Journal of Digital Convergence
Vol. 16. No. 6, pp. 205-212, 2018

ISSN 1738-1916
https://doi.org/10.14400/JDC.2018.16.6.205

정보보안체계 운영경험 진단을 통한 국가 사이버보안 거버넌스 모델 연구 방법

방기천
남서울대학교 멀티미디어학과

A Building Method of Designing National Cyber Security Governance Model Through Diagnosis of Operational Experience

Kee-Chun Bang
Department of Multimedia, Namseoul University

요 약 본 연구에서는 국가 전략적 차원에서 보안 거버넌스를 효율화시키기 위한 새로운 개념의 정보보안 거버넌스 모델 설계 방법을 제안한다. 이를 위해 우리의 운영 경험을 진단하고, 새로운 모델 설계 방법을 도출하였다. 그동안 국가 정보보안 활동은 지식 전달 위주로 인식되었고 활동의 동기 부여와 실행력 확보가 취약하였다. 결과적으로 보안 사각 지대가 늘어나고 대형 보안 사고가 빈발하여 해결이 필요한 과제로 대두되었다. 국가 사이버보안 거버넌스는 국가 리더의 책임하에 상단의 정책에서 하단의 실행까지 총체적으로 시스템화되어야 한다. 본 연구는 이같은 접근 방법에 기반하여 한국형 보안 거버넌스 모델의 종합 프레임워크를 제시하고 이를 비전, 목표, 과정, 수행 등 4개의 아키텍처 설계로 구체화시킴으로써 국가 거버넌스 모델 설계의 기반을 도출하였다. 라이프 사이클 흐름상의 문제점 진단, 환경변화에 기초한 보안 정책, 모든 주체의 참여가 반영되는 새로운 틀에 대하여는 계속적인 연구가 필요하다.

주제어 : 정보보안체계, 운영경험, 진단, 국가사이버보안, 거버넌스모델

Abstract This Study aims to propose a new information security governance model design method for streamlining security governance at national strategic level. The research method of this study is to diagnose our operational experience and to derive a new model design method. In the meantime, national information security activities were perceived to be focused on knowledge transfer, and motivation of activities and securing of executive power were weak. As a result, security blind spots and frequent occurrence of large security incidents have become unresolved challenges. National cyber security governance should be grouped together as a whole systematically from the upper policy to the lower level of performance under the responsibility of the national leader. Based on this approach, this study presented the comprehensive framework of Korean security governance model and embodied it into four architectural designs such as vision, goal, process, and performance, thus deriving the foundation for future national governance model design. Further research is needed to diagnose problems in life cycle flow, security policies based on environmental changes, and new frameworks in which all subjects participate.

Key Words : Information Security System, Operational Experience, Diagnosis, National Cyber Security, Governance Model

*Corresponding Author : Kee-Chun Bang(bangkc@nsu.ac.kr)
Received April 25, 2018 Revised June 8, 2018
Accepted June 20, 2018 Published June 28, 2018

1. 서론

보안 거버넌스는 정보의 기밀성(Confidentiality), 무결성(Integrity), 연속성(Availability)을 위한 '이사회와 고위 경영진의 책임'으로 정의된다. 정보보호 거버넌스의 뿌리는 기업 거버넌스(Corporate Governance)이다. 기업 거버넌스는 그 하위에 여러 거버넌스로 나뉘는데 IT 거버넌스도 그 중 하나이다. IT 거버넌스의 한 부분이던 정보보호가 시간이 지나면서 정보보호 거버넌스로 발전되어 지금은 IT 거버넌스와 상관관계를 갖게 되었다. 보안 거버넌스는 리더십, 조직 구조, 프로세스들로 구성되는데 전체 기능의 흐름이 라이프 사이클을 기반으로 시스템화 되어야 한다. 우리나라는 국가보안 거버넌스 운영 경험에서 몇가지 개선 필요성이 노출되었다. 보안 활동은 지식 전달 위주로 인식되었고 보안 활동의 동기 부여, 실행력 확보가 취약하였다. 결과적으로 보안 사각 지대의 존재와 대형 보안사고 빈발이라는 결과가 초래되었다. 어느 국가나 진단을 실시한다면 같은 현상이 노출되겠지만 국내의 사회 전반을 고려해보면 보안활동 취약 계층, 기업이 존재한다. 국가 리더의 책임하에 전 조직이 상단의 정책에서 하단의 수행 활동까지를 총체적으로 하나로 전략화가 필요하다. 본 연구는 이같은 사상을 반영하는 새로운 개념의 정보보안 거버넌스 모델 설계 방법을 제안한다. 기술 순서는 서론, 관련 연구, 우리의 보안 거버넌스 제도 운영 경험, 새로운 보안 거버넌스 모델 설계 방법, 결론의 순서이다.

