震災リスクを踏まえた地方自治体の個人情報の取り扱いについて

Privacy policy of the local government on the basis of an earthquake disaster risk

所属　　札幌総合情報センター株式会社
氏名　　瀧口樹良
連絡先　　ki_takiguchi@snet.sweb.co.jp

１．はじめに

平成 23 年 3 月 11 日に起きた東日本大震災（以降、「大震災」と称す)」では、いくつかの地方自治体で庁舎そのものまでが大津波に襲われ、地方自治体の窓口機能が全て押し流されて崩壊するといった深刻な事態が生じた。その結果、庁舎の建物だけでなく、宮城県の南三陸町と女川町、岩手県の陸前高田市と大槌町では、戸籍の正本が津波で消失するなど、地方自治体の窓口サービスは大きな打撃を受けることとなった。そのため、東日本大震災は、情報セキュリティの 3 大要素である「可用性（Availability)」「完全性（Integrity)」「機密性（Confidentiality)」との関連で、大きな課題を突きつけることとなった。具体的には、地方自治体の窓口サービスが機能停止するなど、「可用性」を維持することができなくなり、また戸籍の正本が津波で消失するなど、「完全性」の点でも問題を引き起こした。要するに、地方自治体の住民の個人情報が紛失し、利用できなくなってしまったため、地方自治体の窓口サービスが実施できなくなってしまったのである。

一方、「機密性」の点では、支援団体に対して安否確認に必要な住民の個人情報（氏名、住所など）の提供を拒否する地方自治体が出てくる一方で、民間では Google の「Person Finder（消息情報)」などのクラウドを利用した安否情報提供に関する支援サイトが立ち上がり、家族や親族などの安否情報を求める住民への対応が図られた。さらに twitter を使って収集した情報の提供、避難所の名簿情報の提供など、個人情報の機密性に関して、地方自治体などの行政機関と民間との間の個人情報に対する取り扱いのスタンスの違いが散見された。このことは、震災時に、地方自治体の窓口サービスを行う際、どのようなかたちで住民の個人情報を取り扱うのが望ましいのかについて、平常時から地方自治体の側で想定しておく必要があると考えられる。

そこで、本研究では、今回の大震災の経験を踏まえ、震災リスクを想定した平常時からの地方自治体の個人情報の取り扱いについて考察を行うものとする。具体的には、「可用性」の観点から見た平常時における住民の個人情報の保管・管理のあり方と、「機密性」の観点から見た震災時における個人情報の外部提供のあり方について検討してみたい。

２．大震災のリスクとして派生した事実

今回の大震災のリスクについて、改めて情報セキュリティの 3 大要素（機密性、完全性、可用性）の観点に即して考察すると、まず、「機密性」の観点でいえば、震災後、被災した地方自治体に対して、障害者団体が障害者手帳などを持つ住民の個人情報の開示を求めたが、読売新聞が 2011 年 6 月に行った調査では、津波を受けた沿岸や福島第一原発からの避難をした地域で開示の要望を受けた 8 市町村のうち、

応じたのは南相馬市のみで、多くの地方自治体では、個人情報保護を理由に開示を拒んだとされる[1]。その一方で、民間では Google の「Person Finder（消息情報）などのクラウドを利用した安否情報提供に関する支援サイトを立ち上げ、家族や親族などの安否情報を求める住民に対して情報提供を行った。

また、「完全性」の観点では、陸前高田市では、戸籍正本や住民基本台帳など、行政文書すべてが流された。さらに宮城県本吉郡南三陸町，同県牡鹿郡女川町，岩手県上閉伊郡大槌町でも、戸籍の正本が津波で消失した。当初、法務省では各地方自治体を管轄する仙台法務局・盛岡地方法務局の支局には副本（電子データ）や届書が残っており、これらを基に戸籍を復元できるとしていた。しかし、住民が婚姻や養子縁組、出生や死亡など戸籍の変更を市町村に届け出てから、管轄法務局に伝わるまでには時間差があるため、2011 年 2 月～3 月に届け出があった変更については復元できないことが明らかとなり、法務省では前述した 4 市町に対し、当該届出等に関する申出で対応することにしている[2]。

