

국가사이버안보기본법안

(엄태영의원 대표발의)

의안 번호	21584
----------	-------

발의연월일 : 2026. 9. 28.

발 의 자 : 엄태영 · 김태호 · 김은혜
유의동 · 윤한홍 · 김용태
서천호 · 김재섭 · 김상훈
김선교 · 이소희 · 이만희
의원(12인)

제안이유

국제 및 국가배후 해킹조직 등에 의하여 공공 및 민간 영역의 구분이 없이 동시다발적으로 광범위하게 발생하는 사이버공격으로 인한 국가안보와 국익 침해가 심각한 상황임.

그러나 사이버공격에 대한 국가적 대응활동은 각 부처별 소관 개별법령에 따라 제각각 분리, 독립 대응하고 있어 국가 사이버안보위협 상황 발생시 범 정부 차원에서 종합적으로 대응하는 데 한계가 있음. 또한 4차 산업혁명 등 사이버기술의 발전으로 국가 안보 영역이 사이버공간으로 확장되었음에도 불구하고 사이버안보를 담보하기 위한 정책 방향 및 대응책을 수립·시행하는 기본법조차 마련되지 않아 각 부처별 역할의 혼선, 업무영역의 중복 등 비효율화가 초래되고 있음.

따라서 국가 사이버안보 정책 및 사업을 효율적으로 추진하기 위하여 민간전문가가 참여하는 국가사이버안보위원회를 구성하고, 위기시 국가

역량을 결집해 신속한 사고 조사 및 위협정보 공유 등을 수행하는 통합 대응 조직을 별도로 설치·운영하는 등 대통령실 중심의 국가사이버안보 체계를 정립하고자 함. 또한 각 부처의 소관영역 보호책임을 명확히 하여 예방·대응활동을 강화하고, 범정부 차원의 협력을 공고화하여 국가 사이버안보 위협에 효과적으로 대응할 수 있도록 하려는 것임.

주요내용

가. 사이버안보 위협에 대응하기 위한 국가 차원의 사이버안보 대응체계를 마련함으로써 국가안보 및 국익보호에 이바지하고자 함(안 제1조).

나. 사이버안보와 관련된 국가의 정책 및 전략 수립에 관한 사항 등을 심의하기 위하여 대통령 소속으로 국가사이버안보위원회를 두되, 위원장은 국가안보실장으로, 위원은 국가정보원장, 개인정보보호위원장 등 중앙행정기관의 장 중 대통령이 지명하는 사람, 국회 정보위원회의 추천을 받은 사람, 민간 전문가 중 대통령이 위촉한 사람으로 구성토록 함(안 제7조).

다. 사이버위협 대응에 필요한 정보의 효율적 배포·공유·관리를 위해 국가사이버위협정보공유시스템을 구축·운영할 수 있도록 함(안 제9조).

라. 정부는 위협 수준과 발생 가능성 등을 판단해 관심·주의·경계·심각 4단계의 사이버위기 경보를 발령할 수 있고, 경보가 발령되면 중앙

행정기관등의 장이 이를 신속히 전파하고, 단계별로 소관 사무 보호를 위한 대비태세를 강화하는 등 필요한 조치를 취하도록 함(안 제10조).

마. 사이버위협 사고에 대비·대응하기 위해 국가 차원의 일원화된 통보·조사 체계를 구축·운영하도록 하고, 이를 위하여 관계 중앙행정기관, 정보·수사기관, 기업 등이 참여하는 통합대응 조직을 국가정보원에 설치·운영할 수 있도록 함(안 제11조).

바. 사이버안보 업무의 추진상황에 관한 사항을 국회 소관 상임위원회에 반기별로 보고하도록 함(안 제14조).

국가사이버안보기본법안

제1장 총칙

제1조(목적) 이 법은 국가역량을 결집하여 사이버위협에 체계적이고 효과적으로 대응하기 위하여 국가 차원의 사이버안보 대응체계를 마련함으로써 국가안전보장 및 국익보호에 이바지함을 목적으로 한다.

