「地方公共団体における業務の外部委託事業者に対する個人情報の管理に関する検討」

報告書

平成 21 年 3 月

総務省

＜目次＞

1 はじめに

1-1 背景

近年、複数の地方公共団体において、業務の外部委託事業者から個人情報が漏洩する事案が発生している。

これまでも「地方公共団体における情報セキュリティポリシーに関するガイドライン（平成 18 年 9 月全部改訂・総務省）」（以下、「情報セキュリティポリシーガイドライン」という。）や「地方公共団体における情報セキュリティ監査に関するガイドライン（平成 19 年 7 月全部改訂・総務省）」（以下、「情報セキュリティ監査ガイドライン」という。）等、情報セキュリティ対策に関する様々なガイドラインが策定されてきた。また、各地方公共団体においても、情報セキュリティポリシーの策定や個人情報保護条例の制定などの様々な取組が自主的に行われてきた。しかしながら、従前、業務部門にもわかりやすい手段や方法論が提供されてこなかったことなどにより、各地方公共団体においては、個人情報漏洩防止対策の実効性に関する悩みを抱えてきたものと考えられる。具体的には、特に個人情報を取り扱う業務を外部委託するに当たっては、先述のガイドライン等が求めるような地方公共団体内部で個人情報を取り扱う場合と同等の対策を、外部委託先に対して求め、対策を実施させることが必要であるにもかかわらず、それを実現するための手段が提供されていなかった。

また、外部委託において業務の所管部門と契約部門が分かれていることによって、外部委託先における個人情報保護対策がおろそかになっている側面もある。具体的には、個人情報を実際に取り扱っているのは個々の業務部門であり、その業務に携わる個々の職員が、業務で取り扱う個人情報の重要性を理解した上で、必要な注意を払うことが個人情報を保護するためには不可欠であるにもかかわらず、多くの地方公共団体では、個人情報保護条例などの制度面は総務・広報部門が担い、コンピュータシステムのセキュリティに関する部分においては情報政策部門が担い、実際の業務は各業務部門が担うという構造になっている。その結果、それぞれの部門が各々の役割を果たしつつも互いに連携した上で、個人情報保護対策を実施するという仕組が十分に構築されているとは言えない。（「図表 1-1 多くの地方公共団体における各部門の個人情報保護」参照）

図表 1-1 多くの地方公共団体における各部門の個人情報保護への関わり方

		情報政策部門	業務部門	総務・広報部門
制度	個人情報保護条例	△ （システム面）	◎ （個々の業務）	○ （とりまとめ）
	情報セキュリティポリシー	○ （とりまとめ）	◎ （個々の業務））	―
個人情報の取扱	文書管理規定の対象となる文書	―	◎ （個々の業務）	○ （規定のとりまとめ）
	電子データ	○ （取扱制限等の指定）	◎ （個々の業務）	△

◎主たる実施部門、○規定等のとりまとめ、△必要に応じて関わる部門

さらに、システムの構築・利用形態の変化が、職員のセキュリティに対する意識の定着やセキュリティ確保に必要な知識や技術の獲得の妨げになっている。たとえば、ホストコンピュータからオープンシステムへ移行した地方公共団体では、情報政策部門が担っていた役割を業務部門が担うようになっていることが多い。その結果、業務部門が業務システムの予算化から企画・開発・運用を担い、情報政策部門は全庁的な基幹ネットワークや職員用パソコンなどのインフラの整備・運用を担うというように役割分担されるようになった。そのような団体では、個々の業務部門で利用するシステムに関しては、外部委託事業者との契約内容や仕様などについて情報政策部門を通さず、個別に業務部門が契約を締結していることが多い。

そのような状況下では、ホストコンピュータからの移行時（開発時）には、担当する職員も開発を経験する過程で専門的な知識を学んでいるが、運用時にそのような知識のある職員が異動した結果、専門的な知識を前任者ほどは習得していない職員が後任になることが多く、運用年次を重ねる毎に職員の専門的な知識が風化してしまい、本来ならば職員が持つべきセキュリティに関する統制力を、職員よりも長く業務システムに関わっている外部委託事業者に依存せざるを得ない状況を生じさせることとなる。このように外部委託先への統制力が弱まった結果、個人情報漏洩の事案につながる場合が多いと考えられる。

このような傾向を憂慮し、情報政策部門が積極的に業務部門と連携し、業務システムの開発・運用の適正性や外部委託事業者への必要な指導を行うなど、団体として外部委託事業者へ過度に依存しないよう取り組んでいる団体もある。しかしながら、多くの団

体は、その必要性を理解していても情報政策部門の要員が少ないことなどにより十分な対応ができない状況である。

一方で先述のとおり、業務部門では業務システムの運用に携わる職員であっても情報システムに関する知識や情報セキュリティに関する理解が十分ではないことが多く、団体の個人情報保護条例や情報セキュリティポリシーが求める安全確保の措置の実施や外部委託先の管理などが十分に行われていないことが少なくない。

このような地方公共団体自身の問題に加えて、ICT に関する業界の商習慣が外部委託先における個人情報漏洩の事案発生に拍車をかけていると考えられる。具体的には、企業の規模に関わらず関連会社や子会社へ業務の一部を再委託あるいは再々委託することが常態化しており、発注者である地方公共団体が外部委託先に対して積極的に関与し、必要な働きかけを行わないと、必要な個人情報保護の実効性が確保されにくい状況がある。しかしながら、先述のとおり地方公共団体の外部委託先への統制力が弱まっているため、ICT 業界の再委託及びその繰り返しが常態化する中では、個人情報漏洩事案の発生は必然とも考えられる。

以上の地方公共団体における情報システム関連業務の現状及び ICT 業界の現状から、情報政策部門だけでなく、業務部門の職員も含めて、外部委託事業者に対する個人情報の管理のあり方を見直す必要がある。もっとも、外部委託先が原因となった情報漏洩事案は情報システム関連業務を請け負う ICT 業界のみで発生しているわけではなく、例えば、水道メータの検針業務など情報システムと関連性の薄い業務でも発生している。したがって、委託元である地方公共団体と外部委託先との間で、情報システム関連業務以外の業務においても情報システムに関する外部委託業務で挙げたような問題が存在するのであれば、情報システム関連業務と同様に、外部委託事業者に対する個人情報の管理のあり方を見直す必要がある。

（「図表 1-2 地方公共団体で外部委託先が原因となった主な情報漏洩事案の例」参照）

図表 1-2 地方公共団体で外部委託先が原因となった主な情報漏洩事案の例

時期	概要
平成 19 年 5 月	外部委託事業者の再委託先従業員が、住基データ約 7 万件等を自宅に持ち帰り、ファイル交換ソフトを通じて流出
平成 19 年 9 月	住民基本台帳ネットワークシステムの操作者用 IC カードを外部委託事業者が一時紛失

平成 20 年 1 月	業務委託を受けた事業者が 28,000 件の個人情報を含む USB メモリを紛失
平成 20 年 2 月	水道局の検針業務を受託した事業者が 13 件の個人情報を紛失
平成 20 年 3 月	委託している事業者の再委託先が 25 件の個人情報を紛失
平成 20 年 3 月	水道検針を委託している事業者が、検針用の個人情報を自らの販促活動に流用してダイレクトメールを送付
平成 20 年 7 月	G 県から委託を受けた事業者が、外部委託業務が終了したにもかかわらず、使用したパソコン内のデータを抹消するのを怠ったため、別の作業で使用している際に、第三者に不正に閲覧された
平成 20 年 8 月	胸部レントゲン検診の受診者 253 人分の個人情報の入った FD を検診の外部委託事業者に手渡したが、当該事業者が当該 FD を紛失
平成 20 年 9 月	県立病院の保守業務を委託している事業者の担当者が、外部記憶装置を無許可で持ち出し、ファイル交換ソフトを通じて流出
平成 20 年 11 月	教育委員会がシステム開発を委託している事業者の下請事業者の従業員が、個人情報 11 万件を自宅に無断で持ち出し、ファイル交換ソフトを通じて流出
平成 21 年 2 月	水道局お客さまサービスセンターの運営業務を委託されている事業者の下請事業者に属するオペレータが、料金オンラインシステムを不正に操作し、個人情報を第三者に漏洩

具体的な改善の方向性としては、地方公共団体側が個人情報の管理に関する主導権を持ち、外部委託先に統制を利かせることが必要である。そのためには、先に述べたような個人情報保護対策のための組織を設置することが一義的には望ましい。しかしながら、中規模以下の地方公共団体では、職員数削減の流れの中で、情報政策部門においても専任で職務に従事できる職員は少なく、特に小規模団体では、他の業務との兼任で行わなければならないなど、職員の負担増という問題もある。その結果、地方公共団体の規模（具体的には情報セキュリティ対策に関わる職員の数と専任・兼任の比率など）によって対応の格差が生じやすいという問題も抱えるようになってきている。

