Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.33, NO.3, Jun. 2023 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2023.33.3.561

인간중심보안을 위한 인적취약점 분류체계에 관한 연구

박 정 준,[1†] 안 성 진[2‡]
[1,2]성균관대학교 (대학원생, 교수)

A Study on the Human Vulnerability Classification System for People-Centric Security

Jungjun Park,[1†] Seongjin Ahn[2‡]
[1,2]Sungkyunkwan University (Graduate student, Professor)

요 약

정보보안 산업은 지난 수십 년간 매우 다양한 성장을 거듭해왔다. 특히 기술적, 관리적, 제도적 측면에서 다양한 해법을 제시해왔다. 그럼에도 불구하고 매년 보안사고는 지속해서 발생하고 있는데 주목해야 한다. 이는 기존의 보안이 지나치게 기술 중심, 예방 중심의 정책으로 추진되고 있어서 디지털 시대의 다양한 비즈니스 변화에 한계가 있음을 증명하고 있다. 따라서 최근에 전통적인 보안 접근 방식의 한계를 벗어나고자 인간중심 보안(PCS: People-Centric Security)이 화두가 되고 있다. 본 연구에서는 정보보안 위반의 개념, PCS 전략적 원칙, 전문가 인터뷰를 통해 인간이 유발할 수 있는 취약점을 크게 5가지로 구분하고 21개의 세부 구성요소로 분류함으로써 근본적인 보안 사고 대응 방안을 제시하고자 한다.

ABSTRACT

The information security industry has seen a wide variety of growth over the past few decades. In particular, various solutions have been proposed in terms of technology, management, and institutional aspects. Nevertheless, it should be noted that security accidents continue to occur every year. This proves that there are limitations to various business changes in the digital era as existing security is being promoted with technology-oriented and prevention-oriented policies. Thus, people-centric security (PCS) has recently become a hot topic in order to escape the limitations of traditional security approaches. Through the concept of information security violations, PCS strategic principles, and expert interviews, this study aims to present a fundamental security incident response plan by classifying human-caused vulnerabilities into 5 categories and classifying them into 21 detailed components.

Keywords: PCS, Human Vulnerability Classification, Human Vulnerability Components, Security

I. 서 론

정보보안 산업은 지난 수십 년간 괄목할만한 성장을 거듭해 왔다. 특히 기술적인 측면에서의 보안 수준은 한계에 다다를 만큼 대응 방안이나 예방에 있어서 다양한 해법을 충분히 제시해주고 있다. 더불어 관련 법, 제도적인 측면에서의 정보보안 컨설팅도 이젠 정부 공공 기관이나 기업에서는 필수적인 업무로 자리매김해 오고 있다. 그런데도 매년 보안 사고는 지속해서 발생하고 있는데 우리가 주목해볼 필요가 있다. 기술적, 관리적 측면의 보안 외에 우리가 간과하고 있었던 분야는 없었는지 되짚어 봐야 할 시점이다.

인적 보안은 오랫동안 강조되어왔던 보안의 한 분야임에도 불구하고 집중적인 연구나 투자가 지속해서

Received(02. 14. 2023), Modified(1st: 03. 08. 2023, 2nd: 04. 04. 2023), Accepted(04. 04. 2023)
† 주저자, jjpark0822@naver.com
‡ 교신저자, sjahn@skku.edu(Corresponding author)

이루어지지 못했다. 이러한 흐름에서 최근에 인간 중심 보안(People Centric Security, PCS)이 매우 활발히 전개되고 있는데, 이는 더 이상 시스템이나 정책에 의존해서는 IT 기술변화에 따라 고도화되고 지능화되는 위협을 모두 방어할 수 없다는 공감대 때문이다. 따라서 인적 보안을 좀 더 심도 있게 다루는 연구가 필요해졌고, 시스템 보안취약점과 같이 DB, Network, Server, End-Point 등 각각의 영역별 체계적인 분류를 기반으로 대응 방안을 마련해왔던 것처럼, 마찬가지로 인간이 유발할 수 있는 취약점의 유형에 대한 근본적인 분류체계가 매우 중요한 출발점이 될 수 있을 것이다[10][11].

본 연구에서는 인간 중심 보안의 취지와 ISMS-P의 인적 보안 통제기준, 인간 심리적인 측면을 사이버 범죄 프로파일링 관점에서 접근하여 분석하고, 마지막으로 전문가 심층 면접(Focus Group Interview, FGI)과 설문을 통해 인적 취약점 분류체계에 대한 최적화된 모델을 제안함으로써 보안 위협에 대한 보다 근본적인 접근 방안을 제시하고자 한다. 이를 위해 먼저 인적 보안의 개념부터 연구 현황 그리고 인간중심 보안에 대한 개념 정리를 통해서 기존의 통제 중심의 보안, 기술 및 정책 중심의 보안을 탈피해서 다양한 비즈니스 환경에 유연하게 대처할 수 있는 보안 패러다임의 정립이 필요한 시점이다. 또한 새로운 기술들이 융합해서 고도화된 사이버 공격 등 다양한 취약점에 대한 체계적인 분류 및 측정지표를 통해서 기존 인프라 시스템에 대한 보안 수준은 어느 정도 한계점에 도달했으나, 사람 관점에서 사람이 유발할 수 있는 보안취약점에 대한 체계적인 분류나 측정지표에 대한 선행연구는 찾아보기 힘든 실정이다. 이에 따라 먼저 인간중심 보안의 정의부터 살펴보면 인간중심 보안이란 '전사적이고 연속적인 보안문화를 구축하기 위한 전략적 접근 방법으로서, 원칙과 신뢰를 기반으로 개별 사용자의 권한과 이와 관련된 책임을 명확히 부여하고, 인간 관련 위험을 관리하기 위해 강압적, 예방적 보안대책과 이상 징후, 사고의 신속한 탐지 및 대응 대책을 균형적으로 구현하고 지속적 교정을 강조하는 접근 방법'이라고 정의할 수 있다[8].

본 연구에서는 이러한 취지에서 사람이 유발할 수 있는 근본적인 취약점을 심도 있게 분류해보고 이를 통해서 인간중심 보안을 위한 인적 보안의 새로운 패러다임을 제시함으로써 사이버 위협에 대한 기존 방어 체계와 더불어 충분한 시너지(Synergy)가 될 수 있을 것으로 기대한다.

II. 이론적 배경

2.1 인적 보안의 개념과 문제점

2014년 가트너 보고서에 의하면 IT 환경변화에 따른 보안기술 및 보안 위협의 추이가 기존의 기술 중심(Control-centric)에서 사람 중심(People-centric)으로 변화되는 것을 예측하고 있는데, 특히 2015년부터 정부 주도의 사이버 보안 복원력(Resilience)의 중요성을 언급하고 기술적인 보안보다는 사람 중심의 보안 대응에 초점을 맞추는 전략이 수립되었다[1][2].