さらに「可用性」の観点では、いくつかの地方自治体にて庁舎の建物が大津波に襲われ、地方自治体の窓口機能がそっくり押し流されて崩壊し、住民記録等が記載されたシステム等が停止した。その結果、窓口業務に用いるすべてのパソコンが海水をかぶって使い物にならなくなったり、住民基本台帳や戸籍などのデータを格納してあったサーバや磁気媒体が海水に浸ってデータ消失の危機にさらされたりしている[3]。

このように、情報セキュリティの観点においても、大震災は、地方自治体にとって大きなリスクが生じたとして捉えることができる。特に多数の行方不明者の安否確認作業から震災対応を行う等の住民生活を保障する観点での「可用性」の確保は、必要条件といえる。一方で、多数の行方不明者の安否確認を周囲に知らせる意味で、住民の個人情報の「機密性」の確保は、どこまで必要となるかが課題となる。従って、この「可用性」と「機密性」の要素に対する対応策を検討することが不可欠である。

３.「可用性」の観点から見たリスクに対する対応策

まず、「可用性」の観点から、リスクに対する対応策を検討してみたい。これまで、地方自治体では、住民基本台帳や戸籍などの台帳やデータを格納してあったサーバを自庁内に設置するという「リスクの保有」で対応してきた。しかしながら、今回の大震災では、そうした対応策が現実的には不可能であることを突き付けることになった。但し、「リスクの回避」として、地方自治体が住民の個人情報の取得し、保有することをやめることは不可能であることから、「リスクの低減」もしくは「リスク移転」の対応策が求められることになる。例えば、「リスクの低減」として、庁舎の耐震補強が考えられるが、大津波は防ぎようがない。従って、地方自治体の庁舎が被災しても、職員が他の施設でも窓口機能を継続できるように、災害時のバックアップ機能（遠隔地の代替設備・バックアップサーバなど）を確保するか、クラウド機能にデータを移行することが考えられる。例えば、岩手県釜石市では、2012 年 5 月 25 日に若崎正光副市長が北九州市を訪問し、北九州市と近隣自治体（12 市町）で構成する北九州地区電子自治体推進協議会総会（通称：KRIPP）の総会へ出席し、釜石市の KRIPP 加盟承認と釜石市の住民基本台帳

[1] 読売新聞（2012 年 3 月 20 日）「災害時の障害者支援…安否確認、個人情報の壁」（http://www.yomidr.yomiuri.co.jp/page.jsp?id=56251）及び読売新聞（2011 年 6 月 4 日）「障害者の安否確認進まず、個人情報保護法が壁」（http://www.yomiuri.co.jp/national/news/20110604-OYT1T00478.htm）

[2]法務省（2011 年 4 月 26 日）「東日本大震災により滅失した戸籍の再製データの作成完了について」（http://www.moj.go.jp/MINJI/minji04_00024.html）

[3]瀧口樹良（2011 年 4 月 8 日）「第 11 回【番外編】東日本大震災、早急に被災地の自治体窓口機能の支援を」日経 BP ガバメントテクノロジー（http://itpro.nikkeibp.co.jp/article/COLUMN/20110407/359208/?ST=print）

などのバックアップデータを北九州市で受け入れることが承諾されている[4]。

また、クラウドに移行することで、個人情報の保有リスクをクラウド提供事業者の責任に転換させることも考えられるが、リスクがすべて移転できるとは限りらず、新たなリスクが生じる可能性がある。例えば、クラウドの場合、回線の断絶には対応できず、衛星回線などの通信手段や発電機を配備し、いざという時の通信手段を確保しておかなくてはならない。また、外国のデータセンターを利用する場合も考えられ、紛争やテロなどのリスクが新たに発生しデータセンター内のデータについては、日本の法律の制約を受けないこと等、必ずしも「リスクの低減」もしくは「リスクの移転」になりえないことも考えられる。そこで、「可用性」の観点においては、緊急時のリスク管理として住民情報に関するデータや台帳の滅失を想定した「リスク分散」の視点を重視し、バックアップを他の地域に置く等の方法を検討する必要が出てくる。その際、例えば、基礎自治体である市町村は、互いに姉妹友好都市として提携しているところも多いことから、釜石市のような取り組みを広げて、緊急時に備えたバックアップデータ保管等の地方自治体間の協力関係により、災害時の相互支援が行えるような体制を構築すべきではないだろうか。

