経済産業分野のうち信用分野における個人情報保護ガイドライン

Ⅰ．目的及び適用範囲

このガイドラインは、個人情報の保護に関する法律（平成１５年法律第５７号。以下「法」という。）第７条第１項に基づき平成１６年４月２日に閣議決定された「個人情報の保護に関する基本方針」（平成２０年４月一部変更）を踏まえ、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」（平成１６年厚生労働省・経済産業省告示第４号。以下「経済産業分野ガイドライン」という。）を基礎として、また、法第６条及び第８条に基づき、経済産業省が所管する分野のうち信用分野（物品又は役務の取引に係る信用供与に関する分野）におけ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措置を講じ、及び当該分野における事業者等が行う個人情報の適正な取扱いの確保に関する活動を支援する具体的な指針として定めるものである。

本ガイドラインにおいて特に定めのない部分については、経済産業分野ガイドラインが適用される。また、本ガイドラインは、対象となる事業者の従業者の個人情報については適用しない。

本ガイドラインにおいて、「しなければならない」と記載されている規定については、それに従わなかった場合は、経済産業大臣により、法の規定違反と判断され得る。一方、「こととする」と記載されている規定については、それに従わなかった場合でも、原則として法の規定違反と判断されることはないが、「こととする」と記載されている規定についても、個人情報は、個人の人格尊重の理念の下に慎重に取り扱われるべきものであることに配慮して適正な取扱いが図られるべきとする法の基本理念（法第３条）を踏まえ、また、信用分野における個人情報の適正な取扱いの厳格な実施を確保する観点から、社会的責務としてできる限り取り組むよう努めなければならないものである。もっとも、個人情報の保護に当たって個人情報の有用性に配慮することとしている法の目的（法第１条）の趣旨に照らし、公益上必要な活動や正当な事業活動等までも制限するものではない。特に、個人信用情報機関を通じて個人の正確な支払能力に関する情報を得て、当該個人の支払能力を超える信用供与を行わないように努めることは、多重債務の発生や過剰な信用供与を抑制することに資する。

なお、本分野における認定個人情報保護団体、与信事業者等においては、本ガイドライン等を踏まえ、各事業の実態等に応じて個人情報の適正な取扱いを確保するためのさらなる措置を自主的なルールとして定めることとする。

Ⅱ．法令解釈指針・事例

１．定義等（法第２条関連）

(1)「個人情報」（法第２条第１項関連）

経済産業分野ガイドラインの例による。

(2)「個人情報データベース等」（法第２条第２項関連）

経済産業分野ガイドラインの例による。

(3-1)「個人情報取扱事業者」（法第２条第３項関連）

以下の事項の他は経済産業分野ガイドラインの例による。

当該事業者が個人信用情報機関に加入している場合、その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数の合計が過去６か月以内のいずれの日においても５０００人を超えるか否かは、当該事業者の個人情報データベース等に加え、当該個人信用情報機関及び当該個人信用情報機関と提携する他の個人信用情報機関の管理する個人情報データベース等を構成する個人情報によって識別される特定の個人の数の総和により判断する。

(3-2)「与信事業者」

「与信事業者」とは、個人情報取扱事業者のうち、個人の支払能力に関する情報を用いて割賦販売法（昭和３６年法律第１５９号）第２条第１項に規定する割賦販売、同条第２項に規定するローン提携販売、同条第３項に規定する包括信用購入あっせん、同条第４項に規定する個別信用購入あっせんその他の物品又は役務の取引に係る信用供与を業として行う者をいう。

なお、個人情報データベース等を事業の用に供している者で、その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数の合計が過去６か月以内のいずれの日においても５０００人を超えない者であっても、個人の支払能力に関する情報を用いて割賦販売法第２条第１項に規定する割賦販売、同条第２項に規定するローン提携販売、同条第３項に規定する包括信用購入あっせん、同条第４項に規定する個別信用購入あっせんその他の物品又は役務の取引に係る信用供与を業として行う者であれば、本ガイドラインを遵守することとする。

(3-3)「個人信用情報機関」

「個人信用情報機関」とは、個人の支払能力に関する情報の収集及び会員に対する当該情報の提供を業とする者をいう。

(4)「個人データ」（法第２条第４項関連）

経済産業分野ガイドラインの例による。

(5)「保有個人データ」（法第２条第５項関連）

経済産業分野ガイドラインの例による。

(6)「本人」（法第２条第６項関連）

(7)「本人に通知」

経済産業分野ガイドラインの例による。

(8)「公表」

経済産業分野ガイドラインの例による。

(9)「本人に対し、その利用目的を明示」

経済産業分野ガイドラインの例による。

(10)「本人の同意」

以下の事項の他は経済産業分野ガイドラインの例による。

経済産業分野ガイドライン 2-1-10.中【本人の同意を得ている事例】として掲げている事例にかかわらず、本分野においては、「本人の同意を得（る）」とは、原則として、書面（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録を含む。以下同じ。）で同意を確認する方法によらなければ

