文書番号	SPMS03	版数	第１版
文書名	安全管理規程		
作成	年　月　日	（特定） 個人情報保護管理者	印
承認	年　月　日	代表取締役	印

改定履歴

版数	改定年月日	改定内容	作成	承認
第 1 版	/ /	新規制定	（特定）個人情報 保護管理者	代表取締役

第１章　入退館管理

第 1-1 条（建物の解錠、施錠）

事業所施設入口扉の鍵を施錠／解錠できる者は、安全管理責任者が必要と認めた者のみとする。

２　安全管理責任者は必要と認めた者に対し事業所施設入口扉の鍵を交付する。

３　事業所施設入口扉の鍵は、SPMS 記録 18「鍵管理台帳」で管理し、SPMS パトロール時に保持状況を確認する。

４　事業所施設入口扉の鍵を持つ者で、その日の最初の入館者、並びにその日の最後の退館者は、SPMS 記録 19「入退館記録表」に氏名と時刻を記載する。

最終退館者は、退館時に安全状況を確認し、退館時チェックリスト欄にチェックを行う。

第 1-2 条（入退館管理）

事業所施設入口には、来訪を知らせるための内線電話を設置し、入退館管理を行う。

第 1-3 条（訪問者の入退館手続き）

訪問者の入館に際し、受付応対をした従業者は、訪問者から用件を申し受け、SPMS 記録 20「訪問票」に必要事項を記載してもらう。「訪問票」への記載は、従業者が代筆してもよい。

２　訪問者の退館に際し従業者は、訪問者から SPMS 記録 20「訪問票」の返却を受ける。その際、退館時刻が記載されていることを確認すること。

第２章　入退館記録の確認と保管

第 2-1 条（訪問者の入退館記録の確認と保管）

安全管理責任者は、SPMS 記録 20「訪問票」を SPMS 運用点検時毎に確認し、異常がないか点検する。

なお、点検終了後、２年間保管する。

第 2-2 条（解錠・施錠記録の確認と保管）

安全管理責任者は、SPMS 記録 19「入退館記録表」の内容を SPMS パトロール時毎に確認し、異常がないか点検する。なお、点検終了後、２年間保管する。

第３章　区画の区分

第 3-1 条（事務所施設内のセキュリティ区画の区分）

事業所施設内の区画は、その領域の使用目的、物理的条件によって、次の３種類のいずれかに区分する。

（１）共用区画：

訪問者の入室を許す区画。例えば、応接室（会議室）、トイレなど。

（２）業務区画（取扱区域）:

従業者が業務を行っている区画。訪問者のアクセスは、特別な理由がない限り許さない。（例）執務オフィス。

（３）セキュリティ区画（管理区域）:

重要機器、機密情報などが置かれており、限定された者以外のアクセスを許さない区画。特定個人情報ファイルを取り扱う情報システムもここで管理する。

この区域は、専用の部屋又はパーテーションなどで間仕切りを行い、扉には履歴の取れる入退管理システムを設置する。

なお、間切りをした部屋が存在しないうえ、重要機器、機密情報等を管理しているサーバ、保管庫・キャビネット・金庫などがない場合には、セキュリティ区画を用意する必要はない。

安全管理責任者は、各区画とその区分を SPMS 記録 21「オフィス図面」に記録し管理する。

２　安全管理責任者は、区画およびその区分に変更があったときは、速やかに SPMS 記録 21「オフィス図面」を更新する。

第４章　共用区画の入退室管理

第 4-1 条（共用区画の入退室管理）

従業者は、共用区画への入退室は自由とする。

２　訪問者との応対は、原則的に共用区画において行う。その際、必ず従業者が同行すること。

第５章　業務区画の入退室管理

第 5-1 条（業務区画の入退室管理）

従業者は、業務区画への入退室は自由とする。

２　訪問者は、原則として、業務区画へは入室できない。

訪問者が業務区画へ入室する必要が発生した場合には、応対者は安全管理責任者の許可を得て入室させ、業務区画内では応対者が必ず同行すること。

第６章　情報機器の安全管理

第 6-1 条（サーバルームなどに設置する情報機器）

重要な情報機器（サーバ、通信制御装置、ファイアウォールなど）は、その他の情報機器（PC、プリンタなど）と区別して、履歴の取れる入退室管理システムが設置されたセキュリティ区画（管理区域）又はサーバラック内等に設置すること。

