法務研究科・講義用レジュメ　　2005年7月6日

法 情 報 学（第１２回）

弁護士　川　添　　圭
kawazoe@kondolaw.jp

Ⅰ　個人情報取扱事業者の義務（１）－「個人情報」の取扱いに関する義務（続き）

１　個人情報の適正な取得（法17）

（１）立法趣旨

個人情報取扱事業者が個人情報を取得・蓄積する行為自体は問題がないとする前提で，「偽りその他不正な手段による取得」を規制対象とした。

（２）「偽りその他不正な手段」

→詐欺・脅迫等，違法性を有する手段に限定する必要はないが，本人の権利利益の保護という立法趣旨を没却するような態様での取得が許されないことを意味する。

【具体例】（経産省ガイドラインⅡ2.(2)①）

①親の同意がなく，十分な判断能力を有していない子供から家族の個人情報を取得する場合

②第三者提供制限違反(法23)をするよう強要して個人情報を取得した場合

③他の事業者に指示して不正な手段で個人情報を取得させ，その事業者から個人情報を取得する場合

２　個人情報を取得した場合の取扱い（法18）

（１）総論 － 個人情報取得の態様に応じた法規制

①直接取得＝本人が情報を発信し，これを直接取得する場合（契約書等）

②間接取得＝本人の情報発信によらずに取得する場合（公開情報，事業承継等）

（２）<u>個人情報の取得場面① － 書面による直接取得以外の取得（法18Ⅰ）</u>

→(a)あらかじめ利用目的を公表するか，(b)速やかに本人に通知または公表

〔類型〕ⅰ）本人から書面によらない方法で直接取得する場合

→電話による問合せやクレームのように本人により自発的に提供される個人情報を取得する場合

ⅱ）第三者を通じて間接的に取得する場合

→個人情報の第三者提供を受ける場合

ⅲ）公開情報等から取得する場合

→インターネット，官報，職員録等から個人情報を取得する場合

（３）個人情報の取得場面② － 書面による直接取得の場合（法18Ⅱ）

① 原則 ＝ 当該書面上に利用目的をあらかじめ明示

【具体例】（経産省ガイドラインⅡ2.(2)③）

(a)申込書・契約書に記載された個人情報を本人から直接取得する場合

(b)アンケートに記載された個人情報を直接本人から取得する場合

(c)懸賞の応募葉書に記載された個人情報を直接本人から取得する場合

② 例外 ＝人の生命，身体又は財産の保護のために緊急に必要がある場合

（４）利用目的の変更（法18Ⅲ）

→「変更前の利用目的と相当の関連性を有すると合理的に認められる範囲」（法16Ⅱ）を超えて利用目的を変更した場合は，「変更された利用目的について，本人に通知し，又は公表しなければならない。」

（５）通知・公表が必要ない場合（法18Ⅳ，経産省ガイドラインⅡ2.(2)⑤ⅰ～ⅲ）

①利用目的を本人に通知し、又は公表することにより本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合（法18Ⅳ①）

例）総会屋等による不当要求等防止のため，当該個人に関する情報を取得し，相互に情報交換を行っている場合で，利用目的を通知又は公表することにより，当該総会屋等の逆恨みにより，第三者たる情報提供者が被害を被る恐れがある場合

②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（法18Ⅳ②）

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

③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（法18Ⅳ③）

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，利用目的を本人に通知し，又は公表することにより，捜査活動に重大な支障を及ぼすおそれがある場合

④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（法18Ⅳ④）

ア）商品・サービス等を販売・提供する目的に際し住所・電話番号等の個人情報を取得する場合→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は，明示の必要はない。

