http://dx.doi.org/10.3745/KTCCS.2013.2.8.357

Strategies Building Knowledge_Base to Respond Effectively to Advanced Cyber Threats

Tae-Young Lee† · Dong-Gue Park††

ABSTRACT

Our society has evolved into a fully connected society in a mixed reality environment enabling various knowledge sharing / management / control / creation due to the expansion of broadband ICT infrastructure, smart devices, cloud services and social media services. Therefore cyber threats have increased with the convenience.

The society of the future can cause more complex and subtle problems, if you do not have an effective response to cyber threats, due to fusion of logical space and physical space, organic connection of the smart object and the universalization of fully connected society.

In this paper, we propose the strategy to build knowledge-base as the basis to actively respond to new cyber threats caused by future various environmental changes and the universalization of fully connected society.

Keywords : Target Attacks, Advanced Persistent Threats, Cyber Threats, National Security Knowledge_Base

고도화된 사이버 위협에 효과적으로 대응하기 위한 Knowledge__Base 구축전략

이 태 영† · 박 동 규††

요 약

우리 사회는 광대역 ICT 인프라의 확충과 스마트 디바이스, 클라우드 서비스 및 소셜 미디어 서비스의 활성화로 인해 언제 어디서나 다양한 지식의 공유 / 관리 / 제어 / 창조가 가능한 혼합현실 환경의 상시 연결사회로 진화하고 있고 이로 인해 사이버 위협이 점차 증가하고 있는 상황이다.

향후 사회는 물리 및 논리공간의 융합, 스마트 객체의 유기적 연결, 상시연결 사회의 보편화로 인하여 사이버 위협에 대한 효과적 대응을 하지 못하는 경우에 더욱 복잡하고 미묘한 문제를 야기할 수 있어 APT와 같은 고도화된 사이버 위협에 대한 새로운 접근방법과 대응 체계에 관한 연구가 요구된다.

본 논문에서는 향후 다양한 미래서비스 환경 변화와 상시 연결사회의 보편화에 따른 새로운 유형의 사이버 위협에 능동적으로 대응하기 위한 기반으로써 국가 보안 Knowledge-Base 구축 전략을 제시한다.

키워드 : 타켓공격, 지능형지속가능위협, 사이버 위협, 국가 보안 지식베이스

1. 서 론

우리 사회는 광대역 ICT 인프라의 확충과 스마트 디바이스 보급, N드라이브/유클라우드/다음 클라우드 등의 클라우드 서비스 확대와 더불어 페이스북/카카오톡/유튜브와 같은 소셜 미디어 서비스의 활성화로 인해 언제 어디서나 다양한 지식의 공유/관리/제어/창조가 가능한 상시 연결사회로 진화하고 있다. 이로 인해 사람들의 일상생활 패턴은 시간과 공간의 제약을 벗어나게 되었으며, 사이버공간과 현실공간의 구분이 없는 서비스 제공으로 혁신적인 형태로 변화하고 있는 상황이다. 이러한 편의성과 함께 증가하고 있는 사이버 위협은 조직적인 방법으로 진화하고 있고 특정 기업이나 국가를 대상으로 장기간의 기획침투 및 잠복, 정보유출 등의 지능형 지속가능 위협(APT: Advanced Persistent Threats) 공격의 성격을 나타내는 등 정치적인 성격의 공격으로 발전하고 있다. 구글 해킹 사건, 오퍼레이션 오로라(Operation Aurora), 이란 원전을 마비시켰던 스턱스넷(Stuxnet), 글로

※ 이 연구는 2012년 국가정보화전략위원회의 지원에 의하여 수행되었음.
† 준 회 원 : 순천향대학교 정보통신공학과 석사과정
†† 정 회 원 : 순천향대학교 정보통신공학과 교수
논문접수 : 2013년 5월 31일
수 정 일 : 1차 2013년 7월 25일
심사완료 : 2013년 7월 25일
* Corresponding Author : Dong-Gue Park(dgpark@sch.ac.kr)

벌 에너지 기업을 노렸던 나이트 드래건(Night Dragon), RSA 사의 OTP 기술 유출 사고 등은 특정 지역, 특정 국가를 대상으로 한 고도화된 APT 공격의 대표적인 사례로 거론되고 있고 이로 인해 국가 간 사이버전에 대한 우려를 사고 있다. 따라서 이러한 사이버 위협에 효과적으로 대처하지 않으면 국가의 안보가 위태로운 지경에 이를 수 있어 이에 대한 체계적이고 능동적인 대응전략을 국내·외에서 연구, 개발 중에 있지만 아직까지는 미진한 상황이다.

본 논문에서는 인터넷을 통한 물리 및 논리공간의 융합과 스마트 디바이스에 의한 이동성이 극대화되는 환경변화에 따른 고도화된 사이버 위협인 APT를 분석하고, 3장에서는 국가 사이버 공격 대응 기술 현황을, 4장에서는 국가 사이버 공격 대응 체계 현황을 분석하고 이를 기반으로 5장에서 향후 다양한 미래서비스 환경 변화와 상시 연결사회의 보편화에 따른 새로운 유형의 사이버 위협에 능동적으로 대응하기 위한 기반으로써 국가 보안 Knowledge-Base 구축전략을 제안하고, 6장에서 결론을 맺는다.

2. 고도화된 사이버 위협인 APT 분석

APT 공격은 최신 기술로서 기존의 공격이 불특정 다수를 대상으로 시도한 것과는 달리 명확한 표적을 정하여 공격자가 목적을 달성할 때까지 장기간 동안 지속적으로 정보를 수집하고, 이를 바탕으로 치밀한 공격을 감행한다는 점에서보다 지능화된 기법이라고 볼 수 있으며, 공격의 방식도 시스템에 직접 침투하는 것뿐 아니라, 표적이 된 조직의 내부 직원들이 이용하는 다양한 단말기 등에 대한 우회 공격들을 사용한다는 점에서보다 정밀한 공격 방식이라고 할 수 있다. 그러므로 APT와 같은 고도화된 위협에 대응하기 위해서는 기존의 방어보다 심도 있고 조직적인 대응이 필요하며 개별 보안 기술 및 솔루션 적용이 아닌 전사 및 통합 차원의 보안 체계 구성이 필요한 상황이다.

현재 APT 공격을 방어하기 위하여 전 세계의 모든 보안 관련 기업들과 보안 관련 기관에서 많은 연구를 진행하고 있는 중이다[1-13]. 각각의 연구에서는 APT의 피해 사례 분석을 통하여 APT 공격의 특성을 파악하고 APT 공격을 단계별로 분석하여 다 계층화된 데이터 중심의 깊이 있는 방어 대책을 수립하고 있는 중이다. 그러나 아직까지도 완전하다고 할 수 있는 해결 방안은 없으며, 특히 국가적인 대응 체계에 관한 연구는 미진한 편이다.

APT 공격은 일반적인 공격과 더불어 제로데이(Zero-Day) 취약점, 루트킷과 같은 고도의 지능적인 보안 위협을 동시에 이용하여 목표에 침투해 은밀히 정보를 빼돌리는 킬 체인(Kill Chain)을 생성하는 특징을 갖는다. 또한, APT 공격은 보안탐지를 회피하기 위하여 은밀하고, 천천히 움직여야 하기 때문에 일반적인 공격에 비해 몇 배가 되는 긴 시간 동안 공격이 행해진다. 보통 다수의 표적공격이 순식간에 목표를 공격해 필요한 정보를 탈취해 간다면, APT는 목표 시스템에 활동 거점을 마련한 후 은밀히 활동, 새로운 기술과 방식이 적용된 보안 공격들을 지속적으로 공격해 정보 유출이나 삭제, 시스템에 대한 물리적인 피해 등 공격자들이 궁극적으로 원하는 목적을 이루기 위해 행해지는 공격이다.

Fig. 1. APT attack phase

APT는 주로 국가 간 첩보 활동이나 기간 시설 파괴 등의 특정 목적을 달성하기 위해 행해지며, 대부분 배후에 후원하는 첩보 조직이나 단체가 연관되어 있는 경우가 많으며, 이는 APT가 단순히 정보 유출만을 노리는 것이 아니라 공격자가 지속적으로 표적을 원격 조종하여 정보 유출을 포함한 시스템에 운영을 방해하거나 물리적인 타격까지도 유발하는 공격이다[1].

지적 재산권이나 가치 있는 고객 정보를 가진 거의 모든 조직이 표적공격의 대상이라면, APT는 주로 정부기관이나 기간 시설, 방위 산업체, 그리고 전 세계적으로 경쟁력 있는 제품, 기술을 보유한 주요 기업들과 이들의 협력업체 및 파트너 기업들을 대상으로 한다[2].

