국가사이버안보법안

의 안 번 호	4955

제출연월일 : 2017. 1. 3.
제 출 자 : 정 부

제안이유

공공 및 민간 영역의 구분이 없이 광범위하게 발생하는 사이버공격으로 인하여 막대한 경제적 피해와 사회 혼란이 유발되고 있는바, 국가안보를 위협하는 사이버공격을 신속히 차단하고 피해를 최소화하기 위하여 국가사이버안보위원회를 설치하고, 국가기관·지방자치단체 및 국가적으로 중요한 기술을 보유·관리하는 기관 등을 책임기관으로 하여 소관 사이버공간 보호책임을 부여하며, 사이버위협정보의 공유와 사이버공격의 탐지·대응 및 사이버공격으로 인한 사고의 통보·조사 절차를 정하는 등 국가사이버안보를 위한 조직 및 운영에 관한 사항을 체계적으로 정립하려는 것임.

주요내용

가. 사이버안보 추진기구

1) 국가사이버안보위원회의 설치(안 제5조)

사이버안보와 관련된 국가의 정책 및 전략 수립에 관한 사항 등을 심

의하기 위하여 대통령 소속으로 국가사이버안보위원회를 두되, 위원회는 위원장을 포함하여 20명 이내의 위원으로 구성하고, 위원장은 국가안보실장으로, 위원은 국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관 및 중앙행정기관의 차관급 공무원 중 대통령령으로 정하는 사람과 사이버안보에 관하여 전문적인 지식과 경험을 갖춘 사람 중에서 국가안보실장이 임명하거나 위촉하도록 함.

2) 책임기관 및 지원기관(안 제6조 및 제7조)

국가기관·지방자치단체 및 국가적으로 중요한 기술을 보유·관리하는 기관 등은 책임기관으로서 소관 사이버공간을 안전하게 보호하는 책임을 지도록 하고, 국가정보원장은 책임기관을 지원하기 위한 기술적 역량이 있는 기관 또는 단체를 지원기관으로 지정할 수 있도록 함.

나. 사이버안보를 위한 예방활동

1) 사이버안보 기본계획 및 시행계획의 수립(안 제10조)

국가정보원장은 사이버안보 업무를 체계적으로 추진하기 위하여 3년마다 사이버안보의 정책목표와 추진방향 등을 포함한 사이버안보 기본계획을 수립·시행하고, 중앙행정기관 및 시·도 등은 기본계획에 따라 소관 분야의 시행계획을 매년 수립·시행하도록 함.

2) 사이버안보 실태의 평가(안 제11조)

국가정보원장은 중앙행정기관 등을 대상으로 사이버안보를 위한 업

무수행체계 구축, 예방 및 대응활동 등에 관한 실태를 평가할 수 있도록 하고, 중앙행정기관 등의 장은 실태평가 결과에 따라 자체 시정조치를 하거나 예산·인사 등에 연계·반영하는 등 활용할 수 있도록 함.

3) 사이버위협정보의 공유(안 제12조)

사이버위협정보의 공유를 위하여 국가정보원장 소속으로 사이버위협정보공유센터를 두고, 책임기관의 장은 소관 사이버위협정보를 사이버위협정보 공유센터의 장에게 제공하도록 하며, 사이버위협정보 공유센터의 장은 위협정보를 공유하는 경우 국민의 권리가 침해되지 아니하도록 기술적·관리적 및 물리적 보호조치를 마련하도록 함.

다. 사이버안보를 위한 대응활동

1) 사이버공격의 탐지 등(안 제14조)

책임기관의 장은 사이버공격을 탐지·분석하여 즉시 대응할 수 있는 보안관제센터를 구축하거나, 다른 책임기관의 보안관제센터에 그 업무를 위탁할 수 있도록 함.

2) 사이버공격으로 인한 사고의 통보 및 조사(안 제15조)

책임기관의 장은 사이버공격으로 인한 사고가 발생할 경우 상급 책임기관의 장에게 통보하도록 하고, 해당 상급 책임기관의 장은 사이버공격으로 인한 사고의 피해 확인, 원인 분석, 재발 방지를 위한 조사를 실시하도록 하되, 국가안보를 위협하는 사이버공격으로 인한 사고의 경우에는 국가정보원장이 이를 조사하도록 함.

3) 사이버위기경보의 발령 및 사이버위기대책본부의 구성(안 제16조 및 제17조)

국가정보원장은 사이버공격에 대한 체계적인 대응을 위하여 단계별 사이버위기경보를 발령하도록 하고, 중앙행정기관 및 시·도 등 상급 책임기관의 장은 일정 단계 이상의 경보가 발령되거나 사이버공격으로 인하여 그 피해가 심각하다고 판단하는 경우에는 책임기관, 지원기관 및 수사기관이 참여하는 사이버위기대책본부를 구성·운영할 수 있도록 함.

