Journal of the Korea Academia-Industrial cooperation Society
Vol. 24, No. 9 pp. 275-282, 2023

https://doi.org/10.5762/KAIS.2023.24.9.275
ISSN 1975-4701 / eISSN 2288-4688

중소기업에 일반적으로 나타나는 정보보호 취약점 분석
-방산관련업체를 중심으로-

이상열, 유연승*
명지대학교 보안경영공학과

Analysis of Information Protection Vulnerabilities Small and Medium-sized Enterprises: Focusing on Defense-related Companies

Sang Yeol Lee, Yeon Seung Ryu*
Department of Security Management Engineering, Myungji University

요 약 오늘날 정보통신기술의 발달로 급속한 정보화의 물결과 맞물려 산업기밀 유출 등 다양한 역기능으로 인해 기업의 피해가 점차 늘어나고 있으며 중소기업이 전체의 88.5%를 차지하고 있다. 이러한 환경 속에서 중소기업 중 방위산업물자의 구성품을 생산하는 방산관련업체의 정보 유출 피해를 예방하고자 보안측정 자가진단 결괏값을 바탕으로 정보보호 분야 무선 LAN 관리, 디지털복합기 관리, 네트워크 관리, 전산자료 관리, 개인·휴대형 컴퓨터 관리, 보조기억매체 관리, 정보보호시스템 관리 등 7개 분야 28개 항목에 대해 일반적으로 나타나는 취약점을 분석하였다. 분석결과로 서비스 허용 범위를 고려한 AP(Access Point) 설치 위치와 물리적 보호, 숨김모드 미사용, 메모리자동 소거 기능 비활성화, 로그파일 보관 누락, 정보체계 사용자에게 개별적 사용자 계정 부여, 계정별 주요 정보시스템 접근 권한 부여, 서버와 네트워크 장비의 주기적 비밀번호 변경, 자료의 유출·파괴에 대한 보안대책, 사용자가 시스템 접근 시 로그 관리, 보안에 취약한 프로그램의 임의 사용 제한, 필수 프로그램 설치 운용 등이 일반적인 취약점으로 나타났다. 이러한 일반적으로 나타나는 취약점들은 기술적인 면보다 보안정책 설정이 미흡한 것으로 이를 개선하기 위해 담당자들에 대한 관련 교육의 필요성과 함께 본 연구가 이러한 취약점을 해소하는데 활용될 것으로 기대된다.

Abstract With the development of information and communication technology, corporate damage is gradually increasing due to various adverse effects, such as leakage of industrial secrets, and SMEs account for 88.5% of the total effects. In this environment, 28 general vulnerabilities in seven categories were analyzed: wireless LAN management, digital complex management, network management, computer data management, personal and portable computer management, auxiliary storage media management, and information protection system management. The analysis found that AP installation locations, physical protection, non-hidden mode, and automatic memory erasure functions were disabled, and log file storage was omitted. Furthermore, information system users were given individual user accounts, periodic password changes of servers and network equipment, security measures against data leakage and destruction, log management, and mandatory program installation. These general vulnerabilities are expected to be addressed along with the need for related education for those in charge to improve the security policy setting than in the technical aspect.

Keywords : Defense-related Companies, Information Protection, Measurement of Security, Vulnerabilitiy, Security Policy Setting

*Corresponding Author : Yeon Seung Ryu(Myungji Univ.)
email: ysryu@mju.ac.kr
Received June 21, 2023 Revised July 6, 2023
Accepted September 1, 2023 Published September 30, 2023

