[인터넷보안] 인터넷 침해사고의 국제공조, 어떻게 할 것인가?

지난해 정부에서는 OECD 장관회의를 통해 “OECD가 인터넷보안과 정보보호를 위한 국제 공조체계 마련에 나서줄 것”을 요청한 바 있다. 또한, 하마둔 투레 ITU 사무총장도 사이버 안전망 구축을 위한 공동 프레임워크를 구축할 것이며, 범 세계적으로 사이버 평화를 완성하기 위해 적극 나설 것을 천명한 바 있다.

이외에도 서울 선언문을 통하여, 안전한 인터넷, 열린 인터넷, 그린(green) 인터넷이라는 인터넷 경제의 바람직한 미래상을 만들었다. 안전한 인터넷이란 인터넷 경제가 확산되면서 나타나고 있는 각종 역기능들에 대해 세계 각국이 대책마련에 들어가야 함을 말하는 것이다. 열린 인터넷이란 미래의 인터넷 경제가 어느 한 분야에 치우쳐 진행되어서는 안된다는 것이다. 즉, 인터넷은 다양성이 보장된 세계화를 이루는데 기여해야 한다는 것이다. 그린 인터넷이란 친환경을 강조하는 것으로써 정보통신기술(ICT)을 인류의 편의성을 높이는 데만 사용할 것이 아니라 환경문제를 해결하는 친환경의 도구로도 사용해야 한다는 것이다. 또한, 미래 유비쿼터스 사회 구축은 IPv6 체계를 기반으로 단계적으로 유·무선 통신망, 방송망, 인터넷 망과 최종적으로 USN(Ubiquitous Sensor Network)이 All-IP 망으로 통합되는 광대역통합망(BcN, Broadband Convergence Network)을 중심으로 구축될 것으로 예측되고 있다. 이러한 미래의 유비쿼터스 사회는 BcN을 통해 개인정보를 포함한 사회의 모든 정보들이 개인이 필요로 하는 곳에 유통시켜줄 것으로 보인다. 이처럼 방대하고 중요한 정보들이 BcN(인터넷 포함)과 같은 공유 네트워크를 통해 유통되면 이를 보호하기 위한 각종 대책들이 필요하며, 각종 서비스들을 제공하는 여러 업체들간 혹은 국가간의 정보 공유와 협력체계가 필요할 것으로 판단된다.

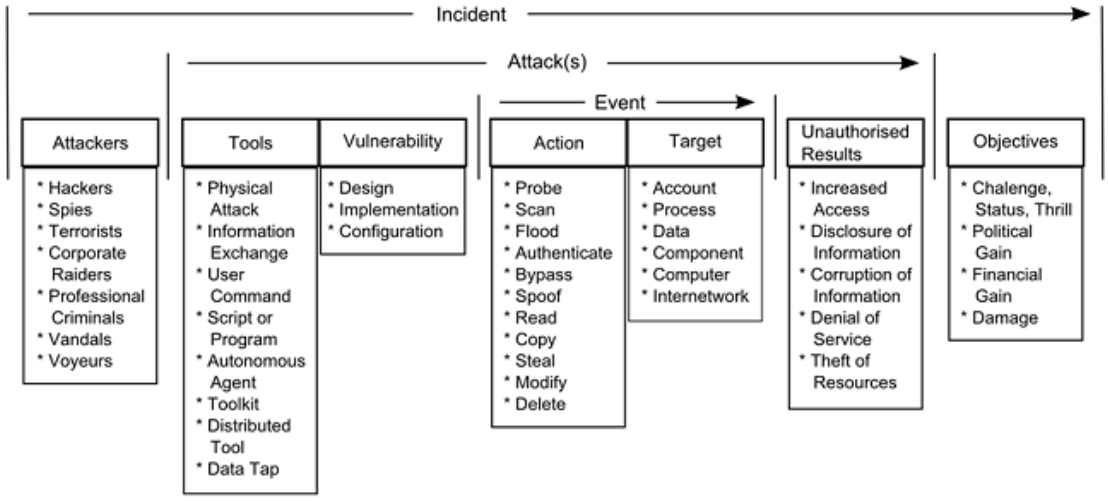
이처럼 국내외에서는 인터넷보안과 정보보호를 위해 각국이 서로 협력하여야 함을 말하고 있으나, 구체적으로 어떻게 할 것인지에 대해서는 아직까지 특별한 방안이 나오지 않고 있다. 본 기고에서는 인터넷 침해사고시 국제공조를 어떻게 할 것인지에 대한 것을 제14차 ASTAP Forum 회의 및 지난 8월 마카오에서 개최된 제16차 회의에서의 토론 결과를 중심으로 살펴보고자 한다. 2007년에 개최된 13차 ASTAP Forum에서는 정보보호전문가그룹의 공동의장인 일본측 Takechi의 발의로, ASTAP 회원국의 자발적인 참여로 각 국가 간에 이동되는 패킷에 대한 흐름을 쉽게 파악하여 해킹이나 기타 인터넷 관련 공격에 함께 대응하자는 WorldMap View project가 총회에서 승인되었다. 즉, 각국의 인터넷 침해 정보들을 공동으로 활용하여 이에 대응할 수 있는 방안을 찾아보자는 것이다. 이어서 지난해 개최된 제14차 ASTAP Forum에서는 이러한 인터넷 침해사고에 대한 국제적인 공조가 필요하다는 공통적인 공감대에 대해서는 대부분의 참석 전문가들이 동의하였으며, 프로젝트의 명칭을 APRISIA(Asia Pacific Region Information Security Initiative Activity)로 변경하였고, 각국 전문가들의 자발적인 지원을 받아 이에 대한 연구를 지속적으로 진행하기로 하였다.

