資料１－１

# ヒアリング結果概要

## （市町村）（４団体）

| ヒアリング事項 | | 回答内容の概要 |
|---|---|---|
| 1 | セキュリティ確保のための措置の規定の有無 | ・条例・セキュリティポリシーで確保措置を規定し、これらの規定を踏まえ、具体的に遵守すべき事項を契約の中で規定している。 |
| 2 | セキュリティ基準遵守のためのチェックの状況 | ・立ち入り調査の権限は有するものの、実際には行っていないなど、チェックは必ずしも十分に行われているとは言えない。 |
| 3 | データ統合などの電算処理業務を市町村職員が直接処理する可能性。 | ・専門性及び効率性の観点から困難としている。 |
| 4 | 委託先選定基準の内容 | ・認証取得などのセキュリティ対策の状況・サポート体制などを考慮し、決定。<br>・地域によっては、事実上事業者を選択する余地がない場合もある。 |
| 5 | データ処理の場所 | ・市町村が指定する場所（庁舎内）で行うことが原則。<br>・例外的に事業者の作業所で処理することもある。<br>・契約に明示していることが通常だが、個別に取り決める場合もある。<br>・作業員の自宅等における処理は認められていない。 |
| 6 | 作業場所の管理 | ・契約上規定されている職員による立ち会いが行われている。<br>・人員配置の問題や実際上目視できるため、立ち会いを行っていない場合もある。<br>・深夜帯などは立ち会わないこともある。<br>・厳格な入退室管理が通常。実態的に把握できるとして、厳格に行っていない場合もある。 |
| 7 | 作業員の特定 | ・作業予定者の事前通告や社員証による確認による。<br>・上記の確認は、契約に定められている場合といない場合がある。 |
| 8 | データのコピーや持ち出しに関する規制の有無、規制の方法。 | ・個人情報保護条例や契約により規制している。<br>・操作ログ記録の確認によりチェック。 |
| 9 | 委託業務終了後のデータの返還・抹消の確認の方法。 | ・契約上、業務終了後データの返還や廃棄が定められている。<br>・報告書による市町村への通知。 |
| 10 | 電算処理業務における再委託の有無、再委託業者に対する管理の方法。 | ・再委託は行われていない。（２団体）<br>・保守業務などベンダーで対応できない場合があるため再委託を前提に契約を行っている。<br>・再委託を行う場合は、事前申請を要する。<br>・再委託業者の管理は、基本的に委託業者が行う。 |

| | | |
|---|---|---|
| 11 | 電算処理業務における派遣職員活用の有無、派遣職員の管理の方法。 | ・派遣職員は活用していない団体が多い。<br>・活用している団体（ＳＥの派遣の例あり）は、職員立ち会いのもと作業。入退室管理簿、ＩＣカードによる管理。鞄等の持ち込みは禁止。 |
| 12 | 委託業者による派遣職員活用の有無。 | ・活用していない団体が多い。<br>・活用している団体は、派遣元の身分等を明確にし、業務内容、体制の報告を受領。 |
| 13 | 電算処理業務の再委託を全面的に禁止した場合の影響。 | ・特に問題ないとする団体もあるが、地理的な条件から大企業に限ると迅速なサービスが受けられなくなる可能性があるという団体もあった。<br>・上記のような場合でも、大企業と地元企業が企業組合（ＪＶ）を作って契約の主体となれば有効。 |
| 14 | 条例、契約違反の場合のペナルティなどについての条例、契約等の規定 | ・個人情報保護条例における罰則。<br>・損害賠償については、契約上で規定。<br>・入札参加資格の停止措置。 |
| 15 | その他 | ・委託業者の作業内容を職員がチェック・記録することをルール化するのは、職員の知識、技術を考えると一般的に困難。<br>・外部委託を行う場合、セキュリティ監査やシステム監査は必要と考えているが、財政面の問題もあり、なかなか難しい。<br>・データ持ち出しの際の暗号化は必要と認識。ただし、委託コスト、データ破損の可能性等の考慮が必要。 |