2. 관련연구

2.1 국제적인 정보보호 패러다임

국제적인 정보보호(Information Security) 패러다임은 기술적 관점에서 관리 중심 조직화 시대 단계를 지나 오늘날의 정보보호 거버넌스 단계로 진입하고 있다. 거버넌스 단계는 보안에 대한 시대적 요구가 정보 보호 활동의 역사와 성숙도를 기초로 하여 전체적인 틀을 구성하여 보안 요구에 대한 해답을 주는 대안이기 때문이다.

Table 1. Changes in international information security paradigm

step	1 step	2 step	3 step	4 step
Age classification	50's - early 80's	Early 80's - mid 90's	Late 90s -2002	2002 - present
paradigm	Technology concentration	Management centered	Organization	Security governance
Interests	Technology and techniques, Introduction of mainframe, operating system	Distributed Computing, WWW Chief Executive Officer, ISSO, Organization	Extensive cooperation system, international standards, certification, culture, measurement	Governance, Compliance, Leadership

2.2 해외 국가 거버넌스 적용 동향

세계 각국은 4차 산업혁명의 거대한 변화와 흐름 속에서 보안의 중요성을 인식하고 사이버 보안 관련 정책들을 발표하고 있다. 이는 사이버 보안 분야의 글로벌 주도권 확보를 위한 노력의 일환이기도 하다. 미국의 '국가 사이버보안 인력양성 종합대책(NICE : National Initiative for Cyber Security Education)'과 이스라엘의 '마그니엄 류미트(Magshimim Lemit)' 등은 이러한 움직임의 대표적인 예이다. 미국, 영국, 독일 등 주요국들의 사이버 방어 추세는 사이버 방어 체제 마련에 있어 민간 영역과의 연계 확대 및 민간 영역 조율 기능을 강화하는 추세이다. 과거 사이버 방어는 국가 안보에 위협이 될 수 있는 군사시설 및 주요 정부기관을 겨냥한 공격에 대해서만 한정적으로 영향력을 행사했지만, 최근 사이버 위협은 사실상 온 오프라인 모든 영역에서 동시다발적으로 발생하기 때문에 국가 사이버 방어 체제도 점차 민간 영역으로 확대되고 있다. 이에 따라 기존 군대 기반의 사이버 방어 체제도 조직 개편을 통해 민간 부문과의 연계를 강화하거나 아예 민간 조직 형태로 전환되어 보다 유연한 사이버 방어 업무를 수행한다[1].

○ 미국 - 거버넌스 구성 요소 간 유기적 기능

보안 거버넌스 구성 요소는 외부 환경 즉, 법령과 예산 및 감사의 통제로부터 각 연방정부는 1)전략 기획 2)정보보안 거버넌스 구조 3)역할과 책임(R&R) 4)연방 엔터프라이즈 아키텍처(FEA) 5)정책과 가이드라인 6)구현 과정을 거쳐 거버넌스를 구현한다. 구성 요소들은 지속적으로 감시되고 1년 회계연도마다 갱신되는 생명 주기를 가진다. 백악관의 행정시행령, 의회에서의 FISMA 법령,

예산청(OMB)의 예산 지원, 감사원(GAO)의 사업 감사 등 외부 지원하에 각 연방 정부에 대한 거버넌스를 요구하고 있다. 그 결과 OMB가 각 연방정부의 보안수준을 의회와 감사원, 백악관에 보고하는 체계를 가지고 있다 [1,2].

○ 영국 - 사이버보안 추진 체계 매년 보완 수정

사이버보안 추진 체계는 개선이 필요한 전략이나 이행사항들은 보완하고 수정해 나감으로써 매년 발전하고 진일보한 전략이 수립된다.

