情報セキュリティ管理細則

制定　平成２４年１２月２０日
改正　平成２５年　６月２８日

目次

第１章　総則

（趣旨）

第１条　この細則は、電子計算組織運用管理規程（平成２４年１２月２０日制定。以下「規程」という。）第７条の規定に基づき、公益財団法人平塚市まちづくり財団（以下「財団」という。）の電子計算組織における情報の安全性と信頼性を確保する情報セキュリティ対策について必要な事項を定めるものとする。

（定義）

第２条　この細則において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

（１）　電子計算組織　電子計算機、電子計算機による電子的方法、磁気的方法等により情報を記録する装置（以下「媒体」という。）、ソフトウエア及び電子計算機によるネットワークシステムをいう。

（２）　情報システム管理者　規程第５条第２項の規定により情報統括管理責任者によって任命され、情報システムの運用、維持及び管理に関する実務上の管理者をいう。

（３）　電子計算機等　電子計算機及び媒体をいう。

（４）　使用者　財団が貸与する電子計算組織を使用して、財団の業務を処理する者をいう。

（業務従事者の責務）

第３条　情報システム管理者は、各部門に設置される電子計算組織の運用上の指導、指示、統制等について、その管理責任を有する。

２　使用者は、規程及びこの細則に基づいて電子計算組織を適正に運用するとともに、自己の業務において関与する情報について、その管理責任を有する。

第２章　電子計算組織の運用

（使用者教育）

第４条　情報システム管理者は、電子計算組織の導入又は変更を行った場合は、使用者に対する教育の必要性を検討し、必要に応じて教育及び訓練を計画し、実行する。

（情報のバックアップ）

第５条　情報システム管理者は、電子計算組織の障害の可能性及び影響度に応じて、情報のバックアップを定期的に行い、その記録を維持する。

（電子計算組織の監視）

第６条　情報システム管理者は、電子計算組織の特性に応じ、電子計算組織の正常運行、障害発生の有無等を適切に管理する。

２　情報システム管理者は、作業ログ、障害ログなどの重要な電子計算組織に係るロギング情報を管理する。

（構成管理）
第７条　情報システム管理者は、ＯＳ、ソフトウエア等について、バージョン情報（変更情報を含む。）の管理を適切に行うものとする。

第３章　ユーザーＩＤ及びパスワードの管理

（ＩＤ及びパスワード管理）
第８条　業務で使用するＩＤ及びパスワードは、次の各号に従って、適切かつ厳格に管理されなければならない。
（１）　ユーザーＩＤの管理（交付含む。）は、情報システム管理者が行うこと。
（２）　パスワードの管理は、情報システム管理者の指示に則って、使用者が行うこと。
（３）　特定の業務で共通のパスワードを使用する場合には、情報システム管理者が付与したパスワードにより行うこと。

（ユーザーＩＤの交付）
第９条　ユーザーＩＤの交付は、理事並びに職員、嘱託職員及び臨時職員（以下「職員等」という。）に対して個人ごとに交付する。
２　業務委託会社の従業員等には、情報システム管理者が業務上必要と認める場合に限り交付する。
３　その他の業務用ユーザーＩＤは、当該業務を所管する情報システム管理者が業務上必要と認めた者に対して交付する。
４　不特定多数で利用するユーザーＩＤは、交付しない。

（ユーザーＩＤの申請等）
第１０条　ユーザーＩＤの登録、変更又は削除の申請は、情報システム管理者に申請するものとする。
（１）　登録　総務施設課長からの入社通知をもって申請手続きとする。
（２）　変更　原則として変更は、行わない。
（３）　削除　使用者が退職等で不要となったユーザーＩＤは、総務施設課長の退職等通知をもって申請とする。

（ユーザーＩＤの適正利用）
第１１条　使用者は、ユーザーＩＤの交付を受けた場合には、業務上での利用を許可された者との認識に立ち、交付を受けたユーザーＩＤの適正利用に対する万全の配慮を心がけなければならない。
２　使用者は、ユーザーＩＤを私的に利用又は財団に損害を与えるような利用をしてはならない。

