업무참고 2016-융합보안-②-09

금융회사 자체 보안성심의 가이드

2016. 7.

금융보안원
FINANCIAL SECURITY INSTITUTE

업무참고 2016-융합보안-②-09

금융회사 자체 보안성심의 가이드

2016. 7.

금융보안원
FINANCIAL SECURITY INSTITUTE

발 간 사

최근 금융권은 사물인터넷(IoT), 빅데이터(Big Data), 클라우드 컴퓨팅(Cloud Computing), 바이오(Bio) 인증, 블록체인(Block Chain) 등 새로운 기술(IT)과 금융이 융합된 혁신적인 금융서비스가 매일 매일 새롭게 등장하고 있습니다.

혁신적인 금융서비스의 성공적인 도입을 위해서는 금융시장의 신뢰성 확보와 금융소비자 보호가 매우 중요하고, 이를 위한 보안성 확보와 보안 리스크 관리가 새로운 선결 과제이자 핵심 이슈로 대두되고 있습니다.

금융보안 패러다임은 정부가 주도하는 '사전적·절차적 규제' 에서 금융회사 등 민간 중심의 '자율적 규제와 사후적 책임 강화' 로 전환되었습니다.

이러한 금융보안 패러다임의 변화에 따라 과거 금융당국이 주도했던 '보안성 심의' 역시 금융회사 등의 '자체 보안성심의' 로 바뀌어 금융회사 스스로 신규 전자금융서비스에 대한 보안성을 확보하고, 책임을 부담하는 자율보안체계로 변모하게 되었습니다.

이에 금융보안원은 금융회사 등의 자율보안체계 확립을 지원하기 위하여 금융회사 등의 자체 보안성 심의에 참고할 수 있는 「금융회사 자체 보안성 심의 가이드」 를 발간하게 되었습니다.

아무쪼록 본 가이드가 금융회사 등의 자체 보안성심의 수행 시 많은 도움이 되길 바라고, 금융보안원은 보안성 검토, 가이드 개발 등을 통해 금융회사 등의 자율보안체계 확립을 지속적으로 지원해 나가도록 하겠습니다.

2016년 7월
금융보안원
원장 허 창 언

목 차

Ⅰ. 개요

1. 목적

본 가이드는 민간 중심의 자율적 보안체계 확립을 지원하기 위하여 금융회사 또는 전자금융업자(이하 '금융회사등'이라 한다)에게 「전자금융감독규정」 제36조에 명시된 자체 보안성심의 시 참고할 수 있는 정보를 제공함을 목적으로 한다.

2. 구성

가이드는 총 5장과 참고자료로 구성된다.

① Ⅰ장에서는 가이드의 목적, 구성, 활용, 용어, 유지관리에 대하여 서술한다.

② Ⅱ장에서는 자체 보안성심의의 주체별 역할과 심의관련 기구에 대하여 서술한다.

③ Ⅲ장에서는 자체 보안성심의 절차를 단계별로 서술한다.

④ Ⅳ장에서는 「전자금융감독규정시행세칙」에 명시되어 있는 8가지 심의기준별 점검항목을 예를 들어 서술한다.

⑤ Ⅴ장에서는 「전자금융감독규정」 제36조에 따라 금융감독원에 제출해야 하는 자체 보안성심의 결과보고서에 대하여 설명한다.

⑥ 기타 자체 보안성심의와 관련된 'FAQ(Frequently Asked Questions)'와 자체 보안성심의 시 참조할 수 있는 '주요기술 관련 참고자료'를 추가적인 참고자료로 기술한다.

3. 활용

① 과거 보안성심의 사례, 금융회사 모범사례, 관련 규정, 유사 제도 등을 종합 분석하여 가이드를 작성하였으며, 회사별(또는 업무별) 상이한 특성이 존재하므로 자체 보안성심의 시 참고자료로 업무에 활용한다.

② 본 가이드는 작성시점(2016.6월)의 「전자금융감독규정」 및 「전자금융감독규정시행세칙」에 기반하여 작성되었으므로 이를 유의하여 활용한다.

③ 본 가이드에 서술된 내용과 관련 법·시행령·감독규정 등에 서술된 내용이 상충될 경우 관련 법·시행령·감독규정 등의 서술내용이 우선한다.

4. 용어

본 가이드에서 사용된 용어는 본문에서 정한 바를 따르며 그 외 용어는 「전자금융거래법」, 「전자금융거래법 시행령」, 「전자금융감독규정」, 「전자금융감독규정시행세칙」 등 관련 법·시행령·감독규정에서 정의한 용어 정의를 따른다.

5. 유지관리

본 가이드는 6개월 주기로 관련 법·시행령·감독규정 등의 개정사항을 반영하는 것을 원칙으로 하되, 관련 법·시행령·감독규정 등의 개정사항이 없거나 개정사항이 중요하지 않은 경우 유지관리 시기를 조정할 수 있다.

Ⅱ. 자체 보안성심의 체계

1. 자체 보안성심의 주체별 역할

가. 금융회사등

① 사업추진부서

신규 전자금융업무에 대한 사업을 추진하는 금융회사등의 실무부서를 의미하며, 추진사업에 대한 보안대책을 수립·적용하는 역할을 수행한다.

② 정보보호부서

- **(보안대책의 적정성 점검)** 금융회사등의 사내 IT분야 정보보호업무를 담당하는 부서를 의미하며 사업추진부서가 수립·적용한 보안대책의 적정성을 점검한다.
- **(심의 결과보고서 제출)** 자체 보안성심의 완료 후 보안성심의 결과 보고서를 금융감독원에 제출한다.
- **(보안성검토 의뢰)** 자체 보안성심의 과정 중 주요 신기술 등에 대하여 세부적인 검토가 필요하다고 판단되면 금융보안원에 보안성검토를 의뢰한다.

③ 보안성심의위원회

정보보호부서의 점검결과를 검토하고 심의대상 신규 전자금융업무에 대한 보안대책의 적정성을 최종 심의·의결한다.

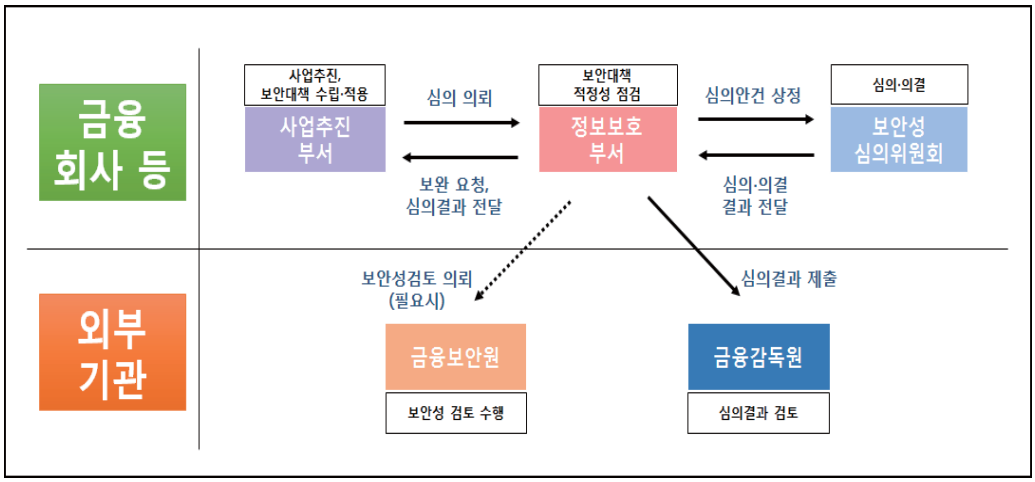
나. 금융감독원

금융회사등이 제출한 자체 보안성심의 결과보고서를 검토하고, 신규 전자금융업무의 보안수준이 충분하지 않다고 판단되면 금융회사등에게 개선·보완을 요구한다.

다. 금융보안원

금융회사등이 적용예정인 주요 신기술을 중심으로 발생가능한 보안문제 및 관련 보안대책의 적정성 여부를 세부적으로 검토한다.

<자체 보안성심의 주체별 역할(예시)>



2. 심의관련 기구

가. 보안성심의위원회

① **(구성)** 회사별 특성에 따라 위원회 구성은 달라질 수 있으나 정보보호최고책임자와 자체 보안성심의와 관련된 부서장 등으로 위원회를 구성하며, 효율적 운영을 위해 실무책임자를 위원회에 포함시킬 수 있다.

- 「전자금융감독규정시행세칙」 제3조에는 정보보호최고책임자가 자체 보안성심의 결과를 승인하도록 명시되어 있으므로, 통상적으로 보안성심의위원회의 위원장은 정보보호최고책임자가 담당한다.

> ☞ **「전자금융감독규정」 제8조의2에 따라 금융회사등은 중요 정보보호에 관한 사항을 심의·의결하는 정보보호위원회(위원장 : 정보보호최고책임자)를 운영해야 하므로, 별도의 보안성심의위원회를 조직하기보다는 정보보호위원회를 활용하는 방안을 고려할 수 있다.**

<보안성심의위원회 구성(예시)>

구분	내용
위원장	정보보호최고책임자(CISO)
위원	정보보호업무 관련 부서장, 전산운영 및 개발 관련 부서장, 준법업무 관련 부서장 등
실무위원	정보보호부서 보안성심의 담당자, 사업추진부서 실무책임자 등

② **(운영)** 자체 보안성심의 최종 단계에서 위원회를 개최하여 신규 전자금융업무에 대한 보안대책의 적정성을 심의·의결한다.