사이버 보안 복원력(Resilience)이란, 조직이나 개인이 보안 사고에 직면했을 때 빠르게 회복할 수 있는 능력을 의미한다. 즉, 기술적인 대책뿐 아니라 사람들의 행동, 조직, 문화, 경영, 전략 등을 종합적으로 고려하는 것을 의미한다. 이러한 복원력은 보안사고가 발생했을 때 빠르고 효율적인 대처가 가능하게 하기 위해서 필요하다. 이를 위해 조직이나 개인은 보안 사고에 대한 대응 계획을 미리 수립하고 이를 지속해서 검토하며 개선해 나가는 것이 중요하다. 또한 보안 인식 교육 등을 통해 사람들이 보안사고를 예방하고 대처할 수 있는 능력을 함양하는 것도 중요하다. 이는 단순히 보안사고 대처 능력뿐 아니라 비즈니스 연속성, 규제 준수 등과도 연관되어 있다. 따라서 조직이나 개인이 보안 사고에 대한 복원력을 구축하는 것은 전체적인 비즈니스 운영의 안정성을 유지하는 데 매우 중요하다[9][18][19].

최근 자동차, 의료, 유통 등 산업 전반의 다양한 분야에서 급속도로 ICT의 발전을 거듭해 오고 있고, 사물인터넷(IoT), 클라우드(Cloud), 빅 데이터(Big Data), 인공지능(AI), 모바일 등 새로운 기술이 시장 전반에 확대되면서 예측하기 어려운 사이버 침해 사고는 더욱 증가할 것으로 전망하고 있다[3].

한국행정연구원에 따르면 2017년 전 세계 인구 중 70%가 인터넷에 접속할 것으로 예상했고, 이러한 상황에서 개인의 '인적 요소'(Human Factor)는 사이버 공간에서 가장 취약한 부분이 될 것으로 전망했다[3]. 한국인터넷진흥원(KISA)에서도 기업의 사이버 침해 신고는 2019년 418건에서 2022년 639건으로 2년 만에 53%가 급증했고, 코로나19 팬데믹으로 비대면과 디지털 전환이 가속됨에 따라 사이버

공격이 증가했다는 사실이 통계적으로 확인되었다[4].

또한 2018년 페이스북 데이터 유출 사건, 2017년 미국의 신용 보고 기관인 에퀴팩스(Equifax) 대규모 데이터 침해 사고, 2021년 3월 마이크로소프트 정보 유출 사건을 비롯해서 국내의 경우 2014년 카드 3사의 개인정보 유출 건수가 1억 400여만 건에 이르고, 소셜 커머스 및 통신사들의 개인정보 유출 등 국내외 인적 보안 위반 사례는 지속적이며 주기적으로 발생하고 있다[15][16][17].

특히, 2019년 국가 인적자원개발 총괄센터 조사 결과에 따르면 인적 취약점이 발생한 기관 수는 1,382개, 발생 건수는 8,508건, 유형으로는 내부정보 유출 및 외부 침해 사고 사회공학적 공격 등으로 집계됐으며 2020년 한국인터넷진흥원(KISA) 보고서에서도 인적 취약점이 발생한 기관 수는 무려 1,170개, 발생 건수 7,734건으로 그 원인 역시 내부정보 유출 및 외부 침해 사고 그리고 사회공학적 공격 등으로 나타났다. 더불어 2021년 제1차 정보보호 컨설팅 서비스 직무능력 평가 결과 정보보호 관련 직무능력 평가를 받은 1,296명 중 인적 취약점 방어 능력이 부족한 비율이 38.3%, 인적 취약점 방어 능력이 가장 부족한 분야로 사회공학적 공격 방어로 나타났다. 이같이 인적 취약점이 매년 증가하는 추세를 보이고 있으며 이에 대한 대응과 보완이 필요한 상황이다.

이처럼 기술적, 관리적, 정책적 보안이 강화됐음에도 불구하고 지속적인 보안 사고가 발생해왔고, 정보보안의 패러다임이 기술 중심에서 사람 중심으로 변화가 점진적으로 필요한 시점임을 확인할 수 있다.

이상과 같이 언급한 사례와 통계를 기반으로 기술 중심에서 사람 중심으로 보안의 패러다임이 변화하고 있는 근거를 정리해 보면 다음과 같이 요약할 수 있다. 첫 번째 인적 취약점의 증가를 꼽을 수 있다. 급격한 인터넷 기술의 발전과 코로나와 같은 팬데믹으로 인해 사람들이 인터넷을 더 많이 사용하게 되면서 인적 취약점이 더욱 증가하게 되는 계기가 되고 있다. 즉, 인터넷 사용의 증가는 사이버 위협의 표적에 노출되는 기회가 증가하고 다양한 공격기법 시도로 이어질 수 있다. 이러한 환경에서 유발되는 인적 취약점은 기술적인 보안대책으로는 완전히 해결될 수 없으며 인간의 실수나 부주의로 인해 발생하는 문제로 접근해야 한다. 따라서 이제는 기술적, 관리적, 정책적 범위에서 탈피해서 사람을 중심으로 한 인적 보안대책을 보완해야 한다. 두 번째 사회공학적 공격의 증가를 들 수 있다. 즉, 사람의 신뢰를 이용한 정보 탈취 방식은 기술적인 대책만으로는 방어하기 어렵다. 세 번째, 보안 인식의 중요성이 부각 되고 있다. 기술적인 보안대책은 보안에 있어서 필수적인 요소이지만, 사람들의 보안 인식이 부족하면 완벽한 보안이 이루어지기 어렵다. 따라서 정보보안 분야에서는 사람들의 보안 인식을 높이기 위한 보안 교육 등 사람 중심의 보안대책이 강조되고 있다. 네 번째 법제도 강화를 들 수 있다. 최근 개인정보 보호법 등 법적인 제도가 강화되면서 기술적인 대책뿐 아니라 개인정보 처리에 대한 인간 중심의 보안대책이 강조되고 있다. 이와 같은 이유로 정보보안 분야에서는 기술 중심에서 사람 중심으로 보안의 패러다임이 변화하고 있음을 확인할 수 있다[9][10].

결론적으로 인적 보안의 의미는 개인적인 관점에서 조직의 구성원이 보안 정책에 따라 충실히 업무를 수행하고 있는가를 판단해서 최소한의 보안인증 규정을 준수하여 사람에 의한 보안 이슈를 예방하기 위한 활동을 통칭한다[1][5]. 물리적, 기술적 관리 수단과는 다르게 인적 보안 관리는 정보를 소지하고 취급하는 직원이 보호 활동의 주체이자 객체이며 보호 수단이기도 하다[6].

2.2 인적 보안 연구 현황

인적 보안 혹은 인원보안은 정보보안(Information Security)의 한 분야로서 조직의 보안 정책에 따라 실행되는 전체의 보안 프로세스에서 중심적이고 주체적인 항목이며 기존의 정보보안 이론과 기준에서 별도의 항목으로 구분하고 있다. 그러나 인적 보안에 대한 세부적인 기준이나 절차가 구체적으로 정립되지 않았으며 대부분 인적 보안을 기준에서 단순하게 명기하고 있다. 인적 보안 관리의 기준은 일반적으로 BS 7799, ISO 17799에 포함된 인적 보안 부분에서 일부 찾을 수 있으며 이 기준은 인원의 고용을 중심으로 관리 영역을 정립하고 이에 따른 부수적인 업무를 포함하고 있다. 또한 미국, 영국, 호주, 캐나다 등 일부 국가에서는 인적 보안 기본 원칙을 제시하고, 이 원칙에 따라 정부 산하 기관이나 주 정부에는 조직의 특성을 고려한 별도의 인적 보안 지침을 유지하고 이를 실행 하는 실정이다[5].

