사회과학연구 제29권 2호(2018) 충남대학교 사회과학연구소 pp. 307-337
http://dx.doi.org/10.16881/jss.2018.04.29.2.307

정보보호 인식과 정책 간의 연관성에 관한 연구

이 기 종, 박 재 정†

국군사이버사령부, 충남대학교

본 연구의 목적은 정보보호 중요성에 대한 국민의 인식과 정부가 수립하고 시행하는 정책 간에 상호 유기적인 연관성이 있음을 검증하는 것이다. 이를 위해 본 연구에서는 정책과 인식 자체의 속성과 정보보호 정책의 성격, 정보보호 인식이 창출해 내는 효과 등의 개념을 정리하였다. 또한 정리된 개념을 바탕으로 정보보호 관련 정책서와 정보보호 실태조사의 내용을 면밀히 분석하여 정보보호 정책과 국민의 정보보호 인식 간의 유효한 관계성을 분석하였다. 본 연구의 결과로서 국민이 정보보호 중요성을 인식하는 데 영향을 주는 특정한 정책적 영향요인들이 존재함을 파악할 수 있었다. 특히, 국내 정보보호 환경과 정부의 정책이 유기적 연관성을 가질 경우에 정보보호의 중요성에 대한 국민의 인식이 상승한 것으로 분석되었다. 최근 사이버 공간에서 새로운 위협들이 증가하는 상황에서 본 연구의 결과를 반영한 정책을 수립한다면 정보보호의 중요성에 대한 국민의 인식이 지금보다 더욱 향상될 것이라고 본다.

주요어: 정보보호인식, 정보보호정책, 국가정보화백서, 국가정보보호백서, 정보보호 실태조사

† 교신저자(Corresponding Author) : 박재정, 충남대학교 정치외교학과 교수, 대전 유성구 궁동 대학로 99, E-mail : savant3@cnu.ac.kr

■ 최초투고일 : 2018년 3월 1일 ■ 심사마감일 : 2018년 3월 27일 ■ 게재확정일 : 2018년 4월 4일

1. 서 론

최근 정부의 2017년 정보보호 실태조사 발표에 의하면 정보보호에 대한 국민의 인식이 해마다 지속적으로 높아지고 있음에도 불구하고 랜섬웨어로 인한 피해율은 오히려 증가하였다(원병철, 2018. 1. 8). 이러한 현상은 정부의 정보보호 대책이 제대로 시행되지 않고 있다는 방증으로 해석할 수 있으며, 아울러 정부의 시각과 국민의 시각이 다소 다를 수 있음을 시사한다.

정부는 '대한민국은 정보보호를 위한 자발적인 노력과 인식이 저조하고 관련 산업기반 및 전문인력, 기술 등 기초체력이 부족'하여 인식의 악순환 구조가 발생한다고 보았다(미래창조과학부, 2015). 반면, 2017년 7월 정보보호의 달을 맞아 국내 한 언론 기관에서 국민을 대상으로 정보보호 인식 제고에 대한 설문조사를 진행한 결과에 의하면 '인식 제고가 쉽지 않다'는 의견이 28.3%를 차지해 두 번째로 많은 의견으로 나타났다(김태형, 2017. 8. 4).

이처럼 현실적인 정보보호 위협과 국민들의 정보보호 인식 간에 차이가 있음을 알 수 있으며, 따라서 이와 같은 인식의 차이를 좁힐 수 있는 현실적인 대응 방안 마련이 필요한 실정이다.

최근 발생하는 정보보안 위협은 국민 개개인의 보안에 대한 인식과 이를 뒷받침하는 정부의 정책이 병행되어야 즉각적이고 효율적인 대응이 가능하다(고려대 산학협력단, 2013). 특히, 국민이 사이버 공간에서 다양한 유형의 위험에 직면할수록 정부의 정보보호 관련 정책수단과 범위는 확장되어야 하고, 정부는 확장된 정보보호 정책을 통하여 국민의 정보보호 중요성 인식을 강화시키는 역할을 해야 한다.

그러므로 정부에서는 추진하고 있는 정보보호 정책과 연계해 정보보호의 중요성을 국민에게 인식시키는 것에 보다 적극적이고 다양한 방법을 강구해야 할 필요가 있다.

이에 따라 학계에서도 정보보호 중요성에 대한 연구를 활발히 수행하고 있다. 정보보호 중요성 인식과 관련하여 그동안 수행된 연구들은 정보보호가 창출해 내는 매개효과에 초점을 두고 조직 차원에서 정보보호 활동 혹은 서비스와 정보보호 효과 간의 연관성 등을 연구하였거나, 개인적 차원으로 정보보호에 관한 인식이나 동기가 실질적인 정보보호에 미치는 영향 등을 연구(김영곤, 2010; 노재인, 서진완, 2016; 문건웅, 2017; 백민정, 손승희, 2010; 이미정, 이선중, 2010; 임채호, 2006; 손승희, 2013; 전인석, 이병권, 김동원, 최진영, 2016)하였다.

이런 맥락으로 볼 때, 정부의 정책결정에 의해 영향을 받는 국민의 정보보호 인식 수준은 실질적인 정보보호 활동과 연결될 수 있는 가능성이 존재함을 보여준다. 그럼에도 불구하고 현재 정보보호 중요성 인식에 대하여 국민의 인식과 정부의 정책을 동시에 살펴본 연구는 거의 이루어지지 않고 있다. 아울러 정부의 효율적이고 실효성 있는 정책결정과 실행이 국민의 정보보호 인식 향상과 연관성이 있다고 검증된다면 그 정책 결정과 실행의 중요성은 매우 크다고 할 수 있다.

따라서 본 연구에서는 정보보호 중요성에 대한 국민의 인식과 정부의 정보보호 정책과의 연관성을 객관적으로 규명하고 분석하여 국민을 대상으로 한 정보보호에 좀 더 실효성이 있는 정책적 대안을 고려하고자 한다. 이를 위해 우선 정보보호 정책과 정보보호 인식에 대한 이론적 고찰을 통하여 이 두 개념 간의 상관성을 도출한다. 이후 상관성 있는 정보보호 정책의 실효성을 강화하기 위한 목적으로 국내 정보보호 위협 등 정보보호 환경을 살펴보고 국가 정보보호 관련 정책서를 분석하여 이들 간의 관계성을 정립하고 향후 정부의 정보보호 정책 수립에 대한 방향을 제시하고자 한다.

2. 이론적 배경

1) 정보보호 정책과 인식

(1) 정책과 인식의 의미

‘정책’이란 사회문제를 해결하기 위한 정부의 의도적인 조치를 의미한다(김정수, 2016). 좀 더 구체적으로 보면 바람직한 사회상태를 이룩하려는 정책목표와 이를 달성하기 위해 필요한 정책수단에 대한 권위 있는 국가기관이 공식적으로 결정하는 방침(정정길, 2015)이라고 할 수 있다. 또한 정책은 의도적 변화를 담고 있는 미래 지향적인 특성도 가지고 있다(임동진, 2002). 따라서 정책은 집행의 주체로서 공공문제 등의 해결이나 목표 달성을 위하여 정부가 시행하는 권위 있는 결정의 산물이다.

한편, ‘인식’은 인간의 실천에서 시작되며, 실천을 통하여 처음으로 감각적 직관에 의한 직접적·개별적·구체적인 감성적 인식이 형성된다. 이는 사물의 본성을 포착하는 것이 아니라 외면적인 인상 같은 것이다. 이 감성적 인식을 바탕으로 하여 다시 실천을 계속하면서 그릇된 점은 점진적으로 정정되고 개선되며, 다른 사물과 비교하고 구별하면서 개념, 판단, 추리를 활용하여(위키피디아, 2017) 사물의 본질에 대한 이성적 인식을 최종적으로 보유하게 된다.

만일 국민이 정부에 대한 부정적인 인식을 가지고 있다면 정부를 신뢰하지 않기 때문에 낮은 정부 지지율이 나타나게 된다. 이로 인해 정부는 정책을 수립하고 실제 수행하는 과정에서 국민의 신뢰나 지지를 확보한 상황에 비해 상대적으로 보다 많은 비용을 지불해야 하고 결과적으로 목표한 정책효과를 얻지 못하여 정책적 실패 또는 정부적 실패로 이어질 수 있다(행정연구원, 2013). 따라서 정책과 정책에 대한 인식 간에는 상호 관계성이 있다고 할 수 있다.

(2) 정책 환류

정책 환류는 정책 시행 과정의 마지막 기능이라 할 수 있다. 환류의 사전적 정의는 어떤 과정이 마무리 단계에서 끝나는 것이 아니라 처음으로 되돌아가서 다시 계속되는 것을 의미한다(김진숙, 2005). 또한, 정책평가에 대한 결과가 다시 정책의 결정체제, 집행 등의 개선에 활용되는 것을 정책 환류로 보는 견해도 있으며(김명수, 2016), 정책이나 사업의 산출 결과를 해당 정책이나 사업에 재투입하는 과정으로 볼 수도 있다(임동진, 강영철, 2009).

정책 환류는 정책의 형성, 집행, 평가의 다음 단계를 구성한다. 즉, 정책평가는 정책집행에 따른 효과를 판단하는 작업이며, 환류는 이와 같은 정책효과를 다시 정책에 대한 정보로 활용하는 것을 의미한다고 할 수 있다. 또한, 정책평가는 정책의 효과성을 검증하는 과정이고 정책 환류는 그 정책이 결정되거나 검증된 후에도 하나의 특정한 과정으로 존재하여 또 다른 정책 결정을 할 때 참고할 수 있다. 그러므로 일단 결정된 정보보호 관련 정책은 차후 생성될 관련 정책들에 계속 긍정적이거나 부정적인 영향을 줄 수 있다.

이러한 관점으로 볼 때, 국민의 정보보호 인식 제고에 긍정적인 영향을 미치게 되는 정책은 해당 정책의 시행내용과 이에 대한 개선정책을 통하여 지속적으로 국민의 정보보호 인식 향상에 기여할 수 있으므로 정책과 정보보호 인식 간의 관계성은 매우 중요하다고 할 수 있다.

(3) 정보보호 정책

정보보호 정책은 본질적으로 조직 전체 차원의

정보보호 원칙과 지침으로 구성되어야 하고, 정보보호 정책에는 개인의 권리, 법적 요건, 기준에 대한 정책을 포함한 광범위한 정책이 반영되어야 한다(한국정보보호진흥원, 2002).

따라서 조직은 정책을 구현하고 조직의 목표와 일치하도록 명확한 접근방식으로 사용자, 관리자, 제공자 모두에게 제공할 수 있는 표준, 지침, 절차를 개발해야 한다. 또한, 표준과 지침은 시스템을 보호하기 위한 기술과 방법을 명시해야 하고, 절차는 정보보호와 관련된 작업을 수행할 수 있도록 상세하게 기술되어야 한다.

이러한 정보보호 정책을 국가적 차원에 적용하기 위해서는 정보보호 정책이 국민의 정보보호 원칙과 지침으로 구성되어야 하는 것은 물론이고, 국민 개개인의 권리, 법적 요건, 기준에 대한 내용을 포함한 보다 광범위한 국가적 정책이어야 한다.

2) 국가 정보보호 정책서 이해

(1) 국가정보화백서

국가정보화백서는 국민이 국가정보화를 쉽게 이해하고 이용할 수 있도록 체계적으로 정리한 문서로서, 국가와 사회 전반의 정보화 현황과 성과, 개선사항 등을 종합적이고 객관적으로 정리하고 분석하여 국가정보화의 발전적인 추진방향을 제시하고 있다(한국정보화진흥원, 2017). <표 1>은 국가정보화백서의 최초 발간본(한국전산원, 1993)과 현재 발간본(한국정보화진흥원, 2016)의 현황을 비교한 것이다.

<표 1>에서 나타나듯이 최초 발간본에 비해 현재의 발간본은 사회 부문과 국민생활 부문이 강조되어 있는 것과 국제화 시대에 발맞추어 세계의 정보화 내용이 추가되어 있는 것을 볼 수 있다. 이는 국민 생활에서 국가정보화 정책이 중요한 역할을 하고 있으며, 세계의 정보화 정책을 확인하고 동향을 파악하는 일 또한 점차 중요해지고 있음을 보여주는 지표이다.

(2) 국가정보보호백서

국가정보보호백서는 2002년부터 '개인정보보호백서'라는 이름으로 발간되었으며, 2008년부터는 국가정보원과 방송통신위원회에서 국민의 안전과 편리한 정보환경을 위해 '국가정보보호백서'라는 이름으로 바꾸어 발간하고 있다. 2010년에는 방송통신위원회, 행정안전부, 지식경제부에서 국가보

<표 1> 국가정보화백서 최초 및 현재 발간 현황 비교

구분	최초	현재
시기	1993년	2016년
발간명	국가정보화백서	국가정보화백서
내용	• 서론(1장) • 정보사회를 향하여(2장) • 우리나라의 국가 정보화(3장) • 정보화 기반체계(4장) • 국내외 환경변화와 우리나라 정보화의 발전방향(5장)	• 지능정보화 추진 현황(1편) • 국가사회 정보화(2편) • 국민생활 부문(3편) • 우리나라 정보화 수준(4편) • 세계의 정보화(5편)
발간 및 집필	• 주관: 한국전산원	• 주관: 한국정보화진흥원 • 추진위원회: 국가 정보화 집필진, 좌담회

<표 2> 개인정보보호백서 최초 및 국가정보보호백서 현재 발간 현황 비교

구분	최초	현재
시기	2002년	2016년
발간명	개인정보보호백서	국가정보보호백서
내용	• 총론(1장) • 개인정보보호정책(2장) • 정보통신기술의 발전과 개인정보보호(3장) • 민간부문의 개인정보보호(4장) • 공공부문의 개인정보보호(5장) • 국외 개인정보보호 동향과 국제협력(6장)	• 특집 • 총론(1편) • 정보보호체계와 제도(2편) • 분야별 정보보호 추진(3편) • 정보보호기반 조성(4편)
발간 및 집필	• 편찬위원장: 한국정보보호진흥원 (개인정보분쟁조정위 사무국) • 편찬위원: 정통부 인원 등 9명 • 집필진: 10여 명	• 발간기관: 국가정보원, 미래부, 방송통신위원회, 행정자치부, 금융위원회 • 지원기관: 한국인터넷진흥원, 국가보안기술연구소

안기술연구소, 한국인터넷진흥원과 합동으로 발간하였으며, 2015년부터는 국가정보원, 미래창조과학부, 방송통신위원회, 행정자치부에서 한국인터넷진흥원, 국가보안기술연구소와 합동으로 발간하고 있다. <표 2>는 국가정보보호백서 최초 발간본과 국가정보보호백서 현재 발간본의 현황을 비교한 것이다.