○ 독일 - 보안체계 민간 비상대응팀과 연계

연방정부 비상대응팀(CERT-Bund)을 구축하고, 이를 민간 비상대응팀과 연계하는 노력을 진행해 왔다. 연방범죄수사청 내에 설치된 연방테러 대책 합동 본부(GTAZ)를 기초로 국가 사이버 방어센터를 구축하였다 [3].

2.3 보안 거버넌스 속성 진단

보안 거버넌스의 필요성은 인지하고 있으나 거버넌스 자체의 속성상 다음과 같이 구현의 어려움이 있다.

- 조직 구성 최적안 도출의 어려움

국가의 전반을 모두 진단하기는 대단히 어려운 일이이다. 종합적 관점으로 거버넌스 측면에서 국가 정보 보안 조직 구성에 대한 최적안 도출은 어려움이 있다. 특히, 각 IT 부처의 업무 분담 구조를 분산형 또는 연방체제로 단순 비교 및 효율성 판단이 어렵다. 사이버 공격과 개인정보 유출, 산업정보 유출 등 많은 정보보안 사건이 발생하면서도 이를 종합적이고 효율적으로 방어하기 위한 최적안 정부 조직을 도출하기란 쉽지 않은 과제이다.

- 보안 거버넌스 성과 측정의 어려움

보안 거버넌스는 상당한 예산이 소요되며 국가의 보안사고 발생 집계만으로는 투자 성과 측정이 어렵다. 구체적으로는 보안 경영 평가 기법에 대한 방법론 문제, 경쟁 모델의 가능성 여부, 성과보상제도 자체의 제도화 과제 등이다. 또한 계획, 운영, 진단, 개선 등 거버넌스 기능의 피드백도 용어는 가능하지만 국가적 거버넌스라는 소재를 대상으로 가능성 여부가 불확실하다고 볼 수 있다. SSE-CMM은 보안시스템의 효과적인 개발을 도모하기 위한 보안공학적 원칙들이 개발 기관에 얼마나 잘 내재화되어 있는지를 평가하기 위한 방법론들로 구성된다. 보안 거버넌스는 다양한 요소간 상호작용으로 기능을 유지하지만 성과 측정의 모델이 존재하지 않고 측정방법론 자체가 어려운 성격을 가지고 있다.

- 시스템화된 기능 구현의 어려움

시스템화는 효율적인 구조화 방법이지만 기존의 운영실태 조직 단위로 주로 지시에 의한 긴급업무 착수, 대책을 일회성으로 시행하는 정책추진방법, 보안사고 발생시 예방보다 사후 처방이 주류를 이루고 있다고 보이며 요소(element), 연계(connectivity), 소통(flow), 종합 제어(control), 입출력(input-output)으로 이루어지는 시스템화된 기능 구현의 어려움이 존재한다.

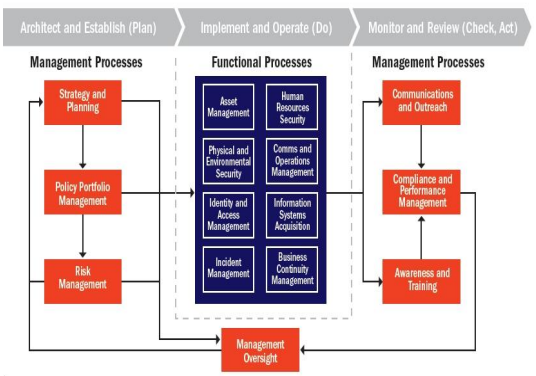

Fig. 1. Security governance system [4]

- 효율적 조직 구성의 어려움

의사결정 구조에서 정보 보안 조직을 어떻게 구성할지에 대한 해답을 찾기 어렵다. 최고보안 책임자인 CSO를 어느 위치에 두는 것이 더 효율적인지 정보 보안 조직을 중앙 집중적으로 체계화하는 것이 나을지 각 IT 부서에 보안 담당자를 두고 총괄적 관리 체제가 더 나을지 등 성과 측정의 어려움이 있다. 보안에는 상당한 투자 금액이 들어간다. 보안 사고가 일어나지 않는 것만으로는 투자의 성과를 측정하기에 어려움이 있다. 보안에 무관심한 경영진과 조직 구성원이 여전히 존재하며 이러한 무관심은 효율적인 보안 거버넌스 체계를 이끌어 내기가 어려워진다.

