安全対策細則

Ver.3.5

株式会社同窓会事務局

承認	作成
個人情報監査責任者	個人情報管理責任者

目　　次

改訂履歴

Ver	年月日	改訂内容
1.0	2005 年 04 月 01 日	制定初版
1.1	2005 年 10 月 20 日	Ⅲ３(1)⑦及びⅣ項目追加
1.2	2005 年 12 月 20 日	Ⅱ１⑦追加 Ⅲ２（２）②b 文章変更 Ⅲ３（２）②文章追加
1.3	2006 年 02 月 10 日	Ⅲ２（２）②b 文章変更
2.0	2007 年 04 月 01 日	JIS Q 15001:2006 対応に伴い全面改訂
2.1	2008 年 04 月 01 日	Ⅵ文章追加
2.2	2008 年 07 月 01 日	Ⅵ文章変更
3.0	2010 年 07 月 01 日	Ⅵ文章追加 a　b
3.1	2011 年 03 月 03 日	社名変更
3.2	2012 年 06 月 30 日	Ⅰ２（１）を変更 Ⅰ３（１）を変更 Ⅱ１（２）② Ⅶ（１）（２）（３）追加
3.3	2016 年 05 月 31 日	Ⅲ２（３）追加
3.3	2016 年 05 月 31 日	Ⅲ３（１）③文章変更
3.4	2018 年 02 月 15 日	Ⅲ２（２）④を変更 Ⅲ３（１）①を変更 Ⅲ３（１）⑥を変更 Ⅳ２（２）を変更 Ⅴ３③を変更
3.5	2018 年 06 月 8 日	Ⅵ. 1. 21 を追加、③を変更

Ⅰ　総則

１．目的

（１）本細則は、当社における個人情報の取得、利用、提供および管理における取扱いの各局面におけるリスク（個人情報の漏えい、滅失又はき損、関連する法令及びその他の規範に対する違反、想定される経済的な不利益及び社会的な信用の失墜、本人への影響などのおそれなど）を低減し、個人情報を確実に保護するための安全対策活動を規定するものである。

２．適用範囲

（１）対象組織

全社（当社に勤務する社員、役員、準社員、契約社員、派遣社員、在宅勤務者、パートおよびアルバイトを含む）

（２）対象業務

全業務

（３）対象となる個人情報

自らの事業の用に供している個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述などによって特定の個人を識別できるもの（他の情報と容易に照合することができ、それによって特定の個人を識別することができることとなるものを含む。）。具体的には、「個人情報管理台帳」に定めた個人情報とする。

３．用語の定義

（１）従業員

当社に勤務する社員、準社員、契約社員、派遣社員、在宅勤務者、パートおよびアルバイトを含む。

（２）来館者

当社本社、支社および営業所等に出入りする当社従業員以外の者。お客様、協力会社等。

（３）事務所等

本社

（４）情報処理責任者

本細則を実施するにあたり、情報処理に関する安全対策を実施する責任者。

（５）部門個人情報管理者

各部門の個人情報の適切な取扱い、利用および管理について責任を持つ者。個人情報管理責任者より、業務の遂行に必要な権限を付与される。

Ⅱ．物理的アクセス管理

１．一般フロアへの入退室管理

（１）事務所への入退室の制限

①事務所への出入りは、当社役員、「Staff Pass」を携帯した従業員、「Guest Pass」を貸与された来館者及び在宅就業者、および当社社員の同伴による案内がある者のみに限定する。

（２）社員証の携帯および管理

①「Staff Pass」の管理は、個人情報管理責任が行う。

②個人情報管理責任者は、事務所への出入りが許可された当社従業員に、従業員番号の付与された「Staff　Pass」を貸与し、「Staff Pass 管理台帳」に記録する。但し在宅勤務者については、Staff Pass を付与する際、履歴書の写真等と照合し、受け取り手が本人であることを確実にする。

