Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.4, Aug. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.4.781

보안취약점 협력대응제도(CVD) 도입을 위한 법제화 방안 연구: 정보통신망법 중심으로

이 태 승†‡
한국인터넷진흥원 (연구위원)

A Study on Legislative Approaches for Introducing Coordinated Vulnerability Disclosure(CVD): Focusing on the Information and Communications Network Act

Taeseung Lee†‡
Korea Internet & Security Agency (Chief Researcher)

요 약

최근 미국과 유럽연합은 ICT 제품 및 서비스에 대한 보안취약점 대응 강화를 위하여 화이트해커와의 협력에 기반한 보안취약점 대응체계인 Coordinated Vulnerability Disclosure(CVD)를 제도적으로 도입 및 확산해 나가고 있다. 이러한 사이버보안 변화에 맞춰 본 논문은 CVD를 정보통신망법에 기반하여 도입하는 방안을 3단계 절차로 제안한다. 첫 번째 단계에서는 CVD 법제화 필요성 및 요구사항을 파악하기 위하여 우리나라 현황과 미국, 유럽연합, OECD의 CVD 관련 동향을 조사한다. 두 번째 단계에서는 CVD 법제화 필요성을 분석하고 CVD를 법제화하기 위해 요구되는 사항을 도출한다. 본 논문에서는 CVD 법제화 필요성을 CVD 도입 필요성, 법률에 기반한 제도화 필요성, 법제화 법률로 정보통신망법의 적합성 등 3가지 측면에서 분석하였으며, CVD 법제화 요구사항으로는 보안취약점 처리방침(VDP, Vulnerability Disclosure Policy) 수립 및 공개, 화이트해커 법적 보호, CVD 운영을 위한 조정기관(coordinator) 지정 및 역할 부여를 도출하였다. 세 번째 단계에서는 CVD 법제화 요구사항을 우리나라 민간 분야 침해사고 예방 및 대응에 관한 법률인 정보통신망법에 적용하는 방안을 소개한다.

ABSTRACT

Recently, the US and EU have been institutionally introducing and promoting Coordinated Vulnerability Disclosure(CVD) to strengthen the response to security vulnerabilities in ICT products and services, based on collaboration with white-hat hackers. In response to these changes in cybersecurity, we propose a three-step approach to introduce CVD through the Information and Communications Network Act(ICNA). In the first step, to comprehend the necessity and requirements for legislating CVD, we survey the current situation in Korea and the trends of CVD in the US, EU, and OECD. In the second step, we analyze the necessity for legislating CVD and derive the requirements for its legislation. In this paper, we analyze the necessity for legislating CVD from three perspectives: the need for introducing CVD, the need for institutionalization based on law, and the suitability of the ICNA as the legislation. The derived requirements for CVD legislation include the establishment and publication of Vulnerability Disclosure Policy(VDP), legal protection for white-hat hackers, and designation and role assignments of coordinator. In the third step, we introduce approaches to apply the requirements for CVD legislation to the ICNA, which is the law governing prevention and response to cybersecurity incidents in private sector.

Keywords: Coordinated Vulnerability Disclosure, Vulnerability Disclosure Policy, White-hat Hacker, Good-Faith Security Research

Received(04. 22. 2024), Modified(07. 01. 2024), Accepted(07. 23. 2024)

† 주저자, tseung@kisa.or.kr
‡ 교신저자, tseung@kisa.or.kr(Corresponding author)

I. 서 론

Coordinated Vulnerability Disclosure(이하 "CVD"라 한다)는 Fig. 1.과 같이 화이트해커, ICT 사업자, 조정기관간의 소통·협력·조정에 기반하여, ICT 제품·서비스에 존재하는 보안취약점을 발견, 신고, 조치, 공개하는 보안취약점 대응 프로세스로[1][2][3][4], 최근 미국, 유럽연합, OECD는 법제화 및 국가사이버안보전략 등을 통해 CVD를 도입·확산해 나가고 있다.

CVD가 처음 소개된 시기는 '10.6월로, 베라코드社(Veracode) 최고기술책임자(CTO)인 웰드폰드(WeldPond)가 트위터를 통해 'Responsible Disclosure' 용어가 가지는 책임감에 대한 부담을 완화하기 위해 'Coordinated Disclosure'를 제안하였으며, 같은 해 7월 마이크로소프트社가 CVD 개념을 정립하여 발표하였다[5].

CVD와 많은 우리나라 기업에서 수행 중인 보안취약점 점검, 보안취약점 평가·분석, 소프트웨어 개발보안을 비교하면, 보안취약점을 발견하고 조치하는 목적은 동일하지만, 수행 결정주체, 적용 단계, 공개 측면에서 아래와 같은 차이점이 있다[6].

CVD는 불특정 또는 익명의 화이트해커가 보안취약점 발견 수행 여부를 결정하지만, 정보통신망법 제47조의4, 정보통신기반보호법 제9조, 소프트웨어진흥법 제29조에 따른 취약점 점검, 취약점 분석·평가, 소프트웨어 개발보안은 정부나 사업자가 수행 여부를 결정한다[7][8][9]. 적용 단계 측면에서 CVD는 제품·서비스가 출시된 이후의 운영 단계에서 주로 적용되지만, 소프트웨어 개발보안은 소프트웨어를 개발하는 단계에서 적용되는 차이가 있다. 또한, CVD는 보안취약점 점검, 보안취약점 분석·평가, 소프트웨어 개발보안과는 달리 보안취약점을 공개한다는 측면에서 차이점이 있다[1][2][3][4]. 다른 사업자도 동일한 보안취약점을 보유할 가능성이 있고 다른 누군가에 의해서도 재발견될 수 있으므로[10], CVD는 사업자들이 신속하게 보안취약점을 개선 조치할 수 있도록 보안취약점을 공개한다. 이는 보안취약점 발견에 기여한 화이트해커에게 학회 등에서 자유롭게 발표할 수 있도록 함으로써 CVD에 참여하게 하는 동기를 제공한다[11].

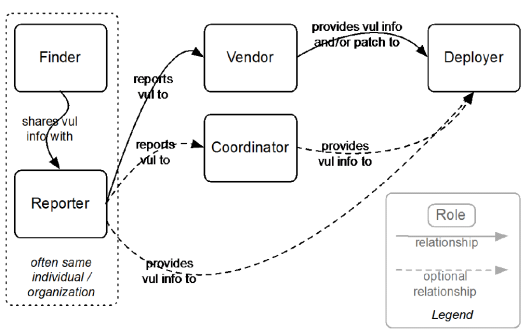


Fig. 1. CVD Role Relations[1]

본 논문은 정보통신망법에 기반한 CVD 법제화 방안을 Fig. 2.과 같이 3단계 절차로 제안한다.

첫 번째 단계에서는 CVD 법제화 필요성과 요구사항을 파악하기 위하여 우리나라 도입 현황과 미국, 유럽연합, OECD의 CVD 동향을 조사한다. 두 번째 단계에서는 CVD 법제화 필요성을 ① CVD 도입 필요성, ② 법률에 기반한 제도화 필요성, ③ 법제화 법률로 정보통신망법의 적합성 등 세 가지 측면에서 분석한다. 또한, CVD 법제화 요구사항으로는 ① CVD 운영 방침인 보안취약점 처리방침(Vulnerability Disclosure Policy, 이하 "VDP"라 한다) 수립·공개, ② 화이트해커 법적 보호, ③ CVD 운영을 위한 조정기관(coordinator) 지정과 역할 부여를 도출한다. 세 번째 단계에서는, 앞서 도출한 CVD 법제화 요구사항을 정보통신망법에 적용하는 방안을 소개한다.

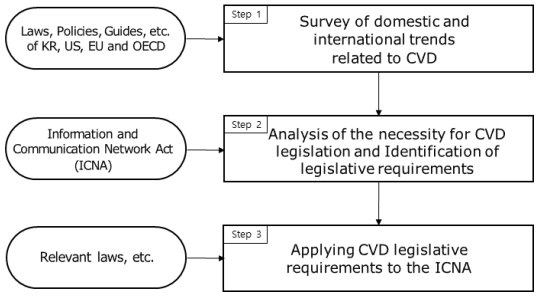


Fig. 2. 3-step approach for legislating CVD based on the ICNA

II. 국내외 CVD 관련 동향

2장에서는 CVD 법제화 필요성과 요구사항을 파악하기 위하여, 우리나라의 도입 현황과 미국, 유럽연합, OECD의 CVD 관련 동향을 법령, 정책, 가이드로 구분하여 조사한다.

2.1 우리나라

우리나라 한국인터넷진흥원은 보안취약점 신고를 촉진하기 위해 2012년부터 보안취약점 신고포상제도를 운영하고 있으며, 국내 기업과의 공동 운영 방식으로 신고 포상을 확대해 나가고 있다[12]. 하지만, 보안취약점 신고포상제도의 법적 근거가 정보통신망법 제47조의6(정보보호 취약점 신고자에 대한 포상)에 따른 포상금 지급에만 기반을 두고 있어, 정보통신망법 제48조(정보통신망 침해행위 등의 금지)에 따른 법적 위험성은 사업자와 화이트해커의 책임 하에 운영되고 있다.

이러한 문제점을 개선하기 위해 최근 학계를 중심으로 CVD 도입 필요성이 제기되고 있다[13][14].

2.2 미국

미국은 법률에 기반하여 연방기관에 대해 CVD 도입을 의무화하고 있으며, 정책·가이드를 통해 민간 분야로 CVD 도입을 확산해 나가고 있다.

