

지방자치단체의 정보보호 현황 및 인식의 변화 분석

노재인*, 서진완**

요약 정보화 수준이 향상됨에 따라 각종 사건들이 증가하면서 정보보호에 대한 중요성 또한 강조되어 왔다. 그동안 정부가 지속적인 노력을 기울여 왔음에도 불구하고 정보보호 관련 사건들은 증가하고 있는 것이 현실이다. 따라서 이 연구는 정부기관 중에서 시민들과 가장 먼저 접촉하는 지방자치단체를 중심으로 정부기관의 정보보호 현실에 있어서 이와 같은 모순적 상황이 발생하는 원인을 확인해 보고자 하였다. 이를 위해 정보보호와 관련한 기존의 연구결과를 토대로 정보보호와 관련한 제도, 예산·인력, 그리고 담당공무원의 인식을 중심으로 그동안 변화가 어떻게 이루어졌는지를 분석하였다. 분석결과, 중앙정부차원의 제도 및 예산의 변화를 확인할 수 있었다. 그러나 지방자치단체의 변화는 미미했으며, 담당공무원들의 정보보호에 대한 인식도 큰 변화가 없는 것으로 나타났다.

주제어: 정보보호, 자치단체 정보보호, 정보보호 인식, 개인정보 보호

Information Security and Its Awareness in Local Governments

Noh Jae In, Seo Jin-Wan

Abstract As the numbers of various cyber-crimes have sharply increased, the importance of securing information has also been emphasized. Despite the government's constant efforts to solve the issue, they hardly work in practice, and cases related to information security are still on the rise. This study investigates the reasons for the discrepancy that occurs when a solution is put to action. The research analyzes the recent shift in the administrative system with regard to information security and officials' awareness of the shift, focusing on members of local government. The results of the study confirm a steady attempt including changes in institutions at the level of the central government. However, there is still a lack of personnel and budget support at the local government level as well as not much change in the awareness of information security.

Keywords: information security, information security of local government, information security awareness, privacy protection.

2016년 1월 8일 접수, 2016년 1월 11일 심사, 2016년 2월 29일 게재확정

* 인천대학교 박사과정(shwodls84@naver.com)

** 교신저자, 인천대학교 교수(sjinwan@inu.ac.kr)

I. 서론

우리나라는 2003년부터 UN에서 시행하고 있는 세계 각국의 전자정부 평가에서 항상 상위권에 위치하였고, 2010년, 2012년, 2014년의 평가에서는 e-Participation과 e-Government Development 부문 모두 1위를 차지할 정도로 수준 높은 전자정부 환경을 구축해 왔다.¹⁾ 더욱이 정보기술의 발전으로 “유비쿼터스(Ubiquitous)” 혹은 “스마트(Smart)”라고 표현되는 정보화 환경이 사회 전반에 구축됨에 따라 공공영역에서의 정보화는 보다 편리하고 신속하게 정보서비스를 제공할 수 있도록 진화하고 있다. 유비쿼터스 환경에서는 민간과 공공부문의 물리적 구분 없이 유비쿼터스 네트워크로 연결되어 주변의 사물 간, 사물과 사람간의 방대한 정보가 빠르게 송수신 된다(한국전산원, 2004). 그러나 네트워크가 광범위해지고, 연결되어 있는 노드가 복잡하게 얽혀 있기 때문에 어느 한곳에서 해킹과 같은 보안사고가 발생하게 되면 네트워크 전체로 정보 유출이나 침해가 빠르게 확산될 수 있다(이미정 외, 2010). 그렇기 때문에 정보화사회의 발전과정에서 정보보호 이슈는 늘 가장 우선적으로 고려되어야 하는 부분으로 지목되어 왔다(서진완 외, 2008).

특히 막대한 양의 공공정보를 활용하는 국가기관이나 공공기관에서의 정보보호는 중요성이 더욱 가중된다. 이러한 이유로 학계에서는 국민의 개인정보 보호, 국가 안보의 측면에서 정보보호와 관련한 논의가 꾸준히 진행되었으며, 최근에는 경제적 측면에서도 정보보호의 중요성이 강조되고 있다. 정부차원에서 정보보호의 중요성을 인지하고 정보보호와 관련한 법제를 마련하거나 예산을 편성하고, 조직을 편성하여 운영하는 등 여러 노력을 기울이고 있다. 그

럼에도 불구하고 우리나라는 1999년 CIH바이러스 대란, 2001년 Code-red, Nimda 사건, 2003년 1·25 인터넷 대란, 2005년 전자문서 위 변조 논란, 2008년 옥션의 개인정보유출, 2009년 7.7 DDos사건, 2010년 중국 해커에 의한 개인정보 유출, 2011년 3.3 DDos, 농협 전산망 마비, 현대캐피탈 해킹, 네이트와 싸이월드의 개인정보 유출 등 정보보호가 제대로 이루어지지 않아 생기는 사건·사고가 꾸준히 발생하고 있으며, 해가 거듭될수록 그 수는 점차 증가하고 있다(서진완 외, 2008; 김동욱 외, 2012b; 정보화백서, 2012; 2013).

정보보호는 지금까지 꾸준히 제기되었던 문제였지만 그동안은 기술적 대응을 중심으로만 발전을 거듭했다. 그러나 정보기술의 활용으로도 예기치 못한 문제들에 직면하면서 기술적 대응으로는 일정 정도의 한계가 있다는 것을 확인할 수밖에 없었다(이미정 외, 2010). 이에 정보보호를 기술적인 차원이 아닌 관리 및 제도적 차원에서 이해해야 한다는 논의가 확산되었다. 실제 정보보호 문제가 발생하는 이유는 기술적 측면 보다는 ‘휴먼에러’에 의한 경우가 많다는 조사가 발표되기도 하였으며, 일부 지방자치단체에서는 공무원이 주민들의 개인정보를 유출하여 처벌받기도 하였다.²⁾

따라서 본 연구는 정보보호를 위한 정부와 학계의 노력에도 불구하고 현실에서의 상황이 긍정적인 방향으로 변화하지 않는 이유가 무엇일까라는 의문에서 출발하였다. 이를 위하여 본 연구는 정부 기관 중 시민들과 가장 먼저 접촉하는 지방자치단체를 중심으로 선행연구에서 제시되었던 개선방안들을 분석기준으로 선정하여 각각의 분석기준을 중심으로 과거부터 현재까지 어떻게 변화하였는지를 살펴보고자 하였으며, 이를 통해 정부와 학계의 그간 노력에 대

1) UN E-Government Survey (<http://unpan3.un.org/egovkb/en-us/Global-Survey>)

2) 이와 관련하여 2015년 9월 국정감사를 위해 행정자치부가 국회에 제출한 자료에 따르면 2011년부터 2015년 6월까지 개인정보 오·남용으로 징계를 받은 공무원은 매년 약 100여명을 넘고 있는 것으로 나타났다. 서울Pn 뉴스

(<http://go.seoul.co.kr/news/newsView.php?id=20151015011020>) 2015년 11월 23일 검색

한 실효성을 논의할 수 있는 토대를 마련해 보고자 하였다.

II. 이론적 논의

1. 정부차원에서의 정보보호와 중요성

1) 정보보호의 개념

정보보호(Information Security)는 주로 기술적 측면에서 정보통신망이나 네트워크를 기반으로 하는 정보를 보호한다는 협의의 정보보호로 이해되는 경향이 있지만, 최근에는 기술적 측면뿐만 아니라 관리적 차원이나 제도적 차원을 포괄하는 광의의 개념으로 이해되고 있다(서진완 외, 2008). 실제, 우리나라의 국가정보화기본법 제3조 제6항에 따르면, “정보보호”는 정보의 수집, 가공, 저장, 검색, 송신, 수신 중 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적·기술적 수단을 마련하는 것을 말한다고 정의하고 있으며, 정보통신용어사전에서도 정보보호를 정보의 수집, 가공, 저장, 검색, 송신, 수신 중 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적·기술적 수단, 또는 그러한 수단으로 이루어지는 행위로 정의하고 있어 더 이상 정보보호의 개념이 기술적 측면에서만 정의되지 않음을 확인할 수 있다. 더욱이 정보보호를 사이버범죄와 같은 응용프로그램에서 발생할 수 있는 행위로부터 정보를 보호하고, 기기의 관리상 발생하는 모든 문제와 사회적·윤리적 문제까지 고려하는 최광의 개념으로 이해하고 정의하는 경우도 있다(UN ICT Taskforce, 2003; 한국정보보호진흥원, 2005; 김성태, 2010; 김동욱·성욱준, 2012a).

