Vol. 139 (April 2019)

인터넷 법제동향

Laws and Policy Trends of the Internet

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

CONTENTS

국내 입법 동향

해외 입법 동향

기고

<공포된 법령>		
법령명	**공포일**	**주요내용**
• 「정보보호산업의 진흥에 관한법률 시행령」 일부개정령	2019. 4. 2.	- 정보보호제품 성능평가기관 지정신청의 접수 및 지정요건 충족 여부 심사를 한국인터넷진흥원에 위탁함
<국회 제출 법률안>		
법령명	**대표발의 의원 (발의날짜)**	**주요내용**
• 「개인정보 보호법」 일부개정법률안	강창일의원 (2019. 4. 12.)	- 60일 이내 집단분쟁조정 절차를 개시할 것을 의무화하고, 분쟁조정 연장요건을 규정
• 「블록체인산업 진흥에 관한 법률」 제정안	송희경의원 (2019. 4. 4.)	- 블록체인 산업 발전을 위해 블록체인 산업의 진흥에 관한 시책을 수립·시행
• 「전자정부법」 일부개정법률안	신용현의원 (2019. 4. 17.)	- 행정기관등의 장이 정보통신망을 구축·운영할 때에는 이중화회선으로 함
• 「청소년보호법」 일부개정법률안	손금주의원 (2019. 4. 30.)	- 디지털 만화를 매체물에 포함하여 청소년 유해매체물로 분류될 경우 정보통신망에 광고나 선전물을 배포·게시할 수 없음

「정보보호산업의 진흥에 관한 법률 시행령」 일부개정령 공포
(공포 2019. 4. 2., 시행 2019. 4. 2.)

▶ 소관부처 : 과학기술정보방송통신위원회

▶ 제안이유

o 정보보호 공시의 명확성, 투명성을 높이기 위해 공시내용의 작성기준, 공시방법 및 절차 등을 고시로 위임하는 근거규정을 마련하고, 사업수행의 전문성과 효율성을 강화하기 위해 정보보호제품 성능평가기관 지정신청의 접수 및 지정요건의 심사업무를 한국인터넷진흥원에 위탁하며, 일부 전문기관에만 위탁되어 있던 정보보호 기업의 해외진출 지원 및 정보보호 인력양성 사업을 전문기관으로 지정받은 모든 기관 중에서 과학기술정보통신부장관이 고시하는 기관에 위탁하도록 하려는 것임

▶ 주요내용

o 법 제17조제2항에 따른 성능평가기관 지정신청의 접수 및 이 영 제10조제2항·제4항에 따른 지정요건의 충족 여부 심사를 한국인터넷진흥원에 위탁함(제27조제2항10호의 2 신설)

※ **Reference**

국가법령정보센터 (http://www.law.go.kr/)

「개인정보 보호법」 일부개정법률안
(강창일의원 대표발의, 2019. 4. 12. 제안)

▶ 소관 상임위원회 : 행정안전위원회

▶ 제안이유

o 분쟁조정제도는 법원판결에 비해 신속한 분쟁해결이 가능하도록 하려는 제도이며, 더 나아가 집단분쟁조정제도는 정보주체의 피해 또는 권리침해가 다수의 정보주체에게 같거나 비슷한 유형으로 발생한 사건을 하나의 분쟁조정절차에서 일괄적으로 해결하여 개별적인 분쟁조정절차에 따른 시간적·비용적 낭비를 해소하고자 하는 제도임

o 그런데 현행법상의 집단분쟁조정제도는 분쟁조정위원회의 의결로써 절차를 개시할 수 있다고만 규정하여 집단분쟁조정을 의뢰 또는 신청하는 자의 입장에서는 집단분쟁조정 절차의 개시 시점을 예측하기 어렵고, 분쟁조정위원회가 개시 여부를 정하는 데에만 수개월이 소요되는 경우가 발생하여 신속한 권리구제의 도모라는 제도 도입 취지를 달성하기 어려운 상황임

o 한편, 현행법은 분쟁조정 및 집단분쟁조정의 분쟁조정기간 연장 요건을 "부득이한 사정이 있는 경우"로 규정하여 포괄적인 해석에 따른 분쟁조정위원회의 재량이 넓게 인정될 여지가 있어 분쟁조정기간이 장기화되는 하나의 요인으로 작용하고 있다는 지적이 있어 왔음

▶ 주요내용

o 예외적인 경우를 제외하고는 분쟁조정위원회의 의결로써 집단분쟁조정을 의뢰받거나 신청받은 날부터 60일 이내에 집단분쟁조정 절차를 개시하도록 의무화하고, 분쟁조정기간의 연장요건을 한정된 개념인 "정당한 사유가 있는 경우"로 보다 엄격히 규정함으로써 신속한 분쟁조정이 이루어질 수 있도록 입법정비를 하려는 것임(안 제44조제1항 단서 및 제49조)

※ **Reference**

의안정보시스템 (http://likms.assembly.go.kr/bill/main.do)

「블록체인산업 진흥에 관한 법률」 제정안
(송희경의원 대표발의, 2019. 4. 5. 제안)

▶ **소관 상임위원회 : 과학기술정보방송통신위원회**

▶ **제안이유**

o 블록체인 시장을 선점하기 위한 글로벌 경쟁이 가속화되고 있으나, 국내 블록체인 기술 경쟁력은 미국, 일본, 중국 등 경쟁국에 비해 낮은 수준이며, 블록체인 기술을 구현할 수 있는 전문인력도 부족한 상황일 뿐 아니라 정부가 블록체인 기술 및 산업 지원을 체계적으로 지원할 수 있는 법적 체계도 미비한 상황임

o 아직 초기단계인 블록체인 기술의 글로벌 시장 선점을 위해 블록체인 산업이 발전할 수 있는 생태계를 조성하고, 블록체인 기술의 장점을 활용하여 공공·민간의 업무를 효율화하여 4차 산업혁명 시대의 새로운 가치 창출에 이바지하기 위한 법적 근거를 마련하려는 것임

▶ **주요내용**

o 과학기술정보통신부장관은 블록체인 기술에 관한 표준의 제정·개정 또는 폐지와 그 표준의 보급 등 블록체인 기술 수준을 향상시키고 서비스의 활용도를 높이기 위하여 표준화 사업을 할 수 있도록 함(안 제8조)

o 과학기술정보통신부장관은 블록체인 기술과 관련된 지식재산권을 보호하기 위하여 지식재산권 보호시책을 강구하도록 하고, 블록체인 산업의 진흥에 필요한 전문인력의 육성 및 관리를 위하여 필요한 시책을 마련하고 추진하도록 함(안 제9조 및 제10조)

o 정부는 블록체인 산업과 관련한 산업계·학계 및 연구계가 일정한 지역에서 유기적 연계를 통하여 블록체인 기술 연구개발의 효율을 높이고, 국내외 블록체인 기술 집약 기업을 유치하거나 육성하기 위하여 블록체인 진흥단지를 지정하거나 조성할 수 있도록 함(안 제12조)

※ **Reference**

의안정보시스템 (http://likms.assembly.go.kr/bill/main.do)

「전자정부법」 일부개정법률안
(신용현의원 대표발의, 2019. 4. 17. 제안)

▶ 소관 상임위원회 : 행정안전위원회

▶ 제안이유

o 2018. 11. 24. KT 아현지사 빌딩 지하 통신구 화재로 KT망의 유·무선 통신 장애가 발생하여 ATM 등 은행업무뿐만 아니라 카드결제기, 경찰 시스템 등에 문제가 발생한 바 있음

o 이 사고 이후에 행정안전부가 중앙부처 및 지방자치단체를 대상으로 조사한 "행정기관 정보 통신망 통신회선 현황"에 따르면, 전체 대상기관 회선 중 이중화 회선은 22%에 불과하며, 사업자를 이원화한 회선도 전체 회선의 6%에 그치는 것으로 나타났음

o 행정기관등의 대국민 서비스가 확대되고, 국민의 안전과 생활에 밀접한 공공서비스의 안정적 제공의 중요성이 높아져 가고 있는 현 시점에서 정보통신망 안전에 대한 특단의 대책이 필요한 실정임.