연방기관의 경우, 연방정보보안현대화법(FISMA)에 근거하여 연방기관의 CVD 도입을 의무화하고 있으며, 실제로 악용된 보안취약점(known exploited vulnerability) 등에 대해서는 의무적으로 개선 조치를 하도록 규정하고 있다. 또한, 관리예산처(OMB)와 법무부(DOJ)는 화이트해커의 보안취약점 발견 등의 행위가 연방기관의 CVD 운영방침인 VDP를 준수하고 선의의 보안연구(good-faith security research)를 충족할 경우 사이버범죄법 위반에서 제외하는 법적 근거 및 기소 정책을 마련하여 발표하였다.

민간에 대해서는 국가사이버안보전략(NCS), 대통령 행정명령(EO 14028), 시큐어 바이 디자인(Secure by Design), 사이버보안관리체계(CSF 2.0) 등을 통해 CVD 도입을 확산해 나가고 있다.

2.2.1 美 법령

○ 연방정보보안현대화법(FISMA)

미국은 '20년부터 연방기관에 대해 CVD를 시행하고 있다. 이와 관련된 법체계는 '14.12월에 개정된 연방정보보안현대화법(Federal Information Security Modernization Act of 2014, 이하 "FISMA"라 한다)의 제3553조 (b)(2)항에 근거를 두고 있으며[15], 이를 기반으로 관리예산처(OMB)와 사이버보안청(CISA)은 연방기관에게 적용되는 메모랜덤(Memorandum)과 의무지침(BOD, Binding Operational Directive)을 '20년과 '22년에 발표하였다.

관리예산처(OMB)가 발표한 메모랜덤 M-20-32는 연방기관에게 CVD 운영 방침인 VDP의 수립·공개를 의무사항으로 요구하고 있으며, 화이트해커의 보안취약점 발견 등의 행위가 VDP를 준수하고 선의의 보안연구를 충족할 경우, 사이버보안 침해사고(incident) 및 개인정보 위반(breach)이 아님을 명시하고 있다[16].

사이버보안청(CISA)의 의무지침 BOD 20-01은 VDP에 포함될 화이트해커와 연방기관의 준수사항을 명시하고 있으며[17], BOD 19-02와 BOD 22-01은 심각(critical) 또는 실제로 악용된 보안취약점 등과 같이 사이버보안 위험성이 높은 보안취약점에 대해서는 의무적으로 개선 조치를 할 것을 연방기관에게 요구하고 있다[18][19].

○ IoT 사이버보안 강화법(IOTA)

미국은 연방기관에서 사용되는 IoT 기기의 사이버보안 강화를 위해 IoT 사이버보안 강화법(IoT Cybersecurity Improvement Act of 2020, 이하 "IOTA"라 한다)을 '20.12월 제정하였다[20]. 이 법의 제5조 (a)(1)항은 관리예산처(OMB)에게 연방기관의 CVD 도입을 감독할 권한을 부여하고 있으며, 제5조 (a)(1)항에 근거하여 국립표준기술연구소(NIST)는 IoT 기기에 대한 CVD 가이드로 NIST SP 800-216을 '23.5월에 발표하였다[21].

2.2.2 美 전략·정책

○ 美 국가사이버안보전략(NCS)

美 백악관이 '23.3월에 발표한 국가사이버안보전략(National Cybersecurity Strategy, 이하 "NCS"라 한다)의 전략목표 3.3절은 민간 분야 소프트웨어 제품·서비스에 대한 사업자의 책임과 의무를 강화하기 위한 법제화를 추진할 것임을 명시하고 있으며, 안전한 소프트웨어 개발을 장려하기 위해 CVD 도입을 촉진할 것임을 밝히고 있다[22].

국가사이버안보전략 이행을 위해 美 백악관이 '23.7월에 발표한 국가사이버안보전략 이행계획 3.3.3절은 CVD 도입·촉진의 책임기관으로 사이버보안청(CISA)을 지정하였으며, 이행 목표시기를 회계연도로 '25년 4분기로 정하고 있다[23].

국가사이버안보전략 이행 계획에 따라 사이버보안청(CISA)이 '23.8월에 수립한 사이버보안 전략 계획의 1.2절은 민간분야에서의 CVD 도입·확산을 목표로 정하고 있다[24].

○ 제로트러스트 및 소프트웨어 공급망 보안

美 백악관이 국가 사이버안보 강화를 위해 '21.5월에 발표한 대통령 행정명령(EO 14028)의 제3조와 제4조는 연방기관에게 '제로트러스트 아키텍처' 및 '소프트웨어 공급망 보안' 구현을 의무사항으로 요구하고 있다[25].

이를 근거로, 관리예산처(OMB)가 '22.1월에 발표한 메모랜덤 M-22-09는 연방기관의 제로트러스트 아키텍처 구현 요구사항으로 CVD를 요구하고 있으며[26], '22.9월에 발표한 M-22-18('23.6월 M-23-16으로 개정)은 연방기관에게 국가표준기술연구소(NIST)의 공급망보안 가이드를 준수할 것으로 요구하고 있다[27][28]. 또한, 소프트웨어 공급망보안 가이드인 NIST SP 800-218은 공급망보안 구현 요구사항으로 대통령 행정명령(EO 14028)의 제4조 (e)(viii)항에 명시된 CVD를 포함하고 있다[25][29].

○ 시큐어 바이 디자인(Secure by Design)

美 사이버보안청(CISA)이 '23.10월에 발표한 시큐어 바이 디자인(Secure by Design)은 기술 제품 제조사에게 안전한 제품 개발 원칙 중 하나로 VDP의 수립·공개를 요구하고 있다[30].

○ 인공지능 보안(Safe and Secure AI)

美 백악관이 '23.11월에 발표한 대통령 행정명령(EO 14110)은 안전하고(safe, secure) 신뢰할 수(trustworthy) 있는 AI 개발·활용을 요구하고 있으며[31], 이에 기반하여 사이버보안청(CISA)이 '23.11월에 발표한 AI 로드맵의 2.5절은 AI 시스템에 대한 CVD 도입을 목표로 정하고 있다[31][32].

○ 오픈소스 소프트웨어(OSS) 보안

美 국가사이버안보전략 전략목표 4.1절에 근거하여 사이버보안청(CISA)이 '23.9월에 발표한 오픈소스 소프트웨어 보안 로드맵의 4.4절은 오픈소스 소프트웨어 보안 강화 방안으로 관련 오픈소스 커뮤니티와의 협력을 통한 CVD 확산을 목표로 정하고 있다[22][33].

○ 화이트해커 법적 보호

美 법무부(DOJ)는 '22.5월 해킹에 대한 사이버범죄법 (Computer Fraud and Abuse Act, 이하 "CFAA"라 한다)에 대한 기소 정책을 개정·발표하였다[34][35]. 주요 개정사항은 화이트해커의 행위가 선의의 보안연구(good-faith security research)를 충족할 경우 CFAA에 대한 기소에서 제외됨을 명시하고 있다.

美 법무부의 기소 정책에 명시되어 있는 Table 1.의 선의의 보안연구는 보안결함 또는 보안취약점에 대한 시험, 조사, 그리고/또는 교정은 선의의 목적으로만 컴퓨터(기기, 기계, 온라인 서비스)에 접근해야 하며, 다음의 (1)와 (2) 조건을 모두를 충족해야 한다. (1) 개인 또는 국민에게 어떠한 피해를 야기하지 않는 방법으로 수행되어야 한다. (2) 보안연구로 발생되는 정보는 컴퓨터(기기, 기계, 온라인 서비스)와 그 이용자의 보안성 또는 안전성을 개선하는 용도로만 활용되어야 한다.

Table 1. good-faith security research[35]

"good faith security research" means accessing a computer solely for purposes of good faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in a manner designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security of safety of the class of devices, machines, or online services to which the accessed computer belongs, or those who use such devices, machines, or online services.

2.2.3 美 가이드

○ 사이버보안 취약점 대응 플레이북

미국 사이버안보 강화를 위한 대통령 행정명령(EO 14028) 제6조에 기반하여, 사이버보안청(CISA)이 '21.11월에 발표한 '사이버보안 침해사고 및 취약점 대응 플레이북'은 실제로 악용된 보안취약점(actively exploited vulnerability)에 대한 연방기관의 대응 절차를 보안취약점 전주기인 발견, 신고, 조치, 공개에 걸쳐 설명하고 있으며, CISA가 조정기관 역할을 담당하고 있음을 설명하고 있다[25][36].

○ CVD 프로그램

美 사이버보안청(CISA)의 CVD 프로그램은 CVD 조정기관을 미국의 사이버침해대응조직(US-CERT)인 사이버보안청(CISA)이 수행함을 명시하고 있으며, 보안취약점을 조정기관에게 신고하도록 명시하고 있다. 특히, 보안취약점 공개 시기를 보안취약점 관련 사업자와 협의를 통해 정하도록 명시하고 있으며, 사업자의 대응이 없을 경우 보안취약점 정보를 사업자에게 제공한 이후 45일이 경과한 시점을 공개시기로 정하고 있다[2].

○ 사이버보안관리체계(CSF 2.0)

美 국가사이버안보전략의 전략목표 1.1절에 따라 국립표준기술연구소(NIST)가 '24.2월 발표한 사이버보안관리체계(Cybersecurity Framework 2.0)의 관리항목 'ID.RA(위험평가)-8'은 CVD를 요구하고 있다[22][37].

참고로 ID.RA-8은 '18.4월 사이버보안관리체계가 V1.0에서 V1.1로 개정될 때 CVD가 신규로 도입되었으며, V1.1에서 V2.0으로 개정될 때 'RS.AN(침해사고 분석)-5'가 'ID.RA(위험평가)-8'로 변경되었다.

