국가 사이버테러 방지 등에 관한 법률안
(서상기의원 대표발의)

의 안 번 호	18583

발의연월일 : 2016. 2. 22.

발 의 자 : 서상기・강석훈・김도읍
김용남・김정훈・김종태
문정림・박대동・박민식
박성호・신동우・신의진
심윤조・원유철・이명수
이상일・이재영・이종배
이철우・조원진・홍철호
황영철・황인자・황진하
의원(24인)

제안이유

과거 1・25 인터넷 대란과 같은 전국적인 규모의 국가 주요 정보통신망 마비사태 발생과 해외로부터 조직적인 사이버테러로 국가기밀 및 첨단기술의 유출 등 국가・사회 전반에 중대한 영향을 미칠 수 있는 사이버위기 발생 가능성이 날로 증대하고 있음.

특히 사이버공간은 국경을 초월하여 범지구적이면서 정부와 민간부분이 상호 밀접히 연계되어 있어 매우 복잡・고도화되며, 시공간의 제약을 벗어나 발생하는 모든 사이버공격을 정부와 민간 어느 하나도 단독으로 차단하기에는 분명한 한계가 있음.

그러나 우리나라는 아직 국가차원에서 사이버테러 방지 및 위기관리

업무를 체계적으로 수행할 수 있는 제도와 구체적 방법·절차가 정립되어 있지 않아 사이버위기 발생 시 국가안보와 국익에 중대한 위험과 막대한 손해를 끼칠 우려가 있음.

따라서 정부와 민간이 참여한 국가차원의 종합적인 대응체계를 구축하도록 하고, 이를 통하여 사이버테러를 사전에 탐지하여 사이버위기 발생 가능성을 조기에 차단하며, 위기 발생 시 국가의 역량을 결집하여 신속히 대응할 수 있도록 하고자 함.

주요내용

가. 사이버테러에 대한 국가차원의 종합적이고 체계적인 예방·대응과 사이버위기관리를 위하여 국가정보원장 소속으로 국가사이버안전센터를 둠(안 제6조).

나. 책임기관의 장은 사이버공격 정보를 탐지·분석하여 즉시 대응할 수 있는 보안관제센터를 구축·운영하거나 다른 기관이나 보안관제 전문업체가 구축·운영하는 보안관제센터에 그 업무를 위탁하여야 함(안 제8조).

다. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 장 및 중앙행정기관의 장은 사이버테러로 인해 피해가 발생한 경우에는 신속하게 사고조사를 실시하고, 중앙행정기관의 장은 그 조사결과를 미래창조과학부장관, 국가정보원장 및 금융위원장 등 관계 중앙행정기관의 장에게 통보하여야 함(안 제9조).

라. 정부는 사이버테러에 대한 체계적인 대비와 대응을 위하여 책임기관의 장의 요청과 수집된 정보를 종합·판단하여 관심·주의·경계·심각 단계의 사이버위기경보를 발령할 수 있음(안 제10조).

마. 정부는 경계단계 이상의 사이버위기경보가 발령된 경우 원인분석, 사고조사, 긴급대응, 피해복구 등의 신속한 조치를 취하기 위하여 국가 역량을 결집한 민·관·군 전문가가 참여하는 사이버위기대책본부를 구성·운영할 수 있음(안 제11조).

바. 정부는 사이버테러 기도에 관한 정보를 제공하거나 사이버테러를 가한 자를 신고한 자 등에 대하여 포상금을 지급할 수 있음(안 제13조).

사. 직무상 비밀을 누설한 경우에는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처하고, 피해의 복구 및 확산방지를 이행하지 아니한 경우에는 1천만원 이하의 과태료에 처할 수 있음(안 제14조 및 제15조).

법률 제 호

국가 사이버테러 방지 등에 관한 법률안

제1조(목적) 이 법은 국가 사이버테러 방지에 관한 기본적인 사항을 규정하여 국가안보를 위협하는 사이버테러를 예방하고 사이버위기 발생 시 국가 역량을 결집하여 신속하게 대처함으로써 국가의 안전 보장과 이익보호에 이바지함을 목적으로 한다.

제2조(정의) 이 법에서 사용하는 용어의 정의는 다음과 같다.

