Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.5, Oct. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.5.1153

국방정보시스템 사이버복원력 수준 평가를 위한 성숙도모델에 관한 연구

최 재 혁,† 김 완 주, 임 재 성‡
아주대학교 NCW학과

A Study on Maturity Model for the Assessment of Cyber Resilience Level in the Defence Information System

Jae-hyeok Choi,† Wan-ju Kim, Jae-sung Lim‡
Ajou University Dept. of NCW

요 약

최근 국방 분야를 포함한 국가정보통신망 및 주요 기반시설 등에 대한 해킹 위협이 증가하고 있다. 국방정보시스템은 망분리를 통해 외부로부터의 위협에 대응하고 있으나, 해킹 성공시 전·평시 군사작전에 큰 영향을 미치게 된다. 오늘날 사이버 공격과 위협은 예측 불가능한 수준으로 높아지고 있어 해킹 위협을 완전히 차단하고 예방하는 것은 현실적으로 불가능하다. 따라서 본 연구에서는 국방정보시스템의 사이버 공격 징후가 예상되거나 발생했을 경우 신속한 대응 및 시스템의 생존성을 보장하고 지속성을 유지할 수 있는 능력인 '사이버복원력(Cyber Resilience)'의 수준을 평가할 수 있는 성숙도모델을 제시하였다. 제시된 성숙도모델을 통해 국방정보시스템의 사이버복원력 수준을 평가하고 부족한 분야를 식별 및 보완함으로써 국방정보시스템의 사이버보안 수준을 향상시키는데 기여할 수 있을 것으로 기대된다.

ABSTRACT

Recently, threats of hacking have been increasing on the national intelligence service network and key infrastructure, including the defense field. The defense information system responds to threats from the outside through the network separation, but if the defense information system is hacked, it has a serious impact on the operations of wartime or peacetime military forces. Today, cyberattacks and threats are rising to unpredictable levels and making it practically impossible to completely block and prevent hacking threats completly. So, in this study proposed a maturity model to assess the level of cyber-resilience, which is the ability to ensure the system's viability and maintain continuity through rapid response and recovery if signs of cyberattacks by the defense information system are expected or occurred. The proposed maturity model is expected to contribute to improving the cyber security level of the defense information system by assessing the level of cyber resilience of the defense information system and identifying and supplementing fields that are lacking.

Keywords: Cyber Resilience, Maturity model, Cyber Security, Defense Information System, Cyber Warfare

I. 서 론

오늘날 국가정보통신망 및 주요 기반시설 등에 대한 사이버 공격은 지속적으로 증가하고 있으며, 이는 국민의 안전과 국가안보에 대한 심각한 위협으로

Received(07. 03. 2019), Modified(08. 31. 2019), Accepted(09. 16. 2019)

† 주저자, urmine0222@ajou.ac.kr
‡ 교신저자, jaslim@ajou.ac.kr(Corresponding author)

다가오고 있다[1]. 심지어 2016년에는 국방부의 내부 전산망이 해킹되어 한·미 연합작전 계획이 유출되는 초유의 사건까지 발생하였다.

국방 분야에 대한 해킹으로 인해 군에서 운영중인 각종 국방정보시스템이 정상적으로 운영이 안 될 경우 전·평시 지휘통제의 혼란이나 군수지원 제한 등 심각한 위협을 초래할 수 있다.

최근 사이버 공격으로 인한 위협은 예측할 수 없을 정도로 수준이 높아지고 있고 이에 대응하기 위한 보안대책 역시 지속적으로 발전되고 있으나, 현실적으로 보안대책이 위협수준을 따라가지 못하고 있다. 결국 사이버공격을 완전하게 차단한다는 것은 사실상 불가능하며, 대부분 신고나 사고 발생 후 대응하는 수준에 불과하다. 그래서 최근 사이버보안과 관련된 연구에서 주목하는 개념이 '사이버복원력(혹은 회복력, Cyber Resilience)'이다.

사이버 보안과 관련된 연구 뿐만 아니라 최근 미국과 영국, 유럽의 여러 국가들 역시 사이버복원력 제고에 큰 관심을 가지고 사이버보안 정책에 반영하고 있다.

미국은 2018년 9월 20일, 15년만에 연방 차원의 'National Cyber Strategy'을 공개하였는데, 국가 사이버 전략 구축의 바탕이 되는 핵심 원칙에서 "국가 정보 및 정보시스템의 보안 및 복원력 강화를 위해 사이버보안 위험을 관리할 것"이라는 목적을 제시하였다[2]. 영국은 2013년 12월 네트워크의 복원력 강화를 강조한 'The National Cyber Security: Our Forward Plans'를 발표하였으며, 2016년 11월에는 'National Cyber Security Strategy 2016 to 2021[3]' 이라는 전략서를 발표하여 핵심 기반시설의 안전을 확보하고 사이버 공격, 특히 사이버 범죄에 대응하는 역량과 네트워크의 복원력을 강조하는 기조를 유지하고 있다[4]. EU는 2013년 'Cybersecurity Strategy of the European Union'에서 '사이버 복원력의 확보'를 5대 전략과제 중 첫 번째 과제로 제시하였다[5].

최근 우리 정부도 대한민국 최초로 발표한 '국가사이버안보 전략'에서 "어떠한 사이버 위협에도 지속적 운영이 가능하도록 국가 핵심 인프라의 생존성과 복원력 강화"를 사이버 안보의 목표로 제시하고 개인•기업•정부가 중점 추진해야하는 전략적 과제로 제시하였다[6].

따라서 본 논문에서는 국방 분야의 사이버 위협이 증가하고 있는 상황하에서 국가안보와 밀접한 연관이 있는 국방정보시스템의 사이버복원력 수준을 평가할 수 있는 성숙도 모델을 제시함으로써, 사이버복원력 강화를 통한 국방 분야의 사이버 보안 수준 향상 및 국가안보에 큰 도움이 될 것으로 기대된다.

본 논문의 구성은 다음과 같다. II장에서는 국방정보시스템의 개념과 특징, 사이버복원력의 정의와 구성요소, 성숙도 모델에 관한 기존 연구를 제시하고, III장에서는 국방정보시스템 성숙도모델 평가영역 및 평가지표를 도출한다. IV장에서는 III장에서 도출한 평가지표에 대해 사이버복원력 수준 평가를 위한 세부 측정항목 제시 및 성숙도 단계를 정의하고, V장에서는 본 연구의 기대효과와 향후 연구를 언급하며 결론을 맺는다.

II. 관련연구

국방정보시스템의 사이버복원력 수준 평가를 위한 성숙도모델을 제시하기 위해 국방정보시스템의 개념과 특징, 사이버복원력의 정의와 구성요소, 성숙도 모델에 관한 기존 연구를 제시한다.

