2026 년 2 월 9 일

전자금융감독규정 내 망분리에 관한
BUSINESS SOFTWARE ALLIANCE(BSA) 의견서

금융위원회 귀하

BSA 비즈니스 소프트웨어연합(The Business Software Alliance, **BSA**)[1]은 망분리와 관련하여 금융위원회의 전자금융감독규정시행세칙 개정안 (이하 '시행세칙')에 대해 BSA 의 의견을 제출할 기회가 주어져 기쁘게 생각합니다.

BSA 는 각국 정부와 세계 시장을 중심으로 글로벌 소프트웨어 산업을 대변하고 있는 연합체로, BSA 회원사들은 클라우드 스토리지 서비스, 고객관계관리소프트웨어, 인적자원관리프로그램, 신원 관리 서비스, 보안 솔루션, 협업 소프트웨어 등 다양한 기업 활동을 뒷받침하는 기술 제품과 서비스를 개발·제공하고 있습니다. 또한 다수의 회원사들은 서비스형 소프트웨어(SaaS) 형태의 제품과 솔루션을 한국 경제 전반에 걸쳐 다양한 기업에 제공하고 있습니다. 이에 BSA 는, 한국 기업들이 회원사들의 솔루션을 신뢰하며, 이를 기반으로 사업을 운영하고 성장해 나가고 있다는 점을 매우 뜻깊게 생각합니다.

BSA 는 금융위원회가 금융 서비스 산업 내에서 SaaS 활용을 촉진하기 위해, 전자금융감독규정에 규정된 망분리의 적용 대상에서 SaaS 를 제외하고자 하는 점에 대해 환영의 뜻을 표합니다.[2] BSA 는 이번 시행세칙 개정안으로 망분리 요건이 일률적으로 적용되지 않게 됨에 따라, 금융기관으로 하여금 내부 업무 및 백오피스 기능을 중심으로 보다 폭넓은 클라우드 기반 SaaS 솔루션의 도입이 가능해질 것을 긍정적으로 보고 있습니다. 아울러 규제 샌드박스 체계 하에서 개별 심사에 의존해 왔던 기존의 접근 방식에서 벗어나, 널리 활용되고 있는 SaaS 솔루션의 성숙도, 안정성 및 보안 수준을 적절히 반영하려는 이번 변화는 의미 있다고 생각합니다. 이는 한국의 금융 규제 체계를 현대적인 IT 아키텍처 및 국제적 관행에 부합하도록 하는 중요한 진전으로 볼 수 있습니다.

---

[1] BSA 의 회원사는 다음 기업들을 포함합니다: Adobe, Alteryx, Amazon Web Services, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systemes, Databricks, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Workday, Zendesk, and Zoom Communications Inc.

[2] 금융위원회, "*클라우드 기반 서비스형 소프트웨어(SaaS) 활용 촉진을 위한 금융권 망분리 규제 완화*", 2026 년 1 월, https://www.fsc.go.kr/no010101/86080 (**이하 "금융위원회 보도자료"**). 해당 보도자료에 따르면, 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 시행령」에 따라 지정된 SaaS 프로그램은 「전자금융거래법」 및 「전자금융감독규정」에 따른 망분리 규제를 적용받지 않도록 명시됩니다.

다만, BSA 는 이번 시행세칙 개정안 중 일부 사항이 망분리 요건 완화의 실질적인 효과를 상당히 제약할 수 있다는 점에서, 다음과 같은 우려를 표합니다.

첫째, BSA 는 SaaS 에 대한 망분리 규제의 예외 사항이 고유식별정보 또는 개인신용정보의 처리에는 적용되지 않는다는 점에 대해 우려를 표합니다.

BSA 는 이러한 제한이 고유식별정보 및 개인신용정보 보호를 위한 보안상 이유에서 비롯된 것임은 이해하고 있습니다. 다만, 고유식별정보 또는 개인신용정보를 처리하는 시스템에 대해 망분리를 유지하는 것만으로는 보안 수준이 강화된다고 보기 어렵습니다. 현대의 클라우드 환경에서는 강력한 암호화, 접근 통제, 지속적인 모니터링, 신속한 위협 탐지 등 다층적인 보안 체계가 적용되고 있으며, 이러한 보안 방식은 물리적 또는 논리적 분리만으로는 달성하기 어려운 효과적인 수단으로 널리 인정되고 있습니다. 그럼에도 불구하고 이러한 시스템에 대해 망분리 요건을 유지할 경우, 클라우드 기반 서비스에서 기본적으로 제공되는 고도화된 보안 기능에 대한 활용이 제한될 수 있으며, 그 결과 전체적인 보안 수준을 강화하기보다는 오히려 저해할 가능성이 있습니다.

