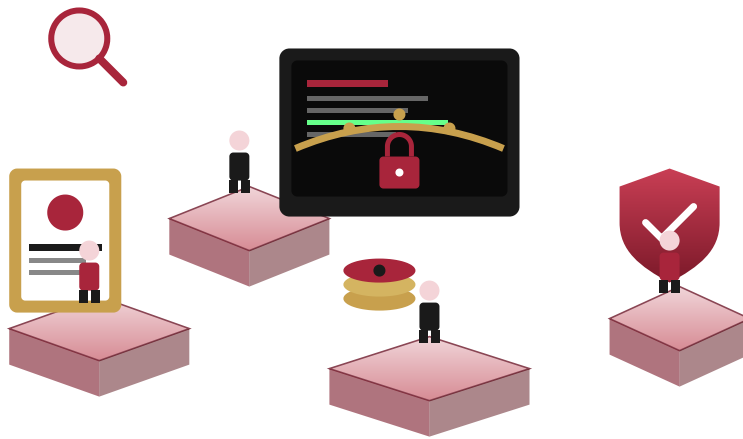


금융분야 침투테스트(모의해킹) 수행 가이드라인

2026. 7.



제 · 개정 이력

REVISION HISTORY

[illegible]

목 차

I. 개요	1
1. 배경 및 목적	1
2. 개념 및 용어	2
3. 가이드 구성	3
II. 수행 절차	4
III. 사전 준비	5
1. 수행 주체 결정	5
2. 수행 인력 요건	5
3. 점검 목표 및 수행 방식 결정	6
IV. 점검 수행	8
1. 점검 계획 협의	8
2. 수행 합의서(RoE) 작성	8
3. 점검 수행	9
4. 연속성 확보(Leg-up)	11
5. 점검 종료	12
V. 결과 보고	13
1. 내부 보고	13
2. 금융당국 보고	13
VI. 사후 관리	14
1. 취약점 조치 및 이행 여부 관리	14
2. 결과 공유 및 보안 내재화	14
VII. 결론	15
VIII. 별첨	16
1. 침투테스트 수행 합의서(RoE) 예시	16
2. 침투테스트 수행 적정성 체크리스트	19



개요

OVERVIEW

1 배경 및 목적

최근 금융권을 겨냥한 사이버 위협은 지속적으로 고도화되고 있다. 단순한 자동화 도구 기반의 공격을 넘어, 공격자는 내부 구조를 사전에 파악하고 **여러 취약점을 연계**하여 침투를 시도하는 양상을 보이고 있다. 이에 따라 기존의 취약점 분석·평가를 넘어, **실제 침해사고로 이어질 가능성까지 선제적으로 대응**할 수 있는 보안 대책이 요구된다.

이러한 환경 변화를 반영하여, 국내외 감독기관에서는 금융회사가 정기적으로 **시나리오 기반의 침투테스트**를 수행하도록 요구하고 있다. 본 가이드라인은 금융회사 보안담당자가 침투테스트를 적절히 수행할 수 있도록 **단계별 실무 기준**을 제시하는 것을 목적으로 한다.

이를 통해 금융회사가 자사 보안체계의 실효성을 주기적으로 점검하고, 발견된 취약점에 대한 **근본적인 개선**을 이끌어 낼 수 있도록 지원하고자 한다.

□ 국내 규제 동향

침투테스트는 다음과 같이 다양한 규제를 통해 확대되고 있다.

- **개인정보 상시평가 모의해킹 항목 신설**: 개인정보 상시평가 기술적 보호조치 중 취약점 점검 항목에 모의해킹 수행 여부가 신설되며, 보안 실효성을 한층 강화하고 있다.
- **ISMS-P 기술심사 모의침투 시험 도입**: 정보보호 및 개인정보보호 관리체계(ISMS-P) 인증심사 시, 기술심사 항목으로 모의침투가 포함되어 형식적인 보안 인증을 탈피하여 기술적 보호 체계의 내실을 기하고 있다.
- **개인정보 안전성 확보조치 기준**: 공공시스템 운영 기관은 외부 전문가를 활용한 침투테스트를 연 1회 이상 수행하도록 규정하고 있으며, 금융권으로의 확대 적용이 논의 중에 있다.

□ 해외 규제 동향

최근 해외 주요 감독기관은 금융권의 사이버 보안 및 운영 안정성 강화를 위해 **위협 정보 기반 침투테스트 프레임워크**와 관련 규제를 도입하여 운영하고 있다.

▶ <표 1> 해외 주요 침투테스트 규제 프레임워크

기준	주관/운영 주체	주요 내용
STAR-FS	영국 금융당국 (BoE/PRA/FCA) · CREST	영국 금융당국·CREST가 운영하는 위협 정보 기반 침투테스트로, 핵심 업무 서비스를 대상으로 수행 후 그 결과를 감독기관에 보고
TIBER-EU	유럽중앙은행(ECB) · 유로시스템	ECB가 주도하는 유럽 공동 프레임워크로, 실제 공격자의 전술·기법·절차(TTP)를 기반으로 핵심 기능과 지원 시스템을 점검
DORA	유럽연합(EU)	금융권 디지털 운영복원력 확보를 위한 EU 규정으로, 일정 요건을 충족하는 기관은 최소 3년마다 위협 정보 기반 침투테스트(TLPT) 수행을 의무화
CREST	CREST (Council of Registered Ethical Security Testers)	침투테스트 수행 인력·서비스 제공자의 자격과 품질을 보증하는 국제 인증체계로, STAR-FS 등 감독 프레임워크의 품질보증 기반으로 활용

2 개념 및 용어

침투테스트(모의해킹)와 관련하여 **취약점 분석평가**와 **유사한 개념이 혼용**되고 있어, 본 가이드라인에서는 다음과 같이 용어와 개념에 대해 정리하고자 한다.