APT는 USB, 외장하드 등 네트워크를 이용하지 않고 정상적인 트래픽 경로를 사용하는 경우가 대부분이기 때문에 방어가 매우 어렵고, 정상적인 메일이나 웹 사이트 등을 통해 악성코드 배포가 가능하기 때문에 이를 사용하여 표적에 가해지는 APT 공격을 완벽하게 차단하기는 매우 어렵다[3].

국내·외의 주요 APT 해킹 피해 사례를 예로 들면 국내에서는 농협 전산망 해킹사건, 현대캐피탈 해킹 사건, 네이트/싸이월드 개인정보 유출 사건, 3.20 전산망 마비사태 등을 들 수 있으며, 국외에서는 달빛 미로 사건, 미국 하원 사건, 미국 국방부 사건, 교황 달라이 라마 사무실 사건, 영국 RBS 월드페이 해킹 사건, 미국 오크리지 국립 연구소 해킹 사건, 이란 원자력 발전시설 해킹 사건(스턱스넷), 다국적 석유회사 해킹 사건(일명 Night Dragon), RSA 해킹사건, 모건 스탠리 해킹사고(일명 오로라 사건), GhostNet 사건, 프랑스 정부 사건, 캐나다 정부 사건, 호주 정부 사건, 록히드 마틴 사건, 국제 통화 기금 (IMF) 사건 등을 예로들 수 있다[4][5].

APT 공격 단계는 각 연구마다 조금씩 차이가 있으며 대표적인 분석단계를 보면 Fig. 1과 같이 정찰, 준비, 타겟팅, 접근 확장, 데이터 수집, 유지의 6단계를 수행한다[5].

3. 국가 사이버 공격 대응 기술 현황

3.1 국내 사이버 공격 대응 기술 현황

국내에서도 사이버 공격 대응을 위한 연구를 수행해 오고 있었다. 한국인터넷진흥원(KISA)에서는 봇 넷 연구를 수행하였으며, 한국전자통신연구원(ETRI)에서도 자스민(ZASMIN)

프로젝트를 수행하여 사이버 공격에 대한 공격 시그니처를 실시간으로 생성·관리하는 방법을 개발하였다[14][15][16].

한국전자통신연구원에서 개발한 악성코드 탐지시스템은 알려지지 않은 공격들에 대한 공격특징을 탐지하고, 이를 기반으로 해당 공격을 네트워크상에서 탐지할 수 있는 공격 시그니처를 실시간으로 생성 및 관리 하는 시스템이다[14].

한국인터넷진흥원(KISA)에서는 봇 넷 연구를 수행하였으며 안전한 인터넷 서비스 제공을 위한 신종 봇 넷 능동형 탐지 및 대응 기술을 개발하였다.

한국인터넷진흥원에서 개발한 봇 넷 능동형 탐지 및 대응 기술은 봇 넷 고유의 그룹행위를 기반으로 다양한 유형의 봇 넷을 탐지/분석할 수 있으며, 악성 봇의 형태 및 특성에 상관없이 네트워크 트래픽 분석을 통한 행위 기반으로 봇을 탐지/분석할 수 있다. 또한, 능동형 악성 봇 탐지 기술을 통해 다양한 악성 봇의 감염 경로를 차단할 수 있으며, 악성 봇의 감염 통보 및 치료 유도가 가능하다[15][16].

그러나 국내에서 수행된 사이버 공격 대응 연구는 고도화된 공격에 대응하기에는 다음과 같이 부족한 점이 존재한다. 한국인터넷진흥원에서 수행된 봇 넷 능동형 탐지 및 대응 기술은 서버의 봇 감염 여부는 알 수 있으나 서버를 통해 감염된 호스트의 정보는 알 수 없는 단점이 있다. 그리고 한국전자통신연구원에서 개발한 자스민 시스템도 사이버 공격에 대한 공격 시그니처를 실시간으로 생성하고 관리할 수 있지만, 비정상행위 분석 시 분석을 통한 결과가 악성코드 데이터베이스하고 매칭이 안 되는 단점을 가지고 있다. 그리고 두 시스템 다 악성코드별 분포 현황, 악성코드 전달 경로 현황, 좀비 연계도 현황 등 고도화된 사이버 공격에 사전 대응을 하기 위한 정보 구축이 불가능한 상황이다.

3.2 국외 사이버 공격 대응 기술 현황

국외에서도 사이버 공격 대응을 위한 연구를 수행해 오고 있었다. 그 중 대표적인 프로젝트로 자동화된 정보 수집과 전달 시스템을 갖춘 에셜론 프로젝트(ECHELON Project)와 연방 망을 통과하는 인터넷 트래픽을 실시간 모니터링하여 사이버 공격의 가능성이 있는 비정상적인 상태를 탐지하는 아인슈타인 프로그램을 들 수 있으며, 또한, 허니팟 기술을 사용하여 공격 정보와 공격 차단 시그니처를 생성하는 노아(NoAH) 프로젝트를 예로 들 수 있다.

에셜론 프로젝트는 전 세계에 걸친 자동화된 정보 수집과 전달 시스템을 지칭하는 암호로, 미국 NSA의 주도하에, 호주 Defense Signals Directorate(DSD)를 비롯한 다른 국가 기관들과 함께 운영되고 있다. 또한, 영국의 Government Communications Headquarters(GCHQ)와 각종 조약에 따른 미국의 여타 동맹 기관들도 이에 가담하고 있다[17]. 이러한 국가들은 1947년의 UKUSA 협정에 따라, 그들의 활동을 조정하기 시작하였고, 에셜론은 전화, 이메일, 인터넷 다운로드, 위성송신 등을 포함하여 매일 30억 통신을 가로챌 수 있다고 알려졌다. 에셜론 시스템은 모든 전파 송신들을 무차별적으로 수집하여, 인공 첩보 프로그램을 통해 가장 핵심적인 정보만을 추출할 수 있다고 한다. 그러나 에셜론의 정확한 능력과 목적은 아직 불분명하다[18].

미국의 국토안보부(DHS)는 군사용 네트워크를 감시하는 국방부의 프로그램을 이용해 2003년에 처음 아인슈타인 프로그램을 개발했다. 이 프로그램은 교통부와 같은 연방정부 기구의 인터넷으로 들어오고 나가는 정보의 흐름을 추적하여 사이버 공격일지 모르는 비정상적인 흐름을 찾아내는 것으로 시작하여, 알려져 있는 사이버 공격 유형을 찾아내 사이버보안센터에 즉각 경보를 발생시킬 수 있는 형태로 발전하게 되었다. 그러나 이 프로그램도 알려지지 않은 정교한 공격을 막거나 찾아내지 못하는 문제가 존재했었다[19]. 아인슈타인은 미국 정부 및 공공 기관의 사이버보안을 강화하기 위해 구축한 보안 프로그램으로 1, 2, 3의 세 가지 버전으로 나누어진다. 아인슈타인 1, 2는 침입 탐지에 중점을 두고 있으며, 아인슈타인 3은 미리 예방하는 데 주력하고 있다[20].

유럽에서는 허니팟 기술에 기초하여 사이버 공격 시그니처를 생성하는 노아 프로젝트를 수행하였다. 노아 프로젝트는 허니팟 기술에 기초하여 보안 모니터링을 위한 인프라의 개발을 위해 필요한 기술적인 작업들을 수행하고 설계하는 데 그 목적이 있었다. 노아가 지향하는 것은 사이버 공격 발생 시 정보 보안 관련 조직들과 인터넷 서비스 제공자들의 피해를 최소화하고, 정보 보안 관련 조직들이 해당 위협에 더욱 능동적으로 대처하도록 하며, 연구자들에게 탐지 기술 향상을 위한 좋은 자료를 제공하는 것이다. 노아 프로젝트는 학계, 연구소, 산업체 등 8개의 파트너가 참여하고 있으며, 유럽 연합의 연구 인프라 프로그램에서 지원하고 있다[14].

국외에서도 위와 같이 사이버 공격 대응을 위한 연구를 수행해 오고 있지만, 국외에서 수행된 사이버 공격 대응 연구도 고도화된 공격에 대응하기에는 다음과 같이 부족한 점이 존재한다. 에셜론 프로젝트는 자동화된 정보 수집과 전달 시스템은 갖추었으나 실행코드를 탐지할 수 없으며, 아인슈타인 프로그램도 트래픽의 실시간 모니터링으로 비정상적인 상태를 탐지할 수는 있지만, 여전히 실행코드를 탐지할 수 없는 문제를 가지고 있다. 또한, 노아 프로젝트도 공격 차단 시그니처를 생성할 수는 있지만, 여전히 고도화된 사이버 공격에 사전 대응을 하기 위한 정보 구축이 불가능한 상황이다.