第 6-2 条（サーバルームなどに設置する情報機器の信頼性・安全性確保）

セキュリティ区画（管理区域）並びにサーバラック内に設置する情報機器については、次のような信頼性・安全性を確保する措置を講ずること。

（１）必要に応じて耐震措置・免震措置を講じる。

（２）必要に応じて機器の二重化を行い、耐障害措置を講じる。

（３）停電および電源の異常から保護するため、無停電電源装置などを設置する。

第 6-3 条（サーバルームなどの外に設置する情報機器の安全性確保）

セキュリティ区画（管理区域）並びにサーバラック外に設置する情報機器については、次のような信頼性・安全性を確保する措置を講ずることが望ましい。

（１）落下、盗難、浸水、不要なアクセスから守られる場所に設置すること。

（２）電源は、簡単に抜けないもの、例えばロック式コンセントを使用すること。

（３）機器およびその周辺の整理整頓を行うこと（各種ケーブル、説明書など）。

（４）年１回の社内大掃除の日に機器およびその周辺の掃除を行うこと。

第 6-4 条（従業者による PC の管理）

従業者は、業務で使用する PC の安全性確保に努めなければならない。

２　従業者は、長時間離席するとき、PC の画面を第三者に見られないよう、次のいずれかの措置を講じる。

（１）PC をシャットダウンする。

（２）アプリケーションあるいはネットワークからログオフする。

（３）パスワード付のスクリーンセーバを手動で起動させる。

（４）一定時間（15 分以内）パソコンをアイドル状態にした場合、自動的にパスワード付スクリーンセーバに切り替わるように設定をする。

３　ノート型 PC を使用している従業者は、帰宅時あるいは長時間外出時などには、パソコンの電源をオフにし、ノート型 PC を次のようなセキュリティの確保された状態に置くこと。

（１）施錠できる机の引出し、キャスター付キャビネット、共有保管庫・キャビネット等に収納する。

（２）机上に置いたままにする場合には、チェーンロックを使用し机にくくり付ける。

第 6-５条（情報機器の社外持出し）

ノート PC を社外に持ち出す必要が発生した場合には、従業者は、所属する部門の（特定）個人情報保護部門管理者の許可を受けなければならない。

２　従業者は、許可を得て社外に持ち出すパソコンに対し、次のような措置を講じる。

（１）BIOS パスワードの設定。

（２）個人情報、マイナンバー（個人番号）、特定個人情報（以下、「個人番号等」を呼ぶ）を入れない、入れる場合には暗号化措置を講じる。

（３）ファイルパスワードの設定。

（４）PC を必ず身辺に置き、紛失・盗難を防止すること。

第７章　アクセス管理

第 7-1 条（アクセス権限の付与）

（特定）個人情報保護部門管理者は、情報システムにアクセスし個人情報等を使用する必要のある従業者に、アクセス権限を与える。その際、従業者の職務内容から判断してアクセスすることが必要な範

囲のアクセス権限を与える。

第 7-2 条（ユーザ ID の登録）

アクセス権限は、ユーザ ID を情報システムに登録することで制御する。（特定）個人情報保護部門管理者は、SPMS 記録 23「ユーザ ID 管理表」に必要事項を記入し、安全管理責任者に申請する。

2　安全管理責任者は、SPMS 記録 23「ユーザ ID 管理表」の内容を確認し、ユーザ ID の登録を行う。

3　登録作業が完了した後、安全管理責任者は、ユーザ ID と仮設定したパスワードを、当該従業者に通知する。

第 7-3 条（アクセス権限の変更）

アクセス権限を持っている者のアクセス権限が変更になった場合、(特定)個人情報保護部門管理者は、当該従業者の SPMS 記録 23「ユーザ ID 管理表」に必要事項を記入して、安全管理責任者に申請する。