1. 서론

오늘날 우리는 정보통신기술의 발달로 빅데이터, 모바일, 인공지능 등의 기술을 이용한 편리하고 고도로 발전된 지능정보사회에 살아가고 있다.이러한 환경에서 방대하고 다양한 기업 정보의 수집과 이에 대한 활발한 이용이 이루어지게 되는데[1], 그 속에 필연적으로 방위사업과 과련된 정보도 포함될 수 밖에 없다. 또한, 초고속 인터넷의 보급과 더불어 인터넷 사용은 개인, 기업, 공공분야 등 전 분야에 걸쳐 보편화되었고, 급속한 정보화의 물결과 맞물려 산업기밀 유출 등 다양한 역기능으로 인해 기업의 피해가 점차 늘어나고 있는 것이 현실이다[2]. 2022년 한국인터넷진흥원이 공개한 연도별 전체 침해사고 건수에 의하면 전체신고 건수는 2021년 640건, 2022년 (1월~11월) 1,045건으로 매년 증가 추세이며, 중소기업이 전체의 88.5%를 차지하고 있다[3]. 침해사고 유형은 랜섬웨어(47.7%), 악성코드(41.9%), 해킹(11.4%), DoS/DDoS(1.8%) 순으로 랜섬웨어가 가장 위협적인 요소였으며[4], 대표적인 사고사례로 2021년 1월 현대자동차 러시아 법인 130만 명 고객의 개인정보 유출, 2월 기아차 북미법인 샘플 유출, 3월 현대자동차그룹의 내부자료 3.2GB 분량 다크웹에 유출, 5월 하도급 제조업 서비스 및 직원 PC 데이터 암호화(1차), 임직원 개인정보 및 해외사업 데이터가 다크웹 유출(2차), DDoS 공격으로 홈페이지가 마비되었고(3차), 2022년 3월에는 해커조직 랩서스가 모바일 메신저 텔레그램을 통해 삼성전자의 서비스를 해킹, 소스코드 등을 탈취, 탈취한 데이터 190GB를 폴더 3개로 압축해 파일 공유 프로그램인 토렌토에 게시하였다[5]. 보안이 강화된 대기업에서도 이러한 사고가 비일비재하게 발생하고 있으며, 보안이 다소 미흡한 중소기업은 보다 손쉽게 자료를 탈취해 갈 것으로 예상된다. 이러한 환경 속에서 중소기업 중 방위산업물자의 구성품 또는 부품을 생산하는 방산관련업체에서 방산관련 정보들이 유출되어 피해를 입는다면 첫째, 이는 회사만의 문제가 아닌 국가의 안보와 직결되는 문제가 될 것이다. 둘째, 1990년대에 K200 장갑차 111대를 말레이시아에 수출하기 시작하면서 첨단무기 수출이 본격화 되고, 방산수출 시장은 전차, 자주포로부터 함정, 항공기 등으로 대상 무기체계가 다양화되었으며, 동남아시아에서 중동, 유럽, 남미까지 지역도 확대되어[6] 2022년 방산 수출액 규모가 173억 달러로 전 세계 방산 수출 시장에서 2.4%를 점유하고, 세계 9위에 올라와 있는 상태[7]에서 유출 사고가 발생한다면 대외 신뢰도 하락에 따른 수출 부진으로 이어져 국가이익에 막대한 피해가 발생할 것이다. 이에 본 연구는 이러한 유출 사고를 예방하기 위해 방산관련업체의 정보보호 수준을 측정하고 취약점을 분석하여 업체의 보안 수준을 강화하는데 이바지하고자 한다.

2. 이론적 배경

2.1 방산관련업체

중소기업이란 자산총액이 5천억 원 미만이며, 해당 기업이 영위하는 주된 업종과 해당 기업의 평균 매출액 또는 연간매출액이 규모 기준 이하의 기업을 말하며, 1차 금속 제조업의 규모 기준은 연간매출액 1,500억 원 이하로 대부분 방산관련업체는 이에 속해있다[8]. 방산관련업체는 주로 방위산업체와 계약에 의해 정해짐으로 정확한 현황을 파악하기에는 한계가 있으며, 2023년 5월 말 기준 601개社가 한국방위산업진흥회에 준회원사로 등록되어 있다[9]. 방산관련업체를 방위사업법에서는 일반업체라고 지칭하고 있으며, 방위산업과 관련된 업체로서 방위산업체가 아닌 업체를 말한다라고 정의하였고[10], 방위산업보안업무훈령에서는 방위산업체 외의 일반업체가 국방부장관의 조정·통제를 받는 기관 및 각 군이나 방위사업청 또는 방위산업체와 방위사업 관련 계약을 체결하고 보안측정을 받은 경우를 말한다[11]. 본 연구에서는 정보보호 수준 측정 시 방위산업보안업무훈령의 자가진단항목을 측정 도구로 사용함에 따라 훈령의 정의를 따랐다.

