AGR-Ⅱ-2023-②-403

연구·개발 목적의 망분리 예외 적용에 따른 보안 유의사항

2023. 3.

금융보안원

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

본 유의사항과 관련한 문의는 금융보안 레그테크 웹페이지(regtech.fsec.or.kr)의 '클라우드 및 망분리 QnA' 를 활용하여 주시기 바랍니다.

Ⅰ. 개요

□ **연구·개발 목적**인 경우 **망분리 적용 예외**가 적용되어 금융회사 등의 **新기술 활용 및 금융혁신의 기회가 확대**될 것으로 보이나, 소스코드 유출 등 **보안사고 발생 가능성도 증가**될 것이 우려

[「전자금융감독규정」內 연구·개발 목적의 망분리 예외 적용 관련 조항]

제15조(해킹 등 방지대책) ① 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운용하여야 한다.

1.~ 2. (생 략)

3. 내부통신망과 연결된 내부 업무용 시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속금지, 다만, **다음 각목의 경우에는 그러하지 아니하다.**

가. 이용자의 고유식별정보 또는 개인신용정보를 처리하지 않는 연구·개발 목적의 경우(단, 금융회사 또는 전자금융업자가 자체 위험성 평가를 실시한 후 금융감독원장이 정한 망분리 대체 정보보호통제를 적용한 경우에 한한다.)

나. 업무상 불가피한 경우로서 금융감독원장의 확인을 받은 경우

4. (생 략)

5. 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리할 것. 다만 다음 각목의 경우에는 그러하지 아니하다.

가. 이용자의 고유식별정보 또는 개인신용정보를 처리하지 않는 연구·개발 목적의 경우(단, 금융회사 또는 전자금융업자가 자체 위험성 평가를 실시한 후 금융감독원장이 정한 망분리 대체 정보보호통제를 적용한 경우에 한한다.)

나. 업무상 불가피한 경우로서 금융감독원장의 확인을 받은 경우

②~⑥ (생 략)

➜ 본 유의사항은 망분리 예외에 따라 예상되는 **위험을 식별**하고 이를 완화하기 위한 **보안대책 등을 검토하여 권고**함으로써 금융회사 등의 **안전한 연구·개발 업무를 지원**하기 위함.

참 고 **전자금융감독규정·시행세칙의 망분리 규제 내용**

<table>
<tr><th colspan="2">구 분</th><th colspan="2">내 용</th></tr>
<tr><td rowspan="4">감독규정
개정안
(제15조)</td><td>방식</td><td>논리적 망분리</td><td>물리적 망분리</td></tr>
<tr><td>대상</td><td>내부망과 연결된
내부 업무시스템</td><td>전산실 內 위치한 시스템과
해당 시스템 관리 단말기</td></tr>
<tr><td>규제
내용</td><td>인터넷 등과 분리, 접속 금지</td><td>인터넷 등과 물리적으로 분리</td></tr>
<tr><td>연구·개발</td><td colspan="2">이용자 고유식별정보 및 개인신용정보를 처리하지 않는 연구·개발목적의 경우 망분리 예외 가능
(단, 자체 위험성 평가 및 정보보호 대체 통제를 적용</td></tr>
<tr><td rowspan="3">감독규정
시행세칙
(제2조의2)</td><td rowspan="3">금감원
인정
예외</td><td>업무상 불가피한 경우로서
금감원장 확인받은 경우</td><td>업무 특성상 분리하기 어려운
경우로 금감원장이 인정</td></tr>
<tr><td>(1) 내부단말기가 업무상 필수로 외부 기관과 연결하는 경우

(2) 보안대책 적용 단말기에서 외부망으로부터 내부시스템 접속(전용회선 또는 VPN 사용)</td><td>(1) 국외 전산센터 정보처리위탁
(2) 전자금융업무 처리를 위해 특정 외부기관과 데이터 송수신
(3) DMZ에서 내부망과 실시간으로 데이터를 송수신하는 시스템
(4) 계열사 공동 사용 시스템
(5) 비상대책에 따른 원격접속
(6) 관리용단말기↔외부망 또는 내부시스템 구간을 차단한 경우</td></tr>
<tr><td colspan="2">(1) 자체 위험성 평가
(2) 망분리 대체 정보보호 통제
(3) 정보보호위원회 승인</td></tr>
<tr><td rowspan="2">감독규정
시행세칙
<별표 7>
망분리
대체
정보보호
통제</td><td>공통</td><td colspan="2">외부→내부 전산자료 악성코드 치료, APT 대책, 전산자료 외부 전송 시 정보 유출 탐지·차단</td></tr>
<tr><td>연구·개발</td><td colspan="2">- 유해 사이트 차단 등 외부 인터넷 접근통제 대책 수립 적용
- 연구 개발망과 내부망간 독립적인 네트워크 구성
- 연구 개발 단말기 및 시스템에 대한 보호대책 수립·적용 및 중요정보(고유식별정보, 개인신용정보) 처리여부 모니터링
- 연구·개발망의 침해사고 예방 및 사고대응 대책 수립
- 중요 소스코드 등에 대한 외부 반출방지 등 보안관리 대책 적용</td></tr>
</table>

Ⅱ. 망분리 예외에 따른 변화와 예상 위험

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

◈ ①소스코드 등 정보 유출, ② 취약한 소스코드 사용으로 인한 보안사고, ③ 내부망으로 침해위협 확산 등의 위험이 예상

1 소스코드 등 정보유출

□ 금융회사 등의 **소스코드***를 **보관·처리**하는 **개발 시스템 등**이 **외부 인터넷에 상시 연결**됨에 따라 **소스코드 유출** 위험이 가중

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

□ 공격자는 **유출된 소스코드를 분석**하여 **보안 취약점을 파악**하고, **전자금융서비스에 대한 공격을 수행**할 가능성이 존재

※ 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, 코드 서명 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