또한 망분리는 운영상의 복잡성을 초래해 보안 설정 오류의 발생 위험을 높이고, 보안 패치의 배포를 지연시키며, 시스템 전반에 대한 실시간 가시성을 제한할 수 있습니다. 이러한 요인들은 기관이 지속적으로 고도화되는 사이버 위협을 적시에 탐지하고 대응하는 역량을 약화시킬 수 있습니다. 따라서 고유식별정보 또는 개인신용정보가 포함된 시스템에서 클라우드 기반 서비스의 활용을 제한하는 것은, 최상급 보안 기능에 대한 접근성을 저해할 수 있으며, 민감한 금융 데이터를 보호하기 위해 국제적으로 인정되고 있는 위험 기반 접근 방식과도 상충될 수 있습니다.

관련하여, 이러한 제한은 고객 식별이나 신용 관련 데이터를 처리하는 경우에, 단순한 내부 운영 목적이라 하더라도 고객관계관리 시스템, 내부 분석 플랫폼, AI 기반 고객 지원 솔루션 등 일반적으로 활용되는 SaaS 도구들조차 사용이 제한되는 결과를 초래합니다. 특히 이는 클라우드 인프라 환경에서의 안전한 운영을 전제로 설계된 고급 데이터 분석 및 AI 기반 서비스의 도입을 제약하는 요인으로 작용하며, 실시간 사기 탐지나, 보다 개인화된 금융 서비스와 같이 고객 경험과 성과를 직접적으로 개선하는 활용 사례의 확산을 저해할 수 있습니다. 이러한 제약은 결과적으로 금융기관의 핵심 업무 프로세스의 현대화를 제한함으로써, 망분리 요건 완화가 갖는 실질적 효과를 축소시키고, 나아가 한국의 금융 디지털 전환 속도를 저하시킬 뿐 아니라 금융 부문에서의 클라우드 도입 및 혁신을 촉진하고자 하는 정책적 목표에도 부정적인 영향을 미칠 수 있습니다.[3]

[3] 클라우드 도입은 금융 서비스 산업 전반에서 효율성, 보안, 혁신을 제고하는 핵심 요소로 널리 인식되고 있으며, 한국 금융 부문 역시 이러한 효과를 보다 적극적으로 활용할 여지가 있습니다. 아시아개발은행에 따르면, 2023 년 기준 한국의 클라우드 서비스 지출 규모는 GDP 대비 0.29%에 그쳐, GDP 대비 약 0.8%를 클라우드 서비스에 지출한 싱가포르 및 뉴질랜드에 비해 낮은 수준이며, 호주와 일본(각각 GDP 대비 0.3~0.5%)과 비교하더라도 상대적으로 제한적인 수준에 머물러 있습니다. 출처: Asian Development Bank, "*Cloud Computing Policies and Their Economic Impacts in Asia and the Pacific*", 2024 년 1 월, https://www.adb.org/publications/cloud-computing-policies-and-their-economic-impacts-in-asia-and-the-pacific.

둘째, 이행 부담이 과도한 정보보호 통제 의무가 도입될 경우, 실질적으로는 금융기관의 SaaS 도입이 지속적으로 제약될 수 있다는 점에 대해 우려를 표합니다.[4]

특히 SaaS 프로그램에 대한 사전 점검 또는 사전 승인 요구, 지나치게 세부적이고 경직된 기술적 통제, 획일적인 암호화 방식 및 운영 기준을 강제하는 것은 금융회사와 SaaS 제공자 모두에게 상당한 규제 이행 부담을 초래할 우려가 있습니다. 보안에 대한 관리·감독이 중요하다는 점에 공감하고 있으나, 이러한 요건들은 세계적인 규모에서 표준화된 절차에 따라 지속적으로 업데이트·개선·보안 관리가 이루어지는 SaaS 의 운영 현실과는 부합하지 않습니다.

