別添資料

個人情報委託の実地検査ポイント Ver.2.1

個人情報の量、期間、作業内容によって漏えい等のリスクが異なります。
記載内容は例示です。現地確認する内容は、記載例を参考にして委託内容に合わせて実地検査を行ってください。

1　実地検査の事前準備

（1）受託者からの提出書類の確認

ア　管理責任者、作業責任者及び作業従事者の報告

イ　個人情報の取扱い及び管理の状況を記録

ウ　緊急時対応計画

エ　教育又は研修の実施状況に係る報告書

オ　外部記憶媒体（USBメモリ）の使用の記録

カ　作業区域に持ち込まれた外部記憶媒体（USBメモリ）の記録

キ　作業区域外への個人情報記録媒体（紙を含む）の持ち運び管理簿

ク　削除、廃棄の証明書

ケ　日本国外で取り扱う場合の許可申請書

コ　再委託申請書

（2）仕様書の確認

（3）業務フロー図の作成

個人情報の管理の状況や再委託先を把握するため、受託者に業務フロー図を作成させ、個人情報の流れを確認する。個人情報の入力（本人からの取得を含む。）、編集、分析、出力、運搬、消去等の処理を誰が行っているかを記載して、委託先の個人情報の取扱い状況を確認する。

＜業務フロー図には以下の事項が分かるように記載する＞
ア　「誰が」　＝委託先名、再委託先名、ＡＳＰサービス名称　など
イ　「処理内容」＝印刷、封入、電話受付、運送、システム管理・運営・保守、廃棄　など
ウ　「受渡手段」＝郵送、ＵＳＢメモリ、クラウドによるファイル共有　など

（4）再委託先の確認

ア　再委託について漏れなく届出されているか確認する。特に、以下の情報システムに関する再委託について注意する。

（ア）クラウドサービスの利用、契約の有無
（イ）ＡＳＰサービスの利用、契約の有無
（ウ）情報システムの管理・運営・保守を他社契約の有無

イ　サービス利用契約も再委託に含まれる。

ウ　業務フロー図により、再委託の有無について不明点を事業者に確認する。

＊ＡＳＰとは
Application Service Provider（アプリケーション・サービス・プロバイダ）の略。インターネット上でアプリケーションを提供するサービスの提供者（事業者）のことを言い、提供されるソフトウェアやサービスのことをASPサービスという。
（総務省ホームページ「国民のためのサイバーセキュリティサイト」より引用）

＊個人情報を取扱う業務の委託とは
契約の形態・種類を問わず、行政機関等が他の者に個人情報の取扱いを行わせることをいいます。再委託においても同じ。

2　実地検査時のチェックポイント

提出書類内容、作業工程を踏まえて下記の各安全管理措置が講じられているか確認する。

（1）組織的安全管理措置	
ア	作業人数が報告書と相違ないか確認する。
イ	作業責任者が作業現場で常時監督しているか、作業責任者不在時の対応が決まっているか確認する。
ウ	緊急時対応計画の内容が実態と相違ないか確認する。
エ	作業手順書の有無と内容を確認する。

（2）人的安全管理措置	
ア	研修で使用した教材を確認する。また、研修の実施方法や実施頻度などをヒアリングで確認する。

（3）物理的安全管理措置		
ア	作業場所の状況を確認する。	
	(ｱ)	第三者が容易に侵入できないような建物・部屋となっているか。 鍵の有無、種類、その他入室の方法が、取り扱う個人情報の内容や量により、施錠方法が適切となっているか。
	(ｲ)	他の作業との分離がされているか。 ①　パーテーションなどでエリアを区分けし、のぞき見等の防止措置をする。 ②　他の作業場所と距離を離す。 ③　作業時間中であっても、不要な書類は都度収納するなど、第三者に見えることのないよう作業をしている。
	(ｳ)	作業場所は適切な広さを確保できているか。
	(ｴ)	作業場所全体が整理整頓されているか。
	(ｵ)	作業場所で飲食をおこなっていないか。汚損を防止しているか。
	(ｶ)	作業場所へ私物モバイル端末、私物パソコン、私物外部記憶媒体等の業務に関係のないものを持ち込んでいないか。
	(ｷ)	監視カメラにより第三者の入室や作業状況を確認できるか。映像の保存期間も確認する。
イ	情報の保管場所を確認する。	
	(ｱ)	日時、随時の一時保管場所が施錠可能な場所となっているか。 全て個人情報記録媒体（書類を含む）は施錠できるキャビネットに収納しているか。
	(ｲ)	長期間保存する場所（倉庫等）の管理状況は適切となっているか。 ①　他の納品物等と仕分けられて、印刷物等の混在が防止されているか。 ②　倉庫の鍵は使用者が限定されているか。 →鍵の使用簿があるなど、入室の記録がされているか。
ウ	作業場所から倉庫等への搬送は第三者の閲覧防止や紛失防止などの措置を講じた搬送となっているか確認する。 →ロビーのような場所を通るのであれば、個人情報が目に留まらないように搬送する。 →建物の外に搬送するのであれば、風に飛ばされないような工夫がされている。	
エ	作業場所から再委託先、郵便局や区への搬送方法を確認する。 ①　「作業区域外への個人情報記録媒体の持ち運び管理簿」が記録されているか。 ②　郵便局への持込の場合は持出件数と受取件数の付け合わせが行われているか。	