2012년에 들어와서 사이버 전을 대비한 새로운 계획을 미국에서 추진하는 중이다. 미국 국방부는 실전투입용 사이버 무기 개발을 위한 대규모 프로젝트 '플랜 X'를 추진하고 있다. '플랜 X'는 국방부 산하 방위 고등 연구 계획국(DARPA)이 주도할 예정으로, 민간기업과 대학, 게임업체들도 대거 참여한다. '플랜 X'는 적국의 방공망과 지휘통신체계를 무력화시키는데 초점을 두어, 미국 사이버 전략의 방향 전환을 시사하고 있다. '플랜 X'는 적군의 통신망 레이더를 무력화시키는 것은 물론 전 세계 수백억대 PC의 위치를 담은 사이버 전자지도 작성 계획도 포함되어 있다. 전 세계

모든 컴퓨터의 도메인을 담은 사이버 지도를 작성하고 견고한 운영체계를 개발하여 사이버전 발생 시 적군의 PC를 한 번에 무력화시키겠다는 의지를 포함하고 있다[21]. 미국의 플랜 X와 같은 최근의 추세를 볼 때 국가적으로 고도화된 사이버 공격에 대응하기 위한 체계적인 방안에 대한 수립이 필수적이라고 할 수 있다.

4. 국가 사이버 공격 대응 체계 현황

4.1 국내 사이버 공격 대응 체계 현황

우리나라의 국가 사이버 안전 체계는 '국가 사이버 안전 관리 규정'에 의해 정부가 국가안보차원의 사이버 위협에 대한 대응을 보다 강화하여 국가 인터넷망의 전자적 침해사고 조기탐지 및 피해확산 방지를 위해 구축한 범국가적 체계이다. 한국인터넷진흥원의 '인터넷 침해 대응 센터'가 민간분야를 담당하고, 국가안전보장회의(NSC) 사무처 주관하에 범정부적 차원에서 출범한 국가정보원 소속의 '국가 사이버 안전 센터 (NCSC :National Cyber Security Center)'가 공공분야를 담당하며, 국방정보본부 산하의 '사이버사령부'가 군 분야를 담당하는 민·관·군 종합 대응 체계이다.

최근 사이버 위협은 단순한 웜 바이러스 유포에서 탈피, 각종 악성코드를 결합한 웹 해킹, 대규모 네트워크를 이용한 DDoS 공격, 무선인터넷 해킹 등 다양한 형태로 고도화되고 발전하고 있다. 따라서 사이버 피해를 최소화하기 위해서는 국가 전산망에 대한 이러한 침입시도를 미연에 탐지하는 활동이 중요하다. 현재까지 사이버 위기 대응과 관련된 업무는 소관부처별로 이루어졌으며, 각 부처의 업무범위는 정보자산과 기반시설에 대한 침해사고 대응 및 복구에 한정되고 있다. 따라서 제어시스템이나 주요 정보통신기반시설로 지정되지 않은 시스템은 현행 법체계로는 보호할 수 없어 사이버 공격에 무방비로 노출되어 있다. 또한, 이에 대한 종합적이고 체계적인 대응이 이루어지고 있지 않아 새로운 국가 안보 위협으로 떠오르고 있는 것이다. 특히 현대의 APT 공격과 같이 고도화된 공격에 의한 사건들을 통해 이미 사이버 공격이 국가·사회적으로 파급력이 막대하여 새로운 국가 안보의 위협 요인으로 대두되고 있다는 것을 잘 보여 주고 있다. 현대의 사이버 위기는 바로 국가적인 위기인 것이다. 이미 사이버 공격은 국가안보의 새로운 위협요인으로 대두되었으나 민·관 분야별 구분대처로 인하여 한계성에 직면하고 있으며, 특히 APT와 같은 고도화된 공격을 방지하기 위해서는 국가 차원의 일원화된 체계적인 사이버 공격 대응 조직이 필요한 상황이다[22].

4.2 국외 사이버 공격 대응 체계 현황

세계 각국은 사이버전 전담부대를 창설하는 등 사이버 공격 대응능력을 국가 및 국방 핵심전략으로 추진하고 있는 상황이다. 이 장에서는 사이버침해를 효과적으로 대응하기 위하여 주요국의 사이버 공격 대응 체계에 대해 살펴보기로 한다[22].

미국은 2008년 1월에 신 사이버보안을 위해 '국가 사이버 보안 종합 전략'이 수립되었으며, 오바마 행정부가 수립된 이후에 2009년 5월 말에는 '사이버공간 정책 리뷰'가 발표되었고, 특히 단기실행계획 첫 번째로 국가 사이버보안정책 추진을 총괄할 사이버보안책임관을 임명할 것을 제안되었다. 이에 따라 오바마 대통령은 2009년 12월 22일에 사이버 보안조정관을 임명하였으며, 사이버보안조정관은 미국 국가안전보장회의(NSC)에 상주하면서 대통령과 NSC에 정기적으로 보고하며, 미군과 민간기관의 연방정부 사이버보안정책 마련을 위한 자문관으로 역할을 수행하고 있다. 특히, 2010년 5월 27일 오바마 정부는 출범 후 처음으로 국가안보의 현황과 지향점을 공개 발표한 국가안보전략에서 사이버 보안의 의미와 향후 정책 방향을 중요한 전략으로 다루고 있다. 이처럼 미국은 사이버보안과 관련한 정책을 추진하는데 있어 가장 의욕적이고 강력하게 추진하고 있는 대표적인 나라로 평가되고 있다[22].

영국은 기술적인 측면에서 미국과 함께 사이버 안보 분야를 선도하고 있는 국가 중 하나이다. 영국 정부의 정보보호에 대한 노력은 법률에 따른 행위규제보다 일반 국민에게 정보침해에 대한 의식을 제고하고 사전적 대처 방안계획과 실행 역할에 중점을 두고 있다. 조사권한규제법(RIPA), 컴퓨터 부정사용법, 대테러 범죄 및 안전 보장법 등으로 해커와 바이러스 유포자를 처벌하고 있으며, 스팸 관련 규제는 프라이버시 법리와 전기통신지침 등으로 이루어지고 있다. 영국은 정보통신 환경 변화와 이에 따른 정보보안 환경 변화에 적극적으로 대처하고 있으며, 이에 따라 정보보안과 관련한 입법 활동도 비교적 활발한 국가 중 하나이다. 정보보안과 관련해서 영국은 사이버범죄를 처벌할 수 있는 법률을 중심으로 상당히 적극적으로 관련 법률과 제도를 발전시켜 왔으며, 특히 EU의 각종 지침을 자국법으로 현실화시켜 국제적으로도 정보보안을 선도하고 있다[22].

독일은 정보 보안을 통해 정보통신기술의 신뢰를 조성하고 정보사회의 기회를 최대한 이용하기 위해 독일 자체의 정보보안 가이드라인을 제정하여 시행하고 있다. 독일은 미래사회에서의 정보보호 및 정보보안에 대한 중요성을 깨닫고 1991년에 연방정보기술안전청(BSI)을 창설하여 상당한 예산 및 인력투자를 해 왔다. 독일의 경우 정보보안을 위해 국가적 차원에서 상당한 지원을 하고 있고, 경제 분야에 있는 기업도 점차 정보 보안과 관련한 책임의 중대성을 인식하고 대비책을 마련하는 과정에 있다[22].

프랑스는 1998년 이후 매우 의욕적이고 계획적으로 정보화를 추진하고 있다. 프랑스는 중앙 정보 시스템 보안국(DCSSI) 내에 프랑스 정부 CERT인 CERTA를 구축 운영하고 있으며, 사이버보안 운영 센터를 구축하여 각급 기관에 대한 사이버 위협정보를 제공하고 있다. 아울러 프랑스 정부는 사이버보안 위기관리 체계를 수립하여 경계 수준을 5단계로 분류하고 DCSSI로 하여금 각 경계단계에 따른 일련의 사이버보안 기능적 조치를 수행하도록 하고 각 정부부처로 하여금 사이버보안 조치를 실행하도록 하고 있다[22].