ISO 27001에서는 정보보안 관리를 위해 실행지침으로 특정 조직이 정보보안 관리체계를 구축하는 경우 유용하게 사용될 수 있으나 모든 보안 관리 영역이 충족되기는 어렵다고 하였다. 즉 인적 보안 관점에서 역시 이러한 인적 보안 관리 지표들은 인적

보안 관리의 어느 일정 수준을 포함하고 있다고 할 수 있겠으나, 개인에 대한 보안 평가와 경력, 개인의 자질에 대한 구체적인 항목의 부재, 개인의 윤리적이거나 도덕적인 문제의 검증, 이를 평가할 별도의 조직의 임무 부재 그리고 지침과 지표의 미흡 등이 있으므로 형식적인 관리항목으로 전락할 위험이 내재하고 있어 관리항목을 보다 구체적으로 개선 발전시키는 별도의 연구가 요구된다[5].

더불어, 산업기밀 유출 범죄의 주체와 동기 연구 결과에 따르면 먼저 국내 정보 유출의 주체를 보면 전직 직원이 52.8%, 현직 직원이 27.1%로 전·현직 직원이 차지하는 비중이 약 80%에 달하고 있다. 또한 당해 기술을 잘 알고 있거나 기술이나 정보에 접근이 쉬운 사람에 의해 이루어진 경우가 대부분이었고, 협력 업체 또는 투자업체의 경우는 7.4%를 점하고 있어서 산업보안의 경우 외부인보다는 내부인의 단속에 더 큰 노력이 필요한 것으로 나타났다[7].

2.3 인간중심 보안(PCS)

뉴노멀(New normal)시대에서의 보안 전략으로 디지털 전환의 가속화로 인해 보안 위험이 다양해지고 고도화됨에 따라 업종의 특성을 고려하면서 위험관리 기반의 자율적 보안을 추구하는 사이버 보안 복원력(Resilience)을 갖춘 디지털 보안 체계를 구축해야 한다. 즉 면역 회복력을 갖춘 디지털 보안 체계란 데이터 기반의 보안(Data-Driven Security), 비즈니스 요구사항(Biz-Aligned Security)을 반영한 인간중심 보안(PCS)을 의미한다.

특히, 2020년 RSA Conference에서는 Human Element가 화두가 되었고, 이 자리에서 Business, Intelligent, Humanizing 등 조직 내의 모든 임직원이 보안의 책임을 강조하는 공감대가 있었다[8].

인간중심 보안(People-Centric Security)이라는 용어는 미국의 시장조사 및 컨설팅 회사로, 정보통신 분야의 연구·자문을 담당하는 가트너(Gartner)社의 Tom Scholtz가 2015년 사용하였으며, 임직원에게 보안역할과 책임을 부여함으로써 임직원이 감시대상이 아닌 보안 주체임을 인지시키고, 통제 중심 보안에서 자율중심 보안으로 전환하는 패러다임의 보안을 의미한다[9].

대표적인 IT 강국인 우리나라의 보안기술은 명실공히 세계 최고의 수준이다. 그러나 이러한 상황에서도 사이버 범죄가 지속 발생하는 현상은, "인간의 심리"라는 요소는 간과해왔기 때문이다. 즉 '왜 인간이 사이버 범죄를 저지를까'에 대한 심리적 분석이 필요한 것임을 의미한다. 또한 최근 2년간 국내 보안사고 발생의 핵심 원인이 주요 시스템 취약점이나 보안담당 부서의 실수보다도 개별 이용자들의 미숙함으로 인한 경우가 약 절반 가까이 차지하였음을 입증할 수 있다[9].

III. 인적 취약점 분류체계 연구

3.1 연구 방법

인적 취약점 분류체계를 연구하기 위하여 국내외 보안 정책, 연구자료 및 학위 논문, 학술지 등을 바탕으로 인적 보안에 대한 개념, 쟁점 등을 분석하였다. 자료 분석을 통하여 정리된 다양한 인적 취약점 분류 요소들을 중심으로 8명의 보안 전문가와 심층 면접(FGI)을 3차에 걸쳐 진행했으며, 기간은 2021년 8월 30일부터 9월 30일까지 약 한 달간 진행했다. 진행 도구는 마인드맵(Mind Map), 엑셀. 파워포인트를 활용하여 결과물을 정리하였다.

마인드맵 정리는 10차에 걸쳐 내용이 수정되면서 인적 취약점 유발 요인에 대한 다양한 경우를 설정하고 이에 따른 그룹화 작업을 통해 인적 취약점 분류체계의 기반이 되는 작업으로 선행되었다. 즉, 해킹 모의 훈련을 통해 사람의 어떤 심리를 이용하여 취약점을 예방하고자 했는지, 보호하고자 하는 자산 유형에는 어떠한 것이 우선순위가 있는지, 계획적, 의도적인 사고는 어떠한 유형이 있을 수 있는지 심리적인 요인으로는 어떠한 부분들이 작용하는지 등을 정리하여 정보보안 분야의 전문가 인터뷰를 통해 확인하고 구체화하는 작업을 진행했다.

FGI에 의하여 최종적으로 인적 취약점의 5가지 대분류와 21개의 구성요소로 도출되었고, 이에 대한 신뢰성을 검증하기 위해 134명의 IT 및 보안 업계 이해관계자를 대상으로 약 3주간 설문조사를 진행하였다. 설문조사 결과로 인적 취약점 분류체계 대분류와 구성요소 간 기술 통계량 분석 및 신뢰도 분석(Reliability analysis) 결과에 따라 인적 취약점 분류체계 모형을 검증하고, 검증된 인적 취약점 분류체계를 제시하고자 한다.

3.2 전문가 심층 면접(FGI)

FGI의 전문가 그룹은 총 8명이었으며, 총 3차에 거쳐 전문가 그룹의 의견을 수렴하고 그룹화하여 분류체계 모형을 구체화하였다. FGI에 참여한 전문가들의 직무는 금융권 CSO 1명, 일반 IT 소프트웨어 개발 업체 CEO 1명, 보안 consultant 2명, SI 보안 PM 그룹 2명, 보안솔루션 엔지니어 2명으로 구성하였다. 전문가 그룹의 구성은 Table 1.과 같다.

1차 FGI에서는 인적 보안 관련 자료 분석 결과를 바탕으로 진행하였다. 인적 보안에 관련된 용어와 보안사고 사례, 인적 보안 지침 및 정책, 법·제도 등을 토대로 정보시스템 자원 오용, 정보보안 일탈행동, 보안 의식 부족 행위(게으른 보안 행동), 잠재적인 위반행위(Low Risk), 직접적인 위반행위(High Risk) 등 총 5가지 분류와 이에 따른 세부적인 취약점 체크리스트를 FGI 참석자들에게 제시하였다. 즉, NIST SP 800-53, ISO/IEC 27001, 인터넷 보안 센터(Center for Internet Security), 국가 인텔리전스 보안 센터(National Counter intelligence and Security Center) 등을 참조하여 접근제어(Access control), 인증(Authentication), 권한 부여(Authorization), 취약점(Vulnerability), 위협(Threat), 인적 보안 검증(Personnel security vetting), 비인가 접근(Unauthorized access), 불법 복제(Unauthorized duplication), 데이터 누출(Data leakage), 인적 보안 교육(Personnel security awareness training) 등의 인적 보안 관련 용어를 정리했다. 더불어 2.1에서 언급된 인적 취약점 관련 보안 사고사례와 통계를 참조했고, 정보보호 관리체계(ISMS), 개인정보보호법, 개인정보보호지침, 정보보호산업협회, 정보보호지식서, 정보보호 교육용 교재 등을 참고해서 FGI를 진행하였다.