2.1 국방정보시스템의 개념과 특징

국방정보시스템은 국방정보의 수집·가공·저장·검색·송신·수신 및 그 활용과 관련되는 기기 등 응용소프트웨어와 기반운영환경의 조직화된 체계로 정의된다[7]. 국방정보시스템은 국방정보통신망, 컴퓨터 체계, 사이버방호 체계, 상호운용성 체계 등과 같이 네트워크를 구성해 장치들을 연결해주는 체계인 기반체계와 전장관리, 자원관리, 국방 M&S와 같이 기반체계를 바탕으로 국방정보를 수집, 가공, 저장, 검색, 송신, 수신하고 그 정보를 활용하는 응용체계로 구분된다[8].

국방정보시스템의 특징은 다음과 같다[9].

첫째, 규모가 크다. 국방정보시스템은 많은 서브시스템들이 지형적으로 넓은 지역에서 운용되고 많은 외부 구성품들과 접속하게 되는데 그러한 시스템을 지원하는 컴퓨터 시스템은 기능과 성능을 고려하여 흔히 대형 분산처리시스템으로 구성된다.

둘째, 대부분 실시간으로 작동한다.

셋째, 고도의 정확성이 요구된다.

넷째, 신뢰성과 가용성이 요구된다. 시스템의 하드웨어나 소프트웨어 구성품이 고장났다 할지라도 그 기능은 계속 수행되어야 한다는 것을 의미한다.

다섯째, 안전한 작동이 요구된다. 비밀성, 무결성,

가용성을 보장하기 위해서 보안 요구조건을 만족시켜야 한다.

여섯째, 과중한 정보를 취급한다. 국방정보시스템은 운용자가 필요에 따라서 적시에 병합되고 반복된다.

2.2 사이버복원력

2.2.1 사이버복원력의 정의

복원력이란 개념은 생태학적 관점, 재난연구 등 생물학·사회학적 관점에 맞춰 연구가 진행되어왔으며, '사이버복원력'이란 개념은 사이버공간 등장 이후 사이버공간에 위협을 주는 여러 요소들에 대응하기 위해 생겨났다. 즉, 재난연구에서 사용되던 복원력 개념을 사이버공간과 결합한 개념으로, 최근 급격히 증가하고 있는 사이버 침해 사고나 기술환경 변화 등에 따라 대두되기 시작했다[10]. 아직 사이버복원력의 개념에 대해 명확하게 정의된 것은 없으며, 아래 Table 1.과 같이 다양하게 정의되고 있다.

본 연구에서는 사이버복원력에 대한 다양한 정의들 중 2016년 국제결재은행(BIS)에서 발표한 '금융시장 인프라에 대한 사이버복원력 지침'의 '사이버 공격을 예상, 대응, 경감하고 신속하게 복구할 수 있는 능력'으로 정의하고 연구를 진행하였다.

Table 1. Defination of cyber resilience

Author	Defination
NIAC (2010) [11]	The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event.
Bodeau and Graubart (2011) [12]	The ability of a nation, organization, or mission or business process to anticipate, withstand, recover from, and evolve to improve capabilities in the face of, adverse conditions, stresses, or attacks on the supporting cyber resources it needs to function
EY (2014) [13]	The ability to powerfully resist, react to and recover from potentially catastrophiccybersecurity threats, and reshape their environments for increasingly secure.
BIS (2016) [14]	FMI's ability to anticipate, withstand, contain and rapidly recover from a cyber attack

2.2.2 사이버복원력의 구성요소

류현숙(2015)은 사이버복원력의 구성요소로 '시스템 견고성, 신속성, 자원동원성, 적응성' 총 네 가지 사이버복원력 요소를 제시하였다.

'시스템 견고성(Robustness)'은 침해 상황에서도 작동하는 견고한 시스템을 의미하며, '신속성(Rapidity)'은 가능한 빨리 정상 또는 원래 상태로 돌아가는 능력을 의미한다. '자원동원성(Resourcefulness)'은 취약성 관리와 이를 담당하는 사람과 지원에 대한 요소를 의미하며, '적응성(Adoptability)'은 사이버침해 결과를 받아들이고 시스템 견고성, 자원동원성, 신속성을 개선 내지 제고하는 능력을 의미한다.

서지영 외(2014)는 시스템 회복력의 구성요소로 '대체성/예비능력, 견고성, 융통성, 신속성, 모듈성/독립성' 총 다섯가지 요소를 제시하였다[15].

'대체성/예비능력(Redundancy)'은 기능 수행을 위한 다양한 방법 즉 분산된 인프라 네트워크, 분산된 자원 네트워크 등을 의미한다. '견고성(Robustness)'은 시스템의 내재적 강도로서 시스템 기능의 약화 혹은 상실없이 외부 충격을 견디는 힘으로서 충격에 대한 완충기능 수행으로 시스템 정체성을 유지하는 것을 의미한다. '융통성(Resourcefulness)'은 자원 동원능력 및 자원의 효율적 관리를 의미하며, '신속성(Rapidity)'은 피해를 줄이기 위해 빠른 시간안에 기능을 회복할 수 있는 능력을 말한다. 마지막으로 '모듈성/독립성(Modularity)'은 시스템이 모듈들 간의 상호작용으로 형성된 집합체로 보고, 모듈성은 하위 시스템들의 자기발전능력이라고 정의하였다.

금융시장인프라(Financal Market Infrastructures)에 대한 사이버복원력 지침[1]에서는 사이버복원력 체계에서 고려해야 하는 5개 리스크 관리항목(Risk management categories)과 3개 지원항목(Overarching components)으로 구분하여 구성요소를 제시하고 있다[16].

5개 리스크 관리항목 - '지배구조(Governance)'

1) 2016년 6월 지급결제 및 시장인프라 위원회 국제증권감독기구가 발표한 'Guidance on cyber resilience for FMIs - CPMI and IOSCO reviews'를 한국은행이 번역한 지침

는 사이버리스크를 관리할 목적으로 조직에서 수립, 구현, 검토되는 제도이며, '식별(Identification)'은 기관이 사이버리스크를 관리하기 위해 자신의 시스템, 자산, 자료 및 능력에 대한 이해를 발전시키는 행동이다. '보호(Protection)'는 핵심적인 인프라 서비스의 제공을 보장하기 위해서 적절한 안전장치, 통제 및 방법론을 시행하는 것이며, '탐지(Detection)'는 사이버사건 발생을 인지하기 위하여 적절한 활동을 계획하고 수행하는 것이다. '복구(Recover) 및 대응(Respond)'은 사이버사건에 의해 저하되었던 각종 능력 및 서비스를 원복시키고, FMI가 사이버사건이 탐지하였을 때 취할 수 있는 적절한 행동을 개발하고 실행하는 것이다.

