Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.33, NO.5, Oct. 2023 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2023.33.5.801

침해사고 신고의 실효성 제고를 위한 정보통신망법 개선 연구

이 태 승†‡
한국인터넷진흥원 (연구위원)

A Study on Improving the Act on Information and Communication Network for Enhancing the Effectiveness of Cyber Incident Reporting

Tae-seung Lee†‡
Korea Internet & Security Agency (Chief Researcher)

요 약

정보통신망 침해사고가 매년 증가하고 있는 가운데, 침해사고 신고율 등을 개선하기 위하여 관련법의 개정이 필요하다는 의견이 제기되고 있다. 이에, 본 논문은 침해사고 신고의 실효성을 향상시키기 위한 법 개선 방안을 제안한다. 먼저 국내 언론에서 보도된 침해사고 신고제도 관련 이슈를 분석하여 현행 침해사고 신고제도의 개선 필요사항으로 "미신고" 및 "적시 미신고"를 정의하고, 해외기관이 발표한 침해사고 신고 이슈사항과의 연관성 및 법 개정 필요성 분석을 통해 "신고 주체", "신고 기점", "신고 기한", "신고정보 보호"의 4가지 법 개정 요구사항을 도출한다. 마지막으로 국내외 입법례 분석을 통해 법 개정 요구사항에 대한 개선안을 제안한다.

ABSTRACT

With the cyber incidents increasing every year, opinions are being raised that legal system relating to incident reporting needs to be revised to improve the cyber incident reporting rate, etc. Accordingly, this paper suggests a legal improvement to enhance the effectiveness of cyber incident reporting. First, by analyzing domestic media coverage, this paper defines the problems which need to be improved regarding an incident reporting system as "unreported" and "not timely reporting". Then, this paper finds four requirements for legal improvement like "a reporting entity", "a starting point of reporting", "a reporting deadline" and "a protection of reporting information" by analyzing the relationship between reporting relating problems and issues published by overseas institutions and additionally by analyzing the need to revise the law. Finally, through an analysis of legislative cases, this paper suggests a legal improvement for the requirements.

Keywords: Cybersecurity, Cybersecurity Laws, Cyber Incident Reporting, Unreported, Not Timely Reporting

I. 서 론

'23년에 들어 샤오치잉 해커조직에 의한 웹변조 공격 및 국내 통신사의 고객정보 유출 등의 침해사고가 다발적으로 발생한 가운데, '22.12월 발표된 "2023 사이버 보안위협 전망"에 따르면 국내 침해사고 발생 건수는 Table 1.과 같이 매년 증가하고 있다[1].

하지만 실제로 발생한 침해사고는 신고 접수 건수보다 많을 것으로 예상되고 있으며 이를 개선하기 위해서는 침해사고 신고제도의 정비가 필요하다는 의견이 국내언론을 통해 보도되었다. '23.1월부터 '23.4월까지 국내 언론에서 보도된 침해사고 신고제도 관련 개선 필요사항은 Table 2.와 같다.

Received(06. 07. 2023), Accepted(08. 29. 2023)
† 주저자, tseung@kisa.or.kr
‡ 교신저자, tseung@kisa.or.kr(Corresponding author)

Table 1. Number of cyber incidents by year

Year	'19	'20	'21	'22.11.
Incidents	418	603	640	1,045

Table 2. domestic media coverage relating to cyber incident reporting system('23.1~'23.4)

domestic media	contents
www.ddaily.co.kr, www.etnews.com, news.bizwatch.co.kr, www.techm.kr, and others	o the need of improving incident reporting related legal system o the need of improving reporting rate o the need of improving timely reporting

우리나라의 침해사고 신고제도는 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 "정보통신망법"이라 한다)의 제48조의3에 근거하고 있으며, 정보통신망법 제48조의3 제1항의 "정보통신서비스 제공자는 침해사고가 발생하면 즉시 그 사실을 과학기술정보통신부장관이나 한국인터넷진흥원에 신고하여야 한다."에 따라 정보통신서비스 제공자에게 침해사고 신고 의무를 부여하고 있다[2].

본 논문은 정보통신망법에 따른 침해사고 신고제도가 현행 보다 더 잘 동작하기 위해서는 먼저 침해사고 신고제도와 관련하여 개선할 사항이 무엇인지 정의할 필요가 있다고 판단하였으며, 이에 국내언론에서 보도된 내용을 분석하여 신고제도의 개선 필요사항으로 2가지를 정의하였다. 첫 번째는 침해사고가 발생하여도 신고로 이어지지 않는 침해사고 "미신고"이다. "미신고"에는 침해사고 발생 자체를 모르는 경우와 침해사고 발생을 알았지만 신고를 하지 않는 신고 회피가 포함될 수 있다. 두 번째는 현행법에서는 "침해사고가 발생하면 즉시" 신고하도록 요구하고 있지만 사실확인 등 여러 요인으로 적시에 신고되지 않을 가능성이 있는 "적시 미신고" 이다.

