로보어드바이저 시스템 보안성심사

2017. 3. 10.

금융보안원
FINANCIAL SECURITY INSTITUTE

시스템 보안성심사 개요 (1/3)

(심사기업) 테스트베드 참여업체 중 상용서비스 제공 예정자

(심사대상) 심사기업이 보유한 로보어드바이저 시스템 전반

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

(심사목표) 보안사고 예방·대응수준 확인 (상용 서비스 대비)

시스템 보안성심사 개요 (2/3)

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

- **서면심사(1단계)** **서면기반** 심사 후 보완사항 권고
- **현장심사(2단계)** 보안대책현황 및 보완조치 이행여부 등 **현장점검**

- **(서비스 유형 별 점검)** 온라인에서의 고객 맞춤형 서비스 제공유무에 따라 온라인 형과 오프라인 형으로 구분하여 점검항목을 적용

※ 온라인 형 : 고객이 홈페이지 등에 직접 접속하여 고객별 수익률 조회, 포트폴리오 조회 등을 제공

시스템 보안성심사 개요 (3/3)

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**

시스템 보안성심사 서류제출 마감기간

- **(제출서류)** 보안대책명세서 (서면심사와 현장심사용 양식 동일)
- **(서면심사)** 심사기업 권역별로 3차에 걸쳐 마감

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

  ※ 마감일정은 변동 가능하며 각 심사기업의 심사 소요기간은 2주 예상
- **(현장심사) 현장심사 시작 일주일 전 마감**

  ※ 현장심사일정은 개별통보 예정이며 각 심사기업의 심사 소요기간은 2일 예상
- **(제출방식) 테스트배드 홈페이지에 전자파일로 업로드(hwp 등)**

  ※ 각 심사대상기관의 보완조치는 **현장심사 이후 15일 까지** 제출

서면심사 (1단계)

- **(심사내용)** 심사대상 기업이 제출한 **서면자료를 기반**으로 심사대상의 서비스 분석 및 점검항목을 검토
- **(심사기준)** 6개 분야 31개 기준
- **(소요시간)** 심사대상 당 2주 소요 예상
- **(심사결과)** 서면심사 완료 후 즉시 참여기업에 송부

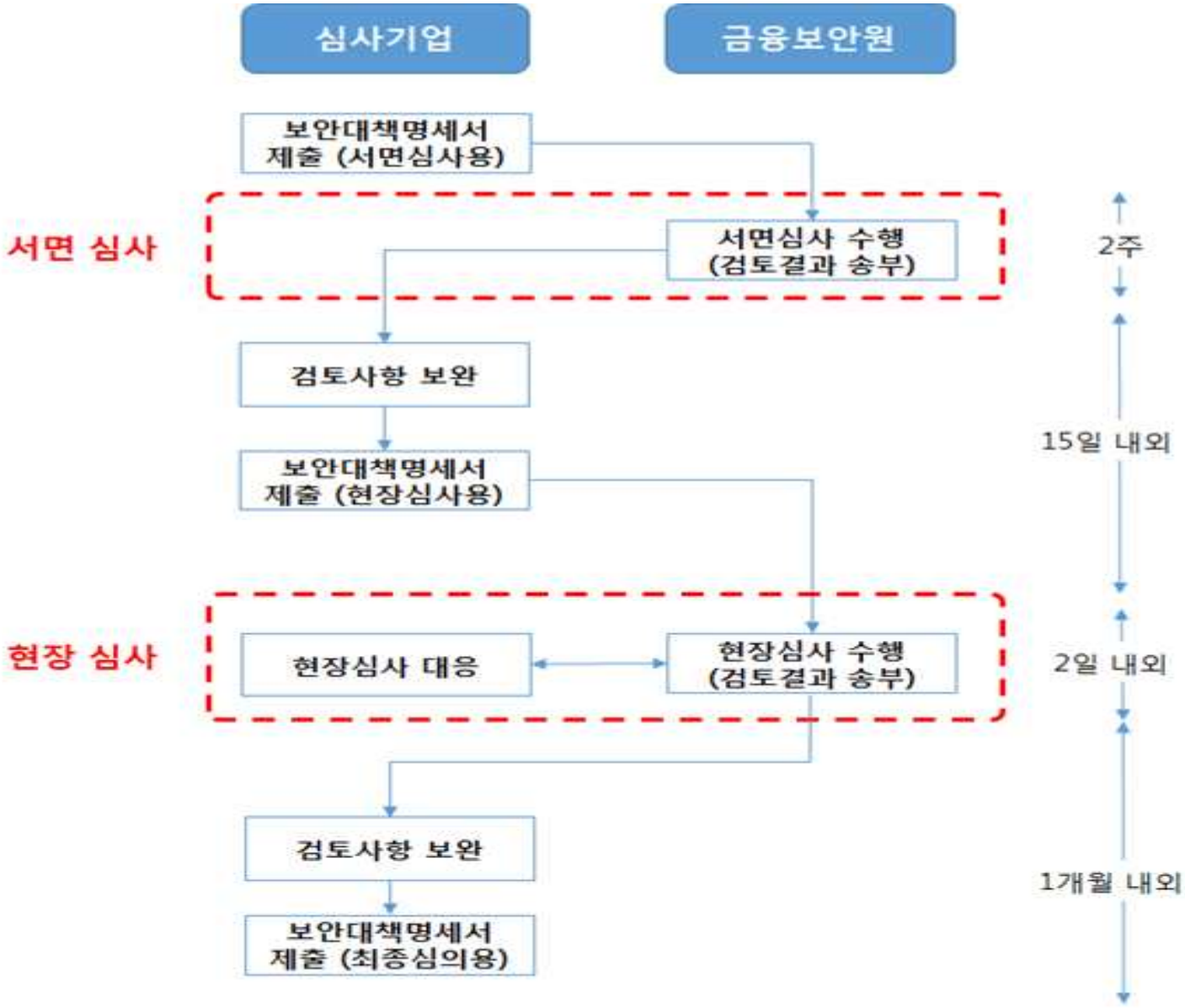
※ 결과보고서에 적시된 미비사항 보완가능 시기는 현장심사 시작 일주일 전까지로 하며, 현장심사 기간은 별도 통지