3개 지원항목 - '테스트(Test)'는 5개 리스크관리 항목에 대한 효과를 점검하기 위하여 발생가능한 시나리오를 바탕으로 취약점 평가, 침투 테스트, 레드팀 테스트 등을 수행하는 것을 말한다. '상황인지(Situation awareness)'는 여러 사이버유형별 공격에 맞는 전략적인 대응방안을 마련하는 한편 안전한 통신망을 통해 이해당사자와 대응방안 관련 정보를 공유하는 것을 의미하며, '학습과 발전(Learning and evolving)'은 신규 기술을 도입하여 사전예방 능력을 제고하고 측정기준, 모범사례 등을 활용하여 관리체계의 지속적 발전을 도모하는 것을 의미한다.

본 연구에서는 사이버복원력 평가영역 도출을 위해 현재 국내 및 군에서 적용되는 가장 권위있고 적용영역이 넓은 상기 3가지 연구를 기준으로 하였으며, NIST 800-160 등 국제적으로 연구되어지고 있는 표준들은 본 연구 범위에 포함하지 않았다.

2.3 성숙도모델

영국 옥스퍼드 대학 글로벌 사이버보안 역량센터가 개발한 'Cyber Security Capability Maturity Model'은 사이버 정책 및 전략 수립, 사회에서 사이버 문화에 대한 책임감 고취, 직장과 관리조직의 사이버 기술 배양, 효과적인 법 규제 프레임워크 구축, 조직, 표준 그리고 기술을 통한 위험통제 등의 영역으로 나누어 사이버보안의 역량을 파악하였으며, 그 성숙도의 기준을 초기(start-up), 형성기(formative), 확립기(established), 전략적 단계(strategic), 그리고 역동적 단계(dynamic)로 제시하고 있다[17].

프로세스의 성숙도를 측정하는 모델로는 'Capability Maturity Model Integration (CMMI)'을 들 수 있다. CMMI는 소프트웨어 개발 및 전산장비 운영 분야의 품질 관련 국제공인 기준으로 프로세스 개선 활동을 수행하는 방법에 있어 초기(initial), 관리(managed), 정의(defined), 정량적 관리(quantitatively managed), 최적화(optimized)의 5단계로 구성된 수준 개념을 제시하고 있다[18]. CMMI에서 제시한 성숙도 기반의 프로세스 개선 개념은 프로세스 발전 단계의 본질적인 측면을 잘 파악하여 반영하고 있기 때문에, 조직의 관리체계나 프로세스의 수준을 평가하고 이를 통해 개선 포인트를 파악하는데 유용하다[19].

'Cybersecurity Capability Maturity Model(C2M2)'은 지속되고 있는 모든 형태의 조직에 대한 정보 위협을 감소시키기 위해 2014년 2월 미국 국토안보부(DHS)와 에너지부(DOE)에 의해 개발되었다. C2M2는 정보기술 및 운영기술에 필요한 자산과 운영환경과 관련한 정보보호 관리체계의 구현과 관리에 중점을 두고 있다.[20]. 역량 평가 수준은 총 4가지의 등급(MIL)을 제시하며, 10개의 평가 영역(domain)과 이에 포함된 37개 수행 활동(practices)으로 구성되어 있다. 본 모델은 각 평가영역(domain)에 독립적으로 적용되는 MIL0(Maturity indicator level 0)에서 MIL3까지의 성숙도 등급을 정의하고 있다[21].

III. 국방정보시스템 사이버복원력 성숙도모델 평가지표

본 연구의 목적은 국방정보시스템의 사이버 공격 징후가 예상되거나 발생했을 경우 신속한 대응 및 복구를 통해 시스템의 지속성을 유지할 수 있는 능력인 사이버복원력의 수준을 평가할 수 있는 성숙도모델을 제시하는 것이다. 이를 위해 III장에서는 우선 사이버복원력의 구성요소로부터 6개의 성숙도모델 평가영역을 도출하였으며, 국방 분야 및 민간 분야의 정보시스템 요구사항을 바탕으로 각 평가영역에 부합하는 26개의 평가지표를 도출하였다.

3.1 성숙도모델 평가영역

본 연구에서는 사이버복원력 구성요소에 대한 이론적 고찰을 통해 6개 평가영역 - 복원력 강화 정책

(Policy), 대체성/예비능력(Redundancy), 견고성(Robustness), 신속성(Rapidity), 융통성(자원동원성, Resourcefulness), 독립성(Independence) - 을 도출하였다.

류현숙(2015)의 구성요소 중 시스템 견고성, 자원동원성, 신속성을 개선 내지 제고하는 능력을 의미하는 '적응성(Adoptability)'과 FMI 사이버복원력 지침(2016)에서의 사이버리스크를 관리할 목적으로 조직에서 수립, 구현, 검토되는 제도를 의미하는 '지배구조'를 포함하는 '복원력 강화정책(Policy)'이라는 평가영역을 새로이 도출하였다. FMI 사이버복원력 지침(2016)의 다른 구성요소들은 사이버복원력에만 한정되는 구성요소로 보기 어렵고, 도출한 다른 구성요소들에 포함시킬 수 있다고 판단하여 평가영역에서 제외하였다.

'복원력 강화 정책(Policy)'은 사이버복원력의 중요성을 인지하고 사이버복원력을 강화하기 위한 계획을 수립 및 점검하여 평가하는 영역이며, '대체성/예비능력(Redundancy)'은 시스템의 지속성을 유지하기 위한 분산된 인프라 네트워크, 분산된 자원 네트워크 등의 대체/예비자원 보유와 관련된 영역이다. '견고성(Robustness)'은 외부의 위협으로부터 견딜 수 있는 시스템의 내재적 강도와 관련된 영역이며, '자원동원성(Resourcefulness)'은 자원 동원능력 및 자원의 효율적 관리와 관련된 영역이다. '신속성(Rapidity)'은 빠른 시간안에 시스템 기능의 복구 가능여부와 관련된 영역이며, '독립성(Independence)'은 다른 시스템 혹은 외부 위협으로부터 영향을 받지 않는 시스템 기능의 유지와 관련된 영역이다.

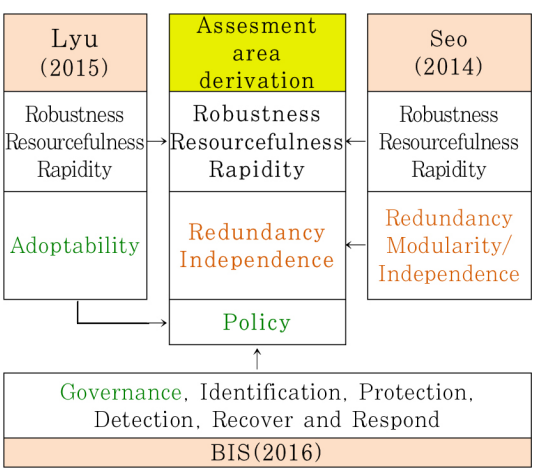

Fig. 1. Derivation process of assesment area

3.2 성숙도모델 평가지표

6개의 평가영역에 부합하는 평가지표를 개발하기 위해 국방 분야의 경우 국방부의 「국방사이버안보 훈령」[22] 제3장 사이버보안 '제1절 국방정보시스템 보호'의 요구사항을 기준으로 하였고, 민간 분야의 경우는 「정보보호 관리체계(ISMS)[2]」[23] 인증기준의 정보시스템 사이버보안 요구사항을 기준으로 사이버복원력 관련 요구사항을 살펴보았다.

