2026년 4월

금융회사 및 전자금융업자 내부 업무망 SaaS 활용시 망분리 예외 적용

2026. 4. 20.부터 금융회사와 전자금융업자(이하 "금융회사등")가 내부 업무망에서 클라우드 기반 응용소프트웨어(Software as a Service, 이하 "SaaS")를 활용할 수 있도록 허용하는 「전자금융감독규정시행세칙」(이하 "개정안")을 개정·시행되었습니다. 이번 개정은 과거 혁신금융서비스 지정을 통해서만 제한적으로 허용하던 내부 업무망에서의 SaaS 이용을 제도화한 것으로, 금융회사등의 업무 방식 혁신 및 협업 강화, 생산성 향상 및 IT 운영 부담 완화, 내부 관리체계의 체계화 등에 기여할 것으로 기대됩니다.

본 뉴스레터에서는 먼저 1) 개정 「전자금융감독규정시행세칙」의 주요 내용과 2) 내부 업무망에서 SaaS 활용시 금융회사등이 준수해야 할 보안관리 방안에 대해 설명 드리고, 이어서 3) 기존 혁신금융서비스 지정을 통한 망분리 예외 적용과의 차이점 및 기타 4) 시사점 및 유의사항에 대하여 살펴보겠습니다.

1. 개정 「전자금융감독규정시행세칙」의 주요 내용

- '클라우드컴퓨팅 발전 및 이용자보호에 관한 법률 시행령' 제3조제2호에 따른 "**응용프로그램 등 소프트웨어를 사용하는 서비스(SaaS)**"는 전자금융감독규정 제15조 제1항 제3호에 따른 망분리 규제(이하 "**3호 망분리**")의 **예외를 인정받을 수 있도록 명시**되었습니다. 3호 망분리는 PC, 랩탑 등 내부업무용 단말기에 적용되는 망분리 규제로서, 이러한 단말기에서 SaaS를 활용하는 경우에는 위 망분리 예외를 적용할 수 있게 됩니다.

- 다만, 개인정보 유출사고 우려 등을 감안하여 이용자의 **고유식별정보 또는 개인신용정보를 처리하는 경우**에는 위 **망분리 예외를 적용 받을 수 없습니다**. 이러한 개인신용정보에는 가명정보도 포함되어, 가명정보를 처리하는 경우에도 개정 「전자금융감독규정시행세칙」에 따른 망분리 예외를 적용 받을 수는 없으며 혁신금융서비스 지정 신청을 통하여 SaaS를 이용하여야 합니다.

- 한편, SaaS에 대한 망분리 규제 예외가 허용되는 만큼, 이를 보완하기 위한 엄격한 정보보호통제장치 마련이 의무화됩니다. 금융회사등은「전자금융감독규정시행세칙」별표7에서 정한 망분리 대체 정보보호통제를 준수하여야 하며, 동 **정보보호통제 이행 여부를 반기에 1회 평가**하고 **정보보호위원회(위원장: CISO)에 보고**하여야 합니다. 상세한 내용은 다음 목차를 참고 부탁드립니다.

<개정안 신·구조문 대비표(별표7 개정내용은 생략)>

현행	개정안
제 2 조의 3(망분리 적용 예외) ① 규정 제 15 조제 1 항제 3 호나목에서 감독원장의 확인을 받은 경우란 다음 각 호와 같다. 1. ~ 2. (생 략)	제 2 조의 3(망분리 적용 예외) ① 규정 제 15 조제 1 항제 3 호나목에서 감독원장의 확인을 받은 경우란 다음 각 호와 같다. 1. ~ 2. (좌 동) 3. <신설> 이용자의 **고유식별정보 또는 개인신용정보를 처리하지 않는**「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 시행령」제 3 조제 2 호에 따른 **"응용프로그램 등 소프트웨어를 제공하는 서비스"** 이용 목적의 경우
② (생 략) ③ 제 1 항 및 제 2 항의 규정은 금융회사 또는 전자금융업자가 자체 위험성 평가를 실시한 후 **별표 7 에서 정한 망분리 대체 정보보호통제를 적용**하고 정보보호위원회가 승인한 경우에 한하여 적용한다.	② (생 략) ③ (좌 동) ④ <신설> 제 1 항제 3 호의 경우 금융회사 또는 전자금융업자는 별표 7 에서 정한 **망분리 대체 정보보호통제의 이행 여부**를 **반기에 1 회 평가**하고 **정보보호위원회에 보고**하여야 한다.

2. 내부 업무망에서 SaaS 활용시 금융회사등이 준수해야 할 보안관리 방안

- 금융보안원은 금융회사등이 준수하여야 할「전자금융감독규정시행세칙」별표7 '망분리 대체 정보보호통제'의 상세 내용을 담은 '내부업무망 SaaS 망분리 예외 적용에 따른 보안 해설서'를 본 개정안의 시행과 함께 배포하였습니다. 그 주요 내용은 다음과 같습니다.