일본은 정부기관인 관방성 주도하에 2006년 2월부터 3개년씩 정보보호 기본 계획을 수립하여 1차와 2차에 걸쳐서 사회기반 및 생산설비에 대한 사이버 테러리즘 대책을 수립·시행하였다. 최근 2010년 7월에 일본정부는 대규모 사이버 공격에 대한 대처, 정보 보안정책의 강화 시책으로 '정보시큐리티 2010'시책을 발표하였고, 대규모 사이버 공격에 대한 대처 시책으로는 적절한 초동 대처를 위해 내각 관방에 태세를 정비하고 훈련을 실시하거나, 방위성에 사이버 기획조정관 (가칭)을 배치, 정보 수집 공유 체제 구축 강화 등이 있다[22].

세계 각국의 보안 정책에서도 명시된 바와 같이 APT와 같은 고도화된 위협에 종합적이고 체계적인 대응하기 위하여 국가 사이버보안정책 추진을 총괄하는 방안이 절실하게 필요한 상황이다.

5. 국가 보안 지식베이스(Knowledge-Base) 구축

우리나라의 사이버 공격 위기관리 체계에서 부분별로 서로 다른 조직에 속한 IT 보안 관리자들은 많은 같은 위협들에 직면하고 유사한 해결 방안을 사용하며, 같은 지식을 수집하고 적용한다. 그러나 그들 대부분은 그들 자신의 지식과 정보에 의존하여 일을 수행하고 있으며, 이것은 매우 비합리적인 방식이라고 할 수 있다. APT 공격과 같은 새로운 유형의 사이버 위협에 능동적으로 대응하기 위하여 국가 차원의 보안 지식베이스 구축 전략 및 이를 기반으로 한 사이버 위협 대응 체계에 관한 연구가 필수적으로 수행되어야 한다.

지식베이스체계를 구축하기 위해서는 공통의 보안 지식베이스를 생성하기 위한 전략이 첫 번째 단계이고 두 번째로 국가 정보통신서비스 인프라의 안전을 도모하기 위한 선제적 공격 대응이 가능한 국가 보안지식 관리 모델 개발이 필요하며, 신뢰를 통한 지식 공유방안 및 공유된 지식을 서비스하기 위한 전략이 수립되어야 한다.

네트워크를 통해 수많은 정상적인 실행 코드와 백신 등에서 탐지가 가능한 악성코드들이 전달되고 있다. 이러한 정상 실행 코드나 알려진 악성코드를 네트워크에서 실시간으로 확인할 수 있는 지식데이터베이스가 구축되고, 이를 실시간으로 확인할 기술이 개발된다면, 데이터베이스에 존재하지 않는 실행코드를 집중 분석하여 새로운 악성코드를 찾을 기회가 만들어질 수 있다. 하지만 현재 이러한 데이터베이스가 존재하지 않을 뿐만 아니라, 알려진 악성코드가 호스트로 유입되어도 전체 네트워크에서 이를 알 수 있는 시스템이 없어 국가적으로 악성코드의 유포나 감염 정도를 실시간 모니터링 할 수 없는 상황이다.

모든 실행 가능한 코드가 국가 네트워크에서 어떻게 유포되고 있으며, 국가 데이터베이스에 존재하지 않는 새로운 코드가 유포되고 있는지 실시간으로 모니터링할 수 있는 국가 보안지식 데이터베이스 구축 및 실시간 검색 기술을 개발함으로써 국가의 보안을 한 단계 업그레이드할 필요가 절실한 상황이다.

5.1 추진 체계

국가 보안 지식베이스란 국내에서 사용되는 모든 실행 가

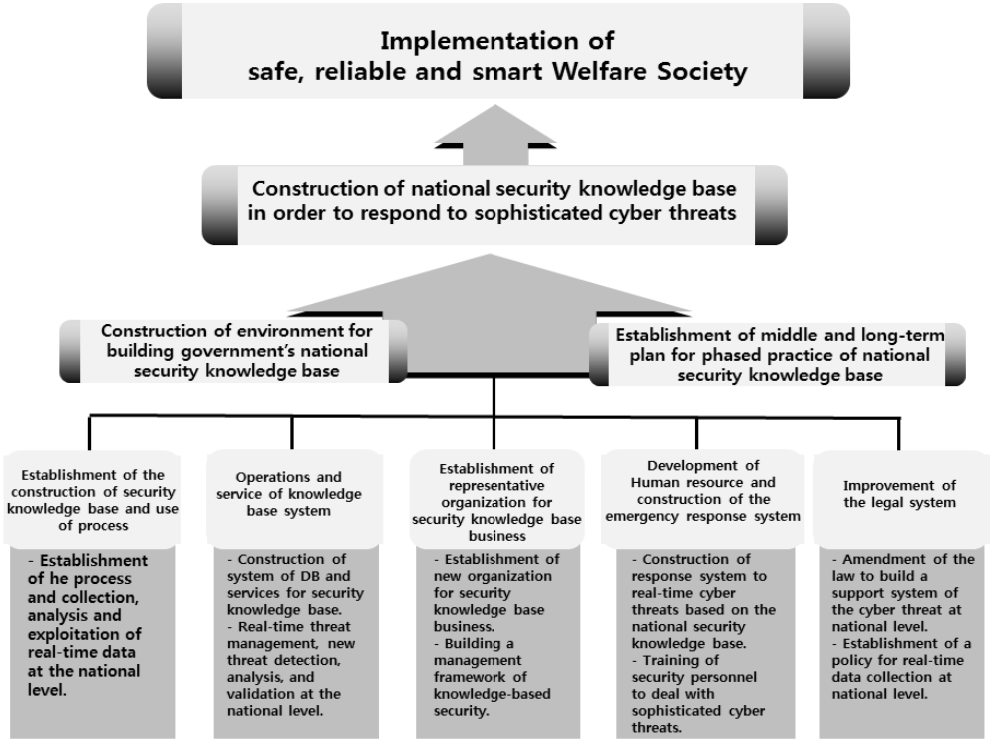

Fig. 2. Promotion system for construction of national security knowledge base

능한 코드에 대한 국가 데이터베이스를 지칭하는 것으로, 이러한 데이터베이스는 정상 파일들과 국내에서 유통되는 모든 종류의 백신에서 탐지되는 악성코드에 대한 데이터베이스를 구축하고 네트워크를 통해 전달되거나 호스트에 새로 유입된 실행 코드를 확인하여 실행 코드의 유통을 검색·제어할 수 있는 국가 정보 시스템을 말한다. 국가 보안 지식베이스 구축을 위하여 본 논문에서는 다음 Fig. 2, 3과 같은 추진전략을 수립한다.

범국가 차원의 실시간 보안 지식베이스의 구축 및 관리 그리고 이를 기반으로 하는 사이버 위협 대응 체계 구축은 오직 정부만이 추진할 수 있다. 정부의 주도하에 조성할 수 있는 보안 지식베이스의 구축 및 환경에 관한 추진전략은 다음과 같다.

- 신뢰할 수 있는 보안 지식베이스 구축 환경조성을 위하여 기본 트래픽 데이터 정보 및 활용 데이터베이스 정보에 대한 검증 및 부실 요소 제거
- 최신의 화이트리스트 및 블랙리스트 데이터베이스의 구축을 위하여 관계기관의 연계 프로세스 수립 및 관련 사업 지원
- 보안 지식베이스를 기반으로 범국가 차원의 위기 대응 체계를 구축하기 위하여 관계기관과의 업무 협조 체제 구축
- 최신의 보안 지식베이스 구축을 위하여 관계 법령 개정을 통한 실시간 데이터 수집을 위한 근거 마련
- 보안 지식베이스가 적극적으로 활용될 수 있도록 대응기관, 학계, 산업계 등에 객관성이 부여된 양질의 정보 제공

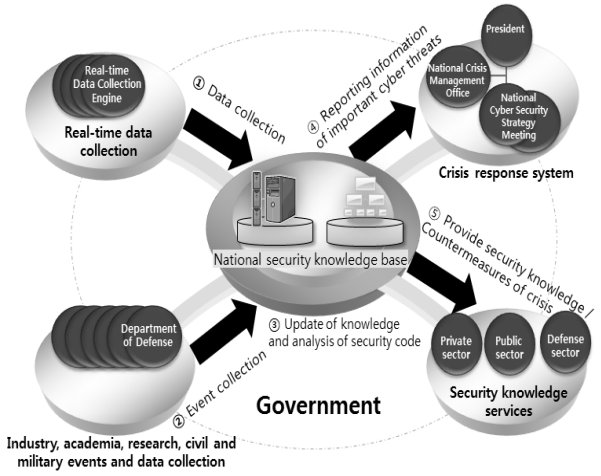

Fig. 3. Construction of environment for building national security knowledge base

국가 차원의 보안 지식베이스의 단계별 추진을 위한 중장기 계획은 다음 Fig. 4와 같다. 1 단계(1차년도)는 보안 지식베이스 구축 마스터플랜 도출을 통하여 중장기 계획을 체계적으로 마련하는 단계로 그 내용은 다음과 같다.

