情報保護學會論文誌
第 22 卷 第 5 號, 2012. 10

secure coding 제도의 생태계 차원의 분석*

김 성 근,[1†‡] 이 재 일[2]
[1]중앙대학교, [2]한국인터넷진흥원

Analyzing Secure Coding Initiatives: An Ecosystem Approach*

Sung Kun Kim,[1†‡] Jae-il Lee[2]
[1]Chung-ang University, [2]KISA

요 약

최근 국내에서도 secure coding 제도화가 처음으로 마련되었다. 개발보안의 체계적 정착을 위한 중요한 첫걸음이라는 점에서 높이 살만하다고 하겠다. 그럼에도 현 제도의 실행 과정에서 예상되는 이슈가 제기되는 등 향후 보완할 점도 제법 있다. 이런 상황에서 본 연구에서는 생태계 차원의 분석을 시도한다. 즉, 개발 보안 제도를 생태계 차원에서 묘사하고, 이를 토대로 현상적 이슈와 문제점을 분석한다. 이런 문제와 이슈의 극복을 위해 향후 강구되어야할 대안을 몇 가지 제시한다.

ABSTRACT

The Korea government has recently announced that secure coding is going to be required when building e-government systems. As its initial effort to enhance the security level of e-government applications, it should be highly valued. In its implementation, however, there are some problematic areas or issues that are expected and need to be supplemented. In this regards, we attempt to analyze the Secure Coding Initiatives and derive some problems using an ecosystem approach. Furthermore, a set of institutional suggestions are made in an effort to get over the problems.

Keywords: secure coding, ecosystem, secure coding initiatives

I. 서 론

정보시스템의 보안에는 다양한 요소가 포함된다. 네트워크 보안, 물리적 보안은 물론이고 안전한(secure) 소프트웨어를 작성하는 노력도 필요하다. 여기서 '안전한 프로그램'(secure program)이란 비정상적으로 작동되게끔 조작되지 못하게 만들어진 프로그램을 의미한다. 예를 들면, 반드시 지켜져야 할 보안 사항을 챙기지 않고 넘어간다거나 작동되어선 안 될 기능이 작동되게끔 또는 작동되지 않아야할 상황에서 작동되게끔 교묘한 조작이 불가능하도록 만들어진 프로그램을 의미한다. 이를 '안전한 프로그래밍'(secure coding) 또는 '소프트웨어개발보안'이라 부른다.

실제 많은 해커는 안전하게 프로그래밍되지 않은 사이트를 주로 공격한다. 2011년말 전세계 백만 개 이상의 웹사이트를 공격한 lilupophilupop.com 해킹 사례도 'SQL injection' 공격 기법이 활용되었다〔Higgins, 2012〕. 2008년, Heartland Payment Systems(신용카드 처리 회사) 사는 유사한 공격에 당해 1억3천4백만 명의 카드고객 정보를 국제범죄 조직에 넘겨주는 피해를 입기도 하였다. 이와 같은 공격이 가능하게 되어 있는, 코딩 상의 허점이 남아 있지

접수일(2012년 9월 12일), 게재확정일(2012년 10월 14일)
* 본 논문은 2012년 한국인터넷진흥원 '시큐어코딩 기반 SW 개발보안 기반기술 연구' 위탁과제의 연구결과로 수행되었음(KISA-2012-024)
† skim@cau.ac.kr
‡ skim@cau.ac.kr

않도록 하자는 노력이 소프트웨어 개발 보안이다.

소프트웨어개발보안을 강화하려는 노력은 날로 증대되고 있다. 이런 추세에 대해 Colley[2010]는 두 가지 관점에서 아주 당연한 조치라고 지적하고 있다. 첫째, 응용시스템 허점으로 인해 뚫려 입는 피해가 세계적으로 연 1800억불에 이르고 있음을 들고 있다. 둘째, 또한 소프트웨어가 인도 또는 설치된 이후에 빠진 보안 요소를 집어넣는 것이 훨씬 비싸게 먹힌다는 점을 지적한다. IBM 통계는 초기 개발 시 보안 요소를 집어넣는 것에 비해 30에서 100 배 이상의 비용이 수반됨을 지적하고 있다.

위와 같은 점을 감안해볼 때 소프트웨어개발보안 노력을 체계적으로 수행할 필요가 있다고 본다. 우리나라 정부에서도 이와 같은 노력을 제도적으로 강구하기 시작했다. 행정안전부는 '정보시스템 구축 운영 지침' 개정안을 마련하여 사이버공격을 유발할 가능성이 있는 잠재적 보안취약점을 개발단계부터 사전 제거하는 기법을 의무화하도록 하였다[조성훈, 2012]. 구체적 접근으로는 감리법인으로 하여금 감리 시 검사항목에 보안약점 제거여부를 반드시 확인하도록 하고 있다. 대상으로는, 2012년 12월부터 행정기관이 추진하는 개발비 40억 이상 정보화사업에 먼저 적용하고, 향후에는 그 대상을 점차 확대해나갈 예정이다. 날로 빈번해지는 사이버공격에 효과적으로 대응하기 위한 노력을 정부 차원에서 시작하였다는 점은 매우 고무적이라 하겠다.

안전한 소프트웨어 개발이란 그 성격상 단순한 문제가 아니다. Davis[2004]는 소프트웨어공학, 보안공학, 관리(management) 등의 다양한 기법과 시각이 반영되어야할 문제라고 지적한 바 있다. 연구자는 다음과 같은 관점에서 다면적 문제라고 본다. 첫째, 다양한 주체가 관련되어 있으며 이들 간의 역할과 책임을 다양하게 규정할 수 있다. 이번에 감리법인으로 하여금 보안약점의 제거를 확인하게 했지만 이들 외에도 다양한 주체의 역할과 책임이 필요하리라 믿는다. 둘째, 특정 기법 또는 도구에 의해서 모든 문제를 단번에 해결할 수 있는 문제가 아니라는 점이다. 흔히 이야기하는 정적 도구를 도입하여 코드를 자동으로 분석하는 것만으로는 해결할 수 없는 것이다. 다양한 기술과 접근이 잘 아울려져야 한다. 마지막으로, 해킹으로부터 안전하다는 것은 정태적 문제일 수가 없고 아주 동태적이라 할 수 밖에 없다. 즉, 해킹과 이로부터의 방어는 창과 방패와 같이, 해킹 기술과 접근이 새로워지면 이에 대응하여 더 진화해나갈 수밖에 없다. 단절된 시스템으로 접근해서는 안 되고, 개방형 즉 피드백 형태로 날로 순화되어 가는 접근이 필요할 듯하다. 이런 이유로 우리나라 정부의 소프트웨어개발보안 정책을 다면적 관점에서 해석해볼 필요가 있다고 본다.

최근 복잡한 문제를 총체적 관점에서 바라보는 생태계(ecosystem 또는 ecology) 접근이 부각되고 있다. Capra[1996]는 "오늘날 우리가 접하는 문제는 매우 복잡하고, 이 문제를 들여다보면 볼수록 개별 요소를 떼 놓고 보아서는 안 되고, 여러 요소가 상호 연결되어 있는 상호의존 되어 있는 시스템적 문제"로 접근되어야 한다고 지적하였다. Bauer & van Eeten[2009]는 사이버보안 이슈도 생태계 방식으로 접근해야만 문제에 대한 정확한 이해와 바람직한 해결책이 마련될 수 있을 것이라고 제시하였다.

