https://doi.org/10.33778/kcsa.2021.21.4.077

사이버 위협 중심의 국방 사이버 방호수준 분석에 관한 연구

최 세 호*, 오 행 록**, 윤 주 범***

요 약

사이버 방호란 사이버 공격 및 위협으로부터 우리가 운영하는 정보시스템을 보호하는 활동[1]이다. 현재 운영중인 사이버 방호체계의 방호수준을 알기 위해서는 시시각각 새롭게 발전하고 있는 사이버 위협을 반영하여 공격기술 현황을 최신화하고 방호기능으로 대응이 가능한지 분석할 필요가 있다. 이에 본 논문에서는 사이버 킬 체인의 공격절차와 방어유형으로 분류한 공격기술을 MITRE의 방어기술(Mitigation ID)과 연관 관계를 분석하고 방어적 사이버활동 중심으로 군 부대 유형별 사이버 방호수준을 제시하고자 한다. 향후 국방영역에서 운영중인 사이버 방호체계의 대응역량을 실시간 분석하여 부대별 방호수준을 가시화하고 알려지지 않은 사이버 위협에 대한 조사 및 적극적인 취약점 보완을 통해 사이버 방호수준이 향상되길 기대한다.

A Study on The Cyber Threat Centered Defense Cyber Protection Level Analysis

Seho Choi*, Haengrok Oh**, Joobeom Yun***

ABSTRACT

Cyber protection is an activity that protects the information systems we operate from cyber attacks and threats. To know the level of protection of the currently operating cyber protection system, it is necessary to update the current state of attack technology by reflecting the constantly evolving cyber threats and to analyze whether it is possible to respond with the protection function. Therefore, in this paper, we analyze the relationship between the attack procedures and defense types of the cyber kill chain with the defense technology(Mitigation ID) of MITRE and present the cyber protection level for each military unit type with a focus on defensive cyber activities. In the future, it is expected that the level of cyber protection will be improved through real-time analysis of the response capabilities of cyber protection systems operating in the defense sector to visualize the level of protection for each unit, investigate unknown cyber threats, and actively complement vulnerabilities.

Key words : Cyber Threat, Cyber Kill Chain, Cyber Protection Level, Protection Function

접수일(2021년 09월 30일), 게재확정일(2021년 10월 18일)

* 세종대학교 정보보호학과(주저자)
** 국방과학연구소 제2기술연구본부(공동저자)
*** 세종대학교 정보보호학과(교신저자)

1. 서 론

인터넷이 급속도록 발전하고 5G 이동통신이 상용화되면서 장소와 상관없이 모바일과 테블릿으로 업무를 손쉽게 처리할 수 있는 인프라가 구축되었다. 문제는 인프라 변환에 따른 적절한 사이버 방호체계가 부재하여 사이버공간에서 악의적 활동이 증가하고 피해 규모 및 심각성 또한 지속적으로 확대되고 있다. 그 가운데 알려지지 않은 지능형 사이버 위협은 공공 및 민간기관 등 모든 조직에서 대응하는데 현실적으로 문제점 및 한계에 직면하고 있다.

민간 기업에서는 2013년부터 정보보호관리체계(Information Security Management System, 이하 ISMS)를 통해 적합한 정보보호 정책을 수립하고 보완하면서 시시각각 발생되는 사이버 위협에 상시 대응하는 등 여러 보안대책을 유기적으로 통합 관리하기 위해 노력하고 있다[2]. 국방영역에서도 민간 기업의 ISMS를 바탕으로 부대별 방어적 사이버활동과 소관 영역에 구축된 인프라 특성을 고려하여 평가항목을 보완하고, 2019년부터 명칭을 '사이버보안 기관평가'로 변경하여 사이버정책, 응용, 감시, 물리적보호의 4가지 분야 평가를 통해 사이버 방호체계를 보강하고 있지만, 급변하는 지능형 사이버 위협을 반영하여 현재 운영중인 사이버 방호체계의 방호수준을 분석하기에는 제한적이다. 그리고 1개의 사이버 위협, 또는 취약점이 다른 사이버 위협이나 취약점에 유입 통로가 될 수 있으므로 사이버 위협간의 관계, 취약점간의 관계, 사이버 위협과 취약점의 관계에 대해 연관 분석이 필요하다.

2017년 KIDA에서 사이버 킬 체인 기반의 국방 사이버 위협 대응체계 구축방안 선행연구를 통해 개념정립 및 기본계획을 수립[3]하였지만, 아직까지는 국방영역에서 운영중인 사이버 방호체계에 적용된 사례는 없었다.

