公益財団法人世田谷区スポーツ振興財団安全対策基準

平成１８年５月３０日
改正平成１９年３月３１日
改正平成２０年９月２５日
改正平成２１年２月１６日
改正平成２３年４月１日
改正平成２３年１２月２６日

この基準は、公益財団法人世田谷区スポーツ振興財団個人情報保護規程（以下「規程」という。）第５条第１項第３号オに定める個人情報保護マネジメントシステムを実現する文書の一部とし、公益財団法人世田谷区スポーツ振興財団個人情報保護規程施行規則（以下「規則」という。）第７条第３項に規定された安全対策は、この基準による。

Ⅰ．総論

（目的）

第１条　本基準は、当財団における個人情報の収集、利用、提供および管理における個人情報に関するリスク（個人情報への不正アクセス、個人情報の紛失、破壊、改ざんおよび漏えい）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。

（用語の定義）

第２条　本基準において使用する用語の意義は、規程において使用する用語の例による。

（適用範囲）

第３条　本基準を適用する範囲は、規程において定める例による。

Ⅱ．物理的アクセス管理

（事務所への入退室の制限）

第４条　事務所への入退室は、当財団役員、ネームプレートを着用した職員、および当財団職員の同伴による案内がある者のみに限定する。

２　事務所への入退室にあたっては、最初に入室する者及び最後に退室する者の記録をとり、個人情報管理者が確認を行う。

（ネームプレートの着用）

第５条　職員は、事務所等での勤務中、所属部署および氏名を識別できるネームプレートを目に見える位置に着用しなければならない。

（不審者の識別および対応）

第６条　事務所内において、ネームプレートを着用しておらず、当財団職員の同伴もない者を見つけた場合には、当財団職員から必ず声をかけ、身元、訪問先、目的を確認する。

２　前項により確認できなかった場合は、氏名および連絡先を確認した上で退出を求める。

（施錠の管理）

第７条　最後に事務所を退出する職員は、ファイリングキャビネットおよびＯＡルームを施錠後、事務所内に不審者がいないことを確認したうえで事務所の出入口を施錠する。

（夜間・休館日の入退室）

第８条　夜間・休館日は、ビルの出入り口は施錠され、解錠は、原則としてビルの警備会社が行う。

２　事務所内への入室は、事前に勤務を命ぜられた職員のみ入室することができる。

（個人情報の分類）

第９条　文書の機密性について以下のとおり分類する。

（１）機　密：内部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や職員の個人情報を含む。

（２）社外秘：職員のみに開示可能な情報。機密情報のうち、部門個人情報管理者によって内部開示を認められたものは社外秘扱いとする。

（３）一　般：公開を目的とした情報（開示後のＩＲ情報含む）または開示されることにより当財団に不利益をもたらさない情報。

（個人情報の媒体の取扱い）

第１０条　個人情報を含む文書の取扱いは、次のとおりとする。

（１）機　密：保管場所を特定するとともに、その利用には所轄部門の部門長の許可を必要とする。また、業務目的以外の複製は不可とする。

（２）社外秘：保管場所を特定するとともに、社外への持ち出しには所轄部門の部門長の許可を必要とする。

（３）一　般：特に定めない。

２　個人情報を含む電子媒体の取扱いは、次のとおりとする。

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

（２）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。

（３）個人情報の入ったデータの受け渡し時には、「個人情報授受簿」に授受の記録をとり、機密度に応じた授受の方法を選択する。

Ⅲ．論理的アクセス／ネットワーク管理

（アクセス権限の管理）

第１１条　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　情報システムに関するアクセス権限の付与、抹消および変更は、情報システム管理者が「アクセス権限管理表」（第１号様式）

により管理する。
（２）アクセス権限の付与・変更・抹消
①　情報システム管理者は、年度当初、当該年度の事務分担表によりアクセス権限を付与または抹消し、「アクセス権限管理表」（第１号様式）に記録する。また、年度途中に変更があった場合も同様とする。
②　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）記録の保管
①　システム担当者は、ファイルサーバーへのアクセスの記録（以下、「ログ」という。）を月に１回以上の頻度で分析し、サーバアクセスログ月次確認報告書を作成する。
②　システム担当者は、サーバアクセスログ月次確認報告書により情報システム管理者に報告する。
③　システム担当者は、ログに異常を発見した場合は、速やかにシステム管理者に報告し、指示をあおぐ。
④　ログの保管期間は、６ヵ月間とする。

