



제 432회 국회 (임시회)
제3차 과학기술정보방송통신위원회

클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 일부개정법률안

검 토 보 고

〈클라우드컴퓨팅서비스 제공자 보안인증 강화 등〉
■ 최형두의원 대표발의(의안번호 제2216227호)

2026. 2.

과학기술정보방송통신위원회
수석전문위원 이복우

목 차

I. 제안경위	1
II. 제안이유 및 주요내용	1
III. 검토의견	3
1. 클라우드컴퓨팅서비스 제공자 보안인증 강화(안 제23조제3항 및 제23조의2제2항 신설)	3
2. 클라우드컴퓨팅서비스 제공자의 정보보호최고책임자 지정 의무(안 제23조의5 신설)	12

I. 제안경위

가. 발 의 자 : 최형두의원 등 14인

나. 발 의 일 : 2026. 1. 22.

다. 회 부 일 : 2026. 1. 23.

II. 제안이유 및 주요내용

제안이유

최근 디지털 전환의 핵심 인프라로 클라우드 이용이 확산되고 있으나, 클라우드컴퓨팅서비스 제공자와 이용 기업 간의 보안 책임이 모호하여 보안 사각지대가 발생하고 있음. 특히 외부 협력사의 보안 취약점이나 클라우드 접근 권한 설정 오류가 대규모 정보 유출 사고의 주원인이 되고 있음에도 불구하고, 이에 대한 규제는 미비한 실정임.

현행법은 클라우드 보안인증(CSAP) 제도를 운영하고 있으나, 이는 주로 국가 및 공공기관 납품을 위한 요건으로 작용할 뿐 민간 대형 클라우드 이용 기업이나 제공자에게는 강제성이 없어 실효적인 보안 관리에 한계가 있다는 지적이 제기됨. 또한, 클라우드 서비스의 복잡성에 비해 내부 보안 감사나 접근 통제는 기업의 자율에 맡겨져 있어 사고 발생 시 원인 규명과 신속한 대응이 어려운 상황임.

이에 일정 규모 이상의 클라우드컴퓨팅서비스 제공자에 대해 보안 인증을 의무화하여 민간 영역의 보안 수준을 공공 수준으로 상향 평

준화하고, 클라우드 전문 정보보호 최고책임자 지정 및 정기적인 보안 감사를 통해 사고 예방 및 원인 규명 체계를 강화하려는 것임.

주요내용

- 가. 클라우드 보안인증기준에 원격 접속자 및 수탁 사업자를 포함한 계정별 식별·인증과 차등적 접근통제, 이용자 정보 유출 방지 및 서비스 안정성 확보를 위한 기술적·물리적 보호조치 항목을 명시하여 공급망 보안 위협에 대응하도록 함(안 제23조제3항 신설).
- 나. 매출액 및 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 클라우드컴퓨팅서비스 제공자의 경우 의무적으로 보안인증을 받도록 하여 이용자 보호를 강화함(안 제23조의2제2항 신설).
- 다. 클라우드컴퓨팅서비스 제공자로 하여금 정보보호 최고책임자를 지정하여 과학기술정보통신부장관에게 신고하도록 하고, 정기적인 감사 및 개선 관련 자료를 의무적으로 보관하도록 함(안 제23조의5 신설).

Ⅲ. 검토의견

1. 클라우드컴퓨팅서비스 제공자 보안인증 강화(안 제23조제3항 및 제23조의2제2항 신설)

가. 개정안 요지

- 과학기술정보통신부장관은 다음의 사항을 포함한 클라우드컴퓨팅서비스의 보안인증기준을 정하여 고시하고 클라우드컴퓨팅서비스 제공자에게 그 기준을 지킬 것을 권고할 수 있음(안 제23조제3항 신설)
- 매출액, 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 클라우드컴퓨팅서비스 제공자는 클라우드컴퓨팅서비스에 대한 보안인증을 받아야 함(안 제23조의2제2항 신설).
- 클라우드컴퓨팅서비스의 보안인증 의무를 이행하지 않은 경우 3천만원 이하의 과태료를 부과함(안 제37조제1항).

