로보어드바이저 테스트베드
시스템 보안성심사 안내

- 제2차 정기심사 -

금융보안원
FINANCIAL SECURITY INSTITUTE

로보어드바이저 시스템 보안성심사 안내

(금융보안원, 2017.3.10.)

1 심사개요

□ **(심사목표) 보안사고 예방·대응수준 확인 (상용 서비스 대비)**

□ **(심사기업) 테스트베드 참여업체 중 상용서비스 제공 예정자**

□ **(심사대상) 심사기업이 보유한 로보어드바이저 시스템 전반**

※ 알고리즘 운영 서버, DB 서버, 웹 서버, 정보보호시스템, 중요 PC 등

□ **(심사방향) 2단계 심사 (서면 및 현장), 서비스 유형별* 맞춤 점검**

* [참고1]『로보어드바이저 시스템 서비스 유형』참조

○ **(2단계 심사)** 서면심사(1단계)에서 보완사항 권고, 현장심사(2단계) 시 보안대책현황 및 보완조치 이행여부 등 점검

○ **(서비스 유형별 맞춤 점검)** 온라인에서의 고객 맞춤형 서비스* 제공유무에 따라 온라인형과 오프라인형으로 구분하여 점검 기준을 적용

* 고객이 홈페이지 등에 직접 접속하여 고객별 수익률 조회, 포트폴리오 조회 등을 제공

□ **(심사기준) 6개 분야 31개 기준***

* [참고2]『로보어드바이저 시스템 보안성심사 기준』참조

○ 온라인 서비스 제공 시 31개 기준, 미 제공시 27개 기준 점검

2 심사 절차 및 구분

□ (심사절차) 『서면 심사』 및 『현장 심사』로 구분

○ **(서면 심사)** 로보어드바이저 시스템의 보안대책 현황을 서면(보안대책명세서)으로 심사

※ **(자료제출)** 심사기업이 사무국 홈페이지로 보안대책명세서를 제출
(결과송부) 금융보안원이 서면심사 후 결과보고서를 심사기업에게 전달

○ **(현장 심사)** 시스템 운영 **현장을 방문하여 시스템 보안현황 일치성, 보완조치 이행여부 등 심사**

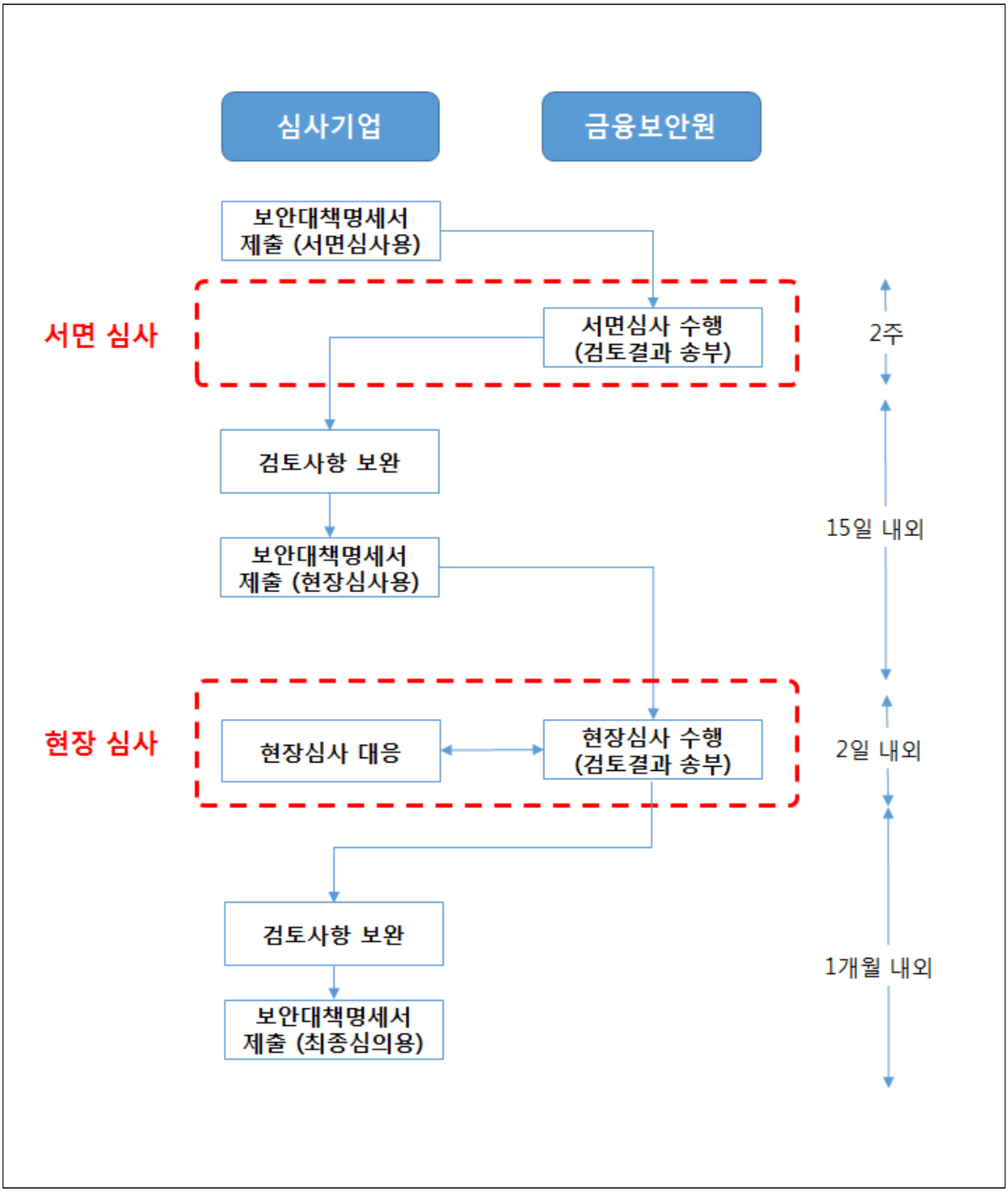
※ 최종(보완) 보안대책명세서, 보완조치의견 등을 토대로 심사진행

□ 심사기업 유형에 따른 서면·현장심사 대상 여부

심사기업유형 / 심사구분	자문일임업, 로보어드바이저 기술보유업체 (단독, 컨소시엄형)	은행 · 증권	
		단독형	컨소시엄형
서면심사	대상	대상	대상
현장심사	대상	비대상	일부대상*

