정 보 보 호 학 회 지
제23권 제6호, 2013. 12

국방망의 지속적인 실시간 보안관리체계

권 오 훈*, 이 명 훈**, 이 재 우***, 임 채 호****

요 약

컴퓨터와 네트워크 기술이 발전하면서 물리적으로 분산되어 있던 시설들이 논리적으로 통합 관리되고 있다. 이 시대에 맞춰 국방부 또한 "국방정보화" 라는 단어를 통해 국방체계를 IT 중심의 군 체계로 전환하고 있는 가운데 네트워크 전체를 마비시키는 사이버 위협은 날이 갈수록 늘어나는 상황이며 사이버 안보에 있어 외부로부터의 침입을 막고 내부로부터의 유출을 막기 위한 실시간 보안관리는 점점 더 중요해지고 있는 상황이다. 또한 군사기반시설에 대한 관리적 및 기술적 환경측면에서 발생할 수 있는 보안 사고에 대응하기 위하여 실시간 보안관리 체계는 수립단계부터 세부적인 평가가 반드시 수행되어야 한다. 이에 본 논문은 국외 관리체계 및 국내기업 우수사례 분석을 통해 보호체계 수립단계에서 세부적인 평가단계까지 실질적으로 보안에서 중요시하는 관리적, 기술적, 개인정보에 근거한 실시간 보안관리 체계를 통하여 군에 효과적으로 적용할 수 있는 국방망의 지속적인 실시간 보안관리 체계를 제안한다.

Ⅰ. 서 론

컴퓨터와 네트워크 기술이 발전하면서 물리적으로 분산되어 있던 시설들이 논리적으로 통합 관리되고 있다. 분산되어 있던 시설들이 통합 관리를 통해 관리할 수 있도록 했지만 반대로 공격자는 특정 시설에 대한 공격이 성공했을 때 모든 것을 공격할 수 있는 권한을 얻을 수도 있다. 이처럼 개별관리보다 통합관리로 전환됨에 따라 보안은 더욱더 중요하여 여겼다. 국방부 또한 이러한 흐름에 맞춰서 국방정보화라는 단어를 통해 국방체계를 IT중심의 군 체계로 전환하고 있다. 국방정보화는 미래 정보전을 대비한 네트워크 중심의 디지털 전장 관리체계, 효율적인 국방자원 관리체계를 구축, 국방정보 환경의 고도화를 추구하고 있다[1].

하지만 보안이라는 것은 사회와 IT 기술의 발달, 사람에 의해서 계속해서 취약점이 발생할 수밖에 없으며 국방망 또한 기존의 사기업과 마찬가지로 보안 에 취약할 수밖에 없다. 게다가 물적·인적 피해를 입힐 수 있는 군사시설은 더욱더 보호에 신경을 써야 한다.

공격자들은 취약점을 이용해 특정 군사 시설 혹은 네트워크망 공격을 감행한다. 3.20 사이버테러는 군사시설에 직접적인 타격을 가한 것은 아니지만, 기존 사기업의 네트워크망을 마비시킴을 보여줌으로써 불능상태만으로도 막대한 손해를 끼칠 수 있다는 것을 증명하였다. 1.25대란은 SQL서버의 취약성을 이용한 공격이고, 이는 인터넷 망을 통한 전산시스템 마비를 초래하였다. 기존의 국방망은 물리적으로 분리되어 있지만 인터넷과 연결되어 있는 망으로써 인터넷을 통한 공격에 충분히 취약할 수 있다. 이렇게 사이버위협은 강력한 무기로써 적대국에게 충분히 군사적 영향을 끼칠 정도로 위협적인 무기가 되었다. 대표적인 예로 Estonia 사태를 들 수 있다. 동유럽의 정보통신강국이라 불리었던 이 나라는 DoS, 애플리케이션 공격, Spam Mail, Web Site Defacement, Phishing 등 5개의 공격에 의해 통신망이 마비되고 말았다. 공격자, 혹은 조직에 의한 동시다발적 공격이 아니라 러시아에 의한 공격으로 밝혀졌다. 적대

본 연구는 지식경제부 및 한국인터넷진흥원의 "고용계약형 지식정보보안 석사과정 지원 사업"의 연구결과로 수행되었습니다.
본 연구는 KAIST 정보보호대학원의 연구지원으로 수행되었습니다.
* 동국대학교 국제정보대학원(ohkwon@dongguk.edu)
** 동국대학교 국제정보대학원(kuki2012@gmail.com)
*** 동국대학교 국제정보대학원(jwlee0904@paran.com)
**** 카이스트 정보보호대학원(chlim@kaist.ac.kr)

국이 존재하는 IT강국인 우리나라도 분명 예외가 될 수 없는 상황이다. 오하이오 핵발전소의 사례는 완벽하게 분리되어 보호되면 안전하다고 하는 사실을 깨트린 대표적인 사례이다. 공격자는 취약점을 이용하여 APT공격을 시행하였다. 이 사례들은 완전한 보호는 어디에도 없으며 보호에 관한 체계적인 관리가 필요하다는 것을 증명한다.

미국은 NIST에서 제작한 FISMA 보안통제를 통해 최상의 보안성능을 유지한다. 그러나 이 보안통제가 항상 완벽한 보안성능을 보장해주진 않는다. 그렇기 때문에 정보보안 측정 프로세스를 통해 지속적인 투자와 보완이 필요하다.

전통적으로 국방력은 나라의 존폐를 논할 만큼 중요하게 여겨왔다. 디지털로 전환한 국방력을 안정적으로 유지하기 위해 외부로부터의 침입을 막고 내부로부터의 유출을 막기 위한 실시간 보안관리의 중요성이가 날로 증가하고 있다.

