한국위기관리논집 제9권 제6호 2013. 06 111~140쪽

개인정보보호의 현황과 개선방안

신원부*, 김태훈**, 김종업***

제4의 혁명으로 불리는 스마트 모바일 혁명은 스마트 폰을 비롯한 다양한 디지털 기기들을 활용해 클라우드 컴퓨팅과 빅 데이터를 활용한 스마트워크 구현과 이전에 누리지 못한 편익을 가져다주었지만, 개인정보의 해킹·유출이라는 과제를 동시에 가져왔다. 2012년 3월에 새로운 개인정보보호법이 발효되었지만, 여전히 개인정보보호는 스마트 모바일 시대의 가장 시급하고 핵심적인 과제로 부상하였다. 따라서 국가 차원의 정보보호 대응체계 마련을 위한 정책 및 제도개선필요(국가정보보호 종합계획수립 등)하고, 해킹 및 사이버테러 방어를 위한 새로운 기술 도입 시급하다고 할 수 있다. 본 연구는 이러한 문제를 인식하고 공공 및 민간(금융)부문 정보보호 실태파악, 현황 및 문제점 분석·진단하였다. 이를 통해, 새로운 정보보안시스템 도입 및 개선방안 도출하였다. 본 연구는 최근 주요 개인정보 유출 사례분석을 통해 피해 유형을 분류하였고, 공공부문을 중심으로 개인정보보호와 관련한 현황 진단을 통해 실태를 분석하였다. 이러한 사례분석 및 현황진단의 결과를 토대로 개선방안 도출하는 문헌연구와 실증연구를 병행하여 사용하였다.

주제어: 개인정보보호, 해킹, 유출, 정보보안시스템

Ⅰ. 서론

정보통신기술(ICT)의 발전은 공공과 민간부문을 막론하고 개인에서부터 국가까지 많은 편익과 변화를 초래하였다. 정보통신기술의 발전은 제4의 혁명으로 불리는 스마트 모바일을 통해 이전에 경험해 보지 못한 다양한 서비스가 가능해졌다. 하지만, 정보통신기술의 발전이 가져다 준 편익의 이면에는 개인정보의 유출과 해킹 등으로 인한 피해가 증가하고, 국가 사회적인 문제가 되고 있다. 특히 2011년에는 네이트(Nate)와 농협 등 많은 곳에서 대규모의 개인정보의 유출 사례가 발생했고, 매년 되풀이 되고 있는 실정이다. 특히 지난 3월 20일에도 금융기관・방송국 6곳을 대상으로 한 사이버 공격으로 인해 큰 피해를 입는 등 매년 그 심각성과 피해가 커지고 있는 실정이다. 즉, 유출과 해킹 등에 의한 대규모 개인 및 고객정보가 전방위적으로 유출되고 있고, 이는 단순한 개인차원이 아닌 정부, 금융권 등 모든 분야에 걸쳐 무차별적으로 이루어져 원인규명 및 대책마련이 시급하다고 할 수 있다.

* 제1저자, ** 제2저자, *** 교신저자.

경찰청장의 이메일 해킹, 현대캐피탈과 삼성카드의 대규모 고객 정보 유출, 네이트·싸이월드의 해킹으로 인한 고객의 개인정보 유출은 우려를 넘어 국가적인 대응을 필요로 하게 되었다. 정보통신기술의 발전에 따라 개인정보보호와 관련한 이슈들은 더욱 다양하고 복잡해지고 있다.

또한, 무선통신, 클라우드 컴퓨팅, 그리고 스마트 워킹 등 유비쿼터스(Ubiquitous) 환경의 구축이 가능해져 보다 편리하고 다양한 서비스를 활용하게 되었다. 많은 혜택만큼 부작용도 증가하여 과거에는 볼 수 없었던 DDos공격, 사이버 테러 같은 대규모·지능화된 보안 침해사례 등이 크게 증가하다. 이러한 개인정보 및 보안위협은 국가 간의 공간적 장벽을 허물고, 단시일 내에 광범위한 범위의 침해를 가져온다. 다시 말해, 공공부문과 민간부문을 구분하지 않고 발생하고, 위협의 방법과 범위가 갈수록 다양해지고 있다. 대표적 사례로, 2007년 4월 에스토니아에서 구(舊)소련군 동상 철거에 대한 보복으로 러시아 해커가 에스토니아의 주요 정부부처, 금융기관 등에 무차별적인 사이버 테러를 감행되었고, 2009년 7월과 2011년 3월 청와대를 비롯한 정부 주요기관 DDos 공격 등 해킹과 사이버 테러가 지속적으로 발생 중에 있다(박동균·김태민, 2012: 36). 농협의 전산망 파괴와 네이트 해킹사고와 같은 개인정보에 대한 보안 위협 역시 가중되고 있다. 금융기관이나 포털 사이트 개인정보의 유출은 2차적인 보안 피해를 초래하였다. 문제는 항상 이러한 사건 이후 철저히 대비하겠다는 정부 및 민간부문의 약속과는 별개로 지속적으로 발생한다는 점이다. 기존의 대응으로는 한계가 있어, 새로운 대안이 필요다. 개인정보의 유출이나 해킹 시 이를 원천적으로 완전 봉쇄할 방법은 현실적으로 어려움이 있다.

그리고 정보통신기술의 활용이 증가했지만 보안관련 예산의 감소와 인력이 부족한 실정인데, 정보보호예산은 2008년 1,600억, 2009년 1,740억, 2010년 2,700억으로 증가하다[1] 2011년 2,030억으로 감소하였다. 중앙 정부부처의 정보화 및 정보보호 예산을 분석한 결과, '11년도에도 대통령실, 민주평통자문위원회, 소방방재청 등 3개 부처에서 정보보호 예산을 전혀 투입하지 않은 것으로 나타났다. 한편, 2011년 8월 현재 중앙부처(42개 기관)의 정보보호 전담인력은 142.5명이며, 15명이 정보보호 관련 자격증을 보유하였는데, 정보보호 인력이 정보보호 자격증을 보유한 기관은 8개 기관(외교통상부, 농림수산식품부, 국방부, 기상청, 방위사업청, 병무청, 특허청, 국민권익위)에 불과하다. 중앙부처의 정보시스템을 통합관리하고 있는 정부통합전산센터 내 정보보호 전담인력은 42명이며, 28명이 정보보호 관련 자격증을 보유하고 있지만, 개인정보보호 추진체계의 중심기관인 행정안전부의 경우 정보보안 자격증 소지자가 한 명도 없는 것으로 나타나는 것처럼 문제의 심각성이 있다고 할 수 있다.

스마트폰의 보급 확대, SNS의 활성화, 그리고 클라우드 컴퓨팅(Cloud computing)과 빅 데이터(Big data) 기술의 발달로 인해 더욱 정보의 수집, 분석, 그리고 활용이 더욱 가속할 되고 있다. 이러한 정보의 활용이 국가경쟁력과 직결되는 시점에 있지만 개인정보의 유출은 가장 큰 걸림돌이다. 비록 개인정보보호법이 2012년 3월 20일에 공포되어 시행되고 있지만, 국가 차원의 정보보호 대응체계 마련

1) 2009년 7월 DDos 공격으로 인해 정보보호에 대한 관심으로 일시적으로 증가하였으나, 정보보호 및 기반시설 보완을 위해 예산이 증가한 것이며, 국가 전체의 예산증가율을 감안할 경우 실질적으로 정보보호와 관련한 예산은 감소한 것으로 볼 수 있다.

을 위한 정책 및 제도 개선이 필요(국가정보보호 종합계획수립 등)하고, 해킹 및 사이버테러 방어 등 국가안보 차원[2]에서도 새로운 기술 도입 시급하다고 할 수 있다. 본 연구는 이러한 문제를 인식하고 공공 및 민간(금융)부문 정보보호 실태파악, 현황 및 문제점 분석·진단하였다. 이를 통해, 새로운 정보보안시스템 도입 및 개선방안 도출하였다. 본 연구는 최근 주요 개인정보 유출 사례분석을 통해 피해 유형을 분류하였고, 공공부문을 중심으로 현황진단을 통해 운영실태 분석했다. 이러한 사례분석 및 현황진단의 결과를 토대로 개선방안 도출하였다.

Ⅱ. 이론적 고찰

1. 개인정보보호의 개념정립

정보화 사회에서는 개인정보의 보호 문제와 관련하여 개인의 권리와 권익을 어떠한 형태로든 침해받지 않도록 해야 한다. 개인정보의 정의는 국가에 따라 다양하게 정의되는데, 식별된 또는 식별할 수 있는 수 있는 개인에 관한 정보(OECD이사회 개인정보보호를 위한 권고 제1호), 특정한 또는 특정 가능한 자연인의 인적·물적 상황에 관한 개별정보(독일 연방정보보호법 제1장), 개인의 이름, 주민등록번호, 신체외형기록, 주소, 전화번호, 교육 수준, 재정상태, 의료기록 및 고용기록 등을 포함하나 이에 한정되지 아니하며, 개인을 식별하거나 묘사하는 기관에 의해 보관되는 정보(미국 캘리포니아주법 제1798조 제29항)라고 한다(문신용 외, 2003; 정대경, 2012: 924). 한편, 영국의 개인정보보호법 제1조에서는 어떤 개인에 관한 의견의 표현을 포함하여 그 정보(또는 데이터 이용자가 가지고 있는 다른 정보)로부터 동일성을 인식할 수 있고, 또는 살아있는 사람에 관한 정보를 구성하는 자료를 말하고 있다(전은정 외, 2012: 68). 우리의 경우 "생존하는 개인에 관한 정보로서 당해 정보에 포함되어 있는 이름, 주민등록번호 등의 사항에 의하여 당해 개인을 식별할 수 있는 정보"로 규정[3]하고 있다.

한편, 개인정보보호와 관련된 법률과 관련하여 그 적용 범위 역시 나라마다 다양하다. 개인정보는 생존하고 있는 개인에 관한 정보로 법적인 자연인으로서 현재 생존하고 있는 개인을 보호대상으로 한다. 따라서 사망하였거나 사망으로 추정되는 자(행방불명 및 소재 불명으로 생존을 담보할 수 없는 자 등)는 제외한다. 개인을 식별할 수 있는 정보로 이름, 생년월일, 주민등록번호 등 타인과 구별할 수 있는 정보이다. 당해 특정 정보를 가지고 식별할 수 없으나, 다른 정보와 쉽게 조합하여 당해 개인을 식별할 수 있는 경우이다. 예를 들어, 주소를 가지고는 당해 개인을 식별할 수 없으나, 이름과 조합할 경우 특정인을 식별할 수 있기 때문에 주소 등도 개인정보에 해당된다. 개인에 관한 기술로서 직업,

2) 정보통신은 포괄적 안보의 관점에서 논의되고 있다(이재은, 2013: 191).
3) 공공기관의 개인정보보호에 관한 법률 제1조 총칙 1항에 의거 이는 당해 정보만으로는 특정개인을 식별할 수 없더라도 다른 정보와 용이하게 결합하여 식별할 수 있는 것을 포함된다.

병력, 종교 등 개인에 관한 신체기록 전반을 의미한다고 볼 수 있으며, 이러한 기록들이 이름 등과 결합하여 당해 개인을 식별할 수 있는 자료가 되면 개인정보라고 할 수 있다. 법인 기타 단체에 관한 정보는 제외, 이는 개인정보를 생존하고 있는 자연인을 대상으로 하고 있기 때문이다. 법인 등의 정보에 포함되어 있는 당해 법인 임직원에 관한 개인정보도 제외된다.

<표 1> 개인정보보호의 정의

구분		주요내용
OECD	가이드라인 제1조	식별된 또는 식별 가능한 개인에 관한 정보
EU	개인정보보호 지침 제2조	정보주체의 신원이 확인되었거나 확인 가능한 정보
프랑스	정보처리축적 및 자유에 관한 법 제14조	형식에 관계없이 직접 또는 간접으로 개인을 식별할 수 있게 하는 정보로서 자연인 또는 법인이 처리하는 정보
독일	연방개인정보법 제4조	신원이 확인되었거나 확인 가능한 정보주체의 인적·물적 환경에 관한 일체의 정보
영국	개인정보보호법 제1조	신원을 확인할 수 있는 생존하고 있는 개인과 관련된 데이터, 데이터로부터 신원이 확인 가능한 생존개인과 관련된 데이터
미국	프라이버시 보호법 Sec. 552a	개인(미국 시민 또는 법적으로 영주권이 인정된 외국인)에 대한 기록(정보기관에 의해 유지·수집·사용 또는 배포되는 개인에 대한 정보의 항목, 수입 또는 집합)
일본	개인정보보호에 과한 법 제2조	생존하는 개인에 대한 정보로서 특정한 개인을 식별할 수 있는 정보
한국	개인정보보호법 제2조	살아있는 개인에 관한 정보로서 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아 볼 수 있는 정보

※ 자료: 정대경(2011: 924)을 중심으로 재구성함.

