特集 **いよいよ本格化するパーソナルデータの利活用**

個人情報のトレーサビリティ要件

崎村夏彦

CONTENTS

要　約

1　改正個人情報保護法で導入された新たな規制に、新25、26条に書かれたトレーサビリティ要件がある。

2　これは、「いわゆる名簿屋」問題を契機に導入されたものだが、文面通りに解釈すると、産業を阻害する可能性が高いことから、国会でも長時間にわたって審議された。

3　法文が許す限り産業阻害度を減らした形で、委員会規則を作る必要がある。そのためには、実際のユースケースに即して検討しなければならない。

4　類型的分析をしたところ、最低限の規制しかかからない規則にしても、若干のシステム変更は避け得ないと見られる。2016年中の施行を考えると、かなり早い段階でのシステム変更準備が必要になる。

Ⅰ トレーサビリティ要件の概要

1 トレーサビリティ要件の背景

2015年９月３日に成立した改正個人情報保護法は、いくつかの重要な変更を含んでいる。その中で、本稿で取り上げるのは、第三者提供に関わるトレーサビリティ要件についてである。

これは、個人情報保護法改正大綱には入っていなかった要件である。大綱が発表された後に発覚した、某通信教育会社の顧客名簿の漏洩に端を発するものである。

同事件にはいくつかの特徴があったが、今回の改正にインパクトを与えたのは、漏洩した情報が「いわゆる名簿屋」を通じてロンダリングされながら、広範に流通してしまったということである。最初に犯人からデータを購入したのは、名簿屋S社であるようだ。同社は、2013年７月から14年６月にかけて、犯人から計13回、延べ１億7500万件の情報を計約280万円で買い取り、ほかの名簿業者や学習塾など全国の46の顧客に計1100万円で転売していた[注1]。さらにこのデータは、３社の名簿業者から少なくとも10以上の名簿業者に転売され、最終的に学習塾や予備校、呉服店など数百社に渡っている[注2]。

また、野村総合研究所（NRI）が2015年７月、独自に行った調査によれば、同じIPアドレスを持つサーバーから、複数の社名を使って、情報が次々に転々流通していたことも分かっている。これは、以前から指摘されていた個人情報保護法第23条第２項の問題点を、マスコミなどにも分かりやすく明るみに出した事例であった。現行の個人情報保護法の第23条を見ると、次のように書いてある。

第二十三条　個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

[..中略..]

２　個人情報取扱事業者は、第三者に提供される個人データについて、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、次に掲げる事項について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。

一　第三者への提供を利用目的とすること。

二　第三者に提供される個人データの項目

三　第三者への提供の手段又は方法

四　本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること。

出所）個人情報の保護に関する法律（平成十五年五月三十日法律第五十七号）

つまり、オプトアウトが提供されていて、「あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いて」おり、上記の一～四を満たしている場合は、個人データの第三者提供は自由というわけだ。

問題は、この「又は本人が容易に知り得る状態に置いているとき」である。

経産省ガイドラインによると、「本人が容易に知り得る状態」とは、「本人が知ろうとすれば、時間的にも、その手段においても、簡単に知ることができる状態に置いていることをいい、事業の性質及び個人情報の取扱状

況に応じ、内容が本人に認識される合理的かつ適切な方法」とあり、その例示として「ウェブ画面中のトップページから１回程度の操作で到達できる場所への掲載等が継続的に行われていること」となっている。

この規定は、素人目には当該個人がその業者やサービスと接する機会がある場合のことを指しているように見えるが、専門家の意見によると、形式的に上記を満たしていればよいとされている。これが、以前から指摘されている個人情報保護法の抜け穴である。

どこの誰かも分からない名簿業者のウェブサイトを、能動的に一件ずつ個人が発見していくことは極めて困難であり、まして、以下のような連鎖攻撃をされたときは絶対に不可能と考えるべきである。