③当社従業員は、事務所等での勤務中、所属部署および氏名を識別できる「Staff Pass」を目に見える位置に携帯しなければならない。

④紛失等により、「Staff Pass」の再発行の依頼があった場合には、個人情報管理責任者は上記②の手続きを行う。

a)その際、従業員本人であることを確認するとともに、紛失状況等の詳細を確認し、二重貸与にならないことを確実にする。

b)紛失等した「Staff Pass」は無効とし、「Staff Pass 管理台帳」にその旨を記入する。

⑤従業員の退職または契約打ち切り等の場合には、「Staff Pass」の返却を求め、「Staff Pass 管理台帳」に返却日および理由を記入する。

⑥従業員間の「Staff Pass」の貸与および共有はしてはならない。

⑦Staff Pass を所有するものは事務所への入退室の際にタイムカードに記録し、毎月末に個人情報管理者もしくは個人情報管理者が任命した者がチェックする。

（３）「Guest Pass」の貸与及び管理

①「Guest Pass」の管理は、個人情報管理責任者が行う。

②来館者があった場合、個人情報管理責任者又は個人情報責任者が任命した者は来館者に対し、社名（学校名）、氏名、訪問先、訪問目的、時刻を「Guest Pass 管理台帳」へ記入するよう依頼する。ただし社名（学校名）、氏名、訪問先、訪問目的が明確な場合は、当社の従業員が代理記入してもよい。

又、滞在時間が短く、滞在範囲が限定されており、かつ滞在時間中つねに当社従業員が同伴する場合は、省略できる。

③個人情報管理責任者又は個人情報管理責任者が任命した者は、記入内容を確認した上で、来館者に「Guest Pass」を貸与する。

④来館者は、当社内での滞在時間中、貸与された「Guest Pass」を目に見える位置に携帯しなければならない。

④個人情報管理責任者又は個人情報管理責任者が任命した者は、来館者が事務所等を退出する際には、「Guest Pass」の返却確認を行ない、返却日時を「Guest Pass 管理台帳」に記録する。

⑤個人情報管理責任者又は個人情報管理責任者が任命した者は、毎月末、「Guest Pass」の現物と「Guest Pass 管理台帳」を照合する。現物の過不足等を発見した場合には、直ちに当該「Guest Pass」を特定し、個人情報管理責任者が、「Guest Pass」の捜索を依頼すると共に、業務上の問題が発生していないことを確認する。

a）問題が発生していた場合、社長に直ちに報告し、指示を受ける。

b）「Guest Pass」が見つからなかった場合、個人情報管理責任者の判断により、当該「Guest Pass」を無効とし、「Guest Pass」管理台帳にその旨記入する。

（４）協力会社社員の管理

①協力会社の従業員がフロアを共有する場合は、協力会社と当社との間で機密保持に関する合意の書面を取り交わす。

②フロアを共有するグループ会社の従業員は、協力会社名、所属部所および氏名がわかるものを携帯し、当社従業員と識別できるようにする。

（５）不審者の識別および対応

①「Staff Pass」、「Guest Pass」のいずれも携帯しておらず、当社社員の同伴もない者を見つけた場合には、当社従業員から必ず声をかけ、身元、訪問先、目的を確認する。

ａ）確認できた場合、個人情報管理責任者にて「Guest Pass」の発行手続きを求める。

ｂ）確認できなかった場合、訪問目的・氏名および連絡先を確認した上で、退出を求め、退出に応じない場合には直ちに警察に通報する。

（６）施錠の管理

①営業時間中、事務所の出入り口を施錠する鍵は、所定のキーボックスに保管する。同鍵は、個人情報管理責任者及び個人情報管理責任者が任命した者の許可無く利用してはならない。

