Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.32, NO.2, Apr. 2022 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2022.32.2.289

국가 사이버보안 수준 향상을 위한 GCI의 지표개선 방안*

김 대 경,[1†] 이 주 현,[2] 김 예 영,[2] 현 다 은,[2] 오 흥 룡,[4] 진 병 문,[3] 염 흥 열[3‡]
[1,2,3]순천향대학교 (대학원생, 학생, 교수), [4]한국정보통신기술협회(수석연구원)

Proposals for GCI Indicators to Improve a National Cybersecurity Level*

Dae kyung Kim,[1†] Ju hyeon Lee,[2] Ye young Kim,[2] Da eun Hyeon,[2]
Heung-Ryong Oh,[4] Byoung moon Chin,[3] Heung Youl Youm[3‡]
[1,2,3]Soonchunhyang University (Graduate student, Undergraduate, Professor),
[4]TTA (Chief Researcher)

요 약

국제전기통신연합(International Telecommunication Union, ITU)에서 개발한 글로벌사이버보안지수(Global Cybersecurity Index, GCI)는 국가의 사이버보안발전 수준을 진단하고, 사이버보안 역량을 강화하기 위해 활용되고 있다. 본 논문은 GCI를 분석하고, 그 효과성을 강화하기 위한 방안을 제시하고자 한다. 또한, GCI 버전1~GCI 버전4 평가지표를 사전 분석하고, SWOT 분석을 통해 발전 방안을 살펴본다. 이를 통해, GCI 개선 및 활용을 위한 기본원칙을 수립하고, GCI 버전5 설문지 관련 신규 지표를 발굴하고 제안하고자 한다. 본 논문은 GCI의 성과 분석 및 개선 방안을 위한 기초 자료로 활용 가능할 것으로 기대된다. 또한, 향후 GCI 평가에서 적용될 보다 발전된 사전대응 지표와 사후대응 지표를 제안하여 GCI의 효과성을 높이고 국가의 사이버보안 역량을 높이는데 기여하고자 한다. 본 논문은 [1]의 연구 결과를 개선 발전시킨 것이다.

ABSTRACT

The Global Cybersecurity Index (GCI) developed by the International Telecommunication Union (ITU) is used to diagnose a country's cybersecurity development level and to strengthen its cybersecurity capabilities. This paper analyzes GCI and tries to suggest a way to strengthen its effectiveness. In addition, we analyze the GCI version 1~GCI version 4 evaluation index in advance, and examine the development plan through SWOT analysis. Through this, basic principles for GCI improvement and utilization will be established, and new indicators related to the GCI version 5 questionnaire will be discovered and suggested. This paper is expected to be used as basic data for GCI performance analysis and improvement plan. In addition, it is intended to contribute to enhance the effectiveness of GCI and the nation's cybersecurity capabilities by proposing more advanced proactive and reactive indicators to be applied to the future GCI evaluations. This paper is an improvement and development for the research result of [1].

Keywords: ITU, GCI, Global Cybersecurity Index, proactive and reactive indicator

I. 서 론

현대 사회는 인공지능, 사물인터넷, 빅데이터, 자율주행 등 ICT 기술 기반의 4차 산업혁명(Fourth Industrial Revolution) 시대를 맞아, 물리적 영역의 보안과 사이버 영역의 보안이 결합하여 새로운

Received(12. 17. 2021), Modified(1st: 02. 08. 2022, 2nd: 02. 15. 2022), Accepted(02. 25. 2022)
* 이 논문은 과학기술정보통신부의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임(과제번호: 2021-0-00112, 차세대보안 표준전문연구실 / 과제번호: 2020-0-0-2006, 글로벌사이버보안지수 분석·개선 연구)
† 주저자, kimdk@korea.kr
‡ 교신저자, hyyoum@sch.ac.kr (Corresponding author)

융합 보안의 시대로 발전하였다.

이러한 상황 속에서 국가 사이버보안의 글로벌 경쟁력을 객관적으로 평가할 수 있는 수치 및 지표의 중요성이 높아졌으며, ITU가 2014년부터 시행하고 있는 GCI(Global Cybersecurity Index, 글로벌 사이버보안지수)는 이를 측정하기 위한 중요한 도구이다. ITU의 GCI는 사이버보안 역량에 대한 전 세계 국가의 수준을 측정하는 지수로서 법적·기술적·조직적 조치와 역량 강화 및 협력의 총 5개 필러 82개 세부 지표로 구성되어 있다. GCI는 2014년부터 시행되어 주기적(약 2년 단위)으로 전 세계 국가의 사이버보안 대응역량을 평가하고 국가별 순위를 발표한다.

한국은 2015년 0.706/1점으로 5위의 높은 순위를 기록하여 사이버보안 분야에 대한 국제적 위상 및 두각을 나타냈지만, 2017년에는 0.782/1점으로 13위에 머물렀고, 2019년에는 0.873/1점으로 15위를 기록하였다. 하지만 2021년에는 98.52/100점으로 세계 4위라는 성과를 달성하였다. ITU의 GCI 순위 상승은 한국의 사이버보안 분야의 국제적 위상이 전 세계적으로 높아졌다는 의미이다.

본 논문은 GCI를 통한 국가의 사이버 보안수준 측정의 효과성을 제고하고, 나아가 전 세계 국가의 사이버보안 수준 향상을 도모할 수 있도록 향후 GCI 평가에 적용할 수 있는 새로운 신규 지표를 발굴하고 제안하고자 한다.

본 논문의 주요 구성으로는 다음과 같다. 2장에서 GCI의 정의와 그 평가범위 및 평가지표의 구성에 대해 알아보고 2015년부터 발표되었던 ITU의 4차례의 평가(버전1~버전4)에 대해 그 특징과 결과를 알아보고자 한다. 3장에서는 GCI 평가에 대한 SWOT 분석을 통해 그 효과성 제고를 위한 발전 방안에 대해 알아보며, GCI와 유사한 평가체계로 에스토니아의 eGA(e-Governance Academy)에서 시행하는 NCSI[12]와의 비교결과를 기술하였다. 4장에서는 GCI 평가지표에서 사전대응 측면의 발전된 신규 지표와 사후대응 측면의 신규 지표를 발굴하여 제안한다. 이러한 과정을 통하여 GCI의 지표개선을 통해 궁극적으로 각 국가의 국가 사이버보안 수준 향상에 기여하고자 한다.

기존 보고서[1]에서는 우리나라가 좋은 평가를 받기 위한 전략과 사전 대응지표를 중심으로 제시하였지만, 본 논문에서는 각 국가의 사이버보안 수준을 정확히 평가하기 위한 GCI 평가모델의 개선과 [1]에서 기술된 사전대응 지표를 개선했고 사후대응 지표를 추가적으로 제시하였다.

또한, 기존의 GCI가 가지고 있는 강점과 약점을 분석하여 약점을 보완할 수 있는 사전대응 지표와 사후대응 지표를 제시한다. 그리고, 기존의 GCI가 주로 사전대응지표 위주로 구성되어 있지만 본 논문에서는 사전대응 지표에 추가하여 사후대응 지표를 제시한다. 사후대응 지표로는 국제 지표인 X.1208에서 조직 단위의 사이버보안 지표를 국가 단위의 사이버보안 지표로 선정하여 변환한 것으로, GCI가 각 국가의 사이버보안 수준을 좀 더 정확히 평가할 수 있도록 개선된 모델을 제시하였다.

한편, 본 논문의 제약점으로 GCI의 평가지표는 지표 선정에 참여하는 국제 전문가 그룹에 의해 선정되어 구성되는 관계로 신규 지표의 효과성을 실증적으로 검증하는데 제약이 있다는 점을 들 수 있다.

II. GCI 프레임워크 및 분석

GCI는 사이버안전에 대한 문제의 중요성과 사이버보안에 대한 인식을 높이기 위해 전 세계적 차원에서의 국가들의 노력을 측정하는 신뢰할 수 있는 평가결과이다. 사이버보안은 국가의 공공 및 민간 분야 전체를 포함하는 광범위한 적용 분야를 가지고 있으며, GCI의 평가는 각 국가의 사이버보안 역량에 대해 법적 조치, 기술적 조치, 조직적 조치, 역량 구축, 협력의 5개 핵심 필러에 대해 평가하고, 종합 점수로 발표한다.

본 장에서는 ITU에서 주관한 GCI의 전체 평가의 범위 및 프레임워크를 분석하고, 아울러 과거 시행된 평가(버전1~버전4)의 결과에 대해 버전별로 간략히 알아보고자 한다.

2.1 GCI 프레임워크

GCI는 ICT 기술 사용에 대한 신뢰와 보안성을 구축하고, 궁극적으로 ICT 핵심 기술을 포함한 사이버보안 역량을 제고하기 위한 글로벌 문화를 육성하는 것을 목표로 하고 있다. 또한, 전 세계 여러 이해관계자와의 노력과 협력을 통해 현재와 미래사회 발전을 위한 시너지효과 창출을 도모하고 있다. 이의 평가에는 법적 조치, 기술적 조치, 조직적 조치, 역량 구축, 협력의 총 5개 필러별로 구성된 세부 지표(총 82개, 버전4)에 대해 평가대상 국가에서 제출한

답변과 증빙 자료의 검증과 평가를 시행한다.

GCI는 GCA(Global Cybersecurity Agenda, 글로벌 사이버보안 의제)의 5개 필러(pillar)에 대하여 국가별 사이버보안 대응수준을 모니터링하고 분석 및 평가하기 위해 각 필러마다 진화하는 지표 수를 하나로 결합한 복합 지수이다. GCI의 5개 핵심 필러(pillar)에 대한 평가 시 중점 고려 사항은 아래와 같다[1].

