국가 정보보안을 위한
대안 법안 연구 보고서

2019. 11.

사단법인 정보인권연구소

이 연구보고서는 2019년도 사단법인 한결 공익활동 지원사업으로 발간되었으며
보고서 내용은 연구자의 견해로서 사단법인 한결의 입장과 다를 수 있습니다.

연구기관 : 사단법인 정보인권연구소
연 구 자 :
이은우 (사단법인 정보인권연구소 이사, 변호사)
오병일 (사단법인 정보인권연구소 연구위원)
장여경 (사단법인 정보인권연구소 상임이사)
조지훈 (법무법인 다산, 변호사)
김 민 (진보네트워크센터 활동가)

목 차

I. 서론

□ 사물인터넷(IoT), 빅데이터, 인공지능 등 신기술의 발전과 이에 기반한 새로운 서비스의 도입이 본격화되면서 사이버보안 혹은 정보보안의 중요성이 갈수록 높아지고 있음. 사물인터넷(IoT)의 발전으로 모든 사람과 사물의 연결성이 증가하고 있으나, 경제적, 기술적인 요인으로 인한 사물인터넷 보안의 취약성이 지적되고 있음.

□ 초연결 사회에서 보안 사고는 한 사회의 경제, 나아가 국가 안보에 치명적인 영향을 미칠 수 있으며, 개인적인 차원에서도 개인의 생명과 인권을 위협할 수 있음. 예를 들어, 자율주행자동차에서의 보안 사고는 생명의 위협으로 이어질 수 있으며, 스마트도시의 보호 체계에 문제가 발생한다면 도시 생태계에 치명적인 영향을 미칠 수 있음.

□ 이처럼 정보보안의 중요성이 커지고 있음에도 불구하고, 정보보안과 관련된 국내 법제 및 거버넌스 체제는 여전히 체계성과 일관성을 결여한 상태로 수년동안 정체 상태에 있음. 논문, 토론회, 기사 등을 통해 현행 정보보안 체제의 문제점에 대한 지적이 이어지고 있음에도 불구하고, 다양한 의견들이 합리적으로 토론되고 수렴될 수 있는 구조의 부재 자체가 국내 정보보안 거버넌스의 핵심적인 문제라고 할 수 있음.

□ 현재 국내 정보보안 정책의 사실상의 컨트롤타워는 국가정보원이라고 할 수 있음. 청와대 국가안보실 내에 사이버안보비서관이 신설되기도 했지만 다시 사라졌고, 청와대에서 실무적인 차원의 컨트롤타워 역할까지 담당할 수는 없을 것임. 반면, 국가정보원은 국가사이버안전센터를 통한 실무적인 역할부터 국가안보와 관련된 보안정책까지 관여하고 있음. 법적으로도 '국가사이버안전관리규정'에 따라 국가 사이버보안 관련 정책 및 관리의 총괄·조정 역할을 맡고 있으며, 정보통신기반보호법'에 따라 공공분야 주요정보통신기반시설의 정보보안을 담당하고 있음. 나아가 국정원은 '사이버테러방지법' 혹은 '국가사이버안보법' 등의 제정을 통해 민간 정보통신망으로의 권한 확대를 추진하고 있음.

□ 그러나 국가정보원이 국가 정보보안을 담당하는 것은 '정보기관'으로서의 직무 범위를 벗어난 것임. 비록 특정 사이버 공격이 국가안보에 영향을 미칠 수 있으나, 개인의 정보보안에서부터 인터넷 상의 사기나 해킹에 이르기까지 주로 민간 부문의 보안이 대부분을 차지하는 것을 고려할 때, 정보보안 업무 전체를 국가안보적 시각에서 바라보는 것은 협소한 시각임.

□ 또한, 정보보안 영역에서도 국정원의 권한 남용으로 인한 감시와 사찰을 우려할 수 밖에 없고, 정보보안 정책에 대한 합리적인 토론과 민간과의 협력을 위축시켜 오히려 국내 정보보안에 부정적인 영향을 초래하고 있음. 현재 국내 정보보안 거버넌스에 대한 합리적인 토론이 제대로 이루어지기 힘든 것도 국정원이 컨트롤타워 역할을 함으로써 발생하는 은밀하고 경직된 분위기가 하나의 원인이라고 할 수 있을 것임.

□ 이에 시민사회에 국정원의 정보보안 권한을 일반 행정부처로 이관해야 한다고 주장해왔음. 즉, 국가 정보통신망의 정보보안에 대한 책임, 정보보호시스템에 대한 인증, 암호 인증 등 현재 국정원이 담당하고 있는 역할을 일반 행정부처로 이관할 필요가 있다는 것임.

□ 한편, 현재 국가정보원 개혁이 추진되고 있으나, 수사권 이관이나 국가정보원에 대한 감독 기능 강화 등만이 이슈가 되고 있을 뿐, 문재인 정부에서도 국가정보원의 정보보안 권한 이양에 대해서는 별다른 관심이 없음. 이에 대안적인 국가 정보보안 거버넌스 구축을 위한 입법을 통해 국가정보원 개혁 법안의 논의 과정에서 정보보안 권한의 이양 문제도 함께 다루어지도록 할 필요가 있음.

□ 시민사회에서는 '사이버테러방지법' 등에 대한 비판을 제기해왔으나, 지금까지 국가 정보보안 거버넌스에 대한 구체적인 대안은 제시하지 못해왔음. 이 연구 보고서는 국내 정보보안 거버넌스에 대한 시민사회의 대안을 수립하고, 이를 실제 입법에 활용될 수 있는 대안 법안의 형태로 제안하고자 함.

Ⅱ. 국내 정보보안 거버넌스 현황 및 문제점

1. 정보보안 관련 법제 현황

1) 개요

□ 국내 정보 보안을 규율하는 일반법은 존재하지 않으며, 각 부문과 목적별로 개별법만이 존재함.

□ ‘국가사이버안전관리규정’과 ‘전자정부법’이 공공부문, ‘정보통신망법’, ‘전자금융거래법’이 민간부문의 정보 보안 관련 규정을 담고 있으며, 공공과 민간부문을 포괄하는 법으로 ‘정보통신기반보호법’과 ‘국가정보화기본법’이 있음.

□ 2001년 민간과 공공의 중요한 정보통신기반시설 보호를 다룬 「정보통신기반보호법」이 제정되었고, 「정보통신망 이용촉진 등에 관한 법률」을 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」로 변경하며 정보보호와 관련된 규정을 강화하였고, 2005년 국가안보와 국가정보통신망을 사이버공격으로부터 보호하기 위해 관련 조직 및 운영을 정립한 「국가사이버안전관리규정」이 대통령훈령으로 제정되었음.

<표 1> 정보보안 관련 법제 현황

	관할 부문	관할 부처
정보통신망법	민간 정보통신망 일반	과학기술정보통신부
정보통신기반보호법	민간 기반 시설	과학기술정보통신부
	공공 기반 시설	국가정보원
국가사이버안전관리규정	공공 정보통신망 일반	국가정보원

2) 정보통신망 이용촉진 및 정보보호 등에 관한 법률

가. 법률의 배경 및 목적

□ 정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 정보통신망법)의 목적은 “정보통신망의 이용을 촉진하고 정보통신서비스를 이용하는 자의 개인정보를 보호함과 아울러 정보통신망을 건전하고 안전하게 이용할 수 있는 환경을 조성하여 국민생활의 향상과 공공복리의 증진에 이바지”하는

것으로 정보통신망의 안정성과 개인정보 보호 등의 정보보호 조치와 추진체계를 규율하고 있음

□ 2001년 기존 「정보통신망 이용촉진 등에 관한 법률」에서 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」로 명칭을 변경하며 정보보호와 관련된 규정이 강화되었고 지속적으로 침해사고 대응 관련 규정 등이 추가적으로 정비됨

나. 주요 내용

□ 정보통신망의 안전성 확보

- 과학기술정보통신부장관은 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치의 구체적 내용을 정한 정보보호지침을 정해 이를 고시하고, 이를 정보통신서비스 제공자가 지키도록 권고할 수 있음
- 정보통신서비스 제공자는 정보통신시스템에 대한 보안 및 정보의 안전한 관리를 위해 정보보호최고책임자를 지정할 수 있으며, 특히 매출액, 종업원 수 등이 대통령령으로 정하는 기준에 해당하는 제공자의 경우, 정보보호최고책임자를 지정하고 이를 과학기술정보통신부장관에게 신고해야 함

□ 집적된 정보통신시설의 보호

- 타인의 정보통신서비스 제공을 위해 집적된 정보통신시설을 운영·관리하는 사업자는 정보통신시설을 안정적으로 운영하기 위해 대통령령으로 정하는 바에 따른 기술적·관리적·물리적 보호조치를 하여야 하며, 기타 운영장애로 발생한 피해를 보상하기 위하여 대통령으로 정하는 바에 따라 보험에 가입하여야 함.

□ 정보보호관리체계의 인증

- 집적정보통신시설 사업자, 매출액 또는 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 자 등은 정보통신망의 안정성과 신뢰성의 확보를 위해 관리적·기술적·물리적 보호조치를 포함한 정보보호 관리체계를 수립·운영하고, 과학기술정보통신부장관이 정해 고시하는 정보보호 관리체계 인증을 받아야 함.

□ 침해사고의 대응

- 과학기술정보통신부장관은 침해사고에 관한 정보의 수집 및 전파, 예보 및 경보, 침해사고에 대한 긴급조치 등의 업무를 수행하고, 한국인터넷진흥원이 업무의 전부 또는 일부를 수행하도록 할 수 있음

- 정보통신서비스 제공자 및 집적정보통신시설 사업자 등은 침해사고의 유형별 통계, 접속 경로별 이용 통계 등 침해사고 관련 정보를 과학기술정보통신부장관 또는 한국인터넷진흥원에 제공해야 함

- 정보통신서비스 제공자 및 집적정보통신시설 사업자는 침해사고가 발생하면 즉시 과학기술정보통신부장관 또는 한국인터넷진행원에 이를 신고해야 하며, 과학기술정보통신부장관은 정보통신망에 중대한 침해사고가 발생하면 피해 확산 방지, 사고대응 등을 위해 민·관합동조사단을 구성해 그 원인을 분석할 수 있음

- 침해사고의 원인을 분석하기 위해 과학기술정보통신부장관이 필요성을 인정한 경우, 정보통신서비스 제공자와 집적정보통신시설 사업자에게 관련 자료의 보전을 명할 수 있으며, 민·관합동조사단에게 관계인의 사업장에 출입해 침해사고의 원인을 조사하도록 명할 수 있지만 통신비밀보호법 제2조제11호에 따른 통신사실확인자료에 해당하는 자료는 불가능함

3) 정보통신기반 보호법

가. 법률의 목적 및 배경

□ 정보통신기반 보호법의 목적은 “전자적 침해행위에 대비하여 주요정보통신기반시설의 보호에 관한 대책을 수립·시행함으로써 동 시설을 안정적으로 운용하도록 하여 국가의 안전과 국민생활의 안정을 보장”하는 것으로 주요 정보통신기반시설을 보호하기 위하여 침해행위 대응을 위한 보호체계, 취약점 분석·평가, 대책의 수립·시행을 규정한 법률임

□ 정보화 사회로 돌입하며 정보통신 시스템의 중요성이 점차 커짐에 따라 2001년 에너지·금융·통신 등 국가와 사회의 중요한 정보통신기반시설 보호를 주 내용으로 제정되었고, 국가 및 공공기관의 정보통신기반시설 뿐만 아니라 민간이 운영하고 관리하는 시설 또한 그 범위가 적용되는 공공부문과 민간부문을 모두 규율하는 법률임

나. 주요 내용

□ 정보통신기반위원회

- 국무총리 소속 하에 국무조정실장을 위원장으로 두고, 대통령령이 정하는 중앙행정기관의 차관급 공무원과 위원장이 위촉하는 위원 25인 이내로 구성됨

- 주요정보통신기반시설 보호정책의 조정, 보호계획의 종합·조정, 보호계획의 추진 실적, 주요정보통신기반시설 보호와 관련된 제도의 개선 및 기반시설의 지정 및 지정 취소 등을 심의

- 정보통신기반보호실무위원회를 두고, 동 위원회에 제출된 안건과 위원회로부터 위임받거나 위원장으로부터 지시받은 사항을 검토 및 심의하며 보호대책 및 보호계획 수립 지침을 배포하고 주요정보통신기반시설의 신규지정 권고 등 역할을 수행함.

- 실무위원회의 구성에 있어 공공분야는 국가정보원 차장을 그 위원장으로 두고, 민간분야는 과학기술정보통신부 차관을 그 위원장으로 둠.

□ 정보통신기반시설 및 주요정보통신기반시설

- 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 정보통신망을 정보통신기반시설로 규정하며, 중앙행정기관은 전자적 침해행위로부터 보호가 필요하다고 인정되는 정보통신기반시설을 정보통신기반보호위원회의 심의를 거쳐 주요 정보통신기반시설로 지정함

- 과학기술정보통신부장관과 국가정보원장 등은 특정한 정보통신기반시설을 주요정보통신기반시설로 지정할 필요가 있다고 판단하고 이를 권고할 수 있음

□ 주요정보통신기반시설 보호 추진 체계 및 대책 수립

- 분야별 정보통신기반시설을 보호하기 위해 침해사고 예방 및 복구 지원, 취약점 및 침해요인과 대응방안에 관한 정보 제공, 실시간 경보 등의 기술적 업무를 수행하고자 하는 자는 정보공유·분석센터를 운영할 수 있으며, 주요정보통신기반시설을 관리하는 기관은 위의 업무를 위탁할 수 있음

- 주요정보통신기반시설을 관리하는 기관은 소관하는 주요정보통신기반시설의 취약점을 분석·평가하며, 국가보안기술연구소, 한국인터넷진흥원, 정보공유·분석센터, 지식정보보안 컨설팅 전문업체에 이를 위탁할 수 있음

- 주요정보통신기반시설을 관리하는 기관은 취약점 분석·평가 결과에 따라 보호대책을 수립·시행하고, 관계 중앙행정기관에게 이를 제출하며 관계 중앙행정기관의 장은 보호계획 수립·시행, 보호지침 제정, 보호조치 명령 또는 권고할 수 있음

- 과학기술정보통신부장관과 국가정보원장은 주요정보통신기반시설 보호대책 및 보호계획 등을 관계 중앙행정기관의 장에게 통보할 수 있고, 이에 대한 이행여부를 확인할 수 있음

□ 침해사고에 대한 통지 및 복구조치

- 관리기관의 장은 침해사고가 발생해 소관하는 주요정보통신기반시설이 교란·마비 또는 파괴된 사실을 인지한 때 관계 행정기관, 수사기관 또는 인터넷진흥원과 같은 관계기관에 통지하고, 복구 및 보호조치에 필요한 지원을 요청할 수 있음

- 관리기관의 장은 소관 주요정보통신기반시설에 대한 침해사고가 발생한 때 해당 정보통신기반시설의 복구 및 보호에 필요한 조치를 취해야 하며, 필요한 경우 관계중앙행정기관의 장 또는 인터넷진흥원의 장에게 지원을 요청할 수 있음

- 국가안전보장에 중대한 영향을 미치는 도로·철도 등 주요 교통시설, 전력·가스 등 에너지·수자원 시설, 방송중계·국가지도통신망 시설과 같은 주요정보통신기반시설의 경우 국가정보원장에게 우선적으로 지원을 요청해야 함

- 정보통신기반위원회의 위원장은 주요정보통신기반시설에 대해 광범위한 침해사고가 발생했을 때 정보통신기반 침해사고 대책본부를 둘 수 있음

4) 국가사이버안전관리규정

가. 규정의 목적 및 배경

□ 2005년 국가안보에 대한 위협을 중심으로 국가정보통신망을 보호하기 위해 관련 조직 및 운영에 대한 사항을 체계적으로 정립한 대통령 훈령임.

□ 공공부문의 정보보호 추진체계를 구성하고 있으며, 국가사이버안전 관련 정책 총괄·조정, 국가사이버안전센터, 사이버위기 대책본부 구성·운영, 관련 연구개발 시책 추진 등 정보보호 체계에 있어 국가정보원이 가진 역할과 권한이 주된 내용으로 함

나. 주요 내용

□ 정의 및 적용범위

- 국가사이버안전관리규정은 중앙행정기관, 지방자치단체 및 공공기관의 국가정보통신망을 그 보호대상으로 하며,

정보통신기반보호법에 따른 주요정보통신기반시설에 대해서는 정보통신기반보호법을 우선 적용함

- 국가사이버안전관리규정은 해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입·교란· 마비·파괴하거나 정보를 절취·훼손하는 공격행위 등을 '사이버공격'으로 정의함

□ 대응체계

- 국가정보원장이 관계 중앙행정기관의 장과 협의해 사이버안전 관련 정책 및 관리를 총괄·조정하며, 이에 대한 체계적 수행을 위하여 관계 중앙행정기관의 장과 협의해 국가사이버안전기본계획을 수립·시행함

- 국가사이버안전전략회의

  - 국가정보원장을 의장, 관계 중앙행정기관의 차관 및 국가정보원장이 지명하는 관계 중앙행정기관의 차관급 공무원을 위원으로 둠

  - 국가사이버안전체계의 수립 및 개선에 관한 사항, 국가사이버안전 관련 정책 및 기관 간 역할조정에 관한 사항, 국가사이버안전 관련 대통령 지시사항에 대한 조치방안 등을 심의

- 국가사이버안전대책회의

  - 국가사이버안전전략회의의 효율적 운영을 위해 전략회의에 국가사이버안전대책회의를 두며, 국가정보원의 사이버안전업무를 담당하는 차장을 대책회의의 의장으로 두고, 전략회의의 위원이 속하는 기관의 실·국장급 공무원을 위원으로 둠

  - 국가사이버안전 관리 대책방안, 전략회의의 결정사항에 대한 시행방안, 전략회의로부터 위임받거나 지시받은 사항 등을 심의

- 국가사이버안전센터

  - 국가정보원장 소속으로 운영되며, 국가차원의 종합적이고 체계적인 대응을 위해 국가사이버안전정책의 수립, 전략회의 및 대책회의의 운영에 대한 지원, 사이버위협 관련 정보의 수집·분석·전파, 국가정보통신망의 안전성 확인, 국가사이버안전매뉴얼의 작성·배포, 사이버공격으로 인하여

발생한 사고의 조사 및 복구 지원, 외국과의 사이버위협 관련 정보의 협력 등의 업무를 수행함

- 국가정보원장은 국가 차원의 사이버위협에 대한 종합 판단, 상황관제, 분석 및 합동조사 등을 위해 센터에 민·관·군 합동대응반을 설치·운영할 수 있음

□ 사전예방 및 사후대응 조치

● 중앙행정기관의 장은 소관분야의 정보통신망을 보호하기 위한 사이버안전대책을 수립·시행하고, 지도·감독해야 하며, 국가정보원장은 관계 중앙행정기관의 장과 협의해 사이버안전대책의 수립에 필요한 국가사이버안전매뉴얼 및 관련 지침을 작성·배포할 수 있고 이에 대한 이행여부 진단·평가 등 정보통신망에 대한 안정성을 확인하고 시정 조치 등을 권고함

● 중앙행정기관, 지방자치단체 및 공공기관의 장은 소관하는 정보통신망을 대상으로 매년 정기적인 사이버위기 대응 훈련을 실시해야 하며, 국가정보원장은 국가 차원의 사이버위기 발생에 대비해 위 규정의 정보통신망을 대상으로 사이버위기 대응 통합훈련을 실시 및 이에 따른 필요한 시정조치를 요청할 수 있음

● 중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장은 국가정보통신망에 대한 사이버 공격의 계획, 공격사실 등의 정보를 입수한 경우 국가안보실장 및 국가정보원장에게 통보해야 하며, 수사사항에 대해서는 수사기관의 장이 국가기밀의 유출·훼손 등 국가안보의 위협을 초래한다고 판단되는 경우에 이를 통보해야 하고, 이러한 정보를 제공 받은 경우 국가정보원장은 대응에 필요한 조치를 강구하고 그 결과를 해당기관의 장에게 통지함

● 보안관제센터의 설치·운영

- 중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장은 사이버공격 정보를 탐지·분석해 즉시 대응 조치를 할 수 있는 기구인 보안관제센터를 설치·운영해야 하며, 그렇지 못하는 경우 국가정보원을 포함한 다른 중앙행정기관의 장 등이 설치·운영하는 보안관제센터에 그 업무를 위탁

- 보안관제센터를 설치·운영하는 기관의 장은 수집·탐지한 사이버공격 정보를 국가정보원장 및 관계 기관의 장에게 제공하며, 미래창조과학부장관이 지정하는 보안관제 전문업체의 인원을 파견받아 보안관제업무를 수행하도록 할 수

있으며, 보안관제전문업체의 지정·관리에 필요한 사항은 미래창조과학부장관이 국가정보원장과 협의하여 정함

- 국가정보원장은 사이버공격에 대한 대응·대비를 위해 사이버공격의 파급영향·피해규모를 고려해 관심·주의·경계·심각 등 수준별 경보를 발령할 수 있으며, 민간분야는 미래창조과학부장관, 국방분야는 국방부장관이 경보를 발령하고, 국가정보원장은 위 규정을 위해 필요한 정보를 관계 중앙행정기관의 장에게 요청할 수 있으며 특별한 사유가 없는 한 이에 협조해야 함

- 중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장은 사이버공격으로 인한 사고의 발생 등을 발견한 경우 피해를 최소화하는 조치를 취한 후, 그 사실을 국가안보실장, 국가정보원장 및 관계 중앙행정기관의 장에게 통보해야 함

- 국가정보원장은 사이버공격으로 인해 발생한 사고에 대해 원인 분석을 위한 조사를 실시할 수 있으며, 경미한 사고의 경우 해당 기관의 장이 자체 조사 후 사고개요 및 조치내용 등 관련 사항을 국가정보원장에게 통보해야 함