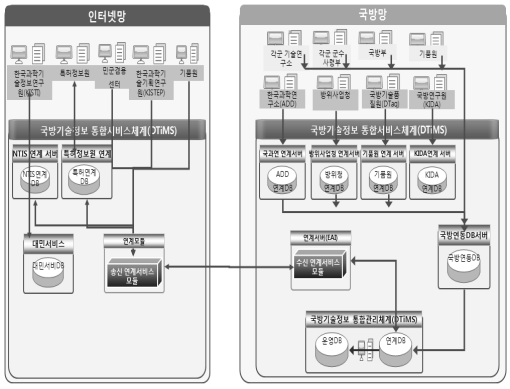
본 논문은 기존의 국내외 실시간 보안관리 체계를 통해 군에 효과적으로 적용시킬 수 있는 국방망의 지속적인 실시간 보안관리 체계를 제안한다. 본 논문의 구성은 다음과 같다. 2장에서는 관련연구로 국방망과 사이버위협 사례, 북한의 사이버전 현황과 대응전략 그리고 FISMA에 대해 살펴보고, 3장에서는 실시간 보안관리 체계 설계를 제안한다. 4장에서는 이 설계에 대해 분석 검증 및 고려사항에 대해 살펴보고 5장에서 결론 및 향후 연구에 대해 설명한다.

Ⅱ. 관련연구

본 장에서는 전반적인 국방망의 현황을 살펴보고 두 번째로는 사례별 사이버 위협을 통해서 공격에 대한 사례분석을 연구하였으며 북한의 사이버전 현황 및 대응전략에 대해 알아보았다. 마지막으로 이러한 위협을 통하여 2002년에 제정된 연방정부정보보호관리법(FISMA)에 대한 보안통제효과를 연구하였다.

2.1 국방망의 현황

먼저 국방망을 포함하고 있는 국방정보통신망은 국방정보화 기반조성 및 국방정보자원관리에 관한 법률에 나온 정의에 의하면 「전기통신기본법」 제2조 제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 국방정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말한다[2]. 국방 정보통신망은 국방망과 전장망, 인터넷이 각각 물리적으로 분리되어 있다. 전장망과 국방망은 인터넷과 물리적으로 분리되어 있다. 전장망은 군 내부에서만 사용하는 별도의 네트워크망이다. 국방망은 인터넷과 수신연계모듈을 통해 연결되어 있다[3].



〔그림 1〕 인터넷과 연결된 국방망

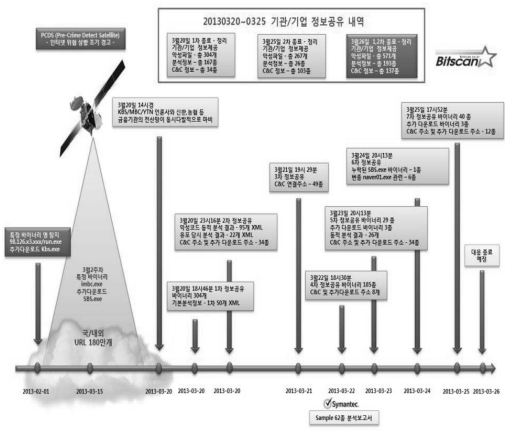
2.2 사례별 분석을 통한 사이버 위협

2.2.1 3.20 사이버테러

〔그림 2〕 3.20 사이버테러 대란 공격구성도

3.20 사이버테러를 일으킨 해커조직이 북한 정찰총국으로 밝혀진 가운데 사이버전이라는 용어는 국가 간

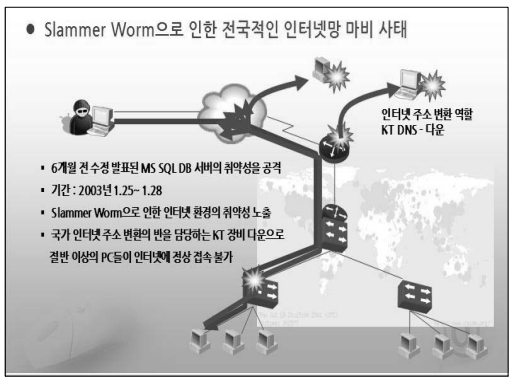
의 보이지 않는 전쟁으로써 국가 간의 핵심 전략으로 부상하고 있다.



〔그림 3〕 3.20 대응 타임라인 - C&C 주소정보 공유[5]

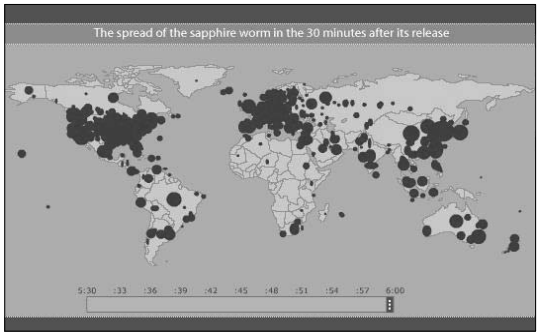
APT 공격으로 이루어진 3.20 사이버테러는 2011년 SK커뮤니케이션즈 3,500만명과 넥슨 1,320만명의 개인정보를 유출시켜 막대한 손실을 입힌 사고보다 더 많은 재산적인 피해를 입었으며 3.20 사이버테러 작전명은 “Operation 1Mission” 이라는 작전 아래, 대규모 사이버 테러를 감행하여 대한민국을 혼란에 빠트렸다.

2.2.2 1.25 대란



〔그림 4〕 공격 개요

Slammer Worm 으로 대변되는 1.25 대란은 SQL 서버의 취약점을 이용하여 1434 포트로 유입되는 형태로 감염되며 감염이 일어나면 무작위로 서버 IP주소를 선정, 초당 1MB 이상의 과도한 패킷을 날려 보냄으로써 서버 부하를 일으켜 시스템을 다운시키는 것으로 분석된다. 이렇듯 1.25 대란의 주요원인인 Slammer Worm의 역할은 사실상 인터넷을 3일간에 걸쳐 마비시키는 역할을 하며, 정보화가 이루어진 국가의 인터넷망에서 대혼란을 나타낸 첫 사례로 볼 수 있다. 이러한 혼란을 야기함으로써 사회적인 불안과 위협을 증가시키고 사이버테러의 목적을 달성한 것이다.



