

원저

방산업체 보안취약점 관리를 위한 공격단계 기반 통합 대응체계 연구

박승수

LIG Defense&Aerospace 정보보호팀장

교신저자: 박승수 (seoungsoo.park@ligdna.com)

요약

방산업체는 국가안보와 직결된 핵심 기술을 보유하고 있으며, 국가 배후 해킹조직의 지속적인 공격 대상이 되고 있다. 최근 공격은 애플리케이션 취약점, 탈취 계정, 외부 노출자산 및 소프트웨어 공급망을 복합적으로 이용하여 정기진단과 개별 취약점 중심 관리만으로는 실제 공격경로에 효과적으로 대응하기 어렵다. 본 연구는 국내외 위협 동향과 공개된 주요 공격사례를 공통항목으로 분석하고, 사이버 킬체인과 MITRE ATT&CK를 종합하여 공격의 단계적 흐름과 지속적 접근유지 활동을 포괄하는 6단계 공격구조를 구성하였다. 이어 모의해킹 기반 공격경로와 진단 제도를 분석하여 관리체계의 구조적 한계를 도출하였다. 이를 바탕으로 6단계 공격구조를 방어자 관점에서 재구성하여, 정찰 및 외부 노출 식별, 초기침투 예방, 권한확대 및 내부이동 차단, 핵심자산 보호, 지속적 점검 및 개선의 5개 대응영역으로 구성된 통합 대응체계를 제안하였다. 또한 방산업체의 인력·예산·기술역량을 고려하여 단계적으로 도입할 수 있도록 기반 구축, 운영 확대, 연계 운영 및 능동방어의 4단계 적용방안을 제시하였다.

핵심어

방산업체, 보안취약점 관리, 통합 대응체계, 공격단계, 공격표면관리, 모의해킹

차례

1. 서론
2. 사이버 위협 및 주요 공격 사례
3. 사이버 공격단계 및 공격경로 분석
4. 방산업체 보안취약점 관리체계 분석
5. 방산업체 보안취약점 통합 대응체계
6. 결론

Open Access

접수일: 2026년 8월 18일
수정일: 2026년 9월 07일
게재승인일: 2026년 9월 16일
출판일: 2026년 9월 30일

Copyright © 2026 Author(s).

This is an Open Access article distributed under the terms of the Creative Commons CC BY 4.0 license (<https://creativecommons.org/licenses/by/4.0/>) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Original Article

A Study on an Attack-Stage-Based Integrated Response Framework for Security Vulnerability Management in Defense Companies

Seoungsoo Park

Information Security Team Manager, LIG Defense&Aerospace, Republic of Korea

Corresponding Author: Seoungsoo Park (seoungsoo.park@ligdna.com)

ABSTRACT

Defense companies possess critical technologies directly linked to national security and remain persistent targets of state-sponsored hacking groups. Recent attacks combine application vulnerabilities, compromised accounts, externally exposed assets, and software supply chains. Consequently, conventional vulnerability management centered on periodic assessments and individual vulnerabilities cannot effectively address actual attack paths. This study analyzes domestic and international threat trends and major cyber incidents and integrates the Cyber Kill Chain and MITRE ATT&CK to construct a six-stage attack structure. The structure is then reorganized from a defender's perspective to propose an integrated response framework comprising five areas: reconnaissance and external exposure identification, initial access prevention, privilege escalation and lateral movement prevention, critical asset protection, and continuous assessment and improvement. In addition, a four-stage implementation approach—foundation building, operational expansion, integrated operation, and active defense—is presented to enable gradual adoption according to each organization's resources, capabilities, and operational conditions.

KEYWORDS

Defense Companies, Security Vulnerability Management, Integrated Response Framework, Attack Stages, Attack Surface Management, Penetration Testing

1. 서론

국가 안보와 직결된 핵심 기술 및 정보를 보유한 방산업체는 국가 배후 해킹조직의 지속적인 표적이 되어 왔다. 실제로 2024년 초 진행된 경찰청·방위사업청·국가정보원 등 관계기관 합동 특별 점검을 통해, 라자루스, 안다리엘, 김수키 등으로 알려진 북한 해킹조직들이 국내 방산기술을 탈취하기 위해 전방위적으로 공격하고 있는 것을 확인하였다. 북한 해킹조직은 방산업체를 직접 침투하기도 하고, 상대적으로 보안이 취약한 방산 협력업체를 해킹하여 방산 업체의 서버 계정정보를 탈취한 후 주요 서버에 무단으로 침투해 악성코드를 유포한 것으로 파악되었다. 일부 피해 업체들은 당국의 연락을 받기 전까지도 해킹 피해 사실을 전혀 모르고 있었다.[1]

최근의 사이버공격은 하나의 취약점을 단독으로 이용하는 방식에서 벗어나 공개 애플리케이션의 취약점, 탈취된 계정정보, 인터넷 노출자산, 원격접속 경로 및 소프트웨어 공급망을 복합적으로 이용하는 형태로 발전하고 있다. 공격자는 외부에 노출된 자산을 식별한 후 취약점이나 계정정보를 이용하여 최초 침투하고, 권한상승과 내부이동을 거쳐 핵심정보에 접근한다. 또한 침투 이후에도 지속성을 확보하여 장기간 내부에 체류하면서 정보유출이나 시스템 파괴를 시도한다. SolarWinds, Log4Shell 및 MOVEit, Ivanti 사례는 각각 신뢰된 소프트웨어 배포체계, 광범위하게 사용되는 오픈소스 구성요소 및 인터넷 노출 시스템의 취약점이 대규모 공격의 진입점으로 이용될 수 있음을 보여준다.[2-5] 국내 침해사고에서도 장기간 미조치된 공개 취약점과 외부 노출 시스템이 초기 침투경로로 이용된 사례가 확인되고 있다.[6]

이러한 위협환경의 변화는 방산업체가 자체적으로 관리하는 정보시스템뿐만 아니라 외부 노출 자산, 개발환경 및 외부 연결접점 전반을 하나의 공격경로로 관리해야 할 필요성을 제기한다. 그러나 기존의 보안취약점 관리는 인프라 진단, 웹 애플리케이션 진단, 개발보안 점검 및 모의해킹 등이 각각의 대상과 시점에 따라 개별적으로 수행되는 경향이 있다. 또한 발견된 취약점의 심각도와 조치 여부를 중심으로 관리하기 때문에, 여러 취약점과 공격기법이 결합하여 형성하는 실제 공격 경로를 충분히 반영하기 어렵다. 정기진단 결과와 보안관계 정보, 개선조치 및 재점검 결과가 유기적으로 연계되지 않을 경우 취약점은 발견되더라도 해당 취약점이 공격과정에서 어떠한 역할을 하는지, 어떤 취약점과 공격경로를 우선 차단해야 하는지에 관한 의사결정이 제한될 수 있다.

이에 본 연구는 최신 사이버 위협과 주요 공격사례를 통해 방산업체를 대상으로 한 공격의 특성을 파악하고, 사이버 킬체인, MITRE ATT&CK 및 모의해킹 관점에서 공격단계와 공격경로를 분석한 후, 방산업체의 보안취약점 관리체계가 지닌 현황과 구조적 한계를 검토 및 종합하여 공격단계에 기반한 통합 대응체계와 조직 여건에 따른 단계적 적용방안을 제안한다. 연구방법으로는 국내외 학술문헌 및 정부·공공기관 발간자료에 대한 문헌연구와 사이버 킬체인 및 MITRE ATT&CK 프레임워크를 종합한 공격단계 분석, 그리고 공개된 모의해킹 방법론에 기반한 공격경로 분석을 활용하였다.

본 논문의 구성은 다음과 같다. 2장에서는 국내외의 사이버 위협 동향과 주요 공격 사례를 분석하여 최근 공격이 어떤 경로로 전개되는지를 확인한다. 3장에서는 이를 바탕으로 사이버 킬체인과 MITRE ATT&CK를 종합하여 6단계 공격구조를 설정하고, 공개된 모의해킹 방법론에 포함된 기술적 행위와 비교하여 해당 구조의 개념적 정합성을 검토한다. 4장에서는 이 분석기준을 적용하여 방산업체의 보안취약점 진단 제도 및 운영 현황을 검토하고 취약점 관리체계의 구조적 한계를 도출하며, 5장에서는 도출된 한계를 바탕으로 6단계 공격구조를 방어자 관점의 대응영역으로 재구성한 통합 대응체계와 조직 여건에 따른 단계적 적용방안을 제시한다. 6장에서는 연구 결과를 요약하고 한계 및 향후 연구방향을 논의한다.

2. 사이버 위협 및 주요 공격 사례

2.1. 국내외 사이버 위협 동향

국내 방산업체에 대한 사이버공격은 국가 배후 해킹조직을 중심으로 지속되고 있다. 경찰청·방위사업청·국가정보원의 합동조사 결과, 라자루스·안다리엘·김수키는 외부망 서버 취약점, 탈취 계정 및 망 연계 구간 등을 이용하여 국내 방산업체의 내부망에 침투하고 기술자료를 탈취한 것으로 확인되었다.[1] 이와 유사한 국가 배후 위협 양상은 중국 배후 APT 그룹에 대한 국내 연구에서도 확인된다. 중국 배후 APT 그룹을 MITRE ATT&CK으로 분석한 선행 연구에서는 주요 그룹이 초기 접근에 스피어피싱을 활용하였으며, 일부 그룹은 제로데이 취약점을 주요 기법으로 사용한 것으로 나타났다.[7]

이러한 국내외 보안 분야의 위협 양상은 글로벌 보안업체가 매년 발간하는 연간 위협 동향 보고서에서 제시하는 추세에서도 나타난다. IBM의 X-Force Threat Intelligence Index 2026에 따르면, 공개 애플리케이션에 대한 취약점 악용이 전년 대비 44% 증가하여 초기침투 경로의 40%를 차지함으로써, 그간 2년 연속 1위였던 자격증명 도용·오남용(32%)을 앞질렀다. 공개된 취약점의 56%는 별도의 인증 없이도 악용이 가능하였으며, 대규모 공급망·협력사 침해는 2020년 대비 약 4배 증가하였고, 활성 랜섬웨어·갈취조직 수는 전년 대비 49% 증가(109개, 전년 73개)하며 소규모·파편화된 형태로 재편되었다. 제조업은 5년 연속 최다 표적 산업(27.7%)이었으며 금융·보험업이 27%로 뒤를 이었다.[8] Palo Alto Networks Unit 42의 Global Incident Response Report 2026(2024년 10월~2025년 9월 기간 750건 이상의 주요 사고대응 사례 분석)은 초기침투의 65%가 신원(자격증명 탈취, MFA 우회, 계정관리 오설정 등) 기반으로 이루어졌으며, 신원 관련 취약점이 전체 조사 사건의 약 90%에서 실질적인 영향을 미쳤다고 밝혔다. 특히 공격 속도가 비약적으로 빨라져, 가장 빠른 상위 25% 침해사고의 경우 최초 침투부터 정보 유출까지 소요된 시간이 전년 285분에서 72분으로 단축되었다.[9] 이러한 해의 동향은 공통적으로 (1) 공개 애플리케이션 취약점 악용과 신원 오남용이 초기침투의 양대 경로로 부상하고 있다는 점, (2) 공급망·협력사를 경유한 공격이 지속적으로 확대되고 있다는 점을 보여준다.

