特定個人情報取扱規程

制定日	2016 年 6 月 1 日
改訂日	2019 年 6 月 1 日

作　成	特定個人情報管理者
承　認	社　長

アドバンスド・ソリューション株式会社

目　次

第１章　本規程の目的

1.1　本規程の目的

本規程は、アドバンスド・ソリューション株式会社（以下、「当社」という。）が、「行政手続における特定の個人を識別するための番号の利用等に関する法律」（平成 25 年法律第 27 号、以下「番号法」という。）、「特定個人情報の適正な取扱いに関するガイドライン（事業者編）」及び「個人情報の保護に関する法律」（平成 15 年法律第 57 号、以下「個人情報保護法」という。）、「個人情報の保護に関する法律についてのガイドライン」に基づき、当社の取り扱う個人番号及び特定個人情報（以下、「特定個人情報等」という。）の適正な取扱いを確保するために定めるものである。特定個人情報等に関しては、当社の他の社内規程又はマニュアルに優先して本規程が適用される。本規程の規定が他の社内規程又はマニュアルの規定と矛盾する場合には本規程の規定が優先的に適用される。

1.2　特定個人情報等の範囲

当社が個人番号を取り扱う事務において使用する個人番号及び個人番号と関連付けて管理する特定個人情報は以下のとおりとする。

(1) 従業者又は従業者以外の個人から、提示を受けた個人番号カード、通知カード、身元確認書類等及びこれらの写し
(2) 当社が税務署等の行政機関等に提出するために作成した法定調書及びその控え
(3) 当社が法定調書を作成するうえで従業者又は従業者以外の個人から受領する個人番号が記載された申告書等
(4) その他個人番号と関連づけて保存される情報

1.3　特定個人情報一覧表の作成

特定個人情報管理者は、当社が扱う特定個人情報等を「特定個人情報一覧表」にて明確にする。作成した「特定個人情報一覧表」は、社長の承認を得る。「特定個人情報一覧表」は常に最新の状態を維持する。

1.4　用語の定義

本規程で用いる用語について、「特定個人情報の適正な取扱いガイドライン（事業者編） 第 2　用語の定義等」及び「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン 2-1 定義」に準じる。ただし、当社において固有の意味で用いる用語については、以下に定義する。

① 従業者
当社内において、直接間接に当社の指揮監督を受けて当社の業務に従事している者。具体的には従業員のほか、取締役、監査役、理事、監事、派遣社員等を含む。

② 事務取扱担当者
当社内において、個人番号を取り扱う事務に従事する者をいう。

③ 特定個人情報管理者
当社内において、特定個人情報等の管理に関する責任を担う者をいう。

第２章　個人情報及び特定個人情報等保護方針

社長は、個人情報及び特定個人情報等保護方針を定め、「個人情報保護規程」に文書化する。

第3章 特定個人情報等の取り扱い

3.1　個人番号の利用制限

3.1.1　　個人番号の原則的な取り扱い

当社は、個人番号を社会保障、税及び災害対策に関する特定の事務のために限定して利用する。
社員管理のために個人番号を社員番号として利用しない。個人番号には死者のものも含まれる。

3.1.2　　利用目的を超えた個人番号の利用禁止

当社は、本人の同意があったとしても、利用目的を超えて個人番号を利用しない。
やむをえず、利用目的を超えて個人番号を利用する場合、当初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内でのみ利用目的を変更し、本人への通知等を行う。

3.1.3　　合併等で個人番号を取得

当社は、合併等で個人番号を取得した場合、承継前に特定されていた利用目的に従って利用する。
たとえ本人の同意があったとしても、承継前に特定されていた利用目的を超えて利用してはならない。

3.1.4　　適用除外

当社は、次にあげる場合は例外的に利用目的を超えた個人番号の利用を行う。

(1) 金融機関が激甚災害時等に金銭の支払いを行う場合
(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であって、本人の同意があり、又は本人の同意を得ることが困難である場合

3.2　特定個人情報ファイルの作成の制限

当社は、必要な範囲を超えた特定個人情報ファイルの作成を禁止する。
また、従業員等の個人番号を利用して営業成績等を管理する等のファイルを作成しない。

3.3　個人番号の提供

3.3.1　　個人番号の提供の求め

事務取扱担当者は、個人番号関係事務の発生が予想できた場合のみ、個人番号の提供を求めることができる。社会保障、税及び災害対策の場合を除き、他人の個人番号を求めてはならない。