- 보안 지식베이스 구축 프로세스의 확립 및 관련 제도를 제·개정하기 위한 준비

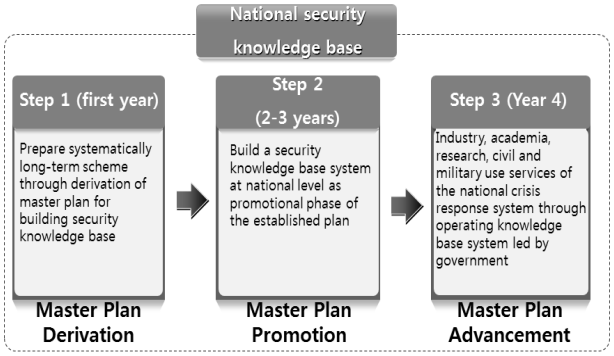

Fig. 4. Long-term plan for promotion of national security knowledge base

- 보안 지식베이스 전담 조직을 신설하는 등 성공적인 정보 공유 체계 구축을 위한 중장기 종합 계획 수립 단계

2 단계(2차년도~3차년도)는 수립된 계획의 추진단계로 국가 차원의 보안 지식베이스 시스템을 구축하며, 그 내용은 다음과 같다.

- 국가 차원의 실시간 데이터 수집 및 분석 프로세스 구축
- 보안 지식베이스 구축프로세스를 도입하고, 실시간 트래픽 수집 및 데이터 분석을 통합 관리하기 위한 데이터베이스 및 관리 시스템 구축
- 보안 지식베이스 시스템 이용을 위한 사용자 인터페이스 개발
- 국가 보안 지식베이스를 기반으로 한 위기 대응 체제 구축
- 국가 차원의 보안 지식베이스 체계 구축 및 위기 대응 체제 구축을 위한 법·제도의 제·개정 추진

3 단계(4차년도 이후)는 국가 차원의 보안 지식베이스 체계 정착 및 고도화 단계로 정보주도로 시스템을 운영하여 국가 위기 대응 체계를 갖추고 산·학·연·민·관·군이 함께 활용하는 단계로 그 내용은 다음과 같다.

- 실시간 위기 대응 체계의 고도화를 위하여 실시간 데이터 수집 및 분석 프로세스의 양적·질적 향상을 수행
- 고도화된 사이버 위협에 대응하기 위하여 실행코드 블랙리스트 및 화이트리스트 데이터베이스의 고도화
- 실행 코드 데이터베이스의 공유 채널을 미국이나 일본 등 국외로 확대
- 국가 보안 지식베이스를 기반으로 한 위기 대응 체제의 고도화

5.2 추진 과제

국가 보안 지식베이스를 구축하기 위한 추진 과제로 다음과 같은 내용을 들 수 있다.

1) 보안 지식베이스 구축 및 활용 프로세스 수립

국가 차원의 실시간 데이터 수집 및 분석 그리고 위기 대응 체계에 관한 프로세스를 정립하고, 보안 지식베이스 전담 기관의 데이터 수집 및 타 기관에서 수집된 정보의 지식

베이스화 및 보안 지식베이스의 활용 프로세스를 수립한다.

국가 보안 지식베이스 구축을 위하여 다음과 같은 단계를 수행하도록 한다.

a) 정상 파일에 대한 데이터베이스 구축을 위해 국내·외에서 개발된 정상 파일에 대한 시그니처와 해시 값 등을 화이트리스트로 구성한다.

b) 국내·외에서 유통되는 백신들을 설치한 시스템을 클라우드로 구성하고 네트워크에서 수집된 모든 실행 파일을 검사하여 탐지되는 경우 자동으로 시그니처 및 해시 값 등을 추출하여 블랙리스트를 구성한다.

이외 현재까지 개발된 비정상행위 탐지 기법 및 실행 기반 악성 유무 탐지를 위한 시스템을 클라우드로 구성하고 a), b)에서 확인되지 않는 모든 파일을 검사하여 화이트리스트, 블랙리스트, undefined 등의 데이터베이스를 자동 구축한다. 또한, 새로운 탐지 기법이 되면 이를 수용하기 위한 open API를 개발한다.

이들 데이터베이스를 구성하고 네트워크에서 전달되는 모든 파일에 대해 실시간 모니터링 할 수 있는 GUI를 구성하여 국가 네트워크에서 전달되는 모든 실행코드의 악성 여부를 파악하고, 데이터베이스의 블랙리스트에 매칭된 코드는 자동 행위 추적 또는 자동 차단하는 기능을 수행하여 새로운 공격에 대응한다.

보안 지식베이스 활용을 위한 시나리오는 다음과 같다.

- 시나리오 1 : 사이버 위협에 대응하기 위하여 보안 지식베이스 전담 기관에서 직접 데이터를 수집 및 분석 후 조치하는 경우의 보안 지식 활용 프로세스

① 실시간 데이터 수집 및 분석 또는 유관 조직에서 제공한 정보 제공을 통해 보안 지식이 될 수 있는 정보 수집

② 보안 지식베이스 전담 기관은 수집된 데이터의 분석 및 보안 지식베이스화를 수행하고 관계기관과의 협력을 통하여 필요하다면 패치 제작과 패치 검증을 수행하고 위기관리 대응 체계에 따라서 민간, 국가·공공, 국방 분야 등 국가적인 사이버 위협 대응을 수행하도록 한다.

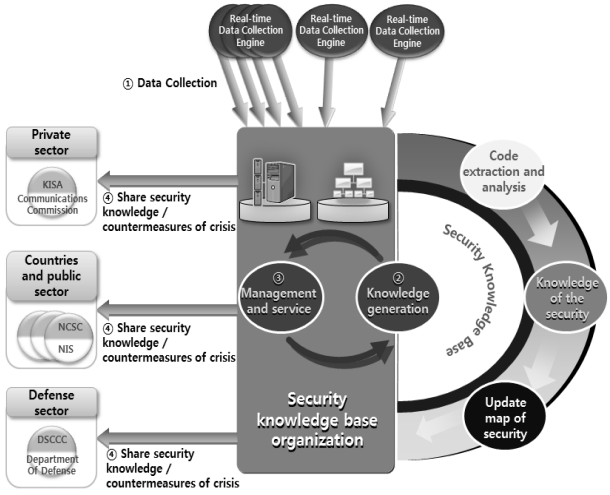

Fig. 5. Scenario 1 for use of national security knowledge base

- 시나리오 2 : 기존 관련 분야 즉 민간, 국가·공공, 국방 분야의 정보보호 업무를 담당하는 기관에서 악성코드 관련 정보 등을 수집한 경우의 보안 지식베이스 정보 구축 및 활용 프로세스

① 기존 악성코드 수집 시스템 및 신고접수로 악성코드 관련 정보가 각 관련 부처별(KISA, NCSC 등)로 수집되는 경우 보안 지식베이스 전담 조직으로 전달되어 분석 및 검증을 거쳐 보안 지식베이스화를 수행한다.

② 보안 지식베이스 전담 기관은 타 기관에서 수집된 정보를 기반으로 악성코드 전달 이력 보안 맵을 갱신하고, 위기관리 대응 체계에 따라서 민간, 국가·공공, 국방 분야 등 범국가적인 사이버 위협 대응을 수행하도록 한다.

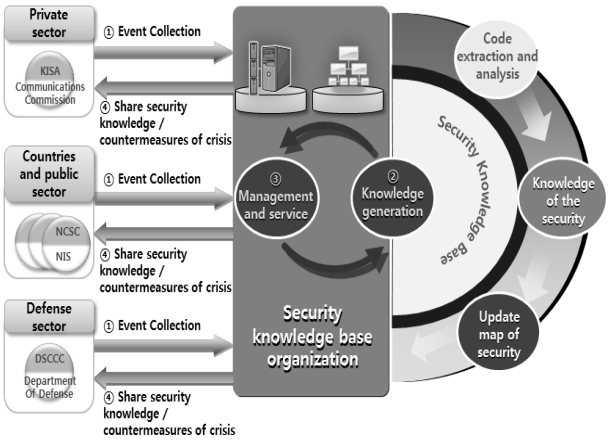

Fig. 6. Scenario 2 for use of national security knowledge base

- 시나리오 3 : 국가적 차원의 축적된 보안 지식베이스를 이용하여 실시간 좀비 현황, 악성코드 전달 경로, 지능화 및 고도화된 사이버 위협 정보, 특정 IP의 과거 이력 정보 등을 실시간으로 조회하는 프로세스

① 국가적인 보안 지식베이스 정보 구축을 통하여 고도화된 사이버 위협과 관련된 신뢰할 수 있는 정보를 받을 수 있게 된다.

