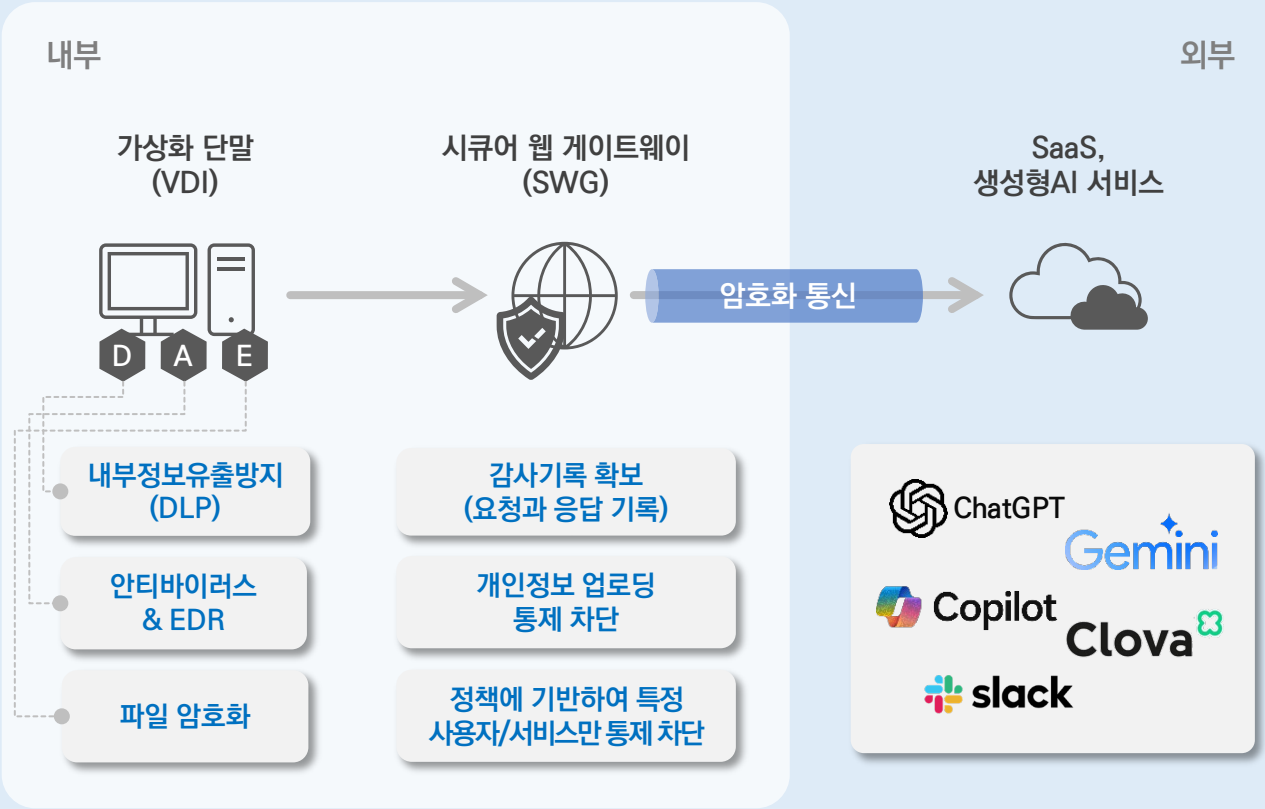
외부 SaaS, 생성형 AI 활용 보안대책

금융 망분리 개선 후 보안 대책

2024.08.22 「금융분야 망분리 개선 로드맵」 설명회

기술적 보호조치 요약



SOMANSA

1. 요약

1. **SaaS서비스/생성형 AI 서비스 접속단말 보안강화** :
   VDI활용과 DLP, 파일암호화, 악성코드 통제체제 구축

2. **단말과 서비스 접근통제 :**
   업무상 허용된 특정 단말과 업무상 허용된 특정 SaaS 서비스로만 접속할 수 있도록 통제 (SWG: Secure Web Gateway 외)

3. **접속 기록 감사로그 확보 :**
   단말과 SaaS 서비스간 요청과 응답값까지 저장 (SWG 외)

4. **이상행위 통제 :**
   단말과 SaaS 서비스간 개인정보 및 신용정보 전송시 차단 (SWG 외)

2. 내부망에서 외부 SaaS 이용 보안대책 (1)

활용범위 확대 및 활용기관의 업무 자율성을 보장하기 위한
기술적 보호조치 구축

구분		보안대책	기술적 보호조치 예
1. 단말기 보안 대책	1.1	SaaS에 접속하는 단말기(이하 SaaS 단말기) 적정성 여부 예) 혁신금융서비스 지정조건에 따라 허용된 단말기만 사용 등	(허가된 사용자에게 허가된 SaaS만 접속하도록) SWG를 통한 SaaS 접속 통제
	1.2	SaaS 단말기에 대한 망분리 대체 통제 (전자금융 감독규정 시행세칙 별표7) 적용여부 예) 관리자 권한제거, 승인 프로그램만 설치·실행, 전산자료 암호화 등	가상화 단말 VDI 활용, DLP, AV/EDR, 파일 암호화
	1.3	SaaS 단말기에서 고객정보 유출방지를 위한 보안대책의 적정성 여부	VDI, DLP, AV/EDR, 파일 암호화
	1.4	SaaS 단말기 내 악성코드 감염 방지대책 마련여부	AV/EDR
	1.5	모바일 단말기에 특화된 보안대책 마련여부	MDM외

