OPINION

선임연구위원
황세운

금융회사 망분리 규제 해외사례와 국내 시사점*

금융회사에 대한 망분리 규제는 금융전산 보안사고를 최소화시키기 위해 도입되었는데, 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 물리적 망분리 규제는 클라우드에 기반한 기술의 활용에 장애요소가 되며, 연구·개발 활동에도 지장을 준다.

미국과 유럽의 망분리 규제는 제도화된 규정의 형태가 아니라 가이드라인과 같은 연성규제의 방식을 따르며, 해당 금융회사의 판단과 선택을 기본적으로 존중한다. 금융회사의 재량권을 인정하는 배경에는 자율규제에 대한 기본적인 신뢰와 사고 발생시 책임을 강하게 묻는 사후규제의 전통이 자리잡고 있다. 금융회사들은 관련 가이드라인을 따라 내부망과 외부망에 대한 보안통제를 실시한다. 망세분화의 기법은 물리적인 접근법과 논리적인 접근법이 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 서비스형 소프트웨어(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.

최근 국내에서 금융회사에 대한 망분리 규제를 개선할 필요성이 있다는 지적이 활발해지고 있다. 국내 망분리 규제는 금융전산상에서 발생하는 보안사고를 최소화시킴으로서 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

* 본고의 견해와 주장은 필자 개인의 것이며, 자본시장연구원의 공식적인 견해가 아님을 밝힙니다.

디지털화되고 있다는 점을 감안할 때 향후 발생할 가능성이 있는 금융보안사고는 예측하기가 더욱 어려워지고 있으며, 사고 발생시 피해규모도 매우 클 것이다. 이러한 측면을 감안할 때 금융회사에 대한 망분리 규제는 존속의 필요성이 크며, 시장환경의 변화에 따라 고도화 및 효율화되어야 할 것이다.

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 국내 금융회사 망분리 규제의 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 금융회사 망분리 규제 개선방안을 제언할 것이다.

국내 금융회사 망분리 규제의 주요 특성 및 문제점

국내에서 금융회사 대한 망분리 규제는 전자금융감독규정에 따라 이루어진다. 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 내부통신망과 연결된 내부 업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리 · 차단하고 접속을 금지해야 한다. 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리해야 한다.[1] 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.[2]

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.[3] 그러나 서비스제공 방식과 업무수행 방식의 변화와 같은 금융시장의 환경변화에 적응하기 힘들고 망분리 규제가 가진 기본적인 업무비효율성에 대해 지속적으로 문

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

2) 전자금융감독규정시행세칙 제2조의2(망분리 적용 예외)

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

제제기가 이루어져 왔다.

금융산업에 ICT기술의 도입이 활발해지면서 금융회사는 ICT기술의 변화를 신속히 서비스 제공에 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 서비스형 소프트웨어(Software as a Service: SaaS)로 전환되고 있다. Chat-GPT가 촉발한 생성형 AI 구축경쟁도 금융회사의 서비스 제공방식에 크게 영향을 미치고 있다. 기술적 진보를 얼마나 신속하고 효과적인 방식으로 업무시스템이 접목하는가가 금융회사의 지속가능성에 유의적인 영향을 미칠 것으로 예상된다.

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. 그런데, 중요업무에서의 클라우드 소프트웨어 필요성이 커지고 있다. 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. 특히 AI의 도입은 금융회사 서비스의 경쟁력 유지를 위해서 필수적인 변화의 방향성이다. 대부분의 생성형 AI는 클라우드 기반의 인터넷 환경에서 제공되는데, 인터넷망에 대한 접근제약이 강한 현재의 망분리 규제 하에서는 생성형 AI를 금융회사의 기본적인 서비스에 활용하는 것에 제약이 따른다.

