資料２

金融分野における個人情報保護に関するガイドライン【要綱】

第１条　目的（法第１条）

１　ガイドラインは、「個人情報の保護に関する法律」（以下、「法」という。）、「個人情報の保護に関する法律施行令」（以下、「施行令」という。）及び「個人情報の保護に関する基本方針」（以下、「基本方針」という。）を踏まえ、「金融分野」における個人情報取扱事業者が講ずべき措置の適切かつ有効な実施を図るための指針として策定。

２　金融分野における個人情報取扱事業者等は、本ガイドライン等を踏まえ、各事業の実態等に応じたさらなる措置を自主的なルールとして策定。

なお、事業者は、個人情報の適正な管理に関し、関係法令等を踏まえて対応する必要。

３　法第２条第３項第４号の規定により「個人情報取扱事業者」から除かれる者においても、本ガイドラインの遵守に努める。

第２条　定義等（法第２条、施行令第１条、施行令第２条、施行令第３条、施行令第４条）

下記について、法に基づき定義を記載。

１　「個人情報」

２　「個人情報データベース等」

３　「個人情報の数」

４　「個人データ」

５　「保有個人データ」

６　「個人信用情報機関」

第３条　利用目的の特定（法第１５条）

１　金融分野における個人情報取扱事業者は、個人情報の取扱いに当たっては、個人情報の利用目的を本人が合理的に予想できるようできる限り特定。

具体的には、「自社の所要の目的で用いる」といった抽象的な利用目的は、「できる限り特定したもの」とはならない。

（利用目的の例示の記載）
・当社の預金の受入れ
・保険金・給付金の支払い　等

２　個人情報の利用目的が法令等に基づき限定されている場合はその旨の明示。

３　与信事業に際しては、利用目的については他の契約条項等と明確に分離して記載。また、個人情報を信用情報機関に提供する場合には、その旨を利用目的に明示。

この他、与信業者における利用目的の特定について金融分野の個人情報取扱事業者に求められる事項。

第４条　「同意」の形式について（法第１６条、第２３条）

金融分野における個人情報取扱事業者は、法第１６条及び第２３条に定める本人の同意を得る場合には、原則として、書面（電子的方法等を含む。）による。

第５条　利用目的による制限（法第１６条）

１　金融分野における個人情報取扱事業者は、あらかじめ本人の同意を得ないで、特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱うことを禁止。

２　合併等による事業の承継に伴って個人情報を取得した場合は、あらかじめ本人の同意を得ないで、承継前における当該個人情報の利用目的の達成に必要な範囲を超えての取扱いを禁止。

３　前二項の規定は、次に掲げる場合については、適用しない。

①　法令に基づく場合

②　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

③　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

④　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

上記各項の具体例を明示。

第６条　機微（センシティブ）情報について

１　「機微（センシティブ）情報」（政治的見解、信教（宗教、思想及び信条をいう。）、労働組合への加盟、人種及び民族、門地及び本籍地、保健医療及び性生活、並びに犯罪歴に関する情報）の取得、利用等は行わない。

例外事項の定め

法令に基づく場合、人の生命、身体又は財産の保護のために必要がある場合、保険業の適切な業務運営に用いる場合等

生体認証情報の取扱い

２　機微(センシティブ)情報を例外的に取得、利用等する場合の慎重な取扱い。

第７条　適正な取得（法第１７条）

金融分野における個人情報取扱事業者は、偽りその他不正の手段による個人情報取得の禁止。第三者からの取得に際しての本人利益の不当侵害の禁止。

第８条　取得に際しての利用目的の通知等（法第１８条）

１　個人情報取扱事業者は、個人情報を取得した場合、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を本人に通知し、又は公表（法第１８条第１項)。

金融分野の個人情報取扱事業者においては、「通知」の方法については原則として、書面（電子的方式等を含む。）による。「公表」の方法については、インターネット上のホームページ等での公表、事業者の窓口等への書面の掲示・備付け等適切な方法による必要。

２　個人情報取扱事業者は、本人との間で、契約を締結することに伴って契約書等に記載された個人情報を取得する場合は、あらかじめ利用目的を明示。金融分野の個人情報取扱事業者は、与信事業を行う場合には、利用目的を明示する書面に確認欄を設ける。

３　「取得の状況から見て利用目的が明らかであると認められる場合」には、通知又は公表は適用除外（法第１８条第４項第４号)。

〔「取得の状況から見て利用目的が明らかであると認められる場合」の例示の記載。〕

第９条　データ内容の正確性の確保（法第１９条）

金融分野における個人情報取扱事業者は、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つ必要。

このため、事業者は、法令等に基づく保存期間の定めがある場合を除き、保有個人データの利用目的に応じ保存期間を定め、当該期間経過後の個人情報を消去。

第１０条　安全管理措置（法第２０条、基本方針）

１　金融分野における個人情報取扱事業者は、安全管理に係る基本方針・取扱規程等の策定及び組織体制の整備等の必要かつ適切な措置を講じる必要。必要かつ適切な措置は、個人情報の収集・利用・送付等の各段階に応じた「組織的安全管理措置」、「人的安全管理措置」及び「技術的安全管理措置」を含む。

