情報保護・管理要領

第１　目的

乙が本件業務において取り扱う各種情報（その意義は「第２　適用範囲」で定めるとおり。）について、適正な情報保護・管理方策、情報システムのセキュリティ方策、及び情報の漏えい、盗難、盗用、亡失、改ざん等（以下、「情報漏えい等」という。）の防止及び発生時に実施すべき事項・手順等について明確にすることを目的とする。

第２　適用範囲

甲が乙に対して開示又は提供する、本件業務の履行に必要な全ての情報（文書、電子メール、電磁的記録等、当該情報を記載・記録した媒体、クラウドサービスを含む。）を対象とする。

第３　乙が遵守すべき事項

乙は、本契約の履行にあたり、以下の項を全て遵守すること。

なお、特定個人情報を取り扱う委託契約について、下請又は再委託（下請契約又は再委託契約が数次にわたるときには、その全てを含む。）することを甲が許諾した場合、下請先又は再委託先以降にも、以下の項を全て遵守させること。

１　情報管理計画書の提出・承認

乙は、２から４までの各項に定める内容について、本件業務の履行開始までに「情報管理計画書」（表１）として取りまとめた上で甲の主管担当（以下、「主管担当」という）に提出し、承認を受けること。

（表１）「情報管理計画書」として提出するもの。

情報取扱者等名簿
教育・周知計画書
情報取扱計画書
作業場所等に係るセキュリティ措置計画書
情報漏えい等発生時の対応手順書

２　作業開始前の遵守事項

(1) 情報取扱者等の指定（情報取扱者等名簿）

乙は、上記「第２　適用範囲」に定める情報を取り扱う者（「情報取扱者」といい、その中でも個人情報（特定個人情報を除く。）を取り扱う者を「個人情報取扱者」、特定個

人情報を取り扱う者を「特定個人情報取扱者」という。以下同じ。）及び、情報取扱者を統括する情報システム部門に精通した課長相当職以上の者（「情報取扱責任者」といい、その中でも個人情報（特定個人情報を除く。）の管理に関する責任を負う者を「個人情報取扱責任者」、特定個人情報の管理に関する責任を負う者を「特定個人情報取扱責任者」という。以下同じ。）を指定し、その所属、役職及び氏名等を記入した「情報取扱者等名簿」を作成すること。下請先又は再委託先も対象とすること。なお、情報取扱者及び情報取扱責任者（以下「情報取扱者等」という。）は、守秘義務等情報の取り扱いに関する社内教育、又はこれに準ずる講習等を受講した者とし、「情報取扱者等名簿」にその受講実績も併せて記入すること。

(2) 個人情報取扱者等の指定（情報取扱者等名簿）

個人情報（特定個人情報を除く。）を取り扱う委託契約については、個人情報取扱者を必要最小限に限定し、取扱者と利用目的を「情報取扱者等名簿」に記入すること。

なお、開発担当者と運用担当者の分離、管理者と担当者の分離を行い、取扱者を必要最小限に限定するとともに、相互牽制が働く体制にすること。

(3) 特定個人情報取扱者等の指定（情報取扱者等名簿）

特定個人情報を取り扱う委託契約については、特定個人情報取扱者を必要最小限に限定し、取扱者と利用目的を「情報取扱者等名簿」に記入すること。

なお、特定個人情報取扱責任者は、情報取扱責任者の中から選定すること。

(4) 情報取扱者等への教育・周知(教育・周知計画書)

乙は、本件業務で取り扱う各情報について、その取り扱いや漏えい防止等に係る「教育・周知計画書」を作成し、表２の内容に関して、情報取扱者等に対する教育及び周知を行うこと。教育及び周知は、本件業務の履行開始前、新たに情報取扱者等を指定したときのほか、定期的（年１回以上）に行うこと。

（表２）

ア	本情報保護･管理要領の内容
イ	個人情報に関する法規
ウ	特定個人情報に関する法規（特定個人情報を取り扱う場合）
エ	アクセス制限の管理ルール（ＩＤ・ＰＷ）
オ	入退館(室)管理ルール、機器管理ルール
カ	ドキュメント、記録媒体の管理ルール
キ	その他、本件業務の内容に関連する規程等

