금융권 정보보호 상시평가제 도입 방안

2020. 12.

금융위원회
금융보안원

목 차

Ⅰ 추진배경

□ 카드사 정보유출 사고 이후, **정보보호 및 재발방지**를 위해 금융회사의 **신용정보관리·보호인에** 대한 **권한**과 **책임**을 **강화**('15)

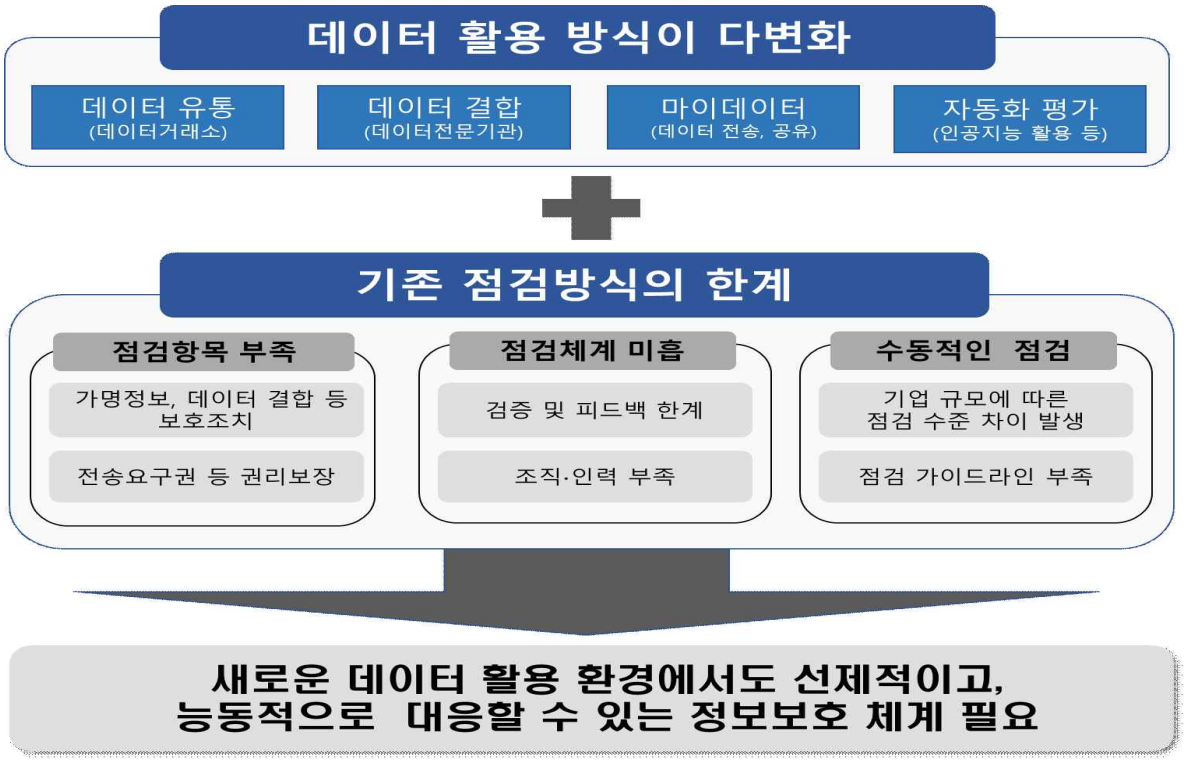
○ 금융회사에 **신용정보 보호**에 대한 **점검·운영** 등에 관한 **실태**를 **연 1회 금융당국**에 **제출**하도록 하는 **의무**도 부여('17)

> **※ 참고 : 신용정보관리·보호인이란?**(신용정보법 §20조③)
> · 신용정보의 **수집·보유·제공·삭제** 등에 대한 **관리**와 **보호계획** 수립, 정보보호 **교육**, **실태조사**, **내부통제시스템** 구축 등 **신용정보관리·보호** 업무를 수행하는 **최고 책임자**

□ 최근 들어, 데이터의 **종류**와 **양**이 많아지고 **활용방식**이 **다변화**됨에 따라 **정보보호 체계**도 **지속적**으로 **개선**될 필요성이 제기

○ 인공지능 등 **신기술, 가명·익명정보**, 데이터 **거래·결합** 등 새로운 **데이터 활용 환경**에서도 적절한 **대응**을 요구

○ **환경 변화**에 **대응**하여 **정보보호 점검체계**를 **보완**하고 **금융권이** 보다 **적극적**인 **역할을** 할 수 있도록 **정보보호 실태 점검방식 개선** 필요



