「한국공공관리학보」 제31권 제4호(2017. 12): *195~216*

우리나라 정보보안제도의 문제점과 개선방안:
공공부문을 중심으로*

*윤 광 석*** · *이 건****

논 문 요 약

현대는 지식정보사회로서 고도로 발전한 정보기술을 기반으로 발전을 거듭하고 있다. 그러나 이와 함께 부정적인 결과도 낳고 있는데 가장 중요한 문제 중 하나는 정보보안이다. 각국은 정보보안문제를 일찍부터 인식하고 관련 법률과 조직을 정비하여 체계적으로 대응하고 있으나 우리나라의 경우 그 대응이 상대적으로 늦은 편이다. 특히 법률상 중복 및 공백, 컨트롤타워 문제, 전문인력 부족, 보안산업 낙후 등 수많은 문제를 갖고 있어 해결이 시급한 상황이다. 그러므로 본 연구의 목적은 정보보안제도의 문제점을 살펴보고 이를 개선하기 위한 정책대안을 제시하는 것이다. 이러한 목적을 달성하기 위하여 공무원 등 전문가를 대상으로 인터뷰조사를 실시하였다. 인터뷰조사는 문헌분석, 자문회의 등을 통하여 개발되었으며, 연구분석틀과 일치하도록 법률, 조직, 정책 등 세 가지 측면으로 구성되었다. 연구 결과 정보보안기본법 제정, 컨트롤타워 설립, 보안기술 개발 및 전문인력 양성 등 다양한 정책의 추진이 필요한 것으로 밝혀져 이와 관련된 대안을 제시하였다.

주제어: 정보보안, 사이버보안, 정보기술

* 본 논문은 한국행정연구원에서 생성된 자료를 활용하였으며, 한국행정연구원 연구자료 관리규칙에 의거 사용허가를 받았습니다.

** 주저자
*** 교신저자

Ⅰ. 서 론

현대는 지식정보사회로서 기술을 기반으로 급격히 발전하고 있다. 현대사회의 중요한 특징 중 하나는 모든 정보를 디지털화하여 저장·공유·활용한다는 것이다. 이러한 정보화는 생활의 편리함과 업무의 효율성 등 긍정적인 효과를 가져왔지만 동시에 사생활침해와 정보유출 등 부정적인 결과도 초래했다.[1] IT 기술이 급격히 발전함에 따라 정보보안은 현대 사회가 직면하고 있는 가장 큰 사회적 문제 중 하나이다 (강현선, 2014; 김건우·김정덕, 2014; 김원필, 2015; 나현대·정현수, 2016; 전정훈, 2011). 세계 각국은 이러한 정보보안 문제에 대응하기 위하여 관련 법률, 정부조직, 그리고 정책 등을 수립하여 운영해오고 있다. 예를 들어 미국은 2000년 정보보안개혁법(Government Information Security Reform Act), 2012년 사이버보안법(Cyber Security Act) 등을 제정하였고, 연방정부 산하에 국토안보부(Department of Homeland Security), 사이버사령부(U.S. Cyber Command) 등을 설치하였다.

우리나라도 1986년 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 2005년 「국가사이버안전관리 규정」 등을 제정하였고, 2004년 국가정보원 산하에 국가사이버안전센터를 설치하여 보안문제에 대응하여 오고 있다.[2]

그러나 관련 전문가들은 여전히 우리나라 정보보안제도에 수많은 문제들이 있다고 주장하고 있다. 예를 들어 법률의 경우 보안 관련 법률 간 중복 및 공백 그리고 핵심적 근간이 되는 「사이버 안전관리 규정」의 법 형식 문제 등이 제기되고 되고 있다(육소영, 2010; 윤해성 외, 2012; 한국인터넷진흥원,2010; 한국인터넷진흥원, 2011). 조직적 차원의 문제로는 국가정보보안을 지휘할 수 있는 컨트롤타워를 정비해야 한다는 문제가 제기되고 있다(교육부, 2011; 이기식, 2006; 한국인터넷진흥원, 2010; 한국인터넷진흥원, 2011). 정책적 이슈로는 취약한 보안기술 수준, 부족한 전문인력 수 및 능력 등이 제기되고 있다(이기식, 2006; 정익재, 2011; 한국정보화진흥원, 2012).

이렇듯 제기된 문제들에 대하여 적절히 대응하지 못한 결과 그동안 우리나라는 수많은 정보보안 사고를 겪어왔다. 예를 들어 2009년 7·7 DDOS 대란, 2011년 농협 전산망마비사고, 2013년 3·20 및 6·25 사이버테러 등 주요 금융사의 초대형 정보유출사고 등이 발생하였다 (안유성, 2014). 2014년 말에서 2015년 상반기까지 한국수자원공사는 무려 6차례의 사이버공격을 받은 바 있다(YTN, 2015.3.23.). 또한 가장 최근의 사례로 2017년 6월 도메인 전문기업 '인터넷나야나'는 랜섬웨어 공격을 받아 약 13억원을 지불하였다(경향신문, 2017.6.30.).

---

1) 최근 영국의 런던로이즈(국제보험업자협회)는 사이버공격으로 산업계 손실(클라우드 서비스 파괴, 기업 OS 공격 등)이 최고 1천 210억 달러(약 135조 4천 200억원)까지 될 수 있다고 보고하였다(연합뉴스, 2017년 7월 17일).

2) 특히 새로 출발한 문재인 정부는 정보보안인력 양성 및 컨트롤타워 설립 등 정보보안 관련 공약을 제시하고 이를 기초로 관련 정책을 본격 추진하려고 준비하고 있다.

이러한 사건 및 문제들을 고려할 때 앞으로 더 큰 보안사고가 발생할 가능성이 매우 높은 상황이라고 할 수 있다. 즉, 정보보안제도를 활성화시키기 위한 정책대안의 개발 및 집행이 절실한 상황이다.

따라서 본 연구의 목적은 우리나라 정보보안제도를 둘러싼 문제들을 분석하고, 이를 해결할 수 있는 정책대안을 개발하는 것이다. 물론 정보보안과 관련된 선행연구가 일부 있는 상황이나, 앞서 언급한 측면의 문제들을 다루고 있는 연구는 거의 없는 상태이며, 최근 발생한 새로운 문제들을 다루고 있는 연구는 더욱 없는 실정이다. 또한 선행연구에서 제기하고 있는 문제 및 대안들의 경험적 타당성을 검증하고 있는 연구 역시 거의 없는 상황이다. 따라서 본 연구는 이러한 두 가지에 역점을 둘 것이며, 여기에 본 연구의 차별성이 있다고 할 수 있다.

본 연구는 정보보안과 관련하여 연구자들의 분석과 전문가 자문을 통하여 가장 시급하고, 중요하다고 판단되는 문제를 취사선택하여 연구의 주된 대상으로 삼고자 한다. 또한 그 일부 문제들 역시 자세히 살펴보면 세부적으로 수없이 많은 문제들을 가지고 있기 때문에 본 연구는 선택된 문제들을 전반적으로 살펴보고, 큰 틀에서 대안을 제시하고자 한다. 문제분석의 틀은 법률, 조직, 정책 등 세 가지 측면으로 구성되어 있다. 본 연구를 통해 첫째, 정보보안제도의 근간이 되는 관련 법률의 개선, 둘째, 제도를 이끌어가는 조직의 정비, 셋째, 주요 문제를 해결할 수 있는 정책대안의 개발 등에 기여하고자 한다.

Ⅱ. 정보보안제도의 이론적 배경 및 선행연구 검토

1. 정보보안의 주요 개념

정보보안제도를 이해하기 위해서는 먼저 정보, 정보의 가치, 정보보안, 정보보안과 정보보호의 구분 등 중요한 개념을 살펴봐야 한다. 우선 정보에 대해서 살펴보면 Stair & Reynolds(2003)는 “자료에 내재된 사실을 의미 있는 방식으로 재구성 한 것”이라고 하였고, Whitten et al(2001)은 “처리와 의도적 지성에 의해 조직화된 자료”라고 정의 한다. 「국가정보화기본법」 제3조 제1항은 “정보란 특정 목적을 위하여 광(光) 또는 전자적 방식으로 처리되어 부호, 문자, 음성, 음향 및 영상 등으로 표현된 모든 종류의 자료 또는 지식을 말한다”고 정의하였다. 정리하면 학문적 측면에서 정보는 자료에 기초하여 의사결정 등 의미 있는 행위에 활용할 목적으로 이에 적합한 형태로 가공한 것이라고 할 수 있다. 그러나 우리나라 관련 법규에서 말하는 정보는 자료와 지식 간 상호 구분을 두지 않고 있어 개선이 필요하다고 할 수 있다.

이러한 정보의 가치에 대하여 Stair & Reynolds(2003)는 수익창출, 비용절감, 의사결정지원 등으로 개념화 될 수 있다고 주장하면서 ‘의사결정을 하는데 줄어든 시간’ 또는 ‘기업의 수익 중 정보에 의해 늘어난 부분’등에 의해 그 가치를 측정할 수 있다고 하였다.

다음으로 본 연구의 핵심적 개념인 정보보안에 대해 살펴보면 한국인터넷진흥원(2011)은 정보보안이란 정보의 비밀성, 무결성 및 이용가능성을 유지하기 위하여 권한 없는 접속, 이용, 공개, 방해, 변경 및 파괴로부터 정보, 정보시스템 및 정보통신망을 보호하는 것이라고 하였다. Pfleeger & Pfleeger(2006)는 보안이란 가치 있는 재산을 은행과 같은 안전한 곳에 보관하는 것이라고 하였다. 이처럼 정보보안의 학문적 정의는 다소 복잡한 것 같지만 간략히 요약하면 정보보안은 정보를 외부의 인가되지 않은 유형적 또는 무형적 접근으로부터 안전하게 지키는 것이라고 할 수 있다.

