機密情報保持に関する特約

日本情報通信株式会社（以下「甲」という。）と受託者（以下「乙」という。）は、本契約に適用される特約として、以下の通り定めるものとする。
本特約は、本契約（注文書・注文請書を含む）について、締結済み「機密保持契約書」、「個人情報および特定個人情報等の開示にかかる覚書」、又は、本契約、若しくは本契約に適用される基本契約に定める機密保持条項の他、甲から乙に対して開示された機密情報および個人情報（以下「情報」という）の情報管理方法を定めるものとする。乙は、甲より情報の開示を受けた場合、情報の管理方法について本特約記載事項を遵守するものとする。

1. 情報管理方法について

1-1 情報管理責任者の明確化

下記 1-2～1-8 の 甲又は甲顧客セキュリティ要求事項を理解し、情報の受領・作成～保管～破棄迄、一元的に管理する責任者を設置すること。

1-2 情報の取扱い

(1)受領・作成

情報（電子ファイル、紙媒体）の受領・作成時に記録を取ること。

(2)利用

①情報の利用者は、本契約の業務従事者に限定すること。

②会社資産以外の端末（私有ＰＣ、ネットカフェのＰＣなど）・記録媒体（HDD、CD、MO、FD、USB メモリなど。以下同様）を用いて、情報の取扱いは行わないこと。

