

金融分野における個人情報保護の取組みについて

平成 23 年 6 月 15 日
金融庁総務企画局

I. 金融分野における個人情報保護に関するガイドライン等の概要

1. 金融分野における個人情報保護

「個人情報保護に関する基本方針」(平成 16 年 4 月 2 日閣議決定)および「個人情報の保護に関する法律案に対する附帯決議」において、金融分野は、医療、情報通信等と並んで、個人情報の性質や利用方法等から特に適正な取扱いの厳格な実施を確保する必要がある分野とされている。

2. ガイドラインおよび実務指針

個人情報保護法や上記の基本方針等に基づき、「金融分野における個人情報保護に関するガイドライン」(平成 16 年 12 月)(以下、「ガイドライン」という。)および「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」(平成 17 年 1 月)(以下「実務指針」という。)を策定。その後、内閣府が作成した「標準的なガイドライン」(平成 20 年 7 月)を参考に、ガイドライン共通化へ対応(ガイドラインに例示等を追加し、平成 21 年 11 月に改正)。

- a. 金融分野における個人情報取扱事業者が個人情報の適正な取扱いの確保に関して行う活動を支援する目的で、ガイドラインおよび実務指針を策定。
- b. ガイドラインの内容の2つの要素は、1)金融機関が講ずべき措置の有効かつ適切な実施をはかるための個人情報保護法の解釈指針、2)金融分野における個人情報の特性及び利用方法を鑑み、個人情報の取扱いにおいて特に厳格な実施が求められる事項(格別の措置)。
- c. 主な「格別の措置」は、次のとおり。
 - ア. 個人情報保護法上は、「個人情報取扱事業者」から除かれる金融機関においても、ガイドラインの遵守に努めるものとする旨の規定。
 - イ. センシティブ情報の取得等の原則禁止。
 - ウ. 信用情報機関への情報提供については、信用情報機関の会員企業及び安全管理措置等を本人に認識させた上で同意取得。
 - エ. 第三者提供にあたっての本人同意は原則書面。
- d. 安全管理措置の内容については、ガイドラインで掲げた基本的事項の詳細な

内容について、実務指針として別途規定。主にガイドラインの 10 条から 12 条（第 10 条：安全管理措置、第 11 条：従業員の監督、第 12 条：委託先の監督）に定められた安全管理措置等の基本的事項について、金融機関が講ずるべき措置を明示。

e. ガイドラインおよび実務指針に関する Q&A を策定、当庁ホームページで公表（平成 19 年 10 月）。

ア. 個人情報保護法施行後、金融機関における個人情報保護に関する実務等について、様々な照会が当庁及び財務局に対して寄せられており、それらの照会を体系づけて整理し、Q&Aの形で公表することが、行政の透明性・予測可能性の向上にとって重要。

イ. 個人情報の漏えい、滅失、き損が生じた場合には、ガイドライン及び実務指針に基づき、金融機関に対して当局への報告や本人への通知、公表を求めているが、それらの具体的な内容や方法等については各金融機関において統一されているわけではなかったため、報告事項等について、当局として一般的な解釈を示すことが各金融機関間における公平性及び行政事務の効率的な運営の観点から有用。

3. 業法等

個人情報保護法上、「個人情報の性質および利用方法にかんがみ、個人の権利利益の一層の保護を図るため特にその適正な取扱いの厳格な実施を確保する必要がある個人情報について、保護のための格別の措置が講じられるよう必要な法制上の措置その他の措置を講ずる」ものとされている。これを踏まえ、平成 17 年以降、銀行法をはじめとする各業法において、法改正の機会をとらえ順次、法律上、顧客情報の適正な取扱い義務を明記。あわせて、次の点について、各業法施行規則（内閣府令）において明記（別添 1、2）。

- a. 安全管理措置、従業員・委託者の監督について必要かつ適切な措置の実施。
- b. センシティブ情報を必要な目的以外に使用することの禁止。
- c. 信用情報機関から提供された借入金返済能力情報を返済能力調査以外の目的に利用することの禁止。