정보보안의 정의와 관련된 중요한 이론적 쟁점 중 하나는 “정보보안이 정보보호와 어떻게 구분되는 것이냐?”하는 것이다. 그동안 우리 정부는 ‘보호’를 ‘보안’을 포함하는 포괄적 개념으로 사용해왔다. 예를 들어 「국가정보화기본법」, 「정보통신기반보호법」 등 여러 실정법의 각 조항을 살펴보면 보호의 개념에 보안도 포함하고 있는 경우가 많이 있다. 그러나 엄밀한 의미에서 보면 정보보안은 정보보호와 구분되는 개념이다. 한국정보보호진흥원(2002)에 의하면, 정보보안은 사람에 의하여 고의적으로 발생하는 정보의 유출, 파괴, 변조에 대한 대응이 강조되는 개념이며, 정보보호는 고의적 침해를 포함할 뿐만 아니라 우연히 발생하는 자연재해 또는 사람의 실수에 의한 재해에 대한 대응까지 포함하는 개념으로 규정하고 있다. 즉, 정보보호는 정보보안을 포함하여 사람이 통제할 수 없는 자연재해 또는 사고로부터 정보가 훼손되지 않도록 지키는 것까지 포함하는 포괄적인 개념으로 볼 수 있다.

2. 정보보안의 대상, 종류, 위협

정보보안의 구체적인 대상은 관련 법률인 정보통신기반보호법」에 명시되어 있다. 동법 제2조는 정보통신기반시설이 보안의 대상이며 이에는 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 등이 포함된다고 규정하고 있다. 또한 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」에 의하면, 정보통신망은 보안의 대상이라고 규정되어 있으며 정보통신망이란 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제라고 정의하고 있다.

정보보안의 종류는 크게 기술적 보안, 행정적 보안, 물리적 보안 등 세 가지로 나누어진다. 기술적 보안은 통제, 암호화, 방화벽 등을 포함하는데 통제란 시스템의 취약점을 탐색하는 행위를 방지하는 것을 말하고(Pfleeger & Pfleeger, 2006), 암호화는 자료에 대한 해석이 불가능하도록 형태를 바꾸는 것을 의미하며, 방화벽은 네트워크에 승인 없이 접근하는 행위를 차단하는 것을 말한다(White, 2002). 행정적 보안은 보안정책 및 절차를 수립하고 내부구성원으로 하여금 이것을 준수하도록 하여 보안을 확보하는 것을 의미하며, 물리적 보안은 시스템에 대한 물리적 접근을 통제하고, 화재 등 재난으로부터 보호하는 것을 말한다.

정보보안에 대한 위협(Security Threat)은 그 정의부터 살펴볼 필요가 있다. 일반적으로 정보보안의 위협이 발생하는 이유는 우리가 사용하는 컴퓨터가 개별적으로 독립되어 있는 시스템이 아니라 네트워크로 타 시스템과 연결되어 있는 개방형 시스템이기 때문이다. 즉 보안에 대한 위협이란 허가받지 않은 자가 네트워크 장치를 통하여 사용자의 시스템에 접근하고, 의도하지 않은 명령을 실행함으로써 자료 및 정보를 위·변조, 파괴, 탈취하는 행위라고 할 수 있다. 이러한 보안위협은 그 종류가 매우 다양하나 일반적으로 불법접근 및 사용, 악성코드에 의한 자료변조 및 파괴, 악성코드에 의한 공격(Spooping, Sniffing, DOS 등) 등을 들 수 있다(강현선, 2014). 이에 대하여 구체적으로 살펴보면, 불법접근 및 사용은 범죄자 해커가 승인받지 않은 권한을 얻으려고 시도하는 행위, 컴퓨터 시스템에 불법으로 접근하여 패스워드를 탈취하려고 하거나, 프로그램을 훼손시키려는 행위 등을 말한다(Stair & Reynolds, 2003). 악성코드에 의한 자료변조 및 파괴는 악성 프로그램을 이용하여 타 조직 또는 컴퓨터 시스템이 보유하고 있는 정보를 탈취, 변조, 또는 파괴하기 위한 보안위협을 말한다. 이 보안위협의 대표적인 예로서 바이러스, 웜, 논리폭탄 등을 제시할 수 있다. 악성코드에 의한 공격에는 스푸핑(Spooping), 스니핑(Sniffing), 서비스거부공격(Denial of Service Attack) 등이 있다(강현선, 2014; Stair & Reynolds, 2003).

3. 정보보안제도 추진체계 현황

현재 우리나라 정보보안제도의 추진체계는 크게 관련 법률과 정부조직으로 구분된다. 첫째, 법률의 경우 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」을 기본법으로 하고, 각 부처가 업무별 또는 부문별로 개별법을 두고 제도를 운영하는 개별법 체계이다. 이를 정리하면 다음의 〈표 1〉과 같다.

〈표 1〉 현행 정보보안 관련법 체계

<table>
<tr><th>구분</th><th colspan="2">공공부문</th><th colspan="2">민간부문</th></tr>
<tr><td>정보보안시책 수립</td><td colspan="2">「국가정보화기본법」: 정보보안전문위원회 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」: 정보보안시책수립</td><td colspan="2"></td></tr>
<tr><td>주요정보통신기반 보안</td><td colspan="2">「정보통신기반보호법」: 공공, 금융, 정보통신등 분야별 주요 정보통신기반보호, 정보통신기반보호위원회</td><td colspan="2"></td></tr>
<tr><td>침해사고 대응</td><td colspan="2">'국가사이버안전관리규정': 공공기관침해사고 대응, 국가사이버안전센터</td><td rowspan="3">「정보통신망법」</td><td>민간침해사고 대응
침해사고대응지원센터</td></tr>
<tr><td>사이버 보안대책 및 조치</td><td rowspan="2">「전자정부법」</td><td>정보통신망 등 보안대책 수립 및 시행</td><td>이용자 정보보호
정보통신망 침해금지</td></tr>
<tr><td>각종 평가·인증, 점검</td><td>전자문서의 보안조치
공공부문 보안적합성 검증제도</td><td>정보보호 안전진단
정보보호관리체계인증</td></tr>
<tr><td></td><td colspan="2">「국가정보화기본법」: 정보보호시스템 평가·인증제도</td><td colspan="2"></td></tr>
<tr><td>전자서명</td><td colspan="2">「전자정부법」: 행정전자서명</td><td colspan="2">「전자서명법」: 공인전자서명</td></tr>
<tr><td>개인정보보호</td><td colspan="2">「공공기관개인정보보호법」
「주민등록법」</td><td colspan="2">「정보통신망 이용촉진 및 정보보호 등에 관한 법률」
「신용정보보호법」</td></tr>
</table>

출처: 방송통신위원회(2011)

〈표 1〉에 나타난 것처럼 정보보안법 체계는 보안업무별로 시책수립, 침해사고 대응 등 크게 7개 분야가 있으며, 보안대상별로는 공공과 민간 등 두 개 분야가 있다. 예를 들어 '정보보안시책 수립' 기능을 수행하면서 공공과 민간을 동시에 규제하는 「정보통신망법」이 있는가 하면, '침해사고 대응' 기능을 수행하면서 공공과 민간을 구분하여 각각 규율하는 「국가사이버안전관리규정」과 「정보통신망 이용촉진 및 정보보호 등에 관한 법률법」(이하 정보통신망법)도 있다. 이외에도 핵심적인 법률은 주요 정보통신기반 보호기능을 수행하면서 공공/민간을 동시에 아우르는 「정보통신기반보호법」, 사이버보안 기능을 수행하지만 공공부문만을 규율하는 「전자정부법」등이 있다.

둘째, 정부조직의 경우 정보보안체계는 각 업무별로 주관 부처가 있는 분산형 체계이다. 이러한 정보보안체계는 크게 공공부문과 민간부문으로 나눠지며, 현재 공공부문은 국가정보원 국가사이버안전센터가, 공공부문 중 전자정부의 정보보안은 행정안전부가, 민간부문은 과학기술정보통신부가, 국방부문은 국방부가 담당하고 있다. 또한 청와대 국가안보실 사이버안보비서관은 지난 2013년 발표된 '국가사이버안보종합대책'에 의거 국가정보보안의 컨트롤타워 역할을 맡고 있다.[3)]

국가정보원 국가사이버안전센터는 공공부문의 국가기밀 유출 방지, 국가정보통신망 보호, 국가사이버안전 정책의 총괄 및 조정, 침해사고조사 및 복구지원, 사이버위기 예방활동 및 공격탐지 등의 기능을 수행하고 있다(service1.nis.go.kr). 행정안전부는 공공부문 중 전자정부 대국민서비스 관련 보안업무를 담당하고 있다. 즉 업무절차상 보안위험요소 발견 및 분석, 각 기관에 보안지침 배포 및 조치 이행여부 조사·평가, 정보보안 솔루션 제공, 보안사고 발생 시 대응 및 보고 등의 기능을 수행하고 있다. 과학기술정보통신부는 민간부문의 정보통신망 안전성 확보, 침해사고 예방 및 확산방지, 사이버보안 강화, 민간정보보호 정책의 수립 및 총괄 등의 기능을 수행하고 있다. 국방부는 국방정보본부 산하에 국군사이버사령부를 설치하고, 군부문의 정보보안 및 사이버전쟁 등을 담당하고 있다.

4. 선행연구 검토

서론에서 언급하였듯이 정보보안제도를 둘러싼 이론 및 실무적 이슈들은 수없이 많이 존재한다. 기존의 연구를 정보보안 중요 이슈별로 법률, 조직, 정책 등의 분야를 중심으로 살펴보고자 한다.

