

계층분석기법을 활용한 전장관리정보체계 소프트웨어 시큐어 코딩룰 선정 평가 방안

최준성*, 김우제*, 박원형**, 국광호^o

Evaluation Method Using Analytic Hierarchy Process for C4I SW Secure Coding Rule Selection

June-sung Choi*, Woo-je Kim*, Won-hyung Park**, Kwang-ho Kook^o

요 약

본 연구에서는 적용대상체계에 적합한 시큐어 코딩룰을 선정 평가하기 위한 방안으로, 적용대상 체계의 특성에 따른 체계적용적합성(개발언어적합성, 플랫폼적합성), 위협평가(침해의 심각성, 침해의 가능성), 적용기대효과(신뢰성/품질향상, 수정 비용) 등을 종합적으로 고려한 시큐어 코딩룰의 선정 평가 방안을 제시하였다. 이를 활용하여, 전장관리정보체계의 체계 특성에 부합하는 197개의 시큐어 코딩룰을 선정하였다. 또한 선정된 각 코딩룰 별로 대상 체계에 대한 적용을 위한 우선 순위를 산정하였다.

Key Words : SW Secure Development, Secure Coding, Warfare System Software, C4I Systems SW

ABSTRACT

In this study, we suggest the selecting evaluation method considering 6 major factors like Compliance system application (Development language conformance, Platform Compliance), threat evaluation (criticality of security incident, possibility of security incident), application benefit (Reliability / quality improvement, Modify Cost) for appropriate secure coding rule selecting evaluation. Using this method, we selected and make a set consist of 197 secure coding rules for Battlefield Management System Software. And calculated the application priority for each rules.

I. 서 론

최근 몇 년간 사회 기반망에 대한 사이버 위협들이 급격하게 증가하고 있다. 사회기반망에 대한 사이버 위협의 증가와 아울러, 실제 전쟁의 전초전으로써, 혹은 비대칭 전력 전개를 통한 병행전인 사이버전의 발생 가능성도 높아지고 있다. 기존에는 사이버전이 단 순히 컴퓨터 네트워크 내부에서만 발생하는 문제로

이해되었다. 그러나, 사회기반망과 무기체계들의 컴퓨터 소프트웨어와 네트워크에 대한 의존도가 증가하면서, 사이버전에서의 위협은 실체화된 위협으로 변화하고 있다. 최근 몇 년간 지속된 각종 사이버 위협, 특히 3.20 사이버 공격의 피해 이후, 실체화된 사이버 위협과 사이버전에 대한 위기감이 증가하고 있다. 우리는 사회 기반시설과 지휘통제통신망의 구성에 있어서 북한에 비해 사이버 의존도가 높다. 북한의 경우, 산업

※ 이 연구는 서울과학기술대학교 교내 학술연구비 지원으로 수행되었습니다.

• 주저자 : 서울과학기술대학교 IT정책전문대학원 산업정보시스템전공, where@seoultech.ac.kr, 학생회원

◦ 교신저자 : 서울과학기술대학교 기술경영융합대학 글로벌융합산업공학과 산업정보시스템, khkook@seoultech.ac.kr, 정회원

* 서울과학기술대학교 기술경영융합대학 글로벌융합산업공학과 산업정보시스템, wjkim@seoultech.ac.kr

** 극동대학교 공학계열 사이버안보학과, whpark@kdu.ac.kr

논문번호 : KICS2013-06-266, 접수일자 : 2013년 6월 27일, 최종논문접수일자 : 2013년 7월 30일

발전과 개방화의 미진함으로 인한 컴퓨터 네트워크와 인터넷의 발전이 미비한 면을 가지고 있다. 그러나, 군사적인 측면에서는 의도적으로도 전자전 및 사이버전의 영향을 최소화할 위해 전자장비와 컴퓨터 네트워크 의존성을 높이지 않는 경우도 있는 것으로 알려져 있다²⁴⁾. 사이버전은 정보체계와만 관련이 있을 것으로만 판단하는 경향이 많다¹¹⁾. 그러나, 이미 사이버전에서의 무기체계에 대한 위협에 대한 우려들은 현실화되고 있다. 특히, 사이버전은 소프트웨어에 의존하고 있는 현대 무기체계에 있어서는 치명적인 부분이 될 것으로 예상되고 있다. 그 구체적인 면을 살펴보자면, 기존 무기체계에 비해 현대 무기체계들은 기능 구현을 하드웨어에만 의존하지 않고, 소프트웨어로 기능을 구현하고 있다. 특히, 항공우주와 정밀기기와 등의 분야에서는 소프트웨어의 의존성이 더욱 커지고 있는 것으로 알려져 있다. F-22와 F-35 같은 전투 항공기들의 경우, 소프트웨어에 대한 의존성이 현재 80%를 상회하는 것으로 알려져 있다^{6,7,11)}. 관련된 최근 연구결과에 따르면, 항공기와 자동차 등에 탑재된 내장형 시스템의 소프트웨어들은 보안에 취약하다. 의외로 침입이 매우 용이하여, 스마트폰 수준의 장비로도 해킹이 가능한 경우가 있다는 사실이 알려진 바도 있다^{10,11)}. 기존 전쟁 수행의 양상에서 사이버전과 가장 유사한 성격을 가진 것으로는 전자전을 들 수 있다. 전자전의 경우 구소련과 북한 등은 전자장비 교란에 의한 전쟁 수행상의 문제를 예방하기 위한 목적을 가지고 의도적으로 전자장비의 의존도는 최소한으로 줄이는 한편, 전자장비에 대한 전자교란 공격기술과 각종 전자정보 작전과 관련된 교리들을 지속적으로 개발하고 발전시켜 것으로 알려져 있다²⁴⁾. 이에 비해 우리는 국가정보화를 위해 많은 노력을 기울여 왔고, 타 공공분야와 마찬가지로 군사분야의 경우에도 지휘 통제분야를 비롯한 무기체계 전반에 걸쳐 소프트웨어와 컴퓨터 네트워크에 대한 의존성이 지속적으로 증가되어왔다. 그러므로, 향후 실체적 위협이 증가되고 있는 사이버전 환경에서 무기체계 무력화를 위한 사이버 공격들이 발생하는 경우, 적에 비해 사이버 위협에 의한 타격이 클 것으로 예상된다. 무기체계에 대한 사이버 위협을 감소시키기 위한 방안들에는 암호화, 망분리의 강화, 통신프로토콜의 강화, 접속 통제 관점에서의 접속 권한 인증 방법의 강화 등 여러 가지 방안들이 있을 수 있다. 본 연구에서는 이러한 무기체계에 대한 사이버 위협 감소 방안들 중에서, 무기체계 소프트웨어의 소프트웨어 개발 보안의 관점에서 시큐어 코딩룰을 적용하기 위해 시큐어 코딩룰을 선정하는

방안에 대해서만 한정하여 논의하고자 한다. 본 논문의 1장 서론에서는 무기체계 소프트웨어 개발 분야에서 시큐어코딩룰의 필요성을 설명한다. 2장에서는 관련연구를 설명한다. 3장에서는 연구방법과 절차를, 4장에서는 시큐어 코딩룰의 선정평가 방안과 선정평가 적용 대상인 전장관리정보체계 시큐어 코딩룰 선정평가 결과를 설명한다. 5장에서는 결론과 향후 연구방향을 정리한다.

