を被る恐れがある場合

ii．法第１８条第４項第２号関連

法第１８条第４項第２号 前三項の規定は、次に掲げる場合については、適用しない。 二　利用目的を本人に通知し、又は公表することにより当該個人情報取扱事業者の権利又は正当な利益を害するおそれがある場合

利用目的を本人に通知し、又は公表することにより企業秘密に関すること等が他社に明らかになり、当該個人情報取扱事業者の権利又は利益が侵害されるおそれがある場合は、その適用を受けない。

事例）通知又は公表される利用目的の内容により、当該個人情報取扱事業者が行う新商品等の開発内容、営業ノウハウ等の企業秘密に関わるようなものが明らかになる場合

iii．法第１８条第４項第３号関連

法第１８条第４項第３号 前三項の規定は、次に掲げる場合については、適用しない。 三　国の機関又は地方公共団体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、利用目的を本人に通知し、又は公表す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。

国の機関等が公的な事務を実施する上で、民間企業等の協力を得る必要がある場合であり、協力する民間企業等が国の機関等から受け取った個人情報の利用目的を本人に通知し、又は公表することにより、当該事務の遂行に支障を及ぼすおそれがある場合は、その適用を受けない。

事例）公開手配を行わないで、被疑者に関する個人情報を、警察から被疑者の立ち回りが予想される個人情報取扱事業者に限って提供する場合、警察から受け取った当該個人情報取扱事業者が、本人の目的外利用の同意を得ることにより、捜査活動に重大な支障を及ぼすおそれがある場合

iv．法第１８条第４項第４号関連

法第１８条第４項第４号

前三項の規定は、次に掲げる場合については、適用しない。
四　取得の状況からみて利用目的が明らかであると認められる場合

個人情報が取得される状況から見て利用目的が自明であると認められる場合は、その適用を受けない。

事例１）　商品・サービス等を販売・提供する場合、住所・電話番号等の個人情報を取得する場合があるが、その利用目的が当該商品の販売、サービスの提供のみを確実に行うためという自明の利用目的である場合

事例２）　一般の慣行として名刺を交換する場合、書面により、直接本人から、氏名・所属・肩書・連絡先等の個人情報を取得することとなるが、その利用目的が今後の連絡のためという自明の利用目的であるような場合（ただし、ダイレクトメール等の目的に名刺を用いる場合を除く）

(3) 個人データの管理（法第１９条～２２条関連）

1)　データ内容の正確性の確保（法第１９条）

法第１９条
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よう努めなければならない。

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、個人情報データベース等への個人情報の入力時の照合・確認の手続の整備、誤り等を発見した場合の訂正等の手続の整備、記録事項の更新、保存期間の設定等を行うことにより、個人データを正確かつ最新の内容に保つよう努めなければならない（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。）。

この場合、保有する個人データを一律に又は常に最新化する必要はなく、それぞれの利用目的に応じて、その必要な範囲内で正確性・最新性を確保すれば足りる。

2)　安全管理措置（法第２０条）

法第２０条
個人情報取扱事業者は、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に必要かつ適切な措置を講じなければならない。

個人情報取扱事業者は、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、及び技術的安全管理措

置を講じなければならない。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い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が望ましい。

【必要かつ適切な安全管理措置を講じているとはいえない場合】

事例１）　公開されることを前提としていない個人データが事業者のホームページ上不特定多数に公開されている状態を個人情報取扱事業者が放置している場合

事例２）　組織変更が行われ、個人データにアクセスする必要がなくなった従事者が個人データにアクセスできる状態を個人情報取扱事業者が放置していた場合で、その従事者が個人データを漏えいした場合

事例３）　本人が継続的にサービスを受けるために登録していた個人データが、個人情報取扱事業者による不適切な取り扱いにより滅失又はき損し、本人がサービスの提供を受けられなくなった場合

事例４）　個人データに対してアクセス制御が実施されておらず、アクセスを許可されていない従業者がそこから個人データを入手して漏えいした場合

事例５）　個人データをバックアップした媒体が、持ち出しを許可されていない者により持ち出し可能な状態になっており、その媒体が持ち出されてしまった場合

組織的安全管理措置

組織的安全管理措置とは、安全管理について従業者（法第２１条参照）の責任と権限を明確に定め、安全管理に対する規程や手順書（以下「規程等」という）を整備運用し、その実施状況を確認することをいう。組織的安全管理措置には以下の事項が含まれる。

①個人データの安全管理措置を講じるための組織体制の整備
②個人データの安全管理措置を定める規程等の整備と規程等に従った運用
③個人データ取扱台帳の整備
④個人データの安全管理措置の評価、見直し及び改善
⑤事故又は違反への対処