국내 동향 역시 이러한 흐름에서 벗어나지 않는다. 한국인터넷진흥원(KISA)이 발표한 2025년 사이버 위협 동향 및 2026년 전망 보고서에 따르면, 국내 민간분야 침해사고 신고 건수는 2023년 1,277건에서 2024년 1,887건(전년 대비 약 48% 증가), 2025년 2,383건(전년 대비 약 26.3% 증가)으로 매년 증가하였다. 2025년 유형별 신고 통계에서는 서버해킹이 44.2%로 가장 높은 비중을 차지하였고, 디도스(DDoS) 공격이 588건으로 전년(285건) 대비 약 2배로 급증하였으며, 랜섬웨어 공격도 274건(비중 11.5%)으로 전년(195건) 대비 40.5% 증가하였다.[10] 국내 보안기업의 분석도 이러한 추세를 뒷받침한다. SK설터스가 최근 5년간의 중소·중견기업 대상 사이버 침해사고를 분석한 결과, 최초 침투부터 사고를 인지하기까지 평균 106.1일이 소요되었으며 전체 사고의 47.4%가 제조업에 집중된 것으로 나타났고, 보안인력과 인프라가 상대적으로 열악한 중소·중견기업이 공격에 특히 취약함을 보여주었다. SK설터스는 이러한 분석을 토대로 랜섬웨어 대응 전략의 축을 사고 발생 이후의 '지불' 중심에서 사전 예방적인 'ASM(공격표면관리)' 중심으로 전환할 필요성을 제시하였다.[11] 이는 본 연구가 5장에서 제안하는 통합 대응체계의 정찰 단계 대응방안(공격표면관리)과 방향을 같이한다. 안랩(AhnLab) ASEC이 발표한 2025년 사이버 위협 동향 및 2026년 전망 보고서에서도 오픈소스 생태계를 이용한 소프트웨어·하드웨어 전반의 공급망 공격 고도화 및 확대를 2026년의 주요 위협 전망으로 제시하였다.[12]

이상의 국내외 위협 동향 보고서들을 종합하면, 방산업체가 직면한 위협은 특정 국가·조직에 국한된 예외적 현상이 아니라 국내외 산업 전반에서 공통적으로 관측되는 구조적 추세의 연장선에

있음을 알 수 있다. 정리해 보면, (1) 공개 애플리케이션 및 자산의 취약점 악용이 초기 침투의 핵심 경로로 부상하고 있다는 점, (2) 자격증명과 취약점 악용을 결합하는 점, (3) 공급망 및 협력사를 경유한 우회 공격이 지속적으로 확대되고 있다는 점으로 정리할 수 있다.

2.2. 주요 사이버 공격 사례

2.1절에서 확인한 바와 같이 최근의 침해사고는 소프트웨어 공급망, 외부 노출 애플리케이션, 원격접속 장비 등 다양한 진입경로를 통해 발생하고 있다. 특히 공급망 공격은 정상적인 업데이트 및 배포체계, 오픈소스 구성요소, 외부 서비스 제공자 등 조직이 신뢰하는 경로를 악용한다는 점에서 전통적인 경계보안만으로 대응하기 어렵다. 본 절에서는 이러한 특성을 고려하여 신뢰된 배포 경로를 통한 유입, 오픈소스 구성요소의 식별 실패, 외부 노출 시스템의 제로데이 악용, 경계장비 취약점의 연쇄 악용, 그리고 국내 기업의 공개 취약점 장기 미조치 및 침투 이후 지속활동의 미탐지 사례를 검토한다. 본 절의 사례는 2020년부터 2026년까지 근래에 발생한 침해사고 중, 정부기관 또는 국제 사이버보안 기관의 공식 권고·보도자료로 확인 가능하고, 취약점 또는 계정정보가 초기 침투경로로 이용되었으며, 공격경로가 진입점부터 목표달성까지 공개된 사례 또는 취약점 관리 측면에서 핵심적인 공격과정이 공식자료를 통해 확인되는 사례로 한정하였다. 자료는 CISA 권고문, 방위사업청 등 정부기관 발표자료, KISA 및 국내의 보안기업의 연간 위협보고서, 국내 학술논문에서 수집하였다. 공격주체나 피해사실만 제시되고 공격경로가 구체적으로 공개되지 않은 사례, 침해 여부가 확정되지 않은 사례는 분석에서 제외하였다. 각 사례는 공격의 진입점, 내부 확산 또는 지속성 확보 방식, 그리고 취약점 관리 측면의 시사점을 중심으로 분석하며, 이는 다음 장에서 제시하는 공격단계별 분석 및 대응체계 설계의 사례적 근거로 활용한다.

표 1. 주요 사이버 공격사례 분석

사례	진입점	공격기법	이동경로	목표	지속성	관리상 시사점
SolarWinds	신뢰된 빌드·배포 체계	개발사 빌드환경 침해	공급사 → 고객망	정보 유출	악성코드로 접근유지	빌드 무결성·배포 검증
Log4Shell	인터넷 노출 Log4j 취약 애플리케이션	취약점 활용 (원격코드 실행)	외부 서비스 → 내부망	정보 유출	악성코드로 접근유지	SBOM 구성요소 가시성
MOVEit	인터넷 노출 파일전송 서버	취약점 활용 (SQL 인젝션)	외부 서비스 → 내부망	정보 유출	웹헬로 접근유지	패치 관리
Ivanti	SSL VPN 장비	취약점 활용 (인증우회 명령 주입)	VPN → 내부망	정보 유출	악성코드로 접근유지	패치 관리
A 방산업체	외부망 서버 망연계 포트	취약점 악용	망연계 → 내부망	정보 유출	악성코드로 접근유지	상시 진단·점검
롯데카드	인터넷 노출 웹서버	취약점 활용 (원격코드 실행)	웹서버 → 내부망	정보 유출	웹헬로 접근유지	패치 관리
SK텔레콤	외부 접점 관리망 서버	악성코드·계정 활용	외부망 서버 → 내부망	정보 유출	악성코드로 접근유지	상시 진단·점검

2.2.1. 공급망 및 외부 접점 공격사례

2.2.1.1. SolarWinds 공급망 침해

정상 소프트웨어 업데이트 과정에 악성코드가 삽입되어 다수 고객에게 배포된 사례로, 신뢰된 빌드·배포 체계가 공격경로가 될 수 있음을 보여주었다. 공격자는 전자서명된 정상 업데이트 파일에

약 4천 줄의 백도어 코드를 삽입하여 개발사의 배포 공급망을 통해 다수 고객사에 악성코드를 유포하였고, 코드를 경량화 및 난독화하였으며 특정 조건에서만 동작하도록 설계되어 개발사의 품질 점검 과정에서 장기간 탐지되지 않았다.[2] 이 사례의 핵심은 개별 고객이 경계취약점을 방어하더라도 공급자의 빌드 무결성과 업데이트 검증이 실패하면 신뢰경로를 통해 악성코드가 유입될 수 있다는 점이다.

2.2.1.2. Log4Shell(CVE-2021-44228) 취약점 확산

Log4Shell은 널리 사용되는 Apache Log4j 2 라이브러리의 JNDI 처리 취약점으로, 공격자가 조작한 로그 메시지 또는 매개변수를 통해 원격 코드를 실행할 수 있었던 사례이다. 해당 취약점은 다양한 기업용 서비스, 웹 애플리케이션 및 다양한 운영 제품에 사용된 오픈소스 구성요소에 영향을 미쳐 전 세계 조직의 긴급 대응을 촉발하였다.[3] 이 사례의 핵심 문제는 취약점 자체뿐 아니라 조직이 자사 제품·서비스 가운데 Log4j 구성요소를 포함한 대상을 신속히 식별하기 어려웠다는 데 있다. 따라서 소프트웨어 자산목록과 SBOM을 통해 구성요소, 버전 및 의존관계를 관리하고, 취약점 공지 이후 영향범위를 신속히 확인하는 체계가 필요하다.

2.2.1.3. MOVEit Transfer 취약점 이용

인터넷에 노출된 파일전송 시스템의 제로데이가 대규모 데이터 탈취로 이어질 수 있음을 보여주었다. 파일전송 제품은 외부기관 및 협력사와의 자료교환 과정에서 민감정보를 처리하며, 내부와 외부의 보안영역을 연결하는 특성으로 인해 주요 보안위협에 노출될 수 있다. 취약점 공지 이후 패치만 적용하더라도 이미 생성된 웹셸, 비정상 계정, 유출 흔적을 제거하지 않으면 침해가 지속될 수 있다. 따라서 패치와 침해지표 탐지, 포렌식 확인, 비밀정보 교체를 동시에 수행해야 한다.[4]

2.2.1.4. Ivanti Connect Secure 계열 취약점 악용

SSL VPN 장비의 취약점이 인증우회, 명령실행, 지속성 확보와 결합되는 전형을 보여준다. 미국 사이버보안·인프라보안국(CISA)은 인증우회(CVE-2023-46805)와 명령주입(CVE-2024-21887) 취약점이 연쇄적으로 악용되어 원격 명령실행이 가능하다고 경고하면서 긴급지침(ED 24-01)을 발령하였으며, 최신 펌웨어로 업데이트 및 해당사에서 제공하는 패치를 적용해야 한다.[5]

2.2.2. 국내 주요 공격사례

2.2.2.1. 방산업체 대상 공격

외부망 서버 침해를 통한 내부망 자료 유출 사례를 보여준다. 라자루스는 2022년 11월경 국내 한 방산업체의 외부망 서버를 해킹하여 악성코드에 감염시킨 후, 시험 목적으로 개방되어 있던 망 연계시스템의 포트를 통해 내부망에 침투하였다. 이후 개발팀 직원의 컴퓨터를 비롯한 내부망 단말에서 중요자료를 수집하고 이를 국외 클라우드 서버로 유출하였다. 수사기관은 내부망 컴퓨터 6대에서 자료가 유출된 사실과 국외 클라우드 서버에 남은 유출 흔적을 확인하였다.[1] 이 사례는 물리적·논리적 망 분리가 적용되어 있더라도 망 연계 구간의 불필요한 포트, 접근권한 및 운영상태가 적절하게 관리되지 않으면 외부망 침해가 내부 개발환경과 중요자료 유출로 이어질 수 있음을 보여준다.