②最後に事務所等を退出する社員は、事務所等を一周し不審者がいないことを確認したうえで、同鍵を用いて出入り口を施錠する。同鍵は、所定の場所に保管する。

（７）夜間・休日の入退室

①夜間・休日は、ビルの出入り口は施錠され、解錠は、社員に付与された鍵によってのみ可能とする。

②事務所内への入室に必要な鍵が保管されている場所は、個人情報管理責任者が必要に応じ許可した従業員のみ知ることができる。

２．情報処理室の管理

（１）情報処理室のセキュリティの為、次の各号の区域を定め、以下の許可者が許可した者のみ入室可能とする。

区域	許可者
情報処理室	情報処理責任者

（２）情報処理室への入室の制限

情報処理室の安全性を確保するため、以下の管理策を実施する。

①本社の作業場所から独立させること。

②施錠管理を行うこと。

③業務に不必要な物品を持ち込まないこと。

④入室許可を与えられた特定者以外が情報処理室に入室する場合、上記（１）の許可者が常に同伴すること。

（３）情報処理室の鍵の管理

①情報処理室の施錠用鍵は、上記（１）の許可者が管理する。

３．個人情報の媒体の取扱い

（１）個人情報の分類

①文書の機密性について以下のとおり分類する。

機　密：社内の特定者のみに開示可能な情報。外部から預かる個人情報を含む。
営業、契約、財務、商品開発関連情報は、原則、機密扱いとする。

社外秘：社員のみに開示可能な情報。社員の個人情報を含む。
機密情報のうち、部門個人情報管理者によって社内開示を認められたものは社外秘扱いとする。

一　般：公開を目的とした情報または開示されることにより当社に不利益をもたらさない情報。

（２）個人情報の媒体の取扱い

①紙媒体の取扱い

機　密：保管場所を特定し、持ち出しには保管場所の所轄部門の部門長の許可を必要とする。業務目的以外の複製は不可とする。
授受については授受を行う部門の部門長がルールを定め、必要に応じて文書化する。

社外秘：社外への持ち出しには保管場所の所轄部門の部門長の許可を必要とする。
授受については授受を行う部門の部門長がルールを定め、必要に応じて

文書化する。

一　般：特に定めない。

②電子媒体の取扱い

・電子媒体を保管する場合、上記３．（１）①の分類に従い、機密および社外秘のものは保管場所を定めて保管する。

・外部から預かる個人情報のうち、一覧またはデータベースに類する状態での電子媒体で授受する場合、パスワードの設定または暗号化を行う。

Ⅲ．論理的アクセス／ネットワーク管理

１．アクセス権限の管理

意図しない情報漏洩および誤操作による情報の破損等、トラブルを未然防止するため、アクセス権限について以下のとおり規定する。

（１）アクセス権限の管理者

①パソコンに関するアクセス権限の付与、抹消および変更は、個人情報管理責任者が「アクセス権限管理台帳」により管理する。

（２）アクセス権限の申請および付与

①アクセス権限の申請は、各部門責任者から、個人情報管理責任者に「アクセス権限申請書」を提出することで行う。その際、各部門責任者は、アクセス権限の利用についても責任を持つ。

②個人情報管理責任者は、申請内容を精査したうえで、アクセス権限を付与し、「アクセス権限管理台帳」に記録する

③付与されたアクセス権限については、他人との共有および許可無く変更を行ってはならない。

（３）アクセス権限の抹消

①部門所属者のアクセス権限が不要になった場合には、各部門責任者は、個人情報管理責任者に、遅滞なく抹消を申請する。申請は、「アクセス権限申請書」を提出することで行う。