【組織的安全管理措置として講じることが望まれる事項】

①個人データの安全管理措置を講じるための組織体制の整備をする上で望まれる事項

- 従業者の役割・責任の明確化

※個人データの安全管理に関する従業者の役割・責任を職務分掌規程、職務権限規程等の内部規程、契約書、職務記述書等に具体的に定めることが望まし

い。

- 個人情報保護管理者（いわゆる、チーフ・プライバシー・オフィサー（ＣＰＯ））の設置
- 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
- 個人データの取扱いに係わるそれぞれの部署の役割と責任の明確化
- 監査責任者の設置
- 監査実施体制の整備
- 個人データの取扱いに関する規程等に違反している事実又は兆候があることに気づいた場合の、代表者等への報告連絡体制の整備
- 個人データの漏えい等の事故が発生した場合、又は発生の可能性が高いと判断した場合の、代表者等への報告連絡体制の整備

  ※個人データの漏えい等についての情報は代表窓口、苦情処理窓口を通じ、外部からもたらされる場合もあるため、苦情の処理体制等との連携を図ることが望ましい。（法第３１条を参照のこと）
- 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の整備
- 漏えい等の事故発生時における主務大臣及び認定個人情報保護団体等に対する報告体制の整備

②個人データの安全管理措置を定める規程等の整備と規程等に従った運用をする上で望まれる事項

- 個人データの取扱いに関する規程等の整備とそれらに従った運用
- 個人データを取り扱う情報システムの安全管理措置に関する規程等の整備とそれらに従った運用

  ※なお、これらについてのより詳細な記載事項については、下記の【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】を参照のこと。
- 個人データの取扱いに係る建物、部屋、保管庫等の安全管理に関する規程等の整備とそれらに従った運用
- 個人データの取扱いを委託する場合における受託者の選定基準、委託契約書のひな型等の整備とそれらに従った運用
- 定められた規程等に従って業務手続が適切に行われたことを示す監査証跡※の保持

  ※保持しておくことが望ましい監査証跡としては、個人データに関する情報システム利用申請書、ある従業者に特別な権限を付与するための権限付与申請書、情報システム上の利用者とその権限の一覧表、建物等への入退館（室）記録、個人データへのアクセスの記録（例えば、誰がどのような操作を行っ

たかを記録)、教育受講者一覧表等が考えられる。

③個人データ取扱台帳の整備をする上で望まれる事項

- 個人データについて、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
- 個人データ取扱台帳の内容の定期的な確認による最新状態の維持

④個人データの安全管理措置の評価、見直し及び改善をする上で望まれる事項

- 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

⑤事故又は違反への対処をする上で望まれる事項

- 事実関係、再発防止策等の公表
- その他、以下の項目等の実施
  ア）事実調査、イ）影響範囲の特定、ウ）影響を受ける可能性のある本人及び主務大臣等への報告、エ）原因の究明、オ）再発防止策の検討・実施

【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】

以下、（ⅰ）取得・入力、（ⅱ）移送・送信、（ⅲ）利用・加工、（ⅳ）保管・バックアップ、（ⅴ）消去・廃棄という、個人データの取り扱いの流れに従い、そのそれぞれにつき規程等に記載することが望まれる事項を列記する。

（ⅰ）取得・入力

ⅰ）作業責任者の明確化

- 個人データを取得する際の作業責任者の明確化
- 取得した個人データを情報システムに入力する際の作業責任者の明確化
  （以下、併せて「取得・入力」という。）

ⅱ）手続の明確化と手続に従った実施

- 取得・入力する際の手続の明確化
- 定められた手続による取得・入力の実施
- 権限を与えられていない者が立ち入れない建物、部屋（以下「建物等」という）での入力作業の実施
- 個人データを入力できる端末の、業務の必要性に基づく限定
- 個人データを入力できる端末に付与する機能の、業務の必要性に基づく限定
  （例えば、個人データを閲覧だけできる端末では、CD-R、USB メモリ等の外部記録媒体を接続できないようにする）

iii) 作業担当者の識別、認証、権限付与

- 個人データを取得・入力できる作業担当者の、業務上の必要性に基づく限定
- ID とパスワードによる認証、生体認証等による作業担当者の識別
- 作業担当者に付与する権限の限定
- 個人データの取得・入力業務を行う作業担当者に付与した権限の記録

iv) 作業担当者及びその権限の確認

- 手続の明確化と手続に従った実施、及び作業担当者の識別、認証、権限付与の実施状況の確認
- アクセスの記録、保管と、権限外作業の有無の確認

（ii）移送・送信

i）作業責任者の明確化

- 個人データを移送・送信する際の作業責任者の明確化

ii）手続の明確化と手続に従った実施

- 個人データを移送・送信する際の手続の明確化
- 定められた手続による移送・送信の実施
- 個人データを移送・送信する場合の個人データの暗号化（例えば、公衆回線を利用して個人データを送信する場合）移送時における宛先確認と受領確認（例えば、配達記録郵便等の利用）
- ＦＡＸ、テレックス等における宛先番号確認と受領確認
- 個人データを記した文書をＦＡＸ、テレックス等に放置することの禁止
- 暗号鍵やパスワードの適切な管理