② 해당 권한을 가진 사용자는 IP나 도메인과 같은 식별 정보를 이용하여 보안 지식베이스 전담 조직에서 관리하고 있는 사이버 위협 관련 정보를 검색한다.

③ 보안 지식베이스 전담 조직은 요청된 정보를 사용자에게 제공하여 고도화된 사이버 위협에 대응할 수 있도록 한다. 그리고 사이버 위협의 위험도 및 시급성에 따른 위협 대응 프로세스를 수립한다.

- 사이버 위협 정보마다 다수 이해관계자가 존재함에 따라 정보마다 이해관계자별 역할을 구분하고 이해관계자별 필요한 정보를 제공한다.
- 사이버 위협 정보의 위험도, 시급성 등에 따라 위협 대응 체계의 프로세스를 결정하며, 위험도가 큰 경우에 정부 및 산·학·연 전문가로 구성된 심의위원회를 통해 대응 방안을 결정한다.

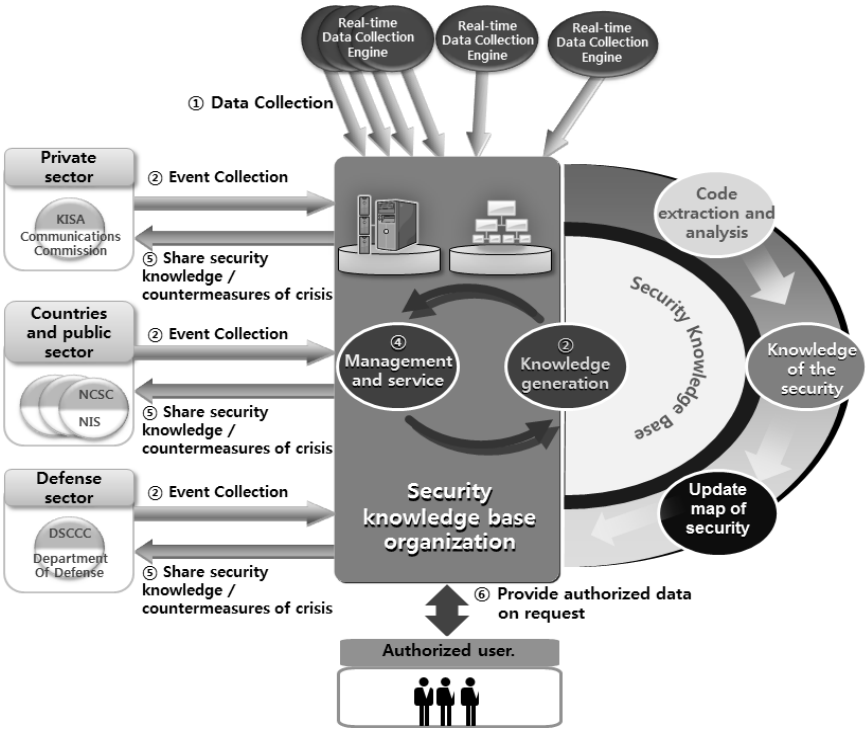

Fig. 7. Scenario 3 for use of national security knowledge base

2) 보안 지식베이스 시스템 운영 및 서비스

국가 차원의 보안 지식베이스 시스템 구축 운영을 위해 다음과 같은 사항이 수행되어야 한다.

- 악성코드 등 위협 관련 이벤트 정보의 실시간 수집, 분석 및 지식베이스화를 자동화할 수 있는 보안 지식베이스 시스템을 구축한다.
- 정부, 산업계, 학계, 연구소 등에서 권한을 가진 사용자가 접근하여 보안 지식베이스 정보를 이용할 수 있는 인터페이스를 개발한다.
- 화이트리스트, 블랙리스트, 악성코드 이동 경로 보안 맵 등 보안 지식베이스를 위한 데이터베이스를 구축한다.
- 수집된 악성코드 등 위협 관련 이벤트 정보를 분석 및 검증하고 관리하기 위한 통합관리 시스템을 구축한다.

그리고 실행코드의 분석을 위하여 악성코드의 블랙리스트 및 실행코드의 화이트리스트 정보를 수집하여 데이터베이스화해야 하며, 사이버 침해 정보 수집을 확대하고 관리해야 한다. 이를 위해 다음과 같은 사항을 추진해야 한다.

- 양질의 풍부한 사이버 위협 정보 수집을 위한 국내·외 수집채널을 확대한다.
- 정부, 산업계, 학계, 연구소 등에서 화이트리스트 실행 코드, 악성코드 및 사이버 침해 관련 정보 수집 채널 및 체계를 확립한다.
- NIST, US-Cert 등 국외 침해사고 대응기관 및 연구기관에서 탐지·분석한 정보 수집 채널 및 체계를 확립한다.
- 모든 사이버 위협 관련 정보를 보안 지식베이스 전담 조직으로 수집하고, 수집된 정보는 분석, 검증, 지식 보호화 과정을 거쳐 실시간으로 보안 지식베이스를 갱신하고, 관계기관과의 연계 체제를 통한 보안 관련 데이터베이스를 확대하여 민, 관, 군 등에서 위기 대응을 위하여 활용될 수 있도록 한다.

또한, 실시간 트래픽 검사를 통해 갱신된 입체적인 보안 지식베이스를 활용하여 국가 차원의 실시간 위협 관리를 수행하고 신규 위협 탐지를 분석하며, 그 사항을 검증해야 한다. 이를 위해 다음과 같은 사항을 추진한다.

- 알려지지 않은 신규 위협 탐지 및 분석과 취약점이 존재하는 실행코드의 실시간 분포 정도, 실시간 좀비 현황 정도 등의 입체적인 정보를 활용할 수 있으며, 관련 정보를 관계기관과 공유하여 위협에 대응·조치하도록 유도한다.

3) 보안 지식베이스 업무 전담조직 신설

국가 차원에서 실시간 데이터 수집 및 관계기관을 통한 사이버 침해 정보를 수집·분석 및 지식베이스화하고 이를 기반으로 국가적인 위기 대응 업무를 수행하기 위하여 국가 보안 지식베이스 전담 조직 신설이 필요하게 된다. 이 전담 조직에서는 다음과 같은 업무를 수행하게 된다.

- 실시간 사이버 위협 분석을 통한 유사 침해사고 재발 방지 및 신규 사이버 위협 정보를 탐지·분석하여 사전 예방 능력을 강화한다.
- 국내·외 관계기관 간의 사이버 위협 정보 협력을 통한 신속한 위기 대응 업무를 추진 및 수행한다.

국가 보안 지식베이스 전담 조직은 다음과 같은 팀으로 구성될 수 있다.

- 실시간 데이터 수집 및 분석팀 : 실시간 데이터 수집 등 위협 정보를 수집 및 분석한다.

- 보안 지식베이스 통합관리팀 : 보안 지식베이스 갱신, 유지 관리 및 서비스 제공 등 보안 지식베이스 시스템 운영
- 국내·외 총괄협력팀 : 국내·외 관계기관 및 산·학·연 등 타 기관과의 협력체계 구축 및 위기 대응 업무 수행

국가 보안 지식베이스 전담조직에서는 정부 부처별로 산재하여 수집되고 공유되는 사이버 위협 정보의 신속한 통합 수집을 위하여 유기적인 공조체계를 구축하고, 수집된 정보의 분석·검증 및 지식베이스화를 통하여 통합 관리를 수행할 수 있는 프레임워크를 구축하도록 한다.

4) 위협 대응 체계 구축 및 인력양성

국가·공공, 민간, 국방 분야, 정보보호 기관 및 산업체, 학계, 연구소 등과 유기적인 공조 채널을 구축하여 사이버 위협 관련 이벤트 데이터를 수집하고 국가 보안 지식베이스를 갱신하여, 이를 기반으로 국가 차원의 실시간 사이버 위협 대응 체계를 완성한다. 이를 위하여 다음과 같은 사항을 수행한다.