우선 법률측면에서는 첫째, 정보보안제도와 관련된 법체계의 조정 필요성이 가장 큰 이슈이다. 보다 세부적으로는 정보보안제도를 뒷받침하고 있는 각 개별법률 간 불균형, 공백[4)] 및

3) 그러나 전문가들은 청와대 사이버안보비서관은 명목상의 컨트롤타워이며, 실질적인 컨트롤타워 역할은 집행 및 실무 총괄권한을 가진 국가정보원이 수행하고 있다고 비판하고 있다. 실제로 청와대에는 정보보안을 담당할 수 있는 전문직원이 없는 상태이다.

중복,[5] 분산 등의 문제가 있다(윤해성 외, 2012; 한국인터넷진흥원, 2010, 2011; 교육부, 2011; 김도승, 2007).

우선 각 개별법률 간 불균형이란 현실 및 현상에 대한 체계적인 분석과 정책적 고민 없이 필요시마다 임기응변식으로 관련 법률을 제·개정해왔기 때문에 형벌의 정도 등 각 법률 간 균형이 맞지 않는 문제를 말한다(윤해성 외, 2012; 한국인터넷진흥원, 2010).

관련 법률 간 공백 및 중복이란 하나의 법률이 아닌 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「정보통신기반보호법」, '국가사이버안전관리규정' 등 다수의 법령에 정보보안 관련 규정을 만들었기 때문에 법규정 및 각 기관의 기능과 책임에 있어 공백 및 중복이 발생하는 문제를 말한다.[6] 예를 들어 특정한 문제가 발생할 경우 이를 처리할 수 있는 법조항이 없거나, 또는 특정한 보안사고가 발생할 경우 책임을 져야하는 기관이 중복되어 누가 책임을 져야할지 불분명해지는 문제가 발생한다는 것이다(김도승, 2007). 보다 구체적인 예로서 '국가사이버안전관리규정'과 「정보통신기반보호법」의 경우 국가의 주요 정보통신망을 동시에 규제하고 있다. 이로 인하여 사고발생시 대응이 늦어지고, 부처 간 역할 및 책임이 불분명한 문제가 있다(김건우·김정덕, 2014; 방송통신위원회, 2011; 윤해성 외, 2012, 한국인터넷진흥원, 2010).

또한 관련 법률의 분산이란 정보보안 추진체계, 사전 및 사후적 예방대책, 보안평가 및 인증, 전자서명 등 중요한 정보보안 관련 기능을 다루는 법규정이 여러 법령에 산재되어 있는 문제를 말한다(한국인터넷진흥원, 2011). 그 결과 관련 법률간 일관성, 체계성, 통일성 등이 없는 문제가 발생하게 되었다는 것이다.

둘째, 「국가사이버안전관리규정」은 법률측면에서 두 번째로 중요한 이슈이다. 보다 세부적으로는 법형식, 구속력 저하, 대응력 미흡 등의 문제가 있다. 우선 「국가사이버안전관리규정」의 법형식이란 현재 국가정보원장이 이에 근거하여 정보보안 관련 정책과 관리를 총괄·조정하고 있으며, 국가사이버안전전략회의도 이에 근거하여 설치, 운영되고 있는데 이렇듯 핵심적인 업무와 권한 그리고 조직의 근거가 법률이 아닌 그 하위의 훈령이기 때문에 문제라는 것을 말한다(김경석, 2014; 육소영, 2010; 한국인터넷진흥원, 2011). 다음으로 '구속력 저하'란 정보보안의 핵심적인 추진체계인 '국가사이버안전전략회의'와 '국가사이버안전센터'의 구성 및 업무의 근거가 법률이나 명령보다 하위인 대통령 훈령, 즉 「국가사이버안전관리규정」에 근거하고 있어 법률에 근거하여 업무를 수행하는 각 부처를 지휘하기 어려운 문제를 말한다(육소영, 2010).[7] 또한 '대응력 미흡'이란 보안사고 발생 시 이에 대한 대응이 대통

---

4) 공백이란 법률의 규제를 받지 않는 사각지대를 의미한다

5) 중복이란 유사한 규정이 동시에 여러 법률에 존재하는 것을 의미한다

6) 실제로 정보보안 전문가들은 급변하는 사이버 공격에 따라 법령을 개정하면서 관련 법률 사이에 규율 대상이 중복되었으며, 특정 사건이 발생하면 어떤 법에 따라 처리해야할지 모호한 경우가 있다고 지적하고 있다(전자신문, 2017년 5월 14일).

령 훈령인 「국가사이버안전관리규정」에 근거하고 있기 때문에 행정기관에 대해서만 규율이 가능하고 DDOS 등 민관협력이 필요한 중요 보안사고에 대해서는 대응할 수 없는 문제를 말한다(한국인터넷진흥원, 2011).

조직적 측면에서는 정보보안제도의 추진체계 정비 필요성이 가장 큰 이슈이다. 보다 세부적으로는 컨트롤타워 정비, 추진체계 통합 등의 문제점이 있다(곽관훈, 2012; 교육부, 2011; 김민식 외, 2009; 육소영, 2010; 윤해성 외, 2012; 한국인터넷진흥원, 2010, 2011).

우선 '컨트롤타워 정비'란 현재 정보보안의 컨트롤타워 역할을 「국가사이버안전관리규정」에 근거하여 국가정보원이 맡고 있는데 이것이 적절하지 않다는 지적을 말한다(김태계, 2014; 육소영, 2010; 윤해성 외, 2012; 이기식, 2006). 이 지적에 대한 근거로서는 ①법률에 근거하여 직무를 수행하는 중앙행정기관이 훈령에 의하여 직무를 수행하는 국가정보원의 지시를 받는 것은 적절하지 않으며(육소영, 2010), ②국가정보원은 정부 각 부처에 분산된 정보보안 대응조직의 협력과 지원을 얻어내기 어려우며(김경석, 2014; 육소영, 2010), ③정보보안은 민관협력이 중요하며, 특히 정보통신기반은 정부 이외에도 민간기업 및 공공기관이 함께 운영하고 있기 때문에 이들의 협조를 얻는 것이 중요하지만 국가정보원은 다양한 외부기관과의 긴밀한 협력체계를 구축하기 어려운 점(안유성, 2014; 이기식, 2006), ④정보보안제도의 발전을 위해서는 여러 부처 간 상호 정보공유가 중요한데 국가정보원은 정보기관의 특성상 정보공유에 한계가 있다는 점(오일석, 2014; 윤해성 외, 2012) 등이 있다.

다음으로 '추진체계의 통합'이란 현재 정보보안의 추진체계가 국가정보원, 행정안전부, 과학기술정보통신부, 국방부 등으로 분산되어 있어 문제라는 지적을 말한다(곽관훈, 2012; 김민식 외, 2009; 교육부, 2011; 윤해성 외, 2012; 한국인터넷진흥원, 2010, 2011). 이 주장에 대한 근거로서는 ① 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「정보통신기반보호법」, 「국가사이버안전관리규정」 등 다수의 법률을 기반으로 여러 정부조직이 동시에 정보보안 기능을 수행하고 있기 때문에 부처 간 업무혼선 및 협력이 원활하지 못한 점(김민식 외, 2009; 한국인터넷진흥원, 2010), ②우리나라 정보보안은 공공부문은 행정안전부와 국가정보원, 민간부문은 과학기술정보통신부, 수사는 경찰과 검찰, 국방부문은 국방부 등으로 분산되어 있어 기능상 중복이 있고, 신속한 대응이 어려운 점(교육부, 2011; 한국인터넷진흥원, 2011), ③정보통신기반시설의 경우 정부부문은 국가정보원 국가사이버안전센터, 민간부문은 한국인터넷진흥원(KISA), 국방부문은 국군기무사령부 국가정보전대응센터 등으로 분산되어 있어 통일된 정책을 추진하기 어려운 점(곽관훈, 2012) 등이 있다.

마지막으로 정책측면에서는 체계적이고, 효과적인 정책의 필요성이 가장 큰 이슈로 논의되고 있다. 예를 들어, 정보보안기술 R&D, 정보보안 전문인력 양성, 정보보안 관리실태 점검 및 평가제도 미흡 등이 가장 시급한 문제로 인식되고 있다(교육부, 2011; 이기식, 2006; 이현

7) 실제로 보안전문가들은 우리나라 정보보안법체계는 머리(법률)는 없고 꼬리(「국가사이버안전관리규정」)가 끌고 가는 형태라고 지적하고 있다(서울경제, 2014년 12월 24일).

도 외, 2012; 정익재, 2011; 진정훈, 2011; 한국인터넷진흥원, 2012; 한국정보화진흥원, 2012).

우선 '정보보안기술의 R&D'에 있어서 현재 우리나라의 정보보안기술이 국내외 침해기술에 적절히 대응할 수 있을 정도로 발전되어 있지 못하고 있다(이기식, 2006; 정익재, 2011; 한국정보화진흥원, 2012). 이에 대한 근거로서는 ①침해기술은 나날이 발전하고 있는 반면 우리나라의 보안기술 연구 및 개발에 대한 투자는 부족한 점(이기식, 2006), ②정보보안사고의 트렌드 분석과 그에 따른 기술적 대응수단 개발 및 관련 정책대안의 연계가 미흡한 점(정익재, 2011), ③최근 보안사고는 지능화, 대형화되어 피해가 재난수준으로 증가했음에도 불구하고 국가정보보안에 대한 투자 및 예산은 미흡한 점(한국정보화진흥원, 2012) 등이 제시되고 있다.