- 시간의 경과에 따른 국가 및 다른 국가에 대한 사이버보안 공약의 형태, 수준 및 발전
- 국제적 관점에서 모든 국가의 사이버보안 공약의 발전
- 지역적 관점의 사이버보안 공약 발전
- 사이버보안 공약에 대한 차이(사이버보안 이니셔티브에 대한 국가 간 참여 수준의 차이)

GCI의 사이버보안 대응역량의 평가는 각 국가별 여건과 환경에 적합한 대응역량을 발전시키는 데 도움을 주며, 전 세계 국가의 사이버안전에 대한 인식 향상과 공감대 형성을 통한 글로벌 협력 문화 육성에 기여하고 있다.

[그림 1]은 GCA 하위의 5개의 필러(pillar), 지표 및 질문의 계층적 관계를 보여주고 있으며, 국가 수준의 사이버보안 대응역량 개발을 위한 정책기관과 전략의 필요성을 보여주는 조직적 조치 필러(pillar)에 대해서만 계층적 관계를 확장하여 나타내고 있다[1].

위와 같은 계층적 구조에서 각 국가별 다양한

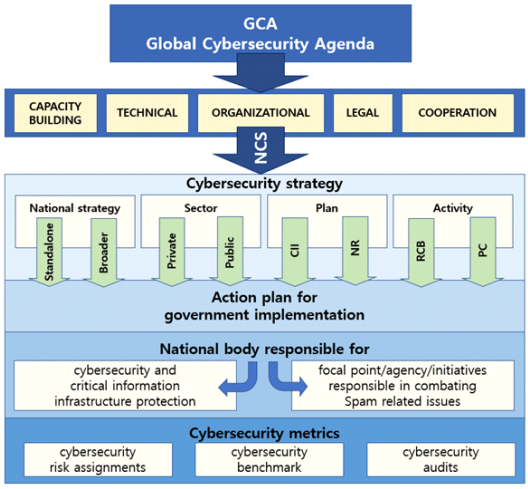

Fig. 1. GCI/GCA mapping of the organizational pillar (adapted from [8])

ICT 발전 상황과 사이버보안발전 수준을 고려한 각기 다른 사이버보안 요구 사항이 고려되고 있다. 위 구조에서는 사이버보안 대응역량이 발전할수록 계층구조와 솔루션이 더 복잡해진다는 점을 가정으로 하였다. 사전 식별된 다양한 사이버보안 솔루션의 존재를 확인하고, 각 필러(pillar)에 대한 계층적 경로를 따라 더 많이 진행될수록 해당 국가의 사이버보안 대응역량 수준이 더욱 포괄적이고 다양하게 되어 더 높은 GCI 점수를 받을 수 있게 된다[1].

(1) 법적 조치(Legal measures)

법적 조치는 입법 및 규제의 기준에 맞도록 조정 가능한 프레임워크를 제공하기 위한 조치이며, 사이버범죄와 사이버보안 관련 프레임워크와 법정 기관의 수를 기반으로 평가된다. 법적 조치는 모든 범주의 공법 및 사법을 의미하는 사이버보안 실체법과 특정 부분의 법제 수행을 위한 사이버보안 규제로 구성된다.

(2) 기술적 조치 (Technical measures)

기술적 조치는 사이버보안 분야의 기술을 담당하는 기관 및 프레임워크를 의미한다. 정보통신 기술(ICT)은 신뢰와 보안성이 보장된 환경에서 지속적으로 발전할 수 있으며, GCI의 회원 국가는 정보통신 시스템 및 응용 프로그램에 적용되는 최소한의 보안기준과 인증 체계 수립을 위한 전략을 개발해야만 한다. 이러한 노력은 사이버 공격에 대한 감시와 경고, 사고 대응을 위한 국가적 대응체계와 함께, 정부기관 및 당국과 협력하여 국가적 수준에서 사이버 사고 처리를 수행하는 조직의 설립과 병행되어야 한다. 하위 그룹은 다음과 같은 성과 지표로 평가된다[1].

- 국가 침해사고 대응팀: 국가 수준에서 컴퓨터 보안 사고에 대한 대응 조정 및 지원 책임이 있는 구체적인 조직
- 분야별 CERT/CIRT/CSIRT: 특정 분야(공공시설, 금융, 의료, 학계 등)별로 구성되어 해당 분야의 사고에 대응하는 침해사고대응 조직.
- 사이버보안 표준 개발을 위한 프레임워크: 공공/민간 분야에서 국제적으로 인정받는 사이버보안 표준 개발을 위한 국가 프레임워크 마련을 평가.
- 온라인 아동보호: COP 전담 국가 기관의 존재, 헬프라인의 가용성, 온라인상의 아동보호를 위해 배치된 기술적 메커니즘 및 기능을 측정하며 정부 또는 비정부 기관의 모든 활동을 포함.

(3) 조직적 조치(Organizational measures)

조직적 조치는 국가 사이버보안 대응역량 전략을 위한 정책기관을 의미한다. 여기에는, 모든 유형의 국가 이니셔티브를 계획대로 시행하고 시행결과를 평가하기 위한 조직 및 절차와 함께 광범위한 전략적 목표 설정 및 구조 수립이 필요하다.

국가의 전략, 거버넌스 모델 및 감독 임무를 담당하는 기관이 없다면, 다양한 부문과 각각의 노력이 서로 연결되지 않아 사이버보안 대응역량 개발에서 상호 간 연결과 조화를 이루려는 노력을 방해하게 된다. 효과적인 조직 구조의 생성은 국가 간, 기존 및 신규 이니셔티브 간, 각 기관 간, 각 부문 간의 조정과 협력에 있어 반드시 필요하다.

(4) 역량 구축(Capacity measures)

역량 구축은 사이버대응 역량 강화를 위한 연구개발, 교육 훈련 프로그램 및 공인된 전문가와 공공기관의 존재 여부를 의미한다. 법적, 기술적, 조직적 조치에 내재하며 기술적인 관점에서 가장 자주 다루어진다. 사이버보안 촉진을 위한 역량 구축 프레임워크는 사이버보안에 대한 인식 제고 활동과 인적, 물적 자원의 가용성을 포함하며, 일부 데이터는 현재 전 세계적으로 인증된 교육을 제공하는 신뢰할 수 있는 보조 소스를 통해 수집된다.

(5) 협력(Cooperation)

협력은 국제적인 파트너십, 협력 절차, 정보를 위한 네트워크를 의미한다. 국경이나 부문별 구분을 알지 못하는 사이버보안 분야 특성상 대화와 조정을 강화하여 포괄적인 다중 이해 관계자 접근 방식을 통한 대처가 필요하다. 더 큰 협력 이니셔티브는 반복적이고 지속적인 온라인 위협을 억제하고 이에 대한 더 나은 법적인 절차와 조치를 가능하게 할 수 있다.

2.2 GCI 버전1~ 버전4 분석

본 절에서는 지금까지 시행된 ITU의 GCI 버전1~버전4의 각 버전별 평가결과를 간략히 알아본다.

먼저 2015년 시행된 GCI 버전1[3]에서는 총 17개의 문항으로 구성되었다(법률2, 기술3, 조직4, 역량4, 협력4). 각 필러별 점수는 총점 1점 만점으로 평가되었으며, 평가결과에 대해서는 각 대륙별로 가장 높은 평가를 받은 대륙부터 가장 낮은 평가를 받은 대륙을 순서별로 표기하였다. 특히, 버전1 결과 리포트에서는 각 국가에서 시행하고 있는 좋은 예시를 들어 설명하고 있는 점이 특징이라 할 수 있다. GCI 버전1 평가결과 한국은 0.706점을 취득해 전체 평가대상 국가 중 5위의 우수한 성적을 기록하였다.

2017년 시행된 버전2[6]의 평가를 위한 질문 항목은 총 114개로 구성되었고, 온라인 아동보호와 기타 의견에 대한 질문이 추가되어 포함되는 등 평가방법에 있어 많은 변화가 있었다. 이로 인해 GCI 버전1과 버전2의 평가결과를 직접 비교하기는 어려운 면이 있으며, GCI 버전2에서 개선된 주요 사항으로 아래와 같은 점을 들 수 있다.

먼저, GCI 버전2는 버전1에 비해 평가의 깊이를 개선하기 위해 5개의 필러별로 각각 여러 항목의 새로운 질문이 추가되었다.

다음, GCI 버전1의 지수는 단순한 평균 방법론을 사용했다면 버전2의 지수는 각 필러에 가중치를 적용했다는 특징이 있다.

그리고, 각국의 ICT 발전에 따른 사이버보안의 중요성에 대한 인식을 높이기 위하여, ITU의 GCI와 IDI(ICT for Development Index)의 상관관계를 비교하고 각 국가의 ICT 발전에 따른 사이버보안 대응수준을 그래프로 나타내었다. 여기에서 GCI와 IDI간의 특별한 상관관계는 표시하지 않고 있으나, 사이버보안에 대한 투자와 헌신의 중요성을 강조하기 위해 기존 국가 프로세스와 어떻게 연관 지을 수 있는지 나타내어 주고 있다.

[그림 2]는 2016년 세계 각국 IDI와 GCI의 발전 수준을 나타낸 그래프이다[6].

GCI 버전2의 평가결과 한국은 0.782점을 획득

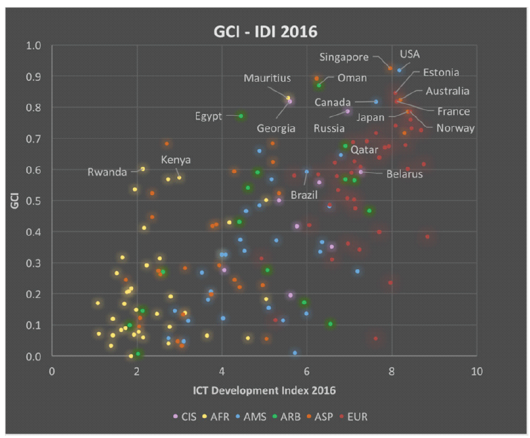

Fig. 2. Global Comparison 2016 IDI and GCI[6].