- 사이버공격으로 인해 피해가 심각하다고 판단되는 경우나 주의 수준 이상의 경보가 발령된 경우, 국가정보원장은 관계 중앙행정기관의 장과 협의해 범정부적 사이버위기 대책본부를 구성·운영할 수 있으며, 사이버위기 대책본부 내에 합동조사팀 등 필요한 하부기구를 둘 수 있고, 이 구성·운영 등의 사항은 국가정보원장이 관계 중앙행정기관의 장과 협의하여 정함

5) 국가사이버안보법안(안)

가. 법안의 목적 및 배경

□ 2016년 국가정보원이 입법예고했던 ‘국가사이버안보기본법’이 수정된 것이며, 기존의 대통령 훈령인 ‘국가사이버안전관리규정’을 기본 틀로 하였으나 그 적용범위를 정보통신기반시설과 주요 민간 사업자의 정보통신망으로 확대하는 등 국가정보원의 정보 보호 관련 권한의 법률적 근거를 마련한 법안으로 2017년 정부가 발의함

나. 주요 내용

□ 정의 및 적용범위

- 국가사이버안보법안은 다른 법률과의 관계에 있어 사이버안보에 관하여는 다른 법률에 우선하여 본 법을 적용함

- 정보통신망법에 따른 정보통신망의 정보처리영역을 ‘사이버공간’으로, 해킹 등의 전자적 방법으로 사이버공간을 불법침입·교란·마비·파괴하거나 정보를 빼내거나 훼손하는 등의 공격행위를 ‘사이버공격’으로 정의함

- 군사분계선 이북지역에 기반을 두고 있는 반국가단체의 구성원또는 그 지령을 받은 자가 하는 사이버공격, 에너지·통신·교통·금융 등 국가기반체계 또는 전자정부를 운영하는 데 사용되는 사이버공간 등 국가적 사이버공간을 불법침입·교란·파괴하는 사이버공격 등을 ‘국가안보위협 사이버공격’으로 정의함

□ 대응 체계

- 국가사이버안보위원회

  - 사이버안보에 관한 국가의 정책 및 전략 수립, 제도 및 법령의 개선, 지원기관 지정 및 취소, 중요 중장기 대책 등을 심의하기 위해 대통령소속으로 국가사이버안보위원회를 둠

  - 위원회의 위원장으로 국가안보실장을 두며, 국가안보실장이 국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관과 대통령 소속 기관과 국무총리 소속 기관을 포함한 중앙행정기관의 차관급 공무원 중에서 대통령령으로 정하는 사람 또는 사이버안보에 관해 전문적 지식과 경험을 갖춘 사람을 위원으로 임명하거나 위촉

  - 위원회는 직무수행을 위해 필요한 자료의 제출을 책임기관과 지원기관에 요청할 수 있으며, 위원회에 국가 사이버안보 실무위원회를 두고, 안건 검토 및 위원회가 위임한 안건을 심의하게 할 수 있음

- 책임기관

  - 국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관 및 그 소속기관 등을 책임기관이라 하며, 해당 기관의 장은 소관하는 사이버공간을 안전하게 보호하는 책임을 짐

- 지원기관

  - 국가정보원장은 위원회의 심의를 거쳐 지원기관을 지정 및 지정취소를 할 수 있으며, 관계 중앙행정기관과 합동으로

지원기관의 기술적 지원 실태를 점검하고 지원기관의 기술적 지원에 드는 비용을 지원

- 사이버공격의 탐지 및 대응, 사이버공격으로 인한 사고의 조사, 피해발생의 최소화 및 피해복구를 위한 조치, 사이버위기대책본부가 하는 원인 분석 등의 조치를 지원

● 국가정보원장은 사이버안보에 필요한 정책과 기술을 연구·개발하기 위해 사이버안보 연구기관을 설립하거나 설립된 기관 또는 기관 부설연구소를 관계 중앙행정기관의 장과 협의해 사이버안보 연구기관으로 지정

□ 사전예방 및 사후대응

● 국가정보원장은 3년마다 위원회의 심의를 거쳐 사이버안보의 정책 목표와 추진방향, 관련 제도 및 법령 개선, 예방 및 대응, 정책·기술의 연구·개발, 교육 및 훈련 등의 사항이 포함된 사이버안보 기본계획을 수립·시행해야 함

● 국가정보원장은 책임기관을 대상으로 사이버안보를 위한 업무수행체계 구축, 사이버공격 예방 및 대응 등에 관한 실태평가를 할 수 있으며, 이에 대한 전문적·기술적 연구 또는 자문을 위해 사이버안보실태 합동평가단을 구성·운영할 수 있음

● 국가정보원장 소속으로 사이버위협정보 공유센터를 두며, 센터는 사이버공격 방법에 관한 정보, 악성프로그램 및 관련 정보, 정보통신망·정보통신기기 및 소프트웨어의 보안상 취약점에 관한 정보 등을 공유함.

● 국가정보원장은 관계 중앙행정기관의 장과 협의해 국가 차원의 사이버공격 탐지·대응체계를 구축·운영해야 하며, 책임기관의 장은 위의 탐지·대응체계를 위해 소관 사이버공간에서 발생하는 사이버공격을 탐지하고 대응할 수 있는 보안관제센터를 설치·운영해야 하고, 보안관제센터를 설치·운영할 수 없는 경우 다른 책임기관의 장이 설치·운영하는 보안관제센터에 그 업무를 위탁할 수 있음

● 국가정보원장은 국가안보위협 사이버공격에 관한 통보를 받은 경우, 상급책임기관의 통보를 받은 경우 등에 있어 사이버공격으로 인한 사고의 피해 확인, 원인 분석 및 재발 방지를 위한 조사를 해야 하며, 민간 분야 책임기관의 경우 관계 중앙행정기관, 수사기관 및 지원기관으로 구성된 합동조사팀을 운영

- 상급책임기관의 장은 관할 사이버공간에 대통령령으로 정하는 단계 이상의 경보 또는 분야별 경보가 발령된 경우나 사이버공격으로 인해 그 피해가 심각하다고 판단하는 경우 책임기관, 지원기관, 수사기관이 참여하는 사이버위기대책본부를 구성·운영할 수 있으며, 2개 이상의 상급책임기관에 대책본부를 구성하는 경우에는 국가정보원장이 상급책임기관의 장과 협의하여 대책본부를 구성·운영할 수 있음

2. 정보보안 관련 국가정보원의 역할[1]

□ 국가정보원은 국가정보원법, 정보통신기반보호법, 전자정부법, 보안업무규정, 국가사이버언전관리규정 등에 근거하여 국가사이버안전정책 및 관리의 총괄·조정, 국가사이버안전센터의 운영, 공공영역의 주요정보통신기반시설의 보호, 정보보안 관리실태 평가, 보안적합성 검증, 암호모듈 검증 등 정보 보호와 관련한 핵심적인 업무를 총괄하고 있음

1) 국가사이버안전 정책·관리 총괄·조정 (국가사이버안전관리규정)

□ 국가사이버안전기본계획 수립·시행

- 국가정보원은 국가사이버안전과 관련된 정책 및 관리를 관계 중앙행정기관의 장과 협의하여 총괄·조정하도록 하고, 이를 위해 국가사이버안전기본계획을 수립·시행하도록 하고 있음

□ 국가사이버안전전략회의

- 국가사이버안전에 관한 수립 및 개선, 정책 및 기관 간 역할조정 등의 사항을 심의하며, 국가정보원장을 의장으로 두고, 관계 중앙행정기관의 차관급 공무원으로 전략회의의 위원이 구성됨.

□ 국가사이버안전대책회의

- 전략회의의 효율적 운영을 위해 국가사이버안전대책회의를 두고 있으며 대책회의의 의장은 국가정보원의 사이버안전업무를 담당하는

[1] 이 절의 내용은 <국가정보원과 국내 사이버 보안 정책 개혁 방안>(이은우, 오병일, 장여경. 2016) 3장 '국내 사이버 보안 정책과 국가정보원'의 내용을 요약한 것임.

차장, 위원은 전략회의의 위원이 속하는 기관의 실·국장급 공무원으로 구성됨

2) 국가사이버안전센터 운영 (국가사이버안전관리규정 제8조)

□ 2003년 1.25 인터넷 대란을 계기로, 2004년 2월 국가정보원이 설립, 국가정보원장 소속

□ 국가보안관제센터로서 부문·단위보안관제센터에 사이버공격을 탐지할 수 있는 기술을 배포하고 국가안보를 위협하는 사이버공격을 탐지·대응, 국가사이버안전매뉴얼 작성·배표, 사이버공격으로 인한 사고의 조사 및 복구지원 등 실무차원의 컨트롤타워 역할을 수행

□ 국가정보원장은 국가 차원의 사이버위협에 대한 종합판단, 상황관제, 위협요인 분석 및 합동조사 등을 위해 사이버안전센터에 민·관·군 합동대응반을 설치·운영

3) 공공분야 주요정보통신기반시설의 보호 (정보통신기반보호법)

□ 국가정보원은 과학기술정보통신부 및 국방부와 함께 주요정보통신기반시설의 보호를 책임지고 있으며, 국가정보원은 공공영역의 주요정보통신기반시설을 관할하지만, 경우에 따라 민간영역의 주요정보통신기반시설의 사이버보안에도 관여

□ 정보통신기반보호법에 따라 국가정보원은 공공영역 정보통신기반시설에 대하여 보호대책 및 수립지침 수립, 기반시설의 사전조사 및 지정권고, 보호대책의 이행 여부 확인 및 개선 권고, 관리기관에 대한 기술적 지원 등 대책 수립부터 피해 조사까지 광범위한 권한을 가지고 있으며, 구체적으로 명시된 권한은 다음과 같음

(a) 국가정보원 차장이 정보통신기반보호위원회 위원으로 참여 (제3조3항, 시행령 제2조)
(b) 국가정보원 차장이 공공분야 실무위원회 위원장을 담당 (제3조 4항, 시행령 제5조)
(c) (공공분야)관리기관에 대하여 주요정보통신기반시설 보호대책의 이행 여부확인
(d) 주요정보통신기반시설 보호대책의 이행 여부 확인을 위하여 필요한 경우, 관계중앙행정기관의 장에게 주요정보통신기반시설보호대책 등의 자료 제출 요청(제5조의2 2항), 보호조치의 세부적인 내용을 확인·점검 (시행령 제9조의2 3항)
(e) 확인한 주요정보통신기반시설보호대책의 이행 여부를 관계중앙행정기관의 장에게 통보(제5조의2 3항)

(f) 과학기술정보통신부 장관과 협의하여, 주요정보통신기반시설보호대책 및 주요정보통신기반시설보호계획의 수립지침을 정하여 이를 관계중앙행정기관의 장에게 통보(제6조 4항)
(g) 관리기관에 대한 기술적 지원(제7조 1항)
(h) 국가안전보장에 중대한 영향을 미치는 주요정보통신기반시설에 대한 관리기관의 장이 기술적 지원을 요청하는 경우에 국가정보원이 우선적으로 지원. 국가안전보장에 현저하고 급박한 위험이 있고, 관리기관의 장이 요청할 때까지 기다릴 경우 그 피해를 회복할 수 없을 때에는 요청이 없더라도 관계중앙행정기관의 장과 협의하여 지원할 수 있음.(제7조 2항) 다만, 금융 정보통신기반시설 등 개인정보가 저장된 모든 정보통신기반시설에 대하여 기술적 지원을 수행해서는 안됨.(제7조 3항)
(i) 필요하다고 판단할 경우, 중앙행정기관의 장에게 특정 정보통신기반시설을 주요정보통신기반시설로 지정하도록 권고할 수 있는 권한(제8조의2 1항)
(j) 이러한 권고를 위해 필요한 경우, 중앙행정기관의 장에게 해당 정보통신기반시설에 관한 자료를 요청(제8조의2 2항), 주요정보통신기반시설지정 조사반을 통해 주요정보통신기반시설 지정 필요성을 검토(시행령 제16조의2 1항)
(k) 과학기술정보통신부 장관과 취약점 분석·평가에 관한 기준을 정할 때 협의 (제9조 4항)

4) 공공기관 정보보안 관리실태 평가

□ 국가 정보보안 정책의 이행실태를 확인하고 각급 기관의 보안관리 체계를 강화하기 위한 제도 (국가정보원법 제3조 제2항, 전자정부법 제56조 제3항, 정부업무평가기본법 제14조.제21조.제22조, 국가사이버안전관리규정 제9조 제4항, 국가정보보안기본지침 제121조)

□ 국가정보원이 매년 평가대상 및 일정을 확정하여 대상기관에 통보하며, 각급 기관이 기관별 자체평가를 진행하고 국가정보원이 현장실사, 평가 증빙, 평가결과 통보하는 등, 전 과정을 관장

<표 2> 정보보안 관리실태 평가 절차

평가 단계	주체
1. 기관 자체 평가	각 기관
2. 현장실사	국가정보원
3. 추가증빙 및 이의신청	각 기관
4. 평가결과 검토·확인	평가위원회

5. 평가결과 통보	국가정보원

* 출처 : 2019 국가정보보호백서

5) 국가·공공기관이 도입하는 정보보호시스템에 대한 보안적합성 검증(전자정부법)

□ 국가·공공기관이 도입하는 정보보호시스템 등 IT제품 보안기능에 대한 안전성을 검증하는 제도

□ 국가정보원이 2001년 9월부터 보안적합성 검증업무를 담당

- 정보보호 시스템 보안적합성 시험 기준.방법 수립
- 국가·공공기관의 보안적합성 검증신청서 접수
- 시험기관에 시험의뢰 및 시험결과 검토
- 검증결과 통보 및 보완조치 이행여부 확인

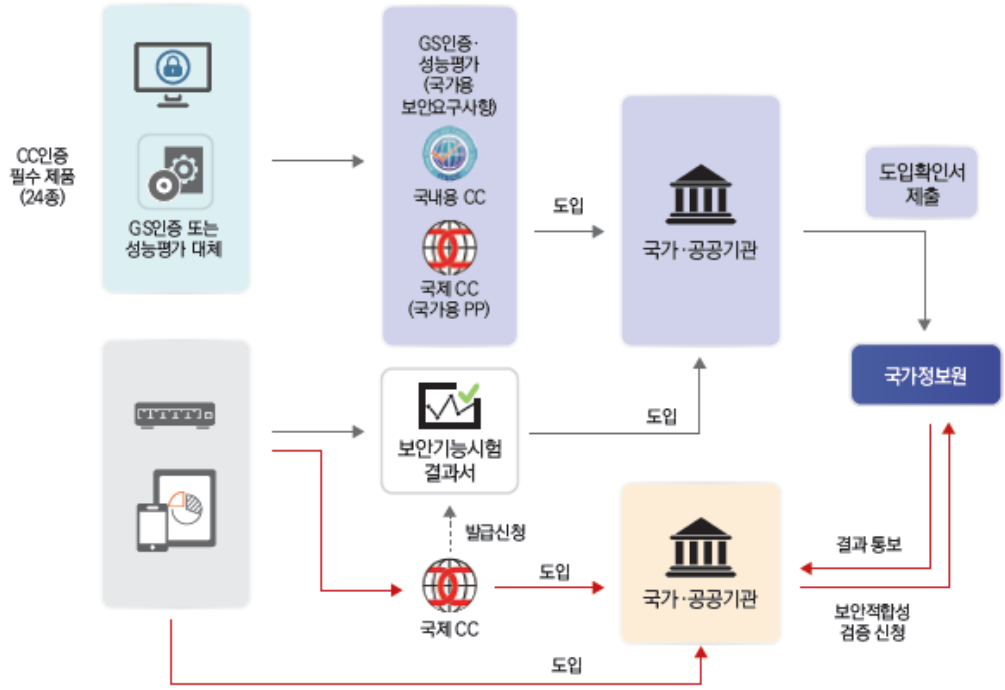
□ 국가보안기술연구소가 보안적합성 시험업무를 담당

- 정보보호시스템 보안적합성 시험기준·방법 연구
- 정보보호시스템에 대한 시험실시 및 시험결과 작성
- 필요 시 보완사항에 대한 추가시험 실시

<그림 1> 보안적합성 검증 절차

* 출처 : 국가정보원

<그림 2> 국가·공공기관의 IT제품 도입 절차



* 출처 : 2019국가정보보호백서

6) 암호모듈 검증(전자정부법 및 암호모듈 시험 및 검증지침)

□ 국가·공공기관 정보통신망에서 소통되는 자료 중에서 비밀로 분류되지 않는 중요 정보를 보호하기 위해 사용되는 암호모듈의 안정성과 구현적합성을 검증하는 제도

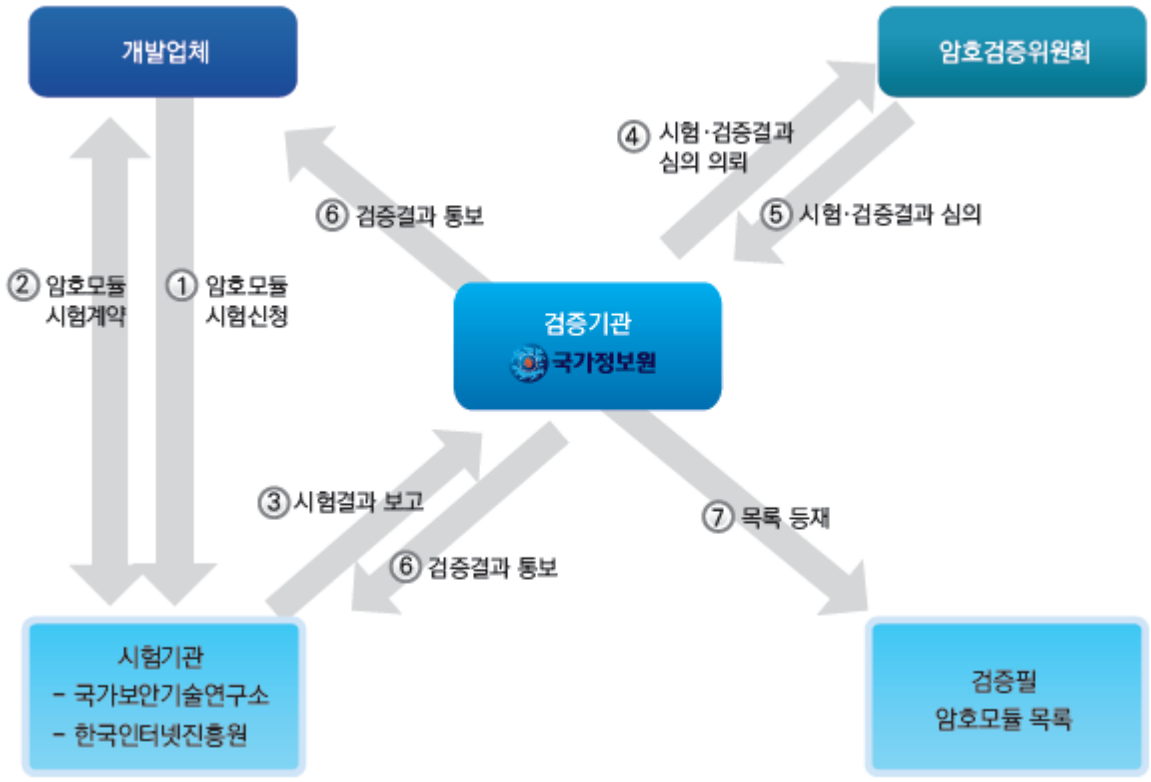
□ 국가·공공기관에서 사용되는 정보보호제품에 중요 자료를 저장·소통하기 위한 암호 기능이 포함될 경우는 반드시 검증필 암호모듈을 탑재해야 함.

□ 국가정보원은 그 검증기관으로 1)암호모듈 검증 관련 정책 수립 및 시행 2)검증 기준 개발 및 시험 관련 기술 승인 3)시험기관 지정·관리·감독 및 시험결과 검증 4)검증위원회 개최 4)검증필 암호모듈 목록 관리

□ ETRI 부설국가보안기술연구소는 그 시험기관으로 1)암호모듈 검증계약 체결 및 시험 업무 수행 2)암호모듈 시험 관련 기준 및 기술연구·개발

□ 2018년 한국인터넷진흥원(KISA)가 암호모듈 시험기관으로 추가 지정

<그림 3> 암호모듈 검증체계



* 출처 : 2019국가정보보호백서

7) 보안관제 및 사이버 공격 정보 수집 (국가사이버안전관리규정)

□ 국가사이버안전관리규정에 따라 국가·공공기관이 직접 보안관제센터를 설치·운영하지 못하는 경우에 국정원 등 다른 중앙행정기관의 장에게 업무를 위탁할 수 있음

□ 국가사이버안전관리규정에 따라 국가정보원장은 각 보안관제센터에서 수집·탐지한 사이버공격 정보를 제공받으며 보안관제센터의 설치·운영 및 사이버공격 정보의 제공 범위, 절차 및 방법 등 세부사항을 관계 중앙행정기관의 장과 협의하여 정함

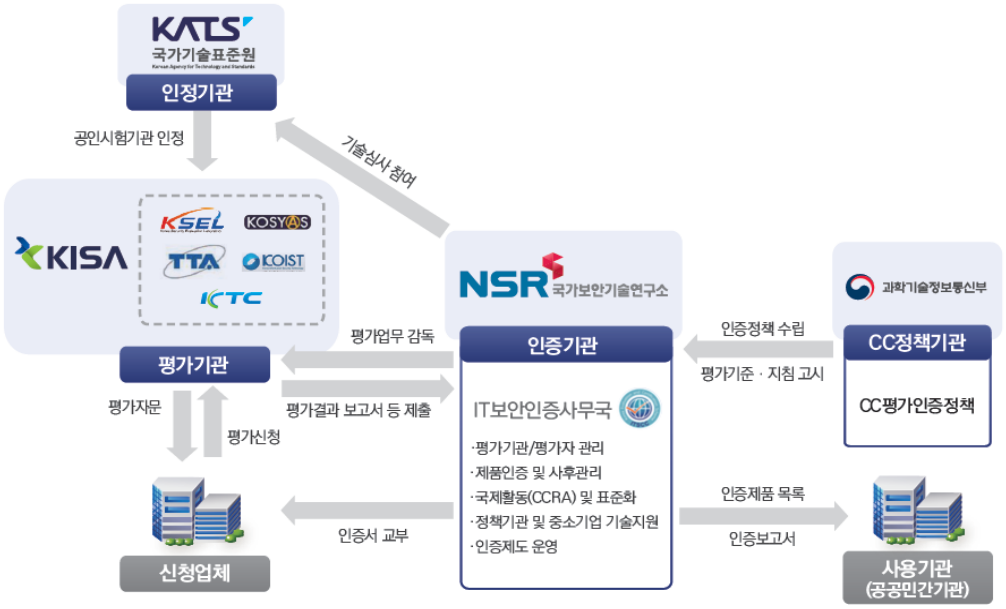
□ 국가정보원 국가사이버안전센터는 단위보안관제(각급기관) -> 부문보안관제(중앙행정기관) ->국가보안관제(국가사이버안전센터)로 구성된

국가·공공기관 3단계 사이버공격 탐지·차단체계의 국가보안관제센터로,
보안관제센터 간 시스템을 통해 실시간으로 사이버공격 정보를 공유

8) 정보보호제품 평가·인증에 관여 (국가정보화기본법, 정보보호시스템 평가·인증지침)

□ 민간업체가 개발한 정보보호시스템에 구현된 보안기능의 안전성과 신뢰성을 보증하여 국가·공공기관이 안전한 정보보호제품을 선택하고 사용할 수 있도록 하는 제도

<그림 4> 정보보호제품 평가 ·인증체계



* 출처 : 2019국가정보보호백서

□ 정보보호시스템평가·인증지침 2.2.1에 따르면 그 인증기관으로 한국전자통신연구원 부설 국가보안기술연구소로 하고 있는데, 국가보안기술연구소는 '국가정보보안에 관련된 임무를 수행하는 연구기관'으로 조직이나 운영과 관련한 자세한 사항이 공개되어 있지 않고, 국가정보원 출신이 연구소장 및 연구원으로 재취업하는 등 공식적으로는 한국전자통신연구원 부설 기관으로 되어 있지만, 사실상 국가정보원 산하 연구소로 역할하고 있는 것으로 보임.

