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た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

※　なお、個人データの漏えい等の事故が発生した場合のみならず、発生するおそれがある場合についても報告連絡体制を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）
- 経済産業省及び認定個人情報保護団体への報告連絡体制

⑥　与信事業者は、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。）の漏えい等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等に関する事項を可能な限り速やかに経済産業省及び認定個人情報保護団体に報告すること。さらに所属する業界団体等の関係機関に報告することが望ましい。

⑦　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

⑧　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。

⑨　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