* 자문일임업, 로보어드바이저 기술보유업체가 보유한 시스템은 현장심사 대상

< 참고 : 시스템 보안성심사 세부절차 >



3 제출 서류

□ **(제출서류)** 『보안대책명세서*』 (서면심사와 현장심사용 양식 동일)

※ [참고4] 『 로보어드바이저 테스트베드 보안대책명세서 샘플』 참고

○ **(구성)** 서비스 개요, 서비스 유형, 서비스 절차, 시스템 및 네트워크 구성도, 심사기준 별 보호대책

□ **(제출마감일자)**

○ **(서면심사) 심사기업 권역별로 3차에 걸쳐 마감**

- **(1차)** 은행('17.6.9.) **(2차)** 증권('17.6.23.) **(3차)** 기타('17.7.7.)

※ 마감일정은 변동가능

○ **(현장심사) 현장심사 시작 일주일 전 마감**

※ 현장심사 일정은 개별통보 예정

□ **(제출방식) 테스트베드 홈페이지에 전자파일로 업로드(hwp 등)**

4 문의

□ **(문의처) 금융보안원 핀테크보안팀**

○ **(절차) 02-3495-9623 (심사기준) 02-3495-9625**

※ 로보어드바이저 기업의 질의응답에 관한 사항은 필요한 경우 FAQ(참고3) 등으로 지속적인 안내 예정

참고 1 로보어드바이저 시스템 서비스 유형

□ 온라인 고객 맞춤형 서비스 제공 유무에 따라 『온라인형』과 『오프라인형』으로 구분

○ **(온라인형)** 고객계정을 기반으로 맞춤형 정보를 웹서비스 등 온라인으로 제공하는 경우

○ **(오프라인형)** 온라인 기반의 고객 맞춤형 서비스가 없는 경우

※ 참고 : 로보어드바이저 유형별 예시

1 온라인형

- 로보어드바이저 홈페이지 내 회원가입 후, 고객별 수익률 조회, 포트폴리오 조회 등을 제공

※ 고객이 회원가입 후 개인정보(핸드폰 번호 등), 금융정보(계좌번호 등)를 조회할 수 있는 경우에도 온라인형에 해당

2 오프라인형

- 로보어드바이저 홈페이지 내 회원가입 없이, 회사 소개, 일반적인 투자성향 분석 등의 서비스만 제공

※ 고객 맞춤형 정보(수익률 및 포트폴리오 정보 등)는 우편, 대면 등의 방식으로 제공

참고 2 로보어드바이저 시스템 보안성심사 기준

□ 시스템 보안성심사 기준

분야	심사기준	온라인형	오프라인형
1. 이용자 및 계좌 소유주 인증 (S2-01-DE)	① 이용자 인증	√	
	② 계좌 소유주 인증	√	
	③ 기록관리	√	
2. 중요정보 보호대책 (S2-02-DE)	① 기밀성 보장	√	√
	② 무결성 보장	√	√
	③ 암호화 알고리즘	√	√
3. 시스템 물리적 통제 (S2-03-DE)	① 보호구역 설정	√	√
	② 출입통제	√	√
	③ 잠금장치 보호	√	√
	④ IDC 계약사항	√	√
4. 시스템 기술적 통제 (S2-04-DE)	① 안전한 비밀번호 적용	√	√
	② 접속단말 지정	√	√
	③ 불필요 통신 및 서비스 차단	√	√
	④ 보안패치 적용	√	√
	⑤ 악성코드 대응	√	√
	⑥ 안전한 서버운영	√	√
	⑦ 정보보호시스템 취약정책 제거	√	√
	⑧ 웹 취약점 점검	√	
5. 중요 PC 통제 (S2-05-DE)	① 불필요 통신 및 프로그램 차단	√	√
	② 안전한 비밀번호 적용	√	√
	③ 보안패치 적용	√	√
	④ 악성코드 대응	√	√
	⑤ 외부반출 통제	√	√
	⑥ 보조기억매체 통제	√	√
	⑦ 중요정보 저장제한	√	√
6. 네트워크 통제 (S2-06-DE)	① 네트워크 분리	√	√
	② 구간별 접근제어	√	√
	③ 대외통신 보호	√	√
	④ 무선 네트워크 통제	√	√
	⑤ 원격통신 통제	√	√
	⑥ 내부 네트워크 통제	√	√

※ 전자금융거래법, 전자금융감독규정 등 관련 법규에 서술된 내용이 본 심사기준과 상충될 경우 관련법규의 내용이 우선되며, 로보어드바이저 서비스 특성에 따라 심사기준 적용대상 변동 가능