<표 2>에서 나타나듯이 최초 발간본에 비해 현재의 발간본은 개인정보뿐만 아니라 각 분야별 정보보호 추진에 대한 내용 등 취급 범위가 확대된 것을 알 수 있고, 발간기관 또한 관련 정부기관이 함께 참여하여 공동으로 발간하고 있는 것이 이전과 변화된 모습이라 할 수 있다.

(3) 정보보호 실태조사

매년 정부(현. 과학기술정보통신부, 구. 미래창조과학부)가 주관하고 한국인터넷진흥원이 개인과 기업을 대상으로 정보보호와 관련된 설문조사인 정보보호 실태조사를 실시한다. 설문조사 기간은 기업의 경우 3개월, 개인의 경우 1개월로 하며 사업체와 가구를 대상으로 방문 설문조사를 실시하고, 이렇게 조사된 결과를 분석한다.

이 보고서는 1998년 정보화 역기능 실태조사라는 명칭으로 출발하였고 조사의 발간 목적은 국내 정보보호와 관련된 다양한 분야의 통계를 심층적으로 파악하여 통계작성 담당자에게 포괄적이고 상세한 정보를 제공하기 위함이다(한국정보보호센타, 1998). 여기에는 통계개요, 통계설계, 자료수집, 자료입력 및 처리, 통계 결과 및 공표, 이용자서비스, 통계 기반 및 개선 등에 대한 설명이 수록되어 있다(미래창조과학부・한국인터넷진흥원, 2016). <표 3>은 인터넷 관련 최초의 실태조사인 정보화 역기능 실태조사 최초의 발간 내용과 정보보호 실태조사 현재의 발간 내용을 비교한 것이다.

3) 정보보호 인식 관련 선행연구 검토

정보보호 인식은 사람들이 본인의 직무를 이행할 때 정보보호의 함축된 상태를 인지하는 과정이라고 할 수 있다. 여기에는 정보보호의 중요성 인식과 사고 발생에 따른 대응 방안, 보고 체계 등을 포함한다(강다연, 장명희, 2014).

<표 3> 정보보호 실태조사 최초 및 현재 발간 현황 비교

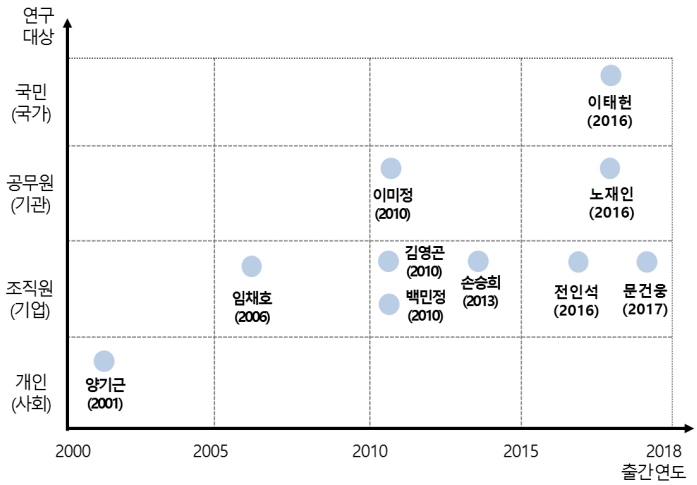
구분	최초 정보화 실태조사	최초 정보보호 실태조사	현재 정보보호 실태조사
시기	1998	2001	2017
발간명	정보화 역기능 실태조사	정보보호 실태조사(민간부문)	정보보호 실태조사(개인부문)
내용	• 개요(1장) • 조사결과(2장) 컴퓨터/인터넷 이용행태, 정보화 역기능 현황, 정보화 역기능 영향 등 • 요약 및 결론(3장) • 부록: 설문지, 자유응답내용 등	• 조사개요(1장) • 조사결과(2장) • 정보보호시스템 구축현황, 정보통신시스템 접근통제 및 운용관리, 정보보호정책 수립현황, 재해현황 및 대응방안 수립, 정보보호 활성화 전망 등 • 요약 및 결론(3장) • 부록: 설문지, 통계표 등	• 조사개요(1장) • 정보보호 인식(2장) • 침해사고 예방(3장) • 침해사고 대응(4장) • 개인정보보호(5장) • 신규서비스 정보보호(6장) • 부록: 주요변경내역, 요약보고서 등
발간	• 주관: 정보통신부 • 시행: 한국정보보호센타 • 기간: 4일(12.4.~12.7.) • 방법: 인터넷 조사	• 주관: 정보통신부 • 시행: 한국정보보호진흥원 • 기간: 1개월(11.27.~12.24.) • 방법: 전화, 이메일, 팩스 등 설문조사	• 주관: 과학기술정보통신부 • 시행: 한국인터넷진흥원 • 기간: 기업(3개월), 국민・개인(2개월) • 방법: 가구 및 기업체 방문조사 * 기업부문은 별도 발간

이러한 정보보호 인식 제고는 조직의 정보를 안전하게 유지할 수 있는 가장 핵심적인 축이기 때문에 정보보호 인식 제고가 성공적인 경우, 조직이 정보보호 이행을 통하여 얻게 되는 효과는 다음과 같이 4가지로 정리할 수 있다(문건웅, 2017). 첫째, 조직의 보안 기능을 적절하게 사용할 수 있게 된다. 둘째, 불법적인 보안 문제, 잠재적 악의가 포함된 사항이 있을 경우 즉각 보고할 수 있게 된다. 셋째, 보안의 심각성을 깨닫게 하므로 직원들의 근면함을 상승시킬 수 있다. 넷째, 조직의 정보에 대한 보안관리가 가장 중요한 것임을 인지하게 된다.

결국 정보보호 인식 제고는 정보 자산에 대한 위협이 되는 요소와 상황을 관리하는 것에 대한 지행합일(知行合一)의 상태를 의미하는 것으로 잠재적인 위협을 인지하여 조직 구성원이 일상에서 경험할 수 있는 어떤 보안 이슈와 사고를 이해시켜 주는 개념인 것이다. 또한, 정보보호 인식 제고를 위한 정책은 자산과 정책, 그리고 정보보호 인식 교육으로 구성되어야 하며, 이러한 정책에 따라 조직의 정보 자산에 대한 정보보호 정책에 준하여 정보보호 인식 제고 과정이 이행되어야 한다.

<그림 1>은 최근 정보보호 인식에 대한 선행연구의 연구 경향을 도식화한 것이다. 그동안 정보보호 인식 관련 선행연구들을 보면, 주로 개인의 정보보호 인식수준이 정보보호 정책에 미치는 영향에 대한 연구들(김영곤, 2010; 노재인, 서진완, 2016; 문건웅, 2017; 백민정, 손승희, 2010; 이미정, 이선중, 2010; 임채호, 2006; 손승희, 2013; 전인석 외, 2016)이 주류를 이루었고, 또한 특정 기업이나 대상을 선정하여 다소 제한적인 사례조사 형태의 연구가 대부분을 차지하였다(이태헌 외, 2016).

이와 같은 정보보호 인식에 대한 접근 이외의 관련 선행연구들을 살펴보면, 김종기와 강다연(2006)은 보안정책이 보안의식과 보안효과에 미치는 영향관계를 연구하였고, 이충희와 신민수(2010)는 정보보안에 대한 인식 수준에 의해 동기 부여된 보안 행위들 간의 차이를 연구하였다.



<그림 1> 2000년 이후 정보보호 인식에 대한 선행연구의 경향

특히, 이태헌 외(2016)는 국가차원에서 정보보호 의식과 관련된 연구를 수행하였다. 이 연구에서는 사이버 관련 핵심국가들인 한국, 미국, 중국 간의 국민의식 비교를 통하여 국가가 국민의 정보보호 중요성 인식을 제고시켰다는 것을 검증하였으며, 국내 사례를 활용하여 정보보호의 중요성 인식 향상에 국가가 영향을 미칠 수 있다는 결론을 도출하였다. 즉, 국가의 정보보호 정책이 국민의 정보보호 중요성 의식에 영향을 미칠 수 있다는 가능성을 제시하였다.

이러한 주장은 그간 개인의 정보보호 인식수준이나 특정 기업의 정보보호 인식수준이 정보보호 정책에 미치는 영향을 거시적인 관점으로 바라보았기에 국가의 정책이 국민의 인식에도 영향을 미칠 수 있다고 주장한 것으로 해석할 수 있다.

따라서 지금까지 살펴본 선행연구의 검토를 토대로 정부의 능률적인 정책결정과 시행이 정보보호 중요성에 대한 국민의 인식에 긍정적 영향을 주어 그 의식수준을 향상시킬 것이라 생각된다. 그럼에도 불구하고, 국민의 정보보호 중요성 인식과 국가의 정보보호 정책에 대해 동시에 살펴본 연구는 매우 드물다.

이에 본 연구에서는 이러한 주장에 근거하여 정책과 인식에 대한 기본적인 개념 이해, 정책 환류에 대한 이해, 정보보호정책의 속성 분석 그리고 정보보호 인식과 관련된 최근 7년간의 선행연구 고찰을 통하여 정보보호 정책과 국민의 정보보호 인식 간의 관계성을 다음과 같이 정립하였다.

첫째, 국가적 측면에서의 정보보호 정책은 국민 전체 차원의 정보보호 원칙과 지침으로 구성되고, 국민 개개인의 권리, 법적 요건, 기준에 대한 정책을 포함한 보다 더 광범위한 국가정책을 결정하고 시행할 의무가 있는 것으로 판단된다. 이에 정책이 국민들의 정보보호 중요성에 대한 인식과 특정한 연관성을 가질 것이라는 전제가 구축되었다.

둘째, 정보보호에 대한 인식 혹은 동기가 실질적인 정보보호 효과에 긍정적인 영향을 준다는 사실이 도출되었다. 그러므로 효과적인 정보보호 정책결정이 국민의 정보보호 인식 향상에 영향을 준다는 사실이 검증된다면 그 향상된 정보보호 인식은 곧 실효성 있는 정보보호 활동을 창출할 수 있다는 가능성 또한 제시된다.

이러한 관계성을 종합해 보면, 국민의 인식이 수렴되는 능률적인 정책결정과 시행은 국민들의 정보보호 인식 향상에 긍정적인 영향을 미칠 것이며, 이 향상된 인식은 그 상호의존적 관계성에 의거하여 향상된 정보보호 활동으로 인해 정보보호를 강화시켜 정부의 정책에 대한 신뢰성에 긍정적인 영향을 줄 수 있다는 본 연구의 논지는 타당성이 있다고 할 수 있다.

따라서 본 연구에서는 국민의 정보보호 인식에 영향을 주는 정책적 요인들을 추출해 내기 위하여 국내 정보보호 환경, 정보보호 정책이 가지는 특성, 환경과 정책 간의 상호 연관성을 분석하고자 한다.

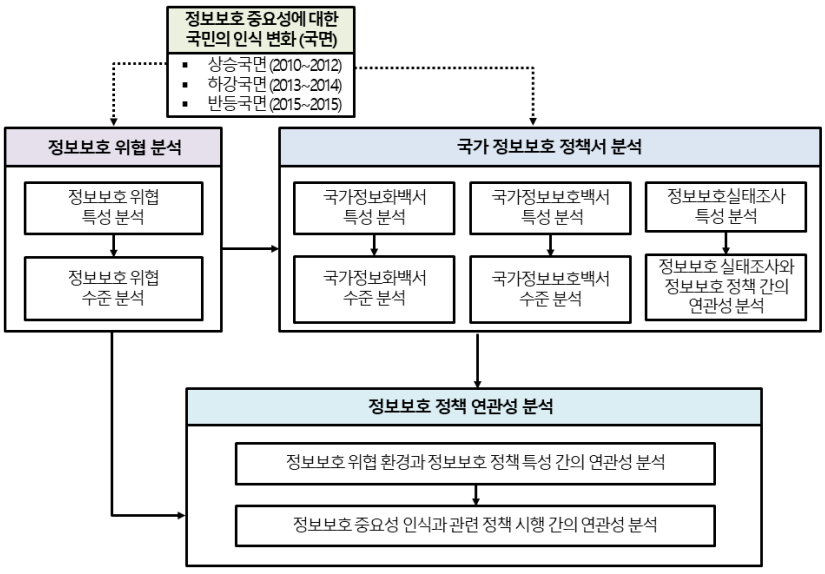
3. 연구의 설계

1) 연구 분석 모형

본 연구에서는 2010년 이후 국민의 정보보호 중요성 인식 변화에 대한 정책적 영향 요인을 확인하기 위해서 정보보호 관련 정책 백서를 활용하여 국내 정보보호 환경과 정보보호정책이 가지는 특성을 분석한다.