현장심사 (2단계)

- **(심사내용)** 서면심사 후 보완조치 적용여부 및 자체점검 이행여부를 심사대상 현장에 방문하여 검토
- **(소요시간)** 심사대상 당 2일 소요 예상
- **(심사일정)** 심사기간은 유동적으로 별도 통지

※ 각 심사대상기관의 보완조치는 **현장심사 이후 15일 까지** 제출

시스템 보안성심사 세부절차



심사항목

(심사항목) 6개 분야 31개 항목 내외 점검

- 온라인 고객 서비스 제공 시 31개 항목, 미 제공 시 27개 항목 점검

온라인 고객 서비스 제공(온라인형)	온라인 고객 서비스 미 제공(오프라인형)
• 고객계정을 기반으로 맞춤형 정보를 웹 서비스 등 온라인으로 제공하는 경우 * 해당사례 : 로보어드바이저 홈페이지 내 회원가입 후, 고객별 수익률 조회, 포트폴리오 조회 등 제공 ※ 고객이 회원가입 후 개인정보(핸드폰번호등), 금융정보(계좌번호 등)를 조회할 수 있는 경우에도 온라인형에 해당	• 온라인 기반의 고객 맞춤형 서비스가 없는 경우 * 해당사례 : 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

보안대책명세서 작성샘플

1. 서비스개요

○ 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.

보안대책명세서 작성샘플

2. 서비스유형

○ **온라인형** (오프라인형인 경우에는 '**오프라인**'으로 표시)

- 서버 운영 형태 : IDC위탁 (위탁 업체명 : XYZ)
- 고객 맞춤형 서비스 종류 : 회원가입, 수익률 및 거래내역 조회, 운용지시

○ **컨소시엄형** (단독형인 경우에는 '**단독형**'으로 표시)