제2조(정의) 이 법에서 사용하는 용어의 정의는 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 유출·훼손하는 등의 행위 또는 활동을 말한다.
3. “사이버위협”이란 국제 및 국가배후 해킹조직과 북한, 외국 및 외국인·외국단체·초국가행위자 또는 이와 연계된 내국인의 국가안보와 국익에 반하는 사이버공격을 말한다.
4. “사이버안보”란 사이버위협을 확인·견제·차단하고 이에 필요한

대응조치를 강구함으로써 국가의 안전을 보장하고 국익을 보호하는 것을 말한다.

제3조(국가 등의 책무) ① 국가와 지방자치단체는 사이버안보가 국가안보에서 차지하는 중요성을 인식하고 서로 긴밀히 협력하여 사이버공간을 사이버위협으로부터 보호하기 위하여 종합적인 시책을 수립·시행하여야 한다.

② 국가와 지방자치단체는 제1항에 따른 책무를 다하기 위하여 필요한 법적·제도적 장치를 마련하고 이에 필요한 재원(財源)을 확보하도록 노력하여야 한다.

③ 국회·법원·중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속기관과 국무총리 소속기관을 포함한다), 「국가인권위원회법」에 따른 국가인권위원회, 「고위공직자범죄수사처 설치 및 운영에 관한 법률」에 따른 고위공직자범죄수사처, 특별시·광역시·특별자치시·도·특별자치도 및 시·도 교육청(이하 “중앙행정기관등”이라 한다)는 사이버공격으로부터 소관 사무를 안전하게 보호할 책임을 진다.

④ 국가와 지방자치단체는 사이버안보를 위하여 개인정보를 처리하는 경우 최소한의 기간에 최소한의 개인정보만을 처리하여야 하며, 개인정보의 안전한 관리와 적절한 처리를 위하여 필요한 조치를 하여야 한다.

제4조(다른 법률과의 관계) 사이버안보에 관하여 이 법에서 정한 사항

에 대하여는 다른 법률에 우선하여 적용한다.

제2장 사이버안보 기본계획 등

제5조(사이버안보 기본계획의 수립·시행) ① 정부는 사이버안보 전략 및 정책의 효율적·체계적 추진을 위하여 3년마다 국가 차원의 전략 방향을 제시하는 사이버안보 기본계획(이하 “기본계획”이라 한다)을 수립하여야 한다.

② 기본계획은 국가정보원장이 「정부조직법」 제2조에 따른 중앙행정기관(이하 “중앙행정기관”이라 한다)의 장과 협의하고, 제7조에 따른 국가사이버안보위원회의 심의를 거쳐 확정한다. 기본계획을 변경하는 경우에도 또한 같다.

③ 기본계획에는 다음 각 호의 사항이 포함되어야 한다.

1. 사이버안보의 정책 목표와 추진방향
2. 사이버안보와 관련된 제도 및 법령의 개선
3. 사이버위협 예방 및 대응
4. 사이버안보 관련 교육·홍보·인력양성 및 국제협력
5. 사이버안보 관련 연구 및 기술개발
6. 사이버안보 정책 추진에 필요한 재원의 조달·운용 및 인력확보 방안
7. 그 밖에 대통령령으로 정하는 사이버안보를 위하여 필요한 사항

④ 제1항부터 제3항까지에 따른 기본계획의 수립 및 변경의 방법·절차 등에 필요한 사항은 대통령령으로 정한다.

제6조(사이버안보 시행계획의 수립) ① 정부는 중앙행정기관등의 장으로부터 기본계획에 따른 추진계획을 제출받아 매년 사이버안보 시행계획(이하 “시행계획”이라 한다)을 수립·시행하여야 한다.

② 시행계획의 수립과 변경에 관한 세부 절차는 대통령령으로 정한다.

제7조(국가사이버안보위원회) ① 사이버안보에 관한 다음 각 호의 사항을 심의하기 위하여 대통령 소속으로 국가사이버안보위원회(이하 “위원회”라 한다)를 둔다.