하여 전체 평가대상 국가 중 13위를 차지하였고, 전 세계 국가의 사이버보안 수준의 평가에 있어 2015년 시행된 버전1 평가결과보다 8단계 하락한 순위를 기록하였다.

2018년에 시행된 버전3[8]는 우선 평가 질문의 총수가 25개(법률3, 기술6, 조직3, 역량7, 협력6)로 줄었으며, 각 평가 항목에 대한 점수의 가중치를 부여하여 평가하였다. 평가결과 한국은 평가대상 전체 국가 중 총 0.873점의 점수를 획득하여 15위를 기록하였으며, 이는 같은 대륙으로 분류된 아시아-태평양 지역의 국가에서도 5위에 해당하는 성적이었다.

버전3의 평가결과[8]에서도 정보 격차의 추세와 발전을 분석한 IDI의 결과를 GCI와 비교하여 제시하였다. 일반적으로 GCI 순위가 높을수록 IDI가 높다는 것으로 나타나고 있으나, 여기에서 특이한 점은 아이슬란드의 경우 IDI가 높은 반면 GCI가 낮게 평가되었으며, 일부 국가(Andorra, Saint Kitts and& Nevis)의 경우 GCI는 높은 반면 IDI는 낮게 평가된 사례도 있었다. 버전3에서는 정보 격차의 추세와 발전을 분석한 IDI의 결과를 버전2보다 구체적으로 GCI와 비교하여 제시하고 있으며, IDI가 효과적이고 탄력적이기 위해서는 사이버보안의 대응에 대해서도 변화하는 요구 사항을 적극 반영하고, 정기적으로 업데이트해야 한다는 의견을 제시하고 있다. 다시 말해, GCI와 IDI의 상관관계에 관한 지속적 연구를 통해 국가의 ICT 발전에 맞는 사이버보안 대응수준을 구축할 수 있음을 시사하고 있다. [그림 3]은 GCI 버전3에서 평가된 세계

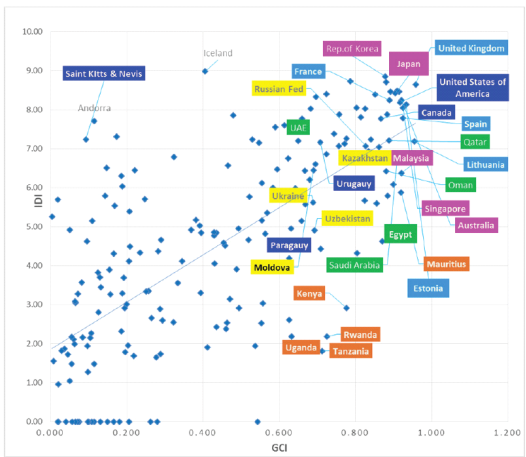

Fig. 3. Comparison of 2018 global IDI and GCI ranking[8]

각국의 GCI 순위와 IDI 순위를 비교하여 표기한 그래프이다[8].

다음으로, 최근 2020년 시행된 GCI 버전4[9]에 대해 알아보자. 버전4의 평가지표는 총 82개의 항목(법17, 기술17, 조직14, 역량23, 협력11)으로 구성되었고, 평가결과는 최상의 평가를 받은 국가(미국)를 기준으로 100점 만점(백분율)으로 표기하였다.

법적 조치 필러에는 사이버보안 관련 국가 실체법을 더 잘 반영하도록 구성되었고, 기술적 조치 필러에는 CIRT의 작동 방식을 더 잘 반영하도록 재구성되었다. 조직적 조치 필러에는 국가적 차원의 지속적인 국가 사이버보안 전략의 정기적인 업데이트와 COVID-19 팬데믹 기간 아동의 온라인학습 시간 증가에 따른 온라인 아동보호 체계를 개발하는 노력이 새롭게 반영되었다. 역량 구축 필러에는 중소기업(SME)에 대한 정부 지원에 대한 인식 제고를 포함하도록 그 범위가 확장되었다. 협력 필러에는 법적 구속력 여부와 관계없이 계약이 서명 또는 비준되었는지를 반영하여 평가되었다.

한국은 총 194개 평가 대상국 중 98.52점으로 4위의 성적을 기록하여, 버전3의 15위에서 11단계 상승한 결과를 받았다. 한국은 전체 5개 필러 중 3개 필러(법률, 역량, 협력)에서 만점을 받았고, 2개 필러(기술, 조직) 또한 상위권 성적을 기록(기술 0.977, 조직 0.949)하여, 전체 GCI 버전4 평가결과에서 4위를 기록하였다[17]. 아래 [그림 4]는 한국이 취득한 각 항목에 대한 평가지표와 분석 결과를 도식화하여 나타낸 것이다[9].

한편, GCI 버전4에서 한국의 종합 점수와 순위의 주요 상승 요인은 다음과 같다.

먼저, 2019년 국가 주도의 '국가 사이버 안보 전략' 수립 이후 국가 주요 기반시설에 대한 보안대책 강화, 사이버 공격에 대한 억제력 확보 등 국가 사

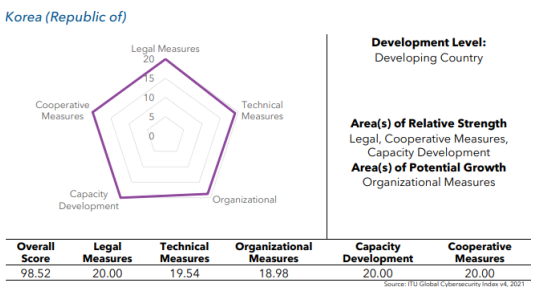

Fig. 4. Global Cybersecurity Index 2020: Country profiles (Republic of Korea) [9]

이버 안보를 위한 대응체계 강화 노력을 지속해 온 것이 주효했다고 볼 수 있다. 그리고, 정부 주도로 적극적으로 추진하고 있는 'K-사이버방역 추진 전략'에 있어 사이버 공격에 대응하기 위한 지속적인 투자와 거버넌스 레벨의 국가적 지원이 있었던 점을 꼽을 수 있다[16].

이상과 같이 2015년 처음 발표된 GCI 버전1의 결과로부터 최근 2021년 발표된 버전4까지의 평가 결과에 이르기까지 간략히 알아보았다.

[표 1]은 GCI 버전1~버전4의 시행연도(데이터 수집, 결과발표), 질문의 수, 평가대상(194개 회원국) 중 자료 제출국 수 및 한국이 취득한 점수와 순위를 도표로 표기한 것이다.

Table 1. Analysis of GCI (V1~V4) (adapted from [6],[7],[8],[9])

Category	GCI1	GCI2	GCI3	GCI4
Data Collecting Years	2013 ~14	2016	2017 ~18	2020
Publishing Year	2015	2017	2019	2021
Questions	17	114	25	82
Participating countries	105	136	155	169
Score (Republic of Korea)	0.706 / 1	0.782 / 1	0.873 / 1	98.52 / 100
Rank (Republic of Korea)	5	13	15	4

III. GCI 지표개선 전략 및 NCSI와의 비교분석

본 장에서는 GCI 지표개선 전략을 마련하기 위한 분석을 시행하고, GCI와 NCSI(National Cyber Security Index)를 비교하여 분석한다.

먼저 GCI의 지표 개발과 평가단계 등의 전체 과정에 대해 간략하게 알아보고, GCI의 내면적 요인과 외부 환경요인 및 영향에 대해 알아봄으로써 각 필러별 평가체계가 가지는 강점의 강화와 약점의 보완, 기회 요인의 부각과 위협 요인의 감소를 위한 방법론을 도출하고, 분석 결과에 따른 평가방법 개선을 위한 기본 방향과 전략을 도출하고자 한다. 궁극적으로 GCI 평가의 효과성을 제고하고 국가 사이버보안 수준의 향상에 기여하는 기반을 마련하고자 한다.

3.1 GCI 평가단계

GCI 지표 개발 및 평가는 모두 4단계의 과정으로 이루어진다. 먼저 1단계에서 평가를 위한 설문지를 준비하고, 2단계에서 온라인상의 설문 조사를 시행한다. 3단계에서는 평가에 참여한 각 국가에서 제출한 데이터에 대한 검증과 평가를 시행하고 최종 평가점수와 순위를 기록한다. 최종적으로 4단계에서 결과보고서를 발간함으로써 모든 과정이 종결된다. GCI의 지표 개발단계부터 최종 결과보고서에 이르기까지 진행된 각 단계의 프로세스는 평가단계와 평가결과의 투명성을 보장하기 위해 ITU의 연구 그룹에 제출된다.

3.2 GCI SWOT 분석

먼저 GCI 평가의 효과성을 개선하기 위한 사전 분석 방법으로 SWOT 분석 기법을 적용하여 분석한다. GCI에 대한 SWOT 분석에는 가장 최근에 시행된 GCI 버전4를 대상으로 하였다.

먼저, GCI 평가의 내면적 요인인 강점과 약점을 식별하고, 외부 환경적 요인인 기회 요인과 위협 요인을 식별한다. 나아가 SWOT 분석으로 식별된 강점, 단점, 기회 및 위협 요인에 대한 크로스 SWOT 분석을 통해 더욱 객관적이고 타당성 있는 분석 결과를 도출하고자 한다.

이러한 분석 과정은 곧 GCI의 지표개선을 위한 사전 작업이며 밑그림이 되는 과정이 될 것이다. 이 과정에서 GCI의 강점 강화, 약점 감소, 기회 요인 부각 및 위협 요인 감소를 통한 GCI 평가체계의 효과성 개선의 기본적인 방향성과 전략을 도출하고자 한다.