▶ 주요내용

o 대통령령으로 정하는 행정기관등의 장이 정보통신망을 구축·운영할 때에는 정보통신망의 회선을 각각 다른 사업자로부터 제공받아 이중화 회선으로 하도록 하려는 것임 (안 제52조의2 신설)

※ **Reference**

의안정보시스템 (http://likms.assembly.go.kr/bill/main.do)

「청소년 보호법」 일부개정법률안
(손금주의원 대표발의, 2019. 4. 30. 제안)

▶ 소관 상임위원회 : 여성가족위원회

▶ 제안이유

o 현행 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」은 청소년 및 아동이 음란물, 유해매체물에 노출되는 것을 방지하기 위해 청소년유해매체물을 광고하는 내용의 정보를 정보통신망을 이용하여 부호·문자·음성·음향·화상 또는 영상 등의 형태로 청소년에게 전송하거나 청소년 접근을 제한하는 조치 없이 공개적으로 전시하지 못하도록 하고 있음

o 그러나 웹툰 등 온라인에 노출된 디지털 만화에 관한 광고나 선전물에 대하여는 이를 여과하는 제도적 장치가 없어 청소년이 선정적이고 자극적인 웹툰 등 디지털 만화에 관한 광고나 선전물에 무방비로 노출되고 있음.

▶ 주요내용

o 웹툰 등 디지털 만화를 매체물에 포함, 청소년보호위원회 및 각 심의기관의 심의를 거쳐 청소년유해매체물로 분류될 경우 광고나 선전물을 배포·게시할 수 없도록 함으로써 청소년을 유해한 환경으로부터 보호하고자 함(안 제2조제2호카목 신설)

※ **Reference**

의안정보시스템 (http://likms.assembly.go.kr/bill/main.do)

해외 입법 동향 EU

유럽 집행위원회, 5G 네트워크의 사이버보안 권고안 발표 (2019. 03. 26.)

유럽 집행위원회는 5G[1] 네트워크의 사이버보안 위험을 평가하고 진화되는 사이버위협에 대한 대응 능력을 강화하기 위해 《5G 네트워크의 사이버보안 권고안》[2]을 발표 (2019. 03. 26.)

▶ 개요 및 경과

o 유럽 집행위원회는 5G 네트워크의 상용화로 예상되는 사이버위협에 대한 EU 공동의 대응 능력을 강화하기 위해 사이버보안 위험 평가를 실시하고 예방 조치를 지원하는 권고안을 발표

- 이 권고안은 ▲국가 수준의 5G 네트워크 사이버보안 위험 평가 ▲유럽네트워크정보보호원(ENISA)[3]을 통한 EU 전역의 사이버보안 위험 현황 정리 및 해결 방안 마련 등을 주요 내용으로 하고 있음

o 유럽 의회에서 최근에 승인한 《EU 사이버보안법》[4]이 발효되면 유럽네트워크정보보호원(ENISA)은 EU 차원의 5G 네트워크 사이버보안 인증체계를 수립할 예정

- ENISA는 회원국들 간의 5G 네트워크 사이버보안 인증계획 수립을 위한 정보 공유와 협력을 촉진

▶ 주요 내용

o **(권고안의 목적)** EU의 5G 네트워크 사이버보안 수준을 향상시키고 관련 산업을 활성화하는 것임

- 회원국은 5G 네트워크의 사이버보안 위험을 평가하고, 국가적인 차원에서 자체적으로 필요한 보안 조치를 취해야 함

---

1) 5세대 이동통신(Fifth Generation Mobile Communications): 최대속도가 20Gbps에 달하는 이동통신의 다섯 번째 세대기술로, 초저지연성과 초연결성을 통해 가상현실, 자율주행, 사물인터넷 기술 등을 구현할 수 있음

2) European Commission recommends common EU approach to the security of 5G networks

3) European Union Agency for Network and Information Security: 유럽 전역의 사이버보안 역량 강화 지원을 위한 기관으로 당초 2020년을 기점으로 임무 수행 기간이 종료될 예정이었으나, 《EU 사이버보안법》 발효 시 한시 조직지위에서 EU 산하의 상설 조직으로 전환될 예정임

4) 2019년 4월 17일에 동 법안의 공식적인 승인절차가 모두 완료되었으며, 유럽 연합의 공식 저널에 게재될 예정임. 승인된 법은 공식 저널을 통해 발행된 날로부터 20일 후에 시행하도록 규정함.

- 국가별 5G 네트워크의 사이버보안 위험 평가 결과를 기초로 EU 전체에 적용 가능한 연합 사이버보안 위험 평가 방법의 개발

o **(주요 내용)** 국가수준과 EU수준에서 지켜야 할 권고사항은 아래와 같음

< EU 5G 네트워크의 사이버보안 강화 권고안>

구분	주요 내용
국가수준 (회원국)	• 회원국은 2019년 6월 30일까지 5G 네트워크의 사이버보안 위험 평가와 아래의 내용을 포함한 대책 수립을 완료해야 함 - 5G 네트워크의 보안성 강화를 위해 기존의 보안 요건을 검토 및 보완 - 5G 대역의 무선 주파수 사용권 부여 시[5] 공공 네트워크의 보안 보장 조건 포함 - 5G 네트워크의 보안을 보장하기 위해 공급업체에 강화된 의무를 부여할 것 • 국가 사이버보안 위험 평가 및 대책은 제3국의 위험을 포함하여 공급업체나 사업자의 행동과 관련된 기술적 위험과 같은 다양한 위험을 고려해야 함
EU수준	• 국가별 사이버보안 위험 평가결과는 2019년 7월 15일까지 ENISA에 보고해야 함 • 회원국들은 서로 정보를 교환해야 하며, 집행위원회와 ENISA의 지원을 받아 2019년 10월 1일까지 조정된 5G 네트워크의 사이버보안 위험 평가를 완료 - ENISA는 국가수준의 5G 네트워크의 사이버보안 위험 평가결과를 기초로 종합적인 사이버보안 위험 현황을 정리하고 평가 항목의 조정 및 보완 작업을 실시 - 사이버보안 인증 제도 구현을 위한 의무 사항과 공공 조달에서 적용될 수 있는 특정 보안 요건을 개발

o **(효과 평가)** 2020년 10월 1일까지 회원국은 위원회 및 ENISA와 협력하여 5G 네트워크 사이버보안 강화를 위한 추가적인 조치가 필요한지 여부를 결정하기 위해 이번 권고안의 효과를 평가해야 함

▶ 시사점

o 유럽은 5G 네트워크의 도입으로 인해 자동차, 건강, 운송과 에너지와 같은 핵심 산업 분야에서의 경제적 이익이 매년 약 1천억 유로에 달할 것으로 예상하고 있으며, EU 공동의 법제도 및 정책 추진을 통해 5G 네트워크와 관련된 글로벌 경쟁력 확보를 모색

5) 전자통신네트워크 및 서비스의 인가에 대한 지침(Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services, Authorisation Directive)에 따라 무선주파수 사용권이 부여됨. 동 지침 제3조(전자통신네트워크 및 서비스의 일반승인), 제5조(무선 주파수 및 번호에 대한 사용 권한),제6조(무선 주파수 및 번호 사용 권한의 일반 승인에 첨부 되는 조건, 구체적 의무) 참조.

o 본 권고안은 EU 최초의 5G 네트워크 사이버보안 강화 방안을 마련하였다는데 그 의의가 있으며, 향후 5G 네트워크의 사이버보안 위험평가 및 인증체계 구축에 대한 다양한 입법과 정책이 시도될 것으로 전망

※ **Reference**

http://europa.eu/rapid/press-release_IP-19-1832_en.htm
https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58154

해외 입법 동향 EU

유럽 집행위원회, 유럽의 디지털 미래 발전을 위한 공동 성명서 발표 (2019. 04. 09.)

유럽 집행위원회와 회원국 대표는 유럽 경제・사회의 가시적인 이익을 가져올 수 있는 핵심 분야를 선정하고, 《유럽의 디지털 미래 발전을 위한 공동 성명서》[1]를 발표 (2019. 04. 09.)

