이슈보고서 24-26

ISSUE
REPORT

금융회사의 망분리 규제 현황 및 개선방향

황세운

자본시장연구원
Korea Capital Market Institute

금융회사의 망분리 규제 현황 및 개선방향

저자 황세운*

금융회사에 대한 망분리 규제를 개선할 필요성이 있다는 지적이 활발해지고 있다. 망분리규제는 금융전산 보안사고를 최소화시키기 위해 도입되었는데, 국내에서는 오랜 기간 물리적 망분리가 엄격히 요구되어 왔다. 그러나 ICT 산업의 급속한 발전과 금융회사 서비스의 경쟁력 유지 필요성을 감안할 때 금융회사에 대한 망분리 규제에 큰 폭의 변화가 필요하다. 클라우드에 기반한 구독형 소프트웨어의 일반화와 생성형 AI의 출현은 가장 대표적인 금융전산환경의 변화로 꼽힌다. 금융회사는 비용절감과 혁신적인 서비스 제공을 위해 이러한 트렌드에 적극적으로 동참해야 하는데 엄격한 물리적 망분리 규제는 클라우드에 기반한 기술의 활용에 큰 장애요소가 되며, 연구·개발 활동에도 지장을 준다.

미국, 유럽, 호주의 망분리 규제는 명문화된 공식 규정의 형태가 아닌 가이드라인과 같은 연성규제의 방식을 따르며, 해당 금융회사의 판단과 선택을 기본적으로 존중한다. 금융회사의 재량권을 인정하는 배경에는 자율규제에 대한 기본적인 신뢰와 사고 발생 시 책임을 강하게 묻는 사후규제의 전통이 자리잡고 있다. 금융회사들은 관련 가이드라인을 따라 내부망과 외부망에 대한 보안통제를 실시한다. 망세분화의 기법은 물리적인 접근법과 논리적인 접근법을 모두 허용하는데, 그럼에도 물리적 망분리만을 선택하는 금융회사는 거의 없다는 점은 시사하는 바가 크다.

장기적인 관점에서 망분리 규제의 방향성은 망분리 방식에 대해 금융회사의 선택권을 인정하되, 금융전산 보안사고가 발생할 경우 그에 대한 책임을 무겁게 하는 방식을 고려해 볼 필요가 있다. 규제샌드박스의 적극적인 활용도 망분리 규제개선에 있어 중요한 요소라 볼 수 있으며, 클라우드 서비스를 통해 제공되는 생성형 AI와 SaaS 활용 범위를 확대하기 위한 노력도 필요하다. 금융회사는 변화될 보안규제 환경에서 고객관리와 영업활동상의 중요한 데이터를 안전하게 관리하기 위한 보안체계를 스스로 마련해야 한다. 금융당국은 금융회사의 자율적인 금융전산 보안체계에 대해 정기적인 검사를 진행하고, 보안상의 문제점이 발견되면 시정조치를 요구해야 할 것이다.

---

* 본고의 견해와 주장은 필자 개인의 것이며, 자본시장연구원의 공식적인 견해가 아님을 밝힙니다.
펀드연금실 선임연구위원 황세운(neptune@kcmi.re.kr)

** 발행: 2024년 11월 22일

Ⅰ. 서론

최근 국내에서 금융회사에 대한 망분리 규제를 개선할 필요성이 있다는 지적이 활발해지고 있다. 국내 망분리 규제는 금융전산상에서 발생하는 보안사고를 최소화함으로써 금융소비자의 중요정보를 안전하게 보호하고 금전적인 피해가 발생하는 것을 방지하기 위해 도입되었다. 대부분의 금융정보가 전산시스템에서 관리되고 있기 때문에 의도하지 않은 사고 또는 해킹으로 인해 금융서비스가 제대로 제공되지 않거나 고객의 정보가 유출되었을 때 그 피해는 막대해진다. 또한 대부분의 경제활동이 디지털화되고 있다는 점을 감안할 때 향후 발생할 가능성이 있는 금융보안사고는 예측하기가 더욱 어려워지고 있으며, 사고 발생 시 피해규모도 매우 클 것이다. 이러한 측면을 감안할 때 금융회사에 대한 망분리 규제는 존속의 필요성이 크며, 시장환경의 변화에 따라 고도화 및 효율화되어야 할 것이다.

금융회사의 망분리 규제가 도입된 이후 국내에서 금융보안 관련 사고가 줄어드는 성과를 보인 것이 사실이다. 그런데 금융회사의 업무환경이 급속히 디지털화되면서 기존의 망분리 규제방식이 가지고 있는 문제점이 드러나고 있다. 금융회사의 IT 경쟁력이 금융회사의 생존과 직결되는 환경에서 금융회사들은 전산시스템의 효율적인 운영을 위해서 클라우드 서비스를 적극적으로 이용하고 있다. 또한 인공지능(AI) 기술이 급속히 발전하면서 이를 활용한 금융서비스의 제공이 중요한 트렌드로 자리 잡았다. 클라우드와 AI의 부상은 현행 망분리 규제와 여러 가지 측면에서 충돌하면서 금융회사의 서비스 제공에 새로운 부담요소로 작용하고 있다. 금융회사가 서비스 개발에 신기술을 더욱 적극적으로 활용할 수 있도록 유도하기 위해 망분리 규제를 합리화할 필요가 있다는 지적이 제기되는 이유이다.

망분리 규제는 다양한 방식으로 설계될 수 있으며 각각의 방식은 고유한 장점과 단점을 모두 가지고 있다. 따라서 특정 방식이 가장 우수한 방식이라 평가하기는 어려우며, 현재의 금융시장 환경과 디지털 기술의 발전정도를 감안하여 최적의 방식을 선택해야 한다. 망분리 규제는 금융사고의 방지와 금융소비자의 보호뿐만 아니라 금융회사의 서비스 개발과 제공이 효율적으로 이루어질 수 있도록 설계되어야 한다. 이에 본고는 금융회사 망분리 규제의 도입 배경과 주요 특성을 검토하고, 금융시장의 건전한 발전을 위한 망분리 제도의 개선방향을 모색해 보고자 한다. 이를 위해 국내 망분리 규제가 가진 문제점을 파악하고, 해외의 망분리 규제 접근방식을 비교 분석한 후 장기적인 망분리 규제 개선방안을 제언할 것이다.

II. 국내 금융회사 망분리 규제의 특징 및 문제점

1. 금융회사 망분리 규제의 도입 배경

우리나라에서 금융회사에 대한 망분리 규제는 2015년에 규정으로 공식화되었지만, 2013년에 발생했던 일부 시중은행의 금융전산 사고가 제도 도입의 결정적인 계기가 되었다. 2013년 3월 20일 시중은행 중 N사의 영업창구 직원 PC 여러대가 바이러스에 감염되어 PC 내 파일이 삭제되고 오프라인 창구가 마비되는 사태가 발생하였다. 또 다른 시중은행인 S사에는 인터넷뱅킹 서버가 다운되어 인터넷뱅킹 거래에 장애가 발생하였다. 일련의 사고들은 바이러스 백신을 업데이트하는 업데이트용 서버를 통해 패치파일을 가장한 악성코드가 내부 업무 PC로 유포되면서 발생했는데, 금융당국은 이를 사이버테러로 규정했다.

기업에 대한 해킹시도는 이전에도 꾸준히 발생해 왔지만 은행에 대한 사이버테러는 국민들의 통상적인 상거래에 미치는 파장이 지대하기 때문에 금융당국은 사이버보안에 대한 규제를 본격적으로 정비해야 했다. 2013년에 이미 전체 금융거래에서 전자금융거래가 차지하는 비중이 87.7%를 차지했고, 인터넷뱅킹과 모바일뱅킹 일평균 거래금액은 33조원을 넘었다. 비대면 방식의 전자금융거래가 보편화된다는 것은 금융소비자들의 효용이 높아진다는 것을 의미하지만 해킹과 같은 불법행위가 발생했을 때 그 피해가 대규모로 발생할 가능성도 높아진다. 이에 2013년 7월 금융당국은 금융보안에 대한 패러다임 전환을 목표로 금융전산 보안 강화 종합대책을 발표하면서 금융회사의 망분리 규제를 공식화하였다.[01]

금융전산 보안을 강화하는 데에 망분리 규제는 핵심적인 역할을 담당하는데, 금융회사의 전산센터부터 우선적으로 물리적 망분리를 의무화하고, 본점 · 영업점에 대해서는 단계적으로 망분리 의무화를 확대하였다. 망분리 이외에도 반복적으로 발생하는 금융회사의 보안사고를 최소화하기 위하여 위기대응 체계를 강화하고 금융회사의 전산시설에 대한 내부통제수준을 높이는 방안을 마련하였다. 아울러 이상거래탐지시스템을 주요 금융권으로 확대하여 관련 정보를 전 금융권과 공유하는 체계도 마련하였다.