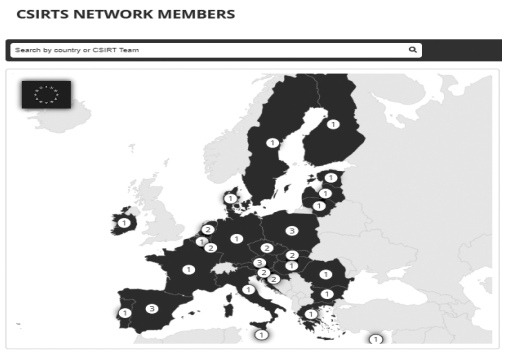
2.3 유럽연합(EU)

최근 유럽연합은 법률에 기반하여 회원국들에게 국가사이버안보전략으로 CVD를 채택할 것을 요구하고 있으며 사업자에게는 보안취약점 신고·조치 등을 의무사항으로 요구하고 있다.

2.3.1 EU 법령

○ 네트워크·정보시스템 보안 개정 지침(NIS2)

유럽연합이 '22.10월에 개정한 네트워크·정보시스템 보안 개정 지침(NIS2)의 제2조와 제3조는 NIS2의 적용 대상을 조직의 규모, 매출액, 중요 분야 등이 고려된 필수(essential)·중요(important) 조직으로 규정하고 있으며, 제7조의 2(c)항은 유럽연합 회원국들에게 CVD를 포함한 보안취약점 정책을 국가사이버안보전략으로 채택할 것을 요구하고 있다. 제12조는 CVD 운영을 수행할 조정기관(coordinator)으로 각 회원국의 침해사고대응조직(CSIRT)을 지정할 것을 규정하고 있으며, 제11조의 5(c)항은 Fig. 3.과 같이 회원국 CSIRT간 CVD 도입·확산을 위한 협력을 요구하고 있다[38][39].



Vulnerability Disclosure Policies

Country	Organisation	Language	CNA	Policy/Reporting
BE	CCB	EN	No	Vulnerability reporting to the CCB (15 February 2023)
BE	CCB	FR	No	Signalement des vulnérabilités au CCB (15 février 2023)
DE	CERT-Bund	DE	No	Leitlinie und Richtlinie für Sicherheitsforschende (Dezember 2022)
DE	CERT-Bund	EN	No	BSI CVD guideline for security researchers (December 2022)
ES	INCIBE-CERT	EN	Yes	Vulnerability disclosure policy
ES	INCIBE-CERT	ES	Yes	CVE Assignment and publication
EU	ENISA	EN	Yes	ENISA Coordinated Vulnerability Disclosure Policy
EUI	CERT-EU	EN	No	Coordinated vulnerability disclosure policy
FI	NCSC-FI	EN	Yes	Vulnerability Coordination and Reporting
FR	ANSSI	FR	No	Vous souhaitez déclarer une faille de sécurité ?
NL	NCSC-NL	EN	Yes	Coordinated Vulnerability Disclosure: the Guideline (02 October 2018)
PL	CERT-PL	EN	Yes	Reporting vulnerabilities to CERT Polska
SK	SK-CERT	EN	Yes	Vulnerability Reporting Guideline (07 October 2019)
LU	CIRCL	EN	No	Responsible Vulnerability Disclosure (October 2019)
LV	CERT-LV	EN	No	Responsible Vulnerability Disclosure (September 2019)

Fig. 3. EU's CSIRTS network for CVD[39]

○ 사이버보안법(CSA)

유럽연합이 '19.4월에 제정한 사이버보안법(Cybersecurity Act, 이하 "CSA"라 한다)의 제6조 1(b)항은 유럽사이버보안청(ENISA)에게 유럽연합 회원국들의 CVD 도입을 지원할 것을 의무사항으로 규정하고 있다[40].

○ 사이버복원력법(CRA)

유럽연합이 '23.11월에 합의하여 '24년 제정 예정인 사이버복원력법(Cyber Resilience Act, 이하 "CRA"라 한다)의 제10조 제6항은 디지털제품 제조사에게 CVD를 의무적으로 도입·운영할 것을 규정하고 있다[41][42].

CRA 제8조는 '24.3월 유럽연합 의회를 통과한 인공지능법[43] 제6조의 제1항 및 제2항에 따라 고위험으로 분류된 인공지능 시스템에 대해서는 CRA에 규정된 사이버보안 필수 요구사항을 준수할 것을 요구하고 있다. CRA 제11조(제조사의 신고 의무사항)의 제1항은 디지털제품 제조사에게 실제로 악용된 보안취약점(actively exploited vulnerability)을 인지한 경우 24시간 이내에 네트워크·정보시스템 보안 개정 지침(NIS2) 제12조에 따라 지정된 CVD 조정기관인 CSIRT로 신고할 것을 요구하고 있으며, 같은 조 제4항은 디지털제품 제조사에게 해당 보안취약점을 디지털제품 이용자에게 지체 없이 통지하도록 규정하고 있다. 또한, CRA 부속서의 제2항은 보안취약점 조치를 위한 보안 업데이트 기능을 디지털제품에 디폴트로 탑재할 것을 요구하고 있다(secure by default).

2.3.2 EU 가이드

유럽사이버보안청(ENISA)이 '23.2월에 발표한 '국가 보안취약점 프로그램' 가이드는 CVD 도입의 가장 큰 장애 요소로 화이트해커 보호를 위한 법체계 미비를 들고 있으며, CVD를 도입을 위해서는 화이트해커에 대한 법적 보호가 필요함을 설명하고 있다[44].

또한, 유럽사이버보안청이 '22.4월에 발표한 '유럽연합 CVD 정책' 가이드[3]의 3.3.1절은 Fig. 4.와 같이 CVD 도입에 영향을 미치는 법률로 사이버범죄법(Directive 2013/40/EU)[45], 개인정보보호법(GDPR)[46] 등을 설명하고 있으며, 프랑스, 네덜란드 등의 유럽연합 회원국은 법률 또는 정책 등을 기반으로 화이트해커를 보호하고 있음을 설명하고 있다. 프랑스의 법률(Code de défense) L2321-4 조항은 화이트해커 법적 보호를 위해 2가지 조건을 충족할 것을 규정하고 있다. 첫 번째 조건은 보안취약점 발견이 선의의 보안연구 목적으로 수행되어야 하고, 두 번째 조건은 발견한 보안취약점을 프랑스 사이버보안청(ANSSI)으로만 신고할 것을 규정하고 있다. 네덜란드는 검찰이 발표한 CVD 정책을 통해 화이트해커 보호할 것임을 밝히고 있다. 3.2.1절은 공개되는 VDP에 포함될 내용을 설명하고 있다.

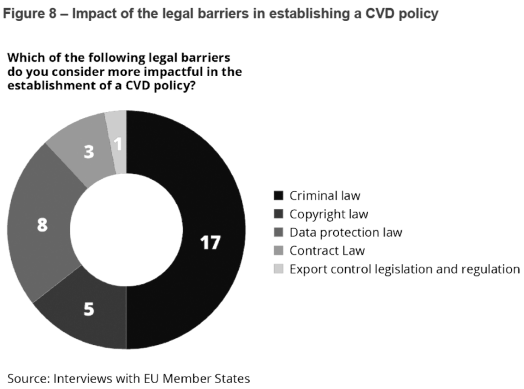


Fig. 4. The legal barriers in establishing CVD[3]

2.4 경제개발협력기구(OECD)

Fig. 5.의 디지털 보안 구축 정책 프레임워크에 기반하여 경제개발협력기구(OECD)가 발표한 5종의 디지털 보안 가이드는 CVD 도입을 권고하고 있다.

① 디지털 보안 위험관리에 관한 권고 : '22.9월에 발표된 본 가이드는 위험관리의 원칙 중 하나로 디지털 보안에 있어 보안취약점 신고 중요성을 설명하고 있다[47].
② 디지털 국가 디지털 안보전략에 관한 권고 : '22.9월에 발표된 본 가이드의 제3장은 CVD를 국가사이버안보전략으로 채택 및 CVD 운영을 위해 한 개 이상의 침해사고대응조직(CSIRT)을 CVD 조정기관으로 지정할 것을 권고하고 있다[48].
③ 주요기반시설의 디지털 보안에 관한 권고 : '19.10월에 발표된 본 가이드의 제4장은 주요기반시설에 대한 보안 방안으로 CVD 도입을 권고

Fig. 5. OECD Policy Framework on Digital Security[47]

하고 있다[49].

④ 디지털 제품·서비스의 보안에 관한 권고 : '22.9월에 발표된 본 가이드의 제4장은 디지털 제품·서비스 공급자의 의무사항으로 CVD 도입을 권고하고 있다[50].

⑤ 디지털 보안 취약점 처리에 관한 권고 : '22.9월에 발표된 본 가이드의 제4장은 화이트해커의 법적 보호를 위해 VDP를 수립·공개할 것을 권고하고 있으며, 제5장은 CVD의 실효적인 운영을 지원하기 위하여 한 개 이상의 신뢰할 수 있는 조정기관을 지정할 것을 권고하고 있다[4].

이 밖에, CVD 도입·확산을 위해 OECD가 '21.3월에 발표한 'CVD 권장' 가이드의 2.2.1절은 CVD 도입의 가장 큰 장애요소로 화이트해커에 대한 법적 보호 미비를 설명하고 있으며, 화이트해커 보호에 영향을 미치는 관련법으로는 사이버범죄법, 개인정보보호법, 저작권법 등을 설명하고 있다. 또한 2.2.2절은 화이트해커 보호 방안으로 VDP를 설명하고 있으며, 2.4.4절에서는 VDP 수립·공개를 권고하고 있다[51].

III. CVD 법제화 필요성 및 요구사항

우리나라 법제처가 발간한 '법령 입안·심사 기준'은 법령안 입안 전에 입법의 필요성에 대한 정책 판단과 입안을 위한 법령 선정, 법령에 포함할 사항을 정할 것을 요구하고 있다[52]. 이에, 3장에서는 2장에서 소개한 우리나라 현황 및 미국, 유럽연합, OECD의 CVD 관련 법령, 정책, 가이드를 분석하여 CVD 법제화 필요성을 파악하고 법제화를 위한 CVD 요구사항을 도출한다.