참 고 소스코드 등의 정보유출 사고 사례

구분		사고 내용
해킹사고에 의한 유출	N사 (`22.2월)	해킹그룹 랩서스가 코드서명 인증서 등을 유출하여 해당 인증서로 서명된 악성코드가 유포
	M사 (`22.3월)	공격자가 내부시스템에 접근하여 일부 서비스 소스코드가 유출되었으며, 이용자 계정 탈취 시도
	S사 (`18.8월)	버그바운티를 하는 개인에 의해 앱의 전반적인 설계가 포함된 소스코드를 무단 공개되었으며, 기업의 주가가 하루 동안 3.4% 하락
	E사 (`21.6월)	공격자가 기업 네트워크에 침투하여 게임 관련 소스코드 및 디버깅 툴, API 키 등 2,800만 달러 상당의 데이터를 도난하였으며, 이를 불법 웹사이트 등에서 판매
	T사 (`21.10월)	공격자가 기업의 내부 소스코드 저장소를 해킹하여 소스코드 및 커밋 히스토리 등이 유출
	S사 (`22.3월)	해킹그룹 랩서스가 S사 모바일 플랫폼의 소스코드를 유출했다고 주장함에 따라 이를 활용하는 기업 피해도 우려
구성 및 설정 오류에 의한 유출	N사 (`22.1월)	소스코드 저장소의 관리자 계정 설정 미흡으로 인해 커넥티드카 서비스 등의 소스코드가 유출
	S사 (`19.9월)	캐나다의 금융회사인 S사는 깃허브에 결제 연동 관련 소스코드 및 자격증명 등을 외부에 노출
내부직원에 의한 유출	A사 (`18.2월)	인턴직원이 계약 만료 시 기업의 소스코드를 깃허브에 업로드하여 무단 공개되었으며, 애플은 관련 법에 따라 깃허브에 게시 중단을 요청
	A사 (`17.7월)	내부 직원이 퇴직하며 핵심 기술 소스코드 등을 USB에 담아 이를 중국의 경쟁업체에 유출

2 취약한 오픈소스 사용으로 인한 보안사고

□ **보안 취약점이 존재하는 오픈소스**를 활용하여 개발한 전자금융 서비스 등에 대한 **보안사고 발생 우려** 증대

○ **누구나 수정 가능한 오픈소스**의 특성상 **취약점이 존재***할 가능성이 높아 이를 검증없이 활용 시 **보안 위협에 노출**

* 오픈소스는 전세계 프로젝트의 97%에서 활용되고 있으며, 이 중 81%는 알려진 오픈소스 취약점을 하나 이상 가지고 있는 것으로 조사(출처 : 시놉시스, `22년)

[취약한 소스코드 사용 관련 예상 피해]

보안위협 전파 경로	예상되는 피해
- 소스코드 공유 플랫폼에 게시된 검증되지 않은 위험한 소스코드를 개발 프로그램에 반영하여 내부망으로 이관 - 취약점이 다수 존재하는 오픈소스를 활용하여 프로그램 개발 - 자주 활용되는 오픈소스의 관리자가 해킹되어 악성코드 등이 유포	- 전자금융서비스에 취약한 오픈소스가 포함되어 취약점 공격 시도 증가 - 악성코드 등이 삽입된 소스코드가 내부망으로 유입되어 감염 전파 - 오픈소스를 사용한 서비스의 라이선스 의무 미이행으로 문제 발생

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

[최근 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 내부망으로 침해위협 확산

□ 연구·개발망 망분리 예외로 인터넷 등 **외부통신망에 상시 연결**됨에 따라 **악성코드 등이 내부망에 유입**될 가능성 존재

○ 연구·개발망과 내부망 간 **정보 송수신이 가능**하거나 **망연계 시스템** 등의 **보안관리가 미흡**할 경우 연구·개발망으로 유입된 악성코드 등이 **내부망까지 전이**될 우려

[내부망 악성코드 감염 등 관련 예상 피해]

보안위협 전파 경로	예상되는 피해
- 내부망으로 파일 반입 시 보안검증이 미흡하여 악성코드가 유입 - 악성코드에 감염된 파일이 유입되어 내부망에서 과도한 트래픽 발생 - 망연계 시스템 등의 보안통제가 미흡하여 연구·개발망에서 내부망으로 공격자의 은닉채널 구성	- 내부망 시스템이 악성코드에 감염되어 연구·개발망을 경유하여 개인정보 등 중요 정보 유출 - 내부망 시스템 및 서비스 등이 중단되어 업무 지장 초래 - 내부망으로 랜섬웨어가 유포되어 업무 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

○ 피해내용

- 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·개발 목적의 망분리 예외 절차

단계	고려사항
망분리 예외 범위 판단	▪ 이용자의 고유식별정보 및 개인신용정보를 미처리 ▪ 업무 관련 서비스 및 소프트웨어 개발을 위한 경우에 해당 ▪ 이용자 등을 대상으로 한 실제 서비스 제공 금지
자체 위험성 평가	▪ 전자금융서비스 관련 소스코드 및 코드서명 등의 외부 유출 ▪ 악성코드 및 취약한 소스코드가 내부망으로 유입될 가능성 ▪ 연구·개발망에서의 정보유출, 악성코드 유입 등 사고 발생 시 전자금융서비스에 대한 영향평가
정보보호 대체통제 및 추가 보안대책 적용	▪ 유해 사이트 차단 등 외부 인터넷 접근통제 대책 수립 적용 ▪ 연구 개발망과 내부망간 독립적인 네트워크 구성 ▪ 연구 개발 단말기 및 시스템에 대한 보호대책 수립·적용 및 중요정보(고유식별정보, 개인신용정보) 처리여부 모니터링 ▪ 연구·개발망의 침해사고 예방 및 사고대응 대책 수립 ▪ 중요 소스코드 등에 대한 외부 반출방지 등 보안관리 대책 적용
정보보호 위원회 의결	▪ 망분리 예외 범위 설정의 적정성 ▪ 자체 위험성 평가의 적정성 ▪ 정보보호 대체통제 등의 적정성

1 연구·개발 목적의 망분리 예외 가능 범위

□ 금융회사 등이 대고객 금융서비스 제공이나 내부 업무 등을 위해 **소프트웨어 등을 연구·개발**하는 경우 망분리 예외 가능

○ **망분리 예외가 적용된 시스템**을 통해 연구·개발 목적 外 대고객 금융서비스 등 **실제 업무를 처리하는 것은 금지**

□ 망분리 예외가 적용되는 연구 · 개발망에서는 **고유식별정보** 또는 **개인신용정보** 등의 **처리**가 금지

※ 가명정보는 가명 처리한 개인신용정보(신용정보법 §2 · 16)로서 처리 금지되며, 익명정보(신용정보법 §2 · 17)는 개인신용정보에 해당하지 않아 처리 가능