▶ <그림 1> 점검 방식별 대상 범위



□ 취약점 분석평가(Vulnerability Assessment)

취약점 분석평가는 각 분야별 IT 시스템에 존재하는 보안 취약점을 **체크리스트화하여 점검**하는 방식이다. 전자금융기반시설을 포함한 주요 시스템에 대해 정기적으로 수행하며, 각 취약점의 양호·취약 여부를 판단하는 것을 목적으로 한다. 취약점 분석평가는 보안 기준 준수 여부를 확인하는 데 효과적이며, 실제 공격자가 복수의 취약점을 연계하여 핵심 자산에 침투하는 가능성을 입증하는 것은 **침투테스트의 영역**이다.

□ 침투테스트(모의해킹·모의침투, Penetration Testing)

침투테스트란 실제 공격자와 동일한 기법을 활용하여 금융회사의 IT 인프라에 대한 침투 가능성을 입증하는 **목표 지향적 점검 방식**이다. 단순한 취약점 목록 도출에 그치지 않고, **초기 침투 → 내부 확산 → 핵심 자산 접근**이라는 공격 흐름(Kill-Chain) 전체를 재현하는 것이 핵심이다.

□ 레드티밍(Red Teaming)

레드티밍이란 실제 위협 행위자(APT 그룹 등)의 **전술·기법·절차(TTP)**를 기반으로 구성된 고도화된 공격 시나리오를 장기간에 걸쳐 수행하는 방식이다. TIBER-EU, DORA 등 해외 기준에서 요구하는 형태로, 사전 위협 정보 수집 단계를 거쳐 실제 공격자의 행위를 최대한 재현한다. 레드티밍은 대형 금융기관의 **사이버 복원력 검증**을 목적으로 하며, 일반적인 침투테스트보다 수행 기간과 비용이 상당히 높다. 다만 현재 국내 금융권에서는 **침투테스트의 내실화**가 우선 과제이며, 레드티밍은 중장기 발전 방향으로 참고할 수 있다.

▶ <표 2> 취약점 분석평가 · 침투테스트 · 레드티밍 비교

구분	취약점 분석평가 (Vulnerability Assessment)	침투테스트 (Penetration Testing)	레드티밍 (Red Teaming)
수행 목적	취약점 목록 도출, 기준 준수 확인	실제 침투 가능성 입증	위협 행위자 기반 사이버 복원력 검증
점검 목표	전자금융기반시설	핵심·중요 서비스 및 자산	핵심·중요 서비스 및 자산
공격 허용 범위	전자금융기반시설	IT 인프라 전체	IT 인프라 외 인력·시설 등 기업의 모든 유/무형 자산
블루팀 인지	전체 공지	일부 공지 또는 비공지 가능	원칙적 비공지
수행 기간	수일~수주	평균 1~2개월 이상	3개월 이상
수행 방식	체크리스트 항목별 점검	공격 단계 구성 후 시나리오 수행	위협 정보 기반 시나리오 수행
결과물	항목별 양호·취약 목록	침투 경로 중심 보고서, 영향도 분석	위협 시나리오별 방어력 평가 보고서

3 가이드 구성

본 가이드라인은 보안담당자가 침투테스트를 기획·관리할 수 있도록 단계별로 구성하였다.

II 수행 절차

전체 수행 흐름을 한눈에 파악할 수 있도록 단계별 구조 제시

III 사전 준비

수행 주체 결정, 인력 요건, 점검 범위·방식 선택, 시나리오
방향 결정

IV 점검 수행

착수 협의, 수행 합의서 작성, 점검 수행, 연속성 확보,
복구작업 등 관리 사항

V 결과 보고

취약점 조치 계획, 내부 경영진 보고, 금융당국 보고 기준

VI 사후 관리

취약점 조치 이행 여부 점검 및 결과 공유 절차

VII 결론

침투테스트의 실질적 활용 방향과 보안 내재화의 중요성 강조

II

수행 절차

PROCESS

침투테스트는 아래의 **4단계**로 구성되며, 금융회사 보안담당자는 각 단계에서의 **역할과 책임**을 명확히 인식하여야 한다.



▶ <표 3> 단계별 주요 활동 및 금융회사 역할

단계	주요 활동	금융회사 역할
사전 준비	대상·방식 결정, 제안요청서(RFP) 작성, 업체 선정	점검 범위 확정, 발주 기준 마련, 업체 자격 검증
점검 수행	계획 협의, 수행 합의서 작성, 점검 수행, 연속성 확보(Leg-up), 복구작업(Clean-up)	수행 합의서 작성·관리, 비상 연락 대응, 진행 모니터링
결과 보고	조치 계획 수립, 내부 보고, 금융당국 보고	취약점 조치 계획 수립, 경영진·당국 보고서 작성
사후 관리	취약점 조치, 이행 점검, 결과 공유	조치 완료 추적, 유사 취약점 자체 점검, 전사 공유

III

사전 준비

PRE-ENGAGEMENT

사전 준비 단계는 침투테스트의 품질을 결정짓는 가장 중요한 단계이다. 점검 범위와 방식을 어떻게 설정하느냐에 따라 이후 수행의 실효성이 크게 달라지기 때문에, 금융회사는 이 단계에서 **충분한 내부 협의**를 거쳐야 한다.

1 수행 주체 결정

침투테스트는 금융회사 **내부 전담반을 구성하여 자체 수행**하거나, **외부 전문업체에 위탁**하여 수행할 수 있다. 금융회사는 보안 인력 현황, 예산, 점검 목적 등을 고려하여 적합한 방식을 선택한다. 외부 전문업체에 위탁하는 경우, 제안요청서(RFP)를 통해 요구사항을 명확히 전달한다. **RFP가 구체적일수록** 업체별 수행 품질의 편차를 줄일 수 있으며, 아래 항목을 포함하여 작성하는 것을 권고한다.

