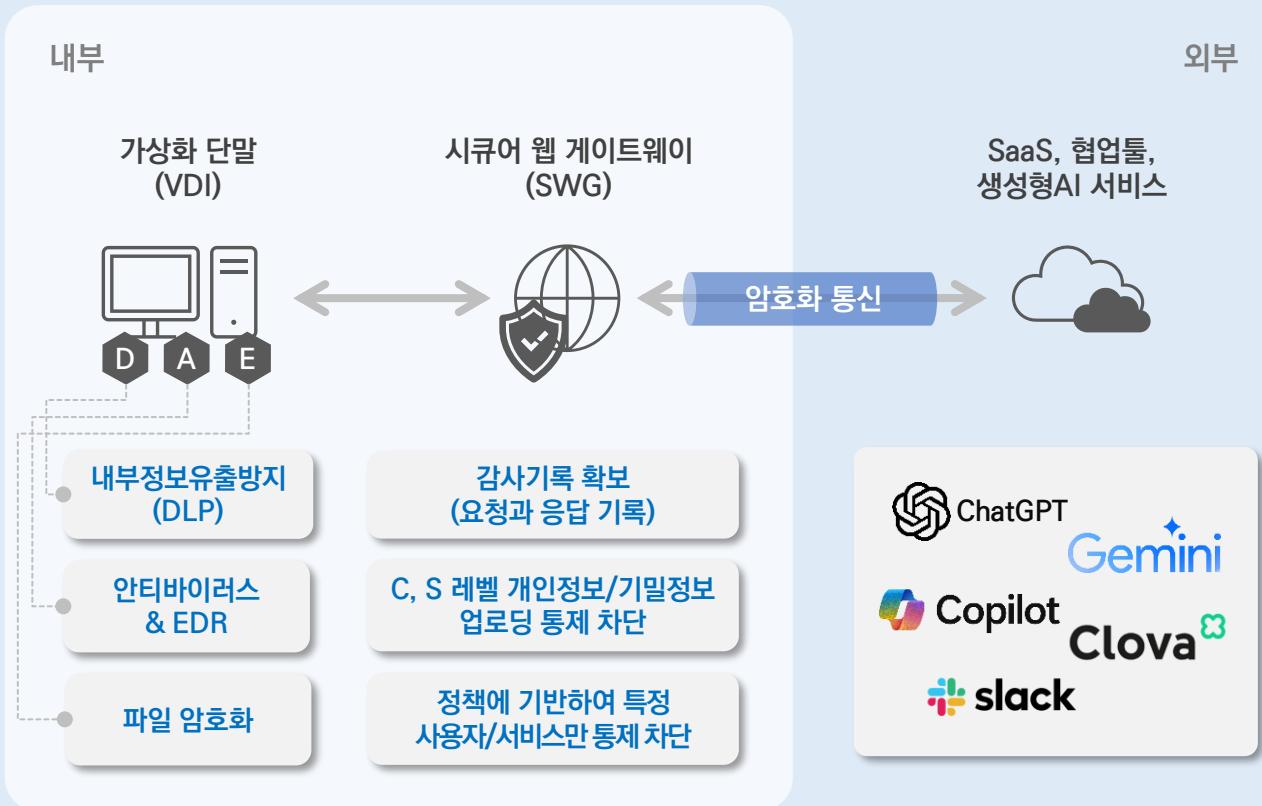


국정원, 공공분야 다층보안체계(MLS) 전환 로드맵 발표

2024년 말 로드맵 최종확정, 2025년 시행예정

2024.09.11 SCK 2024 컨퍼런스 '국가 공급망 보안정책 방향'

공공기관 업무시스템 기술적 보호조치 요약



다층보안체계 전환 절차

- 업무 중요도에 따라 기밀(Classified), 민감(Sensitive), 공개(Open)로 C/S/O 등급을 나누어 차등 보안통제
- 국가 망보안정책 개선 TF를 통해 2024년 말까지 로드맵 최종 확정, 2025년 시행 예정