ならない。

同意を確認する書面においては、個人情報の取扱いに係る条項とその他の契約条項とは別々の書面とし、又は同一の書面であっても個人情報の取扱いに係る条項とその他の契約条項とは明確に区別しなければならない。また、文字の大きさ、文章の表現その他の消費者の理解に影響する事項について、消費者の理解を容易にするための措置を講じることとする。

同意の取得は、本人の同意の意思が反映される方法によらなければならない。

【本人の同意を得ている例】
・書面の場合、署名・押印を求めること
・書面の場合、確認欄を設けること　等

(11)「本人が容易に知り得る状態」

経済産業分野ガイドラインの例による。

(12)「本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）」

経済産業分野ガイドラインの例による。

(13)「提供」

経済産業分野ガイドラインの例による。

２．個人情報取扱事業者の義務等

(1)個人情報の利用目的関係（法第１５条～第１６条関連）

①利用目的の特定（法第１５条第１項関連）

以下の事項の他は経済産業分野ガイドラインの例による。

利用目的の特定に当たっては、個人情報の各項目と利用目的の各項目との対応関係を明らかにすることとする。

なお、与信事業者は、あらかじめ、個人情報を第三者に提供することを想定している場合には、利用目的において、その旨特定しなければならない。特に、与信事業者が個人信用情報機関に加入している場合は、個人信用情報機関に個人情報を登録し、又は個人信用情報機関から必要な個人情報を取得することについても、利用目的において特定しなければならない。

また、与信事業者は、法第２３条第４項第３号に規定する共同利用を行う場合には、利用目的において、その旨特定しなければならない。この場合において、契約に係る同意を確認する書面において、その旨特定することとする。

なお、利用目的を変更する場合で、変更前の利用目的と相当の関連性を有すると認められる範囲を超えて行う場合は、改めて本人の同意を得なければならない。

【個人情報と利用目的の対応関係の示し方の例】

申込者は、下表に示す利用目的のため、以下のⅰ）～ⅳ）の情報を当社が保護措置を講じたうえで取得・利用することに同意します。

企業名	利用目的	利用情報	連絡先等
㈱　A	与信判断・与信後の管理のため	ⅰ）ⅱ）ⅲ）ⅳ）	東京都千代田区○○ TEL　△△ E-mail　□

	○○事業における宣伝物等、営業案内の利用のため	ｉ）ii）	
（共同して利用する者の範囲） 当社の子会社である ㈱　B ㈱　C	○○事業、××事業における与信判断、与信後の管理のため	ｉ）ii）iii）iv）	URL　http://□□/

ｉ）氏名、住所、電話番号、・・・

ii）申込日、商品名、・・・

iii）支払開始後の利用残高、・・・

iv）過去の債務の返済状況、・・・

②利用目的の変更（法第１５条第２項、法第１８条第３項関連）

経済産業分野ガイドラインの例による。

③利用目的による制限（法第１６条第１項関連）

以下の事項の他は経済産業分野ガイドラインの例による。

ダイレクトメールの発送等の販売促進の目的で個人情報を利用することについて本人が同意しなかったときは、与信事業者は、そのことを理由に信用供与に係る契約の締結を拒否しないこととする。

与信事業者及び個人信用情報機関（以下「与信事業者等」という。）は、個人の支払能力に関する情報を当該個人の支払能力の調査以外の目的に自ら使用しないこととし、また、第三者提供を行う場合の第三者若しくは共同利用を行う場合の共同して利用する者で、個人の支払能力に関する情報を当該個人の支払能力の調査以外の目的に使用する者に対しては、使用させないこととする。

また、個人信用情報機関に加入している与信事業者は、与信申込書や契約書等、個人信用情報機関の個人情報データベース等へのアクセスが正当なものであることを証明することができる資料等を保管し、また、個人信用情報機関からの求めに応じてこれらの情報を提供することとする。

④事業の承継（法第１６条第２項関連）

経済産業分野ガイドラインの例による。

⑤適用除外（法第１６条第３項関連）

経済産業分野ガイドラインの例による。

(1-2)機微（センシティブ）情報

与信事業者等は、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）については、取得、利用又は第三者提供を行わないこととする。

【例外事項】

①法令等に基づく場合。
②機微（センシティブ）情報が記載されている戸籍謄本その他の本人を特定できる書類を本人特定のために取得、利用、保管する場合。
※官報に掲載された破産者の情報について、当該破産者の本人確認を行うため、当該破産者の本籍地の情報を取得、利用、保管すること等。
③機微（センシティブ）情報に該当する生体認証情報を本人の同意に基づき、本人確認に用いる場合。
④相続手続による権利義務の移転等の遂行に必要な限りにおいて、機微（センシティブ）情報を取得、利用する場合。

