컴퓨터교육학회 논문지 2024년 제27권 제1호
https://doi.org/10.32431/kace.2024.27.1.014

델파이 조사를 통한 인적 취약점 분류체계 기반 인적보안 측정지표 연구

A Study on the Human Security measurement indicators Based on the Human Vulnerability Classification System through Delphi Survey

박정준† · 안성진††
Jungjun Park† · Seongjin Ahn††

요 약

정보보안 산업은 IT의 다양한 변화와 위협 속에 끊임없이 성장해 왔다. 특히 기술적, 관리적 측면의 보안은 매우 높은 수준의 대응 방안을 제시해왔다. 그런데도 보안 사고는 끊임없이 발생해 왔고, 보안의 한 분야인 인적 보안에 대한 영역은 구체적인 분석과 대안없이 형식적인 가이드 수준에서 벗어나지 못하고 있다. 본 연구에서는 인적 취약점 분류체계 기반의 측정지표를 연구하는 데 중점을 두었고, 보안 전문가, 보안 컨설턴트, 보안 업무 담당자, 보안 책임자, 교수, 심리학자 등 다양한 관련분야 전문가 25명을 대상으로 집중적인 델파이 조사를 통해 총 86개 측정지표를 도출하였고, 타당성과 신뢰성 분석을 통해서 59개의 의미 있는 인적보안 측정지표를 제시했다. 선정된 측정지표는 인적 보안 사고를 예방하기 위한 의미 있는 요소를 식별함으로써 기술적, 관리적 보안과 함께 인적 보안 위협을 예방하기 위한 구체적인 지표로써 설득력 있는 보안정책 및 교육방안을 제시해 줄 수 있을 것으로 기대한다.

주제어: 인적 취약점 분류체계, 인적 보안 측정지표, 인적 보안

ABSTRACT

The field of information security has continuously grown within the ever-changing landscape of IT and threats. Particularly, security in both technical and managerial aspects has consistently presented high-level response strategies. Despite these efforts, security incidents have persisted, and the domain of human security, a facet of security, remains largely confined to formal guide-level discussions without concrete analysis or alternatives. This study focuses on researching a measurement framework based on classifying human vulnerabilities. It emphasizes the derivation of measurement indicators. Through concentrated Delphi surveys targeting 25 experts from various relevant fields such as security professionals, security consultants, security personnel, security managers, professors, and psychologists, a total of 86 measurement indicators were derived. Subsequent validity and reliability analyses led to the identification of 59 meaningful indicators for human security. These selected indicators, identifyig significant elements for preventing human security incidents, are expected to serve as specific measures to prevent human security threats in conjunction with technical and managerial security. It is anticipated that these indicators will provide compelling security policies and educational strategies.

Keywords: Human Vulnerability Classification, Human Security Measurement indicators, Human Security

1. 서론

인적 보안은 보안 분야에서 항상 언급 되어왔고, 그 중요성에 대한 공감대는 오랫동안 형성되어 왔으나, 구체적인 원인 분석이나 관련분야 연구에 대한 자료는 매우 부족한 것이 현실이다. 단적으로 인적 보안에

†정 회 원: 성균관대학교 대학원 컴퓨터교육과 박사수료
††종신회원: 성균관대학교 컴퓨터교육과 교수(교신저자)

논문투고: 2023년 09월 01일, 심사완료: 2023년 10월 27일, 게재확정: 2023년 11월 15일

관한 국내외 정보보호 관리체계 인적 보안 통제 항목을 살펴보면 관련분야 연구가 얼마나 정체되어 있는지 실감할 수 있다. 즉, 정보보호 책임자 선정, 주기적인 교육, 보안 서약서 및 퇴직자에 대한 관리 그리고 출입 통제 등을 언급하고 있다. 이는 기존 수십 년간 기술적, 관리적 중심의 IT 보안에 지극히 표면적이고 상투적인 관점에서 인적 보안의 최소한의 관리적 요소만 언급한 것이 입증됐다고 볼 수 있다[1].

또한, 기존 IT 자산 중심의 보안 위험 관리는 많은 문제점이 제기되어져 왔다. IT 자산에 대한 위험평가와 대책 수립에 초점이 맞추어져, 비즈니스 및 사회적 환경 변화에 대응하는데 한계가 존재했으며, 컴플라이언스 기반의 보안 활동에 익숙하므로 보안 위험 관리는 형식적인 수준에서 수행되고 있다. 따라서, 최근 금융권을 중심으로 컴플라이언스 기반을 벗어나서, 위험 기반의 자율 보안 체계를 시행하고 있으며, 일부 가이드라인이 개정 중이다[2].

또한 현재의 급속한 인터넷 환경변화는 사이버 위협의 지능화, 고도화를 촉진 시켜서 산업 전반의 위협을 확대하고 있다. 2018, 2020년 한국인터넷진흥원 정보보호 실태조사에 따르면 지난 5년간 침해 사고 경험률은 270개 기업, 3%대가 지속되고 있다고 조사되었으며, 응답 기관의 73%는 침해 사고에 대응하기 위한 별다른 활동을 수행하지 않는다고 한다. 이는 정보보안 사고 대비가 매우 취약한 상황을 보여주는 것이며 사회공학적 활동에 따라 침해 사고 발생 시 부차적인 피해를 초래할 가능성이 매우 높다고 볼 수 있다. 또한 실제 산업현장에서는 정보보호 실태조사 미참여 업체 및 침해 사고 피해를 본 업체의 시고 거부 등의 활동을 추산하면 통계조사 수치보다 훨씬 많은 기관이나 기업의 침해 사고 피해를 추정할 수 있다.

따라서, 본 연구에서는 인적 보안에 대한 취약성을 구체적인 유형과 분류에 따라 측정 지표를 도출함으로써, 보안을 한 단계 높은 수준에서 예측하고 예방하는 방안을 제시해 보고자 한다.

2. 이론적 배경

2.1 연구의 필요성 및 연구의 의미

인적 보안은 오랫동안 강조됐던 보안의 한 분야임에도 불구하고 집중적인 연구나 투자가 지속해서 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, 시스템보안 취약점과 같이 DB, Network, Server, End-Point 등 각각의 영역별 체계적인 분류를 기반으로 대응 방안을 마련해 왔던 것처럼, 마찬가지로 인간이 유발할 수 있는 취약점의 유형에 대한 근본적인 분류체계 및 측정 지표가 매우 중요한 출발점이 될 수 있을 것이다[3]. 또한 심리학에는 학습 심리학, 사회심리학, 인지심리학 등 다양한 분야가 있으며, 분야에 따라 관점이 다르지만 인간 행동의 원인을 규명하는 것이라는 공통적인 목적이 있다. 즉, 선천적인 생물학적 요인과 후천적인 환경적 요인이 다양한 심리적 요인에게 영향을 주어 행동으로 연결되는 과정을 연구하는 것이다[1]. 따라서 정보보호 분야에서도 기술적인 도구에 중점을 둔 연구도 중요하지만, 조직의 정보보호 정책을 준수하는 행동에 영향을 주는 다양한 요인을 식별하고 이에 따른 대책에 관한 연구가 수행될 필요가 있다. 글로벌 시장조사 기관인 Gartner에서는 인간중심 보안(People Centric Security)이라는 새로운 패러다임을 제시하였으며, 강압적이고 예방중심의 정보보호 통제가 아닌 임직원에 대한 신뢰를 기반으로 책임과 권한을 할당하고, 교육을 통해 정보보호 인식과 역량을 향상하는 동시에 지속적인 모니터링을 통해 이상 징후를 신속히 탐지하고 대응하는 접근 방법의 중요성을 강조하고 있다[4].

2.2 인적 취약점 분류체계 및 구성요소

인적 보안이란 조직의 구성원이 보안 정책에 따라 보안 업무를 충실히 수행하고 있는지에 대한 개인적 관점에서 보안 지침과 절차를 토대로 사람으로부터 보안 문제가 발생하는 것을 사전에 방지하기 위한 활동을 의미한다. 따라서 물리적 또는 기술적 관리 방법과는 다르게 인적 보안의 핵심은 정보를 활용하는 직원이 주체이며 보호 수단이다[5].

기존의 연구에서 인적 보안에 대한 범위는 통제 관점에서 인적 취약성을 예방하고자 하는 노력이 지속되어 왔다. 즉, 보안 서약서, 퇴사자 관리, 직무 분리, 보안 위반 시 조치, 인식 제고 및 교육 훈련 등 ISMS-P에서 제시된 통제 항목을 보더라도 통제 관점의 인적

보안을 의미하고 있는 것을 알 수 있다. 이는 인적 보안에 대한 근본적인 대안을 수립하기 어렵고, 인간이 왜 보안 사고를 유발하는지에 대한 관점의 전환이 필요하다고 볼 수 있다.

본 연구에서는 인적 보안에 대한 관점을 보다 인간 중심적(PCS, People Centric Security)인 사고를 통해서 근본적으로 인간이 IT 보안을 접하면서 유발할 수 있는 취약점을 근거로 측정 지표를 제시해 보고자 한다. 즉, 개인의 특성에 따른 예상치 못한 우발적인(Accidentality) 요소, 개인이 다른 사람과의 관계를 통해서 유발될 수 있는 관계성(Relationship)에 따른 인적 취약점 요소, 사회 조직적 관점에서 잠재적인(Potentiality) 요소, 인간 심리학적인(Psychological) 요소 그리고 마지막으로 인간 공통적인 기준인 윤리적인(Ethicality) 요소로 분류하고 이에 대한 각각의 구성요소들을 식별함으로써 인적 취약점에 대한 보다 근본적인 이슈들을 파헤치고 이에 대한 측정 지표를 제시함으로써 기술적, 관리적 보안과 더불어 보다 완성된 인간 중심의 보안을 구현하는 데 초점을 맞추고자 한다[6].