II. 관련 연구

무기체계 소프트웨어의 개발단계에서부터 취약점을 제거하기 위한 시큐어 코딩의 적용이 필요하다^{6,7)}. 그러나, 아직까지 국내에서는 무기체계 소프트웨어에 대해서는 시큐어 코딩룰에 대한 적용 의무화가 본격적으로 논의되지 않고 있으며, 무기체계 소프트웨어의 보안성을 보완하고 발전시킬만한 시큐어 코딩룰 개발 방안과 평가 방안, 적용방안 등이 충분히 논의되고 있지 못하다. 학술적으로는 방대한 무기체계 소프트웨어와 국방소프트웨어를 분류하여 각각의 분야별로 개발 보안을 적용하고자 하는 연구^{6,7)}만이 시도되고 있을 뿐이다. 국내 국방분야와 무기체계 분야에서의 시큐어 코딩과 개발보안에 대해서 전반적으로 학술적인 연구와 실무적 논의 모두 매우 미흡한 실정이다. 최근 공공기관 개발보안 적용 의무화 적용 이후, 공공기관 정보화 및 보안분야와 금융전산보안 분야의 경우에는, 시큐어 코딩과 소프트웨어 개발보안은 소프트웨어 개발과 관련하여 코드 리뷰를 위한 기준과 기법에 대해 주로 실무적인 접근을 중심으로 급격하게 발전하고 있다. 그러나, 이 분야 역시 현재까지 학술적으로는 많은 연구들이 이루어지고 있지는 않은 실정이다. 기존 국내에서의 시큐어 코딩룰은 외국의 취약점 분석 공개 목록과 시큐어 코딩룰을 참조하여, 시큐어 코딩 목록을 생성하고, 취약점목록의 상위권 취약점과 시큐어 코딩룰을 매핑하는 형태로 개발되었다. 국외의 시큐어 코딩룰 개발의 경우, 소프트웨어 관련 연구기관에서 정부기관이 연구용역을 통해 언어별 특성에 따라 발생할 수 있는 취약점을 특성별로 분석하여, 평가하고, 목록화한 다음, 해당 언어별 취약점들을 취약점 분석 공개 목록과 매핑하여 개발 언어별 프로그래밍의 취약점 목록을 도출하는 방식으로 개발되었다²¹⁻²³⁾. 이러한, 방식은 기존 개발 언어 표준 연구와 취약점 분석이 추가 된다. 2012년에 행정안전부가 개발보안 의무화 제도를 시행하면서 제시한 코딩룰의 경우, 전자정부프레임워크 개발보안에 대한 시큐어 코딩룰을

기존 개발언어 표준과 취약점 분석과 매핑하여 개발하는데에도 연구용역으로 수 개월에서 수년이 소요되었다. 그러나, 이러한 방식으로 구성된 시큐어 코딩룰들은 적용될 체계에 최적화되지 않고, 개발언어의 특성을 중심으로 구성된 일반적인 목록의 성격을 가지고 있다. 많은 룰을 가지고 있을수록 보다 나은 대응을 할 수도 있겠지만, 개발 제한성이 높아진다. 또한, 테스트 비용도 증가하게 되므로, 적정선을 찾는 것이 필요하다. 이를 위해 적용 우선순위를 고려하여 시큐어 코딩룰을 선정하는 것이 필요하다. 또한, 유사한 룰들이 중복되게 포함되는 경우도 있다. 현재 제공되고 있는 정부의 지침의 경우에도, 유사한 룰의 중복이 상당수 발견되고 있다. 시큐어 코딩룰의 적용 여부는 정적 검사 툴에 의한 자동화 검사를 통한 코드 리뷰를 통해 검증되는 것이 일반적인 절차이다. 많은 룰이 중복되어 적용되는 경우 오탐이 증가하여 검토 결과를 확인하기 어렵다. 또한, 개발된 코드의 수정 과정도 매우 어려우며, 수정과정에서 추가적인 오류가 발생하는 문제들도 있다. 그러므로, 적용 대상 체계에 적용 우선순위가 선별되어 최적화된 코딩룰을 개발하여 활용하는 것이 필요하다. 향후 증가하는 사이버전 위협에 따라, 소프트웨어를 탑재한 모든 무기체계들은 각 무기체계별 특성에 따른 최적화된 시큐어 코딩룰의 개발과 적용이 필요할 것으로 예상된다. 그러나, 매번 새롭게 처음부터 개발하는 것은 많은 예산과 인력이 투입되어야 하는 일어서서 거의 불가능한 일이다. 또한, 기존에 개발 언어별 표준으로 제정된 룰을 중복되게 개발하는 것은 큰 의미가 없다. 오히려, 기존 개발 언어 표준 룰들에서 적용 대상 체계에 적합하게 선별적으로 룰을 적용하는 것이 필요하다.

시큐어 코딩(Secure Coding)은 소프트웨어의 개발과정에서 소프트웨어 개발 언어의 사용에서 정의되지 못한 논리적 오류와, 설계 구현과정에서 개발자의 실수로 인해 발생할 수 있는 보안취약점들을 줄이기 위한 일련의 보안성 향상 활동을 의미하며, 경우에 따라 조금씩 다른 의미들을 가지고 있기도 하다^{6,7)}. 2012년도 행정안전부 지침에 의하면, 소프트웨어 개발보안(Secure Coding)은 해킹 등 사이버공격의 원인인 보안약점을 개발단계에서 사전에 제거하여 안전한 소프트웨어를 개발하는 기법이다. 소프트웨어 보안약점(Weakness)은 소프트웨어 결함, 오류 등으로 해킹 등 사이버공격을 유발할 가능성이 있는 잠재적인 보안취약점을 의미한다^{12,13)}. 시큐어 코딩룰은 형태적으로 기존에 소프트웨어 품질이나 신뢰성 향상을 위해 사용되던, 코딩룰(Coding Rule)과 코드 리뷰(Code

Review)와 유사하다²¹⁾. 또한, 소프트웨어 품질이나 신뢰성 분야에서 사용되는 권장 코딩룰은 상당 부분 보안을 위한 코딩룰에도 포함되고 있다. 그러나, 시큐어 코딩룰은 보안성 향상을 목표로 하고 있어서, 개발언어별 특성에 따라 발생하는 소프트웨어 취약점 분석을 통해 개발되고 있다. 취약점 판단과 분석 근거로는 OWASP(The Open Web Application Security Project)의 웹보안 위협 상위 TOP 10 목록, CWE(Common Weakness Exposure), CVE(Common Vulnerability Exposure), SANS Top 25 Software Errors 등의 보안 취약점 공개 목록들이 주로 활용되고 있다^{6,7)}. 그런데, 이런 취약점 분석들은 그 분석대상을 일반에서 많이 사용하는 정보체계를 중심으로만 하고 있다는 한계가 있다.

표 1. 시큐어 코딩 관련 기존 문헌
Table 1. Secure Coding Literature Review

Author	Contents
Junesung choi, Wooje Kim, Wonhyung Park, Kwangho Kook (2012)	Classification for weapon systems and application level of defense SW ^{[6][7]}
Kim dongwon, Han geunhui (2012)	Self-evaluation method of Mobile Secure Coding ^[4]
Ban gjiho, Ha lan (2013)	Evaluation method of diagnostic tool to evaluate security weaknesses ^[1]
Jeong dahye, Choej inyeong, Lee songhui (2013)	Nuclear-related Software analysis based on secure coding ^[2]
Han gyeongsuk, Kim TaeHwan, Ha giyoung, Im jaemyeong, Pyochangwoo (2012)	An Improvement of the Guideline of Secure Software Development for E-Government, ^[3]
Kim seonggeun, Lee jaeil (2012)	Secure Coding in Software Development ^[5]
Lee Buyoon (2011)	Alerts on Car hacking vulnerability ^[10]
NorHarisah Zainuddin (2011)	Secure Coding in Software Development ^[18]
Kittipong Kittichokechai (2011)	Secure Source Coding with Action-dependent Side Information ^[19]
Ravi Tandon (2011)	Secure Source Coding with Tool Helper ^[20]

시큐어 코딩은 표준의 제정과 적용, 코드리뷰와 같이 다분히 실무적인 접근만이 중심을 이루고 있다. 그러므로 소프트웨어 공학의 다른 분야들에 비해, 상대적으로 현재까지 많은 연구가 이루어지고 있지는 않다.