○ **이용자를 식별**할 수 있는 **계좌번호** 등의 실제 데이터가 **연구·개발망**에서 처리되지 않도록 조치(가상데이터 등으로 변환 활용)

[연구·개발 목적의 망분리 예외 범위(예시)]

구 분	내 용
망분리 예외가 가능한 경우	- 개인신용정보* 등의 미처리(단, 연구·개발 완료 후 업무망에서 서비스 제공 시는 개인신용정보 등 처리 가능) * 익명정보는 개인신용정보가 아니므로 개발 과정에서 처리 가능 - 전자금융서비스 또는 내부 업무 등을 위한 프로그램 개발(마이데이터, AI 빅데이터 기반 개발 등) 가능 - 프로그램 개발 외의 테스트, QA, 개발도구 제작, 연구·개발에 필요한 제품 및 서비스의 개념검증(PoC) 등 가능
망분리 예외가 불가한 경우	- 연구·개발 과정에서 개인신용정보(가명정보 포함)를 처리 - 서비스 기획·설계, 서비스 배포 등 연구·개발 외의 업무 - 시장 분석, 연구 및 리서치 보고서 작성 등 실제 업무 수행 - 내·외부 이용자를 대상으로 실제 서비스를 제공하는 경우 (시범서비스 제공, 베타 테스트 등)

2 자체 위험성 평가

□ 금융회사 등은 **자사의 업무 환경 등을 고려**하여 연구·개발 목적의 망분리 예외에 따른 **자체 위험성 평가**를 실시

○ 망분리 예외에 따라 예상되는 **보안위협**(아래 예시 참조)을 빠짐없이 **식별**하고 그에 따른 **위험성을 평가**

[연구·개발 목적의 망분리 예외 시 예상되는 보안위협(예시)]

구 분	내 용
소스코드 등 정보 유출	- 전자금융서비스 관련 소스코드의 외부 유출 가능성 - 소스코드 유출 시 전자금융서비스에 미칠 영향 ※ 공격자는 소스코드 분석을 통해 전자금융서비스 프로그램의 구조나 취약점 등을 파악 가능 - 서비스의 코드서명(Code Signing) 및 암호키 유출 가능성
취약한 소스코드 사용으로 인한 보안침해	- 취약점이 있는 오픈소스 또는 안전하지 않은 소스코드가 별도의 보안검증 절차 없이 내부망으로 이관될 가능성 - 취약한 소스코드 사용으로 인해 전자금융서비스에 취약점이 발생하여 보안침해 등이 발생할 가능성
내부망으로 보안위험 확산	- 인터넷 연결을 통한 악성코드 감염 위험성 - 망간 연계 구간의 접근통제 적절성

□ 위험성 평가 시 최근 **보안취약점** 및 **보안사고 사례** 등을 **고려**하여 **망분리 예외**에 따른 **보안사고 발생 가능성**을 다각도로 검토

3 보안대책 적용

□ 망분리 예외 적용 시 **전자금융감독규정 시행세칙 <별표 7>**에 명시된 **망분리 대체 정보보호통제**를 이행

[「전자금융감독규정 시행세칙」의 망분리 대체 정보보호 통제 내용(연구·개발 관련)]

① 유해 사이트 차단 등 외부 인터넷 접근통제 대책 수립 적용
② 연구 개발망과 내부망간 독립적인 네트워크 구성
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
⑤ 중요 소스코드 등에 대한 외부 반출방지 등 보안관리 대책 적용

※ 연구·개발 관련 정보보호 통제의 세부 적용방안은 제4장에서 설명

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

4 정보보호위원회 의결

□ 망분리 예외에 따른 **자체 위험성 평가** 결과 및 적용된 **보안대책의 적정성** 등을 **정보보호위원회 의결**을 통해 최종 확인할 것을 권고

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

[정보보호위원회의 연구·개발 목적의 망분리 예외 심의·의결 시 검토사항]

○ 연구·개발 목적의 망분리 예외 범위 설정의 적정성
○ 연구·개발망 관련 위험 식별 등 자체 위험성 평가 수행의 적정성
○ 연구·개발망에 대한 정보보호 대체통제 적용 및 자체 위험성 평가에 따른 추가 보안대책 등의 적정성

※ 망분리 예외 적용 완료 이후 연구·개발망 구성 변화 등으로 보안대책의 중대한 변경이 있는 경우 정보보호위원회 심의·의결을 재수행할 것을 권고

Ⅳ. 연구·개발망 구성 및 보안관리 방안

◈ 본 유의사항에 제시된 보안관리 방안은 금융회사 등의 보안대책 적용 지원을 위해 작성된 것으로 법적 구속력은 없으며,

◈ 금융회사 등은 제시된 보안대책 외에도 자체 위험성 평가 결과 등으로 식별된 보안위험을 완화하기 위해 추가적인 보안대책을 마련하여 시행할 필요

1 유해사이트 차단 등 외부 인터넷 접근통제 대책 수립 적용

□ 인터넷 등 **외부망 접속이 허용되는 범위 및 신청 절차** 등에 대해 **내부 기준을 마련**하여 운영

□ **연구·개발**과 **무관**하거나 **해킹 등에 악용될 수 있는 웹사이트** 등의 접속을 차단

[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) 등에서 접속 차단 관련 웹사이트 등의 최신정보 확인 가능

□ 전자금융서비스 관련 소스코드 등 **중요정보가 저장된 개발 단말기 및 시스템** 등은 **외부 인터넷 연결 제한 권고**

○ 단, 업무상 불가피한 경우 그 **사유**와 **중요정보 유출방지 대책 등을 검토**하여 **정보보호위원회 승인**을 받을 필요

□ 외주개발자를 포함하여 외부에서 연구·개발망으로의 **상시 원격 접속 가능**

○ 원격 접속 시 금융보안원의 「**금융회사 재택근무 보안안내서**('20.10월)」 준수 필요

[참고] 재택근무 시 원격접속 유형(「금융회사 재택근무 보안안내서」 內 발췌)

