경북대학교 법학연구원『법학논고』
제93집 (2026.04) 337~373면.
Kyungpook Natl. Univ. Law Journal
Vol.93 (Apr 2026) pp.337~373.
http://doi.org/10.17248/knulaw..93.202604.337

# 데이터 중심 보안 전환에 따른 망분리 규제의 규범적 한계와 재구성 방향

이 형 균*

〈국문초록〉

디지털 전환(Digital Transformation)이 금융과 공공, 민간 전 분야에서 심화됨에 따라 클라우드 서비스, 생성형 인공지능(AI), SaaS 및 모바일 업무환경의 확산은 기존의 경계 기반 보안 모델이 더 이상 충분한 대응력을 갖기 어렵다는 점을 시사하고 있다. 이에 본 연구는 정보보호의 단위를 네트워크나 시스템이라는 공간적 위상에서 데이터 자체로 전이시키는 '데이터 중심 보안(Data-Centric Security)' 패러다임의 법적·이론적 토대를 고찰하고, 현행 망분리 규제 체계와의 구조적 충돌 양상을 분석하여 미래지향적인 규범 재설계 방향을 제언하고자 하였다.

우리나라의 현행 정보보호 규제 체계는 2010년대 초반 대형 해킹 사고의 경험을 배경으로 형성된 '네트워크 단절' 중심의 망분리 규정을 핵심적 보호 수단으로 삼고 있다. 그러나 이러한 규제는 특정 기술 방식을 법령에 직접 명시함으로써 기술중립성 원칙과 충돌하며, 급격한 기술 발전을 규범이 수용하지 못하는 경직성을 야기한다. 특히 2025년 발생한 대규모 정보 유출 사고들은 물리적 망분리와 기존 경계 기반 통제가 존재했음에도 불구하고, 데이터 단위 보호의 부재가 심각한 피해로 이어질 수 있음을 입증하였다. 이는 네트워크 경계 보호에만 매몰된 현행 규제가 현대의 복합적인 데이터 처리 환경에서 규범적 타당성과 보안 실효성을 상실해가고 있음을 보여준다.

본 연구는 이러한 문제의식 하에 미국, EU, 일본, 싱가포르 등 주요국의 보안 정책 변화를 비교법적으로 검토하였다. 미국은 행정명령(EO 14028)을 통해 제로트러스트 아키텍처(ZTA)를 연방기관의 기본 모델로 채택하여 데이터와 사용자 중심의 보안 구조를 확립하였고, EU는 GDPR과 NIS2 지침을 통해 기술중립성에 기초한 위험 기반 접근법을 명문화하였다. 또한 싱가포르와 일본 역시 특정 기술의 강제보다는 자산의 중요도와 위험 수준에 따른 유연한 통제와 거버넌스를 강조하고 있다.

이러한 분석을 바탕으로 본 연구는 데이터 중심 보안 관점에서의 망분리 규정 개정 방향을 네 가지 측면에서 제시하였다. 첫째, 특정 기술 수단의 채택 여부가 아닌 '정보보호 수준의 실질적 확보'를 준거로 삼는 결과 중심 규제로 전환하여 기술중립성을 확보해야 한다. 둘째, 데이터 민감도와 업무 위험 수준에 따라 통제 강도를 차등화하는 위험 기반(Risk-Based) 규율 체계를 제도화해야 하며, 그 구체

* 경북대 강사, 법학박사

적 모델로서 공공부문의 다중보안체계(MLS) 도입 사례를 주목해야 한다. 셋째, VDI · DaaS, IAM, 데이터 암호화 및 DCAP 등 현대적 보안 기술을 적법한 '대체 통제' 수단으로 정식화하여 피규제자의 법적 예측 가능성을 제고해야 한다. 넷째, '신뢰하지 않고 상시 검증한다'는 ZTA 원칙을 규범 전반에 투영하여 네트워크 경계 유무와 무관하게 데이터 자체에 대한 정밀한 통제력이 작동하도록 보안 표준을 재편해야 한다.

결론적으로, 현행 망분리 규정은 기술적 실재와 동떨어진 규제적 관성에서 벗어나 데이터의 실질적 가치와 안전한 흐름을 보호할 수 있는 현대적 규범 구조로 전면 재설계되어야 한다. 본 연구는 규제의 패러다임을 공간적 경계에서 정보 가치 중심으로 전환함으로써, 디지털 혁신을 저해하지 않으면서도 실질적인 사이버 보안 역량을 강화할 수 있는 법 · 정책적 지향점을 도출하였다는 데 의의가 있다.

주제어 : 망분리, 데이터 중심 보안, 제로 트러스트, 기술중립성, 위험 기반 접근

• 투고일 : 2026.03.31. / 심사일 : 2026.04.26. / 게재확정일 : 2026.04.26.

## Ⅰ. 서론

디지털 전환이 금융 · 공공 · 민간 전 분야에서 심화됨에 따라 정보보호 규제의 기본 구조 역시 새로운 변화에 직면하고 있다. 특히 클라우드 서비스 · SaaS(Software as a Service) · 모바일 업무환경 및 생성형 인공지능 활용의 확산은 기존의 경계 기반 보안모델이 충분한 대응력을 갖기 어렵다는 점을 드러내고 있으며, 이러한 기술 · 산업적 변화 속에서 데이터 중심 보안 개념은 국제적으로 중요한 보안 패러다임으로 자리 잡아가고 있다.[1)]

데이터 중심 보안은 정보보호의 단위를 네트워크나 시스템이 아니라 데이터 자체로 설정한다는 점에서 기존의 통제 방식과 구별할 수 있다. 이러한 접근은 데이터가 다양한 플랫폼을 경유하여 이동 · 저장 · 가공되는 환경을 전제로 하며, 데이터 자체에 지속적으로 보호조치를 적용하는 모델을 지향하고 있다.[2)] 그리고, 이러한 변화는 정보보호 기술의 발전뿐만 아니라, 보호의 기준과 통제 방식에 관한 규범적 논의에도 중대한 영향을 준다고 볼 수 있다.[3)]

---

1) 조병주 · 윤장호 · 이경호, 「금융회사 망분리 정책의 효과성 연구」, 「정보보호학회지」 제25권 제1호, 한국정보보호학회, 2015, 182면.

2) NIST, Zero Trust Architecture, NIST SP 800-207, 2020, p.3.

3) 법무법인(유) 광장, "「전자금융감독규정」 개정 - 자율보안 토대 마련", 「Lee & Ko 뉴스레터」, 2025. 2. 19.https://www.leeko.com/newsl/digitalfinance/202502_2/202502.pdf-

한편 최근 국내에서는 기존 보호체계가 전제로 해 온 네트워크 중심 통제 방식이 오늘날의 복잡한 데이터 처리환경을 충분히 방어하지 못하고 있음을 보여주는 사건들이 연이어 발생하고 있는데, 2025년 SK텔레콤에서 USIM 인증키 · IMEI · IMSI 등 이동통신 가입자 정보가 대규모로 유출된 사건이 대표적이다. 이 사건을 통해 물리적 망분리 및 기존 경계 기반 통제가 존재했음에도 불구하고, 데이터 단위 보호 부재가 심각한 피해로 이어질 수 있음을 확인할 수 있었다. 또한 2025년 롯데카드에서 약 297만 명의 고객정보가 온라인 결제 서버 침해를 통해 유출된 사건 역시 금융회사 보안체계의 구조적 취약성을 적나라하게 드러나게 하였다. 이러한 일련의 사고는 기존의 '망 단절 중심' 규제가 미래 지향적 업무환경 및 생성형 AI · API · SaaS 기반 처리구조에서 여전히 동일한 수준의 규범적 정당성을 유지할 수 있는지 재검토해야 함을 보여주고 있다.

그러나, 우리나라의 정보보호 규제체계는 여전히 망분리 규정을 핵심적 보호수단으로 삼고 있는 것이 현실이다. 전자금융감독규정, 정보통신망법, ISMS 인증기준 등은 내부업무망과 인터넷망을 물리적 · 논리적으로 분리할 것을 요구하고 있으며, 이는 네트워크 단절을 정보보호의 근본적 출발점으로 삼고 있는 현실을 보여 준다. 이와 같은 규범 구조는 2010년대 초반 대형 해킹 사고들의 경험을 배경으로 형성되었으며, 침입 경로를 사전적으로 차단하는 방식이 높은 효과성을 가진다는 인식 아래 제도화되게 되었다.

그러나 기술환경이 클라우드 · 모바일 · AI 기반으로 급격히 전환된 현재, 네트워크 단절을 중심으로 설계된 기존 망분리 규정이 여전히 동일한 규범적 타당성을 유지하는지에 대해서는 재검토가 필요하다고 생각한다. 특히 금융회사 · 공공기관의 업무가 SaaS · API · 외부 데이터 연동을 필수적으로 요구하는 상황에서, 단말기의 인터넷 연결을 금지하는 방식의 망분리는 현실적 업무수행과 충돌하는 사례가 발생하고 있다.

그리고, 해외 주요국의 규제는 이러한 변화에 보다 적극적으로 대응하고 있는데, 미국의 경우 행정명령 14028을 통해 ZTA를 연방기관의 기본보안모델로 채택하여, 네트워크 경계를 신뢰의 기준으로 삼지 않는 데이터 · 사용자 중심의 보안구조를 확립하고 있다.[4] 유럽연합(EU) 또한 GDPR과 NIS2 Directive를 통해 데이터 보호 원칙과 위험 기반 보안조치를 강화하면서, 특정 기술방식의 강제보다는 기술 중립성에 기초한 규제를 확립하고 있다.[5] 이러한 비교법적

4) NIST, Executive Order 14028: Improving the Nation's Cybersecurity, 2021.(https://www.nist.gov/itl/executive-order-14028-improving-nations-cybersecurity)

흐름은 한국의 규제체계가 개선 논의를 진행함에 있어 중요한 기준점을 제공하고 있다고 생각한다.

이에 본 논문은 데이터 중심 보안의 개념과 기술적 특성을 정리하고, 기존 망분리 규정의 규범적 구조를 분석하며, 양자 간 충돌의 구조를 법적·제도적으로 검토하고자 한다. 나아가 주요국의 규제 비교를 통해 한국 규제의 개정 방향을 제시함으로써, 미래 정보보호 규제체계의 정책적·법적 방향성을 도출하고자 한다. 이러한 연구 목적을 달성하기 위해, 본 논문은 데이터 중심 보안을 규범적 분석의 기준으로 설정하고, 이를 체계적으로 검토하기 위한 분석 틀을 제시한다. 본 논문은 데이터 중심 보안을 단순한 기술 개념으로 이해하지 않고, 정보보호 규제의 재구성 기준으로서 다음과 같은 세 가지 규범적 분석 틀을 중심으로 검토한다. 첫째, 보호 대상 설정 기준의 전환이다. 이는 보호의 기준을 네트워크 경계에서 데이터 객체 자체로 이동시키는 문제를 의미한다. 둘째, 통제 방식의 구조 변화이다. 이는 네트워크 단절과 같은 정적 통제에서 접근 권한 및 행위 기반의 동적 통제로의 전환을 포함한다. 셋째, 규제 설계 원리의 변화이다. 이는 특정 기술 수단을 강제하는 기술특정적 규제에서 벗어나, 보호 수준 확보를 중심으로 다양한 기술적 수단을 허용하는 기술중립적 규제로의 전환을 의미한다. 이하에서는 이러한 분석 틀에 기초하여 데이터 중심 보안의 기술적 구성요소와 규범적 함의를 단계적으로 검토한다.

## Ⅱ. 데이터 중심 보안의 개념과 기술적 특성

### 1. 데이터 중심 보안의 개념과 이론적 기반

데이터 중심 보안은 정보보호의 핵심적 준거와 통제의 단위를 네트워크나 시스템이라는 공간적 위상에서 '데이터 자체'로 전이시키는 보안 패러다임을 의미한다. 이는 내부망을 본질적으로 신뢰 영역으로 상정하고 외부로부터의 경계 방어에 치중했던 고전적인 경계 기반 보안 모델(Perimeter-Based Security)이 클라우드 컴퓨팅 및 SaaS의 확산과 같은 현대적 기술 환경에서 실효성을 상실함에 따라 제기된 규범적 대안이라 할 수 있다.[6] 이와 관련하여, 데이터

5) European Union, NIS2 Directive 2022/2555 참조.
6) 한국인터넷진흥원(KISA), 「제로 트러스트 가이드라인 1.0」, 2023, 12-15면.

