사물인터넷융복합논문지 Vol. 11, No. 1, pp. 9-15, 2025 https://doi.org/10.20465/KIOTS.2025.11.1.009

중소기업 대상 정보보호 컨설팅을 통한 보안 취약점 분석 및 대응모델 설계

이근호*
백석대학교 컴퓨터공학부 교수

Design of a Security Vulnerability Analysis and Response Model through Information Security Consulting for SMEs

Keun-Ho Lee*
Professor, Div. of Computer Engineering, BaekSeok University

요 약 사물인터넷 환경에서 중소기업은 지속적으로 진화하는 보안 위협에 노출되고 있으며, 이에 대한 효과적인 대응 전략이 필요하다. 중소기업의 보안 취약점은 외부 공격 및 내부 보안 사고로 인해 심각한 피해를 초래할 수 있으며, 이를 예방하고 대응하기 위한 체계적인 정보보호 컨설팅 모델이 요구된다. 본 연구는 중소기업 10개 기업을 대상으로 정보보호 컨설팅을 수행하여 분석된 자료를 기반으로 보안 취약점 분석 및 대응모델을 설계하는 것을 목표로 한다. 이를 위해 실제 컨설팅 과정에서 도출된 주요 보안 위협요소를 분석하고, 취약점 진단 및 대응 방안을 포함한 맞춤형 보안 컨설팅 프레임워크를 제안한다. 제안된 모델은 위협 유형, 침해 시나리오 및 대응 절차를 포함하여 중소기업 환경에 최적화된 보안 컨설팅 과정으로 설계되었으며, 실무 적용이 가능한 대응 전략을 제안한다.

주제어 : 사물인터넷, 중소기업, 보안 취약점, 정보보호 컨설팅, 대응 모델

Abstract Small and medium-sized enterprises(SMEs) in IoT environment are continuously exposed to evolving security threats, necessitating effective response strategies. Security vulnerabilities in SMEs can result in severe damage due to external attacks and internal security incidents, highlighting the need for a systematic information security consulting model to prevent and mitigate such risks. This study aims to design a security vulnerability analysis and response model based on data obtained through information security consulting for ten SMEs. To achieve this, major security threat factors identified during the consulting process are analyzed, and a tailored security consulting framework incorporating vulnerability assessment and response strategies is proposed. The proposed model is designed as a security consulting process optimized for SMEs, encompassing threat types, breach scenarios, and response procedures. Furthermore, it suggests practical response strategies that can be effectively implemented in real-world SME environments.

Key Words : IoT, SME, Security Vulnerability, Security Consulting, Response Model

*이 논문은 2024학년도 백석대학교 학술연구비 지원을 받아 작성되었음
*교신저자 : 이근호(root1004@bu.ac.kr)
접수일 2024년 10월 12일 수정일 2024년 12월 24일 심사완료일 2025년 01월 06일

1. 서론

4차 산업혁명의 발전과 함께 사물인터넷 기술이 빠르게 확산되면서, 중소기업(SMEs)은 디지털 혁신을 통해 비즈니스 효율성을 높이고 있지만, 동시에 점점 복잡해지는 보안 위협에 노출되고 있다. 중소기업은 대기업에 비해 보안 인프라가 미흡하고 전문 인력이 부족하여 랜섬웨어 공격, 피싱, 내부 데이터 유출, 네트워크 취약점 공격과 같은 보안 위협에 취약한 상황이다. 이러한 위협은 기업의 핵심 정보 유출, 운영 중단, 금전적 피해 등을 초래할 수 있어 효과적인 대응 전략이 필수적이다. 그러나 현재 중소기업을 위한 보안 컨설팅 모델은 대기업 중심의 보안 전략을 단순 적용하는 방식이 많아, 중소기업 환경에 최적화된 맞춤형 보안 취약점 분석 및 대응모델이 요구된다. 이에 본 연구는 중소기업 10개 기업을 대상으로 정보보호 컨설팅을 수행하여 보안 취약점을 분석하고, 이를 기반으로 한 대응모델을 설계하는 것을 목표로 한다. 연구 과정에서 도출된 주요 보안 위협요소를 분석하고, 위협 유형, 침해 시나리오, 대응 절차를 포함한 맞춤형 보안 컨설팅 프레임워크를 제안하여 실무 적용이 가능한 대응 전략 모델을 설계하였다. 연구 방법론으로는 중소기업의 정보보호 환경을 진단하고 보안 취약점을 분석한 후, 이를 기반으로 한 맞춤형 대응모델을 설계하는 과정을 포함하며, 실효성을 평가하여 개선 방안을 제안한다. 본 연구에서 제안하는 보안 대응 모델은 중소기업이 자신의 보안 취약점을 체계적으로 분석하고 대응할 수 있도록 지원하며, 보안 인프라가 부족한 기업들도 실질적으로 적용할 수 있는 실무 중심의 보안 전략을 제공한다. 또한, 향후 중소기업을 대상으로 한 정보보호 컨설팅 및 보안 정책 수립에 기초자료로 활용될 수 있을 것으로 기대된다.

