사이버 전투 피해평가를 위한 긴급 CAS 임무 자산 스코어링 연구

김재근, 김성중, 김국진, 이동환, 신동일, 신동규
세종대학교 컴퓨터공학과
{jaekeun0310, tjdwnd2004, kjkim, dhwlee}@sju.ac.kr, {dshin, shindk}@sejong.ac.kr

Research on Emergency CAS Mission asset scoring for cyber battle damage assesment

Jaekeun Kim, Seongjung Kim, Kookjin Kim, Donghwan Lee,
Dongil Shin, Dongkyoo Shin
Dept. of Computer Engineering, Sejong University

요 약

사이버 공격은 조직과 국가에 큰 피해를 주려는 목적으로 정보를 가로채고 파괴하는 의도적인 행동으로 빚어지는 경우가 많다. 이에 따라 국제 표준화 기구(ISO)는 ISO/IEC 27000 시리즈 등 정보 자산의 보호를 위한 표준 문서를 지침으로 제공한다. 하지만 지침만 제공할 뿐 자산 보호를 위한 구체적인 방법이나 절차가 포함되어 있지 않다. 본 연구에서는 공군의 긴급 CAS(Close Air Support) 작전을 대상으로 추후 사이버 전투 피해평가를 위해 사이버 공격에 의한 정보 자산에 대한 점수를 가산화 한다. 긴급 CAS 작전 시뮬레이션 진행 후 도출된 요소를 가지고 객관적인 수치라고 할 수 있는 CIA(Confidentiality, Integrity, Availability)지표들과 군 정보를 접목시켜 자산의 중요성을 계산하고 나아가 가중치를 주어 차별성을 가지게 된다.

1. 서론

오늘날의 정보 통신 기술 분야의 발전 추세로 볼 때 미래에는 사이버 전쟁 양상으로 나아 갈 것이 필연적이라 판단된다 [1]. 사이버 전쟁 양상으로 나아감으로써 사이버 공격 위협이 국내외를 불문하고 점점 지능적이고 고도화되고 있다. DDoS 공격이나 악성코드, 랜섬웨어, APT공격 등에 의해 네트워크, 시스템 피해를 받게 되는 경우 조직 및 국가가 정상적으로 운영이 어려울 정도로 마비가 되거나 국가 및 군 기밀자료 등이 빠져나갈 수 있다. 2017년 사이버 공격으로 인해 국내의 경제적 손실액이 약 77조 원으로 막대한 피해가 있었지만, 기업의 임원들 중 17%가 사이버 보안 투자를 비즈니스적 차별화 요소로만 생각한다 [2].

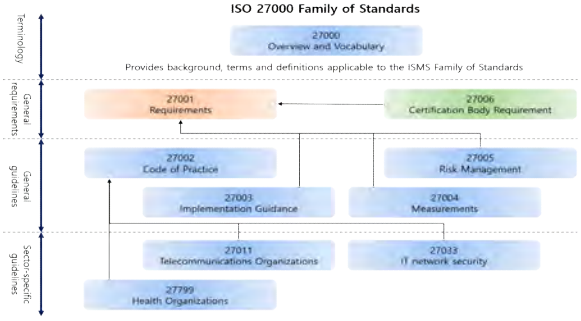
국제 표준화 기구인 ISO/IEC에서 자산을 보호하기 위한 가이드라인 문서들을 내놓았다 [3]. 하지만 ISO/IEC의 경우 지침만 제공하고 구체적인 자산 보호를 위한 방안을 제시하지는 않았다. 국내의 경우 ISO/IEC에서 내놓은 가이드라인을 가지고 다양한 연구가 이루어 지지만 정량적인 평가가 이루어질 수 없다는 문제를 가지고 있다 [4].

본 논문에서는 공군의 근접 항공 지원 작전 중 긴급 CAS 작전에 대한 시뮬레이션이 끝난 후 피해평가를 하기 위해 작전에서 사용되는 문서 및 자산 요소들을 가지고 점수를 책정하고 가 산화한다. 객관적인 수치인 CIA지표와 각 자산들을 군에 맞게 가중치를 줌으로써 차별성을 준다.