이에 본 논문에서는 점차 지능화·은닉화·표적화·조직화되고 있는 사이버 위협을 MITRE의 방어기술(Mitigation ID)을 기반으로 사이버 킬 체인의 공격절차 7단계(정찰 - Reconnaissance, 무기화 - Weaponization, 전달/유포 - Delivery, 악용 - Exploitation, 설치 - Installation, 명령/제어 - Command and Control, 목적 달성 - Actions on Objectives)와 방어유형 6가지(탐지 - Detect, 거부 - Deny, 교란 - Disrupt, 약화 - Degrade, 기만 - Deceive, 파괴 - Destroy)로 분류하고 국방영역에서 운영중인 사이버 방호체계로 대응할 수 있는지 방호수준을 분석하고자 한다.

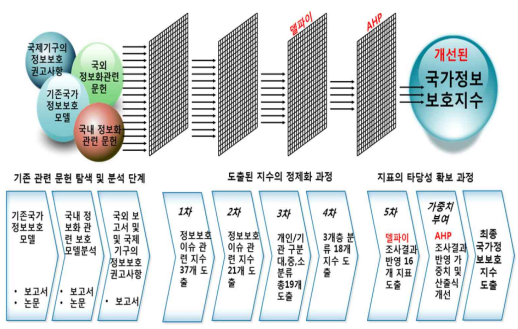
2장에서는 사이버 방호수준에 관한 국가 정보보호수준 평가지표 개선 등 기존 연구와 사이버보안 기관평가, 방어기술(Mitigation ID)에 대해 정리하고, 3장은 사이버 공격 전술, 기법 및 절차(Tactics, Techniques and Procedures, 이하 공격기술(TTPs))와 국방영역에서 운영중인 사이버 방호기능에 대한 분석한 결과를 설명한다. 4장에서는 국방영역에서 방어적 사이버활동 중심으로 부대 유형을 구분하고 사이버 방호수준을 검증한다. 마지막 장에서는 결론 및 향후 연구 방향을 설명하는 순으로 논문을 구성한다.

2. 사이버 방호수준에 관한 기존연구

본 장에서는 서론에서 간략히 설명한 사이버 방호수준과 관련하여 기존에 연구된 국가 정보보호수준 평가지표 개선, 위험 평가 모델 기반의 정량적 사이버 보안 평가 체계에 대한 연구와 국방부의 사이버보안 기관평가, MITRE의 방어기술(Mitigation ID)에 대해 정리한다.

2.1 국가 정보보호수준 평가지표 개선[4]

국가 정보보호수준을 평가하기 위한 방법론으로 계량적인 모델을 제시하기 위해 (그림 1)과 같이 기존 연구를 분석하고 도출된 지수에 대한 정제화 과정을 거친 후 지표의 타당성을 확보하는 과정을 포함했다.



(그림 1) 국가 정보보호 지표 선정 및 지수 산출 과정

국내·외 정보보호 및 정보화 지수모델 관련 연구 및 보고서를 비롯한 국제기구의 권고 기준을 바탕으로 지표 Pool을 구성하고 5차의 지표 정제 과정과 델파이, 전문가들의 의사결정 판단 자료를 기반한 AHP (Analytic Hierarchy Process, 이하 AHP) 분석 방법을 활용하여 지표 및 그 산출 방법의 타당성을 확보했다. 특히 지표 선정을 위해 PRM(Performance Reference Model) 기반의 '입력(Input) - 처리(Process) - 출력(Output)'의 인과적 메커니즘을 바탕으로 '기반(Infra) - 대응활동(Activity) - 성과(Performance)'의 3단계 프레임워크를 고안했다.

임규건은 기존 지표 대비 개인정보 노출률, 악성 봇 감염율, 신기술 환경 대응률, 정보보호관리체계 인증률, 백업 관리율, 패스워드 관리율의 6가지 신규지표 추가하고 지표의 중요도에 따른 가중치가 부여되어 산출된 지표 및 지수의 타당성이 확보되었으나 대응활동 및 성과단계에서 사이버 위협요소와 공개 취약점 조치율에 대한 세부지표를 반영하지 않았다.

2.2 정량적 사이버 보안 평가 체계[5]

정량적 평가의 신뢰성 향상을 위해 운영중인 사이버 방호체계 대상으로 모의 해킹을 통한 실험 데이터 등 많은 통계적 자료의 축적이 제한되었다. 사이버 보안성에 대해 정량적 값을 제시하고 그 객관성을 보장하는데 한계가 있어 자산요소, 위협요소, 취약성요소의 3가지로 평가 척도를 제시하여 평가 척도에 따른 정량적 값 산출 방법을 다음과 같이 제안했다.