(2)個人情報の取得関係（法第１７条～第１８条関連）
①適正取得（法第１７条関連）
経済産業分野ガイドラインの例による。
②利用目的の通知又は公表（法第１８条第１項関連）
以下の事項の他は経済産業分野ガイドラインの例による。
利用目的の通知の方法については、原則として、書面によらなければならない。
③直接書面等による取得（法第１８条第２項関連）
与信事業者は、本人から直接書面に記載された当該本人の個人情報を取得する場合には、経済産業分野ガイドライン2-2-2.(3)の規定にかかわらず、本人の同意を得ることとする。その際、利用目的の明示の方法については、Ⅱ．２．(1)①の例による。
④利用目的の変更（法第１８条第３項関連）
経済産業分野ガイドラインの例による。
⑤適用除外（法第１８条第４項関連）
経済産業分野ガイドラインの例による。

(3)個人データの管理（法第１９条～第２２条関連）
1)データ内容の正確性の確保（法第１９条関連）
以下の事項の他は経済産業分野ガイドラインの例による。
与信事業者等は、保有する個人データの利用目的に応じて保存期間を定め、当該保存期間経過後には当該保有する個人データを消去しなければならない。ただし、法令等に基づく保存期間の定めがある場合には、この限りではない。

2)安全管理措置（法第２０条関連）
以下の事項の他は経済産業分野ガイドラインの例による。
与信事業者等は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のため、組織的、人的、物理的及び技術的な安全管理措置を講じなければならない（経済産業分野ガイドライン2-1-4.「＊電話帳、カーナビゲーションシステム等の取扱いについて」の場合を除く。）。その際、本人の個人データが漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵

害の大きさを考慮し、事業の性質及び個人データの取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講じるものとする。なお、その際には、個人データを記録した媒体の性質に応じた安全管理措置を講じることとする。

また、個人情報の記載されたクレジットカードの申込用紙その他の個人情報データベース等を構成する前の入力帳票についても、個人データに相当する扱いとすることとする。(以下3)〔従業者の監督〕、4)〔委託先の監督〕において同じ。)

また、個人信用情報機関は、その会員が適正に個人の支払能力に関する情報を照会・登録し、個人の支払能力の調査にのみ当該情報を利用することを確保するため、本ガイドライン本文の規定に加え、別紙の取組を講じなければならない。

※なお、「しなければならない」とされている事項の例示については、事業者の参考に供し、またその内容を適切に実現することを促すため、その方法等として想定される事例を明らかにしたものであり、必ずしも各事例に掲げる項目すべてについて実施しなければ直ちに法違反となるものではないし、逆に複数ある事例のうち一つだけ実施していれば十分ということでもない。また、「しなければならない」とされている内容を適切に実現するため、個人データ保護の観点から各事例に掲げた内容より優れている方法を採ることは当然認められる。(以下3)〔従業者の監督〕、4)〔委託先の監督〕において同じ。)

■組織的安全管理措置

①与信事業者等は、個人データの安全管理に関する事項を含んだ個人情報保護に関する考え方や方針に関する宣言を策定し、公表しなければならない。

※「個人データの安全管理に関する事項を含んだ個人情報保護に関する考え方や方針に関する宣言」には、例えば、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が該当する。

②与信事業者等は、本ガイドラインに従った個人データの安全管理措置を定めた規程や手順書等（以下「規程等」という。）を整備しなければならない。

【規程等に記載すべき事項の例】

〔経済産業分野ガイドライン2-2-3-2.の組織的安全管理措置【個人データの取扱いに関する規程等に記載することが望まれる事項の例】に掲げる事項を、【規程等に記載すべき事項の例】として参照。〕

③与信事業者等は、個人データの安全管理に関する従業者の役割及び責任を明確にしなければならない。

その際、与信事業者等は、職務分掌規程、契約書その他の従業者に関する規程類において個人データの安全管理に関する従業者の役割及び責任を具体的に定めなければならない。

なお、「従業者」とは、個人情報取扱事業者の組織内にあって直接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をいい、雇用関係にある従業員（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のみならず、取締役、執行役、理事、監査役、監事、派遣社員等も含まれる。

【明確化すべき役割の例】
・個人データの取扱い（取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄等の作業）における作業責任者及び担当者
・個人データを取り扱う情報システムの運用責任者及び担当者
・個人データを取り扱う部署・支店等（以下「部署等」という。）の役割
・監査責任者

④与信事業者等は、個人情報保護に関する責任者を設置しなければならない。
※上記には、例えば、いわゆる、チーフ・プライバシー・オフィサー（ＣＰＯ）等が該当する。
※個人データの取扱いにおける作業責任者の設置及び作業担当者の限定、個人データを取り扱う情報システム運用責任者の設置及び担当者（システム管理者を含む。）の限定を行うこととする。
⑤与信事業者等は、個人データの管理をする者を、個人データを取り扱う部署等ごとに設置しなければならない。
⑥与信事業者等は、個人データの漏えい等の事故が発生した場合に対処するための以下の報告連絡体制を整備しなければならない。
・個人情報保護に関する責任者等、社内での報告連絡体制。
※なお､個人データの漏えい等の事故が発生した場合の報告連絡体制のみならず、発生する可能性が高い場合に対応するための報告連絡体制についても整備しておくこととする。
・漏えい等の事故による影響を受ける可能性のある本人への情報提供体制（本人に通知し、又は本人が容易に知り得る状態にするための体制）
・経済産業省への報告連絡体制
⑦与信事業者等は、個人データの取扱状況を一覧できる手段を整備し、最新の状態となるように維持しなければならない。