본 논문은 침해사고 신고제도의 개선 필요사항인 "미신고" 및 "적시 미신고" 정의 및 원인 분석 등을 통한 법 개정 요구사항 도출, 국내외 입법례 분석을 통한 법 개정 요구사항별 개선안까지의 전 과정을 Fig.1.과 같이 제시한다.

본 논문의 2장은 해외기관이 발표한 침해사고 신고 관련 이슈사항에 기반하여 "미신고" 및 "적시 미신고의"의 원인을 분석하고 그 결과에 법 개정 필요성

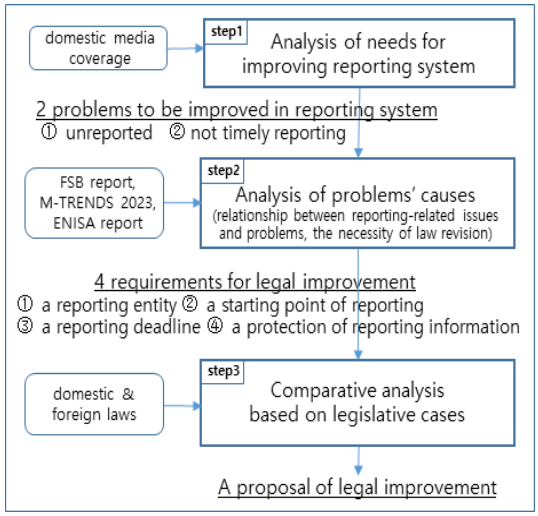

Fig. 1. A process from defining reporting-related problems to a proposal of legal improvement

을 추가적으로 분석하여 4가지 법 개정 요구사항을 도출한다. 3장에서는 국내외 입법례 분석을 통해 법 개정 요구사항에 대한 법 개선안을 제안하고, 4장은 법 개정 요구사항별 개선안을 종합하여 설명한다. 5장에서는 본 논문이 제안한 Fig.1.의 모든 과정을 요약 설명하고, 침해사고의 피해확산 방지를 위한 침해사고 신고제도의 목적을 충족하기 위해서는 법 개선과 함께 침해사고 신고에 대한 인식 제고, 침해사고 대응 역량 강화 등의 노력이 병행해야 되어야 함을 설명하는 것으로 본 논문을 마무리 한다.

II. 법 개정 요구사항

2장에서는 침해사고 신고제도의 개선 필요사항인 "미신고" 및 "적시 미신고"의 원인을 파악하기 위하여 해외기관이 발표한 침해사고 신고 이슈사항 관련 3종 보고서를 분석한다.

2.1절부터 2.3절은 각 보고서의 신고 관련 이슈사항을 설명하고, 각 보고서의 이슈사항과 "미신고" 및 "적시 미신고"와의 연관성 및 법 개정 필요성을 분석하여 "신고 주체", "신고 기점", "신고 기한", "신고정보 보호"의 4가지 법 개정 요구사항을 도출한다.

2.1 FSB의 침해사고 신고 향상 권고사항

국제금융안정위원회(FSB)가 '23.4.13일에 발표

한 “침해사고 신고 컨버전스 향상을 위한 권고사항” 보고서는 금융기관이 현실적으로 직면하고 있는 신고 관련 이슈사항 및 적시 신고를 막는 저해요인을 설명하고 있으며, 이에 대한 개선을 권고하고 있다[3].

2.1.1 신고 이슈사항(6종) 및 적시 신고 저해요인(6종)

국제금융안정위원회(FSB) 보고서에서 설명하는 금융기관이 현실적으로 직면하고 있는 6가지 침해사고 신고 관련 이슈사항은 Table 3.과 같다.

첫 번째 신고 관련 이슈사항 (1)은 운영상의 이슈로서 다양한 사이버보안 제도에서 요구하는 신고의무를 준수해야 하는 어려움이다. 유럽의 경우 유럽사이버보안지침(NIS), 신뢰서비스지침(eIDAS), 개인정보보호법(GDPR) 등에서 침해사고 신고를 요구하고 있다. 두 번째 이슈사항 (2)는 적절한 신고기한 임계값 부여이다. 세 번째 이슈사항 (3)은 Table 4.에서 설명하고 있는 적시 신고를 막는 6가지 저해요인이다. 세부적으로 살펴보면, 첫 번째 저해요인 (3)①은 적시 신고 필요성에 대한 인식 부족, 두 번째 저해요인 (3)②는 신고에 따른 조직의 이미지 실추 및 관련당국 조사에 대한 두려움, 세 번째 저해요인 (3)③은 침해사고 발견 역량 부족, 네 번째 저해요인 (3)④는 여러 해석이 가능한 불명확한 신고 규정, 다섯 번째 저해요인 (3)⑤는 부절적한 내부 절차, 마지막으로 여섯 번째 저해요인 (3)⑥은 신고에 대한 조직 내부 신뢰 부족이다. 다시 신고 관련 이슈사항 설명을 이어가면, 네 번째 신고 관련 이슈사항 (4)는 침해사고 영향분석의 어려움, 다섯 번째 이슈사항 (5)는 신고정보 보호, 마지막 여섯 번째 이슈사항 (6)은 제도간 신고정보 공유이다.