나. 개정안 조문대비표

현 행	개 정 안
제23조(신뢰성 향상) ① (생략)	제23조(신뢰성 향상) ① (현행과 같음)
② 과학기술정보통신부장관은 클라우드컴퓨팅서비스의 품질	② -----
· 성능에 관한 기준 및 정보보호에 관한 기준(관리적·물리	-----

	-----의

현행	개정안
<u>적·기술적 보호조치를 포함한다.</u> 이하 “보안인증기준”이라 한다)을 정하여 고시하고, 클라우드컴퓨팅서비스 제공자에게 그 기준을 지킬 것을 권고할 수 있다. <u><신 설></u>	<u>하</u>----- ----- ----- ----- -----. ③ <u>보안인증기준에는 다음 각 호의 사항이 포함되어야 한다.</u> 1. <u>정당한 권한이 없는 자가 클라우드컴퓨팅서비스에 접근·침입하는 것을 방지하거나 대응하기 위한 기술적·물리적 보호조치</u> 2. <u>원격 접속자·수탁 사업자를 포함한 계정별 식별·인증과 차등적 접근통제 등에 관한 기술적·물리적 보호조치</u> 3. <u>이용자 정보의 불법 유출·위조·변조·삭제 및 내부자의 이상 행위 또는 접근 권한 오남용 등을 방지하기 위한 기술적 보호조치</u> 4. <u>클라우드컴퓨팅서비스의 지속적인 이용이 가능한 상태를 확보하기 위한 기술적·물리</u>

현행	개정안
③ (생략) 제23조의2(클라우드컴퓨팅서비스의 보안인증) ① (생략) <u><신설></u> ② ~ ⑦ (생략) ⑧ 제1항에 따른 보안인증의 대상, 제2항에 따른 유효기간의 연장, 제5항 및 제6항에 따른 인증기관 및 평가기관 지정의 기준·절차·유효기간 등에 필요한 사항은 대통령령으로 정한다. 제23조의4(인증기관 및 평가기관의 지정취소 등) ① 과학기술정보통신부장관은 제23조의2제	<u>적 보호조치</u> 5. 클라우드컴퓨팅서비스의 안정 및 정보보호를 위한 인력·조직·경비의 확보 및 관련 계획수립 등 관리적 보호조치 ④ (현행 제3항과 같음) 제23조의2(클라우드컴퓨팅서비스의 보안인증) ① (현행과 같음) ② 매출액, 이용자 수 등이 대통령령으로 정하는 기준에 해당하는 클라우드컴퓨팅서비스 제공자는 제1항에 따른 인증을 받아야 한다. ③ ~ ⑧ (현행 제2항부터 제7항까지와 같음) ⑨ ----- -----제3항에----- -----제6항 및 제7항에----- ----- ----- -----. 제23조의4(인증기관 및 평가기관의 지정취소 등) ① ----- -----제23조의2

현행	개정안
5항 또는 같은 조 제6항에 따라 인증기관 또는 평가기관으로 지정받은 법인 또는 단체가 다음 각 호의 어느 하나에 해당하면 그 지정을 취소하거나 1년 이내의 기간을 정하여 해당 업무의 전부 또는 일부의 정지를 명할 수 있다. 다만, 제1호 또는 제2호에 해당하는 경우에는 그 지정을 취소하여야 한다. 1. ~ 4. (생략) 5. 제23조의2제8항에 따른 지정기준에 적합하지 아니하게 된 경우 ② (생략) 제37조(과태료) <신설> ① 다음 각 호의 어느 하나에 해당하는 자에게는 1천만원 이하의 과태료를 부과한다.	제6항-----제7항에 ----- ----- ----- ----- ----- ----- ----- ----- ----- ----- ----- 1. ~ 4. (현행과 같음) 5. 제23조의2제9항에----- ----- ----- ② (현행과 같음) 제37조(과태료) ① 제23조의2제2항을 위반하여 보안인증을 받지 아니한 자에게는 3천만원 이하의 과태료를 부과한다. ② ----- ----- ----- ----- -----

현행	개정안
1. 제23조의2제4항을 위반하여 보안인증 표시 또는 이와 유 사한 표시를 한 자	1. 제23조의2제5항을----- ----- -----

다. 검토사항

- 현행 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」(이하 “클라우드컴퓨팅법”)에 따르면 과학기술정보통신부장관은 관리적·물리적·기술적 보호조치를 포함한 보안인증기준을 고시하여 클라우드컴퓨팅 서비스 제공자(CSP, Cloud Service Provider)에게 그 기준을 지킬 것을 권고할 수 있음.
- 이에 따라, 과학기술정보통신부장관은 「클라우드컴퓨팅서비스 보안인증에 관한 고시」¹⁾를 정하여 시행 중이고 별표로 관리적·물리적·기술적 보호조치를 규정하고 있음.
- 그리고, 과학기술정보통신부장관은 정보보호 수준의 향상·보장을 위해 보안인증기준에 적합한 클라우드컴퓨팅서비스에 사업자의 신청을 받아 대통령령으로 정하는 바에 따라 보안인증(CSAP; Cloud Security Assurance Program)을 할 수 있음²⁾.