3.3.2　提供を受けられない場合

事務取扱担当者は、個人番号の提供を受けられない場合、定められた義務であることを本人に伝え提供を求める。個人番号の提供を受けられなかった場合、提供を求めた過程等を「個人番号提供依頼過程記録」に記録し保存する。

3.3.3　特定個人情報の提供制限

当社は、本人に交付する税務関係書類（源泉徴収票・支払通知書等）には、個人番号を含む情報として開示の求めがあった場合を除き、個人番号を記載しない。

また、別法人への出向、転籍、異動等により特定個人情報が移動する場合、改めて本人から提供を受けなければならない。

3.3.4　特定個人情報を提供できる場合

(1) 個人情報保護委員会が特定個人情報の提供を求めた場合提供しなければならない。

(2) 各議院審査等その他公益上の必要がある時は特定個人情報を提供できる。

(3) 人の生命、身体又は財産の保護のために必要である場合特定個人情報を提供できる。

3.4　特定個人情報の収集・保管

当社は、社会保障・税及び災害対策に該当する場合を除き、個人番号を含む特定個人情報を収集又は保管しない。

3.4.1　収集制限

事務取扱担当者（個人番号関係事務者）は、その関係事務以外の目的で他者の特定個人情報をノート等に書き写してはならない。

個人番号が記載された書類等を受取り、関係事務者に受渡し等を行う者は、できる限り速やかに受渡すこととし、従業者は自分の手元に個人番号を残さない。

3.4.2　保管制限と廃棄

必要なくなった個人番号は、所管法令で定められた保存期間を経過したのち、できるだけ速やかに（毎年度末）廃棄又は削除する。

提供を受けた特定個人情報を電磁的記録として保存している場合、その事務に必要がなく所管法令で定められている保存期限を経過した場合は、できるだけ速やかに（毎年度末）削除する。

特定個人情報を保存するシステムは、保存期限経過後における廃棄又は削除を前提としてシステムを構築する。

3.5　本人確認

3.5.1　個人番号の提供を受ける際の本人確認

個人番号の提供を受ける際は、次にあげる方法のいずれかで本人確認を行う。

(1)　個人番号カードの提示

(2)　通知カードと本人の身元確認書類（運転免許証やパスポートなど顔写真入り）の提示

(3)　番号確認書類（マイナンバー入りの住民票や戸籍謄本等）と本人の身元確認書類（運転免許証やパスポートなど顔写真入り）の提示

3.5.2　代理人から個人番号の提供を受ける場合

代理人から個人番号の提供を受ける場合、代理権確認書類(戸籍謄本・委任状等)、代理人の身元確認書類（個人番号カード・運転免許証等)、本人の番号確認書類（本人に関わる個人番号カード等）の提示を受ける。

3.5.3　書面の送付により個人番号の提供を受ける場合

書面の送付により個人番号の提供を受ける場合は、上記(3.5.1～3.5.2)で提示を受けることとされている書類又はその写しの提出を受ける。

3.6　第三者提供の停止

当社は、特定個人情報の第三者への提供の停止の求めがあった場合、違法に提供されている理由により、本人から停止を求められた場合であって、その求めに理由があることが判明した時には、遅滞なく停止しなければならない。

第 4 章　安全管理措置

当社は個人番号及び特定個人情報に対し、必要かつ適切な安全管理措置を以下の通り講じる。特定個人情報等の安全管理措置が適切に講じられるよう従業者に必要かつ適切な監督を行う。

4.1 特定個人情報等の取扱方法

特定個人情報等の取扱は、第 5 章～第 8 章の組織的・人的・物理的・技術的安全管理措置に従った上で次の取扱方法を行う。

(1) 取得する段階での取扱方法

① 特定個人情報等を取得する際は本人確認を行う。
② 入力作業は取扱区域にて行う。
③ 入力作業は「機器管理台帳」で管理されている端末で行う。
④ 入力原票と突合するなど誤入力がないか確認する。

(2) 利用する段階での取扱方法

① 利用する際の作業は取扱区域にて行う。
② 利用する際の作業は「機器管理台帳」で管理されている端末で行う。

(3) 保存する段階での取扱方法

① 所管法令で定められた個人番号を記載する書類等の保存期間を経過するまでの間は、特定個人情報を適正に保存する。
② 保存作業は管理区域にて行う。
③ 保存作業は「機器管理台帳」で管理されている端末で行う。
④ バックアップは以下の要領により行う。
・バックアップ媒体：外付け HDD
・バックアップ頻度：週 1 回

