사이버안보 업무규정

[시행 2025. 1. 1.] [대통령령 제34287호, 2024. 3. 5., 일부개정]

국가정보원 (국가정보원) 111

제1조(목적) 이 영은「국가정보원법」제4조제1항에 따른 국가정보원의 직무 중 사이버안보 업무의 수행에 필요한 사항을 규정함을 목적으로 한다.

[전문개정 2024. 3. 5.]

제2조(정의) 이 영에서 사용하는 용어의 뜻은 다음과 같다. <개정 2024. 3. 5.>

1. "정보통신망"이란「전기통신사업법」제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말한다.
2. "사이버공격·위협"이란 해킹, 컴퓨터 바이러스, 서비스거부(DDoS: Distributed Denial of Service), 전자기파 등 전자적 수단에 의하여 정보통신기기, 정보통신망 또는 이와 관련된 정보시스템을 침입·교란·마비·파괴하거나 정보를 위조·변조·훼손·절취하는 행위 및 그와 관련된 위협을 말한다.

제3조(사이버안보 업무의 수행) 국가정보원은 사이버안보를 위하여 다음 각 호의 업무(이하 "사이버안보 업무"라 한다)를 수행한다.

1. 사이버안보정보 업무
   가.「국가정보원법」(이하 "법"이라 한다) 제4조제1항제1호마목에 따라 국제 및 국가배후 해킹조직 등 사이버안보 관련 정보를 수집·작성·배포하는 업무
   나. 법 제4조제1항제3호에 따라 사이버안보 관련 정보의 수집·작성·배포 업무 수행에 관련된 조치로서 국가안보와 국익에 반하는 북한, 외국 및 외국인·외국단체·초국가행위자 또는 이와 연계된 내국인의 활동을 확인·견제·차단하고 국민의 안전을 보호하기 위하여 취하는 대응조치
   다. 법 제4조제1항제5호에 따라 수행하는 가목 및 나목에 따른 업무의 기획·조정 업무
2. 사이버보안 업무
   가. 법 제4조제1항제4호 각 목의 기관(이하 "중앙행정기관등"이라 한다)을 대상으로 하는 사이버 공격·위협에 대한 예방 및 대응 업무
   나. 법 제4조제1항제5호에 따라 수행하는 사이버공격·위협에 대한 예방 및 대응 관련 기획·조정 업무

[전문개정 2024. 3. 5.]

제3조의2(사이버안보 업무의 기획·조정) ① 국가정보원장은 제3조제1호에 따른 사이버안보정보 업무(이하 "사이버안보정보 업무"라 한다) 및 같은 조 제2호에 따른 사이버보안 업무(이하 "사이버보안 업무"라 한다)에 관한 정책의 수립 등 기획업무를 수행하고, 사이버안보정보 업무 및 사이버보안 업무를 효율적·체계적으로 수행하기 위하여 다음 각 호의 지침 등을 수립·시행해야 한다.

1. 사이버안보정보 업무에 관한 기본지침
2. 사이버보안 업무에 관한 기본지침
3. 새로운 유형의 사이버공격·위협에 대응하기 위한 수시 보안대책

② 국가정보원장은 사이버안보정보 업무 및 사이버보안 업무에 대한 조정이 필요한 경우 국가안보에 중대한 영향을 미치는 긴급사안에 대해서는 직접 조정하고, 그 밖의 사안에 대해서는 제1항제1호 및 제2호에 따른 기본지침으로 정하는 바에 따라 조정한다.

[본조신설 2024. 3. 5.]

제4조(국가사이버안보센터) ① 국가정보원장은 사이버안보 업무를 효율적으로 수행하기 위하여 국가사이버안보센터를 둘 수 있다.

② 제1항에 따른 국가사이버안보센터에는 제6조의2제4항에 따른 민관합동 통합대응체계를 구축·운영하기 위한 전담조직을 둘 수 있다.<신설 2024. 3. 5.>

③ 제1항에 따른 국가사이버안보센터에 사이버안보에 관한 사항을 전문적으로 검토하기 위하여 관계 전문가로 구성된 자문단을 설치·운영할 수 있다.<신설 2024. 3. 5.>

④ 국가정보원장은 제1항에 따른 국가사이버안보센터의 운영을 위하여 필요한 경우 법 제5조제1항에 따른 국가기관이나 그 밖의 관계 기관 또는 단체(이하 "국가기관 등"이라 한다)의 장에게 소속 공무원 또는 임직원의 파견 등 협조를 요청할 수 있다.<개정 2024. 3. 5.>

제5조(기관 간 협력체계 구축) 국가정보원장은 사이버안보정보 업무의 수행을 위하여 필요한 경우 국가기관 등, 외국의 정보·보안기관이나 그 밖의 관계 기관과 정보협력체계를 구축할 수 있다.

