[정보보호] 국제전기통신연합에서 시작되고 있는 글로벌 사이버보안 정보교환 표준화 동향

2009년 5월 30일 미국 오바마 대통령이 직접 발표한 미국정부 사이버보안 정책들을 통해 사이버보안의 범위를 정보통신망, 인터넷, 이동통신망, 컴퓨터 시스템, 제어시스템 등의 모든 중요기반시설의 보호로까지 확대하였고, 이 중요기반시설의 보호 목표와 국내외 표준화 기구들의 목표를 연계해야 한다고 천명한 바 있다.
이와 더불어 최근 2009년 6월 말 스위스 제네바에서 열린 국제전기통신연합 연구반 17(정보보호) 연구과제 4(사이버보안) 인터림(interim) 회의에서는 글로벌 사이버보안 표준을 주도하고자 하는 국제전기통신연합의 의지와 비전이 구체화되기 시작했다.
이번 사이버보안 연구과제 인터림 회의에서는 미국 대표가 미국 정부 사이버보안 정책의 일환으로 해석될 수 있는 새로운 글로벌 사이버보안 정보 교환 프레임워크라는 권고안을 제안했고, 일본, 미국, 한국 등의 사이버보안 전문가들이 참여하여 좀 더 구체화되었다. 이 권고안의 약어는 X.cybief(global CYBsecurity Information Exchange Framework)로 토의를 통해 확정되었고, 최종 드래프트 권고안 채택 여부는 2009년 9월 국제전기통신연합 연구반 17 회의에서 결정될 것으로 기대된다. 이 드래프트 권고안은 한마디로 글로벌 사이버보안 정보교환을 위한 커다란 틀과 비전을 제공함을 기본 목적으로 하고 있다. 특히 이 권고안은 미국 정부부처도 참여함으로써 미국의 사이버보안 국제표준에 대한 주도 의지를 간접적으로 확인할 수 있었다.

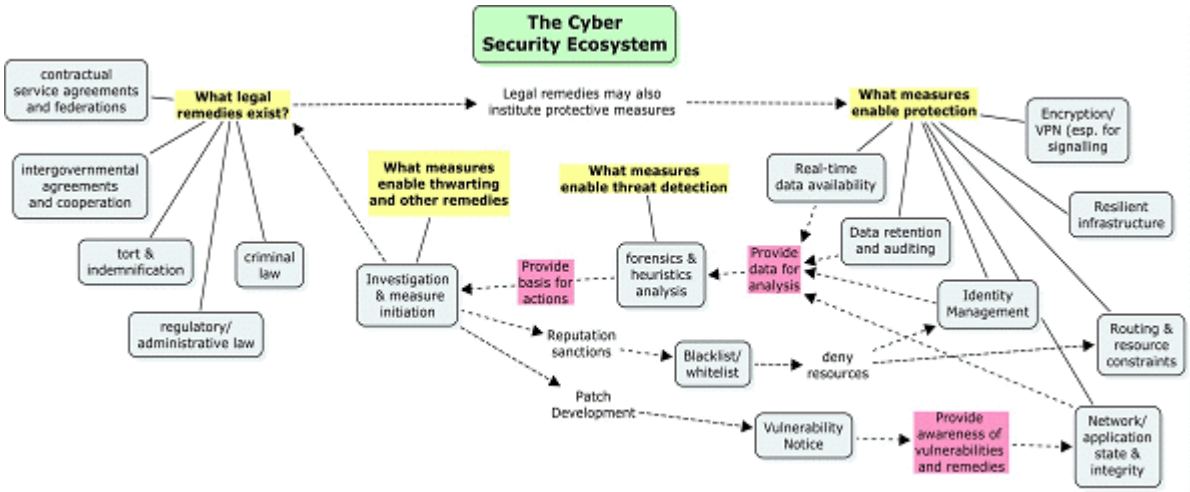
사이버보안 정보교환 프레임워크 권고안 현황

현재 사이버보안을 효율적으로 보장하기 위한 사이버보안 표준화 관련 문제점은 크게 두 가지 정도이다. 첫째, 현재 사이버보안과 관련되는 많은 국제 표준화 활동이 이루어지고 있고 이의 결과로 많은 글로벌 표준들이 개발되었으나, 이를 전체적인 차원에서 사이버 정보 교환하기 위한 프레임워크에 대한 국제 글로벌 표준이 없다는 것이다. 둘째, 여러 표준화기구에서 개발되고 있는 표준들이 한 분야만 적용되어서 서로 어떻게 연결되어야 하고, 어떤 경우에 연결되어야 하며, 어떻게 효율적으로 연계될 수 있는지에 대한 큰 그림이 없다는 것이다. 이번 권고안 제안은 이러한 문제점을 해결하고자 하는 중요한 진전이라고 볼 수 있다.
현재까지 논의되고 있는 사이버보안 정보는 사이버보안과 관련되는 장치, 소프트웨어 등의 상태(취약성 정보 포함), 침해사고와 관련되는 디지털 포렌식 정보, 침해사고 경험으로부터 얻은 서명 및 학습 데이터, 정보교환 주체, 정보교환 규격, 관련 주체 및 정보 아이덴터티, 그리고 구현 요구사항 등에 대한 구조화된 정보로 정의되었다. 따라서 사이버보안 정보는 각 장치가 갖는 취약성 정보, 사이버 공격 증거를 추적하기 위한 특수 침해사고 포렌식 정보, 침입차단시스템 또는 침입방지시스템 등이 수집한 일반 침해사고 포렌식 정보, 그리고 합법 감청 관련 인터페이스 및 정보 등을 포함하며, 여기에 더해 바이러스 정보, 피싱 사이트과 악성코드를 포함하는 웹사이트 정보 등 명성 관련 정보도 포함되며, 네트워크 상에 사

