성균관대학교 원동호 교수

주체별 정보보호 의식 함양을 위해

정보보호 관련 사고가 자주 등장하면서 그 원인과 결과를 놓고 '이렇게 하면 된다 혹은 저렇게 하면 된다'는 식의 해결책이 쏟아지고 있다. 물론 정보보호를 잘할 수 있는 방법은 하나일 수가 없다. 관점에 따라, 한편으로는 상황에 따라 얼마든지 달라질 수 있다. 그 해법에 대해 국내 민간 분야의 정보보호를 담당하고 있는 KISA의 이사진들은 어떻게 생각하고 있을까. 이번 호부터 이들과 함께 그 해법을 찾아 보고자 한다.

| 편집자 주 |

두 차례의 세계대전을 거치면서 정부 주도로 발전한 암호 기술은 70년대 후반을 지나면서 민간에 공개돼 상업적으로 사용되기 시작했다. 이후 암호기술에서 점차 발전한 정보보호 분야는 30여년 만에 비약적인 성장을 이루고 있다.

우리나라는 1999년 말부터 ADSL을 앞세운 초고속 인터넷 보급 확대로 인해, 세계적으로 유례를 찾기 힘들 정도로 짧은 기간 내에 IT 강국으로 부상했다. 하지만 정보화의 필수 기반인 정보보호 기술 수준이나 인식은 높지 않은 것이 사실이다. 일례로, 우리나라는 2008년 9월 현재 스팸메일 발송 도메인 수를 기준으로 전 세계

5위를 기록하고 있으며, 지난 4월 악성코드 유포 및 경유 건수는 841건으로 최고치를 경신한 바 있다. 인터넷 뱅킹이나 모바일 뱅킹, 교통카드, 인터넷 쇼핑 등 보안 기술이 이미 우리의 일상생활에 깊숙하게 자리 잡고 있는 상황에서 사소한 보안 대책 미비는 큰 사고로 이어질 수 있다. 특히 최근 들어 개인정보 유출과 관련된 사고가 끊이지 않고 있는데, 지난 2월 옥션의 1,000만 회원 개인정보 유출을 시작으로, 3월과 4월에는 LG 텔레콤과 하나로텔레콤의 가입자 정보유출이 있었으며, 7월에는 다음 한메일 유출 사고, 9월에는 사상 최대인 1,100만 GS 칼텍스 회원 개인정보가 유출됐다. 이외에도 4월에 발생한 청와대 전산망 해킹 사고나 8월에 발생한 교과부 홈페이지 개인정보 노출사고에서 볼 수 있듯 관련 대책 마련이 시급한 실정이지만, 정작 법·제도적인 측면이나 정보보호 의식, 정보보호 전문 인력은 여전히 부족한 상황이다. 지난해 공공부문의 개인정보보호 예산은 불과 8억원으로, 이는 전체 정보화 예산인 4,187억원의 0.2%에도 미치지 못하는 수치일 뿐만 아니라, 이마저도 관련 사업과 무관한 예산이 6억여 원으로 사실상 정보보호 예산은 전무한 것이나 마찬가지였다.

정보보호, 기업경영의 필수요소로

앞서 나열한 개인정보 유출 사고의 공통된 특징을 보면, 해킹에 의한 것으로 추정되는 옥션이나 청와대 전산망 해킹을 제외하고는 모두 내부자의 고의 또는 실수에 의한 것으로, 조금만 주의를 기울였다면 충분히 막을 수 있는 사고라는 점에서 충격적이며, 우리나라 정보보호의 현주소를 그대로 보여준다고 할 수 있다. 이런 문제를 해결하기 위해 다양한 해결책이 제시되고 있는데, 이는 크게 법·제도의 정비 및 보완, 정보보호 전문인력 양성, 그리고 정보보호 의식 고취로 구분할 수 있다.

이 가운데 법·제도의 정비 및 보완은 최근 정부에서 정보통신기반보호법에 대한 개정(안)을 마련해 지난 9월 1일자로 입법예고하는 등 정보보호에 대한 관련 법률을 정비하고 있다. 하지만 이와 달리, 정보보호 전문인력 양성은 크게 주목받지 못하고 있는 실정임을 감안할 때, 정보보호 의식을 높이는 것은 요원하기만 하다. 실제로 수 백만에서 수 천만의 개인정보를 보유하고 있는 기업을 대상으로 실시한 조사에 따르면, IT 투자 대비 정보보호 투자 비율이 1% 미만이라고 답한 국내 기업은 전체 78.3%로, 미국 12%, 영국 14%와 큰 차이를 보인 것으로 나타났다. 우리나라 기업의 정보보호에 대한 의식이 얼마나 낮은 수준인가를 알 수 있다.

사실 기업의 입장에서 보면 정보보호에 대한 투자가 가시적인 매출이나 이익 증대로 이어지지 않기 때문에 소홀히 할 수도 있지만, 이는 대형 보안 사고의 등장이 회사의 존립 기반을 위태롭게 할 수 있음을 간과하는 것이다. 각 기업의 입장에서 보면, 대형 개인정보 유출 사고가 잇달아 발생하고 있는 지금이 오히려 개인정보보호 수준을 점검하는 기회가 될 수 있다. 고객의 정보를 불필요하게 많이 수집하고 있지는 않은 지, 수집된 정보를 지나치게 남용하고 있지는 않은 지, 그리고 보안 전문인력이 정보의 라이프사이클을 제대로 관리하는 지 등을 점검해 혹시 발생할지 모르는 사고를 방지해야 한다. 아울러, 각 기업의 정보보호에 대한 투자 확대는 기업에게만 맡겨서는 뚜렷한 효과를 보기 힘들기 때문에 정부의 관련 예산 확보와 기업에 대한 재정적 지원도 함께 이루어져야 할 것이다. 이와 함께 각 기업도 정보보호에 대한 투자가 '밑 빠진 독에 물 붓기'라는 인식을 버리고 안정적 기업 경영에 필요한 필수 요소임을 자각해야 할 것이다. **S**