また、乙が乙の社員を甲の社内（本社、貯金事務センター、貯金事務計算センターその他甲が指定する場所をいう。以下同じ。）で事務に従事させる場合は、当行内の情報セキュリティ関係ルールの教育及び周知を行い、ルールを遵守させること。関係ルールの周知・教育の実施状況について本件業務の履行開始前までに主管担当に提出すること。

(5) 情報の取り扱いに関する計画策定（情報取扱計画書）

乙は、本件業務における情報の授受、保管、使用、廃棄等に関するルールを定めて、「情報取扱計画書」を作成し、甲の承認を得ること。

以下の事項はリスク管理に直結する重要な事項のため可能な限り明記すること。

① データの入力・保管・処理・バックアップ・出力の一連のフロー

② 暗号方式、暗号化されている領域とされていない領域

③ システムログの取得範囲・取得頻度・保存期間

④ データコピー（バックアップを含む）の取得内容と保管場所・保管期間

⑤ 暗号鍵の管理方法（ただし、顧客の重要情報（※１）の復号鍵の管理は甲が行うため、これを除く。）

⑥ 暗号化しない場合の代替策

⑦ サービスの利用終了又は契約解除後のデータ移行、消去（バックアップ、災害対策環境等を含む）等の対応

⑧ 不正アクセス防止策・監視体制（システム等の監視状況やシステムログの提出）

なお、情報の複製、破棄及び保管場所の変更等が生じる可能性がある場合はその取り扱いについても記載すること。

個人情報を取り扱う委託契約については、個人情報の暗号化やマスキングのルール、情報を利用する際の利用ルール、電子記録媒体に出力する際の取り扱いルール等の管理ルールを定めて、「情報取扱計画書」に記載又は別紙として添付すること（※２）。

特定個人情報を取り扱う委託契約については、上記個人情報を取り扱う委託契約に定めるルールに加え、以下の事項を「情報取扱計画書」に記載又は別紙として添付すること（※２）。

ア　取り扱う特定個人情報の範囲（甲が指定した範囲に限る）

イ　特定個人情報が記録された電子記録媒体又は書類等を持ち運ぶ方法

性質や量等に応じて以下の項目のいずれか又は複数の措置を講じること。

（甲との授受以外の乙の事業所内の管理区域（特定個人情報ファイル（個人番号をその内容に含む個人情報データベース等をいう。以下同じ。）を取り扱う情報システムを管理する区域をいう。以下同じ。）又は取扱区域（特定個人情報を取り扱う事務を実施する区域をいう。以下同じ。）からの持出しは禁止。）

・持ち運びデータの暗号化及びパスワードによる保護

・施錠できる搬送容器の使用

・追跡可能な移送手段の利用（書留郵便等）

・書類等の封緘、目隠しシールの貼付

なお、「持ち運び」とは、特定個人情報を管理区域又は取扱区域の外へ移動させること又は当該区域の外から当該区域へ移動させる事をいい、事業所内での管理区域又は取扱区域の内外をまたぐ移動等も持ち運びに該当する。

おって、事業所内での移動等については、事前に甲の許可があった場合に限り可とする。

ウ　特定個人情報の利用実績又はシステムログの記録方法

(ｱ) 特定個人情報ファイルの利用・出力状況の記録

(ｲ) 書類・媒体等の持ち運びの記録

(ｳ) 特定個人情報ファイルの削除・廃棄記録

(ｴ) 特定個人情報ファイルを情報システムで取り扱う場合、特定個人情報取扱者の情報システムの利用状況（ログイン実績、アクセスログ等）の記録

※１　顧客の重要情報は、顧客情報の中でも特に厳格な取扱いが求められるもので、以下の「顧客の重要項目」を含む情報。

① 個人番号

② 暗証番号

③ 認証情報

④ クレジットカード情報（クレジットカード番号、セキュリティコード、暗証番号、有効期限）

⑤ 生体認証情報

⑥ 機微情報（要配慮個人情報、本籍地等センシティブ情報）

⑦ その他顧客に損失が発生する可能性のある情報

※２　乙及び下請先又は再委託先以降で管理するシステム（通常業務では使用しないシステム領域を含む）及びネットワーク領域等も対象範囲とすること。

(6) 作業場所等のセキュリティ確保（作業場所等に係るセキュリティ措置計画書）

乙は、甲の社内以外の作業場所において本件業務を行う場合は、作業場所等のセキュリティ確保のため講じる次の措置について、「作業場所等に係るセキュリティ措置計画書」を作成し、甲の承認を得ること。