3. 보안 거버넌스 제도 운영 경험

3.1 보안 거버넌스 국내 도입

기업 거버넌스는 기업의 전략과 목적을 달성하기 위한 리더십, 조직 구조, 프로세스로 구성되어 기업 최고 의사결정 기구인 이사회가 책임지고 이끄는 구조이다. 기업 거버넌스는 여러 거버넌스로 나뉘는데 IT 거버넌스도 그 중 하나이다. 또한 IT 거버넌스의 한 부분이던 정보보호가 시간이 지나면서 정보보호 거버넌스로 발전되어 지금은 IT 거버넌스와 상관관계를 갖게 되었다. 정보보호 거버넌스는 IT 거버넌스와 함께 연구, 발전되고 있다. 우리나라는 거버넌스 용어를 사용하지 않았지만 2009년 국가사이버위기 종합대책에서 종합적인 체계의 보안 대책을 도입하였고 2010년 말 개최된 ISEC(통합 정보 보호 구축전략 컨퍼런스)에서 정보보호 거버넌스를 공개적으로 다루었다. 개인정보보호, 스마트와 모바일 보안관리체계 수립, 위험관리 기반의 정보 보안 등이 거버넌스로 통합되고 전략적으로 수립되어 일괄적으로 관리, 운영 되어야 한다고 정의되었다. 이후 국가보안 거버넌스 적용은 다음과 같은 종합계획에 반영되어 추진되어왔다고 볼 수 있다 [5,6].

○ 2009년 국가 사이버위기 종합대책 수립
○ 2010년 ISEC(통합정보보호 구축전략 컨퍼런스) 개최
○ 2011년 국가 사이버안보 마스터플랜 마련
○ 2013년 국가 사이버안보 종합대책 수립
○ 2015년 국가 사이버안보 강화방안
○ 2016년 IoT, 클라우드, 빅데이터 환경의 국가 사이버안보 대책 수립

3.2 보안 거버넌스 운영 경험

거버넌스는 외형적인 실체가 나타나지 않는 성격이고 형체가 없다. 따라서 우리의 거버넌스 체제에 대한 경험을 운용상 문제점 도출 작업을 소재로 정리하였다. 우리의 경험은 보안 관리의 실태를 참조하고 한국의 보안실태를 진단한 각종 연구 보고서와 시사 자료, 보도 자료를 참조하여 조사하였다.

○ 필요성 인식 부족

2010년도 초반에 소개된 보안 거버넌스 방법론은 조직, 개인 모두 기본 지식과 필요성 인식이 절대 부족했다. 사이버 보안 위협과 일탈 행위를 전통적인 법률과 제도로 관리하였으며 규제 위주였다. 그 결과 법규로 해결 곤란한 사이버 문제가 다양하게 발생하였다. 거버넌스 개념은 생소하고 본격적인 모델 연구와 도입이 미진했다. 빠르게 변화하는 IT 패러다임 환경에서 시대 조류를 반영하는 거버넌스 체계 도입이 신속히 이루어 지지 못하고 법규, 조직, 운영, 경영 관점의 거버넌스 설계, 성과제도 미 도입 등 과거의 비효율 요소는 그대로 지속되었다.

○ 국가 법규 체계의 구조적 문제점 노출

- 법규 체계는 부문별, 목적별로 개별법이 존재하고 있기 때문에 사전에 예상할 수 있을 정도의 사이버 공격에는 대응할 수 있다. 그러나 여러 부문 및 영역에 걸쳐 동시다발적으로 발생하고 있는 사이버 공격의 양상에 비추어 볼 때, 현행 법제는 그 대응성이 떨어진다.

- 사이버 침해 사고가 발생하면 그 영역이 공공이나 민간으로 구분되지 않으며 경계선이 없는 속성을 지닌다. 미디어, 금융기관, 교통 수송, 식품 의약품 등 민간 분야의 사이버 침해 사고는 결국 국가의 안전보장과도 직결되는 상황이다. 대응의 신속성이 미흡하고 국가 컨트롤 타워가 없는 현 체계는 사이버 공격에 따른 피해를 더욱 확산시킬 수밖에 없다.