법률 제 호

국가사이버안보법안

제1장 총칙

제1조(목적) 이 법은 국가안보를 위협하는 사이버공격을 예방하고, 사이버위기에 신속하고 적극적으로 대처함으로써 국가의 안전 보장 및 국민의 이익 보호에 이바지함을 목적으로 한다.

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. “사이버공간”이란 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1호에 따른 정보통신망(이하 “정보통신망”이라 한다)의 정보 처리 영역을 말한다.
2. “사이버공격”이란 해킹, 컴퓨터 바이러스, 서비스 거부 등 전자적 방법으로 사이버공간을 불법침입·교란·마비·파괴하거나 정보를 빼내거나 훼손하는 등의 공격 행위를 말한다.
3. “국가안보위협 사이버공격”이란 다음 각 목의 어느 하나에 해당하는 사이버공격을 말한다.

가. 군사분계선 이북지역에 기반을 두고 있는 반국가단체의 구성원 또는 그 지령을 받은 자가 하는 사이버공격

나. 에너지·통신·교통·금융 등 국가기반체계 또는 전자정부를

운영하는 데 사용되는 사이버공간 등 국가적 사이버공간을 불법 침입·교란·마비·파괴하는 사이버공격

다. 국가기밀, 군사기밀 또는 국가핵심기술 등 국가적으로 중요한 정보를 빼내거나 훼손하는 사이버공격

4. “사이버안보”란 사이버공격으로부터 사이버공간을 보호함으로써 사이버공간의 기능을 정상적으로 유지하거나 정보의 안전성을 유지하여 국가의 안전을 보장하고 국민의 이익을 보호하는 것을 말한다.

제3조(국가 등의 책무) ① 국가와 지방자치단체는 사이버공격으로부터 사이버공간을 보호하기 위하여 노력함과 동시에 사이버공간에서 정보의 자유로운 소통과 표현의 자유 등 국민의 기본권을 보장하는 정책을 균형있게 시행하여야 한다.

② 국가·지방자치단체 및 기업은 사이버안보가 국가안보에서 차지하는 중요성을 인식하고 서로 긴밀히 협력하여 사이버공간을 보호하도록 노력하여야 한다.

③ 국가와 지방자치단체는 외국 및 국제기구·단체와의 적극적인 협력관계를 구축하여 국가적 사이버공간의 안전성과 신뢰성 확보를 위하여 노력하여야 한다.

제4조(다른 법률과의 관계) 사이버안보에 관하여는 다른 법률에 우선하여 이 법을 적용한다.

제2장 사이버안보 추진기구

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

1. 사이버안보에 관한 국가의 정책 및 전략 수립
2. 사이버안보에 관련된 제도 및 법령의 개선에 관한 사항
3. 제7조에 따른 지원기관의 지정 및 취소
4. 제10조에 따른 사이버안보 기본계획 등 중요 중장기 대책
5. 그 밖에 사이버안보에 관한 중요한 사항으로서 위원회의 위원장이 필요하다고 인정하는 사항

② 위원회는 위원장을 포함하여 20명 이내의 위원으로 구성한다.

③ 위원회의 위원장은 국가안보실장이 되고, 위원은 다음 각 호의 사람 중에서 국가안보실장이 임명하거나 위촉한다.

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. 사이버안보에 관하여 전문적인 지식과 경험을 갖춘 사람

④ 위원회는 직무수행을 위하여 필요할 때에는 제6조제1항에 따른 책임기관(같은 항 제1호의 책임기관은 제외한다)과 제7조제1항에 따른 지원기관에 대하여 필요한 자료의 제출을 요청할 수 있다. 이 경우 요

청을 받은 기관의 장은 특별한 사정이 없으면 요청에 따라야 한다.

⑤ 위원회에 상정할 안건을 미리 검토하고 위원회가 위임한 안건을 심의하기 위하여 위원회에 국가 사이버안보 실무위원회(이하 “실무위원회”라 한다)를 둔다.

⑥ 실무위원회의 위원장은 국가안보실과 국가정보원의 공무원 중에서 소속 기관의 장이 지명하는 사람이 공동으로 된다.

⑦ 위원회와 실무위원회의 구성·운영 등에 필요한 사항은 대통령령으로 정한다.