개인에 관한 정보는 공공기록, 내부기록(정보주체로부터 직접 얻어진 기록), 그리고 외부기록(정보주체가 아닌 제3자로부터 얻은 기록)으로 구분 가능하다. 공공기록은 정부의 연구과정, 허가절차, 행정 및 사법절차의 과정에서 수집된 기록으로서 대중에게도 어느 정도 열람의 기회가 제공되는 정보이다. 인구통계조사자료, 부동산양도에 따른 등기이전, 소송, 저당권설정, 판결 및 영업허가 또는 자격인증 등의 기록, 자동차운전면허나 출생 및 사망기록 등이 이에 포함된다. 내부기록은 정보수집자가 정보주체로부터 직접 수집한 자료들로서 각종 거래활동을 통해 얻어진다. 공공부문과 민간부문의 각종 사이트에 가입할 경우에 기입하는 행위를 통해 얻어지는 개인정보가 대표적이다. 외부기록은 정보주체 이외의 제3자로부터 얻는 것으로, 제3자의 범위에는 사회적, 정치적 조직체를 비롯하여 각종 출판물, 개인정보의 내부기록을 판매하는 사람들이 포함된다.

정보통신기술의 발달로 인해 생활방식의 변화와 다양한 서비스를 누릴 수 있는 반면, 해킹이나 사이버 테러 같은 역기능이 수반된다. 새롭고 다각적인 범죄행위 발생하는데, 컴퓨터의 부정조작, 오용, 파괴, 스파이행위, 도청, 정보변조, 음해 및 부정유출, 타 시스템에 불법접근(illegal access) 및 침투 등이다. 또한, 사회적 혼란, 기능마비 발생이 우려되는데, 국가 및 산업 주요 정보 절도 또는 부정유출 등으로 인한 사회적 혼란, 시스템 통합(System Integration: SI)으로 인한 정보통신시스템이나 정보통

신망의 파괴 또는 불시 운영중단으로 인한 기능이 마비될 수 있다. 이를 통해, 개인정보 침해 등에 의한 사회적 물의와 2차적인 피해 등이 발생할 수 있다. 공공부문은 물론, 민간부문(기업·사회집단 등)에 의해서 대량의 개인정보가 축적되며, 개인에 관한 자료가 증대되면서 자신이 모르는 가운데 개인정보의 탈취와 오·남용의 가능성이 증대되었다. 데이터의 축적은 복지, 징세, 의료, 교육 등 여러 분야에서 시간의 절약과 효율성을 높일 수 있으므로, 위험성에도 불구하고 피할 수 없는 현상으로 받아들여진다. 하지만, 개인정보의 누출과 오·남용으로 개인의 삶을 좌우할 수 있는 위험성이 높아지는데, 당사자가 모르는 가운데 개인정보가 활용·통제될 경우, 타율적으로 개인의 운명이 좌우될 수 있다. 예를 들어 개인에 대한 틀린 정보와 불완전한 기록으로 인해 이용자의 정보당사자에 대한 잘못된 인식과 결정을 내리게 할 수 있다. 또한, 해킹으로 인한 유출·조작으로 인한 유사한 상황이 언제든지 발생할 수 있다.

2. 개인정보 보호 활동: 공공부문과 민간부문의 비교

공공기관의 개인정보보호는 개인정보 침해를 막기 위해 국가 주도하에 관련 법률이나 제도, 그리고 정책에 의한 개인정보보호를 의미한다. 개인정보에 관한 성문화된 법률이나 정책을 통한 명확한 규정으로 법적인 대처방안을 통해 적극적인 피해보상과 보호가 가능하다. 개인정보의 탈취와 오·남용을 막고 개인의 이익을 보호하는 것이 목표로 각종 솔루션 지원으로 규제 효과를 상승시킨다. 하지만, 과다한 관리 및 준수로 인해 비용을 증가시키고, 강제 참여로 인한 개인정보에 대한 윤리의식이 미흡하다. 또한, 민간부문에 비해 상대적으로 현실 상황에 대한 이해 부족으로 감독이 미비하고, 관할 범위의 제한이 있다.

반면에, 민간부문의 개인정보보호는 민간 사업자들이 기본법을 토대로 현실적인 수행가능성에 맞추어 세부지침을 마련하여 자율적으로 적용하고 준수해 나가는 제도이다. 자발적인 참여로 개인정보 윤리의식이 고양되고, 이익 달성에 공동체적 시너지 효과를 가진다. 통일된 기준으로 비용과 부담이 절감되고, 급변하는 현실 대응에 민첩하다. 또한 공공부문에 비해 상대적으로 법률이 규제하지 못하는 부분까지 해결이 가능하다. 그렇지만, 각 기업의 지나친 사익 추구와 경쟁으로 인해 전문기술 및 노하우 공유가 어려워 이중적인 비용과 시간이 필요한데, 강제력 결여로 참여 준수율이 불확실하고 전적인 자율참여로 개인정보의 오·남용이 상존한다.

'개인정보보호법'의 제정이후, 개인정보보호에 대한 보호활동은 더욱 강화되었다고 할 수 있다. 동법에 따르면 공공부문과 민간부문은 개인정보 보호활동에 있어서 큰 차이가 없다. 개인정보 보호활동의 필수 조항 ① 개인정보는 필수정보만 최소한으로 수집(추가적인 정보를 수집할 때는 반드시 동의를 받아야 함), ② 주민등록번호와 건강정보 등 민간정보 수집 금지(법령의 근거가 있는 경우가 아니면 주민등록번호, 민간정보 사용 금지), ③ 수집한 목적과 다르게 사용하거나 제3자 제공 금지(법령의 근거 없이 다른 용도로 사용하거나 외부로 유출하지 않도록 주의), ④ 개인정보를 처리할 경우 개인정보

처리방침 공개(개인정보 위탁 사실을 포함한 처리방침을 홈페이지나 사업장에 공개), ⑤ 내부 관리계획, 방화벽・백신・접근통제 등 안전성 확보 조치(개인정보가 해킹 등으로 유출되지 않도록 보호조치를 철저히 이행), ⑥ 개인정보의 이용이 끝난 후에는 반드시 파기(수집한 목적이 달성된 후(서비스 기간 경과 등)에는 즉시 파기), ⑦ 개인정보가 유출되었을 경우 즉시 정보주체에게 통보(유출된 것을 인지하면 5일 이내에 서면・전화・이메일 등의 방법으로 통보), ⑧ CCTV를 운영할 경우 안내판을 설치(설치목적, 장소, 촬영범위, 담당자 등을 안내, 운영방침을 수립하여 공개) 등 8개에서 공공부문과 민간부문은 동일하게 해야 한다. 공공부문은 이에 더해, 홈페이지 회원가입을 받을 경우 주민등록번호 대체수단 도입(I-Pin, 공인인증서 등 주민등록번호 이외의 실명확인 수단을 도입)해야 하는 차이가 있다(http://www.privacy.go.kr, 개인정보보호 종합지원 포털). 또한, 공공과 민간 부문은 <표 2>처럼 개인정보 보호활동은 관리적 조치, 기술적 조치, 그리고 물리적 조치를 공통적으로 해야 한다.

<표 2> 공공부문 vs. 민간부문의 개인정보 보호활동 비교

구분	주요내용
관리적 보호조치	1. 개인정보의 안전한 처리를 위한 내부 관리계획을 수립·시행2. 일반 데이터와 분리하여 보관, 유지함으로써 일반 데이터 보다 접근이 어렵도록 통제컴퓨터를 이용하여 이용자의 개인정보를 처리하는 경우에는 개인정보에 대한 접근권한을 가진 담당자 및 관리자를 지정하여 접근 계정(ID) 및 비밀번호를 부여3. 개인정보의 접근 계정(ID)은 일반 직원 계정과 관리자 계정으로 분리하여 관리하고 인사이동 등이 있을 경우 ID 변경, 말소 등 필요한 조치를 함4. 접근 권한의 관리
기술적 보호조치	1. 네트워크를 통한 접근 통제 및 보안조치2. 접근통제 시스템 설치 및 운영3. 개인정보의 암호화4. 접속기록의 보관 및 위·변조방지5. 보안프로그램 설치 및 운영
물리적 보호조치	1. 개인정보가 저장·처리되는 정보시스템은 안전한 장소, 시설 등에 보관관리하며, 보안구역으로 지정하여 신원확인장치, 잠금 장치, 감시장치 등 물리적 접근제어 장치를 이용하여 인가된 자에 한하여 출입을 허용 2. 24시간 상시 관리감독이 가능토록 담당 인력을 상주시키거나 원격 모니터링을 실시하며 출입자의 신원 및 출입 목적·시간 등 을 기록·관리 3. 출입통제활동을 방해하는 정전, 화재, 지진, 낙뢰 등 긴급 상황에 신속히 대처할 수 있는 장치시설을 마련

※ 자료: http://www.privacy.go.kr(개인정보보호 종합지원 포털).

3. 선행연구와 연구의 분석틀

개인정보보호법이 공표되어 시행되기 이전부터 개인정보보호에 관한 연구는 이루어졌고, 특히 2011년의 경우, DDos 공격과 공공과 민간을 막론하고 지속적으로 발생하는 개인정보의 유출과 해킹이 이루어지면서 관심이 많아졌다. 또한, 지난 3월의 방송사・금융사 6곳을 대상으로 한 사이버 공격으로 정보보안에 대한 관심이 더욱 높아지고 있다.

정보통신기술의 발전에 따른 역기능인 개인정보의 침해와 유출에 대해 다양한 연구들이 있다. 이들 연구를 분류하면 법・제도적 측면, 정책・관리적 측면, 그리고 기술적 측면으로 나눌 수 있다. 먼저, 법・제도적 측면의 연구로는 허진수(2005)는 공공부문에 비해 상대적으로 개인정보호호의 중요성을 인식한 민간부문을 다루었다. 국내・외 민간분야에서의 개인정보보호에 관한 법률과 현황을 비교하여

기본법의 제정을 주장하였고, 주민등록번호의 도용방지, 사자의 정보주체성 등에 관해 세부적 사항을 반영해야 한다고 보았다. 신영진(2011)은 민간부문에서 기업의 마케팅 차원에서 개인정보의 수집과 이용・제공이 증가하므로, 과도한 수집과 이로 인한 유출・해킹 피해가 급증하고 있다고 보고 있다. 따라서 민간부문의 개인정보보호를 위한 보다 안정된 관리체제와 제도가 개인정보보호에 포함되어야 한다고 하였다. 반면, 길준규(2004), 권헌영(2004), 김일환(2007) 등은 공공기관의 개인정보 관리의 효율적 방안으로서 법적 보호규정 및 사전협의를 실시하고, 대장의 작성 및 방침을 수립하며, 사전영향평가를 설치하는 등 관련 제도를 마련하여야 한다고 주장하였다. 고형석(2011)은 개인정보 침해 현황의 분석을 통해 피해구제에 대해 말하였는데, 개인정보보호 침해 예방과 확대 방지를 위한 단체소송제도가 필요하다고 보고 있다. 피해 구제제도로서 손해배상 책임 분쟁조정 제도가 선행되어야 함을 주장하였다. 이해영(2011)은 다른 국가들(영・프・독・일)의 개인정보보호 법제의 분석을 통해, 개인정보보호 전담기구의 증설을 위한 법제가 조속히 마련되어야 한다고 보았다.

둘째, 정책・관리적 측면에서의 연구를 보면, 신영진(2005)과 변미리(2005)는 개인정보보호의 효율적인 개선을 가져오기 위해서는 개인정보보호 예산 및 인력의 확보, 개인정보보호 관리체계의 구축, 정기적인 교육프로그램의 운영, 다양한 개인정보보호시스템의 구축 등이 필요하다고 주장하였다. 성욱준・김동욱(2011)은 AHP 기법을 활용해 정보보호기반 분야와 정보보호 정책 활동 분야로 나누어 분석하였다. 이 연구는 정책 중요도 측면과 정책의 시급성 분석을 통해 정책추진체제의 변화의 필요성, 기술의 발전에 대응하는 제도적・정책적 대응, 그리고 정보보호 전문 인력의 양성과 확충의 시급성을 주장하였다. 반면에, 기업이 고객관계관리(CRM)의 도입을 높이고 있으므로, 개인정보가 무단으로 활용되거나 유출되는 사고가 발생하지 않도록 기업 스스로 지킬 수 있는 안전대책을 마련하여야 한다고 보았다. 김명섭(2010)은 민간부문을 대상으로 관리적 측면에서 연구를 하였는데, 기업이 스스로 개인정보의 관리수준을 진단할 수 있도록 개인정보의 수집부터 파기까지 '정보통신기술망법,' '신용정보법,' '위치정보의 보호 및 이용 등에 관한 법률' 등에 근거한 세부 점검항목을 도출하였다.