②個人情報管理責任者は抹消手続きを行ない、「アクセス権限管理台帳」に記録する。

２．ＩＤおよびパスワード・スクリーンセーバーの管理

（１）個人情報管理責任者によるＩＤおよびパスワードの管理

①利用者から、ＩＤまたはパスワードの再発行の申請等があった場合には、本人であることおよび申請理由の確認を行なう。

②パスワードの発行にあたっては、容易に類推可能なパスワードを使用しないよう指導を行う。

（２）利用者によるＩＤおよびパスワードの管理

パソコンの利用者（以下、利用者）は、次のとおり、ＩＤおよびパスワードを個々の責任において管理する。

①パソコンの利用に関するＩＤが必要な場合には、Ⅲ１（２）に規定する手続により申請を行う。

②与えられたＩＤおよびパスワードについては、利用者自らが厳重な管理を行ない、以下を除くいかなる事情によっても他人に開示してはならない。

ａ）生命の危険および業務遂行に関する全社規模の重大問題を回避するために、必要な場合

ｂ）個人情報管理責任者が、システムのメンテナンスまたは利用者のＩＤ再発行等、業務遂行上の正当な理由によって要求する場合

③ＩＤおよびパスワードの機密性を保持するために、利用者は以下の事項を遵守する。

ａ）初期パスワードは必ず変更してから使用しなければならない。

ｂ）パスワードは６文字以上のものを使用する。その際、社員ＩＤ、誕生日、電話番号等、容易に推測可能なものは使用しない。

ｃ）パスワードは６ヶ月に一度の頻度で更新する。

ｄ）パスワードはメモや紙に記載してはならない。

ｅ）パスワードを入力する際、他人に見られないよう留意する。

④パスワードが何らかの理由で他者に漏洩した可能性がある場合、速やかにパスワードを変更するとともに、情報処理管理者に連絡し、指示を受ける。

（３）利用者によるスクリーンセーバーの管理

ａ）新規パソコン導入時は必ずスクリーンセーバーの設定を行う。

ｂ）業務の重要度において各自でスクリーンセーバーの起動時間を決定するが、最長３分までとする。

ｃ）離席する場合は画面が綴じているか、スクリーンセーバーが起動していることを確認してから離席する。

３．不正アクセスの防止対策

（１）個人情報管理責任者は、パソコンのネットワークの不正アクセスから防護するため、以下の事項を実施する。

①インターネット経由の通信情報は、ＶＰＮなどにより不正アクセスが出来ない設定とする。

②外部から社内ＬＡＮへの無許可のアクセスは不可とする。

③外部と接続する機器は、十分なアクセス制御機能を有したものを利用し、原則的に有線を利用する。無線 LAN を使用する場合は暗号化しＴＫＩＰ以上のセキュリティーを有したものを利用する。