「국방사이버안보 훈령」에서는 국방정보시스템의 기밀성, 무결성, 가용성 측면에서 자산의 중요도에 따라 국방정보시스템을 '가', '나', '다'급으로 분류하고 있으며, 대상 시스템의 구축·운영 환경에 요구되는 정보보호 분야 및 요구사항 수는 Table 2.와 같다.

「정보보호 관리체계(ISMS)」의 '관리체계 수립 및 운영' 영역은 관리체계 기반 마련 등 4개 분야 16개 인증기준으로 구성되어 있으며, '보호대책 요구사항' 영역은 정보시스템 도입 및 개발보안 등 12개 분야 64개 인증기준으로 구성되어 있다. ISMS의 16개 분야와 각 분야별 인증기준 수는 Table 3.과 같다.

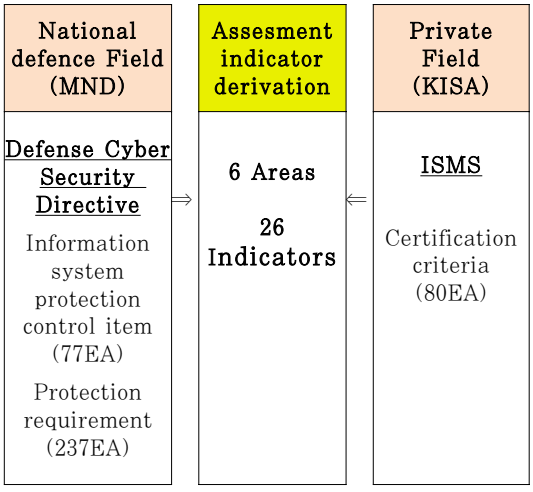

Fig. 2. Derivation process of assesment indicator

2) Information Security Management System: 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제47조(정보보호 관리체계의 인증)를 법적 근거로하여 기업·기관이 각종 위협으로부터 주요 정보자산을 보호하기 위해 수립·관리·운용하는 종합적인 정보체계

Table 2. Information protection sector of defense information system

Information protection sector	Number of Requirements
1. Network Security	19
2. Server Security	38
3. Device Security	11
4. Application system Security	82
5. Security Management	87

Table 3. Certification criteria of ISMS

Area	Number of Requirements
Establishing and operating a management system	16
Requirement for protective measure	64

상기 제시된 「국방사이버안보 훈령」의 보호통제 항목 및 「정보보호 관리체계(ISMS)」의 인증기준 항목 중 사이버복원 관련 요구사항을 식별하여 6개 평가영역에 부합하는 26개의 사이버복원력 수준 평가지표를 Table 4.와 같이 도출하였다.

'복원력 강화정책' 영역은 사이버복원 계획 수립 등 3개 지표, '대체성/예비능력' 영역은 예비사이트 등 3개 지표, '견고성' 영역은 네트워크 침입탐지/차단 및 통제 등 6개 지표, '융통성' 영역은 사이버 복원 인력의 전문성 등 5개 지표, '신속성' 영역은 복원 우선순위 선정 등 3개 지표, '독립성' 영역은 인터넷/외부 네트워크 연동 통제 등 6개 지표이며, 각 성숙도 평가지표는 85개의 세부적인 평가요소에 의해 평가되어진다.

Table 4. Assesment Indicators of Cyber resilience level

Assessment Area	Assessment Indicator	Number of Assessments
Policy	A1. Establishment cyber resilience plan	3
	A2. Awareness and attitude of cyber resilience	3
	A3. Cyber resilience Check and Evaluation	3
Redundancy	B1. Reserve site	3
	B2. System redundancy	2
	B3. Back up/Recovery	7
Robustness	C1. Network intrusion Detection/Blocking and Control	3
	C2. Server security program application	3
	C3. Device security program application	3
	C4. Cyber attack Detection/Blocking/Response system	2
	C5. Computer virus prevention system	3
	C6. Using public software	2
Resourcefulness	D1. Expertise of cyber recovery personnel	3
	D2. System resilience	3
	D3. Close cooperation system with related agencies	4
	D4. Security vulnerabilities remove and patch	4
	D5. Vulnerability analysis and evaluation	3
Rapidity	E1. Selection of restore priority	2
	E2. Setting of restore target time	1
	E3. Performing restore training	4
Independence	F1. Internet/External Network connection control	4
	F2. Defence information system connection control	4
	F3. Network access equipment authorization and control	1
	F4. Wireless LAN security	2
	F5. Remote access control	8
	F6. E-mail security	5

IV. 국방정보시스템 사이버복원력 수준평가를 위한 성숙도모델

이번 장에서는 III장에서 도출한 6개 평가영역 26개의 평가지표에 대해 사이버복원력 수준 평가를 위한 각 지표별 세부 측정항목 및 도출근거를 상세하게 설명하였으며, 성숙도모델에 적용할 사이버복원력 성숙도모델의 예시를 제시하였다.

4.1 평가지표 측정항목

평가지표의 측정항목은 국방정보시스템의 특성을 반영하기 위해 국방사이버안보훈령에서의 사이버복원력 관련 요구근거를 우선적으로 하여 ISMS 인증기준의 유사한 요구근거를 매핑하였다. 따라서 기존의 일반적인 정보시스템 사이버복원력 관련 측정항목과 더불어 군 보안관제체계, 내·외부망 분리 운영, 비밀정보 취급 시스템, 무선 및 원격접속 적극 통제 등 국방정보시스템만의 차별화된 특성을 반영한 측정항목을 도출하였다.

4.1.1 복원력 강화정책(Policy)

'복원력 강화정책'은 사이버복원력의 중요성을 인지하고 복원력을 강화하기 위한 계획 수립을 점검 및 평가하는 영역으로 A1. 사이버 복원계획 수립, A2. 사이버복원력에 대한 인식과 태도, A3. 사이버복원력 점검/평가 3개의 세부영역으로 구성되어 진다.