1) 과학기술정보통신부고시 제2023-4호

2) 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」

제23조의2(클라우드컴퓨팅서비스의 보안인증) ① 과학기술정보통신부장관은 정보보호 수준의 향상 및 보장을 위하여 보안인증기준에 적합한 클라우드컴퓨팅서비스에 대하여 대통령령으로 정하는 바에 따라 인증(이하 “보안인증”이라 한다)을 할 수 있다.

「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 시행령」

- 최근, 기업뿐만 아니라 개인이 저장·처리해야 하는 데이터의 규모가 지속해서 증가하고 있는 만큼 클라우드컴퓨팅서비스 산업도 점차 성장함에 따라 클라우드컴퓨팅서비스의 정보보호도 중요해지고 있음.
- 그런데, 현재 과학기술정보통신부장관이 고시하는 보안인증기준은 권고사항으로 CSP가 이를 준수할 의무는 없으며 자발적인 참여를 유인하기 위하여 CSAP 제도를 운영하고 있으나 인증 표시가 허용되는 것 외에 CSP가 CSAP를 받을 유인은 공공부문에 클라우드컴퓨팅서비스를 제공할 때 받는 국가정보원의 보안성 검증 일부가 간소화된다는 것뿐임.
- 클라우드컴퓨팅법 시행령 제15조의6제8항에 따르면 국가기관등이 이용하는 클라우드컴퓨팅서비스의 보안인증기준은 국가정보원장과, 이용 안전성 확보에 관한 사항은 행정안전부장관과 미리 협의하도록 규정하고 있는데 이에 따라 정부는 국가정보원의 보안성 검증 중 CSAP와 중복되는 부분은 절차를 간소화하고 있음.
- 이에, 개정안은 보안인증기준에 포함하여야 할 관리적·물리적·기술적 보호조치의 내용을 대략적으로 법률에 명시하여 보호인증기준의 법적

제15조의6(클라우드컴퓨팅서비스의 보안인증 절차 등) ① 법 제23조의2제1항에 따라 클라우드컴퓨팅서비스에 대한 보안인증(이하 "보안인증"이라 한다)을 받으려는 자는 과학기술정보통신부령으로 정하는 인증 신청서에 다음 각 호의 서류를 첨부하여 보안인증에 관한 업무를 수행하는 한국인터넷진흥원 또는 같은 조 제5항에 따라 지정된 기관(이하 "인증기관"이라 한다)에 제출해야 한다.

1. 법 제23조제2항에 따른 클라우드컴퓨팅서비스의 정보보호에 관한 기준(관리적·물리적·기술적 보호조치를 포함한다. 이하 "보안인증기준"이라 한다)에 적합한지 여부를 확인할 수 있는 서류
2. 보안인증 대상 목록
3. 그 밖에 보안인증에 필요한 사항으로서 과학기술정보통신부장관이 고시하는 사항에 관한 서류

근거를 강화하는 한편, 규모가 큰 일부 CSP에 대해서는 CSAP를 받도록 의무화하여 CSAP 제도의 실효성을 강화하려는 것임.

- 매출액이 크고 이용자가 많은 대형 CSP에 대해서는 CSAP를 의무화하면 클라우드컴퓨팅서비스를 대상으로 하는 침해사고가 발생하여 다수의 이용자에게 피해가 발생하는 문제를 사전에 방지하는 효과가 있을 것으로 보임.

- 참고로, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 “정보통신망법”)에 따른 정보보호 관리체계(ISMS; Information Security Management System) 인증은 정보통신 분야 서비스의 정보보호 수준을 평가·인증한다는 점에서 CSAP와 유사한데, CSAP와 마찬가지로 사업자의 자발적인 참여를 전제로 하되 주요정보통신서비스 제공자 등³⁾에 대해서는 인증을 의무화하고 있음.

