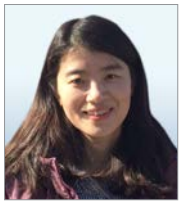
과학기술계 사이버위기대응의 최전선에서

과학기술계 정보보안 컨트롤타워 'S&T-SEC'

글_송보연
한국과학기술정보연구원
과학기술사이버안전센터 선임연구원
bysong@kisti.re.kr



글쓴이는 한국항공대학교 통신정보공학과 졸업 후 한국과학기술원에서 석사학위를, 로열 할로웨이 런던대학교에서 박사학위를 받았다. 몽골국제대학교 조교수, 고려대학교 연구교수, 국가수리과학연구소 연구원 등을 지냈다.

최근 '세월호 침몰' 참사와 같은 국가적 차원의 재난·위기상황 발생시 종합적이고 체계적인 대응방안을 마련해야 한다는 국민적 염원이 연일 언론매체를 통해 표출되고 있다. 일반적으로 '재난'이라함은 날씨 등의 자연현상 변화, 또는 인위적인 사고로 인한 인명이나 재산의 피해를 말한다. 특히, 이러한 재난은 천재지변에 의한 '재해'와 사람의 실수 또는 부주의나 고의로 일어난 '인재'로 구분할 수 있다. 특히, '인재'에 의한 재난이나 위기상황이 자주 발생되는 분야는 사이버위기 분야라 할 수 있을 것이다. 정보화 사회의 도래로 거의 모든 기반시설이 정보통신망에 연결되어 있으며 이에 따른 편리한 생활을 영유하게 되었지만, 악의적 또는 실수에 의한 위기상황이 빈번하게 발생하고 있다.

이러한 사이버위기상황 발생을 미연에 방지하고, 상황발생 시 신속·정확하게 대응하기 위해 한국과학기술정보연구원이 지난 2005년부터 구축·운영하고 있는 과학기술사이버안전센터(S&T-SEC, Science and Technology Security Center)에 대해 중점적으로 조명하고자 한다.

사이버 테러 대응 위한 사이버 안전센터 설립

우리나라 사이버 보안에 경각심을 불러일으켜준 획기적인 사건 중의 하나가 2003년 대한민국 인터넷망을 마비시켰던 1·25 인터넷 대란이다. 2003년 1월 25일 세계적으로 7만5천여 개의 시스템이 슬래머 웜에 감염되어 인터넷 접속이 불가능하게 되었던 보안 사건이다. 슬래머 웜은 마이크로소프트 SQL 서버의 버퍼와 관련된 버그를 이용하여 시스템을 감염시키는 서비

스 거부 공격(DoS)의 일종이다. 특히, 국내에서는 세계 감염대수의 11.8%에 해당하는 8천 800여 대의 PC가 슬래머 웜에 감염되어 인터넷 망이 몇 시간 동안 마비되는 국가적 대혼란을 야기했었다. 이 사건을 계기로 사이버 보안에 대한 종합적이고 체계적인 대응의 필요성이 제기되어 국가 차원의 사이버 보안을 총괄하기 위해 국가사이버안전센터(NCSC)가 2004년 2월 설립되었다.

그 이후, 2004년 4월에 공공기관, 출연(연)의 PC 50여 대 및 민간 PC 278대가 중국 산 해킹 공격인 백도어 Peep에 감염되어 정보가 유출된 사건이 있었다. 심지어 해킹 공격 발생 후 50여 일간 피해 사실조차 파악하지 못하고 있었다. 이에, 정부는 (구)과학기술부를 중심으로 과학기술 분야 정보보안 실태를 점검하고, 사이버 침해위협으로부터 국가 과학기술분야의 핵심 연구정보자원을 보호하는 과학기술분야의 사이버위기대응체계를 확립하고자 과학기술사이버안전센터(S&T-SEC)를 2005년 3월 개소하였다.