본 연구는 소프트웨어개발보안 제도를 생태계 관점에서 분석하고자 한다. 즉, 현 소프트웨어개발보안 제도를 생태계 관점에서 묘사하고, 현재 안고 있는 이슈나 문제점을 도출하고 이런 문제의 해결을 위한 정책적 방향을 제시하고자 함이 본 연구의 목적이다. 이 연구결과는 막 태동하고 있는 국내 소프트웨어개발보안 제도의 올바른 정착과 발전을 위해 어떤 노력이 더 강구될 필요가 있는 지를 이해하는데 크게 기여할 수 있으리라 본다.

II. 소프트웨어개발보안 관련 기존연구

2.1 소프트웨어개발보안 제도

정보시스템 보안에는 제도적 접근이 반드시 수반될 필요가 있다. 이를 가장 체계적으로 실행에 옮긴 국가는 미국이라 할 수 있다. 미국의 경우, 의회와 행정부 관리예산처(Office of Management & Budget: OMB)에서 정보 보안의 중요성을 일찌감치 인식하고 이를 효과적으로 추진하기 위한 제도적 틀을 마련하였다. 그 중에서 가장 기본적인 장치는 〈표 1〉에서 보는 바와 같이 세 가지이다[Bowen, et al., 2007]. 그 외에도 정부업무평가법(Government Performance and Results Act: GPRA, 1993), 문서감축법(Paperwork Reduction Act: PRA, 1995), 정부문서배제법(Government Paperwork Elimination Act: GPEA, 1998), IT관리혁신법(Information Technology Management Reform Act: ITMRA, 1996), 전자정부법(e-Government

〔표 1〕 미국의 정보보안 관련 주요 법제도

법/제도	주요 성격
Federal Information Security Management Act(FISMA), 2002	- 정부에서의 정보보안에 대한 기본법의 역할. 기존의 관련 법제도 성격을 기초로 관리(management)적 성격을 크게 강조하여 새롭게 입법함. - OMB에게 정부기관의 정보보안 노력을 감독할 권한/책임 부여 - 정부 정보자원의 안전을 위한 종합적 프레임워크 제공 ① 기관별 역할과 책임 정립(예:NIST-표준 및 지침서 작성 책임) ② 정보보안을 개별 기관의 투자계획 및 아키텍처(EA)와 연계 ③ 개별기관에게 모든 사업 및 시스템을 정보보안 차원에서 매년 평가하고 그 평가 결과를 OMB에게 제출하도록 요구
OMB 행정명령A-130 (Management of Federal Information Resources) 부록3: Security of Federal Automated Information Resources	- 정보보안 노력에 포함되어야할 최소한의 보안통제 제시 - 전산정보의 보안 관련 기관별 책임 할당 - 정보보안 통제: 정보시스템과 내제된 정보의 기밀성, 온전성, 가용성을 보호하기 위한 관리, 운영, 기술 상의 보호장치 및 대책
Homeland Security Presidential Directive(HSPD-12)	- 국토안보부 대통령명령으로 모든 공무원 및 사업수행자의 신분증명 관련 정책에 대한 규정(2004)

Act, 2002) 등의 내용도 보조적 장치로 작동되고 있다.

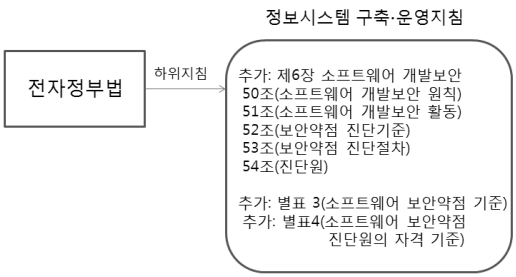
이에 비해 국내 정보보호 관련 법체계는 체계적이지 못하다. 이규정&김현경〔2008〕은 국내 정보 관련 법체계가 개별 정보화 분야별로 흩어져 있고, 이 각 법률의 소관 부처도 다르다는 등 법적 통일성과 체계성이 많이 떨어짐을 지적하고 있다. 정보자원에 관한 외국과의 법제도 연구는 김성근 외〔2005〕, 이창범〔2010〕, 이연수 외〔2009〕를 참조 바란다.

이런 법제도 환경 하에서도 소프트웨어개발보안의 제도화를 위한 여러 연구가 있었다. 김성근〔2009〕은 이런 제도의 필요성을 제시하고, 이 제도화를 위한 다양한 방안을 제시한 바 있다. 이어 제도화 및 활성화를 위한 보다 구체적 방안도 제시된 바 있다〔김성근, 2010〕.

이런 노력의 필요성을 인식한 행정안전부는 수 년간의 검토 끝에 올해 드디어 제도화에 착수하였다. 이 제도의 구조는 〈그림 1〉과 같이 묘사될 수 있다. 전자정부법 제45조 제3항에 따른 "정보시스템 구축·운영지침"에 소프트웨어 개발보안 내용을 별도의 장으로 추가하고 관련 기준 등과 함께 개정하여 고시하였다. 추가된 내용에는 개발보안의 원칙 및 활동, 보안약점 진단 기준과 절차, 그리고 진단원에 대한 내용으로 구성되어 있다. 아울러 별표에는 43개의 소프트웨어 보안약점 기준이 제시되어 있고 소프트웨어 보안약점 진단원의 자격 기준도 포함되어 있다.

구체적으로는 50조에 소프트웨어 개발보안의 개념과 범위를 담고 있다. 51조에는 이와 관련 행정기관장이 제안서 평가 시 관련 진단도구의 사용, 접근방법의 적절성 등을 확인하고 이를 평가에 반영할 수 있음을 담고 있다. 아울러 사업자는 개발자에게 관련 교육을 실시하여야 함을 담고 있다. 보안약점의 기준은 52조에 언급되어 있으며 이에 대한 세부적 내용은 별표3에 정의되어 있다.

보안약점 진단에 관한 구체적 내용은 53조 및 54조에 명시되어 있다. 53조는 진단절차에 관한 것으로 행정기관의 장 및 감리법인과의 역할과 책임이 제시되어 있다. 즉, 행정기관의 장은 감리법인으로 하여금 보안약점 진단을 요구해야 하고, 감리법인은 감리 활동에 이의 진단 및 제거 여부를 확인하게끔 되어 있다. 아울러 진단도구의 사용 시 별도의 기준에 따라 인증된 도구를 사용해야 함을 담고 있다. 마지막으로 전자정부법 시행령에 정의된 정보시스템감리의 대상이 아닌



〔그림 1〕 소프트웨어 개발보안 제도의 구조적 틀

시스템의 경우엔 행정기관의 장은 사업자로 하여금 보안약점을 진단·제거토록 하고 그 결과를 확인할 수 있다고 정의함으로써 적용 범위의 확대 가능성을 열어두긴 하였다.

2.2 IT 정책과 생태계 연구

최근 IT 부문의 중요성은 날로 증대되고 있다. 이 산업 그 자체도 중요하지만, 모든 산업의 경쟁력에도 크게 기여할 수 있기 때문이다. 즉, 생산성, 경제성장, 나아가서 고용창출 등에 크게 이바지할 수 있음은 분명한 사실로 받아들여지고 있다.

