The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 24, No. 4, pp.1-7, Aug. 31, 2024. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2024.24.4.1
JIIBC 2024-4-1

인간중심보안설계 기반 제로 트러스트 보안모델 전개방안에 관한 연구

A Study on the Deployment Strategy of Zero Trust Security Model Based on Human-Centered Security Design

이진용*, 최병훈**, 장수진**, 전삼현***

Jin-Yong Lee*, Byoung-Hoon Choi**, Sujin Jang**, Sam-Hyun Chun***

요 약 기존의 전통적인 보안모델 설계는 대표적 두 가지 문제점을 가지고 있다. 첫째, 인간에 대한 고려보다는 기술중심으로 설계·구현되었다. 이와 같은 구조는 조직 내 심리적 저항, 사용자 실수와 같은 인지적 취약성에 의해 무력화될 수 있다. 둘째, 네트워크 경계기반 보안모델로 설계되었다. 이와 같은 설계는 4차 산업혁명의 패러다임과 코로나19로 인해 빠르게 보편화되고 있는 비경계 기반의 원격업무 환경에서는 적합하지 못하다. 본 논문에서는 이와 같은 전통적인 기술중심 보안모델의 문제점을 개선할 수 있는 방안으로 비경계 기반 최신 보안모델인 제로 트러스트 보안모델 내 인간 특성 위협을 연계하여 보안정책을 수립·반영할 수 있는 방안을 제언하였다. 이를 통해 기술적으로 발생하는 각종 위협 외 인간 특성 위협으로부터도 강건한 보안모델 설계 방안을 제언한다.

Abstract Traditional security model design presents two primary issues. First, these models have been developed and implemented with a technology-centered approach rather than considering human factors. Such structures can be undermined by cognitive vulnerabilities like psychological resistance within organizations and user errors. Second, these models are typically designed based on network perimeter security. This design is unsuitable for the boundary-less remote work environments rapidly becoming prevalent due to the Fourth Industrial Revolution and the COVID-19 pandemic. This paper proposes an approach to address these limitations by integrating human-centered threats within the Zero Trust security model, a state-of-the-art boundary-less security framework. By doing so, we suggest a robust security model design that can protect against both technical and human-centered threats.

Key Words : human-centered security design, human-centered threats, human factors, zero trust security model

*정회원, 숭실대학교 IT정책경영학과
**정회원, 숭실대학교 IT정책경영학과
***정회원, 숭실대학교 IT정책경영학과 (교신저자)
접수일자 2024년 6월 18일, 수정완료 2024년 7월 18일
게재확정일자 2024년 8월 9일

Received: 18 June, 2024 / Revised: 18 July, 2024 /
Accepted: 9 August, 2024
***Corresponding Author: shchun@ssu.ac.kr
Graduate School of IT Policy and Management, Soongsil University, Korea

Ⅰ. 서 론

1. 연구배경

전통적인 네트워크 경계 기반의 보안모델은 4차 산업혁명 시대의 초연결 패러다임 및 코로나19 등에 따른 원격 접속환경의 보편화에 따라 방어체계가 약화되고 있다[1]. 전통적인 경계기반 네트워크 보안 모델의 보안자원은 경계면을 중심으로 선택과 집중이 되어진다. 따라서 사용자 접근 및 인가 절차를 정상적으로 마친 사용자에 대해서는 신뢰된 자로 분류하고 보안자원의 집중이 해제된다. 이와 같은 보안모델에서 공격자는 경계면을 식별하고 우회 혹은 인가를 받을 수 있는 기술에만 선택과 집중을 하면 된다. 따라서 경계기반 네트워크 모델은 지능형·지속 공격을 수행하는 고도의 전문 해킹그룹에 의해 손쉽게 무용지물이 되고 만다. 또한 원격접속 업무환경의 확산은 기존의 네트워크 경계기반의 인프라 아키텍처 조차 무너뜨리고 있다[1, 2, 10]. 이와 같은 보안환경의 위협상황에 실효성있게 대응하기 위해 산업 및 학계 등 다양한 분야에서는 제로 트러스트 보안모델을 대안으로 삼고 활발한 연구를 수행하고 있다. 제로 트러스트 보안모델은 “신뢰하지 않고 항상 검증한다”는 비신뢰 기반 사상의 모델을 제시한다. 따라서 네트워크 경계면에서 접근과 인가 절차 완료한 사용자에 대해서도 예외 없이 보안자원이 지속적으로 투입한다[1, 2, 4].

