AGR-Ⅶ-2025-②-585

연구·개발 목적의 망분리 예외 적용에 따른 보안 해설서

2025. 4.

금융보안원

보안연구부

본 해설서는 연구·개발 목적의 망분리 예외 적용 시 금융회사 등의 이해를 돕고 보안 대책 마련 등을 지원하기 위해 작성한 것으로 법적 구속력은 없습니다.

본 해설서와 관련한 문의는 금융보안 레그테크 웹페이지(regtech.fsec.or.kr)의 '업무 지원 서비스>클라우드 및 망분리 QnA' 서비스를 활용하여 주시기 바랍니다.

목 차

Ⅰ. 개요

본 해설서는 「금융분야 망분리 개선 로드맵」('24.8월, 금융위)과 관련하여 금융회사 등이 연구·개발망을 안전하게 구성하고 보안관리를 수행할 수 있도록 필요한 절차와 대책을 안내

1 연구 · 개발망이란?

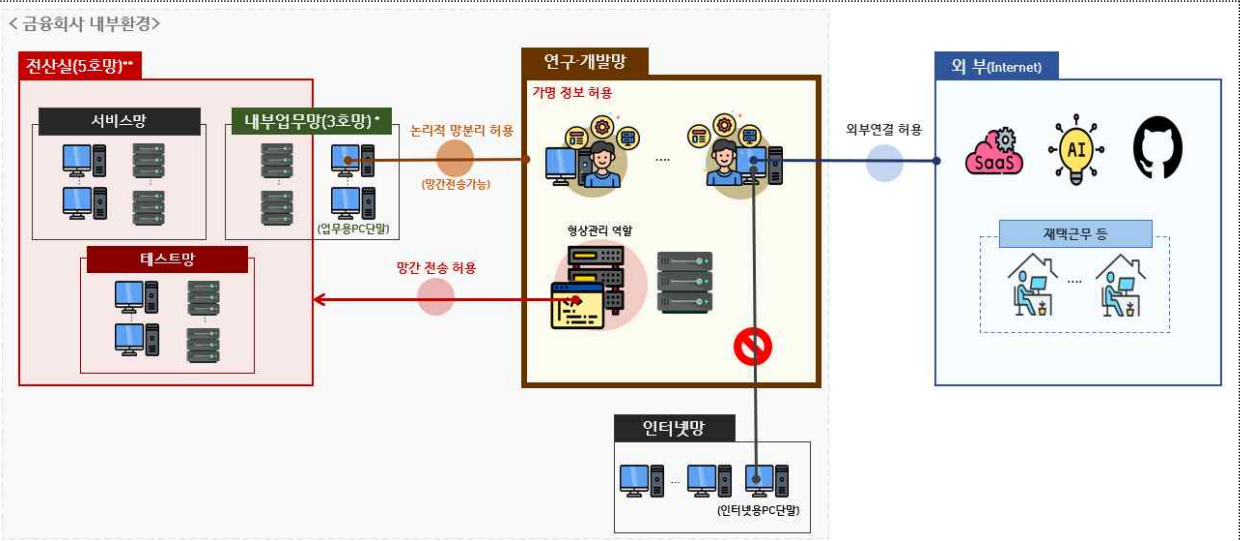
□ **(정의)** 프로그램 개발 등 금융서비스의 **연구·개발***을 할 수 있도록 금융회사의 내부업무망·전산실, 외부망으로부터 **독립적으로 구성된 망**

* 개발(코딩,테스트) 및 AI, SaaS를 활용한 연구·개발

< 망별 수행업무 범위 >

구분	내부업무망(3호망)	전산실(5호망)	연구·개발망	인터넷망
수행 업무	문서 작성, 인트라넷 접속, 민원 등 사무 업무	운영, 보안 관련 업무	개발(코딩,테스트) 및 AI, SaaS를 활용한 연구·개발	인터넷 검색, e-mail 확인 등

< 연구·개발 분야 망분리 구조도(예시) >



* 내부업무망(3호망) : 내부통신망과 연결된 내부 업무용 시스템(전자금융감독규정 §15①3)

** 전산실(5호망) : 전산실 내 위치한 정보처리시스템과 해당 정보처리시스템의 운영,개발, 목적으로 직접 접속하는 단말기(전자금융감독규정 §15①5)

2 주요 규제 개선 내용

□ **(망간 이동 편의 확대)** 연구·개발망과 내부**업무망 간 논리적 망분리**를 **허용**하고, 소스코드 등 **연구·개발 결과물**의 **망간 이동 편의 확대**