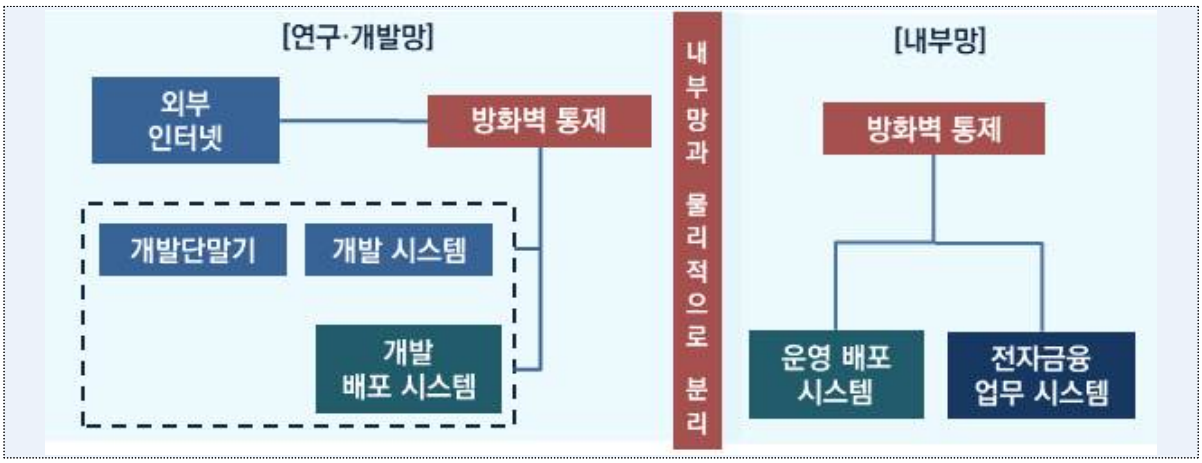
구 분	접속방식 및 특징
가상화 데스크톱 기반(VDI) 방식	- 외부 단말기에서 VDI(DaaS 등 서비스도 활용 가능)의 가상 업무용 단말기를 경유하여 내부망에 접속 - 가상 업무용 단말기에서만 업무를 처리하며 외부 단말기에는 가상화 데스크톱 이미지 등만 표시
원격접속 프로그램 방식	- 외부 단말기에서 원격접속 프로그램을 이용하여 접속(원격접속 중계서버를 통한 접속도 가능) - 원격접속 프로그램 방식은 가상이 아닌 실업무 단말기에 접속하여 업무를 처리
직접 접속 방식	- 외부 단말기에서 내부 업무용 단말기를 경유하지 않고 내부 서버 등에 직접 접속 - 외부 단말기에서 업무 처리 시 업무 데이터가 외부 단말기 내에 저장되므로 정보 유출 등에 대비할 필요

2 연구·개발망과 내부망간 독립적인 네트워크 구성

□ **연구 · 개발망**은 전자금융업무 시스템 등이 위치하는 내부망과 **물리적으로 분리***하여 **독립된 인프라**로 구성 · 운영

* 전자금융서비스를 제공하는 내부망과 별도 회선으로 네트워크 인프라 구성

[참고] 내부망과 독립적으로 구성된 연구·개발망(참조 구성안)



□ 금융회사 등은 **자사 업무 환경 등에 적합**하고 **안전한 방법**으로 연구·개발 관련 네트워크를 구성

○ 네트워크 구성 시 **연구·개발망의 보안위협**이 내부망 또는 금융서비스에 미치는 **영향이 최소화**되도록 고려

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

※ 실제 서비스 제공 등을 수행하는 경우 연구·개발 목적에 미 해당

□ 연구 · 개발망 구성 시 방화벽, 침입방지시스템(IPS), 유해사이트 접속 차단 시스템 등의 **정보보호시스템**을 설치 및 운영

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

※ 금융보안원「금융분야 클라우드컴퓨팅서비스 이용 가이드」참조

3 연구·개발 단말기 및 시스템에 대한 보호대책 수립·적용 및 중요정보 처리 여부 모니터링

□ 인터넷 등 외부망에서 연구 · 개발망으로의 **접속 차단** 권고

※ 단, 내부 절차에 따라 허용된 외부로 부터의 원격 접속은 예외

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

□ 연구 · 개발 단말기 등에서 내부망으로의 접근이 불가하므로 **사내 메신저**나 **그룹웨어** 등은 **별도 단말기**에서 사용

□ 연구 · 개발망에서 무선통신망 사용 시 **전자금융감독규정(제15조 제6항) 준수** 및 사용자 인증 등 **보안대책 적용** 필요

※ 전산실 內 설치되는 개발 관련 시스템 등은 무선통신망 접속 차단

[연구·개발망에서 무선통신망 사용 시 보안대책(예시)]

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

□ 연구·개발 단말기 및 시스템에 저장된 전산자료 內 **개인신용정보 포함 여부**를 **주기적으로 검사 및 삭제** 조치

4 연구·개발망의 침해사고 예방 및 사고대응 대책 수립

□ 연구·개발망에서 발생할 수 있는 **보안사고를 최소화**하기 위한 **추가 보호대책을 검토**하고 이를 **내부 보안정책에 반영**

○ 정보유출 등 **보안사고** 방지를 위해 **연구·개발망을 보안관제** 범위에 포함하고 모니터링 결과를 **주기적**으로 **검토**

※ 금융보안원의 통합보안관제 범위에 연구·개발망을 포함시키는 방안도 고려

○ 연구·개발망의 **인터넷 접속 기록**을 **1년 이상** 보관하고, 주요 **파일 업로드·다운로드 내역**을 **주기적으로 검토**

□ 중요 소스코드 유출* 등 연구·개발망에서 **보안사고 발생** 시에 대비한 **대응절차 마련**

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

[소스코드 유출 시 대응조치(예시)]

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

□ 보안사고 발생 시 **상세 원인분석**을 위해 충분한 **디지털 증거를 보존**해야 하며 원인분석 前 **증거 삭제(PC 포맷 등) 행위 금지**

※ 침해사고대응기관에 상세 원인분석 요청 가능(권고)

□ 연구·개발망에서 발생한 **보안사고**가 **내부망으로 확산**되지 않도록 **네트워크 격리** 등 **긴급 대응 절차**를 이행

□ **소스코드 공유 플랫폼** 등에 중요 **소스코드가 무단 공개**되는 경우에 대비하여 **무단 게시 중단 요청 등 대응절차*** 마련

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

5 중요 소스코드 등에 대한 외부반출 방지 등 보안관리 대책 적용

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

[연구·개발망 內 소스코드 보안관리 정책(예시)]

- 전자금융서비스 관련 소스코드 보관·반출 등 보안관리 방안
- 소스코드 보안 관련 내부정책 위반 시 제재 방안
- 연구·개발망의 코드서명 및 암호키 등의 관리 방안
- 소스코드의 운영 환경으로 이관 절차 및 보안 통제방안
- 소스코드 유출 등 보안사고 발생 시 대응 절차 등

