국가사이버안전관리규정

[시행 2013. 9. 2.] [대통령훈령 제316호, 2013. 9. 2., 일부개정.]

국가정보원

제1조(목적) 이 훈령은 국가사이버안전에 관한 조직체계 및 운영에 대한 사항을 규정하고 사이버안전업무를 수행하는 기관간의 협력을 강화함으로써 국가안보를 위협하는 사이버공격으로부터 국가정보통신망을 보호함을 목적으로 한다.

제2조(정의) 이 훈령에서 사용하는 용어의 정의는 다음과 같다. <개정 2008. 8. 18., 2012. 1. 2.>

1. "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.
2. "사이버공격"이라 함은 해킹·컴퓨터바이러스·논리폭탄·메일폭탄·서비스방해 등 전자적 수단에 의하여 국가정보통신망을 불법침입·교란·마비·파괴하거나 정보를 절취·훼손하는 일체의 공격행위를 말한다.
3. "사이버안전"이라 함은 사이버공격으로부터 국가정보통신망을 보호함으로써 국가정보통신망과 정보의 기밀성·무결성·가용성 등 안전성을 유지하는 상태를 말한다.
4. "사이버위기"란 사이버공격으로 정보통신망을 통해 유통·저장되는 정보를 유출·변경·파괴함으로써 국가안보에 영향을 미치거나 사회·경제적 혼란을 발생시키거나 국가 정보통신시스템의 핵심기능이 훼손·정지되는 등 무력화되는 상황을 말한다.
5. "공공기관"이라 함은 다음 각목의 기관을 말한다.
   가. 「공공기관의 운영에 관한 법률」 제5조에 따라 지정된 공기업 또는 준정부기관인 공공기관
   나. 「공공기관의 운영에 관한 법률」 제5조에 따라 지정된 기타공공기관 중 「정부출연연구기 등의 설립·운영 및 육성에 관한 법률」 제8조제1항 및 「과학기술분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조제1항에 따른 연구기관
   다. 「초·중등교육법」 및 「고등교육법」에 따른 국·공립학교
   라. 그 밖에 다른 법령의 규정에 의하여 설립된 공공기관 중 제6조의 규정에 의한 국가사이버안전전략회의에서 정보통신망의 안전성 확보가 필요하다고 지정한 기관

제3조(적용범위) 이 훈령은 중앙행정기관(대통령 소속 기관, 국무총리 소속 기관 및 국가인권위원회를 포함한다. 이하 같다), 지방자치단체 및 공공기관의 정보통신망에 적용한다. 다만, 「정보통신기반보호법」에 따른 주요정보통신기반시설에 대해서는 「정보통신기반보호법」을 우선 적용한다. <개정 2012. 1. 2., 2013. 9. 2.>

제4조(사이버안전 확보의 책무) ① 중앙행정기관의 장은 소관 정보통신망에 대하여 안전성을 확보할 책임이 있으며 이를 위하여 사이버안전업무를 전담하는 전문인력을 확보하는 등 필요한 조치를 강구하여야 한다.

②관계 중앙행정기관의 장은 소관 공공기관 및 지방자치단체의 장으로 하여금 제1항의 규정에 의한 전문인력의 확보 등 필요한 조치를 강구하도록 하여야 한다.

제5조(국가사이버안전정책 및 관리) ① 국가사이버안전과 관련된 정책 및 관리에 대하여는 국가정보원장이 관계 중앙행정기관의 장과 협의하여 이를 총괄·조정한다. <개정 2012. 1. 2.>

② 국가정보원장은 제1항에 따른 총괄·조정 업무를 효율적이고 체계적으로 수행하기 위하여 관계 중앙행정기관의 장과 협의하여 국가사이버안전기본계획을 수립·시행한다. <신설 2012. 1. 2.>

③ 국가정보원장은 제2항에 따른 국가사이버안전기본계획을 원활하게 추진하기 위하여 관계 기관에 예산 반영 등에 관한 협조를 요청할 수 있다. <신설 2012. 1. 2.>

제6조(국가사이버안전전략회의) ① 국가사이버안전에 관한 중요사항을 심의하기 위하여 국가정보원장 소속하에 국가사이버안전전략회의(이하 "전략회의"라 한다)를 둔다.

