부산대학교 해운통상법연구
제14권 제1호 (통권 제19호)
2023년 12월, pp. 89~128

중요데이터의 식별지침에 대한 각국 비교

- 중요데이터의 식별지침에 대한 중국과 미국 비교 연구를 중심으로 -

이 취 새*

目 次

Ⅰ. 서 론
Ⅱ. 중국 중요데이터의 식별지침
Ⅲ. 미국 CUI의 식별지침
Ⅳ. 비 교
Ⅴ. 결 론

Ⅰ. 서 론

중국의 '중요데이터'와 미국의 'CUI'(Controlled Unclassified Information)는 각 국가의 국가 데이터보안을 강화하는 중요한 제도이다. 중국의 중요데이터는 국가 정보보안을 위한 표준 및 규정을 제공하고, 미국의 CUI는 연방기관과 비연방기관에서 처리되는 미 분류 정보에 대한 통제를 목적으로 한다. 본 연구는 비교법학을 활용하여 중국의 중요데이터와 미국의 CUI를 분석하여 양 국가의 차이점과 공통점을 식별한다.

▌투고일자 : 2023년 11월 20일, 심사일자 : 2023년 12월 19일, 게재확정일자 : 2023년 12월 22일.
* 부산대학교 대학원 법학과 석사과정

Ⅱ. 중국 중요데이터의 식별지침

1. 데이터의 의의와 분류

중국은 영향 대상에 대한 피해 결과에 따라 분류되며 1단계는 일반 데이터, 2단계는 중요데이터, 3단계는 국가 핵심데이터 등 3단계로 나뉘고 있다.[1] 이 등급 시스템은 보안 전략 및 조치를 식별하고 핵심 데이터에 대한 특별한 보호를 보장하는 데 도움이 된다.

(1) 의의

1) 일반 데이터 의의

일반 데이터는 기호 형식으로 저장된 정보이다. 사물의 속성, 관계 및 행동을 기록하고 설명하는 숫자, 문자, 이미지, 소리 및 기타 형태가 될 수 있다. 데이터 자체는 어떤 의미도 가지고 있지 않지만, 적절한 해석과 분석을 통해 데이터를 유용한 정보로 전환하여 의사결정과 행동을 뒷받침할 수 있다.[2]

2) 중요데이터 의의

중요데이터란 전자적 형태로 존재하며 변조, 파기, 유출, 불법 취득, 이용 등이 발생할 경우 국가보안 및 공공이익을 저해할 수 있는 데이터로 정의하였고[3] 동시에 중요데이터는 국가기밀 및 개인정보를 포함하지 않지만, 방대한 개인 정보를 기반으로 형성된 통계 데이터 및 이와 관련된 파생된 데이터도 중요데이터에 속한다.[4]

3) 국가 핵심데이터 의의

국가 핵심데이터는 데이터 보안법에서 국가 안보, 국가 경제의 생명줄, 중요한 국민생활 및 주요 공익과 관련된 데이터로 정의된다. 이러한 국가 핵심 데이터에 대해 국가

---

1) 王文澤, 我國數據分類分級保護法律制度的完善, 2020, 28頁.
2) 白牛數據, 數據是什麼？－－ 認識數據, 2020, https://baijiahao.baidu.com/s?id=1769751007423849122&wfr=spider&for=pc
3) <정보보안기술 중요데이터 식별가이드라인(資訊安全技術重要數據識別指南)(徵求意見稿)>, 제3조 제2항
4) 蔡榮偉・楊傑, "≪重要數據識別指南(征求意見稿)≫概覽", 中倫律師事務所 : http://www.zhonglun.com/Content/2021/11-02/1113533717.html

주권, 안전 및 개발 이익을 보장하기 위해 보다 엄격한 관리 시스템을 구현한다. 국가 핵심 데이터 관리 시스템 위반할 경우에는 관련 부서는 최대 1,000만 위안의 벌금을 부과할 수 있으며 특정 상황에 따라 관련 업무 정지, 관련 업무 허가 취소 또는 영업 허가 취소 등의 처벌 조치를 취할 수 있다. 어떤 경우에는 범죄에 연루된 행위에 대해 형사 책임을 물을 수도 있다.[5)]

(2) 분류

1) 중요데이터

<2022년의 중요데이터 식별가이드라인>에 따르면 중요데이터의 식별 여부를 판단하는 기본적 요건은 다음과 같을 수 있다.(동 가이드라인, 제5조)[6)]

(a) 국가전략비축, 긴급동원능력: 전략물자 생산능력, 비축량

(b) 핵심기반시설 운영이나 중점분양의 산업생산을 지원하는 데이터: 핵심기반시설이 위치한 산업, 핵심 업무의 운영이나 산업생산의 중점영역

(c) 핵심정보인프라시설에 사이버 보안조치가 취해짐으로써 이 시설에 대한 사이버공격에 이용될 수 있는 데이터: 핵심정보인프라시설과 관련된 사이버 보안 계획, 시스템 배치 정보, 핵심 소프트웨어 및 하드웨어의 설계정보, 시스템 토폴로지, 비상 계획 등

(d) 수출통제품목과 관련된 데이터: 수출통제품목의 설계원리, 공정절차, 제작방법 등과 관련 있는 정보의 데이터 및 소스 코드, 집적 회로 배치, 기출 방안, 중요 파라미터, 실험 데이터, 검측보고

(e) 다른 국가나 조직에 의해 자국(중국)에 대한 군사 공격에 이용될 수 있는 데이터: 특정한 정밀성 요구조건을 만족시키는 지리적 정보

(f) 중요 표적이나 중요 장소로서 물리적 보안 상황을 반영하거나 또는 미 공개된 지리적 표식의 위치로서 테러리스트, 범죄자에게 이용됨으로써 파괴될 수 있는 데이터: 주요 보안 단위, 중요 생산 기업, 국가의 중요 자산(예를 들어 철도, 송유관)의 건설도면, 내부 구조, 보안 등의 상황을 반영한 데이터 및 비공개 특수 전용도로, 비공개 공항 등

---

5) 李南欣, 數據安全法中法規的國家覈心數據是什麼？ 2022https://lvlin.baidu.com/question/464864860780386405.html?fr=detail-recommend

6) 이정표, "중국 데이터보안법에 대한 연구 '-중요데이터 식별 가이드라인'을 중심으로-", 홍익법학 제23권 제4호 (2022), 196-198면

의 정보

(g) 핵심 설비. 시스템 구성요소의 공급 망을 파괴하는데 이용될 수 있고, 높은 수준의 지속적 위협 등으로 사이버 공격에 이용될 수 있는 데이터: 중요 고객의 목록, 미공개 핵심정보인프라시설 운영자의 제품. 서비스에 구매 상황 등과 관련 있는 데이터 및 공개되지 않은 중대한 취약점

(h) 집단의 건강 생리상태, 민족의 특성, 유전정보 등을 반영하는 기초 데이터: 인구센서스 자료, 인류의 유전자원 정보, 유전자 염기서열분석 원시 데이터

(i) 국가 천연자원 및 환경기본 데이터: 미공개 수리정보, 수문관측데이터, 기상관측데이터, 환경감시모니터링데이터는 중요데이터

(j) 과학 기술력과 국제 경쟁력에 영향을 미치는 데이터: 국방 및 국가안보와 관련된 지적재산권 데이터

(k) 민감한 품목의 생산, 교역 및 중요 장비의 배치. 사용에 관한 것으로써 외국 정부에 의하여 자국(중국)에 제재가 가해질 수 있는 데이터: 주요 기업의 금융거래 데이터, 중요장비의 생산제조 정보 및 국가 중대 프로젝트 시공과정에서의 중요장비 배치. 시용 등의 생산 활동에 관한 정보

(l) 정부기관, 군수기업 및 기타 민감한 중요 기관에 서비스를 제공하는 과정에서 발생하는 자의적으로 공개하지 아니하는 정보: 비교적 장기간에 걸친 군수기업의 차량 이용 정보.

(m) 미 공개된 공공데이터, 업무기밀데이터 정보데이터 및 사법 집행 데이터: 대 미공개의 통계데이터.

(n) 기타 국가의 정치, 영토, 군사, 경제, 문화, 사회, 과학기술, 생태, 자원, 핵시설, 해외 이익, 생물, 우주, 극지방, 심해의 안보에 영향을 미칠 수 있는 데이터

2) 국가 핵심데이터[7]

(1) 기본 통신, 라디오 및 텔레비전, 국방 산업 및 기타 산업의 주요 데이터: 통신, 미디어 및 국가 안보 분야의 데이터는 국가 안보를 유지하는 것이다.

(2) 금융, 에너지, 의료, 교육 등 국가 경제와 국민 생활과 관련된 중요한 산업의 데이

7) 愛企查企服平臺, 數據安全法中明確覈心數據包含哪些, 2023. https://aiqicha.baidu.com/qifuknowledge/detail?id=10065492222

터: 이러한 산업의 데이터는 국가의 경제, 에너지 공급, 의료 보건 및 교육 등과 직결되기 때문에 전략적이고 중요하다.

(3) 핵심 정보 인프라시설에 운영한 데이터: 사회 운영 및 정보 보안을 유지하기 위해 정보 인프라의 정상적인 운영을 보장하는 것이다.

(4) 핵심 공중 보건, 자연 재해 및 기타 비상사태에 대한 중요한 데이터: 재해 또는 공중 보건 사건에서 관련 데이터는 시기적절하고 효과적인 대응 및 예방에 매우 중요하다.

(5) 위의 데이터를 기반으로 파생된 기타 국가 안보, 사회 질서 또는 공공 이익에 중대한 영향을 미치는 데이터: 데이터의 영향이 원본 데이터 자체를 넘어 전반적인 안전과 공공 이익에 중대한 영향을 미칠 수 있으므로 데이터 파생 효과에 대한 관심을 가지고 있다.

2. 데이터 처리자의 보안의무와 책임

(1) 중요데이터 처리자[8]의 보안의무

8) 핵심정보인프라시설보안조례에서는 중요데이터 처리자의 주요 의무에 관하여 규정하고 있다.

제13조:운영자는 반드시 인터넷 안전 보호 제도와 책임제를 세워, 인력・재력・물력 투입을 보장해야 한다.

운영자의 주요 책임자는 핵심 정보 인프라시설 보안 보호에 대한 총책임을 지니고, 핵심 정보 인프라시설 보안 보호 및 중대한 네트워크 보안사고 처리를 주도하며, 중대한 네트워크 보안 문제를 해결하기 위한 연구를 조직한다.

제14조: 운영자는 특별 안전 관리 기관을 설치하고 특별 안전 관리 기관의 책임자 및 핵심 직책에 대한 안전 배경 심사를 실시하여야 한다. 심사 시 공안 기관과 국가 안전 기관은 협조하여야 한다.

제16조: 운영자는 전문 안전관리기구의 운영 경비를 보장해야 한다.

네트워크 보안 및 정보화와 관련된 의사 결정을 수행하기 위해 해당 인력을 할당하고 전문 보안 관리 기관의 직원이 참여해야 한다.

제17조 운영자는 자체적으로 또는 네트워크 보안 서비스 기관에 위탁하여 핵심 정보 인프라에 대해 연 1회 이상 네트워크 보안 테스트 및 위험 평가를 실시하고 발견된 보안 문제를 적시에 시정하고 보호 부서의 요구 사항에 따라 상황을 보고해야 한다.

제18조 핵심 정보 인프라 시설에서 중대한 사이버 보안 사고가 발생하거나 중대한 사이버 보안 위협이 발견된 경우 운영자는 관련 규정에 따라 보호 작업 부서와 공안 기관에 보고해야 한다.