[참고] 소스코드의 영업비밀 지정 요건 관련 대법원 판결(2008도9066 판결) 내용]

- 퇴직 직원이 소스코드 등을 경쟁사에 유출한 사건에서 보안서약서를 작성했음에도 기업에서 보안조치 및 관련 내부규정이 미흡하여 해당 소스코드를 「부정경쟁방지법」상의 영업비밀로 보지 않아 원고가 패소한 사례
- 해당 판결에 따르면 영업비밀은 비밀로 인식될 수 있는 표시나 고지, 정보에 접근할 수 있는 대상자나 접근방법 제한, 정보를 접근한 자에 대한 비밀준수 의무 부과 등 객관적으로 그 정보가 비밀로 유지·관리되고 있다는 사실이 인식 가능한 상태인 것을 말함.
- 따라서, 금융회사 등이 소스코드 유출 등 사고에 대해 기업이 보호받고 적절한 조치를 취하기 위해서는 **①중요 소스코드 지정 및 보안 관련 내규 수립, ②중요 소스코드에 대한 접근통제 설정, ③소스코드 유출시점 파악을 위한 모니터링 등 통제 조치 적용** 등이 필요

□ 전자금융서비스 등 **주요 업무에 사용되는 소스코드**는 중요 소스코드로 지정하여 **강화된 통제 조치*** 권고

* 주요 직무자 外 접근 금지, 지정된 시스템 및 단말기에서만 소스코드 접근(또는 저장)허용, 소스코드접근 내역 기록, 소스코드 접근 권한자에 대한 보안서약서 징구 등

□ 중요 소스코드의 **외부 반출을 엄격히 금지**하고 필요 시 **정보보호최고책임자의 사전 승인** 필요

○ 특히, **소스코드 공유 플랫폼**(깃허브 등)이나 **메신저** 등에 중요 소스코드가 **업로드**되거나 **공유**되지 않도록 **각별히 유의** 필요

□ 정보유출방지솔루션(DLP) 등을 통해 중요 소스코드의 **외부 유출을 탐지**하고 **차단***할 것을 권고

* DMZ 구간에 네트워크 DLP 장치 구성, 단말기에 호스트 DLP 설치 등

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

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

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

[소스코드 저장소 구성 시 보안 고려사항(예시)]

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

□ 운영시스템으로 **중요 소스코드 이관** 시 **시큐어코딩** 여부 확인 및 **소스코드 무결성 검증** 등 수행

ㅇ **외부주문** 등을 통해 **연구·개발**을 수행하는 경우 **전자금융감독규정 제60조**(외부주문등에 대한 기준)를 준수

□ 기타 오픈소스 라이센스 관리 등에 관한 사항은 금융보안원의 「**금융분야 오픈소스 소프트웨어 활용·관리 안내서**」를 참조

첨부 1 연구·개발망 구성 및 보안관리 방안(요약)

구 분	보안관리 방안
1. 유해 사이트 차단 등 외부 인터넷 접근통제 대책 수립 적용	인터넷 등 외부망 접속이 허용되는 범위 및 신청 절차 등에 대해 내부 기준을 마련하여 운영
	연구·개발과 무관하거나 해킹 등에 악용될 수 있는 웹사이트 등의 접속을 차단
	전자금융서비스 관련 소스코드 등 중요 정보가 저장된 개발 단말기 및 시스템 등은 외부 인터넷 연결 제한 권고 ※ 단, 업무상 불가피한 경우 정보보호위원회 승인 필요
	연구·개발망에서 원격 접속 시 금융보안원의 「금융회사 재택근무 보안 안내서」 준수 필요
2. 연구·개발망과 내부망간 독립적인 네트워크 구성	연구·개발망은 내부망과 물리적으로 분리
	자사 업무 환경 등에 적합하고 안전한 방법으로 연구·개발망 구성
	실 업무 또는 서비스 제공에 필요한 시스템은 연구·개발망 위치 금지
	연구·개발망 구성 시 방화벽, 침입방지시스템(IPS), 유해사이트 접속 차단 시스템 등 정보보호시스템을 설치 및 운영
	클라우드 환경에 연구·개발망 구축 시 전자금융감독규정의 클라우드 이용 관련 사항 준수 ※ 금융보안원의 「금융분야 클라우드컴퓨팅서비스 이용 가이드」 참고
3. 연구·개발 단말기 및 시스템에 대한 보호대책 수립·적용 및 중요정보 처리 여부 모니터링	인터넷 등 외부망에서 연구·개발망으로 접속 차단 권고
	망분리 外 전자금융감독규정의 안전성 확보 의무 준수
	연구·개발 단말기에서 사내 메신저나 그룹웨어 등 사용 금지
	연구·개발망에서 무선통신망 사용 시 전자금융감독규정(제15조 제6항) 준수 및 사용자 인증 등 무선통신망 보안대책 적용
	연구·개발 단말기 및 시스템에 저장된 전산자료 내 개인신용정보 포함 여부를 주기적으로 검사 및 삭제 조치
4. 연구·개발망의 침해사고 예방 및 사고대응 대책 수립	연구·개발망 보안사고 최소화를 위한 추가 보호대책을 내규에 반영
	연구·개발망의 보안관제 범위 추가 및 모니터링 결과의 주기적 검토 이행
	연구·개발망의 인터넷 접속 기록을 1년 이상 보관 및 주요 파일 업로드, 다운로드 내역의 주기적 검토
	연구·개발망에서의 보안사고 발생 시 대응 절차 마련
	보안사고 발생 시 상세 원인분석을 위한 충분한 디지털 증거 보존 및 원인분석 前 증거 삭제 금지
	연구.개발망에서 발생한 보안사고의 내부망 확산 방지를 위해 네트워크 격리 조치 등 긴급 대응 절차 이행
	소스코드 공유 플랫폼 등에 중요 소스코드가 무단 공개되는 경우에 대비하여 무단 게시 중단 요청 등 대응절차 마련

