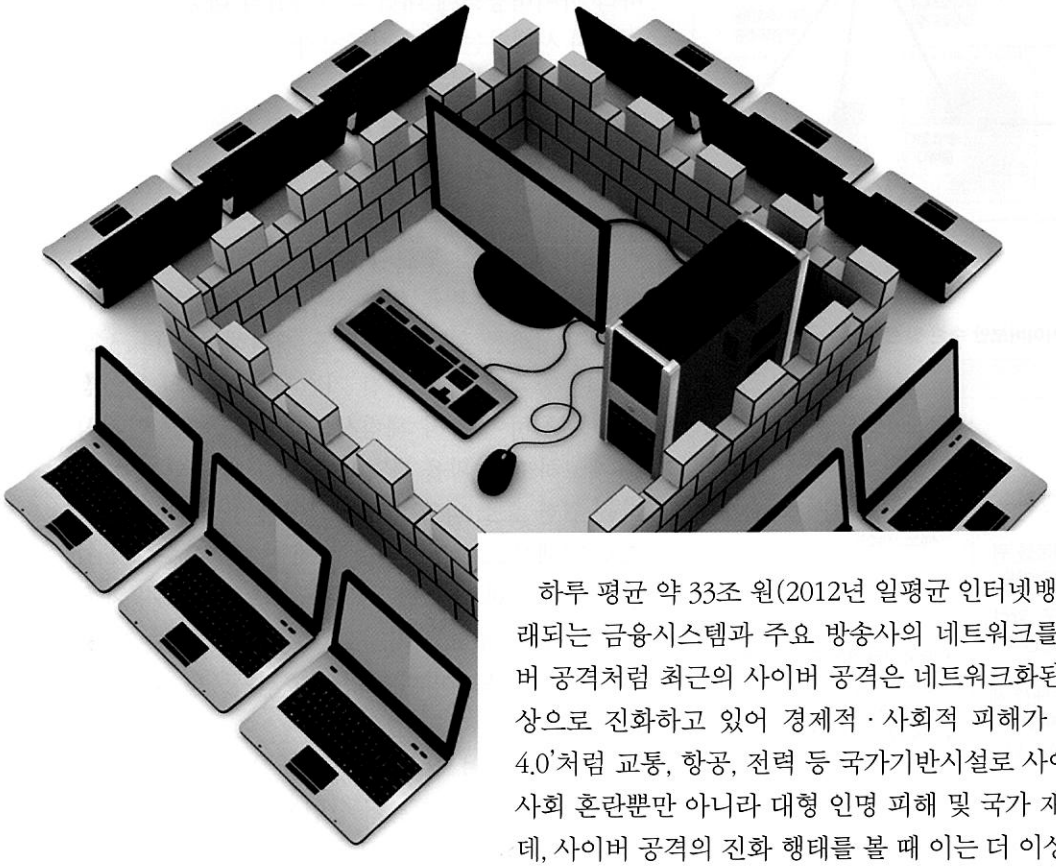
### 사이버 공격대비 국가차원의 대응전략

# 사이버공격 대응하는 총괄 보안 컨트롤타워 필요하다



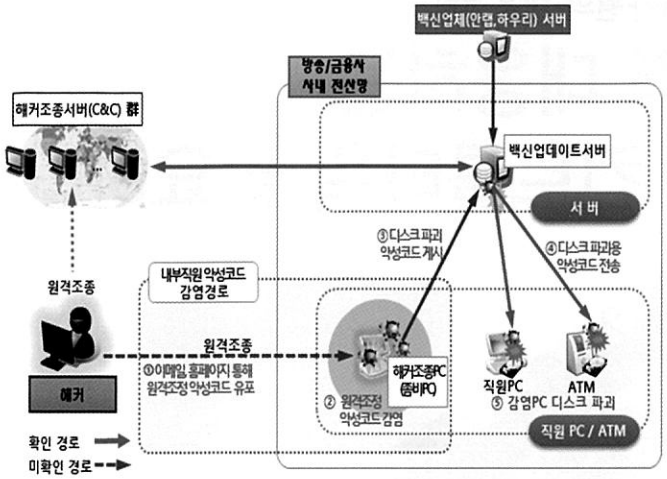
하루 평균 약 33조 원(2012년 일평균 인터넷뱅킹 거래액, 한국은행)이 거래되는 금융시스템과 주요 방송사의 네트워크를 일부 마비시킨 3.20 사이버 공격처럼 최근의 사이버 공격은 네트워크화된 사회기반 시설을 공격 대상으로 진화하고 있어 경제적 · 사회적 피해가 막대하다. 영화 '다이하드 4.0'처럼 교통, 항공, 전력 등 국가기반시설로 사이버 공격이 확대되는 경우 사회 혼란뿐만 아니라 대형 인명 피해 및 국가 재난 사태가 발생할 수 있는데, 사이버 공격의 진화 행태를 볼 때 이는 더 이상 영화 속의 얘기라고 치부할 수만은 없다. 따라서, 최근 발생한 3.20 사이버공격 분석을 통해 국가차원의 사이버공격에 대한 대응전략을 마련할 필요가 있다.