第 7-4 条（アクセス権限の登録抹消）

アクセス権限を持っている者のアクセス権限が取り消された場合、(特定）個人情報保護部門管理者は当該従業者に関する SPMS 記録 23「ユーザ ID 管理表」に必要事項を記し、安全管理責任者に申請する。

2　安全管理責任者は、SPMS 記録 23「ユーザ ID 管理表」の内容を確認し、当該ユーザ ID の登録抹消を行う。

3　安全管理責任者は、ユーザ ID の登録抹消が正しく行われたことを確認した後、SPMS 記録 23「ユーザ ID 管理表」の「ユーザ ID 登録抹消」欄にその旨を記入し、作業が完了した旨を（特定）個人情報保護部門管理者へ通知する。

第 7-5（アドミニストレータ権限）

システムを管理・保守するために必要な特別な作業は、安全管理責任者または、限定された作業担当者が実施する。

また安全管理責任者は、その作業の実施に必要な特別の権限をもったアドミニストレータ権限を作業担当者に付与する。

この際、アドミニストレータ権限は最低限必要な者に必要な期間だけ付与し、安全管理責任者は、当該作業担当者の作業内容を厳格に管理する。

第 7-6 条（仮設定パスワードの変更）

従業者は、安全管理責任者からユーザ ID と仮設定パスワードの通知を受けた後、速やかに、仮設定パスワードを自分だけが知りうるパスワードに変更すること。

第 7-7 条（パスワードの設定ルール）

パスワードの漏えい防止のために、従業者は、次のルールに従ってパスワードを設定すること。

・英数字混在で 6 桁以上とする。

・社員番号、誕生日、電話番号、郵便番号、氏名などの第三者から類推しやすいパスワードは設定しない。

第 7-8 条（パスワードの機密性管理）

パスワードの機密性を守るために、利用者は、次の事項を遵守すること。

・パスワードを第三者に教えない。

・パスワードをメモし人目に触れるところに置かない。

・最低でも３カ月に１度は、パスワードを変更する。

第 7-9 条（パスワードの再発行）

従業者がパスワードを忘れてしまった場合には、(特定）個人情報保護部門管理者の承認を受けたうえで、安全管理責任者に報告すること。

2　安全管理責任者は、指定されたユーザ ID に対して新たに初期パスワードを設定し、申請者に通知する。

第 7-10 条（アクセスログの取得）

安全管理責任者は、業務システムごとにアクセスログを取得するよう検討しなければならない。アクセスログには、アクセス開始時刻、ユーザ ID、アクセス対象ファイル、アクセス内容（参照、更新、削除など)、アクセス終了時刻などが記録されることが望まれる。

2　取得したアクセスログは１年間保管する。

第 7-11 条（アクセスログの分析）

安全管理責任者は、SPMS パトロール確認時に、アクセスログを点検・分析し、不審な動きが見られた場合には、その都度、対策を講じなければならない。

第８章　ネットワーク管理

第 8-1 条（ネットワーク構成図）

安全管理責任者は、当社のネットワーク構成を SPMS 記録 24「ネットワーク図」に記録し、最新の状態に維持・管理する。

第 8-2 条（ファイアウォールの選定と設置）

社内ネットワークとインターネットとの間には、ファイアウォールまたは UTM を設置し、外部からの不正アクセスを防御しなければならない。ただし、ファイアウォールを設置できない場合には、最低でもルータのファイアウォール機能を ON にすること。
2　安全管理責任者は、不正アクセスに対する防御の強度を選定基準の第一として、ファイアウォールや UTM を選定すること。
3　安全管理責任者は、設置したファイアウォール（UTM）に対して、不正アクセスを防止するためのフィルタリング設定を必ず行うこと。