2.3 인적보안 측정지표 현황

먼저 정보보호 관리의 중요성을 살펴보면, 과학기술정보통신부와 한국지능정보사회진흥원(NIA)이 실시한 2020년 인터넷 이용 실태조사에 따르면, 2020년 7월 기준 만 3세 이상 국민 5,097만 명 중 대한민국 인터넷 이용자 수는 약 46,818,750명으로 당시 인터넷 이용률은 91.9%에 달했으며, 우리나라 1,984만 가구 중 1,980만 가구가 인터넷을 사용하고 있는 것으로 조사됐다. 국내뿐 아니라 2019년 11월 기준 세계 인터넷 사용자 수는 43억 명을 넘어섰으며 77억 세계 인구의 절반 이상이 인터넷을 사용하고 있다[7].

이러한 환경에서 사이버 위협 또한 그 규모가 점진적으로 조직적, 대규모 공격 형태와 유형 또한 다양화되고 있다. 특히 사물인터넷의 이용 확산, 빅 데이터 기술의 발달, 사이버 범죄의 지능화에 따라 정보보호 관리는 매우 절실해진 상황이다. 관리적, 기술적 보안에서의 측정 지표는 ISMS-P를 비롯한 다양한 국내외 컴플라이언스를 바탕으로 이에 대한 측정 지표가 오랫동안 개발되고 개정되어 오고 있으며, 기술적인 지표 역시 IT 시스템 운영 관리와 더불어 IT 보안 시스템에 대한 운영 및 지침에 관한 측정 지표가 개발되고 개정되고 있다. 즉, 기존의 보안 관련 측정 지표는 기술 지향의 측정 지표가 대부분이었다. 본 연구에서는 이러한 관리적 기술적 관점에서의 측정 지표를 탈피해서 인간이 취약성을 유발하는 근본적인 이유를 파헤쳐 보고 이에 따라 인적 취약점 관점에서 인적 보안에 대한 측정 지표를 도출해 보고자 노력했다[8].

또한, 인적자산에 의한 보안 사고는 지속해서 증가하는 추세지만, 보안 연구는 기술적 부분에 집중되어 있어서 인적자산 보안에 관한 연구는 매우 부족하며 기업 보안에서 자료 유출의 문제가 인적 보안 연구의 대부분이었다. 또한 인적 보안에 관한 분류나 측정 지표와 관련한 연구가 부족하여 인적 보안 측정지표 도출을 위한 선행연구 자료를 정보보호 관리체계와 인적 보안 통제 항목 중심으로 분석하고 이를 토대로 인적 보안 측정지표의 필요성을 강조하고자 했다. 따라서 국내 및 해외 주요 정보보호 관리체계는 국가별 환경의 특징을 담고 있겠으나 인적 보안의 구체적 현황을 분석하기 위하여 국내 또는 해외의 핵심적인 정보보호 관리체계에서 선정된 인적 보안 내용을 인용했다[9].

ISO27001에서는 재직 중인 직원 대상으로 교육계획을 수립하고 교육 훈련을 시행하고 있으나 ISMS 통제항목에서는 교육과 훈련 별도로 구분하여 전반적인 계획부터 평가에 관한 내용을 기술하고 있었다. ISO27001 및 ISMS에서는 양쪽 모두 상벌에 관한 규정을 두고 있었고, 조직 구성원이 정보보호 관련 정책이나 지침, 절차 등 내부 규정에 명시된 정보보호 책임을 성실히 이행하지 않고 조직 내 중요정보를 훼손하거나 유출한 경우, 규정에 따라 처벌하고 충실히 이행하였을 때 보상 방안도 함께 두고 있었다. 현재 일정 규모 이상의 기관일 경우 반드시 보안 책임자를 두고 총괄하게 되어있다. ISO27001은 업무 시점으로 제한하여 인적자산을 통제하게 되어있었다. NIST 800-53은 매우 상세하게 가이드 되어있어서 효과적인 교육 훈련과 평가 및 의식 증대를 구체적으로 제시하고 있었다. Cyber Security Framework의 경우 5단계의 시차적인 절차로 구성되어 침해 사고가 발생하면 신속한 대응과, 효율적인 교육 프로그램, IT 프로세스가 밀접한 연계성을 강조하는 특징이 있었다[1][10][11][17].

2.4 기존 연구와의 차별성

2.3에서 언급한 바와 같이 지금까지 인적보안 측정지표에 관한 연구는 없었다. 또한 참고문헌에 제시된 '인간중심 보안을 위한 인적 취약점 분류체계에 관한 연구' 에서 인용한 인적 취약점 분류체계 또한 지금까지 연구 사례를 찾아볼 수 없다. 따라서 기존 정보보호 관리체계 기준의 시스템 분류 항목이나 관리적인 통제 항목들이 인적 취약점 분류체계나 측정 지표와 차별성을 따질 수 있는 비교 대상이 될 수 있다.

특히 최근에 전 세계적인 팬데믹으로 인해 인터넷 사용률은 더욱 증가하고 있다. 이러한 환경은 공격자에게 더 많은 기회를 제공할 수 있고, 우리가 지금까지 대응했던 것처럼 시스템이나 컴플라이언스에만 의존하기에는 IT 환경이 너무 복잡해졌다. 따라서, 그동안 연구가 미흡했던 인적 보안 분야를 심도 있게 다뤄서 해법을 찾는 것이 사이버 보안의 시대적 흐름이라고 생각했다. Table 1은 2.3에 현황에서 제시한 인적보안 측정지표에 해당하는 영역별 통제 항목과 본 연구의 내용을 비교 분석했다[1]. 따라서 표면적인 인적보안에 대한 포괄적인 대책에서 벗어나서 인적 취약점 분류체계를 기반으로 인간 개인, 관계, 사회성, 심리적, 윤리적인 측면에서 측정 지표를 도출함으로써 기존에 ISO27001, ISMS-P, NIST, Security Framework에서 제시했던 보안 서약서, 직무 분리 및 퇴직자 관리 등의 통제 항목 수준을 벗어나 보고자 했다[1][6].

Table 1. Current Status of Human Security Control Items and Differentiation of this Study

Division	ISO27001	ISMS-P	NIST 800-53	This Study
Designation and management of key positions	○			Focusing on people themselves, they are classified into five major areas (Accidentality, Relationship, Potential, Psychological, and Ethical) and measurement indicators are derived accordingly.
Retirement and job change management	○			
Access Control	○			
Employment of employees		○		
management responsibility		○		
information protection education	○	○		
Reward and punishment regulations	○	○		
Organizational management			○	
External Management			○	
Human security			○	

즉, Table 1 분석 결과와 같이 본 연구에서 제시하는 사람에 초점을 맞춘 인적보안 측정지표에 대한 선행연구 자료는 없었기 때문에 불가피하게 국내외 정보보호 관리체계 기반의 인적 보안 통제 항목을 참고할 수밖에 없었고, Table 1에서 확인할 수 있는 바와 같이 교육 훈련에 대한 가이드의 구체성, 보안 사고 시 상벌 규정 및 책임 여부, 책임자 지정 평가 방식 등의 내용을 다루고 있었다. 물론 이들 내용이 중요하지 않다는 것이 아니라, 국내외 정보보호 관리체계에서 제시된 인적 보안 통제 항목을 모두 포함하고 관점을 달리해서 사람에 초점을 맞추어 본 연구에서는 그 사람의 성향이나, 관계, 사회성, 심리적인 요인 그리고 윤리적인 측면으로 분류해서 각각의 측정 지표를 도출하면 보다 근본적인 보안 사고를 예방할 수 있는 정보가 축적될 수 있을 것으로 기대한다.

3. 인적 취약점 측정지표 연구

3.1 연구 방법

본 연구에서는 인적 취약점 분류체계의 구성요소를 기반으로 국내외 인적 보안 관련 지침, 통제 항목들을 참고해서 인적보안 측정지표에 적용할 구체적인 측정 항목들을 도출하여 분석했다. 인적 보안에 관한 측정지표는 선행연구 자료가 없어서 국내외 주요 정보보호 관리체계를 비교 분석한 결과를 인용하여 인적 취약성 분류체계에 따른 인적보안 측정지표의 필요성을 강조하고자 했다. 특히, 관련 선행연구 자료가 부족한 상황에서는 인적 취약점 분류체계 및 구성요소 도출 때와 마찬가지로 분야별 전문가 그룹의 인터뷰와 브레인스토밍을 주기적으로 진행하면서 총 86개의 인적보안 측정지표를 도출했는데, 이는 인적 취약점 분류체계의 분류별 각각의 구성요소에 대한 측정 지표를 도출한 것이다. 인적보안 측정지표 도출을 위해서 8명의 관련 업계 전문가 집중 인터뷰(Focus Group Interview)를 5차례 진행하고 이를 토대로 델파이 설

문조사를 2차례 진행한 결과를 정리했다. FGI는 브레인스토밍 방식으로 진행했고, 델파이 조사를 위한 설문 구성이나 이슈 사항에 대해서 마인드맵(MindMap)과 엑셀로 결과를 정리했다. 본격적인 델파이 조사는 관련 업계 전문가 25명을 섭외하여 내용타당도를 CVR 임계치 기준으로 검증했고, 25명 조사 대상에 해당하는 공인된 기준값인 0.37 이하로 측정된 항목들을 제거하면서 최종 선정했다. 특히, 추상적인 개념이 적절히 측정되도록 설문조사 문항을 설계하고 도출된 측정 지표의 신뢰도와 내용타당도가 검증될 수 있도록 통계분석을 활용하여 연구했다[12].

연구 개발 방법 및 평가 과정을 요약하면 Figure 1과 같다. 먼저 선행연구였던 인적 취약점 분류체계 개발 과정은 국내외 관련 문헌을 수집 분석하여 FGI 대상자들과 공유한 후 보안사고 지속 발생 원인과 보안 위반 사례를 주제로 토론하고 이를 인간중심 보안(PCS) 관점에서 인적보안과의 연관성을 따져가면서 분류체계를 완성하였다. 따라서 인적 취약점 분류체계 도출 근거로는 정보보안 위반의 개념, 인간중심 보안(PCS)의 전략적 원칙, 국내외 통제 항목, 사이버 범죄 프로파일링 관점, FGI, 연구자의 의견을 종합해서 결과를 도출했다. 또한 본 연구의 주제인 인적 취약점 분류체계를 기반으로 한 인적보안 측정지표는 국내외 관련 지침과 관련 논문을 수집 분석하여 FGI 대상자들과 공유하고 측정 지표를 도출했으며, 다시 보안 전문가들 대상으로 델파이 조사를 통해서 내용타당도와 신뢰도 분석 후 최종 59개의 유의미한 인적보안 측정지표를 도출했다[13].