글_원유재
한국인터넷진흥원
경영기획실장
yjwon@kisa.or.kr

글쓴이는 충남대학교 전산학과에서 박사학위를 받았으며, 한국전자통신연구원, 안철수연구소 등에서 근무했다. 한국인터넷진흥원 인터넷침해사고대응센터장을 역임하였다.

## 3.20 사이버공격의 시사점

지난 3.20 사이버공격은 악성의도를 가진 공격자 즉, 해커가 한국을 포함한 미국, 호주, 브라질 등 여러 국가를 경유하여 방송 및 금융기관의 취약한 서버나 직원 PC를 통해 백신업데이트 서버에 악성코드를 설치한 후 내부 PC로 유포하여 3월 20일 14시 이후에 PC와 서버 하드디스크 데이터를 동시다발적으로 파괴되도록 한 '지능형 지속 공격(APT)'이다. 사고발생 후 미래창조과학부, 한국인터넷진흥원 등으로 구성된 민 · 관 · 군 합동대응팀은 손상된 시스템 대다수를 복구하였으며, 사후 조치로 76개 민간 기반시설을 24시간 모니터링하고 긴급 보안점검을 수행하였다.




▸▸ 3.20 사이버공격 수행 절차

**3.20 사이버공격으로 바라본 국내 사이버보안 수준 및 문제점**

| 구분 | 문제점 | 대응전략 |
|---|---|---|
| 제도 및 체계 | • 사고발생 • 대응에 대한 보고 • 홍보체계 미흡 • 대응기관 간 자료공유, 협조 등 공조 부족 • 사고 예방 및 신속 대응을 위한 사이버 보안 법제도 미흡 | • 사이버 공격 대응체계(보고, 대국민 홍보 등) 개선 • 사이버 보안강화를 위한 법제도 개선 |
| 전문인력 및 기술 | • 사고 현장조사 및 복구, 악성코드 분석을 위한 전문인력 부족(2) • 최신 APT 공격 등에 대한 해킹기법 탐지 기술 부재(3) • 백신 등 보안제품의 신 · 변종 악성코드 탐지 • 치료 성능 낮음 | • 한국인터넷진흥원 등 대응기관 역량 강화 • 민간 대응능력 강화 • 보안 전문인력 양성 강화 • 사이버 보안 분야의 R&D 강화 |
| 보안의식 및 보안제품 (서비스) | • 방송 · 금융 등 민간기업 및 국민의 사이버 보안의식 수준 미약 ※IT예산대비 5% 이상 정보보호투자기업 3.1% • 사고발생 기관 담당자의 낮은 보안수준 | • 사이버 보안의식 제고 • 국내 IT보안 시장 활성화 및 신규 물리 • 융합보안 시장 창출 • 사이버 보안산업을 해외 진출 주력사업으로 육성 |

금번 사고로 사고발생 대응에 대한 보고 및 대국민 홍보체계를 포함하여, 사이버공격에 대한 대응체계 및 제도 미흡, 전문인력 부족, 낮은 기술수준, 보안의식 수준 미약 등 국내 사이버보안 전략에 대한 총체적인 문제점이 드러났다고 할 수 있다. 이에 따라 사이버공격에 대한 국가차원의 대응전략을 수립하여 시행하는 것이 시급하다.

### 국가차원의 사이버 공격 대응 전략

국가차원의 사이버공격 대응전략은 제도 및 체계, 전문인력 및 기술, 보안제품 및 보안의식 등을 높이기 위한 체계적인 추진이 필요해 보인다. 먼저, 관련 제도 및 체계 정비를 위해 사이버 보안강화 및 보안산업 활성화를 위한 법제도를 개선해야 한다. 3.20 사이버 공격에 따른 민간 기반시설 대상의 보안점검을 실시하여 유사 해킹시도에 대한 시설 안전성을 제고하고, 현황을 파악하여 관련 제도 및 체계 정비를 위한 요소 파악이 선행되어야 한다. 이를 기반으로 침해사고 발생시 신속하게 신고 · 접수하여 원인분석을 통한 정보공유를 할 수 있도록 대응체계를 강화하고, 주요 국가시설 지정을 확대하는 등 관련 규정(정보통신망법, 기반보호법 등)을 제 · 개정하는 것이 필요하다.

또한 전문인력 양성, 기술개발, 불합리한 산업규제 개선, 클라우드 컴퓨팅 산업지원 등 산업 활성화를 위한 사이버 보안산업 진흥법, 클라우드컴퓨팅 발전법 등과 같은 법제를 제 · 개정하는 것도 필요하다. 그리고, 사이버공격에 대한 조기 대응 및 피해확산 방지를 위해 범국가 차원의 사이버 침해정보 공유체계를 구축하여 실시간 침해사고 정보를 공유하고 협력하는 것이 필요하다.