□ 또한 2019국가정보보호백서에 따르면, 2016년 국가정보원·미래창조과학부·국가보안기술연구소 등이 국가·공공기관용 평가·인증대상을 24종으로 개편하고, 국가정보원과 미래창조과학부가 국내용 정보보호제품 보안요구사항만을 보유한 22종을 대상으로 국제용 보호프로파일을 순차적으로 개발하는 데 합의하는 등, 정보보호제품 평가·인증에 있어 국가정보원이 관여하는 것으로 보임

3. 국내 정보보안 거버넌스의 문제점

1) 종합적인 정보보안 전략의 부재

(1) 2009년 : 국가 사이버위기 종합대책 (7.7 디도스 침해사고)
(2) 2011년 : 국가 사이버안보 마스터플랜 (3.4 디도스 침해사고)
(3) 2013년 : 국가 사이버안보 종합대책 (3.20 사이버테러)
(4) 2015년 : 국가 사이버안보태세 강화 종합대책
(5) 2019년 : 국가사이버안보전략

□ 정보보안을 위해 국내에서 지금까지 수립되었던 종합대책들은 ‘‘전략’이라기보다는 특정 사이버 공격에 대응하기 위한 ‘대책’ 위주였으며, 또한 정보보안에 대한 전체적 관점이 아닌 국가안보에 편향된 관점에서 세워지고 수행됨

□ 2019년 국내 최초로 국가사이버안보전략이 발표되었으나, 시민사회를 포함한 이해관계자들과의 사회적 논의없이 만들어졌으며 또한 구체적 이행과 개선방안은 포함하고 있지 않는 등 그 내용이 미비하며 개요 수준에 불과했음

□ 정보보안 전략은 인권, 개방성과 혁신, 이해관계자 간 협력과 신뢰 등 우리가 지향하는 정보사회의 가치와 운영원칙을 포함해, 그러한 가치와 원칙을 지키기 위한 제반 이슈들을 종합적으로 다룰 필요가 있음

- 인권 보장 : 정보 보안의 궁극적인 가치는 오프라인과 마찬가지로 온라인에서도 인간으로서의 기본권을 향유할 수 있는 것이며 모든 사이버 보안 정책은 표현의 자유, 프라이버시 등 기본권 보장의 가치에 기반해야 함
- 인터넷의 개방성과 혁신 : 정보 보안 정책은 인터넷의 자유 및 개방성과 조화를 이룰 필요가 있음, 예를 들어 국가가 특정한 기술을 강요하기 보다는 보다 나은 보안 기술의 발전을 위한 경쟁 환경을 조성할 필요가 있음
- 공공과 민간의 협력 : 대부분의 네트워크는 민간에 의해서 운영, 관리되고 있기에 세계 대부분의 국가들은 민간 주도 혹은 공공과 민간의 협력에 기반한 정책을 정보 보안 정책의 기조로 삼고 있고 그렇기에 경직된 규제보다는 책임성과 함께 자율성을 부여할 필요가 있음

- 민주적인 거버넌스 : 정보 보안 정책의 수립부터 집행에 이르기까지, 관련 이해관계자들 (정부, 기업, 기술자, 시민사회, 이용자 등)이 동등하고 자유롭게 참여할 수 있어야 함
- 국제협력과 신뢰: 인터넷은 세계적인 네트워크이기 때문에 국제적인 협력없이 정보 보안의 목적을 달성할 수 없고 다른 나라에 대한 선제적 공격을 통해 긴장을 유발해서는 안되며, 국가간 신뢰와 평화에 기반할 필요가 있음

<참고> 2013년 EU 사이버 보안 정책수립 원칙

① 유럽의 핵심적 가치는 디지털 세계에도 물리적 세계와 마찬가지로 적용되어야 함, ② 기본권, 표현의 자유, 개인정보 및 프라이버시의 보호, ③ 모두를 위한 접근, ④ 민주적이고 효율적인 멀티스테이크홀더 거버넌스, ⑤ 보안을 보장하기 위한 공유된 책임 – Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace

2) 정보보안 관련 법제의 비체계성

□ 국내 법령에서는 '사이버안전', '정보보호', '정보(통신)보안' 등 용어부터 시작하여, 각 법률마다 정보보호에 대한 개념 정의가 통일되어 있지 않고, 각기 다른 개념이 사용되기도 하며 중복적인 내용도 다수 존재

- 국가사이버안전관리규정은 '사이버안전'과 '사이버공격'을 규정하며 국가정보통신망을 그 대상 및 적용범위로 두고 있는데 이는 정보보안을 위협하는 다양한 종류의 위협(의도적인 공격 외 관리자의 실수, 시스템 오류, 천재지변 등)를 포괄하지 못함
- 국가사이버안보기본법은 '사이버 안보'을 규정하며 여기서 사이버 안보는 "사이버공격과 사이버공격으로 인한 사이버위기로부터 사이버공간을 보호함으로써 국가의 안전과 이익을 수호하는 활동"으로 정의하고 있는데, 이는 일반적인 정보보안보다 훨씬 좁은, 국가 안보와 관련된 활동으로 제한된 개념임.
- 정보통신기반보호법이나 정보통신망법과 같이 민간 영역의 정보보안을 규정하는 법은, 정보보호나 보안조치에 대한 규정을 포함하고 있음에도 불구하고, 정보보안에 대한 명확한 정의 규정을 두고 있지 않음
- 모호한 개념과 중복된 내용 및 대응 체계로 인해 실제 현장에서 침해사고에 대응하는 것에 있어 혼란을 야기하고 해당 업무를 담당하는 기관에게 불필요한 부담만 가중됨

□ 합의된 정보 보안 전략에 기반하여 관련 법령이 뚜렷한 개념 정의와 체계성 및 상호 일관성을 갖도록 정비되어야 함

3) 정보보안 관련 국가정보원의 과도한 역할

□ 2019국가정보보호백서에 따르면 ”국가정보원은 「국가정보원법」,「정보통신기반보호법」,「전자정부법」 등 관계법령에 근거하여 국가의 안전과 국익을 수호하기 위하여 해킹 등 전자적 수단으로 자행되는 안보위해 사이버공격 행위 및 그 공격 주체에 관한 정보를 수집·작성·배포하고, 국가의 기능 유지를 위하여 국가·공공기관을 대상으로 하는 사이버공격에 대한 예방·대응 업무를 수행하고 있다.” 고 설명

- 국가정보원법 제3조의 직무 규정 중 1항2호의 보안 업무와 5호 정보 및 보안 업무의 기획·조정업무가 정보보안과 관련된 관련된 직무일 것이나, 정보보안 정책의 총괄·조정의 역할은 이를 지나치게 확대한 것으로 보임.

- 특정 사이버 공격이 국가안보에 큰 영향을 미칠 수 있지만, 정보보안 정책 전반을 국가안보적 시각에서 바라보는 것은 협소한 접근일 뿐만 아니라, 국가안보의 특성상 정보보안 정책이 통제위주로 추진될 수 있고 기본권과 자율성을 제약할 가능성이 크기에 정보보안 정책 자체에 부정적인 영향을 미칠 수 있음.

- 보안업무규정에 따라 이루어지는 1항2호의 경우에도, 인터넷이 보편화되어 일반 개인 이용자의 통신 보안을 위해 암호 사용이 일반화된 점, 민간 암호개발 업체들이 공공기관 납품에 크게 의존하고 있어 공공 뿐만 아니라 민간영역에서 사용되는 암호기술의 개발 및 이용에 영향을 미칠 수 있는 점 등의 맥락을 고려할 때, 국가정보원이 과거의 관행대로 암호 업무를 담당하는 것은 국가안보를 넘어 민간의 통신 보안에도 관여하게 되는 것임.

□ 국가정보원은 지금까지 국내 정치에 개입하고 현재까지도 민간인 사찰 의혹이 존재하는 정보기관이며, 이로 인한 감시와 사찰 및 인권 침해의 우려가 제기됨

- 보안관제나 침해사고의 분석 등의 과정은 이용자가 발생시키는 모든 데이터의 수집이 가능하고 수집한 정보를 실시간으로 분석할 수 있어 프라이버시 침해 위협이 크며, 이러한 과정에서 기관이나 기업의 민감한 정보가 드러날 수도 있기에 개인정보 보호를 위한 원칙과 보안관제 수행기관에 대한 엄격한 감독이 필요함

- 정보통신망법에서 침해사고의 대응이나 원인 분석 과정에서 '제공받은 정보를 침해사고의 대응을 위하여 필요한 범위에서만 정당하게 사용'하도록 하고(제48조의2 5항), '제출 받은 자료와 조사를 통하여 알게 된 정보를 침해사고의 원인 분석 및 대책 마련 외의 목적으로는사용하지 못하며, 원인 분석이 끝난 후에는 즉시 파기'하도록(제48조의4 5항) 하고 있는 것도 이 때문임
- 또한, 정보통신기반보호법에서도 국정원이 '금융 정보통신기반시설 등개인정보가 저장된 모든 정보통신기반시설에 대하여 기술적 지원을 수행하여서는아니'하도록 규정(제7조 3항)하고 있으며, 제27조에서 비밀유지의무를 두고 있는 것도 이 때문임
- 2015년 국가정보원이 민간인 사찰을 위해 이탈리아 해킹팀의 RCS라는 해킹프로그램을 사용했다는 사실이 드러났으며, 이러한 행위는 정보기관이 국가안보를 명분으로 언제든 사이버 공간의 보안 전체를 약화시킬 수 있다는 것을 보여줌
- 또한 이러한 사건이 알려졌음에도 불구하고 국회의 사후검증마저 실패한 점 등 광범위한 인권침해가 없을 것이라는 보증할 수 있는 사법적, 입법적, 사회적 감독 체계가 부재하며, 권한 남용의 근본 원인으로 지적되는 수사권, 기획조정 권한 등이 현재까지도 남아있음
- 표현의 자유, 프라이버시 등 기본권의 보장, 인터넷의 개방과 혁신, 민주적 거버넌스 등 정보 보안의 핵심적 가치가 정보기관을 통해 달성될 수는 없음

4) 민주적인 정책결정과정 미흡

□ 네트워크의 운영이나 기술 개발은 주로 민간 영역에서 이루어지며 국제기구 및 세계 주요 국가 또한 사이버 보안 정책의 수립과 집행 과정에서 모두 민간 주도의 정보 보안, 이해관계자들의 협력을 강조

□ 정보 보안 관련 정보들은 투명하게 공개되고 공유되어 다양한 이해관계자가 의견을 표명할 수 있어야 함

Ⅲ. 정보보안 거버넌스 모델

□ 유럽, 미국, 중국, 일본 등 해외 주요 국가의 정보보안 거버넌스 사례는 이미 여러 논문을 통해 소개된 바 있음.[2] 각 국가의 역사적인 맥락이나 특수성에 따라 다양한 형태의 거버넌스가 나타나고 있음. 여기서는 정보보안 정책 및 거버넌스의 수립에 참조가 될만한 모델이나 모범사례의 제안을 검토해보고자 함.

1. 유럽연합, 국가사이버보안전략 모범사례 가이드

1) 정보보안 관련 법제의 통합

□ 유럽연합 네트워크 및 정보보안 기구(European Union Agency for Network and Information Security, ENISA)는 유럽연합 차원의 정보보안을 지원하는 전문 기구임. ENISA는 EU 회원국이 관련 법률을 이행하고 정보보안을 증진시킬 수 있도록 지원하고 있음.

□ ENISA는 2016년에 <국가사이버보안전략 모범사례 가이드>를 발간했는데, 이는 2012년에 처음 출간된 가이드를 업데이트한 것으로 EU 회원국이 자신의 국가사이버보안전략을 개발하고 업데이트하는 것을 지원하기 위한 것임.[3]

□ 한편, 유럽연합은 2016년에 네트워크정보보안 지침(NIS Directive)을 채택하였는데, 이 지침은 EU 회원국이 국가사이버보안전략을 채택하도록 요구하고 있으며, 국가사이버보안전략 채택 3개월 이내에 이를 집행위원회(EC)에 전달하도록 하고 있음.

2) 국가사이버보안전략(NCSS) 설계 및 개발을 위한 6단계 가이드

□ 이 가이드는 국가사이버보안전략을 설계하고 개발할 때 고려해야 할 단계를 다음과 같이 6단계로 제시하고 있음.

---

[2] 본 연구진도 <국가정보원과 국내 사이버보안 정책 개혁 방안> (오병일, 장여경, 이은우 공동연구, 정보인권연구소, 2016)에서 미국, 유럽연합, 영국, 일본 등의 사이버 보안 정책을 검토한 바 있음.

[3] ENISA, NCSS Good Practice Guide, 2016.

국가사이버보안전략(NCSS) 설계 및 개발을 위한 6단계 가이드

- 비전, 범위, 목표, 우선순위를 설정할 것
- 위험 평가 접근을 따를 것
- 기존 정책, 규제, 역량을 점검할 것
- 명확한 거버넌스 구조를 설정할 것
- 이해관계자를 파악하고 참여시킬 것
- 신뢰할 수 있는 정보공유 메커니즘을 구축할 것

□ 한국의 경우 정보보안 사고가 있을 때마다 종합대책을 내놓는 수준이었으며, 체계적인 정보보안(혹은 사이버보안) 전략이 수립되고 갱신되지 못했음. 2019년에 와서야 대한민국 정부 처음으로 <국가사이버안보전략>을 발표[4]한 바 있는데, 아직 매우 개략적인 수준이었음. 이런 점을 고려할 때 이 가이드는 국내 사이버보안 전략 수립에 좋은 참조가 될 것으로 보임. 특히, 올해에 처음 만들어진 <국가사이버안보전략> 조차 시민사회를 포함한 이해관계자들과의 사회적 논의없이 만들어졌다는 점에서 위 가이드의 '이해관계자를 파악하고 참여시킬 것' 단계를 유념할 필요가 있음.

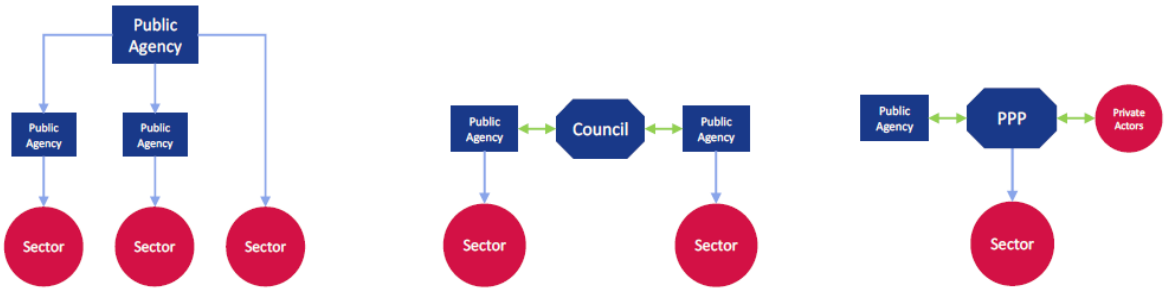
□ 위 가이드는 이와 함께 명확한 거버넌스 구조를 설정할 필요가 있음을 강조하고 있음. 즉, 모든 관련된 이해관계자의 역할, 임무, 책임을 잘 정의해두어야 함. 이때 특정 공공기관이나 부처간 워킹그룹 등이 전략의 코디네이터로 정의될 수 있는데, 각 국의 상황에 따라 서로 다른 거버넌스 구조가 가능하며 이 가이드가 특정한 거버넌스 구조를 권고하는 것은 아님. 그러나 어떠한 형태가 되든, 거버넌스 구조가 명확하게 정의되고 국가사이버보안전략에 반영될 필요가 있음.

□ 예를 들어, 중앙의 특정 기관이 영역을 불문하고 광범한 책임과 권한을 가지고 있는 중앙집중형 모델이 있을 수도 있고, 서로 다른 공공기관의 협업에 초점을 두는 분산형 모델도 있을 수 있음. 또한 민간 부문과도 서로 다른 관계를 맺을 수 있는데, 일부 국가에서는 민관협력(public-private

[4] 대한민국 정부 최초 「국가사이버안보전략」 발간 https://www.gov.kr/portal/puborgNews/1826771

partnership)과 같은 제도화된 공동규제 형태를 가지는 경우도 있다고 함.

<그림 5> 다양한 거버넌스 구조



□ 어떠한 거버넌스 형태가 되는 거버넌스 구조를 설정할 때 다음과 같은 점을 고려할 것을 권고하고 있음.

- 전략 관리와 평가의 궁극적 책임주체는 누구인지 규정. 통상적으로 사이버보안 코디네이터가 담당하게 됨.
- 자문기구와 같은 관리 구조의 정의.
- 이 자문기구의 임무와 업무의 규정.
- 사이버보안 정책의 수립 및 개발을 책임지는 단위의 임무와 업무 규정.
- 위협과 취약점 수집을 책임지는 단위의 임무와 업무 규정.
- 공공 및 민간영역의 국가사이버보안 및 긴급대응팀의 역할 분석 및 규정.

3) 국가사이버보안전략(NCSS) 이행을 위한 목표

□ 이 가이드는 국가사이버보안전략의 이행을 위한 15가지의 목표를 다음과 같이 제시하고 있는데, 이는 국가사이버보안전략이 포함해야 할 주요 요소를 규정하고 있음.

국가사이버보안전략(NCSS) 이행을 위한 목표 15가지
– 국가 사이버 긴급사태 대응계획의 수립 – 핵심적 정보인프라 보호 – 사이버 보안 훈련의 조직

- 기본적 보안 조치의 수립
- 사건 보고 메커니즘의 수립
- 이용자 인식 고양
- 훈련 및 교육 프로그램 강화
- 사건대응(incident response) 역량 수립
- 사이버 범죄 대응
- 국제 협력 참여
- 공공-민간 협력관계 구축
- 보안과 프라이버시의 조화
- 공공기관 간 협력
- 연구개발(R&D) 활성화
- 민간분야가 보안조치에 투자하도록 인센티브 제공

□ 국내 정보보안 관련 조치들을 <국가사이버보안전략(NCSS) 이행을 위한 목표 15가지>에 비추어보면, 국내 정보보안 정책들은 어느 정도 이러한 요소들을 포함하고 있는 것으로 보임.

NCSS 이행을 위한 목표	정보통신기반보호법	국가사이버안전관리규정
국가 사이버 긴급사태 대응계획의 수립	정보통신기반침해사고대책본부(제15조) 구성	사이버위기대책본부(제13조) 구성
핵심적 정보인프라 보호	정보통신기반보호법 자체	
사이버 보안 훈련의 조직		사이버위기대응훈련(제9조의2)
기본적 보안 조치의 수립	기반시설보호대책 수립 (제5조)	사이버안전대책 수립 (제9조)
사건 보고 메커니즘의 수립	침해사고 통지(제13조)	피해사실 통보(제12조)
이용자 인식 고양		교육 및 홍보(제16조)
훈련 및 교육 프로그램 강화		인력양성, 교육, 홍보(제16조)
사건대응(incident response) 역량 수립	복구조치(제14조), 정보공유분석센터(제16조)	국가사이버안전센터(제8조), 사고 복구(제12조)
사이버 범죄 대응	주요정보통신기반시설 침해행위 등의 금지	

	(제12조)	
국제 협력 참여	국제협력(제26조)	
공공-민간 협력관계 구축		
보안과 프라이버시의 조화	금융 정보통신기반시설 등 개인정보가 저장된 모든 정보통신기반시설에 대하여 국가정보원의 기술적 지원 수행 금지(제7조)	
공공기관 간 협력	정보통신기반보호위원회(제3조)	국가사이버안전전략회의(제6조), 전문기관간 협력(제14조)
연구개발(R&D) 활성화	기술개발 지원(제24조)	연구개발(제15조)
민간분야가 보안조치에 투자하도록 인센티브 제공	관리기관에 대해 기술의 이전, 장비의 제공 그 밖의 필요한 지원(제25조)	

□ 사이버 범죄에 대한 대응은 위 법률 뿐만 아니라 정보통신망법, 형법 등 다양한 법률에서 규정된 범죄에 대해 수사기관이 수행을 하고 있음.