Table 2.는 2장의 CVD 동향과 3장의 CVD 법제화 필요성·요구사항간의 대응관계를 보여 주고 있다. CVD 법제화 필요성은 CVD 도입 필요성(3.1.1), 법률에 기반한 제도화 필요성(3.1.2), CVD 법제화 법률로 정보통신망법 적합성(3.1.3) 등 세 가지 측면에서 분석하고, CVD 법제화 요구사항으로는 VDP 수립·공개(3.2.1), 화이트해커 법적 보호(3.2.2), CVD 조정기관 지정 및 역할 부여(3.2.3) 등 세 가지 요구사항을 도출한다.

3.1 CVD 법제화 필요성

3.1.1 CVD 도입 필요성

CVD 법제화를 추진하기 위해서는 CVD 도입이 필요한지에 대한 정책적 판단이 선행되어야 한다[52]. 본 절에서 제시하는 우리나라의 CVD 도입 필요성은 아래 두 가지이다.

첫 번째 필요성은 Table 2. 항목 (1)부터 (20)까지의 법령·정책·가이드로, 미국, 유럽연합, OECD는 이를 통해 화이트해커를 사이버보안체계로 수용하고 있다. 특히 미국은 CVD를 통해 전 세계 화이트해커로부터 수만 개의 보안취약점 신고를 받는 등 CVD를 사이버보안 강화 방안으로 활용하고 있다[53]. 이와 같은 국외 동향에 맞춰 우리나라도 사이버보안 경쟁력 제고를 위한 방안으로 CVD를 도입할 필요가 있다.

두 번째 필요성은 CVD 자율 운영의 법적 부담이다. 사업자와 화이트해커에게 사이버범죄법, 개인정보보호법, 저작권법 등 CVD에 영향을 미치는 모든 관련법을 준수하도록 하는 것은 CVD 도입에 큰 부담과 위축으로 작용한다(chilling effect)[54][55]. 일례로, 한국인터넷진흥원이 운영 중인 보안취약점 신고포상제도는 포상금 지급에 대해서만 법적 근거(정보통신망법 제47조의6)가 있어, 화이트해커가 보안취약점 발견을 위해 실제 서비스 중인 웹사이트나 정보서비스에 접근하는 경우 정보통신망법 제48조에 위반하지 않기 위해서는 사업자의 사전 동의를 받아야 하는 등 법적인 제약이 따른다[12]. 더욱이, 화이트해커가 접근 대상이 개인정보보호법 제2조제1호 및 제3호에 따른 정보주체의 개인정보 및 저작권법 제2조제28호에 따른 기술적 보호조치와 관련된 경우, 화이트해커의 보안취약점 발견 행위가 정보주체와 저작권자의 권리를 침해하지 않기 위해서는 사전 동의를 받아야 할 필요가 있다.

Table 2. The necessity and requirements for CVD legislation based on laws・policies・guides of the US・EU・OECD

CVD-related contents of chapter 2			CVD legislation necessity & reqs. of chapter 3
(1)	FISMA	- legal basis of CVD - application entity : federal agency - application scope : information system - administering the implementation of agency information security policies, practices, etc.	3.1.1. 3.1.2, 3.1.3
(2)	M-20-32 based on FISMA	- establishment and publication of VDP - VDP's compliance with related laws - vulnerability response process	3.1.1 3.2.1
		- legal protection for white-hat hacker : complying with VDP and good-faith security research	3.1.1 3.2.2
(3)	BOD-20-01 based on FISMA	- VDP includes items that white-hat hackers and agencies must comply with	3.1.1 3.2.1. 3.2.2
(4)	BOD-19-02, 22-01 based on FISMA	- remediation for critical vulnerability or known exploited vulnerability	3.1.1 3.2.3
(5)	IOTA	- legal basis of CVD - application entity : federal agency - application scope : IoT device	3.1.1. 3.1.3
(6)	NIST SP 800-216 based on IOTA	- CVD program(vulnerability life cycle)	3.1.1
(7)	NCS	- promotion of CVD in private sector	3.1.1
(8)	NCSIP	- CISA as responsible org. for CVD promotion	3.1.1
(9)	M-22-09, M-23-16 based on EO 14028	- CVD is one of requirements of ZTA and SW supply chain security	3.1.1
(10)	Secure by Design	- VDP is one of the requirements of secure by design	3.1.1 3.2.1
(11)	AI security roadmap	- CVD is one of the requirements of AI security	3.1.1
(12)	OSS Roadmap	- CVD is one of the requirements of OSS security	3.1.1
(13)	DOJ's charging policy	- good-faith security research is excluded from prosecution	3.1.1 3.2.2
(14)	Vulnerability Response Playbook	- CISA as a coordinator - coordinator's roles	3.1.1. 3.1.3 3.2.3
(15)	CVD Program	- CVD program(vulnerability lifecycle) including vulnerability disclosure timing - CISA as a coordinator	3.1.1. 3.1.3 3.2.3
(16)	CSF 2.0	- CVD is one of the requirements of CSF 2.0	3.1.1
(17)	EU's NIS2	- legal basis of CVD - application entity : essential or important organizations based on workforce size, revenue, criticality of sectors, etc. - application scope : ICT service	3.1.1, 3.1.2, 3.1.3
		- CSIRT as a coordinator	3.1.1. 3.1.3 3.2.3
(18)	EU's CRA	- legal basis of CVD - application entity: digital product manufacturer - application scope : digital product	3.1.1, 3.1.2, 3.1.3
		- manufacturer's vulnerability reporting to CSIRT and notification to users - CSIRT is coordinator under NIS2	3.1.1. 3.1.3 3.2.3
(19)	ENISA's guides	- compliance with relevant laws of CVD - legal protection for white-hat hackers : complying with VDP and good-faith security research - designation and roles of coordinator	3.1.1, 3.1.3 3.2.1, 3.2.2, 3.2.3
(20)	OECD's guides		

3.1.2 법률에 기반한 제도화 필요성

본 절에서 제시하는 CVD를 법률에 기반하여 제도화해야 할 필요성은 아래 세 가지이다.

첫 번째는 3.2절에서 소개할 CVD 법제화 요구사항이 법률 소관사항에 속한다는 점이다. 우리나라 법체계에서 법률에서 다루어야할 소관사항은 헌법에서 법률로 정하도록 한 사항과 국민의 권리・의무에 관한 사항이며, 대통령령의 소관사항은 법률에서 위임한 사항이거나 법률을 집행하는 데에 필요한 사항 등이다[52]. 이를 고려할 때, CVD 법제화 요구사항인 사업자의 VDP 수립・공개, 화이트해커 법적 보호, CVD 운영기관인 조정기관 지정과 역할 부여는 사업자・화이트해커・조정기관의 권리와 의무에 관한 사항으로 법률 소관사항에 해당한다. 또한, 이를 뒷받침하는 국외 사례는 Table 2. 항목 (1), (5), (17), (18)로 CVD의 근거가 되는 미국과 유럽연합의 법률이다.

두 번째는 CVD 법제화 요구사항 중 하나인 화이트해커 법적 보호는 형벌(刑罰) 조항에 영향에 미친다는 점이다. 화이트해커 법적 보호는 정보통신망법 제48조(정보통신망 침해행위 등의 금지)와 제71조(벌칙)[7], 개인정보보호법 제59조(금지행위)와 제71조(벌칙)[56], 저작권법 제104조의2(기술적 보호조치의 무력화 금지)와 제136조(벌칙)[57]에 영향을 미치므로 법률로 다룰 필요가 있다.

세 번째는 CVD가 법률에 근거를 둘 경우, 화이트해커가 보안취약점 발견 과정 중에 발생할 수 있는 개인정보 접근이 개인정보보호법에 부합하는 방안이 될 수 있다. 제3자의 개인정보 열람 허용은 개인정보 제3자 제공에 해당한다는 우리나라 법제처의 해석에 기반하여 볼 때[58], CVD가 법률에 기반을 둘 경우, 제3자인 화이트해커가 보안취약점 발견 중에 발생할 수 있는 개인정보 접근이 정보주체의 동의 없이도 개인정보보호법 제18조제2항제2호의 '다른 법률에 특별한 규정이 있는 경우'에 부합될 수 있다[56][59].

3.1.3 CVD 법제화 법률로 정보통신망법 적합성

본 절은 CVD 법제화 법률로 정보통신망법의 적합성을 ① 사이버보안 법체계, ② 침해사고 예방・대응, ③ CVD 목적・대상・범위 등 세 가지 측면에서 분석한다.

① 사이버보안 법체계

우리나라의 사이버보안 법체계는 분야별 소관 법률로 구성되어 있다[60]. 예를 들어, 국가(공공) 분야는 국가정보원법과 이에 기반한 대통령령인 사이버안보 업무규정이 소관 법령이고, 민간 정보통신망・정보통신서비스 분야와 주요정보통신기반시설은 각각 정보통신망법과 정보통신기반보호법이 소관 법률이다. 이와 같은 우리나라 사이버보안 법체계를 고려할 때, 분야별 소관 법률에 기반한 CVD 법제화는 CVD 도입의 방안이 될 수 있다.

한편, Table 2. 항목 (1), (5), (17), (18)에 명시된 미국과 유럽연합의 연방정보보안현대화법(FISMA), IoT 사이버보안 강화법(IOTA), 네트워크・정보시스템 보안 개정 지침(NIS2), 사이버복원력법(CRA)은 법률의 적용 대상과 범위를 연방기관 정보시스템・IoT기기, 필수・중요조직(essential・important entities)의 정보서비스, 디지털제품 제조사로 특정하여 정하고 있다.

