금융분야 개인정보보호 컴플라이언스 향상을 위한 지원 사례

2013. 12. 4

이성욱 팀장

금융보안연구원
Financial Security Agency

Contents

I 금융개인정보 유출 사고

II 금융권 개인정보보호 컴플라이언스 동향

III 금융부문 개인정보보호 컴플라이언스 관리방안

IV 금융부문 개인정보 처리업무 수탁업체 관리방안

I. 금융개인정보 유출 사고

I. 금융개인정보 유출 사고

1. 사고 사례 및 처리결과

회사	개인(금융)정보침해 사고 개요	피해 및 사고내용	처리 결과
은행	• 담당자 실수로 단체메일에 고객 3만여명의 이름, 이메일 등이 포함된 명단을 파일로 첨부해 발송('06)	• 유출 피해자 1,024명 손해배상 소송 제기	• 소송인 대상 배상금 지급 판결('07) -이름, 이메일 : 10만원 -주민등록번호 포함 시 : 20만원
은행	• 시중은행의 현금자동입출기(ATM)을 교체하면서 2천여만건의 개인금융 정보가 담긴 하드디스크 수백개를 중고상이 빼돌려 판매('11.2)	• 중고로 판매된 하드디스크에 저장된 약 1년까지의 저장 데이터(전자저널, 사진 등)	• ATM 운송 폐기업체 대표 이모씨를 불구속 입건 • 금융당국에서 저장매체에 수록된 고객정보 관리 강화 요청
캐피탈社	• 캐피탈의 관리 부실을 이용하여 고객 175만여명의 개인정보를 해킹하고 캐피탈을 협박('11.4)	• H캐피탈이 서버에 접속할 수 있는 ID, 비밀번호와 해킹방지시스템에 대한 관리를 부실하게 한 것이 주요 원인	• 해커 및 개인정보를 판 대부업체 직원 기소(실형 선고) • 금융당국으로부터 "기관경고"와 함께 정보기술・보안 담당 임원 3명에 대한 "감봉 3개월" 의 중징계
카드社	• 카드사 서버를 196회에 걸쳐 해킹해 47만 여건을 노트북 복사 후 일부 유출('11.8)	• 카드사 고객의 이름과 주민번호, 카드 번호 등 개인정보 192만 여건을 조회하고 이 가운데 47만 여건을 노트북에 옮기고, 이중 600여건을 텔레마케팅 업체에 넘김	• 개인정보 유출 혐의(신용정보의 이용 및 보호에 관한 법률 위반)로 고객관리 부서 박 모씨(34)에 대해 불구속 기소 • 금융당국에서 "기관주의"및 과태료 "600만원"을 부과
캐피탈社	• 고객 8,000여명의 개인정보와 신용 정보를 조회하고 유출한 임직원 적발 ('13.5)	• 개인정보처리시스템에 접속해 고객 정보를 조회하고, 고객의 성명· 휴대전화번호·회사명·신용등급 등이 담긴 정보를 별도 엑셀파일로 작성 한 후 회사 프린터 출력 또는 SNS를 통해 문자 또는 조회화면 사진파일을 제3자에게 전달(개인신용정보 516건, 개인식별정보 5,280건 등)	• 금융당국에서 "기관주의"및 과태료 "600만원"을 부과 • 사건에 관여한 직원 3명 '견책', 직원을 관리할 의무가 있는 임원 2명 '주의'의 제재조치

I. 금융개인정보 유출 사고

1. 사고 사례 및 처리결과

기타사항. 2013년 5월 해외 대규모 ATM 현금 인출 사고

- 뉴욕 연방경찰청은 지난해 12월 Ras Al-Khaimah PSC 국립은행과 올 2월 오만 무스카트 은행을 해킹해 전세계 20여개국 ATM에서 불법으로 4,500만 달러(한화 약 500억원)를 인출한 사이버 범죄자 7명을 금융사기 공모 및 돈세탁 등의 협의로 구속함
- 상대적으로 보안이 취약한 중동 은행을 대상으로 했으며 잔고와 인출한도를 조작하여 호텔키 또는 기한이 만료된 신용카드에 정보를 입력하여 카드를 배송하여 캐셔들이 인출함

I. 금융개인정보 유출 사고

2. 피싱 · 파밍 · 스미싱 등을 통한 금융정보 유출 사례

유사도메인을 이용한 피싱

▶ 사고 개요

- 실제 인터넷 뱅킹 사이트 도메인과 유사한 도메인 사용
- 이용자 ID와 주민등록번호, 전화, 계좌번호, 비밀번호 등을 순차적으로 입력하도록 유도
- 미국/중국/홍콩 등에 서버를 두고 있고 도메인 등록자 이름이 동일