□ 위 표에서 볼 수 있다시피 정보통신기반보호법 및 국가사이버안전관리규정에서 <국가사이버보안전략(NCSS) 이행을 위한 목표 15가지>를 일정하게 반영하고 있고, 정보통신망법에서도 일부 관련 규정이 포함되어 있음.

□ 다만, 이러한 내용들이 여러 정보보안 관련 법률에 분산되어 있다는 점, 국가정보원이 정보보안의 사실상 콘트롤타워를 담당함으로써 공공 및 민간의 협력 관계가 원활하지 않다는 점, 개인정보 및 프라이버시에 대한 고려가 불충분하다는 점 등이 문제이며, 위의 각 목표가 실제 얼마나 충실하게 이행되고 있는지는 별도의 평가가 필요함.

2. 정보보안 관할 당국의 성격과 거버넌스 구조

1) 정보보안 관할 당국의 성격

□ 유럽연합 각 국의 정보보안 거버넌스 현황을 파악할 수 있는 문서는 2016년에 ENISA가 발간한 <핵심정보기반시설의 보호에 대한 상황점검, 분석 및 권고> 보고서임.[5] 이 보고서는 유럽연합 회원국 17개 국가와 1개의 EFTA 국가의 서로 다른 거버넌스 구조를 조사한 결과를 싣고 있음.

□ 물론 이 보고서는 핵심정보기반시설(Critical Information Infrastructure)의 정보보안을 담당하는 관할 당국을 중심으로 조사를 한 것이기는 하지만, 핵심정보기반시설의 보호가 국가 정보보안 정책의 중요한 부분을 차지하고 있으며, 이 관할 당국이 정보보안과 관련한 다른 역할까지 맡는다는 것을 고려할 때 국가 정보보안을 담당하는 거버넌스 구조와 크게 다르지 않을 것으로 보임.

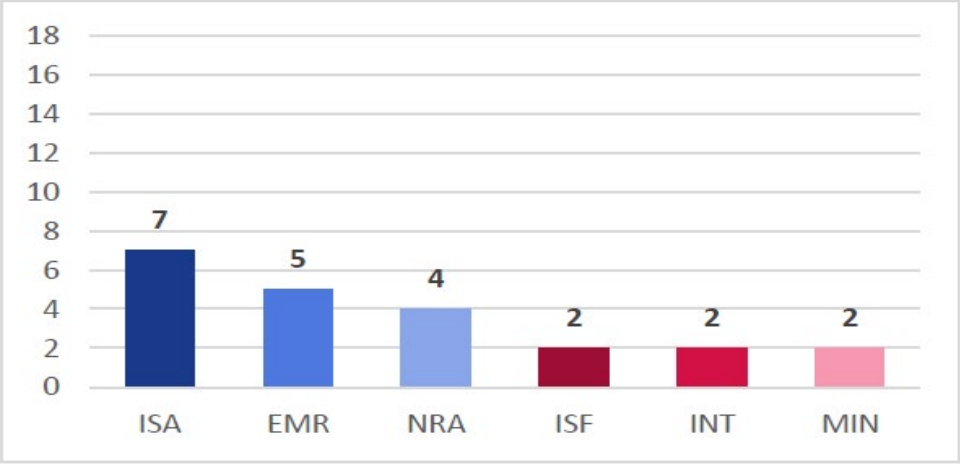
□ 보고서는 핵심 기반시설을 담당하는 관할 당국의 거의 대부분이 사고 보고의 접수, 대응 훈련의 조직, 사고 대응 등 실무적인 업무를 담당하고 있으며, 관할 당국의 ⅔ 정도는 전략문서의 개발, 국가 긴급대응팀(CSIRT)의 감독, 법안 제안 등 전략적, 정치적 수준의 추가적인 업무를 담당하고 있다고 함.

□ 핵심정보기반시설의 보호를 담당하는 관할 당국의 형태는 기본적으로 다양하지만, 주로 정보보안 당국이나 기반시설보호 기관, 통신규제기관에서 담당하고 있음.

- EMR: Emergency or CIP agency (응급 혹은 핵심기반시설보호 당국)
- INT: Intelligence or security service (정보 혹은 보안 기관)
- ISA: Information security agency (정보보안 당국)
- ISF: Information security forum (정보보안 포럼)
- NRA: National regulator or agency (국가통신규제기관)
- MIN: Ministry (정부부처)
- 국내 부처와 비교하자면 EMR은 행정안전부, INT는 국가정보원, ISA는 국가사이버안전센터(혹은 한국인터넷진흥원), NRA는 과학기술정보통신부 라고 볼 수 있음.

<그림 6> 유럽연합 각 국의 정보통신기반시설 관할 당국의 유형

[5] ENISA, Stocktaking, Analysis and Recommendations on the Protection of CIIs, 2016.1



□ ISA는 정보통신기반시설의 보안을 담당하는 전문기관을 의미함. 많은 경우 이 기관 내에 국가 혹은 정부의 긴급대응팀(CSIRT)이 있다고 하며, 이들은 통상 독립된 기관 혹은 독립성을 갖는 부처 산하의 기관이라고 함. EMR이 맡는 국가의 경우에는 핵심정보기반시설이 국가적인 핵심기반시설의 부분이기 때문이며, 통신규제기관인 NRA가 맡은 경우는 핵심정보통신기반시설이 정보통신 기술의 전문성을 강하게 요구하는 경향이 있고 민간 기관이 담당하는 경우가 많기 때문임. 그러나 정보기관이 담당하는 경우는 극소수에 불과함.

2) 정보보안 거버넌스의 구조

□ 이 보고서는 핵심정보기반시설 보안 거버넌스의 구조를 3가지 형태로 구분하고 있음. 이는 관련 기관간의 책임, 절차, 관계 등에 따른 구분인데, 물론 각 국의 거버넌스 구조가 반드시 이 세가지 형태 중 하나에 일치한다기 보다는 일종의 스펙트럼으로 봐야할 것임.

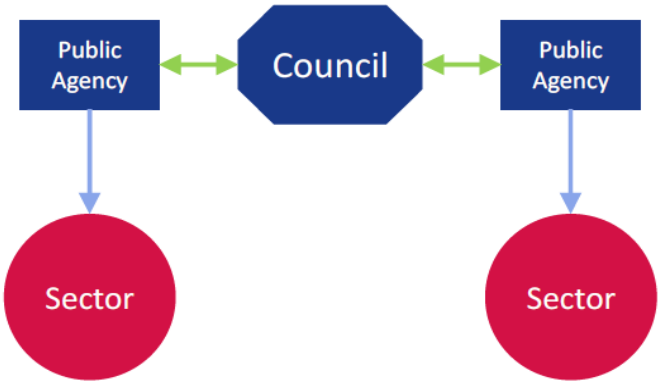
- 분산형 구조 (De-centralized approach)
- 중앙집중형 구조 (Centralized approach)
- 민간영역과의 공동규제 (co-regulation approach)

□ 분산형 구조의 특성

- 보완성의 원리(Principle of subsidiarity)
- 공공 기관 사이의 강한 협력
- 각 영역별 입법
- 기반 시설 보안을 각 부문 기관 혹은 업체에서 담당

- 협력 체계는 비공식적 네트워크, 혹은 조직화된 포럼이나 위원회 형태일 수 있음. 이러한 협력 체계는 정보공유 및 조정에 한정.
- 스웨덴(SAMFI), 아일랜드 등 대부분 유럽국가.

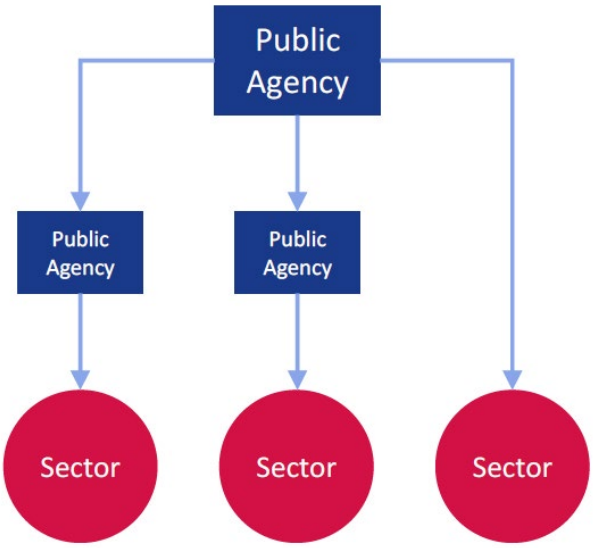
<그림 7> 분산형 구조



□ 중앙집중형 구조

- 영역을 가로지르는 중앙의 관할 기관 존재
- 통합적인 법제
- 중앙 기관이 비상 계획, 응급 관리, 규제업무 및 민간 운영자 지원. 많은 경우 국가적 CSIRT가 주요 권한당국의 일부임.
- 포괄적인 법제가 기반시설 운영자의 의무와 요구조건 규정.
- 프랑스 ANSSI : 기반시설 운영자에게 보안조치를 따를 것을 요구하고 감독. 보안사고시 통보받음. CERT-FR(위협탐지 및 긴급 대응 수행)이 ANSSI 산하.
- 체코, 독일.

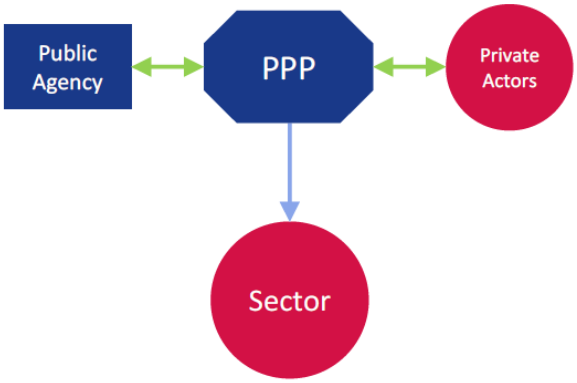
<그림 8> 중앙집중형 구조



□ 민간영역과의 공동규제

- 민간 부문과의 제도화된 협력
- 공공 및 민간 부문의 수평적 관계
- 전형적인 형태가 공공-민간 파트너쉽(PPP) : 통상 당사자간 계약 관계.
- 네덜란드 : 주요 권한기구가 NCSC인데 보안및테러대응국가코디네이터(NCTV) 산하이고 공공 및 민간 사이의 파트너쉽으로 구성됨. Dutch Cyber Security Council이 전략적, 정치적 수준의 조언 제공. Council은 여러 부처, 학계 및 업계 등으로 구성.

<그림 9> 공동규제형



3. ITU의 국가 사이버보안 전략 가이드

□ 국제통신연합 ITU는 2011년에 <ITU 국가 사이버보안 전략 가이드>를 발간한 바 있음.[6] 이후 2018년에 ITU의 주도로 다른 국제 기구, 업계, 시민사회 등의 단체들과 함께 <국가 사이버보안 전략 개발 가이드>를 새로 발간하였음.[7] 이 가이드는 국가 사이버 보안 전략의 개발 절차 뿐만 아니라, 전반적인 원칙, 주요 요소 및 모범 관행을 담고 있음.

1) 국가 사이버보안 전략의 원칙

□ 가이드는 국가 사이버보안 전략의 수립 및 이행 과정에서 적용될 수 있는 9개의 원칙을 제안하고 있음.

비전	전략은 정부 전체와 사회 전체를 아우르는 명확한 비젼을 설정해야 한다.
포괄적 접근과 상황에 맞는 우선순위	전략은 모든 디지털 환경에 대한 전반적인 이해와 분석으로부터 수립되어야 하지만, 각 국의 상황에 따라 조정되고 우선순위가 설정되어야 한다.
포용성	전략은 모든 관련 이해당사자의 활발한 참여 속에서 수립되어야 하며, 그들의 필요와 책임을 다뤄야 한다.
사회, 경제적 번영	전략은 경제적, 사회적 번영을 촉진해야 하며, 지속가능한 개발과 사회의 포용성을 위한 ICT의 활용을 극대화해야 한다.
기본적 인권	전략은 기본적 가치를 존중하고 그에 부합해야 한다.
위험 관리 및 회복력(resilience)	전략은 사이버보안 위험을 효과적으로 관리하고 경제 사회 활동의 회복력을 강화할 수 있어야 한다.
적절한 정책도구들	전략은 각 국의 특정한 환경을 고려하여, 각 목적 달성을 위해 가용한 가장 적절한 정책 수단을 활용해야 한다.
명확한 리더쉽, 역할,	전략은 정부 최고위급에서 설정됨으로써, 관련 역할과 책임의

[6] Frederick Wamala, THE ITU NATIONAL CYBERSECURITY STRATEGY GUIDE, 2011.9 http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

[7] ITU, GUIDE TO DEVELOPING A NATIONAL CYBERSECURITY STRATEGY - STRATEGIC ENGAGEMENT IN CYBERSECURITY, 2018. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

자원배분	지정과 충분한 인적, 재정적 자원의 분배를 책임질 수 있어야 한다.
신뢰할 수 있는 환경	전략은 시민과 기업들이 믿을 수 있는 디지털 환경을 구축할 수 있어야 한다.

□ 이러한 원칙에 비추어 보았을 때, 한국의 정보보안 정책은 2019년 이전에 제대로 된 전략이 부재했을 뿐 아니라, 거버넌스 구조, 역할과 책임도 명확하지 않았고, 이해관계자와의 협의도 부족했으며 그래서 보안 전략에 대한 신뢰를 형성하는데 한계가 있었음.

2) 국가 사이버보안 전략의 요소 및 모범사례

□ 또한 가이드는 국가 사이버보안 전략의 주요 분야별로 모범사례(Best Practice)를 소개하고 있는데, 이는 국가 사이버보안 전략의 기본 요소라고도 볼 수 있음.

거버넌스	– 최고위급의 지지 확보 – 사이버보안 관할 당국의 구축 – 정부간 협력 보장 – 분야간 협력 보장 – 전용 예산 및 자원의 배분 – 이행 계획의 수립
국가 사이버보안의 위험관리	– 위험 관리 접근법의 정의 – 사이버보안 위험 관리를 위한 공통 방법론 수립 – 분야별 사이버보안 위험 개요 개발 – 사이버보안 정책 수립
준비 및 회복력	– 사이버 사고 대응 역량 구축 – 사이버보안 위기 관리를 위한 긴급 계획 수립 – 정보공유 촉진 – 사이버보안 훈련 실시
중요 기반시설 및 핵심 서비스	– 핵심 기반시설 및 서비스를 보호하는 위험관리 접근법 수립 – 명확한 책임을 갖는 거버넌스 모델 채택 – 최소한의 사이버보안 기준의 정의 – 광범한 시장적 조치 활용 – 공공과 민간의 파트너쉽 수립
역량, 역량개발,	– 사이버보안 교재 개발

인식고양	– 기술 개발 및 인력 훈련 촉진 – 조직화된 사이버보안 인식고양 프로그램 이행 – 사이버보안 혁신 및 R&D 촉진
법제 및 규제	– 사이버범죄 법제 수립 – 개인의 권리와 자유 인식 및 보호 – 준수 메커니즘의 형성 – 법집행 역량강화 증진 – 조직간 절차 수립 – 사이버범죄에 대응하는 국제협력 지원
국제협력	– 우선적인 외교정책으로 사이버보안의 중요성 인식 – 국제적인 토론에 참여 – 사이버공간에서의 공식, 비공식 협력 증진 – 일관성있는 국내 및 국제 사이버보안 노력

Ⅳ. 국내 정보보안 거버넌스 개선 방향 및 법률안

1. 개선 방향

□ 지금까지 국내 정보보안 체계에 대한 평가에 기반하여, 대안 법률안은 다음과 같은 세 가지 개선 방향을 중심으로 설계되었음.

1) 정보보안 관련 법제의 통합

□ 정보통신망서비스 제공자의 정보보안을 규정하고 있는 정보통신망법, 주요 정보통신기반시설의 정보보안을 규정하고 있는 정보통신기반보호법, 국가정보통신망의 정보보안을 규정하고 있는 국가사이버안전관리규정 및 이의 법제화를 도모하고 있는 국가사이버안보법안 등 분산된 정보보안 관련 법제를 '통합'하여 정보보안을 위한 기본법을 제정하고자 함.[8]

□ 일관성있는 정보보안 정책 시행을 위해 다음과 같은 내용의 통합을 중점에 두었음.

- 각 법률에 존재하는 유사하지만 서로 다른 용어의 통일
- 내용상 유사한 조항의 통합
- 정보보안 거버넌스 체제의 통합

□ 기존 관행과의 일정한 연속성을 보장하고 법 개정 과정에서 이슈가 지나치게 많아지는 것을 방지하기 위해 서로 중복되지 않는 기존 법률의 조항은 통합 법안에서도 가급적 유지하는 방향으로 함. 향후 새로운 거버넌스 체제 내에서 기존 관행에 대한 전반적인 재검토가 필요함.

2) 대안적 정보보안 거버넌스 체제 구축

---

[8] 양천수 등도 현재 비체계적, 비정합적으로 난립하고 있는 정보통신 관련 법제도를 체계적으로 정립할 필요성을 제기하며, 이에 대한 방안으로 <통합정보보호법> 제정을 제안하고 있음. (양천수, 심우민, 전현욱, 김중길. <디지털 트랜스포메이션과 정보보호>. 박영사. 2019) 다만, 양천수 등은 정보통신망법, 정보통신기반보호법, 정보보호산업법의 통합을 고려하고 있는 반면, 국가사이버안전관리규정이나 국가사이버안보법안 등에 대해서는 검토하고 있지 않음. 이와 달리 우리는 정보통신망법, 정보통신기반보호법, 국가사이버안전관리규정(및 국가사이버안보법안)의 통합을 제안하는 것이며, 정보보안 자체가 아니라 보안산업 육성에 초점을 둔 정보보호산업법은 통합 대상으로 고려하지 않았음.

□ 현재 각 법에서 규정하고 있는 정보보안 거버넌스 기구를 통합하고, 민주적이면서도 효율적인 거버넌스를 구축하고자 함.

□ 정보보안과 관련된 정책 및 관리를 과학기술정보통신부가 총괄·조정하되, 주요 부처 및 민간의 이해관계자가 참여하는 국가정보보호위원회를 통해 부처간 및 민간과의 협력을 촉진하고자 함.

□ 민간 중심의 정보통신망 운영, 민간과의 협력이 중요한 정보보안 거버넌스의 특성, 정보보안의 기술중심적 특성 등을 고려할 때 과학기술정보통신부가 정보보안 거버넌스를 총괄 조정하는 컨트롤타워의 역할을 하는 것이 적절하다고 판단함.

3) 국가정보원의 정보보안 권한을 일반 정부부처로 이관

□ 정보보안은 정보기관으로서 국가정보원의 고유한 업무가 아니었음에도 불구하고 지금까지 정보보안과 관련한 다양한 역할을 담당해왔음. 국가정보원 개혁의 일환으로서 정보보안 관련 국가정보원의 권한을 다른 기관으로 이관할 필요가 있음. 국가정보원의 정보보안 업무의 법적 근거와 대안 법률안이 이를 어떻게 대체하는지, 그리고 개정이 필요한 타 법령은 무엇인지 구체적으로 살펴보면 다음과 같음.

- 국가사이버안전 정책·관리 총괄·조정
  - 국가사이버안전관리규정 → 동 법률안 제정을 통해 과학기술정보통신부로 이관됨.
- 공공부문 주요정보통신기반시설의 보호
  - 정보통신기반보호법 → 동 법률안 제정을 통해 과학기술정보통신부로 이관됨.
- 정보보안 관리실태 평가 : 국가 정보보안 정책의 이행실태를 확인하고 각급 기관의 보안관리 체계를 강화하기 위한 제도임.
  - 국가정보원법 제3조 제2항 → 정보기관이 보안 업무 전반을 총괄하는 것은 적절하지 않으므로 해당 권한을 다른 정부 부처로 이관하는 방향으로 국가정보원법 개정 필요.
  - 전자정부법 제56조 제3항 → 국가정보원의 권한을 과학기술정보통신부로 이관하는 방향으로 전자정부법 개정 필요. 동 법률안에서도 해당 업무가 과학기술정보통신부의 권한임을 명시하였음. (제24조)

- 국가사이버안전관리규정 제9조 제4항 → 동 법률안 제정에 다라 폐지 필요함.

- 국가정보보안기본지침[9] 제121조 → 국가 정보보안 기본지침은 현재 국가정보원이 작성, 배포하는 비공개 규정이지만, 국가정보원법 개정 및 동 법률안 제정에 따라 해당 업무의 관할 부처로 이관되어야 함.

● 보안적합성 검증

- 「전자정부법」 제56조 → 국가정보원의 권한을 과학기술정보통신부로 이관하는 방향으로 전자정부법 개정 필요. 동 법률안에서도 해당 업무가 과학기술정보통신부의 권한임을 명시하였음. (제24조)

● 암호모듈 검증

- 「전자정부법」 시행령 제69조[10] → 시행령 제69조는 법 56조에 따른 시행령 조항이므로, 「전자정부법」 제56조가 전술한 바와 같이 개정되며 그 취지에 맞게 개정되어야 함.