- **① 침해사고대응기관(금융보안원) 평가를 거친 SaaS 이용**

  - 침해사고대응기관(금융보안원 등)이 **「전자금융감독규정」 별표2의2 평가기준 중 SaaS에 적용되는 '필수' 항목**(10개 항목)에 대하여 '충족'이라고 평가한 SaaS만 이용하여야 하고, 관련 서류를 최신 상태로 유지하여야 합니다.

- 금융보안원의 '충족' 평가를 획득한 SaaS는 금융보안원이 레그테크포털 및 CSP 안전성 평가 통합지원시스템에 공개한 '**SaaS 제공자 평가 현황 목록**'에서 확인 가능합니다.

• **② 단말보호**

- **접속 단말기(모바일 단말 포함)에 대해 보호대책 수립·적용**
  비인가 단말기에서 SaaS를 무단 사용할 수 없도록 접속을 통제하여야 하고, SaaS 이용 단말기에 악성코드 감염 방지 대책, 중요정보 유출 방지 등 보호대책을 적용하여야 하며, 모바일 단말기를 이용하는 경우 「금융회사 재택근무 보안 안내서」 中 외부 모바일 기기 특화 보안 통제 권고 사항 등을 참고하여 정한 내부 보안대책을 준수하여야 합니다.

• **③ 접근통제**

- **허용된 SaaS를 제외한 외부 인터넷 접근통제**
  SaaS 이용 단말기에서 허용된 SaaS를 제외한 외부 인터넷 접속이 되지 않도록 네트워크 통제를 적용하여야 합니다.

- **허용된 기능 외 추가 기능(제3자 앱, 플러그인 등)에 대한 접속·이용 통제**
  SaaS 관리자는 비인가 앱·플러그인 설치나 외부 연동을 모니터링하고, 비인가 SaaS 사용을 방지하는 승인 및 통제 절차를 마련하여야 합니다.

- **접속 단말기 및 사용자 등록· 관리, 안전한 인증 방식 적용, 최소 권한 부여 등 접근 제어 및 권한 관리**
  SaaS 접속 단말기 발급·회수 및 사용자 추가·삭제 절차를 마련하고 시행하여야 하며, SaaS 관리자 계정에 멀티팩터(MFA) 인증을 적용하고(예: 비밀번호 외 일회용 비밀번호, 지문 등 추가 인증 적용), 이용자 그룹별 SaaS 권한을 업무에 필요한 최소한의 범위로 제한하고 최소한의 인원에게만 권한을 할당하여야 합니다.

- **SaaS 내 데이터의 불필요한 공유·처리 방지**
  조직 내 SaaS 이용자만 접근 가능하도록 조치하고 인가되지 않은 부적절한 공유 설정 존재 여부를 주기적으로 점검하여야 합니다.

• **④ 운영·관리**

- **SaaS 정보보호 통제를 위한 상시 관리 체계 확보**

SaaS 보안 담당자 및 책임자를 지정하여 보안관리 절차를 수립하고, SaaS 이용자 및 관리자가 보안관리 방안을 명확히 숙지하도록 보안교육을 실시하며, 관련 위협이나 침해사고 등에 신속하게 대응할 수 있도록 비상연락체계 및 대응절차를 마련하여 운영하여야 합니다.

- **⑤ 네트워크 보호**

  - **SaaS 이용을 위한 네트워크 구간에 대한 보호대책(암호화 등) 수립·적용**
    내부 업무망의 SaaS 이용 트래픽이 대고객 서비스 네트워크에 부하를 주지 않도록 상호 간섭을 최소화하여 구성하여야 하며, SaaS 연계 네트워크 구간의 안전한 통신을 위하여 암호화를 적용하여야 합니다.

- **⑥ 이상행위 모니터링**

  - **접속·이용 시 모니터링 및 로그 수집**
    SaaS 제공자가 이용자·관리자 로그를 1년 이상 보존하도록 설정하며, 이상행위 탐지정책을 마련하여 탐지·분석을 수행하고, 이상행위로 인한 경보가 발생한 경우 담당자에게 통지하고 내부에서 마련한 절차에 따라 조치를 이행할 수 있도록 관리하여야 합니다.

- **⑦ 데이터 보호**

  - **중요정보 입력·처리·유출 여부 모니터링 및 통제**
    고유식별정보 또는 개인신용정보를 처리하는 것이 금지되므로 개인신용정보 등 중요정보가 입력 및 저장되지 않도록 사전 필터를 적용하고 주기적으로 중요정보 입력 여부를 점검하여야 합니다. 또한, SaaS 내 악성코드 감염으로 인한 중요정보 유출을 방지하기 위해 악성코드 점검 기능을 적용하고, 중요정보가 포함된 파일 등은 내부 보안 정책에 따라 암호화 등 보호조치를 적용하여야 하며, 어려운 경우 보완할 수 있는 보안대책을 마련 및 적용하여야 합니다.

