信用分野における個人情報保護に関するガイドライン

令和４年４月
個人情報保護委員会
経済産業省

信用分野における個人情報保護に関するガイドライン

目次

Ⅰ．目的等

１．本ガイドラインは、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。）、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。以下「施行令」という。）及び個人情報の保護に関する法律施行規則（平成 28 年個人情報保護委員会規則第３号。以下「施行規則」という。）を踏まえ、個人情報の保護に関する法律についてのガイドライン（通則編）（平成 28 年個人情報保護委員会告示第６号。以下「通則ガイドライン」という。）を基礎として、法第６条及び第９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、及び与信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、通則ガイドライン、個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）（平成 28 年個人情報保護委員会告示第７号。以下「外国第三者提供ガイドライン」という。）、同ガイドライン（第三者提供時の確認・記録義務編）（平成 28 年個人情報保護委員会告示第８号）、同ガイドライン（仮名加工情報・匿名加工情報編）（平成 28 年個人情報保護委員会告示第９号）及び同ガイドライン（認定個人情報保護団体編）（令和３年個人情報保護委員会告示第７号）が適用される。

２．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、これに従わなかった場合、法の規定違反と判断される可能性がある。

一方、「こととする」と記載されている規定については、これに従わなかったことをもって法の規定違反と判断されることはないが、「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鑑み、その適正な取扱いが図られなければならない」とする法の基本理念（法第３条）を踏まえ、信用分野における個人情報の適正な取扱いを確保する観点から、事業者の特性や規模に応じ可能な限り対応することが望まれるものである。

３．本ガイドラインにおいて記載した具体例については、これに限定する趣旨で記載したものではなく、また、個別ケースによって別途考慮すべき要素もあり得るので注意を要する。

４．信用分野における認定個人情報保護団体が個人情報保護指針を作成又は変更し、また、信用分野における事業者団体等が事業の実態及び特性を踏まえ、当該事業者団体等の会員企業等を対象とした自主的ルール（事業者団体ガイドライン等）を作成又は変更することもあり得るが、その場合は、認定個人情報保護団体の対象事業者や事業者団体等の会員企業等は、個人情報の取扱いに当たり、個人情報の保護に関する法令、通則ガイドライン及び本ガイドライン等に加えて、当該指針又はルールに沿った対応を行う必要がある。特に、認定個人情報保護団体においては、認定個人情報保護団体が対象事業者に対し個人情

報保護指針を遵守させるために必要な措置をとらなければならないこととされていることを踏まえることも重要である。

５．与信事業者は、個人情報の漏えい、滅失又は毀損（以下「漏えい等」という。）等を防止等するため、個人情報の保護に関する法令、通則ガイドライン及び本ガイドラインのほか、関係法令等に従い、個人情報の適正な管理体制を整備する必要がある。

Ⅱ．法令解釈指針・事例

１．定義等（法第２条関係）

⑴　「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（以下「割賦販売等」という。）を業として行う者をいう。

⑵　「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与信事業者に対する当該情報の提供を業とする者をいう。

⑶　「本人の同意」

以下の事項の他は通則ガイドラインの例による。

与信事業者は、法第 18 条、第 27 条、第 28 条及び第 31 条第１項第１号（与信事業者が個人関連情報取扱事業者から同項の規定による個人関連情報の提供を受けて個人データとして取得する場合に限る。）に定める本人の同意を得る場合には、原則として、書面（電磁的記録を含む。以下同じ。）によることとする。

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することとする。また、文字の大きさ、文章の表現その他の本人の理解に影響する事項について、本人の理解を容易にするための措置を講ずることとする。

同意の取得は、本人の同意の意思が反映される方法により行うこととする。

⑷　⑴から⑶に定めるもののほか、本ガイドラインにおける用語は、他に特段の定めのない限り、個人情報の保護に関する法令の定義に従う。

２．与信事業者の義務等

⑴　個人情報の利用目的関係（法第 17 条～第 18 条関係）

①　利用目的の特定（法第 17 条関係）

以下の事項の他は通則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。

特に、与信事業者が個人信用情報機関に個人情報を提供し、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。この場合、特定した利用目的について本人の同意を得ることとする。

なお、利用目的を変更する場合で、変更前の利用目的と関連性を有すると合理的に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。