핵심 정보 인프라의 전체 운영 중단 또는 주요 기능 장애, 국가 기반 정보 및 기타 중요한 데이터 누출, 대규모 개인 정보 누출, 큰 경제적 손실 발생, 불법 정보의 광범위한 전파 등 특히 중대한 사이버 보안 사건이 발생하거나 특히 중대한 사이버 보안 위협이 발견된 경우, 보호 업무 부서는 보고를 받은 후 즉시 국가 사이버 정보부서, 국무원 공안 부서에 보고해야 한다.

제19조 운영자는 안전하고 신뢰할 수 있는 네트워크 제품 및 서비스의 구매를 우선시해야 하며 네트워크 제품 및 서비스의 구매가 국가 안보에 영향을 미칠 수 있는 경우 국가 네트워크 보안

중요데이터는 국가와 기업 및 산업계뿐만 아니라 데이터와 관련된 모든 분야에서 핵심적 요소이므로 그 처리를 담당하는 주체에 대한 합리적인 규범이 필요하다.[9] 첫째, 중요데이터 처리자의 범위 및 중요데이터 보안 원칙을 명확히 하고 디지털 경제 데이터 보안 위험의 역동성을 고려하여 처리자가 보안 의무를 다했는지를 측정하는 기준선으로 중요데이터 보안 원칙을 규정해야 한다.[10] 둘째, 중요데이터 처리자는 데이터에 대한 백업. 암호화. 접근통제 등의 기술적 조치를 할 수 있어야 하며 사후적으로 데이터 사고가 발생했을 때 즉시 시정조치를 취할 수 있는 데이터의 보안시스템을 갖추어야 한다.[11] 셋째, 위험 평가는 위험 관리의 기초이자 핵심이며 처리자의 보안 의무의 중요한 부분이므로 중요데이터 처리자에 대한 정기적인 위험 평가 시스템을 규정해야 한다.[12]

(2) 국가핵심데이터 처리자의 보안 의무와 책임

기밀 관련 직원은 다음을 포함하지만 이에 국한되지 않는 여러 기밀 유지 의무 및 직무를 수행해야 한다.[13]

1) 국가 기밀문서, 자료, 장비, 제품을 다룰 때는 정부와 기업 내에서 정확한 기밀 규칙 및 규정을 준수하고 승인 절차를 수행해야 하며 생산 위치는 기밀로 보호되어야 한다. 이를 준수하는 것이 매우 중요하다. 아래는 일반적으로 따라야 할 몇 가지 기밀 보호에 관련된 주요 원칙과 절차이다.

(a) 기밀 규칙 및 규정 준수:

정부 기관이나 조직 내의 기밀 보호 규칙과 규정을 준수해야 한다. 규정 준수를 보장하기 위해 정기적인 교육 및 업데이트를 수행해야 한다.

규정에 따라 보안 심사를 통과해야 한다.

제20조 운영자는 온라인 제품 및 서비스를 구매할 때 관련 국가 규정에 따라 온라인 제품 및 서비스 제공자와 보안 계약을 체결하고 제공자의 기술 지원 및 보안 의무 및 책임을 명확히 하고 의무 및 책임 이행을 수행해야 한다.

제21조 운영자는 합병, 분리, 해산 등이 발생한 경우 적시에 보호업무부서에 보고하고 보호업무부서의 요구에 따라 핵심 정보 인프라 시설를 처리하여 안전을 확보하여야 한다.

9) 이정표, 앞의 각주6) 논문, 199면

10) 劉金瑞, 資料安全範式革新及其立法展開, ≪環球法律評論≫2021年第1期, 18頁.

11) 이정표, 앞의 각주6) 논문, 199면.

12) 劉金瑞, 앞의 각주10) 논문, 19頁.

13) 涉密人員的保密義務和工作責任, 保密網 2023：https://www.baomiwang.com/bmgl/content_726

(b) 승인 절차:

모든 기밀 활동은 해당 기관이나 조직에서 정한 승인 절차에 따라 이루어져야 한다. 기밀 정보에 접근하거나 다루는 모든 활동은 필요한 권한과 승인을 받아야 한다.

(c) 접근 제어:

기밀 자료에 접근할 수 있는 인원은 제한되어야 한다. 물리적인 보안 조치 및 전자적인 접근 제어 시스템을 도입하여 무단 접근을 방지해야 한다.

(d) 통제된 환경:

기밀 자료나 장비를 다루는 생산 위치는 통제된 환경에서 운영되어야 한다. 생산 시설에 대한 출입은 엄격히 관리되어야 하며, 각 지역에는 적절한 보안시스템이 구축되어야 한다.

(e) 통신 보안:

기밀 정보의 전송은 안전한 통신 수단을 통해 이루어져야 한다. 암호화 기술 등을 사용하여 기밀 통신을 보호해야 한다.

(f) 파괴 정책:

더 이상 필요하지 않은 기밀 자료나 장비는 안전하게 파괴되어야 한다. 파괴 절차도 정부나 조직의 규칙을 따라 이루어져야 한다.

(g) 규정 준수 감사:

정기적인 감사와 검토를 통해 규정 준수를 확인하고 개선할 수 있다. 감사 결과에 따라 보완 조치를 취하고 정책을 개선하는 것이 중요하다.

이러한 원칙과 절차를 준수함으로써 국가 기밀에 대한 적절한 보호를 유지할 수 있다.

2) 기밀문서와 기밀상품을 접수・전달할 때의 등록, 번호, 서명 절차를 준수하여야 하며, 전달할 때 전문부서를 거쳐야 하며, 비밀 보호 장비 없이 임의로 범위를 확대하거나 사용해서는 안 된다. 즉, 기밀문서와 기밀상품을 접수・전달할 때의 등록, 번호, 서명 절차를 준수하는 것은 기밀 정보를 안전하게 관리하고 무단 접근을 방지하기 위한 중요한 단계이다. 아래는 이에 관련된 주요 절차와 주의사항들이다.

(a) 등록 및 번호 부여:

접수된 기밀문서와 기밀상품은 등록되어야 하며, 고유한 식별번호가 부여되어야 한다. 등록된 정보에는 해당 문서나 상품의 내용, 등록일, 보안 등급 등이 포함되어야 한다.

(b) 서명 절차:

기밀문서와 기밀상품의 전달 및 접수 시에는 관련된 인원 간에 서명이 이루어져야 한다.

서명은 전달자, 수령자, 그리고 필요한 경우 감독자 등 모든 관련 당사자에 의해 이루어져야 한다.

(c) 전문부서를 통한 전달:

기밀문서와 기밀상품의 전달은 전문적으로 이를 관리하는 부서를 통해 이루어져야 한다.

전달 전문부서는 안전한 통로와 절차를 통해 정보를 전송하고, 전문적인 보안 프로토콜을 준수해야 한다.

(d) 비밀 보호 장비 사용:

기밀 정보를 다룰 때에는 필요한 경우 비밀 보호 장비를 사용해야 한다.

통신 시 암호화 기술을 적용하거나, 물리적 보안 장치를 사용하여 정보를 안전하게 유지해야 한다.

(e) 임의적인 범위 확대 금지:

기밀문서나 기밀상품에 접근할 권한이 있는 인원은 정확한 범위 내에서만 활동해야 한다.

비밀 정보의 범위를 임의로 확대하거나 사용하는 것은 엄격히 금지되어야 한다.

(f) 보안 규정 준수 감사:

정기적으로 보안 규정 준수 감사를 수행하여 기밀 정보의 적절한 관리 여부를 확인해야 한다.

감사 결과에 따라 보완 조치를 취하고 보안 절차를 개선하는 것이 중요하다.

기밀 정보의 안전한 전달과 관리는 조직 내의 보안 체계를 강화하고 무단 접근으로부터 정보를 보호하는 데 기여한다.

3) 기밀문서와 기밀상품을 사용하는 경우에는 규정된 사용범위를 준수하여야 하며 허가 없이 확대하여서는 아니 되며, 열람은 기밀이 보장된 장소에서 하여야 하며, 회람은 등록 절차를 거쳐야 한다.

기밀문서와 기밀상품을 사용할 때의 규정과 주의사항에 대한 내용은 다음과 같다.

(a) 규정된 사용범위 준수:

기밀문서와 기밀상품은 정해진 사용범위 내에서만 사용되어야 한다.

허가 없이 사용범위를 확대하거나 다른 용도로 사용해서는 안 된다.

(b) 열람은 안전한 장소에서:

기밀문서의 열람은 안전한 장소에서 이루어져야 한다.

물리적인 보안 조치와 함께 전자적인 보안 수단을 사용하여 안전한 환경에서 열람이 이루어져야 한다.

(c) 회람은 등록 절차를 거쳐야 함:

기밀문서나 기밀상품을 회람할 때는 등록 절차를 거쳐야 한다.

등록에는 열람한 날짜, 시간, 열람한 담당자 등의 정보가 포함되어야 한다.

(d) 허가 없는 확대 금지:

사용범위를 확대하거나 다른 부서나 인원에게 제공하기 위해서는 적절한 권한과 허가가 필요하다. 허가 없이 기밀 정보를 확대하여 사용하거나 외부로 유출해서는 안 된다.

(e) 정기적인 교육 및 감사:

기밀 정보를 다루는 직원들에게는 정기적인 교육이 제공되어야 한다. 감사를 통해 기밀 정보의 사용이 규정과 규칙을 준수하는지 확인하고, 문제가 발견되면 보완 조치를 취해야 한다.

(f) 기밀 보호 규정 준수:

사용자들은 기밀 보호 규정을 엄격히 준수해야 한다.

규정을 위반하는 행위에 대해서는 조직이 정한 제재가 시행되어야 한다.

기밀 정보의 사용은 규정과 규칙을 준수하는 것이 핵심이며, 이를 통해 정보 유출 및 부적절한 사용으로부터 조직을 보호할 수 있다.

4) 기밀문서를 복사, 추출 및 편집할 때 승인을 받아야 하며 복제는 등록 절차가 필요하며 원본 문서의 기밀 수준 및 기밀 유지 기간은 변경되지 않는다.

기밀문서를 복사, 추출 및 편집하는 경우에는 엄격한 승인 및 관리 절차를 따라야 한다. 아래는 관련된 주요 절차와 원칙에 대한 내용이다.

(a) 승인을 받은 복사 및 추출:

기밀문서를 복사하거나 추출하기 위해서는 해당 작업에 대한 승인을 받아야 한다.

이는 관리자나 권한을 가진 담당자로부터의 명시적인 승인을 포함한다.

(b) 등록 및 복제의 등록 절차:

복사 및 추출된 기밀문서는 등록 절차를 거쳐야 한다.

등록에는 복제한 날짜, 목적, 담당자, 그리고 기밀 등급 등의 정보가 기록되어야 한다.

(c) 기밀 수준과 유지 기간의 변경 금지:

복제된 기밀문서의 기밀 수준 및 기밀 유지 기간은 변경되지 않아야 한다.

기밀 정보의 변경은 명시적인 승인을 받은 경우에만 이루어져야 하며, 이러한 변경은 정확하게 문서화되어야 한다.

(d) 접근 제어 및 보안:

복제된 기밀문서는 원본과 동등한 보안 수준을 유지해야 한다.

물리적 보안과 전자적인 보안 수단을 통해 무단 접근을 방지하는 것이 중요하다.

(e) 편집 및 수정 시 주의사항:

기밀문서를 편집하거나 수정할 때에도 원칙적으로 승인이 필요하다.

편집된 내용은 정확히 문서화되고, 변경 사항이 추적될 수 있도록 보장되어야 한다.

(f) 정기적인 감사와 검토:

정기적인 감사와 검토를 통해 복제된 기밀 정보의 사용과 관리가 규정에 따라 이루어지고 있는지 확인해야 한다. 감사 결과에 따라 보안 절차를 개선하고 규정을 준수할 수 있도록 조치해야 한다.