〔그림 5〕 Slammer Worm 확산도

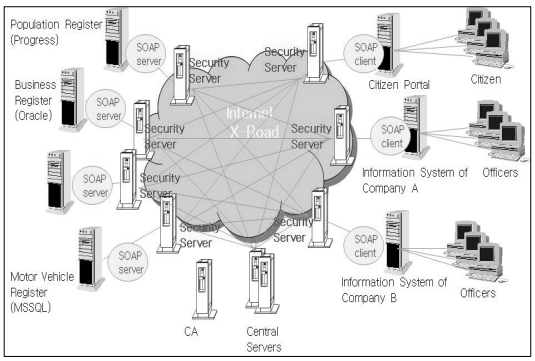
2.2.3 에스토니아 사이버 테러

사이버공간은 새로운 냉전체제의 전쟁터로 진보되고 있다. 사이버전쟁은 가시적으로 보이지가 않기 때문에 합의 및 협정이 쉽지가 않으며 사이버전쟁 1호는 2007년에 발발한 에스토니아가 시발점이다. 수도 탈린에 위치한 소련 참전 용사의 비를 이전하는 과정에서 충돌이 발생하였으며 2007년 4월 27일 이후 약 3주간 5개의 공격유형(DoS, 애플리케이션 공격, Spam Mail, Web Site Defacement, Phishing)으로 통신망을 마비시켰다. 동유럽의 정보통신 강국으로 발전되고 E-Estonia라고 불리었던 이 나라는 공격이 발발한 이래 3주간의 시간은 혼돈의 도가니였을 것이다.

2.3 북한의 사이버전 현황과 대응전략

2.3.1 북한의 사이버전 능력

핵문제와 테러리즘, 사이버 안보를 위협하는 북한은 한반도와 대칭적인 전력에서 재래식 무기의 성능이 떨어지는 것을 인지하고 비대칭적인 전력인 “정보혁명전



〔그림 6〕 에스토니아 행정망 구조

사"를 1993년 이후 인민군 총참모부 산하에 부대를 창설하기 시작하였다. 자위적인 군사노선을 추구하던 북한은 비교적 자원이 적게 들며 파괴적이고 위협할 수 있는 사이버부대를 집중·육성하여 매우 치밀하면서 정보전을 효과적으로 거둘 수 있도록 각 고의 노력을 기울이고 있다.

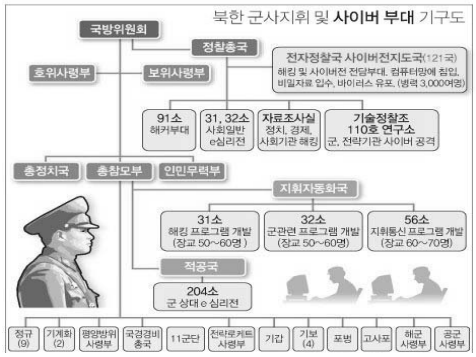
최신 한 언론매체에 의하여 발표한 대학교의 한 교수는 책자를 인용해 항목당 10점을 만점으로 했을 경우 북한은 사이버 기반 시설 관련 의존도 2점△비의전도9점△방어력 7점으로 사이버전이 발생할 경우 대비하는 사이버전 종합대응능력이 18점으로 나타나고 있다고 평가했다. 반면에 이 같은 동일 잣대를 기준으로 우리나라 사이버전 종합대응능력을 평가하면 9점 가량으로 매우 낮다. 미국 사이버전 대응 능력 지표는 사이버 기간시설 관련 의존도 8점△비의존도 2점△방어력 1점으로 사이버전 종합 대응능력은 11점이며 중국은 종합대응능력이 15점으로 북한의 사이버 전쟁 종합 대응능력에 뒤처져있다 라고 주장했다[6]. 이렇듯 북한의 사이버능력은 한반도뿐만 아니라 주변국들에게 대단히 위협적이다. 이러한 사이버 능력은 정보화를 추구하는 글로벌 시대에 시한폭탄 같은 존재가 아닐 수 없다.

북한의 내부 인트라넷에서는 사이버테러 및 전쟁능력을 향상시키기 위하여 경험 및 훈련을 축적하며 새로운 기술을 연구 중이다. 또한 보안의 기초가 되는 수학적인 학문이 북한에서는 제법 잘 구축되어 있어 수학의 근간이 되는 알고리즘의 암호화 및 복호화, 해킹 기술, 프로그래밍 언어를 언제 어디서든지 적합한 활용 및 응용할 수 있도록 훈련이 잘 되어있으며 심지어 실전에서도 적용하여 갖가지 방법으로 훈련 및 효과를 연구한다고 전해진다.

2.3.2 북한의 군사지휘 및 사이버 부대 기구도

북한의 사이버테러를 시행하는 곳은 국방위원회 산하 정찰총국 예하부대인 전자정찰국 사이버전지도국 121국과 91소(해커부대), 31,32(사회일반 e심리전), 자료조사실(정치,경제,사회기관 해킹), 기술정착조 110호 연구소(군전략기관 사이버공격)이 운영되고 있다.

또한 총참모부 예하부대인 지휘자동화국에서는 해킹 프로그램 개발을 관리하는 31소, 군관련 프로그램을 개발하는 32소, 지휘통신 프로그램을 개발하는 56소, 군상대 심리전을 펼치는 204소가 있다.