▶ 시사점

- 실제 사이트와 유사한 도메인 사용
- 국내 금융기관 대상 피싱 공격

I. 금융개인정보 유출 사고

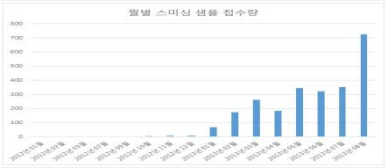
2. 피싱 · 파밍 · 스미싱 등을 통한 금융정보 유출 사례

➢ 가짜 은행사이트에 의한 피해 : SMS를 통한 "보안승급 요청 메시지 +인터넷 사이트 주소" 발송 등을 통한 피싱사이트 방문 유도

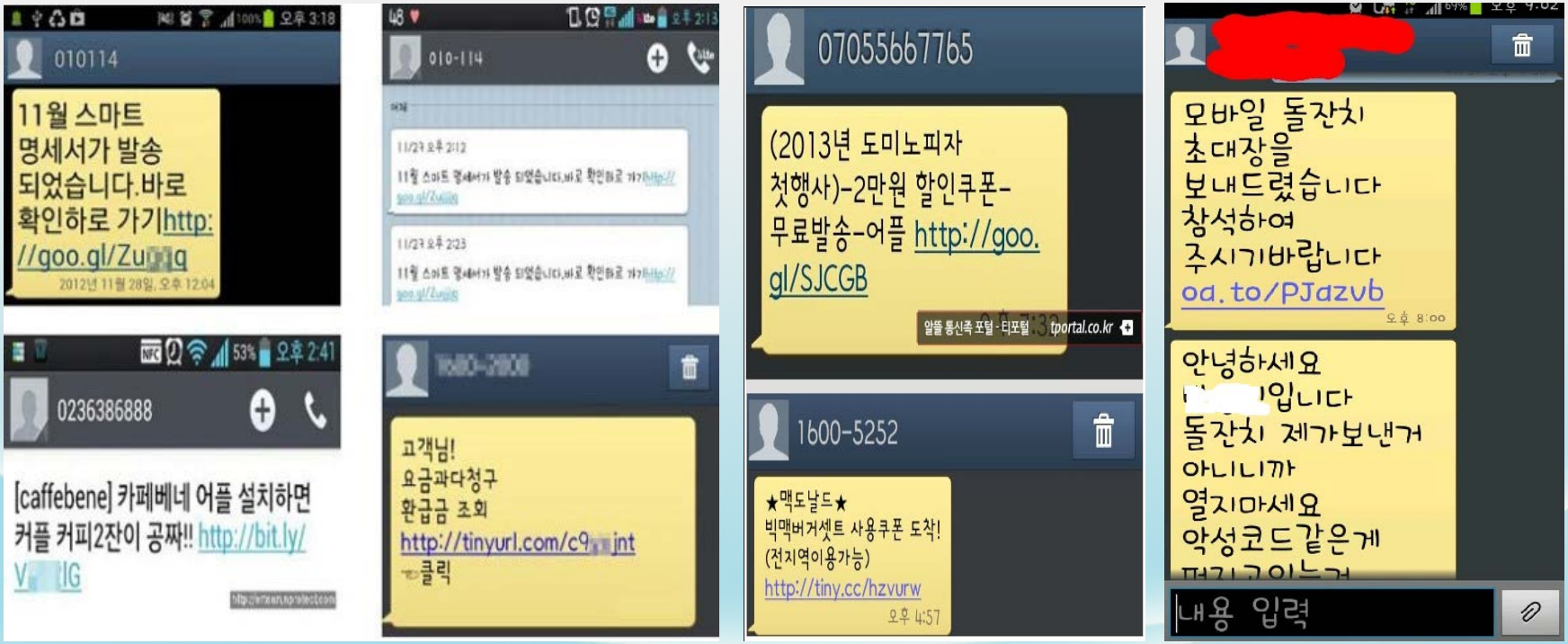
출처 : 2011.4.18 금융감독원 보도자료 ("가짜 은행사이트로 유도하는 문자메시지 조심하세요!")

I. 금융개인정보 유출 사고

2. 피싱 · 파밍 · 스미싱 등을 통한 금융정보 유출 사례



- 신종 스미싱 공격기법 출현 등 소액결제 피해 지속 발생
- 금융정보 유출 시도, 공인인증서 탈취 및 보안카드 번호 입력 유도
- 2012년 발견된 스미싱 악성코드 29개, 2013년 1월~8월까지 총 2,433 개 발견됨



I. 금융개인정보 유출 사고

3. 개인정보 침해로 인한 피해

기업 측면

▶ 개인정보 유출사고로 인한 2차 피해 발생으로 이용자의 정신적/금전적 피해 뿐만 아니라 해당 기업의 비즈니스 연속성에 큰 영향을 미침

개인정보 침해 집단 소송 현황

▶ K이동통신사 "5개월간 800여만명 고객정보 유출" 집단소송 진행중

▶ S사(N포털) 개인정보 유출 "20만원 배상" 위자료 지급 판결(2013. 2)
- 대규모 개인정보 유출사건에 따른 이용자의 정신적 피해를 인정한 첫 판결
- 판결 이후 해당 기업의 주가가 약 7% 이상 폭락

※ 3,500만명(유출 피해자) x 20만원 = 약7조(해당 기업 연 매출액(약 1,900억원의 35배)

▶ 진행 중인 H캐피탈(175만명), K통신회사(800만명)에 대입할 경우
- H캐피탈은 3,500억, K통신회사는 1조 6000억 추정

▶ 법원판결 : 해당 기업이 "일련의 행위들이 피고가 개인정보 보호 의무에 소홀했다는 것을 의미한다" 며 "개인정보 유출이 재산상 피해를 입혔다는 입증 자료는 없으나 개인정보가 회수되지 않았기 때문에 위자료 지급 책임을 면할 수 없다" 고 판결

I. 금융개인정보 유출 사고

3. 개인정보 침해로 인한 피해

금감원, 개인정보 허술 관리 금융회사 CEO에 주의

금감원, BS캐피탈 개인정보 허술 관리 CEO에 '주의' (증권일보/ 2013.09.03) | 기업 동향

2013/09/03 17:48

http://blog.naver.com/enewstock/80197374088 복사

전용뷰어 보기

대출모집인 711명에 개인정보 조회토록 해 말썽

여신전문회사 BS캐피탈이 대출모집인에게 개인신용정보를 부당으로 제공한 혐의로 금융당국으로부터 기관경고 및 CEO등에 대해 문책 조치를 받았다.

금융감독원은 최근 금융감독 보고서를 통해 BS캐피탈(주)에 대해 2012년 9월 10일에서 18일까지 부문검사를 실시한 결과, 대출모집인에 대해 고객의 개인신용정보를 부당 제공한 사실을 확인했다고 밝혔다.

여신전문금융업법 등 관련법규에 따르면 업체가 개인신용정보를 제3자에게 제공하려는 경우 고객에게 사전 동의를 받아야 하고, 신용정보전산시스템의 안전보호를 위해 개인신용정보 조회기록에 대한 구체적인 점검 방법 등이 포함된 기술적, 물리적, 관리적 보안대책을 수립 및 운용하도록 돼 있다.

하지만, BS캐피탈의 경우 이 같은 법규를 무시한 채 고객의 동의없이 대출모집인 711명에게 대출고객 4만2천608명의 개인신용정보를 조회할 수 있도록 신용정보전산시스템에 대한 조회권한을 부여한 것으로 드러났다.

이렇게 해서 2011년 10월 14일부터 2012년 9월 10일까지 대출고객 1만6천875명, 총 1만6천955건의 개인신용정보가 대출모집인 138명에게 부당하게 제공됐다는 것이 금감원의 발표다.

더욱 BS캐피탈 측은 신용정보관리 및 보호인이 대출모집인에 대한 개인신용정보 조회권한 부여 적정성과 대출모집인에 의한 개인신용정보 조회기록의 이상 유무 등을 점검해야 함에도 그렇게 하지 않은 것으로 나타났다.

이에 대해 BS캐피탈 측은 "모집인들이 조회한 정보는 연체 유무만을 확인할 수 있는 정보다"며 "지적 당시 조치해, 현재는 시정된 상태다"고 해명했다.

한편 이에 대해 금감원은 BS캐피탈에 대해 기관경고를 포함해 과태료 6억원을 부과하고 관련 직원에 대해서는 감봉 2명, 견책 1명, 주의 1명의 조치를 명령했다. 특히 이들 중에는 대표이사를 포함한 관련 임원도 포함된 것으로 알려졌다.

