

#### 4 外部結合にかかる個人情報保護対策チェックリスト

|                          | ・対策が可能であれば「○」<br>・対策の必要がない場合は「ー」         | 情報保護対策  |
|--------------------------|--|---|
| 区が行う情報保護対策<br>【運用上の対策】   | ○  | 個人情報保護法及び新宿区情報セキュリティポリシーを遵守するよう指導する。また、クラウドサービスを利用する場合は、総務省「クラウドサービス提供における情報セキュリティ対策ガイドライン」を準拠するよう指導する。 |
|                          | ○  | 必要に応じて、事業者への立入り調査等を実施するとともに、結合先に対し速やかに状況報告をするよう指導する。  |
|                          | ○  | システム上で不要となった電子データを削除し、電子データの消去を行ったことの報告書を提出するよう指導する。  |
|                          | ○  | 業務開始前に、事故、災害、トラブルに対応できる体制及び手順を整備し、結合先と緊急時の連絡体制や対応手順を確認する。   |
|                          | ○  | 事故が発生した場合又は個人情報保護及び情報セキュリティ対策の変更があった場合は、直ちに結合先と今後の対応を協議する。  |
| 区が行う情報保護対策<br>【システム上の対策】 | ○  | 接続するネットワークについては、特定相手以外との通信を不可とする。   |
|                          | ○  | ネットワーク機器やサーバを制御し、通信できるシステムを限定する。  |
|                          | ○  | 通信内容は暗号化し、通信途上の個人情報の盗用、改ざん、成りすましを防止する。  |
|                          | ○  | ファイアウォールの設置、サーバの要塞化、侵入検知、セキュリティパッチの適用等の対策を講じ、外部からの不正侵入やデータ破壊・漏えい等各種の攻撃から防御する。                           |
|                          | ○  | コンピューターウイルス感染等がないよう、ウイルス対策ソフトウェアの導入及び最新のパターンファイルを適用する。  |
|                          | ○  | ID・パスワードやアドレス情報による運用により、第三者による個人情報の盗用、改ざん、成りすましを防止する。   |
|                          | ○  | 個人情報を保存する場合は、保存先フォルダへアクセス権を設定するとともに、ファイルにパスワードを付すなど、情報へのアクセス制御を徹底する。                                    |
|                          | ○  | システム・ネットワークの状態、機器操作、サービス利用等の監視及びアクセスログ等を取得する。取得したログは、定期的に分析する。  |
|                          | ○  | サーバ冗長化、バックアップ等により、事故や障害発生時におけるシステム稼働体制を整備する。  |
|                          | ○  | 入退室管理等により情報資産の危殆化を防止する。   |
| ○                        | システムを提供するサーバは日本国内の法が適用される安全性が確保された環境にする。 |   |