(3)配布

①情報（電子ファイル、紙媒体）の配布時に記録を取ること。

②情報を電子メールで送信する場合は、以下を遵守すること。

・情報を本文に記載しないこと。

・情報を添付する場合は、暗号化を実施すること（ファイルを添付したメールに復号鍵を記載しないこと）。

③情報を FAX で送信する場合は、リダイヤル機能、短縮ダイヤル等の利用による誤送信対策を実施すること。

(4)持ち出し

①原則禁止とすること。

②真に止むを得ない理由により、情報を持ち出す場合は、以下を遵守すること。

・持ち出す必要のある必要最低限の情報に限定すること。

・１項で定めた情報管理責任者の承認を得ること。

・持ち出し及び返却の記録を取ること。

・電子ファイルとして持ち出す場合は、暗号化等のセキュリティ対策を実施すること。

・情報の入った端末（PC、スマートフォンなど）・記録媒体は携帯すること（端末・記録媒体の入った鞄を電車の網棚に置かない、店の席に置いて席を離れない等）。

⑸保管

情報を記録する記録媒体や紙媒体は、関係者以外触れることが出来ないよう、施錠された書庫等に保管すること。

⑹返却・破棄

①情報は、本契約の業務上不要になった時点で破棄もしくは甲へ返却し、その記録を取ること。

②情報を破棄する場合は、

・紙媒体は、細断、溶解等により復元できないようにして破棄すること。

・電子データは消去用専用ソフトウェア等で復元できないように削除すること。

・電子データを記録した媒体、機器は破壊等によりデータが読み取れないようにして破棄すること

1-3 情報を取扱う居室のセキュリティ対策

（甲の管理下にある居室は対象外となります。）

⑴居室管理

情報を取扱う居室は、本契約の業務上必要最低限に限定すること。

⑵アクセス管理

①常時施錠すること。

②入退室権限は、本契約の業務上必要最低限の人員に付与すること。

③不要となった入退室権限は、直ちに停止すること（退職、異動、休職など）。

④不要な入退室権限が残っていないことを、定期的に確認すること。

⑤共連れ防止対策（アンチパスバック、監視カメラなど）の導入が望ましい。

⑶持込管理

①会社資産以外の端末（PC など）・記録媒体の持込みを禁止すること。

1-4 情報を取扱う情報システム（乙の資産）のセキュリティ対策

（甲の管理下にある情報システム・ネットワークは対象外となります。）

⑴情報システムの管理

①業務に関連する情報システムの目録を維持・管理し、情報システムの管理責任者、情報システム利用者の役割を明らかにすること。

②情報システムへの脆弱性対策として、必要に応じパッチ適用等の対応を速やかに実施すること。

⑵アクセス管理

①アカウント（特権アカウント含む）は、本契約の業務上必要最低限の人員に付与すること。

②アカウントは、個人単位に付与すること。

③情報の操作（閲覧、書き出し、更新、印刷など）をできる範囲は、本契約の業務上必要最低限に限定すること。

④不要となったアカウントは、直ちに停止すること（退職、異動、休職など)。

⑤不要なアカウントが残っていないことを、定期的（１回／年以上が望ましい）に確認すること。

(3)ログ管理

①アクセス（ログイン・ログアウト）ログを取得すること（操作[閲覧、書き出し、更新、印刷など]ログも取得することが望ましい)。

②アクセスログを一定期間保管すること。

③不正なログインの形跡が無いか、アクセスログを定期的に確認すること。

(4)端末管理

①情報を取扱う端末（PC、スマートフォンなど）は、本契約の業務上必要最低限に限定すること。

②ログオン認証機能を導入すること。

③認証機能付きスクリーンセーバを設定すること（スクリーンセーバの起動までの時間は５分以下が望ましい)。

④OS・アプリケーションはサポートが終了しておらず、バージョンやパッチ適用を適切に管理すること。

⑤情報漏えいが懸念されるファイル共有ソフトウェア（Winny、Share、WinMX など）の使用はしないこと（システム的にファイル共有ソフトウェアの起動を阻止するのが望ましい)。

⑥日常的に情報を取扱っている端末(PC など)の持ち出しは禁止すること。

⑦ノート型の端末（PC など）は、長時間席を離れる場合（退社、外出など)、必ず施錠保管すること。

⑧記録媒体への書き出しは本契約の業務上必要最低限に制限すること(システム的な制限を設けることが望ましい)。

⑨会社資産以外の端末（PC、スマートフォンなど）の社内ネットワークへの接続をシステム的に拒否することが望ましい。

⑩会社資産以外の記録媒体の端末（PC、スマートフォンなど）への接続をシステム的に拒否することが望ましい。

(5)外部からの不正アクセス対策

①外部ネットワーク（インターネット等）と接続する場合は、ファイヤーウォール、IPS などを導入し、以下を遵守すること。

・ファイヤーウォール、IPS などのログを一定期間保管すること。

・不正アクセスの形跡が無いか、ファイヤーウォール、IPS などのログを定期的に確認すること。

②端末（PC など）には、ウィルス対策ソフトを導入し、以下を遵守すること。

・ウィルス定義ファイルは常に最新の状態にすること。

・リアルタイム検査を行うこと。

・保存されている全てのファイルに対する検査を定期的に行うこと。

③外部との通信は、Proxy またはゲートウェイサーバ経由で行い、その通信ログを一定期間保管することが望ましい。

1-5 貸与物の管理

甲又は甲顧客から乙に貸与した端末（PC、スマートフォンなど）・記録媒体、入館証・事務所内キャビネット及び、ロッカーの鍵などは、常に貸与品を善良な管理者の注意をもって使用し、保管しなければならない。飲酒又は、飲酒が想定される場面においては、貸与物を帯同せずオフィス、自宅等において保管しなければならない。

1-6 業務従事者への周知

(1)「情報管理方法（機密情報保持に関する特約事項）」を本契約の業務開始前に業務従事者に周知・認識させること。

(2)「情報管理方法（機密情報保持に関する特約事項）」を業務従事者に定期的に周知・認識させること。

1-7 委託先（乙の委託先）の管理

(1) 情報を委託先に開示する場合は、業務を遂行する上で必要最低限の範囲に限定すること。

(2)「情報管理方法（機密情報保持に関する特約事項）」と同等の契約を委託先と締結すること。

(3)「情報管理方法（機密情報保持に関する特約事項）」を本契約の業務開始前に委託先に周知・認識させること。

(4)「情報管理方法（機密情報保持に関する特約事項）」が遵守されていることを定期的に確認すること。

(5)乙の委託先が更に第三者に再委託する場合、乙は乙の委託先に対して「情報管理方法（機密情報保持に関する特約事項）」と同等の契約を当該第三者と締結する旨の義務を課すこと。

1-8 インシデントの報告

インシデント（情報の漏えい、紛失、盗難など）が発生した場合は、速やかに報告すること。

1-9 監査

甲は、乙による本特約の遵守状況を確認するため、乙に対して随時報告または乙（再委託がある場合は乙の委託先を含む。）事業所への立ち入り監査をすることを求めることができるものとし、監査に際して、乙は合理的な範囲で協力するものとする。また、報告・監査の結果、本特約の遵守状況につき改善要求が甲からあった場合、乙はこれにすみやかに従うものとする。

以上