平成２４年２月２３日

「個人情報流出時の対応手順」

上條・鶴巻法律事務所

弁護士　鶴巻　暁

1　流出時の「対外的対応 3 点セット」を避けられるか・避けるべきか

個人情報の流出事故が発生したばかりの事業者から、

「本人への連絡・主務大臣への報告・公表（以下、本稿ではこれらを総称して「対外的対応 3 点セット」という。）をしなければならないか？」

という相談をいただくことがたびたびある。「できれば避けたいのだが」というニュアンスを含む場合も少なくない。これらを行うことによって自社の信用が毀損するのではないかという懸念はもっともなことであるが、やるべきことをやっていなかったことが後日発覚することによる信用毀損リスクのほうも決して無視できない。

片や、認定個人情報保護団体の説明会などでは「報告は必須である」というような、単純な説明がなされることがある。「ファクシミリ 1 枚の誤送信であっても、流出した情報が一般に知られたものであっても、個人情報の流出である限りは報告しなければならない」というような表面的な説明を聞くと、逆に、個人情報の内容・種類に応じて重要性が異なるという点について認識が足りないのではないかと不安になってしまう。

そこで本稿では、この問題について、事業者としてどのように対応するべきかを検討する。ポイントは以下のとおりである。

・不必要なら、対外的対応はできるだけ避けたい
・しかし、必要な対外的対応を行わなかったために、後日非難を受けることも避けたい
・「隠して乗り切る」というスタンスには立たない
・対外的に誠意を持って対応したいが、不当な要求に応じることは避けたい

2　法令等の内容を再確認する

（1）個人情報保護法

流出時の対応について、個人情報の保護に関する法律（以下、「個人情報保護法」または単に「法」という。）では「個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失または毀損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない」と定められているだけである（法 20 条）。対外的対応についての具体

的な規定はない[1]。

（2）経済産業分野ガイドライン

各省庁が定めるガイドラインのうち、もっとも代表的なものが「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」（以下、「経済産業分野ガイドライン」という。）である。

同ガイドラインでは、安全管理措置を 4 種類（組織的安全管理措置・人的安全管理措置・物理的安全管理措置・技術的安全管理措置）に分けて詳しく規定している。このうちの【組織的安全管理措置として講じなければならない事項】の 5 項目のひとつとして「事故又は違反への対処」という項目が置かれており、【各項目を実践するために講じることが望まれる手法の例示】として、以下の手順を整備することが挙げられている[2]。このうち（エ）（オ）（カ）が本稿で取り上げる対外的対応 3 点セットである。

(ア)事実調査、原因の究明

(イ)影響範囲の特定

(ウ)再発防止策の検討・実施

(エ)影響を受ける可能性のある本人への連絡

(オ)主務大臣等への報告

(カ)事実関係、再発防止策等の公表

（3）JIS Q 15001 ではどのように定められているか

事業者における個人情報保護の取り組みを標準化したものが、日本工業規格のひとつである「個人情報保護マネジメントシステム要求事項（JIS Q 15001）」である[3]。同規格はプライバシーマーク制度[4]において、認証の基準として用いられている。

同規格において、安全管理措置についての要求事項としては、法 20 条と同様のものがあるだけである[5]が、その他に「緊急事態への準備」についての要求事項が置かれている[6]。同事項においても、次のとおり、対外的対応 3 点セットについて規定されている。

---

[1] 安全管理措置を講じなければならないのは「個人データ」に限定されている。個人データベース（コンピュータを用いて検索することができるように体系的に構成したもの等。法 2 条 2 項）を構成する個人情報が「個人データ」である（同条 4 項）。これに該当しない個人情報は、安全管理措置の対象とならない。

[2] ただし、書店で誰もが容易に入手できる市販名簿等（事業者において全く加工をしていないもの）を紛失等した場合には、以下の対処をする必要はないとされている。

[3] 1999 年（平成 11 年）に制定され、その後、個人情報保護法の制定を踏まえて 2006 年（平成 18 年）に改正された。

[4] 1998 年（平成 10 年）創設。

[5] 要求事項 3.4.3.2

[6] 要求事項 3.3.7

「個人情報[7]の漏えい、滅失又は毀損が発生した場合に備え、次の事項を含む対応手順を確立し、かつ、維持しなければならない。

a）当該漏えい、滅失又は毀損が発生した個人情報の内容を本人に速やかに通知し、又は本人が容易に知りうる状態に置くこと。

b）二次被害の防止、類似事案の発生回避などの観点から、可能な限り事実関係、発生原因及び対応策を、遅滞なく公表すること

c）事実関係、発生原因及び対応策を関係機関に直ちに報告すること」

（4）事業者から見たガイドライン・JIS Q 15001 の問題点

事業者としては、主務大臣の定めるガイドライン（以下、単に「ガイドライン」という。）に基づいて、対外的対応を行うことになる。また、プライバシーマーク取得事業者においては、JIS Q 15001 にも対応する。その際、これらの特徴をよく理解する必要がある。

