資料１－４

個人情報の保護措置

１　相手方の対応措置に関する基準

オンライン結合による個人情報の提供を受ける実施機関以外のもの（以下「相手方」という。）に個人情報保護のための制度が整備されていると認められ、又は提供された個人情報を保護するために適切な措置が講じられていると認められること。

<table>
<tr><th></th><th>千葉県
（千葉県オンライン結合の基準）</th><th>千葉市
（千葉市個人情報オンライン結合基準）</th></tr>
<tr><td>項　目</td><td>内　容</td><td>内　容</td></tr>
<tr><td rowspan="2">１　全般的な措置に関する項目</td><td>相手方が電子計算機処理される個人情報に関しての次の事項を定めた条例、規則、要綱等の規程を制定していること又は、当該オンライン結合により提供される個人情報について次の事項を明記した覚書等を取り交わすこと
ア 目的外の利用及び提供の禁止
イ 個人情報を取り扱う職員の責務
ウ 不要となった個人情報の確実な廃棄
エ その他個人情報保護のために必要な措置</td><td>相手方が電子計算機処理される個人情報に関しての次の事項を定めた条例、規則、要綱等の規程を制定していること又は、当該オンライン結合により提供される個人情報について次の事項を明記した覚書等を取り交わすこと
ア 目的外の利用及び提供の禁止
イ 個人情報を取り扱う職員の責務
ウ 不要となった個人情報の確実な廃棄
エ その他個人情報保護のために必要な措置</td></tr>
<tr><td colspan="2">上の説明：別紙「千葉県森林クラウド利用要領」のとおり。</td></tr>
<tr><td rowspan="4">２　管理的な措置に関する項目</td><td>端末機の管理について適切な措置が講じられていること。
『方策の例』
ア 端末機の管理責任者を定めること。
イ 端末機の使用状況を監視し、及び記録すること。</td><td>電子計算機の管理について、次のような適切な措置が講じられていること。
ａ 電子計算機処理の管理責任者を定めること。
ｂ 電子計算機の使用状況を監視し、及び記録すること。</td></tr>
<tr><td colspan="2">上の説明：別紙「千葉県森林クラウド利用要領」のとおり。</td></tr>
<tr><td>ファイルへの不当なアクセスを防止するため適切な措置が講じられていること。
『方策の例』
ア 無資格者によるアクセスを制限するため原則としてパスワード及びIDカード等が必要なシステムとすること。
イ パスワードが画面に表示されないようにすること。
ウ 端末機は専用回線で接続するか、若しくは、端末機が公衆回線により接続する場合は端末機の確認機能を設けること。
エ 相手方のアクセスをデータの必要箇所のみに制限する機能を設けること。</td><td>個人情報への不当なアクセスを防止するため、次のような適切な措置が講じられていること。
ａ 個人情報へのアクセスの資格を定めること。
ｂ アクセスの資格を確認するためのパスワード、ＩＤカード等が不正に使用されることがないように次のような措置をとること。
（ａ）パスワード、ＩＤカード等の管理者を指定すること。（ｂ）ＩＤカード等の発行手続を明確にすること。（ｃ）有資格者が資格を失ったときは、直ちにその資格を抹消すること。（ｄ）パスワードを他人に知られ、又はＩＤカードを紛失する等の事故があったときは、直ちにそれらの措置を無効とする手段を定めておくこと。（ｅ）その他</td></tr>
<tr><td colspan="2">上の説明：別紙「千葉県森林クラウド利用要領」のとおり。</td></tr>
</table>

２　実施機関が講ずる技術的措置に関する基準

オンライン結合を行うことにより個人情報の改ざん、滅失、き損、漏えい等の危険が生じないようにするために、実施機関において次のようなハードウエア上及びソフトウエア上の適切な措置が講じられていると認められること。

<table>
<tr><th></th><th>千葉県
（千葉県オンライン結合の基準）</th><th>千葉市
（千葉市個人情報オンライン結合基準）</th></tr>
<tr><td>項　目</td><td>内　容</td><td>内　容</td></tr>
<tr><td rowspan="2">１不正アクセスの排除に関する項目</td><td>ファイルへの不正なアクセスを排除するための適切な技術的措置が講じられていること。</td><td>ファイルへの不正なアクセスを排除するための適切、かつ、技術的措置が講じられていること。</td></tr>
<tr><td colspan="2">上の説明［技術的措置］
１ システム構成及びファイアウォール：本システムは、LGWAN（総合行政ネットワーク）-ASP サービス提供事業者により、システムサーバへはファイアウォールを経由しなければ到達できない構成とする。データセンターファシリティスタンダードにてティア３相当以上であるデータセンター上に構築する。
２ アクセス権限の管理：管理権限を持つ職員において、各ユーザの業務権限レベルやレベルによる業務機能の使用可否及び利用可能なデータの範囲の設定を可能とする業務権限設定機能を実装する。
３ システム監視：サービス提供事業者は、監視システムを利用し、本システムの稼働状況及び利用状況等を監視し、障害対応時はその結果や収集したログ等を分析して内容を報告するものとする。
４ ウイルス対策：システムサーバにはウイルス対策ソフトを導入し、常に最新の状態を保つと共に、ＯＳ・アプリケーションについても対策プログラムなどの反映を随時行う。ウイルス対策ソフトは、データをサーバに登録する際にリアルタイムでチェックを行い、最低一日一回の定時ウイルスチェックを行う。</td></tr>
<tr><td rowspan="4">２障害時の予防、回復に関する項目</td><td colspan="2">１ 障害時のファイルの安全性を確保するための適切な技術的措置が講じられていること。</td></tr>
<tr><td colspan="2">上の説明
１ ネットワーク：機器等は冗長化を行い、単一障害点（その箇所が停止するとシステムの全体が停止するような箇所）を作らない。
２ 電源：サーバ機器等は無停電電源装置を装備し、障害時等における電源が確保されている。</td></tr>
<tr><td colspan="2">２　障害を速やかに回復するために適切な措置が講じられていること。</td></tr>
<tr><td colspan="2">上の説明
24 時間365 日機器の稼働監視を実施し、障害が発生した場合には、休日・深夜を問わず、即座に復旧体制を整備し、問合せ対応を行う障害対応窓口を運用する。また、障害が発生した場合において、障害発生前に取得したバックアップ情報が復元できることを保証するものとする。</td></tr>
</table>