- **(연구·개발망 ↔ 내부업무망)** 논리적 망분리 허용
- **(연구·개발망 → 전산실)** 소스코드 등 개발산출물 망간 전송 허용

○ 망분리 예외 허용에 따른 **강화**된 **보안대책** 마련

□ **(가명정보 허용)** 개인신용정보의 활용은 불가하나, **가명 처리한 개인신용정보**에 한해 연구·개발망에서 **활용 가능**

< (참고)전자금융감독규정 시행세칙의 연구·개발 관련 망분리 규제 내용 >

구 분	내 용
감독규정 개정안 (제15조)	이용자 고유식별정보 및 개인신용정보(**「신용정보의 이용 및 보호에 관련 법률」 제40조2에 따른 가명처리에 관한 행위규칙을 준수한 가명정보는 제외)**를 처리하지 않는 연구·개발 목적의 경우 망분리 예외 가능 (단, 자체 위험성 평가 및 정보보호 대체 통제를 적용)
감독규정 시행세칙 <별표 7> 망분리 대체 정보보호통제	- 유해 사이트 차단 등 외부 인터넷 접근통제 대책 수립 적용 - 연구·개발망과 내부망간 **독립적인* 네트워크** 구성 *** 다만, 연구·개발망과 규정 제15조제1항제3호의 내부 업무용시스템간 연결에 한하여 논리적 방식으로 분리 가능** - 연구·개발 단말기 및 시스템에 대한 보호대책 수립·적용 및 중요정보(고유식별정보, 개인신용정보 등) 처리여부 모니터링 - 연구·개발망의 침해사고 예방 및 사고대응 대책 수립·적용 - 중요 소스코드 등에 대한 외부 반출방지 및 **망간 전송* 허용** 등에 따른 보안관리 대책 적용 *** 다만, 연구·개발망과 규정 제15조제1항제5호의 전산실간 전송 시, 개발산출물 등 필수적인 경우에 한함**

□ **(재택근무 허용)** 연구·개발망을 통한 IT개발자 등의 **재택근무 가능**

Ⅱ. 망분리 예외로 인해 발생될 수 있는 예상 위험

◈ 연구·개발 목적으로 망분리 예외 적용 시 외부 인터넷 상시 연결, 오픈소스 반입 및 활용의 증가 등으로 인해

◈ ①소스코드 등 정보 유출, ②오픈소스 등 취약한 소스코드 사용으로 인한 금융사고, ③내부망으로 침해위협 전파 가능 등의 위험이 예상

1 소스코드 등 정보 유출

□ 금융회사 등의 **소스코드***를 **보관·처리**하는 **개발 시스템 등**이 **외부 인터넷**에 **연결**됨에 따라 **소스코드 등 내부 정보 유출**될 **위험** 존재

* S/W 제작 시 프로그램 텍스트, 구성 파일 및 리소스 등을 포함(출처 : NIST)

□ 공격자는 **유출된 소스코드**를 **분석**하여 **보안 취약점**을 **파악**하고, **금융서비스**에 대한 **공격**을 **수행**

※ 금융의 디지털 전환에 따라 소스코드는 높은 가치를 가진 정보자산에 해당되며, 유출 시 영업기밀 등의 노출뿐만 아니라 다양한 피해가 발생될 수 있음을 인지

< 소스코드 등 정보유출 관련 예상 피해 >

보안위협 전파 경로	예상되는 피해
- 개발자의 실수 등으로 소스코드 공유 플랫폼(깃허브 등)에 소스코드 공개 - 인터넷 접속이 가능한 개발 단말기 및 시스템이 악성코드에 감염되어 소스코드 유출 - 개발 관련 시스템의 잘못된 구성 및 설정 등으로 외부에서 소스코드, 코드서명 인증서 등이 유출 - 퇴직 직원이 휴대용 저장장치, 이메일 등을 통해 소스코드를 무단 유출	- 유출된 소스코드 등 정보를 제3자에게 불법 판매(다크웹 등 활용) - 코드서명 유출로 이용자 단말기에 악성코드 설치 및 개인정보 등 유출 - 소스코드에 대한 취약점을 파악하여 전자금융서비스 대상 공격 수행 - 디지털 금융서비스 개발 관련 기업의 주요 지식재산권 유출 - 유출사고의 언론 노출 등에 따른 기업 이미지 및 평판 하락

2 오픈소스 등 취약한 소스코드 사용으로 인한 금융사고

□ **보안 취약점**이 **존재**하는 **오픈소스**를 활용하여 개발한 금융서비스에 대한 **인증우회 등 금융사고 발생 가능**

○ **누구나 수정 가능한 오픈소스** 특성상 **취약점이 존재**할 가능성이 높아 이를 검증 없이 활용 시 **위협에 노출**

< 취약한 소스코드 사용 관련 예상 피해 >

위협 전파 경로	예상되는 피해
- 소스코드 공유 플랫폼에 게시된 검증되지 않은 위험한 소스코드를 개발 프로그램에 반영하여 내부업무망·전산실로 이관 - 취약점이 존재하는 오픈소스를 활용하여 프로그램 개발 - 자주 활용되는 오픈소스의 관리자가 해킹되어 악성코드 등이 유포	- 금융서비스에 취약한 오픈소스가 포함되어 인증우회, APT(지능형지속공격), 내부 침투 등 취약점을 이용한 다양한 공격 시도 가능 - 악성코드 등이 삽입된 소스코드가 내부로 유입되어 감염 전파로 내부 서비스 마비 가능 - 오픈소스를 사용한 서비스의 라이선스 의무 미이행으로 문제 발생 등