（３）物理的安全管理措置		
オ	ＵＳＢメモリ（外部記憶媒体）の管理状況の確認する。	
	(ｱ)	保管場所は常時施錠されているか。
	(ｲ)	保管場所の鍵は作業責任者のみ開けられるようになっているか。
	(ｳ)	ＵＳＢメモリの使用状況が管理台帳に記録されているか。 ＵＳＢメモリの現物の本数と管理台帳に記載されている本数が同一であるか。 →万一の誤りや故意による持出を防止するため、個人情報を取り扱わないＵＳＢメモリも管理対象。
カ	ＰＣの設置状況・使用状況を確認する。	
	(ｱ)	セキュリティワイヤーで固定されているか。
	(ｲ)	タブレット端末の保管場所が施錠させているか。業務終了時の収納先を確認する。
	(ｳ)	第三者から画面が見えないような配置となっているか。
	(ｴ)	離席時のPC画面のぞき見対策がとられているか。スクリーンセイバーの設定を確認する。
	(ｵ)	PC本体にパスワードなど付箋が貼っていないか。
キ	シュレッダーの機種や設置場所、溶解処分の有無を確認する。	
	(ｱ)	シュレッダーの性能が適正なものであるか。 裁断が細かくクロスカットであるか。
	(ｲ)	設置場所が適正な場所か。 書類の一時置場と近いと誤廃棄のおそれがある。
	(ｳ)	シュレッダーの使用について社内ルールを定めているか。
	(ｴ)	溶解処分を行っている場合は再委託の届出の有無を確認する。 マニフェストや最終処分の確認書類の提出内容を確認する。
ク	倉庫、収納庫、ＵＳＢメモリ収納場所、セキュリティワイヤー等の鍵は、決められた人のみが使用できるのか確認する。 キーボックスの暗証番号は、人事異動時に変更しているか確認する。	

（４）技術的安全管理措置		
ア	システム、PC、端末等のアクセス制御について確認する。	
	(ｱ)	作業員一人ひとりに別のID、パスワードの割振となっているか。
	(ｲ)	PCログイン時とアプリやソフトのログイン時にID、パスワード設定されているか。
	(ｳ)	業務上必要な者だけが情報にアクセスできるように設定されているか。
	(ｴ)	作業員が作業に不必要な操作ができないように操作制限がされているか。
	(ｵ)	担当外となった者が、ログイン出来ないように管理されているか。
	(ｶ)	システム管理者の不正行為を監視する仕組みがあるか。
イ	操作ログは取得しているか。定期的に不審な操作がないか分析しているか確認する。 ログの分析はだれが、どの程度の頻度と内容で行っているか確認する。	
ウ	使用するOSやソフトは最新バージョンとなっているか確認する。	
エ	ウイルス対策ソフトが導入されているか確認する。	
オ	ＵＳＢポートは物理的または技術的に接続できない措置が講じられているか確認する。	