まず、ガイドラインは、文字どおり行政上の指針である。より具体的にいえば「主務大臣が監督権を発動する基準を示す指針」であると言い換えることもできよう。主務大臣の権限行使の基準が不明確であると、個人情報取扱事業者において予測可能性が失われ、その活動が萎縮してしまうため、それを避けるという意味がある。しかも、上記の箇所は「望ましい手法の例示」とされているので、その基準を満たさないからといって、主務大臣の監督権が直ちに発動されるわけではない。ケースバイケースで監督権の発動を控える場合もあるということになる。

このように、ガイドラインは事業者と主務大臣との関係を行政的に規律するに過ぎず、事業者と本人との関係を直接に規律するものではない。本人との関係は、契約または不法行為についての各種法令及び判例によって司法的に規律されるのであって「ガイドラインにさえ抵触しなければ、本人に対して損害賠償責任を負うことはない」ということが常に保障されているものではない。

プライバシーマーク取得事業者における JIS Q 15001 も、付与機関との関係を規律するに過ぎず、本人との関係を直接に規律するものではない点では上記と同様である。

したがって、事業者としては、ガイドラインや JIS Q 15001 に対応するだけではなく、以下に詳述するとおり、本人との関係も考慮して対応していく必要がある。

2　各論

（1）本人への連絡は、ほぼ例外なく直ちに行う

[7] 個人情報保護法と異なり、個人データ以外の個人情報も対象となっている。

まず、本人への連絡はいかなる場合においても最重要であり、例外はほとんどないと考えられる。なお、経済産業分野ガイドラインでは、例外として「本人の権利利益が侵害されておらず、今後も権利利益の侵害の可能性がない又は極めて小さいと考えられる場合には、本人への連絡を省略しても構わないものと考えられる」との見解が示されている[8]。前述のとおり、事業者と本人との関係は、契約または不法行為についての各種法令及び判例によって司法的に規律されるのであって「ガイドラインにさえ抵触しなければ、本人に対して損害賠償責任を負うことはない」ということが常に保障されているものではないが、参考にはなると考えられる。

このような例外に該当するとの判断に基づき、本人への連絡を省略する場合、後日説明を求められる場合に備えて、事業者内部におけるその判断プロセス（恣意的判断や、隠蔽の動機に基づく判断でないこと）を記録に残すべきである。

なお、JIS Q 15001 では、本人への連絡（通知）について「速やかに」行うこととされている。関係機関に対しては「直ちに」報告することとされているのと比較すると「本人への連絡は、関係機関に対する報告より後回しにしてもかまわない」かのようである。

しかし、前述のとおり、JIS Q 15001 は、実際上、プライバシーマーク取得事業者と付与機関との関係を規律するために用いられており、本人との間を直接に規律するものではないことからすると、制度上、本人への連絡について、迅速性の要求水準を少し緩和しているに過ぎず、本人との関係では何ら緩和されていない、つまり、直ちに連絡しなければならないと考えるべきである[9]。

本人への連絡内容は、流出の事実を伝えてこれを謝罪するとともに、二次被害を防止するための対応を要請することである。単に連絡するだけではなく、本人が連絡内容を了解し、それ以上の対応を求めていないのか、あるいは、強く苦情を述べていて解決していないのかについても、記録を残すべきである。これは、第一義的には、本人に対して誠意を持って対応するためであるが、あわせて、公表の要否及びその内容を決めるためにも用いることになる（この点については、後述する）。

（2）主務大臣への報告は、二段階方式で行う

---

[8] 経済産業分野ガイドラインでは、以下のような具体例が挙げられている。
・紛失等した個人データを、第三者に見られることなく、速やかに回収した場合
・高度な暗号化等の秘匿化が施されている場合
・漏えい等をした事業者以外では、特定の個人を識別することができない場合

[9] 経済産業分野ガイドラインでは、このような区別はなされていない。なお、本人への連絡は、連絡先が判然としない等の理由により直ちに行うことができない場合があり得る（例えば、大規模な流出事案においては、通知文書を印刷して郵便で発信するだけで数日以上を要する場合がある）ので、そのようなことを許容する趣旨であると解釈できないこともないが、正当な理由による遅延が許容されるのは関係機関に対する報告においても同様である。

経済産業分野ガイドラインでは、個人データの流出があった場合、経済産業大臣（主務大臣）に報告するほか、所属する業界団体等の関係機関に報告を行うことが望ましいとされている[10]。なお、ファクシミリやメールの誤送信[11]については、主務大臣への報告を月に1回ごとにまとめて実施することができる[12]とされている。

このような例外に該当する場合以外は、主務大臣や関係機関に報告することとなる。報告方法としては、以下のとおり、二段階で行うのが効果的である。

（ａ）第一報告

1回目の報告は、次のような意味を持つ。

・まず、その事案についての担当窓口を知ることである。法律には「主務大臣」と書いてあるが、実際には大臣ではなく、担当窓口が存在する。業務によって、担当窓口が明確である場合もあるが、明確でない場合も少なくない。許認可事業を行っていればその許認可を行う官庁が主務大臣であるが、雇用関係の問題であれば、許認可にかかわらず厚生労働大臣となる。