II. 금융권 개인정보보호 컴플라이언스 동향

II. 금융권 개인정보보호 컴플라이언스 동향

1. 컴플라이언스 이슈

- 개인정보보호법, 신용정보법, 정보통신망법 등 법률간 유사, 중복 등이 발생 가능

구분	신용정보법	정보통신망법	개인정보보호법
법률 성격	특별법	특별법	일반법
소관 부처	금융위원회	미래창조과학부	안전행정부
주요 적용 대상	신용정보 제공·이용자 등 (금융회사 등)	정보통신서비스제공자 등 (온라인 포털, 쇼핑몰 등)	공공·민간 사업자 (타 법률에서 정해지지 않은 모든 사업자)
용어	개인신용정보	개인정보	개인정보
기술적/관리적 조치 관련 기준	법 제19조 신용정보전산시스템의 안전보호	법 제28조 개인정보의 보호조치	법 제29조 안전조치의무
	동법 시행령 제16조 신용정보업 감독규정 제20조 (별표3)	동법 시행령 제15조 개인정보의 기술적·관리적 보호 조치 기준	동법 시행령 제30조 개인정보의 안전성 확보 조치 기준

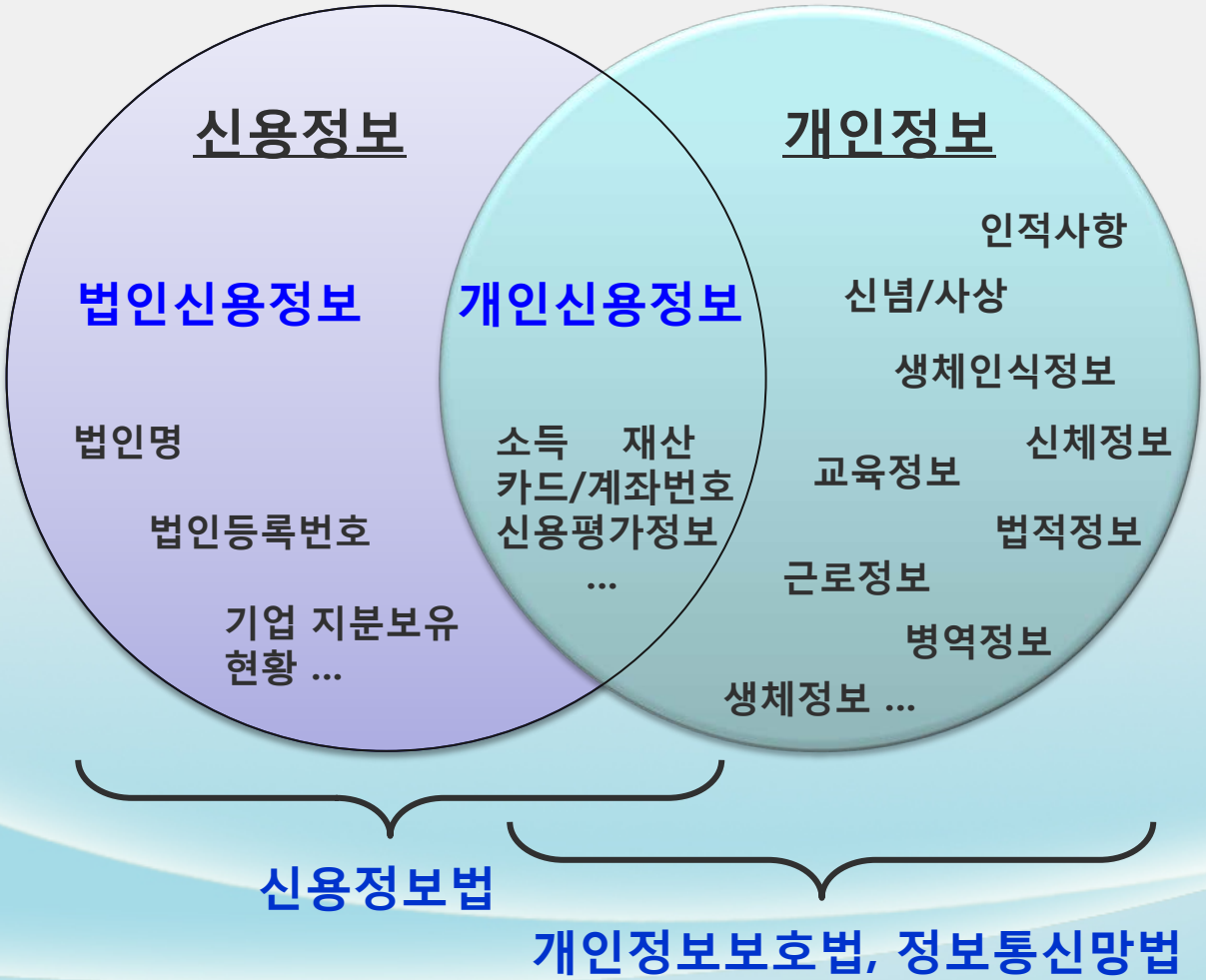
▶ **금융분야 개인정보보호 가이드라인에 따르면, 개인정보보호법, 신용정보법, 전자금융거래법 상 안전성 확보 조치 사항은 상당 부분 유사함**

- **상이한 부분 : 내부관리계획 수정이력 관리(개인정보보호법), 사용자 계정 공동사용 예외적 허용(전자금융거래법), 고유식별정보 내부망 저장시 암호화(개인정보보호법), 개인정보가 수록된 서류/USB 등을 잠금장치가 있는 안전한 장소에 보관(개인정보보호법) 등**
- **법률간 암호화 대상 및 보조저장매체 전달시 암호화, 비밀번호 일방향 암호화 적용 등도 상이**

II. 금융권 개인정보보호 컴플라이언스 동향

1. 컴플라이언스 이슈

신용정보 vs 개인정보



2. 금융부문 개인정보보호 컴플라이언스

개인정보보호 법령 및 지침 고시 해설(안행부, 2011.12)

▶ 개인정보보호 법령 및 지침 · 고시 해설에서는 개인정보보호법, 동법 시행령/시행규칙, 표준지침.고시의 적용기준을 제시하고 있음

▶ 타 법률과의 관계에서 금융 관련은 신용정보법, 정보통신 분야는 정보통신망법을 중심으로 비교 설명하고 있음
– 금융 개인정보보호 관련 법률로 신용정보법, 보험업법, 은행법, 금융실명거래법을 분류