攻撃例：
第三者提供を業とする業者Aが同様の業者Bに提供。さらにそれをBがCに提供。それぞれがウェブサイトを作り、そこから１クリックのところに告示する。これを永遠に続けてゆく。もちろん、これらの業者はすべて第三者提供を業とするところから「適正に取得」しているわけである。

まさにこれが、今回起きたことである。

この点は、長らく「理論的な抜け穴」として扱われていたが、報道などで問題になることは少なかった。今回、実際の事例として被害を生んだため、ようやく12年ぶりに対策が行われることになった。これが改正案に導入されたトレーサビリティ要件である。

このような観点で見ると、2014年12月19日の第13回パーソナルデータ検討会に提示された改定案の概要は妥当なものに思われた。これによると、個人情報の保護を強化するための規定の整備の一環として、以下のようになっていた。

(2) 第三者提供に係る確認及び記録の作成の義務付け
（ア）個人情報取扱事業者は、個人情報データベース等の提供を受けるときは、その提供をする者が当該個人情報データベース等を取得した経緯等を確認するとともに、提供の年月日、当該確認に係る事項等の記録を作成し、一定の期間保存しなければならないこととする。
（イ）個人情報取扱事業者は、個人情報データベース等の第三者提供をしたときは、提供の年月日、提供先の氏名等の記録を作成し、一定の期間保存しなければならないこととする。

出所）内閣官房IT総合戦略室パーソナルデータ関連制度担当室、2014（下線は筆者による）

オプトアウトで名簿という「個人情報データベース」を提供・受領する際に、トレーサビリティの義務規定が加わったと読み取ることができる。

ところが、2015年３月10日に閣議決定された改正案はこれと違っていた。

2　個人情報の第三者提供にかかる義務

個人情報の第三者提供にかかる義務規定は、法案第25条で導入された。

第二十五条　個人情報取扱事業者は、個人データを第三者（第二条第五項各号

に掲げる者を除く。以下この条及び次条において同じ。）に提供したときは、個人情報保護委員会規則で定めるところにより、当該個人データを提供した年月日、当該第三者の氏名又は名称その他の個人情報保護委員会規則で定める事項に関する記録を作成しなければならない。ただし、当該個人データの提供が第二十三条第一項各号又は第五項各号のいずれか（前条の規定による個人データの提供にあっては、第二十三条第一項各号のいずれか）に該当する場合は、この限りではない。

2　個人情報取扱事業者は、前号の記録を、当該記録を作成した日から個人情報保護委員会規則で定める期間保存しなければならない。

出所）内閣官房「個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律案　新旧対照条文」

個人データを第三者に提供する場合は、提供年月日、氏名ほかの提供先に関する事項を記録しなければならないというわけだが、これは、2014年12月の段階で筆者らが期待していたものとは、２つの意味で大きく違った。

①対象がオプトアウトで提供している事業者に限られていない

②個人情報データベースの提供ではなく、個人データの提供になっている

①であるが、筆者らが期待していたのは「第二十三条第二項の規定によって第三者提供する個人情報取扱事業者は」のように、対象に制限が入るものであった。ところが上記では、単に「個人情報取扱事業者は」となっている。これでは名簿屋以外が幅広く入ってしまう。もっとも「ただし」以降に第23条がらみの例外が入っているので、まずはそちらを見てみた。新23条は以下のようになっている。

第二十三条　個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

一　法令に基づく場合

二　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

三　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

四　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

[..中略..]