□ **최근 활용도가 높은 오픈소스**(Log4j 등)를 대상으로 **악성코드를 삽입하여 배포**하는 방식의 공격도 증가하는 추세

< 소프트웨어 공급망 관련 침해 사례 >

○ 오픈소스인 color.js, faker.js의 관리자가 해당 라이브러리에 악성코드를 삽입하여 패키지 매니저를 통해 이를 배포(`22.1월)

○ US-Parser-JS 관리자의 패키지 매니저 계정이 탈취되어 악성 프로그램(암호화폐 채굴기를 설치하여 자격증명을 수집)이 배포(`21.11월)

3 내부로 침해위협 전파

□ 연구·개발망 망분리 예외로 인터넷 등 **외부통신망**에 **연결**됨에 따라 제3자 서비스(클라우드 등)를 통해서 침해 위협이 연구·개발망을 경유하여 **내부업무망·전산실**로 **유입**, 내부 침투 가능성 존재

○ 연구·개발망과 **내부업무망·전산실 간** 데이터 이동 시 **보안관리**가 **미흡**할 경우 연구·개발망으로 유입된 악성코드 등이 **내부까지 전파**

< 악성코드 감염 등 관련 예상 피해 >

보안위협 전파 경로	예상되는 피해
- 3rd Party 보안취약점(취약한 페이지 등)을 통해 내부 침투 - SaaS 등 클라우드 서비스를 통한 악성코드 유입 또는 장애 발생 - 망연계 시스템 등의 보안 통제가 미흡하여 연구·개발망에서 내부업무망·전산실로 공격자의 은닉채널 구성	- 내부 시스템이 악성코드에 감염되어 연구·개발망을 경유하여 개인정보 등 중요정보 유출 - 내부 시스템 및 서비스 등이 중단되어 업무 지장 초래 - 내부로 랜섬웨어가 유포되어 내부 자료 손실

< 망분리 기업 폐쇄망 공격 사례(출처 : 과학기술정보통신부) >

○ **공격 수행단계**

(1) 취약한 버전의 SW가 설치되어 있는 인터넷 PC 장악
(2) 망분리 솔루션 제로데이 취약점 식별
(3) 망분리 솔루션 침투 후 통신 중계용 악성코드 설치
(4) 통신 중계용 악성코드를 통해 인터넷-폐쇄망 구간 제어
(5) 폐쇄망 주요 정보시스템 침투

○ **피해 내용**

- 폐쇄망에 저장된 중요서버의 기밀 데이터 유출 등으로 인한 금전적 피해뿐만 아니라 기업 신뢰 저하 등의 피해 발생

○ **조치사항**

- 액티브X 프로그램 정기적 삭제 등 직원PC 보안조치, 망분리 환경에 대한 보안위협 점검

Ⅲ. 연구 · 개발망 구성 절차 및 보안관리 방안

1 연구 · 개발망 구성 절차

연구·개발망 구성은 ①연구·개발망 활용범위 판단 → ②자체 위험성 평가 → ③정보보호통제 및 추가 보호대책 적용 → ④정보보호위원회 의결 順으로 진행

연구·개발망 활용 범위 판단

- 금융서비스의 **개발**(코딩,테스트) 및 **AI, SaaS**를 활용한 **연구·개발** 가능
- **가명처리**된 **개인신용정보** 활용 가능
- 전산실로 연구·개발 결과물(소스코드 등) 등 **망간 자료 전송** 가능

자체 위험성 평가

- 연구·개발망 대상 **예상**되는 **위협 식별** 및 위협에 대한 **위험성 평가**
  - 소스코드 등 정보가 **외부**로 **유출**될 가능성
  - 오픈소스 등 **취약한 소스코드 사용**으로 인한 **금융사고**가 **발생**될 가능성
  - **제3자 서비스**(클라우드 등)을 **통해 연구·개발망**을 **경유**하여 **내부**로 **침해위협**이 **전파**될 가능성

정보보호통제 및 추가 보호 대책 적용

- [망분리 대체 정보보호통제(「전자금융감독규정 시행세칙」 <별표7>)]
  - 유해 사이트 차단 등 외부 인터넷 **접근통제 대책** 수립·적용
  - 연구·개발망과 내부업무망·전산실 간 **독립적인*** **네트워크** 구성
    * 다만, 연구·개발망과 규정 제15조제1항제3호의 내부 업무용시스템간 연결에 한하여 논리적 방식으로 분리 가능
  - **연구·개발 단말기** 및 **시스템**에 대한 **보호대책** 수립·적용 및 **중요정보**(고유식별정보, 개인신용정보 등) **처리여부** 모니터링
  - 연구·개발망의 **침해사고 예방** 및 **사고대응 대책** 수립·적용
  - **중요 소스코드** 등에 대한 **외부 반출방지** 및 **망간 전송*** **허용** 등에 따른 **보안관리 대책** 수립·적용
    * 다만, 연구·개발망과 규정 제15조제1항제5호의 전산실간 전송 시, 개발산출물 등 필수적인 경우에 한함
- [주요 추가 보호대책]
  - 연구·개발망 **사용자(단말기)**에 대한 **식별** 등 **접근통제 대책** 수립·적용 및 모니터링
  - 가명처리에 관한 행위규칙 준수 등 **가명정보** 활용에 대한 **보호대책** 수립·적용
  - **논리적** 망분리(내부업무망↔연구·개발망) **보호대책** 수립·적용