이러한 절차와 원칙을 준수함으로써 기밀문서의 복사, 추출, 편집 등의 활동을 안전하게 관리할 수 있다.

5) 기밀문서와 기밀상품을 휴대하고 외출할 때에는 필요한 비밀유지조치를 하여야 하며, 관계없는 사항은 취급하지 않으며, 휴대하기 전에 지도자의 승인을 받아야 한다.

(a) 필수 비밀유지조치:

외출 시에는 기밀문서와 기밀상품을 안전하게 보호하기 위한 필수적인 비밀유지조치를 취해야 한다. 이는 물리적인 조치(예: 잠긴 가방, 안전한 보관함 등)와 전자적인 보안 수단을 포함할 수 있다.

(b) 관계없는 사항 제외:

외출 시에는 필요한 기밀 정보만을 휴대해야 하며, 관계없는 사항은 취급하지 않아야 한다. 필요한 기밀 정보만을 휴대함으로써 불필요한 위험을 방지할 수 있다.

(c) 승인 절차:

휴대하기 전에 기밀문서와 기밀상품을 지도자나 상위 관리자로부터 승인을 받아야 한다. 승인은 외출 목적, 휴대 대상, 유지 기간 등에 대한 명확한 지침을 포함해야 한다.

(d) 안전한 보관 및 전송:

외출 중에는 기밀문서와 기밀상품을 안전하게 보관해야 한다.

안전한 전송 수단을 사용하여 정보를 이동시키고, 이동 도중에도 보안 수준을 유지해야 한다.

(e) 기밀 정보의 노출 방지:

공공장소에서는 기밀 정보의 노출을 피하기 위해 특히 주의해야 한다.

다른 사람의 시야에서 기밀 정보가 노출되지 않도록 주의를 기울여야 한다.

(f) 외출 후의 안전한 처리:

외출이 끝난 후에는 기밀문서와 기밀상품을 안전하게 처리해야 한다.

필요한 경우에는 기밀 정보를 안전한 장소에 반납하거나 보안 절차를 따라야 한다.

(g) 기밀유지 교육:

관련 직원들에게는 기밀유지에 관한 교육이 필요하다. 교육을 통해 기밀유지에 대한 이해를 높이고, 정기적인 리마인더를 통해 기밀 보호에 대한 의식을 강화할 수 있다.

기밀 정보를 휴대하고 외출할 때는 신중하게 계획하고 안전한 절차를 준수하여 무단 접근 및 유출을 방지하는 것이 중요하다.

6) 기밀문서와 기밀상품을 보관할 때는 기밀 유지 조건을 갖춘 장소 및 장비를 선택해야 하며 개인은 개인적으로 보관할 수 없다. 아래는 이를 위한 몇 가지 주요 원칙과 규정에 대한 내용이다.

(a) 안전한 보관 장소 선택:

기밀문서와 기밀상품은 안전한 보관이 가능한 장소를 선택해야 한다.

잠긴 서랍, 안전 금고, 또는 특별한 기밀 보관실 등이 가능한 보관 장소로 고려될 수 있다.

(b) 기밀 유지 조건 충족:

보관 장소는 온도, 습도, 빛 등의 기밀 유지 조건을 충족할 수 있도록 유의해야 한다.
특히 일부 기밀 정보는 온도나 습도 등에 민감할 수 있으므로 이를 고려해야 한다.
(c) 전자적 보안시스템 사용:
필요한 경우 전자적인 보안시스템을 도입하여 무단 접근을 방지할 수 있다.
전자적인 비밀번호, 생체 인식 등의 기술을 활용하여 안전성을 높일 수 있다.
(d) 기밀 보관 장비 사용:
안전한 보관을 위해 특별한 기밀 보관 장비를 사용하는 것이 좋다.
예를 들어, 보안 금고나 기밀용 서랍 등이 해당된다.
(e) 공동 보관 고려:
기밀문서와 기밀상품은 가능하면 개인이 아닌 팀 또는 부서 수준에서 공동 보관하는 것이 좋다. 공동 보관은 특히 기밀 정보에 대한 업무가 공동으로 이루어지는 경우 유용하다.
(f) 개인 보관 금지:
개인은 개인적으로 기밀문서와 기밀상품을 보관해서는 안 된다.
보안을 위해 중앙화된 시스템 또는 지정된 보관 시설을 활용해야 한다.
(g) 접근 제어 강화:
보관 장소에 대한 접근 제어를 강화하여 허가 없는 접근을 방지한다.
엄격한 출입 통제 및 기록을 유지하여 무단 접근에 대비한다.
(h) 기밀 보관 규정 준수 감사:
정기적으로 기밀 보관 규정 준수 감사를 수행하여 안전한 보관 및 관리 여부를 확인한다. 감사 결과에 따라 필요한 조치를 취하고 보안 절차를 개선한다.
이러한 조치를 통해 기밀 정보의 안전한 보관을 유지하고 무단 접근으로부터 보호할 수 있다.

7) 기밀문서와 기밀상품을 파기할 경우 등록절차를 거쳐야 하며, 내용이 복원되지 않도록 무단파기를 엄격히 금지한다. 아래는 관련된 주요 원칙과 규정에 대한 내용이다.
(a) 등록 및 파기 절차:
파기되는 기밀문서와 기밀상품은 등록 절차를 거쳐야 한다.
등록에는 파기 대상의 목록, 수량, 등록일 등이 포함되어야 한다.

(b) 안전한 파기 방법 선택:

파기 시에는 안전하고 무효화된 방법을 선택해야 한다.

종이 문서의 경우 쇼더 칫솔, 파쇄기, 혹은 전문 파기 서비스를 활용할 수 있다.

전자적인 형태의 정보는 안전한 디지털 파기 방법을 선택해야 한다.

(c) 내용 복원 방지:

파기된 기밀문서와 기밀상품의 내용이 복원되지 않도록 확실히 보장해야 한다.

특히 디지털 형태의 정보는 안전한 삭제와 함께 데이터의 무결성을 확인해야 한다.

(d) 무단파기 엄격히 금지:

무단파기를 방지하기 위해 파기 절차는 엄격히 시행되어야 한다.

파기 대상이 무단으로 보존되거나 재사용되는 것을 방지하기 위한 강력한 통제가 필요하다.

(e) 기밀 파기 교육:

관련 직원들에게는 기밀 파기에 대한 교육이 제공되어야 한다.

올바른 파기 절차를 이해하고 파기 규정을 준수할 수 있도록 교육이 필요하다.

(f) 파기 기록 보존:

파기된 기밀문서와 기밀상품에 대한 기록은 적절한 기간에 보존되어야 한다.

이는 감사 및 검증 목적으로 필요하다.

(f) 환경적 측면 고려:

파기 시에는 환경적인 측면도 고려하여 환경에 미치는 영향을 최소화해야 한다.

친환경적인 파기 방법을 선택하는 것이 바람직하다.

(g) 법적 규정 준수:

파기 절차는 관련 법적 규정을 준수해야 한다.

특히 개인정보 보호법 등과 관련된 규정을 엄격히 준수해야 한다.

기밀문서와 기밀상품의 파기는 조직의 보안 체계를 유지하고 무단 접근을 방지하는 중요한 단계이다.

8) 기밀 회의를 조직하거나 참여할 때 관련 없는 사람을 안내해서는 안 되며 회의 문서는 등록해야 하며 참석자가 가져온 기밀문서는 적시에 보관해야 한다.아래는 기밀 회의와 관련하여 고려해야 할 주요 사항과 절차에 대한 내용이다.

(a) 관련 없는 사람의 참여 제한:

기밀 회의에는 기밀 정보에 관련된 인원만 참여할 수 있도록 엄격한 접근 제어가 필요하다. 관련 없는 사람은 회의에 참여하지 못하도록 특별한 조치가 필요하다.

(b) 회의 문서의 등록:

기밀 회의에 사용되는 문서는 등록되어야 한다. 등록에는 문서의 내용, 작성일자, 등록 일자, 그리고 관련된 정보들이 포함되어야 한다.

(c) 참석자가 가져온 기밀문서의 관리:

참석자가 개인적으로 가져온 기밀문서에 대해서도 적절한 관리가 필요하다.

참석자가 회의에 가져온 기밀문서는 회의 종료 후에 즉시 안전한 보관 장소에 보관되어야 한다.

(d) 회의 장소의 보안 강화:

회의가 진행되는 장소는 물리적 보안이 강화되어야 한다. 필요한 경우에는 출입 통제, CCTV 등을 활용하여 보안을 강화할 수 있다.

(e) 전자 기기의 사용 제어:

기밀 회의에 참석하는 참석자들의 전자 기기 사용은 제어되어야 한다.

기밀 정보 누설을 방지하기 위해 무단으로 사진 촬영이나 녹음을 방지하는 조치가 필요하다.

(f) 비밀 유출 방지 교육:

관련 직원들에게는 비밀 유출 방지 교육이 필요하다. 회의 참석자들은 기밀 정보를 어떻게 다룰지에 대한 교육을 받아야 한다.

(g) 회의 기록 보존:

회의의 기록은 적절한 보안 수준으로 보관되어야 한다.

회의의 기록이 필요한 경우, 안전한 방식으로 열람 및 검색 가능하도록 보관되어야 한다.

(h) 비상 상황 대비 계획:

기밀 회의 중에 비상 상황이 발생할 경우 대비 계획이 필요하다.

비상 상황 대비 계획은 기밀 정보의 무단 유출을 방지하고 참석자들의 안전을 보장하기 위해 중요하다.

기밀 회의의 경우, 조직은 적절한 절차와 보안 수준을 유지하여 중요한 정보의 안전

성을 보호해야 한다.

9) 외부에 정보, 원고 또는 저서를 보낼 때 기밀 유지 규칙을 준수해야 하며 기밀 검토되지 않은 원고를 비공개로 해외에 보내서는 안 된다. 아래는 외부로의 정보 전달 시에 유의해야 할 주요 사항에 대한 내용이다.

(a) 기밀 유지 규칙 준수:

정보, 원고, 또는 저서를 보낼 때에는 해당 자료가 기밀 정보를 포함하고 있는지를 꼼꼼히 확인하고, 기밀 유지 규칙을 준수해야 한다.

(b) 기밀 검토의 필요성:

기밀 정보가 포함된 자료를 외부로 전달하기 전에는 내부에서의 기밀 검토가 필요하다. 이를 통해 외부로 유출되면 안 되는 정보가 제거되거나 적절히 가려져야 한다.

(c) 원고의 기밀 유지:

원고를 보낼 때에는 특히 기밀 유지가 필요한 경우, 적절한 보안 조치를 취해야 한다. 암호화된 파일을 사용하거나 안전한 전송 수단을 활용하여 정보의 안전성을 유지할 수 있다.

(d) 해외 전송 시의 주의:

특히 기밀 검토되지 않은 원고는 해외로 보내서는 안 된다.

다양한 국가 간의 법적 및 규정적 차이로 인해 기밀 유지가 어려워질 수 있으므로 주의가 필요하다.

(e) 받는 측의 기밀 유지 의무 확인:

정보를 받는 측이 기밀 유지 의무를 이해하고 준수할 것을 확인해야 한다.

필요한 경우 기밀 유지 계약을 체결하여 상호적인 동의를 얻을 수 있다.

(f) 안전한 전송 수단 활용:

정보를 보낼 때에는 안전한 전송 수단을 사용해야 한다. 전자메일 등의 보안성이 낮은 수단을 피하고, 안전한 파일 전송 방식을 선택해야 한다.

(g) 보안 규정 및 가이드 준수:

조직이나 국가에서 제공하는 보안 규정과 가이드를 준수해야 한다.

특히 정보를 보내는 조직의 보안 정책을 엄격히 준수하는 것이 중요하다.

