사이버 위협 대응을 위한 軍 정보화자산관리시스템과 연계한 軍 취약점 관리 방안

김 종 화*, 임 재 성**

요 약

우리 軍의 사이버 공간은 적으로부터 지속적인 위협을 받고 있다. 이 같은 사이버 위협에 대응하기 위해 軍 정보화 자산에 대한 취약점을 조기에 식별하고 제거하여야 한다. 그러나 현재 우리 軍은 취약점에 대한 체계적인 관리가 미흡한 실정이다. 따라서 본 논문에서는 취약점 관리에 대한 각 국의 동향과 軍 취약점 관리 실태를 조사하고, 이를 바탕으로 軍 정보화 자산에 대한 효율적인 취약점 관리를 위해 취약점 데이터베이스와 軍 정보화자산관리시스템을 연계·구축하는 방안을 제시하였다.

Military Vulnerability Management Plan based on Military IT Asset Management System for Cyber Threat Response

Jong Hwa Kim*, Jae Sung Lim**

ABSTRACT

The Cyber space of the ROK Army is constantly threatened by enemy. In order to reponse to such cyber treats, vulnerabilities of information assets of the ROK Army should be identified and eliminated early. However, the ROK Army currently lacks systematic management of vulnerabilities. Therefore, this paper investigates trends of each country's vulnerability management and the actual situation of the management of the vulnerabilities in the ROK Army, and suggests ways of linking vulnerability database and the ROK Army information asset management system for effective vulnerability management of the ROK Army information assets.

Key words : Military information security, Cyber threat response, Vulnerability

접수일(2018년 2월 27일), 수정일(1차: 2018년 3월 23일), 게재확정일(2018년 3월 30일)

* 아주대학교 / NCW학과

** 아주대학교 / NCW학과 (교신저자)

1. 서 론

1차 산업혁명은 기계의 발명으로 인한 자동화의 탄생, 증기기관의 발명을 통한 국가 간의 연결성을 촉진시켰다. 2차 산업혁명은 자동화를 통해 대량 생산이 가능하게 되면서 시작되었고, 노동부문에서의 효율적이고 생산적인 연결성을 촉진하여 대량생산체제를 가능하도록 하였다. 3차 산업혁명은 전자장치, ICT (Information & Communication Technology)를 통한 급진적인 정보처리능력의 발전과 이를 통한 정교한 자동화가 가능해 졌다. 최근 이슈가 되고 있는 4차 사업업 혁명은 인공지능을 통한 자동화 와 연결성이 극대화 되는 단계를 의미하고 있다[1][2].

현재 우리나라는 유엔의 전자정부발전지수 1위 등 정보화 진전은 세계 어느 나라에 뒤지지 않는 선진국 수준에 도달해 있다. 반면에 이를 악용하여 개인정보 등 중요 자료를 2009년 이후 격년 단위로 자주 발생하고 있다. 대표적인 사례로는 7.7 및 3.4 DDoS 공격, 농협 전산망 사이버테러, 3.20 방송 및 금융 사이버테러와 한수원 해킹 등이 있다. 최근 미국의 소니 픽처스사, 영국의 BBC 해킹 등으로 판단해 보았을 때 정보유출이나 해킹 등 사이버 위협 문제는 우리나라 뿐 만 아니라 선진국 모두에게 해결해야 할 큰 현안으로 대두되고 있다[3].

특히 북한이 우리 사회의 취약한 전산망에 대한 충분한 사이버 공격 능력을 갖추고 있어 다양한 대규모의 사이버공격을 시도할 것으로 예상된다. 북한은 수차례 우리사회 기간망에 대한 공격을 통해 우리의 취약점을 속속들이 파악해 왔다. 사이버 테러를 자행할 때마다 공격 목표를 바꾸고 기술적으로 다양한 기능을 추가하는 등 점점 더 정교해지고 있다[4].

이에 民·官·軍은 지능화되어가는 사이버 위협으로부터 정보화 자산을 보호하기 위해 다양한 정보보호체계와 각종 솔루션을 도입하여 운용하고 있으나, 정보보호체계와 솔루션이 가지고 있는 성능의 한계와 이를 우회하여 공격하는 새로운 사이버 위협은 계속되고 있다. 이러한 사이버 위협에 대응하기 위해 매번 정보보호 솔루션을 도입하는 것은 매우 비효율적인 대책으로 방어자의 입장에서 최선의 대책은 취약점이 공지되면, 조직이 보유하고 있는 정보화 자산을 대상으로 해당 취약점이 있는지 식별하고 이를 제거하는 조치를 통해 취약점이 있는 정보화 자산을 외부에 노출시키는 시간을 최소화 시키는 것이다.