ア　作業場所のセキュリティ確保のために講じる措置(技術面)

例：データエントリールーム、データ保管室、電子計算機室等に対する施錠設備、ＩＤカードやパスワードを用いた入退室管理機能等

イ　その他セキュリティ確保のために講じる措置(運用面)

例：システムログインパスワード、データに対する専用のＩＤ、アクセス権限の設定、電子記録媒体の管理等

なお、個人情報を取り扱う委託契約については、個人情報が閲覧可能なＩＤを都度払出しにするなど、上記ア、イについて、より厳格な管理を「作業場所等に係るセキュリティ措置計画書」に具体的に記入すること。

また、個人情報の所在地域（適用される法令が特定できる範囲）を明確にすること。

おって、特定個人情報を取り扱う委託契約については、以下の事項を「作業場所等に係るセキュリティ措置計画書」に明記すること。

ウ　特定個人情報を取り扱う区域の管理方法

管理区域及び取扱区域を明確にし、管理区域については入退室管理に加え、持ち込む機器及び電子記録媒体の制限を、取扱区域については壁又は間仕切り等の設置や特定個人情報取扱者以外の者の往来が少ない場所や、後ろから覗き見される可能性が低い場所への配置等をする等の措置を講じる。

エ　特定個人情報を取り扱う機器、電子記録媒体及び書類等の盗難等の防止措置

(ｱ) 特定個人情報取扱責任者及び特定個人情報取扱者のみが使用、常時施錠できるキャビネット・書庫等に保管する。

(ｲ) 特定個人情報ファイルを取り扱う情報システムが機器のみで運用されている場合は、セキュリティワイヤー等により固定する。

オ　特定個人情報のアクセス制御措置

(ｱ) 個人番号と紐付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。

(ｲ) 特定個人情報ファイルを取り扱う情報システムを、アクセス制御により限定する。

(ｳ) ユーザー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り扱う情報システムを使用できる者を特定個人情報取扱者に限定する。

カ　特定個人情報へのアクセス者の識別・認証措置

特定個人情報を取り扱う情報システムは、ユーザーＩＤ、パスワード、磁気・ＩＣカード等の識別方法により、特定個人情報取扱者が正当なアクセス権を有する者であることを、識別した結果に基づき認証するものとする。

キ　特定個人情報への外部からの不正アクセス等の防止措置

以下の各方法により、情報システムを外部等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ものとする。

(ｱ) 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方法。

(ｲ) 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）を導入する方法。

(ｳ) 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方法。

(ｴ) 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、ソフトウェア等を最新状態とする方法。

(ｵ) ログ等の分析を定期的に行い、不正アクセス等を検知する方法。

ク　特定個人情報の漏えい等の防止措置

特定個人情報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及び情報システムに保存されている特定個人情報の情報漏えい等を防止するものとする。

(ｱ) 通信経路における情報漏えい等の防止策

通信経路の暗号化

(ｲ) 情報システムに保存されている特定個人情報の情報漏えい等の防止策

データの暗号化及びパスワードによる保護

(7) セキュリティ管理状況の事前実査

乙及び下請先又は再委託先以降が甲の社内以外の作業場所において本件業務を行う場合において、主管担当がその施設及び設備に関し、上記(5)、(6)で乙が作成した「情報取扱計画書」及び「作業場所等に係るセキュリティ措置計画書」に則ったセキュリティ確保が図られているかを契約履行前に実査する旨申し出たときは、速やかにこれを受け入れ、またこれを受け入れさせること。また、実査で指摘を受けたときは、速やかに是正措置を主管担当に報告し、承認を受けること。