이에 따라 많은 국가에서 이 IT 정책을 제대로 수립하고 집행하는데 관심이 높은 편이다. 그러나 IT 정책에 관한 이론적 연구가 별로 되어 있지 않다. 아울러 IT 고유의 특성(파급성, 지속적 기술개발, 대규모 투자 요건 등)을 간파하지 못하여 정책수립 및 집행 시 많은 어려움이 처하기도 한다. Ulrich & Chacko〔2005〕는 〈표 2〉와 같은 9개 도전에 직면한다고 지적한 바 있다. 이 간이유 등으로 인다.IT 정책 의사결정자들은 큰 부담을 안고 있다고 볼 수 있다.

실제 많은 국가에서 다양한 형태로 IT 정책을 수립하여 집행해오고 있다. 그러나 그 정책 효과는 쉽게 나오는 편은 아니다. 미국 등과 같은 일부 선진국에서 글로벌 IT 경쟁력을 여전히 주도하고 있는 것을 통해서도 쉽게 알 수 있다. Baqir, et al.〔2009〕는 IT 정책을 설계했던 대로 실제로 잘 받아들여지지 않는 원인을 규명하고자 하였다. 가장 큰 요인으로 부처간 조정 기능의 결여와 일관성 없는 정책을 들고 있다.

최근에는 ICT 부문에 새로운 접근이 시도되고 있다. 생태계적 접근이 바로 그것이다. ICT 부문은 아주 복잡할 뿐만 아니라 기술 발전 등으로 인해 시시각각 변하는 속성이 있으므로 전체적으로(as a whole) 바라보는 시각이 필요하다는 것이다. 직간접으로 연계된 다양한 주체를 수용하고 이들 간의 상호 유기적 관계를 정확하게 이해하려는 노력을 의미한다.

〔표 2〕 ICT 정책 수립상의 도전 요인

1. 비전과 리더쉽 확보
2. 국가적 목표와의 일관성
3. 정부부처 간의 조정
4. 목표와 추진 방안에 대한 컨센서스를 끌어내기 위한 협의
5. 구체적이고 실질적인 실행계획의 수립 및 집행
6. 자원의 선별투자
7. ICT 정책 추진을 위한 법제도 체계 마련
8. 구현을 촉진하기 위한 지원체계 마련
9. 진행상황의 모니터링
출처: Ulrich & Chacko〔2005〕

최근 생태계 차원의 ICT 정책을 모색하려는 움직임이 일고 있다. 가장 대표적 연구자는 Fransman〔2010〕 이다. 그는 ICT 생태계를 크게 네트워크 요소기술 업체, 망 운영업체, 컨텐트/응용시스템 제공업체, 고객 등과 같은 네 계층으로 구분하여 이들 간의 관계를 분석함으로써 해당 국가의 ICT 정책 방향을 도출할 수 있다고 주장한다.

정보보안 이슈에도 생태계 접근이 시도된 적이 있다. Bauer & van Eeten〔2009〕는 사이버 보안에 생태계 접근을 시도한 첫 연구라 하겠다. 이들 연구의 핵심은 사이버 보안에 관한 다양한 주체 별로 그들 행동(보안 노력의 증대 또는 축소)을 유도하는 인센티브 요소를 비교 분석해봄으로써 생태계의 어떤 부문이 순기능(또는 역기능)으로 작동될 여지가 높은지를 추출할 수 있고 이 결과를 기초로 향후 정책 대안을 수립할 수 있다는 것이다. 이와 같은 접근은 다양한 주체가 참여하고 이들 간의 관계가 밀접하게 상호 연계된 문제에서 효과적으로 적용될 수 있으리라 믿는다.

III. 소프트웨어 개발보안 생태계 묘사

앞에서 복잡다단한 문제를 생태계 접근으로 이해하려는 노력이 크게 일고 있음을 보았다. 소프트웨어가 개발 단계에서부터 외부공격자가 이용 가능한 보안약점을 최대한 존재하지 않는 상태로 구축해 나가고자 하는 소프트웨어 개발보안 노력도 상당히 복잡한 문제이다. 여러 가지 기술적 문제도 있지만 다양한 이해관계자의 행동 욕구를 어떻게 효과적으로 조정하고 변화시켜 나갈 것인가와 같은 관리(management) 상의 문제도 깊이 스며들어 있다. 이런 차원에서 생태계 접근이 유용하고 효과적인 방안이 될 수 있다고 본다.

생태계 연구에서 생태계 묘사하는 방법이 매우 다양하다. 주체만 나열하기도 하고 이들 주체 간의 관계를 묘사하기도 한다. 또한 이 관계의 묘사에도 여러 방식이 쓰이고 있다. 어떤 주체 간에 관계가 존재한다는 점만을 화살표로 표기하는 경우도 있고 이들 관계에 대한 정의를 내리는 경우도 있다. 그 외에도 생태계 묘사에 있어 다양한 이슈가 존재한다고 하겠다.

본 연구에서는 소프트웨어 개발보안 생태계 묘사를 위해 몇 가지 원칙을 적용했다. 첫째, 가급적 관련 주체를 최대한 포함시킨다. 둘째, 주체 간의 주요한 관계에 대한 정의를 내린다. 셋째, 생태계 전체가 open

system 으로 묘사되어야 한다. 즉, 피드백 선순환 구조를 의미한다. 마지막으로, 생태계의 직접 참여자와 별도로 환경적 요소도 묘사되어야 한다.

소프트웨어 개발보안 생태계의 묘사를 위해 일련의 과정을 거쳤다. 주체의 식별, 관계의 설정 및 묘사, 이를 토대로 전문가의 피드백 의견을 반영하여 수정보완하는 것이 바로 그것이다.

주체로는 우선 정보시스템을 구축하고 이를 활용하는 부처/기관, 이들에게 시스템을 구축 또는 운영해주는 SI업체, 이들에게 고용되어 시스템을 개발하고 코딩해주는 개발자, 그리고 이들 시스템을 사용하는 사용자를 주요한 주체로 간주하였다. 아울러 소프트웨어 개발보안의 제도화에 관련된 공공 부문의 주체들도 포함시켰다. 여기에는 개발보안 정책부서(행정안전부), 한국인터넷진흥원, 예산부처, 그리고 '기타 보안 관련 기관'이 해당한다. 기타 보안 관련 기관이라 함은 보안과 관련한 KISA 외의 공적 주체를 의미한다. 여기에는 국정원, 금감원, 금융보안연구원, 검찰청, 경찰청 등이 포함된다고 하겠다.