▶ 개요 및 경과

o 유럽 집행위원회와 회원국 대표는 2019년 디지털데이[2] 행사에서 디지털화를 가속화하기 위한 3개 핵심 분야로 ▲문화유산의 디지털화 ▲농업 및 농촌 지역의 디지털화 ▲ICT 관련 직무의 여성 참여 강화를 선정하고, 해당 분야의 공동 성명서를 발표

- 이번에 발표한 성명서에 따라 EU 및 회원국은 선정한 핵심 분야의 효과적인 추진을 위해 신속히 대응하고 긴밀하게 협력하기로 합의

o 디지털데이 행사는 2017년에 슈퍼컴퓨팅을 주제로 최초로 시작되었으며, 2018년에는 인공지능 분야에 대한 회원국 공동의 성명서를 발표한 바 있음

▶ 주요 내용

o **(문화유산의 디지털화)** 유럽의 풍부한 문화유산의 디지털화를 촉진하기 위해 아래 내용을 중심으로 행동을 실천하기로 선언

- 문화유산, 기념물 및 유적지의 3D 디지털화를 위한 유럽 공동의 전략 마련
- 디지털 문화유산 자원의 재사용, 시민의 참여와 혁신적인 활용을 촉진
- 디지털 문화유산 부문에서 국가 간 수평적인 공동의 협력으로 유럽 전체의 디지털 역량을 강화

o **(농업 및 농촌 지역의 디지털화)** 유럽의 농・식품 부문과 농촌 지역의 당면하고 있는 경제・사회, 기후・환경 문제를 해결 할 수 있는 디지털 기술의 잠재력을 활용

1) Joint statement on ensuring Europe´s digital future (Declaration on Digitising Cultural Heritage, Declaration on Digitisation for European Agriculture and rural areas, Declaration on Women in Digital)
2) EU Digital Day: 유럽 집행위원회와 이사회가 공동으로 주최하는 행사로, 디지털 첨단기술과 통신 분야에서 EU 각국의 이해관계자가 참석하여 기술개발과 인프라 투자를 장려하고 유럽의 미래 번영을 위한 협력을 강화하는 것을 목표로 함

- 스마트 팜[3] 기술과 식품이력추적제도[4] 등과 같은 ICT 기술을 활용하는 분야에 대한 연구 지원을 강화

- 모든 유럽의 이해관계자가 실제 환경에서 새로운 스마트 농업·농촌 솔루션을 검증하고 실험·테스트 할 수 있도록 ▲혁신 허브 구축 및 네트워크 연결 ▲최신 전문기술 사용을 위한 도구 및 프로그램 활용 교육 실시 ▲사물인터넷 기술 활용을 위한 농업·농촌 지역의 광대역 무선 네트워크 구축을 추진

- 유럽 공동의 정보공유 플랫폼을 도입하여 농업·농촌과 관련된 공간정보 및 환경·기후·기상 등의 고부가가치 데이터를 개발 및 공개하고, 무인항공기와 자율농업기계 운영을 위한 지원 프로그램[5]을 강화

- 최신 디지털 기술의 발달은 농업의 효율과 경제·환경적 지속가능성을 높일 수 있으므로, 농업·농촌지역의 디지털 전환을 촉진하고 가속화하기 위해 지속적으로 노력

- 디지털 기술의 사용 증대를 통해 농업·농촌지역의 삶의 질을 향상시키고, 젊은 세대의 창업을 유도하여 식량 안보와 일자리 창출에 기여하도록 함

o **(ICT 관련 직무의 여성 참여 강화)** ICT 관련 기술 직무 분야에서 여성들이 적극적이고 중요한 역할을 하도록 장려하기 위해 아래 내용을 중심으로 행동을 실천하기로 함

- 여성의 디지털 기술 부문 참여를 촉진하기 위해 교육과 자격, 근무환경, 기회균등화, 비차별화 등을 포함한 국가별 전략을 수립

- 디지털 분야의 위원회 및 관련 기관에 여성의 참여를 촉진하고, 기술과 과학을 다루는 방송 등에서 ICT 기술 분야의 여성에 대한 성공적인 역할 모델을 바탕으로 인식 개선

- 차별이 없는 기업의 업무문화를 장려하고, 적절한 조치를 위한 인센티브 및 협력 플랫폼 구축, 과학·기술·공학·수학 중심의 직업·진로·창업 교육 지원 등과 같은 조치 실시

3) Smart Farm: 정보통신기술(ICT), 바이오기술(BT), 녹색기술(GT) 등을 농업에 접목하여 지능화한 스마트 농업 기술이며, 농촌지역의 고령화와 인구 감소로 인해 노동력이 부족한 현실을 보완하기 위해 개발됨
4) Food traceability: 식품의 생산부터 소비까지 모든 단계의 식품이력정보를 소비자에게 제공하고 식품사고 발생 시 신속한 유통차단 및 회수·폐기할 수 있도록 한 관리제도 임. EU의 경우 EU 식품법에 따라 식품, 사료, 식품으로 가공된 동물, 가공식품 및 사료의 원료가 되거나 될 것이라고 예상되는 물질에 대하여, 생산·가공·유통의 모든 단계를 추적하고 역으로 조사할 수 있는 능력으로 규정
5) 위성항법을 위한 유럽 우주 프로그램(EU 지역에서 미국의 GPS 정확도와 무결성을 향상시키는 유럽 정지 항법 오버레이 시스템)과 지구 관측 프로그램(EU의 대기 및 해양환경, 토지, 재난 관리 등을 위해 광범위한 지구관측정보를 제공하는 프로그램) 등이 해당

▶ 시사점

o 이번 성명서에 핵심 분야로 선정된 사항은 유럽의 디지털 단일 시장 전략의 일환으로 해당 분야에 대한 디지털화가 촉진되고, 회원국 간의 협력을 통해 공동의 디지털 단일 시장이 단계적으로 실현될 것으로 기대

o 향후 EU 및 회원국에서 문화유산의 디지털화, 농업·농촌지역의 스마트 기술 활용, ICT 관련 직무의 여성 참여 강화와 관련된 입법 및 정책이 추진될 것으로 전망

※ **Reference**

http://europa.eu/rapid/press-release_STATEMENT-19-2070_en.htm
http://europa.eu/rapid/press-release_IP-19-2015_en.htm

해외 입법 동향 EU

유럽네트워크정보보호원(ENISA), 사이버보안 문화에 대한 행동 가이드라인 발표 (2019. 04. 16.)

유럽네트워크정보보호원(ENISA)[1]은 사이버보안 문화[2]의 정착을 위해 정책입안자, 경영·관리자, 보안전문가, 보안담당 직원 등의 적절한 행동을 권장하는 《사이버 보안 문화 가이드라인》[3]을 발표 (2019. 04. 16.)

▶ 개요 및 경과

o 유럽네트워크정보보호원은 정부, 공공기관, 민간기업 등의 조직단위에서 사이버보안 문화가 정착될 수 있도록 보안의식을 높이고 적절한 행동을 권장하는 가이드라인을 발표

- 사이버보안에 대한 태도와 인식을 유지하기 위한 5단계의 순환적인 절차를 제시
- 정책입안자, 경영·관리자, 보안전문가, 보안사고 대응팀 및 보안운영센터 직원 등 역할에 따라 권장하는 행동요소를 포함

o 본 가이드라인은 영국 국가사이버보안센터(UK National Cyber Security Centre)의 지원을 받아 사이버보안과 관련된 심리학과 사회학, 인간학, 인류학, 인간생물학, 행동경제학 등의 688개 출판물을 분석한 결과를 기초로 작성한 것임

▶ 주요 내용

o **(공통 프레임워크 및 정의)** 사이버보안에 대한 태도와 인식을 유지하지 위한 절차는 아래의 5단계로 구분되며, 단계별 정의를 규정

- 1단계 인식 : 현재의 사이버보안 상태를 인식
- 2단계 분석 : 확인된 약점과 문제의 근본 원인을 분석
- 3단계 계획 : 인식과 분석단계에서 파악된 내용을 중심으로 계획을 수립
- 4단계 실행 : 계획에 따라 행동을 변화시키는 것
- 5단계 평가 및 반복 : 행동의 변화가 목표를 달성하였는지 평가하고, 평가결과는 다음의 재순환 과정에서 활용될 수 있도록 함

1) The European Union Agency for Network and Information Security: EU 전역의 네트워크 및 정보보안을 개선하기 위해 2003년 설립된 기관으로 회원국의 사이버보안 관련 전문성 강화를 위한 조정 및 지원역할을 수행함. 또한 다양한 분야의 사이버보안 전문가와 협력하여 관련된 표준과 권고사항을 개발·제공하고, EU 회원국들이 사이버보안과 관련된 법안을 실행하는 것을 지원하고 있음.
2) 사이버보안 문화는 보안의식과 행동이 조직원들의 일상적인 작업에 체화되어 있을 뿐만 아니라 관리자들의 정책적 우선순위에도 최고 위치를 점하도록 하는 문화를 의미
3) Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity

o **(주체별 권고사항)** 사이버보안과 관련된 업무를 수행하는 역할에 따라 정책입안자, 경영・관리자, 보안전문가, 보안사고 대응팀 및 보안운영센터 직원, SW개발자, 교육자, 인식 개선 관리자로 구분하고 아래와 같은 실천사항을 권고