자산은 유형, 특성, 속성 등에 따라 우선순위를 갖는 보안요소와 기밀성(Confidentiality), 무결성(Integrity) 및 가용성(Availability)의 수준에 따라 가중치 값이 달라질 수 있다. 앞 연구[4]와 동일하게 AHP 기법을 적용하여 보안 요소별 가중치 값을 이용한 위협의 영향도 값을 산출하여 자산의 특성 및 속성에 따른 위험분석 결과의 정확도를 높였다. 위협은 자산의 손실을 발생시키거나 보안에 해를 끼치는 원인이나 행위, 사건으로 통계적 수치를 통한 등급별 정량적 값을 도출할 수 없는 경우 주관적 판단에 따라 값이 임의로 배분되기 때문에 등급별 정량적 값에 대한 신뢰성을 높이기 위해 CVSS(Common Vulnerability Scoring System, 이하 CVSS)에서 공격 영향인 Base Score를 산출할 때의 값을 적용했다. 취약성은 자산에 악영향을 주는 위협 수단으로 기술적 결함뿐만 아니라 구조적인 문제가 사이버 위협이 유입되는 통로로 활용된다. 취약성의 정량적 값이 의미하는 위협의 성공 가능성에 대한 값으로는 적절하지 않기에 위협의 성공 가능성에 초점을 두고 CVSS, CWSS(Common Weakness Scoring System)에서의 평가요소와 평가 척도를 적용했다.

김인경은 산출된 취약성 값이 최하점일지라도 취약성으로 인한 위협 발생 가능성은 0%라 단정할 수 없음을 고려하였지만 1개의 사이버 위협이 다른 위협에 영향을 주거나 1개의 취약점이 다른 취약점에 영향을 주지 않는 서로 독립적인 사건으로 가정[5]하여 사이버 위협 및 취약점간의 연관 관계를 분석하지 않았다.

2.3 국방부의 사이버보안 기관평가

국방부는 사이버방호 발전을 위해 노력을 지속하여 왔지만 주로 보호 및 기술적 보호 수단 구축을 중점으로 추진되었으며, 조직 전반에 대해 체계적이고 종합적인 사이버방호 관리 능력의 발전은 미흡하였다.

이에 체계적인 사이버 방호역량 강화의 일환으로 2014년 3월부터 2015년 10월까지 정보보호 관리수준 평가 시범운영을 통해 전군에 평가제도를 정착시킨 후 2016년부터 정식평가로 전환하였다[6]. 지금은 사이버보안 기관평가로 명칭을 변경하여 <표 1>과 같이 중점분야를 평가하고 있다.

<표 1> 사이버보안 기관평가 중점분야

구 분	기관평가 중점분야
사이버방호 정책	리더십, 정책관리, 조직·인원 관리, 도입사업 관리, 개인 평가
운 용	보안취약점 관리, 인증 및 권한 관리, 시스템 및 서비스 운영
감 시	침해사고 관리, 정보보호 시스템 관리, 외주용역 관리
물리적보호	정보자산, 정보시스템 보호, 정보통신 시설보호, 개인정보보호

매년 기관평가의 중점분야는 지난해 평가결과와 최신 사이버보안 트렌드를 반영하여 항목별 배점을 조정하고, 개인정보보호 분야 신설 등과 같이 신규 평가지표를 개발하여 최신화하고 있다. 이렇게 각 군 및 국방

부 소속 기관 전체의 국방 사이버보안 수준을 관리하고 있지만, 정보시스템에 대한 취약점 식별은 상급부대 및 자체 취약점 점검시 식별된 후속조치 이행 여부만 확인할 뿐, 알려지지 않은 사이버 위협에 대한 평가는 전담인력 부족으로 제한적으로 실시되고 있다.

2.4 MITRE의 방어기술(Mitigation ID)

MITRE는 사이버 킬 체인을 이용하여 전 세계 해커 그룹의 행동과 라이프 사이클을 분석하고 유형화하여 공격기술(TTPs)로 분류하였다. 또한, 공격기술(TTPs)로 실행될 수 있는 사이버 위협을 방어기술(Mitigation ID)을 통해 대응할 수 있도록 제시했다. 방어기술(Mitigation ID)은 2017년 7월 업데이트를 시작하여 지속적으로 최신화되고 있으며, 'M####' 형식으로 ID 번호가 지정되고 있다.