バックアップデータを次のとおり管理する。
・暗号化、パスワード認証などにより機密性を確保する。
・バックアップ媒体に異常のないことを月 1 回確認する。
・バックアップ媒体は、施錠された場所に保管する。

(4) 提供する段階での取扱方法

① 行政機関等への法廷調書の提出等、定められた業務範囲にて提供する。
② データ送信で提供する場合、提供作業は取扱区域で行う。
③ データ送信で提供する場合、提供作業は「機器管理台帳」で管理されている端末で行う。

(5) 削除・廃棄する段階での取扱方法

① 必要がなくなり所管法令において定められている保存期間を経過した特定個人情報はできるだけ速やかに復元できない手段で廃棄又は削除する。

② 削除・破棄作業は取扱区域にて行う。

③ 削除・破棄作業は「機器管理台帳」で管理されている端末で行う。

4.2 特定個人情報等の作業責任者の任務

作業責任者（特定個人情報管理者）は事務取扱担当者の監督を行い、本規程で定められた安全管理措置の実施を確認する。

(1) 特定個人情報等の取得、利用、保存、提供、削除・廃棄の承認

(2) 特定個人情報等の取得、利用、保存、提供、削除・廃棄の記録の管理

(3) 特定個人情報等の取得、利用、保存、提供、削除・廃棄の取扱状況の把握

(4) 特定個人情報等の取得、利用、保存、提供、削除・廃棄の監督

(5) 管理区域及び取扱区域での取扱状況の監視

4.3 事務取扱担当者の任務

本規程で定められた安全管理措置を順守し取扱業務を行う。

(1) 特定個人情報等の取得、利用、保存、提供、削除・廃棄の取扱業務

(2) 特定個人情報等の取得、利用、保存、提供、削除・廃棄の取扱状況の報告

(3) 管理区域及び取扱区域での作業順守

4.4 作業責任者（特定個人情報管理者）と事務取扱担当者

特定個人情報等の取扱いを行う際は、取得、利用、保存、提供、削除・廃棄の段階ごとに作業責任者と事務取扱担当者を「特定個人情報取扱担当表」に記載し明確にする。

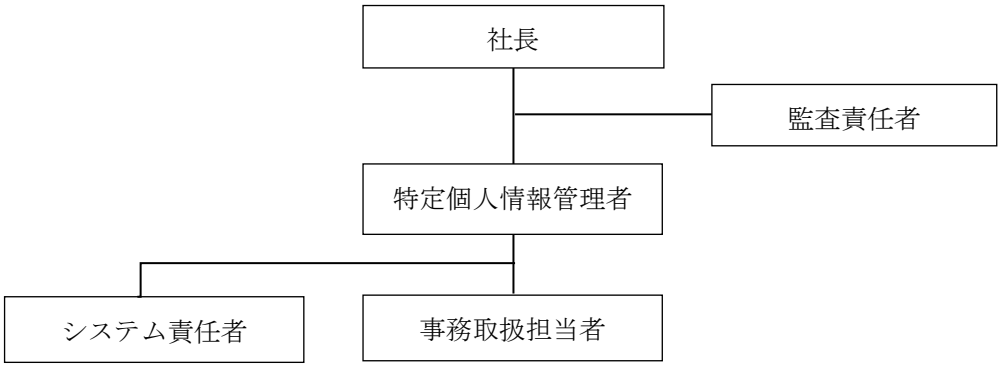
第 5 章　組織的安全管理措置

当社は以下の通り組織的安全管理措置を講じる。

5.1　体制及び責任

特定個人情報等の保護を効果的に実施するための体制を整備し、それぞれの役割、責任および権限を定める。

【特定個人情報等保護の運営体制図】



役　割	担　当	任命者
特定個人情報管理者	及川　紘旭	社長
監査責任者	平田　貴嗣	社長
システム責任者	及川　紘旭	社長
事務取扱担当者	及川　紘旭	社長

5.1.1　責任と権限

特定個人情報等保護に関する管理者･責任者･担当者の責任と権限は以下のとおりとする。

体制・役割	責任及び権限等
社　長	(1) 特定個人情報等の保護に関するすべての指揮権限を有し、当社の保有する特定個人情報等の保護に関する最終的な責任を負う。 (2) 個人情報及び特定個人情報等保護方針を制定し、実行し維持する。 (3) 特定個人情報等の保護の運用に必要となる資源を用意する。 (4) 社内から特定個人情報管理者を任命し、特定個人情報等の保護の運用に関する責任及び権限を与え、業務を遂行させる。 (5) 監査責任者を任命し、特定個人情報等の取扱いの内部監査を行わせる。 (6) 従業者が法令及び特定個人情報等の保護に関する内部規程に違反した場合、就業規則等に則って、懲戒、法的処置等を行う。 (7) 特定個人情報等の保護の運用の見直しを定期的に行い、必要な場合改善の指