□ 시스템 보안성심사 기준 상세

분야	심사기준
1. 이용자 및 계좌 소유주 인증 (S2-01-DE)	**① (이용자 인증)** 이용자 인증을 위한 방법이 적정하게 설계되어 있는가? - 인증방법(패스워드, 생체인증, OTP 등) 자체의 안전성(메커니즘, 알고리즘 등)과 인증 프로세스 전반의 안전성을 함께 고려하여 설계해야 하며, 서비스 이용 시 타인의 명의를 도용할 수 없도록 대책 (특히, 휴대폰 인증의 경우 메시지 탈취, 전화번호 변조, 휴대폰 도난 등의 대책) 필요 - 인증정보 탈취를 위한 공격(세션 가로채기, 비밀번호 무작위 대입공격, 인증정보 재활용 등)에 대한 대책 필요
	② (계좌 소유주 인증) 계좌 소유주 인증을 위한 방법이 적정하게 설계되어 있는가? - 인증방법(계좌 비밀번호, 계좌 입금 금액 입력 등) 자체의 안전성 (메커니즘, 알고리즘 등)과 인증 프로세스 전반의 안전성을 함께 고려하여 설계해야 하며, 계좌 소유주 인증 시 타인의 계좌를 등록할 수 없도록 대책(특히, 휴대폰 인증의 경우 메시지 탈취, 전화번호 변조, 휴대폰 도난 등의 대책) 필요
	③ (기록관리) 인증 및 거래관련 기록(인증시도 및 결과, 접속정보 등)을 보존하고 관련기록의 변경에 대한 보호대책이 마련되어 있는가? - 인증관련 정보가 기록된 데이터베이스, 로그 등은 인가된 사용자만 접근 가능하도록 보호대책 필요
2. 중요정보 보호대책 (기밀성, 무결성) (S2-02-DE)	**① (기밀성 보장)** 중요정보(개인정보, 금융정보, 패스워드 등)는 안전하게 암호화하여 기밀성을 보장할 수 있도록 설계되어 있는가? - 시스템 내에서 처리되는 기밀성이 요구되는 중요정보(개인정보, 금융정보, 패스워드 등)는 기밀성 유지를 위해 암호화 필요
	② (무결성 보장) 중요정보(운용지시 등)는 위변조 여부 등 무결성을 검증할 수 있도록 설계되어 있는가? - 시스템 내에서 처리되는 무결성이 요구되는 중요정보(운용지시 등)는 무결성을 검증할 수 있도록 대책 필요(암호화, 체크섬 등)

분야	심사기준
	③ **(암호화 알고리즘)** S2-02-DE ①, ②에 적용된 암호화 알고리즘은 국내외 전문기관(NIST, KISA 등)에서 권고한 암호화 알고리즘 및 키길이를 사용하고 안전하게 관리되고 있는가? - 암호화 연산은 112비트 이상의 보안강도를 갖는 암호알고리즘 및 암호키 길이 적용 필요 ※ 국내에서 권고하는 112비트 이상의 보안강도를 갖는 암호알고리즘의 목록은 '암호 알고리즘 및 키 길이 이용 안내서(KISA)' 참조 - 암호키는 생성, 분배, 접근, 파기 전반에 걸쳐 안전하게 관리될 수 있도록 절차가 필요하며, 필요 시 암호키 관리를 위한 안전한 물리적 관리적 절차(HSM, 잠금장치가 있는 금고 등) 필요
	* 고려사항 : 관련 법령(개인정보보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 전자금융거래법 등)의 준수여부는 심사기준서 제외
3. 시스템 물리적 통제 (S2-03-DE)	① **(보호구역 설정)** 전산설비에 대한 보호구역 설정이 되어있는가? - 전산설비 설치장소를 보호구역으로 설정하고, 보호구역 내 작업(시스템 유지보수, 시스템 도입 등)이 필요한 경우 작업기록을 관리하며, 보호구역 반출 및 반입 내역 관리 필요
	② **(출입통제)** 전산설비에 대한 출입통제대책(카드키 혹은 지문인식 등)이 수립되어 있는가? - 사전 인가자 인증을 위한 대책(카드키 혹은 지문인식 등)이 마련되어 있어야 하며, 사전 인가자 외 인원은 책임자의 승인을 받아 출입하며(내부 담당자 동행) 출입자 관리기록부에 기록(신원, 방문목적, 방문일시 등) 필요
	③ **(잠금장치 보호)** 중요서버는 잠금장치로 보호되어 있는가? - 중요 서버는 잠금장치로 보호되어 해당 서버 관리자만 접근할 수 있도록 대책 필요. 단, 출입통제대책이 마련된 전산실에 관리자만 출입할 수 있는 경우에는 제외

분야	심사기준
	④ **(IDC 계약사항)** 전산설비를 클라우드 및 IDC에 위탁 운영하는 경우, S2-03-DE ①~③기준에 대한 물리적 통제 관련 요구사항을 계약서에 반영하고 운영상태를 주기적으로 검토하고 있는가? - S2-03-DE ①~③기준에 대한 시스템 물리적 보안요구사항을 위탁운영기관과의 계약서에 반영 필요. 다만 위탁운영기관이 정보보호 인증서(ISMS, ISO 27001, 클라우드 보안인증제도 등 관련 인증서 中1개 이상)를 보유하고 위탁전산설비가 해당 인증서 범위 내에 포함되는 경우 계약서 반영사항을 인증서로 갈음
4. 시스템 기술적 통제 (S2-04-DE)	① **(안전한 비밀번호 적용)** 중요서버에 접근하는 계정은 안전한 비밀번호를 사용하도록 설정 및 적용되고 있는가? - 중요서버에 접근하는 계정 중 root계정은 원격 접속을 제한하여야 하며, 패스워드는 적절한 조합규칙(아이디, 생년월일, 주민번호 등을 포함하지 않은 영문자, 특수문자, 숫자를 혼합한 8자리 이상)으로 설정하고, 분기별 1회 이상 변경, 보관 시 암호화, 시스템마다 관리자 비밀번호가 다르게 지정, 비밀번호 연속오류에 대한 대응 등 필요
	② **(접속단말 지정)** 중요서버에 대한 접근은 중요PC 및 지정된 서버 등에 대해서만 허용하고 있는가? - 중요서버에 접근하는 단말(중요PC 및 지정된 서버)이 중요서버와 다른 네트워크 구간에 위치하는 경우, 침입차단시스템 등의 접근제어를 통해 해당 단말로부터 중요서버의 특정포트로만 통신할 수 있도록 설정 필요
	③ **(불필요 통신 및 서비스 차단)** 중요서버는 업무상의 용도를 제외하고 외부통신망(인터넷 등)의 연결 및 불필요한 서비스가 차단되어 있는가? - 기본적으로 외부통신망과 연결이 차단되어있어야 하며, 중요 PC 및 서버 등이 외부에 있어 부득이하게 통신해야할 경우 침입차단시스템 등의 접근통제 방안이 적용 필요. 서버 내 불필요한 서비스(Finger서비스, r계열서비스, NFS서비스, tftp서비스 등)가 열려 있지 않도록 설정 필요 ※ 불필요한 서비스를 해제하는 방법은 '주요정보통신기반시설 취약점 분석·평가 방법 상세가이드(KISA)' 참조
	④ **(보안패치 적용)** 중요서버에 대해 최신보안패치를 적용하고 있는가? - 중요서버에 적용할 패치의 중요도에 따라 긴급하고 중요한 패치의 경우 즉시, 보통레벨의 패치 사항의 경우 일정기간 내 적용할 수 있도록 관련 절차 필요