イ）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であれば自明となる。

Ⅱ　個人情報取扱事業者の義務（２）－「個人データ」の取扱いに関する義務

１　正確性の確保（法19）

「正確かつ最新の内容に保つ」

＝個人情報データベース等への入力時の照合・確認，誤り発見時の訂正等の手続を整備して継続的に実施すること

※正確性確保の程度と頻度＝「利用目的の達成に必要な範囲内において」

→当該個人データの種類や性質に応じて決定される

例）金融機関の債務者の返済情報：即時の反映かつ金額の正確性が要求される

出版物の場合：次版（または次刷）の際に反映されれば足りる

２　安全措置義務

（１）総論 － 安全措置義務の内容

① 安全措置義務の類型

類型	具体例	条文
第三者による脅威	・不正アクセス ・ウイルス，ワーム被害	安全管理措置義務（法20）
従業者による脅威	・アクセス権限の濫用 ・不正持ち出し ・誤送信，盗難等	従業者の監督義務（法21）
委託先による脅威	・委託先の不正アクセス等 ・委託先従業員の持ち出し等 ・再委託先の不正行為，過失等	委託先の監督義務（法22）

（堀部政男監修・鈴木正朝著『個人情報保護法とコンプライアンス・プログラム』P.179～180）

② 個人情報保護法の安全措置義務とISO（JIS）規格との関係

・ISO（ISO/IEC 17799，JIS X5070，JIS Q15001）

＝ベストプラクティスとしてのスタンダード（世界標準）

（企業としての信用を得るための模範となり得べき基準を提示）

・個人情報保護法上の安全措置義務

＝ミニマムスタンダード（最低限の管理義務）

（主務官庁による措置や刑罰に該当するような杜撰な管理を防止する）

（２）安全措置義務（法20，経産省ガイドラインⅡ2.(3).2)）

①「個人データの安全管理のために必要かつ適切な措置」

＝組織的，人的，物理的及び技術的な安全管理措置を要求

② 組織的安全管理措置

＝(a)安全管理について従業者の責任と権限を明確に定め，(b)安全管理に対する規程や手順書を整備運用し，(c)その実施状況を確認すること

【組織的安全管理措置として講じることが望まれる事項】

ⅰ）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	・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(CPO：チーフ・プライバシー・オフィサー)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 →苦情処理体制（法31参照）との連携を図ることが望ましい。 ・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
ⅱ）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	・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 →規定等に記載すべき内容については【資料】を参照 ・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 ・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，教育受講者一覧表等が考えられる。
ⅲ）個人データ取扱台帳の整備	・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
ⅳ）個人データの安全管理措置の評価，見直し及び改善	・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
ⅴ）事故又は違反への対処	・事実関係，再発防止策等の公表 ・その他，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

③ 人的安全管理措置

＝従業者に対する業務上秘密と指定された個人データの非開示契約の締結や教育・訓練等を行うこと

【人的安全管理措置として講じることが望まれる事項】

ｉ）雇用及び契約時における非開示契約の締結	・従業者の採用時又は委託契約時における非開示契約の締結 →契約終了後も一定期間有効であるようにすることが望ましい。 ・非開示契約に違反した場合の措置に関する規程の整備 →従業者ではないが，個人データにアクセスする可能性がある者（情報システムの開発・保守関係者，清掃担当者，警備員等）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が望ましい。
ⅱ）従業者に対する周知・教育・訓練の実施	・個人データ及び情報システムの安全管理に関する従業者の役割及び責任を定めた内部規程等についての周知 ・個人データ及び情報システムの安全管理に関する従業者の役割及び責任についての教育・訓練の実施 ・従業者に対する教育・訓練が必要かつ適切に実施されていることの確認

④ 物理的安全管理措置

＝入退館（室）の管理，個人データの盗難の防止等の措置

【物理的安全管理措置として講じることが望まれる事項】

ｉ）入退館（室）管理の実施	・個人データを取り扱う業務の，入退館（室）管理を実施している物理的に保護された室内での実施 ・個人データを取り扱う情報システム等の，入退館（室）管理を実施している物理的に保護された室内等への設置
ⅱ）盗難等に対する対策	・離席時の個人データを記した書類，媒体，携帯可能なコンピュータ等の机上等への放置の禁止 ・離席時のパスワード付きスクリーンセイバ等の起動 ・個人データを含む媒体の施錠保管 ・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 ・操作マニュアルの机上等への放置の禁止
ⅲ）機器・装置等の物理的な保護の上で望まれる事項	・個人データを取り扱う機器・装置等の，安全管理上の脅威（例えば，盗難，破壊，破損）や環境上の脅威（例えば，漏水，火災，停電）からの物理的な保護

