2025년 2분기

인터넷·정보보호 법제동향

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

2025년 2분기
인터넷·정보보호 법제동향

CONTENTS

목차

PART I

EU 주요국의 「NIS2 지침」 이행입법 추진현황

1. 개요

○ EU는 유럽 전역의 사이버보안 수준을 강화하기 위하여 필수·중요 조직의 사이버보안 위험관리, 사고보고 의무 등을 규정한 「NIS2 지침」을 마련 ('22.12. 개정, '24.10. 시행)

- 「유럽연합 전역의 높은 공통 수준의 사이버보안을 위한 조치에 관한 지침(NIS2 지침)*」은 기존 「네트워크 및 정보시스템 보안지침(NIS 지침)」을 보완하여 최신화한 것으로 통상 'NIS2 지침'으로 약칭

  * Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

- 「NIS2 지침」은 ▲적용대상 확대(중요 및 필수 조직), ▲보호조치 및 사고보고 의무 강화, ▲사이버보안 담당 기관 역할 확대, ▲국가 간 협력체계를 강화하는 방향으로 전면 개정

〈 「NIS2 지침」 주요 개정사항 〉

구분	「NIS 지침」 ('16.7. 제정, '18.5. 시행)		「NIS2 지침」 ('22.12. 개정, '24.10. 시행)
적용대상 확대	• 필수 서비스(Essential Services) – 에너지, 교통, 은행업, 금융 인프라, 의료, 식수, 디지털 인프라 • 디지털 서비스(Digital Service) – 온라인 마켓, 검색엔진, 클라우드 서비스		• 필수 조직(Essential Entities) – 에너지, 교통, 은행업, 금융 인프라, 의료, 식수, 디지털 인프라, **폐수, ICT 서비스 관리(B2B), 공공행정, 우주** • 중요 조직(Important Entities) – 디지털 서비스(온라인 마켓, 검색엔진, **SNS**), **우편 및 배송 서비스, 폐기물 관리, 화학물질 제조·생산·유통, 식품 생산·가공·유통, 제조, 연구**
보호조치 및 사고보고 의무 강화	• 필수 서비스 및 디지털 서비스 제공자의 네트워크·정보시스템에 대한 적절한 기술적·관리적 보호조치 부과 • 필수 서비스 제공자의 중대한(significant) 사고 보고 의무 및 디지털 서비스 제공자의 심각한(substantial) 사고보고 의무 부과	➡	• 필수 및 중요조직의 네트워크 정보시스템에 대한 보안 **위험관리 조치** 부과 – 위험분석 및 정보시스템 보안 정책, 사고 처리, 백업 관리, 재해복구, 위기관리 등 비즈니스 연속성 보장 등 • 필수 및 중요조직의 **중대한(significant) 사고 보고의무 체계화** – (최초보고) 중대한 사고 인지 후 24시간 이내 – (후속보고) 72시간 이내 최초보고 평가 등 통지 – (중간보고) 상황을 최신화한 중간보고 – (최종보고) 후속보고 후 1개월 이내 최종보고
사이버보안 담당기관 역할 확대	• EU 회원국 국가 단위의 국가사이버보안전략 수립, 사이버침해사고대응팀(CSIRT) 및 사이버 훈련 등 프로그램 실행·운영		• 각 회원국은 지침 이행 여부를 담당하는 **관할 당국** 및 대규모 **사이버보안 사고 위기관리 담당 기관**을 설립

EU 회원국은 '24년 10월 17일까지 「NIS2 지침」을 자국의 국내법으로 전환해야 하나 회원국 중 8개국만이 전환 완료, EU 집행위원회는 미도입 국가에 신속한 이행 촉구 ('25.5.7.)

- 「NIS2 지침」은 '23년 1월 17일에 발효되고, 발효일로부터 21개월 후인 '24년 10월 17일까지 EU 회원국의 국내법 전환이 필요하며, 기존 「NIS 지침」은 '24년 10월 18일부터 폐지
- '25년 5월 7일, 「NIS2 지침」을 국내법으로 완전히 도입한 EU 회원국은 총 8개국으로, 집행위원회는 완전히 도입하지 않은 19개국에 의견서(Reasoned Opinion)를 송달하고*, 불이행 시 유럽사법재판소에 제소한다는 방침

  * **(위반관련 절차(Infringement procedure))** 회원국이 EU 법률을 불이행하거나 위반할 경우, 집행위원회는 ① 서면 통지(letter of formal notice) → ② 의견서 송달(reasoned opinion) → ③ 사법재판소 제소 순으로 집행 가능[1)]

〈 EU 27개 회원국의 「NIS2 지침」 국내법 도입현황 ('25.5.7.) 〉

구분	국가
「NIS2 지침」 도입국 (8개국)	• 이탈리아, 벨기에, 그리스, 루마니아, 리투아니아, 몰타, 슬로바키아, 크로아티아
「NIS2 지침」 미도입국 (19개국)	• 독일, 프랑스, 스페인, 네덜란드, 아일랜드, 덴마크, 핀란드, 스웨덴, 헝가리, 오스트리아, 폴란드, 포르투갈, 체코, 불가리아, 에스토니아, 키프로스, 라트비아, 룩셈부르크, 슬로베니아

- 인구, 경제 규모, 정치적 영향력 등의 기준에서 EU 주요국으로 평가받는 독일, 프랑스, 이탈리아, 스페인 중 「NIS2 지침」을 국내법으로 완전히 도입한 나라는 이탈리아뿐이며, 주요국의 이행현황은 다음과 같음

〈 독일, 프랑스 등 EU 주요국의 「NIS2 지침」 도입현황 〉

구분	주요내용		
	이행현황	법안명	비고
독일	• **내무부 초안 발표**(Referentenentwurf, '25. 6.)	• 「NIS-2 이행 및 사이버보안 강화법안 (NIS-2-Umsetzungs-und Cybersicherheitsstärkungsgesetz)	옴니버스 방식의 개정[2)]
프랑스	• **입법안 상원 심의**('25. 3.) – 향후 하원 심의 및 국무회의 절차 예정	• 「주요기반시설 복원력 및 사이버보안 강화법안」 (Senate Bill No. 78 Projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la)	옴니버스 방식의 개정[3)]
이탈리아	• **도입완료**('24. 9.) – 보완 시행령(입법령 221호) 발효('25.2)	• 「2024년 9월 4일 이탈리아 입법령 제138호」 (Decreto Legislativo 4 settembre 2024, n. 138)	신규 입법
스페인	• **정부초안**('25. 2.) – 각료회의에서 법안 초안 승인	• 「사이버보안 조정 및 거버넌스에 관한 법률 초안」 (ANTEPROYECTO DE LEY DE COORDINACIÓN Y GOBERNANZA DE LA CIBERSEGURIDAD)	신규 입법

※ **(옴니버스 방식)** 여러 관련 법령이나 규정을 하나의 법령을 통해 동시에 개정하는 방식

1) [출처] https://commission.europa.eu/law/application-eu-law/implementing-eu-law/infringement-procedure_en
2) 「연방정보기술보안청법(Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen)」, 「연방정보국법(Änderung des BND-Gesetzes)」 등을 개정
3) 「주요기반시설 복원력 및 사이버보안 강화법안」을 통해, EU의 「주요조직 복원력지침(CER지침)」, 「NIS2 지침」을 국방법전(code de la défense) 등에 「디지털운영복원력법(DORA)」을 통화 및 금융법전(le code monétaire et financier) 등에 포함

2. EU 주요국의 「NIS2 지침」 이행입법 주요내용

EU 「NIS2 지침」은 적용대상의 범위를 필수·중요조직으로 구분하고, 회원국이 자국의 상황에 따라 재량으로 필수·중요조직을 지정할 수 있도록 규정

- **(「NIS2 지침」의 적용대상)** 「NIS2 지침」은 적용대상을 필수조직(Essential Entities)과 중요조직(Important Entities)으로 구분하고, 부속서 I 및 부속서 II에 언급된 분야 중 필수조직에 해당하는 경우를 다음과 같이 규정하며, 필수조직에 해당하지 않는 경우 중요조직으로 간주

〈 「NIS2 지침」 상의 필수·중요조직 구분 기준 〉

<table>
<tr><th colspan="2">구분</th><th>주요내용</th></tr>
<tr><td rowspan="3">필수 조직
(Essential Entities)</td><td>규모</td><td>• 중견기업 규모(medium-sized)*를 초과하는 조직으로서 부속서 I에 언급된 중요도가 높은 분야(sectors of high criticality)**에 해당하는 조직
* ▲50인 이상 250인 미만의 직원 ▲연 매출액 1,000만 유로 이상 5,000만 유로 이하 ▲연간 대차대조표 총액 1,000만 유로 이상 4,300만 유로 이하를 모두 충족하는 조직 규모(중견기업의 정의에 관한 2003년 5월 6일자 EU 집행위원회 권고 (2003/361/EC) 부속서 제2조)
** ▲에너지(전기, 지역 냉난방, 석유, 가스, 수력), ▲교통(공항, 철도, 하천, 도로), ▲은행, ▲금융시장 인프라, ▲의료, ▲식수, ▲폐수, ▲디지털 인프라, ▲ICT 서비스 관리(B2B), ▲공공행정, ▲우주
• 중견기업 규모의 공공 전자 통신 네트워크 제공자 또는 공개적으로 이용가능한 전자 통신 서비스 제공업체</td></tr>
<tr><td>기타</td><td>• 규모에 관계없이 적격 트러스트 서비스(QSTP), 최상위 도메인 네임 레지스트리(TLD), 도메인 네임 시스템(DNS) 서비스 제공업체</td></tr>
<tr><td>회원국 재량</td><td>• ▲회원국의 국내법에 따른 중앙정부 또는 ▲회원국이 위험기반 평가를 통해 서비스 중단이 주요 사회·경제 활동에 심각한 영향을 미칠 수 있다고 규정한 지역 수준의 공공 행정기관
• 부속서 I(중요도가 높은 분야) 또는 II(기타 중요분야)에 언급된 분야의 조직으로서 다음에 해당하는 경우, 회원국이 필수조직으로 지정한 조직
– 회원국 내에서 주요 사회·경제 활동 유지에 필수적인 서비스의 유일한 제공자인 경우
– 조직이 제공하는 서비스 중단이 공공안전·보안·보건에 중대한 영향을 미치는 경우
– 조직이 제공하는 서비스 중단이 중대하고 체계적인 위험을 유발할 수 있고, 특히 대외적으로 영향을 미칠 수 있는 경우
– 조직이 회원국의 특정 분야, 서비스 유형, 또는 기타 상호의존적 분야에 대한 국가나 지역적 수준의 특수한 중요성을 지니고 있어 필수적인 경우
• 회원국이 「NIS 지침」 또는 국내법에 따라 필수 서비스 운영자로 지정한 조직
• EU 「주요 조직 복원력 지침(CER 지침)」에 따라 주요 조직(Critical Entities)으로 지정되는 조직</td></tr>
<tr><td colspan="2">중요 조직
(Important Entities)</td><td>• 필수조직에 해당하지 않으면서, 부속서 I(중요도가 높은 분야) 또는 II(기타 중요분야*)에 언급된 조직
* ▲우편 및 배송 서비스 ▲폐기물 관리 ▲화학물질 제조·생산·유통 ▲식품의 생산·가공·유통 ▲제조(의료기기, 컴퓨터·전자·광학제품, 전기설비, 기계·장비, 자동차·트레일러, 기타 운송 장비) ▲디지털 서비스(온라인 마켓플레이스, 온라인 검색엔진, 소셜 네트워크 서비스 플랫폼) ▲연구
• 부속서 I(중요도가 높은 분야) 또는 II(기타 중요분야)에 언급된 분야의 조직으로서 회원국 내에서 주요 사회·경제 활동 유지에 필수적인 서비스의 유일한 제공자 등에 해당하는 경우, 회원국이 중요조직으로 지정한 조직</td></tr>
</table>