5　次に掲げる場合において、当該個人データの提供を受ける者は、前各項の規定の適用については、第三者に該当しないものとする。

一　個人情報取扱事業者が利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託することに伴って当該個人データが提供される場合

二　合併その他の事由による事業の承継に伴って個人データが提供される場合

三　特定の者との間で共同して利用される個人データが当該特定の者に提供される

場合であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき。

出所）内閣官房「個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律案　新旧対照条文」

まず簡単な方の例外である第５項を見よう。これによると、例外になっているのは「委託」「合併」およびグループ内などの「共同利用」のケースとなる。これらの場合は記録をとらなくてよいことになっている。これは適切といえる。問題は第１項の方である。

第１項は「個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない」から始まるので、一見すると本人の同意を得ている場合は第25条の例外に当たるかのように錯覚しがちがだが、例外になっているのは「第二十三条第一項各号」に当たる場合であって、この柱書は関係ない。つまり、同意の有無とは関係なく、第25条の規制はかかってくるということである。

当初、これは「バグ」であろうと考えた。だが、2015年４月１日に担当室を訪問して「個人的」見解を伺ったところ、本人同意がある場合が除外されていないのは意図的だそうである。第三者提供全体にトレーサビリティが必要だと考えており、法案第25条、26条の記録義務はこれを担保するためのものだから、同意がある場合も対象にすべく起草したとのことであった。やや驚きではあるが、バグではなかった。

3　トレーサビリティ要件の現実性

同意がない場合の第三者提供にかかる記録義務の規制は、諸外国にも存在する。だが、同意がある場合にも同様の義務を置くのは、異例の厳しい規制といえる。また、その実施可能性ないしは実効性にも大いに疑問符がつく。そこで、同意のある第三者提供の事例をいくつか考えてみよう。

事例１：SNS事業者が提供する場合

まず、フェイスブックなどのSNS（ソーシャルネットワーキングサービス）におけるプロフィールページの提供を考えてみよう。

SNSにおいては、本人その他からのデータをいったんSNSのデータベースに溜め、それを加工してさまざまな対象に、本人同意の下で提供する。本人同意があっても、それは第三者提供に係る本人同意であって、本人からの提供指示ではないので、本人からの委託ではない。フェイスブックが北米外個人のデータを管理しているアイルランドのデータ保護コミッショナーオフィスによる、Facebook-Irelandについての監査レポート（2011年）[注3]でも、その位置付けとなっている。このような場合にも改正法文を素直に読むと義務がかかってしまうことになる。

なお、同様のことは、社員の紹介を自社のウェブサイトに載せる場合にもいえるであろう。社員は当然そのことに同意していることが想定されるが、社員の委託を受けて載せているわけではないから、やはり第三者提供と位置付けられる。

事例２：八百屋が魚屋にお客の電話番号を伝える場合

2015年５月13日の内閣委員会審議で出た事

例の一つに、「八百屋が隣の魚屋に客の電話番号を伝える場合」がある。このようなケースは、これまでは第２条の小規模事業者を例外とする規定によって考えなくてもよかったものが、考えなければならなくなった事例である。

この事例では、客は八百屋も魚屋も信頼しており、必要に応じて八百屋が魚屋に自分の連絡先を伝達するのも構わないと思っている。つまり、同意がある。そのような場合であっても、八百屋が魚屋に電話番号を伝えたら、委託で伝えているわけではないので第三者提供になる。諸外国であれば、これは同意に基づく第三者提供であるから、何ら問題はない。しかし、改正案ではこれにも記録義務がついて回る。これは明らかに過剰であろうというのが、国会論戦のポイントであった。

4　提供者の記録義務の内容

新25条で規定している義務は以下の記録である。

- 提供したデータの内容
- 提供年月日
- **当該第三者の氏名又は名称その他の個人情報保護委員会規則で定める事項**

2015年４月１日の訪問時には、これらは普通にログを取っていれば記録されているはずとのことであった。ページを閲覧している人が誰かは記録を取っているであろうし、「IPアドレスがあれば、参照者の氏名・名称も分かるだろう」との考えであったようだ。しかし、公開プロフィールページやタイムラインの場合には、どのユーザーかは分からないし、IPアドレスを見てもそれが誰のものか、どの社のものか分かるとは限らない。したがって、氏名や名称、住所などを記録することは現実的でない。