- 다만, 개정안은 다음과 같은 사항을 고려할 필요가 있음.
- 먼저, 개정안이 시행되면 구글과 같이 클라우드컴퓨팅서비스를 운영하는 해외 사업자에게도 CSAP 의무가 부과될 것으로 보이는데 이는 통상 마찰로 이어질 우려가 있어 이에 대한 면밀한 검토가 필요함.

3) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

제47조(정보보호 관리체계의 인증) ② 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다.

1. 「전기통신사업법」 제6조제1항에 따른 등록을 한 자로서 대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자(이하 “주요정보통신서비스 제공자”라 한다)
2. 집적정보통신시설 사업자
3. 전년도 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상 또는 전년도 일일평균 이용자수 100만명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자

- 미국 상공회의소와 컴퓨터통신산업협회(CCIA) 등 관련 단체는 미국 상무부를 통해 디지털 무역 장벽 해소를 위하여 개선해야 할 국내 제도로 CSAP를 지목한 바 있음.
- 이에 따르면, 현재 CSAP는 국내 기업뿐만 아니라 해외 기업도 받을 수 있으나 마이크로소프트(MS), 구글, 아마존 웹 서비스(AWS) 등 미국 CSP는 국내 서비스 운영 시 물리적 망분리가 어려우므로 CSAP 심사 시 실질적으로 중·상등급을 받지 못하고 ‘하’등급을 받을 가능성이 매우 커 공공기관의 민간 클라우드 도입 사업에 참여하는데 실질적인 제한을 받고 있다고 주장하고 있음.
- 현재 CSAP의 운영방식이 디지털 무역 장벽에 해당하는지는 별도로 논의가 필요한 사항이나 CSAP 관련 국가 간 논의가 진행 중인 상황에서 미국의 주요 CSP에게 CSAP를 받아야 하는 의무가 새롭게 부과되면 디지털 무역 장벽과 관련한 통상마찰이 심화될 가능성도 배제할 수 없음.
- 둘째, 일부 CSP는 현행 정보통신망법에 따른 ISMS 인증 의무 대상이 될 수 있어 CSAP 의무 제도가 도입되면 같은 사업자가 정보보호에 대한 유사한 의무를 중복하여 이행해야 하므로 과도한 부담으로 작용할 우려는 없는지 논의가 필요함.
- 과학기술정보통신부는 클라우드컴퓨팅 서비스의 운영 관리를 위한 외부 협력업체의 증가에 따라 보안과 관련된 인증 기준이 반영될 필요성이 있으나 이러한 인증 기준에 대한 사항은 법률이 아닌 고시인

「클라우드컴퓨팅서비스 보안 인증에 관한 고시」에 반영하는 것이 바람직하고,

CSAP의 취지 자체는 공공기관이 민간 클라우드 서비스를 이용할 때 안전성을 확인할 수 있는 인증 제도를 운영하는 것인 만큼 클라우드 컴퓨팅서비스 제공자에 대한 보안인증을 의무화하여 클라우드컴퓨팅 서비스 제공자에 대한 부담을 가중하는 것은 제도의 도입 목적에 다소 부합하지 않는 측면이 있어 신중한 검토가 필요하다는 입장임.

2. 클라우드컴퓨팅서비스 제공자의 정보보호최고책임자 지정 의무 (안 제23조의5 신설)

가. 개정안 요지

- 클라우드컴퓨팅서비스 제공자는 대통령령으로 정하는 기준에 해당하는 임직원을 정보보호 최고책임자로 지정하고 과학기술정보통신부장관에게 신고하여야 함(안 제23조의5제1항)
- 클라우드컴퓨팅서비스 제공자는 정기적인 감사 및 개선 관련 자료를 대통령령으로 정하는 기간 동안 보관하여야 함(제4항)
- 과학기술정보통신부장관은 이용자 정보의 안전성과 신뢰성 확보를 현저히 해치는 사건·사고 등이 발생하였거나 발생할 가능성이 있는 경우 해당 클라우드컴퓨팅서비스 제공자에게 제4항에 따른 자료의 제출을 요구할 수 있고, 자료제출 요구를 받은 자는 정당한 사유가 없으면 그 요구에 따라야 함(제5항).
- 안 제23조의5제4항 및 제5항을 위반한 경우 1천만원 이하의 과태료를 부과함(안 제37조제2항제2호 및 제3호).