②전략회의의 의장은 국가정보원장이 된다.

③ 전략회의의 위원은 다음 각 호의 사람과 전략회의 의장이 지명하는 관계 중앙행정기관의 차관급 공무원이 된다. 이 경우 차관 또는 차관급 공무원이 2명 이상인 기관은 사이버 안전 업무를 담당하는 차관 또는 차관급 공무원이 위원이 된다. <개정 2012. 1. 2., 2013. 5. 24., 2013. 9. 2.>

1. 기획재정부차관

2. 미래창조과학부차관
3. 교육부차관
4. 외교부차관
5. 통일부차관
6. 법무부차관
7. 국방부차관
8. 안전행정부차관
9. 산업통상자원부차관
10. 보건복지부차관
11. 국토교통부차관
12. 금융위원회 부위원장
13. 대통령비서실 사이버안전 담당 수석비서관
14. 국가안보실 사이버안전 담당 비서관
15. 국무조정실 국무차장

④전략회의는 다음 각호의 사항을 심의한다.
1. 국가사이버안전체계의 수립 및 개선에 관한 사항
2. 국가사이버안전 관련 정책 및 기관간 역할조정에 관한 사항
3. 국가사이버안전 관련 대통령 지시사항에 대한 조치방안
4. 그 밖에 전략회의 의장이 부의하는 사항

⑤ 제4항에 따라 전략회의의 심의를 거친 사항 중 중요 사항은 대통령 및 국무총리에게 보고한다. <신설 2012. 1. 2.>

⑥전략회의의 구성·운영 등에 관하여 필요한 사항은 전략회의의 의장이 따로 정한다. <개정 2012. 1. 2.>

제7조(국가사이버안전대책회의) ① 전략회의의 효율적인 운영을 위하여 전략회의에 국가사이버안전대책회의(이하 "대책회의"라 한다)를 둔다.

②대책회의의 의장은 국가정보원의 사이버안전업무를 담당하는 차장이 되며, 위원은 전략회의의 위원이 속하는 기관의 실·국장급 공무원으로 한다.

③대책회의는 다음 각호의 사항을 심의한다.
1. 국가사이버안전 관리 및 대책방안
2. 전략회의의 결정사항에 대한 시행방안
3. 전략회의로부터 위임받거나 전략회의의 의장으로부터 지시받은 사항
4. 그 밖에 대책회의의 의장이 부의하는 사항

④대책회의의 구성·운영 등에 관하여 필요한 사항은 대책회의의 의장이 따로 정한다.

제8조(국가사이버안전센터) ① 사이버공격에 대한 국가차원의 종합적이고 체계적인 대응을 위하여 국가정보원장 소속하에 국가사이버안전센터(이하 "사이버안전센터"라 한다)를 둔다.

②사이버안전센터는 다음 각호의 업무를 수행한다.
1. 국가사이버안전정책의 수립
2. 전략회의 및 대책회의의 운영에 대한 지원
3. 사이버위협 관련 정보의 수집·분석·전파
4. 국가정보통신망의 안전성 확인
5. 국가사이버안전매뉴얼의 작성·배표
6. 사이버공격으로 인하여 발생한 사고의 조사 및 복구 지원
7. 외국과의 사이버위협 관련 정보의 협력

③ 국가정보원장은 국가 차원의 사이버위협에 대한 종합판단, 상황관제, 위협요인 분석 및 합동조사 등을 위해 사이버안전센터에 민·관·군 합동대응반(이하 "합동대응반"이라 한다)을 설치·운영할 수 있다. <개정 2012. 1. 2.>

④국가정보원장은 합동대응반을 설치·운영하기 위하여 필요한 경우에는 관계 중앙행정기관, 지방자치단체 및 공공기관의 장에게 소속 공무원 및 직원의 파견을 요청할 수 있다. <신설 2012. 1. 2.>

제9조(사이버안전대책의 수립·시행 등) ① 중앙행정기관의 장은 소관 정보통신망을 보호하기 위하여 사이버안전대책을 수립·시행하고, 이를 지도·감독하여야 한다.