利用目的	利用情報	連絡先等
与信判断・与信後の管理のため	ⅰ） ⅱ） ⅲ） ⅳ）	東京都千代田区〇〇 TEL △△ E-mail □
〇〇事業における宣伝物等、営業案内の利用のため	ⅰ） ⅱ）	

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　利用目的による制限（法第 18 条関係）

以下の事項の他は通則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。

与信事業者は、個人信用情報機関から得た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しないこととする。

⑵　機微（センシティブ）情報

1）　与信事業者は、法第２条第３項に定める要配慮個人情報並びに労働組合への加盟、門地、本籍地、保健医療及び性生活（これらのうち要配慮個人情報に該当するものを

除く。）に関する情報（本人、国の機関、地方公共団体、学術研究機関等、法第 57 条第１項各号に掲げる者若しくは施行規則第６条各号に掲げる者により公開されているもの、又は、本人を目視し、若しくは撮影することにより取得するその外形上明らかなものを除く。以下「機微（センシティブ）情報」という。）については、次に掲げる場合を除くほか、取得、利用又は第三者提供を行わないこととする。

① 法令等に基づく場合
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
③ 公衆衛生の向上又は児童の健全な育成の推進のため特に必要がある場合
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
⑤ 法第 18 条第３項第６号に掲げる場合に機微（センシティブ）情報を利用する場合、法第 20 条第２項第６号に掲げる場合に機微（センシティブ）情報を取得する場合、又は法第 27 条第１項第７号に掲げる場合に機微（センシティブ）情報を第三者提供する場合
⑥ 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、利用又は保管する場合
※ 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、利用又は保管すること等。
⑦ 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、利用又は第三者提供する場合
⑧ 信用分野の事業の適切な業務運営を確保する必要性から、本人の同意に基づき業務遂行上必要な範囲で機微（センシティブ）情報を取得、利用又は第三者提供する場合
⑨ 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

2) 与信事業者は、機微（センシティブ）情報を、1)に掲げる場合に取得、利用又は第三者提供する場合には、1)に掲げる事由を逸脱した取得、利用又は第三者提供を行うことのないよう、特に慎重に取り扱うこととする。

3) 与信事業者は、機微（センシティブ）情報を、1)に掲げる場合に取得、利用又は第三者提供する場合には、例えば、要配慮個人情報を取得するに当たっては、法第 20 条第２項に従い、あらかじめ本人の同意を得なければならないとされていることなど、個人情報の保護に関する法令等に従い適切に対応しなければならないことに留意する。

4)　与信事業者は、機微（センシティブ）情報を第三者へ提供するに当たっては、法第27条第２項（オプトアウト）の規定を適用しないこととする。なお、機微（センシティブ）情報のうち要配慮個人情報については、同項において、オプトアウトを用いることができないとされていることに留意する。

⑶　個人情報の取得関係（法第21条関係）

①　利用目的の通知又は公表

以下の事項の他は通則ガイドラインの例による。

信用分野に関する事業における利用目的の通知の方法については、原則として、書面によることとする。

②　直接書面等による取得

以下の事項の他は通則ガイドラインの例による。

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、利用目的について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.⑴①の例による。

⑷　個人データの管理（法第22条～第26条関係）

1)　データ内容の正確性の確保（法第22条関係）

以下の事項の他は通則ガイドラインの例による。

与信事業者は、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することとする。

2)　安全管理措置（法第23条関係）

以下の事項の他は通則ガイドラインの例による。

与信事業者は、その取り扱う個人データの漏えい等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。また、外国において個人データを取り扱う場合には、外的環境の把握を行った上で、これらの安全管理措置を講じなければならない。

安全管理措置を講ずるための具体的な手法については、個人データが漏えい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（取り扱うデータの性質及び量を含む。）、個人データを記録した媒体の性質等に起因するリスクに応じ、必要かつ適切な内容とすべきものであるため、必ずしも次に掲げる措置の例示については全てを講じなければならないわけではなく、また、適切な手法はこれらの例示の内容に限られない。なお、個人データ保護の観点から各事例に掲げる内容より優れている手法を採用することは、より望ましい対応

である。

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信用分野に係る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。)

■ 組織的安全管理措置

① 与信事業者は、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(以下「個人情報保護に関する考え方や方針に関する宣言」という。)を策定し、公表しなければならない。