중심 보안은 정보보호의 보호 단위를 네트워크나 시스템이 아닌 '데이터 자체'로 설정하고, 데이터의 생성 · 저장 · 이용 · 이동 전 과정에 걸쳐 지속적으로 보호조치를 적용하는 보안 패러다임으로 정의할 수 있다. 이는 보호 대상의 기준을 물리적 · 논리적 네트워크 경계에서 정보 객체 자체로 전환한다는 점에서, 전통적인 경계 기반 보안 모델과 본질적으로 구별된다. 즉, 데이터가 조직의 물리적 경계를 벗어나 다양한 인프라를 거치며 처리 · 저장되는 기술 구조하에서는 데이터의 전 생애주기에 걸쳐 일관된 보호 수준을 유지하는 것이 보안의 최우선 과제라고 볼 수 있을 것이다.

이러한 데이터 중심 보안은 단순한 기술적 변화에 그치는 것이 아니라, 정보보호의 규범 구조를 재구성하는 기준으로 기능한다는 점에서 법제적 의미를 가진다. 특히 데이터의 이동성과 분산성이 극대화된 클라우드 및 SaaS 환경에서는 특정 네트워크 경계를 기준으로 보호 수준을 설정하는 방식이 실질적 보호 기능을 충분히 수행하기 어려우며, 이에 따라 보호의 기준을 데이터 자체의 민감도와 처리 맥락으로 전환할 필요성이 제기된다.

이와 같은 데이터 중심 보안의 이론적 토대는 위험 기반 접근의 제도적 확립에서 찾을 수 있는데, 이는 데이터의 민감도와 처리 목적, 그리고 접근 주체의 위험 수준을 입체적으로 평가하여 보안 통제의 강도와 형식을 차등화하는 방식이다.[7] 이와 같은 접근은 규제가 행정법상의 비례성 원칙을 준수하기 위해 반드시 전제되어야 할 논리적 기초가 되며, 한정된 자원을 실질적인 위협 영역에 효율적으로 집중시킴으로써 규제의 합리성과 경제적 실효성을 동시에 확보하는 기제로 기능할 수 있을 것이다.

또한, 최근 글로벌 정보보호 표준으로 정착 중인 ZTA는 데이터 중심 보안의 실천적 원리를 제공하는데, ZTA는 "기본적으로 아무것도 신뢰하지 않는다(Never Trust, Always Verify)"는 원칙에 근거하여 모든 접근 요청을 맥락 기반으로 상시 검증하며, 네트워크상의 물리적 위치를 신뢰의 척도로 삼지 않는다.[8] 여기서 데이터 중심 보안이 보호의 '대상'을 규정한다면, ZTA는 그 대상을 보호하기 위한 '동적 검증 절차'를 구체화한다는 점에서 양자는 불가분의 보완 관계를 형성하게 된다고 볼 수 있다. 결과적으로 ZTA의 구현은 데이터 단위의 미세한 통제를 가능케 함으로써 데이터 중심 보안이 단순한 선언적 의

7) 성승제, "신기술기반 전자금융 안전성 확보 법제 연구", 연구보고 2015-05, 한국법제연구원, 2020, 124-128면

8) 금융보안원, "연구 · 개발 목적 망분리 예외 보안 해설서", 2025.5.6. "ZTA Never Trust 원칙의 전자금융감독규정 적용 가이드라인." https://www.fsec.or.kr/bbs/detail?menuNo=69&bbsNo=11688

미를 넘어 실무적 유효성을 갖게 하는 결정적 수단이 될 수 있을 것이다.

종합적으로 볼 때, 데이터 중심 보안은 개별 보안 기술의 단순한 집합을 넘어 정보보호의 기준점을 물리적 경계에서 실질적 정보 가치로 재편하는 규범적 이행으로 정의할 수 있다. 그리고, 기술적 개방성과 위협의 지능화가 가속화되는 현대 정보사회에서 규제 체계가 지향해야 할 현대적 보호 모델의 핵심적 지표가 된다는 점에서 중대한 법치주의적 의미를 가지게 될 것 이다.

## 2. 데이터 중심 보안의 핵심 구성요소

데이터 중심 보안 체계의 실질적 구현은 개별 보안 기술의 단순한 병렬적 배치가 아니라, 복수의 기술 요소들이 유기적으로 결합하여 통합적으로 작동할 때 비로소 완성된다. 이하에서는 주요 기술적 수단을 검토하고, 이들의 도입이 현행 망분리 규제 체계에 던지는 규범적 시사점에 대해 분석하고자 한다.

### 1) 데이터 분류 및 식별 체계와 위험 관리의 합리화

데이터 중심 보안은 자산의 민감도와 중요도에 따른 정교한 분류를 전제로 하는 위험 기반 접근의 핵심이며, 데이터의 실질적 가치에 부합하는 통제 수준을 설정할 수 있도록 돕는 체계적인 규범적 기준을 제시하고 있다.[9] 그리고, 법률적 관점에서 이러한 분류 체계는 보호 조치의 구체적 강도와 범위를 결정하는 기준이 되며, 향후 데이터 중심 규제 체계가 정립될 경우 규제의 비례성과 실효성을 담보하는 핵심적인 제도적 장치로 기능할 것이다.

### 2) 데이터 자체 보호 기술과 네트워크 중심 규제의 탈피

데이터의 저장 · 전송 · 처리 전 과정에 걸친 암호화와 가명 · 익명화, 그리고 속성 기반 암호화와 같은 기술들은 데이터 객체에 직접 구현되는 핵심 수단으로서,[10] 네트워크의 물리적 분리 여부에 의존하지 않고도 데이터 자체의 기밀성과 무결성을 실질적으로 보장하는 규범적 · 기술적 안전성을 확보할 수 있게 한다. 그리고, 네트워크 격리라는 공간적 차단 방식을 유일한 보호 수단으로 상정해 온 기존 망분리 규제의 기술특정적 한계를 보완하거나 대체할 수 있는

9) 법무법인(유) 세종, 「금융사도 생성형 AI를 활용할 수 있도록, 망분리 제도가 완화될 예정입니다」, SHIN & KIM 뉴스레터, 2024. , https://shinkim.com/kor/media/newsletter/pdf/2533

10) NIST, Guide to Attribute Based Access Control (ABAC) Definition and Considerations, Special Publication 800-162, 2014, pp. 12-15.

강력한 규범적 대안을 제시하고 있다.

3) 신원 및 접근 관리(IAM)를 통한 권한 통제의 정밀화

신원 및 접근 관리(Identity and Access Management, 이하 'IAM')는 사용자 · 기기 · 프로세스의 권한을 체계적으로 통제하는 기술로서, 그 근저에는 '최소 권한의 원칙(Principle of Least Privilege)'이 자리 잡고 있다.[11] 그리고, 특정 네트워크 내의 모든 주체를 신뢰하는 전통적 방식에서 벗어나, 업무 수행에 필요한 최소한의 범위 내에서만 권한을 동적으로 부여하는 구조를 지향하고 있으며, 이러한 정교한 권한 제어는 네트워크 단절에 의존하는 획일적 통제보다 고도화된 보안성을 제공하며, 데이터 중심 보안 체계의 실질적 통제 기제로 작동하고 있다.

4) 데이터 활동 통제(DCAP)와 책임추적성의 강화

실시간 접근 분석 및 이상 징후 탐지를 핵심으로 하는 '데이터 중심 감사 및 보호(Data-Centric Audit and Protection, 이하 'DCAP')' 기술은 데이터 처리 전 과정을 상시 추적 · 감시함으로써, 단발적인 네트워크 차단에만 의존하는 기존의 경직된 보안 규제와는 차별화된 능동적인 보안 체계를 구축할 수 있게 한다. 특히 이러한 로그(Log) 기반의 행위 모니터링은 보안 사고 발생 시 명확한 책임추적성과 투명성을 제공함으로써, 사후적 감독 체계의 실효성을 뒷받침하는 법적 증거력을 가진다고 볼 수 있다.

5) 가상화 기반 업무환경(VDI · DaaS)과 위험 구조의 재편

가상 데스크톱 인프라(VDI)와 서비스형 데스크톱(DaaS)은 데이터를 개별 단말기가 아닌 중앙 서버에 집중시켜 통합 관리함으로써 엔드 포인트의 보안 취약성을 근본적으로 개선하며, 이러한 가상화 환경의 특성상 단말기의 외부 인터넷 연결 상태가 정보 유출의 실질적 위험 수준을 결정하는 절대적 척도가 되지 않는다는 규범적 시사점을 제공하고 있다.[12] 결과적으로 가상화 기술의 보급은 물리적 단말 격리를 절대적 보안 요건으로 전제하는 현행 망분리 규정의 사실적 기초를 약화시키며, 규제 패러다임의 전환을 요구하는 기술적 동인으로 작용하고 있다.

---

11) NIST, Zero Trust Architecture, Special Publication 800-207, 2020, pp. 4-9.

12) 법무법인(유) 광장, "「전자금융감독규정」 개정 - 자율보안 토대 마련", 「Lee & Ko 뉴스레터」, 2025. 2. 19.

### 3. 클라우드 및 SaaS 환경에서의 경계 중심 보안의 한계

클라우드 컴퓨팅과 SaaS의 보편화로 인해 데이터가 특정 플랫폼이나 물리적 장소에 머물지 않고 복합적인 인프라를 유동적으로 오가는 환경이 정착되었으며, 이러한 구조적 변화 속에서는 내부와 외부를 엄격히 구분하는 기존의 이분법적 망 분리 체계가 기술적 한계에 부딪히거나 실질적인 보안 효익을 상실하는 지점에 이르게 된다.[13] 따라서 네트워크 단절에 기반한 기존의 정보보호 모델은 현대적 정보처리 환경에서 다음과 같은 규범적·실무적 한계에 직면할 수 있을 것이다. 먼저, 데이터의 고유한 이동성과 확장성으로 인해 네트워크 경계 자체를 보호의 유일한 준거로 삼기 어려워졌다는 점을 지적할 수 있는데, 이는 데이터가 온프레미스(On-premise)와 복수의 퍼블릭 클라우드를 수시로 넘나드는 상황에서는 고정된 '망'을 방어하는 것보다, 데이터 객체 자체에 보안 정책을 결합하여 이동 경로와 무관하게 보호 수준을 유지하는 것이 법리적으로 더욱 타당하기 때문이다. 또한 API(Application Programming Interface) 연동이 필수적인 업무 생태계에서 물리적 망분리는 혁신의 제약이라는 중대한 부작용을 낳을 수 있다. 현대의 기업 정보시스템은 외부 서비스와의 실시간 상호작용을 동력으로 삼고 있으므로, 인터넷 연결의 차단을 전제로 하는 규제는 업무의 연속성을 저해할 뿐만 아니라 보안을 명분으로 기술적 고립을 강요하는 결과를 초래할 수 있다. 그리고, 규제의 목적 달성을 위해 피규제자의 수단 선택권을 과도하게 제한한다는 점에서 비례성 원칙에 관한 논란으로 이어질 수 있을 것이다. 그리고, 특히 클라우드 보안의 핵심 가치가 데이터 암호화, 세밀한 접근 권한 관리(IAM), 실시간 행위 가시성 확보에 있다는 점을 고려할 때, 경계 기반의 차단 방식은 보안의 실질적 지표로서의 지위를 상실하고 있다. 네트워크 격리는 다층적 방어 체계 중 지엽적인 일부분에 불과하며, 이를 절대적인 보호 기준으로 삼는 규제 설계는 실제 발생 가능한 지능형 위협에 대한 대응력을 오히려 약화시킬 우려가 있어 보인다.

