Vol. 140 (May 2019)

인터넷 법제동향

Laws and Policy Trends of the Internet

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

CONTENTS

국내 입법 동향

해외 입법 동향

기고

<국회 제출 법률안>		
법령명	**대표발의 의원 (발의날짜)**	**주요내용**
• 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안	박완수의원 (2019. 5. 1.)	- 정보통신망을 통해 사람을 모욕한 자에 대하여 「형법」상의 모욕죄보다 무겁게 처벌함
• 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안	유의동의원 (2019. 5. 13.)	- 정보통신서비자에게 규제나 간섭을 하지 못하게 하여 정보통신서비스제공자의 공적 책임과 공익성을 강화함
• 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안	백혜련의원 (2019. 5. 22.)	- 정보통신망 유통금지 불법정보의 대상에 마약·향정신성 의약품 또는 대마의 사용 및 제조 매매 알선 규정을 정하고 형사처벌 하도록 함
• 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안	하태경의원 (2019. 5. 29.)	- 불법정보 유통 목적이거나 불법정보가 전체 정보의 20%이상인 정보통신망서비스에 대해 처벌할 수 있도록 함
• 「개인정보 보호법」 일부개정법률안	최인호의원 (2019. 5. 3.)	- 신기술 개발 목적으로 자율주행차량 영상정보를 목적 외 이용이나 제3자에게 제공할 수 있도록 함
• 「성폭력범죄의 처벌등에 관한 특례법」 일부개정법률안	유승희의원 (2019. 5. 3.)	- 성폭력범죄의 정의규정에 「정보통신망 이용촉진 및 정보호호 등에 관한 법률」상의 음란물 유포죄를 추가함

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안
(박완수의원 대표발의, 2019. 5. 1. 제안)

▶ 소관 상임위원회 : 과학기술정보방송통신위원회

▶ 제안이유

o 현행법은 사람을 비방할 목적으로 정보통신망을 통하여 공공연하게 사실을 드러내어 다른 사람의 명예를 훼손한 자는 「형법」상의 명예훼손죄보다 무겁게 처벌하도록 하고 있으나, 정보통신망을 통하여 공공연하게 사람을 모욕한 자에 대하여는 현행법에 관련 규정이 없어 「형법」에 따른 모욕죄로만 처벌을 하고 있음

o 그러나 최근 인터넷에서 특정인을 공공연하게 모욕하는 내용의 게시물로 인한 인격권 침해가 발생하고 있으며, 인터넷에서 이러한 정보가 쉽고 광범위하게 유통되어 피해의 정도가 심각하다는 점에서 이에 대한 처벌을 강화해야 한다는 의견이 제기되고 있음

▶ 주요내용

o 정보통신망을 통하여 공공연하게 사람을 모욕한 자에 대하여 「형법」상의 모욕죄보다 무겁게 처벌함으로써 건전한 인터넷 문화 형성에 기여하려는 것임(안 제70조의2 신설)

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

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안
(유의동의원 대표발의, 2019. 5. 13. 제안)

▶ 소관 상임위원회 : 과학기술정보방송통신위원회

▶ 제안이유

o 현행법상 정보통신서비스 제공자의 자유와 독립을 유지하기 위한 보호장치와 공적 책임, 공정성 및 공익성을 담보하는 의무장치가 미비한 상태임

o 수많은 이용자들이 정보통신서비스 제공자의 정보통신서비스를 통해 뉴스 기사 등을 검색하는 현실에서 권력기관 등의 부당한 압력으로 특정 정권 등에 유리한 뉴스 기사의 의도적인 노출과 편성이 이루어질 가능성이 있다는 지적이 있음

▶ 주요내용

o 정보통신서비스 제공자로 하여금 정보통신서비스를 공정하고 객관적으로 제공하고 지역 간·세대 간·계층 간·성별 간의 갈등을 조장하지 못하도록 하며, 누구든지 정보통신서비스 제공자에 대하여 어떠한 규제나 간섭을 하지 못하게 하여 정보통신서비스 제공의 자유와 독립을 보장함으로써 정보통신서비스 제공자의 공적 책임과 공익성을 강화하려고 함(안 제3조제2항 신설 등)

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

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안
(백혜련의원 대표발의, 2019. 5. 22. 제안)

▶ 소관 상임위원회 : 과학기술정보방송통신위원회

▶ 제안이유

o 현행법에서는 정보통신망을 통하여 유통이 금지되는 불법정보의 대상을 범죄를 목적으로 하는 내용의 정보 등으로 포괄적으로 규정하고 있고, 삭제 요구 등의 시정조치에 그치고 있는 상황으로 정보통신망에 마약류의 사용, 제조, 매매, 매매의 알선 등의 정보가 게시되더라도 실제 범죄로 이어졌다는 사실이 입증되지 않는 한 형사처벌도 불가능한 실정임

o 최근 성범죄에 악용되고 있는 마약, 향정신성의약품이 해외 블로그나 SNS, 포털사이트의 블로그, 카페, 게시판 등을 통하여 공공연하게 거래되면서 성범죄에 이용되는 등 2차 범죄를 유발하고 있어 심각한 사회문제로 대두되고 있음

▶ 주요내용

o 정보통신망을 통하여 유통이 금지되는 불법정보의 대상에 마약·향정신성의약품 또는 대마의 사용, 제조, 매매, 매매를 알선하는 내용의 정보를 명확히 규정하고, 이를 위반하는 경우 형사처벌 할 수 있도록 규정하려는 것임(안 제44조의7제1항제8호의2 신설 등)

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

「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 일부개정법률안

(하태경의원 대표발의, 2019. 5. 29. 제안)

▶ 소관 상임위원회 : 과학기술정보방송통신위원회

▶ 제안이유

o 최근 특정 커뮤니티가 안타까운 희생을 조롱하거나 성별 등을 이유로 비하, 욕설은 물론이며 무차별적 신상털기・특정인에 대한 성적 희화화 혹은 합성된 음란물 유포・살해협박・테러위협 등 반사회적 범죄를 조장 혹은 방조하는 내용의 정보를 유통시키고 있어 사회적 문제가 되고 있음

o 하지만, 반사회적 경향의 사이트에 대한 처벌조항이 별도로 규정되어 있지 않아서 사회적인 해악을 끼치는 사이트에 대한 규제가 쉽지 않음

o 현행법으로 규정하고 있는 불법정보에 성별, 나이, 지역, 피부색, 장애를 이유로 한 비방, 조롱, 욕설, 음란한 부호・문언 등의 내용이거나, 폭력・살인・테러 등의 사회의 규범이나 질서를 위협하는 반사회적 범죄를 조장 혹은 방조하는 정보를 포함시키고자 함

▶ 주요내용

o 불법정보를 유통할 목적으로 회원, 운영방침 또는 게시물 작성방침, 운영체계 등을 갖추고 있거나 불법정보가 전체 정보의 100분의 20 이상인 정보통신망서비스에 대해 이용해지, 접속차단을 하도록 하며, 관련자에 대해서는 처벌할 수 있도록 함(안 제44조의7제1항제2호의2, 제44조의7제3항, 제74조제1항제2호의2 신설)

※ **Reference**

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

「개인정보 보호법」 일부개정법률안
(최인호의원 대표발의, 2019. 5. 3. 제안)

▶ 소관 상임위원회 : 행정안전위원회

▶ 제안이유

o 사회전반 디지털화 및 인공지능의 발달로 교통분야에서도 자동차 스스로 주변환경을 인식하여 운행하는 자율주행자동차 시대로 빠르게 진화하고 있음.

o 세계 5위 자동차 산업국가인 우리나라의 경우도 2020년 자율주행자동차 상용화를 목표로 자율주행자동차의 개발 및 양산에 총력을 기울이고 있는 상황으로 자율주행자동차 기술개발을 위한 도로에서의 운행 시험 및 연구 등이 필수적이라 하겠음

o 그러나 현행법에서 도로에서 영상정보처리기기에 촬영된 자율주행자동차의 시범운행 영상을 촬영하거나 해당 영상을 이용·제공하는 것이 금지되어 있어 이에 대한 개선방안을 마련할 필요가 있다는 지적이 제기됨

▶ 주요내용

o 대통령령으로 정하는 신기술 개발 목적을 위하여 필요한 경우 보호위원회의 심의·의결을 거친 경우에 한하여 해당 영상정보를 목적 외 용도로 이용하거나 제3자에게 제공할 수 있도록 함으로써 자율주행자동차 신기술 개발을 지원할 수 있는 방안을 마련하고자 함(안 제18조제2항제4호 및 같은 호 단서 신설)

※ **Reference**

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

「성폭력범죄의 처벌등에 관한 특례법」 일부개정법률안
(유승희의원 대표발의, 2019. 5. 3. 제안)

▶ 소관 상임위원회 : 법제사법위원회

▶ 제안이유

o 최근 성범죄를 저지른 현직 초등학교 교사가 음란물 유포죄로 처벌을 받은 사실을 수사기관으로부터 통보받고도 해당 교육청은 관련법상 직위해제 기준이 모호하다는 이유로 직위해제를 하지 않아 논란이 된 바 있음.

o 해당 교사는「정보통신망 이용촉진 및 정보호호 등에 관한 법률」제74조제1항제2호의 죄(음란물 유포 등)에 따라 처벌되었지만, 이 법률을 근거로 처벌받은 교사나 공무원은 직위해제 대상이 아니라는 해석에 따라 담임교사직을 유지할 수 있었던 것임

o 성폭력범죄의 처벌 등에 관한 특례법 제2조 성폭력범죄의 정의 규정에「정보통신망 이용촉진 및 정보호호 등에 관한 법률」상의 음란물 유포죄를 추가하여 성범죄를 저지른 교사와 공무원에 대해 직위해제 등의 엄격한 법적용을 함으로써 피해자를 두텁게 보호하려는 것임

▶ 주요내용

o 현행법 제2조(성폭력범죄 정의규정)에「정보통신망 이용촉진 및 정보호호 등에 관한 법률」상의 음란물 유포죄를 추가함(안 제2조제1항제6호 신설)

※ **Reference**

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

미국 상원, 연방정부 사이버보안 인력의 순환·교류 활성화 법안 승인 (2019. 4. 30.)

