정 보 보 호 학 회 지
제27권 제5호, 2017. 10

중국 핵심 정보 인프라 시설 보호 동향

정 태 인*, 김 주 영**, 김 원***

요 약

핵심 정보 인프라 시설(关键信息基础设施)은 서비스가 중단될 경우, 사회에 막대한 영향을 초래하는 시설을 의미한다. 중국은 <네트워크 안전법(中华人民共和国网络安全法)>을 시행하여, 핵심 정보 인프라 시설 보호를 강화하고 있다. 본 고에서는 관련 해당 법령들의 주요 내용을 소개하고, 그 의미를 고찰하고자 한다.

Ⅰ. 서 론

인터넷의 급속한 발전과 스마트폰의 보급에 따라, 중국에서 스마트폰을 통해 금융 거래, 메신저, 공유 차량 예약 등을 이용하는 것은 이미 생활의 일부가 되었다. 따라서 이러한 서비스가 갑자기 중단된다면, 커다란 불편을 초래할 뿐만 아니라, 심각한 사회 혼란과 막대한 경제적 손실이 발생할 것으로 예상된다. 이러한 상황을 예방하기 위하여 중국은 핵심 정보 인프라 시설(关键信息基础设施)에 대한 보호를 강화하고 있다.

한국은 통신기반시설을 보호하기 위하여, <정보통신기반 보호법>을 제정 및 시행하고 있으나, 중국은 이와 달리 2017년 6월 시행된 <네트워크 안전법(中华人民共和国网络安全法), 이하 "안전법">에 해당 내용을 포함하고 있다. 안전법이 2016년 11월 제정된 이후, 핵심 정보 인프라 시설에 관련된 하위 법령, 표준들이 지속적으로 제정되어 의견 수렴 과정을 거치고 있다.

본 고에서는 네트워크 안전법 중 핵심 정보 인프라 시설에 중점을 두어서, 법률 및 관련 하위 법령들을 소개하고, 주요 내용을 분석하려고 한다.

Ⅱ. 핵심 정보 인프라 시설 관련 법률

2.1. 관련 법령

안전법 제정 이후, <개인정보와 중요 데이터 국외 반출 안전 평가 방법(의견 수렴안)>[1], <네트워크 제품과 서비스 안전 심사 방법(시행)>[2], <정보 안전 기술, 데이터 국외 반출 안전 평가 지침>[3], <네트워크 핵심 설비와 네트워크 안전 전용 제품 목록(1차)>[4], <핵심 정보 인프라 시설 안전 보호 조례(의견 수렴안)>[5]이 지속적으로 발표되었다. 관련 법령 목록은 [표 1]과 같다.

특이한 점은 한국의 법령 명명 체계와 방식이 상이하다는 점이다. 한국에서는 일반적으로 법, 시행령, 시행규칙/고시 등이 동일한 이름을 사용한다. 예를 들어, <정보통신기반 보호법>, <정보통신기반 보호법 시행령>, <정보통신기반 보호법 시행규칙> 등으로 명명하고, 상위 법령에서 "상세한 사항은 하위 법령에서 정한다"라고 명시하여 법령간의 계층 구조가 비교적 분명한 편이다. 그러나 중국 법령은 비록 본문에서 상위 법령을 명시하고 있지만, 이름만으로는 관련성을 확인하기 어렵다는 특징을 가진다. [표 2]는 관련 법령과 안전법과의 관계를 보여 준다.

관련 법령을 간략히 설명하면 다음과 같다. <네트워크 핵심 설비와 네트워크 안전 전용 제품 목록>은 안전법 제23조의 네트워크 핵심 설비 및 네트워크 안전 전용 제품에 대해서 규정하고 있다. 네트워크 핵심 설비와 네트워크 안전 전용 제품은 안전 인증 합격 또는 안전 검측 기준에 부합하여야, 중국 내에서 판매 또는 제공이 가능하다. 본 목록은 1차로 공개한 것으로, 네트워크 핵심 설비 4종, 네트워크 안전 전용 제품 11종 및 각각의 구체적인 규격을 명시하고 있다. 예를 들어 라우터 장비는 처리량이 12Tbps 이상, 라우팅 테이블이 55만 라인 이상인 제품으로 규정하고 있다. <핵심 정보 인프라 시설 안전 보

한국인터넷진흥원 (tijung@kisa.or.kr, kjy@kisa.or.kr, wkim1015@kisa.or.kr)

〔표 1〕 안전법 및 관련 법령 목록

제정 일자	이름(국문)	이름(중문)	성격	제정 주체
2016.11. 7.	네트워크 안전법	中華人民共和國网絡安全法	법률	전국인민대표대회
2017. 4.11.	개인정보와 중요 데이터 국외 반출 안전 평가 방법(의견 수렴안)	个人信息和重要數据出境安全評估辦法 (征求意見稿)	부문규장	국가 인터넷 정보 판공실
2017. 5. 2.	네트워크 제품과 서비스 안전 심사 방법(시행)	网絡産品和服務安全審查辦法 (試行)	부문규장	국가 인터넷 정보 판공실
2017. 5.27.	정보 안전 기술, 데이터 국외 반출 안전 평가 지침	信息安全技術數据出境安全評估指南	추천성 국가 표준(GB/T)	전국정보안전 표준화기술위원회
2017. 6. 1.	네트워크 핵심 설비와 네트워크 안전 전용 제품 목록(1차)	网絡關鍵設備和网絡安全專用産品目彔 (第一批)	참고 자료	국가 인터넷 정보 판공실
2017. 7.10.	핵심 정보 인프라 시설 안전 보호 조례(의견 수렴안)	關鍵信息基础設施安全保護條例 (征求意見稿)	부문규장	국가 인터넷 정보 판공실