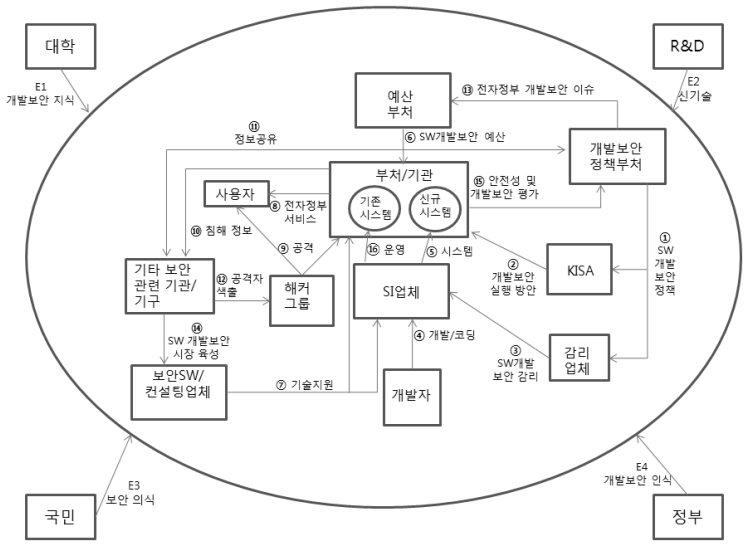
또한 소프트웨어 개발보안과 관련된 산업체도 주요한 주체일 수밖에 없다. 여기에는 현재 보안약점의 식별 및 제거 여부를 확인하게끔 되어 있는 감리법인, 보안SW/컨설팅업체 등이 포함된다. 아울러 보안약점을 악용해 정보시스템에 침입하는 공격자 즉 해커도 생태계의 한 요소임에 틀림이 없다.

앞에서 제시된 생태계에 직접 참여하는 주체 외에도 생태계의 환경 요소도 고려될 필요가 있다. 여기에는 대학, R&D 담당조직, 정부, 국민이 이들 환경 요소라고 하겠다. 한 예를 들어 이들 요소가 소프트웨어 개발보안 생태계에서 왜 필요한 지를 제시한다. 개발자들은 나름대로 자신만의 코딩 스타일을 갖고 있다. 한번 습득하면 그 코딩 스타일을 바꾸기가 쉽지 않다고 알려져 있다. 예를 들면, 시스템 사용자로부터 입력받은 데이터는 처리에 활용하기 전, 반드시 일정한 입력값 확인(validation)을 거쳐서 통과된 경우만 다음 단계로 넘어가고 그렇지 않을 경우 오류로 간주하여 입력 데이터를 무효화시켜야 한다. 이런 절차는 코딩의 표준에 해당한다. 이런 secure coding standard를 지켜나가지 않을 경우 보안약점에 노출될 가능성이 높아지게 되어 있다. 그러므로 이런 코딩 스타일 또는 표준 가이드라인을 대학교에서부터 인식시키고 교육시켜야 한다. 이런 차원에서 대학도 생태계 환경의 주요한 요소이어야 한다.

다음으로 수행될 일은 주체 간의 관계를 묘사하고 이 관계의 대표적 역할을 정의하는 것이다. 본 연구에서 이들 관계가 일련번호로 표시되어 있고 그 관계의 정의가 제시되어 있다. ([그림 2] 참조). 아울러 이들 간의 관계에 대한 구체적 묘사는 [표 3]에 제시된 바와 같다.

IV. 소프트웨어 개발보안 생태계 현상 분석

앞 절에서 소프트웨어 개발보안 생태계 모형을 제시하였다. 이 절에서는 이 소프트웨어 개발보안 생태



[그림 2] SW 개발보안 생태계

〔표 3〕 SW개발보안 생태계 주체별 역할

주체	화살표	역할
개발보안 정책부처	① SW 개발보안 정책	• 소프트웨어 보안성강화체계 관련 법·제도 정비, 체계관련 기준 및 지침 고시. (정보시스템구축·운영지침(행안부 고시, 2012. 6)) • 감리 활동에 반영되어야할 개발보안의 기준 및 가이드라인의 제정 및 보완 • 개발보안 관련 교육 프로그램의 기획 및 실행 지원
	⑬ 전자정부 개발보안 이슈	• 전자정부 시스템의 보안 실상과 이슈를 제시하여 이에 효과적으로 대응하기 위한 정책 방향 및 예산 지원 방향을 결정하는데 지원
KISA	② 개발보안 실행방안	• 소프트웨어 보안성 강화체계의 진단 및 시험과 관련된 규정을 수립. • 소프트웨어 보안강화 진단 방법론 및 기술을 개발하고, 관련 기준을 개발 및 공지 • 검증기관을 지정하고 기술지원 및 진단 결과를 인증. • 발주 공무원 및 개발자를 대상으로 소프트웨어 보안성 강화체계 교육을 수행. • 국외 전문기관과의 정책 및 기술 공유.
예산 부처	⑥ SW개발보안 예산	• 부처의 SW개발 시 보안성 강화를 고려한 예산 지원.
부처/기관	⑮ 개발보안 효과 및 수준	• 보유 정보자원의 보안성 수준과 이슈의 제공 • 시스템 구축 및 운영 상에 발견된 보안약점 및 제거 여부 등과 관련된 이슈 전달 • 개발보안 효과성 측정 및 제공
SI업체	⑤ 시스템	• SW보안성강화 기준에 따라 안전한 정보시스템 구축 제공
	⑯ 시스템 운영	• 기존 시스템의 운영 및 유지보수
개발자	④ 개발/코딩	• SW 개발보안 관련 기준에 입각한 개발 및 코딩 노력 수행
감리업체	③ SW개발보안 감리	• 신규 구축사업의 감리 수행시 SW개발보안 활동 수행 여부의 점검 • 구축한 소스코드 상의 보안약점 제거 여부 확인
기타 보안관련 기관/기구	⑪ 정보 공유 및 대응 방안	• 해커그룹의 정보시스템 공격 및 정보침해 발생 정보 공유 • 진화하는 해커그룹의 정보침해 사례나 유형 에 관해 관련 부처와의 정보 공유. • 정책 부처와의 연계를 통해 정보침해 예방 방안 마련.
	⑫ 공격자 색출	• 공격 및 침해 정보를 통한 공격지 파악 및 공격자 추적. • 공격 및 침해 유형 분석을 통한 공격자 추적
	⑭ SW 개발보안 시장 육성	• 관련 시장의 창출을 통한 전문업체 육성 • 해외 공격 유형, 관련 기술 및 연구 동향 정보 제공
보안 SW/컨설팅 업체	⑦ 기술지원	• 보안관련 기술을 가진 전문 인력이나 정보, 기술에 대한 자문 제공. • 정보보호 솔루션을 제시하고 정보보호 컨설팅 및 보안시스템 통합구축 업무 지원.
사용자	⑩ 침해 정보	• 외부 공격자로부터 시스템 공격이나 피해 발생 시 관련 기관 및 기구에 신고.
해커그룹	⑨ 공격	• 정보 시스템에 정보시스템이나 소프트웨어 내의 허점을 이용한 의도적인 침입 및 공격.
개별 부처/기관	⑧ 전자정부 서비스	• 안전한 정보시스템 및 서비스를 사용자 국민에게 제공
	⑮ 안전성 및 개발보안 평가	• 보유 정보자원의 안전성 평가 정보를 제공 • SW개발보안을 통한 안전성 기여 효과의 측정 및 제공

계 상의 현상적 문제점 및 이슈를 분석하고자 한다. 즉, 최근 첫걸음을 시작한 국내 소프트웨어 개발보안 제도화를 생태계 관점에서 어떤 문제점을 안고 있는지, 어떤 부분이 잘 작동되지 않는 지 등을 도출함으로써 향후 정책 방향을 수립하는데 기초자료로 활용하고자 함이다.