〔그림 7〕 사이버 부대 기구도

〔그림 8〕 주요 사이버 부대 주둔지

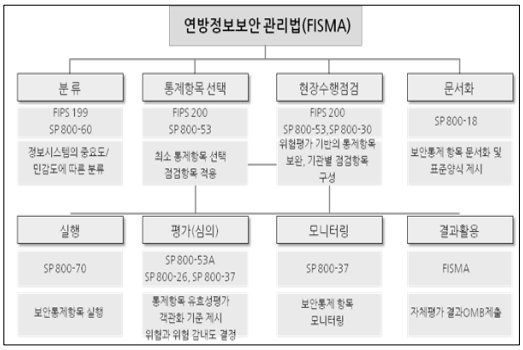
2.3.3 북한의 사이버 위협 대응 전략

7·7 DDoS 공격 사건과 2011년 3·4 DDoS 공격 사건, 2011년 농협 전산망 해킹사고 및 개인정보 유출사고 등 사이버 위협이 점점 증가하고 있는 현실이다. 이에 따라 군은 영토·영해·영공뿐만 아니라 사이버공간(Cyberspace) 또한 보호해야할 영역으로 인지하여 정보

보안대책을 수립해야 한다.

특히 사령부 및 군단급 이상 부대는 컴퓨터 침해사고 대응반(CERT) 편성과 정보보호 특기병을 모집·육성하여 보안인력의 안정적인 수급 및 확보에 최선을 다해야 할 것이다. 또한 민간보안기업과 상호 긴밀한 관계를 공조하여 국방 관제시스템, 강화된 국방네트워크를 수립하여 국방자산을 방호하며 특히 DDoS 같은 사이버위협에 대비하기 위하여 대응체계 확립과 구체적인 문서화 및 보안 프로세스 절차를 반드시 수립하여야 한다.

2.4 FISMA 보안관리

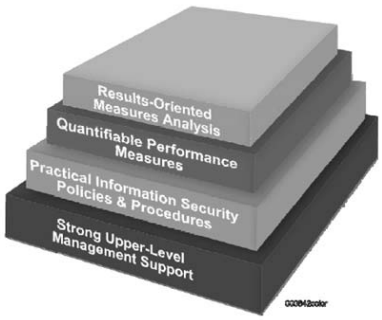


〔그림 9〕 FISMA 구조

FISMA 보안통제는 NIST가, 보안예산 검토, 배정, 감사 등은 OMB가 맡고 있으며 검토, 신청, 수행 및 결과보고의 과정이 있다. 보안통제, 성능평가 및 집계관리는 SP-53 및 SP-55에 정의되어 있으며 각각의 개별적인 보안통제의 성능평가는 집계를 내는데 다음을 기대하고 있다.

- 효과성(Effectiveness) ; 적용한 통제가 적절한가를 파악
- 효율성(Efficiency) ; 적용한 통제가 성능이 있는가를 파악
- 책임추적성(Accountability) ; 통제가 적절치 못하면 개선시킬 수 있는가를 파악
- 법적준수사항 확인(Compliance) ; 법에서 요구사항을 지키고 있는가를 파악

FISMA에 의한 보안의 성공은 다음과 같은 4가지 부분으로 발전될 것으로 판단하고 있다.



〔그림 10〕 정보보안 측정 프로그램 구조[11]

"강력한 상위경영진의 지원(Strong Upper-Level Management Support)"은 단순히 프로그램의 성공뿐 아니라 구현에도 매우 중요하다. 만약 조직의 최상위에서 지원이 없다면 정보보안 성능측정프로그램은 조직의 다양성과 예산 등의 문제로 실패할 것이다.

"실무적인 보안 정책 및 절차(Practical Information Security & Procedures)"는 법률 준수에 따르는 권한을 익히게 하는 것이다. 보안정책은 보안관리 정책을 만들어 주며 보안권한을 명백하게 하고 측정방안의 구축과 법률준수를 가능케 한다.

"정량적 성능측정(Quantifiable Performance Measures)"은 의미 있는 성능데이터를 구하는 부분인데 정보보안 성능의 목적과 목표를 얼마나 쉽게 획득하느냐의 문제이다. 이는 반복적으로 관련된 성능데이터 경향을 시간에 걸쳐 보여주고 자원에 대한 추적이 가능한지를 보여주어야 한다.

마지막으로 "측정데이터의 주기적인 분석(Results-Oriented Measures Analysis)"이 요구된다. 분석결과에서 교훈을 얻어 현재의 보안통제의 효과를 검증하고 향후 보안통제의 계획에 사용해야 한다. 이해관계자와 사용자로부터의 정확한 데이터 수집이 중요하며 이는 정보보안 프로그램의 전반적인 향상을 가져올 것이다[11].

Ⅲ. 국방망의 실시간 보안관리 체계 설계

본 장에서는 G-ISMS, NIST SP 800-55 및 ISO 27001을 참조하여 제안한다[7][9][11]. 통제 후보군은 4개 분야, 8개의 도메인, 18개의 통제항목, 69개 세부통제항목으로 이루어져있으며 각 세부통제마다 해당하는 인증심사기준으로 평가를 실시한다.