【個人データの取扱状況を一覧できる手段の整備の例】
取得する項目、通知した利用目的、保管場所、保管方法、アクセス権限を有する者、利用期限、その他個人データの適正な取扱いに必要な情報を記した個人データ取扱台帳の整備

⑧与信事業者等は、外部監査その他の本ガイドラインに従った安全管理措置が実施されていることを確認する仕組みを導入しなければならない。
⑨与信事業者等は、個人データの安全管理措置の評価、見直し及び改善をしなければならない。

【安全管理措置の評価、見直し及び改善の仕方の例】
・監査計画の立案と、計画に基づく監査（内部監査又は外部監査）の実施
・監査実施結果の取りまとめと、代表者への報告
・監査責任者から受ける監査報告、個人データに対する社会通念の変化及び情報技術の進歩に応じた定期的な安全管理措置の見直し及び改善

⑩与信事業者等は、自己の取り扱う個人データ（受託者が取り扱うものを含む。）の漏えいに係る二次被害の防止、類似事案の発生回避等の観点から以下のよう

な適切な対処を行わなければならない。
・事実関係を本人に速やかに通知し又は本人が容易に知り得る状態に置くこと。
・可能な限り事実関係等を遅滞なく公表すること。
・事実関係、発生原因、対応策その他の漏えいに関する事項を可能な限り速やかに経済産業省に報告すること。

■人的安全管理措置
①与信事業者等は、雇用契約時及び委託契約時において、非開示契約その他の個人データの安全管理措置に関する事項を盛り込んだ契約を締結しなければならない。
※雇用契約又は委託契約等における非開示条項は、一定期間ごとに確認することとし、また、契約終了後も一定期間有効であるようにすることとする。
※個人データを取り扱う従業者ではないが、個人データを保有する建物等に立ち入る可能性がある者、個人データを取り扱う情報システムにアクセスする可能性がある者についてもアクセス可能な関係者の範囲及びアクセス条件について契約書等に明記することとする。なお、個人データを取り扱う従業者以外の者には、情報システムの開発・保守関係者、清掃担当者、警備員等が含まれる。
②与信事業者等は、職務規程等に、個人データの安全管理措置に関する事項を盛り込まなければならない。

【職務規程等に記載すべき事項の例】
・本ガイドラインに従った安全管理措置に関する事項
・故意又は過失により個人データを漏洩又は流出した場合の従業員に対する懲戒及び会社に対する損害賠償に関する事項

③与信事業者等は、従業者に対し、個人データの安全管理に関する教育・訓練を継続的に実施しなければならない。

【個人データの安全管理に関する教育・訓練を継続的に実施している例】
・個人データの安全管理に関する教育・訓練の計画の作成
・個人データの安全管理に関する教育・訓練の実施に必要なカリキュラム等の整備
・定期的な（例えば、年1回）又は従業者の監督のために必要と判断した時ごとの教育・訓練の実施
・教育・訓練の実施状況の定期的な確認

■物理的安全管理措置
①与信事業者等は、個人データを取り扱う施設に応じて、 以下の管理を行わなければならない。
（事務施設及び個人データ処理施設における管理）
・施錠等による施設及び室の管理
（個人データ処理施設における管理）
・入退館（室）をする者の資格付与及び認証
・入退館（室）の記録

※「事務施設」とは、例えば本社、支社、営業店等の執務室を含み、「個人データ処理施設」とは、例えば電算センター、コールセンター、サーバルーム等を含む。

②与信事業者等は、個人データ自体、又は個人データを含む書類、磁気媒体等の盗難を防止するための対策を行わなければならない。

【盗難を防止するための対策の例】
・離席時の個人データを記した書類、媒体、携帯可能なノートパソコン等の机上等への放置の禁止
・離席時のパスワード付スクリーンセイバ等の起動
・個人データを含む媒体等の施錠保管
・個人データを表示されている機器の画面を第三者が見えないようにする措置の実施
・氏名、住所、メールアドレス等を記載した個人データとそれ以外の個人データの分離保管
・個人データを取り扱う情報システムの操作マニュアルの机上等への放置の禁止

③与信事業者等は、機器・装置等を物理的に保護しなければならない。

【物理的な保護対策の例】
・入退館（室）管理をしている物理的に保護された室内への設置
・施錠されたラック等内への設置
・敷地外への持出し禁止
・地震等による転倒防止対策
・停電・過電流からの保護対策
・防火・防水対策

