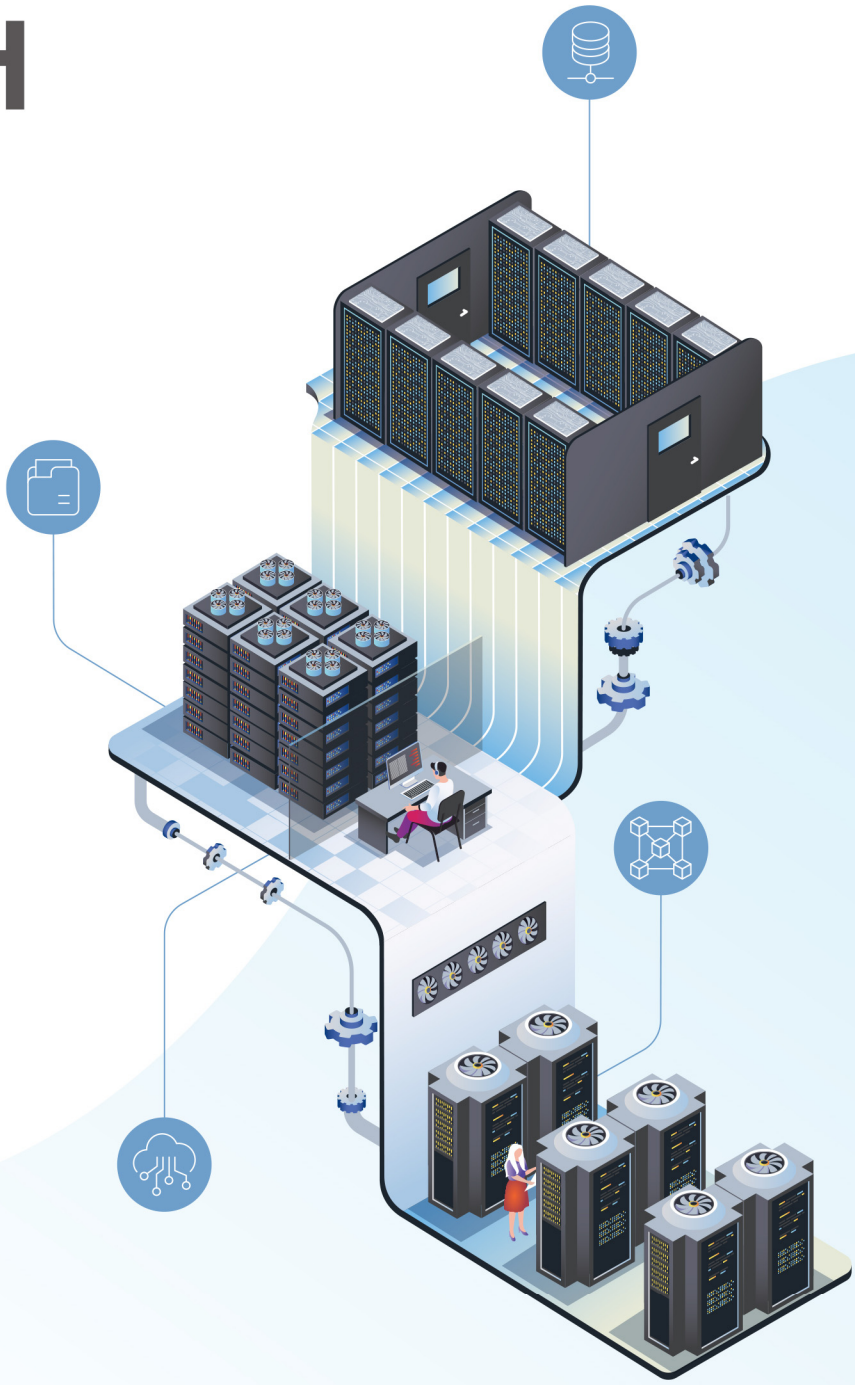
발간번호 | 2026 - 비정기 - AGR - 클라우드평가 - 687

금융미래를 열어가는 금융보안파트너

내부업무망 SaaS 망분리 예외 적용에 따른 보안 해설서

2026. 4.



금융보안원
FINANCIAL SECURITY INSTITUTE


SaaS

목차 CONTENTS

내부업무망 SaaS 망분리
예외 적용에 따른 보안 해설서

PART I

개 요

PART

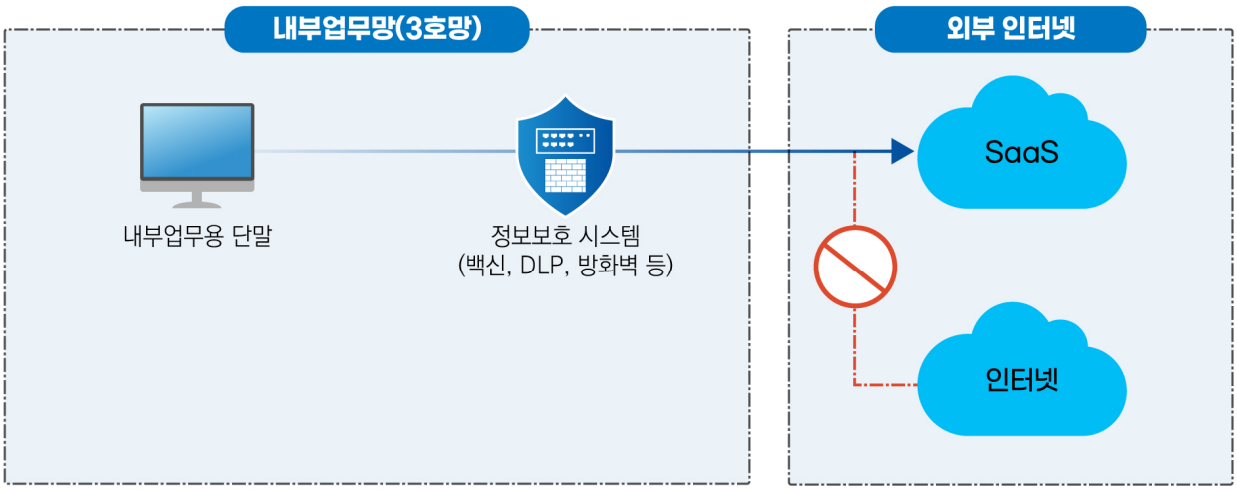
Ⅰ. 개요

본 해설서는 국내 금융회사 등이 내부업무망에서 SaaS를 안전하게 이용할 수 있도록 예상되는 보안 위협을 식별하고, 이를 대응하기 위한 보안관리 방안을 안내

1 내부업무망 SaaS 이용

◆ **(정의)** 금융회사 등이 내부업무망(망분리 환경)에서 인터넷 구간에 위치한 SaaS를 업무 목적으로 안전하게 연계·이용하는 것을 의미

〈 금융회사 네트워크 구성도(예시) 〉



* 내부업무망(3호망): 내부 통신망과 연결된 내부업무용 시스템(전자금융감독규정§15①3)

2 주요 규제 개선 내용

◆ **(내부업무망에서 SaaS 이용 허용)** 금융회사 등은 「전자금융감독규정 시행세칙」 **제2조의3 제1항제3호**에 따라 **내부업무망**에서 **고유식별정보** 또는 **개인신용정보(가명정보 포함)를 처리하지 않는 SaaS 이용 가능**

〈 전자금융감독규정 시행세칙 제2조의3제1항 〉

■ **제2조의3(망분리 적용 예외)** ① 규정 제15조제1항제3호나목에서 감독원장의 확인을 받은 경우란 다음 각 호와 같다.