제6조(책임기관) ① 다음 각 호의 기관의 장은 이 법에 따라 소관 사이버공간을 안전하게 보호하는 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

7. 「정보통신기반 보호법」 제8조에 따라 지정된 주요정보통신기반시설을 관리하는 기관

8. 「산업기술의 유출방지 및 보호에 관한 법률 」 제9조에 따라 지정된 국가핵심기술을 보유·관리하는 기관

9. 「방위사업법」 제3조제9호에 따른 방위산업체 및 같은 조 제10호에 따른 전문연구기관

10. 「방위산업기술 보호법」 제2조제1호에 따른 방위산업기술을 보유한 기관

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 사이버공격으로부터 소관 사이버공간을 보호하기 위하여 전담조직을 설치하고, 관련 예산을 확보하여야 한다.

③ 국가와 지방자치단체는 책임기관의 장이 사이버안보 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.

제7조(지원기관) ① 다음 각 호의 기관 또는 단체는 책임기관의 장이 요청하는 경우 대통령령으로 정하는 바에 따라 책임기관에 사이버공간의보호를 지원하기 위한 기술적 지원을 할 수 있다.

1. 「과학기술분야 정부출연연구기관 등의 설립·운영 및 육성에 관한

법률」 제8조에 따라 설립된 한국전자통신연구원의 국가보안기술 연구·개발을 전담하는 부설연구소

2. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조에 따른 한국인터넷진흥원

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. 제8조에 따른 사이버안보 전문기업

10. 제2항에 따라 지원기관으로 지정된 기관

② 국가정보원장은 사이버공간을 보호하기 위하여 필요한 기술적 지원의 역량이 있는 것으로 인정되는 기관 또는 단체를 위원회의 심의를 거쳐 제1항에 따라 사이버공간의 보호를 지원하는 기관(이하 “지원기관”이라 한다)으로 지정할 수 있다.

③ 제1항에 따른 기술적 지원의 범위는 다음 각 호와 같다.

1. 제14조에 따른 사이버공격의 탐지 및 대응

2. 제15조에 따른 사이버공격으로 인한 사고의 조사

3. 제16조제3항에 따른 피해발생의 최소화 및 피해복구를 위한 조치

4. 제17조에 따른 사이버위기대책본부가 하는 원인 분석 등의 조치

5. 그 밖에 사이버안보를 위하여 대통령령으로 정하는 사항

④ 국가정보원장은 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 국가정보원장에게 요청할 수 있다.

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

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

제8조(사이버안보 전문기업) ① 미래창조과학부장관은 사이버공간을 보호하기 위하여 다음 각 호의 기관 또는 단체를 사이버안보 전문기업(이하 “전문기업”이라 한다)으로 지정·관리할 수 있다.

1. 「정보보호산업의 진흥에 관한 법률」 제23조에 따라 지정된 정보보호 전문서비스 기업

2. 사이버공간의 보호와 관련된 시설·인력 및 실적 등 기술적 지원 역량에 관하여 대통령령으로 정하는 기준에 맞는 기관 또는 단체

② 미래창조과학부장관은 전문기업이 다음 각 호의 어느 하나에 해당

하는 경우에는 전문기업의 지정을 취소하거나 3개월 이내의 기간을 정하여 지원기관으로서의 업무의 전부 또는 일부의 정지를 명할 수 있다. 다만, 제1호의 경우에는 지정을 취소하여야 한다.

1. 속임수나 그 밖의 부정한 방법으로 지정된 경우
2. 제1항에 따른 지정 기준에 맞지 아니한 경우
3. 사이버안보에 관한 업무 기록 및 자료를 안전하게 보존하지 아니한 경우

③ 전문기업의 지정·관리에 필요한 사항은 대통령령으로 정한다.

제9조(사이버안보 연구기관) ① 국가정보원장은 사이버안보에 필요한 정책과 기술을 연구·개발하기 위하여 사이버안보 연구기관을 설립하거나, 다른 법령에 따라 설립된 기관 또는 기관 부설연구소를 관계 중앙행정기관의 장과 협의하여 사이버안보 연구기관으로 지정할 수 있다.

② 사이버안보 정책·기술의 연구·개발에 관한 절차와 방법 등 세부적인 사항은 대통령령으로 정한다.

제3장 사이버안보를 위한 예방활동

제10조(사이버안보 기본계획의 수립 등) ① 국가정보원장은 사이버안보 업무를 효율적이고 체계적으로 추진하기 위하여 3년마다 위원회의 심의를 거쳐 다음 각 호의 사항이 포함된 사이버안보 기본계획(이하 “기

본계획”이라 한다)을 수립·시행하여야 한다.

1. 사이버안보의 정책 목표와 추진방향

2. 사이버안보와 관련된 제도 및 법령의 개선

3. 사이버공격의 예방 및 대응

4. 사이버안보 정책·기술의 연구·개발

5. 사이버안보 관련 교육 및 훈련

6. 그 밖에 대통령령으로 정하는 사이버안보를 위하여 필요한 사항

② 상급책임기관의 장은 기본계획에 따라 사이버안보 시행계획(이하 “시행계획”이라 한다)을 매년 작성하여 관할 책임기관의 장에게 통보하여야 한다.