②관계 중앙행정기관의 장은 공공기관의 장 및 지방자치단체의 장으로 하여금 제1항의 규정에 의한 사이버안전

대책을 수립·시행하도록 할 수 있다.
③국가정보원장은 제1항 및 제2항에 따른 사이버안전대책의 수립에 필요한 국가사이버안전매뉴얼 및 관련 지침을 작성 배포할 수 있다. 이 경우 국가정보원장은 미리 관계 중앙행정기관의 장과 협의하여야 한다. <개정 2012. 1. 2.>
④국가정보원장은 제1항 및 제2항에 따른 사이버안전대책의 이행여부 진단·평가 등 정보통신망에 대한 안전성을 확인할 수 있으며 필요하다고 인정하는 경우에는 해당 중앙행정기관의 장에게 시정 등 필요한 조치를 권고할 수 있다. 다만, 지방자치단체 및 공공기관의 정보통신망에 대한 안전성 확인은 관계 중앙행정기관의 장과 협의하여 수행한다. <개정 2012. 1. 2.>

제9조의2(사이버위기 대응 훈련) ① 중앙행정기관, 지방자치단체 및 공공기관의 장은 소관 정보통신망을 대상으로 매년 정기적으로 사이버위기 대응 훈련을 실시하여야 한다.
② 국가정보원장은 국가 차원의 사이버위기 발생에 대비하여 중앙행정기관, 지방자치단체 및 공공기관의 정보통신망을 대상으로 사이버위기 대응 통합훈련을 실시할 수 있다. 이 경우 국가정보원장은 특별한 사유가 없으면 사전에 훈련 일정 등을 해당 기관의 장에게 통보하여야 한다.
③ 국가정보원장은 제2항의 훈련 결과 필요하다고 판단하는 경우에는 중앙행정기관, 지방자치단체 및 공공기관의 장에게 필요한 시정조치를 요청할 수 있다. 이 경우 해당 기관의 장은 특별한 사유가 없는 한 그 요청에 따라야 한다.
[본조신설 2012. 1. 2.]

제10조(사이버공격과 관련한 정보의 협력) ① 중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장은 국가정보통신망에 대한 사이버 공격의 계획 또는 공격사실, 사이버안전에 위협을 초래할 수 있는 정보를 입수한 경우에는 지체없이 그 사실을 국가안보실장 및 국가정보원장에게 통보하여야 한다. 다만, 수사사항에 대하여는 수사기관의 장이 국가기밀의 유출·훼손 등 국가안보의 위협을 초래한다고 판단되는 경우에 입수한 정보를 국가안보실장 및 국가정보원장에게 통보하여야 한다. <개정 2013. 9. 2.>
②국가정보원장은 제1항의 규정에 의하여 관련 정보를 제공받은 경우에는 대응에 필요한 조치를 강구하고 그 결과를 정보를 제공한 해당기관의 장에게 통지한다.

제10조의2(보안관제센터의 설치·운영) ① 중앙행정기관의 장, 지방자치단체의 장 및 공공기관의 장은 사이버공격 정보를 탐지·분석하여 즉시 대응 조치를 할 수 있는 기구(이하 "보안관제센터"라 한다)를 설치·운영하여야 한다. 다만, 보안관제센터를 설치·운영하지 못하는 경우에는 다른 중앙행정기관(국가정보원을 포함한다)의 장, 지방자치단체의 장 및 관계 공공기관의 장이 설치·운영하는 보안관제센터에 그 업무를 위탁할 수 있다.
② 보안관제센터를 설치·운영하는 기관의 장은 수집·탐지한 사이버공격 정보를 국가정보원장 및 관계 기관의 장에게 제공하여야 한다.
③ 보안관제센터를 설치·운영하는 기관의 장은 보안관제센터의 운영에 필요한 전담직원을 상시 배치하여야 한다.
④ 보안관제센터를 운영하는 기관의 장은 필요한 경우에는 미래창조과학부장관이 지정하는 보안관제전문업체의 인원을 파견받아 보안관제업무를 수행하도록 할 수 있다. 이 경우 보안관제전문업체의 지정·관리 등에 필요한 사항은 미래창조과학부장관이 국가정보원장과 협의하여 정한다. <개정 2013. 5. 24.>
⑤ 제1항의 보안관제센터의 설치·운영 및 제2항의 사이버공격 정보의 제공 범위, 절차 및 방법 등 세부사항은 국가정보원장이 관계 중앙행정기관의 장과 협의하여 정한다.
[본조신설 2010. 4. 16.]