이를 위해 우리는 두 가지 분석을 시도하였다. 첫째는 소프트웨어 개발보안 생태계에서 흐름의 단절 여부를 파악하는 분석이다. 둘째는 생태계 주요 주체의 경제적 동인(incentive)을 분석함으로써 이들 주체의 기능성(functionality)을 판단하는 기법이다. 아래에서는 이 각각에 대해 제시한다.

4.1 생태계 연결고리 단절 분석

생태계는 노드(node)간의 연결고리(link)가 망

〔표 4〕 작동되지 못하는 연결흐름 및 원인

작동하지 않는 연결흐름	원인 및 배경
⑯ 시스템 운영	현 개발보안 지침에서는 신규 시스템 구축의 감리 시 약점의 제거 여부를 확인하도록 요구할 뿐, 기존 시스템은 이 지침에 해당되지 않음
⑮ 안전성 및 개발보안 평가	부처로 하여금 보유 전체 정보자원의 안전성 수준 및 개발보안 노력의 수준 및 성과를 피드백 형태로 제공하게끔 요구하는 사항 없음
⑩ 침해 정보	외부의 공격이 감지 또는 확인이 되었을 경우 공격자, 공격유형, 대응 내용, 피해 등을 관련 기관에게 제공하게끔 명문화되어 있지 못함
⑫ 공격자 색출	⑩ 등의 이유로 인해 공격자 추적, 색출, 공격패턴 파악이 체계적으로 이루어지고 있지 못함
⑥ SW개발보안 예산	예산 부처의 개발보안 중요성 인식 미비 및 한정된 정보화 예산으로 인해 개발보안 소요 경비의 미반영
⑬ 전자정부 개발보안 이슈	개발보안의 중요성, 이의 효과, 협력 및 거버넌스 방안 등에 대한 정보를 체계적으로 전달하고 공유하는 장치 미비
⑩ 침해 정보 공유	공격 및 침해 정보의 기관 간 공유가 제대로 이루어지지 못하고 있음
⑭ SW개발보안 시장 육성	코딩 차원에서만 보안약점의 제거를 추구하다 보니, 개발보안의 기획에서부터 구축 및 운영 전 단계에 걸친 전문 경험을 필요로 하지 않음.

형태로 구성되어 있는 것으로 이해할 수 있다〔Basole & Karla, 2011〕. 생태계의 이런 묘사는 수학의 그래프(graph) 이론과 유사하다. 실제 생태계로 묘사된 문제의 경우 그래프 이론을 적용한 다양한 분석이 시도되고 있다〔Wardle, 1998; Erdelyi, 2006〕. 한 예로 Allesina, et al.〔2005〕은 자연생태계에서 중요하게 연계된 실체의 식별에 그래프 이론을 적용하고 있다.

본 연구에서는 생태계의 작동을 위해선 당연하게 연결되어 있어야 하는데 그러지 못한 연결고리를 찾아내는 방법을 적용한다. 즉, 현 생태계에서 작동되지 않고 있거나 고려되지 못한 연결 흐름을 도출해내는 것이다. 이 기법은 그래프 이론의 초보적인(primitive) 적용에 가깝다고 볼 수 있다.

현 소프트웨어 개발보안 생태계에서 제 역할을 하지 못하는 연결흐름도 몇 가지가 존재한다. 이들과 그의 원인은 〈표 4〉에 제시되어 있다. 한 예로, 현재의 소프트웨어 개발보안 제도는 신규 시스템의 구축 사업에 감리가 이루어질 경우 이 감리법인에게 구축된 코드에 보안 약점의 존재 및 제거 여부의 확인을 요구하고 있으므로, 기존 시스템의 경우 이 지침 적용의 범위에서 제외되어 있다. 실제 우리 정부의 현존 시스템의 숫자는 1만5천개 이상[1]이고 여기엔 민원24를 포함한 대부분의 주요 민원 시스템이 여기에 포함된다. 이와 같이 중요한 현존 시스템을 제외한 채 전자정부 시스템의 안전성을 논하기는 어려울 것이다.

그 외에도 소프트웨어 개발보안 생태계를 구성하고 있는 환경적 요소도 고려해볼 필요가 있다. 이들 요소들도 현재 생태계에서 잘 작동되고 있다고 보긴 힘들 것이다. 컴퓨터 프로그래머 및 개발자를 교육하고 양성하는 대학교에서 아직까지 secure coding 을 집중적으로 또는 프로그래밍 교육의 기본적 사항으로 교육을 시키지 못하는 형편이다. 아울러, 개발보안 관련 기술과 지식은 날로 변화하고 진화하고 있으며 외국에선 정부 차원에서 관련 연구자들의 정보 공유 및 공동연구가 활발히 전개되고 있다. 미국의 SAMATE 프로젝트가 좋은 사례에 속한다고 하겠다〔Black, 2007〕. 그러나 우리 나라에선 아직 이와 관련한 R&D 역량을 결집시키거나 관련 기술 개발에의 지속적 지원 노력이 부족하다고 하겠다. 아울러 국민이나 정부도 아직까지 소프트웨어 개발보안에 대한 인식이 결여되어 있다고 하지 않을 수 없다.

4.2 생태계 주요 주체의 동인 분석

생태계의 또 다른 주요한 특징은 여러 다른 주체가 존재하고 이들은 독자적이고 분권화된 의사결정을 수행한다는 점이다〔Tian, et al., 2008〕. 즉, 생태계의 전체 수준은 이들이 내린 의사결정의 총체적 결과에 기인한다고 볼 수 있다. 이들이 어떤 의사결정을 내리는지 또는 어떤 요인들이 이 과정에 영향을 주는 지를 분석하는 것은 생태계 연구에서 의미 있는 시도라 하겠다.

1) 2012년 8월말 현재, 정부 정보자원 데이타베이스에 등록되어있는 시스템은 15,197대이다. 기관별로는 중앙행정부처(소속 포함) 2,366대, 자치단체(광역/기초) 7,461대, 공공기관 4,883대, 기타(입/사/헌법, 교육기관, 기타 공공) 487대이다.

Bauer & van Eeten(2009)은 cyber security 생태계 연구에 이런 접근을 시도하였다. 이들은 ISP업체, 소프트웨어업체, 전자상거래업체(금융기관 포함), 사용자를 주요 주체로 간주하여, 이들 각자가 보안을 강화하려는 동인과 보안 강화를 기피하는 동인(incentives)을 분석함으로써 이들 행동을 보다 심층적으로 이해할 수 있다고 강조하였다.

한 예로 ISP 업체를 들어 설명한다. ISP 업체는 보안을 강화하려는 동인으로 첫째 고객 지원 비용을 제시하였다. 보안이 뚫려 고객의 컴퓨터가 오염될 경우, 수많은 사용자가 해당 ISP 업체의 콜센터로 전화를 하게 될 것이고 이는 엄청나게 많은 고객 대응 비용을 발생시킬 수 있을 것으로 예상할 수 있다. 둘째, 브랜드 가치도 또 다른 동인으로 지적된다. 즉, 보안이 취약하여 서비스 중단이 되거나 고객 정보 등이 유출될 경우 ISP 업체의 명성은 추락하고 브랜드 가치는 하락할 것이다.