금융 개인정보보호관련 법률	관련부처	제 · 개정일
신용정보의 이용 및 보호에 관한 법률	금융위원회(서민금융팀)	2011.9.30
보험업법	금융위원회(보험과)	2011.7.21
은행법	금융위원회(은행과)	2011.7.21
금융실명거래 및 비밀보장에 관한 법률	금융위원회(은행과)	2011.3.31

2. 금융부문 개인정보보호 컴플라이언스

개인정보보호 법령집(안행부/NIA, 2012.3)

▶ 일반법인 개인정보보호법 관련 법규 및 각 분야별 개인정보보호 관련 법률을 분류함

– 개인정보보호법의 경우 관련 지침.고시.규칙 등 관련 법규 소개

– 개인정보 법률을 12개 분야*로 관련 법령 분류

* 행정일반, 재정.경제, 교육학술, 형사.사법, 병역.보훈, 농림.수산, 산업.공정거래, 보건.복지, 노동, 국토개발.교통, 금융.신용, 정보통신

▶ 금융 · 신용 분야에서 개인정보보호 관련 법률로 다음과 같이 총 10개 법률로 분류함

금융·신용 분야 개인정보보호관련 법률	관련부처	제 · 개정일
공중 등 협박목적을 위한 자금조달 행위의 금지에 관한 법률	금융위원회(금융정보분석원)	2011.9.15
금융실명거래 및 비밀보장에 관한 법률	금융위원회(은행과)	2011.3.31
금융지주회사법	금융위원회(금융정책과)	2010.6.8
보험업법	금융위원회(보험과)	2011.7.21
상호저축은행법	금융위원회(중소금융과)	2011.7.21
신용정보의 이용 및 보호에 관한 법률	금융위원회(서민금융팀)	2011.9.30
여신전문금융업법	금융위원회(중소금융과)	2012.3.21
은행법	금융위원회(은행과)	2011.7.21
전기통신금융사기 피해금 환급에 관한 특별법	금융위원회(은행과)	2011.3.29
전자금융거래법	금융위원회(전자금융팀)	2012.6.1

II. 금융권 개인정보보호 컴플라이언스 동향

2. 금융부문 개인정보보호 컴플라이언스

금융회사 개인정보보호 자체점검 체크리스트(금감원 개인정보TF, 2012.9)

▶ 개인정보보호 자체점검 체크리스트에서는 개인정보보호법 및 동법 시행령, 표준 지침, 안전성 확보조치 기준 고시를 반영하여 금융회사의 개인정보 자체점검 시 도움을 주기 위해 작성됨

– 개인정보의 Life Cycle에 따라 아래와 같이 4개 단계, 35개 점검항목으로 구성

금융회사 CCTV 설치 · 운영시 유의사항(금감원 개인정보보호T/F, 2013.4)

▶ 개인정보보호법 시행(2011.9.30)으로 CCTV 설치.운영에 대한 의무사항이 크게 강화되었으며, 안전행정부는 「민간분야 영상정보처리기기 설치.운영 가이드라인」을 마련하여 인터넷에 공개(2012.12월)

▶ 이와 관련하여 금융회사가 CCTV 설치.운영 시 유의하여야 할 사항을 안내하고자 함

▶ 11개 주요항목, 20개 체크리스트로 구성됨

2. 금융부문 개인정보보호 컴플라이언스

금융분야 개인정보보호 가이드라인(2013.7)

발간 배경

▶ 개인정보 보호에 대한 사회적 요구 증가

- 개인정보의 오.남용이나 해킹 등을 통한 유출 사건이 발생함에 따라 개인정보 보호 강화를 위한 「개인정보 보호법」제정(2011.9.30일 시행)

▶ 금융기관의 개인정보 보호를 위한 명확한 기준 제시 필요

- 기존 금융관련 법령과 중첩되는 내용이나 새롭게 적용되는 내용 등과 관련하여 금융업 담당자들의 실무상 혼란을 방지할 수 있도록 명확한 기준을 제시할 필요

발간 목적

▶ 금융업무 담당자의 개인정보 처리 지원

- 관계 법령의 제정 취지 및 내용, 업종별 특수성 등을 종합적으로 고려, 금융업 담당자가 실무에 참고할 수 있는 개인정보 처리 기준 제시

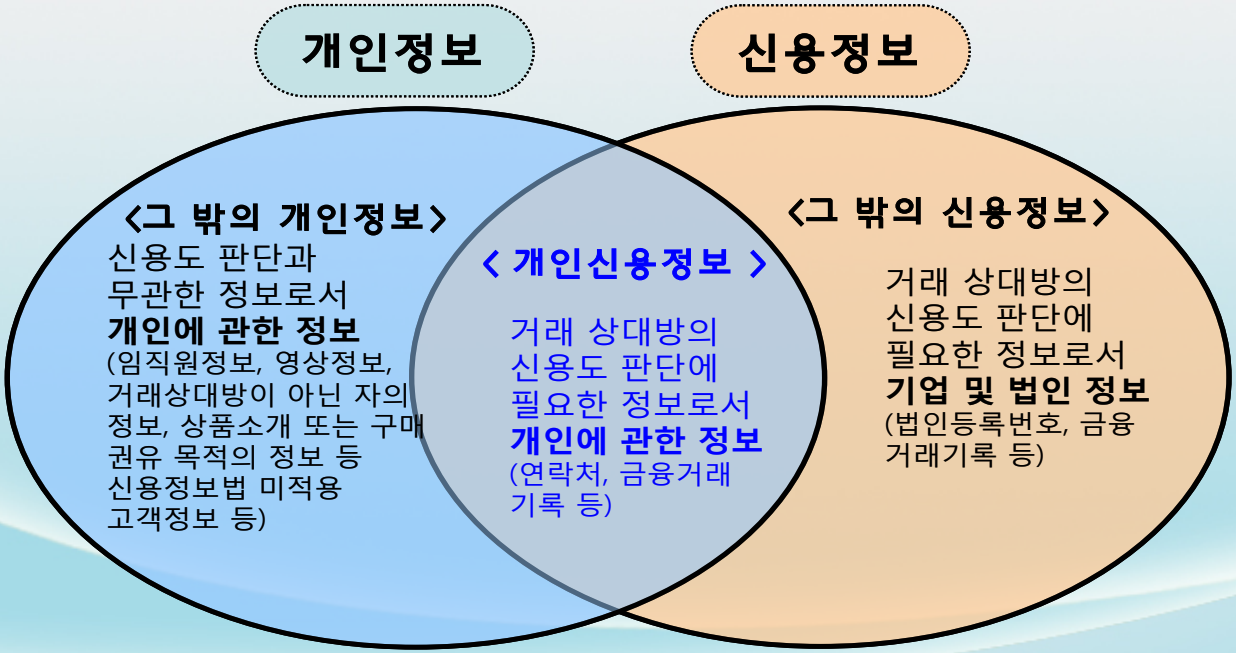
▶ 개인정보보호법 조기 정착

- 은행, 보험, 증권 등 금융 분야의 단계별 개인정보 처리 기준 및 유의사항을 관련 질의응답 사례 등을 통해 이해하기 쉽게 설명

2. 금융부문 개인정보보호 컴플라이언스

금융분야 개인정보보호 가이드라인(2013.7)

