사이버전 위협에 대비한 전사적 조기경보체계 구축 방안

엄정호*, 박선호**, 정태명*
*성균관대학교 정보통신공학부
**성균관대학교 전자전기컴퓨터공학과
e-mail:jheom@imtl.skku.ac.kr

A S초듣 of Enterprise Early Warning Structure for defending the Threat of Cyberwarfare

Jung-Ho Eom*, Seon-Ho Park**, Tai-Myoung Chung*
*School of Information Communication Engineering, Sungkyunkwan University
**Dept. of Electrical and Computer Engineering, Sungkyunkwan University

요 약

본 논문은 국가 정보통신 인프라체계를 대상으로 한 사이버 위협에 대해서 전사적 조기경보체계 구축 방안을 제시하였다. 전사적 조기경보체계는 조기경보시스템을 활용하여 사이버 공격의 징후정보를 초기에 수집, 분석하고 이를 통해 예측할 수 있는 사이버 공격 경로를 사전에 파악하여 공격이 더 이상 진행되지 않고 심각한 피해가 발생하지 않도록 네트워크로 연결된 모든 정보통신체계나 보안 관리자들에게 관련 정보를 신속하게 전파하여 위협을 제거할 수 있도록 하는 체계이다. 국가 정보통신 인프라체계에서 사이버전의 확산과 피해를 줄이기 위해서는 조기경보체계를 국가 기간망 체계와 사이버전의 특성을 고려하여 구축하여야 한다. 본 논문에서는 국가 대상 사이버전이 발생할 경우를 대비하여 조기경보체계 구축 방안을 정책적 및 기술적 측면에서 제시하였다.

1. 서론

최근 초특급 사이버 무기로 알려진 스턱스넷(Stuxnet)[1]이 전 세계의 SCADA를 위협하고 있는 가운데 사이버 공격에 대한 관심이 한층 증가되고 있다. 스턱스넷은 독일 기업인 지멘스의 소프트웨어 및 시스템만을 공격해 파괴하는 사이버 웜으로 이란, 중국 등의 SCADA와 관련된 시스템을 공격한 바 있다. 또한, '09년 4월 미국 국방부에서 해킹공격으로 차세대 전투기 개발에 관련된 정보가 유출[2]되었다. 정체불명의 해커들이 지난 2년간 국방부 연구개발 네트워크에 침투하여 3000억달러의 개발비를 투입한 차세대 통합 전투기 F-35의 설계도와 시스템 관련 정보들을 빼낸 사실이 뒤늦게 들어났다. 최근 사이버 공격이 특정 공격대상 시스템을 목표로 하여 공격을 수행하기 때문에 국가 기간망도 사이버 위협으로부터 안전을 보장받을 수 없다. 국가 기간망을 가장 위협하는 사이버 공격은 중국과 북한 등 조직적으로 구성된 사이버 범죄 집단이나 사이버전 부대로 추정되며, 최근에는 북한 해커로 명확하게 드러나는 사례도 늘고 있다.

이렇듯 국가 핵심 기간망을 공격하여 네트워크를 마비시키고 컴퓨터의 오작동을 유발시켜 국가 정보통신체계의 성능을 저하시키거나 기능을 파괴시키는 사이버 공격이 국가 안보에 중대한 위협요소로 대두되고 있다. 국가 기간망이 무선, 센서 기술을 포함한 유비쿼터스 컴퓨터 환경으로 발전해 가면서 사이버 공격경로가 증가하고 공격표적도 다양화되고 있는 실정이다. 또한, 최근 사이버 공격이 해킹기술과 웜, 바이러스 등의 해킹 도구의 진화로 인해 점차 복잡해지고 지능적으로 변화함에 따라 위협의 파괴력이 증대되고 범위가 넓어지고 있어 그에 대한 대응체계를 철저하게 준비할 필요가 있다.

본 논문에서는 이러한 문제를 해결하기 위해 2장에서 사이버전의 개념과 특징, 3장에서는 조기경보체계의 개념과 주변국의 조기경보체계 구축 현황을 고찰한다. 4장에서는 사이버전에 대비한 전사적 조기경보체계 구축 방안을 제시하고 5장에서 결론을 맺는다.