- 분권형(De-Centralized) 거버넌스 구조는 구조 자체가 가지는 업무 유연성을 장점으로 제시하지만 위기상황에서 업무 한계가 모호하여 적시 위기관리가 어렵다는 의견이 대두되고 있다. 또한 사이버 위협이 복잡한 구조를 가지고 있어 이에 대응하는 강력한 국가 적 최고기관의 역할이 무엇보다 효율성을 보장할 수 있어야 하는 경우가 수시로 등장한다. 따라서 우리의 전통적인 법제인 '정보통신기반보호법', '정보통신망 이용촉진 및 정보보호 등에 관한 법률' 등에서 위임하고 있는 다양한 분권형 기조는 효율성 측면에서 재진단이 필요하다고 본다[1].

4. 보안 거버넌스 모델 설계 방법

4.1 거버넌스 모델의 사상

먼저 설계 측면에서 거버넌스 라이프사이클 프로세스, 거버넌스 프레임워크가 설계되어야 한다. 운용 측면에서

거버넌스 운용 효율성 방안, 최종 목표 달성을 위한 연구 단계 정립, 라이프사이클 흐름의 운용상 문제점 진단 도출, 환경 변화에 기초한 보안 정책 도입, 민간 부문 보안 강화와 모든 주체의 참여 노력이 반영되는 새로운 틀의 거버넌스가 되어야 한다. 국가 사이버보안 거버넌스 라이프사이클을 설계, 체계, 전략, 범위, 운용, 법규, 경영, 의식, 피드백의 9개 단계로 구분하여 문제점을 진단한다. 진단 결과를 토대로 개선해야할 분야를 도출하고 새로운 설계를 진행한다[7,8].

COBIT(Control Objectives for Information and Related Technology:정보 및 관련 기술 제어 목표)은 정보기술(IT) 관리 및 IT 거버넌스를 위해 ISACA (Information Systems Audit and Control Association)가 만든 우수 사례 프레임워크이다. COBIT은 구현 가능한 '정보 기술 통제'를 제공하고 IT 관련 프로세스와 원동력의 논리적 프레임워크를 중심으로 구성한다. ISACA는 원래 회계 감사 공동체가 IT 관련 환경에서보다 효과적으로 기동할 수 있도록 도와주는 일련의 제어 목표로서 COBIT를 1996년에 발표했다. COBIT은 관리자가 통제 요구 사항, 기술적 문제 및 비즈니스 위험 사이의 격차를 해소할 수 있게 해주는 IT 거버넌스 프레임워크이자 지원 도구 세트이다. COBIT은 조직 전체에서 IT 통제를 위한 명확한 정책 개발 및 우수 사례를 제공한다. COBIT은 규제 컴플라이언스를 강조하고 조직이 IT에서 얻는 가치를 높이고 기업의 IT 거버넌스 및 제어 프레임 워크의 조정을 단순화하고 구현을 도와준다[4,9,10].

Fig. 2. COBIT 5 Principles [9]

4.2 모델 연구 프로세스

'보안 전략'을 보안 거버넌스 체계로 먼저 설계해야 하며 사전 예방 차원의 라이프사이클에 기반하여야 한다. 전문가 모델은 이를 Architect and Establish (Plan) Implement and Operate (Do) Monitor and Review (Check, Act)로 구성하고 있으며 ISO27001은 Plan - Do - Check 순환 과정에 기반을 두고 있다. 라이프 사이클은 이같은 전문 모델에 기초하여 보안 거버넌스 전략 체계 구축, 취약점 분석 평가 등 사전 예방 활동으로부터 알고리즘과 기술 개발, 평가와 피드백 프로세스로 이루어져야 한다[11,12].