- ▶ 가이드라인 적용 대상 : 금융회사
- ▶ 발간부처 : 금융위원회, 금융감독원, 안전행정부
- ▶ 관련법 : 신용정보법, 전자금융거래법, 개인정보보호법
- ▶ 신용정보법과의 관계



<개인신용정보>와 <그 밖의 개인정보>를 포함하여 이하 "개인(신용)정보" 라 함

2. 금융부문 개인정보보호 컴플라이언스

금융분야 개인정보보호 가이드라인(2013.7)

▶ 법률 적용 원칙

○ 개인신용정보

- 신용정보법을 우선 적용하고 신용정보법에 규정되어 있지 않은 사항은 개인정보보호법을 적용하되, 전자금융거래법, 금융실명법 등 개별법에서 특별히 정하는 사항에 대해서는 해당 법률 적용

○ 개인신용정보를 제외한 개인정보 (그 밖의 개인정보)

- 금융실명법, 은행법 등 개별 법률에서 특별히 정하는 사항*을 우선 적용하고, 특별히 정하지 않은 사항에 대하여는 개인정보보호법 적용

* (예시) 금융실명법(§3), 은행법(§35의5), 자본시장법(§189), 금융지주회사법(§48의2) 등

○ 신용정보 중 기업 · 법인에 관한 정보 (그 밖의 신용정보)

- 신용정보법을 우선 적용하되, 신용정보법 미적용 업종은 개별 법률 적용

※ 신용정보법은 신용정보제공이용자, 신용정보집중기관 및 신용정보회사에 대하여 적용

2. 금융부문 개인정보보호 컴플라이언스

금융회사의 개인정보문서 관리 유의사항(2013.8)

▶ 금융회사의 개인정보 중 종이와 같은 출력물 형태 문서 유출 방지를 위한 유의사항으로서 아래 3개의 주요 항목으로 구분됨 (금융감독원, 13. 8.2)

- 종이문서의 관리절차
  - 내부관리계획(법§ 29, 영§ 30, 고시§ 3) 및 개인정보처리방침 (법§ 30,영§ 31,지침§ 37)
  - 종이문서의 안전관리 (고시§ 10)
- 종이문서의 파기 절차 준수
  - 파기의 시점 (법§ 21, 영§ 16조, 지침§ 11①)
  - 파기 방법 및 절차 (영§ 16, 지침§ 11②~⑤)
- 종이문서의 위탁관리 강화(법§ 26①, 법§ 26②, 법§ 26④, 영§ 28①, 영§ 28②, 영28§ ⑥, 지침§ 19①)

※법 : 개인정보보호법, 영 : 개인정보보호법 시행령, 고시 : 개인정보의 안전성 확보조치 기준 고시, 지침 : 표준개인정보보호지침

※ 붙임으로서 개인정보보법령 및 관련 규정·고시·지침을 정리한 자체점검 체크리스트* 제공

*금융회사의 개인정보문서 관리 자체점검 체크리스트(금감원, '13. 8.2)

II. 금융권 개인정보보호 컴플라이언스 동향

2. 금융부문 개인정보보호 컴플라이언스

금융회사의 개인정보 처리시 유의사항 발표 (2013.9, 금감원)

▶ 금융회사 개인정보보호 실태에 대한 점검 결과, 주요 위반사항 내용

- 마케팅 목적의 개인정보 수집 시 미동의로 인한 서비스 거부
- 개인정보 처리 위탁계약서에 필수기재사항 누락
- PC에 보관된 개인정보파일에 안전성 확보조치 미흡
- 자동화기기 CCTV로 계좌번호 및 비밀번호를 촬영 · 보관
- 개인정보문서 파기 시 수탁업체에 대한 관리 소홀 등

온라인상 주민번호 수집·이용 최소화 모범사례 (2013.10, 금감원)

▶ 금융권역별 의견을 수렴하여 마련한 온라인상 주민번호 대체가 가능한 모범사례 제공

- 금융서비스와 관련이 적은 서비스의 경우, 아이핀(i-PIN), 휴대폰 인증 등을 이용한 본인확인 방법으로 주민번호 사용을 대체

2. 금융부문 개인정보보호 컴플라이언스

금융회사의 개인정보보호 자가진단·조치 매뉴얼 (2013.11, 금감원)

▶ 금융회사에서 개인정보보호 업무 관련 **자가진단 및 조치**에 유용하게 활용할 수 있는 **자가진단 체크리스트가 포함된 업무 매뉴얼**을 마련하여 배포

- 개인정보보호제도 시행에 따른 자율규제의 강화를 위한 자료로 활용
- 개인정보보호 업무 일반(관리체계 구축, 처리단계별 보호기준 준수, **위탁업체 관리 강화**, 암호화 등 안전성 확보조치 마련, 개인정보취급자에 대한 교육 강화)
- CCTV 설치운영(설치운영 제한, 설치 운영 금지, 임의조작/녹음 금지, 안내판 설치, 운영/관리 방침 수립, 관리책임자 지정, **목적외 이용 및 제3자 제공**, 보관 및 파기, **설치/운영 위탁**, 설치/운영에 대한 점검 등)
- 개인정보문서 관리(관리절차 마련, 파기절차 준수, 위탁관리 강화)
- 개인정보 유출시 조치방법(5일이내 통지 또는 홈페이지 고지, 1만명 이상 유출된 경우 5일이내 안행부(KISA)에 신고, **금융위/금감원에 사고보고 등**)

III. 금융부문 개인정보보호 컴플라이언스 관리방안

(금융개인정보보호 컴플라이언스 참조가이드)

III. 금융부문 개인정보보호 컴플라이언스 관리방안

1. Silo Approach(개별 접근 방식) Problems

- ◆ 많은 비용 소모
  - 컨설턴트들이 특정 분야에서 대해서만 전문성을 지니고 있어, 여러 분야의 Compliance 요구사항을 적용하는 기업은 많은 비용이 들어감
- ◆ 전반적인 Compliance에 대한 효과성 측정이 어려움
  - Compliance 활동의 중복성 및 불일치가 발생할 가능성이 높으며, 통합화된 감시가 어려움