정보보호 위원회 의결

- **연구·개발망 활용 범위**(세부 업무 범위, 접근 대상 등) **설정**의 적정성
- **망간 자료 전송** 관련 사항에 대한 적정성
- **자체 위험성 평가**의 적정성
- **정보보호 대체통제** 등의 적정성

1 연구 · 개발망 활용 범위 판단

□ 연구·개발망에서는 금융서비스의 **개발**(코딩,테스트) 및 **AI, SaaS**를 활용한 **연구·개발 업무**에 한해 수행 가능

○ 구체적인 **업무수행 범위**(업무 종류, 접근 대상 등)는 **금융회사**에서 **자율적**으로 **정의**

※ 연구·개발망에서 개발 관련 기획·설계 업무 수행이 불가피한 경우에 한해서 보안 대책을 마련하고 정보보호위원회 승인 후 한시적으로 사용 가능(원칙적으로 연구·개발망에서 기획·설계 업무 수행 불가)

< 연구·개발망에서 수행이 불가능한 업무(예시) >

○ 연구·개발 목적 外 실 데이터를 활용한 테스트
○ 내·외부 이용자를 대상으로 제공하는 서비스(시범서비스 제공, 베타 테스트 등) 등 실제 업무

□ **연구·개발 목적**에 한해 **가명처리된 개인신용정보** 활용 가능

○ **가명정보 관련 법령** 등을 **준수**하여 **보호대책 수립·적용**

※ 가명정보는 「신용정보의 이용 및 보호에 관한 법률」에 따른 행위규칙 준수 및 「금융분야 가명 익명처리 안내서」를 참고하여 안전한 방법으로 처리 필요

□ **전산실로** 연구·개발 **결과물**(소스코드 등) 등 **망간 자료 전송** 가능

○ 연구·개발망→전산실 간 연구·개발 결과물의 전송은 **인가된 서버**(형상관리 역할을 하는 서버)만 **제한적**으로 **가능**하며, **서버 간 연결**은 **단방향 통신***을 **한시적으로 허용**

* 업무상 불가피하게 전산실 → 연구·개발망으로 소스코드 반출 등 통신이 필요한 경우에는 CISO의 승인 아래 허용

○ 망간 자료 전송에 대한 **구체적인 방식**은 금융회사 등이 **자율적**으로 **구성**

※ 다만, 취약한 파일 전송 프로토콜 및 원격접속 프로토콜 사용 제한

2 자체 위험성 평가

□ 금융회사 등은 자사의 업무 환경 등을 고려하여 **연구·개발망 구성**에 따른 **자체 위험성 평가**를 실시

○ **예상**되는 **보안 위협**(아래 예시 참조)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

< 연구·개발 목적의 망분리 예외 시 예상되는 보안위협(예시) >

구 분	내 용
소스코드 등 정보 유출	- 금융서비스 관련 소스코드의 외부 유출 가능성 - 소스코드 유출 시 금융서비스에 미칠 영향 ※ 공격자는 소스코드 분석을 통해 금융서비스 프로그램의 구조나 취약점 등을 파악 가능 - 서비스의 코드서명(Code Signing) 및 암호키 등 유출 가능성
오픈소스 등 취약한 소스코드 사용으로 인한 금융사고	- 취약점이 있는 오픈소스 또는 안전하지 않은 소스코드가 별도의 보안검증 절차 없이 업무망 및 전산실로 이관될 가능성 - 취약한 소스코드 사용으로 인해 금융서비스에 취약점이 발생하여 침해사고 등이 발생할 가능성
내부로 침해위협 전파 가능	- 연구·개발망의 인터넷 연결에 따른 악성코드 감염 위험성 - 망간 연계 구간의 접근통제 적절성 - 연구·개발망을 통해 업무망 및 전산실로의 침해 시도 가능성