A1. 사이버 복원계획 수립은 사이버안보훈령 제26조 및 ISMS의 정책수립(1.1.5항)과 재해 재난 대비 안전조치(2.12.1항)를 참고하여 계획상 복원절차, 책임, 역할의 명확성, 계획의 주기적 수정보완 여부, 하위 실행문서 수립 및 사용자에게 제공 여부를 평가한다. **A2. 사이버복원력에 대한 인식과 태도**는 사이버안보훈령 제26조 및 ISMS의 인식제고 및 교육 훈련(2.2.4항)을 참고하여 사이버복원력 관련 교육 훈련 계획수립 및 교육 훈련 수행 여부, 교육 후 교육 효과와 적정성을 평가하여 다음 계획 수립 시 반영 여부, 인식제고를 위한 활동 수행 여부를 평가한다. **A3. 사이버복원력 점검/평가**는 사이버안보훈령 제26조 및 ISMS의 자원할당(1.1.6항)을 참고하여 사이버복원 계획에 따른 추진결과에 대한 점검/평가 수행 여부, 점검/평가 결과의 상급자 보고 여부, 사이버복원력 관련 상급부대 지시·강조사항 이행 여부를 평가한다.

Table 5. Basis for deriving assesment indicator A

Defense cyber security directive	Assessment Indicator	ISMS
Article 26, AT[3] 1. SM-1	A1	Item 1.1.5 / 2.12.1
Article 26	A2	Item 2.2.4
Article 26	A3	Item 1.1.6

4.1.2 대체성/예비능력(Redundancy)

'대체성/예비능력'은 시스템의 지속성을 유지하기 위한 분산된 인프라 네트워크, 분산된 자원 네트워크 등의 대체/예비자원 보유와 관련된 영역으로 B1. 예비사이트, B2. 체계 이중화, B3. 백업/복구 3개의 세부영역으로 구성되어 진다.

B1. 예비사이트는 사이버안보훈령 별표1 SM-1-3 및 ISMS의 백업 및 복구관리(2.9.3항)를 참고하여 체계 기능/서비스의 중단이나 장애발생 즉시 대체 지원할 수 있는 예비사이트의 구축 유무, 예비사이트가 체계의 복원 목표에 맞추어 필수 서비스 우선순위에 따라 즉시 대체지원 가능 여부, 예비사이트가 동일한 보안위험에 영향을 받지 않는 위치에 있는지 여부를 평가한다. **B2. 체계 이중화**는 사이버안보훈령 별표1 SM-1-4 및 ISMS의 백업 및 복구관리(2.9.3항)를 참고하여 주요시스템 및 네트워크의 이중화 구성, 관리 여부, 예비 네트워크 운영 시 주 네트워크 서비스 제공을 위한 시스템이나 네트워크 장치를 공유하지 않도록 구성되었는지 여부를 평가한다. **B3. 백업/복구**는 사이버안보훈령 별표1 SM-1-5 및 ISMS의 백업 및 복구관리(2.9.3항)를 참고하여 백업이 필요한 데이터와 관련자원을 식별하고, 우선순위에 따른 백업 및 복구절차 수립 여부, 백업 데이터 저장매체 및 관리시스템 등은 해당 데이터의 보안 요구사항과 동일하게 보호 가능 여부, 백업용·복구용 시스템이 물리적/지리적으로 떨어진 장소에 위치 여부, 백업 데이터가 인가된 사용자만이 수정/변경 가능토록 보호되는지 여부, 백업 데이터는 복원 시, 선택적으로 사용할 수 있도록 백업, 관리되는지 여부, 백업 주기에 따른 백업 수행 여부, 백업 정보의 완전성과 정확성, 복구절차의 적절성 확인

3) AT : Attached Table

Table 6. Basis for deriving assesment indicator B

Defense cyber security directive	Assessment Indicator	ISMS
AT 1. SM-1-3	B1	Item 2.9.3
AT 1. SM-1-4	B2	Item 2.9.3
AT 1. SM-1-5	B3	Item 2.9.3

을 위해 정기적으로 복구 테스트 실시 여부를 평가한다.

4.1.3 견고성(Robustness)

'견고성'은 외부의 위협으로부터 견딜 수 있는 시스템의 내재적 강도와 관련된 영역으로 C1. 네트워크 침입탐지/차단 및 통제, C2. 서버 보호 프로그램 적용, C3. 단말기 보호 프로그램 적용, C4. 사이버 공격 탐지/차단/대응체계, C5. 컴퓨터 바이러스 방역체계, C6. 공개 소프트웨어 활용 6개의 세부영역으로 구성되어 진다.

C1. 네트워크 침입탐지/차단 및 통제는 사이버안보훈령 별표1 NS-1-1 및 ISMS의 이상행위 분석 및 모니터링(2.11.3항)을 참고하여 네트워크 경계에 침입차단/침입탐지시스템 또는 동등 기능을 수행하는 시스템 적용 여부, 침입차단/침입탐지시스템이 국방통합보안관제체계와 연계되도록 구성, 운영되는지 여부, 침해시도 여부를 판단하기 위한 기준 및 임계치를 정의하고, 이상행위의 판단 및 조사 등 후속조치의 적시성 여부를 평가한다. **C2. 서버 보호 프로그램 적용**은 사이버안보 훈령 별표1 SS-4-1, 2 및 ISMS의 악성코드 통제(2.10.9항)를 참고하여 중요 서버시스템에 보안OS 설치 여부, 서버용 백신 프로그램 설치 여부, 서버용 백신 프로그램 운영 시 자동 업데이트 기능 보유 여부를 평가한다. **C3. 단말기 보호 프로그램 적용**은 사이버안보훈령 별표1 PS-2 및 ISMS의 업무용 단말기 보안을(2.10.6항) 참고하여 단말기 보호를 위해 필요한 승인된 보호 프로그램 설치, 운영 여부, 단말기 원격 데스크탑 서비스 해제 여부, Windows OS 보안 업데이트 주기적 실시 여부를 평가한다. **C4. 사이버공격 탐지/차단/대응체계**는 사이버안보훈령 별표1 SM-2-3 및 ISMS의 사고예방 및 대응체계 구축(2.11.1항)을 참고하여 국방통합보안관제체계 외 별도의 보호시스템 구축·운영 여부, 별도 보호시스템 구축 시 국방통합 보안 관제체계와의 중복성, 연계성 검토 여부를 평가한다. **C5. 컴퓨터 바이러스 방역체계**는 사이버안보훈령 별표1 SM-2-4 및 ISMS의 악성코드 통제(2.10.9항)를 참고하여 모든 서버, 단말기에 국방 바이러스 방역체계 또는 국방부에서 인가된 백신 프로그램 사용 여부, 별도의 백신 프로그램 사용 시, 자동 업데이트 기능 보유 여부, 스팸 및 스파이웨어로부터 시스템 보호대책을 평가한다. **C6. 공개 소프트웨어 활용**은 사이버안보훈령 별표1 SM-4-2 및 ISMS의 패치관리(2.10.8항)를 참고하여 공개 소프트웨어 적용 여부, 공개 소프트웨어 적용/활용 시 소스코드 분석/수정이 제한되는 것에 대한 영향도 검토 및 보호대책에 포함시켜 검토, 승인하는지 여부를 평가한다.