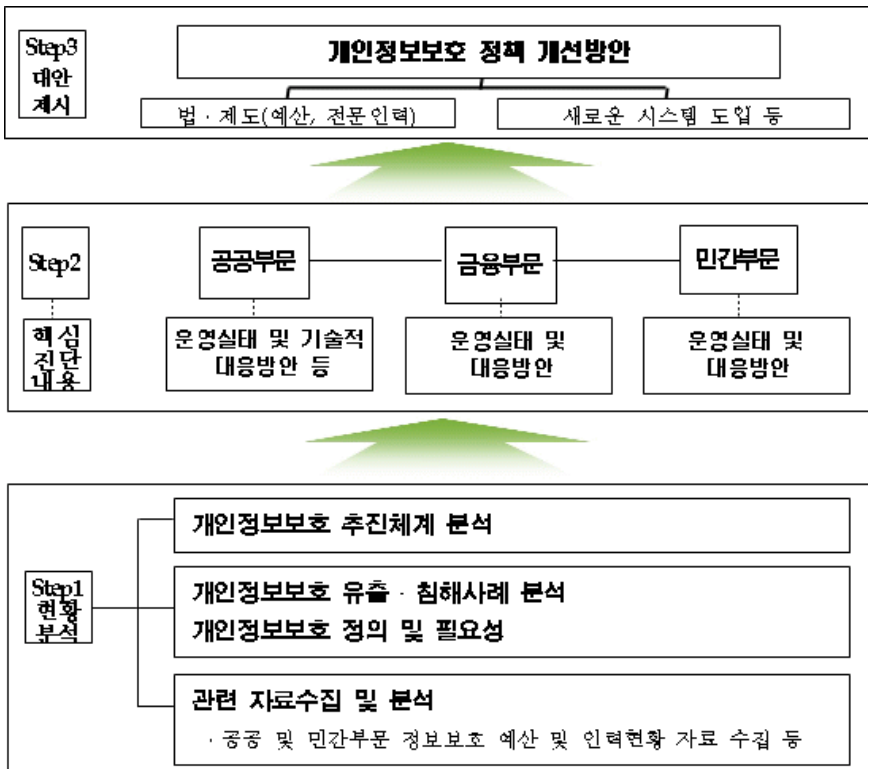
마지막으로, 기술적 측면에서의 연구는 개인정보가 외부로부터 침입 및 내부로의 불법적 유통을 방지하기 위한 기술적 대응체계를 제시하였다. 송유진(2006)은 개인정보의 수집・저장・관리・이용・제공・파기 등에 따른 개인정보의 접근통제, 보유데이터의 정보공유, 개인정보의 노출방지대책 등에 관한 기술적 보호조치가 필요하다고 보았다. 이 연구는 로그기록 및 부정접근방지를 위한 암호화, 인증강화 등의 보호조치의 필요성을 제시하였다. 김형종 외(2010)는 정보유출방지기술의 필요성과 현황을 분석하였는데, 유출방지를 위해 정보의 사용, 이동, 그리고 저장으로 나누어서 맞춤형 정보유출 탐지기술과 방지 솔루션을 제시하였다. 장현미 외(2009)는 인터넷 환경 내의 개인정보보호에 초점을 두고 아키텍처 설계방안이 필요하다고 하였다. 이 연구는 정보보호 관련 연구와 이슈별 프라이버시 문제점을 설명하고, 개인정보보호 시스템 제시 및 세부적 기능을 다루었고, 이를 통해 개인정보보호 시스템(Privacy Information Protection System, PIPS)을 제시하였다. 한편, 권자경・맹두열(2010)은 정보보호를 위해 지식정보 보안 산업에 대한 중요성을 부각시키면서, 국내의 산업차원에서 핵심 산업으로

육성・발전시키는 것이 필요하다고 하였다.

<표 3> 주요 선행연구의 요약

구분		주요내용
법·제도 측면	공공	-길준규(2004)/권헌영(2004)/김일환(2007): 공공기관의 개인정보 관리의 효율적 방안으로서 법적 보호규정 및 사전협의를 실시하고, 대장의 작성 및 방침을 수립하며, 사전영향평가를 설치하는 등 관련 제도를 마련하여야 함 -고형석(2011): 개인정보 침해 현황의 분석을 통해 피해구제에 대해 말하였는데, 개인정보보호 침해 예방과 확대 방지를 위한 단체소송제도가 필요. 피해 구제제도로서 손해배상 책임 분쟁조정 제도가 선행되어야 함
	민간	-허진수(2005): 국내외 민간분야에서의 개인정보보호에 관한 법률과 현황을 비교하여 기본법의 제정을 주장하였고, 주민등록번호의 도용방지, 사자의 정보주체성 등에 관해 세부적 사항을 반영 -신영진(2011): 민간부문에서 기업의 마케팅 차원에서 개인정보의 수집과 이용·제공이 증가하므로, 과도한 수집과 이로 인한 유출·해킹 피해가 급증. 따라서 민간부문의 개인정보보호를 위한 보다 안정된 관리체제와 제도가 개인정보보호에 포함되어야 함
정책관리 측면	공공	- 신영진(2005)/변미리(2005): 개인정보보호의 효율적인 개선을 가져오기 위해서는 개인정보보호 예산 및 인력의 확보, 개인정보보호 관리체계의 구축, 정기적인 교육프로그램의 운영, 다양한 개인정보보호시스템의 구축 등이 필요 - 성욱준·김동욱(2011): AHP 기법을 활용해 정보보호기반 분야와 정보보호 정책 활동 분야로 나누어 분석. 정책 중요도 측면과 정책의 시급성 분석을 통해 정책추진체제의 변화의 필요성, 기술의 발전에 대응하는 제도적·정책적 대응, 그리고 정보보호 전문 인력의 양성과 확충의 시급성을 주장
	민간	- 김명섭(2010): 기업이 스스로 개인정보의 관리수준을 진단할 수 있도록 개인정보의 수집부터 파기까지 '정보통신기술망법,' '신용정보법,' '위치정보의 보호 및 이용 등에 관한 법률' 등에 근거한 세부 점검항목을 도출함
기술적 측면	공공	- 송유진(2006): 개인정보의 수집·저장·관리·이용·제공·파기 등에 따른 개인정보의 접근통제, 보유데이터의 정보공유, 개인정보의 노출방지대책 등에 관한 기술적 보호조치가 필요. 로그기록 및 부정접근방지를 위한 암호화, 인증강화 등의 보호조치의 필요성 제기 - 김형종 외(2010): 정보유출방지기술의 필요성과 현황을 분석하였는데, 유출방지를 위해 정보의 사용, 이동, 그리고 저장으로 나누어서 맞춤형 정보유출 탐지 기술과 방지 솔루션을 제시
	민간	- 권자경·맹두열(2010)은 정보보호를 위해 지식정보 보안 산업에 대한 중요성을 부각시키면서, 국내의 산업차원에서 핵심 산업으로 육성·발전시키는 것이 필요성 제기

개인정보보호에 관한 다양한 선행연구의 분석을 통해, 개인정보보호와 관련해 현황의 정확한 진단을 통한 개인정보의 유형분류, 그리고 정보보호 피해사례에 대한 다각적인 접근이 필요함을 보여준다. 이를 통해, 새로운 개인정보보호법 하에서의 개인정보보호가 이루어질 수 있을 것이다. 따라서 본 연구는 선행연구를 토대로 <그림 1>과 같이 개인정보보호에 대한 문제 인식을 통해 현황을 진단하고, 각각의 정보보호 피해사례 분석을 통해, 하루가 다르게 발전을 거듭하는 정보통신기술의 발전에 부응하는 개인정보보호를 위한 개선방안을 제시하였다.



<그림 1> 연구의 분석틀

III. 개인정보보호의 현황과 진단

1. 개인정보 보호의 필요성과 피해 현황

개인정보보호는 이용자의 프라이버시 보호 및 공공기관의 정보 활용과 기업의 리스크 관리를 위해서도 중요성 부각되고 있는데, 기업이 개인정보를 제대로 관리하지 못할 경우에는 고객의 신뢰성 저하로 인하여 이미지가 크게 훼손될 수 있다. 최근 들어 기업의 개인정보 유출 사건에 대해 개인정보 유출 피해자들이 대규모 소송을 제기하고 일부 소송에서는 기업의 손해배상이 판결되는 점을 감안할 때, 개인정보보호는 기업의 경영 수익과 직결된다. 기업 간 경쟁심화에 따라 영리 극대화 및 업무 효율성 제고 등을 위해 개인정보의 제3자 제공 및 개인정보 취급의 위탁행위가 갈수록 증가하고 있다. 이로 인해 개인정보에 접근하여 취급할 수 있는 자의 범위 또한 확대되어 개인정보의 유출 및 오·남용 위험성이 높아지고 있으며, 개인정보보호 관련법규도 갈수록 강화되고 있는 추세이다.

공공부문의 경우에도 전자정부를 통한 다양한 행정정보의 활용이 개인정보 침해사고로 이어지는 경우가 발생하고 있다. 전자정부 고도화에 따른 전자적 행정서비스의 활성화, 효율적 업무수행을 위한

정보공동이용의 확산, 신속한 정보 집적과 통합처리가 가능해짐에 따라 공공기관에서 수집・보유하고 있는 개인정보에 대한 체계적이고 안전한 보호 관리의 필요성이 강조되어야 한다. 특히 최근 들어 새로운 정보통신 서비스가 등장하면서 기존에 없었던 새로운 유형의 개인정보 침해 행위 또한 지속적으로 발생하고 있는데, 스마트폰 등 신규 디지털 기기들(Digital Devices)의 급속한 확산, 소셜 네트워크 서비스(SNS, Social Network Service) 등의 확대에 따라 사회 전반의 개인정보보호에 대한 인식전환이 요구되어진다.

개인정보 유출・침해 사례는 2010년 한국인터넷진흥원 개인정보 침해 신고센터와 개인정보 분쟁 조정위원회에 총 54,832건의 개인정보 침해 관련 민원 접수되었다. 2009년 35,167건과 비교해 55.9% 증가, 이는 개인정보보호에 대한 관심과 더불어 개인정보 침해사례가 증가하고 있고, 그 문제의 심각성을 알려 주고 있다고 할 수 있다. 최근 3년간('08-'10) 개인정보 침해 관련 민원 현황을 보면 2010년에 급격하게 증가[4] 했음을 알 수 있다(<표 4 참조>).

<표 4> 최근 3년간 개인정보 피해구제 신청현황

(단위: 건)

구분	2008		2009		2010	
	공공	민간	공공	민간	공공	민간
신고	50	938	30	2,109	10	1,778
상담	166	38,657	393	32,635	462	52,582
합계	216	39,595	423	34,744	472	54,360

※ 자료: 안전행정부(2011) 내부자료.

개인정보 관련 피해유형을 살펴보면, 2010년에 접수된 개인정보 피해구제 신청건수 중 전체 88.5%가 신용정보 관련 문의 및 타인 정보의 훼손・침해・도용으로 분석되었다. 신용정보 관련 문의[5]는 38,414건(70.0%), 주민등록번호 등 타인 정보의 훼손・침해・도용이 10,137건(18.49%)으로 나타났다. 이는 각종 개인정보 유・노출 사례를 접한 이용자들이 개인정보 수집 행위자체를 민감하게 받아들였고, 개인정보에 대한 관심 및 보호의식이 높아졌음을 의미한다. 이러한 유형 외에도 웹사이트 상 개인정보의 수집・저장 단계에서 기술・관리적 조치가 미비하다는 문의가 증가하고 있다.

2009년 819건에서 2010년에는 1,551건이 접수, 다른 유형에 비해 높은 증가 수치를 보였다. 이용자들이 웹사이트 보안서버 미적용, 불합리한 개인정보 취급・관리 등 비교적 알기 쉬운 사항에 대하여 적극적으로 개선을 요구하며 민원을 접수하는 사례가 많이 증가하였기 때문으로 분석된다. 2010년 개인정보 침해신고 조치현황 전체 1,788건 중 1,331건은 고충 및 당사자 합의로 마무리된 반면 위원회 분쟁조정 148건, 사실조사 불가 247건, 민원이첩 15건 등으로 분석되었다.