[전문개정 2024. 3. 5.]

제5조의2(사이버안보정보의 임의제출) 국가정보원장이 법 제5조제2항에 따라 사이버안보 관련 정보의 수집을 위해 필요한 조사를 실시하는 경우, 사이버안보 관련 정보가 수록·기재된 디지털자료 등의 소유자·소지자 또는 보관자는 조사에 응하여 그 디지털자료 등을 임의로 국가정보원장에게 제출할 수 있다. 다만, 그 디지털자료 등이 「통신비밀보호법」 제2조제11호에 따른 통신사실확인자료에 해당하는 경우에는 같은 법 제2조제4호에 따른 당사자의 동의를 받아야 한다.

[본조신설 2024. 3. 5.]

제5조의3(사이버안보정보의 작성) 국가정보원장은 사이버안보정보 업무를 통해 수집한 국내외 정보를 종합·분석·평가하여 위해(危害) 행위의 수준, 국가안전보장에 미치는 영향 및 국민의 안전을 보호하기 위한 대응조치 등이 포함된 사이버안보정보를 작성해야 한다.

[본조신설 2024. 3. 5.]

제6조(정보공유시스템 구축) ① 국가정보원장은 사이버안보 관련 정보를 배포·공유하기 위하여 정보공유시스템을 구축·운영할 수 있다. <개정 2024. 3. 5.>

② 제1항에 따른 정보공유시스템의 활용 대상 및 범위 등 운영에 필요한 사항은 국가정보원장이 관계 중앙행정기관 등과 협의하여 정한다.

제6조의2(사이버안보정보 업무 수행 관련 대응조치 등) ① 국가정보원장은 국가안보와 국익에 반하는 활동에 악용되거나 악용될 만한 상당한 개연성이 있는 정보통신기기·소프트웨어의 안전성을 확인하기 위하여 정보통신기기·소프트웨어에 대한 기술적인 시험·분석을 할 수 있다.

② 국가정보원장은 제1항에 따른 시험·분석 결과에 따라 국가기관 등에 위험을 최소화할 수 있는 필요한 조치를 취하도록 요청할 수 있고, 그 요청을 받은 국가기관 등은 필요한 조치의 이행을 위하여 국가정보원장에게 지원을 요청할 수 있다.

③ 국가정보원장은 국가안보와 국익에 반하는 국제 및 국가배후 해킹조직 등의 활동을 선제적으로 확인·견제·차단하기 위하여 국외 및 북한 소재 거점을 대상으로 추적, 무력화 등 필요한 조치를 할 수 있다.

④ 국가정보원장은 국가안보나 국익에 반하는 활동으로부터 국민의 안전을 보호하기 위한 대응조치로서 국가안보실장과 협의하여 위기상황을 관리하기 위한 민관합동 통합대응체계를 구축·운영할 수 있다.

[본조신설 2024. 3. 5.]

제7조(사이버보안 업무 대상 공공기관의 범위) 법 제4조제1항제4호다목에서 "대통령령으로 정하는 공공기관"이란 다음 각 호의 기관을 말한다. <개정 2024. 3. 5.>

1. 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관
2. 「지방공기업법」에 따른 지방공사 및 지방공단

2의2. 「지방자치단체 출자·출연 기관의 운영에 관한 법률」 제2조제1항에 따른 출자·출연 기관 중 해당 지방자치단체의 조례로 정하는 기관
3. 특별법에 따라 설립된 법인. 다만, 「지방문화원진흥법」에 따른 지방문화원 및 특별법에 따라 설립된 조합·협회는 제외한다.
4. 「초·중등교육법」, 「고등교육법」 및 그 밖의 다른 법률에 따라 설치된 국립·공립 학교
5. 「정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조제1항 및 「과학기술분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조제1항에 따른 연구기관

[제목개정 2024. 3. 5.]

제8조(사이버보안 세부지침의 수립·시행) 중앙행정기관등의 장은 제3조의2제1항제2호에 따른 기본지침에 따라 해당 기관의 특성 및 보안수준 등을 반영하여 해당 기관을 대상으로 한 사이버보안 세부지침을 수립·시행해야 한다.

[전문개정 2024. 3. 5.]