そのためか、国会答弁においては「本人がフェイスブックなどにアップする場合に、基本的に大体そのまま載るようになってございますので、そういう、載るものを本人が全てコントロールできるようなものについては、そもそも提供に当たるのかという問題もあろうかと思います。実際に、そのような場合に、たとえば本人、あるいはフェイスブックなどの、そういうSNSを運用している会社にすべてそれを義務付けるのはやや無理があると考えられますので、それらにつきましては基本的に必要のない方向で検討してまいりたい」[注4]とされた。

また、同様に、八百屋のユースケースに関しては、「（事前同意なら）法の趣旨から見て必要ないとする規則も考えられる」[注5]との答弁もあった。

とはいえ、法律に書いてあることを委員会規則で必要なしとすることは難しいと考えられるので、何らかの記録義務は生じると考えるべきであろう。実際、前述の答弁の後に「やや法文を逸脱するというなら、こういうことをしているというふうなことだけを書くというふうな最も簡易な方法もあり得る」[注6]との答弁が行われている。

そこで問題になるのが、新25条の「氏名又は名称」である。これを記録するのはいかにも無理だ。一つ考えられるのは、法文が「氏名又は名称その他の個人情報保護委員会規則で定める事項」であり、「氏名又は名称及びその他の個人情報保護委員会規則で定める事項」ではない[注7]ことを利用して委員会規則を定めるやり方だ。この法文であると、「（氏名）又は（名称その他の個人情報保護委員会規則で定める事項）」であり、（名称その他の個人情報保護委員会規則で定める事項）が１単語

であるとの論を立てることができる。そうであれば、（名称その他の個人情報保護委員会規則で定める事項）として、たとえばIPアドレス単体を定める事項とすると、ログにあるIPアドレスでもよさそうだ。ただし、ログに記録されるページのアドレスが、どの個人データを含んでいるか分かるものにする必要はあるため、システム改変が必要になる場合もあり得る。

5 個人事業取扱事業者がSNSを参照した場合

一方、新26条では参照側が個人情報取扱事業者（個人情報データベースなどを事業の用に供している者）だった場合の義務を記載している。

第二十六条　個人情報取扱事業者は、第三者から個人データの提供を受けるに際しては、個人情報保護委員会規則で定めるところにより、次に掲げる事項の確認を行わなければならない。ただし、当該個人データの提供が第二十三条第一項各号又は第五項各号のいずれかに該当する場合は、この限りでない。

一　当該第三者の氏名又は名称及び住所並びに法人にあっては、その代表者（法人でない団体で代表者又は管理人の定めのあるものにあっては、その代表者又は管理人）の氏名

二　当該第三者による当該個人データの取得の経緯

2　前項の第三者は、個人情報取扱事業者が同項の規定による確認を行う場合において、当該個人情報取扱事業者に対して、当該確認に係る事項を偽ってはならない。

3　個人情報取扱事業者は、第一項の規定による確認を行ったときは、個人情報保護委員会規則で定めるところにより、当該個人データの提供を受けた年月日、当該確認に係る事項その他の個人情報保護委員会規則で定める事項に関する記録を作成しなければならない。

4　個人情報取扱事業者は、前項の記録を、当該記録を作成した日から個人情報保護委員会規則で定める期間保存しなければならない。

出所）内閣官房「個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律案　新旧対照条文」

これによると、個人情報取扱事業者の社員が、業務でSNSのページなどを参照した場合、SNSの名称、代表者氏名および個人データ取得の経緯を調べ、「当該個人データの提供を受けた年月日、当該確認に係る事項その他の個人情報保護委員会規則で定める事項」を記録しなければならないことになる。

ここでも「当該確認に係る事項その他の個人情報保護委員会規則で定める事項」の解釈が問題になる。もしもこれに「誰の情報を取得したか」が入るとすると、かなり難しくなるケースが想定される。