	示を出す。
特定個人情報管理者	(1) 特定個人情報等の保護の運用について統括する。 (2) 事務取扱担当者に特定個人情報等の保護に関する教育を実施及び指導する。 (3) 特定個人情報等の保護の運用に際し、関連する法令及びその他の規範を遵守し運用・実施について統括する。 (4) その他、社長の指示による対処、指示を行う。
監査責任者	特定個人情報等の保護の運用状況に係わる内部監査を実施し、その結果を社長に報告する。
システム責任者	社内情報システムを管理するとともに､情報システムの適正な利用が行えるよう、必要な対策を講じ、指示する。
事務取扱担当者	特定個人情報管理者の監督のもと規程を遵守し特定個人情報の取り扱いを行う。

5.1.2　報告連絡体制

特定個人情報管理者は事務取扱担当者が取扱規程等に違反している事実又は兆候を把握した場合その実態を調査し社長に報告する。従業員は情報漏えい等、事案の発生又は兆候を把握した場合特定個人情報管理者に報告する。

5.1.3　任務分担及び責任

特定個人情報を複数の部署で取り扱う場合、各部署の任務分担及び責任を「特定個人情報一覧表」で明確にする。

5.2　規程等に基づく運用

特定個人情報ファイルのシステムログ又は利用実績に関し以下の項目について「特定個人情報利用実績表」に記録する。特定個人情報ファイルの削除・廃棄を委託した場合はこれを証明する記録を入手し保管する。

①特定個人情報ファイルの利用・出力状況
②書類・媒体等の持ち出し
③特定個人情報ファイルの削除・廃棄
④特定個人情報ファイルを情報システムで取扱う場合、事務取扱担当者の情報システムの利用状況

5.3　取扱状況を確認する手段の整備

特定個人情報ファイルの取扱状況に関し以下の項目について「特定個人情報利用実績表」に記録する。なお、取扱状況を確認するための記録等には、特定個人情報等は記載しない。

①特定個人情報ファイルの種類、名称
②責任者、取扱部署
③利用目的
④削除・廃棄状況
⑤アクセス権を有する者

5.4　情報漏えい等事案に対応する体制の整備

情報漏えい等の事案の発生又は兆候を把握した場合、適切かつ迅速に対応するための体制を整備する。

情報漏えい等の事案が発生した場合、事案に応じて、事実関係及び再発防止策等を早急に公表する。

①特定個人情報管理者は事実関係の調査及び原因の究明を行う

②特定個人情報管理者は影響を受ける可能性のある本人への連絡を行う

③特定個人情報管理者は「個人情報保護に関する緊急連絡網」記載の個人情報保護委員会及び主務大臣への報告を行う

④特定個人情報管理者は再発防止策を検討し社長に報告して決定する

⑤特定個人情報管理者は事実関係及び再発防止策等の公表について社長と協議して実施する

5.5　取扱状況の把握及び安全管理措置の見直し

特定個人情報等の取扱状況につき監査責任者は定期的な監査を実施し社長に報告する。社長は特定個人情報等の取扱状況を把握し、安全管理措置の評価、見直し及び改善を指示し、特定個人情報管理者が改善に取り組む。