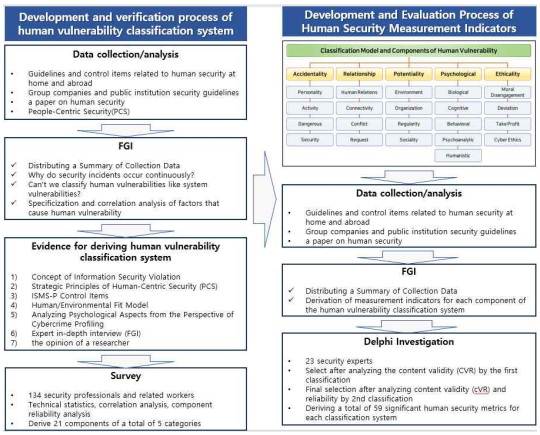


Figure 1. Research and development process and evaluation process

3.2 전문가 집중 인터뷰(FGI)

인적 취약성 분류체계 및 구성요소 그리고 관련된 측정 지표 도출을 위한 전문가 구성은 Table 2와 같다. FGI 전문가 그룹은 금융권 CSO, IT 소프트웨어 개발 업체 대표, 보안 컨설턴트, 보안 SI 시니어 PM 그룹, 그리고 보안 솔루션 엔지니어로 총 8명으로 구성하여 5차례에 걸쳐 관련 내용이 대한 의견을 수집하고, 국내외 정보보호 관리체계 및 보안 지침과 현장에서의 경험을 토대로 다양한 의견을 수렴하고 이를 토대로 인적보안 측정지표 항목들을 도출하였고, 신뢰성과 내용타당도 검증을 위해 델파이 설문조사 내용에 대한 리뷰를 반복적으로 진행했다.

특히, 보안 SI PM 그룹은 분야별 보안 현황과 컴플라이언스에 대한 지식을 갖고 있고, 인적 취약점 분류체계 및 구성요소 도출에 참여했던 전문가들로 관련해서 인적보안 측정지표 초안을 작성하는데 일관성이 있는 조언을 받을 수 있었다.

Table 2. information of experts group

Division	Number of experts(%)	information security related career(Average.year)	Average age
CSO	1(12.5%)	20	52
IT/CEO	1(12.5%)	25	56
Consultant	2(25.0%)	15	46
SI(PM)	2(25.0%)	15	48
Security Solution Engineer	2(25.09%)	10	40

3.2.1 델파이 조사 대상 선정

5차례의 전문가 인터뷰는 인적 취약점 분류체계에 대한 구성 요소별 측정 지표 도출을 위한 핵심적인 키워드를 브레인스토밍하여 결과를 정리했고, 조사 대상자 선정에도 보안 컨설턴트 및 보안 업무 담당자, 보안 책임자, 컨설턴트, 교수 등 다양한 직군을 섭외하여 검증하고자 했다. 특히 인적 취약점 분류체계 중 심리학적인 분야에 대해서는 관련분야 전공자를 섭외하여 조사에 참여시켰으며, 주로 컴퓨터 교육, 정보보호, 정보통신, IT 컨설팅 분야 전공자를 대상으로 진행했다. 특히 전문가들은 인적 취약점 분류체계와 구성요소에 공감하고, 이에 대한 측정 지표 도출이 매우 의미 있는 기준이 될 수 있다는 데 동의했다. 또한, 인적 보안에 대한 접근 방법이 기존의 보안 서약서, 교

육 및 인식 제고에서 벗어나 인간 본성의 근본적인 취약점을 식별하고, 이를 기반으로 유의미한 측정값을 도출함으로써, 향후 인적 보안 평가 및 교육 방향을 제시하는데 중복된 의견들이 많았다. 그리고, 델파이 조사를 위해 도출된 측정 지표 들은 인적 취약점 분류 체계 및 구성요소 도출에 참여했던 인력들로 충분한 공감대를 바탕으로 관련된 측정 지표 항목들을 도출하고 이를 토대로 국내외 정보보호 관리체계 및 현황에 대한 정보를 비교 분석하면서 측정 지표 항목들을 정리했다[15][16][17][18].

3.2.2 델파이 조사 내용 구성

5차례 전문가 인터뷰를 통해서 총 86개 인적 취약점 분류 항목의 구성 요소별 측정 지표 문항을 검토하고 지속적인 브레인스토밍을 진행했다. 검토 과정에서 비슷한 유형이거나, 의미가 중복되는 항목들은 제거했으며, 인적 취약점 분류체계 구성요소 취지에 맞지 않는 내용들은 충분한 의견을 수렴하여 과감하게 제거했다. 따라서 총 5개 분류 중 우발성(Accidentality) 항목의 구성요소 즉, 개인성(Personal Propensity) 지표 4종, 활동성(Personal Authority) 지표 4종, 위험성(Personal Carelessness) 지표 4종, 보안성(Personal Security Level) 지표 4종이 도출됐으며, 관계성(Relationship) 항목의 구성요소 즉, 인맥(Personal Connectivity) 3종, 연결성(Social Networking) 3종, 갈등(Social conflict) 3종, 청탁(Illegal Solicitation) 3종이 선정됐다. 그리고, 잠재성(Potentiality) 항목의 업무환경(Organizational Culture) 지표 4종, 조직성(Customary Practice) 지표 3종, 규칙성(Security Compliance) 지표 6종, 사회성(Social influence) 지표 2종이 선정되었다. 네 번째 분류 항목인 심릭학적(Psychological) 분야에서는 생물적(Biological) 6종, 인지적(Cognitive) 지표 6종, 행동적(Behavioral) 지표 6종, 정신분석적(Psychoanalytic) 지표 6종, 인본주의적(Humanistic) 지표 6종이 도출되었고, 마지막 윤리성(Ethicality) 항목의 도덕적 이탈(Moral Disengagement) 지표 3종, 탈선(Intentional Crime) 지표 3종, 이익 실현(Ill-gotten Profit) 지표 3종, 사이버 윤리(Cyber ethics) 지표 4종이 최종 도출했다. 특히 심리학적 항목의 측정 지표는 지나친 개인정보 침해로 삭제하자는 의견이 있었으나 1차 델파이 진행을 통해서 결과를 취합하여 제거하기로 했다.

3.3 인적보안 측정지표 제안

인적 취약성 분류체계와 구성요소를 토대로 인적보안 측정지표를 Table 3과 같이 정리하여 1차 델파이 조사에 활용했다. 도출된 측정 지표는 총 5개 항목 21개 구성 요소별 86개 항목의 측정 지표를 제시했다. 개인정보보호법 등 다소 무리가 가는 지표도 있을 수 있으나 1차 델파이 조사를 통한 결과를 반영해서 최적화시킬 수 있을 것으로 판단했다. 특히, 심리학적인 요소들은 개인정보보호뿐 아니라 개인 프라이버시 침해 가능성이 높아서 전문가들의 지적이 매우 심했다.

Table 3. Proposed items of human security metrics based on FGI results(86)

Division	Component	items Measurement indicators
Accidentality	Personal Propensity	• Transparency of Authority and Roles • Transparency in the Use of Authority • Designation and Management of Key Personnel Roles • Separation of Duties for the Prevention of Potential Harms like Authority Misuse
	Personal Authority	• Document Management for Personal Information-related Matters • Online Personal Information Management • Analysis of Online Public Information • Analysis of Social Media Membership Status
	Personal Carelessness	• Recognition of Attack Patterns in Social Engineering Techniques • Background Research on the Source of Online Communication • Analysis of Work Attitudes • Work Performance Evaluation for Personality Analysis
	Personal Security Level	• Regular Education and Training • Regular System Updates • Security Pledge for Awareness of Compliance Guidelines • Career Analysis for Past Behavior Assessment
Relationship	Personal Connectivity	• Utilization of Social Engineering Attack Techniques • Analysis of Relationships within the Same Industry (Competition Analysis) • Identification of Internal Conflict Factors
	Social Networking	• Regular Education and Training • Background Research on the Source of Online Communication • Continuous Propagation of Incident Cases
	Social	• Identification of Internal Conflict

	conflict	Factors • Analysis of the Importance of Assigned Tasks • Analysis of Work Attitudes
	Illegal Solicitation	• Identification of Financial Gain Necessity • Identification of Job Transition Possibility • Identification of Internal Conflict Factors
Potentiality	Organizational Culture	• Transparency in Task Handling • Transparency in Work Performance • Transparency in Work Responsibilities • Ensuring Transparency in Security Rule Compliance
	Customary Practice	• Transparency in Work Collaboration • Ensuring Fairness in Work Performance Measurement • Elimination of Conventional Work Habits
	Security Compliance	• Security Issue Analysis for Emerging Technologies • Periodic Sharing of Security Incident Cases
	Social influence	• Transparency in Compliance Adherence Status • Prevention of Compliance Evasion Strategies • Implementation of Periodic Security Awareness Training • Elimination of Coercive Security Directives • Retirement and Job Transition Management • Actions in the Event of Security Violations
Psychological	Biological	• Personality Analysis for Behavioral Profiling • Analysis of Growth Process • Tendency Analysis for Behavioral Profiling • Identification of Nervous System Activities • Hormone Levels • Genes and Genetic Vulnerability
	Cognitive	• Analysis of Judgement Capability • Work Collaboration Attitude • Cognitive Ability Test • Perceptual Ability Test • Cognitive Development Assessment • Cognitive Flexibility Assessment
	Behavioral	• Job Competency Analysis • Analysis of Work Activities • Behavior Observation for Behavior Pattern Analysis • Behavioral Recording for Behavior Pattern Analysis • Self-Reporting Method for Behavior Pattern Analysis • Behavior Assessment Scale
	Psychoanalytic	• Work Performance Analysis • Incident History Analysis • Projection Test • Free Association for Unconscious Analysis • Dream Interpretation for Unconscious Analysis • Self-Analysis through Inner Exploration
	Humanistic	• Subjective Experience-based Personality Analysis • Identification of Internal Conflict Factors • Identity-based Self-Concept • Values Assessment • Measurement of Autonomy • Life Satisfaction Scale
Ethicality	Moral Disengagement	• Ethical Education • Enhancing Ethical Judgment • Regular Ethical Education
	Intentional Crime	• Cognitive Deviation Analysis • Emotional Deviation Analysis • Behavioral Deviation Analysis
	Ill-gotten Profit	• Transparency in Achieving Economic Gains • Transparency in Achieving Social Benefits • Transparency in Achieving Emotional Benefits
	Cyber ethics	• Personal Information Protection • Online Communication • Respect for Copyright • Prevention of Cybercrime

FGI를 통해 최초 도출된 측정 지표와 1차 델파이 조사 진행 후의 선정된 측정 항목을 비교한 현황은 Table 4와 같다.