이버 공격을 실시간으로 추적하기 위한 증거 데이터까지도 포함하고 있다. 현재 이 표준은 사이버보안 정보 교환을 위한 모든 표준화 기구와 관련 조직에 의해 만들어진 기존 표준들을 확인하고 일부 필요하다고 판단되면, 이들 중 필요한 경우 일부를 국제전기통신연합 표준으로 채택하며, 필요한 경우 기존 표준을 개선하고 새로운 표준을 개발하여 사이버보안 정보교환을 위한 글로벌 표준으로 만드는 것에 목적이 있다. 이 표준의 범위는 다음과 같다.

- 교환이 가능한 사이버보안 정보의 구조
- 사이버보안 정보의 확인 및 발견
- 네트워크를 통해 신뢰된 사이버보안 정보의 획득 및 교환
- 다만, 사이버정보 정보의 획득 방법과 사용은 범위에서 제외함

현재 <그림 1>은 연구과제 4(사이버보안)에서 합의한 사이버보안의 능력과 문맥을 나타내고 있다.



<그림 1> 사이버보안 능력 및 문맥

(출처: 국제전기통신연합 연구반 17 연구과제 4의 연구과제 텍스트에서 발췌)

<그림 1>에서 알 수 있듯이 사이버보안은 침해사고 관련 데이터의 실시간 제공 수단, 실시간 데이터를 근거로 침해사고의 발생 여부를 검출하는 수단, 검출 결과를 근거로 필요한 조치를 취하는 기술적 수단, 이를 지원하기 위한 법제도적 지원 등으로 달성된다. 이 생태계가 적절하게 동작하기 위해서는 각 수단 간에 적절한 사이버 정보가 안전하고 신뢰적으로 교환되어야 한다. 따라서 이 권고안은 이러한 사이버보안 문맥 하에서 서로 교환되어야 할 사이버 정보 교환을 위한 프레임워크를 제공할 것이다.

예측되는 권고안의 논쟁사항

권고안은 지금 초기 버전이므로, 앞으로 많은 논쟁사항이 예상된다. 드래프트 권고안은 기존의 국제전기통신연합에서 표준화되지는 않았지만 널리 사용되고 있는 MITRE(미국 연방정부 출연 정보보안 연구개발 기관)가 제공하는 취약성 관련 데이터에 대한 취약성 및 평가 언어 XML 규격을 이용하려 하고 있고, FIRST (미국 침해사고 긴급대응 국제 포럼)의 공통 취약성 평가 시스템 표준을 활용한다고 되어 있다. 그러나 이를 이용하고 국제전기통신연합 권고안으로 채택하는 작업은 쉬운 일이 많은 노력과 시간이 소요될 것으로 예측된다. 둘째, 이 프레임워크의 완전성을 위해서는 현재 국제전기통신연합에서 개발하고 있는 많은 권고안을 이용해야 하는데, 이를 완성하기 위한 상당히 많은 시간이 소요될 것으로 예측된다. 셋째, 합법 감청 등의 관련 표준은 ATIS나 ETSI에서 개발된 기존 표준을 이용하고자 하는데, 합법 감청은 비단 기술적 대책뿐만 아니라 각 나라 법제도적 환경에 영향을 많이 받으므로, 이를 일관적으로 표준화하는 것은 많은 어려움이 봉착할 것으로 예측된다. 마지막으로 침해사고 데이터는 IETF 표준 등을 이용할 수 있지만, 기본 표준의 분석과 변경에 필요한 노력과 시간이 만만치 않을 것이다. 이러한 여러 어려움이 예측되지만, 이번 시도와 노력은 사이버보안을 위해 충분히 의미있는 활동으로 생각된다.

향후 추진 전망

현재 이 드래프트 권고안은 개념 형성 단계에 있고, 범위에 대한 논의가 향후에도 진행될 예정이며, 다음 9월 연구반 17 회의에서 새로운 권고안으로 확정될 것으로 예측되며, 상당한 시간에 경과한 후에 국제전기통신연합 권고안으로 최종 채택될 것이다. 결론적으로, 이 표준이 완성되기까지는 아직 시간과 노력이 필요할 듯하다. 그러나 이 표준이 개발되고 나면, 사이버보안 관련 조직, 정보, 그리고 대응 방안 등에 대한 커다란 비전이 제시될 것이며, 국제전기통신연합이 사이버보안 표준에 대한 글로벌 리더십을 확보할 수 있는 계기를 마련해 줄 것이며, 글로벌 사이버보안을 강화하기 위한 표준의 역할을 강화하는 결정적 계기를 마련해줄 것으로 판단된다. 국내 사이버보안 조직과 단체의 적극적인 관찰과 참여가 요구되고 있는 시점이다.

염흥열 (ITU-T SG17 Vice-chairman, 순천향대 교수, hyyoum@sch.ac.kr)