자체 수행 시 준비 사항

- 점검 대상 시스템과의 이해충돌 여부 검토 (담당자는 점검 대상 시스템의 운영·관리 업무와 분리)
- 수행 합의서(RoE) 작성 (4.2항 참조)

외부 위탁 시 RFP 포함 항목

- **수행 방식:** 점검 유형(블랙박스/그레이박스/화이트박스)
- **점검 시나리오:** (필요시) 특화 시나리오 요구사항 명시
- **점검 목표:** 핵심·중요 서비스 및 자산 등 점검을 통해 검증하고자 하는 목표 명시
- **인력 요건:** 수행 책임자(PM) 자격 기준, 팀 구성 요건
- **수행 기간 및 일정:** 착수일, 완료일, 중간 보고 일정
- **결과물 기준:** 보고서 필수 포함 항목, 제출 형식 및 기한

2 수행 인력 요건

자체 수행 또는 외부업체 위탁 여부와 관계없이, 침투테스트 수행 인력을 구성할 때 아래 요건을 고려할 것을 권고한다.

□ 역량 요구 사항

- 초기 침투 이후 권한 상승, 내부 확산, 망분리 우회 등 후속 공격 수행 경험
- 상용 자동화 도구 외 자체 공격 도구 제작·수정 역량
- 침투테스트(모의해킹) 수행 경력 및 관련 자격(OSCP, CREST 등)
- 전자금융기반시설 취약점 분석평가 업무 경력자 최소 1명 이상 포함

3 점검 목표 및 수행 방식 결정

수행 주체와 인력 요건이 확정되면, 실제 점검의 범위와 방식을 결정한다.

□ 점검 목표 결정

공격 허용 범위는 금융회사의 **전체 IT 인프라**를 기준으로 설정하는 것을 권장하며, 점검 목표는 **핵심·중요 서비스 및 자산**을 중심으로 설정한다.

· 전자금융기반시설

대외(인터넷·기업·모바일뱅킹, 트레이딩)

내부(계정계·정보계·대외계·SWIFT)

· 개인정보처리시스템

고객 및 임직원의 개인정보

· 정보보호시스템

접근제어, 단말기관리, NAC, AD, LDAP 등

· 내부업무용시스템

그룹웨어, ERP, 형상관리시스템 등

□ 수행 방식 결정

점검자에게 **사전 제공하는 정보 수준에 따라 세 가지**로 구분된다. 금융회사는 점검 목적과 일정에 따라 적합한 유형을 선택하여야 한다.

▶ <표 4> 수행 방식 비교

유형	사전 제공 정보	적합한 목적
블랙박스 (Black-box)	없음 (공개 정보만 활용)	외부 공격자 관점의 침투 가능성 검증
그레이박스 (Gray-box)	일부 제공 (IP 대역, 계정 일부, 서버·PC 접근권한 등)	내부자 또는 부분 정보(일부 시스템 접근 권한) 획득 상황 재현
화이트박스 (White-box)	전체 제공 (소스코드, API, 관리자 계정)	코드·설계 수준의 취약점 심층 분석

실제 침해사고 가능성 검증이 목적이라면 **블랙박스 또는 그레이박스 방식**이 적합하다. 화이트박스 방식은 **소스코드·설계 수준의 잠재적 취약점**을 심층적으로 분석할 수 있어, 코드 품질 점검이나 특정 취약점 정밀 검증에 효과적이다.

사전 준비 단계에서 결정한 점검 유형, 사전 제공 정보 범위, 시나리오 구성, 블루팀 인지 수준 및 연속성 확보 운영 원칙은 **4.2항의 수행 합의서(RoE)**에 반영하여 최종 확정하여야 한다.

□ 시나리오 결정

침투테스트는 공격 방향과 목표에 따라 검증할 수 있는 보안위협 성격이 달라진다. 외부에서 내부로의 초기 침투 여부뿐만 아니라, 내부망 진입 이후의 **서버 간 이동(Lateral Movement)**, 핵심 자산 접근, 외부로의 정보 유출 경로까지 연계하여 검증할 때 보안체계의 실제 취약점을 보다 입체적으로 파악할 수 있다.

아래 시나리오 유형은 점검 대상을 선택적으로 한정하기 위한 항목이 아니라, 앞서 정한 점검 대상 범위(전체 IT 인프라)를 전제로 어떠한 공격 흐름과 검증 목적을 중점적으로 반영할 것인지 구성하기 위한 예시이다. 따라서 금융회사는 전체 IT 인프라를 대상으로 **외부 침투 → 내부 확산 → 정보 유출**로 이어지는 **시나리오를 기본 축**으로 하고, 연도별 중점 테마에 따라 특정 목적의 시나리오를 추가 수행할 것을 권고한다.

▶ <표 5> 시나리오 유형 예시

시나리오	점검 목표 및 내용
외부 → 내부 침투	인터넷 노출 자산(홈페이지, VPN, 원격접속)을 거점 삼아 내부망까지 진입 가능한지 검증 - 인터넷 노출 웹 서버·애플리케이션의 취약점(원격코드실행, 파일 업로드 등)으로 웹shell을 확보해 DMZ를 장악하고 내부망으로 피벗(Pivoting) 가능한지 검증 - VPN·원격접속(RDP/SSH) 게이트웨이의 취약한 패스워드 인증·다중인증(MFA) 우회·유출 계정 악용으로 원격 접근 권한을 확보하고 내부망에 진입 가능한지 검증 - 노출된 관리 인터페이스·클라우드 설정 오류(공개 스토리지, 관리 콘솔·API 키 노출)를 통해 초기 거점을 확보하고 내부 자원에 접근 가능한지 검증 그 외 기타 - 트레이딩 시스템(HTS/MTS/WTS) 등 전용 매체·프로토콜의 취약점을 통한 비인가 주문·거래 조작 가능 여부 - 마이데이터·뱅킹 API 등 대외 연동 접점의 인증·인가 우회로 타인 정보 조회·비인가 거래가 가능한지 검증 - 비대면 실명인증·중요 기능 승인 절차 등의 논리 결함을 악용해 타인 계정 탈취(Account Takeover)·권한 상승까지 이어지는지 검증
내부망 확산	내부망 진입 후 서버 간 이동(Lateral Movement)을 통해 핵심 자산(DB, 관리 서버)의 제어권 확보 여부 외주·임직원·개발·운영망 간 통제 정책 오류를 이용한 망 간 우회 가능성
정보 유출·자산 탈취	내부망에서 인터넷망으로의 비정상 연결·데이터 반출 경로 존재 여부, 나아가 실제 자금·자산 탈취로 이어질 수 있는지 실증 - 고객 개인정보·금융 거래 데이터 등 핵심 정보의 외부 반출(정보 유출) 가능 여부 - 거래 통제 우회·이체 파라미터 변조 등을 연계한 실제 부정 거래(금전·자산 탈취) 가능 여부