미국 상원은 연방정부의 사이버보안 인력이 다양한 실무 기술과 경험을 습득하도록 기관 간 인력 교류를 촉진하는 《사이버보안 인력의 순환·교류 활성화 법안》[1]을 승인 (2019. 4. 30.)

▶ 개요 및 경과

o 미국 상원은 연방정부에서 사이버보안 업무를 담당하는 공무원의 실무 역량을 향상하기 위해 사이버보안 실무 기술과 관련된 공공·민간 기관의 업무를 고루 경험 할 수 있도록 지원하는 《사이버보안 인력의 순환·교류 활성화 법안》을 승인

- 동 법안의 주요내용은 ▲사이버보안 인력의 순환 배치 목록 작성 ▲사이버보안 인력의 순환·교류를 위한 운영계획 개발 및 추진 ▲사이버보안 인력 순환·교류 프로그램의 운영 성과 및 효과성 평가임

o 2017년에 미국 회계 감사원(GAO)[2]은 국가 사이버보안 수준의 향상을 위해 연방정부가 주도적으로 사이버보안 인력에 대한 교육훈련 및 양성에 노력을 기울여야 한다고 권고[3]

- 전 국가적인 사이버보안 담당 인력의 보안기술 격차를 해소하고 높은 역량의 전문 인력 육성을 목표로 연방기관에서 추진해야 하는 인적자원개발 정책 방향을 제시

▶ 주요 내용

o **(법안의 목적)** 동 법안은 연방정부의 사이버보안 관련 인력을 충원하고 유지하기 위한 노력을 강화하고 인력 운영계획을 개선하도록 촉진하는데 그 목적이 있음

o **(인력 순환 배치 목록의 작성)**

- 연방정부 기관의 인사관리책임자는 최고인적자원관리위원회[4]와 국토안보부 장관의

1) Federal Rotational Cyber Workforce Program Act of 2019 (S.406)
2) Government Accountability Office: 미국 의회 소속의 감사기구로 1921년 예산회계법(Budget and Accounting Act) 제정에 근거하여 설립됨. 정부기관 등에 대한 감사, 정부의 사업과 활동에 대한 평가, 정부 회계기준 및 정부감사기준의 제정과 공포가 주요 기능이며, 최근 업무 중심이 기존의 회계 감사 기능에서 개별 정책에 대한 성과 분석 및 평가업무로 확대되고 있음.
3) CYBERSECURITY-Actions Needed to Strengthen U.S. Capabilities(GAO-17-440T), Government Accountability Office, 2017, 출처: https://www.gao.gov/assets/690/682756.pdf

도움을 받아 사이버보안과 관련된 직무내용 및 필요한 역량 수준을 포함한 인력의 순환 배치 목록을 작성해야 함

- 각 연방정부 기관의 장은 기관 내에 소속된 사이버보안 인력에 대하여 타 기관 과의 순환·교류 프로그램 참가 자격을 자체적으로 판단 및 부여할 수 있음

o **(인력 순환·교류를 위한 운영계획 개발 및 추진)**

- 동 법안의 제정일로부터 270일 이내에 연방정부 각 기관의 인사관리책임자는 국토안보부 최고정보보호책임자 등과 협의하여 사이버보안 인력의 순환·교류를 위한 운영계획을 개발 및 발표해야 함

- 운영계획에 담아야 할 주요내용과 관련 행정절차는 아래와 같음

< 사이버보안 인력 순환·교류 운영계획에 포함해야 하는 내용 및 관련 행정절차>

구분	주요 내용
운영계획에 포함해야 하는 내용	• 사이버보안 인력에 대한 교육훈련 및 경력개발 참여에 필요한 요구사항 - 본 프로그램에 대한 참여는 자발적이어야 하며, 소속 기관장이 참여를 승인하는 경우 참여할 수 있는 자격을 부여 • 사이버보안 인력 순환·교류 프로그램에 참여하는 인력에 대한 성과 측정 • 사이버보안 인력 순환·교류에 대한 참여하는 경우 공석인 업무 대체 방안 • 사이버보안 인력 순환·교류 종료 후 해당 직위로 복귀할 수 있는 권리 보장
관련 행정절차	• 연방정부의 각 기관장은 미국연방법전 제2301조[5]에 따른 성과체계 원칙을 준수하여 사이버보안 인력 순환·교류 프로그램 참여자를 선정해야 함 • 연방정부의 각 기관에서 사이버보안 업무에 종사하는 직원은 기관장의 승인을 받아 인력 순환·교류 프로그램 참여 신청서를 제출 • 사이버보안 인력의 순환·교류의 기간은 180일 이상 1년 이하를 원칙으로 하며, 60일 까지 연장이 가능

o **(운영 성과 및 효과성 평가)** 회계 감사원장은 사이버보안 인력의 순환·교류 운영계획이 발표된 이후 2년 후 회계연도 종료일까지 동 계획의 운영 성과 및 효과를 평가한 보고서를 의회에 제출하여야 함

o **(기타 사항)** 동 법안은 제정일로부터 5년 후에 폐지됨

4) 2002년에 제정된 최고인적자원관리법(Chief Human Capital Officers Act of 2002)에 의해 설립된 최고인적자원관리위원회(Chief Human Capital Officers Council)로 동 위원회의 주요 역할은 미국 인사관리청 (Office of Personnel Management)의 인적자원관리전략에 대한 자문 및 조정을 담당함.

5) U.S. Code § 2301. Merit system principles: 연방정부 기관의 인사관리에 대한 성과시스템 원칙을 규정하고 있으며, 선발과 승진은 모두가 동등한 기회를 얻는 공정하고 열린 경쟁 후에 상대적인 능력, 지식 및 기술에 근거하여 결정하도록 함.

▶ 시사점

o 미국 정부는 사이버보안 업무를 담당하는 인력이 다양한 실무분야에서 기술과 경험을 체득하는 것이 전 국가적인 사이버보안 수준을 강화하는데 매우 필요하다는 것을 공감하고 다양한 법제도를 개발 및 도입하고 있음

o 본 법안은 국가 사이버보안 인재육성 정책의 일환으로 연방정부가 주도하여 공공기관 및 민간기관 간 인력 순환 및 교류를 촉진하는 것으로, 향후 국가의 전반적인 사이버보안 기술개발이 활성화되고 높은 성과를 거둔 전문 인력에 대한 적절한 보상과 함께 사이버보안 위험 대응 능력도 강화될 것으로 기대

※ **Reference**

https://www.congress.gov/bill/116th-congress/senate-bill/406/text
https://www.infosecurity-magazine.com/news/senate-passed-fed-cyber-workforce-1/

미국 정부, 사이버보안 인력 양성을 위한 행정명령 시행 (2019. 5. 2.)

미국 정부는 국가 사이버보안 전문 인력 양성을 위해 교육훈련 및 투자를 강화하고, 우수한 인재에게 보상을 강화하는 《사이버보안 인력 양성을 위한 행정명령》[1]을 시행 (2019. 5. 2.)

▶ 개요 및 경과

o 미국 정부는 연방정부의 사이버보안 실무자의 역량 향상을 위해 새로운 교육훈련 체계를 수립하고, 공공과 민간부문을 아우르는 사이버보안 전문 인력 양성을 통해 급증하는 사이버보안 실무 인력 수요에 대응하도록 권고하는 행정명령을 시행

- 국토안보부장관이 새로운 사이버보안 인력 교육 체계를 수립하고, 국방부장관 및 과학기술정책국장이 사이버보안 경진대회 시행계획을 수립하도록 규정

- 연방기관이 사이버보안 분야의 성과와 업적을 장려하는 새로운 상훈 등을 수여할 수 있도록 관련 법규의 개정 및 계획을 수립하도록 함

o 지난 2017년 5월에 사이버보안 인력의 역량강화 방향을 개념적으로 제시한 《연방 네트워크 및 핵심 인프라의 사이버보안 강화를 위한 행정명령》[2]이 시행된 바 있으며, 이번에 시행된 행정명령은 그 내용을 구체화하고 중요한 사항을 실행하도록 규정한 것임

▶ 주요 내용

o **(목적)** 국가의 사이버보안 실무 역량 수준을 향상하기 위해 실무자에게 지식・기술・능력을 극대화하는 체계화된 교육훈련을 실시하고, 사이버보안 분야의 발전에 기여한 우수한 인재에게 성과 보상을 강화하는 것을 그 목적으로 함

o **(연방정부의 사이버보안 인재개발)**

- 연방정부의 인사관리책임자는 사이버보안 실무자를 위한 인재개발 과제를 도출하고, 국토안보부장관은 동 명령 시행일로부터 90일 이내에 도출된 과제들을 종합하여 실행에 필요한 조치[3]를 담은 보고서를 대통령에게 제출해야 함