Table 4. Status of the number of items Measurement indicators verification by component

Division	Component	Number of Derived Measurement Items	Number of Initially Selected Measurement Items
Accidentality	Personal Propensity	4	4
	Personal Authority	4	3
	Personal Carelessness	4	2
	Personal Security Level	4	3
Relationship	Personal Connectivity	3	3
	Social Networking	3	3
	Social conflict	3	1
	Illegal Solicitation	3	2
Potentiality	Organizational Culture	4	4
	Customary Practice	3	3
	Security Compliance	2	2
	Social influence	6	6
Psychological	Biological	6	1
	Cognitive	6	3
	Behavioral	6	3
	Psychoanalytic	6	2
	Humanistic	6	2

Ethicality	Moral Disengagement	3	3
	Intentional Crime	3	3
	Ill-gotten Profit	3	3
	Cyber ethics	4	4
Total		86	60

4. 설문조사 분석 및 델파이 조사 결과

4.1 조사 대상 및 인구통계학적 특성

본 연구는 정보보안 분야별 경력자 관련분야 컨설턴트, SI PM, 개발자, 엔지니어, 심리학자 등 전문가의 경험, 지식, 의견을 통한 문제해결 방법과 미래 예측을 위한 델파이 조사 기법을 활용하여 진행될 것이며, 전문가 조사는 2회에 걸쳐서 실시했다. 1차 조사에서는 문헌 및 사례 연구로 정리하여 전문가 인터뷰를 통해 도출된 인적 취약점 분류 유형과 항목별 측정 지표의 적절성을 리커트(Likert) 5점 척도와 개방형 의견을 통해 검증하고자 한다. 2차 조사에서는 1차 조사 결과를 바탕으로 타당도(CVR)가 기준치(0.37) 이하의 항목들은 제거하여 정리했다. 델파이 조사에 참여한 인력은 25명이며, Lawshe가 제안한 전문가 패널 수에 따른 CVR(Content Validity Ratio) 임계값을 참고하여 CVR은 0.37을 기준으로 분석했다. 구체적인 인구통계학적 특성은 Table 5와 같다.

Table 5. Demographic characteristics of Delphi Participation Specialists (N=25)

Division		Frequency (persons)	Percent (%)
Gender	Male	24	96.0
	Female	1	4.0
	Total	25	100
Age	20 ~ 29	2	8.0
	30 ~ 39	10	40.0
	40 ~ 49	4	16.0
	50 ~	9	36.0
	Total	25	100
Education	Bachelor's degree	8	32.0
	Master's degree	13	52.0
	Doctorate	4	16.0
	Total	25	100
Stakeholder	IT developer(engineer)	1	4.0
	IT Solution Consultant	1	4.0
	Police Officer (Criminal Psychology)	1	4.0
	Professor	1	4.0
	Security Officer	6	24.0
	Security Manager	3	12.0
	Security Consultant/SI	10	40.0
	Operational Staff	2	8.0
	Tortal	25	100

4.3 1차 델파이 설문조사 결과

1차 문항은 Likert 척도 5점으로 개방형 문항으로 구성했으며 2023년 5월 12일부터 5월 19일까지 8일간 진행되었다. 인적 취약점 분류 체계별 각각의 항목별 내용타당도 및 선정 결과는 다음과 같다.

4.3.1 우발성(Accidentality)에 대한 내용타당도 분석 및 선정 결과(CVR=0.37)

우발성 영역의 구성요소로 총 4가지 구성요소에서 인적 보안 관련 측정 지표 항목에 대한 타당도 및 선정 결과는 Table 6과 같다. CVR 기준값 0.37보다 낮게 나타난 항목은 제거했다. 응답자들은 SNS 가입 현황 분석, 업무 태도 분석, 성향 분석을 위한 업무 평가 조회, 과거 행동 분석을 위한 경력 분석 등의 측정 지표 항목들은 개인 프라이버시 침해의 소지를 심각하게 우려했다.

Table 6. Content Feasibility Analysis and Selection Status for Accidentality Components (CVR=0.37)

Division	measurement indicator items	N	M	SD*	CVR	Result
Personal Propensity	Transparency of Authority and Roles	25	4.52	0.700	0.92	○
	Transparency in the Use of Authority	25	4.48	0.755	0.84	○
	Designation and Management of Key Personnel Roles	25	4.40	0.938	0.76	○
	Separation of Duties for the Prevention of Potential Harms like Authority Misuse	25	4.48	0.900	0.84	○
Personal Authority	Document Management for Personal Information-related Matters	25	4.44	0.898	0.84	○
	Online Personal Information Management	25	4.04	0.958	0.68	○
	Analysis of Online Public Information	25	4.04	0.916	0.60	○
	Analysis of Social Media Membership	25	3.44	1.023	0.20	-

	Status					
Personal Carelessness	Recognition of Attack Patterns in Social Engineering Techniques	25	4.48	0.574	0.92	○
	Background Research on the Source of Online Communication	25	4.56	0.804	0.76	○
	Analysis of Work Attitudes	25	3.72	1.001	0.28	-
	Work Performance Evaluation for Personality Analysis	25	3.40	1.058	0.20	-
Personal Security Level	Regular Education and Training	25	4.92	0.271	1.00	○
	Regular System Updates	25	4.72	0.531	0.92	○
	Security Pledge for Awareness of Compliance Guidelines	25	4.64	0.557	0.92	○
	Career Analysis for Past Behavior Assessment	25	3.76	1.031	0.36	-
king	Background Research on the Source of Online Communication	25	4.12	0.652	0.68	○
	Continuous Propagation of Incident Cases	25	4.88	0.325	1.00	○
Social conflict	Identification of Internal Conflict Factors	25	3.88	0.993	0.36	-
	Analysis of the Importance of Assigned Tasks	25	4.40	0.693	0.76	○
	Analysis of Work Attitudes	25	3.80	1.131	0.36	-
Illegal Solicitation	Identification of Financial Gain Necessity	25	4.44	0.804	0.76	○
	Identification of Job Transition Possibility	25	4.16	0.880	0.52	○
	Identification of Internal Conflict Factors	25	3.84	0.880	0.20	-

*N(number of experts), M(Mean), SD(Standard Deviation), CVR(Content Validity Ratio)

4.3.2 관계성(Relationship)에 대한 내용타당도 분석 및 선정 결과(CVR=0.37)

관계성 영역의 구성요소로 총 4가지 요소에서 인적보안 관련 측정 지표 항목에 대한 타당도 및 선정 결과는 Table 7과 같다. 마찬가지로 CVR 기준값 0.37 보다 낮게 측정된 항목들은 제거했다. 제거된 항목 중 내부 갈등 요소 식별, 업무 태도 분석 등은 Table 6의 위험성 지표와 보안성 지표의 내용과 중복된다고 판단했고 측정 방법에 대해서도 실효성에 대한 의문을 제기했다.

Table 7. Content Feasibility Analysis and Selection Status for Relationship Components (CVR=0.37)

Division	measurement indicator items	N	M	SD*	CVR	Result
Personal Connectivity	Utilization of Social Engineering Attack Techniques	25	4.36	0.843	0.84	○
	Analysis of Relationships within the Same Industry (Competition Analysis)	25	3.92	1.055	0.52	○
	Identification of Internal Conflict Factors	25	4.04	0.871	0.60	○
Social Networ	Regular Education and Training	25	4.80	0.490	0.92	○

4.3.3 잠재성(Potentiality)에 대한 내용타당도 분석 및 선정 결과(CVR=0.37)

잠재성 영역의 구성요소로 총 4가지 요소에서 인적보안 관련 측정지표 항목에 대한 타당도 및 선정 결과는 Table 8과 같다. 잠재성 영역의 측정 지표 항목들은 모두 CVR 기준값 0.37보다 높게 나타났으므로 제거 항목 없이 모두 채택됐다.

Table 8. Content Feasibility Analysis and Selection Status for Potentiality Components (CVR=0.37)

Division	measurement indicator items	N	M	SD*	CVR	Result
Organizational Culture	Transparency in Task Handling	25	4.48	0.574	0.92	○
	Transparency in Work Performance	25	4.28	0.960	0.60	○
	Transparency in Work Responsibilities	25	4.64	0.557	0.92	○
	Ensuring Transparency in Security Rule Compliance	25	4.64	0.625	0.84	○
Customary Practice	Transparency in Work Collaboration	25	4.40	0.693	0.76	○
	Ensuring Fairness in Work Performance Measurement	25	4.48	0.574	0.92	○
	Elimination of Conventional Work Habits	25	4.48	0.755	0.68	○

Security Compliance	Security Issue Analysis for Emerging Technologies	25	4.64	0.557	0.92	○
	Periodic Sharing of Security Incident Cases	25	4.72	0.601	0.84	○
Social influence	Transparency in Compliance Adherence Status	25	4.56	0.571	0.92	○
	Prevention of Compliance Evasion Strategies	25	4.56	0.637	0.84	○
	Implementation of Periodic Security Awareness Training	25	4.76	0.512	0.92	○
	Elimination of Coercive Security Directives	25	4.12	0.952	0.52	○
	Retirement and Job Transition Management	25	4.60	0.566	0.92	○
	Actions in the Event of Security Violations	25	4.76	0.427	1.00	○

*N(number of experts), M(Mean), SD(Standard Deviation), CVR(Content Validity Ratio)

4.3.4 심리학적(Psychological) 특성에 대한 내용타당도 분석 및 선정 결과(CVR=0.37)

심리학적 영역의 구성요소로 총 5가지 요소에서 인적 보안 관련 측정 지표 항목에 대한 타당도 및 선정 결과는 Table 9와 같다. 역시 CVR 기준값 보다 낮게 측정된 항목들은 모두 제거했다. 심리학적 영역의 측정 지표 항목들은 다소 많이 도출되었고 제거된 항목들은 대부분 측정의 실효성에 의문을 제기했거나 개인 프라이버시 침해 위험에 많은 의견이 있었다. 따라서 다른 영역에 비해서 다소 많은 항목이 제거되었다.