※ 「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を整備しなければならない。

③ 与信事業者は、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。

④ 与信事業者は、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
- 個人データの安全管理に関する従業者の役割及び責任
- 故意又は過失により個人データを漏えい又は流出した場合の懲戒処分及び会社に対する損害賠償に関する事項

なお、「従業者」とは、与信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。

【役割及び責任の明確化の例】

・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・支店等の役割
・監査責任者

⑤　与信事業者は、個人データの漏えい等の事故が発生し、又は発生したおそれがある場合に対処するための以下の体制を整備しなければならない。
・社内での報告連絡体制
・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
・経済産業省への報告連絡体制

⑥　与信事業者は、個人データの取扱状況を確認できる手段を整備しなければならない。

【個人データの取扱状況を確認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

⑦　与信事業者は、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。

⑧　与信事業者は、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

■　人的安全管理措置

①　与信事業者は、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継続的な教育・訓練の例】
- ・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 与信事業者は、個人データを取り扱う施設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の例）
- ・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の例）
- ・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】
- ・個人データを含む媒体等の施錠保管
- ・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

③ 与信事業者は、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

■ 技術的安全管理措置

① 与信事業者は、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ずることとする。
・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等からの適切な保護

※　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侵害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。

■　外的環境の把握

①　与信事業者は、外国において個人データを取り扱う場合、当該外国の個人情報の保護に関する制度等を把握した上で、個人データの安全管理のために必要かつ適切な措置を講じなければならない。

3)　従業者の監督（法第 24 条関係）

以下の事項の他は通則ガイドラインの例による。

①　与信事業者は、従業者に対して、法第 23 条に基づく安全管理措置を遵守させるよう、適切に監督しなければならない。

②　与信事業者は、監督の結果、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 25 条関係）

以下の事項の他は通則ガイドラインの例による。

①　与信事業者は、委託先の選定に当たっては、委託先における組織体制の整備並びに安全管理に係る基本方針及び取扱規定の策定状況等を選定基準に定め、必要に応じて個人データを取り扱う場所に赴く方法（テレビ会議システム等（映像と音声

の送受信により相手の状態を相互に認識できる方法をいう。）を利用する方法を含む。以下、⑸第三者への提供及び、⑹個人関連情報の第三者提供の制限等において同じ。）又はこれに代わる合理的な方法による確認を行った上で、当該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。

【選定基準の項目の例】
- 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。

【委託契約書の記載項目の例】
- 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　与信事業者は、委託先が契約内容を確実に遵守していることを定期的又は随時に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

5)　個人データの漏えい等の報告等（法第 26 条関係）

以下の事項の他は通則ガイドラインの例による。

与信事業者は、施行規則第７条各号に定める事態を知ったときは、通則ガイドライン 3-5-3（個人情報保護委員会への報告）に従って、個人情報保護委員会（法第 147 条の規定により経済産業大臣等が報告を受理する権限の委任を受けている場合には、経済産業大臣等。）に報告しなければならない。

個人データであるクレジットカード番号については、クレジットカード番号のみの漏えい等であっても、施行規則第７条第２号の規定する「不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等」に該当するため、留意すること。なお、以下の場合には、直ちに「不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等」に該当するものではない。

・　個人データであるクレジットカード番号の下４桁のみとその有効期限の組合せが漏えい等した場合
・　無効化されたクレジットカードに係るクレジットカード番号が漏えい等した場合

⑸　第三者への提供（法第 27 条～第 30 条関係）

①　原則

以下の事項の他は通則ガイドラインの例による。

与信事業者は、法第 27 条に従い、個人データの第三者提供についての同意を得る際には、原則として、書面によることとし、当該書面における記載を通じて、

・　個人データの提供先の第三者
・　提供先の第三者における利用目的

・　第三者に提供される個人データの項目

を本人に認識させた上で同意を得ることとする。

本人の同意を得ようとする時点において、個人データの提供先の第三者が特定できない場合には、個人データの提供先の第三者に代わる本人に参考となるべき情報を本人に認識させた上で同意を得ることとする。当該情報としては、次に掲げる例が考えられる。

（例）

・　提供先の第三者の範囲や属性に関する情報

なお、個人データの提供先の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】

（個人データの提供先の第三者及び利用目的）

会社名	利用目的	利用情報	連絡先
㈱Ａ	与信判断・与信後の管理のため	２．(1)①のⅰ）ⅱ）ⅲ）ⅳ）	東京都千代田区〇〇 TEL △△ E-mail □
	〇〇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）	
㈱Ｂ	〇〇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）	東京都千代田区〇〇 TEL △△ E-mail □