출연연 · 공공기관 사이버 위기에 대응하는 'S&T-SEC'

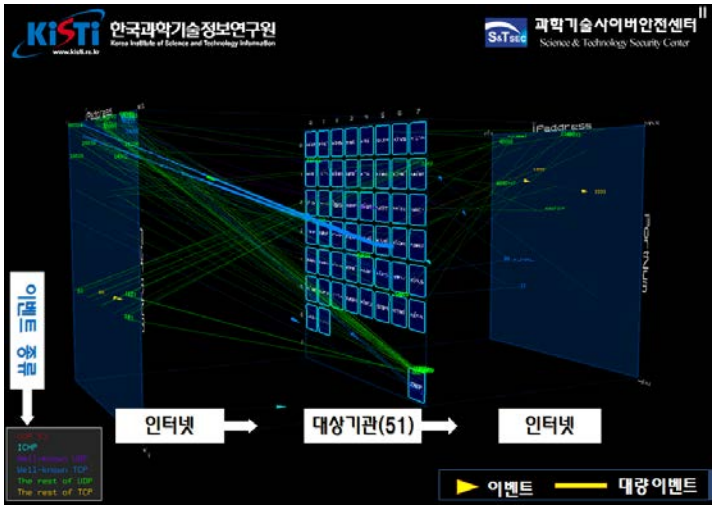
우리나라의 사이버위기대응체계는 국가보안관제센터인 NCSC를 중심으로 행정, 국방, 금융, 과학기술, 교육 등 주요 분야별 부문보안관제센터를 구축하고, 각급기관은 사이버위기상황에 대한 자체대응이 가능하도록 단위보안관제센터를 운영하도록 하고 있다. S&T-SEC은 과학기술 분야 사이버위기대응을 위한 '정보보안 컨트롤타워' 역할을 수행하는 국가 지정 부문보안관제센터로서, 우리나라 과학기술계 출연(연) 및 공공기관에 대한 사이버 침해위협을 실시간으로 탐지·분석하고 신속·정확한 대응활동 수행을 기반으로 사이버위기상황 사전예방 및 피해발생 최소화를 위해 불철주야 최선의 노력을 기울이고 있다.

S&T-SEC의 기본 임무는 과학기술계 51개 출연(연) 및 공공기관에 대한 실시간 보안관제를 수행하는 것이다. '보안관제'란 정보보안시스템(침입탐지시스템, 침입방지시스템, 방화벽 등)을 통해 수집되는 로그를 분석하고 실제 해킹 공격이 발생할 경우 이에 대한 분석 및 대응조치를 수행하는 일을 말한다.

S&T-SEC의 보안관제 활동은 4단계로 이루어진다. 보안관제시스템을 통해 침해시도를 실시간으로 모니터링하는 단계, 대상기관에 피해를 발생시킬 것으로 판단되는 침해시도 이벤트를 탐지하고 분석하는 단계, 침해공격으로 판단된 경우 대상기관에 탐지내용을 통보하고 대응할 수 있도록 조치하는 단계, 그리고 대상기관 담당자가 보안 이벤트에 대응한 결과를 확인하는 단계로 구분된다.

S&T-SEC에서는 '종합상황실'을 중심으로 24시간 365일 상시 보안관제 체제를 구축하여 운영하고 있으며, 2014년 현재 S&T-SEC이 보안관제 대상기관으로부터 일일 평균 약 2천만 건 이상의 보안이벤트가 발생되고 있는 것으로 분석되고 있다 또한, S&T-SEC에서는 사이버위기상황 발생에 대한 대응활동 이외에도 사전에 위기상황 발생을 방지하기 위한 예방활동도 적극적으로 수행하고 있다. 대상기관에 구축·운영 중인 정보시스템에 잔존하는 근원적 취약요소를 사전에 점검·분석하여 개선토록 권고하고 있으며, 각급기관 구성원이 위기상황 발생에 따른 대응요령을 상시 체득할 수 있도록 지원하기 위한 상시 사이버전 모의훈련 등을 중점적으로 지원하고 있다.