このような状況の中で、職員（情報政策部門等の個人情報保護対策を主導的に行う部門及び業務部門）の負担を軽減することに留意しながらも、地方公共団体が、自らの責任で、外部委託事業者に対して、必要な個人情報の漏洩防止対策を実施させることのできる実効性ある手段や方法論を検討し、実践する必要がある。

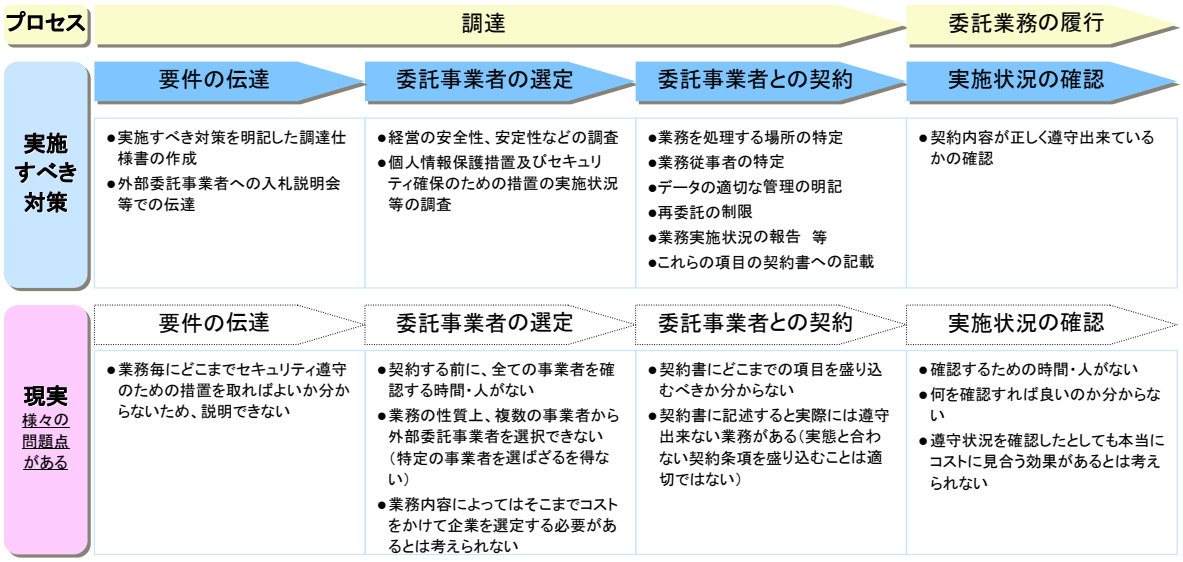
1-2　個人情報保護対策を実施する上での問題点

地方公共団体の個人情報の取扱いについては、国における情報セキュリティ対策に関する様々なガイドラインの策定、各地方公共団体における情報セキュリティポリシーの策定や個人情報保護条例の制定などの様々な取組が行われている。この中では、個人情報保護対策として、実施すべき対策が提供されている。

しかし、人員不足、対策を実施するための時間が確保できない等、これらの実施すべき対策を実施する上で様々な問題点があるため、実施すべき個人情報保護対策が実施できていない現状がある。

（「図表 1-3 実施すべき対策を目指す上での問題点」参照）

図表 1-3 実施すべき対策を目指す上での問題点



「要件の伝達」、「委託事業者の選定」、「委託事業者との契約」、「実施状況の確認」という、調達から委託業務の履行の流れの大きな枠組みで「外部委託における個人情報保護」の実施すべき対策と現状の問題を整理すると、下記のとおりとなる。

1-2-1　要件の伝達

各団体が、個人情報保護について外部委託事業者に求める事項を、委託の要件として、あらかじめ、受託対象事業者に伝えることが必要となる。各団体の業務部門において、調達準備の一環として実施すべき事項は以下のとおりである。

- 調達仕様書へ反映すべき個人情報保護の要件の整理と記述

- 入札説明会等で事前に伝達すべき事項の確認と実施

しかしながら、現状では「どの程度まで個人情報保護の対策を実施すれば良いか」あるいは「外部委託事業者にどの程度までの個人情報保護措置の実施を求めれば良いのか」を業務の実務に即して業務部門が十分に理解していないため、個人情報保護のために実施すべき内容を、外部委託事業者に対して適切に伝えることが不十分であることが少なくない。

1-2-2 委託事業者の選定

業務を外部委託する場合、個人情報保護措置を適切に実施可能な外部委託事業者を選定することが重要な取組内容の一つであると考えられるが、この事業者の選定にあたり実施すべき事項として以下のようなものがあげられる。

- 経営の安全性、安定性などの調査
- 個人情報保護措置及びセキュリティ確保のための措置の実施状況等の調査

いずれも、委託する業務の内容や委託する期間、取り扱う個人情報の種類や量などによって、どの程度まで精緻に行うかについては、個別の案件に応じた判断が必要である。

しかしながら、以下のような理由から、外部委託事業者の選定を十分には行えないという現状がある。

- 契約する前に、全ての事業者を確認する時間・要員が十分にはない
- 業務の性質上、複数の事業者から外部委託先を選択できない（特定の事業者を選ばざるを得ない）場合がある
- 業務内容によっては、コストをかけてまで、個人情報の保護に関して、事業者を選定する必要があるとは考えられない

1-2-3 委託事業者との契約

適切と思われる外部委託事業者を選定し契約を取り交わす場合、実施すべき事項や必要に応じて実施状況を確認することなどを契約書に明記することによって、双方がリスクと責任を承知しておくことが必要である。現状では「契約書にどの項目を記載すれば十分であるのか」という契約の技術的な判断が業務部門では難しいといった問題もあり、この判断のよりどころが求められている。

1-2-4 実施状況の確認

必要な項目が明記された契約書を外部委託事業者と取り交わした後、委託する業務内容や取り扱う個人情報の種類や量に応じ、個人情報保護措置の実施状況について適切に管理監督することが求められる。

しかし、現状では「対応のための要員や時間の確保が難しい」「どういった点を確認すれば良いのかがわからない」等の管理監督を実施する上での課題を抱えており、実効性を伴う確認方法や考え方が求められている。

1-3 検討の目的

これまで述べてきた実施すべき対策が実施できていない原因を深堀すると「実施すべき対策を実施するための方法がない」等の手段・手順の問題に加えて、「対策を実施する人の能力が足りない」等の人的要素の問題、「対策を実施するための予算・人員が足りない」等の予算・制度等の問題があることがわかった。

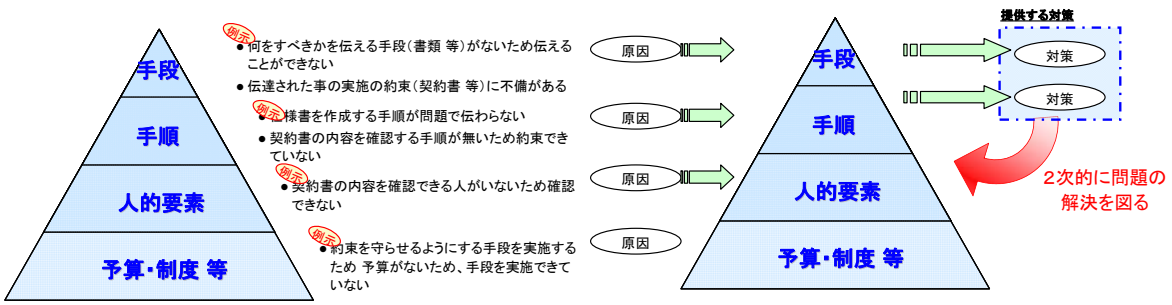
しかしながら、人的要素の問題や予算・制度の問題は、地方公共団体が単独で解決できる問題でもなく、短期的に解決できる問題でもない。しかし、その一方で、現実問題として個人情報の漏洩事案が多発し、住民の権利が脅かされる実情があるため、即効性のある対策が望まれているところである。

そこで、本検討では、個人情報保護対策が実施できていない原因の１つである手段・手順の問題を解決するために、多くのガイドライン等で求められている実施すべき対策の方法（手段・手順）を作成し、提供することを目的とした。

