個人情報の取扱いに関するチェックリスト（情報システムあり）

別紙４

事業者		委託業務	

業務受託時の個人情報（以下「保有個人情報」といいます。）の取り扱いについて、以下の項目について対応内容を記載されている中から番号でお答えください。
記載されている対応以外の定めにて同程度の対応ができる場合には、その他の欄に対応内容を具体的に記載ください。

No	項目	問	対応内容の該当番号を枠内に記載ください		4.その他 （具体的内容を記載ください）
1 規程の整備等					
1	規程の整備等	個人情報の適切な管理に関する定めを整備していますか。		1.組織全体に適用される規程を策定している 2.組織における個々の部署（局、部、課等）に適用される規程を策定している 3.特定の業務に携わる者のみに適用される規程（担当者マニュアル）を策定している 4.その他	
2 教育研修					
2	従業員に対する研修	1.個人情報の取扱いに従事する従業員等に対する教育研修について		1.着任時等個人情報を取り扱うこととなった最初に研修を行っている 2.毎年又は着任後数年おき等、一定の期間経過ごとに研修を行っている 3.昇任時や異動時等、一定の事象が起きるごとに研修を行っている 4.その他	
		2.研修方法について		研修方法について 1.e-learningを採用している 2.研修資料の作成、実施環境の整備、講師、受講状況の管理等、研修に関する何らかの業務を外部委託している（外部のセミナーを受講させている場合等も含む。） 3.その他	
		3.研修対象となる従業員について		1.従業員に対して実施している。 2.情報システムを管理する従業員に対して実施している。 3.保護管理者や保護担当者に対して実施している。 4.その他	
3	研修未受講者に対するフォローアップ	研修の受講状況の把握について		1.従業員に自己申告させている 2.受講したか否かが自動的に登録されるシステムを採用している 3.対面で実施し、出席者を記録している 4.外部セミナーの受講証等の写しを提出させている 5.その他	

No	項目	問	対応内容の該当番号を枠内に記載ください		4.その他 (具体的内容を記載ください)
3	個人情報の取扱い				
4		本委託業務上の目的で個人情報を取り扱う場合、保護管理者は、個人情報の複製・送信・記録されている媒体の外部への送付又は持ち出し(その他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を含む)の取り扱いの保護管理者から従業員への指示について		1.許可された端末以外ではUSBメモリやHDD等の外部記憶媒体へのデータの書き出しができないようにした上で、指示に従うこととしている。 2.許可された外部記憶媒体のみ端末への接続を許可し、指示に従うこととしている 3.個人情報が記載された書類を持ち運ぶ際は持ち出し記録簿に記帳し、指示に従うこととしている 4.その他	
5	誤りの訂正等	従業員が個人情報の内容に誤り等を発見した場合の、保護管理者の指示と訂正等について		1.従業員が誤り等を発見した場合の訂正手続を定めている 2.従業員が誤り等を発見した場合、自身だけの判断で訂正せず、まずは上長に一報するよう周知している 3.情報システム内の個人情報を従業員が訂正等をした場合、上長が許可しなければ当該訂正等が反映されないシステムを採用している 4.その他	
6	媒体の管理等	1.個人情報が記録されている媒体の保管に関する保護管理者から従業員への指示について		1.終業時には個人情報が含まれる書類等を机上に放置せず、必ず所定の場所に保管することとしている 2.USBメモリや外付けHDD等、電磁的記録媒体の保管場所が指定されている 3.特に機微性の高い個人情報については、施錠できるキャビネットや金庫に保管している 4.委託者へ提出前の個人情報が記録されている場合は、焼失等による消去がないよう耐火金庫等へ保管している 5.その他	
		2.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の、アクセス制御のために講じている措置について		(原則として、権限を識別する機能を設定するためのパスワード等[パスワード、ICカード、生体情報等をいう]を使用した上で) 1.USBメモリによる外部持ち出し時にはデータに手動でパスワードを設定するようルールを定めている 2.データ記録後端末から取り外したときに自動的にデータにパスワードが設定されるUSBメモリを使用している 3.あらかじめ登録した端末でしかデータを閲覧できないUSBメモリを使用している 4.その他	