본 연구에서는 보안 컨설팅 관련 연구를 통해 기존의 정보보호 컨설팅 방법을 분석하고, 이를 기반으로 중소기업을 대상으로 한 보안 취약점 분석 및 대응 모델을 설계하는 것을 목표로 한다. 이를 위해 기존의 정보보호 컨설팅 사례를 검토하고, 실제 컨설팅 과정에서 도출된 주요 보안 취약점을 분석하여 대응 방안을 도출한다. 또한, 컨설팅을 통한 취약점 도출 경험을 바탕으로 맞춤형 대응 모델을 설계하고, 실무에서 적용 가능한 보안 프레임워크를 제안하고자 한다. 본 연구에서 제안하는 대응 모델은 중소기업 환경에 최적화된 보안 전략을 포함하며, 위협 유형 분석, 침해 시나리오 정의, 대응 절차 설계 등을 포함한다. 이를 통해 중소기업이 자체적으로 보안 취약점을 진단하고 대응할 수 있도록 지원하며, 보안 인프라가 부족한 기업들도 실질적으로 활용할 수 있는 모델을 제공한다. 본 연구의 결과는 중소기업을 대상으로 한 정보보호 컨설팅 및 보안 정책 수립에 기초 자료로 활용될 것으로 기대된다.

2. 관련 연구

2.1 보안 컨설팅 방법론

보안 컨설팅은 기업이 보안 리스크를 식별하고 효과적인 대응 전략을 수립할 수 있도록 지원하는 핵심 과정이다. 기존 연구에서는 ISO/IEC 27001, NIST 사이버 보안 프레임워크, ISMS-P 등 다양한 정보보호 컨설팅 방법론이 활용되고 있으며, 이를 기반으로 조직의 보안 수준을 평가하고 개선하는 방식이 제안되었다. 특히, 중소기업을 위한 맞춤형 보안 컨설팅 방법론을 제시하는 연구들이 수행되었으며, 비용 및 인력 부족 등의 문제를 해결하기 위한 효율적인 보안 컨설팅 방안이 연구되고 있다. 예를 들어, 리스크 기반 보안 컨설팅 모델을 적용하여 기업의 보안 요구사항을 반영하고 맞춤형 보안 정책을 제안하는 연구가 진행되었다. 본 연구에서는 기존의 보안 컨설팅 방법론을 검토하고, 이를 기반으로 중소기업 맞춤형 컨설팅 모델을 설계하고자 한다[1-8].

2.2 보안 취약점 분석

보안 취약점 분석은 보안 사고를 예방하고 대응하기 위한 필수 과정으로, 기존 연구에서는 공격 벡터 분석, 취약점 진단 도구 활용, AI 기반 이상 탐지 시스템 등의 접근 방식이 제안되었다. 특히, OWASP Top 10, CVSS (Common Vulnerability Scoring System), MITRE ATT&CK 프레임워크 등을 활용하여 취약점을 평가하고 분류하는 연구가 활발히 진행되었다. 또한, 기업 환경에서 발생하는 실제 보안 침해 사례를 분석하여 주요 취약점을 식별하고 대응 방안을 제시하는 연구도 수행되었다. 본 연구에서는 기존 연구에서 다룬 보안 취약점 분석 방법을 활용하여 중소기업 10개사를 대상으로 한 컨설팅 데이터를 기반으로 주요 보안 취약점을 도출하고, 이를 분석하여 대응모델을 설계하고자 한다[9-17].