〔표 1〕 국방망의 실시간 보안관리 관리적 통제 후보군

	분야		통제		세부통제	인증심사기준
1	관리적	1.1	군사보안정책	1.1.1	군사보안 정책의 문서화	군사보안 정책문서는 사령관의 승인을 받아야 하고 반드시 공지되어야 한다.
				1.1.2	군사보안 정책의 검토	군사보안 정책/대책/계획은 정기적으로 또는 적합성과 효과성에 있어 중대한 변화가 발생된 경우에 검토되어야 한다.
				1.1.3	군사보안 지휘통제	군사보안 정책에 관한 문제가 발생할 경우 해당 지휘관에게 체계적으로 보고되어야 한다.
				1.1.4	군사보안 정책의 사후관리	군사보안 정책의 사후관리는 반드시 수정 및 파기에 관한 책임자에 한하여 관리 되어야 한다.
2		2.1	군사보안 조직	2.1.1	군사보안을 위한 지휘관 역할	지휘관은 군사보안 방향 제시 및 검토, 역할 및 책임 승인, 군사조직의 협력 및 조정 확인 등의 역할수행을 통하여 군사보안 활동을 능동적으로 지원하여야 한다.
				2.1.2	군사보안 관련 위원회 구성 및 운영	군사보안관련 위원회를 구성하여 기관 전반에 걸친 중요한 군사보안 관련 심의 및 승인기능을 수행하며 필요한 자원 할당을 통해 군사적인 보안관리 적절하게 수행될 수 있도록 하여야 한다.
				2.1.3	군사보안 책임의 할당	군사보안 책임은 명확해야 하며 해당 지휘관은 사고 발생시, 해당 책임을 반드시 정의되어야 한다.
				2.1.4	정보시스템 도입에 대한 인가절차	신규 정보시스템(PC,테블릿,노트북) 도입시, 군사보안에 관련한 정책 및 요구사항에 부합되는 인가절차를 반드시 수립하여야 한다.
				2.1.5	민간기관의 연계	민간기관과 상호협력 시, 군사보안 서약서 작성 및 정책을 숙지/전달시켜야 한다.
3		3.1	자산에 대한 책임	3.1.1	자산목록	주요 정보자산에 대한 목록을 작성 및 관리하여야 한다.
				3.1.2	자산관리자	정보자산에 대하여 책임자를 (정),(부)를 통하여 임명하여야 한다.
				3.1.3	사용규정의 문서화	정보자산의 사용규정을 명백히 정의하고 문서화하여야 한다.
				3.1.4	인가된 사용자의 접근	인가된 사용자로부터 접근을 하여야 한다.
		3.2	자산에 대한 분류	3.2.1	분류 등급 및 규정	자산에 대한 데이터 등급을 매겨 분류하여야 한다.
				3.2.2	처리방식 규정	자산 분류에 근거하여 처리방식을 규정하고 적용시킨다.

〔표 2〕 국방망의 실시간 보안관리 물리적 통제 후보군

	분야		통제		세부통제	인증심사기준
1	물리적	1.1	보호구역	1.1.1	물리적 보호구역	군 기밀 및 군 정보처리시설이 설치된 장소를 보호하기 위해 물리적 보호구역(제한지역, 보호구역, 통제구역)을 지정하여야 한다.
				1.1.2	물리적 출입통제	보호구역은 인가된 사용자만 출입이 가능하도록 출입통제 장치를 설치하고 운영하여야 한다.
				1.1.2	시설 및 설비 공간 보호	시설 및 설비 공간에 대한 물리적인 보호방안을 수립하고 적용하여야 한다.
				1.2.3	외부 및 환경 위협에 대한 보호	자연재해 및 외부로 인한 피해에 대비하기 위해 물리적인 보호방안을 수립하고 적용하여야 한다.
				1.2.4	보호구역 작업	보호구역에서의 작업을 위한 물리적인 보호방안을 수립하고 적용하여야 한다.
				1.2.5	공공장소 및 운송·하역구역	공공장소 및 운송·하역을 위한 구역은 내부 군 정보처리시설로부터 분리 및 통제하여야 한다.
2		2.1	군정보처리시설 및 군장비 보호	2.1.1	군정보처리시설의 배치	군정보처리시설은 물리적인 위협과 비인가된 접근으로부터 보호될 수 있도록 배치하여야 한다.
				2.1.2	설비 지원	군정보처리시설은 전원 장애 및 공조시설의 장애에 따른 중단으로부터 보호되어야 한다.
				2.1.3	케이블 보호	전원을 공급하는 전력선과 데이터를 전송하는 통신선은 손상이나 도청으로부터 보호하여야 한다.
				2.1.4	군시설 및 군장비 유지보수	군정보처리시설은 가용성과 무결성을 지속적으로 보장할 수 있도록 유지보수 하여야 한다.
				2.1.5	외부 반출 장비의 보안	외부로 반출된 군사정보시스템 장비는 사용과정에서 발생할 수 있는 위험에 대한 적절한 대책을 수립 및 적용하여야 한다.
				2.1.6	군장비의 폐기 및 재사용	기밀저장매체를 가지고 있는 장비의 폐기 및 재사용 시 기밀정보 및 소프트웨어가 안전하게 삭제되었는지 점검하여야 한다.
				2.1.7	군장비의 반출·입	군장비 및 기밀저장매체를 반입 및 반출하기 위한 안전한 승인 절차를 마련하여야 한다.