• **(EU 주요국의 적용대상 비교)** 독일은 기존 주요기반시설 규정(KRITIS-Verordnung)에 따른 주요기반시설 운영자(Betreiber kritischer Anlagen)를 필수조직으로, 프랑스는 「CER 지침」에 따라 지정한 핵심 운영자(Opérateurs d'importance vitale)를 필수조직으로 포함하는 등 국가별로 필수·중요조직 지정에 차이

〈 「NIS2 지침」에 따른 EU 주요국의 필수·중요조직 지정 〉

구분	주요내용	
	필수조직	중요조직
공통사항 	• 중견기업 규모를 초과하는 중요도가 높은 분야 해당 조직 • 중견기업 규모의 전자 통신 네트워크 제공업체 또는 공개적으로 이용가능한 전자 통신 서비스 제공업체 • 적격 트러스트(QSTP), 최상위 도메인 네임 레지스트리(TLD), 도메인 네임 시스템(DNS) 서비스 제공업체	• 필수 조직에 해당하지 않으면서, 중요도가 높은 분야 또는 기타 중요분야에 해당하는 조직
독일 	• **주요기반시설 운영자**(Betreiber kritischer Anlagen) ※ 특정 임계값을 초과하는 에너지, 물, 식품, 의료, 교통, IT·통신, 금융·보험, 폐기물 처리 부문의 주요기반시설 운영자 • **연방행정기관**(Einrichtungen der Bundesverwaltung)은 별도로 규제되지만, 필수조직에 준하여 적용 ※ 사회보장기관 및 독일연방은행을 제외한 연방당국, 공법에 따라 조직된 연방행정기관의 IT 서비스 제공자 등	• 트러스트 서비스 제공업체 • 중견기업 규모 미만의 전자 통신 네트워크 제공업체 또는 공개적으로 이용가능한 전자 통신 서비스 제공업체
프랑스 	• 주요조직 복원력지침(EU CER 지침)에 따라 **핵심 운영자**(Opérateurs d'importance vitale)로 지정된 자 ※ ▲프랑스 국토에 위치한 하나 이상의 주요기반시설을 통해 핵심 활동을 수행하는 공공 또는 민간 운영자, ▲원자력 시설을 포함하는 시설의 공공 또는 민간 운영자, 관리자, 소유자 등 • 기존 「NIS 지침」 이행법인 「보안 분야에서 EU 법률에 적응하기 위한 다양한 조항에 관한 법률(LOI n° 2018-133)」 제5조에 따라 지정된 **필수 서비스 운영자** • 인구가 3만명을 초과하는 도시 및 교외 공동체 중 「NIS2 지침」 부속서에 규정된 중요분야 및 기타 중요분야에 해당하는 **공공행정 기관 등** • 주요 사회·경제 활동 유지에 필수적인 서비스의 유일한 제공자 등에 해당하는 **연구활동 수행 교육기관**	• 필수조직이 아닌 전자 통신 사업자 • 필수조직이 아닌 트러스트 서비스 제공업체 • 국무총리가 중요조직으로 지정한 공공행정 기관 • 법령에 따라 공공행정 서비스 업무를 위임받은 자 중 국무총리가 중요조직으로 지정한 자 • 필수조직이 아닌 연구 활동을 수행하는 교육기관
이탈리아 	• EU 「CER 지침」 이행법(Legislative Decree 134/2024)에 따라 **주요 조직 운영자**로 지정된 자 • 「2024년 9월 4일 이탈리아 입법령 제138호」(NIS2 이행법)의 부속서 III 제1조(a)항에 규정된 **중앙 행정기관**(헌법기관 및 헌법적 지위를 갖는 기관, 총리실 및 각 부처, 세무기관, 독립 행정기관) • 당국이 주요 사회·경제 활동 유지에 필수적인 서비스의 유일한 제공자 등에 해당하는 「NIS 이행법」의 부속서 IV에 규정된 조직(지역 대중교통 서비스 제공조직, 연구활동 수행 교육기관 등) 중 필수 조직으로 인정하는 경우	-
스페인 	• 당국이 주요 사회·경제 활동 유지에 필수적인 서비스의 유일한 제공자 등에 해당하여 필수조직으로 지정한 경우 • 기존 「NIS 지침」 이행법인 「네트워크·정보시스템 보안에 관한 법령(Ley 12/2018)」에 따라 지정된 필수 서비스 운영자	• 필수조직이 아닌 인구 2만명 이상의 지자체와 산하 공공부문 조직을 포함

「NIS2 지침」은 필수·중요조직이 네트워크·정보시스템 보안 위험관리 조치를 이행하도록 규정

• **(「NIS2 지침」의 위험관리 의무)** 필수·중요조직은 네트워크·정보시스템의 보안에 제기된 위험을 관리하고 사고가 서비스 등에 영향을 미치는 것을 방지하거나 최소화하기 위하여 적절하고 비례적인 기술적, 운영적, 조직적 조치를 이행해야 함

– EU 집행위원회는 「NIS2 지침」 제21조제5항에 따라 특정 디지털기반·서비스 제공자, ICT 서비스 관리부문 조직의 사이버보안 위험관리 조치 요구사항 및 중대한 사고 기준을 구체화하는 이행규정 채택('24.10)

※ 이행규정 세부내용은 한국인터넷진흥원 '[2024년 10월] 인터넷·정보보호 법제동향 제205호'의 해외 단신을 참고

• **(EU 주요국의 위험관리 의무 비교)** EU 주요국은 「NIS2 지침」에서 규정하는 사이버보안 위험관리에 관한 10가지 조치 사항을 공통으로 반영하면서, 국가별로 특정한 위험관리조치를 구체적으로 요구하기도 함

– EU 사이버보안인증을 받은 특정 ICT제품·서비스·프로세스의 사용, 주요기반운영자의 공격탐지시스템 사용(독일), 복원력 계획 등 특정 위험관리 요구사항의 이행(프랑스), 위험관리 조치의무 준수 인증(스페인) 등

〈 「NIS2 지침」에 따른 EU 주요국의 위험관리 조치의무 비교 〉

구분	주요내용
공통사항	• ① 위험분석 및 정보시스템 보안에 관한 정책, ② 사고처리, ③ 백업관리, 재해복구, 위기관리와 같은 비즈니스 연속성, ④ 공급망 보안, ⑤ 네트워크·정보시스템의 취득, 개발, 유지 관리에 관한 보안, ⑥ 위험관리 조치의 효과를 평가하기 위한 정책 및 절차, ⑦ 사이버보안 교육, ⑧ 암호 정책 및 절차, ⑨인적보안, 접근통제 정책, 자산관리, ⑩ 다중요소 인증 사용 등의 조치
독일	• 필수조직과 관련 산업협회는 위험관리 조치의무를 준수하기 위해 「NIS2 지침 EU 집행위원회 이행규정」의 요구사항과 모순되지 않는 **산업별 안전 표준**을 제안할 수 있음 ※ 연방정보보안청은 연방시민보호 및 재난지원청 및 관할 연방감독기관과 협의하여, 제안된 표준이 ▲부문별로 적합하고, ▲적절하며 비례적이고 효과적인 기술·조직적 위험관리 조치를 보장하는데 적합한지 여부를 결정 • 주요기반시설 운영자(Betreiber kritischer Anlagen)는 **공격 탐지 시스템(OH SzA)***을 사용해야 함 * 진행 중인 작업에서 적절한 매개변수와 특성을 자동으로 기록·분석해야 하고, 지속적으로 위협을 식별·예방하며 발생한 결함에 대해 적절한 수정 조치를 제공해야 함 • **연방행정기관**은 **연방정보기술보안청 표준(BSI-Standards)** 및 **IT 기본 보호 개요서(IT-Grundschutz)**의 연방 정보기술 보안에 관한 **최소 기준을 준수**해야 하고, 해당 표준은 정기적으로 평가 및 추가적으로 개발되어야 함 • 연방행정기관은 해당 기관의 **정보보안 책임자**를 지정해야 함
프랑스	• 핵심 운영자(Opérateurs d'importance vitale)는 위험관리 조치의무 및 **특정 요구사항***을 이행해야 함 ※ 핵심 활동 또는 주요기반시설, 핵심 지점의 보안을 방해할 수 있는 테러 등 모든 종류의 위험을 분석하고, 특별 복원력 계획을 행정당국에 수립·제출해야 함 • 적격 트러스트 서비스 제공업체(QSTP)를 포함한 암호화 서비스 제공업체는 마스터 복호화 키 또는 보호된 데이터에 무단으로 액세스할 수 있는 기타 메커니즘 등 **정보시스템 및 전자통신의 보안을 의도적으로 약화시키기 위한 기술적 조치를 통합할 필요가 없음** ※ 올리비에 카딕(Olivier Cadic) 상원의원은 「NIS2 지침 이행법안」의 심의과정에서 당국에 의해 감시 기술로 악용되거나 악의적 사이버 행위자 또는 적대국에 의해 악용될 수 있는 '백도어 프로그램'의 도입을 방지하기 위하여 해당 조항을 신설
스페인	• 필수조직은 **위험관리 조치의무 준수 인증서***를 획득하고 유지해야 함 * 국가사이버보안센터는 필요성, 비례성 및 효율성의 원칙에 따라 인증절차를 수립해야 하고 인증 획득을 위한 절차와 요건이 국가 보안체계 및 국제 기술표준과 일치하는 수준에서 구성되어야 함 • 필수·중요조직은 **정보보안 책임자***를 지정하여 당국 및 CSIRT간 연락창구 등의 역할을 수행 * **(자격요건)** 사이버보안에 대한 법률적, 조직적, 기술적 전문지식과 경험을 갖추고 업무수행에 적합한 직원 등

※ 이탈리아는 「NIS2 지침」의 공통사항과 유사

❍ 「NIS2 지침」은 서비스 제공에 중대한 영향을 미치는 사고를 관할 당국 등에 보고하도록 규정

• **(「NIS2 지침」의 사고 보고·통지 의무)** 필수·중요조직은 서비스 제공에 중대한 영향을 미치는 중대 사고*를 지체없이 컴퓨터보안사고대응팀(CSIRT) 또는 관할 당국에 보고해야 하며, 그러한 사고로 부정적 영향을 받을 수 있는 사용자(recipient)에게도 통지해야 함

* ▲해당 조직 서비스에 심각한 운영중단 또는 재정적 손실을 유발했거나 유발할 수 있는 경우, ▲물질적·비물질적으로 상당한 피해를 유발하여 다른 자연인 또는 법인에 영향을 주었거나 줄 수 있는 경우

– 중대한 사이버위협의 경우에도 해당 위협의 잠재적인 영향을 받는 사용자에게 지체없이 대응조치, 구제방법을 알려야 하고, 적절하다고 판단되면 사이버위협의 내용도 통지해야 함

〈 「NIS2 지침」 상 필수·중요조직의 사이버보안 사고 보고체계 〉

① 조기경보	② 사고통지	③ 중간보고	④ 최종보고
중대한 사고 인지한 후 **24시간 이내**	▶ **72시간 이내에** 조기 경보 내용 최신화 및 사고 초기평가를 포함한 **사고통지**	▶ CSIRT 또는 당국 요청에 따라 상황을 최신화한 **중간보고**	▶ **사고통지 후 1개월 내** 심각도·영향을 포함한 사고설명·원인, 조치 등을 포함한 **최종 보고**