2.3 보안 대응모델 설계

보안 사고 발생 시 효과적인 대응을 위해서는 침해 시

나리오 기반 대응 모델, 위협 탐지 및 대응 자동화 시스템, 보안 운영 센터 모델 등이 연구되고 있다. 기존 연구에서는 사전 예방 및 실시간 탐지를 위한 인공지능 기반 보안 대응 모델과, 보안 위협 발생 후 빠른 복구를 위한 포렌식 기반 대응 모델 등이 제안되었다. 특히, 제로트러스트 및 보안 액세스 서비스 에지 모델을 활용한 보안 대응 체계가 최근 연구의 중심이 되고 있으며, 클라우드 및 엣지 컴퓨팅 환경에서도 적용 가능한 보안 모델이 활발히 연구되고 있다. 이러한 기존 연구를 참고하여 중소기업 환경에서 실질적으로 적용할 수 있는 맞춤형 대응 모델을 설계하고, 기업이 자체적으로 취약점을 진단하고 대응할 수 있는 실무 중심의 보안 프레임워크를 제안하고, 기업 내부의 보안 역량 강화를 위한 체계적인 가이드라인을 제공하는 것을 목표로 한다[18-19].

3. 정보보호 컨설팅 취약점 분석

본 연구는 충남지역 특화사업의 중소기업 정보보호 관리체계 취약점 진단 보고서를 기반으로 중소기업의 보안 취약점을 심층적으로 분석하고, 효과적인 대응 모델을 도출하는 것을 목표로 한다. 이를 위해 총 10개 기업을 대상으로 정보보호 컨설팅을 수행하였으며, 각 기업의 보안 체계를 다각도로 점검하여 주요 취약점을 도출하였다. 특히, 본 연구에서는 중소기업의 정보보호 수준을 향상시키기 위해 기술적·관리적·물리적 보안 요소를 종합적으로 고려하였으며, 기업별 보안 환경과 산업 특성을 반영한 맞춤형 보안 전략을 수립하였다. 또한, 도출된 취약점에 대한 실질적인 보완 조치를 제안하고, 지속적인 보안 수준 유지를 위한 정책적·운영적 개선 방안을 모색하였다. 이러한 연구 과정을 통해 중소기업이 직면한 보안 위협을 보다 효과적으로 대응할 수 있도록 체계적인 취약점 분석 방법론을 적용하였으며, 분석 과정은 다음과 같이 진행되었다.

3.1 보안 취약점 분석 절차

3.1.1 사전 준비 단계

- 기업 환경 및 보안 요구사항 분석
  - · 기업별 보안 목표 및 운영 환경 파악
  - · 클라이언트의 주요 정보자산 및 보호 대상 정의
  - · 기업의 정보보호 정책 및 보안 관련 내부 프로세스 검토
- 정보보호 관리체계(ISMS-P) 기반 점검 항목 설정
  - · 기업의 보안 수준을 평가하기 위해 ISMS-P 기준의 점검 항목 설정
  - · 평가 항목: 관리적 보안, 기술적 보안, 물리적 보안

3.1.2 취약점 점검 및 분석 단계

- 정보보호 관리체계(ISMS-P) 기반 취약점 점검
  - · 주요 보안 관리 영역을 대상으로 평가 수행
  - · 평가 방식: 문서 점검, 현장 실사, 인터뷰 및 테스트 수행
- 기술적 보안 점검 수행
  - · 네트워크 및 시스템 보안 점검
    방화벽, IDS/IPS, VPN 등의 보안 설정 검토
    무선 네트워크(Wi-Fi) 보안 점검
    원격 접속 및 네트워크 트래픽 모니터링
  - · 웹 및 애플리케이션 보안 점검
    OWASP Top 10 기반 웹 애플리케이션 취약점 점검
    SQL Injection, XSS, CSRF 검토
  - · 사용자 및 접근제어 점검
    관리자 및 사용자 계정 관리 정책 점검
    다중 인증(MFA) 적용 여부 확인
    권한 부여 및 접근통제 정책 적절성 평가
  - · 로그 및 보안 모니터링 점검
    로그 수집 및 분석 시스템(SIEM) 운영 여부 확인
    실시간 이상 행위 탐지 여부 평가
- 물리적 보안 점검 수행
  - · 데이터센터 및 서버룸 출입 통제 확인
  - · CCTV, 출입 관리 시스템, 서버실 보안 환경 점검
- 인적 보안 점검 수행
  - · 보안 교육 이수 여부 및 교육 프로그램 운영 현황 점검
  - · 직원 보안 인식 수준 평가(소셜 엔지니어링 테스트 활용)
  - · 위험 평가 수행
    취약점 발견 시, 위험 평가 기준(상/중/하)으로 분류
    위험 평가 기준:
    상(High): 즉각적인 조치가 필요한 심각한 취약점
    중(Medium): 개선이 필요하지만, 보완 조치로 완화 가능
    하(Low): 보안 강화가 필요하지만, 즉시 조치가 필요하지 않은 사항