1. ~ 2. (생 략)

3. 이용자의 고유식별정보 또는 개인신용정보를 처리하지 않는 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률 시행령」 제3조제2호에 따른 "응용프로그램 등 소프트웨어를 제공하는 서비스" 이용 목적의 경우

② (생 략)

③ 제1항 및 제2항의 규정은 금융회사 또는 전자금융업자가 자체 위험성 평가를 실시한 후 **별표 7**에서 정한 **망분리 대체 정보보호통제**를 **적용**하고 정보보호위원회가 승인한 경우에 한하여 적용한다.

④ 제1항제3호의 경우 금융회사 또는 전자금융업자는 별표 7에서 정한 **망분리 대체 정보보호통제의 이행 여부**를 **반기에 1회 평가하고 정보보호위원회에 보고**하여야 한다.

• 망분리 예외에 따른 보안성 확보를 위해 **SaaS 특화 망분리 대체 정보보호통제 적용** 및 **정보보호위원회 승인** 필요

〈 망분리 대체 정보보호통제(시행세칙 [별표7]) 〉

구분	통제 사항
내부업무망 SaaS	• 침해사고대응기관의 평가결과 '충족'을 획득한 SaaS를 이용하고 관련 서류를 최신 상태로 유지 * 규정 〈별표 2의2〉 평가항목 중 SaaS에 적용되는 '필수' 항목에 대한 평가 • 접속 단말기(모바일 단말 포함)에 대한 보호대책 수립·적용 • 접속 단말기 및 사용자 등록·관리, 안전한 인증 방식* 적용, 최소 권한 부여 등 접근 제어 및 권한 관리 * SaaS 관리자 계정 등 중요계정에 대한 다중 인증 적용(예 : ID/PW + OTP) • 중요정보 입력·처리·유출 여부 모니터링 및 통제 • SaaS 내 데이터의 불필요한 공유·처리 방지 • 허용된 SaaS를 제외한 외부 인터넷 접근통제 • SaaS 이용을 위한 네트워크 구간에 대한 보호대책(암호화 등) 수립·적용 • 접속·이용시 모니터링 및 로그 수집 • 허용된 기능 외 추가 기능(제3자 앱, 플러그인 등)에 대한 접속·이용 통제 • SaaS 정보보호 통제를 위한 상시 관리 체계 확보

내부업무망 SaaS 망분리
예외 적용에 따른 보안 해설서

PART Ⅱ

내부업무망 SaaS 이용 시 발생 가능한 보안 위협

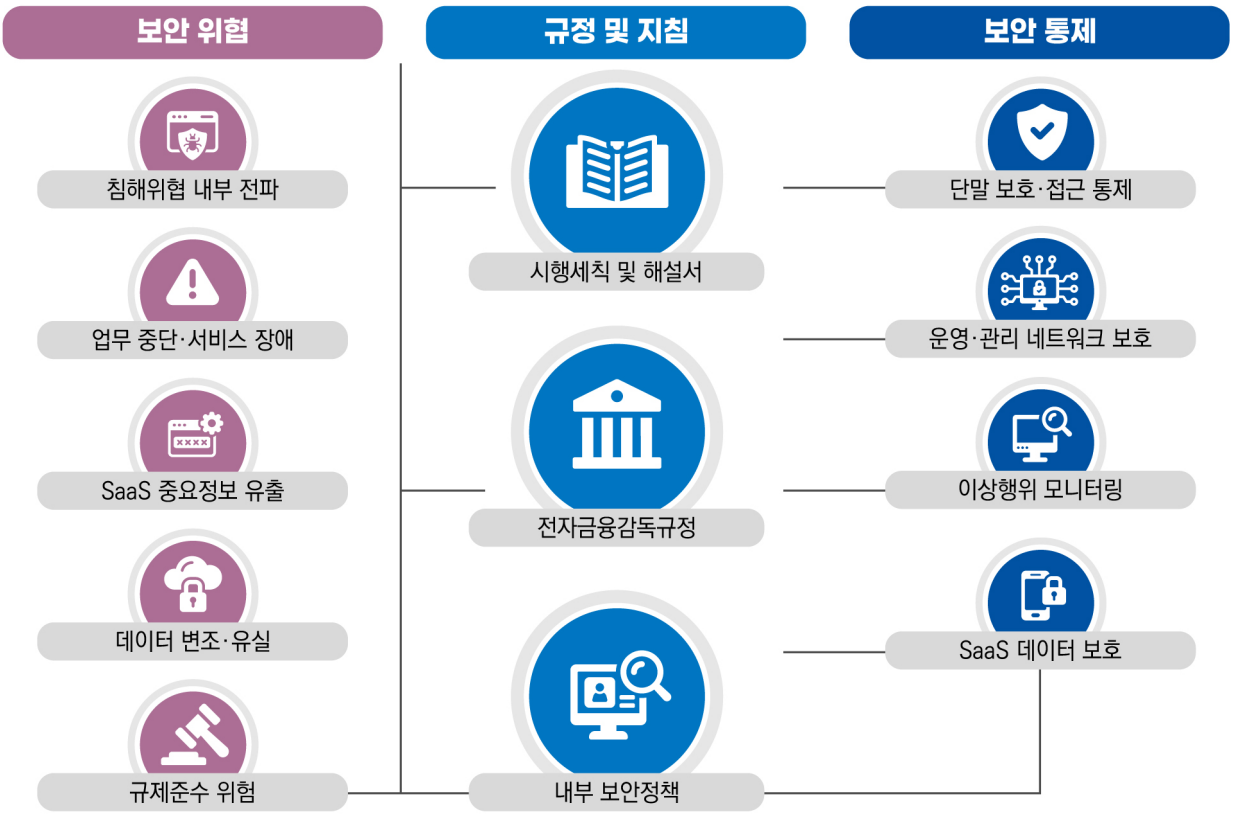
PART

Ⅱ. 내부업무망 SaaS 이용 시 발생 가능한 보안 위협

◈ 내부업무망에서 SaaS 이용 시 SaaS 서비스 취약점, 인프라 장애·프로그램 오류, SaaS 이용자의 보안 설정 미흡 등으로 인해

◈ 내부업무망으로 침해위협 전파, 업무 중단·서비스 장애, SaaS 중요정보 유출, 데이터 변조·유실, 규제준수 위험 등의 보안위협 예상

◆ 금융회사 등은 SaaS 이용에 따른 **예상되는 보안 위협**을 **식별**하고, 규정 및 내부 보안정책, 보안 해설서, 가이드 등에 근거하여 **안전한 SaaS 도입**을 위한 **보안 통제**를 **수립·적용**해야 함