Ⅱ 현황 및 문제점

□1 **(추상적 점검기준) 정보보호 실태**를 점검하기 위한 **구체적 기준**이 부족하고 **새롭게 도입**되는 **제도**와 관련된 **평가**가 **어려움**

○ ①신용정보 보호계획 **수립·시행**, ②정보보호 **실태조사**, ③신용정보보호 **교육 시행** 등 점검기준이 **지나치게 포괄적**으로 구성

○ **가명·익명정보의 처리**, **전송요구권** 행사 등 신용정보법 개정에 따라 **새롭게 도입**되는 내용에 대한 **점검항목** 부족

□2 **(점검체계 미흡)** 약 3,000 개의 금융기관* 등에 대한 **정보보호 실태 점검**이 필요하나, **체계적 점검**을 수행하기 **어려운** 상황

* 은행, 카드, 보험, 금투, 상호금융, 대부, CB사, MyData 사업자 등

○ **금융당국의 한정된 인력을 보완**해 금융권 **정보보호 실태**를 **체계적***으로 **점검**할 수 있도록 지원하는 **자율규제기구**가 **필요**

* 점검과정이 **서면 또는 팩스**로 이루어져 업무처리에 **많은 시간**이 소요

○ **금융기관**의 정보보호 실태에 대한 **금융당국**의 **피드백** 부족

· **(조직·인력상 한계)** 별도의 **전산화**된 **검증시스템 없이** 소수의 인원(5명 이하)이 약 **3,000개 금융기관**에 대한 **정보보호 실태**를 **확인**하고 있는 상황

- 금융회사 등의 **업무수행 실적**과 **증빙자료** 등에 대한 **상세한 점검**이 어려움

· **(피드백 부족)** 신용정보법에 따른 반복적이고 사소한 **정보보호 위반 사항***에 대한 적절한 **피드백**이 없어 **유사한 위반 사례**가 **지속적**으로 **발생**

* 상거래 관계가 종료된 고객에 대한 개인신용정보의 삭제기간 경과, 권한 착오에 따른 개인신용정보 조회 등

□3 **(수동적인 점검)** 점검 가이드라인 등 금융회사가 스스로 **정보보호 수준**을 **진단**해 볼 수 있는 **기준** 부족

○ ①금융회사의 **규모**, ②정보보호에 대한 **관심**, ③신용정보관리·보호인의 **역량**에 따라 회사별 **정보보호 수준**의 **차이** 발생

구 분	은행	카드	자산운용
금융업권별 평균 자체점검 기준 수	18개	9.7개	6.6개
금융업권별 평균 증빙자료 수	6개	7개	0.6개

Ⅲ 상시평가제를 통한 금융권 정보보호 체계 개선

□ 금융권이 **활용·관리**하는 **개인신용정보**에 대한 **보호실태**를 **총체적**으로 **점검**하는 **정보보호 상시평가제** 도입

○ 신용정보법 **전 범위**에 대한 **정보보호 규제**를 **체계적·상시적**으로 **준수·검증**할 수 있는 **자동화 시스템**

○ **❶점검항목 개선, ❷효율적 검증시스템, ❸적극적 점검 환경 조성**을 통해 금융권 정보보호 수준을 **종합적**으로 진단

가. 점검항목 개선 및 평가기준

1 **[정밀한 점검기준 마련]** 금융권 **정보보호 실태**를 **면밀히 점검**할 수 있도록 **점검항목**을 **9개 대항목 143개 소항목**으로 정밀하게 **제시**

