インターネットと匿名性

平成 20 年 3 月

総務省　情報通信政策研究所

はじめに

現在、ブロードバンドの普及や多様なコンテンツが提供されることにより、インターネット利用が人々の生活の中に浸透して利便性が向上している。総務省が打ち出した「u-Japan 政策」が着実に進捗しているといえるが、一方、「u-Japan 政策」の中でも言及されている「影」の課題についての取組も一層重要になってきている。

本研究では、情報通信環境のユビキタス化に伴って注目されている利用者の「匿名性」について、利用者の意識、法的な位置づけ、技術的な可能性等について、それぞれの分野の専門家・有識者の方々が分析を行っている。実際、インターネットの利便性が向上することと、個人に対する様々な識別符号（ＩＤ）の付与を通じて個人の活動と個人の各種属性との紐付け（リンケージ）が可能になっていることは表裏の関係にあり、過度の楽観論も過度の悲観論も廃しつつ、冷静にそのバランスの落ち着きどころについて様々な側面から検討を積み重ねることが、今後のユビキタスネット社会において必要な知恵である。

以上のような問題意識から、利用者の意識調査を行うとともに（第一部）、先に述べたように法的な背景や位置づけを踏まえた現状分析と今後の方向性を論じ（第二部）、匿名性に関連する法的概念を念頭に技術的な対応可能範囲に関する考察を行った（第三部）。

もとより、「匿名性」に対する利用者の意識は固定化されたものではなく、時代とともに、あるいはネット利用の普及・深化とともに変遷するものであろう。本研究の成果が、変遷する時代の方向性を見据え、顕在化する諸課題への対応を検討する際になんらかの参考になれば幸いである。

最後に本プロジェクトの実施にあたっては、岡田仁志国立情報学研究所情報社会相関研究系準教授、新保史生筑波大学大学院図書館情報メディア研究科準教授、高橋郁夫弁護士、町村泰貴北海道大学大学院法学研究科教授、及び株式会社情報通信政策研究所にご協力いただいた。
心よりお礼を申し上げたい。

総務省情報通信政策研究所調査研究部

目次　（括弧内は執筆担当者）

執筆者

＜学識経験者＞（五十音順、敬称略）

岡田仁志　国立情報学研究所情報社会相関研究系准教授
新保史生　筑波大学大学院図書館情報メディア研究科准教授
高橋郁夫　ＩＴ法律事務所所長・弁護士
町村泰貴　北海道大学大学院法学研究科教授

＜総務省＞

新堀修己　前総務省情報通信政策研究所所長
近藤勝則　総務省情報通信政策研究所調査研究部長
堀川　亮　総務省情報通信政策研究所調査研究部研究官

第一部　　匿名性に関するインターネットユーザの意識

１．ネットユーザのプライバシーの価値評価について

１－１　調査の目的

ユビキタスネット社会が進展するにつれ、個人に関するさまざまな情報がネット上を流通することになる。これにより生活の利便性等が向上するが、同時に個人の識別符号（ＩＤ等）と個人の行動や属性がリンクさせることが可能となり、場合によっては情報漏れ等の事故が発生することに対する不安が生じることにもなる。

本調査では、インターネットユーザが各種の個人情報の漏洩に関してどのような評価をしているのか、アンケート調査に基づいて把握する。

１－２　調査概要

上記の目的のため、個人情報の漏洩・公開などに関する問題意識について、下記のとおりアンケート調査を実施した。

■方法：インターネット上の Web アンケート調査

■対象：NTT ナビスペース㈱の調査モニタを対象に調査を実施

■時期：平成 19 年 2 月 22 日(木)～23 日(金)

■有効回答：1,500 人(年齢・性別分布は下記のとおり(*1))

■調査結果　（単位:人）

		15～19歳	20～29歳	30～39歳	40～49歳	50～59歳	60歳以上					
								60～64歳	65歳以上			
										65～69歳	70～79歳	80歳以上
男性	525	48	113	103	102	96	63	33	30	23	7	0
女性	474	46	110	99	95	83	42	26	16	11	4	1