구 분	보안관리 방안
5. 중요 소스코드 등에 대한 외부반출 방지 등 보안관리 대책 적용	연구·개발망 內 소스코드 보호를 위한 추가 보안대책을 내규에 반영
	주요 업무에 사용되는 소스코드는 중요 소스코드로 지정하여 강화된 통제조치 적용
	중요 소스코드의 외부 반출 금지 및 필요 시 정보보호책임자가 사전 승인
	소스코드 공유 플랫폼이나 메신저 등에 소스코드가 업로드 되거나 공유되지 않도록 유의
	정보유출방지솔루션(DLP) 등을 통해 중요 소스코드의 외부 유출을 탐지·차단할 것을 권고
	연구·개발 시 실제 서비스 운영 과정에서 사용되는 중요 정보(코드서명 인증서 등) 활용 금지
	소스코드 저장소에 보관된 중요 소스코드 접근 시 다중 인증을 수행하고 접근 내역을 기록·관리
	운영시스템으로 중요 소스코드 이관 시 시큐어코딩 여부 확인 및 소스코드 무결성 검증 등 수행
	오픈소스 라이센스 관리 등은 금융보안원의 「금융분야 오픈소스 소프트웨어 활용·관리 안내서」 참조
	외부주문 등을 통해 연구·개발을 수행하는 경우 전자금융감독규정 제60조 준수

첨부 2 안전한 연구·개발 환경 구성을 위한 참고자료

1. 안전한 개발 및 배포 지침 (영국 국립사이버보안센터)

* 원문 : National Cyber Security Centre(NCSC), "Secure development and deployment guidance", 2019.2.

원칙	실천 사항
1. 안전한 개발에 대한 전사적 관심	기획 단계부터 보안 요구사항을 명확히 정의
	보안은 모든 구성원의 필수 요소로 일상적 관행이 되어야 함
	직원들이 보안 이슈를 제기하고 질문하도록 장려
	기능이나 제공 기한을 위해 보안조치를 미루는 행위 지양
	프로젝트 설계 및 개발 관련 보안전문 지식 보유
	보안 지식 확장을 위해 전문가 지원 요청
	보안 개발 지원 교육, 도구 및 개발 환경 제공
	신속한 보안 문제 발견을 위해 비난하지 않는 문화 장려
	제품을 지원하기 위한 합리적 보안(과도한 경우 보안 우회 시도 증가)
2. 보안 지식을 유지	개발자는 소스코드 관련 보안위협을 인지하고 있어야 함
	개발자 채용 프로세스를 통해 기본적인 보안지식을 확인
	지속적인 보안 지식 및 기술 개발을 위한 시간과 자원 확보
	개발자에게 소스코드 관련 위협 유형에 대해 교육(워크샵 등)
	개발자에게 소스코드 보안 관련 책임을 부여
	중요 요소 구현시 코드를 방어적으로 작성(입력값 검사 등)
	보안 전문가가 보안 관련 중요 구성요소를 개발자에게 설명
	자체적 보안 구성 대신 충분히 검증된 보안 구성 사용(솔루션 등)
	자사 제품의 실제 이슈를 통해 실수로부터 배우는 세션 수행
	제품과 관련된 유용한 보안 교육 목록 유지
	공개 프로필에서 공격자가 사용할 수 있는 정보 제한
	사용하는 도구, 언어 및 기술의 보안 기능을 최신상태로 유지
3. 명확하고 유지가능한 코드 개발	코드 레이아웃을 논리적으로 설계(SOLID 원칙 준수 등)
	보안 코딩 표준 준수
	명확한 명명 규칙 사용(클래스, 메서드, 파일 및 폴더명 등)

원칙	실천 사항
3. 명확하고 유지가능한 코드 개발	개발자에게 좋은 지원 도구 제공(린팅을 지원하는 IDE 등)
	일관된 코딩 스타일 유지
	코드 블록 책임을 명확하게 설명(주석을 통한 설명 등)
	논리적으로 격리된 별도의 자격증명 유지(자격증명 하드코딩 금지)
	검토 및 롤백 단순화를 위해 작고 규칙적인 코드 커밋 수행
	코드 작성자 또는 상태를 위조할 수 없도록 강력한 통제 적용
	피어리뷰를 통해 안전하지 않는 코딩 관행을 검토
	동일한 코드를 작업할 때 규칙적인 팀 커뮤니케이션 수행
	개발 관련 결과를 명확하고 일관되게 문서화하고 주석 처리
	제품에 대한 지식이 유지되도록 신규 인력에게 충분한 지원 제공
	반환 값을 확인하고 적절하게 오류 처리
4. 개발 환경 보호	필요한 도구와 환경 제공(부족한 경우 위험한 방법을 선택할 우려)
	사용자를 교육하고 의심스러운 활동 또는 침해 탐지 기능 구현
	개발 단말기에 대한 엔드포인트 보안 통제 적용
	중요 시스템 등에 대한 자격증명 및 암호키 보호
	침해의 영향을 평가하고 후속 보안통제 적용
	개발 환경에서 실제 운영 서비스 실행 금지
	안전한 네트워크 아키텍처 적용(심층 방어 네트워크 등)
	개발 환경에 대한 보안 모니터링 수행
5. 소스코드 저장소 보호	신뢰할 수 있는 소스코드 저장소 선택
	코드 저장소를 변경, 관리할 수 있는 인력을 최소 권한으로 적용
	접근 자격증명 보호(FIDO U2F 등 하드웨어 기반 토큰 고려)
	소스코드에서 기밀 자격증명 분리(중요정보 자동 스캔 등)
	소스코드 저장소에 대한 불필요한 접근권한을 신속하게 회수
	일부에 대해 자동 테스트 및 피어리뷰 등 공개 코딩 활용
	악성코드가 포함되지 않도록 모든 코드 변경사항 검토
	공개 코딩 시 위장된 공격 코드 등 악의적인 코드에 유의
	공개적으로 접근 가능한 저장소를 사용할 경우 계정 관리
	소스코드 저장소가 실패할 경우를 대비해 코드 백업