분야	심사기준
	⑤ **(악성코드 대응)** 중요서버에 대해 악성코드 대응 방안을 적용하고 있는가? - 중요서버에 악성코드탐지 프로그램을 설치하고 정기적으로 악성코드탐지 프로그램을 업데이트 하며 실시간 검사가 이뤄질 수 있도록 설정필요. 단, UNIX계열의 서버는 제외
	⑥ **(안전한 서버운영)** 중요서버는 독립서버로 운영하고, 정보보안시스템(차단시스템 등)을 적용하여 보호하고 있는가? - 시스템 용도(웹/WAS, 어플리케이션, DB 등)별로 독립된 서버의 운영이 필요하며 서버 가상화(가상머신 등)를 이용하는 경우 별도의 보호대책 필요 (예: 가상머신별 접근관리, 데이터 분리 및 보호, 하이퍼바이저와 가상머신사이의 인터페이스 취약점에 대한 보호대책 수립 등)
	⑦ **(정보보호시스템 취약정책 제거)** 정보보호시스템(침입차단시스템 등)내 취약한 정책이 존재하지 않는가? - 기본적으로 All Deny정책이 적용되어 있고, 접근이 필요한 최소한의 서비스만 허용되어 있어야 하며, 취약한 정책(네트워크IP주소 단위로 허용된 정책, 출발지 포트 기반의 정책, 양방향으로 설정된 정책 등)이 없는지 주기적으로 확인 필요.
	⑧ **(웹 취약점 점검)** 인터넷에 공개된 웹 서버에 대해 웹 취약점 점검을 수행하였는가? - 자체 혹은 외부기관에서 점검한 수행결과 및 조치계획서 첨부
	* 고려사항 : 중요서버는 중요도를 고려하여 사전 지정 필수(예: DB, 웹 등)
5. 중요 PC 통제 (S2-05-DE)	① **(불필요 통신 및 프로그램 차단)** 중요PC(관리자 PC, 개발 PC 등)는 업무상의 용도를 제외하고 외부통신망(인터넷 등)의 연결 및 불필요한 프로그램이 설치되어 있는가? - 중요PC는 외부통신망과 물리적 혹은 논리적 망분리가 적용되어야 하며, 불필요한 프로그램(상용 메신저 등)의 제거 필요
	② **(안전한 비밀번호 적용)** 중요PC에 대한 계정은 안전한 비밀번호를 사용하도록 설정 및 적용되고 있는가?

분야	심사기준
	- 패스워드는 적절한 조합규칙(아이디, 생년월일, 주민번호 등을 포함하지 않은 영문자, 특수문자, 숫자를 혼합한 8자리 이상)으로 설정하고, 분기별 1회 이상 변경, 보관시 암호화 등 필요
	③ **(보안패치 적용)** 중요PC에 대해 최신보안패치를 적용하고 있는가? - 중요PC는 HOT Fix등 최신보안패치를 적용하며, 설치된 응용 프로그램(한글, MS-Office, 어도브 아크로뱃 등)에 대해 정기적으로 패치할 수 있도록 관련 절차 필요
	④ **(악성코드 대응)** 중요PC에 대해 악성코드 대응 방안을 적용하고 있는가? - 중요서버에 악성코드탐지 프로그램을 설치하고 정기적으로 악성코드탐지 프로그램을 업데이트 하며, 실시간 검사 및 OS에서 제공하는 침입차단 기능 활성화 필요
	⑤ **(외부반출 통제)** 중요PC에 대해 외부반출을 통제하고 있는가? - 중요PC는 원칙적으로 외부로 반출하지 않도록 통제하여야 하며, 외부반출 시 중요서버에 접근금지 및 중요데이터 삭제 등의 조치 필요
	⑥ **(보조기억매체 통제)** 중요PC에서 보조기억매체 및 휴대용전산장비에 접근하는 것을 통제하고 있는가? - 중요PC의 보조기억매체 및 휴대용전산장비 접근은 원칙적으로 금지하나, 필요가 불가피한 경우 별도의 보호대책 마련 필요 (예: 악성코드탐지, 접근관리대장 관리, 관리자 통제 하에서만 사용 등)
	⑦ **(중요정보 저장제한)** 비중요 PC 내에 중요정보(개인정보, 암호키 등) 저장을 제한하고 있는가? - 주기적으로 비중요 PC내에 중요정보가 저장되어 있는지 여부를 확인할 수 있는 관련 절차 필요
	* 고려사항 : 중요PC 사전 지정 필수 (예: 중요서버에 접근 가능한 PC, 개인정보를 취급하는 PC 등)
6. 네트워크 통제	① **(네트워크 분리)** 시스템 용도(웹, DB 등)에 따라 네트워크 구간이 분리되어 있는가?