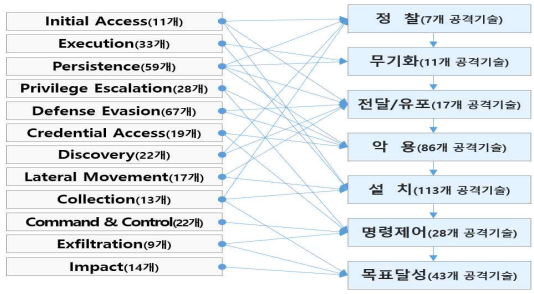
예로 들어, T1110(Brute Force) 공격기술(TTPs)은 공격자가 체계에 접근하는 암호를 알지 못하거나 암호 Hash 정보를 획득한 경우 무차별 대입 기술을 이용하여 정상적인 계정으로 로그인이 가능하다. MITRE에서는 해당 사이버 공격에 적합한 방어기술(Mitigation ID)로 M1018(User Account Management, 알려진 사용자 계정 또는 무차별 대입 시도를 감지한 후 재설정), M1027(Password Policies, 비밀번호 설정시 암호 정책 준수), M1032(Multi-factor Authentication, 외부 서비스에 대한 다단계 인증 활성화), M1036(Account Use Policies, 특정 횟수의 로그인 시도 실패 후 계정 잠금 정책 설정)[7]을 통해 사이버 방호체계에서 대응할 수 있도록 프레임워크를 제공해 주고 있다.

3. 사이버 공격기술과 방호기능 분석

MITRE에서 제안한 12가지 공격영역의 세부 공격기술(TTPs)과 방호기능간 연관 관계를 분석하기 위해 각각의 공격기술(TTPs)을 록히드마틴의 사이버 킬 체인 공격 7단계로 분류하고 국방영역에서 실행될 수 있는 공격기술(TTPs)을 식별한다. 그리고 MITRE에서 정의한 방어기술(Mitigation ID)을 기준으로 국방영역에서 운영중인 사이버 방호체계가 공격기술(TTPs)에 대응할 수 있는지 방호기능을 분석한다.

3.1 사이버 공격기술(TTPs) 분석

MITRE의 12가지 공격영역에 속한 공격기술(TTPs)의 특성을 고려하여 사이버 킬 체인 공격 7단계 별로 분류한 과정은 (그림 2)와 같으며, MITRE의 2019년 10월 기준의 공격기술(TTPs)을 활용했다[8].



(그림 2) 사이버 킬 체인 공격 7단계로 분류

사이버 킬 체인의 각 공격단계로 분류된 공격기술(TTPs) 중 우리 국방영역에 적합하지 않는 공격기술(TTPs)과 중복기술을 제외하여 235개의 공격기술(TTPs)을 식별한 결과 '설치' 단계에서 실행되는 공격기술(TTPs)이 가장 많은 비중을 차지했다.

국방영역에서 실행되는 235개의 공격기술(TTPs)과 사이버 킬 체인 공격단계, 공격대상을 분류하면 (그림 3)과 같이 구성된다. 공격기술(TTPs) 가운데 T1003 등 62개의 공격기술(TTPs)이 2가지 이상의 사이버 킬 체인 공격단계에 중복되고, T1049 등 155개의 공격기술(TTPs)은 2가지 이상의 공격대상에 중복된 것으로 1개의 사이버 위협이 다른 사이버 위협이나 다른 취약점과 연관성이 있다는 것을 확인했다.

MITRE 공격기술		사이버 킬 체인 공격단계							공격대상					
TTPs 코드	공격 TTPs명	정찰	무기화	전달/유포	악용	설치	명령제어	목적달성	네트워크	서버	단말기	응용체계	보호관리	
T1003	인증정보 획득				0	0				0	0			
T1009	바이너리 패딩		0		0					0	0			
T1011	다른 네트워크 매체를 통한 데이터 유출						0	0	0					
T1014	루트킷(RootKit)		0			0				0	0			
T1015	접근성 기능				0	0				0	0			
T1018	원격 시스템 발견	0				0				0	0			
T1027	난독화된 파일 또는 정보				0	0				0	0			
T1034	경로 차단				0	0				0	0	0		
T1041	명령 및 제어 채널을 통한 데이터 유출						0	0		0	0			
T1044	파일시스템 권한 취약점				0	0				0	0			
T1045	소프트웨어 패킹		0		0					0	0			
T1048	대체 프로토콜을 통한 데이터 유출						0	0	0					
T1049	시스템 네트워크 연결 탐지	0					0		0	0	0			

(그림 3) 공격기술(TTPs) 분류

공격대상은 국방부 국방사이버안보 훈령 제24조의 국방정보시스템 보호기준 및 보호 요구사항 중에서 정보시스템 보호기준에 따라 네트워크, 서버, 단말기(PC), 응용체계, 보호관리의 5가지 분야로 구분했다[9].