〔표 2〕 관련 법령과 안전법과의 관계

성격	키워드(법 조항)			
	안전 인증, 안전 검측 (제23조)	핵심 정보 인프라 시설(제31조)	안전 심사(제35조)	안전 평가(제37조)
부문 규장		핵심 정보 인프라 시설 안전 보호 조례	네트워크 제품과 서비스 안전 심사 방법	개인정보와 중요 데이터 국외 반출 안전 평가 방법
표준				정보 안전 기술, 데이터 국외 반출 안전 평가 지침
기타	네트워크 핵심 설비와 네트워크 안전 전용 제품 목록			

호 조례>는 안전법 제31조의 핵심 정보 시설 인프라에 대해서 규정하고 있다. 향후 이 규정에 근거하여 <핵심 정보 인프라 시설 식별 지침>을 개발하고, 해당 부처에서 핵심 정보 인프라 시설 지정이 진행될 것으로 생각된다. <네트워크 제품과 서비스 안전 심사 방법>은 안전법 제35조의 안전 심사에 대해서 규정하고 있다. 안전 심사 대상은 핵심 정보 인프라 시설 사업자가 사용하는 네트워크 제품 및 서비스이다. 즉, 핵심 정보 인프라 시설 사업자는 안전 심사에 통과한 제품 및 서비스만을 구매하여 사용할 수 있다. <개인정보와 중요 데이터 국외 반출 안전 평가 방법>, <정보 보안 기술, 데이터 국외 반출 안전 평가 지침>은 안전법 제37조의 안전 평가에 대해서 규정하고 있다. 이는 개인정보와 중요 데이터를 국외 반출하는 경우, 필요한 안전 평가에 대한 것이다. 특이한 점은 <정보 보안 기술, 데이터 국외 반출 안전 평가 지침>은 중국의 추천성 국가표준인 GB/T의 형식이라는 것이다. 2건의 방법에 대해서는 이전 논문 〔6〕 에서 설명한 적이 있으므로, 본 고에서는 조례, 지침, 목록에 대해서 주요 내용을 설명하겠다.

2.2. 주요 용어 정의

본 고에서 중점을 두어 설명하려는 핵심 정보 인프라 시설은 한국의 정보통신기반시설, ENISA의 CII(Critical Information Infrastructure) 〔7〕 와 유사한 개념으로 생각된다. 이외 몇 가지 주요 용어는 [표 3]과 같다.

안전 인증(安全认证), 안전 검측(安全检测)은 네트워크 핵심 설비와 네트워크 안전 전용 제품에 대한 인증, 검측을 의미한다. 이는 일반적인 의미의 제품 인증과 제품 테스트로 생각된다. 인증, 검측 모두 관련 기준이 있고, 이에 근거하여 기준을 모두 만족하면, 인증 합격, 검측 통과 여부가 결정된다. 안전 심사(安全审查)는 핵심 정보 인프라 시설 사업자가 사용하는 네트워크 제품 및 서비스를 대상으로 하며, 핵심 정보 인프라 시설은 안전 심사에 통과한 제품 및 서비스만 구매하여 사용할 수 있다. 즉, 핵심 정보 인프라 시설에 해당 제품, 서비스를 판매하기 위해서는 반드시 통과하여야 하는 심사다. 안전 평가(安全评估)는 개인정보와 중요 데이터를 보유한 사업자가 해당 정보, 데이터를 국외 반출 시, 수행하는 평가를 의미한다.

〔표 3〕 주요 용어

용어	대상	설명
안전 인증, 안전 검측	네트워크 핵심 설비와 네트워크 안전 전용 제품	중국 내에서 판매를 위한 필수 사항으로, 기존 제품 인증/검측 제도를 활용할 것으로 예상
안전 심사	핵심 정보 인프라 시설 사업자가 사용하는 네트워크 제품 및 서비스	일반 기업/사용자와는 무관
안전 평가	개인정보와 중요 데이터를 보유한 사업자	국외 반출 시, 사업자가 자기 평가로 수행

기본적으로 사업자는 자기 평가를 수행하고, 이에 근거하여 국외 반출 여부를 결정하게 된다.

Ⅲ. 핵심 정보 인프라 시설 안전 보호 조례

3.1. 개요

해당 조례는 2017년 7월, 국가 인터넷 정보 판공실(国家互联网信息办公室)에서 공고하였다. 조례는 8장, 55조로 구성되었으며, 안전법의 제31조에서 제39조까지를 보충하여 상세 내용을 규정하고 있다. 목적은 "중국에서 핵심 정보 인프라 시설을 계획, 구축, 운영, 유지, 사용하고 핵심 정보 인프라 시설 안전 보호를 진행"하는 것이다. 향후 <핵심 정보 인프라 시설 식별 지침(关键信息基础设施识别指南)>을 추가 제정하고, 이에 근거하여 각 부처가 핵심 정보 인프라 시설 식별을 진행하고, 식별 결과를 보고하도록 요구하고 있다.

3.2. 주요 내용

3.2.1. 적용 대상(제2조)

- 중화인민공화국 경내에서 핵심 정보 인프라 시설을 계획, 구축, 운영, 유지, 사용하고 핵심 정보 인프라 시설의 안전 보호를 진행하는데 본 조례를 적용

3.2.2. 집행 주체(제4조)

- 정부의 산업 주무 부처 혹은 감독 관리 기관은 국무원이 규정한 직책 분업에 따라 해당 산업, 해당 분야의 핵심 정보 인프라 시설의 안전 보호 업무에 대한 지도와 감독을 책임짐
- 국가 인터넷 통신 부처는 핵심 정보 인프라 시설의 안전 보호 업무와 관련 감독 관리 업무에 대한 통합 조율을 책임짐
- 현급(县级) 이상 지방 인민 정부의 유관 기관은 국가의 유관 규정에 따라 핵심 정보 인프라 시설의 안전 보호 업무를 진행

3.2.3. 핵심 정보 인프라 시설 운영자의 의무(제5조)