3.2 취약점 평가 기준 및 모델

- ISMS-P 기반 관리적 취약점 평가
  · 정보보호 정책 및 조직 구조 검토
  · 기업의 보안 관련 프로세스 및 대응 체계 평가
- CVSS(Common Vulnerability Scoring System) 기반 기술적 취약점 평가
  · 보안 취약점을 정량적으로 분석하여 CVSS 점수 부여
  · 취약점별 위험도 분석을 통해 우선순위 결정
- 위험 관리 체계 적용
  · 조직의 보안 수준 및 보안 요구사항을 반영하여 맞춤형 개선방안 도출

3.3 취약점 분석 결과

이번에 수행한 보안 취약점 분석 방법론을 통해 중소기업의 보안 수준을 정량적으로 평가하고, 주요 보안 취약점을 도출할 수 있었다. 이를 기반으로 기업 환경에 최적화된 맞춤형 대응 전략을 수립하여 보안 수준을 향상시키고, 기업의 보안 리스크를 줄이는 것을 목표로 한다. 또한, 자동화된 위협 탐지 및 대응 체계를 도입하여 보안 사고를 사전에 예방하고, 발생 시 신속하게 대응할 수 있도록 지원한다.

- 중소기업의 보안 수준 향상: 정보보호 컨설팅을 통해 기존 보안 취약점을 분석하고 개선하여 전반적인 보안 수준을 높일 수 있다.
- 침해사고 대응력 강화: 보안 사고 발생 시 신속한 대응을 위한 프로세스 및 위기 관리 체계 구축 가능하다.
- 법적 요구사항 준수: ISMS-P 및 개인정보 보호법 등 관련 법규 준수를 지원하여 법적 리스크를 감소한다.

[표1]은 중소기업을 대상으로 진행한 정보보호 컨설팅을 통해 관리적 보안, 계정 및 접근제어, 네트워크 보안, 애플리케이션 보안, 물리적 보안, 인적 보안의 6대 주요 보안 영역에서 취약점이 식별되었다. 주요 취약점으로는 보안 정책 부재, 접근통제 미흡, 네트워크 보안 취약점, 웹 보안 패치 부족, 물리적 보안 미흡, 직원 보안 인식 부족 등이 확인되었으며, 이러한 문제들은 기업의 보안 위협을 증가시키고 침해사고 발생 가능성을 높이는 요인으로 작용하고 있다.

이를 해결하기 위해 맞춤형 보안 개선 방안을 제안하였다. 관리적 보안 강화를 위해 보안 정책을 수립하고 경영진의 보안 참여를 확대하는 것이 필요하며, 접근통제 개선을 위해 다중 인증 도입 및 계정 관리 정책을 강화해야 한다. 네트워크 보안 강화를 위해 방화벽 정책을 강화하고 원격 접근을 제한하며, 애플리케이션 보안 강화를 위해 보안 패치를 적용하고 웹 방화벽을 구성하는 것이 효과적이다. 또한, 물리적 보안 강화를 위해 출입 통제 및 접근 기록 관리 시스템을 도입하고, 보안 인식 제고를 위해 정기적인 보안 교육 및 내부자 위협 관리를 강화할 필요가 있다.