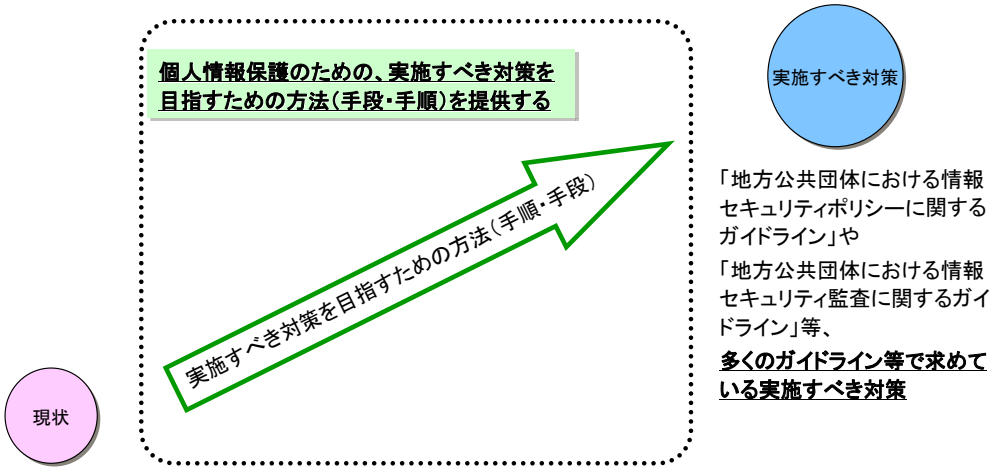
また、手段・手順の提供によって、担当職員の能力向上や意識改革を図るというように、人的要素の問題を間接的に解決することが可能となる。そこで、個人情報の保護対策を実施する職員の能力が不足している等の人的要素の問題について、具体的な対策の方法（手段・手順）論の提供により、すべての問題は解決できないまでも現状の改善が促進されることを期待している。

（「図表 1-4 本検討で解決を目指す原因」図表 1-5 本検討の目的」参照）

図表 1-4 本検討で解決を目指す原因



図表 1-5 本検討の目的



1-4 個人情報保護対策実施の基本的な考え方

前項で説明したように、個人情報保護対策を実施する上で、多くの地方公共団体では、人員不足、対策を実施するための時間が確保できない等、様々の課題がある。そのため、実施すべき個人情報保護対策が実施できていない現状がある。そこで、本検討では実施すべき対策に至るための方法（手段・手順）を提供し、個人情報保護対策を実施するためのツールを提供した。しかし、予算・人員が足りないなどの問題を本ツールで解決することは難しい。また、本ツールの利用によって、個人情報保護対策を強化すると事業者側及び地方公共団体のコスト負担が増える可能性がある。

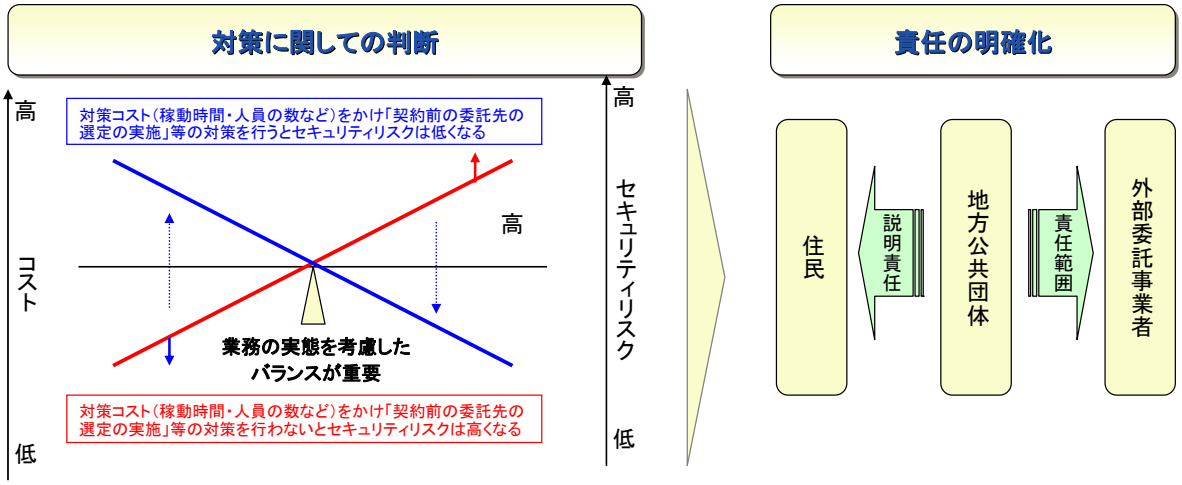
しかし、コスト負担が増えることを理由に個人情報保護対策を一律実施しないということでは、現状から何も変わらない。そこで、業務の実態（業務の性質や調達方法、取り扱う個人情報の内容及び現状の取扱いなど）を考慮し、対策にかかるコスト（外部委託事業者の選定に必要な稼動時間・人員の数・予算など）とセキュリティリスクのバランスから、個人情報保護対策をどのレベルで実施するかを地方公共団体が業務毎に主体的に判断、決定する必要がある。

その際に、このツールを用いて個人情報保護対策の実施状況を明確化することによって、完全に定量的にではないものの実施されている対策とコストの対比を実現することが可能になる。これによって、コストをかけて対策を実施した場合に低減されるリスクが明確になるとともにコストをかけなかった場合に高まるリスクを明らかにすることが

可能になる。すなわち、この対比を明確にすることによって、対策を実施するあるいはしないといった選択の結果についての責任も同時に明確にすることになる。

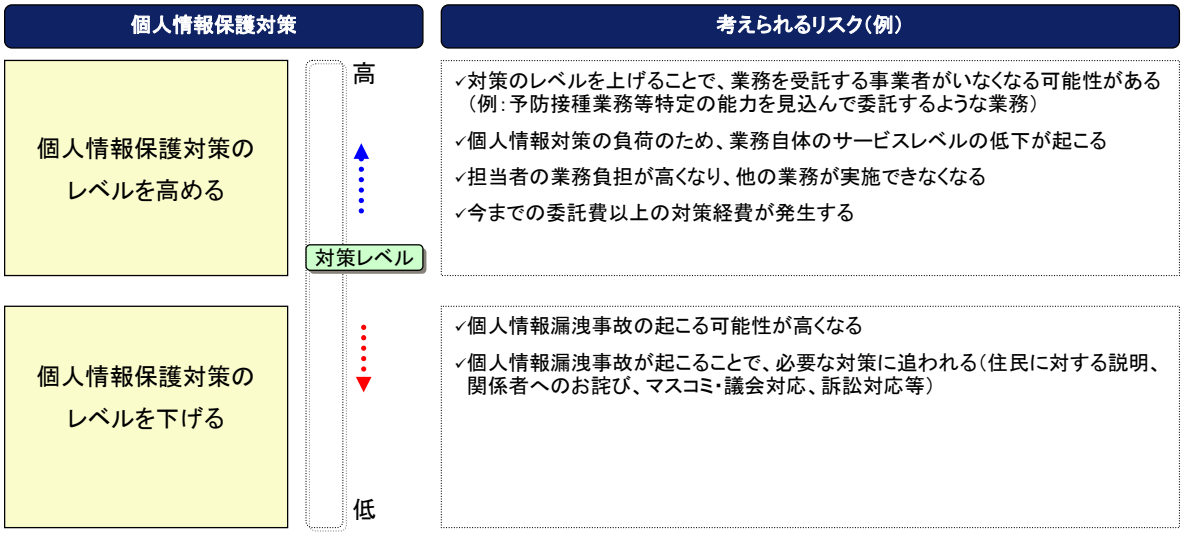
このように、実施する対策を地方公共団体が自ら主体的に決定することで、地域住民への説明責任や、外部委託事業者との地方公共団体の責任範囲を明確にすることができる。(「図表 1-6 個人情報保護対策実施の基本的な考え方」参照)

図表 1-6 個人情報保護対策実施の基本的な考え方



また、コストとのバランスに加えて、「業務を遂行する」という本来の目的とのバランスも踏まえ、どのような対策を実施するかについては業務の実態を考慮した判断が必要である。(「図表 1-7 対策に関して判断する上でのポイント」参照)