결론적으로 데이터 중심 보안은 클라우드 시대가 요구하는 기술적 유연성과 정보보호의 규범적 안전성을 조화시키는 필연적인 보호 체계로 이해될 수 있으며, 보호의 패러다임을 공간적 경계에서 정보의 실질 가치로 전환함으로써 급변하는 기술 환경 속에서도 데이터에 대한 실질적 지배력을 확보하는 합리

13) 황세운, "금융회사의 망분리 규제 현황 및 개선방향", KCMI 24-26, 자본시장 연구원, 2024, 18-22면

적인 규제 대안으로서 중대한 법치주의적 함의를 가질 수 있을 것이다.[14]

## Ⅲ. 기존 망분리 규정의 입법 구조와 규범적 특성

### 1. 망분리 규제의 형성 배경과 입법 목적

우리나라에서 망분리 규제가 제도화된 것은 2010년대 초반 연속적으로 발생한 대규모 사이버 침해사고의 경험에 기초하고 있다. 당시 사고들은 악성코드를 통한 내부망 감염, 대규모 정보 유출, 서비스 장애 등을 초래하였고, 이는 내부업무망과 외부 인터넷망이 연결된 구조에서 비롯된 것으로 평가되었다. 이러한 상황에서 입법자와 규제기관은 외부 침입 경로를 사전적으로 차단하기 위한 기술적 조치로서 망분리를 최적의 수단으로 보았고, 이로 인해 망분리가 금융·공공부문에서 핵심적인 보호조치로 자리 잡게 되었다.[15]

당시의 기술 환경은 대부분의 정보처리가 온프레미스 방식으로 이루어지며 데이터가 조직 내부의 폐쇄적 네트워크 내에서 관리되었는데, 이렇듯 네트워크 경계가 비교적 명확했던 시기에는 네트워크 단절이라는 정적(靜的) 통제 방식이 상당한 보안 실효성을 가질 수 있었다.[16] 이러한 점에서 망분리 규정은 당시의 기술적·사회적 배경을 투영한 실정법적 규율로 이해될 수 있으나, 제도 도입 후 10년이 경과한 현재의 정보기술 환경은 클라우드 서비스의 확산과 SaaS 도입의 가속화, 그리고 원격근무의 일상화로 인해 과거와는 비교할 수 없는 급격한 변화를 맞이하였다. 이처럼 네트워크 경계의 의미가 현저히 약화된 기술적 현실은 기존 망분리 규정의 규범적 타당성과 실효성을 근본적으로 재검토해야 할 필연적인 사유를 제공하고 있다고 보여진다.

---

14) 황세운, 금융회사 망분리 규제 해외사례와 국내 시사점, 자본시장포커스 2024-20호, 2024, 3-4면

15) 박지윤, 정윤선, 이재우, “금융권 망분리 현황과 망분리 정책 개선에 대한 고찰”, 정보보호학회논문지 제26권 제3호, 한국정보보호학회, 2016. 58-59면

16) 금융위원회, “금융분야 망분리 개선 로드맵 발표”, 보도자료, 2024.08.13. (https://www.fsc.go.kr/no010101/82885)

## 2. 전자금융거래법 및 전자금융감독규정의 규정체계

### 1) 법률 · 감독규정 상의 구조

전자금융거래법 제21조는 금융회사 등이 전자금융기반시설의 안정성을 확보하기 위해 필요한 보호조치를 이행할 의무가 있음을 명시하고 있다.[17] 이를 실무적으로 구체화한 전자금융감독규정 제15조는 '내부 업무망과 외부 인터넷망의 분리'를 필수 요건으로 내세움으로써, 망분리를 전자금융기반시설 보호를 위한 최우선적인 물리적 통제 수단으로 규정하고 있는 상황이다.[18] 이와 같이 감독규정이 특정 기술 조치를 명문화한 것은 기술특정적 규제구조의 전형적 예로 볼 수 있다.

또한 감독규정은 중요정보 취급 시스템에 대하여 인터넷 연결을 원칙적으로 금지하되 예외적인 경우에 한하여 강도 높은 보안조치를 부과함으로써, 개별적 위험 수준에 대한 정밀한 고려보다 네트워크 단절 자체를 앞세우는 규범적 통제 기제를 형성하고 있다.

### 2) 기술 방식의 규범화와 그 한계

문제는 특정 기술 방식이 법규에 직접 명시될 경우 기술 환경의 급격한 변화를 규제가 적기에 수용하지 못하는 경직성이 발생한다는 점이다. 일례로 암호화, 권한 관리(IAM), 데이터 중심 감사 및 보호(DCAP)와 같은 고도화된 기술이 탁월한 보안 효익을 제공하더라도, 단말기의 인터넷 연결 여부만을 준거집단으로 삼는 현행 규제 체계하에서는 이러한 신기술들이 실효적인 대체 수단으로 인정받는 데 한계가 따를 수밖에 없다.

이는 기술 중립성과 규범적 비례성 원칙의 관점에서 문제가 될 수 있기 때문에, 이는 규제가 특정 기술의 활용을 사실상 강제하는 경우, 기술 발전을 수용하지 못하는 경직성이 발생하며 이는 금융회사 · 공공기관의 혁신에도 장애가 될 수 있다.

## 3. 정보통신망법 및 ISMS 인증기준에서의 망분리 관련 규정

정보통신망법 제45조의3은 정보통신서비스 제공자에게 기술적 · 관리적 보호

17) 전자금융거래법 제21조(안전성의 확보의무). "금융회사 전자금융기반시설 안정성 확보 의무."
18) 전자금융감독규정 제15조 제1항. "'중요정보 취급시스템은 인터넷망과 분리 운영' 명문화."

조치 이행 의무를 부과하고 있으며, 이에 근거한 ISMS 인증기준은 네트워크 구분, 접속 통제, 원격접속 제한 등 다각적인 보호 장치를 명시하고 있다.[19] 비록 ISMS 기준 자체가 망분리를 명문으로 요구하고 있지는 않으나, 실제 심사 과정에서는 내부 업무망과 외부망의 분리 여부가 보안성을 가늠하는 실질적인 평가 척도로 작용하고 있다는 점에 주목해야 한다.[20] 요컨대 정보통신망법 체계는 전자금융감독규정에 비해 기술 중립적인 성격이 짙은 것으로 보이나, 실질적인 운영 단계에서는 네트워크 기반의 통제 방식을 고수함으로써 망분리에 준하는 규제 효과를 도출하고 있다. 이러한 괴리는 법규범의 문언과 집행 현장 사이의 불일치를 야기하며, 결과적으로 피규제자의 예측 가능성을 저해하고 규제의 명확성 원칙에 반하는 법적 불확실성을 초래할 소지가 크다고 볼 수 있다.

## 4. 공공부문의 망분리 정책과 제도적 변화

공공부문은 2010년대 초반부터 이중 PC를 활용한 물리적 망분리를 전면 도입하여 운용해 왔으나, 코로나19 이후 원격근무가 일상화되면서 기존 방식은 업무 비효율과 비용 증대, 사용자 편의성 저하라는 한계에 직면하게 되었다. 이에 정부는 이러한 경직성을 해소하고자 단일 단말 기반의 클라우드 및 SaaS 활용을 부분적으로 수용하는 등, 기술 환경 변화에 대응하여 정책 기조를 점진적으로 전환하고 있다.[21]

이러한 정책적 기조의 변화는 망분리가 더 이상 절대불변의 보호 수단이 아님을 제도적으로 수인하는 과정으로 풀이되며, 이와 같은 공공부문의 선제적 행보는 향후 금융권 규제 지형에도 유의미한 파급 효과를 미칠 것으로 전망된다. 다만, 현행 전자금융감독규정이 여전히 망분리를 보안의 근간으로 고수하고 있다는 점을 고려할 때, 공공 분야의 유연화 조치가 금융 규제 체계로까지 온전히 전이되었다고 판단하기에는 아직 시기상조적인 측면이 있다.

---

19) 한국인터넷진흥원, “ISMS-P 인증기준”(2024.12 개정), 4.3.3 네트워크 구분, 4.3.4 접속통제. “망분리 명문 규정 없으나 네트워크 분리 권고.”-

20) 자본시장연구원, “금융회사의 망분리 규제 현황 및 개선방향”, KCMI 24-26, 2024.11, pp.42-48. “ISMS 실무심사에서 내부망-외부망 분리 실질적 평가척도화.” -

21) 행정안전부고시 제2025-79호, 「행정기관 및 공공기관의 클라우드컴퓨팅서비스 이용 기준 및 안전성 확보 등에 관한 고시」, 제11조 및 제11조의2.-

## 5. 현행 망분리 규정의 규범적 구조와 문제점

현행 망분리 규정의 규범구조는 단순한 기술적 요구사항을 넘어, 규제의 설계 원리 · 감독 방식 · 보안 아키텍처 전반과 구조적으로 연결되어 있다. 이를 체계적으로 분석할 때 도출되는 주요 쟁점은 다음과 같다.

1) 기술 특정성과 기술중립성 원칙의 충돌

망분리 규정은 네트워크 단절이라는 특정 기술적 수단을 사실상 필수 요건으로 강제하는 구조를 취하고 있는데, 이는 규제의 초점을 특정 수단에 고착시키기보다 '보호 결과'의 실질에 두어야 한다는 기술 중립성 원칙과 정면으로 충돌한다. 이와 같은 기술 특정적 규제 설계는 고도화된 대체 보안 기술이 규제 체계 내로 유연하게 편입되는 것을 저해할 뿐만 아니라, 비약적인 기술 발전 속도를 규범이 수용하지 못하는 이른바 '규제의 경직성'을 심화시킨다. 특히 클라우드, VDI, DaaS 등을 활용한 현대적 보안 아키텍처는 물리적 네트워크 단절 없이도 데이터 접근에 대한 정밀한 통제가 가능함에도 불구하고, 기술 특정성에 매몰된 현행 망분리 규정하에서는 이러한 대안적 기술들이 법적 실효성을 온전히 인정받기 어려운 실정이다.[22]

2) 위험 기반 접근의 부재와 비례성 부족

글로벌 사이버 보안 규범의 핵심은 보호 조치를 데이터와 환경의 '위험도'에 따라 차등적으로 적용하는 위험 기반 접근법(Risk-Based Approach, RBA)에 있다. NIST의 위험 관리 프레임워크(RMF) 및 사이버 보안 프레임워크(CSF) 역시 위험도를 중심으로 보안 통제 항목을 설정하는 것을 대원칙으로 삼고 있다.[23] 그러나 현행 망분리 규정은 데이터의 민감도나 업무의 성격, 접근 주체의 위해 성향 등을 도외시한 채 일률적인 통제만을 강제함으로써 법익의 균형을 꾀하는 비례성 원칙을 충실히 이행하지 못하고 있다. 그 결과 위험도가 낮은 업무에는 과도한 규제 준수 비용이 전가되는 반면, 클라우드와 AI가 주도하는 고위험 업무 영역에서는 오히려 실질적인 통제 공백이 초래될 우려가 크다. 이는 결과적으로 국제적 가이드라인이 지향하는 '위험 기반 사이버 보안'의

22) 법무법인(유) 세종, 「금융사도 생성형 AI를 활용할 수 있도록, 망분리 제도가 완화될 예정입니다」, SHIN & KIM 뉴스레터, 2024. (https://www.shinkim.com/kor/media/newsletter/2533)-

23) 법무법인(유) 광장, "「전자금융감독규정」 개정 - 자율보안 토대 마련", 「Lee & Ko 뉴스레터」, 2025. 2. 19.https://www.leeko.com/newsl/digitalfinance/202502_2/202502.pdf-

본질적 가치와 정면으로 배치되는 대목이라 할 수 있다.[24]

3) 클라우드 · SaaS 환경과의 낮은 정합성

클라우드와 SaaS가 주도하는 현대적 IT 환경에서 '내부망과 외부망'이라는 이분법적 경계 설정은 기술적으로 그 유효성을 점차 상실하고 있다. 이에 따라 네트워크 경계가 무력화된 환경하에서 단말기의 접속 여부와 같은 외형적 요소만으로 보안 수준을 가늠하는 것은 실효적인 통제 기제로 기능하기 어렵다. 이와 관련하여 싱가포르 금융감독청(MAS)은 TRM 가이드라인을 통해 데이터 암호화, 접근 제어, 감사 및 모니터링 등 데이터 단위의 직접적인 통제를 보안 정책의 중핵으로 설정할 것을 명시하고 있다.[25] 결국 이는 망분리를 경직된 필수 요건으로 강제하지 않으면서도 실질적인 정보 보호를 도모하는 대안적 규제 모델을 제시한다는 점에서 시사하는 바가 크다. 나아가 미국 CISA의 TIC(Trusted Internet Connections) 3.0 프레임워크는 클라우드와 SaaS 환경을 전제로 한 보안 모델을 제시하며, 물리적 망분리 대신 대체 통제와 마이크로 세그멘테이션을 통한 정밀한 데이터 경로 제어에 집중하고 있다.[26] 이러한 국제적 표준의 변화는 네트워크 단절에만 고착된 한국의 현행 규제 방식이 이미 변화된 기술적 실재와 상당한 괴리를 보이고 있음을 방증한다고 볼 수 있다.