3.2.1 GCI SWOT 여건 분석

GCI에 대한 강점, 약점, 기회, 위협 요인 도출 과정에서는 관련 분야 전문가들 7~8명이 수차례 모여 Brain Storming 과정을 거쳐 보다 객관화된 요인들을 도출하였으며, 이후 이 요인들에 대한 추가적 분석 과정을 거쳐서 GCI 개선 전략을 도출하고자 한다.

CGI에 대한 SWOT 분석을 통해 내면적 요인인 강점과 약점, 외부적 요인인 기회와 위협에 대해 분석한 결과는 아래와 같다. 강점 요인은 GCI가 가지

고 있는 긍정적인 요인이며, 기회 요인은 정보통신 기술의 발전과 연관되는 외부 환경요인이다.

첫째, GCI의 강점은 5가지 필러에 대해 각국의 사이버보안에 대한 대비와 보호 및 사전대응 능력을 평가하는 지표로 구성되어 있어, 사이버보안 위협에 대한 자국의 준비성을 검토하고 보완할 수 있도록 하는 데 도움이 된다. 또한, 국제적 협력 관계에 의해 각 국가의 사이버보안 대응역량을 평가하여 순위가 결정되기 때문에 평가 대상국들이 국가, 지역 및 국제 수준에서의 사이버보안 인식을 높이고 사이버보안 역량을 스스로 구축할 수 있도록 하는데 기여하고 있다.

아울러, 5개 필러 82개 세부 지표에 대해 모든 항목을 망라하여 평가하고 있어 각 국가의 사이버보안 수준을 평가하는 강력한 틀이 되며, 국가 사이버보안 수준을 측정하는 데 도움이 된다.

둘째, GCI의 약점으로는 사이버보안을 구현하고 촉진하기 위한 국가적, 구조적 준비의 존재 여부 등 포괄적 평가 요소를 통해 각 국가의 사이버보안 대응 역량의 순위를 평가한다는 점으로, 사전대응 역량을 평가하는 지표 중심으로 구성되어 있다는 점이다.

최근 진행되었던 GCI 버전4의 질의서 항목에는 침해사고 대응 기관 및 책임 기관의 존재 여부, 사이버보안 역량 강화 활동에 대한 국가적 지원 여부 등 침해사고가 발생했을 때 대응할 수 있는 기관 및 정책의 유무 등을 포괄적으로 평가하였다.

GCI의 5가지 필러 각 분야에 대한 평가를 통해 사전 대응능력을 향상시키는 효과는 있을 수 있지만, 포괄적으로 구성된 평가지표는 실제 사이버보안 위협이 발생하였을 때 실제로 시행되는 대응책의 적용 여부와 그 효과에 대한 사후대응 측면의 역량을 정확하게 측정할 수 없다는 약점이 존재한다.

셋째, GCI의 기회 요인으로 대다수의 개도국은 사이버보안에 대한 인식 및 인적, 물적 자원이 부족한 관계로 GCI에 대한 의존도가 매우 높다는 점이다. GCI는 국제적 협력 관계를 기반으로 사이버보안에 대한 입법, 규제 및 기술 분야 등의 지침을 마련하고, 사이버보안 환경 개선을 위해 어떠한 문제가 중요하고 개선되어야 하는지 등 개도국에 대한 사이버보안 인식 개선과 대응역량의 강화에 도움을 주고 있다. 이러한 GCI의 긍정적인 역할은 개도국과 선진국의 보안수준 차를 줄이고, 나아가 온라인을 통해 글로벌 차원의 전자거래가 활성화되도록 할 수 있으며, 전 세계 국가가 GCI 평가를 통해 글로벌 통신망 안전성이 향상되고 사이버 공간의 안전성을 높일 수 있어 디지털 경제, 사이버 공간 신뢰성을 높일 수 있다.

넷째, GCI의 위협 요인으로 4차 산업혁명 기술 중심의 디지털 시대로의 발전에 따른 전 세계 국가의 밀접한 연결로 인해 ICT 기술과 디지털 인프라에 대한 의존도가 점점 높아지고 있다는 점이다.

이러한 상호 연결성뿐만 아니라, 기술의 발전 및 융합이 가속화되면서 국가와 지역 단위를 넘어 국제적 공조의 수준에서 관리해야 하는 새로운 보안 위협과 취약점이 날로 증가하고 있다. 이는 곧 사이버 분야에 대한 단 한 번의 공격만으로도 치명적인 피해가 발생할 수 있음을 의미하며, 각 국가는 새롭게 생성되는 위협에 대한 심각성의 인식과 적극적인 대응책의 마련에 노력해야 할 것이다.

3.2.2 GCI 지표개선을 위한 전략

앞에서 먼저 살펴본 GCI SWOT 여건 분석을 통해 GCI의 강점과 약점, 기회와 위협 요인에 대하여 알아보았다. 이번에는 이를 바탕으로 하여 각 요인별 크로스 SWOT 분석을 통한 교차 분석(강점×기회/강점×위협, 약점×기회/약점×위협)을 실시하고, 그 결과를 바탕으로 GCI 지표개선을 위한 전략의 기본 방향을 도출하고자 한다.

첫째, GCI의 강점과 기회의 크로스 SWOT 분석을 통해 외부의 기회를 활용하여 내부의 강점을 극대화시킬 수 있는 방법을 알아보자.

앞에서 알아본 바와 같이 GCI의 강점은 5가지 필러에 대하여 사이버보안에 대한 대비와 보호 및 사전대응 능력을 평가하는 지표로 구성되어 있어 국가의 사이버보안 위협에 대한 준비성을 검토 및 보완할 수 있도록 한다는 점이다. 이와 함께 GCI의 기회 요인으로는 개도국에 대한 사이버보안 인식 개선에 지속적으로 기여하고, 해당 국가의 사이버보안 역량을 강화하는 데 큰 도움이 되고 있다는 점이다.

이러한 GCI의 강점과 기회 요인의 교차 분석을 통해 개도국에서의 GCI 평가 필요성이 더욱 크게 부각 될 것이며, 개도국에서의 사이버보안 인식 제고와 대응체계의 구축과 발전에 있어 하나의 표준화된 모델로서 적용되어 긍정적인 역할을 수행할 수 있을 것으로 판단된다.

둘째, 외부의 위협을 피해 내부의 강점을 최대한 부각시킬 수 있는 방법을 알아보기 위해 GCI의 강점과 외부의 위협 요인에 대한 크로스 SWOT 분석을 실시하였다.

GCI 평가는 사이버보안 역량의 5가지 필러에 대한 체계화된 지표로 구성되어 있어 사이버보안 위협 대응에 대한 준비성을 검토하고 보완할 수 있는 강점을 지니고 있다는 점과 다양한 사이버위협과 공격이 증가하고 있다는 외부의 위협 요인을 크로스 SWOT 분석을 통해 알아보았다. 이를 통해 증가하는 사이버보안 위협과 공격에 대응할 수 있는 보다 체계화되고 세분된 새로운 평가지표의 개발이 필요하다는 개선 방향을 도출할 수 있다.

셋째, GCI 평가의 약점으로 인해 외부의 기회를 놓치지 않기 위한 대책에 대하여 알아보자. 다시 말해 내부의 약점을 보완하여 외부의 기회를 살릴 수 있는 방안을 찾아보자.

GCI의 약점으로는 앞서 살펴본 바와 같이 사전대응 측면의 포괄적 평가를 꼽을 수 있으며, GCI의 기회 요인으로는 개도국의 사이버보안 인식 개선과 사이버보안 역량 강화에 지속적으로 기여한다는 점을 들 수 있다. 위와 같은 GCI의 약점과 기회 요인에 대한 크로스 SWOT 분석을 통해 기존 지표의 평가대상을 국가 또는 기업 단위로 구체화하고, 사전대응 측면 역량의 효과를 높일 수 있는 세부적인 신규 지표를 새롭게 개발하여, 개도국과 선진국의 보안수준 차를 줄이고, 나아가 전 세계 안전한 온라인 거래의 활성화에 크게 기여할 수 있을 것이다.

넷째, 내부의 약점과 위협으로 인해 올 수 있는 최악의 사태를 피하기 위한 방법에 대해 알아보자. 이를 위해 내부의 약점과 외부의 위협에 대한 크로스 SWOT 분석을 실시하였다.

외부의 위협을 피하고 약점을 극복하기 위한 전략으로서 다양하고 가속화되는 사이버 보안공격의 증가에 효과적으로 대응하기 위하여, 포괄적이고 사전대응 위주의 GCI 평가 프레임워크와 지표를 더욱 구체화하여 세분화하고, 사전대응 중심에서 사후대응 측면의 새로운 지표를 개발하고 적용하여야 할 것이다. 다시 말해 국가별 구체적인 대응능력을 평가하는 프레임워크 개발 및 장기적인 관점의 지표 구성이 필요하며, 사후대응 지표의 개발과 적용 등을 통해 GCI 평가의 효과를 더욱 강화할 수 있을 것이다.

3.3 국가사이버안보지수(NCSI)와의 비교

이번 절에서는 GCI와 NCSI와의 비교분석을 통해, GCI의 보완점과 개선점을 찾고 GCI 평가체계 발전을 위한 개선 방안을 도출하고자 한다.

국가의 사이버보안 대응능력을 평가하는 또 다른 지수로 국가사이버안보지수(National Cyber Security Index, NCSI)가 있다. GCI는 국제기구인 ITU에서 주관하여 전 세계 국가들에 대한 사이버보안 성숙도 수준을 평가하고 발표하는 반면, NCSI는 에스토니아의 eGA(e-Governance Academy Foundation)에서 주관하여 국가별 사이버보안 성숙도 수준을 평가하고, 그 결과를 발표하고 있어 그 적용의 대상이나 신뢰성에서 차이가 있다.