- 심의결과는 정보보호최고책임자의 승인을 받아야 하지만 보안성심의위원회 운영은 의무사항이 아니므로, 회사별 특성(규모, 조직구성 등)에 따라 보안성심의위원회를 운영하지 않을 수 있으며, 위원회의 명칭은 자체적으로 명명할 수 있다.

☞ 정보보호최고책임자 단독으로 자체 보안성심의 결과를 승인하기보다는 위원회에서 심의·의결하는 것이 보다 효율적이므로 일반적으로 위원회를 운영한다.

나. 정보보호실무협의회

① **(구성)** 회사별 특성에 따라 협의회 구성은 달라질 수 있으나 정보보호부서 부서장과 사내 IT분야 정보보호와 관련된 실무책임자 등으로 협의회를 구성한다.

<정보보호실무협의회 구성(예시)>

구분	내용
의장	정보보호부서 부서장
위원	정보보호부서・정보시스템(NW, 서버 등) 담당부서・사업추진부서 실무책임자 등

② **(운영)** 심의대상 여부의 판단 등을 지원하는 실무인력 위주의 협의회를 조직・활용할 수 있다.

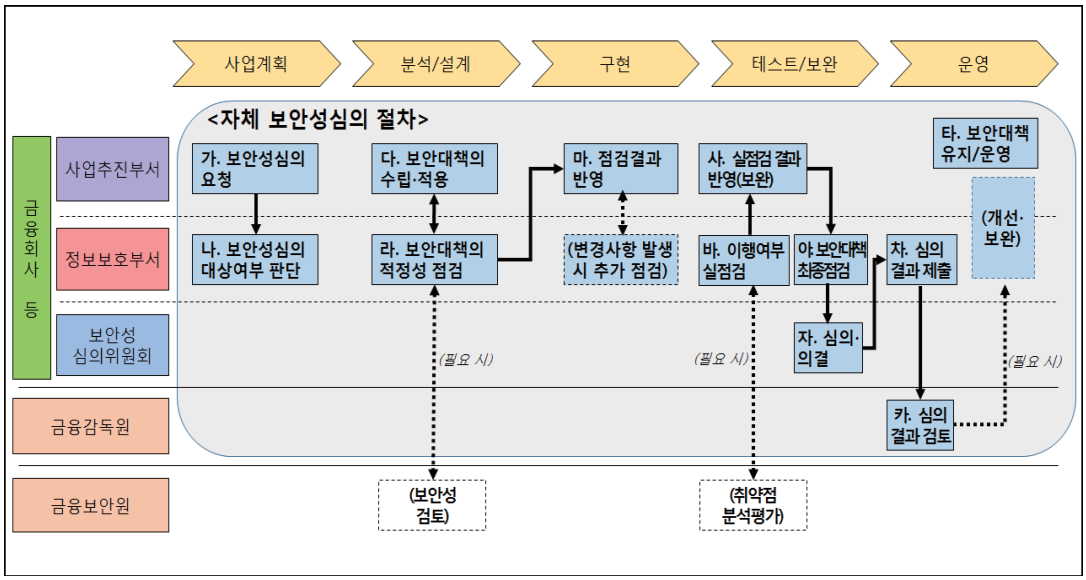
- 정보보호실무협의회 운영은 의무사항이 아니므로 회사별 특성(규모, 조직구성 등)에 따라 정보보호실무협의회를 운영하지 않을 수 있으며, 협의회의 명칭은 자체적으로 명명할 수 있다.

☞ 통상 심의체계가 잘 갖추어진 대형금융회사는 상기 형태의 정보보호실무협의회를 운영하고 있다.

- 협의회는 신규 전자금융업무 외 업무에 대하여 보안대책의 적정성을 내부적으로 검토(이하 '내부 보안성검토')하는 역할을 추가적으로 수행할 수 있다.

Ⅲ. 자체 보안성심의 절차

<자체 보안성심의 절차(예시)>



가. 보안성심의 요청

① **(심의 요청)** 사업추진부서는 신규 전자금융업무에 대하여 사업추진계획서를 작성하여 정보보호부서에 보안성심의를 요청한다.

② **(자료 제출)** 사업추진부서는 보안성심의 요청 시 업무의 개요 및 범위, 정보시스템 현황, 업무처리 절차 등의 내용을 정보보호부서에 제출하여 정보보호부서가 해당 업무를 적절히 이해할 수 있도록 한다.

- 정보보호부서는 내부 정보보안규정 등 보안대책 수립을 위한 참고자료를 사전에 제공할 수 있으며, 사업추진부서는 이를 바탕으로 추진하고자 하는 업무의 보안대책을 수립하여 심의 요청 시 제출할 수 있다.

☞ **보안대책은 분석/설계 단계에서 수립·적용되는 것이 보다 일반적이지만, 사업계획 단계에서도 보안대책의 수립(및 적용)이 가능하다.**

나. 보안성심의 대상여부 판단

정보보호부서는 사업추진부서에서 추진하고자 하는 신규 업무에 대해 이해하고, 해당 업무가 신규 전자금융업무인지 여부를 판단한다.

- 대상여부에 대한 판단이 어려운 경우 또는 효율적 판단을 위해 정보보호 실무협의회 등을 통해 대상여부를 결정할 수 있다.
- 신규 전자금융업무에 해당된다고 판단되면 보안성심의 절차에 따라 자체 보안성심의를 진행하고, 신규 전자금융업무에 해당되지 않는다고 판단되면 내규에 따라 내부 보안성검토를 수행할 수 있다.

> ☞ **정보보호최고책임자가 결과를 승인하는 자체 보안성심의 외에도 금융회사등은 추진사업의 보안성 강화를 위하여 정보보호부서장 등의 책임하에 운영되는 유사형태의 내부 보안성검토를 수행할 수 있다.**

다. 보안대책의 수립·적용

① **(보안대책 수립 등)** 사업추진부서는 신규 전자금융업무가 안전하게 제공될 수 있도록 분석/설계 시 적정한 보안대책을 수립하고 이에 대한 적용방안을 구체화한다.

- 사업계획 시 보안대책을 수립한 경우 분석/설계 단계에서 해당 보안대책을 재검토 또는 적용방안을 구체화한다.

② **(보안대책 제출)** 사업추진부서는 수립·적용된 보안대책을 정보보호부서에 제출하여 적정성을 심의받는다.

라. 보안대책의 적정성 점검

① **(보안대책 점검)** 정보보호부서는 사업추진부서가 제출한 업무의 개요 및 범위, 정보시스템 현황, 업무처리 절차 등이 포함된 사업추진계획 자료와 보안대책 적용방안을 종합 검토하여 보안대책의 적정성을 점검한다.

- 사업추진부서에서 제공한 자료가 구체적이지 않을 경우, 정보보호부서는 사업추진부서에 추가 자료를 요청할 수 있다.

② **(보안성검토 의뢰)** 상기 과정에서 신기술 도입으로 자체적인 보안 적정성 판단이 어렵거나 신기술에 대한 보다 세부적인 검토가 필요하다고 판단되면 금융보안원에 보안성검토를 요청할 수 있다.

- 금융보안원의 보안성검토 결과는 자체 보안성심의의 참고자료로 활용은 가능하지만, 자체 보안성심의 결과를 대체할 수 없다.

마. 점검결과 반영

① **(점검결과 반영)** 사업추진부서는 정보보호부서의 보안대책 점검결과에 따라 보안대책을 변경·강화하는 등 점검결과를 반영하여 업무를 구현한다.

② **(추가 점검)** 사업추진부서는 구현과정에서 보안관련 변경사항이 발생한 경우 해당 내용을 정보보호부서에 통보하고, 정보보호부서는 심의대상 업무의 보안성이 적정하게 유지되는지 추가적으로 점검한다.

- 추가 점검 결과 보안대책의 보완이 필요하다고 판단되면 사업추진부서는 보안대책을 보완하여 업무를 구현한다.

바. 이행여부 실점검(취약점 분석평가 등)

① **(이행여부 실점검)** 사업추진부서는 업무의 구현내역을 정보보호부서에 제공하고, 정보보호부서는 업무의 구현내역에 대하여 취약점 분석평가 등을 통하여 보안대책이 적정하게 구현되었는지 이행여부를 실점검한다.

② **(외부 점검 의뢰)** 정보보호부서는 이행여부 실점검 시 외부 전문기관의 점검이 필요하다고 판단되면 금융보안원 등에 취약점 분석평가를 의뢰할 수 있다.

사. 실점검 결과 반영(보완)

① **(보안대책 보완)** 사업추진부서는 정보보호부서의 실점검 결과를 바탕으로 보안대책을 보완한다. 다만, 즉시 보완이 어려운 경우 보완 이행계획을 수립한다.

② **(보완내역 제출)** 사업추진부서는 최종 보완내역 또는 이행계획을 정보보호부서에 제출한다.

아. 보안대책 최종점검

정보보호부서는 사업추진부서가 제출한 최종 보완내역 또는 이행계획을 검토하여 보안대책의 적정성을 최종 점검한다.

- 점검결과가 적정하다고 판단되면 보안성심의위원회에 심의안건으로 상정한다.