Table 9. Content Feasibility Analysis and Selection Status for Psychological Components (CVR=0.37)

Division	measurement indicator items	N	M	SD*	CVR	Result
Biological	Personality Analysis for Behavioral Profiling	25	3.56	1.061	0.12	-
	Analysis of Growth Process	25	3.40	1.020	0.04	-
	Tendency Analysis for Behavioral Profiling	25	3.60	1.058	0.20	-
	Identification of Nervous System Activities	25	3.28	1.078	0.04	-
	Hormone Levels	25	3.04	1.076	0.36	-
	Genes and Genetic Vulnerability	25	3.08	1.129	0.12	-
Cognitive	Analysis of Judgement Capability	25	3.96	1.076	0.52	○
	Work Collaboration Attitude	25	4.04	1.113	0.52	○
	Cognitive Ability Test	25	3.72	1.150	0.20	-
	Perceptual Ability Test	25	3.48	1.300	0.20	-
	Cognitive Development Assessment	25	3.60	1.020	0.28	-
	Cognitive Flexibility Assessment	25	3.80	1.131	0.44	○
Behavioral	Job Competency Analysis	25	3.76	1.209	0.36	-
	Analysis of Work Activities	25	3.88	1.177	0.36	-
	Behavior Observation for Behavior Pattern Analysis	25	3.84	1.084	0.52	○
	Behavioral Recording for Behavior Pattern Analysis	25	3.80	0.938	0.60	○
	Self-Reporting Method for Behavior Pattern Analysis	25	3.64	1.091	0.36	-
	Behavior Assessment Scale	25	3.84	1.046	0.44	○
Psychoanalytic	Work Performance Analysis	25	3.84	1.189	0.52	○
	Incident History Analysis	25	4.00	1.131	0.44	○
	Projection Test	25	3.80	1.131	0.36	-
	Free Association for Unconscious Analysis	25	3.44	1.134	0.04	-
	Dream Interpretation for Unconscious Analysis	25	3.48	1.100	0.04	-
	Self-Analysis through Inner Exploration	25	3.40	0.938	0.12	-
Humanistic	Subjective Experience-based Personality Analysis	25	3.68	1.121	0.20	-
	Identification of Internal Conflict Factors	25	3.84	1.120	0.28	-
	Identity-based Self-Concept	25	3.68	1.009	0.28	-
	Values Assessment	25	4.08	1.055	0.52	○
	Measurement of Autonomy	25	3.92	1.017	0.44	○
	Life Satisfaction Scale	25	3.88	1.107	0.36	-

*N(number of experts), M(Mean), SD(Standard Deviation), CVR(Content Validity Ratio)

심리학적 영역의 측정 지표들은 관련 문헌과 FGI를 통해 선정했으며 보안성과 접목하여 전문가들의 의견과 연구자의 경험치에 의존해서 도출해야만 했다

[19][20][21][22][23][24].

4.3.5 윤리성(Ethicality)에 대한 내용타당도 분석 및 선정 결과(CVR=0.37)

윤리성 영역의 구성요소로 총 4가지 요소에서 인적 보안 관련 측정 지표 항목에 대한 타당도 및 선정 결과는 Table 10과 같다. 윤리성과 관련된 측정 지표 항목들은 응답자들의 높은 공감대가 형성됐고, 제거 항목 없이 모두 채택되었다.

Table 10. Content Feasibility Analysis and Selection Status for Ethicality Components (CVR=0.37)

Division	measurement indicator items	N	M	SD*	CVR	Result
Moral Disengagement	Ethical Education	25	4.64	0.557	0.92	○
	Enhancing Ethical Judgment	25	4.60	0.632	0.84	○
	Regular Ethical Education	25	4.76	0.512	0.92	○
Intentional Crime	Cognitive Deviation Analysis	25	4.04	0.916	0.60	○
	Emotional Deviation Analysis	25	4.08	0.935	0.60	○
	Behavioral Deviation Analysis	25	4.16	0.967	0.60	○
Ill-gotten Profit	Transparency in Achieving Economic Gains	25	4.52	0.806	0.76	○
	Transparency in Achieving Social Benefits	25	4.12	1.032	0.60	○
	Transparency in Achieving Emotional Benefits	25	4.16	1.046	0.60	○
Cyber ethics	Personal Information Protection	25	4.88	0.325	1.00	○
	Online Communication		4.48	0.854	0.92	○
	Respect for Copyright	25	4.72	0.531	0.92	○
	Prevention of Cybercrime	25	4.68	0.676	0.92	○

*N(number of experts), M(Mean), SD(Standard Deviation), CVR(Content Validity Ratio)

윤리성 영역의 측정 지표들은 관련 문헌과 FGI를 통해 선정했으며 보안성과 접목하여 전문가들의 의견과 연구자의 경험치에 의존해서 도출해야만 했다[25][26].

4.4 2차 델파이 설문조사 결과

2차 델파이 설문 문항 역시 Likert 척도 5점으로 개방형 문항으로 구성했으며 2023년 6월 7일부터 6월 16일까지 10일간 진행되었다. 인적 취약점 분류 체계별 각각의 항목별 내용타당도 및 신뢰도를 기반으로 최종 선정 결과는 다음과 같다.

4.4.1 우발성(Accidentality)에 대한 내용타당도 및 신뢰도 분석(N=25)

우발성 영역의 구성요소로 총 4가지 요소에서 인적 보안 관련 측정 지표 항목에 대한 타당도와 신뢰도 그리고 최종 선정 결과는 Table 11과 같다. CVR은 모두 기준값 보다 높게 측정됐으며 신뢰도 값은 0.616으로 나타났다. 따라서 제거 항목 없이 최종 채택 항목이 확정됐다.

Table 11. Content validity and reliability analysis of Accidentality Components(N=25)

Division	measurement indicator items	M	SD*	stability	CVR	α	Result
Personal Propensity	Transparency of Authority and Roles	4.72	0.449	0.10	1.00	0.616	○
	Transparency in the Use of Authority	4.60	0.566	0.12	0.92		○
	Designation and Management of Key Personnel Roles	4.76	0.427	0.09	1.00		○
	Separation of Duties for the Prevention of Potential Harms like Authority Misuse	4.80	0.400	0.08	1.00		○
Personal Authority	Document Management for Personal Information-related Matters	4.48	0.574	0.13	0.92		○
	Online Personal Information Management	4.32	0.786	0.18	0.76		○
	Analysis of Online Public Information	4.16	0.731	0.18	0.76		○
Personal Carelessness	Recognition of Attack Patterns in Social Engineering Techniques	4.44	0.637	0.14	0.84		○
	Background Research on the Source of Online Communication	4.72	0.449	0.10	1.00		○
Personal	Regular Education and	4.80	0.400	0.08	1.00		○

Security Level	Training						
	Regular System Updates	4.84	0.367	0.08	1.00		○
	Security Pledge for Awareness of Compliance Guidelines	4.68	0.466	0.10	1.00		○

*M(Mean), SD(Standard Deviation),CVR(Content Validity Ratio), α(Cronbach α, Reliability Analysis)

4.4.2 관계성(Relationship)에 대한 내용타당도 및 신뢰도 분석(N=25)

관계성 영역의 구성요소로 총 4가지 요소에서 인적 보안 관련 측정 지표 항목에 대한 타당도와 신뢰도 그리고 최종 선정 결과는 Table 12와 같다. CVR은 모두 기준값 보다 높게 측정됐으며 신뢰도 값은 0.709로 높게 나타났다. 따라서 제거 항목 없이 최종 채택 항목이 확정됐다.

Table 12. Content validity and reliability analysis of Relationship Components(N=25)

Division	measurement indicator items	M	SD*	stability	CVR	α	Result
Personal Connectivity	Utilization of Social Engineering Attack Techniques	4.36	0.975	0.22	0.84	0.709	○
	Analysis of Relationships within the Same Industry (Competition Analysis)	4.00	0.938	0.23	0.52		○
	Identification of Internal Conflict Factors	4.12	0.909	0.22	0.68		○
Social Networking	Regular Education and Training	4.76	0.427	0.09	1.00		○
	Background Research on the Source of Online Communication	4.44	0.637	0.14	0.84		○
	Continuous Propagation of Incident Cases	4.72	0.531	0.11	0.92		○
Social conflict	Analysis of the Importance of Assigned Tasks	4.68	0.546	0.12	0.92		○
Illegal Solicitation	Identification of Financial Gain Necessity	4.40	0.849	0.19	0.68		○
	Identification of Job Transition Possibility	4.32	0.835	0.19	0.68		○

*M(Mean), SD(Standard Deviation),CVR(Content Validity Ratio), α(Cronbach α, Reliability Analysis)

4.4.3 잠재성(Potentiality)에 대한 내용타당도 및 신뢰도 분석(N=25)

잠재성 영역의 구성요소로 총 4가지 요소에서 인적 보안 관련 측정 지표 항목에 대한 타당도와 신뢰도 그리고 최종 선정 결과는 Table 13과 같다. CVR은 모두 기준값 보다 높게 측정됐으며 신뢰도 값은 0.843으로 매우 높게 나타났다. 따라서 제거 항목 없이 최종 채택 항목이 확정됐다.