1 SaaS 제공자 보안 위협

◆ **(침해위협 내부 전파)** SaaS 애플리케이션의 **취약점**을 악용해 인증 절차를 우회하여 **계정 권한**을 **획득**한 후, **제공자 시스템**을 통해 금융회사에 **악성코드 유포**

◆ **(업무 중단·서비스 장애)** SaaS 제공자의 클라우드 **인프라 장애** 또는 **소프트웨어** 업데이트 **오류·결함**으로 인한 서비스 지연·장애로 **내부업무 영향**

◆ **(중요정보 유출·데이터 변조)** SaaS 제공자의 **관리자**나 **운영 인력**이 **권한**을 **오남용**하여 **금융회사 중요정보**를 **무단 열람**하거나 **변조**

◆ **(규제준수 위험)** 국외 소재 SaaS 제공자와 서비스 이용 계약 시 **국내 규정 준수 및 의무 이행 협조 조항 누락**

〈 SaaS 제공자에 의한 규제준수 위험 예시 〉

- 금융회사에 맞춤형 SaaS 형태로 도입 시, 표준 계약서의 정책과 개별 금융회사가 체결하는 정책이 상이
- SaaS 제공자의 폐업 또는 인수합병 등으로 서비스가 중단될 수 있으며, 관련 백업 데이터 등의 이관이 적절히 수행되지 않는 경우 SaaS 이용자 정보 유실
- SaaS 제공자의 소재지가 국외인 경우, 이용자 서비스 장애 발생 시 관련 근거 미흡으로 적절한 협조와 지원을 받지 못할 가능성 존재
- 계약서 및 SLA(Service Level Agreement, 서비스 수준 협약)에 로그 보존기간·백업주체 등이 명시적으로 정의되지 않아 법적 보존 기간 미충족

2 SaaS 이용자 보안 위협

◆ **(침해위협 내부 전파)** SaaS 이용 **단말·계정 관리**가 **미흡**하여 **관리자 권한**이 **탈취**되거나 **내부 시스템**으로 **악성코드 감염·전파**

〈 침해위협 내부 전파 위협 예시 〉

구 분	내 용
SaaS 이용 단말 관리 미흡	• 인가되지 않은 단말·외부 IP를 통한 SaaS 계정 로그인 시 내부 데이터 무단 접근 • SaaS 이용 단말 백신의 실시간 감시 기능이 임의로 해제되면, SaaS를 통해 유입되는 파일의 미검증으로 내부 시스템이 악성코드에 감염
비인가 SaaS·플러그인 오남용	• 비인가 SaaS·플러그인 설치로 인한 전송·동기화 과정에서 SaaS가 악성코드 은닉 통로로 활용되어 내부 시스템이 악성코드에 감염
불필요 사이트 접근 허용	• 인가되지 않은 외부 사이트·앱을 통한 데이터 전송·동기화를 내부업무망 통제를 벗어난 경로로 악용하여 무단 데이터 유입·반출

◆ **(업무 중단·서비스 장애)** SaaS 운영·관리 미흡으로 **데이터 유실** 및 **업무 지연**이 발생할 수 있으며, **SaaS 이용망**과 **대고객망**을 **혼용**하는 경우 **서비스 장애**에 **취약**

〈 업무 중단·서비스 장애 위협 예시 〉

구 분	내 용
SaaS 운영·관리 미흡	• SaaS 시스템 장애 시 이용자의 운영·관리 절차(장애 대응 체계 등)가 마련되어 있지 않아 업무 지연 및 중단
SaaS 이용 네트워크 혼용	• SaaS를 내부업무망과 대고객 전자금융거래망을 동일 네트워크로 구성한 경우, SaaS로 인한 네트워크 장애가 대고객 전자금융서비스에 간접적으로 영향

◆ **(중요정보 유출)** SaaS **로그 수집·탐지 규칙 및 점검 절차 부재**, **과도한 공유·접근 권한 허용** 등 보안통제가 미흡한 경우 **위협**이 **식별되지 않거나 정보 유출** 등 **피해 확산**

〈 정보유출 위협 예시 〉

구 분	내 용
감사 모니터링 미흡	• SaaS 로그를 수집하더라도 중요정보 유출 탐지 및 공유 설정 점검을 수행하지 않는 경우 중요정보 유출이 식별되지 않아 피해 확산 지속
SaaS 데이터 통제 미흡	• 생성형 AI의 피드백·학습 전송 차단 기능이 미적용될 경우, 입력된 중요정보가 재노출되거나 삭제되지 않을 가능성
파일 공유·API 오남용	• 파일·폴더, 링크, 공유, API 접근 권한을 외부에 허용한 경우 무단 접근 경로가 형성되어 중요정보가 외부로 반출
단말·권한관리 미흡	• 모바일 단말에서 SaaS 이용 시 파일 복사 제한 등 통제 정책을 미적용하는 경우, 앱 간 데이터 복제를 통해 SaaS 업로드 정보가 외부에 유출
멀티 테넌트 접근통제 미흡	• 내부 SaaS 단말에서 인가되지 않은 외부 테넌트나 개인 계정 접속이 가능한 경우, 내부 단말에서 외부 계정으로 SaaS에 접속하여 파일 다운로드 및 업로드를 통해 데이터 유출·반입

◆ **(데이터 변조·유실)** SaaS **설정 변경 모니터링**, 관리자 계정 **인증**, 전송 구간 **암호화** 등이 미흡한 경우 **데이터 무결성 훼손**, **중간자 공격**으로 **피해 확산**

〈 데이터 변조·유실 위협 예시 〉

구 분	내 용
감사 모니터링 미흡	• SaaS 중요 설정 변경(예: 관리자 계정 추가·삭제, 라이선스 정책 변경, 추가 SaaS 설치 허용·차단 등)이 모니터링되지 않는 경우 보안정책이 무력화되어 데이터 무결성을 훼손하는 등 피해 확대
단말·권한 관리 미흡	• 관리자 계정에 다중인증(MFA)이 적용되지 않고 ID·PW만 사용할 경우 계정 탈취를 통한 보안정책 무단 변경 및 무력화 가능
전송 시 암호화 미적용	• 내부업무망-외부 SaaS 연계 구간에 암호화를 적용하지 않을 경우, 네트워크 구간에서 중요정보가 노출되어 중간자 공격을 통한 데이터 위변조 가능