なお、戸籍の管理は戸籍法によって厳格に定められ、第 8 条で「正本は、これを市役所又は町村役場に備え、副本は、管轄法務局若しくは地方法務局又はその支局がこれを保存する」となっている。さらに、戸籍法施行規則第 7 条では「戸籍簿又は除籍簿は、事変を避けるためでなければ、市役所又は町村役場の外にこれを持ち出すことができない」とされており、一部事務組合を設置して管理しているケース以外、戸籍のサーバを庁舎外に設置しているケースはほとんど無い。そこで法務省では、戸籍副本データ管理システムの導入を 2013 年 9 月稼働させる予定としている[5]。この戸籍副本データ管理システムの運用が開始されると、副本は地方自治体から遠隔地となる全国 2 か所の副本データ管理センターで保存されることになる。

このように「可用性」の観点に対する対応策では、現在の住民の個人情報の集中化（集約化）から分散化であるが、現行の法制度（特に地方自治体にとっては、法定受託事務に該当する窓口業務に関する法制度）では、外部への個人情報の持ち出しを禁止しているケースもあり、法的な見直しも求められてくる。

４.「機密性」の観点から見たリスクに対する対応策

次に、「機密性」の観点から、リスクに対する対応策を検討してみたい。今回の大震災に限らず、安否確認等を行うためには、特にいわゆる災害弱者といわれる災害時要援護者に関する個人情報が必要となる。平成 18 年 3 月 28 日に内閣府が公表した「災害時要援護者の避難支援ガイドライン[6]」では「要援護者の避難支援は自助・地域（近隣）の共助を基本とし、市町村は、要援護者への避難支援対策と対応した避難準備（要援護者避難）情報（以下、「避難準備情報」という。）を発令するとともに、要援護者及び避難支援者までの迅速・確実な伝達体制の整備が不可欠である。また、要援護者に関する情報（住居、情報伝達体制、必要な支援内容等）を平常時から収集し、電子データ、ファイル等で管理・共有すると

[4] 林雅之（2012 年 09 月 27 日）「東北で導入が進む自治体クラウドのこれから」ITmedia（http://www.itmedia.co.jp/enterprise/articles/1209/27/news008.html）
[5] 読売新聞（2011 年 9 月 27 日）「戸籍データ、遠隔地バックアップへ…震災教訓に」（http://www.yomiuri.co.jp/politics/news/20110927-OYT1T00710.htm）
[6]内閣府（2006 年 3 月 28 日）「災害時要援護者の避難支援ガイドラインについて 」（http://www.bousai.go.jp/hinan_kentou/060328/index.html）

ともに、一人ひとりの要援護者に対して複数の避難支援者を定める等、具体的な避難支援計画（以下「避難支援プラン」と称する。）を策定しておくことが必要である」としている。しかしながら、現実的には、多くの地方自治体の現場で、前述の通り、住民の個人情報の「機密性」を理由に部外者への提供を拒否するケースが生じている。地方自治体の「個人情報保護条例」の多くは、その例外規定の「取得に際する利用目的の明示が不要な場合」や「利用目的以外の利用・提供ができる場合」として、「生命、身体、財産の保護のための緊急を要する場合」が掲げられている。但し、災害時要援護者に関する個人情報には、いわゆる「公知の情報」と合わせて「非公知の情報」や「機微な情報」も含まれていることから、各地方自治体の判断として、その取扱いが慎重とならざるを得ないのが実態である。なぜなら、一般的に地方自治体では、その職員に対して「個人情報保護条例」に基づく罰則（正当な理由なく個人の秘密に属する事項が記録された 公文書を提供する等の行為に対して）と、地方公務員法に基づく罰則（秘密を守る義務に対して）を課されている。そのため、守秘義務とそれに伴う刑罰が科せられている地方自治体の職員にとって、職員以外に対する外部提供に慎重になるのは、「法律による行政の原理」に基づく「法律の留保」の観点からすれば、ある意味で必然の結果といえる。