Table 3. 6 practical issues to achieve greater convergence in cyber incident reporting

category	reporting-related issues
(1)	operational challenges
(2)	setting reporting criteria
(3)	culture of timely reporting
(4)	early assessment challenges
(5)	secure communications
(6)	cross-border and cross-sectoral issues

Table 4. 6 factors impeding timely reporting of the reporting-related issue (3)

category	6 factors impeding timely reporting
(3)①	a lack of awareness
(3)②	a fear of reputation damage and scrutiny from the authority
(3)③	inadequate detection capabilities
(3)④	unclear reporting requirements open to interpretation
(3)⑤	inadequate internal reporting procedures
(3)⑥	a lack of trust on organizational units

2.1.2 신고 이슈사항 연관성 및 법 개정 필요성 분석

본 절은 앞 절에서 설명한 FSB 보고서의 침해사고 신고 관련 이슈사항과 1장에서 침해사고 신고제도의 개선 필요사항으로 정의한 “미신고”, “적시 미신고”와의 연관성 및 법 개정 필요성을 분석함으로써 법 개정 요구사항을 도출한다.

먼저 본 절에서는 FSB 보고서의 6가지 침해사고 신고 관련 이슈사항 및 6가지 적시 신고 저해요인을 내용 유사성을 기준으로 8가지 이슈사항으로 재분류하였다. 재분류 과정을 설명하면, 신고 이슈사항 (1)과 (6)은 침해사고 신고제도와 관련된 사항이라고 판단하여 하나로 묶었고, 이슈사항 (3)은 (3)의 세부내용인 6가지 적시 신고 저해요인으로 대체하였다. 이슈사항 (4)는 저해요인 (3)③과 역량 측면에서 유사하다고 판단하여 하나로 묶었고, (3)⑤와 (3)⑥은 조직 내 신고 절차와 관련되어 하나로 묶었다.

법 개정 요구사항을 도출하기 위하여 재분류한 8가지 이슈사항과 “미신고”, “적시 미신고”와의 연관성을 분석하였고, 연관성이 있는 경우 법 개정을 통해 개선할 사항인지 여부를 추가로 분석하였다.

Table 5.의 분석 결과를 살펴보면, 다양한 제도에서 요구되는 이슈사항 (1)과 제도간 신고정보 공유 이슈사항 (6)은 “미신고”, “적시 미신고”와는 연관성이 있지만 법 개정 필요성은 없다고 판단하였다. 법 개정 필요성이 없다고 판단한 이유는 ’22.6.10 일자 정보통신망법 개정에서, 제48조의3의 제1항 후단(“이 경우 정보통신서비스 제공자가 이미 다른 법률에 따른 침해사고 통지 또는 신고를 했으면 전단에 따른 신고를 한 것으로 본다.”)과 제3항(“제1항 후단에 따른 침해사고의 통지 또는 신고를 받은 관계 기관의 장은 이와 관련된 정보를 과학기술정보통신부장관 또는 한국인터넷진흥원에 지체 없이 공유하여야

한다.")이 신설되었기 때문이다[2]. 신고 이슈사항 (2)의 적절한 신고기한 임계값 부여는 "적시 미신고"와 연관성이 있다고 판단하였고, 이는 법 개정을 통해 개선할 사항이라고 판단하였다. 이슈사항 (3)①의 적시 신고 필요성에 대한 인식 부족은 "적시 미신고"와 연관성은 있지만, 법 개정이 아닌 교육·훈련을 통해 개선할 사항이라고 판단하였다. 이슈사항 (3)②의 신고에 따른 기관의 이미지 및 관련기관 조사에 대한 두려움은 "미신고"와 연관성이 있지만, 조직의 침해사고 신고 부담감에 해당하는 사항이어서 법 개정 보다는 인식 제고 등을 통해 개선할 사항이라고 판단하였다. 이슈사항 (3)③과 (4)의 역량부족은 "적시 미신고"와 연관되지만 법 개정이 아닌 침해사고 탐지·대응 관련 역량 강화를 통해 개선할 사항이라고 판단하였다. 이슈사항 (3)④의 여러 해석이 가능한 불명확한 신고 규정은 "적시 미신고" 와 연관되고 정보통신망법 제48조의3 제1항의 신고기준에 대한 법 개정이 필요한 사항이라고 판단하였다. 이슈사항 (3)⑤의 부적절한 조직 내부 보고 절차와 (3)⑥의 조직 내부의 신고에 대한 신뢰 부족은 "미신고" 및 "적시 미신고"에 해당되나 법 개정사항은 아닌 인식 제고 등을 통해 개선할 사항이라고 판단하였다. 이슈사항 (5)의 신고정보의 보호는 "미신고"와 연관성이 있고 법 개정이 요구된다고 판단하였다.