C 등급 (Classified)
국가 기반시설, 국가 중대
이익관련 정보
(안보, 국가안전, 국방, 통일, 외교 등)

S 등급 (Sensitive)
비공개 업무자료를
포함 · 운영하는
시스템 및 행정 내부 업무

O 등급 (Open)
공개 가능한
공공데이터
(민간클라우드 허용 추정)

단계		주요 내용
1	준비	다층 보안체계 적용을 위한 현황파악 및 분석
2	C/S/O 등급분류	업무 중요도에 따라 정보시스템 대상 C/S/O 등급분류
3	정보서비스모델링	정보서비스 구성환경 모델링 및 평가
4	보안대책 수립	모델링 평가결과 토대로 보안원칙에 따라 보안통제 선정
5	적절성 평가 조정	등급 분류, 보안통제 적절성 평가 및 재조정

다층보안체계 전환 8개 추진과제 요약

1. 공공데이터 외부 AI 융합 추진

- 디지털플랫폼정부위, 행안부 등 관계 기관 추진
- 범정부 초거대 AI와 공공데이터 융합하여 민간에서도 공공데이터 활용할 수 있도록 기회확대

2. 인터넷 단말 업무효율성 확대

- 인터넷 접속 전용 단말에서도 **문서편집기, 협업용 SW, 클라우드 및 기타 필요한 SW를 설치/사용**하여 업무에 활용 가능

3. 업무환경에서 생성형 AI 활용 가능

- 업무단말에서 **챗GPT 등 생성형 AI 접속허용 및 업무에 활용** 가능

4. 외부클라우드 활용 업무협업 체계 구현

- 업무 생산성, 효율성 확대에 필요한 **외부 클라우드 협업도구 활용** 가능

다층보안체계 전환 8개 추진과제 요약

5. 업무단말 인터넷 이용 가능

- 업무단말 OS에 악성코드 감염 차단 환경이 구축된 경우
업무상 필요한 인터넷 서비스 접속 및 업무활용 가능

6. 연구목적 단말 신기술 활용 허용

- 연구목적 업무환경에서 국내외 제한없이 연구에 필요한 신기술 활용

7. 개발환경 편의성 향상

- 개발에 필요한 오픈소스는 인터넷 접속 통해 활용 가능
- 필요시 원격개발 수행 허용

8. 클라우드 기반 통합 문서체계 구축

- 기관 내외부에서 단말유형에 관계없이 업무자료 생산/공유/협업가능

필요한 기술적 보호조치

공공분야 AI 및 SaaS 클라우드 활용 망분리 규제완화에 의한 서비스 오남용을 통한 개인/기밀정보 유출사고가 발생하지 않도록 기술적 보호조치 구축

클라우드 SaaS, 생성형 AI서비스 접속단말 보안강화

- VDI, DLP, 파일암호화 등
개인정보유출 통제체제 강화
- SWG, Endpoint AV, EDR 등
악성코드유입 통제체제 강화

접속단말과 SaaS 서비스 간 접근통제

- 업무상 허용된 단말만
서비스 접근 가능하도록 통제 (SWG)
- 접속기록과 감사로그 확보 (SWG)

이상행위 통제

- 업무단말과 SaaS 서비스 간
C(Classified), S(Sensitive) 레벨 수준의
개인정보/기밀정보 전송시 차단 (SWG)

참고자료

[스페셜리포트]밀그림 나온 신보안체계...올해 안에 로드맵 최종 확정

<https://www.etnews.com/20240911000194>

공공 데이터 빗장 풀린다...정부, 18년 만에 공공망 분리 규제 개선

https://www.newsis.com/view/NISX20240911_0002884654

빗장 풀리는 '망분리' 규제...C·S·O 3등급으로 차등 적용

https://byline.network/2024/09/240911_003/