2.2 정보보호의 개념

정보보호란 정보통신 수단에 의하여 처리, 저장, 소통되는 자료를 도청, 해킹 등 외부 위협으로부터 보호하거나 취약 요인을 제거하기 위한 각종 수단과 방법 등의 일체 행위[12] 또는 정보를 여러 가지 위협으로부터 보호하는 것을 뜻하며 정보의 수집, 가공, 저장, 검색, 송신, 수신 도중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적, 기술적 방법을 의미한다. 이러한 정보보호의 의미는 사용자 측면에서는 개인정보 유출, 남용을 방지하기 위한 일련의 행위를 뜻하고, 공급자 측면에서는 내·외부의 위협 요인들로부터 네트워크, 시스템 등의 하드웨어 데이터베이스, 통신 및 전산시설 등 정보자산을 안전하게 보호 및 운영하기 위한 제반활동을 의미한다[13].

2.3 보안측정

보안측정에 대해 대통령령인 보안업무규정에서는 국가 중요시설의 장비·지역을 파괴, 기능 마비, 비밀 누설로부터 보호하기 위한 보안대책 제공 활동이라고 정의하였으며[14], 방위사업법 시행령에서는 방산시설이 충분히 보호될 수 있는 지역 및 시설에 관한 보안대책, 비밀문서의 취급 및 보관·관리에 관한 보안대책, 방산물자 및 원자재에 관한 보호대책, 장비 및 설비의 보호대책, 통신시설 및 통신수단에 대한 보안대책, 각종 자료의 정보처리 과정 및 정보처리 결과 자료의 보호대책, 보안사고에 대비한 관계 정보기관과의 유기적인 통신수단, 그 밖에 보안 유지를 위하여 방위사업청장이 필요하다고 인정하는 보안대책을 마련하였는지 확인하는 행위를 보안측정이라고 하였다[15]. 또한 국방보안업무훈령에서는 군사보안에 관련된 시설·자재 또는 지역을 파괴·기능 마비 또는 비밀 누설로부터 보호하기 위한 행위라고 하였으며[16], 방위산업보안업무훈령에서는 방산보안의 대상인 시설, 장비 등을 테러나 파괴, 도청, 해킹 등 각종 위협요소로부터 보호하는데 필요한 보안대책을 강구하기 위하여 문서·인원·시설·정보통신 등 보안업무 전반에 걸쳐 보안 취약 요인을 종합적으로 진단하는 보안조사 활동이라고 하였다[17]. 앞서 설명하였듯이 보안측정에 대해 다양하게 개념을 정의하고 있으나 공통점을 살펴보면 모두 보안사고 예방을 목적으로 하고 있음을 알 수 있었다. 따라서 본 연구에서는 보안 대상 시설에 대한 보안사고 예방을 위해 보안 취약 요소를 종합적으로 진단하는 활동이라고 정의하였다.

3. 연구 방법

3.1 조사대상 및 자료수집

조사대상은 방산관련업체로 지역에 관계없이 정보보호 수준을 평가할 수 있는 방산관련업체의 정보통신보안 분야 보안측정 자가진단 결괏값을 대상으로 하였으며, 69개를 수집하였다. 또한 평가항목이 업체의 정보보호 수준을 평가하기에 타당한지에 대해 설문을 2023년 3월 22일부터 2023년 5월 26일까지 설문을 실시하였다. 설문 대상은 방산관련업체에서 방산보안 또는 방산기술보호 업무에 종사하는 인원으로 기업 전반의 보안업무를 숙지하고 보안측정 이유 발생 시 수시로 측정을 수검 받고 있으므로 경력 기간에 상관없이 설문 대상으로 선정하였으며, Table 1과 같이 108명이 설문에 참여하였다.