따라서 본 연구에서는 軍이 보유하고 있는 정보화 자산 내 취약점 식별과 처리절차를 연구하여 사이버 위협으로부터 정보화 자산을 안전하게 보호하기 위한 방안을 제시한다. 2장은 취약점 관리를 위한 각 국의 동향과 軍 취약점 관리 실태를 알아보고, 3장에서는 軍 취약점 관리를 위해 취약점 데이터베이스와 연계하여 정보화 자산에 대한 취약점을 어떻게 식별하고 제거하여야 안정성을 확보할 수 있는지에 대한 방안을 제시한 후, 4장에서 결론을 맺겠다.

2. 관련 동향 및 軍 취약점 관리 실태

취약점 관리는 컴퓨터 정보자산의 기밀성 또는 가용성을 손상시키는데 사용될 수 있는 취약점을 파악하여 제거하는 과정으로 악의적 해커가 컴퓨터 정보자산을 손상시키는데 사용되기 전에 취약점을 파악하여 제거하는 예방차원의 정보보안 수단이다[5].

그러면, 정보화자산에 대한 취약점 관리를 위해 각국의 동향과 우리 軍의 취약점 관리 실태를 먼저 살펴보겠다.

2.1 각 국의 동향

1990년대부터 취약점 관리에 앞장 선 미국은 미국 표준기술연구소에서 통합 취약점 DB인 NVD(National Vulnerabilities Database)를 구축하여 소프트웨어 벤더들로부터 취약점 정보 및 자금 지원을 받으며, 취약점 관리 자동화 서비스를 제공하고 있다. 또 NVD 이외의 취약점 DB가 생겨나자, 서로 다른 취약점 DB가 상이한 분석을 내놓을 수 있다는 우려 때문에 사이버 보안 정보공유 프로젝트를 추진하여 정형화된 기준에 의한 정보공유모델인 CVE(Common Vulnerabilities and Exposures)를 구축했다. 이를 바탕으로 적합한 취약점 관리체계와 통합 취약점 DB를 구축했으며, 최근 이를 프로토콜로 규정하고 일본, 중국, 유럽과의 연계체계를 통해 취약점 관련 정보를 제공하고 있다.

일본은 2000년대부터 미국의 취약점 분류체계, 평가체계와 전반적인 취약점정보를 활용해 다양한 서비스

를 민간이나 기업 등에 제공하고 있다.

중국은 4만 여개의 취약점 정보를 제공하는 통합 취약점 DB를 구축·운영하는 등 보안 취약점 관리 체계를 완비했고 유럽 또한 EU의 각 회원국 컴퓨터비상대응팀(CERT)이 취약점 관리체계를 구축하고 있는 것으로 나타났다.

국내에서도 2000년 초반 미국의 NVD나 CVE를 벤치마킹한 KCVE의 구축을 계획했지만, 현재 진행사항에 대해 알 수 없었으며, 2010년에도 취약점과 관련된 국가차원의 연구는 일부 있었으나 취약점에 대한 체계적인 관리와 공유 또는 통합된 DB가 존재하지 않는다[6][7].

2.2 軍 취약점 관리실태

현재 軍은 국방정보화 사업 예산으로 획득 혹은 운영·유지하는 IT 자산과 책임운영기관의 예산으로 운영·유지하는 IT 자산, 軍에서 개발한 응용SW를 국방정보자원관리시스템인 DRIMS(Defense IT Resource Information Management System)에 입력하여 자산을 관리를 하고 있으며, 軍이 자체 개발하는 응용SW 자산에 대해서는 SW개발관리시스템을 이용하여 개발관리와 개발 이후의 프로그램 소스코드 관리 등 형상관리를 실시하고 있다[8][9][10].

軍은 취약점 관리를 위해 획득된 정보화 자산 중 정보체계에 대해 매년 국방정보체계 취약점 분석 및 평가 실무지침서를 기준으로 취약점 점검계획에 의거 취약점을 식별하여 제거함으로써 안정성을 확보하는 노력을 하고 있으며, 軍 정보화 자산에 대한 취약점 식별과 제거는 (그림 1)과 같은 절차와 수단에 의해 취약점 관리를 수행하고 있다.