자. 심의·의결

보안성심의위원회는 정보보호부서의 점검결과를 검토하고, 심의대상 신규 전자금융업무에 대한 보안대책의 적정성을 최종 심의·의결한다.

차. 심의결과 제출

정보보호부서는 해당 신규 전자금융업무에 대한 심의·의결 후 정보보호 최고책임자가 승인한 자체 보안성심의 결과보고서를 신규 전자금융업무가 제공 또는 시행된 날부터 7일 이내에 금융감독원에 제출한다.

☞ **신규 전자금융업무가 제공 또는 시행된 날을 기준으로 과거 1년 이내에 전자금융사고가 발생하지 않은 기관으로서, 일정 요건(전자금융업무를 신규로 수행한 날부터 1년이 경과 등)을 만족하는 금융회사등은 금융감독원에 결과보고서를 제출하지 아니할 수 있다.**

카. 심의결과 검토

금융감독원은 금융회사등이 제출한 자체 보안성심의 결과보고서를 검토하고 신규 전자금융업무의 보안수준이 충분하지 않다고 판단되면 금융회사등에게 개선·보완을 요구한다.

- 개선·보완을 요구받은 금융회사등은 사업추진부서와 정보보호부서가 협의하여 요구사항을 충족시킬 수 있도록 신규 전자금융업무를 개선·보완한다.

타. 보안대책 유지/운영

사업추진부서는 적정한 보안대책이 유지되도록 신규 전자금융업무를 운영한다.

☞ **정보보호부서는 내부 보안감사 등을 통하여 적정한 보안대책이 유지되는지 확인한다.**

Ⅳ. 심의기준별 점검항목 예시

1. 점검항목 개요

① 금융회사등이 「전자금융감독규정시행세칙」 <별표 1>에 명시되어 있는 8가지 심의기준에 따라 신규 전자금융업무에 대한 보안성심의를 적정하게 수행할 수 있도록, 심의기준별 점검항목을 예시한다.

- 각 사업에 일반적으로 적용될 수 있는 항목을 예시하였으나, 금융회사등은 자체 보안성심의 시 예시된 항목 등을 참고하여 심의대상 사업특성에 적합한 점검항목을 자체적으로 구성한다.

> ☞ **예시된 항목은 자체 보안성심의를 준비하는 금융회사등의 이해를 돕기 위한 목적으로 작성되었으며, 절대적인 점검항목으로 활용하는 것은 적절치 않다.**

② 8개 심의기준에 대하여 예시된 점검항목은 총 82개이며, 금융회사등은 예시된 항목을 참고하여(선택・확장 적용, 수정 등) 실제 심의 시 점검항목을 구성할 수 있다.

<심의기준별 예시된 점검항목 수>

심의기준	점검항목 수
거래 당사자 인증	12
거래정보의 기밀성 및 무결성	5
정보처리시스템 보호대책	21
고객단말기 보호대책	14
정보유출 방지대책	10
이상금융거래 방지대책	3
시스템 가용성 확보 및 비상대책	12
시스템 설치장소에 대한 물리적 접근통제	5
계	82

2. 점검항목 세부내역

가. 거래 당사자 인증

‘거래 당사자 인증’에 대한 12개의 점검항목을 예시한다.

<‘거래 당사자 인증’ 점검항목(예시)>

번호	항목명	점검내용	비고
1	인증방법의 적정성	전자금융거래의 종류, 성격, 위험수준 등을 고려하여 안전한 인증방법을 사용하는지 점검	- 인증수단 선택 시 안전성, 보안성, 이용편의성 등을 충분히 고려 - 일반적으로 지식기반(비밀번호 등 본인만 알고 있는 정보), 소유기반(휴대폰, 공인인증서, H/W 토큰 등 전자적 장치 소유), 특징기반(지문인식 등 신체정보 및 서명 등 행위기반 정보 활용) 이용자 인증 실시 - 인증방법 자체의 안전성(메커니즘, 알고리즘 등)과 인증 프로세스 전반의 안전성을 함께 검토 - 인증정보와 인증정보를 생성하는데 직접적으로 사용되는 값(예 ; PKI 기반의 개인키, OTP 생성키 등(존재할 경우))은 적절히 보호되어야 함
2	서비스 가입 시 이용자 인증	서비스 가입 시 적절히 이용자 인증이 실시되는지 점검	- 타인의 명의를 도용하여 서비스 가입이 이루어지지 않도록 서비스 가입 시 지식기반, 소유기반, 특징기반 등의 이용자 인증 필요 - 인증과정에서 휴대폰이 활용될 경우 통신사 명의확인, 단말기 지정 등 본인확인 강화 방안을 고려하고, 메시지 탈취, 전화번호 변조, 휴대폰 도난 및 분실 등에 대한 대응방안 마련
3	서비스 이용 시 이용자 인증	서비스 이용(로그인, 이체, 결제 등) 시 적절히 이용자 인증이 실시되는지 점검	- 타인의 명의를 도용하여 로그인, 이체, 결제 등이 이루어지지 않도록 지식기반, 소유기반, 특징기반 등의 이용자 인증 필요 - 인증과정에서 휴대폰이 활용될 경우 통신사 명의확인, 단말기 지정 등 본인확인 강화 방안을 고려하고, 메시지 탈취, 전화번호 변조, 휴대폰 도난 및 분실 등에 대한 대응방안 마련

번호	항목명	점검내용	비고
4	세션 가로채기 방지	이용자와 정보처리시스템 사이에 인증세션이 생성된 후 비인가자의 해당 세션정보를 이용한 인증이 불가능한지 점검	- 관련 대응 방안의 예 · 서비스 매 세션마다 단말기 인증(기기 고유식별정보 확인, 통신사명의확인 등)과 이용자 인증 실시 · 세션 타임아웃을 설정하고, 세션타임아웃 시 재인증 · 세션값이 노출되지 않도록 이용자와 정보처리시스템 사이에 전송되는 데이터를 암호화 등
5	다단계 가입자 확인	전자금융서비스 가입 시 다단계로 가입자를 확인하고 있는지 점검	- 통신사 본인 인증, 기계좌정보 확인, 공인인증서 기반 인증 등 다단계 가입자 확인 고려
6	거래 재활용 방지	악의적인 의도를 가진 자가 기존 인증·거래정보를 재활용하여 부정 인증·거래를 시도하는 것을 방지하는지 점검	- 관련 대응 방안의 예 · 인증·거래 시 일회성 정보 활용
7	인증 우회방지	사용자 확인을 위한 인증단계를 우회하여(예 ; 비밀번호 입력 단계 우회 등), 전자금융 서비스를 이용할 수 있는지 점검	- 인증단계를 거치지 않고 인증성공 후 단계로 진입할 수 있는지(로직 변경 등) 확인
8	비밀번호 추측방지	비인가자가 인증정보 등을 추측하여 인증을 시도하는 공격을 방지하는지 점검	- 인증수단 또는 인증정보를 보유하지 않은 비인가자가 공격하고자 하는 대상의 비밀정보 등을 추측하여 반복적으로 인증을 시도하는 공격에 대한 대응방안 마련 - 비인가자는 수학적 계산, 사전공격, 무차별 대입(전수조사) 공격 등을 통해 비밀정보 추측을 시도할 수 있으며, 비밀정보 추측 엔트로피가 높아질수록 비인가자가 인증정보를 추측하기 어려움(적절한 조합규칙 사용, 취약한 비밀번호 사용금지 등) - 비인가자에 의한 무차별적인 인증시도를 방지하기 위해 인증시도 실패횟수(5회 이내 등) 혹은 허용시간 간격을 제한하는 방법 등 고려

번호	항목명	점검내용	비고
9	정보처리 시스템 인증	전자금융거래 이용자(또는 전자금융거래 이용자 프로그램)가 접속한 정보처리시스템이 정당한지 여부를 식별 및 인증하는지 점검	- 서버 인증서 또는 이용자가 사전 등록한 이미지/문자열 활용 등 - 서버 인증서를 이용하여 정보처리시스템 인증을 수행할 경우 서버 인증서 내 포함된 서버주소, 유효기간, 발급기관, 소유자 등을 확인하여 서버 인증서의 유효성 검증 - 이용자와 정보처리시스템 사이에 개입하여 이용자의 인증정보를 획득하는 중간자 공격 방지 - 전자금융거래 이용자가 피싱, 파밍 등의 공격에 의해 정당하지 않은 웹사이트 혹은 정보처리시스템으로 접속하는 것을 방지
10	인증 및 거래 관련 기록관리	인증 및 거래 관련 기록을 보존하고, 관련 기록의 변경에 대한 보호대책을 제공하는지 점검	- 인증관련 기록 ; 인증 시도 및 결과, 인증수단을 발급받기 위한 등록정보, 접속정보 등 - 「전자금융거래법 시행령」에 따라 다음의 각 전자금융거래기록은 보존되어야 함 · 5년간 보존 필요(전자금융보조업자는 3년간 보존) ; 전자금융거래의 종류(보험계약의 경우, 보험계약의 종류를 말함) 및 금액, 전자금융거래의 상대방에 관한 정보, 지급인의 출금 동의에 관한 사항, 해당 전자금융거래와 관련한 전자적 장치의 접속기록, 전자금융거래의 신청 및 조건의 변경에 관한 사항, 건당 거래금액이 1만원을 초과하는 전자금융거래에 관한 기록 · 1년간 보존 필요 ; 건당 거래금액이 1만원 이하인 전자금융거래에 관한 기록, 전자지급수단의 이용과 관련된 거래승인에 관한 기록, 오류정정 요구사실 및 처리결과에 관한 사항 - 상기 인증 및 거래 관련 정보가 기록된 데이터베이스, 로그 등에 대한 보호대책 마련

번호	항목명	점검내용	비고
11	인증수단의 관리	인증수단의 등록, 발급, 배포, 폐기와 관련하여 안전한 관리 방안을 갖추고 있는지 점검	- 전자금융거래에 사용되는 접근매체를 발급받기 위해서는 반드시 실명확인 후 교부 - 전자금융거래 서비스 이용자의 인증수단(접근매체 포함) 발급/등록 시 신분위장, 인증정보 유출, 비인가자에 의한 발급/등록 등에 대한 대응방안 마련 - 인증수단의 갱신관리, 안전한 폐기 등 인증수단 관리에 관한 적절한 운영방안 마련
12	금융수단 등록 시 개별 인증	한 번의 사용자 인증으로 복수 개의 금융수단이 등록되지 않는지 점검	- 금융수단의 예 ; 신용카드, 직불카드, 선불카드, 현금카드, 계좌정보 등

나. 거래정보의 기밀성 및 무결성

‘거래정보의 기밀성 및 무결성’에 대한 5개의 점검항목을 예시한다.