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の会員企業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することとする。その際、個人信用情報機関についての本人の理解を容易にするための措置を講ずることとする。

【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Ｃ（加盟先）	東京都千代田区〇〇 〇〇－〇〇〇〇－〇〇〇〇	http://www.〇〇/
株式会社Ｄ情報センター（提携先）	東京都千代田区△△ △△－△△△△－△△△△	http://www.△△/
Ｅ情報センター（提携先）	東京都千代田区□□ □□－□□□□－□□□□	http://www.□□/

株式会社Ｃ：主に××会社を加盟会員とする個人信用情報機関

株式会社Ｄ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

Ｅ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Ｃ（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Ｄ情報センター（提携先）	〇	－	〇
Ｅ情報センター（提携先）	〇	〇	－

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。

② オプトアウト

以下の事項の他は通則ガイドラインの例による。

与信事業者は、個人の支払能力に関する情報を個人信用情報機関へ提供するに当たっては、法第 27 条第２項の規定を適用しないこととし、Ⅱ．２．⑸①に従い本人の同意を得ることとする。

③ 第三者に該当しないもの

以下の事項の他は通則ガイドラインの例による。

・ 共同利用

与信事業者は、法第 27 条第５項第３号に定める「通知」は原則として書面によることとする。

「共同して利用する者の範囲」の通知等については、原則として個別企業名を列挙することとする。また、共同して利用する者の外延を示すことにより本人に通知等する場合には、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しなければならない。

※ なお、同号は、同号に定める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。

【共同して利用する者の外延の示し方の事例】

・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、当社の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．⑴①の事例による。

④ 外国にある第三者への提供の制限

以下の事項の他は通則ガイドラインの例による。

ア 与信事業者は、法第 28 条第１項に従い、外国にある第三者への個人データの提供を認める旨の本人の同意を得る際には、原則として、書面によることとし、当該書面における記載を通じて、施行規則第 17 条第２項から第４項までの規定により情報提供が求められる事項に加えて、

・個人データの提供先の第三者

・提供を受けた第三者における利用目的

・第三者に提供される個人データの項目

を本人に認識させた上で同意を得ることとする。

本人の同意を得ようとする時点において、個人データの提供先の第三者が特定できない場合には、個人データの提供先の第三者に代わる本人に参考となるべき情報を本人に認識させた上で同意を得ることとする。当該情報としては、次に掲げる情報が考えられる。

（例）

・提供先の第三者の範囲や属性に関する情報

また、事業者があらかじめ作成された同意書面を用いる場合には、文字の大きさ及び文章の表現を変えること等により、外国にある第三者への提供に関する条項が他の個人情報の取扱いに関する条項等と明確に区別され、本人に理解されることが望ましい。

イ　法第 28 条第１項の規定により本人の同意を得ようとする時点において、個人データの提供先の第三者が所在する外国が特定できない場合には、特定できない旨及びその具体的な理由（提供先が定まる前に本人同意を得る必要性を含む。）を情報提供するとともに、外国の名称に代わる本人に参考となるべき情報の提供が可能である場合には、当該情報を提供しなければならない。例えば、本人の同意を得ようとする時点において、移転先となる外国の候補が具体的に定まっており、当該候補となる外国の名称等、外国の名称に代わる本人に参考となるべき情報の提供が可能であるにもかかわらず、これを本人に情報提供しなかった場合は、同項及び施行規則第 17 条第３項に基づく適法な情報提供とは認められない。したがって、この場合、与信事業者は、同条第２項から第４項までの規定により情報提供が求められる事項を本人に改めて提供した上で、外国にある第三者への個人データの提供を認める旨の本人の同意を得なければならない。なお、改めて情報提供する際には、Ⅱ．２．（５）④アにおける規定にも留意することとする。

