個人情報の保護に関する安全管理措置の実施状況通知

令和　年　月　日

柏市長　宛

団体名

個人情報の保護に関する法律第６６条第2項の規定により準用する同条第１項に規定する安全管理のために必要かつ適切な措置とその実施状況について，下記のとおり実施していることを通知します。

	安全管理措置	内容	実施例	実施状況（○，×を記載）	備考
組織的安全管理措置	組織体制の整備	受注者において保有個人情報を保護するための体制を整備している	・組織体制の整備のため、総括保護管理者、保護管理者、保護担当者を設置する。		
	個人情報の取扱に係る規律に従った運用	保有個人情報の秘匿性等その内容に応じて、保有個人情報にアクセスする権限を有する職員の範囲と権限の内容を、当該職員が業務を行う上で必要最小限の範囲に限定している	・保護管理者は、職員のアクセス権限が業務上適切なものとなっているか、業務に必要がない権限が付与されていないか等を確認する。 ・職員の異動や配置転換等によりアクセス権限が不要となった場合には、アクセス権限の削除・無効化の措置を講じる。 ・職員が長期間にわたり休職している場合には、休職期間を考慮し、アクセス権限の削除・無効化の措置を講じる。		
	個人情報の取扱状況を確認する手段の整備	保有個人情報の秘匿性等に応じて、当該保有個人情報の利用及び保管等の取扱状況について記録している	・個人情報が記録された電子媒体等を外部に持ち出す場合や利用する場合は、その状況を記録する		
		保有個人情報の秘匿性等その内容に応じて、当該保有個人情報へのアクセス状況を記録し、その記録を一定の期間保存し、及びアクセス記録を定期的に分析するために必要な措置を講じている	・アクセス記録（ログ）の分析を行うためのマニュアルや手順書等を定める。 ・ログの分析は、職員が業務には関係がない特定の人物の個人情報の閲覧やデータの書き出し等をしていないか、深夜帯や休日などの時間帯に不正なアクセスをしていないか等の観点で分析を行う。 ・ログ分析の頻度は、毎月または隔月といった短い頻度で実施する。		
	漏えい等事案に対応する体制の整備	漏えい等事案の発生又は兆候を把握した場合に適切かつ迅速に対応するための体制を整備している	・漏えい等事案の発生に備え、漏えい等事案発生時の対応マニュアルや報告フロー図等を整備し、職員に周知する。		
	取扱状況の把握及び安全管理措置の見直し	保有個人情報の記録媒体や保管方法等について、定期に点検を行っている	・チェックリスト等を作成し、取扱い状況等の確認を行う。不備事項が認められた場合には、改善策を実行する。		
人的安全管理措置	教育研修	受託者における従事者に対して，個人情報の保護に関する研修を実施している	・研修実施計画を立て、従業員に周知する ・個人情報保護委員会作成の研修資料を配布する		
物理的安全管理措置	入退室の管理	保有個人情報を取り扱う基幹的なサーバ等の機器を設置する区域について，入退室の管理を行っている	・サーバ等の機器を設置する区域に立ち入る権限を有する者を定める。 ・入室用件の確認、入退の記録、部外者についての識別化、部外者が立ち入る場合の職員の立会い又は監視設備による監視、外部電磁的記録媒体等の持込み、利用及び持ち出しの制限又は検査等を行う。		
	第三者の閲覧防止	端末の使用に当たっては、保有個人情報が第三者に閲覧されることがないよう措置を講じている	・離席する際は，端末のログオフ処理を行う。 ・間仕切り等の設置、座席配置の工夫等を行い，のぞき込みを防止する		
	媒体の管理等	保有個人情報が記録されている媒体の保管及び運搬に関し，必要な措置を講じている	・保有個人情報が記録されている媒体を定められた場所に保管するとともに、必要があると認めるときは、耐火金庫への保管、施錠等を行う。 ・保有個人情報が記録されている媒体を外部へ送付し又は持ち出す場合には、原則として、パスワード等を使用して権限を識別する機能を設定する等のアクセス制御のために必要な措置を講じる。		
	端末の盗難防止等	端末の盗難又は紛失の防止のため、端末の固定、執務室の施錠等の必要な措置を講じている	・端末をワイヤーで固定し，盗難を防止する。		
	廃棄等	保有個人情報及び保有個人情報が記録された媒体を廃棄する際，適切な手法を採用している	・書類に関しては，焼却、溶解、適切なシュレッダー処理等の復元不可能な手段を採用する。 ・電子媒体に関しては，容易に復元できない手段を採用専用のデータ削除ソフトウェアの利用又は物理的な破壊等の手段を採用する。		
技術的安全管理措置	アクセス制御	情報システムで取り扱う保有個人情報の秘匿性等その内容に応じて、当該職員が業務を行う上で必要最小限の範囲で、アクセス制御のために必要な措置を講ずる。	・保有個人情報を取り扱うことができる情報システムの端末を限定する。 ・保有個人情報ファイルへのアクセス権を付与すべき者を最小化する。		
	アクセス者の識別と認証	アクセス制御のために、認証機能を設定する等の措置を講ずる。	機器に標準装備されているユーザー制御機能（ユーザーアカウント制御）により、保有個人情報を取り扱う情報システムを使用する担当職員を識別・認証する。		
	外部からの不正アクセス等の防止	保有個人情報を取り扱う情報システムに対する外部からの不正アクセス等を防止するための必要な措置を講じている	・情報システムと外部ネットワークとの接続箇所にファイアウォール等を設置し、不正アクセスを遮断する。 ・保有個人情報を取り扱う情報システムにセキュリティ対策ソフトウェア等を導入し、自動更新機能等の活用により、これを最新状態とする。		
	情報システムの使用に伴う漏えい等の防止	保有個人情報の秘匿性等その内容に応じて、暗号化及び分散保管その他必要な措置を講じている	・やむを得ずメール等により外部に保有個人情報が含まれるファイルを送信する場合は、当該ファイルへのパスワードを設定する。 ・やむを得ず保有個人情報が記録されている媒体を外部に持ち出す場合には、暗号化の処理を行う。		