4) 2010년 민간분야 상담건수가 급증한 이유는 주민번호클린센터 개통으로 이용문의가 많아졌기 때문이다.
5) 정보통신망 이용 촉진 및 정보보호 등에 관한 법률의 적용을 받지 않는다.

<표 5> 2010년 개인정보 피해구제 신청유형

(단위: 건)

접수유형	2008	2009	2010	
			신고	상담
이용자의 동의 없는 개인정보 수집 관련	1,129	1,075	225	1,042
개인정보 수집시 고지 또는 명시 의무 관련	6	15	29	46
과도한 개인정보 수집	87	115	28	118
목적 외 이용 또는 제3자 제공 관련	1,037	1,171	306	896
개인정보 취급자에 의한 훼손·침해 등	125	158	51	107
개인정보 처리 위탁시 고지의무	6	6	3	22
영업의 양수 등의 통지의무	9	6	4	18
개인정보관리책임자 관련	26	10	2	19
기술적·관리적 조치 미비 관련	1,321	819	273	1,278
수집 또는 제공받은 목적 달성 후 개인정보 미파기	294	294	138	185
동의철회·열람 또는 정정 요구 관련	949	680	337	489
동의철회, 열람·정정을 수집보다 쉽게 해야 할 조치	503	603	265	365
아동의 개인정보 수집	27	19	6	29
주민등록번호 등 타인 정보의 훼손·침해·도용	10,148	6,303	103	10,034
신용정보 관련 문의 등 타부처 소관질의	24,144	23,893	18	38,396
합계	39,811	35,167	1,788	53,044

※ 자료: 안전행정부(2011) 내부자료.

※ 주 1: 접수유형별 건수는 민간분야와 공공분야를 합한 수치

주 2: 2010년 하반기부터 주민번호클린센터 운영으로 이용 관련 문의 급증('주민등록번호 등 타인 정보의 훼손·침해·도용' 접수유형에 포함)

<표 6> 최근 3년간 개인정보 침해신고 조치현황

(단위: 건)

조치내역		2008	2009	2010
피해구제 신청 철회		72	103	126
고충 해결		538	1,448	1,161
조정 전 당사자 합의		41	61	44
위원회 분쟁조정	조정성립	32	68	39
	조정불성립	4	60	50
	기각	2	3	58
	각하	0	0	1
소계		689	1,743	1,479
법위반 사항 없음		62	10	47
사실조사 불가		175	329	247
민원 이첩(수사기관, 행정기관, 기타)		62	57	15
소계		299	396	309
합계		988	2,139	1,788

※ 자료: 안전행정부(2011) 내부자료.

2. 개인정보 유출·침해 사례

1) 공공부문

2006년부터 2010년까지 해킹 및 웜·바이러스 감염 등의 사이버 침해사고는 총 30,498건이 발생했는데, 해킹은 총 9,170건, 웜·바이러스 감염 등 총 21,328건이다. 그 중 지방자치단체가 12,762건(41.85%)으로 제일 높았으며, 교육기관, 산하기관, 국가기관 순으로 발생하였다.

<표 7> 최근 4년간(2006-2009) 정부·공공부문 침해사고 현황

(단위: 건)

구 분		웜·바이러스 감염	해 킹				합계
			경유지 악용	홈페이지 변조	자료훼손& 유출	기타	
2006년	국가기관	316	59	16	49	16	456
	지자체	1,233	162	38	21	16	1,470
	연구기관	110	125	5	17	3	260
	교육기관	489	821	145	7	2	1,464
	산하기관	396	146	49	23	6	620
	기타	4	3	-	6	3	16
	합계	2,548	1,316	253	123	46	4,286
2007년	국가기관	498	29	21	55	22	625
	지자체	3,583	94	111	24	15	3,827
	연구소	145	20	8	19	6	198
	교육기관	1,504	513	91	18	22	2,148
	산하기관	448	85	143	26	4	706
	기 타	16	26	5	34	3	84
	합 계	6,194	767	379	176	72	7,588
2008년	국가기관	813	67	23	204	80	1,187
	지자체	2,443	224	64	283	53	3,067
	연구소	698	31	6	65	18	818
	교육기관	1,210	454	82	73	48	1,867
	산하기관	418	104	36	92	22	672
	기 타	73	104	17	72	88	354
	합 계	5,655	984	228	789	309	7,965
2009년	국가기관	562	1,172		-	-	1,734
	지자체	3,580	818		-	-	4,398
	교육기관	784	503		-	-	1,287
	산하기관	1,972	681		-	-	2,653
	기 타	33	554		-	-	587
	합 계	6,931	3,728		-	-	10,659
계	국가기관	2,189	1,813		-	-	4,002
	지자체	10,839	1,923		-	-	12,762
	교육기관	3,987	2,779		-	-	6,766
	산하기관	4,187	1,740		-	-	5,927
	기 타	126	915		-	-	1,041
	합 계	21,328	9,170		-	-	30,498

※ 자료: 국가정보원 외(2011)에서 재구성.

해킹과 관련하여 교육기관이 총 9,170건 중 30.3%인 2,779건으로 가장 많은 침해사고가 발생하였으며, 그 다음으로 지방자치단체, 국가기관, 산하기관 순이다. 주목할 점은 2009년의 경우 국가기관이 1,172건으로 제일 높았으며, 증가율 면에서 매년 300% 가까운 추세이다. 이는 국가기관의 중요 정보를 노리는 해킹시도가 잦아지고 있다는 것으로 해석할 수 있어, 이에 대한 체계적이고 종합적인 대비책 즉시 수립 필요하다. 웜·바이러스 관련해서는 총 21,328건 중 지방자치단체가 50.8%인 10,839건으로 가장 높았으며 다음으로 산하기관, 교육기관, 국가기관 순으로 발생하였다.

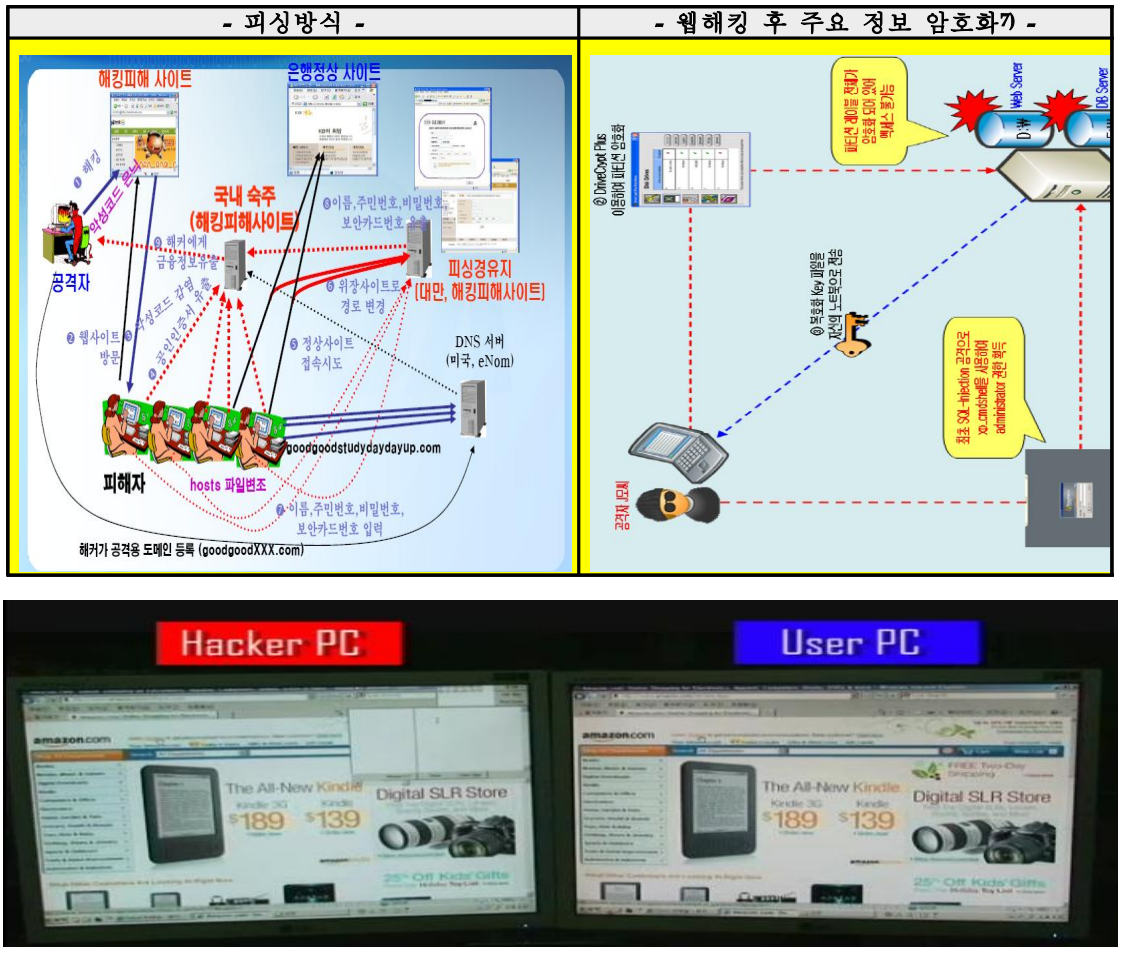
2) 금융부문

금융기관들은 이중 삼중의 보안시스템이 구축되어 공공기관이나 다른 민간 기업들에 상대적으로 안전한 것으로 인식되고 있다. 공인인증서, 보안카드, 키보드 보안프로그램, 1회용 비밀번호 생성기, OTP 등을 사용해 해킹이나 정보침해에 대응하고 있다. 그러나 해킹이나 사이버 테러, 그리고 내부자에 의한 고의적인 개인정보의 유출과 훼손이 빈번하게 발생 중[6]이다. 예를 들어, 농협의 전산망 마비로 인한 금융대란, SC 제일은행과 현대 캐피탈의 개인정보 유출 사례가 대표적이다. 또한, 2007년 국민은행처럼 개인의 동의를 구하지 않고 개인정보를 임의로 사용하여 사회적 물의를 야기했다.

반면, 정부기관과 함께 금융기관은 해킹이나 사이버 테러의 주요한 목표가 되고 있고, 다양한 방법에 의해 개인정보의 유출과 시스템 파괴가 발생하고 있다. 2011년 4월 발생한 사상 최악의 농협 금융전산 사고는 사전 치밀하게 준비된 사이버테러에 의한 것으로 확인되었다. 농협 전산망 파괴는 사고나 과실이 아닌 고의적인 범행으로, 특히 이동식 저장장치(USB)를 통한 새로운 수법이었다. 또한, 2011년 4월 현대캐피탈은 해커의 침입으로 인해 175만 명의 개인정보가 유출되었는데, 해킹사고의 원인은 현대캐피탈이 전자금융거래법 등 관련 법규에서 정한 사고예방대책 이행을 소홀히 했기 때문이다. 즉, 서버에 접근할 수 있는 계정과 비밀번호 관리에 허술했고, 광고메일 서버에 접속할 수 있는 계정과 비밀번호 5개를 외부인에게 부여하고, 퇴직 직원이 재직시절 계정과 비밀번호를 이용해 정비내역 조회 서버에 7차례나 무단 접속하는 것을 방치했다. 또한 2011년 2월 15일부터 4월 7일까지 해킹사건의 주범이 이용한 것과 같은 인터넷프로토콜(IP) 주소에서 해킹시도가 이뤄진 것을 포착하고서도 예방조치를 하지 않았다. 그리고 고객의 다양한 개인정보를 유출시켜 피해를 주기도 했는데, 2007년 3월 국민은행은 자사 인터넷복권 통장 가입고객 중 접속 빈도가 낮은 32,277명에게 인터넷복권 구매 안내메일을 발송하였다. 그러나 발송 대상인 고객들의 명단을 파일로 첨부해 개인정보인 고객 이름과 주민등록번호, 이메일 주소 등이 노출되었다.

---

6) 원격제어도구를 통해 정보 탈취, 키보드 보안기능을 통해 키보드의 보안 상태가 향상되었으나 원격제어도구로 사용자의 행동(인터넷거래 등)을 감시하여 비밀번호 등 유출, 도구에 감염된 사용자 PC 내부의 모든 자료 유출 가능하다.



<그림 2> 해킹방식 예시

※ 자료: 한국정보보호진흥원(2009)의 대학의 개인 및 문서정보 보안 위협과 대응전략 PT자료.