Table 1. Survey Target

Work Experience	Number of Respondents
less than a year	22
1 year or more to less than 3 years	23
3 years or more to less than 5 years	16
5 year or more to less than 10 years	21
10 year or more to less than 20 years	18
more than 20 years	8
Total	108

3.2 설문지 구성

설문지 문항은 정보보호 분야에 영향을 주는 요인을 기준으로 평가영역과 평가항목에 근거하여 연구 목적에 적합하게 구성하였으며, 각 문항은 모두 보안조치 이행 여부를 측정하는 형태로 Fig. 1과 같이 설문하였고, Table 2~Table 8과 같이 방산관련업체 보안측정 자가진단 항목표를 적용하였다[18].

Inspection Categories	Assessment Items	Fulfillment	Unfulfillment
Wireless LAN Management	Is it used after changing the initial password value for wireless LAN in the company?		

Fig. 1. Example of a Security Measurement Self-Diagnosis Questionnaire

3.3 자료분석

수집된 자료 중 평가항목의 타당도를 검증하기 위해 설문조사 결과를 기초로 내용타당도 비율(Content Validity Ratio)을 수식(1)에 대입하여 계산한 결과 “로그파일을 2년간 보관하고 있는가?”에 대한 항목이 0.55로 가장 낮았고, “휴대형 컴퓨터(노트북, PDA 등) 외부 반출 절차 및 보호대책을 보안내규에 명시하였는가?”에 대한 항목이0.96으로 가장 높았다. 따라서 0.55~0.96의 범위를 나타내어 타당도의 최소 기준보다 높은 것으로 분석되었다[19].

$$\text{Construct Validity Ratio} = \frac{n_e - \frac{N}{2}}{\frac{N}{2}} \quad (1)$$

N : Number of respondents

n_e : Number of people who answered ‘Reasonable’

또한, 69개의 보안측정 자가진단 결괏값 신뢰도를 검증하기 위해 SPSS Statistics 27.0 버전을 이용하여 분석하였으며, Cronbach's α계수는 0~1 사이의 값을 가지고 계수가 높을수록 신뢰도가 높은 것으로 판단한다. 보통 결괏값이 0.8~0.9 사이면 바람직하고, 0.6~0.7 정도면 수용할 만하고, 0.6보다 작으면 신뢰도가 결여된 것으로 판단하며[20], 분석결과 Cronbach's α 값은 0.99로 신뢰도가 매우 높게 나타났다. 따라서 설문에 대한 타당도와 보안측정 결괏값에 대한 신뢰도가 검증되었으며, 보안 취약 여부 판단은 보안측정 결괏값의 보안조치 이행률이 75%를 기준으로 미만일 경우 취약한 것으로 판단하였다. 이는 방위산업보안업무훈령의 기준을 따른 것이다[21].

4. 결과 분석

결과 분석은 앞서 연구 방법의 3.2 설문지 구성에서 설명하였듯이 Table 2~Table 8에 따라 방산관련업체 보안측정 자가진단 시 평가하는 6가지 영역별로 분류하여 보안 취약점을 분석하였다.

4.1 무선 LAN 관리

정보보호 수준을 가시적으로 보여주는 무선 LAN 관리는 보안측정 자가진단 결괏값 69개 중 32개의 결측값이 발생하였는데, 무선 LAN을 운용하지 않는 업체로 인하여 발생하였으며, Table 2와 같이 AP(Access Point) 설치 시 서비스 허용 범위를 고려하여 울타리 밖에서 접속이 차단되도록 실내에 설치하고 잠금장치가 된 보호용기로 보호하여 사용하는 기업이 40.5%로 37개社 중 15개社만 보안 조치를 시행하고 있었으며, AP 숨김모드 사용과 관련해서는 25개 기업만 시행하고 있어 67.6%를 나타내었다. 따라서 무선 LAN 관리 분야에서는 이 두 부분이 일반적으로 나타는 취약점으로 분석되었다.