• **(EU 주요국의 사고 보고·통지 의무)** EU 주요국은 사고 보고·통지 의무와 관련하여 「NIS2 지침」을 대부분 반영하면서 사용자에 대한 통지의무를 구체화함

〈 「NIS2 지침」에 따른 EU 주요국의 사이버보안 사고 보고의무 비교 〉

구분	주요내용
공통사항	• 필수·중요조직은 서비스 제공에 중대한 영향을 미치는 모든 사고를 지체없이 CSIRT 또는 당국에 보고 • 필수·중요조직은 해당되는 경우 잠재적 영향을 받게 될 서비스 사용자에게 해당 위협에 대응하여 취할 수 있는 조치나 구제책을 지체없이 전달하고 적절한 경우 중대한 사이버위협 발생 사실을 통지
독일	• **주요기반시설 운영자**(Betreiber kritischer Anlagen)는 중대한 사고가 시설에 영향을 미쳤거나 미칠 가능성이 있는 경우, 당국에 영향을 받은 시설 및 서비스 유형, 사고가 해당 서비스에 미치는 영향에 대한 정보 등을 보고 • 중대한 사이버위협에 잠재적으로 영향을 받게 될 **서비스 사용자**에게 구제책 등을 **통지해야 하는 산업 부문**을 구체화**(금융, 사회보험, 디지털 인프라, ICT 서비스, 디지털 서비스 부문의 조직)**
프랑스	• **서비스 사용자에게** 직접적인 영향을 미치는 **중대한 사고의 유형**을 구체화(민감정보 유출, 서비스 사용자의 사망 또는 건강에 상당한 피해 초래, 심각한 운영중단을 초래할 수 있는 법인의 정보·네트워크 시스템에 대한 무단 액세스) ※ 서비스 사용자 통지 의무는 공개될 경우, 국가방위 및 안보 이익을 해칠 수 있는 정보에 적용되지 않음
스페인	• 국가사이버보안센터(CNC)의 지시에 따라 국립암호센터 CERT(CCN-CERT)가 **사이버사고 보고 및 모니터링을 위한 플랫폼**을 조정, 유지 관리 ※ 플랫폼은 연중무휴 24시간 동안 사고보고 및 관리 절차를 수행하고 사이버사고 관리기능, 정보공유 역량, 샘플 분석기능, 취약점 로깅 및 보고 기능 등을 갖춰야 함 – 해당 플랫폼을 통해 필수·중요조직 등은 개인정보 보호 요구사항을 침해하지 않고 안전하고 신뢰할 수 있는 방식으로 정보공유 및 후속조치 집행 가능

※ 이탈리아는 「NIS2 지침」의 공통사항과 유사

EU 주요국은 「NIS2 지침」에 따라 사이버보안 업무를 전담하는 관할 당국, 단일 연락창구 등을 지정

• **(「NIS2 지침」 상 관할 당국 등 지정)** 「NIS2 지침」은 각 회원국이 관할 당국(Competent Authorities), 단일 연락창구(Single Point of Contact), 컴퓨터 보안사고 대응팀(CSIRTs)을 지정하도록 규정

〈 「NIS2 지침」 상 관할 당국 등 지정 〉

구분	주요내용
관할 당국	• 각 회원국은 사이버보안 및 감독 업무를 담당하는 하나 이상의 관할 당국을 지정하거나 설립해야 하며, 해당 관할 당국은 국가차원에서 NIS2 지침의 이행여부를 감독해야 함
단일 연락창구	• 각 회원국은 단일연락창구를 지정하거나 설립해야 하며, 단일 관할 당국을 지정하거나 설립하는 경우, 해당 관할당국이 해당 회원국의 단일 연락창구도 담당 ※ 단일 연락창구는 회원국 당국이 다른 회원국의 관련 당국과 대외적 협력하도록 보장하고, 적절한 경우 EU 집행위원회, 유럽연합 사이버보안청(ENISA)와 협력하도록 보장해야 함
컴퓨터 보안사고 대응팀	• 각 회원국은 사이버위협, 취약점, 사고 모니터링·분석, 조기경보, 사고 대응 지원 등 업무를 수행하는 컴퓨터 보안사고 대응팀(CSIRTs)을 하나 이상 지정하거나 설립해야 함

• **(EU 주요국의 관할 당국 등 비교)** EU 주요국의 사이버보안 관할 당국은 독일의 경우 연방정보보안청(BSI)이, 프랑스는 정보시스템보안청(ANSSI)이, 이탈리아는 사이버보안청(ACN)이, 스페인은 신설 예정인 국가사이버보안센터(CNC)가 담당

〈 EU 주요국의 관할 당국 등 비교 〉

구분	주요내용	
	관할 당국 및 단일 연락창구	컴퓨터 보안사고 대응팀
독일 	• 연방정보보안청(BSI) (Bundesamt für Sicherheit in der Informationstechnik)	• 연방정보보안청 산하의 컴퓨터 보안사고 대응팀(CERT-Bund)
프랑스 	• 정보시스템보안청(ANSSI) (Agence nationale de la sécurité des systèmes d'information)	• 정보시스템보안청 산하의 컴퓨터 보안사고 대응팀(CERT-FR)
이탈리아 	• 사이버보안청(ACN) (Agenzia Nazionale per la Sicurezza Cibernetica)	• 사이버보안청(ACN) 산하의 이탈리아 컴퓨터 보안사고 대응팀(CSIRT-Italia)
스페인 	• 국가사이버보안센터(Centro Nacional de Ciberseguridad) 신설 예정 • 사이버보안 감독 당국을 다음과 같이 구분	• ▲국립암호센터(CCN)-CERT, ▲국립 사이버보안연구소(INCIBE)-CERT, ▲합동 사이버방위 사령부 ESPDEF)-CERT

〈 스페인 사이버보안 감독 당국 〉

구분	분야별 담당조직
국립암호센터	• 공공부문의 법적제도에 관한 법(Ley40/2015)의 적용범위에 포함되는 필수·중요조직 감독
디지털전환 및 공공행정부	• 디지털 인프라 및 디지털 서비스 제공업체 부문의 필수·중요조직 감독
사이버보안 조정실	• 상기 소관 부문을 제외한 필수·중요조직 감독

〈 스페인 컴퓨터 보안사고 대응팀 〉

구분	분야별 담당조직
CCN-CERT	• 공공부문의 법적제도에 관한 법(Ley40/2015)의 적용범위에 포함되는 필수·중요조직 감독
INCIBE-CERT	• 공공부문의 법적제도에 관한 법(Ley40/2015)의 적용범위에 포함되지 않은 필수·중요조직 감독
ESPDEF-CERT	• 국방에 영향을 미치는 조직

3. 시사점

○ EU 회원국은 「NIS2 지침」에 따라 필수·중요조직의 사이버보안 위험관리 및 사고보고 체계 구축을 위한 이행 입법을 추진 중이나, 최종 완료까지는 다소 시일이 소요될 전망

- EU 회원국은 '24년 10월 17일까지 동 지침을 국내법으로 전환해야 하나, '25년 5월 7일 기준 유럽연합 27개국 중 이탈리아, 벨기에, 그리스 등을 포함한 8개국만이 동 지침을 자국법으로 도입
- EU 집행위원회는 동 지침을 완전히 도입하지 않은 독일, 프랑스 등 19개 회원국에 '이유를 명시한 의견서'를 송달하여 신속한 국내법 전환을 촉구했고, 불이행 시 추후 유럽사법재판소에 제소할 것으로 전망
- 각국의 입법 추진 상황 등을 볼 때 '25년 말에서 '26년 초 사이에 모든 국가의 자국법 전환이 완료될 것으로 전망되나 회원국마다 도입 시점, 적용 범위, 관련 의무사항 등에서 일부 차이가 발생할 것으로 예상

○ 각 회원국이 동 지침을 자국의 법체계에 반영하여 공공 및 민간의 많은 조직에 적용되는 사이버보안 입법을 정비하게 되면, EU 사이버보안 수준 제고에 기여할 것으로 평가

- 「NIS2 지침」은 유럽연합 전역의 높은 사이버보안 수준 달성을 목표로, 기존 「NIS 지침」의 적용대상을 대폭 확대하고 사이버보안 위험관리 조치 및 단계적 사고 보고 의무 등 보호체계를 강화
- 향후 각 회원국이 이러한 강화된 사이버보안 지침을 자국 법체계에 도입할 경우, EU 전역에서 일정 수준 이상의 사이버보안 체계가 갖추어질 것으로 평가
  - 「NIS2 지침」 이행입법 도입 시 사이버보안 위험관리 등 의무를 준수해야 하는 조직의 수가 독일의 경우 최소 30,000개(주요기반시설 운영자 5,000개를 포함한 필수조직 8,250개와 중요조직 21,600개), 프랑스는 15,000개로 확대될 것이라는 전망

○ EU 내 필수·중요서비스 분야 진출을 고려하는 국내 기업은 회원국의 이행입법 제정 동향을 파악하고 국가별 적용대상, 위험관리 조치 이행과 관련된 표준이나 인증제도 등을 고려할 필요

- EU 필수·중요서비스 부문 시장에 진출했거나 준비 중인 기업은 회원국마다 상이한 필수·중요조직의 범위를 파악하고, 사이버보안 위험관리 조치, 등록의무 등 의무사항을 준수하기 위한 계획 및 전략을 수립할 필요성
  ※ 필수·중요조직이 아니더라도 해당 조직에 제품·서비스를 공급하는 협력기업도 공급망 요구사항을 충족하는 등 영향을 받을 가능성이 있음
- 최근 유럽사이버보안청(ENISA)은 중견기업 규모의 조직이 「NIS2 지침」 상 사이버보안 의무 사항을 준수하는데에 필요한 역할과 기술, 단계별 접근법 등을 제공하기 위하여, 법적 구속력 없는 가이드(「NIS2 지침」의 필수·중요조직을 위한 사이버보안 역할 및 역량)를 발표 ('25. 6. 26.)
  - 조직적 프레임워크를 개발하고 전담팀을 구성하여 위험관리 조치 및 사고 보고 의무를 효과적으로 이행할 수 있는 방법 등을 제시하고 있어, 해당 조직의 「NIS2 지침」 대비 상태를 평가·개선하는 데 도움이 될 것으로 예상

Reference

- https://www.nis-2-directive.com/
- https://digital-strategy.ec.europa.eu/en/news/commission-calls-19-member-states-fully-transpose-nis2-directive
- https://commission.europa.eu/law/application-eu-law/implementing-eu-law/infringement-procedure_en
- https://www.consilium.europa.eu/en/press/press-releases/2025/06/06/eu-adopts-blueprint-to-better-manage-european-cyber-crises-and-incidents/
- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52025DC0066
- https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/CI1/nis2umsucg.html (독일)
- https://www.openkritis.de/eu/eu-nis-2-germany.htmll (독일)
- https://www.assemblee-nationale.fr/dyn/17/dossiers/DLR5L17N50731 (프랑스)
- https://www.senat.fr/seances/s202503/s20250312/s20250312008.html#section1188 (프랑스)
- https://www.openkritis.de/eu/eu-nis-2-france.html (프랑스)
- https://www.gazzettaufficiale.it/eli/id/2024/10/01/24G00155/SG (이탈리아)
- https://www.gazzettaufficiale.it/eli/id/2025/02/10/25G00017/sg (이탈리아)
- https://www.interior.gob.es/opencms/ca/detalle/articulo/El-Consejo-de-Ministros-aprueba-el-anteproyecto-de-Ley-de-Coordinacion-y-Gobernanza-de-la-Ciberseguridad/ (스페인)
- https://www.enisa.europa.eu/publications/cybersecurity-roles-and-skills-for-nis2-essential-and-important-entities
- 한국인터넷진흥원, 「EU 집행위원회, 연합 전체의 높은 공통 수준의 사이버보안에 관한 지침 이행규정 채택 (2024. 10. 17.)」, 『[2024년 10월] 인터넷·정보보호 법제동향 제205호』, 2024. 11. 19.
- 한국인터넷진흥원, 『2024 해외 사이버보안 입법동향』, 2024. 12.
- 한국인터넷진흥원, 『[25-10] 스페인 「사이버보안 조정 및 거버넌스에 관한 법률」 초안 의견수렴』, 2024. 3. 13.
- 한국인터넷진흥원, 『[25-12] 프랑스 상원 「주요기반시설 복원력 및 사이버보안 강화법안」 승인』, 2024. 4. 10.
- 한국인터넷진흥원, 「독일 연방 내무부, NIS2 지침 이행법(안) 공식 초안 발표(2024. 5. 7.)」, 『[2024년 5월] 인터넷·정보보호 법제동향 제200호』, 2024. 6. 5.