〔표 3〕 국방망의 실시간 보안관리 기술적 통제 후보군

	분야		통제		세부통제	인증심사기준
1	기술적	1.1	운영절차 및 책임	1.1.1	운영절차의 문서화	군사정보시스템 운영절차를 문서화하고 관리하여야 한다.
				1.1.2	변경관리	군사정보시스템의 변경에 대한 통제 방안을 수립하고 시행하여야 한다.
				1.1.3	직무분리	군사정보시스템에 대한 고의적 또는 우발적 오용의 위험을 감소시키기 위해 직무가 분리되어야 한다.
				1.1.4	개발, 시험 및 운영환경의 분리	군사정보시스템의 개발, 시험 및 운영환경은 비인가된 접근 또는 변경의 위험을 최소화하기 위해 분리되어야 한다.
		1.2	군사정보시스템 도입	1.2.1	군사정보시스템 도입 계획	군사정보시스템의 처리 속도와 용량에 대하여 주기적인 모니터링을 수행하고 안정성과 기밀성 확보에 필요한 시스템 도입 계획을 수립하여야 한다.
				1.2.2	군사정보시스템 인수	새로 도입되는 군사정보시스템에 대한 인수 기준이 수립되어야 하며, 인수전에 테스트가 반드시 수행되어야 한다.
2		2.1	유해소프트웨어 통제	2.1.1	악성코드 통제	악성코드로부터 군사정보시스템의 보호를 위한 통제 방안을 수립하고 사용자 교육 및 훈련을 수행하여야 한다.
				2.1.2	모바일 코드 통제	모바일 코드(자바스크립트, 액티브엑스 등)의 제한적인 실행을 위한 통제 방안을 수립하여야 한다.
		2.2	백업	2.2.1	정보 백업	기밀 정보와 소프트웨어의 백업을 위한 규정을 수립하고 주기적으로 백업을 수행하여야 한다.
		2.3	네트워크 보안	2.3.1	네트워크 통제	네트워크로 전송되는 정보와 네트워크에 연결된 군사정보시스템에 대한 보안을 유지하기 위하여 통제 방안을 수립하고 운영하여야 한다.
				2.3.2	네트워크 서비스 보안	네트워크 서비스에 대한 보안 기능, 서비스 수준, 관리 요구사항을 고려하여 네트워크 서비스 계약을 체결하여야 한다.
		2.4	매체 관리	2.4.1	휴대용 저장매체의 관리	휴대용 저장매체에 대한 관리 방안이 수립되어야 한다.
				2.4.2	매체 폐기	매체의 불용처리 시 저장내용을 식별할 수 없도록 소각, 파쇄 등의 폐기 방안을 수립하여야 한다.
				2.4.3	정보 취급 절차	매체에 포함된 정보의 비 인가된 유출, 변경, 손상으로부터 보호하기 위한 취급 방안을 수립하여야 한다.
				2.4.4	시스템 문서의 보안	시스템 문서를 비인가된 접근으로부터 보호하기 위한 관리 방안을 수립하여야 한다.
		2.5	정보의 교환	2.5.1	정보 교환의 통제	통신 설비를 사용한 정보의 교환 시 안전한 절차와 통제가 수립되어야 한다.
				2.5.3	운송중인 매체의 보호	정보를 포함한 매체는 시설 외부로 운송 시 인가되지 않은 접근, 변경, 손상으로부터 보호하여야 한다.
				2.5.4	전자적 교환 보안	전자 메일, 메신저 및 P2P 통신과 같은 전자적인 교환에 대한 보호 방안을 수립하여야 한다.

	분야		통제		세부통제	인증심사기준
				2.5.5	군사정보시스템 접속 통제	군사정보시스템 간의 안전한 접속을 보장하고 관련 정보를 보호하기 위한 방안을 수립하여야 한다.
		2.6	모니터링	2.6.1	감사 로그	사용자 활동, 예외 처리, 정보보호 사고에 대한 조사와 모니터링을 지원하기 위해 감사 로그를 기록하고 관리하여야 한다.
				2.6.2	군사정보시스템 사용 모니터링	정보처리시설의 사용에 대한 모니터링 방안을 수립하여야 하고 모니터링 결과를 주기적으로 검토하여야 한다.
				2.6.3	로그 정보의 보호	로그 기록 장치와 로그 정보는 비인가된 접근 및 변경으로부터 보호하여야 한다.
				2.6.4	관리자 및 운영자 로그	군사정보시스템 관리자와 운영자의 활동을 기록 및 검토하여야 한다.
				2.6.5	장애 로그	장애 로그를 기록하고 분석하여 적절한 대응 방안을 수립하여야 한다.
				2.6.6	시간 동기화	기관 내부의 군사정보시스템은 정확한 시간으로 동기화하여야 한다.
		2.7	네트워크 접근통제	2.7.1	네트워크 서비스의 사용정책	사용자가 인가를 받은 서비스에만 접속할 수 있도록 통제하는 방안을 수립하여야 한다.
				2.7.2	원격접속 사용자 인증	원격 사용자의 접속을 통제하기 위해 적절한 인증방법을 사용하여야 한다.
				2.7.3	네트워크에서의 장비 인식	특정 위치 및 장비로부터의 접속을 인증하기 위한 자동 장비 인식 방식을 사용하여야 한다.
				2.7.4	원격 진단 및 포트 설정 보호	포트를 구성하고 진단하기 위한 물리적·논리적 접속을 통제하여야 한다.
				2.7.5	네트워크 분리	서비스 그룹 및 사용자, 정보 시스템 별로 네트워크를 분리하여 운영하야 한다.
				2.7.6	네트워크 연결 제어	외부의 네트워크 접속은 접근통제 정책과 업무 요구사항에 따라 제한하여야 한다.
				2.7.7	네트워크 경로 제어	업무 응용의 접근통제 정책에 따른 컴퓨터 접속과 정보 흐름 통제를 위한 경로 제어를 수행하여야 한다.

〔표 4〕 국방망의 실시간 보안관리 개인정보보호 통제 후보군

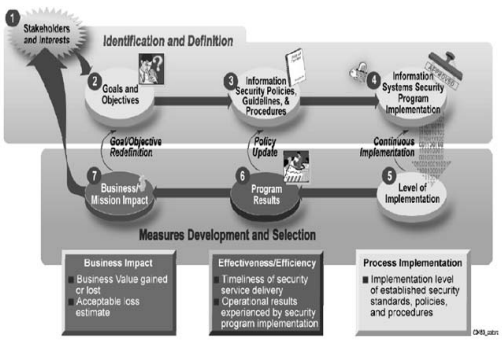
	분야		통제		세부통제	인증심사기준
1	개인 정보 보호	1.1	사용자 접근 관리	1.1.1	사용자 등록	정보시스템과 서비스에 접근을 허용하거나 취소하기 위한 공식적인 사용자 등록 및 해지 절차가 있어야 한다.
				1.1.2	특수권한 관리	특수권한의 할당이나 사용을 제한하고 통제하여야 한다.
				1.1.3	패스워드 관리	패스워드는 승인된 절차에 의해 통제 및 관리되어야 한다.
				1.1.4	접근권한의 검토	사용자의 접근권한을 주기적으로 검토하여야 한다.
		1.2	사용자 책임	1.2.1	패스워드 사용	안전한 패스워드 사용 및 관리지침을 수행하여야 한다.
				1.2.2	정보시스템의 보안	사용자가 자리를 비울 때 비인가된 접근으로부터 장비를 보호하기 위한 방안을 수립하여야 한다.
				1.2.3	개인정보 흔적의 삭제	정보시스템으로 남은 개인정보는 반드시 삭제되어야 한다.
		1.3	정보의 유출	1.3.1	사고체계의 문서화	정보 유출 사고가 났을 경우 반드시 사고 체계에 대한 문서화를 수립하여야 한다.
				1.3.2	지휘관에게 보고	사고가 났을 경우 반드시 책임 지휘관에게 신속히 보고하여야 한다.