④長期間利用しない機器は、ネットワークに接続しない。

⑤システムファイルまたはデータへのアクセス権限は、必要最小限の範囲とする。

⑥データの特性上必要な場合は、個人情報管理責任者と協議したうえで、個別に防止策を講ずる。

（２）個人情報管理責任者は、パソコンのネットワークの不正アクセスの早期発見につなげるため、以下の事項に努める。

①不正アクセスを発見するため、アクセス履歴を「個人情報管理実施細則　ＸＩ運用の確認」に基づき毎月分析し確認する。

②問題発生時および情報システム管理者が必要と判断したタイミングで、ソフトウェアおよびシステムファイルの改ざんが生じてないことを確認する。

Ⅳ．情報処理室及び事務所コンピュータの管理

１．コンピュータの物理的セキュリティ

（１）情報処理室の物理的セキュリティ

情報処理責任者は、作業区画において、次に定める物理的なセキュリティ対策を実施し、コンピュータおよびネットワーク機器関連の事故発生の可能性を低減する。

①誤って手を触れる等、不用意な操作ミスの発生の低減を考慮した措置。これにはコンピュータの施錠管理を含む。

②機器の落下や損傷の防止措置。

③耐震、耐火、耐水、避雷等の防災対策。システムおよび電源や空調設備等も併せて行う。

④無停電電源設備または電圧安定化設備による電源対策。

⑤ ケーブルは損傷や回線の盗聴を避けるため、埋設を原則とする。ただし、ケーブルの埋設が不可能である場合には、保護用のカバー等を使用する。

（２）情報処理室物理的セキュリティ

情報処理室のデータなどの一部を、社外の外注マシン室に設置する場合には、以下の事項を実施する。

①情報処理責任者は、外注マシン室を、次の基準を考慮して選定する。

ａ）厳重な入出制限がされており、入室の際は本人確認の仕組みを有すること。

ｂ）他の入室者が誤って手を触れる等、不用意な操作ミスの防止を考慮した措置が講じられていること。

ｃ）機器の落下や損傷の防止措置が講じられていること。

ｄ）耐震、耐火、耐水、避雷等の防災対策および電源対策が施されていること。

②上記①以外の詳細な安全対策については、外注マシン室の安全基準に従う。

③外注マシン室とは、安全対策に関する事項を含めた契約を締結する。

④当社従業員が外注マシン室へ入室する際は、情報処理管理責任者に事前の了解を得る。

２．データのバックアップおよびリストア

（１）バックアップの実施手順

情報処理管理責任者は、システム上のデータについて、バックアップの実施手順を以下のとおり明確にし、実施する。

①バックアップの頻度は、原則として３ヶ月に１回とする。

②バックアップの媒体は、MO・HD・ROM とする。

③バックアップ媒体は、銀行系の貸金庫に保管する。

④バックアップデータは、３世代前までの保管を行う。

（２）リストアの実施手順

情報システム管理者は、情報システム上のデータについて、リストアの実施手順を以下のとおり明確にし、実施する。

①リストア直前のデータをバックアップする。

②情報処理管理者の責任の下、リストアを実施する。

３．ウィルス等、悪質なソフトウェアからの防護

コンピュータウィルス等、悪質なソフトウェアおよびこれらを用いた攻撃からコンピュータネットワーク防護するために、次の事項を規定する。

（１）社内のコンピュータネットワークシステム

①当社内で使用するコンピュータネットワークシステムには、ウィルスチェッカ等を設置し、悪質なソフトウェアからの防護対策を行う。

②個人情報管理責任者は、ウィルスチェッカ等のバージョン更新情報の確認を適宜行う。

③個人情報管理責任者は、ウィルス情報について常に取得に努め、必要に応じて、各利用者に対策を指示する。

（２）外部から持ち込むコンピュータ

①顧客や協力会社等、外部から持ち込まれるコンピュータは、原則として、当社のネットワークへの接続を認めない。ただし、ウィルスチェッカ等悪質なソフトウェアからの防護対策が十分なされていると個人情報管理責任者又は情報処理責任者が認めた場合は、接続を許可することをさまたげない。

４．システムの設置および変更

コンピュータネットワークに関する設置、変更および撤去ならびに情報システムを管理するため、以下を規定する。

（１）情報システムの構成要素

本項で意図する情報システムとは以下のものを含む。

① パソコン（デスクトップおよびノート）

② 入出力装置（キーボード、マウス、スキャナ、ディスプレイ、プリンタ）

③ 媒体記録装置（ＦＤ、ＭＯ、ＣＤ－Ｒ、ＤＶＤ－Ｒ、外部メモリ等）

④ 外部記憶装置（外付けハードディスク等）

⑤ ＯＳ

⑥　アプリケーション（電子メールソフト／Ｗｅｂブラウザ含む）
⑦　ユーティリティソフト
⑧　ルータ、スイッチングハブ
⑨　その他、ネットワーク関連設備

（２）コンピュータおよびネットワークの設置・変更の管理

①コンピュータおよびネットワークの設置・変更および撤去作業は、以下の者（以下、作業者）が行う。

ａ）個人情報管理責任者又は情報処理責任者

ｂ）個人情報管理責任者又は情報処理責任者より権限を委譲された社員

ｃ）個人情報管理責任者又は情報処理責任者が承認の上、当社と契約を締結した外部委託先

②コンピュータおよびネットワークの設置・変更または撤去を行う場合、作業者は、「作業手順書」またはこれに替わるもの（チェックリスト等）を、個人情報管理責任者又は情報処理責任者に提出する。