第９章　コンピュータウイルス対策

第 9-1 条（アンチウイルスソフトの導入）
当社は、情報システムを構成するすべてのサーバおよび PC にアンチウイルスソフトを導入する。
2　導入するアンチウイルスソフトは、以下の要件が満たされていることを条件に、安全管理責任者が選定する。
（1）最新のパターンファイル、セキュリティパッチのタイムリーな更新。
（2）常時ウイルススキャン機能（ファイル、電子メールの添付ファイルなどのスキャン）。
（3）ベンダがウイルスに関する豊富な情報を提供している。
（4）アンチウイルスソフトの適切なバージョンアップが行われている。
3　すべてのサーバおよび PC に選定したアンチウイルスソフトを必ずインストールし、従業者は他のアンチウイルスソフトを勝手にインストールしてはならない。
4　特に、Winny や Share などのファイル交換ソフトのウイルス感染により、個人情報等の流出が相次いでいることから、ファイル交換ソフトは、会社 PC で使用してはならない。
5　個人情報等を取り扱うデータベースを構築する際は、SQL インジェクションなどの不正アクセス・不正個人情報等取得技術などの対策を必ず行うこと。
6　個人情報等を取得するための入力フィールドをホームページ上に作成する場合には、クロスサイトスクリプティング対策を必ず行うこと。
7　個人情報等を入力する Web 画面から個人情報等を取得する際は、SSL 通信を導入し暗号化対策を実施すること。

第 9-2 条（アンチウイルスソフトの設定）
安全管理責任者は、パターンファイル、セキュリティパッチの更新および常時ウイルススキャン機能が正しく動作するように、アンチウイルスソフトの設定を定め、各部門並びに各従業者への周知を図る。
2　各部門の（特定）個人情報保護部門管理者は、安全管理責任者が定めた設定に従って、部門のサーバおよび従業者が使用する PC のアンチウイルスソフトの設定を行う。
3　従業者は、自分が使用する PC のアンチウイルスソフトの設定を、勝手に変更してはならない。

第 9-3 条（アンチウイルスソフトの利用）
従業者は、アンチウイルスソフトの常時スキャン機能を、作動している途中で終了させてはならない。
2　従業者は、当社外から持ち込んだノート PC などの情報機器、並びに CD-R、USB メモリなどの記録媒体を会社の PC で使用する場合には、必ず事前にアンチウイルスソフトを利用してウイルススキャンを行わなければならない。

第 9-4 条（メール送受信時の留意事項）
ウイルスは電子メールの添付ファイルとして社内に侵入するケースが最も多いので、電子メール受信時には、アンチウイルスソフトの常時ウイルススキャン機能によって、自動的にウイルスチェックを行うよう設定しなければならない。
2　従業者は、電子メールを利用している最中にウイルスに感染したと感じた場合には、速やかに安全管理責任者に報告を行い、対応についての指示を受けること。
3　従業者は、送信元不明の電子メールおよびその添付ファイルに対しては、操作を加えずに削除するか、安全管理責任者へ報告を行い、対応についての指示を受けること。

第 9-5 条（ウイルス感染時の報告）
従業者は、次のようなウイルス感染の可能性が考えられる現象があった場合には、パソコンの利用を中止し、速やかに（特定）個人情報保護部門管理者に連絡し、協力して対応を行うこと。
（1）業務システムやワード、エクセルソフトなどが頻繁にハングアップする。パソコンが起動しない。
（2）ファイルがなくなっている。見知らぬファイルが作成されている。
（3）PC のデスクトップに不審なアイコンができている。
（4）パソコン利用者の意図に関係なく、インターネットに接続しようとする。
（5）パソコン利用者の意図しないメールの送信が行われる。
（6）パソコンの動作がいつもと違うと感じる。
2　（特定）個人情報保護部門管理者は、安全管理責任者に報告し対応を協議する。