No	項目	問	対応内容の該当番号を枠内に記載ください		4.その他 (具体的内容を記載ください)
7	誤送付等の防止	個人情報を含む電磁的記録又は媒体の誤送信・誤送付、誤交付、又はウェブサイト等への誤掲載を防止するための措置について		(個人情報を含む電磁的記録又は媒体の送信・送付・交付・誤掲載防止のための措置として) 1.必ず二者以上でのダブルチェックをするフローとしている 2.チェックリストを活用している 3.外部メールもしくは添付ファイルメールの送信時に一時保留する仕組みになっている 4.個人情報を含む添付ファイルは暗号化の上送信している 5.誤送信防止のための訓練をしている 6.その他	
8	個人情報の取扱状況の記録	個人情報の利用及び保管等の取扱いの状況の台帳整備と記録について		1.情報資産管理ソフトを用いている 2.紙媒体で台帳管理をしている 3.文書管理システム上で利用及び保管の記録をとっている 4.その他	
4 情報システムにおける安全の確保等					
9	アクセス制限	1.個人情報を取り扱うシステムや個人情報を含むデータへのアクセス権限の管理について		1.従業員ごとにアクセスできるシステムやデータを限定している 2.部課室や担当業務ごとにアクセスできるシステムやデータを限定している 3.誰がどのシステムやデータにアクセスできるか一覧化する等、容易に確認できる方法を備えている 4.人事異動と共にアクセス権限の付与や抹消が行われるシステムを採用している 5.不要な権限が付与されていないか、定期的に確認するルールとなっている 6.その他	
		2.個人情報を取り扱うシステムや個人情報が含まれるデータへのアクセスログについて		1.自動的にアクセスログが保存されるようになっている 2.アクセスログの保存を外部に委託している 3.その他	
	アクセス制御	3.個人情報(情報システムで取り扱うものに限る。)の認証機能を設定する等のアクセス制御のために必要な措置について		1.利用時間や利用時間帯によるアクセス制御をしている 2.同一主体による複数アクセスの制限をしている 3.接続元のIP アドレスを制限することで、接続できる端末を制限をしている 4.ネットワークセグメントの分割によるアクセス制御を行っている 5.秘匿性の高い情報が含まれる文書については暗号化している 6. 取り扱う必要のある従業員にのみ権限を付与している 7. 二要素認証を取り入れている 8.その他	

No	項目	問	対応内容の該当番号を枠内に記載ください		4.その他 (具体的内容を記載ください)
		4.アクセス権限の管理のためのパスワード等の管理に関する定めの整備(その定期又は随時の見直しを含む。)、及びパスワード等の読取防止等について		1.推測困難な複雑なパスワードを設定している 2.アクセス権が必要なくなった従業員については遅滞なくその権限を削除している 3.パスワードポリシーを策定している 4.その他	
10	アクセス記録	1.個人情報へのアクセス状況の記録・保存、及びアクセス記録の分析について		1.1～3か月間隔でアクセスログの分析を行っている 2.6か月以上の間隔でアクセスログの分析を行っている 3.アクセスログを1年間以上保存している 4.アクセスログを目視で分析をしている 5.アクセスログをシステムで分析をしている 6.その他	
		2.アクセス記録の改ざん、窃取又は不正な消去の防止に対する措置について		1.アクセスログにアクセスできる従業員を少数に限定している 2.アクセスログへのアクセス元のIPアドレスを限定している 3.その他	
11	アクセス状況の監視	個人情報への不適切なアクセスの監視のための、個人情報を含むか又は含むおそれがある一定量以上の情報が情報システムからダウンロードされた場合の措置について		(個人情報を含むか又は含むおそれがある一定量以上の情報が情報システムからダウンロードされた場合の警告表示機能とその設定の定期的確認等のため) 1.情報資産管理ソフトを使用している 2.定期的に設定の見直しをするルールにしている 3.定期的に委託先から運用報告を受けている 4.その他	
12	管理者権限の設定	情報システムの管理者権限の特権に関する不正な窃取による被害の最小化及び内部からの不正操作等防止のための、当該特権の最小化等の措置について		1.管理者権限をシステムごとに細分化している 2.管理者権限はごく限られた少数者にのみ付与している 3.その他	
13	外部からの不正アクセスの防止	個人情報を取り扱う情報システムへの外部からの不正アクセス防止のための、ファイアウォール等による経路制御等の措置について		1.ファイアウォールを設置している 2.ファイアウォールの設定を定期的に見直している 3.ネットワークに適切なアクセス制御を施している 4.その他	