図表 1-7 対策に関して判断する上でのポイント

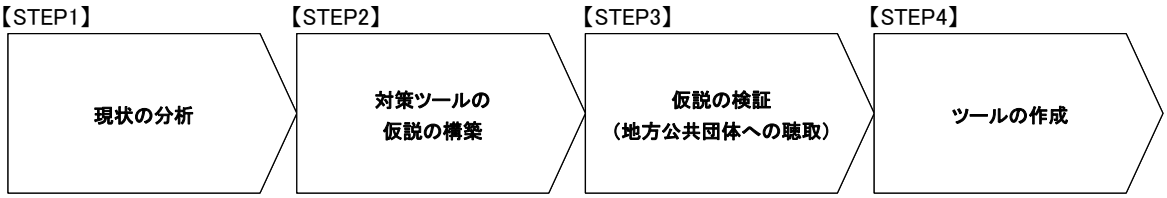


具体的には、個人情報保護対策のレベルを高くすることで、個人情報保護対策に要する負荷が高まり、業務自体のサービスレベルの低下の発生や委託する事業者がいなくなるなどの様々なリスクが発生する。また、逆に個人情報保護対策のレベルを低くすると、個人情報漏洩の可能性が高くなるなどのリスクが発生する。

このように、個人情報保護対策のレベルに応じて様々のリスクが発生するため、個人情報保護対策は全ての業務に対して一律に同様の対策を実施すれば良いわけではなく、業務の円滑な遂行と個人情報保護対策の必要性とのバランスを考慮して検討する必要がある。

2 提供ツールの作成に当たって

対策ツールを作成する上で、地方公共団体の実態にあったツールを作成するため、まず作成ツールの仮説を構築した後、複数の地方公共団体に対して、実際に行われている個人情報の管理方策に関するヒアリングを行うことで仮説の検証を行った。その後、地方公共団体へのヒアリングの結果や各種ガイドライン、事故の事例を参考にツールの作成を行った。



2-1 現状の分析

これまで述べてきたとおり、近年、外部委託事業者からの個人情報漏洩事案が多発している状況であるが、様々の地方公共団体の実情を調査すると「町村など小規模な団体では個人情報を取り扱う業務部門の職員の理解不足やITに関する知識が十分ではない」、「情報政策部門の担当者が対応すべき職員数が多く十分な対応が難しい」という問題を抱えていることが多く、特に、情報政策部門の担当者からは「個人情報を取り扱う業務システムに携わる事業者への外注管理の在り方や必要な対策実施の検討などに不安を感じている」という声が少なくないことが判明した。

また、同調査の中規模以下の団体へのヒアリングを通じて、以下のような課題が存在することも判明した。

1. 業務部門が管理運用している情報システムについて、どのような個人情報が取り扱われているのか情報政策部門が十分に承知していないことが少なくない

2. 業務部門では頻繁にシステム担当者が異動するため、個人情報保護対策など情報セキュリティに関する専門知識の蓄積が乏しい

3. 業務部門の職員であっても業務手順の整備などは行われておらず、職員の経験に依存している

4. 業務部門の職員が委託事業者に依存しており、適切な管理監督が十分には行えていない

特に、調査をした複数の団体から「契約書にこちらが必要とすることを加えようと思っても、法務部門を持たない小規模な地方公共団体では、事業者の法務部門にはかなわない」といった意見があり、個人情報保護対策として必要な事項を盛り込んだ指標となる契約書ひな型の提供が強く求められていることが分かった。

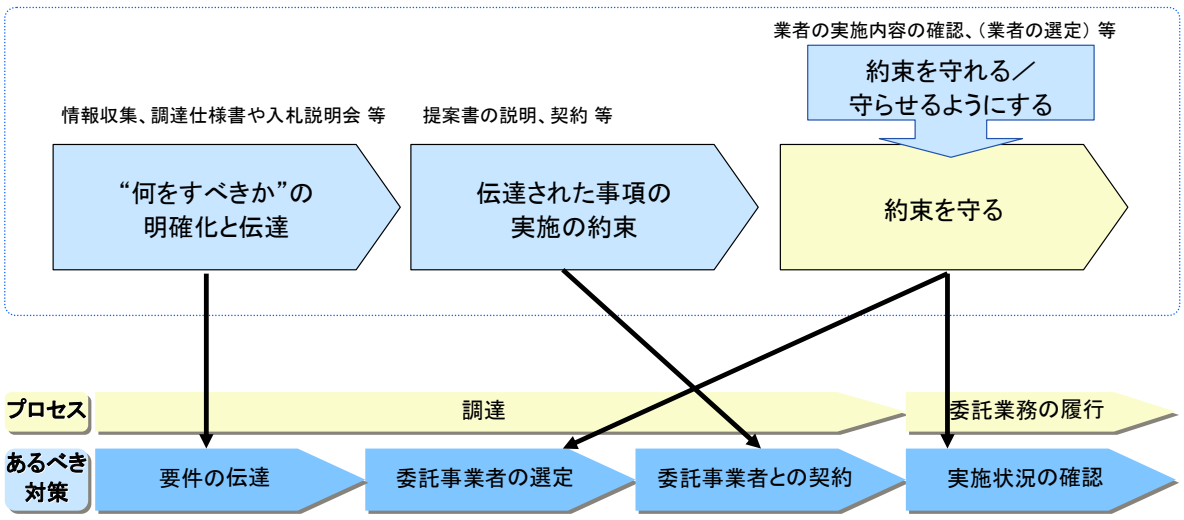
2-2 対策ツールの仮説の構築

調査の結果から、実際に個人情報を取り扱う業務部門の職員が適切な外部委託事業者を適切に指導・管理し、外部委託事業者からの情報漏洩などを防ぐために、「スキルや特別な法的知識を有しない業務部門の職員であっても必要な事項を契約書に盛り込めるようにするための契約書ひな型」と「委託事業者の個人情報保護体制をチェックするためのチェックシートやチェックポイントなどの方法（手段・手順））」を提供する必要があることが得られた。

そこで、外部委託における個人情報保護の課題を解決するためには、外部委託の業務の流れの中で、「“何をすべきか”の明確化と伝達」を行った後、「伝達された事項の実施の約束」を行い、「約束を守れる／守らせるようにする」ことが必要であると想定した。

そして、想定した枠組みを利用して、地方公共団体が実際に行っている個人情報保護対策、個人情報保護対策を実施する上での問題点のヒアリングを行った。（「図表 2-1 外部委託における個人情報保護の課題を解決するための枠組み」参照）

図表 2-1 外部委託における個人情報保護の課題を解決するための枠組み



2-3　仮説の検証

外部委託における個人情報保護の課題を解決するための枠組みをもとに構築した仮説を検証するために、２つの地方公共団体にどのような対策を行っているかヒアリングを行った。

この２つの地方公共団体は、過去に外部委託先からの個人情報漏洩事故を経験した後、その教訓を元に地方公共団体の外部委託における問題の改善に取り組んでいる。

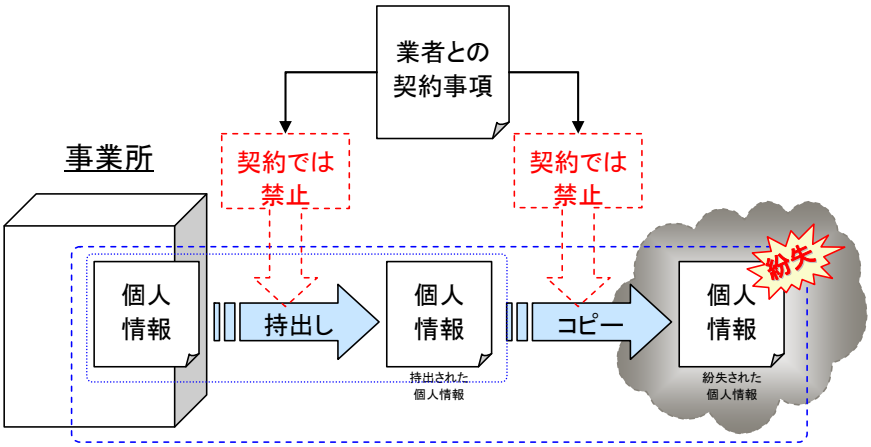
2-3-1　A 自治体の取組

A 自治体では、委託を受けている事業者の作業員が、個人情報が含まれた書類をコンビニエンスストアでコピーした際に、コピー機に置き忘れるなどして紛失する事故が発生した。

外部委託事業者との間の契約では複写、複製及び持ち出しは禁止されていた。しかし、委託した業務は、個人情報を帯同しながら個々の家庭を訪問する業務であったため、そもそも個人情報を事業所から持ち出す必要があった。すなわち、契約内容と業務実態の間に乖離があり、その乖離を地方公共団体側が把握しておらず、契約内容が遵守できていないことによって発生する事態の予測や業務実態に合わせた代替策の提供など、その予防を実施する機会を逸していた。