4) 규제의 경직성 및 개정 지연

무엇보다 기술의 비약적인 발전 속도를 규제 개정의 시차가 따라잡지 못하는 현상은 사이버 보안 분야 전반의 고질적인 난제로 지적되고 있다. 실제로 미국과 EU 등 주요국에서도 규제 관성이 디지털 혁신의 저해 요인으로 작용하고 있다는 논의가 지속되어 왔으며, 이러한 한계는 한국의 망분리 규정에서도 고스란히 재현되고 있다. 특히 기술 및 산업 환경이 클라우드, AI, API 중심의 개방형 구조로 급격히 재편되는 상황에서, 기존의 망분리 규정은 변화의 속도와 수용 방식 측면에서 시대적 요구를 온전히 담아내지 못하고 있는 실정이다. 결과적으로 이러한 규제의 경직성은 장기적으로 보안 통제의 실효성을 저하시킬 뿐만 아니라, 국내 산업의 글로벌 경쟁력마저 잠식하는 부정적 기제로 작용할 우려가 크다고 보여 진다.[27]

---

24) 법무법인(유) 세종, 「금융사도 생성형 AI를 활용할 수 있도록, 망분리 제도가 완화될 예정입니다」, SHIN & KIM 뉴스레터, 2024.

25) MAS, "Technology Risk Management Guidelines(TRM)", 2024, 제1.1조.

26) CISA, Trusted Internet Connections (TIC) 3.0 – Cloud Use Case, 2023.

## 6. 규제 패러다임의 전환 필요성

2025년 개정을 통해 전자금융감독규정 제15조는 연구 · 개발 목적 등에 한하여 '망분리 대체 정보보호통제' 개념을 도입하였다. 그러나 이는 망분리 의무라는 규범적 원칙을 유지한 채, 감독기관 승인 하에서만 허용되는 제한적 예외에 그친다. 따라서 본질적으로는 기술특정적 규제 구조가 그대로 유지되고 있으며, 위험 기반 접근이나 데이터 중심 보안 패러다임이 규제의 기본 원칙으로 전환되었다고 평가하기는 어렵다. 본 연구가 제시하는 전환 모델은 이러한 '예외적 완화'가 아니라, 규범 구조 자체의 전면적 재설계를 요구한다.

이와 같은 평가를 전제로 할 때, 지금까지 살펴본 바와 같이 현행 망분리 규정은 도입 당시의 기술 환경에서는 유효한 방어 기제로 기능하였으나, 클라우드와 AI 중심의 현행 정보처리 생태계에서는 그 규범적 전제가 한계에 봉착했음을 부정할 수 없다. 특히 네트워크 경계에 함몰된 현행 보호 체계는 데이터의 이동성이 극대화된 작금의 현실을 온전히 담아내지 못하고 있다. 이러한 괴리는 단순히 기술적 부적합의 문제를 넘어, 기술 중립성 · 비례성 · 위험 기반 규율이라는 현대 정보보호법제의 핵심 원칙과도 조응하지 못하는 구조적 결함을 드러내는 것으로 보인다.

더 나아가, 특정 기술적 수단을 강제하는 경직된 규제 설계는 대체 보안 기술의 수용을 가로막아 규제의 적응성을 저해할 뿐만 아니라, 위험도와 무관한 일률적 통제로 인해 과잉 규제와 규제 공백이라는 모순적 결과를 초래하고 있다. 무엇보다 '내 · 외부'의 경계가 무너진 환경에서 단말기 접속 여부에만 매몰된 현행 기준은 기술적 실재와 동떨어진 규제적 관성에 가깝다. 나아가 명확한 대체 통제 기준의 부재는 피규제자의 법적 예측 가능성을 저해하며, 결국 기술 발전과 규제 개정 사이의 시차를 더욱 벌리는 악순환을 낳고 있다. 결국 망분리 규정은 그간의 기여에도 불구하고, 이제는 데이터 중심의 보안 패러다임을 수용할 수 있는 규범 구조의 전면적 재정립이 필요한 시점에 도달했다.

본 연구에서의 비판적 검토는 단순한 요약을 넘어, 망분리 규제가 새로운 정보 생태계 내에서 어떠한 논리적 토대 위에 재구성되어야 하는지를 밝히는 데 의의가 있다. 이를 바탕으로 다음 장에서는 데이터 중심 보안과 망분리 규제 간의 구체적인 충돌 양상을 분석하고, 향후 규제 개선의 법 · 정책적 지향점을 제시하고자 한다.

---

27) OECD, Regulatory Policy Outlook, 2021.

## Ⅳ. 데이터 중심 보안 체계와 현행 망분리 규정 간의 규범적 충돌

데이터 중심 보안이 정보보호의 새로운 패러다임으로 자리 잡으면서, 기존 망분리 규정이 전제해 온 위험 관리 모델 및 기술 구조와의 충돌이 본격화되고 있다. 특히 네트워크 경계 중심의 전통적 방식은 고도화된 데이터 보호 요구를 수용하는 데 한계를 보이며 규제 전반에서 구조적 긴장을 발생시키고 있다. 이러한 충돌은 단순한 기술적 불일치의 문제가 아니라, 보호 대상의 설정, 통제 방식의 구조, 규제 설계 원리라는 규범적 차원에서 발생하는 문제로 이해될 수 있다. 이는 서론에서 제시한 바와 같이 보호 대상 설정 기준의 전환, 통제 방식의 구조 변화, 규제 설계 원리의 변화라는 세 가지 규범적 분석 틀에 따라 체계적으로 파악될 수 있다. 이하에서는 이러한 분석 틀에 기초하여 각 쟁점을 구체적으로 검토한다.

### 1. 보호대상 설정 기준의 전환과 망분리 규정의 한계

현행 망분리 규정은 내부 업무망과 외부 인터넷망을 물리적·논리적으로 차단하여 악성코드 유입이나 사이버 공격을 원천 봉쇄하는 것을 핵심 목표로 한다. 이러한 방식은 네트워크 경계를 보안의 절대적 기준으로 삼는 전통적인 '경계 기반 보안 모델'을 충실히 반영한 결과라 할 수 있다. 반면 데이터 중심 보안은 네트워크의 분리 여부보다는 데이터 자체에 대한 통제에 보호의 중심을 두며, 접근권한 관리, 암호화, 감사기록(log) 작성, DCAP 등 데이터 단위의 보호조치를 핵심 요소로 한다.[28] 이러한 차이는 보호 대상의 설정 기준이 '공간적 경계'에 있는지, 아니면 '정보 객체 자체'에 있는지에 관한 규범적 차이로 이해될 수 있으며, 이는 단순한 기술 선택의 문제가 아니라 정보보호 체계의 기본 구조를 결정하는 기준이라는 점에서 중요한 의미를 가진다. 이러한 접근은 데이터가 어떤 주체에 의해 어떤 맥락에서 처리되는지를 지속적으로 검증한다는 점에서, 보호 대상의 설정 기준부터 기존 망분리 규정과 본질적인 궤를 달리하고 있다.

이러한 기준의 차이는 결국 두 체계 간의 구조적 긴장을 야기하고 있다. 우선, 망분리 규정이 네트워크 단절이라는 정적 구조에 의존하는 반면, 데이터 중심 보안은 데이터의 흐름과 이용을 전제로 한 동적 통제를 지향한다. 또한,

28) NIST, Zero Trust Architecture, SP 800-207, 2020, p. 3.

두 방식 모두 정보 보호라는 동일한 목적을 지니고 있음에도 규제 수단이 상이하여, 실무적으로는 중복되거나 과잉된 규제 비용을 발생시킬 우려가 있다. 무엇보다 네트워크 중심의 고정된 방식은 데이터 활용 방식과 위협 양상이 급변하는 현대 정보 환경의 다양성을 충분히 반영하기에는 구조적인 한계가 뚜렷하다고 볼 수 있다.

결국 망분리 규정과 데이터 중심 보안 체계는 정보 보호라는 궁극적인 가치를 공유하면서도, 보호 대상을 정의하는 기준과 이를 실현하는 수단에 있어 근본적인 차이를 보이기 때문에, 이와 같은 차이는 단순히 기술적인 불일치에 그치는 것이 아니라, 망분리 규정이 전제해 온 보안 모델 자체가 변화된 정보처리 환경에서도 여전히 타당한가에 대한 근본적인 의문이 생길 수밖에 없다.[29]

## 2. 위험기반 규제원칙과 망분리 규정의 긴장관계

현행 망분리 규정은 정보의 민감도나 업무의 위험 수준에 관계없이 내부망과 외부 인터넷망의 분리를 원칙으로 하는 일률적 통제 구조를 취하고 있다. 이에 따라 내부망은 원칙적으로 인터넷과 물리적·논리적으로 차단되며, 예외적인 연결조차 엄격한 사전 요건과 제한적 조건하에서만 허용된다. 이러한 방식은 규제의 명확성과 집행 가능성 측면에서는 강점을 지니지만, 위험도에 따라 통제 강도를 차등화하는 현대적 정보보호 규제 흐름과는 상당한 괴리를 보이고 있다.[30]

반면 데이터 중심 보안 체계는 '위험 기반 접근' 원칙에 따라 보호 조치를 설계한다. 즉, 데이터의 민감도와 접근 주체의 신뢰 수준, 처리 목적 및 맥락 등을 종합적으로 고려하여 통제 강도를 차등화하는 방식이다. 이에 따라 중요도가 높은 정보에는 강화된 접근 제어와 감사를 적용하고, 위험이 낮은 영역에서는 효율성을 고려해 유연한 통제를 허용한다. 이러한 접근은 보안 목표를 달성하면서도 불필요한 과잉 규제를 방지할 수 있는 합리적인 구조를 제공하고 있다. 이처럼 상이한 위험 평가 방식은 현행 망분리 규정과 위험 기반 규제 원칙 사이에 규범적 긴장을 발생시킨다. 우선, 위험 수준과 무관하게 획일적인 통제를 강제하는 망분리 방식은 자칫 규제 목적에 비해 과도한 비용을 발생시켜 비례성 원칙을 저해할 소지가 있다. 또한, 망분리의 일률적 구조는 탄력적

29) 김도형, "금융회사 제로트러스트 모델 적용방안에 대한 연구", 「정보보안논문지」 제24권 제4호, 2024, 68-69면.
30) 성승제, 앞의 글, 126면.

인 규범 설계를 지향하는 위험 기반 접근을 제도적으로 수용하는 데 근본적인 한계를 지닌다. 마지막으로 통제 강도의 획일화는 보안 자원의 효율적인 배분을 가로막아, 결과적으로 조직 전체의 정보 보호 역량을 상향 평준화하는 데 오히려 장애가 될 우려가 있다.

결국 데이터 중심 보안 체계는 위험 기반 접근 원칙에 따라 통제 강도를 차등화함으로써, 현행 망분리 규정의 획일적·정태적 구조를 보완할 수 있는 대안적 규범 모델을 제시한다. 이러한 관점에서 볼 때, 망분리 규정은 단순히 기술적 보안 수단에 머무를 것이 아니라, 현대 정보보호의 핵심 원칙인 위험 기반 규제와의 조화와 공존을 중심으로 전면적인 재검토가 이루어져야 할 것이다.

## 3. 기술발전 수용성 측면에서 본 망분리 규정의 규범적 한계

현행 망분리 규정은 단말기의 인터넷 접속 차단, 망별 PC 분리 사용, 망 간 데이터 전송 제한 등 특정 기술적 구현 방식을 규범적 요건으로 명시하고 있다.[31] 이와 같은 규제 구조는 특정 기술을 사실상 유일한 보호 수단으로 전제한다는 점에서 기술 중립성 원칙과의 긴장을 발생시키며, 기술 발전에 따른 대체 수단의 등장 가능성을 구조적으로 제한하는 효과를 초래한다. 이러한 방식은 보안 수준을 정량적으로 확보하고 집행의 명확성을 높인다는 장점이 있다. 그러나 보안 목표의 실질적 달성 여부보다 특정 수단의 채택 자체를 규제 기준으로 삼는다는 점에서, 현대 정보보호법제의 대원칙인 기술 중립성 원칙과 충돌할 소지가 크다.

기술 중립성 원칙은 동일한 규제 목적을 달성할 수 있는 한, 구체적인 기술 수단의 선택권은 피규제자의 자율에 맡겨야 한다는 규범적 요청을 핵심으로 한다. 그러나 현행 망분리 규정은 특정 기술 구조를 사실상 유일한 보안 표준으로 강제하고 있다. 이로 인해 기술 발전에 따라 등장하는 새롭고 동등한 수준의 대체 보안 수단들을 규제 체계 내로 수용하는 데 구조적인 한계를 드러내고 있다.[32]

이에 반해 데이터 중심 보안 체계는 암호화, 접근통제, DCAP, ZTA 등 다양한 기술을 결합하여 보호목표를 달성할 수 있도록 설계되어 있으며, 특정 기

31) 전자금융감독규정, 제15조 제1항 및 시행세칙.