3) 민간부문

민간기업의 경우 필요 이상으로 광범위하게 개인정보를 보유하고 있지만, 개인정보보호에 대한 의식과 예산, 그리고 기술의 확보는 낮아 개인정보 유출과 침해 사고가 빈번하게 발생하고 있다. 주요한 사고 현황을 보면 2008년도 옥션 개인정보 유출 사건(1,863만 명), GS칼텍스 개인정보 유출(1,125만 명), 2010년 중국해커 관여 개인정보매매(2,000만 명), 2011년 네이트 개인정보 유출(3,500만 명)과 가비아 & 한국엡손 개인정보유출 등 매년 발생하고 있다. 민간 기업에서의 개인정보 유출·침해는 외부에서의 해킹이나 내부인사의 저장장치나 서류를 통한 유출 등 다양한 방법으로 이루어질 정도로 철저

7) 기관내부에 침투한 후 주요 정보가 들어 있는 시스템의 디스크를 암호화해 협박, 웹 해킹, 악성코드 이메일 등을 통해 기관 내부 시스템에 침입고도의 암호화 프로그램을 통해 디스크를 암호화하고 협박하였다.

한 보안의식 및 기술적 대안이 미흡한 것이 현실이다.

2011년 7월 26일, 국내 대형 포털 사이트인 네이트온-싸이월드가 소위 '맞춤형 악성코드'에 의해 해킹을 당했는데, 약 3,500만 명에 달하는 회원들의 이름, 아이디, e-메일, 비밀번호, 주민등록번호 등이 모두 유출되어 상당한 충격이었다. 한국의 인터넷 활용인구가 약 3,700만 명 정도라는 사실을 감안할 때 우리나라 인터넷 사용인구 대부분의 개인정보가 유출된 것으로, 국내 해킹 사고 중 사상 최대 규모이다. 이러한 개인정보 유출사고가 더욱 문제인 것은 비교적 정보보호에 만전을 기하고 있을 것으로 기대되었던 대형 포털 사이트의 개인정보들이 유출되었다는 점이다. 가장 유력한 해킹경로로는 무료 백신 업데이트 과정에서 악성코드에 감염된 개발자의 컴퓨터인 것으로 추정되고 있고, 이는 최근에 발생한 농협 및 현대캐피털의 개인정보 유출 사례와 유사한 양상을 보인다.

3. 개인정보보호의 침해 유형과 대응방안

개인정보보호와 관련된 유출·침해 사례의 증가는 사회적·국가적인 문제로 부각 되었지만, 여전히 그 대응은 미흡한 실정임을 알 수 있다. 먼저, 개인정보 유출·침해 사례 분류가 필요하다. 민간(개인), 기업, 국가 전체적으로 개인정보 및 사이버테러가 감행 중인데, 민간 및 개인 피해유형(이메일 해킹, 시스템 파괴 등), 기업수준(개인정보 유출, 시스템 파괴 등), 그리고 국가수준(사이버테러 등)으로 구분된다.

<표 8> 개인정보 및 사이버테러 유형분류

수준	피해 유형	대표 피해 사례
개인 수준	e-mail 해킹	- 경찰청장 메일 초기화면을 외부에 공개
	시스템 파괴	- 해킹을 통해 웜 바이러스·좀비화 등을 통한 시스템 마비
기업 수준	개인정보 유출	- SK커뮤니케이션스(해킹) - GS칼텍스(내부직원의 유출)
	시스템 파괴	- 농협 전산망마비(외장형 USB를 활용한 시스템 파괴)
국가 수준	사이버 테러	- 2009년 7·7 DDos 사례 - 에스토니아에 대한 러시아 해커의 공격 등

해킹 및 사이버 테러에 의한 개인정보보호의 어려움이 지속적으로 증가할 것으로 전망된다. 해킹이나 사이버 테러에 의한 개인정보의 유출과 침해, 그리고 오·남용은 발전하고 있지만, 개인정보보호를 위한 법·제도적 기반, 보안의식과 방어기술은 유출·침해 사고가 발생하고 난 이후 사후약방문처럼 이루어지고 있다. 특히, 2011년 최대 규모의 개인정보 유출사건으로 기록된 SK 커뮤니케이션즈 유출사고처럼, 특정 기업을 타깃으로 한 지능형 타깃 지속 공격(APT)이 증가할 것으로 예상되고 더욱 다양한 방법으로 개인정보의 침해와 탈취가 나타나고, 나타날 것이다. 이에 대한 대책으로 종합적인 대책(IRCT[8]) 마련이 시급한데, 법·제도적 차원, 자원(정보보호 관련 예산 및 인력) 차원, 보안의식 차

원, 그리고 정보보안 기술 차원으로 나눌 수 있다.

먼저, 법·제도적 차원과 관련해서는 개인정보와 관련해 공공기관뿐만 아니라 포털을 비롯한 인터넷서비스제공자의 개인정보 유출 위험성이 만연화 되어 있다. 그 핵심적인 원인 제공은 바로 인터넷 실명제 의무화 조항인데, 현행 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하, 정보통신망법)」 제44조의 제1항 제2호는 일일평균 이용자수 10만 이상으로서 대통령령의 기준에 해당하는 정보통신서비스 제공자들은 의무적으로 상시적 실명제(제한적 본인 확인제)를 실시하도록 하고 있다. 결과적으로, 이러한 인터넷 실명제는 주민등록번호의 수집을 부추기는 요인으로 작용하고 있으며, 대형 포털사이트의 개인정보 해킹 사건은 이러한 실명제에 의한 개인정보 수집 및 보관의 보안 취약성을 여실히 보여 주고 있다.

다음으로 자원(정보보호 관련 예산 및 인력) 차원이다. DDos와 같은 사이버 테러와 해킹이 빈번한 공공부문은 정보보안의 위험성이 날로 높아지는 현실과는 반대로 역주행하는 모습을 보인다. 2011년 정보화 예산 중 정보보안과 관련한 예산은 감소했고, 민간부문의 경우 공공부문에 비해 정보보안과 관련한 예산투자와 인력의 확보가 더욱 적어 해킹이나 사이버 테러에 더욱 취약한 모습을 보인다.

셋째, 보안의식 차원이다. 정보보안 이슈는 중요해졌지만, 여전히 정부기관들과 국내 기업들의 보안 인식은 뒤쳐지고 있는 것이 현실이다. '2010 국가 정보보호백서'에 따르면 조사 민간기업 중 63%가 정보보호에 대한 지출이 아주 없는데, 정보보호 지출을 전혀 하지 않은 이유에 대해 보안 사고로 인한 피해가 거의 없어 필요성을 느끼지 못했기 때문(65%)이라고 응답하였다. 2011년 SK커뮤니케이션즈 해킹 사고 경찰조사 분석결과 두 곳의 소규모 업체의 서버도 해킹돼 개인정보유출에 악용됐지만, 이들 업체는 경찰이 이 사실을 알려주기 전까지 자신들 회사의 서버 해킹 여부를 인지하지 못했다. 기업들의 이 같은 보안 인식은 결국 투자 저조로 이어지고, 허술한 보안을 틈타 해킹에 악용되는 악순환을 거듭되고 있다.

마지막으로, 정보보안 기술 차원이다. 개인정보의 탈취를 위한 해킹과 2차적인 피해까지 발생하는 등의 새로운 유형의 해킹 및 사이버 테러가 빈번하게 일어나고 있지만, 공공부문과 민간부문 모두 새로운 기술의 개발이나 도입은 미비하다. 농협, SK커뮤니케이션즈 등 대표적인 사례가 국내에서도 속속 발견되면서 이제 더 이상 APT[9]를 해외 보안 이슈로만 치부할 수 없는 상황이다. 특히, 2011년 SK커뮤니케이션즈 해킹 사례를 통해 알 수 있듯, APT를 통해 단 열흘 만에 3,500만 건에 달하는 개인정보를 빼낼 수 있었던 이유는 치밀하고 지능적인 공격이었기 때문이다. 이 같은 공격에 대응하기 위해서는 가장 기본적인 해킹의 방지 기술에서부터 사이버 테러에 대비하기 위한 전 방위적 보안시스

8) IRCT: Institution, Resource, Consciousness, Technology.

9) APT: Advanced Persistent Threat(지능형 타깃 지속 공격): 다양한 IT 기술과 방식을 이용해 ▲조직적으로 ▲경제적이거나 사회적인 목적을 위해 ▲다양한 보안 위협을 이용해 ▲특정 대상을 겨냥해 ▲지속적으로 공격한다는 것이 특징이다. 또한 APT의 주된 타깃은 정부기관과 사회 기간산업 시설, 정보통신 기업과 제조 기업과 금융기관 등이다. 이는 APT 공격자의 목적이 사회적 시위 또는 경제적 이익 확보임을 시사한다(안철수 연구소의 '지능적 타깃 공격 APT 대책발표'에서 발췌하였다).

템을 갖춰야 하나 현실적으로 기술적 어려움 존재한다.

4. 개인정보보호 추진체계와 현황 분석

1) 개인정보보호 추진체계

공공기관에서 수집·처리되는 개인정보보호를 위하여「공공기관의 개인정보보호에 관한 법률」에서는 공공부문의 개인정보보호체계를 규정하고 있다(<그림 5> 참조). 국무총리 소속 하에 행정안전부 차관을 위원장으로 하여 설치된 '공공기관 개인정보보호 심의위원회'는 개인정보보호에 관한 정책 및 제도 개선, 처리정보의 이용 및 제공에 대한 공공기관간의 의견조정 등 공공기관의 개인정보보호에 관한 전반적인 사항을 심의한다.

행정안전부 개인정보보호 관련 주요 권한을 살펴보면, 개인정보보호 의견 제시 및 권고, 개인정보 처리에 관한 자료제출을 요구, 필요한 경우 개인정보 처리에 관한 실태점검 등을 실시, 그리고 개인정보 파일보유와 관련하여 공공기관과 사전 협의한 내용 등을 공고하고 인터넷 상에서의 개인정보보호를 위하여 관련 법령 정비, 계획 수립, 시설 및 시스템 구축 등 제반 조치가 가능하다.

<그림 3> 공공부문 개인정보보호 추진체계

※ 자료: 안전행정부(2008)의 공공기관 개인정보관리 업무 매뉴얼.

공공기관은 관계 중앙행정기관을 통해 행정안전부와 사전 협의를 거친 다음 개인정보파일을 보유할 수 있으며 개인정보 보유에 따른 개인정보보호 방침을 수립·공고하고 개인정보파일을 보유목적 외로 이용하거나 제공하지 않아야 한다. 개인정보 주체는 처리정보에 대한 열람, 정정·삭제를 청구할 수 있으며 개인정보에 관리 또는 이익을 침해 받은 자가 행정안전부에 침해사실을 신고할 경우 공공기관은 침해사실에 대한 처리결과를 행정안전부를 통해 신고인에게 통지해야한다.

그렇지만, 대응 중심의 국가정보원과 정책수립 중심의 안전행정부는 정보보호를 바라보는 핵심가치

가 달라 통합된 정책 수립이 어렵고 중복규제와 부처 간의 협의가 잘 이루어지지 않을 수 있다. 특히, 사이버테러에 대해서는 국가정보원이 정보를 독점함으로 인해 개인정보가 침해된 기관간의 원활한 정보공유가 어려움이 있다.

2) 개인정보보호 현황 분석과 문제점

공공부문의 정보화 관련 예산은 2008년 3조 4천억 원을 정점으로 2009년 7.9%가 감소하였다가, 2010~11년에 소폭 상승하였다. 연도별 정보화 예산을 자세히 살펴보면, 2008년 3조 4,060 억원, 2009년 3조 1,370 억원, 2010년 3조 2,860 억원, 그리고 2011년 3조 3,020 억원이었다. 한편, 정보보호와 관련된 예산을 보며, 2008년 1,600 억원, 2009년 1,740 억원, 2010년 2,700 억원, 그리고 2011년 2,030 억원으로 조금씩 증가하고 있음을 볼 있다.

국가 전체의 예산증가율을 감안할 경우 실질적으로 정보보호와 관련한 예산은 감소한 것으로 볼 수 있다. DDos와 같은 사이버 테러의 위험이 더욱 증가되었고, 정보통신기술의 발전과 더불어 해킹, 개인정보의 탈취와 오·남용 사례가 증가하였음에도 2011년은 소폭 증가하였다. 개인정보보호 예산의 경우 장기적인 정책방향이 부족해 DDos와 같은 공격 건수가 해마다 증가하고 있다. 45개 중앙 정부부처의 정보화 및 정보보호 예산을 분석한 결과, 정보화 예산은 책정되어 있지만 정보보호 예산이 없는 부처는 2008년 13개(33%), 20'09년 12개(12%), 2010년 5개(11%), 2011년 3개(7%)로 점차 감소하고 있지만 여전히 정보보호에 대한 인식이 낮은 것으로 볼 수 있다.