반대로 보안 강화 노력을 적극적으로 하지 않으려는 데 나름대로의 동인이 작용한다고 볼 수 있다. ISP 업체의 경우, 보안 강화에 요구되는 비용 부담이 큰 동인으로 작용할 수 있다. 아울러 고객 확보에 소요되는 비용의 증가도 또 다른 요인이다.

본 연구에서도 이와 비슷한 방법으로 분석하였다. 우리는 소프트웨어 개발보안 생태계의 주요 주체로 SI업체, 개발자(개발전문 하청회사, 프리랜서 개발자, 계약직 개발자를 모두 포함하는 주체), 감리업체, 보안SW/컨설팅업체를 꼽았다. 이들은 모두 산업을 구성하는 주체이므로 경제적 동인에 입각해 그들의 행동을 결정하는 경향이 강하다. 이들 외의 정부기관 및 부처 등은 상대적으로 경제적 동인에 영향을 덜 받는다고 보았으므로 이들은 우리 분석의 주요 주체에서 제외되었다.

이들 주요한 산업 주체 별 보안강화 동인과 보안강화 기피 동인은 〈표 5〉에 제시된 바와 같다. 감리업체를 들어 이들의 동인을 분석해보기로 한다. 우선, 개발보안 강화 역량을 키우려는 동인으로 사후 문제 발생 시 책임소재 문제, 감리전문업체로의 명성 상실, 향후 감리사업에의 참여 기회 박탈을 들었다. 보안 약점이 있는 채로 시스템 구축 사업이 종료된 후 운영되는 과정에서 보안 약점을 이용한 공격에 노출되었을 경우 책임 소재 문제가 발생할 수 있으며, 아울러 감리전문업체로의 명성에 큰 상처를 입약점이 있다. 마지막으로 향후 감리사업에의 참여가 근원적으로 박탈되는 경우까지 고려해볼 수 있다.

감리업체가 오히려 개발보안 강화 역량을 기피하는 동인도 존재한다. 여기에는 다양한 동인이 존재한다. 기술력을 갖춘 보안 약점 전문진단원의 확보, 양성, 유지에 소요되는 비용, 보안 약점 진단도구의 도입 및

〔표 5〕 주요 주체별 인센티브 분석

주체	개발보안 강화 동인	개발보안 강화 기피 동인
감리업체	• 사후 문제 발생 시 책임소재 문제 • 감리전문업체로의 명성 상실 • 향후 감리사업에의 참여 기회 박탈	• 기술력 갖춘 전문진단원의 확보 비용 • 진단원 양성 비용 과다 • 감리활동 대가 미흡으로 인한 수익성 악화 • 진단도구 등의 도입 및 이의 숙련화 소요 비용 • 보안약점 완전제거 가능성에의 의문 • 길지 않은 감리활동 기간의 지체 가능성 • 보안약점 이슈로 전체 감리활동 미종료 가능성
SI업체	• SI 업체 명성에 피해 • 사후 보완 및 지원 소요 비용 과다 • 사후 문제 발생시 책임 소재 문제 • 이후 정보화 사업에의 참여기회 박탈	• 개발보안 기술력을 확보한 개발자의 확보 난망 • 개발자 교육 및 의식 변화 비용 과다 • 이에 따른 개발기간 지체 • 수익성 악화 가능성 • 보안약점 완전제거 가능성에의 의문 • 품질요원, 분석요원 등의 추가 확보 및 교육 소요 비용
개발자	• 전문 개발자의 명성에 피해 • 사후 문제 발생시 책임 소재 문제 • 이후 프로젝트 참여 기회 박탈	• 개발 소요 업무 확대 및 소요 기간 증대 • 자신에게 익숙한 코딩 스타일 미준수와 이에 따른 기술력 확보 난망 • 개발보안 기법 학습 비용 및 기간 증대 • 노력 투입 대비 비용효과 악화
보안SW/ 컨설팅업체	• 업체 명성에 피해 • 시큐어 코딩 분야에의 진출 기회 확보	• 전문 기술인력의 확보 난망 • 수익성 악화 • 보안약점 완전제거 가능성에의 의문 • 핵심 사업영역과의 마찰 가능성

숙련화 비용 부담이 가장 큰 동인이라 하겠다. 또한 전문진단원을 두었다 하더라도 소스코드 상의 보안 약점을 기술적으로 완벽하게 식별하고 이를 완전히 제거할 수 있는 것인가에 대한 의문이 존재한다. 기술적으로 완벽하게 할 수 없는 것이라면 개발보안 노력을 적당한 수준에서 수행하는 것이 최선이라며 행동에 임할 수 있다고 본다. 그 외에도 불분명한 보안 약점 이슈로 인해 길지 않은 감리활동 종료 시점이 지연될 경우 입을 경제적 피해 및 수익성 악화도 개발보안 강화 노력을 기피하는 요인의 하나이다.

주체별 동인 분석의 결과, 우리는 다음과 같은 몇 가지 공통점을 식별할 수 있었다. 첫째, 개발 보안을 강화하려는 동인보다 오히려 이를 기피하려는 동인이 훨씬 더 크고 다양하다. 둘째, 개발 보안 강화 동인은 주로 간접적이고 미래에 발생하는 가치에 관련 된 것임에 비해, 그 반대 동인은 훨씬 더 현실적이고 지금 바로 당면하는 이슈에 속한다.

4.3 개발보안 생태계 분석 종합 결과

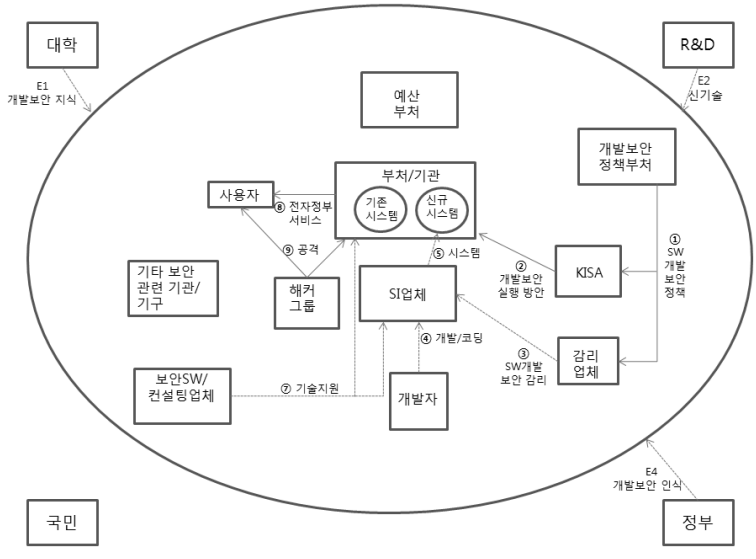
여기서는 앞에서 이루어진 단절된 연결흐름 분석과 주요 주체의 동인 분석을 통해 나온 내용을 간략하게 종합해보기로 한다. Moore〔1993〕는 생태계가 제대로 작동하기 위해서는 이에 참여하는 각 주체가 전체적인 변화 방향에 맞춰 각 주체가 자신의 역량과 역할을 공진화(co-evolve)해 가야함을 역설하고 있다. 제도적 또는 경제적 요인 등으로 인해 특정 주체가 자신의 역할을 다하지 못하거나 자신의 역량을 적극 키우려 하지 않는 생태계는 건강한 생태계라 할 수 없다.