<‘거래정보의 기밀성 및 무결성’ 점검항목(예시)>

번호	항목명	점검내용	비고
1	거래정보 등의 기밀성	전자금융거래 이용자와 정보처리시스템 사이에 전송되거나 저장되는 전자금융거래내역 등 중요정보는 안전하게 암호화하여 기밀성을 보장하는지 점검	- 이용자와 정보처리시스템 간에 전송되거나 저장되는 금융거래 내역 등 중요정보는 도청, 노출로 인한 피해를 방지하기 위하여 암호화되어야 함 - 중요정보는 이용자 입력시부터 정보처리 시스템까지 기밀성이 보장되어야 함 (예 ; E2E 암호화 적용 등)
2	거래정보 등의 무결성	전자금융거래내역(거래전문포함) 등 주요 보호대상은 위변조 여부 등 무결성을 검증할 수 있는지 점검	- 전자금융거래내역(거래전문포함)에 대하여 해당 전자금융 거래내역 중 최소 정보 단위의 내용이 변경되더라도 변경 여부를 확인할 수 있어야 함 - 보호대상은 저장데이터, 전송데이터 등 다양한 형태가 될 수 있음 - 단말기에서 입력한 거래정보는 이용자 입력시부터 정보처리시스템까지 무결성이 보장되어야 함
3	안전한 암호 알고리즘 사용	기밀성 및 무결성을 지원하기 위하여 암호 연산이 사용되었을 경우, 안전성이 입증된 암호 알고리즘과 키길이를 사용하는지 점검	- 국내외 전문기관(NIST, KISA 등)에서 발표한 자료 등을 참고하여 안전한 암호 알고리즘 및 키길이를 사용 - 인증서 사용 시 인증서에 대해서도 안전한 암호 알고리즘 및 키길이가 사용되어야 함 - 안전성이 검증된 암호모듈 사용(CMVP, KCMVP 검증 암호모듈 사용) 권고 - 구간별 별도의 암호화 세션이 형성될 경우, 각 구간별 모든 암호화 세션에 대하여 안전한 암호알고리즘/키길이가 사용되었는지 확인 필요

번호	항목명	점검내용	비고
4	안전한 키관리	암호화에 사용하는 암호키는 암호키의 생명주기(생성, 분배, 접근, 파기 등) 전반에 걸쳐 안전하게 관리되는지 점검	- 안전한 암호키 생성, 분배, 접근, 파기 절차를 가져야 함 - 필요 시 암호키 관리를 위한 안전한 물리적·관리적 절차 고려(HSM, 잠금장치가 있는 금고 등) - 암호 및 인증시스템에 적용되는 키는 주입·운용·갱신·폐기에 대한 절차 및 방법에 따라 안전하게 관리 - 구간별 별도의 암호화 세션이 형성될 경우, 각 구간별 모든 암호화 세션에 대하여 암호키가 생명주기 전반에 걸쳐 안전하게 관리되는지 확인 필요
5	안전한 암호 프로그램 관리	암호프로그램에 대하여 담당자 지정, 담당자 이외의 이용 통제 및 원시프로그램(source program) 별도 보관 등을 준수하여 유포 및 부당 이용이 발생하지 않도록 하는지 점검	

다. 정보처리시스템 보호대책

‘정보처리시스템 보호대책’에 대한 21개의 점검항목을 예시한다.

<‘정보처리시스템 보호대책’ 점검항목(예시)>

번호	항목명	점검내용	비고
1	책임자 지정・운영	정보처리시스템의 책임자를 지정・운영하는지 점검	- 책임자는 시스템 관리자를 적절히 관리 감독해야 함
2	유지보수 관리	데이터베이스관리시스템(DBMS)・운영체제・웹프로그램 등 주요 프로그램에 대하여 정기적으로 유지보수를 실시하고 작업일, 작업내용, 작업결과 등을 기록한 유지보수관리대장을 작성・보관하는지 점검	- 유지보수 시 유의사항 ・ 인가된 인력만 유지보수에 참여하도록 통제 ・ 설치장소 외 다른 장소로 정보시스템 이동 시 통제수단 강구 ・ 유지보수 관련 장비・도구 등 반출입 시 악성코드 감염여부, 자료 무단반출 여부 확인 ・ 외부에서 원격으로 유지보수 하는 것을 원칙적으로 금지
3	장애 기록 관리	장애발생 시 장애일시, 장애내용 및 조치사항 등을 기록한 장애상황기록부를 상세히 작성・보관하는지 점검	
4	통제절차 준수	시스템 통합, 전환 및 재개발 시 장애 등으로 인하여 정보처리시스템의 운영에 지장이 초래되지 않도록 통제 절차를 마련하여 준수하는지 점검	
5	중요 패치 수행	정보처리시스템의 운영체제, 시스템 유틸리티 등의 긴급하고 중요한 보정(patch) 사항에 대하여 즉시 보정 작업을 실시하는지 점검	
6	운영체제 계정 추가인증	정보처리시스템의 운영체제 계정으로 로그인 할 경우 계정 및 비밀번호 이외에 별도의 추가인증 절차를 시행하는지 점검	

번호	항목명	점검내용	비고
7	운영체제 계정 모니터링	정보처리시스템 운영체제 계정에 대한 사용권한, 접근 기록, 작업 내역 등에 대한 상시 모니터링 체계를 수립하고, 이상 징후 발생 시 필요한 통제 조치를 즉시 시행하는지 점검	
8	비밀번호 설정	비밀번호는 적절한 조합규칙으로 설정하고, 분기별 1회 이상 변경하며, 보관 시 암호화하고, 시스템마다 관리자 비밀번호를 다르게 설정하는지 점검	- 비밀번호의 적절한 조합규칙의 예 · (필수) 이용자 식별부호(아이디), 생년월일, 주민등록번호, 전화번호를 포함하지 않은 숫자와 영문자 및 특수문자 등을 혼합하여 8자리 이상 · (권고) 비밀번호 조합 시 사전 등록단어 금지, 동일 단어/숫자 반복사용 금지, 기사용 비밀번호 금지 등
9	비밀번호 연속오류 대응	비밀번호 입력 시 5회 이내의 범위에서 미리 정한 횟수 이상의 입력오류가 연속하여 발생한 경우 즉시 적절한 조치를 수행하는지 점검	- 비밀번호 연속오류 시 적절한 조치의 예 · 해당 비밀번호를 이용하는 접속을 차단 · 비인가자의 침입 여부를 점검 · 본인 확인 후 비밀번호 재부여 및 초기화
10	서비스 관리	운영에 필요한 서비스 포트 외에 불필요한 서비스 포트와 업무목적 외 기능 및 프로그램(시험·개발 도구 등 포함) 등을 제거하고, 관리용 서비스와 사용자용 서비스를 분리운영하는지 점검	- 전산시스템은 가급적 단일 서비스에 대하여 독립적으로 사용할 것을 고려
11	서버접근 중요단말 보호	정보처리시스템에 접속하는 단말을 중요단말로 지정하고 적절한 보호대책을 적용하는지 점검	- 중요단말 보호대책 · 담당자 이외 무단조작 방지 조치(로그인 비밀번호 설정 등 포함) · 정보처리시스템에 접속하는 단말기에 대해 정당한 사용자인가의 여부를 확인할 수 있는 기록 유지 · 외부반출, 인터넷 접속, 그룹웨어 접속의 금지 등 강화된 보호대책적용 · 정보유출, 악성코드 감염 등을 방지할 수 있도록 단말기에서 보조기억매체 및 휴대용 전산장비에 접근하는 것을 통제 · 중요단말은 악성코드 감염여부를 매일 점검