iii) 作業担当者の識別、認証、権限付与

- 個人データを移送・送信できる作業担当者の、業務上の必要性に基づく限定
- ID とパスワードによる認証、生体認証等による作業担当者の識別
- 作業担当者に付与する権限の限定（例えば、個人データを、コンピュータネットワークを介して送信する場合、送信する者は個人データの内容を閲覧、変更する権限は必要ない）
- 個人データの移送・送信業務を行う作業担当者に付与した権限の記録

iv) 作業担当者及びその権限の確認

- 手続の明確化と手続に従った実施、及び作業担当者の識別、認証、権限付与の実施状況の確認
- アクセスの記録、保管と、権限外作業の有無の確認

（iii）利用・加工

i）作業責任者の明確化

- 個人データを利用・加工する際の作業責任者の明確化

ii）手続の明確化と手続に従った実施

- 個人データを利用・加工する際の手続の明確化
- 定められた手続による利用・加工の実施
- 権限を与えられていない者が立ち入れない建物等での利用・加工の実施
- 個人データを利用・加工できる端末の、業務の必要性に基づく限定
- 個人データを利用・加工できる端末に付与する機能の、業務の必要性に基づく、限定（例えば、個人データを閲覧だけできる端末では、CD-R、USB メモリ等の外部記録媒体を接続できないようにする）

iii）作業担当者の識別、認証、権限付与

- 個人データを利用・加工する作業担当者の、業務上の必要性に基づく限定
- ID とパスワードによる認証、生体認証等による作業担当者の識別
- 作業担当者に付与する権限の限定（例えば、個人データを閲覧することのみが業務上必要とされる作業担当者に対し、個人データの複写、複製を行う権限は必要ない）
- 個人データの利用・加工する作業担当者に付与した権限（例えば、複写、複製、印刷、削除、変更等）の記録

iv）作業担当者及びその権限の確認

- 手続の明確化と手続に従った実施、及び作業担当者の識別、認証、権限付与の実施状況の確認
- アクセスの記録、保管と権限外作業の有無の確認

（iv）保管・バックアップ

i）作業責任者の明確化

- 個人データを保管・バックアップする際の作業責任者の明確化

ii）手続の明確化と手続に従った実施

- 個人データを保管・バックアップする際の手続※の明確化

  ※　情報システムで個人データを処理している場合は、個人データのみならず、オペレーティングシステム（ＯＳ）やアプリケーションのバックアップも必要となる場合がある
- 定められた手続による保管・バックアップの実施
- 個人データを保管・バックアップする場合の個人データの暗号化
- 暗号鍵やパスワードの適切な管理
- 個人データを記録している媒体を保管する場合の施錠管理
- 個人データを記録している媒体を保管する部屋、保管庫等の鍵の管理
- 個人データのバックアップから迅速にデータが復元できることのテストの実施
- 個人データのバックアップに関する各種事象や障害の記録

iii) 作業担当者の識別、認証、権限付与

- 個人データを保管・バックアップする作業担当者の、業務上の必要性に基づく限定
- ID とパスワードによる認証、生体認証等による作業担当者の識別
- 作業担当者に付与する権限の限定（例えば、個人データをバックアップする場合、その作業担当者は個人データの内容を閲覧、変更する権限は必要ない）
- 個人データの保管・バックアップ業務を行う作業担当者に付与した権限（例えば、バックアップの実行、保管庫の鍵の管理等）の記録

iv) 作業担当者及びその権限の確認

- 手続の明確化と手続に従った実施、及び作業担当者の識別、認証、権限付与の実施状況の確認
- アクセスの記録、保管と権限外作業の有無の確認

（v）消去・廃棄

i）作業責任者の明確化

- 個人データを消去する際の作業責任者の明確化
- 個人データを保管している機器、記録している媒体を廃棄する際の作業責任者の明確化

ii）手続の明確化と手続に従った実施

- 消去・廃棄する際の手続の明確化
- 定められた手続による消去・廃棄の実施
- 権限を与えられていない者が立ち入れない建物等での消去・廃棄作業の実施
- 個人データを消去できる端末の、業務の必要性に基づく限定
- 個人データが記録された媒体や機器をリース会社に返却する前の、データの完全消去（例えば、意味のないデータを媒体に１回又は複数回上書きする）
- 個人データが記録された媒体の物理的な破壊（例えば、シュレッダー、メディアシュレッダー等で破壊する）

iii) 作業担当者の識別、認証、権限付与

- 個人データを消去・廃棄できる作業担当者の、業務上の必要性に基づく限定
- ID とパスワードによる認証、生体認証等による作業担当者の識別
- 作業担当者に付与する権限の限定
- 個人データの消去・廃棄を行う作業担当者に付与した権限の記録

iv) 作業担当者及びその権限の確認

- 手続の明確化と手続に従った実施、及び作業担当者の識別、認証、権限付与の実施状況の確認
- アクセスの記録、保管、権限外作業の有無の確認