（４）技術的安全管理措置	
カ	ファイアウォールの設定が「有効」となっているか確認する。IDS/IPSやWAFが導入されているとなおよい。 ＊IDS（Intrusion Detection System＝不正侵入検知システム） ネットワーク通信を監視して不正アクセスや攻撃などの兆候や深刻な脅威を検知する。 ＊IPS（Intrusion Prevention System＝不正侵入防御システム） 外部から不正な攻撃を検知した場合に、その不正な通信を遮断したり、アクセスログを不正に改ざんすることを防御する。 ＊WAF（Web Application Firewall） Webサイトを含めたWebアプリケーションの脆弱性を狙ったサイバー攻撃を防御する。
キ	無線LANを使用している場合は、アクセスポイントで適切な暗号化を設定しているか確認する。WEP方式は脆弱性があるためNG。
ク	クラウドサービスを利用している場合は、仕様書の記載内容と同一であるか確認する。 ①　海外のクラウドサービスの利用を禁止している場合には、その旨確認する。 ②　ISOやISMPなど認証取得していることを条件としている場合には、その旨確認する。 ＊ISO（International Organization for Standardization＝国際標準化機構） ISOが制定した規格をISO規格という。基準を満たしていると認証証明書が発行される。 ISO27017はクラウドサービスに関する情報セキュリティ管理策のガイドライン規格。 ＊ISMP（Information system Security Management and Assessment Program ＝政府情報システムのためのセキュリティ評価制度） 政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録することにより、政府のクラウドサービス調達におけるセキュリティ水準の確保を図り、もってクラウドサービスの円滑な導入に資することを目的とした制度。
ケ	作業に関係のないアプリなどがインストールされていないか確認する。特に、ファイル共有のアプリ（P2P）などがインストールされていないか確認する。 ＊P2P（Peer to Peer） インターネットを利用して不特定多数のコンピュータ間でファイルの共有や交換を行うソフトウェアのこと。
コ	許可されていない端末や媒体へ情報をコピーまたは送信できないように管理されているか確認する。 ①　許可された媒体や端末のみが、情報を扱う端末に接続できるようになっているか確認する。 ②　メールやファイル転送システムが、上長承認など送信者以外の確認を経て送信できるようになっているか確認する。

（５）再委託先の安全管理措置		
ア	再委託先事業者を全て把握できているか確認する。	
	(ｱ)	コールセンター
	(ｲ)	クラウドサービス・ＡＳＰサービス
	(ｳ)	情報システムの管理・運用・保守
	(ｴ)	印刷・運送
	(ｵ)	廃棄・溶解
イ	委託先が再委託の監督を適切に行われているか確認する。	
	(ｱ)	委託先が区に提出する書類と同様に書面提出を求めているか。
	(ｲ)	再々委託について把握しているか。
	(ｳ)	再委託先に対して「仕様書」「個人情報約款別紙」の内容を遵守させているか。
	(ｴ)	再委託先に対して実地検査を実施しているか。