III. 금융부문 개인정보보호 컴플라이언스 관리방안

2. Unified Approach(통합 접근 방식)

개요

- ▶ Network Frontiers LLC와 Latham & Watkins LLP(law firm)가 공동으로 2005년 최초 개발하였으며, 전 세계 법규, 표준 및 우수 사례를 분석하여 IT통제에 대한 단일 매트릭스 개발을 목표로 시작
- ▶ 현재 전 세계 500여개 법규 및 표준에 대해 분석함
- ▶ Microsoft, CA, OpenPages 등 많은 회사들이 라이센스 계약을 체결하여 GRC 솔루션에 콘텐츠로 활용하고 있음

주요 내용

▶ 중복사항 매핑
- 주요 법규 또는 표준 기준으로 다른 법규 또는 표준들이 공통으로 갖고 있는 통제들을 매핑

▶ 통제 리스트 작성
- 조직과 관련 있는 법규 및 표준을 선택하여 이를 기준으로 조직의 통제 리스트를 생성

▶ 상충되는 부분 명확화
- 각 법규 및 표준이 요구하는 사항이 중복되는 부분에 대해 여러 전문가들의 의견을 참조하여 의사결정을 진행함

III. 금융부문 개인정보보호 컴플라이언스 관리방안

3. 컴플라이언스 통합 프레임워크 연구

연구 추진 배경 및 목적

추진배경

- ▶ 다양한 금융부문 정보보안 컴플라이언스의 중복 적용
- ▶ 금융부문 정보보안 체크리스트 일원화 필요
- ▶ 금융부문별 정보보안 적용 수준의 차이 발생

추진목적

- ▶ 금융회사의 정보보호 규제 준수 여부 확인 및 보안관리 강화
- ▶ 금융회사 정보보안 컴플라이언스 관리의 효율성 제고 및 비용절감
- ▶ 금융 부문별로 적합한 컴플라이언스 자가진단도구 개발

III. 금융부문 개인정보보호 컴플라이언스 관리방안

3. 컴플라이언스 통합 프레임워크 연구

◆금융권에서 많이 적용되는 법률, 표준, 기준 등을 중심으로 상관관계 분석

금융권 정보보안 규제의 중점 분석

국내외 기준	보안관련 규제	금융관련 규제	기타 규제
▶ISO27001	▶정보보호안전진단	▶전자금융거래법	▶국가정보화 기본법
▶KISA ISMS	▶정보통신망법	▶금융실명거래법	▶전자정부법
▶PCI-DSS	▶개인정보보호법	▶전자서명법	▶장애인차별금지법
▶Basel II	▶정보통신기반보호법	▶신용정보이용보호법	▶전자상거래 소비자보호법
▶SOX		▶전자거래기본법	
		▶자본시장금융투자법	

IT컴플라이언스 항목 도출

정보보안 관련 통제의 분류 및 상관관계 분석

4. 금융IT 보안 컴플라이언스 참조가이드 개발(2012)

개발 배경

▶ 금융회사가 직면한 다양한 보안 규제(전자금융감독규정·모범규준, 타법률 등)에 대해 보다 체계적으로 컴플라이언스 활동을 지원할 수 있는 참조 가이드 개발

필요성

▶ 보안 위협이 증가함에 따라 금융당국은 정보보호 강화 정책의 일환으로 관련 법규 개정 작업을 통해 금융IT 보안 컴플라이언스 통제를 강화

▶ 금융회사에 필요한 금융IT 보안규제 사항을 중심으로 각 규제 사항을 이해하는데 참고할 수 있도록 전자금융거래법 중심의 『금융IT 보안 컴플라이언스 참조 가이드』를 개발

4. 금융IT 보안 컴플라이언스 참조가이드 개발(2012)

도메인/통제항목

▶ 금융IT 보안 컴플라이언스 통제항목은 11개 도메인, 47개 세부도메인, 204개 통제 항목

분석 대상		영역 구분	도메인 구성
전자금융 감독법규	전자금융거래법 전자금융거래법 시행령 전자금융감독규정 전자금융감독규정 시행세칙 IT부문 보호업무 모범규준 전산장비 내부통제 모범규준 취약점 분석 · 평가 기준 가이드라인	관리적 기술적 물리적	1. 정보보호 정책 2. 정보보호 조직 3. 인적보안 4. 물리적 · 환경적 보안 5. 운영관리 6. 전산장비 내부통제 및 접근통제 7. IT 도입개발유지보수 관리 8. 업무연속성관리 9. 전자금융거래 보안 10 외부주문 보안 11. 보안사고 대응
컴플라이언스 참고 참고	전자금융감독규정 해설 정보보호관리체계인증 등에 관한 고시 개인정보보호관리체계 PCI DSS 2.0 ISO/IEC 27001:2005 바젤 II 下의 통합리스크관리 모범규준		

4. 금융IT 보안 컴플라이언스 참조가이드 개발(2012)

참조가이드 구성

보안영역	도메인	세부 도메인	통제 항목	통제 내용
관리적 보안	정보보호정책 정보보호 조직 인적보안 업무연속성 관리 외부주문보안	47개 도메인	204개 통제 항목	통제항목 가이드
기술적 보안	운영관리 전산장비 내부통제 및 접근통제 IT 도입·개발·유지 보수 관리 전자금융거래 보안 보안사고 대응			타법률 참고사항
물리적 보안	물리적·환경적 보안			국내외 표준 참고사항

전자금융거래법, 전자금융감독규정, 모범규준 등

5. 금융개인정보보호 컴플라이언스 참조가이드 개발(2013.11)

개발 배경

▶ 금융권에 적용되는 개인정보보호 관련 법규 사항을 조사·분석하고, 각 규제사항을 이해하는데 참고할 수 있는 다양한 정보를 제공하기 위해 컴플라이언스 참조가이드 개발

필요성

▶ 각종 고객 개인정보 유출사고 등으로 인하여 개인정보보호법 등 관련 규제 강화

▶ 신용정보법, 금융실명제법 등 개인정보와 관련된 법률과의 중복, 상충 등 이슈 존재

▶ 개인정보와 신용정보(이하 개인정보) 보호를 위해 다양한 법규에서 요구하는 법률적 사항들을 분석하여 관련 도메인/통제항목을 도출 후 금융회사에서 관련 법규 및 정보를 쉽게 참조가 가능한 『 금융개인정보보호 컴플라이언스 가이드 』 개발

5. 금융개인정보보호 컴플라이언스 참조가이드 개발(2013.11)

도메인/통제항목

▶ 개인정보보호법 및 신용정보법을 중심으로 9개 도메인 **84개의 통제항목** 작성

금융개인정보보호 컴플라이언스 참조가이드

도메인 및 통제 항목(9개 도메인, 84개 통제)