1) Executive Order on America's Cybersecurity Workforce
2) Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, 2017
3) 주요 조치사항의 예: 사이버보안 인력이 국토안보부 등 타 기관에 일정기간 동안 필요한 실무를 습득할 수 있도록 지원, 기술 수준 향상을 위한 교육 커리큘럼의 제공 및 학습 경험의 확대, 동료 간의 멘토링 제도 등

- 미국 인사관리처장(Director of the Office of Personnel Management)은 동 명령 시행일로부터 180일 이내에 상무부장관 및 국토안보부장, 기타 관계기관의 장과 협의하여 사이버보안 업무의 적성 평가[4]를 위한 기초 항목을 작성해야 함

- 연방정부의 기관장은 사이버보안 분야의 종사자에게 해당 분야에서 노력한 성과와 업적을 인정·장려하는 상훈 등을 수여해야 하며, 필요한 경우 관련 법규에 대한 개정을 실시할 수 있음

o **(국가 사이버보안 인력 양성)**

- 본 규정은 공공과 민간부문을 모두 포함한 국가 전체의 사이버보안 전문 인력을 양성하기 위한 것으로 주요 내용은 아래와 같음

< 국가 사이버보안 인력 양성과 관련된 주요 규정 >

구분	주요 내용
국가 사이버보안 인력 양성을 위한 권고 보고서의 작성	• 상무부장관 및 국토안보부장관은 교육부장관과 기타 관계기관의 장과 협력하여 국가 사이버보안 인력 양성을 위한 권고 보고서를 작성해야 함 - 최근 급증하는 사이버보안 인력 수요를 충족하기 위한 대응방안 - 사이버보안 전문 교육훈련 환경의 혁신·고도화방안 - 사이버보안 인력 양성을 위한 투자 계획과 예상되는 효과 등
국가 중요 인프라의 사이버보안 취약점 완화를 위한 교육훈련 계획 보고서의 작성	• 국가 중요 인프라와 관련된 사이버-물리적 시스템의 보안 취약점 완화 능력을 강화하기 위해 국토안보부장관과 노동부장관은 동 명령 시행일로부터 180일 이내에 대통령에게 다음의 내용을 담은 보고서를 제출해야 함 - 국가 중요 인프라 관련 업무를 수행하는 사이버보안 인력에게 필요한 역량 수준과 교육훈련 간의 차이를 파악 및 평가 - 확인된 기술 격차를 해소하기 위한 교육훈련 프로그램 개발 지원 등
사이버보안 교육과 관련된 상훈	• 동 명령 시행일로부터 1년 이내에 교육부장관은 국립과학재단[5]과 협의하여 대통령이 우수한 교육자에게 사이버보안 교육 상훈을 수여하도록 함 - 상훈의 선정은 사이버보안과 관련된 주제에 대한 기술·지식·열정이 입증된 우수 교육자를 대상으로 하고, 교육생의 성취도를 고려

4) aptitude assessments: 일반적으로 업무 수행에 필요한 기본 지식과 소양, 자질 등을 평가하는 것을 의미하며, 본 행정명령에서의 업무 적성 평가는 각 연방정부 기관에 소속된 전 직원이 대상이며, 사이버보안 기술에 소질과 발전 가능성이 높은 인력을 발굴하는데 사용함.

5) National Science Foundation: 미국 상무부 산하의 기관으로 과학기술 분야의 연구 지원 및 계획 수립을 담당

▶ 시사점

o 이번에 시행한 행정명령으로 미국 정부는 사이버보안 관련 직무에 우수한 전문 인력들이 확충되고, 체계적인 교육훈련을 통해 실무 역량 수준이 높아질 것으로 기대

o 또한 사이버보안 분야의 성과와 업적을 장려하는 환경이 조성됨에 따라 상훈법 등 관련된 법규의 개정 및 다양한 성과 보상 정책도 추진 될 것으로 전망

※ **Reference**

https://www.whitehouse.gov/presidential-actions/executive-order-americas-cybersecurity-workforce/
https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-strengthening-americas-cybersecurity-workforce-secure-nation-promote-prosperity/
https://gdpr.report/news/2019/05/03/us-government-releases-executive-order-on-us-cybersecurity-workforce/

미국 국가사이버보안센터(NCCoE), 에너지 산업 부문의 IoT 보안 가이드 초안 발표 (2019. 5. 6.)

미국 NIST 국가사이버보안센터(NCCoE)[1]는 에너지 산업 분야의 IoT 사이버보안 위험에 대한 적절한 대응 방안을 안내하는 《에너지 산업 부문의 IoT 보안 가이드》[2]초안을 발표 (2019. 5. 6.)

▶ 개요 및 경과

o 미국 NIST 국가사이버보안센터는 최근 에너지 산업 분야에서 IoT 기술 활용이 증가하고 분산형 에너지 자원(Distributed Energy Resources, DERs)[3]의 안전한 정보교환이 요구됨에 따라 사이버보안 위험에 대한 적절한 대응 방안을 안내하는 《에너지 산업 부문의 IoT 보안 가이드》초안을 발표

- 최근에 DERs의 활용이 확대됨에 따라 에너지 산업 분야의 기관 및 기업에 발생할 수 있는 IoT 사이버보안 위험 시나리오를 주요 유형별로 제시하고, 조치할 수 있는 적절한 방법을 권고함

- DERs 시스템 인프라에서 요구되는 기본적인 IoT 사이버보안 기능을 제시하고, NIST 사이버보안 프레임워크[4]와 관련된 내용을 참조할 수 있도록 안내

o 이번에 발표한 가이드라인 초안에 대한 대국민 의견수렴은 2019년 6월 5일 까지 실시

▶ 주요 내용

o **(목적)** 에너지 산업 분야에서 IoT 기술을 이용한 DERs의 원활한 정보 교환을 위해 관련 기관 및 기업에게 사이버보안 위험에 대한 적절한 대응 방안을 제공

---

1) National Cybersecurity Center of Excellence: 사이버보안 도구・기술의 보급을 지원하는 민간 협력기관으로, 국립표준기술연구소의 주도로 메릴랜드주 및 몽고메리카운티와 제휴하여 2012년에 설립함. 정부・공공기관 및 민간기관이 함께 협력하여 기업의 시급한 사이버보안 문제를 해결하는 공동의 허브로 실질적인 사이버보안 솔루션을 제공하고 있음.

2) SECURING THE INDUSTRIAL INTERNET OF THINGS - Scenario-Based Cybersecurity for the Energy Sector

3) 규모가 작고 지리적으로 분산된 발전원을 의미하며, 중앙 집중식 에너지 공급 체계의 단점을 보완하기 위한 용도로 적용한 발전 방식인 소규모 풍력 및 태양광, 바이오매스 등을 들 수 있음.

4) NIST Cybersecurity Framework: 주요 사회기반시설에 대한 사이버 위협에 대비하기 위해 국가 주요 기반시설의 운영 주체가 사이버 위협 상황에 대한 인식 및 적절한 대응을 수행할 수 있도록 단계별 활동 및 위험관리 방식을 제시하는 사이버보안 기준임. 1.0버전이 2014년 2월에 최초로 발간되었으며, 공급망 위험 관리 등의 내용을 추가하여 2018년 4월에 한차례의 개정을 통해 현재 1.1버전이 공개되어 있음. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf 참조

o **(DERs 시스템 인프라의 구성)**

- 분산 제어 시스템, 마이크로그리드(Microgrid)[5] 관리 시스템, 에너지 저장 시스템 등의 정보 교환과 관련된 시스템 구성도를 사례로 제시

o **(IoT 사이버보안 위험 시나리오와 조치 사항)**

- 본 시나리오는 전력연구소가 2015년에 발표한 DERs 시스템의 사이버보안 사고 시나리오[6]에서 중요한 사항을 도출한 것으로, 유형별 IoT 사이버보안 위험 발생 시의 적절한 조치 사항을 안내

< 에너지 산업 분야의 주요 IoT 사이버보안 위험 시나리오 및 조치 사항 >

구분	주요 내용	
산업 제어 멀웨어[7] 방지 및 탐지	시나리오	• 마이크로 그리드 관리 시스템에 악의적인 행위자가 악성코드를 이식한 후 제어 시스템의 구조와 정보 교환 방식을 파악하고 제어 장치를 조작 및 손상시킴
	조치사항	• 멀웨어 감염 방지 및 이식된 멀웨어가 기능을 하지 못하도록 보호 기능을 실현, 보호를 우회하는 멀웨어를 탐지하는 기법 실현
데이터의 무결성	시나리오	• 악의적인 행위자가 산업 제어 시스템에 대한 관찰을 통해 얻은 정보를 이용하여 유틸리티의 DERs 시스템에 스푸핑(spoofing)[8]을 시도하고 제어 시스템의 오류를 증가시킴
	조치사항	• DERs를 모니터링 및 제어하는데 사용하는 정보의 신뢰성을 보장하도록 데이터의 무결성을 보호하는 조치 실현
장치 및 데이터의 진본성[9]	시나리오	• 악의적인 행위자가 분산 제어 시스템으로 가장하고 분산 시스템에 연결된 마이크로 그리드와 관련 SW에 유효한 명령을 만들어 전달
	조치사항	• DERs 관리 시스템의 동작 및 성능 이상을 감지하고 잠재적 손상을 탐지하는 조치 실현, 시스템이 손상되지 않도록 보호

5) 소규모 지역에서 에너지를 자급자족 할 수 있는 작은 단위의 스마트그리드 시스템으로, 신재생 에너지원과 에너지저장장치가 융・복합된 차세대 전력 체계임.
6) Electric Sector Failure Scenarios and Impact Analyses–Version 3.0, Electric Power Research Institute, National Electric Sector Cybersecurity Organization Resource, Dec. 2015
7) 악의적인 목적을 위해 작성된 실행 가능한 코드로 악성 코드 또는 악성 프로그램 등을 의미함.
8) 의도적인 행위를 위해 타인의 신분으로 위장하는 것으로, 승인받은 사용자인 것처럼 시스템에 접근하거나 네트워크상에서 허가된 주소로 가장하여 접근 제어를 우회하는 사이버 공격 행위.
9) Authenticity: 정보보호 차원에서 전자적으로 의사표시를 한 자의 신원이 주장한대로 맞는가 또는 원래의 원본과 같은가를 확증(보증)하는 것.