(그림 1) 현행 취약점 관리절차

세부적인 취약점 식별 및 제거 절차를 다음과 같다. 위협정보공유로 획득한 취약점 정보는 침해대응시스템을 통해 상황실로 취약점이 전파되면 Step1) 해당 취약점을 접수 후, <표 1>과 같이 전자결재시스템의 메모보고 형식으로 전 부대 정보보호부서 및 정보체계 운영부서로 전파한다.

<표 1> 취약점 주요 전파내용

구 분	내 용
관련근거	국방사이버안보훈령 0장 0조 정보작전방호태세규정 0장 0조
주요내용	취약제품, 취약점 정보 등
조치사항	공식 패치사이트, 버전정보 등
보 고	부대별 조치내용 등

Step2) 전파를 받은 부대의 정보보호부서는 해 부대 정보체계 운영부서와 협조하여 해당 취약점을 지닌 정보화 자산의 보유여부를 자산관리자와 개발자가 개별적으로 확인하여 보고 후, 해당 취약점에 대한 후속조치를 실시하고 Step3) 취약점 조치결과를 최초 전파된 메모보고에 부대별 의견으로 보고하는 절차로 수행하고 있다.

그러나 현행 취약점 식별 및 제거절차는 다음과 같은 문제점을 갖고 있다. 첫째, 전파된 취약점을 관리하는 별도의 데이터베이스가 없어 취약점에 대한 이력관리가 전혀 이루어지지 않고 있으며 둘째, 취약점을 지닌 정보화자산 식별은 해당 정보화 자산관리자와 개발자에 의해서만 확인이 가능하기 때문에 신속한 자산식별이 제한되며 셋째, 취약점 조치를 위한 후속조치 방안 수립 및 시행을 위한 주무부서의 선정절차가 신속하게 이루어지지 못하고 있다.

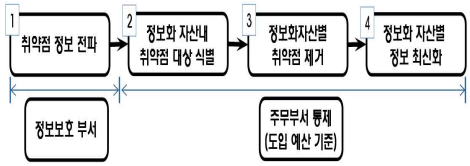
결국 이러한 문제점들을 해결하지 않으면 사이버 위협의 주요원인인 취약점을 제거하는데 많은 시간이 소요되어 취약점을 지닌 정보화자산을 외부에 장기간 노출시킬 수밖에 없게 된다. 따라서 이러한 문제점을 해결하기 위한 효율적인 취약점 관리방안이 필요하다.

3. 효율적인 軍 취약점 관리방안

앞서 2장에서 살펴본 바와 같이 취약점 관리는 세계적인 추세임에도 불구하고 軍은 취약점 관리에 대한 구체적인 임무정립과 세부 절차가 미흡한 실정으로, 이를 보완하기 위해 軍 취약점 관리에 대한 절차와 이를 구현하기 위해 취약점 정보의 저장, 취약점 대상인 자산 식별, 자산의 정보변경 등을 위한 취약점 관리구조를 제안하고자 한다.

3.1 취약점 관리 절차

취약점 관리 절차를 정립하기 위한 첫 출발은 취약점 관리를 누구의 임무로 할 것인지에 대한 것으로 이것이 전제 되지 않으면 신속한 취약점 조치는 기대하기가 어렵다. 따라서 본 논문에서 제안하고자 하는 취약점 관리에 대한 임무분장은 (그림 2)와 같이 모든 취약점 전파는 정보보호부서에서 실시하되, 취약점 후속조치와 관련된 업무는 취약점을 지닌 정보화 자산을 도입한 예산을 기준으로 후속조치 주무부서를 선정 후, 해 부서가 주도적으로 해당 취약점에 대한 후속조치를 시행하는 것을 제안하고자 한다.