한편 정보보호라는 개념과 비슷한 개념으로 정보보안이 있다. 이연수(1998)는 정보보안을 정보의 가치가 상실되지 않도록 보호하기 위해 제반수단 및 대책을 강구하기 위한 행위로 보고 구체적으로 문서보안, 전산보안, 통신보안, 인원보안, 물리적 보안 등

으로 구분하였다. 반면, 정보보호는 정보의 정상적 유지를 위해 물리적, 기술적, 자연적 장애 기능을 사전에 예방하거나 사후 회복 조치하도록 하는 것으로 구분하여 정보보안과 정보보호를 구분하고 있다(이연수, 1998; 서진완 외, 2008). 실제로 사전적 의미로 보호는 위협이나 곤란 따위가 미치지 않도록 잘 보살피며 돌보거나 잘 지켜 원래대로 보존되도록 함을 의미하며 보안은 안전을 유지한다는 뜻으로 제시되어 있다. 두 개념 자체의 차이는 존재하지만, 최근 정보보호 개념 논의에서는 정보보안의 개념을 포괄하는 추세를 보이고 있다. 과거 정보보호의 중심개념이 통신보안, 네트워크 보안과 같이 기술적으로 안전을 유지할 수 있도록 하는 기술중심적 보안에 맞춰져 있었으나 최근에는 정보를 관리하는 차원에서 정보가 원래대로 잘 보존되도록 하는 관리적 정보보호로 옮겨지고 있는 추세이며(한국인터넷진흥원, 2008), 실제로 최근 정보화 사회의 고도화로 정보보호와 관련한 문제가 복잡한 형태를 띠고 있어 두 개념을 구분하여 사용하기 보다는 포괄적으로 정의하는 것이 바람직하다.

본 연구에서도 이러한 추세에 따라 정보보호의 개념을 국가정보화기본법의 정의와 연구대상을 고려하여 관리적·제도적 차원을 포괄하는 광의의 개념으로 한정하였으며, 이연수(1998)의 연구에서 정의된 정보보안의 개념이 국가정보화기본법에서 언급한 관리적 수단을 마련하는 행위에 해당된다고 판단하여 정보보안을 포함하는 개념으로 파악하였다.

2) 정보보호의 중요성

Beck(2006)은 1986년 새로운 형태의 산업사회 및 새로운 근대화에 대한 논의를 시작하면서 ‘위험사회(Risk Society)’라는 개념을 사용하였다. 그는 기술의 발전과 위험의 발전을 정의의 관계, 즉 불가분의 관계로 이해했다. 미국의 사회학자인 Perrow 역시 고 위험 기술과 복잡한 체계가 결합되면 필연적으로 사고가 발생하며, 이는 체계의 특성에 의해 정상

적으로 발생한다고 언급하고 있다(홍성태, 2014; Perrow, 1984). 이를 정보화 사회와 연결지어본다면, 정보화 사회에서의 편익과 더불어 개인 사생활 침해나 불건전한 정보의 유통, 시스템의 파괴, 해킹 등과 같은 여러 종류의 역기능은 네트워크를 기반으로 정보가 자유롭게 유통되고 이를 공유하는 환경이 존재하는 한 항상 존재할 수밖에 없다(서진완 외, 2008). 실제로 「The Global Risks Report 2015」에 따르면 사이버 공격으로 인한 위기는 매우 큰 규모로 증가하고 있으며, 사물인터넷(IoT, Internt of Things)과 같은 혁신적 기술은 기존과는 전혀 다른 새로운 위기를 초래하고 있다.

이렇듯 정보화가 고도화 된 시점에서 국가차원의 정보보호가 중요성을 갖는 이유는 세 가지로 정리 할 수 있다. 첫 번째 이유는 국민의 정부신뢰와 관련된다. 국민의 신뢰를 얻는 정부는 정책을 효과적으로 추진할 수 있지만 국민이 정보를 신뢰하지 못하는 상황에서는 정책추진을 위한 국민의 지지와 협력을 이끌어 내기 어렵다(박희봉 외, 2003; 황창호 외, 2015). 만일 국가차원의 정보보호가 제대로 이루어지지 않아 국민들로 하여금 ‘위험하다’는 인식이 확산될 경우, 국민들의 불안감은 가중된다. 불안감이 생기면 이를 통한 불안감의 악순환이 발생하는데, 불안이 불확실성을 높이고 이는 다시 불안을 고조시키는 것이다(Sofsky, 2007). 결국 이러한 불안감의 확산은 결과적으로 국민의 정부신뢰를 낮춘다. EU에서 조사한 미래사회 위협요인으로 정보보호의 취약으로 인한 정부와 시민간의 신뢰위기를 들고 있으며(한국정보화진흥원, 2007; 윤상오, 2009; Punie, Delaritre, Maghiros and Wright, 2006), 실제 우리나라 국민을 대상으로 조사 결과 우리나라의 국민들은 개인정보 유출, 사생활 침해 등에 대한 우려가 심각한 수준이며(한국정보화진흥원, 2007) 이로 인해 전자정부 서비스를 꺼리는 현상도 발생하고 있다(윤상오, 2009).

두 번째 이유는 국가 자체의 존립에 위협을 받을

수 있기 때문이다. 과거엔 개인정보를 통해 이윤을 추구하는 형태의 사이버범죄가 많았으나, 점차 국가간의 역사 분쟁이나 자국의 이익 추구 등의 이유로 정부기관 표적형 공격이나 국가기반시설 및 산업을 위협하는 대정부적 범죄 형태가 증가하고 있다(한국인터넷진흥원, 2015). 실제로 우리나라의 경우, 1999년 CIH바이러스 대란, 2003년 1·25 인터넷 대란, 2005년 전자문서 위변조 논란, 2008년 옥션의 개인정보유출, 2010년 중국 해커에 의한 개인정보 유출, 2011년 농협 전산망 마비, 현대캐피탈 해킹, 네이트와 싸이월드의 개인정보 유출 등 불특정 다수의 개인을 대상으로 한 범죄들이 일어나기도 했지만, 2009년 7.7DDos 사이버테러, 2011년 3.3DDos 사이버테러, 2013년 6.25 사이버 테러 등과 같이 대정부적 사이버 범죄를 경험한 바 있다.

끝으로 정보보호는 단순히 개인의 사생활이나 국가안보의 차원에서 뿐만 아니라 국가의 경제적 측면에서도 매우 중요하다. 2000년 미국의 CSI(Computer Security Institute)와 FBI(Federal Bureau of Investigation)의 설문결과에서 보안사고로 인한 손실은 연간 2억 달러 이상으로 추정되었으며(신진, 2012), 2003년 1월 25일에 슬래머웜에 의해 발생한 인터넷 침해사고로 인한 세계적 손실을 영국의 Mi2g는 9억 5천만~12억 달러, 미국의 CE는 10억 달러, 한국의 KISA는 1,055억~1,675억 원으로 추산하였다(신진, 2013). 노턴사이버범죄보고서(2011)를 기준으로 우리나라의 사이버범죄 피해액을 추정 한 신진(2013)의 연구결과에 따르면, 우리나라의 연간 피해액은 80억 달러~122억 달러로 추정되며, 이를 원화로 환산하면 9조~13조원에 이른다. 이 수치가 현재 일어나고 있는 피해를 대상으로 추정하였다는 전제조건이 있기 때문에, 잠재적 피해에 대한 기회비용을 포함한다면 경제적 비용 규모는 크게 증가할 것이라고 분석하였다(신진, 2013). 2015년 우리나라 일반회계 예산 총액이 약 250조 규모였음을 감안한다면³⁾, 이는 전체 일반회계 예산의 약 1/25에 해

당하는 금액이다.

앞서 언급한 위험사회라는 측면에서 볼 때, 위험관리의 주체라고 할 수 있는 정부가 위험에 어떻게 대비하는지는 매우 중요하다. 그러나 우리나라의 경우 위험에 대한 준비와 인식은 대체적으로 사고가 발생했을 때만 이슈화되어 잠시 논의가 될 뿐 그 다음으로의 진전은 없는 실정이다(홍성태, 2014). 정보화사회의 고도화에 따라 정보보호에 대한 사회적 불안은 점차 고조되고 있는 현 시점에서 사회적 불안은 낮추고 안전한 사회로 나아가기 위해 국가차원에서의 정보보호는 필수적이다.

2. 정보보호의 연구동향 분석

정부기관을 대상으로 정보보호 이슈를 다룬 기존 연구들을 살펴보면, 의미 있는 몇 가지 경향을 확인할 수 있다. 우선 기존의 정보보호와 관련한 연구 대부분 '개인정보' 보호에 초점이 맞춰져 있다. 정부의 개인정보보호에 관한 연구들을 조금 더 구체적으로 살펴보면, 전자정부 추진 및 구현이라는 측면에서 개인정보보호 분석(문신용, 2003; 윤상오, 2009), 공공기관의 개인정보 침해(문신용 외, 2004; 신영진, 2008)에 중점을 두고 연구가 이루어졌다. 또한 이외에도 개인정보보호 수준의 개선방안(신영진, 2009), 지방정부에서의 개인정보보호 제도 분석(이자성, 2008), 생애주기와 사회문화적 가치, 개인적 성향의 관점에서 개인정보보호의 관심 분석(이향수, 2008), 개인정보보호를 위한 기술개발·기술정책(한국전산원, 2004) 등 개인정보에 대한 집중적인 연구가 이루어졌다.

두 번째 경향은 예방적 차원의 연구가 많다. 즉, 정보를 어떻게 활용해야 안전한지, 혹은 피해에 대한 대응은 어떻게 해야 하는지 보다는 예방 차원에서 정보보호에 더 초점이 맞춰져 있다. 이와 관련된 대표

적인 연구들은 개인 사생활과 관련한 정보보호를 위한 자율규제가 갖는 한계점을 연구한 강휘원(2000)의 연구, 공공기관의 개인정보보호를 위한 제도와 정책적, 기술적 개선방안 등을 연구한 문신용(2003)의 연구, 지방자치단체의 정보보호 현황을 분석하고 지방자치단체의 정보보호의 중요성을 언급한 서진완 외(2008)의 연구, 서울시 전자정부의 개인정보보호와 관련한 총체적 분석을 한 변미리(2004)의 연구 등이 있다.