이러한 보안 개선 조치를 통해 중소기업은 보안 리스크를 최소화하고, 전반적인 보안 수준을 향상하며, 사이버 위협에 대한 대응력을 높일 수 있을 것으로 기대된다. 지속적인 보안 모니터링과 개선 활동을 통해 기업의 보안 체계를 더욱 견고하게 구축하는 것이 필수적이며, 향후 정보보호 정책 수립 및 실행에 대한 지속적인 관리가 요구된다.

〈Table 1〉 Security Vulnerability Analysis Results

Security Area	Description of Vulnerability	Risk Level	Improvement Measures
Administrative Security	Lack of information security policies, insufficient management participation	High	Establish security policies, provide management security training
Account & Access Control	Shared administrator accounts, lack of multi-factor authentication (MFA)	Medium	Implement MFA, strengthen account policies
Network Security	Weak firewall settings, lack of external access management	High	Strengthen firewall policies, restrict remote access
Application Security	Presence of web vulnerabilities (SQL Injection, XSS)	High	Apply security patches, configure Web Application Firewall (WAF)
Physical Security	Inadequate server room access control	Medium	Implement access log management system
Human Security	Lack of security training, insufficient insider threat management	Medium	Conduct regular security training programs

4. 중소기업 맞춤형 보안 대응모델

본 연구에서 도출된 보안 취약점을 해결하기 위해 중소기업 환경에 최적화된 보안 대응 모델을 제안한다. 해당 모델은 [표2]의 관리적 보안, 기술적 보안, 물리적 보안, 인적 보안의 4대 보안 영역을 중심으로, 선제적 예방(Security Prevention), 실시간 탐지(Security Detection), 신속 대응(Security Response), 지속적 개선(Security Enhancement)의 4단계 접근 방식을 적용하였다. 이를 통해 중소기업이 최소한의 자원으로도 보안 리스크를 줄이고, 지속적인 개선을 통해 보안 체계를 강화할 수 있도록 설계하였다.

먼저, 관리적 보안 측면에서는 정보보호 정책을 수립하고 보안 조직을 구성하며, 경영진의 보안 참여를 확대하는 것이 필요하다. 기업 규모에 맞는 ISMS-P 기반 보안 정책을 수립하고 운영 가이드라인을 마련하여, 보안 운영의 체계성을 확보해야 한다. 또한, 경영진이 보안 리스크를 명확하게 인식하고 대응할 수 있도록 정기적인 보안 회의를 개최하고 보안 브리핑을 제공하는 것이 중요하다.

기술적 보안 측면에서는 네트워크 및 시스템 보안을 강화하기 위해 네트워크 방화벽, 침입 탐지 시스템(IDS/IPS), 실시간 로그 분석 시스템을 도입하고 운영을 최적화해야 한다. 특히, 웹 및 애플리케이션 보안을 강화하기 위해 OWASP Top 10 기준 웹 애플리케이션 취약점을 점검하고, 웹 방화벽 및 API 보안 솔루션을 적용하는 것이 필수적이다. 또한, 랜섬웨어 및 데이터 유출 사고를 예방하기 위해 중요 데이터 암호화 및 오프라인 백업 정책을 구축해야 한다.

물리적 보안 측면에서는 출입 통제 시스템을 구축하고, 서버룸 및 중요 시설의 접근 관리체계를 강화하는 것이 필요하다. 출입 카드를 활용한 접근 제어, CCTV 운영 모니터링 강화, 출입 로그 관리 시스템 도입 등을 통해 물리적인 보안 사고를 예방할 수 있다. 또한, 클라우드 보안을 고려하는 기업의 경우 클라우드 접근 통제 정책을 수립하고, 데이터 보호를 위한 암호화 및 접근 권한 관리를 철저히 수행하는 것이 중요하다.

마지막으로, 인적 보안 측면에서는 보안 인식을 강화하고 내부자 위협을 예방하기 위한 교육과 정책이 필요하다. 기업 내 모든 직원이 보안 정책을 준수하고 위험 요소를 인식할 수 있도록 연 2회 이상의 보안 교육을 시행하고, 실전 대응 능력 강화를 위한 피싱 이메일 대응 훈련을 수행하는 것이 효과적이다. 또한, 내부 보안 위협을 사전에 예방하기 위해 보안 서약서를 도입하고, 직원의 보안 정책 준수 여부를 정기적으로 점검하는 것이 필요하다.