- 핵심 정보 인프라 시설의 운영자는 본 기관의 핵심 정보 인프라 시설 보안에 대하여 책임을 지고 네트워크 안전 보호 의무를 이행

3.2.4. 정부 지원(제9조)

- 정부는 산업, 세금, 금융, 인재 등 정책을 제정하고 핵심 정보 인프라 시설 보안 관련 기술, 제품, 서비스 혁신을 지원하며 안전하고 믿을 수 있는 네트워크 상품과 서비스를 널리 보급하고 네트워크 보안 인력을 양성 및 선발

3.2.5. 에너지, 통신, 교통 업계 지원(제14조)

- 에너지, 통신, 교통 등 업계는 핵심 정보 인프라 시설의 네트워크 보안 사태 비상 대처 및 네트워크 기능 회복을 위해 전력 공급, 네트워크 통신, 교통 운수 등 분야의 중점 보장과 지원을 제공

3.2.6. 범죄 활동 수사(제15조)

- 공안 기관 등 부처는 법에 의해 핵심 정보 인프라 시설을 이용하는 범법 범죄 활동을 수사하고 단속

3.2.7. 핵심 정보 인프라 시설에 대한 위해 활동 금지(제16조)

- 어떠한 개인과 조직도 핵심 정보 인프라 시설을 해치는 활동과 행위를 해서는 안됨

3.2.8 핵심 정보 인프라 시설 범위(제18조)

- 해당 기관이 운행 및 관리하는 네트워크 시설과 정보 시스템이 일단 파괴당하고 기능을 상실하거나 혹은 데이터가 유출되면 국가 안보, 국가 경제와 국민 생활, 공공 이익을 심각하게 위협하므로, 핵심 정보 인프라 시설 보호 범위에 포함
  - 정부기관과 에너지, 금융, 교통, 수리, 위생의료, 교육, 사회보험, 환경보호, 공공사업 등 업계의 분야와 기관
  - 전신망, 방송망, 인터넷망 등 정보 네트워크 및 클라우드 컴퓨팅, 빅데이터와 기타 대형 공공정보 네트워크 서비스를 제공하는 기관
  - 국방 기술공업, 대형 장비, 화학공업, 식품약품 등 분야의 연구 생산 기관
  - 라디오 방송국, TV방송국, 통신사 등 언론기관
  - 기타 중점 기관

3.2.9. 핵심 정보 인프라 시설 식별 지침 수립 및 식별 (제19조)

- 국가 네트워크 통신기관은 국무원 통신 주무 부처, 공안 기관 등 부처와 함께 <핵심 정보 인프라 시설 식별 지침(关键信息基础设施识别指南)>을 수립
- 국가 산업 주무 부처 혹은 감독 관리 기관은 핵심 정보 인프라 시설 식별 지침에 따라 해당 업계, 해당 분야의 핵심 정보 인프라 시설을 구성 식별하고 절차에 따라 식별 결과를 보고

3.2.10. 안전 보호 의무(제23조)

- 운영자는 네트워크 보안 등급 보호 제도의 기준에 따라 안전 보호 의무를 이행하고 핵심 정보 인프라 시설이 교란, 파괴당하지 않거나 혹은 인가받지 않은 방문을 차단하도록 보장하고 네트워크 데이터의 유출 혹은 도난, 무단 수정을 방지

3.2.11. 네트워크 핵심 장비, 네트워크 보안 전용 상품 (제30조)

- 운영자가 구매, 사용하는 네트워크 핵심 장비, 네트워크 보안 전용 상품은 법률, 행정 법규의 규정과 관련 국가표준의 강제성 기준에 부합해야 함

3.2.12. 네트워크 보안 모니터링 사전 경보 및 정보 통보 제도(제37조)

- 국가의 산업 주무 부처 혹은 감독 관리기간은 해당 업계, 해당 분야의 핵심 정보 인프라 시설 네트워크 보안 모니터링 사전 경보 및 정보 통보 제도를 구축
- 즉시 해당 업계, 해당 분야의 핵심 정보 인프라 시설 운행 현황과 보안 리스크를 파악하고 유관 운영자에게 보안 리스크와 관련 업무 정보를 통보

3.2.13. 운영자 처벌(제45조)

- 운영자가 네트워크 안전 보호 의무를 이행하지 않는 경우, 유관 주무 부처는 시정 명령을 내리고 경고 조치를 취함
- 시정 명령을 거부하고 시정하지 않는 경우, 10만 위안 이상 100만 위안 이하의 벌금을 부과하며, 직접적인 책임자는 1만 위안 이상 10만 위안 이하의 벌금을 부과

3.2.14 운영자 처벌(제46조)

- 운영자가 해외에 네트워크 데이터를 저장하거나 제공하는 경우, 유관 주무 부처는 시정 명령을 내리고 경고 조치를 취함
- 불법 소득을 몰수하고, 5만 위안 이상 50만 위안 이하의 벌금을 부과. 관련 업무 일시 중단, 영업 정지, 정리정돈, 사이트 폐쇄, 관련 업무 허가증 말소 등 명령
- 직접적인 책임자 등에게는 1만 위안 이상 10만 위안 이하의 벌금을 부과

3.2.15 운영자 처벌(제47조)

- 운영자가 보안 심사를 통과하지 못한 네트워크 상품 또는 서비스를 사용하는 경우, 유관 주무 부처는 사용 중단 명령을 내리고, 구매 금액의 1배 이상 10배 이하의 벌금을 부과
- 직접적인 책임자 등에게는 1만 위안 이상 10만 위안 이하의 벌금을 부과

3.2.16 공격자 처벌(제48조)

- (개인) 제16조의 규정을 위반했지만 범죄가 구성되지 않을 경우, 불법 소득을 몰수하고, 5일 이하 구속, 5만 위안 이상 50만 위안 이하의 벌금을 부과
- (개인) 경위가 심각한 경우, 5일 이상 15일 이하 구속, 10만 위안 이상 100만 위안 이하의 벌금을 부과
- (기관) 위반 행위를 한 경우, 불법 소득을 몰수하고, 10만 위안 이상 100만 위안 이하의 벌금을 부과하며, 직접적인 책임자에게도 벌금 부과