기존 문헌연구는 [표 1]과 같이 정리할 수 있다. 기존 문헌 연구를 통해 확인할 수 있는 것은 시큐어 코딩에 대한 기존 연구들은 연구자들 각자의 관심분야로 연구 영역이 산재하고 있어 그 연구가 체계적이지 못하다. 무기체계 소프트웨어 분야의 경우에는 기존 정보체계 분야와는 기존 정부 개발보안 가이드 등의 지원이나 공식적인 기준이나 표준이 준비되지 않은 상황임을 알 수 있다. 앞서 살펴본 바와 같이, 일반적인 시큐어 코딩이나 개발보안에 비해, 국방 분야와 무기체계 분야에 대한 사이버 위협과 관련된 시큐어 코딩이나 개발보안과 관련된 학술연구와 실무적 논의는 현재 그 필요성에 비해 미비하다.

본 연구의 연구자는 기존 선행 연구에서 무기체계 분야에서 시큐어 코딩률의 적용과 관련해서는 국방 분야 특히 무기체계는 그 분야가 다양하므로, 개별 무기체계분야별 해당 무기체계 특성에 적합한 무기체계 시큐어 코딩률의 개발이 필요함을 제시하고, 국방SW와 무기체계 SW에 대한 개발보안 적용 대상 계층을 8대 무기체계 기준으로 분류하였다^{6,7)}. 국내에서 활용되는 정부지침에서는 공공기관의 정보시스템이 JAVA SPRING 프레임워크 기반인 전자정부 프레임워크 (E-Gov Framework)을 활용하여 개발된다는 점에 착안하여, 전자정부 프레임워크 기반 개발에서 개발보안을 적용할 수 있도록 주요 43개 취약점 해소를 위한 43개의 시큐어 코딩률로 개발하여 7개 특성으로 분류하였다¹⁴⁻¹⁷⁾. 이와 같은 국내 시큐어 코딩률은 외국의 취약점 분석 공개 목록과 시큐어 코딩률을 참조하여, 주로 상위권 취약점을 시큐어 코딩률과 매핑하는 형태로 개발되었다.¹²¹⁻²³⁾

CERT(Computer Emergency Response Team)의 시큐어 코딩률은 18개 구현기능영역에서 156개의 시큐어 코딩률을 정의하고 있다²¹⁻²³⁾. 반면, 행정안전부 공공 정보체계 대상 개발보안 지침에 의한 시큐어 코딩률은 7개 취약점 분야에 43개의 코딩률을 정의하고 있다¹⁷⁾. 이들은 모두 CWE, CVE를 기본적으로 참조하고 있다.¹²¹⁾ 본 연구에서는 지휘소용 전장관리 정보체계에 적합한 시큐어 코딩률을 선별하여 시큐어 코딩률 셋을 구성함에 있어, 행정안전부와 CERT의 시큐어 코딩률 등을 모두 참조할 필요가 있다.

기존 연구들은, 향후 다양하고 광범위한 무기체계별 시큐어 코딩률을 개발하기 위한 방안과 시큐어 코딩

률의 개발에서 각 체계별 특성을 고려한 시큐어 코딩률을 선정하고 평가하기 위한 방안은 제시하지 못하고 있다. 또한, 개발된 시큐어 코딩률이 적용될 체계에 최적화되어 있지 않다. 한편으로 유사한 물들이 중복된 경우도 있고, 적용효과가 검증되지 않은 경우도 있다. 그러므로, 적용 대상 체계에 적용 우선순위가 선별되어 최적화된 코딩률을 개발하여 활용하는 것이 필요하다. 본 연구에서는 향후 증가하는 사이버 위협에 따라, 소프트웨어를 탑재한 모든 무기체계들은 각 무기체계별 특성에 따른 최적화된 시큐어 코딩률의 개발과 적용이 필요할 것으로 예상된다. 각 적용대상 체계별로 적용하기에 적합한 시큐어 코딩률들을 선정하기 위한 일종의 시큐어 코딩률 최적화 방안으로 시큐어 코딩률에 대한 선정 평가 방안을 제시하고자 한다

III. 연구 방법과 절차

본 연구에서는 기존에 개발된 시큐어 코딩률들을 활용하여, 무기체계 특성에 맞는 무기체계별 시큐어 코딩률을 선별하기 위한 방안으로 기존 시큐어 코딩률들에서 중복을 배제하고, 누락 없이 종합하여 구성한 슈퍼셋(Super Set, 상위집합)에서 무기체계 특성에 적합한 시큐어 코딩률을 선정 평가하는 방안을 단계별로 제시하고자 한다. 적용대상 무기체계에 대한 시큐어 코딩률의 요구사항과 평가요소 도출에는 KJ-브레인스토밍을 실시한다. 도출된 평가요소에 대한 가중치(중요도)에 대한 적용 우선 순위를 평가하는 작업에는 계층분석기법을 활용하여, 평가요소별 가중치와 평가요소별 가중치의 평점에 대한 가중치를 도출하였다. KJ-브레인스토밍과 설문조사 대상 집단은 소프트웨어 개발보안 전문가 과정에 해당하는 교육 또는 유사/대체 교육을 이수한 지휘소용 전장관리정보체계 소프트웨어 개발 전문가 10명으로 구성되어 있다. 개발자 집단은 8년 이상 ~ 15년의 경력보유 집단으로, 전장관리정보체계소프트웨어와 지휘통제무기체계 소프트웨어 분야 관련 개발 경력을 보유한 인원들이다. 본 연구에서는 전장관리정보체계소프트웨어 또는 지휘통제무기체계 소프트웨어분야 관련 개발 경력이 선정평가의 핵심요소인 관계로, 단순하게 개발보안 전문가 과정이나 개발보안 진단원 과정을 이수한 인원을 전문가로 선정하지는 않았다.

3.1. 요구사항 및 평가요소의 도출

시큐어 코딩 적용 대상 무기체계 특성에 따른 시큐

어 코딩룰 요구사항과 평가요소의 도출과 계층화에는 간단한 구조의 브레인 스토밍 기법인 KJ(Kawagita Jiro)기법을 활용하였다. KJ기법은 브레인스토밍 기법의 일종으로 도출된 항목간의 포함/상하 관계와 계층 구조를 비교적 단순하고 쉬운 과정을 거쳐 구성할 수 있다. KJ기법은 단순하고 간단한 브레인스토밍 기법으로 팀단위의 브레인스토밍 TKJ(Team-KJ기법)으로도 활용한다. KJ기법에서는 해결하고자 하는 문제나 항목을 결정하고, 대상 과제와 관련된 현상의 사실을 라벨에 기입 하고, 과제와 현상 라벨들을 분류하고 정렬한다⁹⁾. 이러한 과정을 거쳐 정리된 시큐어 코딩 적용 대상 체계의 시큐어 코딩 요구사항을 목록으로 작성한다. 이 목록의 요소들은 시큐어 코딩룰 선정을 위한 평정표에 활용되게 된다.

3.2. 계층구조의 설계와 검증

계층분석기법(AHP, Analytic Hierarchy Process)의 활용에는 평가대상 항목에 대한 계층구조를 구성하는 것이 필요하다. 본 연구에서는 앞서 언급된 비교적 단순하고 간단하지만, 계층구조를 구성하는데 도움이 되는 브레인스토밍 기법인 KJ기법을 활용하여, 계층구조를 구성하고, 구성한 계층구조의 적합성 평가와 검증을 위해 QFD 분석을 실시한다. 품질기능전개(QFD, Quality Function Deployment)는 고객 요구에서 제품으로 만들어내기까지 일련의 체계적인 과정을 제공하기 위한 방법으로 개발되었다. 신제품의 개발기간을 단축하기 위해 설계 의도를 제조자에 효율적으로 전달하기 위한 도구로써 개발되었으나, 점차 그 기법이 정교해지면서 고객의 요구사항을 포함시키는 단계까지 발전하였다. 고객의 요구수집에 의해 해당되는 기술적 특성의 수집, 고객의 요구와 기술적 특성간의 상관관계를 확인하고 이를 이용하여 설계 목표를 결정하는 품질의 집을 적용하는 과정을 설명할 수 있다. 아울러, 상대적 중요도와 기술적 특성의 상쇄관계, 고객의 경쟁력평가, 객관적 측정치를 이용하여 보다 용이하게 설계목표를 설정할 수 있도록 도와줄 수 있는 기법이다. 품질기능전개(QFD)는 계층분석기법(AHP)의 분석 대상에 대한 중복과 누락 없는 계층구조의 설계에도 사용될 수 있다⁸⁾.