3 정보보호통제 및 추가 보호대책 적용

□ 망분리 예외 적용 시 「전자금융감독규정 시행세칙」 <별표7>에 명시된 **망분리 대체 정보보호통제**(연구·개발 부문) 이행

< 「전자금융감독규정 시행세칙」의 망분리 대체 정보보호통제 내용(연구·개발 관련) >

① 유해 사이트 차단 등 외부 인터넷 접근통제 대책 수립·적용
② 연구·개발망과 내부망간 독립적인* 네트워크 구성
* 다만, 연구·개발망과 규정 제15조제1항제3호의 내부 업무용시스템간 연결에 한하여 논리적 방식으로 분리 가능
③ 연구·개발 단말기 및 시스템에 대한 보호대책 수립·적용 및 중요정보(고유식별정보, 개인신용정보) 처리 여부 모니터링
④ 연구·개발망의 침해사고 예방 및 사고대응 대책 수립·적용
⑤ 중요 소스코드 등에 대한 외부 반출방지 및 망간 전송* 허용 등에 따른 보안관리 대책 수립·적용
* 다만, 연구·개발망과 규정 제15조제1항제5호의 전산실간 전송시 개발산출물 등 필수적인 경우에 한함

□ 정보보호통제 이행 시 **자체 위험성 평가**에서 도출된 **위험이 충분히 완화**되었는지 확인하고 **필요시 추가 보호대책**을 **적용**

< 추가 보호대책(예시) >

ㅇ 연구·개발망 사용자(단말기)에 대한 식별 등 접근통제 대책 수립·적용 및 모니터링
ㅇ 가명처리에 관한 행위규칙 준수 등 가명정보 활용에 대한 보호대책 수립·적용
ㅇ 논리적 망분리(업무망↔연구·개발망) 보호대책 수립·적용 등

※ 정보보호통제 및 추가 보안대책의 세부 사항은 '2. 연구·개발망 구성 및 보호대책' 참고

4 정보보호위원회 의결

□ 망분리 예외에 따른 **자체 위험성 평가 결과** 및 적용된 **보호대책의 적정성** 등에 대해 **정보보호위원회 의결**

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

< 정보보호위원회의 연구·개발 목적의 망분리 예외 심의·의결 시 검토사항(예시) >

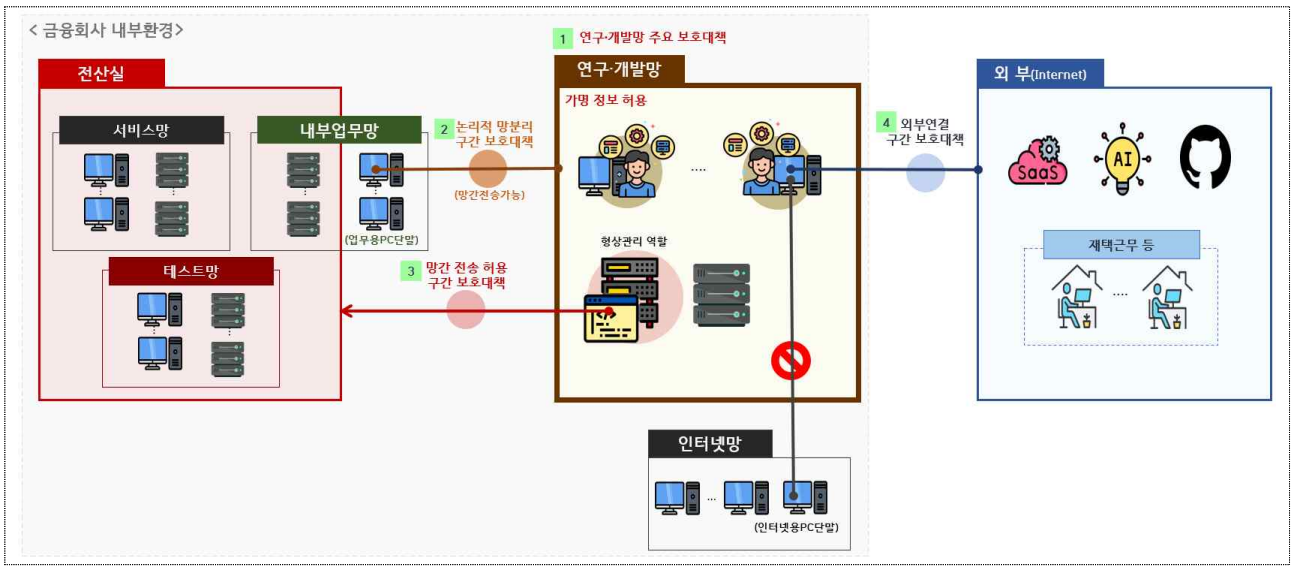
○ 연구·개발망 활용 범위 설정의 적정성
○ 망간 자료 전송 관련 사항에 대한 적성성
○ 연구·개발망 관련 위험 식별 등 자체 위험성 평가 수행의 적정성
○ 연구·개발망에 대한 정보보호 대체통제 적용 및 자체 위험성 평가에 따른 추가 보호대책 등의 적정성

□ **정보보호위원회 의결 이후**에도 **정기적**으로 연구·개발망에 대한 **위험성 평가***를 **실시**할 것을 권고

* 연 1회 정기 모의해킹 실시 등

○ 연구·개발망 구성의 변화 등 **보호대책**의 **중대한 변경**이 있는 경우 **정보보호위원회 심의·의결 재수행** 필요

2 연구 · 개발망 구성 및 보안관리 방안



1 연구 · 개발망 주요 보호대책

가. 독립적인 네트워크 구성

□ **연구·개발망**은 **내부업무망·전산실, 외부망**으로부터 **독립된 인프라**로 **구성·운영**

※ 다만, 연구개발 목적으로 망분리 예외 적용 시, 인터넷망에서 활용 중인 정보보호 시스템(백신 등)은 활용 가능 (내부망 자원은 활용 불가)