PART Ⅲ

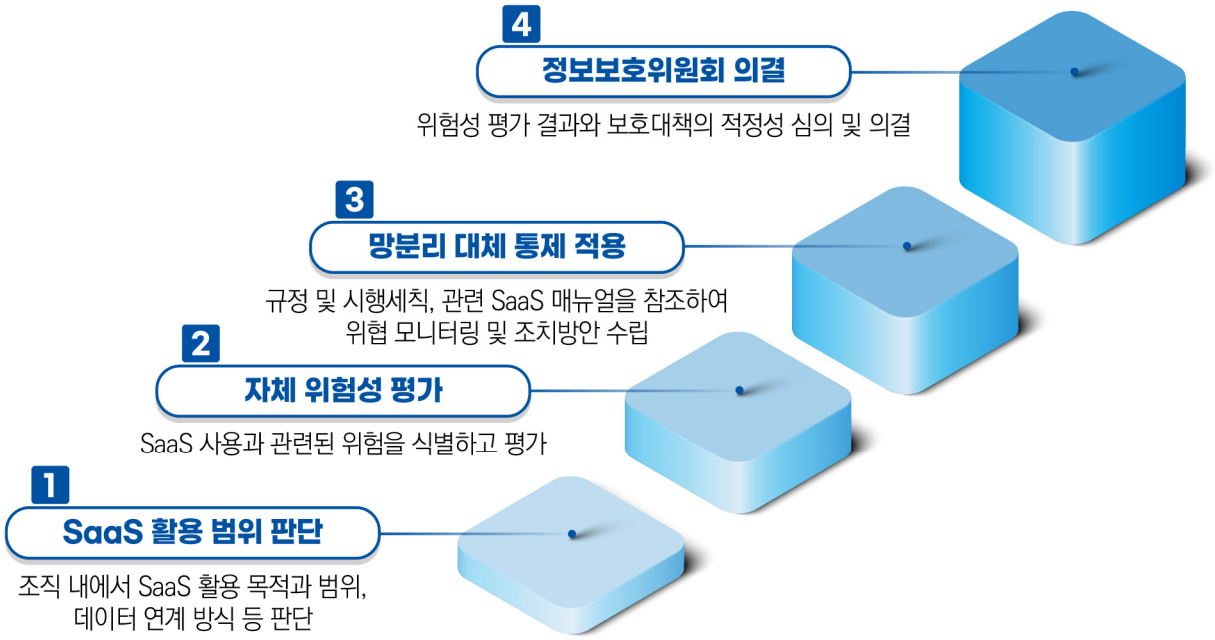
내부업무망 SaaS 이용 보안관리 방안

PART

Ⅲ. 내부업무망 SaaS 이용 보안관리 방안

1 내부업무망 SaaS 도입 절차

내부업무망 SaaS 도입은 ①SaaS 활용 범위 판단 → ②자체 위험성 평가 → ③망분리 대체 정보보호통제 및 추가 보호대책 적용 → ④정보보호위원회 의결 순으로 진행



1. SaaS 활용 범위 판단

◆ SaaS 활용 **범위·목적**, 데이터 **연계 구간·방식** 등을 사전에 확인

- 구체적인 **업무 수행 범위**(업무 종류, 접근 대상, 처리 데이터 등)는 **금융회사**에서 **자율적**으로 **정의**
- 업무 목적에 부합하는 SaaS를 선별하여 도입

2. 자체 위험성 평가

◆ 금융회사 등은 자사의 **업무 환경** 등을 **고려**하여 내부업무망에서 SaaS를 도입(이용)하기 전 **자체 위험성 평가**를 실시

- **예상**되는 **보안 위협**을 빠짐없이 **식별**하고 위협에 대한 **위험성**을 **평가**

※ 위험성 평가 시 최근 보안 취약점 및 보안사고 사례 등을 고려하여 망분리 예외에 따른 보안사고 발생 가능성을 다각도로 검토

3. 망분리 대체 정보보호통제 및 추가 보호대책 적용

◆ **위험성 평가 결과**를 토대로 관련 **규정** 및 **시행세칙**, 관련 **SaaS 매뉴얼**을 참조하여 **자사 환경**에 **적절한 보안 통제 방안** 수립

- SaaS 보안 위협에 따른 **모니터링·조치 방안**을 수립하고, SaaS 특화 「**망분리 대체 정보보호 통제***」**를 적용**

* 「전자금융감독규정 시행세칙」 [별표 7]

- 금융회사 등은 자사의 **업무 환경** 등을 **고려**하여 **필요시 추가 보호대책**을 적용

4. 정보보호위원회 의결

◆ 망분리 예외에 따른 **자체 위험성 평가 결과,** 적용된 **보호대책의 적정성** 등에 대해 **정보보호위원회 의결**

- 자체 위험성 평가를 통해 도출된 **보안위험**이 보호대책 적용 등을 통해 **충분히 완화**되었는지 검토

◆ 정보보호위원회 의결 이후 **망분리 대체 정보보호통제의 이행여부**를 **반기에 1회 평가**하고 **정보보호위원회**에 **보고**

- 내부업무망 SaaS 이용에 대한 **정기적**인 **위험성 평가* 실시** 권고

* 연 1회 보안점검 실시 등

- 내부업무망 SaaS의 추가 이용 및 대상·범위 변경, 주요기능의 추가·변경으로 인한 **보호대책**의 **중대한 변경**이 있는 경우 **정보보호위원회 심의·의결 재수행** 필요

〈 정보보호위원회의 내부업무망 SaaS 도입 심의·의결 시 검토사항(예시) 〉

- 내부업무망 SaaS 활용 범위 설정의 적정성
- 내부업무망 SaaS 이용에 따른 위협 식별 등 자체 위험성 평가 수행의 적정성
- 내부업무망 SaaS 이용에 따라 수립된 보안 통제 방안의 적정성
- 취약점 점검을 포함하여 수립·적용한 보안대책의 적정성
- SLA(Service Level Agreement, 서비스 수준 협약) 및 보안 조건을 포함한 계약의 적정성
  ※ SaaS 제공자와 SLA 및 보안 조건을 계약서에 명시하고 관련 내용을 주기적으로 검토·갱신

- 중요사항 관련 망분리 예외의 경우, 필요 시 이사회 보고

  * 「전자금융감독규정 해설서」('25.8.) 참조

◆ 금융회사 등은 「전자금융감독규정」 제14조의2에서 정한 **기존 클라우드 이용 절차 또한 준수***해야 하며, **내부업무망 SaaS 이용**을 **포함**한 **클라우드 이용**에 관한 **보고의무 이행** 필요

  * 「금융분야 클라우드컴퓨팅서비스 이용 가이드」 참조

2 내부업무망 SaaS 제공자 평가

클라우드서비스 제공자의 안전성이 내부업무망에서 SaaS를 이용하기에 적합한지를 평가

※ (관련 망분리 대체 정보보호통제) 침해사고대응기관의 평가결과 '충족'을 획득한 SaaS를 이용하고 관련 서류를 최신 상태로 유지

1. 평가 개요

◆ **내부업무망 SaaS 「망분리 대체 정보보호통제*」 적용**을 지원하기 위해 **침해사고대응기관**은 **클라우드서비스 제공자**에 대한 **안전성 평가**를 **대표**로 **수행**하고 **결과 공유**

* 침해사고대응기관의 평가결과 충족을 획득한 SaaS 이용

2. 평가 결과

◆ 「전자금융감독규정」의 〈**별표2의2**〉 평가 기준 중 **SaaS 적용 필수 항목***을 **기준**으로하는 **평가 결과 공유**

* [첨부] 내부업무망 SaaS 제공자 평가 항목 참조

3. 평가 결과 활용

◆ **SaaS 적용 필수 항목**이 **모두 충족**인 경우 **평가 결과**를 **내부업무망 SaaS 망분리 적용 예외**에 따른 **정보보호위원회 심의·의결 자료**로 **활용**