유럽의 금융회사 망분리 규제 접근방식

유럽은 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(pseudonymisation)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.[4)]

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.[5)]

유럽 금융회사들의 전산보안에 가장 구체적인 방향성을 제시하고 있는 것은 EBA가 발표한 금융회사 ICT 및 보안위험 관리 가이드라인(이하 EBA 가이드라인)이라고 할 수 있다. EBA 가이드라인은 금융회사 ICT와 보안위험은 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.[6)]

미국의 금융회사 망분리 규제 접근방식

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.

---

4) General Data Protection Regulation(GDPR), Chapter 4. Article 32.

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

6) EBA, 2019, *Guidelines on ICT and Security Risk Management*.

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)가 발간한 Information Technology Examination Handbook, Information Security[7]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 위험 특성에 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.

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 신뢰구역내에서 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 관찰되지 않는다.

규제기관이 제시한 가이드라인은 아니지만 신용카드업계 데이터보안표준(Payment Card Industry Data Security Standard, 이하 PCI DSS)도 금융회사의 금융전산보안 관리에 중요한 영향을 미치고 있다.[8] PCI DSS는 신용카드 회원의 개인정보를 보호하는 것을 목적으로 정해진 신용카드업

7) FFIEC, 2016, *Information Technology Examination Handbook, Information Security.*

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

계의 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.

해외사례로부터의 시사점 및 국내 금융회사 망분리 규제 개선방향

해외의 망분리 규제 사례분석을 통해 알 수 있는 사실은 해외의 금융당국과 금융회사는 망분리 규제에 대해 포괄적인 관점에서 유연하게 접근하고 있다는 점이다. 미국과 유럽의 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 네트워크간의 연계를 어떠한 방식으로 통제할 것인가에 초점을 맞추고 있음이 관찰된다.

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 접근법이 모두 허용한다. 물리적인 접근법을 쓰는 금융회사들이 일부 관찰되지만 대체로 논리적인 접근법을 다양한 방식으로 활용하여 금융전산 보안관리를 하고 있음이 관찰된다. 주목할만한 점은 물리적 망분리가 허용되어 있음에도 물리적 망분리만을 선택하는 금융회사는 찾아보기 어려우며, 대형 금융회사들중에 물리적 망분리만을 선택하는 경우는 거의 없다고 볼 수 있다.

해외의 망분리 규제체계와 금융회사들의 망분리 접근방식을 참고하여 우리도 금융회사 망분리 규제를 합리적인 방향으로 수정할 필요가 있다. 장기적인 관점에서 망분리 규제의 방향성은 망분리 방식에 대해 금융회사의 선택권을 인정하되, 금융전산사고가 발생할 경우 그에 대한 책임을 무겁게 하는 방식을 고려해 볼 필요가 있다. 소프트웨어 활용방식이 자체구축형에서 구독형으로 바뀌고 있고 클라

우드 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. 해외의 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 망분리 접근방식에 대한 재량권을 가지게 될 때 필수적으로 동반되어야 할 사항은 금융전산사고 발생에 대한 책임을 무겁게 물을 수 있는 제도적 환경이다. 금융회사들은 구조적으로 정보보안에 대한 투자를 인색하게 가져갈 유인을 가진다. 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 금융회사가 최적보다 낮은 수준의 보안투자를 하지 않도록 보안사고에 대해 배상책임을 강화하고, 실효성있는 과징금을 부과하는 것은 안정적인 보안환경을 구축하기 위해 매우 중요한 사안이다. 금융회사에 정보보안에 관한 내부통제 시스템 강화를 요구하고, 중요 보안사항에 대한 경영진의 의무를 높이는 방향으로 조직체계를 변화시킬 필요가 있다.

망분리 규제의 변화는 점진적이고 단계적인 방식으로 진행할 필요가 있다. 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 않았다. 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. 규제샌드박스를 적극적으로 활용해 금융회사들에게 망분리 규제 완화에 필요한 사항을 준비할 시간을 충분히 부여함으로써 자율적인 정보보안 관리에 필요한 노하우를 쌓을 수 있도록 유도해야 할 것이다.