①　実施

・定期監査：毎年 6 月

・臨時監査：監査責任者・特定個人情報保護管理者・社長が認めた場合適宜

②　報告

監査責任者は、「特定個人情報監査チェック表」に監査結果を記入し社長に報告する。

③　改善

改善しなければならない事項が発生した場合社長は改善を指示する。

第 6 章　人的安全管理措置

当社は以下のような人的安全管理措置を講じる。

6.1　事務取扱担当者の監督

特定個人情報管理者は、特定個人情報等が本規程に基づき適正に取り扱われるよう、事務取扱担当者及び従業者に必要かつ適切な監督を行う。

6.2　教育・研修

事業者は、事務取扱担当者及び従業者に定期的な教育を行う。

(1)　事務取扱担当者

① 特定個人情報等の適正な取扱いの周知徹底

② 年に一度（6 月）に定期的な教育を行い、「教育実施記録」に記録する。

(2)　従業者

① 特定個人情報等の取扱いに関する留意事項等について

② 年に一度（6 月）に定期的な教育を行い、「教育実施記録」に記録する。

6.3　機密保持

当社は、特定個人情報等についての秘密保持に関する事項を就業規則等に盛り込む。

第 7 章　物理的安全管理措置

当社は以下のような物理的安全措置を講じる。

7.1　特定個人情報等を取扱う区域の管理

特定個人情報等の漏えい等を防止するために、特定個人情報ファイルを取り扱う情報システムを管理する区域（以下「管理区域」という。）及び特定個人情報等を取り扱う事務を実施する区域（以下「取扱区域」という。）を明確にする。

(1) 管理区域へ業務上許可を得ていない記録機能を持つ媒体及び機器の持ち込み及び持ち出しを禁止する。

(2) 管理区域の入退室の管理を行う。管理区域へ入退室の際に「管理区域入退室記録簿」に記録する。

(3) 取扱区域は、壁又は間仕切り等の設置、事務取扱担当者以外の者の往来が少ない場所への座席配置、後ろから覗き見される可能性が低い場所への座席配置等を工夫するものとする。

7.2　機器及び電子媒体等の盗難等の防止

(1) 特定個人情報を取扱う機器、電子媒体、または書類等は「鍵管理一覧」で施錠管理されているキャビネット・書庫などに保管する。

(2) 特定個人情報を取扱う機器はセキュリティワイヤー等で固定する。

7.3　電子媒体等を持ち出す場合の漏えい防止

(1) 電子記録媒体又は書類を持ち出す際は、容易に個人番号が判明しない措置を実施する。（持出しデータの暗号化、パスワードによる保護、施錠できる搬送容器の使用等、書類等は封緘、目隠しシール貼付等）

(2) 電子記録媒体又は書類を持ち出す（移送する）際は、簡易書留等の追跡可能な移送手段を利用する。

7.4　特定個人情報の削除、機器及び電子媒体等の廃棄

(1) 特定個人情報を削除又は廃棄する場合は「特定個人情報一覧表」に記録する。

(2) 特定個人情報の削除又は廃棄を委託している場合、委託先が確実に削除又は廃棄した事の証明書等を確認する。

(3) 特定個人情報が記載された書類等を廃棄する場合、復元不可能な手段として焼却又は溶解等を行う。

(4) 特定個人情報が格納された機器及び電子媒体等を廃棄する場合、復元不可能な手段として専用のデータ削除ソフトウェアの利用又は物理的な破壊等を行う。

(5) 特定個人情報ファイル中の個人番号又は一部の特定個人情報を削除する場合、容易に復元できない手段（消去ツール等）を利用して行う。

(6) 個人番号が記載された書類等は、法的な保存期間経過後に廃棄をする。

第 8 章　技術的安全管理措置

当社は以下のような技術的安全管理措置を講じる。

8.1　アクセス制御

(1) 取扱う特定個人情報ファイルの範囲を限定するため、適切なアクセス制御を行う。
(2) 個人番号と紐づけてアクセスできる情報の範囲を、アクセス制御により限定する。
(3) 特定個人情報ファイルを取扱う情報システムを、アクセス制御により限定する。
(4) ユーザ ID に付与するアクセス権により、特定個人情報ファイルを取扱う情報システムを使用できる者を、事務取扱担当者のみに限定する。
(5) 特定個人情報を取扱うシステムは、事務取扱担当が正当なアクセス権を有する者であることを（ユーザ ID で、パスワードで、磁気 IC カードで）識別、認証する。