③ 기본계획과 시행계획의 작성 방법·절차 및 세부 내용 등에 관하여 필요한 사항은 대통령령으로 정한다.

제11조(사이버안보 실태평가) ① 국가정보원장은 제6조제1항제2호부터 제6호까지의 책임기관 중에서 대통령령으로 정하는 책임기관을 대상으로 사이버안보를 위한 업무수행체계 구축, 사이버공격 예방 및 대응 활동 등에 관한 실태평가(이하 “실태평가”라 한다)를 할 수 있다.

② 국가정보원장은 실태평가를 하거나 실태평가에 관한 전문적·기술적인 연구 또는 자문을 위하여 사이버안보실태 합동평가단을 구성·운영할 수 있다.

③ 국가정보원장은 실태평가의 결과를 평가를 받은 책임기관의 장에게 통보하여야 한다.

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

⑤ 실태평가의 절차와 방법, 결과의 처리 및 사이버안보실태 합동평가단의 구성·운영 등에 필요한 사항은 대통령령으로 정한다.

제12조(사이버위협정보의 공유) ① 다음 각 호의 정보를 공유하기 위하여 국가정보원장 소속으로 사이버위협정보 공유센터를 둔다.

1. 사이버공격 방법에 관한 정보

2. 악성프로그램 및 이와 관련된 정보

3. 정보통신망, 정보통신기기 및 소프트웨어의 보안상 취약점에 관한 정보

4. 그 밖에 사이버공격의 예방을 위한 정보

② 책임기관의 장은 소관 사이버공간의 제1항에 따른 정보(이하 “위협정보”라 한다)가 다른 책임기관의 사이버안보를 위하여 필요하다고 인정하는 경우 대통령령으로 정하는 바에 따라 소관 사이버공간의 위협정보를 제1항에 따른 사이버위협정보 공유센터(이하 “공유센터”라 한다)의 장에게 제공할 수 있다. 이 경우 공유센터의 장은 사이버안보를 위하여 위협정보의 공유가 필요하다고 판단되는 책임기관의 장에게 위협정보를 제공하여야 한다.

③ 누구든지 제2항에 따라 공유된 위협정보를 사용할 때에는 사이버안보 목적에 필요한 최소한의 범위에서 사용·관리하여야 한다.

④ 공유센터의 장은 위협정보를 공유하는 경우 국민의 권리가 침해되지 아니하도록 기술적·관리적 또는 물리적 보호조치를 마련하여야 한다.

⑤ 공유센터의 장은 제4항에 따른 기술적·관리적 또는 물리적 보호조치에 관한 사항을 심의하기 위하여 책임기관 및 민간 전문가 등이 참여하는 사이버위협정보 공유협의회를 구성·운영하여야 한다.

⑥ 제1항부터 제5항까지의 규정에 따른 공유센터의 설치·운영, 공유센터의 장에게 제공하는 위협정보의 범위 등에 필요한 사항은 대통령령으로 정한다.

제13조(사이버위기 대응 훈련) ① 상급책임기관의 장은 사이버위기(사이버공격으로 인하여 사이버공간의 기능 및 정보의 안전성을 위협하는 상황을 말한다. 이하 같다)에 효율적으로 대응하기 위하여 소관 사이버공간을 대상으로 사이버위기 대응 훈련을 정기적으로 실시하여야 한다.

② 국가정보원장은 사이버위기 발생에 대비하여 책임기관의 사이버공간을 대상으로 사이버위기 대응 통합훈련을 실시할 수 있다. 이 경우 국가정보원장은 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 비상대비훈련과 함께 실시할 수 있다.

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

제4장 사이버안보를 위한 대응활동

제14조(사이버공격의 탐지 등) ① 국가정보원장은 국가적 사이버공간에 대한 사이버공격에 신속하고 효율적으로 대응하기 위하여 관계 중앙행정기관의 장과 협의하여 국가 차원의 사이버공격 탐지・대응체계를 구축・운영하여야 한다.

② 책임기관의 장은 제1항에 따른 국가 차원의 사이버공격 탐지・대응체계를 위하여 대통령령으로 정하는 바에 따라 소관 사이버공간에서 발생하는 사이버공격을 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 사이버공격 탐지・대응에 필요한 범위에서 「개인정보 보호법」 제2조제1호에 따른 개인정보를 수집・이용할 수 있다.