1. “사이버테러”란 외국이나 대한민국의 통치권이 사실상 미치지 아니하는 한반도내의 집단, 해킹·범죄조직 및 이들과 연계되거나 후원을 받는 자 등이 국가안보 또는 공공의 안전을 위태롭게 할 목적으로 해킹·컴퓨터 바이러스·서비스방해·전자기파 등 전자적 수단에 의하여 정보통신망을 공격하는 행위를 말한다.
2. “사이버안전”이란 사이버테러로부터 정보통신시설과 정보를 보호하기 위하여 수행하는 관리적·물리적·기술적 수단 및 대응조치 등을 포함한 활동으로서 사이버위기관리를 포함한다.
3. “사이버위기”란 사이버테러로 인하여 국가 기반시설의 핵심기능이 훼손·정지·무력화 또는 국가기밀과 중요정보가 대량 유출되어 국가안보에 영향을 미치거나 사회·경제적 혼란을 유발하는 상황을 말한다.

4. “사이버테러정보”란 정보시스템 및 정보보호시스템(소프트웨어를 포함한다) 등에 의해 사이버테러 행위로 판단되는 정보로서 사이버테러 근원지를 파악하기 위한 인터넷프로토콜주소(IP)와 네트워크카드주소(MAC)를 포함한다.

5. “사이버테러 방지 및 위기관리 책임기관(이하 “책임기관”이라 한다)”이란 사이버테러 방지 및 위기관리에 관한 업무를 수행하고 있는 다음 각 목의 기관을 말한다.

가. 「대한민국헌법」, 「정부조직법」, 그 밖의 법령에 따라 설치된 국가기관(그 소속·산하기관을 포함한다)과 지방자치단체(그 소속·산하기관을 포함한다) 및 「국가정보화 기본법」 제3조제10호에 따른 공공기관

나. 「정보통신기반 보호법」 제5조제1항에 따른 주요정보통신기반시설을 관리하는 기관

다. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제46조제1항에 따른 집적정보통신시설사업자 및 같은 법 제47조의4제2항에 따른 주요정보통신서비스 제공자

라. 「산업기술의 유출방지 및 보호에 관한 법률」 제9조에 따른 국가핵심기술을 보유한 기업체나 연구기관

마. 「방위사업법」 제3조제9호에 따른 방위산업체 및 같은 법 제3조제10호에 따른 전문연구기관

6. “사이버테러 방지 및 위기관리 지원기관(이하 “지원기관”이라 한

다)”이란 사이버테러에 대한 신속한 탐지·대응 및 사고조사·복구 등을 지원하는 다음 각 목의 기관 또는 업체를 말한다.

가. 「과학기술분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조에 따른 한국전자통신연구원

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

다. 「소프트웨어산업 진흥법」제24조에 따라 소프트웨어사업자로 신고한 자 중 컴퓨터바이러스 백신소프트웨어를 제작 또는 판매하는 자

라. 「국가정보화 기본법」 제3조제6호의 정보보호시스템을 제작하거나 수입하는 자

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

바. 관계 행정기관의 장이 지정한 보안관제전문업체

제3조(사이버안전관리의 책임) ① 책임기관의 장 및 이를 지휘·감독할 의무가 있는 기관의 장은 사이버안전관리에 대한 책임을 진다.

② 책임기관의 장은 소관 정보통신망에 대한 보안대책을 마련하는 등 사이버안전관리를 위해 자율보안관리 체계를 구축·운영하여야 한다.

제4조(국가사이버테러 방지 및 위기관리 기본계획 수립 등) ① 정부는 사이버테러 방지 및 위기관리 대책의 효율적이고 체계적인 추진을

위하여 국가사이버테러 방지 및 위기관리 기본계획(이하 “기본계획”이라한다)을 수립·시행하여야 한다.

② 국회, 법원, 헌법재판소, 중앙선거관리위원회의 장(국회사무총장, 법원행정처장, 헌법재판소 사무처장, 중앙선거관리위원회 사무총장을 말한다. 이하 같다) 및 중앙행정기관의 장은 제1항의 기본계획에 따라 소관 책임기관의 장이 활용할 수 있도록 국가사이버테러 방지 및 위기관리 시행계획(이하 “시행계획”이라고 한다)을 작성하여 소관 책임기관의 장에게 배포하여야 한다.

제5조(시행계획의 이행여부 확인) ① 국회, 법원, 헌법재판소, 중앙선거관리위원회의 장 및 중앙행정기관의 장은 소관 책임기관에 대하여 매년 시행계획의 이행여부를 확인하여야 한다.