제9조(사이버보안 예방 조치 등) ① 국가정보원장은 중앙행정기관등에 대한 사이버공격·위협을 예방하기 위하여 중앙행정기관등의 장이 시행하는 정보화사업(「지능정보화 기본법」 제11조제1항에 따른 지능정보화계획에 따른 사업을 포함한다)에 대하여 보안성 검토를 실시하고, 그 보안성 검토 결과의 이행 여부를 확인할 수 있다.

② 국가정보원장은 중앙행정기관등의 정보보호시스템, 암호장치, 암호모듈 및 보안기능이 있는 정보통신기기(이하 "정보보호시스템등"이라 한다)의 도입·운영 및 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제3호에 따른 클라우드컴퓨팅서비스(이하 이 조에서 "클라우드컴퓨팅서비스"라 한다)의 이용에 관한 보안대책을 수립할 수 있다.<개정 2024. 3. 5.>

③ 국가정보원장은 중앙행정기관등이 도입·운영하거나 이용하는 정보보호시스템등 및 클라우드컴퓨팅서비스가 제2항에 따른 보안대책에 적합한지 검증할 수 있다.<개정 2024. 3. 5.>

④ 국가정보원장은 정보보호시스템등을 직접 개발하여 중앙행정기관등에 보급할 수 있다.

⑤ 국가정보원장은 중앙행정기관등의 정보통신기기, 정보통신망 또는 이와 관련된 정보시스템의 취약요소를 발굴·개선하기 위해 보안관리 수준을 측정할 수 있다. 이 경우 그 항목·절차·시기 등을 해당 중앙행정기관등의 장에게 미리 통보해야 한다.<개정 2024. 3. 5.>

⑥ 제5항에도 불구하고 제7조 각 호에 따른 기관 중 국가정보원장과 국방부장관이 협의하여 정하는 기관에 대해서는 국방부장관이 보안관리 수준을 측정한다. 이 경우 국가안보에 필요하다고 판단되거나 국가정보원장의 요청이 있는 경우에는 관련 내용을 국가정보원장에게 통보해야 한다.<신설 2024. 3. 5.>

[제목개정 2024. 3. 5.]

제10조(사이버보안 교육) ① 중앙행정기관등의 장은 소속 공무원 및 임직원의 사이버보안에 대한 인식과 사이버보안 업무를 수행하는 소속 공무원 및 임직원의 직무역량을 높이기 위하여 필요한 교육을 실시해야 한다. <개정 2024. 3. 5.>

② 국가정보원장은 제1항에 따른 사이버보안 교육을 위하여 필요한 경우 관련 교육과정을 직접 운영하거나 다른 기관·단체가 운영하는 교육과정을 사이버보안 교육과정으로 지정할 수 있다.<개정 2024. 3. 5.>

③ 중앙행정기관등의 장은 국가정보원장에게 제1항에 따른 사이버보안 교육을 위하여 필요한 지원을 요청할 수 있다.<신설 2024. 3. 5.>

[제목개정 2024. 3. 5.]

제11조(사이버보안 훈련) ① 중앙행정기관등의 장은 매년 해당 기관에 대한 사이버공격·위협에 대응하기 위한 훈련을 실시해야 한다.

② 국가정보원장은 국가안보실장과 협의하여 중앙행정기관등에 대한 사이버공격·위협에 대비한 통합 훈련을 실시할 수 있다.

③ 국가정보원장은 제2항에 따른 통합 훈련을 실시하려는 경우 특별한 사유가 없으면 사전에 훈련 일정 등을 해당 중앙행정기관등의 장에게 통보해야 한다.
④ 국가정보원장은 제2항에 따른 통합 훈련 결과 필요하다고 판단하는 경우에는 해당 중앙행정기관등의 장에게 시정조치를 요청할 수 있다.
⑤ 제1항에 따른 훈련 및 제2항에 따른 통합 훈련의 범위와 세부 내용에 관하여 필요한 사항은 국가정보원장이 정한다.
[제목개정 2024. 3. 5.]