---

[9] 국가 정보보안 기본지침은 국가정보원이 작성, 배포, 관리하는 비공개(외부공개제한) 규정이다. 국가정보원법, 보안업무규정 및 보안업무기획, 조정규정, 국가사이버안전관리규정 및 전자정부법, 정보통신기반보호법, 공공기록물관리에 관한 법률 시행령 등에 따라, 국가 정보보안을 위하여 각급 기관이 수행하여야 할 기본활동을 규정한다. 중앙행정기관(대통령 소속기관 및 국무총리 소속 기관 포함), 그 소속기관, 지방자치단체와 그 소속기관 및 공공기관에 적용된다. 이 지침이 비공개로 관리되는 이유는 정보통신업무의 특성 상 해당 업무 내용이 정보통신망을 통하여 노출될 수 있기 때문이라고 하며, 이 때문에 지침의 수량과 배포대상을 제한하고 있다고 한다.
http://www.securitya.kr/eduwiz/bb/bbs/board.php?bo_table=c402&wr_id=5

[10] 제69조(전자문서의 보관 · 유통 관련 보안조치) ① 행정기관의 장은 정보통신망을 이용하여 전자문서를 보관·유통할 때에는 법 제56조제3항에 따라 국가정보원장이 안전성을 확인한 다음 각 호의 보안조치를 하여야 한다.
1. 국가정보원장이 개발하거나 안전성을 검증한 암호장치와 정보보호시스템의 도입·운용
2. 전자문서가 보관·유통되는 정보통신망에 대한 보안대책의 시행
② 행정기관의 장이 제1항의 보안조치를 이행하는 경우에는 미리 국가정보원장에게 보안성 검토를 요청하여야 한다.
③ 제1항 및 제2항에서 규정한 사항 외에 정보통신망을 이용한 전자문서의 보관·유통 관련 보안조치에 관하여 필요한 사항은 국가정보원장이 따로 지침으로 정할 수 있다.

- ‘암호모듈 시험 및 검증지침’ → 법 제57조 및 시행령 제69조 개정에 따라 관련 지침도 개정되어야 함.

● 보안관제 및 사이버공격 정보 수집

- 국가사이버안전관리규정 → 동 법률안 제정을 통해 과학기술정보통신부로 이관됨.

2. 대안 법률안 개요

1) 명칭 : 정보보호기본법

□ 정보보호, 정보보안, 사이버보안 등 여러 개념이 있으나, ‘보안’ 개념이 국내에서 정보기관이나 감시의 느낌을 불러오는 측면이 있고, 기존의 ‘정보보호산업의 진흥에 관한 법률’에서 ‘정보보호’라는 개념을 사용하고 있고 현행 ‘정보통신기반보호법’에서도 ‘보호’ 개념을 사용해온 바, ‘정보보호기본법’으로 하기로 함.[11]

□ 정보보호산업의 진흥에 관한 법률에서는 ‘정보보호’를 다음과 같이 규정하고 있음.

● "정보보호"란 다음 각 목의 활동을 위한 관리적·기술적·물리적 수단(이하 "정보보호시스템"이라 한다)을 마련하는 것을 말한다.

● 가. 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지 및 복구하는 것

● 나. 암호·인증·인식·감시 등의 보안기술을 활용하여 재난·재해·범죄 등에 대응하거나 관련 장비·시설을 안전하게 운영하는 것

□ 사이버안보는 사이버보안 혹은 정보보안(information security / cyber security)을 지나치게 국가안보(national security)적 관점에서 규정하고 있는데, 일부 보안 사고는 국가안보 위협으로 이어질 수 있으나 정보 및 네트워크 시스템의 보호에 있어 국가안보 위협만을 상정하는 것이 아니라 모든 수준의 위협을 고려해야 하고 위협의 수준에 따라 그에 상응하는 대응이 필요하다는 점에서 사이버안보 개념을 사용하는 것은 적절하지 않음.

---

[11] 그러나 '정보보호' 개념을 사용하는 것에 대해서도 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」의 ‘정보보호’와 중복되는 면이 있고, 개인정보 보호와 혼동이 될 수 있다는 점 등의 우려가 있음.

2) 법률안의 체계

□ 법제 통합 과정에서 서로 중복되지 않는 기존 법률의 조항은 통합 법안에서도 가급적 유지하는 방향으로 했기 때문에, 정보통신망서비스 제공자의 정보보안을 규정하고 있는 정보통신망법, 주요 정보통신기반시설의 정보보안을 규정하고 있는 정보통신기반보호법, 국가 정보통신망의 정보보안을 규정하고 있는 국가사이버안전관리규정 및 이의 법제화를 도모하고 있는 국가사이버안보법안 등의 주요 내용을 별도의 장으로 구성하되, 1장은 총칙, 2장은 통합적인 정보보호 추진체계(거버넌스)를 다루도록 하였음. 또한, 세 법안에서 서로 조금씩 다르지만 유사한 취지의 내용을 다루고 있는 '사고의 대응' 부분은 내용을 통합, 조정한 후에 별도의 장으로 구성하였음.

□ 이에 법률안은 다음과 같은 구성으로 되어 있음.

- 제1장 총칙
- 제2장 정보보호 추진체계
- 제3장 정보통신망에서의 정보보호
- 제4장 공공기관 정보보호
- 제5장 주요 정보통신기반시설의 보호
- 제6장 사고의 대응
- 제7장 보칙
- 제8장 벌칙

□ <제1장 총칙>은 법의 제정 목적, 정의규정, 기본원칙, 다른 법률과의 관계 등에 대한 조항을 포함하고 있음.

□ <제2장 정보보호 추진체계>는 통합된 정보보호 거버넌스를 다루고 있음. 정보보호 관련 정책 심의 및 조정을 위한 기구로서 국가정보보호위원회, 정보보호 콘트롤타워로서 과학기술정보통신부, 정보보호 기본계획의 수립, 실제 정보보호 업무를 담당할 국가정보보호센터 및 이를 지원하기 위한 한국정보보호진흥원 설립 규정 등을 포함하고 있음.

□ <제3장 정보통신망에서의 정보보호>는 정보통신망법 <제6장 정보통신망의 안정성 확보 등>의 정보보호와 직접적인 관련이 없는 일부 조항을 제외한 대부분의 내용을 가져옴.

□ <제4장 공공기관 정보보호>는 국가사이버안전관리규정 및 국가사이버안보법의 내용 중, 공공기관 자체의 정보보호 조치 및 이에 대한 점검과 관련한 조항을 가져옴.

□ <제5장 주요 정보통신기반시설의 보호>는 정보통신기반보호법의 내용 중, 거버넌스 및 사고 대응을 제외하고, 주요 정보통신기반시설의 지정, 보호대책 수립 및 이에 대한 점검 등과 관련한 조항을 가져옴.

□ <제6장 사고의 대응>은 정보통신망법, 국가사이버안전관리규정, 정보통신기반보호법에서 침해 사고 발생 시 신고, 사고에 대한 대응, 위협 정보의 공유 등과 관련한 조항을 가져와 통합, 정리하였음.

□ <제7장 보칙>은 기술개발, 인력양성 및 홍보, 국제협력 등의 조항을 포함하고 있으며, 제8장은 벌칙 규정임.

3) 개념 정의

□ 현재 정보보안 관련 법들은 유사한 내용에 대해 서로 다른 개념을 쓰고 있다. 예를 들어, 정보보안 사고와 관련하여 정보통신망법은 '침해사고', 정보통신기반보호법은 '전자적 침해행위'와 '침해사고' 개념을 정의하고 있으며, 국가사이버안전관리규정은 전자적 침해행위에 해당하는 개념인 '사이버공격', 정보보호에 해당하는 개념인 '사이버안전', 침해사고 등으로 인해 발생할 수 있는 상황을 '사이버위기'라는 개념으로 정의하고 있으나 정작 '침해사고'에 대응되는 개념은 없음. 국가사이버안보법은 마찬가지로 '사이버공격'이라는 개념과 함께 '국가안보를 위협하는 사이버공격'이라는 추가 개념을 정의하고 있음. 또한 '사이버안전' 개념 대신 '사이버안보'라는 개념을 사용하고 있음. 그러나 '국가안보를 위협하는 사이버공격'과 '사이버공격'의 경계는 모호하며 '국가안보를 위협하는 사이버공격'인지 여부를 공격 당시에 파악하기도 쉽지 않음. 또한, '사이버안보'는 '정보보호'에 비해 지나치게 협소한 규정인데, 법 조항의 내용을 고려할 때 일반적인 '정보보호'와 분리불가능함.

□ 또한 현행 법제들은 해커 등 외부의 공격, 이에 따른 침해 사고만을 전제로 하고 있음. 그러나 실제로 보안 사고는 외부의 의도적인 공격 뿐만 아니라, 천재지변이나 관리상의 문제 등에 의해서도 발생할 수 있음. 보안의 목적은 궁극적으로 정보 및 네트워크의 기밀성・무결성・가용성을 유지하는 것이며, 이를 위협하는 모든 상황에 대비할 필요가 있음.

□ 그래서 대안 법률안에서는 '전자적 침해행위' 혹은 '사이버공격'이라는 개념 대신 보안을 위협하는 잠재적인 모든 것을 '위험'으로, 그리고 위험이 실제

발생한 것을 '사고'로 정의하였음.[12] 기존의 전자적 침해행위 및 사이버공격 역시 '위험' 개념에 포함이 됨.

4) 기본 원칙

□ 법률안 제3조에서 기본원칙을 규정하고 있음. 이는 정보보안이 기본권 침해를 정당화하는 명분으로 사용되어서는 안된다는 것, 정보보안을 이유로 인터넷의 기술 표준이나 개방성을 위협해서는 안된다는 것, 정보보안에 있어서 민간의 역할이 크기 때문에 정책의 수립과 집행 과정에서 이해관계자들과 소통 및 협력해야 한다는 것, 인터넷의 세계적인 특성을 고려할 때 정보보안에 있어서도 국제협력이 중요하다는 것을 강조하고 있음.

5) 정보보호 추진체계

□ 과학기술정보통신부가 국가적인 정보보호 거버넌스를 총괄 조정하는 컨트롤타워의 역할을 맡게됨. (제6조 1항) 민간 중심의 정보통신망 운영, 민간과의 협력이 중요한 정보보안 거버넌스의 특성, 정보보안의 기술중심적 특성 등을 고려할 때 과학기술정보통신부가 컨트롤타워의 역할을 담당하는 것이 적절하다고 판단하였음.[13]

□ 그러나 정보보안(보호) 업무는 서로 다른 부처가 주무를 맡고 있는 여러 업무들과 연결되어 있음. 예를 들어, 행정안전부는 전자정부의 총괄책임을, 경찰청은 사이버범죄 수사를, 외교부는 국제협력을, 국방부는 사이버국방에

---

[12] 참고로 유럽연합의 '정보 및 네트워크 보안 지침(Network and Information Security directive, EU 2016/1148) 역시 사고(incident), 사고 대응(incident handling), 위험(risk)에 대한 정의규정을 다음과 같이 두고 있음.

(7) 'incident' means any event having an actual adverse effect on the security of network and information systems;
'사고'는 네트워크 및 정보 시스템의 보안에 실질적으로 부정적인 영향을 미치는 사건을 의미한다.
(8) 'incident handling' means all procedures supporting the detection, analysis and containment of an incident and the response thereto;
'사고 대응'은 사고의 탐지, 분석, 억제 및 대응을 지원하는 모든 절차를 의미한다.
(9) 'risk' means any reasonably identifiable circumstance or event having a potential adverse effect on the security of network and information systems;
'위험'은 네트워크 및 정보 시스템의 보안에 잠재적으로 부정적인 영향을 미칠 수 있는 합리적으로 식별 가능한 환경 혹은 사건을 의미한다.

[13] 2014년 변재일 의원은 "미래창조과학부와 국가정보원으로 이원화되어 있는 대응체계를 미래창조과학부로 일원화"하는 내용의 정보통신기반보호법 개정안을 발의한 바 있으나 임기만료로 폐기된 바 있음.

대한 책임을 맡고 있음. 따라서 국가정보보호위원회를 통해 부처간 협력 및 조정을 도모하도록 하였음. 또한 국가정보보호위원회는 정보보안 관련 정책, 제도, 기본계획 등의 심의를 담당함으로써 과학기술정보통신부가 다른 부처의 의견을 수렴하여 관련 정책과 계획을 수립하도록 하였음.

□ 정보보호 정책과 운영이 개인정보 자기결정권을 비롯한 인권에 기반할 수 있도록 하기 위해, 국가인권위원회 및 개인정보보호위원회가 국가정보보호위원회에 반드시 참여하도록 규정하였음. 또한, 민간 이해관계자와의 소통과 협력을 강화하기 위해 정보보호에 전문적이면서도 관련 이해관계자를 대표할 수 있는 사람이 국가정보보호위원회 위원으로 참여할 수 있도록 열어둠.

□ 국가정보보호위원회의 사무국은 과학기술정보통신부 산하의 국가정보보호센터에서 담당하도록 함.[14] 현재 국가사이버안전관리규정에 따른 국가정보원 산하 국가사이버안전센터의 역할을 이전하게 되며, 과학기술정보통신부 내에서 정보보호 관련 업무를 실질적으로 담당함. (제7조)

□ 또한 정보보호 관련 업무를 실무적으로 지원할 수 있는 공공기관으로 한국정보보호진흥원 설립 규정을 둠.(제8조) 현재 정보통신망법의 규정에 따라 설립된 한국인터넷진흥원의 업무 중에 정보보호 관련 업무를 수행하게 됨.[15]

□ 한국정보보호진흥원 등 각 분야에서 기술적 역량을 가지고 있는 기관들을 지원기관으로 규정하여 필요할 경우 기술적 지원을 할 수 있도록 함. (제9조)

---

[14] 국내에서도 종종 '사이버보안청' 설립의 필요성이 제안된 바 있음. 예를 들어, 2014년 국정감사에서 김재경 의원은 '국가사이버안보 전담기구' 사이버보안청 설립의 필요성을 제기하면서, "우리나라 국가사이버안보의 총괄 책임은 국가정보원에 있음. 그러나 국가 최고 정보기관으로서 업무 특성상 폐쇄성, 기밀성, 비공개성 원칙에 따라 움직이기에 국제적 대응과 국내 민·관·학·연·산 등의 사이버보안 (외교, 기술, 정책, 서비스, 교육 등) 관련 기관들에 대한 통합적 리더쉽은 매우 제한적일 수 밖에 없음"이라고 지적한 바 있음. 명칭은 다르지만, 국가정보보호센터는 사이버보안청과 같이 정보보안을 전담하는 정부기관이라고 볼 수 있음.

[15] 법률안에서 구체적으로 다루지는 않았으나, 개인정보보호, 주소자원 관리 등 한국인터넷진흥원이 맡고 있는 서로 다른 여러 업무의 조정 및 이를 위한 조직의 재구성이 필요함. 예를 들어, 정보보안 업무는 본 법률안에 따라 설립된 한국정보보호진흥원으로, 개인정보보호 업무는 개인정보보호법 개정을 통해 (가칭)개인정보보호원으로, 주소자원 관리 업무는 인터넷주소자원법 개정을 통해 한국인터넷정보센터로 각각 분리, 이관될 수 있을 것임.

6) 정보통신망에서의 정보보호

□ 정보통신망법 <제6장 정보통신망의 안정성 확보 등>의 조항 중 정보보호 관련 조항의 내용을 <제6장 사고의 대응>에 배치된 조항을 제외하고는, 대부분 별다른 수정없이 가져옴.

정보통신망법	대안 법률안
제45조(정보통신망의 안정성 확보 등)	제10조(정보통신망의 안정성 확보 등)
제45조의2(정보보호 사전점검)	제11조(정보보호 사전점검)
제45조의3(정보보호 최고책임자의 지정 등)	제12조(정보보호 최고책임자의 지정 등)
제46조(집적된 정보통신시설의 보호)	제13조(집적된 정보통신시설의 보호)
제46조의2(집적정보통신시설 사업자의 긴급대응)	제14조(집적정보통신시설 사업자의 긴급대응)
제47조(정보보호 관리체계의 인증)	
제47조의2(정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관의 지정취소 등)	제15조(정보보호 관리체계의 인증) 제16조(정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관의 지정취소 등)
제47조의3(개인정보보호 관리체계의 인증)	정보통신망법에 존치
제47조의4(이용자의 정보보호)	제17조(이용자의 정보보호)
제47조의5(정보보호 관리등급 부여)	제18조(정보보호 관리등급 부여)
제48조(정보통신망 침해행위 등의 금지)	제41조(정보통신망 침해행위 등의 금지)
제48조의2(침해사고의 대응 등)	제39조(사고통계 및 분석)
제48조의3(침해사고의 신고 등)	제35조(사고의 신고 및 통보)
제48조의4(침해사고의 원인 분석 등)	제36조(사고의 조사 및 복구)
제49조(비밀 등의 보호)	제20조(비밀 등의 보호)
제49조의2(속이는 행위에 의한 개인정보의 수집금지 등)	정보통신망법에 존치
제50조(영리목적의 광고성 정보 전송 제한)	
제50조의3(영리목적의 광고성 정보 전송의 위탁 등)	정보통신망법에 존치
제50조의4(정보 전송 역무 제공 등의 제한)	정보통신망법에 존치
제50조의5(영리목적의 광고성 프로그램 등의 설치)	정보통신망법에 존치 정보통신망법에 존치
제50조의6(영리목적의 광고성 정보 전송차단 소프트웨어의 보급 등)	정보통신망법에 존치
제50조의7(영리목적의 광고성 정보 게시의 제한)	정보통신망법에 존치
제50조의8(불법행위를 위한 광고성 정보 전송금지)	정보통신망법에 존치
제51조(중요 정보의 국외유출 제한 등)	
제52조(한국인터넷진흥원)	제19조(중요 정보의 국외유출 제한 등)

	제8조(한국정보보호진흥원)

7) 공공기관 정보보호

□ 국가사이버안보법안과 같이 정부 및 지방자치단체, 공공기관 등을 책임기관으로 두고 각 기관이 자신의 정보통신망에서의 정보보호 책임을 두도록 함.[16]

□ 그러나 국가사이버안보법안과 달리 민간기관은 책임기관에서 제외하였으며, 책임기관에 대한 지원 및 (정보보호와 관련된) 감독의 역할을 국가정보원이 아니라 과학기술정보통신부가 수행하도록 하였음. 이에 따라 각 기관의 정보보안 관리체계의 평가도 국가정보원이 아니라 과학기술정보통신부(실무적으로는 국가정보보호센터)에서 수행하기 됨.

8) 주요 정보통신기반시설의 보호

□ 정보통신기반보호법에 따른 정보통신기반보호위원회의 역할은 법률안에서는 국가정보보호위원회가 수행하게 됨. 국가정보원과 과학기술정보통신부가 각각 공공 및 민간 부문을 맡고 있던 실무위원회는 없어지고 과학기술정보통신부가 정보보호의 컨트롤타워로서 현재 국가정보원이 맡고 있던 역할까지 하게되며, 사무국의 역할은 국가정보보호센터에서 맡게됨.

□ 그러나 그 외에 정보통신기반보호법에 따른 규제 방식은 일단 동 법률안에 거의 그대로 반영되었음. 이는 정보보안 관련 법제의 통합에 대한 혼란을 최소화하기 위한 것임. 즉, 현재와 마찬가지로 중앙행정기관의 장이 소관분야에서 주요정보통신기반시설을 지정하고, 주요정보통신기반시설을 관리하는 '관리기관'은 취약점 분석·평가의 결과에 따라 주요정보통신기반시설 보호대책을 수립·시행하고 이를 관계중앙행정기관에 제출하며, 관계중앙행정기관의 장은 보호대책을 종합·조정하여 소관분야의 보호계획을 수립·시행하고 보호지침을 제정하는 역할을 계속 하게 됨.

□ 다만, 주요정보통신기반시설의 지정을 권고하고 관리기관의 보호대책 이행 여부를 확인하며 관리기관에 기술적 지원을 하는 등 국가정보원이 단독으로

---

[16] 본 법안 초안에 대한 의견 수렴 과정에서, '책임기관'과 '중앙행정기관'의 차이가 무엇인지 애매하기 때문에 책임기관이라는 표현을 굳이 활용할 필요성이 있는지에 대한 의문이 제기되었으나, 제21조 1항에서 규정하고 있는 바와 같이 책임기관은 중앙행정기관 외에도 '국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관 및 그 소속 기관', 지방자치단체 등을 모두 포함하는 개념이기 때문에, 본 법에서는 경우에 따라 중앙행정기관, 책임기관 개념을 각각 사용함.

혹은 과학기술정보통신부와 함께 수행하던 역할은 과학기술정보통신부가 맡게 됨.[17]

□ 다른 법률과 중복적인 내용을 다루고 있는 침해 사고의 대응과 관련한 조항은 통합되어 동 법률안의 <제6장 사고의 대응>에 반영됨. 정보통신기반보호법의 조항들 중 <제5장 주요 정보통신기반시설의 보호>으로 반영된 것들은 아래와 같음.

정보통신기반보호법	대안 법률안
제5조(주요정보통신기반시설보호대책의 수립 등) 제5조의2(주요정보통신기반시설보호대책 이행 여부의 확인) 제6조(주요정보통신기반시설보호계획의 수립 등) 제7조(주요정보통신기반시설의 보호지원) 제8조(주요정보통신기반시설의 지정 등) 제8조의2(주요정보통신기반시설의 지정 권고) 제9조(취약점의 분석·평가) 제10조(보호지침) 제11조(보호조치 명령 등) 제25조(관리기관에 대한 지원)	제25조(주요정보통신기반시설보호대책의 수립 등) 제26조(주요정보통신기반시설보호대책 이행 여부의 확인) 제27조(주요정보통신기반시설보호계획의 수립 등) 제28조(주요정보통신기반시설의 보호지원) 제29조(주요정보통신기반시설의 지정 등) 제30조(주요정보통신기반시설의 지정 권고) 제31조(취약점의 분석·평가) 제32조(보호지침) 제33조(보호조치 명령 등) 제34조(관리기관에 대한 지원)

9) 사고의 대응

□ 정보보호 정책수립 및 점검 등 예방과 관련한 규정은 기관의 성격에 따라 3장~5장에서 규정됨. 제6장에서는 실제 사고가 발생했을 경우의 대응을 다루고 있음. 사고가 발생하면 신고(제35조)를 해야 하고 조사 및 복구 등 대응(제36조)이 이루어져야 하며, 피해가 심각할 경우 대책본부를

[17] 본 법안 초안에 대한 의견 수렴 과정에서, 주요정보통신기반시설 지정절차의 통제 가능성을 확보할 필요성에 대한 문제가 제기되었음. 즉 특정 시설을 불필요하게 주요정보통신기반시설로 지정함으로써 사실상 민간 사찰이 이루어질 수 있는 등의 역기능에 대한 대비책이 필요하다는 것임. 이는 현행 법률인 정보통신기반보호법에 대한 문제제기이기도 함. 그런데 법안에서는 기반시설 지정권고 등 국정원의 권한을 폐지하였기 때문에 민간 사찰의 위험성이 축소되었고, 너무 많은 이슈를 만드는 것은 법안 논의를 어렵게 하기 때문에 이 법안에서 초점을 두는 몇 가지 이슈에 집중하는게 좋겠다는 정책적 판단에 따라 본 법안에서는 이 이슈를 다루지 않았음.