業法上、立入検査権限、監督命令権限（業務改善命令、業務停止命令等）があるほか、金融 ADR 制度も適用。

II. 認定個人情報保護団体の取組の状況

1. 認定状況

金融分野の認定個人情報保護団体は9団体。

日本証券業協会
日本生命保険協会
日本損害保険協会
外国損害保険協会
全国銀行個人情報保護協議会
信託協会
投資信託協会
日本証券投資顧問業協会
日本貸金業協会

2. 取組状況

- a. 個人情報保護指針の作成・公表、金融機関向けのセミナーや研修、また、相談や問い合わせへの対応により、情報提供等を実施。その他、漏えい事案等の状況集計や好取組事例にかかる意見交換会の実施。
- b. 個人情報保護法第 42 条及び第 43 条に基づく苦情処理等の件数は、次のとおり。

年度	苦情処理	説明要求	資料要求	指導	勧告	その他の措置*
17 年度	237	55	1	135	1	0
18 年度	248	36	0	40	1	0
19 年度	199	50	1	44	0	4
20 年度	165	36	0	49	0	2
21 年度	179	42	0	49	2	1
22 年度	194	81	0	52	0	0

* 「その他の措置」とは、認定個人情報保護団体が、法第 43 条に基づき自ら作成・公表した個人情報保護指針を対象事業者に遵守させるために行った措置で、「指導」及び「勧告」以外のものを指す。

III. 金融機関に対する検査・監督の状況

1. 金融検査

- a. 立入検査を定期的実施する中で、顧客情報保護の管理態勢を検査。
金融検査マニュアルにも、顧客情報保護の管理態勢を検査項目として明記、公表。
- b. 検査での主な指摘事項を検査指摘事例集として公表（別添3）。

2. 漏えい事案等

個人情報漏えい事案等のうち、当局に届出され、公表された事案

年度	漏えい事案等*
17年度	607(33)
18年度	231(17)
19年度	187(8)
20年度	135(12)
21年度	150(10)
22年度	92(5)

* カッコ内は、漏えい等をした個人情報 が 50,001 件以上の事案。

* 公表されていない漏えい等事案の主なものは、メール、ファックス、郵便の送付ミス。

3. 金融機関に対する監督

- a. 個人情報の漏えい等が発生し金融機関が金融庁に報告した事案や、金融検査で発覚した事案等のうち、漏えい等の状況、漏えいした個人情報の規模および内容を踏まえ、報告徴収を実施。
- b. 当該報告徴収を踏まえ、個人情報保護法に基づく勧告、業法に基づく業務改善命令を発動。

年度	個人情報保護法				業法*	
	報告徴収	助言	勧告	命令	業務改善命令	業務停止命令
16年度	—	—	—	—	2	0
17年度	83	0	1	0	1	0
18年度	52	0	1	0	1	0
19年度	78	0	0	0	0	0
20年度	26	0	0	0	0	0
21年度	16	0	2	0	2	0
22年度	14	0	0	0	1	0

* 個人情報に関連する行政処分の件数。

- c. 平成16年度以降、個人情報保護法上の勧告、および／または、業法上の業務改善命令は、7件発動。うち、漏えい事案等の報告により把握した案件は4件、金融検査で把握した案件は3件。