API（アプリケーションプログラミングインターフェース）でプロフィール情報などを取得している場合には、恐らくログを残しているであろうと考えられるのでまだよい。しかし、プロフィールページ閲覧の場合にログを残しているかは疑わしい。数週間分程度であれば、ブラウザーの閲覧履歴に残っているかもしれないが、シークレットモードで参照

した場合には残らない。そもそも保存期間は５年などを考えているとされるため、通常のブラウザーの履歴では、ブラウザーにプラグインなどを追加しないと難しい。

また、取得の経緯は通常提供されないため、これをいかにして取得するかについても問題になる。API経由での取得の場合、提供元が日本の事業者であれば、特別に項目を作って対応してくれる可能性もある[注8]が、海外事業者だと難しいだろう（取得の経緯について、多くのSNSでは、本人による直接入力以外に、機械によって自動的に記入されるものや、他事業者経由で取得するものもあるが、どこかで本人同意が入っていれば、これらはみな、「本人同意による」と記載すればよいらしい。個社のウェブサイト掲載する場合も同様であろう）。

また、現状ではページを閲覧するときに、そのページの提供者の「氏名＋住所」あるいは「名称＋住所＋代表者氏名」を記録しているわけではない。自動化するには、サイト側がこうしたメタデータを標準化された形式で提供する必要がある。これらは、API経由の取得でも同じことがいえる。動的に新しいサーバーに接続して個人データを取得する場合はもちろん、最初に登録したときに記録したとしても、その後代表者が変わったときにそれを記録するためには、やはりプロトコル的に自動で提供されるようになっていないと厳しい。

6　日本の事業者が直面する不利な状況

前述の通り、このような規制は他国では類を見ないように思われる。従って、他国の事業者がこのような対応をするかは甚だ疑わしい。日本の事業者だけが追加コストを払うことになり、不利な状況に置かれるのではないかとの疑問が上がってくる。

場合によっては海外への移転を考えたり、同意モデルを捨てて名簿屋モデルに走ったりすることもあり得る。現在は遵法精神をもって、第23条第２項の抜け穴は使わずに同意を取得してデータの提供を行っているわけであるが、この同意の取得は離脱率が２～３割程度もあり、かなりコストの高いものである。これに対して、名簿屋モデルだと、委員会に届け出するだけで、脱落率は原理的にゼロである。コスト換算をすると、名簿屋モデルの方が望ましいとの判断をすることも想像に難くない。

この点について前述の担当者に質問したところ、「もしも海外に移転させて日本向けのサービス提供を行う事業者が出た場合には、域外適用の対象となるであろう」とのことであった。また、名簿屋として届け出をした場合は、委員会の監視をずっと受けることになるので、そのコストを勘案する必要は生じる。だが、３割の脱落は、売上の３割のコストにも相当し得る。これに比べると、監視されるコストは小さいとも考えられる。

7　委員会規則が重要

以上から分かるのは、委員会規則をどう定めるかが極めて重要になるということである。委員会規則で「名称その他の個人情報保護委員会規則で定める事項」が「事業者の名称＋住所＋代表者氏名」などとされれば、提供側にとって死活問題となる。逆に、「IPアドレスでOK」となれば、対応可能かもしれない。取得の経緯も、「本人同意と書けばよい」となれば問題ないだろうが、「直接の受領元と日時」のようになったら、対応しきれないだろう。

受領者側に関しては、上記のように、提供側が機械可読な形で情報提供するとともに、ブラウザーにプラグインなどを追加しない限り、法令遵守は難しそうだ。

そう考えると、交通法規のように、「大部分の人は違反しているが、その人たちは捕まえない。事故を起こした人と、明らかに怪しい人だけを、この法文を使って捕まえる」という運用でカバーする対応になるのかもしれない。だがそれでは裁量行政の最たるものとなり、国民の自由を守るという点でも明らかに望ましくない。従って、規則は法文が許す限り、産業阻害度を減らした形で作ることが望ましい。それには、実際のユースケースに即して検討する必要がある。そこで、第Ⅱ章では、現在利用が多い形態のシステムを類型的に分析して、どのような対応が可能かを考える。