8.1.1　ユーザ ID の付与

(1) システム責任者は、特定個人情報ファイルにアクセスできる権限（ユーザ ID）を事務取扱担当者に付与する。
(2) システム責任者は、アカウント名、対象者、付与したアクセス権限などを、「ユーザ ID 管理台帳」に記録し、ユーザ ID の付与に伴って、随時更新し、最新の状態に維持する。
(3) システム責任者は、退職・異動の反映もれ等により付与したアクセス権限の適切性が損なわれていないか、「ユーザ ID 管理台帳」の見直しを定期的に行う。
(4) 特権 ID はシステム責任者のみが使用する。
(5) システム責任者は、初期設定されている特権 ID のパスワード変更を実施する。
(6) 特定個人情報を格納したデータベースに直接アクセスできるのはシステム責任者のみとする。
(7) システム責任者は、不要アカウントがあれば速やかに無効化し、「ユーザ ID 管理台帳」の内容を更新する。
(8) また、システム責任者は、次の場合ユーザ ID を速やかに無効化する。
    (ア) ユーザ ID を利用する従業者が、退職、解雇、契約解除、休職、異動等により、その利用権限を失った場合
    (イ) ユーザ ID を利用する従業者の内部規程違反が判明し、当該ユーザ ID を利用し続けることが適切でないと判断される場合

8.2　外部からの不正アクセス等の防止

特定個人情報ファイルを取り扱う情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、運用する。

(1) 特定個人情報ファイルを取り扱う情報システムと外部ネットワークとの接続箇所に、ファイアウォール等を設置し、不正アクセスを遮断する。
(2) 特定個人情報ファイルを取り扱う情報システム及び機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入する。

(3) 導入したセキュリティ対策ソフトウェア等により、入出力データにおける不正ソフトウェアの有無を確認する。
(4) 機器やソフトウェア等に標準装備されている自動更新機能等の活用により、セキュリティ対策ソフトウェア等を最新状態にする。
(5) アクセスログを定期的に分析し、不正アクセス等を検知する。

8.3 情報漏えい等の防止

特定個人情報等をインターネット等により外部に送信する場合、通信経路における情報漏えい等を防止する。

情報システム内の特定個人情報のデータは暗号化又はパスワードにより保護する。

(1) 通信経路における情報漏えい等の防止策として、SSL や VPN 等の通信の暗号化を行う。
(2) 電子メールを特定個人情報等の機密データの送信には極力利用しない。業務上やむをえない場合は、特定個人情報等の機密データに対し暗号化やパスワードなどの策を講じる。
(3) 情報システム内に保存されている特定個人情報等の漏えい等の防止策として、データの暗号化又はパスワードによる保護等を行う。
(4) アプリケーションレベルでのパスワードのポリシー
    ① 仮のパスワードは、最初のログオン時点で変更する。
    ② パスワードを秘密にしておく。
    ③ パスワードを紙に記録して保管しない。
    ④ パスワードは、6 文字以上で設定する。
    ⑤ パスワードは、3 か月に 1 回以上及び必要に応じて適宜、変更する。
    ⑥ パスワードには英数字や記号等を混在させる。

第 9 章　委託先における安全管理措置

9.1　委託先の監督

当社は、個人番号関係事務又は個人番号利用事務の全部又は一部を委託する場合には、当社自らが果たすべき安全管理措置と同等の措置が委託先において適切に講じられるよう、必要かつ適切な監督を行なうものとする。

(1) 委託先の選定

当社は、委託先の選定において、当社自ら果たすべき安全管理措置と同等の措置が講じられているか、あらかじめ確認する。

(2) 委託先に安全管理措置を遵守させるために必要な契約の締結（誓約書、同意書等）を行う。また、委託先における特定個人情報の取扱状況を把握する。

当社と委託先との委託契約には次の事項を含める。

① 秘密保持義務
② 事業所内からの特定個人情報の持出しの禁止
③ 特定個人情報の目的外利用の禁止
④ 再委託における条件
⑤ 漏えい事案等が発生した場合の委託先の責任
⑥ 委託契約終了後の特定個人情報の返却又は廃棄
⑦ 従業者に対する監督・教育
⑧ 契約内容の遵守状況について報告を求める規定
⑨ 特定個人情報を取扱う従業者の明確化
⑩ 委託者（当社）が委託先に対し実地の調査を行うことができる旨の規定

9.2　再委託

(1) 委託を受けた者は、委託者（当社）の許諾を得た場合に限り、再委託を行うことができる。
(2) 再委託を受けた者は、委託者(当社)の許諾を得た場合に限り、更に再委託を行うことができる。
(3) 委託先は、再委託先を監督する義務があるため、委託契約に再委託する場合の取扱いを定め、再委託を行う場合の条件、再委託した場合の委託先に対する通知義務等を盛り込むことを指導する。
(4) 委託者は、委託先や再委託先以下すべての委託先に監督義務を負う。