Table 13. Content validity and reliability analysis of Potentiality Components(N=25)

Division	measurement indicator items	M	SD*	stability	CVR	α	Result
Organizational Culture	Transparency in Task Handling	4.68	0.546	0.12	0.92	0.843	○
	Transparency in Work Performance	4.36	0.794	0.18	0.76		○
	Transparency in Work Responsibilities	4.68	0.466	0.10	1.00		○
	Ensuring Transparency in Security Rule Compliance	4.76	0.427	0.09	1.00		○
Customary Practice	Transparency in Work Collaboration	4.44	0.496	0.11	1.00		○
	Ensuring Fairness in Work Performance Measurement	4.56	0.571	0.13	0.92		○
	Elimination of Conventional Work Habits	4.72	0.601	0.13	0.84		○
Security Compliance	Security Issue Analysis for Emerging Technologies	4.72	0.449	0.10	1.00		○
	Periodic Sharing of Security Incident Cases	4.76	0.427	0.09	1.00		○
Social influence	Transparency in Compliance Adherence Status	4.56	0.637	0.14	0.84		○
	Prevention of Compliance Evasion Strategies	4.36	0.625	0.14	0.84		○
	Implementation of Periodic Security	4.84	0.367	0.08	1.00		○

	Awareness Training						
	Elimination of Coercive Security Directives	4.00	0.894	0.22	0.52		○
	Retirement and Job Transition Management	4.68	0.466	0.10	1.00		○
	Actions in the Event of Security Violations	4.76	0.427	0.09	1.00		○

*M(Mean), SD(Standard Deviation),CVR(Content Validity Ratio), α(Cronbach α, Reliability Analysis)

4.4.4 심리학적(Psychological) 특성에 대한 내용타당도 및 신뢰도 분석(N=25)

심리학적 영역의 구성요소로 총 5가지 요소에서 인적 보안 관련 측정 지표 항목에 대한 타당도와 신뢰도 그리고 최종 선정 결과는 Table 14와 같다. 성장 과정 분석을 제외하고 CVR은 모두 기준값 보다 높게 측정됐으며 신뢰도 값은 0.933으로 매우 높게 측정되었다. 따라서 성장 과정 분석을 제거하고 최종 채택 항목이 확정됐다.

Table 14. Content validity and reliability analysis of Psychological Components(N=25)

Division	measurement indicator items	M	SD*	stability	CVR	α	Result
Biological	Analysis of Growth Process	3.52	0.854	0.24	0.12		-
Cognitive	Analysis of Judgement Capability	4.12	0.652	0.16	0.68	0.933	○
	Work Collaboration Attitude	4.36	0.686	0.16	0.76		○
	Cognitive Flexibility Assessment	4.24	0.709	0.17	0.68		○
Behavioral	Behavior Observation for Behavior Pattern Analysis	4.20	0.632	0.15	0.76		○
	Behavioral Recording for Behavior Pattern Analysis	4.08	0.627	0.15	0.68		○
	Behavior Assessment Scale	4.12	0.765	0.19	0.68		○
Psychoanalytic	Work Performance Analysis	4.16	0.731	0.18	0.76		○
	Incident History Analysis	4.24	0.650	0.15	0.76		○
Humanistic	Values Assessment	4.24	0.763	0.18	0.60		○
	Measurement of Autonomy	4.32	0.676	0.16	0.76		○

*M(Mean), SD(Standard Deviation),CVR(Content Validity Ratio), α(Cronbach α, Reliability Analysis)

4.4.5 윤리성(Ethicality)에 대한 내용타당도 및 신뢰도 분석(N=25)

윤리성 영역의 구성요소로 총 4가지 요소에서 인적 보안 관련 측정지표 항목에 대한 타당도와 신뢰도 그리고 최종 선정 결과는 Table 15와 같다. 1차 조사와 마찬가지로 CVR은 모두 기준값 보다 높게 측정됐으며 신뢰도 값은 0.856으로 매우 높게 나타났다. 따라서 제거 항목 없이 최종 채택 항목이 확정됐다.

Table 15. Content validity and reliability analysis of Ethicality Components(N=25)

Division	measurement indicator items	M	SD*	stability	CVR	α	Result
Moral Disengagement	Ethical Education	4.72	0.531	0.11	0.92	0.856	○
	Enhancing Ethical Judgment	4.64	0.625	0.13	0.84		○
	Regular Ethical Education	4.76	0.512	0.11	0.92		○
Intentional Crime	Cognitive Deviation Analysis	4.16	0.612	0.15	0.76		○
	Emotional Deviation Analysis	4.16	0.612	0.15	0.76		○
	Behavioral Deviation Analysis	4.24	0.650	0.15	0.76		○
Ill-gotten Profit	Transparency in Achieving Economic Gains	4.40	0.693	0.16	0.76		○
	Transparency in Achieving Social Benefits	4.24	0.709	0.17	0.68		○
	Transparency in Achieving Emotional Benefits	4.16	0.880	0.21	0.52		○
Cyber ethics	Personal Information Protection	4.72	0.665	0.14	0.92		○
	Online	4.48	0.700	0.16	0.92		○

	Communication						
	Respect for Copyright	4.76	0.585	0.12	0.84		○
	Prevention of Cybercrime	4.76	0.427	0.09	1.00		○

*M(Mean), SD(Standard Deviation),CVR(Content Validity Ratio), α(Cronbach α, Reliability Analysis)

2차 조사에서는 개인정보보호법 침해 우려, 민감하고 지나친 프라이버시 이슈, 측정할 수 없는 추상적인 지표들 특히, 심리학적 영역에 다수 존재했던 내용들이 삭제되고 조사되어서 항목 대부분이 CRV 기준치인 0.37 이상, 신뢰도 0.6 이상으로 조사됐으며, 결론적으로 총 59개의 유의미한 인적 보안 평가지표를 도출했다.

4.5 인적 취약점에 대한 측정지표 제안

1, 2차 델파이 조사 결과를 분석하여 최종 Table 16과 같이 인적 취약점 분류체계 기반의 총 59개 유의미한 인적보안 측정지표를 정리할 수 있다.

Table 16. Human security measurement index based on human vulnerability classification system

Division	Component	Measurement Items
Accidentality	Personal Propensity (4)	Transparency of Authority and Roles
		Transparency in the Use of Authority
		Designation and Management of Key Personnel Roles
		Separation of Duties for the Prevention of Potential Harms like Authority Misuse
	Personal Authority (3)	Document Management for Personal Information-related Matters
		Online Personal Information Management
		Analysis of Online Public Information
	Personal Carelessness (2)	Recognition of Attack Patterns in Social Engineering Techniques
		Background Research on the Source of Online Communication
	Personal Security Level (3)	Regular Education and Training
		Regular System Updates
		Security Pledge for Awareness of Compliance Guidelines
Relationship	Personal Connectivity (3)	Utilization of Social Engineering Attack Techniques
		Analysis of Relationships within the Same Industry (Competition Analysis)
		Identification of Internal Conflict Factors
	Social Networking (3)	Regular Education and Training
		Background Research on the Source of Online Communication
		Continuous Propagation of Incident Cases
	Social conflict (1)	Analysis of the Importance of Assigned Tasks
	Illegal Solicitation (2)	Identification of Financial Gain Necessity
		Identification of Job Transition Possibility
Potentiality	Organizational Culture (4)	Transparency in Task Handling
		Transparency in Work Performance
		Transparency in Work Responsibilities
		Ensuring Transparency in Security Rule Compliance
	Customary Practice (3)	Transparency in Work Collaboration
		Ensuring Fairness in Work Performance Measurement
		Elimination of Conventional Work Habits
	Security Compliance (2)	Security Issue Analysis for Emerging Technologies
		Periodic Sharing of Security Incident Cases
	Social influence (6)	Transparency in Compliance Adherence Status
		Prevention of Compliance Evasion Strategies
		Implementation of Periodic Security Awareness Training
		Elimination of Coercive Security Directives
		Retirement and Job Transition Management
		Actions in the Event of Security Violations
Psychological	Cognitive (3)	Analysis of Judgement Capability
		Work Collaboration Attitude
		Cognitive Flexibility Assessment
	Behavioral (3)	Behavior Observation for Behavior Pattern Analysis
		Behavioral Recording for Behavior Pattern Analysis
		Behavior Assessment Scale
	Psychoanalytic (2)	Work Performance Analysis
		Incident History Analysis
	Humanistic (2)	Values Assessment
		Measurement of Autonomy
Ethicality	Moral Disengagement (3)	Ethical Education
		Enhancing Ethical Judgment
		Regular Ethical Education
	Intentional Crime (3)	Cognitive Deviation Analysis
		Emotional Deviation Analysis
		Behavioral Deviation Analysis
	Ill-gotten Profit (3)	Transparency in Achieving Economic Gains
		Transparency in Achieving Social Benefits

		Transparency in Achieving Emotional Benefits
	Cyber ethics (4)	Personal Information Protection
		Online Communication
		Respect for Copyright
		Prevention of Cybercrime

5. 결론

지금까지 인적 취약점 분류체계 기반의 인적보안 측정지표 도출 과정과 델파이 조사를 통한 결론을 정리했다. 인적 취약점 분류체계를 기반으로 각각의 구성 요소별 측정 지표를 도출한 목적은 크게 네 가지로 요약할 수 있다. 첫 번째 정형화된 보안 컴플라이언스가 수년간 정착되고 반복적으로 시행됨에 따라 보안 담당자들이 효율적인 업무 진행을 위해 이를 우회하거나 회피하는 요령이 생겼고 이로 인한 보안의 리스크(Risk)가 매우 심각해졌다. 따라서 사람에 초점을 맞춘 인적 취약점 분류체계를 참고하고 이를 토대로 구체적인 상황별 측정 지표를 제시함으로써 이를 인적 보안 체크리스트로 활용하여 보안 컨설팅의 한 분야로 자리매김할 수 있다. 두 번째는 보안 솔루션으로 복잡한 IT 환경에서 발생하는 모든 공격을 방어하기 어렵다는 것이다. 사이버상의 위협을 방어하는 것도 매우 중요하지만, 상당한 비중이 사람으로부터 유발되고 있다. 따라서 인적 취약점 분류체계는 사람 관점에서 유발될 수 있는 거의 모든 취약한 행위를 광범위하고 포괄적으로 담고 있어서 내부 조직 관리에 있어서 직무를 분석하고 배치하는 데 활용될 수 있다. 세 번째는 기존 사이버상의 외부 위협과 이에 따른 대응에 초점을 맞춘 보안 인식 교육과 업무 지침에서 사람 중심의 보안 교육으로 전환하는 계기가 될 수 있다는 점에서 의미가 매우 크다고 할 수 있다. 즉, 기존의 보안 인식 교육은 일률적인 내용으로 전 부서 전사원을 대상으로 진행하는 것이 일반적이었으나, 인적 취약점 분류체계에 대한 이해와 이를 기반으로 한 인적보안 측정지표를 활용하면 부서별, 인원별 맞춤형 보안 인식 교육을 개발하고 적용함으로써 사람으로 인해 유발되는 다양한 유형의 위협을 사전에 차단하고 관리할 수 있다. 네 번째는 인간 중심 보안(PCS)의 전략적 가치와 연계한 구성원들의 적극적인 참여와 협업을 통해 자발적 보안 활동을 도모하고 전사적으로 긍정적인 보안 문화를 구현하는 데 매우 긍정적인 모델이 될 수 있다. IT의 출현은 새로운 보안 위협을 초래하며 이를 해결하기 위해서는 기술적인 보안대책과 보안 관리 프로세스가 중요하다는 점은 당연한 사실이다. 인간, 프로세스, 기술(PPT: People, Process, Technology)이라는 보안 관리 체계 3대 요소 중 보안 프로세스와 기술에 대한 괄목할 만한 발전과 구현이 있었다. 그럼에도 불구하고 여전히 보안 사고는 발생하고 있다. 이는 임직원들의 보안 활동에 대한 이해가 부족했다는 사실을 반증한다. 더불어 임직원들이야말로 보안의 주체요, 살아 있는 방화벽이 될 수 있다는 점을 충분히 인지하지 못했다[27][28][29].