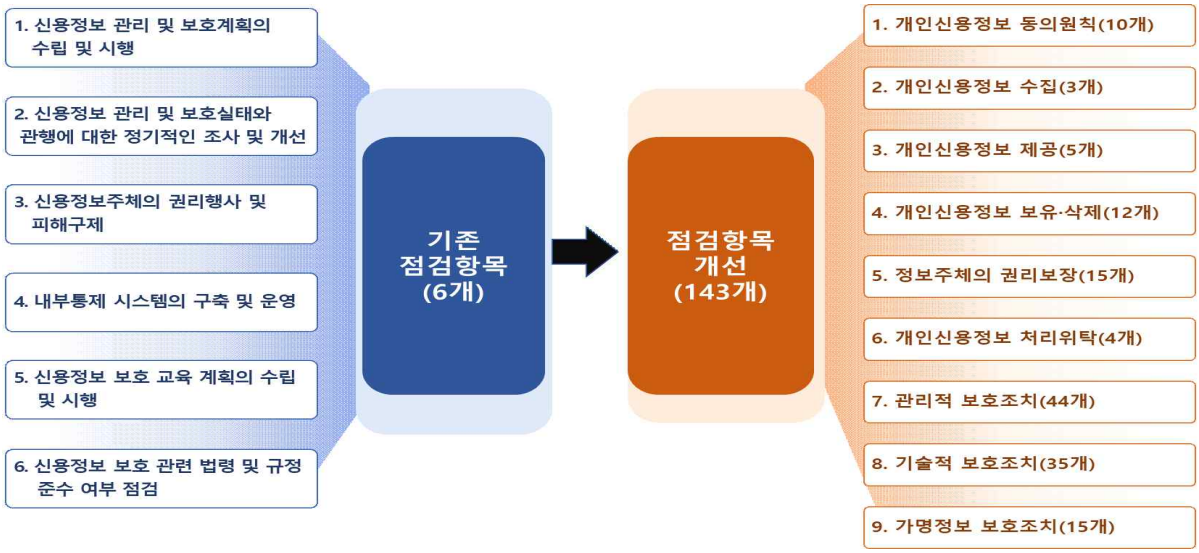
○ 동의·수집·제공·삭제 등 **정보의 생애주기***(Data Life-Cycle)에 따른 **전반적인 사항**을 **점검**할 수 있도록 **평가항목**을 **구체화**

* ①동의원칙, ②수집, ③제공, ④보유·삭제, ⑤권리보장, ⑥처리위탁, ⑦관리적 보호조치, ⑧기술적 보호조치, ⑨가명정보 보호조치

※ 금융당국, 금융보안원, 금융업권별 협회, 금융회사 등과 함께 **상시평가**를 위한 **점검항목** 기준을 **마련**('20.5월~'20.10월)

· 평가기준이 **정보보호 준수 사항**을 **구체적**으로 반영하고 있어, 금융회사의 상황에 따라 **최적화된 정보보호 체계**를 **구축**할 것으로 **기대**된다는 **의견**

※ 점검항목 주요 개선 내용



○ 정보보호 점검항목별로 **준수정도**에 따라 **①이행, ②부분이행, ③미이행, ④해당없음 4단계**로 구분

○ **행태주의적 접근**(Behavioral approach)을 통해 금융회사의 **업무부담**을 줄이면서도 **촘촘한 정보보호 체계**를 마련

- 업무 담당자가 **이해하기 쉽게** 점검항목을 **구성**하고, **점검현황·결과**를 **시각적인 화면**으로 **제공**하여 점검 **효율 제고**

※ 점검항목 입력 화면 및 평가결과 화면(예시)

2 **(새로운 평가기준 도입) 새로 도입**되는 제도를 체계적으로 **관리**하고 **파악**할 수 있도록 **평가기준**을 마련

○ **가명정보** 처리, **전송요구** 이행, 데이터 **결합** 등에 관한 **기술적·관리적 정보보호*** 조치에 대한 **이행 여부**를 점검

* ①가명정보와 추가정보의 분리보관, ②전송요구·철회 이행 현황, ③데이터 전문결합을 통해 데이터 결합하였는지 여부 등

○ 일정기간 **점수**가 **우수**하고 **사고가 없는 기업**은 사고발생시 **제재감면 등의 혜택**을 부여하는 '**안전성 인증마크**'를 부여