② 정부는 제1항의 확인결과를 종합하여 국가사이버테러 방지 및 위기관리 실태를 점검·평가하여야 한다. 다만, 국회, 법원, 헌법재판소, 중앙선거관리위원회에 대한 점검·평가는 해당기관의 장이 요청한 경우에 한정한다.

③ 제1항 및 제2항의 절차와 방법 등에 관하여 필요한 사항은 대통령령으로 정한다.

제6조(국가사이버안전센터의 설치) ① 사이버테러에 대한 국가차원의 종합적이고 체계적인 예방·대응과 사이버위기관리를 위하여 국가정보원장 소속으로 국가사이버안전센터(이하 “안전센터”라 한다)를 둔다.

② 안전센터는 다음 각 호의 업무를 수행한다.

1. 국가사이버테러 방지 및 위기관리 정책의 수립

2. 사이버테러 관련 정보의 수집·분석·전파

3. 사이버테러로 인하여 발생한 사고의 조사 및 복구 지원

③ 국가정보원장은 제1항의 안전센터를 운영함에 있어 국가차원의 종합판단, 상황관제, 위협요인 분석, 사고 조사 등을 위해 민·관·군 합동대응팀(이하 “합동대응팀”이라 한다)을 설치·운영할 수 있다.

④ 국가정보원장은 합동대응팀을 설치·운영하기 위하여 필요한 경우에는 책임기관 및 지원기관의 장에게 인력의 파견과 장비의 지원을 요청할 수 있다.

제7조(사이버테러 방지대책의 수립·시행) ① 책임기관의 장은 소관 정보통신망과 정보 등의 안전성 및 신뢰성 확보를 위한 사이버테러 방지대책을 강구하여야 한다.

② 국가정보원장은 관계 중앙행정기관의 장과 협의하여 제1항에 따른 사이버테러 방지대책의 수립에 필요한 지침을 작성 배포할 수 있다. 다만, 국회, 법원, 헌법재판소 및 중앙선거관리위원회의 경우에는 해당 기관의 장이 필요하다고 인정하는 경우에 적용한다.

제8조(보안관제센터 등의 설치) ① 책임기관의 장은 사이버테러 정보를 탐지·분석하여 즉시 대응 조치를 할 수 있는 기구(이하 “보안관제센터”라 한다)를 구축·운영하거나 다음 각 호의 기관이 구축·운영

하는 보안관제센터에 그 업무를 위탁하여야 한다. 다만, 「정보통신기반 보호법」 제16조에 따른 정보공유·분석센터는 보안관제센터로 본다.

1. 제2조제5호가목의 기관

2. 제2조제6호바목의 보안관제전문업체

② 책임기관의 장은 제1항에 따른 사이버테러 정보와 정보통신망·소프트웨어의 취약점 등의 정보(이하 “사이버위협정보”라 한다)를 관계 중앙행정기관의 장 및 국가정보원장과 공유하여야 한다.

③ 정부는 제2항의 사이버위협정보의 효율적인 관리 및 활용을 위하여 관계기관의 장과 공동으로 사이버위협정보통합공유체계를 구축·운영할 수 있다.

④ 누구든지 제2항에 따라 공유하는 정보에 대하여는 사이버위기관리를 위하여 필요한 업무범위에 한하여 정당하게 사용 관리하여야 한다.

⑤ 제1항에 따른 보안관제센터와 제3항에 따른 사이버위협정보통합공유체계 구축·운영 및 정보 관리에 관한 사항과 제2항에 따른 사이버위협정보의 공유에 관한 범위·절차·방법 등에 관한 사항은 대통령령으로 정한다.

제9조(사고조사) ① 국회, 법원, 헌법재판소, 중앙선거관리위원회의 장 및 중앙행정기관의 장은 사이버테러로 인하여 소관분야에 피해가 발생한 경우에는 그 원인과 피해내용 등에 관하여 신속히 사고조사

를 실시하여야 한다. 또한, 중앙행정기관의 장은 그 조사결과를 미래창조과학부장관, 국가정보원장 및 금융위원장 등 관계 중앙행정기관의 장에게 통보하여야 한다.