이와 같은 제로 트러스트 보안모델이 이상적으로 구축될 경우 이론상 보안위협은 존재하지 않게 된다.

그러나 이론상 완벽해 보이는 제로 트러스트 보안모델 또한 고유의 취약점이 존재한다. 그것은 모든 보안모델이 가지고 있는 취약점이기도 한 인간적 요소이다. 보안의 가장 큰 취약점은 인간이라는 주장도 있듯이 보안모델은 조직 내 저항, 사용자의 실수 및 정책 위반 등에 의해 실패한다. 즉 인간은 본인이 구축한 시스템의 스스로 무너뜨릴 수 있는 존재이다[3, 5, 6, 7].

2. 연구목적

본 논문에서는 기술중심설계 기반의 제로 트러스트 모델을 구축이 가지고 있는 근원적 취약점에 대한 분석과 탐구를 통해 제로 트러스트의 효과적 전개방안을 제안하는 것을 목적으로 하고 있다.

기술중심보안설계는 사용자의 행동과 심리적 요소를 충분히 고려하지 않아 사용자 편의성, 효율성 등에 따른 저항감, 실수 및 착오 등과 같은 인지적 오류로 인해 초기 계획했던 목표를 실현하기 어려운 취약성을 내포하고 있다[3, 6, 7].

본 논문에서는 이와 같은 기술중심보안설계 기반의 제로 트러스트 모델의 문제점을 개선하기 위해 사용자 행동, 사용성, 인식수준 등을 고려한 인간중심보안설계를 요소를 부가하여 인지적 오류의 위험에 견고한 제로 트러스트 보안모델을 구성하기 위한 방안을 제언한다.

Ⅱ. 관련 연구

1. 제로 트러스트 아키텍처

제로 트러스트는 보안의 핵심 관점을 네트워크 기반 경계면서 사용자, 자원 중심으로 옮겨가는 사상이다. 즉 제로 트러스트는 네트워크 경로에 대한 통제 및 대역 설정은 더 이상 보안설계의 핵심요소로 보지 않는다.

제로 트러스트는 조직의 모든 자산(어플리케이션, 컴포넌트, 데이터, 인프라 등)과 주체(어플리케이션, 리소

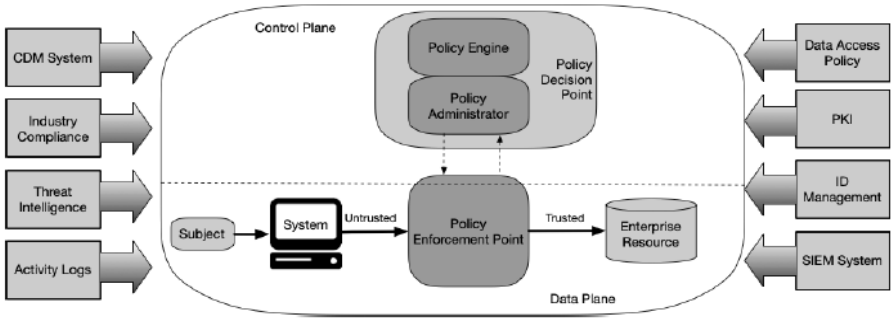

그림 1. 제로 트러스트 보안모델[2]
Fig. 1. Zero Trust Security Model[2]

스를 요청하는 객체, 모바일 기기 등)가 신뢰성이 전혀 보장되지 않는 환경에서 운영되고 있다는 것을 전제로 보안전략을 수립한다[1, 2].

이와 같은 제로 트러스트는 기술이나 통합솔루션을 의미하는 것은 아니며, 보안 아키텍처를 설계하는 철학의 개념이다[5].

NIST(미국 국립표준기술연구소)에서는 제로 트러스트 철학을 7개의 기본 개념으로 다음과 같이 정의하였다[1, 2].

