서울특별시 사이버보안에 관한 조례안

검 토 보 고

의 안 번 호	3043

2025. 9. 1.
주택공간위원회
수 석 전 문 위 원

1. 제안경위

○ 2025. 8. 11. 서울특별시장 제출 (2025. 8. 14. 회부)

2. 제안이유

○ AI, 클라우드 등 신기술 발전에 따른 사이버공격·위협의 고도화·지능화에 대비하여 안전하고 신뢰할 수 있는 사이버보안 체계를 구축하여 중단 없는 대시민 서비스를 제공하고자 함

3. 주요내용

가. 기관별 사이버보안관리관 임명 및 사이버보안담당자 지정을 통해 사이버보안 역량을 높이고 책임성을 제고하고자 함

나. 5년 주기 기본계획 수립을 통하여 연속적이고 체계적인 정책을 추진하고자 함

다. 사이버공격·위협으로 인한 사고 발생 시 사고 영향을 최소화하기 위하여 비상대책반 구성·운영 등의 제도적 기반을 마련하고자 함

라. 사이버보안 수준 향상을 도모하기 위하여 국내외 협력체계를 강화하고자 함

마. 사이버보안 업무 및 활동을 조사·점검하기 위하여 연 1회 이상 사이버보안 감사를 실시하고자 함

4. 검토의견 (수석전문위원 윤은정)

○ 이 제정조례안(이하 “조례안”)은 AI, 클라우드 등 신기술 발전에 따른 사이버공격 및 위협이 고도화·지능화되는 상황에 대응하여, 안전하고 신뢰할 수 있는 사이버보안 체계를 구축하고 중단 없는 대시민 서비스를 제공하기 위한 제도적 기반을 마련하려는 것임.

가. 조례 제정의 배경

○ 최근 디지털 전환이 가속화됨에 따라 행정서비스의 전자화·온라인화도 확대되고 있으며, AI·IoT·클라우드 등 신기술 도입 증가로 사이버 위협이 복합·지능화되고 있는 추세임.

< 최근 5년간 서울시 사이버공격·위협 탐지 및 차단 현황 >

구 분	2021년	2022년	2023년	2024년	2025년 (1~7월)
탐지 건수	6,158,233	7,142,393	6,793,449	6,832,921	6,535,555
차단 건수	2,771,204	3,214,076	3,057,052	2,856,161	2,583,053

*출처: 서울시 디지털도시국 정보보안과 제출 자료, ‘25.7월 기준

○ 사이버보안과 관련하여 정부 차원에서는 「전자정부법」, 「정보통신기반보호법」, 「국가정보원법」, 「사이버안보 업무규정」 등 법령이 존재하나,

- 서울시는 「서울특별시 스마트도시 및 정보화 조례」(이하 “스마트도시 조례”) 상 사이버보안 관련 사항을 일부 선언적 규정만 있을 뿐, 실제 운영은 「서울특별시 정보통신 보안업무 처리규칙」(이하 “규칙”)에 따라 시행해 왔음.

○ 2024년 서울시는 정보보안정책을 강화하기 위해 전담조직을 신설(정보보안과)하고, 「서울시 AI기반 사이버보안 종합계획」을 수립('24.8.16.)하는 등 조직적·행정적 체계를 갖추어왔음.

- 서울시는 본청과 직속기관·사업소·자치구가 하나의 통합망으로 연결되어 있는데, 일부 시스템에서 보안사고가 발생할 경우 연쇄적 피해로 확산될 위험이 크며, 출자·출연기관과 연계된 다양한 시스템까지 고려할 때, 사이버보안 안정성, 정책의 지속성과 실효성 담보를 위해 조례로서 명확한 근거를 두려는 것으로 이해됨[1].

○ 참고로, 국회에서는 '국가사이버안보법안'[2]이 논의되고 있어, 국가 차원의 기본 틀이 마련될 예정인바, 서울시가 선제적으로 조례를 제정하고 대응체계를 갖추어 간다면 지방자치단체 차원에서 선도적 사례가 될 것임.

나. 조례안의 주요내용

○ 조례안[3]은 총 26개의 조문과 4개의 부칙으로 이루어져 있고, 그 주요 내용으로는 사이버보안관리관, 기본계획 수립·시행, 자문위원회 설치 및 운영, 사이버보안 감사와 협력체계 구축 등으로 구성됨.

- 아울러, 본 조례안은 기존 "스마트도시 조례"에 규정되어 있던 사이버보안 관련 조항을 이관하여 구체화하고, 규칙에 따라 운영되던 사항을 조례로 격상하며 그 밖의 관리·대응 체계를 구축하는 내용을 신설하였음.

---

1) 「지방자치법」상 규칙은 '집행기관 내부 사무를 규율'하는 데 한정되므로, 조례안과 같이 사이버보안과 관련하여 각급기관(자치구 및 출자·출연기관 등)에 대외적 의무를 부과하기 위해서는 조례에 근거를 두는 것이 타당함. 다만, 과도한 의무 부과는 기관별 여건 차이를 고려하지 못해 실효성을 저하시킬 우려가 있음.

2) [2211450] 국가사이버안보법안(유용원의원 등 10인), 2025.7.11. 발의

3) 조례안은 관계 기관(국정원, 행정안전부 등)의 의견을 조회(6월)하고, 서울시 조례·규칙심의회의 심의·의결을 거치면서 자치법규 입안의 기본원칙(소관사무의 원칙, 법령 우위의 원칙, 법률 유보의 원칙 등)은 준수한 것으로 사료됨.