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

제15조(사이버공격으로 인한 사고의 통보 및 조사) ① 국가정보원장은 책임기관의 사이버공간에서 사이버공격으로 인한 사고가 발생하는 경

우에 대비하여 국가 차원의 일원화된 통보 및 조사 체계를 구축·운영하여야 한다.

② 책임기관의 장은 소관 사이버공간에서 사이버공격으로 인한 사고가 발생한 경우에는 피해를 최소화하는 조치를 하고, 그 사실을 다음 각 호의 구분에 따른 사람에게 통보하여야 한다. 이 경우 국가안보위협 사이버공격에 관한 사항은 국가정보원장에게 함께 통보하여야 한다.

1. 상급책임기관: 국가정보원장. 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

③ 상급책임기관의 장은 제2항제2호부터 제4호까지의 통보(국가안보위협 사이버공격에 관한 통보는 제외한다)를 받은 경우 신속히 사이버공격으로 인한 사고의 그 피해 확인, 원인 분석 및 재발 방지를 위한 조사를 하여야 한다. 이 경우 해당 기관의 장은 필요하면 지원기관의 장에게 기술적 지원을 요청할 수 있다.

④ 국가정보원장은 다음 각 호의 경우(제6조제1항제1호에 따른 책임기관 소관 사이버공간에서 사이버공격으로 인한 사고가 발생한 경우에 대해서는 해당 기관의 장이 요청하는 경우로 한정한다)에는 지체 없이 사이버공격으로 인한 사고의 피해 확인, 원인 분석 및 재발 방지를 위한 조사를 하여야 한다. 이 경우 민간 분야 책임기관을 대상으로 사고 조사를 할 때에는 대통령령으로 정하는 바에 따라 관계 중앙행정기관, 수사기관 및 지원기관으로 구성된 합동조사팀을 운영하여야 한다.

1. 제2항 각 호 외의 부분 후단에 따라 국가안보위협 사이버공격에 관한 통보를 받은 경우
2. 제2항제1호에 따른 통보를 받은 경우
3. 국가안보위협 사이버공격으로 인한 사고가 발생하였으나 제2항 각 호 외의 부분 후단에 따른 통보를 받지 못한 경우

⑤ 제6조제1항제1호의 책임기관은 소관 사이버공간에서 사이버공격으로 인한 사고가 발생한 경우로서 국가정보원장에게 제4항 각 호 외의 부분 전단에 따른 조사 요청을 하지 아니하는 경우에는 직접 그 조사를 하여야 한다.

⑥ 누구든지 제3항부터 제5항까지의 규정에 따른 조사에 협조하여야 하며, 그 조사를 완료하기 전에 사이버공격과 관련된 자료를 임의로 삭제·훼손하거나 변조해서는 아니 된다.

⑦ 상급책임기관의 장과 국가정보원장은 제3항부터 제5항까지의 규정

에 따라 조사를 하는 과정에서 사이버공격과 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.

제16조(사이버위기경보의 발령 및 조치) ① 국가정보원장은 사이버공격에 국가 차원에서 체계적으로 대응하기 위하여 단계별 국가사이버위기경보(이하 “경보”라 한다)를 발령할 수 있다. 이 경우 국가정보원장은 경보의 발령 시점과 단계 등에 관하여 국가안보실장과 미리 협의하여야 한다.

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

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

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

제17조(사이버위기대책본부의 구성·운영) ① 상급책임기관의 장은 관할 사이버공간이 다음 각 호의 어느 하나에 해당하는 경우에는 사이버

공격에 대한 원인 분석, 사고 조사, 긴급 대응, 피해 복구 등의 신속한 조치를 하기 위하여 책임기관, 지원기관 및 수사기관이 참여하는 사이버위기대책본부(이하 “대책본부”라 한다)를 구성·운영할 수 있다. 다만, 2개 이상의 상급책임기관에 대책본부를 구성하여야 하는 경우에는 이를 갈음하여 국가정보원장이 관련 상급책임기관의 장과 협의하여 대책본부를 구성·운영할 수 있다.

1. 대통령령으로 정하는 단계 이상의 경보 또는 분야별 경보가 발령된 경우
2. 사이버공격으로 인하여 그 피해가 심각하다고 판단하는 경우

② 대책본부의 장은 대책본부를 설치하는 기관의 장이 국가안보실장과 협의하여 정한다.

③ 대책본부의 장은 대책본부의 구성·운영을 위하여 필요한 경우 책임기관과 지원기관의 장에게 인력 파견 또는 장비 제공을 요청할 수 있다.

④ 제1항부터 제3항까지의 규정에 따른 대책본부의 구성·운영 등에 필요한 구체적인 사항은 대통령령으로 정한다.