구체적으로는 2010년부터 2015년 사이 국민의 정보보호 중요성 인식에 있어서 상하 곡선이 발생하여 연관성을 가지는 환경적 및 정책적 요인을 도출하여 국민의 정보보호 중요성 인식을 향상시킬 수 있는 정책적 방향을 제시한다. 이러한 연구의 목적을 달성하기 위하여 연구모형을 <그림 2>와 같이 설계하였다.

본 연구에서는 <그림 2>와 같이 정보보호 중요성에 대한 국민의 인식 변화를 상승국면, 하강국면, 반동국면으로 구분하여 살펴볼 것이다. 이후, 정보보호 위협 분석과 국가 정보보호 정책서를 분석할 것이며, 정보보호 위협 분석의 경우 특성과 수준을 구분하여 살펴보고자 한다. 국가 정보보호 정책서는 국가정보화백서의 특성과 수준, 국가정보보호백서의 특성과 수준, 정보보호 실태



<그림 2> 연구모형

조사의 특성과 정보보호 정책 간의 연관성을 살펴보고자 한다. 이후 정보보호 정책 간의 연관성을 분석하고자 하며, 특히 정보보호 위협 환경과 정보보호 정책 특성 간의 연관성과, 정보보호 중요성 인식과 관련 정보보호 정책 시행 간의 연관성을 살펴보고자 한다.

연구설계의 중점은 <표 4>와 같이 국내 정보보호 위협 분석과 국가 정보보호 정책서 분석을 통하여 국가적인 정보보호 정책에서 상호 연관성 여부를 확인하고 분석하는 것이다.

이에 첫 번째 연구분석인 '정보보호 위협 분석'에서는 2010년부터 2015년 사이에 발생한 정보보호 위협 사건의 특성과 수준을 비교하고 분석하였다. 이 '정보보호 위협 분석'은 우리가 상식적으로 생각하는 정보보호 위협 수준(시기, 강도 등)이 높을수록 국민이 인식하는 정보보호 중요성 인식이 높아졌는가를 분석하기 위한 것이다.

두 번째 분석인 '국가 정보보호 정책서 분석'은 특정 국면 시기에 따라 발행된 정책서의 종류별로 특성 및 수분 차원 분석과, 특성 및 연관성 분석을 하였다. 정책서의 종류에는 계획서인 국가정보화백서와 국가정보보호백서가 있고, 평가서인 '정보보호 실태조사'가 있다. 계획서 분석은 특성 및 수준 차원으로 정보보호의 정책적 방향성과 내용의 차이점을 비교하였으며, 평가서 분석은 특성 및 연관성 차원으로 실태조사에 나타난 국민의 정보보호 중요성 인식의 특성과 국민의 정보보호 중요성에 관한 인식을 향상시키기 위하여 실태조사가 현실적인 내용으로 조사를 하였는가 여부와 평가서와 계획서 작성에 참여한 기관의 연관성을 통하여 항목을 신설하고 국민의 인식을 국가 정책서에 반영하고 계획을 수립하였는가 여부의 상호 연관성을 분석하였다.

계획서 분석에서 특성 분석이란 각 백서에서 제시한 정책 방향 및 주요 내용을 대표하는 표현을 분석하는 것이며, 수준 분석이란 계획서에서 나타난 국가의 정보보호 준비도 수준을 국가에서 제시한 기업의 정보보호 준비도 평가를 적용하여 평가하는 것이다. 즉, '국가 정보보호 정책서 분석'은 우리가 일반적으로 생각하는 국가의 연도별 정책이 시기적절하게 정책으로 수립되어 국민의 정보보호 중요성 인식에 영향을 주었는가를 분석하기 위한 것이다.

따라서 이 연구의 최종적인 분석은 '정보보호 정책 연관성 분석'에서 이루어지고, 이는 첫 번째 분석과 두 번째 분석에 도출된 시사점을 통하여 정보보호 중요성 인식과 정책적 관계성을 도출하는 것이다.

이 연구를 설계한 이론적 근거는 다음과 같다. 첫째, 매년 실시되는 정보보호 실태조사의 의미에 있다. 매년 국민의 정보보호 인식을 조사하는 근원적인 이유 측면과 실태조사의 활용 등 정책적

<표 4> 연구의 분석 유형

분석 영역	분석 유형		
	계획서 분석		평가서 분석
분석 대상	국가정보화백서	국가정보보호백서	정보보호 실태조사
특성 분석	국가 정보보호의 "정책 방향 및 주요 내용"을 대표하는 내용 분석	국가 정보보호의 "정책 방향 및 주요 내용"을 대표하는 내용 분석	연도별로 조사된 실태조사 항목(내용) 분석
수준 분석	계획서에 나타난 정보보호 준비도	계획서에 나타난 정보보호 준비도	X
연관성 분석	X	X	평가서와 계획서 간 참여기관 연관성 분석

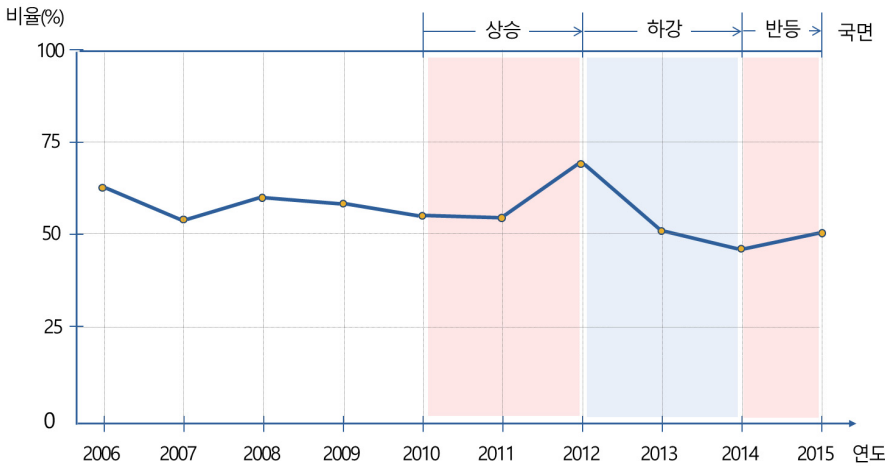
인 환류 측면에서 보면, 국민의 정보보호 인식 변화와 정보보호 위협 환경, 그리고 정보보호 정책 상호 간에 연관성이 있어야 한다고 본다. 즉, 실태조사에서 나타난 국민의 정보보호 중요성 인식 변화는 정보보호 위협 환경과 정책 간에서 영향을 받고 또한 정책적 환류의 특성에 따라 영향을 준다는 것이다.

둘째, 매년 수립하고 발간하는 국가 정보보호 정책도 마찬가지이다. 국가정보화백서와 국가정보보호백서가 매년 시행되고 발간될 이유는 국내·외적인 요인들에 의하여 정보보호 정책이 영향을 받고 있기 때문이라고 해석할 수 있다. 특히, 정보보호 위협에 대한 사건이 발생하면 정부에서 이 사건에 대한 국가적인 대책과 방안을 마련하고자 할 것이며 이를 정보보호 정책서에 반영할 것으로 판단하였기 때문이다. 따라서 국가 정보보호 정책서들 간의 특성과 그에 대한 수준분석이 객관적이고 타당하게 이루어져야 정보보호 정책 간의 연관성을 판단할 수 있는 근거가 될 것으로 보았다.

2) 연구 대상 및 범위

연구 대상 및 범위는 정부가 시행한 정보보호 실태조사(정보보호의 중요성 인식)에 관한 설문조사에서 <그림 3>과 같이 상하 곡선의 흐름을 보이는 2010년부터 2015년 사이의 정보보호 정책 관련 문헌을 분석한 후, 이를 연도별로 분류하여 정보보호 중요성 인식에 대한 상승곡선과 하강곡선을 구분하고 이와 연관된 정보보호 정책서를 연구 대상으로 선정하였다.

<그림 3>에서 알 수 있듯이, 정보보호의 인식 변화는 2006년부터 2007년까지는 인식의 변화가 감소 추세에 있으나, 2008년부터 2009년까지는 정보보호 중요성 인식의 변화가 거의 없음을 알 수 있다. 하지만, 2010년부터 2015년까지 정보보호 중요성의 인식 곡선이 두드러지게 변화함을 알 수 있는데, 이러한 변화로 보아 5년 동안 정보보호와 관련된 사건이 발생한 것으로 예상된다. 따라서 본 연구의 범위를 2010년부터 2015년까지로 선정하고자 한다.



<그림 3> 정보보호 인식 변화
출처: 통계청(2016)

이 연구 범위를 2010년부터 2015년까지 설정한 일반적인 이유는 실패조사 시점 기준으로 최신 자료이면서도 통계적 의미를 가지고 있고, 정보보호 실태조사의 결과 항목에서 가장 우선하여 해석하고 있기 때문이다.

또한, 이 통계적 수치를 연구적인 측면의 활용도를 고려해보았다. 즉, 실태조사 결과에서 나타나는 국민의 정보보호 인식과 관련하여 평균적으로 보이는 수치로써는 그 현상을 파악하는 것이 제한되나 '매우 중요하지 않음', '중요하지 않음', '중요한편', '중요하게 생각함', '매우 중요하게 생각함' 등 5개의 인식 계층을 연도별로 비교하면 그 의미를 구체화할 수 있다.

특히, 최근 수치 중 2016년과 2017년의 자료를 제외하고 2010년부터 2015년까지 해당 비율만 적용한 이유는 '매우 중요' 비중 수치 비교인 <표 5>를 보면 알 수 있다. 매우 중요의 비중도를 %로 계산해 보면 2011년에는 73.1%, 2012년에는 78.9%, 2013년에는 68.6%, 2014년에는 63.9%, 2015년에는 69.8%이다. 중요의 비중도를 %로 계산해 보면 2011년에는 28.8%, 2012년에는 21.2%, 2013년에는 31.6%, 2014년에는 36.6%, 2015년에는 30.5%이며, 이 비교는 리커트 5점 척도의 기법에 근거하였다. 이 리커트 5점 척도의 경우, '매우 중요하지 않음', '중요하지 않음', '중요한편', '중요하게 생각함', '매우 중요하게 생각함'으로 구성되는데, 이 척도의 측정 방식은 대상자의 태도가 한 측면의 극단적 단계에서 중립 단계를 지나 다른 측면의 상반된 단계에 이르는 양분론적 가정에 근거하고 있다.

<표 5> 5점 척도 '매우 중요' 비중 수치 비교

구분	매우 중요	중요	보통	중요하지 않음	전혀 중요하지 않음
2010년	1.122	0.434	-	-0.004	-0.002
2011년	1.090	0.429	-	-0.025	-0.002
2012년	1.284	0.345	0	-0.001	0
2013년	1.006	0.463	0	-0.002	0
2014년	0.876	0.501	0	-0.007	0
2015년	1.010	0.441	0	-0.003	-0.002
2016년	0.980	0.451	0	-0.005	0
2017년	0.998	0.443	0	-0.004	0

* 본 표에서 매우 중요는 수치x2이며, 중요는 수치x1, 중요하지 않음은 수치x-1, 전혀 중요하지 않음은 수치x-2가 적용된 수치이다.

따라서 본 연구를 위하여 정보보호 중요성 인식 변화를 5점 척도로 변환한 결과, '매우 중요하게 생각한다' 비율(%)이 매우 높아 변화의 수치와 그 의미를 강하게 드러낸다고 보았기에 정보보호 인식 변화의 국면을 해석하기에 적절하다고 판단하였다.

정보보호 중요성 인식에 대한 상승국면, 하강국

<표 6> 연구 대상 및 범위

국면		연구 대상 및 범위
정보보호 중요성 인식	상승국면 (2010~2012)	2010 국가정보보호백서 → 2010 국가정보화백서 → 2010 정보보호 실태조사 → 2011 국가정보보호백서 → 2011 국가정보화백서 → 2011 정보보호 실태조사 → 2012 국가정보보호백서 → 2012 국가정보화백서 → 2012 정보보호 실태조사
	하강국면 (2013~2014)	2013 국가정보보호백서 → 2013 국가정보화백서 → 2013 정보보호 실태조사 → 2014 국가정보보호백서 → 2014 국가정보화백서 → 2014 정보보호 실태조사
	반등국면 (2015~2015)	2015 국가정보보호백서 → 2015 국가정보화백서 → 2015 정보보호 실태조사

면, 반등국면은 해당 기간에 통계청에서 발표한 정보보호 중요성 인식의 변화 중 '매우 중요하게 생각한다'는 인식 비율과 그 추세를 적용하였다.

이러한 국면 구분에 따라 연구 대상 및 범위는 <표 6>과 같이 상승국면의 경우 2010년부터 2012년까지 국가정보보호백서, 국가정보화백서, 정보보호 실태조사의 순으로 정보보호 중요성 인식을 살펴보고자 하며, 하강국면의 경우 2013년부터 2014년까지 국가정보보호백서, 국가정보화백서, 정보보호 실태조사의 순으로 정보보호 중요성 인식을 살펴보고자 한다. 반등국면은 2015년의 국가정보보호백서, 국가정보화백서, 정보보호 실태조사에 대해 살펴볼 것이다.

3) 연구 방법

본 연구는 문헌 중심의 연구 방법으로써 정보보호 위협 분석, 국가 정보보호 정책서 분석, 그리고 국민의 정보보호 중요성에 대하여 정책 상호 연관성을 분석한다.

첫째, 정보보호 위협 분석에서는 국내 정보보호에 대한 위협의 변화를 중심으로 분석한다. 먼저 2003년부터 최근까지 정보보호 위협의 사례를 발췌하고 그중에서 국면별로 특성을 분석한 이후 이에 대한 3개의 정책서들 간의 연관성을 분석한다.