■調査結果(比率)　（単位:%）

		15～19歳	20～29歳	30～39歳	40～49歳	50～59歳	60歳以上					
								60～64歳	65歳以上			
										65～69歳	70～79歳	80歳以上
男性	52.5	4.8	11.3	10.3	10.2	9.6	6.3	3.3	3.0	2.3	0.7	0.0
女性	47.4	4.6	11.0	9.9	9.5	8.3	4.2	2.6	1.6	1.1	0.4	0.1

本調査では、ユーザが守りたいと意識している「匿名性」の構造について分析を試みる。「匿名」という概念によって、秘『匿』されるべき『名』は、単純に「氏名」を意味するだけではなく、「住所」・「電話番号」・「クレジットカード番号」などといったプライバシーないし個人情報を意味しており、インターネットユーザ個々人によって、秘匿したい情報を異にしていると考えられる。

したがって、ここでは、これら個人情報のうち、

①氏名　　②性別

③住所　　④生年月日

(*1)本調査における回答者の性別・年代別分布は、平成17年通信利用動向調査における我が国の15歳以上のインターネットユーザ分布とほぼ一致しており、その観点からは、本調査の回答者は我が国のインターネットユーザを代表しているものと考えることができる。

⑤家族構成　　⑥PC メールアドレス
⑦携帯メールアドレス　　⑧電話番号
⑨クレジットカードﾞ情報

の 9 項目について、インターネットユーザにとってのウェイトの評価(各項目に対する心理的な重みづけの推定)を推計することとした。

１－３　調査結果

以下では、これらの情報のインターネット上での「秘匿性」または「漏洩・(無断)公開」の際の心理的なダメージの大きさについて、漏洩元の主体別に 4 つのケースを想定し、それぞれのケースについて分析をおこなった結果を示す。

【ケース１】個人情報が、個人情報を管理する会社・団体等の組織・事業者等から漏洩したケース

実際の類似事例としては、2004 年に「YAHOO! BB」の加入者など約 450 万人分の個人情報(住所・氏名・電話番号・申し込み時のメールアドレス・Yahoo!メールアドレス・Yahoo! JAPAN ID・申し込み日)が不正に持ち出され、ソフトバンク BB は、YAHOO! BB 全会員に対し、500 円相当の金券を贈り謝罪した。また、これを不服として訴訟を起こした加入者を対象に、同社に対して、慰謝料各 6,000 円の支払いを命じる判決が出されている。

【ケース２】個人情報が、個人情報を管理する官公庁から漏洩したケース

実際の類似事例としては、1998 年に京都府宇治市約 22 万人分の住民基本台帳データ(住民番号・住所・氏名・性別・生年月日・転入日・転出先・世帯主氏名・世帯主との続柄など)がシステム開発業者を通じて漏洩し、訴訟を起こした住民を対象に、同市に対して、慰謝料各 1 万円の支払いを命じる判決が出されている。

【ケース３】個人情報が、個人情報を管理する会社・団体等の組織・事業者によって、無断で公開または提供されたケース

実際の類似事例としては、1998 年に中国の江沢民主席(当時)の講演会が早稲田大学で開催された際、早稲田大学が警視庁に対し、聴講学生約 1,400 人の名簿(氏名・学籍番号・住所・電話番号)を学生に無断で提出したところ、訴訟を起こした学生を対象に、同大学に対して、慰謝料各 5,000～1 万円の支払いを命じる判決が出されている。

【ケース４】医師である会員の個人情報(氏名・職業・診療所の住所・電話番号)が、第三者によって、無断で掲示板に公開されたケース

実際の類似事例としては、1997 年にニフティ(当時)のパソコン通信利用者により掲示板に個人情報が書き込まれたことに対し、書き込んだ者が約 20 万円の慰謝料等の支払いを命じられた判決が出されている。

【ケース１について】

個人情報が、個人情報を管理する会社・団体等の組織・事業者等から漏洩したケースについて、まず、上記の 9 項目のうち、①氏名、②性別、③住所、④生年月日、⑤家族構成、の 5 項目について、コンジョイント分析により、各項目のウェイトを評価した。その結果は図表１－１のとおりである。(*2)

項目名	最大値	最小値	レンジ	重要度
氏名	1.2530	-1.2530	2.5060	35.6%
住所	0.8363	-0.8363	1.6727	23.8%
性別	0.6380	-0.6380	1.2760	18.1%
家族構成	0.4227	-0.4227	0.8453	12.0%
生年月日	0.3667	-0.3667	0.7333	10.4%
		計	7.0333	100.0%