Table 5. An analysis for deriving requirements for legal improvement

reclassified reporting-related issues	A	B	A & B
	reporting-related problems (unreported, not timely reporting)	a need of law revision	legal improving requirements
(1), (6)	○	X	X
(2)	○	○	O
(3)①	○	X	X
(3)②	○	X	X
(3)③, (4)	○	X	X
(3)④	○	○	O
(3)⑤, (3)⑥	○	X	X
(5)	○	○	O

2.1.3 법 개정 요구사항 도출

앞 절의 신고 관련 이슈사항과의 연관성 및 법 개정 필요성 분석 결과를 기반으로, 본 절은 이슈사항 (2)에 따른 "신고 기한", 이슈사항 (3)④에 따른 "신고 기점", 이슈사항 (5)에 따른 "신고정보 보호" 등 3가지 법 개정 요구사항을 도출하였다.

2.2 M-TRENDS 2023

구글이 인수한 보안기업 맨디언트(MANDIANT)가 '23.4.18일 발표한 "M-TRENDS 2023" 보고서는 '22년 침해사고 발견 출처의 63%가 외부이고 37%가 내부임을 설명하고 있다[4]. 침해사고 외부 발견은 외부 기관이 침해사고로 인한 피해 사실을 해당 기관에게 알려주었음을 의미하고, 내부 발견은 해당 기관이 독립적으로 피해 사실을 발견한 것을 의미한다. Fig.2.의 침해사고 발견 출처를 권역별로 살펴보면 북남미 권역은 외부 발견이 55%, 내부 발견이 45%로 비슷한 반면, 아시아·태평양 권역은 외부가 67%, 내부가 33%로 2배 이상 차이가 나고, 유럽·중동·아프리카 권역은 외부 발견이 74%, 내부 발견이 32%로 2.8배 이상 차이가 남을 알 수 있다. 이를 통해 모든 권역에서 침해사고 발견의 외부 의존도가 높은 가운데 특히 북미권을 제외한 권역에서 외부 발견의 의존도가 매우 높음을 알 수 있다.

본 절은 "M-TRENDS 2023"에서 설명하는 침해사고 발견 출처가 "미신고"와 연관성이 있으며 정보통신망법 제48조의3의 "신고 주체"에 해당한다고 판단하였다. 따라서 제48조의3 제1항의 "신고 주체"에 외부 출처가 추가될 필요가 있다고 판단하였다.

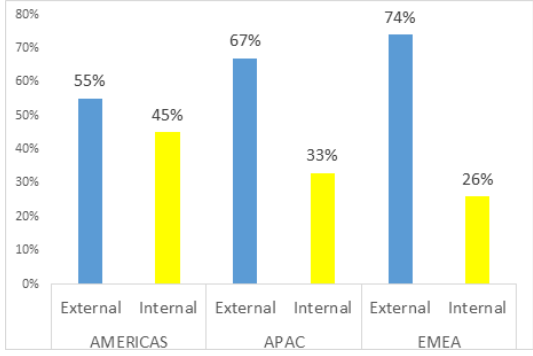

Fig. 2. Cyber Incident detection by external or internal source

2.3 EU의 침해사고 신고 모범사례

유럽사이버보안원(ENISA)이 2009년에 발표한 “침해사고 신고 모범사례” 보고서는 유럽 회원국의 침해사고대응조직(CERT), 통신사, 규제기관 등의 침해사고 신고 모범사례를 설명하고 있으며, 이중 독일의 통신서비스 규제기관인 Bundesnetzagentur는 시민 또는 언론으로부터 많은 침해사고 정보를 획득하고 있음을 설명하고 있다[5]. 이는 2.2절에서와 같이 “신고 주체”와 관련된 법 개정 요구사항이라고 판단하였다.

2.4 법 개정 요구사항(4종)

앞 절에서 도출한 법 개정 요구사항을 종합하면, 2.1절로부터 “신고 기점”, “신고 기한”, “신고정보 보호” 3가지 법 개정 요구사항을 도출하였고, 2.2절과 2.3절로부터는 “신고 주체” 요구사항을 도출하여 총 4가지 법 개정 요구사항을 도출하였다.

III. 법 개정 요구사항에 대한 법 개선안

3장에서는 우리나라를 비롯한 미국, 유럽, 호주의 침해사고 신고제도 관련 입법례 분석을 통해, 2장에서 도출한 4가지 법 개정 요구사항에 대한 법 개선안을 제안한다.

3.1 신고 주체(a reporting entity)

현행 정보통신망법 제48조의3은 침해사고 “신고 주체”를 정보통신서비스 제공자로 규정하고 있다[2]. 하지만 2장에서 살펴본 바와 같이 외부 출처를 통한 침해사고 발견 의존도가 높은 점을 고려할 때, 침해사고 확산 방지라는 침해사고 신고제도의 목적을 충족하기 위해서는 “신고 주체”를 확대할 필요가 있다고 판단하였다. 이에 본 절은 현행 신고 주체인 “정보통신서비스 제공자” 외에 침해사고 신고를 할 수 있는 주체로 “누구든지”를 추가하는 방안을 제안한다.