1) 자원에 접근하는 모든 데이터와 서비스는 그 소유권과 무관하게 리소스로 간주한다.
2) 네트워크의 위치와 무관하게 모든 통신을 보호되어야 한다.
3) 자원에 대한 접근은 세션단위여야 한다.
4) 자원에 대한 접근은 동적정책으로 관리한다.
5) 모든 자산의 무결성과 보안상태는 모니터링되고 관리되어야 한다.
6) 모든 접근주체의 인증 및 인가는 동적 검증된 후 접근을 허용해야 한다.
7) 조직은 자산, 네트워크, 인프라 등의 현 상태에서 최대한 많은 정보를 수집할 수 있어야 한다.

이와 같은 사상에 입각하여 NIST에서는 그림 1과 같이 이상적인 제로 트러스트 보안모델을 제시하였다.

이상적인 제로 트러스트 보안모델은 네트워크 기반 경계를 넘어 접근주체(Subject)와 기업의 리소스(Enterprise Resource) 간의 연결 및 동작상태를 지속적으로 감시하고 통제한다. 이때 정책결정포인트(PDP: Policy Decision Point)에서는 접근주체와 리소스사이에서 발생하는 모든 정보를 취합하여 분석하고 정책을 동적으로 수립한다. 동적으로 수립된 정책은 접근주체와 리소스간의 접근통제 정책을 실제 구현하는 정책집행 포인트(PEP: Policy Enforcement Point)로 전달되어 실시간 동적 차단정책을 적용하게 된다.

이때 동적으로 정책이 수립된다는 것은 획득한 정보를 분석하여 시간적, 상황적 속성 기반으로 문맥적 분석을 통한 정책이 수립된다는 것을 의미한다. 따라서 인가받은 모든 접근주체라 할지라도 위반행위에 대해 지속적으로 검증받는 무결한 시스템이 구성되게 된다[1, 2].

2. 인간중심보안설계

인간중심보안설계는 보안모델을 구현할 때 사용자의 요구, 행동, 경험을 두고 접근하는 방식을 의미한다. 즉 사용자의 편의성을 증대시키고 거부감을 최소화하여 바람직한 행동을 유도하기 위한 설계이다.

인간중심보안설계에 대한 연구는 편향적 사고에 따른 보안정책 및 사고 등의 연관성 분석, 인적 취약점에 대한 분류 식별, 인간 친화적인 보안정책 개발 등 다양한 방향으로 수행되고 있다[3, 6, 7, 8].

표 1에서는 이와 같은 인간중심보안설계의 특징을 기술중심보안설계와 비교하여 보여준다.

표 1. 기술중심보안설계와 인간중심보안설계의 비교
Table 1. Comparison of Technology-Centered Security Design and Human-Centered Security Design

구분	기술중심보안설계	인간중심보안설계
사상	기술적 제어, 자동화시스템 중시	인간의 행동과 사용성 중시
목표	강력한 보안기술 설계	사용자 편의성 및 수용성을 고려한 보안설계
구현	방화벽, 암호화 등	인지과정을 고려한 절차 등
배경 이론	네트워크, 암호학, DBMS	인지심리학, 인간공학 등
위협 대응	기술적 취약점 보완조치	인간의 바람직하지 않은 행동의 교정
측정 지표	기술적 지표 (악성코드 차단 횟수 등)	행동인식 수준 (보안정책 준수 등)

기술중심보안설계는 보안시스템의 기술적 동작에 초점을 맞추고 있으며, 보안시스템 동작의 최적화를 기반으로 효과성을 측정한다. 이와 같은 기술중심보안설계의 근원적 취약점은 운영하는 주체인 인간의 고의적·비고의적 운영에 따라 스스로의 시스템 아키텍처를 무너뜨리는데 있다. 그림 2는 이와 같은 인간이 비합리적 행위를 하는 이유에 대한 단서를 제공해주는 인간의 뇌구조이다. 사건의 발생하는 단계에서 감정적 인지가 발생 할 경우 합리적 판단을 하는 전두엽은 비활성화되고 인간의 생리적 특성인 편도체의 영향을 받게 되는데 이때 바람직하

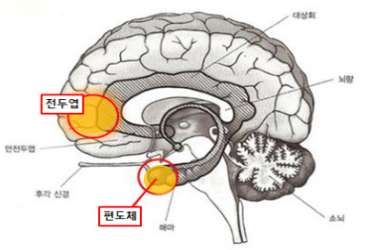

그림 2. 인간 뇌구조[3]
Fig. 2. The structure of the human brain[3]

지 않은 무의식적 편향적 반응을 일으킨다. 편향적 반응은 동조효과, 손실혐오, 인지부조화 등의 비합리적인 판단과 행동을 유도하기도 하고 과도한 자신감 등으로 합리적이지 않은 신념을 가지게 하여 비인지적 취약점을 파생한다. 따라서 비합리적인 판단을 유도하는 원인인 무의식적 자동반응에 식별하여 통제할 수 있는 대응전략을 구축하는 것이 중요하다[3].