※ 점수·등급부여 방안 및 안전성 인증마크 운영 세부사항은 추후 안내

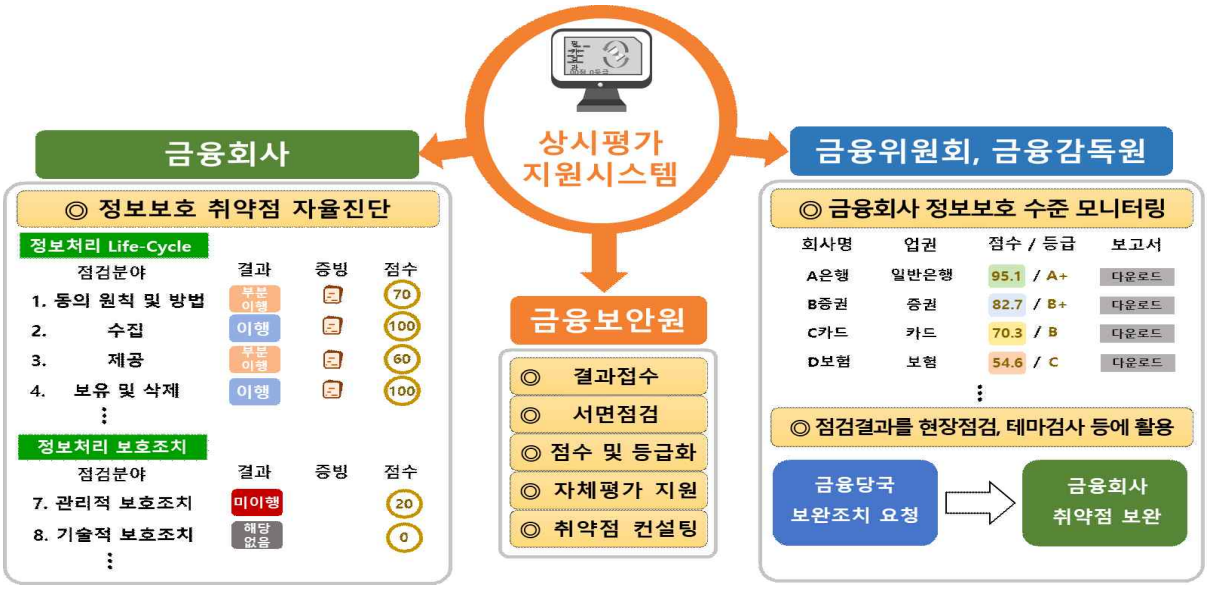
나. 효율적인 검증시스템 도입

1 **(점검 효율화)** 전문기관인 **자율규제기구**(금보원)를 통해 **금융권 정보보호 실태** 점검을 **수행**하여 **점검**의 **효율성**을 제고

○ 정보보호 **실태 점검**을 위한 **인력**을 **보강**하고, **레그테크*** **기반 상시평가지원시스템**을 구축하여 **점검 과정**을 **자동화**

* 레그테크(RegTech) : 규제(Regulation)와 기술(Technology)의 합성어로 복잡한 금융규제들을 비대면·자동화를 통해 쉽게 준수할 수 있도록 지원하는 기술

○ 금융권 **정보보호 수준**을 수치화, 통계화 등을 통한 **전산자료 형태**로 **축적**하여 **금융당국의 감독·검사**에 활용



2 **(피드백 제공)** 금융권에 대한 **정보보호 실태** 점검을 **3단계**로 **세분화**하고, **점검결과**에 대해 **피드백** 제공

○ ❶금융회사의 **자체평가**, ❷**자율규제기구**(금융보안원)의 **점검** 및 **점수**(등급) **부여**, ❸**금융당국**의 **감독·검사** 순으로 구성

절차	세부 내용
❶ 자체평가	· **금융회사 등**은 직전연도 개인신용정보 보호 실태에 대한 **자체평가**를 **수행**하고 **금융보안원**에 **결과 제출**
❷ 점수 및 등급부여	· **금융보안원**은 금융회사의 **제출내역**에 대해 **점검을 수행**하고, 점검결과를 기반으로 **점수·등급 부여**
❸ 감독·검사	· **금융당국**은 금융회사 등의 **평가결과**를 기반으로 **현장점검, 테마검사** 등 취약점 **보완 조치**를 수행

다. 적극적 점검 환경 조성

1 **(지원시스템 마련)** 금융회사 등의 **규모·역량과 관계없이 일정 수준 이상의 정보보호 체계**를 스스로 **갖출 수 있도록 지원**

○ **중·소형 금융회사**도 **대형** 금융회사와 **유사한 수준의 정보보호 역량**을 **갖출 수** 있도록 **유도***

* 금융회사의 정보보호 취약점을 점검하고, 기업 환경에 최적화된 보호 수준을 갖출 수 있도록 교육 및 컨설팅 제공(금융보안원)