< 제정조례안의 구성 및 주요내용 >

구 분	조 항	내 용	비고
제1조 ~ 제5조	목적, 정의, 책무 등	· 사이버공격·위협에 체계적이고 효과적 대응 · 사이버보안 강화 및 관계 기관 협력 체계 강화 · 사이버보안 업무가 원활히 수행될 수 있도록 지도·감독	-
제6조 ~ 제9조	사이버보안관리관	· 체계적인 업무 수행을 위한 사이버보안 전담조직 구성·운영에 관한 사항	현행 규칙
	기본(추진)계획 수립	· 사이버보안 업무의 효율적 추진을 위한 계획 수립 · 연도별 추진계획 수립·제출 의무(각급기관)	(신설)
제10조 ~ 제11조	사이버보안 자문위원회	· (역할) 추진성과 평가; 국내외 사이버보안 환경 반영 등 · (구성) 15인 이내: 공무원, 시의원, 외부전문가 등 · (운영) 과반수 출석으로 개의, 과반수 찬성으로 의결	(신설)
제12조 ~ 제15조	사이버보안 업무에 관한 사항	· 사이버보안 교육, 예방 조치, 자체 진단·점검	**조례 이관**
제16조	인공지능 보안 강화	· 신기술 활용에 따른 보안 강화 조치	(신설)
제17조 ~ 제22조	보안관제센터 운영에 관한 사항	· 보안관제센터 설치·운영, 경보 발령 시 조치 · 사고 조사·보고, 비상대책반 구성·운영 · 대응훈련 실시 및 위협정보의 공유	현행 규칙
제23조 ~ 제24조	대내외 협력체계 강화	· 위기 대응 체계 구축 및 포럼 등의 개최 · 정책 조정 및 정보 공유 강화를 위한 협의회 참여	(신설)
제25조 ~ 제26조	사이버보안 감사	· 사이버보안 업무 및 활동 조사·점검 · 위규자 처리기준 마련·시행	**조례 이관**
부칙	경과조치 및 타조례 개정	· 제정에 따른 경과조치 및 관련 조례 개정	-

① 신설 사항

(1) 용어의 정의(안 제2조)

○ **안 제2조**는 사이버보안과 관련된 핵심 용어를 규정하고 있는데, '정보시스템'[4], '정보보호시스템'[5], '정보통신기기등'의 정의를 각 개별 법령으

4) 「전자정부법」 제2조(정의)

로부터 그대로 인용하여 기술하였으나, 정의한 내용상 서로 중복이 많아 혼선의 우려가 있어 보임.

- 따라서, 법 조문을 직접 명시하면서 “정보시스템(보호 대상)→ 정보보호시스템(보호 수단) → 정보통신기기등(구성 요소)”으로 위계적 구조로 재정리하여 각 용어 간 관계를 명확히 하고 불필요한 중복을 최소화할 필요가 있겠음.

○ 한편, **안 제2조제2호의 ‘각급기관’**의 경우, 조례안에서 시장에게 ‘각급기관(의회사무처 포함)’에 대한 추진계획 의무 제출(안 제9조), 자료제출 요구(안 제12조), 감사 실시(안 제25조) 등 권한을 부여하고 있는데,

- 의회사무처의 경우 「지방자치법」에 따라 시장에게 자료제출이나 감사에 응할 의무를 지지 않으므로, ‘각급기관’의 범위에서 의회사무처를 제외하는 것이 바람직할 것임.

제 정 안	수 정 안
제2조(정의) 이 조례에서 사용하는 용어의 뜻은 다음과 같다. 1. (생 략) 2. “각급기관”이란 서울특별시 직속기관·사업소·합의제 **행정기관·의회사무처·자치구**, 「지방공기업법」에 따른 공사·공단 및 「서울특별시 출자·출연 기관의 운영에 관한 조례」에 따른 출자·출연 기관을 말한다. **3. “정보보호시스템”이란 정보의 수집·**	제2조(정의) ----------. 1. (제정안과 같음) 2. ---------- **행정기관·자치구**----------. **3. “정보시스템”이란 「전자정부법」 제**

13. “정보시스템”이란 정보의 수집·가공·저장·검색·송신·수신 및 그 활용과 관련되는 기기와 소프트웨어의 조직화된 체계를 말한다.

5) **「지능정보화 기본법」 제2조(정의)**

15. “정보보호”란 정보의 수집·가공·저장·검색·송신 또는 수신 중 발생할 수 있는 정보의 훼손·변조·유출 등을 방지하기 위한 관리적·기술적 수단(이하 “정보보호시스템”이라 한다)을 마련하는 것을 말한다.

가공·저장·검색·송신 또는 수신 중 발생할 수 있는 정보의 훼손·변조·유출 등을 방지하기 위한 관리적·기술적 수단을 말한다.	2조제13호의 정보시스템을 말한다.
<신 설>	4. “정보보호시스템”이란 「지능정보화 기본법」 제2조제15호에 따른 정보보호시스템을 말한다.
4. “정보통신기기등”이란 정보의 수집·가공·저장·검색·송신·수신 및 그 활용과 관련되는 기기·설비·소프트웨어 및 정보통신서비스를 말한다.	5. (제정안 제4호와 같음)
5. “정보시스템”이란 정보의 수집·가공·저장·검색·송신·수신 및 그 활용과 관련되는 기기와 소프트웨어의 조직화된 체계를 말한다.	<삭 제>
6. (생 략)	6. (제정안과 같음)

(2) 계획수립 및 자문위원회 설치(안 제8조~제11조)

○ **안 제8조**와 **안 제9조**는 사이버보안 기본계획(5년 단위)과 연도별 추진계획의 수립 근거를 마련하여 중장기적 전략과 단기 실행력을 동시에 확보하려는 취지를 담고 있으며, 이는 변화하는 보안 위협에 체계적으로 대응하기 위한 제도적 기반을 마련하려는 것으로 이해됨.