01 금융위원회(2013.7.10)

2. 국내 금융회사 망분리 규제의 주요 특성

망분리(network separation)는 네트워크 보안기법의 일종으로 외부 인터넷망을 통한 불법적인 접근과 내부정보 유출을 차단하기 위해 업무망과 외부 인터넷망을 분리하여 두 영역이 서로 접근할 수 없도록 차단하는 것을 의미한다.[02] 망분리와 비슷한 개념으로 망세분화(network segmentation 또는 zoning)라는 용어도 사용되지만 이는 네크워크 구성을 계층화시키고 이에 대한 접근을 통제하는 방식이며 분리된 망간의 연결도 가능하다는 점에서 망분리와 차이가 있다.[03]

망분리는 설계방식에 따라 물리적 망분리와 논리적 망분리로 구분할 수 있다. 물리적 망분리는 통신망, 장비 등을 물리적으로 이원화하여 인터넷 접속이 불가능한 컴퓨터와 인터넷 접속만 가능한 컴퓨터로 분리하는 방식이다. 논리적 망분리는 물리적으로 하나의 통신망, 장비 등을 사용하지만 가상화 등의 방법으로 인터넷 접속이 불가능한 내부 업무영역과 인터넷 접속영역을 분리하는 방식이다.[04] 물리적 망분리는 보안성이 높다는 장점을 가지고 있으나 구축비용이 상대적으로 많이 들고 업무효율성이 떨어지는 단점을 가진다. 반면 논리적 망분리는 구축환경에 따라 차이가 있기는 하지만 상대적으로 구축비용이 적고 관리가 용이해 업무효율성 확보에 있어서 유리하다. 다만 보안성이 상대적으로 떨어진다는 단점을 가진다.

<표 II-1> 물리적 망분리와 논리적 망분리의 특성 비교

구분	물리적 망분리	논리적 망분리
운영방법	업무용 망과 인터넷 망을 물리적으로 분리	가상화 등의 기술을 이용하여 논리적으로 분리
도입비용	높음(추가 PC, 별도 망 구축 등)	구축환경에 따라 상이함
보안성	높은 보안성(근본적 분리)	상대적으로 낮은 보안성
효율성	업무환경의 효율성 저하	상대적으로 관리 용이

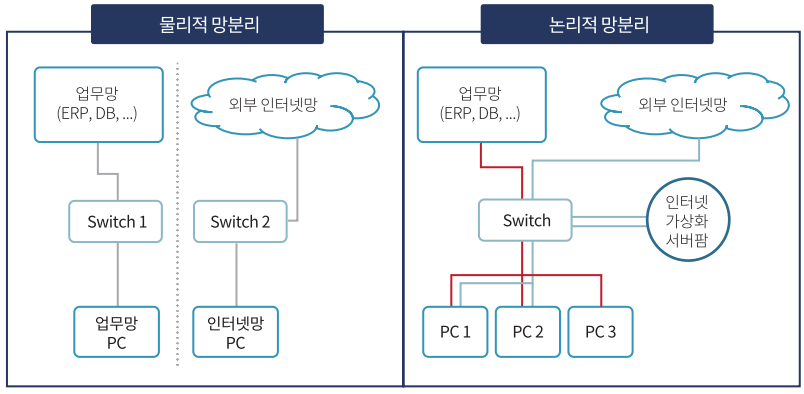
자료: 개인정보보호위원회 · 한국인터넷진흥원(2022)

02 조병주 · 윤장호 · 이경호(2015)

03 정다빈 · 나현대 · 김선우(2020)

04 개인정보보호위원회 · 한국인터넷진흥원(2022)

<그림 II-1> 물리적 망분리와 논리적 망분리의 구조 비교



국내에서 금융회사 대한 망분리 규제는 전자금융감독규정에 따라 이루어진다. 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망 해킹 등과 같은 전자적 침해행위를 방지하기 위하여 내부통신망과 연결된 내부 업무용시스템을 인터넷(무선통신망 포함) 등 외부통신망과 분리 · 차단해야 한다. 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리해야 한다.[05] 금융회사에 대해 이와 같이 엄격한 물리적 망분리가 요구되고 있지만 내부통신망에 연결된 단말기가 업무상 필수적으로 외부기관과 연결되어야 하는 경우에는 물리적 망분리 적용에 대한 예외가 인정된다. 또한 전자금융업무의 처리를 위하여 특정 외부기관과 데이터를 송수신하는 정보처리시스템과 다른 계열사와 공동으로 사용하는 정보처리시스템에 대해서도 물리적 망분리에 대한 예외가 허용된다. 물리적 망분리에 대한 예외가 허용되는 경우라 하더라도 금융회사 또는 전자금융업자는 자체 위험성 평가를 실시한 후 망분리 대체 정보보호통제를 적용해야 하고 정보보호위원회가 이를 승인해야 한다.[06]

물리적 망분리는 업무망 컴퓨터에서 인터넷망을 완전히 분리하여 인터넷망을 경유해서 시도될 수 있는 악성코드 감염, 해킹, 개인정보 유출 등의 위험성을 제거하는 방법이다. 물리적 망분리를 구축하는 방법에는 2대의 컴퓨터를 이용하여 망을 분리하는 방법, 망전환장치를 이용하여 망을 분리하는 방법, 물리적 폐쇄망을 구축하는 방법 등을 선택할 수 있다.[07] 2대의 컴퓨터를 이용해

05 전자금융감독규정 제15조(해킹 등 방지대책) 제1항 제3호 및 제5호

06 전자금융감독규정시행세칙 제2조의2(망분리 적용 예외)

07 개인정보보호위원회 · 한국인터넷진흥원(2022)

서 망을 분리하는 방법은 인터넷용 컴퓨터와 업무용 컴퓨터를 별도로 분리한 후, 인터넷용 컴퓨터는 인터넷망에만 접속하고 업무용 컴퓨터는 업무망에만 연결시킨다. 이렇게 망분리를 할 경우 인터넷망과 업무망 간 접근경로가 물리적으로 차단되기 때문에 보안성이 높아진다. 다만 개별적인 네트워크와 전용 컴퓨터의 설치 등으로 인해 비용부담과 관리부담이 커진다. 망전환장치를 이용해서 망을 분리하는 방법은 정보처리와 네트워크 연결을 분할한 컴퓨터를 활용하는 방식인데 망전환장치를 이용해 인터넷망과 업무망을 배타적으로 접속하도록 설계된다. 공간에 대한 부담이 상대적으로 적다는 장점이 있으나 망전환 시 부팅을 다시 해야 하는 불편함이 발생할 수 있다. 물리적 폐쇄망은 업무망 컴퓨터에 인터넷망과의 연결점을 제거한 후 특정 물리적 공간을 폐쇄하는 방식으로 설계된다. 물리적으로 접근이 통제된 공간을 폐쇄망으로 구성하여 개인정보와 같은 중요 정보를 관리하도록 하는 방식이다. 공간에 대한 접근성을 제한하는 방식이므로 보안성을 크게 개선할 수 있는 장점이 있으나 업무 불편성과 구축비용이 커지는 단점이 있다.

3. 금융시장 변화와 현행 망분리 규제의 문제점

현행 망분리 규제는 내부 정보의 유출 및 외부에서의 해킹 등을 차단하는데 상당한 효과가 있고, 정보의 순환이 차단됨에 따라 데이터 순환 연결고리 전체를 점검하는 관제 비용을 부담하지 않아도 되기 때문에 비용상의 장점이 존재한다.[08] 그러나 서비스제공 방식과 업무수행 방식의 변화와 같은 금융시장의 환경변화에 적응하기 힘들고 망분리 규제가 가진 기본적인 업무비효율성에 대해 지속적으로 문제 제기가 이루어져 왔다.

금융산업에 ICT기술의 도입이 활발해지면서 금융회사는 ICT기술의 변화를 서비스 제공에 신속히 받아들여야 하는 상황에 직면하고 있다. 금융시장의 변화중에 가장 주목할만한 부분은 클라우드(cloud) 환경으로의 전환과 인공지능(AI)의 급속한 성장이다. 금융회사는 전통적으로 자신에게 필요한 소프트웨어를 자체적으로 시스템에 구축하여 사용하는 접근법을 선호하였다. 그러나 소프트웨어 시장은 자체 구축형에서 클라우드 기반의 구독형으로 전환되고 있다. Chat-GPT가 촉발한 생성형 AI 구축경쟁도 금융회사의 서비스 제공방식에 크게 영향을 미치고 있다. 금융회사의 직원은 Chat-GPT, MS 코파일럿, 구글 제미나이 등의 생성형 AI를 활용하여 업무분석에 필요한 경제 데이터나 통계를 조사하고 요약함으로써 업무효율성을 높일 수 있다. 그런데 생성형 AI의 대부분이 클라우드에 기반하여 서비스가 제공되고 있기 때문에 국내 금융회사들은 생성

08 이수환(2021)

형 AI를 업무에 활용하는 데에 있어 상당한 불편을 겪고 있다. 기술적 진보를 얼마나 신속하고 효과적인 방식으로 업무시스템이 접목하는가는 금융회사의 지속가능성에 유의적인 영향을 미친다. 생성형 AI와 같은 신기술을 접목하여 새로운 업무시스템을 개발하고 고객에게 더 편리한 금융상품을 제공하는 데에 망분리 규제가 큰 부담요소로 지목되고 있으며, 연구 · 개발 과정에서의 비효율성이 여전히 크다는 지적이 이어진다.