なお、実査にあたっては、主管担当のほか甲の内部監査部署、金融監督当局及び主管担当が指定した外部監査人も立ち入りを可能とする。

(8) 情報漏えい等発生時の対応手順作成

乙は、情報漏えい等が発生した場合を想定し、その情報漏えい等発生時の対応手順書を作成し、甲の承認を得ること。

3　作業中における遵守事項

(1) 情報管理計画書の遵守

乙は、甲の承認を受けた「情報管理計画書」を遵守すること。

(2) 情報管理簿等の作成

乙は、甲から開示又は提供された情報のうち、別途主管担当が指定する情報（指定がない場合はすべての情報）について、データの種類・名称、責任者、授受方法、保管場所、保管方法、使用場所、使用目的、個人情報の廃棄等の取扱方法を明確にするため「情報管理簿」を作成し、作業中の取扱状況を記録すること。

特定個人情報ファイルを取り扱う委託契約については、上記に加えさらに、特定個人

情報ファイルの取扱部署、アクセス権を有する者、データの削除・廃棄状況等を明確にするために「特定個人情報ファイル管理台帳」を作成し、作業中の取扱状況を記録すること。

(3) 作業場所の監査

乙及び下請先又は再委託先以降は、甲の社内以外の作業場所において本件業務を行っている場合に、主管担当がその施設及び設備に関し、上記２(5)、(6)で乙が作成した「情報取扱計画書」及び「作業場所等に係るセキュリティ措置計画書」に則ったセキュリティ確保が図られているか監査する旨申し出たときは、定期・不定期にかかわらず、速やかに監査に応じること。また、監査で指摘を受けたときは、速やかに是正措置を主管担当に報告し、承認を受けること。

なお、監査にあたっては、主管担当のほか甲の内部監査部署、金融監督当局及び主管担当が指定した外部監査人も立ち入りを可能とする。

(4) 情報の取り扱い

乙は、本件業務において取り扱う情報に関し、情報取扱責任者に以下の作業を行わせること。

ア　情報取扱者の作業に立ち会う等適切な管理を行うこと。

イ　情報取扱者を作業に従事させる前に、情報取扱者ごとに使用するユーザーＩＤ等、主管担当が事前に指定する事項について報告を行い、主管担当の承認を受けること。

なお、報告する時期等は主管担当の指示に従うこと。

また、報告した内容に変更が生じる場合も、事前に主管担当の承認を受けること。

ウ　作業に従事する予定の情報取扱者について、事前に氏名、勤務時間、作業内容及び取扱情報を記入した作業予定表を提出し、主管担当の承認を受けること。

エ　作業に従事した情報取扱者が作業を終了し、作業場所を離れる際は、情報の持ち出しの有無を厳重に検査すること。

オ　作業終了後、作業に従事した情報取扱者の氏名、勤務時間、作業内容、取扱情報及び情報の持ち出しの有無等を記入した作業結果表を主管担当へ提出すること。その際、当初予定していた勤務時間を超えている場合は、その理由も併せて記入すること。

なお、作業結果表の提出時期については、主管担当の指示によること。

カ　データのトレーサビリティの確保及び定期的な確認

個人データを取り扱う委託契約については、個人データの漏えい対策としてシステム等の監視状況やシステムログなどを管理し、甲の求めに応じて速やかに提出できる体制にすること。

また、個人データに対する不正アクセスがないか定期的にログを確認し、主管担当に

報告すること。

キ　データの消失防止対策

クラウドサービスやホスティング等受託者側でデータを管理する役務を提供する場合は、乙の責任においてバックアップデータを確保するとともに、あらかじめバックアップデータを含めたデータの消失防止対策書を提出し、甲の了承を得ること。

ク　個人情報の廃棄

個人情報を取り扱う委託契約について、個人情報を保持する場合は必要性を定期的に見直し、不必要となった情報を速やかに廃棄すること。廃棄の際は、「情報取扱計画書」に定めたルールに従い、下記４の処理を実施すること。

なお、乙及び下請先又は再委託先以降で保持する記憶装置等の故障等により、個人情報を記録している可能性がある記憶装置及び部品等を廃棄する場合も、下記４の手続に従うこと。

ケ　特定個人情報の削除・廃棄

特定個人情報を取り扱う委託契約については、あらかじめ定められた期間のみ特定個人情報を保持することができることとし、当該期間経過後速やかにデータの削除、廃棄を実施すること。