No	項目	問	対応内容の該当番号を枠内に記載ください		4.その他 (具体的内容を記載ください)
14	不正プログラムによる漏えい等の防止	ソフトウェアに関する公開された脆弱性の解消、把握された不正プログラムの感染防止等に関する措置について		(導入したソフトウェアを常に最新の状態に保った上で) 1.脆弱性情報を定期的に確認している 2.外部から受領したデータをシステムに登録する際には不正プログラム感染の有無を確認する 3.セキュリティを外部に委託し、適時に脆弱性に対応させている 4.その他	
15	情報システムにおける個人情報の処理	1.一時的に加工等の処理を行うため複製等を行う場合の対象となる個人情報の範囲と、処理終了後の消去について		扱う個人情報の対象を必要最小限に限り、処理終了後の不要となった情報を速やかに消去することとした上で 1.紙媒体に印刷した個人情報は、ファイルにつづり込んだもの等保存が必要なものを除き当日中に裁断処理をしている 2.原則として個人情報の紙媒体への印刷はしないこととなっている 3.作業用に複製したデータの保存場所が指定されており、そこに保存されたデータは定期的にクリーンアップされる 4.その他	
		2.保護管理者による消去等の実施状況の確認について		1.不要な個人情報を保持していないか、保護管理者が課室内の従業員に対し定期的に声かけをしている 2.ファイルサーバー等共用部分に記録されている個人情報について、定期的に状況を確認し、不要なものは削除している 3.情報資産管理ソフトを用いて不要な個人情報が適時に消去されているか、定期的に確認している 4.機微性の高い個人情報については台帳を作成しており、それを用いて一定期間ごとに削除の要否を確認している 5.その他	
16	暗号化	暗号化について		1.ＨＤＤを暗号化している 2.特に秘匿性の高い情報を抽出し、その情報が保存されているデータベースを暗号化している 3.情報システムへのアクセス権限を付与した者のパスワードを暗号化している 4.その他	

No	項目	問	対応内容の該当番号を枠内に記載ください		4.その他 (具体的内容を記載ください)
17	記録機能を有する機器・媒体の接続制限	スマートフォン、USBメモリ等の記録機能を有する機器・媒体の情報システム端末等への接続の制限（当該機器の更新への対応を含む。）等について		（個人情報を取り扱う情報システム端末等へ接続する端末（当該機器の更新への対応を含む。）について） 1.端末には利用許可された媒体のみ接続可能としている 2.データは暗号化しパスワードを設定している 3.利用媒体は、全て管理し利用履歴を残している 4.データの受渡しには、必ず情報セキュリティ管理者の承認を受けることとし、その記録を残している 5.その他	
18	端末の限定	個人情報の処理を行う端末の限定について		1.秘匿性の高い個人情報を取り扱うための専用端末を設けている 2.秘匿性の高い個人情報についてはアクセス元のIPアドレスを制限している 3.その他	
19	端末の盗難防止等	1.端末の固定、執務室での施錠等について		1.端末をセキュリティワイヤーで固定している 2.端末を設置している執務室は施錠をしている 3.退庁時は端末を施錠できる机やキャビネット等の中に保管している 4.その他	
		2.従業員は、保護管理者が必要であると認めるときを除き、端末を外部へ持ち出し、又は外部から持ち込んではならないこととしていますか。		1.端末等の持ち出し及び持込みについて、記録を作成し、保管している 2.端末等の持ち出し及び持込みが必要なときは上長の許可を得なければならない 3.その他	
20	入力情報の照合等	入力原票と入力内容との照合、処理前後の当該個人情報の内容の確認、既存の個人情報との照合について		1.入力時にダブルチェックをしている 2.システムや表計算ソフト等のツールを利用している 3.その他	
21	バックアップ	バックアップの作成及び分散保管について		1.オンラインでバックアップデータを収集し分離したネットワークに保存している 2.オフラインでバックアップデータを保管している 3.磁気テープを使用してバックアップをしている 4.その他	
22	情報システム設計書等の管理	個人情報に係る情報システムの設計書、構成図等の文書の保管、複製、廃棄等について		（個人情報に係る情報システムの設計書、構成図等の文書について外部に知られないために） 1.アクセスできる者を必要最小限に限定している 2.暗号化もしくは鍵のかかるキャビネット等で保管している 3.耐火、耐熱、耐水及び耐湿を講じた施錠可能な場所に保管している 4.保管又は保存場所を一定の範囲の者にのみ伝えている 5.その他	