세 번째로 정보보호와 관련한 정책 및 제도에 관한 연구가 많다. 이는 다시 정책 연구와 제도 연구로 구분해 살펴볼 수 있다. 정보보호 정책을 분석하거나, 정책적 우선순위를 연구하거나, 정부신뢰 차원에서의 정책 연구와 같은 정책 연구는 윤상오(2009), 신영진 외(2004), 오길영(2005), 신영진(2010) 등의 연구가 있으며, 정보보호와 관련한 법·제도의 구축, 개선, 해외 정보보호 관련 법제와의 비교, 입법과정 및 법제 자체의 분석 등과 같은 법·제도 관련 연구는 이자성(2008), 한국전산원(2004), 김철완 외(2000), 가천대학교 산학협력단(2012) 등의 연구가 있다.

끝으로, 우리나라에서 공공기관을 대상으로 정보보호와 관련한 담당 공무원들의 인식을 다룬 선행연구들이 있다. 정보보호와 관련한 선행연구들을 살펴보면 대체적으로 2000년 이후에 연구가 집중되고 있지만, 담당 공무원들의 인식과 관련한 연구는 최근에 연구 빈도가 증가하고 있는 경향을 보이고 있다. 정보보호 담당 공무원의 인식을 연구 주제로 다루었던 연구는 서울시 정보보호 현황 및 정보보호 관련한 시민과 공무원들의 인식을 분석한 변미리(2004)의 연구, 정보보호 수준을 측정하는데 관리적 차원에서 지방자치단체의 정보보호 담당공무원들의 인식을 파악하고 분석한 이미정 외(2010)의 연구, 조직 내에서 정보보호 최고 책임자(CISO)의 역할인식이 정보보

3) 예결산정보시스템 <http://nafs.assembly.go.kr:83/index.htm> (2015년 12월 28일 검색)

〈표 1〉 정부기관을 대상으로 정보보호를 다룬 연구논문들의 연구 경향

연구경향	연구논문	개선방향
개인정보보호	<ul style="list-style-type: none"> - 개인정보보호 분석 (문신용, 2003; 윤상오, 2009) - 공공기관의 개인정보 침해 (문신용 외, 2004; 신영진, 2008) - 개인정보보호 수준의 개선방안 (신영진, 2009) - 개인정보보호의 관심 분석 (이향수, 2008) - 개인정보보호를 위한 기술개발·기술정책 연구 (한국전산원, 2004) 	<ul style="list-style-type: none"> • 법·제도 개선 • 인력 및 예산 확보 • 총괄책임자 책임강화 • 담당자들의 윤리의식강화 • 제도의 내실화
예방적 차원	<ul style="list-style-type: none"> - 사생활 보호 (강휘원, 2000) - 지방자치단체 보호 현황 (서진완 외, 2008) - 서울시 개인정보보호 총체적 분석 (변미리, 2004) 	<ul style="list-style-type: none"> • 제도적 재정비 • 인력 및 예산 확보 • 담당자의 인식변화 • 최고책임자의 인식변화
정책 및 제도	<ul style="list-style-type: none"> - 정보보호정책연구 (윤상오, 2009; 신영진 외, 2004; 오길영, 2005; 신영진, 2010) - 정보보호 관련 법·제도 연구 (이자성, 2008; 한국전산원, 2004; 김철완 외, 2000; 가천대학교 산학협력단, 2012) 	<ul style="list-style-type: none"> • 제도적 정비 • 인프라구축 • 조직 설치 및 정비 • 인력과 예산 확보 • 정책결정자의 인식변화
공무원의 인식	<ul style="list-style-type: none"> - 지방자치단체 담당자 인식분석 (이미정 외, 2010; 변미리, 2004; 행정자치부, 2014) - 지방공무원과 행정인턴간 개인정보보호 인식 비교(정진우, 2013) 	<ul style="list-style-type: none"> • 인력 및 예산 확보 • 담당자의 인식 및 행태 변화 • 정책결정자의 인식변화

호 성과에 어떠한 영향을 미치는지 살펴본 김지수 외 (2012)의 연구, 지방공무원과 행정인턴의 개인정보 보호인식을 비교한 정진우(2013)의 연구, 인천시 정보보호담당자들의 인식을 통한 정보보호 수준을 확인한 행정자치부(2014)의 보고서 등이 있다.

선행연구를 분석하면서 네 가지의 연구경향 이외에 정보보호와 관련한 선행연구의 특징으로 확인할 수 있는 것은 정보보호의 중요성이 강조된 것에 비하면 전체적인 관련 연구의 양 자체가 많지 않다는 것이다. 또한, 정책 환경의 변화 내지 새로운 사이버 범죄의 영향으로 정보보호와 관련한 새로운 분야의 연구가 이루어지고 있지만, 대부분의 연구들이 일회적인 연구로 그쳤다. 더욱이 정부기관의 정보보호를 대하는 기본적인 시각이나 방법론 등은 과거와 현재에 이르기 까지 변화되는 모습을 보였다고 보기 어렵다. 이는 선행연구들이 제시하고 있는 개선방안을 통해서 확인이 가능하다. 선행연구에서 제시하고 있는 개선방안은 대부분 비슷한 대안을 제시하고 있으며, 이는 크게 법·제도의 재정비, 인력 및 예산의 확보, 담당자 및

정책결정자의 인식 등으로 요약할 수 있는데, 연구 당시의 상황에서 정태적인 분석에 그치는 한편 변화라는 측면에서 바라보지 못한 아쉬움이 있다.

Ⅲ. 분석 방법 및 분석틀

앞서 살펴본 바와 같이 정부에서의 정보보호는 점차 중요성이 가중되고 있으나, 이에 따라 정보보호와 관련한 연구는 변화를 확인할 수 있는 시계열적 분석이나 이로 인한 효과 및 성과 등을 확인할 수 있는 연구는 부족했다. 따라서 본 연구는 정부차원에서 과거부터 현재에 이르기까지 정보보호와 관련한 전반적인 현황과 인식을 변화의 관점에서 추적하고자 하였다.

우선, 일반 국민과 밀접한 위치에 있는 지방자치단체에서의 정보보호는 국가차원에서의 정보보호를 위한 체계화된 관리의 시발점이자 연결고리이기 때문에(서진완 외, 2008) 지방자치단체를 분석단위로 선정하였다. 그러나 우리나라의 경우 지방자치제를 시

〈표 2〉 지방자치단체의 정보보호 현황 및 인식 변화 분석을 위한 분석틀

분석기준	분석내용
법·제도 개선 변화	- 정보보호 관계법령의 제·개정 - 지역정보화 조례 제·개정
예산·인력 확보 변화	- 정보보호 예산 변화 - 인천광역시 정보보호 예산·인력의 변화
담당공무원 인식 변화	- 정보보호 담당 공무원들의 정보보호 현실과 업무 태도 - 정보보호 강화를 위한 우선순위 및 평가

행하고 있지만 대부분의 정책이 자치단체의 상황에 맞게 유동적으로 변화하기 보다는 중앙정부의 정책 결정에 의존하는 경우가 많기 때문에 지방자치단체의 정보보호 변화에 연구 비중을 두면서 동시에 중앙정부의 변화 역시 살펴볼 필요가 있다.

또한, 선행연구 분석에 근거하여 기존 연구들이 개선방안으로 공통되게 제시한 제도의 재정비, 인력과 예산의 확충, 인식의 개선이라는 세 측면을 분석 기준으로 삼았다. 이는 기존의 연구들이 지속적으로 지적하고 언급했던 부분들이 실제 현실에서 긍정적 변화로 이어졌는가를 확인하기 매우 적합한 요소이며, 기존 연구들의 실효성을 판단하기에도 적합하다고 보여 진다.

본 연구는 메타분석과 시계열 분석에 기초하고 있다. 따라서 각 분석내용은 시계열 분석이 가능하고, 자료의 객관성을 확보 할 수 있다고 판단되는 항목으로 구성하여 자료를 수집하였다. 객관적 통계자료 및 보고서, 선행연구 등을 기초로 자료를 재구성 하여 분석을 진행하였으나, 자료와 분석의 객관성을 더하기 위해 인천광역시와 인천광역시의 각 기초자치단체에서 정보보호 업무를 실제로 담당하고 있는 담당

공무원들과의 인터뷰 방식을 병행하였다.⁴⁾

우선, 법·제도의 개선을 확인하기 위하여 중앙정부차원에서는 정보보호 관계 법령의 제·개정 현황을 살펴보았으며, 지방정부차원에서는 지역정보화조례의 제·개정 현황을 살펴보았다. 두 번째로, 예산과 인력의 확보를 확인하기 위하여 중앙정부차원에서는 정보보호 예산의 변화를, 지방정부차원에서는 인천광역시의 예산·인력의 변화 현황을 살펴보았다. 끝으로 담당공무원의 인식 변화를 확인하기 위해서는 정보보호 담당 공무원들의 인식을 정보보호 현실에 대한 인식 및 업무 태도, 그리고 정보보호 강화를 위한 우선순위 및 평가라는 두 측면으로 보다 세분화하여 살펴보았다.