2.2.2.2. 2025년 롯데카드 침해사고

취약점 패치 지연이 대규모 정보유출로 직결된 전형을 보여준다. 공격은 2017년에 이미 알려진 오라클 웹로직 서버의 원격코드 실행 취약점(CVE-2017-10271)을 이용하여 서버 관리자 권한을 취득해 웹셸 프로그램을 설치하는 방식으로 이루어졌다.[13] 조사 결과 이번 해킹으로 온라인 결제 서버의 자료 약 200GB가 외부로 유출된 것으로 나타났다.[6] 공개된 지 8년이 지난 취약점이 인터넷에 노출된 웹 애플리케이션 서버에 그대로 남아 있었다는 점에서, 이 사건은 취약점 자체의 난이도보다 자산 식별과 패치 거버넌스의 실패가 근본 원인이었다고 평가된다.

2.2.2.3. SK텔레콤 유심정보 유출사고

장기간 탐지되지 않은 침해의 위험성을 보여준다. 공격자는 가입자 인증을 처리하는 핵심 서버에 BPFDoor 계열의 백도어 악성코드를 설치하여 가입자식별키(IMSI) 등 유심 복제에 활용될 수 있는 정보를 유출하였으며, 민관합동조사단 조사 과정에서 다수의 악성코드가 추가로 발견되었다.[14] 이 사고는 침투 자체보다 장기간 탐지되지 않은 지속성 확보와 상시 모니터링의 공백이 피해 규모를 결정한다는 점을 시사한다.

이상의 사례는 최근 사이버공격이 외부 노출자산, 취약점, 탈취된 계정정보 및 소프트웨어 공급망을 복합적으로 이용하여, 외부 노출자산 탐색부터 초기침투, 권한상승과 내부이동, 목표달성 및 지속성 확보로 이어지는 공격경로로 전개됨을 보여준다. 따라서 개별 취약점의 식별과 조치뿐만 아니라 여러 취약점과 공격기법의 결합으로 형성되는 전체 공격경로를 분석할 필요가 있다. 다음 장에서는 사이버 킬체인과 MITRE ATT&CK을 종합하여 공격의 단계별 흐름과 주요 공격기법을 정리하고, 공개된 모의해킹 방법론의 기술적 공격행위와 비교하여 외부 노출자산에서 내부 핵심자산까지 이어지는 공격경로를 분석한다.

3. 사이버 공격단계 및 공격경로 분석

3.1. 사이버 공격단계와 주요 공격기법

사이버공격은 서버, 네트워크, 애플리케이션 및 소프트웨어의 설계·구현·운영 과정에서 발생한 취약점이나 탈취된 계정정보 등을 이용하여 비인가 접근과 권한 획득을 시도하고, 자료유출·파괴 또는 시스템 장애를 유발하는 방식으로 이루어진다. 이러한 공격은 일반적으로 하나의 행위만으로 완결되지 않고, 경찰에서 초기침투, 권한상승과 내부이동을 거쳐 목표달성에 이르는 복수의 공격 활동이 연계되어 전개된다. 다만 실제 공격에서는 일부 활동이 생략되거나 반복·병행될 수 있으며, 이를 설명하는 프레임워크마다 공격과정을 구분하는 기준과 세분화 수준에는 차이가 있다.

3.1.1. Cyber Kill Chain

Lockheed Martin이 제시한 사이버 킬체인(Cyber Kill Chain)은 정찰(Reconnaissance) → 무기화(Weaponization) → 전달(Delivery) → 취약점 공격(Exploitation) → 설치(Installation) → 명령제어(Command & Control) → 목표실행(Actions on Objectives)의 7단계로 공격의 진행 과정을 설명하는 초기의 대표적 모델이다. 이 모델은 공격이 순차적인 단계를 거쳐 진행되며, 방어자가 이 중 어느 한 단계에서라도 공격 사슬을 차단하면 전체 공격을 무력화할 수 있다는 착안에 기반한다. 다만 킬체인은 공격의 전체적인 흐름을 이해하는 데는 유용하나, 각 단계

에서 실제로 사용되는 세부 기법까지는 다루지 않는다는 한계가 있다.[15]

3.1.2. MITRE ATT&CK Framework

미국의 비영리기관인 MITRE Corporation이 개발한 MITRE ATT&CK Framework는 실제 공격사례에서 관찰된 공격자의 전술·기법·절차(Tactics, Techniques, and Procedures: TTP)를 체계적으로 분류한 지식베이스로, 보안전문가들이 위협을 탐지하고 방어전략을 수립하도록 지원한다.[16] 사이버 킬체인이 공격의 전반적인 진행과정을 순차적으로 설명하는 데 중점을 두는 반면, MITRE ATT&CK은 정찰(Reconnaissance), 초기접근(Initial Access), 실행(Execution), 권한상승(Privilege Escalation), 방어회피(Defense Evasion), 탐색(Discovery), 횡적이동(Lateral Movement), 수집(Collection), 유출(Exfiltration) 및 영향(Impact) 등의 전술과 그 하위 기술을 구체화하여 공격행위 분석과 탐지·대응 방안 수립에 활용된다.[17]

이와 관련한 선행연구들을 보면, 위협 모델링은 시스템에 가해질 수 있는 잠재적 위협을 체계적으로 식별·분석·평가하는 구조화된 활동으로, MITRE ATT&CK은 이러한 위협 모델링에 강력한 도구가 된다. 이와 관련하여 김도훈(2023)은 MITRE ATT&CK을 NIST SP 800-53 통제항목과 연계하여 공격 트리(Attack Tree)와 방어 트리(Defense Tree)를 구성하는 방법론을 제시한 바 있다.[18] 아울러 신강식, 조호목(2025)은 MITRE ATT&CK을 D3FEND 프레임워크와 연계하여 실제 공격 로그 분석을 통해 효과적인 정보보호 솔루션을 도출하는 방법론도 제시하였다.[16] 이러한 두 모델의 상대적 유용성은 실제 APT 공격 사례 분석을 통해서도 확인된 바 있다. 윤영인 등(2020)은 차밍키튼, 폰스툼, 씨엠스타, 블랙오아시스 등 해외 APT 공격 4건을 사이버 킬체인 모델과 TTP(MITRE ATT&CK) 모델로 각각 분석하여, 킬체인 모델은 공격의 전체적인 윤곽을 파악하는 데는 효과적이거나 실제 사례에서는 7단계가 모두 명확히 구분되지 않는 경우가 많아 구체적인 방어 전략 수립에는 한계가 있는 반면, TTP 모델은 공격 기법(Technique)별로 탐지·대응 방안을 구체화할 수 있어 심층방어(defense-in-depth) 체계 구축에 더 적합하다고 제시하였다.[19] 이는 본 연구가 킬체인의 순차적 구조와 ATT&CK의 세부 전술을 함께 활용하되, 실제 방어방안 도출 및 방어계층 설계는 ATT&CK 기반 기법 단위로 구체화하는 근거가 된다. 이처럼 두 프레임워크는 서로 다른 강점을 지닌다. 사이버 킬체인은 공격의 순차적 흐름을 이해하는 데 효과적이고, MITRE ATT&CK은 각 단계에서 사용되는 구체적인 기술(Technique)을 식별하는 데 강점을 지닌다. 본 연구는 이 두 관점, 즉 공격 진행 순서(킬체인)와 세부 전술 분류(ATT&CK)를 종합하여 ① 정찰, ② 초기침투, ③ 실행 및 권한상승, ④ 내부정찰 및 횡적이동, ⑤ 목표달성(유출·파괴), ⑥ 지속성 확보의 6단계로 재구성하였다. 본 연구에서 사이버 킬체인과 MITRE ATT&CK을 종합하여 재구성한 6단계는 주요 공격사례의 공격경로를 일관되게 분석하고, 단계별 보안취약점 대응방안을 도출하기 위한 분석틀이 된다. 실제 공격에서는 공격대상과 목적에 따라 일부 단계가 생략되거나 반복·병행될 수 있으며, 공급망 공격과 같이 신뢰된 경로를 이용한 침투 역시 여러 공격단계에 걸쳐 복합적으로 전개될 수 있다.

본 연구는 MITRE ATT&CK Matrix for Enterprise v18.1을 적용하였다. 14개 전술을 모두 반영하여, Reconnaissance와 Resource Development는 공격자가 표적 환경에 접촉하기 이전에 수행하는 준비활동이므로 ① 정찰로 통합하였다. Initial Access는 표적 환경에 최초 접근하는 활동이므로 ② 초기침투에, 침투 후 악성 명령이나 코드를 실행하는 활동인 Execution과 Privilege Escalation, Defense Evasion, Credential Access는 시스템 내부에서 권한을 확보·유지하는 활동으로 ③에, Discovery, Lateral Movement, Command and Control은 내부 확산 활동으로 ④에 배치하였다. Collection, Exfiltration, Impact는 공격 목적의 실현에 해당하므로 ⑤로 통합하였다. 한편 Persistence는 ATT&CK Matrix에서 Execution 다음에 위치하며

침투 직후부터 수행될 수 있는 활동으로 분류된다. 그럼에도 본 연구에서는 이를 별도의 분석영역인 ⑥으로 구분하였다. 그 이유는 다음과 같다. 지속성 확보는 특정 시점에 한 번 수행되고 종료되는 활동이 아니라, 초기침투 이후 권한상승, 내부이동, 목표달성 과정 전반에서 접근권한과 공격거점을 유지하기 위해 반복·병행되는 횡단적 활동이다. 이에 따라 지속성 확보를 ⑥으로 구분한 것은 발생 순서를 의미하는 것이 아니라, 특정단계에 종속시키지 않고 초기침투부터 목표달성에 이르는 전과정에 걸쳐 별도로 점검·대응해야 할 대상으로 관리하기 위한 것이다. 따라서 본 연구의 6단계 공격 구조는 엄격한 시간적 공격순서가 아닌 공격목적과 관리상 대응지점에 따른 분석영역이며, 실제 공격에서는 각 단계가 중첩되거나 반복될 수 있다.

