시 사업기획 단계부터 운영·유지보수 단계까지 전체 과정에 적용하는데 기초자료로 활용되기 바라고, 국가에서 도입하는 정보시스템 개발완료 이전에 프로그램 내의 취약점을 사전 제거하여 우리나라 전자정부의 안전성과 신뢰성이 대폭 향상되기를 기대한다.

참고문헌

[1] 한국경영정보학회, "정보시스템 보안강화체계 적용을 위한 제도화 방안개발", 한국인터넷진흥원, 2009. 12.

[2] 행정안전부, "행정기관을 위한 정보화사업 단계별 관리·점검가이드", 2008. 12.

[3] 행정안전부, "정보보호 중기 종합계획", 국무회의 보고자료, 2008년 8월.

[4] FISMA : Federal Information Security Management Act of 2002

[5] OMB, "Fiscal Year 2008 Report to Congress on Implementation of The Federal Information Security Management Act of 2002", OMB, 2009.

[6] www.whitehouse.gov/omb

[7] Homeland Security Presidential Directive / HSPD-7

[8] OMB Circular No. A-130, OMB

[9] NIST FIPS Pub 199 Standards for Security Categorization of Federal Information and Information Systems, NIST, Feb. 2004

[10] NIST FIPS Pub 200 Minimum Security Requirements for Federal Information and Information Systems, NIST, Mar. 2006

[11] NIST Special Publication 800-18 Rev. 1 Guide for Developing Security Plans for Federal Information Systems, NIST, Feb. 2006

[12] NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems, NIST, Jul. 2002

[13] NIST Special Publication 800-37 Rev 1 Guide for the Security Certification and Accreditation of Federal Information Systems, NIST, Aug. 2008

[14] NIST Special Publication 800-53 Rev 3 Recommended Security Controls for Federal Information Systems and Organizations, NIST, Aug. 2009

[15] NIST Special Publication 800-53A Guide for Assessing the Security Controls in Federal Information Systems, NIST, Jul. 2008

[16] NIST Special Publication 800-60 Rev 1 Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices, NIST, Aug. 2008

[17] NIST Special Publication 800-64 Rev 2 Security Considerations in the System Development Life Cycle, NIST, Oct. 2008

[18] NIST Special Publication 800-70 Rev 1 National Checklist Program for IT Products-Guidelines for Checklist Users and Developers, NIST, Sep. 2009

김 성 근

미국 New York 대학교에서 정보시스템 전공으로 박사학위 취득 후 동 대학 전임강사를 거쳐 중앙대학교 상경학부 교수로 근무중. 현재 국가정보화 전략위원으로 국가정보화 체계 개편을 위한 특별위원회 위원장으로 활동중임. 아울러, 한국EA포럼 의장, 한국CIO포럼 대표간사로 활동 중이다.

관심분야 : Enterprise Architecture, IT Governance 등
E-mail : sungkun@gmail.com

최 명 길

1993 부산대학교 학사
1995 부산대학교 석사
2004 한국과학기술원 박사
1995～2000 국방과학연구소 연구원
2000～2005 한국전자통신연구원 국가보안기술연구소 선임연구원
2005～2007 인제대학교 조교수
2008～현재 중앙대학교 조교수
관심분야 : 보안성평가, 홈네트워크 보안, 정보보호정책 및 관리
E-mail : mgchoi@cau.ac.kr

한 근 희

1986 서울산업대학교 컴퓨터학과 학사
1988 한양대학교 공과대학원 컴퓨터학과 공학석사(정보보안 전공)
2006 고려대학교 대학원 컴퓨터학과 이학박사(정보보안 전공)
2006～현재 행정안전부 정보보호정책과 근무
2002～현재 건국대학교 정보통신대학원 겸임교수
관심분야 : 인터넷 보안, 통합보안관리, 모바일 보안, 차세대 인터넷 등
E-mail : hankeunhee@nate.com, khhan@korea.kr