3.2 국방영역에서 운영중인 방호기능 분석

사이버 방호기능은 지난 연구[10]를 통해 2019년 한국정보보호산업협회(KISIA)에서 조사된 국내 정보보안업체가 개발한 사이버 방호체계를 네트워크, 시스템, 정보유출 방지, 암호인증, 보안관리의 5가지 방어영역 31개 사이버 방호체계 및 서비스로 분류했다[11]. 또한, 각각의 사이버 방호체계가 보유하고 있는 공통된 핵심기능을 도출하여 (그림 4)와 같이 국방영역에서 운영중인 사이버 방호기능을 분석했다.

(그림 4) 국방영역의 사이버 방호기능 분석결과

국방영역에서 운영중인 25개 사이버 방호체계가 보유한 125개 사이버 방호기능에 따른 방어유형과 방어위치는 (그림 5)와 같이 도출했다. 1개의 공격기술(TTPs)에 대응하기 위한 사이버 방호기능은 1개 이상 존재하며, 방어유형과 사이버 방호체계가 다양하게 존재한다. T1021(Remote Services, 원격 연결을 허용) 사례와 같이 공격기술(TTPs)에 대응하기 위한 방호기능은 공격의 최종종점인 서버나 단말기(PC)에서 대응능력을 보유할 수 있지만, M1027(Password Policies, 동적 비밀번호 생성) 방어기술(Mitigation ID)로 보호관리에서 공격을 약화하거나 M1030(Network Segmentation, IP 및 PORT 차단) 방어기술(Mitigation ID)로 네트워크에서 공격을 거부시킬 수 있다는 것을 확인했다.

MITRE 공격기술		방어기술		방어유형							방어위치				
TTPs 코드	공격 TTPs명	Mitigation ID	방호기능	탐지	거부	교란	약화	기만	파괴	지휘통제	네트워크	서버	단말기	응용체계	보호관리
T1021	원격 서비스	M1018	계정 관리(사용자)		0							0	0		
T1021	원격 서비스	M1018	시스템 접근제어		0							0	0		
T1021	원격 서비스	M1019	인증 로깅	0							0				
T1021	원격 서비스	M1027	동적 비밀번호 생성				0								0
T1021	원격 서비스	M1030	IP, PORT 차단		0						0				0
T1021	원격 서비스	M1031	프로토콜 필터링		0						0				
T1021	원격 서비스	M1032	일회용 비밀번호			0									0
T1021	원격 서비스	M1047	내부 시스템 이용 로깅	0								0	0		
T1021	원격 서비스	M1047	로그 수집	0								0	0		

(그림 5) T1021 공격기술(TTPs)에 대한 방어기술 (Mitigation ID)

공격기술(TTPs)에 대응하기 위해 사이버 킬 체인의 방어유형과 각 기능을 통합할 수 있는 지휘통제를 추가하여 국방영역에서 운영중인 125개의 방호기능에 대한 방어영역을 분류한 현황은 <표 2>와 같다.

<표 2> 방어유형과 방어영역간 방호기능 현황

구분	탐지	거부	교란	약화	기만	파괴	지휘통제	계
네트워크	13	7	3	6	0	0	0	29
시스템	17	5	5	1	0	2	4	34
정보유출	6	4	2	9	0	0	2	23
암호인증	6	6	1	1	0	0	0	14
보호관리	17	1	1	5	0	0	1	25
계	59	23	12	22	0	2	7	125

방어유형 중심으로 방호기능을 분류한 결과 '탐지'가 59개로 가장 높은 가운데 거부, 약화, 교란, 지휘통제, 파괴의 순으로 식별되었다. 사이버 공격으로부터 허위정보를 제공하여 진행중인 공격을 방해하는 기만 방호기능은 확인할 수 없었으며, 유입된 악성코드를 파괴하는 방호기능은 거의 식별되지 않았다. 반면에 방어영역 중심으로 방호기능을 분류한 결과 시스템(서버/단말기(PC)), 네트워크, 보호관리, 정보유출 방지, 암호인증의 순으로 고르게 식별했다.