- **안 제9조제2항**에서는 각급기관(자치구, 출자·출연기관 등)에게 연도별 추진계획 제출 의무를 부과하고 있는데, 이는 개인정보 보호 기본계획과는 달리 상위 지침상 시장에게 관할 기관을 포함한 연도 추진계획의 수립 의무를 부과하였기 때문임[6].

6) 「국가 정보보안 기본지침」 **제6조(연도 추진계획 수립)** ① 상급기관(특별시·광역시·도 등)의 장은 매년 해당 기관 및 관할 하급기관(공공기관, 시·군·자치구 등)에 대한 「연도 정보보안업무 추진계획」(「국가사이버안전관리규정」 제9조에 따른 사이버안전대책을 포함한다. 이하 같다)을 수립·시행하여야 한다.

- 다만, 각급기관별 연도별 추진계획의 형식과 내용이 상이할 경우 종합적 관리와 성과분석이 곤란할 수 있으므로, 향후 추진계획 수립 시 서울시가 가이드라인을 정하여 제출받는 것을 고려해 볼 수 있겠음.

제 정 안
제9조(추진계획의 수립) ① 시장은 제8조의 기본계획에 따라 매년 사이버보안 업무에 대한 연도별 추진계획을 수립·시행하여야 한다. ② 각급기관의 장은 매년 해당 기관의 사이버보안 업무에 대한 연도별 추진계획을 수립·시행하고, 시장에게 제출하여야 한다.

- 한편, 서울시는 「서울특별시 디지털재난 대비 및 대응 조례」에 따라 해킹 등 전자적 침해행위[7]로 인한 재난과 자연 재난 등을 대비하기 위한 디지털재난 대비 및 대응을 위한 기본계획(시행계획)을 5년(매년)마다 수립하고 있는데, 사이버보안계획과의 정합성·연계성을 고려할 필요가 있을 것임[8].

○ **안 제10조**와 **안 제11조**는 사이버보안 관련 주요 사항에 대해 전문성과 공정성을 확보하기 위해 자문위원회(비상설)를 설치·운영할 수 있도록 규정하고 있음[9].

---

7) 「정보통신기반 보호법」 제2조(정의)
2. "전자적 침해행위"란 다음 각 목의 방법으로 정보통신기반시설을 공격하는 행위를 말한다.
가. 해킹, 컴퓨터바이러스, 논리·메일폭탄, 서비스거부 또는 고출력 전자기파 등의 방법
나. 정상적인 보호·인증 절차를 우회하여 정보통신기반시설에 접근할 수 있도록 하는 프로그램이나 기술적 장치 등을 정보통신기반시설에 설치하는 방법

8) 디지털재난 대비 및 대응 기본계획 수립 시 침해행위와 관련된 사항은 사이버보안 기본계획을 참고하여 수립하는 등의 연계성이 필요할 것임.

9) 이 조례안은 위원회 신설과 관련하여 조직담당관의 사전검토를 받아 「서울특별시 각종 위원회의 설치·운영에 관한 조례」의 목적과 기본원칙을 준수하였으며, 비상설로 운영키로 결정하였음.
※ 「서울특별시 각종 위원회의 설치·운영에 관한 조례」 제6조(위원회의 설치요건) ③ 제1항에 따라 위원회를 설치할 경우에는 비상설(안건이 발생하면 구성하고, 해당 안건이 심의·의결된 후 자동 해산하는 형태)로 운영하는 것을 원칙으로 한다. 다만 다음 각 호의 경우에는 예외로 한다. <신설 2023.7.24.>
1. 법령에 위원회 설치 및 구성 방법 등이 다르게 명시된 경우
2. 위원회의 회의가 분기별 1회 또는 연간 4회 이상 개최할 것이 예상되어 회의 개최 시마다 위원을 위촉하는 것이 적절하지 않은 경우
3. 안건 발생 후 위원 구성 시 심의의 공정성을 현저히 훼손할 우려가 있는 경우

- 다만, **안 제11조**는 자문위원회 성격과 부합하지 않는 “의결”이라는 용어를 사용하고 있으므로, 이를 수정할 필요가 있겠음.

제 정 안	수 정 안
제11조(위원회 구성) ① ~ ④ (생 략) ⑤ **위원회는** 안건이 발생하면 구성하고, **심의·의결** 후 자동 해산한다. ⑥ 위원회의 회의는 위원 과반수의 출석으로 개의하고 **출석위원 과반수의 찬성으로 의결한다**. ⑦·⑧ (생 략)	제11조(위원회 구성) ① ~ ④ (제정안과 같음) ⑤ **위원회는 비상설로 운영하며,** ---------- **심의·자문** ----------. ⑥ ---------- **회의결과는 출석위원 과반수의 찬성으로 결정한다**. ⑦·⑧ (제정안과 같음)

(3) 신기술 활용에 대한 보안 강화(안 제16조)

○ **안 제16조**는 인공지능(AI), 사물인터넷(IoT), 클라우드 등 신기술을 행정서비스에 적용할 때 발생할 수 있는 새로운 유형의 보안위협에 대응하기 위하여 사전에 보안대책을 수립하고, 시장과 협의토록 하고 있음.

- 한편, **안 제14조제3항**은 각급기관의 장이 정보화사업을 수행할 때 보안대책을 수립·이행하도록 규정하고 있는데, **안 제16조**는 그 중 신기술 특유의 위험에 주목하여 사전 협의 절차를 추가한 것으로, 첨단기술 도입 과정에서 발생할 수 있는 특수 위험을 보완하는 성격을 지님.