다음은 보안 전문인력 및 기술 강화 및 개선을 위해 한국인터넷진흥원 등 대응기관 역량과 보안 전문인력 양성 등을 강화해야 한다. 민간 인터넷침해사고 대응을 담당하고 있는 한국인터넷진흥원의 사이버 대응역량 강화를 위해 사이버대응 전담시설 확충 · 고도화 및 전문인력을 확보하는 것이 필요하다. 또한, 침해사고 발생시 원활한 초기 대응 및 증거인멸 방지를 위한 자료제출 요구 및 현장을 조사할 수 있는 법적 근거를 마련하여, 긴급 조치사항을 전파하고 피해 확산 방지를 신속하게 수행할 수 있도록 하는 것이 필요하다.

방송 · 금융 · 에너지 등 국가 기간산업 분야의 정보통신시스템 및 제어시스템을 주요 정보

통신 기반시설로 지정하여 보호범위를 확대하고, 기업의 사회적 책임성을 강화하기 위한 기업 정보보호 관리체계(ISMS) 인증 확대 및 기업 사이버 보안수준을 객관적으로 감사하고 관련 정보를 외부에 공시하는 제도 도입을 고려해야 한다. 보안이 취약한 중소기업의 경우, 인력 지원 및 취약점 점검 등 종합적인 기술지원 체계를 마련하는 것이 필요하다. 사이버공격 대응 기술 개발을 위해 국가 R&D 예산 확대(2012년 민간수요 사이버보안 기술개발 비용은 국가 R&D예산 16조 원의 0.14%인 220억 원) 및 악성코드 탐지 · 분석 등과 같은 대응기술을 국가 핵심기술로 지정하여 연구를 강화하는 것이 필요하다. 그리고 무엇보다 전문인력 양성 및 확보가 시급한데, 단시간에 고급인력 확보가 어렵기 때문에 제도권 안에서 화이트 해커를 양성하고, 대학(원)의 정보보호학과 신설 및 정원 확대, 국가 차원의 정보보안 인력 양성 기관 설립 방안을 고려하는 것도 필요하다.

마지막으로, 보안의식 강화 및 보안제품(서비스) 경쟁력 제고를 위해 사이버공격시 대국민 홍보체계를 개선하고, 국내 IT 보안시장 활성화 및 신규 물리 · 융합보안 시장을 육성 및 창출해야 한다. 보안의식 강화를 위해 사이버 보안을 문화 차원에서 접근하도록 공감대를 형성하고, 생활화할 수 있도록 대국민 사이버 보안 교육과정 개설 · 확대, 매체를 활용한 사이버 보안 알림 환경을 구축하여 사이버 보안 캠페인 활동을 지원해야 한다.

국내 IT 보안시장 활성화를 위해 혁신형 사이버 보안 창업기업을 발굴하여 육성하고, 보안기술의 거래 활성화를 위한 유통체계 구축 및 타산업에서의 활용을 증대시키기 위한 생태계를 조성해야 한다. 또한, 보안제품 및 서비스 발주시 저평가된 유지관리율을 현실화하고 하도급 저가발주 등의 SW 일괄발주의 폐해 방지를 위한 분리발주를 정착시킬 필요가 있다. 또한, 사이버 보안산업을 수출주력 품목으로 정하고 품목별, 지역별, 기업의 성장단계별로 특화된 지원 프로그램을 제공하여 해외진출 킬러 콘텐츠로 육성하는 것을 고려해야 한다. 사이버 보안센터의 구축 및 운영 노하우 등 우리의 사이버 보안 체계 구축 경험을 비즈니스 모델화(한국형 사이버 보안 모델)하여 개도국에 전수하고, 국가별 거점확보와 개발은행과의 협력인프라 설립 등을 통한 사이버 보안 글로벌 협력벨트 구축을 도모해야 한다.

### 사이버공격 대응전략 수립 및 시행시 고려사항

사이버공격 대응전략의 효과적인 시행을 위해 민간분야 사이버 보안 강화 종합대책 관련 정책은 미래창조과학부에서 총괄 조정하여 종합대책 이행관리, 부처 간 정책 및 이견 조정 등의 역할을 수행해야 한다. 또한 정보보안 전문기관인 한국인터넷진흥원이 종합대책에 따른 연차별 이행계획을 수립하고 중점 실행 및 관리를 수행하여 사이버 보안 컨트롤타워 부재를 해결하는 것이 필요하다.

또한 사이버 공간을 영토, 영해, 영공, 우주에 이은 제5의 영역으로 인식하고 사이버 보안을 국가보안의 차원에서 접근할 수 있도록 공감대를 형성하는 것이 가장 중요하다. 국가 차원에서의 정보보안과 관련 예산을 확보하고 인력을 마련한다고 해도 기관 및 기업 스스로 보안의식이 결여되어 있다면 사이버 공격에 효과적으로 대응할 수 없다. 그리고 국민 보안의식 제고를 위해 방송매체 등을 활용하여 사이버 보안 공유 환경을 마련하고 정보보안을 하나의 생활로 받아들일 수 있도록 분위기를 조성할 필요가 있다. 이러한 노력으로 모든 국민 개개인이 사이버 보안의 중요성을 깨닫고 대비해 나갈 때 대한민국이 진정한 인터넷 강국으로 거듭날 수 있을 것이다. ST