（「図表 2-2 個人情報漏洩概要（A 自治体）」参照）

図表 2-2 個人情報漏洩概要（A 自治体）



A 自治体では漏洩事故を受けて、以下のような個人情報保護対策を検討した。

- 外部委託事業者の情報セキュリティの遵守状況を確認し、業務の実態と契約内容に乖離があることに気づくための手段、手順

- 業務を実施する担当（地方公共団体、外部委託事業者）のセキュリティに対する意識を向上させる手段、手順

その結果、A 自治体では、個人情報保護対策として情報セキュリティ点検手順書を整備し、業務主管課の職員が外部委託事業者に対して、委託契約の個人情報保護の特記仕様書に明記されている内容の遵守状況の点検を実施している。遵守状況を確認した後に改善指示を出すことで、正しく履行が行われていない場合の個人情報漏洩リスクを減らすことができる。さらに、業務主管課の職員が外部委託事業者の遵守状況を点検することで、業務の実態と契約内容との乖離や契約内容の不備があることに気づき、業務の実態に沿ったより良い契約を実施できるようになる効果も期待できる。

また、所定の様式に基づいた報告を行うことを特記仕様書に明記し、情報セキュリティ点検を行うことを事業者に対して義務付けている。同時に、特記仕様書によって、事業者側に個人情報保護対策として「何をすべきか」を明確に伝え、意識させることが可能である。

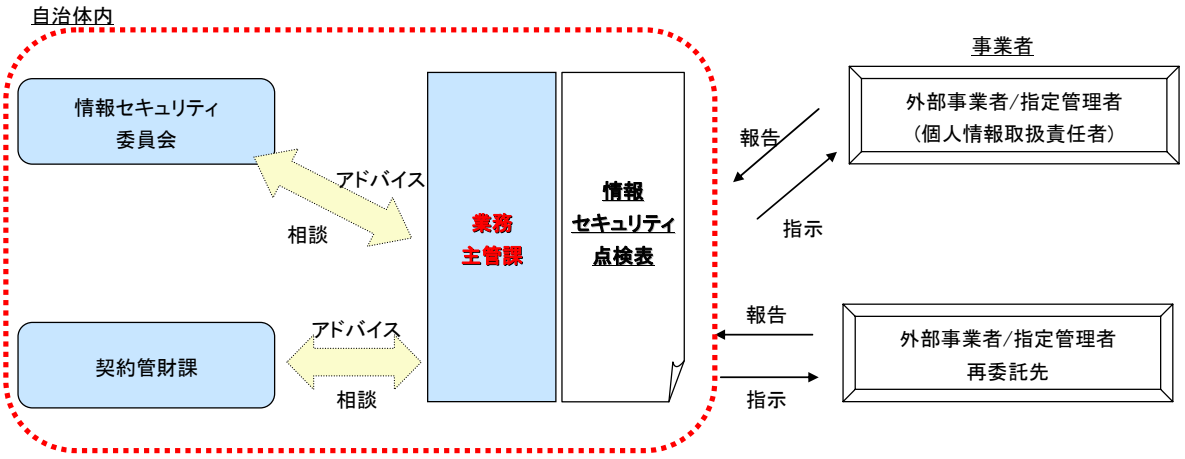
さらに、業務主管課の職員が自ら外部委託事業者に対して遵守状況を確認することで、業務を実施する担当（地方公共団体、外部委託事業者）のセキュリティに対する意識向上の効果も期待している。

（1）A 自治体の実施体制

A 自治体では、情報セキュリティ点検を業務の主管課が実施している。また、業務主管課の職員で解決できない内容については、情報セキュリティ委員会、契約管財課に相談することができるようにしている。このように、業務主管課が個人情報保護対策を行うにあたり、業務主管課をフォローする体制が構築されている。

（図表 2-3A 自治体の実施体制参照）

図表 2-3A 自治体の実施体制

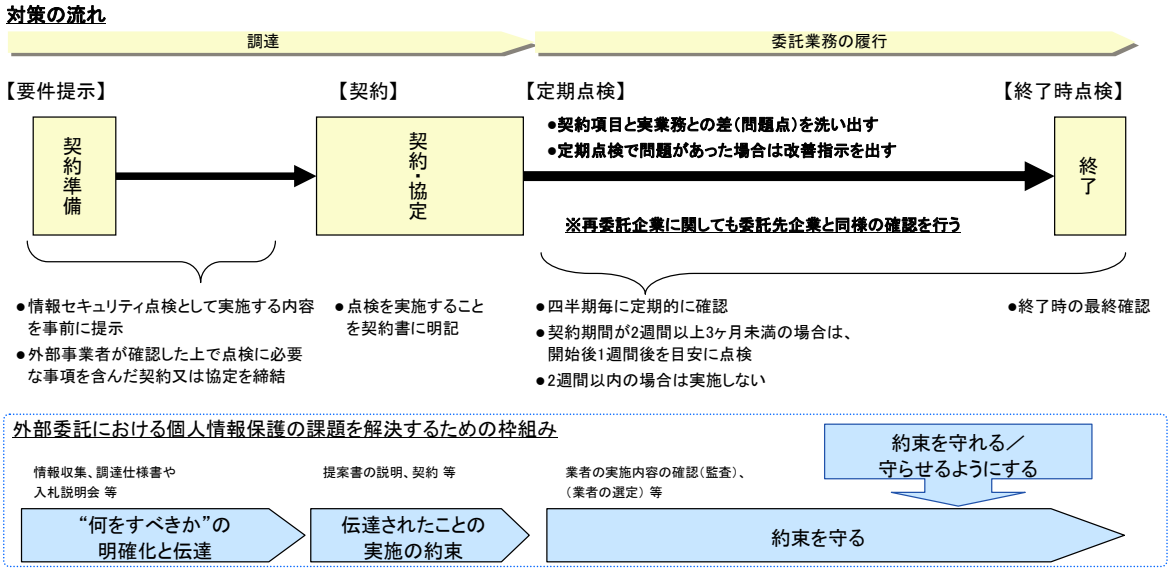


（2）A 自治体の対策内容

A 自治体では、情報セキュリティ点検表を契約前に事業者に公開している。事前に公開することによって、事業に応募する事業者に求められる対策を明確に予告するとともに、その負荷を知った上での応募となる効果を期待した取組である。その上で、契約後に情報セキュリティ点検を実施したのち、問題点があれば改善の指導を行っている。

（「図表 2-4 地方公共団体 A の対策内容」参照）

図表 2-4 地方公共団体 A の対策内容



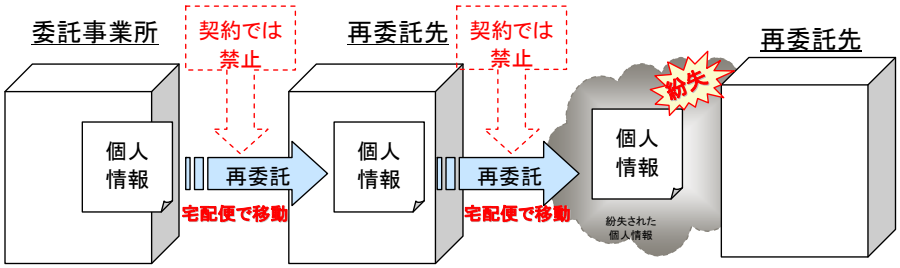
2-3-2 B 自治体の取組

B 自治体では、外部委託事業者が個人情報の入力業務を無断で他の事業者に再委託した。つまり、B 自治体は再委託の事実を把握していなかった。また、さらに再委託先からの再委託、いわゆる再々委託が行われていた。その過程で、委託事業者が再委託事業者にデータを渡す際に個人情報が紛失する事故が発生した。

本事案では、先述のとおり再委託事業者から更に再々委託が行われ、最終的には三社を経由した後、在宅勤務者までデータが渡っていた。事故が起こった当時、B 自治体と外部委託事業者との間の契約書には再委託の禁止項目が盛り込まれていた。外部委託事業者は再委託が禁止であることを知っていたが、それにも関らず無断で再委託を行っていた。一方で、B 自治体の業務主管課の担当者は、当該入力業務を毎年同じ事業者に委託していることから、外部委託事業者が信頼できると考えていた。

（「図表 2-5 個人情報漏洩概要（B 自治体）」参照）

図表 2-5 個人情報漏洩概要（B 自治体）



B 自治体では、この漏洩事故を受けて、以下のような個人情報保護対策を検討した。

- 外部委託事業者が個人情報保護対策を実施できるかを確認するための手段、手順
- 業務を実施する担当（地方公共団体、外部委託事業者）のセキュリティに対する意識を向上させる手段、手順