2. 관련 연구

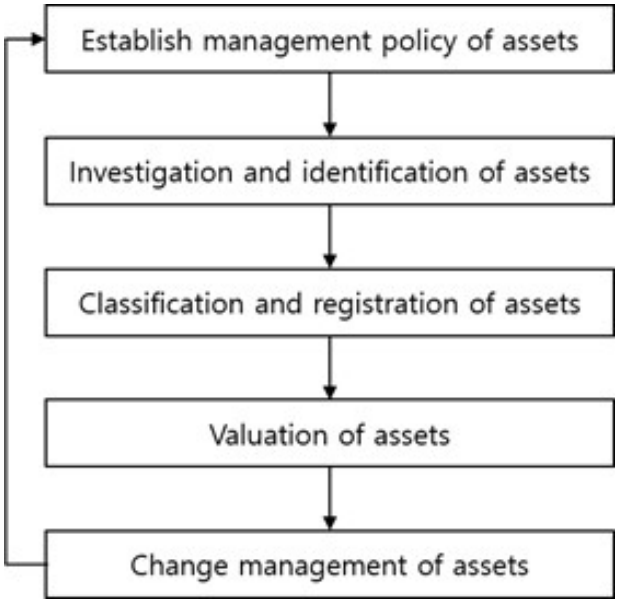
2.1. ISO/IEC 27000 시리즈

ISO/IEC 27000 시리즈는 ISO/IEC 정보보안 관리 시스템(ISMS) 표준 계열의 일부이다. ISO/IEC 27000 표준에는 ISMS를 수립과 인증에 관련된 여러 가지 약속 그리고 용어들이 정의되어있다.



(그림 1) ISO/IEC 27000 표준 시리즈 상호 관계도[5]

ISO/IEC 27001 표준은 ISMS를 수립, 구현, 운영, 모니터링, 검토, 유지 그리고 개선하기 위한 요구사항들이 명시돼 있다 [5]. ISO/IEC 27002 표준은 27001 표준을 기반하고 있다. 27002 표준은 ISMS를 구현하는 과정에서 통제를 선택하거나 일반적으로 수용되는 정보보안 통제를 구현하는 조직을 위한 지침 문서로 사용될 수 있도록 고안되었다 [6]. 또한 ISO/IEC 27000 시리즈 중 ISO/IEC 27002 표준은 ISMS의 구현을 위한 지침 문서이기 때문에 여러 자산관리 방안에 관한 연구나 논문들에서 원용하는 경향이 있다. 하단의 그림2는 27002에 정의된 자산관리 절차이다.



(그림 2) ISO/IEC 27002에 정의된 자산관리 절차[6]

ISO/IEC 27002 이외에도 ISO/IEC 27003은 구체적인 구현 권고사항 규정, ISO/IEC 27004는 개선하는 방안, ISO/IEC 27005는 위험 관리 과정을 6개의 프로세스로 구분, ISO/IEC 27006은 ISMS 인증기관 및 심사인의 자격요건, ISO/IEC 27011은 통신분야의 특화된 ISM 적용 실무지침, ISO/IEC 27033은 네트워크 시스템의 보안 관리와 운영에 대한 실무지침이다 [7].

2.2. CAS

근접항공지원(CAS : Close Air Support, 이하 CAS) 작전은 공대지 작전 중 하나로, 아군과 근접하게 대치 중인 적을 항공기로 공격하는 작전이다. 이는 지상/해상 군의 유리한 작전 여건을 조성하거나, 작전을 지원하여 군사 목표 달성에 핵심적인 임무를 수행하는 작전으로 정의한다 [8].

(그림 3) 긴급 CAS 운용 절차

그림 3은 한국에서 운용중인 긴급 CAS 운용 절차의 간략한 도식이다 [9, 10]. 적과 대치하고 있는 대대 혹은 연대 지휘관의 CAS 요청이 발생하면 항공지원 작전본부(ASOC:Air Support Operation Center)에서 요청을 종합하여 사용 가능한 CAS 자산을 각 부대에 분배한다. 그 후 명령을 지시받은 항공기가 목표를 공격하는 흐름으로 작전이 진행된다. 긴급 CAS는 요청 시간과 공격 시간 사이는 2~5분으로 틈이 짧아 빠른 의사결정이 요구된다. 이를 위하여 지휘관 결심에 근거할 지표 분석이 신뢰도를 가져야 하며 분석에 대한 명령체계의 신속한 전산처리 역시 동반되어야 한다.

3. 긴급 CAS 임무 자산 스코어링 방안

본 논문의 연구는 긴급 CAS 작전 시뮬레이션을 진행한 후 피해평가를 하기 전 임무에 관련된 자산 요소들의 중요도를 가 산화 하는 것이다. 긴급 CAS 작전을 시뮬레이션 중 자산으로 뽑은 것 중 문서는 첩보 보고서, 대대 or 연대 지휘관의 CAS 요청서, TACP의 CAS 요청서, ASOC의 CAS 승인서, ASOC의 MSN Info이다. 그중 대대 지휘관의 긴급 CAS 요청서를 가지고 기밀성, 무결성, 가용성 지표와 가중치를 통하여 자산의 중요도를 가 산화 한다. 대대 지휘관의 긴급 CAS 요청서 안 요소는 적 병력(규모), 적 전투력 수준(보병, 탱크), 적 표적 위치, 아군 소속 및 관등성명, 첩보한 위치, 긴급 CAS 작전 실시 여부, 항공기의 생존도이며 총 8개의 요소가 포함된다 [11].