IV. 정보보호의 현황 및 인식의 변화

1. 법·제도의 개선

한국인터넷진흥원에 따르면, 현재 정보보호와 관련한 관계법령은 「정보통신망이용촉진및정보보호등에관한법률」을 포함하여 총 5개, 개인정보보호와 관

4) 본 연구는 대민서비스의 접점이라고 할 수 있는 시청 및 기초자치단체에서 실제 정보보호 업무를 담당하는 담당자들의 인터뷰를 통해 현황 정보 및 인식 내용의 객관성을 확보하고자 하였다. 모든 지방자치단체 중에 정보보호와 관련한 연구를 하기 위해서는 인구 수, 연령, 도시화 정도 등의 요소들이 고려되어야 할 것으로 판단되었으며, 광역자치단체가 시 단위로 이루어진 곳이 본 연구를 위한 분석 단위로 적절하다고 판단하였다. 특별시를 포함하여 총 7개의 광역시 중 조사의 편의와 자료수집의 용의성을 고려하여 인터뷰 대상자를 인천광역시청 및 인천광역시 기초자치단체의 담당공무원으로 한정하였다. 인터뷰 조사는 2015년 9월 16일부터 9월 25일까지 인천광역시의 기초자치단체를 전수조사 하였다. 인천광역시의 시청 및 기초자치단체는 총 11개 기관에 계직 중인 정보보호담당자를 대상으로 직접 방문 또는 전화 인터뷰를 통해 이루어졌다.

〈표 3〉 지방자치단체 지역정보화조례 제정 현황

(단위: 개)

	2010년	2011년	2012년	2013년	2014년	2015년
자치구	21	21	18	32	24	6
누적	21	42	60	92	116	122

출처: 자치법규정보시스템(www.elis.go.kr) 2015년 3월 30일 기준

련한 관계법령은 「개인정보보호법」을 포함하여 총 3개의 법령이 있다(한국인터넷진흥원 홈페이지, 2015). 제도적 측면에서 정보보호와 관련한 변화를 확인할 수 있는 법률로서 「정보통신망이용촉진 및 정보보호 등에 관한 법률」과 「개인정보보호법」, 그리고 「국가정보화기본법」이 있다. 우선, 「정보통신망이용촉진 및 정보보호 등에 관한 법률」은 2001년 1월 전면 개정되어 같은 해 7월 공포되었다. 이 법률은 기존의 「정보통신망이용촉진에 관한 법률」에서 정보보호와 관련한 제도적 부분이 대폭 개선되었으며, 이후 정보보호 등의 내용을 포함하는 다양한 정보화 관련 법령에 영향을 주었다. 「정보통신기반 보호법」이 같은 해에 제정·공포 되었고, 「전자서명법」은 1997년 2월 제정되었으나, 「정보통신망이용촉진 및 정보보호 등에 관한 법률」의 제정과 함께 전면 개정되었다.

다음으로 「개인정보보호법」은 2011년 3월 제정되어 같은 해 9월 시행되었다. 이 법률은 다른 법률에 비해 법령제정이 가장 최근에 이루어졌다. 제정이유에서 최근 개인정보의 유출, 오·남용 등 개인정보 침해 사례가 지속적으로 발생함에 따라 피해 구제를 강화하고 개인정보에 대한 권리와 이익을 보장한다는 뜻을 밝혀, 2000년대 이후부터 발생한 각종 정보유출, DDos 공격, 해킹 등과 같은 일련의 사건들이 법제정에 영향을 준 결과이다.

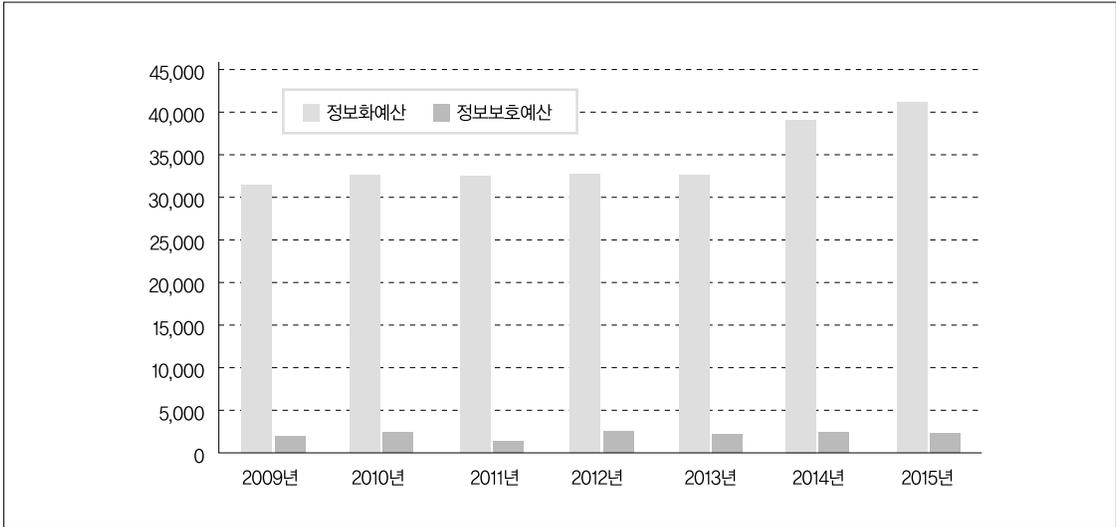
끝으로, 「국가정보화기본법」은 1995년 제정된 「정보화촉진기본법」이 2009년 5월에 전면 개정되면서

법명이 변경된 것인데, 정보화를 촉진하는 단계에서 활용하는 단계로 환경이 변화하고 자치단체로 정보화의 영역이 분산되어 전면개정을 시행하였다. 전면 개정과 함께 정보이용의 안전성과 신뢰성을 보장하는 측면을 내용에 포함시켰다. 이 법은 지방자치단체가 제정한 「지역정보화조례」의 근간이 되는 법이다.

지방자치단체의 경우, 「지역정보화조례」를 통해 정보보호를 제도화하고 있는데, 우리나라의 지방자치단체는 총 227개로 이중 「지역정보화조례」가 있는 지방자치단체는 총 122개이고, 64곳의 지방자치단체는 「지역정보화촉진조례」의 형태로만 제정되어 있다.⁵⁾ 지역정보화조례와 관련하여, 지역정보화조례가 있는 122개의 지방자치단체의 조례제정시기를 살펴보면, 〈표 3〉에서 나타난 바와 같이 2010년 4월 이후부터 시작하여 2015년 3월 현재까지 연도별로 조례 제정 상황을 확인할 수 있다.

지방자치단체의 「지역정보화조례」의 내용을 살펴보면, 지방자치단체 간의 차이보다는 대체적으로 동일하게 구성되어 있음을 확인할 수 있다. 특히, 「지역정보화조례」의 내용 중, 정보보호와 관련한 내용 역시 대체적으로 동일하였는데 여러 지방자치단체들의 조문을 비교해보더라도, 정보보호에 해당하는 조문의 내용은 ‘전산실 출입 권한 등 정보자원에 대한 물리적 보안’, ‘행정정보 및 개인정보의 수집, 처리, 활용, 폐기 등 전 단계에 걸친 관리’, ‘정보유출 방지를 위한 감독 체계’, ‘그 밖에 정보보호를 위하여 필요한 사항’ 등으로 동일하게 구성되어 있었다. 이러

5) 행정자치부 홈페이지 2013년 지방자치단체 행정구역 및 인구현황자료를 토대로 하였으며, 법의 제·개정 내용은 모두 법제처 홈페이지(www.moleg.go.kr/)를 참조하였다.



출처: 한국정보화진흥원(2013) "국가정보화 투자의 특성과 시사점"; 미래창조과학부 보도자료(2014, 2015) 재구성.

〈그림 1〉 연도별 정보화 예산 및 정보보호 예산 현황

한 내용은 2010년을 전후로 조례가 전면 개정되면서 추가되거나 개정된 경우가 많았다.

이는 지역정보화조례가 「국가정보화기본법」에 위임된 사항을 조례로 재정한 것으로, 자치단체 필요에 의한 조례개정이 아니라 중앙정부의 정책 추진에 따라 지방자치단체가 영향을 받았기 때문이다. 또한 2015년 3월 현재, 지방자치단체 중에서 122개의 자치단체만이 조례를 제정하였고, 촉진조례를 제정한 64개의 지방자치단체를 포함한다 하더라도 여전히 41개의 지방자치단체들은 정보보호와 관련한 조례를 아직 제정하지 않은 것으로 나타났다.