< 사이버보안 문화 정착을 위한 관련 업무수행 주체별 행동 권고사항 >

구분	주요 행동 권고사항
정책입안자	• 정보보호 관리 책임을 이행할 능력이 있는 자에게 책임을 부여 • 사이버 보안을 위한 조직 전반의 협업 강화 및 조직원 간의 신뢰 구축을 위해 노력 • 기술・사회・행동과 관련된 전문가 간의 협력을 장려하고 지원 • 사이버위협에 대한 인식 증진과 함께 모든 조직구성원들이 사이버 위협에 대응할 수 있는 기술을 확보하도록 지원
경영・관리자	• 관리할 보안 위험을 결정하고 필요한 자원에 투자 • 조직 구성원이 사이버보안에 투입해야 하는 시간을 보장해야 함 • 보안 정책을 준수하고 보안전문가 및 직원들과 협력하여 전문 분야(운영, 재무, 마케팅 등)에 유용한 솔루션을 찾도록 시간을 투자
보안전문가 (정보보호최고책임자 포함)	• 사이버보안 대책을 마련하기 전에 규정 준수에 필요한 시간과 노력을 파악 • 조직구성이 보안전문가와 쉽게 접근 할 수 있도록 하고 의견을 경청 • 타인에 대한 존중을 바탕으로 비전문가에 대한 고정관념에서 탈피하고, 누구나 이해하기 쉬운 용어를 사용
보안사고 대응팀 및 보안운영센터 직원	• 사이버보안 사고 발생 시 유연하게 대응할 수 있도록 팀 구성 및 배치를 실시하고, 충분한 인력을 확보 • 교육훈련과 개인의 능력 향상에 중점적으로 투자하며, 실질적인 사례 분석과 사이버공격 대응 실습훈련 등 효과적인 기술 능력 확보에 노력 • 팀워크 구축에 주력하여 사이버위협 대응능력을 향상
SW개발자	• SW개발 전체 단계에 걸쳐 요구되는 보안사항을 고려 • 보안전문가와 지속적인 협력을 통해 보안과 관련된 내용을 설계하고 테스트를 실시
SW개발 관리자 및 교육자	• 개발자에게 헬프 데스크 및 지원업무를 경험하도록 할당 • 사이버보안 과정을 컴퓨터공학과 공학과목에서 필수과목으로 지정
사이버보안 인식 개선 관련 관리자	• 사이버위협의 규모와 취약성에 대한 인식에 시간과 에너지를 소비하기 보다는 사이버위협에 대처할 수 있는 기술 제공을 목표로 행동 • 간단한 행동(예: 신속한 업데이트 등)이 효과적인 보호가 될 수 있다는 인식을 확산시킴

▶ 시사점

o 최근 전 세계적으로 사이버보안과 인간행동에 대한 다양한 연구가 진행되고 있으며, 이번 가이드라인은 심리학 및 사회학 등 인문사회학적인 그 동안의 관련 연구결과를 종합하여 유럽 전역의 사이버보안 인식 개선 방향을 제시하였다는데 의의가 있음

o 향후 사이버보안 문화의 정착을 위해 인간의 행동요소를 과학적으로 분석하고, 그 결과를 바탕으로 업무수행 주체별 역할과 책임을 정확히 이해하도록 유도하는 제도와 정책이 추진될 것으로 예상

※ **Reference**

https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity/at_download/fullReport

https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity

https://www.enisa.europa.eu/news/enisa-news/behavioural-aspects-of-cybersecurity

미국 상원, 안전한 5G 보안 전략 수립을 위한 법안 발의 (2019. 03. 27.)

미국 상원은 미래의 통신시스템 기술의 우위 확보를 위해 정부기관 간 협력을 통한 사이버 보안 전략을 수립하도록 요구하는《Secure 5G and Beyond Act》를 발의 (2019. 03. 27.)

▶ 개요 및 경과

o 미국 상원은 5G 기술의 상용화가 시작됨에 따라 관련 통신 시스템과 인프라의 보안을 보장하고 기술우위를 확보하기 위해 5G 네트워크의 국가 사이버보안 전략 수립을 요구하는《Secure 5G and Beyond Act (S.893)》를 발의

- 대통령이 5G 기술 및 정책과 관련된 정부부처와 협력하여 5G 보안 전략을 개발하고 의회에 제출하도록 규정
- 5G 통신 기술의 경쟁력, 프라이버시 보호 및 표준 설정, 전략에 필수적으로 포함되어야 할 내용을 제시

o 지난 2017년 상원과 하원에서 5G 네트워크 및 차세대 유무선 기술을 미국 전역에 배치하여 경제발전과 디지털 혁신을 촉진하는 결의안[1]이 소개된 바 있음

▶ 주요 내용

o **(전략 수립의 목표 및 절차)** 동 법의 제정일로부터 180일 이내에 대통령은 연방통신위원회, 국가통신정보국, 국토안보부, 국가정보국, 법무부와 협의하여 아래의 내용을 목표로 5G 보안전략을 수립하고 의회에 제출해야 함

- 국내의 5G 및 미래 세대의 이동 통신 시스템과 인프라의 보안성 보장
- 자국의 안보 이익을 목적으로 동맹국과 전략적 파트너에 5G 및 미래 세대의 이동 통신 시스템 및 기반 구조 개선을 지원
- 기업의 경쟁력을 확보하고, 소비자의 프라이버시를 보호

1) A resolution expressing the sense of the Senate about a strategy to deploy fifth generation mobile networks (5G networks) and next-generation wireless and wired technologies to promote economic development and digital innovation throughout the United States (S.Res.242).
Expressing the sense of the House of Representatives about a strategy to deploy fifth generation mobile networks (5G networks) and next-generation wireless and wired technologies to promote economic development and digital innovation throughout the United States (H.Res.521).

o **(전략에 포함될 내용)** 5G 보안 전략은 범정부 차원의 접근방식을 제시하고, 다음의 내용을 포함하여야 함

< 5G 보안 전략에 포함되어야 할 내용 >

구분	주요 내용
대내적	• 5G 이동 통신 시스템 및 기반 구조 구축과 관련된 국가의 경제안보[2] 이익에 대한 설명 • 5G 이동 통신 시스템과 인프라를 지원하는 기반시설, 장비, 시스템, SW 및 네트워크에 대한 잠재적인 보안 위협·취약성의 식별 및 평가 • 관련 주요 기술의 연구개발 및 전문 인력 양성을 포함하여 국내 산업기반의 보안 격차를 좁히는데 도움이 되는 인센티브 및 정책 발굴 • 관련 표준의 정보 공유를 위한 민간 부문 통신 시스템 및 인프라 장비 개발업체와의 협약
대외적	• 동맹국과 전략적 파트너인 국가의 5G 이동통신 장비 및 인프라 지원 등 - 생산·공급업체의 능력을 평가하고, 신뢰할 수 있는 공급업체를 식별 - 보안 수준의 격차를 파악하고, 사이버보안 위험의 완화를 위한 정보를 공유 - 정보 공유를 위한 표준 설정 기관과의 교류 전략 및 플랫폼 구축 - 보안 결함 또는 취약성이 발견된 장비의 위험 식별 및 완화를 지원 - 관련 시장 확보를 위한 공동시험 환경 구성 및 추진 - 보안 취약점 완화를 위한 연구개발 전략
입법 및 행정조치 등	• 전략을 수행하는데 필요한 입법 또는 행정조치에 대한 설명 • 연방통신위원회, 국가통신정보국, 국토안보부, 법무부, 국방부 등 관계 기관의 적절한 역할 및 임무에 대한 설명 • 구체적인 예산요청을 포함하여 전략 수행에 필요한 주요 정보 및 경제자원 등의 파악

▶ 시사점

o 이번에 발의한 법안은 5G 보안과 관련된 미국의 국가 전략을 개발하고, 전략 수립에 포함되어야 할 주요 내용을 구체적으로 제안하는 등 5G 시대에 신속한 대응을 촉구한다는 특징이 있음

o 미국은 5G 기술의 상용화로 인해 네트워크의 복잡성, 밀도와 속도가 기하급수적으로 늘어날 것으로 예상하고 있으며, 이에 따라 우려되는 사이버위협에 대한 범정부적 대응력 확보와 5G 기술의 안전한 활용을 유도하는 방향으로 전략이 마련될 것으로 기대

※ **Reference**

https://www.congress.gov/bill/116th-congress/senate-bill/893/text
https://scipol.org/track/s-893-secure-5g-and-beyond-act-2019
http://www.etcentric.org/senators-introduce-5g-security-bill-for-next-gen-networks/

2) 경제안보(economic security): 미국 정부가 2017년 12월에 발표한 국가안보전략(National Security Strategy)에서 등장한 개념으로 자국의 경제적 번영과 성장이 곧 국가안보(national security)와 직결된다는 의미

호주 사이버보안센터(ACSC), 네트워크 및 데이터 서비스의 보안 권고안 발표 (2019. 04. 18.)

호주 사이버보안센터(ACSC)[1]는 날로 지능화되는 사이버공격에 호주 내 기업과 조직의 대응방안을 내용으로 한 《네트워크 및 데이터 서비스 보안 권고안》[2]을 발표 (2019. 04. 18.)