第 9-6 条（ウイルス感染状況の確認）

ウイルス感染の報告を受けた安全管理責任者は、報告元の（特定）個人情報保護部門管理者と協力して、ウイルス感染の状況について、以下の点を確認すること。

（１）ウイルス検知の状況。

（２）ウイルスの種類、特徴。

（３）被害状況、他への二次感染の有無。

（４）ウイルス感染が発見されたファイル名。

（５）そのファイルが発見された場所（受信した電子メールの添付ファイル、CD-R 内のファイルなど）。

（６）使用機種、OS の種類。

２　安全管理責任者は、状況によりベンダとも連絡をとり、早急に状況を確認すること。

第 9-7 条（ウイルス感染の記録）

安全管理責任者は、ウイルス感染の状況を SPMS 記録 09「事件事故報告書」に記録する。

第 9-8 条（ウイルス被害拡大の防止）

安全管理責任者は、ウイルス感染の状況に応じて、ウイルス被害の拡大を防止するために次の事柄を参考に、必要な措置を速やかに講じること。

（１）ウイルスに感染したと思われるサーバおよび PC を、社内ネットワークから切り離す。

（２）ウイルス感染が発生したこと、感染時の状況、対処方法などを、関係する部署に連絡する。

（３）社外にもウイルス被害が及んだ可能性がある場合には、個人情報等を提供した本人や当社の取引先等に対して上記（２）と同様の内容を連絡する。

第 9-9 条（ウイルスの駆除および被害の復旧）

安全管理責任者は、ウイルスを駆除し、システムを正常な状態に復旧させるために、次の事柄を参考に、必要な措置を速やかに講じること。

（１）アンチウイルスソフトを利用して、ウイルス感染したサーバや PC のウイルスを駆除する。

（２）ウイルス感染したファイルやプログラムを削除し又はディスクフォーマットを行い、バックアップ媒体から復旧作業を行う。

（３）ウイルス感染した CD-R などの媒体を粉砕・廃棄処分する。

２　第 9-8 条（１）でサーバおよび PC を社内ネットワークから切り離した場合、上記のウイルス駆除および被害復旧措置が完了するまで、社内ネットワークに再接続してはならない。

３　ウイルス駆除および被害復旧措置が完了した後、安全管理責任者は、その旨を第 9-8 条（２）で連絡した社内関係部署および第 9-8 条（３）で連絡した社外関係先に連絡する。

第 9-10 条（再発防止への取組み）

ウイルス感染の再発を防止するために、安全管理責任者は、ウイルス感染経路の特定、ウイルス感染に至った根本原因（技術的原因、運用面での原因など）を究明し、再発防止策を策定すること。

第 9-11 条（ウイルス対応完了の記録）

安全管理責任者は、ウイルス駆除および被害復旧措置が完了した後、ウイルス感染発生時に起票した SPMS 記録 09「事件事故報告書」に被害状況の詳細、実施した措置、根本原因と再発防止策、対応完了日などを記録する。

第 9-12 条（ウイルス対応の報告）

安全管理責任者は、ウイルスの発生から対応が完了するまでの状況について、（特定）個人情報保護管理者に報告する。報告は SPMS 記録 09「事件事故報告書」をもって行う。

２　安全管理責任者は、ウイルス感染によって被害を被った場合、経済産業省より指定されている独立行政法人情報処理推進機構（IPA）に報告する。報告様式は IPA 指定の様式を、IPA のホームページからダウンロードして使用する。

第１０章　データバックアップ

第 10-1 条（目的）

個人情報等に係る事故が発生し、個人情報等の漏えい、滅失、き損などが発生した場合に備え、個人情報等を速やかに復元させるために、個人情報等を管理・記録されているデータベースやハードディスク等について、定期的にバックアップを取得する。

第 10-2 条（バックアップ仕様の設定）

安全管理責任者は、システム障害などによって個人情報等が記録されているデータベースやハードディスク等が被害を受けた場合に備え、業務システムの重要度及び取り扱っている個人情報等の機密度等を考慮しながら個人情報等のバックアップ仕様を検討する。

２　バックアップ仕様としては、バックアップを取得する頻度、バックアップの実施手順（システムによる自動バックアップ、手動など）、バックアップを取得する媒体、バックアップデータの保管方法、バックアップデータの保管期間などを設定する。

第 10-3 条（バックアップの取得）

安全管理責任者は、別途定めた社内バックアップ規定に則り、データのバックアップを取得する。

第 10-4 条（バックアップ媒体の保管）

安全管理責任者は、バックアップを取得した記録媒体を、バックアップ仕様に従って保管する。

2　バックアップ媒体は、元の個人情報等と同等の機密度で保管する。

3　バックアップデータの保管場所は、元のデータがある場所（サーバなど）の近くは避け、距離を置いたセキュリティの確保された場所（施錠できる共有保管庫・キャビネット、耐火金庫など）に保管する。機密度の高いデータについては、外部倉庫業者などへの委託保管も検討すること。