Table 7. Basis for deriving assesment indicator C

Defense cyber security directive	Assessment Indicator	ISMS
AT 1. NS-1-1	C1	Item 2.11.3
AT 1. SS-4-1, 2	C2	Item 2.10.9
AT 1. PS-2	C3	Item 2.10.6
AT 1. SM-2-3	C4	Item 2.11.1
AT 1. SM-2-4	C5	Item 2.10.9
AT 1. SM-4-2	C6	Item 2.10.8

4.1.4 자원동원성(Resourceulness)

'자원동원성'은 자원 동원능력 및 자원의 효율적 관리와 관련된 영역으로 D1. 사이버 복원 인력의 전문성, D2. 시스템 복원 능력, D3. 유관기관 상시 협력체계, D4. 보안취약점 제거 및 패치, D5. 취약점 분석·평가 4개의 세부영역으로 구성되어 진다.

D1. 사이버 복원 인력의 전문성은 ISMS의 자원할당(1.1.6항)을 참고하여 전문지식 및 관련 자격 보유 유무, 사이버복원 관련 실무경력 유무, 사이버 복원 관련 직무교육 이수 여부를 평가한다. **D2. 시스템 복원 능력**은 사이버안보훈령 별표1 SM-5-4를 참고하여 자체적으로 복원 가능 여부, 자체 복원 불가 시 외부기관을 이용하여 복원목표 시간 내 복원 가능 여부, 원격 복원이 부득이한 경우 보안대책 수립 여부를 평가한다. **D3. 유관기관 상시 협력체계**는 사이버안보훈령 별표1 SM-2-2와 별표5 및 ISMS의 사고예방 및 대응체계 구축(2.11.1항)을 참고하여 전군 차원의 사이버안전 위기관리체계와 유기적으로 연계 여부, 긴급 연락체계 구축 및 최신화 여부, 침해사고의 대응 및 처리를 위하여 외부전문가 등과의 협력체계 구축 여부, 외부 업체를 통한 복원

체계를 운영하는 경우 대응절차 세부사항에 대해 계약서에 반영 여부를 평가한다. **D4. 보안취약점 제거 및 패치**는 사이버안보훈령 별표1 AS-5-3 및 ISMS의 패치관리(2.10.8항)를 참고하여 알려진 오류 및 보안 취약점에 영향을 받을 수 있는 체계 S/W 및 어플리케이션을 식별하고 이를 제거할 수 있는 대책 수립 여부, 운영체제 및 필수 S/W의 보안패치 및 업데이트 주기적 시행 여부, 운영체제 및 필수 S/W의 보안패치 및 업데이트가 자동화된 수단으로 점검·관리되는지 여부, 최신 패치 적용이 어려운 경우 보완대책 마련 여부를 평가한다. **D5. 취약점 분석·평가**는 사이버안보훈령 별표1 SM-2-1 및 ISMS의 취약점 점검 및 조치(2.11.2항)를 참고하여 관련 규정에 따라 취약점 분석·평가 및 보안 측정 실시 여부, 취약점 분석·평가 및 보안측정을 통해 해킹 취약점을 식별/조치 여부, 최신 취약점 발생 여부를 지속적으로 파악하고 시스템에 미치는 영향을 분석 및 조치하는지 여부를 평가한다.

Table 8. Basis for deriving assesment indicator D

Defense cyber security directive	Assessment Indicator	ISMS
-	D1	Item 1.1.6
AT 1. SM-5-4	D2	-
AT 1. SM-2-2, AT 5.	D3	Item 2.11.1
AT 1. SM-2-3	D4	Item 2.11.1
AT 1. SM-2-1	D5	Item 2.11.2

4.1.5 신속성(Rapidity)

'신속성'은 빠른 시간안에 시스템 기능의 복구 가능 여부와 관련된 영역으로 E1. 복원 우선순위 선정, E2. 복원목표시간 설정, E3. 복원 훈련 수행 3개의 세부영역으로 구성되어 진다.

E1. 복원 우선순위 선정은 사이버안보훈령 별표1 SM-1-5 및 ISMS의 재해 재난 대비 안전 조치(2.12.1항)를 참고하여 시스템 기능에 대한 복원 우선순위 선정 여부, 핵심기능 복원 우선순위 및 복원목표시간 충족을 위한 정보자산의 복원 우선순위 선정 여부를 평가하며, **E2. 복원목표시간 설정**은 사이버안보훈령 별표1 SM-1-1 및 ISMS의 재해 재난 대비 안전조치(2.12.1항)를 참고하여 핵심기능 수행을 위한 복원목표시간 설정 여부를 평가한다. **E3. 복원 훈련 수행**은 사이버안보훈령 별표1 SM-1-2 및 ISMS의 사고 대응 훈련 및 개선(2.11.4항)을 참고하여 복원계획의 적절성·유효성을 점검할 수 있는 훈련의 주기적 수행 여부, 실제 상황에서의 대응태세를 점검할 수 있는 모의훈련 수행 여부, 예비/백업 사이트(존재시)를 포함한 모의훈련 수행 여부, 복원훈련 결과를 반영하여 복원체계를 개선하는지 여부를 평가한다.

Table 9. Basis for deriving assesment indicator E

Defense cyber security directive	Assessment Indicator	ISMS
AT 1. SM-1-5	E1	Item 2.12.1
AT 1. SM-1-1	E2	Item 2.12.1
AT 1. SM-1-2,	E3	Item 2.11.4

4.1.6 독립성(Independence)

'독립성'은 다른 시스템 혹은 외부 위협으로부터 영향을 받지 않는 시스템 기능 유지와 관련된 영역으로 F1. 인터넷/외부 네트워크 연동 통제, F2. 국방정보통신망 연동 통제, F3. 네트워크 접속 장비 인증 및 통제, F4. 무선 LAN 보호, F5. 원격접속 통제, F6. 전자우편 보호 6개의 세부영역으로 구성되어 진다.