3.2.17. 공격자 처벌(제52조)

- 해외 기관, 조직, 개인이 중국 핵심 정보 인프라 시설을 공격, 침해, 교란, 파괴 등 활동을 하여 심각한 결과를 초래한 경우, 법적 책임을 추궁
- 국무원의 공안 기관, 국가 안보기관 등은 재산 동결 혹은 필요한 제재 조치

Ⅳ. 정보 안전 기술, 데이터 국외 반출 안전 평가 지침

4.1. 개요

해당 지침은 2017년 5월, 중국 전국정보안전표준화기술위원회(全国信息安全标准化技术委员会)〔8〕에서 발표하여, 표준화 절차를 진행 중이다. 지침은 본문, 별첨A(중요 데이터 식별 지침), 별첨B(개인정보와 중요 데이터의 국외 반출 보안 리스크 평가 방법)로 구성되어 있다.

지침은 안전법 제37조, <개인정보와 중요 데이터 국외 반출 안전 평가 방법> 제2조를 보충하여 상세 내용을 규정하고 있다. 법과 방법은 주체에 대해서 상충되게 규정하고 있는데, 지침은 방법을 준용하고 있다. 즉 지침은 "네트워크 사업자가 진행하는 개인정보와 중요 데이터의 국외 반출 안전 평가 업무에 적용한다"고 명시하고 있다.

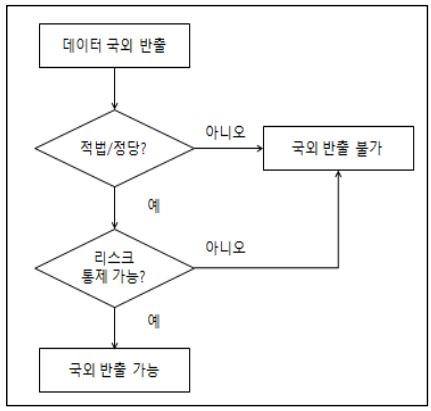
- <네트워크 안전법 제37조> 핵심 정보 인프라 시설 사업자(关键信息基础设施的运营者)는 중화인민공화국 경내에서 운영 중 수집하고 생성한 개인정보와 중요 데이터를 반드시 경내에 저장하여야 한다. 업무의 필요에 의해 반드시 해외에서 저장 또는 해외 기관 또는 개인에게 제공해야 할 경우, 국가 네트워크 정보 부문이 국무원의 유관 부문과 함께 제정한 방법에 따라 안전 평가(安全评估)를 진행하여야 한다. 법률, 행정 법규에 별도의 규정이 있을 경우, 해당 규정을 따른다.
- <개인정보와 중요 데이터 국외 반출 안전 평가 방법 제2조> 네트워크 사업자(网络运营者)는 중화인민공화국 경내에서 수집하거나 생산한 개인정보와 중요 데이터를 경내에 저장해야 한다. 업무의 필요로 인해 경외에 제공할 필요가 있을 시에는 본 방법에 따라 안전 평가(安全评估)를 진행해야 한다.

지침은 추천성 국가 표준(GB/T)으로, 강제성은 없지만, 법·방법 시행을 위한 구체적인 내용을 규정하고 있어, 참고 자료(guideline)의 역할을 할 것으로 생각된다. 중국의 국가 표준은 강제성 국가 표준(GB), 추천성 국가 표준(GB/T), 국가 표준 기술 문서(GB/Z) 등으로 구분된다.[9]

4.2. 주요 내용

지침은 일반적인 표준 문서 양식을 따르고 있으며, 용어 정의, 평가 절차, 평가 요점 등을 규정하고 있다. 용어 정의에서는 개인정보, 주요 데이터 등 10개 용어를 규정하고 있으며, 데이터에서 민감한 개인정보를 제거하는 민감성 제거(data desensitization)도 포함하고 있다.

평가 절차는 [그림 1]과 같으며, 자체 평가, 데이터 국외 반출 계획 수립, 적법성 및 리스크 통제 가능 평가, 평가 보고서 작성, 검사/수정 등으로 구성된다. 네트워크 사업자가 자체 평가를 진행하여 국외 반출 여부를 결정하도록 규정하고 있다. 만약 자체 평가 결과, 보안 리스크가



〔그림 1〕 평가 절차

상위 2단계(아주 높음, 높음)에 해당되면, 반출해서는 안 된다.

별첨A는 중요 데이터 식별 지침으로, 석유, 석탄, 전력, 통신, 금융 등 28개 업종 별로 주무 부처, 중요 데이터에 대하여 규정하고 있다. 주요 내용은 [표 4]와 같다.

별첨B는 개인정보와 중요 데이터의 국외 반출 보안 리스크 평가 방법이다. 보안 리스크는 영향 등급과 보안 사건 가능성 등급을 각각 구하고, 이를 매트릭스에 대입해서 4단계 등급을 계산한다. 보안 리스크는 낮음, 중간, 높음, 아주 높음의 4단계이다. 영향 등급은 각기 개인정보, 중요 데이터로 구분하여 수량, 범위, 기술 처리 현황 등에 따라 가감하여 결정한다. 기본적으로 개인 정보의 영향 등급은 1에서 3이며, 중요 정보는 4에 해당한다. 보안 사건 가능성은 발송인의 보안 보장 능력, 수신인의 보안 보장 능력, 수신 국가의 정치 법률 환경 등을 고려하여 고, 중, 저 3단계로 판단한다. 최종적인 보안 리스크 평가 방법은 [표 5]과 같다.