표 2. 본 연구의 6단계와 Cyber Kill Chain 및 MITRE ATT&CK 매핑

본 연구의 단계	Cyber Kill Chain	MITRE ATT&CK
① 정찰	Reconnaissance, Weaponization	Reconnaissance, Resource Development
② 초기침투	Delivery, Exploitation	Initial Access
③ 실행·권한 상승	Installation	Execution, Privilege Escalation, Credential Access, Defense Evasion
④ 내부정찰·횡적이동	Command and Control	Discovery, Lateral Movement, Command and Control
⑤ 목표달성	Actions on Objectives	Collection, Exfiltration, Impact
⑥ 지속성 확보	Installation, C2 및 재침투 활동	Persistence, C2 및 Defense Evasion 일부

3.2. 모의해킹 관점의 공격경로 분석

취약점 진단은 알려진 취약점과 설정 오류를 폭넓게 식별하는 데 적합하지만, 개별 발견사항이 실제 공격목표까지 연결되는지를 항상 증명하지는 않는다. 모의해킹은 허가된 범위에서 공격자의 관점으로 취약점을 결합하여 침투 가능성과 업무 영향을 제한적으로 검증한다. 본 절에서는 국제 표준과 국내 실무에서 정립된 모의해킹 수행절차를 살펴보고, 3.1절에서 분석한 공격단계가 방어자 관점의 검증 활동에서도 동일하게 나타나는지를 확인한다.

3.2.1. NIST SP 800-115

미국 국립표준기술연구소(NIST)의 SP 800-115(Technical Guide to Information Security Testing and Assessment)는 정보보안 시험·평가에 관한 대표적인 기술지침으로, 모의해킹을 계획(Planning) → 탐색(Discovery) → 공격(Attack) → 보고(Reporting)의 4단계로 구성한다. 계획 단계에서는 시험의 목적, 범위, 법적·행정적 승인 사항을 정의하며, 탐색 단계에서는 정보수집·스캐닝과 취약점 분석을 함께 수행한다. 공격단계에서는 발견된 취약점을 실제로 악용하여 접근권한 획득, 권한상승, 횡적이동 등을 시도하며, 이 과정에서 새로운 시스템이 발견되면 다시 탐색 단계로 순환하는 반복적 구조를 지닌다. 보고 단계에서는 발견된 취약점과 공격경로, 위험도, 개선권고사항을 정리한 보고서를 작성한다.[20]

3.2.2. PTES

PTES(Penetration Testing Execution Standard)는 업계 실무자들이 공동으로 개발한 모의해킹 실행 표준으로, 사전 협의(Pre-engagement) → 정보 수집(Intelligence Gathering) → 위

협 모델링(Threat Modeling) → 취약점 분석(Vulnerability Analysis) → 취약점 이용 공격(Exploitation) → 침투 후 활동(Post-Exploitation) → 보고(Reporting)의 7단계로 구성된다. 사전 협의에서는 시험의 목적과 범위, 수행규칙 및 승인사항을 정의하고, 정보 수집과 위협 모델링을 통해 공격대상과 예상 공격경로를 분석한다. 이후 취약점 분석 및 이를 통해 실제 침투 가능성을 확인하며, 침투 후 활동에서는 손상된 자산의 가치와 영향 범위, 추가 접근 및 접근권한 유지 가능성 등을 평가한다.[21]

3.2.3. 전문업체 모의해킹

모의해킹은 실제 공격자와 유사한 방식으로 침투를 시도하여 취약점이 실제 공격으로 이어질 가능성을 확인하는 데 목적이 있다. 이는 단순히 취약점을 식별하는 것을 넘어 공격경로와 침투 가능성, 예상되는 영향까지 함께 확인한다는 점에서 기존의 취약점 점검과 차별화된다. 국내 대표 보안 컨설팅업체들의 모의해킹 방법론을 보면, 예컨대 SK실터스의 IPTM(Infosec Penetration Test Methodology)과 안랩의 APTM(AhnLab Penetration Test Methodology)은 세부 절차와 점검범위에는 차이가 있으나, 공개자료를 종합하면 대상 범위 설정, 대상 정보 수집, 취약점 분석, 시나리오 기반 공격 시도, 결과 및 영향 분석, 대응방안 도출과 결과보고로 이어지는 공통적인 수행 흐름을 확인할 수 있다.[22,23] 이는 모의해킹이 개별 취약점의 존재 여부만을 확인하는 활동이 아니라, 여러 취약점과 공격기법이 실제 침투경로로 연결될 가능성과 보안통제의 실효성을 공격자 관점에서 점검하는 활동임을 보여준다.

3.2.4. 공격 시나리오 분석

모의해킹은 사이버 공격과 유사한 절차로 공격대상에 대한 정보수집 후 초기 침투경로 탐색 → 취약점·계정 악용 → 권한상승 → 내부이동 → 핵심시스템에 접근하여 자료 탈취 가능성 확인을 진행한다. 대표적으로 홈페이지나 업무포털 등 외부 웹서비스를 통한 내부 침투, 외부에 노출된 임직원 이메일 및 계정 정보를 통한 외부 인증시스템 접근을 통한 내부 침투, 악성메일 기반 첨부파일 실행을 통한 내부 침투 등 다양한 공격 시나리오를 통해 공격을 시도한다. 가장 일반적인 외부 웹서비스를 통한 내부 침투 시나리오를 보면, 정보수집(공개 도메인과 IP, 서비스 포트 등 수집) 및 외부 노출자산 식별, 인증 우회 및 파일 업로드 등의 취약점 확인, 여러 취약점을 연계하여 웹서버 또는 애플리케이션 권한 획득, 서버 내부 설정파일에서 DB계정이나 연계시스템 정보 확인 후 다른 서버로 이동, DB 또는 기술자료 관리시스템에 접근하여 자료 탈취 가능성 확인 순으로 진행한다.

이상을 종합하면, NIST SP 800-115, PTES 및 국내 전문업체의 공개 모의해킹 방법론에는 정보수집, 취약점 식별·이용, 권한획득, 내부이동, 핵심자산 접근 등 본 연구의 6단계 공격구조와 연계되는 주요 기술적 행위가 공통적으로 포함되어 있다. 다만 이러한 방법론은 계획·승인·보고를 포함하는 보안평가수행절차이므로, 본 연구에서는 공격경로 분석과 관련된 기술적 행위만을 추출하여 6단계 공격구조와의 개념적 정합성을 확인하였다. 실제 사이버공격이 공격자의 목적과 상황에 따라 단계가 생략·반복·병행되는 비인가 행위인 데 비해, 모의해킹은 사전에 승인된 범위와 수행규칙에 따라 공격기법과 경로를 제한적으로 재현하고 그 결과를 개선조치에 활용하는 보안평가 활동이라는 점에서 차이가 있다. 그럼에도 모의해킹은 개별 취약점이 실제 침투와 권한상승, 내부이동 및 핵심자산 접근으로 이어질 가능성을 단계별로 점검하는 수단이 된다. 이에 따라 본 연구의 6단계 공격구조는 공격자의 행위를 분석하는 틀이자 방어자의 대응 상태를 점검하기 위한 기준으로 활용될 수 있다. 다만 본 연구는 실제 방산업체의 모의해킹 결과를 실증적으로 분석한 것이 아니라, 공개된 모의해킹 방법론과 대표적인 공격 시나리오를 바탕으로 공격경로 분석틀을 개념적으로

구성하였다는 한계가 있다. 그럼에도 불구하고 이러한 분석은 개별 취약점의 기술적 심각도와 조치 여부만을 관리하기보다, 복수의 취약점과 공격기법이 결합하여 외부 노출자산에서 내부 핵심자산까지 이어지는 공격경로를 중심으로 보안취약점을 관리할 필요가 있음을 보여준다. 다음 장에서는 이러한 분석기준을 바탕으로 현행 방산업체의 보안취약점 진단제도와 운영 현황을 분석하고, 공격단계별 대응 관점에서 보안취약점 관리체계의 구조적 한계를 도출한다.

4. 방산업체 보안취약점 관리체계 분석

4.1. 보안취약점 진단 제도 및 운영 현황

방위사업청은 방산업체의 보안취약점 점검을 지원하기 위해 2021년부터 현재까지 사이버 보안 취약점 진단사업을 통해 연 1회 취약점 점검을 지원하고 있다. 사업에 선정된 보안컨설팅 전문업체는 방산업체와 협력업체를 대상으로 취약점 진단 및 모의해킹, 해킹메일 대응훈련을 실시하고 있다. 2026년 사업은 대상 기업을 105개사로 확대하는 한편, 외부 공격에 대한 직접적인 대응 능력 강화를 위해 모의해킹의 비중을 한층 강화하고, 점검 범위를 초기 침투 가능 경로 분석과 시스템 기능별 취약점 분석까지 확장하였으며, 이를 위한 점검 인력도 증원하였다.[24] 이러한 변화는 진단사업의 무게중심이 정적인 취약점 진단에서 실제 공격경로를 재현하는 모의해킹 중심으로 이동하고 있음을 보여준다.

이러한 진단사업의 필요성은 방위산업 분야의 실제 침해사고 통계에서도 확인된다. 방위사업청이 국회에 제출한 자료에 따르면, 2020년부터 2024년 8월까지 방위산업기술 유출·침해사고 신고센터에 접수된 신고는 총 82건이었으며, 이 가운데 37건은 실제 기술 유출로 이어졌고 그중 29건이 사이버 해킹에 의한 것으로 확인되었다. 특히 2024년의 경우 8월까지만 19건이 신고되어 5년 이래 최대치를 기록하였는데, 이는 방산 분야를 겨냥한 사이버 공격 시도가 지속적으로 증가하고 있음을 보여준다.[25]

현재 방산업체 대상 취약점 진단 및 모의해킹 수행은 인터넷망에 위치한 대외 서비스 및 관련 서버군을 주요 점검대상으로 하고 있다. 즉, 인터넷 서버, 보안장비, 네트워크 장비, 해킹메일 대응훈련, 시나리오 기반 모의해킹 등은 제도적으로 비교적 명확히 자리를 잡고 있으나, 외부 공격표면관리(ASM), 오픈소스 구성요소 관리, SBOM 기반 공급망 가시성 확보, DevSecOps 기반 개발단계 취약점 제거 등은 현재 사업 범위에 포함되어 있지 않으며, 일부 방산업체가 자체 투자와 운영 역량에 따라 개별적으로 수행하는 수준에 머물러 있다. 따라서 현행 진단 제도와 운영은 방산업체의 기본적인 보안수준을 향상하는 데 실질적으로 기여하고 있으나, 실제 공격자의 침투단계와 개발·운영 전 주기를 포괄하는 상시적이고 통합적인 취약점 관리체계로 발전하기 위해서는 많은 보완이 필요하다.