4.2.1 거버넌스 설계 요구사항 정의

○ 환경 변화에 기초한 보안 정책의 도입

20세기가 유선통신 시대였다면 21세기를 지배하는 키워드는 모바일, 스마트, 클라우드 컴퓨팅, 빅데이터, 사물인터넷 등으로 표현된다. 지금은 4차 산업혁명시대의 IT 패러다임 시대에 진입하고 있다. 새로운 IT 환경에서는 다양한 단말 노드가 클라우드 인프라에 연결되면서 네트워크 접속점의 다양화가 이루어지고 네트워크 자체가 무선 환경이 되면서 사이버 공격이 더욱 다양화될 수 있다[11].

○ 법규 체계 개선 필요성

주요 기반 시설의 사이버보안을 실제에 맞게 합리적으로 규율하기 위하여 보호 대상을 주요 기반 시설 개념을 중심으로 정하고 또 그 사이버보안 범위를 지정된 시설에 국한하지 않고 해당 주요 기반 시설의 정보시스템 전체로 넓게 인정하는 것이 필요하다. 개별 법령에 산재해 있는 사이버보안 조직 체계를 단순화하고, 특히 사이버보안 컨트롤 타워와 관련 유관 기관간의 유기적 협조 체제 구축 등을 고려해야 한다.

○ 보안 활동 연계성 요구

사이버공간의 연결성은 단순한 개인적·집단적 차원의 정보보안의 문제를 넘어 국가·지역 공동체의 보안 문제에 관심을 가질 필요성을 제기한다. 오늘날 사이버공간의 법 규범은 사물인터넷 또는 만물인터넷과 같은 개념이 도입되면서, 연결성이 극대화된 사회가 되고 있어 보안 문제는 매우 중요한 의미를 가진다. 이는 법적 규율간 경계 파괴와 오프라인의 정보 보호와 사이버공간에서의 정보보호가 괴리될 수 없음을 의미한다[13].

○ 민간 부문의 보안 강화와 모든 주체의 참여

이 부분에 대해서는 미국의 CSIS 보고서와 오바마 정

부의 사이버보안 강화위원회 보고서, 유럽과 일본을 포함한 주요 국가들의 사이버 보안정책 사례를 통해 벤치마크해볼 수 있다. 이들 사례에서 관찰되는 것은 새로운 국가 사이버보안 정책의 공통된 핵심이 국가 사이버보안 강화를 위해 민간 부문의 보안 강화와 모든 주체의 참여 노력이라는 것이다. 우리는 이 부분에 대한 많은 관심과 방법론 도출이 필요하다[13,14].

4.2.2 거버넌스 프레임워크 구성

보안 활동을 위해서는 업무의 전체적인 프레임워크가 구성되어져야 하고 그 속에서 법규, 정책, 기술 분야가 포함되어 보안 체계를 구성한다. 전체적인 프레임워크는 프로세스 측면에서 종적으로, 업무 영역에서 횡적으로 이루어지는 큰 그림이다. 따라서 이 사상에 기초하여 고유한 응용 모델의 발굴이 필요하다. 이때 참조할 수 있는 국제적인 거버넌스를 지원하는 프레임워크 모델은 COBIT, ITIL, ISO38500, BS25999, 의사 결정 모델 등이 있으며, 이 모델들은 IT투자의 목적에 따라 선택적으로 활용할 수 있다. 거버넌스 프레임워크 구성작업은 최상위의 정책을 실현할 수 있는 일종의 설계도 작성 작업으로서 요소의 구성, 요소간 연동, 연동 구조 속에서 기능의 흐름, 입출력, 전체적인 종합 제어의 사상이 시스템적으로 작동되도록 설계되어져야 한다. 이때 운용 사이클은 거버넌스 설계(Design), 구축(Construct), 이행(Implement), 평가 (Assess), 운영/개선(Operate/Review) 5개 단계로 정립된다[14-16].

4.2.3 국가 사이버보안 거버넌스 모델 연구 방법

○ 4차 산업혁명에 걸맞는 국가 사이버보안 거버넌스 모델 발굴

세계 각국은 이미 4차 산업혁명의 거대한 변화와 흐름 속에서 보안의 중요성을 인식하고 이에 대응하기 위한 사이버 보안 관련 정책들을 발표하고 있다. 우리도 이에 걸맞는 한국형 4차 산업혁명의 국가 사이버 보안 거버넌스 모델을 발굴해야 한다. 이 모델은 과학기술 관련분야 뿐 아니라 인문, 사회, 예체능 분야 등 그동안 보안과는 거리가 멀다고 생각되었던 다양한 분야들과도 융합이 필요하다. 국가 사이버보안 역량을 강화하기 위해서는 다양한 학문 및 산업과의 연계를 활성화시키는 방안이 필요하며 보안 기술이 이러한 다양한 분야에서 활용될 수 있는 기반기술로 자리 잡아야 한다.