▶ 시사점

o 미국은 에너지 산업 분야에서 IoT의 활용이 확대되고, 소규모로 분산되어 있는 에너지 자원의 교환이 활발히 이루어지고 있어 사전에 예방이 가능한 사이버보안 대응 체계를 모색하고 있음

o 이번에 발표한 가이드라인은 산업 에너지 분야의 IoT 보안과 관련된 최초의 보안 기준이라는 점에서 그 의의가 있으며, 향후 입법 및 정책 추진, 표준 개발 등의 방향도 이에 맞추어 진행될 것으로 예상

※ **Reference**

https://www.nccoe.nist.gov/news/nccoe-seeks-comments-cybersecurity-iiot-energy-sector
https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/es-iiot-project-description-draft.pdf

미국 정부, 정보통신기술 및 서비스 공급망 확보에 대한 행정명령 시행 (2019. 5. 15.)

미국 정부는 자국의 정보통신 기술과 서비스[1]를 보호하기 위해 국가비상사태를 선포하는 《정보통신 기술과 서비스 공급망 확보에 대한 행정명령》[2]을 시행 (2019. 5. 15.)

▶ 개요 및 경과

o 미국 정부는 자국의 정보통신 기술과 서비스를 보호하기 위해 국제긴급경제권한법(IEEPA)[3] 및 국가비상사태선포법[4]에 따라 사이버보안에 위협이 되는 특정 기업의 거래와 교역을 차단할 수 있는 《정보통신 기술과 서비스 공급망 확보에 대한 행정명령》을 시행

- 상무부장관이 동 명령 시행일로부터 150일 이내에 관계기관의 장과 협의하여 세부 시행규칙을 발표하도록 규정
- 국가정보국장은 정보통신 기술과 서비스에 대한 보안 위협 평가 보고서를 작성하여 대통령 및 관계기관의 장에게 제공해야 하며, 매년 정기적인 평가를 실시하도록 함

▶ 주요 내용

o **(금지 행위)** 동 명령 시행일부터 미국의 국가 안보를 위협하는 해외 적국[5]의 지시에 따라 통제되는 특정 기업[6]이 설계・개발・제조・공급하는 정보통신 기술과 서비스에 대하여 미국 정부 및 기업에 취득・설치・거래 및 사용이 금지됨

- 거래 등의 행위가 금지되는 특정 기업 목록은 상무부장관과 관계기관의 장이 결정

---

1) 동 명령에서 정의하고 있는 정보통신 기술과 서비스(information and communications technology or services)란 전송・저장・디스플레이를 포함한 전자적 방법에 의한 정보 또는 데이터 처리・저장・검색・통신 기능을 수행하거나 활성화하기 위한 하드웨어・소프트웨어 및 제품・서비스를 의미함.

2) Executive Order on Securing the Information and Communications Technology and Services Supply Chain

3) International Emergency Economic Powers Act, (50 U.S.C. 1701 et seq.): 1977년에 제정되어 미국의 안보, 외교, 경제에 현저한 위협이 발생할 경우에 그 대상이 되는 국가와 국민의 거래 금지, 자산 몰수 등을 명할 수 있는 대통령의 권한을 규정함. 미국연방법전 제1701조(특정위협, 국가비상사태 선언)는 대통령이 특정 위협으로 인해 국가비상사태를 선언한 경우에 미국밖의 전체적 또는 실질적 부분에서 미국의 경제, 대외정책, 국가안보에 대한 근원이 되는 특정위협에 대처 할 수 있는 권한을 부여하고 있음.

4) National Emergencies Act (50 U.S.C. 1601 et seq.): 1976년에 제정되었으며, 대통령이 국가 위기 상황이 발생한 경우 신속한 대응을 위해 국가비상사태를 선포할 수 있고, 의회의 승인 없이 예산의 배정 및 법률에서 정한 광범위한 권한을 행사할 수 있음.

5) 미국의 국가 안보 또는 개인의 안전에 심각한 악영향을 미치는 외국 정부 및 비정부인을 의미함.

6) 법인, 협회, 합작 투자, 파트너십, 그룹 및 기타 조직을 모두 포함

- 상무부장관은 관계기관의 장과 협의하여 금지되는 거래 등에 따른 위험[7]을 완화하기 위한 조치 사항을 제시 할 수 있고, 해당 조치 사항은 금지되는 거래 등의 승인을 위한 전제 조건이 될 수 있음

o **(권한)**

- 상무부장관에게 관계기관의 장과 협의하여 동 명령에서 금지된 행위와 관련된 시기와 방법을 지시하고, 적절한 조치를 취할 수 있는 권한을 부여
- 상무부장관은 국무장관과 협의하여 동 명령에 의해 선언된 국가비상사태에 대한 최종적인 보고서를 의회에 제출할 수 있는 권한이 있음
- 동 명령 시행일로부터 150일 이내에 상무부장관은 재무부장관, 국무장관, 국방부장관, 법무부장관, 국토안보부장관, 미국무역대표부, 국가정보국장, 연방통신위원회 및 기타 관계 기관의 장과 협의하여 위임된 권한을 실행하는 규칙을 발표해야 함

o **(평가 및 보고서)**

- 국가정보국장은 국가의 정보통신 기술과 서비스에 대한 사이버보안 위협을 지속적으로 매년 평가해야 하며, 동 명령 시행일로부터 40일 이내에 대통령 및 관계기관의 장에게 최초의 사이버보안 위협 평가 보고서를 제출하여야 함
- 국토안보부장관은 국가 중요 인프라 및 통신서비스의 사이버보안 위협에 영향을 미치는 기관, 하드웨어 및 소프트웨어, 서비스를 지속적으로 평가하고 식별해야 하며, 동 명령 시행일로부터 80일 이내에 평가 보고서를 작성해야 함
- 동 명령 시행일로부터 1년 이내에 상무부장관은 관계기관의 장과 협의하여 보고된 사이버보안 위험 평가 결과에 대한 적절한 조치를 실시하고, 연방통신위원회는 해당 조치가 충분한지 검토 후 대통령에게 보고해야 함

▶ 시사점

o 본 행정명령은 특정 국가나 기업을 지목하지는 않았으나, 주요 언론들은 이번 조치가 중국 화웨이사 등을 겨냥한 것이라는 분석을 내놓고 있음

o 상무부 산업안전국은 2019년 5월 16일에 특정 기업 목록[8]을 추가한 법인 규칙을 게시하였으며, 이 명단에 포함되는 기업들은 향후 미국 정부의 허가 없이 미국 기업들과 거래를 할 수 없으므로 제품 판매를 하지 못하는 등의 타격을 받을 것으로 전망

7) 미국 내 정보 통신 기술 또는 서비스의 설계・무결성・제조・생산・유통・설치・운영 또는 유지보수에 대한 파괴 행위 또는 파괴를 초래할 수 있는 과도한 위험, 중요한 인프라 또는 디지털 경제에 치명적인 영향을 미칠 수 있는 위험, 국가 안보 또는 자국인의 안전에 영향을 미치는 위험.

8) 미국 상무부 산업안전국에서 이번 행정명령과 관련하여 공표한 특정기업목록은 다음의 링크를 참조. https://www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-entities-to-the-entity-list

※ **Reference**

https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/

https://www.whitehouse.gov/briefings-statements/message-congress-securing-information-communications-technology-services-supply-chain/

https://www.govinfo.gov/content/pkg/FR-2019-05-17/pdf/2019-10538.pdf

해외 입법 동향 호주

호주 사이버보안센터(ACSC), 데이터 유출 관리 가이드의 개정판 공개 (2019. 5. 17.)

호주 사이버보안센터(ACSC)는 최근에 증가하는 데이터 유출 사고의 방지를 위해 모든 조직에게 적용할 수 있는 조치 사항을 안내하는 《데이터 유출 관리 가이드》[1]의 개정판을 공개 (2019. 5. 17.)