32) Asia cloud computing association, 국내 금융권 망분리 규제의 영향 및 개선방향 2024, pp. 4-6 https://asiacloudcomputing.org/wp-content/uploads/2024/06/ACCA-2024_NetworkSeparationInSouthKorea_KR.pdf?utm_source=chatgpt.com

술의 채택 여부보다는 전체적인 보호수준의 확보를 중심으로 통제 구조를 형성한다. 기술이 발전함에 따라 동일한 보호목표를 달성할 수 있는 수단이 다원화될수록, 규제 역시 그 적용 방식에 있어 보다 유연하게 조정될 수 있다는 점에서 데이터 중심 보안 체계는 기술중립적 규제 설계와 높은 친화성을 가진다고 평가할 수 있다.

그럼에도 현행 망분리 규정은 특정 기술만을 규범적으로 승인하는 방식에 고착되어 있어, 혁신적인 보안 기술이 등장하더라도 이를 기존 체계의 대체 수단으로 인정하는 데 소극적이다. 일례로 VDI(가상 데스크톱 인프라) 기반의 중앙 집중식 관리나 사용자·행위 분석 기반의 고도화된 접근 제어는 기존 단말기 중심의 망분리보다 우수한 보안성을 제공할 수 있음에도, 현행 규정상으로는 예외적인 수단으로만 제한적으로 수용될 뿐이다.

이러한 규제 구조는 기술 발전과 제도 변화 사이의 시차를 심화시키며, 결과적으로 규제의 실효성과 적합성을 저해하는 원인이 된다. 따라서 망분리 규정은 특정 기술의 고착화에서 벗어나, 보안 목표의 달성 여부를 기준으로 다양한 기술적 대안을 포괄할 수 있는 유연한 규범 구조로 전환되어야 할 것이다.

## 4. 디지털 업무환경 변화와 망분리 규정의 적합성 문제

현행 망분리 규정은 단말기의 인터넷 접속을 제한하거나 차단함으로써 정보자산을 보호하는 보호모델을 기본 전제로 하고 있다.[33] 이러한 규제 구조는 내부업무가 폐쇄적인 네트워크 환경에서 수행되고, 외부 네트워크와의 접점이 제한적인 상황을 상정한 것으로 이해할 수 있다. 그러나 최근의 정보처리 환경은 클라우드 및 SaaS 기반 서비스의 확산을 중심으로 급속히 변화하고 있으며, 생성형 인공지능을 포함한 다수의 디지털 업무 도구 역시 상시적인 인터넷 연결을 전제로 작동하고 있다.

이와 같은 환경 변화 하에서 네트워크의 물리적·논리적 단절을 핵심 보호수단으로 하는 망분리 규정은 업무수행 자체와 직접적인 긴장관계를 형성한다. 예컨대 금융회사가 외부 데이터 분석 도구, API 연동 서비스, 협업 플랫폼 등을 활용하기 위해서는 단말기의 인터넷 접근이 필수적인 경우가 많으며, 인공지능 기반의 업무 자동화나 데이터 분석 서비스 역시 외부 네트워크와의 연계를 전제로 한다.[34] 이러한 현실은 망분리 규정이 예정한 업무 수행 방식과 실

33) 전자금융감독규정, 제15조 제1항 제5호.

제 업무 환경 간의 괴리를 명확히 드러낸다고 볼 수 있다.

결과적으로 디지털 업무환경의 변화는 망분리 규정이 전제하고 있는 보호모델의 사실적 기반을 약화시키고 있으며, 규제가 예정한 보호수단이 오히려 업무의 효율성과 정보 활용을 과도하게 제한하는 결과를 초래할 가능성도 배제하기 어렵다.[35] 이는 망분리 규정의 문제를 단순한 기술적 적합성의 차원을 넘어, 변화된 정보처리 환경에 비추어 규제의 실효성과 적합성이 여전히 유지될 수 있는지에 대한 규범적 재검토의 문제로 전환시킨다. 따라서 디지털 업무환경을 전제로 한 현대적 정보보호 체계 하에서는, 네트워크 단절 자체를 보호의 핵심 수단으로 설정하는 규제 방식이 여전히 타당한지 여부에 대한 근본적인 검토가 요구된다.

## 5. 망분리 규정의 운영상 비용구조와 효율성 문제

현행 망분리 규정은 내부 업무망과 외부 인터넷망의 엄격한 분리를 원칙으로 하는바, 이는 필연적으로 업무환경의 이중화와 네트워크 인프라의 중복 구축을 강제하여 상당한 운영 비용을 발생시킨다. 특히 이러한 비용 부담은 인프라 규모가 방대한 대형 금융기관일수록 더욱 가중되는 양상을 보인다. 나아가 데이터의 빈번한 이동과 결합을 전제로 하는 연구·개발이나 인공지능(AI) 활용 업무의 경우, 망간 데이터 전송 절차의 복잡성으로 인해 업무 효율성이 구조적으로 저해되는 결과에 이르고 있다.[36]

반면, 데이터 중심 보안 체계는 단일 단말 혹은 통합 업무환경 하에서 데이터 접근 권한에 대한 중앙집중적 관리·집행 구조를 채택한다. 이는 물리적·논리적 망의 이중화 조치 없이도 보호 목표를 효과적으로 달성할 수 있게 하며, 운영 및 관리 측면에서 우수한 유연성을 제공한다. 특히 VDI나 DaaS 등의 가상화 기술은 개별 단말기의 보안 의존도를 낮추는 대신, 중앙에서 정책을 일괄 집행함으로써 보안성과 업무 효율성의 조화를 도모한다.

이러한 구조적 차이는 망분리 규제와 데이터 중심 보안 체계가 상이한 비용구조 및 운영 원리에 기반하고 있음을 시사한다. 기존 망분리 규정이 막대한

---

34) 황세운, “금융회사의 망분리 규제 현황 및 개선방향”, KCMI 24-26, 자본시장 연구원, 2024, 16-17면.

35) 오정주·이환수, “디지털 금융산업 활성화를 위한 망분리 규제 개선방안”, 한국금융학회지 제21권 제5호, 한국융합보안학회, 2021, 51-53면

36) 금융위원회, 「금융분야 망분리 개선 로드맵」, 2024.08.13, 2-5면, (https://www.fsc.go.kr/no010101/82885)

고정 비용과 경직된 운영 부담을 수반하는 것과 달리, 데이터 중심 보안 체계는 보안 수준을 견지하면서도 비용 구조의 탄력적 설계를 가능케 한다. 따라서 현행 망분리 규정이 입법 목적 달성에 비추어 과도한 비용을 강제하고 있지는 않은지, 동일한 목적을 보다 낮은 사회적 비용으로 달성할 수 있는 대체 수단이 존재하는지에 대한 비판적 검토가 요구된다.

결국 망분리 규정의 비용 구조는 규제의 실효성뿐만 아니라, 행정법상 효율성 및 비례성 원칙의 관점에서 재평가되어야 한다고 생각한다. 이러한 논의는 향후 망분리 규제의 존치 여부나 보완, 혹은 대안적 규범 체계로의 전환을 결정 짓는 핵심적인 법리적 판단 근거가 될 것이다

## Ⅴ. 주요 국가 및 국제기구의 데이터 중심 보안 정책 비교

데이터 중심 보안 체계는 국제적으로 사이버보안 정책의 핵심 원칙으로 자리잡아가고 있으며, 이에 따라 주요 국가 및 국제기구는 기술 중립성, 위험 기반 접근, ZTA를 중심으로 규범체계를 재편하고 있다. 본 장에서는 미국, EU, 일본, 싱가포르 등 주요 규제권역의 제도와 정책을 비교하여, 한국의 망분리 규정과의 구조적 차이를 검토하고자 한다.

### 1. 미국: 제로 트러스트 아키텍처(ZTA) 도입과 기술 중립적 규제체계

#### 1) 행정명령을 통한 연방정부 보안 패러다임의 전환

미국은 2021년 바이든 행정부가 발표한 「행정명령 제14028호」[37]를 통해 국가 사이버보안 정책을 근본적으로 재편하였는데, 이는 기존의 경계 중심 보안 모델을 대체하는 새로운 규범적 패러다임으로서 ZTA를 공식 채택한 것이다.

(1) 규범적 근거와 정책적 목표 행정명령 제3조는 클라우드 서비스로의 전환과 함께 ZTA 구현을 연방기관의 의무로 명시하고 있다.

행정명령 제14028호 제3조(연방정부 사이버보안의 현대화) “(b) 연방정부는 제로 트러스트 아키텍처(Zero Trust Architecture)를 향한 진전된 조치를 취해야 한다. (c) 연방정부가 클라우드 기술을 현대화하고 구현함에 있어, 보안 모

37) Executive Order 14028, Improving the Nation’s Cybersecurity. 2021.

범 사례와 제로 트러스트 아키텍처 내에서의 기술적 진보를 보호하는 방식으로 추진해야 한다."

이와 같은 조치는 단순한 기술적 권고를 넘어 연방기관 전체의 보안 거버넌스를 데이터 · 사용자 · 기기 중심의 동적 통제로 전환하라는 규범적 명령의 성격을 갖는다고 볼 수 있다.

(2) 단계적 구현 및 거버넌스의 통합 행정명령을 구체화하기 위해 관리예산국(OMB)과 사이버보안 및 인프라 보안국(CISA)은 각각 「연방 제로 트러스트 전략」[38]과 「제로 트러스트 성숙도 모델」[39]을 발표하였다. 이는 연방기관이 2024년까지 ZTA를 단계적으로 구현하도록 요구하며, 기관의 예산 책정 및 감사 기준에 ZTA 원칙을 통합함으로써 '망을 신뢰하지 않는다(Never Trust)'는 원칙을 제도적으로 명문화하고 잇다.

2) 금융분야의 기술 중립적 규제체계 확립

미국의 금융 규제체계는 특정 보안기술의 채택 자체를 일률적으로 강제하기보다, 금융기관이 자율적인 위험평가를 바탕으로 적절한 기술적 · 관리적 통제를 설계 · 운영하도록 요구하는 구조를 취하고 있다. 이러한 점에서 미국의 금융 정보보호 규율은 기술특정적 규제보다는 위험기반 접근에 가까우며, 결과적으로 기술중립성 원칙과 높은 친화성을 가진다고 볼 수 있다.

(1) FFIEC IT Examination Handbook의 규율 방식

연방금융기관검사위원회(FFIEC)의 「IT Examination Handbook: Information Security Booklet」은 금융기관의 정보보호 프로그램이 기관의 위험평가에 기초하여 수립 · 운영되어야 함을 전제로 하며, 정보자산 보호를 위한 관리적 · 기술적 통제의 적정성을 종합적으로 점검하는 방식을 취한다.[40] 이 문서는 정보보호 프로그램의 목적, 범위, 통제체계, 위험관리, 모니터링, 테스트 및 대응 절차 등을 평가하도록 하고 있으나, 망분리와 같은 특정 기술수단을 일률적 · 절대적 의무로 명시하지는 않는다. 따라서 FFIEC 체계는 보호목표의 실질적 달성 여

38) OMB Memorandum M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles.
39) CISA, Zero Trust Maturity Model Version 2.0. 2023.
40) FFIEC, IT Examination Handbook: Information Security Booklet, 2016.

부를 중시하는 결과중심적 감독방식으로 볼 수 있을 것이다.

(2) 거버넌스 중심의 통제 구조

또한 FFIEC의 「IT Examination Handbook: Management Booklet」은 정보기술 및 정보보호에 관한 책임이 단순히 실무 부서에 한정되지 않고, 이사회와 경영진의 감독 및 승인 체계와 긴밀히 연결되어 있음을 보여준다.[41] 즉 금융기관은 정보보호 프로그램과 정보기술 리스크 관리체계를 조직 차원의 거버넌스 아래 운영하여야 하며, 감독당국은 개별 기술의 사용 여부 자체보다는 그러한 거버넌스가 적절히 작동하고 있는지, 그리고 결과적으로 위험이 효과적으로 관리되고 있는지를 중점적으로 평가한다. 이는 기술의 세부 구현 방식을 직접 규정하지 않으면서도 금융기관으로 하여금 적정한 보호수준을 확보하도록 하는 제도적 균형을 보여준다.