（ユーザーＩＤの利用状況の監視）
第１２条　情報システム管理者は、ユーザーＩＤの利用状況をログ（操作記録）分析により監視を行うことができる。

（パスワードの管理）
第１３条　使用者は、次に掲げるところにより、パスワードを設定するのもとする。
（１）　パスワードは、８桁とし、数字、ローマ字を混合すること。
（２）　パスワードは、年１回以上変更すること。
（３）　パスワードは、他者に知られないよう適切に管理すること。
２　共通パスワードを使用する場合には、前項の規定にかかわらず、共有パスワード利用者に退職又は人事異動があった場合は、速やかに、変更するものとする。

第４章　アクセス権限の管理

（アクセス権限の付与）
第１４条　媒体に保存している情報（以下「情報」という。）へのアクセス権限は、次に掲げるところにより、付与するものとする。
（１）　職員等は、職務及び業務上の必要性に応じて、情報に対してアクセスすることを可能とする。
（２）　業務委託会社の従業員等は、情報に対してアクセスできないものとする。ただし、業務上の必要

性から、業務委託会社の従業員等に対して当該情報にアクセスしなければならない場合は、当該業務所管の情報システム責任者がアクセス権限を許可することができる。

（3）　情報システム管理者は、その管理対象媒体のすべての情報に対してアクセスすることができるものとする。

（アクセス権限の付与単位）

第１５条　　情報へのアクセス権限（以下「アクセス権限」という。）は、使用者別又は使用部門別の単位で設定するものとする。

（アクセス権限を有する者の削除等）

第１６条　情報システム管理者は、アクセス権限を有する者が退職した場合、総務施設課長からの退職通知をもって当該アクセス権限を有する者を削除するものとする。

２　情報システム管理者は、アクセス権限を有する者が異動した場合は、事務の引き継ぎが終了した時点で、速やかに、アクセス権限を有する者を変更するものとする。

（媒体への保存）

第１７条　使用者は、媒体に情報を保存・保管する場合は、当該保存・保管する情報に対し、アクセス権限を有する者の範囲を認識した上で、安全性を確認し、保存・保管するものとする。

（共有領域のアクセス権限）

第１８条　電子計算組織の共有領域に対するアクセス権限は、使用者又は使用部門ごと設定するものとする。

２　情報システム管理者は、前項の共有領域を新たに作成する場合は、アクセス権限を有する者の範囲を特定し、適切に設定するものとする。

（自己の情報へのアクセス制限）

第１９条　使用者は、共有されていない情報について、必要に応じてパスワードを設定するなどにより、他者が安易にアクセスできないよう制限するものとする。

（不正アクセスの監視）

第２０条　情報システム管理者は、使用者による操作ログを収集し、アクセス権限がない使用者によるアクセスの監視を行うことができる。

第5章　コンピュータウイルス対策

（コンピュータウイルス対策ソフトウエアのインストール）

第２１条　情報システム管理者は、業務上使用する電子計算機に対して、コンピュータウイルス対策ソフトウエアをインストールしなければならない。

（コンピュータウイルス情報データの更新）

第２２条　情報システム管理者は、コンピュータウイルス対策ソフトウエアのウイルス情報データ（パターンファイル）を常に最新の状態を維持するように設定するものとする。

（コンピュータウイルス感染時の対応）

第２３条　使用者は、使用している電子計算機がコンピュータウイルスに感染した場合又はその感染の疑いがある場合には、直ちに、情報システム管理者に報告の上、その指示に基づいてコンピュータウイルスを駆除しなければならない。

２　使用者は、コンピュータウイルスの感染の拡大を防止するため、情報システム管理者の指示に従い、コンピュータウイルスの感染経路、その複製等を確認し、感染経路を遮断する等の措置を講じなければならない。

（コンピュータウイルスチェックの実施）

第２４条　使用者は、次に掲げる場合は、必ずコンピュータウイルスチェックを実施しなければならない。

（1）　新たな電子計算機を導入するとき。

（2）　外部の者が修理等で電子計算機を使用したとき。

（3）　情報システム管理者が承認していない電子計算機を外部から持込み電子計算組織に接続したとき。
（4）　新たなソフトウエアをインストールしたとき。
（5）　使用している電子計算機で、直接、外部との情報の受渡しを行ったとき。