통제와 기술 중심의 보안 전략은 창의와 자율이 요구되는 디지털 시대에 적절하지 않으며 실제 사이버 보안 사고의 50% 이상이 임직원의 잘못으로 발생한다. 인간 중심 보안(PCS)이 거론되는 이유가 바로 여기에 있다. 인간 중심 보안은 지속 가능한 보안 문화를 구축하기 위한 전략으로 조직을 자율성과 책임성이 장려되는 신뢰 공간으로 구축해 보안 문제에 대응하는 접근법이다. 인간 중심 보안이 실현되기 위해서는 정교한 보안 문화 변화 관리 프로그램과 모니터링 프로그램이 전제돼야 한다. 보호 동기이론(PMT), 경쟁 가치 모델, 고신뢰 조직 등 조직 이론과 모델을 보안에 적용해 보안 행위와 보안 문화를 진단하고 전환할 수 있다[25].

'인간을 위한, 인간에 의한 보안' 에 대한 논의는 2010년대 초반 이후부터 시작됐다. 그 이전에도 보안에 있어 인간이 취약점이 될 수 있다는 인식이 존재했으며 조직 구성원을 위한 보안 교육 및 훈련 프로그램 개발과 운영 이슈, 임직원의 보안 준수성 등 사람과 관련된 대책들이 연구 개발됐지만 단편적인 수준에 그쳤다. 2012년 시장 조사 기관 가트너는 기존 질서를 뒤집는 연구를 소개하는 매버릭(Maverick) 리서치에서 보안 위험을 줄이기 위해서 오히려 보안 통제를 줄여야 한다는 극단적인 주장을 피력하면서 '인간 중심 보안' 을 제시했다. 그 이후 인간의 보안 행위에 대한 행동과학, 심리학 등 연구들이 이어졌고 실제 정부나 기업 정책에도 인간 중심 보안 개념이 적용되기 시작했다[28].

'인간 중심 보안이 예방적, 기술적 보안대책을 무시한다' 라고 오해할 수도 있다. 그러나 인간 중심 보안에서도 예방적 대책과 기술은 필요하다. 단, 과거와 달리 올바른 행위를 유도할 수 있는 가드레일 역할 또는 안전망(Safety Net) 역할을 해야 한다. 즉, 보안기술 사용에 대한 인식을 바꾸고 자율성을 보장하면서 보안대책의 투명성을 제고하는 방향으로 기술이 적용돼야 한다. DRM(Digital Right Management, 디지털 콘

텐츠 저작권 관리 기술)과 같이 선택적으로 비밀문서를 보호하거나 UBA와 같이 사용자 행동을 예측할 수 있는 애널리틱스 기술, 이벤트 기반의 IAM(Identity and Access Management, 접근권한 관리) 기술 등을 적극적으로 활용해야 한다. 그와 동시에 모범 사례를 제시하고 가이드해 줄 수 있는 기술을 적용해야 한다[29][30][31][32].

인적 취약점 분류체계 기반의 인적보안 측정지표는 지금까지 어떤 연구에서도 제시하지 못한 새로운 제안이다. 따라서, 그 근거는 FGI와 델파이 조사를 통해서 입증할 수밖에 없었다. 본 연구를 토대로 인적 보안에 대한 연구 개발이 더욱 활발히 진행되기를 기대한다. 특히, 최근에 금융권을 비롯한 자율 보안 체계가 확산할 것으로 전망되고 있어서, 더 이상 단순히 기술적인 측면, 컴플라이언스에 의존한 보안은 이제 사고를 예방하기 어려운 상황이 됐다. 기술적, 관리적, 법 제도적 측면의 보안은 기본적으로 갖추어야 할 조건 들이고 보안 강화를 위해선 다른 시도가 진행되어야 한다. 인적 보안이 바로 이러한 부분을 메워줄 충분한 동기부여가 될 것으로 기대한다[33][34].

참고문헌

[1] Hyeon-Dae Rha, Hyun-Soo Chung. (2016). A Theoretical Comparative Study of Human Resource Security Based on Korean and Int'l Information Security Management Systems. *Journal of Convergence for Information Technology, 6*(3), 13-19. DOI: http://dx.doi.org/10.22156/CS4SMB.2016.6.3.013

[2] Gim-Gisam. (2019). A Study on the Development of Information Security Risk Appetite Indicators. *The Graduate School of Chung-Ang University.* Major in Industrial Convergence Security. 1-2.

[3] Jeong Hye-in and Kim Seong-jun(2018). 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, 145-163.

[4] Kunwoo Kim, Jungduk Kim(2017), A Study on Research Trends Analysis about Human Aspect of Information Security. *Dept. of Security Convergence, Graduate School of Chung-Ang University*, 332 - 335

[5] I. H. Cha(2009). An Empirical Research on Developing Personnel Security Management Indicators in Information Security. *Master Thesis, Kwangwoon University*, 19.

[6] Jungjun Park, Seongjin Ahn. (2023). A Study on the Human Vulnerability Classification System for People-Centric Security. *Journal of The Korea Institute of Information Security and Cryptology.* 33(3). 561-575. DOI:10.13089/JKIISC.2023.33.3.561

[7] KANG, YOUNCHUL(2021).Development of Business Oriented Information Security Index(BOISI). *The Graduate School of Korea University.* 1-5.

[8] Ma, Q., Schmidt, M. B., and Pearson, J. M. (2009). An Integrated Framework for Information Security Management. *Review of Business* (30:1), 58-69.

[9] S. Y. Kim(2013). A Study of Human Security Control Model Utilizing the Information Security Management System. *Master Thesis, Kangwon University*, 78-89.

[10] Cha, I.-H., & Kim, J.-D. (2009). An Empirical Research on Human Factor Management Indicators for Information Security. Journal of the Korea Institute of Information Security & Cryptology, 19(6), 153-160. https://doi.org/10.13089/JKIISC.2009.19.6.153

[11] Suh Joon Bae, Hee S. Shim. (2017). A study on the occupational fraud symptoms and detection methods for managing human element vulnerability in financial industry security. *Korea Security Science Association*,(53),35-60. DOI : https://doi.org/10.36623/kssa.2017.53.2

[12] JS Lee(2020). Delphi method. *Educational Science Publishing Company,* 138.

[13] Kim, Sanghyun, Young-Mi Song. (2011). An Empirical Study on Motivational Factors Influencing Information Security Policy Compliance and Security Behavior of End-Users(Employees) in Organizations. *e-biz*, 12(3), 95-115.

[14] SH Lee, MY Jung, EY Yoo. (2021). Developing Social Play Evaluation Items for Preschool Children: A Delphi Study. *Therapeutic Science for Rehabilitation*, Vol.10. No.3. 97-110. https://doi.org/10.22683/tsnr.2021.10.3.097

[15] CH Lee, SM Hwang, SY Park, SE Chae, JR Kim. (2020). Development of Guidelines for Setting Up Sensory Integration Rooms in Korea Using the Delphi Method. *The Journal of Korean Academy of Sensory Integration,* Vol.18, No.2, 1-14.

[16] Song, H., & Ahn, S. (2023). A study on the measurement indicators for risk prevention of AI robots.

Journal of Internet Computing and Services, 24(3), 27-41. https://doi.org/10.7472/JKSII.2023.24.3.27

[17] So, S., & Ahn, S. (2022). A Study on the Artificial Intelligence Ethics Measurement indicators for the Protection of Personal Rights and Property Based on the Principles of Artificial Intelligence Ethics. *Journal of Internet Computing and Services*, 23(3), 111-123. https://doi.org/10.7472/JKSII.2022.23.3.111

[18] Suh, J.-B., & Shim, H.-S. (2017). A study on the occupational fraud symptoms and detection methods for managing human element vulnerability in financial industry security. *Korean Security Science Review. Korean Security Science Association.* https://doi.org/10.36623/kssa.2019.53.2

[19] Baek, Seung Hye Hyun, Myung Ho. (2008). Hostility, Anger Experience and Anger Expression in Overt and Covert Narcissists. *Korean Journal of Clinical Psychology*, 27(4), 1001-1017.

[20] Lee Hee Kyung, Lee, Dong-Gwi. (2007). Human Understanding and Change through the Positive Psychological Perspective. *Institute of Anthropology*, 13, 16-43.

[21] Kyungok Sim, Chun Woo Young. (2014). Psychological Significance of Finger Length Ratio: 2D:4D as a Marker of Prenatal Testosterone. *Kor. J. Psychol.: Gen.* 33(4), 787-814.

[22] Won Ho Taek,Lee, Min Kyou. (1990). THE RESEARCH DIRECTIONS IN PSYCHOLOGICAL APPROACHES TO CRIMINAL BEHAVIORS. *Korean criminological review* v.1 no.1 , 63 - 91.

