資料１－３

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。

項　目	千葉市 （千葉市個人情報オンライン結合基準）	八千代市 （八千代市個人情報オンライン結合基準）
１　全般的な措置に関する項目	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	オンライン結合により相手方に提供される個人情報に関して，次の事項について個人情報の保護に関する定めがあるか，定めがない場合には，個人情報の保護について覚書等を取り交わすこと。 ①　目的外の利用及び提供の禁止 ②　個人情報を取り扱う事務に従事している者の責務 ③　不要となった個人情報の確実な廃棄 ④　その他個人情報保護のために必要な事項
２　管理的な措置に関する項目	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。	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と認められること。 ア　電子計算機処理の管理責任者を定めること。 イ　電子計算機の使用状況を監視し，及び記録すること。 ウ　その他個人情報保護のために必要な措置
	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	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と認められること。 ア　個人情報へのアクセス資格を定めること。 イ　アクセス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。 (ｱ)　パスワード，ＩＤカード等の管理者を指定すること。 (ｲ)　ＩＤカード等の発行手続きを明確にすること。 (ｳ)　有資格者が資格を失ったときは，直ちに資格を抹消すること。 (ｴ)　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，直ちに無効とする手続きを定めておくこと。 (ｵ)　その他パスワードについては，次のような措置をとること。 ａ　適宜変更し，かつ，推測が困難なものとすること。 ｂ　他人に教えないよう徹底すること。 ｃ　書き留めておかないよう徹底すること。 ウ　その他個人情報保護のために必要な措置
	八千代市においても、千葉市とほぼ同様の規定となっている。 また、事務局を担うフェリカポケットマーケティング㈱への業務委託契約においても、両市ともに個人情報取扱特記事項を定めている。	

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>項　目</th><th>千葉市
（千葉市個人情報オンライン結合基準）</th><th>八千代市
（八千代市個人情報オンライン結合基準）</th></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、かつ、技術的措置が講じられていること。
（ア）無資格者によるアクセスを禁止するため、原則としてパスワード、ＩＤカード等の措置が講じられた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）通信回線は専用回線とするか、公衆回線とする場合は、接続する相手方を確認する機能を確保すること。
（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>ファイルへの不正なアクセスを排除するため，次のような適切な技術的措置が講じられていること。
①　無資格者によるアクセスを禁止するため，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。
②　パスワードが画面に表示されないようにすること。
③　電子計算機は専用回線で接続するか，若しくは，電子計算機を公衆回線により接続する場合は，接続する相手方の確認機能を設けること。
④　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。
⑤　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［技術的措置］
１システム構成及びファイアウォール：Microsoft Azureの「App Service Environment」を利用しており、Azure Storage に書き込まれるすべてのデータ（メタデータを含む）は、Storage Service Encryption (SSE) を使用して自動的に暗号化されます。 File Server及びDatabaseへのアクセスではファイアウォールで特定のIPアドレスからのみアクセス可能としている。
２アクセス権限の管理：ログイン時にID・パスワードを利用し、各ユーザの業務権限レベルを設け、レベルによる業務機能の使用可能及び利用可能なデータの範囲の設定を可能とする機能が利用できる。外部からのAPIを利用した Azure Storageへのファイル取得では、制限付アクセス権を付与する Shared Access Signature (SAS)を利用し指定した期間のみリソースへのアクセスを許可する。
３システム監視： Azureのシステム監視を利用し、CPU,DTU, Database等を監視しアラートを検知または障害対応時は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： Microsoft Azure のPaaSサービスを利用してシステムを構築しており、ウイルス対策はMicrosoft社により、迅速・高度に保護されている。</td></tr>
<tr><td rowspan="3">２障害時の予防、回復に関する項目</td><td>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。
ａ　機器の能力及び容量を越えないように負荷状態を監視し、又は把握できる機能を設けること。
ｂ　更新が終わるまで同一のファイルに対する他のアクセスを禁止する機能を設けること。</td><td>１ 障害時のファイルの安全性を確保するため，次のような適切な措置が講じられていること。
ア　機器の能力及び容量を越えないように負荷状況を監視し，又は把握できる機能を設けること。
イ　更新が終わるまで同一のファイルに対する他のアクセスを禁止する機能を設けること。</td></tr>
<tr><td colspan="2">上の説明
Microsoft Azure Storageを利用しており、Azure Storage内のデータはハードウエア障害やネットワークの停止または停電などから保護するために常にレプリケートし持続性・高可用性が保証されている。また、Azure Storageは格納データの整合性を定期的に検証し、データの破損が検出された場合は、冗長データを使用され復元される。</td></tr>
<tr><td>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。
ａ　回線の接続状況等システムの運転状況を把握する機能を設けること。
ｂ　定期的にデータのバックアップ及びバックアップ時以降の更新データを保存する等の措置を行い、障害発生時にはこれらのデータをもとに速やかにシステムを回復させる機能を設けること。</td><td>２　障害を速やかに回復するため，次のような適切な措置が講じられていること。
ア　回線の接続状況等，システムの運転状況を把握する機能を設けること。
イ　定期的にデータのバックアップ及びバックアップ時以降の更新データを保存する等の措置を行い，障害発生時には，これらのデータを基に速やかにシステムを回復させる機能を設けること。</td></tr>
<tr><td colspan="2">上の説明
Azureのシステムによる稼働監視は24時間365日実施し、障害が発生した場合は、平日の09:30～18:00で復旧体制を整備し対応を行う。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 Azureの機能で復元できることを保証している。</td></tr>
</table>