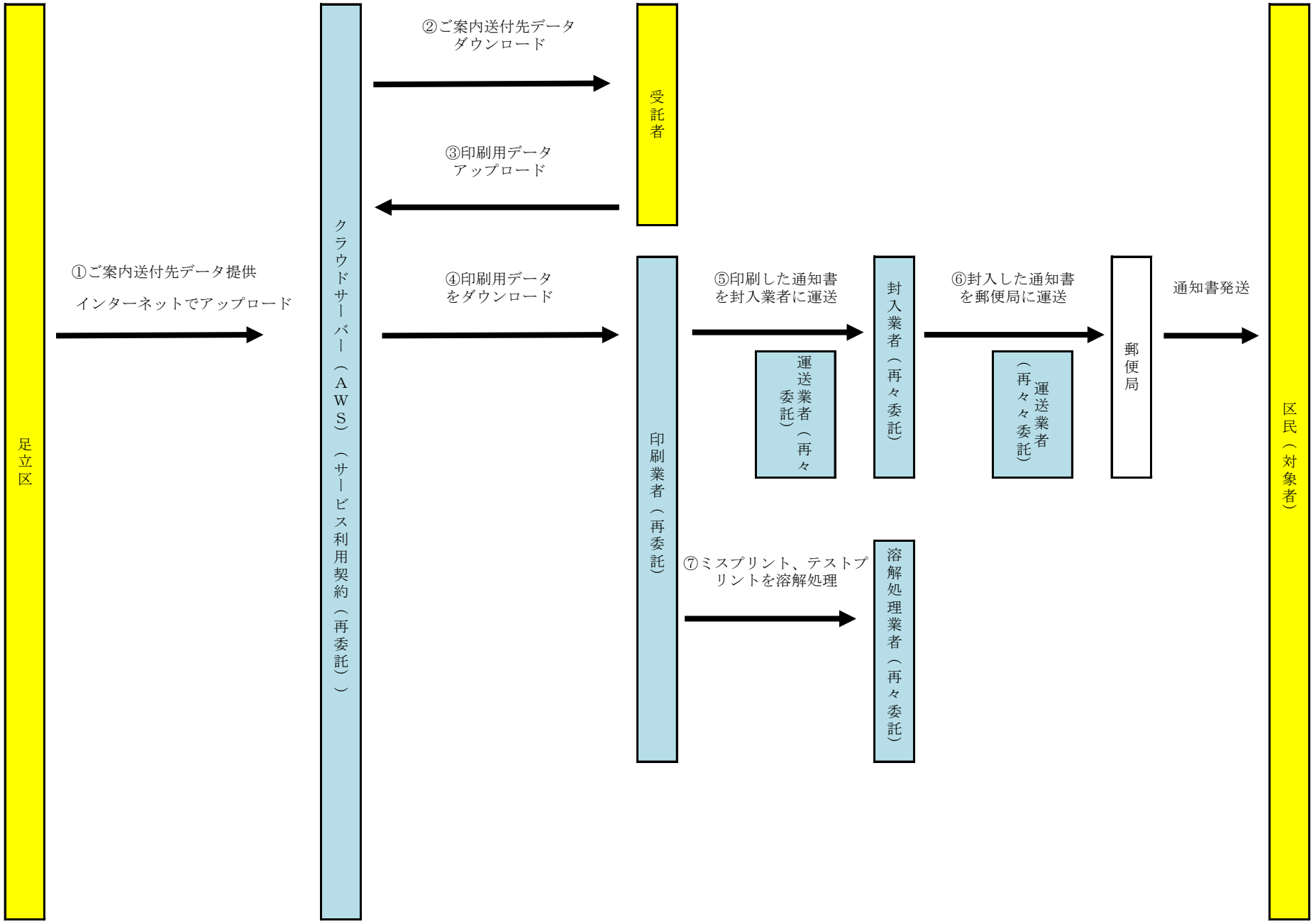
契約書約款別紙　書面報告させるもの

【参考】

条文	提出内容	見本様式の名称	提出時期
２条	管理責任者、作業責任者及び作業従事者の報告	個人情報取扱者名簿	契約業務着手前+変更時
４条	個人情報の取扱い及び管理の状況を記録	個人情報の取扱い及び管理の状況	原則３か月に一度＋区の求めに応じて
５条	緊急時対応計画	＊見本なし	契約業務着手前
６条	教育又は研修の実施状況に係る報告書	研修実績報告書	原則３か月に一度＋区の求めに応じて
９条	外部記憶媒体（USBメモリ）の使用の記録	外部記憶媒体使用簿	原則３か月に一度＋区の求めに応じて
９条	持ち込まれた外部記憶媒体（USBメモリ）の記録	外部記憶媒体持込管理簿	原則３か月に一度＋区の求めに応じて
10条	作業区域外への個人情報記録媒体の持ち運び管理簿	個人情報記録媒体運搬管理簿	原則３か月に一度＋区の求めに応じて
11条	削除、廃棄の証明書	＊見本なし	削除、廃棄したとき
16条	日本国外で取り扱う場合の許可申請書	＊見本なし	取り扱い前
18条	再委託申請書	再委託関係書面	再委託前
その他	窓口委託における誓約書	誓約書（受注者、従事者用）	委託業務着手前、従事者追加時