제11조(경보 발령) ① 국가정보원장은 사이버공격에 대한 체계적인 대응 및 대비를 위하여 사이버공격의 파급영향, 피해규모 등을 고려하여 관심·주의·경계·심각 등 수준별 경보를 발령할 수 있다. 다만, 민간분야에 대하여는 미래창조과학부장관이 경보를 발령하고, 국방분야에 대하여는 국방부장관이 경보를 발령하며, 국가정보원장, 미래창조과학부장관 및 국방부장관은 국가차원에서의 효율적인 경보 업무를 수행하기 위하여 경보 관련 정보를 발령 전에 상호 교환하여야 한다. <개정 2008. 8. 18., 2013. 5. 24., 2013. 9. 2.>
②제1항의 규정에 의하여 경보를 발령하였을 때에는 관계 중앙행정기관의 장은 공공기관의 장 및 지방자치단체의 장에게 이를 신속히 전파하고 적절한 조치를 취하여야 한다.
③국가정보원장은 사이버공격이 국가안보에 중대한 위해를 초래할 것으로 판단되는 경우에는 국가안보실장과 협의하여 심각 수준의 경보를 발령할 수 있다. <개정 2008. 8. 18., 2013. 5. 24.>
④국가정보원장은 제1항의 규정에 의한 경보 발령에 필요한 정보를 관계 중앙행정기관의 장에게 요청할 수 있다. 이 경우 관계 중앙행정기관의 장은 특별한 사유가 없는 한 이에 협조하여야 한다.

제12조(사고통보 및 복구) ① 중앙행정기관의 장은 사이버공격으로 인한 사고의 발생 또는 징후를 발견한 경우에는 피해를 최소화하는 조치를 취하고 지체없이 그 사실을 국가안보실장 및 국가정보원장에게 통보하여야 한다. <개정 2013. 9. 2.>
② 지방자치단체의 장 및 공공기관의 장은 사이버공격으로 인한 사고의 발생 또는 징후를 발견한 경우에는 피해를 최소화하는 조치를 취한 후 그 사실을 지체 없이 국가안보실장, 국가정보원장 및 관계 중앙행정기관의 장에게 통보하여야 한다. <개정 2013. 9. 2.>
③국가정보원장은 사이버공격으로 인한 사고의 발생 또는 징후를 발견하거나 제1항 및 제2항의 규정에 의한 통보를 받은 때에는 관계 중앙행정기관의 장에게 사고복구 및 피해의 확산방지에 필요한 조치를 요청할 수 있으며, 요청받은 관계 중앙행정기관의 장은 특별한 사유가 없는 한 이에 협조하여야 한다.

제13조(사고조사 및 처리) ① 국가정보원장은 사이버공격으로 인하여 발생한 사고에 대하여 그 원인 분석을 위한 조사를 실시할 수 있다. 다만, 경미한 사고라고 판단되는 경우에는 해당 기관의 장이 자체적으로 조사하게 할 수 있으며, 이 경우 해당 기관의 장은 사고개요 및 조치내용 등 관련 사항을 국가정보원장에게 통보하여야 한다.
②국가정보원장은 제1항의 규정에 의하여 조사한 결과 범죄혐의가 있다고 판단되는 경우에는 해당 기관의 장과 협의하여 수사기관의 장에게 그 내용을 통보할 수 있다.
③국가정보원장은 사이버공격으로 인하여 그 피해가 심각하다고 판단되는 경우나 주의 수준 이상의 경보가 발령된 경우에는 관계 중앙행정기관의 장과 협의하여 범정부적 사이버위기 대책본부(이하 "대책본부"라 한다)를 구성·운영할 수 있다. <개정 2010. 4. 16.>
④ 사이버공격에 대한 원인분석, 사고조사, 긴급대응 및 피해복구 등의 조치를 취하기 위하여 대책본부 내에 합동조사팀 등 필요한 하부기구를 둘 수 있다. 이 경우 하부기구의 구성·운영 등에 필요한 사항은 국가정보원장이 관계 중앙행정기관의 장과 협의하여 정한다. <신설 2010. 4. 16.>
⑤ 국가정보원장은 제4항에 따른 사고조사 및 피해복구 등의 조치를 위하여 관계 중앙행정기관의 장에게 필요한 인력·장비 및 관련 자료의 지원을 요청할 수 있다. <개정 2010. 4. 16.>
⑥ 국가정보원장은 사이버공격에 의한 피해 및 대책본부의 대응 상황을 국가안보실장에게 통보하고, 국가안보실장은 이를 종합하여 대통령에게 보고한다. <신설 2013. 9. 2.>