図表１－１　コンジョイント分析(ケース１)（その１）

この場合、各項目のウェイトとしては、

①氏名　35.6%

②性別　18.1%

③住所　23.8%

④生年月日　10.4%

⑤家族構成　12.0%

となり、氏名のウェイトが最も大きく、次いで、住所、性別、と評価されていることがわかる。

また、同様に、上記の 9 項目のうち、①氏名、⑥PC メールアドレス、⑦携帯メールアドレス、⑧電話番号、⑨クレジットカードﾞ情報、の 5 項目について、コンジョイント

(*2)各項目の水準は、それぞれ、「漏洩あり」「漏洩なし」の 2 水準としている。また、決定係数は 0.9983 であり、p 値からも一定の妥当性を備えたモデルと判断することができる。

分析を行い、各項目のウェイトを評価すると図表１－２のようになる。(*3)

項目名	最大値	最小値	レンジ	重要度
氏名	1.3245	-1.3245	2.6490	38.4%
クレジットカード情報	1.0810	-1.5450	2.6260	38.1%
PC メールアドレス	0.4285	-0.4285	0.8570	12.4%
携帯メールアドレス	0.2618	-0.2618	0.5237	7.6%
電話番号	0.1202	-0.1202	0.2403	3.5%
		計	6.8960	100.0%

図表１－２　コンジョイント分析(ケース１)（その２）

この場合、各項目のウェイトとしては、

①氏名　38.4%

⑥PC メールアドレス　12.4%

⑦携帯メールアドレス　7.6%

⑧電話番号　3.5%

⑨クレジットカードﾞ情報　38.1%

となり、氏名とクレジットカード情報のウェイトが同程度に大きく、次いで、PC メールアドレスが重く評価されていることがわかる。

この 2 セットの評価で共通の「氏名」をキーとして、①氏名、②性別、③住所、④生年月日、⑤家族構成、⑥PC メールアドレス、⑦携帯メールアドレス、⑧電話番号、⑨クレジットカードﾞ情報、の 9 項目すべてを対象としたウェイトを算定すると、下記のように推定することができる。

①氏名　22.7%

⑨クレジットカードﾞ情報　22.5%

③住所　15.1%

(*3)各項目の水準は、それぞれ、「漏洩あり」「漏洩なし」の 2 水準としているが、クレジットカード情報についてのみ「クレジットカード番号+有効期限漏洩あり」「クレジットカード番号のみ漏洩あり」「漏洩なし」の 3 水準としている。クレジットカード情報について、アンケート調査結果のコンジョイント分析では、「カード番号のみ漏洩」の場合の部分効用が「カード番号+有効期限の漏洩」の部分効用を上回っているが、これは、Web アンケート調査票の画面イメージから、回答者に「クレジットカード有効期限」が『水準』ではなく、別な『項目』と誤解されてしまったケースが多々あるものと推測されるため、クレジットカード情報についても、「クレジットカード番号のみ漏洩あり」「漏洩なし」の 2 水準とみなして分析を行う。このような混乱もあり、有効な p 値が得られていないが、決定係数は 0.9924 であり、一定の妥当性を備えたモデルと判断することができる。

②性別　11.5%

⑤家族構成　7.6%

⑥PC メールアドレス　7.3%

④生年月日　6.6%

⑦携帯メールアドレス　4.5%

⑧電話番号　2.1%

インターネットユーザによって、最もウェイトが大きく評価されているのは「氏名」であり、匿名性への志向を考える上で参考となる[4]。

次いで大きなウェイトで評価されているのは「クレジットカード情報」である。これは、「クレジットカード情報」が漏洩した場合、その情報を悪用されて、ネットショッピングでの不正利用などの被害が容易に想定できるからと考えられる。