Ⅲ. 인간중심보안설계 기반 제로 트러스트 보안모델 전개방안

본 논문에서는 제로 트러스트 보안모델 내 인간 특성에 따른 보안 위협을 분석하여 인간중심보안설계에 기반한 제로 트러스트 보안 모델 전개방안에 대해 제시한다.

1. 인간 보안 위협분석

표 2는 인간 특성에 따른 위협의 예시이다. 신념 및 고정관념 등에 의해 형성된 편향적 사고는 바람직한 행동을 저해하는 실수의 결과를 유도한다. 확증편향은 성향에 맞는 위협에만 몰입되는 현상을 바탕으로 다단계 관점의 보안전략 추구를 저해하여 비인지적인 단순실수, 위반을 유발할 수 있다.

미래가치 편향은 즉각적인 위험이 없다는 믿음 혹은 과도한 업무 등에 따른 위험관리 소홀로 지식 및 규칙기반 실수, 위반 등의 결과를 파생할 수 있다.

과도한 자신감은 위반행위, 규칙 미준수 혹은 충분히 보안 매뉴얼을 인지하고 있다는 비합리적 믿음으로 인해 규칙 및 지식기반 실수, 내부 부정행위 유도 등을 이끌어 낼 수 있다. 이와 같은 편향은 모든 인간이 가진 보편적 특성이자 보안 위협에 대한 취약한 인자이며, 이에 대한 대응방안이 구축되지 않을 경우 어떠한 견고한 시스템이라도 인간 스스로의 취약점에 의해 스스로 무너질 수 있는 위험을 내포하게 된다[3, 6, 7].

표 2. 인간 특성에 따른 보안 위협분석 예시
Table 2. Examples of Security Threat Analysis Based on Human Characteristics

구분	위협인자	위협 발생원인
신념 (원인)	확증편향	자산이 예상한 보안 위협 유형에만 대응
	미래가치 편향	단기적인 이익에 집중하여 부정행위 유발
	과도한 자신감	위반행위가 적발되지 않을 것으로 판단함
실수 (결과)	단순실수 및 착오	주의력 및 기억력 저하
	규칙기반 실수	절차의 오해
	지식기반 실수	지식 부족
	규칙위반	저항감, 업무압박, 개인 이익 추구

2. 제로 트러스트 보안모델 기반 인간 보안 위협분석

그림 3는 제로 트러스트 보안모델에서의 핵심요소인 접근주체(Subject), 자원(Resource)의 관계를 통제하는 정책결정포인트(PDP)와 정책집행포인트(PEP) 부분을 도식화한 부분이다.

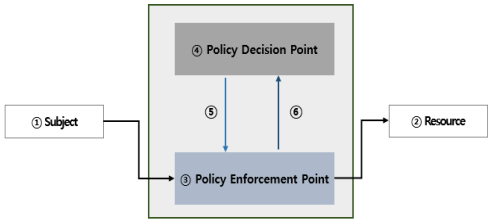

그림 3. 제로 트러스트 보안모델의 핵심 통제요소
Fig. 3. Key Control Elements of the Zero Trust Security Model

그림 3의 각 구간별 특징에 따라 다음과 같은 인간 보안 위협을 식별할 수 있다.

① 고의·비고의적 내부정책을 위반한 각종 접근 주체(PC, 모바일 기기, API 등)의 위협을 내포하고 있다. 이때 위협의 요인은 승인받지 않은 기기, 악성코드에 감염된 단말뿐만 아니라 정상적인 기기일지라도 내부자 소행에 의한 정보탈취 등을 포함한다. 이와 같은 행위를 유발하는 심리적 요인으로 신념은 과도한 자신감, 미래가치 편향에 기반한 규칙위반의 실수를 파생한다.