일반기업과 유사하게 금융회사의 클라우드 서비스 활용도는 꾸준하게 증가하고 있다. 클라우드 서비스가 가진 비용적인 이점에도 불구하고 그간 금융회사의 클라우드 활용은 이메일이나 사내 메신저와 같은 단순한 내부업무나 고객서비스 업무로 한정되어 있었다. 금융회사가 필요로 하는 소프트웨어가 자체 구축형에서 구독형(SaaS)[09]으로 급속히 전환되고 있는 환경에서 기존의 엄격한 물리적 망분리 규제는 클라우드 서비스를 활용해 금융서비스 제공의 비용을 줄이고 서비스 품질을 높이려는 금융회사의 수요와 상충한다. 예를 들어 금융회사 직원들이 업무처리에 많이 활용하는 MS365의 경우 문서작성, 통계 처리 등에 매우 효과적이기 때문에 SaaS로서의 수요가 매우 높다. 그런데 망분리 규제로 인해 내부망에 연결된 PC에서는 MS365를 사용하여 업무처리를 할 수 없는 비효율이 발생한다. 소프트웨어 서비스의 제공방식이 변화함을 감안하여 망분리 규제에 대한 접근법도 변화할 필요가 있을 것이다. 클라우드 서비스에 대한 수요를 감안하여 금융당국은 전자금융감독규정을 개정하여 2022년부터 개인정보를 처리하지 않는 것을 전제로 하는 연구 개발 분야에 대해서는 망분리 규제를 예외적으로 완화하였고, 금융거래와 무관한 비중요업무에 대해서는 금융규제 샌드박스를 통해 망분리 예외를 허용하였다. 이를 통해 망분리 규제로부터 발생하는 금융회사의 업무상 어려움을 일정부분 완화시켰지만 여전히 개선의 필요성이 크다고 볼 수 있다.

중요업무에서의 클라우드 소프트웨어 필요성이 커지고 있다는 점도 망분리 규제에 대한 변화가 필요한 이유이다. 금융회사가 수행하는 비중요업무뿐만 아니라 중요업무에 있어서도 외부 소프트웨어의 활용이 증가하고 있다. 고객과의 거래데이터 분석, 시스템 관리, 인터넷 뱅킹 · 모바일 뱅킹과 같은 기본적인 업무영역에서도 클라우드 서비스에 대한 수요가 증가하고 있다. 보안관리나 고객관리 등의 업무에서도 클라우드 활용수요가 커지고 있다. 해외의 금융회사들은 핵심업무의 클라우드 전환을 가속화시키고 있다. 예를 들어 도이치뱅크(Deutsche Bank)는 2020년에 차세대 뱅킹시스템을 구글 클라우드로 구축하는 작업을 시작했다. 이를 통해 파트너사의 서

09 SaaS(Software as a Service)는 소프트웨어를 사용한 만큼 비용을 지불하는 방식의 클라우드 서비스 모형이다. 소프트웨어를 로컬 PC에 설치해서 사용하는 것이 아니라 인터넷상에 존재하는 클라우드 서비스에 접속해서 이용한다. 대표적인 SaaS로 MS365, 한컴오피스웹 등이 있다.

비스를 도이치뱅크의 서비스 플랫폼에 직접 구현하는 형태로 뱅킹서비스를 제공한다. 미국 은행인 웰스파고(Wells Fargo)도 구글 클라우드 플랫폼을 활용해 고난이도 은행데이터 분석업무를 수행하는 작업을 진행해 왔다. 해외의 금융회사들은 완전 개방형 플랫폼(클라우드 기반)을 통해 금융 솔루션 제공업체와 금융회사 고객(기관 또는 고액개인자산가 등)을 연결해 주거나, 금융회사 자체 솔루션을 고객 시스템과 통합시키는 방향으로 진화하고 있다. 그러나 국내 금융회사들이 핵심적인 중요업무에 클라우드를 도입하는 것에는 망분리 규제가 큰 부담이 되는데, 클라우드는 외부 인터넷망에서 서비스되는 반면 핵심적인 중요업무를 위해서는 내부망에 있는 데이터를 활용해야 하는 경우가 일반적이기 때문이다. 클라우드를 활용할 경우 더 효율적인 업무진행이 가능하고, 해당업무에 필요한 시스템 구축 비용도 최대 30%까지 절감될 수 있음에도 불구하고 망분리 규제로 인해 해당 소프트웨어의 도입이 불가능한 것이다. 망분리 규제가 금융업에 신규 진출하는 기업들의 장벽으로 작용할 수 있다는 지적도 이어지고 있다.[10]

망분리 규제는 금융회사의 연구 · 개발 환경에 여전히 부담요소로 인식되고 있다. 정부는 2022년 금융회사의 연구 · 개발 활동을 장려하기 위하여 연구 · 개발 활동에 대해서는 인터넷망을 충분히 활용할 수 있도록 망분리 규제의 예외를 허용하였다. 그렇지만 연구 · 개발 환경의 물리적 분리 및 개인신용정보 활용 금지 등에 따라 고객별 특성 · 수요에 부합하는 새로운 서비스의 개발에 제약이 여전하다는 지적이 이어지고 있다. 최근의 개발환경에서 오픈소스와 API 등의 활용은 필수적이다. 망분리 규제 아래에서는 오픈소스 등의 활용이 어려워 속도와 다양성, 유연성 차원에서 개발의 질이 떨어질 수 있다.[11] 금융회사의 신규 서비스 제공은 신속성이 매우 중요하다는 점을 감안하여 연구 · 개발의 속도가 높아질 수 있도록 연구환경을 개선하고 개발된 서비스가 즉각적으로 제공될 수 있게 물리적 제한을 완화하는 방향으로 규제개선이 필요할 것이다.

III. 해외의 망분리 규제 접근방식

금융전산과 관련된 보안확보는 해외에서도 매우 중요한 이슈이다. 미국과 유럽의 망분리 규제는 우리나라와 같이 명문화된 의무규정의 형태가 아니라 가이드라인과 같은 연성규제의 방식을 따

10 오정주 · 이환수(2021)

11 오정주 · 이환수(2021)

르며, 해당 금융회사의 판단과 선택을 기본적으로 존중한다. 물론 이와 같이 금융회사의 재량권을 인정하는 배경에는 자율규제에 대한 기본적인 신뢰와 사고 발생 시 책임을 강하게 묻는 사후규제의 전통이 자리잡고 있다. 주요국의 망분리 규제와 국제기구의 권고사항을 비교 · 분석함으로써 국내 망분리 규제의 개선방향에 의미있는 시사점을 찾을 수 있을 것이다.

1. 미국의 망분리 규제

미국은 우리나라처럼 망분리에 대해 직접적이고 구체적인 규정으로 규제하기 보다는 가이드라인의 성격을 가진 핸드북을 통해 망분리의 효과성을 안내하고 기본적인 방향성에 대해 권고하는 방식을 따른다. 또한 단순한 망분리 방식이 아니라 망분리의 포괄적인 개념인 망세분화의 개념으로 접근한다. 민감한 고객정보나 거래정보를 다루는 시스템이라고 하더라도 기계적으로 망분리를 실행하는 것이 아니라 여러 수준의 망세분화를 고려하여 금융회사가 가장 합리적인 대안을 선택하도록 하고 있다.

미국의 망분리 규제의 기본적인 방향성을 제시하는 것은 연방금융기관 검사위원회(Federal Financial Institutions Examination Council, 이하 FFIEC)[12]가 발간한 Information Technology Examination Handbook, Information Security[13]이다. 핸드북의 기본 성격은 금융회사 검사기관의 검사역과 금융회사의 경영진이 해당 금융회사에 대한 IT 검사를 실행할 때 활용할 수 있는 표준기준으로 정의할 수 있다. 정보기술검사 핸드북 정보보안편에서 망분리에 대한 가이드라인은 II.C.9(Network controls)에 구체적으로 기술되어 있다. II.C.9은 금융회사의 경영진은 접근경로를 다층화함으로써 컴퓨터 네트워크에 대한 접근 안전성을 확보해야 함을 밝히고 있다. 네트워크를 신뢰구역(trusted zones)과 비신뢰구역(untrusted zones)으로 구분하고 구역 간의 접근을 통제해야 한다. 신뢰구역과 비신뢰구역은 해당 구역에 포함되어 있는 자산의 중요성과 위험특성에 따라 구분하며, 구역 간에 적절한 수준의 접근 통제가 이루어져야 한다. 네트워크 구조도와 데이터 흐름도를 실제와 동일하게 유지해야 하고, 유선 · 무선 네트워크에 대해 적절한 수준의 통제체계를 갖추어야 한다.