원칙	실천 사항
6. 빌드 및 배포 파이프라인 보호	신뢰할 수 있는 파이프라인 사용(소스코드 변조 확인 절차 적용)
	배포 전 소스코드 피어리뷰(우회되지 않도록 기술적 통제 적용)
	운영 환경으로 배포를 자동화하는 코드는 신중하게 관리 및 통제
	배포 과정의 일부로 자동화된 테스트 수행
	비밀 토큰 및 자격증명을 노출되지 않도록 신중하게 관리
	배포 파이프라인 통제를 우회하거나 재구성할 수 없는지 확인
	개인이 배포 통제를 수정하거나 자체 구현하지 못하도록 관리
	신뢰할 수 없는 브랜치(branch) 및 풀 요청(pull request)에 주의
	취약한 타사 라이브러리 적용에 유의하고 합법적 출처인지 확인
	필요한 경우 배포의 긴급중단 절차 고려
7. 지속적 보안 테스트	소프트웨어 개발 생명주기에 따라 보안 테스트 수행
	기존 보안 테스트를 간단하고 자동화된 테스트로 변환
	응용 프로그램에 맞게 테스트 조정
	보안 문제가 발견되는 경우 관련 테스트 수행 고려
	테스트 결과를 개발자와 공유하고 커뮤니케이션 수행
	쉽게 자동화할 수 없는 테스트에 보안 전문가 투입
	느리거나 수동의 테스트를 식별하고 빌드 파이프라인 외부로 이동
	실패한 테스트에 대해 수정 또는 제거
	코드 변경 등을 통해 보안 테스트의 정합성을 검증
	보안 테스트를 지원하기 위한 내부 기술 구축
	코드에 대한 테스트가 불가한 경우 해당되는 범위 식별
8. 보안 결함에 대한 계획	취약점 관리 프로세스를 통해 패치 배포 및 취약한 구성 식별
	개발 중 누적된 보안 부채(security debt) 등록부 유지
	보안 이슈 식별, 해결을 위해 보안 기술에 투자
	근본 원인분석 수행 및 해결
	보안 결함을 책임 공개할 수 있는 방법 제공(취약점 책임 공개)
	식별된 문제에 대한 보안 테스트 생성

2. 소스코드 유출위험 방지방안 (싱가포르 은행연합회)

* 원문 : The Association of Banks in Singapore(ABS), "Study on Risk and Impact of Source Code Leakage form Software Vendors", 2021.4.

구 분		통제 사항
1. 민감한 소스코드 식별		권한 없는 자가 소스코드를 악용하여 재정적 또는 평판 관련 피해를 끼칠 수 있는 경우 해당 코드는 민감한 것으로 간주 (예: 독점적인 처리 방식, 지적 재산권, 보안 및 구성 관련 코드, 지급결제시스템 또는 ATM 소프트웨어 관련 코드 등)
		민감한 소스코드를 식별하기 위한 기준을 마련하고 소스코드 목록을 분석하여 민감한 소스코드를 식별
		제3자는 자동 코드 스캔을 통해 코드에서 자격증명과 개발자가 소스코드 저장소에 추가한 암호화 키 등을 탐지·차단
2. 통제 환경 평가	외주 개발	ISO 27001과 같은 보안관리 통제 프레임워크 구축 여부 확인
		정기적 보안 스캔 및 자격 검토 등을 통해 규정 준수 입증
		피싱 및 사회적 공학 위협과 이를 방지하기 위해 취해할 조치 등에 대한 지속적인 사용자 교육 수행
		소스코드 등 민감한 정보의 송신되는 메일 및 파일 업로드 스캔
		민감한 소스코드에 접근할 수 있는 비인가 소프트웨어의 탐지 및 제거 등 효과적인 엔드포인트 통제 구현
	상용 S/W	금융회사의 시스템과 상용 S/W 간의 연결 현황 파악
		상용 S/W 내 저장된 정보 유형 파악하여 각 상용 S/W마다 허용 가능한 위험수준 결정
		상용 S/W 공급업체가 독립적인 감사를 허용하는지 고려
		상용 S/W 공급업체의 평판과 자격 평가
		공급업체의 금융회사에 대한 통지 메커니즘이 적절한지 평가
		상용 S/W 공급업체가 제공하는 서비스 등이 적절한지 평가
		이메일, 클라우드 업로드, 휴대용 매체 사용 등을 통해 소스코드 유출 행위를 모니터링하기 위한 내부 환경 마련
3. 계약상 의무	외주 개발	소스코드 유출 관련 보안사고를 인지하는 경우 적시에 금융회사에 통지(에스컬레이션 보고라인 등을 포함해 계약에 반영)
		지적재작권 침해가 의심되거나 발생된 경우 금융회사에 통보
		S/W 및 데이터 관련 사고에 대한 근본 원인 및 영향분석 수행
		금융회사의 합당한 요청에 성실하게 협력하고 지원
	상용 S/W	소스코드 유출 위험 및 영향 등을 평가하여 금융회사가 규정한 계약상 최소 요구사항을 충족하는지 확인

구 분		통제 사항
4. 접근 통제 관리	금융 회사	민감한 소스코드가 깃허브와 같은 제3자에 의해 관리되는 경우 소스코드 저장소를 내부에서 관리하고 다른 저장소와 분리 고려
		민감한 소스코드로의 접근에 대한 적절한 통제 및 모니터링
		계약 종료 시 민감한 소스코드에 대한 제3자의 접근권한 제거
	제3자	민감한 소스코드 저장소에 접근하기 전 사용자 인증 (관리되지 않는 환경에서의 원격 접근 시에는 추가적인 통제 필요)
		민감한 소스코드 저장소 및 아티펙트에 대한 최소한의 권한과 알필요성의 원칙에 따라 엄격하게 접근권한 부여
		소스코드 저장소에 접근하는 사용자에 대한 암호기반 통제 적용
		민감한 소스코드 저장소로의 모든 접근은 기록되어야 하며, 무단 접근 및 이상 로그 등을 정기적으로 검토
		민감한 소스코드에 대한 계정 부여 요청을 검토하는 절차를 마련하고, 접근권한에 대해 정기적으로 검토하여 역할, 고용 상태 등에 변경이 있는 경우 즉시 반영
		정보유출방지 솔루션(DLP)에 소스코드 탐지와 관련된 규칙을 포함하여 민감한 소스코드가 외부로 전송되지 않도록 통제
		민감한 소스코드에 접근하는 개발자 단말기에 강력한 보안통제를 구현하여 민감한 소스코드가 보호되지 않는 환경에서 접근되지 않도록 조치해야 함
5. 소스코드 유출 사고대응	준비	사고대응 계획 문서화(역할 및 책임 정의) 및 필요 자원 지원
		금융회사는 소스코드 유출사고에 따라 영향을 받을 수 있는 시스템을 신속하게 식별할 수 있어야 함
		소프트웨어·시스템의 목록화 및 관련된 위험의 관리
	식별	소스코드 유출 등 위반 행위에 대한 위협 인텔리전스 탐지
		제3자가 위협을 식별하기 위한 메커니즘을 갖췄는지 확인
	억제	유출된 소스코드에 대한 영향분석을 수행하고 보안 검토를 통해 잠재적으로 악용될 수 있는 취약성과 해결방법을 식별
		영향받는 시스템에 대한 로그 모니터링 및 탐지 강화
		식별된 최신 보안 취약점에 대한 신속한 패치 적용
	근절	사고 재발방지를 위해 악성코드 제거 및 소스코드 저장소에 대한 추가적인 보안통제 구현 등을 적용
	복구	소프트웨어 또는 시스템의 무결성 손상 등 위험을 확인하고 위험 해결이 어려운 경우 대체 공급방안 등을 고려
	교훈	금융권 전반의 교훈과 공유된 정보를 지속적으로 검토하고 이를 사고대응 계획에 통합