2. 사이버전

사이버전(Cyberwarfare)은 "사이버 공간에서 일어나는 새로운 형태의 전쟁수단으로써, 시스템 및 데이터 통신망 등을 교란, 마비 및 무력화함으로써 공격대상 사이버체계를 파괴하고 자국의 사이버 체계를 보호하는 모든 제반 행동을 의미한다[3,4]. 사이버전도 물리적 전쟁과 마찬가지로 사이버전 수행 주체와 공격 대상, 수행공간 및 무기체계가 반드시 있다. 즉, 사이버전은 사이버 전사, 사이버 전장, 사이버 무기, 사이버 표적 등으로 수행된다[5].

사이버전은 다면적인 특징을 갖고 있기 때문에 어느 한 가지 측면만을 강조한 사이버전의 의미는 특정한 유형만을 지칭하게 된다. 따라서 사이버전의 유형도 사이버전의 범주와 시각에 따라 다양하게 나누어진다. 사이버전의

특징을 살펴보면 다음과 같이 요약할 수 있다[3,5].

첫째, 저비용의 전쟁수행이 가능하다. 사이버전에서는 몇 대의 시스템과 프로그램 작성 능력만 있으면 해킹 도구를 제작할 수 있으며, 인터넷 상에서 공개된 해킹 도구를 싼 값에 구입한 후 소스코드를 변경하여 조작만 하면 필요한 공격 도구로 제작할 수 있다.

둘째, 사이버 공격에 대한 전투평가와 경보체제구축이 재래식 전쟁보다 어렵다. 재래식 전쟁에서는 공격 이후에 정찰기나 위공위성 등을 통해 전투피해효과를 측정할 수 있는 반면, 사이버 공격은 전투피해효과를 평가할 메커니즘이 없다. 또한, 공격 준비, 실행, 종료를 포함한 모든 공격 프로세스가 초고속화 및 최단기화로 이루어지기 때문에 공격징후를 포착하기가 용이하지 않다.

셋째, 사이버 공격자는 다양화해지고, 사이버 공격 기술은 언제 어디서든지 구할 수 있다. 따라서 다양한 형태의 사이버전을 전개할 수 있는 잠재적 사이버 공격자들이 크게 확대되었으며, 그들이 사용하는 해킹 기술이나 도구는 적대 국가들 간에 비슷한 양과 질로 사이버 공간에서 얻을 수 있다.

넷째, 사이버 공격기술에 의한 수행 속도가 초고속화 및 초단기화 되는 반면에, 공격을 받는 국가는 조기에 공격 징후를 식별할 수 없기 때문에 대응할 수 있는 시간적 여유가 거의 없다. 21세기의 사이버 공격은 시간적 공백 없이 제로데이(Zero-Day) 공격이 가능하다.

마지막으로, 정보수집 양상이 변화되고 있다. 사이버전에서는 공격자의 정체가 불분명하고 그들의 공격 의도와 목표를 파악할 수 없다. 또한, 공격대상 목표가 명확하게 드러나지 않고 공격 진행이 매우 빠르게 변하기 때문에 정보 수집을 위해 배정해야 하는 자원을 조정하기란 쉽지 않다. 따라서 사이버전에 초점을 맞춘 새로운 정보수집 활동영역의 분석이 필요하다.

<표 1> 사이버전의 주요 사례

날 짜	주 요 내 용
2004년	중국 해커, 한국 국방연구소, 외교부 등 웹사이트 집중 공격
2007년	러시아 해커, 에스토니아 정부, 언론, 방송, 금융전산망 집중 공격
	중국 해커, 미국 국방부 동아태국 집중 공격으로 초토화, 로버트 게이츠 국방장관 컴퓨터까지 침입
2008년	러시아 '러시아비즈니스네트워크' 사이버범죄 조직이 그루지아 대통령 홈페이지를 비롯한 의회/국방부/외교부 사이트에 대해 서비스 거부 공격 집중
	이스라엘-하마스 분쟁시 아랍권 해커집단 '팀 이블'이 이스라엘 일간지 와이네트 등 400개 이상의 사이트를 해킹·변조했으며, 이스라엘의 가자 침략 부도덕성을 선전하는 정치적 도구로 이용
2009년	16개국 86개 IP 이용 DDoS 공격으로 국가 주요 전산망 공격
	한/미 연합사 USB 저장 작계 5027 해킹으로 유출
2010년	스턱스넷을 이용하여 이란, 중국 등 국가 SCADA 관련 시스템 감염