올해 개최된 제16차 회의에서는 그 동안의 활동결과를 논의하고, 이러한 정보보호 침해사고의 정보를 상호 교환하기 위한 표준화를 ITU-T에서 좀 더 큰 규모로 진행하고 있는 바, 향후 관련 논의는 ITU-T에서 추진하기로 하고 ASTAP Forum의 활동 영역에서는 더 이상 추진하지 않는 것으로 결정하였으며, ITU-T 활동에 적극적으로 참여할 것을 권장하였다.

특히 최근의 사이버 침해사고들이 어느 한 국가에 한정되어 나타나는 것이 아니라 각국을 경유하거나 혹은 서로 연관된 형태의 공격, 피해 등이 발생되므로 이들에 대해 즉각적이고 효율적인 대응을 위해서는 국가간 인터넷 침해사고에 대한 공통적인 대응이 필요하다는 것에 서로가 공감하였다. 그러나, 이러한 공동대응을 위해서는 국가간에 여러 가지 인터넷 침해사고와 관련된 정보들이 상호 공유가 되어야 하나, 이를 위해서는 단순한 표준화 관점뿐만 아니라 각국의 법률적, 사회문화적 제약 사항들이 있으므로 손쉽게 결정할 수는 없으며 신중한 접근이 필요하다는 것에 참석 전문가들이 모두 동의했다.

최근의 국제적인 연구결과를 살펴보면, ITU-T SG17에서 침해사고의 국제 공조를 위한 여러가지 표준화 방안을 연구하고 있으며, IETF INCH(INCident Handling) 워킹그룹에 의해 연구된 IODEF(Incident Object Description and Exchange Format, RFC3067 and RFC5070), IDMEF(Intrusion Detection Message Exchange Format, RFC4765 and RFC4766), IDXP(Intrusion Detection Exchange Protocol, RFC4767), RID(Real-time Inter-network Defense) 프로토콜이 있다. 이러한 표준들에서 사용되어지는 Incident(침해사고) 정보들은 <그림 1>과 같은 라이프 싸이클(life cycle)을 가지고 있으며, IODEF에서 사용되어지는 Incident 정보들은 <그림 2>와 같다.

<그림 1> Incident Handling Life Cycle



<그림 2> IODEF 정보들 (RFC5070)

결언

앞에서 살펴본 연구결과들을 바탕으로 인터넷 침해사고의 국제 공동 대응을 위한 여러 가지 표준화 필요사항들이 ASTAP Forum 정보보호 전문가그룹, ITU-T SG17, ISO/IEC JTC1, IETF 등에서 지속적으로 논의될 것으로 보이며, 본 표준화 결과는 개인정보보호 등과 관련하여 매우 중요한 결과를 포함하고 있으므로 국내에서도 많은 관심을 가지고서 적극적으로 참여해야 할 것이다.

서동일 (한국전자통신연구원 인프라보호연구팀 팀장, bluesea@etri.re.kr)