지능화·첨예화하는 사이버위기상황을 보다 정확하고 효율적으로 탐지하고 대응하기 위해



▸▸ 1. 보안이벤트 가시화 : K-Cube

서는 관련 기술에 대한 끊임없는 연구·개발이 필수적이다. 이에, S&T-SEC에서는 지속적으로 증가하는 대용량 보안이벤트에 대한 신속·정확한 탐지 및 분석을 가능하게 하기 위해 '실시간 보안이벤트 가시화 기술'과 신·변종 해킹공격에 대한 사전예측 및 선제적 대응을 위한 '사이버 예·경보 기술'을 중점적으로 연구하고 있다.

실시간 보안이벤트 가시화 시스템 'K-Cube'

기존의 보안관제는 보안이벤트 모니터링 및 분석을 위해 텍스트 기반 인터페이스를 활용하였다. 즉, 보안이벤트의 상세 정보가 문자열로 표시된다. 매초 쏟아지는 방대한 보안이벤트가 인터페이스 화면 안에 모두 나열되기도 어렵거니와 관제요원이 모든 이벤트를 놓치지 않고 다 확인하기도 어려운 것이 현실정이다. 이러한 기존 보안관제의 한계를 극복하기 위해, S&T-SEC에서는 실시간 보안이벤트 가시화 시스템인 'K-Cube'를 개발하여 구축·운영하고 있다.

대규모 데이터를 효과적으로 관찰하거나 이해하려고 데이터를 시각화하는 것은 널리 사용되는 방법이다. 데이터의 단순한 나열보다 사진 한 장이 직관적·효과적으로 더 많은 정보를 전달할 수 있기 때문이다. 데이터 가시화란 데이터의 속성을 그래프라는 수단을 통해 공간에 배치해 보여줌으로써 그 패턴을 쉽게 인지할 수 있도록 시각적으로 표현하고 전달하는 과정을 말한다.

'K-Cube'에서는 보안관제시스템을 통해 탐지되는 보안이벤트를 3차원으로 가시화하였다. 〈그림 1〉과 같이 'K-Cube'를 통해서 보안관제 대상기관 내부로 들어오는 보안 이벤트와 외부로 나가는 보안 이벤트의 흐름을 한눈에 확인할 수 있다.

'K-Cube'의 구조는 2개의 육면체(Cube)가 인접하여 붙어 있는 형태이다. 세 개의 평면으로 구성이 되어 있고 왼편의 평면은 이벤트의 근원지가 되는 인터넷 구간, 가운데 평면은 대상기관의 네트워크 구간, 그리고 오른편에 위치한 평면은 이벤트의 목적지가 되는 인터넷 구간으로 분리된다. 가운데 평면은 보안관제 대상기관을 표시하는 셀로 구분되어 각 셀 안에는 해당 대상기관을 나타내는 약어가 투명하게 표시되어 있다. 그리고 보안관제시스템을 통해 탐지되는 보안이벤트는 평면과 평면 사이를 이동하는 화살표로 표시된다. 이벤트 중 일정 시간에 대량으로 발생하는 경우에는 화살표 대신 실선으로 표시하여 대량 발생 공격도 직관적으로 확인할 수 있다.

S&T-SEC의 종합상황실에서는 'K-Cube'를 통해 실시간으로 어떤 대상기관이 공격을 많이 받고 있으며, 어떤 대상기관의 시스템이 외부로 공격을 시도하고 있는지 총체적으로 파악이 가능하다. 또한, 기존에 발생하지 않았던 해킹 공격에 대한 이상 징후도 효율적으로 관측·분석할 수 있는 이점이 있다.