IV

점검수행

EXECUTION

점검 수행 단계는 사전 준비 단계에서 결정한 사항을 실제 점검으로 옮기는 단계이다. **점검 계획 협의 및 수행 합의서 작성**을 통해 수행 기준을 확정하고, 합의된 시나리오에 따라 점검을 수행한다. 보안담당자는 전 과정에서 수행팀과 긴밀히 협력하며, 진행 상황을 공유받고 **비상 상황 발생 시 즉각 대응**할 수 있는 체계를 갖추어야 한다.

1 점검 계획 협의

점검 착수 전 수행팀과 점검 목표·시나리오·수행 합의서 등에 대해 사전 협의를 진행한다. 이 단계에서의 **충분한 협의가 이후 점검의 원활한 진행을 좌우**하므로, 다음 사항을 중심으로 협의·확정한다.

- 점검 목표 및 시나리오 결정
- 수행 합의서(RoE) 검토 및 서명
- 비상 연락망 수립
- 연속성 확보(Leg-up) 요청 기준, 승인 절차 및 기록 방식 결정
- 점검 수행 기간 및 산출물 전달 기한 등 일정 확정

2 수행 합의서(RoE) 작성

수행 합의서(Rules of Engagement, RoE)는 점검 과정에서 발생할 수 있는 운영 리스크를 방지하고, **합법적이고 통제된 점검 수행의 근거**를 확보하기 위한 문서이다. 사전 준비 단계에서 결정한 내용을 RoE에 반영하여 최종 확정하여야 하며, **합의서에 명시된 범위를 벗어난 수행은 금지**한다.

▶ <표 6> 수행 합의서 포함 항목

항목	세부 내용
담당자·비상 연락망	비상 시 즉시 연락 가능한 보안담당자, 정보보호책임자, 수행팀 연락처 상호 등재
수행 일정·범위	수행 기간, 공격 허용 시간대, 점검 제외 시스템·IP·도메인 명시
연속성 확보 기준	블루팀 차단·운영 리스크 등으로 점검이 중단되는 경우 연속성 확보를 위한 정보 요청 기준 명시
금지 행위	장애 유발 공격, 고객 데이터 삭제·변조, 네트워크 장비 변경, 합의 외 공격 등
장애 관리	이상 징후 발생 즉시 중단 → 보안담당자 통보 → 영향 파악·복구 후 재개 협의
승인·서명	금융회사 정보보호책임자, 보안담당자, 수행 책임자 서명

RoE는 형식적으로 작성하기보다, **점검 범위·수행 방식·시나리오 구성·연속성 확보 절차·복구작업** 등 점검 전반의 통제사항을 구체적으로 반영하여야 한다. 점검 중 변경이 필요한 경우 사전 협의를 거쳐 변경 내용을 기록·관리한다.

3 점검 수행

침투테스트는 실무에서 널리 활용되는 **MITRE ATT&CK**의 공격 전술(Tactics)·기법(Techniques)과 록히드 마틴(Lockheed Martin)의 **사이버 킬체인(Cyber Kill Chain)** 등 공격자의 실제 침투 절차를 참고하여 정보 수집부터 목표 달성까지의 전 과정을 단계적으로 수행한다. 각 단계에서 발견된 취약점은 개별적으로 처리하는 것이 아니라 **연계하여 공격 체인을 구성함**으로써, 실제 침해사고 가능성을 입체적으로 검증한다.

특히 **MITRE ATT&CK**는 실제 침해사고에서 관찰된 공격 행위를 **14개 전술(Tactics)**과 세부 기법(Techniques) 단위로 체계화한 지식 베이스로, 시나리오 설계·수행 범위 협의·결과 보고의 **공통 언어**로 국내외 침투테스트 실무에서 가장 널리 활용된다. <그림 2>와 같이 ATT&CK의 각 전술은 사이버 킬체인의 단계에 대응되므로, 두 체계를 함께 참조하면 공격 경로를 단계별로 정의하고 시나리오·결과를 체계적으로 관리할 수 있다.

발견된 공격 경로를 ATT&CK 전술·기법에 대응시켜 보면 공격이 어느 단계까지 진행되었고 어느 지점에서 탐지·차단되었는지를 한눈에 파악할 수 있으므로, 점검 결과를 **탐지·대응 체계 개선에 참고**하는 데 유용하다.



수행 합의서(RoE)에서 정한 기준과 범위에 따라 합의된 시나리오를 단계적으로 수행한다.

□ 점검 수행 중 관리 사항

보안담당자는 점검 수행 기간 동안 아래 사항을 관리하여야 한다.

- 수행팀과 사전에 합의한 주기 및 방식에 따라 진행 현황을 파악하고, 합의된 범위 내에서 수행되고 있는지 확인
- 점검 과정에서 서비스 장애 등 운영 영향이 발생한 경우 RoE 장애 관리 절차에 따른 **점검 중단·통보 및 원인 파악**

□ AI 활용 및 유의사항

침투테스트 수행 과정에서 취약점 분석, 공격 코드·페이로드 생성, 정찰 자동화, 보고서 초안 작성 등에 **생성형 AI**를 활용하면 점검의 효율성과 깊이를 높일 수 있다. 다만 금융권의 민감 정보를 다루는 특성상, AI 활용은 아래의 데이터 보호 요건을 충족하는 범위 내에서 이루어져야 한다.