이와 같이, 우리나라 사이버보안 법체계 및 미국, 유럽연합의 CVD의 근거 법률을 고려할 때, 우리나라 민간 분야 소관 법률인 정보통신망법은 CVD 법제화 대상 법률로 적합하다고 판단된다.

② 침해사고 예방・대응

CVD는 화이트해커의 보안취약점 발견을 통해 침해사고를 예방하는 것이 주된 목적이므로, 민간 분야 침해사고 예방・대응체계를 다루고 있는 정보통신망법은 이에 부합한다.

Table 2. 항목 (1), (5), (17), (18)의 미국과 유럽연합의 CVD 근거 법률도 보안취약점 뿐만 아니라 침해사고 예방・대응도 함께 규정하고 있다. 특히, CVD 조정기관으로 침해사고 대응조직(CSIRT) 지정은 민간 분야 침해사고 예방・대응을 한국인터넷진흥원(KrCERT/CC)의 역할로 규정하고 있는 정보통신망법 제52조제3항제11호에도 부합한다. 이와 관련된 Table 2.의 항목은 (5), (14), (15), (17)~(20)이다.

이에, 침해사고 예방・대응체계를 규정하고 있는 정보통신망법은 침해사고 예방이 주된 목적인 CVD의 법제화 법률로 적합하다고 판단된다.

③ CVD 목적・대상・범위

CVD 목적은 보안취약점 발견・조치를 통해 침해사고를 예방하는 것이다. 정보통신망법 제1조는 정보통신서비스를 이용하는 자를 보호하고 정보통신망을 안전하게 이용할 수 있는 환경을 조성하는 것을 법의 목적으로 정하고 있다. 이에 정보통신망법의 목적은 CVD 목적에 부합한다.

CVD 적용 대상과 범위는 ICT 사업자와 ICT 제품・서비스이다. 정보통신망법의 제2조는 적용 대상과 범위를 정보통신서비스 제공자 및 정보통신망 또는 이와 관련된 정보시스템으로 정하고 있고, 제45조에서는 정보통신망에 연결된 IoT 기기를 제조하거나 수입한 자로 정하고 있어 CVD 적용 대상・범위에 부합한다.

Table 2. 항목 (1), (5), (17), (18)의 미국과 유럽연합 CVD 근거 법률과 정보통신망법(ICNA)을 비교하였을 때에도, CVD 적용 대상은 연방기관, 필수・중요 사업자, 정보통신서비스 제공자로 다르지만 적용 범위는 ICT 서비스 및 제품으로 Table 3.과 같이 일치한다.

Table 3. Comparison of the application scope of CVD-related laws

US		EU		KR
FISMA	IOTA	NIS2	CRA	ICNA
ICT system	IoT device	ICT service	digital product	ICT service, IoT device

3.2 CVD 법제화 요구사항

본 절에서는 2장에서 소개한 미국, 유럽연합, OECD의 법령・정책・가이드에 기반하여 Fig. 6과 같이 VDP 수립・공개, 화이트해커 법적 보호, 조정기관 지정・역할 부여로 구성된 3가지 CVD 법제화 요구사항을 도출한다.

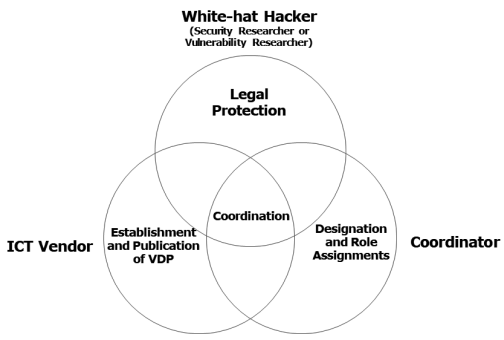


Fig. 6. The requirements for legislating CVD

3.2.1 VDP 수립・공개

화이트해커가 사업자의 동의를 받을 필요 없이 사업자의 ICT 제품・서비스에 접근하기 위해서는 사업자의 VDP 수립・공개가 선행되어야 하며, 이를 사업자에게 공통적으로 적용하기 위해서는 법제화가 요구된다.

Table 2.의 항목 (2) 美 관리예산처(OMB) M-20-32, (3) 美 사이버보안청(CISA) BOD 20-01, (10) 시큐어 바이 디자인(Secure by Design). (19) 유럽사이버보안청(ENISA) 가이드, (20) OECD 가이드는 VDP 수립・공개와 VDP에 포함되는 내용을 설명하고 있다.

VDP에 포함되어야할 내용은 Table 4.와 같이 화이트해커와 사업자가 준수해야할 요구사항 10개이다. 화이트해커가 준수할 사항은 ① 보안취약점 발견 중 접근한 개인정보 유출 금지, ② 사업자가 허용한 범위・방법에 기반하여 보안취약점 발견 수행, ③ 발견한 보안취약점 신고, ④ 사업자와의 협의에 기반한 보안취약점 공개, ⑤ 발견한 보안취약점에 대한 조치 협력 등 5개이며, 사업자가 준수할 사항은 ⑥ VDP 내용의 관련법 준수, ⑦ 보안취약점 신고 방법・내용 공개(익명신고 포함), ⑧ VDP 준수 및 선의의 보안연구를 충족한 화이트해커에 대해서는 법적 문제를 제기하지 않을 것임을 공개적으로 선언, ⑨ 화이트해커에게 보안취약점 진행사항 공유, ⑩ VDP 공개방법・버전 관리 등 5개이다.

이에 따라 도출된 법제화 요구사항은 Table 4.의 내용이 포함된 VDP의 수립 및 공개이다.

Table 4. VDP contents

Subjects	VDP contents
white-hat hackers	① A prohibition against leaking personal information accessed
	② The scope and method of discovering the vulnerability
	③ Reporting vulnerabilities
	④ Coordinating with vendor on vulnerability disclosure timing
	⑤ Cooperating with vendor to remediate vulnerabilities

Subjects	VDP contents
vendors	⑥ VDP in compliance with relevant laws
	⑦ Announcement of reporting methods and content(including anonymous reporting)
	⑧ Declaration of legal protection for white-hat hackers adhering to VDP and good-faith security research
	⑨ Sharing progress after reporting with white-hat hackers
	⑩ VDP publishing method and version control

3.2.2 화이트해커 법적 보호

화이트해커의 법적 보호를 위해서는, 정보통신망법 제48조(정보통신망법 침해행위 등의 금지) 제1항에 명시된 '정당한 접근권한' 및 '허용된 접근권한', 개인정보보호법 제59조(금지행위) 제3호에 명시된 '정당한 권한' 및 '허용된 권한', 저작권법 제104조의2(기술적 보호조치의 무력화 금지) 제1항에 명시된 '정당한 권한'에 부합하는 화이트해커 준수 규정이 마련되어야 한다.

미국과 유럽연합의 화이트해커의 법적 보호를 위한 방안으로 Table 2.의 (2) 美 관리예산처(OMB) M-20-32, (3) 美 사이버보안청(CISA) BOD-20-01, (13) 美 법무부(DOJ) 기소 정책, (19) 유럽사이버보안청(ENISA) 가이드, (20) OECD 가이드는 화이트해커의 VDP 준수와 선의의 보안연구(good-faith security research) 충족을 설명하고 있다.

이에 따라 도출된 법제화 요구사항은 화이트해커의 Table 4.에 명시된 VDP 항목 ①~⑤ 준수 및 Table 1.에 명시된 선의의 보안연구 충족이다.

3.2.3 조정기관 지정・역할 부여

○ 조정기관 지정

보안취약점 발견 및 조치 등이 실효적으로 수행되기 위해서는 화이트해커와 사업자간에 이견 조정, 보안취약점 개선 조치 명령 등의 역할을 수행할 조정기관(coordinator) 지정이 요구된다.

Table 2.의 (14) 사이버보안 취약점 대응 플레이북, (15) CVD 프로그램, (17) 네트워크・정보시스템 보안 개정 지침(NIS2), (18) 사이버복원력법(CRA), (19) 유럽사이버보안청(ENISA) 가이드, (20) OECD 가이드는 조정기관 역할을 CISA(US-CERT) 및 유럽연합 회원국이 지정한 침해사고대응조직(CSIRT)이 담당하여 수행하고 있음을 설명하고 있다.

○ 조정기관 역할 부여

3.1.2에서 설명한 조정기관의 역할과 권한은 사업자와 화이트해커에 영향을 미치므로 법률로 규정될 필요가 있다.

Table 2.의 (4) 美 사이버보안청(CISA) BOD 19-02와 BOD 22-01의 심각(critical) 또는 알려진 악용된 보안취약점에 대한 조치, (14) 사이버보안 취약점 대응 플레이북의 보안취약점 발견, 신고, 조치, 공개로 구성된 보안취약점 대응 프로세스, (15) CVD 프로그램의 보안취약점 신고, 조치 공개, (18) 사이버복원력법(CRA)에 규정된 실제로 악용된 보안취약점 신고・통지와 보안업데이트를 통한 보안취약점 조치, (19)・(20) 유럽사이버보안청(ENISA) 및 OECD 가이드에 명시된 보안취약점 신고 및 조치는 조정기관의 역할을 설명하고 있다.

이에 따라 도출된 조정기관의 역할은 CVD 운영과 보안취약점 신고・통지・조치・공개이다.

IV. CVD 도입을 위한 정보통신망법 개선방안

4장에서는 3.2절에서 도출한 CVD 법제화 요구사항을 정보통신망법에 적용하는 방안을 설명한다.

4.1절에서는 CVD 법제화 요구사항이 現 정보통신망법에 포함되어 있는지 확인하고, 4.2절에서는 CVD 주요 용어에 대한 한글 용어를 제안한다. 4.3절에서는 CVD 법제화 요구사항을 정보통신망법에 적용하기 위한 방안을 신설 조항, 수행 주체, 수행 내용, 참고 법령 등을 기반으로 소개한다.