〔표 4〕 28개 업종 및 주무 부처

분야	주무 부처
A.1. 석유/천연가스	국가발전개혁위원회, 에너지국
A2. 석탄	국가발전개혁위원회, 에너지국
A.3. 석유화학	에너지국
A.4. 전력	국가발전개혁위원회, 에너지국
A.5. 통신	공업정보화부
A.6. 전자정보	공업정보화부
A.7. 철강	공업정보화부
A.8. 비철금속	공업정보화부
A.9. 장비 제조	공업정보화부
A.10. 화학공업	공업정보화부
A.11. 국방군수공업	국방과학 기술공업국
A.12. 기타 공업	공업정보화부
A.13. 지리 정보	국토자원부
A.14. 민용 핵시설	국방과학 기술공업에너지국
A.15. 교통 운수	국가교통전시대비판공실, 교통운수부, 국가철도국, 중국철도총공사
A.16. 우체국 택배	우체국
A.17. 수리(水利)	수리부
A.18. 인구 건강	위생계획생육위원회
A.19. 금융	중국인민은행
A.20. 신용 조회	중국인민은행
A.21. 식품약품	식품약품감독관리총국
A.22. 통계	통계국
A.23. 기상	기상국
A.24. 환경 보호	환경보호부
A.25. 방송	국가신문출판광전총국
A.26. 해양 환경	국가해양국
A.27. 전자상거래	상무부
A.28. 기타	

〔표 5〕 보안 리스크 등급 판정 참고표

	보안 사건 가능성 등급		
영향 정도 등급	1	2	3
≥ 5	높음	아주 높음	아주 높음
4	중간	높음	높음
3	낮음	중간	높음
2	낮음	중간	중간
1	낮음	낮음	중간

Ⅴ. 네트워크 핵심 설비와 네트워크 안전 전용 제품 목록

5.1. 개요 및 주요 내용

해당 목록은 2017년 6월 국가 인터넷 정보 판공실에서 1차로 공고한 것이다. 향후 추가적인 목록이 발표될 것으로 예상된다. 목록은 안전법 제23조에서 규정하고 있는 목록에 해당하는 것으로, 부문규장 등의 공식적인 법령은 아니고 참고 자료의 성격을 가진다. 따라서 목록의 제정, 개정은 비교적 용이할 것으로 예상되며, 필요에 따라서 국가 인터넷 정보 판공실에서 관리할 것으로 추정된다. 다만 인증, 검측을 위해서는 기준이 필요하기 때문에, 기준이 마련되기 전까지는 실질적인 인증, 검측은 어려울 것이다. 또한 목록에 해당하는 제품군 중, 인증 합격 또는 안전 검측 기준 부합된 구체적인 제품 목록도 소비자의 편의를 위해서 추가로 공개될 가능성이 높다.

- <네트워크 안전법 제23조> 네트워크 핵심 설비와 네트워크 보안 전용 제품은 국가표준, 업계표준의 강제성 기준에 따라 자격이 있는 기관의 안전 인증에 합격(安全认证合格) 또는 안전 검측(安全检测) 기준에 부합된 후에야 판매 또는 제공이 가능하다. 국가 네트워크 정보 부문은 국무원의 유관 부문과 함께 네트워크 핵심 설비와 네트워크 안전 전용 제품의 목록을 제정 및 발표하고 안전 인증과 안전 검측 결과의 상호 인증을 추진하여 중복 인증 및 검사를 방지한다.

이미 중국에는 강제성 인증 제도로, CCC, ISCCC 등의 제도를 운영하고 있다. 따라서 본 목록에 해당하는 제품군의 경우, 별도의 제도를 신설하는 것보다는, 기존 인증, 검측 제도를 활용할 가능성이 높다.

목록은 네트워크 핵심 설비 4종과 네트워크 보안 전용 제품 11종을 규정하고 있으며, 각 유형별로 규격을 명시하고 있다. 상세한 내용은 [표 6]과 같다.

〔표 6〕 1차 목록

	설비/제품 유형	범위
네트워크 핵심 설비	1.라우터	전 시스템 처리량(양방향)≥12Tbps
		전 시스템 라우터 테이블 용량≥55만줄
	2.스위치	전 시스템 처리량(양방향)≥30Tbps
		전 시스템 패킷 포워딩률≥10Gpps
	3.서버 (랙장착형)	CPU 수량≥8개
		단일 CPU 커널 수≥14개
		메모리 용량≥256GB
	4. 프로그램 가능 논리 제어 장치(PLC설비)	제어기 명령 집행 시간≤0.08μs
네트워크 보안 전용 제품	5. 데이터 백업 복합기	백업 용량≥20T
		백업 속도≥60MB/s
		백업 시간 간격≤1시간
	6. 방화벽 (하드웨어)	완제품 처리량≥80Gbps
		최대 동시 발송 연결 수≥300만
		초당 신규 연결 수≥25만
	7. WEB 응용방화벽 (WAF)	완제품 응용 처리량≥6Gbps
		최대 HTTP 동시 발송 연결 수≥200만
	8. 침입탐지시스템 (IDS)	전체검사 속도≥15Gbps
		최대 동시 발송 연결 수≥500만
	9.침입방지시스템 (IPS)	전체검사 속도≥20Gbps
		최대 동시 발송 연결 수≥500만
	10.보안격리 및 정보스위치제품 (게이트키퍼)	처리량≥1Gbps
		시스템 지연시간≤5ms
	11.스팸메일 방지제품	연결 처리 속도(연결/초)〉100
		평균 지연 시간〈100ms
	12.네트워크 종합 검사시스템	패킷 스니퍼 속도≥5Gbps
		사건 기록 능력≥5만줄/초
	13.네트워크 취약성 스캔 제품	최대 병행 스캔 IP 수량≥60개
	14. 보안 데이터베이스 시스템	TPC-E tpsE(초당 교역 가능 수량)≥4500개
	15. 웹사이트 복구 제품(하드웨어)	회복 시간≤2ms
		사이트의 최장 경로≥10급

Ⅵ. 고 찰

6.1. 핵심 정보 인프라 시설의 한중 비교

핵심 정보 인프라 시설에 대한 법적 정의를 비교하면 다음과 같다. 관련 법률, 지정 주체, 의무, 처벌 등에 대한 비교는 [표 7]과 같다.