1차 인터뷰는 브레인스토밍 방식으로 약 2시간 정도 진행했으며, 브레인스토밍 후 결과에 대한 정리는 마인드맵 도구를 사용하여 정리하였다. 1차 진행 과정에서는 인적 보안에 관한 관심과 중요성에 초점을 맞추고, Table 2.와 같이 검증 항목을 도출하였다. 즉, 인적 취약점 중심의 보안사고 패러다임 전환 여부와 제시된 인적 취약점 분류체계의 구체적인 실행방안 등을 주제로 토론하였다.

그리고, 인적 취약점 분류체계 점검의 실효성에 대해서 Table 3. 과같이 5가지 질문을 통해서 그 중요성과 실현 가능성에 대해서 각각 0~5점(소수점 첫째 자리까지)의 정량적 점수를 부여하여 측정 후 분석했다.

결과는 참여자들 대부분이 중요성과 실현 가능성에 대해서 매우 강한 공감대가 있었고, 대부분 긍정

Table 1. Information of experts group

Occupation	Number of experts (%)	information security -related career (Average. years)	Average age
CSO	1(12.5)	20	52
IT/CEO	1(12.5)	5	56
Consultant	2(25.0%)	15	46
SI(PM)	2(25.0%)	15	48
Security Solution Engineer	2(25.0%)	10	40

Table 2. Derivation of verification items

Division	Operational Definition	Measurement
importance	Whether it is important to shift the paradigm of security thinking centered on human vulnerabilities.	• Possibility of causing accidents due to weaknesses in human resources • Limitations of Security Solutions • Limitations of Security Compliance
feasibility	Whether the classification system proposed for the paradigm shift of security accidents centered on human vulnerabilities can be a concrete action plan.	• Effectiveness of Human Vulnerability Checklist • Expected Effects of Human Vulnerability Checklist

Table 3. Effectiveness of Human Vulnerability Classification Model Inspection

Division	Effectiveness of Inspection of Human Vulnerability Classification System	import ance	feasibi lity
1	The severity of accidents caused by human vulnerability	4.3	4.6
2	Limitations of Response to Infringement by Security Solutions	3.6	4.1
3	Limitations of responding to infringement by security compliance	3.7	4.1
4	Effectiveness of Human Vulnerability Prevention Items	4.1	4.4
5	Expected Effects of Human Vulnerability Prevention Items	3.9	3.9

적인 의견을 주었으며 관련해서 기타 의견에 대해서는 Table 4. 와 같이 요약 정리하였다.

1차 인터뷰 정리 결과를 바탕으로 2차 FGI를 진행했고, 1차 의견의 정리된 결과를 사전에 참여자에게 배포하고 내용을 검토한 후 참여할 수 있도록 하였다. 불가피한 사유로 인터뷰에 참여하지 못한 경우는 전화 및 이메일을 활용하여 의견을 충분히 수렴하였다. 특히 해당 시기에 코로나 예방 차원에서 참여자들의 안전을 고려하여 비대면 프로그램을 사용했다. 2차 인터뷰에서는 1차 인터뷰의 내용을 토대로 작성된 인적 취약점 분류체계 초안에 대해서 반복해서 Review 하였다. 즉, 도출된 주요 내용은 먼저 우발적인 상황에서 발생할 수 있는 개인의 특성에 초점을 맞추어 개인의 성향, 활동성, 위험성, 보안 수준 등을 인적 취약점 요소로 도출하였으며, 개인의

Table 4. Other Opinions

Division	Other Opinions
CSO	• Human vulnerability requires continuous education. • The limitations of security solutions are clear. • Compliance may be exploited.
CEO	• Need to redefine terminology from a security perspective. • Human vulnerabilities need continuous management.
Consultant	• "Moral deviation theory perspective" and "People-Centric security" need to reinterpret justice.
	• In addition to experience/witness, 'aids' should also be considered. • Need to approach in terms of psychological/social/human relationship norms. • It is also necessary to review the request of acquaintances, self-knowledge accumulation, self-interest realization, monetary counter-payment in terms of malicious behavior (illegality), or information leakage for reflective interests. • A 'human psychological' approach to why information leakage is needed (simple curiosity/self-exaggeration/self-satisfaction, etc.) • The most common case is the solicitation of acquaintances and stakeholders. • A review of the relevance of human relations theory, behavior organization theory, and behavioral theory in the humanities and social sciences.
SI(PM)	• Classification and inspection items need to be used as indicators to identify the overall level by giving differential scores according to the risk level for each vulnerability, or to derive improvement directions for improvement.
	• Potential threats include the absence of departmental security personnel.

Division	Other Opinions
SI(PM)	• Lack of security awareness also includes actions such as not conducting periodic security checks.
Security Solution Engineer	• Misuse of information system resources requires criteria for information. • Information security deviant behavior should be limited that the standards for the internal system are clear and personal information related to the company. • Direct violations should be written so that the violations and measures are not mixed.
	• It should also include information on critical system access rights under task delegation. • It is thought that the importance of the classification system or checklist will differ depending on the task in charge.

특성을 벗어나 사람의 관계에서 비롯되는 측면에서는 인맥, 갈등, 청탁 등이 중요한 인적 취약점 요소로 도출되었다. 특히, 현재 사이버상의 SNS나 채팅 등 다양한 형태의 인적 네트워킹이 복잡하게 얽혀 있는 점도 사람과의 관계에서 매우 중요한 인적 취약점 유발 요인으로 식별할 수 있었다. 잠재적 측면에서의 인적 취약점 유발 요인은 개인, 사람과의 관계보다 더 큰 범위의 조직, 사회 전반의 관계를 의미하는 것으로 업무환경이나 문화, 조직의 특성 그리고, 그 조직의 보안 통제 수준 등이 인적 취약점 유발 요인이 될 수 있는 것으로 나타났다. 그리고 심리학적인 영역에서는 일반적으로 사람이 가질 수 있는 근본적인 인적 취약성 요인을 정의하고 왜 사람이 보안 사고를 유발할 수밖에 없었는지에 대한 생물학적, 정신분석적 관점에서의 근본적인 문제들을 도출하고자 노력했다. 마지막으로 윤리적인 측면에서는 사회 공통적인 시각으로 적용될 수 있는 윤리적인 요인 등이 도출되었다. 따라서 3.1의 참고 자료와 FGI를 통해 권한 위반 및 접근제어 등 4건의 위반행위와 정보시스템 자원 오용, 자기 과시 및 자기만족 등 8건의 정보보안 일탈행동, 그리고 보안 프로그램 업데이트 및 암호 변경 등 17건의 보안 의식 부족 행위(게으른 보안 행동), 마지막으로 업무 부주의 및 보안 관리 등 13건의 잠재적인 위반행위, 악의적 목적의 위반 및 금전적 이익을 목적으로 한 위반 등 24건의 직접적인 위반행위까지 총 5가지 대분류에 66건의 점검 항목을 도출했고 이를 토대로 FGI를 통해 중복되거나 불필요한 부분을 제거해가면서 Review를 진행했다. FGI를 수행하면서 충분한 의견을 수렴했고 자유롭게 토론하면서 전문가들의 지식과 경험, 인사이트(insight)를 기반으로 내용을 정리한 후에 마인드맵을 활용하여 연관된 내용을 그룹화하고 최종 그룹화된 내용에 대해서 재차 FGI를 수행하면서 분류체계 모델을 구현하기 위한 핵심 키워드를 도출하였다.