② 자원에 대해서는 편의를 위한 보안설정 값의 임의적 변경, 손쉽거나 본인이 중요하다고 판단되는 취약점에 대한 선별적 이행조치 등의 관리적 위험이 발생할 수 있다. 이와 같은 위험은 확증편향, 미래가치 편향 등에 의해서 유발되며 마찬가지로 규칙위반이라는 부정적 행위를 유발한다.

③, ⑥ 정책집행포인트의 경우 탐지모드 운영 및 예외정책 적용을 통해 정책이 적정하게 집행되지 않을 위험이 존재한다. 이와 같은 위협은 마찬가지로 확증편향, 미래가치 편향, 과도한 자신감에 의해 발생하며, 규칙위반, 지식기반 실수를 유도할 수 있다.

④, ⑤ 접근 주체, 접근대상, 정책집행포인트의 정보들이 정상적으로 전달되지 않을 경우 정책결정포인트 적절한 정책을 결정할 수 없게 되어 사실상의 제로 트러스트 모델이 붕괴된다. 위 언급한 각 구간에서 발생할 수 있는 인간 보안 위협과 정책결정포인트 자체 운영 미흡에서 발생할 수 있는 위협이 보합적으로 작용하는 구간이다. 해당 구간 또한 마찬가지로 확증편향 등에 따른 규칙위반 및 규칙·지식기반의 실수가 동반될 수 있다.

표 3은 이와 같은 인간의 위협을 NIST의 제로 트러스트 모델 7원칙에 기반하여 연계 및 분석한 내용이다.

표 3. 제로 트러스트 원칙과 인간 보안위협 연계
Table 3. Linking Zero Trust Principles with Human Security Threats

원칙	구간	원인적 요소	결과적 요소	발생 위협
(1)리소스	①, ②	과도한 자신감, 미래가치 편향	규칙위반	비정상적 접근허용, 정보탈취
(2)네트워크	③	확증편향, 미래가치 편향, 과도한 자신감	규칙위반, 지식기반 실수	접근통제 및 네트워크 보안 우회구간 허용
(3)접근통제				
(4)정책관리	④, ⑤	확증편향, 미래가치 편향	규칙위반, 규칙 및 지식기반실수	제로 트러스트 모델 무력화
(5)모니터링	③~⑤	확증편향, 미래가치 편향, 과도한 자신감	규칙위반, 지식기반 실수	비정상적인 불완전한 모니터링 (정책관리 실패 유도)
(6)인증/인가	③	확증편향, 미래가치 편향, 과도한 자신감	규칙위반, 지식기반 실수	비정상적 인증 및 인가 허용
(7)정보수집	⑥	확증편향, 미래가치 편향, 과도한 자신감	규칙위반, 지식기반 실수	비정상적인 불완전한 정보수집 (정책관리 실패 유도)

3. 인간중심보안설계 기반 제로트러스트 보안모델 전개

그림 4는 앞서 언급된 제로 트러스트의 인간 위협에 따른 근원적 취약점을 개선하기 위한 인간중심보안설계 기반의 제로 트러스트 모델 전개하기 위한 개념도이다.

컨트롤 영역은 제로 트러스트 보안모델의 핵심 두뇌 역할을 하는 곳으로 제로 트러스트 보안모델을 실행하기 위한 각종 정책을 수립한다. 데이터 영역은 접근주체와 접근대상인 자원간의 접근통제 정책이 실집행되는 구간으로 컨트롤 영역에서 수립된 정책이 실현되는 구간이다.

인간중심보안설계 기반 제로 트러스트 전개 전략은 NIST의 제로 트러스트 7원칙에 기반한 인간 보안위협 연계 분석에 대한 표 3의 내용을 그림 4에 도식화하였으며, 다음과 같이 구성된다.

(1) 리소스 대상이 되는 접근주체 및 자원에 대한 부분으로 규칙위반에 대한 원인적 요소에 대한 점수 실제 발생한 규칙위반과의 관계를 바탕으로 인간위협을 점수화하여 접근에 대한 규칙을 생성할 수 있도록 한다. 이때 점수화 기준은 상황적 속성(설정 값 등) 및 동적 속성(문맥적 이상행위 등)을 종합하여 산출할 수 있도록 한다.

(2), (3) 무결성 검증 및 최소 접근통제 정책은 리소스 내 인간 위협 점수 검증 및 컨트롤 영역의 정책결정포인트에서 전달받은 점수를 고려하여 판단하고 실행한 결과를 정책결정포인트로 재전송하여 실행의 타당성을 재검증받을 수 있돌고 한다.