2. 내부망에서 외부 SaaS 이용 보안대책 (2)

활용범위 확대 및 활용기관의 업무 자율성을 보장하기 위한
기술적 보호조치 구축

구분		보안대책	기술적 보호조치 예
2. SaaS 연계 보안 대책	2.1	SaaS 단말기 ↔ SaaS 간 인가된 SaaS 단말기만 접속할 수 있도록 구성	(허가된 사용자에게 허가된 SaaS만 접속하도록) SWG를 통한 SaaS 접속 통제
	2.2	SaaS 비인가 접근 방지를 위한 안전한 인증방식 적용여부	SaaS 솔루션 인증 강화 DLP 솔루션 강화된 인증 외
	2.3	SaaS이용 네트워크 트래픽과 전자금융거래 등 대고객 네트워크 트래픽이 상호 혼용되지 않도록 네트워크를 구성하고 있는지 여부	가상화 단말(VDI) 네트워크 영역을 통해서만 접근 (허가된 단말만 접속하도록) SWG를 통한 SaaS 접속 통제 외
	2.4	SaaS 단말기 ↔ SaaS 연계 네트워크 구간에 안전한 암호 알고리즘을 통한 암호화 적용여부	TLS 1.3 통신 외

2. 내부망에서 외부 SaaS 이용 보안대책 (3)

활용범위 확대 및 활용기관의 업무 자율성을 보장하기 위한 기술적 보호조치 구축

구분		보안대책	기술적 보호조치 예
3. SaaS 관리 보안 대책	3.1	**사용자 또는 그룹별 SaaS 역할 및 권한이 업무에 필요한 최소한의 범위로 제한되어 있는지 여부**	**(허가된 사용자에게 허가된 SaaS만 접속하도록) SWG를 통한 SaaS 접속 통제**
	3.2	SaaS 관리자는 부적절한 공유설정이 존재하는지 여부를 주기적으로 점검하고, 부적절한 공유설정이 확인되는 경우 이를 제거하는 체계가 마련되어 있는지 여부	
	3.3	**SaaS 사용자 및 관리자의 SaaS 접속 및 이용로그를 기록하고 로그 보존기간을 1년 이상으로 설정하고 있는지 여부**	**SaaS 접속 기록 저장, 요청과 응답값 모두 저장 (SWG외)**
	3.4	SaaS 관리자는 SaaS 이용로그, SaaS 접속 인증 오류, SaaS 중요 구성 변경 등에 대해 모니터링하고 이상징후 발견시 확인 등 보안조치를 이행하는지 여부	SaaS에서 제공하는 보안 감사로그 SWG 통해 확보한 SaaS 접속기록 검토

2. 내부망에서 외부 SaaS 이용 보안대책 (4)

활용범위 확대 및 활용기관의 업무 자율성을 보장하기 위한
기술적 보호조치 구축

구분		보안대책	기술적 보호조치 예
3. SaaS 관리 보안 대책	3.5	SaaS 내 파일 악성코드 감염 방지대책 마련여부	SaaS 내 데이터 악성코드 통제 체계
	3.6	SaaS에 가명처리를 하지 않은 개인신용정보 등 중요정보가 업로드 되는지 주기적으로 점검하고 업로드 확인시 보안조치 이행여부	SWG를 통한 SaaS 접속기록 저장 및 (개인정보 업로드시) 차단
	3.7	SaaS 내 업무정보가 외부에 유출되지 않도록 보호대책을 적용하고 있는지 여부	외부에서 SaaS 접속 시 반드시 사내 네트워크 경유하도록 통제 DLP 외
	3.8	SaaS와 연계된 제3자 제공 앱 설치시 관리자 승인 및 설치내역의 기록·관리 여부	PC보안의 프로세스 통제

3. 생성형 AI 보안대책 (학습 데이터 보호대책 부분 제외)

서비스 오남용으로 인하여 개인/기밀정보 유출사고가 발생하지 않도록 기술적 보호조치 구축

단말 (PC)	• 개인신용정보가 유출되지 않도록 방지대책 마련 • 개인정보/기밀정보 입력/업로드 모니터링 및 차단 • 중요정보 암호화 보관 • USB 등 매체 통제
전송구간 네트워크	• 전용회선 또는 VPN 활용하여 전송구간 보호 • AI모델 연계구간은 안전한 암호 알고리즘 활용하여 전송자료 암호화 • 입출력 데이터는 로그기록 및 저장, 주기적 감시
기타 (관리)	• 전자금융 감독규정에 기반한 안전성 확보조치 구축 • 생성형 AI 전반 관리감독 책임자 지정 • 안전한 생성형 AI 활용을 위한 임직원 대상 교육 실시

참고자료

금융위원회 〈금융분야 망분리 개선 로드맵 설명회〉 보도자료
https://www.fsc.go.kr/no010101/82937?srchCtgry=&curPage=&srchKey=&srchText=&srchBeginDt=&srchEndDt=

금융위원회 〈금융분야 망분리 개선 로드맵 발표〉 보도자료
https://www.fsc.go.kr/no010101/82885?srchCtgry=&curPage=2&srchKey=&srchText=&srchBeginDt=&srchEndDt=