3.3. 선정 평가 모형

기존 표준과 지침 등을 참고하여 구성된 시큐어 코딩룰 상위집합(Super Set)의 개별 항목은 델파이 설문 조사를 통해 개별 항목의 적합성을 조정하고 배점평가를 실시한다. 위에서 도출된 요구사항을 기반으로,

시큐어 코딩룰 선정 평가를 실시하게 된다. 델파이 기법이란, 전문가를 대상으로 집단의 의견들을 조정하여 우선순위를 확인 또는 서열화하는 방법이다. 수집된 설문을 다시 설문자들에게 보내, 타인과 의견을 비교하여, 의견과 평정을 수정함으로써, 일치된 의견을 생성하게 한다⁹⁾. 델파이 기법으로 종합된 평가요소별 평가점수는 계층분석기법을 활용하여 도출된 평가요소별 적용 우선순위 가중치에 의해 평가한다. 계층분석기법은 여러 가지 의사결정 기준을 고려한 의사결정을 해야 하는 경우 활용하게 되는 다기준의사결정 기법(MCDM, Multi Criteria Decision Making)으로 활용된다. 본 연구에서는 분야 전문가 평가에 의한 가중치 산정을 통한 우선 순위 데이터 분석을 하려고 하고 있으므로, 다기준의사결정기법 중, 이러한 의사결정에 가장 적합한 것으로 판단되는 계층분석기법(AHP)을 활용한다.

3.4. 연구 절차

본 연구에서는 기존의 검증된 시큐어 코딩룰들을 종합하여 중복과 누락이 배제된 시큐어 코딩룰 슈퍼셋을 구성한다. 적용대상 체계에 따른 요구사항과 평가요소를 KJ-브레인스토밍을 통해 도출하고, AHP의 계층구조를 설계한다. 설계된 계층구조는 QFD를 통해 검증한다. 개별 시큐어 코딩룰들을 델파이기법으로 평가한다. 평가된 시큐어 코딩룰들은 AHP 분석을 통해 부여된 가중치를 적용한 배점평가를 통해 선정 평가한다. 본 연구의 전체적인 수행 절차는 [그림 1]과 같이 정리할 수 있다.

IV. 시큐어 코딩룰 선정 평가 방안

본 연구에서는 시큐어 코딩룰 선정평가를 위해 6개의 선정 평가 항목을 도출하고, 6개의 선정 평가 항목에 대해 계층분석(AHP)을 통해, 적용 우선 순위 가중치를 산출하였다. 산출된 가중치에 의해, 각 시큐어 코딩룰 배점을 가중치로 환산하여 총점 환산하여, 높은 점수순으로 시큐어 코딩룰 셋을 선정하는 방안을 제시하고 있다. 우선, 적용 대상 체계의 특성을 분석하고, 시큐어 코딩룰의 평가요소를 도출한다. 기존 참조 시큐어 코딩룰을 중복과 누락 없이 매핑하여 시큐어 코딩룰 슈퍼셋을 구성하고, 시큐어 코딩룰 슈퍼셋을 평가요소 가중치를 활용하여 평가하여 시큐어 코딩룰을 산정한다.

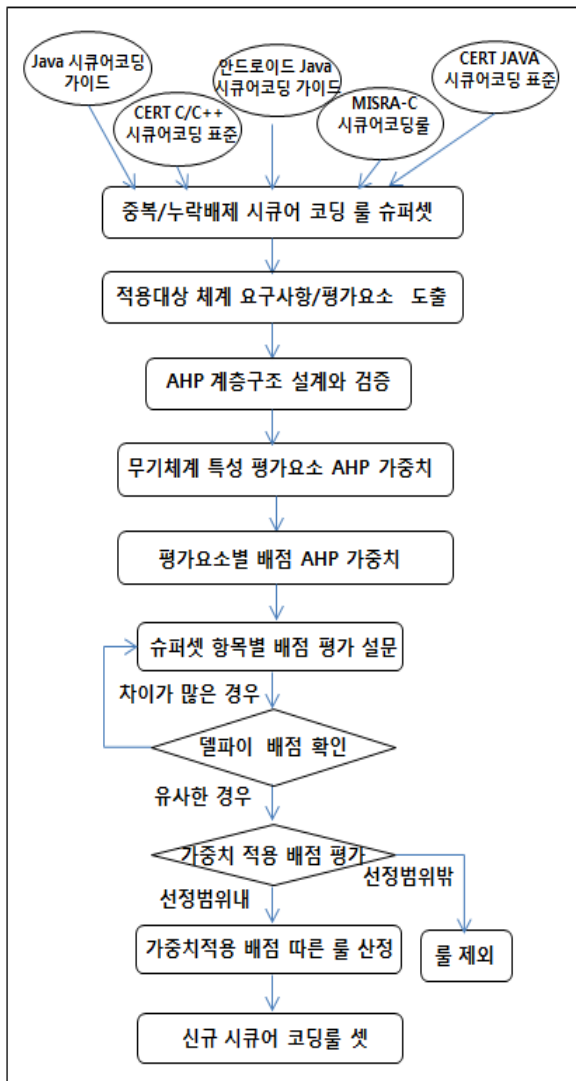


그림 1. 연구 절차
Fig. 1. Research Flow

4.1. 적용대상 체계 특성 분석

본 연구에서 제안한 무기체계별 시큐어 코딩룰 선정 평가 방안을 활용하여, 특정한 1개 분야를 선정하여 적용해보고자 한다. 본 연구에서 선정한 적용 대상 체계는 지휘소용 전장관리정보체계 소프트웨어이다. 해당체계는 연구자 선행 연구의 국방 소프트웨어 분류^[6,7]에 따르면, 본 연구에서의 적용대상체계는 전력 체계-전장관리정보체계-C4I 체계응용소프트웨어이다.

무기체계 SW 시큐어 코딩과 관련한 연구자의 선행 연구에서는 지휘소용 전장관리정보체계 소프트웨어에 대해 일반적인 정보체계와 형태적 유사점을 바탕으로, 기존 전자정부 시큐어 코딩룰의 적용이 가능할 것으로 판단하고, 기존 전자정부 시큐어 코딩룰을 우선적으로 적용하는 것이 필요함을 언급한바 있다^[6,7]. 지휘

소용 전장관리정보체계 소프트웨어는 웹기반으로 운영되는 정보체계의 형상을 가지고 있다. 지휘소용 전장관리정보체계소프트웨어는 무기체계 소프트웨어로 분류되고 있지만, 일반적인 정보체계와 유사한 구성과 성격을 가지고 있다. 해당 체계의 지휘소 단말기는 일반적인 PC에서 설치 및 구동이 가능해야하고, 향후에는 이동 지휘소 활용 향상을 위해 안드로이드와 유사한 환경인 전용통신단말기에서도 서비스가 구동될 수 있어야 한다. 하드웨어 계층은 지휘소 단말기 기능의 PC단과 웹서비스 등을 제공하는 서버등으로 구분된다. 지휘소 단말기인 PC 단에서도 메시지와 지리 정보 등의 입력, 조회 등의 기능이 구현된다. 이동형 단말기에서 메시지와 지리 정보 등의 입력, 조회 등의 기능 구현도 가능해야 한다. 주요 개발환경은 JAVA이며, 적용 요구되는 개발방법론은 국방 CBD 방법론이다. 적용대상 체계의 시큐어 코딩 주요 요구사항은 JAVA 언어 특성에 부합해야하며, JAVA 환경에 웹 환경과 모바일 플랫폼 환경에 대해 소프트웨어 보안 기능을 보장해야 한다.