■技術的安全管理措置

①与信事業者等は、個人データへのアクセスにおける識別と認証を行わなければならない。

【識別と認証の例】
・IDとパスワードによる認証
※IDとパスワードを利用する場合には、パスワードの有効期限の設定、同一又は類似パスワードの再利用の制限、最低パスワード文字数の設定、一定回数以上ログインに失敗したIDを停止する等の措置を講じることとする。
・生体認証
・端末等の機器に対する電子証明書を利用したクライアント認証

②与信事業者等は、個人データへのアクセス制御を行わなければならない。

【アクセス制御の例】
・個人データへのアクセス権限を付与すべき従業者数の最小化
・識別に基づいたアクセス制御
・個人データを格納した情報システムへの同時利用者数の制限
・個人データを格納した情報システムの利用時間の制限（例えば、休業日や業務時間外等の時間帯には情報システムにアクセスできないようにする等）
・個人データを取り扱う情報システムに導入したアクセス制御機能の有効性の検証（例え

ば、ウェブアプリケーションの脆弱性有無の検証）
・パスワードの適切な管理（例えば、パスワードをメモしない等）
・ネットワークを介して外部から個人データにアクセスできる通信経路及び端末の限定
・従業者に付与するアクセス権限の最小化
・個人データを格納した情報システムへの無権限アクセスからの保護（例えば、ファイアウォール、ルータ等の設定）
・個人データにアクセス可能なアプリケーションの無権限利用の防止（例えば、アプリケーションシステムに認証システムを実装する、業務上必要となる従業者が利用するコンピュータのみに必要なアプリケーションシステムをインストールする、業務上必要な機能のみメニューに表示させる等）

③与信事業者等は、個人データへのアクセス権限の管理を行わなければならない。

【アクセス権限の管理の例】
・個人データにアクセスできる者を許可する権限管理の適切な実施（例えば、個人データにアクセスする者の登録を行う作業担当者が適当であることを十分に審査し、その者だけが、登録等の作業を行えるようにする）
・業務内容に照らしたアクセス権限の妥当性に関する定期的な見直し
・退職者、異動者等のアクセス権限の速やかな剥奪

④与信事業者等は、個人データのアクセスの記録を行わなければならない。

【アクセスの記録の例】
・個人データへのアクセスや操作の成功と失敗の記録（例えば、個人データへのアクセスや操作を記録できない場合には、情報システムへのアクセスの成功と失敗の記録）
・採取した記録の漏えい、滅失及びき損からの適切な保護

※個人データを取り扱う情報システムの記録が個人情報に該当する場合があることに留意する。

⑤与信事業者等は、個人データを取り扱う情報システムに対する不正ソフトウェア対策を行わなければならない。

【不正ソフトウェア対策の例】
・ウイルス対策ソフトウェアの導入
・オペレーティングシステム（ＯＳ）、アプリケーション等に対するセキュリティ対策用修正ソフトウェア（いわゆる、セキュリティパッチ）の適用
・不正ソフトウェア対策の有効性・安定性の確認（例えば、パターンファイルや修正ソフトウェアの更新の確認）
・システム管理者が許可していないソフトウェアの使用禁止

⑥与信事業者等は、個人データの移送・送信時における適切な対策を実施しなければならない。

【適切な対策の例】
・個人データを含む電子媒体を移送する場合、暗号化又はパスワードロックを行うこと。
・インターネットを経由して電子メールに添付して個人データを送信する場合に、電子メール自体を暗号化すること。

※なお、暗号鍵の長さ、使用する暗号アルゴリズム、パスワードの文字数や複雑

性については、個人データを含む電子媒体を紛失した場合に本人が被る権利利益の大きさを考慮し適切に設定することが望ましい。

⑦与信事業者等は、個人データを取り扱う情報システムの動作確認時の対策を行わなければならない。

【個人データを取り扱う情報システムの動作確認時に行う対策の例】
・情報システムの動作確認時のテストデータとして個人データを利用することの禁止
・情報システムの変更時に、それらの変更によって情報システム又は運用環境のセキュリティが損なわれないことの検証
・ネットワークを介して外部からシステム管理を行う場合には、適切な認証機能、暗号機能及びアクセス制御機能の導入

⑧与信事業者等は、個人データを取り扱う情報システムを監視しなければならない。

【個人データを取り扱う情報システムの監視の例】
・個人データを取り扱う情報システムの使用状況の監視
・個人データへのアクセス状況（操作内容も含む）の監視

※個人データを取り扱う情報システムを監視した結果の記録が個人情報に該当する場合があることに留意する。

3)従業者の監督（法第２１条関連）

以下の事項の他は経済産業分野ガイドラインの例による。

①与信事業者等は、従業者に対して、法第２０条に基づく安全管理措置を遵守させるよう、適切にモニタリングしなければならない。

②与信事業者等は、モニタリングの結果、従業者に問題があった場合には適切な指示・命令を行わなければならない。

4)委託先の監督（法第２２条関連）

以下の事項の他は経済産業分野ガイドラインの例による。

①与信事業者等は、委託先の選定に当たっては、あらかじめ定めた選定基準に基づき、個人データの取扱いに関して適切な者を選定しなければならない。

【選定基準に含まれるべき事項の例】
・委託業務の受注実績
・委託元自らが実施しているルール又は本ガイドライン等を遵守できる体制
・委託業務に係る個人データの取扱手順の整備・実施状況
・委託業務に係る個人データの安全管理措置の整備・実施状況
・過去の個人情報の漏えい等に係る問題発生事実及び再発防止措置の内容と実施状況等