（個人ＩＤおよびパスワードの管理）

第１２条　情報システム管理者は、利用者から、個人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う。また、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　情報システムの利用者（以下「利用者」という。）は、次のとおり、個人ＩＤおよびパスワードを個々の責任において管理する。
（１）付与された個人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。
①　生命の危険および業務遂行に関する重大問題を回避するために、必要な場合
②　情報システム管理者が、システムのメンテナンスまたは利用者の個人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
（２）個人ＩＤ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。
①　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。
②　パスワードは６文字以上のものを使用する。その際、誕生日、電話番号等、容易に推測可能なものは使用してはならない。
③　パスワードは６ヶ月に一度の頻度で更新しなければならない。
④　パスワードはメモや紙に記載してはならない。
⑤　パスワードを入力する際、他人に見られないよう留意しなければならない。
（３）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、情報システム管理者に連絡し、指示を受ける。
３　第１項および前項第１号から第２号の規定は、当財団のシステム

環境上運用が可能になった時から適用する。それまでの間は、情報システム管理者が、業務ＩＤのパスワードを１ヶ月に一度の頻度で更新することにより対応する。

（不正アクセスの防止対策）

第１３条　情報システム管理者は、情報システムを不正アクセスから防護するため、以下の事項を必要に応じ実施する。

（１）通信経路上の情報は、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を防止する対策を講じる。

（３）無線ＬＡＮを採用する場合は、暗号化の設定を行う等、通信内容の傍受を防止する対策を講じる。

（４）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する。

（５）長期間利用しない機器は、ネットワークに接続しない。

（６）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。

（７）データの特性上必要な場合は、データの所有者と協議したうえで、個別に防止策を講ずる。

２　情報システム管理者は、情報システム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、アクセス履歴を定期的に分析する。ただし、ＷＷＷサーバ・メールサーバなどがホスティングによる場合を除く。

（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．サーバ／端末管理

（サーバの物理的セキュリティ）

第１４条　情報システム管理者は、ＯＡルームにおいて、次に定める物理的なセキュリティ対策を実施し、サーバ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。

（２）機器の落下や損傷の防止措置。

（３）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　情報システムの一部を、社外データセンター内のマシン室またはサーバラック内に設置する場合には、以下の事項を実施する。

（１）情報システム管理者は、データセンターを次の基準を考慮して選定する。

①　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。
② 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。
③ 機器の落下や損傷の防止措置が講じられていること。
④ 耐震、耐火、耐水、避雷等の防災対策おおび電源対策が施されていること。
（２）前号以外の詳細な安全対策については、当該データセンターの安全基準に従う。
（３）データセンターとは、安全対策に関する事項を含めた契約を締結する。
（４）当財団職員がデータセンターへ入室する際は、情報システム管理者に事前の了解を得る。

（データのバックアップおよびリストア）

第１５条 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、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、原則として週次とする。
（２）バックアップの方法は、原則として、同一ネットワーク上のファイルサーバまたはＤＡＴテープとする。
（３）バックアップ媒体は、施錠可能なキャビネット等に保管し、容易に持ち出しが出来ないよう管理する。
（４）バックアップデータは、３世代前までの保管を行う。
２ 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）情報システム管理者の責任の下、リストアを実施する。

（ウィルス等、悪質なソフトウェアからの防護）

第１６条 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情報システムを防護するために、次の事項を規定する。
（１）財団内の情報システム
① 当財団内で使用する情報システムには、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 情報システム管理者は、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 情報システム管理者は、ウィルス情報について常に収集に努め、必要に応じて、各利用者に対策を指示する。
（２）外部から持ち込む情報システム
① 顧客や協力会社等、外部から持ち込まれる端末は、原則として、当財団の情報システム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各部門個人情報管理者が認めた場合は、接続を許可することを妨げない。