▶ 개요 및 경과

o 호주 사이버보안센터(ACSC)는 호주 IP 주소 범위에서 호스팅되는 보안이 취약한 네트워크 및 데이터베이스 등의 적절한 접근 제어 및 정보보호 방법을 권고하는 《네트워크 및 데이터 서비스 보안 권고안》을 발표

- 모든 호주 내의 기업과 단체는 권고안에서 제시한 사항에 따라 네트워크 인프라 및 데이터베이스가 적절한[3] 사용자 인증 및 접근 제어를 구현했는지 확인해야 함
- 데이터 유출 사고가 발생한 경우 ACSC에 보고해야 하며, 이 중 보안이 취약한 네트워크 및 서비스로 인해 사고가 발생한 경우 호주 정보위원회(OAIC)[4]에 보고해야 함

o ACSC는 2017년에 AISI(Australian Internet Security Initiative) 프로그램의 기초 연구 보고서를 최초로 발간하였고, 이번에 발표한 권고안은 2017년 이후 더욱 지능화되고 있는 사이버공격 현황과 취약성을 분석한 결과를 토대로 네트워크 및 데이터베이스의 보안관리 사항을 규정한 것임

▶ 주요 내용

o **(보안 취약성 검토 결과)** 2019년 1분기에 AISI 프로그램을 통해 보고된 웹 서비스 분석 결과를 토대로 네트워크 및 데이터베이스의 보안 취약점이 다수 발견됨

- 랜섬웨어, APT 공격, 서비스 거부 공격 등을 통해 호주 전역에서 매일 약 600개의 데이터베이스의 노출이 탐지되었으며, 잠재적으로 취약한 오픈 네트워크 서비스는 약 20,000개로 파악됨

1) Australian Cyber Security Centre: 2014년에 설립된 호주 신호국(ACS) 산하의 기관으로 사이버보안 위협과 사고에 대응하고, 사이버위협 정보 공유를 위해 공공과 민간의 협력을 지원하며, 사이버보안 인식 개선 및 모든 국민에게 사이버보안과 관련된 정보・조언을 제공함.
2) Securing Unprotected Network and Data Services(Advisory 2019-009)
3) strong authentication(개체 인증을 위해 개인 생체 정보, 공개 키 인증서 등 2개 이상의 인증 요소(factor)를 사용하는 인증)과 같은 방법을 의미함.
4) Office of the Australian Information Commissioner: 호주 법무부 소속의 독립기관으로, 개인정보보호 및 정보의 자유와 관련된 조사・검토・정책자문 등의 업무를 담당

o **(권고사항)** 모든 호주 내의 기업과 단체는 기획, 개발, 테스트, 배포 등의 모든 작업에서 네트워크 인프라 및 데이터베이스에 대하여 아래의 권고사항에 따라 강력한 사용자 인증 및 접근 제어를 구현했는지 확인해야 함

< 네트워크 및 데이터 서비스의 보안성 강화를 위한 권고안 >

번호	권고사항
1	• 필요 없는 서비스 인터페이스가 인터넷에 노출되지 않도록 함
2	• 원격 액세스가 필요하지 않는 경우 서비스 인터페이스가 로컬 호스트에서만 수신되는지 확인
3	• 서비스 관리 인터페이스가 인터넷에 노출되지 않도록 보장
4	• 필요한 경우 가상 사설 통신망(Virtual Private Network, VPN) 연결을 사용
5	• IP 허용 목록, 사용자 계정 및 역할 기반 접근 제어[5]를 포함한 적절한 접근 제어 구현
6	• 권한이 가장 적은 사용자 계정을 사용
7	• 침입 탐지 시스템(Intrusion Detection System, IDS)[6] 사용
8	• 사용자 및 서비스 계정 모두에 대한 강력한 암호 정책
9	• 가능한 경우 다중 요인 인증[7]을 사용
10	• 네트워크 분할 및 분리 구현
11	• 접속기록로그의 정기적인 모니터링
12	• 정부 정보 보안 매뉴얼(Australian Government Information Security Manual, ISM)[8] 준수 및 전송 계층 보안(Transport Layer Security, TLS)[9] 사용
13	• 제품 공급업체의 보안 지침을 검토
14	• 권고사항에 대한 조치 지원 및 데이터 유출 사고는 ACSC에 보고
15	• 보호되지 않은 서비스에서 데이터 침해 사고가 발생한 경우 호주정보위원회(OAIC)에 보고 - 보고여부는 호주 NDB(Notifiable Data Breakes Scheme)[10] 참고하여 판단

5) Role-Based Access Control: 사용자의 조직에서의 역할을 기반으로 접근 권한을 특정 사용자가 아닌 해당 역할을 가진 사용자 그룹에게 부여하는 방식
6) 데이터 유출 방지(Data Loss Prevention, DLP) 및 침입 방지 시스템(Intrusion Prevention System, IPS)과 같은 침입 탐지 도구를 이용하여 네트워크 모니터링 및 침입을 탐지하고, 잠재적인 악성 트래픽 등을 자동으로 막을 수 있도록 함
7) Multi-Factor Authentication: 최소 두 가지 이상의 인증 요소를 이용하여 본인 여부를 인증하는 것
8) 조직이 위험 관리 프레임 워크를 사용하여 정보 시스템을 사이버 위협으로부터 호호 할 수 있도록 도와주는 것을 목적으로 ACSC에서 발간한 호주 정부의 공식 사이버보안 매뉴얼, https://www.cyber.gov.au/ism 참조.
9) 인터넷상에서 데이터의 도청이나 변조를 막기 위해 사용되는 보안 소켓 계층(SSL: Security Sockets Layer) 프로토콜 보다 보안성이 강화된 프로토콜.
10) https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme

▶ 시사점

o 호주 정부는 2017년에 시작한 AISI 프로그램에 따라 지능화되고 있는 사이버위협 현황을 체계적으로 모니터링하고 보안 취약점을 분석하고 있으며, 이번에 발견된 사항은 호주 전역의 신속하고 방대한 조치를 요구하고 있음

o 최근 사물인터넷 기기가 확대되고, 5G 서비스가 상용화됨에 따라 광범위한 지역에서 새로운 보안 취약점이 나타날 것으로 예상되며, ACSC의 역할에 대한 중요도가 더욱 높아질 것으로 전망

※ **Reference**

https://www.cyber.gov.au/sites/default/files/2019-04/2019-009%20Securing%20Unprotected%20Network%20and%20Data%20Services.pdf
https://www.cyber.gov.au/publications/Advisory-2019-009

해외 입법 동향 일본

일본 정보처리추진기구(IPA), 중소기업의 정보보안대책 가이드라인 개정 (2019. 04. 09.)

일본 정보처리추진기구(IPA)[1]는 최근의 ICT 환경과 정책 방향에 맞추어 중소기업에 올바른 정보보안 관리 등을 지원하도록 《중소기업의 정보보안대책 가이드라인》[2]을 개정 (2019. 04. 09.)

▶ 개요 및 경과

o 일본 정보처리추진기구(IPA)는 최근 급변하고 있는 ICT 환경의 변화와 정책 추진 방향에 따라 중소기업의 바람직한 정보보안 관리와 실천을 지원하기 위해 《중소기업의 정보보안대책 가이드라인》을 개정

- 이번에 발간된 개정판은 2017년 11월에 개정된 《사이버보안 관리 지침》[3]과 최근 활용이 급증하고 있는 클라우드 서비스에 대한 내용을 반영한 것임
- 보안대책의 실천을 위한 단계별 절차는 웹사이트 및 클라우드 서비스의 정보보안 사항을 고려하여 개선

o 본 가이드라인은 2009년에 최초로 발간되었으며, 2016년에 제2판이 개정된 바 있음

▶ 주요 내용

o **(구성)** 본 가이드라인은 경영자를 위한 정보보안 지침과 기업 내부의 보안대책 실행 절차를 수록하고 있으며, 본문과 관련된 7개의 부록으로 구성

- 경영자가 정보보안 측면에서 인식하고 실행해야 하는 방침을 제시
- 기업 내부의 보안대책 실천을 위한 4단계의 절차와 단계별 내용을 수록
- 부록은 ▲정보보안 5개조 ▲정보보안 기본 방침 ▲정보보안 자체 진단 ▲정보보안 핸드북 ▲정보보안 관련 규정 ▲클라우드 서비스 안전 사용 가이드 ▲위험 분석 시트가 별도로 분리되어 있음

---

1) Information-technology Promotion Agency(独立行政法人情報処理推進機構). 일본 IT 전략을 기술 및 인재 면에서 지원하기 위해 경제산업성 소관 하에 2004년 설립한 조직

2) 「中小企業の情報セキュリティ対策ガイドライン」: 중소기업의 경영자 및 실무담당자가 정보보안 대책의 필요성을 이해하고 정보를 안전하게 관리하도록 적절한 절차와 방법을 권고하는 지침서