▶ 개요 및 경과

o 호주 사이버보안센터(ACSC)는 최근 소셜 미디어나 클라우드 기반 서비스 등을 통한 데이터 유출 사고가 증가함에 따라 정부 및 공공기관, 기업, 단체 등의 조직이 일반적으로 수행할 수 있는 데이터 유출 대응 절차를 안내하는 《데이터 유출 관리 가이드》의 개정판을 공개

- 데이터 유출 사고가 발생한 경우에 조직 내에서 취해야 할 적절한 대응 및 관리 절차를 5단계로 구분하여 제시

- 조직의 정보보호책임자 또는 대표자는 유출된 데이터의 관리자·제공자에게 데이터 유출 사실을 통지하고, 데이터 유출 사고의 내용을 호주 사이버보안센터에 보고[2]해야 함

o 이번 가이드는 2012년에 최초로 발표된 이후 최근의 ICT 환경 변화를 반영하여 7년 만에 개정한 것임

▶ 주요 내용

o **(정의 및 범위)** 데이터 유출은 통제되지 않거나 허가되지 않은 환경 또는 알 필요가 없는 자에게 정보를 우발적으로 노출하는 것으로 정의하며, 아래와 같은 내용을 포함

- 유출한 정보를 이메일 또는 디지털 미디어[3] 등을 이용하여 정보 취급 권한이 없는 시스템으로 정보를 전송

- 유출한 정보를 웹 포럼[4] 및 소셜 미디어, 클라우드 기반 스토리지 등을 통해 무단으로 공개

1) Data Spill Management Guide
2) 사이버 보안 사고의 보고는 호주 사이버보안센터의 홈페이지에서 개인, 중소기업, 정부, 대기업 및 인프라 부문으로 구분하여 세부 절차와 방법을 안내하고 있음. https://www.cyber.gov.au/report 참조.
3) 디지털 영상 및 오디오, 디스크, 스마트 폰 등 디지털 코드를 기반으로 동작하는 전자적 매체를 의미함.
4) 사용자가 만든 내용물을 관리하는 웹 애플리케이션으로, 인터넷 커뮤니티, 토론 그룹 및 포럼, 게시판 등을 포함

o **(데이터 유출 관리 절차)**

- 데이터 유출이 발생한 경우 ▲1단계: 식별 ▲2단계: 봉쇄 ▲3단계: 평가 ▲4단계: 치료 ▲5단계: 방지 순으로 대응하며, 단계별 세부 실천 사항은 아래와 같음

< 데이터 유출 관리 절차 및 주요 내용 >

구분	주요 내용
1단계: 식별	• 데이터 유출이 발생했음을 인식하는 것 • 데이터 유출이 의심되는 경우 또는 접근 권한이 없는 정보에 대한 접근 사항을 정보보호책임자에게 통지해야 함 • 데이터 유출은 모니터링 및 로그 등을 통해서 확인할 수 있음
2단계: 봉쇄	• 데이터 유출의 범위를 결정하고 영향을 받는 시스템을 봉쇄 • 소프트웨어 기능의 일시적인 제거, 시스템 접근 제어, 네트워크로부터의 물리적·논리적 분리를 포함 • 이메일의 경우 접근 및 전달 등 추가적인 배포를 금지
3단계: 평가	• 데이터 유출 문제를 해결하기 위한 가장 적절한 조치 방안을 결정 • 워크스테이션, 백업 스토리지, 프린터 및 인쇄 서버, 네트워크 공유, 전자 메일 서버, 웹 메일 및 관련 외부 시스템을 포함한 철저한 평가를 실시 • 조직의 정보보호책임자 또는 대표자는 유출된 데이터의 관리자·제공자에게 데이터 유출 사실을 통지하고, 데이터 유출 사고의 내용을 호주 사이버보안센터에 보고해야 함
4단계: 치료	• 정보의 소유자들과 협력하여 선정한 조치 방법에 따라 교정 조치를 실시 • 데이터를 보관하는 시스템에 대한 접근 제어, 시스템의 사업적인 중요도, 데이터의 노출 기간, 스토리지의 활용률, 시스템의 교체 및 처분 등을 고려하여 조치하고, 그 영향과 재무비용 등을 문서화
5단계: 방지	• 데이터 유출의 원인을 파악하고 검토 • 향후 데이터 유출 방생 가능성을 줄이기 위한 정책 개선, 기술적인 개선, 교육훈련 강화 등의 예방 조치를 구현

▶ 시사점

o 본 가이드라인은 호주 정부 보안 매뉴얼(ISM)[5]과는 별도로 데이터 유출 사고 발생 시 그 내용을 호주 사이버보안센터에 보고하도록 규정하였다는 점에서 그 의의가 있음

5) Australian Government Information Security Manual (ISM): 사이버보안 전문가 및 정보기술 관리자를 대상으로 조직의 정보 및 시스템 보호를 지원하기 위해 호주 사이버보안센터에서 발간하는 지침으로, 현재 사이버보안 프레임 워크 및 세부 23개 지침을 포함하고 있음.

o 현행 데이터 유출 사고의 보고 의무[6]는 호주 정부 및 비영리 기관, 신용보고 기관, 개인 정보 및 세금 파일 번호를 받는 자로 국한 되었으나, 이번에 발표한 가이드에서는 정부 및 공공기관, 기업, 단체 등 모든 조직을 대상으로 안내하고 있으므로 향후 데이터 유출 사고의 보고 의무 대상이 확대될 것으로 예상됨

※ **Reference**

https://www.cyber.gov.au/sites/default/files/2019-05/PROTECT%20-%20Data%20Spill%20Management%20Guide%20%28April%202019%29.pdf

https://www.cyber.gov.au/publications/data-spill-management-guide

6) 호주의 개인정보보호기관인 호주 정보위원회(Office of the Australian Information Commissioner, OAIC)는 프라이버시법(Privacy Act 1988) 및 프라이버시 수정법(Privacy Amendment 2017)에 따라 호주 사이버보안센터(ACSC)와 협력하여 데이터 유출 알림(Notifiable Data Breaches, NDB) 제도를 운영 중임. 동 법의 규정에 따라 호주 정부기관, 연간 매출액 3백만 호주 달러 이상의 비영리 조직 및 민간 부문 보건 서비스 제공 업체, 신용보고 기관 및 제공자, 개인 정보 및 세금 파일 번호를 받는 자는 개인정보 데이터의 유출 사고 발생 시 그 내용을 위원회에 보고해야 함.

해외 입법 동향 일본

일본 총무성, 사이버보안 정보 공개 지침(안) 발표 및 의견수렴 실시 (2019. 5. 17.)

일본 총무성은 민간기업의 사이버보안 대책에 대한 정보 공개를 촉진하기 위해 《사이버보안 정보 공개 지침(안)》[1]을 발표하고 대국민 의견수렴을 실시 (2019. 5. 17.)

▶ 개요 및 경과

o 일본 총무성은 기업이 사이버보안[2] 대책에 대한 정보를 공개하는 것이 기업의 사회적 책임[3]을 달성하기 위한 중요 요소로 보고, 적절한 정보 공개의 기준을 포함한 《사이버보안 정보 공개 지침(안)》을 발표하고 의견수렴을 실시

- 본 지침은 사이버보안 대책의 공개와 관련한 모범사례 등 참고자료를 제공하는 것을 목적으로 하며, 정보의 공개는 각 기업이 자율적으로 준수하도록 유도
- 기업의 사이버보안을 위한 10대 기준을 제공하고, 현재 기업에서 외부에 공개하는 연차보고서 등에 사이버보안 대책을 포함하여 공개하는 방법을 권장

o 일본 총무성은 민간기업의 사이버보안 대책에 대한 정보 공개를 지원하기 위해 사이버보안 테스크포스(TF)[4]를 2017년부터 운영해 왔음

▶ 주요 내용

o **(목적)** 본 지침은 기업이 자발적으로 사이버보안 대책에 대한 정보를 공개하는데 참고가 되는 안내서로 정보 공개 실행에 도움을 주는데 그 목적이 있음

---

1) 「サイバーセキュリティ対策情報開示の手引き（案）」
2) 「사이버시큐리티 기본법(2014년 법률 제104호)」 제2조(정의) 이 법에서 "사이버 시큐리티"란 전자적 방식, 자기적 방식, 기타 사람의 지각으로는 인식할 수 없는 방식(이하 이 조에서 "전자적(電磁的) 방식"이라 한다)으로 기록되거나 발신·전달 또는 수신되는 정보의 누설, 멸실 또는 훼손의 방지, 그 밖에 해당 정보의 안전관리를 위하여 필요한 조치, 정보 시스템 및 정보통신 네트워크의 안전성 및 신뢰성 확보를 위하여 필요한 조치[정보통신 네트워크 또는 전자적 방식으로 작성된 기록에 관련된 기록매체(이하 "전자적 기록매체"라 한다)를 통한 컴퓨터에 대한 부정한 활동에 의한 피해를 방지하기 위하여 필요한 조치를 포함한다]가 마련되고, 그 상태가 적절히 유지·관리되는 것을 말한다.
3) CSR(Corporate Social Responsibility): 기업이 지속적으로 존속하기 위한 이윤추구활동 이외에 법령과 윤리를 준수하고, 기업의 이해관계자의 요구에 적절히 대응함으로써 사회에 긍정적 영향을 미치는 책임 있는 활동
4) 총무성에서 2017년에 발표한 「IoT 사이버 보안 액션 프로그램 2017」에 따라 IoT 및 AI 시대의 사이버보안 대응 방안을 중점적으로 연구하는 정보보안대책실 산하의 연구회로 2017년 1월 30일부터 운영되어 왔음. 정보공개분과회는 민간 기업의 보안 대책에 대한 정보 공개와 관련된 추진 과제를 연구하고 정책 검토 및 보급을 위한 지침 개발 등의 역할을 수행함.