3. 연구·개발 환경의 위험분석 및 보안대책 도출(예시)

구 분	내용
환경 분석	- 코드 변경 빈도가 높아지며 취약한 코드 식별이 어려워짐 - 기밀 정보 누출 가능성, 지적 재산권 보호, 코드 내 취약성 등에 따라 소스코드 저장소에 대한 보안 관련 검토 필요 - 외부 개발자에게 소스코드 저장소에 대한 접근권한이 필요하며 비인가자에 대한 접근통제 등도 필요
주요 자산	- 소스코드 관리 및 버전관리 시스템 - 소스코드 저장소 - 개발자 워크스테이션 - CI/CD 파이프라인
위협 모델	- 인적 오류 : 소스코드에 암호키 포함, 액세스 토큰 노출 등 - 배포 결함으로 이어지는 절차 : 개발자가 취약한 코드를 소스코드 저장소에 커밋하여 보안 취약점이 프로그램에 포함 - 잘못된 데이터 또는 소스코드 등 데이터 손실 - 웹 애플리케이션 공격 또는 코드 주입 - 애플리케이션 코드의 무단 변경 또는 조작 : 개발자가 의도적으로 취약한 코드를 커밋하거나 무단으로 변경 - 다중 테넌트 환경에서 격리 위반 : 소스코드가 잘못된 저장소에 커밋되거나 권한 경계를 넘어 무단 변경을 수행 - 데이터 기록의 무단 변경 또는 조작 : 소스코드 저장소를 무단으로 조작하여 랜섬웨어 등을 통해 소스코드 암호화 - 기밀정보 손상 또는 데이터 침해 : 소스코드 저장소에 접근하는 제3자 애플리케이션에 대한 보안 검증 미흡 시 무단 접근으로 이어져 중요 소스코드 및 기능이 노출되는 결과 초래 가능
보안 대책	- 소스코드 또는 구성 파일에 기밀 정보 저장 금지 - 코드 커밋 중 코드에서 기밀 및 자격증명 스캔 - 개발자에 대한 이중 인증 활성화 - 접근을 요청하는 모든 클라이언트 및 제3자 애플리케이션 검증 - CI/CD 파이프라인에 보안 테스트를 추가하여 취약점 탐지 - 개발자가 사용하는 SSH 키 및 액세스 토큰 등 자격증명을 정기적으로 교체 - 저장소간 명확하게 분리된 경계 및 접근통제 정책 유지

※ 참고 : SecurityPatterns.io(Source code management)

4. 시스템 및 단말기에서의 주요 디지털 증거 및 기록

구 분		디지털 증거 및 기록
정보보호 시스템	공통 사항	- 감사 로그(시스템 로그인 정보 등)
	침입탐지시스템(IDS)	- 침입 탐지 및 차단 로그 - 패킷 헤더와 플로우 기록 정보, 패킷 페이로드 - 출발지/목적지 IP 주소, TCP/UDP 포트, 네트워크 - 이벤트 발생 시간
	방화벽(F/W)	- 허용 및 차단 정책 - 접근 및 에러 로그
	네트워크 접근 제어(NAC 등)	- 네트워크 비정상 행위 탐지 로그(Spoofing 등) - 업데이트 파일 배포 로그 등
	서버보안 (Secure OS 등)	- 시스템 접속 로그, 중요 파일 실행 로그 - 서버보안 데몬 실행 로그
	디도스 대응 시스템	- 트래픽 발생 추이 - 디도스 공격 패킷
	USB 통제	- USB 연결 정보
	백신	- 악성프로그램 탐지, 삭제 로그
	데이터유출방지 시스템(DLP)	- 프로그램 설치 정보, 응용 프로그램 접속 로그, - 매체 사용로그
	문서암호화관리 시스템(DRM)	- 프로그램 설치 정보, 응용 프로그램 접속 로그, - 매체 사용로그
	APT탐지시스템	- APT 탐지 로그(유입 실행파일 관련 정보)
	DB보안	- 질의 및 응답 관련 로그 - DB 변경 관련 로그
	패치관리 서버	- 파일 배포 정보
	무선침입방지시스템 (WIPS)	- 무선 침입 탐지 및 차단 로그
	인증서버	- 로그인 성공/실패 로그 등 인증 관련 로그
	이메일 보안	- 비정상 파일이 포함된 이메일 송수신 로그
윈도우 OS	레지스트리	- Windows OS의 설정 및 선택 항목을 기록하는 데이터베이스
	이벤트 로그	- 시스템의 보안, 응용프로그램, 하드웨어 정보
	계정(Account) 사용 기록	- 계정의 사용내역 및 접근시도 등에 관한 정보
	파일 및 디렉터리 정보	- 파일시스템의 디렉터리 및 파일에 대한 접근, 생성, 수정된 정보 등
	실행파일 기록	- 프리패치(Prefetch), 슈퍼패치(Superfetch) 등 실행된 파일에 관한 기록
	인터넷 접속 기록	- 웹 기록, 쿠키, 세션 정보, 캐시 등 인터넷 사용에 관한 기록
	이메일 사용 기록	- 웹메일, 메일 클라이언트에 사용기록 등
	파일 복구	- 크래시 덤프, 시스템 복원지점 복사본 등

AGR-Ⅱ-2023-②-403

연구·개발 목적의 망분리 예외 적용에 따른 보안 유의사항

발행일 : 2023년 3월
발행인 : 김 철 웅
발행처 : 금융보안원
경기도 용인시 수지구 대지로 132
전 화 : (02) 3495-9000

금융보안원
FINANCIAL SECURITY INSTITUTE