(3) 한국 망분리 규정과의 비교 및 시사점

미국의 이러한 규율체계는 한국의 망분리 중심 규제와 뚜렷한 대비를 이룬다. 첫째, 한국이 네트워크 분리를 중심으로 보호체계를 구성하는 데 비하여, 미국은 위험평가와 거버넌스를 토대로 데이터, 사용자, 시스템 및 업무환경 전반에 대한 통제를 설계한다. 둘째, 미국은 특정 보안기술에 독점적 규범 지위를 부여하지 않으므로 기술 변화에 대한 적응성이 높다. 셋째, 규제 판단의 기준이 특정 수단의 채택 여부가 아니라 위험완화의 실효성에 놓여 있다는 점에서 결과중심적 성격이 강하다. 이러한 비교는 향후 한국의 정보보호 규제체계가 망분리라는 특정 수단의 강제에서 벗어나, 데이터 중심 보호와 위험기반 통제를 수용하는 방향으로 재구성될 필요가 있음을 시사한다.

## 2. EU: 데이터 보호와 사이버보안의 위험 기반 접근

1) GDPR의 데이터 중심 보호원칙과 기술 중립성

유럽연합의 「일반개인정보보호법(GDPR)」은 개인정보 처리 전반을 규율하며, 네트워크 경계라는 물리적 장소성에 함몰되지 않고 '데이터 처리 과정' 자체를 보호의 중심으로 삼는 데이터 중심 보안 패러다임을 법제화하고 있다.

41) FFIEC, IT Examination Handbook: Management Booklet, 2015.

(1) 규범적 근거와 보안 원칙

GDPR 제5조는 데이터 최소처리, 목적 제한, 무결성 및 기밀성 보장의 원칙을 선언하며, 이는 데이터가 수집 · 저장 · 이용 · 이동되는 전 과정에서 일관된 법적 · 기술적 통제가 적용되어야 함을 의미한다. 특히 제32조는 특정 보안 기술을 강제하지 않고 위험도에 따른 최적의 조치를 선택하도록 규정하고 있다.

GDPR 제32조(처리의 안전성) 제1항 "컨트롤러와 프로세서는 최신 기술 수준(state of the art)과 구현 비용, 처리의 성격 · 범위 · 맥락 및 목적, 그리고 자연인의 권리와 자유에 대한 다양한 가능성과 심각성을 가진 위험을 고려하여, 위험에 적절한 수준의 보안을 보장하기 위한 기술적 · 관리적 조치를 시행하여야 한다."

(2) 데이터 중심 통제 수단의 제도화

동 조항은 안전성 확보를 위한 예시적 수단으로 암호화(encryption)와 가명처리(pseudonymization) 등을 명시하고 있다.[42] 이는 보호 의무의 기준을 내부망과 외부망이라는 공간적 구조에 두는 것이 아니라, 데이터 자체의 민감도와 실제적 위험 요소에 두고 있다는 점에서 전형적인 데이터 중심 규율의 성격을 가지고 있다. 이와 같은 구조는 네트워크 단절을 기본 통제로 설정하는 경계 중심 보안 모델과 본질적으로 차별화 될 수 있을 것이다.

2) NIS2 지침을 통한 위험 기반 보안체계의 확립

2024년부터 전면 시행된 「NIS2 지침(Directive 2022/2555)」[43]은 유럽 전역의 필수 및 중요 엔티티를 대상으로 통합적인 사이버보안 위험 관리 의무를 부과하며 위험 기반 접근법을 명문화하였다.

(1) 위험 관리 의무의 구체적 내용

NIS2 제21조는 보안 조치의 선택 기준을 특정 기술의 도입 여부가 아니라, 보호가 필요한 자산의 중요도와 조직이 직면한 위험 수준에 따라 결정하도록 요구한다.

NIS2 지침 제21조(사이버보안 위험 관리 조치) 제2항 "제1항에 따른 조치는

42) GDPR, Art. 32(1)(a): "the pseudonymisation and encryption of personal data."
43) NIS2 Directive 2022/2555, 2022.

위험 기반 접근법(risk-based approach)에 기초하여야 하며, 최소한 다음 각 호를 포함하여야 한다: (a) 정보 시스템 보안 및 위험 분석 정책, (b) 사고 처리, (c) 비즈니스 연속성 관리, (d) 공급망 보안... (g) 암호화 및 가용성 확보 정책."

(2) 거버넌스 및 책임의 현대화

NIS2는 사이버보안의 책임을 기술 부서에 국한하지 않고 경영진의 관리·감독 의무로 확장하였다. 이는 규제의 초점을 특정 기술방식의 이행 여부에서 '적정한 보안 수준의 확보'라는 결과 중심으로 전환한 것이다. 결과적으로 조직은 망분리 외에도 제로 트러스트(Zero Trust) 등 다양한 기술적 대안을 위험 평가 결과에 따라 유연하게 채택할 수 있게 된다.

3) 한국 망분리 규정과의 비교법적 고찰

유럽연합의 규범 구조는 한국의 망분리 중심 규제와 비교할 때 다음과 같은 법적 시사점을 제공하고 있다. 먼저, 보호 객체의 실질화이다. 한국은 네트워크 구조라는 물리적 요소를 기준으로 보안 체계를 구성하나, EU는 데이터 및 업무의 위험도를 기준으로 보호 조치를 설계한다. 그리고, 기술 중립성의 보장이다. 특정 기술을 규범적으로 우월한 위치에 두지 않음으로써 기술 발전에 따른 보안 패러다임의 변화를 규제 체계 내로 원활히 수용하고 있다. 마지막으로, 비례 원칙의 실현이다. 획일적인 망분리 강제에서 벗어나 자산의 중요도에 따른 차등적 규제를 적용함으로써 규제의 합리성을 제고하고 있다.

## 3. 일본: 공공·금융부문의 점진적 ZTA 전환

1) 공공부문의 보안 패러다임 변화와 ZTA 도입

일본 정부는 공공부문 정보시스템 보안체계를 기존의 경계 기반 망분리 모델에서 탈피하여, 데이터 중심의 ZTA로 전환하는 정책을 추진하고 있다.

(1) 규범적 지침과 도입 배경

일본 정부 CIO 포털이 발행한 지침서[44]는 클라우드 활용 확대와 원격 근무의 증가 등 변화된 정보처리 환경을 반영하여, 전통적 경계형 보안모델의 한계

44) 政府CIO補佐官等,「政府情報システムにおけるゼロトラスト適用に向けた考え方」.2020.

를 지적하고 ZTA 적용 방안을 명시하고 있다.

「일본 정부 정보시스템에서의 제로 트러스트 도입 접근법」 “클라우드 서비스 및 모바일 업무 환경의 확산으로 인해 더 이상 내부망을 절대적 안전 영역으로 간주할 수 없다. 보안의 기준을 네트워크 경계가 아닌 사용자, 기기, 접근 행위, 데이터 상태라는 맥락적 위험 요소에 두고 지속적인 검증 체계를 구축하여야 한다.”

(2) 기술 특정적 규제에서 성과 중심 규제로의 이행

이러한 전환은 단순한 기술적 보완을 넘어 보안 규범의 기본 패러다임을 재설계하려는 시도로 평가할 수 있다. 일본 정부는 로그인 인증 강화, 권한 및 접근관리(IAM), 데이터 암호화, 실시간 접근 평가 등 다층적 보안 통제를 강조하며, 규제의 기준을 기술 방식이 아닌 ‘보호 성과’에 두고 있는데, 이는 기술 중립성과 위험 기반 접근 원칙을 공법적 체계 내로 수용하려는 시도로 해석될 수 있다.

2) 금융부문의 위험 기반 규제 체계

일본 금융청(Financial Services Agency, FSA)은 금융부문의 사이버보안 규율에 있어 망분리 중심의 획일적 통제보다는 정보자산의 중요도에 따른 위험 기반 접근을 강조하고 있다.[45]

(1) 보안 수준 평가의 핵심 항목

금융청이 매년 실시하는 「금융기관 사이버보안 리뷰」[46]에서는 금융기관의 보안 수준을 평가할 때 특정 기술 도입 여부가 아닌 거버넌스와 실질적 통제 능력을 검증하고 있다.

「금융기관 사이버보안 리뷰」 주요 평가 항목 “금융기관은 사이버 위협의 복잡성에 대응하기 위해 보호의 기준을 네트워크 경계가 아니라 정보자산 자체의 위험도에 두어야 한다. ID 및 접근관리(IAM), 로그 모니터링 체계, 데이터 암호화 및 엔드포인트 관리 등이 핵심적인 통제 요소가 된다.”

45) 金融廳, 「金融分野におけるサイバーセキュリティに關するガイドライン」, 2024.
46) 金融廳, 「金融分野におけるサイバーセキュリティ强化に向けた取組方針 (Ver.3.0) 」, 2022.

(2) 망분리의 규범적 지위 변화

일본 금융청은 망분리를 필수적 의무 사항으로 규정하지 않으며, 이를 다양한 보안 통제 수단 중 하나로 간주한다. 즉, 금융기관은 자사의 업무 특성과 위험 수준에 따라 최적의 기술 조합을 선택할 자율성을 가지며, 이는 “망분리=필수 보안수단”으로 인식되는 한국의 규제 구조와 명확히 대비되고 있다.

3) 비교법적 시사점

일본의 사례는 한국의 망분리 규제 체계에 대해 다음과 같은 교훈을 제공하고 있다. 먼저, 공공부문 정보시스템 보안의 현대화이다. 이는 내부망 단절만으로는 보안과 업무 효율성을 동시에 달성하기 어렵다는 점을 정부 스스로 인정하고 제도적 전환을 꾀하고 있다는 점은 주목할 만하다. 그리고, 기술 중립적 규제의 정착으로서, 특정 보안 기술이 규범적으로 독점적 지위를 갖지 않도록 하여 금융기관의 디지털 전환을 지원하고 있다. 마지막으로, 위험 기반 접근의 제도적 내실화이다. 이는 보호의 단위를 네트워크 구조에서 정보자산과 행위 중심으로 이동시킴으로써, 현대적 사이버 위협에 보다 실효성 있게 대응하는 규범적 기반을 마련하고 있다.

## 4. 싱가포르: MAS TRM 가이드라인을 통한 위험 기반 통제 체계

1) TRM 가이드라인의 규범적 프레임워크와 기술 리스크 관리

싱가포르 금융통화청(Monetary Authority of Singapore, 이하 ‘MAS’)은 2021년 개정된 「기술 리스크 관리 가이드라인(Technology Risk Management Guidelines, 이하 ‘TRM 가이드라인’)」[47]을 통해 금융기관의 정보보호 및 기술 리스크 관리에 관한 현대적 규범 체계를 제시하고 있다.

(1) 규제 철학의 전환

경계 보안에서 데이터 보안으로 동 가이드라인은 클라우드 및 제3자 서비스 이용 확대 등 급격한 디지털 전환 환경을 반영하여, 물리적 망분리라는 단일한 수단에 의존하기보다 데이터 중심의 통제와 위험 기반 접근을 핵심 축으로 설정하고 있다.

47) MAS, Technology Risk Management Guidelines(TRM). 2021.

MAS TRM Guidelines Sec 1.1 “금융기관은 기술 리스크 관리 프레임워크를 수립함에 있어, 단순히 특정 기술의 도입 여부에 집중하기보다 기관이 직면한 사이버 위협의 성격과 데이터의 중요도를 고려한 위험 기반 접근법(Risk-Based Approach)을 채택해야 한다.”

(2) 구체적 통제 조치 및 운영 원칙

TRM 가이드라인은 금융기관에 다음과 같은 실질적 보안 통제를 요구함으로써 규제의 실효성을 확보한다. 첫째, 데이터 저장 · 전송 · 처리 전 과정에 걸친 암호화 및 보호 체계 구축을 통해 데이터의 기밀성을 보장한다. 둘째, 신원 및 접근 관리(IAM)를 강화하여 사용자 · 기기 · 서비스별 최소 권한 원칙을 적용하도록 한다. 셋째, 공급망 보안을 강조하며 외부 API 및 제3자 서비스 제공자에 대한 사전 평가와 지속적 모니터링 의무를 부과한다. 마지막으로 기술적 변경 시 내부 거버넌스를 통한 위험 평가와 감사 절차를 필수적으로 거치도록 규정하고 있다.

2) 기술 중립성과 자율 규제 모델의 구현

싱가포르의 규정 구조는 특정 기술 수단(예: 망분리)을 강제하기보다, 금융기관이 스스로 위험 수준을 진단하고 적절한 통제 수단을 선택할 수 있는 ‘자율과 책임’의 원칙을 견지하고 있다.