나. 개정안 조문대비표

현 행	개 정 안
<신 설>	제23조의5(정보보호 최고책임자의 지정 등) ① 클라우드컴퓨

현행	개정안
	<u>팅서비스 제공자는 클라우드컴퓨팅서비스의 보안 및 정보의 안전한 관리를 위하여 대통령령으로 정하는 기준에 해당하는 임직원을 정보보호 최고책임자로 지정하고 과학기술정보통신부장관에게 신고하여야 한다. 다만, 자산총액, 매출액 등이 대통령령으로 정하는 기준에 해당하는 클라우드컴퓨팅서비스 제공자의 경우에는 정보보호 최고책임자를 신고하지 아니할 수 있다.</u> <u>② 제1항 본문에 따라 지정 및 신고된 정보보호 최고책임자(자산총액, 매출액 등 대통령령으로 정하는 기준에 해당하는 클라우드컴퓨팅서비스 제공자의 경우로 한정한다)는 제3항의 업무 외의 다른 업무를 겸직할 수 없다.</u> <u>③ 정보보호 최고책임자의 업무는 다음 각 호와 같다.</u> <u>1. 정보보호 계획의 수립·시행 및 개선</u>

현행	개정안
	2. 정보보호 실태와 관행의 정기적인 감사 및 개선 3. 정보보호 위협의 식별 평가 및 정보보호 대책 마련 4. 정보보호 교육과 모의 훈련 계획의 수립 및 시행 5. 그 밖에 클라우드컴퓨팅서비스의 안정성 확보를 위하여 대통령령으로 정하는 사항 ④ 클라우드컴퓨팅서비스 제공자는 제3항제2호에 따른 정기적인 감사 및 개선 관련 자료를 대통령령으로 정하는 기간 동안 보관하여야 한다. ⑤ 과학기술정보통신부장관은 이용자 정보의 안전성과 신뢰성 확보를 현저히 해치는 사건·사고 등이 발생하였거나 발생할 가능성이 있는 경우 해당 클라우드컴퓨팅서비스 제공자에게 제4항에 따른 자료의 제출을 요구할 수 있다. 이 경우 자료제출 요구를 받은 자는 정당한 사유가 없으면 그 요구에 따라야 한다.

현행	개정안
제37조(과태료) <신설>	⑥ 제1항에 따른 정보보호 최고책임자의 자격요건, 신고의 방법, 제3항에 따른 업무, 제5항에 따른 자료제출 요구의 절차·방법 등에 필요한 사항은 대통령령으로 정한다.
① 다음 각 호의 어느 하나에 해당하는 자에게는 1천만원 이하의 과태료를 부과한다.	제37조(과태료) ① 제23조의2제2항을 위반하여 보안인증을 받지 아니한 자에게는 3천만원 이하의 과태료를 부과한다.
<신설>	② ----- ----- ----- ---
<신설>	2. 제23조의5제4항을 위반하여 자료를 보관하지 아니한 자
<신설>	3. 제23조의5제5항을 위반하여 자료의 제출요구에 정당한 사유 없이 따르지 아니한 자

다. 검토사항

- 정보보호최고책임자(CISO; Chief Information Security Officer)는 정보통신서비스 제공자의 정보통신시스템 보호를 강화하는 한편 정보보호 업무의 책임성을 확보하기 위하여 정보통신방법을 통해 도입⁴⁾된

제도로 정보보호최고책임자 지정은 원래 사업자의 재량이었으나 정보통신망법 개정⁵⁾을 통해 지정 및 신고가 의무 사항으로 변경됨.

○ 그리고, 이와 유사한 제도로 「정보통신기반 보호법」 제5조제5항에 따른 정보보호책임자, 「전자금융거래법」 제21조의2제4항에 따른 정보보호최고책임자, 「개인정보 보호법」 제31조제2항에 따른 개인정보보호책임자 등이 도입되어 운영 중임.

○ 개정안은 클라우드컴퓨팅서비스의 정보보호를 강화하고 관련된 책임 소재를 명확히 하기 위하여 정보통신망법과 마찬가지로 CSP에게 정보보호최고책임자 지정 및 신고 의무를 부과하고 정보보호최고책임자

4) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」

제45조의3(정보보호 최고책임자의 지정 등) ① 정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 대통령령으로 정하는 기준에 해당하는 임직원을 정보보호 최고책임자로 지정하고 과학기술정보통신부장관에게 신고하여야 한다. 다만, 자산총액, 매출액 등이 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우에는 정보보호 최고책임자를 신고하지 아니할 수 있다.

② 제1항에 따른 신고의 방법 및 절차 등에 대해서는 대통령령으로 정한다.