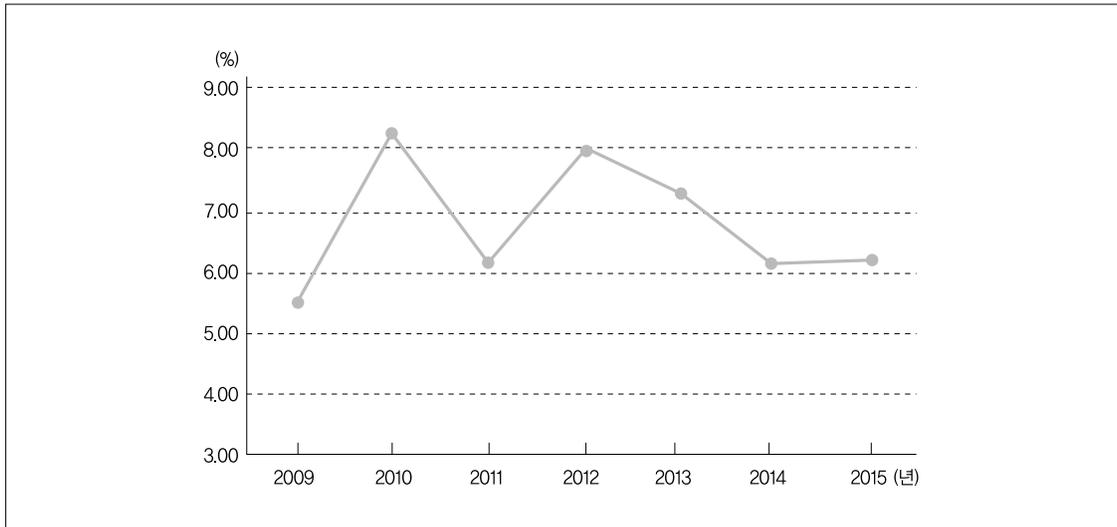
2. 예산 및 인력 확보

1) 예산의 변화

한국정보화진흥원(2013)과 미래창조과학부의 자료(2015)에 따르면, 중앙정부에서의 정보화 예산은 2009년 31,378억 원에서 2010년 32,869억 원, 2011년 32,897억 원, 2012년 33,053억 원, 2013년 32,967억 원, 2014년 39,404억 원, 그리고 올해 처

음으로 4조억 원을 넘어서며 증가추세를 보이고 있다. 이에 반해 정보보호 예산의 경우 2009년 1,742억 원, 2010년 2,702억 원, 2011년 2,034억 원, 2012년 2,633억 원, 2013년 2,402억 원, 2014년 2,460억 원, 그리고 2015년 2,543억 원으로 조사되었다. 이처럼 정보화 예산은 꾸준히 증가하지만, 정보보호 예산은 일정한 추세를 보이지 않고 있으며, 3조원 이상이 편성되고 있는 정보화예산에서 평균 6~8% 수준을 유지하고 있을 뿐이다.

최근 정부는 정보보호를 지속적으로 강화하기 위하여 새로운 사업 개발 및 인터넷 침해대응센터 이중화를 본격적으로 추진하겠다고 발표(미래창조과학부, 2015)한 점에 미루어 향후 정보보호 관련 예산의 증가를 기대할 수는 있다. 그러나 현재까지 전체 정보화 예산에서 정보보호 예산이 차지하는 비율을 보면 특별한 계기가 아닌 한 여전히 기존과 비슷한 수준에 머물러 있을 가능성이 높다. 〈그림 2〉와 같이, 지금까지 정보보호 예산의 비율이 일시적으로 증가하는 시기를 추적해보면, 7.7 DDos 사건이 발생하자 이듬해 정보보호 예산이 꺾충 뛰었지만, 1년 뒤인



출처: 한국정보화진흥원(2013) “국가정보화 투자의 특성과 시사점” ; 미래창조과학부 보도자료(2014,2015) 재구성.

〈그림 2〉 연도별 정보보호 예산 비율 추이

2011년 2,034억 원으로 예산이 대폭 줄었고, 2011년 3.4 DDos 공격과 농협전산시스템 마비사건 등이 발생하자 다시 예산이 2%정도 증가 했다는 것으로 볼 때, 정보보호와 관련한 예산은 장기적 안목으로 관리해야 하는 대상임에도 불구하고 일시적인 관심으로 임시방편식의 예산편성이 이루어지고 있다.⁶⁾

지방자치단체에서는 정보보호예산을 따로 편성하지 않고, 정보화예산 중 일부를 정보보호 예산으로 활용하고 있다. 지방자치단체의 정보화 예산과 정보보호 예산의 비율이 중앙정부의 비율과는 또 다른 모습을 띄는 것은 주목할 만한 특징이다. <표 4>에서 나타난 결과를 보면, 인천광역시의 각 구별 정보화 및 정보보호 예산은 연도별로, 구별로 매우 차이가 크고, 정보보호 예산 편성의 비율도 적게는 1%에서 많게는 26%까지 편차가 매우 크다. 예산 편성의 내용을 살펴보면 대체적으로 정보보호 예산이 많이 편성될 때는 보안시스템의 교체와 같은 시설 및 시스템

의 유지·보수를 위한 기술지원적 예산편성인 경우가 대부분이었다(행정자치부, 2014).

2) 인력의 확보

정보보호 인력의 경우, 정보보호 전담 인력의 비율은 대체적으로 평균 17%정도이다. 2008년 자료에 따르면, 정보화담당 인력 대비 정보보호 인력의 비율은 10.8%였다(서진완 외, 2008). 2008년과 비교 하였을 때, 정보보호의 인력 비율은 약 7%가량 증가한 것으로 보인다. 그러나 중요한 것은 정보화 인력 대비 정보보호의 인력의 비중이 아니라 실제 정보보호 업무를 하는 인력의 수가 중요하다. 아래 <표5>에서 확인할 수 있듯이 서울시의 경우 정보보호 인력이 여느 시·도 보다 월등하게 많지만, 정보화 인력이 많은 이유로 비율이 낮게 측정된다. 따라서 정보보호 전담 인력의 인원수로만 인력을 확인한다면, 정보보호 전담 조직을 구축하고 있는 서울시, 인천시, 경기도를

6) Ahnlab 최신 보안뉴스 2014.2.10 (2015.3.30검색)

(http://www.ahnlab.co.kr/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=1&seq=22149)

〈표 4〉 인천시 각 구별 정보보호 예산현황

(단위: 백만 원, %)

지자체 예산		A구	B구	C구	D구	E구	F구	G구	H구	I군	J군
2009년	정보화총예산	837	598	1,928	1,635	1,555	1,477	886	1,383	1,504	645
	정보보호예산	204	21	11	48	298	176	25	121	239	80
	비율	24	4	1	3	19	12	3	9	16	12
2010년	정보화총예산	1,061	533	1,530	1,949	1,054	983	608	1,245	1,311	833
	정보보호예산	250	14	81	100	9	27	23	300	90	98
	비율	24	3	5	5	1	3	4	24	7	12
2011년	정보화총예산	800	979	1,365	1,400	1,439	2,065	535	1,114	1,660	518
	정보보호예산	117	73	20	178	96	17	52	193	214	48
	비율	15	7	1	13	7	1	10	17	13	9
2012년	정보화총예산	519	1,380	1,009	1,237	1,722	1,007	862	985	1,208	822
	정보보호예산	134	46	23	159	123	82	76	185	451	66
	비율	26	3	2	13	7	8	9	19	37	8
2013년	정보화총예산	2,009	1,744	1,041	1,108	2,696	1,694	664	1,835	1,006	932
	정보보호예산	231	240	67	169	203	181	31	146	145	166
	비율	11	13	7	15	8	11	5	8	14	18
계	정보화총예산	7,141	6,917	10,033	10,436	10,644	9,548	4,884	8,695	8,737	5,756
	정보보호예산	1,081	524	222	909	751	620	421	1,131	1,264	543
	비율	15.1	7.6	2.2	8.7	7.1	6.5	8.6	13.0	14.5	9.4

출처: 인천광역시 구·구 행정내부자료.

제외한 대부분의 시·도가 5-8명 정도의 정보보호 인력을 확보하고 있는 것으로 나타났다.

서진완 외(2008)의 연구 자료와 현재의 자료를 비교해 보면 정보보호 인력이 증가한 것으로 보여질 수 있다. 하지만, 몇몇 정보화 전담 조직을 구성한 지방자치단체를 제외하고는 여전히 대부분의 지방자치단체들은 기획조정실 산하에 정보담당부서를 둔 채, 업무 내용의 구분만을 통해 정보보호 담당자를 지정하고 있는 실정이다. 더욱이 구 단위의 기초자치단체의 경우는 그 변화가 더욱 미미하다. 실제로 인천광역시의 정보보호 담당자들을 인터뷰 한 결과, 인천광역시의 기초자치단체들은 정보보호 업무 담당자가 1명으로 지정되어 있으나, 담당자는 정보보호 업무 이외에도 다른 정보화 관련 업무 내지는 전산관련 업무를

병행하고 있기 때문에 정보보호 업무만을 따져본다면 담당자는 1명이 채 되지 않는다는 답변이 대부분이었다. 이를 수치화 해본다면 평균적으로 정보보호 업무 담당자는 약 0.5명 정도로 나타난다. 신영진(2009: 48)의 연구에서도 “273개 기관에서 개인정보보호담당자를 지정하고 있었으나, 대부분 다른 업무를 겸직하고 있어 전임인력이 필요한 실정이다.”라고 언급하고 있다. 즉, 2009년의 연구에서도 지적되었던 인력 문제는 현재에도 전혀 개선되지 않고 지속되고 있다는 것을 의미한다.