제5장 보칙

제18조(비밀 엄수의 의무) 사이버안보에 관한 업무에 종사하고 있거나 종사하였던 사람은 직무상 알게 된 비밀을 누설하거나 직무상 목적 외

의 용도에 이용해서는 아니 된다.

제19조(포상 등) ① 국가정보원장은 다음 각 호의 어느 하나에 해당하는 자에게 포상하고, 예산의 범위에서 포상금을 지급할 수 있다.

1. 위협정보 제공에 기여한 자

2. 사이버공격 기도(企圖)에 관한 정보를 제공한 자

3. 사이버공격을 가한 자를 신고한 자

4. 사이버공격의 탐지 및 대응·복구에 기여한 자

5. 사이버공격의 예방 및 탐지·대응·복구에 필요한 신기술을 개발한 자

② 제1항에 따른 포상과 포상금 지급의 기준·방법과 절차, 지급액 등은 대통령령으로 정한다.

제20조(국방 분야에 대한 특례) ① 전시(戰時)의 경우 이 법에 따른 사이버안보에 관한 업무는 군사작전을 지원하기 위하여 수행되어야 한다.

② 제6조제1항제4호에 따른 책임기관에 대한 다음 각 호의 업무는 제11조 및 제15조제4항에도 불구하고 국방부장관이 수행한다.

1. 제11조에 따른 사이버안보 실태평가

2. 제15조제4항에 따른 사이버공격으로 인한 사고의 조사

③ 제16조제2항에 따라 국방부장관이 제6조제1항제4호에 따른 책임기관에 관한 분야별 경보를 발령하는 경우에는 같은 항 후단을 적용하지 아니한다.

④ 국방부장관은 제2항 또는 제3항에 따른 업무를 수행함에 있어 국가

안보에 필요하다고 판단되거나 국가정보원장의 요청이 있는 경우에는 관련 내용을 국가정보원장에게 통보하여야 한다.

제21조(개인정보 처리 등) 사이버안보를 위하여 처리되는 개인정보는 「개인정보 보호법」 제58조제1항에 따라 같은 법이 적용되지 아니하는 개인정보로 본다. 다만, 사이버안보를 위하여 개인정보를 처리하는 경우 개인정보 처리 기준 및 필요한 조치 마련 등에 관하여는 같은 법 제58조제4항을 준용한다.

제6장 벌칙

제22조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

1. 제12조제3항을 위반하여 위협정보를 사이버안보에 필요한 업무 외의 용도에 영리 또는 부정한 목적을 위하여 사용하거나 관리한 자
2. 제15조제6항을 위반하여 조사를 방해할 목적으로 사이버공격과 관련된 자료를 삭제·훼손하거나 변조한 자
3. 제18조를 위반하여 직무상 알게 된 비밀을 누설하거나 직무상 목적 외의 용도에 이용한 자

제23조(과태료) ① 제15조제2항을 위반하여 사이버공격으로 인한 사고를 통보하지 아니한 자(제6조제1항제1호부터 제6호까지의 책임기관의 장은 제외한다)에게는 1천만원 이하의 과태료를 부과한다.

② 제1항에 따른 과태료는 대통령령으로 정하는 바에 따라 해당 기관을 관리·감독하는 상급책임기관의 장이 부과·징수한다.

부 칙

제1조(시행일) 이 법은 공포 후 6개월이 경과한 날부터 시행한다.

제2조(최초 기본계획 수립 시기 등에 관한 특례) 국가정보원장은 제10조에도 불구하고 이 법 시행일부터 3개월 이내에 기본계획을 수립·시행하여야 한다. 이 경우 최초로 수립하는 기본계획의 기간은 이 법 시행일이 속하는 연도와 그 다음 연도부터 3년까지로 한다.

국가사이버안보법 제정안 비용추계서 미첨부사유서

1. 재정수반요인

가. 상급책임기관의 사이버안보 전담조직 설치(안 제6조제2항)

상급책임기관의 장은 사이버공격으로부터 소관 영역의 사이버공간을 보호하기 위한 전담조직을 설치하고 관련 예산을 확보하도록 규정함에 따라 재정소요가 예상된다.

나. 지원기관의 기술적 지원비용 보전(안 제7조제7항)

국가정보원장은 관계 중앙행정기관의 장은 지원기관의 기술적 지원에 소요되는 비용의 전부 또는 일부를 지원기관에게 지원할 수 있다고 규정함에 따라 재정소요가 예상된다.

다. 사이버안보 연구기관의 설립(안 제9조제1항)

국가정보원장은 사이버안보에 필요한 정책과 기술을 연구·개발하기 위하여 사이버안보 연구기관을 설립하거나, 다른 법령에 따라 설립된 기관 또는 기관 부설연구소를 관계 중앙행정기관의 장과 협의하여 사이버안보 연구기관으로 지정할 수 있도록 규정함에 따라 재정소요가 예상된다.