Table 2. Information Protection Level Assessment Items (Wireless LAN Management)

Inspection Categories	Assessment Items	Security Measure Rate(%)
Wireless LAN Management	Is it used after changing the initial password value for wireless LAN in the company?	97.3
	Is the AP installation protected by indoor installation and locked protective containers considering the service tolerance?	40.5
	Do you use AP names in hidden mode?	67.6
	Do I use a password for access?	100.0
	Do you set up and use the encryption communication function between the terminal repeaters?	97.3

4.2 디지털복합기 관리

디지털복합기 관리는 69개 보안측정 자가진단 결괏값 중 14개의 결측값이 발생하였는데 이는 디지털복합기를 보유하고 있지 않는 업체로 인하여 발생하였으며, Table 3와 같이 메모리 자동 소거 기능을 사용하고 있는 기업이 56.4%로 55개社 중 31개社만 사용하고 있었으며, 사용 로그를 2년간 보관하고 있는 기업은 54.5%로 30개社만이 보관하고 있었다. 그러므로 디지털복합기 관리 분야에서는 메모리 자동 소거 기능 비활성화와 로그파일 미보관이 문제점으로 나타났다.

Table 3. Information Protection Level Assessment Items (Digital-composite unit Management)

Inspection Categories	Assessment Items	Security Measure Rate(%)
Digital-composite unit Management	Has the head of management for digital multifunctional units been appointed?	90.9
	Is the administrator password set?	85.5
	Do you use the memory auto-erase feature?	56.4
	Do you keep log files for 2 years?	54.5

4.3 네트워크 관리

네트워크 관리 분야에서는 결측값이 없었으며, 보안측정 자가진단 결괏값 69개 모두 분석하였고, Table 4와 같이 모든 항목에서 기준치인 75%를 미달하였다. 즉, 사용자 계정 관리대장 기록·유지, 모든 정보체계 사용자에게 개별적 사용자

계정 부여, 사용자 계정별 주요 정보시스템 접근 권한 부여, 서버와 네트워크 장비의 주기적 비밀번호 변경 시행에 대해 69개社 중 각각 37개社(53.6%), 41개社(59.4%), 39개社(56.5%), 31개社(44.9%)만 보안조치를 시행하여 이행률이 저조하였으며, 일반적인 취약점으로 식별되었다.

Table 4. Information Protection Level Assessment Items (Network Management)

Inspection Categories	Assessment Items	Security Measure Rate(%)
Network Management	Do you have a user account management ledger?	53.6
	Are individual user accounts assigned to all information system users?	59.4
	Has access rights been granted to major information systems for each user account?	56.5
	Do passwords for servers, network equipment, etc. change more than once a quarter?	44.9

4.4 전산자료 관리

전산자료 관리 역시 결측값 없이 보안측정 자가진단 결괏값 69개 모두 분석하였으며, Table 5와 같이 설계도면 등의 방산자료에 대한 관리절차가 보안내규에 명시되어 관리하고 있는지 여부에 대한 항목은 32개社만이 시행하고 있어 46.4%의 보안조치 이행률을 나타내었으며, 전산자료의 보호 대책 강구 여부에 대한 항목은 38개社만 시행하여 55.1%를 나타내었다. 또한, 사용자가 시스템에 접근 시 관련 기록을 자동으로 저장하고 있는 기업은 43개社로 62.3%만이 시행하고 있었다. 따라서 전산자료 관리 분야에서는 설계도면 등의 방산자료 관리와 전산자료 유출, 파괴에 대비한 보안대책 마련 및 사용자가 시스템 접근에 따른로그 관리가 미흡하였다.

Table 5. Information Protection Level Assessment Items (Computerized data Management)

Inspection Categories	Assessment Items	Security Measure Rate(%)
Computerized data Management	Are defense data (technical data, design drawings, etc.) stored separately from civilian data in separate facilities and devices where security measures have been devised?	81.1
	Are the management procedures for drawings specified in the company's security bylaws?	46.4
	Have all measures to protect computer data specified in the directive been taken in preparation for leakage or destruction of computer data?	55.1
	Does the head of the computer data department limit the scope of data access so that only minimal data is used for each data?	79.7
	Does the system administrator ensure that relevant records are automatically saved when users access the system?	62.3

4.5 개인 · 휴대형 컴퓨터 관리

개인 · 휴대형 컴퓨터 관리 분야에서도 결측값이 없었으며, 보안측정 자가진단 결괏값 69개 모두를 분석하였다. Table 6과 같이 기준치인 75%를 미달한 항목은 P2P, 웹하드, 메신저, SNS 등 보안에 취약한 프로그램 임의 사용을 제한하는 것과 악성코드 백신프로그램, 파일 완전소거프로그램 등 필수 프로그램 설치 운용에 관한 항목이었다. 이 두 항목은 각각 보안조치 이행률이 66.7%와 73.9%로 69개社 중 46개社, 51개社만이 보안조치를 시행하고 있어 일반적으로 나타나는 취약점으로 식별되었다.