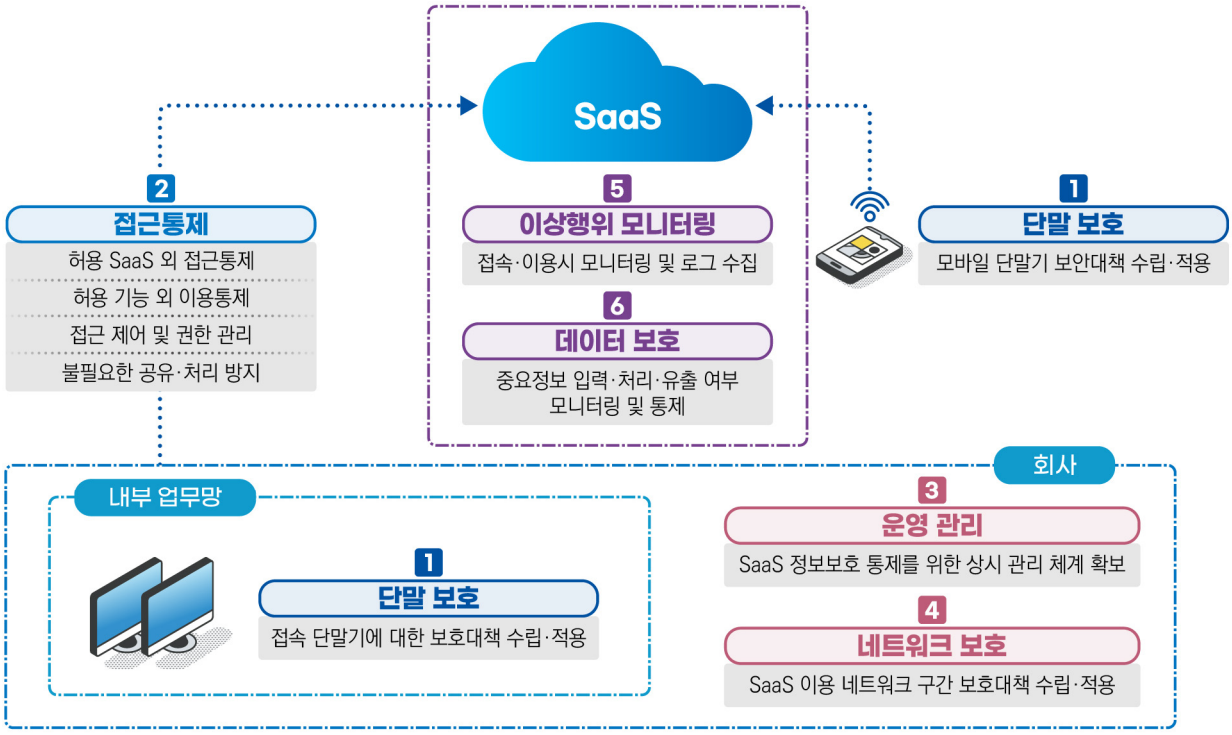
◆ 또한 「**전자금융감독규정**」 제14조의2에 따른 **클라우드 이용 보고 의무 이행***시 **클라우드서비스 제공자 안전성 평가 결과**의 일부로 **활용 가능**

* 「금융분야 클라우드컴퓨팅서비스 이용 가이드」 참조

◆ 금융회사 등은 SaaS 기능 변동 등으로 인해 **클라우드서비스 제공자**의 **안전성이 저하되지 않도록 평가관련 서류**를 **최신 상태로 유지**

3 내부업무망 SaaS 이용 보안대책

내부업무망에서 SaaS 이용 시 발생 가능한 보안 위협과 발생 원인에 대한 보안대책을 안내



통제 분야	망분리 대체 정보보호통제	보안 위협	주요 발생 원인
1 단말보호	• 접속 단말기(모바일 단말 포함)에 대한 보호대책 수립·적용	침해위협 내부전파	• SaaS 이용 단말 관리 미흡
2 접근통제	• 허용된 SaaS를 제외한 외부 인터넷 접근통제	침해위협 내부전파	• 불필요 사이트 접근 허용
	• 허용된 기능 외 추가 기능(제3자 앱, 플러그인 등)에 대한 접속·이용 통제	침해위협 내부전파	• 비인가 SaaS 플러그인 오남용
	• 접속 단말기 및 사용자 등록· 관리, 안전한 인증 방식 적용, 최소 권한 부여 등 접근제어 및 권한 관리	중요정보 유출 데이터 변조	• 단말·권한관리 미흡 • 멀티 테넌트 접근통제 미흡
	• SaaS 내 데이터의 불필요한 공유·처리 방지	중요정보 유출 데이터 변조	• 파일 공유· API오남용
3 운영·관리	• SaaS 정보보호 통제를 위한 상시 관리 체계 확보	업무중단 서비스장애	• SaaS 운영 관리 미흡

통제 분야	망분리 대체 정보보호통제	보안 위협	주요 발생 원인
4 네트워크 보호	• SaaS 이용을 위한 네트워크 구간에 대한 보호대책(암호화 등) 수립·적용	업무중단 서비스장애	• SaaS 이용 네트워크 혼용
		중요정보 유출 데이터 변조	• 전송 시 암호화 미적용
5 이상행위 모니터링	• 접속·이용 시 모니터링 및 로그 수집	중요정보 유출 데이터 변조	• 감사 모니터링 미흡
6 데이터 보호	• 중요정보 처리·유출 여부 모니터링 및 통제	중요정보 유출 데이터 변조	• 감사 모니터링 미흡 • 데이터 통제 미흡
그 외	• 이용자는 SaaS 제공자와 SLA 및 보안 조건을 포함한 이용 연장 계약 시 관련 규제 준수 여부 주기적 검토 필요 • 이용자는 보안교육, 백업 및 재해복구 등 망분리 대체 정보보호통제 항목 외 관련 규제 준수 여부 주기적 검토 필요		

1. 단말 보호

- **접속 단말기(모바일 단말 포함)에 대한 보호대책 수립·적용**
  - 비인가 SaaS 단말기 접속 통제
  - SaaS 이용 단말기 보안대책 적용
  - 모바일 단말기 보안대책 적용

◆ 비인가 SaaS 단말기 접속 통제

- **(단말 보안)** SaaS 이용 단말기 **인가 체계**를 마련하여, 비인가된 단말기에서 SaaS의 **무단 사용을 방지**하는 등 보안 조치 적용
- **(외부 → 내부 접근 제한)** 인가된 단말기, IP, 계정으로만 접근이 **가능하도록** 접근 통제 설정 등 **보안 조치**를 적용
- **(내부 → 외부 멀티 테넌트 제한) 내부 SaaS 이용 단말**에서 **외부 타 테넌트** 및 **개인 계정**으로 접속이 되지 않도록 **보안 조치** 적용