라. 사이버위협정보공유센터의 설치(안 제12조제1항 및 제5항)

사이버위협정보의 공유를 위하여 국가정보원장 소속으로 사이버위협정보공유센터를 두도록 규정하고 책임기관·민간전문가들로 구성되는 사이버위협정보 공유협의회를 구성·운영함에 따라 재정소요가 예상된

다.

마. 책임기관의 보안관제센터 설치(안 제14조 제1항 및 제2항)

국가정보원장은 국가적 사이버공간에 대한 사이버공격에 신속하고 효율적으로 대응하기 위하여 관계 중앙행정기관의 장과 협의하여 국가 차원의 사이버공격 탐지·대응체계를 구축·운영하여야 하며, 책임기관의 장은 대통령령이 정하는 바에 따라 소관 사이버공간에 대한 사이버공격을 탐지·분석하여 즉시 대응 조치를 할 수 있는 기구(이하 “보안관제센터”라 한다)를 구축·운영하거나 다른 책임기관의 장이 구축·운영하는 보안관제센터에 그 업무를 위탁하는 등의 조치를 취하도록 규정함에 따라 재정소요가 예상된다.

바. 합동조사팀 및 사이버위기대책본부의 구성(안 제15조제4항 및 제17조제1항)

국가정보원장은 민간 분야 책임기관을 대상으로 사고 조사를 할 때에는 대통령령으로 정하는 바에 따라 관계 중앙행정기관, 수사기관 및 지원기관으로 구성된 합동조사팀을 운영하도록 규정하고 있고, 상급책임기관의 장 또는 국가정보원장은 대통령령으로 정하는 단계 이상의 사이버위기경보가 발령된 경우 또는 사이버공격으로 인하여 그 피해가 심각하다고 판단하는 경우, 사이버공격에 대한 원인 분석, 사고 조사, 긴급대응, 피해 복구 등의 신속한 조치를 하기 위하여 책임기관, 지원기관 및 수사기관이 참여하는 사이버위기대책본부를 구성·운영토록 규정함에 따라 재정소요가 예상된다.

사. 포상(안 제19조)

국가정보원장은 사이버공격 기도에 관한 정보를 제공한 자 등에게 포상하고, 예산의 범위에서 포상금을 지급할 수 있도록 규정함에 따라 재정소요가 예상된다.

2. 미첨부 근거 규정

「의안의 비용추계에 관한 규칙」 제3조제1항 단서 중 제2호(비용추계의 대상이 국가안전보장·군사기밀에 관한 사항인 경우) 및 제3호(의안의 내용이 선언적, 권고적인 형식으로 규정되는 등 기술적으로 추계가 어려운 경우)에 해당한다.

3. 미첨부 사유

제정안에 따라 재정소요가 발생할 것으로 예상되는 부분 중 제정안 제6조제2항 상급 책임기관의 사이버안보 전담조직의 설치와 관련하여서는 현재 「국가사이버안전관리규정(이하 “안전관리규정”이라 한다)」[1] 제4조 및 제17조에 의하여 중앙행정기관의 장은 소관 정보통신망에 대하여 사이버안전업무를 전담하는 전문인력을 확보하는 등 필요한 조치를 강구하여야 하고, 소관분야와 관련된 사이버안전대책 수립·시행에 필요한 재정상의 조치를 강구토록 되어 있어 중앙행정기관의 전문인력을 활용하여 사이버안보 전담조직을 편성할 수 있을 것으로 보이므로, 추가 재정소요는 경미할 것으로 보인다.

1) 대통령훈령 제316호, 2013. 9. 2. 일부개정

제정안 제12조제1항의 사이버위협정보공유센터는 안전관리규정 제10조에 따라 국가정보원장이 중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장 등과 사이버공격에 관련한 정보의 협력을 위해 실무적으로 旣 구축하여 운영중인 국가사이버위협정보공유시스템을 그대로 활용할 것이 예상됨에 따라 추가 재정소요는 극히 미미할 것으로 보인다.

제정안 제14조제2항의 책임기관의 보안관제센터 등의 설치와 관련해서는 현재 안전관리규정 제10조의2에 의거하여 중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장은 보안관제센터를 이미 설치·운영하고 있으며, 그 현황은 [표 1]과 같다. 따라서 이로 인한 추가 재정소요는 없거나 미미할 것으로 추정된다.