1. 기본계획의 수립에 관한 사항
2. 사이버안보와 관련한 정책·법령 및 예산에 관한 사항
3. 사이버안보 위해자 및 배후 국가·단체에 대한 대응조치에 관한 사항
4. 그 밖에 위원회의 위원장이 부의하거나 위원이 제출한 사항

② 위원회는 위원장 1명을 포함하여 20명 이내의 위원으로 구성한다.

③ 위원회의 위원장은 국가안보실장이 되고, 위원은 다음 각 호의 사람이 된다.

1. 국가정보원장
2. 개인정보보호위원장

3. 과학기술정보통신부장관
 4. 대통령령으로 정하는 관계 중앙행정기관의 장
 5. 국회 해당 상임위원회에서 추천한 사람 중에서 대통령이 위촉하는 사람 3명
 6. 사이버안보에 관하여 전문적인 식견을 갖춘 사람 중에서 대통령이 위촉하는 사람 3명
- ④ 위원회에 상정할 안건을 미리 검토하고 위원회가 위임한 사항을 처리하기 위하여 위원회에 사이버안보 실무위원회(이하 “실무위원회”라 한다)를 둘 수 있다.
- ⑤ 위원회와 실무위원회의 구성·운영 등에 필요한 사항은 대통령령으로 정한다.

제3장 사이버안보 활동

제8조(예방·대응활동) ① 중앙행정기관등은 사이버위협에 대한 국가차원의 종합적 관리를 위해 소관 사무에 대하여 다음 각 호의 예방·대응 활동을 수행하여야 한다.

1. 정기적인 사이버위협 점검 및 사이버안보 훈련 실시
2. 안전한 정보통신기기등의 도입 및 활용
3. 사이버위협 탐지, 정보공유, 사고신고 등 예방·대응 체계의 구축·운영

4. 전문인력 확보 및 직무교육 실시

5. 그 밖에 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙 또는 대통령령으로 정하는 사항

② 제1항제1호의 사이버보안 점검·훈련은 매년 정기적으로 또는 수시로 실시할 수 있으며, 정기 훈련은 「비상대비에 관한 법률」 제14조에 따른 비상대비훈련과 함께 실시할 수 있다.

③ 그 밖에 예방·대응활동의 방법·절차 및 세부 내용 등에 필요한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙 또는 대통령령으로 정한다.

제9조(정보의 공유) ① 정부는 사이버위협 대응에 필요한 정보의 효율적인 배포, 공유 및 관리를 위하여 국가사이버위협정보공유시스템(이하 “정보공유시스템”이라 한다)을 구축·운영할 수 있다.

② 다음 각 호의 정보를 수집·작성·배포하거나 처리하는 중앙행정기관등의 장 또는 그 밖의 기관·단체의 장은 다른 중앙행정기관등의 소관 사무 영역 보호활동을 지원하기 위하여 정보공유시스템을 통하여 해당 정보를 공유하고 상호 협력하여야 한다.

1. 「국가정보원법」 제4조제1항제1호마목에 따른 국제 및 국가배후 해킹조직 등 사이버안보 정보

2. 「국방정보화 기반조성 및 국방정보자원관리에 관한 법률」 제21조에 따른 국방정보침해에 관한 정보

3. 「의료법」 제23조의4제1항제1호에 따른 진료정보 침해사고에 관

한 정보

4. 「전자금융거래법」 제21조의6제1항제1호에 따른 침해사고에 관한 정보

5. 「전자정부법」 제54조제3항에 따른 통합관리기관이 대통령령에 따라 수행하는 침해대응에 관한 정보

6. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제48조의2에 따른 침해사고에 관한 정보

7. 그 밖에 사이버안보에 필요한 정보로서 대통령령으로 정하는 정보

③ 중앙행정기관등은 사이버공격 정보의 공유 및 관리 과정에서 발생할 수 있는 권리 침해를 방지하기 위한 관리적·물리적·기술적 대책을 수립·시행하여야 한다.

④ 그 밖에 정보공유시스템의 구축·운영 등에 필요한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙 또는 대통령령으로 정한다.

제10조(사이버위기 경보의 발령) ① 정부는 사이버위협에 대한 체계적인 대응을 위하여 위협 수준, 발생 가능성 등을 판단하여 관심·주의·경계·심각 단계의 사이버위기(이하 “경보”라 한다)를 발령할 수 있다.