3. 담당 공무원의 정보보호 인식 변화

정보보호에 관한 선행연구를 통해 정보보호를 직

〈표 5〉 정보화 담당 및 정보보호 담당 인력의 변화

(단위: 명)

시도	정보화 전담인력		정보보호 전담인력/비중
	2010년	2015년	2015년
서울특별시	217	375	30 (8.0%)
부산광역시	59	32	8 (25.0%)
대구광역시	50	35	5 (14.3%)
인천광역시	52	63	22 (34.9%)
광주광역시	10	39	4 (10.3%)
대전광역시	38	43	5 (11.6%)
울산광역시	33	34	6 (17.6%)
경기도	33	66	28 (5-42.4%)
강원도	33	37	5 (13.5%)
충청북도	35	32	5 (15.6%)
충청남도	39	38	7 (18.4%)
전라북도	6	28	4 (14.3%)
전라남도	21	33	5 (15.2%)
경상북도	29	37	7 (18.9%)
경상남도	39	40	5 (12.5%)
제주특별자치도	22	21	2 (9.5%)

출처: 지역정보개발원(2010), 김구(2011), 각 시도청 홈페이지⁷⁾

접 담당하는 담당자들의 인식이 중요하다라는 것이 최근 논의되고 있다는 것을 확인할 수 있었다. 일반적으로 정보보호를 위한 방안은 기술적 방안과 법·제도적 방안에 주력한 것이 사실이나, 기술적 방안의 경우 보안기술 못지않게 해킹기술 역시 지속적으로 발전하고 있기 때문에 완벽한 대안이 될 수 없으며, 아무리 기술적으로 완벽하더라도 내부자에 의한 시스템 조작 및 개인정보 유출 등 인적요인으로 인한 문제는 기술적으로 차단하기 어렵다(윤상오, 2009). 더욱이 일반 국민의 개인정보 등과 관련한 행정처리를 담당하는 일선 공공기관에서 정보보호 담당자들의 정보보호에 대한 인식은 그 중요성을 더 한다고

할 수 있다(서진완 외, 2008).

1) 정보보호 현실에 대한 인식과 담당공무원의 업무 태도

정보보호와 관련한 담당공무원의 인식을 분석한 연구들을 시계열적으로 살펴보면 분석에 사용된 모든 논문에서 정보보호에 대한 중요성을 강조하면서, 연구시점에서 정보보호의 현실이 크게 나아지지 않고 있다는 점을 강조한 점에 주목할 필요가 있다. 그동안 인식 조사에서 나타난 공통점은 담당 공무원들 모두 정보보호 현실에 대한 심각성을 인식하고 있으며, 정보보호에 대해서도 대체적으로 변화가 필요하

7) 2010년의 자료는 한국지역정보개발원(2010)의 각 시도 본청 자료를 기준으로 하였다. 한국지역정보개발원 자료에 포함되지 않은 부산광역시와 대구광역시의 자료는 김구(2011)의 연구논문을 참고로 하였다. 그리고 2015년 자료의 경우 각 시도청 홈페이지에 올라와있는 자료를 토대로 재구성하였으며, 2015년 4월 29일 검색을 기준으로 하였다.

다고 생각하는 것으로 나타났다(변미리, 2004; 정진우, 2013; 행정자치부, 2014).

이러한 의견은 인터뷰에 응했던 모든 담당자들을 통해서도 동일하게 확인되었다. 특히, 과거와 현재의 정보보호 현실의 차이에 대해 대부분의 담당자들은 ‘과거에 비해 정보보호 현실이 더 심각해졌다’고 응답했으며, 이렇게 달라진 정보보호 현실의 심각성이 본인의 업무에도 영향을 주고 있음을 언급했다.

“정보보호는 예전보다 중요해졌고, 필요성도 높아졌다. 특히 정보보호 업무도 예전에는 방화벽 하나면 되던 시절이 있었지만, 지금은 그 안에서 일어나는 일을 일일이 모니터링도 해야 하고, 흐름을 보면서 문제가 무엇인지 문제의 원인이 무엇인지 등을 파악해야 한다. 동일한 정보보호 업무를 하더라도 예전보다 업무량도 많아지고, 업무 자체도 매우 세분화 되고 있다”

(인천광역시 B구 정보보호담당자)⁸⁾

한편, 기존 연구들에서 지적한 핵심적인 특징은 정보보호 담당자들의 수동적인 업무 태도로 요약된다. 정보보호 담당공무원들이 업무태도가 소극적으로 될 수밖에 없는 이유를 설명하면서 보안사고의 발생이나 정보보호와 관련한 이슈 보다는 상위기관의 지시라는 지적이 있었으며(행정자치부, 2014), 정보보호 정책결정자의 소극적인 자세도 현재의 상황을 가져온 원인으로 지적하기도 했다(변미리, 2004). 이와 관련하여 “직접 업무를 수행해야 하는 정보보호 담당자는 업무 부담과 책임감을 느끼게 되어 정보보호 업무를 보수적이며 수동적으로 접근하게 되는 경향이 있다”(행정자치부, 2014: 229)는 주장도 주목된다.

하지만, 실제 담당자들과의 인터뷰를 통해 확인한 결과 담당자들은 본인들의 업무 태도를 수동적으로 평가하지 않았다. 물론, 업무태도가 보안사고의 발생

이나 정보보호와 관련한 이슈 보다는 상위기관이나 상관의 지시에 더 많은 영향을 받기는 하지만, 그로 인해 업무가 수동적이지는 않다고 언급했다. C 기초자치단체 담당자는 이와 관련하여 “업무 자체의 책임성이 높은 편이다. 예를 들어 개인정보유출과 같은 정보보호 관련 사고가 발생할 경우, 1차적인 문제 원인은 이를 유출한 담당자의 책임이지만, 관리감독의 책임 역시 중요하기 때문에 책임감이 높다. 이것이 공무원들의 기피업무가 되는 원인이 되기도 하지만, 일단 업무를 맡게 되면 관리감독에 대한 면피를 위해 서라도 더욱 열심히 일을 하는 편이다.” 라고 이야기 하기도 하였으며, E 기초자치단체 담당자는 “다른 업무들에 비해 책임성이 높다는 것을 체감하고 있다. 그렇기 때문에 업무 자체가 매우 조심스럽고 뭔가 빠뜨리지는 않았는지, 놓친 부분이 있지는 않은지 하는 등 업무에 보다 신경을 많이 쓰게 된다.”고 언급하기도 하였다. 또한, A 기초자치단체 담당자는 “이전보다는 업무 태도가 적극적으로 변화했다.”라고도 언급하였다.

기존의 연구들에서 담당공무원의 업무태도를 수동적이라고 여겼던 이유는 적극적 문제 해결을 위한 노력이 부족했기 때문이었다. 하지만 실제 담당 공무원들을 인터뷰 했을 때, 담당자들은 본인들이 업무를 수동적으로 하는 것이 아니라고 여겼다. 그러나 업무의 우선순위를 묻는 질문에서 “현재 문제가 발생하거나 긴급하게 처리해야 하는 업무가 아니기 때문에 업무 우선순위에서 밀리는 경우가 있다”는 답변을 하거나, 혹은 “기초자치단체에서는 정보보안 사고가 없기 때문에, 직접적인 문제가 발생해야 변화가 생긴다.”는 언급 등을 미루어 본다면 정보보호 업무가 예방차원에서의 적극적 노력이 이루어지고 있지 않다는 것을 짐작할 수 있다.

또한, 기존 연구들을 통해 확인되는 또 다른 특징은 담당공무원들의 업무 태도에 대한 인식과 실제 정

8) 본 연구의 인터뷰 내용은 각 기초자치단체 정보보호 담당자들의 요청에 따라 익명으로 처리함.

보보호 현실간의 차이가 나타난다는 점이다. 이미정 외(2010: 468)의 연구에서는 “정보보호와 관련한 이해나 지식은 일정 정도 갖추었으나 이것이 행태로까지 연결되는 정보보호의 내재화에는 아직 이르지 못했다는 것을 알 수 있다”고 분석하고 있으며, 행정자치부(2014: 225)의 보고서에서는 “보안점검 및 평가 항목에서 정보보호 수준이 높은 편으로 평가되고 있지만 현황자료와 비교해 보았을 때 현실과 차이가 있는 인식으로 판단된다”고 언급하고 있다. 실제 인터뷰에서도 본인들의 업무에 대한 태도는 적극적인 편이지만, 현실적으로 업무에 집중하기 어려운 상황들 때문에 정보보호 업무에만 치중해서 업무를 할 수는 없다는 반응들이 대부분이었다. 즉, 정보보호 담당 공무원들은 머리로는 필요성이나 상황의 심각성을 어느 정도 인지하고 있으나, 실제 행동으로까지 연결되지 못하고 있다는 의미가 되며, 과거부터 현재까지 비교해 보더라도 이런 상황이 반복되고 있다는 것을 확인할 수 있다.

2) 정보보호 강화를 위한 우선순위 및 평가

정보보호 담당자들의 인식조사를 분석한 기존의 연구결과를 토대로, 정보보호 강화를 위한 우선순위를 정리해 보면, 행정적 지원과 담당 공무원들의 인식 및 태도 변화가 거의 비슷한 수준으로 중요함을 확인할 수 있었다.

우선, 행정적 지원이라는 측면에서 이를 보다 구체적으로 살펴보면, 담당공무원들은 정보보호를 위해 기술적 지원보다는 독립적인 기구를 설치하거나 운영하고, 전문적 인력을 확보하며, 정보보호 예산을 증액하는 등 행정적 지원이 필요하다고 응답했다(변미리, 2004; 이미정 외, 2010; 정진우, 2013; 행정자치부, 2014 재구성). 실제 담당자들의 인터뷰에서도 인력부족과 예산지원의 문제는 모든 기초자치단체의 담당자들이 지적한 부분이다. 특히, 기초자치단체의 정보보호 담당 인력은 평균적으로 0.4~0.5명 정도에 해당한다. 물론 이러한 수치는 담당자들이 체

감하는 정도에 따라 기초자치단체별로 차이를 보이고 있지만, 중요한 점은 정보보호를 담당하는 인력이 채 1명이 되지 않는다는 점이었다. 시정을 제외한 모든 기초자치단체에서는 정보보호 업무 이외에도 홈페이지 관리나 전산업무 등과 같은 업무를 병행하고 있었으며, 정보보호 업무량도 매년 증가하고 있다고 이야기 했다.