- 5G, IoT, AI와 같은 ICT의 활용이 사회·경제적으로 큰 영향을 미치고 있는 현실에서 기업의 사이버보안 대책에 대한 정보를 투자자 및 고객에게 공개하는 것이 기업의 신뢰도 확보 측면에서 경영층[5]이 다루어야 할 중요한 경영과제로 봄

o **(정보 공개의 수단)** 사이버보안 대책의 정보 공개는 다음과 같이 다양한 공개 보고서 및 서류를 활용할 수 있음

- 유가증권보고서, 기업지배구조보고서, 사회적책임보고서, 통합기업보고서, 기업연차보고서, 정보보안보고서 등

o **(정보 공개 방법)**

- 기업의 경영 전략과 사업내용을 기초로 최적의 사이버보안 대책을 수립하되, 아래 표에서 제시한 사항을 고려하여 해당 정보를 공개

< 기업의 사이버보안 경영을 위한 10대 기준 >

구분	주요 내용
기본 전략 수립	• 사이버보안 위험을 경영의 위험 관리의 하나로 인식하고, 조직 전체의 사이버보안 대응 기본 전략을 수립
위험관리 체제 구축	• 사이버보안 위험과 관련된 각 관계자의 책임을 명확히 하는 관리 체계 구축
자원의 확보	• 사이버보안 위험 대책을 실행하기 위한 자금과 전문 인력을 확보
위험 현황 파악 및 대응 계획 수립	• 경영전략 관점에서 보호해야 할 정보를 구분하고, 사이버 공격의 위협 현황과 그 영향을 파악한 후 위험에 대응하기 위한 계획을 수립
보호 대책 실시	• 사이버보안 위험 대응 계획에 따라 탐지·분석·방어를 위한 실질적인 보호 대책을 실시
PDCA[6] 실시	• 정기적으로 경영자에게 계획된 대책의 실행 상황을 보고하고, 문제가 발생할 경우 개선
긴급 대응 체제 정비	• 초기 대응 및 재발 방지 등을 위한 비상대응팀을 운영 • 피해 발생 후 통지처나 공개가 필요한 정보를 파악하고, 정보 공개 시 경영자가 조직내외에 설명할 수 있는 방안을 마련
복구 체계의 정비	• 사이버보안 사고로 업무 정지 등에 이른 경우, 기업 경영에 대한 영향을 고려하여 복구를 위한 절차와 대응체제를 정비하고 복구 연습을 실시
그룹단위의 대책 실시	• 거래처·위탁업체와 이와 관련한 사내 세부 조직의 사이버 보안 대책을 실시
정보공유 활동 참여	• 최신의 사이버 공격에 효율적으로 대응할 수 있도록 사이버 공격 정보 공유를 위한 활동에 적극적으로 참여

5) 기업의 의사결정을 책임지는 경영층을 의미하나, 사내의 사이버보안 업무 관련 실무담당자, 홍보 및 정보 공시 관련 담당자, 업무 시스템 관리 담당자도 본 지침을 활용하는 것을 권장함.
6) PDCA(plan-do-check-act): 계획→실천→확인→조치를 반복해서 실행하여 목표를 달성하고자 하는데 사용하는 기법

o **(기타 유의 사항)** 목적의 적합성, 표현의 진정성, 정량적인 비교 가능성, 이해의 용이성, 적시공표성을 고려하여 정보를 공개

▶ 시사점

o 일본은 기업의 사회적 책임을 달성하기 위해 중요한 요소로 사이버보안 부문을 포함하고 있으며, 이번에 공개한 지침(안)은 기업이 자체적으로 사이버보안 대책의 정보 공개 방식을 검토하는데 참고할 수 있는 최초의 지침이란 점에서 그 의의가 있음

o 이번 지침에 따라 향후 기업에서 사이버보안 부문의 중요성이 더욱 부각되고, 관련된 투자와 전문 인력의 확보, 정보공유 활동 참여가 증가할 것으로 기대

※ **Reference**

http://www.soumu.go.jp/main_content/000619819.pdf
http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00024.html

기고

융합보안의 쟁점과 과제[1)]

정필운 한국교원대학교 교수
- (現) 한국공법학회 재무이사
- (現) 한국헌법학회 학술이사, 편집위원
- (現) 한국인터넷진흥원 인터넷법제도포럼 회원
- (前) 한국인터넷법학회 총무이사

Ⅰ. 융합제품과 융합서비스의 등장으로 인한 새로운 도전

자율주행자동차, 드론과 같이 전통적인 제품에 정보통신기술(ICT)이 접목된 제품, 스마트 시티(smart city)와 같이 기존 서비스에 정보통신기술이 접목된 서비스(이하 '융합제품과 서비스'로 줄이기도 함)가 늘어나고 있다.[2)] 한국인터넷진흥원도 2019년 2월 조직 개편을 하며 이에 대응하는 전담 조직을 신설하였다.[3)] 이와 같은 제품과 서비스에 권한 없는 접속과 명령을 하여 침해사고가 발생하는 경우 현행 법제에 따른 집행체계가 그에 대하여 적절히 대처할 수 있는지 의문이다. 그러한 침해사고가 발생하였을 때 어느 부처가 나서서 어떤 절차에 따라 대처하여야 하는지 불명확하다. 제품을 관할하는 부처인 국토교통부, 산업자원부 등과 정보보안을 관할하는 부처인 과학기술정보통신부 사이에 서로 어떤 권한과 의무가 존재하는지도 불분명하다. 그로 인하여 결과적으로 시민의 생명, 신체, 재산 등의 침해가 확대될 염려가 있다. 따라서 이에 대한 적절한 대처를 위하여 법제 정비가 필요하다.

이에 따라 이 글은 융합제품과 서비스에 적절한 대처를 위하여 단기적인 법제 정비 방안을 제시하는 것을 그 목적으로 한다. 이를 위하여 융합제품과 서비스의 정의 신설, 인증제도 도입, 침해사고 대응 업무 권한 확장, 침해사고 신고 대상자와 피해 조치 대상자 확대, 정보보안에서 새로운 추진체계의 마련이 필요한지 등의 쟁점이 검토되어야 한다. 이러한 쟁점을 사전 예방적 관점(Ⅱ), 사후 대응적 관점(Ⅲ), 거버넌스 관점(Ⅳ)으로 나누어 현행 법제의 현황과 문제점을 검토하고 개선 방안을 제시한다. 마지막으로 이상의

1) 이 글은 2017-2018년 필자의 연구 결과를 정리하여 지난 2018년 8월 29일 "혁신성장을 위한 ICT 법제도 현안과 전망"이라는 제목으로 인터넷법제도 포럼, 한국과학기술법학회, 한국인공지능법학회가 공동 주최한 세미나에서 필자가 발표한 글("융합 환경에서 대응체계 개선방안")을 수정한 글입니다. 이 글의 일부는 정필운, 정경오, 심우민, 김대규, "사이버보안체계 내실화를 위한 정보통신기반보호법 개정안 연구", 과학기술정보통신부, IITP 연구보고서, 2018,12.)에도 실려 있습니다.
2) 국가정보원 외, 「2018 국가정보보호백서」, 국가정보원 등, 2018, 42쪽.
3) 매일경제, "인터넷진흥원, 15일 조직개편…융합보안 대응 조직 신설", 2019년 2월 7일 인터넷 기사.

기고

논의를 정리하며 글을 마친다(Ⅴ).

Ⅱ. 사전 예방적 관점에서 쟁점과 과제

1. 융합제품과 서비스 제공자에게 정보보호 지침 준수 의무 부과 등

현행 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 '망법'으로 줄임) 제2조 제3호는 "정보통신서비스 제공자"란 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다."고 규정하고, 제45조에서 "정보통신서비스 제공자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하여야 한다(제1항).", "과학기술정보통신부장관은 제1항에 따른 보호조치의 구체적 내용을 정한 정보보호조치에 관한 지침(이하 "정보보호지침"이라 한다)을 정하여 고시하고 정보통신서비스 제공자에게 이를 지키도록 권고할 수 있다(제2항)."고 규정하여 융합제품 제조·수입자와 융합서비스 제공자(이하 '융합서비스 제공자 등'으로 줄이기도 함)에게 보호조치 의무와 과학기술정보통신부장관이 정보보호 지침을 준수하도록 권고할 수 있는 근거가 있다고 해석할 여지도 있다. 그러나 망법 제2조 제3호가 지금까지 좁게 해석되어 왔기 때문에 이를 근거로 융합제품 제조자와 융합서비스 제공자에게 보호조치 의무와 과학기술정보통신부장관이 정보보호 지침을 준수하도록 권고하는 것은 사실상 어려움이 있을 것으로 보인다.

또한, 과학기술정보통신부장관이 정보보호 지침을 준수하도록 권고하는 것만으로는 충분하지 않다. 자율주행자동차나 드론과 같이 생명·신체, 사생활 및 재산상 피해를 야기할 우려가 있는 융합서비스 제공자 등에게는 지침 준수를 의무화하는 것이 필요하다. 이와 같은 이유로 입법론적 대응이 필요하다.

따라서 융합서비스 제공자 등에게 정보보호를 위한 보호조치 의무를 부과하고, 과학기술정보통신부장관이 정한 정보보호 지침을 준수하도록 의무화할 수 있는 명시적인 근거를 마련하는 것이 타당하다. 이러한 의무 부과는 융합제품을 사용하거나 융합서비스를 제공받는 일반 시민의 정보보안권[4] 증진에 기여할 것이다. 다시 말하면 융합제품을 사용하거나 융합서비스를 제공받는 일반 시민의 정보보안권이 객관적 질서로서 성격이 발현되면 기본권은 보편적 성격을 가지게 될 것이다. 그러므로 기본권은 국가뿐 아니라 사회구성원을 수범자로 한다.[5] 따라서 국가는 제3자인 융합서비스 제공자 등에게 이를

4) 이에 관해서는 정필운, 김형준, "제4차 산업혁명 시대 개인 정보보안 방안", 「사이버안보법정책논집」 2018년 제3호, 2018, 131-154쪽.
5) 이상 전광석, 「한국헌법론」, 집현재, 2018, 239쪽.