(그림 2) 예산관점의 취약점관리 임무분장

예를 들면, 정보체계 부서의 예산으로 도입된 정보화 자산의 경우에는 취약점 조치의 주무부서는 운용부서가 되며 정보보호부서의 예산으로 도입된 정보화 자산일 경우에는 정보보호 부서가 주무부서가 되어 전파된 취약점의 위험도를 근거로 그 영향성을 판단하여 해당 서비스를 계속 지원할 지 또는 중지할 지에 대한 정책적 결정을 내리고 취약점에 따라 단순한 패치 또는 제조사와의 협업을 통해 패치 등을 시행하고, 신규사업 추진 시 관련 취약점은 사업 제안요청서에 반영하는 등 신속한 취약점 조치와 관련 업무에 반영시키는 일련의 조치를 수행하여야 한다.

다음은 효율적인 취약점 관리를 위한 軍 취약점 관리절차로 취약점관리시스템 구축을 전제로 아래 (그림 3)과 같다.

구 분	Step1	Step2	Step3
조치사항	① 취약점 접수/입력 ② 관련 부대(서) 전파 ③ 조치 방안 검토/시행	① 취약점 자산식별 ② 취약점 제거	① 취약점이력관리
활용수단	① 취약점관리시스템 ② 침해대응시스템 ③ 전자결재시스템	① 취약점관리시스템 ② 자산관리시스템 (DRIMS, 개발관련 시스템)	① 취약점관리시스템 ② 자산관리시스템 ③ 전자결재시스템

(그림 3) 제안하는 취약점 관리절차

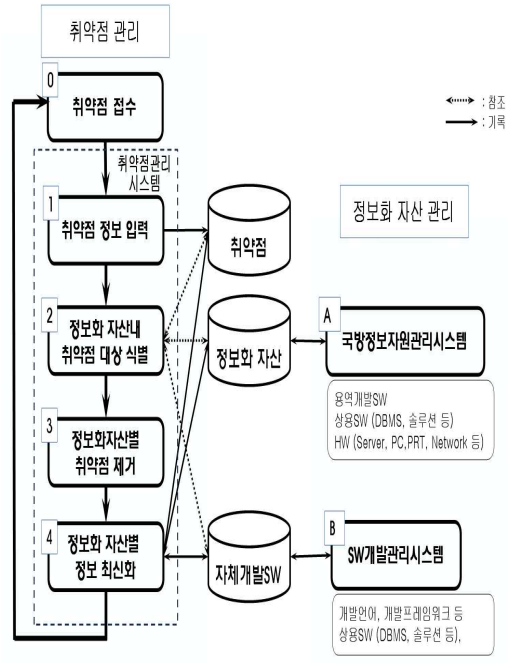
먼저, Step1) 정보보호부서는 취약점이 침해대응시스템으로 전파되면 취약점관리시스템을 이용하여 취약점을 입력하고 관련 취약점을 정보체계 운용부서와 정보보호 부서로 전파하고 취약점 관리 주무부서에서는 서비스 지속여부 판단과 취약점 제거를 위한 후속조치 방안을 검토 후, 선정·하달한다. Step2) 각급제대 주무부서는 자산관리 시스템과 연계된 취약점관리시스템을 통해 취약점 조치대상 정보화 자산목록을 식별하고, 식별된 정보화 자산에 대해 취약점 제거 조치를 통해 보유한 정보화 자산에 대한 취약점 제거업무를 수행한다. Step3) 취약점 제거가 완료되면 정보보호부서는 취약점관리시스템에, 주무부서는 자산관리시스템에 해당 취약점에 관한 이력을 입력하여 해당 취약점에 대한 조치를 완결한다.

3.2 취약점 관리구조

취약점 관리구조란 그동안 일회성으로 처리하던 취약점 조치를 (그림 4)와 같은 취약점 관리 생명주기를 기반으로 앞서 제안한 취약점 관리절차와 그 절차에서 사용하는 취약점관리체계 및 정보화자산관리체계의 연계를 통해 취약점을 관리하는 기반구조를 말한다.

(그림 4) 취약점 관리 생명주기

본 논문이 제안하고자하는 軍 취약점 관리를 위한 취약점 관리구조는 (그림 5)와 같이 취약점 관리와 정보화자산관리의 2개 영역이 연계되어 구조화되며 관리구조의 업무흐름을 모듈별로 설명하면 다음과 같다.