번호	항목명	점검내용	비고
12	공개용 서버 설치 및 접근통제	공개용 웹서버 등 공개용 서버는 내부통신망과 외부통신망사이의 독립된 통신망(DMZ구간)에 설치하고 접근제어하는지 점검	
13	DMZ구간 내 중요 정보 저장 제한	DMZ구간 내 이용자 정보 등 주요 정보 저장을 금지하는지 점검	- 다만, 거래로그 관리 목적의 경우 암호화하여 관리
14	공개용 서버 게시자료 보안	게시자료에 대한 사전 내부통제 실시(중요업무 자료, 민감내용 게시방지 등 포함), 무기명 또는 가명에 의한 게시금지, 자료 게시 담당자 지정·운영, 개인정보 유출 및 위·변조 방지가 수행되는지 점검	
15	서버 해킹 방지	서버가 저장자료의 절취, 위·변조 및 분산서비스거부 공격 등 해킹(전자적 침해행위) 공격에 노출되지 않도록 대응조치 하는지 점검	- 침입차단시스템, 침입탐지시스템, DDoS 공격대응시스템, 서버보안솔루션(SecureOS) 등 서버 보호를 위한 적절한 정보보호시스템 설치·운영 고려 - 웹서버의 경우 OWASP TOP 10 등 주요 취약점 대응
16	악성코드 감염 방지	출처·유통경로·제작자가 명확하지 않은 응용프로그램은 악성코드 진단후 사용하고 악성코드 검색/치료 프로그램의 최신 버전을 유지하는지 점검	
17	보안성 검증 및 취약점 점검	전자금융서비스 개시 또는 전자금융거래 프로그램 변경(개편, 기능추가) 전 취약점 점검, 정적/동적 테스트 등 자체 보안성 검증을 실시하고, 관련 시스템에 대하여 모의해킹 및 점검툴 등을 활용한 주기적인 취약점 점검을 수행하는지 점검	
18	정보보호시스템 원격관리 금지 등	정보보호시스템의 원격관리는 원칙적으로 금지하고, 주기적으로 작동상태를 점검하는지 점검	- 원격관리가 불가피한 경우에는 사용시간, 접속자, 비밀번호변경, 수행업무내용 기록 등에 대한 원격관리절차를 수립·운영

번호	항목명	점검내용	비고
19	외부통신망 무단 접속 금지	외부통신망과 연결될 필요가 없는 내부 시스템은 외부통신망과 분리·차단 및 접속을 금지하고, 정보보호시스템을 우회한 외부통신망 접속이 불가한지 점검	- 내부통신망과 연결된 내부 업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속 금지(업무상 불가피하여 금융감독원장의 확인을 받은 경우 예외) - 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리(업무 특성상 분리하기 어렵다고 금융감독원장이 인정하는 경우는 예외)
20	IP 주소 관리	내부통신망에서 사용하는 IP 주소의 경우 사설 IP주소를 사용하고, 정보처리시스템의 운영담당, 개발담당 및 외부직원 등 업무 특성별로 네트워크를 적절하게 분리하여 IP주소를 사용하는지 점검	- 다만, 외부직원 등과의 공동작업 수행 등 네트워크의 분리가 어렵다고 금융감독원장이 정하는 경우에는 업무특성별로 접근권한을 분리하여 IP주소를 사용
21	고객단말 원장 접속 금지	고객단말기가 고객 원장이 보관되어 있는 Host(Server/DB)에 직접 접속이 불가한지 점검	- 고객단말기는 대고객 접속시스템까지만 접속하도록 구성

라. 고객단말기 보호대책

‘고객단말기 보호대책’에 대한 14개의 점검항목을 예시한다.

<‘고객단말기 보호대책’ 점검항목(예시)>

번호	항목명	점검내용	비고
1	시큐어코딩 적용	전자금융거래 프로그램이 시큐어코딩을 적용하여 개발되었는지 점검	
2	역분석 방지기술 적용	전자금융거래 프로그램에 난독화, 네이티브 라이브러리 구현, 안티디버깅 등의 역분석 방지 기술이 적용되었는지 점검	- 무료 난독화 솔루션 ‘Proguard’는 2013년 감사원 감사지적사항으로서 사용에 유의
3	운영체제 임의개조 탐지 및 서비스 이용제한	루팅 등 운영체제의 임의 개조를 탐지하고, 임의 개조된 상태에서 전자금융거래가 수행되지 않도록 전자금융거래 서비스 이용을 제한하는지 점검	- 운영체제 임의개조 탐지 시 전자금융거래 프로그램 또는 전자금융거래 세션 종료 등
4	운영체제 임의개조 탐지 우회 대응	운영체제 임의개조 탐지 기능을 우회하여 전자금융 서비스를 이용하고자 하는 시도를 대응하는지 점검	- 운영체제 임의개조(루팅 등) 탐지 기능을 우회하는 기술이 지속적으로 진화하고 있으므로, 관련 기능이 이를 지속적으로 대응(최신 우회기술 대응 등)하고 있는지 확인
5	프로그램 무결성 검증	전자금융거래 프로그램 등 보호대상에 대하여 코드, 리소스 파일 등에 대한 무결성을 검증하는지 점검	
6	악성코드 탐지	중요시점에서 악성코드 감염을 검사하는지 점검	- 중요시점은 전자금융거래 서비스 특성에 따라 전자금융거래 프로그램 구동 시, 결제 과정 중, 인증 시, 중요정보 입력 시 등이 될 수 있음
7	단말기 보안로그 기록	운영체제 임의개조, 앱 위·변조 등 단말기 보안과 관련된 로그를 기록하는지 점검	- 관련 로그는 서버에 기록될 수 있음
8	분실·도난 대책	단말기의 분실·도난 시 대응 절차를 마련하고 있는지 점검	- 단말기의 분실·도난이 전자금융거래에 영향을 미치는 경우 적용

번호	항목명	점검내용	비고
9	중요정보 평문저장 금지	전자금융 서비스에서 사용된 중요정보가 단말기 내 평문으로 저장되지 않는지 점검	- 중요정보의 예 ; 금융정보, 개인정보, 로그인/이체/공인인증서 비밀번호, 거래정보 등
10	입력정보보호	중요정보 입력 시 보안키패드 등을 사용하여 입력정보가 보호되는지와, 보안키패드가 적용되더라도 악용(입력정보 유추/식별, 화면캡처 등)하여 입력정보를 획득할 수 있는지 점검	
11	서명 인증서 관리	전자금융거래 프로그램 서명용 인증서 관리의 적정성 점검	- 해커가 전자금융거래 프로그램 서명용 인증서를 악용하지 못하도록 서명용 인증서를 철저히 관리
12	다중 접속관리	동시에 2대의 기기(스마트폰, PC 등)에서 동일 계정으로 접속하여 전자금융거래가 수행되지 않도록 다중 접속을 관리하는지 점검	- 업권별(업무별) 특성을 고려하여 반영
13	최근 접속기록 정보제공	최종 접속 정보 등 이용자가 최근 접속 정보를 확인할 수 있는 기능을 제공하는지 점검	
14	거래내역 정보 제공	전자금융서비스 거래 내역 등의 정보를 이용자에게 제공하는지 점검	

마. 정보유출 방지대책

‘정보유출 방지대책’에 대한 10개의 점검항목을 예시한다.

<‘정보유출 방지대책’ 점검항목(예시)>

번호	항목명	점검내용	비고
1	전산자료 현황 관리	전산자료 보유현황을 관리하고, 책임자를 지정·운영하는지 점검	
2	전산자료 접근통제	단말기와 전산자료의 접근권한이 부여되는 정보처리시스템 관리자/사용자에 대하여 적절한 통제장치를 마련·운영하고 적절히 통제를 수행하는지 점검	- 저장자료의 업무별·자료별 중요도에 따라 사용자의 접근권한/접근범위를 제한하고, 인가된 범위 이외의 자료접근 통제(외부 사용자는 최소한의 작업권한만 할당) - 전산원장, 주요정보 또는 이용자 정보 등이 저장된 정보처리시스템에 대한 관리자의 주요 업무 관련 행위는 책임자가 이중확인 및 모니터링 - IP·MAC 주소를 지정하여 관리용/사용자용 서비스 접속 단말 지정운영
3	접근계정 관리	개인별 사용자 계정 및 비밀번호를 부여하고, 이를 철저히 관리(등록, 변경, 폐기 등)하는지 점검	- 관리자/사용자 전출·퇴직 등 인사조치가 있을 때에는 지체 없이 해당 관리자/사용자 계정 삭제, 계정 사용 중지, 공동 사용 계정 변경 등 정보처리시스템에 대한 접근 통제 - 불가피하게 사용자 계정을 공동으로 사용하는 경우 개인별 사용내용의 기록 및 관리
4	전산 자료 및 장비 반출·입 통제	내부 직원의 전산 자료 및 장비에 대한 반출·입을 통제하는지 점검	- 전산자료가 저장된 시스템의 교체/반납/폐기/수리의뢰 시 자료유출, 훼손방지
5	보조기억매체 관리	정기적으로 보조기억매체의 보유현황 및 관리실태를 점검하는지 점검	- 점검 시 책임자 확인 포함
6	전산자료 안전지출 및 긴급파기 계획	비상시에 대비하여 보조기억매체 등 전산자료에 대한 안전지출 및 긴급파기 계획을 수립·운영하는지 점검	- 보조기억매체 파기 등 불용처리 시 정보복구가 불가능하도록 완전삭제 프로그램 등을 사용