２　「組織的安全管理措置」：個人情報取扱事業者の体制整備及び実施措置。

３　「人的安全管理措置」：個人データの安全管理が図られるように従業者を監督。

４　「技術的安全管理措置」：個人データに対する技術的な措置。

５　安全管理に係る基本方針・取扱規程等の整備として、以下の「組織的安全管理措置」。

（組織的安全管理措置）

（１）規程の策定

〔 安全管理に係る基本方針、取扱規程等の策定、その他求められる規程を記載。 〕

（２）管理手順の明確化

〔 具体的な手順を明示 〕

６　個人情報の安全管理に関する組織体制の整備として、以下の「組織的安全管理措置」、「人的安全管理措置」及び「技術的安全管理措置」。

（組織的安全管理措置）

〔 個人情報の管理責任者の設置、雇用・雇用契約における安全管理措置等求められる措置を記載。 〕

（人的安全管理措置）

〔 従業者との個人情報非開示契約の締結、従業者への安全管理措置の周知徹底、教育及び訓練等求められる措置を記載。 〕

（技術的安全管理措置）

〔 個人データ利用者の識別と認証、個人データへのアクセス権限の管理、個人データへのアクセス記録と分析、個人データを取扱う情報システムの稼働状況の記録と分析等求められる措置を記載。 〕

第１１条　従業者の監督（法第２１条、基本方針）

１　金融分野における個人情報取扱事業者は、適切な内部管理体制を構築し、その従業者に対する必要かつ適切な監督を行う必要。

２　「従業者」とは、個人情報取扱事業者の組織内にあって直接又は間接に事業者の指揮監督を受けて事業者の業務に従事している者

〔 具体的な監督内容の記載
　従業者等の守秘義務等の確認等、従業者への安全管理義務の周知徹底、教育及び訓練等、社内での安全管理措置の運用状況等の確認や従業者の個人情報保護に対する点検・監査制度の整備等。 〕

第１２条　委託先の監督（法第２２条、基本方針）

１　金融分野における個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、委託を受けた者に対する必要かつ適切な監督を行う必要。

２　「委託」とは、契約の形態や種類を問わず、金融分野における個人情報取扱事業者が他の者に個人データの取扱いの全部又は一部を行わせることを内容とする契約。

３　金融分野における個人情報取扱事業者は、個人データを適正に取り扱っていると認められる者を選定し委託。当該個人情報取扱事業者は、個人情報の安全管理のための措置を委託先（再委託先を含む）においても確保することが必要。

〔具体的な監督内容の記載
　委託先基準の内容、委託契約の内容等。〕

第１３条　第三者提供の制限（法第２３条）

１　金融分野における個人情報取扱事業者は、法第２３条に従い、次に掲げる場合を除くほか、あらかじめ本人に同意を得ることなく、個人データを第三者に提供することを禁止。

①　法令に基づく場合

②　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

③　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

④　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

〔具体例については、第５条３項①～④の箇所で例示を記載。〕

なお、第三者への提供の同意を得る際には、原則として書面(電子的方式等を含む。)による。

〔同意書面の記載事項について記載。〕

２　「第三者」とは、個人データを提供しようとする個人情報取扱事業者及び当該個人データに係る本人のいずれにも該当しないもの。

３　個人信用情報機関に対する提供について

個人信用情報機関に対して個人データが提供される場合には、本人の同意を取得。

〔信用情報機関への提供について同意を得る書面において特に求められる記載内容。〕

金融分野の個人情報取扱事業者は、資金需要者の返済能力に関する情報については、慎重に取扱う必要。

４　法第２３条第２項について

法第２３条第２項においては、個人情報取扱事業者が、第三者に提供される個人データに

ついて、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、同項各号に掲げる事項について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているときは、当該個人データを第三者に提供することが可能。

この際の、「本人が容易に知り得る状態」とは、本人が知ろうと思えば、時間的にも、その手段においても、容易に知ることができる状態。

〔「本人が容易に知り得る状態」の例示の記載。〕

5　与信事業における法第２３条第２項の適用について

〔返済能力に不安のある個人が個人信用情報機関への提供の停止を求めた場合〕

6　法第２３条第４項第３号について

個人データを特定の者との間で共同して利用する場合であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているときは、第三者に当たらない。金融分野の個人情報取扱事業者においては、この場合の「通知」は、書面(電子的方式等を含む。)による。

〔共同利用者の外延を示す場合において、本人が容易に理解できるよう、「共同して利用する者」を具体的に特定する望ましい示し方〕

7　経過措置

法施行前において、個人信用情報機関への提供の同意を本人から得ている場合も、加入資格に関する当該機関の規約及び会員企業名の公表は法の施行前に実施されることが適当（法附則第３条関連)。