◆ SaaS 이용 단말기 보안대책 적용

- **(악성코드 감염 예방)** 내부 정책에 따라 악성코드 감염 방지 대책을 운영하고, 이에 대한 주기적인 점검을 실시

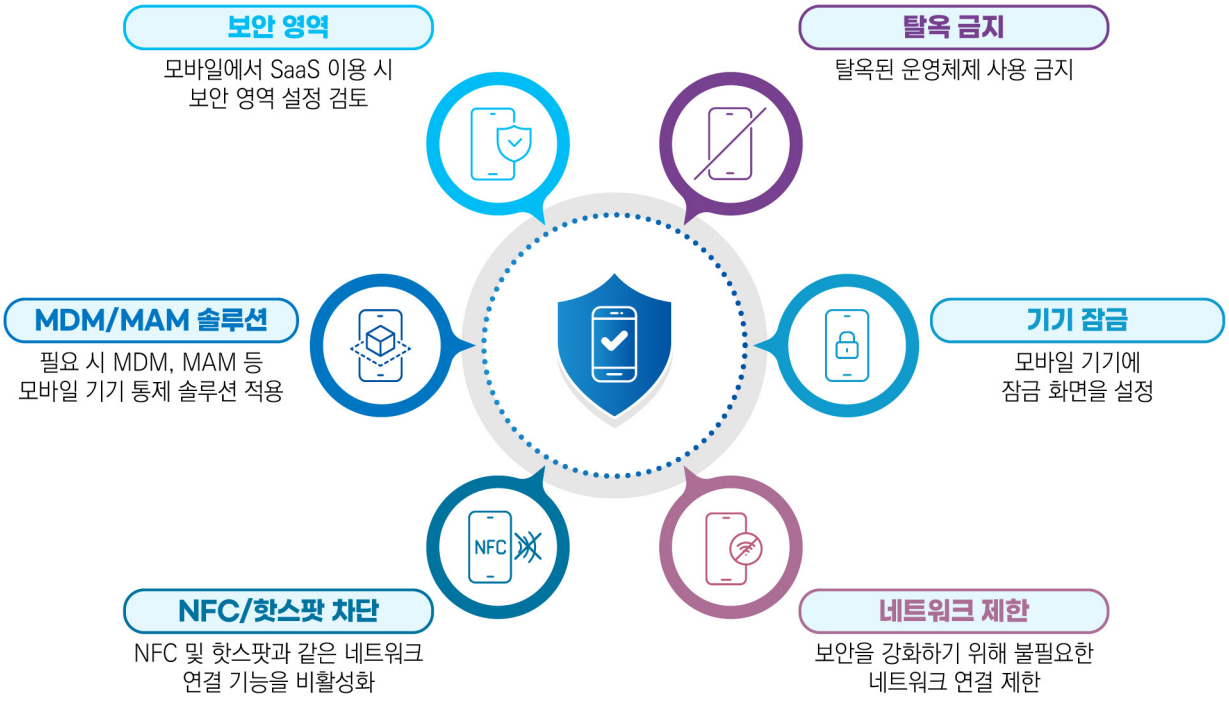
• **(중요정보 유출 방지)** SaaS 이용 단말기(또는 VDI)에서 개인신용정보 등 중요정보 유출 방지를 위해 규정 및 내부 정책에 따른 기술적·관리적 보호대책을 적용

◆ 모바일 단말기 보안대책 적용

• **(모바일 단말 보안) 모바일 단말 환경**에서 SaaS를 이용하는 경우 관련 규정 및 기관별 **내부 보안정책을 준수하고, 중요정보**가 외부로 유출되지 않도록 모바일 기기에 **기술적·관리적**(예: 읽기 권한만 부여) **조치 적용**

※「금융회사 재택근무 보안 안내서」中 외부 모바일 기기 특화 보안 통제 권고 사항 참고

〈 모바일 단말에서 SaaS 이용 시 보안대책(예시) 〉



2. 접근 통제

- **허용된 SaaS를 제외한 외부 인터넷 접근통제**
  - SaaS 이용 단말기 네트워크 통제 적용
- **허용된 기능 외 추가 기능(제3자 앱, 플러그인 등)에 대한 접속·이용 통제**
  - SaaS 연계 및 제3자 제공 앱 통제
- **접속 단말기 및 사용자 등록·관리, 안전한 인증 방식 적용, 최소 권한 부여 등 접근 제어 및 권한 관리**
  - SaaS 접속 단말기 및 사용자 등록·관리
  - 안전한 인증 수단 적용
  - 안전한 계정관리 정책 적용
  - 최소 권한(역할) 설정
- **SaaS 내 데이터의 불필요한 공유·처리 방지**
  - 부적절한 공유 설정 점검 및 제거