- ○○금융사 : 고객정보 제공 및 운용지시
- ○○자문사 : 포트폴리오 제공

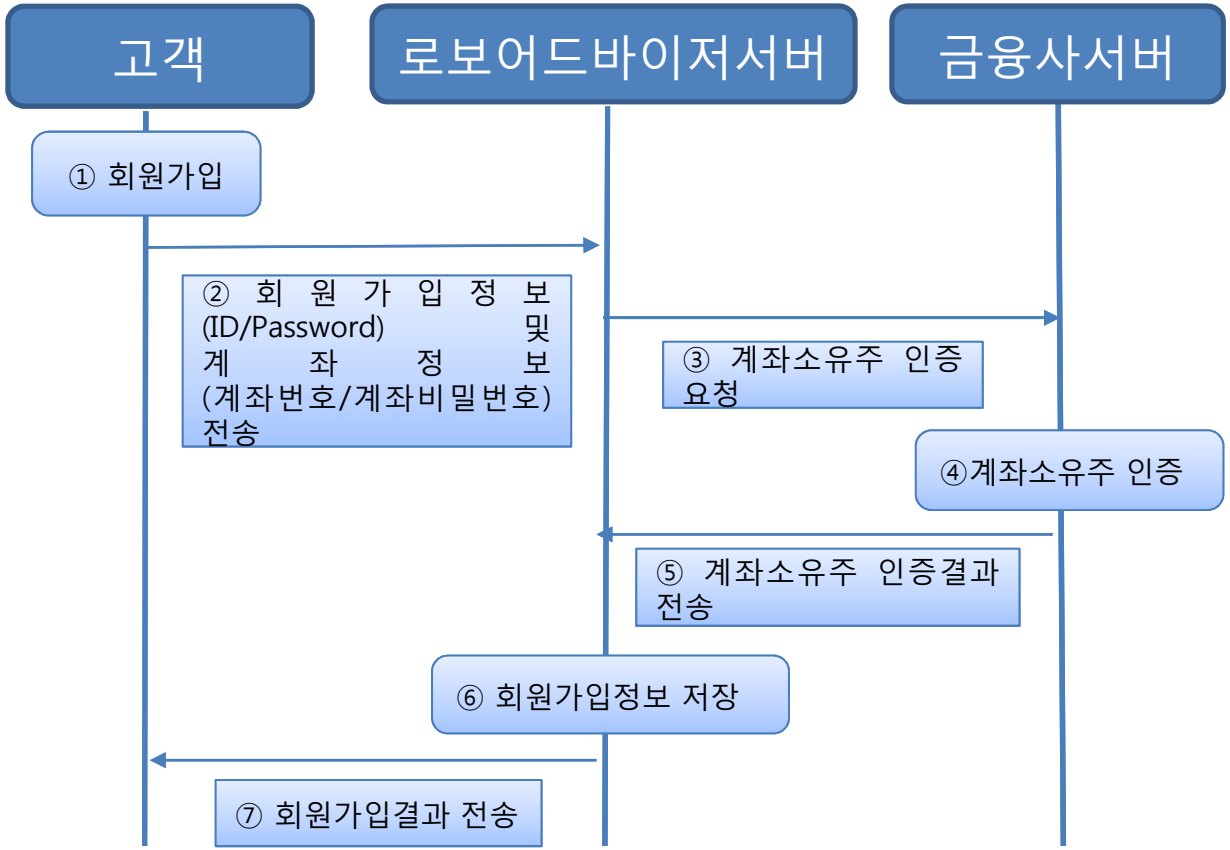
(시스템 위치 : 금융회사 내부)

※ 시스템 위치 꼭 명시, 금융회사 외부에 위치한 경우에는 '외부'로 표시

보안대책명세서 작성샘플

3. 서비스절차 (1/3)

○ 회원가입



※ 회원가입 뿐만 아니라 로보어드바이저와 관련된 모든 서비스 절차를 명시

보안대책명세서 작성샘플

3. 서비스절차 (2/3)

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 E2E암호화제품은 ABC사의DEF임
③ 계좌 소유주 인증 요청	- 로보어드바이저 서버는 E2E암호화한 계좌정보를 금융사서버로 전달	
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-256이용
⑦ 회원가입결과 전송	- 금융사 서버는 회원가입 여부를 고객에게 전송	

보안대책명세서 작성샘플

3. 서비스절차 (3/3)