PART Ⅱ

트럼프 2기 행정부의 사이버보안 관련 행정명령

1. 개요

○ 트럼프 2기 행정부는 정부 효율화 기조를 강조하며 연방정부 역할을 축소하면서도, 국가 배후 사이버위협 증가에 대비하여 중국 등 국가에 대한 견제 지속

- ’25년 1월 20일, 재임에 성공한 트럼프 대통령은 100건에 가까운 행정명령에 서명할 것을 예고하며 바이든 전임 행정부의 정책을 철회*하고 ‘미국 우선주의’ 기조에 입각한 공약을 재추진하겠다는 의지 강조

  * 트럼프 대통령은 제47대 대통령 취임 직후, 행정명령 제14148호(유해한 행정명령 및 조치의 초기 철회, Initial Rescissions of Harmful Executive Orders and Actions)에 서명하여 바이든 행정부의 규제 정책 등을 철회

- 특히 ‘대통령의 정부효율부 인력 최적화 이니셔티브 시행에 관한 행정명령 제14158호’를 통해 정부효율부(Department of Government Efficiency, DOGE)를 신설하고, 정부 인력·예산 감축 등 비용 절감을 추진하여 연방정부 시스템의 효율성을 제고하는 정책 추진

- 한편, 특정 국가 배후 해커조직으로 알려진 솔트 타이푼(Salt Typhoon)의 통신사 해킹* 사건과 같이 국가 주요 기반시설을 겨냥한 사이버위협·공격에 대한 우려가 증가하면서, 중국 등 적대국에 대한 견제 필요성 제기

  * ’24년 12월, 버라이즌, AT&T, T모바일 등 미국의 3대 통신사를 포함한 최소 9개의 주요 통신사가 해킹 공격을 받아 이용자의 통신 메타데이터(전화번호, 통화시간, 날짜, 위치 등), 통신감청시스템의 도·감청 정보 등이 유출된 사건

  – ’25년 5월, 미국 연방통신위원회(FCC)는 미국의 통신 네트워크 및 장비 전반에 대해 중국 등 적대국이 소유·통제하는 조직의 영향력을 줄이기 위해 이들이 통신인증기관(TCB) 역할을 수행하지 못하도록 금지하는 등의 조치*를 취한 바 있음

  * 자세한 내용은 인터넷·정보보호 법제동향, 『[25-19] 미국 FCC, 통신 부문에서의 적대국의 위협에 대한 대응조치 발표』 자료 참고

- 트럼프 2기 행정부는 ’25년 상반기에 이러한 사이버보안 정책 방향과 기조를 반영하는 행정명령 2건을 발표

〈 트럼프 2기 행정부의 사이버보안 관련 행정명령 〉

구분	주요내용
행정명령 제14239호 (주 및 지역의 대응력 강화를 통한 효율의 달성)	• 주 및 지방정부가 **사이버 공격**, 기상 이변 등과 같은 사고에 **효과적으로 대비**할 수 있도록 **연방 대비·대응 정책을 간소화**하고 관련 정책 등을 **재검토**할 것을 명령 (’25.3.18.) ※ **Executive Order 14239** (Achieving Efficiency Through State and Local Preparedness)
행정명령 제14306호 (국가 사이버보안 강화를 위한 선별된 노력 유지)	• 오바마·바이든 행정부의 사이버보안 관련 행정명령을 일부 수정하여, **사이버위협 행위 국가의 범위를 확대**하고 소프트웨어 공급망 보안 등 **연방 사이버보안 정책을 간소화** (’25.6.6.) ※ **Executive Order 14306** (Sustaining Select Efforts To Strengthen the Nation's Cybersecurity and Amending EO 13694 and EO 14144)

2. 행정명령 제14239호 및 제14306호의 주요내용

1) 주 및 지역의 대응력 강화를 통한 효율의 달성(행정명령 제14239호)

○ 트럼프 대통령은 주 및 지방정부가 사이버 공격 및 특정 기상 현상과 같은 사고를 보다 효과적으로 대비할 수 있도록 연방정부의 접근방식을 단순화 및 축소하는 행정명령을 발표 ('25. 3. 18.)

- **(목적)** 미국 전역의 인프라에 대한 주 및 지방정부의 상식적인 접근방식과 투자를 통해 국가 안보를 강화하고 보다 회복력있는 국가를 구축하기 위하여, 연방정책의 대비 태세가 주, 지방, 개인 수준에서 가장 효과적으로 소유·관리되어야 하고, 역량 있고 접근 가능하며 효율적인 연방정부의 지원을 받아야 한다는 점을 강조

  ※ 시민은 사이버 공격, 산불, 허리케인 등 위험에 대처하기 위한 올바른 지역적 결정과 투자의 주체로서, 각 주에서 현명한 인프라를 선택할 수 있는 권한이 부여되면 납세자에게도 혜택이 돌아갈 것이라 밝힘

  - 주, 지역, 개인의 대비 능력을 강화하고 위험 기반 결정을 통해 인프라 우선순위 지정과 전략적 투자에 상식을 도입하여 인프라, 지역사회, 경제가 글로벌하고 역동적인 위협에 회복력있게 대응할 수 있도록 함

- **(정책 목표)** 주 및 지방정부와 개인이 국가 회복력과 대비에 보다 적극적이고 중요한 역할을 수행함으로써 미국인의 생명을 구하고, 생계를 보장하며, 효율성을 통해 납세자 부담을 줄이고 공동 번영을 실현

  - 행정부는 대비 운영 간소화 및 관련 정부 정책 최신화를 통해 복잡성을 줄이고 미국인을 더 잘 보호하며, 주 및 지방정부가 시민의 요구를 더 잘 이해하고 궁극적으로 해결할 수 있도록 지원

- **(주요내용)** 미국인의 생명을 구하고 부실한 보조금 관리를 종식하기 위하여, ▲국가 복원력 전략을 발표하고, ▲관련 주요기반시설 및 연속성 정책을 검토·수정하며, ▲국가 위험 등록부 개발을 권고

〈 행정명령 14239의 주요내용 〉

구분	주요내용
국가 복원력 전략 (National Resilience Strategy)	• 명령일로부터 **90일 이내**에, 대통령 국가안보보좌관(APNSA)은 대통령 경제정책보좌관 및 관련 행정부처 및 기관의 장과 협력하여 국가 복원력 증진을 위한 우선순위, 수단 및 방법을 명시하는 국가 복원력 전략을 발표 – 국가 복원력 전략은 최소 4년마다 또는 적절할 때마다 검토·수정
▼	
국가 주요기반시설 정책 (National Critical Infrastructure Policy)	• 명령일로부터 **180일 이내**에 대통령 국가안보보좌관은 과학기술정책실 국장 및 관련 기관의 장과 협력하여 모든 주요기반시설 정책을 검토 • 보다 회복력 있는 태세를 달성하는 데 필요한 정책의 수정, 폐기 및 대체를 대통령에게 권고하고 위험정보에 기반한 접근방식으로 전환하며 국가 복원력 전략을 이행 **〈 검토 및 수정 권고 대상 정책 〉** • 국가안보각서 16(미국 식량 및 농업 안보와 회복력 강화, '22.11.10.) • 국가안보각서 22(주요기반시설 보안 및 복원력, '24.4.30.) • 행정명령 제14017호(미국의 공급망, '21.2.24.) • 행정명령 제14123호(백악관 공급망 회복력 위원회, '24.6.14.)

<table>
<tr><th>구분</th><th>주요내용</th></tr>
<tr><td>국가 연속성 정책
(National Continuity Policy)</td><td>• 명령일로부터 180일 이내에, 대통령 국가안보보좌관은 관련 기관의 장과 협력하여 모든 국가 연속성 정책을 검토하고 국가 연속성 역량에 대한 접근방식을 현대화 및 간소화하고 지속적인 대비 태세를 달성하는 데 필요한 방법론과 아키텍처를 재구성
• 국가 복원력 전략을 이행하는 데 필요한 정책의 개정, 폐기 및 대체를 대통령에게 권고
〈 검토 및 수정 권고 대상 정책 〉
• 행정명령 제13618호(국가 안보 및 비상대응 통신 기능의 할당, ’12.7.6.)
• 행정명령 제13961호(연방 임무 복원력의 거버넌스 및 통합, ’20.12.7.)
• 국가안보각서 32(국가 연속성 정책, ’25.1.19.)
• 행정명령 제14146호(행정명령 제13961호의 일부 취소, ’25.1.19.)</td></tr>
<tr><td colspan="2">▼</td></tr>
<tr><td>대비 및 대응 정책
(Preparedness and Response Policies)</td><td>• 명령일로부터 240일 이내에, 대통령 국가안보보좌관은 관련 기관의 장과 협력하고 행정명령 제14180호에 따라 설립된 연방 비상 관리기관 평가위원회의 보고서 및 결과에 따라 모든 국가 대비 및 대응정책을 검토하고 연방책임의 절차와 지표를 재구성
• 국가 복원력 전략을 이행하는 데 필요한 정책의 개정, 폐기 및 대체를 대통령에게 권고
〈 검토 및 수정 권고 대상 정책 〉
• 행정명령 제12656호(비상 대비 책임의 할당, 1988.11.18.)
• 국토안보부 대통령 지침 5(국내 사고 관리, ’03.2.28.)
• 대통령 정책 지침 8(국가 특별 안보 사건, ’13.3.28.)
• 대통령 정책 지침 44(국내 사고 대응 강화, ’16.11.7.)</td></tr>
<tr><td>국가 위험 등록부
(National Risk Register)</td><td>• 명령일로부터 240일 이내에, 대통령 국가안보보좌관은 관리예산국 국장 및 관련 기관의 장과 협력하여 국가 인프라, 관련 시스템 및 그 사용자에 대한 자연적 및 악의적 위험을 식별, 명시 및 정량화하는 국가 위험 등록부의 개발을 조율
– 국가 위험 등록부를 통해 생성된 정량화(quantification)는 정보 커뮤니티, 민간 부문 투자, 주 투자 및 연방 예산 우선순위를 알리는 데 사용
– 국가 위험 등록부는 최소 4년마다 또는 역동적인 위험 환경에 따라 적절하게 검토·수정</td></tr>
<tr><td colspan="2">▼</td></tr>
<tr><td>연방 국가 기능 구성
(Federal National Functions Constructs)</td><td>• 명령일로부터 1년 이내에 국토안보부 장관은 주 및 지방정부, 개인이 연방 공무원과의 소통을 개선하고 연방의 역할을 보다 잘 이해할 수 있도록 해당 프레임워크 및 모든 시행 문서를 개괄하는 정책의 변경을 제안해야 함
※ 지금껏 연방정부가 국가 필수 기능, 주요 임무 필수 기능, 국가 중요 기능, 긴급 지원 기능, 복구 지원 기능, 지역사회 복지 프로그램(lifeline) 등 중복되고 광범위한 ‘기능’의 관료적이고 복잡한 관점에서 국가 대비 및 연속성을 조직하고 있음을 지적
• 국가 안보 각서(국가안보위원회 및 소위원회 조직) 또는 후속 절차에 의해 정해진 절차를 통해 조율한 후, 국가안보보좌관을 통해 대통령에게 제출</td></tr>
</table>

2) 국가 사이버보안을 강화하기 위한 선별된 노력 유지(행정명령 제14306호)

○ 오바마 및 바이든 전 행정부의 사이버보안 행정명령(제13694호 및 제14144호)을 일부 수정하여, 외국의 사이버위협에 대한 자국 보호를 강화하고 연방 사이버보안 정책 전반을 간소화('25. 6. 6.)