소프트웨어 개발보안 생태계의 경우 일부 연결고리가 작동하지 않고 있다. 아울러 주요 주체들이 자신의 역량을 강화할 동인이 별로 크지 않다는 현실적 이슈도 존재하고 있다. 이런 분석 결과를 종합하여 현 개발보안 생태계를 〈그림 3〉과 같이 묘사할 수 있을 것이다. 단절된 연결고리는 표기되지 않았으며 스스로의 역량을 강화할만한 동인이 부족한 주체로부터의 연결고리는 점선으로 표기되었다.

이 생태계의 현상적 특징은 몇 가지로 묘사될 수 있다. 첫째, 주요한 주체의 역할이 배제되어 있음을 알 수 있다. 예산부처, 기타 보안 관련 기관/기구 등이 대표적이다. 둘째, 주요한 연결고리가 점선으로 표기되어 있어 이들의 역할이 소극적 또는 명목상으로만 수행될 가능성이 존재한다. 마지막으로, 생태계의 전체 흐름이 피드백 회로(feedback loop) 형태로 작동되지 않음을 알 수 있다. 한 예로, 부처/기관으로 다양한 입력이 작동되고 있으나 이들로부터의 출력은 이루어지지 않아 현재 노력이 발전적 선순환 형태로 작동되기 어렵다는 점을 시사한다고 하겠다.

V. 개발보안 생태계의 향후 발전 방향

앞에서 소프트웨어 개발보안의 현상적 이슈와 문제점을 살펴보았다. 여기서는 이런 생태계적 문제점을 극복하기 위한 방안을 간략하게 제시한다.



〔그림 3〕 개발보안 생태계 현상

〔표 6〕 개발보안 생태계 향후 발전 방향

구분	주요 내용	기대효과
1. 기존 시스템의 개발보안 적용	- 운영중인 시스템에도 보안약점의 식별 및 제거 노력이 이루어지도록 제도 개편 - 다양한 정책 대안이 가능(예: 기관별 정보화 수준 측정시 개발보안 성도 평가)	⑮, ⑯
2. 개발보안 노력의 성과 측정 및 효과성 공지	- 부처별 개발보안 노력에 투입된 비용 대비 효과 측정 - 이를 관련 부처와의 공유를 통한 개발보안 인식 확산	⑮, ⑬, ⑥, ⑦, E3, E4
3. 침해 정보의 공유 및 기관 간 협력 강화	- 개발보안 정책부처 및 기타 관련 기관과의 정보 공유 - 기관간 역할 분담 명확화 및 관련 거버넌스 구조 개편	⑩, ⑪, ⑫, ⑭
4. 개발보안 R&D 활성화	- 개발보안 기술 및 이론 개발 연구에 지속적 지원 - 산학관 공동 노력의 활성화	E2, E1
5. 개발보안 적용 시 추가경비 인정	- 개발보안 적용 적정예산의 편성 및 지원 - 관련 전문가의 노임 적용 단가 대폭 인상	⑥, ⑭
6. 개발보안 노력을 코딩에서 개발 전단계로 확장	- 시스템 기획 단계에서부터 구축 및 운영 전 과정에 적용	④, ⑤, ⑯
7. 관련 가이드라인을 이해하기 쉽도록 개편	- 개발보안 노력은 개발자에게 기술적으로 큰 부담으로 작용되지 않고, 정해진 가이드라인을 따르기만 하면 되도록 관련 가이드라인의 개편	②, ③ ④, ⑤, ⑯

생태계를 건강하고 미래 지향적으로 바꾸어 나가는 방법에는 다양한 접근이 가능하다. 어떤 점에서 보면 한두 가지 방안으로 문제를 다 해결할 수 있다고 말하기도 어렵다. 무엇보다 중요한 것은 생태계의 각 주체가 전체적인 변화 방향에 맞춰 스스로의 역량을 강화해나가고 스스로 진화 및 혁신해 나가야 하는 원칙이 작동되게끔 하는 것이라 할 수 있다.

본 논문에서는 이런 원칙이 작동되게끔 기여할 수 있는 몇 가지 대안을 제시하고자 한다. 이들 대안과 기대 효과를 〈표 6〉과 같이 제시한다. 가장 우선적으로 고려되어야할 대안은 기존 시스템에 개발보안을 적용하기 위한 제도화가 필요하다. 수많은 시스템이 구축되어 365일 24시간 이용되고 있는 현실에서 이에 대한 시스템 안전성을 증대시키기 위한 제도는 필요하다고 본다. 여기에 적용될 수 있는 대안은 다양하다. 현재에도 수행되고 있는 매년 기관별 정보화 수준 지표의 하나로 기관 보유 정보시스템의 개발보안성을 추가하는 것도 방안이 될 수 있고, 또 다른 대안으로는 향후 수년 내에 기관 보유 정보자원의 개발보안성을 점검하고 확인을 거치는 사업을 점진적으로 수행하는 것도 한 방편이 될 수 있다. 이런 제도가 마련됨으로써 얻을 수 있는 기대효과도 다양하다. 기존 정보시스템의 운영이 보다 안정적으로 이루어질 수 있고(⑯), 정보자원의 안전성 및 개발보안 노력에 대한 체계적 평가가 이루어질 수 있다(⑮).

둘째로 개발보안의 인식 확산이다. 개발보안 노력의 성과 측정 모델을 개발하고 정기적으로 실시함으로써 개발보안 노력의 중요성을 입증시킬 뿐만 아니라 국민, 정부 등 제 주체의 인식을 새롭게 정립하는 효과를 기대할 수 있다.

셋째, 침해 정보의 공유를 활성화하는 것이다. 현재는 특정 시스템이 공격을 당하여 피해를 입을 경우, 이를 외부에 알리지 않고 내부적으로만 수습하려는 경향이 강하다. 특히 공공 부문의 경우 이런 현상이 더욱 심하다고 말할 수 있다. 이런 접근에서 탈피하여 공격 또는 침해 관련 정보를 기관 간에 공유함으로써 이렇게 취합된 실시간 정보를 토대로 모니터링을 강화하고 공격패턴 분석 등을 통한 공격자 추적 및 색출을 보다 용이하게 할 수 있을 것이다.

넷째는 개발보안 관련 R&D 강화이다. 개발보안 문제는 아직 기술적으로 풀어야할 이슈가 아주 많다. 이에 대한 기술 개발 및 공유를 보다 활성화하여 나날이 발전되고 있는 공격 기술에 효과적으로 대응하려는 노력이 필요하다.

다섯째, 개발보안 적용 시 소요 비용을 인정해주는 제도적 장치의 마련이 시급히 필요하다. 감리의 경우, 현재에도 부가가치가 높지 않은데 개발보안까지 떠맡게 됨으로써 수익성이 더 악화될 가능성이 아주 높다. SI업체 및 개발자도 마찬가지이다. 개발보안을 적용하는데 추가적으로 발생하는 경비를 예산에 반영해주는 노력이 강구되어야 한다.