FGI는 3차까지 진행하였으며, 3차 FGI는 인적 취약점 분류체계를 구성하기 위한 최종 인터뷰로 진행하였다. 마인드맵을 활용하여 그동안 도출되었던 인적 취약점 구성요소를 정리하고, 항목별 정의를 진행하였다. 2차 FGI에서 도출한 핵심 키워드로 7개의 대분류와 30여 개의 구성요소 중 의미를 부여하기 어려운 항목을 제외한 5개의 대분류와 21개 항목의 구성요소로 압축하여 최종적으로 선정하였다. 2차 FGI에서 도출된 내용 중 의미가 중복되거나 모호한 항목들은 제외하였다.

따라서 결론적으로 최종 도출된 인적 취약점 분류체계의 구성요소는 대분류 기준 첫 번째 우발적인 상황에서 유발되는 인적 취약점인 우발성(Accidentality) 영역으로 이에 따른 세부 구성요소로 개인성, 활동성, 위험성, 보안성을 핵심 구성요소로 도출하였다. 두 번째, 개인의 우발적인 상황에서 벗어나 다른 사람과의 관계로부터 유발될 수 있는 인적 취약점인 관계성(relationship) 영역에서는 인맥, 연결성, 갈등, 청탁을 구성요소로 도출하였으며, 세 번째, 조직, 사회 전반적인 측면에서 유발될 수 있는 인적 취약점 유발 요인을 잠재성(potentiality)이라 정의하고 업무환경, 조직성, 규칙성, 사회성을 핵심 구성요소로 도출하였다. 네 번째, 인적 취약점을 유발하는 심리학적인 접근을 심리학적(psychological) 영역으로 정의하고 심리학의 5대 관점인 생물적, 인지적, 행동적, 정신분석적, 인본주의적 관점을 핵심 구성요소로 도출하였다. 즉, 인간의 심리학적인 측면에서 유발될 수 있는 요소에 초점을 맞추었다. 마지막으로 다섯 번째, 윤리성(ethicality) 영역에서는 도덕적 이탈, 탈선, 이익실현, 사이버 윤리까지 충분히 공감할 수 있는 옳고 그름의 행위들을 기준으로 구성요소를 최종 도출하였다.

3.3 인적 취약점 분류체계 및 구성요소 제안

이처럼 전문가 그룹의 의견을 정리하여 도출된 5개의 인적 취약점 분류체계는 우발성, 관계성, 잠재성, 심리학적, 윤리성으로 분류하여 Table 5.과 같이 정의하였고, 각각의 인적 취약점 분류체계와 이에 따른 항목별 구성요소는 Table 6.과 같이 정의하여 인적 취약점 분류체계를 제시하였다.

Table 5. Composition and definition of human vulnerability classification system

Components	Definition
Accidentality	• Vulnerability due to individual characteristics of a person • Personal Propensity,Personal Authority,Personal Carelessness,Personal Security Level
relationship	• Vulnerability due to relationships with others • Personal Connectivity, Social Networking, Social conflict, Illegal Solicitation
potentiality	• vulnerability due to relationships across society as a whole • Organizational Culture, Customary Practice, Security Compliance, social influence
psychological	• fundamental human vulnerability • Biological, Cognitive, Behavioral, Psychoanalytic, Humanistic
ethicality	• common ethical vulnerability • Moral Disengagement, Intentional Crime, Ill-gotten Profit, Cyber Ethics

Table 6. Definition by Human Vulnerability Component

Division	Component	Component Definition
Accidentality	Personal Propensity	• a sense of superiority using one's position or privilege • an act solely to make oneself stand out
	Personal Authority	• individual characteristics, tendencies, and interests • Personal activities such as e-mail, SNS, blogs, etc.
	Personal Carelessness	• individual characteristics such as mistakes/reminds/errors/aids[12] • Characteristics of Personal Perception
	Personal Security Level	• Security Knowledge, Ideas, and Consciousness Levels
Relationship	Personal Connectivity	• Relationships according to social activities such as meetings, organizations, etc. • a relationship of friendship, power, compassion, trust
	Social Networking	• Complex networks of e-mail, SNS, blogs, chat, etc.
	Social conflict	• Various issues related to relationships with people.
	Illegal Solicitation	• Conflicts of interest due to relationships with people
Potentiality	Organizational Culture	• the characteristics or culture of an organization/society
	Customary Practice	• Organization/society work processes and division of work
	Security Compliance	• Strength of security compliance implementation

Division	Component	Component Definition
Potentiality	Social influence	• Increasing Non-face-to-face IT Environment Due to Pandemic • Communication, Financial Transactions, and Changes in Cultural Life
Psychological	Biological	• Vulnerability from a Biological Functional Perspective
	Cognitive	• Vulnerability in the Thinking Process
	Behavioral	• Vulnerability in observable behavior
	Psychoanalytic	• the vulnerability of unconscious factors
	Humanistic	• Potential human desires (human perspective, hierarchy of needs)
ethicality	Moral Disengagement	• a distortion of behavior
	Intentional Crime	• Blind self-avoidance, self-satisfaction, self-indulgence.
	Ill-gotten Profit	• economic transactions with social stakeholders
	Cyber ethics	• moral responsibility and obligations for Internet activities

IV. 설문조사 분석 및 연구 결과

4.1 설문조사 방법 및 대상

설문지 문항은 FGI에 따른 의견들과 자료를 기반으로 한 연구자 의견을 정리해서 인적 취약점 분류체계 및 세부 구성요소를 검증할 수 있도록 진행하였다. 즉 인적 취약점 5개 대분류에 따른 세부 구성요소를 질문 문항으로 작성하였으며, 측정용 도구의 척도는 5점 척도 (매우 적합하지 않다, 적합하지 않다, 보통이다, 적합하다, 매우 적합하다)로 구성하였다. 설문지 설계는 인적 취약점 분류체계에 포함된 구성요소 간의 관계가 성립되는지 검증할 수 있도록 설계되었다. 즉 대분류별 구성요소를 변수로 하여 구성요소별 기술 통계량과 신뢰도를 분석할 수 있도록 진행하였다. 설문조사 대상은 정보보안 관련 분야에서 보안 Consultant 및 SI PM Group 그리고, 보안 분야에 종사하는 전문가(보안업무 담당자, 보안솔루션 개발책임자, 개발자, 일반 업무 관리자와 실무자, 영업담당자 등)와 일반적인 조직 내 보안과 관련된 업무를 경험해볼 수 있는 이용자를 선정하여 설문하였다.

4.2 인구통계학적 특성 및 기술 통계량 분석

본 연구에 참여한 응답자는 총 134명이며, 남성 101명, 75.4%이며, 여성 33명, 24.6%가 설문에 응답하였다. 전체 참여자의 인구통계학적 특성은 Table 7.과 같다.