사용하는 일반 시민의 정보보안권을 향상하기 위한 일정한 의무를 부과할 수 있다.

그렇다고 이와 같은 의무를 모든 융합서비스 제공자 등에게 부과하는 것은 지나치다고 판단된다. 망법 제45조 제1항의 보호조치 의무는 다른 적극적인 작위 의무 부과의 전제로서 모든 융합제품 제조·수입자와 융합서비스 제공자에게 부과하는 것이 타당하지만, 과학기술정보통신부장관이 정한 정보보호 지침을 준수하도록 의무화할 수 있는 대상은 자율주행자동차나 드론 제조자와 같이 생명·신체, 사생활 및 재산상 피해를 야기할 우려가 있는 사업자로 제한하고, 로봇 완구 제조자와 같이 생명·신체, 사생활 및 재산상 피해를 야기할 우려가 없는 사업자는 제외하는 것이 타당하다. 그리고 이들이 준수할 정보보호 지침을 제정하거나 고시할 때, 이와 같은 정보보호 지침을 준수하여야 할 의무가 있는 사업자를 선정할 때에 관계부처 장관과 협의하도록 함으로써 좀 더 효율적인 행정을 할 수 있을 것이다.

2. 민간분야 정보보호지침 등 이행 여부 점검 근거 마련

현행 망법 제45조는 "정보통신서비스 제공자는 정보통신서비스의 제공에 사용되는 정보통신망의 안정성 및 정보의 신뢰성을 확보하기 위한 보호조치를 하여야 한다(제1항).", "과학기술정보통신부장관은 제1항에 따른 보호조치의 구체적 내용을 정한 정보보호조치에 관한 지침(이하 "정보보호지침"이라 한다)을 정하여 고시하고 정보통신서비스 제공자에게 이를 지키도록 권고할 수 있다(제2항)."고 규정하고 있다. 그러나 그것을 그 이행 여부를 점검할 수 있는 근거가 없다.

그런데 침해사고의 피해 예방 및 확산방지를 위해서는 정보보호지침의 준수와 이행 실태를 조사 또는 점검할 필요가 있다. 따라서 그 근거 규정을 신설하고 정당한 사유가 없는 한 조사 또는 점검에 응하도록 하는 의무 규정도 신설할 필요가 있다.

3. 인증제도 도입

정보통신기술(ICT) 영역에서는 어떤 제품이나 서비스, 행위가 일정한 수준을 갖추고 있음을 공적 기관이 증명하는 인증제도가 있다. 「소프트웨어산업 진흥법」에서 소프트웨어프로세스 품질인증 제도(제23조), 「개인정보 보호법」에서 개인정보 보호 인증 제도(제32조의2) 등이 그것이다.

자율주행자동차, 드론과 같이 정보통신기술(ICT)이 접목된 비정보통신제품과 서비스의 정보보안을 강화하기 위하여 이와 같은 제품과 서비스를 침해 사고를 걱정하지 않고 안전하게 사용할 수 있도록 인증제도 도입을 검토할 필요가 있다. 이러한 인증제도는 도입하기 위해서는 (ⅰ) 누가 인증을 하도록 할 것인지, (ⅱ) 임의로 할 것인지 의무로 할

것인지, (iii) 그 대상을 어느 범위까지 할 것인지 등이 결정되어야 한다.

필자는 우선 (ii) 융합서비스 등에 대해서 인증은 임의 제도로 두는 것이 낫다고 생각한다. 의무 인증은 새로운 규제이며 생산 비용 증가 요소인데 현재 상황에서 의무적으로 인증을 받도록 하는 것은 과하기 때문이다. (iii) 그 대상은 모든 융합제품과 융합서비스로 할 수 있고, 로봇 완구 제조자와 같이 생명·신체, 사생활 및 재산상 피해를 야기할 우려가 상대적으로 낮은 제품과 서비스는 제외하고, 자율주행자동차나 드론 제조자와 같이 생명·신체, 사생활 및 재산상 피해를 야기할 우려가 상대적으로 높은 제품과 서비스로 한정할 수 있다. 인증을 임의로 하였기 때문에 그 대상을 제한할 필요는 없다고 판단된다. 따라서 모든 융합제품과 서비스를 대상으로 하는 것에 찬성한다. 마지막으로 (i) 누가 인증을 하도록 할 것인지 결정하여야 한다. 민간 주도의 사업자단체 또는 정보보호 관련 기관·단체에서 자율적으로 하도록 할 수 있고, 과학기술정보통신부장관이 지정한 기관에서 할 수 있도록 할 수도 있다. 과학기술정보통신부장관이 관련 협회를 지정할 수도 있으므로 후자도 선택 가능한 하나이다. 그러나 과학기술정보통신부장관이 인증제도를 시행할 경우 자율인증이라 하더라도 기업은 사실상 의무인 것으로 받아들여질 수 있는 가능성이 있다. 따라서 민간 주도의 사업자단체 또는 정보보호 관련 기관·단체에서 자율인증제도를 실시할 수 있도록 하는 전자를 채택하는 것이 타당하다.

Ⅲ. 사후 대응의 관점에서 쟁점과 과제

1. 침해사고 대응 업무 권한 확장

현행 망법은 제48조의2에서 "과학기술정보통신부장관은 침해사고에 적절히 대응하기 위하여 다음 각 호의 업무를 수행하고, 필요하면 업무의 전부 또는 일부를 한국인터넷진흥원이 수행하도록 할 수 있다."고 규정하고, 각 호로 "1. 침해사고에 관한 정보의 수집·전파, 2. 침해사고의 예보·경보, 3. 침해사고에 대한 긴급조치, 4. 그 밖에 대통령령으로 정하는 침해사고 대응조치"를 나열하고 있다.

그런데 침해사고 발생 시 원인분석과 조사를 위한 업무 근거가 없어 침해사고 발생에 대응하기 위한 업무를 수행을 위하여 현장에 나가도 적절한 원인분석과 조사를 할 수 없는 문제가 있다. 따라서 이와 같은 업무를 할 수 있는 명시적 근거의 신설이 필요하다. 그리고 융합서비스 제공자 등을 포함해 침해사고를 신고한 사업자에게 이용자 피해예방조치 안내와 공개조치를 하도록 할 필요가 있다.

2. 침해사고 신고 대상자와 피해 조치 대상자 확대

현행 망법 제48조의3은 "다음 각 호의 어느 하나에 해당하는 자는 침해사고가 발생하면 즉시 그 사실을 과학기술정보통신부장관이나 한국인터넷진흥원에 신고하여야 한다. 이 경우 「정보통신기반 보호법」 제13조제1항에 따른 통지가 있으면 전단에 따른 신고를 한 것으로 본다."고 규정하고, 각 호로 "1. 정보통신서비스 제공자, 2. 집적정보통신시설 사업자"를 나열하고 있다. 그리고 제48조의4에서는 "정보통신서비스 제공자 등 정보통신망을 운영하는 자는 침해사고가 발생하면 침해사고의 원인을 분석하고 피해의 확산을 방지하여야 한다."고 규정하고 있다. 따라서 융합서비스 제공자 등이 이에 속하는지 불분명하다. 그런데 이미 설명한 것처럼 융합제품과 서비스가 침해사고가 발생하면 침해사고 신고를 하도록 하여야 하며, 침해사고가 발생하면 침해사고의 원인을 분석하고 피해의 확산을 방지하여야 하여야 한다. 따라서 그 대상자에 융합서비스 제공자 등을 명시할 필요가 있다.

IV. 거버넌스의 관점에서 쟁점과 과제

1. 심의·조정 추진체계 확립

현행 정보보안법제에서는 다음과 같은 거버넌스를 예정하고 있다. 우선 「정보통신 진흥 및 융합 활성화 등에 관한 특별법」에서 정보보호 정책의 수립과 조정 역할을 하는 정보통신전략위원회에 두고 있다. 한편, 그와 별도로 「정보통신기반 보호법」에서는 정보통신기반보호위원회를 두고 있다.

그런데 정보통신전략위원회는 정보보호 정책의 수립과 조정에 제 역할을 하지 못하고 있다. 「정보통신 진흥 및 융합 활성화 등에 관한 특별법」의 태생적 한계와 정보통신전략위원회의 소극적인 운영이 문제의 근원이다. 따라서 앞으로도 그것이 의미 있게 작동하지 못할 것으로 예상된다. 한편, 「정보통신기반 보호법」의 정보통신기반보호위원회는 근거법률인 「정보통신기반 보호법」이 정보보안 전반을 규율하는 법이 아니어서 정보보안 전반을 아우르지 못하는 추진체계라는 한계가 있다. 따라서 새로운 정보보안법은 정보보안 전반을 아우르는 추진체계를 새롭게 구축하는 것이 타당하다.

한편, 자율주행자동차, 드론과 같이 정보통신기술(ICT)이 접목된 비정보통신제품과 서비스에 대한 규율은 기존에는 과학기술정보통신부가 아니라 다른 부처의 권한이었다. 예를 들어, 자율주행자동차와 스마트시티는 국토교통부가 관할하는 제품과 서비스이고, 드론은 산업자원부가 관할하는 제품이다. 따라서 이들 제품과 서비스를 정보보안의 관점에서 과학기술정보통신부가 규율하는 것은 국토교통부, 산업자원부 등 관련부처와

협업이 필요하다. 이러한 협업과 이를 위한 활발한 의사소통을 위해서도 새로운 정보보호 추진체계가 필요하다.