ITU의 GCI는 각 국가별 사이버보안 대응역량에 대해 정기적으로 평가를 실시하고 그 결과를 발표하고 있는 반면, NCSI는 정기적, 연례적으로 평가를 시행하지 않고, 수시 자료수집과 평가를 거쳐 해당 웹사이트(https://ncsi.ega.ee/ncsi-index/)를 통해 그 결과를 발표하고 있다. GCI는 5개 필러에 대한 사이버보안 대응 역량을 평가하고, NCSI는 3 영역(categories), 12 역량(capacities), 46 지표

Table 2. NCSI Structure (3 Categories and their associated 12 capacities for NCSI) (adapted from [12])

Category \ Capacity				
General cyber security indicators	Cyber security policy development	Cyber threat analysis and information	Education and professional development	Contribution to global cyber services
Baseline cyber security indicators	Protection of digital services	Protection of essential services	E-identification and trust services	Protection of personal data
Incident & crisis management indicators	Cyber incidents response	Cyber crisis management	Fight against cyber crime	Military cyber operations

(indicators)에 대한 평가결과를 100점 만점으로 발표한다. NCSI의 평가 구조는 〔표 2〕와 같다.

아래 〔표 3〕은 GCI와 NCSI를 비교하여 나타낸 도표이다.

GCI와 NCSI는 데이터 검증에 대한 접근 방식이 비슷하지만, 지표와 평가 시스템이 다르다. 여기서 눈여겨볼 사항은 NCSI의 지표 중에는 정책 현황의 유무뿐만 아니라 해당 정책이 잘 이뤄지고 있는지를 사후 평가하는 지표가 있다는 점이다, 아래 〔표 4〕에서는 NCSI의 사이버보안 대응역량평가 지표 중 사후 평가에 해당하는 지표를 선별하여 표기하였다.

〔표 4〕의 지표는 일정 기간 해당 정책이 얼마나 시행되었는지를 판단하여 해당 국가의 정책들이 잘 이행되고 있는지를 평가할 수 있다는 장점이 있다. 이뿐만 아니라 NCSI는 교육 및 전문성 개발 지표 중 청소년, 학사, 석사, 박사, 전문가 등 평가 분야를 세부적으로 나누어 평가하였다는 특징을 갖고 있다.

위에서 제시된 NCSI의 사후대응 측면의 지표를 참고하고, 향후 CGI 평가지표에 대한 반영을 통해 사전대응 지표 중심으로 구성된 CGI의 약점을 보완하고 효과성을 더욱 강화할 수 있을 것으로 판단된다. 또한, CGI에 적용할 구체적인 사후대응 지표에 대해서는 면밀한 검토를 통해 CGI의 효과성을 극대화할 수 있는 지표를 개발하여야 할 것이다. 아울러, CGI 버전 5부터의 적용을 통해 장기적인 관점에서 CGI 평가체계를 더욱 강화하고 점진적으로 개선해 나갈 수 있을 것이다.

결론적으로, CGI와 NCSI는 저마다 평가 항목과 방법에 차이가 있고 서로의 강점이 존재하기 때문에, 서로의 강·약점을 분석하고 NCSI의 강점을 CGI에 적용하고 CGI의 약점을 보완하는 과정이 필요하다. 이를 통해 국가의 사이버보안 대응능력을 평가하는 CGI 평가를 좀 더 체계적이고 효과적으로 발전시킬 수 있을 것이다.

Table 3. Comparison between GCI V4 and NCSI

Category	GCI	NCSI
Publication Agency	ITU	eGA
Evaluation period	Every 2 years	Non Regular
Number of Pillar (Category)	5	12
Number of Indicators	82	46

Table 4. NCSI Indicators related to reactive indicators〔12〕.

Indicators	Description of indicators
National-level cyber crisis management exercise	The government has conducted a national-level cyber crisis management exercise or a crisis management exercise with a cyber component in the last 3 years.
Participation in international cyber crisis exercises	The country's team has participated in an international cyber crisis management exercise in the last 3 years.
Regular monitoring of security measures	Operators of essential services must regularly (at least once every 3 years) provide evidence of the effective implementation of cyber/information security policies (e.g. audit result, documentation, specific report).
Cyber security capacity building for other countries	The country has (co-)financed or (co-)organized at least one capacity building project for another country in the last 3 years.
Cyber operations exercise	Military forces have conducted a cyber operations exercise or an exercise with a cyber operations component in the country in the last 3 years.
Participation in international cyber exercises	The country's military team has participated in an international cyber operations exercise in the last 3 years.

IV. GCI 효과 강화를 위한 신규 지표 제안

이번 장에서는 GCI 발전을 위한 구체적인 방법과 내용에 대해서 알아보고자 한다. 앞서 언급한 것처럼

기존 GCI(버전4 기준)는 5개 필러에 82개 평가지표를 제시하여 각 국가가 사이버보안 대응역량을 구축하도록 하는 것에 강점을 가진다. 그러나 이는 사전대응 위주의 지표로 구성되어 있어 실제 사이버위협이 발생했을 때 실질적인 대응역량과 효과성을 측정하는 것에 어려움이 있다.

이에, 실질적인 사이버보안 대응역량을 평가할 수 있는 프레임워크를 제안하고 장기적인 지표(로드맵)를 구성하여야 한다. 그리고 사전·사후 대응역량을 평가하는 세부적인 지표 개발 및 모의 평가 등 국가별 사이버보안 대응력을 세부적으로 측정하는 신규 지표를 제안하여 GCI가 가지고 있는 기존의 강점은 강화하고 약점을 보완해야 한다.

다시 말하자면 포괄적으로 구성된 사전대응 위주의 기존 지표를 구체화하고, 사후대응능력을 측정할 수 있는 새로운 지표를 개발하여 적용하는 것이 효과적일 것이다.

또한, 이를 위해서는 가장 우선적으로 고려하고 지켜져야 할 기본원칙이 필요하며, 이에 대해 아래 7가지 원칙을 제시한다. 다시 말해, 기존 GCI 평가지표에 대한 강점들을 강화하고 약점을 보완하기 위해서는 다음 기본원칙을 준수하여야 한다[1].

본 논문에서 제시한 원칙들은 ITU-T X.1208(정보통신기술의 이용에 있어서 신뢰와 보안을 향상하기 위한 사이버보안 지표)[19]에서 정의된 일반 원칙을 활용하였다. X.1208에서 정의된 원칙은 조직에 대한 사이버보안 향상을 위한 지표의 원칙이 제시되어 있으며, 조직 단위의 지표를 국가 단위의 지표로 적용 가능하므로, 본 논문에서 이 원칙을 적용했다.

이 원칙들은 앞으로 본 논문에서 제시하고자 하는 GCI의 새로운 지표를 도출하는 데 있어서 정확성, 객관성과 타당성을 확보하기 위하여 우선적으로 고려되어야 한다.

첫째, 조직에 대한 사이버보안 지표를 계산할 때 국제 표준에 정의된 지표 세트를 사용하는 것이 우선되어야 한다.

둘째, 사이버보안 지표는 국가의 사이버보안 사전준비태세를 측정할 뿐만이 아니라, 사후의 위협에 대한 사이버보안 대응역량의 현황을 측정해야 한다.

셋째, 사이버보안 지표는 위험에 대한 사이버보안 지표의 계산을 위한 기초로 수집되고 사용되는 원시 데이터의 정확성과 보관 및 전송되는 원시 데이터의 기밀성이 유지되어야 한다.

넷째, 수집 프로세스는 위험에 대한 사이버보안 지표 계산의 기초로 사용되는 원시 데이터의 무결성을 유지해야 한다.

다섯째, 정책 입안자들이 사이버보안 프로그램의 효과성을 측정하고 진행 상황을 점검하는 데 도움이 될 수 있도록 세부 지표가 구성되어야 한다.

여섯째, 빠르게 변화하는 ICT 서비스 및 기술에 대응하여 새로운 추가 지표를 개발하거나 기존 지표를 적시에 업데이트해야 한다.

일곱째, 추가적인 측정 센서의 설치 없이 회원국으로부터 신뢰성 있는 데이터를 모을 수 있는 사후대응 지표를 선정한다.

이상과 같은 GCI 발전을 위한 기본원칙을 바탕으로 하여 GCI 발전의 방법으로 크게 다음 두 가지를 제시한다.

첫째, 현재의 GCI 평가지표 중 사전대응 평가지표에 대한 세부적 항목의 도출과 개선이 필요하다. 둘째, GCI에서 부족한 사후대응 평가지표에 대한 도출과 향후 적용이 필요할 것이다.

이에 4.1절에서는 사전대응을 위한 세부적인 신규 지표를 새롭게 도출하여 제안하고, 4.2절에서 사후대응을 위한 신규 지표를 새롭게 도출하고 제안한다. 사전 대응을 위해 제안하는 14가지 지표는 국내 스터디그룹의 전문가들이 수차례 회의를 거쳐 확정한 지표이며, 사후대응을 위해 새롭게 도출하여 제안하는 신규 지표는 X.1208[19]에서 제시된 조직 단위의 지표 중에서 국가 단위의 지표를 선정하여 변환한 것이다.

이를 통해 앞에서 언급한 GCI의 문제점, 발전 방향 및 신규 지표 도출의 기본원칙을 기준으로 기존의 GCI 지표에 대한 실질적인 문제점을 해결하고자 하며, 또한 앞으로 이루어질 향후 GCI 평가에 대한 개선된 지표를 적용함으로써 국가적 차원의 사이버보안 능력을 실질적·세부적으로 발전시키고자 한다.