'정보보안 전문인력 양성'의 문제는 보안사고는 그 빈도와 규모가 갈수록 급증하는 반면 이에 대응할 수 있는 전문인력이 부족하고 정보보호를 담당하는 인력의 지식수준이 미흡하다는 것을 의미한다(최동근 외, 2015; 교육부, 2011; 한국인터넷진흥원, 2012; 이기식, 2006; 금융보안연구원, 2011a, 2011b). 이 지적에 대한 근거로서는 ①보안사고의 배경에는 많은 원인이 있지만 그중에서도 가장 큰 원인은 정보보안 전담조직 및 전문인력이 부족한 점(금융보안연구원, 2011a), ②공공기관의 경우 정보보안인력 중 관련 학위소지자 및 관련 자격증 소지자가 부족하고 중앙부처의 경우 정보보안 전담인력이 없는 부처가 많은 점(교육부, 2011), ③정보보안기술을 전문적으로 개발하는 기업들조차 보안기술을 개발하기 위한 전문인력을 확보하기가 어려운 점(한국인터넷진흥원, 2012), ④ 정보보안을 담당하는 전문인력에 대한 교육과정 및 정보보호 연구가 미흡한 점(김건우·김정덕, 2014; 윤주범, 2016; 이근호, 2014; 전정훈, 2011) 등이 있다.

다음으로 '보안관리실태 점검 및 평가제도 미흡'이란 대부분의 중앙 및 지방자치단체, 공공기관, 그리고 민간기업들이 정부의 사이버보안관제 서비스를 받고 있거나 자체 사이버안전센터를 구축하여 운영하고 있으나, 보안관리실태를 점검하고 평가할 수 있는 제도가 미흡함을 말한다(이현도 외, 2012; 진정훈, 2011). 이 지적에 대한 근거로서 ①정부 각 부처에 보안예산을 포함한 보안지수 도입 및 보안수준 평가를 통해 현 실태분석 및 개선이 필요한 점(교육부, 2011), ②보안장비의 도입 및 운영에도 불구하고 정보자산의 평가 및 위험평가가 이루어지지 않고 있는 점(전정훈, 2011), ③각 기관의 보안관제업무를 평가할 수 있는 지표제도가 미흡한 점(이현도 외, 2012) 등이 있다.

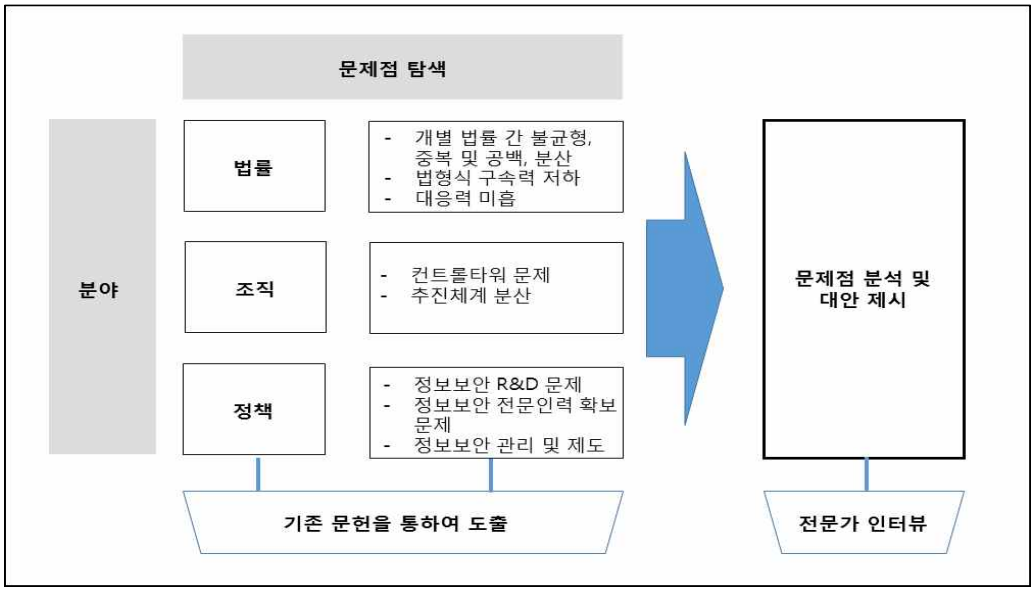
본 연구는 기존의 문헌에서 도출된 문제점을 바탕으로 전문가 인터뷰를 통하여 제시된 문제점들을 분석하고 이러한 이슈들을 극복할 수 있는 대안 제시에 중점을 두고자 한다.

Ⅲ. 연구설계

1. 조사방법 및 연구분석틀

연구설계는 '정보보안제도의 문제점 분석 및 효과적인 대안개발'이라는 본 연구의 목적에 초점을 두고 만들어졌다. 질문의 난이도가 높은 연구주제의 특성상 설문조사보다는 전문가 인터뷰조사를 연구방법으로 채택하였다. 인터뷰조사는 분석틀과 일치하도록 법률, 조직, 정책 등 세 가지 측면으로 구성되어 있으며, 문헌분석을 통해 발견된 문제점들이 실제로 타당성을 가지는지 진단하고, 추가적인 문제점과 대안들을 발견할 수 있도록 설계하였다. 각 측면의 문제점들은 질문항목으로 변환되어 전문가에게 사전에 검증받는 방식으로 객관적 타당성을 확인하였다. 이러한 분석틀을 요약하면 다음의 〈표 1〉과 같다.

〈그림 1〉 연구분석틀



2. 조사대상 및 자료수집

인터뷰조사 대상은 정보보안을 직접 담당하고 있는 관련 부처 공무원과 정보보안 관련 연구 및 실무경험을 가지고 있는 연구기관 박사 및 대학교수 등으로 나누어진다. 인터뷰조사는 2013년 직접 대면상태에서 사전 설계된 질문지에 따라 진행하거나 서면으로 이루어졌다. 인터뷰조사 참여자를 보다 상세히 설명하면 다음의 〈표 2〉와 같다.

〈표 2〉 인터뷰조사 인구통계

단위: 명

구분	정부	학계	연구계	합계
	공무원	교수	연구위원 (박사급)	
인터뷰 대상자	2 (20.0%)	5 (50.0%)	3 (30.0%)	10 (100.0%)

Ⅳ. 연구결과

연구결과의 분석은 본 연구의 분석틀과 일치하도록 법률, 조직, 정책 등 세 가지 측면으로 나누어져있다. 연구결과는 주로 주요 쟁점 및 정책적 시사점을 가지는 핵심적인 결과만을 분석하여 제시하였다. 우선 법률부문의 결과를 요약하여 제시하면 다음의 〈표 3〉과 같다.

〈표 3〉 법률부문의 연구결과

구분	대안/기능	동의	일부 동의	아니오	결측치	합계
관련 법체계 조정 필요성	각 개별 법령 간 불균형	9 (90.0%)	1 (10.0%)	0 (0.0%)	0 (0.0%)	10 (100.0%)
	각 개별 법령간 중복 및 공백	10 (100.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	10 (100.0%)
	관련 법률의 분산	5 (50.0%)	2 (20.0%)	0 (0.0%)	3 (30.0%)	10 (100.0%)
국가사이버안전관리규정	법형식	7 (70.0%)	0 (0.0%)	1 (10.0%)	2 (2.0%)	10 (100.0%)
	구속력 저하	6 (60.0%)	0 (0.0%)	0 (0.0%)	4 (40.0%)	10 (100.0%)
	대응력 미흡	5 (50.0%)	2 (20.0%)	0 (0.0%)	3 (30.0%)	10 (100.0%)

우선 정보보안관련 법체계의 조정 필요성과 관련하여 각 개별 법령간 불균형, 중복 및 공백, 분산 등의 문제에 대한 전문가들의 의견은 다음과 같다. 7명의 전문가들이 전부 동의, 3명의 전문가들이 일부 동의하는 것으로 나타났다. 답변에 대한 근거로서는 주로 ①정보보안 거버넌스가 공공과 민간으로 분리되어 국가정보원과 행정안전부 그리고 과학기술정보통신부 등으로 구성된 점, ②현 정보보안 관련 법령들이 지나치게 시스템 관점에서 제정된 점(이상 분산), ③하나의 수범자인 통신사가 「정보통신기반보호법」, 「정보통신망법」 등 여러 법률

에 의해 동시에 규제를 받고 있는 점, ④예를 들어 「개인정보보호법」과 「정보통신망법」에 개인정보보호에 관한 조항이 중복되는 점(이상 중복), ⑤정보보안 관련 법률간 형벌수준이 통일되어 있지 않아 형평성을 고려하여 일부 조정할 필요가 있는 점 (이상 불균형) 등을 제시하였다.

또한 이러한 문제들에 대하여 일부 동의하지 않는 의견도 있는 것으로 나타났다. 그 근거로서는 ①각 개별 법령들이 고유의 규제영역과 특성을 가지고 있기 때문에 서로 다른 기준을 가지고 있다고 해서 반드시 문제라고 말하기는 어려운 점,[8] ②동일한 한 법령 내에서도 규제대상에 따라 서로 다른 규제수준을 적용하고 있는 점[9] 등이 있다.

다음으로 '국가사이버안전관리규정'과 관련하여 '법형식', '구속력 저하', '대응력 미흡' 등의 문제에 대한 인식을 조사하였다.[10] 이러한 문제들에 대하여 대부분의 전문가들이 전부 또는 일부 동의하는 것으로 나타났다. 답변에 대한 근거로서는 주로 ①현재 국가정보보안을 총괄할 수 있는 법률이 필요하지만 훈령인 '국가사이버안전관리규정'은 그 역할을 할 수 없는 점, ②훈령은 행정기관 내부를 규율하는 법형식이기 때문에 처음부터 '국가사이버안전관리규정'은 국가정보보안을 총괄할 수 없었다는 점, ③훈령을 근거로 국가정보원이 법률을 집행하는 정부기관들을 통제하고 있기 때문에 각 기관들이 법률과 훈령 사이에서 혼란을 겪고 있는 점, ④처음부터 「정보통신기반보호법」개정을 통하여 정보보안문제에 대응했어야 했으나 오히려 '국가사이버안전관리규정'을 만들어 문제를 발생시킨 점, ⑤훈령은 실질적인 구속력이 없기 때문에 각 기관들이 위반할 가능성이 있는 점 등을 제시하였다.