- **비학습 모델 서비스 이용:** 입력한 데이터를 학습에 사용하지 않고 서버에도 저장하지 않는 비학습 모델 기반 서비스를 이용한다. OpenAI(GPT)·Anthropic(Claude)·Google(Gemini) 등 주요 상용 LLM이 기업 계약 또는 API에서 이러한 조건을 제공하므로, 도입 전 **데이터 처리·보관 정책과 계약 조건**을 확인한다.
- **장애 복구 대책 확보:** AI를 활용한 침투테스트 시 자동화된 공격이 빠르게 진행되어 예기치 못한 장애로 이어질 수 있으므로, 점검을 즉시 중단할 수 있는 수단(kill-switch)을 갖춘다. 또한 이 중단 수단이 정상 동작하지 않는 경우까지 감안하여, 점검 대상 시스템의 백업·롤백 등 복구 방안을 사전에 마련하여야 한다.
- **부정확한 결과 도출:** 환각 및 부적절한 문맥 전달로 인해 취약점의 오탐지(False-positive)·미탐지(False-negative)가 발생할 수 있으므로, 생성된 공격 코드·분석 결과의 정확성과 점검 범위 준수 여부는 반드시 점검 인력이 직접 검증한다.
- **생성 코드 실행 통제:** AI가 생성한 공격 코드를 검증 없이 그대로 실행하거나 AI에 실행 권한을 위임할 경우 점검 범위 이탈, 시스템 장애, 비인가 권한 취득 등 의도치 않은 피해가 발생할 수 있으므로, 실제 공격 행위는 반드시 점검 인력의 통제 하에 수행한다.

4 연속성 확보 (Leg-up)

□ 개념

연속성 확보란 점검 진행 중 합의된 시나리오의 연속성을 확보하기 위하여, 금융회사가 수행팀에 **제한적인 정보 또는 접근 권한을 예외적으로 제공**하는 조치이다. 탐지·차단으로 거점이 소실되거나, 시간 제약 또는 운영 안정성 사유로 다음 공격 단계 검증이 곤란한 경우 활용할 수 있다.

□ 요청 가능 기준 및 허용 범위

- 시스템 설정 변경 등 운영 리스크 우려로 다음 단계 진행이 사실상 곤란한 경우
- 이미 확인된 침투 경로·권한 획득 가능성을 근거로, 점검의 연속성 확보가 필요한 경우
- 제공 수준이 점검의 현실성을 훼손하지 않고, 충분한 시간·자원이 있었다면 공격자가 확보할 수 있었을 범위로 합리적으로 볼 수 있는 경우

□ 연속성 확보 미제공 시 처리

연속성 확보 요청을 거절한 경우, 수행팀은 아래 사항을 보고서에 반영하여야 한다.

- 요청 일시·사유·거절 사실의 요청 내역서 기록 및 결과 보고서 포함
- 침투 가능성이 확인된 지점까지의 공격 경로 및 증적 기술
- 이후 단계에서 예상되는 공격 흐름과 잠재적 영향도 명시

※ 실제 공격 진행이 불가한 경우에도 확보된 증적을 근거로 **공격 성공 시의 영향도**가 구체적으로 산정되어야 하며, 단순히 “미수행”으로 기재된 경우 보완을 요청한다.

▶ <표 7> 연속성 확보 예시

상황	요청 내용	제공 예시
서버 제어권 획득 후 권한 상승 가능성 확인, 시스템 중단 우려가 있는 경우	증적 확보 후 시스템 관리자 권한 요청	root 계정 관리자 계정
웹쉘 업로드 성공 후 블루팀이 고의로 삭제하여 거점 소실	동일 수준의 서버 접근 권한 요청	Shell 접근 권한 테스트 계정
관리자 비밀번호 변경 가능성 확인, 변경 시 운영 영향 우려	증적 확보 후 해당 관리자 계정 요청	서버접근제어 관리자 보안솔루션 콘솔

※ 제공된 정보 및 권한은 **승인된 범위 내에서만 사용**하여야 하며, 점검 목적 외 사용을 금지한다.

5 점검 종료

점검 종료 시에는 수행팀이 점검 과정에서 **생성·변경한 항목을 복구**하고, 점검을 위해 제공된 **접근 권한을 회수**한 후 종료하여야 한다. **복구작업(Clean-up)이 완료되지 않으면** 점검용 파일, 테스트 계정, 임시 설정 등이 잔존 위험으로 이어질 수 있으므로 종료 절차의 일부로 반드시 수행하여야 한다.

□ 복구작업 대상

- 점검 과정에서 업로드·설치한 웹шел, 실행 파일, 테스트용 스크립트
- 점검 목적으로 생성한 시스템·서비스 계정, 테스트용 API 키, 인증정보
- 권한 상승 또는 내부 확산 과정에서 추가·변경한 시스템 설정, 권한, 임시 정책
- 연속성 확보로 제공한 테스트 계정·자격증명·테스트 단말 및 임시 접근 권한

□ 확인 및 종료 절차

수행팀은 생성·변경 항목 목록을 작성하여 보안담당자에게 제출하고, 금융회사는 해당 목록을 기반으로 보안담당자 또는 인프라 운영팀이 **직접 삭제·복구**를 수행한 후 ① 목록 완전성 검토 ② 삭제·복구 완료 확인 ③ 연속성 확보 권한 회수·비활성화 확인 ④ 수행팀의 점검 시스템 접근 권한 회수 확인을 거쳐 점검을 종료한다.

결과 보고

REPORTING

점검 수행이 완료되면 금융회사는 점검 결과를 체계적으로 정리하여 **경영진 및 필요 시 감독기관에 보고**한다. 결과 보고는 **시나리오별 공격 흐름과 비즈니스 영향도**를 중심으로 구성하며, 발견된 취약점에 대한 조치 계획을 함께 수립하여야 한다.