(1) 적절성 중심의 규범 판단

MAS의 규제 체계에서 준수 여부는 특정 기술의 도입 여부가 아니라, 선택된 통제 수단이 해당 리스크를 완화하기에 ‘적절’한지, 그리고 ‘유지관리’가 실질적으로 이루어지고 있는지에 의해 판단된다. 이는 기술 방식 자체를 규제 기준으로 삼는 기술 특정적 규제와 대조되는 기술 중립적 규제 모델의 전형이다.[48]

(2) 디지털 금융 환경에의 적합성

다양한 클라우드 서비스와 오픈 API가 활용되는 현대 디지털 금융 생태계에서, 물리적 망분리 중심의 경계 보안은 내부 권한 오남용이나 제3자 리스크 대응에 한계를 가질 수밖에 없다. MAS는 이러한 현실을 법제도적으로 수용하

48) MAS TRM Guidelines – Section 3 (Governance), 2021.

여 ‘경계 보안’을 넘어선 ‘데이터 중심 위험 보안’ 체계를 확립하고 있다.[49]

3) 비교법적 시사점

MAS TRM 가이드라인은 데이터 중심 보안 모델이 법적 유효성을 가질 수 있음을 입증하는 대표적 국제 사례로서 다음과 같은 시사점을 제공한다. 먼저, 규제의 유연성과 적응성 확보로서. 기술 중립적 원칙을 통해 핀테크 혁신과 보안 강화라는 두 가지 목표를 동시에 달성하고 있다. 그리고, 리스크 기반 통제의 고도화이다. 이는 망분리라는 물리적 기준을 넘어 데이터의 흐름과 접근 주체에 기반한 동적 통제 모델을 제시하고 있다. 마지막으로, 거버넌스 중심의 책임 체계이다. 이를 위해 금융기관 스스로 위험을 평가하고 보안 설계를 최적화하도록 유도함으로써 조직 내부의 보안 내실화를 꾀하고 있다. 이는 향후 한국의 금융 보안 규제가 기술 변화에 발맞추어 재설계될 때 참고할 만한 핵심적 비교법적 지표가 될 수 있다고 생각한다.

## 5. 비교 평가 및 정책적 시사점

해외 주요국의 정보보호 규범과 한국의 망분리 규정을 비교분석한 결과, 양자 간에는 규제 설계의 철학적 기반과 보호의 단위, 기술 수용 방식에 있어 본질적인 구조적 차이가 존재한다. 이는 단순히 보안기술의 선택 문제를 넘어, 규범이 지향하는 보호 모델 자체가 상이함을 시사한다.

첫째, 기술 중립성 원칙의 적용 여부이다. 미국, EU, 싱가포르 등 주요국 규범은 보안의 목표를 기술 방식이 아니라 ‘보호의 결과’에 두는 기술 중립적 규율 구조를 견지한다. 암호화, 접근 통제, 모니터링 등 다양한 기술적 수단을 위험도에 따라 조합하도록 허용함으로써 규제의 유연성을 확보하고 있다. 반면 한국은 「전자금융감독규정」[50] 및 「정보통신망법」[51] 등에서 물리적 · 논리적 망분리를 직접 규정하여 특정 기술에 독점적 규범 지위를 부여하고 있으며, 이는 신기술 도입을 저해하는 규제의 경직성으로 이어진다.

둘째, 보호 단위와 통제 중심의 패러다임 차이이다. 해외 규범은 데이터 자체의 위험도와 처리 행위의 특성을 기준으로 하는 ‘데이터 중심 통제(Data-Centric Security)’를 핵심 축으로 삼는다. 이는 ZTA나 IAM 등을 통해 데이터

49) MAS TRM Guidelines – Section 7, 2021.
50) 전자금융감독규정 제15조 제1항 제3호 등 참조.
51) 정보통신망 이용촉진 및 정보보호 등에 관한 법률 제45조 및 관련 시행령 참조.

의 이동성을 보장하면서도 안전성을 확보하는 구조다. 반면 한국의 망분리 규정은 내부망과 외부망의 단절을 전제로 하는 '경계 기반 통제'에 집중하고 있어, 클라우드와 SaaS 등 플랫폼의 다양성이 확대된 현대 디지털 환경과의 정합성이 낮다.

셋째, 위험 기반 접근의 제도화 수준이다. 주요국은 기관의 규모, 산업 특성, 데이터의 민감도에 따라 차등적·비례적 보호 조치를 요구함으로써 규제의 실효성을 높이고 있다. 그러나 한국은 위험의 개별적 특성을 고려하지 않고 일률적인 망분리 의무를 부과하고 있어, 규제의 비례성 원칙 측면에서 한계를 드러내며 산업 전반의 비용 효율성을 저하시키고 있는 것이 현실이다.

결론적으로, 해외 주요국이 데이터 중심 보호와 기술 중립성, 위험 기반 규율이라는 현대적 원칙을 수용하여 규범을 재설계하고 있는 반면, 한국은 여전히 과거 침해사고 대응 논리에 기초한 네트워크 단절 모델에 머물러 있다.[52] 따라서 향후 한국의 정보보호 체계는 단순한 기술적 보완을 넘어, 규제 설계의 철학을 데이터와 사용자 중심으로 전환하고 위험도에 따른 유연한 기술 선택권을 보장하는 방향으로 근본적인 법제도적 재구조화가 이루어져야 한다. 이는 디지털 전환기 속에서 국가 사이버 보안의 실효성을 확보하고 산업 혁신을 지원하기 위한 필수적 과제라 생각한다.

## Ⅵ. 데이터 중심 보안을 위한 망분리 규정의 개정 방향

현행 망분리 규정이 직면한 구조적 한계는 단순히 지엽적인 예외 조항의 신설만으로 해결될 수 있는 성격의 것이 아니다. 데이터 중심 보안 체계로의 패러다임 이행은 규제의 기본 설계를 근본적으로 재구조화할 것을 요구하는바, 이하에서는 기술중립성 회복과 위험 기반 규율의 도입, 그리고 대체통제의 정식화 등을 중심으로 구체적인 입법론적 대안을 제시하고자 한다.

### 1. 결과 중심 규제로의 전환과 기술중립성의 확보

망분리 규정은 내부망과 외부망의 물리적 단절이라는 특정한 기술적 구현

52) 서병호, "주요국의 전자금융거래 규제 및 시사점: 사업자 분류 및 관련 주요 개념을 중심으로", KIF 이슈리포트, 한국금융연구원, 2025, 3-9면(https://www.kif.re.kr/kif4/publication/viewer?mid=10&vid=0&cno=347613)

방식을 규범적 요건으로 강제함으로써 보안 기술의 수용성을 저해해 왔다.[53] 이후 개정 방향은 특정 기술의 준수 여부가 아닌, '정보보호 수준의 실질적 확보'를 준거로 삼는 성과 중심 규제로의 전환을 지향해야 할 것이다. 이는 동일한 보호 목표를 달성할 수 있다면 구체적인 수단 선택은 기업의 자율에 맡겨야 한다는 기술중립성 원칙의 실질적 구현이며, 이를 통해 암호화나 신원 기반 접근 제어(IAM) 등이 적법한 보안 통제로 제도적 지위를 확보할 수 있는 법적 토대가 마련되어야 할 것이다. 이러한 방식은 미국의 FFIEC 감독 체계나 유럽연합의 NIS2 지침 등 글로벌 규범 흐름과 궤를 같이하며, 규제의 유연성과 기술 환경 변화에 대한 적응성을 동시에 확보하는 핵심적 방안이 될 수 있을 것이다.

## 2. 위험 기반(Risk-Based) 규율 체계의 제도적 정착

데이터 중심 보안 체계로의 규범적 이행을 위한 핵심적 선결 과제는 데이터의 민감도, 업무의 성격, 그리고 접근 주체의 위험 수준에 따라 보호 조치의 강도를 차등화하는 위험 기반 접근의 법제화이다. 기존의 획일적 망분리 규제는 기술적 환경의 변화를 수용하지 못하는 경직성을 노출해 왔으며, 이는 정보자산의 중요도와 무관하게 동일한 수준의 물리적 통제를 강제함으로써 자원 배분의 비효율성을 초래하였다.

위험 기반 접근은 제한된 보안 자원을 실제 위협이 집중된 고위험 영역에 전략적으로 배분함으로써 규제의 실효성을 제고하는 동시에, 저위험 영역에서의 불필요한 규제 비용을 절감하여 행정법상 비례성 원칙을 실현하는 합리적 경로가 될 수 있다. 이러한 체계의 제도적 모델로서 2026년 현재 공공부문에서 전면 시행 중인 다중보안체계(Multi-Level Security, 이하 MLS)에 주목할 필요가 있다. MLS는 정보자산의 가치와 영향도에 따라 보안 등급을 다음과 같이 세분화하여 통제 체계를 최적화한다. 첫째, 기밀(C, Confidential) 등급은 국가 안보나 외교적 기밀 등 고도의 민감 정보를 포함하며, 침입 경로의 원천적 차단을 위해 기존의 강력한 물리적 망분리 수준의 통제를 유지한다. 둘째, 민감(S, Sensitive) 등급은 유출 시 국민 생활 및 공공 안전에 지장을 줄 수 있는 정보로, 고도화된 대체 통제(VDI, IAM, 데이터 암호화 등)의 적용을 조건

53) Asia cloud computing association, 국내 금융권 망분리 규제의 영향 및 개선방향 2024, 5-6면.

으로 논리적 망분리 및 외부 클라우드와의 연동을 허용한다.[54] 셋째, 공개(O, Open) 등급은 대국민 서비스 등 일반 정보를 의미하며, 원칙적으로 망분리 제한 없이 자유로운 SaaS 활용과 업무 혁신을 보장한다.

이러한 등급제 모델은 금융권 규제 체계에도 시급히 이행되어야 한다. 단순히 특정 기술적 수단의 채택 여부를 규정하기보다, 법령상 데이터 민감도에 따른 세부 분류 체계를 수립하고 위험 평가 결과가 통제 수단의 선택과 강도를 정당화하는 법적 구조를 명시화해야 한다. 아울러 위험 평가 절차의 투명성과 책임성을 확보함으로써, 피규제 기관의 자율적 보안 설계와 감독 당국의 성과 중심 감독이 상호 보완적으로 작동하는 규제 거버넌스를 구축하는 것이 바람직하다.

### 3. 대체통제의 정식화와 실효성 확보

물리적 망분리를 원칙대로 적용하기 어려운 환경에서 동등하거나 그 이상의 위험 감소 효과를 제공하는 보안 조치를 의미하는 '대체통제'의 개념을 제도적으로 정식화해야 한다. 이는 현행 규정 역시 예외를 인정하고 있으나, 대체통제의 법적 정의와 적용 범위가 불명확하여 피규제자의 예측 가능성이 저하되는 측면이 존재하기 때문이다.[55]

이를 위해 개정안에는 대체통제의 개념을 명문화하고, 가상화 보안(VDI · DaaS)이나 행위 기반 실시간 모니터링 체계 등을 망분리에 상응하는 대안으로 인정하는 근거를 마련해야 할 것이다. 다만, 이러한 대체 수단이 실질적인 보안 수준을 담보하는지 검증하기 위한 기술적 가이드라인을 구체화함으로써 자율 보안의 확대에 따른 책임성을 강화하는 장치가 반드시 수반되어야 할 것이다.

### 4. 클라우드 · AI 환경 및 ZTA 원칙의 규범적 수용

상시적인 네트워크 연결을 전제로 작동하는 클라우드, SaaS, 생성형 AI 기반 업무 인프라의 확산을 고려할 때, 규제의 초점은 '단말기 차단'에서 '데이터 흐름 통제'로 과감히 전환되어야 한다. 이는 모든 접근 요청을 신뢰하지 않고 지

54) 한국인터넷진흥원, 「제로 트러스트 가이드라인 2.0」, 2024, 45면.
55) 금융위원회, 「전자금융감독규정 개정안 규정변경예고 및 향후 추진일정」, 보도자료, 2022. 5. 2. (https://www.fsc.go.kr/no010101/77740)

속적으로 검증하는 ZTA 원칙을 규범 체계 전반에 투영하는 과정이기도 하다.