(h) 기밀 정보의 교육:

기밀 정보와 관련된 직원들에게는 기밀 정보에 대한 교육을 제공하여 올바른 절차를 이해하고 준수할 수 있도록 한다.

기밀 정보의 외부 전송은 신중하게 이루어져야 하며, 안전한 방법과 적절한 보안 절차를 준수하여 정보의 무단 접근 및 유출을 방지해야 한다.

10) 사회적 교류에서 국가 기밀은 사적인 통신에 포함되거나 공공장소에서 국가 기밀에 대해 논의되어서는 안 되며 관련 없는 사람을 기밀 중요 부서 및 군사 금지 구역으로 안내해서는 안 된다. 아래는 사회적 교류 시에 국가 기밀에 대한 주의사항에 대한 내용이다.

(a) 사적인 통신에 대한 주의:

사회적 교류에서 국가 기밀에 관한 어떠한 내용도 사적인 통신 수단을 통해 전달해서는 안 된다. 휴대전화, 전자메일 등의 통신 수단에서는 국가 기밀 정보가 논의되어서는 안 된다.

(b) 공공장소에서의 논의 방지:

국가 기밀은 공공장소에서 논의되서는 안 된다.

특히 카페, 레스토랑, 대중 교통 수단 등에서는 언급되어서는 안 되며, 화면을 통해 누군가에게 노출되는 것도 피해야 한다.

(c) 관련 없는 사람의 참여 방지:

국가 기밀에 대한 사회적 교류에서는 해당 주제에 관련 없는 사람을 피하고, 기밀 정보에 접근할 수 있는 권한이 없는 사람을 국가 기밀 중요 부서 및 군사 금지 구역으로 안내해서는 안 된다.

(d) 국가 기밀 중요 부서 및 군사 금지 구역 안내 금지:

외부인이나 국가 기밀에 권한이 없는 사람을 국가 기밀 중요 부서나 군사 금지 구역으로 안내해서는 안 된다. 출입 권한이 없는 사람은 해당 지역에 접근하지 못하도록 보안 절차가 엄격히 시행되어야 한다.

(e) 회의나 이벤트에서의 주의:

사회적 이벤트나 회의에서는 국가 기밀에 대한 논의를 최소화해야 한다. 만약 국가 기밀에 대한 이야기가 필요한 경우, 적절한 보안 조치를 취하고 공식적인 비밀 유지가 가능한 장소에서 진행되어야 한다.

(f) 기밀 정보의 훼손 방지:

기밀 정보가 논의되었던 장소에서는 해당 정보의 훼손을 방지하기 위해 정리 작업을 철저히 해야 한다. 기밀 정보가 남아있으면 안 되며, 필요한 경우에는 안전한 장소에 저장 또는 파기해야 한다.

국가 기밀 정보는 극도로 중요하며, 사회적 교류에서는 이러한 정보의 유출을 방지하기 위해 신중하고 책임감 있게 행동해야 한다.

3. 중요데이터와 국가 핵심데이터 구분

'데이터 보안법' 제21조 제2항은 '국가핵심데이터'의 개념을 정의하고 있으며 '데이터 출국 안전 평가 조치' 제19조는 '중요데이터'의 개념을 정의하고 있다.[14)]

우선 중요한 관점에서 '데이터보안법'은 국가가 데이터 분류 및 보호 시스템을 구축할 것을 제안하고 '네트워크 데이터 보안 관리 규정(의견 초안)'은 '데이터 보안법'의 데이터 분류 및 보호 시스템을 계속하고 이를 기반으로 국가 안보, 공익 또는 개인 및 조직의 합법적 권익에 대한 데이터의 영향과 중요도에 따라 데이터를 일반 데이터, 중요데이터 및 국가핵심데이터의 세 가지 범주로 나눈다. 중요데이터에 비해 국가핵심데이터가 더 중요함을 알 수 있다.

둘째, 관리 시스템의 관점에서 국가핵심데이터의 관리 시스템은 중요데이터의 관리 시스템보다 더 엄격한다. '네트워크 데이터 보안 관리에 관한 규정(의견 초안)'은 중요데이터와 국가핵심데이터에 대한 다양한 보호 조치를 취하고 개인정보와 중요데이터를 중점적으로 보호하며 국가핵심데이터를 엄격하게 보호할 것을 제안한다.

셋째, 처벌 조치의 관점에서 중요데이터에 비해 국가핵심데이터 관리 시스템을 위반할 경우 벌금 액수가 더 높고 처벌 조치가 더 엄격하며 법에 따라 형사 책임을 물을 수 있다.

4. 중요데이터와 국가 핵심데이터의 관계?[15)]

중국에서 중요데이터와 국가핵심데이터는 모두 데이터보안 분야의 개념이며 그 관계는 주로 데이터 수준과 보호 수준에 있다. 일반적인 관계는 다음과 같다.

---

14) 張燕, 王冰洋, 個人資訊保護法實施一周年|漢盛個人數據保護的法律與合規百問百答(三), 2022 http://hanshenglaw.cn/CN/08/a6eb7396d5ea7e7a.aspx

15) 藍藍, 資料安全立法視角下的重要數據：內涵、識別與保護, 2022, 110頁

(1) **보호** 수준: 국가핵심데이터는 종종 국가 안보, 국가 경제의 생명줄, 사람들의 생명, 건강과 같은 핵심 이익과 직접적인 관련이 있기 때문에 더 높은 보호 수준을 갖다. 중요데이터도 중요하지만, 보호 수준이 상대적으로 낮을 수 있다.

(2) **관련** 분야: 국가핵심데이터는 일반적으로 국가 안보 분야, 국가 경제의 핵심부서, 사람들의 생명, 건강과 같은 핵심 분야를 포함한다. 중요데이터는 금융, 교육, 의료 등 국가경제와 민생과 관련된 분야를 포함해 더 광범위할 수 있다.

(3) **규정** 준수: 이 둘의 정의와 관계는 일반적으로 '중화인민공화국 데이터 보안법'과 같은 관련 규정에 반영된다. 이러한 규정은 국가 핵심데이터와 중요데이터에 대한 관리 조치 및 보호 요구 사항을 규정한다.

따라서 일반적으로 국가 핵심데이터와 중요데이터는 중국 데이터 보안법에 따라 분류되며 국가 안보, 사회질서 및 공익을 유지하기 위해 다양한 데이터 범주의 보호 요구 사항을 명확히 하는 데 도움이 된다.

5. 중요데이터와 중요한 데이터 구분

중요데이터와 중요한 데이터는 문맥에 따라 다르게 해석될 수 있다. 중요데이터는 법적으로 중점적인 보호가 필요한 데이터를 의미하는 반면에는 중요한 데이터는 보다 일반적으로 중요성을 갖는 데이터를 나타낼 수 있다. 예컨대, 기업의 독점기술, 영업비밀은 기업의 생존을 위한 중요한 데이터이지만, 이러한 중요한 데이터가 유출, 변조, 훼손된 결과가 국가안전, 경제운영, 사회안정, 공공안전에 직접적인 위해를 끼칠 수 있는 수준까지 오르지 않는다면, 이러한 중요한 데이터는 법적으로 중점 보호를 요구하는 중요데이터가 아니며 해당 데이터 처리자는 중요데이터 처리자의 중점보호의무를 부담할 필요가 없다. 반면에 기업의 독점기술 및 영업 비밀이 유출, 변조 및 훼손된 결과가 국가 안보, 경제운영, 사회안정 및 공공안전을 직접적으로 위협하는 수준에 도달할 수 있는 경우 이러한 데이터는 기업에 중요한 데이터이며 법적 중요데이터 범주에 속한다. 즉, 중요데이터를 식별할 때 손해 행위에서 고려해야 한다.

6. 중요데이터에 개인정보가 포함되어 있는지?

'산업정보화 분야 데이터보안 관리 방법'은 2019년 기업의 생산, 운영, 내부 관리 정보

및 개인정보를 중요데이터 범위에 포함하지 않았다. 2020년 제정된 '식별지침가이드라인'도 비슷한 관행을 취하면서도 다량의 개인정보를 바탕으로 한 통계자료, 파생 데이터가 중요데이터일 수 있다고 언급하였다. 따라서 개인정보 자체가 중요데이터로 정의되는 것은 아니지만, 다량의 개인정보에 기초하여 형성된 데이터, 그리고 일부 특정 개인정보(즉, 중요 인물에 관한 개인정보)가 중요데이터로 인정될 수 있다. 그런 측면에서 중요데이터가 개인정보와 전혀 무관한 것은 아니다.

또한, 인터넷 데이터 보안관리 조례(의견수렴 초안)에서는 개인정보와 중요데이터에 대해 각각 별도의 규정을 두고 중점보호를 하고 있지만, 개인정보와 중요데이터가 동시 발생할 경우에는 데이터 처리자는 100만 명 이상의 개인정보를 처리하는 경우 개인정보 보호 규정을 준수하는 것 외에도 중요데이터 처리자에 대한 인터넷 데이터 보안관리 조례(의견수렴 초안)의 제4장을 준수하고 중요데이터와 동일한 보호 조치를 취하고 해당 의무를 이행해야 한다.[16] 즉, 100만 명 이상의 개인정보를 취급할 경우 개인정보보호규칙을 준수하는 것 외에 중요데이터와 동일한 보호 조치를 하고 의무를 이행해야 한다.[17]

7. 중요데이터와 관련된 판례

디디글로벌주식회사 처벌 사건[18]

(1) 사실관계

2022년 7월 21일에 디디글로벌주식회사는 647억900만 건의 개인정보를 불법 처리하여, 그중에 얼굴인식정보, 정확한 위치정보, 주민번호 등 여러 종류의 민감한 개인정보를 포함하고 있으므로 국가인터넷정보국은 '사이버보안법', '데이터보안법', '개인정보보호법', '행정처벌법' 및 기타 법규에 따라 디디글로벌주식회사에 80억 2600만 위안의 벌금을 부과했으며, 디디글로벌주식회사의 회장 겸 CEO인 청웨이(程維), 류칭(柳青) 회장에게도 각각 100만 위안의 벌금을 부과하였다.

16) 인터넷 데이터 보안관리 조례(의견수렴 초안) 제26조: 데이터 처리자가 100만 명 이상의 개인 정보를 처리하는 경우 이 규정 제4장의 중요 데이터 처리자에 대한 규정도 준수해야 한다.
17) Ibid
18) 蘭台商規|滴滴處罰案評析：80億買來的教訓, Lantai partners, 2022-08-23.: http://www.lantai.cn/news_view.aspx?nid=2&id=946

(2) 판결 요지

i): 이용자의 휴대전화 사진첩에 담긴 캡처정보 1196만 3900 건 불법 수집하였다.

ii): 83억 2300만 건의 사용자 클립보드 정보, 애플리케이션 목록 정보 수집하였다.

iii) 승객의 얼굴인식 정보 1억 700만 건, 연령대 정보 5350만 9200 건, 직업 정보 1633만 5600 건, 가족 관계 정보 138만 2900 건, '집'과 '회사'의 택시 주소 정보 1억 5300만 건 수집하였다.

iv) 승객이 대리운전 서비스를 평가할 때, 앱 백그라운드에서 실행 시, 휴대전화로 기록기 장비를 연결할 때 정확한 위치(경위도) 정보 1억 6700만 건을 과도하게 수집한다.

v) 운전자 학력정보 14만 2900 건 과다하게 수집하고, 운전자 주민번호 정보 5780만 2600 건 명문으로 저장하였다.

vi): 승객의 이동 의도 정보 539억 7600만 건, 상주 도시 정보 15억 3800만 건, 타지역 비즈니스/타지역 관광 정보 304억 건을 명확하게 알리지 않고 분석한다.

vii): 승객들이 무임승차 서비스를 이용할 때 관련 없는 "전화 권한"을 빈번히 요구한다.

viii): 사용자 기기 정보 등 19개 개인정보 처리 목적을 정확하고 명확하게 설명하지 않았다.

