시큐리티 라운드 대응방안

김문규 KT플랫폼연구팀/팀장

e비즈니스 기반의 정보보호 환경을 구현하는 것은 국가 경쟁력 강화 차원에 있어서 매우 중요하다. 이에 정부차원에서도 금융, 통신 등 시큐리티 강화를 위해 주요 시설의 인프라를 확고히 다지는데 본격적으로 지원하고 있으며 글로벌 경쟁력의 핵심요소로서의 정보보호 위상을 강화시켜 나가고 있다.

이는 사회 환경이 인터넷 보급이 확대되면서 오프라인 중심에서 온라인 중심으로 급격히 변화하면서 개인 및 기업, 국가에 대한 정보보호의 필요성이 한층 증대되고 있기 때문이다. 정보보호는 전통적인 오프라인상의 방식과는 전혀 다른 사이버 공간에서의 개인정보 유출과 방지에 대비하여 신속한 대응책을 강구해야만 하는 것이 현실적인 문제이다.

최근에 세계 어느 나라를 막론하고 기술선진국에서는 각 나라마다 e비즈니스 정보보호를 위한 국가 정보보호 정책을 경쟁적으로 수립하고 있으며, 특히 인터넷을 기반으

로 한 조직적이고 체계적인 시큐리티 환경을 구현해 나가고 있다. 이는 사이버 범죄로부터 해방되어 선진국 대열 진입하고자 할 경우 반드시 갖춰져야 할 기본 항목이라 할 수 있다.

현재 전세계는 e비즈니스를 기반으로 한 사회 환경의 변화로 급격한 변화에 직면하고 있는 가운데 미국, 이스라엘, 유럽 등의 선진국은 물론 각 나라마다 사이버 범죄에 대한 대응책 마련에 부심하고 있다. 특히 정부기관, 금융, 통신 등의 주요 국가 기반 시설에 대한 정보 보호 정책 수립이 본격화되고 있음은 주지의 사실이다.

가트너 그룹에서 조사된 세계 정보통신 시장은 지난 2002년 3조 2,000억 달러 규모에서 오는 2004년에는 4조 1,200억 달러의 규모로 연평균 약 12.5%의 고속성장을 할 전망이다. 특히 지난 2000년 이후부터는 전통적 통신장비 및 서비스 시장과 새롭게 부각되는 IT 산업과 격차가 나타나면서 전통적인 산업을 오는 2004년에는 역전할 것으로 보인다.

세계적으로 정보보호산업은 미국과 이스라엘이 선두그룹을 형성하면서 기술을 주도하고 있고 영국, 프랑스, 독일 등을 포함한 유럽권, 그리고 일본, 우리나라 등이 그 뒤를 추격하고 있는 상황이다. 2000년 9월 가트너 그룹의 조사에 따르면 세계 정보보호산업은 2002년 110억 달러, 2004년 200억 달러로 연평균 32%의 대폭적인 기록으로 성장할

것으로 전망했다.

특히 최근 선진 각국에서 정보보호기술이전과 관련 시스템에 대한 수출 규제를 가하고 있는 상황을 고려하면 정보주권을 유지하기 위해서는 반드시 국내 기술력 향상 및 시스템개발이 시급하다는 정부 방침으로, 이를 위해 정부에서는 정보통신망 이용 촉진 및 정보보호 등에 관한 법률 및 정보통신기반보호법 등의 법제개정을 추진했으며 올해 IT부문 3000억원 중 300억원을 정보보호기술 예산으로 책정하고 있는 실정이다.

또한, 시큐리티 라운드라 불리울 만한 국제공통평가기준(CC: Common Criteria)에 대응한 CCRA(Common Criteria Recognition Arrangement)가입을 위한 대책 마련에도 적극적이다.

무엇보다 정부는 인터넷 보급률이 세계적인 수준이면서 자주 기술강국을 위해 분발해 세계 3위 그 이상의 위상 확립을 위해 지속적으로 노력중이다.

영국 정부가 주도적으로 하는 정보보안 표준규격 BS7799는 기업이나 정부기관들이 정보를 얼마나 체계적으로 관리하고 보호하고 있는지 국제적으로 보증 받는 인증제도다. 특히 지난해에는 국제표준화기구(ISO)가 국제표준(ISO17799)으로 채택하면서 BS7799 인증은 이른바 미래의 '시큐리티라운드(Security Round)' 의 핵으로 부상했다.

이에 따라 국내업계 에서는 벌써부터 BS7799 인증을 획득하지 못할 경우 국내 시장개척은 물론 해외 수출 노선에 커다란 걸림돌로 작용할 것이라는 우려가 제기되고 있다. 이런 가운데 국내 정보보안업체 및 컨설팅업체들의 BS7799 획득 붐이 일고 있어 국내 보안 수준을 한 단계 높이는 전기가 될 것으로 예상된다.

또한, 미국은 연방수사국(FBI)내 '국가기반구조보호센터(NIPC)' 이 사이버범죄를 수사 지휘할 사령탑으로 본부에만 1백40명의 보안전문가가 있으며, 지난해 해킹방지 기술개발에만15억 달러를 투자하는 등 보안의 중요성이 커지고 있다. 이외에도 유럽연합은 유럽국가간 인터넷 보안 지침을 마련하고 공동대응 체계 구축 등 신속한 움직임을 진행하고 있다.

지금 전세계는 새로운 시큐리티 라운드 경쟁 체제에서 생존경쟁을 하는 가운데 핵심 인프라로 정보보호 환경 구축에 그 역점을 두고 있으며, 이와 더불어 우리나라도 국가 정책적으로 보안전문임원(CSO)의 지속적인 전문인력 양성확보에 적극적으로 나서야할 때라고 본다.

현재 국내에서는 정보보호 환경 구현을 위한 제1단계로서 기반보호법을 통해 인프라 기반 확립에 본격적으로 나서고 있으며 특히 금융, 통신, 건설교통 등의 민간기관을 대상으로 한 주요기반 시설에도 정부 차원에서의 지원이 원활히 이뤄질 수 있도록 추진하고 있다.

이에 따라 주요 정부기관의 기반시설에 대한 취약성 분석과 이에 대한 보완책을 준비하고 있는 실정으로 이를 토대로 시큐리티 분야에서 경쟁력을 확보, 향후 국민이 신뢰할 수 있는 안정화된 대국민 민원서비스뿐만 아니라 국가주도로 앞으로 다가올 국제간의 이슈가 되는 시큐리티 라운드 차원의 대응책 수립이 불가피하다고 사료된다.