4.1 정보통신망법의 법제화 요구사항 포함 여부

現 정보통신망법의 보안취약점 관련 조항은 제47조의4(이용자의 정보보호) 제1항과 제4항, 제47조의6(정보보호 취약점 신고자에 대한 포상), 제48조의5(정보통신망연결기기등 관련 침해사고의 대응 등)

제3항으로, 3.2절에서 도출한 CVD 법제화 요구사항과의 관련성은 아래와 같다.

○ 제47조의4(이용자의 정보보호) 제1항과 제4항 : 정보통신망 이용자 보호를 위한 취약점 점검을 규정하고 있는 제47조의4제1항은 앞서 제1장에서 설명한 바와 같이 수행 결정주체, 수행 단계, 공개 측면에서 CVD와는 차이점이 있어 CVD 법제화 요구사항은 아니다. 제4항은 소프트웨어 사업자가 보안취약점에 대한 보안패치를 개발한 경우 한국인터넷진흥원과 소프트웨어 사용자에게 통지할 것을 규정하고 있으며, 이는 조정기관의 역할 중 보안취약점 통지와 관련된다.

○ 제47조의6(정보보호 취약점 신고자에 대한 포상) : 보안취약점 신고자에 대한 포상금 지급 근거를 규정하고 있는 제47조의6은 CVD와 연계하여 화이트해커의 보안취약점 신고를 촉진하는 수단으로 활용될 수는 있으나, 3.2절에서 도출된 CVD 법제화 요구사항과는 직접적인 관련성은 없다.

○ 제48조의5(정보통신망연결기기등 관련 침해사고의 대응 등) 제3항 : 침해사고가 발생한 경우 정보통신망연결기기 제조사 및 수입사에 대한 보안취약점 개선 권고를 규정하고 있는 제48조의5제3항은 CVD 법제화 요구사항 중 조정기관의 보안취약점 조치 역할과 관련성이 있다.

이에 따라, 現 정보통신망법(ICNA)은 Table 5.

Table 5. The inclusion relation between CVD legislation requirements and current ICNA

The requirements for CVD legislation		ICNA
establishment and publication of VDP		not included
legal protection for white-hat hackers		
③ coordinator	designation	
	operation and support	
	vuln. reporting and notification	partially included (Art. 47-1④, Art. 48-5③)
	vuln. remediation and disclosure	

와 같이 CVD 법제화 요구사항 중 VDP 수립·공개, 화이트해커 법적 보호를 포함하지 않으며, 제47조의4 제4항과 제48조의5 제3항이 CVD 법제화 요구사항 중 하나인 조정기관의 역할에 포함됨을 확인할 수 있다.

4.2 CVD 법제화를 위한 한글 용어

CVD 법제화 및 도입 확산을 위해서는 CVD 주요 용어에 대한 한글 용어를 정의할 필요가 있다.

○ **CVD : '보안취약점 협력대응제도' 또는 '조정기반 보안취약점 공개제도'**

본 절에서는 'Coordinated Vulnerability Disclosure'에 대한 한글 용어로 '보안취약점 협력대응제도'와 '조정기반 보안취약점 공개제도'를 제안한다. CVD를 한글로 직역하면 '조정기반 보안취약점 공개제도' 등이 될 수 있으나, 이 경우, '공개'의 의미만 인식될 가능성이 높아 CVD의 의미를 완전히 표현하지 못하는 한계가 있다. CVD 용어를 세부적으로 분석하면, 카네기멜론 대학교의 CVD 가이드의 1.2.5절은 CVD를 참여자간 협력·조정에 기반한 보안취약점 대응 프로세스로 설명하고 있다[1]. 또한, OECD 가이드[49] 1.1.4절은 CVD를 보안취약점 발견, 신고, 처리, 공개로 구성된 보안취약점 전주기(life cycle)에 대한 프로세스로 설명하고 있으며, CVD의 첫 번째 글자 'C'의 'Coordinated는 참여자간의 소통, 협력 및 조정의 3가지 의미를 포함하고, 마지막 글자 'D'의 'Disclosure'는 보안취약점 제공(provision), 신고(reporting), 공개(disclosure)의 3가지 의미를 포함한다고 설명하고 있다.

이에, 본 논문은 CVD의 한글 용어로 대응(response), 전주기(life cycle), 프로세스(process), 신고(reporting), 제공(provision), 공개(disclosure), 소통·협력·조정(coordination)의 의미를 모두 포함하는 '보안취약점 협력대응제도'를 제안하며, 이에 추가하여 제1장에서 설명한 바와 같이 CVD가 책임감 있는 보안취약점 공개(Responsible Disclosure)에서 유래한 점을 고려하여 '조정기반 보안취약점 공개제도'도 함께 제안한다.

○ VDP : ‘보안취약점 처리방침’ 또는 ‘보안취약점 공개방침’

본 논문은 ‘Vulnerability Disclosure Policy’에 대한 한글 용어로 ‘보안취약점 처리방침’과 ‘보안취약점 공개방침’을 제안한다. VDP를 한글로 직역하면 ‘보안취약점 공개 정책’ 등으로 번역될 수 있으나, 이는 앞서 CVD와 같이 의미를 완전히 표현하지 못하는 한계가 있으며, 또한 ‘정책’이란 단어가 포함될 경우 VDP의 수립·공개 주체가 사업자가 아닌 정부로 잘못 해석될 소지가 있다. 또한 우리나라 개인정보보호법의 경우 ‘개인정보 처리방침’을 ‘Privacy Policy’로 번역하고 있다[56].

이에, 본 논문은 개인정보보호법 제30조(개인정보 처리방침의 수립 및 공개)에서 정의된 ‘개인정보 처리방침’ 용어를 참고하여 VDP를 ‘보안취약점 처리방침’으로 제안한다. ‘개인정보 처리방침’은 개인정보 ‘처리(processing)’ 의미이고, VDP는 보안취약점 취급·처리(handling, treatment)의 의미이지만[49][50], ‘개인정보 처리방침’이 개인정보 전주기(수집, 이용, 처리, 파기)를 다루고 VDP도 보안취약점 전주기(발견, 신고, 조치, 공개)를 다룬다는 점, 그리고 사업자가 모두 수립·공개해야 하는 점에서 공통점이 있다.

이에 따라 본 논문은 VDP의 한글 용어로 ‘보안취약점 처리방침’으로 제안하며, 앞서 CVD 한글 용어에서 설명한 바와 같이 ‘보안취약점 공개방침’도 추가로 제안한다.

○ White-Hat Hacker : 취약점연구자 또는 보안연구자

미국, 유럽연합, OECD는 CVD에서 보안취약점 발견 등의 역할을 수행하는 화이트해커를 Table 1.과 같이 취약점연구자 또는 보안연구자 용어로 정의하여 사용하고 있다[3][4][35]. 이에 따라 본 논문에서는 화이트해커에 대한 한글 용어로 취약점연구자 또는 보안연구자를 사용한다.

Table 6. white-hat hacker under CVD

US[35]	EU[3]	OECD[4]
Security Researcher	Security Researcher	Security Researcher, Vulnerability Researcher

4.3 정보통신망법에 법제화 요구사항 적용 방안

본 절에서는 CVD의 법제화 요구사항 ① 보안취약점 처리방침 수립·공개, ② 취약점연구자 법적 보호, ③ 조정기관 지정·역할을 정보통신망법에 적용하는 방안을 소개한다.

4.3.1 보안취약점 처리방침(VDP) 수립·공개

본 절에서는 3.2.1절에서 도출된 법제화 요구사항인 보안취약점 처리방침(VDP) 수립·공개를 정보통신망법에 적용하기 위한 방안을 조항 신설, 수립 주체, 수립 내용, 공개 방법 등을 중심으로 설명하고, 이와 관련되어 참고한 국내외 법령을 소개한다.

○ (안 제47조의8 신설) 4.1절에서 살펴본 바와 같이, 보안취약점 수립·공개 법제화 요구사항은 現 정보통신망법에 포함되어 있지 않으므로, 신규 조항 신설이 요구된다. 정보통신망법의 구성 측면에서 침해사고 예방은 제47조부터 제47조의7까지 구성되어 있고, 침해사고 대응은 제48조부터 제48조의6까지 구성되어 있으므로, 침해사고 예방 측면이 강한 보안취약점 협력대응제도(CVD)의 보안취약점 처리방침의 수립·공개를 안 제47조의8(보안취약점 처리방침의 수립 및 공개)로 신설하는 방안을 제안한다.

○ (수립 주체) 보안취약점 처리방침 수립 주체는 정보통신망법 제2조제1항제2호에 따른 정보통신서비스 제공자, 제45조제1항제2호에 따른 정보통신망에 연결된 정보통신망연결기기등을 제조한 자, 제47조의4 제4항의 소프트웨어진흥법 제2조에 따른 소프트웨어사업자(이하 “취약점방침수립자”라 한다)이다. 취약점방침수립자의 세부 범위는 유럽연합의 네트워크·정보시스템 보안 개정 지침(NIS2)의 제3조의 필수 및 중요 조직, 정보통신망법 제47조의제2항의 매출액 등을 고려한 정보보호관리체계(ISMS) 인증 의무대상 등을 고려하여 정책적으로 정할 필요가 있다.

○ (수립 내용) 보안취약점 처리방침에는 Table 4.에 명시된 VDP 내용이 포함된다.

○ (공개 방법) 개인정보 처리방침의 공개 방법을 규정한 개인정보보호법 제30조제2항을 참고하여, Table 4.의 ⑩ 항목의 보안취약점 처리방침 공개

방법은 보안취약점 처리방침 신설 조항에 “취약점방침수립자는 보안취약점 처리방침을 수립하거나 변경하는 경우에는 취약점연구자가 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.”로 명시한다.