データの削除・廃棄の際は、「情報取扱計画書」に定めたルールに従い、下記４の処理を実施すること。

４　委託作業完了時の遵守事項

(1) 情報返却等処理

乙は、本契約終了時に、甲の求めに応じ、上記３(2)で作成した「情報管理簿」に記載されている全ての情報（バックアップを含む）について、返却、消去、廃棄等の措置を行うこと。

なお、その処理について方法、日時、場所、立会い者、作業責任者等の事項を網羅した、「情報返却等計画書」を事前に主管担当あて提出し、承認を得た上で、処理を実施すること。

(2) 記録媒体上のデータ処分方法

乙は、記録媒体上のデータを処分する際は、施設外に搬出する前に復元不可能となる手段で物理的破壊（記録部位の破壊）又は消去を行うこと。ただし、媒体の廃棄を行う場合については、物理的破壊を行うこと。

ただし、施設内での破壊又は消去が困難な場合は、復元を不可能または著しく困難な状態にする等の情報漏えい等の対策を「情報返却等計画書」に記載し、事前に主管担当の承認を得た上で持ち出すことを可とする。（特定個人情報を除く。）

※　破壊　…　物理的に復元不可能な状態に破壊

※　消去　…　専用ツールによる完全消去、または、専用装置による消磁

(3) 作業後の報告

乙は、上記(1)(2) に基づく返却等の処理終了後、その結果を記載した「情報管理簿」（特定個人情報ファイルの返却等の処理であった場合、「特定個人情報ファイル管理台帳」）を主管担当あて提出し、承認を受けること。

また、「情報管理簿」（特定個人情報ファイルの返却等の処理であった場合、「特定個人情報ファイル管理台帳」）に記載された情報について、主管担当の承認を得た場合を除き、情報を複製していない旨の証明書（様式適宜）を主管担当あて提出するものとし、主管担当の承認を得て情報を複製した場合には、作業終了後、直ちに一切の情報を消去し、情報の消去に関する報告書（様式適宜）を提出すること。この他、「情報管理簿」（特定個人情報ファイルの返却等の処理であった場合、「特定個人情報ファイル管理台帳」）に記載の情報について廃棄処分を行った場合には廃棄証明書およびその証跡（外見上破壊したことが分かる場合は対象機器等が判別できる廃棄処理後の写真、消去時のデータ消去ツールから出力された対象機器等が判別できる消去レポート・実行ログ　等）を提出しなければならない。

なお、「情報管理簿」（特定個人情報ファイルの返却等の処理であった場合、「特定個人情報ファイル管理台帳」）及び廃棄証明書については、当該処理の実施方法、実施日時、実施者、確認者（又は立会者）等、当該作業が確実に実施されたことが確認できる事項を記載すること。

5　情報漏えい等発生時の対応

乙は、本件業務に関し、情報漏えい等が発生した場合は、以下により、直ちに対応を図ること。

なお、特定個人情報については、情報漏えい等の発生に加え、情報漏えい等の兆候及び契約内容に違反している事実又は兆候を把握した場合も、同様に以下により対応を図ることとする。

(1)　発生状況報告

本件業務中に、情報漏えい等が発生した場合は、情報漏えい等が発生した日時、場所、原因、発生時の情報取扱者を明らかにし、直ちに主管担当に連絡するとともに、事故の概要等について書面により主管担当あて報告すること。

(2)　対応措置

乙は、主管担当の指示に基づき、直ちに漏えい等した情報の捜索・回収等二次被害防止のための措置を実施すること。

(3)　報告書の提出

乙は、主管担当が指定する期日までに、発生した事態の具体的内容、原因、実施した対処措置等を内容とする報告書を作成の上、提出すること。

(4)　再発防止策の策定・提出

乙は、情報漏えい等が発生した場合、その対応措置後に発生原因等を検証して再発を防止するための措置内容を策定し、主管担当の承認を得た後、速やかに情報漏えい等再発防止策を実施すること。

6　個人情報を保持する委託先の経営不安発生時の対応

個人情報を取り扱う委託契約について、乙及び個人情報を保持する下請先又は再委託先等の経営不安が発生した場合、甲もしくは甲が指定する専門業者が、必要に応じ施設に立ち入り、個人データや関連著作物・成果物の保全を行うこと。