다음으로 조직부문의 결과를 요약하여 제시하면 다음의 〈표 4〉와 같다.

〈표 4〉 조직부문의 연구결과

구분	대안/기능	예	아니오	결측치	합계
추진체계의 정비 필요성	컨트롤타워 정비	7 (70.0%)	1 (1.0%)	2 (20.0%)	10
	추진체계 통합	1 (10.0%)	9 (90.0%)	0	10

추진체계의 정비 필요성과 관련하여 '컨트롤타워 정비', '추진체계 통합' 등의 문제가 사실인지 조사하였다. 우선 컨트롤타워 정비 필요성에 대하여 7명의 전문가들이 전적으로

8) 예를 들어 「정보통신기반보호법」은 국가주요시설의 보호가 목적이며, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」은 정보통신망 및 정보통신사업자 통제가 목적이다.

9) 예를 들어 「정보통신망법」은 정보통신사업자에 대해서는 다소 높은 규제수준을, 준용사업자에 대해서는 상대적으로 완화된 규제수준을 적용하고 있다.

10) 이러한 문제들은 서로 다른 것처럼 보이지만 결국은 '국가사이버안전관리규정'의 법형식이라는 근본적인 문제 때문에 파생되는 문제들이다.

동의, 1명의 전문가는 반대, 2명의 전문가들은 동의 여부를 명확히 밝히지 않은 것으로 나타났다. 답변에 대한 근거로서는 주로 ①미국과 일본의 사례를 참고하여 청와대를 정보보안의 컨트롤타워로 설정하는 것이 바람직하다는 점, ②현재 정보보안사고 발생 시 각 부처가 주도권을 잡기 위하여 서로 경쟁하고 있는 점, ③정보보안사고는 각 부처의 협력이 가장 중요한데 국가정보원은 그 협력이 원활히 이루어지도록 조정할 수 없는 점, ④정보기관이 정보보안업무까지 맡는 것은 해외에서도 사례가 없으며, '빅브라더(Big Brother)'가 될 위험이 있는 점, ④현재 보안사고가 끊임없이 발생하고 있음에도 불구하고, 적절히 대응하지 못하고 있는 점, ⑤정보기관은 본연의 기능인 첩보(Intelligence)에 충실하도록 하고, 정보보안(Information Security)은 별도의 기관을 설립하여 대응하도록 하는 것이 바람직한 점, ⑥국가정보원은 국가기밀에 대한 정보보안이 주요 관심사이기 때문에 일반 정보보안사고에 대해서는 관심도가 떨어질 수밖에 없는 점, ⑦국가정보원은 정보기관의 특성상 뒤에서 정보기술 보완, 재발방지책 등을 마련할 수는 있으나, 앞에 나서서 대국민 홍보 및 안심, 제도개선, 언론대응 등의 컨트롤타워 역할을 할 수 없는 점 등을 제시하였다.

이외에도 반대 또는 동의여부를 명확히 밝히지 않은 답변에 대한 근거로서는 ①현재 국가정보보안을 총괄하는 기관이 있다면 그 기관이 컨트롤타워 역할을 하면 되지만 아직 그런 기구가 없기 때문에, 즉 현재 상황에서는 불가피하게 국가정보원이 맡는 것이 적절한 점, ②국가정보원법상 정보, 보안업무기획 및 조정 등의 근거가 있는 점, ③「국가사이버안전관리규정」이 남북이 대치하는 상황의 연장선에서 제정된 점 등을 제시하였다.

다음으로 추진체계 통합 필요성에 대하여 1명의 전문가가 동의, 9명의 전문가는 반대하는 것으로 나타났다. 동의하는 답변에 대한 근거로서는 미국의 DHS(Department of Homeland Security)와 같이 각 부처에 흩어져있는 정보보안 관련 부서를 하나의 동일한 전담부처에 통합시키면 효과적으로 정보보안 기능을 수행할 수 있는 점이 제시되었다. 반대하는 의견에 대한 근거로서는 ①정보보안부 또는 청 등 하나의 기관에 기능을 통합시키면 타 부처의 반발을 초래하고, 협조를 얻기 어려운 점, ②각 부처가 고유의 기능과 관련하여 정보보안업무를 수행하고 있기 때문에 통합이 불가능한 업무도 있는 점, ③현재 각 부처의 정보보안인력은 전문가 집단이 아니며, 따라서 이들을 통합한다고 해서 효과를 얻기 어려운 점, ④현재와 같이 각 부처의 고유의 영역에서 정보보안업무를 수행하고, 문제해결을 위하여 협력하도록 하는 것이 바람직한 점, ⑤현재 정보통신망이 연계되어 있고 사고발생시 여러 부처가 동시에 영향을 받아 관련이 되기 때문, ⑥현재 복잡하게 중복, 산재되어 있는 정보보안 관련 법률을 하나로 통합하는 등 정비하기가 어렵고, 따라서 독립 부처보다는 컨트롤타워를 두고 총괄하는 것이 더 바람직한 점, ⑦각 부처가 고유의 영역에서 전문화되어 있기 때문에 해당 영역에 대한 이해가 높으며, 따라서 보안업무도 스스로 하도록 맡기는 것이 바람직한 점 등을 제시하였다.

다음으로 정책부문의 결과를 요약하여 제시하면 다음의 〈표 5〉와 같다.

〈표 5〉 정책부문의 연구결과

구분	대안/기능	예	아니오	결측치	합계
체계적, 효과적 정책 필요성	정보보안기술 R&D	8 (80.0%)	0 (0.0%)	2 (20.0%)	10
	정보보안 전문인력 양성	9 (90.0%)	0 (0.0%)	1 (10.0%)	10
	정보보안 관리실태 점검 및 평가제도	6 (60.0%)	1 (10.0%)	3 (30.0%)	10

체계적이고, 효과적인 정책의 필요성과 관련하여 '정보보안기술 R&D', '정보보안 전문인력 양성', '정보보안 관리실태 점검 및 평가제도' 등의 문제가 사실인지 조사하였다. 우선 정보보안기술 R&D의 필요성에 대하여 8명의 전문가들이 전적으로 동의, 2명의 전문가는 관련 의견을 명확히 밝히지 않은 것으로 나타났다. 동의하는 답변에 대한 근거로서는 주로 ①현재 정부의 IT 및 정보보안관련 예산이 매우 작은 점, ②정보보안 위협측정체계의 구축이 필요한데 현재 없는 점, ③정보보안의 중요성이 나날이 높아짐에도 불구하고 보안기술의 개발을 민간에 맡겨두고 있는 점, ④현재 우리나라의 정보보안산업이 매우 영세한 점, ⑤현재 우리나라의 정보보안기술의 글로벌 마켓에서 경쟁력이 전혀 없을 정도로 낙후된 점, ⑥국내 정보보안업체들이 국가정보원의 보안성평가를 등에 업고, 기술개발에 대한 투자 없이 국내에서만 영업하려는 행태를 보이는 점 등을 제시하였다.

다음으로 '정보보안 전문인력 양성'에 대하여 9명의 전문가들이 동의, 1명의 전문가는 관련 의견을 명확히 밝히지 않은 것으로 나타났다. 동의하는 답변에 대한 근거로서는 ①현재도 정보보안 전문인력이 양성되고 있으나 보안기업들이 요구하는 전문기술과 지식을 갖춘 인재가 없는 점,[11] 동시에 그들의 숫자도 절대적으로 부족한 점 ②정보보안 전문인력에 대한 처우가 열악하며 이것이 빈약한 인력풀의 직접적인 원인이 되고 있는 점, ③수도권 대학의 경우 정보보안 전문인력 양성을 위한 학과신설이 어려운 점, ④정부가 그동안 정보보안 전문인력에 대한 수요예측과 양성계획에 미흡했던 점, ⑤그동안 정부가 정보보안기술 개발, 전문인력 양성, 교육 및 인증체계 개발 등 총체적으로 정보보안에 미흡했던 점 등을 제시하였다.

다음으로 '정보보안 관리실태 점검 및 평가제도'에 대하여 7명의 전문가들이 동의, 3명의 전문가는 관련 의견을 명확히 밝히지 않은 것으로 나타났다. 동의하는 답변에 대한 근거로서는 ①현재 민간기업의 ISMS(Information Security Management System)과 같이 보안실태를 객관적으로 측정할 수 있는 지표를 개발할 필요가 있는 점, ②보안사고 예방을 위한 정부의 점검, 감독, 제재 등이 제대로 이루어지지 않고 있는 점, ③기존 지표체계가 급변하는 정보보

11) 전반적으로 전문가들은 KISA 등 공공기관, 각 학교의 정보보호대학원 등 기존의 정보보안 전문인력 양성체계가 진정으로 보안기술 전문성과 R&D 능력을 갖추고 있는지 의문이라고 지적하였다

안상황에 맞게 짧은 간격으로 변화, 발전되어야 하는데 그렇지 못한 점, ④기존 지표체계가 관련 법률의 구현과 일치성이 미흡한 점, ⑤각 부처에 정보보안 전문인력과 전담부서가 없으며 따라서 기존의 보안관제서비스에 대한 평가 및 자체 실태평가 그리고 이를 위한 지표 역시 미흡한 점, ⑥보안전문인력과 기술도 미흡한 상황에서 이에 대한 평가 및 점검 역시 제대로 이루지기 어려운 점 등을 제시하였다.