- <정보통신기반 보호법 제2조> "정보통신기반시설"이라 함은 국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 전자적 제어·관리시스템 및 <정보통신망 이용촉진 및 정보보호 등에 관한 법률> 제2조제1항제1호의 규정에 의한 정보통신망을 말한다.
- <네트워크 안전법 제31조> 국가는 공공통신과 정보서비스・에너지・교통・수리・금융・공공서비스・전자정부 등 중요 산업과 영역, 그리고 기타 영역에서 일단 파괴・기능 상실・데이터 유출이 발생하면 국가안전, 국가 경제, 국민 생활, 공공이익에 중대한 손상을 줄 수 있는 핵심 정보 인프라 시설에 대하여, 네트워크 안전 등급 보호 제도에 기초하여, 중점 보호를 실행한다. 핵심 정보 인프라 시설의 구체적인 범위와 안전 보호 방법은 국무원이 제정한다.

지정 및 보호 취지 등은 대부분 유사하지만, 의무, 처벌 등에서는 다른 부분이 많다. 예를 들어, 한국과 달리 중국은 핵심 정보 인프라 시설 운영자에게 보다 많은 의무를 부과하고 있고, 특히 위법 시 처벌 조항이 한국에 비해 중하다. 또한 영업 정지나 업무 허가증 말소까지 가능하기 때문에, 강력한 법 집행이 가능할 것으로 생각된다.

6.2. 안전 심사 및 안전 검측/인증의 차이점

안전 심사는 핵심 정보 인프라 시설에서 사용하는 네트워크 제품 및 서비스가 반드시 통과하여야 하는 심사다. 안전 심사를 통과하지 않은 제품 및 서비스를 사용하는 경우, 운영자는 처벌을 받는다. 그렇다면 안전 심사와 안전 검측/인증은 어떠한 차이점이 있는 것일까?

기본적으로 안전 심사는 핵심 정보 인프라 시설에 사용하는 제품 및 서비스가 대상이기 때문에, 안정 검측, 인

증에 비해서 보안성을 중시할 것으로 생각된다. 해당되는 안전법 조항은 다음과 같다.

- <네트워크 안전법 제35조> 핵심 정보 인프라 시설 사업자의 네트워크 제품 또는 서비스 구매가 국가 안보에 영향을 줄 수 있을 경우, 국가 네트워크 정보 부문이 국무원의 관련 부문과 함께 구성한 국가 안전 심사(安全审查)에 통과하여야 한다.

안전 심사는 핵심 정보 인프라 시설에서 사용하는 네트워크 제품 및 서비스에 대한 요구 사항이기 때문에, 일반적인 제품이나 서비스에 비해서 강화된 기준이 적용될 것으로 생각된다. <네트워크 제품과 서비스 안전 심사 방법>에서는 안전 심사 내용을 다음과 같이 규정하고 있다.

- <네트워크 제품과 서비스 안전 심사 방법 제4조> 네트워크 제품과 서비스의 보안성, 통제 가능성을 중점적으로 심사한다. 주로 다음의 내용을 심사한다.
  - 제품과 서비스 자체의 보안 위험 그리고 불법적으로 통제, 간섭 및 운영 중단될 위험
  - 제품과 핵심 부품의 생산, 테스트, 인도, 기술 지원 과정에서의 공급 사슬 보안 위험
  - 제품과 서비스 공급업자가 제품과 서비스를 제공하는 편의 조건을 이용하여 사용자의 관련 정보를 불법적으로 수집, 저장, 처리, 이용하는 위험
  - 제품과 서비스 공급업자가 제품과 서비스에 대한 의존성에 의해 네트워크 보안과 사용자의 이익을 훼손하는 위험
  - 국가의 보안을 훼손하는 기타 위험 등

즉, 제품이나 서비스가 보안 위험 등에 의하여 중단되지 않고, 지속적으로 운영되는 것을 중시하고 있다. 중국은 MS의 윈도 보안 업데이트 등 기술 지원 중단으로 고생한 경험 [10] 이 있기 때문에, 이러한 내용을 포함한 것으로 생각된다. 또한 주요 IT 기업들이 제공하는 제품이나 서비스에 백도어 등 보안 위험이 없는 것이 확인되어야지만 핵심 정보 인프라 시설에서의 사용을 허가하겠다는 의지를 엿볼 수 있다. 현재까지는 관련 제품 목록과 상세 기준이 공개되지 않은 상태다.

이에 비해 안전 검측, 안전 인증은 일반 기업이나 개인이 사용하는 네트워크 핵심 장비와 네트워크 안전 전용 제품을 대상으로 한다. 따라서 기존의 ISCCC 인증 제도를 그대로 활용하되, 강화된 기준을 사용할 가능성이 높다.

6.3. 핵심 정보 인프라 시설 사업자의 검사 및 평가

핵심 정보 인프라 시설 사업자는 매년 1회 이상, 네트워크 안전성 등을 검사, 평가하고, 이 결과를 해당 부처에 보고하여야 한다. 해당되는 안전법 조항은 다음과 같다.

- <네트워크 안전법 제38조> 핵심 정보 인프라 시설 사업자는 자체적으로 또는 전문기관에 의뢰하여 네트워크 안전성과 존재 가능한 위험에 대해 매년 최소한 한 차례의 검사와 평가를 진행하여 검사 평가 상황과 개선 조치에 대해 네트워크 안전 보고를 제출하고 관련 핵심 정보 인프라 시설 안전 보호 업무 부문에 보고하여야 한다.