③個人情報管理責任者又は情報処理責任者は、常に、コンピュータ及びネットワークの構成を把握し、作業を実施または指示する。

④個人情報管理責任者又は情報処理責任者以外の者は、当社のコンピュータ及びネットワークへの外部からの接続を、許可無く行ってはならない。

⑤コンピュータの撤去および廃棄を行う場合には、情報の消去等必要な対策を行う。

⑥作業終了後、個人情報管理責任者または権限を委譲された者は、変更の検証を実施し、変更点と動作を確認する。

⑦パソコンはワイヤーロック等、物理的な盗難対策を行なう。

５．パッチ等システムの更新（Windows Update 等）

個人情報管理責任者又情報処理責任者は、情報システムへのパッチ等の適用の要否を判断し、必要な更新を行うと共に、利用者に対する指示を行う。

６．外部公開サーバの管理とデータの更新

（１）定義

外部公開サーバとは、インターネットなどを使用して外部の者に情報を公開するサーバを指し、Ｗｅｂサーバ等を含む。契約に基づき特定企業と定型的に情報交換を行なうサーバについては、本項の対象とはしない。

（２）外部公開サーバの管理

外部公開サーバについては、サーバ管理者を明確にし、以下の管理を実施する。

①３．（１）および（２）に従い、不正アクセスの対策を講ずる。

②ぜい弱性攻撃など、外部からの攻撃に関する情報を適宜取得し、情報セキュリティ上の対策の改善を継続的に実施する。

③外部公開サーバのシステム設定などを更新可能な権限者は限定する。

④上記①、②、③を実施することが困難な場合および①、②、③を実施したとしても情報セキュリティ上の問題が残る場合は、遅滞なく個人情報管理責任者に報告する。

⑤外部公開サーバのメンテナンスまたは廃棄の際には、情報が漏えいしないよう、データ消去などの対策を行う。

（３）外部公開サーバに対する入力データの暗号化

採用や資料請求申込みなど、外部公開サーバで個人情報を取得する場合、サーバ管理者は、ＳＳＬ等の通信の暗号化を行うこと。

（４）外部公開サーバ上のデータの更新

外部公開サーバ上に情報を公開する場合または外部公開サーバ上に情報を保管する場合、以下の管理を実施する。

①外部公開サーバ上に情報を公開するために、データ更新を行うことができる権限者は限定する。また、作業履歴が特定できるよう外部公開サーバ用にアクセスするためのＩＤは個別に与える。

②外部公開サーバ上に情報を公開する場合、新規または更新情報の適切性を、更新者以外の者が確認する。

③外部公開サーバ上での情報の保管は、短時間に限るものとする。情報が一時的に外部公開サーバ上に置かれる場合であっても、速やかに情報を社内のサーバ等に移管し、外部公開サーバ上に長期間放置されないよう、システムの設計および運用を行なう。

Ｖ．コンピュータネットワークの利用

１．コンピュータネットワークの利用

（１）利用状況の監視

当社は情報セキュリティの実現のために、利用者に事前承諾を得ることなく、利用者の使用状況について監視を行ない、電磁的記録（ＨＤ、ＦＤ、ＭＯ等）を調査することができる。またこの調査結果に関して、以下の場合には利用者に事前承諾を得ることなく、利用者以外に開示する場合がある。

①公的機関から法的な強制力のある命令があったとき

②会社が関与する紛争を解決するために必要と判断したとき

（２）コンピュータネットワーク利用にあたっての遵守事項

①コンピュータネットワークは、利用を許可された者のみが操作可能とする。利用者は、来訪者など利用を許可されていない者が情報システムの利用を試みた場合に、これを許してはならない。

②コンピュータおよび記憶装置及び媒体は、許可無く外部に持ち出してはならない。

③コンピュータネットワークは原則、当社から貸与されたものを用い、個人所有のものおよび他社所有のもの等は持ち込まない。ただし、やむを得ない理由により、部門長が認めた場合は、この限りではない。

④個人情報を含むファイルは、指定のファイルに保管し、端末には、作業用の必要最小限かつ一時的なもの以外は保存してはならない。端末上の個人情報は、作業が終了次第、直ちにファイルを完全削除する。

（３）個人用端末の管理

①個人用端末は、原則、個人情報管理者又は情報処理責任者から貸与されたものを用い、プライベートなもの（個人所有のものなど）は持ち込まない。ただし、やむを得ない理由により、個人情報管理責任者が認めた場合は、この限りではない。