신고 주체를 “누구든지”로 규정하고 있는 국내법은 공익신고자보호법이 있으며, 제6조에서 “누구든지 공익침해행위가 발생하였거나 발생할 우려가 있다고 인정하는 경우에는 〈중략〉 공익신고를 할 수 있다”로 규정하고 있다[6]. 미국 연방정보보안현대화법(FISMA)은 신고 주체를 연방기관으로 명시하고 있으며[7], 이에 기반하여 침해사고 신고 제도를 운영중인 사이버보안·인프라보호청(CISA)의 신고 홈페이지는 “신고 주체”에 개인을 포함하고 있다[8]. Table 6.은 “신고 주체” 관련 국내외 입법례를 소개하고 있다.

또한 Table 7.의 국외 입법례를 살펴보면 침해사고 신고 대상을 실제 발생한 침해사고로 한정하여 규정하고 있는 정보통신망법과는 달리, 미국 연방정보보안현대화법(FISMA)은 침해사고 용어에 해당하는 “incident”에 실제 발생을 비롯하여 임박한(imminent) 위험 또는 위협을 포함하며[7], 유럽 사이버보안지침(NIS2)은 침해사고로 의심되는 경우 조기경고(early warning)를 하도록 규정하고 있다[11]. 호주 주요기반보호법(SOCI Act)은 실제 발생한 침해사고 뿐만 아니라 침해사고가 자산에 영향을 미쳤거나, 미치고 있는 중, 미칠 가능성이 있는 경우도 침해사고 신고 대상에 포함하고 있다[12].

Table 6. Laws relating to a reporting entity

related laws	a reporting entity
Public Interest Whistleblower Protection Act (Korea)	(Article 6) Any person
FISMA 2014 (US)	(§3554) Federal Agency ※ Reporting System (www.cisa.gov) ☐ the impacted user ☐ reporting on behalf of the impacted user ※ Types of reporting entity's organizations include an individual
Act on the Protection of Information and Communication Infrastructure[9] (Korea)	(Article 13) The head of a management organization
Personal Information Protection Act[10] (Korea)	(Article 34) Personal Information Controller
NIS2[11] (EU)	(Article 23) Essential or important entities in each member state
SOCI Act[12] (Australia)	(30BA) The responsible entity for the asset

Table 7. Laws including reporting incident occurrence and reporting incident possibility

related laws	types of reporting target
FISMA 2014 (US)	(§3552) 'incident' means an occurrence that (A) actually or imminently jeopardizes, without lawful authority, 〈 *omitted* 〉 or (B) constitutes a violation or imminent threat of violation of law, security policies 〈 *omitted* 〉
NIS2 (EU)	(Article 23) early warning. which, where applicable, shall indicate whether the significant incident is suspect of being caused by unlawful or malicious acts 〈 *omitted* 〉
SOCI Act (Australia)	(30BD) (i) a cyber security incident has occurred, is occurring or is imminent; and (ii) the incident has had, is having, or is likely to have, a relevant impact on the asset

따라서 본 절은 신고 의무 주체로 "정보통신서비스 제공자"를 규정하고 있는 현행 정보통신망법 제48조의3에 신고할 수 있는 주체로서의 "누구든지" 및 침해사고 우려가 높은 임박한 경우를 신고 대상으로 추가하는 개선안을 Table 8.과 같이 제시한다. 이를 통해 침해사고 발견 외부 출처인 제3자의 신고(제보)를 수용할 수 있으며 침해사고 신고의 목적을 침해사고 예방까지로 확대할 수 있을 것으로 기대된다. 다만 신고 대상 등의 추가로 발생할 수 있는 부정한 목적의 신고 등은 충분한 검토가 필요할 것이다.

Table 8. A proposal of legal improvement relating to a reporting entity of article 48-3

As-Is	To-be
Provider of information and communications services shall report the cyber incident	① Any person can report the actually occurred or imminent incident.
	② Where any person under clause ① is a provider of information and communication service, the provider shall immediately report the occurrence of incident.

3.2 신고 기점(a starting point of reporting)

현행 정보통신망법 제48조의3은 침해사고 신고 의무 발생 시점을 "정보통신서비스 제공자는 침해사고가 발생하면 즉시"로 규정하고 있다[2]. 이에 반해 Table 9.에서 설명하는 국내외 신고 관련법은 신고 의무 발생 시점을 신고 주체가 침해사고 발생 사실을 "인지한 때" 또는 "알게 된 때"로 명확히 규정하고 있다. 정보통신기반보호법 제13조는 "인지한 때"로 규정하고 있으며[9], 개인정보보호법 제34조는 "알게 된 때"로 규정하고 있다[10]. 미국 연방정보보안현대화법(FISMA)의 하위규정인 미 관리예산처(OMB)의 M-15-01은 "확인된 손실이 기관의 최상위 조직에 도달한 때"로 규정하고 있으며[13], 유럽사이버보안지침(NIS2) 제23조와 호주 주요기반보호법(SOCI Act)의 30BD는 "알게 된"(becoming

Table 9. Laws relating a starting point of reporting

related laws	a starting point of reporting
Act on the Protection of Information and Communication Infrastructure (Korea)	(Article 13) When the head of a management organization recognizes that the occurrence of incidents
Personal Information Protection Act (Korea)	(Article 34) when the personal information controller becomes aware of leakage of personal information
OMB M-15-01 based on FISMA 2014 (US)	Federal agencies to notify 〈 *omitted* 〉 with confirmed loss of 〈 *omitted* 〉 of reaching the agency's top-level CSIRT, SOC, or IT department.
NIS2 (EU)	(Article 23) early warning 〈 *omitted* 〉 of becoming aware of the significant incident,
SOCI Act (Australia)	(30BD) the entity becomes aware that: 〈 *omitted* 〉

aware of)" 경우로 규정하고 있다[11][12].