第１４条　保有個人データに関する事項の公表等（法第２４条、施行令第５条）

金融分野における個人情報取扱事業者は、保有個人データに関し、利用目的、開示等の手続等法２４条第１項に定める事項を本人の知り得る状態に置く必要。

「本人の知り得る状態」とは、本人が知ろうと思えば知ることができる状態。

〔「本人の知り得る状態」例示の記載。〕

第１５条　開示（法第２５条）

金融分野における個人情報取扱事業者は、本人から、当該本人が識別される保有個人データの開示を求められたときは、本人に対し、遅滞なく、保有個人データを開示しなければならない。ただし、次の各号のいずれかに該当する場合には、その全部又は一部を開示

しないことができる。

① 本人又は第三者の生命、身体、財産その他の権利利益を害する場合

② 当該個人情報取扱事業者の業務の適正な実施に著しい支障を及ぼす場合

③ 他の法令に違反することとなる場合

〔上記②について具体例の記載。〕

金融分野における個人情報取扱事業者が開示しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知する必要。決定の理由について、根拠とした法の条文及び判断の基準となる事実を示して説明。

第１６条　訂正等（法第２６条、施行令第６条）

金融分野における個人情報取扱事業者は、本人から、当該本人が識別される保有個人データの内容が事実でないという理由によって当該保有個人データの内容の訂正等を求められた場合には、利用目的の達成に必要な範囲内において、遅滞なく必要な調査を行い、その結果に基づき、当該保有個人データの内容を訂正等する。

訂正等を行った場合、又は訂正等を行わないこととした場合は、本人に対し、遅滞なくその旨を通知。

なお、事業者が訂正等を行わない場合は、訂正を行わない根拠及びその根拠となる事実を示し、その理由を説明。

第１７条　利用停止等（法第２７条）

１　金融分野における個人情報取扱事業者は、当該保有個人データの利用停止等または第三者提供の停止等を求められた場合であって、その求めに理由があることが判明したときは、違反を是正するために必要な限度で、遅滞なく、当該保有個人データの利用停止等を行う必要。ただし、当該保有個人データの利用停止等に多額の費用を要する場合その他の利用停止等を行うことが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

２　金融分野における個人情報取扱事業者は、利用停止等を行ったとき若しくは利用停止等を行わない旨の決定をしたとき、第三者への提供を停止したとき若しくは第三者への提供を停止しない旨の決定をしたときは、本人に対し、遅滞なく、その旨を通知する必要。

第１８条　理由の説明（法第２８条）

金融分野における個人情報取扱事業者は、本人から求められた開示・訂正・利用停止等の全部又は一部について、その措置をとらない旨を通知する場合又はその措置と異なる措置をとる旨を通知する場合は、本人に対し、判断の根拠及び根拠となる事実を示し、その理由を説明。

第１９条　開示等の求めに応じる手続（法第２９条、施行令第７条、施行令第８条）

１　金融分野における個人情報取扱事業者は、開示等の求めを受け付ける方法を定めた場合には、「個人情報保護宣言」と一体としてインターネットのホームページに常時掲載もしくは事務所の窓口等に掲示・備付け。

２　開示等の求めをする者が本人又は代理人であることの確認の方法を定めるに当たっては、十分かつ適切な確認手続とするよう留意。

なお、施行令第８条第２項の代理人による求めに対して、事業者が本人にのみ直接開示することも可。

第２０条　手数料（法第３０条）

金融分野における個人情報取扱事業者は、同様の内容の開示等の手続の平均的な実費を予測し、合理的な手数料額を算定する等の方法で、実費を勘案して合理的な範囲内で手数料を徴収。

第２１条　個人情報取扱事業者による苦情の処理（法第３１条）

１　金融分野における個人情報取扱事業者は、個人情報に関する苦情を受けたときは、その内容について調査し、適切かつ迅速に処理。

２　金融分野における個人情報取扱事業者は、適切かつ迅速な苦情処理のために、必要な体制を整備。

〔「必要な体制整備」の具体的措置を記載。〕

第２２条　漏えい事案への対応（基本方針）

金融分野における個人情報取扱事業者は、個人情報の漏えい等の事故が発生した場合には、

①監督当局に直ちに報告

②漏えい等の事実関係及び再発防止策等を早急に公表

③漏えい等の対象となった本人に速やかに漏えい等の事実関係等の通知。

第２３条　個人情報保護宣言の策定（法第１８条、法第２４条、基本方針）

金融分野における個人情報取扱事業者は、事業者の個人情報保護に関する考え方や方針に関する宣言（いわゆるプライバシーポリシー、プライバシーステートメント等。以下、「個人情報保護宣言」という。）を策定、公表。

〔「個人情報保護宣言」に記載されるべき事項の記載。〕

（以　上）