V. 우리나라 정보보안제도 개선을 위한 정부의 역할

우리나라 정보보안제도 개선을 위한 정부의 역할은 전문가 인터뷰조사의 결과를 기초로 제시되었다. 앞서 언급한 바와 같이 우리나라 정보보안제도는 수많은 문제점들을 안고 있으며 그중에는 심각한 문제들도 많이 있다. 따라서 본 연구에서는 많은 정책을 제시하기 보다는 상대적으로 시급하고, 중요성이 높은 정책들을 선별하여 제시하고자 한다. 여기서 상대적으로 중요한 정책의 선별은 선행연구분석, 전문가 인터뷰조사 당시 자문 등을 기초로 연구자들의 토론과 판단을 통하여 이루어졌다.

법률부문에서는 다른 모든 문제들보다도 우선 정보보안기본법 제정을 통해 정보보안 관련 법체계를 체계적으로 정비할 필요가 있다. 물론 기본법 제정 이외에도 통합된 단일 법률의 제정, 모든 개별 법률의 필요 조항 개정, 기존 「국가사이버안전관리규정」의 일반법화[12] 등 다양한 방안이 논의되고 있다. 그러나 이러한 방안들은 각각 소관 부처의 반발 및 협조를 얻기 어려운 점, 개별 법률을 일일이 개정하는 것은 오랜 시간과 비용이 소요되고 현실적으로 어려운 점, 「국가사이버안전관리규정」을 법제화하면 오히려 기존 법률과 충돌을 일으킬 가능성이 높은 점 등 여러 이유로 인하여 제외되었다.

따라서 본 연구는 정보보안기본법을 제정하고, 이를 기준으로 「정보통신망법」 등 관련 법률들을 개정하는 방안을 제안한다. 정보보안기본법(가칭)을 제정할 때에는 기본원칙과 함께 기존 추진체계의 거버넌스 구조를 명확히 정리, 제시하여 그동안 논란이 되어 왔던 각 기관의 역할과 책임이 더 이상 문제가 되지 않도록 해야 한다. 또한 관련 법률들을 정비할 때에는 일관성과 통일성을 최우선으로 고려하여 그동안 꾸준히 제기되어 온 법률간 불균형, 중복 및 공백 등의 문제가 더 이상 발생하지 않도록 해야 한다.

또한 그동안 문제가 되어온 「국가사이버안전관리규정」에서 국가안보 등 국가정보원 고유의 기능을 뺀 나머지 규정들은 새롭게 제정되는 기본법으로 가져와야 한다. 특히 정보보안 관련 총괄 및 조정기능 그리고 국가사이버안전전략회의 등의 거버넌스 관련 규정을 기본법

12) 실제로 최근 발의되고 있는 사이버안보 관련 법률들은 사실상 국가정보원을 컨트롤타워로 두는 대응체계를 갖추고 있어 기존 '국가사이버안보규정'의 체계를 그대로 따로 있다. 이러한 법률안들은 국가정보원의 과도한 권한 집중에 대한 우려를 낳고 있다(보안뉴스, 2017년 5월 29일).

으로 편입시켜야 한다. 왜냐하면 ①이는 중앙행정기관을 규율하는 것이기 때문에 훈령이 아닌 법률에 근거를 두어야하기 때문이며, ②기본법은 기본적인 원칙 및 정책, 그리고 거버넌스 체계 등에 대한 선언적 규정을 담는 것이기 때문이다.

정보보안기본법 제정의 장점은 ①각 기관들이 각자 개별 법률에 근거하여 고유 영역의 정보보안을 담당함으로써 전문성을 살릴 수 있고, ②고유의 업무와 기능을 지키고자 하는 각 부처의 반발을 최소화할 수 있으며, ③어느 한 부처 또는 기관의 정보보안 헤게모니 장악에 대한 우려와 잠재적 위험(예: 프라이버시, 빅브라더 등)을 방지할 수 있으며, ④개별법 개정을 통해 각 기관 간 역할과 책임을 명확히 할 수 있으며, ⑤개별법 개정을 통해 각 법률간 일관성 및 통일성을 확보할 수 있으며, ⑥법체계 측면에서도 각자의 고유영역을 가지고 있는 개별법체계가 더 효과적인 점 등이 있다.

조직부문에서는 청와대를 실질적인 컨트롤타워로 설정함으로써 정보보안 관련 거버넌스 체계를 효과적으로 정비할 필요가 있다. 물론 이 대안 이외에도 사이버보안청 등 통합된 추진체계의 설립,[13] 국가정보원의 기능강화, 과학기술정보통신부 등 어느 한 부처에 컨트롤타워 기능부여 등 다양한 방안을 생각해볼 수 있다. 그러나 이러한 방안들은 각각 각 부처 고유의 업무 및 보안기능 저하, 부처의 반발 및 비협조, 부처 간 총괄 및 조정능력 미흡 등 여러 이유로 채택되지 않았다.

따라서 본 연구는 청와대를 정보보안의 실제 컨트롤타워로 하고, 이를 중심으로 국가정보원, 행정안전부, 과학기술정보통신부, 국방부 등 유관 기관들이 서로 협력해 나가는 방안을 제안한다. 물론 이 방식은 지난 2013년 발표되고, 2015년 확정된 '국가사이버안보종합대책'에도 유사하게 담겨져 있다. 그러나 본 연구의 제안과 정부의 대책이 다른 점은 국가정보보안의 실무 및 총괄이 국가정보원이 아닌 청와대가 되어야 한다는 점이다.

여러 선행연구를 분석하고 전문가 인터뷰조사를 실시한 결과 현재 국가정보원을 실질적인 컨트롤 타워로 삼고 있는 정부의 '국가사이버안보종합대책'은 전문가들의 동의를 받지 못하고 있다. 따라서 본 연구는 현재와 같이 각 부처가 고유의 영역에서 정보보안 업무를 수행하되, 국가정보원은 현재의 실질적인 정보보안 총괄 및 조정기능을 청와대 '사이버안보비서관'에게 넘기고 정보보안을 위한 범부처 협력체계의 한 축으로서만 참여해야 한다.

또한 청와대가 실질적인 정보보안 컨트롤타워 역할을 수행하기 위해서는 ①현재의 '사이버안보비서관'을 수석급으로 격상시켜야 하며, ②이를 보좌할 수 있는 국가정보보안위원회(가칭)를 청와대 소속으로 설립해야 하며, ③현재 청와대 소속 각종 위원회의 실효성에 대한

13) 2017년 대선 당시 선거대책위원회 균형발전 정책추진위원장을 맡은 이상민 의원은 독자적 사이버보안 전문 부처의 신설을 내세운 바 있고, 현재 정부는 독자적인 사이버 보안전략 컨트롤타워의 설치를 골자로 하는 국가적 종합대책을 다시 수립하려고 준비하는 중이다(디지털데일리, 2017년 5월 10일). 그러나 독자적인 전문부처는 본 연구에서 제시한 이유 등으로 바람직하지 않으며 NSA와 같은 집행기능을 가진 소속기관의 설립이 더 바람직하다는 것이 본 연구진의 판단이다.

회의가 많은 점을 고려하여, 집행기능까지 갖춘 위원회가 될 수 있도록 결정사항을 집행하는 미국의 NSA(National Security Agency)와 같은 별도의 소속기관을 설립해야 하며, ④현재 국가정보원 소속의 국가사이버안전센터를 분리시켜 제안된 별도의 기관에 편입시켜야 한다.

청와대가 국가정보보안의 실질적인 컨트롤타워가 될 때의 장점은 ①국가정보보안 발전을 위한 부처 간 총괄 및 조정능력 향상, ②부처 간 정보보안 업무협력 및 정보공유 유도, ③각 부처 고유의 업무 및 보안기능 유지, ④국가정보원 또는 행정안전부와 같은 어느 한 부처에 기능을 집중시켰을 때 예상되는 각 부처의 반발 및 비협조 방지, ⑤국가정보원은 본연의 기능인 국가안보에 충실, ⑥동시에 '국가사이버안전센터' 시절부터 축적한 전문적 지식과 경험 유지, ⑦청와대의 결정을 효과적으로 직접 집행함으로써 국가정보보안 활성화 등이 있다.

정책부문에서는 정보보안기술 R&D, 정보보안 전문인력 양성, 정보보안 관리실태 점검 및 평가 등 가장 시급하고 중요한 대안을 우선적으로 집행하는 등 정보보안정책을 체계적으로 재정비할 필요가 있다. 물론 이외에도 보안산업육성, 예산정책 강화, 위협측정체계 구축, 보상체계 구축, 보안의식 및 문화개선, 민관협력 등 다양한 방안이 필요하고, 이에 대해 논의가 진행되고 있다. 그러나 이러한 방안들도 중요하지만 앞서 제기한 세 가지 대안이 보다 시급하며, 중요하기 때문에 본 연구에서는 이를 중점적으로 다루기로 한다.

우선 정부는 정보보안기술 R&D를 국가 최우선 과제 중 하나로 지정하고, 이를 위하여 직·간접적인 정책을 추진해야 한다. 우선 간접적인 정책으로서는 ①KISA, ETRI 등 보안기술개발 관련 공공기관에 대한 인적, 물적 지원을 통한 정보보안기술 개발 유도, ②정보보호대학원 등 학계에 대한 예산지원 등을 통한 기술개발 독려, ③낙후된 정보보안산업에 대한 예산지원을 통한 기술개발 유도 등이 필요하다. 이중에서도 특히 보안산업에 대한 지원이 가장 중요하다. 보안산업이 성장하지 않고서는 시장의 논리로 움직이는 민간기업의 보안기술 개발 및 연구도 요원하기 때문이다.