Ⅲ. 미국 CUI[19]의 식별지침

19) 미국 연방법규 제32조 2002부(32 CFR Part 2002)에 따르면, 그 내용은 ① CUI 보유자는 CUI를 획득 및 저장 단계에서 무단 접근 또는 공개로부터 보호하기 위해 합리적인(Reasonable) 조치를 취해야 하며, 제어 가능한 보안 환경을 구축하여 CUI를 무단 접근, 관찰, 경청을 방지하며 CUI를 법적 보유자의 직접 통제하에 유지하거나 적어도 물리적 격리 상태로 유지해야 하며, CUI를 연방 시스템이 아닌 경우에는 NIST SP 800-171의 보안 통제 요구를 준수해야 한다. (2 CFR §2002. 14 (a) (b) (c) (d)
② 전파 단계에서는 권한을 부여받은 CUI 보유자는 CUI에 표시를 적용해야 한다. 이 표시에는 CUI의 전체 표시, 소속 기관 및 연락처 및 기타 관련 정보가 포함되어야 한다.(32 CFR §2002. 16 (a) (3))
권한을 부여받은 CUI 보유자는 모든 수신자가 합법적인 목적에 따라 CUI를 받을 것으로 합리적으로 기대할 수 있어야 하며, CUI를 전송할 때 사용하는 시스템 및 구성 요소는 NIST의 지침에 따라야 하며, 기관은 NIST의 관련 표준에 따라 기밀성을 보장해야 한다. (32 CFR §2002. 16 (c))
③ 아웃소싱 및 공유 단계에서는 CUI 권한을 부여받은 보유자가 CUI를 비행정적 실체에 전송할 경우, 모든 수신자가 합법적인 권한을 기반으로 CUI를 어떻게 처리하는지에 대한 이해를 합리적으로 기대(Reasonable Expectation)해야 하고 기관이 비행정적 실체 또는 외국 실체와 CUI를 공유하

1. 정보의 의의

(1) CUI의 의의

미국의 통제된 비기밀 정보(CUI)란 국가 기밀이 아닌데도 불구하고 미국 연방 정부나 이에 봉사하는 비정부기구가 수신, 보유 또는 생성하는 정보로 법적, 규정적, 정책적인 요구에 따라 보호되고 전파가 제한되는 정보를 의미한다.[20] 또한, 미국은 CUI(controlled Unclassified Information)를 대통령령 12958호에 정의된 국가 안정 정보 기준에 부합하지 않지만, 국가이익이나 연방 정부 이외의 중요한 이해관계가 있으며, 법적 또는 정책적 보호를 받아 안전하게 처리되며, 무단 공개를 회피하고 안전보장, 교환 또는 전파 제한이 보장된다.[21]

(2) 미국 연방비밀제도의 의의

미국 연방비밀제도의 주요 의의는 국가 안보와 정보의 기밀성을 보호하여 국가의 안전과 안정을 유지하는 데에 있다. 이 제도의 주요 의의는 다음과 같다.[22]

1) 국가 안보 강화

연방비밀제도는 국가 안보를 강화하고 국가의 핵심 이익을 보호하기 위한 도구로 작용한다. 또한 민감하고 중요한 정보를 효과적으로 관리하고 안전하게 유지함으로써 국가의 안보를 향상시킨다.

2) 국가 간 경쟁에서 우위 유지:

냉전 시기에는 주로 소련과의 경쟁 상황에서, 그리고 현재에는 다양한 국제적 도전에 직면하면서, 미국은 자국의 연구, 기술, 정보를 안전하게 보호하여 국가 간 경쟁에서 우위를 유지하려고 한다.

거나 공유하려는 경우 적절한 계약을 체결해야 한다. (32 CFR §2002. 16(a)(4)(5)(6))

④ 파기 단계에서는 CUI 합법 소유자는 법률 규정 및 NIST 관련 기준을 준수하여 CUI를 파기 후 읽기, 번역 또는 구제할 수 없도록 처리해야 한다.(32 CFR §2002. 14(f)(1)(2))

20) 張濤, “美國受控非密資訊制度及其啓示”, 北京交通大學經濟管理學院,2023, 197頁.

21) 張敏, 王玥, “美國“受控非秘資訊”協同治理路徑及對我國“重要數據”立法的啓示“, 西安交通大學法學院, 2022, 37頁.

22) 美國聯邦制, 政治體制.: https://baike.baidu.com/item/美國聯邦制/10141127?fr=ge_ala

3) 기밀 정보의 유출 방지

연방비밀제도는 국가의 정보를 무단 유출로부터 보호하는 역할을 한다. 과거에는 원자력 및 군사 기술 등에서 유출 우려가 컸으며, 현재에는 사이버 공격과 같은 다양한 위협에 대응하기 위한 방어 수단으로 활용된다.

4) 정보 수집 및 분석 강화

연방비밀제도는 중앙정보국(CIA) 등을 통해 국가 안보에 필요한 정보를 수집하고 분석하는 데에 도움을 준다. 이는 국가의 정책 결정과 국제 사건에 대한 이해를 높이는데 기여한다.

5) 연구 및 개발의 촉진

안보와 국방 분양에서의 연구 및 개발은 연방비밀제도 아래에서 안정학[진행된다. 기술력의 혁신과 새로운 발견이 국가의 안정성과 경제적인 우위에 기여할 수 있다.

2. 도입 배경

(1) CUI 도입 배경

미국의 통제된 비기밀 정보는 “민감하지만 비기밀 정보”(Sen-sitive But Unclassified)에서 파생되었다. 1977년 11월에 제임스 카터 대통령이 발표한 국가 전기 통시 보호정책(National Telecommunications Protection Policy)은 정부와 청부업자 간에 전송되는 민감한 전기통신 자료를 보호해야 하며, 국방부는 국가 안보와 관련된 국가 기밀 정보와 비기밀 민감한 정보의 통신 보안을 담당하도록 정책을 제정하였다. 또한, “민감하지만 비기밀 정보”의 개념과 범위가 모호하고 관리가 불완전하여 해당 정보의 사용 및 관리에 다양한 문제가 발생할 수 있기 때문이다.[23)]

(2) 미국 연방비밀제도 도입 배경[24)25)26)]

23) 張濤, 앞의 각주20) 논문 197-198頁.
24) 吳桂文, 論國家保密制度的完善-基於美國聯邦保密制度, 2017, 19-26頁.
25) 基於公民資訊獲取保障的國家保密制度-美國聯邦保密制度以啓示-連志英, 2011.
26) 美國聯邦保密制度簡介, 程邁, 2008.

1) 제2차 세계 대전 이후의 안보 상황:

제2차 세계 대전 이후, 미국은 국가 안보에 대한 심각한 우려를 가지게 되었다. 전쟁 중에는 많은 정보가 국가 간에 교환되었고, 전쟁 후에도 새로운 지정학적 형태와 정치적 대립이 생긴다.

2) 소련과의 냉전 기간:

냉전 기간 동안 미국과 소련 간의 국제적인 긴장이 높아졌다. 양쪽 모드 국가 안보에 대한 우려를 갖고, 정보의 안전과 기밀성이 중요한 문제로 부각된다.

3) 원자력과 군사 기술의 발전:

1940년대 후반부터 1950년대 초반까지, 미국은 원자력 및 군사 기술 분야에서 중요한 발전을 이루었다. 이러한 분야에서의 연구 및 개발은 미국의 안보에 큰 기여를 했지만, 동시에 그 정보의 보안성이 중요해진다.

4) 정보 유출 및 감시의 필요성:

국가가 직면한 새로운 위협으로부터 국가 안보를 지키기 위해 정보의 유출을 방지하고 안전한 통신 및 기밀 정보 관리 시스템이 필요해진다.

5) 국가 안보법과 연방정보 보호법의 제정:

1947년에 제정된 국가안보법(National Secuirity Act)은 중앙정보국(CIA)를 창설하고 국가 안보에 필요한 정보 수집 및 분석을 촉진하기 위한 법률이다. 또한 2002년에는 연방정보 보호법(FISM)이 제정되어 연방 기관의 정보 시스템을 안전하게 관리하기 위한 법률적 기반을 제공한다.

3. 분류

3.1 CUI 분류

CUI는 연방 정보시스템 및 비연방 정보시스템에 분류된다.

(1) 연방 정보시스템 CUI 분류

2011년부터 현재까지 CUI EA에서 공개한 CUI는 20개 범주와 124개[27]의 하위 범주로

나뉘어져 있다. 이 범주에는 핵심 인프라 시설, 국방, 수출 통제, 금융, 이민, 정보, 국제 협약, 법집행, 법률, 자연과 문화 자원, 북대서양조약기구(NATO), 핵, 특허, 프라이버시, 구매 및 수매, 독점상업정보, 임시 정보, 통계, 세금, 교통 운송이 포함된다. 이 하위 범주들은 더 세분화되어 있지만 각 범주가 하위 범주를 설정하는 것은 아니고 필요에 따라 설정된다.[28]

(1) 핵심 인프라 시설: 질산암모늄, 화학테러 관련 취약성 정보, 핵심 에너지 인프라 시설 정보, 비상관리, 일반 주요 인프라 시설 정보, 정보시스템 취약점 정보, 물리적 보안, 보호된 핵심 인프라시설 정보, 보안법 관련 정보, 독성물질 및 수자원 평가(11)

(2) 국방: 통제된 기술 정보, 국방부의 핵심 인프라 시설 정보, 해군 핵전력 정보, 국방과 관련된 통제된 비비밀 핵 정보(4)

(3) 수출 통제: 수출 통제정보, 수출 통제연구(2)

(4) 금융: 은행비밀정보, 예산, 총감사관, 소비자불만정보, 전자이체, 연방주택금융비공개정보, 금융규제정보, 일반금융정보, 국제금융기관, 인수합병(M&A), 순가치 및 퇴직금(12)

(5) 이민: 난민보호, 학대받는 배우자 또는 아동, 영주권자 신분, 신분변경, 임시보호자 신분, 인신매매 피해자, 비자정보(7)

(6) 정보: 농업생산 또는 토지관련정보, 외국정보모니터링법에 따라 수집된 개인정보 및 암호해제정보, 외국정보모니터링법의 상업기록, 일반정보, 지리측량 및 제품정보, 정보재정기록, 내부자료(7)

(7) 국제협약: 국제 협약 정보(1)

(8) 법집행: 사고조사, 활동기금, 서약자, 통신, 통제물품, 범죄이력정보, 유전자정보, 일반법집행정보, 제보지, 수사정보, 청소년정보, 법집행재무기록, 국가안전편지, 기록/함정 및 추적장비, 포상정보, 성범죄피해자, 테러리스트 심사 및 제보자 신원정보(18)

(9) 법률: 행정소송, 아동음란물, 아동피해자/증인, 단체협상, 연방대배심, 법적특권, 입법자료, 판결전보고서, 이전체포기록, 보호령, 피해자, 증인보호(12)

(10) 자연과 문화자원: 고고학적 자원, 역사적 유산, 국립공원 시스템 자원(3)

(11) 북대서양조약기구(NATO): NATO 제한 정보, NATO 비기밀 정보(2)

---

27) 周亞超, 左曉棟, 美國受控非密資訊分類與安全控制解析, 2020, 13-14頁.
28) 張敏, 王玥, 앞의 각주21) 논문 39頁.