여섯째는 개발 보안 노력을 코딩에만 머무르지 않고 구축 전 단계로 확장시킬 필요가 있다. 즉, 시스템의 기획에서부터 분석, 설계, 구축, 테스트, 그리고 운

영 등 전 단계에 결쳐 수행되게끔 제도의 틀을 수정보완할 필요가 있다[Colley, 2010].

마지막으로 개발자에게 개발보안에 대한 부담을 덜어주기 위한 조치가 필요하다. 현재의 개발보안 관련 가이드라인은 상당히 복잡하고 난해한 편이다. 앞으로는 개발자가 해당 단계에서 반드시 따라야할 내용을 알기 쉽게 제시하는 방향으로 개편될 필요가 있다. 즉, 개발 보안 노력이란 이 가이드라인을 준수하기만 하면 되는 것이라고 개발자가 인식할 수 있도록 되어야 한다.

VI. 결언 및 향후 연구 방향

본 연구는 소프트웨어 개발보안을 생태계 관점으로 접근한 연구이다. 개발 보안 생태계를 묘사하였고, 이를 토대로 현재의 개발보안 생태계 문제와 이슈를 제시하였다. 나아가서 이 개발보안 생태계의 발전을 위한 정책 방향을 제시하였다.

본 연구는 정보시스템 보안 이슈를 국내에서 처음으로 생태계 접근의 분석을 시도하였다는 점에서 의미있다고 하겠다. 아울러 여기서 제시된 생태계 모델 및 분석 결과는 이후 정책적 논의의 출발점이 될 수 있을 것이다. 즉, 더 많은 관련 주체를 끌어들여 현재 처한 상황적 이슈를 논의하고 향후 정책적 대안을 모색해나가는 데 있어 기초 프레임워크로 활용되었으면 하는 바람이다.

그런 기여에도 불구하고 실증연구가 시도되지 않았다는 점이 큰 한계라고 본다. 아울러 외국의 개발 보안 생태계와의 비교 분석이 실시되었더라면 우리에게 시사하는 바가 클 수도 있었다고 본다. 향후에는 본 생태계를 기초로 다양한 이해관계자를 대상으로 설문 또는 인터뷰 조사를 실시함으로써 더 피부에 와 닿는 이슈와 대안을 모색할 수 있을 것이다. 아울러 미국, 일본 등과 같이 개발 보안 분야에서 앞선 국가들과의 비교 분석을 통해 우리 제도의 특성과 향후 대안을 도출해내는 연구도 시도될 필요가 있다고 본다.

참고문헌

[1] 김성근, "정보시스템 보안강화체계 적용을 위한 제도화 방안 개발," 한국인터넷진흥원, 2009.

[2] 김성근, "정보시스템 소프트웨어 보안성강화체계 제도화 및 활성화 방안 개발," 한국인터넷진흥원, 2010.

[3] 김성근, 안남규, 이진실, "정보자원관리 관련 법체계 분석: 미국과의 비교 분석을 중심으로," Information Systems Review, 7(1), pp. 21-40. 2005.

[4] 이규정, 김현경, "신정부의 정보화 법체계 개편방향과 과제," 한국정보사회진흥원 IT정책연구시리즈 2, 2008.

[5] 이연수, 이수연, 윤석구, 전재성, "주요국의 사이버안전 관련 법·조직체계 비교 및 발전방안 연구," 국가정보연구, 1(2), pp. 35-116, 2009.

[6] 이창범, "미국, 영국, 독일의 기반보호법 체계에 관한 연구," 한국인터넷진흥원, 2010.

[7] 조성훈, "행안부, SW개발시 보안기법 적용 의무화," 중앙일보, May 17 2012.

[8] C. Tian, B. Ray, J. Lee, R. Cao, and W. Ding, "BEAM: A Framework for business ecosystem analysis and modeling," IBM Systems Journal, vol. 47, no. 1, 2008.

[9] E. Erdelyi, "Graph theory application for investigating agro-ecosystems effected by extreme weather conditions," Applied Ecology and Environmental Research, vol. 4, no. 2, pp. 181-187, 2006.

[10] F. Capra, The web of life, Doubleday Anchor Books, 1996.

[11] F. M. James, "Predators and Prey: A New Ecology of Competition," Harvard Business Review, May-June, pp. 75-86, 1993.

[12] G. Wardle, "A Graph Theory Approach To Demographic Loop Analysis," Ecology, vol. 79, pp. 2539 - 2549, 1998.

[13] J. Bauer and M. van Eeten, "Cybersecurity: Stakeholder incentives, externalities, and policy options," Telecommunication Policy, vol. 33, no. 10, pp. 706-719, 2009.

[14] J. Colley, N. Pohlmann, H. Reimer and W. Schneider, "Why secure coding is not enough: Professionals' perspective," (Editors), ISSE 2009 Securing Electronic Business Processes, Viewegg + Teubner, pp. 302-311, 2010.

[15] K. Higgins, "SQL Injection hack infects 1 million web pages," InformationWeek,

August 10, 2012.
〔16〕 M. Baqir, P. Palvia, and H. Nemati, "Evaluating Government ICT Policies: An Extended Design-Actuality Gaps Framework," Proceedings of Seconds Annual SIG GlobDev Workshop, Phoenix, USA, Dec. 14, 2009.
〔17〕 N. Davis, "Processes for producing secure software," Security & Privacy, vol. 2, no. 3, May-June, 2004.
〔18〕 OECD, "Information Technology Policies: Organizational Structure in Member Countries," OECD, 1995.
〔19〕 P. Black, "SAMATE and Evaluating Static Analysis Tools," Ada User Journal, vol. 28, Number 3, 2007.
〔20〕 P. Bowen, E. Chew, and J. Hash, "Information Security Guide for Government Executives," NIST, 2007.
〔21〕 P. Ulrich and J. Chacko, "Overview of ICT Policies and E-Strategies: An Assessment on the Role of Governments," nformation Technology for Development, vol. 11, no. 2, pp. 195-197, 2005.
〔22〕 R. Basole and J. Karla, "On the Evolution of Mobile Platform Ecosystem Structure and Strategy," Business & Information Systems Engineering, pp. 313-322, 2011.
〔23〕 S. Allesina, A. Bodini and C. Bondavalli, "Ecological subsystems via graph theory: the role of strongly connected components," OIKOS, vol. 110, pp. 164-176, 2005.

〈著者紹介〉

김 성 근 (Sung Kun Kim) 정회원
1979년 8월: 국립부산수산대학교 경영학사
1985년 12월: New York University 석사(전공: 정보시스템, 부전공: 컴퓨터과학)
1988년 6월: New York University 박사(전공: 정보시스템, 부전공: 컴퓨터과학)
현재: 중앙대학교 경영학부 교수 및 국가정보화전략위원회 위원(실무위원장)
〈관심분야〉 enterprise architecture, ICT 정책, ICT 생태계 등

이 재 일 (Jae-il Lee) 정회원
1986년 2월: 서울대학교 계산통계학과 졸업
1988년 2월: 서울대학교 계산통계학과 석사
2006년 2월: 연세대학교 컴퓨터과학과 박사
현재: 한국인터넷진흥원(KISA) 정보보호본부장
〈관심분야〉 SW 개발보안, 개인정보보호, 정보보호 정책 등