○ 경영적 관점의 거버넌스 모델 도입 연구

정보보안 관리의 목적은 변화하는 정보보안 위험을 관리하는 동시에 정부기관이 사전에 비용 효율적인 방식으로 적절한 보안 통제를 구현할 수 있도록 하는 것이다. 연구하는 모델의 구상은 보안 위험 관리 과정을 구현하는 프로세스가 반영되도록 한다. 즉, 자산의 평가, 취약점 진단, 위협 진단, 대책의 진단, 위험도 산정, 보완 부분 도출과 제안으로 구성되어야 한다. 경영적 관점의 거버넌스 모델 도입 연구는 이상의 보안위험관리 사이클을 기초로 그 성과 측정이 가능한 모델이 발굴되어야 한다.

○ 국가 거버넌스 성과 측정 모델 발굴

보안 거버넌스의 효과적인 달성을 도모하기 위한 보안 공학적 원칙들이 얼마나 잘 반영되었는지를 평가하기 위한 방법론으로 진단 항목 발굴, 서브 항목 발굴, 진단 매트릭스 발굴, 평가 가중치 적용방법 발굴 4개 분야로 구성된다.

보안성과 측정 모델은 각 개별 기관마다 이들 항목별 중요도가 다르고, 효과성(Effectiveness), 효율성(Efficiency), 준수사항(Compliance)의 준수 여부, 성과 측정 항목은 다음과 같은 기준으로 발굴되어야 한다.

1)국가 보안 수준을 종합적으로 파악
2)국가 안보를 위협하는 공격을 알아내는 방법
3)어디에 어떤 문제가 있는지 알아내는 방법
4)보안 개선 방안과 소요 예산을 알아내는 방법
5)보안 개선을 잘하는 조직을 한번에 아는 방법,
6)보안의 최하위 실무 분야 현황을 파악
7)어떤 문제의 개선이 이루어 졌는지 아는 방법

○ 전체적인 관리 프로세스 정립

각 부처와 조직간 프로세스 개선이 요구되는 분야의 식별과 신규 애플리케이션 도입 타당성 을 검토하되, 범정부 토대 아래 기존의 시스템 을 최대한 활용할 수 있는 방안을 모색하고, 중복 개발을 방지하여야 한다. 거버넌스 고유의 프로세스 효율성을 도입하되 사이버보안 거버넌스의 개념은 전체 그림을 하나의 거버넌스 프로세스로 봐도 되며 피드백이 필요하다. 또한, 위험 관리의 하나로 인식해도 되며, 보안성 구현은 조직의 비즈니스 목적에 알맞는 보안 통제의 구현이 조직의 목적에 부합되는지 지속적인 모니터링이 중요하다. 본 연구에서 제안하는 한국형 보안 거버넌스 모델의 종합 프레임워크는 비전,

목표, 과정, 수행 등 4개의 아키텍처로 구성된다. 비전은 통합 체계 프레임워크 개발이며 비전 목표와 함께 비전 창출 과정이 필요하다. 종합 프레임워크는 다음 Table 2 와 같다.

Table 2. Security governance model research framework

Research Vision					
Developed a new Korean security governance model					
Achievement goal					
Goal Setting	Model excavation	Deriving security system	Activation plan	Feedback scheme	
Research course					
Diagnosis	Advanced case BMT	Direction of improvement	Organizatio n of action	Derive procedural measures	
Research Field					
Regulatory system	Organizati on system	process design	Framewor k design	Roadmap design	Organizatio n of action