분야	심사기준
(S2-06-DE)	- 웹, DB 등 시스템 용도별로 네트워크를 분리하여야 하며, 네트워크 가상화(가상 스위치 등)를 이용하는 경우 별도의 보호대책 필요 (예: 가상 스위치별 VLAN설정 등)
	② **(구간별 접근제어)** 네트워크 구간별로 접근제어가 설정되어 있는가? - 웹은 DMZ, DB는 내부망 등 네트워크 구간별로 허용 IP 및 포트를 관리를 통해 접근제어 필요
	③ **(대외통신 보호)** 대외기관(금융회사 등)과의 통신 시 보안통신(전용회선 혹은 VPN 등)이 적용되어 있는가? - 대외기관과의 통신 시에는 전용회선 혹은 VPN을 사용하여야 하나, 전송계층에서의 보안통신(SSL등)을 사용하여야할 경우 해당 별도의 보호대책 필요 (예 : 취약한 버전의 SSL 프로토콜 사용 금지 등) - 단, 대외기관과 HTS 등 별도의 통신프로토콜을 사용하여야 하는 경우, 정해진 프로토콜 내에서 중요정보가 암호화되어 전송되도록 보호대책 필요
	④ **(무선네트워크 통제)** 무선네트워크는 통제 하에 이용을 최소화하며, 이용 시 보호대책을 적용하였는가? - 무선네트워크 이용 시 SSID는 hidden, 암호정책은 WPA이상, MAC필터링 적용, 중요서버가 위치한 네트워크에서는 사용금지 확인
	⑤ **(원격통신 통제)** 중요서버 원격 통신 시 보안통신(전용회선 혹은 VPN 등)이 적용되어 있는가? - IDC 및 클라우드 등에 위치한 중요서버와의 원격 통신 시 전용회선 혹은 VPN(SSH등 포함) 사용 여부 확인
	⑥ **(내부 네트워크 통제)** 인가된 사용자만이 중요서버가 위치한 네트워크에 접근할 수 있도록 통제하고 있는가? - 내부망에 접근가능한 네트워크장비(스위치, 라우터, VPN 등)에 비인가자가 접근할 수 없도록 물리적, 관리적, 혹은 기술적 통제 필요 (예: 네트워크 포트에 접근할 수 없도록 포트잠금장치 설치, 인가된 사용자만 네트워크 식별자(IP 등)할당 등)

참고 3 자주하는 질문(FAQ)

Q1) 단독, 컨소시엄 두 가지 방식으로 신청하려 합니다. 시스템 보안성심사를 두 번 받아야 하나요?

⇒ 원칙적으로 각각 시스템 보안성심사를 받아야 하며, 시스템 및 네트워크의 구성이 동일한 경우에는 한번으로 갈음할 수 있습니다.

Q2) 로보어드바이저 시스템을 자체전산설비가 아닌 클라우드, IDC 등 외부환경에 운영 중입니다. 현장심사(2단계)는 어떻게 하게 되나요?

⇒ 서비스제공자(클라우드, IDC 등)와 로보어드바이저 기업 간 계약서 및 서비스제공자의 관련인증서 보유여부 등을 종합적으로 고려하여 일부 심사기준은 서면심사(1단계)로 갈음할 수 있습니다.

Q3) 시스템 보안성심사 시 서면심사(1단계)는 필수인가요?

⇒ 서면심사(1단계)는 사전에 보안 취약점을 점검하여 로보어드바이저 기업이 보완할 수 있도록 함으로써 로보어드바이저 기업의 현장심사(2단계)를 지원하는 목적으로 필수입니다.

Q4) 보안시스템 구축에 필요한 예산은 대략 얼마인가요?

⇒ 보안시스템 구축 시 예산에 관한 사항은 금융보안원의 보안성심사와 관련이 없습니다.

Q5) 온라인 및 오프라인 형을 구분하는 기준은 어떻게 됩니까?

⇒ 웹 서비스 상에서 고객 계정을 기반으로 고객 맞춤형 정보를 제공하는 경우가 온라인에 해당됩니다.

Q6) IDC 및 클라우드서비스 이용 시 시스템 물리적 통제 요구사항 대해 어떻게 증빙자료를 제출해야하나요?

⇒ IDC 및 클라우드에서 물리적 통제를 위해 마련한 보안대책을 증빙할 수 있다면 어떤 형식(계약서, 홈페이지, 이메일 등)의 증빙자료이던 괜찮습니다. 만일 ISO 27001과 같은 인증서 보유 시 해당 인증서로도 갈음할 수 있습니다.

Q7) 기존 인터넷뱅킹을 이용한 고객을 대상으로 상품을 추천하는 경우, '온라인형' 인가요 '오프라인형' 인가요?

⇒ '온라인' 형이며, 이때 사용자인증 및 계좌소유주인증의 증빙자료는 기존 사용자인증방식(공인인증서 등)을 기술함으로써 갈음할 수 있습니다.

Q8) 기존 금융회사 내부의 보안성심사를 받은 시스템을 대부분 이용하는데, 이때에도 해당 시스템에 대한 심사자료를 제출해야하나요?

⇒ 기본적으로 심사자료는 제출해야하며, 편의에 따라 자체보안성 심사를 받은 자료를 첨부하고, 심사기준별로 해당되는 부분을 표기하여 제출해 주시면 됩니다.

Q9) 금융회사 내부의 모든 시스템에 대해 시스템 및 네트워크 구성도를 작성해야하나요?

⇒ 로보어드바이저와 관계된 서버(운용지시 서버 등)를 중심으로 해당 서버가 어떻게 보호되고 있는지 알 수 있도록 시스템 및 네트워크 구성도를 작성하시면 됩니다.

Q10) 금융회사가 자문·일임업 및 로보어드바이저 기술보유업체(이하 핀테크 업체)와 컨소시엄으로 참여하려 합니다. 현장심사(2단계)는 어떤 경우에 받아야 하나요?

⇒ 핀테크 업체가 금융회사 밖에서 별도의 시스템을 운영하는 경우 핀테크 업체가 운영하는 시스템은 현장심사를 받으셔야 합니다.