②与信事業者等は、委託契約において、個人データの取扱いに関して委託元、委託先双方が同意した内容を契約に盛り込まなければならない。

【契約書に盛り込むべき事項の例】
・委託業務に係る個人情報の利用目的（委託先における利用目的の特定）に関する事項
・委託元及び委託先の責任の明確化に関する事項

・個人データの取扱いに係る責任者の選任及び個人データを取り扱う従業者の特定に関する事項
・個人データ及び委託業務結果の授受及び配送に関する事項
・個人データ及び記録媒体の保管方法・保管場所に関する事項
・個人データ及び記録媒体の保有期間及び返還・消去・廃棄方法に関する事項
・個人データの漏えい防止、盗用禁止に関する事項
・委託契約に係る個人データの第三者提供等の禁止に関する事項
・委託契約範囲外の加工、利用の禁止
・委託契約範囲外の複写、複製の禁止
・委託契約の目的のために必要となるもの以外の個人データの取扱いの禁止に関する事項
・再委託に関する事項
・個人データの取扱状況に関する委託元への報告の内容及び頻度に関する事項
・委託先への立入検査、報告徴収に係る事業者の権利に関する事項
・委託先における監査の実施又は事業者による監査実施の権利に関する事項
・漏えい等の事故発生時の危機管理・危機対応手順等に基づいた対応・措置に関する事項
・契約に違反した場合における損害賠償及び契約の解除に関する事項

③与信事業者等は、委託先が契約内容を確実に遵守していることを確認しなければならない。

【確認の際の実施事項の例】
・個人データ管理者による委託先の監督に関する業務の実施
・委託先からの作業状況・ルール遵守状況等に関する定期的な報告
・委託先からの作業状況・ルール遵守状況等の確認のために必要な証拠等の提出
・再委託先の監督状況を確認するために必要な証拠等の提出

(4)第三者への提供（法第２３条関連）

①原則（法第２３条第１項関連）

以下の事項の他は経済産業分野ガイドラインの例による。

個人データを提供する第三者については、原則としてその氏名又は名称を記載することにより、特定しなければならない。なお、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をいい、自然人、法人その他の団体を問わない。

与信事業者は、第三者としての個人信用情報機関に対し個人データを提供する場合には、あらかじめ本人の同意を得なければならない。その場合には、個人データが個人信用情報機関及び当該個人信用情報機関と提携する個人信用情報機関並びにこれらの会員企業にも提供されることを書面に明記しなければならない。その際、個人信用情報機関についての消費者の理解を容易にするための措置を講じなければならない。

第三者に提供される個人データの項目については、個人データを提供する第三者ごとに記載することとする。

【個人信用情報機関の示し方の例】

申込者は、契約者の本契約に関する客観的な取引事実に基づく個人情報が、当社の加盟する個人信用情報機関（個人の支払能力に関する情報の収集及び会員に対する当該情報の提供を業とする者）に下表に定める期間登録され、当社が加盟する個人信用情報機関及び当該機関と提携する個人信用情報機関の加盟会員により、契約者の支払能力に関する調査のために利用されることに同意します。

当社が加盟する個人信用情報機関及び当社が加盟する個人信用情報機関が提携する個人信用情報機関の名称及び連絡先等は以下のとおりです。

会社名	住所 電話番号	ホームページアドレス
株式会社○○ （加盟先）	東京都千代田区○○ ○○－○○○○－○○○○	http://www.○○/
株式会社△△情報センター（提携先）	東京都千代田区△△ △△－△△△△－△△△△	http://www.△△/
□□情報センター （提携先）	東京都千代田区□□ □□－□□□□－□□□□	http://www.□□/

株式会社○○：主に××会社を加盟会員とする個人信用情報機関

株式会社△△情報センター：××協会に加盟する企業を会員とする個人信用情報機関

□□情報センター：主に××業者を加盟会員とする個人信用情報機関

【個人データの項目及び登録期間の示し方の例】

項目 会社名	A情報	B情報	C情報
株式会社○○ （加盟先）	～の日から ××ヶ月間	～の日から ××年間	～の日から ××年間
株式会社△△情報センター（提携先）	○	－	○
□□情報センター （提携先）	○	○	－

個人信用情報機関の加入資格に関する規約、個人信用情報機関及び当該個人信用情報機関と提携する個人信用情報機関に加入する会員企業のリストについては、本人が容易に知り得る状態に置くこととし、個人信用情報機関の規約等においては、加入資格のある企業の外延が明確になるよう、加入資格、加入企業の業務、業務違反に対する制裁措置等について、できる限り具体的に記載することとする。