이는 한국의 정보통신기반시설의 취약점 점검 및 평가

[표 7] 핵심 정보 인프라 시설의 한중 비교

	한국	중국
용어	정보통신기반시설	핵심 정보 인프라 시설
관련 법률	정보통신기반 보호법	네트워크 안전법
정책 조정 주체	정보통신기반보호위원회	국무원
지정 주체	중앙행정기관의 장	국가 산업 주무 부처, 감독 기관
의무	취약점 분석 및 평가, 보호대책 수립, 침해사고의 통지, 복구 조치	안전 보호 의무, 안전 심사 통과한 네트워크 제품 및 서비스 구매, 개인정보 및 중요 데이터 중국 내 저장, 네트워크 안전성 검사 및 평가
공격자 처벌	10년 이하의 징역 또는 1억원 이하 벌금	15일 이하 구속, 100만 위안 이하 벌금
운영자 처벌	1천만원 이하 과태료	100만 위안 이하의 벌금, 구매 금액 10배 이하의 벌금, 영업 정지, 업무 허가증 말소 등
기타	정보공유·분석센터 구축 및 운영	네트워크 보안 모니터링 사전 경보 체계, 정보 통보 제도 구축

와 유사한 방식으로 운영될 것으로 생각된다. 즉, 해당 부처에서 직접 모든 시설의 취약점을 점검하고, 보완하는 것은 많은 시간, 인력과 고도의 전문성이 요구되기 때문에 쉽지 않다. 따라서 시설이 자체 혹은 전문기관을 활용하여 검사 및 평가를 하는 방식으로 운영할 것이다. 이때, 매년 취합된 결과를 분석하여, 주요한 취약점 목록을 제공하고, 이를 다음 해에 집중 검사하는 방식도 가능할 것으로 예상된다. 한편 이를 통하여, 한국의 "정보보호 전문서비스 기업"과 같은 정보보호 컨설팅 기업을 지정하여 활용할 수 있을 것이다.

6.4. 개인 정보 및 중요 데이터 국외 이전

중국에서 사업을 하는 많은 기업들의 경우, 개인 정보 및 중요 데이터 국외 이전의 대상이 되는지가 제일 궁금한 사항일 것이다. 현재 방법, 지침에 의하면, 네트워크 사업자에게는 모두 해당 의무를 부과하고 있다. 즉, 핵심 정보 인프라 시설이 아니라, 네트워크 사업자에 해당되더라도 대상이 된다. 따라서 기업들은 일단 지침에 명시된 업종, 중요 데이터에 해당되는지를 확인하고, 최종적으로는 주무 부처를 통해 대상 여부를 확인하여야 한다. 대상이라고 확인된 이후에는 지침에서 규정하는 자체 평가를 수행하여야 한다. 이를 위해서는 개인 정보 및 중요 데이터에 대한 식별, 업무 프로세스 분석 등이 선행되어야 할 것이다. 이후 중국 내에 데이터를 저장하고, 안전 평가를 진행하여 국외 반출 여부를 결정해야 할 것이다. 현재로서는 지침의 내용을 면밀히 검토하고, 향후 <핵심 정보 인프라 시설 식별 지침>이 발표되면 이에 대한 추가적인 검토도 필요하다.

6.5. <정보 안전 기술, 데이터 국외 반출 안전 평가 지침>을 표준으로 제정한 이유

<정보 안전 기술, 데이터 국외 반출 안전 평가 지침>은 표준이다. 지침을 제정한 전국정보안전표준화기술위원회(TC260)는 정보 안전(information security) 분야의 국가 표준(GB)을 제정하는 위원회로, 중국국가표준화관리위원회(中国国家标准化管理委员会)가 관리하는 여러 위원회중 하나이다. 기술위원회는 정부 기관이 아니며, 위원회 구성원에는 정부 기관, 민간 기업, 대학 등이 모두 포함된다. 즉, 해당 지침을 정부 기관에서 제정하지 않고, 의원회에서 표준 형식으로 제정하는 것이다. 여기에는 다음과 같은 이유가 있을 것으로 추정된다. 첫 번째는 지침 제정, 개정이 비교적 용이하다는 것이다. 일반적으로 표준은 정부 기관의 공식적인 지침과 달리, 기술 변화 등을 고려하여 적시에 제정, 개정할 수 있다. 즉, 향후 서비스나 산업에 변화가 생겼을 때, 용이하게 반영할 수 있다. 두 번째로 표준화 과정은 의견 수렴이라는 절차를 이미 포함하고 있다는 것이다. 위원회 구성원에 기업, 대학 등이 포함되어 있고, 의견 수렴 시, 관련 협회, 기업 등이 표준안을 열람하고 의견을 제출할 수 있다. 따라서 제정 이후, 지침이 특정 정부 부처에서 독단적으로 제정했다는 지적을 피할 수 있다. 세 번째는 해당 지침을 국제 표준으로 제정할 수 있다. 향후 국제 표준으로 제정되면, 해당 제도는 국제 표준을 준용하여 운영된다는 주장의 근거로 활용될 수 있을 것이다.

6.6. 재중 외국 기업에 대한 영향

중국에 있는 외국 기업도 안전법의 적용 대상이 된다. 만약 핵심 정보 인프라 시설에 해당된다면, 의무 사항 준수를 위해서 상당한 비용과 노력이 소요될 것으로 생각된다. 첫 번째는 개인정보 및 중요 정보 중국 내 보관이다. 개인정보, 중요 정보에 대한 식별과 업무 프로세스 분석이 끝나고 나면, 업무 프로세스를 변경하고, 중국 내 정보 저장을 위한 시설 구축이 필요하다. 또한 안정성을 고려하여 테스트 서버를 구축하고, 충분한 테스트를 거친 이후, 실제 중국 내 데이터 저장이 이루어져야 할 것이다. 두 번째는 네트워크 제품 및 서비스의 교체이다. 안전 심사를 통과한 제품 및 서비스를 사용해야 하기 때문인데, 역시 안정성을 고려하여 충분한 테스트를 거친 이후, 교체가 이루어져야 한다. 세 번째는 안전 보호 의무, 안전성 검사와 평가 등이다. 이것은 안전법 제34조, 제38조에서 규정하고 있다. 기업 입장에서는 규정 제정, 조직 개편, 예산 편성 등 상당한 부담이 발생할 것으로 생각된다.