SaaS 제공자 입장에서는 이러한 요건이 적용될 경우, 금융회사에 서비스를 제공하는 것이 현실적으로 어렵거나 비효율적일 수 있습니다. 예를 들어, 개별 금융회사별 맞춤형 설정, 고정된 형태의 소프트웨어 버전 유지, 또는 서비스가 업데이트될 때마다 반복적인 국내 승인 절차가 요구될 수 있습니다. 이는 표준화된 서비스 제공, 보안 패치의 신속한 배포, 공동 플랫폼 상에서의 지속적인 개선을 핵심으로 하는 SaaS 운영 모델의 근간을 훼손할 우려가 있습니다. 그 결과, 서비스 제공자는 업데이트의 적시성을 보장하거나 일관된 보안 수준을 유지하는 데 제약을 받을 수 있으며, 금융 부문의 고객에 대해서는 기능을 제한한 형태로 서비스를 제공할 수밖에 없어, 전반적으로 서비스의 효용성과 실효성이 저하될 수 있습니다.

이와 같은 문제는 기업용 SaaS 서비스에 AI 기반 기능이 서비스의 필수적인 구성 요소로 포함되는 경우가 일반화됨에 따라 더욱 뚜렷해지고 있습니다. 이에, AI 기반 SaaS 가 망분리 예외 적용 범위에 포함됨을 명확히 한다면, 금융회사와 서비스 제공자는 중복적인 승인 절차를 거치지 않고도 통상적인 SaaS 도입 방식으로 해당 기능을 활용할 수 있어, 규제적 확실성을 확보할 수 있을 것입니다. 반대로 이러한 명확성이 확보되지 않을 경우, 위와 같은 요건은 금융 부문에서 활용 가능한 안전하고 혁신적인 솔루션의 범위를 제한할 위험이 있습니다. 나아가, 일부 서비스 제공자들은 규제 준수에 따른 부담이 금융회사를 대상으로 서비스 제공을 지속하기에 과도하다고 판단하여, 금융권에 대한 서비스 제공을 중단하거나 제한하게 될 가능성도 있으며, 이는 결과적으로 시장 전반에서 이용 가능한 안전하고 혁신적인 솔루션의 선택지를 더욱 축소시키는 결과로 이어질 수 있습니다.

앞서 제기한 우려를 종합하여, BSA 는 금융위원회가 SaaS 및 망분리 규제와 관련한 개정안을 보다 위험 기반·성과 중심의 방향으로 검토해 주시기를 기대합니다. 이에 다음과 같은 사항을 참고하여 주시기를 제언드립니다.

- **고유식별정보 또는 개인신용정보를 처리하는 시스템에 대해서도 클라우드 기반 SaaS 활용을 허용해 주실 것을 제언드립니다.**
- **SaaS 에 내재된 AI 기반 기능이 SaaS 예외 적용 범위에 포함됨을 명확히 함으로써, 금융회사와 서비스 제공자가 중복적이거나 수시적인 승인 절차를 추가적으로 거치지 않고 통상적인 SaaS 도입 과정에서 해당 기능을 활용할 수 있도록 규제적 확실성을 제공할 것을 제언드립니다.**

[4] 금융위원회의 보도자료에 따르면, 금융회사는 다음과 같은 사항을 이행해야 합니다: (a) 침해사고 대응기관(금융보안원 등) 평가를 거친 SaaS 를 이용, (b) 접속 단말기(컴퓨터, 모바일단말 등)에 대해 보호대책 수립, 안전한 인증방식 적용, 최소권한 부여 등 엄격한 보안관리, (c) 중요정보 입력·처리·유출 여부 모니터링 및 통제, (d) SaaS 내 데이터의 불필요한 공유·처리 방지나 허용되지 않은 외부 인터넷 접근 통제, (e) SaaS 이용 네트워크 구간 암호화 수립 적용 등 규율을 마련.

- **SaaS 제공 모델과 부합하지 않는 지나치게 세부적이거나 경직된 정보보호 통제 조치는 지양하고, 지속적인 개선과 중앙집중적 보안 관리, 보안 업데이트의 신속한 적용을 가능하게 하는 국제적으로 인정된 보안 관행을 반영해 주실 것을 제언드립니다.**

위와 같은 조치가 이루어질 경우, 금융회사는 보안성과 혁신성을 갖춘 AI 기반 SaaS 솔루션을 보다 원활히 도입할 수 있게 될 것이며, 사이버 보안 수준을 강화하는 동시에 민감한 금융 데이터에 대한 보호를 유지하면서 한국 금융 부문의 디지털 전환 목표를 진전시키는 데에도 기여할 것입니다.

본 의견이 시행세칙 개정 사안에 대한 검토 및 논의 과정에 도움이 되기를 바라며, 본 의견서와 관련하여 문의 사항이 있으시거나 추가 필요하신 부분이 있으면 언제든지 연락 주시기 바랍니다.

감사합니다.

Tham Shen Hong
BSA 아태지역 정책 이사