4.2. 시큐어 코딩룰 평가 요소 도출

본 연구에서 추구하는 시큐어 코딩룰 선정 평가 방안의 제시를 위해서는 시큐어 코딩룰 선정을 위한 기초자료와 평가요소의 도출이 필요하다. 기존 연구에서는 취약성에 대한 위험평가를 심각도, 발생 가능성, 영향도로 구분하고, 3점 척도로 낮음(1), 보통(2), 높음(3)으로 평가하였다^[4,22,23]. 본 연구에서는 시큐어 코딩룰 개별 평가에서 코딩룰에 대해 기본적으로 고려할 요소로 위험평가 요소인 심각도, 발생 가능성, 영향도를 브레인스토밍 대상자들에게 제시하였다. 제시된 평가요소를 바탕으로, 전장관리정보체계 개발 전문가 10인에 대한 KJ기법을 활용한 브레인스토밍을 통해 [그림 2]와 같이 체계 적용적합성, 침해의 심각성, 침해의 가능성, 신뢰성/품질향상, 수정 비용, 룰 적용 기대 효과의 6개 요소가 각 시큐어 코딩룰 선정을 위한 평가 요소로 도출 되었다. [그림 2]와 같이 도출된 체계 적용적합성, 침해의 심각성, 침해의 가능성, 신뢰성/품질향상, 수정 비용, 룰 적용 기대 효과 요소들은 계층분석기법(AHP)에서 활용될 평가대상 항목에 대한 계층구조를 구성하기 위해, KJ기법을 활용하였다. [그림 3]과 같은 계층 구조를 설계하기 위하여, KJ-브레인스토밍 과정을 거치게 되었다. 계층분석을 위한 계층구조 도출과정에서, [그림 4]와 같이 체계적용적합성은 개발언어적합성, 플랫폼적합성의 두가지 항목의 하위 항목으로 세분화 되면서 계층화 되었다.

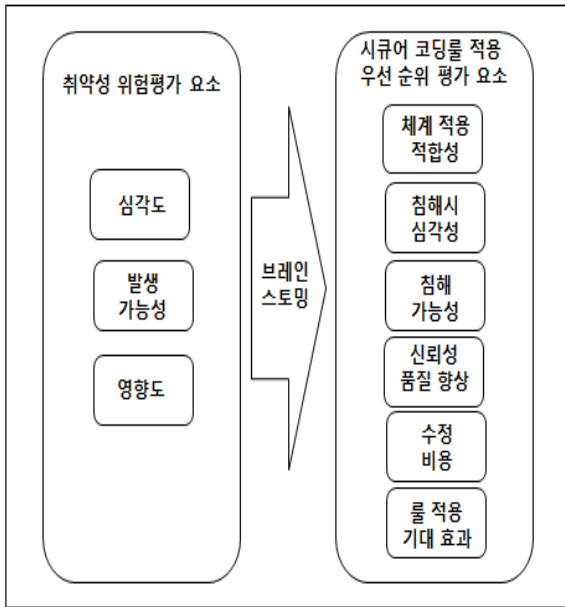


그림 2. 시큐어 코딩룰 평가요소 도출
Fig. 2. Secure Coding Rule Evaluation factors

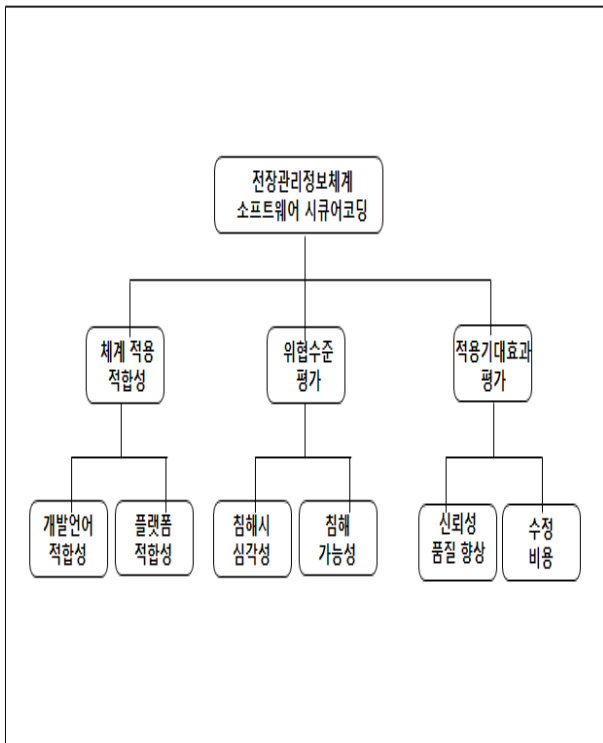


그림 3. 평가요소간의 계층 구조
Fig. 3. AHP Hierarchy for Evaluation

침해시 심각성과 침해가능성의 두가지 항목은 위협 수준평가의 항목으로 상위 항목이 생기면서 계층화 되었다. 적용기대효과평가, 신뢰성 품질 향상, 수정비용의 3개 항목은 적용기대효과평가에 신뢰성 품질 향상과 수정비용의 두가지 항목이 하위 항목으로 조정되면서 상위항목과 하위항목의 계층구조가 구성되었

다. [그림 4]은 이 과정을 정리한 것이다.

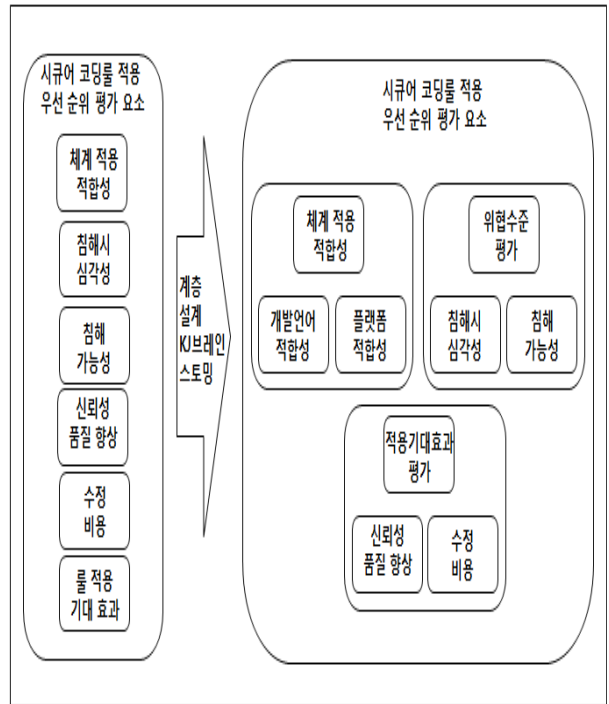


그림 4. 계층설계를 위한 KJ-브레인스토밍 과정 결과
Fig. 4. KJ-Brain Storming Result for AHP Hierarchy

계층분석(AHP)의 적용에서는 [그림 3]과 같이 도출된 계층구조의 각 항목들이 누락되거나 중복되지 않게 계층구조를 적합하게 설계하였는지의 여부가 매우 중요하다^{8,9)}. 적합한 계층구조를 설계하는 방법에는 여러 가지 방법들이 연구되고 있다. 본 연구에서는 KJ-브레인스토밍으로 설계한 계층구조를 품질기능 전개(QFD)를 활용한 방법을 활용하여, 설계된 계층구조의 적합성을 검증하는 간략화된 방안을 적용하여 계층구조의 적합성을 검증하였다.