구성(제37조)하여 대응해야 함. 위험의 확산을 방지하기 위해 위험정보는 공유되어야(제38조) 하고, 사고와 관련한 통계가 수집되고 분석(제39조)되어 향후 정책에 반영되어야 함. 위험 수준에 따라 국가차원의 체계적인 대응을 위해 위험경보를 발령할 수 있음. (제40조)

□ 사고의 신고/통보

- 정보통신망법 제48조의3(침해사고의 신고 등), 정보통신기반보호법 제13조(침해사고의 통지), 국가사이버안전관리규정 제12조(사고통보 및 복구), 국가사이버안보법안 제15조(사이버공격으로 인한 사고의 통보 및 조사) 등 각 법안은 사고 발생시 정보통신서비스 제공자, 관리기관, 책임기관 등으로 하여금 관할 당국에 신고 혹은 통보하도록 하고 있음. 가급적 각 법의 규정을 존중하는 방향으로 통합하였으며, 과학기술정보통신부가 국가차원의 일원화된 체계를 구축하도록 함.

□ 사고의 조사 및 복구

- 정보통신망법 제48조의4(침해사고의 원인분석), 정보통신기반보호법 제14조(복구조치), 국가사이버안전관리규정 제13조(사고조사 및 처리), 국가사이버안보법안 제15조(사이버공격으로 인한 사고의 통보 및 조사)의 (대책기구와 관련된 내용을 제외한) 일부 내용들을 각 법의 규정을 존중하는 방향으로 통합함.

□ 대책본부의 구성 및 운영

- 정보통신기반보호법, 국가사이버안전관리규정, 국가사이버안보법안의 대책본부와 관련된 내용을 다음과 같이 통합함.

대안 법률안	정보통신기반보호법	국가사이버안전관리규정	국가사이버안보법안
사고대책본부	정보통신기반침해사고대책본부	범정부적 사이버위기대책본부	사이버위기대책본부
상급책임기관의 장/과학기술정보통신부장관	위원회의 위원장	국가정보원장	상급책임기관의 장/국가정보원장
1. 대통령령으로 정하는 단계 이상의 경보 또는 분야별 경보가 발령된 경우	주요정보통신기반시설에 대하여 침해사고가	사이버공격으로 인하여 그 피해가 심각하다고 판단되는 경우나	1. 대통령령으로 정하는 단계 이상의 경보 또는 분야별 경보가 발령된 경우

2. 사고 발생으로 인한 피해가 심각하다고 판단하는 경우	광범위하게 발생한 경우	주의 수준 이상의 경보가 발령된 경우	2. 사이버공격으로 인하여 그 피해가 심각하다고 판단하는 경우
사고에 대한 원인 분석, 사고 조사, 긴급 대응, 피해 복구 등의 신속한 조치를 하기 위하여	필요한 응급대책, 기술지원 및 피해복구 등을 수행하기 위한 기간을 정하여	사이버공격에 대한 원인분석, 사고조사, 긴급대응 및 피해복구 등의 조치를 취하기 위하여	사이버공격에 대한 원인 분석, 사고 조사, 긴급 대응, 피해 복구 등의 신속한 조치를 하기 위하여
대책본부의 장 임명 인력 파견 또는 장비 제공 등 협력과 지원 요청	공무원 파견요청 대책본부장 임명 협력 및 지원 요청	하부기구 구성 권한 인력, 장비, 자료 지원 요청	대책본부의 장 임명 인력, 장비 요청

□ 위험정보의 공유

- 정보통신기반보호법 제16조(정보공유・분석센터), 국가사이버안보법안 제12조(사이버위협정보의 공유)의 내용을 통합함. 정보통신기반보호법 상의 각 분야별 정보공유분석센터는 유지하되, 국가적 위험정보의 공유를 위해 국가정보보호센터 내에 <위험정보공유센터>를 두도록 함.

- 위험정보 공유시에 개인정보와 관련된 논란이 있을 수 있는데, 가능하면 익명처리, 불가피할 경우 가명처리하여 공유하도록 하고, 안전조치와 관련하여 개인정보보호위원회와 협의하도록 함.

□ 사고통계 및 분석

- 정보통신망법 제48조의2(침해사고의 대응 등)에서 규정하고 있는 통계수집 및 분석 활동을 민간의 주요정보통신서비스제공자 등 뿐만 아니라 관리기관 및 책임기관으로 확대하였음.

□ 위험경보의 발령 및 조치

- 정보통신망법 제48조의2(침해사고의 대응 등), 국가사이버안전관리규정 제11조(경보발령), 국가사이버안보법안 제16조(사이버위기경보의 발령 및 조치)을 통합함. 분야별 경보는 중앙행정기관의 장이, 국가차원의 경보는 과학기술정보통신부장관이 발령함.

10) 보칙

□ 정보통신망 침해행위 금지, 기술개발 및 연구, 인력양성 및 교육, 국제협력, 비밀엄수의무 등을 규정함.

정보보호기본법 (안)

제1장 총칙

제1조(목적) 이 법은 정보보호에 대한 위험의 예방 및 탐지, 사고에 대한 신속한 대응 등 체계적인 정보보호를 위한 정책 수립, 조직 체계, 기관간의 협력 등 필요한 조치를 규정함으로써 정보 및 정보통신망의 안정적인 운용을 보장하는 것을 목적으로 한다.

제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

1. "정보보호"란 정보 및 정보통신망의 기밀성・무결성・가용성을 유지하기 위해, 다음 각 목의 활동을 위한 관리적・기술적・물리적 수단을 마련하는 것을 말한다.

   가. 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 발생할 수 있는 정보의 훼손, 변조, 유출 등을 방지 및 복구하는 것

   나. 암호・인증・인식・감시 등의 보안기술을 활용하여 재난・재해・범죄 등에 대응하거나 관련 장비・시설을 안전하게 운영하는 것

2. "정보통신망"이라 함은 「전기통신기본법」 제2조제2호의 규정에 의한 전기통신설비를 활용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말한다.

3. "정보통신기반시설"이라 함은 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 정보통신망을 말한다.

4. "위험"이란 다음 각 목을 포함하여 전자적 제어·관리시스템 혹은 정보통신망의 정보보호에 잠재적으로 부정적인 영향을 미칠 수 있는 환경이나 사건을 말한다.

   가. 재난・재해의 발생

나. 해킹, 컴퓨터 바이러스, 서비스 거부 등 전자적 방법으로 전자적 제어·관리시스템 및 정보통신망을 불법침입・교란・마비・파괴하거나 정보를 빼내거나 훼손하는 등의 공격 행위

5. "사고"란 위험이 실제로 발생하여 전자적 제어·관리시스템 혹은 정보통신망의 정보보호에 실질적으로 부정적인 영향을 미치는 사건을 말한다.

제3조(기본원칙) 국가는 정보보호 정책의 수립과 시행 과정에서 다음의 원칙을 준수하여야 한다.

① 표현의 자유, 개인정보 자기결정권 등 기본권을 보장한다.

② 정보의 자유로운 유통과 인터넷의 개방성 및 표준을 존중한다.

③ 관련 업계, 시민사회, 학계, 이용자 등 이해관계자의 참여를 보장한다.

④ 외국 및 국제기구·단체와의 적극적인 협력관계를 구축한다.

제4조(다른 법률과의 관계) 정보보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법을 우선하여 적용한다.

제2장 정보보호 추진체계

제5조(국가정보보호위원회) ① 정보보호에 관한 다음 각 호의 사항을 심의하기 위하여 대통령 소속으로 국가정보보호위원회(이하 “위원회”라 한다)를 둔다.

1. 정보보호에 관한 국가의 정책 및 전략 수립
2. 정보보호에 관련된 제도 및 법령의 개선에 관한 사항
3. 정보보호에 관한 정책 및 기관간 역할조정에 관한 사항
4. 제6조에 따른 정보보호 기본계획 등 중요 중장기 대책
5. 제9조에 따른 지원기관의 지정 및 지정 취소에 관한 사항
6. 제28조에 따른 주요정보통신기반시설에 관한 보호계획의 종합・조정 및 추진 실적에 관한 사항
7. 제30조에 따른 주요정보통신기반시설의 지정 및 지정 취소에 관한 사항

8. 제31조에 따른 주요정보통신기반시설의 지정 여부에 관한 사항.

9. 그 밖에 정보보호에 관한 중요한 사항으로서 위원회의 위원장이 필요하다고 인정하는 사항

② 위원회는 위원장을 포함하여 25명 이내의 위원으로 구성한다.

③ 위원회의 위원장은 과학기술정보통신부장관이 되고, 위원은 다음 각 호의 사람중에서 위원장이 위촉하는 자로 하되, 국가인권위원회 및 개인정보보호위원회의 차관급 공무원을 포함한다.

1. 국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관과 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다. 이하 같다)의 차관급 공무원 중에서 대통령령으로 정하는 사람.

2. 관련 업계, 시민사회, 학계, 이용자 등 이해관계자를 대표할 수 있는 사람으로서 정보보호에 관하여 전문적인 지식과 경험을 갖춘 사람

④ 위원회는 직무수행을 위하여 필요할 때에는 제21조제1항에 따른 책임기관(같은 항 제1호의 책임기관은 제외한다)과 제9조제1항에 따른 지원기관에 대하여 필요한 자료의 제출을 요청할 수 있다. 이 경우 요청을 받은 기관의 장은 특별한 사정이 없으면 요청에 따라야 한다.

⑤ 제7조에 따른 국가정보보호센터가 위원회의 사무를 지원한다.

⑥ 위원회의 구성·운영 등에 필요한 사항은 대통령령으로 정한다.

제6조(정보보호기본계획의 수립) ① 정보보호와 관련된 정책 및 관리에 대하여는 과학기술정보통신부장관이 관계 중앙행정기관의 장과 협의하여 이를 총괄·조정한다.

② 과학기술정보통신부장관은 정보보호 업무를 효율적이고 체계적으로 추진하기 위하여 3년마다 다음 각 호의 사항이 포함된 정보보호기본계획(이하 “기본계획”이라 한다)을 위원회의 심의를 거쳐 수립·시행하여야 한다.

1. 정보보호의 정책 목표와 추진방향

2. 정보보호와 관련된 제도 및 법령의 개선

3. 위험의 예방 및 사고 대응

4. 정보보호 관련 정책·기술의 연구·개발

5. 정보보호 관련 교육 및 훈련

6. 정보보호 관련 민간 이해관계자와의 협력

7. 정보보호 관련 국제협력

8. 그 밖에 대통령령으로 정하는 정보보호를 위하여 필요한 사항

③ 제21조2항에 따른 상급책임기관의 장은 기본계획에 따라 정보보호 시행계획(이하 “시행계획”이라 한다)을 매년 작성하여 관할 책임기관의 장에게 통보하여야 한다.

④ 기본계획과 시행계획의 작성 방법・절차 및 세부 내용 등에 관하여 필요한 사항은 대통령령으로 정한다.

제7조(국가정보보호센터) ① 정보보호와 관련된 국가차원의 종합적이고 체계적인 대응을 위하여 과학기술정보통신부 장관 소속 하에 국가정보보호센터(이하 “정보보호센터”라 한다)를 둔다.

② 정보보호센터는 다음 각 호의 업무를 수행한다.

1. 국가정보보호위원회 운영 지원

2. 정보보호에 관한 국가의 정책 및 전략 수립 지원

3. 제6조에 따른 정보보호 기본계획의 수립 지원

4. 제10조에 따른 정보보호지침의 작성 및 배포

5. 제23조에 따른 정보보호 실태 평가

6. 제27조에 따른 주요정보통신기반시설보호대책 이행 여부의 확인

7. 제28조에 따른 주요정보통신기반시설보호대책 및 주요정보통신기반시설보호계획의 수립지침 수립 및 통보

8. 위험 및 사고 관련 정보의 수집·분석·전파

9. 사고의 처리·원인분석 및 대응체계 운영

10. 정보보호 관련 법·제도 및 정책의 조사·연구

11. 정보보호 관련 기술 개발 및 표준화

12. 정보보호산업 정책지원 및 인력양성

13. 정보보호 관련 국제적인 정보공유 및 협력

14. 그 밖에 이 법 또는 다른 법령에 따라 국가정보보호센터의 업무로 정하거나 과학기술정보통신부로부터 위탁받은 사업

③ 과학기술정보통신부 장관은 국가 차원의 정보보호 위협에 대한 종합판단, 상황관제, 위협요인 분석 및 합동조사 등을 위해 정보보호센터에 민·관·군 합동대응반(이하 "합동대응반"이라 한다)을 설치·운영할 수 있다.

④ 정보보호센터의 운영 및 업무수행에 필요한 사항은 대통령령으로 정한다.

제8조(한국정보보호진흥원) ① 정부는 정보보호 업무를 효율적으로 추진하기 위하여 한국정보보호진흥원(이하 "정보보호진흥원"이라 한다)을 설립한다.

② 정보보호진흥원은 법인으로 한다.

③ 정보보호진흥원은 다음 각 호의 사업을 한다.

1. 정보보호를 위한 법・정책 및 제도의 조사・연구

2. 정보보호와 관련한 통계의 조사・분석

3. 정보보호를 위한 홍보 및 이용자 지원

4. 정보보호 관련 기술 개발 및 표준화 지원

5. 정보보호 관련 교육・훈련 등 인력양성 지원

6. 정보보호산업 정책 지원

7. 정보보호 관리체계의 인증, 정보보호시스템 평가・인증 등 정보보호 인증・평가 등의 실시 및 지원

8. 민간 정보통신망 사고의 처리・원인분석 및 대응체계 운영

9.「전자서명법」 제25조제1항에 따른 전자서명인증관리

10.「정보보호산업의 진흥에 관한 법률」 제25조제7항에 따른 조정위원회의 운영지원

11. 정보보호 관련 국제협력 지원

12. 그 밖에 이 법 또는 다른 법령에 따라 정보보호진흥원의 업무로 정하거나 위탁한 사업이나 과학기술정보통신부장관으로부터 위탁받은 사업

④ 정보보호진흥원이 사업을 수행하는 데 필요한 경비는 다음 각 호의 재원으로 충당한다.

1. 정부의 출연금

2. 제3항 각 호의 사업수행에 따른 수입금

3. 그 밖에 정보보호진흥원의 운영에 따른 수입금

⑤ 정보보호진흥원에 관하여 이 법에서 정하지 아니한 사항에 대하여는 「민법」의 재단법인에 관한 규정을 준용한다.

⑥ 정보보호진흥원이 아닌 자는 한국정보보호진흥원의 명칭을 사용하지 못한다.

⑦ 정보보호진흥원의 운영 및 업무수행에 필요한 사항은 대통령령으로 정한다.

제9조(지원기관) ① 다음 각 호의 기관 또는 단체는 제21호에 따른 책임기관의 장 및 제26조에 따른 관리기관의 장이 요청하는 경우 대통령령으로 정하는 바에 따라 책임기관 및 관리기관에 정보보호를 위한 기술적 지원을 할 수 있다.

1. 한국정보보호진흥원

2.「과학기술분야 정부출연연구기관 등의 설립・운영 및 육성에 관한 법률」 제8조에 따라 설립된 한국전자통신연구원의 국가보안기술 연구・개발을 전담하는 부설연구소

3.「전자정부법」 제72조에 따른 한국지역정보개발원

4.「한국교육학술정보원법」에 따른 한국교육학술정보원

5.「한국재정정보원법」에 따른 한국재정정보원

6.「전자금융거래법」 제21조의6제1항제4호에 따라 금융위원회가 침해사고 대응을 위하여 지정한 기관

7.「산업기술의 유출방지 및 보호에 관한 법률」 제16조에 따른 산업기술보호협회

8.「정보보호산업의 진흥에 관한 법률」 제24조에 따른 한국정보보호산업협회

9. 제2항에 따라 지원기관으로 지정된 기관

② 과학기술정보통신부 장관은 정보보호를 위해 필요한 기술적 지원의 역량이 있는 것으로 인정되는 기관 또는 단체를 위원회의 심의를 거쳐 제1항에 따라 정보보호를 지원하는 기관(이하 “지원기관”이라 한다)으로 지정할 수 있다.

③ 제1항에 따른 기술적 지원의 범위는 다음 각 호와 같다.

1. 제22조에 따른 위험의 탐지

2. 제37조에 따른 사고의 조사 및 복구를 위한 조치

3. 제38조에 따른 사고대책본부가 하는 원인 분석 등의 조치

4. 그 밖에 정보보호를 위하여 대통령령으로 정하는 사항

④ 과학기술정보통신부 장관은 제3항 각 호의 기술적 지원이 불가능하다고 인정하는 경우에는 위원회의 심의를 거쳐 지원기관의 지정을 취소할 수 있다.

⑤ 중앙행정기관의 장은 그 직무와 관련된 기관 또는 단체를 지원기관으로 지정하거나 취소할 것을 과학기술정보통신부 장관에게 요청할 수 있다.

⑥ 과학기술정보통신부 장관은 관계 중앙행정기관과 합동으로 대통령령으로 정하는 바에 따라 지원기관의 기술적 지원 실태를 점검할 수 있다.

⑦ 과학기술정보통신부 장관 및 관계 중앙행정기관의 장은 지원기관의 기술적 지원에 드는 비용의 전부 또는 일부를 예산의 범위에서 지원할 수 있다.

제3장 정보통신망에서의 정보보호

제10조(정보통신망의 안정성 확보 등) ① 정보통신서비스 제공자(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제3호에 따른 "정보통신서비스 제공자"를 말한다)는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하여야 한다.

② 과학기술정보통신부장관은 제1항에 따른 보호조치의 구체적 내용을 정한 정보보호조치에 관한 지침(이하 "정보보호지침"이라 한다)을 정하여 고시하고 정보통신서비스 제공자에게 이를 지키도록 권고할 수 있다.

③ 정보보호지침에는 다음 각 호의 사항이 포함되어야 한다.

1. 정당한 권한이 없는 자가 정보통신망에 접근・침입하는 것을 방지하거나 대응하기 위한 정보보호시스템의 설치・운영 등 기술적・물리적 보호조치

2. 정보의 불법 유출・위조・변조・삭제 등을 방지하기 위한 기술적 보호조치

3. 정보통신망의 지속적인 이용이 가능한 상태를 확보하기 위한 기술적・물리적 보호조치

4. 정보통신망의 안정 및 정보보호를 위한 인력・조직・경비의 확보 및 관련 계획수립 등 관리적 보호조치

제11조(정보보호 사전점검) ① 정보통신서비스 제공자는 새로이 정보통신망을 구축하거나 정보통신서비스를 제공하고자 하는 때에는 그 계획 또는 설계에 정보보호에 관한 사항을 고려하여야 한다.

② 과학기술정보통신부장관은 다음 각 호의 어느 하나에 해당하는 정보통신서비스 또는 전기통신사업을 시행하고자 하는 자에게 대통령령으로 정하는 정보보호 사전점검기준에 따라 보호조치를 하도록 권고할 수 있다.

1. 이 법 또는 다른 법령에 따라 과학기술정보통신부장관의 인가·허가를 받거나 등록·신고를 하도록 되어 있는 사업으로서 대통령령으로 정하는 정보통신서비스 또는 전기통신사업

2. 과학기술정보통신부장관이 사업비의 전부 또는 일부를 지원하는 사업으로서 대통령령으로 정하는 정보통신서비스 또는 전기통신사업

③ 제2항에 따른 정보보호 사전점검의 기준·방법·절차·수수료 등 필요한 사항은 대통령령으로 정한다.

제12조(정보보호 최고책임자의 지정 등) ① 정보통신서비스 제공자는 정보보호를 위하여 임원급의 정보보호 최고책임자를 지정하고 과학기술정보통신부장관에게 신고하여야 한다. 다만, 자산총액, 매출액 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 지정하지 아니할 수 있다.

② 제1항에 따른 신고의 방법 및 절차 등에 대해서는 대통령령으로 정한다.

③ 제1항 본문에 따라 지정 및 신고된 정보보호 최고책임자(자산총액, 매출액 등 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우로 한정한다)는 제4항의 업무 외의 다른 업무를 겸직할 수 없다.

④ 정보보호 최고책임자는 다음 각 호의 업무를 총괄한다.

1. 정보보호관리체계의 수립 및 관리·운영

2. 정보보호 취약점 분석·평가 및 개선

3. 사고의 예방 및 대응

4. 사전 정보보호대책 마련 및 보안조치 설계·구현 등

5. 정보보호 사전 보안성 검토

6. 중요 정보의 암호화 및 보안서버 적합성 검토

7. 그 밖에 이 법 또는 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행

⑤ 정보통신서비스 제공자는 사고에 대한 공동 예방 및 대응, 필요한 정보의 교류, 그 밖에 대통령령으로 정하는 공동의 사업을 수행하기 위하여 제1항에 따른 정보보호 최고책임자를 구성원으로 하는 정보보호 최고책임자 협의회를 구성·운영할 수 있다.

⑥ 정부는 제5항에 따른 정보보호 최고책임자 협의회의 활동에 필요한 경비의 전부 또는 일부를 지원할 수 있다.

⑦ 정보보호 최고책임자의 자격요건 등에 필요한 사항은 대통령령으로 정한다.

제13조(집적된 정보통신시설의 보호) ① 타인의 정보통신서비스 제공을 위하여 집적된 정보통신시설을 운영·관리하는 사업자(이하 "집적정보통신시설 사업자"라 한다)는 정보통신시설을 안정적으로 운영하기 위하여 대통령령으로 정하는 바에 따른 보호조치를 하여야 한다.