참고 4 로보어드바이저 테스트베드 보안대책명세서 샘플

보안대책명세서

심사기업 : ○○○○

[심사알고리즘 : ○○○○**]**

1. 서비스 개요

○ 서비스 명

— ABC 로보어드바이저

○ 서비스 특징

— 고객의 일임동의를 얻은 후, 펀드 및 주식을 운용자산으로 하여 고객의 자산을 운용하는 서비스로 고객은 홈페이지 회원가입 후 매매내역 및 수익률 등을 조회할 수 있으며, 필요시 포트폴리오 구성을 다시 할 수 있도록 지시할 수 있다.

2. 서비스 유형

○ 온라인형 *(오프라인형인 경우에는 '오프라인'으로 표시)*

— 서버 운영 형태 : IDC위탁 (위탁 업체명 : XYZ)

— 고객 맞춤형 서비스 종류 : 회원가입, 수익률 및 포트폴리오 조회

○ 컨소시엄형 *(단독형인 경우에는 '단독형'으로 표시)*

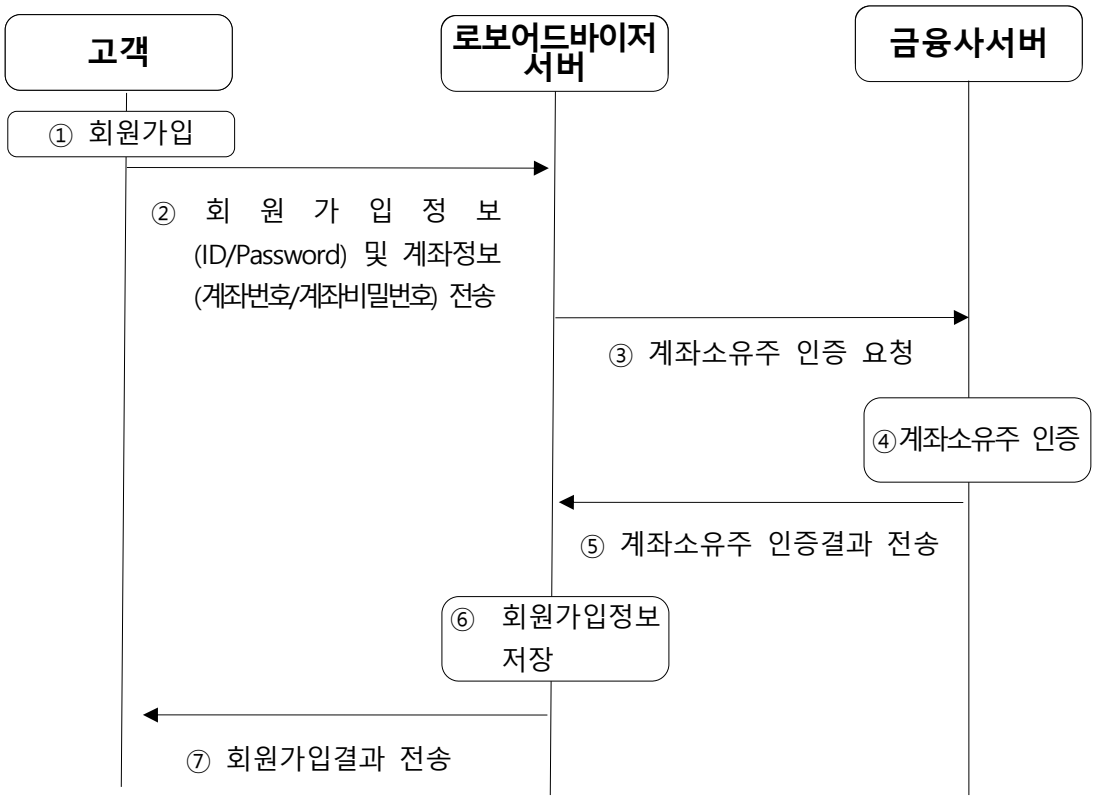
— ○○금융사 : 고객정보 제공 및 운용지시

— ○○자문사 : 포트폴리오 제공
(시스템 위치 : 금융회사 내부)
(금융회사 외부에 위치한 경우에는 '외부'로 표시)

3. 서비스 절차

○ 회원가입 *(모든 서비스 절차(포트폴리오 제공, 운용지시 등)에 대해 기술)*

— 서비스 프로세스



절차	상세 내용	비고
① 회원가입	- 고객이 로보어드바이저 홈페이지를 방문하여 회원가입 진행	
② 회원가입정보 및 계좌정보 전송	- Password는 고객 입력부터 로보어드바이저 서버까지 E2E암호화 솔루션을 적용하여 전송 - 계좌정보는 고객 입력부터 금융사서버까지 E2E암호화 솔루션을 적용하여 전송	적용한 E2E암호화 제품은 ABC사의 DEF 임
③ 계좌 소유주 인증 요청	- 로보어드바이저 서버는 E2E암호화한 계좌정보를 금융사서버로 전달	

절차	상세 내용	비고
④ 계좌 소유주 인증	- 금융사서버는 E2E암호화된 계좌정보를 복호화하여 원장에 기록된 계좌정보와의 일치여부 확인	
⑤ 계좌 소유주 인증결과 전송	- 계좌소유주 인증결과를 로보어드바이저 서버로 전달	
⑥ 회원가입정보 저장	- 로보어드바이저 서버는 계좌소유주 인증을 통과한 고객에 한하여 회원 ID 및 단방향으로 암호화한 Password를 저장	단방향 암호화는 SHA-256 이용
⑦ 회원가입결과 전송	- 금융사 서버는 회원가입 여부를 고객에게 전송	

— 화면정의서

//회원가입화면

— 주요 보호정보 및 보호방안

주요 보호정보	보호방안
계좌정보	- 계좌정보는 입력부터 전송 및 처리완료시점까지 E2E암호화 적용 - 입력시 가상키패드 활용
회원 Password	- Password는 입력부터 전송 및 처리완료시점까지 E2E암호화 적용 - Password는 8자리이상 문자, 숫자 및 특수문자를 포함하도록 설정 - 주기적으로 Password를 변경할 수 있도록 관리