본 대응 모델을 적용함으로써 중소기업은 보안 리스크를 줄이고, 전반적인 보안 수준을 향상하며, 사이버 위협에 대한 대응력을 높일 수 있을 것으로 기대된다. 체계적인 정보보호 정책 및 기술적 보안 강화로 보안 위협을 사전에 차단할 수 있으며, 실시간 보안 모니터링 및 대응 체계를 구축하여 침해사고 발생 시 신속한 조치가 가능해진다. 또한, 지속적인 교육과 내부 보안 강화 조치를 통해 전 직원의 보안 의식을 높이고, 기업의 보안 문화를 정착시킬 수 있다.

본 연구에서 제안한 보안 대응 모델은 중소기업이 실질적으로 적용할 수 있는 맞춤형 보안 체계로, 기업의 보안 리스크를 효과적으로 줄이고 지속적인 보안 성숙도를 높이는 데 기여할 것으로 기대된다. 이를 통해 중소기업이 자율적으로 정보보호 체계를 강화하고 보안 사고를 예방할 수 있도록 지속적인 관리와 지원이 필요하다.

〈Table 2〉 Overview of the Security Response Model for SMEs

Security Area	Response Phase	Key Response Measures
Administrative Security	Prevention (Security Prevention)	- Establishment of ISMS-P-based security policies - Formation of security teams and increased management involvement
Technical Security	Detection (Security Detection)	- Implementation of Intrusion Detection System (IDS) - Adoption of Security Information and Event Management (SIEM) for real-time log monitoring
Physical Security	Response (Security Response)	- Deployment of access control systems and entry log management - Strengthening data center and server room security
Human Security	Enhancement (Security Enhancement)	- Regular security training and internal threat management - Simulated training programs (e.g., phishing email tests) to raise awareness

5. 결론

본 연구에서는 중소기업을 대상으로 한 정보보호 컨설팅을 수행하여 주요 보안 취약점을 분석하고, 이를 기반으로 효과적인 보안 대응 모델을 제안하였다. 중소기업의 보안 환경은 대기업에 비해 상대적으로 취약하며, 정보보호 인프라 및 전문 인력 부족으로 인해 보안 위협에 쉽게 노출될 수 있다. 이에 본 연구는 관리적 보안, 기술적 보안, 물리적 보안, 인적 보안의 4대 보안 영역을 중심으로 예방(Security Prevention), 탐지(Security Detection), 대응(Security Response), 개선(Security Enhancement)의 단계별 보안 대응 모델을 설계하였다. 연구 결과, 중소기업의 주요 보안 취약점으로 보안 정책 부재, 계정 및 접근 통제 미흡, 네트워크 및 애플리케이션 보안 취약점, 물리적 보안 미비, 직원 보안 인식 부족 등이 확인되었다. 이러한 문제를 해결하기 위해 ISMS-P 기반의 정보보호 정책 수립, 다중 인증 및 접근통제 강화, 네트워크 및 애플리케이션 보안 솔루션 도입, 출입 통제 시스템 구축, 정기적인 보안 교육 및 내부 보안 점검 등의 대응 방안을 제시하였다. 본 연구에서 제안한 보안 대응 모델을 적용함으로써 중소기업은 체계적인 보안 체계를 구축하고, 보안 리스크를 최소화하며, 사이버 공격 및 침해사고에 대한 대응력을 높일 수 있을 것으로 기대된다. 특히, 본 모델은 중소기업의 환경과 예산을 고려하여 비용 효율적인 보안 강화 전략을 포함하고 있어, 현실적인 보안 대응 체계를 구축하는 데 유용할 것으로 판단된다. 향후 연구에서는 본 연구에서 제안한 보안 대응 모델의 실효성을 검증하기 위한 실증 연구 및 기업별 맞춤형 보안 전략 개발이 필요할 것이다. 또한, 최신 보안 위협에 대응할 수 있도록 AI 기반 보안 자동화, 클라우드 보안 강화, IoT 보안 모델 적용 등의 연구가 추가적으로 이루어져야 한다. 이를 통해 중소기업의 보안 역량을 지속적으로 향상시키고, 기업이 스스로 보안 체계를 관리하고 발전시킬 수 있도록 지원해야 한다.