제12조(사이버보안 자체 진단·점검) ① 중앙행정기관등의 장은 해당 기관에 대한 사이버공격·위협에 대한 예방 및 대응에 필요한 자체 진단·점검을 연 1회 이상 실시해야 한다. <개정 2024. 3. 5.>
② 제1항에도 불구하고 중앙행정기관등의 장이 다음 각 호의 어느 하나에 해당하는 조치를 한 경우에는 제1항에 따른 자체 진단·점검을 실시한 것으로 본다.<개정 2024. 3. 5.>
1. 삭제<2024. 3. 5.>
2.「정보통신기반 보호법」제9조에 따른 취약점 분석·평가
3. 제9조제5항에 따른 보안관리 수준 측정
4.「전자금융거래법」제21조의3에 따른 전자금융기반시설의 취약점 분석·평가
③ 중앙행정기관등의 장은 제1항에 따른 진단·점검 결과 취약요소가 발견된 경우 이를 시정하는 등 필요한 조치를 해야 한다.
④ 국가정보원장은 사이버공격·위협이 발생하거나 발생할 우려가 있는 중앙행정기관등의 장에게 제1항에 따른 자체 진단·점검 결과 및 제3항에 따른 조치 결과를 제출할 것을 요청할 수 있다. 이 경우 요청을 받은 중앙행정기관등의 장은 정당한 사유가 없으면 그 요청에 따라야 한다.<신설 2024. 3. 5.>
[제목개정 2024. 3. 5.]

제13조(사이버보안 실태 평가) ① 국가정보원장은 중앙행정기관등의 사이버보안 업무 수행을 위한 조직, 인력, 예산, 직무교육 및 사이버보안에 대한 자체 진단·점검 등 사이버보안 실태를 평가할 수 있다. <개정 2024. 3. 5.>
② 국가정보원장은 제1항에 따른 평가를 하려는 경우 평가의 항목·절차·시기 등을 해당 중앙행정기관등의 장에게 미리 통보해야 한다.
③ 국가정보원장은 제1항에 따른 평가의 결과를 해당 중앙행정기관등의 장에게 통보해야 한다.
④ 제3항에 따라 평가 결과를 통보받은 해당 중앙행정기관등의 장은 평가의 결과에 따라 문제점이 발견된 경우에는 그 결과를 통보받은 날부터 3개월 이내에 개선대책을 마련하고 국가정보원장에게 통보해야 한다.<신설 2024. 3. 5.>
⑤ 국가정보원장은 중앙행정기관등의 장이 제4항에 따라 통보한 개선대책에 대한 이행 여부를 확인할 수 있다.<신설 2024. 3. 5.>
⑥ 국가정보원장은 국가안전보장에 지장이 없는 범위에서 제1항에 따른 실태 평가 결과를 공개할 수 있다.<신설 2024. 3. 5.>
⑦ 국가정보원장은 제1항에 따른 평가의 효율적 수행, 평가에 관한 전문적·기술적인 연구 등을 위하여 필요한 경우 관계 전문가를 활용할 수 있다.<신설 2024. 3. 5.>
[제목개정 2024. 3. 5.]

제14조(통합보안관제) ① 국가정보원장은 중앙행정기관등에 대한 사이버공격·위협을 즉시 탐지·대응[이하 "보안관제(保安管制)"라 한다]하기 위하여 통합보안관제체계를 구축·운영해야 한다. <개정 2024. 3. 5.>
② 중앙행정기관등의 장은 해당 기관의 보안관제를 위하여 제1항에 따른 통합보안관제체계와 연계된 보안관제센터를 설치·운영해야 한다. 다만, 다른 기관이 운영하는 보안관제센터를 활용하는 것이 더 효율적인 경우에는 직접 설치하지 않고 다른 기관의 보안관제센터를 활용할 수 있다.<개정 2024. 3. 5.>

③ 국가정보원장은 제1항에 따른 통합보안관제체계를 활용하여 각 중앙행정기관등의 장과 합동으로 해당 중앙행정기관등에 대한 보안관제를 실시할 수 있다.<개정 2024. 3. 5.>

④ 국가정보원장은 제3항에 따른 보안관제를 위하여 법 제5조제1항에 따라 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제4호에 따른 클라우드컴퓨팅서비스 제공자에게 필요한 협조 또는 지원을 요청할 수 있다.<신설 2024. 3. 5.>

⑤ 제1항부터 제4항까지에서 규정한 사항 외에 보안관제센터의 설치·운영 및 그 밖에 필요한 사항은 국가정보원장이 관계 중앙행정기관의 장과 협의하여 정한다.<개정 2024. 3. 5.>

[제목개정 2024. 3. 5.]

제15조(경보 발령) ① 국가정보원장은 중앙행정기관등에 대한 사이버공격·위협에 체계적으로 대응 및 대비하기 위하여 파급영향 및 피해규모 등을 고려하여 단계별로 경보를 발령할 수 있다. 이 경우 국가안보실장과 미리 협의해야 한다.