1 내부 보고

금융회사는 침투테스트 결과를 검토하고, **요약 보고서·시나리오별 상세 보고서**와 함께 시나리오별 취약점에 대한 조치 계획을 수립하여 경영진에 보고한다.

요약 보고서

- 결과 총평 (주요 침투 경로, 취약 영역 요약)
- 시나리오별 결과 요약 표 (시나리오명·위험등급·결과)

시나리오별 상세 보고서

- 시나리오 개요 (대상, 결과 요약, 절차 흐름도)
- 공격 단계별 상세 결과 (캡처·로그)
- 시나리오 영향도 평가 (위험등급 산정)
- 취약점 목록 및 조치 방안·권고사항

□ 시나리오 위험 등급 기준

위험 등급	판단 기준	시나리오 결과 (예시)
긴급 CRITICAL	점검 목표에 대한 완전한 침해가 가능한 경우 또는 외부 서비스를 통해 다수 고객 대상 금융계정·금전 탈취가 가능한 경우	대외 서버 장악 후 내부망 침투 및 망분리 우회, 금융망·계정관리시스템 장악, 외부 서비스 취약점을 통한 실제 금전 탈취
높음 HIGH	점검 목표에 대한 권한 확보·상승이 가능하거나 금융서비스·개인정보 대량 탈취가 가능한 경우	핵심 금융 시스템 서버·DB 장악, 대량 고객 데이터 유출, 외부 서비스 취약점을 통한 다수 고객정보 조회
중간 MEDIUM	일부 계정 침해로 제한적 접근이 가능하거나 제한된 조건에서 타인의 금융정보가 조회 가능한 경우	제한된 시스템 권한 상승 또는 획득, 외부 서비스 취약점을 통한 일부 고객정보 조회 가능
낮음 LOW	단독으로는 침투에 활용 어려우나, 다른 취약점과 연계 시 위험도 상승 가능한 경우	내부 시스템 식별자·서비스 구성 정보 노출, 금융 서비스 로직 구조 파악 가능

※ 위험 등급은 단일 취약점의 위험도가 아닌 **공격 시나리오 전체의 연계 영향도**를 기준으로 판단한다.

□ 조치 계획 수립

시나리오별 각 취약점에 대해 조치 계획을 수립하여야 한다. 조치 계획서에는 **취약점별 담당자, 조치 완료일자, 예정일자, 조치 방안** 등이 포함되어야 하며, 시나리오 위험 등급 기준을 참고하여 우선순위를 정하고 계획을 수립한다.

2 금융당국 보고

금융회사는 자사에 적용되는 관련 법률 및 감독 규정에 **보고 의무가 있는 경우**, 해당 규정에서 정하는 절차와 내용에 따라 침투테스트 이행 결과를 감독기관에 보고한다.

VI

사 후 관 리

POST-ENGAGEMENT

사후 관리는 점검 결과를 실질적인 보안 수준 향상으로 이어지게 하는 핵심 단계이다. 발견된 취약점의 단순한 조치를 넘어, 조직 전체의 **보안 아키텍처와 탐지·대응 프로세스를 근본적으로 개선**하는 것이 매우 중요하다.

1 취약점 조치 및 이행 여부 관리

금융회사는 **취약점별 조치 완료 여부**를 주기적으로 검토하고, 완료된 항목에 대해서는 **실제 조치 효과를 검증**하여야 한다.

- 시나리오에서 발견된 취약점은 **조치 계획을 수립**하여야 하며, 조치 완료 후에는 이행 점검을 통해 조치 완료 여부를 확인하되, 위험도가 높은 시나리오를 **우선 조치**
- 조치 완료된 취약점과 유사한 취약점이 타 시스템에도 존재할 가능성을 검토하여 자체 개선 및 병행 점검 실시 권고
- 조치 지연 항목에 대해서는 사유를 기록하고 경영진에 보고

2 결과 공유 및 보안 내재화

발견된 시나리오와 취약점은 단순히 해당 시스템만의 문제가 아닌 경우가 많다. 동일한 구성·설정을 공유하는 다른 시스템이나 업무 환경에서도 **유사한 취약점이 존재**할 수 있으므로, 특정 점검의 결과를 그 범위에만 국한하지 않고 **조직 전반의 관점**에서 활용하는 것이 중요하다.

이를 위해 점검 결과와 공격 시나리오, 대응 사례를 관련 부서와 **전사적으로 공유**하고, 주요 취약점과 공격 기법을 **임직원 보안 교육·인식 제고 활동**에 반영한다.

또한 동일·유사 취약점이 신규 시스템에서 재발생하지 않도록, 점검 결과를 설계·개발·구축·운영 등 정보시스템 생명주기 전반의 보안 점검 기준과 개발 표준에 반영함으로써, 일회성 조치에 그치지 않고 **보안이 조직 문화와 업무 프로세스에 내재화**되도록 한다.

내부 공유

발견된 주요 취약점 유형, 공격 흐름, 근본 원인을 보안팀·개발팀·IT 운영팀과 공유하고, 재발 방지를 위한 개발·운영 기준 개선에 반영한다.

향후 점검 계획 반영

이번 점검에서 미흡했던 사항이나 새롭게 발견된 공격 경로를 다음 침투테스트 시나리오에 반영 여부를 검토한다.

VII

결론

CONCLUSION

금융권의 사이버 위협은 갈수록 고도화되고 있어, 취약점 목록을 나열하는 수준의 점검만으로는 **실제 침해사고를 예방하는 데 한계**가 있다. 침투테스트는 금융회사가 자사의 보안체계가 **실제 공격에 얼마나 효과적으로 대응하는지**를 직접 확인하는 수단이다. 다만 이는 취약점 분석평가의 역할이 줄어든다는 의미가 아니다. **전체 자산의 보안 수준을 빠짐없이 상시 점검·관리하는 취약점 분석평가는 여전히 중요하며**, 침투테스트와 상호 보완적으로 운영될 때 금융회사의 보안 대응 능력이 완성된다.