また、与信事業者は、事後的に提供先の第三者が所在する外国を特定できた場合には、本人の求めに応じて、施行規則第 17 条第２項第１号及び第２号に掲げる事項について情報を提供することとする。また、事後的に提供先の第三者が講ずる個人情報の保護のための措置についての情報提供が可能となった場合には、本人の求めに応じて、同項第３号に掲げる事項について情報を提供することとする。このような情報提供の求めが可能である旨をⅡ．２．（５）④アに定める書面における記載を通じて本人に認識させるとともに、Ⅱ．２．（４）２）①に定める「個人情報保護に関する考え方や方針に関する宣言」に記載の上公表することとする。ただし、本人から情報提供の求めがあった場合であっても、例えば、情報提供することにより与信事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合等は、同項各号に定める情報の全部又は一部について情報提供しないことができる。情報提供しない場合であっても、与信事業者は、本人に対し、遅滞なくその旨を通知するとともに、その理由を説明することとする（情報提供により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おそれがある場合の具体例については、外国第三者提供ガイドライン 6-2-2（提供すべき情報）参照）。

ウ　与信事業者は、個人データの取扱いについて法第４章第２節の規定により個人情報取扱事業者が講ずべき措置に相当する措置（以下「相当措置」という。）を継続的に講ずるために必要なものとして施行規則第 16 条に定める基準に適合する体制を整備していることを根拠として外国にある第三者に個人データを提供した場合に、施行規則第 18 条第１項第１号の規定により当該第三者による相当措置の実施状況を確認する際には、個人データを取り扱う場所に赴く方法又は書面により報告を受ける方法により確認を行うこととする。当該方法は、外国にある第三者に提供する個人データの規模及び性質並びに個人データの取扱状況等に起因するリスクに応じたものとする。また、与信事業者は、法第 28 条第３項及び施行規則第 18 条に基づき、本人の求めに応じて事後的に情報を提供する旨Ⅱ．２．（４）２）①に定める「個人情報保護に関する考え方や方針に関する宣言」に記載の上公表することとする。

エ　与信事業者は、Ⅱ．２．（５）④イ又はⅡ．２．（５）④ウに定めるところにより、外国にある第三者に個人データを提供した場合には、提供先の第三者が所在する外国（Ⅱ．２．（５）④イの場合においては、事後的に提供先の第三者が所在する外国が特定できた場合の当該外国）の名称をインターネットのホームページに掲載を行うこと等により、公表し定期的に更新することが望ましい。

⑹　個人関連情報の第三者提供の制限等（法第 31 条関係）

以下の事項の他は通則ガイドラインの例による。

与信事業者は、個人関連情報取扱事業者から法第 31 条第１項の規定による個人関連情報の提供を受けて個人データとして取得するにあたり、法第 31 条第１項第１号の本人の同意を得る（提供元の個人関連情報取扱事業者に同意取得を代行させる場合を含む。）際には、原則として、書面によることとし、当該書面における記載を通じて、対象となる個人関連情報の項目及び個人関連情報を個人データとして取得した後の利用目的を本人に認識させた上で同意を得ることとする。

なお、与信事業者は、個人関連情報の提供を受けて個人データとして取得した場合には、法第 21 条に従い、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、又は公表しなければならないとされていることに留意する。

個人関連情報取扱事業者のうち割賦販売等を業として行う者は、法第 31 条第２項において読み替えて準用する法第 28 条第３項に従い、外国にある第三者による相当措置の実施状況を定期的に確認する際には、個人データの内容や規模等に応じて個人データを取り扱う場所に赴く方法又は書面により報告を受ける方法によることとする。

⑺　保有個人データの開示（法第 33 条関係）

与信事業者は、保有個人データを開示するに当たっては、その具体的な開示方法に応じて、漏えい等の防止の観点も踏まえて、適切な措置を講ずることとする。例えば，電磁的記録の提供による方法によって保有個人データを開示する場合には、当該電磁的記録にパスワードを付す等の措置を講ずることとする。

⑻　開示等の請求等に応じる手続（法第 37 条関係）

以下の事項の他は通則ガイドラインの例による。

与信事業者は、開示等の請求等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こととする。

なお、施行令第 13 条第２号の代理人による開示等の請求等に対して、与信事業者が本人にのみ直接開示等することは妨げられない。

Ⅲ．ガイドラインの見直し

個人情報の保護についての考え方は、社会情勢の変化、国民の認識の変化、技術の進歩、国際動向等に応じて変わり得るものであり、本ガイドラインは、法の施行後の状況等諸環境の変化を踏まえて、必要に応じ見直しを行うものとする。