その結果、B 自治体では、委託することに決定した事業者の契約を保留し、「委託候補」と位置づけ、委託契約前に「委託候補」に対してセキュリティ調査を実施し、個人情報保護対策を実施できるか確認を行っている。その上で、庁内の外部委託審査会の承認を得て契約を締結することとしている。この B 自治体の例では、契約前に個人情報保護対策が実施できるかを確認するため、外部委託事業者が契約書に記述されている内容を履行できないということがない。

さらに、遵守状況の確認を業務主管課の職員が外部委託事業者に対して行うことで、業務を実施する担当者（地方公共団体、外部委託事業者）のセキュリティに対する意識向上の効果が期待される。また、外部委託事業者への啓発として、B 自治体が作成している「個人情報に係る外部委託に関するガイドライン」に基づく研修の受講を、外部委託事業者の個人情報保護責任者に対して義務付けている。すなわち、B 自治体の業務を委託するためには、研修を受ける必要がある。

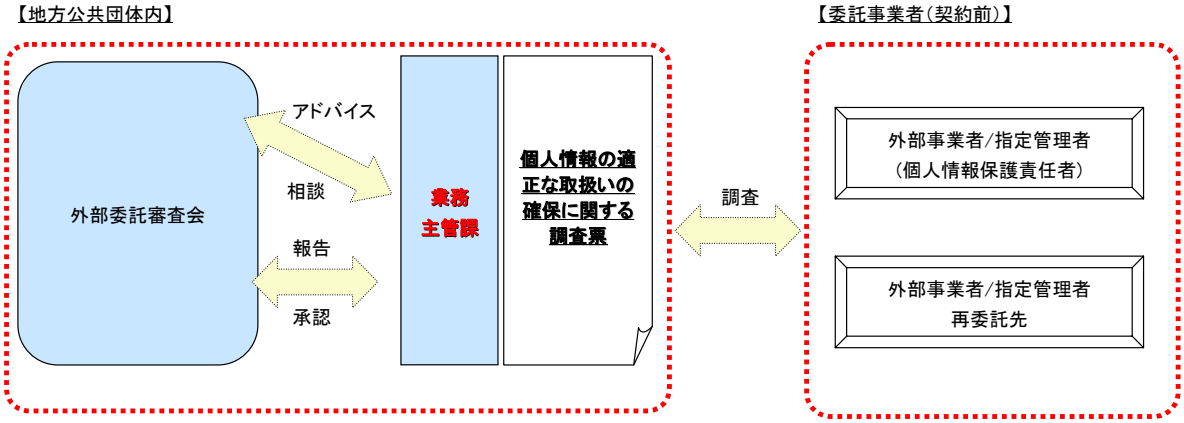
また、B 自治体内の職員に対しても、セキュリティ研修や日々の外部委託業務時のセキュリティ対策のアドバイスなどセキュリティに関する情報提供を行うことで、職員のセキュリティ意識の向上を目指している。

（1）B 自治体の実施体制

B 自治体では、情報セキュリティ点検を各業務の主管課が外部委託事業者に対して実施している。業務主管課の職員で解決できない事項については、外部委託の適正性を審査する外部委託審査会と協力し対応している。このように、業務主管課が個人情報保護

対策を行うにあたり、業務主管課をフォローする体制が構築されている。(「図表 2-6B 自治体の実施体制」参照)

図表 2-6B 自治体の実施体制

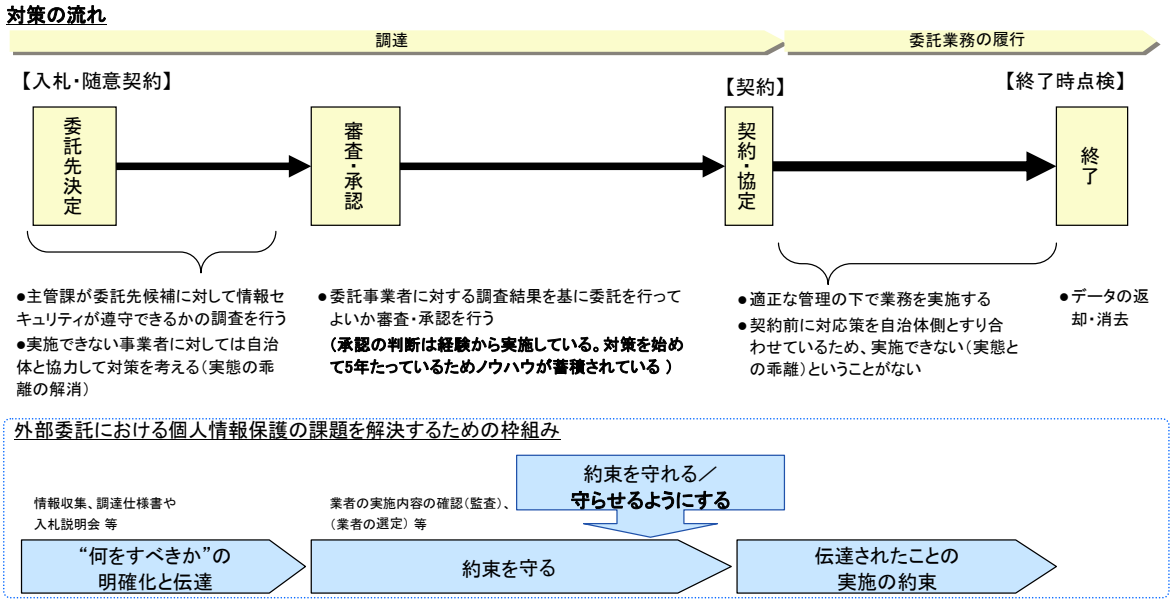


(2) B 自治体の対策内容

B 自治体の取組は、まず業務を委託する事業者を一社に絞り込み、その事業者を「委託候補」とした上で、業務主管課は「委託候補」に対して個人情報の適切な取扱いの確保が可能かを調査(セキュリティ調査)した後、「委託候補」が個人情報保護のために実施すべきセキュリティ計画を作成する。その上で、外部委託審査会の承認を得て契約を締結するため、契約後に個人情報保護対策が実施できない(実態との乖離)ということがない。

(「図表 2-7B 自治体の対策内容」参照)

図表 2-7B 自治体の対策内容



2-3-3 検証結果

A 自治体と B 自治体へのヒアリングの結果、どちらの団体でも今回設定した「外部委託における個人情報保護の課題を解決するための枠組み」が適用できることが分った。そのため、外部委託に係る個人情報保護対策では、外部委託のプロセス中で、「“何をすべきか”の明確化と伝達」を行った後、「伝達された事項の実施の約束」を行い、「約束を守れる／守らせるようにする」ことが重要であることが確認できた。

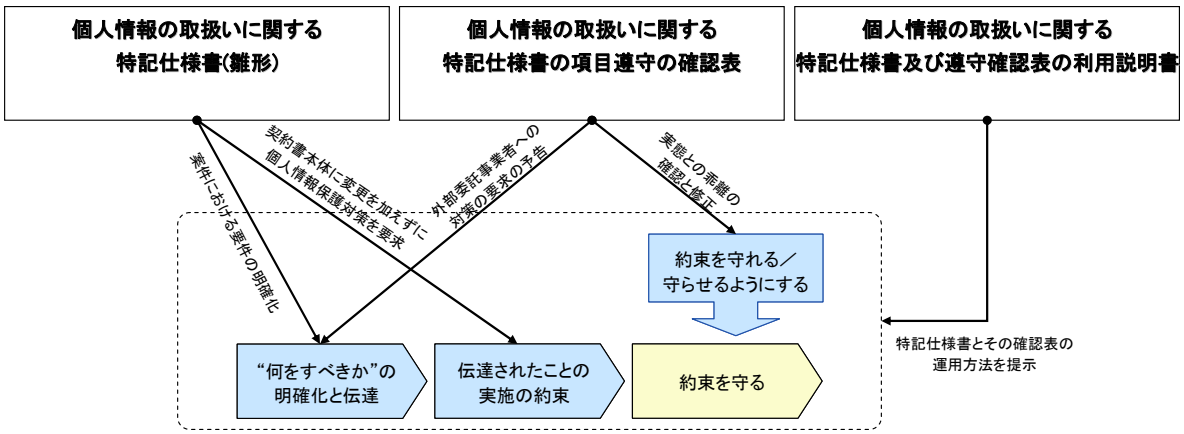
また、個人情報保護対策を実施するのは業務の主管課の担当者であり、業務主管課の担当者を支援する仕組みを構築することが実効的な取組を行うに当たり重要であるという示唆も得られた。さらに、外部委託のプロセスにおいて個人情報保護対策を実施することで、地方公共団体の職員や外部委託事業者のセキュリティ意識の向上にもつながることが分かった。

