심 사 보 고 서

충청북도 공공기관 사이버보안에 관한 조례안

충청북도 공공기관 사이버보안에 관한 조례안

심 사 보 고 서

의안 번호	798

2024. 12. 11.(수)
행정문화위원회

1. 심사경과

가. 발 의 자 : 안지윤 의원 등 7인

나. 발의일자 : 2024년 11월 15일

다. 회부일자 : 2024년 11월 15일

라. 상정일자 : 2024년 11월 28일

- 제422회 충청북도의회 정례회 제4차 행정문화위원회 : 상정・의결

마. 주요내용

- 제안설명, 검토보고, 질의답변, 심사의결(원안의결)

2. 제안 설명 요지(제안설명자 : 안지윤 의원)

가. 제안사유

○ 날로 진화하는 사이버 위협에 대응하고 도와 산하 공공기관을 포함한 사이버보안 업무의 효율적, 체계적 수행을 위해 필요한 내용을 규정하고자 함.

나. 주요내용

○ 공공기관 사이버보안에 관한 추진계획 수립에 대하여 규정함(안 제5조).

○ 공공기관에 대한 사이버공격·위협이 발생한 경우 이에 대해 취할 수 있는 조치사항을 규정함(안 제7조).

○ 「사이버안보 업무규정」 제7조제2호의2에 따른 사이버보안 업무 대상 출자·출연 기관의 범위를 규정함(안 제8조).

○ 공공기관의 사이버보안 실태 점검에 관한 사항을 규정함(안 제9조).

3. 검토보고 요지(수석전문위원 : 신복순)

○ 본 조례는 충청북도 공공기관의 사이버보안체계를 확립하여 사이버 공격과 위협을 예방하고, 체계적이고 효과적으로 대응할 수 있도록 함으로써 공공기관의 정보 자산을 보호하는 것을 목적으로 함.

○ 조례의 주요 내용을 살펴보면, 안 제2조는 사이버보안, 사이버공격·위협에 대해 정의하고, 동조 제3호에서는「지방공기업법」제49조 및 제79조에 따라 설립한 기업과「지방자치단체 출자·출연 기관의 운영에 관한 법률」제4조에 따른 공공기관이 대상이 됨을 명확히 규정하고 있음.

○ 안 제3조와 제5조에서는 도지사의 책무를 규정하며, 사이버보안의 중요성에 대한 사회적 공감대 형성과 도민 참여 증진, 관련 시책을 종합적으로 추진하도록 하고, 매년 사이버보안 추진계획을 수립하고 시행할 것을 명시함.

○ 안 제6조에서는 효과적인 사이버보안 정책의 수립과 시행을 위해 현황과 실태 조사를 할 수 있도록 규정하고 있으며, 안 제7조에서는 사이버공격·위협 발생 시 원인분석, 악성프로그램 차단, 보안 취약점 제거 등 구체적인 대응조치 사항 등을 포함하고 있음.

○ 안 제8조는 사이버보안 업무 대상이 되는 출자출연기관의 범위를 규정하고 있으며, 제9조는 공공기관 사이버보안 대책 수립·이행 여부 및 실태 점검을 통해 보안 수준 강화를 도모하며, 실태 점검 결과 미흡 시 보완대책을 마련하고 도지사에게 기술적 지원을 요청할 수 있도록 하여 실질적 실행력을 확보하고 있음.

○ 본 조례안은 공공기관의 사이버보안 체계 강화를 통해 개인정보, 대외비 등 사이버상에서 공공기관의 정보보호 수준을 강화하고 안전을 확보할 수 있도록 체계 확립과 관련된 구체적인 사항을 조례로 규정하는 것으로 제정의 필요성과 내용이 타당한 것으로 판단됨.

4. 질의 및 답변요지 : “생략”

5. 토 론 요 지 : “생략”

6. 심 사 결 과 : “원안가결”

7. 소 수 의 견 요 지 : “없음”

8. 기타 필요한 사항 : “없음”

9. 심사보고서 첨부서류

○「충청북도 공공기관 사이버보안에 관한 조례안」

충청북도조례 제 호

충청북도 공공기관 사이버보안에 관한 조례

제1조(목적) 이 조례는 충청북도 공공기관 사이버보안체계를 확립하고 사이버공격·위협의 예방 및 대응에 관한 사항을 규정함으로써 도민 권익 보호에 이바지함을 목적으로 한다.

제2조(정의) 이 조례에서 사용하는 용어의 뜻은 다음과 같다.