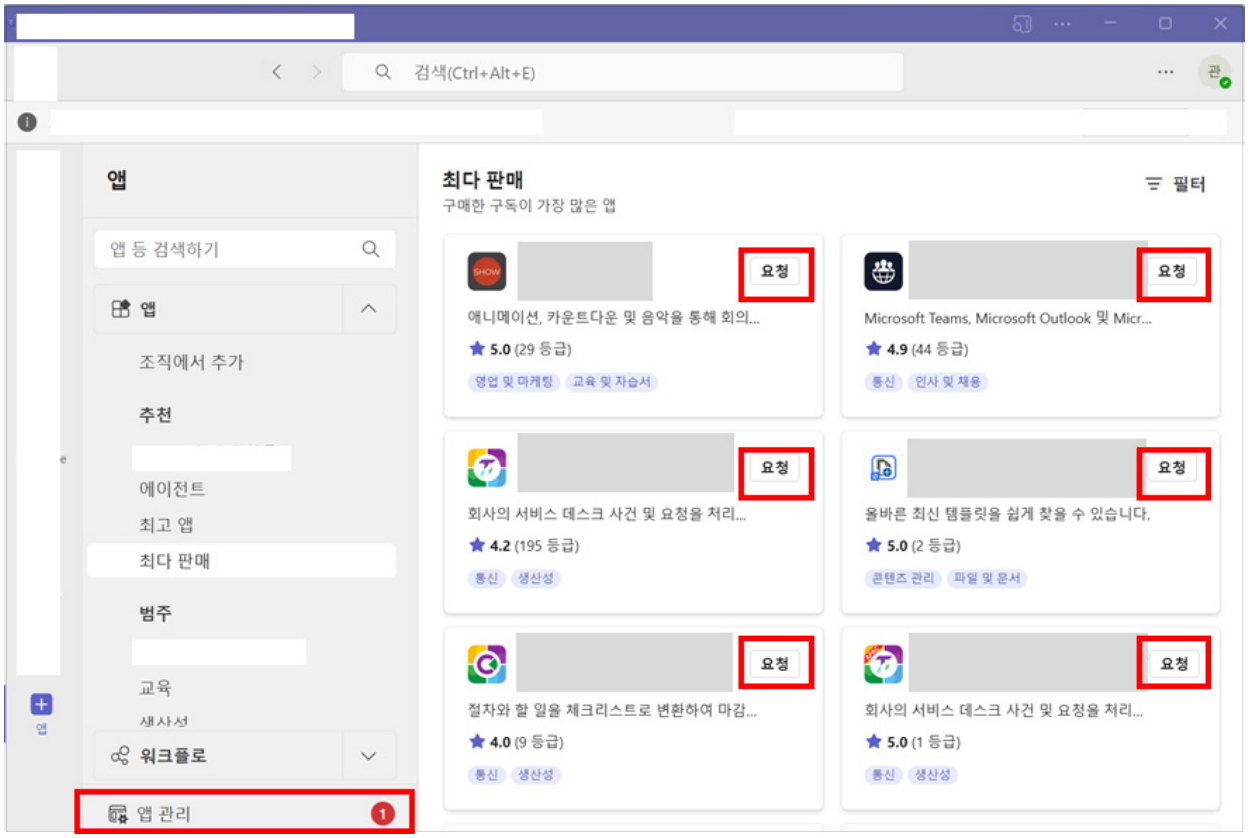
◆ SaaS 이용 단말기 네트워크 통제 적용

- **(허용 SaaS 외 접근통제) SaaS 이용 단말기**에서 **외부 인터넷 및** 허용 SaaS 외 **다른 SaaS**로 접속이 되지 않도록 **접근 통제 설정 적용**

◆ SaaS 연계 및 제3자 제공 앱 통제

- **(안전한 제3자 앱 관리)** SaaS 관리자는 **비인가 앱·플러그인** 설치나 **외부 연동**을 모니터링하고, 내부 정책에 따라 **비인가 SaaS 사용**을 **방지**하는 **승인 및 통제 절차**를 **마련**

〈 외부 SaaS 연동 및 플러그인 설치 화면(예시) 〉



◆ SaaS 접속 단말기 및 사용자 등록·관리

- **(SaaS 단말·사용자 관리 절차 준수)** 내부 정책에 따라 SaaS 접속 단말기 발급·회수, 사용자 추가·삭제 등 관련 **절차**를 **마련**하여 **시행**

◆ 안전한 인증 수단 적용

- **(로그인 시 다중 인증 적용) SaaS 관리자** 계정의 **멀티팩터(MFA) 인증 적용** (예: 비밀번호 외 일회용 비밀번호(OTP), 지문 등 추가 인증 적용)

◆ 안전한 계정관리 정책 적용

- **(비밀번호·계정 관리)** 내부 보안정책에 따른 **비밀번호 설정**, **계정 잠금·해제 등** 안전한 계정관리 정책 적용

◆ 최소 권한(역할) 설정

- **(주기적 권한 검토)** 관리자 또는 이용자 그룹별 **SaaS 역할**과 **권한은** 업무에 필요한 **최소한**의 **범위**로 **제한**하고, 내부 권한 신청·회수 절차에 따라 **최소한**의 **인원**에 **권한**을 **할당**하도록 검토 수행

※ 화이트리스트 기반 또는 역할 기반 접근통제(RBAC) 적용 권고

◆ 부적절한 공유 설정 점검 및 제거

- **(안전한 공유 설정 및 점검)** 조직 내 이용자만 접근이 가능하도록 조치하고, **인가되지 않은 부적절한 공유 설정** 존재 여부를 주기적으로 **점검**

※ 내부↔외부 단말 간 공유 파일(링크)에 대한 접근 가능 여부를 양방향 점검

3. 운영·관리

- **SaaS 정보보호 통제를 위한 상시 관리 체계 확보**
  - 클라우드 서비스 보안 관리
  - SaaS 이용·관리 등 보안교육 실시
  - SaaS 상시 관리 체계 확보

◆ 클라우드 서비스 보안 관리

- **(보안관리 대상 식별 및 관리) SaaS**를 보안 관리 대상으로 **식별**하여 보안 **담당자 및 책임자를 지정**하여 보안 관리 절차 수립

◆ SaaS 이용·관리 등 보안교육 실시

- **(SaaS 이용·보안교육 실시) SaaS 이용자 및 관리자**가 각 **서비스**에 대한 **보안관리 방안**을 명확히 **숙지**하도록 **정기 또는 수시 교육 실시**

◆ SaaS 상시 관리 체계 확보

- **(상시 관리 체계 확보) SaaS 관련 위협, 침해사고** 등에 **신속하게 대응**할 수 있도록 **SaaS 제공자, 관리자, 이용자 간** 비상 연락 체계를 상시 유지(비상연락망 최신화)하고, 담당자별 역할 정의와 대응 절차를 마련하여 상시 운영

※ SaaS 관리자 권한이 국외 또는 타조직에 있어 보안설정 및 망분리 대체 정보보호통제를 직접 수행하기 어려운 경우, 이용자의 보안 통제 요구사항이 반영될 수 있도록 절차 마련

4. 네트워크 보호

- **SaaS 이용을 위한 네트워크 구간에 대한 보호대책(암호화 등) 수립·적용**
  - SaaS 이용 및 대고객 서비스 네트워크 트래픽 상호 영향 최소화
  - SaaS 연계 구간 암호화 적용

◆ SaaS 이용 및 대고객 서비스 네트워크 간 상호 영향 최소화

- **(네트워크 영향 최소화)** 내부업무망의 **SaaS 이용 트래픽이 대고객 서비스 네트워크에 부하를 주지 않도록 상호 간섭을 최소화하여 구성**

◆ SaaS 연계 구간 암호화 적용

- **(안전한 암호화 통신 적용)** SaaS 연계 네트워크 구간에서 안전한 통신을 위한 **암호화 적용**

5. 이상행위 모니터링

- **접속·이용시 모니터링 및 로그 수집**
  - SaaS 이용자·관리자 로그 기록 보존
  - SaaS 이상행위 및 주요 설정 변경 탐지
  - 모니터링 체계 구축

◆ SaaS 이용자·관리자 로그 기록 보존

- **(SaaS 로그 보존)** SaaS 이용 시 제공자가 **이용자·관리자 로그**를 **1년 이상 보존***하도록 설정

  * 「전자금융감독규정」 제13조제1항제9호 참고

◆ SaaS 이상행위 및 주요 설정 변경 탐지

- **(이상행위 탐지)** 감사로그 기반으로 **이상행위**를 **정의***하고, **탐지정책 적용**에 따른 **탐지·분석**을 수행하며, **지속적인 개선** 수행

  * (예) 관리자 계정 접속 시도, 로그인 실패, 해외 로그인 성공 탐지, 관리자 계정 추가·삭제 및 권한 변경, SaaS 주요 설정 변경 등 이상행위

◆ 모니터링 체계 구축

- **(탐지 알람 통지)** 이상행위로 인한 **경보(알람)**가 **발생**한 경우, 담당자가 **인지**할 수 있도록 **SMS, 이메일 등 통지 절차**마련