F1. 인터넷/외부 네트워크 연동 통제는 사이버안보훈령 별표1 NS-3-1 및 ISMS의 인터넷 접속 통제(2.6.7항)를 참고하여 군·외부 인터넷망간 연동 시 DMZ 등을 구성하여 망간 직접 연결 통제 여부, 국방정보통신망과 인터넷망 연동시 망간 물리적 분리 특성이 훼손되지 않게 구성되었는지 여부, 외부 네트워크를 통해 외부기관/정보시스템과 자료를 교환/전달하는 경우 관계기관간 보안책임과 교환/전달되는 자료 범위의 명확성, 비밀정보를 취급하는 국방정보통신망의 인터넷과 연동 여부를 평가한다. **F2. 국방정보통신망 연동 통제**는 사이버안보훈령 별표1 NS-3-1을 참고하여 국방정보통신망 내 단위 통신망 및 정보체계들 간의 연동 시 합참 '네트워크 연동 보안 통제' 기준에 부합하도록 계획 및 시행 여부, 연동하는 타 정보시스템 목록 및 연동 방법이 체계보호 대책에 명확히 식별·기술되었는지 여부, 연동에 적용되는 접근통제 규칙이 체계내부의 접근통제 규칙과 구분되어 관리·적용되는지 여부, 비밀정보를 취급하는 정보시스템이 연동 시 승인된 보안통제장비를 이용하는지 여부를 평가한다. **F3. 네트워크 접속 장**

비 인증 및 통제는 사이버안보훈령 별표1 NS-2-1 및 ISMS의 네트워크 접근 통제를 참고하여 네트워크 장비의 관리/통제(2.6.1항)에 관한 적절한 계획을 수립하고, 이를 문서화하여 관리하는지 여부를 평가하며, **F4. 무선 LAN 보호**는 사이버안보훈령 별표1 AS-5-4 및 ISMS의 무선 네트워크 접근(2.6.5항)을 참고하여 승인되지 않은 무선접속점을 주기적으로 점검하는지 여부, 기술적 보호수단 강구 여부를 평가한다. **F5. 원격접속 통제**는 사이버안보훈령 별표1 SS-2-5 및 ISMS의 원격접근 통제(2.6.6항)를 참고하여 '가'급 체계 및 '비밀정보'를 처리하는 체계의 원격접속 허용 여부, 원격접속을 위한 정보 및 원격접속을 통해 유통되는 정보는 보호요구수준에 부합하게 보호되는지 여부, 원격접속 관련 정보책임자가 주기적으로 검토하는지 여부, 접근권한에는 대외비 이상으로 보호·관리 여부, 원격접속은 최소한의 필수 업무, 인원으로 제한하여 운영하는지 여부, 원격접속 내용을 감사로그에 기록하고, 정보보호 지침에 따른 원격사용자 접근통제 여부, 원격접속장비에 대한 보호대책 강구 여부, 서버 시스템의 시스템관리자(root) 계정은 시스템 콘솔에서만 접근되는지 여부를 평가한다. **F6. 전자우편 보호**는 사이버안보훈령 별표1 AS-5-6 및 ISMS의 인터넷 접속 통제(2.6.7항)를 참고하여 HTML 형식의 메시지를 텍스트 형식으로 읽도록 구성되었는지 여부, 첨부파일이 자동적으로 열리지 않는지 여부, 첨부파일을 열 경우 악성코드 포함에 대한 경고창 공지 여부, 바이러스탐지 S/W와 연계하여 첨부파일 검사 가능 여부, 메일 릴레이 기능 차단 여부를 평가한다.

Table 10. Basis for deriving assesment indicator F

Defense cyber security directive	Assessment Indicator	ISMS
AT 1. NS-3-1	F1	Item 2.6.7
AT 1. NS-3-2	F2	-
AT 1. NS-2-1	F3	Item 2.6.1
AT 1. AS-5-4	F4	Item 2.6.5
AT 1. SS-2-5	F5	Item 2.6.6
AT 1. AS-5-6	F6	Item 2.6.7

4.2 국방정보시스템 사이버복원력 성숙도단계 정의

국방정보시스템의 사이버복원력 성숙도를 평가하기 위한 성숙도단계는 「사이버보안 역량 성숙도모델(C2M2)」에서 제시한 MIL0~MIL3의 4가지 단계를 적용하였다. 왜냐하면 C2M2는 조직이 보안활동 및 프로세스의 현재 역량 상태를 평가하고 달성 목표를 설정한 후 목표까지의 격차를 식별해 투자 우선순위를 설정하기 위한 기준을 제시한 모델로 정보보호 관리체계의 구현과 관리에 중점을 두고 있어 국방정보시스템의 사이버복원력 성숙도를 평가하기에 적합하며, C2M2에서 제시한 4가지 수준이 사이버복원력 수준을 평가하기에 용이하다고 판단했기 때문이다.

하지만 각 등급별 특성을 정의함에 있어서 C2M2에서 제시한 MIL2 등급과 MIL3 등급의 특성에 대한 명확한 구분이 어렵다고 판단하여, 본 연구에서는 국방정보시스템의 사이버복원력 성숙도 수준을 좀 더 용이하고 명확하게 평가하기 위해 MIL2 등급과 MIL3 등급 특성을 구체화하여 Table 11. 과 같이 정의하였다.

우선 MIL0(미추진 단계)은 평가지표에 대해 인지하지 못하고, 관련된 활동과 행위를 전혀 수행하고 있지 않은 단계이며, MIL1(추진 단계)은 평가지표에 대해 인지는 하고 있으나, 명문화되지 않은 상태에서 관련된 활동과 행위가 상급 기관의 지시 등에 의해 즉흥적이며 임기응변식의 대응을 하는 초기(임시) 수행 단계이다. MIL2(관리 단계)는 평가지표에 대한 중요성을 인지하고 규정 또는 지침에 명문화하였으나, 관련된 활동과 행위가 잘 이루어지지 않는 단계이며, MIL3(최적화 단계)은 평가지표에 대한 중요성을 인지하고 규정 또는 지침에 명문화하여 관련된 활동과 행위를 정기적으로 수행 및 평가하는 단

Table 11. Definition of Maturity Indicator Level

Level	Definition
MIL 0	• The level in which not aware of the assessment indicator and are not performing any relevant activities and activities.
MIL 1	• Although the assessment indicator is recognized, but the related activities and activities are not documented.
MIL 2	• The level where the importance of assessment indicator is aware and documented, but related activities and actions are not well performed.
MIL 3	• The level at which the relevant activities and actions are regularly performed and evaluated by aware and documented the importance of the assessment indicator

계이다.

4.3 국방정보시스템 사이버복원력 수준평가를 위한 성숙도모델 예시

위에서 제시한 성숙도 모델의 평가지표 측정항목 및 성숙도단계를 적용한 국방정보시스템 사이버복원력 수준평가를 위한 성숙도모델 예시는 Table 12. 와 같다.

Table 12. Example of maturity model for the assessment of cyber resilience level in the defence information system

Assesment Area	Policy			
Assesment Indicator	A1. Establishment cyber resilience plan			
Assesment Item	Maturity Indicator Level			
	0	1	2	3
Are resilience procedures, responsibili-ty, and roles clear in plan?	not plan-ed	plan is established / not stipulated	unclearly stipulated	clearly stipulated
Are the plan regularly modified and supplement-ed?	not modi-fied	regularly modified / not stipulated	stipulated / cycle is not obeyed	stipulated / cycle is obeyed
Is a sub-execution document established and provided to the user to implement the resilience?	not established and provi-ded	document is established and provided / not stipulated	stipulatd / do not establish-ed and provided	stipulated / establish-ed and provided

V. 결론 및 향후 연구

본 연구에서는 사이버복원력과 관련된 선행연구와 「국방사이버안보 훈령」 및 「정보보호 관리체계(ISMS)」의 사이버복원 관련 요구사항을 식별하여 사이버복원력 평가를 위한 6개 평가영역 및 26개의 평가지표를 도출하였으며, 각 지표의 성숙도 수준을 용이하고 명확하게 평가할 수 있는 성숙도모델을 제시하였다.