4.3. 시큐어 코딩룰 상위집합의 구성

본 연구에서는 지휘소용 전장관리정보체계 소프트웨어에 적합한 시큐어 코딩룰을 선정하기 위한 작업으로, 기존 시큐어 코딩룰들의 분석을 통해 중복과 누락을 배제하여, 총 670개의 시큐어 코딩룰 상위집합의 기초데이터를 구성하였다. 기초 데이터의 구성에는 CERT C, CERT C++, CERT JAVA Standard와 상용 MISRA C 2004, MISRA C++^[21-23], 안드로이드 JAVA 개발보안가이드, JAVA 개발보안가이드, C 개발보안가이드, 소프트웨어 보안약점진단가이드^[14-17] 등의 문헌상의 기존 시큐어 코딩룰 정보들을 활용하여 총 1112개의 기초 데이터 셋을 구성하였다. 이 과정에서 기존에 활용되고 있는 코딩룰과 시큐어 코딩

물들을 참고하여, 시큐어 코딩룰의 각 분야별로 재분류와 중복과 누락배제 작업을 실시하였다. 누락 배제를 위해 앞서 언급된 바와 같이 전체 코딩룰은 분야별로 분류하여, 나열하였다. 여기에서, 1차적으로 중복되는 내용의 코딩룰 442개를 제외하고, 각각의 내용을 대표하는 1개의 룰만을 남겨 670개의 룰을 구성하였다. 중복 제거의 원칙은 단순하다. 시큐어 코딩룰 중 동일한 내용을 다르게 표현하거나, 동일한 내용은 모두 제거하였다. 중복의 예를 들면, “자원삽입이 가능해서는 안된다” 같은 항목은 모든 코딩룰이 모두 가지고 있는 사항으로, 중복이 매우 심하다. 때문에 해당 항목들은 모두 1가지의 대표항목만을 남기고 제외하였다. 구성된 시큐어 코딩룰 상위집합 기초데이터가 가진 670개의 룰들은 현재 활용되고 있는 여타 코딩룰들이 50여개에서 200여개 정도의 코딩룰을 사용하는 것에 비해 그 수가 현저히 많다. 이는 상위집합의 기초데이터 구성 과정에서, 중복과 누락은 배제하였지만, 개발 언어의 차이를 반영하지 않았기 때문이다. 그러므로, JAVA 환경에서 활용이 어렵거나 제한되고, 타 개발언어에만 활용 가능한 시큐어 코딩룰의 배제가 필요하다. 연구자는 시큐어 코딩룰 항목별 특성을 분석하여, JAVA 환경에 부적합한 372개의 코딩룰들을 추려내어 상위집합 기초데이터에서 우선적으로 제외하였다. 부적합 룰의 제거 원칙은 C언어에만 적용 가능한 코딩룰, C++언어에만 적용 가능한 코딩룰이다. 때문에 C언어와 C++언어의 컴파일러에만 적용되는 코딩룰은 모두 제외되었다. 제외의 예를 들면, “포인터 지정 오류”와 같은 항목은 JAVA 언어와는 무관하게 C언어의 특징적인 항목이므로 제외대상이 되었다. 결과적으로 위의 중복배제 과정과 언어부적합성 배제과정을 통해, 개발언어 적합성에 적합할 것으로 예상되는 298개의 시큐어 코딩룰이 JAVA 언어 기반의 시큐어 코딩룰 선정 평가의 대상 집합으로 남게 되었다.

4.4. 시큐어 코딩룰 선정 평가

앞 절에서 구성한 298개의 시큐어 코딩룰 상위집합(Super Set)은 분석대상 체계인 지휘소용 전장관리 정보체계의 특성에서 일반적으로 예측 가능한 범위의 시큐어 코딩룰을 중복과 누락을 배제하여 선별하여 구성된 JAVA 언어 시큐어 코딩룰의 상위집합(Super Set)이다. 이러한 상위집합은 여러 분야별 특성에 따른 시큐어 코딩룰의 선정시 필요한 시큐어 코딩룰을 참조할 수 있는 사전적 기능을 제공한다. 본 연구에서는 시큐어 코딩룰 상위집합이 가진 298개의 시큐어

코딩룰에 대해서 전장관리정보체계 소프트웨어에 적합한 선정평가를 위해 각 룰별로, 체계적용적합성(개발언어적합성, 플랫폼적합성), 위협평가(침해의 심각성, 침해의 가능성), 적용기대효과(신뢰성/품질향상, 수정 비용)의 요소들을 평가하게 된다. 본 연구에서는 적용대상 체계에 적합한 시큐어 코딩룰을 선정하기 위한 평가항목에 대한 가중치 산정 과정에 계층분석기법을 활용하고자 한다. 본 연구에서 제안하는 선정평가 과정에서 계층분석기법을 활용해야만 하는 이유는 본 연구의 대상이 가진, 전문가 수의 희박함에 있다. 일반적으로 통계기법을 활용한 분석에서는 많은 수의 설문이 필요하다. 그러나, 시큐어 코딩이나 전장관리정보체계에 대해서는 많은 전문가가 존재하지 않는다. 통계적인 방법에서 활용할만한 유의미한 규모의 전문가를 확보하고 이들에게 통계조사를 하는 것은 매우 어렵다. 그러나, 계층분석기법의 경우에는 동일한 분야의 전문가 집단이라면 10~15명 정도의 전문가 설문만으로도 유의미한 분석결과를 얻을 수 있다. 계층분석기법(AHP)은 쌍대비교를 통해 일관성의 분석이 가능하다. 이 과정에서 불성실한 답변이나 전문성이 결여된 답변에 대해서는 답변 제외를 통해 신뢰성의 확보가 가능하다. 본 연구에서와 같이 여러 평가요소들을 복합적으로 고려하여 그 우선순위나 가중치를 다루고자 하는 경우 다기준의사결정기법중에 계층분석기법(AHP)이 가장 적합한 것으로 알려져 있다^{18,9)}. 본 연구에서는 계층분석을 보다 용이하게 활용하기 위하여, 상용 패키지 분석 프로그램인 Expert Choice 11을 활용하였다. [표 2]는 평가요소별 가중치 산정결과이다. 계층별로 부여된 가중치들의 전문가별 의견은 계층분석기법에 활용될 수 있게 기하평균으로 종합되었다⁹⁾. 기존 연구들에 따르면, CR값이 0.1 이하이면 타당한 것으로 알려져 있다^{18,9)}. 본 연구에서의 CR값은 0.01이 나왔으므로, 본 연구에서 조사된 결과값은 타당한 범위의 결과로 판단된다. 각각의 선정 평가 항목은 5점의 등급척도로 중요도를 평가한다. 본 평가에서 각 배점은 “1점은 포함될 필요가 없다. 2점은 포함되거나 포함되지 않거나 별 상관이 없다. 3점은 포함될 필요가 있는지 검토해 보아야 한다. 4점은 포함되어야 한다. 5점은 꼭 포함되어야 한다.”으로 구분하였다. 여기서, 주목할 점은 1-2점은 포함될 필요가 없는 항목이라는 점이다. 3점은 포함여부에 대해 검토가 필요한 항목이고, 4-5점은 포함되어야만 하는 항목이다. 그런데, 여기서 적용되는 항목들에 대한 5점 척도는 정성적인 면을 가지고 있으므로, 일정한 정량적 기준으로 변환되어야 할 필요가 있다. 그러

므로 등급척도에 대해서도 계층분석기법을 활용한 쌍 대비교를 통해 상대적 중요도를 도출할 필요가 있다.

표 2. 평가요소별 가중치
Table 2. Weight of Evaluation Factors

Evaluation Factors (high level)		Evaluation Factors (low level)	
Factors	Weight	Factors	Weight
Compliance system application (A)	0.352	Language Compliance (A-1)	0.593
		Platform Compliance (A-2)	0.407
Threat evaluation (B)	0.304	Criticality (B-1)	0.603
		possibility (B-2)	0.397
Application benefit (C)	0.344	Reliability Quality (C-1)	0.418
		Modify Cost (C-2)	0.582

시큐어 코딩룰 상위집합(Super Set)으로 목록화된 평가대상 코딩룰은 위와 같은 배점 방식을 활용하여 델파이 순환평가를 통해 [그림 5]과 같은 평정표를 활용하여, 298개의 시큐어 코딩룰들에 대한 각 평가요소별 평정을 실시하였다. 평가 결과를 종합하여 가중치가 부여된 각 평가요소를 기준으로, 각 항목별 적용 우선 순위가 산정되게 된다. [표 3]은 각 평가요소와 등급척도에 대한 상대중요도를 구하고, 복합 중요도를 구한 결과이다. 이 결과를 활용하여, [그림 6]과 같은 결과를 얻을 수 있다. [그림 6]는 복합가중치를 반영하여 산정한 시큐어 코딩룰의 환산 평정 결과표이다. 계층분석된 복합 가중치를 반영하여 실시한 선정 평가에서는 를 기준으로 각 코딩룰들에서 산정되는 복합 가중치 적용 총점의 차이는 0.0X 정도만 차이가 나는 반면, 198위부터 0.12이상의 현격한 차이가 발생한다. 이 점수 차이 발생을 임계치로 설정하면, 점수 차이가 0.12점 이상 발생하고 있는 198위부터 시큐어 코딩룰이 다른 코딩룰들에 비해, 적용 우선순위가 낮은 것으로 보고 제외할 수 있다.