（システムの設置および変更）

第１７条 情報システム（財団内ＬＡＮ含む）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。本条で意図する情報システムとは以下のものを含む。
①　サーバ
②　ＰＣ（デスクトップおよびノート）
③　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）
④　媒体記録装置（ＦＤ、ＭＯ、ＣＤ－Ｒ、ＤＶＤ－Ｒ、外部メモリ等）
⑤　外部記憶装置（外付けハードディスク等）
⑥　ＯＳ
⑦　アプリケーション（電子メールソフト／Ｗｅｂブラウザ含む）
⑧　ユーティリティソフト
⑨　Ｆ／Ｗ、ゲートウェイ
⑩　ルータ、スイッチングハブ
⑪　その他、ネットワーク関連設備
（２）情報システムの設置・変更の管理は、以下のとおり行う。
①　情報システムの設置・変更および撤去作業は、以下の者（以下「作業者」という。）が行う。
ａ）情報システム管理者
ｂ）情報システム管理者より権限を委譲された職員
ｃ）情報システム管理者が承認の上、当財団と契約を締結した外部委託先
②　情報システムの設置・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、情報システム管理者に提出する。
③　情報システム管理者は、常に、情報システムの構成を把握し、作業を実施または指示する。
④　情報システム管理者以外の者は、当財団の情報システムへの外部からの接続を、許可無く行ってはならない。
⑤　情報システム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、情報システム管理者または権限を委譲された職員は、変更の検証を実施し、変更点と動作を確認する。
⑦　ＰＣはワイヤーロック等、物理的な盗難対策を行う。

（パッチ等システムの更新（Windows Update 等））

第１８条　情報システム管理者は、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。

（外部公開サーバの管理とデータの更新）

第１９条　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。

（１）第16条の規定に基づき、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収集し、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）前各号を実施することが困難な場合および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、遅滞なく情報システム管理者に報告する。
（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　教室やイベント申込みなど、外部公開サーバで個人情報を収集する場合、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は、以下の管理を実施する。
（１）外部公開サーバ上のデータ更新を行うことができる者は限定する。
（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について、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う。

Ｖ．情報システムの利用

（利用状況の監視）

第２０条　当財団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の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）財団が関与する紛争を解決するために必要と判断したとき。

（情報システム（財団内ＬＡＮ含む）利用にあたっての遵守事項）

第２１条　情報システムは、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　情報システムは、許可無く外部に持ち出してはならない。
３　情報システムは原則、当財団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んではならない。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、指定のファイルサーバに保管し、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しなければならない。

（個人用端末の管理）

第２２条　個人用端末は、原則、情報システム管理者から貸与されたものを用い、個人所有のものなどは持ち込んではならない。ただし、やむを得ない理由により、情報システム管理者が認めた場合は、この限りではない。

（個人用端末の持ち出し）

第２３条　個人用端末の持ち出しは、一切禁止する。ただし、当財団が管理する他施設へ配置転換する場合は、この限りではない。

（媒体記録装置の利用）

第２３条の２　媒体記録装置（ＦＤ、ＭＯ、ＣＤ－Ｒ、ＤＶＤ－Ｒ、外部メモリ等。以下同じ。）をパソコン等機器に接続してはならない。ただし、業務上必要な場合で次に掲げる事項に全て該当し、かつ個人情報管理責任者の許可を得た場合は、この限りでない。

（１）業務上必要な処理で代替手段がないとき。

（２）記録媒体の管理を適切に行う手順を講じているとき。

２　媒体記録装置を用いてデータを持ち込む場合は、ファイルを開く前にウイルスチェックを実施する。

（電子メールの利用）

第２４条　情報システム利用者は、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し、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。

（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、業務利用を目的とし、私的な利用を禁ずる。

（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。直ちに情報システム管理者に連絡する。

（５）電子メールソフトについては、当財団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。

（Web（ホームページ）等の利用）

第２５条　情報システムの利用者は、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。

（２）Webブラウザについては、当財団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）財団内外の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

財団内外のシステムを利用してはならない。

（障害発生時の対応）

第２６条　ウィルス感染の可能性がある場合は、以下のとおり対応する。

（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）情報システム管理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は、以下のとおり対応する。

（１）情報システム管理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、情報システム管理者の許可なしに行ってはならない。

附則

この基準は平成１９年３月３１日から施行する。

附則

この基準は平成２０年９月２５日から施行する。

附則

この基準は平成２１年２月１６日から施行する。

附則

この基準は平成２３年４月１日から施行する。

附則

この基準は平成２３年１２月２６日から施行する。