번호	항목명	점검내용	비고
7	이용자 정보 사용 통제	이용자 정보의 조회·출력에 대한 통제를 하고 테스트 시 이용자 정보를 사용 금지하는지 점검	- 부하 테스트 등 사용이 불가피한 경우 이용자 정보를 변환하여 사용하고 테스트 종료 시 즉시 삭제
8	정보시스템 로그 기록 및 분석	정보처리시스템의 가동기록 등 로그를 1년 이상 보존하고, 정기적인 로그 분석을 수행하는지 점검	- 기록·유지 되어야 하는 로그 내용 · 정보처리시스템에 접속한 일시, 접속자, 및 접근을 확인할 수 있는 접근기록 · 전산자료를 사용한 일시, 사용자 및 자료의 내용을 확인할 수 있는 접근기록 · 정보처리시스템 내 전산자료의 처리 내용을 확인할 수 있는 사용자 로그인, 액세스 로그 등 접근기록
9	이용자 정보 보관 관리	단말기에는 원칙적으로 이용자 정보를 보관하지 아니하고, 수집/보관되는 이용자(고객) 정보는 선별하고 보호하는지 점검	- 불가피하게 단말기에 보관할 필요가 있는 경우 보관사유, 보관기간 및 관리 비밀번호 등을 정하여 책임자의 승인을 받아야 함 - 목적 외 고객정보 수집 및 활용 금지 - 적절한 고객정보 보호대책 마련(접근통제, 암호화 등)
10	핀패드(PIN pad) 등 보안장치 운영	전자금융거래 신청시 핀패드(PIN pad) 등을 사용하여, 이용자 비밀번호 노출을 방지하는지 점검	- 신청서에 비밀번호란 삭제 - 이용자 비밀번호는 핀패드(PIN pad) 등 보안장치를 이용하거나 이용자가 사후에 전자적 장치를 이용하여 직접 입력하는 방식으로 운영

바. 이상금융거래 방지대책

‘이상금융거래 방지대책’에 대한 3개의 점검항목을 예시한다.

<‘이상금융거래 방지대책’ 점검항목(예시)>

번호	항목명	점검내용	비고
1	이상금융거래 모니터링 및 탐지	이상금융거래를 판단할 수 있는 적절한 시스템을 갖추어 모니터링을 실시하고, 이상금융거래 발생 시 이를 탐지하는지 점검	
2	이상금융거래 탐지 시 대응	이상금융거래 시도가 탐지될 경우 적절한 대응방안을 마련하고 있는지 점검	- 대응방안의 예 · 추가 인증 수행 · 유선을 통한 상담원 확인 등
3	중요거래 고객통지	전자금융사고를 예방하기 위하여 비대면 전자금융거래를 허용하지 않는 계좌 개설 및 중요거래 정보에 대하여, 이용자가 희망할 경우 문자메시지 및 이메일 등을 통하여 통지하는지 점검	

사. 시스템 가용성 확보 및 비상대책

'시스템 가용성 확보 및 비상대책'에 대한 12개의 점검항목을 예시한다.

<'시스템 가용성 확보 및 비상대책' 점검항목(예시)>

번호	항목명	점검내용	비고
1	업무지속성 확보방안 수립	장애·재해·파업·테러 등 긴급한 상황이 발생하더라도 업무가 중단되지 않도록 다음 내용을 포함한 업무지속성 확보 대책을 수립하고, 확보대책의 실효성·적정성 등을 매년 1회 이상 점검하여 최신상태로 유지하고 관리하는지 점검 - 상황별 대응절차 - 백업 또는 재해복구센터를 활용한 재해복구계획 - 비상대응조직의 구성 및 운영 - 입력대행, 수작업 등의 조건 및 절차 - 모의훈련의 실시 - 유관기관 및 관련업체와의 비상연락체계 구축 - 보고 및 대외통보의 범위와 절차 등	- 업무지속성 확보대책에는 비상사태에 대비한 다음의 안전대책 반영 필요 · 파업 시 핵심전산업무 종사자의 근무지 이탈에 따른 정보처리시스템의 마비를 방지하기 위하여 비상지원인력을 확보·운영 · 비상사태 발생 시에도 정보처리시스템의 마비를 방지하고 신속히 원상복구가 될 수 있도록 정보처리시스템 운영에 대한 비상지원인력 또는 외부 전문업체를 활용하는 방안을 수립·운영 · 비상지원인력이 사용법을 충분히 이해하고 업무운영이 가능한 수준으로 전산시스템 운영지침서, 사용자매뉴얼 등을 쉽고 자세하게 작성하고 최신상태로 유지 · 핵심전산업무 담당자 부재 시에도 비상지원 인력이 업무를 수행할 수 있도록 비상지원인력에 대한 연수를 실시
2	위기대응행동 매뉴얼 수립 및 보고	금융위원회 지정 금융회사는 「금융전산분야 위기대응 실무매뉴얼」에 따라 위기대응행동매뉴얼(이외 금융회사·전자금융업자는 비상대책)을 수립하고 금융위원회에 보고하는지 점검	- 금융위원회가 별도로 지정하지 아니한 금융회사 또는 전자금융업자는 자연 재해, 인적 재해, 기술적 재해, 전자적 침해 등으로 인한 전산시스템의 마비 방지와 신속한 복구를 위한 비상대책을 수립 - 위기대응행동매뉴얼 또는 비상대책에는 업무지속성 확보대책 반영 필요
3	주요 전산장비 이중화	중앙처리장치, 데이터저장장치 등 주요 전산장비에 대하여 이중화 또는 예비장치를 확보하는지 점검	

번호	항목명	점검내용	비고
4	재해복구센터의 구축·운영	시스템 오류, 자연재해 등으로 인한 전산센터 마비에 대비하여 업무지속성을 확보할 수 있도록 적정 규모·인력을 구비한 재해복구센터를 주전산센터와 일정 거리 이상 떨어진 안전한 장소에 구축·운영하는지 점검	
5	재해복구전환 훈련 실시	재해복구센터를 운영하는 금융회사가 매년 1회 이상 재해복구센터로 실제 전환하는 재해복구 전환훈련을 실시하는지 점검	- 훈련 시 대상업무, 방법, 훈련주기, 실적 등 관리
6	비상대응훈련 실시 및 보고	위기대응행동매뉴얼 또는 비상대책에 따라 연 1회의 비상대응 훈련을 실시하고 그 결과를 금융위원회에 보고하는지 점검	- 재해복구전환훈련을 포함하여 실시 가능 - 훈련 시 대상업무, 방법, 훈련주기, 실적 등 관리
7	침해사고 대응 및 복구 훈련 실시	침해사고에 대한 대응능력 확보를 위하여 연 1회 이상 침해사고 대응 및 복구 훈련 계획을 수립·시행하고 그 결과를 침해사고 대응기관의 장에게 제출하는지 점검	- 훈련 시 대상업무, 방법, 훈련주기, 실적 등 관리
8	핵심업무 복구목표시간 설정	업무별로 업무지속성 확보의 중요도를 분석하여 핵심업무 선정 및 업무별 복구목표시간을 설정하는지 점검	- 금융회사의 핵심업무 복구목표시간 ; 3시간 이내 - 보험회사의 핵심업무 복구목표시간 ; 24시간 이내
9	백업·소산 관리	중요도에 따라 정보처리시스템의 운영체제 및 설정내용, 주요 자료 등을 정기 백업 및 원격 안전지역에 소산하고 백업자료는 1년 이상 기록·관리하는지 점검	- 주요 백업 전산자료는 정기적 검증 - 백업대상, 백업방법, 백업주기, 백업매체, 소산위치 등 적절히 설정하여 관리

번호	항목명	점검내용	비고
10	운영 및 개발 매뉴얼 작성	시스템 운영 및 개발에 대한 매뉴얼을 작성 및 관리하는지 점검	- 주요 정보처리시스템에 대한 구동, 조작 방법, 명령어 사용법, 운용순서, 장애조치 및 연락처 등을 명시 - 재해시 프로그램 및 기기 확보 방안 수립
11	모니터링 시스템 구축 및 운영	장애예방 및 성능 최적화, 정보처리시스템의 정상작동여부 확인 등을 위하여 시스템 자원 상태의 감시, 경고 및 제어 가능한 모니터링시스템을 구축하고 운영(정기분석 포함)하는지 점검	- 모니터링 시스템 구축 후 정기적인 시스템의 운영/사용 현황 및 추이 분석 - 시스템 이벤트에 대해서도 모니터링 및 관제 권고
12	적정 용량 산정 및 확보	정보처리시스템의 적정 용량을 산정하고, 산정된 용량을 확보하는지 점검	

아. 시스템 설치장소에 대한 물리적 접근통제

'시스템 설치장소에 대한 물리적 접근통제'에 대한 5개의 점검항목을 예시한다.