표 3. 평가요소별 상대중요도와 복합중요도 산정결과
Table 3. Relative and Complex importance of Factors Calculation Result

Evaluation Factors (high rank)	Evaluation Factors (low rank)	Unit	Relative Weight	Complex Weight
A (0.352)	A-1 (0.593)	5	0.586	0.123
		4	0.239	0.05
		3	0.125	0.027
		2	0.032	0.007
		1	0.018	0.004
	A-2 (0.407)	5	0.439	0.063
		4	0.290	0.042
		3	0.175	0.026
		2	0.058	0.009
		1	0.039	0.006
B (0.304)	B-1 (0.603)	5	0.458	0.084
		4	0.215	0.04
		3	0.163	0.03
		2	0.093	0.018
		1	0.072	0.014
	B-2 (0.397)	5	0.349	0.043
		4	0.215	0.026
		3	0.189	0.023
		2	0.134	0.017
		1	0.113	0.014
C (0.344)	C-1 (0.418)	5	0.503	0.073
		4	0.203	0.03
		3	0.142	0.021
		2	0.088	0.013
		1	0.064	0.01
	C-2 (0.582)	5	0.326	0.066
		4	0.298	0.06
		3	0.199	0.04
		2	0.109	0.022
		1	0.068	0.014

V. 결 론

순번	대상	평가항목	평가내용	평가					
				가	나	다	라	마	바
1	전통언어	평가항목	가용성이 가능해진다	5	4	5	5	5	5
2	전통언어	평가항목	크로스사이트 소호로이 가능해진다	5	4	5	5	5	5
3	전통언어	평가항목	운영체제 별이 가능해진다	5	5	5	5	5	4
4	전통언어	평가항목	이슈, 명령어 삽입이 가능해진다	5	5	5	5	5	4
5	전통언어	평가항목	위험한 형식 파일 업로드로 가능해진다	5	5	4	4	4	5
6	전통언어	평가항목	신뢰성은 낮다, 주소로 자동등록 연결이 가능해진다	4	4	3	3	3	3
7	전통언어	평가항목	다량의 링크 공유가 가능해진다	5	4	5	5	5	5
8	전통언어	평가항목	HTTP 용량 분할이 가능해진다	4	4	3	3	3	3
9	전통언어	평가항목	보조 기능나눔을 활용할 수 있는 일관된 형태로 가 용해진다	5	4	5	4	5	5
10	전통언어	평가항목	시스템 부하 분할을 외부에서 가능해진다	5	4	5	4	5	5
11	전통언어	평가항목	문자 생성 수월 명령어 삽입이 가능해진다	5	4	5	4	5	5
12	전통언어	평가항목	프로세스 제어	5	4	5	4	3	5
13	전통언어	평가항목	안전하지 않은 리눅스	4	4	3	3	3	4
14	전통언어	평가항목	부정확한 명령어 삽입이 가능해진다	3	3	3	3	3	3
15	전통언어	평가항목	보안성능을 신뢰하기 전에 평가	3	3	3	3	3	3
16	전통언어	평가항목	문자열을 검색하기 전 규격	4	4	4	4	3	3
17	전통언어	평가항목	문자열을 검색하기 전 규격	4	4	4	4	3	3
18	전통언어	평가항목	서버에서부터 많은 사용자 등록은 로그 남기지 않는다	4	4	3	3	3	2

그림 5. 평가대상 시큐어 코딩률별 델파이 순환 평정표
Fig. 5. Delphi Score for Evaluation

본 연구에서는 날로 증가하는 사이버 위협, 특히 사 이버전에서 무기체계 소프트웨어에 대한 사이버위협 을 방지하기 위한 무기체계별 시큐어 코딩률을 개발 하기 위한 방안으로 계층분석기법을 활용하여, 적용대 상체계에 적합한 가중치를 부여하여 시큐어 코딩률을 선정 평가하는 방안을 제시하고, 전장관리정보체계의 시큐어 코딩률을 선정평가하는 데 활용 하였다. 이를 통해 총 총 197개의 시큐어 코딩률로 구성된 지휘소 용 전장관리정보체계용의 시큐어 코딩률 셋을 개발하 였다. 각 시큐어 코딩률 배점을 가중치로 환산하여 총 점 환산하여, 높은 점수순으로 시큐어 코딩률 셋을 선 정한다. 선정된 셋은 필요에 따라, 우선순위를 고려하 여 적용할 수 있을 것이다. 본 연구에서는 적용대상 체계에 적합한 시큐어 코딩률을 선정하기 위한 평가 항목에 대한 가중치 산정에 계층분석기법(AHP)을 활 용하였다. 본 연구에서 다루지 않은 다른 적용 대상 체계들의 경우에도 각 적용대상 체계에 적합한 가중 치 산정만을 다시 하면, 본 연구의 절차를 활용하여 비교적 간단한 방법으로 각 체계에 적합한 시큐어 코 디ング률의 선정 우선 순위를 구하는 것이 가능하다.

기존 시큐어 코딩률의 선정기준은 취약점 분석 공 개문서의 중요도만을 중심으로 하고 있었다. 반면, 본 연구에서는 적용대상 체계의 특성에 따른 체계적용적 합성(개발언어적합성, 플랫폼적합성), 위협평가(침해 의 심각성, 침해의 가능성), 적용기대효과(신뢰성/품질 향상, 수정 비용) 등의 여러 가지 요소들을 종합적으 로 고려하여 기존에 시큐어 코딩률을 가지고 있지 않 은 분야에 대해서, 기존의 코딩률들을 활용하여, 적용 대상체계에 적합한 시큐어 코딩률을 선정하는 방안을 제시하였다. 본 연구를 통해, 향후 시큐어 코딩률이 적용되어야 할 다양한 체계별 적합성을 고려하여 개 발되어야 할 다양한 시큐어 코딩률들의 선정과 적용 이 보다 용이해질 수 있을 것을 기대한다. 향후 연구 에서는 본 연구에서 제시한 선정평가방안을 일반화하 여 다른 분야에 대한 시큐어 코딩률 선정평가에 활용 할 수 있는 방안을 모색할 필요가 있다. 또한, 시큐어 코딩률의 개별 항목 선정에서 또 다른 다기준의사결 정 기법인 자료포락분석기법을 활용하여, 적용 효율을 중심으로 선정평가 모델을 개발하는 것도 가능할 것 이다. 또한 본 연구의 계층분석기법을 활용한 선정 방 법과 자료포락분석기법을 활용한 방법을 결합한 하이 브리드 모형의 개발도 가능할 것이다.