[표 1] 중앙행정기관 보안관제센터 운영 현황 (2016년 기준)

부문	담당기관	관제센터
행정	행정자치부	정부통합전산센터(대전)
		정부통합전산센터(광주)
		사이버침해대응센터(G-CERT)
국방	국방부	사이버사령부
외교	외교부	외교 사이버안전센터
국토교통	국토교통부	국토교통 사이버안전센터
보건·의료	보건복지부	보건의료 사이버안전센터
교육	교육부	교육 사이버안전센터
에너지	산업통상자원부	산업통상 사이버안전센터
통신・과학기술	미래창조과학부	미래창조과학 사이버안전센터
		KISA 인터넷침해대응센터
		과학기술 정보보호센터
금융	금융위원회	금융ISAC(금융결제원)・
		금융ISAC(KOSCOM)
치안	경찰청	경찰 전산보호센터
특허	특허청	특허 관제센터
관세	관세청	관세 관제센터
국세	국세청	국세 관제센터
방위산업	방위사업청	방위사업 관제센터

부문	담당기관	관제센터
재정	기획재정부	재정 관제센터
문화	문화체육관광부	문화체육관광 관제센터
기상	기상청	기상 관제센터
노동	고용노동부	노동 관제센터
환경	환경부	환경 관제센터
법무	법무부	법무 관제센터
통일	통일부	통일 관제센터
농식품	농림축산식품부	농식품부 사이버안전센터
검찰	대검찰청	대검 사이버안전센터
병무	병무청	병무청 사이버안전센터
해양	해양수산부	해양수산 사이버안전센터
중소기업	중소기업청	중기청 사이버안전센터
공정위	공정거래위원회	공정위 사이버안전센터
조달	조달청	조달청 사이버안전센터
통계	통계청	통계청 사이버안전센터
안전	국민안전처	국민안전처 사이버안전센터

제정안 제12조제5항의 사이버위협정보 공유협의회, 제15조제4항의 합동조사팀 및 제17조제1항의 사이버위기대책본부에 대해서는 안전관리규정 제8조제3항에 따라 국가정보원장이 국가 차원의 사이버위협에 대한 합동조사 등을 위하여 설치·운영할 수 있는 민·관·군 합동대응반, 그리고 안전관리규정 제13조제3항에 따라 국가정보원장이 구성·운영할 수 있는 범정부적 사이버위기 대책본부와 그 구성 및 임무가 유사하다. 따라서 현재의 민·관·군 합동대응반, 대책본부의 운영을 위한 국가정보원 등의 인력, 예산 및 사무실을 활용할 수 있으므로 추가 재정소요는 경미할 것으로 보인다.

다만, 제정안 제7조에 따라 정부는 지원기관의 기술적 지원에 소요되는 비용의 전부 또는 일부를 지원기관에게 지원할 수 있고, 그 외에도 상급 책임기관의 전담조직 및 책임기관 보안관제센터 조직의 구체적 임무

에 따라 추후 재정소요의 변화가 발생할 가능성이 있다. 또한 제정안 제9조제1항의 사이버안보 연구기관의 설립에 따라서도 추후 재정소요의 변화가 발생할 수 있다. 그러나 관련 기관・조직들의 운영 및 사업내역은 국가안전보장에 관한 사항으로서 그 재정소요 첨부가 곤란한 한계가 있다.[2)3)]

또한 제정안은 사이버테러 기도에 관한 정보를 제공한 자 등에 대하여 포상하고 예산의 범위에서 포상금을 지급할 수 있도록 규정하고 있는데, 구체적인 지급 기준・지급액 등 필요한 사항은 대통령령으로 정하도록 되어 있어 현재로서는 추가 재정소요의 발생 여부를 예상하기 어렵다.

이처럼 제정안의 재정수반요인을 검토한 결과, 국가의 안전보장 사항에 해당하여 재정소요추계의 내용 첨부가 곤란하거나 법령안의 성격상 재정소요 추계가 기술적 한계가 있어, 본 법안은 「의안의 비용추계 등에 관한 규칙」 제3조제1항 단서 중 제2호 내지 제3호에 해당되어 비용추계서를 미첨부한다.

4. 작성자

국가정보원 (성명 생략)
(02-557-0194, cyberlaw@ncsc.go.kr)

---

2) 제6조(조직 등의 비공개) 국정원의 조직·소재지 및 정원은 국가안전보장을 위하여 필요한 경우에는 그 내용을 공개하지 아니할 수 있다.

3) 「국회법」 제54조의2제1항에 따라 국가정보원 소관 예산안 및 결산 심사 시 정보위원회 회의는 공개하지 않으며, 동법 제84조제4항에서 정보위원회의 예산안 및 결산 등의 심사에 있어 일반 상임위원회와 달리 특례규정을 두어 그 심사 결과를 총액으로만 의장에게 보고하도록 하고 있다.