(12) 핵: 원자로, 재료 또는 안전에 관한 일반 보호 정보, 핵 권장 재료, 핵 안전 관련 정보, 안전 보호 정보, 통제된 비기밀 핵 에너지 정보(5)

(13) 특허: 특허출원을 제출한 정보, 법률의 보호를 받고 연방정부의 이익을 주는 발명정보, 국가안전문제로 출원 또는 특허부여를 거부한 비밀유지명령(3)

(14) 프라이버시: 계약사용, 사망기록, 일반사생활정보, 유전정보, 건강정보, 집행기관의 감사관에게 보고하는 인적정보, 군인기록, 인사기록, 학생기록(9)

(15) 구매 및 수매: 일반 구매 및 수매, 중소기업 연구 및 기술, 출처 선택(3)

(16) 독점상업정보: 일반전유상업정보, 해운공영운송인 및 해운부두사업자계약, 해운공영운송인 서비스계약, 전문제조업체, 전문우편, 인센티브관리시스템(6)

(17) 임시 정보/ 협의 정보: 국토안보협의정보, 국토안보부, 법집행정부, DHS 내부정보시스템의 취약점정보 및 그 기술적 우위를 해칠 우려가 있는 정보, DHS가 외국 또는 국제정보공유협약 또는 약정에 따라 수신하여 보호 요청된 정보, 운영안전정보, DHS 담당자 또는 DHS가 보호를 담당하는 다른 사람의 신변안전위험을 초래할 우려가 있는 정보, DHS 담당자 또는 DHS가 보호를 담당하는 다른 사람의 신변안전위험을 초래할 우려가 있는 정보, DHS 물리적 보안, 프라이버시 정보, 민감한 개인 식별정보(9)

(18) 통계: 투자조사, 농약생산자조사, 통계정보, 인구센서스 정보(4)

(19) 세금: 연방 납세자 정보, 조세 협정, 납세자 옹호자 정보 및 결정서, 결의서, 기술자문 각서 등 결의문서(4)

(20) 교통 운송: 철도 안전 분석기록, 민감 안전정보(2)

(2) 비연방기구 CUI의 일반적인 안전 통제

비연방기관의 정보시스템에서 통제된 비기밀 정보를 보호하기 위해 미국 국립표준기술연구원(National Institute of Standards and Technology, NIST)은 비연방기관의 NIST SP 800-171 시리즈[29] 기술 표준을 제정하였다.[30][31]

---

29) (1) NIST SP 800171 '비연방 시스템 및 기관의 통제된 비기밀 정보 보호'는 FIPS200을 기반으로 한 일반 보안 제어와 NIST SP 80053을 기반으로 한 확장 보안 제어를 제안한다.
(2) NIST SP 800171B '비연방 시스템 및 조직의 통제된 비기밀 정보 보호: 핵심 절차 및 고부가가치자산에 대한 향상된 보안 요구 사항'은 NIST SP 80053을 기반으로 한 향상된 보안 제어를 제안한다.
(3) NIST SP 800171A '통제된 비기밀 정보 보안 요구 사항 평가'는 CUI 보안 요구 사항을 평가하는 절차 및 방법을 제공한다.

1) 보호 요구 사항

NIST SP 800-171(비연방 시스템 및 조직의 통제된 비기밀 정보 보호: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations)의 통제된 비기밀 정보에 대한 보호 요구 사항의 14가지 측면을 언급하였다. 이러한 측면은 정보시스템 보안의 여러 핵심 분야를 포괄하여 종합적인 정보보안 관리를 확보한다. 다음은 이러한 측면에 대한 간략한 개요이다.

1. 액세스 제어: 시스템 및 정보에 대한 액세스를 제한하여 승인된 사용자만 특정 정보를 얻을 수 있도록 한다.

2. 인식 및 교육: 조직 구성원의 정보보안 인식을 개선하고 해당 교육을 제공하여 보안 기술을 강화한다.

3. 감사 및 책임: 시스템 활동을 기록 및 감사하여 특정 사용자의 작업을 추적할 수 있도록 하고 위반 사항에 대해 책임을 진다.

4. 구성 관리: 시스템 및 구성요소의 구성이 보안 정책을 준수하는지 확인하고 잠재적인 보안 위험을 줄이기 위해 변경 사항을 관리한다.

5. 인증: 유효한 인증 수단을 통해 사용자의 신분을 확인하여 합법적인 사용자만 시스템에 액세스할 수 있도록 한다.

6. 이벤트 대응: 정보보안 이벤트를 효과적으로 처리하고 복구하기 위한 대응 계획을 설계하고 구현한다.

7. 운영 및 유지보수: 지속적인 모니터링, 유지보수 및 업데이트를 포함한 정보시스템의 정상적인 작동을 보장한다.

8. 매체 보호: 저장매체의 정보가 무단 액세스나 유출을 방지하기 위해 적절하게 보호되어야 한다.

9. 직원 안전: 직원과 계약자의 신뢰를 보장하고 적절한 조치를 통해 시스템에 대한 액세스를 보호한다.

10. 물리적 보호: 허가받지 않은 사람이 정보시스템과 주요 장비에 물리적으로 접근하는 것을 방지하기 위해 적절한 물리적 보안조치를 취한다.

11. 위험 관리: 잠재적인 정보보안 위험을 식별, 평가 및 관리한다.

---

30) 張濤, 앞의 각주20) 논문 200頁.

31) 周亞超, 左曉棟, 앞의 각주27) 논문, 13-15頁.

12. 안전성평가 : 정기적으로 안전성평가를 실시하여 시스템의 안전결함을 검출하고 시정한다.

13. 시스템 및 통신보호 : 시스템 및 통신의 보안을 보호하기 위한 적절한 기술적 조치를 취한다.

14. 시스템 및 정보 완전성: 정보의 완전성을 보장하기 위해 적절한 수단을 통해 무단 수정 또는 파괴를 방지한다.

2) 주요 정보

NIST SP 800-171의 정보는 다음과 같다.

(1) 목적: NIST SP 800-171의 목적은 비연방 시스템 및 조직에 CUI(Control Non-Control National Information)를 처리하기 위한 보안 요구 사항을 제공하는 것이다. 이러한 요구 사항은 무단 액세스 및 누설을 방지하기 위해 분류되지 않았지만 통제된 정보에 대해 적절한 보안 조치가 구현되도록 하는 것을 목표로 한다.

(2) 내용: 이 표준은 액세스 제어, 인증, 구성 관리, 데이터 보호 등을 포함한 일련의 보안 관리를 포함한다. 이러한 통제의 목적은 정보시스템이 잠재적인 위험과 위협에 대처하기 위해 적절한 보안을 갖추고 있는지 확인하는 것이다.

(3) 적용 범위: NIST SP 800-171은 주로 비연방 시스템, 즉 연방 정부가 직접 관리하지 않는 시스템 및 조직에 적용된다. 여기에는 공급업체, 계약자 및 기타 연방 계약을 처리하는 주체가 포함될 수 있다.

(4) 준수 요구 사항: 조직이 연방 계약을 처리할 때 일반적으로 NIST SP 800-171의 요구 사항을 충족해야 한다. 연방정부가 수급사업자와 공급자에게 정보자원을 보호하기 위한 적절한 보안조치를 요구하기 때문이다.

(5) 평가 및 규정 준수: 조직은 시스템이 SP800-171의 요구 사항을 충족하는지 확인하기 위해 안전성 평가를 수행해야 할 수 있다. 이것은 보안을 검증하고 정보시스템을 개선하는 방향을 제공하는 데 도움이 된다.

따라서 전반적으로 NIST SP 800-171은 조직이 통제된 비기밀 정보를 처리할 때 정보시스템의 보안을 보장하기 위한 지침과 표준을 제공한다.

3.2 미국 연방비밀제도 분류

미국 연방비밀제도는 주로 최상위 기밀도, 중간 기밀도, 하위 기밀도의 등급으로 분

류된다.[32] 이러한 분류 등급은 정보의 중요성가 민감도에 따라 접근 권한을 제어하고 안전하게 관리하기 위해 사용된다. 분류된 정보는 해당 등급에 따라 적절한 보안 절차에 따라 다루어지며, 기밀 정보의 유출을 방지하고 국가 안보를 유지하기 위해 이러한 체계가 존재한다.

1) 최상위 기밀도(Top Secret)

최상위기밀도는 미국 연방비밀제도에서 사용되는 분류 중 가장 높은 등급으로, 정보의 국가 안보에 매우 중대한 영향을 미칠 수 있는 경우에 적용된다. 또한 최상위기밀도로 분류된 정보는 매우 제한적인 접근을 필요로 하며, 이 정보에 대한 접근 권한은 특정한 권한과 교육을 받은 개인에게만 부여된다. 그리고 최상위기밀도로 분류된 정보는 다양한 분야에서 발생할 수 있으며, 주로 국가 안보, 군사 작선, 외교 정책, 정보수집 및 분석, 특수 작전 등과 관련된 정보에 해당한다. 이 정보들은 국가의 안전과 안정성에 직접적인 영향을 미칠 수 있는 것들로서, 그 민감성과 중요성에 비례하여 최상위 기밀도로 분류된다.

최상위 기밀도 정보에 접근하려면 해당 정보에 대한 특별한 인가와 보안 검토가 필요하며, 접근자는 엄격한 교육 및 훈련을 받아야 한다. 또한 이 정보에 접근한 모든 활동은 정밀한 감시와 기록이 이루어져야 하며, 정보의 보안성은 매우 높아야 한다. 이러한 절차와 제약은 정보의 무단 유출을 방지하고 국가의 안전을 보장하기 위해 수립된다.

2) 중간 기밀도(Secret)

최상위 기밀도보다는 낮은 기밀도로, 국가 안보에 중요한 영향을 미칠 수 있는 정보가 해당된다. 중간 기밀도 정보에 대한 접근도 엄격하게 제어되며, 접근자는 특정한 권한과 교육을 받아야 한다.

중간 기밀도로 분류된 정보는 국가 안보에 중요한 영향을 미칠 수 있는 내용을 다룬다. 이 정보는 주로 국방, 외교, 정보수집, 특정 프로젝트, 기밀 연구 등과 관련된 내용을 포함한다. 또한 중간 기밀도 정보에 접근하기 위해서는 해당 정보에 대한 특별한 권한이 필요하며, 접근자는 교육과 훈련을 받아야 한다. 엄격한 접근 제어가 시해되어 정보에 대한 접근이 특정한 권한이 있는 개인들로 제한된다. 그리고 중간 기밀도 정보는

32) 絶密、秘密、機密：揭秘美國保密檔案分類依據, 2023.: https://baijiahao.baidu.com/s?id=1757259532969026397&wfr=spider&for=pc

안전한 환경에서 보관되어야 하며, 정보에 접근한 활동은 감시되고 기록된다. 정보의 무단 유출을 방지하고 보안성을 강화하기 위한 다양한 조치가 취해진다. 중간 기밀도 정보의 노출은 국가 안보에 중대한 영향을 미칠 수 있으므로 해당 정보의 기밀성을 유지하기 위해 최선의 노력이 기울여진다. 정보의 공개나 무단 유출은 엄격히 금지되어 있다.

3) 하위 기밀도(Confidential)

하위 기밀도는 미국 연방비밀제도에서 사용되는 분류 중에서 가장 낮은 기밀도로 분류되는 등급이다. 하위 기밀도 등급은 정보의 민감도가 낮지만 여전히 국가의 이익에 영향을 미칠 수 있는 내용을 다룬다. 이 등급의 정보는 주로 해정, 조직 운영, 프로젝트 등과 관련된 내용을 포함하며, 정보의 무단 공개는 피해야 하는 것이 원칙이다. 이 정보에 접근하기 위해서는 여전히 특별한 권한이 필요하지만, 최상위 기밀도 및 중간 기밀도에 비해 상대적으로 더 폭넓은 범위의 인원에게 접근이 허용된다. 또한 정보의 기밀성을 유지하기 위해 적절한 보안 조치가 취해진다. 그러나 이는 최상위 기밀도 및 중간 기밀도에 비해 덜 엄격한 수준일 수 있다. 그리고 하위 기밀도 정보는 일정한 기간이 지나면 해제될 수 있는 가능성이 있다. 기밀성 해제는 정보의 민감도와 필요성에 따라 정해진 기간 후에 이루어질 수 있다. 하위 기밀도 정보는 더 낮은 기밀도로 분류되지만, 여전히 국가의 이익과 안전에 영향을 미칠 수 있는 정보들을 다루고 있으므로 자주 사용된다.