가중치 지표의 경우 ISO/IEC 27002 표준을 토대로 군 정보와 접목시켜 산출하였다. 대대 지휘관의 긴급 CAS 요청서로 산출된 기밀성, 무결성, 가용성 가중치 가 산화 지표 예시는 다음과 같다.

<표 1> 기밀성 지표

기밀성 지표	1	2	3	4	5	점수	가중치
<기밀성 지표>							
정보의 노출 방지 필요 수준					✓	5	상
정보의 열람 수준이나 열람 대상을 제한할 필요성			✓			3	삼
정보의 내·외부 노출 시 예상할 수 있는 악용범위				✓		4	상
정보의 무단 노출 시 피해 발생 가능성				✓		4	상
정보를 열람한 사실을 확인하는 감사기록의 필요성		✓				2	정
정보의 비인가 노출이 군 업무수행에 미치는 영향					✓	5	상
정보와 군의 인사정보에 대한 관련성			✓			3	삼
정보의 무단 노출 시 군의 재정에 미치는 영향	✓					1	상
정보와 군이 국민에게 제공하는 서비스에 대한 관련성	✓					1	상
정보와 시스템 개발에 대한 관련성		✓				2	상
<공동 지표>							
정보와 진행 중인 연구 및 개발 프로젝트에 대한 관련성		✓				2	하
정보와 군의 재정에 대한 관련성			✓			3	하
정보와 재난 감시 및 예측에 대한 관련성					✓	5	하
정보와 에너지에 대한 관련성		✓				2	하
정보와 군 관계자의 개인 정보에 대한 관련성		✓				2	하

기밀성 분류 지표의 경우 표1에 제시한 바와 같이 기밀성 지표 10개, 공동지표 5개로 구성된다. 기밀성 지표의 가중치를 "상"으로 공동지표 5개의 경우 가중치는 "하"로 적용한다.

<표 2> 무결성 지표

무결성 지표	1	2	3	4	5	점수	가중치
<무결성 지표>							
정보의 수정·삭제를 감시하는 감사기록의 필요 수준					✓	5	상
정보가 무단으로 변조·삭제될 경우 악용범위					✓	5	삼
정보의 무단 변조·삭제를 방지하기 위한 특정한 도구 및 방법의 필요 수준				✓		4	상
정보에 접근하기 위해 공인 인증서를 사용해야 할 필요성	✓					1	상
정보가 무단 변조·삭제될 경우 정상적인 업무 수행에 미치는 영향					✓	5	상
정보와 지적재산권·개인정보 등과의 관련성			✓			3	상
정보와 군의 비상계획과의 관련성				✓		4	삼
정보와 안보 및 외교와의 관련성	✓					1	상
정보와 국가 주요 인프라 정보와의 관련성					✓	5	상
정보가 군 외부로 공개될 시 요구되는 신뢰도 수준			✓			3	상
<공동 지표>							
정보와 진행 중인 연구 및 개발 프로젝트에 대한 관련성		✓				2	하
정보와 군의 재정에 대한 관련성			✓			3	하
정보와 재난 감시 및 예측에 대한 관련성					✓	5	하
정보와 에너지에 대한 관련성		✓				2	하
정보와 군 관계자의 개인 정보에 대한 관련성		✓				2	하

무결성 분류 지표의 경우 표2에 제시한 바와 같이 무결성 지표 10개, 공동지표 5개로 구성된다. 무결성 지표의 가중치를 "상"으로 공동지표 5개의 경우 가중치는 "하"로 적용한다.

<표 3> 가용성 지표

가용성 지표	1	2	3	4	5	점수	가중치
<가용성 지표>							
정보의 상시 접근 및 사용이 보장될 필요성		✓				2	상
군의 고유 업무를 지속적으로 지원하기 위한 정보의 필요성				✓		4	상
정보에 접근하고 사용하는 범위					✓	5	상
정보의 사용·접근의 방해 시 예상 가능한 악용범위					✓	5	상
재해 및 공격의 발생 시 예상되는 정보의 복구 우선순위				✓		4	상
정보의 사용·접근 방해 시 군의 정상적인 업무 수행에 미치는 영향				✓		4	상
정보의 사용·접근 방해 시 재정에 미치는 영향		✓				2	상
정보의 사용·접근 방해에 대비하여 정보에 대한 접근 방식을 이중화할 필요성					✓	5	상
정보의 백업 필요성	✓					1	상
정보의 재무 및 회계와 관련성	✓					1	상
<공동 지표>							
정보와 진행 중인 연구 및 개발 프로젝트에 대한 관련성		✓				2	하
정보와 군의 재정에 대한 관련성			✓			3	하
정보와 재난 감시 및 예측에 대한 관련성					✓	5	하
정보와 에너지에 대한 관련성		✓				2	하
정보와 군 관계자의 개인 정보에 대한 관련성		✓				2	하

가용성 분류 지표의 경우 표3에 제시한 바와 같이 가용성 지표 10개, 공동지표 5개로 구성된다. 가용성 지표의 가중치를 "상"으로 공동지표 5개의 경우 가중치는 "하"로 적용한다.