- **(보안 조치 이행)** 담당자의 이상행위 인지 이후, 내부에서 수립한 **대응 절차***에 따라 조치 이행

  * 침해사고 대응 절차 등

6. SaaS 데이터 보호

• **중요정보 입력·처리·유출 여부 모니터링 및 통제**
- 중요정보 입력 및 저장 방지
- SaaS 내 중요정보 식별
- SaaS 내 악성코드 감염 점검
- SaaS 내 중요정보 유출 방지 대책 적용

※ 내부업무망에서 SaaS 이용시 고유식별정보 및 개인신용정보 처리 불가

◆ 중요정보 입력 및 저장 방지

- **(중요정보 입력 제한·필터링)** 개인신용정보 등 **입력 제한 데이터**를 명확화하여 **기준**을 **마련**하고, **데이터 입력** 시 사전에 **필터 적용**
- **(중요정보 입력 점검)** SaaS 이용 로그를 **주기적**으로 **점검**하여 **입력 제한 데이터**가 **저장·처리**되었는지 **점검**
- **(생성형 AI 학습 방지)** 생성형 AI 모델 개선 등 **이용자 정보 활용 설정**을 **비활성화**하고 **피드백 기능 제한** 등 **데이터 보호 조치 적용**

◆ SaaS 내 중요정보 식별

- **(중요정보 식별) SaaS 내 데이터 생성·저장·처리시 중요정보를 식별하여 SaaS**를 통해 **중요정보가 오남용**되지 않도록 **관리**

◆ SaaS 내 악성코드 감염 점검

- **(악성코드 감염 예방)** 랜섬웨어 등 **SaaS 내 악성코드**로 인한 **감염 및 중요정보 유출**을 **방지하기** 위해 **악성코드 점검 기능**이 있는 경우 **보안 조치**를 **적용**하고, 기능이 없는 경우 단말 또는 네트워크에서 이를 **보완**할 수 있는 **보안대책 적용**

◆ SaaS 내 중요정보 유출 방지 대책 적용

- **(중요정보 보호대책 적용) 중요정보**가 포함된 SaaS 내 파일 등은 내부 보안 정책에 따라 **암호화** 등 **보호 조치 적용**하고, 기능이 없는 경우 이를 **보완**할 수 있는 **보안대책 적용**
- **(중요정보 탐지내역 점검)** 중요정보 **오남용·유출 방지**를 위해 **주기적**으로 **점검**하는 절차 마련

첨부. 내부업무망 SaaS 제공자 평가 항목

◆ 「**전자금융감독규정**」의 〈**별표2의2**〉 평가 기준 중 **SaaS 대상 필수 항목**을 **기준**으로 **평가** 수행

• 필수 항목 중, 해당 사항이 없는 항목은 평가 생략 가능

구분		평가항목	항목	적용대상	비고
1 정보보호 정책 및 법규 준수	1.3 법 및 정책 준수	1.3.1 이용자가 법령 등 의무준수를 위해 필요한 사항을 지원 및 협조하도록 체계가 마련되어있는가?	필수	IaaS, PaaS, SaaS	
	1.4 보안 감사	1.4.1 접근기록 대상을 정의하고 서비스 통제, 관리, 사고 발생 책임 추적성 등을 보장할 수 있는 보안감사 증적(로그)은 식별할 수 있는 형태로 기록 및 모니터링 되고, 비인가된 접근 및 변조로부터 보호되고 있는가?	필수	IaaS, PaaS, SaaS	
5 업무연속성 계획 및 재해복구	5.1 장애 대응	5.1.2 클라우드서비스 중단이나 피해가 발생한 경우 장애보고 절차에 따라 장애상황을 기록하고 이용자에게 현황을 파악할 수 있도록 관련 정보를 제공하는가?	필수	IaaS, PaaS, SaaS	
	5.2 서비스 가용성	5.2.1 가상화 서버, 설비 등 정보처리설비의 장애로 인해 서비스가 중단되지 않도록 관련 설비를 이중화하고, 백업 체계를 마련하고 이행하는가?	필수	IaaS, PaaS, SaaS	
6 침해사고 대응 및 관리	6.2 침해 사고 대응	6.2.1 침해사고 발생 시 침해사고 대응절차에 따라 클라우드 컴퓨팅서비스 이용자에게 발생 내용, 원인, 조치 현황 등을 신속하게 알리고 있는가?	필수	IaaS, PaaS, SaaS	
7 사용자 인증 및 접근통제	7.2 접근 권한 관리	7.2.2 이용자의 정보처리시스템과 관련된 단말기 및 전산자료에 접근권한이 부여되는 정보처리시스템 관리자에 대하여 적절한 통제장치를 마련하고 적용하고 있는가?	필수	IaaS, PaaS, SaaS	
8 가상화 및 인프라 보안	8.1 가상화 보안	8.1.2 이용자가 클라우드서비스 이용 중 가상자원*을 삭제할 경우 삭제대상과 관련된 모든 자원이 복구되지 않는 방법으로 삭제되는가? * 가상머신(이미지,백업,스냅샷등), 가상스토리지, 가상소프트웨어, 가상환경 설정정보 등	필수	IaaS, PaaS, SaaS	
		8.1.3 가상자원에 대한 무결성을 보장하고 가상자원 손상 시 이용자에게 안내하고 있는가?	필수	IaaS, PaaS, SaaS	

구분		평가항목	항목	적용대상	비고
		8.1.5 가상자원 관리 시스템*과 가상 소프트웨어(앱, 응용 프로그램)를 배포하기 위한 공개서버에 대한 관리적, 물리적, 기술적 보호대책을 수립하고 이행하는가? * 가상자원을 제공하기 위한 웹사이트(클라우드 포탈, 클라우드 콘솔, API등)	필수	IaaS, PaaS, SaaS	
10 암호화 및 데이터 보호	10.1 데이터 보호	10.1.6 이용자의 클라우드서비스 이용 계약 종료 시 이용자의 모든 가상자원은 복구가 불가능하도록 삭제하고 있는가?	필수	IaaS, PaaS, SaaS	
11 물리적 보안	11.1 물리적 보호 구역	11.1.2 고유식별정보 또는 개인신용정보 처리 시 전산실 내 무선통신망 사용을 제한(통제) 하고 있는가?	필수	IaaS, PaaS, SaaS	평가 생략[1)]
	11.2 정보 처리 시설 및 장비 보호	11.2.1 고유식별정보 또는 개인신용정보를 처리하는 모든 정보처리시스템을 국내에 설치하고 있는가?	필수	IaaS, PaaS, SaaS	평가 생략[1)]

1) 내부업무망 SaaS에서 고유식별정보 및 개인신용정보를 처리하지 않으므로 평가 생략

2026-비정기-AGR-클라우드평가-687

내부업무망 SaaS
망분리 예외 적용에 따른 보안 해설서

발 행 일 2026년 4월
발 행 인 박 상 원
발 행 처 금융보안원
경기도 용인시 수지구 대지로 132

금융보안원
FINANCIAL SECURITY INSTITUTE

내부업무망 SaaS 망분리 예외 적용에 따른 보안 해설서

금융보안원
FINANCIAL SECURITY INSTITUTE
16881 경기도 용인시 수지구 대지로 132
TEL 02-3495-9000 www.fsec.or.kr