(4), (6) 실행된 인가 정책에 대해 확증편향 등 인간위협 점수화를 판단하여 동적으로 인증/인가 정책을 지속적으로 갱신할 수 있도록 한다.

(5) 모니터링을 통해 수집된 각종 정보에서는 인간이 발생시킨 실수에 대해 집중적으로 탐지할 수 있는 시나

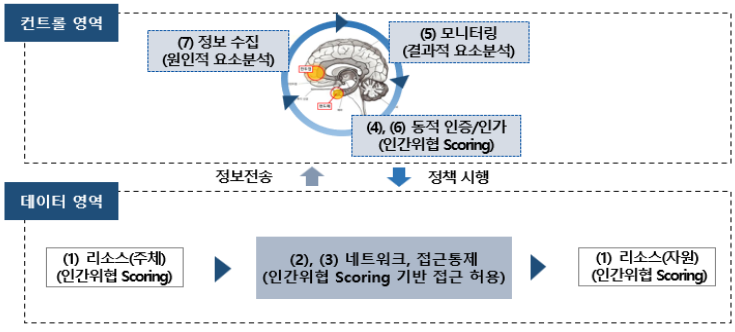

그림 4. 인간중심보안설계 기반 제로 트러스트 보안모델
Fig. 4. Human-Centered Security Design-Based Zero Trust Security Model

리오 기반 규칙이 적용될 수 있어야 한다.

(7) 수집된 인간실수인 결과적 요소의 원인을 분석하여 인간의 비합리적 요인에 대한 대응정책의 가중치 및 동적 전략을 수립할 수 있는 기반을 마련하도록 한다.

Ⅳ. 결 론

기존의 전통적인 보안모델은 기술중심의 네트워크 경계기반으로 설계·구축되었다. 이와 같은 구조는 다음과 같은 두 가지 문제점을 내포하고 있다. 첫째, 사용자의 심리적 저항 및 실수 등과 같은 인지적 오류에 취약한 점이다. 둘째, 네트워크 경계기반의 설계는 4차 산업혁명 시대의 언제 어디서나 접속 가능한 비경계 기반의 원격 업무 환경에서는 접합하지 못하다.

본 논문에서는 이와 같은 문제점을 개선하기 위해 네트워크 경계기반 보안모델을 대처하기 위한 최신 보안모델로 각광받고 있는 제로 트러스트 모델을 인간중심보안 설계를 기반으로 전개될 수 있는 방안을 제언하고자 하였다. 이를 위해 다음과 같은 접근방법을 취하였다.

첫째, 인간 특성에 따른 위협을 분석하였다. 인지적 오류를 유발하는 생각(원인)과 실수(결과)를 바탕으로 부정적 행위를 발생시키는 인지적 취약성을 식별하였다.

둘째, 제로 트러스트 보안모델의 핵심요소를 인간 특성에 따른 위협과의 연계를 시도하였다. 이를 위해 NIST에서 제시한 원칙 및 가이드에 기반하여 제로 트러스트 모델의 구축·운영 상에서 발생할 수 있는 인지적 위협을 식별하여 연계하였다.

마지막으로, 인간중심보안설계가 반영된 제로 트러스트 보안모델 전개 방법을 제언하였다. 식별된 인간 특성 위협이 측정되어 제로 트러스트 모델의 정책설정 및 집행에 반영되는 모델을 제시하였다.

이와 같은 접근방법을 통하여 기술적 이상행위 외 인간의 인지적 오류(사용자 저항, 실수, 고의·비고의적 부정행위)로부터 발생할 수 있는 위협을 방어하기 위한 모델 구축 전략을 제언하였다. 향후 인간 특성 위협에 대한 추가 식별 및 다양한 환경의 제로 트러스트 보안모델과의 연계에 대한 연구를 수행 할 경우, 인지적 오류에 보다 강건한 제로 트러스트 보안모델 전개 전략으로 발전할 수 있을 것으로 기대된다.