우리나라 정보보안산업의 규모는 2016년 기준 2조 2천억원에 불과하며(서울경제, 2017년 7월 10일), 이는 2017년 기준 미국의 보안산업규모 317억 달러(약 36조 4천억원, 디지털타임스, 2017년 7월 11일)에 비해 약 16.5%에 불과한 것이다. KT, AhnLab 등 일부 기업을 제외한 대부분의 정보보안 관련 기업들은 영세한 업체들이며, 그나마도 정부의 외면, 각 기업들의 정보보안에 대한 불감증 등으로 어려움을 겪고 있다. 해외 보안시장으로 눈을 돌린다고 해도 McAfee, Norton 등 유명 글로벌 보안기업들이 장악한 시장에서 경쟁력을 갖추는 것은 매우 어려운 일이다. 그러므로 정부는 국내 보안산업이 일정 규모 이상 성장할 때까지 중앙 및 지자체, 각 급 공공기관의 정보보안 관련 H/W와 S/W의 구입, 민간기업의 정보보안장비 및 기술의 도입을 위한 홍보 및 권장, 정부 보조금 등 예산지원, 세금감면 등 각종 세제혜택, 수출지원, 특허등록지원 등 각종 정책적 지원을 아끼지 말아야 한다.

또한 직접적인 정책으로서 정부는 미국의 INQTEL 사례를 참고하여 한국형 보안기술개발 펀드를 조성하고, KT, Ahn Lab 등과 같은 국내 민간보안기술업체의 참여를 적극적으로 유도

해야 한다. 미국은 CIA의 주도하에 각 보안기업의 참여와 기술개발을 공동으로 이루어왔으며 현재까지 매우 성공적이었다. 특히 국내 전문가들은 정부와 민간기업의 협력 부재를 큰 문제 중 하나로 지적하고 있기 때문에 보안기술개발펀드의 조성 및 집행은 우리나라 정보보안기술 발전을 위해 매우 중요한 정책이라고 할 수 있다.

다음으로 정부는 정보보안 전문인력 양성을 우선과제로 선정하고, 이를 위하여 다양한 측면의 세부정책들을 추진해야 한다. 현재 우리나라는 급증하고 있으며, 날로 그 피해규모도 커지고 있는 정보보안사고에 대응할 수 없을 정도로 전문인력이 질적으로, 양적으로 모두 부족한 상황이다. 이렇게 된 원인으로서는 IT인력에 대한 미흡한 대우, 전통적으로 제조업 등 H/W에 치중한 산업구조, 그에 따른 S/W산업에 대한 경시, 정부 및 민간기업의 정보보안에 대한 미흡한 인식, 대학교 등 교육기관에 정보보안 관련 전공이 거의 없는 점, 낙후된 보안산업 등 수많은 문제들을 꼽을 수 있다.

전문인력을 양성하기 위해서는 ①보안시장이 요구하고 있는 전문적인 지식과 기술 및 그 수준 등을 정확히 분석한 후 그에 맞게 교육 프로그램을 설계하고, 실력 있는 강사진을 확보하는 등 중장기적이고도 체계적인 접근이 필요하며,[14] ②대학교, 공공기관, 민간기업 등 교육기능을 맡은 각 기관들에게 충분한 예산지원이 이루어져야 하며, ③정보보안에 특화된 자격증 제도의 점검/보완 및 신설이 이루어져야 하며, ④수도권 내 대학 및 대학원에 대한 정원 제한에서 정보보안 관련 학과는 예외로 하여 전문인력이 배출될 수 있도록 하되, 우리나라 보안시장이 요구하는 규모를 조사하여 수요공급이 적절히 이루어지도록 해야 하며, ⑤KISA, ETRI, 국가보안기술연구소 등 공공기관과 Ahn Lab, KT, Symantec Korea, McAfee Korea 등 민간 정보보안기업의 협조를 얻어 전문인력 양성 프로그램 설치하고 정부가 이를 적극 지원해야 하며, ⑥지속적인 정보보안 전문인력 수요가 발생할 수 있도록 중앙[15] 및 지방자치단체, 공공기관, 그리고 요건을 충족하는 민간기업에 일정비율의 정보보안인력의 채용을 의무화하고, 이를 준수/비준수할 경우를 대비한 적절한 보상과 제재수단을 마련해야 할 것이다.

끝으로 정부는 정보보안 관리실태 점검 및 평가를 우선과제로 선정하고, 이를 위하여 다양한 세부전략들을 수립하여 집행해야 한다. 앞서 살펴본 것과 같이 현재 중앙 및 지자체 등 대부분의 기관들은 정보보안 관리실태 점검 및 평가가 미흡한 상황이다. 문제의 원인으로서는 정보보안에 대한 인식이 부족한 점, 보안실태 점검을 위한 측정체계가 미흡한 점, 기존 및 현존 관리실태 점검 및 평가가 보안수준 향상 보다는 내부의 효율성에 초점을 맞춘 점 등이 있다.

그러므로 보안실태 점검 및 평가가 효과적으로 이루어지기 위해서는 ①KISA, ETRI 등 정보보안을 연구하고 있는 국책연구기관에 의뢰하여 보안실태를 정확하고도 객관적으로 측정

14) 현재 우리나라 정보보안 전문인력의 현주소는 질적으로는 보안기업이 요구하는 능력을 갖춘 인재가 거의 없으며, 양적으로는 공급되는 인재의 수가 절대적으로 부족하다는 것이다.

15) 현재 40개 부처 186명의 정보보안 담당자 중 84명(45.2%)은 관련 학위나 자격증을 소유하고 있지 않으며, 관련 경력도 2년 미만이다(전자신문, 2016년 5월 1일).

할 수 있는 새로운 지표체계의 개발하여 적용해야 하며, ②개발된 지표를 가지고 정기적으로 또는 필요시 수시로 정보보안 관리실태를 점검, 평가하여 문제점을 발견하고 개선을 위한 대책을 수립·이행해야 하며, ③정보보안 관리실태 점검 및 평가결과를 기관평가에 반영하여 각 기관의 관심과 적극적인 이행의지를 확보해야 하며, ④정보보안 관리실태를 실시간으로 점검하고, 평가할 수 있는 프로그램을 개발하여 전 기관에 적용해야 하며,[16] ⑤각 기관별로 정보보안 관련 규칙 등 내부관리정책을 수립하여 스스로 정기적으로 준수 여부를 점검하도록 하는 등 다양한 세부전략의 마련 및 이행이 이루어져야 할 것이다.

Ⅵ. 결론: 연구의 한계 및 미래연구방향

이상으로 우리나라 정보보안제도의 현황과 문제점 그리고 개선을 위한 대안들을 살펴보았다. 많은 문제점들과 그에 따른 대안을 제시하였으나 핵심을 다시 요약하면 첫째, 우리나라 정보보안제도를 둘러싼 문제들은 수없이 많이 있기 때문에 정부는 그중에서 가장 시급하고 중요한 문제들을 우선적으로 선별하여 체계적이고 단계적으로 문제해결에 접근을 해야 한다. 정보체계가 존재하는 한 정보보안 문제 역시 영원히 존재할 것이기 때문에 서두르지 않는 통찰력 있는 접근이 필요하다는 것이다.

둘째, 정보보호를 위한 컨트롤타워가 시급히 세워져야 한다. 현재 우리나라는 정보보안기능이 국가정보원, 행정안전부, 국무총리실, 과학기술정보통신부 등 다수 부처에 분산되어 있다. 이에 대하여 새로이 출범한 문재인 정부도 독자적인 컨트롤타워 건설의 의지를 보이고 있는 실정이다(조선일보, 2017.5.12.). 컨트롤타워와 같이 정보보안에 참여하고 있는 각 기관들이 매우 민감하게 생각하는 문제의 경우 각 기관들의 입장과 정보보안 분야 각계(정부, 학계, 보안산업계, 연구계 등) 전문가들의 의견을 충분히 수렴하여 신중하게 접근해야 한다. 일부 기관 또는 일부 전문가들의 주장만을 믿고 편향적으로 문제 해결을 시도해서는 안되며, 한 문제라고 해도 여러 전문가들의 의견을 종합적으로 취합하고, 분석하여 객관적이고 경험적 타당성을 가졌으며, 전부는 아니더라도 일정 수준이상 동의와 합의를 가진 해결책을 찾아야 할 것이다.

셋째, 타 분야의 연구도 동일하겠으나 특히 정보보안분야 문제의 경우 각 부문 간 문제들이 서로 밀접하게 연계되어 있는 특성이 있기 때문에 어느 한 문제에 대해 접근할 경우 그 원인과 배경을 면밀히 살펴보고, 동시에 연계되어 있는 타 부문의 문제들까지 체계적으로 분석할 필요가 있다. 예를 들어 정보보안기술의 경우 단순히 낙후된 보안기술의 개발 및 발전에

16) 이에는 실시간으로 보안USB 사용여부, 보안문서 생산 및 저장 시 절차준수 여부, 보안 프로그램의 설치 및 사용 여부, 이메일 내용 및 첨부자료의 대외비 여부, 대외비 자료 인쇄 시 권한획득 여부, 바이러스 등 악성코드의 감염 여부 등을 점검하는 기능을 포함해야 한다.

집중해서는 안되며, 그렇게 된 배경과 원인, 즉 저조한 보안산업과 부족한 보안기술인력, 그리고 정부의 인식부족과 그에 따른 부족한 예산지원 등 수많은 연계된 요인들을 종합적으로 분석한 후 체계적으로 접근할 수 있어야 한다.