그리고 2023년 정부합동 방산기술보호 통합실태조사 결과는 방산 생태계 내부의 보안수준 격차를 실증적으로 드러냈다. 방산 대기업의 기술보호 수준은 80.5점이었던 반면, 중소기업은 72.5점, 일반 협력업체는 59.7점에 그쳐 기업 규모에 따라 뚜렷한 편차가 확인되었다.[25] 이는 방산업체가 자체적으로 일정 수준의 보안체계를 갖추고 있더라도, 이를 뒷받침하는 취약점 관리 역량은 조직의 규모와 투자 여력에 따라 크게 달라질 수 있음을 시사하고 있다.

운영 측면에서 국내 취약점 진단은 한국인터넷진흥원(KISA)의 주요정보통신기반시설 기술적 취약점 분석·평가 가이드를 대표적으로 참고하여 기술적 취약점 분석·평가를 수행하고 있다. 해당 가이드는 서버, 보안장비, 네트워크 장비, 단말, 애플리케이션 등 자산 유형별 점검항목을 제시하고, 계정관리, 접근권한, 서비스 관리, 패치관리, 로그관리 등 세부 점검영역을 체계화하고 있

다.[26]

대형 방산업체는 자체 예산을 투자하여 전문업체를 통한 정기적인 취약점 진단 및 모의해킹을 수행하거나 자체 전문 진단 인력을 보유하고 있으나, 중견업체 및 중소·협력업체들은 방위사업청 보안취약점 진단사업에 의존하고 있는 실정으로, 기업 규모와 투자 여건에 따라 자체 진단 역량 및 외부 지원사업 활용 수준에 차이가 있을 것으로 판단된다.

4.2. 보안취약점 관리체계의 구조적 한계

본 절에서 제시하는 구조적 한계는 개별 방산업체의 운영실태를 실증적으로 평가한 결과가 아니라, 공개된 제도자료와 선행연구를 바탕으로 제2·3장의 최신 보안위협 및 공격경로 분석과 제4.1 절의 제도·운영 현황을 종합하여 현행 관리체계에서 보완이 필요한 영역을 도출한 것이다.

첫째, 공격경로 분석에서 확인된 정찰 활동에 대응하기 위한 외부 공격표면관리가 미흡하다. 공격자는 본격적인 침투에 앞서 외부에 노출된 서버, 도메인, 원격접속 지점, 계정정보 및 공개된 취약정보를 지속적으로 수집하고 공격대상을 선정한다. 그러나 제4.1절에서 검토한 현행 진단체계는 사전에 확정된 자산과 점검범위를 중심으로 연 단위로 수행하고 있어, 관리부서가 인지하지 못한 외부 노출자산이나 수시로 변경되는 공격표면을 지속적으로 식별하는 데에는 보완이 필요하다. 또한 최강석, 이수진(2025)의 연구에서도 ASM솔루션으로 10개 민간기업의 공개 홈페이지 대상 취약점을 식별한 결과 10개 기업 홈페이지 모두에서 공개 취약점이 발견될 정도로 공격표면관리에 대한 중요성이 확인되었다.[27]

둘째, 초기침투 과정에서 이용될 수 있는 신규 취약점의 발생속도와 정기진단 주기 사이에 시간적 공백이 발생할 수 있다. 공격자는 고위험 취약점이 공개되거나 시스템의 설정 및 외부 노출상태가 변경된 직후 이를 침투경로로 이용할 수 있다. 반면 특정 시점 또는 연 단위로 수행되는 진단만으로는 진단 이후 새롭게 발생한 취약점과 환경변화를 적시에 식별하기 어렵다.[22]

셋째, 공격자의 목표달성으로 발생할 수 있는 실질적 피해를 고려하여 발견된 취약점을 평가하고 우선순위화하는 기능이 충분하지 않다. 동일한 기술적 심각도를 가진 취약점이라도 외부 노출 여부, 초기침투 가능성, 실행 및 권한상승으로의 이용 가능성, 내부이동 경로와의 연결성 및 핵심 자산에 대한 접근 가능성에 따라 실제 위험은 달라진다. 특히 공격이 목표달성으로 이어지면 방산 기술자료의 탈취·파괴와 업무중단 등 실질적인 피해가 발생하므로, 취약점의 위험도를 핵심자산과 공격경로의 연계성까지 고려하여 평가할 필요가 있다.

넷째, 실행·권한상승 및 내부정찰·횡적이동 단계에 대응하기 위한 보안관제와 취약점 관리활동 간의 연계가 미흡하다. 취약점 진단은 공격자가 이용할 수 있는 잠재적 약점을 사전에 식별하는 활동인 반면, 보안관제는 악성코드 실행, 비정상적인 권한 사용, 내부 탐색 및 원격접속 등 실제 공격 징후를 탐지하는 활동이다. 두 활동은 예방과 탐지라는 서로 다른 기능을 수행하지만, 동일한 공격 단계를 대상으로 한다는 점에서 상호 보완적이다. 즉 관제에서 확인된 공격기법과 공격징후는 어떤 취약점이 실제로 이용되고 있는지를 보여주므로 다음 진단의 범위와 대상을 정하는 근거가 되고, 반대로 진단에서 식별된 취약자산과 공격경로는 관제의 탐지규칙을 구체화하는 기준이 된다. 그러나 공개된 제도자료와 선행연구를 통해서는 이러한 정보가 상호 반영되는 운영절차가 충분히 확인되지 않는다.

다섯째, 운영 인프라와 개발환경을 통한 초기침투 경로를 통합적으로 관리하는 데 한계가 있다. 공격자는 운영 중인 서버와 네트워크 등의 인프라 취약점뿐만 아니라 소스코드, 오픈소스 구성요소, 빌드환경 및 소프트웨어 배포과정에서 발생하거나 유입되는 취약점을 침투경로로 이용할 수 있다. 그러나 인프라 중심의 취약점 진단만으로는 개발과정에서 생성되거나 외부 구성요소를 통해

유입되는 취약점을 배포 이전에 식별·조치하기 어렵고, 개발환경에서 확인된 취약점이 실제 운영·배포 자산에 미치는 영향도 파악하기 어렵다. 또한 서버·네트워크·단말·애플리케이션을 대상으로 하는 운영환경의 취약점 진단과 개발단계의 시큐어코딩, 정적 분석(SAST), 동적 분석(DAST), 소프트웨어 구성분석(SCA) 및 SBOM 기반 공급망 가시성 확보가 하나의 관리체계 안에서 연계되지 않을 경우, 개발단계에서 운영환경에 이르는 취약점의 유입·배포·노출 경로를 일관되게 추적하고 관리하는 데 한계가 있다.

여섯째, 취약점 진단과 개선조치의 결과를 지속적으로 확인하고 후속 관리활동에 반영하는 상시적이고 순환적인 운영이 부족하다. 취약점 관리는 특정 시점의 진단과 조치로 종료되는 것이 아니라, 신규 취약점과 자산변경을 지속적으로 식별하고, 개선조치의 이행 여부와 효과를 재점검하며, 모의해킹 및 보안관계에서 확인된 공격기법과 취약정보를 다음 진단과 조치 우선순위에 반영하는 순환구조로 운영될 필요가 있다. 그러나 공개자료에서 확인되는 현행 관리방식은 정기적인 진단과 해당 시점의 개선조치에 중점을 두고 있어, 이에 대한 보완이 필요하다. 아울러 국내 방산 대기업 및 중견기업의 보안인력 비율이 전체 인원 대비 1% 미만이라는 지적은 이러한 상시 관리기능을 개별 기업이 자체적으로 운영하는 데 인력상 제약이 있음을 시사한다.[25]

이상에서 살펴본 구조적 한계는 공격과정에서 요구되는 대응기능이 현행 관리체계에 충분히 반영되지 않은 문제와 개별적으로 수행되는 관리활동이 공격경로와 핵심자산을 기준으로 연계되지 않는 문제로 구분할 수 있다. 전자에는 외부 공격표면관리와 개발환경을 포함한 초기침투 경로 관리의 한계가 해당한다. 후자에는 신규 취약점의 발생속도와 정기진단 주기 간의 시간적 공백, 공격 경로와 핵심자산 영향을 반영한 우선순위화의 부족, 보안관계와 취약점 관리 간 정보연계의 미흡 및 상시·순환적 운영기능의 부족이 해당한다.

다음 장에서는 이러한 구분을 바탕으로, 공격단계별로 필요한 대응수단을 배치하고 이들 활동이 상호 연계되어 상시적으로 운영되도록 구성한 통합 대응체계를 제시한다.

5. 방산업체 보안취약점 통합 대응체계

5.1. 공격단계 기반 대응체계 구성

본 연구에서 제안하는 공격단계별 통합 대응체계는 제3장에서 도출한 6단계 공격구조를 방어자 관점에서 재해석하고, 단계별로 요구되는 대응기능을 통합·재구성하는 데서 출발한다. 4.2절에서는 이 6단계 공격구조를 분석기준으로 하여 현행 보안취약점 관리체계를 검토하고, 공격단계별로 요구되는 방어기능과 현행 관리방식 사이의 구조적 한계를 도출하였다. 본 절에서는 이러한 분석 결과를 바탕으로 6단계 공격구조를 방어자 관점의 대응영역으로 재구성하였으며, 다음 두 가지 기준을 적용하였다.

첫째, 서로 다른 공격단계라도 이를 차단하기 위한 방어목적과 주요 통제수단이 유사한 경우에는 하나의 대응영역으로 통합하였다.