○ (참고 법령) 안 제47조의8(보안취약점 처리방침의 수립 및 공개) 조항 신설시, 참고한 법령과 가이드는 Table 2.의 항목 (2), (3), (10), (19), (20)이며, 추가적으로 취약점방침수립자 범위에 대해 참고한 법령은 유럽연합의 네트워크·정보시스템 보안 개정 지침(NIS2)의 제3조에 규정된 필수 및 중요 조직과 정보통신망법 제47조의제2항의 매출액 등을 고려한 ISMS 인증 의무대상이다. 신설 조항 구성에 관한 참고 법령 조항은 개인정보보호법 제30조(개인정보 처리방침의 수립 및 공개)와 동법 시행령 제31조(개인정보 처리방침의 내용 및 공개방법 등)이다.

4.3.2 취약점연구자(화이트해커) 법적 보호

3.2.2절에서 도출된 법제화 요구사항인 화이트해커 법적 보호를 정보통신망법에 적용하는 방안은 아래와 같다.

○ (안 제47조의9 신설) 취약점연구자가 법적 보호를 받기 위해서는 제48조(정보통신망법 침해행위 등의 금지) 제1항에 명시된 ‘정당한 접근권한’ 및 ‘허용된 접근권한’, 개인정보보호법 제59조(금지행위) 제3호에 명시된 ‘정당한 권한’ 및 ‘허용된 권한’, 저작권법 제104조의2(기술적 보호조치의 무력화 금지) 제1항에 명시된 ‘정당한 권한’에 부합하는 취약점연구자 준수 규정 신설이 요구된다.

이를 위한 신설 조항은 안 제47조의9(취약점연구자의 책무)로, 신설 조항의 내용은 3.2.2절에서 설명한 보안취약점 처리방침 준수 및 선의의 보안연구 충족에 기반하며, 신설 조항의 제목과 구성과 관련하여 참고한 법령은 정보통신망법 제3조(정보통신서비스 제공자 및 이용자의 책무)이다.

○ (책무 주체) 보안취약점 처리방침 준수와 선의의 보안연구를 충족해야 하는 주체인 취약점연구자를 「보안취약점 발견을 목적으로 제2조(정의)에 따른 정보통신망 및 정보통신서비스, 제45조제1항제2호에 따른 정보통신망연결기기등, 소프트웨어진흥법 제2조에 따른 소프트웨어에 접근한 자(이하 “취약점연구자”라 한다)」로 규정한다.

○ (책무 내용) 취약점연구자가 준수할 사항은 아래 ①부터 ⑤까지의 내용이다. ①은 안 47조의8에 따라 수립·공개된 보안취약점 처리방침이고, ②~④는 Table 1.에 명시된 선의의 보안연구 내용이다. ⑤는 정보통신망법·개인정보보호법·저작권법의 금지행위 조항 내용 중 ①~④에 해당하지 않는 부분이다.

① 취약점연구자는 안 제47조의8에 따라 수립·공개된 보안취약점 처리방침을 준수하여야 한다.
② 취약점연구자는 보안취약점 발견 목적으로만 정보통신망법 제2조제1항제1호 및 제2호에 따른 정보통신망과 정보통신서비스, 제45조제1항제2호에 따른 정보통신망연결기기등, 소프트웨어진흥법 제2조제1호에 따른 소프트웨어(이하 “정보통신망등”이라 한다)에 접근하여야 한다.
③ 취약점연구자는 보안취약점 발견 과정에서 취약점방침수립자 및 취약점방침수립자가 제공·제조·개발한 정보통신망등의 이용자에게 피해를 주지 않아야 한다.
④ 취약점연구자는 발견한 보안취약점 및 이와 관련된 정보를 정보통신망법 제1조(목적)에 맞게 사용하여야 한다.
⑤ 취약점연구자는 보안취약점 발견 등을 수행하는 과정에서 정보통신망법 제48조(정보통신망 침해행위 등의 금지), 개인정보보호법 제59조(금지행위), 저작권법 제104조의2(기술적 보호조치의 무력화 금지)를 준수하여야 한다.

○ (참고 법령) 안 제47조의9(취약점연구자의 책무) 조항 신설시 참고한 법령·정책·가이드는 Table 2.의 항목 (2), (3), (13), (19), (20)이며, 추가적으로 참고한 법령 조항은 정보통신망법 제1조(목적), 제2조(정의), 제3조(정보통신서비스 제공자 및 이용자의 책무), 제45조(정보통신망의 안정성 확보 등), 제48조(정보통신망 침해행위 등의 금지), 개인정보보호법 제59조(금지행위), 저작권법 제104조의2(기술적 보호조치의 무력화 금지), 소프트웨어진흥법 제2조(정의)이다.

4.3.3 CVD 조정기관 지정 및 역할 부여

3.2.3절에서 도출된 법제화 요구사항인 조정기관 지정・역할 부여를 정보통신망법에 적용하는 방안은 아래와 같다.

○ (조항 신설) 수행 주체와 내용이 앞서 신설한 안 제47조의8과 안 제47조의9와는 다르므로, 조정기관 지정・역할 부여에 대한 조항을 신설한다. 또한 정보통신망법의 침해사고 대응 관련 조항인 제48조의3(침해사고의 신고 등), 제48조의4(침해사고의 원인분석 등) 등을 참고하여, 조정기관에게 부여되는 권한과 수행 내용에 따라 개별 조항을 신설한다.

○ (조정기관 지정) 조정기관 역할 중에서 권한과 관련된 역할은 정보통신망법의 소관 부처인 과학기술정보통신부가 수행하고, 신고접수 등의 집행과 관련된 역할은 과학기술정보통신부 또는 한국인터넷진흥원이 수행한다. 이와 관련하여 참고한 법령과 가이드는 Table 2의 (14), (15), (17), (18), (19), (20)이며, 추가적으로 참고한 법령은 정보통신망법의 침해사고 대응 관련 조항인 제48조의3(침해사고의 신고 등)와 제48조의4(침해사고의 원인분석 등)이다.

○ (역할 추가 : 보안취약점 협력대응제도 운영) 한국인터넷진흥원의 침해사고 대응 업무를 규정한 제52조제3항제11호의 '침해사고의 처리・원인분석・대응체계 운영'에 '보안취약점 발견・신고・조치・공개 체계 운영 및 조정 역할 수행'을 추가함으로써 한국인터넷진흥원이 보안취약점 협력대응제도 운영을 담당하도록 한다. 이와 관련되어 참고한 법령은 Table 2.의 (14), (15), (19), (20)이며, 추가적으로 참고한 법령은 정보통신망법 제52조제3항제11호이다.

○ (안 제47조의10 조항 신설 : 보안취약점 신고) 취약점방침수립자는 악용 가능성이 높거나 실제로 악용된 보안취약점을 알게된 때에는 지체 없이 과학기술정보통신부 또는 한국인터넷진흥원에 신고하는 내용의 안 제47조의10을 신설한다. 이와 관련하여 참고한 법령과 가이드는 Table 2.의 항목 (4), (14), (15), (18), (19), (20)이며, 추가적으로 참고한 법령은 제48조의3(침해사고의 신고), 개인정보보호법 제34조(개인정보 유출 등의 통지・신고)이다.

○ (안 제47조의11 신설 : 보안취약점 통지) 취약점방침수립자가 제공・제조・개발한 정보통신망등에서 악용 가능성이 높거나 실제로 악용된 보안취약점이 발견된 경우, 해당 취약점방침수립자는 지체 없이 정보통신망등의 이용자에게 보안취약점에 관한 정보와 개선조치 방법을 통지하고 이용자에게 통지한 사실을 과학기술정보통신부 또는 한국인터넷진흥원에게 알리는 내용으로 안 제47조의11 조항을 신설한다. 이와 관련하여 참고한 법령은 Table 2.의 항목 (18)이며, 특히 악용 가능성이 높거나 실제로 악용된 보안취약점 등의 통지 대상 범위에 대해 참고한 법령은 Table 2.의 항목 (4)와 (18)이다. 또한, 신설 조항 구성에 관해 참고한 법령은 개인정보보호법 제34조(개인정보 유출 등의 통지・신고)이다.

○ (안 제47조의12 신설 : 보안취약점 조치) 과학기술정보통신부가 악용 가능성이 높거나 실제로 악용된 보안취약점이 발견된 취약점방침수립자에게 보안취약점을 개선 조치하도록 권고 또는 명령할 수 있는 안 제47조의12 조항을 신설한다. 이와 관련하여 참고한 법령과 가이드는 Table 2.의 (4), (14), (5), (18), (19), (20)이며, 추가적으로 참고한 법령은 정보통신망법 제48조의4(침해사고의 원인분석 등)이다.

V. 결 론

최근 미국・유럽연합・OECD는 보안취약점 협력대응제도(CVD)의 법제화를 통해 화이트해커의 역량을 사이버보안 강화에 활용하고 있다. 이에, 우리나라도 이러한 변화에 맞춰 보안취약점 협력대응제도를 도입이 요구된다.

본 논문은 보안취약점 협력대응제도를 법제화하여 도입하는 방안을 정보통신망법을 중심으로 소개하였다. 본 논문의 2장은 보안취약점 협력대응제도와 관련하여 우리나라 현황 및 미국・유럽연합・OECD의 동향을 법률・정책・가이드를 기반으로 소개하였으며, 이를 기반으로 3장에서는 법제화 필요성과 요구사항을 파악하고 도출하였다. 4장에서는 앞서 도출된 법제화 요구사항인 보안취약점 처리방침(VDP)의 수립・공개, 취약점연구자(화이트해커) 법적 보호, 조정기관 지정 및 역할 부여를 정보통신망법에 적용하기 위한 방안을 소개하였다.