따라서 본 절은 현행 정보통신망법 제48조의3에 규정된 "정보통신서비스 제공자는 침해사고가 발생하면"을 "정보통신서비스 제공자가 침해사고 발생 사실을 알게 된 때"로 개정할 것을 제안한다. 이를 통해 침해사고 발생의 인지 주체를 명확하게 규정함과 동시에 "알 게 된 때"를 "신고 기점"으로 명확히 정할 수 있을 것이다.

하지만, 여전히 침해사고 발생 사실을 안 때를 신고 기점으로 하는 것만으로는 불명확성이 존재한다. 즉, 침해사고 발생 사실을 안 때를 특정하기 어렵기 때문이다. 따라서 본 절은 Fig.3.의 ①과 ②를 침해사고 "신고 기점"으로 고려하는 방안을 제안한다.

Fig.3. ①은 침해사고가 가시적이어서 다른 침해사고 보다는 침해사고 발생 여부를 쉽게 알 수 있는 경우이다. 웹변조, 랜섬웨어 공격 등으로 인한 침해사고가 이에 해당 될 수 있으며 이 경우 침해사고 발생 시점을 "신고 기점"으로 고려 할 수 있을 것이다. Fig.3. ②(i)는 침해사고 발생 사실을 관련 기관으로부터 안내받은 경우이다. 이 경우 침해사고 안내받은 시점이 신고 기점으로 고려될 수 있다. Fig.3. ②(ii)는 외부출처에 침해사고 관련 사항이 공개된 경우로 외부출처에 공개된 시점이 신고 기점으로 고려될 수 있다. 다만 외부출처의 범위는 명확히 정할 필요가 있다. 이는 정보통신서비스 제공자의 침해사고 발견 역량과도 관련된 부분이어서 침해사고가 국민에게 큰 영향을 미치는 주요정보통신서비스 제공자와 그 밖의 중소 정보통신서비스 제공자로 구분하여 주요정보통신서비스 제공자에게 우선 적용하는 것을 고려할 수 있다. 또한 주요정보통신서비스 제공자에게 적용되는 외부출처 범위는 국내 언론뿐만 아니라 해킹 관련 사이트 등이 고려될 수 있을 것이다.

Table 10.은 본 절에서 제안한 침해사고 신고 의무 발생 시점인 신고 기점과 신고 기점으로 고려될

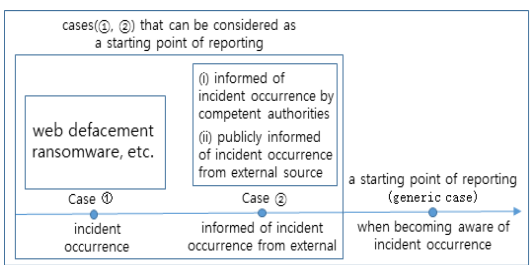

Fig. 3. Cases(①, ②) that can be considered as a starting point of reporting

Table 10. A proposal of legal improvement relating a starting point of reporting of article 48-3

As-Is	To-be
If a cyber incident occurs, a provider of information and communications services	When a provider of information and communications services becomes aware of the occurrence of cyber incident
〈 newly added 〉	Below (i) and (ii) can be considered as the time of becoming aware of incident occurrence (i) the time of incident occurrences like web defacement and ransomware (ii) when the incident is informed from external source

수 있는 경우를 포함한 개선안이다.

3.3 신고 기한(a reporting deadline)

본 절은 국내외 입법례를 기반하여 정보통신망법 제48조의3의 "즉시"에 대한 신고 기한을 정함으로써 신고의 즉시성을 명확히 하는 방안을 제안한다. 법제처의 법령 용어는 "즉시"와 "지체 없이"를 다음과 같이 정의하고 있다[14]. "즉시"는 "어떤 일이 행하여지는 바로 그때"라는 뜻으로 시간적 즉시성이 좀 더 강하다. "지체 없이"는 시간적 즉시성이 강하게 요구되지만 정당하거나 합리적인 이유에 따른 지체는 허용되는 것으로 해석되며, 사정이 허락하는 범위에서 가장 신속하게 해야 한다는 뜻으로 사용한다.

일부 국내법에서는 "즉시"에 대한 기한을 시행령 등에서 세부적으로 정하고 있다. 민원처리법 시행령 제19조는 민원의 처리기간을 "즉시"로 정한 경우에는 정당한 사유가 있는 경우를 제외하고는 3근무시간 이내로 규정하고 있고[15], 병적정리 매뉴얼에 관한 규정 제2조는 "즉시"를 1일 이내로 규정하고 있으며[16], 화학물질관리법에 따른 화학사고 즉시 신고에 관한 규정 제3조는 화학사고의 상황별로 즉시 신고 기준을 15분 이내 등으로 규정하고 있다[17].