둘째, 공격단계별 특성을 유지하면서도 특정 공격활동이 여러 단계에서 반복·병행될 수 있다는 점을 반영하였다. 이에 지속성 확보는 공격구조상 독립된 단계로 구분하되, 실제 공격과정 전반에서 반복될 수 있는 특성을 고려하여 관련 수단을 식별·제거하고 잔존·재발 여부를 반복적으로 확인하는 ‘지속적 점검 및 개선’ 영역에 대응시켰다.

첫 번째 기준에 따라 ③ 실행·권한상승과 ④ 내부정찰·형적이동은 하나의 대응영역으로 통합하였다. 두 단계는 공격자의 행위를 분석하는 과정에서는 구분할 필요가 있지만, 방어체계를 설계하는 관점에서는 계정·권한 관리, 접근통제, 네트워크 분리, 엔드포인트 통제 및 이상행위 탐지 등 상

호 연계된 통제수단이 적용된다. 따라서 두 단계를 별도의 방어영역으로 분리하기보다 ‘권한확대 및 내부이동 차단’이라는 하나의 대응영역으로 구성하였다. 반면 ① 정찰과 ② 초기침투는 각각 외부 공격표면의 식별과 침투경로의 사전 차단이라는 서로 다른 방어목적과 관리활동을 요구하므로 독립된 대응영역으로 유지하였다. 또한 ⑤ 목표달성은 앞선 단계의 차단에 실패했을 때 방산기술 자료의 유출·파괴와 업무중단 등 실질적인 피해를 억제하기 위한 데이터 및 핵심자산 중심의 보호 수단이 요구되므로 ‘핵심자산 보호’라는 별도의 대응영역으로 구성하였다. 두 번째 기준은 공격단계별 특성을 유지하되, 특정 공격활동이 다른 단계에서도 반복·병행될 수 있다는 점을 고려하는 것이다. ⑥ 지속성 확보는 공격자가 초기침투 이후 획득한 접근 권한과 공격거점을 유지하기 위한 공격단계이지만, 실행·권한상승, 내부정찰·횡적이동 및 목표달성 과정에서도 반복적으로 나타날 수 있다. 따라서 비인가 계정 생성, 자동실행 등록, 악성코드 설치 및 인증정보 유지 등 지속성 확보 수단을 일회성으로 조치하는 데 그치지 않고, 잔존 여부와 재발 여부를 주기적으로 확인해야 한다. 이에 지속성 확보에 이용되는 행위를 지속적으로 식별·제거하고, 그 결과를 추가 진단, 개선조치 및 재진단에 반영하는 ‘지속적 점검 및 개선’ 영역으로 구성하였다.

이러한 재구성을 통해 본 연구의 통합 대응체계는 정찰 및 외부 노출 식별, 초기침투 예방, 권한확대 및 내부이동 차단, 핵심자산 보호, 지속적 점검 및 개선의 5개 대응영역으로 구성된다. 각 공격단계에 대응하는 주요 관리활동과 기술적 통제수단은 표 3과 같다.

표 3. 공격단계 기반 보안취약점 통합 대응체계

공격단계	대응영역	통합 대응체계	
		주요 관리활동	주요 기술통제 수단
① 정찰	정찰 및 외부 노출 식별	외부 노출자산 상시적 탐색, 자산 식별 및 노출 위험도 평가	ASM 솔루션(서비스)
② 초기침투	초기침투 예방	인프라 웹서비스 정기/수시 취약점 진단, 고 위험 취약점 즉시 패치, 시큐어코딩 가이드 준수, CI/CD 자동검증(커밋·빌드·배포시), SBOM 기반 구성요소·오픈소스 이력관리, (관리자)계정 보안 강화	취약점 진단 자동화 솔루션, 웹 취약점 스캐너, SAST·DAST·SCA 도구, SBOM 생성·관리 도구, 다중인증(MFA)
③ 실행·권한상승 ④ 내부정찰·횡적 이동	권한확대 및 내부이동 차단	계정 및 권한 관리, 중요정보 접근통제, AD 보안 강화, 이상행위 탐지, 보안관제 연계 분석	이상행위탐지(EDR/NDR), 통합관제(SIEM /SOAR)
⑤ 목표달성 (유출·파괴)	핵심자산 보호	최소권한 부여 및 이력 관리, 이상트래픽 탐지, 백업 및 복구 체계	접근통제 솔루션, 데이터유출방지(DLP), DB/문서 암호화, 백업 솔루션
⑥ 지속성 확보	지속적 점검 및 개선	정기 진단·재진단, 개선조치 이행점검, 위협-통제 연계 관리, 모의해킹	-

5.1.1. 정찰 및 외부 노출 식별 단계

공격표면관리(ASM)를 통해 인터넷 노출자산, 서브도메인, 공개 포트, 인증서, 취약 서비스, 유출 계정 여부를 상시 식별하고 우선순위를 평가해야 한다. 이 단계는 외부 노출자산의 가시성을 확보함으로써 공격자의 정찰 우위를 감소시키는 역할을 한다.

5.1.2. 초기침투 예방 단계

운영 인프라와 개발환경 양쪽에서 침투 경로를 사전에 차단해야 한다. 인프라 측면에서는 서버, 네트워크, 애플리케이션에 대한 솔루션 기반 자동 점검과 신규 서비스 오픈 등 이벤트 발생 시에는

수시 점검을 병행하는 정기·수시 취약점 진단이 필요하며, 고위험 취약점에 대해서는 즉시 패치, 설정 변경, 접근통제 강화 등을 적용해야 한다. 특히 취약점 진단 자동화 솔루션, 웹 취약점 스캐너, (관리자)계정 보안 강화, 다중인증(MFA) 확대는 초기침투 경로를 줄이는 핵심 통제수단이 된다. 한편 자체 개발한 웹서비스나 응용시스템에 내재된 취약점 역시 주요 침투 경로가 되므로, 개발 단계에서부터 취약점 유입을 차단하는 조치가 병행되어야 한다. 시큐어코딩 가이드라인 준수, CI/CD 파이프라인과 연계한 SAST·DAST·SCA 기반의 자동화된 개발보안 점검과 SBOM 생성 및 오픈소스 구성요소 이력관리를 결합함으로써 배포 이전에 취약점을 제거할 수 있다.[28-30] 이는 외부에 노출되는 서비스의 초기 침투면을 근본적으로 축소하는 예방조치에 해당한다.

5.1.3. 권한확대 및 내부이동 차단 단계

초기침투 이후의 피해 확산을 방지하기 위해서는 계정 및 권한 관리, 중요정보 접근통제, 중요시스템 최소권한 부여, 디렉터리 서비스(AD) 보안 강화, 이상행위 탐지, 보안관제 연계 분석이 중요하다. 기술적으로는 엔드포인트 및 네트워크 이상행위 탐지(EDR/NDR)와 통합관제(SIEM/SOAR)를 연계하여 내부 확산 징후를 조기에 포착할 수 있는 보안관제 체계를 갖추어야 한다. 이와 함께 모의해킹을 통해 실제 권한상승과 내부이동 가능 경로를 반복적으로 점검해야 하고, 진단에서 확인된 공격기법이 관제의 탐지규칙으로 반영되도록 설계되어야 한다.

5.1.4. 핵심자산 보호 단계

공격자가 최종 목표에 도달하더라도 실제 유출과 피해로 이어지지 않도록 하는 방어수단이 요구된다. 방산업체의 경우 방산기술이 포함된 설계자료, 시험평가 데이터, 기술문서 등이 최종 표적이 되므로, 이러한 핵심자산에 대한 접근통제와 데이터 중심 보호가 핵심이 된다. 구체적으로는 기술자료 관리시스템에 대한 접근권한 최소화과 이력관리, 중요자료의 암호화 적용, 데이터 유출방지(DLP)를 통한 반출 통제, 대량 다운로드·비정상 반출 등 이상 트래픽에 대한 탐지와 차단이 포함된다. 아울러 랜섬웨어 등에 의한 자료 파괴에 대비하여 백업·복구 체계를 갖추고 주기적으로 복구가능성을 확인해야 한다.

5.1.5. 지속적 점검 및 개선 단계

정기·수시 진단, 모의해킹 및 개선조치 이행점검을 연계하는 순환 체계를 구축해야 한다. 이 단계는 공격자가 확보한 접근권한과 공격거점의 잔존·재발 여부를 반복적으로 확인하고, 비인가 계정, 자동실행 항목, 비정상 서비스, 악성코드 및 탈취된 인증정보 등 지속성 확보수단을 식별·제거하는 기능을 담당한다. 진단에서 확인된 취약점은 개선조치 이후 이행점검을 통해 실제로 해소되었는지 확인하고, 모의해킹에서 확인된 공격경로는 해당 경로상의 대응수단이 적절하게 보완되었는지 재점검해야 한다. 결국 이 단계의 핵심은 단발성 진단 중심의 구조를 상시적이고 순환적인 운영체제로 전환하는 데 있으며, 구체적인 실행방안은 조직 여건에 따라 달라지므로 5.2절에서 단계적 적용방안으로 제시한다.

5.2. 통합 대응체계의 단계적 적용방안

본 연구에서는 방산업체 간 보안인력, 예산, 기술역량 및 운영환경의 차이를 고려하여, 제5.1절에서 제시한 공격단계별 통합 대응체계를 일시에 적용하기보다는 조직의 관리역량에 따라 단계적으로 도입할 수 있도록 적용 수준을 4단계로 구분하였다. 각 단계는 제4장에서 도출한 구조적 한계

와 제5.1절의 대응영역을 바탕으로 본 연구에서 재구성한 적용방안이다.

각 단계에는 통합 대응체계의 성숙도를 높이기 위해 우선적으로 확보해야 할 핵심 활동을 제시하였고, 단계가 높아질수록 이전 단계에서 구축한 기능을 지속적으로 운영하면서 자동화, 상시성 및 대응영역 간 연계를 확대하는 누적적 구조로 설계하였다. 그리고 보안관제는 고도화 단계에서 새롭게 도입되는 선택적 기능이 아니라 모든 성숙도 단계에서 요구되는 기본기능으로 설정하였다. 다만 방산업체의 인력·예산 및 기술역량을 고려하여 관제범위, 운영시간, 분석수준 및 자동화 정도를 단계적으로 확대하도록 구성하였다. 따라서 방산업체는 현재의 운영수준과 부족한 역량을 확인하고, 조직의 인력·예산·기술 여건을 고려하여 다음 단계로의 이행계획과 우선순위를 수립할 수 있다.