다음으로, 담당공무원들의 인식 및 태도의 변화라는 측면에서 정보보호 강화를 위한 방안들을 보다 구체적으로 살펴보면, 소극적이고 책임회피적인 담당자들의 태도 개선과 개인정보보호 및 정보보호에 대한 인식 변화의 확산이 필요하다고 응답했다(변미리, 2004; 정진우, 2013). 이미정 외(2010:471)의 연구에서도 정보보호에 대한 전반적인 문제점과 대응방안에 대해서는 이미 숙지하고 있지만, 실질적인 형태로 외면화 되는데 현재 정보보호 업무 담당자들의 역량이 미치지 못한다고 언급하면서, 담당공무원들의 인식이 정보보호 강화를 위한 가장 중요한 요소임을 강조한 바 있다. 사람들이 위협에 대해 어떻게 생각하고 있는가에 따라서 ‘위험사회’의 문제에 대한 대응은 크게 달라질 수 있다는 사실을 상기할 때(홍성태, 2014), 단순히 문제를 알고 있다고만 해서 문제가 해결되는 것은 아니다.

담당공무원들의 인식 및 태도 개선이라는 측면에서 짚고 넘어가야 할 부분은 정보보호 담당공무원들이 자신의 업무 자체를 대하는 태도인데, 기초자치단체의 담당자들 대부분이 자신의 업무에 대한 보람을 잘 느끼지 못하고 있는 것으로 확인되었다. 담당자들이 정보보호 업무 자체의 낮은 만족도는 업무를 적극적으로 능동적으로 대하는 태도를 갖는다는 것을 사실상 어렵게 만드는 원인이 된다.

“정보보호 업무는 사고가 터지지 않으면 잘해봐야 본전인 업무이다. 사고가 터지면 담당자가 아무리 본인의 업무를 잘했더라도 피해를 입게 된다. 그렇기 때문에 업무에서 문제가 생기지 않도록 최선을 다해 일을 하지만, 조직에서

는 이러한 부분을 전혀 반영해주지 않는다. 업무는 점차 중요해지고 이에 따라 업무량도 점차 증가하고 있다. 과거에는 부각되지 않았던 부분들, 예를 들면 무선네트워크와 같은 부분들도 부각이 되면서 업무량은 점차 많아지고 있어 업무를 잘 하고 싶어도 잘 하기 어려운 현실이 되어가고 있다. 그러나 늘어나는 업무만큼 인력이나 예산이 고려되지 않아 업무를 하는데 보람이 없는 것이 사실이다.”

(인전광역시 D구 정보보호담당자)

결국 정보보호를 담당하고 있는 공무원들은 정보보호의 중요성이나 필요성에는 전적으로 동의를 하지만, 업무를 대하는 태도가 그다지 능동적이라고 보기 어려웠으며, 정보보호를 강화하기 위해서는 행정적 지원이 필수적으로 뒷받침 되어야 하며, 이와 함께 담당공무원인 자신들의 업무를 대하는 태도가 보다 긍정적으로 변해야 한다는 것을 확인할 수 있었다.

V. 결론 및 제언

기술의 발전은 곧 위험의 증가를 야기하는 측면이 있다. 정보화사회가 도래한 이후, ICT 관련 기술은 매우 빠르게 발전하였으나, 정보화의 역기능으로 오래전부터 강조되어 왔던 정보보호의 중요성은 여전히 강조되고 있다. 더욱이 막대한 양의 공공정보를 활용하는 국가기관에서의 정보보호는 그 중요성이 강조되고 있지만(서진완 외, 2008), 여전히 정부는 정보보호와 관련한 사건들에 노출되고 있는 것도 사실이다. 이에 본 연구에서는 그간 정부와 학계의 노력이 현장에서 긍정적 변화를 가져왔는지를 지방자치단체를 중심으로 제도적 측면, 예산과 인력적 측면, 담당공무원들의 인식 측면에서 그 변화를 살펴보았다.

분석결과를 요약하면 제도적 측면이나 예산 및 인력이라는 측면에서 중앙정부의 변화는 확인할 수 있었으나, 지방자치단체에서는 변화가 나타난다고 보

기 어려웠다. 그러나 중앙정부의 변화도 정보보호와 관련한 문제가 발생한 후에 기존 보다 강화될 뿐 지속적으로 강화가 확대된다고 보기도 어려웠다. 또한 지방자치단체에서 업무를 하는 정보보호 담당 공무원들의 정보보호에 대한 중요성이나 심각성의 인식은 높아졌으나 업무 자체에 대한 인식이나 태도는 부정적이거나 수동적으로, 과거와 비교해 변화하지 않았음을 확인할 수 있었다. 즉, 이러한 결과는 기존 정부의 노력이나 학계의 연구가 실제로 실효성을 발휘하지 못하고 있음을 시사한다. 본 연구의 분석을 통해 그 원인을 다음과 같이 추론할 수 있다.

첫째, 기존 정부의 정보보호 정책은 실제 정보보호가 갖는 중요성에 비해 그 우선순위 높지 않다. 정보화 사회에서 정보보호는 건물의 기초공사와 같은 것이다. 그러나 현재 시행되고 있는 정보보호와 관련한 중앙정부 및 지방자치단체의 정책은 정보보호에 대한 기본적인 이해조차 제대로 이루어지지 않은 형태로 밖에는 볼 수 없다. 일례로, 우리나라의 정보보호 정책이나 예산이 강화되는 추세를 볼 때, 사고가 일어났을 때만 잠시 논의가 될 뿐 그 다음으로의 발전이 이루어지지 못하는 경우가 많았으며, 지방자치단체의 조례 제정도 중앙정부의 제도 변화에 따라 이루어 질 뿐이었다.

둘째, 정보보호 업무는 복잡하고 종합적인 성격임에도 불구하고 여전히 기술적 측면에서만 이를 보는 경향이 있다. 대부분의 기초자치단체는 정보화 부서 내지는 전산부서에서 정보보호 업무를 담당하고 있다. 기존 연구들을 통해서 정보보호가 단순히 기술적 보안을 넘어 정보의 관리와 감독 등의 업무도 중요하다는 것을 오랫동안 언급하고 있음에도, 여전히 변화하지 않고 있는 것이다. 조직 내부적으로 볼 때도 정보보호 업무는 직원들에게 일정 정도의 강제성을 행사해야 하는 경우도 존재하지만, 이를 뒷받침 할 만한 권한이 담당직원에게는 없다.⁹⁾

9) 이러한 이유로 인터뷰 대상자 중 일부 담당공무원은 정보보호업무가 감사부서로 이전되어야 한다는 의견을 제시하기도 하였다.

따라서 정부는 정보보호를 위한 기존의 접근을 보완하는 차원이 아닌 완전히 새로운 차원에서 정책적 접근을 모색할 필요가 있다. 예를 들어, 분석에서 언급한 바와 같이 담당자의 입장에서 정보보호와 그 외 업무의 업무 상충이 발생했을 경우 정보보호업무가 업무 우선순위에서 밀리지 않기 위해서는 단순히 이를 보완하는 차원을 넘어 새로운 업무의 재설계(re-Design)가 필요하다. 즉, 정보보호를 정보화 사회의 기본적인 토대로 이해하고 이에 맞는 새로운 정책을 강구할 필요가 있는 것이다.

본 연구는 몇 가지 한계점을 가지고 있다. 우선, 본 연구는 기존의 정책과 연구들의 실효성에 대한 문제제기 가능성에 답을 하는 정도에서 그치고 있다. 또한 기존의 연구 자료를 시계열적으로 분석하는 과정에서 한계에 직면하였다. 서로 다른 기준에 따라 이루어진 기존 연구 자료를 토대로 동일한 기준으로 분석하는 데 나타나는 필연적인 결과로 볼 수 있다. 끝으로, 인천광역시와 그 자치구만을 대상으로 분석이 이루어졌기 때문에 분석 내용을 일반화하기에는 다소 문제가 있을 수 있다. 다만, 본 연구는 기존의 연구결과를 토대로 정보보호가 우리사회의 사회 안정을 위한 중요한 요소이며 장기적인 안목으로 관리되어야 하는 투자의 대상이며 관리의 대상으로 정책적인 측면에서 우선적으로 고려되어야 한다는 점에서 이루어진 시도로 평가되었으면 한다. 또한, 본 연구의 한계와 제언을 토대로 정책적·관리적 차원에서 보다 실효성 있는 후속 연구가 필요하다.