② 중앙행정기관등의 장은 제1항에 따른 경보가 발령된 경우 이를 신속하게 전파하고 경보 단계별로 사이버위협으로부터 소관 사무

영역을 보호할 대비태세를 강화하는 등 필요한 조치를 취하여야 한다.

③ 경보 발령의 기준·절차 및 중앙행정기관등의 장의 조치 등에 필요한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙, 중앙선거관리위원회규칙 또는 대통령령으로 정한다.

제11조(통합대응 조직의 운영) ① 정부는 사이버위협으로 인한 사고에 대비하거나 사고 발생에 대응하기 위하여 국가 차원의 일원화된 통보·조사 등 대응체계를 구축·운영하여야 한다.

② 제1항의 체계를 구축하기 위하여 대통령령이 정하는 관계 중앙행정기관, 정보·수사기관, 기업 등이 참여하는 통합대응 조직을 국가정보원에 설치·운영할 수 있다.

③ 위원회는 제2항의 통합대응 조직의 업무를 감독하기 위하여 필요한 경우 해당 업무를 보고하게 할 수 있다.

④ 제2항의 통합대응 조직의 구성 및 운영에 필요한 사항은 대통령령으로 정한다

제12조(사이버위기대책본부) ① 정부는 제10조제1항에 따른 경계 또는 심각 단계의 경보가 발령된 경우 사이버위협에 대한 원인분석, 긴급 대응, 피해복구 등 신속한 국민안전 보호조치를 취하기 위하여 사이버위기대책본부(이하 “대책본부”라 한다)를 구성·운영할 수 있다.

② 대책본부의 장(이하 “대책본부장”이라 한다)은 국가안보실장이 지명한다.

③ 대책본부장은 대책본부를 구성·운영하기 위하여 중앙행정기관 등 및 그 밖에 대통령령으로 정하는 기관·단체의 장에게 참여를 요청할 수 있다.

④ 그 밖에 대책본부의 구성·운영 등에 필요한 사항은 대통령령으로 정한다.

제4장 보칙

제13조(국제협력) 정부는 사이버안보에 관하여 외국의 정부, 관련 분야 국제기구 및 단체와의 협력을 증진하기 위하여 다음 각 호의 업무를 수행할 수 있다.

1. 사이버안보를 위한 상호간 협력체계 구축
2. 사이버안보 기술에 관한 정보의 교류와 공동대응
3. 사이버안보 전담인력의 상호간 파견교육

제14조(국회 보고) ① 정부는 이 법에 따른 사이버안보 업무의 추진상황에 관한 사항을 국회 소관 상임위원회에 반기별로 보고하여야 한다.

② 국가정보원장은 국가 기밀에 속하는 사항에 관한 보고에 대하여 이를 공개하지 아니할 것을 요청할 수 있다.

제15조(전문연구기관 설립 등) ① 정부는 이 법에 따른 사이버안보 관련 업무를 효율적으로 수행하기 위하여 전문연구기관을 설립·운영

할 수 있다.

② 제1항에 따른 전문연구기관의 설립·운영에 필요한 사항은 따로 법률로 정한다.

제16조(업무의 위임·위탁) ① 정부는 필요하다고 인정하는 경우 이 법에 따른 사이버안보 관련 업무를 대통령령으로 정하는 바에 따라 그 일부를 제15조의 전문연구기관 또는 대통령령으로 정하는 기관·단체에 위탁할 수 있다.

② 제1항의 업무의 위임·위탁 등에 필요한 사항은 대통령령으로 정한다.

제17조(비밀 엄수의 의무) 사이버안보에 관한 업무에 종사하고 있거나 종사하였던 사람은 직무상 알게 된 비밀을 누설하거나 직무상 목적 외의 용도에 이용해서는 아니 된다.

제5장 벌칙

제18조(벌칙) 제17조를 위반하여 직무상 알게 된 비밀을 누설하거나 직무상 목적 외의 용도에 사용한 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.

부 칙

이 법은 공포 후 6개월이 경과한 날부터 시행한다.