5. 결론

20세기가 유선통신의 시대였다면 21세기를 지배하는 키워드는 모바일, 스마트, 클라우드 컴퓨팅, 빅데이터, 사물인터넷 등으로 표현된다. 4차 산업혁명 시대에서의 IT 패러다임을 기반으로 하여 사이버보안 강화는 산업 활성화 측면의 효과로 신성장동력 창출, 글로벌 경쟁력 확보, 보안 산업 활성화를 통해 차세대 산업 발전 동력을 확보하고 글로벌 경쟁력을 높일 수 있다. 국가 전략적 차원에서 보안 거버넌스를 효율화시키면 경쟁력 있는 미래 신성장 동력의 창출을 기대할 수 있다. 사이버 보안 강화는 사회안전망 고도화 효과로 긴급 상황에서 생명을 보호하기 위한 긴급구조 서비스에 이용되는 등 사회안전망으로서의 활용도 증가에 기여한다. 제안하는 한국형 보안 거버넌스 모델의 종합 프레임워크는 비전, 목표, 과정, 수행 등 4개의 아키텍처로 구성된다. 비전은 통합 체계 프레임워크 개발이며 비전 목표와 함께 비전 창출 과정이 필요하다. 앞으로 라이프 사이클 흐름상의 문제점 진단, 환경변화에 기초한 보안 정책, 모든 주체의 참여가 반영되는 새로운 틀에 대하여는 계속적인 연구가 필요하다.

REFERENCES

[1] YSC Research and Business Foundation. (2015). *A Comparative Law Study on the Cybersecurity Response System.* Naju:KISA.

[2] E. H. Kim & J. I. Lee. (2011. 8). Net Focus - US Obama Government's Cyber Security Key Policies and Measure. *Internet & Security Issue*, Naju:KISA, 5-30.

[3] S. C. Kim. (2014). Cyber Security Law of Germany. *The Journal of Cyber Security Law, 1*, 1-22.

[4] J. Miller, L. Candler & H. Wald. (2009. 11). *Information Security Government., Technology, 5.*

[5] K. T. Hwang. (2005). Basic concept of IT governance. *Local Informatization*, *32*, 106-109.

[6] D. H. Kim. (2017). The Study on Corporate Information Security Governance Model for CEO. *Jouranl of Information and Security, 17(1)*, 39-44.

[7] S. K. Kang, H. S. Yoon, Y. W. Park, M. H. Kim, H. Y. Kwan, D. S. Kim & K. B .Kim. (2010). *A Study on the Construction*, Korean Institute of Criminology.

[8] Korea Communications & Commission. (2011. 8. 8). Government, Establishment of "National Cyber Security Master Plan" - Establishment of blueprints for the protection of national cyber space. Seoul:KCC.

[9] ISACA. (2012). *COBIT 5*, 14.

[10] Information Week. (2014. 6. 13). FCC Wants More Cybersecurity Collaboration. *Less Regulation.*

[11] Media & Future Institute. (2012). *International cyber space forum strategy study*, Seoul:KCC.

[12] TechCrunch. (2014. 6. 12). *FCC Chairman Tom Wheeler Outlines New Cybersecurity Paradigm Led By Private Sector.*

[13] National Intelligence Service, Ministry of Science, ICT and Future Planning, Korea Communications Commission &, Ministry of Government Administration and Home Affairs. (2015). *2015 National Informatization White Paper.*

[14] National Information Society Agency. (2014. 7). *ICT Issues Weekly, 463,* 1-5.

[15] Wall Street Cheat Sheet. (2014. 6. 12). *What the FCC's 'New Regulatory Paradigm' Means for Network Providers.*

[16] Office for Government Policy Coordination. (2015. 3. 17). *Strengthen National Cyber Security Stance Capacity.*

방 기 천(Bang, Kee Chun) [종신회원]

- 1981년 2월 : 서울대학교 전자공학과(학사)
- 1988년 8월 : 성균관대학교 정보처리학(석사)
- 1996년 2월 : 성균관대학교 전산통계학(박사)
- 1984년 1월 ~ 1995년 2월 : MBC 기술연구소
- 2000년 3월 ~ 2013년 12월 : (사)한국디지털콘텐츠학회 회장
- 1995년 3월 ~ 현재 : 남서울대학교 멀티미디어학과 교수
- 관심분야 : 디지털콘텐츠, 웹기반 정보시스템, 멀티미디어 응용
- E-Mail : bangkc21@gmail.com