<표 9> 연도별, 세 사업별 예산편성·집행액

(단위: 백만원)

사업명	2006		2007		2008		2009		2010		2011	
	예산	집행	예산	집행	예산	집행	예산	집행	예산	집행	예산	집행
정보보호 인프라확충[1]	18,954	13,293	14,675	13,824	7,856	7,559	6,901	6,251	12,356	12,163	12,388	10,468
전자서명인증	3,540	3,540	2,800	2,800	2,200	1,895	1,530	1,530	1,630	1,630	1,560	952
정보보호시스템 평가 & 인증기반강화[2]	-	-	-	-	4,320	4,320	2,802	2,802	3,002	3,002	2,302	1,606
개인정보 유출 & 오남용 방지[3]	-	-	797 (251)	751 (251)	824	652	3,059	3,059	4,000	3,999	4,652	4,127

※ 자료: 안전행정부(2011) 내부자료.

※ 주 1: 2006~2008년 전자정부보안등기반확충 사업이 2009년부터 '정보보호인프라확충'으로 사업명 변경

주 2: 2008년 정보보호산업경쟁력강화 사업이 2009년부터 '정보보호시스템 평가 및 인증기반 강화'로 사업명 변경

주 3: 2007년은 국가 행정정보화예산 797백만원 중 251백만원임

정보보호에 대한 예산계획의 부재는 곧 정보보호 사업계획의 부재를 뜻하며, 계획 없이 사안별로 추진되는 정보보호는 효율성을 보장할 수 없다. 정보화 예산 대비 정보보호 예산이 5% 미만인 부처도 2011년 25개(56%)에 이르는 것으로 나타났다[10]. 중앙행정기관들이 여전히 정보보호 예산 투자에 인색한 것으로 나타나 침해사고에 신속하고 적절하게 대응하지 못하고 있다는 것을 간접적으로 보여준다 (<표 10> 참조).

<표 10> 정부 부처별 정보화 예산 대비 정보보호

(단위: 백만원, %)

소관	2008년			2009년			2010년			2011년(안)		
	정보화 예산(A)	정보보호 예산(B)	비율(B/A)	정보화 예산(A)	정보보호 예산(B)	비율(B/A)	정보화 예산(A)	정보보호 예산(B)	비율(B/A)	정보화 예산(A)	정보보호 예산(B)	비율(B/A)
합계	3,406,161	160,756	4.72	3,137,783	174,246	5.55	3,286,946	270,192	8.22	3,302,324	203,451	6.16
대통령실	5,103	-	-	4,930	-	-	5,313	-	-	4,827	-	-
국회	23,503	4,982	21.20	23,059	2,387	10.35	24,912	3,766	15.12	25,552	1,000	3.91
대법원	114,935	2,580	2.24	113,809	3,937	3.46	118,643	2,487	2.10	129,226	820	0.63
헌법재판소	1,436	-	-	1,791	-	-	2,564	216	8.42	2,753	251	9.12
중앙선관위	6,158	-	-	4,942	-	-	5,264	300	5.70	8,261	196	2.37
민주평통	266	-	-	236	33	13.98	351	-	-	361	-	-
감사원	1,488	-	-	1,293	-	-	1,349	-	-	2,720	10	0.37
국무총리실	3,208	-	-	3,480	-	-	3,786	342	9.03	4,206	201	4.78
기획재정부	99,750	1,466	1.47	52,869	1,450	2.74	24,562	3,424	13.94	32,383	4,665	14.41
교과학부	65,674	3,961	6.03	71,048	4,072	5.73	79,569	6,431	8.08	84,384	9,906	11.74
외교통상부	34,893	604	1.73	73,407	557	0.76	88,193	1,074	1.22	97,568	7,809	8.00
통일부	2,394	26	1.09	1,812	66	3.64	3,132	210	6.70	10,629	3,986	37.50
법무부	58,366	6,834	11.71	66,029	9,090	13.77	78,061	12,005	15.38	79,146	15,772	19.93
행안부	588,472	63,909	10.86	522,385	53,911	10.32	653,649	80,923	12.38	621,001	36,790	5.92

10) 2008년 39개, 87%→ 2009년 37개, 82% → 2010년 20개, 44%.

<표 10> 정부 부처별 정보화 예산 대비 정보보호(계속)

(단위: 백만원, %)

소관	2008년			2009년			2010년			2011년(안)		
	정보화 예산(A)	정보보호 예산(B)	비율 (B/A)	정보화 예산(A)	정보보호 예산(B)	비율 (B/A)	정보화 예산(A)	정보보호 예산(B)	비율 (B/A)	정보화 예산(A)	정보보호 예산(B)	비율 (B/A)
문관부	53,187	1,149	2.16	57,168	1,890	3.31	53,164	3,503	6.59	48,515	4,226	8.71
농림식품부	39,763	479	1.20	39,727	640	1.61	37,784	242	0.64	37,022	778	2.10
지경부	1,336,340	28,680	2.15	1,172,745	34,858	2.97	1,143,665	44,133	3.86	962,763	18,606	1.93
보복부	84,124	1,450	1.72	86,377	2,014	2.33	97,792	10,332	10.57	79,277	2,333	2.94
환경부	15,364	359	2.34	21,378	306	1.43	14,880	997	6.70	17,906	2,173	12.14
노동부	67,299	2,086	3.10	65,119	1,220	1.87	66,714	104	0.16	76,945	842	1.09
여성부	2,284	-	-	1,386	-	-	2,062	192	9.31	3,077	140	4.55
국토해양부	162,032	709	0.44	125,867	2,181	1.73	88,270	2,968	3.36	102,205	3,187	3.12
법제처	5,325	32	0.60	4,552	115	2.53	4,073	234	5.75	4,306	6	0.14
국가보훈처	2,381	-	-	2,079	-	-	1,913	352	18.40	2,763	142	5.14
국가인권위	1,206	-	-	1,001	-	-	747	5	0.67	742	50	6.74
방송통신위	169,563	30,062	17.73	170,254	37,038	21.75	192,835	74,023	38.39	386,725	65,634	16.97
공정거래위	2,151	-	-	5,155	-	-	3,355	115	3.43	5,116	993	19.41
금융위원회	30,496	-	-	29,581	-	-	29,114	1,711	5.88	30,813	4,052	13.15
국민권익위	2,160	-	-	2,180	64	2.94	3,009	169	5.62	3,208	302	9.41
국세청	93,378	2,801	3.00	82,544	7,160	8.67	129,907	2,157	1.66	96,893	2,878	2.97
관세청	39,170	1,679	4.29	42,179	1,418	3.36	43,589	2,960	6.79	44,895	883	1.97
조달청	14,218	-	-	15,106	-	-	15,864	504	3.18	22,208	350	1.58
통계청	15,254	353	2.31	18,747	225	1.20	11,658	-	-	10,960	470	4.29
병무청	8,316	404	4.86	7,385	175	2.37	7,820	635	8.12	7,974	403	5.05
경찰청	69,000	3,395	4.92	61,236	2,962	4.84	66,505	5,124	7.70	63,062	7,413	11.76

<표 10> 정부 부처별 정보화 예산 대비 정보보호(계속)

(단위: 백만원, %)

소관	2008년			2009년			2010년			2011년(안)		
	정보화 예산(A)	정보보호 예산(B)	비율 (B/A)	정보화 예산(A)	정보보호 예산(B)	비율 (B/A)	정보화 예산(A)	정보보호 예산(B)	비율 (B/A)	정보화 예산(A)	정보보호 예산(B)	비율 (B/A)
소방방재청	24,823	-	-	24,037	96	0.40	21,184	-	-	18,382	-	-
문화재청	5,219	15	0.29	7,710	50	0.65	5,189	14	0.27	4,669	52	1.11
농촌진흥청	18,286	445	2.43	16,201	533	3.29	15,939	778	4.88	15,702	481	3.06
산림청	7,796	347	4.45	6,928	332	4.79	6,798	434	6.38	8,219	166	2.02
중기청	29,317	84	0.29	29,941	72	0.24	26,623	275	1.03	31,326	2,096	6.69
특허청	50,898	1,310	2.57	45,284	1,371	3.03	43,344	1,276	2.94	44,177	151	0.34
식약청	6,502	140	2.15	9,550	85	0.89	10,658	552	5.18	11,240	276	2.46
기상청	37,007	37	0.10	37,050	3,537	9.55	43,949	3,800	8.65	49,963	2,710	5.42
해양경찰청	7,589	378	4.98	7,226	401	5.55	7,427	341	4.59	7,826	172	2.20
행복청	67	-	-	1,000	-	-	1,767	1,084	61.35	428	80	18.69

※ 자료: 기획재정부(2010) 국회 제출자료.

반면에, 공공부문 정보보호 인력 현황은, 2009년 기준 정부·공공기관정보보호 업무 수행 인력 중 정보보호 관련 학위 소지자는 2007년 이후 약 1/3 수준으로 감소한 것으로 나타난다. 체계적이고 전문적인 교육을 받지 않은 인력이 정보보호 업무를 수행할 경우, 보안 관련 사고에 대한 적절한 판단을 하지 못하여 대형 사고로 이어질 위험성이 있다. 2009년 기준 정부·공공기관의 정보보호 업무 수행 인력 중에서 정보보호 관련 공인 자격증 소지자 역시 2006년 이후 절반 수준으로 감소한 것으로 나타난다. 정보보호 관련 공인 자격증은 CISSP(Certified Information System Security Professional), CISA(Certified Information Systems Auditor), SIS(Specialist for Information Security) 등을 의미하는데, 중앙부처(42개 기관)의 정보보호 전담인력은 '11년 8월 현재 142.5명이며, 이들 중 15명이 정보보호 관련 자격증을 보유하고 있다.

<표 11> 중앙부처 정보보호 조직·인력 현황

(단위: 명, %)

구 분	조직·인력 현황	
	전담조직	인력(평균)
중앙부처 (42개 부·처·청)	9개 기관(21.4%)/계 단위(2~3명 이상)	142.5명(3.39명)/1명 이하 4개 기관

※ 자료: 안전행정부(2011) 행정기관 정보보호 전담조직 및 인력 조사결과.

중앙부처별 평균 정보보호 인력은 3.39명이며, 여성가족부, 행복도시건설청, 그리고 민주평통은 정보보호 인력이 1명이 안 된다. 정부·공공기관 정보보호 관련 학위 및 공인자격증 소지자 비율은 매년 감소하는 것으로 분석[11] 되었다. 42개 중앙부처 중 정보보호 인력이 정보보호 자격증을 보유한 기관은 외교통상부, 농림수산식품부, 국방부, 기상청, 방위사업청, 병무청, 특허청, 국민권익위 등 8개 기관에 불과하다. 개인정보보호 추진체계의 중심기관인 안전행정부의 경우 정보보안 자격증 소지자가 한 명도 없는 것으로 나타날 정도로 정보보호에 대한 정부의 태도를 엿볼 수 있다.