⑤ 技術的安全管理措置

＝個人データ及びそれを取り扱う情報システムへのアクセス制御，不正ソフトウェア対策，情報システムの監視等，個人データに対する技術的な安全管理措置

【技術的安全管理措置として講じることが望まれる事項】

ｉ）個人データへのアクセスにおける識別と認証	・個人データに対する正当なアクセスであることを確認するためにアクセス権限を有する従業者本人であることの識別と認証（IDとパスワードによる認証，生体認証等）の実施 →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が望ましい。 ・個人データへのアクセス権限を有する各従業者が使用できる端末又はアドレス等の識別と認証（MACアドレス認証，IPアドレス認証等）の実施
ⅱ）個人データへのアクセス制御	・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（パスワード設定をしたファイルが誰でもアクセスできる状態は，アクセス制御はされているが，識別がされていないことになる。このような場合には，パスワードを知っている者が特定され，かつ，アクセスを許可する者に変更があるたびに，適切にパスワードを変更する必要がある） ・従業者に付与するアクセス権限の最少化 ・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） →情報システムの特権ユーザーであっても，情報システムの管理上個人データの内容を知らなくてもよいのであれば，個人データへ直接アクセスできないようにアクセス制御をすることが望ましい。 ・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）
ⅲ）個人データへのアクセス権限の管理	・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） ・個人データを取り扱う情報システムへの必要最小限のアクセス制御の実施
ⅳ）個人データへのアクセスの記録	・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
ⅴ）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の実施	・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）
ⅵ）個人データの移送（運搬，郵送，宅配便等）・通信時の対策	・移送時における紛失・盗難した際の対策（例えば，媒体に保管されている個人データの暗号化） ・盗聴される可能性のあるネットワーク（例えば，インターネットや無線ＬＡＮ等）で個人データを通信（例えば，本人及び従業者による入力やアクセス，メールに添付してファイルを送信する等を含むデータの転送等）する際の，個人データの暗号化
ⅶ）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	・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
ⅷ）個人データを取り扱う情報システムの監視	・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

（３）従業者の監督（法21，経産省ガイドラインⅡ2.(3).3)）

① 従業者＝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・派遣社員も含まれる。

② 「必要かつ適切な管理」

【従業者に対して必要かつ適切な監督を行っていない場合】

(a)従業者が，個人データの安全管理措置を定める規程等に従って業務を行っていることを，予め定めた間隔で定期的に確認せず，結果，個人データが漏えいした場合

(b)内部規程等に違反して個人データが入ったノート型パソコンを繰り返し持ち出し，それを放置した結果，紛失し，個人データが漏えいした場合

③ 雇用管理に関する個人データの取扱いについて

（雇用管理に関する個人情報の適正な取扱いを確保するために事業者が講ずべき措置に関する指針〔厚労省ガイドライン〕第三・三）

事業者は、雇用管理に関する個人データの安全管理のために次に掲げる措置を講ずるように努めるものとすること。

（一）雇用管理に関する個人データを取り扱う従業者及びその権限を明確にした上で、その業務を行わせること。

（二）雇用管理に関する個人データは、その取扱いについての権限を与えられた者のみが業務の遂行上必要な限りにおいて取り扱うこと。

（三）雇用管理に関する個人データを取り扱う者は、業務上知り得た個人データの内容をみだりに第三者に知らせ、又は不当な目的に使用してはならないこと。その業務に係る職を退いた後も同様とすること。

（四）雇用管理に関する個人データの取扱いの管理に関する事項を行わせるため、当該事項を行うために必要な知識及び経験を有していると認められる者のうちから個人データ管理責任者を選任すること。