Ⅱ 考えられるシステム的対応

本稿執筆時点（2015年９月）では委員会規則がないので、最終的に内容がどうなるかは分からない。とはいえ、2016年中に改正法が施行されることを考えた場合、ある程度予測して動き始めることは必要であろう。ここでは、法文を無理やり負荷がないように解釈した上で、必要になりそうなシステム的手当を、次の類型に分類して考える。

ケース分析

ケースP–A：提供者システム（API提供）

具体性を持たせるために、昨今主流になっているOAuth 2.0[注9]／OpenID Connectベースの提供を考える。OAuth 2.0は、APIに対するアクセス制御を行うためのプロトコルで、OpenID ConnectはOAuth 2.0を使ってユーザーの情報をサーバー間で転送するための仕組み／APIである。ほかのAPIの場合は適宜読み替えていただきたい。

提供者として記録しなければならないのは次の通りである。

- 提供したデータの内容
- 提供年月日
- **当該第三者の氏名又は名称その他の個人情報保護委員会規則で定める事項**

提供先からは取得の経緯も要求されるので、これも別の形で記録しておいて、同時に提供する必要がある。

提供したデータの内容は、ある程度包括的に記録することが許されると考えると、OAuthの場合はscopeを記録すればよいと考えられる。OAuthのscopeは、アクセスの範囲などを示すために使われるパラメーターで、たとえばOpenID Connectでは「profile」「email」のような形で定義している[注10]。

提供年月日は問題ない。そのAPIがアクセスされた年月日を使えばよい。

「当該第三者の氏名又は名称その他」は、現段階だと何になるのか予断を許さない。担当室がいうようにIPアドレスでよいのであれば、それは今でも記録しているであろうが、先方が動的に割り当てられるIPアドレスを使っている場合、それを記録しておくことに何の意味があるか、いささか疑問である。また、１つのIPアドレスで複数の主体にサービスが提供されている場合、そのIPアドレスからは結局誰が当該第三者だったのか分からない。

表1　必要になりそうなシステム手当

	提供者システム（P）	受領者システム（R）
API提供	ケースP–A	ケースR–A
ページ提供	ケースP–P	ケースR–P
音声・メールなど非定型提供	ケースP–M	ケースR–M

OAuthでは、要求送信元をClient IDと呼ばれる識別子で判別するので、これを記録すればよいが、OAuth 2.0［RFC6750］でのAPIアクセス時には、クライアントはClient IDを送らない。送るのはAccess Tokenと呼ばれる、APIのアクセス許可の状態を示す文字列だけである。そこで、このような場合には、Access TokenがどのClient IDに対して発行されたかを記録しておいて、ログにはAccess Tokenから引いたそのClient IDを記録するということになろう。

ただし、Public Clientと呼ばれるタイプの要求送信元の場合は、Client IDが分かったところで、ほとんどは単に使用ソフトウエアが分かるだけであるし、なりすましも容易であるから意味がない。この場合は、IPアドレスの方がまだ特定性があると考えられるので、IPアドレスを記録するほうがよいであろう。

また、提供者の記録義務にはないが、受領者の記録義務にある「取得の経緯」を、提供者は別途記録し、何らかの形で受領者に伝えなければならない。方式として考えられるのは、サーバー設定ファイルに記録して公開（例：OpenID Provider Metadata[注11]）するか、APIのレスポンスに挿入するかである。どちらの場合も、受領者側が自動処理をするためには、標準プロトコルを整備する必要があろう。

