（要領 3）　要領3については、歩数計アプリを活用した仕組みの構築・運用事業者のみ提出してください。

提出日：　　年　　月　　日

横浜市長

所　在　地

商号又は名称

代表者職氏名　　印

サーバ等及び情報システムに関するセキュリティ対策

下記項目はセキュリティ対策として必須項目です。各項目の内容を満たしていることがわかるように記載してください。

1　サーバ等の設置場所			具体的な状況
	(1)	サーバ等の設置場所は、①第三者が自由に操作できない場所とし、②サーバ等の設置場所であるようなことを示す表示をしておらず、③必要十分な電源を確保し、④施錠設備を有する必要最小限の出入口を備えた部屋とする。動作に空調設備が必要なサーバ等を設置した場合には、空調設備を用意する。	
	(2)	サーバ等を設置した部屋内の機器は、保守等を容易にするため合理的で適切な配置とし、コピー又は FAX 等、データの複写や送信のための設備を設置しない。万一、設備を同一室内に設置された場合は、部外者が利用できないよう保護措置を講じる。	
	(3)	サーバ等に使用する物品や出力物の受け渡しは、サーバ等を設置した場所とは別の場所とし、同一室内の場合、サーバ等に物理的及びネットワーク的に接触できないよう保護措置が講じられ、受け渡しの際に入室権限がある者が立ち会っている。	
	(4)	特に重要なサーバ等を設置した部屋には、防犯カメラ、侵入報知機等の防犯設備と、非常電話、非常ベル等の非常用連絡設備を設置し、無停電電源装置を用意している。	
2　サーバ等の設置場所の運用			具体的な状況
	(1)	サーバ等を設置した部屋への未登録者の入室および作業実施については、事前に部屋の管理者の許可を得た上で、入室権限のある者が同伴する。サーバ等を設置した部屋内に入室権限のある者が不在となる場合、入室権限の無い者を退室させた上で、施錠する。サーバ等を設置した部屋への入室権限は、職員の異動などにあわせて速やかに見直し、入室不要となった者は速やかに登録を抹消し、入室のための認証を無効にする。	
	(2)	サーバ等を設置した部屋への入退室を記録する。	
	(3)	サーバ等を設置した部屋内では、部屋の管理者の許可なく撮影・模写・録音等を行わせない。また、作業に必要のないものを置かない。また、部屋内の環境（機器・設備の有無、配置、利用状況等）に問題がないことを定期的に点検する。	
	(4)	特に重要なサーバ等について、停電や落雷、水害等への対策を行う。	
3　機密情報を格納しているサーバ等の廃棄・返却・修理等			具体的な状況
	(1)	サーバ等を廃棄する場合は、原則として、削除した情報の復元が困難な方法で情報を削除してから廃棄する。	
	(2)	サーバ等を返却する際、機密情報を格納しているサーバ等については、原則として､削除した情報の復元が困難な方法で情報を削除してから返却する。	
	(3)	機密情報を格納しているサーバ等を修理するために外部へ持ち出す場合は、事前に、削除した情報の復元が困難な方法で情報を削除する。機密情報を格納しているかどうか不明な場合には、機密情報を格納しているものとして取り扱う。	

裏面あり

4　通信機器等の管理			具体的な状況
	(1)	サーバ等のための通信機器等は、容易に第三者が触れられないように、かつ接触による断線や電源断などが起きないように敷設する。	
	(2)	ファイヤウォール､ルータ等の設定を行えるサーバ等のための通信機器等は､パスワードを設定するなどして､第三者が設定の変更等を行えないようにする。	
	(3)	ファームウェアの更新や適切な設定を行うなど､不正な利用がされないようにする。	
5　情報システム開発時			具体的な状況
	(1)	管理するデータについて、漏えい・改ざん・破壊といった問題が発生した場合の影響の評価などのリスク分析を実施する。	
	(2)	データの入力チェック、内部でのデータの処理プロセスの正当性評価、出力されるデータの妥当性評価などの、データの完全性に関する検査を実施する。	
	(3)	サーバ等には、情報システムの趣旨、用途に応じた必要最低限のソフトウェア以外のものをインストールしない。	
	(4)	管理者を含む開発用の利用者登録では、個人ごとに ID を発行し、それぞれに推測困難なパスワードを設定する。	
6　情報システム導入時			具体的な状況
	(1)	データ及び情報システムの安全かつ正常な運用を確実にするために､情報資産の一覧を作成し、各情報資産の情報資産管理者を明確にする。	
	(2)	運用のための手順書及び､情報セキュリティ事故に備え､事故時のための手順書を作成する。	
	(3)	使用するソフトウェアについて、信頼性の高い安全なものを導入する。	
	(4)	基本ソフトウェアのアクセス制御、ファイルのアクセス制御、業務用のソフトウェアの実行権限の制御等に関して､厳密なアクセス権を設定する。また、利用者に対して、必要最低限のアクセス権限のみ許可するようにする。	
	(5)	端末機等及び携帯端末を権限のない者に利用されないようにするため、正当な利用者 ID 及びパスワードを入力させるなど、サーバ等と接続された端末機等及び携帯端末の利用時には利用者の認証をする。	
7　情報システム運用時			具体的な状況
	(1)	製造元が提供する修正プログラム等を導入するなど､使用するソフトウェアを常に安全で正しく機能する状態で使用するよう努める。	
	(2)	通信経路の暗号化、通信回線の監視、ファイヤウォールやウイルス対策ソフトの導入など、安全な管理のために必要な対策を行う。	
	(3)	情報システムの管理・運用を行う者には、個人ごとに ID を発行し、それぞれに推測困難なパスワードを設定する。また､パスワードを短いサイクルで変更させる。	
	(4)	特に重要な権限を持つ利用者のパスワードは､漏れることのないよう厳重に管理する。	
	(5)	情報システムの保守の記録を残す。	
	(6)	個人情報を扱う情報システムでは、「個人情報を記録したシステムにおける端末機によるデータの更新､検索等の操作の記録に関する要綱」(アクセスログ要綱）に基づき、操作記録の採取を行う。	
	(7)	復元が容易なもの、重要性が低いものを除き、定期的にデータのバックアップを取得し、安全に保管する。また、障害時の代替品を用意するなど、障害発生時の対策を用意する。	
	(8)	端末機等及び携帯端末について、新規利用者の登録･既存利用者の利用者コード又はパスワード変更･利用者の登録抹消の申請を受けた場合には、正当性を審査し、速やかに対応する。	
	(9)	定期的に次のような検査を行い、不備が発見された場合には、速やかに是正する。また、検査結果は、必ず記録し、５年間保管する。 ア　脆弱性検査ソフトによる最新の脆弱性情報を含む検査 イ　情報システムの仕様書と実際の利用機器との整合性 ウ　不要なアクセス権が存在しないこと エ　不要なサービスの起動が存在しないこと オ　不要なアカウントが存在しないこと カ　推測されやすいパスワードが設定されていないこと	
	(10)	著作権を侵害することがないように､ソフトウェアのライセンス管理を適切に行う。	