신 · 변종 해킹 수집 및 조기 대응 '사이버 예 · 경보 시스템'

기존의 보안관제는 해킹사고 발생사례를 토대로 하여 만든 정형화된 규칙을 기반으로 보안관제시스템을 구축·운영함에 따라 알려진 해킹공격에 대에서만 탐지 및 대응이 가능하다는 단점을 갖는다. 그러나, 최근 지속적으로 언론에 공개되는 대부분의 사이버위기상황들(2013년 6·25대란, 언론사·금융사 해킹사고 등)은 알려지지 않은 새로운 공격기술을 사용하여 발생되고 있다. 즉, 아무리 24시간 365일 철통 보안관제를 수행한다고 해도 해커가 새로운 기술을 이용하여 공격을 수행한다면 기존의 보안관제시스템으로는 탐지조차 불가능한 것이 현실이다.

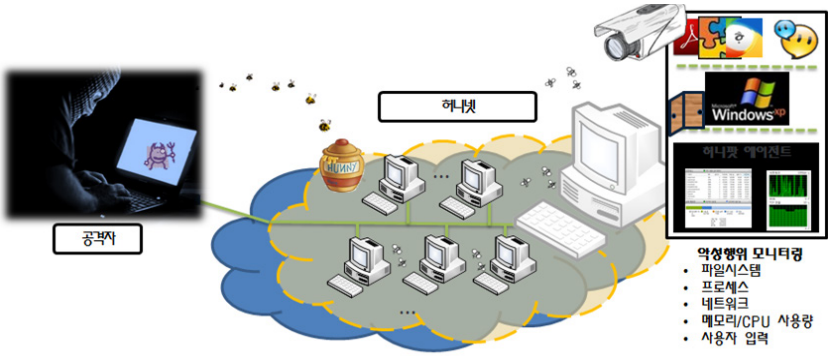
이러한 고민에 기초하여, S&T-SEC에서는 신·변종 해킹공격 수집 및 조기대응을 위한 '사이버 예·경보 시스템'을 개발하고 있다. '사이버 예·경보 시스템'은 허니넷(Honeynet)의 확장된 형태라고 볼 수 있다. 허니넷이란 허니팟(Honeypot)의 네트워크를 말하고, 허니팟은 꿀단지, 즉 글자 뜻이 의미하는 대로 공격자를 유인할 수 있는 취약점을 가진 시스템이다.

〈그림 2〉와 같이 S&T SEC의 '사이버 예·경보 시스템'은 실제로 운영하는 것처럼 보이는 보안상 취약점을 가진 PC 및 서버, 그리고 모바일 기기를 가상으로 구축하여 해커들이 접근할 수 있게 하고, 시스템 상에 남겨진 해커들의 자취를 수집하여 분석할 수 있도록 구축한 시스템이다. 이를 통해 해커들이 현재 실제로 사용하고 있는 신·변종 해킹공격 기술에 대한 사전 예측 및 선제적 대응이 가능하게 될 것이다.

최신 사이버위기 대응 기술 연구 확대

영화 '다이하드 3.0'에서 악당들이 해커들을 동원하여 국가기반시설인 교통, 전기 등을 무력하게 만든 것이 단순히 영화적 상상이 아닌 현실에서의 안전문제로 대두되고 있는 실정이다. 또한, 사이버위기는 재난의 범주를 넘어 국가안보와도 직결되는 매우 중차대한 현안사항이 되어가고 있다. 수년간 연구해 온 핵심 과학기술 연구자료들이 개발도상국과 적성국가의 해커부대에 탈취되어 막대한 경제적 손실이 발생되고 있으며 앞으로도 지속적으로 증가할 것으로 예상된다.

이러한 시대적 상황에서 S&T-SEC은 사이버위기상황 최전선에서 과학기술 분야 핵심 연구정보자원을 보호하기 위한 '과학기술계 정보보안 컨트롤타워' 역할을 충실히 수행해 나갈 것이며, 이를 위해 빅데이터 기반의 보안관제·침해대응 기술과 같은 최신 사이버위기대응 관련 기술에 대한 연구 개발도 지속적으로 확대해 나갈 예정이다. ST



▸▸ 2. 사이버 예 · 경보 시스템