금융회사는 침투테스트를 의무 이행 차원에서 접근하기보다, 사전준비·점검수행·결과 보고 및 사후관리의 전 과정에서 **능동적인 역할**을 수행하는 것이 중요하다. 특히 점검 결과를 **경영진의 의사결정**으로 연결하고, **정보보호 전략을 개선 및 반영**하는 것이 침투테스트의 효과를 높이는 핵심이다.

또한 침투테스트는 한 차례의 점검으로 끝나는 일회성 활동이 아니다. 정보보호 관리체계(ISMS 등)와 마찬가지로 **계획-점검-조치-개선이 반복되는 순환 체계** 안에서 운영될 때 제 효과를 발휘한다. 금융회사는 점검에서 드러난 취약점을 조치하는 데 그치지 않고, 조치 이후의 보안 수준을 유지·강화하기 위한 전략까지 세워 다음 점검에 반영함으로써 보안 역량을 꾸준히 다져 나가야 한다.

□ 침투테스트의 반복·개선 체계



⑤단계의 개선 결과가 다시 ①단계 점검 계획으로 이어지는 **반복·개선 구조**로 운영될 때, 침투테스트는 일회성 점검을 넘어 조직의 보안 수준을 꾸준히 높이는 관리 체계로 작동한다.

침투테스트 수행 합의서(RoE) 예시

침투테스트 수행 합의서

RULES OF ENGAGEMENT (RoE)

1. 개요

본 합의서는 [수행업체명](이하 "점검팀")이 [금융회사명](이하 "당사") 시스템을 대상으로 침투테스트를 수행함에 있어, 점검 권한의 범위, 제약 사항, 데이터 취급 기준 및 비상시 대응 절차를 명확히 규정함을 목적으로 한다. 본 문서는 점검팀에 합법적 점검 권한이 부여되었음을 증명하는 공식 승인 문서로서, 양측 서명으로 효력이 발생한다.

2. 수행 일정 및 시간

- 수행 기간: _____년 _____월 _____일 ~ _____년 _____월 _____일
- 점검 허용 시간대: _____ (예) 09:00~18:00
- 스캔 일정: (예) 추후 협의

3. 인력 및 비상 연락처

※ 수행 인력 명단은 운영 부서와 독립된 외부 전문 인력 또는 이해충돌이 없는 내부 전담반을 구성하여야 한다.

소속	성명	역할(Role)	직책	비상 연락처
○○은행		총괄 책임자	CISO	010-0000-0000
○○은행		실무 총괄	팀장	010-0000-0000
○○은행		실무 담당자	과장	010-0000-0000
○○○업체		수행 총괄	팀장	010-0000-0000
○○○업체		수행 책임자(PM)	수석	010-0000-0000
○○○업체		수행 담당자	책임	010-0000-0000

4. 사전 공지 사항

- (당사) 임직원 대상 사전 공지, 제공된 점검 IP에 대한 보안시스템 차단 예외 처리
- (점검팀) 점검 시작 전 내외부 관제팀에 점검 IP 공유

5. 수행 범위

· 수행 범위: IT 인프라 전체

※ 초기 정보 수집 단계에서는 IT 인프라 전체를 대상으로 하며, 이후 침투 가능성이 확인된 시스템에 한해 집중 점검을 수행한다.

· 제외 범위 (해당 없을 시 생략)

서비스	범위	제외 범위	제외 사유
HTS	hts.fsec.or.kr	스캔 제외	트레이딩 시스템 장애 우려
접근제어서버	192.168.10.121-122	점검 제외	차세대 시(3월 이후) 서비스 종료 예정

6. 수행 방식

· 점검 시나리오

구분	대상	요청 시나리오	점검 유형
종합	전체 IT 인프라	외부 → 내부 침투, 내부 → 내부 횡적 이동 등 전반적인 침투테스트	블랙박스
선택	메신저 솔루션	메신저를 통한 임직원PC 탈취 가능 여부	화이트박스 (소스코드 제공)
선택	메인 홈페이지	DMZ 서버 탈취 이후 공격으로 인한 파급력 확인	그레이박스 (웹셀 제공)

7. 수행 시 준수 사항

당사 당사는 점검 수행 기간 중 다음 사항을 준수한다.

활동 유형	상세 설명
임의 설정 강화	점검 기간 중 한시적으로 방화벽 포트 차단 또는 침입 탐지 시스템 실시간 반영 등 평시와 다른 환경으로 적용하는 행위 금지
점검 중 임시 조치	발견된 취약점을 임시 조치하여 후속 공격을 차단하는 행위 금지
점검 방해	점검에 사용되는 파일·도구를 임의로 삭제 금지 (백신·탐지 시스템 예외)
결과 임의 변경	취약점 삭제, 등급 하향, 보고서 임의 수정 등 점검 결과 왜곡 보고 금지

점검팀 점검팀은 시스템 안정성·가용성 확보를 위해 다음 사항을 준수한다.

활동 유형	상세 설명
DoS 공격	의도적인 시스템 가용성 침해 금지
데이터 파괴	운영 시스템 데이터 삭제·암호화 금지
고객 데이터 변조	실제 고객 데이터 변조 금지

※ 점검팀이 본 합의서에서 정한 범위와 절차를 준수하여 수행한 점검 활동에 대해서는 그 결과에 대한 책임을 묻지 않는다.

8. 연속성 확보(Leg-up)

점검팀은 블루팀의 탐지·차단으로 거점이 소실되거나, 시간 제약 또는 운영 안정성 등의 사유로 다음 공격 단계에 대한 검증이 곤란한 경우, 아래 요건을 충족하는 범위 내에서 정보 및 접근 권한을 요청할 수 있다.