1. 정책(3개) 2. 조직 및 책임(3개) 3. 인적보안(2개) 4. 영상정보 처리기기의 보안(5개) 5. 위수탁 보안(6개) 6. 보안사고 대응(4개)
7. 안전성 확보조치(8개) 8. 처리단계별 보호(38개) 9. 정보주체의 권리보장(15개)

통제항목가이드

- 금융분야 개인 정보보호 가이드라인
- 개인정보자체점검체크리스트
- 개인정보보호법령 및 지침고시 해설서
- 개인정보의 안전성확보조치 기준 고시 및 해설서
- 개인정보 위험도 분석 기준 및 해설서
- 개인정보 암호화 조치 안내서
- 개인정보 영향평가고시 및 해설서
- 개인정보영향평가 수행안내서

금융관련 특별법

- 전자금융거래법
- 금융실명제법
- 금융지주회사법
- 은행법
- 자본시장법
- 보험업법
- 여신전문금융업법
- 상호저축은행법
- 공중 등 협박목적을 위한 자금조달 행위 금지법
- 전기통신금융사기 피해급 환급에 관한 특별법
- 금융기관의 업무 위탁등에 대한 규정

기타 타법관련

- 정보통신망법
- 위치정보법
- 통신비밀보호법
- 인터넷주소자원에 관한 법률
- 근로기준법
- 국세기본법
- 주민등록법
- 전자서명법
- 국가인권위원회법
- 소비자기본법
- 전자거래기본법
- 전자상거래법
- 전자어음발행유통법
- 외부감사에 관한 법률
- 외국환거래법

국내외 표준

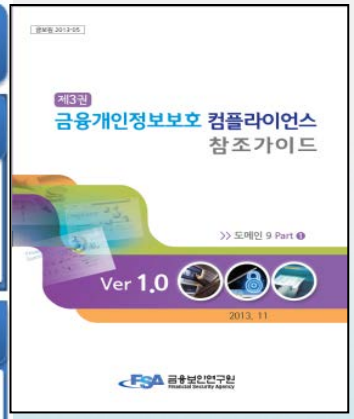
- PCI DSS Ver2.0
- ISO 27001
- 정보보호관리체계 인증 (K-ISMS)
- BASEL Ⅲ
- 개인정보보호관리체계인증 (PIMS)

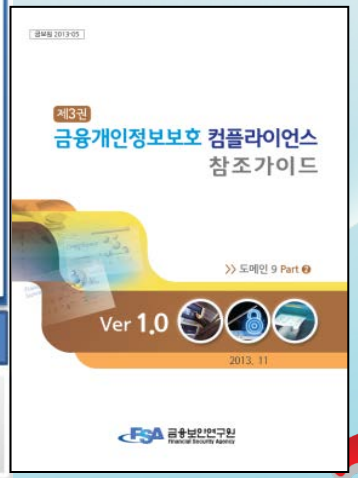
개인정보보호법

- 동법 시행령, 시행규칙
- 표준 개인정보보호 지침
- 개인정보의 안전성 확보 조치

신용정보법

- 동법 시행령, 시행규칙
- 신용정보감독규정
- 신용정보감독업무 시행세칙





5. 금융개인정보보호 컴플라이언스 참조가이드 개발(2013.11)

참조가이드 내용

가 — 도메인 | 도메인명 | 개인정보보호법 | 신용정보법

나 — 통제사항

통제번호	통제항목
	통제항목 내용
아 래	

다 — 근거 법규

관련근거

신용 정보법	동법 시행령	동법 시행규칙	신용정보 감독규정	동 규정 시행세칙
개인정보 보호법	동법 시행령	동법 시행규칙	안전성 확보 조치 고시	표준개인정보 보호 지침

라 — 참조 내용

요 약

마 — 1. 용어정의

바 — 2. 통제항목 가이드

사 — 3. 금융 관련 특별법 참고 사항

아 — 4. 기타 타 법률 참고 사항

자 — 5. 국내외 표준 참고사항

구 분	내 용
가. 도메인 및 적용법률 분류	도메인 이름과 관련 개인정보보호법 및 신용정보법 분류 등을 표현
나. 통제 사항	각도메인별 통제항목과 통제 내용 등을 표현
다. 근거 법규	통제항목이 근거하고 있는 개인정보보호법 및 신용정보법을 비교 분석
라. 요약	주요 참조 사항 및 해당 내용에 대한 요약 설명
마. 용어정의	관련 통제의 주요 단어에 대한 근거 법규 용어정의 인용
바. 통제항목 가이드	금융당국 및 중앙행정기관(안전행정부 등) 공식적인 문서(해설서, 가이드 등) 비교 분석
사. 금융관련특별법참고사항	금융 관련법내 개인정보보호 관련 내용 비교 분석
아. 기타 타 법률 참고 사항	타 분야에서 관련 참고 내용 비교 분석
자. 국내외 표준 참고사항	ISO27001, K-ISMS 등 국내외 표준 내용 비교 분석

IV. 금융부문 개인정보 처리업무 수탁업체 관리방안

Ⅳ. 금융부문 개인정보 처리업무 수탁업체 관리방안

1. 법률 요구사항 및 현황

□ 개인정보보호법 제26조 제4항에 따른 수탁자 감독 및 교육

<개인정보보호법 제26조제4항>
위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실 · 도난 · 유출 · 변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

- 금융회사는 업무 특성상 많은 수탁사업자*와 계약(최소 수십개 회사)
  * DM업체, 신용정보회사, (위탁회사 통제 하의)공동 전산개발 및 유지 지원 업무 등
- 금융회사간의 업무 위수탁 관계*도 존재, 금융회사가 제3자로 부터 업무 수탁 받는 경우**
  * 제휴 현금카드 발급업무 , 계좌개설 관련 자료 관리업무, 증권계좌 개설대행 업무 위탁 등
  ** 은행의 아파트 관리비 수납 대행업무, 각종 공과금 수납 대행업무 등
- 다수의 회사와 계약을 맺은 수탁사업자는 다수의 회사로부터 감독 및 교육을 받아야 함

Ⅳ. 금융부문 개인정보 처리업무 수탁업체 관리방안

2. 대응 현황

□ 개인정보 관련 업무 수탁자 감독

▶ 금융회사별 수탁자에 대한 개별 점검 수행(업무 부담)

- 금융보안연구원에서 "개인정보 수탁업체 안전성 점검 체크리스트" 작성 및 제공
- 금융회사 점검 수행자 대상 점검 방법 등 교육 수행(요청시)
- 향후 금융권에서 공동으로 계약하고 있는 대규모 수탁업체(신용정보회사 등)에 대한 합동 점검 등의 효율적인 방안 마련 필요