둘째, 국가 정보보호 정책서 분석에서는 먼저, 국가정보화백서를 대상으로 국면별 정책적 특성을 분석하고, 이후 이를 국내기업 및 단체를 대상으로 정보보호 수준 평가를 시행하는 정보보호 준비도 평가 기준을 적용하여 연도별 및 국면별 국가의 정보보호 수준을 평가한다. <표 7>은 국가의 정보보호 수준을 평가하기 위한 정보보호 준비도 세부 평가 지표[1]이다.

정보보호 준비도 평가 세부 평가지표를 적용하는 이유는 연도별, 국면별로 국가의 정보화정책 수준을 공식적인 기준에 의거해 비교할 수 있기 때문이다.

또한, 정보보호 준비도 평가 세부 평가지표의 적용은 모든 기업을 대상으로 하나, 기업의 경우 규모가 소규모부터 대규모까지 매우 광범위하며, 더욱이 국가적인 측면에서 기업을 보편적으로 평가하기 위하여 지표가 개발된 것이므로 거시적 관점에서 해당 지표를 국가에 적용하여도 적절하다고 판단하였다. 또한, 국가에서 시행하는 정책 또한 기업의 정보보호 준비도 평가 지표를 측정하는 것과 같은 취지와 목적을 가지고 있기 때문이다. 평가지표를 적용할 때의 제한 조건으로, 활동지표 중 현장 중심의 평가항목(인적보안, 외부자 보안, 정보통신시설의 환경보안, 정보통신시설의 출입관리, 사무실 보안, 취약점 점검)은 현장 중심의 평가로 문서를 통하여 평가하는 것이 제한되어 동일한 점수를 부여하고 평가의 오차를 최소화하였다.

셋째, 정책 연관성 분석에서는 국민의 정보보호 중요성 인식에 대한 국면(상승, 하락, 반등)별로 정보보호 중요성 인식과 정보보호 정책 특성 간의 연관성 분석, 정보보호 위협 시기와 정보보호 정책 간의 연관성 분석, 정보보호 중요성 인식과 관련 정책 시행 간의 연관성 분석을 실시한다.

이러한 분석을 종합하여 최종적으로 정보보호 중요성 인식, 정보보호 위협 시기, 그리고 정보보호 정책 간의 상호 연관성을 분석한다.

1) 정보보호 준비도 평가는 기업의 정보보호 수준을 진단하는 것으로써, 미래창조과학부가 민간 자율의 정보보호 활성화를 위해 만든 평가 모델이다. 정보보호 준비등급은 기업의 정보보호 인프라 확충 수준 및 정보보호 활동 수행 여부 등을 고려하여 AAA, AA, A, BB, B 등 5등급으로 나뉜다.

<표 7> 정보보호 준비도 평가 세부 평가지표

지표	구분	평가 지표			평가 적용	
		내용		점수	기준	점수 부여
기반지표	1. 정보보호 리더십	1.1	정보보호 최고책임자(CISO)지정	5	정책 여부	2.5 또는 5
		1.2	정보보호 의사소통 및 정보제공	5		
		1.3	정보보호 운영방침	4		2 또는 4
	2. 정보보호 자원관리	2.1	정보보호 추진계획	4	계획 여부	2 또는 4
		2.2	정보보호 인력 및 조직	4	인력 여부	2 또는 4
		2.3	정보보호 예산 수립 및 집행	4	예산 여부	2 또는 4
		2.4	정보보호 이행점검	4	점검 여부	2 또는 4
활동지표	1. 관리적 보호활동	1.1	정보보호 교육수행	5	교육 여부	2.5 또는 5
		1.2	자산 관리	4	자산 여부	2 또는 4
		1.3	인적 보안	4	점수통일 - 현장평가제한요인	4
		1.4	외부자 보안	5		5
	2. 물리적 보호활동	2.1	정보통신시설의 환경보안	4		4
		2.2	정보통신시설의 출입관리	4		4
		2.3	사무실보안	4		4
	3. 기술적 보호활동	3.1	취약점 점검	5		5
		3.2	정보보호 사고탐지 및 대응	5	기술보안 여부	2.5 또는 5
		3.3	시스템 개발 보안	4		2 또는 4
		3.4	네트워크 보안	4		2 또는 4
		3.5	정보시스템 및 응용프로그램 인증	5		2.5 또는 5
		3.6	자료유출 방지	4		2 또는 4
		3.7	시스템 및 서비스 운영 보안	5		2.5 또는 5
		3.8	백업 및 IT재해 복구	4		2 또는 4
		3.9	PC 및 모바일기기 보안	4		2 또는 4
계				100		

4. 연구 결과

1) 정보보호 위협 분석

(1) 정보보호 위협 특성 분석

과학기술과 정보통신기술의 발전에 힘입어 정보보호 환경은 그 수준이 지속적으로 향상되어 왔다. <표 8>에서 나타난 2003년 이후 정보보호 위협 형태의 시계열 동향을 보면(위키피디아, 2017. 10.20), 2000년대 초반에는 옥션, GS 칼텍스 대상으로 일어난 해킹은 개인적 수준의 정보 유출 피해가 다수 발생하였다. 그러나 2000년도 후반으로 갈수록 그 공격대상과 수준이 공공기관 등 공공영역을 대상으로 공격의 대상이 확대된다. 이러한 대표적인 사례가 2009년에 발생한 7·7 DDoS 공격이었다.

2010년부터 2015년까지 공격빈도와 그에 따른 피해 정도가 지속적으로 심화되었다. 특히, 사회적으로 인식이 높은 3·4 DDoS 공격, 농협전산망 마비 사태, 10·26 DDoS 공격, 3·20 전산대란, 농협전산망 마비 사태, 10·26 DDoS 공격, 3·20 전산대란, 한수원 사이버테러 등이 발생하였다. 이러한 사례는 개인적인 수준에서 이루어지

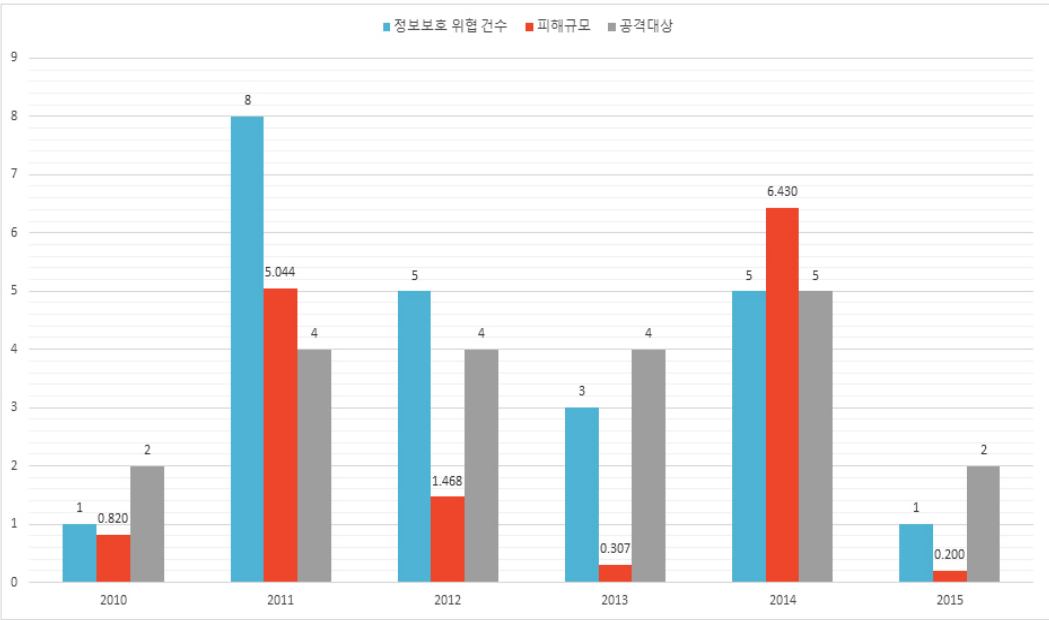
는 해킹 사고가 아니라 어느 특정 집단(단체)에서 이루어진 사회적 및 정치적 목적을 띤 해킹이라고 볼 수 있는 것이다. 이러한 정보보호의 상황 변화로 정보보호는 개인의 정보보호 차원을 넘어서 국가의 정보보호 차원으로 그 중요성이 확대되었고, 이는 이러한 새로운 정보보호 위협 변화에 부합한 정책적 대응이 필요하다는 것을 의미한다. 2015년 이후에도 국방부 해킹 등으로 정보보호 위협이 지속되고 있다.

(2) 정보보호 위협 수준 비교

앞의 2010년 이후 정보보호 위협 형태의 시계열 동향인 <표 8>을 연도별도 나타난 피해규모와 공격대상 등을 수준별 비교로 전환하면 <그림 4>와 같다.

<표 8> 2003년 이후 정보보호 위협 형태의 시계열 동향

시기	대상	피해유형	피해규모	정보보호 위협에 대한 사회적 인식
2003. 01.	KT	DNS서버공격	9시간 마비	1·25 인터넷 대란
2008. 02.	옥션	개인정보유출	1,863만 명	옥션 개인정보유출사건
2008. 04.	하나로 텔레콤	개인정보유출	600만 명	
2008. 09.	GS칼텍스	개인정보유출	1,125만 명	
2009. 07.	정부, 포털, 은행	사이트 마비		7·7 DDoS 공격
2010. 03.	신세계몰	개인정보유출	820만 명	2010년 대량 정보유출 사건
2011. 03.	정부, 포털, 은행	사이트 마비		3·4 DDoS 공격
2011. 04.	현대캐피탈	개인정보유출	175만 명	현대캐피탈 해킹 사건
2011. 04.	농협	전산망 마비	수백억 원(추정)	농협전산망 마비 사태
2011. 05.	네이버, 다음 등	개인정보유출	14만 명	
2011. 07.	네이트(SK컴즈)	개인정보유출	3,500만 명	네이트 개인정보유출사건
2011. 08.	한국앱손	개인정보유출	35만 명	
2011. 10.	선거관리위원회	사이트 마비		10·26 DDoS 공격
2011. 11.	넥슨	개인정보유출	1,320만 명	
2012. 03.	SK, KT	개인정보유출	20만 명	
2012. 05.	EBS	개인정보유출	400만 명	
2012. 06.	코웨이	개인정보유출	198만 명	
2012. 06.	중앙일보	전산망 해킹		
2012. 07.	KT	개인정보유출	870만 명	
2013. 03.	주요방송사, 은행 등	전산망 마비		3·20 전산대란
2013. 04.	SC제일, 시티은행	개인정보유출	13만 명	
2013. 06.	정당, 청와대, 주한미군	개인정보유출	294만 명	6·25 사이버테러
2014. 01.	카드, 농협은행	개인정보유출	2,000만 명	2014년 대량 개인정보 유출 사건
2014. 03.	KT	개인정보유출	1,200만 명	
2014. 03.	SKT, LG 등	개인정보유출	1,230만 명	
2014. 03.	국토교통부	개인정보유출	2,000만 명	정보유출
2014. 12.	한수원	시스템 침투	시스템위협	한수원 사이버테러
2015. 09.	뽐뿌	개인정보유출	200만 명	
2016. 07.	인터파크	개인정보유출	1,030만 건	
2016. 09.	국방부	군사비밀유출	공개 제한	국방부 최초 해킹 사건
2017. 07.	20개 업체	개인정보유출	3,300만 건	
2017. 09.	하나투어	개인정보유출	100만 건	



<그림 4> 연도별 정보보호 위협의 건수, 피해규모, 공격대상 수준 비교

정보보호 위협 건수가 많은 연도는 2011년, 2012년, 2014년이었다. 피해규모 누적 정도에 있어서 큰 시기는 2011년, 2012년, 2014년으로 나타났다. 그리고 공격대상(① 업무방해, ② 데이터 탈취, ③ 사이버범죄, ④ 정치적 목적, ⑤ 파괴목적)의 수준(Jiransecurity, 2016. 6. 30)을 비교하면 높은 위협 시기는 2011년, 2012년, 2014년이다. 이처럼 정보보호 위협 건수의 피해 누적 정도는 2011년과 2012년이 다른 연도에 비해 높은 것을 알 수 있고 이에 대해 정보보호 위협이 많았기 때문에 피해 누적 정도도 커진 것으로 해석할 수 있다.

게다가 정보보호 위협과 피해의 심각성이 지속 유지됨에 따라 국민들의 정보보호 중요성 인식도 점차 높아진다고 볼 수 있는데, 이는 정보보호 중요성 인식의 상승국면(2010~2012)이 이러한 해석을 지지해준다고 생각된다.

하지만, 2014년은 이러한 해석과 다소 상반된 결과를 보인다. 즉, 2014년에는 정보보호 위협 강도와 피해 누적 정도가 큰 것으로 나타났으나, 정보보호 중요성에 대한 인식 경향은 2013년부터 하강하고 있는데 이 시기에 반등으로 이어지지 못하고 지속 하락하였다. 반면 2015년은 2014년보다 위협 건수와 피해 정도가 낮았는데 정보보호 중요성 인식이 반등하여 2014년과 2015년 사이에 국민의 정보보호 중요성 인식에 다른 영향요인이 있을 것으로 예측할 수 있다.

따라서 국내적으로 정보보호 위협 특성과 그 피해 양상 수준의 심화에 따라 사이버 공간에서 국민의 자유로운 활동을 보장하기 위하여 개인 또는 기업 차원의 정책 수립보다 국가의 전 영역에서 사이버 안보를 형성할 수 있는 국가적인 정책 수립이 필요할 것이고, 국민이 느끼고 인식하는 정보보호 중요성 인식을 향상시키기 위하여 교육 및 홍보 등 정책적인 활동도 필요할 것으로 본다(김태형, 2017. 8. 4).