5.2.1. 1단계(기반 구축)

전담인력과 상시 솔루션 운영이 제한적인 방산업체를 가정한 기반 구축 단계로, 방위사업청 또는 협회의 취약점 진단사업을 통한 점검과 자체 투자에 의한 연 1회 점검을 합하여 상·하반기 정기 진단 체계를 확보하는 수준이다. 또한 외부 노출자산은 별도 솔루션 없이 담당자가 수동으로 목록을 관리하며, 대응단계 관점에서는 ① 정찰 및 외부 노출 식별과 ② 초기침투 예방이 부분적으로 이루어지는 수준에 해당한다. 이 단계에서는 전담인력 없이도 활용 가능한 관계기관의 지원사업과 전문업체를 활용하는 것이 현실적이다. 또한 보안관제는 핵심시스템과 주요 보안장비를 대상으로 로그와 보안이벤트를 수집하고, 중요 경보를 담당자에게 통보·확인하는 최소 관제기능을 확보한다. 자체 운영역량이 부족한 업체는 외부 전문기관의 관제서비스를 활용할 수 있다. 이를 통해 취약점 진단과 개선조치 이후에도 비인가 계정 생성, 권한변경, 비정상 로그인, 악성 프로세스 실행 등 주요 이상행위를 확인할 수 있는 기반을 마련한다.

5.2.2. 2단계(운영 확대)

1단계에서 구축한 정기진단체계를 기반으로 점검대상과 수행주기를 확대하고, 취약점의 식별·조치·재점검에 관한 표준 운영절차를 정립하는 단계이다. 인터넷 노출자산뿐만 아니라 내부 서버, 네트워크, 단말 및 주요 애플리케이션으로 진단범위를 확대하며, 자산 중요도와 취약점의 기술적 심각도를 기준으로 조치 우선순위와 기한을 관리한다. 외부 노출자산은 담당자가 정기적으로 확인 하되, 자산의 신규 등록·변경·폐기 정보를 취약점 관리대장에 반영한다. 개발환경에는 시큐어코딩과 정적 분석(SAST)을 우선 적용하고, 주요 웹 애플리케이션에는 동적 분석(DAST)을 단계적으로 도입한다. 공격단계별 대응 관점에서는 정찰 및 초기침투 예방과 함께 실행·권한상승 및 내부이동에 이용될 수 있는 취약점의 관리범위를 확대하는 수준이다. 보안관제는 핵심시스템 중심의 최소 관제에서 주요 서버·네트워크·단말 및 보안장비를 포함하는 기본 관제로 확대한다. 관제시간, 경보 등급, 담당자 통보, 초동조치 및 사고보고 기준을 표준화하고, 주요 경보의 확인·조치 결과를 이력으로 관리한다. 비인가 계정과 권한변경, 비정상 원격접속, 악성코드 탐지, 중요 서비스와 자동실행 항목의 변경, 중요자료의 대량조치·압축·반출 징후 등을 주요 관제대상으로 설정한다. 다만 이 단계에서는 취약점 관리와 관제활동이 각각 운영되며, 고위험 정보나 반복적으로 발생하는 이상행위에 한하여 관련 자산의 추가 진단과 점검주기 조정에 반영한다.

5.2.3. 3단계(연계 운영)

인프라와 개발환경에서 수행되는 취약점 관리활동을 실제 자산·서비스·배포정보를 기준으로 연계하고, 취약점 진단, 모의해킹 및 보안관제의 결과를 상호 반영하는 단계이다. 인프라 영역의 서

버 및 운영체제, 네트워크, 보안설정에 대한 진단결과와 개발환경의 SAST·DAST·SCA 및 SBOM 정보를 실제 운영·배포 자산에 매핑한다. 취약점의 기술적 심각도뿐만 아니라 외부 노출 여부, 실제 배포 여부, 악용 가능성, 공격경로 및 핵심자산에 미치는 영향을 종합하여 조치 우선순위를 결정한다. 또한 운영환경에서 확인된 취약점과 공격기법을 시큐어코딩 기준, 보안시험 항목 및 CI/CD 보안정책에 반영하고, 개발단계에서 확인된 고위험 취약점과 구성요소 정보는 운영 인프라의 추가 점검대상에 반영한다. 보안관계는 취약점 관리시스템, 자산정보, 외부 노출자산 점검 및 모의해킹 결과와 연계하여 운영한다. 고위험 취약자산과 모의해킹에서 확인된 공격경로를 중점 관제대상으로 지정하고, 관련 공격기법과 TTP를 탐지규칙 및 분석 시나리오에 반영한다. 반대로 관제과정에서 확인된 공격징후, 반복 경보 및 취약자산 정보는 취약점의 조치 우선순위 조정, 추가 진단, 개선조치와 재점검에 반영한다. 이를 통해 취약점 진단과 보안관계가 각각 수행되는 구조에서 벗어나, 잠재적인 약점과 실제 공격징후를 함께 분석하는 연계 운영체제를 구축한다.

5.2.4. 4단계(능동 방어)

인프라, 개발환경 및 외부 공격표면의 취약점 정보를 통합하고, 실제 공격경로와 핵심자산 영향을 기반으로 상시적인 위협관리와 자동화된 대응체계를 운영하는 단계이다. ASM을 활용하여 외부 노출자산과 공격표면의 변화를 지속적으로 식별하고, 인프라 진단결과와 SAST·DAST·SCA·SBOM 및 배포정보를 자동 연계한다. 또한 위협정보, 실제 악용 여부, 자산 중요도, 공격경로 및 핵심자산 영향을 반영하여 위험도를 동적으로 산정하고, 고위험 취약점의 조치·재점검 및 예외승인 과정을 통합적으로 관리한다. 모의해킹과 레드팀 활동을 통해 개별 취약점뿐만 아니라 복수의 취약점과 보안통제 우회가 결합된 공격경로를 지속적으로 확인한다. 보안관계는 24시간 상시관제를 기반으로 보안시스템의 정보를 통합분석하고, MITRE ATT&CK 기반 탐지 시나리오, 위협헌팅 및 자동화된 초동대응 기능을 운영한다. 취약점 진단, ASM, SAST·DAST·SCA, SBOM, 모의해킹 및 레드팀 결과를 SIEM의 자산정보와 탐지규칙에 연계하여 고위험 취약자산에 대한 관제 수준을 강화한다. 관제 과정에서 새롭게 확인된 TTP와 공격경로는 취약점 진단항목, 개발단계의 보안통제 및 공격 시뮬레이션 시나리오에 자동(또는 일부 자동)으로 반영한다. 이를 통해 개발-배포-운영-관제-재점검 전 과정의 정보를 연계하고, 변화하는 위협과 공격표면에 지속적으로 대응하는 능동방어 체계를 구축한다.

이러한 단계별 강화를 위해서는 계속된 예산 및 인력 투자가 수반되므로, 회사 경영진의 지속적인 관심과 투자 의지가 가장 중요하며, 이에 따라 회사의 보안 수준이 결정되는 요인으로 작용한다. 현실적 여건을 고려하여 방위사업청 등 관계기관의 취약점 진단사업 확대나 보안관계 서비스, 컨설팅 지원 등과 연계하여 단계적으로 추진하는 것도 하나의 방법이 될 수 있다.

본 연구가 제안한 대응영역과 단계적 적용방안을 기존 사이버보안 체계와 비교하면 다음과 같다. NIST CSF 2.0은 Govern, Identify, Protect, Detect, Respond 및 Recover의 기능을 통해 조직의 보안관리체계 전반을 포괄하지만, 특정 통제가 실제 공격경로의 어느 지점에 대응하는지를 직접 제시하지는 않는다. 그리고 기존 사이버보안 성숙도 모형은 조직의 사이버보안 활동이 얼마나 체계적으로 수행·관리·측정되는지 평가한다. 이에 비해 본 연구의 4단계 적용방안은 종합적인 보안성숙도를 판정하는 모형이 아니라, 방산업체가 보안취약점 관리기능의 범위와 수행주기, 자동화 및 대응영역 간 연계수준을 기반 구축, 운영 확대, 연계 운영 및 능동방어의 순서로 확대하기 위한 실행경로이다. 따라서 업체는 공격단계별 대응 공백과 자체 인력·예산·기술역량을 함께 고려하여 다음 단계로의 이행 우선순위를 결정할 수 있다. 그리고 방산업체를 대상으로 하는 국내법 기반의 통합실태조사와 보안측정, 미국 전쟁부 계약시 필요한 보안인증인 CMMC 등의 방산분야 보안 기준은 보호요건의 이행과 준수 여부를 평가하는 데 중점을 둔다. 본 연구는 이러한 기준을 대체하

거나 새로운 통제목록을 제시하려는 것이 아니라, 기존 통제수단을 실제 공격경로에 따라 재배치하고 외부 노출자산, 운영 인프라, 개발환경, 핵심자산 및 지속적 개선활동을 연계함으로써 제한된 자원 아래에서 통제수단의 도입과 고도화 순서를 결정할 수 있는 적용구조를 제시한 데에 의의가 있다.

6. 결론

본 연구는 최신 사이버위협 동향과 주요 공격사례를 분석하고, 사이버 공격단계와 모의해킹 관점의 공격경로 분석을 종합한 후, 방산업체 보안취약점 관리체계의 제도·운영 현황과 구조적 한계를 검토하여 공격단계 기반의 통합 대응체계와 단계적 적용방안을 제안하였다. 국내외 위협 동향과 주요 사고를 통해 공개 애플리케이션, 탈취 계정, 외부 점점과 소프트웨어 공급망이 결합된 공격이 빠르게 전개됨을 확인하였으며, 방위사업청 진단사업의 운영 현황과 선행연구 분석을 통해 외부 공격표면의 관리 미흡, 정기진단 주기와 신규 취약점 발생속도 간의 시간적 공백, 공격경로와 핵심자산 영향을 반영한 우선순위화 기능의 부족, 보안관제와 취약점 관리활동 간 연계 미흡, 운영 인프라와 개발환경의 통합관리 한계, 상시·순환적 운영기능의 부족이라는 여섯 가지 구조적 한계를 도출하였다. 이러한 한계를 극복하기 위해 본 연구는 사이버 킬체인과 MITRE ATT&CK를 종합한 6단계 공격구조를 방어자 관점에서 재구성하였다. 방어목적과 통제수단이 유사한 단계는 하나의 대응영역으로 통합하고, 여러 단계에 걸쳐 반복·병행되는 공격활동에 대해서는 일회성 조치에 그치지 않고 잔존 여부와 재발 여부를 주기적으로 확인하는 대응영역으로 구성하였다. 그 결과 정찰 및 외부 노출 식별, 초기침투 예방, 권한확대 및 내부이동 차단, 핵심자산 보호, 지속적 점검 및 개선의 5개 대응영역으로 구성된 통합 대응체계를 설계하였다. 아울러 방산업체 간 보안인력 및 예산 등의 차이를 고려하여 기반 구축, 운영 확대, 연계 운영, 능동방어의 4단계 적용방안을 제시하였으며, 보안관제를 모든 단계의 기본기능으로 설정하되 관제범위와 분석수준을 단계적으로 확대하도록 구성함으로써 조직 여건에 따른 점진적 고도화가 가능하도록 하였다.