② 제1항의 경우 피해가 중대하거나 확산될 우려가 있는 경우 중앙행정기관의 장은 즉시 미래창조과학부장관, 국가정보원장 및 금융위원장 등 대통령령으로 정하는 전문기관의 장에게 사고조사 등 기술적 지원을 요청할 수 있다. 다만, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 해당기관의 장이 필요하다고 인정하는 경우에 한한다.

③ 미래창조과학부장관, 국가정보원장 및 금융위원장 등 관계 중앙행정기관의 장은 제1항에 따라 사고조사 결과를 통보받거나 제2항에 따라 기술적 지원을 한 결과, 피해의 복구 및 확산방지를 위하여 신속한 시정이 필요하다고 판단되는 경우 책임기관의 장에게 필요한 조치를 요청할 수 있다. 이 경우 책임기관의 장은 특별한 사유가 없는 한 이에 따라야 한다.

④ 누구든지 제1항 및 제2항에 따른 사고조사를 완료하기 전에 사이버테러와 관련된 자료를 임의로 삭제·훼손·변조하여서는 아니 된다.

제10조(사이버위기경보의 발령) ① 정부는 사이버테러에 대한 체계적인 대비와 대응을 위하여 책임기관의 장의 요청과 제8조제2항에 따라 수집된 정보를 종합·판단하여 관심·주의·경계·심각 단계의 사이버위기경보를 발령할 수 있다. 이 경우 국가안보실장과 미리 협의하

여야 한다.

② 정부는 제1항의 사이버위기경보를 발령할 경우 관계기관의 장과 경보 수준을 사전 협의하여야 한다.

③ 책임기관의 장은 제1항에 따른 사이버위기경보가 발령된 경우 즉시 피해발생의 최소화 및 피해복구를 위한 조치를 취하여야 한다.

④ 사이버위기경보 발령의 주체·절차·기준 및 책임기관의 장의 조치 등에 관하여 필요한 사항은 대통령령으로 정한다.

제11조(사이버위기대책본부의 구성) ① 정부는 경계단계 이상의 사이버위기경보가 발령된 경우 원인분석, 사고조사, 긴급대응, 피해복구 등의 신속한 조치를 취하기 위하여 국가 역량을 결집한 민·관·군 전문가가 참여하는 사이버위기대책본부(이하 “대책본부”라 한다)를 구성·운영할 수 있다.

② 대책본부의 장(이하 “대책본부장”이라 한다)은 관계 중앙행정기관의 장이 국가안보실장과 협의하여 정하고, 대책본부의 구성·운영 등에 관하여 필요한 사항은 대책본부장이 관계 중앙행정기관의 장과 협의하여 정한다.

③ 대책본부장은 제1항에 따른 대책본부를 구성·운영하기 위하여 책임기관 및 지원기관의 장에게 필요한 인력의 파견 및 장비의 제공을 요청할 수 있다.

제12조(비밀 엄수의 의무) 이 법에 따라 사이버테러 방지 및 위기관리 업무에 종사하거나 종사하였던 자는 그 직무상 알게 된 비밀을 타

인에게 누설하거나 직무상 목적 외에 이를 사용하여서는 아니 된다.

제13조(포상 등) ① 정부는 사이버테러 방지 및 위기관리와 관련하여 다음 각 호의 어느 하나에 해당하는 자에 대하여 포상하고, 예산의 범위에서 포상금을 지급할 수 있다.

1. 사이버테러 기도에 관한 정보를 제공한 자

2. 사이버테러를 가한 자를 신고한 자

3. 사이버테러의 탐지 및 대응·복구에 공이 많은 자

② 제1항에 따른 포상과 포상금 지급의 기준·방법과 절차, 구체적인 지급액 등 필요한 사항은 대통령령으로 정한다.

제14조(벌칙) ① 다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.

1. 제8조제2항 및 제4항을 위반한 자

2. 제9조제4항을 위반한 자

3. 제12조를 위반한 자

② 업무상 과실로 인하여 제1항의 죄를 범한 자는 2년 이하의 징역 또는 1천만원 이하의 벌금에 처한다.

제15조(과태료) ① 제9조제3항을 위반한 자는 1천만원 이하의 과태료에 처한다.

② 제1항에 따른 과태료는 대통령령이 정하는 바에 따라 관계 중앙행정기관의 장이 부과·징수한다.

부 칙

이 법은 공포한 날부터 시행한다.