4. 관리 부서

4.1 CUI 관리 부서

미국은 주로 연방기관, 집행기관(Execute Agency, EA), 두 부서에서 통제된 비기밀 정보 관리 기능을 수행하고 있으며, 각각 집행 기능, 지도 감독 기능 및 자문 기능을 수행한다.

1) 연방기관

연방기관[33]은 통제된 비기밀 정보 계획을 실행하는 행동 주체이며 통제된 비기밀 정

33) 張濤, 앞의 각주20) 논문 201頁.

보를 관리하고 관련 법률 및 규정의 요구 사항을 이행하는 구체적인 직무를 담당한다. 이들 기관의 책임은 주로 다음과 같다.

(1) 집행기관 감독: 연방기관은 규정 및 표준을 준수하는지 확인하기 위해 집행 기관(Executive Agency, EA)의 CUI 관리 조치를 감독할 책임이 있다.

(2) 가이드라인 제정: 연방기관은 때때로 일관성과 규정 준수를 보장하기 위해 CUI 관리에 대한 가이드라인을 작성하거나 개발에 참여한다.

(3) 정부 차원의 CUI 관리 조정: 다양한 기관 간의 조정을 촉진하여 연방 정부에 CUI를 일관되게 관리하도록 한다.

(4) 분쟁, 불만 및 제안: 공정하고 효과적인 CUI 관리를 보장하기 위해 CUI 관리와 관련된 분쟁, 불만 및 제안을 처리하는 정부 안팎의 분쟁 및 제안에 대응한다.

(5) 정책 수립 참여: 연방기관은 CUI 관리에 대한 더 높은 수준의 정책을 수립하여 이러한 정책이 연방 정부 전체에 적용되도록 할 수 있다.

이러한 기관의 조정된 협력은 CUI가 적절하게 보호되고 처리되도록 포괄적인 통제된 비기밀 정보 관리 프레임워크를 구축하는 데 도움이 된다.

2) 집행기관(Execute Agency, EA)

CUI의 집행기관(EA)은 미국에서 국가 기록 보관국(National Archives and Records Administration, NARA)를 의미한다. 집행 기관은 CUI의 보호 및 관리가 관련 규정 및 표준을 준수하는지 확인하기 위해 통제된 비기밀 정보(CUI)에 대한 관리 정책을 구현하고 시행할 책임이 있다. 집행 기관의 책임은 다음과 같다.[34][35][36]

(1) 정책 수립 및 시행: 안전 표준 및 관리 절차를 포함하여 CUI에 대한 정책을 결정하고 시행한다.

(2) 감독 기관의 조치: 규정된 기준을 충족하는지 확인하기 위해 기관의 CUI 관리 조치를 감독한다.

(3) 법령 준수 보장: CUI의 관리 및 보호가 해당 법률 및 규정을 준수하는지 확인한다.

(4) 지침 및 교육 개발: CUI 관리에 대한 지침을 개발하고 조직이 관련 정책을 이해하

34) 吳沈括, 崔婷婷, “美國受控非密資訊管理制度研究”, 2019 87-89頁
35) 張濤, 앞의 각주20) 논문 201頁.
36) 張敏, 王玥, 앞의 각주21) 논문 37-38頁.

고 준수하도록 교육을 제공한다.

(5) 다른 기관과의 협력 조정: CUI 관리 정책의 일관성을 촉진하고 CUI의 효과적인 관리를 촉진하기 위해 다른 연방기관과의 협력을 촉진한다.

따라서, 일반적으로 집행 기관은 CUI가 국가의 안전과 이익을 보호하기 위해 적절하게 보호되고 관리되도록 CUI 관리 시스템에서 중요한 역할을 한다.

4.2 미국 연방비밀제도 관리 부서

1) 중앙정보국 (CIA - Central Intelligence Agency): 미국의 중앙정보국은 국가 안보에 필요한 정보를 수집하고 분석하는 임무를 수행한다. CIA는 연방비밀제도 아래에서 작동하며, 최고 기밀 정보에 대한 관리와 감독을 담당한다.[37]

2) 미국 국가안보국 (NSA - National Security Agency): NSA는 통신 및 전자 정보 수집과 처리를 담당하는 국가 기관이다. 정보통신 기술 및 네트워크를 통해 안보 관련 정보를 수집하고 해독하는 데에 중요한 역할을 한다.[38]

3) 미국 국가안전국 (NRO - National Reconnaissance Office): NRO는 위성 및 우주정보 수집에 특화된 기관으로, 위성을 통해 국가 안보와 국방 분야에서 중요한 정보를 수집한다.[39]

4) 미국 국가안보국 (ODNI - Office of the Director of National Intelligence): ODNI는 국가 정보 및 연방비밀제도에 관한 정책을 수립하고 조정하는 역할을 한다. 중앙정보국과 다른 정보 기관 간의 협력을 촉진하며 정보의 일관된 관리를 지원한다.[40]

5) 미국 국가 안전성 및 기밀성 평가국 (NCSC - National Counterintelligence and Security Center): NCSC는 연방정부 기관 및 계열 단체의 침해와 스파이 활동으로부터 국가를 보호하는 데에 중점을 둔다. 연방비밀제도를 통해 보호되어야 하는 정보의 안전성을 평가하고 강화하는 역할을 한다.[41]

---

37) 乾萊資訊諮詢, 請問美國FBI, CIA, NSA分別是什麼？有什麼區別？？,2022.: https://zhidao.baidu.com/question/1934141481433510427.html

38) 美國國家安全局, 美國政府機構中最大的情報部門. https://baike.baidu.com/item/美國國家安全局/300052?fr=ge_ala

39) 美國17大間諜機构揭秘, 2020.: https://www.sohu.com/a/379439424_120169927

40) Ibid

41) 國家電腦安全中心, 美國國家安全局下屬組織. https://baike.baidu.com/item/國家計算机安全中心/17718946?fr=ge_ala

이러한 부서는 각각 자체적인 임무와 책임을 가지며, 연방비밀제도의 원활한 운영과 안전한 기밀 정보의 관리를 담당한다. 이들은 국가의 안보를 보장하고 국제적으로 경쟁력을 유지하기 위한 핵심부문으로 작용된다.

5. 미국 연방비밀제도와 CUI의 차이점

미국 연방비밀제도와 CUI의 차이점은 주로 분류된 정보의 범위, 분류 기준, 관리 체계 등에 있다.

1) 범위 및 종류

연방비밀제도: 국가 안보에 관련된 기밀 정보를 보호하는 미국의 분류체계로, 최상위 기밀 등급에는 “최상위 기밀도” “중간 기밀도” “하위 기밀도”가 포함된다.

CUI (Controlled Unclassified Information): 연방정부가 분류하지 않지만 여전히 민감한 정보로 분류되어 있는 정보를 지칭한다. CUI에는 여러 범주가 포함되며, 예를 들어, 건강 정보, 금융 정보, 법적인 정보 등이 해당된다.

2) 분류 기준

연방비밀제도: 주로 국가 안보와 관련된 정보로, 분류 기준은 위험 정도, 민감도, 비밀 유출 시의 잠재적 영향 등이 고려된다.

CUI: 연방정부의 일반적인 분류를 받지 않았지만 여전히 보호가 필요한 정보를 위한 분류이다. CUI는 분야별로 정의되어 있으며, 분류 근거는 주로 법적 규정에 따른다.

3) 관리 체계

연방비밀제도: 국가 안보 정보를 위한 엄격한 분류 및 관리 시스템이 존재하며, 해당 정보에 접근은 제한되고 감독된다.

CUI: CUI 관리는 관련 규정과 지침에 따라 이루어지며, 해당 정보의 적절한 처리, 전송, 저장 및 파기를 보장한다.

이러한 차이점들은 미국에서 민감한 정보를 관리하고 보호하기 위해 사용되는 여러 분류 시스템 간의 기본적인 차이를 나타낸다.

6. 관련된 판례 (개인 정보)(patel v. Facebook, Inc.,No. 18-15982(9th Cir.2019).)

(1) 사실관계

새로운 사용자가 페이스북 계정에 등록할 때 사용자는 프로필을 생성하고 페이스북이 페이스북 정책에 따라 데이터를 수집하고 사용하는 것을 허용하는 페이스북 이용 약관에 동의해야 한다. 플랫폼에서 다른 사용자와 상호 작용하기 위해 페이스북 사용자는 다른 사용자를 친구로 식별하고 친구 요청을 보낸다, 요청이 수락되면 두 사용자는 텍스트, 사진 등의 콘텐츠를 공유할 수 있다. 수년 동안 페이스북에서는 사용자 페이스북에 게시된 사진에 페이스북 친구를 태그할 수 있도록 허용해 온다. 태그는 사진 속 친구를 이름으로 식별하고 해당 친구의 페이스북 프로필에 대한 링크를 포함한다. 태그가 지정된 사용자는 태그에 대한 알림을 받고, 사진에 대한 액세스 권한을 부여받으며, 원하는 경우 다른 친구와 사진을 공유하거나 스스로 태그를 해제할 수 있다.

2010년 패이스북은 태그 제안이라는 기능을 출시한다. 태그 제안이 활성화된 경우 페이스북은 얼굴 인식 기술을 사용하여 사용자가 업로드한 사진에 사용자의 페이스북 친구가 있는지 분석할 수 있다. 사진이 업로드되면 기술이 사진을 스캔하여 얼굴 이미지가 포함되어 있는지 감지한다. 그렇다면 눈, 코, 귀 사이의 거리 등 얼굴을 독특하게 만드는 다양한 가하학적 데이터 포인트를 추출해 얼굴 서명이나 지도를 만드를 기술이다. 그런 다음 이 기술은 얼굴 서명을 페이스북의 사용자 얼굴 템플릿이 일치하는 경우 페이스북은 사진 속 사람을 태그하도록 제안할 수 있다. 페이스북의 얼굴 템플릿은 페이스북이 관리하는 9개 데이터 센터에 있는 서버에 저장된다. 미국에 위치한 6게의 데이터 센터는 오리건, 캘리포니아, 아이오와, 텍사스, 버지니아, 노스캐롤라이나에 있다. 페이스북의 본사는 캘리포니아에 있다.

일리노이주에 거주하는 페이스북 사용자들은 페이스북의 안면인식 기술이 일리노이주 법을 위반한다고 주장하며 페이스북을 상대로 집단소송을 제기한다. 학급 대표인 Adam Pezen, Carlo Licata, Nimesh Patel은 각각 일리노주에 거주한다. 이들은 각각 2005년, 2009년, 2008년에 페이스북에 가입했고 일리노이주에 있는 동안 각각 페이스북에 사진을 올렸다. 페이스북은 각 원고의 얼국 템플릿을 생성하고 저장하였다.

2015년 5월에 일리노이주의 페이스북 사용자들은 업로드된 사진의 데이터를 사용하여 사이트의 사용자들이 친구를 인식할 수 있는 "태그 제안" 기능을 위한 얼굴인식 소프트웨어를 생성함으로써 일리노이 생체 개인 정보 보호법(BIPA)을 위반했다고 주장하

는 세 가지 추정 집단 소송을 제기하였다. 원고들은 2015년 9월에 캘리포니아주로 소송을 이전하기로 합의하였고, 그 곳에서 그들은 하나의 제안된 집단 소송으로 통합되었다.