순번	대상	평가항목	평가내용	평가						총점	점수순위
				가	나	다	라	마	바		
1	전통언어	평가항목	가용성이 가능해진다	0.123	0.042	0.084	0.043	0.073	0.089	7.60239	3
2	전통언어	평가항목	크로스사이트 소호로이 가능해진다	0.123	0.042	0.084	0.043	0.021	0.089	6.65363	8
3	전통언어	평가항목	운영체제 별이 가능해진다	0.123	0.083	0.084	0.043	0.073	0.08	7.70234	1
4	전통언어	평가항목	이슈, 명령어 삽입이 가능해진다	0.123	0.083	0.084	0.043	0.073	0.08	7.70234	1
5	전통언어	평가항목	위험한 형식 파일 업로드로 가능해진다	0.123	0.083	0.04	0.028	0.03	0.088	6.27483	20
6	전통언어	평가항목	신뢰성은 낮다, 주소로 자동등록 연결이 가능해진다	0.06	0.042	0.03	0.023	0.021	0.04	3.57885	89
7	전통언어	평가항목	다량의 링크 공유가 가능해진다	0.123	0.042	0.084	0.043	0.073	0.088	7.60239	3
8	전통언어	평가항목	HTTP 용량 분할이 가능해진다	0.06	0.042	0.03	0.023	0.021	0.04	3.57885	89
9	전통언어	평가항목	보조 기능나눔을 활용할 수 있는 일관된 형태로 가 용해진다	0.123	0.042	0.084	0.028	0.073	0.088	7.3962	5
10	전통언어	평가항목	시스템 부하 분할을 외부에서 가능해진다	0.123	0.042	0.084	0.028	0.073	0.088	7.3962	5
11	전통언어	평가항목	문자 생성 수월 명령어 삽입이 가능해진다	0.123	0.042	0.084	0.028	0.073	0.088	7.3962	5
12	전통언어	평가항목	프로세스 제어	0.123	0.042	0.084	0.028	0.021	0.088	6.64844	15
13	전통언어	평가항목	안전하지 않은 리눅스	0.06	0.042	0.03	0.023	0.021	0.08	3.97745	75
14	전통언어	평가항목	부정확한 명령어 삽입이 가능해진다	0.027	0.028	0.03	0.023	0.021	0.04	1.86733	140
15	전통언어	평가항목	보안성능을 신뢰하기 전에 평가	0.027	0.028	0.03	0.023	0.021	0.04	1.86733	140
16	전통언어	평가항목	문자열을 검색하기 전 규격	0.06	0.042	0.04	0.028	0.021	0.04	3.78646	84
17	전통언어	평가항목	문자열을 검색하기 전 규격	0.06	0.042	0.04	0.028	0.021	0.04	3.78646	84
18	전통언어	평가항목	서버에서부터 많은 사용자 등록은 로그 남기지 않는다	0.06	0.042	0.03	0.023	0.021	0.022	3.21851	122

그림 6. 복합가중치를 반영한 환산 평정표
Fig. 6. Complex Weighted Score for Evaluation

기존의 코딩률들이 200개 내외의 코딩률을 선정하고 있는 것을 참조할 때에, 197개의 코딩률이 선정되는 것은 복합가중치를 통해 선정된 시큐어 코딩률이 기 존의 다른 코딩률이나 시큐어 코딩률과 유사성을 가 질 수 있음을 시사한다. 결과적으로 총 197개의 시큐 어 코딩률이 선정되었고, 197개 각각의 시큐어 코딩 률들은 우선 순위가 산정되었다. 선정된 시큐어 코딩 률은 필요에 따라 부여된 우선순위를 활용하여 확대 또는 축소 적용하는 것이 가능하다.

References

- [1] Ban gijho, Halan, Evaluation Methodology of Diagnostic Tool for Security Weakness of e-GOV Software, THE JOURNAL OF KOREA INFORMATION AND COMMUNICATIONS SOCIETY(KICS), vol. 38, no. 4, pp 335-343, 2013
- [2] Jeong dahye, Choejin-yeong, Leesonghui, Nuclear-related Software analysis based on secure coding, Journal of Korea Institute of Information Security and Cryptology, vol. 23 no. 2, pp. 243-250, 2013
- [3] Hangyeongsuk, KimTaeHwan, Hagiyoung, Imjaemyeong, Pyochangwoo, An Improvement of the Guideline of Secure Software Development for Korea E-Government, Journal of Korea Institute of Information Security and Cryptology, vol. 22 no. 5, pp1179-1189, 2012
- [4] Kim dongwon, Han geunhui, A Study on Self Assessment of Mobile Secure Coding, Journal of Korea Institute of Information Security and Cryptology, vol. 22 no. 4, pp. 901-911, 2012
- [5] Kim seonggeun, Lee jaeil, Analyzing Secure Coding Initiatives: An Ecosystem Approach, Journal of Korea Institute of Information Security and Cryptology, vol. 22 no. 5, pp. 1205-1216, 2012
- [6] Junesung choi, Wooje Kim, Wonhyung Park, Kwangho Kook, Defense SW Secure Coding Application Method for Cyberwarfare Focused on the warfare System Embedded SW Application Level, Journal of Korea Association of Defense Industry Studies, vol. 19, no. 2, pp. 91-103, 2012
- [7] Junesung choi, Wooje Kim, Kwangho Kook, warfare System Embedded SW Secure Coding Application Method, 2012 KORMS Proceedings pp. 1454-1466, 2012
- [8] Bongwoo Lee, JaHee Kim, wooje Kim, "ITS project manager research core competencies Using QFD and AHP", Journal of IT Service, vol. 10, no. 1, pp. 89-103, 2011
- [9] JaHee Kim, Wooje Kim, hyeongi Cho, eunyoung Lee, minwoo Seo, A Study on the Development of Evaluation Model for Selecting a Standard for DITA using AHP, IE Interfaces, vol. 25, no. 1, pp. 96-105, 2012
- [10] LeeBuyoon, Alerts on Car hacking vulnerability, Journal of Mechanics , vol. 51, no. 11, pp. 10-11, 2011
- [11] Kimjungkook, Kimseyoung, Threat to weapon system in the cyberwar, Latest Technology Trends, Defense Technology and Quality, pp. 4-9, 2011
- [12] MOPAS, Administrative information system notice amendment to the operating instructions, 2012
- [13] MOPAS, Information System Audit Guide Line, 2012
- [14] MOPAS, Software Development Secure Coding Guide, 2012
- [15] MOPAS, JAVA Security Coding Guide, 2012
- [16] MOPAS, Android Security Coding Guide, 2012
- [17] MOPAS, Diagnostic software security weaknesses Guide, 2012
- [18] Nor Harisah Zainuddin, "Secure Coding in Software Development", 2011 5th Malaysian Conference in Software Engineering, 2011
- [19] Kittipong Kittichoekchai, "Secure Source Coding with Action-dependent Side Information", 2011 IEEE Inetrnational Symposium on Information Theory Procdeedings
- [20] Ravi Tandon, "Secure Source Coding with a Helper", IEEE TRANSACTIONS ON INFORMATION THEORY, 2011
- [21] Robert C. Seacord, "Secure Coding in C and C++", Addison-Wesley Professional, 2005
- [22] Fred Long, Dhruv Mohindra, Robert C. Seacord, Dean F.Sutherland, David Svoboda, "The Cert Oracle Secure Coding Standard for Java", Prentice Hall, (2008)
- [23] Robert C. Seacord, "The CERT Secure Coding Standard for C", Addison-Wesley, 2008
- [24] James F Dunnigan, "How to Make War : A Comprehensive Guide to Modern Warfare in the Twenty-First Century", Quill, 2003
- [25] <http://www.misra-c.com/Activities/MISRAC/tabid/160/Default.a>, 2012.6.1

최 준 성 (June-sung Choi)



1999년 공군사관학교 산업공학사
1999년~2008년:국방부 등
2008년~현재:삼성탈레스(주)
2010년 KNOU 정보과학석사
2011년~현재 서울과학기술대
IT정책전문대학원 산업정보시
스템전공 박사과정

<관심분야> 정보보호, 사이버전, 디지털 포렌식

박 원 형 (Won-hyung Park)



2002년 서울과학기술대
산업정보시스템공학 학사
2005년 서울과학기술대
대학원 산업정보시스템 석사
2009년 경기대학교 대학원
정보보호학 박사
2012년~현재 극동대학교

사이버안보학과 교수, 학과장
<관심분야> 정보보호, 디지털 포렌식

김 우 제 (Woo-je Kim)



1986년 서울대학교 산업공학사
1988년 서울대학교 대학원
산업공학석사
1994년 서울대학교 대학원
산업공학박사
1996년~2003년 대진대학교
산업시스템공학과 부교수

2003년~현재 서울과학기술대학교 산업정보시스템
공학과 교수

<관심분야> IT서비스, 소프트웨어공학

국 광 호 (Kwang-ho Kook)



1979년 서울대학교 산업공학학
사
1981년 서울대학교 대학원
산업공학 석사
1989년 조지아공과대학 대학
원
산업공학 박사

1989년~1993년 한국전자통신
연구원(ETRI) 선임연구원

1993년~현재 서울과학기술대학교 산업정보시스템
공학과 교수

<관심분야> 정보보호, 정보통신