IT 정보보안에 관련된 이해관계자는 IT 개발자나 엔지니어가 38명(28.4%) 가장 많았으며, 보안

Table 7. Demographic characteristics

Division		Frequency(persons)	Percent
Gender	Male	101	75.4
	Female	33	24.6
	Total	134	100
Age	20 ~ 29	13	9.7
	30 ~ 39	34	25.4
	40 ~ 49	61	45.5
	50 ~	26	19.4
	Total	134	100
Stakeholder	Security practitioner	15	11.2
	Security Solution Developers	2	1.5
	Security Consultant/SI	21	15.7
	Security Officer (manager)	9	6.7
	IT developer (engineer)	38	28.4
	a business manager	18	13.4
	General Operations Officer	16	11.9
	Sales Representative	3	2.2
	etc.	12	9.0
	Total	134	100

consultant 및 SI PM Group이 21명(15.7%), 일반 IT 업무관리자 18명(13.4%), 일반 업무실무자 16명(11.9%), 보안업무 담당자 15(11.2%), 보안책임자나 관리자 9명(6.7%), 영업담당자 3명(2.2%), 보안솔루션개발자 2명(1.5%), 기타 12명(9.0%) 분포로 조사 되었다.

인적 취약점 분류와 각 분류별 구성요소에 관한 기술 통계량 분석은 Table 8.과 같이 산출되었다. 134개의 표본은 모두 유효한 것으로 나타났으며, 기술 통계량 결과 최솟값(Min. Value)은 3.50 이상, 최댓값(Max. Value)은 4.05로 나타났다. 결론적으로 평균값(Mean, 이하 'M')이 3.0 이상이므로 인적 취약점 분류에 대한 세부 구성요소가 모두 인정되는 것으로 확인되었다.

즉, 5가지 인적 취약점과 이에 대한 세부 구성요소의 분석 결과가 본 연구에서 유 의미하게 해석되는 이유는 사람의 철저히 개인적인 관점에서 발생할 수 있는 우발적인 인적 취약점에서 출발해서 다른 사람과의 복잡한 관계에 따른 인적 취약점인 관계성 그리고 조직 및 사회 전반적인 관계에서 발생할 수 있는 인적 취약점으로 점진적인 대상의 확장에 따라 분류하고 심리학적인 측면에서의 인적 취약점 유발 가능성과 윤리적인 측면을 포함함으로써 인간이 취약점을 유발할 수 있는 분류의 범주를 크게 5가지가 적합한지의 분석 결과로 볼 수 있다.

Table 8. Component descriptive statistics

Division	Component	N	Min. value	Max. value	M	SD*
Accidentality	Personal Propensity	134	1	5	3.62	0.679
	Personal Authority	134	1	5	3.56	0.821
	Personal Carelessness	134	1	5	3.78	0.986
	Personal Security Level	134	1	5	3.91	0.812
Relationship	Personal Connectivity	134	1	5	4.02	0.829
	Social Networking	134	1	5	3.91	0.905
	Social conflict	134	1	5	3.75	0.928
	Illegal Solicitation	134	1	5	3.99	0.947
Potentiality	Organizational Culture	134	1	5	3.81	0.649
	Customary Practice	134	1	5	3.78	0.884
	Security Compliance	134	1	5	3.64	0.927
	Social influence	134	1	5	3.67	0.956
Potentiality	Organizational Culture	134	1	5	3.81	0.649
	Customary Practice	134	1	5	3.78	0.884
	Security Compliance	134	1	5	3.64	0.927
	Social influence	134	1	5	3.67	0.956
Psychological	Biological	134	1	5	3.50	0.882
	cognitive	134	1	5	3.77	0.948
	Behavioral	134	1	5	3.63	0.769
	Psychoanalytic	134	1	5	3.72	0.889
	Humanistic	134	1	5	3.65	0.775
Ethicality	Moral Disengagement	134	1	5	3.95	0.674
	Intentional Crime	134	1	5	3.71	0.772
	Ill-gotten Profit	134	1	5	3.95	0.801
	Cyber ethics	134	1	5	4.05	0.915

* SD : Standard Deviations

4.3 인적 취약점 분류체계 및 구성요소 신뢰도 분석

인적 취약점 분류체계별에 대한 신뢰도 분석은 Table 9.와 같이 산출되었다. 구성요소 즉, 측정 변수들의 신뢰도 분석을 통하여 변수의 문항 내적 일관성을 파악할 수 있는 크론바흐 알파 계수(Cronbach α)를 확인할 수 있다.

인적 취약점 분류체계의 신뢰도 분석 결과 5가지 분류에 대한 항목별 Cronbach α 값이 0.874로 나타났으며, 항목별 항목 제거 시 값은 Cronbach α 값이 0.874보다 낮게 나타났기 때문에 항목을 제거하면 신뢰수준이 낮아지므로 인적 취약점에 대한 5

Table 9. Reliability analysis of Components

Division	Cronbach α when removing items	Cronbach α
Accidentality	.838	.874
Relationship	.855	
Potentiality	.843	
Psychological	.855	
Ethicality	.844	

가지 각 항목은 신뢰수준을 저해하는 항목이 없다고 볼 수 있다. 따라서 선행 연구가 없었던 분류체계 모형이고 보안사고 예방을 위한 인적 취약점 분류에 대해 매우 중요한 특성을 표현하고 있어서 제시된 바와 같이 신뢰성 측정 결과를 통해 검증을 진행했다.

인적 취약점 분류체계별 구성요소 간 신뢰도 분석은 Table 10.과같이 나타났다. 인적 취약점 분류체계 각각의 신뢰도 분석은 Table 10.에 제시된 바와 같이 Cronbach α가 0.8 이상의 신뢰계수이므로 측정항목 간의 신뢰도에는 이슈가 없는 것으로 나타났다.

우발적인 상황에서의 인적 취약점 유발과 관련한 4가지 구성요소의 Cronbach α 값은 0.838의 수치로 높은 신뢰도를 형성하고 있는 것으로 나타났으며, 관계성의 특성에서 인적 취약점 유발과 관련한 4가지 구성요소 역시 Cronbach α 값은 0.855로 유의미한 신뢰도를 보였다. 그리고 잠재적인 인적 취약점 유발과 관련한 4가지 구성요소 또한 0.843으로 높은 신뢰도를 보였고, 심리적인 상태의 인적 취약점 유발 요인 5가지와 윤리성 관련 인적 취약점 유발 요소 4가지 역시 Cronbach α 이 각각 0.855, 0.844로 유의미한 신뢰도를 나타냈다.

모든 항목의 문항 제거 시 척도 값과 Cronbach α 값의 결과가 0.6 이상으로 유의미한 측정값을 나타내고 있으므로 5가지 분류 항목별 구성요소에 따른 신뢰도 측정항목에는 이슈가 없었다.