○ 포트폴리오 제공

(회원가입과 동일한 방식으로 기술하며, 특히 고객, 로보어드바이저 서버, 금융사 서버간 주고받는 중요정보의 처리, 저장, 전송 내역은 반드시 포함)

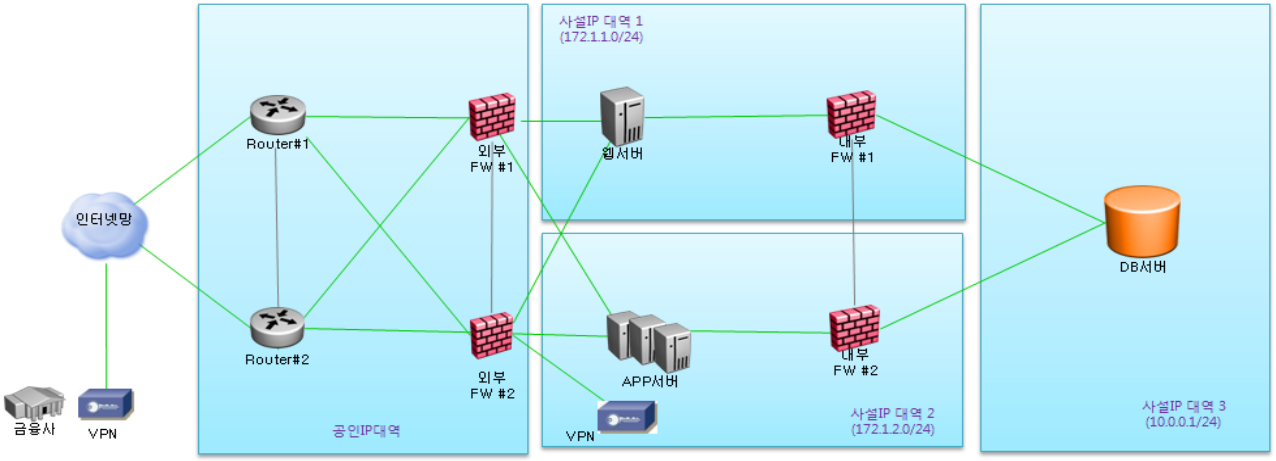
○ 운용지시

(회원가입과 동일한 방식으로 기술하며, 특히 고객, 로보어드바이저 서버, 금융사 서버간 주고받는 중요정보의 처리, 저장, 전송 내역은 반드시 포함)

4. 시스템 및 네트워크 구성도

(중요서버 리스트 및 각각의 역할을 기술하고, 중요서버에서 처리되는 중요정보, 중요서버 보호를 위한 보호조치(정보보호시스템, 네트워크 통제사항 등) 표기)

(컨소시엄 형태로 한 개 이상의 사이트에서 시스템 운영 시 각 사이트별로 시스템 및 네트워크 구성도 표기)



중요서버	역할	중요 처리정보	보호조치
웹서버	– 회원 로그인 – 수익률 조회	– 인증정보 – 개인정보 – 금융정보	– 방화벽 적용 – 최신 보안패치, 악성코드 탐지프로그램 적용 – 인터넷 차단 및 불필요한 통신포트 차단
APP서버	– 시세정보 수집 – 로보어드바이저 알고리즘 엔진 탑재 – 매매지시	– 개인정보 – 금융정보 – 운용지시	– 방화벽 적용 – 최신 보안패치, 악성코드 탐지프로그램 적용 – 금융사 통신시 VPN이용 – 인터넷 차단 및 불필요한 통신포트 차단
DB서버	– 데이터 저장	– 개인정보 – 금융정보 – 인증정보	– 2중 방화벽 적용 – 최신 보안패치, 악성코드 탐지프로그램 적용 – 인터넷 차단 및 불필요한 통신포트 차단

5. 심사기준 별 보호대책

○ 검토결과 요약

(단위 : 개)

총 심사기준	적합(예)	부적합(아니오)	N/A*
31	31	0	0

* N/A : 로보어드바이저 유형이 심사기준에 부합하지 않는 경우 N/A처리가능

○ 상세 검토내역

분야	심사 번호	심사기준	확인결과	증적자료*
이용자 및 계좌소유주 인증	S2-01-DE	① 이용자 인증 방법이 적정하게 설계되어 있는가?	□예 □아니오 □N/A	
		② 계좌 소유주 인증 방법이 적정하게 설계되어 있는가?	□예 □아니오 □N/A	
		③ 인증 및 거래관련 기록(인증시도 및 결과, 접속정보 등)을 보존하고 관련기록의 변경에 대한 보호대책이 마련되어 있는가?	□예 □아니오 □N/A	
중요정보 보호대책	S2-02-DE	① 중요정보(개인정보, 금융정보, 패스워드 등)는 안전하게 암호화하여 기밀성을 보장할 수 있도록 설계되어 있는가?	□예 □아니오 □N/A	
		② 중요정보(운용지시 등)는 위변조 여부 등 무결성을 검증할 수 있도록 설계되어 있는가?	□예 □아니오 □N/A	
		③ S2-02-DE ①, ②에 적용된 암호화 알고리즘은 국내외 전문기관(NIST, KISA 등)에서 권고한 암호화 알고리즘 및 키길이를 사용하고 안전하게 관리되고 있는가?	□예 □아니오 □N/A	