Ⅳ. 분석 검증 및 고려사항

4.1 국외 관리체계 분석

4.1.1 SP 800-55

정보보안 성능측정 프로그램을 사전에 구성하는 것은 시스템개발주기(SDLC)에서 보안 요구사항 분석을 초기에 배치하는 것과 같으며 구성 후에 적용하는 것보다 더 많은 보안적인 지표들을 창출할 수 있다. 정보보안 성능측정 프로그램을 구성하는데 있어 주요 고려사항은 다음과 같다.



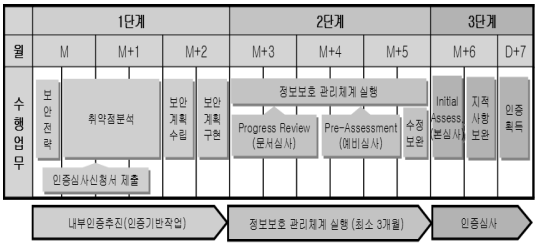
〔그림 11〕 SP 800-55

- 조직의 전략, 사업환경, 정보보안 우선순위 등에 가장 적합한 측정 지표를 선택한다.
- 이해관계자들로부터 정보를 얻거나 교육할 시간을 구성한다.
- 적절한 기술 및 프로세스 기반구조가 제대로 구성되었는지 검증한다.

(그림 11)은 정보보안 측정지표 개발 프로세스를 나타낸 것이다. 그림에서 정의한 작업들은 측정지표에 대한 고려, 특정 조직과 유관 부서에 적합하게 구성된 측정지표를 파악하는 수단으로 사용하며 순차적인 실행절차를 의미하지는 않는다.

4.1.2 ISO 27001

조직의 정보유출의 예방과 사고 발생, 사이버테러에 신속하게 대응하기 위한 체계가 필요하게 되었다. 국제표준화기구(ISO)에서 제정한 ISO27001은 정보보호관리체계에 관한 국제 규격이며 정보보호관리체계에 대해서 국제 인증을 할 때의 요구사항을 정의하고 있다.



〔그림 12〕 ISO 27001 인증절차

정보보호 분야의 가장 공신력 있는 국제 인증으로써 정보보호정책, 자산관리, 정보 통제 등 정보보안과 관련된 11개 영역, 133개 항목에 대해서 국제 심판원들의 엄정한 심사와 검증을 통과해야만 인증된다. (그림 12)에 의하면 인증을 받으려면 정보보호관리체계의 수립단계, 이행단계, 심사단계로 구분할 수 있다.

조직의 자산 보안 위험수준을 분석해서 Best Practice를 활용, 보호대책을 적용할 수 있도록 한다. ISO27001은 영국 표준협회의 BS7799 규격에 기반을 두고 있다[9].

4.2 우수사례 분석

4.2.1 한국 K연구소 보안관리체계

본 논문에서는 연구·분석한 한국 K연구소의 사례가 있다. NIST SP-53과 SP-55를 참조하여 보안통제 구성, 지표 설계와 절차, 설계 내용, 측정절차를 개발하였다. 또한 이 보안수준 측정을 자동화 시스템으로 구축, 정규 프로세스화하여 실시간 보안관리가 가능토록 하였다.

〔표 5〕 한국 K연구소 보안관리체계

단계 및 절차	설 명
1단계: 측정지표 개발	• 보안통제 구성은 NIST SP 800-53 참고 • 지표 설계절차와 설계 내용은 NIST SP 800-55의 20개 지표를 참고 • 지표 개발 및 보안수준측정 모두를 진행하기 위하여 데이터가 있는 업무를 대상으로 진행
2단계: 보안수준 측정 PLOT	• 개발한 측정지표를 업무에 적용하여 보안성능 측정 • 측정절차는 NIST 800-55 참고 • 측정결과 분석 방식 및 활용 방안 수립 • 2단계 완료 후 보안수준측정 작업의 결과물이 작성되며 이를 토대로 업무개선 방안을 도출할 수 있음.
3단계: 측정지표 보완 및 확장 & 정책/절차개선	• 보안수준 측정대상을 확대하여 지표 설계 및 측정을 진행 • 측정결과를 토대로 보안수준 개선 방안 도출 • 이 단계부터는 데이터가 관리되지 않던 업무도 포함하여 진행(지표설계->데이터 관리->보안수준 측정의 순서로 진행)
4단계: 데이터수집 및 측정 자동화시스템 구축	• 측정 자동화 시스템 구축 - 데이터를 DB에 관리하고 보안수준 측정 및 이력관리를 위한 시스템 구축
5단계: 정규 프로세스화	• 보안성능측정 및 보안수준 개선 방안 도출하는 전 과정을 정규 업무 프로세스로 구성 • 3단계 완료 후, 정기적으로 보안수준 측정을 진행하면서 4,5단계를 진행

4.2.2 국내 포털사이트 N사 보안관리체계

다른 사례로는 국내 포털사이트의 적합한 구체적인 지표 주제를 제시함으로써 효과적인 보안통제를 한다.