1. “사이버보안”이란 전자적 침해행위로부터 사이버공간과 정보의 안전성·신뢰성을 확보하기 위한 모든 활동 및 그 활동을 통해 안전하게 보호되는 상태를 말한다.
2. “사이버공격·위협”이란 해킹, 컴퓨터 바이러스, 서비스거부(DDoS: Distributed Denial of Service), 전자기파 등 전자적 수단에 따라 정보통신기기, 정보통신망 또는 이와 관련된 정보시스템을 침입·교란·마비·파괴하거나 정보를 위조·변조·훼손·절취하는 행위 및 그와 관련된 위협을 말한다.
3. “공공기관”이란 다음 각 목에 따른 기관을 말한다.

가. 「지방공기업법」 제49조 및 제76조에 따라 충청북도(이하 “도”라 한다)가 설립한 기업

나. 「지방자치단체 출자·출연 기관의 운영에 관한 법률」 제4조에 따라 도가 설립한 출자·출연 기관

제3조(도지사의 책무) ① 충청북도지사(이하 “도지사”라 한다)은 공공기관의 사이버보안 중요성에 대한 사회적 공감대를 형성하고 도민의 참여를

증진하기 위해 노력해야 한다.

② 도지사는 공공기관에 대한 사이버공격·위협 예방·대응, 사이버보안 기반 조성 등 사이버보안 관련 시책을 종합적으로 추진해야 한다.

제4조(다른 조례와의 관계) 공공기관의 사이버보안에 관해 다른 조례에 특별한 규정이 있는 경우를 제외하고 이 조례에서 정하는 바에 따른다.

제5조(추진계획 수립) 도지사는 공공기관에 대한 사이버공격·위협에 대응하기 위한 시책을 포함하는 사이버보안 추진계획을 매년 수립·시행해야 한다.

제6조(실태 조사) 도지사는 공공기관의 사이버보안에 관한 정책의 효과적인 수립·시행에 필요한 사이버보안 현황과 실태를 조사할 수 있다.

제7조(사이버공격·위협 대응조치) ① 도지사는 공공기관에 대한 사이버공격·위협에 대비하기 위해 원인분석 등 필요한 조사를 할 수 있다.

② 도지사는 공공기관의 사이버공격·위협에 대한 대응, 복구 및 피해확산 방지를 위해 다음 각 호의 조치를 할 수 있다.

1. 사이버공격·위협 관련 악성프로그램의 제공 요청, 삭제 또는 차단
2. 사이버공격·위협 관련 정보의 공유 및 공개
3. 보안취약점의 차단 및 피해확산 방지 조치
4. 그 밖에 사이버공격·위협에 효과적으로 대응하기 위해 필요하다고 인정되는 조치

③ 도지사는 공공기관의 장에게 소관 분야에서 발생한 사이버공격·위협에 따른 피해 확산 방지를 위해 제1항 및 제2항의 조치를 하도록 요구할 수 있다. 공공기관의 장은 특별한 사유가 없으면 이에 따라야

한다.

제8조(사이버보안 업무 대상 출자·출연 기관의 범위) ①「사이버안보 업무규정」제7조제2호의2에서 “조례로 정하는 기관”이란「지방자치단체 출자·출연 기관의 운영에 관한 법률」제2조에 따른 출자·출연 기관으로서 도가 설립한 출자·출연 기관을 말한다.

② 제1항에 따른 기관 중 도의 지분이 100분의 50 미만인 출자 기관에 대해서는 이 조례를 적용하지 않는다. 다만,「지방자치단체 출자·출연 기관의 운영에 관한 법률」제2조제3항 각 호의 어느 하나에 해당하는 경우는 예외로 한다.

제9조(사이버보안 실태 점검 등) ① 도지사는 공공기관을 대상으로 사이버보안 대책의 수립·이행 여부를 확인하고 사이버공격·위협 및 예방·대응 등 사이버보안에 관한 실태 점검을 할 수 있다.

② 도지사는 제1항에 따른 실태 점검 결과를 해당 공공기관의 장에게 통보해야 한다.

③ 공공기관의 장은 제2항에 따라 제1항에 따른 실태 점검 결과가 미흡하다고 통보 받은 경우 그 보완대책을 마련해 도지사에게 통보해야 한다. 이 경우 공공기관의 장은 보완대책 이행을 위해 도지사에게 기술적 지원을 요청할 수 있다.

제10조(사업 추진) 도지사는 공공기관의 사이버보안을 위해 다음 각 호의 사업을 추진할 수 있다.

1. 사이버보안 관련 전문 인력 양성
2. 사이버보안 관련 산업 육성

3. 사이버보안에 관한 도민의 인식 제고를 위한 교육훈련·홍보

4. 그 밖에 도지사가 사이버보안을 위해 필요하다고 인정하는 사업

제11조(비밀 준수의 의무) 이 조례에 따라 사이버보안 업무에 종사하거나 종사했던 사람은 그 직무상 알게 된 비밀을 다른 사람에게 누설하거나 직무상 목적 외의 용도로 이용해서는 안 된다.

부 칙

이 조례는 공포한 날부터 시행한다.