② 집적정보통신시설 사업자는 집적된 정보통신시설의 멸실, 훼손, 그 밖의 운영장애로 발생한 피해를 보상하기 위하여 대통령령으로 정하는 바에 따라 보험에 가입하여야 한다.

제14조(집적정보통신시설 사업자의 긴급대응) ① 집적정보통신시설 사업자는 다음 각 호의 어느 하나에 해당하는 경우에는 이용약관으로 정하는 바에 따라 해당 서비스의 전부 또는 일부의 제공을 중단할 수 있다.

1. 집적정보통신시설을 이용하는 자(이하 "시설이용자"라 한다)의 정보시스템에서 발생한 이상현상으로 다른 시설이용자의 정보통신망 또는 집적된 정보통신시설의 정보통신망에 심각한 장애를 발생시킬 우려가 있다고 판단되는 경우

2. 외부에서 발생한 사고로 집적된 정보통신시설에 심각한 장애가 발생할 우려가 있다고 판단되는 경우

3. 중대한 사고가 발생하여 과학기술정보통신부장관이나 한국인터넷진흥원이 요청하는 경우

② 집적정보통신시설 사업자는 제1항에 따라 해당 서비스의 제공을 중단하는 경우에는 중단사유, 발생일시, 기간 및 내용 등을 구체적으로 밝혀 시설이용자에게 즉시 알려야 한다.

③ 집적정보통신시설 사업자는 중단사유가 없어지면 즉시 해당 서비스의 제공을 재개하여야 한다.

제15조(정보보호 관리체계의 인증) ① 과학기술정보통신부장관은 정보통신망의 안정성·신뢰성 확보를 위하여 관리적·기술적·물리적 보호조치를 포함한 종합적 관리체계(이하 "정보보호 관리체계"라 한다)를 수립·운영하고 있는 자에 대하여 제4항에 따른 기준에 적합한지에 관하여 인증을 할 수 있다.

② 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다.

1. 「전기통신사업법」 제6조제1항에 따른 등록을 한 자로서 대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자
2. 집적정보통신시설 사업자
3. 연간 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상 또는 3개월간의 일일평균 이용자수 100만명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자

③ 과학기술정보통신부장관은 제2항에 따라 인증을 받아야 하는 자가 과학기술정보통신부령으로 정하는 바에 따라 국제표준 정보보호 인증을 받거나 정보보호 조치를 취한 경우에는 제1항에 따른 인증 심사의 일부를 생략할 수 있다. 이 경우 인증 심사의 세부 생략 범위에 대해서는 과학기술정보통신부장관이 정하여 고시한다.

④ 과학기술정보통신부장관은 제1항에 따른 정보보호 관리체계 인증을 위하여 관리적·기술적·물리적 보호대책을 포함한 인증기준 등 그 밖에 필요한 사항을 정하여 고시할 수 있다.

⑤ 제1항에 따른 정보보호 관리체계 인증의 유효기간은 3년으로 한다. 다만, 제47조의5제1항에 따라 정보보호 관리등급을 받은 경우 그 유효기간 동안 제1항의 인증을 받은 것으로 본다.

⑥ 과학기술정보통신부장관은 정보보호진흥원 또는 과학기술정보통신부장관이 지정한 기관(이하 "정보보호 관리체계 인증기관"이라 한다)으로 하여금 제1항 및 제2항에 따른 인증에 관한 업무로서 다음 각 호의 업무를 수행하게 할 수 있다.

1. 인증 신청인이 수립한 정보보호 관리체계가 제4항에 따른 인증기준에 적합한지 여부를 확인하기 위한 심사(이하 "인증심사"라 한다)
2. 인증심사 결과의 심의
3. 인증서 발급·관리

4. 인증의 사후관리

5. 정보보호 관리체계 인증심사원의 양성 및 자격관리

6. 그 밖에 정보보호 관리체계 인증에 관한 업무

⑦ 과학기술정보통신부장관은 인증에 관한 업무를 효율적으로 수행하기 위하여 필요한 경우 인증심사 업무를 수행하는 기관(이하 "정보보호 관리체계 심사기관"이라 한다)을 지정할 수 있다.

⑧ 정보보호진흥원, 정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관은 정보보호 관리체계의 실효성 제고를 위하여 연 1회 이상 사후관리를 실시하고 그 결과를 과학기술정보통신부장관에게 통보하여야 한다.

⑨ 제1항 및 제2항에 따라 정보보호 관리체계의 인증을 받은 자는 대통령령으로 정하는 바에 따라 인증의 내용을 표시하거나 홍보할 수 있다.

⑩ 과학기술정보통신부장관은 다음 각 호의 어느 하나에 해당하는 사유를 발견한 경우에는 인증을 취소할 수 있다. 다만, 제1호에 해당하는 경우에는 인증을 취소하여야 한다.

1. 거짓이나 그 밖의 부정한 방법으로 정보보호 관리체계 인증을 받은 경우

2. 제4항에 따른 인증기준에 미달하게 된 경우

3. 제8항에 따른 사후관리를 거부 또는 방해한 경우

⑪ 제1항 및 제2항에 따른 인증의 방법·절차·범위·수수료, 제8항에 따른 사후관리의 방법·절차, 제10항에 따른 인증취소의 방법·절차, 그 밖에 필요한 사항은 대통령령으로 정한다.

⑫ 정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관 지정의 기준·절차·유효기간 등에 필요한 사항은 대통령령으로 정한다.

제16조(정보보호 관리체계 인증기관 및 정보보호 관리체계 심사기관의 지정취소 등)

① 과학기술정보통신부장관은 제15조에 따라 정보보호 관리체계 인증기관 또는 정보보호 관리체계 심사기관으로 지정받은 법인 또는 단체가 다음 각 호의 어느 하나에 해당하면 그 지정을 취소하거나 1년 이내의 기간을 정하여 해당 업무의 전부 또는 일부의 정지를 명할 수 있다. 다만, 제1호나 제2호에 해당하는 경우에는 그 지정을 취소하여야 한다.

1. 거짓이나 그 밖의 부정한 방법으로 정보보호 관리체계 인증기관 또는 정보보호 관리체계 심사기관의 지정을 받은 경우

2. 업무정지기간 중에 인증 또는 인증심사를 한 경우

3. 정당한 사유 없이 인증 또는 인증심사를 하지 아니한 경우

4. 제15조제11항을 위반하여 인증 또는 인증심사를 한 경우

5. 제15조제12항에 따른 지정기준에 적합하지 아니하게 된 경우

② 제1항에 따른 지정취소 및 업무정지 등에 필요한 사항은 대통령령으로 정한다.

제17조(이용자의 정보보호) ① 정부는 이용자의 정보보호에 필요한 기준을 정하여 이용자에게 권고하고 사고의 예방 및 확산 방지를 위하여 취약점 점검, 기술 지원 등 필요한 조치를 할 수 있다.

② 주요정보통신서비스 제공자는 정보통신망에 중대한 사고가 발생하여 자신의 서비스를 이용하는 이용자의 정보시스템 또는 정보통신망 등에 심각한 장애가 발생할 가능성이 있으면 이용약관으로 정하는 바에 따라 그 이용자에게 보호조치를 취하도록 요청하고, 이를 이행하지 아니하는 경우에는 해당 정보통신망으로의 접속을 일시적으로 제한할 수 있다.

③ 「소프트웨어산업 진흥법」 제2조에 따른 소프트웨어사업자는 보안에 관한 취약점을 보완하는 프로그램을 제작하였을 때에는 정보보호진흥원에 알려야 하고, 그 소프트웨어 사용자에게는 제작한 날부터 1개월 이내에 2회 이상 알려야 한다.

④ 제2항에 따른 보호조치의 요청 등에 관하여 이용약관으로 정하여야 하는 구체적인 사항은 대통령령으로 정한다.

제18조(정보보호 관리등급 부여) ① 제15조에 따라 정보보호 관리체계 인증을 받은 자는 기업의 통합적 정보보호 관리수준을 제고하고 이용자로부터 정보보호 서비스에 대한 신뢰를 확보하기 위하여 과학기술정보통신부장관으로부터 정보보호 관리등급을 받을 수 있다.

② 과학기술정보통신부장관은 정보보호진흥원으로 하여금 제1항에 따른 등급 부여에 관한 업무를 수행하게 할 수 있다.

③ 제1항에 따라 정보보호 관리등급을 받은 자는 대통령령으로 정하는 바에 따라 해당 등급의 내용을 표시하거나 홍보에 활용할 수 있다.

④ 과학기술정보통신부장관은 다음 각 호의 어느 하나에 해당하는 사유를 발견한 경우에는 부여한 등급을 취소할 수 있다. 다만, 제1호에 해당하는 경우에는 부여한 등급을 취소하여야 한다.

1. 거짓이나 그 밖의 부정한 방법으로 정보보호 관리등급을 받은 경우

2. 제5항에 따른 등급기준에 미달하게 된 경우

⑤ 제1항에 따른 등급 부여의 심사기준 및 등급 부여의 방법·절차·수수료, 등급의 유효기간, 제4항에 따른 등급취소의 방법·절차, 그 밖에 필요한 사항은 대통령령으로 정한다.

제19조(중요 정보의 국외유출 제한 등) ① 정부는 국내의 산업·경제 및 과학기술 등에 관한 중요 정보가 정보통신망을 통하여 국외로 유출되는 것을 방지하기 위하여 정보통신서비스 제공자 또는 이용자에게 필요한 조치를 하도록 할 수 있다.

② 제1항에 따른 중요 정보의 범위는 다음 각 호와 같다.

1. 국가안전보장과 관련된 보안정보 및 주요 정책에 관한 정보

2. 국내에서 개발된 첨단과학 기술 또는 기기의 내용에 관한 정보

③ 정부는 제2항 각 호에 따른 정보를 처리하는 정보통신서비스 제공자에게 다음 각 호의 조치를 하도록 할 수 있다.

1. 정보통신망의 부당한 이용을 방지할 수 있는 제도적·기술적 장치의 설정

2. 정보의 불법파괴 또는 불법조작을 방지할 수 있는 제도적·기술적 조치

3. 정보통신서비스 제공자가 처리 중 알게 된 중요 정보의 유출을 방지할 수 있는 조치

제20조(비밀 등의 보호) 누구든지 정보통신망에 의하여 처리·보관 또는 전송되는 타인의 정보를 훼손하거나 타인의 비밀을 침해·도용 또는 누설하여서는 아니 된다.

제4장 공공기관 정보보호

제21조(책임기관) ① 다음 각 호의 기관의 장은 이 법에 따라 소관 정보통신망에서의 정보보호 책임을 진다.

1. 국회・법원・헌법재판소・중앙선거관리위원회의 행정사무를 처리하는 기관 및 그 소속 기관
2. 중앙행정기관 및 그 소속 기관
3. 특별시・광역시・특별자치시・도・특별자치도(이하 “시・도”라 한다)와 시・군・자치구 및 그 소속 기관, 시・도 교육청과 교육지원청 및 그 소속 기관
4.「국군조직법」에 따른 각 군, 합동참모본부, 국방부 직할 부대 및 직할 기관
5.「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관
6.「지방공기업법」 제49조에 따른 지방공사 및 같은 법 제76조에 따른 지방공단

② 제1항에 따른 기관(이하 “책임기관”이라 한다) 중 국회・법원・헌법재판소・중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관, 시・도 및 시・도 교육청(이하 “상급책임기관”이라 한다)의 장은 정보보호를 위한 전담 조직을 설치하고, 관련 예산을 확보하여야 한다.

③ 국가와 지방자치단체는 책임기관의 장이 정보보호 업무를 수행하는 데 필요한 행정적・재정적・기술적 지원을 할 수 있다.

④ 제3항에 따른 지원의 요건, 지원 대상의 선정과 관리 등에 필요한 사항은 대통령령으로 정한다.

제22조(책임기관의 위험 탐지체계 등) ① 과학기술정보통신부장관은 국가 정보통신망에 대한 위험에 대해 신속하고 효율적으로 대응하기 위하여 관계 중앙행정기관의 장과 협의하여 국가 차원의 위험 탐지・대응체계를 구축・운영하여야 한다.

② 책임기관의 장은 제1항에 따른 위험에 대한 탐지・대응체계를 위하여 대통령령으로 정하는 바에 따라 소관 정보통신망에서 발생하는 위험을 탐지하여 즉시 대응할 수 있는 기구(이하 “보안관제센터”라 한다)를 설치・운영하여야 한다. 다만, 보안관제센터를 설치・운영할 수 없는 경우에는 다른 책임기관의 장이 설치・운영하는 보안관제센터에 그 업무를 위탁할 수 있다.

③ 보안관제센터는 위험의 탐지·대응에 필요한 최소한의 범위에서 「개인정보 보호법」 제2조제1호에 따른 개인정보를 수집·이용할 수 있다. 다만, 수집된 개인정보의 안전성을 확보하기 위한 기술적·관리적 조치를 하여야 한다.

④ 제2항에 따른 보안관제센터의 설치·운영, 위험의 탐지 범위 등에 관하여 필요한 사항은 대통령령으로 정한다.

제23조(정보보호 실태평가) ① 과학기술정보통신부장관은 제21조제1항제2호부터 제6호까지의 책임기관 중에서 대통령령으로 정하는 책임기관을 대상으로 정보보호를 위한 업무수행체계 구축, 위험 예방 및 대응활동 등에 관한 실태평가(이하 "실태평가"라 한다)를 할 수 있다.

② 과학기술정보통신부장관은 실태평가를 하거나 실태평가에 관한 전문적·기술적인 연구 또는 자문을 위하여 정보보호실태지원단을 구성·운영할 수 있다.

③ 과학기술정보통신부장관은 실태평가의 결과를 평가를 받은 책임기관의 장에게 통보하여야 한다.

④ 평가를 받은 책임기관의 장은 실태평가 결과에서 나타난 미비사항에 대해서는 개선 대책을 마련하여 과학기술정보통신부장관에게 통보하여야 한다.

⑤ 실태평가의 절차와 방법, 결과의 처리 등에 필요한 사항은 대통령령으로 정한다.

제24조(전자정부서비스의 보호) ① 과학기술정보통신부장관은 「전자정부법」 제24조에 따른 전자적 대민서비스와 관련된 보안대책에 대해 행정안전부장관에게 의견을 제시할 수 있다.

② 과학기술정보통신부장관은 정보통신망을 이용하여 전자문서를 보관·유통할 때 위조·변조·훼손 또는 유출을 방지하기 위한 보안조치(「전자정부법」 제56조제3항에 따른 보안조치를 말한다)의 안전성을 개발·검증하고 그 이행 여부를 확인할 수 있다.

③ 제2항의 보안조치는 암호장치와 정보보호시스템의 도입·운용을 포함한다.

제25조(사고 대응 훈련) ① 상급책임기관의 장은 정보보호 사고에 효율적으로 대응하기 위하여 소관 정보통신망을 대상으로 사고 대응 훈련을 정기적으로 실시하여야 한다.

② 과학기술정보통신부장관은 사고 발생에 대비하여 책임기관의 정보통신망을 대상으로 사고 대응 통합훈련을 실시할 수 있다. 이 경우 과학기술정보통신부장관은 특별한 사유가 없으면 사전에 훈련 일정 등을 해당 기관의 장에게 통보하여야 한다.

③ 제2항에 따른 통합훈련은 매년 정기훈련과 수시훈련으로 구분하여 실시할 수 있으며, 「비상대비자원 관리법」 제14조에 따른 비상대비 훈련과 함께 실시할 수 있다.

④ 제1항부터 제3항까지의 규정에 따른 훈련 대상・실시방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

제5장 주요 정보통신기반시설의 보호

제26조(주요정보통신기반시설보호대책의 수립 등) ①주요정보통신기반시설을 관리하는 기관(이하 "관리기관"이라 한다)의 장은 제32조제1항의 규정에 의한 취약점 분석・평가의 결과에 따라 소관 주요정보통신기반시설 및 관리 정보를 안전하게 보호하기 위한 예방, 백업, 복구 등 물리적・기술적 대책을 포함한 관리대책(이하 "주요정보통신기반시설보호대책"이라 한다)을 수립・시행하여야 한다.

②관리기관의 장은 제1항의 규정에 의하여 주요정보통신기반시설보호대책을 수립한 때에는 이를 주요정보통신기반시설을 관할하는 중앙행정기관(이하 "관계중앙행정기관"이라 한다)의 장에게 제출하여야 한다. 다만, 관리기관의 장이 관계중앙행정기관의 장인 경우에는 그러하지 아니하다.

③지방자치단체의 장이 관리・감독하는 관리기관의 주요정보통신기반시설보호대책은 지방자치단체의 장이 행정안전부장관에게 제출하여야 한다.

④관리기관의 장은 소관 주요정보통신기반시설의 보호에 관한 업무를 총괄하는 자(이하 "정보보호책임자"라 한다)를 지정하여야 한다. 다만, 관리기관의 장이 관계중앙행정기관의 장인 경우에는 그러하지 아니하다.

⑤정보보호책임자의 지정 및 업무 등에 관하여 필요한 사항은 대통령령으로 정한다.

제27조(주요정보통신기반시설보호대책 이행 여부의 확인) ① 과학기술정보통신부장관은 관리기관에 대하여 주요정보통신기반시설보호대책의 이행 여부를 확인할 수 있다.

② 과학기술정보통신부장관은 제1항에 따른 확인을 위하여 필요한 경우 관계중앙행정기관의 장에게 제26조제2항에 따라 제출받은 주요정보통신기반시설보호대책 등의 자료 제출을 요청할 수 있다.

③ 과학기술정보통신부장관은 제1항에 따라 확인한 주요정보통신기반시설보호대책의 이행 여부를 관계중앙행정기관의 장에게 통보할 수 있다.

④ 제1항에 따른 주요정보통신기반시설보호대책 이행 여부의 확인절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

제28조(주요정보통신기반시설보호계획의 수립 등) ① 관계중앙행정기관의 장은 제26조 제2항의 규정에 의하여 제출받은 주요정보통신기반시설보호대책을 종합·조정하여 소관분야에 대한 주요정보통신기반시설에 관한 보호계획(이하 "주요정보통신기반시설보호계획"이라 한다)을 수립·시행하여야 한다.

②관계중앙행정기관의 장은 전년도 주요정보통신기반시설보호계획의 추진실적과 다음 연도의 주요정보통신기반시설보호계획을 위원회에 제출하여 그 심의를 받아야 한다. 다만, 위원회의 위원장이 보안이 요구된다고 인정하는 사항에 대하여는 그러하지 아니하다.

③주요정보통신기반시설보호계획에는 다음 각호의 사항이 포함되어야 한다.

1. 주요정보통신기반시설의 취약점 분석·평가에 관한 사항
2. 주요정보통신기반시설 및 관리 정보의 침해사고에 대한 예방, 백업, 복구대책에 관한 사항
3. 그 밖에 주요정보통신기반시설의 보호에 관하여 필요한 사항

④과학기술정보통신부장관은 주요정보통신기반시설보호대책 및 주요정보통신기반시설보호계획의 수립지침을 정하여 이를 관계중앙행정기관의 장에게 통보할 수 있다.

⑤관계중앙행정기관의 장은 소관분야의 주요정보통신기반시설의 보호에 관한 업무를 총괄하는 자(이하 "정보보호책임관"이라 한다)를 지정하여야 한다.

⑥주요정보통신기반시설보호계획의 수립·시행에 관한 사항과 정보보호책임관의 지정 및 업무 등에 관하여 필요한 사항은 대통령령으로 정한다.

제29조(주요정보통신기반시설의 보호지원) ①관리기관의 장이 필요하다고 인정하거나 위원회의 위원장이 특정 관리기관의 주요정보통신기반시설보호대책의 미흡으로 국가안전보장이나 경제사회전반에 피해가 우려된다고 판단하여 그 보완을 명하는 경우 해당 관리기관의 장은 과학기술정보통신부장관 또는 필요한 경우 제9조에 따른 지원기관의 장에게 다음 각 호의 업무에 대한 기술적 지원을 요청할 수 있다.

1. 주요정보통신기반시설보호대책의 수립

2. 주요정보통신기반시설의 사고 예방 및 복구

3. 제33조에 따른 보호조치 명령·권고의 이행

②국가안전보장에 중대한 영향을 미치는 다음 각 호의 주요정보통신기반시설에 대한 관리기관의 장이 제1항에 따라 기술적 지원을 요청하는 경우 과학기술정보통신부장관에게 우선적으로 그 지원을 요청하여야 한다. 다만, 국가안전보장에 현저하고 급박한 위험이 있고, 관리기관의 장이 요청할 때까지 기다릴 경우 그 피해를 회복할 수 없을 때에는 과학기술정보통신부장관은 관계중앙행정기관의 장과 협의하여 그 지원을 할 수 있다.

1. 도로·철도·지하철·공항·항만 등 주요 교통시설

2. 전력, 가스, 석유 등 에너지·수자원 시설

3. 방송중계·국가지도통신망 시설

4. 원자력·국방과학·첨단방위산업관련 정부출연연구기관의 연구시설

제30조(주요정보통신기반시설의 지정 등) ①중앙행정기관의 장은 소관분야의 정보통신기반시설중 다음 각호의 사항을 고려하여 정보보호 위험으로부터의 보호가 필요하다고 인정되는 정보통신기반시설을 주요정보통신기반시설로 지정할 수 있다.

1. 당해 정보통신기반시설을 관리하는 기관이 수행하는 업무의 국가사회적 중요성

2. 제1호의 규정에 의한 기관이 수행하는 업무의 정보통신기반시설에 대한 의존도

3. 다른 정보통신기반시설과의 상호연계성

4. 사고가 발생할 경우 국가안전보장과 경제사회에 미치는 피해규모 및 범위

5. 사고의 발생가능성 또는 그 복구의 용이성

②중앙행정기관의 장은 제1항의 규정에 의한 지정 여부를 결정하기 위하여 필요한 자료의 제출을 해당 관리기관에 요구할 수 있다.

③관계중앙행정기관의 장은 관리기관이 해당 업무를 폐지・정지 또는 변경하는 경우에는 직권 또는 해당 관리기관의 신청에 의하여 주요정보통신기반시설의 지정을 취소할 수 있다.