〔표 6〕 국내 포털사이트 N사 보안관리체계

보안통제	지표주제
취약성진단	• 취약성 진단 수행 현황 및 진단 결과 • 보안패치 적용 • 필수 보안프로그램 설치 및 결과분석
접근제어	• ACL 정책 준수 • ACL의 사용기간 준수
사고대응	• 침해사고 분석 및 침해원인 • 2차 침해사고 및 동일 취약점에 의한 재 침해사고 • 침해사고에 대한 보안권고 이행 및 이행점검 • DDoS로 인한 장애 발생 • 보안사고 및 이벤트 전파
보안성검수	• 신규서비스 및 시스템의 보안성검수 및 이행점검 • 변경관리 대상 시스템의 보안성검수 및 이행점검
아웃소싱	• 서비스 아웃소싱의 보안권고 이행 및 이행점검
PC보안	• 필수 보안프로그램 설치 및 결과분석 • 사용제한 프로그램 및 서비스의 사용 • 보안패치 적용

보안통제	지표주제
	● 로그인 보안 ● 악성코드 감염 및 치료 ● 중요정보 보호 (DRM관련)
어플리케이션 보안	● 서비스 Application의 취약점 제거 ● 비정상 로그인 시도의 차단
유지보수	● 보안시스템 구성요소의 유지보수 이행

Ⅴ. 결론 및 향후과제

군사보안시설의 실시간 보안관리 체계는 반드시 수행되고 각각의 분야와 세부통제는 요구조건에 대해 보안성이 철저하게 입증되어야 한다. 이를 위해서는 사고를 유발할 수 있는 원인을 모두 고려하고 보안 통제 프로그램에 대한 구현 및 효과성과 관련된 데이터 수집, 분석 및 보고를 통하여 완전한 책임추적성(Accountability)을 보증하여야 한다. 아울러서 성능평가 척도를 수집하고 개발하기 위해서는 첫 번째, 보안정책을 수행하는 척도를 평가하는 수단의 개발을 하고 둘째, 보안서비스 전달과정의 결과와 효과성 및 효율성 측정, 마지막으로 보안 이벤트나 사고가 비즈니스와 업무 수행 목표에 미친 영향력 평가를 통하여 실시간으로 보안관리 체계를 구현하여야 한다.

본 논문에서는 국외 관리체계 및 국내기업 우수사례 분석을 통해 보호체계 수립단계부터 세부적인 평가까지 실질적으로 보안에서 중요시하는 관리적, 물리적, 기술적에 근거하여 국방망의 실시간 보안관리 체계를 위해 많은 연구가 이루어졌다. 특히 본 연구를 진행하면서 보안사고시, 국방망의 지휘보고체계가 보안 프로세스만큼 매우 중요하며 서로간의 상호의존성을 고려하고 적절한 문서화가 이뤄질 수 있도록 반드시 수행하여야 한다.

본 연구를 통해 보다 효율적이고 보안사고를 최소화시킬 수 있는 지표가 될 국방망의 실시간 보안관리 체계를 제안하였다. 향후 이러한 보안 관리체계가 적용 후, 실증적인 연구모델과 적용 후에 얼마만큼 효과성을 창출할 수 있는지, 또한 이러한 점을 입증할 수 있는 연구가 이루어져야 할 것이다.

참고문헌

[1] 정교일, “IT-국방 발전 방향”, ETRI, 2010 Sep.
[2] 국방부 “국방정보화 기반조성 및 국방정보자원관리에 관한 법률”, 2013 Sep.
[3] 김동규, “전장망 바이러스, USB로 전파된다.” 한겨레, 2012 Sep.
[4] 보안뉴스, “3.20 사이버테러 내부 침입경로 수수께끼 풀렸다.”, 2013 Apr.
[5] 빛스캔, “3.20 대란의 추적과 대응”, Mar 2013.
[6] 장윤정, “북 사이버 전쟁능력, 한.미.중을 압도한다.”, 전자신문, 2010 Dec.
[7] 행정안전부, 전자정부 정보보호관리체계(G-ISMS) 인증안내서, 2011.
[8] 인증심사기준, “G-ISMS 정보보호 대책 통제사항“, 국가법령정보센터, 2010.
[9] Daminda Perera, “ISO/IEC 27001, Information Security Management System”, 2008.
[10] E. Humphreys, “Implementing the ISO/IEC 27001 information security management system standard”, Artech House, 2006.
[11] Carlos M. Gutierrez, Secretary “NIST SP 800-55 Revision 1 – Performance Measurement Guide for Information Security”, U.S Department of Commerce, 2007.

〈저 자 소 개〉

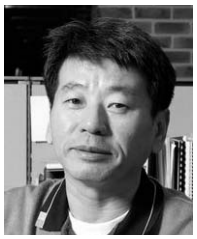
권 오 훈 (Kwon Oh Hun)
학생회원

2012년 2월 : 호서대학교 정보보호학과 졸업
2012년 3월~현재 : 동국대학교 정보보호학과 석사과정
<관심분야> 정보보안관리 및 정책, 네트워크 보안

이 명 훈 (Lee Myoung Hun)
학생회원

2012년 2월 : 중부대학교 정보보호학과 졸업
2012년 3월~현재 : 동국대학교 정보보호학과 석사과정
<관심분야> 암호학, 클라우드보안

이 재 우 (Lee Jae Woo)
- 동국대학교 국제정보대학원 석좌교수(현)
- 한국포렌식조사전문가협회 회장(현)
- ISC2 Fellow, Asia Board 의장(현)
- 한국 CSO 협회 자문위원장(현)
- 한국정보보호진흥원 초대 원장



임 채 호 (Chae-ho Lim)
종신회원

1986년 : 홍익대학교 전산학과 학사
2001년 : 홍익대학교 전자계산학과 박사
2006년~2009년 : NHN(주) 보안실 실장, 연구센터 수석
2009년 : 한국정보보호학회 부회장
2010년 8월~현재 : KAIST 사이버보안연구센터 연구부소장
2011년 2월~현재 : KAIST 정보보호대학원 연구교수
<관심분야> 인터넷 보안, 정보보호 위험 관리, 정보보호 관리 및 정책