2 **(점검 가이드라인 마련)** 금융회사 등이 **사례별·유형별**로 **정보보호**를 스스로 수행할 수 있는 **가이드라인**을 마련

<※참고 : 정보보호 취약 사례 및 가이드라인 내용 예시>

	정보보호 취약 사례(As is)	가이드라인 내용(To be)
❶	· 문자, 숫자, 특수문자 중 **2종류**만 **조합**하여 **비밀번호**를 생성	· **3종류 이상 조합**하여 비밀번호 생성
❷	· 상거래관계가 **종료된 개인신용정보**를 **상거래 중**인 개인신용정보와 **함께 보관**	· 상거래관계 종료된 개인신용정보는 **다른 DB**에 **분리**하여 보관
❸	· 개인신용정보 **처리 수탁자**에 대한 정보보호 실태 **관리감독 미수행**	· **연 1회** 이상 수탁자에 대한 정보보호 실태 **관리·감독 수행**

○ ❶정보보호 **평가항목** 및 근거법령 내용해설, ❷**평가방법**, ❸**증빙방법**(예시 등)으로 구성하여 **자가점검** 및 **개선**을 지원

	구 분	내 용
❶	**평가항목 및 근거법령**	· 평가항목별 **법령·규정**해설 및 **유권해석** 안내
❷	**평가방법**	· 평가항목별 중점적인 **점검·평가 사항** 안내
❸	**증빙방법**	· 평가항목별 요구되는 **증빙자료**에 대한 제출범위, 방법에 대한 **예시와 사례**를 나열

3 **(소통창구 마련)** **상시평가지원시스템**을 통해 금융권 정보보호 **자율점검 체계 형성**에 필요한 **다양한 지원 프로그램***을 제공

* ①정보보호 관련 교육자료 배포, ②우수 정보보호 사례 공유, ③정보보호 커뮤니티, ④실시간 응답 챗봇 등 금융당국과의 상시적 소통창구 마련 등

Ⅳ 기대효과

◇ **급변**하는 **데이터 산업 환경** 속에서도 금융권이 **효과적**으로 **개인신용정보**를 **보호**할 수 있는 **정보보호 체계**로 **탈바꿈**

○ AI 등 **신기술** 도입, 가명정보 등 새로운 **데이터 처리 환경**에서도 **일관성** 있는 **정보보호**를 통해 **국민**의 **신뢰성 제고**

1 **(체계적 점검)** 금융권의 **개인신용정보 활용·관리** 수준에 대한 **세부적**이고 **면밀한 점검**을 통해 **객관적인 평가** 가능

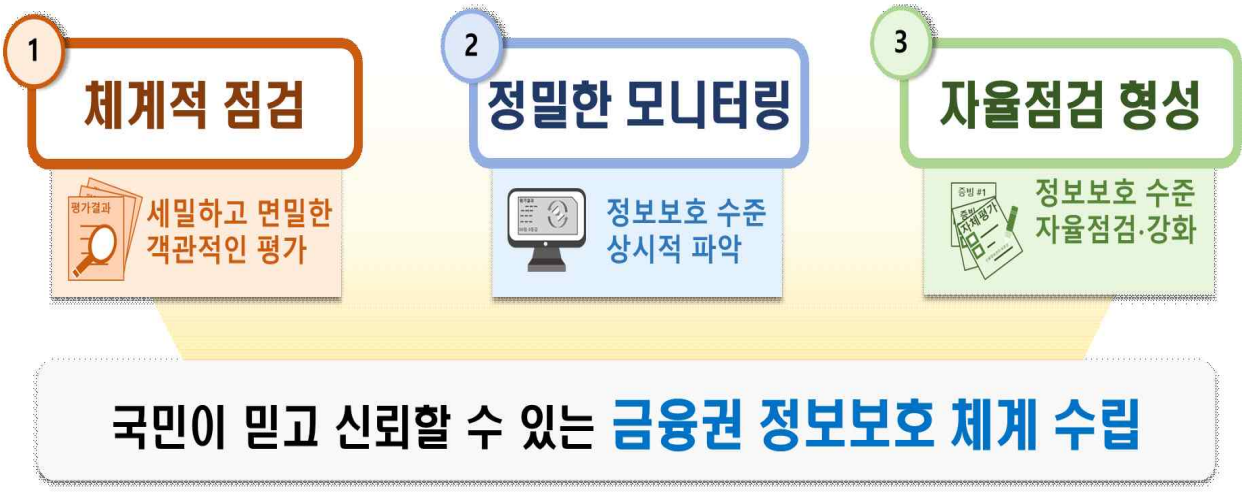
○ **3단계**로 **구성**되는 **중첩적**인 **점검**과 **점검결과**에 대한 **점수화·등급화**를 통해 금융권 **정보보호 수준**을 **체계적**으로 **관리**