지속적으로 사이버 위협이 지능화·은닉화·표적화·조직화 되고 응용체계, 시스템, 네트워크 등을 보호하는 단편적인 사이버 방호체계의 한계로 인하여 기만 및 파괴, 지휘통제의 방어유형에서 방호기능이 상당히 미식별 되었다. 이를 개선하기 위해 기만 및 파괴 방어유형의 역량을 향상시킬 수 있는 사이버 방호체계를 시급히 확보하고 고도화해야 한다. 또한, 서로 다른 사이버 방호체계간 실시간 탐지 및 수집된 데이터를 연관 분석할 수 있도록 지휘통제를 구축할 필요가 있다.

3.3 공격기술(TTPs)과 방호기능의 연관 분석

사이버 킬 체인의 공격단계를 기준으로 분류된 공격기술(TTPs)과 상용화된 사이버 방호체계에서 방호기능을 식별하였으며, 국방영역에 실행 가능한 235개의 공격기술(TTPs)과 각 공격기술(TTPs)에 대응하기 위한 125개 방호기능의 연관 관계를 분석하여 (그림 6)과 같이 매핑했다.

공격기술(TTPs)과 방호기능의 연관 관계 분석을 통해 다음과 같은 3가지 결과를 도출했다.

첫째, 1개의 공격기술(TTPs)에 대응할 수 있는 다양한 방호기능이 존재한다. 둘째, 1개의 공격기술(TTPs)에 대응할 수 있는 1가지 이상의 방어위치가 존재한다. 셋째, 1개의 공격기술(TTPs)에 대응하기 위해서 기존 방호기능 이외에 추가적인 방호기능을 식별하여 기만, 파괴, 교란 등 공동 대응할 수 있도록 지속적으로 연관 관계를 분석해야 한다.

4. 국방 사이버 방호수준 분석

국방영역에서 사이버 방호수준을 분석하기 위해 방어적 사이버활동 중심으로 부대 유형을 구분하고, 사이버 방호수준 분석 모델을 정의한다. 그리고 부대 유형별 운영중인 사이버 방호체계의 방호기능을 반영하여 방호수준을 분석한다.

4.1 부대 유형별 방어적 사이버활동

방어적 사이버활동은 사이버 공격 및 위협으로부터 부대 소관 영역에서 운영중인 응용체계, 서버, 단말기(PC) 등 정보시스템을 보호하는 활동이다. 사이버 방호체계를 운영하면서 침해예방 및 탐지, 조사분석, 대응 등 방어적 사이버활동 중심으로 <표 3>과 같이 부대 유형[12]을 구분했다.

<표 3> 방어적 사이버활동 중심의 부대 유형[12]

구 분	방어적 사이버활동 내용
A유형	자 군(예하부대 포함)과 타 군 대상으로 서비스 중인 응용체계와 하드웨어에 대한 사이버 방호체계를 운영, 탐지, 조사분석, 대응 등 임무 수행
B유형	자 군 및 예하부대 대상으로 서비스중인 응용체계와 하드웨어에 대한 사이버 방호체계를 운영, 예방, 탐지, 대응 등 임무 수행
C유형	상급 및 인접부대의 네트워크를 이용하여 응용체계에 접속하여 업무를 수행하며, 단말기(PC) 중심으로 예방 및 대응 등 임무 수행

(그림 6) 공격기술(TTPs)과 방호기능간의 연관 관계를 분석

4.2 사이버 방호수준 분석 모델 정의

사이버 방호체계의 방호수준을 분석시 보안 정책 설정 및 적용 수준 등 다양한 요소가 존재하지만, 부대 유형별 운영중인 사이버 방호체계는 기능이 최신 패치되어 정상적으로 운영되고 있다고 전제하고, 소관 영역에서 운영중인 사이버 방호체계의 방호수준 분석 모델(D)을 다음과 같이 정의했다.

$$D = \frac{(U_i s_j \cup U_i d_k) \cap (U_i d_k \cup U_i t_l)}{ad} \times 100$$

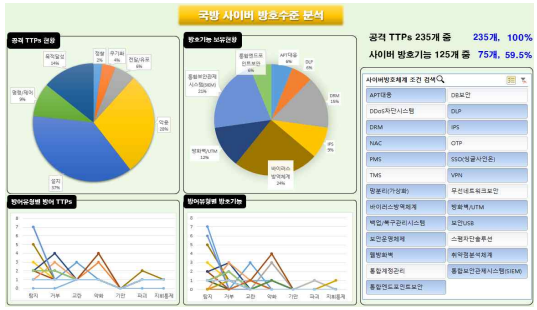
D : 부대의 소관 영역에 대한 사이버 방호수준
ad : 국방영역에서 보유중인 전체 사이버 방호기능
U_i : 부대 유형
s_j : 부대에서 운영중인 사이버 방호체계
d_k : 부대의 사이버 방호체계가 보유한 방호기능
t_l : 공격기술(TTPs)에 대응하기 위한 방어유형