본 논문의 연구결과는 정보통신망법을 비롯하여 우리나라 다른 분야의 소관 법률을 통해 보안취약점

협력대응제도를 도입하는데 있어 도움이 될 거라 판단되며, 이를 통해 우리나라 사이버보안 강화에 기여하기를 기대한다.

References

[1] Allen D. Householder, Garret Wassermann, Art Manion, Chris King, "The CERT Guide to Coordinated Vulnerability Disclosure," pp. 1-7, pp. 42-44, Carnegie Mellon University, Aug. 2017

[2] CISA, "Coordinated Vulnerability Disclosure Program," www.cisa.gov

[3] ENISA, "Coordinated Vulnerability Disclosure Policies in the EU," www.enisa.europa.eu, Apr. 2022

[4] OECD, "Recommendation of the Council on the Treatment of Digital Security Vulnerabilities," pp. 7-10, OECD/LEGAL/0482, legalinstruments.oecd.org, Sep. 2022

[5] Microsoft, "Coordinated Vulnerability Disclosure: Bring Balance to the Force," msrc.microsoft.com, Jul. 2010

[6] Daniel Votipka, Rock Stevens, Elissa Redmiles, Jeremy Hu, Michelle Mazurek, "Hackers vs. Testers: A Comparison of Software Vulnerability Discovery Process," 2018 IEEE Symposium on Security and Privacy (SP) pp. 374-391, May 2018

[7] Korean Law Information Center, "Act on Promotion of Information and Communications Network Utilization and Information Protection," Act No. 20260, www.law.go.kr, Feb. 2024

[8] Korean Law Information Center, "Act on the Protection of Information and Communications Infrastructure," Act No. 20068, www.law.go.kr, Jan. 2024

[9] Korean Law Information Center, "Software Promotion Act," Act No. 20061, www.law.go.kr, Jan. 2024

[10] Trey Herr, Bruce Schneier, Christopher Morris, "Taking Stock Estimating Vulnerability Rediscovery", pp. 1-8, pp 31-33, Harvard Kennedy School, www.belfercenter.org, Jul. 2017

[11] Nate Cardozo, Kurt Opsahl, Katitza Rodriguez, Ramiro Ugarte, Jamie Lee Williams, "Protecting Security Researchers' Rights in the Americas", Electronic Frontier Foundation, pp. 5-19, Sep. 2018

[12] KISA Cybersecurity Vulnerability Information Portal, knvd.krcert.or.kr

[13] Yongdae Kim, "[ET Column] Reflections on the Domestic Bug Bounty System," www.etnews.com, Mar. 2024

[14] Sangpil Yoon, "On the Security Vulnerability Disclosure Policy of the United States," Journal of Law & Economic Regulation Vol. 15. No. 1, pp. 241-246, May 2022

[15] US Congress, "Federal Information Security Modernization Act of 2014," Public Law 113-283, www.congress.gov, Dec. 2014

[16] OMB, "Improving Vulnerability Identification, Management, and Remediation," pp. 1-5, M-20-32, www.whitehouse. gov, Sep. 2020

[17] CISA, "Develop and Publish a Vulnerability Disclosure Policy," BOD 20-01, www.cisa.gov, Sep. 2020

[18] CISA, "Vulnerability Remediation Requirements for Internet-Accessible Systems," BOD 19-02, www.cisa.gov, Apr. 2019

[19] CISA, "Reducing the Significant Risk of Known Exploited Vulnerabilities," BOD 22-01, www.cisa.gov, Nov. 2021

[20] US Congress, "IoT Cybersecurity Improvement Act of 2020," Public Law 116-207, www.congress.gov, Dec. 2020

[21] NIST, “Recommendations for Federal Vulnerability Disclosure Guidelines,” NIST SP 800-216, csrc.nist.gov, pp. 1-23, May 2023
[22] The White House, “National Cybersecurity Strategy,” www.whitehouse.gov, Mar. 2023
[23] The White House, “National Cybersecurity Strategy Implementation Plan,” www.whitehouse.gov, Jul. 2023
[24] CISA, “FY2024-2026 CISA Cybersecurity Strategic Plan,” www.cisa.gov, Aug. 2023
[25] The White House, “Improving the Nations’s Cybersecurity,” Executive Order 14028, Federal Register Vol. 86 No. 93 Presidential Documents, https://federalregister.gov, May 2021
[26] OMB, “Moving the U.S. Government Toward Zero Trust Cybersecurity Principles,” M-22-09, www.whitehouse.gov, Jan. 2022
[27] OMB, “Enhancing the Security of the Software Supply Chain through Secure Software Development Practices,” M-22-18, www.whitehouse.gov, Sep. 2022
[28] OMB, “Update to Memorandum M-22-18,” M-23-16, www.whitehouse.gov, Jun. 2023
[29] NIST, “Secure Software Development Framework(SSDF) Version 1.1,” NIST SP 800-218,“ csrc.nist.gov, Feb. 2022
[30] CISA, “Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software,” pp. 24, www.cisa.gov, Oct. 2023
[31] The White House, “Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,” Executive Order 14110, www.whitehouse.gov, Oct. 2023
[32] CISA, “2023-2024 CISA Roadmap for Artificial Intelligence,” pp. 8, www.cisa. gov, Nov. 2023
[33] CISA, “CISA Open Source Software Security Roadmap,” www.cisa.gov, Sep. 2023
[34] The US Congress, “Computer Fraud and Abuse Act,” Public Law 99-474, www.congress.gov, Oct 1986
[35] DOJ, “Department of Justice Announces New Policy for Charging Cases under the Computer Fraud and Abuse Act,” www.justice.gov, May 2022
[36] CISA, “Cybersecurity Incident & Vulnerability Response Playbooks,” pp. 21-24, pp. 34, www.cisa.gov, Nov. 2021
[37] NIST, “The NIST Cybersecurity Framework 2.0,” nvlpubs.nist.gov, Feb. 2024
[38] The EU, “Official Journal of the European Union, Directive(EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive)”, eur-lex.europa.eu, Dec. 2022
[39] CSIRTs NETWORK, csirtsnetwork.eu
[40] The EU, “Official Journal of the European Union, REGULATION (EU) 2019/881 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)”, eur-lex.europa.eu, April. 2019

[41] The European Council, "Cyber resilience act: Council and Parliament strike a deal on security requirements for digital products," www.consilium.europa.eu, Nov. 2023
[42] The EU, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020," COM/2022/454 final, eur-lex.europa.eu, 2022
[43] The EU, "Proposal for a Regulation of the European Parliament and of the Council on laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts," 2021/0106(COD), eur-lex.europa.eu, Apr. 2021
[44] ENISA, "Developing National Vulnerability Programs," www.enisa.europa.eu, Feb. 2023
[45] The EU, "Official Journal of the European Union, Directive(EU) 2013/40/EU OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA", eur-lex.europa.eu, Aug. 2013
[46] The EU, "Official Journal of the European Union, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)", eur-lex.europa.eu, Apr. 2016
[47] OECD, "Recommendation of the Council on Digital Security Risk Management," OECD/LEGAL/0479, legalinstruments.oecd.org, Sep. 2022
[48] OECD, "Recommendation of the Council on National Digital Security Strategy," OECD/LEGAL/0480, legalinstruments.oecd.org, Sep. 2022
[49] OECD, "Recommendation of the Council on Digital Security of Critical Activities," OECD/LEGAL/0456, legalinstruments.oecd.org, Dec. 2019
[50] OECD, "Recommendation of the Council on Digital Security Products and Services," OECD/LEGAL/0481, legalinstruments.oecd.org, Sep. 2022
[51] OECD, "Encouraging Vulnerability Treatment," https://one.oecd.org/document/DSTI/CDEP/SDE(2020)/12/FINAL/en/pdf, Feb. 2021
[52] Ministry of Government Legislation, "Criteria for drafting and reviewing legislation," pp. 8-39, www.lawmaking.go.kr, Dec. 2023
[53] T. Walshe, A.C. Simpson, "Coordinated Vulnerability Disclosure programme effectiveness: Issues and recommendations," Computers & Security Journal Volume 123, pp. 1-2. pp. 5-7, Dec. 2022
[54] Amit Elazari, "Private Ordering Shaping Cybersecurity Policy: The Case of Bug Bounties," pp. 3, pp. 7-13, pp. 26, pp. 33-41, papers.ssrn.com, Oct. 2019
[55] DANIEL ETCOVITCH, THYLA VAN DER MERWE, "Coming in from the Cold: A Safe Harbor from the CFAA and DMCA §1201 for Security Researchers," pp. 2-17, Harvard University, dash.harvard.edu, Jun. 2018
[56] Korean Law Information Center,

"Personal Information Protection Act," Act No. 19234, www.law.go.kr, Mar. 2023
〔57〕 Korean Law Information Center, "Copyright Act," Act No. 20358, www.law.go.kr, Feb. 2024
〔58〕 Ministry of Government Legislation, moleg.go.kr, legal interpretation case number 18-0583, Oct. 2018
〔59〕 PIPC, "Interpretation of the Personal Information Protection Act", pp. 37-29, pipc.go.kr, Dec. 2020
〔60〕 Hong Jun Ho, "A study on the Improvement of Legal System for Cyber Security," pp. 63-81, Interdisciplinary graduate program in IT law Graduate School of Dankook University, Dec. 2017

〈저자소개〉

이 태 승 (Taeseung Lee) 정회원
1994년 2월: 광운대학교 전자계산학과 졸업
1996년 2월: 포항공과대학교 컴퓨터공학과 석사
2014년 2월: 성균관대학교 컴퓨터공학과 박사
1996년 2월~2001년 12월 삼성전자 책임연구원
2002년 1월~현재: 한국인터넷진흥원 연구위원
〈관심분야〉 사이버보안 정책·법제도, 침해사고 예방·대응, AI 보안, 개인정보보호, ISMS