第 10-5 条（バックアップデータによる復旧テスト）

安全管理責任者は、取得・保管されているバックアップデータが再利用可能であるかどうかについて、定期的に確認を行うこと。

第１１章　個人情報等の送信管理（メール・ファックス等）

第 11-1 条（送信者の限定）

（特定）個人情報保護部門管理者は、職務内容に基づいて、個人情報**等**の送信（メール・ファックス等）ができる者を限定し、権限を与える。

第 11-2 条（送受信記録）

権限を与えられた者は、個人情報等の送信（メール・ファックス等）を行った場合、SPMS 記録 25「個人情報等授受記録表」に記録する。

2　送信を行った後は、電話等を利用して、受信者が、個人情報等が添付されたメールやファックスを確実に受信したことを確認し、SPMS 記録 25「個人情報等授受記録表」に受信記録を記載する。

3　SPMS 記録 25「個人情報等授受記録表」は２年間保管する。

第 11-3 条（送信時のセキュリティ対策）

個人情報等をメールやファックス等で送信する場合には、次のようなセキュリティが確保される対策を講じること。

（１）　個人情報等が記載されたファイルをメールに添付して送信する場合には、ファイルをパスワード付き圧縮またはパスワードロックで保護すること。

（２）　メールを送信する際は、メールアドレスに間違いがないか２度以上確認を行った後、送信すること。

（３）　個人情報等が記載されている書類をファックスで送信する場合には、送信先のファックス番号をファックス機の短縮ボタンに予め登録すること。

（４）　ファックス機の短縮ボタン登録を行った場合には、登録番号に間違いがないか登録時に２人以上で確認すること。

（５）　ファックス番号を直接入力して送信する場合には、ファックス番号に間違いがないか送信者（１名）が２回確認した後、送信を行う。

第12章　その他全般事項

第 12-1 条（書類の送付）

個人情報等が記載された書類を送付する際は、書留、簡易書留、配達記録郵便、郵パック、宅急便など安全性の高いものを利用し、確実に相手方に届くようにする（配達記録のあるものを利用する）こと。

2　送付先の住所・氏名などに間違いがないか送付前に2人以上で確認すること。

3　個人情報等を送付した後は、電話等を利用して、受信者が確実に受領したことを確認すること。その際、SPMS 記録 25「個人情報等授受記録表」に受領記録を記載する。

4　誤送信したことに気が付いた場合には、SPMS02「（特定）個人情報保護基本規程 3.3.7　緊急事態への準備」に従って対応すること。

第 12-2 条（自席デスクにおける飲食について）

個人情報等が記載された重要書類を自席デスク上で取り扱うときは、飲食を行わないこと。

2　自席デスク上で飲食を行う際は、クリアデスクにすること。

第 12-3条（書類の管理について）

個人情報等などが記載された重要書類については、来客者に見られないよう保管管理を徹底すること。

2　離席する際は、重要書類を自席キャビネットに格納すること。但し、外出の際は、自席キャビネットを施錠しなければならない。

3　重要書類を自席デスク上で取り扱う際は、他の書類を一度自席キャビネットへ格納しクリアデスクにすること。これは処理の混同を避ける目的がある。

4　机の上はもちろんのこと、机の下や書棚との隙間、キャビネットの上、複合機周辺、ファックス周辺などに個人情報等が記載された書類を放置してはならない。

第 12-4条（鍵管理について）

オフィス内の保管庫、キャビネット、金庫、戸、扉などの鍵は、SPMS 記録 18「鍵管理台帳」を作成し、鍵の管理を徹底しなければならない。

第 12 –5 条（外出前の確認について）

外出する際は、持ち出す必要のない個人情報等が記載・記録された書類や記録媒体がかばんの中に入っていないか確認をすること。

第 12 –6 条（裏紙の取扱いについて）

個人情報等が記載された紙書類は、その裏面をプリンタ用紙、コピー用紙、メモ用紙などに再利用せず、必ずシュレッダー処分すること。

第 12-7条（PC内のデータ管理について）

PC内に電子データ（ファイル）を保存する場合には、電子データを紛失したり誤って消去したりしないよう、管理に最適なフォルダ構成を考案し保存すること。またフォルダの全体構成が電子データの管理に適しているかについて、定期的に見直すこと。