2 **(정밀한 모니터링)** 금융권 **정보보호 수준**을 **상시적**으로 파악하고, **새로운 데이터 활용** 환경에서도 정보유출 등 **사고발생**을 **예방**

○ 수집·제공·삭제 등 **정보처리 단계별 취약점**을 **개선**하고, 가명정보 활용, 마이데이터 등 **신규 제도**에 대한 **모니터링**도 강화

3 **(자체 점검능력 향상)** 새로운 **데이터 활용 환경**(AI, 가명정보 등)에 금융권이 신속히 **대응**할 수 있는 **능력 제고**

○ 상시평가지원시스템, 가이드라인 등을 통해 자신의 **정보보호 수준**을 **스스로 점검**하고 취약점에 대한 **선제적 대응**을 **강화**



Ⅳ 향후계획

1 상시평가제 **온라인 설명회 개최**(12월4일)

2 상시평가지원시스템 **오픈 및 시범 운영**('20.12월~'21.1월)

3 상시평가제 운영에 대한 **공정성·객관성** 등을 확보하기 위해 **금융보안원**에 **상시평가위원회**를 구성(12월 중)

○ 금융분야 정보보호에 대한 **경험과 학식**을 갖춘 **전문가**를 중심으로 **10명 이내**로 구성

4 상시평가 운영을 위한 **가이드라인 배포** ('21.1월 중, 금보원)

5 '20년도 **개인신용정보 관리·보호 실태 평가결과 제출***('21.3.31.)

* 상시평가 대상 금융기관(상세 참고)

추진 과제		일정
1	**정보보호 상시평가제 온라인 설명회**	'20.12.4.
2	**상시평가지원시스템 오픈** 및 **시범운영**	'20.12월~ '21.1월
3	상시평가 및 자체평가 방법 등을 담은 **가이드라인 배포**	'21.1월
4	**정보보호** 상시평가제 **시행**	'21.2.4.

※ 금융분야 상시평가제 관련 문의처
· 02-3495-9931~6(금융보안원)

참고 **상시평가 대상기관('20.10월 기준)**

□ 금융당국에 신용정보 **활용·보호 실태**에 대한 **점검결과**를 **제출해야 하는 대상**은 **금융회사 등** 약 **3,653**개 기관*

* 신용정보법 시행령 제17조제7항에서 규정하고 있는 기관

※ 참고 : 상시평가 대상 기관 요약

구 분	평가대상	기관수
금융지주	· **금융지주회사(10)**	10
은행	· **일반은행(50)** - 시중은행(6), 지방은행(6), 인터넷전문은행(2), 외국은행 국내지점(36) · **특수은행(5)** - 산업은행, 수출입은행, 농협은행, 수협은행, 중소기업은행	55
보험	· **생명보험회사(24), 손해보험회사(31)**	55
금융투자	· **금융투자업자(816)** - 투자일임·자문업자(417), 자산운용회사(311), 증권회사(42), 부동산신탁회사(14), 외국증권회사 국내지점(11), 외국환중개회사(7), 온라인소액투자중개업자(9), 선물회사(4), 종합금융회사(1), · **금융투자업관계기관(4)** - 증권금융회사(1), 자금중개회사(2), 명의개서대행회사(1)	820
여신금융	· **여신전문금융회사(112)** - 신용카드업(8), 할부금융업(23), 시설대여업(26), 신기술사업금융업(62) · **겸영여신업자(1)** - 새마을금고연합회 신용카드업 부문	120
저축은행	· **상호저축은행 및 중앙회**	80
상호금융	· **농협(1,119), 수협(91), 산림조합(145), 신협(883) 및 각 중앙회**	2,238
대부업	· **대부업자*등(236)**	236
신용정보회사등	· **신용정보회사(7)** - 개인신용평가회사·기업신용조회회사(6), 신용조사회사(1), 개인사업자신용평가회사(미정) · **본인신용정보관리회사**(미정) · **채권추심회사**(22)	29
공공기관	· **한국자산관리공사, 한국주택금융공사, 한국무역보험공사, 신용보증기금, 근로복지공단, 서민금융진흥원**	6
기타	· **케이알앤씨**(舊 정리금융공사), **신용회복위원회, 한국신용정보원, 한국정보통신진흥협회**	4
합 계		**3,653**