②個人情報を含むファイルは、セキュリティが確保されたファイルに保管し、個人用端末には、作業用の必要最小限かつ一時的なもの以外は保存してはならない。個人端末上の個人情報は、作業が終了次第、直ちにファイルを完全削除する。

（４）個人用端末の持ち出し

①個人用端末の持ち出しは、個人情報管理責任者が認定した端末のみとする。

②個人情報管理責任者が持ち出しを許可した個人用端末は、パスワードによる厳重なアクセス制限を施す。原則、外付け用の機器は接続しない。

③個人用端末を社外に持ち出す際は、利用者は「ＰＣ持ち出し管理台帳」を記入し、端末の所在を明らかにする。

④持ち出しを許可したノートパソコンには、個人情報は保存しない。ただし、個人情報又は情報処理責任者が、やむをえない事由と認めた場合には、暗号化されたデータ領域を設置し、その領域を用いることで許可する。

⑤持ち出したノートＰＣは可能な限り携帯し、自らの監視の元におく。

２．電子メールの利用

（１）コンピュータネットワーク利用者は電子メールの利用に際して、次の事項を遵守しなければならない。

①電子メールは秘匿性がないことに留意する。機密性を要する情報については、可能な限り電子メール以外の伝達手段を使用する。やむを得ず電子メールを利用する場合には、パスワードの設定又は暗号化しなければならない。

②外部にファイルを添付して電子メールを送信する際には、システム上でファイルについてウィルスチェックを実施してから送信する。

③電子メールは、業務利用を目的とする。私的利用は、業務に影響を及ぼさない程度であれば許容するが、この場合であっても本項に反してはならない。電子メールの内容について、社員のプライバシーは保護されない。