4.4 연구 결과

연구 결과에서 검증된 바와 같이 5개의 인적 취약점 대분류가 명확하게 완성되었으며, 영역별 구성요소 간 신뢰도 검증은 유의미한 것으로 나타났다. 따라서 본 연구에서 제시하는 인적 취약점 분류체계 및 구성요소를 Fig. 1.과 같이 정리할 수 있다. 즉, 인간 중심 보안의 취지에 따라 인적 취약점 분류체계를 개인의 특성에서, 다른 사람과의 관계, 조직 및 사회

Table 10. Reliability analysis of Components

Division	Component	Alpha if Item Deleted	Cronbach α
Accidentality	Personal Propensity	.957	.838
	Personal Authority	.956	
	Personal Carelessness	.955	
	Personal Security Level	.956	
Relationship	Personal Connectivity	.954	.855
	Social Networking	.954	
	Social conflict	.955	
	Illegal Solicitation	.954	
Potentiality	Organizational Culture	.955	.843
	Customary Practice	.954	
	Security Compliance	.955	
	Social influence	.955	
Psychological	Biological	.955	.855
	Cognitive	.954	
	Behavioral	.955	
	Psychoanalytic	.955	
	Humanistic	.955	
Ethicality	Moral Disengagement	.954	.844
	Intentional Crime	.954	
	Ill-gotten Profit	.955	
	Cyber ethics	.955	

전반의 관계, 일반적인 사람과의 관계 그리고 마지막으로 사회 공통적인 기준의 흐름으로 개인에서 점진적으로 복잡성을 띠는 사회적 관점에서 분류 기준을 수립했다. 이에 따라 대분류로 우발성, 관계성, 잠재성, 심리학적, 윤리성의 다섯까지 큰 틀에서 21개의 세부 구성요소를 구성했다. 인적 취약점은 사람들의 행동이나 실수, 부주의 등으로 인해 발생하는 보안 위협이다. 인적 취약점은 매우 다양한 유형이 존재할 것으로 유추하지만 구체적인 선행연구 사례는 없었다. 따라서 다음과 같이 구분해 볼 수 있다. 첫 번째 사회 공학적 취약점(Social engineering vulnerabilities), 인적오류 취약점 (Human error vulnerabilities), 인적 기반 취약점 (Human-based vulnerabilities), 기술적인 취약점에 대한 사람들의 활동 (Human activity related vulnerabilities)으로 구분해서 볼 수 있

고 이러한 취약점들은 조직이나 개인이 보안대책을 수립할 때 고려해야 할 요소로 판단 된다. 즉, 사회공학적 취약점은 Fig. 1. 의 분류 모델에서 찾아보면 우발성, 관계성, 잠재성 영역에 해당할 것이며, 인적오류 취약점 역시 우발성, 심리학적인 영역과 관련된 취약점으로 볼 수 있다. 인적 기반의 취약점은 우발성, 관계성, 잠재성, 심리학적 영역이 모두 포함될 수 있으며 기술적인 취약점에 대한 사람들의 활동은 잠재적인 영역으로 볼 수 있다. 따라서 본 연구에서 제시하고 인적 취약점 분류체계를 바탕으로 구체적인 측정지표와 점검 항목을 도출함으로써 기술적 및 정책적 보안과 함께 고려하면 좀 더 효율적인 보안대책을 마련하고 실효성 있는 보안 교육으로 연계될 수 있을 것으로 기대된다.

또한, 인간 중심 보안을 위한 인적 취약점 분류체계가 갖는 의미는 첫 번째, 사람은 기술보다 약하기 때문에 최첨단 기술이 사용자의 실수나 부주의로 인해 보안 위협을 생산해 낼 수 있다. 따라서 완벽한 방어 시스템이 구축되어 있더라도 사용자들은 이를 무시하거나 우회하기 쉽다. 인간 중심적인 보안 접근 방식은 사용자의 실수를 최소화하면서 보안을 강화할 수 있다. 두 번째, 인간 중심적인 보안은 사용자의 편의성과 보안성을 모두 고려할 수 있다. 즉, 사용자들이 보안 규정을 준수하기 어려워하거나, 규정 준수가 불편하다면 보안 위협에 대한 대응이 더 어려워질 수 있다. 그러나 사용자들이 보안 규정을 따르기 쉽게 만들면 보안 위협을 예방하고 대응할 수 있다. 세 번째, 사회공학 기술(Social Engineering)은 사람들의 신뢰나 인내심을 이용해 보안 시스템을 우회하는 기술이다. 인간 중심적인 보안은 이러한 공격에 대한 방어력을 향상하는 데 도움을 줄 수 있다. 사용자들이 보안 시스템을 믿고 쉽게 따르게 하는 것이 사회 공학적 기술에 대한 방어력을 높이는 데 매우 중요하다고 볼 수 있다. 마지막으로 새로운 기술의 사회적 확산이 보안 측면에서는 복합적인 취약점을 가질 수 있다. 따라서 인간 중심적인 보안 접근 방식과 인적 취약점 분류체계를 기반으로 사용자들이 새로운 기술을 쉽고 안전하게 받아들일 수 있는 기반이 조성될 것이다[9].

V. 결 론

빠르게 변화하는 정보통신 환경에 적응하고 유연하게 대응하기 위해서 보안의 중요성을 빼놓을 수 없다. 앞서 살펴본 바와 같이 그동안 정보보안이 기술적, 정책적, 관리적 측면에 집중됐다면 이제는 인간 중심 보안의 패러다임에 따라 사람에 초점이 맞춰져야 하고 인적 취약점에는 어떠한 특성들이 있는지 분석해야 한다.

이러한 취지에서 인간중심 보안은 기존 통제 중심의 보안에서 사람 중심으로 보안의 패러다임을 바꾸고 자율성과 책임성을 보장하면서 빠르게 전파되는

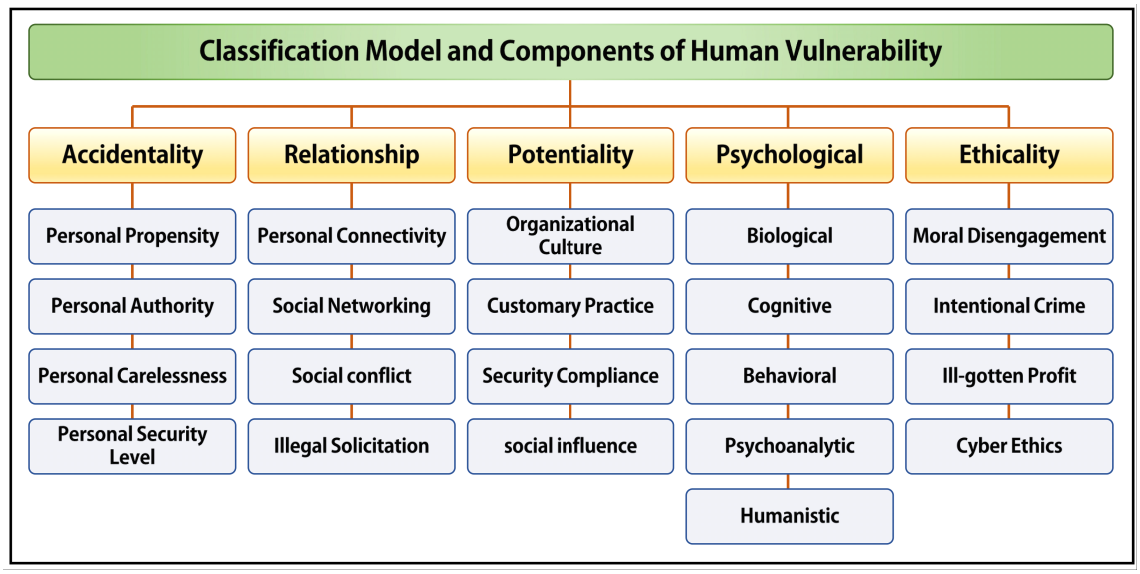


Fig. 1. Classification Model and Components of Human Vulnerability

IT 신기술의 흐름 속에서 근본적인 보안의 문제를 인식하는 전환점이 될 것이다.