No	項目	問	対応内容の該当番号を枠内に記載ください		4.その他 (具体的内容を記載ください)
5 情報システム室等の安全管理					
23	入退管理	1.情報システム室に立ち入る際の、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従業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について		1.入退室を許可された者のみに制限している 2.IC カード、指紋認証等の生体認証や入退室管理簿の記載による入退室管理を行っている 3.外部からの訪問者が入室する場合には、入退室を許可された従業員等が付き添うものとし、外見上従業員等と区別できる措置を講じている 4.関連しない、又は個人所有であるコンピュータ、モバイル端末、通信回線装置、電磁的記録媒体等を持ち込ませないようにしている 5.その他	
		2.個人情報を記録する媒体を保管するための施設（以下「保管施設」という。）を設けている場合について		1.情報システム室と同じ措置を講じている 2.その他	
		3.情報システム室・保管施設の出入口の特定化について		1.出入口は一か所にとどめている 2.所在表示は最小限にしている 3.その他	
		4.情報システム室等及び保管施設の入退の管理に関するパスワード等の読取防止等の」について		立入りに係る認証機能を設定し、及びパスワード等の管理に関する定めの整備（その定期又は随時の見直しを含む。）、パスワード等の読取防止等を行うために必要な措置を講じていますか。 1.ICカードによる認証を設定している 2.指紋認証等の生体認証を設定している 3.パスワードによる認証を設定している 4.その他	
24	情報システム室等の管理	1.外部からの不正な侵入に備えた、情報システム室・保管施設等の措置について		1.施錠装置を設置している 2.警報装置を設置している 3.監視設備を設置している	
		2.災害等に備えた、情報システム室・サーバ等の機器の予備電源・配線等の措置について		1.サーバ等の予備電源を確保している 2.配線の損傷防止等の措置を講じている 3.代替機を用意している 4.自動消火装置を設置している 5.その他	

No	項目	問	対応内容の該当番号を枠内に記載ください		4.その他 (具体的内容を記載ください)
6 安全管理上の問題への対応					
25	事案の報告及び再発防止措置	1.個人情報の漏えい等安全管理の上で問題となる事案又は問題となる事案の発生のおそれを認識した場合の措置について		1.漏えい発生時に直ちに保護管理者に報告するためのマニュアルが整備されている 2.漏えい発生時の報告方法等を定期的にメールで周知している 3.漏えい発生時の報告方法を定期的に掲示板等（従業員のポータルサイト等を含む）で周知している 4.その他	
		2.漏えい等事案が発生した場合の被害の拡大防止又は復旧、外部からの不正アクセス・不正プログラムの感染時の被害拡大防止について		1.漏えい発生時に速やかに被害の拡大防止又は復旧等のために対応できるようマニュアルを整備している 2.漏えい等が発生した場合に備えて訓練を行っている 3.CSIRTを設置し、CSIRTに連絡するよう教育している 4.委託業務を行う従業員の内、最低一人はセキュリティ研修を受けさせている 5.その他	
		3.保護管理者は、漏えい等事案が発生した場合、当該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とともに、同種の業務を実施している部局等に再発防止措置を共有することとしていますか。		1.事案が発生した場合は、原因を分析の上マニュアルやルールの見直しを行っている 2.事案が発生した場合は、部局内で共有している 3.必要に応じて専門家に相談できる体制を構築している 4.CSIRTを設置している 5.その他	