個人データを提供される第三者における利用目的は、できる限り具体的に記載しなければならない。

【具体的な記載の事例】

（取得、利用、提供、預託する個人情報）

会社名	利用目的	利用情報	連絡先
（株）B	与信判断・与信後の管理のため	2．(1)①のⅰ）ⅱ）ⅲ）ⅳ)	東京都千代田区○○ TEL　△△ E-mail　□
	○○事業における宣伝物等、営業案内の利用のため	Ⅱ2．(1)①のⅰ）ⅱ）	
（株）C	○○事業における宣伝物等、営業案内の利用のため	2．(1)①のⅰ）ⅱ）	東京都千代田区○○ TEL　△△ E-mail　□

②オプトアウト（法第２３条第２項関連）

本分野においてオプトアウトを利用すると、支払困難に陥った債務者が、個人信用情報機関を通じた当該債務者の個人の支払能力に関する情報の利用を停止できることとなり、個人信用情報機関を通じた情報交流により適正与信の確保、多重債務者問題への対応を図る目的が達成されなくなるおそれがあること等の問題に留意して、経済産業分野ガイドラインの規定にかかわらず、本分野においてはオプトアウトを利用しないこととする。

③第三者に該当しないもの（法第２３条第４項関連）

以下の事項の他は経済産業分野ガイドラインの例による。

ⅲ．共同利用（法第２３条第４項第３号関連）

与信事業者は、グループ企業において当該与信事業者が他の事業者と法第２３条第４項第３号の共同利用を行う際には、同意を確認する書面においてその範囲が明確になるように示すこととし、範囲の明確化に当たっては、原則として個別企業名を列挙することとする。また、そのグループを構成する個別企業名を本人が容易に知り得る状態に置かなければならない。

※なお、同号は、個人データの管理について責任を有する者以外の共同利用を行う者における安全管理等の責任を免除する趣旨ではない。

【グループ企業での共同利用の範囲の示し方の事例】
・当社の子会社である㈱A、㈱B、㈱C・・・・・・㈱Z
・当社及び有価証券報告書等に記載されている、当社の子会社
・当社及び有価証券報告書等に記載されている、連結対象会社及び持分法適用会社

「利用する者の利用目的」は、できる限り具体的に記載しなければならない。具体的には、Ⅱ．２．(1)①の事例による。

④ 雇用管理に関する個人データ関連

経済産業分野ガイドラインの例による。

(5)保有個人データに関する事項の公表、保有個人データの開示・訂正・利用停止

等（法第２４条～第３０条関連）

1)保有個人データに関する事項の公表等（法第２４条関連）

経済産業分野ガイドラインの例による。

2)保有個人データの開示（法第２５条関連）

経済産業分野ガイドラインの例による。

3)保有個人データの訂正等（法第２６条関連）

経済産業分野ガイドラインの例による。

4)保有個人データの利用停止等（法第２７条関連）

経済産業分野ガイドラインの例による。

5)理由の説明（法第２８条関連）

経済産業分野ガイドラインの例による。

6)開示等の求めに応じる手続（法第２９条関連）

以下の事項の他は経済産業分野ガイドラインの例による。

与信事業者等は、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にしなければならない。

なお、個人情報の保護に関する法律施行令（平成１５年政令第５０７号）第８条第２項の代理人による開示等の求めに対して、与信事業者等が本人にのみ直接開示等することは妨げられない。

7)手数料（法第３０条関連）

経済産業分野ガイドラインの例による。

(6)苦情の処理（法第３１条関連）

経済産業分野ガイドラインの例による。

(7)経過措置（法附則第２条～第５条関連）

経済産業分野ガイドラインの例による。

３．民間団体付属の研究機関等における個人情報の取扱いについて

経済産業分野ガイドラインの例による。

Ⅲ.「勧告」、「命令」及び「緊急命令」についての考え方

以下の事項の他は経済産業分野ガイドラインの例による。

本ガイドラインにおいて、「しなければならない」と記載されている規定について、それに従わなかった場合は、法第１６条から第１８条まで、第２０条から第２７条まで又は第３０条第２項の規定違反と判断され得る。違反と判断された際、実際、「勧告」を行うこととなるのは、個人の権利利益を保護するため必要があると認めるときである。一方、本ガイドライン中、「こととする」と記載されている規定については、それに従わなかった場合でも、原則として法第１６条から第１８条まで、第２０条から第２７条まで又は第３０条第２項の規定違反と判断されることはないが、個人情報保護の推進の観点から与信