（五）雇用管理に関する個人データ管理責任者及び個人データを取り扱う従業者に対し、その責務の重要性を認識させ、具体的な個人データの保護措置に習熟させるため、必要な教育及び研修を行うこと。

（４）委託先の監督（法22）

① 趣旨＝委託先は第三者提供の制限における第三者には該当しない（法23Ⅳ②）が，本の立場からみれば，本人の個人情報が委託先に流通することを直接コントロールできないことに変わりがないことから，個人情報の安全性確保の責任を，委託元である個人事業取扱事業者に負わせることとした。

②必要かつ適切な監督を行っていない場合（経産省ガイドラインⅡ2.(3).4)）

(a)個人データの安全管理措置の状況を契約締結時及びそれ以後も定期的に把握せず外部の事業者に委託した場合で，受託者が個人データを漏えいした場合

(b)個人データの取扱いに関して定めた安全管理措置の内容を受託者に指示せず，結果，受託者が個人データを漏えいした場合

(c)再委託の条件に関する指示を受託者に行わず，かつ受託者の個人データの取扱状況の確認を怠り，受託者が個人データの処理を再委託し，結果，再委託先が個人データを漏えいした場合

③ 委託契約上の留意点

(a) 経産省ガイドラインⅡ2.(3).4)

ⅰ）委託者及び受託者の責任の明確化

ⅱ）個人データの安全管理に関する事項

・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

・委託処理期間

・委託処理終了後の個人データの返還・消去・廃棄に関する事項

ⅲ）再委託に関する事項

・再委託を行うにあたっての委託者への文書による報告

・個人データの取扱状況に関する委託者への報告の内容及び頻度

・契約内容が遵守されていることの確認

・契約内容が遵守されなかった場合の措置

・セキュリティ事件・事故が発生した場合の報告・連絡に関する事項

(b) 厚労省ガイドライン第三・四

（一）個人情報の保護について十分な措置を講じている者を委託先として選定するための基準を設けること。

（二）委託先が委託を受けた個人データの保護のために講ずべき措置の内容が委託契約において明確化されていること。具体的な措置としては，以下の事項が考えられること。

(1)委託先においてｐその従業者に対し当該個人データの取扱いを通じて知り得た個人情報を漏らし,又は盗用してはならないこととされていること。

(2)当該個人データの取扱いの再委託を行うに当たっては，委託元へその旨文書をもって報告すること。

(3)委託契約期間等を明記すること。

(4)利用目的達成後の個人データの返却又は委託先における破棄若しくは削除が適切かつ確実になされること。

(5)委託先における個人データの加工（委託契約の範囲内のものを除く。），改ざん等を禁止し，又は制限すること。

(6)委託先における個人データの複写又は複製（安全管理上必要なバックアップを目的とするもの等委託契約範囲内のものを除く。）を禁止すること。

(7)委託先において個人データの漏えい等の事故が発生した場合における委託元への報告義務を課すこと。

(8)委託先において個人データの漏えい等の事故が発生した場合における委託先の責任が明確化されていること。

3　第三者提供の制限（法23）

（1）総論 －個人データの提供が許される場合

「第三者」への提供	本人の同意を得た第三者提供	法23Ⅰ柱書
	本人の同意を得ない第三者提供	法23Ⅰ①～④
	オプトアウトによる第三者提供	法23Ⅱ，Ⅲ
「第三者」以外の者への提供	委託先への提供	法23Ⅳ①，21
	合併その他事業承継後の事業者への提供	法23Ⅳ②
	共同利用事業者への提供	法23Ⅳ③，Ⅴ
本人への提供		（原則適法）