③ 제1항 본문에 따라 지정 및 신고된 정보보호 최고책임자(자산총액, 매출액 등 대통령령으로 정하는 기준에 해당하는 정보통신서비스 제공자의 경우로 한정한다)는 제4항의 업무 외의 다른 업무를 겸직할 수 없다.

④ 정보보호 최고책임자의 업무는 다음 각 호와 같다.

1. 정보보호 최고책임자는 다음 각 목의 업무를 총괄한다.

가. 정보보호 계획의 수립·시행 및 개선

나. 정보보호 실태와 관행의 정기적인 감사 및 개선

다. 정보보호 위협의 식별 평가 및 정보보호 대책 마련

라. 정보보호 교육과 모의 훈련 계획의 수립 및 시행

2. 정보보호 최고책임자는 다음 각 목의 업무를 겸할 수 있다.

가. 「정보보호산업의 진흥에 관한 법률」 제13조에 따른 정보보호 공시에 관한 업무

나. 「정보통신기반 보호법」 제5조제5항에 따른 정보보호책임자의 업무

다. 「전자금융거래법」 제21조의2제4항에 따른 정보보호최고책임자의 업무

라. 「개인정보 보호법」 제31조제2항에 따른 개인정보 보호책임자의 업무

마. 그 밖에 이 법 또는 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행

⑤ 정보통신서비스 제공자는 침해사고에 대한 공동 예방 및 대응, 필요한 정보의 교류, 그 밖에 대통령령으로 정하는 공동의 사업을 수행하기 위하여 제1항에 따른 정보보호 최고책임자를 구성원으로 하는 정보보호 최고책임자 협의회를 구성·운영할 수 있다.

⑥ 정부는 제5항에 따른 정보보호 최고책임자 협의회 활동에 필요한 경비의 전부 또는 일부를 지원할 수 있다.

⑦ 정보보호 최고책임자의 자격요건 등에 필요한 사항은 대통령령으로 정한다

5) 법률 제15628호, 2018.6.12. 일부 개정

로 하여금 정기감사 및 개선 관련 자료를 보관하고 정부에 제출할 의무를 부과하려는 것임.

- 정보보호 부문에 전문성을 가진 임직원이 클라우드컴퓨팅서비스의 정보보호 업무를 총괄하는 정보보호최고책임자로 지정되면 클라우드컴퓨팅서비스에 침해사고에 대한 사전 예방을 강화하고 침해사고가 발생한 경우 정보보호최고책임자를 중심으로 신속한 대응이 가능해지는 효과가 있을 것으로 보임.
- 다만, 정보통신망법에 따른 정보통신서비스 제공자와 클라우드컴퓨팅법에 따른 CSP는 그 범위가 독립적이지 않고 중복되므로 일부 CSP는 이미 현행 정보통신망법에 따른 정보보호최고책임자를 지정하고 있음.
- 그러므로, 개정안과 같이 모든 CSP에게 정보보호최고책임자 지정 의무가 부과되면 CSP이면서 정보통신서비스 제공자인 사업자는 유사한 업무를 하는 정보보호최고책임자를 두 법률에 따라 각각 지정해야 하는 문제가 발생할 수 있으므로 중복 규제의 가능성에 대한 논의가 필요해 보임.
- 참고로, 현행 정보통신망법은 정보보호최고책임자의 업무를 정보보호 관련 업무로 명확하게 제한하고 겸직을 금지하되, 유사한 업무인 「정보통신기반 보호법」 제5조제5항에 따른 정보보호책임자, 「전자금융거래법」 제21조의2제4항에 따른 정보보호최고책임자, 「개인정보 보호법」 제31조제2항에 따른 개인정보 보호책임자 등의 업무

를 겸할 수 있도록 규정하고 있어 유사한 업무를 수행하는 직위가 중복하여 다수 운영되는 것을 방지하고 있음.

- 이를 감안할 때, CSP에 대한 정보보호최고책임자 지정을 의무로 하더라도 겸직 허가 등을 통해 정보통신망법에 따른 정보보호최고책임자로 갈음할 수 있도록 하는 방안도 고려해 볼 수 있을 것임.
- 과학기술정보통신부는 클라우드컴퓨팅법에 따른 정보보호최고책임자와 정보통신망법에 따른 정보보호최고책임자의 적용 대상 및 업무 범위가 중복된다는 점에서 신중한 검토가 필요하다는 입장임.

문 의 처
02)6788-5230