12 FFIEC는 1979년에 설립된 5개의 정부관련 기관이 참여하는 협의체 성격의 정부단체이다. 멤버는 Board of Governors of the Federal Reserve System(FRB), Federal Deposit Insurance Corporation(FDIC), National Credit Union Administration(NCUA), Office of the Comptroller of the Currency(OCC), Consumer Financial Protection Bureau(CFPB)로 구성된다. 금융회사 감독에 대한 일관성과 완결성을 제고하기 위해 설립되었다.

13 FFIEC(2016)

신뢰구역의 네트워크에 대해서는 적절한 수준의 환경설정 및 패치관리, 접근통제에 대한 엄격한 관리, 관리의무의 구분, 효과적인 보안정책의 수립 및 실행, 승인받지 않은 네트워크 접속시도를 차단함과 동시에 색출해 내기 위한 주변장치의 활용방안이 마련되어야 한다. 불법적인 네트워크 접속시도를 차단하고 탐지하기 위해서 활용할 주변장치에는 라우터, 방화벽, 침입탐지시스템, 침입방지시스템, 게이트웨이 등이 포함된다. 금융회사의 내부망은 신뢰구역에 해당하는데, 내부망에 대한 접근통제는 일률적으로 이루어지는 것이 아니라 해당구역에 포함되어 있는 자산의 내용과 역할을 감안하여 필요할 경우 신뢰구역 내에서 다시 계층화시킬 수 있다. 계층화가 이루어질 경우 각각의 신뢰구역 계층에 대해 해당 계층의 자산특성(위험특성, 민감한 데이터의 포함 여부, 사용자의 역할 등)을 감안하여 적절한 수준의 보안정책을 마련해야 한다. 전술한 FFIEC의 핸드북 내용을 종합해 보면 미국의 주요 금융당국은 총론적인 원칙만을 핸드북의 형태로 제시하고 구체적인 방법론에 있어서는 특별한 제한을 설정하고 있지 않다는 사실을 확인할 수 있다. 정보의 중요도에 따라 구역을 나누고 접근을 통제하는 망 세분화에 대한 설명을 제시하고 있지만 물리적 망분리나 논리적 망분리를 시스템화시켜야 한다는 방식의 요구사항은 관찰할 수 없다.

미국이 금융회사에게 망분리 방식에 대한 재량권을 인정하는 배경에는 사고발생 시 높은 수준의 처벌이 이루어지는 사후규제가 자리잡고 있다. 금융회사나 일반기업이 전산보안에 대해 적절한 수준의 노력을 기울이지 않았다는 판결이 나오면 미국 금융당국은 기업에게 상당한 부담을 주는 페널티를 부과하며, 이러한 페널티는 주로 금전적 제재의 형식을 가진다. 금융전산사고에 대한 벌금규정은 Gramm-Leach-Bliley Act에서 찾아볼 수 있는데, 금융전산보안사고가 발생하는 경우 연방 또는 주 금융 감독 당국은 해당 금융회사에 대해 벌금을 부과할 수 있다. 벌금 금액은 규정 위반의 심각성, 반복성 및 금융소비자 피해규모, 기관의 협력여부에 따라 달라질 수 있는데 특별히 상한선이 존재하지는 않는다. 예를 들어 미국의 FTC(Federal Trade Commission)는 2016년 발생한 데이터 유출사고에 대한 책임을 묻기 위해 2019년 Facebook에 50억달러에 이르는 벌금을 부과한 사례가 있다. 50억달러는 Facebook의 이전 회계연도 매출의 약 9%에 해당하는 금액인데, 미국의 전산보안에 대한 사후규제가 얼마나 강한 수준인지를 단적으로 보여주는 사례라 할 것이다.

2. 유럽의 망분리 규제

유럽의 망분리 규제는 미국의 접근방식과 유사하다. 금융회사가 ICT 및 보안 리스크 관리 시 필요한 사항을 명시한 가이드라인을 제시하되, 구체적인 실행방안은 금융회사가 판단하여 선택하도록 재량권을 부여하고 있다. 가이드라인과 더불어 유럽의 데이터 보안에 중요한 역할을 하는 규제로 유럽연합 일반 데이터 보호 규제(General Data Protection Regulation, 이하 GDPR)와 유럽은행감독청(European Banking Authority, 이하 EBA)이 주도한 결제서비스지침2(Payment Services Directive 2, 이하 PSD2)도 참고할 필요가 있다.

GDPR은 유럽연합의 공식적인 규제인데, 회원국 국민들의 개인정보보호를 위해 2018년 5월부터 시행되었다. GDPR은 금융회사를 포함한 모든 기업들의 정보보안의무에 대해 규정하고 있으며, EU 회원국 거주자의 개인정보를 다루는 모든 기업이나 단체에 대해 개인정보보호의무에 관한 광범위한 규정을 준수하도록 강제하고 있다. GDPR의 적용을 받는 데이터 관리 · 처리업자는 적정 수준의 데이터 보안을 유지하기 위해 필요한 기술적 · 조직적 수단을 확보해야 한다. 보안 유지를 위한 수단으로 개인정보는 가명화(pseudonymization)와 암호화(encryption)를 통해 보호하고, 물리적 사고나 기술적 사고가 발생한 경우에도 개인정보를 복구하고 신속히 접근할 수 있는 시스템을 갖출 것을 요구한다. 또한 개인정보와 데이터를 보호하기 위해 데이터 통제 · 처리 담당자들이 준수해야 할 내부통제 기준도 마련해야 한다.[14]

PSD2는 EBA가 마련한 결제서비스지침 개정안으로 2018년 1월부터 EU회원국에 대해 시행되고 있다. PSD2의 개정은 비은행금융회사가 결제업무에 참여하도록 허용함으로써 유럽 금융산업의 경쟁력을 제고함과 동시에 금융소비자 보호에 대한 결제서비스 제공업자의 의무를 명확히 함으로써 안전한 금융거래환경을 조성하는 것이었다. PSD2는 결제서비스를 제공하는 금융회사에 대하여 금융보안과 관련된 시스템을 갖출 것을 요구하고 있다. EU 회원국의 금융당국은 결제서비스 제공업자가 보안위험을 통제하기 위해 적절한 수준의 통제수단을 갖추었는지 확인해야 한다. 이를 위해 결제서비스 제공업자는 보안사고의 유형을 분류하고 각각의 유형에 대해 효과적인 탐지체계를 갖춘 사고관리절차를 구축해야 한다.[15]

유럽 금융회사들의 전산보안에 가장 구체적인 방향성을 제시하고 있는 것은 EBA가 발표한 금융

14 General Data Protection Regulation(GDPR), Chapter 4. Article 32.(Security of processing)

15 DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015, Chapter 5, Article 95.

회사 ICT 및 보안위험 관리 가이드라인(이하 EBA 가이드라인)이라고 할 수 있다. EBA 가이드라인은 금융회사 ICT와 보안위험이 갈수록 복잡한 형태로 진화하고 있고 금융전산 관련 사고도 증가추세에 있음을 감안하여 금융회사에게 요구되는 ICT 보안에 필수적으로 고려할 사항을 제시하기 위하여 작성되었다. 또한 Directive 2015/2366/EU(PSD2) 제95조가 규정하고 있는 보안위험을 통제하기 위한 수단에 대해 구체적인 지침을 제공한다. EBA 가이드라인은 금융회사 경영진의 책임을 명확히 규정한 효율적인 내부 통제구조를 확립함으로써 ICT 및 보안위험을 관리하고 최소화하는 것을 목적으로 작성되었다. 이를 위해 금융회사는 전반적인 경영전략과 일관성을 가지는 ICT전략을 수립해야 한다. 금융회사는 ICT 자원을 외부 또는 제3의 ICT 서비스 제공자에 의존할 경우 실효성이 있는 위험통제 수단을 마련해야 하며, 위험통제에 관한 내용은 법적인 구속력이 있는 계약의 형태로 준비해야 한다.[16]

EBA 가이드라인 Section 3.4는 적절한 수준의 정보보안을 유지하기 위해 요구되는 사항을 설명하고 있다. 금융회사는 고객 및 회사의 정보 데이터에 대한 기밀성, 완전성, 이용가능성을 보장하기 위해 기본적인 원칙 및 규칙을 수립하고 이를 바탕으로 정보보안 정책을 수립해야 하며, 정보보안 정책은 경영진에 의해 승인되어야 한다. 정보보안 정책에 포함되어야 하는 사항은 해당 금융회사의 ICT 및 정보보안 위험 특성에 따라 달라지지만, 기본적으로 1) 논리적 보안, 2) 물리적 보안, 3) ICT 운영상의 보안, 4) 보안 모니터링, 5) 정보보안 리뷰, 평가 및 테스트, 6) 정보보안 교육 및 인지도 제고 등의 사항을 기본적으로 고려하여 수립되어야 한다.