[23] Chon Soo Jin. (2010). The Effect of Leader Trust on Job Attitude of Secretaries. *Journal of Secretarial Studies*, vol.19, no.2, 29-48.

[24] Lee Jong Hun, Tae Young Choi, Kim Ji-Hyun, Shin Im-Hee, JUNGMIN WOO. (2012). Study for Relations between Smart-Phone Addiction Level and Korea Youth Self Report. *Korea Society of Biological Therapies in Psychiarty*, 18(2), 223-230.

[25] Ae Kyung Kim. (2010). A study on Unonscious realms on Chagall's works -based on C. G. Jung's Analytic Psychology-. *Journal of Communication Design*. 32, 100-110.

[26] Chu Beong Wan. (2020). The implications of moral disengagement to moral education. *Journal of Moral & Ethics Education*, 67, 75-98.

[27] Jungduk Kim. (2022). In the end, security should change the culture before people's problem strategy. *DBR*. https://dbr.donga.com/article/view/1206/article_no/10429/ac/magazine

[28] Gartner.(2012), Maverick Research:kill Off Security Controls to Reduce Risk.

[29] Gartner.(2013), Consider a People-Centric Security Stragegy.

[30] Gatner. (2013). People-Centric Security Challenges Require Careful Planning.

[31] Gartner. (2019). Fight Unsecure Employee Behaviors by Fixing Your Risk Culture.

[32] Lance Hayden. (2016). People-Centric Security:Transforming Your Enterprise Security Culture, *McGraw-Hill.*

[33] NCSC(2023). People-centred security ‘; https://www.ncsc.gov.uk/section/advice-guidance/all-topics?allTopics=true&topics=people-centred%20security&sort=date%2Bdesc

[34] ENISA. (2018). Cybersecurity Culture Guidelines:Behavioural Aspects of Cybersecurity.

박 정 준

1997년 우석대학교 수학과(이학사)
2015년 성균관대학교 IT컨설팅학 (공학석사)
2017년 ~ 현재 성균관대학교 대학원 컴퓨터교육과(박사과정수료)

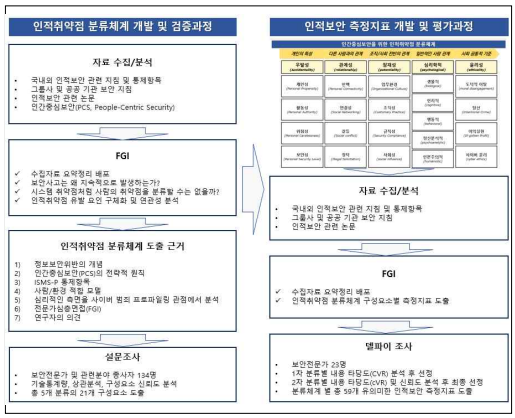
관심분야: 정보보안, 인적보안, 인간중심보안(PCS), 컴퓨터교육
E-Mail: jjpark0822@naver.com

안 성 진

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
E-Mail: sjahn@skku.edu

부 록



[그림 1] 연구개발과정 및 평가과정

<표 1> 인적보안 통제항목 현황과 본연구의 차별성

구분	ISO27001	ISMS-P	NIST 800-53	본연구 관점
주요 직무자 지정 및 관리	○			사람 자체에 초점을 맞추어 크게 다섯 가지(우발성, 관계성, 잠재성, 심리학적, 윤리성) 영역으로 분류하고 이에 따른 측정지표를 도출함.
퇴직 및 직무변경 관리	○			
접근권한	○			
직원 고용		○		
경영진 책임		○		
정보보호 교육	○	○		
징계	○	○		
조직			○	
외부자 관리			○	
인적보안			○	

<표 3> FGI 결과에 따른 인적보안 측정지표 제안(86)

인적 취약점 대분류	인적 취약점 구성요소	구성 요소별 측정지표
우발성	개인성	• 권한 및 역할의 투명성 • 권한 사용에 대한 투명성 • 주요 직무자 지정 및 관리 • 권한 오남용
	활동성	• 개인정보와 관련한 문서관리 • 온라인상의 개인정보 관리 • 온라인 공개 정보 분석 • SNS 가입 현황 분석
	위험성	• 사회공학적 공격 형태인지 • 온라인 소통 출처 배경 조사 • 업무태도 분석 • 성향 분석을 위한 업무 평가조회
	보안성	• 주기적인 교육 훈련 • 주기적인 시스템 업데이트 • 준수사항 인지를 위한 보안 서약서
		• 과거행동 분석을 위한 경력 분석
관계성	인맥	• 사회공학적 공격 기법의 활용 • 동종(경쟁) 업계 관계 분석 • 내부 갈등 요소 식별
	연결성	• 주기적인 교육 훈련 • 온라인 소통 출처 배경 조사 • 지속적인 사고사례 전파
	갈등	• 내부 갈등 요소 식별 • 담당 업무의 중요도 분석 • 평상시 업무태도 분석
	청탁	• 금전적 이득의 필요성 • 이직 가능성 식별 • 내부 갈등 요소 식별
잠재성	업무환경	• 업무 처리의 투명성 • 업무 성과의 투명성 • 업무 책임의 투명성 • 보안 규칙 준수의 투명성
	조직성	• 업무 협업의 투명성 • 업무 성과 측정의 공정성 확보 • 관행적 업무 습관의 제거
	규칙성	• 신기술에 대한 보안 이슈 분석 • 주기적 보안 사고사례 공유
	사회성	• 컴플라이언스 이행 여부 투명성 • 컴플라이언스 회피 방안 예방 • 주기적 보안 인식 교육의 시행 • 강압적인 보안지침 제거 • 퇴직 및 직무 변경 관리 • 보안 위반 시 조치
심리학적	생물적	• 행동 분석을 위한 성격 분석 • 성장 과정 분석 • 행동 분석을 위한 성향 분석 • 신경 체계 활동 식별 • 호르몬 수준 • 유전자적 취약성 식별
	인지적	• 판단력 분석 • 업무 협업 태도 • 인지 능력 테스트 • 지각 능력 테스트 • 인지 발달 검사 • 인지적 유연성 평가
	행동적	• 업무 역량 분석 • 업무 활동 분석 • 행동 패턴 분석을 위한 행동 관찰 • 행동 패턴 분석을 위한 행동 기록 • 행동 패턴 분석을 위한 자기보고법 • 행동 평가 척도
	정신분석적	• 업무 성과 분석 • 사고 이력 분석 • 프로젝션 테스트 • 무의식 분석을 위한 자유 연상 • 무의식 분석을 위한 꿈 해석 • 내면 분석을 통한 자기 분석
	인본주의적	• 주관적 경험 기반의 성향 분석 • 내부 갈등 요소 • 정체성 기반의 자아개념 • 가치관 평가 • 자율성 측정 • 삶의 만족도 척도
윤리성	도덕적 이탈	• 도덕적 교육

		• 윤리적 판단력 • 주기적인 윤리 교육
	탈선	• 인지적 탈선 분석 • 정서적 탈선 분석 • 행동적 탈선 분석
	이익 실현	• 경제적 이익 실현의 투명성 • 사회적 이익 실현의 투명성 • 정서적 이익 실현의 투명성
	사이버 윤리	• 개인정보보호 • 온라인 소통 • 저작권 존중 • 사이버 범죄 예방

<표 16> 델파이 결과에 따른 인적 취약점 분류체계 기반 인적보안 측정지표(59)

인적 취약점 대분류	인적 취약점 구성요소	구성 요소별 측정 지표
우발성	개인성 (4)	권한 및 역할의 투명성
		권한 사용에 대한 투명성
		주요 직무자 지정 및 관리
		권한 오남용 등의 잠재적 피해 예방을 위한 직무 분리
	활동성 (3)	개인의 정보와 관련한 문서관리
		온라인상의 개인정보 관리
		온라인 공개 정보 분석
	위험성 (2)	사회공학 기법의 공격 형태 인지
		온라인 소통 출처 배경 조사
	보안성 (3)	주기적인 교육과 훈련
		주기적인 시스템 업데이트
		준수사항 인지를 위한 보안 서약
관계성	인맥 (3)	사회공학적 공격 기법의 활용
		동종(경쟁) 업계 관계 분석
		내부 갈등 요소 식별
	연결성 (3)	주기적인 교육과 훈련
		온라인 소통 출처 배경 조사
		지속적인 사고사례 전파
	갈등(1)	담당 업무의 중요도 분석
	청탁 (2)	금전적 이득의 필요성 식별
		이직 가능성 식별
잠재성	업무환경 (4)	업무 처리의 투명성
		업무 성과의 투명성
		업무 책임의 투명성
		보안 규칙 준수의 투명성 확보
	조직성 (3)	업무 협업의 투명성
		업무 성과 측정의 공정성 확보
		관행적 업무 습관의 제거
	규칙성 (2)	신기술에 대한 보안 이슈 분석
		주기적 보안 사고사례 공유
	사회성 (6)	컴플라이언스 이행 여부 투명성
		컴플라이언스 회피 방안 예방
		주기적인 보안 인식 교육의 시행
		강압적인 보안지침 제거
		퇴직 및 직무 변경 관리
		보안 위반 시 조치
심리학적	인지적 (3)	판단력 분석
		업무 협업 태도
		인지적 유연성 평가
	행동적	행동 패턴 분석을 위한 행동 관찰
	(3)	행동 패턴 분석을 위한 행동 기록
		행동 평가 척도
	정신분석적 (2)	업무 성과 분석
		사고 이력 분석
	인본주의적 (2)	가치관 평가
		자율성 측정
윤리성	도덕적 이탈 (3)	도덕적 교육
		윤리적 판단력 강화
		주기적인 윤리 교육
	탈선 (3)	인지적 탈선 분석
		정서적 탈선 분석
		행동적 탈선 분석
	이익 실현 (3)	경제적 이익 실현의 투명성
		사회적 이익 실현의 투명성
		정서적 이익 실현의 투명성
	사이버 윤리 (4)	개인 정보 보호
		온라인 소통
		저작권 존중
		사이버 범죄 예방