- <네트워크 안전법 제34조> 본법 제21조의 규정 외에 핵심 정보 인프라 시설 사업자는 다음과 같은 안전 보호 의무를 이행하여야 한다.
  - 전문 안전 관리 기구를 설치하고, 안전 관리 책임자를 지정하여, 동 책임자와 핵심 업무 담당자에 대해 안전 배경 심사를 진행한다.

- 종사자에 대한 네트워크 안전 교육, 기술 교육과 기능 평가를 정기적으로 진행한다.
- 주요 시스템과 데이터베이스에 대한 재난 대비 백업을 진행한다.
- 네트워크 안전 사건의 비상 매뉴얼을 제정하고 정기 훈련을 진행한다.
- 법률, 행정 법규에서 규정한 기타 의무.

이러한 규제 준수에 대한 비용과 노력은 당연히 기업에 큰 부담으로 작용한다. 하지만 많은 국가들이 자국에서 영업 활동을 하는 기업들에게 규제 준수를 요구하는 것은 어떤 면에서는 매우 당연한 일이기도 하다. 핵심 정보 인프라 시설의 중요도를 감안하면, 해당 기업들은 이러한 규제를 적극적으로 준수하려는 노력을 하는 것이 필요하다고 생각된다. 한편, 기업의 시행착오를 최소한으로 줄이기 위해서, 중국 정부에서 핵심 정보 인프라 시설 해당 여부 등을 확인할 수 있는 상세한 법령과 참고 자료를 제정하고 배포하는 것이 필요하다. 또한 일정 기간 유예 기간을 두어, 위법 사항을 바로 처벌하기 보다는 계도하는 방식도 유용할 것으로 생각된다.

Ⅶ. 결 론

본 고에서는 중국의 <네트워크 안전법>과 관련 법령을 중심으로 핵심 정보 인프라 시설 보호 동향을 살펴보았다. 핵심 정보 인프라 시설은 서비스가 중단될 경우, 국민들에게 미치는 영향력이 막대하기 때문에 각국에서는 관련 법률을 제정하여 적극적으로 보호하고 있다. 이에 비하면 중국은 약간 늦은 감이 있지만, 안전법에 다양한 의무 조항과 처벌 조항을 모두 포함하고 있어서, 매우 강력한 정책 집행이 가능할 것으로 생각된다. 이 법은 중국에 진출하여 활동하는 많은 외국 기업들에게도 큰 영향을 미칠 것으로 생각된다. 향후에도 관련 세부 법령 제정에 관심을 가지고 지켜보는 것이 필요할 것으로 생각된다.

참 고 문 헌

[1] 개인정보와 중요 데이터 국외 반출 안전 평가 방법(www.cac.gov.cn/2017-02/04/c_1120407082.htm)
[2] 네트워크 제품과 서비스 안전 심사 방법(www.cac.gov.cn/2017-05/02/c_1120904567.htm)
[3] 정보 안전 기술, 데이터 국외 반출 안전 평가 지침(www.tc260.org.cn/zdetail.jsp?id=20170527173820)
[4] 네트워크 핵심 설비와 네트워크 안전 전용 제품 목록(www.cac.gov.cn/2017-06/09/c_1121113591.htm)
[5] 핵심 정보 인프라 시설 안전 보호 조례(www.cac.gov.cn/2017-07/11/c_1121294220.htm)
[6] 정태인, 김주영, 김원, “중국 네트워크 안전법 동향”, 정보보호학회지, 27(3), 2017
[7] CII 정의(www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/cii)
[8] 全國信息安全標准化技術委員會(www.tc260.org.cn/)
[9] 중국 국가 표준(baike.baidu.com/item/%E5%9B%BD%E5%AE%B6%E6%A0%87%E5%87%86/596584?fr=aladdin)
[10] 중국서 된서리 맞았던 MS, 토종업체와 맞춤형 윈도 개발(www.yonhapnews.co.kr/bulletin/2016/09/22/0200000000AKR20160922138600009.HTML?input=1179m)

〈저 자 소 개〉

정 태 인 (Jung Taein)
정회원

1998년 2월 : 한양대학교 전기공학과 학사 졸업
2000년 2월 : KAIST 전기 및 전자공학과 석사 졸업
2000년 1월~2001년 6월 : 데이콤
2001년 7월~현재 : 한국인터넷진흥원 수석연구원
관심분야 : 개인정보보호, 정보보호

김 주 영(Kim JuYoung)
정회원

2005년 8월 : 한양대 공학대학원 컴퓨터공학 석사 졸업
2016년 8월 : 숭실대 IT정책경영학과 공학박사
2001년 1월~2002년 3월 : 정보통신교육원
2002년 4월~현재 : 한국인터넷진흥원 개인정보대응센터장
관심분야 : 개인정보보호, 정보보호

김 원 (Kim Weon)
정회원

1984년 2월 : 한양대학교 전자공학과 학사 졸업
1989년 2월 : 한양대학교 일반대학원 전자공학과 석사 졸업
2002년 8월 : 경희대학교 일반대학원 전자공학과 박사 졸업
1989년 1월~1992년 6월 : 데이콤
1992년 7월~1999년 6월 : 한국전산원
1999년 7월~2017년 5월 : 한국인터넷진흥원 본부장
2017년 6월~현재 : 개인정보보호본부 연구위원
2017년 9월~현재 : 한양대학교 공학대학원 겸임교수
관심분야 : 컴퓨터 네트워킹 및 보안, 개인정보보호