□ **자사 업무 환경** 등에 **적합**하고 **안전한 방법**으로 연구·개발 관련 **네트워크**를 **구성**

○ 네트워크 구성 시 **연구·개발망**의 **보안위협**이 **내부업무망·전산실** 또는 금융서비스에 미치는 **영향**이 **최소화**되도록 고려

□ **실 업무** 또는 **서비스 제공**에 필요한 시스템(공개용 웹서버, 모바일 앱 배포 서버 등)은 **연구·개발망**에 **위치 불가**

※ 실제 서비스 제공 등을 수행하는 경우 연구·개발 목적에 미 해당

□ **클라우드 환경**에 연구·개발망 구축 시 **전자금융감독규정**에서 정한 **클라우드 이용 관련 사항 준수** 필요

※ 금융보안원「금융분야 클라우드컴퓨팅서비스 이용 가이드」참조

□ 연구·개발망에서 무선통신망 사용 시 **전자금융감독규정(제15조제6항) 준수** 및 사용자 인증 등 **보호대책 적용** 필요

※ 전산실 內 설치되는 개발 관련 시스템 등은 무선통신망 접속 차단

< 연구·개발망에서 무선통신망 사용 시 보안대책(예시) >

- ㅇ 내부망 및 외부인이 사용하는 무선통신망과 분리
- ㅇ 무선통신망 접속 차단시스템 구축 및 실시간 모니터링 수행
- ㅇ 무선통신망 관련 장비에 대한 주기적 보안패치 적용
- ㅇ 비인가 무선접속장비(AP) 설치 여부 및 중요정보 노출 여부를 주기적으로 점검
- ㅇ AP 접속 시 단말기 인증(MAC 인증 등) 및 사용자 인증 적용
- ㅇ 정보 송·수신 시 암호화 적용
- ㅇ 보안 프로토콜 설정(WPA2 이상) 및 SSID 숨김 설정
- ㅇ 무선통신망 사용 신청 및 해지 절차 수립 등

나. 단말기 및 시스템 보호대책

□ 연구·개발망에는 **인가된 대상***만 **접근**할 수 있도록 하고, 이에 대한 **접근통제 대책 수립·적용**

* 사용자(단말기), 서버, 네트워크, 시스템 등

ㅇ **내부업무망 단말기**에서 **논리적 분리**를 통해 연구·개발망으로 **접속** 가능하며, **구체적인 방식**은 내부 환경을 고려하여 **자율적**으로 결정

※ 인터넷망에서 사용중인 단말기에서는 연구·개발망 접속 불가

□ 연구·개발 단말기 및 시스템에 대해서도 망분리 外 **전자금융감독규정**에서 정한 **안전성 확보 의무 준수** 필요

□ 연구·개발 시 **실제 서비스 운영** 과정에서 사용되는 **중요정보*** **활용 금지**

* 자격증명(Credential), 시스템 접근 키, 코드서명(code signing) 인증서, 암호키 등

□ **실 데이터**를 **활용**한 **테스트, 내·외부 이용자 대상 서비스**(시범 서비스 제공, 베타 테스트 등) 등은 **처리 금지**

□ 연구·개발 관련 **문서**의 **작성 및 저장**이 필요한 경우 **문서보안(암호화)** 등 **보호대책 수립·적용**

다. 가명정보 활용에 대한 보호대책

□ **연구·개발 목적**으로만 **가명처리된 개인신용정보 활용**이 **가능**하며, 활용 시 가명정보 관련 법령 등을 준수하여 **보호대책 수립·적용**

<가명정보 관련 법령>

① 「전자금융감독규정」 제14조의2(클라우드컴퓨팅 서비스 이용절차 등) 제7항
② 「신용정보의 이용 및 보호에 관한 법률」 제32조(개인신용정보의 제공·활용에 대한 동의) 제6항 9의2.
③ 「개인정보보호법」 제28조의8(개인정보의 국외 이전) 등

※ 가명정보 활용시 「전자금융감독규정」, 「개인정보보호법」에 따른 국외 이전 제한에 대해 유의할 필요

○ **재식별**이 가능한 **추가 정보**나 이용자의 **고유식별정보 또는 개인신용정보** 저장 여부를 **주기적**으로 **모니터링 및 삭제** 조치

※ 「신용정보의 이용 및 보호에 관한 법률」에 따른 행위규칙 준수 및 「금융분야 가명 익명처리 안내서」를 참고하여 안전한 방법으로 처리 필요

라. 침해사고 예방 및 사고대응 대책

□ 연구·개발망에서 **보안사고** 발생을 **최소화**하기 위해 필요한 **보호대책**을 **검토**하고 이를 **내부 보안정책**에 **반영**