- 신기술을 활용하는 과정에서 보안 요구사항을 조기에 반영함으로써 안전한 시스템 구축을 가능하게 하고, 민간 서비스 및 외부 기관과의 연계가 잦은 신기술 도입 시에도 공동의 대응체계를 마련할 수 있어, 시민에게 보다 안전하고 신뢰할 수 있는 디지털 행정환경을 제공하는 기반이 될

것으로 판단됨.

(4) 협력체계 구축 ·협의회(안 제23조~제24조)

○ **안 제23조**와 **안 제24조**는 국가기관, 민간기업, 학계·연구기관 등과의 협력체계를 구축하고, 이를 위한 협의회를 설치·운영할 수 있도록 규정하는 것임.

- 이는 사이버보안 정책의 실효성을 높이고 위협정보 공유·대응 역량을 강화하는 근거를 마련함과 동시에, 서울시가 추진하고 있는 전국 정보보호 정책협의회(**붙임2**)의 제도적 근거를 마련하여 향후 지속성과 안정성을 확보하는 역할을 할 것으로 판단됨.

② 다른 조례(“스마트도시 조례”)로부터 이관 받은 사항

○ **안 부칙 제4조**(다른 조례의 개정)는 “스마트도시 조례” 제21조제2항부터 제5항까지를 삭제[10]하면서 정보보호와 관련된 사항은 조례안을 따르도록 하고 있음.

- 조례 제정에 따라 규범 체계의 정합성을 높이고 중복을 해소하는 효과가 있으나, 내용 중 보안컨설팅 관련 규정만 누락된 것으로 확인되는데, 집행기관에서는 안 제15조의 진단·점검을 통해 컨설팅 효과를 볼 수 있다는 입장임[11].

---

10) 「서울특별시 스마트도시 및 정보화 조례」 제21조(정보보호) ① 시장은 정보를 처리하는 모든 과정에서 정보의 안전한 유통을 위하여 정보보호 시책을 마련하여야 한다.
② 시장은 정보보안 수준향상을 위해 **보안컨설팅**, 교육, 정보보안 진단 및 관리실태 점검을 해야하며, 정보보안 감사 및 조사 등을 시행할 수 있다.
③ 시장은 정보화사업 계획단계부터 완료단계까지 정보보안 대책을 마련해야 하며, 보안성 검토를 이행해야 한다.
④ 시장은 해킹 등 각종 사이버 공격에 상시 대응체계를 운영하여야 하며, 이를 위한 통합관제운영센터를 설립 및 운영해야 한다.
⑤ 그 밖의 정보보호에 관한 사항은 규칙으로 정할 수 있다.

스마트도시 조례 개정	조례안 반영 내용
제21조(정보보호) ① 시장은 정보를 처리하는 모든 과정에서 정보의 안전한 유통을 위하여 정보보호 시책을 마련하여야 한다.	해당 없음
② 시장은 정보보안 수준향상을 위해 **보안컨설팅**, **교육**, **정보보안 진단 및 관리실태 점검**을 해야하며, **정보보안 감사 및 조사** 등을 시행할 수 있다. < **삭 제** >	보안컨설팅 미반영 안 제13조(사이버보안 교육) 안 제15조(사이버보안 자체 진단·점검) 안 제25조(사이버보안 감사)
③ 시장은 정보화사업 계획단계부터 완료단계까지 정보보안 대책을 마련해야 하며, **보안성 검토**를 이행해야 한다. < **삭 제** >	안 제14조(사이버보안 예방 조치 등)
④ 시장은 해킹 등 각종 사이버 공격에 상시 대응체계를 운영하여야 하며, 이를 위한 **통합관제운영센터**를 설립 및 운영해야 한다. < **삭 제** >	안 제17조(보안관제센터 설치·운영)
⑤ 그 밖의 정보보호에 관한 사항은 규칙으로 정할 수 있다. < **삭 제** >	해당 없음
② 그 밖의 정보보호에 관한 사항은 「서울특별시 사이버보안에 관한 조례」에 따른다. < **신 설** >	해당 없음

(5) 사이버보안 업무에 관한 사항(안 제13조~제15조)

○ 안 제13조(**교육**)부터 안 제15조(**진단·점검**)까지는 스마트도시 조례에서 선언적으로 규정되었던 내용을 이관하고, 그동안 규칙에 따라 시행되어 온 절차를 조례안으로 격상하여 법적 안정성과 지속성을 확보하려는 것임.

○ 다만, **안 제14조**는 각급기관의 장이 정보화사업을 추진할 때 보안대책을 수립·이행하도록 하고, 시장은 **보안성 검토**를 실시하며 매월 셋째 주를 '사이버보안 진단의 날'로 지정하여 정기적인 점검을 실시하도록 규정하고 있는데,

- 사이버보안진단의 날의 구체적 시기, 보안대책 수립의 규모·범위 등 행정적·기술적 집행 절차를 조례에 명시할 경우 경직성이 발생한다는 점

11) 진단점검을 통해 기관별 취약점을 확인하고 개선 방향을 제시하는 과정에서 컨설팅적 성격이 자연스럽게 구현될 수 있어 일정 부분 타당성이 인정되나, 향후 규칙 정비 과정에서 진단점검과 컨설팅의 연계성을 보다 명확히 하여 제도의 실효성을 높일 필요가 있겠음.

을 고려하여, 원칙은 조례에 두되, 세부절차는 규칙으로 정하도록 수정하는 것이 바람직하다고 사료됨.