금융회사는 정보보안을 확보하기 위해 논리적 접근 통제 시스템을 갖추어야 한다. 논리적 접근 통제 시스템은 주기적으로 모니터링과 유효성 검증을 받아야 하며, 특이현상에 대한 모니터링이 가능해야 한다. 금융회사는 기본적으로 정보자산 및 관련된 지원시스템에 대한 접근 권한을 '꼭 필요한 때 꼭 필요한 것만 알려주는 방식(Need-to-know basis)'으로 관리해야 한다. 정보사용자들은 해당 직무를 수행하기 위해 필요한 최소 수준의 접근 권한만을 부여받아야 한다. 이를 통해 대규모 데이터에 대해 부정한 접근이 발생하는 것을 최소화하고, 접근통제 시스템을 우회하려는 시도를 차단해야 한다.[17]

금융회사는 데이터에 대한 물리적 보안을 확보하기 위해 사업상의 부지, 데이터센터 및 관련된 민감지역을 불법적인 접근시도나 환경적인 위험요소로부터 보호하기 위한 수단을 확보해야 한

16 EBA(2019)

17 EBA Guidelines on ICT and security risk management 3.4.2. Logical security

다. ICT 시스템에 대한 물리적 접근은 승인된 개인들에 대해서만 허용되어야 한다. 직원에 대한 접근승인은 해당개인들의 직무내용과 책임수준을 감안하여 결정되어야 하며, 적절한 수준의 교육을 받았고 모니터링이 이루어지는 직원들에 대해서만 승인이 이루어져야 한다. 물리적 접근 시스템은 불필요한 접근 권한을 즉시 취소할 수 있도록 주기적으로 점검되어야 한다. 환경적인 위험요소로부터 물리적 접근 시스템이 보호될 수 있는 수단도 확보해야 하며, 해당 빌딩에서 제공되는 영업행위 및 ICT 시스템의 중요성을 감안하여 상응하는 수준의 보호수단을 확보해야 한다.[18]

금융회사는 ICT 시스템 및 ICT 서비스에 전산사고가 발생하는 것을 방지하기 위한 수단을 마련해야 하고, 이를 통해 전산사고가 ICT 서비스의 제공에 미치는 영향을 최소화시켜야 한다. 금융전산사고 방지를 위해 시스템상 잠재적인 취약점이 확인되는지 파악하고, 확인된 취약점에 대해서는 소프트웨어와 펌웨어를 가장 최신버전으로 업데이트하고 금융회사가 내부 및 외부 사용자들에게 제공하는 소프트웨어에 대해 보안패치를 배포해야 한다. 모든 네트워크 구성요소에 대해 적정수준의 보안설정을 일관되게 실행하고, 망세분화 · 데이터 손실 방지 시스템 · 네트워크 트래픽에 대한 암호화 방안을 마련해야 한다. 최종 접근지점(서버, 워크스테이션, 모바일 장치 등)에 대한 보호 시스템을 확립해야 하고, 최종 접근지점에 대해 기업 내부망 접근을 허용하기 전에 해당 지점에서 정보보안 정책 기준들이 적절하게 유지되고 있는지를 평가해야 한다. 사용중이지 않은 데이터와 전송중인 데이터는 모두 암호화되어야 한다. 이외에도 금융회사는 영업환경의 변화가 보안 시스템에 어떠한 영향을 미칠지에 대해 평가하고, 필요한 경우 변화된 위험을 적절히 통제하기 위해 추가적인 보안수단을 확보해야 한다.[19]

유럽이 금융회사에게 망분리에 대한 재량권을 인정하는 것은 미국과 유사한 방식으로 사고발생에 대해 강하게 처벌하는 사후규제가 존재하기 때문이다. 유럽의 GDPR은 전산보안 사고에 대한 사후 규제를 명시하고 있는데, 주로 금전적 제재의 형식을 가진다. 구체적으로 살펴보면 EU는 기업이 정보보안을 적절히 수행하지 못해서 개인정보를 유출하거나 다른 유형의 소비자 피해가 발생할 경우 2천만유로와 기업 전체 매출의 4%중에서 높은 금액을 과징금으로 부과하는데, 이는 매우 강력한 수준의 금전적 제재라 평가할 수 있다.[20]

18 EBA Guidelines on ICT and security risk management 3.4.3. Physical security

19 EBA Guidelines on ICT and security risk management 3.4.4. ICT operations security

20 General Data Protection Regulation(GDPR), Chapter 4. Article 83.(General Conditions for imposing administrative fines)

3. 호주의 망분리 규제

호주는 망분리에 대해 직접적이고 공식적인 규정으로 규제하기 보다는 연성규범인 가이드라인을 통해 금융전산 보안의 중요성을 강조하고, 효율적인 보안정책 수립을 위한 기본적인 방향성에 대해 권고하고 있다. 또한 단순한 망분리 방식보다는 망세분화의 개념으로 접근하고 있으며, 망분리는 금융전산 보안 체계를 구축할 때 고려할 수 있는 보안통제 수단의 하나로 인식한다. 호주의 망분리 규제는 기본적으로 호주 건전성 감독청(Australian Prudential Regulation Authority, 이하 APRA)의 정보보안 가이드와 정부기관인 호주 사이버 보안센터(Australian Cyber Security Center, 이하 ACSC)의 세부안내지침을 통해 이루어진다.

APRA는 2019년 금융회사에 대한 건전성 감독의 일환으로 정보보안에 관한 가이드를 발표했다.[21] 규제의 성격은 금융회사 경영진 등이 IT 보안 관련 리스크를 충실히 이해하도록 유도하고, 관련 규정 준수를 위하여 필요한 사항을 숙지하도록 만들기 위해 제정한 연성규정인 실무 가이드라인이다. 동 가이드는 금융회사가 정보보안 정책체계를 구축할 때 활용할 수 있는 정보보안 원칙을 제시하고 있다. 정보보안원칙의 구체적인 내용을 살펴보면 다음과 같다.[22]

a) 금융회사는 정보보안 통제장치를 설계할 때 하나의 통제수단이 훼손되더라도 다른 통제수단이 작동할 수 있도록 다층화된 방식으로 설계
b) 외부로부터의 공격가능성을 줄이기 위해 정보자산에 대한 접근은 영업목적을 달성하기 위한 최소한의 수준으로 허용
c) 정보보안 사고가 발생할 경우 사고로부터의 충격을 최소화하기 위해 신속한 탐지 필요
d) 정보보안체계는 전체 정보시스템 설계의 일환으로 접근
e) 정보자산에 대한 접근과 활용은 모니터링이 가능한 경로를 통해서만 허용
f) 실수나 오류가 정보자산에 대해 승인되지 않은 접근을 허용하지 않도록 시스템 설계
g) 정보자산에 대한 접근과 이용에 있어서 제로베이스 원칙을 실행(the principle of never trust, always identify)
h) 직무역할과 책임수준을 적절히 배분함으로써 직무세분화를 실시
i) 정보보안 정책체계 내에 개인의 판단에 따른 결정을 줄일 수 있도록 내부통제 시스템을 설계
j) 금융전산 사고에 대한 예방적인 조치가 제대로 작동하지 않을 경우에 대비해서 탐지 및 대응체계를 설계

21 APRA(2019), Prudential Practice Guide, CPG 234 Information Security

22 APRA(2019), Prudential Practice Guide, CPG 234 Information Security, Attachment A: Security Principles

APRA 가이드는 정보보안에 대한 통제수단으로 다양한 수단을 활용할 수 있으며, 망세분화(network zones/segments)도 보안통제 수단의 하나로 활용될 수 있음을 명시하고 있다. 금융회사의 정보보안 정책체계는 방화벽, 백신 소프트웨어, 침입 탐지/방지 시스템, 암호화시스템, 모니터링 · 접속분석도구와 같은 정보보안 솔루션 관리방안이 포함되어야 한다. 금융회사는 정보보안에 대한 통제수단으로 망세분화, 종점 통제(end point controls), 게이트웨이 설계, 인증, ID 관리, 인터페이스 통제, 소프트웨어 공학화, 정보보안 솔루션 구축 등의 접근법을 활용할 수 있다. 이상에서 설명한 내용을 종합해 보면 APRA 가이드는 정보보안에 대한 기본적인 원칙을 제시하면서 금융회사가 정보보안에 대한 통제수단을 갖출 것을 요구하고 있다. 정보보안에 대한 다양한 통제수단을 제시하고 있지만, 어떤 조합의 통제수단을 어떤 수준에서 활용할 것인가에 대해서는 구체적인 가이드가 없으며 금융회사가 적절한 접근방식을 선택해야 한다.