- 오바마 전 행정부의 행정명령 제13694호(중대하고 악의적인 사이버 기반 활동에 가담하는 특정인의 재산 차단) 및 바이든 전 행정부의 행정명령 제14144호(국가 사이버보안의 혁신 강화 및 촉진)를 일부 수정

〈 행정명령 14306을 통해 개정되는 기존 행정명령 〉

구분	주요내용
행정명령 제13694호 (중대하고 악의적인 사이버 기반 활동에 가담하는 특정인의 재산 차단)	• **오바마** 전 행정부는 미국의 국가안보, 외교 정책 및 경제에 특별한 위협이 되는 **악의적 사이버 행위자**에 대하여 **경제적 제재**를 부과할 수 있는 **재무부 등의 권한** 부여 ('15.4.1.) ※ Executive Order 13694 (Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities)
행정명령 제14144호 (국가 사이버보안의 혁신 강화 및 촉진)	• **바이든** 전 행정부는 미국의 **사이버보안 수준을 개선**하기 위하여 **소프트웨어·클라우드 서비스 제공업체에 대한 책임** 강화, **연방통신 및 신원관리 시스템 보안강화** 등을 명령 ('25.1.16.) ※ Executive Order 14144 (Strengthening and Promoting Innovation in the Nation's Cybersecurity)

○ '중대하고 악의적인 사이버 활동에 가담하는 특정인의 재산 차단에 관한 행정명령 제13694호' 일부 수정

- **(적용대상의 명확화)** 악의적 사이버 활동에 관한 제재대상을 "모든 사람(any person)"에서 "모든 외국인(any foreign person)"으로 수정하여, 해외 사이버위협 행위자에 대한 경제 제재임을 명확화

행정명령 제13694호(오바마 행정부)	행정명령 제14306호(트럼프 행정부)
• **(제1조제(a)항제(ii)호)** 재무부장관이 법무부 및 국무부장관과 협의하여 국가안보, 외교 또는 경제 건전성 또는 재정 안전성에 대한 중대한 위협을 초래하거나 실질적인 기여 가능성이 합리적으로 있는 미국 외부에 있는 자가 이행하거나 지시하는 사이버기반 활동에 직·간접적으로 책임이 있거나 연루된 것으로 판단하는 모든 사람(any person)	• 모든 사람(any person)을 삭제하고, 모든 외국인(any foreign person)으로 수정

○ '국가 사이버보안의 혁신 강화 및 촉진에 관한 행정명령 제14144호' 일부 수정

- **(사이버 위협국의 범위)** 사이버 위협국의 범위를 기존 중국에서 러시아, 이란, 북한 등으로 확장

행정명령 제14144호(바이든 행정부)	행정명령 제14306호(트럼프 행정부)
• **(제1조)** 적대국과 범죄자들은 미국과 미국인을 대상으로 사이버 활동을 수행하고 있으며, 중국은 미국 정부, 민간 부문 및 주요기반시설 네트워크에 가장 적극적이고 지속적인 사이버위협을 행사	• 사이버 위협을 행사하는 국가에 러시아, 이란, 북한 및 기타 국가를 추가

• **(소프트웨어 공급망 보안 증명)** 공급망 보안 측면에서 연방 소프트웨어 공급업체에 소프트웨어 개발 인증서, 검증을 위한 아티팩트 등 증명을 요구한 내용을 삭제하며, 해당 요구사항이 "진정한 보안 투자보다 규정 준수 체크리스트만을 우선시하는 입증되지 않고 부담스러운 회계 절차(Accounting Process)"라고 지적

행정명령 제14144호(바이든 행정부)	행정명령 제14306호(트럼프 행정부)
• **(제2조제(a)항)** 연방정부 및 소프트웨어 제공업체가 보안 소프트웨어 구매 및 개발 관행을 지속적으로 채택·사용하여 소프트웨어 취약점 수와 심각도를 줄이는 조치를 이행 • **(제2조제(b)항) 연방정부는** 보다 엄격한 제3자 위험관리 관행을 채택하고 **중요한 정부 서비스를 지원하는 소프트웨어 제공업체가** 입증된 **관행을 채택하고 있음을 보장** – **소프트웨어 공급업체가** ▲기계가 판독할 수 있는 안전한 소프트웨어 개발 **인증서**, ▲해당 인증서를 검증하기 위한 높은 수준의 **아티팩트**, ▲공급업체의 연방민간행정기관 소프트웨어 **고객 목록**을 CISA에 제출하도록 권고 등	• 제2조제(a)항에서 제(b)항까지 삭제 • 제2조제(c)항, 제(d)항, 제(e)항을 각각 제2조제(a)항, 제(b)항, 제(c)항으로 수정

• **(연방 사이버보안 및 공급망 보안 지침)** 연방 사이버보안 및 공급망 보안 지침에 관한 업데이트 등은 그대로 유지하고 기한을 구체화하는 한편, NIST의 특별 간행물 800-218(안전한 소프트웨어 개발 프레임워크)을 기반으로 연방기관에 소프트웨어 공급망 보안을 지시하는 OMB 각서 M-22-18의 수정 조치를 삭제하며, 지금껏 연방정부가 "기술적 사이버보안 결정을 연방 차원에서 과도하게 관리(Micromanaging)하고 있음"을 지적

행정명령 제14144호(바이든 행정부)	행정명령 제14306호(트럼프 행정부)
	• 제2조제(c)항제(i)호에서 제(iii)호까지의 내용은 유지하는 한편, 기한을 구체화
• **(제2조제(c)항제(i)호)** 상무부장관은 NIST국장을 통해 국가사이버보안우수센터(NCCoE)에 업계와 컨소시엄을 구성하여 NIST 특별 간행물 800-218(안전한 소프트웨어 개발 프레임워크)을 기반으로 보안 소프트웨어 개발, 보안 및 운영 관행을 구현	• **(제2조제(c)항제(i)호)** '25년 8월 1일까지 … (이하 동일) …
• **(제2조제(c)항제(ii)호)** 상무부장관은 NIST 국장을 통해, 'NIST 특별 간행물 800-53(정보시스템 및 조직에 대한 보안 및 개인정보보호 제어)'을 최신화하여 패치 및 업데이트를 안전하고 안정적으로 배포하는 방법에 대한 지침을 제공	• **(제2조제(c)항제(ii)호)** '25년 9월 2일까지 … (이하 동일) …
• **(제2조제(c)항제(iii)호)** 상무부장관은 NIST 국장을 통해 NIST 국장이 적절하다고 판단하는 기관의 장과 협의하여 예비 업데이트를 개발하고 SSDF에 게시	• **(제2조제(c)항제(iii)호)** '25년 12월 1일까지 … (이하 동일) …
• **(제2조제(c)항제(iv)호)** SSDF에 대한 최종 업데이트 후 해당 SSDF에 포함된 소프트웨어의 안전한 개발·제공을 위해 선별된 관행을 OMB각서 M-22-18 또는 관련 요구사항에 통합 • **(제2조제(c)항제(v)호)** 제(iv)호에 명시된 OMB의 최신화된 요구사항을 발행한 후 OMB의 요구사항을 준수하기 위해 보안 소프트웨어 개발 증명을 위한 CISA 공통 양식에 대한 개정안을 준비	• 제2조제(c)항제(iv)호에서 제(v)호까지의 내용 삭제

• **(연방 시스템 및 통신 인프라 강화 관련 지침 등)** 연방민간행정기관이 피싱 방지 표준을 적절하게 사용하고, 국립표준기술연구소(NIST)가 경계 경로 프로토콜(BGP) 사용에 대한 지침을 발행하며, 관리예산국(OMB)이 기관의 이메일 송수신을 위한 전송 계층 보안(TLS) 사용을 확대하도록 권고하는 요구사항을 삭제하는 등 연방정부 및 기관에 부과된 세부적인 지침 발행 의무 등 부담을 줄임

행정명령 제14144호(바이든 행정부)	행정명령 제14306호(트럼프 행정부)
• **(제3조제(a)항)** 연방정부는 ID·액세스 관리를 위하여, 산업계에서 입증된 보안 관행을 채택 • **(제3조제(b)항)** 미래의 혁신적인 ID기술 및 프로세스와 피싱 방지 인증옵션에 대한 투자 우선순위를 정하기 위해, 연방민간행정기관이 OMB 및 CISA가 개발·수립한 간행물을 기반으로 하는 피싱 방지 표준을 적절하게 사용	• 제3조제(a)항에서 제(b)항까지 삭제 • 제3조제(c)항, 제(d)항, 제(e)항을 각각 제3조제(a)항, 제(b)항, 제(c)항으로 수정
• **(제4조제(b)항제(iv)호)** NIST 국장이 연방정부 네트워크 및 서비스 제공업체를 위한 운영상 실행 가능한 BGP 보안 방법의 배포에 대한 업데이트된 지침을 기관에 게시 등	• 제4조제(b)항제(iv)호 삭제
• **(제4조제(d)항제(ii)호)** OMB 국장이 명령일로부터 180일 이내에 연방민간행정기관이 이메일을 송수신하기 위해 사용하는 이메일 서버 간 인증된 전송 계층 암호화의 확장된 사용에 대한 요구사항을 수립 • **(제4조제(d)항제(iii)호)** 해당 요구사항이 수립된 날로부터 90일 이내에 국토안보부 장관이 CISA 국장을 통해 해당 요구사항을 충족할 수 있는 적절한 조치를 이행	• 제4조제(d)항제(ii)호에서 (iii)호까지 삭제

• **(디지털 ID 관련 정책 폐지)** 국립표준기술연구소(NIST)가 공공 혜택 프로그램에 대한 액세스 권한을 부여하기 위해 디지털 ID 수용을 장려하는 정책을 주도하도록 지시한 내용 등을 전부 삭제하며, "불법 이민자들이 공공 혜택을 부적절하게 이용하는 등 광범위한 남용의 위험"이 있음을 지적