2018년 4월에 미국 캘리포니아 북부 지방 법원의 제임스 도나토 판사는 "2011년 6월 7일 이후 페이스북이 일리노이주에 위치한 페이스북 사용자의 얼굴으로 템플릿을 생성하는 것을 인증하였다. 동시에 페이스북은 이 결정에 항소하였다.

2019년 8월 8일에 제9번째 순회 위원회는 페이스북의 얼굴인식 기술이 "개인의 사적인 일과 구체적인 이익을 침해한다"라는 것을 확인하였다. 또한, 2019년 10월 18일에 제9번째 순회법원은 페이스북의 전원합의체 재심리 동의를 거부하였다.

(2) 판결요지

제9번째 순회법원(9th Circuit Court of Appeals)은 BIPA가 원고의 특정 프라이버시 이익을 보호하고 BIPA 절차를 위반하여 실제로 이러한 프라이버시 이익을 침해하거나 이러한 프라이버시 이익에 중대한 위험을 초래하기 때문에 원고가 제3조의 자격을 부여하기에 충분하다고 주장한다. 그리고 법원은 태그 제안 기능이 업로드된 사진 속 얼굴의 세부 사항을 분석하여 얼굴을 인식하고 자동으로 태그를 제안하는 기능이 개인의 사생활과 구체적인 이익을 침해한다고 판결하였다. 또한, 전문가 그룹은 페이스북의 논점을 기각하고 지방법원이 집단을 인정하면서 재량권을 남용하지 않았다고 판단하였다. 결과 페이스북은 2021년 2월 26일에 6억 5000만 달러의 화해금을 지불하고 이 사건을 해결하였으며, 이로써 페이스북의 얼굴인식 데이터 남용 사건이 종결되었다.

Ⅳ. 비 교

미국의 CUI와 중국의 중요 데이터는 차이점뿐만 아니라 공통점도 있다.

1. 차이점

첫째, 미국과 중국은 각각 독자적인 법적 및 규제 체계를 갖고 있다. 미국은 CUI에 대한 규제와 보호를 위해 NIST SP 800-171과 같은 표준을 사용하고 있다. 중국은 개인

정보 보호 및 사이버 보안 등과 관련된 규정을 강조하고 있다.

둘째, 미국의 CUI는 주로 연방 정부와 연관된 정보에 적용된다. 중국에서는 중요 데이터의 범위가 더 광범위할 수 있으며, 국가 안보 및 중국 경제의 안정성과 연관된 데이터 등이 중요데이터로 간주될 수 있다.

셋째, 중국과 미국은 각각 독자적인 사이버 보안 규제를 시행하고 있다. 중국은 사이버 공격에 대한 방어를 강조하고 국내 기업 및 기관에 대한 사이버 보안 표준을 설정하고 있다. 미국도 사이버 보안에 중점을 두고 있으며, 특히 연방 시스템 및 데이터에 대한 보안이 강조되고 있다.

2. 공통점

첫째, 미국의 CUI 및 중국의 중요데이터는 모두 높은 수준의 보안 요구 사항을 가지고 있다. 이는 데이터의 수집, 저장, 처리, 전송 및 공유에 관한 엄격한 규정을 포함할 수 있다.

둘째, 미국 및 중국은 각각 개인 정보 보호를 강화하는 방향으로 나아가고 있다. 이는 민감한 개인정보를 보호하고 권리를 존중하는 것에 중점을 둔다.

셋째, 미국과 중국은 사이버 보안을 강조하고 있으며, 중요데이터 및 CUI에 대한 사이버공격 방지 및 대응에 대한 규제를 시행하고 있다.

넷째, 미국 및 중국은 각각 규제 및 표준을 통해 중요데이터 및 민감한 정보를 관리하고 보호하기 위한 지침을 제공하고 있다.

다섯째, 양국은 데이터 보호 및 사이버 보안 규정을 어기는 기업이나 기관에 대해 법적 책임과 제재를 부과할 수 있다.

Ⅴ. 결 론

본 논문의 연구를 통해 최근 몇 년 동안 중국과 미국은 중요데이터와 민감한 공개 데이터보안을 보장하는 것이 각각 중국과 미국의 보안 초점을 맞춤을 알 수 있다. 중국의 중요데이터는 국가 안보를 보장하고 공공이익을 보호하며 경제를 발전시키는 데 중점

을 두는 것으로 알려져 있다. 중국은 최근 몇 년 동안 데이터 보호 및 사이버 보안에 관한 법률과 규정을 강화하여 기업과 기관의 중요한 데이터를 보호하려는 노력을 기울이고 있다. 미국의 CUI는 안전과 공유의 균형을 기본 목표로 하고 있다. CUI는 주로 연방정부에서 발생하는 중요한 정보를 다루며, 국가 안보, 경제, 특허, 통신 등과 관련된 정보를 보호하는 데 중점을 둔다. 미국은 연방기관 간의 정보 공유와 안전한 보관을 도모하면서도 기술 혁신과 경제 성장을 지원하려는 노력을 기울이고 있다. 양국 간에는 다양한 방식으로 데이터 보호와 관리를 시행하고 있지만, 중국이 미국의 CUI를 참고하여 중요데이터에 대한 입법을 개선하고 보안 능력을 향상시키는 것은 국제적인 정보 보호 수준을 향상시키는 데 기여할 수 있다고 생각한다. 상호 협력과 정보 공유는 전 세계적으로 안전한 디지털 환경을 유지하기 위해 중요한 부분이 될 수 있다. 이러한 노력은 국가 간의 디지털 환경에서 발생할 수 있는 위협에 대비하고 대응하기 위한 중요한 기반을 마련하는 데 도움이 될 것이다.

참 고 문 헌

이정표, “중국 데이터보안법에 대한 연구- ‘중요데이터 식별 가이드라인’을 중심으로-”, 홍익법학 제23권 제4호 (2022), 196-198면

乾萊資訊諮詢, 請問美國FBI, CIA, NSA分別是什麼？ 有什麼區別？？,2022.: https://zhidao.baidu.com/question/1934141481433510427.html

國家電腦安全中心, 美國國家安全局下屬組織. https://baike.baidu.com/item/國家計算机安全中心/17718946?fr=ge_ala

國聯邦保密制度簡介, 程邁, 2008.

基於公民資訊獲取保障的國家保密制度-美國聯邦保密制度以啓示-連志英, 2011.

蘭台商規|滴滴處罰案評析：80億買來的教訓, Lantai partners, 2022-08-23.: http://www.lantai.cn/news_view.aspx?nid=2&id=946

藍藍, 資料安全立法視角下的重要數據：內涵、識別與保護, 2022, 110頁

劉金瑞, 資料安全範式革新及其立法展開, ≪環球法律評論≫2021年第1期, 18頁.

李南欣, 數據安全法中法規的國家覈心數據是什麼？ 2022 https://lvlin.baidu.com/question/464864860780386405.html?fr=detail-recommend

美國17大間諜機构揭秘, 2020.: https://www.sohu.com/a/379439424_120169927

美國國家安全局, 美國政府機構中最大的情報部門. https://baike.baidu.com/item/美國國家安全局/300052?fr=ge_ala

美國聯邦制, 政治體制.: https://baike.baidu.com/item/美國聯邦制/10141127?fr=ge_ala

白牛數據, 數據是什麼？－－ 認識數據, 2020, https://baijiahao.baidu.com/s?id=1769751007423849122&wfr=spider&for=pc

涉密人員的保密義務和工作責任, 保密網, 2023： https://www.baomiwang.com/bmgl/content_726

愛企查企服平臺, 數據安全法中明確覈心數據包含哪些, 2023. https://aiqicha.baidu.com/qifuknowledge/detail?id=10065492222

吳桂文, 論國家保密制度的完善-基於美國聯邦保密制度, 2017, 19-26頁.

吳沈括, 崔婷婷, “美國受控非密資訊管理制度研究”, 2019, 87-89頁

王文澤, 我國數據分類分級保護法律制度的完善, 2020, 28頁.

張濤, “美國受控非密資訊制度及其啓示”, 北京交通大學經濟管理學院,2023, 197頁.

張敏, 王玥, “美國“受控非秘資訊”協同治理路徑及對我國“重要數據”立法的啓示”, 西安交通大學法學院, 2022, 37頁.

張燕, 王冰洋, 個人資訊保護法實施一周年|漢盛個人數據保護的法律與合規百問百答(三), 2022. http://hanshenglaw.cn/CN/08/a6eb7396d5ea7e7a.aspx

絶密、秘密、機密：揭秘美國保密檔案分類依據, 2023.: https://baijiahao.baidu.com/s?id=1757259532969026397&wfr=spider&for=p

周亞超, 左曉棟, 美國受控非密資訊分類與安全控制解析, 2020, 13-14頁.

蔡榮偉・楊傑, “≪重要數據識別指南(征求意見稿)≫概覽”, 中倫律師事務所：http://www.zhonglun.com/Content/2021/11-02/1113533717.html

<국문초록>

중국의 중요 데이터와 미국의 CUI(Critical Unclassified Information)는 각 국가에서 자국의 중요 정보와 기밀 정보를 나타낸다. 중국은 국가 안보 및 경제적인 이유로 중요한 데이터를 보호하고 있으며, 미국은 CUI를 통해 국가 안보와 국가 운영에 필수적인 정보를 지키고 있다. 양 국의 데이터 보호 및 기밀 정보 관리는 각자의 국가 정책과 법규에 근거하고 있다.

중국의 중요 데이터는 광범위하게 다양하며, 국가 안보, 경제, 기술, 인프라 등 다양한 영역에 관련되어 있다. 이에는 정부 기관, 기업, 인구 통계, 연구 및 개발 데이터 등이 포함될 수 있다. 중국은 이러한 데이터를 보호하고 국가 이익을 유지하기 위해 다양한 안전 조치를 시행하고 있다.

미국의 CUI는 “Critical Unclassified Information”의 약어로, 국가 안보 및 국가 운영에 중요한 비기밀 정보를 가리킨다. 이는 미국 정부 기관이나 계약자가 다루는 중요한 데이터로, 기밀로 분류되지 않지만 그 중요성으로 인해 보호되어야 하는 정보를 포함한다. CUI에는 국가 안보, 경제, 기술, 기밀 프로젝트 등 다양한 범주의 정보가 포함될 수 있다. 미국은 CUI를 보호하기 위해 관련 법규와 정책을 시행하고 있다.

주제어 : 중요데이터, CUI, 데이터, 법규와 정책

<Abstract>

Comparison of identification guidelines for key data among countries

- Centered on a comparative study of key data identification guidelines between China and the United States -

*Li, Cui Sai**

The important data of China and the Critical Unclassified Information (CUI) of the United States reflect the important and confidential information of each country towards its own country. China protects important data for national security and economic reasons, while the United States protects information necessary for national security and operations through CUI. The data protection and confidential information management of both countries are based on their respective national policies and regulations.

China's important data is extensive and diverse, involving multiple fields such as national security, economy, technology, and infrastructure. This may include government agencies, businesses, demographics, research and development data, etc. China is implementing various security measures to protect this data and safeguard national interests.

The US CUI stands for Critical Unclassified Information, which refers to non confidential information that is crucial to national security and operations. This is important data processed by US government agencies or contractors, including information that is not classified but needs to be protected due to its importance. CUI may include different categories of information such as national security, economy, technology, and confidential projects. The United States is implementing relevant regulations and policies to protect CUI.

Keywords : Key Data, CUI, Data, Law and Policy

---

* Major in Commercial Law Department of law The Graduate School of Pusan University.