④ウィルスの疑いがあるメールを受信した場合、添付ファイルを開封もしくは保存等操作をしてはならない。直ちに個人情報管理責任者に連絡する。

⑤電子メールソフトについては、当社で指定したものを使用し、許可無く設定を変更してはならない。

⑥電子メールの利用者は、自己の責においてメールアドレス（ＩＤ）とパスワードを管理する。

３．Ｗｅｂ（ホームページ）等の利用

（１）コンピュータネットワークの利用者は、Ｗｅｂ（ホームページ）等の利用に際して、次の事項を遵守する。

①インターネット上のサイトへのアクセスに関しては、業務目的以外の利用を禁ずる。

②Ｗｅｂブラウザについては、当社標準のものを使用する。

③ファイルのダウンロードを行う場合、ダウンロードしたファイルはウィルスチェックしてから使用する。

④フリーメール等、インターネット上のＷｅｂサーバを利用した電子メールの利用

は許可無く行ってはならない。

⑤社内外のＷｅｂサーバおよび関連機器等について、攻撃等不正なアクセスを行ってはならない。またこうした目的のために社内外のシステムを利用してはならない。

４．障害発生時の対応

（１）ウィルス感染の可能性がある場合

①ウィルス感染によりシステムに不具合が発生していると想定される場合、ただちにネットワークケーブルを取り外すなどにより、端末機をネットワークから物理的に切り離す。

②ネットワークに接続されていない状態でウィルスチェッカを作動させる。

③個人情報管理責任者に直ちに状況を報告し、指示に従う。

（２）その他、物理的障害などの場合

①個人情報責任者に速やかに状況を報告し、指示に従う。

②外部への修理の依頼等は、情報漏えいの危険がありうるため、個人情報管理責任者の許可なしに行ってはならない。

Ⅵ　リスク対策

１．運用におけるリスク対策

①営業ファイルはナンバリングし施錠管理を行う

②名刺等は営業上収集した個人情報は帰社後直ちに所定のファイルに保管し施錠管理を行う。

③ 個人情報を含むデータをパソコンに入力した場合は、パスワードをかけたうえで所定のＨＤファイルに保存する。パソコンは、セキュリテーワイヤーで施錠する。

④ 各パソコン利用者は、セキュリティーソフトの更新切れに留意し、ウイルスの侵入やネットワークからの漏洩に常に注意をはらう。

⑤ 新規の顧客･新規雇用従業員･新規在宅者･新規協力会社などが発生した場合は、機密保持契約を終結するまで取引・雇用してはならない。

⑥ 学校ファイル一覧とファイルは毎月１回営業会議時にチェックし紛失や盗難がないか確認する。業務終了時は施錠管理を行う。

⑦ 運転中の事故による個人情報の紛失・盗難を防ぐ為、営業車両は常に整備点検を行い運転者は安全運転・事故防衛運転に努める

⑧ 紛失･逸失リスクを避ける為委託先から入力原簿を預かる時は原本を預からず複製を預かる。又社内での入力原簿等個人情報の複写を禁ずる。

但し業務上必要がある場合には必要最低限に絞り込み個人情報責任者がその作

業を行う。

⑨ 原則的に電子メールでの個人情報の受渡しを禁止する。
但しやむおえない場合には、パスワード及び暗号化しネットワーク上の漏洩を防ぐ

⑩ 預託された個人情報漏洩を防ぐため、バックアップを除き情報処理分室以外にマスターデータを置かない。

⑪ ハッカー対策としてマスターデータが保管されているコンピュータは、ネットワークにつなげることを禁止する。

⑫ マスターデータは厳重なセキュリティー対策を講ずる。

⑬ 宅急便会社での紛失漏洩を防ぐため、宅急便での受渡し内容の確認は都度行い毎月末に、すべての宅配伝票を監査する。

⑭ 個人情報を含む媒体（紙・電子・その他）の受渡しは必ず授受時に数量確認を行い授受記録、送付記録、受取記録を保管する。

⑮ 往復はがきの発送などを受託した場合には、できるかぎりプライバシーシールと併せて発送するように、委託者に勧める。

⑯ 個人情報を含むファックスを受け取る場合は、紙媒体で出力せず画面で確認する。

⑰ 毎月　キャビネット内容物を各キャビネットの在庫表に基づきチェックを行い、紛失・持ち出し新規在庫を管理する。

⑱ 情報処理室などの他部門及び協力会社との個人情報を含む媒体をやりとりする際、送付記録や受取記録などを送付記録・受取記録・宅急便伝票・納品書などの紙媒体もしくは電話で内容物の受渡し確認を行う。

⑲ 名簿印刷等、個人情報を含む業務を委託する場合には「名簿印刷管理監督書」を用いて個人情報管理を徹底する。

⑳ 事務所からの最終退出時（業務終了時）に最終退出者は「最終退室チェックリスト」を用いて施錠を確認する。

21　個人情報を含む媒体（紙、電子機器）を廃棄する場合は、必ず焼却又は、シュレッダーを掛けてから廃棄する。電子機器の場合は、必ず完全消去を行う。

a　データ移送時は媒体を鍵付の耐火性のある強固な鞄に入れ 2 名以上で移送する。

b　名簿等の個人情報が従業者による不正持ち出し及び不正に第三者に提供されることを防止するために、従業者に不振な行動が認められた場合や管理者が必要だと判断した場合においては、手荷物等のチェックを行う。

Ⅶ　在宅者の管理

（1）在宅者への発注は封入作業を主とし、採用及び業務の発注においては、以下の条件を満たしているものとする。

①秘密保持に関する誓約書を提出できること。

②犯罪歴が無いこと。

③業務遂行できる健康状態であること。

④本社より５Km 以内に２人以上で在住しており、住居は自己所有もしくは５年以上住んでいること。

⑤常時連絡が取れる環境であること。

⑥受注及び納品に本人又は家族が本社へ運搬できること。

⑦担当者の特別な指示が無い限り、発注より中４日以内に納品すること。

⑧在宅者は会社で指示した教育を受けること。

（２）発注においては、発注数量と納品数量の確認を『在宅発注書』にて行う。

（３）上記の（１）・（２）の規定外での採用及び発注の必要がある場合は個人情報管理責任者の承認を得なければならない。