A 銀行（平成22年5月27日）

- ア. 顧客からの同意を得ずに顧客情報を第三者に提供を行い、法令違反となるおそれがある行為が発生。
- イ. 銀行法上の業務改善命令。

B 保険会社（平成22年2月24日）

- ア. 業務委託先の従業員がホストコンピュータにアクセスし、顧客情報を社外に持ち出し、漏えい。
- イ. 保険業上の業務改善命令、個人情報保護法上の勧告。

C 証券会社（平成21年6月25日）

- ア. 従業員が顧客情報をコンパクトディスクに保存させ、第三者に売却。
- イ. 金融商品取引法上の業務改善命令、個人情報保護法上の勧告。

D 銀行（平成18年4月25日）

- ア. 支店課長職の者が顧客情報を不正に持ち出し、漏えい。
- イ. 銀行法上の業務改善命令、個人情報保護法上の勧告。

E 銀行（平成17年5月20日）

- ア. 顧客情報が記録されたCD-ROM3枚を紛失。
- イ. 銀行法上の業務改善命令、個人情報保護法上の勧告。

F 銀行（平成16年6月11日）

- ア. 顧客情報を記録するバックアップ・データが、データ処理等の業務を外部委託するデータ・センターの搬送途上で紛失。
- イ. 銀行法上の業務改善命令。

G 銀行（平成 16 年 5 月 20 日）

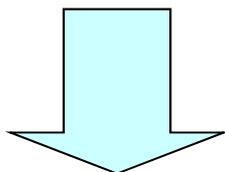
- ア. 行員の転籍に伴う顧客情報の電子記憶媒体等によるグループ他社への持出し、顧客に対する与信情報等の不適切な管理。
- イ. 銀行法上の業務改善命令。

以上

個人情報保護法と業法の関係について(銀行法の例)

個人情報保護法 第6条(法制上の措置等)

政府は、個人情報の性質及び利用方法にかんがみ、個人の権利利益の一層の保護を図るため特にその適正な取扱いの厳格な実施を確保する必要がある個人情報について、保護のための格別の措置が講じられるよう必要な法制上の措置その他の措置を講ずるものとする。



銀行法 第12条の2第2項(預金者等に対する情報の提供等)

前項及び第十三条の四並びに他の法律に定めるもののほか、銀行は、内閣府令で定めるところにより(※)、その業務に係る重要な事項の顧客への説明、その業務に関して取得した顧客に関する情報の適正な取扱い、その業務を第三者に委託する場合における当該業務の的確な遂行その他の健全かつ適切な運営を確保するための措置を講じなければならない。

銀行法施行規則

第十三条の六の五(個人顧客情報の安全管理措置等)

銀行は、その取り扱う個人である顧客に関する情報の安全管理、従業者の監督及び当該情報の取扱いを委託する場合にはその委託先の監督について、当該情報の漏えい、滅失又はき損の防止を図るために必要かつ適切な措置を講じなければならない。

第十三条の六の六(返済能力情報の取扱い)

銀行は、信用情報に関する機関(資金需要者の借入金返済能力に関する情報の収集及び銀行に対する当該情報の提供を行うものをいう。)から提供を受けた情報であつて個人である資金需要者の借入金返済能力に関するものを、資金需要者の返済能力の調査以外の目的のために利用しないことを確保するための措置を講じなければならない。

第十三条の六の七(特別の非公開情報の取扱い)

銀行は、その取り扱う個人である顧客に関する人種、信条、門地、本籍地、保健医療又は犯罪経歴についての情報その他の特別の非公開情報(その業務上知り得た公表されていない情報をいう。)を、適切な業務の運営の確保その他必要と認められる目的以外の目的のために利用しないことを確保するための措置を講じなければなら

※

金融機関に対する個人情報保護方策の義務付けと履行担保措置

1. 金融機関に対する個人情報保護方策の法的義務付け

- (1) 一般の民間事業者と同様、金融機関にも個人情報保護法上の保護方策が義務付け（5千人超の場合）。
- (2) 上記に加え、銀行法等の各業法では、
- ① 個人情報保護法上の安全管理措置に相当する義務
 - ② 個人情報保護法上の目的外利用・提供の制限（センシティブ情報と信用情報にかかるもの）に相当する義務
- についても、別途、法律措置済み（5千人以下にも適用）。

2. その履行を担保するための法的措置

- (1) 一般の民間事業者と同様、金融機関も個人情報保護法上の履行担保措置の対象。
- (2) 上記に加え、銀行法等の各業法では、より厳格な履行担保措置が規定。当庁ではその適切な行使に尽力。