■ 참고문헌

- 가천대학교 산학협력단 (2012). “빅데이터 환경에서 개인 정보보호 강화를 위한 법제도적 대책방안 연구.” 「개인정보보호위원회 연구보고서」
- 강휘원 (2000). “정보프라이버시 보호를 위한 자율규제: 한계와 정책적 시사.” 「한국행정학보」, 34(3): 111-128.
- 개인정보보호위원회 (2014). 「2013년도 개인정보보호 연구보고서」
- 개인정보보호위원회 (2012). 「빅데이터 환경에서 개인정보보호 강화를 위한 법제도적 대책방안 연구」.
- 김구 (2011). “지방정부의 정보화 전담조직과 전담조직의 예산 비교 분석: 광역자치단체를 중심으로.” 「한국지역정보학회지」, 14(2): 57~83.
- 김동욱·성욱준 (2012a). “공공부문 정보보호인력의 직군 이탈의도에 관한 연구.” 「사회과학연구」, 28(2): 1-24.
- 김동욱·성욱준 (2012b). “스마트시대 정보보호정책에 관한 연구.” 「정보보호학회논문지」, 22(4): 883-899.
- 김성태 (2010). 「신 정보정책론: 이론과 전략」. 파주: 법문사
- 김지수·김종배·신용태 (2012). “조직내 정보보호최고책임자(CISO)의 역할인식이 정보보호성과에 미치는 영향에 관한 연구.” 「경영컨설팅연구」, 12(4): 21-34.
- 김철완·이민영 (2000). “지방자치단체의 정보보호 현황 분석.” 「한국행정연구」, 17(1): 221-245
- 문신용 (2003). 「전자정부 추진에 따른 공공기관의 개인정보보호 제고방안」. 한국행정연구원 연구보고서.
- 문신용·윤기찬 (2004). “공공기관의 개인정보 침해사례 분석의 함의 및 과제.” 「한국행정연구」, 13(4): 210-249.
- 미래창조과학부(2014) “국가기관·지자체, ICT를 활용한 창조경제 실현에 박차” 3월 10일. http://www.mile창조과학부.org/www/brd/m_211/view.do?seq=1441#contents_wrap (검색일: 2015.06.15.)
- 미래창조과학부(2015) “국가기관·지자체, 올해 정보화에 5조 2,094억원 투자” 1월 22일 <http://www.msip.go.kr/web/msipContents/contentsView.do?catelD=mssw311&artId=1247090> (검색일: 2015.06.15.)
- 박희봉·이희창·조연상 (2003). “우리나라 정부신뢰 특성 및 영향 요인 분석.” 「한국행정학보」, 37(3): 45-66.
- 방민석·오철호 (2014). “개인정보 연구동향과 과제.” 「정보화정책」, 21(1): 3-16.
- 법제처 홈페이지 www.moleg.go.kr
- 변미리 (2004). 「서울시 전자정부의 개인정보보호에 관한 연구」. 서울시정개발연구원 연구보고서.

- 서진완·이미정 (2008). “지방자치단체의 정보보호 현황 분석.” 「한국행정연구」, 17(1): 221-245
- 신영진·김성태 (2004). “지방자치단체의 정보보호 현황 분석.” 「한국행정연구」, 17(1): 221-245
- 신영진 (2008). “공공기관의 CCTV도입에 따른 개인정보 보호에 관한 연구.” 「한국지역정보화학회지」, 11(2): 1-21
- 신영진 (2009). “우리나라 개인정보보호수준의 개선방안에 관한 연구 : 중앙행정기관과 지방자치단체의 개인정보관리를 중심으로.” 「정보화정책」, 16(1): 41-53
- 신영진 (2010). “유비쿼터스 사회에서의 국가정보보호에 관한 연구: 미래예측기법을 통한 정보보호 정책 과제를 중심으로.” 「한국지역정보화학회지」, 13(3): 65-90.
- 신진 (2012). “사이버공격의 국가 경제적 손실분석-보이스피싱을 중심으로.” 「한국정보통신학회논문지」, 16(11): 1-6.
- 신진 (2013). “사이버정보보호의 경제적 효과분석-국가적 피해액 산전을 중심으로.” 「정보보호학회논문지」, 23(1): 89-96
- 연합뉴스(2012) “안랩 ‘올해 정치적 목적 해킹·디도스 늘어날 것’” 1월 2일. <http://www.yonhapnews.co.kr/bulletin/2012/01/02/0200000000AKR20120102068600017.HTML>(검색일: 2015.04.20).
- 오길영 (2005). “개인정보보호를 위한 RFID 규제에 관한 연구.” 「정보화정책」, 12(2): 47-69.
- 윤상오 (2009). “전자정부 구현을 위한 개인정보보호 정책에 관한 연구: 정부신뢰 구축의 관점에서.” 「한국지역정보화학회지」, 12(2): 1-29.
- 이동규·민연경 (2014). “정부위기 이후, 재난안전인식이 정부신뢰에 미치는 영향: 세월호 참사를 중심으로.” 「한국정책학회 동계학술발표논문집」, 2014. 1150-1168
- 이미정·이선중 (2010). “지방공무원의 정보보호 인식 및 행태에 관한 연구.” 「한국사회와 행정연구」, 20(4): 453-478.
- 이자성 (2008). “한국지방정부의 개인정보보호 제도화에 관한 연구: 우리나라·일본·국제기구의 법률을 중심으로.” 「한국지역정보화학회지」, 11(4): 81-108
- 이향수 (2008). “개인정보보호에의 관심과 대응.” 「정책 분석평가학회보」, 18(2): 205-230
- 자치법규정보시스템 www.elis.go.kr
- 정진우 (2013). “지방공무원과 행정인턴의 개인정보보호 인식 비교연구.” 「한국지역정보화학회지」, 16(4): 55-109.
- 한국방송통신전파진흥원 (2013). 「방송통신기술 이슈&전망」. 제23호.
- 한국인터넷진흥원 (2008). 정보보호관리체계 교육자료 <https://www.kisa.or.kr/jsp/common/libraryDownload.jsp?folder=012146>(검색일: 2015.04.30)
- 한국인터넷진흥원 (2013). 「국가정보보호백서」
- 한국인터넷진흥원 (2015). 「INTERNET & SECURITY FOCUS」 2015년 1월호. “인터넷 및 정보보호 10대 산업이슈 전망”
- 한국전산원 (2004). 「전자정부시대 개인정보보호법제정립방안 연구」
- 한국정보보호진흥원 (2005). 일본의 차세대 정보보호 정책방향과 최근 동향, 「정책기획」, 5(5)
- 한국정보화학진흥원 (2007). “유비쿼터스사회의 진전에 따른 부작용 전망” 「유비쿼터스사회연구시리즈」 34호.
- 한국정보화학진흥원 (2012). 「2012 국가정보화백서」
- 한국정보화학진흥원 (2013a). 「2013 국가정보화백서」
- 한국정보화학진흥원 (2013b). “국가정보화 투자의 특성과 시사점” 「정책연구」 2013-07.
- 한국지역정보개발원 (2009) 「자치단체 정보화 조직 및 인력 운용개선방안 연구」.
- 한국지역정보개발원 (2012). “2012년 행정기관의 정보화 사업 추진 전망” 「지역정보화 동향분석」 제1호.
- 한국정보통신기술협회 홈페이지 www.tta.or.kr
- 행정자치부 (2014). “정보화담당공무원의 정보보호 인식 분석 및 정책방향 연구” 「제31회 지방행정정보화 연찬회 시도별 연구보고서」. 181-252.
- 홍성태 (2014) 「위험사회를 진단한다: 사고사회를 넘어 안전사회로」. 서울: 아로파
- 황창호, 김태형, 문명재 (2015). “정부신뢰에 영향을 미치는 요인에 대한 연구-정책홍보, 정책수단, 정책산출에 대한 국민만족도를 중심으로” 「한국지방정부학회 학술대회자료집」. 545-561.
- AhnLab 보안뉴스(2014) “국가 정보보호예산 2600억… 대형 사고에도 전년비 7.7%만 증가” 2월 10일. http://www.ahnlab.co.kr/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=1&seq=22149(검색일: 2015.3.30).
- Beck Ulrich 저·홍성태 역 (2006). 「위험사회」. 서울: 새물결

- CSI/FBI 2000 Computer Crime and Security Survey
<http://www-tc.pbs.org/wgbh/pages/frontline/shows/hackers/risks/csi-fbi2000.pdf> (검색일: 2015.05.20).
- ETNnews (2012), “진화하는 DDos 공격, 그 끝은 어디인가?” 5월 28일. http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menu_dist=2&seq=19421 (검색일: 2015.04.20.).
- Gonzales, J. & A. Sawicka (2002). “A framework for Human Factors in Information Security.” WSEAS International Conference on Information Security, Rio De Janeiro, Brazil.
- Perrow, Charles (1984), *Normal Accidents : Living with High Risk Technologies*, Basic Books.
- Sofsky Wolfgang 저·이한우 역 (2007). 「안전의 원칙: 위험사회, 자유냐 안전이냐」. 파주: 푸른숲
- UN ICT Taskforce (2003). *Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar*, UN ICT Taskforce, https://www.itu.int/dms_pub/itu-s/md/03/wsis/c/S03-WSIS-C-0006!!PDF-E.pdf (검색일: 2015.04.18)
- UN “E-Government Survey” www.unpan.org/e-government (검색일: 2015.3.30).
- Thomson, Kerry-Lynn, R. von Solms & L. Louw (2006). “Cultivating an Organizational Information Security Culture.” *Computer Fraud and Security*, October. 7-11.
- World Economic Forum (2015). The Global Risks report 2015. <http://reports.weforum.org/global-risks-2015/part-1-global-risks-2015/technological-risks-back-to-the-future/#view/fn-23> (검색일: 2015.3.30).
- Yves Punie, Sabine Delaitre, Ioannis Maghiros & David Wright (2006). *Dark scenarios in ambient intelligence: Highlighting risks and vulnerabilities*. SWAMI Deliverable D2. http://is.jrc.ec.europa.eu/pages/TFS/documents/SWAMI_D2_scenarios_Final_ESvf_003.pdf (검색일: 2015.05.20)