국외 입법례에서는 Table 11.과 같이 침해사고 발생 사실을 인지한 이후부터 일정 시간을 신고 기한으로 부여하고 있다. 미국 연방정보보안현대화법(FISMA)에 따른 미 관리예산처(OMB)의 M-15-01은 1시간 이내[13], 유럽 사이버보안지침(NIS2)는 지체 없이 24시간 이내[11], 호주 주요 기반보호법(SOCI Act)은 중요 침해사고는 12시간 이내, 일반 침해사고는 72시간 이내로 이원화하여 규정하고 있다[12]. 그 밖에 '22.5.24일자 MEDIANAMA 사이트는 프랑스, 이탈리아, 스페인, 영국, 일본, 싱가포르, 인도, 인도네시아의 침해사고 신고 기한이 서비스 분야별로 다양함을 설명하고 있다[18]. 이를 종합하면 침해사고 신고 기한을 신고 주체, 서비스 분야, 침해사고의 영향 등을 고려하여 1시간부터 72시간 이내에서 정하고 있음을 알 수 있다.

따라서 본 절에서는 국내외 입법례를 기반하여 "즉시"에 대한 침해사고 신고기한을 1시간부터 72시간 범위 내에서 신고 주체, 서비스 분야, 침해사고 영향 등을 고려하여 Table 12.와 같이 시행령에 구체적으로 정하는 방안을 제안한다.

Table 11. Laws relating to a reporting deadline

related laws	a reporting deadline
OMB M-15-01 based on FISMA 2014 (US)	within one hour
NIS2 (EU)	(Article 23) early warning without undue delay and in any event within 24 hours
SOCI Act (Australia)	(30BC) within 12 hours in significant incident (30BD) within 72 hours in incident

Table 12. A proposal of legal improvement relating a reporting deadline of article 48-3

As-Is	To-be
immediately	(In Act) immediately (In Enforcement Decree) within 1~72 hours ※ it needs to define the specific deadline with consideration of reporting entity, the effect of incident, etc

3.4 신고정보 보호(a protection of reporting information)

본 절은 현행 정보통신망법 제48조의3에 침해사고 신고정보의 보호 규정을 신설하는 방안을 제안한다. Table 13.의 국내외 입법례는 신고정보의 보호와 관련된 사항을 규정하고 있다. 개인정보보호법 제34조는 개인정보 유출시 신고해야하는 정보를 규정하고 있다. 미국 연방정보보안현대화법(FISMA)은 신고 처리에 대한 표준과 가이드를 마련하고 미국표준기술연구소(NIST)와 협의할 것을 규정하고 있으며, 이에 따라 사이버보안·인프라보호청(CISA)은 NIST SP 800-61 Rev2[19] 및 US-CERT Federal Incident Notification Guideline[20]에 기반하여 침해사고 신고를 받고 있다. 호주의 주요기반보호법(SOCI Act)은 수집과 이용 측면에서의 신고정보 보호를 규정하고 있다.

따라서 본 절은 국내외 입법례를 기반하여 정보통신망법 제48조의3에 신고정보 보호에 관한 조항 신설을 Table 14.와 같이 제안한다.

Table 13. Laws relating to a protection of reporting information

related laws	a protection of reporting information
Personal Information Protection Act (Korea)	(Article 34) reporting information when personal information leakage
FISMA 2014 (US)	(§3553, §3556) standards and guidelines of reporting
SOCI Act (Australia)	(Part 4) gathering and using reporting information

Table 14. A proposal of legal improvement relating a protection of reporting information

As-Is	To-be
〈 newly added 〉	Reporting information shall be protected safely. ※ The details of a protection of reporting information shall be prescribed by enforcement deecree

IV. 침해사고 신고 관련 법 개선안

4장은 3장에서 제안한 법 개정 요구사항에 대한 법 개선안을 종합하여 설명한다.

“신고 주체”와 관련하여 현행 신고 의무 주체인 “정보통신서비스 제공자” 외에 “누구든지”를 신고를 할 수 있는 주체로 추가하고, 침해사고 발생 뿐만 아니라 침해사고 가능성이 높은 경우도 신고 대상에 추가하는 방안을 제안하였다. “신고 기점”과 관련하여 현행 “정보통신서비스 제공자는 침해사고가 발생하면”을 “정보통신서비스 제공자가 침해사고 발생 사실을 알게 된 때”로 개정하여 신고 주체의 침해사고 발생 인지를 명확히 하고, “신고 기점”으로 고려될 수 있는 경우를 제안하였다. “신고 기한”과 관련하여서는 “즉시”에 대한 “신고 기한”을 국내외 입법례를 기반하여 1~72시간 범위에서 신고 주체 및 침해사고의 영향 수준 등을 고려하여 시행령에 세부적으로 정하는 방안을 제안하였다. 마지막으로 신고정보의 보호를 국내외 입법례를 기반하여 신설하는 방안을 제안하였다. Table 15.는 본 논문이 제안한 정보통신망법 제48조의3의 제1항 전단에 대한 개선안이다.