정부기관인 ACSC는 호주 내 주요기반시설, 정부, 기업 등 국가 전반의 사이버보안을 담당하는 전담기관이다. ACSC는 금융회사를 포함한 호주 내 다양한 기관의 네트워크 담당자가 망분리 시 고려해야 할 세부사항을 기재한 안내서[23]를 발간하였다. 안내서는 망세분화가 네트워크 침입행위로부터 발생하는 피해를 줄일 수 있는 매우 효과적인 방법임을 설명하고 있다. 정확하게 실행될 경우 망세분화는 악의적인 네트워크 침입자가 기업의 가장 민감한 정보에 접근하는 데에 있어 큰 제약요소가 될 수 있으며, 악의적인 접근을 신속히 탐지하는 데에도 상당히 효과적이다. 전통적으로 망세분화는 해당 기업의 인터넷 접속 게이트웨이에 방화벽을 설치하거나 이중의 방화벽을 설치하여 내부망과 외부망을 분리하는 방식으로 설계된다. 그런데 전체 내부망을 획일적인 신뢰구역으로 인식하는 것은 악의적인 네트워크 침입자가 한번만 방화벽을 돌파할 경우 전체 정보에 대한 광범위한 접근이 가능해지는 문제가 발생한다. 따라서 금융회사는 데이터의 민감수준을 바탕으로 망세분화를 통해 내부망을 계층화시킴으로 민감정보에 대한 보호를 두텁게 유지할 필요가 있다. 동 안내서는 망세분화가 반드시 물리적인 세분화의 형태가 되어야 한다고 기술하지 않으며, 사례를 통해 논리적인 세분화도 금융회사의 선택지가 될 수 있음을 인정하고 있다.

호주는 망분리 방식에 대해 금융회사들의 선택권을 존중하지만 정보보안 사고가 발생할 경우 금융회사는 무거운 책임을 피할 수 없다. 금융회사가 정보보안과 관련된 법률을 위반하거나 책임을 충실히 다했다고 보기 어려운 경우 금융회사는 벌금, 제재 또는 면허정지 등의 행정처벌을 받을 수 있다. 호주의 개인정보 보호법(Privacy Act 1988)은 심각한 수준의 규정위반에 대해 2백

23 ACSC(2021), Implementing Network Segmentation and Segregation

만호주달러 수준의 벌금을 부과할 수 있으며[24], APRA는 위반의 중대성에 따라 벌금, 시정명령, 면허정지 등의 제재를 부과할 수 있다.

4. 국제적 기구의 권고사항

정부의 공식적인 규제 또는 연성규제의 영역은 아니지만 국제적 기구에서 제안하는 정보보안 관련 기준도 망분리 규제설계에 활용할 수 있는 유용한 비교자료이다. 가장 대표적인 국제적 기준으로 신용카드업계 데이터보안표준(Payment Card Industry Data Security Standard, 이하 PCI DSS)과 국제표준화기구(International Standardization Organization, 이하 ISO)와 국제전자기술위원회(International Electro-technical Commission, 이하 IEC)가 제안한 정보보안, 사이버보안 및 개인정보 보호-정보보안 통제지침[25]을 들 수 있다.

PCI DSS는 신용카드 회원의 개인정보를 보호하는 것을 목적으로 정해진 신용카드업계의 대표적인 정보보안 표준이다. 2004년 글로벌 카드사인 VISA, MasterCard, American Express, Discover, JCB의 5개사로 구성된 PCI Security Standards Council에 의해 최초로 제정되었다. 이후 지속적인 개정이 이루어졌고 2024년 6월 PCI DSS v.4.0.1이 발간되어 신용카드 업계의 표준으로 활용되고 있다. PCI DSS는 카드사용자에 관한 데이터(Cardholder Data Environment, 이하 CDE)는 카드사의 다른 네트워크로부터 분리할 것을 권고한다. CDE를 카드사 네트워크로부터 분리할 경우 PCI DSS를 실행하고 유지하는 데에 드는 비용과 기술적 어려움을 줄일 수 있음을 밝히고 있다. 적절한 수준의 망세분화를 실행하지 않은 채 전체 망을 단일망(flat network)으로 관리할 경우 PCI DSS가 전체 단일망에 적용되어 관리비용이 크게 증가할 수 있다. 망세분화는 다양한 물리적인 방식과 논리적인 방식중에 선택하여 활용할 수 있으며, 카드사는 확보한 CDE를 관리하는 데에 있어 최적의 방법의 선택하여 망세분화를 구축할 수 있다.

24 Privacy Act 1988, Section 74, Section 80U

25 ISO/IEC 27002:2022, Information security, cybersecurity and privacy protection – Information security controls(2022)

<표 III-1> PCI-DSS와 우리나라의 망분리 접근방식 비교

	PCI-DSS	한국
망분리 개념	망세분화(network segmentation)	내부망과 외부망 차단
망분리 목적	관리비용 절감 & 기술적 전문화	사고발생 방지
망분리 방식	물리적 망분리와 논리적 망분리 모두 가능	물리적 망분리
보호대상	핵심정보	내부정보

ISO/IEC 정보보안 통제지침(ISO/IEC 27002:2022)은 금융회사뿐만 아니라 정보보안관리시스템을 운영하는 모든 단체에 적용할 수 있는 기본적인 정보보안 안내지침서이다. 안내지침서는 네트워크 보안 통제를 위하여 네트워크를 신뢰수준이나 조직특성별로 세분화하는 방법론을 제시한다. 세분화의 방법으로는 물리적 통제와 기술적 통제가 있음을 설명하고 있는데, 물리적 통제와 기술적 통제는 상호 배타적인 것이 아니며 해당 조직의 데이터 특성 및 보안위험을 감안하여 적절한 방법론을 선택할 수 있음을 설명한다. 정보보안 통제지침은 데이터 분류와 처리방법에 대한 지침도 포함하고 있다. 효율적인 정보보안관리시스템은 체계적으로 정리된 데이터분류체계에 기반하고 있음을 강조하고, 정보자산의 기밀성, 무결성, 가용성을 확보하기 위해 적절한 분류체계를 수립할 것을 권장하고 있다.

5. 국가간 망분리 규제방식 비교 및 해외사례로부터의 시사점

해외의 망분리 규제 사례분석을 통해 알 수 있는 사실은 해외의 금융당국과 금융회사는 망분리 규제에 대해 포괄적인 관점에서 유연하게 접근하고 있다는 점이다. 기본적인 규제원칙에 있어서 금융회사의 망분리에 관한 재량권을 존중하되 보안책임은 무겁게 묻는다는 공통점이 관찰된다. 전산보안관리가 충실히 이루어진다면 망분리의 방식에 금융회사들의 자율적 재량권을 높은 수준으로 인정한다. 미국, 유럽, 호주의 금융당국은 망분리를 금융전산 보안을 위해 필수적인 요소로 인식하는 것이 아니라 신뢰구역(내부망)을 보호하기 위해 고려할 수 있는 선택수단중의 하나로 인식한다. 이러한 인식은 망분리에 대한 접근방식에 있어서도 차이를 가져오는데, 국내 망분리가 내부망과 외부망의 차단에 초점을 맞추고 있는 것과는 대조적으로 해외의 경우 네트워크 간의 연계를 어떠한 방식으로 통제할 것인가에 초점을 맞추고 있음이 관찰된다. 망분리에 관한 접근방식의 차이는 금융회사의 금융서비스 구조설계에 반영되어 나타나는데, 예를 들어 해외 금융회사들의 클라우드 서비스 활용수준에서 차이가 관찰된다. 해외 금융회사들에 대한 설

문조사 결과를 살펴보면 금융업권 중 안정성 문제 때문에 클라우드 이용에 가장 소극적인 은행조차도 2022년 기준 조사대상의 82%가 메인프레임의 50% 이상을 클라우드로 전환했거나 전환할 계획인 것으로 나타났다.[26] 2023년의 조사에서는 글로벌 금융회사의 66%가 성장과 혁신을 위해 클라우드 전환을 추진하고 있는 것으로 나타났다.[27] 총자산 기준 세계 20위인 스페인의 산탄데르은행은 2022년에 전 세계에 분포된 그룹 전산시스템의 80% 이상을 클라우드로 이관한 사례도 관찰된다. 이와는 대조적으로 국내 금융회사의 클라우드 이용은 완만하게 확대되고 있으나 아직은 초기단계에 머무르고 있다.[28] 전술한 해외 주요 국가의 망분리 규제방식을 요약해서 설명하면 <표 III-2>와 같다.