<'시스템 설치장소에 대한 물리적 접근통제' 점검항목(예시)>

번호	항목명	점검내용	비고
1	보호구역 설정	보호대상 시스템 설치장소(이하 주요시설)를 보호구역으로 설정하는지 점검	- 보호대상 시스템 설치장소(예 ; 전산센터 및 재해복구센터, 전산자료 보관실, 정보보호 시스템 설치장소, 보안관리가 필요한 정보처리시스템 설치장소 등)를 보호구역으로 설정
2	출입통제	주요시설에 대한 상시 출입문은 한 곳으로 하고, 인가된 자만 출입이 가능하도록 출입문에는 출입자의 신원확인을 통해 개폐되는 장치를 설치하며, 주요시설이 위치한 건물에는 24시간 경비업무를 수행하는 상근 경비원이 근무하는지 점검	- 출입문은 이중 안전장치로 보호하며 외벽이 유리인 경우 유리창문을 통하여 접근할 수 없도록 조치 - 사전 인가자 외 인원은 책임자의 승인을 받아 출입하도록 하며(내부 담당자 동행), 출입자 관리기록부에 기록(신원, 방문목적, 방문일시 등 기록)
3	출입 모니터링 및 기록관리	주요시설의 출입문과 전산실/통신장비실 내부는 CCTV를 설치하고, 출입기록(모든 출입자의 신원과 방문목적 및 방문일시에 대한 기록, CCTV녹화, 출입통제 장치의 로그기록)을 사고 시 추적이 가능하도록 일정기간 동안 보관하는지 점검	- CCTV카메라, 관제서버 등은 비인가자의 임의조작이 불가하도록 설치하고, 관련 망구성 시 별도의 망 운영 또는 전송구간 암호화(인터넷망 이용 시) 등 조치 - 중앙감시실을 통해 전산실/통신장비실 내 각 시설의 기능별 작동상황 및 사고발생 여부를 확인(중앙감시실에는 CCTV가 촬영한 영상을 24시간 감시할 수 있는 모니터 설치)
4	주요 정보시스템 보호	주요 정보시스템은 잠금장치가 있는 구조물(Rack)에 설치되는지 점검	
5	물리적 환경 관리	전산센터 운영기준에 적합한 환경관리 및 안전대책을 수립하고 있는지 점검	- 주요시설에 무선통신망 설치 금지 - 전력이중화, 소방설비, 방호설비, 자가발전설비, 항온항습기, UPS, 축전지설비, 비상조명, 유도등 등 운영 - 건물시공(내진, 난연재, 누수탐지, 방수시공, 무창구조) - 장애대비 유지보수계약 체결, 정기점검실시

Ⅴ. 자체 보안성심의 결과보고서

1. 결과보고서 구성

① 자체 보안성심의 결과보고서의 내용은 크게 '자체 보안성심의 개요'와 '자체 보안성심의 결과'로 구성된다.

② '자체 보안성심의 개요'에는 업무명, 업무적용일, 업무개요, 업무처리 절차, 담당자 등을 기술하며, '자체 보안성심의 결과'에는 보안성심의 기준별 심의결과 및 판단근거 등을 기술한다.

<「전자금융감독규정시행세칙」의 자체 보안성심의 결과보고서 붙임 양식>

(붙임1)

자체 보안성심의 개요

1. 업무명 : |

2. 업무적용일 : 20 년 월 일 완료

3. 업무개요

※ 서비스 목적, 대상 및 주요 내용을 기재

4. 업무처리 절차

※ 가입절차, 이용절차 등을 기재

5. 자체 보안성심의 결과

☐ 20 년 월 일 완료 ('붙임2. 자체 보안성심의 결과' 참조)

6. 담당자

소 속	직 위	이 름	담당업무	연락처	e-mail

(붙임2)

자체 보안성심의 결과

※ 보안성심의 기준별 심의 결과 및 판단근거 등을 상세하게 기재

※「전자금융감독규정시행세칙」의 <별지 제3호 서식> 중 (붙임 1), (붙임 2)

2. ‘자체 보안성심의 개요’ 작성

① 업무명

- 자체 보안성심의 대상 업무명을 기술한다.

② 업무적용일

- 자체 보안성심의 대상 업무가 제공 또는 시행될 일자를 기술한다.

③ 업무개요

- 서비스 목적, 대상, 주요 내용을 기술한다. 주요 내용 기술 시 업무에 대한 시스템 구성이 명확히 파악될 수 있도록 시스템 구성도를 포함한다.

④ 업무처리 절차

- 서비스 가입절차, 이용절차 등 업무처리 절차를 기술한다. 순서도(흐름도), 주요 UI 등을 적절히 포함하여 관련 절차가 명확히 파악될 수 있도록 기술한다.

⑤ 자체 보안성심의 결과

- 자체 보안성심의가 완료된 날짜를 명기하며, 세부적인 자체 보안성심의 결과는 ‘(붙임 2) 자체 보안성심의 결과’에 기술한다.

⑥ 담당자

- 자체 보안성심의 결과보고서의 내용에 대하여 답변할 수 있는 업무 담당자를 기술한다.

3. ‘자체 보안성심의 결과’ 작성

가. ‘자체 보안성심의 결과’ 작성 시 유의사항

① ‘자체 보안성심의 결과’에는 보안성심의 기준별 심의결과와 그에 대한 판단근거 등을 상세하게 기술하여야 하며, 심의결과는 정보보호최고책임자의 승인을 득해야 한다.

② 금융회사 자체 보안성심의 자료, 금융보안원 보안성검토 결과(해당 사항 있을 경우) 등 상세한 심의 관련 자료는 별도로 첨부하여 금융감독원에 제출한다.

나. ‘자체 보안성심의 결과’ 작성 예시

<자체 보안성심의 결과보고서 주요내용(예시)>

□ 자체 보안성심의 결과

심의기준	점검항목	점검내용	판단근거	최종결과
거래 당사자 인증	인증방법의 적절성	전자금융거래의 종류, 성격, 위험 수준 등을 고려하여 안전한 인증방법을 사용하는지 점검	지문인식 기반의 FIDO 인증을 구현하였고, FIDO alliance로부터 인증을 획득한 … (별첨 1 참조)	적합
	서비스 가입 시 이용자 인증	서비스 가입 시 적절히 이용자 인증이 실시되는지 점검	…	적합
	…	…	…	…
거래정보의 기밀성 및 무결성	거래정보 등의 기밀성	전자금융거래 이용자와 정보처리시스템 사이에 전송되거나 저장되는 전자금융거래정보 등 중요정보는 안전하게 암호화하여 기밀성을 보장하는지 점검	…	…
	…	…	…	…
…	…	…	…	…
시스템 설치장소에 대한 물리적 접근통제	보호구역 설정	보호대상 시스템 설치장소(이하 주요 시설)를 보호구역으로 설정하는지 점검	…	…
	출입통제	…	…	…
	…	…	…	…

(첨부)

□ 자체 보안성심의 결과요약

심의기준	점검항목	최종결과
거래 당사자 인증	인증방법의 적절성	적합
	서비스 가입 시 이용자 인증	적합
	…	…
거래정보의 기밀성 및 무결성	거래정보 등의 기밀성	적합
	거래정보 등의 무결성	적합
		…
정보처리시스템 보호대책	책임자 지정·운영	적합
	유지보수 관리	적합
	…	…
시스템 가용성 확보 및 비상대책	업무지속성 확보방안 수립	
	위기대응형동매뉴얼 수립 및 보고	
시스템 설치장소에 대한 물리적 접근통제	보호구역 설정	…
	출입통제	…
	…	…

위원장 000 (인)

위원 000 (인)
000 (인)
000 (인)

실무위원 000 (인)
000 (인)
000 (인)

① 자체 보안성심의 결과는 8가지 심의기준, 기준별 점검항목, 점검항목별 점검내용·판단근거·최종결과를 명시하는 형태로 서술할 수 있다.

- 판단근거 작성 시 내용이 많거나 별도의 추가자료가 포함된 경우 관련내용을 별도로 첨부할 수 있다.

② 자체 보안성심의 결과요약에는 심의기준별 점검항목에 대한 최종결과와 동 결과에 대한 보안성심의위원회의 위원장(정보보호최고책임자), 위원 등의 서명을 기재한다.

☞ **결과요약은 일반적으로 금융회사등의 보안성심의위원회의 심의·의결 과정에서 산출되는 문서로 회사별 양식 등을 활용할 수 있다.**

[참고자료 1] FAQ(Frequently Asked Questions)

1. 「금융회사 자체 보안성심의 가이드」의 목적 및 활용용도는?

○ 민간 중심의 자율적 보안체계를 지원하기 위하여 개발되었으며, 자체 보안성심의 체계 마련을 준비중인 금융회사등에 참고자료로 제공

○ 금융회사별로 상이한 업권 특성, 규모, 조직구성을 갖고 있고, 각 전자금융업무별로 다양한 특성이 존재하므로,

- 동 가이드의 내용을 일률적으로 적용하는 것은 부적절하며, 참고자료로 한정하여 활용하는 것이 바람직(회사별/업무별 특성을 반영한 응용 활용 권고)

○ 또한, 자율적 보안체계에 역행하는 타용도(감사 시 기준자료 등) 활용은 부적절

2. 금융보안원의 '보안성검토'와 금융회사의 '자체 보안성심의'와의 관계는?

○ 금융보안원은 금융회사등의 자체 보안성심의 등을 지원하기 위하여 신규 전자금융업무에 대한 보안대책의 적정성 여부를 검토하는 보안성검토 업무를 제공(2015.7~)

- 「전자금융감독규정시행세칙」 제3조제3항에 따라 금융보안원은 금융회사등의 의뢰 시 보안대책의 적성성 여부 등에 대하여 검토

○ 금융회사등은 금융보안원의 보안성검토 결과를 자체 보안성심의 시 참고자료로 활용할 수 있지만, 자체 보안성심의로 대체하는 것은 불가

- 「전자금융감독규정」 제36조에 따라 금융회사등은 신규 전자금융업무를 수행하고자 할 경우 자체 보안성심의를 실시(금융회사등의 의무)
- 보안성검토는 심의대상 업무전체에 대한 8가지 기준별 충족여부를 검토하기보다는 주로 금융회사등이 적용예정인 주요 신기술을 중심으로 발생가능한 보안문제 및 관련 보안대책의 적정성 여부를 비정형적으로 세부 검토

3. 「전자금융감독규정」상 자체 보안성심의 대상인 "신규 전자금융업무"의 구체적 의미는?