사이버 방호수준 분석 모델은 첫째, 부대의 소관 영역을 보호하기 위해 운영중인 사이버 방호체계별로 보유한 방호기능을 모두 합한 전체 집합을 식별한다. 둘째, 사이버 방호기능별로 공격기술(TTPs)에 대응하기 위한 방어유형을 모두 합한 전체 집합을 식별한다. 마지막으로 첫째 집합과 둘째 집합에 공동으로 속해 있는 방호기능의 개수를 국방영역에서 보유중인 전체 방호기능 개수로 나눈 뒤 백분율화해 구한다.

4.3 사이버 방호수준 적용

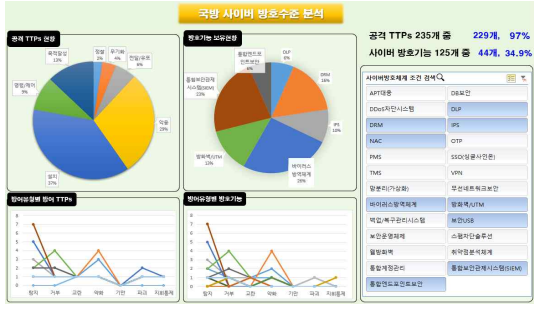
2014년 후반에 국방부 및 육·해·공군, 해병대에서 분산 운영하던 국방망 및 군 인터넷의 서버들을 국방통합데이터센터로 이전 및 이관을 실시하였으나 각 군은 업무 효율성을 고려하여 정보시스템을 일부 잔류시켰다. 각 군에서는 잔류 서버 및 응용체계를 보호하기 위해 사이버 방호체계를 구축하여 방호임무를 수행하고 있다. 앞에서 제시된 <표 3>의 기준으로 육군 내 유형에 맞는 부대를 선정하여 사이버 방호수준을 적용하였으며, 미식별된 사이버 방호체계도 존재할 수 있다.

A유형은 18개의 사이버 방호체계를 운영한다. 사이버 방호수준은 (그림 7)과 같이 공격기술(TTPs)의 100%가 실행될 수 있으며, 국방영역에서 보유한 사이버 방호기능 중 59.5%의 대응역량을 보유하고 있다.



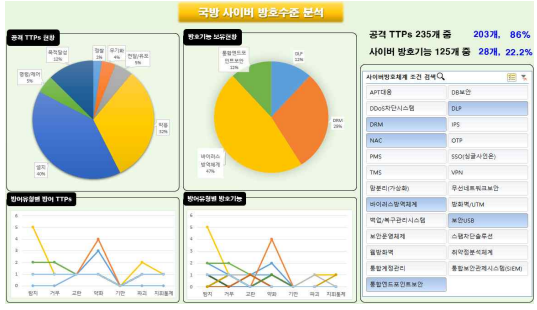
(그림 7) A유형 부대의 사이버 방호수준

B유형은 9개의 사이버 방호체계를 운영한다. 사이버 방호수준은 (그림 8)과 같이 공격기술(TTPs)의 97%가 실행될 수 있으며, 국방영역에서 보유한 사이버 방호기능 중 34.9%의 대응역량을 보유하고 있다.



(그림 8) B유형 부대의 사이버 방호수준

C유형은 6개의 사이버 방호체계를 운영한다. 사이버 방호수준은 (그림 9)와 같이 공격기술(TTPs)의 86%가 실행될 수 있으며, 국방영역에서 보유한 사이버 방호기능 중 22.2%의 대응역량을 보유하고 있다.



(그림 9) C유형 부대의 사이버 방호수준

육군 중 일부 부대의 사이버 방호수준을 살펴본 결과는 국방망 내 잔류한 서버를 운영하는 A유형의 부대는 다른 유형과 비교해 높은 대응역량을 유지하고 있으나 파괴 및 지휘통제의 방어영역에서 방호기능 확보가 필요하다. 또한, 사용자 중심, 단말기(PC)의 사이버 공격 비중이 절대적으로 높은 상황에서 B·C유형에 대해 맞춤식 방호체계로 개선이 필요하다.

공격기술(TTPs)은 부대 유형에 상관없이 86% 이상 실행될 수 있으므로, 사이버 방호체계가 미구축된 상태에서 응용체계 및 서버 등 비인가 정보시스템을 운영하는 것은 사이버 공격 및 위협에 쉽게 노출되어 정보유출 등 매우 위험한 상황으로 발전될 수 있다.