4.1 사전대응을 위한 신규 지표 제안

본 장에서는 앞의 SWOT 분석 등을 통해 도출한 사이버보안 사전준비태세 측면의 문제점을 보완한 14개의 신규 지표를 제안한다.

본 절에서 제안된 사전 대응지표를 도출하는 연구방법으로는 미래 결과를 예측하고 정책대안을 제시하는 데 대표적으로 사용되고 있는 "델파이 기법[20]"

을 응용하여 본 논문에서 선정한 “일부 수정된 델파이 기법”을 적용하였다. 먼저 국내의 환경에 적합한 신규 GCI 지표를 발굴하고 설문지를 개발하였고, 이를 국내 GCI 전문가들을 대상으로 설문 조사를 실시하였다. 설문대상 국내 GCI 전문가로는 TTA (한국정보통신기술협회), KISDI(정보통신정책연구원), 현대오토에버 등 ITU-T SG17 국내 연구반 사이버보안 표준 전문가 8명을 선정하였다. 설문 조사 결과를 근거로 우리나라의 법, 제도, 규제 등을 고려하여, 전문가 상호 간 의견교환과 협의와 조정을 거쳐 신규 지표(13개)를 최종 선정하였다[1], 이후, 본 논문의 지속적인 연구 과정에서 1개의 신규 지표를 추가 도출하여 총 14개의 신규 지표를 아래 [표 5]와 같이 제안한다. 또한, 새롭게 제안된 지표 중 2건(10. 정보보호협회의 존재, 12. 사이버보안 평가 검증 프로그램)의 지표가 ITU의 지표개선 전문가 회의에 기고서로 제출되었고, GCI 버전5의 신규 지표 4.2 및 5.4로 반영되어 본 논문의 효과성을 간접적으로 증명할 수 있었다.

[표 5]는 각 필러(세부분야)별로 제안된 신규 지표와 국내 적용사례를 나타낸다.

Table 5. New indicators in terms of proactive response[1]

No	Pillar (Detailed area)	New Indicators	Example of Domestic application
1	Legal Measures (Is there any cybersecurity regulation related to…)	Are there any regulations on the use of digital signatures in private services and applications?	Digital Signature Act
2	Legal Measures (Is there any cybersecurity regulation related to…)	Are there cybersecurity regulations on identity verification?	Act on Promotion of Information and Communications Network Utilization and Information Protection. (Article 23-3), (Article 23-4)
3	Legal Measures (Is there any cybersecurity regulation related to…)	Are there regulations to improve the reliability of cloud services and protect cloud users?	Act on the development of cloud computing and protection of ITS users (Article 4)
4	Technical Measures (National CERT/CIRT/CSIRT)	Does your country have a technical support to the general public and SMEs?	KISA Small and Medium Business Cyber Security Support Service
5	Technical Measures (National CERT/CIRT/CSIRT)	Does your country have a framework for cybersecurity risk reduction and remediation for incident prevention, detection, response, and recovery?	Kr-CERT/CC Incident Framework
6	Technical Measures (National framework for implementation of cybersecurity standards)	Does your country have a framework of public/private partnerships exist to develop cybersecurity standards?	ICT Standardization Forum
7	Organizational Measures (National Cybersecurity Strategy)	Does your country have a cyber national strategy for each sector, such as government sector, finance sector, and ICT sector?	Cybersecurity national strategy by sector of each government department
8	Capacity Development (Public cybersecurity awareness campaigns)	Does your country have public awareness campaigns for youth?	Public awareness campaign through university club support project

9	Capacity Development (Public cybersecurity awareness campaigns)	Does your country have a designated information security day for awareness raising?	Second Wednesday in July(information security day)
10	Capacity Development (Public cybersecurity awareness campaigns)	Does your country have the information security industry association?	Information Security Industry Association
11	Capacity Development (Are there any government incentive mechanisms in place...)	Is there a bug bounty program for hardware/software vulnerabilities?	KISA bug bounty system
12	Capacity Development (Research and development programs)	Does your country have an evaluation program for cybersecurity products?	Information protection product evaluation and certification system
13	Cooperative Measures (Bilateral agreements on cybersecurity cooperation with other countries)	Does your country have a SPAM response as part of the agreement?	SPAM response agreements in major countries
14	Cooperative Measures (Developing country cooperation)	Does your country have a cybersecurity cooperation programs for developing countries?	Cybersecurity Support Program in Developing Countries

〔표 5〕에서 제시한 각 항목(1~14)에 대한 선정 타당성은 아래와 같다〔1〕.

(1) 민간 서비스와 응용에서 디지털서명 사용 규제가 있는가?
⇨ 온라인 거래에서의 신뢰성 확보 및 개선

(2) 본인확인에 대한 사이버보안 규제가 있는가?
⇨ 온라인에서 이용자의 신원확인 신뢰성 개선

(3) 클라우드 서비스의 신뢰성을 향상하고 서비스 이용자 보호를 위한 규제가 있는가?
⇨ 클라우드 서비스의 신뢰성 개선

(4) 일반 시민과 SME에게 기술적 지원을 제공하는가? ⇨ SME 사이버보안 대응능력 향상

(5) 침해사고 예방, 발견, 대응 및 복구를 포함하는 사이버보안 위협을 감소, 치료하는 등의 프레임워크가 있는가? ⇨ 사이버보안 대응능력 향상

(6) 공공/민간 분야의 사이버보안 표준을 공동 개발하는 협력 프레임워크가 존재하는가?
⇨ 사이버보안 표준품질 향상 및 활용 가능성 향상

(7) 전체 분야(정부, 금융, ICT 등)에 대한 분야별 사이버보안에 대한 국가의 전략이 있는가?
⇨ 국가 차원의 사이버보안 대응능력 향상

(8) 청소년을 위한 공공인식 제고 캠페인이 존재하는가?
⇨ 청소년의 사이버보안 인식 제고

(9) 인식 제고를 위한 지정된 정보보호의 날이 존재하는가? ⇨ 사이버보안 인식 제고

(10) 정보보호 산업협회가 있는가?
⇨ 사이버보안 기술적 역량 향상

(11) 하드웨어와 소프트웨어의 취약점 발견에 대한 보상프로그램이 있는가?
⇨ 하드웨어/소프트웨어 취약성 제거

(12) 사이버보안 제품에 대한 평가프로그램이 있는가?
⇨ 사이버보안 제품의 신뢰성 향상

(13) 협약의 일부분으로 SPAM 대응이 있는가?
⇨ SPAM 대응능력 향상

(14) 개도국과의 사이버보안 분야 협력 프로그램이 있는가? ⇨ 글로벌 사이버보안 수준 향상

위와 같이 각 항목별로 알아본 선정 타당성을 통해, 제안된 사전대응 측면의 신규 지표가 GCI의 효과를 실질적으로 향상시킬 수 있음을 알 수 있다. 향후, GCI의 평가지표 구성에 있어 제안된 신규 지표를 우선순위에 따라 적용하고, 장기적 관점에서 개선, 발전시킨다면 GCI 평가의 효과성을 크게 향상시킬 수 있을 것이다.

4.2 사후대응을 위한 신규 지표 제안

GCI 평가의 효과성 향상을 위해서는 사전대응 측면의 평가지표와 함께 사후대응 측면의 평가지표가

강화되어야 한다. 해킹, 개인정보 유출 등 침해사고 발생을 대비한 대응책이 실제로 얼마나 적용되고 있는지를 평가해야 실질적인 사이버보안 대응역량의 평가가 가능하다. 예를 들어 민간 차원에서의 인증서 존재 여부를 평가하는 것이 아니라, 전체 국민 중 몇 %의 국민이 실제로 인증서를 사용하는지를 평가하는 등 실제 적용되고 있는 사후대응 측면의 지표를 수치화하여 평가하는 것이 필요하다.

본 논문에서는 사후대응 측면의 역량 평가를 위한 새로운 평가지표 10개를 〔표 6〕와 같이 제안한다.

Table 6. Newly proposed reactive indicators

No.	Pillar (Detailed area)	Reactive indicators	How to measure the indicators
1	Legal Measures (Is there any cybersecurity regulation related to…)	Does your country have a personal data/privacy protection?	Number of companies with ISMS certification per million population
2	Legal Measures (Cybercrime substantive law)	Does your country have substantive law on illegal access on devices, computer systems and data?	Number of companies with firewalls and IDS installation with more than a certain sales amount.
3	Legal Measures (Is there any cybersecurity regulation related to…)	How many individuals in your country are using digital certificates for government services and applications?	Percentage of digital signature certificates issued per million population
4	Legal Measures (Cybercrime substantive law)	How many organizations are using SSL digital signature certificate for end-to-end communications	SSL certificate issuance rate per million population
5	Technical Measures (National CERT/CIRT/CSIRT)	Does your country have a National/Government CIRT, CSIRT or CERT?	Ratio of incident response teams in the public domain per million population
6	Legal Measures (Is there any cybersecurity regulation related to…)	How many organizations in your country are designated as a national critical infrastructures ?	Number of designated major information and communications infrastructure per million population
7	Capacity Development (Public cybersecurity awareness campaigns)	Does your country have a public cybersecurity awareness campaigns targeting SMEs, private sector companies and government agencies〔1〕?	Ratio of operation of cybersecurity awareness raising programs (including public relations activities, campaigns, educational lectures, etc) in educational institutions
8	Technical Measures (National CERT/CIRT/CSIRT)	Does your country have a certification scheme for cybersecurity products?	Percentage of CC-certified products among information security products
9	Legal Measures (Is there any cybersecurity regulation related to…)	How many public organizations are operating cybersecurity audit program?	Ratio of cybersecurity audit program operation among all public organizations
10	Capacity Development (Are there any government incentive mechanisms in place…)	Does your country have incentive programs for strengthening cybersecurity development capability?	Ratio of internationally accepted information security certifications per million population

〔표 6〕은 각 필러와 사후대응 측면 10개의 신규 지표 및 구체적 평가방법을 나타내고 있다. 새롭게 제안한 10개의 사후대응 지표에 대한 선정 타당성은 다음과 같다.