（2）本人の同意を得た第三者提供（法23Ⅰ柱書，経産省ガイドラインⅡ2.(4)）

【第三者提供とされる事例】

① 親子兄弟会社・グループ会社の間で個人データを交換する場合

② フランチャイズ組織の本部と加盟店の間で個人データを交換する場合

③ 同業者間で特定の個人データを交換する場合

④ 外国の会社に国内に居住している個人の個人データを提供する場合

【第三者提供とされない事例】

⑤ 同一事業者内で他部門へ個人データを提供すること
（ただし，利用目的による制限を受けることに注意。）

（3）本人の同意を得ない第三者提供（適用除外条項）

① 法令に基づく場合（法23Ⅰ①）

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であって，本人の同意を得ることが困難であるとき（法23Ⅰ②）

③ 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって，本人の同意を得ることが困難であるとき（法23Ⅰ③）

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であって，本人の同意を得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（法23Ⅰ④）

→基本的に，法16Ⅲ（利用目的による制限）各号における除外事由と同じ。

（4）オプトアウト（法23Ⅱ，Ⅲ）

オプトアウト＝以下の情報を本人が容易に知りうる状態に置いておくとともに，本人の求めに応じて第三者へ提供することを停止すること。

(a) 第三者への提供を利用目的とすること

(b) 第三者に提供される個人データの項目

(c) 第三者への提供の手段又は方法

(d) 本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること

【オプトアウトが認められている事例】

①住宅地図業者（表札を調べて住宅地図を作成し，販売（不特定多数への第三者提供））

②データベース事業者（ダイレクトメール用の名簿等を作成し，販売）

（５）委託先への提供（法23Ⅳ①）

① 第三者提供と委託との違い

・第三者提供＝提供先が取得した個人データを返還・消去しない

・委託＝取得先が取得した個人データを委託元へ返還するか，消去が予定

② 委託の類型

ア）個人データが委託元から提供される場合

【事例】（経産省ガイドラインⅡ2.(4).③.ｉ）

① データの打ち込み等，情報処理を委託するために個人データを渡す場合

② 百貨店が注文を受けた商品の配送のために宅配業者に個人データを渡す場合

イ）個人データが委託先から提供される場合

→企業のキャンペーン企画を委託された広告企画会社が，委託元の企業名で銘打ったキャンペーンを通じて取得した個人情報をデータ入力し，委託元へ提供する場合

（６）合併等事業承継後の事業者への提供（法23Ⅳ②）

→法16Ⅱを参照

（第１１回レジュメ６ページ，利用目的の制限を受けることに注意）

（７）共同利用事業者への提供（法23Ⅳ③，Ⅴ）

① 要件

以下の情報をあらかじめ本人に通知し，または本人が容易に知りうる状態に置いておくとともに，共同して利用することを明らかにしている場合。

ア）個人データを特定の者との間で共同して利用する旨

イ）共同して利用される個人データの項目

ウ）共同して利用する者の範囲

エ）利用する者の利用目的

オ）当該個人データの管理について責任を有する者の氏名又は名称

【具体例】（経産省ガイドラインⅡ2.(3).③.ⅲ）

ⅰ）グループ企業で総合的なサービスを提供するために利用目的の範囲内で情報を共同利用する場合

ⅱ）親子兄弟会社の間で利用目的の範囲内で個人データを共同利用する場合

ⅲ）外国の会社と利用目的の範囲内で個人データを共同利用する場合

Ⅲ　個人情報取扱事業者の義務（３）－「保有個人データ」の取扱いに関する義務

１　保有個人データの公表等（法24）

（１）趣旨

＝個人情報の取扱いに関する透明性の確保

※法施行前から保有している個人情報ついては，法施行当時の取得行為がないため，利用目的の明示（法18）の手続を履践していない。そのため，法24の措置を講じておく必要がある（経産省ガイドラインⅡ2.(5).1).①）。

（２）公表すべき事項

① 当該個人情報取扱事業者の氏名又は名称（法24Ⅰ①）

② すべての保有個人データの利用目的（法24Ⅰ②）

→法18Ⅳ①～③に該当する場合を除く

③ 開示等の求めの手続（法24Ⅱ，25Ⅰ，26Ⅰ，27Ⅰ）及び保有個人データの利用目的の通知，保有個人データの開示の手続について手数料を定めたときはその額（法24Ⅰ③）