○ 정보유출 등 **보안사고** 방지를 위해 **연구·개발망**을 **보안관제 범위**에 **포함**하고 모니터링 결과를 **주기적**으로 **검토**

○ 연구·개발망의 **인터넷 접속 기록**을 **1년 이상 보관**하고, 주요 **파일 업로드·다운로드 내역**을 **주기적**으로 **검토**

□ 중요 정보(소스코드 등) 유출* 등 **보안사고 발생**에 대비한 **대응절차 마련**

* (예) 소스코드 깃허브 등 공유 플랫폼에 무단 게시된 사실 확인, 연구·개발망 모니터링 과정에서 유출 사실 확인, 퇴사 직원이 중요 소스코드를 무단 반출 등

< 소스코드 유출 시 대응조치(예시) >

ㅇ 소스코드 유출에 따른 위험성 분석(금융서비스 영향도, 취약성 등)
ㅇ 소스코드 유출시, 유출 소스코드 폐기 및 보안관제 강화 등 필요 절차 마련
ㅇ 코드서명 및 암호키 등이 유출된 경우 즉시 관련 서비스 변경 배포
ㅇ 침해사고대응기관 등에 협조 요청 및 침해 원인 분석 수행 등
ㅇ 소스코드 노출 시 무단 게시 중단 요청 등

□ 보안사고 발생 시 **상세 원인·분석**을 위해 충분한 **디지털 증거**를 **보존**해야 하며 원인분석 前 **증거 삭제(PC 포맷 등) 행위 금지**
※ 사고 시 금융보안원에 상세 원인분석 요청 가능

□ 연구·개발망에서 발생한 **보안사고가 내부**로 **확산**되는 것을 **방지**하기 위해 **네트워크 격리** 등 **긴급 대응 절차**를 이행

마. 소스코드 등 보호대책

□ **중요 소스코드**는 **강화된 통제 조치*** 권고
* 주요 직무자 外 접근 금지, 지정된 시스템 및 단말기에서만 소스코드 접근(또는 저장)허용, 소스코드 접근내역 기록, 소스코드 접근 권한자에 대한 보안서약서 징구 등

□ 소스코드 저장소에 보관된 **중요 소스코드 접근** 시 **다중**(multi-factor) 인증 등 **강화된 인증**을 수행하고, **접근 내역**을 **기록·관리** 필요

< 소스코드 저장소 구성 시 보안 고려사항(예시) >

ㅇ 사용자별 최소권한 부여를 위한 세부 권한 설정 지원
ㅇ 소스코드 內 노출된 자격증명 및 민감한 정보 점검 지원
ㅇ 소스코드 저장소 접근 시 멀티팩터(multi-factor) 인증 지원
ㅇ 소스코드 및 리소스 등의 모든 변경 사항에 대한 감사로그 생성
ㅇ 소스코드 구성요소 식별 및 소스코드의 알려진 취약성 점검 지원 등

□ 연구·개발망 內 **소스코드 보호**를 위한 **추가 보호대책**을 **검토**하여 **내부 보안정책** 등에 **반영**

< 연구·개발망 內 소스코드 보안관리 정책(예시) >

ㅇ 금융서비스 관련 소스코드 보관·반출 등 보안관리 방안
ㅇ 구간별(내부업무망,전산실,외부) 중요 소스코드 반입·반출 탐지 등의 관리 방안
ㅇ 소스코드 보안 관련 내부정책 위반 시 제재 방안
ㅇ 연구·개발망의 코드서명 및 암호키 등의 관리 방안
ㅇ 소스코드의 운영 환경으로 이관 절차 및 보안 통제방안
ㅇ 소스코드 유출 등 보안사고 발생 시 대응 절차 등
ㅇ 프로젝트 종료 시 연구·개발 단말 내 소스코드 등 주요 정보 삭제 절차

□ 연구·개발에 필요한 **오픈소스** 소프트웨어를 안전하게 **활용**하기 위한 **보호대책 수립·적용**

※ 기타 오픈소스 라이센스 관리 등에 관한 사항은 금융보안원의 「금융분야 오픈소스 소프트웨어 활용·관리 안내서('22.12월)」 참조

□ 소스코드 등 데이터의 **외부 반출**을 **엄격**하게 **관리·통제**

ㅇ 특히, 중요 소스코드가 **소스코드 공유 플랫폼**(깃허브 등), **생성형 AI 모델, 이메일·메신저** 등에 **업로드**되거나 **공유**되지 않도록 모니터링 등 **통제**

□ **소스코드 공유 플랫폼** 등에 중요 **소스코드**가 **무단 공개**되는 경우에 대비하여 **무단 게시 중단 요청 등 대응 절차** 마련

< (참고)무단 게시 중단 요청 등 대응절차 >

미국은 밀레니엄저작권법(DCMA)에 의거 무단 게시된 기업 소스코드의 저작권을 주장하여 게시 중단요청 가능 (저작물의 보호를 위한 베른 협약에 의거하여 소스코드가 국내 관련법에 따라 보호받는 경우 게시 중단 요청 가능)