Table 6. Information Protection Level Assessment Items (Personal · Portable computer Management)

Inspection Categories	Assessment Items	Security Measure Rate(%)
Personal · Portable computer Management	Do personal computer passwords use mixed numbers, characters, and special characters with 9 or more digits set?	94.2
	Is the screen saver set to 5 minutes or less?	91.3
	Do you limit the arbitrary use of security-sensitive programs such as P2P, Webhard, Messenger, and SNS on your personal computer?	66.7
	Do you use computer malware vaccine programs, file full erase programs, shared folder automatic release programs, and other programs that have been supplemented and distributed?	73.9
	Are procedures and protective measures for taking out portable computers(Laptops, PDA, etc) from the company specified in the company's security bylaws?	84.0

4.6 보조기억매체 관리

보조기억매체 관리 분야 역시 결측값은 없었으며, 69개 모두 보안측정 자가진단 결괏값을 분석하였다. Table 7와 같이 모든 항목에서 기준치인 75%를 초과하였으며, 62개社와, 61개社가 보안조치를 시행하고 있어 일부 기업에서만 나타나는 취약점인 것으로 판별되었다.

Table 7. Information Protection Level Assessment Items (Auxiliary storage media Management)

Inspection Categories	Assessment Items	Security Measure Rate(%)
Auxiliary storage media Management	Are auxiliary storage media managed through a separate management ledger?	89.9
	Does the company specify the procedures for managing auxiliary storage media in the company's security bylaws?	88.4

4.7 정보보호시스템 관리

정보보호시스템 관리 분야도 결측값이 없었으며, 69개 모두 보안측정 자가진단 결괏값을 분석하였고, Table 8과 같이 모든 항목에서 기준치인 75%를 미달하였다. 즉, 정보보호시스템의 CC인증 제품 사용, 시스템 관리자 임명과 매일 정보보호시스템 점검 후 월 1회 이상 정보통신담당자에게 점검 결과 보고 여부에 대해 69개社 중 각각 38개社(55.1%), 40개社(58.0%), 25개社(36.2%)만 보안조치를 이행하여 이행률이 저조하였으며, 일반적으로 나타나는 취약점으로 식별되었다.

Table 8. Information Protection Level Assessment Items (Information protection system Management)

Inspection Categories	Assessment Items	Security Measure Rate(%)
Information protection system Management	Is the information protection system operated by the company's operating information system CC-certified domestic and foreign information protection products?	55.1
	Has the information protection system manager been appointed?	58.0
	Does the information protection system manager check the information protection system once a month and get confirmation from the information and communication division security officer?	36.2