2) 국가 정보보호 정책서 분석

(1) 국가정보화백서

① 특성 분석

국가정보화백서는 연도별로 각각의 특성이 나타나며, 이를 국면별로 대조하여 구체적으로 파악해 보면 <표 9>와 같이 3가지로 그 특성을 정리할 수 있다.

상승국면에서는 2010년의 '정보보호 기반조성'의 정보보호 정책 주제가 2011년부터 변경되어 2012년까지 '안전한 사이버 환경조성'으로 변화하였다. 이는 새로운 정보보호 환경 변화에 부합한 정보보호 정책이 수립되었음을 보여준다.

그러나 하강국면에서는 2012년도 '안전한 사이버 환경조성'의 주제가 2013년도와 2014년도에 이르러서 2010년도의 '정보보호 기반조성'으로 변화하였다. 이는 새로운 정보보호 위협 환경에 부합하지 못하고 기존의 주제로 복귀하였음을 보여준다.

반등국면에서는 2014년도의 '정보보호 기반조성'이 2015년에 '정보보호'로 변화하고 항목도 간소화되었다. 그러나 이 시기에 정보보호 위협을 보면 상승과 하강국면에서 나타난 심각한 피해와 사회적 인식이 크지 않다.

좀 더 구체적으로 2010년부터 2015년 사이에 출판된 6권의 '국가정보화 백서'에서 제시된 '정보보호의 정책 방향 및 주요 내용'을 대표하는 내용으로 비교하면 '정보보호 기반 조성'과 '안전한 사이버 환경조성'으로 2가지 유형으로 구분할 수 있다.

'정보보호 기반 조성'의 의미를 2010년 국가정보화백서가 기술한 내용을 통하여 그 의미를 파악해 보면(국가정보화백서, 2010), 정보호호 현황 및 정책(사이버침해사고 발생 현황, 해킹사고 발생현황), 정보보호 관련 주요 이슈 사항(침해사고 발

<표 9> 국면별 기간에 출판된 국가정보화백서들에 나타난 정보보호 정책방향 분석

주제	정보보호 기반조성	안전한 사이버환경 조성	정보보호 기반조성	정보보호 기반조성	정보보호
세부항목		정보보호관리체계와 소프트웨어 개발보안체계			
		정보보호시스템 평가・인증 제도 운영			
		정보통신기반시설 보호			
		전자서명인증체계 구축			
	정보보호 기술 개발 및 연구	사이버 침해사고 예방 및 대응	정보보호 기술 개발 및 연구	정보보호 기술 개발 및 연구	향후 전망
	정보보호 현황 및 정책	정보보호 정책수립	정보보호 현황 및 법・제도	정보보호 현황 및 법・제도	기술 현황
년도	2010	2011 2012	2013	2014	2015
국면	상승국면		하강국면		반등국면

생, 소셜네트워크에 대한 사회공학적 공격 급증, 새로운 ICT 서비스의 등장과 정보보호 중요성 부각), 정보보호 주요정책 현황 및 추진방향(제2의 디도스 공격 예방・대응체계 고도화, 개인정보보호체계 강화, 국가 주요 정보통신기반시설 보호체계 강화, 인터넷뱅킹 및 전자결재 사고 예방・대응 체계 강화, 공인인증서 이용활성화로 인터넷 신뢰 기반 조성, 정보보호 전문 인력 양성 및 고용 확대, 스마트폰 등 신규 IT 융합서비스 보안체계 강화, e콜센터 118 개소)으로 기술하고 있다. 또한 2012년 이후 국가정보화백서를 보면 2013년에는 정보보호 및 법・제도(사이버침해사고 현황, 분야별 정보보호실태, 정보보호 법제도, 정보보호 기술개발 및 연구 등)로 기술하고 있다. 이는 2014년과 동일하다. 즉, 기존 정보보호 수준에 기반한 정책적 방향을 결정하였다고 할 수 있다.

반면 '안전한 사이버 환경조성' 의미를 2011년 국가정보화백서가 기술한 내용을 통하여 살펴보면(국가정보화백서, 2011), 정보보호 정책 수립(우리나라 정보보호 현 위치, 전자정부비스 보안수준 제고, 정보보호 중기 종합계획, 정보보호교육・홍보), 사이버 침해사고 예방 및 대응(사이버침해사고 발생 현황, 사이버침해 예방・대응체계 강화), 전자서명인증체계 구축(공인전자서명인증체계 활성화, 공인인증기관 지정 및 공인인증서 발급 현황), 정보통신기반시설보호, 정보보호시스템평가・인증제도, 정보보호 관리체계와 소프트웨어 개발보안체계 등으로 기술하고 있다. 특히, 정보보호 정책 변화에 관련하여 "2011년 3・4 DDoS 공격 이후 국가적인 사이버위기에 대응하기 위해, 국가정보원, 행정안전부, 방송통신위원회, 경찰청, 금융결제원 등 유관기관이 합동으로 '국가 사이버안보 마스터플랜(2011.8)'을 마련하는 등 국가적인 대응이 필요한 사이버 공격에 대해 범정부적인 공조체제를 가동하고 있으며, 지자체 위협정보 연계 확대를 위한 위협정보 분석시스템을 보강하였다"고 국가적 차원의 활동을 기술하고 있다. 즉, 새로운 위협인 사이버 공격에 기반한 정책적 방향을 결정하였다고 할 수 있다. 2015년에는 그동안 금융・통신・인터넷 등 다양한 분야에서 발생하는 사이버 위협에 대응하기 위하여 '정보보호가 기본이 되는 사회, 창조경제 먹거리 사업화'라는 비전과 중요 추진 과제를 담은 'K-ICT 시큐리티 발전 전략(2015. 4)'을 수립하였다고 기술하고 있다.

따라서 정보보호 중요성에 대한 국민의 인식은 정보보호 정책 방향에 따라 좌우될 수 있음을 확인할 수 있다.

② 수준 분석

연도별 국가정보화백서 수준평가는 <표 10>과 같이 93.5점에서 100점까지 측정되었다. 현장 평가가 제한되는 항목을 만점으로 부여하고 기타 세부항목에서도 관련 항목이 기재되어 있으면 만점을 부여하여 100점에 이른다.

국가정보화백서에 정보보호 준비도 평가 세부평가지표를 적용하여 살펴본 결과는 다음과 같다. 정보보호리더십에서 2010년부터 2015년까지 정보보호 최고책임자 지정, 정보보호 의사소통 및 정보제공, 정보보호 운영방침에 대한 정책은 잘 이루어졌기에 모든 항목에 대하여 최고점 5점, 5점, 4점을 부여하였다. 2010년에는 소프트웨어 강국 도약 전략이나 정부차원의 3D 산업 발전전략 등을 발표하였고, 2011년과 2012년에는 스마트 전자 정부 계획, 2013년에는 정부 3.0추진 기본 계획 등을 통해 정부서비스를 국가 핵심 추진 과제로 삼아 해당 활동들이 잘 이루어짐을 알 수 있다.

정보보호 자원관리에서 2010년부터 2015년까지 정보보호 추진계획과 정보보호 이행점검과 같은 정보보호에 대한 계획과 점검 여부는 잘 이루어져 4점을 부여하였고, 정보보호 인력 및 조직, 정보보

<표 10> 연도별 국가정보화백서 수준평가 지표 및 내용

지표	구분	평가지표		평가내용					
		항목	점수	2010	2011	2012	2013	2014	2015
기반지표	1. 정보보호 리더십	1.1	5	5	5	5	5	5	5
		1.2	5	5	5	5	5	5	5
		1.3	4	4	4	4	4	4	4
	2. 정보보호 자원관리	2.1	4	4	4	4	4	4	4
		2.2	4	2	2	4	2	2	2
		2.3	4	2	4	4	2	2	2
		2.4	4	4	4	4	4	4	4
활동지표	1. 관리적 보호활동	1.1	5	2.5	5	5	2.5	2.5	2.5
		1.2	4	4	4	4	4	4	4
		1.3	4	4	4	4	4	4	4
		1.4	5	5	5	5	5	5	5
	2. 물리적 보호활동	2.1	4	4	4	4	4	4	4
		2.2	4	4	4	4	4	4	4
		2.3	4	4	4	4	4	4	4
	3. 기술적 보호활동	3.1	5	5	5	5	5	5	5
		3.2	5	5	5	5	5	5	5
		3.3	4	4	4	4	4	4	4
		3.4	4	4	4	4	4	4	4
		3.5	5	5	5	5	5	5	5
		3.6	4	4	4	4	4	4	4
		3.7	5	5	5	5	5	5	5
		3.8	4	4	4	4	4	4	4
		3.9	4	4	4	4	4	4	4
합계			100	93.5	98	100	93.5	93.5	93.5

호 예산 수립 및 집행과 같은 정보보호에 대한 인력과 예산 여부는 비교적 잘 이루어지지 않았기에 2점을 부여하였다.

관리적 보호활동에서 2010년부터 2015년까지 자산 관리, 인적 보안, 외부자 보안은 잘 이루어졌기에 최고점 5점과 4점을 부여하였다. 특히 우리나라의 관리적 보호활동은 세계적으로도 수준이 높으며, 이는 2014년에 공공데이터 관련 보호활동이 우수한 평가를 받은 것에서도 알 수 있다. 반면에, 정보보호 교육수행의 경우 2010년과 2013년부터 2015년까지는 교육 수행이 매우 미흡하게 나타났다.

물리적 보호활동에서 2010년부터 2015년까지 정보통신시설의 환경보안 및 출입관리, 사무실보안의 경우 매우 잘 이루어지고 있었기에 모두 최고점 4점을 부여하였다.

기술적 보호활동에서 2010년부터 2015년까지 취약점 점검, 정보보호 사고탐지 및 대응, 시스템 개발 보안, 네트워크 보안, 정보시스템 및 응용프로그램 인증, 자료유출 방지, 시스템 및 서비스 운영 보안, 백업 및 IT 재해 복구, PC 및 모바일 기기 보안과 같은 기술보안 여부는 매우 잘 이루어지고 있어, 모두 최고점 5점 및 4점을 부여하였다. 2010년에는 스마트폰 무선 서비스를 제공하였고, 6년간 다수 부처의 정보 시스템을 상호 연계하여 정보시스템의 취약점을 점검하고 서비스 운영과 보안을 통해 효율성을 제고하였다는 점에서 해당 활동들이 잘 이루어짐을 알 수 있다.

그러므로 국가정보화백서에 정보보호 준비도 평가 세부 평가지표를 적용하여 분석된 평가결과를 국면별로 비교해 보면, <표 11>과 같이 상승국면

<표 11> 국면별 국가정보화백서 수준 분석

구분	분석대상	수준분석
상승국면	2010 ~ 2012 국가정보화백서	93.5(2010) → 98(2011) → 100(2012)
하강국면	2013 ~ 2014 국가정보화백서	100(2012) → 93.5(2013) → 93.5(2014)
반등국면	2015 ~ 2015 국가정보화백서	93.5(2014) → 93.5(2015)

에서는 평가점수가 93.5(2010)에서 100(2012)으로 상승하였고, 하강국면에서는 평가점수가 100(2012)에서 93.5(2014)로 하락하였으며, 반등국면에서는 93.5(2015)로 동일하였다.

따라서 상승국면에서는 수준평가가 상승하였고, 하강국면에서는 수준평가가 하락하여, 국민의 정보보호 중요성과 정부의 정보보호 정책반영에 상호연관성이 있는 것으로 나타났다.

(2) 국가정보보호백서

① 특성 분석

국가정보보호백서는 연도별로 각각의 특성이 나타났고, 2010년부터 2015년까지의 전체적인 내용을 국면별로 종합해 보면, <표 12>와 같이 동일하거나 유사한 주제 및 내용으로 기술되고 있는 것을 확인할 수 있다.

세부적인 내용을 살펴보면 다음과 같다. 상승국면에서 2010년에는 '국민생활 정보보호 활동'의 주제를 통하여 정보보호 홍보 및 인식 제고 활동, 대국민 정보보호 교육사업, 불법 스팸 메일 장비, 불건전 정보유통 대응을 기술하고 있고, 2012년에는 '대국민 정보보호 활동'의 주제를 통하여 불법 스팸메일 방지, 불건전 정보유통 대응, 정보보호 상담 및 처리, 정보보호 홍보 및 인식 제고 활동, 대국민 정보보호 교육 사업으로 주제 및 항목이 발전되었다. 따라서 상승국면에서는 국민의 정보보호 인식에 대한 중요성이 증가함으로 인해 정보보호 상담 및 처리와 정보보호 홍보 및 인식 제고 활동 내용이 새로 추가된 것을 알 수 있다. 이에 국가정보보호백서에 기술된 내용이 국민의 정보보호 인식에 대한 중요성을 온전하게 반영하

<표 12> 국면별 국가정보보호백서 특성 분석

주제	국민생활 정보보호 활동	국민생활 정보보호 활동	대국민 정보보호 활동	대국민 정보보호 활동	대국민 정보보호 활동	대국민 정보보호
내용		융합서비스 사업의 정보보호 활동				
		정보보호 상담 및 처리	정보보호 상담 및 처리	정보보호 상담 및 처리	정보보호 상담 및 처리	정보보호 상담 및 처리
	대국민 정보보호 교육 사업	대국민 정보보호 교육 사업	대국민 정보보호 교육 사업	대국민 정보보호 교육 사업		
	정보보호 홍보	정보보호 홍보	정보보호 홍보	정보보호 홍보		
	및 인식제고 활동	및 인식제고 활동	및 인식제고 활동	및 인식제고 활동	대국민 정보보호 인식제고	정보보호 인식제고
	불건전 정보유통 대응	불건전 정보유통 대응	불건전 정보유통 대응	불건전 정보유통 대응	불건전 정보유통 대응	불법 스팸 및 불건전 정보유통
	불법 스팸메일 방지	불법 스팸메일 방지	불법 스팸메일 방지	불법 스팸메일 방지	불법 스팸메일 방지	
년도	2010	2011	2012	2013	2014	2015
국면	상승국면			하강국면		반등국면

고 있다는 것으로 해석할 수 있다.