事業者等においては、できる限り取り組むよう努めなければならない。

Ⅳ．ガイドラインの見直し

経済産業分野ガイドラインの例による。

Ⅴ．個人情報取扱事業者がその義務等を適切かつ有効に履行するために参考となる事項・規格

経済産業分野ガイドラインの例による。

附　則（平成１８年１０月１６日経済産業省告示第３１２号）

１　この告示は、公布の日から施行する。

２　この告示による改正後の別紙の２－１－３の規定は、平成１９年１月１日から適用する。

３　この告示による改正後の別紙の２－２の規定は、平成１９年４月１日から適用し、この告示による改正前のⅡの２の（３）の２）の規定による個人信用情報機関の会員に対するモニタリングについては、平成１９年３月３１日までの間はなお従前の例による。

附　則（平成２１年１０月９日経済産業省告示第３０１号）

この告示は、公布の日から施行する。

（別紙）個人信用情報機関における取組について

１．個人信用情報機関自らの安全管理措置

１－１　複数の個人信用情報機関が各々の保有個人データを共通の情報処理会社に委託してその個人情報データベース等に集約して管理している場合には、当該個人情報データベース等にアクセス可能なすべての個人信用情報機関は、同様の高い水準の安全管理措置を講じなければならない。また、当該個人情報データベース等へのアクセスと情報保護に関してそれぞれの責任関係を明確にしておかなければならない。

１－２　個人信用情報機関は、個人情報データベース等へのアクセスを伴う業務を取り扱うフロア（以下「業務フロア」という）については、消費者への開示スペース等、他のフロアとは構造的に隔離されているようにしなければならない。

１－３　個人信用情報機関は、業務フロアの出入り口については、ＩＣカード認証等により電子的に入退室の認証管理を行い、その入退室記録が電子的に一定期間保存される仕組みを採用しなければならない。

１－４　個人信用情報機関は、業務フロア内については、監視カメラにより定常的に室内状況を記録し、その映像を一定期間保存することとし、管理責任者が定期的に記録をチェックしなければならない。

１－５　個人信用情報機関は、個人情報データベース等にアクセスするパソコン端末については、指紋認証など起動時及び一定時間離席時のアクセス認証を行い、そのアクセス記録を一定期間保存することとする仕組みにしなければならない。

２．個人信用情報機関による会員管理

２－１　入会審査等

２－１－１　個人信用情報機関は、新たに入会する会員について、当該個人信用情報機関の個人情報データベース等にアクセスする会員の照会端末の設置状況及びアクセス権限の設定状況の確認を行うこととする。そのほか、個人情報データベース等にアクセスすることについて適正な事業者のみ会員となるようあらかじめ定めた入会審査基準に基づき、厳正に入会審査を行うこととする。

２－１－２　個人信用情報機関は、会員が入会審査基準を満たし続けているかどうか定期的に確認することとする。

２－１－３　個人信用情報機関は、法の制定に伴い入会審査基準を改定している場合には、改定前の入会審査基準により入会した会員を改定後の入会審査基準に基づいて再審査をすることとする。

２－１－４　会員においては、入会後も個人信用情報機関によるモニタリングに協力することが求められ、個人信用情報機関からの求めに応じて必要な情報を提供できるよう、与信申込書や契約書等、個人信用情報機関の個人情報データベース等へのアクセスが正当なものであることを証明することができる資料等を保管しておく必

要があるところ、個人信用情報機関は、これらの事項を入会審査基準や会員規約に盛り込む等必要なルールを定めることとする。

２－２　会員モニタリング

個人信用情報機関は、会員が、消費者からの与信申込みがないにもかかわらず任意の個人について個人信用情報機関の個人情報データベース等にアクセスして情報を入手する等の不正利用をすることのないよう、会員に対する必要かつ適切なモニタリングを行うこととする。そのほか、個人信用情報機関は、会員が、個人信用情報機関の個人情報データベース等に適正にアクセスして入手した個人の支払能力に関する情報を支払能力調査目的以外の目的に不正利用することのないよう、会員に対する必要かつ適切なモニタリングを行うこととする。また、個人信用情報機関は、会員モニタリングの運用基準についても整理することとする。

２－３　不正利用に対する処分

２－３－１　個人信用情報機関は、会員による上記の不正利用があった場合、あらかじめ定めた処分に関する規程に基づき、公表、利用停止、退会その他の処分をすることとする。

２－３－２　個人信用情報機関は、どのような不正についてどの処分をするか、また、処分をするか否かの判断基準、その判断を行うための組織体制・意思決定プロセスを予め明確に定めておくこととする。

３．透明性確保等

３－１　個人信用情報機関は、１．の安全管理措置、２．の会員管理の状況や、監査の内容、結果について、行政に報告し、セキュリティ上支障のある部分を除いて一般に公表することとする。

３－２　個人信用情報機関は、自社からの情報漏洩や会員からの許容された利用目的を逸脱した利用については、行政への報告、一般への実績の公表を行うこと及び被害にあった個人への通知がなされるようにすることとする。

３－３　個人信用情報機関は、行政に対して定期的に安全管理措置の履行状況について報告することとする。

４．外部監査

個人信用情報機関は、本ガイドラインに従った取組が確実に実施されていることを確認する仕組みとして、外部監査を行うこととする。