기밀성, 무결성, 가용성 가중 점수는 각 지표별 척도와 가중치를 곱한 값의 항목 가중치를 나누어 산출한다. 표4의 임무 자산 중요도 점수의 경우 각 가중 점수를 더해서 지표 수 만큼 나누게 된다. 가중 점수와 임무 자산 중요도는 "상","중","하"로 구분하며 각각의 범위로는 "상"등급은 3.30~4.89, "중"등급은 1.70~3.29, "하"등급은 0~1.69로 규정한다.

가중치 공식은 다음과 같다.

$$\text{가중평점} = \sum(\text{지표척도} \times \text{가중치}) / \sum(\text{항목의가중치})$$

"상"등급 정보 : $3.30 \leq$ 가중 평점 ≤ 4.89

"중"등급 정보 : $1.70 \leq$ 가중 평점 ≤ 3.29

"하"등급 정보 : $0 \leq$ 가중 평점 ≤ 1.69

가중치 공식을 적용한 결과는 다음과 같다.

<표 4> 대대 지휘관의 CAS 요청서 임무 자산 중요도

구 분	기 밀 성	무 결 성	가 용 성
평균 점수	2.93	3.33	3.13
가중 점수	2.96	3.44	3.20
등 급	중	상	중
임무 자산 중요도	3.20(중)		

표 4의 결과를 보면 대대 지휘관의 CAS 요청서에 대한 임무 자산 중요도는 3.20으로 (중) 등급에 들어가게 된다. 이처럼 임무 자산 중요도 점수를 책정하고 등급화한다면 사이버 공격에 대한 자산 관련 피해평가는 수월해질 것이다. 다만 가중치가 있는 만큼 모든 지표 척도를 중요하다고 판단하게 되면 임무 자산 중요도가 상향될 가능성이 있다는 점은 보완해야 할 문제이다.

4. 결론

본 논문에서는 긴급 CAS 시나리오 중 대대 지휘관의 CAS 요청서를 ISO/IEC 27002 기반의 기밀성, 무결성, 가용성 임무 자산 가중치 지표를 산출하였다. 산출한 임무 자산 가중치 지표들을 이용하여 임무 자산 중요도 점수 산출하는 방법을 제시하였다.

기밀성, 무결성, 가용성 가중치 지표의 가중치 공식을 적용하여 영향도를 "상","중","하"로 등급화 하였으며, 최종적으로 문서가 가진 등급과 점수를 결정하게 된다.

이를 발전시켜 가중치 조정과 모든 지표 척도를 중요하다고 판단하게 되면 임무 자산 중요도 점수가 상향될 가능성이 있는 점을 보완할 예정이다. 추후 가 산화한 임무 자산 중요도 점수를 가지고 사이버 공격 피해평가에 반영하여 사이버 공격 별 얼마나 임무 자산피해를 받는지 산출할 예정이다.

ACKNOWLEDGMENT

“본 연구는 방위사업청과 국방과학연구소의 지원으로 수행되었습니다(UD190016ED).”

참고문헌

[1]오제상, "미래 사이버전 능력 필요",국방과 기술, 272호, 52-57, 2001

[2]Frost&Sullivan, Microsoft, “Understanding the Cybersecurity Threat Landscape in Asia Pacific: Securing the Modern Enterprise in a Digital World,”Frost&Sullivan and Microsoft Corp., Korea, Jun. 2018.

[3]Disterer, G. (2013) ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal of Information Security, 4, 92-100.

[4]나관식,"정보 보호 관리 체계(ISMS)의 국제 표준과 국내 표준 비교",과학과 문화, 제 8권 27호, 23-36, 2011. 2

[5]Information technology-Security techniques-Information security management systems-Requirements, ISO/IEC 27001, 2013.

[6]Information technology-Security techniques-Code of practice for information security controls, ISO/IEC 27002, 2015.

[7]윤현수. "사이버 정보 자산의 분류 및 정량적 중요도 산출에 최적화된 지표 설계", 세종대학교 석사학위논문(2019)

[8]Joint Chiefs of staff. Close Air Support., Joint Publication 3-09.3, Jul. 2009

[9]공군본부, 공군 기본교리, 2007.

[10] 장용진; 이태공; 김영동. 긴급 근접항공지원작전 전력 분배 방법. 한국통신학회논문지, 39.11: 1050-1067,2014.

[11]장용진. "긴급 근접항공지원작전 전력 분배 모델",아주대학교 석사학위논문(2015)