<표 12> 중앙부처별 정보보호 전담인력 및 자격취득 현황

(단위: 명, 개)

부처명	정보보호 업무인력	정보화 담당부서	정보보호 담당부서	정보보호자격증수
합계	142.5	행정관리담당관		15
통일부	2.1	정보화담당관	-	0
행정안전부	3.5	정보화담당관	정보보안계	0
외교통상부	6.0	정보화담당관	사이버총괄팀	3
기획재정부	3.7	정보화담당관	-	0
고용노동부	3.7	정보화담당관	-	0
환경부	4.1	정보화담당관	-	0
농림수산식품부	2.0	정보화담당관	-	2
국토해양부	5.0	정보화통계담당관	-	0
문화체육관광부	4.2	정보통계담당관	-	0
교육과학기술부	5.0	행정관리담당관	정보보호팀	0
법무부	4.4	정보화담당관	-	0
지식경제부	5.0	정보화담당관	-	0
보건복지부	4.0	정보화담당관	-	0
여성가족부	0.3	법무정보화담당관	-	1
국방부	10.0	정보화기획관	정보보호팀	0
법제처	1.6	법제정보과	-	0
국가보훈처	1.0	정보화팀	-	0
국세청	7.0	전산정보관리관	전산보안계	1
기상청	4.0	정보통신기술과	-	0
농촌진흥청	1.2	지식정보화담당관실	-	0
대검찰청	2.0	정보통신과	-	0

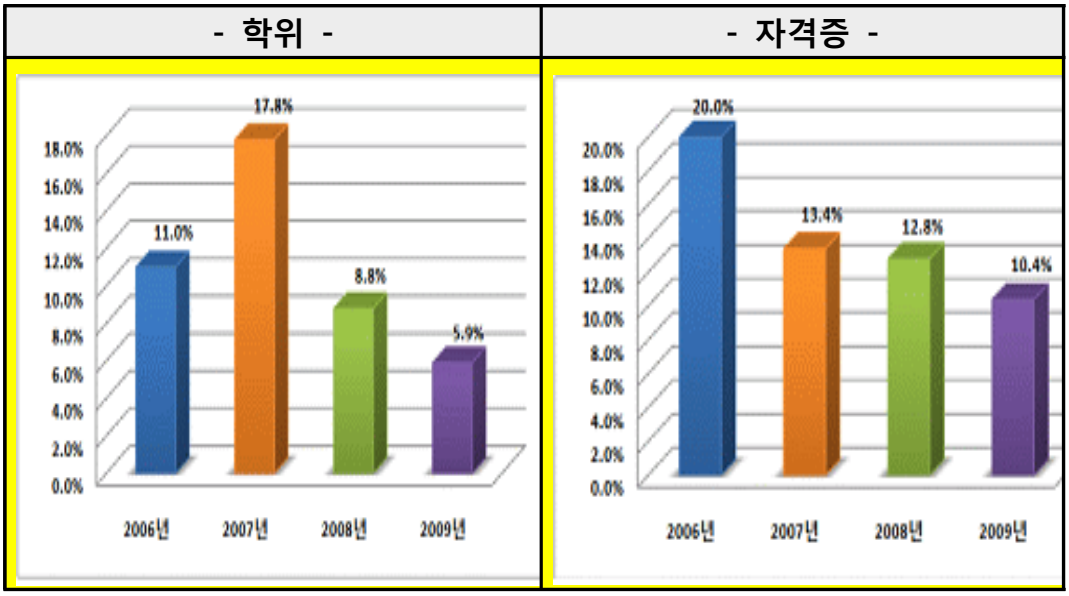
11) 정보보호 관련 학위로는 정보보호 관련 학과에서 부여하는 석사 학위 이상의 학위를 의미한다.

<표 12> 중앙부처별 정보보호 전담인력 및 자격취득 현황(계속)

(단위: 명, 개)

부처명	정보보호 업무인력	정보화 담당부서	정보보호 담당부서	정보보호자격증수
문화재청	1.3	정보화기획팀	-	0
행복도시건설청	0.4	정보인프라과	-	0
방위사업청	3.5	전산정보관리소	-	4
병무청	2.5	정보기획과	-	1
산림청	1.3	정보통계담당관실	-	0
관세청	4.5	정보협력국	-	0
경찰청	22.0	정보통신관리관실	정보통신보안계	0
소방방재청	1.6	정보화담당관	-	0
식약청	1.5	정보화담당관	-	0
조달청	1.6	정보기획과	-	0
중소기업청	1.3	고객정보화담당관	-	0
통계청	3.0	정보화기획과	정보보안팀	0
특허청	5.0	정보기획국	정보기반과	1
해양경찰청	3.0	정보통신과	정보통신보안계	0
방통위	3.6	정보전략팀	-	0
국무총리실	1.5	인사과	-	0
민주평통	0.5	기획재정담당관	-	1
공정거래위	1.5	정보화담당관	-	0
금융위	1.4	규제개혁법무담당관	-	0
국가인권위	0.6	행정법무담당관	-	0
국민권익위	1.1	행정관리담당관	-	1

※ 자료: 안전행정부(2011) 내부자료.



<그림 4> 정보보호 관련 학위 및 공인자격증 소지자 비율

※ 자료: 국가정보원 외(2011).

Ⅳ. 스마트시대 개인정보보호: 개선방안 및 정책제언

1. 개인정보보호 개선방안

1) 법 · 제도 보완 및 마련

개인정보보호와 관련해 인터넷 실명제 보완과 새로운 인식 코드의 필요성과 개인정보 관리체계 개선, 그리고 개인정보보호법의 보완이 우선되어야 한다. 먼저, 인터넷 실명제 보완과 새로운 인식 코드의 필요성과 관련해서는 결과적으로 구조적 측면의 법적 규제가 개인정보 유출과 비즈니스 차원의 유용 가능성을 부추기는 상황이다. 즉, 인터넷 실명제의 의무화를 통하여 개인정보 수집이 사실상 강제되고 있어, 관련 규정들을 재고할 필요가 있다. 더욱이, 사업자의 입장에서는 이러한 규정들을 빌미로 이용자들에게 각종 정보를 요구하여, 이를 마케팅의 목적으로 활용이 가능하다. 「정보통신망법」 제23조의2 제1항과 「개인정보보호법」 제24조 제2항은 주민등록번호 이외의 실명 인증 방법을 규정하고 있다. 이와 관련하여 주로 논의되고 있는 방법은 아이핀(i-Pin)으로 주민등록번호를 대체한다기보다는 주민등록번호의 다른 형태일 뿐이고, 기존에 주민등록번호가 가지는 유출 위험성을 그대로 아이핀이 보유하고 있다는 것이다. 예를 들어, 행정안전부'민원24'의 서류 발급 시 I-PIN을 사용하여도 해커에게 개인정보 유출이 가능하다. 따라서 궁극적으로는 주민등록번호 및 개인식별번호 자체의 수집과 활용을 가급적 자제하는 방향으로 법과 제도의 개선이 이루어질 필요가 있다고 할 수 있다.

다음으로, 개인정보 관리체계 역시 개선되어야 한다. 현대의 정보화 사회에서 개인정보보호의 문제는 단지 제도적인 차원에서 이를 규제 및 강제한다고 완전히 해결될 수 있는 문제는 아니다. 급변하는 기술적 보안 및 해킹방식의 발전을 법적 규제방식이 따라가기란 사실상 어려움이 있다. 사업자들의 정보보안에 대한 자발적 관리체계 구축을 위해 「정보통신망법」 제47조에서는 정보보호관리체계(ISMS: Information Security Management System)을 자율적으로 인증 받도록 규정하고 있다. 하지만, 인증이 의무적인 것은 아니라서 SK커뮤니케이션즈는 ISMS인증을 받지 않은 상태에서 개인정보 유출이 되었다. 따라서 이미 ISMS인증을 받은 다른 대형 포털사들(다음, NHN 등)처럼 인증을 의무화 하여 해킹이나 침해를 최소화[12]해야 한다. 이와 더불어, SK커뮤니케이션즈의 경우 개인정보보호에 특화된 또 다른 관리체계 인증인 개인정보보호 관리체계(PIMS: Personal Information Management System) 인증[13]을 '11년 초에 신청한 바 있으며, 3분기에 심사를 희망한 것으로 조사되었다. 이는 문

12) ISMS 인증심사기준에서는 15개 분야에 대하여 120개 통제사항을 제시하고 있다. 또한 이를 인증 받은 사업자들에게는 기관간 협의를 통하여 가산점 부여, 요금할인, 면제 등 일정한 혜택이 부여(ISMS인증서 발급현황, http://isms.kisa.or.kr).

13) PIMS 인증심사 기준은 개인정보관리과정, 개인정보보호대책 및 개인정보생명주기 3개 분야의 119개 통제 항목, 325개의 세부점검 사항으로 구성된다. 또한 인증 받은 사업자들에게는 「방송통신위원회고시 제2011-2호」 및 「정보통신망법 시행령」에 의해 과징금 및 과태료 경감혜택이 부여된다.

제시된 SK커뮤니케이션즈가 이미 오랜 기간 동안 포털사이트를 운영해 오면서 어떠한 공식적인 정보관리체계 인증을 받은 사실이 없다는 점을 드러내었다. 개인정보를 취급하는 모든 사이트에 대해서는 ISMS와 PIMS 인증의 의무화하여 도입해야 한다.

마지막으로, 개인정보보호법의 보완이다. 2012년 3월 개인정보보호법이 발효되었는데, 동법 23조에는 고유정보식별 정보의 처리 제한 규정을 두어 개인정보 암호화 등 안전성 확보에 필요한 조치를 하도록 하고 있지만, 현실적으로 현재 기술적, 제도적 방편으로는 해커를 원천적으로 막을 수 있기에는 한계가 존재하여 새로운 안전장치 도입이 필요하다. 예를 들어 사용자 비밀번호를 자주 바꾼다고 해킹의 위험이 사라지는 것은 아니기에, 해커에 의한 사용자의 아이디, 비밀번호 등 화면상에서 이루어질 수 있는 최신 해커방식에 의한 대응의 일환으로 화면해킹 보호에 관한 규정을 마련해야 한다.

2) 예산 및 전문 인력 확충

정보보안 관련 예산 선진국 수준으로 증대와 함께 정보보안 관련 전문인력 확대가 필요하다. 먼저, 미국을 비롯한 선진국의 경우 정보화 예산과 정보보안과 관련한 예산이 이전에 비해 둔화되었지만, 여전히 꾸준한 증가를 보이는 추세이며, 그 관심이 갈수록 높아지고 있다. 가장 빈번하게 해킹이나 사이버 테러 공격과 위협이 많은 미국은 정보화 예산 중 정보보호 예산이 최근 4년간(2006~2009) 평균 9.08%로 우리와 비교 시 높은 편이다. 반면에, 우리의 경우 4년간(2007~2011) 평균 6.16%에 그쳤다.

<표 13> 미국의 정보화 예산 & 정보보호 예산 추이

(단위: 백만달러, %)

구분	정보화 예산 추이	정보보호 예산 비율
2006년	66,215	8.3
2007년	64,911	9.1
2008년	68,121	9.2
2009년	70,716	9.7

※ 자료: 한국정보사회진흥원(2010).

한편, 정보보안 관련 전문인력 확대가 시급히 이루어져야 한다. 공공부문뿐만 아니라 민간부문까지 정보보안과 관련한 전문 인력을 확대하여 취약한 보안문제 해결을 해야 한다. 공공부문의 경우 중앙부처에 정보보안 관련 자격증 소지자가 없는 경우가 많은데 이 부분에 대한 확충이 시급한 과제이다. 한편, 민간부문의 경우 CEO(최고경영자)의 정보보안에 대한 의식이 낮고 투자에 인색한 면을 보이는데 보안 관련 인력의 확보를 의무화해야 하며, 보안 관련해 많은 기업들이 아웃 소싱을 하고 있는데 이에 대한 관리·감독이 필요하다.

3) 개인정보보호 유출방지 시스템 구축과 신기술 도입

화면해킹, 악성코드 등 개인정보의 유출·침해하는 악성코드는 증가추세를 보이고 있고, 현재의 보안 프로그램으로는 대비가 어려움이 있다. 따라서 화면보호를 위한 사이버 키보드 보안 같은 기술의 도입과 각 사안에 대한 맞춤형 보안기술의 적용이 필요하다. 2007년 이후 악성코드는 전년 대비 약 200%씩 급증하였는데, 2007년 708,742건, 2008년 1,691,323건, 2009년 2,395,802건 등이었다. 이중 유명 보안제품의 악성코드 초기 탐지율을 살펴보면, BitDefender(46%), Kaspersky(44%), NOD(40%), 안철수연구소(25%) 등 악성코드의 최소 50% 이상이 백신 등 기존 보안솔루션에 탐지되지 않고 있는 실정이다. 세계적 정보보안업체인 시만텍의 인터넷 보안 위협보고서에 따르면, 악성코드를 이용한 공격은 월 평균 2억 4천 5백만 건(시만텍에 의해서 차단된 악성코드 공격 건수) 중 76%(1억8천6백만 건)가 키보드로 입력하는 개인정보를 빼내기 위한 공격이었다. 개인정보 유출 후 악·남용이 가능한 것은 화면해킹을 통해 개인정보를 활용하기 때문으로 즉, 새로운 형태의 악성코드를 활용한 개인정보의 오·남용이 가능하기에 화면해킹과 같은 형태에 대한 대비가 필요하다.

4) 새로운 개인정보보호·보안 이슈에 대한 대비

네트워크의 발전은 점차 개인적 차원의 소통을 증대시키는 방향으로 발전하고 있고, 그 결과 대형 포털 사이트들은 서비스를 이러한 개인화된 방식의 서비스에 접목시켜 그 시장성을 확장하고 있다. 특히, 최근 트렌드가 되고 있는 SNS는 과거에 비해 정보이용자의 주체성을 더욱 부각시키는 특성을 가지고 있는데 이에 대한 대비책이 필요하다. 또한 포털 사이트들은 온라인 가계부와 같이 개인에게 최적화된 다양한 서비스들을 제공하고 있는데, 이러한 서비스의 활용을 위해서 이용자 자신은 본인의 정보들을 스스로 네트워크에 저장할 수밖에 없는 상황이다. 이와 같이 개인화된 서비스의 증대는 개인정보의 집적 및 유출 위험성을 증대시키는 역할을 하고 있으므로, 이에 대한 제도적인 마련이 필요하다.