제 정 안	수 정 안
제14조(사이버보안 예방 조치 등) ① (생 략) ② 시장 및 각급기관의 장은 해당 기관의 실정에 맞게 **매월 세 번째 수요일을 사이버보안진단의 날로 지정·시행**하여야 한다. ③ 시장 및 각급기관의 장은 정보화사업을 수행할 때에는 **다음 각 호와 관련된 보안대책을 수립·이행하여야 한다.** 1. ~ 6. (생 략) ④ (생 략)	제14조(사이버보안 예방 조치 등) ① (제정안과 같음) ② ---------- **사이버보안진단의 날을 지정하고, 정기적으로 시행**----------. ③ ---------- **보안대책을 수립·이행하여야 하며, 구체적 범위·방법 등은 규칙으로 정한다.** **<삭 제>** ④ (제정안과 같음)

(6) 보안관제센터 설치·운영(안 제17조~제22조)

○ **안 제17조**는 서울시 및 각급기관의 사이버보안 위협에 신속히 대응하기 위하여 시장이 보안관제센터를 설치·운영하도록 하고, 사이버공격 탐지·차단, 사고 대응 지원, 보안 로그 관리 및 위협정보 공유 등을 주요 기능으로 규정하고 있음.

- 이는 스마트도시 조례에서 규정하고 있던 '통합관제운영센터'('09.12.1.개소)의 명칭을 현행에 맞춰 변경하고, 그 업무내역과 각급기관의 연계 내용을 상세히 규정하려는 것이며[12], 그 내용은 국가정보원에서 운영하는 통합보안관제체계를 준용한 것으로 확인되어 특이사항 없음(**붙임3**).

12) 「서울특별시 스마트도시 및 정보화 조례」 제21조(정보보호)
④ 시장은 해킹 등 각종 사이버 공격에 상시 대응체계를 운영하여야 하며, 이를 위한 통합관제운영센터를 설립 및 운영해야 한다.

○ **안 제18조**부터 **안 제22조**까지는 사이버위기 발생 시 경보 발령, 사고조사·보고, 복구체계, 정기 훈련, 위협정보 공유 등 보안관제센터의 주요 기능을 규정하고 있음.

- 이는 현재까지 규칙에 따라 서울시 내부적으로 개별적으로 운영되던 절차를 조례로 격상하고, 서울시와 각급기관 전반에서 동일한 기준과 절차를 적용하도록 한 점에서 의의가 있겠음.

- 특히, 사이버위기 상황이 발생했을 때 보안관제센터가 중심이 되어 경보 발령(**안 제18조**) → 사고조사 및 보고(**안 제19조**) → 복구체계 마련(**안 제20조**)으로 이어지는 일련의 위기 대응 프로세스를 통일하여 신속하고 체계적인 대응이 가능해질 것임.

- 또한, 실제 위기 상황 이전 단계에서 대응훈련(**안 제21조**)과 위협정보 공유(**안 제22조**)를 통해 보안 역량을 강화하고, 잠재적 위협에 대한 대비 태세를 점검과 함께 기관별 대응 역량을 상향평준화 할 수 있을 것으로 사료됨.

(7) 사이버보안 감사(안 제25조)

○ **안 제25조**는 시장이 각급기관의 사이버보안 업무 및 활동을 연 1회 이상 조사·점검하도록 규정하고 있으며, 그 기준을 「사이버안보 업무규정」에서 위임한 국가 정보보안 기본지침에 두고 있음[13].

---

13) 「국가 정보보안 기본지침」 **제8조(정보보안감사 등)** ① 각급기관의 장은 해당 기관 및 관할 하급기관의 정보보안업무 및 활동을 조사·점검하기 위하여 연1회 이상 정보보안감사를 실시하여야 하며, 이를 위하여 필요한 경우 정보보안담당관을 감사 또는 감찰업무를 수행하는 부서에 배속하여 정보보안감사를 수행하도록 할 수 있다.
② 각급기관의 장이 해당 기관을 자체 감사하는 경우 이외 관할 하급기관에 대한 정보보안감사의 대상 및 주관기관은 다음 각 호와 같다.
1. 산하 공공기관, 군(軍)기관 : 해당 중앙행정기관의 장 또는 지방자치단체의 장
2. 시·도 : 행정안전부장관
3. 시·군·자치구 : 행정안전부장관 또는 시·도 지사

- 현재 서울시는 국가정보원이 매년 실시하는 정보보안 관리실태 평가에서 지속적으로 미흡(100점 만점 중 60점 이하)한 수준을 기록하고 있는바, 사이버보안 감사 제도의 의무화를 통해 서울시와 각급기관 전반의 보안 수준을 정기적으로 점검할 수 있는 근거를 명확히 하고, 이를 바탕으로 취약점을 개선하여 행정 전반의 보안 역량을 강화할 필요가 있겠음.