3) 「サイバーセキュリティ経営ガイドライン」 Ver 2.0, 2017, 経済産業省, 独立行政法人 情報処理推進機構: 대기업 및 중소기업의 경영자를 대상으로 사이버위협으로부터 기업을 지키는 관점에서 정보보호최고책임자에게 지시해야 할 주요 항목을 규정한 것임.

o **(경영자를 위한 지침)** 경영자가 인식해야 할 3대 원칙과 실행해야 할 7개 항목을 아래와 같이 제시함

< 경영자를 위한 정보보안 지침 >

구분	주요 내용
경영자가 인식해야 할 정보보안 원칙	• 경영자가 리더십을 발휘하여 정보보안 대책 실행을 주도 • 위탁업체가 실시하는 정보보안 대책을 확인하고, 불충분한 경우 대처 • 정보보안 대응 방침을 관계자에 전달하고, 의사소통이 원활하도록 유지
경영자가 실행해야 할 주요 권고 사항	• 정보보안에 대한 조직전체의 대응 방침을 정함 • 정보보안 대책을 위한 예산과 인재를 확보 • 필요한 정보보안 대책을 검토 및 수립하고 실행을 지시 • 정보보안 대책에 대한 적절한 재검토를 지시 • 긴급 시 대응이나 복구를 위한 체계를 정비 • 위탁이나 외부 서비스를 이용할 때는 보안 책임을 명확하게 함 • 정보보안에 대한 최신 동향을 수집

o **(기업내부의 보안대책 실행 절차)** 기업 내부의 보안대책 실천을 위한 4단계의 절차와 단계별 주요 내용은 다음과 같음

< 기업 내부의 보안대책 실천을 위한 절차 및 주요내용 >

절차	주요 내용	참조부록
1단계 (할 수 있는 것부터 시작)	• SW의 최신버전 유지, 바이러스 대책 SW 도입 • 비밀번호 강화, 공유설정 재검토 • 다양한 사이버위협 기법을 이해하고 대처	정보보안 5개조
2단계 (조직적인 대처)	• 경영자는 정보보안 기본 방침을 작성하고, 모든 관계자에게 그 내용을 이해하도록 전달 • 정보보안 자체진단을 통해 조직의 보안대책의 실시 상황을 파악	정보보안 기본방침, 정보보안 자체진단 정보보안 핸드북
3단계 (본격적 실행)	• 조직에 적합한 정보보안 규정을 작성하고 공유 • IT 자원 현황 파악 및 정보보안에 필요한 예산 확보 • 보안 위험도가 높은 사항에 우선하여 대책을 실시 • 위탁에 관한 보안대책 및 감독 실시, 점검과 개선	정보보안 관련규정
4단계 (견고한 보안 방안)	• 정보보안을 더욱 공고히 하기 위해 사이버위협 정보수집과 공유, 웹사이트 및 클라우드 서비스의 정보보안, 상세 위험 분석을 실시	클라우드 서비스 안전 사용 가이드, 위험 분석 시트

▶ 시사점

o 일본은 최근 중소기업의 업무에서 웹기반 및 클라우드 서비스 등 ICT 활용이 일상화됨에 따라 고도화되는 사이버위협에 신속히 대응할 수 있도록 관련 지침을 개정하는 등 구체적인 대응책을 내놓고 있음

o 이와 같은 제도 개선과 정책의 추진을 통해 정부 및 공공기관, 대기업 등에 비해 상대적으로 사이버공격에 취약한 중소기업의 사이버보안 대응 능력이 향상될 것으로 기대

※ **Reference**

https://www.ipa.go.jp/security/keihatsu/sme/guideline/
https://www.ipa.go.jp/about/press/20190319.html

해외 입법 동향 독일

독일 연방정보보안국(BSI), 공예산업을 위한 IT 정보보호 기준 발표 (2019. 03. 28.)

독일 연방정보보안국(BSI)은 공예산업의 디지털화로 인해 증가하는 사이버보안 위험에 대응하고자 세계 최초로 《공예산업을 위한 IT 정보보호 기준》[1]을 발표 (2019. 03. 28.)

▶ 개요 및 경과

o 독일 연방정보보안국(BSI)은 독일공예중앙협회(ZDH)[2] 및 디지털공예역량센터(KDH)[3]와 협력하여 수십년 동안 독일의 경제발전에 주요 원동력이 된 공예산업의 디지털화로 인한 사이버보안 위험에 대응하기 위해 《공예산업을 위한 IT 정보보호 기준》을 개발

- 공예산업 전문기업에게 기본적인 IT 정보보호 구성요소와 실천기준을 안내
- 공예와 관련된 기업을 위한 IT 비즈니스 프로세스의 정보보안 기준과 사이버보안 안내서[4]로 구성됨

o 본 기준은 2017년에 연방정보보안국(BSI)과 독일공예중앙협회(ZDH)가 체결한 사이버보안연합계획의 일환으로 추진되었고, 공예산업 전문가의 참여를 통해 개발한 것임

▶ 주요 내용

o **(목적)** 본 기준은 공예산업과 관련된 모든 기업의 IT 보안 수준을 높이기 위한 검증된 방법으로, 기업이 IT 보안 문제에 대한 목표를 설정하고 실행할 수 있는 기준을 제공하는 데 그 목적이 있음

o **(정보보호 대상)** IT 시스템과 네트워크 통신, SW 프로그램과 같은 모든 IT 관련 기기와 관련된 인프라를 대상으로 적절한 정보보호 조치를 취하여 함

- IT시스템 : PC, 서버, 노트북, 스마트 폰, 복합기(프린터, 스캐너, 팩스), 제품 생산 기기 및 SW 프로그램, 사물인터넷(측정기, 계량기) 등
- 네트워크 통신 : 인터넷, 라우터, IP 전화 시스템, 클라우드 서비스 등
- 인프라 : 사무실, 작업실, 창고, 재택 근무지 등

1) IT-Grundschutz-Profil für Handwerksbetriebe
2) Zentralverband des Deutschen Handwerks
3) Kompetenzzentrum Digitales Handwerk
4) ROUTENPLANER : Cyber-Sicherheit für Handwerksbetriebe

- 위에 기술한 정보보호 대상 외에 기업의 특성에 따라 보호해야 할 대상이 있는 경우 정보보호 대상 목록에 추가해야 함

o **(유형별 정보보호 기준)** 사이버보안 강화를 위해 공예산업과 관련된 업무수행 시 적용할 수 있는 정보보호 조치사항을 유형별로 구분하여 안내

< 공예산업의 사이버보안 강화를 위한 정보보호 기준 >

구분	주요 내용
공통 적용 사항	• 정보보호의 책임 인식, 정보보호 담당자 지정 및 관련 조직 구축 • 정보보호와 관련된 내용의 문서화 • 사이버보안 관련 보험 등을 통해 사고 및 재해 발생을 대비
조직 및 직원	• 조직특성에 따른 정보보호 규정을 작성하고, 전 직원이 숙지하도록 함 • 정보보호 책임을 명확히 할당하고, 적절한 접근 권한을 부여 • 신입사원에 대한 교육훈련, 외부 인력 사용 시 비밀 유지 계약 실행
개념과 접근	• 정기적인 데이터 백업, 인증된 소프트웨어의 설치 및 사용
운영	• 비상 대책 수립 및 역할 명시, 제조업체가 제공하는 보안 패치 실시 • 바이러스 백신 프로그램 설치 및 최신 상태 유지 • 재택근무자에 대한 보안의식 향상 교육 실시, 원격 접근의 철저한 관리
감지와 반응	• 사이버보안 위협을 지속적으로 탐지, 사고대응을 위한 비상연락망 준비
응용 프로그램	• 오피스 제품, 웹 브라우저, 모바일 앱, 그룹웨어의 보안관리 철저
정보시스템	• 일반 작업 PC의 로그인 및 화면 잠금 설정 • 노트북 도난 방지 장치 사용, 스마트 폰의 계정과 GPS 보호 조치 실행 • 복합기는 안전한 위치에 설치하고, 접근 권한을 관리 • 사물인터넷 장치는 필수적으로 암호를 변경 및 관리
산업 IT	• 산업제어시스템의 물리적 보호 수단 강구, 산업용 센서가 적절한 기상조건을 충족하도록 유지하고, 먼지 및 진동에 노출되지 않도록 조치 • 기계의 안전한 원격 접속을 유지, 보증 기간 후 예방 정비 상시 수행
네트워크와 통신	• 안전하지 않은 환경에서 핫스팟 등 무선 인터넷 사용을 피하도록 함 • 네트워크 세분화 및 DMZ 구성 • 중요정보는 별도의 보안구역에 보관하며, 보안구역의 전원은 따로 분리
인프라	• 허가받지 않은 사람의 출입금지, 연기감지기 설치 등 화재 안전 규정 준수 • 전문가에 의해 안전하게 케이블이 설치 및 유지・관리 되어야 함