第6章　電子メール等の管理

（電子メール等の適正利用）

第２５条　使用者は、電子メール等を使用する場合は、その適正利用に万全の配慮を心がけるものとする。
２　使用者は、電子メール等を業務上の必要な範囲内で使用し、私的及び財団に損害を与えるような使用をしてはならない。

（メールアドレスの交付）

第２６条　メールアドレスは、原則として、情報システム管理者が使用者ごとに交付するものとする。

（メールアドレスの削除）

第２７条　情報システム管理者は、使用者の退職等によりメールアドレスを削除する場合は、総務施設課長からの退職通知又は業務委託会社の異動通知をもって行うものとする。

（電子メール等でのbccの利用）

第２８条　複数の者に電子メール等を送信する場合は、個人情報を適切に保護するために、bcc(Blind Carbon Copy)機能を有効に活用するものとする。

第7章　インターネットの利用管理

（インターネットの適正利用）

第２９条　インターネットへのアクセスは、業務上必要な範囲に限定し、私的な利用及び財団に損害を与えるような利用をしてはならない。

（インターネットへのアクセス方法）

第３０条　使用者は、電子計算機でインターネットにアクセスする場合、自己のネットワークＩＤを使用し、必ず財団の電子計算機によるネットワークシステムを経由してアクセスするものとする。

（情報のダウンロードとアップロード）

第３１条　使用者は、業務上、インターネット等から情報の取込み（ダウンロード）を行う場合は、必ずコンピューウイルスチェックを実施しなければならない。
２　インターネット等への情報の登録（アップロード）は、原則として、行ってはならない。
３　情報の登録（アップロード）が必要な場合は、情報システム管理者の許可を得て行わなければならない。

（インターネットへの会員登録）

第３２条　使用者は、インターネットを利用する場合で、そのインターネット利用が会員登録を必要としているときは、その都度、情報システム管理者の許可を得て行わなければならない。

（有料サイトの利用）

第３３条　有料情報を提供するインターネットへのアクセスは、原則として、行わないものとする。ただし、業務上その利用が必要な場合は、情報システム管理者の許可を得て行わなければならない。

（インターネットのアクセスの監視）

第３４条　情報システム管理者は、インターネットへのアクセス状況をログ（閲覧履歴）分析により監視を行うことができる。

第8章　その他

（電子計算機の持出し及び持込み）

第３５条　使用者は、原則として、電子計算機を事務所等の外への持出し又は外部の電子計算機を事務所等への持込みを禁止するものとする。ただし、業務上必要な場合は、情報システム管理者の許可を得て行うことができる。

（媒体の保護）

第３６条　情報システム管理者は、媒体の重要な設備機器について、盗難、破壊等から保護する方法を措置するものとする。

（情報の管理）

第３７条　使用者は、情報の不正使用、改ざん、紛失等を防止するため、情報の授受、保存・保管及び廃棄について、次に掲げるところにより、行わなければならない。

（１）　媒体により外部と情報の授受を行う場合は、その媒体の紛失や漏えいを防止するために、受渡し方法及び記録方法を具体的に定め、行うこと。

（２）　不要となった情報は、保存・保管期間の終了後、定められた方法によって、速やかに、廃棄すること。

（３）　情報の漏えい又は流出を防止するため、外部の媒体に情報の複写を行わないこと。ただし、業務上必要な場合は、情報システム管理者の許可を得て行うこと。

（４）　重要な情報の破損や障害等の発生に備え、情報のバックアップを行うこと。

（離席時の措置）

第３８条　使用者は、電子計算機を使用している途中で離席する場合は、離席中に当該電子計算機の画面を他者に見られないよう、又は操作されないよう、次のいずれかの措置を講ずるものとする。

（１）　電源を切ること。

（２）　ログオフすること。

（３）　パスワード付スクリーンセイバーを設定すること。

（４）　その他必要な措置をとること。

（ソフトウエアの導入）

第３９条　使用者は、電子計算機に情報システム管理者が許可したソフトウエア以外のソフトウエアを導入（インストール）してはならない。

（その他）

第４０条　この細則に定めるもののほか、情報セキュリティ対策について必要な事項は、別に定める。

附　則

この細則は、平成２４年１２月２０日から施行する。

附　則

この細則は、平成２５年6月２８日から施行する。