References

[1] J. Y. Lee, B. H. Choi, S. H. Chun, "A Study on How to Build a Zero Trust Security Model," KIPS Transactions on Computer and Communication Systems, Vol.12, No.6, pp.189-196, 2023.
DOI: https://doi.org/10.3745/KTCCS.2023.12.6.189

[2] Scott Rose, Oliver Borchert, Stu Mitchell, Sean Connelly, "NIST Special Publication 800-207, Zero Trust Architecture", National Institute of Standards and Technology, 2020.

[3] J. Y. Lee, K. C. Jung, J. S. Ahan, "A Study on th Analysis of Relation to Biased Thinking and Response to Security Accident", Korean Industrial Security Research, Vol.7, No.2, pp. 53-81, 2017
DOI: https://doi.org/10.1016/j.jsr.2023.07.012

[4] T. R. M, M. Arunachalam, R. R, K. Rammaraj, M. Arunachalam, K. P, "A Review on the Detection of Deep Fake and Propaganda Videos and Images-based Voice and Facial Manipulation using AI Techniques", IEEE ICACRS-2023, pp.1083-1087, 2023
DOI: https://doi.org/10.3390/s22124556

[5] M. L. Casiano, "Shaping the Security Environment: Incorporating Human-Centered Design Within Security Cooperation Planning," M.S. thesis, U.S. Army Command and General Staff College, Fort Leavenworth, KS, USA, 2018.

[6] K. S. Im and H. Y. Kwon, "A Study on Influence of Information Security Stress and Behavioral Intention for Characteristic Factors of Information Security Policy Perceived by Employee," The Journal of The Institute of Internet, Broadcasting and Communication, Vol.16, No.6, pp.243-253, 2016.
DOI: https://doi.org/10.7236/JIIBC.2016.16.6.243

[7] J. Heo and S. Ahn, "Effects of Biased Awareness of Security Policies on Security Compliance Behavior," Journal of Korean Association of Computer Education, Vol.23, No.1, pp.63-75, 2020.
DOI: https://doi.org/10.32431/kace.2020.23.1.006

[8] I. Hwang, "A study on the Effects of Organization Justice and Organization Trust on Mitigation of Techno-stress Related to Information," Journal of the Korea Academia-Industrial cooperation Society, Vol.22, No.7, pp.435-448, 2021.
DOI: https://doi.org/10.5762/KAIS.2021.22.7.435

[9] D. H. Kim, Y. Lee, "A Study on the ISMS-P Accreditation Effect Using the Seven Threats of Security- Focused on Enterprise Size and Career," Journal of KIIT, Vol.18, No.4, pp.109-119, 2020.
DOI: http://dx.doi.org/10.14801/jkiit.2020.18.4.109

[10] S. K. Park, "Development of Software-Defined Perimeter-based Access Control System for Security of Cloud and IoT System," The Journal of The Institute of Internet, Broadcasting and Communication, Vol.21, No.2, pp.15-26, 2021.
DOI: https://doi.org/10.7236/JIIBC.2021.21.2.15

저 자 소 개

이 진 용(정회원)

- 2008년 : 연세대학교 컴퓨터과학과(석사)
- 2022년 ~ 현재 : 숭실대학교 IT정책경영학과 박사과정
- 관심분야 : 인간중심보안설계, 제로트러스트, 블록체인 보안, 정보보호 및 개인정보보호 관리체계, IT 및 정보보호 법률·정책

최 병 훈(정회원)

- 2004년 : 숭실대학교 산업정보시스템공학(석사)
- 2022년 ~ 현재 : 숭실대학교 IT정책경영학과 박사과정
- 관심분야 : 인간중심보안설계, 제로트러스트, 정보보안, 블록체인, E-Commerce, IT 및 정보보호 법률·정책

장 수 진(정회원)

- 2004년 : 국방대학교 무기체계공학(석사)
- 2014년 ~ 현재 : 숭실대학교 IT정책경영학과 박사과정
- 관심분야 : 인간중심보안설계, 제로트러스트, 인공지능 보안, 무기체계 보안

전 삼 현(정회원)

- 1989년 : 숭실대학교 법학과(석사)
- 1992년 : 프랑크푸르트대학교 법학과(박사)
- 1993년 ~ 현재 : 숭실대학교 법학과, 숭실대학교 IT정책경영학과 교수
- 관심분야 : 인간중심보안설계, 제로트러스트, 블록체인 보안, 정보보호 및 개인정보보호 관리체계, IT 및 정보보호 법률·정책