2-4 提供ツールの概要

外部委託のプロセス中で「外部委託における個人情報保護の課題を解決するための枠組み」を実現するためのツールとして、「個人情報の取扱いに関する特記仕様書(雛形)」、「個人情報の取扱いに関する特記仕様書の項目遵守の確認表」、「個人情報の取扱いに関する特記仕様書及び遵守確認表の利用説明書」を作成することとした。

（「図表 2-8 作成ツール」参照）

図表 2-8 作成ツール



提供ツールは、予算・人員など取組実施のための環境が十分整備された一部の地方公共団体だけではなく、そのような環境にない多くの地方公共団体で利用可能なものとなるように工夫している。また、地方公共団体ではシステム開発や運用に関係する業務だけにとどまらず、多数の業務で個人情報を取り扱っていることが分っている。その様な状況も踏まえ、大量に個人情報を取り扱う業務では情報システムが利用されることが多いことを考慮しつつも、個人情報を扱う全ての業務の外部委託で利用できるように工夫している。

（「図表 2-9 提供ツールの特徴」参照）

図表 2-9 提供ツールの特徴

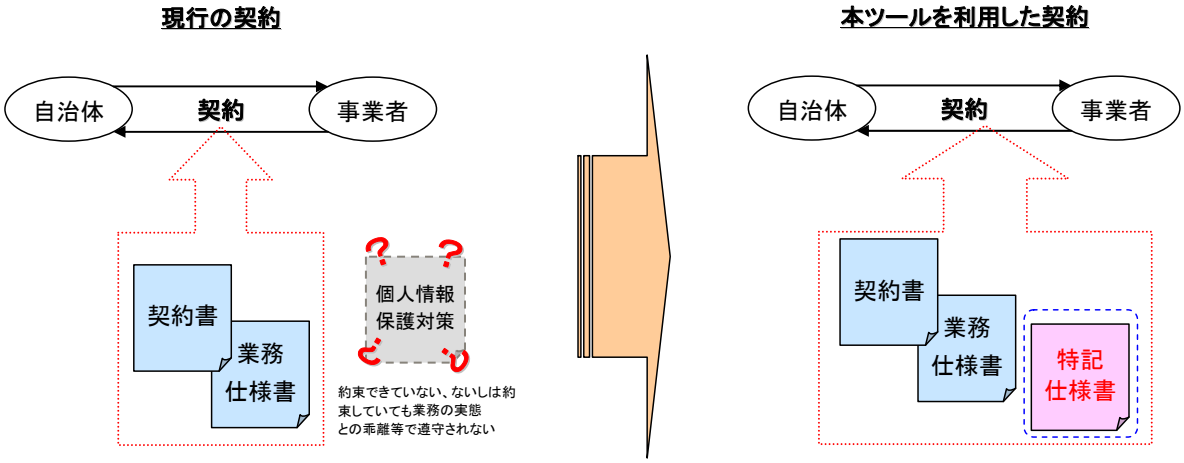
提供ツール	工夫した内容
個人情報の取扱いに関する特記仕様書（雛形）	✓ どのような業務でも汎用的に利用できるように考慮して作成した ✓ 特記仕様書（雛形）を利用することで、個人情報保護のためのあるべき契約が結べるように、様々なガイドラインを参考にして条文を作成した ✓ 特記仕様書（雛形）の条文の内容を理解して業務担当者が利用できるように、なぜこの契約内容が必要かが分かる説明資料を作成した
個人情報の取扱いに関する特記仕様書の項目遵守の確認表	✓ 特記仕様書に記述されている内容を確認するためには、具体的に何を確認すべきかが分かる確認項目となっている ✓ 確認表の確認項目がなぜ必要かが分かる説明資料を作成した ✓ 確認項目は「対策があること」と「運用が実施されていること」が確認できるようになっている（対策があるだけで、実施されていない可能性もある）
個人情報の取扱いに関する特記仕様書及び遵守確認表の利用説明書	✓ 実際にツールを利用する担当者が読みやすいように、業務で外部委託を実施する場合を想定して、文書を記述した

2-4-1　個人情報の取扱いに関する特記仕様書について

「特記仕様書（雛形）」は、地方公共団体で現在行われている業務の手順やそこで利用されている業務の遂行上必要な外部委託契約の内容を変更しなくても適用できるように、既存の契約書に付帯して、実施すべき対策が盛り込まれた契約とすることができる形で提供する。

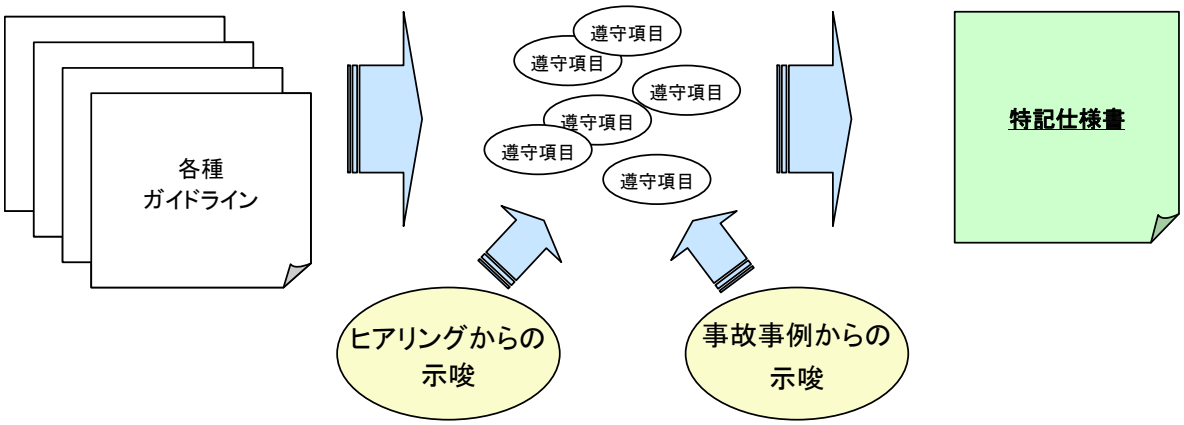
（「図表 2-10 個人情報の取扱いに関する特記仕様書の利用イメージ」参照）

図表 2-10 個人情報の取扱いに関する特記仕様書の利用イメージ



また、特記仕様書（雛形）の項目は、「情報セキュリティポリシーガイドライン」等、情報セキュリティ対策に関する様々なガイドラインや地方公共団体で実際に利用されている特記仕様書の項目、事故事例から得られた示唆などを参考にして作成した。（「図表 2-11 個人情報の取扱いに関する特記仕様書の作成イメージ」参照）

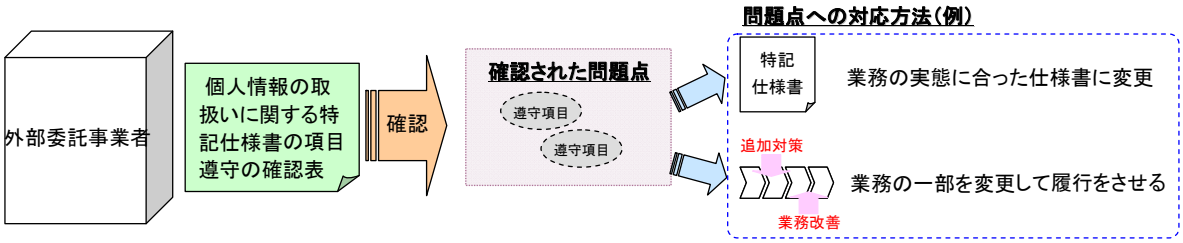
図表 2-11 個人情報の取扱いに関する特記仕様書の作成イメージ



2-4-2 個人情報の取扱いに関する特記仕様書の項目遵守の確認表について

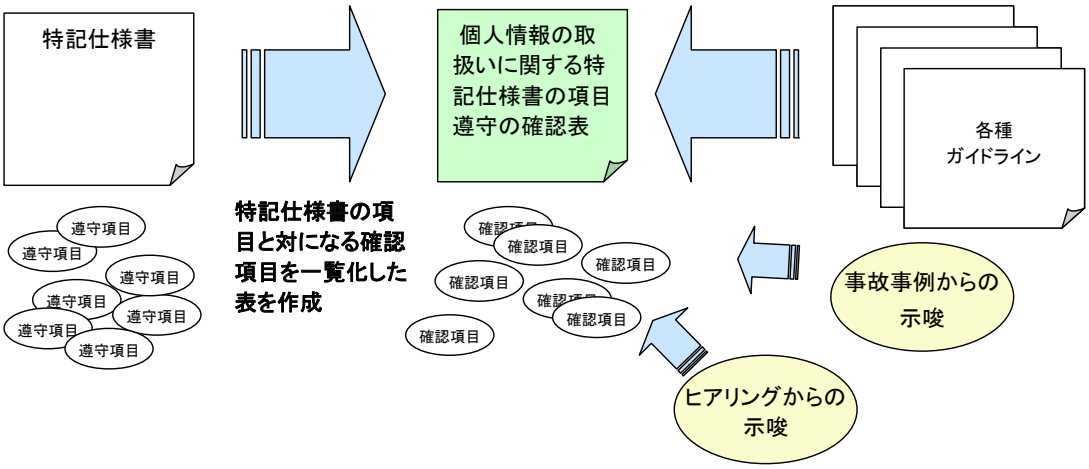
「遵守確認表」は、「特記仕様書」の項目を外部委託事業者が「履行できるか」または「履行できているか」を確認するために利用する。このような確認をすることで、実態との乖離の解消・現状の問題点の改善を行うことができる。
（「図表 2-12 個人情報の取扱いに関する特記仕様書の項目遵守の確認表の利用イメージ」参照）