▶ 시사점

o 독일은 100만개 이상의 공예 관련 사업체가 운영 중에 있으며, 최근 스마트 팩토리, 클라우드 서비스, 사물인터넷 등의 기술 활용이 확대됨에 따라 소규모 기업이 대다수인 공예산업에서 사이버보안 위험이 더욱 증가할 것으로 전망

o 이번에 발표한 IT 정보보호 기준과 사이버보안 안내서를 통해 공예산업과 관련된 기업 및 단체 등의 정보보호 수준이 향상될 것으로 기대

※ **Reference**

https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2019/GS-Profil-Handwerk_280319.html
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Profil_Handwerksbetriebe.pdf?__blob=publicationFile&v=5
https://www.bsi.bund.de/SharedDocs/Downloads/ACS/routenplaner_print.pdf?__blob=publicationFile&v=6

기고

프랑스의 IT 법제 동향 및 시사점

오승규 한국지방세연구원 연구위원
- (現) 한국공법학회 국제이사, 유럽헌법학회 총무이사
- (前) 중원대학교 법무법학과 교수
- (前) 대법원 재판연구관
- (前) 법무부 법무자문위원회 전문위원

Ⅰ. 시작하며

변화무쌍한 21세기 소위 4차 산업혁명시대의 파고를 헤쳐 나가기 위해 프랑스는 지속적으로 노력중이다. 1978년부터 개인정보보호법을 제정하고 CNIL[1]이라는 강력한 개인정보보호기구를 두어 정보법 위주의 운영을 해온 프랑스는 그간 영역별 칸막이 식으로 운영되었던 관련법들을 연결하여 미래 먹거리 창출을 위한 국가역량 강화 지원 목적의 법제 개혁을 전개하고 있다. 큰 줄기는 유럽연합의 일반정보보호규정(GDPR)의 시행에 따른 국내 정보보호법 개혁이고, 그 가지로는 정보를 활용한 산업의 육성, 정보조작의 규제, 디지털세 도입 등을 들 수 있다.

Ⅱ. GDPR에 따른 개인정보보호법의 개정

2016년 5월 유럽연합(EU)은 일반정보보호규정(General Data Protection Regulation, 약칭 'GDPR')을 제정하였고, 2018년 5월부터 본격적으로 시행하였다. EU 회원국들은 이에 맞춰 국내법을 개정하면서 그 구체적인 적용을 위한 가이드라인을 정비하는 등 다양한 준비를 해왔다. 이미 강력한 개인정보보호 규범과 감독기구를 가지고 있는 프랑스는 개인정보주체의 권리와 감독기구의 권한을 더 강화하면서도 신기술 관련 정보의 수집과 이용 가능성을 법에 담아내는 노력을 기울였다.

2018년 6월 21일에 「개인정보보호에 관한 법률 제2018-493호(LOI n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles)」가 공포되었다. 주로 기존의

1) Commission Nationale de l'Informatique et des Libertés, https://www.cnil.fr/ 참조

개인정보호법(Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés)을 개정하면서 여타 관련법들을 개정하는 내용의 이 법률은 GDPR의 국내법적 적용을 구체화하기 위한 목적으로 제정되었다.[2)]

GDPR은 바로 회원국에 적용되는 직접적 효력을 가지고 있으나 각 회원국의 사정을 고려하여 어느 정도 융통성을 가질 필요가 있다. 이번의 입법으로 프랑스는 개인의 권리와 감독기구인 CNIL의 위상을 강화하면서 한편으로 국가기관과 국제기구의 협력체계를 국내법상으로도 구축하였다. 개인정보보호 관련 규정은 유럽연합규정을 직접 적용하게 되었지만, 형사법 관련 정보, 국가안보 관련 정보들은 여전히 프랑스의 개인정보보호법의 적용 영역으로 남겨두었다. 이 법률을 더 구체화시킬 목적으로 법률대위명령인 오르도낭스(ordonnance)가 법률 시행 후 공포[3)]되어 법률을 구체화시켰다.

Ⅲ. 데이터 개방을 통한 신산업의 육성

프랑스는 개인정보보호제도의 토대 위에서 IT 기반 서비스, Big Data 등 새로운 문제에 대처하기 위하여 끊임없이 노력하고 있다. 특히 디지털 사회에 적응하기 위한 법제구축의 일환으로 「디지털 공화국을 위한 법률 제2016-1321호(Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique), 약칭 '디지털공화국법'」를 제정하였다.

프랑스는 2016년 2년여의 논의 끝에 디지털공화국법을 제정했다. 이 법은 4차 산업혁명 시대를 대비해 프랑스 사회 전체의 변화를 염두에 두고 '데이터'에 대한 입장을 정리한 것이다. 디지털공화국법을 기반으로 공공 데이터의 자유로운 활용, 모든 국민의 인터넷 접근권 보장, 정부 투자 프로젝트의 지식재산권 1년 이후 일반 공개, 사후(死後) 디지털 세상에서 '사라질' 권리인 디지털장례권 등 개인정보 보호 강화 조항들이 명문화됐다.

디지털공화국법의 핵심 내용은 '데이터 개방'이라고 할 수 있다. 데이터의 적극적인 개방과 이를 경제적 목적으로 활용할 수 있도록 해 프랑스를 '디지털공화국'으로 만들겠다는 취지로 제정된 법이라 할 수 있다. 개방된 데이터의 범위가 넓을수록 더욱 의미 있는 빅데이터가 형성되고 이를 인공지능을 동원하여 분석할 수 있게 되어, 관련 기업들은 물론 일반 개인들 특히 (학술) 전문가들에게 새로운 분석과 연구의 기회를 제공할 수 있게 된다. 프랑스 정부는 법 제정 초기부터 정부 및 공공기관이 생성하는 데이터는

2) https://www.inc-conso.fr/sites/default/files/pdf/Tableau-loi-Informatique-libertes-1978.pdf
3) Ordonnance n° 2018-1125 du 12 décembre 2018 prise en application de l'article 32 de la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et portant modification de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel.

예외 없이 공개하는 것을 원칙으로 삼았다. 더 나아가 정부 및 공공기관 등이 의뢰하거나 이들과 관련된 사업을 통해 민간 기업들이 생성하게 되는 데이터까지 공개하는 것을 목표로 삼았다.

민간기업 가운데에는 금융기관, 의료기관 등이 포함돼 있어 개인의 신상정보가 외부에 노출될 수 있다는 문제가 있다. 때문에 디지털공화국법은 개인정보 개방으로 인해 일어날 수 있는 권리침해 문제를 꼼꼼히 검토해 이를 방지할 수 있는 대책까지 담았다. 데이터를 한데 모아 이른바 '공익 데이터 (des données d'intérêt général)'라는 개념을 도입한 것이다.

결국 프랑스는 디지털 전환의 핵심 내용을 데이터의 적극적인 개방과 이를 경제적 (혹은 사회적) 목적으로 활용할 수 있게 하는 데 있다고 생각하고, 이를 통해 프랑스를 이른바 '디지털 공화국'으로 만들겠다는 야심찬 취지를 가지고 이 법을 제정하려 했던 것이다. 여기서 흥미로운 점은 이 법의 이름으로 '디지털 사회'보다는 '디지털 공화국'이라는 용어가 채택되었다는 사실인데, 프랑스는 이 법 속에 프랑스 왕정을 무너뜨리고 공화정을 세울 당시에 추구한 프랑스 공화국의 3대 기본정신인 '자유 (liberté)', '평등 (égalité)', '박애 (fraternité)'의 정신을 녹여 넣고자 노력했다는 사실이다. 먼저 자유의 정신은 데이터의 개방을 가능한 한 극대화하여 프랑스 경제에 자유경쟁의 가능성을 더욱 불어넣고자 하는 데서 찾을 수 있다. 다음으로 평등의 정신은 이들 데이터를 개인 연구자들은 물론 관심을 가진 개인들도 서비스 플랫폼을 활용하여 얼마든지 자유로우면서도 쉽게 활용할 수 있는 여건을 만들고자 하는 데서 찾을 수 있다. 마지막으로 박애의 정신은 데이터에 대한 접근성 즉, 인터넷에 대한 접근성 수준을 프랑스 전역(프랑스 해외 영토 포함)에서 똑같이 되도록 하고, 장애인들을 포함한 모든 사회적 약자들에게도 비슷한 수준의 데이터 이용 가능성을 제공할 수 있는 환경을 만들고자 하는 데서 찾을 수 있다. 이어지는 법 제정 과정의 논의 속에서도 이들 내용들이 모두 다루어졌다는 사실도 흥미로운 점이다.