따라서 현행 정보통신기반보호위원회를 정보보안위원회로 확대·개편하고, 국가정보원을 중심으로 공공부문의 정보보안을, 과학기술정보통신부를 중심으로 민간부문의 정보보안을 관리하도록 하는 현행 정보보안체계를 유지하되, 국가안보실장이 정점에서 컨트롤타워로서 정보보안 정책을 총괄·조정하는 방안이다. 위원회의 위원은 대통령령이 정하는 중앙행정기관의 차관급 공무원과 민간위원이 되도록 한다.

현행 정보통신기반보호위원회의 예에 따라 위원장 1인을 포함하여 25인 이내의 위원으로 구성하고 반드시 민간위원이 포함되도록 하는 것이 타당하다. 그리고 이러한 민간위원 중 일정 수를 산업계와 시민단체에게 추천권을 부여하는 것이 타당하다. 정보보호 정책의 수립부터 집행에 이르는 일련의 과정을 심의할 수 있는 민간위원을 두고 일정 수 이상을 산업계와 시민단체에 추천권을 부여하는 것은 정보보호를 명분으로 국가가 시민의 정보와 정보활동을 감시하는 것은 아닐까 하는 일각의 우려를 해소시킬 수 있는 좋은 방법이다.

이와 같은 위원회는 정보보호를 위한 기본계획 및 시행계획의 수립·시행에 관한 사항, 기본계획 및 시행계획의 종합·조정에 관한 사항, 기본계획 및 시행계획의 추진 실적 점검에 관한 사항, 정보보호와 관련된 제도의 개선에 관한 사항 등을 심의하도록 한다. 그리고 위원회의 효율적인 운영을 위하여 위원회에 공공분야와 민간분야를 각각 담당하는 실무위원회를 반드시 두도록 하고, 필요한 경우 법령에 근거하여 5개 내외의 실무위원회를 둘 수 있도록 하는 것이 타당하다. 아래에서 제안하는 융합정책 실무위원회가 그 하나의 예가 될 수 있을 것이다.

2. 융합보안정책 협의를 위한 실무위원회 마련

이미 설명한 것처럼 융합제품과 서비스는 기존에는 과학기술정보통신부가 아니라 다른 부처의 권한 범위 내에 있는 대상들이었다. 따라서 이들 제품과 서비스를 정보보안의 관점에서 과학기술정보통신부가 규율하기 위해서는 국토교통부, 산업자원부 등 관련부처와 협업이 필요하다. 이러한 협업과 이를 위한 활발한 의사소통을 위하여 협의체를 신설하여 운영할 필요가 있다.

이 협의체의 목적은 융합제품과 서비스의 정보보호에 관하여 관계 중앙행정기관과의 협력이 필요한 사항을 협의·조정하기 위한 것이다. 부처 정책 조정권은 원래 국무총리 권한이므로 이러한 협의체는 국무총리 소속으로 두고 그 위원장은 국무조정실의 차관급 공무원으로서 국무총리가 지명하는 자로 하고, 위원은 대통령령으로 정하는 중앙행정기관의 고위공무원단에 속하는 공무원으로 하는 것이 타당하다. 이 협의체의 간사는 과학기술정보통신부장관

소속 고위공무원이 하도록 한다. 만약 정보보안에 있어서 (가칭) 정보보안위원회 같은 새로운 추진체계가 신설된다면 이 협의체는 그 위원회의 실무위원회 중 하나로 두는 것이 타당하다.

그리고 스마트 시티와 같이 그 규모가 크고 추진주체가 다양한 융합서비스 등은 협업하고 활발한 의사소통을 위하여 자체 법령에서 별도의 협의체를 신설하여 운영할 수도 있다. 실무위원회가 이 경우까지 다룰 필요는 없다. 따라서 이를 소관 사무에서 제외하는 것이 타당하다.

Ⅴ. 결론

이상의 논의를 정리하면 다음과 같다.

첫째, 융합제품과 서비스가 급격히 늘어나면서 그 침해사고에 대한 우려도 함께 커지고 있다. 그러나 융합제품과 서비스를 제조·수입·제공하는 자에게 정보보호의 관점에서 어떤 의무 부과를 하고 있는지 명확하지 않다. 현행과 같이 과학기술정보통신부장관이 정보보호 지침을 준수하도록 권고하는 것만으로는 충분하지 않다. 자율주행자동차나 드론과 같이 생명·신체, 사생활 및 재산상 피해를 야기할 우려가 상대적으로 높은 융합제품과 서비스 제공자에게는 지침 준수의 의무화가 필요하다. 또한, 정보보호지침의 준수와 이행 실태 조사 또는 점검 근거 규정을 신설하고 정당한 사유가 없는 한 조사 또는 점검에 응하도록 하는 의무 규정 신설을 권고하였다. 이러한 의무 부과는 융합제품이나 융합서비스를 이용하는 일반 시민의 정보보안권 증진에 기여할 것이다.

둘째, 융합제품과 서비스 이용자가 침해사고를 걱정하지 않고 안전하게 사용할 수 있도록 임의적인 인증제도를 도입할 것을 권고하고, 인증주체는 민간 주도의 사업자단체 또는 정보보호 관련 기관·단체에서 자율인증제도를 실시할 수 있도록 할 것을 제안하였다.

셋째, 현행 망법은 침해사고 발생 시 원인분석과 조사를 위한 업무 근거가 없어 침해사고 발생에 대응하기 위한 업무 수행을 위하여 현장에 나가도 적절한 원인분석과 조사를 할 수 없는 문제가 있다. 따라서 이와 같은 업무를 할 수 있는 명시적 근거 신설을 권고하였다. 그리고 융합서비스 제공자등을 포함한 침해사고를 신고한 사업자에게 이용자 피해예방조치 안내와 공개조치를 하도록 권고하였다.

넷째, 현행 망법은 침해사고가 발생하면 즉시 그 사실을 과학기술정보통신부장관이나 한국인터넷진흥원에 신고하도록 규정하고 있으며, 침해사고의 원인을 분석하고 피해의 확산을 방지하도록 규정하고 있다. 융합제품과 서비스 제공자가 이에 속하는지 불분명하다. 융합제품과 서비스에 침해사고가 발생하면 이를 신고를 하도록 하며, 침해사고가 발생하면 침해사고의 원인을 분석하고 피해의 확산을 방지하여야 하여야 한다. 따라서 그 대상자에 융합제품과 서비스 제공자를 명시하도록 권고하였다.

기고

다섯째, 현행 정보보안법제에서는 「정보통신 진흥 및 융합 활성화 등에 관한 특별법」에서 정보보호 정책의 수립과 조정 역할을 하는 정보통신전략위원회, 「정보통신기반보호법」에서는 정보통신기반보호위원회를 두고 있다. 그런데 정보통신전략위원회는 정보보호 정책의 수립과 조정에 제 역할을 하지 못하고 있다. 「정보통신기반 보호법」의 정보통신기반보호위원회는 이 법이 정보보안 전반을 규율하는 법이 아니어서 정보보안 전반을 아우르지 못하는 추진체계라는 한계가 있다. 따라서 정보보안 전반을 아우르는 추진체계를 새롭게 구축할 것을 제안하였다. 한편, 융합제품과 서비스 규율은 과학기술정보통신부가 아니라 국토교통부, 산업자원부의 권한이다. 그런데 이 제품과 서비스에 대한 침해사고 예방과 대응은 국토교통부, 산업자원부 등 관련부처와 과학기술정보통신부의 협업이 필요하다. 이러한 협업과 이를 위한 활발한 의사소통을 위해서도 새로운 정보보호 추진체계가 필요하다. 따라서 현행 정보통신기반보호위원회를 정보보안위원회로 확대·개편할 것을 권고하였다. 그리고 여러 부처의 협업과 이를 위한 활발한 의사소통을 위하여 협의체를 신설하여 운영할 필요가 있다. 새로운 추진체계가 신설된다면 이 협의체는 그 위원회의 실무위원회의 하나로 두는 것이 타당하다.

이 글은 당장 현실화된 자율주행자동차, 드론, 로봇 완구 등과 같이 당장 시장에서 문제가 되고 있는 융합제품과 서비스가 야기하는 침해사고의 예방과 대응에 단기적으로 대처하기 위하여 세부 쟁점을 추출하고 그에 대한 대안을 제시하다보니, 스마트 시티, 스마트 공장과 같이 당장 시장에서 문제가 되고 있지 않은 융합제품과 서비스가 야기하는 정보보안 문제에 대해서는 본격적인 논의를 하지 못하였다. 그리고 「정보통신기반보호법」의 개정, 통합 정보보안법의 제정과 같은 중장기적인 대처에 대해서도 논의를 하지 못하였다. 의욕에 찬 연구자에게 주어진 앞으로 연구 과제이다.

※ **Reference**

1. 국가정보원 외, 「2018 국가정보보호백서」, 국가정보원 등, 2018.
2. 매일경제, "인터넷진흥원, 15일 조직개편...융합보안 대응 조직 신설", 2019년 2월 7일 인터넷 기사.
3. 전광석, 「한국헌법론」, 집현재, 2018.
4. 정필운, 김형준, "제4차 산업혁명 시대 개인 정보보안 방안", 「사이버안보법정책논집」 2018년 제3호, 2018.

인터넷 법제동향
Vol. 140 (May 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