REFERENCES

[1] A.Smith and B.Johnson, "A risk-based security consulting model for SMEs," International Journal of Information Security, Vol.22, No.3, pp.215-230, 2020.

[2] C.Wang and D.Brown, "Cybersecurity frameworks for small and medium-sized enterprises: A comparative analysis of ISO 27001 and NIST," Journal of Information Security Research, Vol.18, No.2, pp.123-137, 2019.

[3] S.Choi, "Design of an effective security consulting framework for SMEs," Journal of Information and Security Research, Vol.9, No.2, pp.78-95, 2020.

[4] B.Kim, "Cloud security risks and mitigation strategies for small enterprises," Journal of Cloud Computing Research, Vol.11, No.2, pp.45-63, 2020.

[5] H.Takahashi, "Implementing a layered security approach for SMEs: Challenges and best practices," Journal of Information Systems Security, Vol.17, No.1, pp.112-129, 2019.

[6] T.Evans and R.Carter, "Developing a cost-effective cybersecurity strategy for SMEs," Small Business Cybersecurity Review, Vol.8, No.3, pp.67-82, 2021.

[7] D.Kim and M.Lee, "Implementing ISO/IEC 27001 in small businesses: Lessons learned," Journal of Information Security Compliance, Vol.7, No.4, pp.178-195, 2019.

[8] K.Ahmed and F.Hassan, "Cyber risk assessment frameworks for small enterprises," Risk Management & Cybersecurity Review, Vol.8, No.2, pp. 130-150, 2022.

[9] M.Thompson, "Assessing vulnerabilities in IoT-based business environments," IEEE Internet of Things Journal, Vol.6, No.5, pp.1034-1047, 2019.

[10] P.Garcia, "Application of OWASP Top 10 and CVSS methodologies for SME security assessments," Journal of Network Security, Vol.14, No.4, pp.310-324, 2018.

[11] J.H.Lee, "Security threats and response methods in the Internet of Things (IoT) environment," Journal of the Korea Institute of Information Security and Cryptology, Vol.27, No.4, pp.697-706, 2017.

[12] L.Kim and T.Nguyen, "Mitigating cyber threats through AI-based anomaly detection in IoT networks," ACM Transactions on Cyber-Physical Systems, Vol.7, No.3, pp.205-222, 2022.

[13] R.White, "Incident response and forensic investigation methodologies for SME cybersecurity," Computers & Security, Vol.92, pp.123-138, 2021.

[14] K.Tanaka and J.Park, "Threat intelligence sharing frameworks for SMEs: A systematic review," Cybersecurity Journal, Vol.10, No.1, pp.56-78, 2021.

[15] S.H.Park and M.J.Yoo, "A study on Zero Trust security and micro-segmentation in enterprise networks," Journal of Network and Security Studies, Vol.13, No.2, pp.78-95, 2020.

[16] R.Singh and A.Verma, "AI-driven security analytics for detecting advanced cyber threats," IEEE Transactions on Information Forensics and Security, Vol.15, No.7, pp.1098-1114, 2020.

[17] Y.Nakamura, "Security challenges and best practices in IoT-driven smart manufacturing," International Journal of Industrial IoT Security, Vol.5, No.2, pp.87-102, 2021.

[18] K.Patel and S.Sharma, "A study on Zero Trust security

models in modern enterprise environments," Journal of Cyber Security and Privacy, Vol.5, No.1, pp.89-102, 2021.

[19] D.Martinez, "Evaluating endpoint security solutions for small businesses," International Journal of Cybersecurity, Vol.15, No.4, pp.220-234, 2022.

이 근 호(Keun Ho Lee) [종신회원]

■ 2006년 8월 : 고려대학교 컴퓨터학과(이학박사)
■ 2006년 9월 ~ 2010년 2월 : 삼성전자 DMC연구소 책임연구원
■ 2010년 3월 ~ 현재 : 백석대학교 컴퓨터공학부 교수

〈관심분야〉
침해사고대응, 융합보안, 개인정보보호, 블록체인, 산업보안, 모의해킹 등