3. 기존 혁신금융서비스 지정을 통한 망분리 예외 적용과 비교

- 금융회사등이 내부 업무망에서 SaaS 이용시 엄격한 정보보호통제장치를 마련하고 준수해야 한다는 점은 동일하나, 기존에는 혁신금융서비스 지정 신청시 금융회사등이 관련 내용을 금융당국에 제출하고 검토를 받아야 했다면, 개정안 시행에 따라 금융회사등이 **정보보호통제항목 이행여부를 자율적으로 평가**하고 그 결과를 **정보보호위원회에 보고**하는 것으로 절차가 간소화되었습니다.

- 클라우드 사업자에 대한 평가는 동일하게 CSP 안전성 평가 형태로 침해사고대응기관(금융보안원)이 담당하나, 별도 평가를 추가 수행할 필요 없이 **CSP 안전성 평가('필수' 10개 항목)**만 수행하면 되도록 **일원화**되었으며, 금융회사등이 준수해야 할 보안대책 항목은 기존과 거의 유사하나 21개에서 9개 항목으로 통합 조정되었고 '**SaaS 정보보호 통제를 위한 상시 관리 체계 확보**' **항목이 새롭게 추가**되었습니다.

- 금융보안원의 '내부업무망 SaaS 이용 제도화 관련 FAQ'에 따르면 기존 혁신금융서비스로 지정 및 부가조건을 모두 준수하여 업무개시를 보고한 건은 계속 이용 가능하며, 이미 기존 혁신금융서비스 지정 신청시 침해사고대응기관(금융보안원)으로부터 SaaS 제공자 평가결과를 획득하였다면 이는 제도화 이후에도 유효한 것으로 인정되므로 다시 평가를 거치 않아도 될 것으로 보입니다.

4. 시사점 및 유의사항

- 개정「전자금융감독규정시행세칙」시행에 따라 금융회사등은 다양한 SaaS 형태의 협업도구, 화상회의, 성과관리시스템 등을 이용할 수 있게 되어 업무 및 협업 효율성이 크게 증대될 것으로 보입니다. 다만, 규제 완화에 상응하여 엄격한 정보보호통제가 강조되는 만큼 금융회사등은 다음과 같은 사항을 선제적으로 점검할 필요가 있습니다.

- **(1) SaaS 제공자와 계약시 관련 규제 준수 여부 검토**
  - 이용자는 SaaS 제공자와 계약시 SLA 및 보안 조건을 포함하여 관련 규제 준수 여부를 면밀히 검토하여야 하며, 이용 연장 계약 시에도 관련 규제 준수 여부 주기적으로 검토할 필요가 있습니다.

- **(2) SaaS 특성에 맞는 보안관리 방안 마련 및 관련 평가·관리 체계 수립**
  - 도입하고자 하는 SaaS의 활용 범위와 처리하는 데이터의 성격 등을 고려하여 관련 법령상 요구되는 정보보호통제를 준수할 수 있도록 보안관리 방안을 마련하여야 합니다.
  - 아울러 관련 법령상 요구되는 정보보호통제 이행 여부를 주기적으로 평가하고 미흡한 사항은 즉시 조치할 수 있도록 관련 평가·관리 체계를 수립할 필요가 있습니다.

- **(3) 기타 관련 규제 준수 여부 점검**
  - 개정「전자금융감독규정시행세칙」제2조의3 제4항에 따른 정보보호통제 수행과 별도로, **「전자금융감독규정」 제14조의2에 따른 클라우드 이용보고**는 동일하게 수행할 필요가 있으며, 망분리 대체 정보보호통제 항목 외 **보안교육, 백업 및 재해복구** 등 관련 규제 준수 여부 또한 주기적으로 검토할 필요가 있습니다.
  - 또한, 서버 등 정보처리시스템에 적용되는 전자금융감독규정 제15조제1항제5호의 망분리에는 위와 같은 예외 규정이 마련되지 않았으므로, **정보처리시스템에서 이용하는**

SaaS까지 망분리 예외가 허용되지는 않음에 유의하여야 합니다. AI의 경우에는 기존과 동일하게 혁신금융서비스 지정 절차를 통하여 사용할 수 있을 것입니다.

Authors

김준영
02-3703-1824
joonyoung.kim@kimchang.com

이정민
02-3703-1671
jungmin.lee@kimchang.com

김계정
02-3703-4550
gyejeong.kim@kimchang.com

김영준
02-3703-4640
youngjoon.kim1@kimchang.com