□ 개인정보 관련 업무 수탁자 교육

▶ 공동/개별 수탁자 교육 수행

- (금융회사간 업무위수탁 관계에 있는 금융회사 대상)금융권 수탁업무 관련 개인정보 보호 교육 수행(2013.5, 금감원, 안행부, 금보원 참여), 하반기(2013. 10) 추가 교육
- 일부 금융회사에서는 수탁업체 대상 자체 교육 수행(업무 부담)
- 2014년도에는 금융회사와 수탁관계가 있는 비금융회사 대상 교육 진행 예정

IV. 금융부문 개인정보 처리업무 수탁업체 관리방안

2. 대응 현황

개인정보 수탁업체 안전성 점검 체크리스트

영역	세부 영역	문항수
관리적	계약사항의 검토, 이행, 개선	3
	내부관리계획의 수립 및 시행	2
기술적	접근권한의 관리	3
	사용자계정 및 비밀번호 관리	2
	비인가 사용자 접근통제	4
	개인정보 암호화	5
	접근기록의 보관	2
	보안프로그램 설치 및 운영	2
물리적	물리적 접근통제	1
	중요정보 보관관리	1
합 계		25

※ 점검항목은 당일(1일) 점검이 수행이 가능 하도록 구성

- 점검문항은 '개인정보의안전성확보조치 기준고시' 와 관련 규정을 기준으로 작성
- 관리적, 기술적, 물리적 영역으로 구분
- 관리적 점검문항 5개 항목, 기술적 점검문항 18개 항목, 물리적 점검 문항 2개 항목으로 구성
- 관리적 영역은 계약 이행 및 내부관리계획 수립 및 관리, 기술적 영역은 시스템 접근통제 및 관리 영역에 대한 점검을 주요 목적으로 함,
- 물리적 영역은 주요 통제구역의 인력 및 주요자산의 접근통제와 중요정보의 물리적 보관관리를 주요 점검 목적으로 함

Ⅳ. 금융부문 개인정보 처리업무 수탁업체 관리방안

3. 업무 제휴, 위탁 등 외부 주문 관련 기타 이슈

전자금융보조업자 안전성 합동 점검

배 경

□ **전자금융감독규정 제60조(외부주문등에 대한 기준)** ① 금융기관 또는 전자금융업자는 전자금융거래를 위한 외부주문등의 경우에는 다음 각 호의 사항을 준수하여야 한다.

10. 전자금융보조업자에 대한 **재무건전성을 연1회 이상 평가**하여 재무상태 악화에 따른 도산에 대비하고 전자금융보조업자의 주요 경영활동에 대해 상시 모니터링을 실시
11. 전자금융보조업자가 제공하는 **서비스의 품질수준을 연1회 이상 평가**할 것
14. 외부주문등은 자체 보안성검토 및 **정기 보안점검 실시**

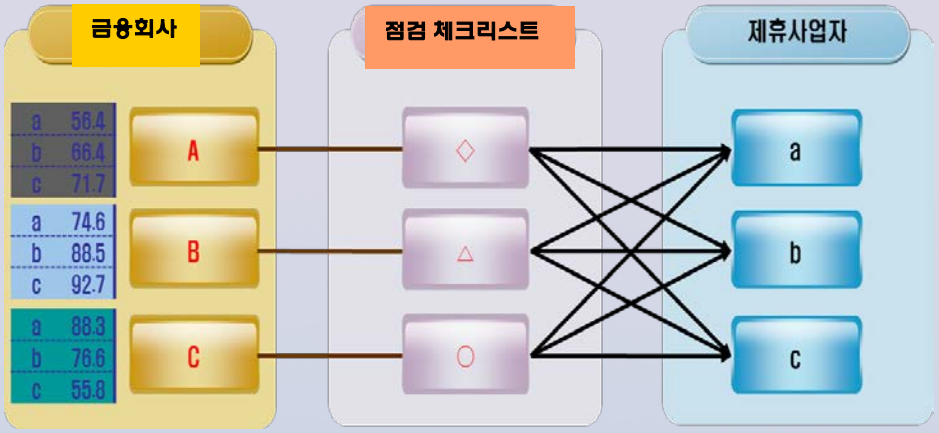
② 금융기관 또는 전자금융업자는 제1항제10호 및 제11호의 평가결과를 **금융감독원장에게 보고**하여야 한다.

IV. 금융부문 개인정보 처리업무 수탁업체 관리방안

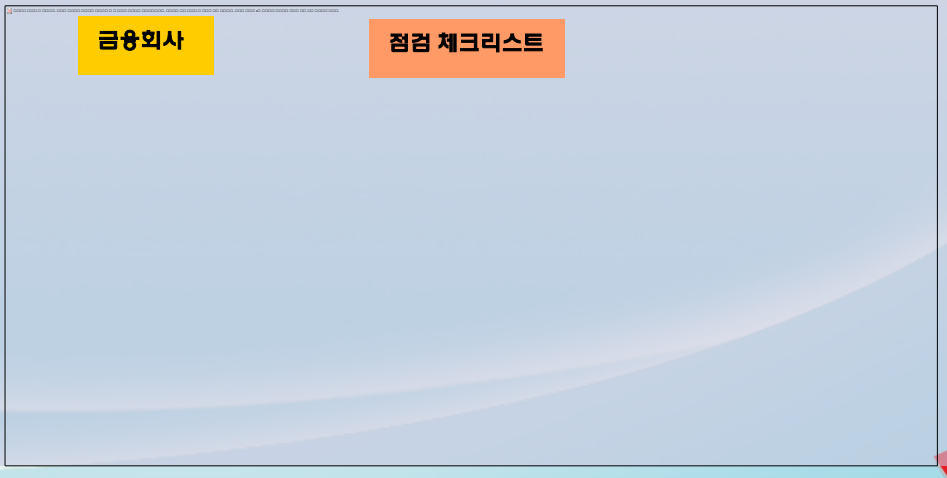
3. 업무 제휴, 위탁 등 외부 주문 관련 기타 이슈

전자금융보조업자 안전성 합동 점검

- **개별 점검**
  - 금융회사/제휴사업자 모두 많은 인력 및 비용 소모
  - 기준이 달라 서로 다른 결과 도출



- **합동 점검**
  - 공통의 목적을 가진 금융회사가 참여하여 점검대상 사업자에 대해 합동점검반을 구성하여 일관성있는 점검 체크리스트를 통해 점검 후 결과를 공유함으로 효율적인 점검



감사합니다