第 12-8 条（社外での書類の扱いについて）

必要な場所以外では、個人情報等などが記載された重要書類を、かばんの中から取り出してはならない。

2 個人情報等が記載された書類や記録されたノートパソコン・記録メディアなどを持ち歩く（徒歩、電車、タクシー、トイレなど）場合には、置き忘れ、置き引き、窃盗、強盗、引ったくり、車上荒らしなどに十分注意をはらうこと。

第 12-9条（火災発生時の対応マニュアル）

オフィス内ならびに自社建物周辺にて火災を発見した者は、直ちに全従業者へ大声で報告し、非難を促す。

2 避難の際、各部署にてあらかじめ選定された最重要個人情報等を持ち出せるか瞬時に判断をおこなうこと。

3 あらかじめ選定された最重要個人情報等とは、CD-R などに保存されたバックアップ媒体であり、これが焼失することにより、事業の継続に大きな影響を与える価値のあるものである。

4 消防への通報、初期消火活動の対応については、別途「火災発生時避難マニュアル」などを参照にすること。

5 火災発生により、万が一、取引先から預託された個人情報等を焼失してしまった場合には、SPMS02「（特定）個人情報保護実務規程 3.3.7 緊急事態への準備」に従って対応すること。

第 12-10条（レンタル・リース品返却、PC、サーバ処分時の注意）

パソコンやサーバ、プリンタや複合機、レンタル・リース品の返却、処分の際は、それら機器の記憶メモリに記録されている個人情報等を含むデータが、完全に消去されるよう業者に消去依頼を行うか、専用のソフトウェアを利用すること。

第 12-11 条（個人情報等の預託について）

個人情報等の処理ならびに保管管理業務を受託する場合には、当社内において預託された個人情報等が滅失することを鑑みて、預託を受ける個人情報等と同じ内容のものを委託元にも保管してもらうよう要請すること。

第 12-12 条（テストデータ使用制限について）

個人情報等を処理するためのソフトウェアを開発する際は、本物の個人情報等を利用して、テスト評価を実施してはならない。テスト評価を実施する際はダミーの個人情報等を作成し、実施すること。

第 12-13 条（誤入力チェックについて）

個人情報等をパソコンやサーバ上のソフトウェアデータベースに入力する際は、ソフトウェアシステムによる自動誤入力検出プログラムを導入するとともに、入力作業の終了時に目視確認を行い、二重チェックを行うこと。

第 12-14 条（廃棄処分について）

個人情報等が記載された書類は、必ずシュレッダー処分を行うこと。CD、DVDなどのメディア媒体については、メディアシュレッダーもしくは、破壊を原則とする。ハードディスクの廃棄に際しては、初期化するだけでなく、内容を再読することが不可能な方法を取るために、専用のソフトウェアによって上書き消去しなければならない。

第 12-15 条 （書類を作成する際の注意）

個人情報等が含まれる書類を作成する際は、書類作成の終了時に間違いがないか目視確認を行い、二重チェックを行うこと。

第 12-16 条 （個人情報等漏洩事件・事故等の情報収集について）

JIPDEC や日本データ通信協会、経済産業省や総務省、内閣官房、厚生労働省、国税庁、その他警察庁や各種セキュリティ会社から提供されている、個人情報等漏洩・流出事件に関する注意喚起情報を常に確認し、必要に応じて当社の SPMS に反映させること。

第 12-17 条 （SPMS の取組みについて）

作成した SPMS が完璧であるとは考えずに、毎年の内部監査のタイミングにおいて、少しでも自社に最適な SPMS になるように、無理・無駄な取組みを削除し必要なものを追加して行くこと。

（改廃の手順）

本規程の改廃は、（特定）個人情報保護管理者が起案し、取締役会の承認を得て行う。

（適用）

本規程第 1 版は、　年　月　日から適用する。