모든 연구와 마찬가지로 본 연구도 한계를 가지고 있다. 본 연구의 한계는 첫째, 본 연구가 정보보안제도와 관련된 모든 문제를 다루지는 못하고 있으며, 선택된 중요한 문제들에 집중하고 있다는 것이다. 따라서 연구자들의 판단과 전문가들의 자문에 기초하여 우선순위가 높은 문제와 대안들에 집중하고 있다고 하더라도 또 다른 중요한 문제들을 다루지 못하고 있을 수 있다는 한계가 있다. 둘째, 본 연구의 목적은 정보보안제도를 둘러싼 문제점들을 큰 틀에서 전반적으로 살펴보는 것이기 때문에 선택된 하나의 문제 만에 대하여 실무적으로 즉시 적용 가능한 매우 구체적인 대안을 제시하지는 않았다. 예를 들어 정보보안기본법 제정, 컨트롤타워 정비, 정보보안 전문인력 양성, 정보보안 기술개발 등 각각의 주제가 하나의 거대한 연구대상이기 때문에 지면을 제한받는 학술논문에서 이 모두를 매우 자세히 다룰 수는 없는 한계가 있다. 셋째, 인터뷰조사에 참여하고 있는 전문가의 수가 10명이기 때문에, 만약 30명, 50명의 전문가가 참여하는 대형연구가 있다면 그 결과에 비해서는 보다 다양한 분석과 대안을 제시하기에 한계가 있을 수밖에 없다.

정보보안제도를 보다 발전시키기 위한 미래연구방향은 앞서 연구의 한계에서 언급한 바와 같이 첫째, 본 연구에서 제외한 나머지 문제들과 대안들에 대한 추가 연구가 필요하다. 예를 들어 정보보안산업 활성화 방안, 정보보안 관련 조직문화에 영향을 미치는 요인 등에 대한 추가 연구가 필요하다. 둘째, 본 연구에서 큰 틀에서 바라본 각 분야의 문제점들과 대안들을 그 범위를 좁혀 한 주제씩 선택하여 다시 집중적으로 연구를 진행할 필요가 있다. 예를 들어 정보보안기본법 제정과 관련 법체계 정비의 경우 연구의 범위가 매우 크며 다루어야 할 세부문제도 매우 많은 하나의 거대한 프로젝트이다. 정보보안 분야의 기본법 제정과 관련 법령의 정비는 관련된 수많은 개별법령들을 일일이 분석하고, 상호간의 일관성, 불균형, 중복 및 공백, 분산 등을 종합적으로 분석해야 하는 매우 어렵고 시간도 오래 걸리는 연구이기 때문이다. 그럼에도 불구하고 이러한 연구는 우리나라 정보보안 분야 법령의 발전을 위해서 반드시 필요한 것이라고 할 수 있다.

끝으로 정보보안제도는 지난 2013년 정부가 국가사이버안보종합대책을 발표한 이후로 이렇다 할 변화나 개선이 없이 답보상태에 있다. 물론 제도의 개선은 법령의 제·개정이 수반되기 때문에 시간이 오래 걸리는 특성이 있는 점을 감안하더라도 사안의 시급성을 고려할 때 더 이상 미룰 수 없는 상황이다. 다행히 2017년 출범한 새 정부는 사안의 중요성을 인식하고 그 어느 때보다 제도개선의 의지를 보이고 있는 만큼 본 연구에서 살펴본 다양한 문제들과 대안들을 참고하여 정보보안이 국가발전의 저해요인이 아닌 성장요인으로 작용하도록 해야 할 것이다.

≤참 고 문 헌≥

강현선(2014). 정보보안을 위한 정보보호 관리체계 및 인증체계 분석.「보안공학연구논문지」, 11(6): 455-468.

곽관훈(2012). 일본의 정보통신기반보호제도의 현황 및 시사점.「IT와 법 연구」, 147-175.

교육부(2011).「국가 사이버보안 대응체계 혁신에 관한 연구」, 교육부.

금융보안연구원(2011a). 금융 IT 내부통제 강화 전략: 내부자 위협 중심으로.「이슈 리포트」, 2011-008: 1-6.

금융보안연구원(2011b). 금융보안 전문인력 양성을 위한 교육의 필요성 및 발전방향.「이슈리포트」, 2011-016: 1-8.

나현대·정현수(2016). 국내·외 정보보호 관리체계기반의 인적보안의 이론적 비교연구.「중소기업융합학회 논문지」, 6(3): 13-19.

김건우·김정덕(2014). 정보보호 교육에 대한 연구 동향 분석.「정보보호학회논문지」, 26(2): 489-499.

김경석(2014). 정보보안법제의 문제점과 개선방안-해외의 관련규정과의 비교를 중심으로-.「법학연구」, 55(4): 123-146.

김도승(2007). 공공부문 소프트웨어 분리발주의 법적문제.「방송통신정책」, 19(10): 1-6.

김민식 외(2009). 통합적 사이버 위기관리 체계의 필요성에 관한 연구.「정보보안논문지」, 9(1): 29-37.

김원필(2015). 정보보안에 대한 연구 트렌드 분석.「한국정보통신학회논문지」, 19(5): 123-146.

김태계(2014). 사이버테러 범죄 대응에 관한 제도적 문제점과 대책.「법과 법학연구」, 14(3): 1110-1116.

방송통신위원회(2011).「사이버 보안법제 선진화 방안 연구」, 방송통신위원회.

안유성(2014). 사이버 안보 대응 역량 강화방안 연구.「정보보호학회지」, 24(6): 60-68.

오일석(2014). 보안기관의 사이버 보안 활동 강화에 대한 법적 고찰.「과학기술법연구」, 20(3): 41-90.

육소영(2010)사이버보안법의 제정 필요성에 관한 연구.「공법학연구」, 11(2): 313-335.

윤주범(2016). 공공분야 정보보안 역량 강화를 위한 단기 교육과정 연구.「정보보호학회논문지」, 26(3): 769-776.

윤해성 외(2012).「사이버테러의 동향과 대응방안에 관한 연구」, 한국형사정책연구원.

이기식(2006). 네트워크시대 사이버보안의 문제점 및 정책대안.「한국지역정보화학회지」, 9(1): 109-128.

이근호(2014). 정보보호 인력양성을 위한 효율적인 정보보호관리체계의 융합 관리 방안.「한국융합학회논문지」, 5(4): 81-86.

이현도·이상진(2012). 보안관제 업무에 대한 평가지표 개발 연구.「정보보호학회논문지」, 22(5): 1133-1143.
전정훈(2011). 보안시스템으로 인해 추가되는 예산 외 비용의 요인에 관한 연구.「한국통신학회논문지」, 36(12): 1481-1488.
정익재(2011). 정보사회의 불확실성 관리를 위한 정책 논리와 대응: 정보보안사고의 유형화와 대응책.「국가정책연구」, 25(4): 55-77.
한국인터넷진흥원(2010).「미국, 영국, 독일의 기반보호법체계에 관한 연구」, 한국인터넷진흥원.
한국인터넷진흥원(2011).「2011 국내 정보보안 산업 실태조사」, 한국인터넷진흥원.
한국인터넷진흥원(2012).「국내 지식정보보안산업 실태조사」, 한국인터넷진흥원.
한국정보화진흥원(2012).「2012 국가정보화백서」, 한국정보화진흥원.
한국정보보호진흥원(2001).「정보보호관리와 정책」, 한국정보보호진흥원.
Pfleeger & Pfleeger(2006). Security in Computing. Upper Saddle River, NJ: Prentice Hall.
Stair & Reynolds(2003). Principles of Information Systems. Boston, MA: Thomson.
White(2002). Data Communications and Computer Networks. Boston, MA: Thomson.
Whitten et al(2001). Systems Analysis and Design Methods. New York, NY: McGraw-Hill.

경향신문. “인터넷 나야나, 랜섬웨어 공격에 13억원 지불하고도 일부 서버 복구 실패”, 207.6.30.
디지털타임스. “미국의 보안시장 기술과 동향”, 2017.7.11.
디지털데일리. “문 당선, 사이버보안 컨트롤타워 신설될까?”, 2017.5.10.
보안뉴스. “사이버테러방지법 제정 놓고 대통령-국정원장 이견 노출 왜?”, 2017.5.29.
서울경제. “국내는 막막” 해외서 새 길 찾는 보안업체“, 2017.7.10.
전자신문. “사이버보안 새틀을 짜자〈5〉 법제와 정책 실효성을 높이자”, 2017.5.14..
전자신문. “정부 정보보호 인력 정원 늘리고도 안뽑아”, 2017.5.1.
조선일보. “문재인 정부 출범, 사이버 보안 전담 컨트롤 타워 신설되나”, 2017.5.12.

---

* **윤광석(尹光錫)**: 뉴욕주립대(SUNY Albany)에서 정보학 박사(논문: Testing the Firestone and McElory Knowledge Management Model: An Empirical Study, 2008)를 취득하고, 현재 한국행정연구원 연구위원으로 재직 중이다. 주요 연구관심 분야는 정보정책, 연구방법, 조직 등이다(sky@kipa.re.kr).

* **이건(李鍵)**: 일리노이주립대(University of Illinois, Chicago)에서 행정학 박사(논문: Pay-for-performance System and Job Attitudes in Government Agencies, 2011)를 취득하고, 한국행정연구원 초청연구위원을 역임하고 현재 경기대학교 행정학과 조교수로 재직 중이다. 주요 연구관심 분야는 공공관리, 거버넌스, ICT & 정보정책 등이다(givethanks@kgu.ac.kr).

논문투고일: 2017.8.28 / 심사일: 2017.11.14 / 게재확정일: 2017.12.5