본 연구의 학술적 의의는 기존 연구에서 개별적으로 논의된 공격표면관리, 인프라 취약점 진단, 개발보안, 보안관제 및 모의해킹을 공격경로 중심의 단일 분석틀로 재구성했다는 데 있다. 특히 사이버 킬체인의 단계적 흐름과 MITRE ATT&CK의 TTP 관점을 결합하되, 공격단계와 방어영역을 기계적으로 일대일 대응시키지 않고 방어목적과 통제수단의 유사성에 따라 5개 대응영역으로 재구성하고 단계별 적용방안을 제시했다는 점에서 본 연구의 차별성이 있다. 실무적으로는 방산업체가 외부 노출자산에서 내부 핵심자산까지 이어지는 공격경로를 기준으로 현재의 취약점 관리활동을 점검하고, 제한된 인력과 예산을 우선적으로 보완해야 할 영역에 배분할 수 있는 기준을 제시하였다. 아울러 방위사업청의 취약점 진단 지원이 정기적인 인프라 점검과 모의해킹을 넘어 외부 공격표면관리, 개발환경 보안, 관제정보 연계 및 개선조치 이행점검으로 확대될 필요성을 제시하였다. 다만 이러한 정책적 확대는 모든 방산업체에 동일한 수준으로 적용하기보다 업체별 관리역량과 보유자산의 중요도 및 위협수준을 고려하여 단계적으로 추진할 필요가 있다.

본 연구에는 다음과 같은 한계가 있다. 첫째, 방산 분야의 보안 민감성과 자료 접근의 제약으로 인해 개별 방산업체의 자산·취약점·보안관제 및 침해사고 데이터를 충분히 확보하지 못하였다. 둘째, 공개된 모의해킹 방법론을 바탕으로 공격경로를 개념적으로 구성하였으므로 실제 방산업체의 망 구성, 접근통제 및 개발·운영환경에 따라 발생할 수 있는 다양한 공격경로를 모두 반영하지 못하였다. 셋째, 연구범위를 방산업체 자체의 관리체계로 한정하여, 협력업체를 포함한 방산 공급망 전반의 관리방안은 구체적으로 다루지 않았다.

향후 연구에서는 방산업체 보안담당자와 진단·관제 전문가를 대상으로 설문조사와 델파이 조사

또는 AHP 분석을 실시하여 대응영역과 세부 통제수단의 적용 현황을 파악하고, 그 중요도와 우선 순위를 평가할 필요가 있다. 또한 연구범위를 협력업체까지 확대하여 원청 방산업체와 협력업체 간 취약점 정보공유와 보안지원 및 공동대응 방안을 구체화하는 후속 연구가 필요하다.

참고문헌

- [1] 경찰청. 경찰청·방위사업청 등 관계기관 합동 특별점검을 통해 북한의 케이(K)-방산업체 해킹 공격 규명 및 보호조치 실시. 2024. https://www.police.go.kr/user/bbs/BD_selectBbs.do?q_bbsCode=1002&q_bbscttSn=20240423132830276 (검색일 2026. 6. 12).
- [2] Cybersecurity and Infrastructure Security Agency (CISA). Advanced persistent threat compromise of government agencies, critical infrastructure, and private sector organizations (AA20-352A). 2020. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a> (검색일 2026. 6. 12).
- [3] Cybersecurity and Infrastructure Security Agency (CISA). Apache Log4j vulnerability guidance. 2021. <https://www.cisa.gov/news-events/news/apache-log4j-vulnerability-guidance> (검색일 2026. 6. 12).
- [4] Cybersecurity and Infrastructure Security Agency (CISA). #StopRansomware: CLOP ransomware gang exploits CVE-2023-34362 MOVEit vulnerability (AA23-158A). 2023. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a> (검색일 2026. 6. 12).
- [5] Cybersecurity and Infrastructure Security Agency (CISA). Threat actors exploit multiple vulnerabilities in Ivanti Connect Secure and Policy Secure gateways (AA24-060B). 2024. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-060b> (검색일 2026. 6. 12).
- [6] 금융위원회. 롯데카드 정보유출 관련 긴급 대책회의 개최. 2025. <https://www.fsc.go.kr/no010101/85319> (검색일 2026. 6. 12).
- [7] 유도진. 중국 배후의 주요 APT 그룹들의 공격 패턴 및 전략 분석: MITRE ATT&CK Framework를 중심으로. 한국과학기술학회논문지, 제25권 제9호, pp. 262-269. 2024. <https://doi.org/10.5762/KAIS.2024.25.9.262>
- [8] IBM Security. X-Force Threat Intelligence Index 2026. 2026. <https://www.ibm.com/reports/threat-intelligence> (검색일 2026. 6. 15).
- [9] Palo Alto Networks. Unit 42 Global Incident Response Report 2026. 2026. <https://www.paloaltonetworks.com/resources/research/unit-42-incident-response-report> (검색일 2026. 6. 15).
- [10] 한국인터넷진흥원. 2025년 사이버 위협 동향 및 2026년 전망 보고서. 2026.
- [11] SK실터스. AI시대 해킹 대응 전략, 중소기업에 MDR이 필요한 이유는? 2026. <https://www.skshieldus.com/security-insights/trends/ai-hacking-response-mdr-smb-security-strategy> (검색일 2026. 6. 15).
- [12] 안랩. 2025년 사이버 위협 동향 및 2026년 전망 보고서. 2025. <https://www.ahnlab.com/ko/contents/content-center/36017> (검색일 2026. 6. 15).
- [13] 보안뉴스. 롯데카드, 2017년 공개된 취약점에 당했다...제2금융권 전반 기본적 보안 미흡 투영. 2025. <https://www.boannews.com/media/view.asp?idx=139047> (검색일 2026. 6. 15).
- [14] 과학기술정보통신부. 민관합동조사단, SK텔레콤 침해사고 조사결과 2차 발표. 2025. <https://www.msit.go.kr/bbs/view.do?sCode=user&mId=307&mPid=208&bbsSeqNo=94&ntSeqNo=3185809> (검색일 2026. 6. 15).
- [15] Hutchins E et al. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Leading Issues in Information Warfare & Security Research, Vol. 1, No. 1, pp. 80-106. 2011.
- [16] 신강식, 조호목. MITRE ATT&CK 및 D3FEND를 활용한 효율적인 정보보호 솔루션 도입 방안 연구. 정보보호학회논문지, 제35권 제4호, pp. 887-906. 2025. <https://doi.org/10.13089/JKIISC.2025.35.4.887>

- [17] MITRE Corporation. MITRE ATT&CK Matrix for Enterprise v18.1. <https://attack.mitre.org/versions/v18/> (검색일 2026. 7. 2).
- [18] 김도훈. NIST 800-53을 고려한 MITRE 프레임워크 기반의 사이버 위협과 그 방어 모델링 방법. 한국정보기술학회지, 제21권 제1호, pp. 25-30. 2023.
- [19] 윤영인 등. APT 공격 사례 분석을 통한 사이버 킬체인과 TTP에 대한 연구. 융합보안논문지, 제20권 제4호, pp. 91-101. 2020. <https://doi.org/10.33778/kcsa.2020.20.4.091>
- [20] National Institute of Standards and Technology. Technical guide to information security testing and assessment (NIST SP 800-115). 2008.
- [21] Penetration Testing Execution Standard (PTES). The Penetration Testing Execution Standard, Version 1.0. 2014. http://www.pentest-standard.org/index.php/Main_Page (검색일 2026. 6. 20).
- [22] SK쉴더스. 모의해킹이 중요해진 이유, ISMS 개편 이후 달라지는 기업 보안 기준. 2026. <https://www.skshieldus.com/security-insights/trends/penetration-testing-isms-security-standards> (검색일 2026. 6. 15).
- [23] 안랩. AhnLab 침투테스트 컨설팅 소개자료. https://image.ahnlab.com/img_upload/product/2312222132686220.pdf (검색일 2026. 6. 20).
- [24] 대한민국 정책브리핑. '26년 사이버보안 취약점 진단사업 착수. 2026. <https://www.korea.kr/briefing/pressReleaseView.do?newsId=156753106> (검색일 2026. 7. 2).
- [25] 뉴시스. '방산 협력사에 해킹 시도' 5년 사이 최대...“보안책 절실”. 2024. https://www.newsis.com/view/NISX20241015_0002920926 (검색일 2026. 7. 2).
- [26] 한국인터넷진흥원. 주요정보통신기반시설 기술적 취약점 분석·평가 방법 상세가이드. 2025.
- [27] 최강석, 이수진. ASM 솔루션을 활용한 공개 홈페이지 보안 취약점 분석 및 효율적인 대응방안 연구. 한국정보기술학회논문지, 제23권 제1호, pp. 201-212. 2025. <https://doi.org/10.14801/jkiit.2025.23.1.201>
- [28] 김형배. 소프트웨어 개발 생명주기(SSDLC)의 보안 적용 실태와 AI 기반 DevSecOps 전환 트렌드에 관한 연구. 정보보호학회논문지, 제36권 제2호, pp. 675-680. 2026.
- [29] 최영해 등. 오픈소스 취약점 점검 도구 및 종합 보안 메트릭 설계를 통한 DevSecOps 구축방안 연구. 정보보호학회논문지, 제33권 제4호, pp. 699-707. 2023.
- [30] 손효현 등. 사이버안보 강화를 위한 소프트웨어 공급망 보안 정책 연구: SBOM 정책 추진 사례를 중심으로. 디지털융복합연구, 제20권 제2호, pp. 9-20. 2022. <https://doi.org/10.14400/JDC.2022.20.2.009>