그러나 하강국면에서 2012년 '대국민 정보보호 활동'의 주제와 항목을 2014년의 주제와 항목을 비교하면 주제('대국민 정보보호 활동')와 불법 스팸메일 방지, 불건전 정보유통 대응, 정보보호 상담 및 처리, 대국민 정보보호 인식 제고 등은 동일하지만 홍보 및 교육 항목이 기술되지 않고 있다. 따라서 이 시기에는 국민의 정보보호 인식에 대한 중요성이 낮아짐으로 인해 해당 항목과 내용이 반영되지 않은 것으로 해석할 수 있다. 반등국면에서 주제와 항목은 하강국면과 유사하며, 정책 분석에서 4가지 유형이 3가지 유형으로 축소되었다.

그러므로 상승국면에서의 2012년 기준으로 비교하면 정보보호 홍보 활동, 대국민 정보보호 교육사업 여부에 따라 차이가 발생할 수 있음을 확인할 수 있었다.

② 수준 분석

연도별 국가정보보호백서 수준평가는 <표 13>과 같이 98점에서 100점까지 측정되었다. 현장평가가 제한되는 항목을 만점으로 부여하고 기타 세부항목에서도 관련 항목이 기재되어 있으면 만점을 부여하여 100점에 이르게 되었다.

국가정보보호백서에 정보보호 준비도 평가 세부평가지표를 적용하여 살펴본 결과는 다음과 같다. 정보보호리더십에서 2010년부터 2015년까지 정보보호 최고책임자 지정, 정보보호 의사소통 및 정보제공, 정보보호 운영방침에 대한 정책은 잘 이루어졌기에 모든 항목에 대하여 모두 최고점을 부여하였다. 2010년에는 스마트 모바일 시큐리티 종합 계획을 발표하였고, 2011년에는 국가 사이버 안보 마스터플랜 등의 계획이 수립되었다.

<표 13>연도별 국가정보보호백서 수준평가 지표 및 내용

지표	구분	평가지표		평가내용					
		항목	점수	2010	2011	2012	2013	2014	2015
기반지표	1. 정보보호 리더십	1.1	5	5	5	5	5	5	5
		1.2	5	5	5	5	5	5	5
		1.3	4	4	4	4	4	4	4
	2. 정보보호 자원관리	2.1	4	4	4	4	4	4	4
		2.2	4	2	2	4	2	2	2
		2.3	4	4	4	4	4	4	4
		2.4	4	4	4	4	4	4	4
활동지표	1. 관리적 보호활동	1.1	5	5	5	5	5	5	5
		1.2	4	4	4	4	4	4	4
		1.3	4	4	4	4	4	4	4
		1.4	5	5	5	5	5	5	5
	2. 물리적 보호활동	2.1	4	4	4	4	4	4	4
		2.2	4	4	4	4	4	4	4
		2.3	4	4	4	4	4	4	4
	3. 기술적 보호활동	3.1	5	5	5	5	5	5	5
		3.2	5	5	5	5	5	5	5
		3.3	4	4	4	4	4	4	4
		3.4	4	4	4	4	4	4	4
		3.5	5	5	5	5	5	5	5
		3.6	4	4	4	4	4	4	4
		3.7	5	5	5	5	5	5	5
		3.8	4	4	4	4	4	4	4
		3.9	4	4	4	4	4	4	4
합계			100	98	98	100	98	98	98

<표 14> 국면별 국가정보보호백서 수준 분석

구분	분석대상	수준분석
상승국면	2010 ~ 2012 국가정보보호백서	98(2010, 2011) → 100(2012)
하강국면	2013 ~ 2014 국가정보보호백서	100(2012) → 98(2013, 2014)
반등국면	2015 ~ 2015 국가정보보호백서	98(2014) → 98(2015)

정보보호 자원관리에서 2010년부터 2015년까지 정보보호 추진계획과 정보보호 이행점검, 정보보호 예산 수립 및 집행과 같은 정보보호에 대한 계획과 점검 여부는 잘 이루어져 최고점을 부여하였고, 정보보호 인력 및 조직은 비교적 잘 이루어지지 않았기에 2점을 부여하였다. 하지만, 2012년에 각종 사이버위협에 대응할 수 있도록 국가사이버위협 협동대응팀이 구성되었으므로 4점을 부여하였다.

관리적 보호활동에서 2010년부터 2015년까지 자산 관리, 인적 보안, 외부자 보안은 잘 이루어졌기에 모두 최고점을 부여하였다. 특히 2010년에 다양한 전자금융 서비스를 제공하고자 하였고, 2013년에는 개인정보보호와 관련된 보안교육이 실시되었다.

물리적 보호활동에서 2010년부터 2015년까지 정보통신시설의 환경보안 및 출입관리, 사무실보안의 경우 매우 잘 이루어지고 있었기에 모두 최고점을 부여하였다. 특히 2010년에 스턱스넷으로 인한 피해를 미리 예방하기 위하여 주요기반시설에 대한 비상대응체계를 운영한 것으로 나타났다.

기술적 보호활동에서 2010년부터 2015년까지 취약점 점검, 정보보호 사고탐지 및 대응, 시스템 개발 보안, 네트워크 보안, 정보시스템 및 응용프로그램 인증, 자료유출 방지, 시스템 및 서비스 운영 보안, 백업 및 IT 재해 복구, PC 및 모바일 기기 보안 모두 잘 이루어지고 있어 모든 항목에 최고점을 부여하였다. 예를 들어, 2010년에는 악성코드 감염피해를 예방하고자 관련 보안 서비스를 보완하거나 사이버 대피소 등을 구축하였다.

국가정보보호백서에 정보보호 준비도 평가 세부평가지표를 적용하여 분석된 수준 분석결과를 국면별로 비교해 보면, <표 14>와 같이 상승국면에서는 평가점수가 98(2010, 2011)에서 100(2012)으로 상승하였고, 하강국면에서는 평가점수가 100(2012)에서 98(2013, 2014)로 하락하였으며, 반등국면에서는 98(2014, 2015)로 동일하였다.

따라서 상승국면에서는 수준평가가 상승하였고, 하강국면에서는 수준평가가 하락하여, 국민의 정보보호 중요성과 정부의 정보보호 정책반영에 상호연관성이 있는 것으로 나타났다.

(3) 정보보호 실태조사

① 특성 분석

연도별 정보보호 실태조사에 대하여 2009년을 기준으로 보면 2010년부터 2013년까지 항목들이 확대되었고, 2014년과 2015년에는 항목별로 축소되거나 확대되는 변동이 있었다.

연도별 특성을 국면별로 대비해 보면 <표 15>와 같이 국면별 상승국면에서 2010년과 2011년에는 4항목이 2015년에는 6항목(정보보호 인식, 인터넷 역기능 대응 실태, 신규 서비스 정보보호 인식/대책, 정보화 역기능 피해 현황, 정보보호·개인 정보보호정책 성과 평가)으로 늘었고, 하강국면에서 2012년과 2013년에서 6항목이 2014년에는 5항목(정보보호 인식, 침해사고 예방 및 대응, 개인정보보호 및 스팸 대응, 신규 서비스 정보보호)으로 변화하였다.

<표 15> 국면별 정보보호 실태조사 특성 분석

구분	1장	2장	3장	4장	5장	6장
2010	조사개요	정보보호 인식	정보보호 관련 인터넷 역기능 대응 실태	정보보호 관련 인터넷 역기능 피해 현황	신규 서비스에 대한 정보보호 인식 및 보안대책	-
2011		정보보호 인식	정보화 역기능 대응 실태	정보화 역기능 피해 현황		-
2012	조사개요	정보보호에 대한 인식과 실천	인터넷 역기능 대응 실태	신규 서비스에 대한 정보보호 인식 및 보안대책	정보화 역기능 피해 현황	정보보호 및 개인 정보보호 정책성과 평가
2013	조사개요		인터넷 역기능 대응	인터넷 역기능 피해	신규 서비스에 대한 정보보호 인식 및 활동	
2014	조사개요	정보보호 인식	침해사고 예방 및 대응	개인정보보호 및 스팸 대응	신규서비스 정보보호	-
2015	조사개요	정보보호 인식	침해사고 예방	침해사고 대응	개인정보보호	신규서비스 정보보호

반등국면에서 2014년의 5항목이 2015년에는 6항목(정보보호인식, 침해사고 예방, 침해사고 대응, 개인정보보호, 신규서비스 정보보호)으로 변화하였다.

특히, 2012년과 2013년에 보이는 정보보호·개인정보보호 정책성과 평가와 관련하여 구체적인 그 내용을 보면 정책 인지 및 효과 평가(정책 인지 및 효과 평가), 홍보 및 캠페인(정보보호 관련 홍보물 접촉 경험, 정보보호 관련 홍보물의 도움 정도, 정보보호 관련 홍보물 접촉 매체, 정보보호 관련 홍보물 인지 여부, 정보보호 관련 홍보물 접촉 경로, 정보보호 관련 홍보물 도움 정도)항목으로 국민이 인식하는 정보보호 중요성 인식과 관련하여 정책지원을 평가하였다.

그러므로 국면별 정보보호 실태조사의 상승국면에는 신규 서비스 정보보호 인식 및 대책, 정보보호 및 개인정보보호정책 성과 평가의 세부항목이 다른 국면에서 실행한 정보보호 실태조사의 주제와 그에 따른 세부항목과 차이점이 발생하고 이 항목의 변화 및 누락은 정부의 정책적 평가와 국민의 인식 반영과 연관성이 있음을 의미한다.

② 연관성 분석

국면별 정보보호 실태조사와 정보보호 정책들 간의 연관성 분석은 각 정책서를 발간하기 위해서 참여 및 지원한 기관의 연속성을 통하여 분석하였다. 이는 정책을 수립하고 평가하는 측면에서 보면 정책적 환류를 가능하게 하는 계기가 되기 때문이다.

<표 16>을 구체적으로 살펴보면, 국가정보화백서는 2010년, 2012년, 2015년에만 참여 및 지원기관을 공개하였고, 그 외에는 공개하지 않았다. 국가정보보호백서는 2010년부터 2012년까지 방송통신위원회, 행정안전부, 지식경제부, 국가보안기술연구소, 한국인터넷진흥원이 참여 및 지원하였고, 2013년부터 2015년까지 국가정보원, 방송통신위원회, 미래창조과학부, 안전행정부(행정자치부), 국가보안기술연구소, 한국인터넷진흥원이 참여 및 지원하였다. 그리고 정보보호 실태조사는 2010년부터 2012년까지 방송통신위원회, 한국인터넷진흥원이 참여 및 지원하였고, 2013년부터 2015년까지 미래창조과학부, 한국인터넷진흥원이 참여 및 지원하였다.

<표 16> 국면별 정보보호 실태조사 특성 분석

구분	상승국면			하강국면		반등국면
	2010	2011	2012	2013	2014	2015
국가정보화 백서	한국정보화진흥원 (한국인터넷진흥원 등)	한국정보화진흥원 (미공개)	방송통신위원회, 행정안전부, 지식경제부, 한국정보화진흥원	한국정보화진흥원 (미공개)		한국정보화진흥원 (한국인터넷진흥원 등)
국가정보보호 백서	방송통신위원회, 행정안전부, 지식경제부 (국가보안기술연구소, 한국인터넷진흥원)			국가정보원, 방송통신위원회, 미래창조과학부, 안전행정부 (국가보안기술연구소, 한국인터넷진흥원)		
정보보호 실태조사	방송통신위원회 (한국인터넷진흥원)			미래창조과학부 (한국인터넷진흥원)		
공통참여기관	방송통신위원회			-		한국인터넷진흥원
다수참여기관	한국인터넷진흥원			한국인터넷진흥원		-

이러한 연도별 발간기관을 비교하면 상승국면에서는 방송통신위원회와 한국인터넷진흥원이 공통 및 다수 참여하여 정책의 상호 연관성을 높였다고 할 수 있으며, 하강국면에서는 공통기관이 없고 다수 참여기관은 한국인터넷진흥원이었다. 또한 반등국면에서는 공통기관은 한국인터넷진흥원이었다.

국가정보화백서에서 참여 및 지원 기관이 공개되지 않는 시기가 있어서 일반화하기에는 다소 어렵겠지만 공개한 연도를 비교하면 방송통신위원회와 한국인터넷진흥원의 역할에 따라 국민이 인식하는 정보보호의 중요성에 영향을 줄 수 있다는 정책적인 연관성을 이해할 수 있다. 즉, 발간의 주체로서 참여한 방송통신위원회와 발간의 지원 기관으로 참여한 한국인터넷진흥원의 역할은 차이가 있고 이러한 차이가 정책적 상관성을 제시한다고 할 수 있다. 또한 이 표를 통하여 하강국면에서 국가정보보호백서의 직접적인 집필 기관으로 국가정보원이 참여하면서 나타난 것도 향후의 연구가 필요한 부분일 것이다.