프랑스 재정경제부 기업일반사무국(Direction generale des entreprises[4])에서 작성한 '디지털 공화국을 위한 법률'의 요약보고서에 따르면 이러한 노력이 주는 가장 큰 시사점은 이 법을 제정하는 목적이 결코 관련 기업들이 데이터 활용을 통해 얻을 수 있는 경제적 이익을 확보하는 데에만 있는 것이 아니라 프랑스 국민 모두가 자유롭고 평등한 데이터 사용의 권리와 의무를 가지는 것을 인식하게 만드는 데에도 있다는 점을 알게 함으로써 이 법의 제정 과정에 프랑스 국민 모두가 관심을 가지게 만들었다는 점일 것이다.[5]

4) 기업일반사무국(DGE)은 프랑스 재정경제부 산하의 사무국이다. 2014년 이전에는 경쟁, 산업 및 서비스 일반사무국으로 불리웠다. 기업일반사무국은 재정경제부 산하에서 서비스, 장인, 상업, 관광, 디지털 경제, 산업과 관련된 공공정책을 구상하고 시행한다. https://fr.wikipedia.org/wiki/Direction_g%C3%A9n%C3%A9rale_des_entreprises

5) Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique, Direction generale des entreprises(PDF), 2016, p. 2.

기고

디지털공화국법이 발효된 2017년부터 프랑스 스타트업들이 르네상스를 맞게 됐다는 평가가 지배적이다.

Ⅳ. 정보조작의 규제

2018년 11월 20일(현지 시각 기준), 프랑스 하원이 「정보조작 대처에 관한 법안들(Les propositions de loi contre la manipulation de l'information, Proposition de loi organique)[6], 약칭 '정보조작대처법'」을 통과시켰다.[7] 상원에 의해 두 번 연속 거부됐던 법안들이 긴 진통 끝에 가결된 것이다.[8]

정보조작대처법은 크게 두 가지 법안으로 구성된다.

1. 하나는 국가 조직법의 차원에서 발의됐다. 즉, 허위 정보 대처에 관한 통상법에 의해 이미 확립된 법적 조치들을 대선 캠페인에 적용하는 것을 목표로 한다. 헌법 제6조에 따라 공화국 대통령 선거 방식은 국가 조직법으로 정해져있기 때문에 이러한 적용을 목적으로 하는 법안은 국가 조직법의 개정안으로 간주된다. 이 법안은 183 : 111로 통과됐다.
2. 나머지 하나는 통상법의 범주에서 선거 중에 발생할 수 있는, 허위정보를 이용해 선거를 방해하기 위한 시도들을 저지하는 것을 목표로 한다. 이 법안은 347 : 204로 통과됐다.

정보조작대처법의 핵심 내용은 다음과 같다.

선거기간 동안 인터넷과 소셜 미디어에서 정보의 왜곡에 대응하기 위해 마련된 이 법안은 허위정보의 배포를 판사가 중지시킬 수 있도록 하고 있다. 시사적인 정보는 그것이 선거와 직접적인 연관이 없더라도, 혹은 언론이 보도했는지의 여부와 관계없이 소송 대상이 될 수 있다. 이러한 허위정보의 유포를 중지시키기 위해 짧은 시간 내에 법원이 명령을 내릴 수 있도록 하고 있다. 물론 판사가 아무 때나 개입할 수 있는 것은 아니다. 판사의 개입이 정당화되기 위해서는 정보는 '명백하게 허위'여야 하고, 의도적(인위적)이며, 대량으로 배포되어야 한다. 또한, 디지털 플랫폼, 특히 소셜 네트워크에 이들이 수수료를 받는 콘텐츠, 즉 광고 콘텐츠에 한하여 투명성 의무 조항을 부과하고 있다.

아울러 시청각최고위원회(Conseil superieur de l'audiovisuel; 이하 'CSA')에는 한 국가가 의도적으로 선거에 영향을 미치기 위해 허위정보를 배포하는 경우, 그 국가의 영향 아래

6) 위 법률안은 조직법률안으로써 프랑스에서 이러한 법률안은 공포 전 필수적으로 사전위헌법률심판을 받는다.
7) 위 법률안의 자세한 제정 과정은 http://www.assemblee-nationale.fr/dyn/15/dossiers/alt/lutte_fausses_informations 참조.
8) 프랑스 헌법재판소(le Conseil constitutionnel)는 2018년 11월 20일, 위 법률에 대하여 합헌결정을 하였다. 결정문의 자세한 내용은 https://www.senat.fr/espace_presse/actualites/201806/lutte_contre_les_fausses_informations.html 참조.

통제되는 방송서비스에 한해, "방송 중지 명령"을 내릴 수 있도록 하는 권한을 부여하고 있다. 물론 누구나 짐작하듯 이는 러시아 방송채널을 통제하기 위한 목적이다.

끝으로 이 법은 온라인 공중 커뮤니케이션 사용 방식, 비판적으로 정보 읽기 등을 의무적으로 교육하게 하는 등 미디어 교육에 관한 조치들을 포함한다.

Ⅴ. 디지털세 도입

2019년 1월 6일 프랑스 정부는 구글・애플・아마존 등 거대 IT 공룡들에게 세금을 별도로 부과하는 '디지털세' 법안을 공식 발표했다.

LE FIGARO(2019. 3. 6)에 따르면 이 법의 주요 타깃은 구글 애플 페이스북 아마존 등으로, 이들 기업의 이름 앞글자를 따 'GAFA세'로 불린다. 프랑스 정부는 전 세계에서 연 매출이 7억5,000만 유로 이상이거나 프랑스에서 2,500만 유로 이상의 매출을 올리는 인터넷 기업에 대해 연 매출 최대 5%만큼 과세한다는 계획이다. 브루노 르 마리 프랑스 재무장관은 정부안을 이달 안으로 의회에 제출할 예정이며 의회에서 의결되면 법은 올해 1월분부터 소급 적용된다고 밝혔다. 디지털세는 법인세처럼 이익에 과세하는 게 아니라 매출에 과세한다. 그래서 그 액수가 만만치 않다. 회사 법인이 어디 있는지가 아니라 그들의 상품을 소비하는 소비자가 어디에 있는지에 따라 세금을 부과한다.[9)]

일부 EU 국가 반대에도 프랑스 정부는 디지털세에 대해 강경한 태도를 취하고 있다. 프랑스는 지난해 아마존에서도 2억200만유로 미납세금 납부를 이끌어냈다.

프랑스가 독자적으로 GAFA세 부과로 돌아선 데는 유럽연합(EU) 차원의 디지털세 도입이 아일랜드 등의 반대로 지난해 실패했기 때문이다. 아울러 '노란조끼' 시위로 유류세 인상이 좌절되면서 추가 세원 발굴이 절실한 상황도 작용했다.

Ⅵ. 마치며

프랑스는 타 국가에 비해 일찍부터 개인정보보호에 관심을 갖고 지속적으로 노력해 왔으며, 최근에는 다양한 법률제정과 더불어 사회 전반에 걸친 정책 등의 추진으로 이어지고 있다. 특히 주목할 점은 '공익 데이터' 라는 개념을 도입하여 개인의 권리침해 문제까지도 다루고 있으며, 더 나아가 국민에 대한 미디어 교육과 추가 세원까지 발굴하고

9) http://www.lefigaro.fr/conjoncture/2019/03/05/20002-20190305ARTFIG00247-la-france-degaine-sa-taxe-des-geants-du-numerique.php

있다는 점이다.

하지만 복잡하고 빠르게 발전하는 사회현실 속에서 법적 구속력을 높이기 위해서는 여전히 관련 법률과 정책들에 관한 고민이 필요한 상황이다. 왜냐하면, 이제 데이터는 단순한 자료로서의 가치를 넘어 세상을 변화시키고, 경제를 성장시키며 개인에게 많은 권한을 부여하는 융합 보안의 형태로 변모하고 있기 때문이다.

※ **Reference**

1. https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033202746&categorieLien=id
2. https://www.inc-conso.fr/sites/default/files/pdf/Tableau-loi-Informatique-libertes-1978.pdf
3. https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037800506&categorieLien=id
4. https://fr.wikipedia.org/wiki/Direction_g%C3%A9n%C3%A9rale_des_entreprises
5. http://www.assemblee-nationale.fr/dyn/15/dossiers/alt/lutte_fausses_informations
6. https://www.senat.fr/espace_presse/actualites/201806/lutte_contre_les_fausses_inf ormations.html
7. http://www.lefigaro.fr/conjoncture/2019/03/05/20002-20190305ARTFIG00247-la-france-degaine-sa-taxe-des-geants-du-numerique.php

인터넷 법제동향
Vol. 139 (April 2019)

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

| 발 행 처 | 한국인터넷진흥원
(58324) 전라남도 나주시 진흥길 9 한국인터넷진흥원
Tel. 1544-5118
| 기획・편집 | 법제연구팀
| 발간・배포 | www.kisa.or.kr