④ 上記のほか，保有個人データの適正な取扱いの確保に関し必要な事項として政令で定めるもの（法24Ⅰ④）

※「政令で定めるもの」（施行令5①②）

① 当該個人情報取扱事業者が行う保有個人データの取扱いに関する苦情の申出先

② 当該個人情報取扱事業者が認定個人情報保護団体の対象事業者である場合にあっては，当該認定個人情報保護団体の名称及び苦情の解決の申出先

（３）利用目的の通知の求め（法24Ⅱ）

〔除外事由〕

① 法24Ⅰの規定により当該本人が識別される保有個人データの利用目的が明らかな場合

② 法18Ⅳ①～③に該当する場合

２　開示の求め

（１）開示の求め（法25Ⅰ）

① 主体：当該保有個人データの「本人」またはその代理人（法29Ⅲ）

② 相手方：当該保有個人データを保有している個人情報取扱事業者

③ 開示の対象となる情報：当該本人が識別される保有個人データ

※対象は「個人情報」ではなく，「個人情報データベース」を構成する「保有個人データ」に限定されるため，個人情報データベースから当該本人が識別されるものを検索・抽出する方法により行われる。

④ 開示の方法：書面の交付(請求者が他の方法で同意したときはその方法)（施行令6）

（２）不開示事由（法25Ⅰただし書き）

① 本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合

【具体例】（経産省ガイドラインⅡ2.(5).2).ⅰ）

・医療機関等において、病名等を開示することにより、本人の心身状況を悪化させるおそれがある場合

② 当該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

【具体例】（経産省ガイドラインⅡ2.(5).2).ⅱ）

・検査機関等において，検査情報を開示することにより本人と検査機関との信頼関係を損ない，業務上著しい支障を及ぼすおそれがある場合

・同一の本人から複雑な対応を要する同一内容について繰り返し開示の求めがあり，事実上問い合わせ窓口が占有されることによって他の問い合わせ対応業務が立ち行かなくなる等、業務上著しい支障を及ぼすおそれがある場合

③ 他の法令に違反することとなる場合

【具体例】（経産省ガイドラインⅡ2.(5).2).ⅲ）

・金融機関が組織犯罪処罰犯罪収益規制法54Ⅰに基づいて，主務大臣に取引の届出を行っていたときに，当該届出を行ったことが記録されている保有個人データを開示することが同条Ⅱ(届出の守秘義務)の規定に違反する場合

（３）不開示の通知（法25Ⅱ）

→本人へ通知

（４）開示の求めに対する企業の対応

＝個人情報の保存義務？との関係

3　訂正等

（１）訂正等の求め（法26Ⅰ）

① 主体：当該保有個人データの「本人」またはその代理人（法29Ⅲ）

② 相手方：当該保有個人データを保有している個人情報取扱事業者

③ 訂正理由：「当該本人が識別される保有個人データの内容が事実でない」こと

④ 対応方法：利用目的の達成に必要な範囲内において、遅滞なく必要な調査を行う

【訂正を行う必要がない事例】（経産省ガイドラインⅡ2.(5).3)）

・訂正等の対象が事実でなく評価に関する情報である場合

（２）訂正等をしない旨の通知（法26Ⅱ）

→本人へ通知

4　利用停止等

（１）利用停止等の求め（法27Ⅰ，Ⅱ）

① 主体：当該保有個人データの「本人」またはその代理人（法29Ⅲ）

② 相手方：当該保有個人データを保有している個人情報取扱事業者

③ 停止理由：

ア）本人の同意を得ない目的外利用（法16）又は不正な取得（法17）を行っている場合（法27Ⅰ）

イ）本人の同意及びオプトアウトを行わず第三者提供を行っている場合（法27Ⅱ）

（2）応じる必要がない場合（法27Ⅰただし書き，27Ⅱただし書き）

＝当該保有個人データの利用停止等に多額の費用を要する場合その他の利用停止等を行うことが困難な場合であって，本人の権利利益を保護するため必要なこれに代わるべき措置をとるとき