분야	심사 번호	심사기준	확인결과	증적자료*
시스템 물리적통제	S2-03-SE	① 전산설비에 대한 보호구역 설정이 되어 있는가?	□예 □아니오 □N/A	
		② 전산설비에 대한 출입통제대책(카드키 혹은 지문인식 등)이 수립되어 있는가?	□예 □아니오 □N/A	
		③ 중요서버는 잠금장치로 보호되어 있는가?	□예 □아니오 □N/A	
		④ 전산설비를 클라우드 및 IDC에 위탁 운영하는 경우, S2-03-SE ①~③기준에 대한 물리적 통제 관련 요구사항을 계약서에 반영하고 운영상태를 주기적으로 검토하고 있는가?	□예 □아니오 □N/A	
시스템 기술적통제	S2-04-SE	① 중요서버(중요도를 고려하여 사전 지정 필수(예: DB, 웹 등))에 접근하는 계정은 안전한 비밀번호를 사용하도록 설정 및 적용되고 있는가?	□예 □아니오 □N/A	
		② 중요서버에 대한 접근은 중요PC 및 지정된 서버 등에 대해서만 허용하고 있는가?	□예 □아니오 □N/A	
		③ 중요서버는 업무상의 용도를 제외하고 외부통신망(인터넷 등)의 연결 및 불필요한 서비스가 차단되어 있는가?	□예 □아니오 □N/A	
		④ 중요서버에 대해 최신보안패치를 적용하고 있는가?	□예 □아니오 □N/A	
		⑤ 중요서버에 대해 악성코드 대응 방안을 적용하고 있는가?	□예 □아니오 □N/A	
		⑥ 중요서버는 독립서버로 운영하고, 정보보안 시스템(차단시스템 등)을 적용하여 보호하고 있는가?	□예 □아니오 □N/A	
		⑦ 정보보호시스템(침입차단시스템 등)내 취약한 정책이 존재하지 않는가?	□예 □아니오 □N/A	
		⑧ 인터넷에 공개된 웹 서버에 대해 웹 취약점 점검을 수행하였는가?	□예 □아니오 □N/A	

분야	심사 번호	심사기준	확인결과	증적자료*
중요PC 통제	S2-05-SE	① 중요PC(관리자 PC, 개발 PC 등)는 업무상의 용도를 제외하고 외부통신망(인터넷 등)의 연결이 차단되고 및 불필요한 프로그램이 제거되어 있는가?	□예 □아니오 □N/A	
		② 중요PC에 대한 계정은 안전한 비밀번호를 사용하도록 설정 및 적용되고 있는가?	□예 □아니오 □N/A	
		③ 중요PC에 대해 최신보안패치를 적용하고 있는가?	□예 □아니오 □N/A	
		④ 중요PC에 대해 악성코드 대응 방안을 적용하고 있는가?	□예 □아니오 □N/A	
		⑤ 중요PC에 대해 외부반출을 통제하고 있는가?	□예 □아니오 □N/A	
		⑥ 중요PC에서 보조기억매체 및 휴대용전산장비에 접근하는 것을 통제하고 있는가?	□예 □아니오 □N/A	
		⑦ 비중요 PC 내에 중요정보(개인정보, 암호키 등) 저장을 제한하고 있는가?	□예 □아니오 □N/A	
네트워크 통제	S2-06-SE	① 시스템 용도(웹, DB 등)에 따라 네트워크 구간이 분리되어 있는가?	□예 □아니오 □N/A	
		② 네트워크 구간별로 접근제어가 설정되어 있는가?	□예 □아니오 □N/A	
		③ 대외기관(금융회사 등)과의 통신 시 보안통신(전용회선 혹은 VPN 등)이 적용되어 있는가?	□예 □아니오 □N/A	
		④ 무선네트워크는 통제 하에 이용을 최소화하며, 이용 시 보호대책을 적용하였는가?	□예 □아니오 □N/A	
		⑤ 중요서버 원격 통신 시 보안통신(전용회선 혹은 VPN 등)이 적용되어 있는가?	□예 □아니오 □N/A	
		⑥ 인가된 사용자만이 중요서버가 위치한 네트워크에 접근할 수 있도록 통제하고 있는가?	□예 □아니오 □N/A	

* 증적자료는 표 안에 입력하거나, 자유형식으로 별도 첨부 가능

증적자료 작성 시 고려사항

① **(보안대책 기술)** 각 기준별로 보안대책을 **육하원칙으로 상세히 기재**

※「시스템 보안성심사 기준 상세」(p7 ~ 12)를 참고하여 **각 세부심사기준에 보안대책이 어떻게 부합하는지를 기술**

확인결과에 **'예'**를 선택하지 않은 경우 **미선택의 사유를 반드시 작성**

② **(객관적 증빙자료 첨부)** 기술한 내용을 객관적으로 증빙할 수 있는 자료를 첨부

※ (증빙자료의 예) 스크린 샷, 소스코드 일부발췌, 심사기준을 만족하는 내용이 포함되어있는 운영기록(증적자료)의 제목(파일명), 관련 증적이 시스템으로 관리되는 경우 해당 시스템 위치, 시스템명 등

※ 심사기준별 증적자료 작성 예시

[심사기준]
1.1 (이용자 인증) 이용자 인증을 위한 방법이 적정하게 설계되어 있는가?

- 인증방법(패스워드, 생체인증, OTP 등) 자체의 안전성(메커니즘, 알고리즘 등)과 인증 프로세스 전반의 안전성을 함께 고려하여 설계해야 하며, 서비스 이용 시 타인의 명의를 도용할 수 없도록 대책 (특히, 휴대폰 인증의 경우 메시지 탈취, 전화번호 변조, 휴대폰 도난 등의 대책) 필요
- 인증정보 탈취를 위한 공격(세션 가로채기, 비밀번호 무작위 대입공격, 인증정보 재활용 등)에 대한 대책 필요

[증적자료]

(보안대책) 사용자 인증을 위해 패스워드인증 및 구글에서 지원하는 OTP인증을 사용하고 있으며, 패스워드의 경우 8자리 이상(특수문자, 영문, 숫자 혼합)을 요구하고 있음. 비밀번호 탈취공격을 막기 위해, 패스워드 및 OTP입력부터 검증까지 모든 과정을 세션으로 관리하고 있으며, 세션 유효시간을 30분으로 한정하고 있음. 또한 5회 이상 패스워드 및 OTP인증이 틀릴 경우, 사용자의 웹서비스 이용을 차단

(증빙자료)

패스워드 인증화면	OTP사용화면