행정명령 제14144호(바이든 행정부)	행정명령 제14306호(트럼프 행정부)
• **(제5조)** 도용하거나 합성한 ID를 악용하는 사이버범죄를 해결하기 위해 행정부가 취약 계층에 대한 광범위한 프로그램 접근을 유지하고 개인정보보호, 데이터 최소화 및 상호운영성을 보장 등 – 보조금 지급 권한이 있는 기관의 모바일 운전 면허증 개발, NIST 국장의 디지털 ID 확인을 지원하기 위한 지침 발행 등	• 제5조 삭제 • 제6조에서 제11까지를 제5조에서 제10조로 수정

• **(양자내성암호)** CISA가 양자내성 암호를 지원하는 제품을 쉽게 구할 수 있도록 제품범주 목록을 게시하도록 요구하는 내용 등을 유지하는 한편, 기관이 기술 요청에 양자내성암호 요구사항을 포함하고 국무부, 상무부가 NIST에서 발행한 양자내성암호 표준을 채택하도록 권고한다는 내용은 삭제

행정명령 제14144호(바이든 행정부)	행정명령 제14306호(트럼프 행정부)
• **(제4조제(f)항제(i)호)** 국토안보부장관은 CISA 국장을 통해 양자내성암호(PQC)를 지원하는 제품이 널리 사용가능한 제품 범주목록을 발표하고 정기적으로 최신화	• 제4조제(f)항을 삭제하고 다음을 추가 • **(제4조제(f)항제(i)호)** '25년 12월 1일까지 국토안보부장관은 CISA 국장을 통해 국가안보국장과 협의하여 양자내성암호(PQC)를 지원하는 제품이 널리 사용가능한 제품 범주목록을 발표하고 정기적으로 최신화

행정명령 제14144호(바이든 행정부)	행정명령 제14306호(트럼프 행정부)
• **(제4조제(f)항제(ii)호)** 제품 목록 발표 후 기관은 해당 제품에 대한 요청에 해당 제품이 PQC를 지원한다는 요구사항을 포함하기 위한 조치를 이행 • **(제4조제(f)항제(iii)호)** 기관은 이미 공급된 네트워크 보안 제품·서비스에 최대한 신속하게 PQC 알고리즘을 포함한 PQC 키 설정 또는 하이브리드 키 설정을 구현 • **(제4조제(f)항제(iv)호)** 국무부·상무부 장관은 NIST 국장 및 국제무역 차관을 통해 주요국의 정부 및 산업계를 파악하고 참여시켜 NIST의PQC 알고리즘 표준 전환을 장려	• **(제4조제(f)항제(ii)호)** '25년 12월 1일까지 양자내성암호로 전환을 준비하기 위하여, 국가안보국장과 OMB 국장은 각각 조속히, '30년 1월 2일까지 전송 계층 보안 프로토콜 버전 1.3 또는 후속 버전을 지원하기 위한 요구사항을 발행

• **(사이버방어를 위한 AI 연구)** 연방정부 역할을 사이버방어를 위한 AI 사용에 대한 광범위한 연구, 파일럿 프로그램 실시보다는 사이버방어 연구를 위한 데이터세트 공개, AI소프트웨어 취약점 추적 및 완화에 집중

행정명령 제14144호(바이든 행정부)	행정명령 제14306호(트럼프 행정부)
• **(제6조제(a)항)** 에너지 부문의 주요기반시설에 대한 사이버 방어를 강화하기 위한 AI 사용에 대해 부합하는 파일럿 프로그램을 시작하고, 완료 시 프로그램에 대한 평가를 실시 • **(제6조제(b)항)** 사이버방어를 위해 첨단 AI 모델을 사용하기 위한 프로그램 수립 • **(제6조제(d)항)** 방어적 사이버 분석을 지원하기 위한 인간과 AI간 상호작용 방법, AI 코딩 지원의 보안, 안전한 AI 시스템 설계방법, AI 시스템 관련 사이버사고 예방, 대응, 수정·복구 방법 등의 연구 우선순위를 지정	• 제6조제(a)항, 제(b)항 및 제(d)항의 내용 삭제
• **(제6조제(c)항)** 상무부장관은 NIST 국장을 통해,영업 기밀 유지 및 국가안보를 고려하여 실현 가능한 최대한의 범위까지 사이버방어 연구를 위한 기존 데이터 세트가 광범위한 학술 연구 커뮤니티에 액세스할 수 있도록 보장 • **(제6조제(e)항)** 국방부장관, 국토안보부장관 및 국가정보국장 등은 AI 소프트웨어 취약점 관리*를 해당 기관의 기존 프로세스에 통합	• 제6조제(c)항 및 제(e)항의 내용 유지 • **(제5조제(a)항)** '25년 11월 1일까지 … (이하 동일) … • **(제5조제(b)항)** '25년 11월 1일까지 … (이하 동일) …

• **(사물인터넷(IoT) 보안)** 연방기관에 사물인터넷(IoT) 제품을 공급하는 업체는 '미국 사이버 트러스트 마크' 라벨을 부착하도록 연방조달규정(FAR) 개정을 권고하는 내용을 유지

행정명령 제14144호(바이든 행정부)	행정명령 제14306호(트럼프 행정부)
• **(제7조제(c)항(ii)호)** '27년 1월 4일까지, 연방규정집 제47편 8.203(b)에 정의된 IoT 제품의 공급업체가 해당 제품에 대하여, 미국 사이버 트러스트 마크 라벨을 부착	• **(제7조제(c)항)** 명령일로부터 1년 이내에 연방조달규정 위원회은 해당 법률에 따라 적절하고 일관성 있게 '27년 1월 4일까지 연방규정집 제47편 8.203(b)에 정의된 소비자 IoT 제품의 연방정부 계약업체에게 해당 제품에 대한 사이버 트러스트 마크 라벨을 부착하도록 요구하는 사항을 채택하기 위해 연방조달규정을 개정하는 조치를 공동으로 이행

3. 시사점

○ '주 및 지역의 대응력 강화를 통한 효율의 달성에 관한 행정명령 제14239호('25.3.18.)'는 사이버 공격, 기상 이변 등과 같은 사고·재난 대응의 부담을 연방정부에서 주 및 지역 정부로 전환하고, 관련 전략·정책들을 검토하여 수정할 것을 촉구

- 중국 등 국가 배후 조직의 사이버 위협이 증가하는 가운데, 재임에 성공한 트럼프 2기 행정부는 '정부 효율화'를 강조하고 민간 부문의 자율성을 확대하는 방향으로 사이버보안 정책을 추진
- 트럼프 대통령은 행정명령 제14239호를 통해 모든 주요기반시설, 연속성 및 대비·대응 관련 정책을 단순화하고 위기가 닥쳤을 경우 지방정부가 시민의 요구사항을 보다 잘 이해하고 계획하며 해결할 수 있음을 강조
- 다만, 일각에서는 주요 재난이 선포되었을 때, 인력·예산 등 연방정부의 도움이 없다면 지방정부는 피해 조사, 재난 지원, 공공기반시설 재건 등을 위해 수천 명의 추가 인력을 뽑아야 하고 자체적으로 수십억 달러의 복구 비용을 조달해야 하므로 국가 차원의 대비·대응 태세가 오히려 약화할 수 있음을 우려

○ '국가 사이버보안 강화를 위한 선별된 노력 유지에 관한 행정명령 제14306호('25.6.6.)'는 중대한 악의적 사이버 활동에 관여하는 자에 대한 경제적 제재범위를 외국인으로 제한하고, 사이버보안에 관한 연방정부의 접근방식을 간소화

- 트럼프 대통령은 오바마 전 대통령의 행정명령을 수정하여 악의적 사이버 활동에 관여하는 자를 외국인으로 제한하고, 바이든 전 대통령의 행정명령을 수정하여 사이버 위협국의 범위를 기존 중국에서 러시아, 이란, 북한까지 확장하는 등 국가 안보 관점에서 적대국의 사이버위협 대응을 강조
- 또한 연방기관이 관련 사이버보안 지침을 업데이트하고 차세대 보안기술을 채택하도록 명시한 기존 바이든 전 행정부의 행정명령 제14144호의 큰 틀은 유지하면서도, 연방정부 부담을 줄이고 간소화하는 방향으로 전환
  - 소프트웨어 공급망 보안과 관련하여, 국립표준기술연구소(NIST)의 '안전한 소프트웨어 개발을 위한 지침(NIST 특별 간행물 800-218)' 등을 기반으로 민간의 자율적 참여를 유도하여 과도한 규제 부담을 줄였다는 평가
  - 더불어, 민간 부문과의 협력을 통해 보안 관행을 수립하는 등 규제 완화와 효율성 추구를 중심으로 사이버보안 정책을 재조정할 것으로 예상
- 다만, 일부 사이버보안 전문가들은 기존 행정명령 제14144호의 핵심 요소 중 하나였던 디지털 ID 정책의 삭제와 관련하여, "디지털 ID 의무화 폐지에 대한 집착은 입증된 사이버보안 혜택보다 불법 이민 문제를 우선시한 것"이라고 비판
- 국립표준기술연구소(NIST)등은 동 행정명령에 따라 큰 역할을 수행해야 하나 최근 NIST는 트럼프 2기 행정부의 정부 효율화 기조에 따라 인력·예산 감축에 직면한 연방기관 중 하나로, 관리· 감독에 있어 어려움이 발생할 것이라는 지적도 제기

Reference

- https://www.whitehouse.gov/fact-sheets/2025/03/fact-sheet-president-donald-j-trump-achieves-efficiency-through-state-and-local-preparedness/
- https://www.federalregister.gov/documents/2025/03/21/2025-04973/achieving-efficiency-through-state-and-local-preparedness
- https://www.whitehouse.gov/fact-sheets/2025/06/fact-sheet-president-donald-j-trump-reprioritizes-cybersecurity-efforts-to-protect-america/
- https://www.federalregister.gov/documents/2025/06/11/2025-10804/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694
- https://www.wiley.law/alert-President-Trump-Cyber-Mandate-Analysis-of-Executive-Order-on-Strengthening-US-Cybersecurity
- https://blog.ucs.org/shana-udvardy/7-takeaways-from-trumps-disaster-preparedness-executive-order-and-what-it-means-for-us/
- https://www.politico.com/news/2025/06/06/trump-cyber-executive-order-hacker-sanctions-00393241
- https://www.dwt.com/blogs/privacy—security-law-blog/2025/06/trump-cyber-order-changes-biden-eo-14144
- https://www.mayerbrown.com/en/insights/publications/2025/06/president-trump-signs-cybersecurity-executive-order
- 한국인터넷진흥원, 『[25-19] 미국 FCC, 통신 부문에서의 적대국의 위협에 대한 대응조치 발표』, 2025. 6. 23.