최근 정부를 대상으로 이루어지는 사이버 공격으로 인해 각국 정부 당국들이 대응책 마련에 부심하고 있다. 미 국방부와 국무부가 사이버 공격으로 인해 침입당하고 영국, 독일, 프랑스의 정부 및 주요기간 전산망에 사이버 전사들이 휘젓고 다니고 있어 이들 국가들의 보안상태가 취약한 것으로 드러나고 있다. <표 1>은 최근에 발생한 사이버전의 사례를 보여 준다[4].

21세기에 들어서면서 미 군용기 충돌 사건, 이라크전, 러시아의 에스토니아와 그루지아에 대한 사이버 공격은 개인 차원이 아니라 그야말로 사이버전이라 할 수 있을 만큼의 규모나 대상이 전혀 다른 양상으로 전개되고 있다. 특히, 2007년, 2008년에 러시아에 의해 수행된 것으로 의심받고 있는 에스토니아와 그루지아에 대한 분산 서비스 거부공격(DDoS; Distributed Denial of service)은 정부, 방송국 그리고 금융과 같은 주요 전산망을 대상으로 집중적으로 수행되었다.

3. 조기경보체계 및 주변국의 구축 현황

3.1. 조기경보체계의 개념

사이버전에서 사이버 공격 양상은 매우 빠른 속도로 진화하고 있다. 사이버 공격기술은 스텔스 기법을 사용하거나 바이러스와 해킹 기술이 융합되어 점점 지능화 및 고도화되며, 공격경로가 다양화되고 분산서비스거부공격처럼 모든 시스템을 활용하도록 에이전트화되고 있다. 또한, 수 초, 분 내에 공격을 끝낼 수 있을 정도로 초고속화되고 있다. 사이버전에서 사이버 공격의 징후를 나타내는 다양한 정보들을 정확하게 분석하고 불법적인 침입으로 판정할 수 있는 경보정보의 속성을 분석하여 보안 관리자에게 신속히 경보함으로써 피해발생의 가능성과 범위를 최소화하는 일련의 능동적인 대응절차를 구축, 운영하는 것이 매우 중요하다[6].

조기경보체계는 사이버 공격과 같은 악의적이고 불법적인 침입이나 공격 징후정보를 초기에 수집, 분석하여 이를 통해 예측할 수 있는 사이버 공격 경로를 사전에 파악하여 침입이나 사이버 공격이 더 이상 진행되지 않도록 모든 관련 기관이나 관리자에게 관련 정보를 전파하여 위협을 사전에 제거할 수 있게끔 하는 체계를 말한다[7].

3.2. 국내/외 조기경보체계 구축 현황

국내에서는 2003년 1.25 인터넷 침해사고 이후 웜·바이러스뿐만 아니라 변종 및 신종 위협요소들에 대한 분석과 신속한 대응기법 개발 등 사전 경보 및 예방 기술의 개발과 활동을 강화하였다[8,9,10].

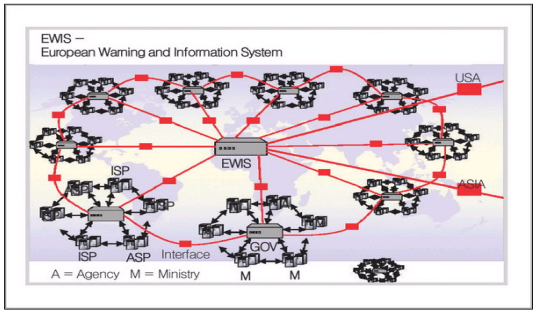
국가사이버안전센터(NCSC : National Cyber Security Center)에서는 인터넷 침해사고에 대한 사이버 공격 감시, 사이버 안전 예방 활동, 국가 사이버 위협정보 종합 수집 및 분석, 침해사고 긴급대응, 조사 및 복구, 국내외 사이버 위협 정보 공유 및 공조 대응 등 종합 보안서비스를 제공하고 있다.