ケースR-A：受領者システム（API提供）

さて、プロバイダーの提供にかかる点を切り出した「ケースP-A」と対になるのが、受領者の受け取りを扱う「ケースR-A」である。

まず、記録しなければいけない事項をもう一度復習すると、次の通りである。

- 氏名（個人）又は名称（法人）
- 住所
- （法人、その他団体の場合）代表者
- 当該個人データの取得の経緯

まず、「氏名又は名称」であるが、OAuth/OpenID Connectの場合、必ずTLS[注12]を使うので、少なくともX.509証明書レベルでの提供者（多くの場合は提供ドメインのみだが）は分かる。このドメインを記録しておいて、後から必要であれば調べる[注13]という仕組みが考えられる。

「住所」はそもそも、国によっては「住所」という概念がなかったりするなど解釈が難しい。日本における住所とは、伝統的に①相手を一意に特定するための準識別子の一部②連絡先③相手の身柄を押さえるのに役立つ情報、などの意味を持っているようだが、もし①の意味でここに書いているのであれば、そもそもドメイン名で事足りる。②の意味であれば、ドメイン名からwhoisで検索することによって、住所が分かる可能性がある。また、少なくとも「postmaster@ドメイン名」などのアドレスでメールが届くはずであるので、やはりドメイン名で「住所」に代えるというのが現実線であろう。

次に「代表者」であるが、これもドメイン名から後付で調べるという方式が妥当であろう[注14]。

最後の「当該個人データの取得の経緯」であるが、これは提供者側が能動的に提供するより方法がない。前述のサーバー設定ファイルかAPIレスポンスに記述してあれば、それをログに残すという対応が考えられる。ただし、海外のサービスは基本的に対応してくれないと思われるので、ここをどう取り扱うかが課題であろう。

ケースP–P：提供者システム（ページ提供）

ウェブページなどで提供する場合は、システムがRESTベースであるか否かによって対応が分かれる。

RESTベースのシステムであれば、通常のウェブサーバーのログだけで、提供した情報の種類と日時は記録されている。さらに、ユーザー認証をしているページであれば、そのユーザー名も合わせて取ることが可能であるので、きちんとユーザーのID管理をして、過去分も取っておけばよい。

一方、RESTベースでないシステムの場合は、リクエストのパラメーターも含めてログに保存する必要がある。これは行っていないサーバーも多いと思われるので、対応が必要だ。ただし、単純に記録すると、今度はセキュリティリスクが増加する恐れがあるので注意が必要である。

また、公開ページである場合には、原則的にアクセスしているユーザーは分からない。IPアドレスの記録はできるが、そこから当該事業者としてはユーザーに遡ることはできないことが多い（立ち入り捜査権でもない限り、難しいことが多い）。しかし、ほかに方法がないので、IPアドレスの記録をするのであろう。

取得の経緯の提供は、そのページのメタデータに埋め込むのがベストと考えられる。すべての個人情報が本人同意によるものならば、サーバーの設定に一行追加することで事足りる。ただしこれも、表現方式の標準化が必要である。

ケースR–P：受領者システム（ページ提供）

この場合の一番典型的な受領形態は、社員がウェブブラウザーでページを参照することであろう。ここから、前述の「氏名（個人）又は名称（法人）」「住所」「（法人、その他団体の場合）代表者」「当該個人データの取得の経緯」をどうやって記録するかということが問題である。

APIの場合と取得する情報は同じであるが、大きな問題は、どの要求が個人データを含むもので、どれがそうでないかは分からないということである。

ケースP–M：提供者システム（音声・メールなど非定型提供）

電話やメールなどの問い合わせに対して、自分以外の個人情報を答えた場合にも第三者提供になる。しかし、API提供やページ提供のようなシステムが提供する場合と違って、自動記録は難しい。何らかの手動処理が入ることは避けられない。