<표 III-2> 주요 국가의 망분리 규제방식 비교

	규제원칙	재량권 수준	금융회사의 책임성
미국	– 네트워크 구분 및 접근 통제를 통한 보안 확보 – 금융회사의 책임성	높음(망분리 방식 선택)	– 규제위반의 심각성을 고려한 사후 규제 – 금전적 제재 중심
유럽	– 정보데이터의 기밀성, 무결성, 가용성 보장 – 금융회사에 대해 높은 수준의 책임 요구	높음(망분리 방식 선택)	– 엄중한 금전적 제재를 통한 사후규제
호주	– 다층화된 정보보안 통제장치의 마련 – 금융회사의 책임성 강조	높음(망분리 방식 선택)	– 다양한 사후규제 적용 – 벌금, 시정명령, 면허정지 등의 제재
한국	– 망분리 의무 부과 – 금융회사의 책임인식 저조	낮음(망분리 방식 지정)	– 낮은 수준의 과징금 및 과태료

해외 망분리 규제에서 관찰되는 또 하나의 특징은 금융회사에 재량권이 부여되어 있음에도 불구하고 우리나라와 같은 물리적 망분리를 선택하는 금융회사가 많지 않다는 것이다. 미국이나 유럽의 금융회사들은 관련 가이드라인을 따라 내부망과 외부망에 대한 보안통제를 실시하는데, 망세분화의 기법은 물리적인 접근법과 논리적인 접근법을 모두 허용한다. 물리적인 접근법을 쓰는 금융회사들이 일부 관찰되지만 대체로 논리적인 접근법을 다양한 방식으로 활용하여 금

26 Accenture(2022)

27 PwC(2023)

28 서병호(2022)

융전산 보안관리를 하고 있음이 관찰된다. 주목할만한 점은 물리적 망분리가 허용되어 있음에도 물리적 망분리만을 선택하는 금융회사는 찾아보기 어려우며, 특히 대형 금융회사들중에 물리적 망분리만을 선택하는 경우는 없다고 볼 수 있다. 자산규모 기준 글로벌 주요 금융회사를 살펴보면 물리적 망분리에 전적으로 의존하는 경우는 없으며, 논리적 망분리를 포함한 다양한 방식으로 핵심정보를 보호하고 있다. 이는 물리적 망분리가 가진 장점에도 불구하고 IT환경의 변화에 대한 적응이 느리고 새로운 서비스의 개발에 불편함이 크다는 점이 금융회사들의 선택기준에 중요하게 작용하고 있음을 의미한다. 물리적 망분리를 적용하고 있지는 않지만 글로벌 금융회사들은 금융전산 보안관리에 높은 수준의 시스템을 개발하여 운용하고 있다. 금융서비스가 고도로 디지털화되고 있음을 감안할 때 해외 금융회사들의 이러한 선택이 가지는 의미를 잘 판단할 필요가 있을 것이다.

해외의 금융회사들은 금융전산 보안관리를 위해 국내 금융회사 대비 상대적으로 높은 수준의 비용을 지출하고 있음도 주목할만한 사실이다. 국내의 물리적 망분리는 신뢰구간과 비신뢰구간을 물리적으로 차단하는 것으로 지출되는 비용에 비해 보안관리 효과가 상대적으로 좋은 접근방법이라 평가할 수 있다. 해외의 금융회사들도 이러한 점은 충분히 인식하고 있으나 시장변화에 적응함으로써 경쟁력을 유지하는 데에는 한계가 있다는 인식하에 높은 비용이 들어가지만 유연성을 가질 수 있는 다양한 접근법을 활용하고 있다. 높은 인적 · 물적 투자를 기꺼이 감수하는 모습을 보이는데, 이는 적정한 수준의 시스템 유연성과 높은 수준의 보안환경을 가지려면 그에 상응하는 투자가 동반되어야 함을 의미한다. 글로벌 기업들의 IT투자중에서 정보보안을 위해 지출하는 비용의 비중은 산업별로 상이한데, 금융회사의 경우 2023년 기준 9.6%인 것으로 나타났다.[29] 글로벌 시장에서 기업들은 정보보안 비용으로 2023년 1,621억달러를 지출했고, 2024년에는 1,838억달러를 지출할 것으로 추정된다.[30] 반면 국내 금융회사들은 오랜 기간 물리적 망분리에 의존해 왔기에 해외 금융회사들처럼 보안투자를 적극적으로 실행하기가 부담스러울 가능성이 크다. 망분리 규제 방향성에 변화가 필요하다는 점은 대체로 인정하는 추세이지만, 망분리 규제변화를 내재화시킬 수 있을만큼 국내 금융회사들의 보안투자가 성숙해 있다고 평가하기는 어려울 것이다.

29 Kolodiy(2024)

30 Gartner(2024)

IV. 금융회사 망분리 규제의 개선방향

1. 망분리 규제개선을 위한 기본 정책방향

장기적인 관점에서 망분리 규제의 방향성은 망분리 방식에 대해 금융회사의 선택권을 인정하되, 금융전산사고가 발생할 경우 그에 대한 책임을 무겁게 하는 방식을 고려해 볼 필요가 있다. 금융회사마다 영업특성에 따라 정보보안의 적정수준이 달라질 수 있음에도 현재의 망분리 규제는 모든 금융회사에 대해 물리적 망분리를 의무화하고 있다. 소프트웨어 활용방식이 자체구축형에서 구독형으로 바뀌고 있고 클라우드 서비스가 보편화되고 있음을 감안할 때 금융서비스의 개발에 있어 획일적인 물리적 망분리가 가진 한계가 점점 뚜렷해지고 있다. 해외 금융당국과 금융회사들의 사례에서 보듯이 금융회사가 스스로의 보안수요에 상응하는 정보보안 접근법을 선택할 수 있도록 허용하는 것은 ICT시장의 진화방향성과 금융서비스의 제공방식의 상관관계를 고려할 때 불가피한 선택일 것이다. 전술한 바와 같이 해외의 대형 금융회사들은 보안효과가 상대적으로 선명한 물리적 망분리를 선택할 수 있음에도 불구하고 물리적 망분리를 활발하게 활용하고 있지는 않음을 관찰할 수 있다. 논리적 망분리 방식이 물리적 망분리 방식에 비해 결코 비용이 적게 든다고 평가하기 어려움에도 물리적 망분리에 대한 선택이 활발하지 않다는 점은 국내 망분리 규제에 시사하는 바가 크다. 금융회사가 자율적으로 망분리 방식을 선택할 수 있도록 허용할 경우 금융회사들은 정보보안에 대한 수요에 따라 현재와 같은 물리적 망분리를 선택할 수도 있고, 반대로 유연성이 상대적으로 높은 여러 가지 접근법을 혼합해서 사용할 수도 있을 것이다.

금융회사가 망분리 접근방식에 대한 재량권을 가지게 될 때 필수적으로 동반되어야 할 사항은 금융전산사고 발생에 대한 책임을 무겁게 물을 수 있는 제도적 환경이 조성되어야 한다는 것이다. 금융회사들은 구조적으로 정보보안에 대한 투자를 인색하게 가져갈 유인을 가진다. 정보보안을 두텁게 한다는 것은 그만큼 많은 인적 · 물적 자원을 투입한다는 것인데, 이는 금융회사의 비용을 증가시키는 요소이다. 사고가 나지 않는 상황에서 정보보안에 대한 비용지출은 경영진에게 높은 심리적 부담감을 줄 수 있으며, 정보보안 방식에 재량권이 있는 금융회사는 보안투자를 줄이는 결정을 할 위험이 있다. 금융전산사고는 자주 발생하는 것은 아니지만 한번 발생할 때 그 피해규모가 상당히 크며, 피해를 보는 고객의 숫자도 광범위한 경우가 많다. 따라서 금융회사

가 최적보다 낮은 수준의 보안투자를 하지 않도록 보안사고에 대해 배상책임을 강화하고, 실효성있는 과징금을 부과하는 것은 안정적인 보안환경을 구축하기 위해 매우 중요한 사안이다. 국내에서는 금융회사의 보안관련 사고에 대한 처벌이 느슨하다는 비판이 이어지고 있다. 예를 들어 2020년 N은행·K카드·L카드의 개인정보 유출사건에 대해 불과 1,000~1,500만원의 벌금형이 선고된 사례가 있다. 이들 업체는 2012~2013년 외부 용역업체를 통해 총 1억 건의 개인정보가 무단 유출된 것을 방치한 혐의를 받았다. 금융당국은 이들 금융사에 업무정지 3개월 및 관련 임직원의 해임권고·직무정지 등의 중징계를 처분했지만, 실질적인 과징금은 수천만원에 그쳐 처벌이 너무 약하다는 평가를 받았다. 개인 정보 유출에 대한 소비자의 거부감, 개인 정보 보호의 책임이 있는 자에 대한 가벼운 처벌과 실효성 없는 보상 등 종래 자주 보아왔던 문제점을 감안하여 사고발생 시 높은 수준의 과징금을 부과하여 금융회사의 책임을 지금보다 훨씬 더 무겁게 묻고 피해자에 대한 보상을 두텁게 가져가야 할 것이다.