< 최근 5년간 정보보안 관리실태 평가결과(국가정보원) >

구 분	2020	2021	2022	2023	2024
평가일자	'20.12.10.	'21.11.23.	'22.10.26.	'23.10.26.	'24.10.21.
평가결과	미흡	미흡	미흡	미흡	미흡

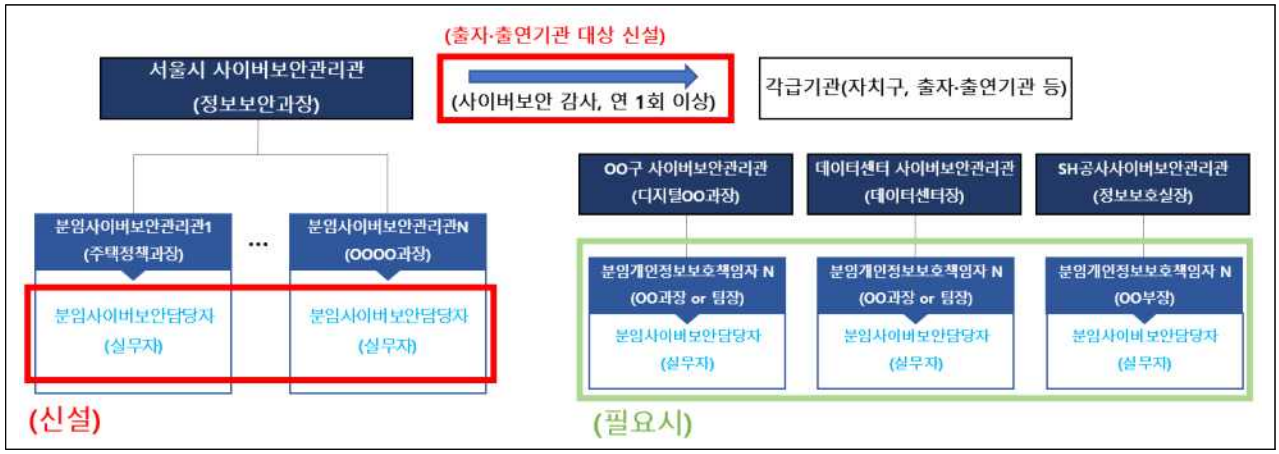
- 다만, 조문에서 법령이 아닌 행정지침(국가정보보안 기본지침)을 따르도록 하고 있어 문제의 소지가 있는바, 지침을 참고하여 시장이 별도로 정하도록 수정할 필요가 있겠음.

제 정 안	수 정 안
제25조(사이버보안 감사) ① 시장은 **「사이버안보 업무규정」 제3조의2제1항제2호의 지침(국가 정보보안 기본지침)에 따라 각급기관등의** 사이버보안 업무 및 활동을 조사·점검하기 위하여 연 1회 이상 사이버보안 감사를 **실시하여야 한다.**	제25조(사이버보안 감사) ① 시장은 **각급기관등의** 사이버보안 업무 및 활동을 조사·점검하기 위하여 연 1회 이상 사이버보안 감사를 **실시하여야 하며, 그 기준과 절차는 「사이버안보 업무규정」 제3조의2제1항제2호의 지침을 준용하여 시장이 정한다.**
② 시장은 제1항에 따른 사이버보안 감사를 실시한 결과 필요한 경우 「공공감사에 관한 법률」에 따른 자체감사기구에 자체감사를 요청할 수 있다.	② (제정안과 같음)
③ 시장은 제15조에 따라 자체 진단·점검을 실시할 때에 각급기관에서 제출한 자료를 제1항에 따른 사이버보안 감사에 활용할 수 있다.	③ (제정안과 같음)

(8) **사이버보안관리관**(안 제6조~제7조, 안 부칙 제3조)

○ **안 제6조부터 제7조**까지는 서울시 및 각급기관에 '사이버보안관리관'과 '사이버보안담당자'를 두고, 이를 보조하는 '분임사이버보안관리관'(이하 "분임관리관")과 '분임사이버보안담당자'**(신설)**(이하 "분임담당자")를 지정(서울시-의무, 각급기관-필요시)하도록 하는 등 다층적 관리체계를 규정하고 있음.

< 사이버보안관리관 운영 예시도 >



- 이는 현행 규칙에서 이미 운영되던 체계를 조례로 격상하여 규범력을 높이는 한편, 실무적으로 운영되고 있던 분임사이버보안담당자를 명시하여, 기관별 책임소재를 명확히 하고 실무의 효율성을 확보한 것으로 사료됨.

○ 다만, **안 부칙 제3조**에 따라 서울시의 '사이버보안관리관'은 디지털도시국 정보보안과장(현행 규칙상 '정보보안담당관')이 되는 상황으로, 분임관리관(서울시 각 부서장(과장))에 대한 업무 감독**(안 제6조제2항제10호)**이 효과적으로 가능할지 의문이 제기되는바,

- **안 제7조제1항**의 분임관리관의 임명에 대해서는 규칙으로 위임하여 실

제 제도를 운영하는 집행기관에서 적정한 기준을 정해 운영토록 할 필요가 있겠음.

- 또한, 안 제7조제3항은 사이버보안관리관 업무의 일부를 분임관리관에게 위임토록 하고 있는데, 조례상 **"위임"**은 법률적 권한 이양으로 오해의 소지가 있으므로, 분임관리관의 업무의 범위[14]에 대해서는 별도로 규칙으로 정할 필요가 있겠음.

제 정 안	수 정 안
제7조(분임사이버보안관리관 운영) ① 시장은 사이버보안관리관이 직무를 효율적으로 수행할 수 있도록 각 부서의 분임사이버보안관리관을 임명하고, 이를 보조할 분임사이버보안담당자를 지정하여야 한다. **별도로 임명하지 않은 경우 각 부서의 장을 분임사이버보안관리관으로 임명한 것으로 본다.** ② (생 략) **③ 제6조제2항 및 제3항에 따른 사이버보안관리관은 업무를 수행하는 데에 필요한 경우 해당 업무의 일부를 분임사이버보안관리관에게 위임할 수 있다.**	제7조(분임사이버보안관리관 운영) ① ---------- ---------- ---------- ---------- ---------- -. **이 경우, 분임사이버보안관리관의 자격요건, 임명 절차 및 업무범위 등 필요한 사항은 규칙으로 정한다.** ② (제정안과 같음) <삭 제>

- 한편 디지털도시국에서는 제도의 효율적 운영을 위해 규칙에서 각급기관별 직급기준과 자격, 역할 등을 명시할 필요가 있겠으며, 분임관리관과 분임담당자에 대한 가이드라인 마련과 함께 지속적인 교육이 필요하겠음.