제14조(전문기관간 협력) ① 사이버안전업무를 전담하는 전문기구를 운영하는 기관은 국가사이버안전업무를 효율적으로 수행하기 위하여 다음 각호의 사항을 상호 긴밀히 협력하여야 한다.
1. 사이버위협 관련 정보의 탐지 및 정보공유체계의 구축·운영
2. 사이버안전 관련 정보의 분석·전파
3. 사이버안전 위해 요소에 대한 조치방안
4. 공격기법 분석 및 공격차단 등 대응방안
5. 그 밖에 경보의 수준별 세부 대응조치 등 필요한 사항
②사이버안전센터장은 제1항의 규정에 의한 전문기구를 운영하는 기관간 협력을 원활하게 하기 위하여 관계전문가 회의를 소집할 수 있다.

제15조(연구개발) ① 국가정보원장은 국가사이버안전에 필요한 기술개발과 기술수준의 향상을 위하여 필요한 시책을 추진할 수 있다.
②중앙행정기관의 장은 공공분야의 사이버안전 관련 기술의 확보를 위하여 「과학기술분야 정부출연연구기관 등의 설립·운영 및 육성에 관한 법률」 제8조제1항의 규정에 의하여 설립된 한국전자통신연구원의 국가보안기술 연구·개발을 전담하는 부설연구소로 하여금 관련 연구개발을 수행(연구개발을 위하여 보안관제업무를 수행하는 것을 포함한다)하게 할 수 있다. <개정 2010. 4. 16.>
③제2항의 규정에 의한 사이버안전에 필요한 기술의 연구개발에 관한 세부사항은 국가정보원장이 따로 정한다.

제16조(인력양성 및 교육홍보) ① 관계 중앙행정기관의 장은 사이버안전의 기반 조성에 필요한 기술인력을 양성하고 국민의 인식제고를 위하여 다음 각호의 시책을 강구하여야 한다.
1. 사이버안전 관련 전문기술인력의 확보 및 양성
2. 사이버안전 교육프로그램의 개발 및 투자
3. 그 밖에 전문인력 양성, 교육 및 홍보 등에 관하여 필요한 사항
②국가정보원장은 관계 중앙행정기관의 장이 사이버안전과 관련한 전문인력의 양성, 교육 및 홍보를 위하여 필요한 지원을 요청하는 경우 이에 대하여 지원할 수 있다.

제17조(예산) 중앙행정기관의 장은 소관분야와 관련된 사이버안전대책의 수립·시행에 필요한 재정상의 조치를

강구하여야 한다.

제18조(안전성 확인 등에 대한 특례) ① 제9조, 제12조 및 제13조에도 불구하고 국방분야의 사이버안전과 관련한 다음 각호에 대하여는 국방부장관이 그 업무를 수행한다. <개정 2013. 9. 2.>

1. 제9조제4항의 규정에 의한 안전성 확인
2. 삭제 <2013. 9. 2.>
3. 제12조제1항의 규정에 의한 사고통보
4. 제13조제1항의 규정에 의한 사고조사

②국방부장관은 제1항의 규정에 의한 업무를 수행함에 있어 국가안보에 필요하다고 판단되는 경우에는 관련 내용을 국가정보원장에게 통보하여야 한다.

부칙 <제316호, 2013. 9. 2.>

이 훈령은 발령한 날부터 시행한다.