(注) 個人情報保護法には規定のない立入検査権限、より幅広い監督命令権限（業務改善命令、業務停止命令等）

個人情報保護にかかる金融機関に対する検査の指摘事例

職員数(人)				検査実績(社)						
年度末	金融庁検査局	財務省財務局	監視委証券検査課	事務年度	主要行等	地域銀行	信用金庫	信用組合	生損保	証券会社等
20	441	509		19	28	41	111	65	16	219
21	430	500	111	20	23	58	101	67	19	220
22	423	518	114	21	16	46	135	62	17	211
検査指摘事項の例(概要)										
主要行等 (都市銀行等及び「地域銀行」を除くその他の銀行)	顧客情報を別の顧客に送付したにもかかわらず、事実関係の説明を行っていない事例がある。									
	個人情報を登録している一部のソフトウェアについて、顧客情報の漏えいを防止するための対処方針を検討していないため、海外拠点の利用者が、承認なしに個人情報へのアクセス権限を取得できる状態にあることを把握していない。									
	個人情報管理責任者を任命しているが、再委託先における個人情報漏えいについて、事実関係の把握や再発防止策の徹底が不十分であったため、再委託先において情報漏えいが再発している。									
地域銀行 (地方銀行、第二地方銀行等)	文書管理ルールを明確に定めていないため、一部営業店において、顧客情報管理台帳の記載漏れや顧客情報を含む廃棄予定文書等を営業店通路等に放置している事例がある。									
	顧客情報管理部門が、営業店に対し、顧客情報に関する台帳整備につき指示を徹底していないため、営業店において、一部の情報が台帳に記載されていない。									
	顧客管理部門が、営業店に対し、郵便物発送やFAX送信の際の役席者による検証を徹底していないため、漏えい事案が繰り返し発生している。									
信用金庫・信用組合	個人データ管理規定において、情報を外部に持ち出す際には記録表に記載することとしているが、記録表の記録が正確でないため、営業店において、渉外担当者の持ち出した情報を特定できない事例がある。									
	理事会が顧客情報保護等関連諸規定を策定していないことなどにより、重要な顧客情報が無施錠のキャビネットで保管されていたり、帳票が机上に放置されるなどの事例がある。									
	対応マニュアルにおいて総務部門が全ての漏えい事案を当局に報告することとしているが、営業店から事務ミスとして報告された事案につき、検証を十分行っていないことから、個人情報漏えいしていることを見落としている。									
保険会社	顧客情報統括管理部門は、個人データの消去・廃棄の記録を行っておらず、適切に消去等が行われたか把握していないほか、顧客データへのアクセス記録を保管・分析していない。									
	各部門長が、部門内職員に対し、業務の実情に応じて、顧客情報の閲覧権限を付与することとしているが、権限付与の適切性を検証する態勢を構築していないため、業務上の必要がなく誤って権限を付与された職員が顧客情報を閲覧している事例を看過している。									
	委託先における顧客情報管理態勢が未整備であることを把握しているにもかかわらず、委託先に対して体制整備を求めている。									
証券会社等	センシティブ情報の取扱いについての社内規程を整備しておらず、相続手続業務に伴い取得したセンシティブ情報を含む戸籍謄本等をPDFファイル化して保存しているものの、付与する必要のない職員に対してもアクセス権限が付与されていた。									
	個人データに関する利用目的、保管場所・保管方法・保管期限等の状況を、台帳に未記載であり、また、本店各部、支店及び営業所に管理台帳が送付されていなかったため、管理台帳に従った個人データの管理が行われていなかった。									
	関係会社との間において、個人情報の取扱いに係る契約(以下「覚書」という。)を定める旨の利用契約を締結したものの、当該覚書が締結される以前に、当該関係会社に対して、顧客約8万人分の「顧客カタカナ情報」、「顧客漢字氏名」、「メールアドレス」及び「ログインID」の情報を提供した。									

(注)証券会社等の実績は、19年度～21年度のもの。