14) 분임사이버보안관리관은 사이버보안관리관을 보조하기 위한 제도로, 사이버보안관리관의 업무의 일부를 대신하는 것이 아닌 분임관리관이 소관하는 각 부서의 정보시스템 등에 대한 사이버보안 현황을 점검하는 등 역할을 규정하여야 할 것임.

다. 종합의견

○ 종합하면, 조례안은 AI·클라우드 등 신기술 확산에 따른 사이버공격의 복합·지능화에 대응하여, 서울시와 산하기관 전반에 걸쳐 통합적이고 지속가능한 보안 체계를 마련하려는 것으로, 조례 제정을 통해 규칙 수준의 내부 규범에 머물던 사항을 상위 자치법규로 격상했다는 점에서 의의가 있겠음.

- 다만, 정의 규정의 중복·혼선, 의회사무처에 대한 의무 부과 관련 포함의 법적 근거 미비, 추진계획·진단의 날 등 일부 조항의 경직성 해소를 위한 규칙 위임 등은 보완이 필요함.

- 디지털도시국은 조례안의 실효적 운영을 위하여 가이드라인을 마련하여 각급기관과의 원활한 소통을 도모하고, 서울시 및 각급기관의 보안 수준을 제고하며 위기 대응 역량을 강화하는 한편, 조례안 제정에 따른 규칙의 정비(제명, 규정 체계의 일관성, 위계 정합성 등)를 조속히 시행하는 것이 바람직할 것임.

- 또한 분임관리관과 관련하여 디지털도시국 소관으로 2개의 분임제도(개인정보보호, 사이버보안)를 운영할 예정인 바, 서울시 각 부서에서 이를 혼용하지 않도록, 일관된 기준과 매뉴얼을 마련·배포하여 각 분임관리관 제도가 효율적이고 내실 있게 운영될 수 있도록 관리·지원해 나가야 할 것임.

의안심사지원팀장 강대만	02-2180-8204
입 법 조 사 관 김태훈	02-2180-8203

붙임1 관계법령

■ 「전자정부법」

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

13. **“정보시스템”** 이란 정보의 수집ㆍ가공ㆍ저장ㆍ검색ㆍ송신ㆍ수신 및 그 활용과 관련되는 기기와 소프트웨어의 조직화된 체계를 말한다.

제24조(전자적 대민서비스 보안대책) ① 행정안전부장관은 전자적 대민서비스와 관련된 보안대책을 국가정보원장과 사전 협의를 거쳐 마련하여야 한다. <개정 2013. 3. 23., 2014. 11. 19., 2017. 7. 26.>

② 중앙행정기관과 그 소속 기관 및 지방자치단체의 장은 제1항의 보안대책에 따라 해당 기관의 보안대책을 수립ㆍ시행하여야 한다.

■ 「지능정보화 기본법」

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

15. **“정보보호”** 란 정보의 수집ㆍ가공ㆍ저장ㆍ검색ㆍ송신 또는 수신 중 발생할 수 있는 정보의 훼손ㆍ변조ㆍ유출 등을 방지하기 위한 관리적ㆍ기술적 수단(이하 **“정보보호시스템”** 이라 한다)을 마련하는 것을 말한다.

제60조(안전성 보호조치) ① 과학기술정보통신부장관은 행정안전부장관 등 관계 기관의 장과 협의하여 지능정보기술 및 지능정보서비스의 안전성을 확보하기 위하여 다음 각 호와 같은 필요한 최소한도의 보호조치의 내용과 방법을 정하여 고시할 수 있다.

1. 지능정보기술과 지능정보서비스의 오작동 방지에 관한 사항
2. 지능정보기술 및 지능정보서비스에 대한 권한 없는 자의 접근, 조작 등 전자적 침해행위의 방지에 관한 사항
3. 지능정보기술 및 지능정보서비스의 접속기록, 운용ㆍ활용기록의 저장ㆍ관리 및 제공 등에 관한 사항
4. 지능정보기술의 동작 및 지능정보서비스 제공을 외부에서 긴급하게 정지하는 것(이하 **“비상정지”** 라 한다)과 비상정지에 필요한 알고리즘의 제공에 관한 사항
5. 기타 지능정보기술 및 지능정보서비스의 안전성 확보를 위해 필요한 사항

② 과학기술정보통신부장관은 지능정보기술을 개발 또는 활용하는 자와 지능정보서비스

를 제공하는 자에게 제1항에 따른 고시가 정하는 바에 따라 안전성 보호조치를 하도록 권고할 수 있다.

③ 중앙행정기관의 장은 사람의 생명 또는 신체에 대한 긴급한 위해를 방지하기 위하여 필요한 때에는 지능정보기술을 개발 또는 활용하는 자와 지능정보서비스를 제공하는 자에게 비상정지를 요청할 수 있다. 이 경우 요청받은 자는 정당한 사유가 없으면 이에 응하여야 한다.

■ 「사이버안보 업무규정」

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

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.]

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 교육과정

을 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.>

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.

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.>

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.>

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 사이버

공격·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.>

■ 「서울특별시 스마트도시 및 정보화 조례」

제21조(정보보호) ① 시장은 정보를 처리하는 모든 과정에서 정보의 안전한 유통을 위하여 정보보호 시책을 마련하여야 한다.