たとえば、メールの場合には、件名に［個人情報］のような文字列を必ず入れることにして、それをメールアーカイブから検索できるようにするなどであろう。電話での応対は基本的に行わないことをポリシーとして、必ずメールで上記のルールで送るようにすれば、先方のメールアドレスが「氏名等」に該当し、送信日時が「年月日」、送信内容は、事後的に本文から探すことができるところで留める、というようなことが考えられるであろう。

ケースR–M：受領者システム（音声・メールなど非定型提供）

さて、提供者側は自分で定めたルールに従ってメールを送ればよいが、受け取る側にはそれぞれの提供者側が勝手に決めたフォーマットで届くので、その記録は一筋縄ではいかない。また、当然、提供者側が必要な情報を

つけてこないこともあり得るであろう。

その場合、別途必要な情報を問い合わせ、それを記録することになる。システム的に最も簡単なのは、記録用のメールアドレスを社内に作って、必要事項を書き込んだメールを転送することだろうか。

Ⅲ 終わりに ―委員会規則の形の展望

トレーサビリティを取るというのは、特に名簿屋対策としての一般論としては望ましいことであろう。しかし、これを本人同意があるような場合にまで拡張して、法文を厳格な方向に解釈すると、産業を大きく阻害することになる。ただし、一般企業に影響がないところまで緩めると、今度は名簿屋対策としての意味が薄れてしまう。

本稿執筆時点では、まだ改正個人情報保護法は成立したばかりであり、当然委員会規則も出ていない。その中で、法文を逸脱しない範囲でできるだけ緩く解釈し、その際に企業として取り得る対策の例を挙げた。実際に委員会規則ができるときには、せめてこの程度まで緩く解釈した上で、たとえば「一定期間内に同一の提供先に5000件以上提供するときには」といったように、いわゆる名簿屋に実質的な網がかかる委員会規則にしていく必要があるように思われる。

注

1 2014年10月28日の朝日新聞記事
2 2014年７月11日の毎日新聞記事
3 Data Protection Commissioner : Facebook Ireland Report of Audit (2011), https://www.dataprotection.ie/documents/facebook%20report/final%20report/report.pdf (2015/７/１取得)
4 2015/５/15 内閣委員会、向井治紀参考人発言。
5 2015/５/20 内閣委員会、向井治紀参考人発言。
6 2014/５/20 内閣委員会、向井治紀参考人発言。
7 吉田利宏『元法制局キャリアが教える 法律を読む技術・学ぶ技術［第２版］』による。この解釈について板倉陽一郎弁護士（産業技術総合研究所高木浩光先生）と鈴木教授（直接）にも確認してみた。板倉弁護士の見解は「『氏名　OR　規則で定める事項（∋名称)』、『規則で定める事項（∋氏名　OR　名称)』双方あり得る。『AまたはBその他の規則で定めるC』というときに、AやBは例示であって入らない場合もある」。これに対して鈴木正朝新潟大学教授の見解は、「例示列挙だとしても、典型例として条文冒頭に掲げておいて、ご都合主義的に省略していいわという運用は、は？という感じではある」とのことで、悩ましい
8 国内のみで通用する独自仕様でよいとするのか、それともIETF、OIDF、OASIS、W3Cなど各プロトコルを担当している国際標準化団体で標準化するのか決める必要がある
9 RFC6749、RFC6750
10 http://openid.net/specs/openid-connect-core-1_0.html#ScopeClaims
11 http://openid.net/specs/openid-connect-discovery-1_0.html#ProviderMetadata
12 Transport Layer Security。通信相手を確認し、通信を暗号化する方式
13 直近分については、whoisという仕組みで、組織名やドメイン管理者およびその連絡先を取得することができる。過去分においても、それを提供するサービスがある。ただし、匿名化されている場合があり、この場合はこの方法では対応が難しい
14 もちろん分かるとは限らないが、それ以上を求めるとインターネットが使えなくなってしまう

著者

崎村夏彦（さきむらなつひこ）
ITイノベーション推進部上席研究員
専門はデジタル・アイデンティティとプライバシー技術