국방부 국방정보전대응센터에서는 국방전산망에 대한 침해정보 경보, 탐지 및 분석, 각급 부대 CERT에 대한 조정 통제, 예방 및 조사활동, 원격 및 현장 피해복구 지원, 국내외 정보전 관련 정보 분석 등을 담당하고 국가사이버안전센터와 연동하여 국방 C4ISR을 대상으로 보안관제 업무를 지원하고 있다.

인터넷침해사고대응지원센터(KISC : Korea Internet Security Center)에서는 상시 모니터링 체계를 갖추어 주요 인터넷서비스 제공자(ISP : Internet Service Provider)를 비롯한 국내관련 기업들로부터 트래픽양, 공격 정보 등 이상 징후를 탐지하는 역할을 담당하고 있다. 또한, 국내외에서 발생하는 각종 취약점, 웜·바이러스 정보 등 사이버 공간 위협에 대한 종합적인 정보를 수집하고 국내 주요 ISP 및 보안 업체들과 협력관계를 강화하여 침해사고 예방 활동을 한다.

국외 현황[8,10]으로 미국은 2004년부터 US-CERT에서 취약성과 침해사고 관리 및 경보를 위한 국가 사이버 경보시스템(NCAS : National Cyber Alert System)을 운영하고 있다. 국가 사이버 경보시스템은 사이버 위협에 대한 정보를 적소 적시에 미 국민들에게 제공함으로써 이들이 자신들의 컴퓨터를 보호할 수 있도록 하는 운영 시스템이다. NCAS에 의하여 제공되는 정보들은 모든 컴퓨터 사용자들이 쉽게 이해할 수 있도록 작성되고 있으며, 광범위한 인터넷 사용 실태를 반영하고 있다.

유럽 연합의 ENISA(European Network and Information Security Agency)는 (그림 1)처럼 유럽 조기경보 시스템(EWIS : European Warning and Information System)을 구축하여 각 회원국가의 국가 정보보호조직, 침해사고대응팀, 정보공유 및 분석센터, 기업의 정보보호조직, 개인 등을 연결하는 작업 등을 수행하고 있다.



(그림 1) 유럽의 조기경보체계

일본에서는 2007년부터 3단계의 인터넷 위험 정보 공유 시스템(IRISS : Internet Risk Information Sharing System) 프로젝트를 추진하고 있다. 이 체계는 조기 경보 및 알려지지 않은 공격 분석, 지역 또는 광역 사고의 탐지, 대규모 사이버 공격 예측, 인터넷 위험 상황의 실시간 및 시각적 인식, 악의적인 호스트 목록 작성 등의 기능을 수행하여 기관, 기업 등의 회원사들과 정보를 공유한다.

호주는 미국의 도움으로 기존의 CERT를 중요 정보통신기반구조와 전자정부 상위위원회를 조직하고 정부 및 공공기관, ISAC(Information Sharing and Analysis Centers), CERT간 정보를 공유하는 정책을 택하고 있다. 여기에 조기경보시스템에 활용할 신뢰정보 공유 네트워크를 구축해 각 기관에 공유할 대상정보와 협력관계 및 기술적인 구조를 구현하고 있다.

4. 전사적 조기경보체계 구축 방안

조기경보체계를 구축하기 위해서는 보안정책을 체계적으로 수립하여야 하며, 사이버 공격에 대하여 신속하고 정확한 조기 경보를 위해서는 구현적인 측면에서도 방안을 모색하여야 한다.