(1) 인구 100만 명당 ISMS 인증을 받은 기업의 수
⇨ ISMS 인증 체계가 포괄적인 기업의 보안수준을 제고하기 때문에, ISMS 인증을 받은 기업이 많다면 해당 국가의 사이버보안 대응능력이 높다고 평가된다.
(2) 일정 매출액(예:년 매출 100억 원) 이상의 기업에 대한 방화벽 및 IDS 설치 기업의 수
⇨ firewall 또는 IDS 설치 수치는 기업의 네트워크 차원의 접근통제가 얼마나 잘 이뤄지는지 측정할 수 있으므로 기업의 사이버보안 대응능력을 평가할 수 있다.
(3) 인구 100만 명당 전자서명용 인증서 발급비율
⇨ 전자서명 인증서를 발급하는 비율이 높을수록 인증 능력이 높아 사이버보안 능력이 높아진다.
(4) 인구 100만 명당 SSL 인증서 발급비율
⇨ 데이터 전송 시 종단 간 암호 채널을 통해 정보를 보호하므로 사이버보안 수준이 높아진다.
(5) 인구 100만 명당 공공영역 침해사고 대응팀 비율
⇨ 국가의 공공기관 침해사고 대응팀 보유량을 확인하여 국가 차원의 침해사고 대응에 대한 실질적인 사이버보안 대응 준비가 얼마나 되었는지 보여주는 지표가 된다
(6) 인구 100만 명당 주요 정보통신기반시설 지정 수
⇨ 국가시설 중 주요 정보통신기반시설 지정 현황을 통해 국가 차원의 사이버보안 준비태세 확립을 측정할 수 있다.
(7) 국내 초, 중, 고등학교 및 대학을 포함한 교육기관에서의 사이버보안 인식 제고 프로그램(홍보활동, 캠페인, 교육 강연 등 포함) 운영 비율
⇨ 청소년 세대부터의 사이버보안 교육을 통해 전문가를 양성하고, 사이버보안 인식을 개선할 수 있어 사이버보안 대응역량을 강화할 수 있다.
(8) 정보보호 제품 중 CC 인증을 받은 제품 목록의 비율
⇨ 인증 또는 평가를 받은 제품이 많을수록 전반적 정보보호 제품의 안정성 및 신뢰성이 높아진다.
(9) 전체 공공기관 중 사이버보안 감사 프로그램 운영 비율
⇨ 보안 감사를 통해서 미흡했던 사항을 탐색하고 보안 취약점을 찾아 사전에 보안 조치를 취함으로써 조직의 사이버보안 대응능력을 높이다.
(10) 인구 100만 명당 국제통용 정보보호 자격증 보유 비율
⇨ 정보보호 자격증 보유자가 많을수록 사이버보안에 대한 인식, 전문성, 역량 등이 높아지고, 국민의 사이버보안 수준이 높아진다.

본 논문에서 제시한 사후대응 지표는 ITU-T X.1208〔19〕에서 표준화된 조직 단위의 사이버보안 수준 지표를 국가 단위의 사이버보안 지표로 변환한 결과이다. 이에 대한 반영은 ITU 전문가 그룹의 참여를 통해 향후 반영이 필요하다.

4.3 제안된 신규 지표의 기대효과

앞에서 제시한 바와 같이 기존의 GCI 평가지표는 사전대응 측면의 포괄적인 지표 위주로 구성되어 있어 실제 시행되고 있는 세부적 분야의 평가가 힘든 부분이 있었다. 이러한 문제점을 개선하고 GCI평가의 효과를 향상시키기 위하여 본 논문에서는 크게 두 가지 측면의 발전 방안을 제안하였다.

첫째, 기존 지표보다 좀 더 구체화되고 세분화된 사전대응 측면의 신규 지표 14개를 새롭게 제안하였다. 제안된 지표를 통해 평가 분야를 좀 더 세분화하고 보다 깊이 있게 평가할 수 있다. 예를 들어 법적 조치의 경우, 기존 평가지표가 실체법의 유무를 중심으로 평가하는 반면 디지털 서명사용 규제, 본인확인에 대한 규제, 클라우드 이용자 보호 규제 등에 대해 더욱 세부적인 신규 지표를 제시함으로써 정확하고 깊이 있는 평가가 이루어지도록 하였다.

두 번째로 GCI의 기존 지표가 사전대응 위주의 지표로 구성되어 실제 적용되고 시행되는 사이버보안 역량에 대한 평가가 부족하다는 문제를 해결하기 위해 사후대응 측면의 신규 지표 10개를 제안하였다. 제안된 신규 지표에는 ISMS 인증 기업 수, 전자서명용 인증서 및 SSL 인증서 발급비율, 침해사고 대응팀 비율 및 CC 인증 제품 비율 등 사이버보안 대응역량을 강화하기 위해 실제 적용되어 시행되고 있는 사항들을 구체적으로 평가할 수 있다.

아울러, 본 논문에서 제안한 두 가지 측면의 신규 지표를 통해 사전대응 측면과 사후대응 측면을 모두

고려한 보다 종합적이고 정확한 평가가 이루어질 수 있을 것이며, 향후 국가의 사이버보안 대응 정책과 체계를 수립하고 발전시키는 데 크게 도움이 될 것이다.

4.4 향후 GCI 평가 향상을 위한 국내 대응방안 총론

지금까지 네 번의 GCI 평가결과에서 세계 주요 국가의 순위는 매 버전마다 크게 변화하고 있다. 예를 들어, 영국의 경우, GCI 버전2에서 12등, GCI 버전3에서 1등, GCI 버전4에서 2등이 되었으며, 리투아니아는 GCI 버전2에서 56등, GCI 버전3에서 4등, GCI 버전4에서 6등이 되었고, 싱가포르는 GCI 버전2에서 1등, GCI 버전3에서 6등, GCI 버전4에서 4등이 되었다. 한국은 GCI 버전1에서 5등, GCI 버전2에서 13등, GCI 버전3에서 15등이 되었고 GCI 버전4에서 4등을 차지했다. 이를 보면 매 평가마다 순위의 변동성이 매우 크며, 어느 국가나 잠시만 노력을 게을리하면 순위가 크게 하락할 가능성이 매우 크다는 것을 알 수 있다.

또한, 2021년 중반부터 ITU에서 준비 작업을 시작한 GCI 버전5의 세부 지표는 과학기술정보통신부만의 활동을 넘어 범부처 영역에 걸쳐있다. 예를 들어, 온라인 아동보호는 여성가족부와 방통위 산하 방송통신심의위원회 활동과 연관되며, 국가기반시설 보호는 국정원과 행안부의 정책과 연관되며, 법률전문가에 대한 사이버보안 인식 제고 활동은 법무부의 활동과 연계된다. GCI 순위 상승을 위해서는 과학기술정보통신부만의 준비 활동으로는 부족할 수 있다. 이에, 국가적 최고 차원의 사이버보안 대응역량에 대한 조정 역할이 필요하다. 다시 말해 GCI 버전4 평가에서 미흡한 지표인 온라인 아동보호의 지표를 개선하기 위해서도 과학기술정보통신부와 관련 정부 부처들과의 긴밀한 협력을 통해 향후 시행되는 GCI 평가에서 높은 점수를 획득해야 할 것이다[1]. 따라서 국가 최고 수준의 사이버보안 콘트롤타워가 조정하는 Task Force를 구성하여 GCI 평가에서 높은 순위를 유지하고 지속적인 향상을 위해 조정과 협력, 평가에 대한 지속적이고 적극적인 대응과 모니터링 활동이 반드시 필요하다. 한편 GCI 평가가 영문 자료만으로 이루어지므로, 주요 국내 정보보호 관련 행사와 제반 사이버보안 활동 자료의 영문화 노력도 필요하다.

V. 결 론

본 논문에서는 2014년부터 ITU에서 격년으로 시행 중인 국가 사이버보안 수준 측정 프로젝트인 GCI를 체계적으로 분석한 후, GCI의 사전대응 능력을 향상시키는 지표 및 사후대응 능력을 평가하는 지표를 추가로 발굴, 제안함으로써 GCI의 지속적인 발전 방향을 제시하고자 하였다.

먼저, 1장 서론에서는 GCI의 효과성을 제고하고 나아가 전 세계 국가의 사이버보안 수준 향상을 도모할 수 있도록 하기 위하여 GCI의 새로운 신규 지표를 도출하고 제안하고자 하는 본 논문의 목적을 명확히 제시하였다.

2장에서는 GCI 평가의 프레임워크를 제시하고 지금까지 시행되었던 GCI 버전1~버전4 평가를 검토 후 그 결과(2014~2021)를 분석하여 기술하였다.

3장에서는 GCI 지표개선 전략 및 NCSI와의 비교분석을 실시하였다. GCI 지표에 대한 SWOT 분석을 실시하였고, 아울러 NCSI 지수와의 비교를 통해 GCI의 약점 보완 및 강점 강화를 위한 GCI 개선 방안으로서 사전 대응능력을 평가하는 지표를 더욱 세분화하고, 사후대응 능력을 평가하는 지표가 추가적으로 필요함을 제시하였다.

4장에서는 GCI 효과성을 강화하기 위한 기본원칙을 제시하고 사전대응 측면에서의 14개의 신규 지표와 사후대응 측면에서의 신규 지표 10가지를 도출하고 제안하였다. 아울러, 이를 통한 효과성을 언급하였다.