つまり、「災害救助という公事（被災者本人の生命・安全・財産を確保するという法益）に対して、「プライバシーという公事（プライバシーを確保するという法益）」という二律背反の相反関係のバランスを、「法律の留保」の観点から、どのように保つべきかが課題といえる。その際、そのバランスを判断するための基準と方法（手続き）が重要である。例えば、守秘義務とそれに伴う刑罰が科せられている地方自治体の職員以外に避難支援に直接携わる団体等の要援護者支援機関に対する第三者への要援護者情報の提供については、契約、誓約書の提出等により、要援護者の個人情報を受ける側に対して守秘義務を確保することが考えられるが、受ける側で法的責務や制裁を受けることのリスクまで引き受けることに対する責任の負担を重荷に感じてしまうケースもある[7]。

そのため、「機密性」の観点においては、地方自治体が保有する個人情報には、①公知な情報と②非公知な情報、さらに③機微（センシティブ）な情報が含まれている。そのため、①は公知な情報として本人同意を得ずに外部提供することは、災害時においては「生命、身体、財産の保護のための緊急を要する場合」として社会的受忍義務の範囲と認められるとした基準を、「個人情報保護条例」の施行細則等に定めておくことが必要ではないだろうか。但し、②、③に関して、個人情報の機密性を判断するプライバシーの基準は、取り扱う個人情報の性質の有無を問わず、本人同意という主観的判断に依存せざるを得ないことになる。そこで、②、③に関しては、予め、地方自治体側で要援護者支援機関を特定し、その間で、事前に個人情報の提供に関する協定を締結し、必要に応じて簡易で迅速な手続で第三者への情報提供が可能なことを、同じく「個人情報保護条例」の施行細則等に定め、地方自治体の職員の守秘義務の除外規定として法的に担保してく必要があるのではないだろうか。但し、その際には、住民の個人情報を提供した事後的な対応として、類型ごとに提供先と提供内容を本人に通知等を行うことで、個人情報の提供に対する差止請求権や、個人情報の適正な取扱いについて苦情処理をする窓口を設け、本人からの苦情申出権を保障し、適切な事後的救済措置を講じるようにすることが必要であろう。さらに、適正な取扱いをしない要援護者支援機関の団体等に対しては、行政罰や氏名等公表等の制裁措置をあらかじめ規定しておく等、二律背反の相反関係のバランスを保つための配慮が必要とされる。

---

[7] 読売新聞（2009 年 4 月 23 日）「三原市災害時要援護者避難支援プラン　個人情報管理住民に不安」（ http://www.yomiuri.co.jp/e-japan/hiroshima/feature/hiroshima1197001129611_02/news/20090422-OYT8T01066.htm）

５．おわりに

これまで震災リスクを踏まえた地方自治体の個人情報の取り扱いについて、情報セキュリティの観点から考察してきたが、今回の大震災の最大の教訓は、地方自治体の業務は、基本的に「決まったことを」「間違いなく」「確実に」行うという平時のオペレーションには長けているが、いわゆる「想定外」のリスク意識の欠如していることが明らかとなった。その結果、地方自治体の住民の個人情報の保管・管理や外部提供について、「想定外」の事態が陥った場合、その対応が適正な法的手続きを踏むことができずに問題を生み出してしまったのである。そのため、今後は、法的拘束力の乏しい国が提示する「ガイドライン・指針」の類ではなく、地方自治体の責務として「想定外」の場合を想定した「平常時」における地方自治体の住民の個人情報の保管・管理や外部提供のあり方を、地方自治体の「例規（条例や規則等の総称)」に定め、明確な基準と適正な法的手続きにて、情報セキュリティの「可用性」と「機密性」が担保されることが求められる。