5. 결론

오늘날 우리는 정보통신기술의 발달로 급속한 정보화의 물결 속에서 성장을 이루었으나, 산업기밀 유출 등 다양한 역기능 발생으로 기업의 피해가 점차 늘어나고 있으며, 특히 중소기업의 피해가 전체의 88.5%를 차지하고 있다. 이러한 피해를 예방하고자 방산관련업체의 정보보호 분야에 일반적으로 나타나는 보안 취약점 도출을 위해 보안측정 자가진단 결과를 분석하였으며, 자가진단 결괏값에 대해 신뢰도와 타당도를 검증하였다. 타당도 검증은 보안측정 자가진단 항목에 대한 타당도 설문을 시행하였고, 신뢰도 검증은 결괏값에 대해 통계프로그램 SPSS 27.0를 활용하여 신뢰도를 검증하였다. 검증한 결괏값을 토대로 방산관련업체에 일반적으로 나타나는 정보보호 분야의 취약점을 도출하기 위해 69개社의 보안측정 자가진단 결괏값 중 정보통신보안의 7개 분야 28개 항목을 분석하였으며, 일반적으로 나타나는 취약점은 다음과 같았다. 첫째, 무선 LAN 관리 분야는 서비스 허용 범위를 고려한 AP 설치 위치와 물리적 보호, 숨김모드 사용이 미흡하였다. 둘째, 디지털복합기 관리 분야에서는 메모리자동 소거 기능을 비활성화하였고, 로그파일 보관을 누락하고 있었다. 셋째, 네트워크 관리 분야는 사용자 계정 관리, 모든 정보체계 사용자에게 개별적 사용자 계정 부여, 사용자 계정별 주요 정보시스템 접근 권한 부여, 서버와 네트워크 장비의 주기적 비밀번호 변경을 시행하고 있지 않았다. 넷째, 전산자료 관리 분야는 방산자료 관리와 자료의 유출·파괴에 대한 대책이 미비하였고, 사용자가 시스템 접근 시 관련 기록을 자동으로 저장하도록 설정하지 않았다. 다섯째, 개인·휴대형 컴퓨터 관리 분야에서는 보안에 취약한 프로그램의 임의 사용 제한과 필수 프로그램 설치 운용이 미흡하였다. 여섯째, 정보보호시스템 관리 분야는 정보보호시스템의 CC인증 제품 사용, 시스템 관리자 임명 및 일일 단위 정보보호시스템 점검을 시행하지 않은 것으로 나타났다. 앞에서 살펴본 바와 같이 일반적으로 나타나는 취약점들을 보면 기술적인 면보다 보안정책 설정이 미흡한 부분이 많았다.

본 연구는 방산관련업체의 정보보호 수준 대한 체계적인 학술 연구이며, 보안사고를 야기할 수 있는 취약 요인에 대한 분석으로 업체들의 보안환경을 연구하는데 시금석이 될 것으로 판단 된다. 또한, 현재 적용 중인 군사기밀보호법, 방위사업법, 방위산업기술보호법, 보안업무규정과 관련된 이론을 참조하여 연구를 수행함으로써 방산보안에 대한 이론적인 배경과 실용성을 갖춘 연구로 볼 수 있다.

그러나, 수집된 자료의 보안측정 자가진단 결괏값은 전문 평가기관에서 시행한 결괏값이 아닌 기업이 자체적으로 측정한 결괏값으로 측정관에 따라 측정 결과가 달

라질 수 있다는 한계점이 있다. 따라서 향후 전문 평가기관에서 측정한 결괏값에 의한 보안 취약점 분석과 함께 정보보호 분야에 한정하지 않고 인원·시설·기업보안 등 전 분야에 대한 보안측정 결괏값을 통한 취약점을 도출하고 개선 방안을 제시하는 후속연구도 필요할 것으로 보인다.

References

[1] S. H. Kim, C. M. Lee, "A Comparative Analysis of EU GDPR with Privacy Laws in South Korea", *Convergence security Journal*, Vol.18, No.5, pp.83-92, Dec. 2018.

[2] K. M. Ko, J. S. Lim, S. S. Jang, "An Analysis of General Defect Cases in the Establishment of Information Security Management Sysyem", *Journal of The Korea Institute of Information Security & Cryptology*, Vol.17, No.4, pp.34-41, Agu. 2007.

[3] H. J. Yun, Y. W. Lee, H. D. Heo, S. H. Chun, "Improvement Research for Information Protection Management System of Small and Medium Enterprises", *The Journal of The Institute of Internet Broadcasting and Communication*, Vol.23, No.2, pp.15-20, Apr. 2023. DOI: https://doi.org/10.7236/JIIBC.2023.23.2.15

[4] South Korea Policy Briefing, "Information protection violations last year, the number of individuals increased, and the number of companies decreased", Korea Google Survey, [cited July 4, 2023], Available From: https://www.korea.kr/news/policyNewsView.do?newsId=148900771 (accessed April 14, 2022)

[5] J. M. Kim, M. H. Lee, J. H. Lee, "Cyber Security Policies for Small and Medium-sized Enterprises: A Case Study on the Cyber Security Breaches in Manufacturing SMEs in Korea", *The e-Business Studies*, Vol.23, No.3, pp.41-63, June, 2022. DOI: https://dx.doi.org/10.20462/tebs.2022.6.23.3.41

[6] H. G. Cho, "Defense Export as a New Leap Forward in the Defense Industry", *Monthly Korea Institute for Industrial Economics & Trade*, Vol.23, No.3, pp.69-72, Mar. 2023.