3) 정보보호 정책 연관성 분석

본 연구에서는 2010년부터 2015년까지의 정보보호 정책서와 실태조사에서 나타난 국민들의 정보보호 중요성 인식에 있어서의 변동 시기를 기준점으로 하여 앞에서 적용한 바와 같이 중요성 인식이 상승되는 국면, 하락되는 국면, 그리고 반등하는 국면 3개의 국면을 설정하였다. 그리고 이에 따른 정보보호 위협, 정보보호 중요성 인식, 정보보호 정책 간의 상호 연관성에 대하여 다음의 2가지로 분류하고 분석한 내용을 결론적으로 다음과 같이 정리하였다.

(1) 정보보호 위협 환경과 정보보호 정책 특성 간의 연관성 분석

정보보호 위협 환경과 정보보호 정책 특성 간의 연관성 분석은 정보보호 위협을 받은 대상과 피해 유형별로 빈도 등의 특성과 정보보호 관련 정책서에 담긴 정책 방향과 주요 내용들의 특성을 비교하여 살펴보았다. 그 결과 <표 17>에서와 같이 각각의 정보보호 위협 환경에 따른 현실적인 정책의 유무 여부가 국민의 정보보호 인식에 영향을 미쳤다고 볼 수 있다.

상승국면에서 '정보보호 기반조성'의 정책방향이 '안전한 사이버 환경 조성'으로 변화하면서 국가정보보호백서도 정보보호 홍보 및 인식제고 활동, 정보보호 상담 및 처리 활동이 추가되고, 정보보

<표 17> 정보보호 위협과 정보보호 정책 특성 간의 연관성 분석

구분	정보보호 위협		국가 정보보호 정책자료			정책방향
	연도	공격건수(공격대상) 대표사례	국가정보화 백서	국가정보보호 백서	정보보호 실태조사	
상승국면 (2010-2012)	2010	1건(개인) 신세계몰 정보유출	정보보호 기반조성	국민생활 정보보호 활동	4항목	정보보호 인식 정책 → 사이버 인식 정책
	2011	8건(개인~정부) 3·4 DDos공격, 농협 전산망 마비사태, 10·26 DDos 공격 등	안전한 사이버환경 조성	대국민 정보보호 활동 (정보보호 홍보 및 인식제고 활동, 정보보호 상담 및 처리)	4항목	
	2012	5건(개인~정부) EBS, 중앙일보, KT 등 정보유출			5항목 (정책성과평가 추가)	
하강국면 (2013-2014)	2013	3건(개인~정부) 3·20 전산대란 6·25 사이버테러	정보보호 기반조성	대국민 정보보호 활동	5항목 (정책성과평가 추가)	사이버 인식 정책 → 정보보호 인식 정책
	2014	5건(개인~정부) 한수원 사이버테러 등			4항목	
반등국면 (2015)	2015	1건(개인) 뽐뿌 정보유출	정보보호	대국민 정보보호	5항목 (신규위협추가)	

호 실태조사에서도 신규위협이 추가된 것으로 조사되었다. 하강국면에서 '정보보호 기반조성의 정책방향'으로 전개되어 대국민 정보보호 활동과 정보보호 실태평가의 활동과 연계되지 못하였다. 반등국면도 또한 마찬가지이다.

따라서 상승국면인 2011년과 2012년에 많은 사이버 해킹 사고로 인해 개인정보 유출과 기관 전산망 마비 등의 피해가 많이 발생하고 개인부터 국가에 이르기까지 현실적인 사이버 위협에 대한 국가의 종합적인 사이버 인식 중심의 정책이 수립되어 국민이 인식하는 정보보호 중요성 인식에 상호 연관성이 있다고 볼 수 있다.

구체적인 사례를 보면, 정책적 인식에 있어서 2011년의 국가정보화백서는 사이버 인식 중심의 정책을 잘 설명해주고 있는데, "2011년 3·4 DDoS 공격 이후 국가적인 사이버위기에 대응하기 위해, 국가정보원, 행정안전부, 방송통신위원회, 경찰청, 금융결제원 등 유관 기관이 합동으로 '국가 사이버안보 마스터플랜'을 마련하는 등 국가적인 대응이 필요한 사이버 공격에 대해 범정부적인 공조체제를 가동하고 있으며, 지자체 위협정보 연계 확대를 위한 위협정보 분석시스템을 보강하였다"고 국가적 차원의 활동을 기술하고 있다. 즉, 새로운 위협인 사이버 공격에 기반한 정책적 방향을 결정하였다고 할 수 있다. 또한, 국가정보보호백서는 정보보호 상담 및 처리, 정보보호 홍보 및 인식 제고 활동을 새롭게 추가하거나 병행하여 국민의 정보보호 중요성 인식을 고취시켰다.

반면, 정보보호 인식 중심의 정책은 2013년 국가정보보호백서에서 잘 나타나 있는데, "정부는 해킹

에 의한 개인정보의 대규모 유출 등 날로 심각해지는 사이버 공격에 대응하기 위하여 세계 최초로 7월 둘째 수요일을 '정보보호의 날'로 지정하였다. 이와 함께 7월을 '정보보호의 달'로 지정하여 관계부처 합동으로 다양한 정보보호 행사를 개최하고 이를 통하여 국민들의 정보보호 인식 제고와 실천을 높여 나갈 것"이라고 강조하고 있다. 이 행사의 내용을 보면 국가정보원, 방송통신위원회, 행정안전부, 지식경제부 등 4개 기관은 2012년 7월 11일 제1회 정보보호의 날 기념식을 공동주최하여 이 행사에 국가, 사회 각 분야의 정보보호 연구·발전과 사이버침해대응에 공로가 있는 공로자 대상으로 유공 포창을 하고 국제 정보보호 컨퍼런스와 정보보안 인력채용 등의 행사를 한다는 것인데 이 행사가 바로 실질적인 국민의 정보보호 중요성 인식과 연결될 수 있는지를 재검토해 볼 필요성이 있다.

이렇게 정보보호 관련 국가 정보보호 백서들에 기술된 정책방향과 내용으로 국민의 정보보호 인식에 대한 중요성을 고취시키거나 국민의 인식을 온전하게 반영한 것인지를 판단할 수 있으며 또한, 매년 실시되는 정보보호 실태조사가 새로운 위협에 대한 인식 조사 등을 통하여 정보보호 위협과 정책서 간의 연관성을 잇는 정책적 매개체 역할을 하였다고 볼 수 있다.

(2) 정보보호 중요성 인식과 관련 정책 시행 간의 연관성 분석

2017년 7월 정보보호의 달을 맞아 국내 한 언론기관에서 국민들을 대상으로 정보보호 인식 제고에 대한 설문조사를 진행한 결과에 의하면 '인식 제고가 쉽지 않다'는 의견이 28.3%를 차지해 두 번째로 많은 의견으로 나타났다(김태형, 2017. 8. 4). 이러한 국민의 설문의견을 고려한다면 국민의 정보보호 중요성 인식과 정보보호 정책 시행 간의 연관성에 있어서 국민의 정보보호 중요성 인식을 제고할 수 있는 정부의 정책 시행 내용이 문제 해결의 관건이 될 것이다.

<표 18> 정보보호 중요성 인식과 관련 정책 시행 간의 연관성 분석

<table>
<tr><th rowspan="3">구분</th><th colspan="5">국가 정보보호 정책자료</th></tr>
<tr><th rowspan="2">국가정보화
백서
(년도)</th><th colspan="3">국가정보보호백서</th><th rowspan="2">정보보호
실태조사
(년도)</th></tr>
<tr><th>교육현황
(년도)</th><th>동아리 지원
(년도)</th><th>온라인 학습장
(년도)</th></tr>
<tr><td>상승 국면
(2010-2012)</td><td>우리나라 정보보호
현위치 설명
(2011, 2012)</td><td>76회
(2010)
85회
(2011)
67회
(2012)</td><td>35개
(2010)
40개
(2011)
42개
(2012)</td><td>22,728명
(2010)
37,616명
(2011)
50,836명
(2012)</td><td>정보보호·개인정보보호
정책성과 평가
(2012)</td></tr>
<tr><td rowspan="2">하강 국면
(2013-2014)</td><td rowspan="2">없음</td><td>54회
(2013)</td><td>40개
(2013)
42개
(2014)</td><td>없음</td><td>정보보호·개인정보보호
정책성과 평가
(2013)</td></tr>
<tr><td colspan="3">정보보호 기념식 설명
(2013, 2014)</td><td>없음</td></tr>
<tr><td rowspan="2">반등 국면
(2015)</td><td rowspan="2">없음</td><td>없음</td><td>없음</td><td>없음</td><td rowspan="2">없음</td></tr>
<tr><td colspan="3">정보보호 기념식 설명</td></tr>
</table>

정보보호 중요성 인식과 관련한 정책 시행 간의 연관성을 분석한 <표 18>을 보면, 상승국면에서 국가정보화백서는 2011년과 2012년 '우리나라 정보보호 현위치' 분석을 통하여 정보보호 예산 수준, 사이버침해건수, 사이버위협에 대한 대책 마련을 강조하였다.

국가정보보호백서는 정보보호 중요성 인식을 위한 교육, 동아리지원, 온라인 학습장 운영 등 다양한 정책 시행을 하였으며, 정보보호 실태조사에서 이를 평가하였다. 그러나 하강국면에서 국가정보화백서는 '정보보호 인식'과 관련한 정책적인 시행이 없었고, 국가정보보호백서는 교육, 동아리지원, 온라인 학습장 지원은 상승국면과 비교하면 일반적인 지원이 저조하다. 또한 반등국면에서도 국가정보화백서와 국가정보보호백서의 정책 시행은 특별한 것이 없다. 반면, 하강국면과 반등국면에서 정보보호 기념식과 관련한 설명은 상승국면과 대조적이었다.

정보보호에 대한 국민 인식을 고취시키기 위하여 정부가 국민의 '정보보호 인식'을 중요시하고, 국민을 대상으로 실시한 관련 교육과 홍보 지원은 어느 정도 긍정적인 영향을 미쳤다고 판단할 수 있고, 또한 하강국면에서 이러한 기술이 되지 않은 것은 정보보호 기념식을 설명한 것처럼 정부의 특정 행사에 치우쳐 국민을 대상으로 하는 일반적인 지원을 소홀히 했음을 보여주고 있다. 따라서 국민의 정보보호 중요성 인식과 정보보호 정책 시행 간의 연관성이 높은 것은 상승국면에서 나타난 사이버 인식 중심의 국가 정보보호 정책들이었음을 실증적으로 확인하였다.

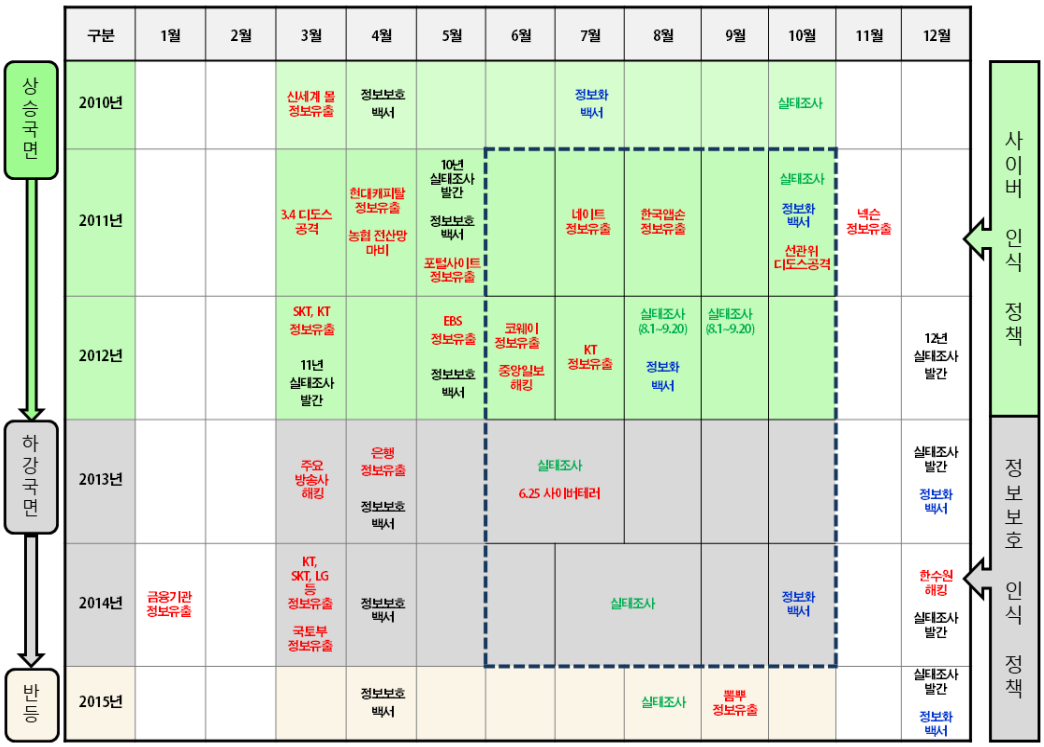
5. 결 론

본 연구는 정부의 적합한 정책결정과 시행이 국민들의 정보보호 중요성에 대한 인식에 긍정적 영향을 끼쳐 그 인식수준을 향상시킬 수 있다는 것을 검증하는 데 목적이 있었다. 특히, 2010년부터 2015년까지의 정보보호 실태조사에서 나타난 국민들의 정보보호 중요성 인식에 있어서의 변동을 그 기준점으로 하여, 중요성 인식이 상승되는 국면, 하락되는 국면 그리고 반등하는 국면, 이상 3개의 국면들로 구분하여 연구범위를 구축하고 대상을 설정한 후 여기에서 나타나는 정책들(국가정보화백서, 국가정보보호백서, 정보보호 실태조사)을 활용하여 연구결과를 도출하였다.

앞서 분석한 정보보호 관련 정책 연관성을 정리하면 <그림 5>와 같다.