부록

국내 인터넷·정보보호 입법동향 목록

○ 입법예고된 법령

법령명	입법예고 기간	주요내용
「전기통신사업법 시행령」 일부개정령안 입법예고	2025. 5. 30. ~ 2025. 7. 9.	• **(소관부처)** 과학기술정보통신부 • **(개정이유)** 문자사업자의 등록요건 준수 여부 등을 점검할 수 있도록 점검사항 · 방법 · 절차 등의 구체화 등 위임사항을 규정하고, 불법스팸 방지 종합대책('24.11.28.)의 후속조치 등을 반영하기 위함 • **(주요내용)** – 「전기통신사업법」 제22조제4항 신설에 따라 문자사업자의 등록요건 준수 여부 등을 정기 점검할 수 있도록 점검사항 · 방법 · 절차 등 규정 – 등록요건 미준수 및 불법스팸 관련 시정명령 불이행 사업자에 대해 사업 정지, 등록취소 할 수 있도록 처분기준 마련 – 문자사업자의 기술적 · 관리적 조치의 강화, 자본금 요건 강화, 인력 요건 명확화 등 불법스팸 방지를 위해 갖춰야 할 사전적 의무를 등록요건에 반영

○ 공포된 법령

법령명	공포일	주요내용
「개인정보 보호법」 일부개정	2025. 4. 1.	• **(소관부처)** 개인정보보호위원회 • **(개정이유)** 개인정보처리자의 국내대리인 관리·감독 의무에 대한 규정과 국내대리인 지정 요건에 국내 소재 외에 그 형태나 운영방식에 대한 별도 규정이 없다는 지적 제기 • **(주요내용)** – 개인정보처리자에게 국내대리인 관리·감독 의무를 부과 – 개인정보처리자가 국내 법인을 설립·운영 중인 경우, 해당 법인을 국내대리인으로 지정하도록 규정 – 국내대리인 관리·감독을 소홀히 하거나 지정 요건에 따라 국내대리인을 지정하지 않는 경우 등에 과태료 부과
「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령」 일부개정	2025. 5. 20.	• **(소관부처)** 과학기술정보통신부 • **(개정이유)** 연계정보 생성 · 처리의 안전성 확보를 위해 본인확인기관 및 연계정보 이용기관이 이행해야 하는 조치를 정하고, 불법정보 유통 방지를 위한 기술적 · 관리적 조치 의무 대상자의 기준 등을 정하기 위함 • **(주요내용)** – 본인확인기관의 연계정보 생성 · 처리 안정성 확보를 위한 조치 및 연계정보 이용기관의 연계정보 분실 · 도난 방지를 위한 안전조치 규정 – 불법정보의 유통 방지를 위한 기술적 · 관리적 조치를 해야 하는 의무 대상자의 기준을 규정

○ 발의된 법률안

법령명	공포일	주요내용
「지능정보화 기본법」 일부개정법률안 (이언주의원 대표발의)	2025. 4. 11.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 데이터센터가 전자파 유해성 등을 이유로 기피시설로 인식됨에 따라 수도권 지역 등에서 데이터센터 구축이 지연·취소되는 사례 발생 • **(주요내용)** – 정부는 수도권 외 지역 또는 산업단지 등에 구축 · 운영하는 데이터센터를 우선 지원하고, 수도권으로부터의 거리, 인구수 등을 고려하여 지원비율 차등화
「지능정보화 기본법」 일부개정법률안 (윤준병의원 대표발의)	2025. 4. 18.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 데이터센터가 수도권 등에 집중되어 발전소와의 거리로 발생하는 송전비용, 송전탑 건설 등으로 초래되는 환경문제, 그리고 국토균형발전에 역행하는 문제 등을 제대로 고려하지 않았다는 비판 제기 • **(주요내용)** – 데이터센터의 구축 및 운영 활성화 시책을 수립 · 시행할 경우, 발전소와의 근접성, 국토균형발전 등 대통령령으로 정하는 요소를 고려하도록 함
「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법」 일부개정법률안 (이언주의원 대표발의)	2025. 4. 11.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** AI 데이터센터 건립 필요성이 증대되고 있으나 데이터센터가 기피시설로 인식됨에 따라 데이터센터 구축이 지연·취소되는 사례 발생 • **(주요내용)** – 정부는 수도권 외 지역 또는 산업단지 등에 구축·운영하는 데이터센터를 우선 지원하고 수도권으로부터 거리, 인구수 등을 고려하여 지원규모 차등화
「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법」 일부개정법률안 (황정아의원 대표발의)	2025. 4. 17.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 미국은 AI 행정명령 폐기 및 혁신 중심 정책을 추진하는 등 EU, 일본을 포함한 전세계적 AI 트렌드가 규제에서 진흥으로 전환됨에 따라 현행법에서 규제관련 규정의 적용을 일정 기간 유예할 필요성 제기 • **(주요내용)** – AI 사업자에 대한 의무나 책임을 부과하는 일부 규제조항(AI 투명성·안전성 확보의무, 고영향 AI 관련의무)에 대하여 그 시행일을 3년 유예
「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법」 일부개정법률안 (이정헌의원 대표발의)	2025. 5. 29.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** AI 기술 전문인력의 근로환경 개선 및 처우개선 등 복지지원 체계를 마련하기 위함 • **(주요내용)** – 과기정통부장관이 전문인력의 직무역량 강화 및 경력개발을 위한 교육훈련 프로그램 개발·활용 등을 포함한 사업을 추진할 수 있도록 함
「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법」 일부개정법률안 (박수현의원 대표발의)	2025. 6. 13.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 현행법은 생성형 인공지능의 학습용 데이터 공개 의무 등 창작자 보호를 위한 구체적 규정을 두고 있지 않아 창작자의 권리 침해될 우려가 제기 • **(주요내용)** – 저작물 등의 권리자가 자신의 저작물 등이 학습용 데이터로 이용되었는지 확인을 요청하는 경우 해당 여부를 확인할 수 있는 절차를 마련 – AI 사업자들이 투명성 확보 의무를 자율적으로 준수할 수 있도록 민관 협의체를 구성할 수 있는 근거 마련

법령명	공포일	주요내용
「인공지능 발전과 신뢰 기반 조성 등에 관한 기본법」 일부개정법률안 (김기현의원 대표발의)	2025. 6. 17.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 현행법은 생성형 인공지능의 학습용 데이터를 확인할 수 있는 절차 등 창작자 보호를 위한 구체적 규정이 미비 • **(주요내용)** – 저작물 등의 권리자가 자신의 저작물 등이 학습용 데이터로 이용되었는지 확인을 요청하는 경우 해당 여부를 확인할 수 있는 절차를 마련
「인공지능산업 인재 육성에 관한 특별법안」 제정법률안 (정동영의원 대표발의)	2025. 5. 9.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 산업 전반에 걸쳐 AI 전문인재에 대한 수요가 급증하고 있으나 국내 인재양성 속도는 이에 부응하지 못한다는 의견 제기 • **(주요내용)** – 과기정통부장관은 AI산업 인재의 체계적 육성을 위하여, 5년마다 기본계획을 수립하고 관계 중앙행정기관의장 및 시도지사 등은 시행계획을 수립·시행 – 대통령령으로 정하는 공공기관에 AI산업 인재육성센터를 구축 – 과기정통부장관은 기업부설 교육훈련기관 또는 기업의 교육훈련부서를 기업 AI산업 인재개발기관 또는 전담부서로 지정 가능 – 국가 및 지자체는 AI 교육기관 등의 시설·설비 확보, 장학금·실습비 등 지급 및 대학 또는 대학원의 정원 조정 등에 필요한 지원 가능 – 과기정통부장관은 지역별 AI 거점대학을 지정 가능 – 국가 및 지자체는 우수 해외인재 유치를 위하여 국내 정착을 위한 지원 사업을 할 수 있고 법무부장관은 이민절차 완화 등 필요한 시책을 추진 가능
「인공지능산업 육성 및 강국 도약을 위한 특별법안」 제정법률안 (최민희의원 대표발의)	2025. 6. 20.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 우리나라는 세계에서 두 번째로 「AI 기본법」을 제정('25.1.)하여 AI 산업 육성의 틀을 마련하였으나, AI 산업을 체계적으로 진흥하고 육성하기 위한 제도적 기반이 부족한 상황 • **(주요내용)** – AI기술·산업 육성을 위하여 AI 산업경쟁력강화전략계획의 수립, AI 메가 클러스터의 지정 및 조성·운영 지원 등에 필요한 근거 마련 – AI 신기술 연구사업의 추진·실증 및 확산 등을 위하여 AI 신기술의 지정, AI 전략사업에 관한 특례 등에 필요한 근거 마련 – AI산업 인력 육성시책 마련, 해외 우수인력 유치, AI 산업 분야 인력 수급 동향 조사, AI 산업 지역인력 확보 등에 필요한 근거 마련 – AI 인프라 확충 지원 및 관계 법률에 관한 특례, AI 데이터센터 특구 지정 및 지원, 예비타당성조사에 관한 특례 등에 필요한 근거 마련
「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안 (조인철의원 대표발의)	2025. 4. 14.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 정보통신서비스 제공자등의 국내대리인의 지정 요건에 국내 소재 외에 그 형태나 운영방식에 대한 별도 규정이 없다는 지적 제기 • **(주요내용)** – 정보통신서비스 제공자등이 국내 법인을 설립 · 운영 중인 경우, 해당 법인을 국내대리인으로 지정 – 정보통신서비스 제공자등이 국내대리인을 지정하거나 변경하는 경우 방송통신위원회에 통보

법령명	공포일	주요내용
		- 국내대리인은 이 법에 따른 업무 수행을 위한 담당자를 지정하여야 하며, 담당자는 국내대리인, 정보통신서비스 제공자등, 방송통신위원회 또는 과학기술정보통신부와 상시 연락이 가능하도록 필요한 조치를 이행
「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안 (조인철의원 대표발의)	2025. 4. 15.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 해외 온라인플랫폼을 통해 불법정보 등이 유통되는 사례가 발생하고 있으나 해외 사업자의 경우 신속한 제재가 어렵다는 문제점 제기 • **(주요내용)** - 국내대리인으로 하여금 불법정보에 대한 방송통신위원회 명령의 이행계획, 이행상황 및 이행결과를 통보하는 업무를 대리하도록 규정
「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안 (김상훈의원 대표발의)	2025. 5. 1.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 정보통신망에서의 AI 기술 활용 생성물의 유통을 규제하기 위한 직접적 규정이 미비하여, 실제와 구분하기 어려운 합성물이 급증 • **(주요내용)** - 정보제공자에게 AI기술로 생성한 딥페이크 영상 등의 표시의무를 규정하고, 해당 표시를 훼손하고 영리목적으로 제공하는 내용의 정보를 불법정보로 규정
「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안 (조인철의원 대표발의)	2025. 5. 22.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 최근 침해사고 발생으로 대규모 개인정보가 유출되었음에도 해당 정보통신서비스 제공자의 소극적 대응과 미흡한 피해구제 조치 등으로 이용자 우려가 급증 • **(주요내용)** - 과기정통부장관이 침해사고 예방 및 피해확산 방지를 위하여, 침해사고 관리/대응 매뉴얼 표준안을 마련하여 보급하도록 규정 - 정보통신서비스 제공자가 침해사고 관련 자료 제출명령을 이행하지 않는 경우 이행강제금을 부과하는 근거 마련
「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안 (김상훈의원 대표발의)	2025. 6. 11.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 최근 이동통신사 해킹 사고를 비롯한 정보통신망 침해사고가 반복되고 있고, 향후 유사사고의 재발을 방지하기 위하여 정보보호 관리 인증체계에 대한 개선과 함께 인증 관리·감독체계를 강화할 필요성 • **(주요내용)** - 정보보호 관리체계를 수립·운영하고 있는 자 중 이동통신 등 보안 관련 고위험 산업군에 대하여, 강화된 정보보호 인증기준을 적용 - 정보보호 관련 법령의 중대한 위반 시 인증을 취소할 수 있도록 하고, 인증 사후관리 시 현장심사 강화와 인증 미이행 시 과징금 부과
「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안 (이해민의원 대표발의)	2025. 6. 12.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 사이버 침해사고 발생 시, 관련 사업자가 과기정통부장관의 협조요청을 거부하거나 거짓자료를 제출하더라도 1천만원 이하의 과태료 외에 실질적 제재수단이 없어 조사의 실효성이 저하된다는 지적 • **(주요내용)** - 과기정통부장관이 사업자의 자료제출 거부나 현장조사 방해 등에 대하여 이행강제금을 부과할 수 있도록 규정