- 사이버 위협 정보 수집 및 공조채널을 다변화하여 침해사고와 연계된 위협정보를 보안 지식베이스화하여 신속 정확하게 입체적으로 관리한다.
- 사이버 위협 대응 관련 정책을 제정 및 활성화하여 국가 위기관리 체계를 강화하고 공조체계를 활성화한다.
- 해외 관계기관 및 산업계와의 협력 채널을 확보하고 공조체계를 구성하여 국가 위기 상황에 대한 실시간 사이버 위협 대응 프로세스 구축

그리고 사이버 위협 대응 정책, 기술, 표준화 연구를 위한 산업계, 학계, 연구소, 정부기관, 군 등으로 구성된 협의체를 구성 및 운영한다. 이 협의체를 통하여 국가 사이버 위협 대응을 위한 보안 지식베이스 전담 조직의 중요 정보 및 사이버 위협의 위험도에 따른 대응 방안 및 연계된 종합 대책을 함께 협의할 기회를 제공한다.

또한, 고도화된 사이버 위협에 대처하고 보안 지식베이스 전담 조직을 운영하기 위하여 보안 지식을 갖춘 고급 인력을 양성해야 한다. 산업계, 학계, 정부기관, 군의 보안 교육을 위한 활동을 지원하고 모의 해킹 등 실무를 통하여 위협에 대응 능력을 갖춘 실무 인력을 양성하고 사이버 위협 데이터 탐지 분석 및 보안 지식화 등 특화된 연구 활동 지원을 통하여 고급 인력을 양성한다. 또한, 화이트 해커의 양성화 활동 및 양성을 위하여 다음과 같은 내용을 수행한다.

- 해킹방어대회, 사이버 공격 시나리오 공모전과 같은 활동을 통하여 국내 화이트 해커의 양성화 활동을 활성화하고, 학계 및 민간 부분 연구 지원을 통하여 화이트 해커의 연구 참여를 지원한다.
- 화이트 해커들과의 교류를 활성화하고, 화이트 해커들과의 연합 모임을 구성하여 다양한 보안 정보 수집 및 전문가로서 활동할 기회를 제공한다.

5) 법제도 개선

사이버 위협 대응을 위한 보안 지식베이스 전담 조직 신설을 위하여 법 제정이 필요하며, 이를 위하여 다음과 같은 내용을 수행한다.

- 보안 지식베이스 전담 조직 신설을 위한 법률 제정 및 침해사고 위기 대응 체계 통합 구축·운영을 위한 법률을 개정한다.
- 신설 조직의 법률적 근거를 위해 조직의 구성 및 운영에 관련된 '국가 보안 지식베이스 센터 규정' (가칭) 또는 법률을 제정한다.

그리고 국가 차원의 실시간 데이터 수집 체계와 사이버 위협 대응 체계 구축을 위한 제도마련 및 법률 제·개정을 위하여 다음 내용을 수행한다.

- 고도화된 사이버 위협에 대응하기 위하여 실시간 데이터 수집과 관련된 정책을 마련한다.
- 공조 체계에 있는 관계기관에서 사이버 위협 관련 정보 확보 시 즉각적인 신고 의무화 정책을 마련한다.
- 국가 차원의 사이버 위협 대응 프로세스 이행 의무화 및 이해관계자별 역할을 규정한다.
- 사이버 안전 관리 규정 및 정보통신기반 보호법 등 위기 대응 관련 기존 법제 통합을 개정한다.

또한, 사이버 위협 대응 방안을 위한 인식제고 프로그램을 수행하여 사이버 위협에 대한 인식을 높이고 이를 기반으로 사이버 위협 관련 데이터의 수집과 위기 대응 조치를 수행하도록 한다. 이를 위해 다음 사항을 수행한다.

- 사이버 위협 대상별, 수준별 대응 방안에 대한 교육·훈련을 추진한다.
- 위협 대응 체계 구축을 통한 사이버 위협 대응 및 예방 사례에 대한 교육 및 대국민 홍보 활동을 수행한다.
- 국민을 대상으로 사고정보 및 위협정보의 등록을 유도한다.

5.3 추진 방안

앞에서 설명한 추진 체계를 실행하기 위한 추진 방안은 다음과 같다.

1) 국가보안 지식베이스 구축 프로세스 수립방안

범부처 및 산업체, 학계, 연구소 전문가들로 구성된 전담반을 구성하여 국가 보안 지식베이스 구축 프로세스를 수립한다. 구축 프로세스 내용은 다음과 같다.

- 산·학·연·민·관·군 등 범부처를 포괄하는 국가 보안 지식베이스 구축 프로세스 수립
- 실시간 데이터 수집을 위한 데이터 수집 프로세스 개발
- 타 기관에서 수집된 정보의 검증을 위한 검증 프로세스 개발
- 화이트리스트 및 블랙리스트 수집과 리스트 데이터베이스 갱신 프로세스 개발
- 실시간 실행코드 분석을 위한 빅 데이터 분석 프로세스 개발
- 실시간 보안 지식베이스 갱신 프로세스 개발

2) 사이버 위협 대응 협의체 및 국가 보안 지식베이스 시스템 구축

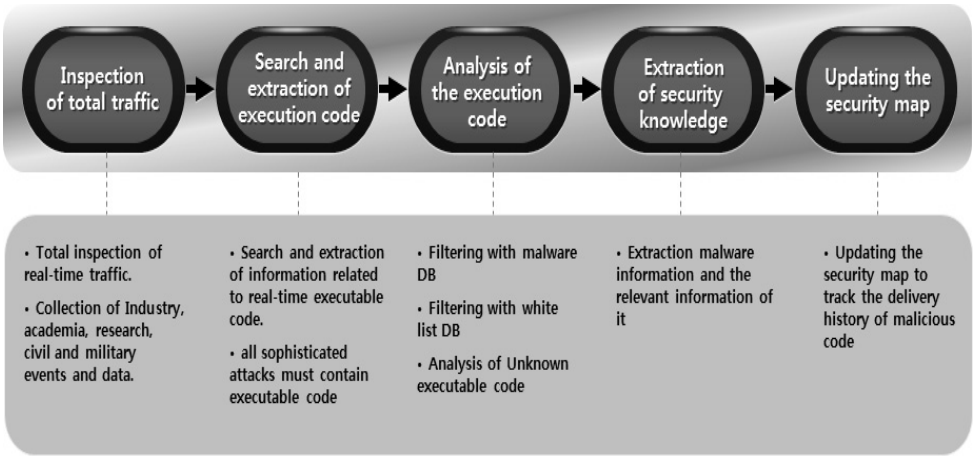

Fig. 8. Process for generation of national security knowledge base

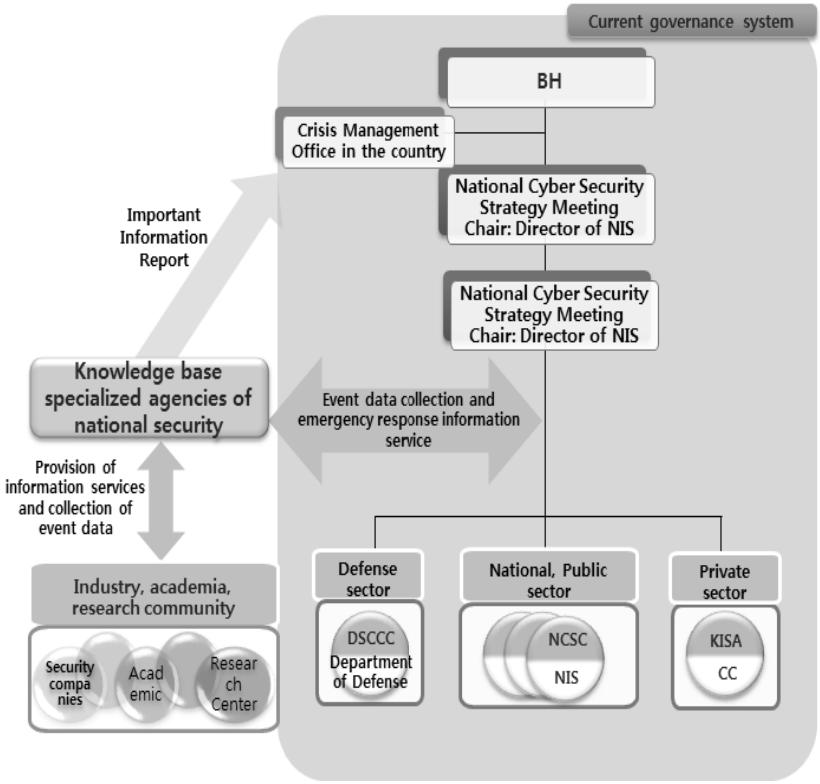

Fig. 9. An example of agency for national security knowledge base

국가 보안 지식베이스 구축 및 사이버 위협 대응 정책, 기술, 표준화 연구를 위한 산업계, 학계, 연구소, 정부기관, 군 등으로 구성된 협의체를 구성 및 운영한다. 그리고 국가 차원의 대규모 데이터의 실시간 수집, 수집된 빅 데이터의 실시간 분석, 분석된 정보의 지식베이스화, 보안 지식의 활용방법 등 고도화된 사이버 위협에 대응하기 위한 신기술 연구를 추진한다. 또한, 고도화된 사이버 위협에 대응하기 위한 국가 차원의 사이버 위협 정보를 실시간으로 수집, 분석, 지식베이스화하는 독립적인 국가 보안 지식베이스 시스템을 구축하고, 구축된 보안 지식을 사용하여 사이버 위협 정보의 위험도, 시급한 정도 등에 따라 위협 대응을 수행하는 사이버 위협 대응 체계를 수립한다.

APT와 같이 고도화된 사이버 공격에 대응하기 위한 지식베이스를 구축하기 위해서 먼저 실시간 데이터 패킷의 전수 검사를 통하여 필요한 이벤트들을 수집할 수 있어야 하며, 수집된 정보를 사용하여 실행코드 관련 정보 검색 및 실행코드 추출이 필요하며, 실행코드를 악성코드 데이터베이스와 화이트리스트 데이터베이스와의 비교 분석을 통하여 알려진 악성코드는 추적을 수행하고, 알려지지 않은 실행코드는 연관성 분석을 통하여 악성코드 분석을 수행하고, 악

성코드일 경우 지식베이스화하여 실행코드 전달 이력 추적을 위한 보안 맵을 갱신한다. 다음 Fig. 8은 국가 보안 지식베이스 생성 과정을 나타낸다. 이 과정을 통하여 생성된 실행코드 전달 이력 보안 맵은 고도화된 공격에 대하여 대응 전략 수립 및 조기 공격 대응 방안 확립이 가능하게 된다. 또한, 국가보안 지식베이스를 사용하여 다음과 같은 서비스가 가능하리라 기대된다.

- Inbound/Outbound 트래픽 상세 모니터링 분석 체계 확보
- 고급화된 또는 숨겨진 위협 탐지/대응 방안 제시
- 위협이 되는 사이트 접근 행위 탐지 및 통제
- 공격의 Life cycle을 제공
- 악성코드 유입 경로 분석
- 감염된 시스템 트래픽 분석

3) 국가보안 지식베이스 전담조직 운영 방안

고도화된 사이버 위협으로 인한 위기 상황이 발생하는 경우에 신속하게 국가적인 차원에서 대응하기 위하여 일관성 있는 정책 수립 및 운영이 필요하며 이를 위해 정부 주도의 독립적인 전담 조직으로 운영하고 기존의 위기관리체제와 연계하여 수행한다. 국가보안 지식베이스 전담조직은 다음과 같이 세 개의 팀으로 구성하여 운영한다.

- 실시간 데이터 수집 및 분석팀 : 실시간 데이터 수집 등 위협 정보를 수집 및 분석한다.
- 보안 지식베이스 통합관리팀 : 보안 지식베이스 갱신, 유지 관리 및 서비스 제공 등 보안 지식베이스 시스템을 운영한다.
- 국내·외 총괄협력팀 : 국내·외 관계기관 및 산·학·연 등 타 기관과의 협력체계 구축 및 위기 대응 업무를 수행한다.

국가보안 지식베이스 전담조직은 현재의 국가 위기 대응 체제와 유기적으로 연관된 독립적인 조직으로 구성되며, 산·학·연 단체와 민·관·군 사이버 위협 대응 체제와 연계하여 정책 및 종합대책을 수립하여 운영한다. 국가보안 지식베이스 전담조직의 운영 예는 다음 Fig. 9와 같다.

우선 실행코드 전달 이력 보안 맵을 작성하기 위해서는 실행코드 실시간 추적기술과 분석기술이 필요하다. 또한, 기존에 알려진 악성코드와 관련된 데이터베이스가 필요하며, 이것을 실시간으로 검색할 수 있는 기술이 필요하다. APT 등과 같이 고도화된 공격도 실제 공격 진행 과정 중에 반드시 네트워크를 통한 실행코드 전달이 포함되어 있으며, 실행코드 전달시 이미 구축된 국가 보안 지식베이스인 실행코드 전달 이력 보안 맵을 이용하여 실시간 추적 및 분석이 가능하게 된다. 그리고 민간과 국가·공공 기관 및 군을 포함한 국가 차원의 체계적인 이벤트 수집 및 보안 지식베이스의 구축 및 관리, 서비스를 제공하기 위하여 일원화된 조직이 구축되어야 한다.

6. 결 론

본 논문에서는 인터넷을 통한 물리 및 논리공간의 융합과 스마트 디바이스에 의한 이동성이 극대화되는 환경변화 상황에서의 APT 사이버 위협 및 공격단계를 분석하였다. 또한, 국내·외 사이버 공격 대응 기술 현황 및 사이버 공격 대응 체계 현황을 조사 분석하였다. 그리고 이를 기반으로 새로운 유형의 고도화된 사이버 위협에 능동적으로 대응하기 위한 기반으로써 국가 보안 지식베이스 구축 전략을 수립하였다. 본 논문의 결과를 활용하여 APT 등 고도화된 사이버 위협에 국가 차원의 효과적인 위기 대응이 가능하리라 사료된다.

참 고 문 헌

[1] http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=16854

[2] http://yjlee.delighit.net/i/entry/75

[3] http://blog.daum.net/saschajin/12603

[4] Nam Ki-Hyo, Kim Youn-Hong, Kwon Hwan-Woo, “Trends in information protection latest technology: APT and its corresponding”, Information and communication industry Agency, 2011. 9.

[5] http://www.isssource.com/wp-content/uploads/2012/04/040412C5_APT_ADecadeInReview.pdf

[6] http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?curPage=1&menu_dist=2&seq=18487&dir_group_dist=0

[7] http://docs.media.bitpipe.com/io_10x/io_105022/item_550605/Lifecycle_of_the_Advanced_Persistent_Threat%5B1%5D.pdf

[8] http://www.Websense.com/assets/white-papers/whitepa per-Websense-advanced-persistent-threats-and-other-advanced-attacks-en.pdf

[9] http://www.trendmicro.com/us/enterprise/challenges/ad vance-targeted-attacks/index.html#understand-an-attack

[10] http://www.trendmicro.com/cloud-content/us/pdfs/busi ness/datasheets/ds_deep-discovery.pdf

[11] Kim Hyung-Wook, “0-Day Attack Protection for IBM's multi-tier pre-emptive countermeasures”, IBM Security Summit, 2011.

[12] http://www.it-win.co.kr/EMC_RSA_NetWitness.pdf

[13] http://www.zdnet.co.kr/news/news_view.asp?artice_id=20120918220326&type=det

[14] http://image.itstv.net/upload_files/infocenter/file32599 -137302.pdf

[15] http://www.eurosouthkorea-ict.org/documents/forum2_ppt/mijoo_kim.pdf

[16] “Corresponds to the current state of the 2010 virus hacking”, KISA Final Research Report, KISA-RP-2010-0051

[17] http://epc.neograph.co.kr/kor/info/kor_info_dic_list.ht tml?sval=&mode=h8&page=3#

[18] http://blog.daum.net/damulkan/7563870

[19] http://blog.hitoos.com/radiohankook/44961

[20] Lee Chang-bum, Kang Lee-Seock, “Internet Law Trends No. 22”, KISA, Trends in Internet legislation 2009-07.

[21] http://netsquare.kisa.or.kr/report/securityTrend/[June 3 weeks] “United States, for cyber security 'Plan X' strategy promotion” 2012-06-21.
[22] Kim Il-Soo, Kang Seock-Gu, Yoon Hee-Sang And five others, “Study on the Construction of cyber security system”, Korea Criminal Policy Research Institute, 2010.

이 태 영
e-mail : nednottokow00@nate.com
2012년 순천향대학교 정보통신공학과(학사)
2010년～현 재 순천향대학교 정보통신공학과 석사과정
관심분야 : 네트워크 보안, 시스템 보안

박 동 규
e-mail : dgpark@sch.ac.kr
1992년 한양대학교 전자공학과(공학박사)
1992년～현 재 순천향대학교 정보통신공학과 교수
관심분야 : 네트워크 보안, 유비쿼터스 컴퓨팅 보안