또한, 빅 데이터와 클라우드 컴퓨팅 서비스 확대에 대한 대비도 필요하다. 스마트폰 등의 뉴미디어 활용이 본격화되면서, 이용자가 네트워크상에 저장해 놓은 정보를 언제 어디서나 접속하여 활용할 수 있게 해 주는 클라우드(cloud) 서비스가 새로운 컴퓨팅의 방식으로 급부상하고 있다. 대형 포털 사이트들도 클라우드 서비스를 통한 이용자 확대를 도모하고 있는데, 클라우드 서비스는 이용자의 측면에서 매우 유용한 서비스임에는 틀림없지만, 개인들이 가지는 정보를 네트워크상에 집적·저장시킴으로써 그 유출위험성 증대되고 있다. 대형 포털사이트의 개인정보 유출사례는 추후 본격화될 클라우드 서비스의 대규모 정보유출 위험성을 가늠해 볼 수 있게 해 주는 전형적인 사례라고 할 수 있기에 새로운 환경에 맞춘 법·제도적 뒷받침이 있어야 한다.

2. 정책제언

정보통신기술의 발전에 따른 장점과 단점이 동시에 부각되고 있는데, 무선통신, 클라우딩 컴퓨팅, 그리고 스마트 워킹을 통한 유비쿼터스 사회의 구현으로 윤택한 삶의 기회 제공이다. 하지만, 해킹으로 인한 개인정보의 탈취와 오·남용, 사이버 테러로 인한 전산시스템 파괴로 인한 사회적 불안을 야기한다. 공공부문과 민간부문을 불문하고 개인정보의 해킹과 사이버 테러로 인해 많은 피해가 발생하고 있다. 공공부문의 경우 법·제도적 미비와 함께 정부 예산에서 정보보안 예산의 감소와 전문 인력의 부족 등 정보보안에 대한 관심이 감소되고 있다. 또한 민간부문(금융부문 포함)의 경우 심각해지는 정보보안 문제에 대해 의식의 결여로 공공부문에 비해 더욱 적은 예산과 인력으로 피해가 급증하고 있다. 다양한 법률과 인터넷 실명제처럼 불필요하고 과다한 개인정보를 요구하는 현재의 법·제도의 보완이 필요하다. 최소한의 개인정보로 다양한 서비스를 누리게 하도록 개선되어야 할 것이다. 개인정보보호법에 화면해킹 보호에 관한 제도적 안전장치 등 시대의 변화에 따른 조항의 추가가 요구된다.

정보보안과 관련한 예산과 인력의 확대가 필요하다. 정부기관의 경우 선진국 수준의 정보보안 관련 예산의 확충과 부처별 전문지식을 갖춘 보안 인력이 배치이다. 민간부문은 관련 예산의 투입 증가와 아웃 소싱 보다는 직접 고용을 통한 전문 인력의 확대가 바람직하다. 보안 위협은 다양해지고 범위가 넓어지고 있는데, 그에 대응 가능한 맞춤형 보안기술과 시스템 도입이 요구된다. 예를 들어, 가장 쉽고 빈번하게 발생하며 현재의 보안 프로그램으로는 해결이 불가능한 화면해킹 악성코드는 끊임없이 새로운 변종을 양산하는데, 화면해킹을 방지하기 위한 사이버 키보드 같은 쉽고 적은 예산으로 가능한 보안 솔루션의 도입이 우선되어야 한다. 더불어 개인정보의 해킹과 사이버 테러에 대한 공공부문과 민간부문의 지속적이고 높은 보안의식 강화되어야 한다.

정보보호는 전 국가적인 차원의 문제로 ① 지속적인 투자와 전문 인력의 양성, ② 일상적인 감시활동 강화, ③ 정보보호 보안의식 증대, ④ 정보보호 관련 기관간 정보공유 및 공동대응체계 구축, ⑤ 새로운 보안솔루션 및 시스템 도입 등을 통한 철저한 대응이 필요하고 할 수 있다.

참고문헌

고형석. 2011. 개인정보보호침해와 피해구제에 관한 연구. 법조. 661: 272-317.

국가정보원. 2011. 국가정보보호백서 2007년-2010년. 서울: 국가정보원.

권자경, 맹두열. 2010. 한국 지식정보 보안산업 활성화를 위한 요건: 지식정보 보안산업체의 인식을 중심으로. 한국지역정보화학회지. 13(1): 77-102.

김동욱, 성욱준. 2012. 스마트시대 정보보호 정책에 관한 연구. 정보보호학회 논문지. 22(4): 883-899.

김동욱, 성욱준. 2011. AHP를 이용한 정보보호정책 우선순위에 관한 연구. 한국행정학회 학술대회 논문집. 2011(2): 1-21.

김현정. 2010. 전자정부의 개인정보 공동이용에 따른 개인정보보호에 관한 법적 연구. 법학논총. 34(2):

277-307.

김형종, 김진형, 이 알렉산더. 2010. 정보유출 탐지 기술의 동향 및 개인정보보호 관점에서의 고찰. 정보처리학회지. 17(2): 52-58.

문신용. 2003. 공공기관 개인정보보호. 서울: 한국행정연구원.

박대하, 백태석. 2011. 클라우드 컴퓨팅 개인정보보호 연구동향과 과제. 정보보호학회지. 21(5): 37-44.

박동균, 김태민. 2012. 미국 사이버테러 대응 시스템의 특징 및 함의. 한국위기관리논집. 12(6): 31-49.

방송통신위원회, 행정안전부, 지식경제부. 2011. 국가정보보호백서 2011. 서울: 방송통신위원회, 행정안전부, 지식경제부.

방송통신위원회, 한국인터넷진흥원. 2010. 2010년 인터넷 이용실태 조사. 서울: 방송통신위원회, 한국인터넷진흥원.

심우민. 2011. 네이트 해킹사고와 포털의 개인정보보호. 이슈와 논점. 282: 1-4.

신영진. 2011. 민간분야에서의 개인정보보호에 관한 연구: 기업마케팅을 위한 개인정보보호의 수집 및 이용・제공 제한을 중심으로. 국가정책연구. 25(2): 57-79.

신영진. 2010. 우리나라의 개인정보보호 수준 향상 및 개선을 위한 연구. 한국행정학회 학술대회논문집. 2008(3): 1-16.

윤수영. 2010. 개인정보보호법 시행으로 인한 개인정보보호 규제 환경 변화 대응전략. 정보처리학회지. 17(2): 3-9.

이재은. 2013. 국가안보 환경의 변화와 국가위기관리: 포괄적 안보 개념 하에서의 국가위기 유형. 한국위기관리논집. 9(1): 177-198.

이해영. 2011. 개인정보보호 전담기구의 법적 쟁점. 법조. 655: 76-118.

장현미, 김경미, 김혜리, 정지희, 홍승필, 강성민. 2009. 인터넷 환경 내 개인정보보호 아키텍처 설계 방안. Entrue Journal of Information Technology. 8(1): 117-131.

전은정, 김학범, 염홍열. 2012. 유럽의 개인정보보호 법・제도 동향. 정보보호학회지. 22(2): 58-72.

정대경. 2012. 국내・외 개인정보보호 정책 비교분석: 개인정보보호 법률과 전담조직을 중심으로. 정보보호학회지. 22(4): 923-939.

한국인터넷진흥원. 2009. ☎118 업무 매뉴얼. 서울: 한국인터넷진흥원.

한국인터넷진흥원. 2010. 정보보호 실태조사 2007-2009년. 서울: 한국인터넷진흥원.

한국정보보호진흥원. 2009. 대학의 개인 및 문서정보 보안 위협과 대응전략. 서울: 한국정보보호진흥원.

한국정보사회진흥원. 2010. 2007-2010 국가정보화백서. 서울: 한국정보사회진흥원.

행정안전부. 2008. 공공기관 개인정보 관리업무매뉴얼. 서울: 행정안전부.

행정안전부. 2011. 행정기관 정보보호 전담조직 및 인력 조사결과. 서울: 행정안전부

개인정보보호법. 2013. 개정 2013. 03. 23. 법률 제11690호.

공공기관의 개인정보보호에 관한 법률. 2011. 폐지 2011. 03. 29. 법률 제10465호.
http://www.privacy.go.kr. 개인정보보호 종합지원 포털.
뉴시스. 2011. http://www.newsis.com/ar_detail/(검색일: 2011. 07. 28).
서울신문. 2011. http://www.seoul.co.kr/news/newsView.php?id=201104200100(검색일: 2011. 04. 20).
연합뉴스. 2011. http://www.yonhapnews.co.kr/bulletin/2011/09/08(검색일: 2011. 09. 08).
YTN News. 2011. "경찰청장 이메일 해킹. 보안취약." http://www.ytn.co.kr/_ln/0103_201108121859373787(검색일: 2011. 08. 12).

辛源富: 연세대학교에서 행정학 박사학위를 취득하였으며(공무원 전문성의 영향요인에 관한 연구: 서울시 사례의 통합적 분석방법을 중심으로, 2013), 행정안전부 자치제도과 사무관을 거쳐 현재 한국조직진단평가원 원장으로 재직 중이다. 조직진단, 인력산정, 성과관리 등이 주요 관심분야이며, 주요 논문으로는 "지방자치단체 행정기능별 인력규모 분석(2008)"과 "지방자치단체 합리적 정원 산정모델에 관한 연구(2010)," "18대 국회 지역균형발전 관련 입법실태 분석을 통한 바람직한 입법 방향에 관한 연구(2012)" 등이 있다(applaud@hanmail.net).

金泰勳: 성균관대학교에서 행정학 박사학위를 취득하였으며(책임운영기관 사업성과 메타평가에 관한 연구: 국립중앙극장을 중심으로, 2005), 행정안전부 사무관을 거쳐 현재 국회 사무처 정책보좌관으로 재직 중이다. 문화관광정책 및 정책평가 등이 주요 관심분야이며, 「반정부시대의 행정」(2001)을 공동 번역하였다, 주요 논문으로는 "문화예술부문 책임운영기관 사업성과 메타평가지표개발 및 실증적 적용(2006)"과 "정부연구용역 평가지표 및 모형 개발(2007)," "18대 국회 지역균형발전 관련 입법실태 분석을 통한 바람직한 입법 방향에 관한 연구(2012)" 등이 있다(kendoin98@hanmail.net).

金鍾業: 영국 웨일즈대학교(University of Wales) 'Political and Cultural Studies'에서 정치학 박사학위를 취득하였으며((Local Government Reform and Political Management in the UK and South Korea: Responses to the 2000 & 2004 Acts, 2013), 현재 동아대학교・창원대학교 행정학과에 출강 중이다. 도시 및 지방행정, 지방의회론, 도시정부의 재난관리 등이 주요 관심분야이며, 주요 논문으로는 "Immigration and the National Security: A study of Philippines' territorial claim to Sabah, Malaysia(2010)," "스마트시대의 보안위협: EU5 국가를 중심으로(2011)," "한・일 지방정부의 위기관리체계에 관한 연구: BCP를 중심으로(2012)," "Illegal Immigrants and the Election in Malaysia(2012)," "18대 국회 지역균형발전 관련 입법실태 분석을 통한 바람직한 입법 방향에 관한 연구(2012)," "도시재생을 통한 창조도시 구현 방안 연구: 부산시 구도심의 문화거리 활용을 중심으로(2012)" 등이 있다(kimje49@hanmail.net).

투 고 일: 2013년 05월 05일
수 정 일: 2013년 06월 19일
게재확정일: 2013년 06월 24일

Research on Protection Statement and Improvement of Personal Information

Won Boo Shin, Tai Hoon Kim, Jong Eop Kim

Information & Communication Technology(ICT) is constantly evolving and providing new digital devices and services, such as smart-phone, SNS and cloud computing. "Smart Mobile Revolution" as called "the 4th Revolution has brought various conveniences more than we had previously thought. However, the Revolution has led to pressing questions like hacking & leak of personal information at the same time. In other words, with cloud computing and big data, the digital revolution has now brought smart working, but hacking & leak of personal information are soaring day by day. Protection of personal information will become even more important because of increase of smart phone use, SNS and cloud computing. At the same time, the use of information is directly linked to national competitiveness, so the leak personal information is the biggest stumbling block and issue. Therefore, central government should plan to introduce the protection system and technology of personal information. This study explores the statement and improvement of personal information focused on public sector. The study used the literature and empirical research method.

Key words: information protection, personal information, hacking, information security system