（ベンダー）

| ヒアリング事項 | | 回答内容の概要 |
|---|---|---|
| 1 | システム開発やデータ処理等の委託（請負）業務実施に当たり、情報セキュリティの確保、特に個人情報保護の観点から遵守すべき事項を定める社内規程の内容。 | ・社内の情報の取扱いを定めた情報管理規程の下に、個人情報に関する個人情報管理規程等を規定。 |
| 2 | 契約締結から契約に基づく個々の業務実施、完了確認に至るまで、１の社内規程はどのように反映されているのか。 | ・契約締結に際しては、顧客情報安全確保のための基本条項（作業場所からの情報持出の禁止、秘密保持等）を盛り込んでいる。<br>・作業を行うメンバーへの教育、作業場所の指定、当該作業場所への入退出管理、データへのアクセスコントロール等を行っている。 |
| 3 | 市町村合併に伴うデータ移行を行う場合の人員等の作業体制。 | ・地方公共団体の規模や移行作業の期間によって異なる。 |
| 4 | 市町村との業務の受託又は請負業務に関する契約は、支社、支店において行うのか。その際の契約の責任主体。 | ・市町村との契約は、支社、支店で行っている。契約の責任主体は、法人としての会社。 |
| 5 | 支社、支店の契約締結、業務実施に当たり、上記の社内規程の遵守についての本社のチェック体制。子会社、関連会社の場合はどうか。 | ・支社・支店の契約についても、社内規程によりチェック、又は本社スタッフとの連携によりチェック。<br>・契約の主体が関係会社の場合はそれぞれの規程による。ただし、会社本体から委託している場合は、会社本体の規程による。<br>・子会社・関連会社については、自主点検を行うよう指導。本社からの委託の場合は、立ち入り監査を行う。 |
| 6 | 作業場所の確保方法。 | ・個人情報を取り扱う作業を実施する場合は、顧客の側で作業場所を確保。 |
| 7 | 庁舎内で作業ができない場合の作業場所。 | ・個人情報を取り扱う作業を実施する場合は、庁舎内作業とする。<br>・顧客と同意の上、セキュリティの確保される場所で行う。 |
| 8 | 作業を管理している者 | ・幹部職員又は管理職員。 |
| 9 | 作業員を特定するための対策 | ・作業員名簿を顧客に提示し、顧客の入退室管理のもと作業を実施。 |
| 10 | データが過失等により流出した場合における被害を縮小するため、データの暗号化などの対策を行っているのか。行っている場合、どのような | ・原則として顧客先で作業を実施し、個人情報は持ち出さないこととしているが、どうしても持ち出しが必要な場合は、個人が特定できないよう顧客において加工。<br>・データの暗号化の措置。 |

| | | |
|---|---|---|
| | 対策か。 | |
| 11 | データの移行作業に伴い、データのバックアップは頻繁に行われているのか。データのバックアップを制限することについてどのように考えるか。 | ・作業のスケジュール等個々の状況によって、データのバックアップの頻度は変わる。<br>・顧客先で作業を実施しているため、バックアップ作業の制限は行っていない。<br>・データ保全の観点からバックアップの制限は難しい。 |
| 12 | 委託業務終了後のデータの返還・抹消の確認はどのように行っているか。 | ・顧客の立ち会いのもと返却又は消去を行う。 |
| 13 | 再委託、再々委託は一般的に行われているのか。協力会社に応援を頼んだり、協力会社から派遣社員を受け入れることは一般的に行われているのか。 | ・基本的には顧客との契約による。 |
| 14 | 再委託する場合、情報セキュリティの確保、個人情報保護の観点から再委託先の要件等についての定めがあるのか。 | ・顧客との契約にもよるが、基本的に会社の責任で請け負っている場合、会社として委託先にも同様の情報管理を義務付けた契約を締結。委託先に対しても、教育や情報セキュリティ監査を実施。<br>・教育については自社従業員に対するものと同様 |
| 15 | 再委託、再々委託を禁止した場合に生じる問題。その場合、どのような対応をとることが考えられるか。 | ・再委託禁止となった場合、人員の問題により、請け負えない場合が発生する可能性がある。<br>・地場産業振興の観点からの地場のＩＴ企業との協業が行いにくくなる。<br>・コンソーシアム形式の契約か、業務を細分化して、業務単位で個別に契約を行うこととなるが、顧客にとっては煩雑な事務が発生する。 |