Table 15. A proposal of legal improvement of the front part of clause 1 of article 48-3

As-Is	To-be
① If a cyber incident occurs, a provider of information and communication services shall immediately report the fact of incident to MSIT or KISA.	① Any person can report a cyber incident to MSIT or KISA when becoming aware of the actually occurred incident or imminent incident
〈 newly added 〉	② Where any person under clause ① is a provider of information and communication service, the provider shall immediately report the incident. ※ In an enforcement decree, it needs to define the specific deadline within 1~72 hours of becoming aware of the incident occurrence with consideration of reporting entity, the effect of incident, etc
〈 newly added 〉	③ Below (i) and (ii) can be considered as the time of becoming aware of incident occurrence. (i) the time of incident occurrences like web defacement and ransomware (ii) when the incident is informed from external source
〈 newly added 〉	④ Reporting information shall be protected safely.
〈 newly added 〉	⑤ The details from ① to ④ shall be prescribed by enforcement decree.

V. 결 론

본 논문은 침해사고 예방·대응에 있어 중요한 역할을 수행하는 침해사고 신고의 실효성을 향상시키기 위한 법 개선안 마련 과정을 제시하였다. 첫 번째 단계로 국내 언론보도 내용을 분석하여 현행 정보통신망법의 침해사고 신고제도 관련 개선 필요사항으로 “미신고” 및 “적시 미신고”를 정의하였다. 두 번째 단계는 “미신고” 및 “적시 미신고”의 원인을 파악하기 위하여 해외기관이 발표한 침해사고 신고 관련 이슈사항과의 연관성 분석 및 법 개정 필요성을 분석하였고, 이를 통해 4가지 법 개정 요구사항인 “신고 주체”, “신고 기점”, “신고 기한”, “신고정보 보호”를 도출하였다. 마지막 단계는 국내외 입법례를 분석하여 법 개정 요구사항에 대한 법 개선안을 제안하였다. 본 논문에서 제안한 법 개선안은 “미신고”, “적시 미신고” 측면에서 침해사고 신고제도의 실효성을 향상시킬 것으로 기대된다.

하지만 앞서 2장에 언급한 바와 같이, 침해사고 신고제도가 침해사고 확산 방지라는 목적을 충족하기 위해서는 법제도 개선 뿐만 아니라 침해사고 신고 중요성에 관한 인식 제고와 신속한 침해사고 발견·대응을 위한 역량 향상이 함께 병행되어야 할 것이다.

References

[1] Ministry of Science and ICT and Korea Internet & Security Agency, "Cyber Security Forecast 2023," www.krcert.or.kr, pp. 5, Dec. 2022

[2] "Act on Promotion of Information and Communications Network Utilization and Information Protection," www.law.go.kr, article 48-3, Jan. 2023

[3] Financial Stability Board, "Recommendations to Achieve Greater Convergence in Cyber Incident Reporting," FSB Final Report, pp. 9-23, Apr. 2023

[4] MANDIANT, "M-TRENDS 2023," MANDIANT SPECIAL REPORT, pp. 6-9, Apr. 2023

[5] ENISA, "Good Practices on Reporting Security Incidents," www.enisa.europa.eu, pp. 26, 2009

[6] "Public Interest Whistleblower Protection Act," www.law.go.kr, article 6, Apr. 2022

[7] "Federal Information Security Modernization Act of 2014," www.congress.gov, §3552-§3554, §3556, Dec. 2014

[8] CISA, "Incident Reporting System," www.cisa.gov/forms/report

[9] "Act on the Protection of Information and Communication Infrastructure," www.law.go.kr, article 13, Sep. 2022

[10] "Personal Information Protection Act," www.law.go.kr, article 34, Mar. 2023

[11] "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," www.europa.eu, article 6 & article 23, Dec. 2022

[12] "Security of Critical Infrastructure Act 2018," www.legislation.gov.au, pp. 101-104, pp. 179-190, 2018

[13] OMB, "Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices," M-15-01, pp. 12, Oct. 2014

[14] Ministry of Government Legislation, "Criteria for Drafting and Reviewing of Legal," www.lawmaking.go.kr, pp. 788, Dec. 2022

[15] "Enforcement Decree of the Civil Petitions Treatment Act," www.law.go.kr, article 19, Jul. 2022

[16] "Regulation on the Military Registration Manual," www.law.go.kr, article 2, Jun. 2020

[17] "Regulation on Immediate Reporting of Chemical Incident," www.law.go.kr, article 3, Apr. 2021

[18] MEDIANAMA, "Fact Check: Do Other Countries Have Lesser Than 6 Hours To Report Cybersecurity Incidents?," www.medianama.com, May 2022

[19] NIST, "Computer Security Incident Handling Guide," Special Publication 800-61 Rev2, pp. 21-44, Aug. 2012

[20] CISA, "US-CERT Federal Incident Notification Guidelines," www.cisa.gov, pp. 1-9, Apr. 2017

〈저자소개〉

이 태 승 (Tae-seung 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, 개인정보보호, CC인증, ISMS