그리고, 최소 권한 원칙과 컨텍스트 기반 접근 통제 등을 보안 표준의 핵심 요소로 포섭하여, 네트워크의 물리적 경계 유무와 무관하게 데이터 자체에 대한 정밀한 통제력이 작동하는지를 보안의 핵심 준거로 삼아야 할 것이다. 이러한 규제 설계는 정보보호 규제가 기술 현실과의 정합성을 확보하면서도, 데이터 보호라는 본연의 목적을 효과적으로 달성할 수 있는 규범적 기반을 제공할 것으로 기대할 수 있다.

## Ⅶ. 결론

디지털 전환과 함께 클라우드 · AI · SaaS 중심의 정보처리 환경이 정착된 오늘날, 정보보호 규제의 기본 전제 또한 근본적인 재검토를 요구받고 있다. 본 연구의 검토 결과, 현행 망분리 규제는 도입 당시의 기술 환경에서는 일정한 보안 효익을 제공하였으나, 데이터의 이동성과 활용이 급격히 확대된 현재의 정보 생태계에서는 그 규범적 전제가 더 이상 충분한 타당성을 유지하기 어렵다는 한계를 지닌다. 특히 네트워크 경계에 기초한 기존의 보호 방식은 데이터 중심 보안 및 위험 기반 접근이라는 현대 정보보호법제의 핵심 원칙과 조응하지 못하고 있으며, 기술 환경 변화에 비추어 규제 구조 전반의 재설계가 요청되고 있다.

이러한 문제의식은 2025년 발생한 대규모 보안 사고들을 거치며 더욱 극명해졌다. ‘경계’가 아닌 ‘데이터’ 자체에 대한 보호 부재가 초래하는 치명적 결과는 역설적으로 규제 패러다임의 전환을 가속화하는 계기가 되었다. 이에 대응하여 2026년 현재 공공부문에서 시행 중인 MLS의 도입과 금융부문의 ‘원칙 중심 자율보안’으로의 전환은, 규제 패러다임이 이미 물리적 ‘단절’에서 데이터의 안전한 ‘흐름’으로 이동했음을 보여주는 실정법적 증거라 할 수 있다.

다만, 2025년 개정을 통해 전자금융감독규정 제15조 등에 도입된 ‘망분리 대체 정보보호통제’ 제도는 망분리 규제의 경직성을 일부 완화하려는 정책적 진전을 보였음에도 불구하고, 망분리 의무를 여전히 규범의 원칙으로 유지한 채 감독기관 승인 하의 예외로서만 대체통제를 허용하고 있다는 한계가 있다. 이는 위험 기반 규율이나 데이터 중심 보안 패러다임이 규제의 기본 구조로 완전히 안착되었다고 보기 어렵게 만들며, 기술특정적 규제 구조의 잔재가 여전

히 규범 체계의 중심을 이루고 있음을 시사한다.

이에 비추어 볼 때, 향후 정보보호 규제 체계는 특정 기술 수단의 채택 여부에 대한 통제에서 벗어나, 정보자산 보호라는 규제 목적이 실제로 달성되고 있는지 여부, 즉 위험 완화의 실질적 성과를 중심으로 재구성될 필요가 있다. 이러한 규범 전환은 단순한 기술 선택의 문제가 아니라, 규제 목적·수단·평가 기준 전반을 재편하는 구조적 개혁을 의미한다. 특히 데이터 중심 보안과 위험 기반 접근을 규범의 기본 원칙으로 통합하는 것은 기술 발전의 속도와 규제의 안정성을 조화시키는 동시에, 정보보호의 실질적 수준을 제고하기 위한 필수적인 방향이다.

나아가 이러한 전환은 규제의 실효성과 정당성을 동시에 강화하는 효과를 기대할 수 있다. 획일적인 망분리 의무는 변화된 환경에서 과잉 규제와 규제 공백이라는 이중적 모순을 초래해 왔다. 반면, 위험 기반 규율에 기초한 성과 중심 규제 체계는 자원의 효율적 배분을 가능하게 하고, 보호가 필요한 영역에 규제 역량을 집중함으로써 전체적인 보안 수준을 향상시킬 수 있다. 이는 행정법상의 비례성 원칙 및 기술 중립성 원칙에 부합하는 설계로서, 현대 규제 원리에 보다 부합하는 방향이다.

본 연구의 분석을 종합하면, 현행 망분리 규정의 한계는 단순히 특정 기술 수단의 적합성 문제에 그치는 것이 아니라, 정보보호 규제의 기본 구조가 변화된 기술 환경과 정합성을 상실하고 있다는 점에서 비롯된 것으로 이해할 수 있다. 특히 본 논문에서 제시한 바와 같이, 향후 규제 체계의 재구성은 보호 대상 설정 기준의 전환, 통제 방식의 구조 변화, 규제 설계 원리의 전환이라는 세 가지 규범적 차원을 중심으로 이루어질 필요가 있다. 즉 보호의 기준을 네트워크 경계에서 데이터 객체 자체로 이동시키고, 정적·일률적 통제에서 위험 기반의 동적 통제로 전환하며, 특정 기술 수단을 강제하는 규제 구조에서 벗어나 기술 중립성과 결과 중심의 규범 설계를 지향하는 방향으로 재편되어야 할 것이다.

본 연구는 망분리 규제를 단순한 기술적 수단의 문제를 넘어 규범 구조 자체의 재검토 대상으로 위치시키고, 데이터 중심·위험 기반 규율로의 전환 필요성을 법제론적으로 정리하였다는 점에 그 의의가 있다. 향후 입법 논의에서는 본 연구를 토대로 대체통제 인정 기준의 명확화, 위험 평가 절차의 제도화, 성과 중심 감독 체계의 구축 등 구체적인 제도 설계가 이어져야 할 것이다. 이러한 노력이 축적될 때, 정보보호 규제는 급변하는 기술 환경 속에서도 안정성과 유연성을 동시에 갖춘 지속 가능한 규범 체계로 자리매김할 수 있을 것이다.

[참고문헌]

1. 국내 문헌

김도형, 「금융회사 제로트러스트 모델 적용방안에 대한 연구」, 「정보보안논문지」 제24권 제4호, 2024.

박지윤 · 정윤선 · 이재우, 「금융권 망분리 현황과 망분리 정책 개선에 대한 고찰」, 「정보보호학회논문지」 제26권 제3호, 한국정보보호학회, 2016.

서병호, 「주요국의 전자금융거래 규제 및 시사점: 사업자 분류 및 관련 주요 개념을 중심으로」, KIF 이슈리포트, 한국금융연구원, 2025.

성승제, 「신기술기반 전자금융 안전성 확보 법제 연구」, 연구보고 2015-05, 한국법제연구원, 2015.

오정주 · 이환수, 「디지털 금융산업 활성화를 위한 망분리 규제 개선방안」, 「한국금융학회지」 제21권 제5호, 한국융합보안학회, 2021.

조병주 · 윤장호 · 이경호, 「금융회사 망분리 정책의 효과성 연구」, 「정보보호학회지」 제25권 제1호, 한국정보보호학회, 2015.

황세운, 「금융회사의 망분리 규제 현황 및 개선방향」, KCMI 24-26, 자본시장연구원, 2024.

_____, 「금융회사 망분리 규제 해외사례와 국내 시사점」, 「자본시장포커스」 2024-20호, 자본시장연구원, 2024.

과학기술정보통신부 · 한국인터넷진흥원(KISA), 「제로 트러스트 가이드라인 1.0」, 2023.

금융보안원, 「연구 · 개발 목적 망분리 예외 보안 해설서」, 2025.05.06.

금융위원회, 「금융분야 망분리 개선 로드맵 발표」, 보도자료, 2024.08.13.

금융위원회, 「전자금융감독규정 개정안 규정변경예고 및 향후 추진일정」, 보도자료, 2022.05.02.

한국인터넷진흥원(KISA), 「제로 트러스트 가이드라인 2.0」, 2024.

한국인터넷진흥원, 「ISMS-P 인증기준」, 2024.

행정안전부, 「행정기관 및 공공기관의 클라우드컴퓨팅서비스 이용 기준 및 안전성 확보 등에 관한 고시」, 행정안전부고시 제2025-79호.

법무법인(유) 광장, “전자금융감독규정 개정 자율보안 토대 마련”, 「Lee & Ko 뉴스레터」, 2025.02.19.

법무법인(유) 세종, “금융사도 생성형 AI를 활용할 수 있도록, 망분리 제도가 완화될 예정입니다”, 「SHIN & KIM 뉴스레터」, 2024.

2. 국외 문헌

Asia Cloud Computing Association (ACCA), Network Separation in South Korea: Impact and Directions for Improvement, 2024.-

CISA, Trusted Internet Connections (TIC) 3.0 Cloud Use Case, 2023.-

CISA, Zero Trust Maturity Model Version 2.0, 2023.-

European Union, Directive (EU) 2022/2555 (NIS2 Directive), 2022.-

FFIEC, IT Examination Handbook: Information Security Booklet, 2016.-

FFIEC, IT Examination Handbook: Management Booklet, 2015-

MAS, Technology Risk Management Guidelines(TRM). 2021.-

NIST, Guide to Attribute Based Access Control (ABAC) Definition and Considerations, Special Publication 800-162, 2014.-

NIST, Zero Trust Architecture, NIST Special Publication 800-207, 2020.-

OECD, Regulatory Policy Outlook, 2021.-

OMB, Memorandum M-22-09: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, 2022.-

金融廳,「金融分野におけるサイバーセキュリティ強化に向けた取組方針 (Ver.3.0)」, 2022.-

金融廳,「金融分野におけるサイバーセキュリティに關するガイドライン」, 2024.-

政府CIO補佐官等,「政府情報システムにおけるゼロトラスト適用に向けた考え方」.2020.-

[Abstract]

# Normative Limitations and the Reconstruction of Network Separation Regulations in the Transition to Data-Centric Security

LEE, Hyung-Kyun*

As digital transformation intensifies across financial, public, and private sectors, the proliferation of cloud computing, Generative AI, SaaS, and mobile work environments suggests that traditional boundary-based security models are no longer sufficient. This study examines the legal and theoretical foundations of the "Data-Centric Security" paradigm—which shifts the unit of information protection from spatial locations like networks or systems to the data itself—and analyzes its structural conflicts with current network separation regulations to propose a future-oriented redesign of the regulatory framework.

Korea's current information protection regulations are centered on "network separation" (physical and logical isolation), a system established in response to large-scale hacking incidents in the early 2010s. However, by prescribing specific technical methods in legislation, these regulations conflict with the principle of technology neutrality and create rigidity that fails to accommodate rapid technological advancements. Notably, major data breach incidents in 2025 demonstrated that even within physically isolated environments, the absence of data-level protection can lead to catastrophic consequences. This suggests that current regulations, preoccupied with network boundary protection, are losing their normative validity and security effectiveness in modern, complex data-processing environments.

Against this backdrop, this study conducts a comparative legal analysis of security policy shifts in major jurisdictions, including the United States, the EU, Japan, and Singapore. The U.S. adopted Zero Trust Architecture (ZTA) as the default model for federal agencies through Executive Order 14028, establishing a data-and-user-centric security structure. Similarly, the EU

* Lecture, Kyungpook National University, Ph.D. in Law.

codified a risk-based approach grounded in technology neutrality through the GDPR and NIS2 Directive. Singapore and Japan also emphasize flexible controls and governance based on asset importance and risk levels rather than mandating specific technologies.

Based on these analyses, this study proposes four directions for reforming network separation regulations from a data-centric security perspective. First, the regulatory framework should shift toward "performance-based regulation," where the actual achievement of information protection levels—rather than the adoption of specific technical means—serves as the criteria, thereby ensuring technology neutrality. Second, a "Risk-Based Approach (RBA)" must be institutionalized to differentiate control intensity according to data sensitivity and business risk levels, with particular attention to the Multi-Level Security (MLS) model in the public sector. Third, modern security technologies such as VDI/DaaS, IAM, and data encryption/DCAP should be formalized as legitimate "alternative controls" to enhance legal predictability for regulated entities. Fourth, the principles of ZTA—"never trust, always verify"—should be integrated into the legal framework to ensure precise control over data regardless of network boundaries.

In conclusion, current network separation regulations must move beyond regulatory inertia detached from technical reality and be redesigned into a modern normative structure that protects the actual value and secure flow of data. By shifting the regulatory paradigm from spatial boundaries to information value, this study seeks to establish a legal and policy foundation that enhances substantial cybersecurity capabilities without hindering digital innovation.

Keywords : Network Separation, Data-Centric Security, Zero Trust Architecture (ZTA), Technology Neutrality, Risk-Based Approach