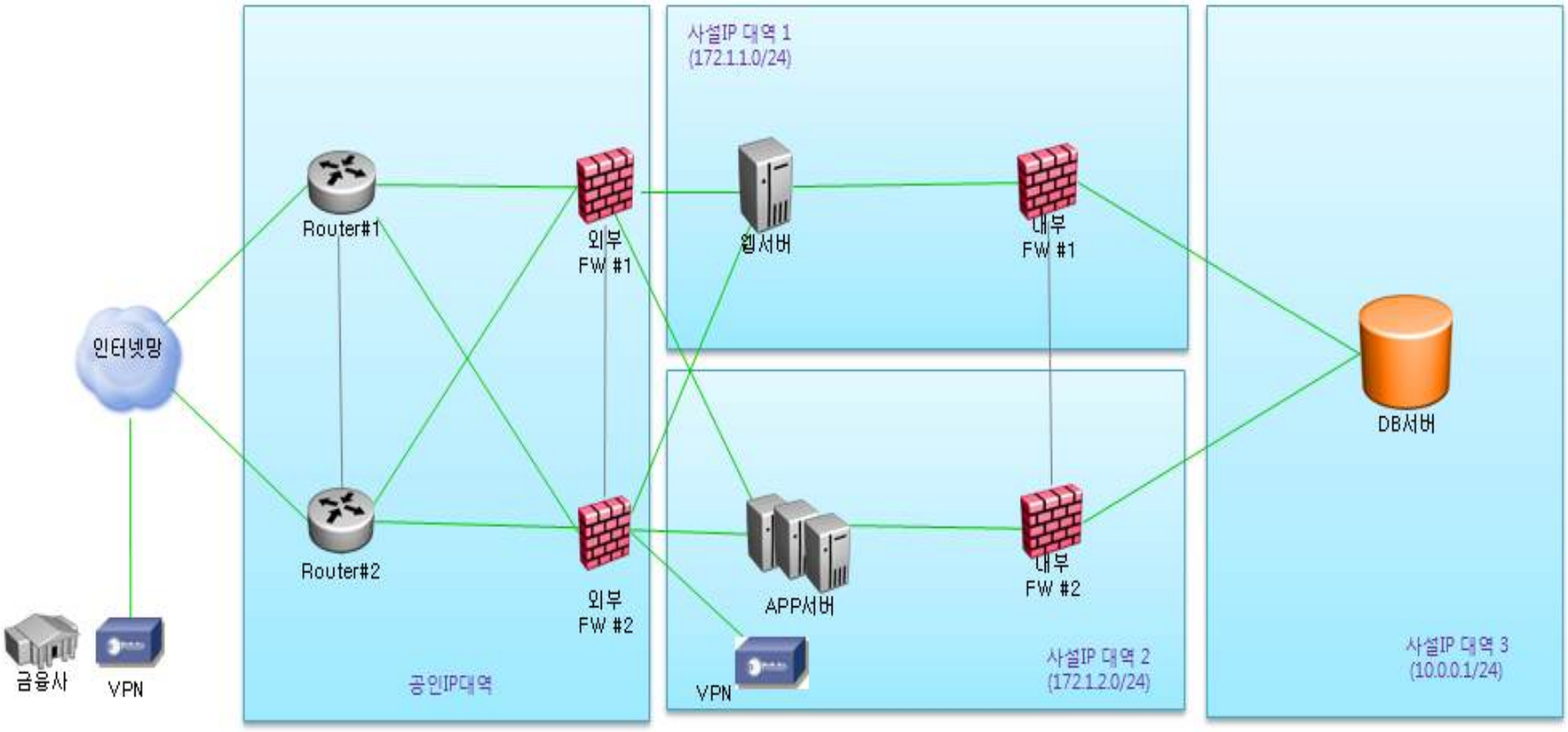
- 주요 보호정보 및 보호방안

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

- 화면 정의서

보안대책명세서 작성샘플

4. 시스템 및 네트워크 구성도 (1/2)



※ 로보어드바이저와 관련된 한 개 이상의 사이트가 있는 경우 해당 시스템 및 네트워크 구성도 모두 표기 (컨소시엄 등)

보안대책명세서 작성샘플

4. 시스템 및 네트워크 구성도 (2/2)

중요서버	역할	중요처리정보	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	

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

보안대책명세서 작성샘플

5. 심사항목 별 보호대책

○ 검토결과 요약

총 심사항목	적합(예)	부적합(아니오)	N/A
31	31	0	0

○ 상세 검토결과

항목	심사번호	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	첨부1

※ 확인결과에 '아니오, N/A'를 선택한 경우라도 선택 사유를 반드시 작성

보안대책명세서 작성요령

[증적자료 작성 시 고려사항]

- **(보안대책기술)** 각 심사기준 별로 보안대책을 **육하원칙으로 상세히 기재**

※「시스템 보안성심사 기준 상세」를 참고하여 각 세부심사기준에 보안대책이 어떻게 부합하는지를 기술

- **(객관적 증빙자료 첨부)** 작성내용을 객관적으로 증빙할 수 있는 자료를 첨부

※ 증빙자료예시 : 스크린 샷, 소스코드 일부 발췌, 심사기준을 만족하는 내용이 포함되어있는 운영기록(증적자료)의 제목(파일명), 관련 증적이 시스템으로 관리되는 경우 해당 시스템 위치, 시스템 명 등

Q & A

금융보안원
FINANCIAL SECURITY INSTITUTE