④지방자치단체의 장이 관리・감독하는 기관의 정보통신기반시설에 대하여는 행정안전부장관이 지방자치단체의 장과 협의하여 주요정보통신기반시설로 지정하거나 그 지정을 취소할 수 있다.

⑤중앙행정기관의 장이 제1항 및 제3항의 규정에 의하여 지정 또는 지정 취소를 하고자 하는 경우에는 위원회의 심의를 받아야 한다. 이 경우 위원회는 제1항 및 제3항의 규정에 의하여 지정 또는 지정취소의 대상이 되는 관리기관의 장을 위원회에 출석하게 하여 그 의견을 들을 수 있다.

⑥중앙행정기관의 장은 제1항 및 제3항의 규정에 의하여 주요정보통신기반시설을 지정 또는 지정 취소한 때에는 이를 고시하여야 한다. 다만, 국가안전보장을 위하여 필요한 경우에는 위원회의 심의를 받아 이를 고시하지 아니할 수 있다.

⑦주요정보통신기반시설의 지정 및 지정취소 등에 관하여 필요한 사항은 이를 대통령령으로 정한다.

제31조(주요정보통신기반시설의 지정 권고) ① 과학기술정보통신부장관은 특정한 정보통신기반시설을 주요정보통신기반시설로 지정할 필요가 있다고 판단되는 경우에는 중앙행정기관의 장에게 해당 정보통신기반시설을 주요정보통신기반시설로 지정하도록 권고할 수 있다. 이 경우 지정 권고를 받은 중앙행정기관의 장은 위원회의 심의를 거쳐 지정 여부를 결정하여야 한다.

② 과학기술정보통신부장관은 제1항에 따른 권고를 위하여 필요한 경우에는 중앙행정기관의 장에게 해당 정보통신기반시설에 관한 자료를 요청할 수 있다.

③ 제1항에 따른 주요정보통신기반시설의 지정 권고 절차, 그 밖에 필요한 사항은 대통령령으로 정한다.

제32조(취약점의 분석・평가) ①관리기관의 장은 대통령령이 정하는 바에 따라 정기적으로 소관 주요정보통신기반시설의 취약점을 분석・평가하여야 한다.

②관리기관의 장은 제1항의 규정에 의하여 취약점을 분석·평가하고자 하는 경우에는 대통령령이 정하는 바에 따라 취약점을 분석·평가하는 전담반을 구성하여야 한다.

③관리기관의 장은 제1항의 규정에 의하여 취약점을 분석·평가하고자 하는 경우에는 제9조에 따른 지원기관으로 하여금 소관 주요정보통신기반시설의 취약점을 분석·평가하게 할 수 있다. 이 경우 제2항의 규정에 의한 전담반을 구성하지 아니할 수 있다.

④과학기술정보통신부장관은 관계중앙행정기관의 장과 협의하여 제1항의 규정에 의한 취약점 분석·평가에 관한 기준을 정하고 이를 관계중앙행정기관의 장에게 통보하여야 한다.

⑤주요정보통신기반시설의 취약점 분석·평가의 방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

제33조(보호지침) ①관계중앙행정기관의 장은 소관분야의 주요정보통신기반시설에 대하여 보호지침을 제정하고 해당분야의 관리기관의 장에게 이를 지키도록 권고할 수 있다.

②관계중앙행정기관의 장은 기술의 발전 등을 감안하여 제1항의 규정에 의한 보호지침을 주기적으로 수정·보완하여야 한다.

제34조(보호조치 명령 등) 관계중앙행정기관의 장은 다음 각 호의 어느 하나에 해당하는 경우 해당 관리기관의 장에게 주요정보통신기반시설의 보호에 필요한 조치를 명령 또는 권고할 수 있다.

1. 제26조제2항에 따라 제출받은 주요정보통신기반시설보호대책을 분석하여 별도의 보호조치가 필요하다고 인정하는 경우

2. 제27조제3항에 따라 통보된 주요정보통신기반시설보호대책의 이행 여부를 분석하여 별도의 보호조치가 필요하다고 인정하는 경우

제35조(관리기관에 대한 지원) 정부는 관리기관에 대하여 주요정보통신기반시설을 보호하기 위하여 필요한 기술의 이전, 장비의 제공 그 밖의 필요한 지원을 할 수있다.

제6장 사고의 대응

제36조(사고의 신고 및 통보) ① 과학기술정보통신부장관은 사고에 신속히 대응하기 위하여 사고의 신고 혹은 통보 및 조사를 위한 국가 차원의 일원화된 체계를 구축・운영하여야 한다.

② 다음 각 호의 어느 하나에 해당하는 자는 사고가 발생한 경우에는 피해를 최소화하는 조치를 하고, 그 사실을 과학기술정보통신부장관이나 정보보호진흥원에 신고하여야 한다.

1. 정보통신서비스 제공자
2. 집적정보통신시설 사업자
3. 주요정보통신기반시설의 관리기관

③ 책임기관의 장은 소관 정보통신망에서 사고가 발생한 경우에는 피해를 최소화하는 조치를 하고, 그 사실을 다음 각 호의 구분에 따른 사람에게 통보하여야 한다.

1. 상급책임기관: 과학기술정보통신부장관 . 이 경우 특별시장・광역시장・특별자치시장・도지사・특별자치도지사(이하 “시・도지사”라 한다)는 행정자치부장관에게, 시・도 교육감은 교육부장관에게 함께 통보하여야 한다.
2. 시・군・자치구: 해당 시・군・자치구를 관할구역으로 하는 시・도지사
3. 교육지원청: 해당 교육지원청을 관할하는 시・도 교육감
4. 그 밖의 책임기관: 해당 책임기관을 관리・감독하는 상급책임기관의 장

④ 정부는 제2항 및 제3항의 규정에 의하여 사고를 신고 혹은 통보함으로써 피해확산의 방지에 기여한 기관에 예산의 범위안에서 복구비 등 재정적 지원을 할 수 있다.

제37조(사고의 조사 및 복구) ① 정보통신서비스 제공자 등 정보통신망을 운영하는 자・주요정보통신기반시설 관리기관・책임기관은 사고가 발생한 때에는 사고의 원인 분석, 피해 확산의 방지, 복구 및 보호에 필요한 조치를 신속히 취하여야 한다.

② 과학기술정보통신부장관은 정보통신서비스 제공자의 정보통신망에 중대한 사고가 발생하면 사고의 원인 분석, 피해 확산의 방지, 복구 및 보호에 필요한 조치를 위하여 정보보호에 전문성을 갖춘 민・관합동조사단을 구성할 수 있다.

③ 과학기술정보통신부장관은 제2항에 따른 사고의 원인을 분석하기 위하여 필요하다고 인정하면 정보통신서비스 제공자와 집적정보통신시설 사업자에게 정보통신망의 접속기록 등 관련 자료의 보전을 명할 수 있다.

④ 과학기술정보통신부장관은 사고의 원인을 분석하기 위하여 필요하면 정보통신서비스 제공자와 집적정보통신시설 사업자에게 사고 관련 자료의 제출을 요구할 수 있으며, 제2항에 따른 민・관합동조사단에게 관계인의 사업장에 출입하여 사고 원인을 조사하도록 할 수 있다. 다만, 「통신비밀보호법」 제2조제11호에 따른 통신사실확인자료에 해당하는 자료의 제출은 같은 법으로 정하는 바에 따른다.

⑤ 과학기술정보통신부장관이나 민・관합동조사단은 제4항에 따라 제출받은 자료와 조사를 통하여 알게 된 정보를 사고의 원인 분석 및 대책 마련 외의 목적으로는 사용하지 못하며, 원인 분석이 끝난 후에는 즉시 파기하여야 한다.

⑥ 제2항에 따른 민・관합동조사단의 구성과 제4항에 따라 제출된 침해사고 관련 자료의 보호 등에 필요한 사항은 대통령령으로 정한다.

⑦ 관리기관의 장은 제1항의 조치를 위하여 필요한 경우 관계중앙행정기관의 장 또는 지원기관의 장에게 지원을 요청할 수 있다.

⑧ 관계중앙행정기관의 장 또는 지원기관의 장은 제7항의 규정에 의한 지원요청을 받은 때에는 피해복구가 신속히 이루어질 수 있도록 기술지원 등 필요한 지원을 하여야 하고, 피해확산을 방지할 수 있도록 관리기관의 장과 함께 적절한 조치를 취하여야 한다.

⑨ 상급책임기관의 장은 제36조 3항 제2호부터 제4호까지의 통보를 받은 경우 신속히 사고로 인한 피해 확인, 원인 분석 및 재발 방지를 위한 조사를 하여야 한다. 이 경우 해당 기관의 장은 필요하면 지원기관의 장에게 기술적 지원을 요청할 수 있다.

⑩ 과학기술정보통신부장관은 제36조 3항 제1호에 따른 통보를 받은 경우 또는 국가 정보통신망에 중대한 사고가 발생한 경우에는 지체 없이 사고의 피해 확인, 원인 분석 및 재발 방지를 위한 조사를 하여야 한다.

⑪ 상급책임기관의 장과 과학기술정보통신부장관은 조사를 하는 과정에서 사고와 관련된 악성프로그램 또는 악성프로그램에 감염되도록 유인하는 전자적 정보(이하 “악성프로그램등”이라 한다)가 포함된 컴퓨터, 웹사이트 또는 소프트웨어 등을 발견한 경우에는 관리자에게 관련 악성프로그램등의 제공을

요청하거나 백신프로그램 제공 등을 통하여 악성프로그램등의 삭제 또는 차단을 요청할 수 있다.

제38조(대책본부의 구성・운영) ① 상급책임기관의 장은 관할 정보통신망에 각 호의 어느 하나에 해당하는 사고가 발생한 경우 사고에 대한 원인 분석, 사고 조사, 긴급 대응, 피해 복구 등의 신속한 조치를 하기 위하여 책임기관, 지원기관 및 수사기관이 참여하는 사고대책본부(이하 “대책본부”라 한다)를 구성・운영할 수 있다. 다만, 2개 이상의 상급책임기관에 대책본부를 구성하여야 하는 경우에는 이를 갈음하여 과학기술정보통신부장관이 관련 상급책임기관의 장과 협의하여 대책본부를 구성・운영할 수 있다.

1. 대통령령으로 정하는 단계 이상의 경보 또는 분야별 경보가 발령된 경우

2. 사고 발생으로 인한 피해가 심각하다고 판단하는 경우

② 주요정보통신기반시설에 대하여 제1항 각 호의 사고가 발생한 경우, 과학기술정보통신부장관은 대책본부를 구성・운영할 수 있다.

③ 대책본부의 장은 대책본부를 설치하는 기관의 장이 과학기술정보통신부장관과 협의하여 임명한다. 주요정보통신기반시설의 사고 대응을 위한 대책본부의 장은 과학기술정보통신부장관이 해당 정보통신기반시설을 관할하는 중앙행정기관의 장과 협의하여 임명한다.

④ 대책본부의 장은 대책본부의 구성・운영을 위하여 필요한 경우 책임기관, 관할 중앙행정기관, 지원기관의 장에게 인력 파견 또는 장비 제공 등 협력과 지원을 요청할 수 있다.

⑤ 제4항의 규정에 의하여 협력과 지원을 요청받은 책임기관, 관할 중앙행정기관, 지원기관의 장 등은 특별한 사유가 없는 한 이에 응하여야 한다.

⑥ 대책본부의 구성・운영 등에 관하여 필요한 사항은 대통령령으로 정한다.

제39조(위험정보의 공유) ① 금융・통신 등 분야별 정보통신기반시설을 보호하기 위하여 다음 각호의 업무를 수행하고자 하는 자는 정보공유・분석센터를 구축・운영할 수 있다.

1. 취약점 및 침해요인과 그 대응방안에 관한 정보 제공

2. 사고가 발생하는 경우 실시간 경보・분석체계 운영

② 정부는 제1항 각호의 업무를 수행하는 정보공유・분석센터의 구축을 장려하고 그에 대한 재정적・기술적 지원을 할 수 있다.

③ 정보보호에 대한 위험 및 예방에 관련된 정보(이하 “위험 정보”라 한다.)를 공유하기 위하여 정보보호센터 내에 위험정보 공유센터(이하 “공유센터”라 한다)를 둔다.

④ 책임기관의 장은 소관 정보통신망의 위험 정보가 다른 책임기관의 정보보호를 위하여 필요하다고 인정하는 경우 대통령령으로 정하는 바에 따라 소관 정보통신망의 위험정보를 제3항에 따른 공유센터의 장에게 제공할 수 있다. 이 경우 공유센터의 장은 정보보호를 위하여 위험정보의 공유가 필요하다고 판단되는 책임기관의 장에게 위험정보를 제공하여야 한다.

⑤ 위험정보에 개인정보가 포함되어 있을 경우 「개인정보보호법」 제O조에 따라 가명처리 혹은 가능한 한 익명처리한 후 제공해야 한다.

⑥ 누구든지 공유된 위험정보를 사용할 때에는 정보보호 목적에 필요한 최소한의 범위에서 사용・관리하여야 한다.

⑦ 공유센터의 장은 위험정보를 공유하는 경우 국민의 권리가 침해되지 아니하도록 기술적・관리적 또는 물리적 보호조치를 마련하여야 한다.

⑧ 공유센터의 장은 기술적・관리적 또는 물리적 보호조치에 관하여 개인정보보호위원회와 협의해야 한다.

⑨ 공유센터의 설치・운영, 공유센터의 장에게 제공하는 위험정보의 범위 등에 필요한 사항은 대통령령으로 정한다.

제40조(사고통계 및 분석) ① 다음 각 호의 어느 하나에 해당하는 자는 대통령령으로 정하는 바에 따라 사고의 유형별 통계, 해당 정보통신망의 소통량 통계 및 접속경로별 이용 통계 등 사고 관련 정보를 정보보호센터에 제공하여야 한다.

1. 주요정보통신서비스 제공자
2. 집적정보통신시설 사업자
3. 주요 정보통신기반시설 관리기관
4. 책임기관
5. 그 밖에 정보통신망을 운영하는 자로서 대통령령으로 정하는 자

② 정보보호센터는 제1항에 따른 정보를 분석하여 과학기술정보통신부장관에게 보고하여야 한다.

③ 과학기술정보통신부장관은 제1항에 따라 정보를 제공하여야 하는 자가 정당한 사유 없이 정보의 제공을 거부하거나 거짓 정보를 제공하면 상당한 기간을 정하여 시정을 명할 수 있다.

④ 과학기술정보통신부장관이나 정보보호센터는 제1항에 따라 제공받은 정보를 침해사고의 대응을 위하여 필요한 범위에서만 정당하게 사용하여야 한다.

제41조(위험경보의 발령 및 조치) ① 과학기술정보통신부장관은 위험에 대해 국가 차원에서 체계적으로 대응하기 위하여 단계별 위험경보(이하 “경보”라 한다)를 발령할 수 있다.

② 대통령령으로 정하는 중앙행정기관의 장은 소관 분야를 대상으로 분야별 위험경보(이하 “분야별 경보”라 한다)를 발령할 수 있다. 이 경우 중앙행정기관의 장은 분야별 경보의 발령 시점과 단계 등에 관하여 과학기술정보통신부장관과 미리 협의하여야 한다.

③ 책임기관의 장은 경보 또는 분야별 경보가 발령된 경우 즉시 피해발생의 최소화 및 피해복구를 위한 조치를 하여야 한다.

④ 경보 및 분야별 경보 발령의 기준・절차 및 책임기관의 장의 조치 등에 필요한 사항은 대통령령으로 정한다.

제7장 보칙

제42조(정보통신망 침해행위 등의 금지) 누구든지 다음 각 호의 1에 해당하는 행위를 하여서는 아니된다.

1. 정당한 접근권한 없이 정보통신망 또는 주요정보통신기반시설에 접근하는 행위

2. 정당한 접근권한 없이 또는 허용된 접근권한을 넘어 정보통신망 또는 주요정보통신기반시설에 저장된 데이터를 훼손・멸실・변경・위조・유출하는 행위

3. 정보통신망 또는 주요정보통신기반시설의 운영을 방해할 목적으로 컴퓨터바이러스・논리폭탄 등의 프로그램(“이하 악성프로그램”이라 한다)을 전달 또는 유포하는 행위

4. 정보통신망 또는 주요정보통신기반시설의 운영을 방해할 목적으로 일시에 대량의 신호를 보내거나 부정한 명령을 처리하도록 하는 등의 방법으로 장애가 발생하도록 하는 행위

제43조(기술개발 등) ①정부는 정보보호를 위하여 필요한 기술의 연구 및 개발에 관한 시책을 강구할 수 있다.

② 정부는 정보보호에 필요한 기술개발을 효율적으로 추진하기 위하여 필요한 때에는 정보보호 기술개발과 관련된 연구기관 및 민간단체로 하여금 이를 대행하게 할 수 있다. 이 경우 이에 소요되는 비용의 전부 또는 일부를 지원할 수 있다.

③ 과학기술정보통신부장관은 정보보호에 필요한 정책과 기술을 연구·개발하기 위하여 정보보호 연구기관을 설립하거나, 다른 법령에 따라 설립된 기관 또는 기관 부설연구소를 관계 중앙행정기관의 장과 협의하여 정보보호 연구기관으로 지정할 수 있다.

④ 정보보호 기술의 연구·개발에 관한 절차와 방법 등 세부적인 사항은 대통령령으로 정한다.

제44조(인력양성 및 교육홍보) 정부는 정보보호의 기반 조성에 필요한 기술인력을 양성하고 국민의 인식제고를 위하여 다음 각호의 시책을 강구하여야 한다.

1. 정보보호 관련 전문 기술인력의 확보 및 양성

2. 정보보호 교육프로그램의 개발 및 투자

3. 그 밖에 전문인력 양성, 교육 및 홍보 등에 관하여 필요한 사항

제45조(국제협력) ①정부는 정보보호에 관한 국제적 동향을 파악하고 국제협력을 추진하여야 한다.

②정부는 정보보호에 관한 국제협력을 촉진하기 위하여 관련기술 및 인력의 국제교류와 국제표준화 및 국제공동연구개발 등에 관한 사업을 지원할 수 있다.

제46조(비밀 엄수의 의무) 정보보호에 관한 업무에 종사하고 있거나 종사하였던 사람은 직무상 알게 된 비밀을 누설하거나 직무상 목적 외의 용도에 이용해서는 아니 된다. 다만, 다른 법률에 특별한 규정이 있는 경우에는 그러하지 아니하다.

제8장 벌칙

제47조(벌칙) ①제42조의 규정을 위반하여 주요정보통신기반시설을 교란·마비 또는 파괴한 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다.

②제1항의 미수범은 처벌한다.

제48조(벌칙) 제42조제3호를 위반하여 악성프로그램을 전달 또는 유포하는 자는 7년 이하의 징역 또는 7천만원 이하의 벌금에 처한다.

제49조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

1. 제39조제5항을 위반하여 위험정보를 정보보호에 필요한 업무 외의 용도에 영리 또는 부정한 목적을 위하여 사용하거나 관리한 자
2. 제46조를 위반하여 직무상 알게 된 비밀을 누설하거나 직무상 목적 외의 용도에 이용한 자
3. 제42조제1호을 위반하여 정보통신망에 침입한 자
4. 제42조제4호을 위반하여 정보통신망에 장애가 발생하게 한 자
5. 제20조를 위반하여 타인의 정보를 훼손하거나 타인의 비밀을 침해・도용 또는 누설한 자

② 제1항제3호의 미수범은 처벌한다.

제50조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.

1. 제37조제3항에 따른 명령을 위반하여 관련 자료를 보전하지 아니한 자

제51조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.

1. 제12조제1항을 위반하여 정보보호 최고책임자의 지정을 신고하지 아니한 자

2. 제15조제2항을 위반하여 정보보호 관리체계 인증을 받지 아니한 자

② 다음 각 호의 어느 하나에 해당하는 자에게는 1천만원 이하의 과태료를 부과한다.

1. 제8조제6항을 위반하여 한국정보보호진흥원의 명칭을 사용한 자

2. 제15조제9항을 위반하여 인증받은 내용을 거짓으로 홍보한 자

3. 제17조제3항을 위반하여 소프트웨어 사용자에게 알리지 아니한 자

4. 제34조에 따른 보호조치 명령을 위반한 자

5. 제36조제2항을 위반하여 침해사고의 신고를 하지 아니한 자

6. 제37조제4항에 따른 사업장 출입 및 조사를 방해하거나 거부 또는 기피한 자

7. 제40조제3항에 따른 시정명령을 이행하지 아니한 자

③ 제1항 및 제 2항의 규정에 의한 과태료는 대통령령이 정하는 바에 따라 관계중앙행정기관의 장 또는 과학기술정보통신부장관이 부과·징수한다.

참고 문헌

<단행본>

- 양천수, 심우민, 전현욱, 김중길. <디지털 트랜스포메이션과 정보보호>. 박영사. 2019

<논문/보고서>

- 이은우, 오병일, 장여경. 국가정보원과 국내 사이버 보안 정책 개혁 방안. 정보인권연구소 연구보고서. 2016.
- 황성기, 사이버 안보 관련 법제의 문제점과 개선방향, 경제규제와 법 제12권 제1호 (통권 제23호). 2019.5
- 김상배, 세계 주요국의 사이버 안보 전략: 비교 국가전략론의 시각, 국제. 지역연구 26권 3호 2017 가을, 2017.
- ENISA, NCSS Good Practice Guide, 2016.
- ENISA, Stocktaking, Analysis and Recommendations on the Protection of CIIs, 2016.1
- Frederick Wamala, THE ITU NATIONAL CYBERSECURITY STRATEGY GUIDE, 2011.9
- ITU, GUIDE TO DEVELOPING A NATIONAL CYBERSECURITY STRATEGY – STRATEGIC ENGAGEMENT IN CYBERSECURITY, 2018.

발행일 : 2019년 11월

연구기관 : 사단법인 정보인권연구소

서울시 서대문구 독립문로 8길 23 3층

02) 701-7687, idr.sec@gmail.com

홈페이지 : http://idr.jinbo.net