- 시스템 설정 변경 등 운영 리스크 우려로 다음 단계 진행이 사실상 곤란한 경우
- 이미 확인된 침투 경로 및 권한 획득 가능성을 근거로 점검의 연속성 확보가 필요한 경우
- 제공 수준이 점검의 현실성을 훼손하지 않고, 충분한 시간과 자원이 있었다면 공격자가 확보할 수 있었을 것으로 합리적으로 볼 수 있는 범위인 경우

9. 장애 관리

1. **상황 인지·보고:** 이상 징후(응답 지연, 서비스 오류, 접속 불가 등) 감지 즉시 비상 연락망을 통해 상대측 책임자에게 통보
2. **점검 일시 정지:** 점검팀은 모든 공격 시나리오 및 스캔 작업 중단
3. **원인 분석·복구:** 당사는 로그·상태 분석으로 점검팀 활동 여부 판단, 점검팀은 수행 이력 및 관련 데이터 제공
4. **점검 재개 여부:** 총괄 책임자가 정상화 확인 및 장애 원인에 대한 양측 검토·합의 후에만 재개 승인

10. 복구작업(Clean-up) 수행

□ 대상

- 업로드·설치한 웹shell, 실행 파일, 스크립트
- 점검용 시스템·서비스 계정, API 키, 인증정보
- 추가·변경한 시스템 설정, 권한, 임시 정책
- 연속성 확보 제공 계정·자격증명·테스트 단말

□ 확인·종료 절차

1. 점검팀이 변경 항목 목록 제출
2. 당사 보안·운영팀이 직접 삭제·복구 수행
3. 목록 완전성·삭제 완료·권한 회수 확인 후 종료

11. 승인 및 서명

본 합의서의 내용을 충분히 숙지하였으며, 이에 따른 침투테스트 수행을 공식적으로 합의한다. 점검팀은 합의된 범위와 절차에 따라 안전하게 점검을 수행하고, 당사는 점검팀이 독립적이고 객관적으로 수행할 수 있도록 협조한다. 합의된 범위와 절차를 준수한 점검 활동에 대해서는 그 결과에 대한 책임을 묻지 않는다.

_____년 _____월 _____일

소속	직책	성명	서명
○○은행	CISO	000	
○○은행	과장	000	
○○업체	수석	000	
○○업체	책임	000	

침투테스트 수행 적정성 체크리스트

※ 본 체크리스트는 금융회사의 침투테스트 수행 적정성을 점검·평가할 때 활용하는 것을 목적으로 한다.

1. 사전준비

No	점검 항목	판단기준	판단 결과	근거
1	CISO 서명이 포함된 수행 합의서(RoE)가 존재하는가	양호 수행 합의서에 점검 범위, 금지 행위 등 주요 항목이 구체적으로 명시되어 있으며, CISO 서명이 포함된 경우 미흡 수행 합의서가 없거나, 주요 항목이 누락된 형식적 문서이거나, CISO 서명이 없는 경우	양호 / 미흡	

2. 수행 및 범위

No	점검 항목	판단기준	판단 결과	근거
2	취약점을 연계한 침투테스트 시나리오 기반으로 수행하였는가	양호 보고서에 복수의 취약점을 연계한 공격 단계 흐름이 구체적으로 기술된 경우 미흡 보고서가 취약점별 개별 항목으로만 구성되고 단계 간 연결 흐름을 설명하는 시나리오가 없거나, 수동 진단 없이 자동 스캔·AI 산출 결과에만 의존한 경우	양호 / 미흡	
3	전자금융기반시설 등 핵심·중요 서비스 및 자산을 점검 목표로 설정하였는가	양호 수행 합의서 또는 보고서에 전자금융기반시설 등 핵심·중요 서비스 및 자산이 점검 목표로 명시된 경우 미흡 점검 목표가 설정되지 않았거나, 핵심 서비스가 목표에서 누락된 경우	양호 / 미흡	

3. 결과 보고 및 사후관리

No	점검 항목	판단기준	판단 결과	근거
4	최종 보고서에 정보수집부터 목표 달성까지의 공격 경로 전체가 재현 가능한 수준으로 기술되어 있는가	양호 공격 흐름도와 단계별 화면 캡처·로그·명령어 이력이 보고서에 포함된 경우 미흡 취약점 목록만 기재되고 공격 경로 재현에 필요한 증거가 없거나, 발견된 취약점을 임의로 삭제·누락하여 보고한 경우	양호 / 미흡	
5	비즈니스 영향도(자금 탈취, 정보 유출 등) 기준으로 시나리오 위험 등급을 산정하였는가	양호 위험 등급 산정 기준이 명확히 정의되어 있으며, 해당 기준에 따라 자금 탈취·고객정보 유출·서비스 중단 등 실질적 피해를 기반으로 등급이 산정된 경우 미흡 산정 기준 없이 주관적으로 등급을 부여하거나 단순 CVSS 점수만으로 산정한 경우, 또는 실제 영향도와 다르게 위험 등급을 임의로 하향한 경우	양호 / 미흡	
6	시나리오별 취약점에 대한 조치 계획을 수립하고 경영진에 보고하였는가	양호 시나리오별 취약점에 대한 담당자·조치 방안 등이 명시된 조치 계획서가 존재하고, 경영진 보고 기록이 확인되는 경우 미흡 조치 계획서가 없거나 "검토 중" 등으로만 기재된 경우, 경영진 보고 기록이 없거나, 조치 계획에 따른 사후 조치가 이행되지 않고 재점검 기록도 없는 경우	양호 / 미흡	

금융분야 침투테스트(모의해킹) 수행 가이드라인

발행일 : 2026년 7월
발행인 : 박 상 원
발행처 : 금융보안원
경기도 용인시 수지구 대지로 132
전 화 : (02) 3495-9000

< 비 매 품 >

본 안내서 내용의 무단전재를 금하며, 가공 인용할 때에는 반드시 금융보안원 「금융분야 침투테스트(모의해킹) 수행 가이드라인」 이라고 밝혀 주시기 바랍니다.