본 연구에서는 이러한 인간중심 보안의 패러다임 속에서 사람의 취약점에 대해서 체계적인 분류를 통해서, 정성적, 정량적인 가치를 부여함으로써 기존 통제 중심의 보안과 함께 매우 긍정적인 시너지가 될 것이다. 특히, 집중적인 전문가 인터뷰 및 설문조사를 통해서 인적 취약점의 5가지 영역과 세부 구성요소에 대한 신뢰도 검증이 매우 긍정적으로 분석됨으로써 그동안 인적 보안이 교육이나, 보안 인식에 집중되었던 한계에서 벗어나 새로운 전환점이 마련될 것으로 기대한다[12][13][14].

다양한 조사 결과에 따르면 실제 보안 사고의 원인 중 대다수가 사용자의 실수에 기인하고 있다. 예컨대 악성코드를 내려받는 경우, 악성 이메일에 첨부된 파일을 실행하는 경우, 피싱 사이트에 개인정보를 입력하는 경우 등이 대표적인 예라고 할 수 있다. 따라서, 사용자들의 편의성과 보안성을 모두 고려하는 인간 중심 보안은 필수적이라고 할 수 있다. 또한 인간 중심 보안은 사용자가 보안 규정을 따르기 쉽게 만든다. 예를 들어, 복잡한 비밀번호를 요구하는 것보다, 사용자가 쉽게 기억할 수 있는 비밀번호를 사용하도록 권장하는 것이 보안 규정 준수를 높이는 데에 효과적이다. 이는 보안 위협에 대한 대응력을 높이는 데에도 도움을 준다. 인간 중심 보안은 조직 내 보안문화를 강화하는 데에도 도움이 된다. 보안 규정 준수를 쉽게 만들어 줌으로써, 사용자들이 보안을 중요하게 생각하도록 유도할 수 있다. 이는 보안사고를 예방하고, 조직 내 보안 인식을 높이는 데에 효과적이다. 더불어 새로운 기술의 도입은 복합적인 취약점을 가질 수 있다. 따라서 인간중심 보안을 고려함으로써, 사용자들이 새로운 기술을 쉽게 받아들이도록 만들 수 있다. 이는 새로운 기술의 도입 속도를 높이는 데에도 도움이 된다. 인간 중심 보안은 사회공학 기술(Social engineering) 공격에 대한 대비책을 제공할 수 있다. 결론적으로 인간 중심 보안의 관점에서 인적 취약점 분류체계를 참고하면 기술, 정책 중심의 보안에서 인간 중심 보안으로 패러다임 전환의 흐름에 실효성 있는 접근이 될 것으로 기대한다[9].

무엇보다도 본 연구에서 제시하는 인적 취약점 분류체계는 철저하게 사람 관점에서의 취약점을 유발할 수 있는 상황을 분류함으로써 기술적, 정책적 보안에 편중되었던 보안의 패러다임을 전환하고 새로운 관점에서 새로운 기술변화에 적응할 수 있는 보안대책을 제시할 수 있을 것으로 기대하고 이를 토대로 향후 인적 보안 연구에 활발한 기폭제가 될 것으로 확신한다.

References

[1] Hyeon-Dae Rha and Hyun-soo Chung, "A Theoretical Comparative Study of Human Resource Security Based on Korean and Int'l Information Security Management Systems," *Convergence Society for SMB*, 6(3), pp. 14-15, Sep. 2016

[2] inistry of Science ICT and Future Planning, "K-ICT Security SAPAR", M, pp. 9-10, Apr. 2015

[3] Economic Review, "Cyber War", https://www.econovill.com/news/articleView.html?idxno=289519, 25 May 2016

[4] Etnews, "Cyber incidents", https://www.etnews.com/20220418000218, 18 Apr. 2022

[5] Cha, In hwa, "An Empirical Research on Developing Personnel Security Management Indicators in Information Security", doctor thesis , Kwangwoon University, pp. 19-20, 40-68, Aug. 2009

[6] T.K. Lee, "Prevention of Industrial Information Leakage & Methods for Managing Personnel Security",Master Thesis, Sungkyunkwan University, pp. 13, Jun. 2011

[7] Jinhyeong Cho, Yongki Chung, Hyeonho Park,"A Study on the Improvement of Physical and Personnel Security System in Industry Field", Korean Police Studies,17(2), pp. 7-10, Jun. 2018

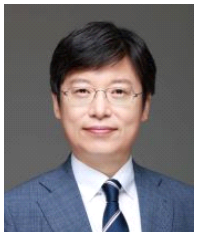
[8] Jungduk Kim, "People Centric Security for Digital Financial Innovation and Stability", e-Finance and Financial Security, Financial Security Institute, 25, pp. 8-9 ,3Q. 2021

[9] D.H. Yoo, "Research on People-Centered Security Policy to Strengthen Research

Security", doctor thesis, Myongji University, pp. 27-29 , Aug. 2021
〔10〕 Shin Min-ju, Baek Dong-hyun, Kim Dong-san, and Yoon Wan-cheol, "Development of a framework for supporting system for human error analysis", "the Korea Management Information Society conference", pp.617-622, 2007
〔11〕 Jeong Hye-in and Kim Seong-jun,"Influence on Information Security Behavior of Members of Organizations: Based on Integration of Theory of Planned Behavior (TPB) and Theory of Protection Motivation (TPM)", "security studies", 56, pp.151-152, 2018
〔12〕 J.H. Lee, H.Y. Kown, "A Study on Human Vulnerability Factors of Companies : Through Spam Mail Simulation Training Experiments", Journal of The Korea Institute of Information Security & Cryptology, 29(4), pp. 3-4, Aug. 2019
〔13〕 C.H. Lee, M.S. Shin,"A Study on the Influence of Security Perception in the Relationship between Internal and External Motivation and Security Behavior in the Organization", Korea Management Information Society Conference, pp.437-442, 2010
〔14〕 M.H. Lee, J.H Lee, "Effects of administrative security activities and expertise of security personnel on technology leakage prevention", Korean Security Administration Review, 12(2), pp. 165-182, 2015
〔15〕 Theguardian, "Facebook-Cambridge Analytica" https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election, Sat 17 Mar 2018
〔16〕 boannews, "Equifax data breach", https://www.boannews.com/media/view.asp?idx=85845, 17 January 2020
〔17〕 boannews, "Personal information leakage",https://www.boannews.com/media/view.asp?idx=88340, 25 May 2020
〔18〕 boannews, "human-centric", https://www.boannews.com/media/view.asp?idx=117091, 13 April 2023
〔19〕 YouTube, "people-centric security". https://www.youtube.com/watch?v=zGDN-WKGcDI, 18 March 2022

〈저자소개〉

박 정 준 (Jungjun Park) 정회원
1997년: 우석대학교 수학과 (이학사)
2015년: 성균관대학교 IT컨설팅학과 (공학석사)
2019년: 성균관대학교 대학원 컨퓨터교육과 (박사수료)
〈관심분야〉 정보보호, 시스템보안, 인적보안, 인간중심보안, 컴퓨터교육



안 성 진 (Seongjin Ahn) 종신회원
1988년: 성균관대학교 정보공학과 (학사)
1990년: 성균관대학교 정보공학과 (석사)
1998년: 성균관대학교 정보공학과 (박사)
1996년: 정보통신기술사
1999년~현재: 성균관대학교 컴퓨터교육과 교수
〈관심분야〉 네트워크관리, 산업보안, SW·AI 교육, AI 윤리