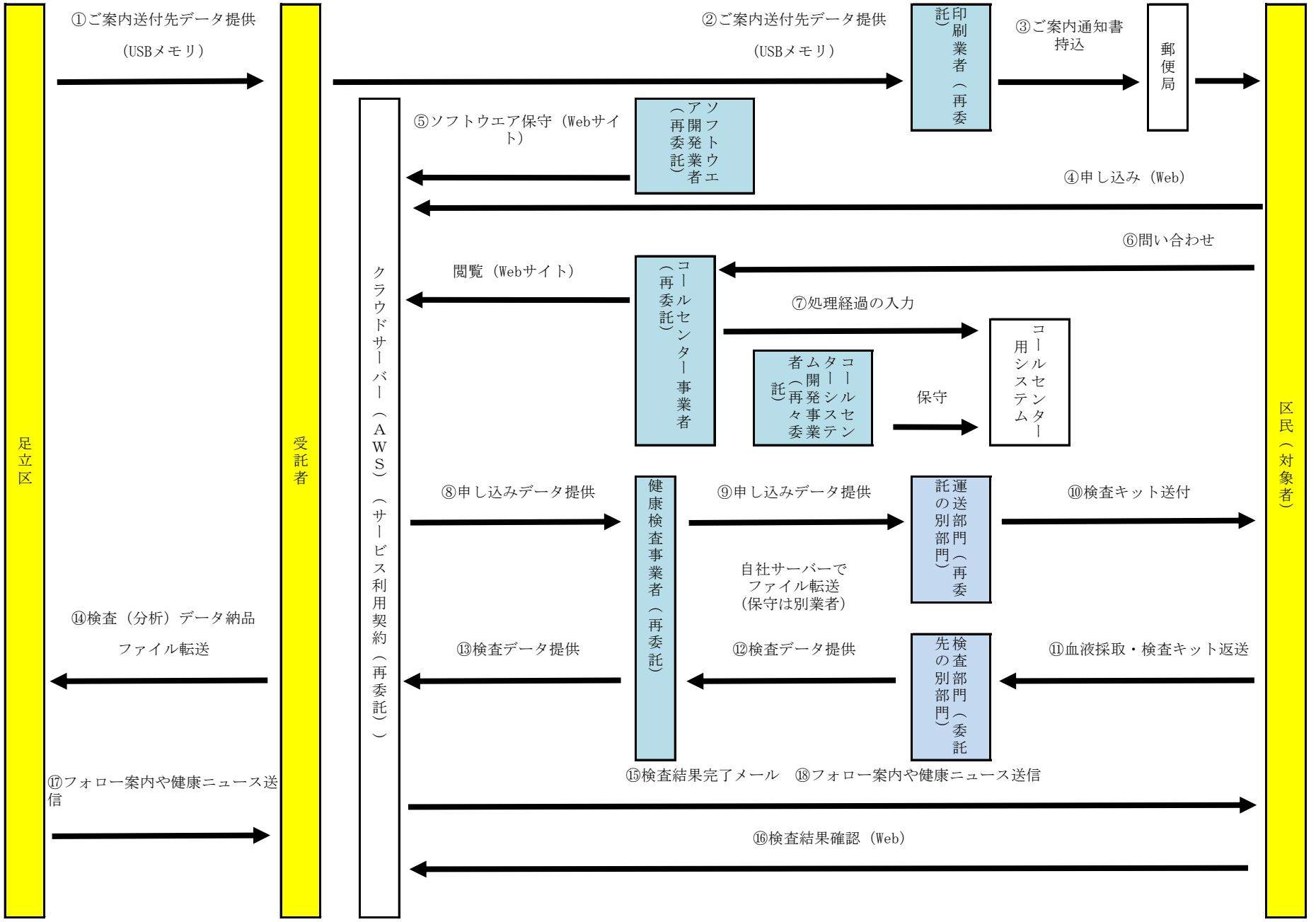
【個人情報委託の業務フロー図作成例：印刷委託】

【参考】



【個人情報委託の業務フロー図作成例：コールセンターを含む委託】

【参考】



実地検査チェックリスト

担当所管名：
契約名：
履行期間：
実地検査日：

見本

課長	係長	担当

		確認欄	指導内容
1　組織的安全管理措置			
ア	作業人数が報告書のとおりである。		
イ	作業責任者が作業現場で常時監督してる。		
ウ	作業手順書があり、手順書のとおり作業している。		
2　人的安全管理措置			
ア	業務内容に則した研修を行っている。		
3　物理的安全管理措置			
ア	作業は適切な場所で行っている。		
イ	保管場所は適切に管理されいる		
ウ	作業場所から倉庫等への搬送方法は適切である。		
エ	ＵＳＢメモリ等の外部記憶媒体の管理は適切である。		
オ	ＰＣの設置・使用状況は適切である		
カ	シュレッダーの機種、設置場所は適切である。		
キ	個人情報の収納場所の鍵の使用や管理は適切である。		
ク	溶解処理をしている場合は再委託申請書が提出している		
4　技術的安全管理措置			
ア	作業員一人ひとりに別のID、パスワードが割り振られている。		
イ	使用するOSやソフトは最新バージョンである。		
ウ	ウイルス対策ソフトが導入されている。		
エ	ファイアウォールの設定が「有効」となっている。		
オ	無線LANのアクセスポイントは適切な暗号化がされている。		
カ	クラウドサービスは仕様書の条件を満たしている。		
キ	作業に関係のないアプリなどがインストールされていない。		
ク	作業に使用している情報が、許可なく外部記憶媒体やメール等を使用して持ち出せないように管理されている。		
ケ	操作ログは取得している。定期的に不審な操作がないか分析している。		
コ	ＵＳＢポートは外部媒体が接続できないよう制御している。		
（5）再委託先の安全管理措置			
ア	再委託先の個人情報の取扱いについて書類提出させている		
イ	再委託先に対して実地検査等を行い個人情報の安全管理措置が適切であるかを確認している。		