5. 결 론

본 연구를 통해 국방영역에서 운영중인 25개의 사이버 방호체계에서 125개의 방호기능을 확인하였으며, 사이버 킬 체인의 공격절차와 방어유형으로 분류한 공격기술(TTPs)을 MITRE의 방어기술(Mitigation ID)과 연관 관계를 분석하여 부대 유형별 사이버 방호수준을 제시하였다. 그러나, 사이버 공격 및 위협은 지능화·은닉화·표적화·조직화하는 등 공격기술(TTPs)이 하루가 다르게 급속도로 발전하고 있어 지속적인 사이버 위협 사례를 분석하고 현재 운영중인 사이버 방호체계의 기능 개선과 성능보강 사업을 통해 방호기능의 대응역량을 확대할 필요가 있다.

급변하고 있는 전장환경에 대비한 사이버 방호체계의 고도화 및 신규 사이버 위협의 탐지에 따라 대응결과는 달라질 수 있으나 부대 유형에 맞게 사이버 방호체계에 대한 방호수준을 평가하고 부족한 사이버 방호체계를 조기 확보한다면 국방 사이버 방호수준은 강화될 수 있을 것이다.

향후에는 국방영역에서 운영중인 사이버 방호체계 대응역량을 실시간 분석하여 부대별 방호수준을 자동으로 가시화할 수 있는 지휘통제를 구현할 것이다.

참고문헌

[1] 합동참모본부, 합동교육회장 17-1(합동사이버작전), pp. 13-18, 2017.12.

[2] 김기홍, 정보보호 관리체계(ISMS) 인증제도 발전방향, 미래창조과학부, pp. 3-7, 2017.4.

[3] 손태종 외, “국방 사이버 위협 대응체계 구축방안 선행연구(사이버킬체인 개념 중심으로)”, 한국국방연구원, pp. 18-20, 2017.4.

[4] 임규건 외, “국가정보보호수준 평가지표 개선 및 지수 산출에 관한 연구”, 한국IT서비스학회지, 제12권, 제4호, pp. 187-204, 2013.12.

[5] 김인경 외, “위험 평가 모델 기반의 정량적 사이버 보안 평가 체계”, 정보보호학회논문지, 제29권 제5호, pp. 1179-1189, 2019.10.

[6] 최인수 외, “국방정보보호 표준평가체계 연구(정보보호 기관평가체계 구축을 중심으로)”, 한국국방연구원, pp. 7, 2012.9.

[7] The MITRE Corporation, “MITRE ATT&CK”, https://attack.mitre.org/version/v9/techniques/T1110/.

[8] The MITRE Corporation, “MITRE ATT&CK”, https://attack.mitre.org/resources/updates/updates-october-2019/index.html.

[9] 국방부, 국방부 훈령, 제2361호(국방사이버안보 훈령), pp. 44-46, 2019.12.

[10] 최세호 외, “사이버 방호기능 분석을 통한 지휘통제에 관한 연구”, 한국군사과학기술학회지, 제24권, 제5호, pp. 537-544, 2021.10.

[11] 한국정보보호산업협회, 2019, 국내 정보보호산업 실태조사, 한국정보보호산업협회, pp. 149-155, 2019.12.

[12] 최세호 외, “국방 사이버 대응체계 평가를 위한 방어지표에 관한 연구”, 한국군사과학기술학회 추계학술대회, pp. 646-647, 2019.11.

〔저자소개〕

최 세 호 (Seho Choi)
2002년 2월 육군3사관학교 학사
2002년 3월 ~ 현재 국방부
2019년 9월 ~ 현재
세종대학교 정보보호학과
석사과정
email : hoseya79@naver.com

오 행 록 (Haengrok Oh)
1987년 2월 인하대학교 컴퓨터공학 학사
1989년 2월 인하대학교 컴퓨터공학 석사
2004년 8월 고려대학교 컴퓨터공학 박사 수료
1992년 1월~1998년 12월 국방정보체계연구소
수석연구원
1999년 1월~현재 국방과학연구소 수석연구원
email : haengrok@add.re.kr

윤 주 범 (Joobeom Yun)
1999년 2월 고려대학교 컴퓨터학과 학사
2001년 2월 서울대학교 컴퓨터공학과 석사
2012년 2월 KAIST 전산학과 박사
2001년 3월~2015년 2월 ETRI부설연구소
선임연구원
2015년 3월~현재 세종대학교 정보보호학과
부교수
email : jbyun@sejong.ac.kr