(그림 5) 취약점 관리구조

⓪ 모듈 : 외부 사이버 위협 정보 공유체계에 의해 신규 취약점 접수(CVE 기준)

① 모듈 : 해당 취약점은 취약점 DB에 취약점 관리를 위한 기초 데이터로 관리되며 향후 취약점별 정보화자산 정보 이력 관리

② 모듈 : 軍내 국방정보자원관리시스템과 SW개발관리시스템에 의해 생성된 정보화자산 DB와 자체개발 SW DB를 대상으로 취약점 조치대상 자산 보유여부를 확인 후, 취약점을 지닌 정보화자산 목록 산출

③ 모듈 : 해당 취약점에 대한 후속조치 시행

④ 모듈 : 정보화 자산 DB 및 자체개발SW DB에 해당 취약점 관련 정보이력 최신화 및 취약점 DB에 관련 정보화 자산 이력 최신화 관리

Ⓐ 모듈 : 국방정보자원관리시스템에 의해 용역 개발SW, 상용SW(DBMS, 솔루션 등), HW(서버, PC, 프린터, 네트워크 장비 등) 관련 정보화자산 DB 최신화 관리

Ⓑ 모듈 : SW개발관리시스템에 의해 개발언어, 개발프레임워크, 상용SW(DBMS, 솔루션 등) 자체개발 SW DB 최신화 관리

제안한 취약점 관리구조는 사이버 위협으로부터 정보화 자산을 안전하게 지키기 위한 취약점 관리 도구로서 軍 정보화 자산의 안정성을 확보에 기여할 수 있을 것이다.

4. 결론 및 향후연구

본 논문을 통하여 우리는 취약점 관리절차와 관리구조를 제안함으로써 취약점 업무 수행 간 현업에서 발생하는 다양한 문제점을 해결하고 신속한 취약점 식별 및 제거를 위한 정보화 자산의 안정성을 확보하는 방법을 제시하였다.

특히 취약점 발생 시 후속조치를 위한 신속한 주무부서 선정절차는 빠른 의사결정을 통해 취약점을 조기에 식별하여 제거할 수 있는 기회를 제공할 수 있을 것이다.

향후 연구할 분야는 본 논문이 제안한 관리구조를 실제 구현하기 위해 위협정보공유체계를 활용한 취약점 관리시스템의 설계와 현재 軍이 구축·운영 중인 정보화자산관리시스템 내 취약점 식별이 신속하게 이루어질 수 있도록 개선방안을 세분화하여 연구할 필요가 있다.

이를 통해 관리구조가 체계화 되면 정보화 자산 정보와 연계된 취약점 전반에 대한 이력관리로 정보체계의 안정성을 확보함으로써 제 5전장이라고 일컫는 사이버 공간을 안전하게 지키는데 기여하게 될 것이다.

참고문헌

[1] Baweja, B., et al. "Extreme automation and connectivity: the global, regional, and investment implications of the Fourth Industrial Revolution. "UBS White Paper for the World Economic Forum Annual Meeting. 2016.
[2] 헌승천, 백용재, "4차 산업혁명 시대의 미디어 서비스의 한국통신학회지, 제7권 별책 : 정보와 통신 열린강좌, pp22~31, 2017.11.
[3] 윤오준 외 3명, "사이버공격 대응 분석을 통한 사이버안보 강화 방안 연구", 융합보안학회지, 제15권, 제4호, pp.71~78, 2015.06.
[4] 정영도 외 1명, "북한 사이버공격에 대한 대응방안에 관한 연구", 융합보안학회지, 제16권, 제6호, pp.43~50, 2016.10.
[5] 국방기술품질원, 국방과학기술용어사전, http://www.dtaq.re.kr, 2011.
[6] 한국인터넷진흥원, "정보신기술 취약점 관리체계 구축(안)", 2010.8.
[7] 김지선, "늘어나는 SW보안사고 취약점 관리체계 급선무", 디지털타임즈, 2010.11.30.
[8] 한국인터넷진흥원, "소프트웨어 보안 취약점 평가체계 연구", 2013.8.
[9] 국방부, "국방정보 자원관리 지시", 2016.7.
[10] 육군본부, "육군 SW개발/관리 지시", 2017.6.

〔저자소개〕

김 종 화 (Jong-hwa Kim)
2001년 국방대학원 전산정보 석사
현 재 아주대학교 NCW학과
박사과정
email : joaakim@hanmail.net

임 재 성 (Jae-sung Lim)
1983년 아주대학교 전자공학 학사
1985년 한국과학기술원 전자공학 석사
1994년 한국과학기술원 전자공학 박사
email : jaslim@ajou.ac.kr