4.1. 정책적 측면에서 구축 방안

○ 네트워크 구조의 조기경보시스템 구축

현재 국가 정보보안체계, 사이버안전 관리체계 등은 트리 구조로 구축되어 있다. 그래서 지휘/통제/조정 등의 역할을 수행하는 부모트리가 있고, 통제/조정 받는 자식트리가 있다. 사이버 안전관리를 목적으로 하는 경우에는 이러한 트리구조가 효율적으로 운영될 수 있다. 그러나 사이버 공격에 대한 조기경보시스템을 트리구조로 구축하면 효과적으로 그 기능을 발휘하지 못한다. 사이버 공격은 아주 짧은 시간에 여러 나라, 지역, 기관, 시스템을 동시에 공격할 수 있기 때문에 어느 기관의 시스템이 공격을 받았다면, 다른 기관의 시스템도 동시에 공격을 받고 있다고 생각해도 무방하다. 그래서 조기경보시스템은 맨 하부 트리에 속해 있는 부서가 민간이나 공공기관에 있는 부서에도 경보가 가능할 수 있도록 구축해야 한다.

○ 글로벌 조기경보시스템 구축

보안위협에 효과적인 대응을 위해서는 이홍섭의 'IT839 3대 인프라보호를 위한 사이버공격 예방 및 대응체계 고도화[9]'에서 언급한 바와 같이 사이버 공간을 구성하는 요소들과 각 요소들이 주로 작용하는 계층으로 분류한 후, 계층별 특성에 따라 각각 글로벌 방어체계, 국가 사이버 방어체계, 민간방어체계, 개인 방어체계 등 계층적 방어체계 구축이 바람직하다.

즉, 침해사고가 발생할 수 있는 가능성을 응용의 영역 계층으로 분리하고, 각각의 계층에 따라 적절한 방어체계를 구축함으로써 전체적인 안전성을 확보하도록 하는 것이다. 또한, 신속한 침해사고 공동대응을 위하여 국가 CERT간 협력체계 구축은 필수적이다. 이를 위하여 한국(KrCERT)은 인접국인 중국(CNCERT), 일본(JPCERT)과 전용 회선망을 통해 네트워크 공동 모니터링 체계를 구축하고 한·중·일 3국간의 협력체계 시범 운영을 추진하고 있다. 주변국의 조기경보시스템이 구축되면 미국, 호주 등을 포함한 APEC 회원국으로 점차적인 확대해야 한다.

○ 사이버전 전략과 연계된 조기경보시스템 구축

실질적으로 사이버전을 위한 조기경보시스템은 국가 안보전략의 사이버전 전략과 연계되어 운용되어야 하지만, 현실정은 그렇지 못하다. 미국의 사이버전 대응을 위한 종심

방어전략과 같은 기본개념을 정립하고 국방부가 주도적인 역할을 수행할 수 있는 지휘체계가 갖추어져야 하며, 이를 위해서는 심도 있는 연구와 지원이 선행되어야 한다.

4.2. 기술적 측면에서 구축 방안

○ 전사적 조기경보체계 구축을 위한 조기경보시스템 설계

조기경보시스템에서 사이버 공격 징후 및 발생에 대하여 보안 관리자에게 관련 정보를 제공하는 역할을 수행하는 것을 조기경보센서라 정의할 수 있다. 조기경보센서는 실시간으로 공격 징후를 얼마나 신속하게 감지하는가가 관건이다. 조기경보센서가 얼마나 능동적이고 적극적으로 사이버 공격에 대한 징후를 감지하느냐에 따라서 조기경보시스템의 기능과 성능이 결정된다. 본 논문에서 제안하는 조기경보센서는 비정상행위 기반 센서, 오용행위 기반 센서와 공격 패턴 기반 센서를 융합한 센서이다.

비정상행위 기반 센서(Anomaly based Sensor)는 정상적인 사용자들의 프로파일, 즉 미리 결정된 사용자의 패턴이나 행위를 데이터베이스에 저장하여 탐지한 패턴과 비교하여 공격여부를 판단하는 것이다.

오용행위 기반 센서(Misuse based Sensor)는 일반적으로 알려진 공격 방법을 데이터베이스에 저장하여 탐지한 행동가 비교하여 데이터베이스와 일치하면 공격으로 판단하는 것이다.

공격 패턴 기반 센서(Attack Pattern based Sensor)는 모든 공격이 패턴과 절차를 갖고 있기 때문에 그러한 침입절차를 정의한 후에 탐지한 행위에 대한 절차를 분석하여 탐지하는 것이다.