법령명	공포일	주요내용
		※ 이행기한이 지난 날부터 1일당 대통령령으로 정하는 1일 평균 매출액의 1천분의 3의 범위에서 이행강제금 부과가능한 한편, 매출이 없거나 매출액 산정이 곤란한 경우 이행기한이 지난날부터 1일당 200만원의 범위에서 이행강제금 부과 가능
「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안 (최민희의원 대표발의)	2025. 6. 19.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 침해사고가 발생하였으나 정부와 해당 정보통신서비스 제공자의 소극적 대응과 미흡한 피해구제 조치 등으로 인한 피해 확산 • **(주요내용)** – 중대한 침해사고 발생 시 예보·경보·통지의 방법을 구체적으로 규정 – 침해사고로 인한 이용자 피해 확산 방지와 신속한 피해구제에 대한 정보통신서비스 제공자의 의무부과 및 미이행시 과태료 상향
「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안 (구자근의원 대표발의)	2025. 6. 24.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** '24년 기준 SKT의 정보기술 투자금액 대비 정보보호 투자금액 비율은 4.1%로 타사에 비해 낮은 수준이었는바, 정보보호 투자금액을 일정 비율 이상 확보하기 위함 • **(주요내용)** – 주요 정보통신서비스 제공자 등에게 정보기술부문 예산에 일정 비율 이상의 정보보호 예산을 반영하도록 규정을 마련
「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안 (김장겸의원 대표발의)	2025. 6. 26.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 해외사업자의 형식적인 국내대리인 제도 운영으로 인하여 국내 이용자의 권리가 제대로 보호되고 있지 않다는 지적이 제기 • **(주요내용)** – 정보통신서비스 제공자가 국내대리인을 지정하거나 변경하는 경우 방송통신위원회에 통보하도록 규정 – 정보통신서비스 제공자가 설립한 국내 법인이나 지배적인 영향력을 행사하는 법인이 있는 경우 해당 법인을 국내대리인으로 지정하도록 규정
「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안 (이해민의원 대표발의)	2025. 6. 30.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 정보보호 예산 투자나 정보보호 관리체계 운영 실태 등 정보통신망 사업자의 정보보호 수준을 체계적으로 평가하고 관리하는 제도적 장치가 부족하다는 지적 제기 • **(주요내용)** – 일정 규모 이상 정보통신망 사업자를 대상으로 하는 정보보호 수준 평가를 의무화하고 평가 결과를 공개하도록 규정
「디지털포용법」 일부개정법률안 (정진욱의원 대표발의)	2025. 6. 9.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** '26년 1월 22일 시행을 앞둔 동법은 침해사고와 같은 긴급 상황에서의 신속한 지원이나 보호조치가 규정되어 있지 않다는 문제 제기 • **(주요내용)** – 국가·지자체가 침해사고 발생 시 디지털 취약계층의 침해사고 대응을 지원할 수 있는 법적 근거 마련

법령명	공포일	주요내용
「디지털포용법」 일부개정법률안 (최민희의원 대표발의)	2025. 6. 19.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 고령층, 장애인 등 디지털 취약계층에 대한 지원 근거나 보호 조치가 구체적으로 규정되어 있지 않아 침해사고 발생 시 피해를 예방하거나 확산방지 조치를 취하기 어렵다는 지적 제기 • **(주요내용)** – 디지털 취약계층의 침해사고 대응 지원에 관한 근거 조항 신설 – 국가·지자체의 침해사고 발생 시 디지털 취약계층 침해사고 대응 지원 책무 규정
「개인정보 보호법」 일부개정법률안 (이정문의원 대표발의)	2025. 5. 1.	• **(소관위원회)** 정무위원회 • **(제안이유)** SKT의 유심정보 유출 사례 등 개인정보처리자가 사후 유통 실태를 추적하고 확산을 방지하는 노력이 미흡하다는 지적 제기 • **(주요내용)** – 개인정보처리자가 일정 건수 이상의 개인정보 유출사고가 발생한 경우 등 일정기간 동안 불법거래 사이트 등을 모니터링하고 유출 정보의 고발 등 후속조치를 수행하도록 규정
「개인정보 보호법」 일부개정법률안 (이해민의원 대표발의)	2025. 6. 12.	• **(소관위원회)** 정무위원회 • **(제안이유)** 침해사고 지체뿐 아니라, 사고 발생 이후 미흡한 후속조치가 소비자 불안과 사회 혼란을 더욱 증폭시킨다는 지적이 제기 • **(주요내용)** – 개인정보처리자가 유출 등을 알게 된 경우, 정보주체에게 알려야 할 정보를 구체화하고 개별 통지를 의무화함 – 개인정보처리자가 사고 발생 후 후속조치 계획을 수립하여 개인정보보호위원회 및 정보주체에게 이를 알리도록 규정
「개인정보 보호법」 일부개정법률안 (이헌승의원 대표발의)	2025. 6. 13.	• **(소관위원회)** 정무위원회 • **(제안이유)** 「정보통신망법」 상 침해사고 신고는 24시간 이내에, 「개인정보보호법」은 개인정보 유출을 인지한 때로부터 72시간 이내에 신고하도록 규정되어 제도상 신고기한의 불일치가 발생 • **(주요내용)** – 개인정보 유출 · 침해사고를 인지한 때로부터 24시간 이내에 관계기관에 신고하도록 의무를 강화
「개인정보 보호법」 일부개정법률안 (최민희의원 대표발의)	2025. 6. 19.	• **(소관위원회)** 정무위원회 • **(제안이유)** 개인정보처리자가 유출사고 발생 시 법정 사항에 대한 개별적 통지 없이 홈페이지에 간략한 안내만을 게시할 경우, 적절한 대응조치를 취할 기회를 놓치게 만든다는 지적 • **(주요내용)** – 유출된 개인정보의 주체를 특정할 수 없고, 유출 규모가 대통령령으로 정한 기준 이상일 경우, 개인정보처리자가 유출 등이 확인된 정보주체 및 유출 가능성이 있는 모든 정보주체에 법정 통지사항을 개별 통지하도록 규정

법령명	공포일	주요내용
「전기통신사업법」 일부개정법률안 (전용기의원 대표발의)	2025. 5. 1.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** SKT 유심정보 유출 사고 등 이용자가 계약을 해지하더라도 약정 위약금이 부과되어 자유로운 해지가 어렵다는 지적 제기 • **(주요내용)** – 전기통신사업자의 귀책사유를 법률에 명시하여, 이용자가 해당 사유로 계약을 해지할 경우 위약금이나 할인반환금 등 명칭에 제한없이 해지에 따른 경제적 부담을 면제하도록 규정
「전기통신사업법」 일부개정법률안 (한정애의원 대표발의)	2025. 5. 8.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 이동통신단말장치 개통 시 대포폰 개통 및 사용에 대한 불법성 등 고지절차가 없어 범죄 이용가능성에 대한 인지없이 대포폰 개통이 이뤄지는 경우가 많다는 지적 제기 • **(주요내용)** – 전기통신사업자가 전기통신역무 제공에 관한 계약을 체결하기 위한 본인 확인 절차에서 이용자에게 대포폰 개통 및 사용의 불법성과 범죄 연루 위험성 등 내용을 고지하는 의무부과 – 해당 위반사실에 대하여 자진신고하는 경우 형을 감경하거나 면제할 수 있는 근거 마련
「전기통신사업법」 일부개정법률안 (최민희의원 대표발의)	2025. 6. 27.	• **(소관위원회)** 과학기술정보방송통신위원회 • **(제안이유)** 최근 SKT 해킹사고 발생 시, 과기정통부장관이 이용자 피해 확산 방지를 위하여 유심보호서비스를 제공하도록 행정지도하였으나, 방통위가 동법에 따른 이동통신사업자에 대한 금지행위로 해석함에 따라 긴급한 이용자 보호조치의 법적 근거와 관련한 논란이 제기 • **(주요내용)** – 과기정통부장관이 해킹 등 정보통신망 침해사고로 인한 피해확산 방지 등 이용자 보호가 긴급히 필요하다고 판단하는 경우, 해당 이동통신사업자에게 특정 부가서비스 제공 등 필요한 조치를 명할 수 있는 근거 마련 – 이동통신사업자가 이러한 명령 이행을 위해 이용약관과 다르게 서비스를 제공하는 경우를 금지행위의 예외로 명시

부록

해외 인터넷·정보보호 입법동향 목록

○ ’25년 1월

국가	입법동향
튀르키예	• 사이버보안기구 설립을 위한 대통령령 공포 (’25.1.8.)
영국	• 랜섬웨어 법안 추진을 위한 의견수렴 (’25.1.14.)
미국	• 연방통신위원회(FCC), 국가통신시스템의 사이버보안 강화를 위한 잠정규정예고문 발표 (’25.1.16.)

○ ’25년 2월

국가	입법동향
미국	• 미시시피 주 하원, 「사이버보안 표준준수 조직의 면책법(안)」 발의 (’25.1.20.)
미국	• 상원, 「사이버보안 보험법(안)」 발의 (’25.1.24.)
미국	• 상원, 「라우터법(안)」 발의 (’25.1.27.)
EU	• 개정 「사이버보안법」 및 「사이버연대법」 발효 (’25.2.4.)
일본	• 일본, 「사이버 대응역량 강화법(안)」 국회제출 (’25.2.7.)

○ ’25년 3월

국가	입법동향
호주	• 「스캠 방지 프레임워크법」 제정 (’25.2.20.)
스페인	• 「사이버보안 조정 및 거버넌스에 관한 법률」 초안 의견수렴 (’25.2.10.)
EU	• 집행위원회, 「사이버복원력법」 이행규정 초안 발표 (’25.3.14.)

○ ’25년 4월

국가	입법동향
프랑스	• 상원, 「주요기반시설 복원력 및 사이버보안 강화법안」 승인 (’25.3.12.)
중국	• 「네트워크안전법」 개정안 의견수렴 (’25.3.28.)
영국	• 사이버보안 및 복원력 법안 관련 정책문서 발표 (’25.4.1.)
미국	• 하원, 「국가 배후 위협 행위에 대한 사이버 복원력 강화법안」 발의 (’25.4.7.)
EU	• 「사이버보안법」 개정 관련 의견수렴 (’25.4.11.)

’25년 5월

국가	입법동향
미국	• 하원, 「양자내성 사이버보안 표준법안」 발의 (’25.5.7.)
일본	• 일본 의회, 「사이버 대응능력 강화법안」 통과 (’25.5.16.)

’25년 6월

국가	입법동향
미국	• 연방통신위원회, 통신 부문에서의 적대국의 위협에 대한 대응조치 발표 (’25.5.27.)
일본	• 일본, 「인공지능 관련 기술의 연구개발 및 활용 촉진에 관한 법률」 제정 (’25.6.4.)

※ 해외 인터넷·정보보호 입법동향 목록은 한국인터넷진흥원의 공식 홈페이지(지식플랫폼)에 수시로 게재되는 「인터넷·정보보호 법제동향」 목록임을 안내드립니다.

2025년 2분기

인터넷·정보보호 법제동향

『인터넷·정보보호 법제동향』은 디지털·정보보호 관련 입법동향 및 주요 이슈를 분석하여 정책 자료로 활용하기 위해 한국인터넷진흥원에서 기획, 발간하는 분석보고서입니다.

한국인터넷진흥원(KISA) 정책연구실 법제연구팀

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY