情報セキュリティ規定

株式会社プラムファイブ　システム事業部

２０１６年５月９日（第６版）

承認	査閲	作成
		沖田

改版記事

版数	年 月 日	記　　事	担当
1	2009.10.20	新規に制定する。	木村
2	2009.10.27	管理すべき情報、社内文書の秘密区分を追加	木村
3	2010.04.09	3.1 社内におけるアクセス制限の c と d を追加	木村
4	2010.04.20	個人情報保護を追加	木村
5	2010.05.01	3.9 ファイルサーバーのバックアップを追加	木村
6	2016.05.09	ノートパソコンの取り扱い（社内での管理と持出し時の扱い）	沖田

目　次

１．目的

この規定は、株式会社プラムファイブ　システム事業部（以下「当（事）」という。）の情報セキュリティ遵守に関する必要事項を定め、適正に維持管理することを目的とする。

２．管理すべき情報

１）企業秘密とは、当該業務に関する情報で公然と外部に知られていない情報を指す。

２）個人情報とは、個人情報保護法で定める個人情報を指す。

３）お客様情報とは、お客様の保有する情報（お客様自身の個人情報を含む）を言い

a）お客様から預かった情報

b）お客様から提供された情報

c）お客様から開示された情報

d）業務遂行過程で知り得た情報　　を指す。

但し、以下のものは含まない。

・開示を受けた時点で、既に公知もしくは公用であったもの。

・開示を受けた時点で、既に自ら保有していたもの。

・開示を受けた後、自己の責めによらず公知もしくは公用となったもの。

３．業務遂行上遵守すべき事項

3.1 社内におけるアクセス制限

管理責任者および従事者以外の者がアクセスできないよう、次の対策を行う。

a）部外者は、指定された場所以外は原則として立ち入り禁止とする。

b）紙や CD-ROM、USB メモリ、ポータブルハードディスク等の可搬記憶媒体（モバイルパソコンを含む）は使用後机上に置かず、ロッカーや事務机の引き出し等に保管する。

c）ログイン時のパスワードを設定する。

3.2 社外で使用する可搬記憶媒体のセキュリティ要件

お客様作業等で使用する可搬記憶媒体の内、USB メモリとポータブルハードディスクは以下のセキュリティ要件をみたしたものを使用すること。その他の可搬記録媒体についても、状況に応じて可能な範囲で最適なセキュリティ対策を実施する。

a）メモリまたはディスク内のデータを暗号化できる機能があること

b）パスワードによるロック機能があること

c）ノートＰＣはＢＩＯＳパスワードを設定すること。

3.3 携帯電話のセキュリティ要件

万一、携帯電話の紛失・盗難事故が起きた場合でも、第三者に個人情報（電話帳）、業務に関連するメール内容を勝手に閲覧・利用されないために、下記のセキュリティ対策を実施すること。

a）初期設定の暗証番号を変更

b）本体および外部メモリに業務関連の公開情報以外の秘密情報・個人情報の保存禁止

3.4 ウィルス対策

ウィルス感染によって情報が消滅若しくは漏洩しないよう、次の対策を徹底して行うこと。

〔パソコンへの対策〕

a) 会社が指定するウィルス対策ソフトウェアを必ずインストールすること。
・パソコン起動時にウィルス定義ファイルを最新にすること。
・定期的にウィルス定義ファイルを更新し、常に最新の状態に保つこと。
・自動監視機能（リアルタイム保護）、常時監視機能（Auto-Protect）を有効に設定すること。
・全ファイルスキャンを定期的に行い、ウィルス感染のないことを確認すること。

b) OS やアプリケーションに最新のセキュリティ修正を適用すること。
① Windows や Office 等の Windows 関連ソフトウェアについて、Microsoft Update 等を実行し、最新のセキュリティ修正を適用すること。

c)電子メール（e-mail）利用上の注意事項
・見知らぬ送信元から来た電子メールの添付ファイルは、開かずに削除すること。
・タイトルが不審な電子メールは、削除すること。
・電子メールに記載されている URL を、不用意にクリックしないこと。
・電子メール（e-mail）で２項に示す管理すべき情報が含まれた文書等を添付する場合は添付ファイルにパスワードを設定すること。

d)ファイル交換ソフトウェアの使用禁止
・Winny、Share 等のファイル交換ソフトウェアをインストールしないこと。
・ファイル交換ソフトウェアの例
Winny Share WinMX Gnutella Limewire Cabos BitTorrent Blubster Kazaa Freenet 等

e)パソコン内の情報を社外サーバに自動的に複製してしまう機能の使用禁止
・Google デスクトップの「複数のコンピュータ上のデータ検索（search across computer）等、パソコン内の情報を外部のサーバへ自動的に複製する機能を無効に設定すること。

f)社外でパソコンをインターネット接続した後に、社内でパソコンを使用するときは、事前に以下の事項を再確認すること。
・最新のセキュリティ修正が適用されていること
・ウィルス定義ファイルが最新になっていること
・最新のウィルス定義ファイルによるウィルススキャンを実施して、ウィルスに感染していないことを確認すること

3.5 情報の持ち出し制限
止むを得ず秘密情報を所定の作業場所から持ち出すときは、次の対策を実施すること。

a)持ち出す情報は、必要最小限に限定し、事前に管理責任者の許可が出た時に限り、持ち出しすることがでる。
b)管理責任者は、情報名、使用目的、返却等を管理する。
c)許可された情報を、ノートパソコンや USB メモリ等の可搬機能媒体に格納して持ち出すときは、以下のセキュリティ対策を行った上で持ち出すこと。

＜ノートパソコンの場合＞
・BIOS パスワードを設定する。
・ログイン時のパスワードを設定する。
・パスワード付きスクリーンセーバーを設定する。
・OS やアプリケーションに最新のセキュリティ修正を適用する。
・最新のウィルス定義ファイルを適用し、全ファイルスキャンを実施する。

＜可搬記憶媒体の場合＞
・パスワードを設定する。
・ファイルの暗号化を行う。
・最新のウィルス定義ファイルを適用し、全ファイルスキャンを実施すること。

3.6 持ち出し中の遵守事項

ノートパソコンや USB メモリ等の可搬記憶媒体、紙の媒体を所持して移動するときは、以下の盗難・紛失の防止策を講じること。

a)荷物を身から離さない
b)荷物から目を離さない
c)荷物から意識を離さない
d)電車内ではカバンや荷物を網棚に置かない。
e)自動車から離れるときは、荷物を車内に放置しない。
f)酒席が予定されているときは、ノートパソコン、可搬記憶媒体、紙の媒体等を持ち歩かず、事務所に保管しておくこと。「飲むなら持つな、持つなら飲むな」

3.7 持ち出し先での遵守事項

作業場所等では、紛失・盗難防止のために、以下の対策を講ずること。

a)ノートパソコンの場合
・持ち帰りを原則とするが、作業場所に置く場合は、社内での使用に準じることとするが、収納可能なロッカーが無い場合、セキュリティワイヤー等で机等に固定する。
・離席する場合には、パスワード付スクリーンセーバーを起動させるか、電源を切る等、他者がパソコンを使用する事ができないようにすること。

ｂ） 可搬記憶媒体の場合
・作業場所から離れる場合には、接続したままにせず作業者が所持した後、離れること。
・作業場所への保管は行わないこと。

c)持ち帰った情報は、ノートパソコン、可搬記憶媒体から削除し、最新のウィルス定義ファイルによるウィルススキャンを実施してウィルスに感染していないことを確認する。

3.8 お客様情報の入手、利用、廃棄

お客様情報について、次のことを注意する。

a)お客様の事前承諾なく、お客様情報を持ち出さない。
b)お客様情報を受け取る際は、お客様の指示に従う。
c)特別にお客様の指示があった場合は、お客様の指示に従う。
d)入手または預かったお客様情報は適切に管理する。
e)お客様情報は、業務の遂行のためにのみ使用すること。
（他の業務に使用したり、管理責任者および従事者以外に開示・提供することは出来ません。）

f)お客様情報を複製（電子メールの配布を含む）する場合は、事前にお客様に確認の上、
お客様の指示に従うこと。
複製した情報（資料）名称、配布先等を記録し、適切な管理を行うこと。

g)お客様業務終了で不要となったお客様情報（複製含む）は、お客様と合意した方法で速やかに返還または廃棄する。

h)不要となった記憶媒体は復元不可能となるように、上書き消去・物理破壊・シュレッダー処理・融解処理等により破棄する。

3.9 ファイルサーバーのバックアップ

管理責任者は、データの破損を防止するためファイルサーバーのデータはミラーリングすると共に毎日バックアップすること。

４．業務での個人所有パソコンおよび個人所有可搬記憶媒体の利用禁止

情報セキュリティ対策を徹底するため、個人所有のパソコン（自宅に設置しているパソコン、家族との共用パソコンを含む）および個人所有可搬記憶媒体（USB メモリ、ポータブルハードディスク等）を業務に利用することを禁止する。

５．情報セキュリティ事故への対処

情報を格納したノートパソコン・USB メモリ・CD-ROM 等の紛失・盗難、パソコンのウィルスによる情報漏洩等、情報セキュリティ事故が発生したときは、ただちに管理責任者に連絡する。

６．お客様貸与品に関する遵守事項

6.1 お客様発行の入場証の管理

お客様発行の入場許可証（含むマシン室入退場カード)、名札等（以下、「入場証」と略す。）は、厳重に管理し以下を厳守する。

a)入場証の貸し借りはしない。
b)入場証の紛失・盗難防止に細心の注意を払う。
c)お客様指定の入場証取扱いに関するルールを遵守する。
d)ゲストとして入退場する場合もお客様構内ルールを遵守する。
e)入場証等の借用、返却は当社業務管理者が台帳等で記録・管理すること。
この場合お客様が容易に確認できる方法であること。

6.2 お客様システム操作者用カード等の取扱い

お客様システムを操作（開発、保守、運用等）するためのカード（ＩＣカード、ＩＤカード等。以下「操作者用カード等」という）は、作業毎に事前にお客様に作業内容の承認を得たうえで借用し、借用中は以下を遵守すること。

a)操作者用カード等を貸し借りしない。
b)操作者用カード等の紛失・盗難防止に細心の注意を払う。
c)操作者用カード等はお客様指定場所（マシン室等）から持ち出さない。
止むを得ず操作者用カード等を持ち出す場合は、お客様の事前承認を得ること。
d)操者車用カード等の借用、返却は当社業務管理者が台帳等で記録・管理すること。

この場合お客様が容易に確認できる方法であること。

6.3 事故発生時の対応

事故発生時には以下の対応を行う。

a) 一人で解決しようとせず、直ちに上司（当社責任者を含む）に報告すること

b)当社業務責任者を通じてお客様に第一報を行うこと。

c)紛失・盗難の場合は、お客様と相談したうえで警察、交通機関にも届けを出すこと。

以上

社内文書の秘密区分

１．目的

本区分は社内で使用する全ての文書の秘密区分を明確にするため制定する。

２．適用範囲

社内で作成した文書に適用する。

３．文書とは

日常業務の円滑な遂行のために必要な情報を記録した書類（印刷物）、電磁的記録またはその他の媒体（電子文書）を指す。

なお、各種手続き用紙ならびに伝票類のように、定形用紙として開示範囲や取扱ルールが定められた印刷帳票あるいは電子帳票については本要領の適用から外す。

４．守秘レベル

今後、社内で作成される文書は、含まれる情報に応じ以下の３レベルに分類する。

よって、文書作成側には明確に意思表示をする義務が生じるとともに受取側には遵守義務が生じる。

・秘密　　：作成部門（作成者）の指定した者（個人）以外への情報開示を禁止

・社外秘　：当社従業員以外への情報開示を禁止

従業員とは、当社の役員およびこれに準ずる者ならびに他社からの出向を含む社員を指す。

・一般　　：特に制約を必要としない一般文書

一般文書とは、ＰＦＣグループ外の他社、マスコミ、調査会社、学校、学生等に開示しても差し支えない情報で構成されているもののこと。

５．文書タグ

守秘レベルの伝達ツールとして文書タグを指定する。

原則、作成文書のトップに『秘密文書管理要領』で示す定型の文書タグを必ず貼付することを義務付ける。

（例）守秘レベル・秘密、開示範囲・〇〇会議メンバ印刷文書の場合

秘密	〇〇会議メンバ

電子文書の場合

（秘密）：〇〇会議メンバ

６．適用時期

即日

個人情報保護

１．目的

当（事）における個人情報の取り扱いに関する基本的事項を定め、当（事）の業務の適性かつ円滑な運営を図りつつ、個人の権利利益を保護することを目的とする。

２．対象

当（事）が保有する個人情報を対象とする。

３．定義

用語の定義は、次のとおりとする。

１）「個人情報」とは、氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と照合することができ、それにより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）をいう。

２）「保有個人情報」とは、当（事）の従業員が業務上作成、又は取得した個人情報であって、当（事）の従業員が組織的に利用するものとして、当（事）が保有しているものをいう。

３）「個人情報ファイル」とは、保有個人情報を含む情報の集合物であって、次に掲げるものをいう。

① 一定の業務の目的を達成するために特定の保有個人情報をパソコンにて検索することができるように体系的に構成したもの

② ①に掲げるものの他、一定の業務の目的を達成するために氏名、生年月日、その他の記述等により特定の保有個人情報を容易に検索ことができるように体系的に構成したもの

４）「総括個人情報保護管理者」（以下「総括管理者」という。）とは、当（事）に１人を置き、保有個人情報保護に関する事務を総括する者をいう。

５）「個人情報管理責任者」（以下「管理責任者」という。）とは、各課に１人を置き、保有個人情報を適切に管理する者をいう。

６）「個人情報監査責任者」（以下「監査責任者」という。）とは、当（事）に１人を置き、保有個人情報の管理の状況について監査する者をいう。

４．保有個人情報の適切な管理のための委員会

総括管理者は、保有個人情報の管理に係る重要事項の決定、連絡・調整等を行うため必要があると認めたときには、個人情報公開委員会を開催する。

５．教育研修

管理責任者は、保有個人情報の取り扱いに従事する従業員に対し、保有個人情報の取り扱いについて理解を深め、個人情報の保護に関する意識の高揚を図るための啓発その他必要な教育研修を行う。

２ 管理責任者は、保有個人情報の管理に関する事務に従事する従業員に対し、保有個人情報の適切な管理、運用及びセキュリティ対策に関する必要な教育研修を行うものとする。

６．従業員の責務等

保有個人情報の取り扱いに従事する従業員は、その業務に関して知り得た個人情報の内容をみだりに他人に知らせ、又は不当な目的に利用してはならない。

２ 従業員は法の趣旨に則り、関連する法令及び規定等の定めに並びに管理責任者の指示に従い、保有個人情報を取り扱わなければならない。

７．個人情報の収集

収集目的を明確に定め、その目的の達せに必要な限度において行わなければならない。また、新しい目的で個人情報を収集するときは、管理責任者に届け出なければならない。

２　個人情報の収集目的は、業務で必要な事項などで利用することである。従業員についての個人情報の収集目的は、雇用管理のためである。

３　個人情報の収集方法の制限は、適法、かつ公正な手段によって行わなければならない。

４　個人情報を収集する方法は、次に掲げる方法による。

①　本人の申告および提供
②　関係者等からの提供
③　関連会社からによる提供
④　その他の場合は、同意を得て収集する。

５　次に掲げる個人情報の収集は行ってはならない。

①　犯罪歴、その他社会的差別の原因となる事項
②　思想、信条及び宗教に関する事項

８．保有個人情報の利用範囲の制限

保有個人情報の利用範囲の制限は、次に掲げる。

①　保有個人情報の利用は、原則として目的の範囲内で、具体的な業務に応じて権限を与えられた者が、業務の遂行上必要な限り利用する。
②　管理責任者の承諾を得ないで、保有個人情報の目的外利用、第三者への提供、通常の利用場所からの持ち出し、外部への送信等の漏えい行為をしてはならない。
③　従業員は、業務上知り得た個人情報の内容をみだりに第三者に知らせ、又は不当な目的に使用してはならない。その業務に係る職を退いた後も、同様とする。
④　従業員から自己情報についての利用又は第三者への提供を拒まれた場合、これに応じなければならない。ただし、裁判所および令状に基づく権限の行使により開示請求等が必要な場合について、この限りではない。

９．アクセス制限

管理責任者は、保有個人情報の秘匿性等の内容に応じて、保有個人情報にアクセスする権限を有する者をその利用目的に考慮し、必要最小限の従業員に限らなければならない。また、保有個人情報の秘匿性等の内容に応じて、アクセス制御、アクセス記録、外部からの不正アクセスの防止、コンピュータウィルスによる漏えい等の防止､その処理を行うパソコンの限定及びパソコンの盗難防止等のための措置を講じなければならない。

２　アクセス権限を有しない従業員は、保有個人情報にアクセスしてはならない。

３　従業員は、アクセス権限を有する場合であっても、業務上の目的以外の目的で保有個人情報にアクセスしてはならない。

１０．複製等の制限

従業員は、業務上の目的で保有個人情報を取り扱う場合であっても、次の各号に掲げる行為については、管理責任者の指示に従い、行うものとする。

①　保有個人情報の複製
②　保有個人情報の送信
③　保有個人情報が記録されている可搬記憶媒体の外部への送付又は持ち出し
④　その他保有個人情報の適切な管理に支障を及ぼすおそれのある行為

１１．第三者の閲覧防止

従業員は、保有個人情報が保管されているパソコンの使用に当たっては、第三者の閲覧されることがないよう、その処理するパソコンから離れる等使用状況に応じて利用停止の処理を行う等の必要な処置を講じなければならない。

１２．誤りの訂正等

従業員は、保有個人情報の内容に誤り等を発見した場合には、管理責任者の指示に従い、訂正等を行うものとする。

１３．廃棄等

従業員は、保有個人情報又は保有個人情報が記録されている可搬記憶媒体（パソコン及びサーバに内蔵されているものも含む）が不要となった場合は、管理責任者の指示に従い、当該保有個人情報の復元又は判読が不可能な方法により当該情報の消去又は当該可搬記憶媒体の廃棄を行わなければならない。

１４． 保有個人情報の提供

管理責任者は、従業員以外の者に保有個人情報を提供する場合は、原則として、提供先における利用目的、利用する業務の根拠、利用する記録範囲及び記録項目並びに利用形態等について書面を取り交わすものとする。

１５． 事案の報告及び再発防止措置

保有個人情報の漏えい等安全確保の上で問題となる事案が発生した場合に、その事実を知った従業員は、速やかに管理責任者に報告するものとする。

２ 管理責任者は、前項の報告を受けた場合は、被害の拡大防止又は復旧等のために必要な措置を講ずるとともに事案の発生した経緯及び被害状況を調査し、総括管理者に報告しなければならない。ただし、特に重大と認める事案が発生した場合には、直ちに総括管理者に当該事案の内容等について報告するものとする。

３ 管理責任者は、事案の発生した原因を分析し、再発防止のために必要な措置を講ずるものとする。

４ 総括管理者は、当該事案の内容、影響等に応じて、事案関係及び再発防止策の公表、並びに当該事案に係る本人への対応等の措置を講ずるものとする。

１６．苦情処理

総括管理者は、保有個人情報の取り扱いに関する苦情の適切かつ迅速な処理に努めなければならない。

２ 苦情の相談の受付等を行う窓口を置く。

３ 苦情を受け付けたときは、関係する課は、苦情に関する当該保有個人情報の取り扱い状況等を迅速に調査し、適切な処置について総括管理者及び管理責任者と協議しなければならない。

４ 苦情の処理は、必要と認めるときは総括管理者のもとで行うものとする。

５ 苦情の処理結果は、必要と認めるときは苦情を申し出た者に書面で通知するものとする。

１７．監査

監査責任者は、保有個人情報の管理の状況について、定期的に、又は随時に監査を行い、その結果を保存し管理しなければならない。

１８．点検

管理責任者は、保有個人情報の可搬記憶媒体、処理経路及び保管方法等について、定期的に、又は随時に点検を行い、必要があると認めたときは、その結果を総括管理者に報告するものとする。

１９．評価及び見直し

総括管理者は、保有個人情報の適切な管理のための措置について、実効性等の観点から評価し、必要があると認めたときは、その見直し等の措置を講ずるものとする。

２０．懲戒等

違反した従業員に対して就業規則に基づき懲戒を行うことがある。

以上