○ 상관성 분석 모듈 기능 강화

네트워크상에서 운용되는 다양한 보안 시스템은 개별적인 형태의 침입탐지/차단 로그를 생성한다. 이러한 로그 데이터들 간의 상관관계를 분석하여 공격을 신속하게 탐지하는 것은 조기경보시스템에서는 매우 중요하다. 분산되어 있는 여러 보안 시스템으로부터 수집한 로그 정보들간의 상관성을 분석하여 공격발생 가능성을 보다 정확히 감지하고 공격요소를 예측하며 임박한 사이버 공격경보를 신속히 전파할 수 있게 하는 것이 상관성 분석 모듈이다. 상관성 분석 방식은 수행시점, 주체, 대상에 따라 분류된다. 수행시점에 따라서는 실시간으로 수집되는 로그가 데이터베이스로 변환되는 과정의 어느 시점에 상관성 분석이 이루어지는가에 따라 분류되는 것으로 실시간, 근실시간, 사후 상관성 분석으로 있다. 사이버전을 위한 조기경보시스템에서는 실시간 상관성 분석을 수행하는 것이 바람직하다. 수행주체에 따른 분류는 시스템의 과부하를 줄이면서 분석 효과를 증대하고 전파속도를 증가시킬 수 있는 분산 분석을 추천한다. 수행대상에 따른 분류에는 하나의 장비 이벤트 내에서 발생하는 패턴 또는 연관성을 분석하는 단일 수준 상관성 분석과 서로 다른 종류의 장비 이벤트 간의 분석 방법으로 이기종 장비간의 관계적 요소 또는 발생순서에 따른 인과적 요소를 분석하는 다중 수준 상관성 분석을 혼합하여 사용하는 것이 바람직하다.

5. 결론

본 논문은 국가 기간망을 대상으로 사이버 공격을 대비한 전사적 조기경보체계 구축 방안을 제시하였다. 전사적 조기경보체계는 조기경보시스템을 통하여 관련기관이나 관리자간 사이버 공격에 대한 정보를 서로 공유하며, 실시간으로 위협경보를 상호 교환하는 체계를 의미한다.

우리는 국외의 조기경보체계와 조기경보시스템의 특징을 분석하여 국가 기간망에 적합한 전사적 조기경보체계 구축 방안을 수립하였다. 정책적 측면에서는 네트워크 구조 및 글로벌 성격의 조기경보체계를 구축하고, 사이버전 전략과 연계된 조기경보시스템을 구축해야 한다. 기술적인 측면에서는 조기경보시스템의 성능 향상을 위해 능동적이고 적극적이며 신속히 공격 징후를 감지할 수 있는 조기경보센서를 설계하고, 상관성 분석 모듈 기능을 강화해야 한다.

참고문헌

[1] Aleksandr Matrosov et al, “Stuxnet Under the Microscope”, www.eset.com/resources/white-papers/Stux-net_under_the_Microscope.pdf, 2010.

[2] www.yonhapnews.co.kr

[3] 엄정호 외 3명, “사이버 공격과 보안기술”, 홍릉과학출판사, 2009.

[4] 남길현, “군의 사이버전 대응체계 현재와 미래”, 정보과학회지, 제23권 제7호, 2005.

[5] 노훈, 이재훈, “사이버전의 출현과 영향, 그리고 대응방안”, 국방정책연구, 가을호, 2001.

[6] 구자현, “유해 트래픽 조기경보 프레임워크”, 주간기술동향, 통권 1285호, 2007.

[7] 문호건 외 3명, “취약점과 위협의 상관성 분석을 통한 네트워크 위험 조기경보 시스템 설계”, 정보보호학회지, 제15권 제1호, 2005.

[8] 정일안 외 2명, “보안 정보 공유 기술 및 표준화 동향”, 전자통신동향분석, 제23권 제4호, 2008.

[9] 이홍섭, “IT839 3대 인프라보호를 위한 사이버공격 예방 및 대응체계 고도화”, Information Security Review, 제1권 제3호, 2004.

[10] 오일석 외 2명, “미국과 프랑스 정부의 사이버조기경보 체계”, 정보보호학회지, 제15권 제1호, 2005.