구체적인 내용을 보면 상승국면은 정보보호위협의 정도가 심화가 되면서 정부의 정책방향이 사이버인식정책으로서 변화하였고 그에 따른 대응 및 예방하는 정책내용이 시행되었다. 이러한 정부의 활동이 2012년에 이르러 정보보호 실태조사에서 나타났다. 하강국면은 정보보호위협의 정도가 여전히 개인 및 국가적으로 큰 영향을 주고 있는데도 과거 정보보호 정책 중심으로 환원하고 그에 부합한 정책내용이 시행되었다. 반등국면에서 상승국면과 하강국면처럼 정보보호위협의 정도가 심하지 않았고 하강국면의 정보보호정책이 지속되면서 정보보호 중요성 인식에 영향을 주지 않아 반등하였다고 볼 수 있다.

이에 변화하는 정보보호 환경과 그 시대적 흐름에 따른 정책 반영 등이 결합되었을 때 정책의 실효성이 발휘되고 국민의 정보보호 인식이 상승하는 것으로 해석할 수 있다. 특히, 상승국면에서 나타나듯이 정책 시행 관점에서 사이버 공간에서 새로운 위험이 증가하는 현실을 반영된 사이버 인식 중심의 정책 시행이 정보보호 인식 중심의 정책 시행보다 국민의 정보보호 중요성 인식에 더 큰 영향을 미친 것으로 분석되었다.



<그림 5> 정보보호 인식 국면별 정보보호 환경과 정책 연관성 요약

또한, 국가정보화정책이 국가정보보호정책보다 더 연관성이 나타난 것으로 조사되었다. 이러한 결과는 '국가정보화'라는 포괄적인 정책은 국가적으로 정보화의 신뢰도와 효율성을 높이기 위하여 과학기술의 변화에 따른 새로운 위협을 조기에 인식하고 그에 맞게 대응계획을 수립할 필요성이 있기 때문일 것이다.

따라서 국민의 정보보호 중요성 인식과 정책 간의 연관성이 존재함을 파악할 수 있었다. 즉, 국가정책에 포함되어야 할 필수적인 정보보호 정책 내용이 최종적으로 도출되어 정보보호 정책서에 반영되었고, 적절한 정보보호 실태조사가 이루어진 것을 확인할 수 있었다.

본 연구 결과를 토대로 시사점을 정리하면 다음과 같다. 첫째, 정부는 국민들의 정보보호 인식을 향상시킬 수 있는 특정 정보보호 정책들을 구축하고 시행할 책임이 있다. 둘째, 정보보호 정책을 수립할 때 현재 사이버 공간에서 발생하는 상황 또는 환경 분석이 선행되어야 하고 정책을 수립하고 시행하는 기관(부서)은 정책방향과 내용이 결정되면 그것을 일관되게 추진하여야 한다. 즉, 국내 정치적인 영역(특정 기관에 의한 주도, 특정 국가적 목적에 의한 정책 결정 등)에 의하여 영향을 받지 않도록 해야 한다는 것이다.

이와 같은 시사점이 현 정부에게 전달하는 제언은 다음과 같을 것이다. 정부는 과거를 답습하는 정보보호 정책에서 탈피하고 정보보호 환경에서 사이버 환경으로 변화하는 미래지향적인 정보보호 정책과 국민들의 정보보호 인식 수준과 연계되는 현실적인 정책을 수립하여야 한다. 이를 실

현하기 위해서는 이에 상응하는 사이버 안보 정책의 원칙과 기준, 국제적 법과 제도 적용, 국민의 사이버 안보 인식 연구 등을 구축해야 할 것이다.

이번 연구는 국가 정보보호 관련 정책의 특성과 그 상호 연관성을 분석하여 문헌 중심의 연구에서 나타나는 일반적인 한계점을 가지고 있다. 이에 국내에서 발생하는 해킹과 그에 따른 인식 변화 간의 관계를 설문조사 등 양적분석을 통하여 검증할 필요가 있다.

최근 사이버 공간에서 정보보호의 안전이 급격하게 위협받고 있는 상황에서 본 연구의 내용과 결과가 정보보호 중요성에 대한 국민들의 인식 제고를 위하여 실효성 있는 정부의 정보보호 정책 수립에 도움이 될 것으로 기대한다.

참 고 문 헌

강다연 · 장명희 (2014). 정보보안정책 준수가 정보보안능력 및 행동에 미치는 영향 분석: 해운항만조직 구성원을 대상으로. <한국항만경제학회지>, 30(1), 97-118.

고려대 산학협력단 (2013). 국가 사이버범죄 대응전략 설계. Available: http://www.prism.go.kr/homepage/main/retrieveMain.do

국가정보원 · 미래창조과학부 · 방송통신위원회 · 안전행정부 (2013~2014). 국가정보보호백서. 서울: 대한민국정부.

국가정보원 · 미래창조과학부 · 방송통신위원회 · 행정자치부 (2015~2017). 국가정보보호백서. 서울: 대한민국정부.

국가정보원 · 방송통신위원회 (2008). 국가정보보호백서. 서울: 대한민국정부.

국가정보원 · 방송통신위원회 · 행정안전부 · 지식경제부 (2009). 국가정보보호백서. 서울: 대한민국정부.

김영곤 (2010). 항공 응용 분야: 정보보안 거버넌스의 구성요소가 종업원의 보안 인식과 행위에 미치는 영향에 관한 연구. <한국항행학회논문지>, 14(6), 935-950.

김정수 (2016). <정책학 입문>. 서울: 문우사.

김종기 · 강다연 (2008), 보안정책, 보안의식, 개인적 특성이 패스워드 보안효과에 미치는 영향. <정보보호학회논문지>, 18(4), 123-133.

김지수 · 김종배 · 신용태 (2012). 조직내 정보보호최고책임자(CISO)의 역할인식이 정보보호성과에 미치는 영향에 관한 연구. <경영컨설팅연구>, 12(4), 21-34.

김진숙 (2005). 근무성적평정결과 환류 및 활용에 관한 연구. 이화여자대학교 대학원 석사학위논문.

김태형 (2017. 8. 4). 대국민 정보보호 인식제고 가장 효과적인 방법은? 보안뉴스, Available: http://www.boannews.com/media/view.asp?idx=47272.

노재인 · 서진완 (2016). 지방자치단체의 정보보호 현황 및 인식의 변화 분석. <정보화정책>, 23(1), 20-37.

노화준 (2012). <정책평가론: 프로그램 성과와 정책혁신의 효과평가>. 서울: 법문사.

문건웅 (2017). 기업의 정보보호 활동과 정보침해사고 간의 관계: 정보보호인식의 매개효과를 중심으로. 고려대학교 정보보호대학원 석사학위논문.

미래창조과학부 (2015). K-ICT 시큐리티 발전 전략(안). Available: http://www.kisa.or.kr/notice/notice_View.jsp?mode=view&p_No=4&b_No=4&d_No=1556

미래창조과학부・한국인터넷진흥원 (2013～2016). 정보보호 실태조사. 서울: 대한민국 정부.

박희봉・이희창・조연상 (2003). 우리나라 정부신뢰 특성 및 영향 요인 분석. <한국행정학보>, 37(3), 45-66.

방송통신위원회・한국인터넷진흥원 (2009～2012). 정보보호 실태조사. 서울: 대한민국 정부.

방송통신위원회・한국정보보호진흥원 (2008). 정보보호 실태조사. 서울: 대한민국 정부.

방송통신위원회・행정안전부・지식경제부(2010～2012). 국가정보보호백서. 서울: 대한민국정부.

백민정・손승희 (2010). 조직의 정보윤리실천이 구성원의 정보보안 인식과 행동에 미치는 영향에 관한 연구. <경상논총>, 28(4), 119-145.

손승희 (2013). 스마트워크 근무환경 특성이 개인의 정보 보안인식 행동에 미치는 영향에 관한 연구: 자율성 과 이동성 그리고 책임을 중심으로. <경상논총>, 31(4), 17-39.

양기근 (2001). 정보보호 전문인력 양성 방안. 경희대학교 대학원 석사학위논문.

양승일 (2014). <정책변동론>. 서울: 박영사.

엄석진・윤영근 (2012). 행정의 공정성에 대한 시론적 연구: 개념 정의와 인식조사결과 분석을 중심으로. <충남대학교 사회과학연구>, 23(4), 245-265.

원병철 (2018. 1. 8). 정보보호 인식은 높아졌지만 랜섬웨어 피해도 증가했다. 보안뉴스, Available: http://www.boannews.com/media/view.asp?idx=65956

위키피디아 (2017). 인식. Available: https://ko.wikipedia.org/wiki/%EC%9D%B8%EC%8B%9D

이미정・이선중 (2010). 지방공무원의 정보보호 인식 및 행태에 관한 연구. <한국사회와 행정연구>, 20(4) 453-478.

이충희・신민수 (2010). 조직 내에서 내・외재적 동기와 보안행위와의 관계에서 보안인식이 미치는 영향력에 대한 연구. <한국경영정보학회 학술대회발표논문>, 437-442.

이태헌・윤영주・김희웅 (2016). 텍스트 마이닝을 이용한 정보보호인식 분석 및 강화 방안. <정보화정책>, 23(4), 76-94.

임동진 (2012). 정책의 원리 및 정책분석 평가 이해. <한국청소년정책연구원 세미나자료집>, 12(S14),1-47.

임동진・강영철 (2008). 정부업무평가결과 환류의 정착방안 연구. 서울: 한국행정연구원.

임채호 (2006). 효과적인 정보보호인식제고 방안. <정보보호학회지>, 16(2), 30-36.

전성형 (2014). 국가정보화 정책 인식구조에 대한 고찰. <한국EA학회>, 11(4), 393-407.

전인석・이병권・김동원・최진영 (2016). 마트공장 정보보호 인식교육을 위한 커리큘럼 개발. <정보보호학회논문지>, 26(5), 1335-1348.

정명주 (2012). 한국 외국인 정책의 정책체계 분석: 정책내용, 정책수단, 정책과정을 중심으로. <충남대학교사회과학연구>, 23(4), 291-317.

정보통신부・한국정보보호진흥원 (2007). 정보보호 실태조사. 서울: 대한민국 정부.

정보통신정책연구원 (2005). <정보사회와 정보화정책>. 서울: 법영사.

정정길 (2015). <정책학원론>. 서울: 대명출판사.

통계청 (2016). 정보보호실태조사 통계정보 보고서. 대전: 대한민국정부.

하연섭・조윤직・문명재・엄태호・정헌주・장용석 (2015). <위험사회와 국가정책>. 서울: 박영사.

한국전산원 (1993). 국가정보화백서. 서울: 한국정보화진흥원.

한국전산원 (1997). 국가정보화백서. 서울: 한국정보화진흥원.

한국정보보호센타 (1998). 98 정보화 역기능 실태조사. 서울: 한국정보보호센타.

한국정보보호진흥원 (2002). 정보 보호 정책 수립 지침. 기반보호연구, 2-7.

한국정보보호진흥원 (2002～2003). 개인정보보호백서. 서울: 한국정보보호진흥원.

한국정보화진흥원 (2009～2016). 국가정보화백서. 서울: 한국정보화진흥원.

한국정보화진흥원 (2017). 국가정보화백서 발간. Available: http://alio.go.kr/mobile/tender_view.do?idx=2275652&pageNo=1

한세억 (2002). 정보화정책의 변위(變位)와 특성: 행위자 수준을 중심으로. <한국정책학회보>, 11(3), 21-47.

한세억 (2010). 한국 정보화정책의 변천과 특징: 행위자 연결망을 중심으로. <정보화정책>, 17(4), 23-43.

행정자치부 (2014). 정보화담당공무원의 정보보호 인식 분석 및 정책방향 연구. <제31회 지방행정정보화 연찬회 시도별 연구보고서>, 181-252.

황창호 · 김태형 · 문명재 (2015). 정부신뢰에 영향을 미치는 요인에 대한 연구-정책홍보, 정책수단, 정책산출에 대한 국민만족도를 중심으로. <한국지방정부학회 학술대회 논문집>, 545-561.

Bauer, S., & Chudzikowski, K. (2015). Mind the Threat! A Qualitative Case Study on Information Security Awareness Programs in European Banks. *Proceedings of the Americas Conference on Information Systems (AMCIS)*.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *Management Information Systems Quarterly*, 34(3), 523-548.

Cavusoglu, H., Son, J. Y., & Benbasat, I. (2009). Information security control resources in organizations: A multidimensional view and their key drivers. working paper, Sauder School of Business. *University of British Columbia*.

Gonzales, J., & Sawicka A. (2002). A framework for Human Factors in Information Security. *WSEAS International Conference on Inforamation Security*, Rio De Janeiro, Brazil.

Jiransecurity (2016. 6. 30). 사이버 위협 지형도. JS market intelligence. Available: http://mi.jiransecurity.com/1407

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1), 31-41.

Study on the Correlation between Information Security Awareness and Information security policy

ki-jong Lee, Jae Jeong Park

ROK Cyber Command, Chungnam National University

The purpose of this research was to verify the mutual correlation between the public awareness of information security and the policies established and executed by the government. This research organized concepts, such as the properties of policy and awareness, characteristics of information security policy, and effects of information security awareness. In addition, a valid relationship was drawn between policy and public awareness of information security through detailed analysis of a policy paper and a Survey of information Security based on the aforementioned concepts. The existence of particular policy factors influencing public awareness of information security was verified. In particular, public awareness of information security improved when domestic information security environment and government policy had a mutual correlation. In light of the increase in emerging cyber threats, the implementation of policies reflecting the results of this research has high prospect of significantly improving public awareness of information security.

Keywords: Information Security Awareness, Policy of Information Security, National Informatization White Paper, National Information Security White Paper, Survey on Information Security