② 시장은 정보보안 수준향상을 위해 보안컨설팅, 교육, 정보보안 진단 및 관리실태 점검을 해야하며, 정보보안 감사 및 조사 등을 시행할 수 있다.

③ 시장은 정보화사업 계획단계부터 완료단계까지 정보보안 대책을 마련해야 하며, 보안성 검토를 이행해야 한다.

④ 시장은 해킹 등 각종 사이버 공격에 상시 대응체계를 운영하여야 하며, 이를 위한 통합관제운영센터를 설립 및 운영해야 한다.

⑤ 그 밖의 정보보호에 관한 사항은 규칙으로 정할 수 있다.

붙임2 서울시 전국 정보보호정책협의회 운영 현황

○ **협의회명: 전국 정보보호정책협의회**

○ **추진목표: 전국 지자체·공공기관, 중앙정부 등 유관기관 간 협력체계 활성화**

○ **주요내용: 정보보호·개인정보보호에 대한 정보보호정책 및 기관 간 협력사항 등 공유를 위한 합동 콘퍼런스·포럼 등 개최**

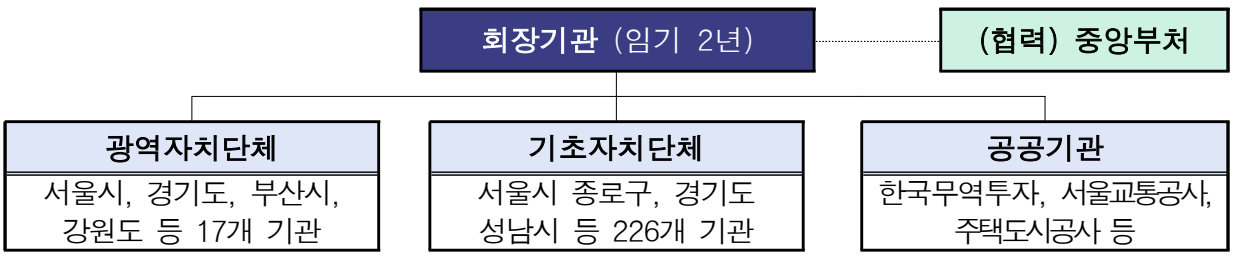
○ **사업기간: '25. 1. ~ 12.**

○ **사업예산: 10,000천원**

○ **회원기관: 381개 지자체 및 공공기관**(16개 광역, 105개 기초, 260개 공공기관)

※ 지자체 출자·출연기관의 정보보호 수준강화를 위해 '25년부터 공공기관까지 확대

○ **협력기관: 중앙부처**(과기부, 국정원, 개인정보보호위원회, 행안부, 국방부 등)



- 회장기관: 정보 공유 및 협력 강화를 위한 정기·임시회의 개최 등

○ **회의주기 : 정기회의 연 2회**(임시회의 필요시 개최)

○ **주요기능**

① 국가 新보안체계 적용을 위한 지자체·공공기관 간 기술·정보 공유 등 협력
② 지자체·공공기관을 대표로 중앙부처 및 유관기관 등에 대한 협의당사자 역할
③ 지자체·공공기관 간 정보보호·개인정보보호 정책 공유 및 사이버보안 종합대책 수립 협력
④ 新보안기술의 지자체·공공기관 도입·적용을 위한 기술 협력(AI보안관제, 제로트러스트 등)
⑤ 중앙부처에 정보보호·개인정보보호 국비지원, 인력확충 및 담당자 인센티브(수당, 승진 등) 등에 관한 사항 지자체·공공기관 의견 공유 및 정책 제안
⑥ AI기반 사이버위협 공동 대응을 위한 각급기관 간 AI학습데이터 공유 등
⑦ 보안 관련 국내·외 유관기관 대상 정책 및 교육 등 협력 강화(국내 연구기관·보안기업 및 국외 미국·영국·일본 등)

○ **추진실적**

- 중앙정부 협력 정기총회 및 세미나 개최 4회 ('24. 11., '25. 2., '25. 3., '25. 8.)

붙임3 사이버안보 업무규정 및 조례안의 보안관제센터 관련 조문 비교표

사이버안보 업무규정	제 정 안
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.>	제17조(보안관제센터 설치·운영) ① 시장은 각급기관등에 대한 사이버공격·위협을 즉시 탐지·대응(이하 “보안관제”라 한다)하기 위하여 보안관제센터를 설치·운영하여야 한다.
	② 보안관제센터는 다음 각 호의 업무를 수행한다. 1. 각급기관등의 정보보호시스템에서 생성된 로그의 수집 및 저장 2. 각급기관등에 대한 사이버공격·위협 탐지 및 분석 3. 각급기관등에 대한 사이버공격·위협 대응 및 초동 조치 4. 각급기관등에 대한 사이버공격·위협으로 인한 사고 조사 5. 각급기관등에 대한 사이버공격·위협에 대응하기 위한 훈련
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 각급기관의 장은 해당 기관의 보안관제를 위하여 제1항에 따른 보안관제센터와 연계된 보안관제센터를 설치·운영하여야 한다. 다만, 해당 기관의 규모와 소관 업무의 성질 등을 고려하여 다른 기관이 운영하는 보안관제센터를 활용하는 것이 더 효율적인 경우에는 직접 설치하지 않고 다른 기관의 보안관제센터를 활용할 수 있다.
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.>	④ 시장은 제1항에 따른 보안관제를 위하여 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제4호에 따른 클라우드컴퓨팅서비스 제공자에게 필요한 협조 또는 지원을 요청할 수 있다.