특히, 평가지표 측정항목 도출 시 기존의 일반적인 정보시스템에 대한 측정항목과 더불어 군 보안관제체계, 내·외부망 분리 운영, 비밀정보 취급 시스템, 무선 및 원격접속 적극 통제 등 국방정보시스템만의 차별화된 특성을 반영한 측정항목을 도출함으로써, 높은 신뢰성과 가용성, 실시간 작동 및 안전한 작동이 요구되는 국방정보시스템의 실질적인 사이버복원력 수준 평가가 가능할 것이다.

따라서 본 연구에서 제시한 성숙도모델을 이용하여 사이버복원력 수준 평가를 수행 후 시스템의 미흡한 분야를 식별 및 보완한다면, 해당 시스템의 사이버복원력 강화를 통해 국방 분야의 사이버보안 수준 향상 및 국가안보에 큰 도움이 될 것으로 기대된다.

본 연구의 향후 연구 방향은 다음과 같다. 첫째, 본 연구에서 제시한 성숙도모델의 평가영역 및 평가지표에 대해 실증적인 타당성을 검증하는 것이다. 이를 위해 NIST 800-160 등 국제적으로 연구되어지고 있는 표준들에 대한 연구도 포함할 필요가 있을 것이다. 둘째, 국방정보시스템에 대한 실제 사이버복원력 수준 평가 사례를 통해 모델 전반의 유용성에 대해 지속적으로 검증 노력을 기울여 나가는 것이다. 마지막으로 국방정보시스템에 대한 성숙도모델의 타당성과 유용성이 검증된다면 국가 및 기업의 주요 정보시스템을 대상으로 하는 사이버복원력 수준 평가를 위한 공통적인 성숙도평가 영역 및 지표를 도출해 나가는 모델로 발전시켜 나갈 수 있을 것으로 기대한다.

References

[1] National Intelligence Science, Ministry of Science & ICT, Korea Communications Commission, Financial Services Commission Ministry of Public Administration & Security, "National information security white paper 2018," May. 2018.

[2] U.S. White House, "National Cyber Strategy," pp. 6, Sep. 2018.

[3] U.K. HM government, "National Cyber Security Strategy 2016-2021," Nov. 2016.

[4] Sangbae Kim, "Cyber security strategegies of major powers in world

politics," Review of International and Area studies, 26(3), pp. 67-108, Sep. 2017.
[5] S.Y. Son, H.Y. Kim and J.Y. Yu, "The safety of the Hyper-connected society and measures for securement of cyber resilience," Dec. 2017.
[6] National Security Office, " National cybersecurity strategy," pp. 12, Apr. 2019.
[7] Ministry of National Defend(MND), "Defence informatization task directive," May. 2019.
[8] B.J. Jeon, J.H. Kang, J.C. Yoo and K.Y. Shin, "An Analysis of IPv6 Transition Status and Efficient Address Allocation for the Defense Information Systems," Korean Journal of Military Art and Science, 73(3), pp. 227-249, Oct. 2017.
[9] Y.N. Oh and K.S. Hwang, "A study on the impact of vendor relationship on the success of the National Defence Information System for outsourcing," The Korean Operations Research and Management Science Society, pp. 475-478, Oct. 2005.
[10] Hyeon-suk Lyu, "A Study on Cyber Security Policy and Governance in the ICT Convergence Environment: Focused on "Authentication'," pp. 16, Dec. 2015
[11] National Infrastructure Advisory Council, "A framework for establishing critical infrastructure resilience Goals," pp. 15, Oct. 2010.
[12] Bodeau, D and Graubart R, "Cyber resiliency engineering framework," The MITRE Coporation, pp. 8, Jan. 2011.
[13] EY, "Achieving resilience in the cyber ecosystem," pp. 1, Dec. 2014.
[14] Bank for Internal Settlements(BIS) CPMI - IOSCO, "Guidance on cyber resilience for financial market infrastructures," pp. 4, Jun. 2016.
[15] J.Y. Suh, B.W. Park, S.H. Lee, K.I. Cho and J.H. Yun, "Future Risk and Resilience," 2014.
[16] Heejun Yu, "Reinforcement measures of the cyber resilience of domestic FMI reflecting the recent trends of onternational discussion," Korea Bank, Apr. 2016.
[17] Jaesuk Yun, "Development and Application of Global Cybersecurity Maturity Index Model," Ph.D. Thesis, Korea University, Dec. 2016.
[18] Carnegie Mellon University Software Engineering Institute, "CMMI for Development, Ver1.3," Nov. 2010.
[19] G.R. Choi and C.J. Kim, "A Study on BigData Capability Maturity Model," Journal of Korean institute of information technology, 12(12), pp. 149-162, Dec. 2014.
[20] S.K. Lee and I.S. Kim, "A Study on the Method of Checking the Level of Information Security Management Using Security Maturity Model," Journal of the Korea Institute of Information Security & Cryptology, 28(6), pp. 1585-1594, Dec. 2018.
[21] U.S. Department of Homeland Security and Department of Energy, "Cybersecurity Capability Maturity Model Version 1.1," Feb. 2014.
[22] MND, "Defense cyber security directive," Dec. 2018.
[23] Korea Internet & Security Agency(KISA), "Personal information & Information Security Management System Certification Guide," Jan. 2019.

〈저자소개〉

최 재 혁 (Jae-hyeok Choi) 정회원
2003년 3월: 해군사관학교 군사전략학과 졸업
2009년 2월: 고려대학교 국제경영학과 석사
2018년 3월~현재: 아주대학교 NCW학과 박사과정
〈관심분야〉 사이버전, 사이버보안, 사이버복원력, 방산기술보호

김 완 주 (Wan-ju Kim) 종신회원
1998년 2월: 서울과학기술대학교 전자공학 학사
2008년 1월: 국방대학교 전산정보 석사
2017년 2월: 아주대학교 NCW공학 박사
2017년 3월~현재: 아주대학교 NCW학과 겸임교수
〈관심분야〉 사이버전, 국방전술통신, 정보보증, 사이버위협예측

임 재 성 (Jae-sung Lim) 종신회원
1983년 2월: 아주대학교 전자공학 학사
1985년 2월: KAIST 영상통신 석사
1994년 8월: KAIST 전자공학 박사
1998년 3월~현재: 아주대학교 소프트웨어융합학과 교수
〈관심분야〉 Military&Mobile Communications, Wireless Networks, 사이버전