図表 2-12 個人情報の取扱いに関する特記仕様書の項目遵守の確認表の利用イメージ



また、「特記仕様書」の遵守状況の確認または契約前に履行できるか否かの確認のためのヒアリングを事業者に行うために、特記仕様書と対になる「遵守確認表」を作成した。
（「図表 2-13 個人情報の取扱いに関する特記仕様書の項目遵守の確認表の作成イメージ」参照）

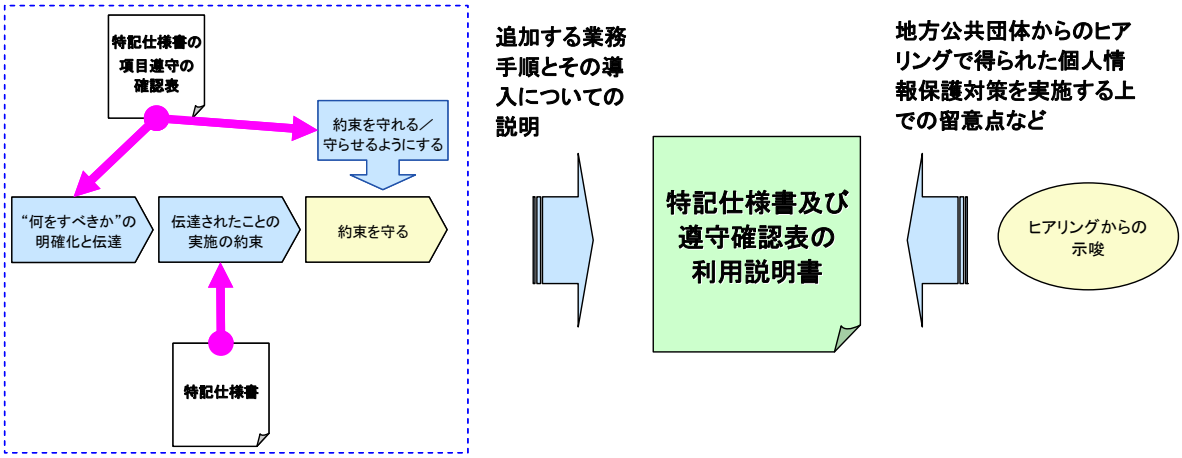
図表 2-13 個人情報の取扱いに関する特記仕様書の項目遵守の確認表の作成イメージ



2-4-3 個人情報の取扱いに関する特記仕様書及び遵守確認表の利用説明書について

特記仕様書及びその項目の遵守確認表の利用方法を利用説明書として取りまとめた。（「図表 2-14 個人情報の取扱いに関する特記仕様書及び遵守確認表の利用説明書の作成イメージ」参照）

図表 2-14 個人情報の取扱いに関する特記仕様書及び遵守確認表の利用説明書の作成イメージ



3 残された課題

外部委託事業者に対する個人情報の管理の在り方については、本検討において地方公共団体が実施すべき対策の具体的な方法論を提供をしたところであるが、この方法論の実践に関連した次のような解決困難な課題が存在する。

＜再委託についての課題＞

外部委託事業者からの個人情報の漏洩が増加している要因の一つには、外部委託事業者がコスト削減のため受託業務の遂行に当たって必要な要員を自社よりも低コストである社外に求めていることがあげられる。ICT 業界においては、冒頭で述べたとおり、再委託・再々委託という形で業務が取り扱われていることが常態化している。

現状では、元々社内にあったエンジニア部門や保守部門などを子会社化している、開発のために必要な技術者を案件に応じて外部から調達しているといったように、業務の再委託・再々委託は外部委託事業者の事業戦略に関わる場合が多く、一律に再委託・再々委託を禁止すると、委託先が確保できないといった事態が生じるおそれが高い。したがって、個人情報の取り扱い上問題が発生しやすい再委託・再々委託といった形態を一律に禁止するかどうかについては、今後も慎重な検討が必要である。

しかしながら、業務の再委託・再々委託は原則禁止であると契約上確実に明記し、契約に反して再委託・再々委託が行われた場合には厳格に事業者の責任を追及するといった対応・事例を確実に積み上げることにより、安易な再委託・再々委託を消滅させる不断の努力が必要である。

＜新たな脅威に対する課題＞

近年までの個人情報漏洩事案の原因の多くは内部の不正行為が主な原因であった。このような不正に対しては、規則等の整備による人的な統制、及びシステム的な統制により、ある程度の防止はできてきた。

しかし、新しい技術の進歩や個人の ICT 利用の高まりによって、これまでは想定しなった脅威やコントロール不能ないしは回復不能な被害が増えている。例えば、Ｗｉｎｎｙ やＳｈａｒｅといったファイル交換ソフトなどによってインターネット空間に流出してしまった個人情報の回収は極めて難しく、一度流出してしまった場合その回収は不可能に近い。そうならないためには、外部委託事業者の従業員等に対して、そのようなファイル交換ソフトの利用を厳しく制限することも必要となるであろう。

たしかに、地方公共団体の立場から一私企業に勤める従業員の私的な行動に言及することは難しいと考えられる。

しかし、今後は地方公共団体の業務を受託しようとする企業に対して、従業員がそのようなソフトウェアを利用することの危険性を熟知し、委託業務に携わる従業員が

私的にファイル交換ソフトを利用しないことを誓約させるなどの対応が迫られるであろう。

これらの課題の解決には、環境の変化に対応すべく、定期的に本ツールのあり方や内容を見直すことが必要であると考えられる。

4 参考資料

(1) 行政機関の保有する個人情報の保護に関する法律（平成 15 年 5 月 法律第 58 号）
(2) 住民票に係る磁気ディスクへの記録、その利用並びに磁気ディスク及びこれに関連する施設又は設備の管理の方法に関する技術的基準(昭和 61 年　自治省告示第 15 号）第１０「外部に委託して処理する場合に講ずるべき措置」
(3) 個人情報の保護に関する基本方針（平成 16 年 4 月　閣議決定）
(4) 電気通信回線を通じた送信又は磁気ディスクの送付の方法並びに磁気ディスクへの記録及びその保存の方法に関する技術的基準（平成 14 年　総務省告示第 334 号）
(5) 個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン（平成２０年２月２９日　厚生労働省・経済産業省告示第１号）
(6) 行政機関の保有する個人情報の保護に関する法律の施行に当たって（通知）（平成 17 年 3 月　総務省通知）
(7) 外部委託に伴う個人情報漏えい防止対策に関する対応及び留意事項（平成 19 年 6 月 総務省通知）
(8) 行政機関の保有する個人情報の適切な管理のための措置に関する指針について（通知）（平成 16 年 9 月　総務省通知）
(9) 公共 IT におけるアウトソーシングに関するガイドライン（平成 15 年 3 月　総務省）
(10) 地方公共団体における情報セキュリティポリシーに関するガイドライン（平成 18 年 9 月全部改訂　総務省）
(11) 地方公共団体における情報セキュリティ監査に関するガイドライン（平成 19 年 7 月全部改訂　総務省）
(12) 外部委託における情報セキュリティ対策実施規程策定手引書（平成 18 年 3 月 内閣官房情報セキュリティセンター）
(13) 政府機関の情報セキュリティ対策のための統一基準（第 3 版）（平成 20 年 2 月 内閣官房情報セキュリティセンター）