○ 「전자금융감독규정」 제36조에서의 '전자금융업무'란

- PG업, 에스크로업과 같이 전자금융업 등록 단위가 아닌 계좌이체, 멤버십 기능 추가, 본인인증 방식 추가 등 세부적 단위의 업무를 뜻함

○ 아래의 경우 새로운 서비스가 추가된다면 신규 전자금융업무에 해당

1. 신규로 전자금융업 중 하나를 등록하면서 약관도 제정하여 신고하는 경우
2. 기존 영위 중인 전자금융서비스 중 일부 서비스에 새로운 유형의 전자금융서비스를 추가하여 출시하는 경우
3. 기존 전자금융업으로 등록한 서비스 또는 금융회사가 제공중인 전자금융서비스와 동일 유형의 전자금융서비스를 추가로 출시하는 경우
4. 기존 전자금융업으로 등록한 서비스 또는 금융회사가 제공중인 전자금융서비스의 전자금융업무 유형을 유지하면서 관련한 서비스를 추가로 출시하는 경우
   (다만, 단순 메뉴 추가, 디자인 변경 등 신규성이 있다고 보기 어려운 경우에는 보안리스크가 상당히 증가할 때에만 신규성이 있다고 판단)
5. 기존 전자금융업으로 등록된 서비스 또는 금융회사가 제공중인 전자금융서비스의 일부 변경, 개편, 기능추가 등으로 신규 서비스가 추가되는 경우
   (다만, 단순 메뉴 추가, 디자인 변경 등 신규성이 있다고 보기 어려운 경우에는 보안리스크가 상당히 증가할 때에만 신규성이 있다고 판단)

○ 상기 내용은 금융규제민원포털(http://better.fsc.go.kr)의 법령해석 부분에 회신문(2016.01.12.) 형태로 게시됨

○ 다만, 자체 보안성심의 대상 여부를 결정하기 어려울 경우 금융감독원에 사전 문의

☞ 자체 보안성심의 대상인 "신규 전자금융업무"가 아닌 사례

- 금융회사가 차세대 시스템 구축 등 자체 인프라를 개선하는 경우
- 금융회사가 스마트워크(예 ; 포터블 브랜치) 등 임직원용 서비스를 오픈하는 경우
- 금융회사가 핀테크기업에게 Open API만 제공하고, 핀테크기업이 이를 바탕으로 신규 전자금융업무를 개시하는 경우(금융회사 또는 전자금융업자가 아닌 핀테크기업은 「전자금융감독규정」의 자체 보안성심의 조항에 적용받지 않음)

4. 자체 보안성심의를 수행해야 하는 경우와 자체 보안성심의 결과보고서를 금융감독원에 제출해야 되는 경우는? 각각의 상관관계는?

○ 금융회사등은 「전자금융감독규정」 제36조에 따라 결과보고서 제출과 관계없이 정보통신망을 이용하여 이용자를 대상으로 신규 전자금융업무를 수행하고자 하는 경우 자체 보안성심의를 실시하여야 함

○ 금융회사등은 상기 심의를 마친 후 신규 전자금융업무가 제공 또는 시행된 날부터 7일 이내에 금융감독원에 자체 보안성심의 결과보고서를 제출하여야 하지만, 아래의 해당하는 경우에는 그러하지 않을 수 있음

- 신규 전자금융업무가 제공 또는 시행된 날을 기준으로 과거 1년 이내에 전자금융사고가 발생하지 않은 기관으로서,

  ① 전자금융거래법 제28조에 따라 금융위원회로부터 허가를 받았거나 금융위원회에 등록한 날 및 전자금융업무를 신규로 수행한 날부터 1년이 경과한 '전자금융업자'

  ② 전자금융업무를 신규로 수행한 날부터 1년이 경과한 '금융회사'

[참고자료 2] 주요기술 관련 참고자료

자체 보안성심의 시 다음과 같은 주요기술 관련 자료를 참고할 수 있다.

<주요기술 관련 참고자료>

주요기술	관련자료	발행처
NFC	대면 거래에서의 전자서명 규격(2014.12월)	한국정보통신기술협회
IC카드	보안토큰 기반 공인인증서 저장형식 기술규격(2016.1월)	한국인터넷진흥원
	KLSC(Korea Local Smart Card) 규격(2009)	여신금융협회
	금융IC카드 보안토큰(공인인증서 기반 거래용) 규격(2008.4월)	한국은행
OTP	스마트OTP 연동 규격서 v5.0(2016.3월)	금융결제원
	일회용패스워드(OTP) 검증 서버 보안 요구사항(2011.12월)	한국정보통신기술협회
	일회용패스워드(OTP) 기반 전자금융 거래 검증 프로토콜(2011.12월)	한국정보통신기술협회
	일회용패스워드(OTP) 토큰 보안 요구 사항(2010.12월)	한국정보통신기술협회
모바일전자금융 (모바일 앱)	스마트폰 앱 보안 검증 절차 및 기준(2014.12월)	한국정보통신기술협회
	스마트폰 전자금융서비스 보안 가이드(2014.7월)	舊 금융보안연구원
	모바일 전자정부서비스 앱 소스코드 보안성 검증 안내서(2012.8월)	행정자치부
	앱 개발자를 위한 개인정보보호 안내서(2012.3월)	한국인터넷진흥원
가상화	서버 가상화 시스템 보안 관리 항목 및 세부 기능(2014.12월)	한국정보통신기술협회
	저장장치 가상화 시스템 보안 관리 항목 및 세부 기능(2014.12월)	한국정보통신기술협회
	서버 가상화 시스템 보안 요구사항(2013.12월)	한국정보통신기술협회
	저장장치 가상화 시스템 보안 요구사항(2013.12월)	한국정보통신기술협회

주요기술	관련자료	발행처
생체정보	바이오정보 연계 등 스마트폰 환경에서 공인인증서 안전 이용 구현 가이드라인(2016.5월)	한국인터넷진흥원
	금융서비스 바이오정보 인증관리 가이드라인(2016.2월)	금융보안원
	KS X ISO/IEC 24745 생체인식 정보보호(2014.12월)	국가기술표준원
	바이오인식 정보의 보호를 위한 기술적 관리적 지침(2013.12월)	한국정보통신기술협회
	바이오인식 정보 및 개인 식별 정보 데이터베이스의 분리 운영방법(2010.12월)	한국정보통신기술협회
FDS	이상금융거래 탐지시스템 기술 가이드(2014.8월)	舊 금융보안연구원
	이상금융거래 탐지 및 대응 프레임워크(2011.12월)	한국정보통신기술협회
암호기술	암호 키 관리 안내서(2014.12월)	한국인터넷진흥원
	금융부문 암호기술 활용 가이드(2014.12월)	舊 금융보안연구원
	암호정책 수립기준 안내서(2013.12월)	한국인터넷진흥원
	암호기술 구현 안내서(2013.12월)	한국인터넷진흥원
	암호알고리즘 및 키 길이 이용 안내서(2013.1월)	한국인터넷진흥원
보조기억매체	보조기억매체 이용 안내서(2010.1월)	한국인터넷진흥원
재해복구	금융회사 재해복구센터 구축·운영 가이드(2015.1월)	舊 금융보안연구원
	정보시스템 재해복구 지침(2007.12월)	한국정보통신기술협회

주요기술	관련자료	발행처
개발보안	소프트웨어 보안약점 진단가이드(2013.11월)	행정자치부
	홈페이지 SW(웹) 개발보안 가이드(2012.11월)	행정자치부
	시큐어코딩가이드(Java)(2012.9월)	행정자치부
	시큐어코딩가이드(C)(2012.9월)	행정자치부
	소프트웨어 개발보안가이드(2012.5월)	행정자치부
	Android-JAVA 시큐어 코딩 가이드(2011.9월)	행정자치부
	홈페이지 개발 보안 안내서(2010.1월)	한국인터넷진흥원
스마트워크	모바일오피스 정보보호 안내서(2013.12월)	한국인터넷진흥원
	스마트워크 활성화를 위한 정보보호 권고 해설서(2011.12월)	한국인터넷진흥원
	금융권 스마트워크 정보보호 가이드라인(2011.6월)	금융감독원
전산실	전산기계실 관리 지침(2007.12월)	한국정보통신기술협회
웹 서버	홈페이지 개인정보 노출방지 가이드라인(2012.7월)	행정자치부
	웹 서버 구축 보안점검 안내서(2010.1월)	한국인터넷진흥원
무선랜	무선랜 보안 안내서(2010.1월)	한국인터넷진흥원
DB	데이터베이스 보안 가이드라인(2014)	한국데이터베이스진흥원
VoIP	인터넷전화(VoIP) 보안 권고 해설서(2012.10월)	한국인터넷진흥원
	모바일 인터넷전화(mVoIP) 정보보호 안내서(2011.12월)	한국인터넷진흥원

업무참고 2016-융합보안-②-09

금융회사 자체 보안성심의 가이드

금융보안원
FINANCIAL SECURITY INSTITUTE