망분리 규제의 변화는 점진적이고 단계적인 방식으로 진행할 필요가 있다. 네트워크 관리방식에 대해 유연성을 부여하는 것은 ICT 시장변화와 금융회사의 경쟁력 유지 차원에서 불가피한 방향성이지만 현재 국내의 금융회사들이 자율적이면서 유연한 정보보안체계를 운영할만한 역량을 갖췄다고 평가하기는 힘들다. 국내 금융회사들은 오랜 기간 정보보안 관리를 물리적 망분리에 의존해 왔다. 물리적 망분리는 적용방식이 상대적으로 단순하고 보안효과가 양호한 편이기 때문에 금융회사는 정보보안에서 발생할 수 있는 복잡한 상황에 직면하는 경우가 많지 않다. 논리적 망분리를 포함한 여러 가지 접근방식에 대한 선택이 가능해지더라도 유연한 시스템에서 발생할 수 있는 복잡한 문제에 대한 해결능력이 충분하지 못하다면 접근방식의 변화에서 많은 시행착오를 겪게 될 것이며, 그 피해는 결국 금융소비자들에게 전가될 위험성이 크다. 금융회사들에게 규제방식의 변화방향성을 사전에 예고한 후 준비할 수 있는 시간을 충분히 부여함으로써 금융회사들이 자율적인 정보보안 관리에 필요한 노하우를 쌓을 수 있도록 유도해야 할 것이다.

2. 망분리 규제개선을 위한 세부 고려사항

망분리 규제의 합리적인 개선을 위해서는 정보보안의 다양한 영역에서 세부적인 개선방안을 마련해야 한다. 우선적으로 준비할 필요성이 있는 부분으로 데이터 분류의 표준화작업을 들 수 있다. 정보보안에서 가장 핵심적인 사안은 결국 데이터의 문제로 귀결된다. 망분리 규제가 실행되어 온 중요한 목적은 금융회사가 보유한 핵심적인 데이터를 보호하기 위함이다. 금융회사는 여

러 가지 종류의 데이터를 관리하는 데 데이터 변수마다 특성과 중요성이 달라질 수 있다. 강하게 보호해야 하는 데이터와 상대적으로 보호의 중요성이 떨어지는 데이터가 있을 수 있다. 금융산업에서 활용되는 데이터 분류를 위한 표준화 기준을 마련함으로써 데이터 분류체계를 고도화시킬 필요성이 크다. 이러한 분류체계를 통해 정보보안이 강하게 필요한 데이터의 종류를 정의함으로써 데이터를 관리하고 정보보안에 소요되는 비용을 최소화시킬 수 있을 것이다.

규제샌드박스의 적극적인 활용도 망분리 규제개선에 있어 중요한 요소라 볼 수 있다. 국내 금융회사들은 오랜 기간 이어져 온 물리적 망분리 규제로 인해 망분리를 다양한 방식으로 접근하는 것에 대해 충분한 노하우를 축적하고 있다고 보기 힘들다. 금융회사들의 망분리 규제전환에 대한 준비가 충분한 상태에서 망분리 규제가 먼저 완화될 경우 금융회사들이 상당한 시행착오를 겪을 가능성이 존재한다. 금융회사들이 다양한 유형의 망분리 접근방식을 시도하고 경험을 쌓을 수 있는 시간을 부여하고 단계적으로 숙련도를 높이기 위해서 규제샌드박스는 유용한 도구가 될 수 있다. 현행 망분리 규제에서 허용되지 않는 접근법이라고 하더라도 금융전산보안상의 우려가 크지 않은 영역에서 금융회사들이 물리적 망분리에서 벗어나 새로운 형태의 망분리 시스템을 운영해 볼 기회를 부여하는 것이다. 이를 통해 금융회사들은 단계적으로 논리적 망분리를 포함한 다양한 가능성을 테스트하고, 망분리 시스템을 효율적으로 이용할 수 있는 경험을 축적할 것이다.

데이터 분류체계를 토대로 개인신용에 관한 정보를 AI와 SaaS에서 활용할 수 있는 방안도 마련할 필요가 있다. 현행 개인정보보호법과 전자금융감독규정은 개인신용정보의 활용에 대해 매우 엄격한 규제를 적용하고 있다. 개인정보는 원칙적으로 국내에서 처리와 보관하도록 의무화하고 있으며, 클라우드로 개인신용정보를 처리할 경우 해당 클라우드의 서버는 국내에 위치하고 있어야 한다. ICT산업에서 가명화 · 암호화 기술의 발전으로 인해 개인신용정보를 가명으로 전환하여 개인정보를 안전하게 처리하고 보관하는 기법이 확대되고 있는 상황을 감안하여 생성형 AI가 암호화를 통해 처리된 개인신용정보를 처리할 수 있도록 허용하고 SaaS로도 동일한 접근방식을 허용하는 방안을 마련해야 할 것이다.

금융회사는 변화될 보안규제 환경에서 고객관리와 영업활동상의 중요한 데이터를 안전하게 관리하기 위한 보안체계를 스스로 마련해야 한다. 중요한 보안사항을 정의하고 경영진의 보안 안전에 대한 의무를 강화하는 방향으로 내부 보안체계를 마련해야 할 것이다. 보안규제가 완화될 때 금융회사는 대규모 보안사고의 위험성이 오히려 높아질 수 있음을 감안하여 다소간의 비용증가가 수반되더라도 높은 수준의 보안리스크 통제체계를 확립해야 한다. 금융당국은 금융회

사의 자율적인 금융전산 보안체계에 대해 정기적인 검사를 진행하고, 보안상의 문제점이 발견될 경우 이에 대한 시정조치를 요구하고, 사고발생 시에는 금융회사에 엄격한 제재를 부과해야 할 것이다.

참고문헌

금융위원회, 2013.7.10, 보도자료, 금융전산 보안 강화 종합대책.

개인정보보호위원회 · 한국인터넷진흥원, 2022, 개인정보의 기술적 · 관리적 보호조치 기준 해설서.

박지윤 · 정윤선 · 이재우, 2016, 금융권 망분리 현황과 망분리 정책 개선에 대한 고찰,『정보보호학회지』26(3), 58-63.

서병호, 2022, 국내 금융회사의 클라우드 현황 및 과제, 한국금융연구원,『금융브리프』31(26).

오정주 · 이환수, 2021, 디지털 금융 산업 활성화를 위한 망분리 규제 개선 방안,『융합보안논문지』21(5), 51-60.

이수환, 2021, 디지털 금융혁신 관련 입법 · 정책과제 –금융부문 망분리 규제 개선을 중심으로-, 국회입법조사처,『NARS 현안분석』제202호.

정다빈 · 나현대 · 김선우, 2020, 디지털 금융 산업 활성화를 위한 망분리 규제개혁 정책 연구 –데이터 중심의 핵심가치 보호와 개발 효율성을 중심으로-, 한국4차산업혁명정책센터,『KPC4IR REPORT』No.11.

조병주 · 윤장호 · 이경호, 2015, 금융회사 망분리 정책의 효과성 연구,『정보보호학회지』25(1), 181-195.

전자금융감독규정 https://www.law.go.kr

Accenture, 2022, The great cloud mainframe migration: What banks need to know, Banking Cloud Altimeter.

ACSC, 2021, Implementing Network Segmentation and Segregation.

APRA, 2019, Prudential Practice Guide, CPG 234 Information Security.

EBA, 2019, Guidelines on ICT and security risk management.

FFIEC, 2016, Information Technology Examination Handbook, Information Security.

Gartner, 2024, Gartner forecasts global information security spending to grow 15% in 2025, Press release.

International Organization for Standardization & International Electro-technical Commission, 2022, Information security, cybersecurity and privacy protection – Information security controls (ISO/IEC 27002:2022).

Kolodiy, 2024, How to create an effective cybersecurity budget in 2024, TechMagic.

Payment Card Industry Security Standard Council, 2024, Payment Card Industry Data Security Standard, Requirements and Testing Procedures.

PwC, 2023, Cloud is the engine required to drive the next wave of innovation within financial services.

DIRECTIVE (EU) 2015/2366 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2015, on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC. https://eur-lex.europa.eu

General Data Protection Regulation https://gdpr-info.eu