・二段階方式において1回目の報告は、後に2回目の報告をすることを前提とする「速報」としての意味を持つ。そのことを担当窓口にも明示的に説明しておく。

・したがって、本人への連絡が完了していなくてもかまわない。「本人への連絡に手間取って報告が遅れ、その間にマスコミが知るところとなって、主務大臣から報告の遅延を指摘され、隠蔽の疑いをかけられる」という悪循環を避けることが可能となる。

・本人への連絡も流出原因の調査も完了していないので、公表するかどうかの方針が未確定でもかまわない。「公表するか否かについては、社内にて検討中」と報告することができる。その際に、「どのような問題があれば公表が避けられないか」について主務大臣の考えを聞くことができる。つまり、第二報告までの間に解決すべき問題を知ることができる。

（ｂ）第二報告

2回目の報告は、次のような意味を持つ。

・1回目の報告により、担当窓口がわかっているので、円滑に報告することができる。

・1回目の報告を済ませてあるので、2回目の報告までは少々の時間がかかっても、隠蔽の疑いをかけられることはない。

---

[10] 主務大臣への報告について、経済産業分野ガイドラインでは、個人情報取扱事業者が認定個人情報保護団体の対象事業者であるか否かに分けて規定されているが、本稿では、紙幅の関係で、より一般的であると考えられる「認定個人情報保護団体の対象事業者でない場合」について説明する。

[11] 宛名及び送信者名以外に個人情報が含まれていない場合に限る。

[12] なお、内容物に個人情報が含まれない荷物等の宅配又は郵送を委託したところ、誤配によって宛名に記載された個人データが第三者に開示された場合については、報告する必要はないとされている。

・1 回目の報告後の経過を報告する。本人への連絡は完了し、流出原因の調査も可能な範囲で完了している。

・1 回目の報告の際に聞いた主務大臣の考えから窺い知ることができた公表を避けるための諸条件をクリアした場合には、自社として公表はしないとの判断も含めて報告することができる。不必要な公表を避けることが可能となるだけでなく、公表を避ける判断をしたことを主務大臣に報告すること（その判断に対して主務大臣から異論が述べられていないこと）により、自社の判断に客観性が備わることになり、恣意的判断との批判を避けることが可能となる（判断の正当性が強化される）。

（3）公表

経済産業分野ガイドラインでは、個人データの流出があった場合、「二次被害の防止、類似事案の発生回避等の観点から、個人データの漏えい等の事案が発生した場合は、可能な限り事実関係、再発防止策等を公表することが重要である」とされている一方、「二次被害の防止の観点から公表の必要性がない場合には、事実関係等の公表を省略しても構わないものと考えられる」とされている[13]。公表の必要性がないと認められる具体例は、以下のとおりとされている[14]。

・影響を受ける可能性のある本人すべてに連絡がついた場合

・紛失等した個人データを、第三者に見られることなく、速やかに回収した場合

・高度な暗号化等の秘匿化が施されている場合

・漏えい等をした事業者以外では、特定の個人を識別することができない場合

個人情報の流出事故が発生した場合、事業者としては、二次被害の防止のためにできる限りの措置を講じなければならない。これは、本来的には本人の利益を保護するために行われるものであるが、同時に、その付随的効果として、不必要な公表を避けることにより自社の信用が不必要に毀損することを防止することも可能となる。

そして、公表をしないという判断が、単に事業者内部での判断であった場合には、それが真摯な検討の結果であったとしても、恣意的な判断であるとの批判を受ける可能性が残ってしまうが、上記のとおり、主務大臣への報告の機会を活用することにより、そのような批判を避けることが可能となる。事案の性質にかかわらず、本人が公表を要求してくる場合もあるが、以上の手順で公表しない判断に至ったのであれば、自信を持って拒絶する

[13] なお、公表を省略する場合も、類似事案の発生回避の観点から、同業種間等で、当該事案に関する情報が共有されることが望ましいとされている。

[14] これらの具体例のうち「影響を受ける可能性のある本人すべてに連絡がついた場合」以外は、本人への連絡を省略することが認められる場合の具体例（前述）と同じである。

ことができる。

　このように、本人の利益を保護しつつ、事業者の信用が毀損することを可能な限り避けるという観点から、主務大臣への報告は、避けるのではなく、むしろ積極的に活用すべきである。

以上

著者略歴

1987 年北海道立釧路湖陵高等学校卒業

1993 年一橋大学法学部卒業・東京都庁入庁

1995 年東京都庁退職・司法修習生

1997 年弁護士登録

2002 年上條・鶴巻法律事務所開設

東京弁護士会・民事介入暴力対策特別委員会・副委員長

日本弁護士連合会・民事介入暴力対策委員会・事務局次長

主要取扱分野

事業再生・倒産処理、反社会的勢力との関係遮断対応、

会社法務全般、訴訟・民事保全・民事執行

筆者への問合せ先

〒101-0052

東京都千代田区神田小川町 2-2-8

天下堂ビル 4 階

上條・鶴巻法律事務所

電話：03-5577-8236

FAX：03-5577-8200

email:tsurumaki.aki@ktlaw.jp

掲載日：平成２４年３月２１日