5　理由の説明義務（法28）

＝努力義務にとどまる。

6　開示等の求めに応じる手続（法29）

（1）開示・訂正・利用停止の求めを受け付ける方法の定め（法29Ⅰ）

① 趣旨

法は開示等の求めの方式や方法を限定していないため，個人情報取扱事業者による対応が煩雑になることを避けるため，開示の求めに関する書式や窓口の特定，郵送による受け付けを認めるか否かといった具体的手続を定めることができるものとし，反面，当該定めを「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。）」に置いたときは，本人は当該定めに従った方法で開示等の求めをしなければならないものとした。

② 「政令で定めるところにより」（施行令7）

「法第二十九条第一項の規定により個人情報取扱事業者が開示等の求めを受け付ける方法として定めることができる事項は、次に掲げるとおりとする。

一　開示等の求めの申出先

二　開示等の求めに際して提出すべき書面（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。）の様式その他の開示等の求めの方式

三　開示等の求めをする者が本人又は次条に規定する代理人であることの確認の方法

四　法第三十条第一項の手数料の徴収方法」

③ 保有個人データを特定するに足りる事項の提示の求め（法29Ⅱ）

→住所，ID，パスワード，会員番号等

④ 本人の負担に対する配慮義務（法29Ⅳ）

＝努力義務にとどまる。

7　手数料の定め

（1）手数料を徴収できる場合（法30Ⅰ）

① 保有個人データに関する利用目的の通知（法24Ⅰ）

② 本人の求めによる利用目的の開示（法25Ⅰ）

（2）金額の決定（法30Ⅱ）

→「実費を勘案して合理的であると認められる範囲内」

Ⅳ　その他

1　苦情処理体制の整備（法31）

＝努力義務にとどまる。

※参考：JIS Z 9920（苦情対応マネジメント・システムの指針）

2　主務大臣の関与

種　類	内　　容	拘束力	対象となる条文
報告の徴収 (法32)	個人情報取扱事業者に対し報告義務を課すことができる（行政調査）	罰金刑あり (法57)	個人情報取扱事業者の義務全般（法15～36）
助言 (法33)	必要な助言をすることができる（助言的行政指導）	なし	
勧告 (法34Ⅰ)	当該違反行為の中止その他違反を是正するために必要な措置をとるべき旨を勧告することができる（規制的行政指導）	行政手続法2⑥の行政指導に該当	利用目的による制限(法16) 適正な取得(法17) 利用目的の通知等(法18) 安全管理措置(法20) 従業者の監督(法21) 委託先の監督(法22) 第三者提供の制限(法23) 保有個人データの公表(法24) 開示，訂正，利用停止(法25～27) 手数料(法30Ⅱ)
命令 (法34Ⅱ)	勧告に係る措置を採らなかった場合に，その勧告に係る措置をとるべきことを命ずることができる（行政処分）	懲役又は罰金刑あり (法56)	
緊急命令 (法34Ⅲ)	当該違反行為の中止その大半を是正するために必要な措置をとるべきことを命ずることができる（行政処分）		利用目的による制限(法16) 適正な取得(法17) 安全管理措置(法20) 従業者の監督(法21) 委託先の監督(法22) 第三者提供の制限(法23)

【資料】「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」（経産省ガイドラインⅡ2.(3).2)による）

	ⅰ）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	ⅲ）作業担当者の識別，認証，権限付与	ⅳ）作業担当者及びその権限の確認
１．個人データの取得・入力	・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	・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）	・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	・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
２．個人データの移送・送信	・個人データを移送・送信する際の作業責任者の明確化	・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	・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	・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
３．個人データの利用・加工	・個人データを利用・加工する際の作業責任者の明確化	・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）	・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	・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
４．個人データの保管・バックアップ	・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	・個人データを保管・バックアップする際の手続※の明確化 ・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	・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	・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
５．個人データの消去・廃棄	・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	・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）	・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	・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