이와 같이 본 논문에서는 GCI의 사전대응 지표를 보완 제시하고 사후대응을 위한 신규 지표를 추가적으로 개발하여 제안함으로써 GCI 평가체계를 더욱 개선 발전시키고자 하였다.

GCI 지표개선에 있어서는 특히 ITU-D SG2 Q3의 전문가 그룹과 GCI 가중치 전문가 위원회에 지속적으로 참여해 GCI 자체의 발전을 위한 세부 신규 지표를 도출하고 세부 가중치를 반영할 예정이다. 또한, 본 논문을 통해 구축된 국내외 협력 네트워크를 지속적으로 활용하여 GCI를 통한 사이버보안 역량의 꾸준한 향상을 도모할 예정이다.

추후 연구로서 실증 연구를 국내 실정을 반영해 추진할 필요가 있다. 또한, 향후 연구과제로 본 논문에서 제시된 신규 사전대응 및 사후대응 지표를 GCI 버전6를 위한 지표개선 전문가 그룹에 적극적으로 참여하여 반영할 계획이다. 이를 위한 향후 전

략으로 GCI 버전6 지표개선 및 각 지표의 가중치 산정 ITU 전문가 그룹에 적극적으로 참여하여 본 논문에서 제시된 신규 지표를 반영하고, 우리나라가 강점을 갖는 지표가 높은 가중치를 갖도록 ITU 가중치 산정 전문가 그룹에 적극 참여할 예정이다.

References

[1] Heung Youl Youm, Byoung moon Chin, Chan jin Kim and Dong hyen Kim, "A study on the Analysis and Improvement of Global Cybersecurity Index", IITP Project Report(ICT Policy Project: 2020-0-02206), Dec. 2020

[2] Heung Youl Youm, "A Study on Development and Methodology of Globally Standardized Cybersecurity index", Korea Communication Commission, Nov. 2010, https://kcc.go.kr/user.do?mode=view&page=A02160000&dc=K00000001&boardId=1022&boardSeq=31824

[3] Brahima Sanou, "Global Cybersecurity Index & Cyber wellness Profiles Report", ITU Telecommunication Development Bureau, April 2015, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf

[4] Global Cybersecurity Index Conceptual Framework, "GCI Framework", Oct. 10, 2021, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCI_Conceptual_Framework.pdf

[5] Brahima Sanou, "Global Cybersecurity Index Information Letter", ITU Telecommunication Development Bureau, Oct. 2013, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Global_Cybersecurity_Index_DM365_Signed.pdf

[6] Brahima Sanou, "Global Cybersecurity Index (GCI) 2017", July 2017, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

[7] Global Cybersecurity Index (GCI) 2015 /16 Questionnaire Guide, "GCI 2015", Oct. 10, 2021, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/QuestionnaireGuide-E.pdf

[8] Global Cybersecurity Index(GCI) 2018, "GCI 2018", Oct. 10, 2021, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

[9] Doreen Bogdan-Martin, "Global Cybersecurity Index 2020", ITU Telecommunication Development Bureau, 2021, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

[10] V. M. Kravets, "Comparative Analysis of the Cybersecurity Indices and Their Applications", Cybersecurity state compliances, Vol. 1 No. 1, pp. 97-102, May 2019, http://tacs.ipt.kpi.ua/article/view/169090

[11] How much data is generated each day?, "WEF Data" Oct. 10, 2021, https://www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/

[12] National Cyber Security Index(NCSI), "NCSI", Oct. 20, 2021 https://ncsi.ega.ee/ncsi-index/, https://ncsi.ega.ee/country/kr/

[13] GCI scope and framework - ITU, "GCI framework", Oct 10, 2021, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/New_Reference_Model_GCIv4_V2_.pdf

[14] ITU/BDT Cyber Security Programme Global Cybersecurity Index(GCI), Gruidelines for Member States (Version 0.9), "GCI 2019", Oct. 10, 2021, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv4/GCI_V4_Guidelines_for_Member%20States.pdf

[15] Jaemin Song, Arum Park and Sae Bom Lee, "Trend of Technology in Video Surveillance System", Journal of

the Korea Society of Computer and Information, Vol. 25 no. 6, pp. 57-64, June 2020 http://koreascience.or.kr/article/JAKO202018955008640.page

[16] KBS NEWS(Korea ranks 4th in the world in the International Information Security Index, 11 steps up in 2 years). "GCI", June 30, 2021, https://news.kbs.co.kr/news/view.do?ncd=5221876&ref=A

[17] Ministry of Science and ICT(Ranked 4th in the world in Korea International Information Security Index (GCI)), "GCI", June 30, 2021, https://blog.naver.com/with_msip/222415064655

[18] YUN, Jaesuk and Lim, Jong In, "Development and Application of Global Cybersecurity Maturity Index Model", Korea University, Dec. 2016

[19] Recommendation ITU-T X.1208(A cybersecurity indicator of risk to enhance confidence and security in the use of telecommunication/information and communication technologies), "GCI Indicator", Oct 12, 2021 https://www.itu.int/rec/T-REC-X.1208/en

[20] Seungyong Noh, "The Delphi Technique: Forecasting the Future with Expert Insight", Human Settlements Vol. 299 No. 0, pp. 53-62, Korea Research Institute For Human Settlements, Sep. 2006, https://kiss.kstudy.com/thesis/thesis-view.asp?key=2560191

[21] Yong-ju Kang, "Understanding and application of Delphi technique", EDI Report 08-20, Korea Employment Agency for the Disabled, July. 2008, https://edi.kead.or.kr/BoardType02.do?cmd=_view&bid=3&mid=23&idx=424

[22] Kyung-Su Lee, Tae-Hyeong Kim, Tai-Hoon Kim and Sang-Hyuk Park, "Analysis of Risk Factor for Sinkhole Formation by using Delphi", The Journal of the Korea Contents Association Vol.16 No. 4, pp. 65-75, April, 2016

〈저자소개〉

김 대 경 (Dae kyung Kim) 종신회원
1995년 2월: 경성대학교 컴퓨터공학과 학사
2004년 2월: 순천향대학교 정보보호학과 석사
2007년 2월: 순천향대학교 정보보호학과 박사과정(수료)
〈관심 분야〉 정보보호 관리 및 평가체계, 드론 보안, 분산원장기술 보안, 개인정보보호

이 주 현 (Ju hyeon Lee) 학생회원
2022년 2월: 순천향대학교 정보보호학과 학사
2022년 3월: 가천대학교 정보보호학과 석사과정
〈관심 분야〉 분산원장기술 보안, IoT 보안, 네트워크 보안, OT 보안

김 예 영 (Ye young Kim) 학생회원
2019년 3월~현재: 순천향대학교 정보보호학과 학사과정
〈관심 분야〉 IoT 보안, 네트워크 보안, 보안성 평가/인증

현 다 은 (Da eun Hyeon) 학생회원
2019년 3월~현재: 순천향대학교 정보보호학과 학사과정
〈관심 분야〉 정보보호 관리 및 평가체계, 분산원장기술 보안, IoT 보안, 개인정보보호

오 흥 룡 (Heung-Ryong Oh) 종신회원
2002년 2월:순천향대학교 전자공학과 학사
2004년 2월:순천향대학교 정보보호학과 석사
2018년 2월:순천향대학교 정보보호학과 박사
2004년 2월~현재:한국정보통신기술협회 표준화본부 수석연구원
2005년 3월~현재:ITU-T SG17 국내 연구반 간사(역) 및 위원
2009년~2016년:ITU-T SG17 Q2 Associate Rapporteur
2017년~현재:ITU-T SG17 Q2 Co-Rapporteur
2011년~현재:한국정보보호학회 학회지 편집위원
2012년 8월~현재:국방부 국방정보기술표준(DITA) 자문위원
2017년 9월~현재:금융결제원 바이오인증 성능위원회 자문위원
2019년 4월~현재:용인시 지역정보화위원회 자문위원
〈관심 분야〉 보안프로토콜, 정보보호표준

진 병 문 (Byoung moon Chin) 종신회원
1976년 2월 서울대학교 전기공학과 학사
1983년 8월 서울대학교 전자계산기공학과 석사
1996년 2월 KAIST 전산과 박사
1980년 4월~2001년 3월: 한국전자통신연구원 표준연구센터장
2001년 3월~2013년 12월: 한국정보통신기술협회 표준화본부장
2012년 9월~2019년 12월: 순천향대학교 공과대학 정보보호학과 초빙교수
2020년 3월~현재: 순천향대학교 산학협력단 연구교수
2001년 1월~2007년 12월: ITU-T SG 17 부의장
〈관심 분야〉 네트워크 보안, 프로토콜 공학, 정보보호관리체계, 개인정보보호, 5G 보안

염 흥 열 (Heung Youl Youm) 종신회원
1981년 2월: 한양대학교 전자공학과 학사
1983년 9월: 한양대학교 대학원 전자공학과 석사
1990년 2월: 한양대학교 대학원 전자공학과 박사
1982년 12월~1990년 9월: 한국전자통신연구원 선임연구원
1990년 9월~현재: 순천향대학교 공과대학 정보보호학과 정교수
2011년 1월~12월: 한국정보보호학회 회장(역), 명예회장(현재)
2007년 3월~현재: 한국인터넷진흥원 ISMS/PIMS 인증위원회 위원장
2009년~2016년: ITU-T SG17 부의장, ITU-T SG17 WP2/WP3 의장
2017년~현재: ITU-T SG17 의장
2020년 8월~현재: 분산신원증명기술·표준화포럼 의장
〈관심 분야〉 정보보호관리체계, 개인정보보호, IoT 보안, 개인정보영향평가, 암호 프로토콜, 5G 보안, 분산원장기술 보안