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。

3) 従業者の監督（法第21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20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。

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、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