② 제1항에도 불구하고 제7조 각 호에 따른 기관 중 국가정보원장과 국방부장관이 협의하여 정하는 기관에 대해서는 국방부장관이 경보를 발령한다. 이 경우 국가안보에 필요하다고 판단되거나 국가정보원장의 요청이 있는 경우에는 관련 내용을 국가정보원장에게 통보해야 한다.<개정 2024. 3. 5.>

③ 국가정보원장, 국방부장관 및 다른 법령에 따라 사이버공격·위협에 대응 및 대비하기 위한 경보를 발령하는 중앙행정기관의 장은 국가 차원에서의 효율적인 경보 업무를 수행하기 위하여 경보 관련 정보를 경보 발령 전에 상호 교환해야 한다.<개정 2024. 3. 5.>

제16조(사고 조사) ① 국가정보원장은 중앙행정기관등에 대한 사이버공격·위협으로 사고가 발생한 경우 공격 주체 규명, 원인 분석 및 피해 내역 확인 등을 위한 조사를 실시할 수 있다. 다만, 제7조 각 호에 따른 기관 중 국가정보원장과 국방부장관이 협의하여 정하는 기관에 대해서는 국방부장관이 조사를 실시할 수 있다. <개정 2024. 3. 5.>

② 제1항에도 불구하고 국가정보원장 또는 국방부장관은 중앙행정기관등에 대한 사이버공격·위협으로 인한 사고가 국제 및 국가배후 해킹조직 등의 위해 행위에 해당되지 않거나, 그 밖의 경미한 사고라고 판단될 경우 해당 중앙행정기관등의 장이 자체적으로 조사하게 할 수 있다.<개정 2024. 3. 5.>

③ 국가정보원장은 제1항 및 제2항에 따른 조사 결과 해당 사고로 유출된 것으로 판단되는 자료에 대하여 해당 중앙행정기관등의 장과 합동으로 국가안보, 국익 및 정부 정책에 미치는 영향을 평가할 수 있다.

④ 국가정보원장은 해당 중앙행정기관등의 장에게 제3항에 따른 국가안보, 국익 및 정부 정책에 미치는 영향을 최소화하기 위하여 필요한 조치를 할 것을 요청할 수 있다.

⑤ 국가정보원장은 사이버보안 업무의 수행과 관련하여 필요한 경우 중앙행정기관등의 장에게 제1항 단서 및 제2항에 따른 조사 결과, 제4항에 따른 조치 결과의 제출을 요청할 수 있다. 이 경우 요청을 받은 중앙행정기관등의 장은 정당한 사유가 없으면 그 요청에 따라야 한다.<신설 2024. 3. 5.>

제17조(사이버안보 업무 관련 전략 등의 연구·개발) ① 국가정보원장은 사이버안보 업무의 수행에 필요한 전략·정책 및 기술을 연구·개발할 수 있다.

② 국가정보원장은 제1항에 따른 연구·개발을 위하여 다음 각 호의 어느 하나에 해당하는 기관을 전문기관으로 지정할 수 있다.<개정 2024. 3. 5.>

1. 「과학기술분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조제1항에 따라 설립된 연구기관
2. 「민법」 제32조에 따라 설립된 비영리법인으로서 사이버안보 관련 학회 또는 학술단체

③ 제2항에 따른 전문기관을 지정하기 위하여 필요한 지정기준·절차 및 지정방법 등 세부 사항은 국가정보원장이 정한다.<신설 2024. 3. 5.>

④ 국가정보원장은 제2항에 따라 지정된 전문기관의 업무 수행을 위하여 그 필요한 경비의 전부 또는 일부를 예산의 범위에서 지원할 수 있다.<개정 2024. 3. 5.>

제18조(고유식별정보의 처리) 국가정보원장 및 중앙행정기관등의 장은 다음 각 호의 업무를 수행하기 위하여 불가피한 경우「개인정보 보호법 시행령」제19조제1호 또는 제4호에 따른 주민등록번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다. <개정 2024. 3. 5.>

1. 법 제5조제2항에 따른 사이버안보정보 업무의 수행을 위한 조사 업무
2. 제16조에 따른 사고 조사 업무

부칙 <제34287호,2024. 3. 5.>

제1조(시행일) 이 영은 공포한 날부터 시행한다. 다만, 제10조의 개정규정은 2025년 1월 1일부터 시행한다.

제2조(사이버보안 실태 평가 결과에 따른 개선대책 마련 등에 관한 적용례) 제13조제4항 및 제5항의 개정규정은 이 영 시행 이후 국가정보원장이 제13조제1항의 개정규정에 따라 사이버보안 실태를 평가하는 경우부터 적용한다.