2 논리적 망분리(내부업무망↔연구·개발망) 구간 보호대책

□ 내부업무망(3호망)에서 **인가된 사용자(단말기)만** 연구·개발망에 **접근**할 수 있도록 **통제**

ㅇ 인가된 사용자에 대한 **적정성**(퇴직, 휴직, 인사이동 등) **여부** 등은 주기적으로 **모니터링**

□ 망간 안전한 데이터 이동을 위한 **보호대책*** **적용 및 모니터링**

* 데이터 이동 내역 등 감사 기록 생성·보관, 사전 악성코드 감염 여부 점검, 망연계 구간 상시 모니터링 등

○ 망 구성, 자료 전송 방법 등에 대한 **구체적인 사항은 금융회사**가 자사 IT 환경 및 위험 등을 고려하여 **자율적**으로 결정

3 망간 전송 허용(연구 · 개발망→전산실) 구간 보호대책

□ 연구·개발망의 **인가된 서버**(형상관리 역할을 하는 서버)**만 전산실**에 **접속**할 수 있도록 **통제**하고, 서버 간 연결은 **단방향**(연구·개발망→전산실) **통신을 한시적**으로 **허용**

○ 다만, 전산실에서 연구·개발망으로 **소스코드 반출** 등 업무상 불가피한 **예외사항**은 **CISO 승인** 및 **정보보호위원회 의결 후 개발 산출물 반출 허용**

□ 망간 자료 전송 채널 및 방법에 대한 **구체적인 방식**은 **금융회사**가 자사 IT 환경 및 위험 등을 고려하여 **자율적**으로 **결정**

○ 다만, **취약한 전송 프로토콜** 및 **원격접속 프로토콜** 사용은 **제한**

□ 전산실로 **소스코드 등 데이터 전송** 시 사전에 **시큐어코딩 점검** 및 **소스코드 무결성 검증** 등 **강화된 보호대책*** **수립·적용**

* 데이터 이동 내역 및 망분리 예외 사항 등 감사 기록 생성·보관, 사전 악성코드 감염 여부 점검, 망연계 구간 상시 모니터링 등

4 외부연결 구간 보호대책

가. 원격 등 외부 접근통제 대책

□ 연구·개발 업무 수행을 위해 **외부 인터넷 환경***(재택 등)에서 연구·개발망으로 **원격 접속**이 **가능**하며, 이에 대한 **보호대책 수립·적용** 필요

* 기존 인터넷망의 단말기에서는 접근 불가

○ 구체적인 **접속 방식**은 금융회사 등의 내부 환경에 따라 **자율적**으로 구성

※ 금융보안원의「금융회사 재택근무 보안안내서(`20.10월)」참고 및 외부주문 등을 통해 연구·개발을 수행하는 경우「전자금융감독규정(제60조)」준수

나. 유해사이트 차단 등 외부 인터넷 접근통제 대책

□ 인터넷 등 **외부 접속**이 **허용**되는 **범위** 및 **신청 절차** 등에 대해 **내부 기준**을 **마련**하여 운영

○ **인터넷 접근 대상**(단말기, 연구·개발 서버 등)을 **지정**하고 이에 대한 **접근통제 대책 수립·적용, 접근로그 저장 및 모니터링**

○ **연구·개발**과 **무관**하거나 **해킹** 등에 **악용**될 수 있는 **웹사이트** 등의 접속 차단 권고

< 연구·개발망에서 차단해야 하는 웹사이트 등(예시) >

○ 악성코드 유포지 및 침해 관련 도메인 및 IP
○ 연구·개발 업무와 무관한 유해사이트 (불법 도박, 상용 이메일 등)
○ 파일공유 사이트 (웹하드, P2P 사이트, 클라우드 드라이브 등)
○ 외부 단말기 및 시스템으로의 원격접속 통신
○ 사내 전자금융서비스를 제공하는 DMZ 구간으로의 접속 등

※ 금융보안원 금융보안정보공유포털(kfisac.or.kr)에서 접속차단 웹사이트 최신정보 확인 가능

다. SaaS 등 접근통제 대책

□ **연구·개발**에 **필요한 경우**에 한해 **SaaS, 생성형 AI**는 **이용**이 **가능**하며 필요 **보호대책 수립·적용**

※「전자금융감독규정(제14조의2)」클라우드컴퓨팅서비스 이용절차 준수

○ 다만, **혁신금융서비스**로 **지정**되어 **내부업무망**에서 **사용**하는 SaaS는 **연구·개발망**에서 **사용 불가**

AGR-Ⅶ-2025-②-585

연구·개발 목적의
망분리 예외 적용에 따른 보안 해설서

발행일 : 2025년 4월
발행인 : 박 상 원
발행처 : 금융보안원
경기도 용인시 수지구 대지로 132

금융보안원
FINANCIAL SECURITY INSTITUTE