[7] Chosun Ilbo, "We beat Isrel...Challenges for Advancing to the Semifinals of the World's K-Defens Industry Mountain", Korea Google Survey, [cited June 1, 2023], Available From: https://www.chosun.com/politics/politics_general/2023/06/01/33EZCWBB5BA5PBSJ3UHEQWSEUQ/ (accessed June 3, 2023)

[8] Ministry of SMEs and Startups, "Enforcement Ordinance of the Framework Act on Small and Medium Enterprises", Nov. 2022, p.1

[9] Korea Defense Industry Association, "Current Status of Member Companies", Korea Google Survey, [cited 2023 May. 31], Available From: https://www.kdia.or.kr/kdia/contents/member3.do (accessed Jun. 3, 2023)

[10] ROK Ministry of National Defense, "Defense Acquisition Program Act", May. 2022, p.1

[11] ROK Ministry of National Defense, "Defense Industry Security Service Instruction", Dec. 2022, p.133

[12] ROK Ministry of National Defense, "Defense Industry Security Service Instruction", Dec. 2022, p.126

[13] K. W. Moon, Seung Joo Kim, "Relationship between Information Security Activities of Enterprise and Its Infringement : Maninly on the Effect of Information Security Awareness", *Journal of The Korea Institute of Information Security & Cryptology*, Vol.27, No.4, pp.897-911, Agu. 2017. DOI: https://doi.org/10.13089/JKIISC.2017.27.4.897

[14] National Intelligence Service, "Security Operational Rule", Jan. 2021, p.6

[15] ROK Ministry of National Defense, "Enforcement Ordinance of the Defense Acquisition Program Act", Oct. 2022, p.21

[16] ROK Ministry of National Defense, "Defense Security Service Instruction", Dec. 2022, p.166

[17] ROK Ministry of National Defense, "Defense Industry Security Service Instruction", Dec. 2022, p.128

[18] Korea Defense Industry Association, "Defense Industry Realated Companies Security Measurement Self-inspection Item table", Korea Google Suvey, [cited 2022 Jun. 13], Available From: https://www.kdia.or.kr/kdia/contents/member-services11.do?&schM=list&page=1&viewCount=10&id=&schGroupCode=&schFld=0&schStr=보안측정 (accessed Jun. 3, 2023)

[19] Ayre, C., & Scally, A. J., "Critical values for Lawshe's content validity ratio: Revisiting the original method of calculation", *Measurement and Evaluation in Counseling and Development*, Vol.47, No.1, pp.79-86, 2014.

[20] Y. R. Par, *A Study on information security level assessment and vulnerability improvement for financial-sector information security level enhancement*, Ph.D dissertation, Yonsel University, Seoul, Korea, pp.63, 2014.

[21] ROK Ministry of National Defense, "Defense Industry Security Service Instruction", Dec. 2022, p.98

이 상 열(Sang Yeol Lee) [정회원]

- 2005년 7월 ~ 2013년 11월 : 육군종합정비창 군수담당
- 2019년 2월 : 아주대학교 사이버보안전공 (석사)
- 2021년 8월 ~ 현재 : 명지대학교 보안경영공학 박사과정 재학

〈관심분야〉
사이버보안, 방위산업보안, 개인정보보호

유 연 승(Yeon Seung Ryu) [정회원]

- 1990년 2월 : 서울대학교 계산통계학과 (학사)
- 1992년 2월 : 서울대학교 계산통계학과 전산과학전공 (석사)
- 1996년 8월 : 서울대학교 계산통계학과 전산과학전공 (박사)
- 2003년 3월 ~ 현재 : 명지대학교 컴퓨터공학과 교수
- 2015년 3월 ~ 현재 : 명지대학교 대학원 보안경영공학과 교수
- 2022년 3월 ~ 현재 : 명지대학교 대학원 방산안보학과 교수

〈관심분야〉
보안경영, 방산안보, 사이버보안