一般的に、いわゆる「基本情報」が大きなウェイトを占めていることが分かるが、例えば、同じ電子メールアドレスであっても、「PC メールアドレス」は「携帯メールアドレス」よりも重要性を評価されている、などの特徴もある。これは、「PC メールアドレス」の場合、ドメイン名の形で、所属する企業や学校などを推測できる情報や、アカウント部分ではユーザの氏名や社員番号・学籍番号などを推測できる情報が含まれるケースがあることや、ユーザ側の立場からはアドレスの変更が必ずしも容易ではないことなどが理由として考えられる。それに比して、「携帯メールアドレス」の場合は、ドメイン名からは携帯キャリア(移動体通信事業者)や九州・四国[5]といったレベルでの地域程度の情報しか含まれておらず、ユーザ側でもアドレスの変更が容易に行えることもあり、相対的に重要視されていないと考えることができる[6]。

また、電話番号については、最近では固定電話を利用していないユーザもあり、また、携帯電話・PHS・IP 電話などの普及に伴い、例えば市内局番から居住地域の推測が可能、などといった電話番号の特徴も失われつつあると同時に、電話番号の変更も容易になってきていることから、重要性が低く評価されているものと考えることができよう[7]。

---

4 情報が漏洩した場合とネット利用上の意識的な行動の場合とを同一に論じることはできないが、秘匿しておきたい情報という心理において共通の要素も考えられる。

5 現在は、携帯電話の新規契約ユーザ(またはメールアドレス変更手続きユーザ)に付与される「携帯メールアドレス」は、どのキャリアでも全国一律のドメインを適用しているが、一部キャリアの旧来からのユーザは、現在でも、契約地域ごとに異なった(サブ)ドメインの「携帯メールアドレス」を利用している。

6 ＰＣと携帯の両方の利用者の場合。

7 ここでの議論は漏洩した場合に対する表明選好であり、例えばスイッチングコストの分析等とは電話番号の意味合いが異なる。

【ケース２】個人情報を管理する官公庁から漏洩したケース

個人情報が、個人情報を管理する官公庁から漏洩したケースについて、まず、上記の9項目のうち、①氏名、②性別、③住所、④生年月日、⑤家族構成、の5項目について、コンジョイント分析により、各項目のウェイトを評価すると図表１－３のようになる。(*8)

項目名	最大値	最小値	レンジ	重要度
氏名	1.2782	-1.2782	2.5563	35.7%
住所	0.8375	-0.8375	1.6750	23.4%
性別	0.6477	-0.6477	1.2953	18.1%
家族構成	0.4433	-0.4433	0.8867	12.4%
生年月日	0.3778	-0.3778	0.7557	10.5%
		計	7.1690	100.0%

図表１－３　コンジョイント分析(ケース２)（その１）

この場合、各項目のウェイトとしては、

①氏名　35.7%

②性別　18.1%

③住所　23.4%

④生年月日　10.5%

⑤家族構成　12.4%

となり、氏名のウェイトが最も大きく、次いで、住所、性別、と評価されていることがわかる。

また、先ほどと同様に、上記の9項目のうち、①氏名、⑥PCメールアドレス、⑦携帯メールアドレス、⑧電話番号、⑨クレジットカード情報、の5項目について、コンジョイント分析により、各項目のウェイトを評価すると図表１－４のようになる。(*9)

項目名	最大値	最小値	レンジ	重要度
氏名	1.3663	-1.3663	2.7327	39.2%
クレジットカード情報	1.0743	-1.5533	2.6277	37.7%

(*8)各項目の水準は、それぞれ、「漏洩あり」「漏洩なし」の2水準としている。また、決定係数は0.9973であり、p値からも一定の妥当性を備えたモデルと判断することができる。

(*9)ケース1と同様にWebアンケート調査票の誤解等のため、有効なp値が得られていないが、決定係数は0.9927であり、一定の妥当性を備えたモデルと判断することができる。

PC メールアドレス	0.4548	-0.4548	0.9097	13.1%
携帯メールアドレス	0.2633	-0.2633	0.5267	7.6%
電話番号	0.0858	-0.0858	0.1717	2.5%
		計	6.9683	100.0%

図表１－４　コンジョイント分析(ケース２)（その２）

この場合、各項目のウェイトとしては、

①氏名　39.2%

⑥PC メールアドレス　13.1%

⑦携帯メールアドレス　7.6%

⑧電話番号　2.5%

⑨クレジットカード情報　37.7%

となり、氏名とクレジットカード情報のウェイトが同程度に大きく、次いで、PC メールアドレスが重く評価されていることがわかる。

この 2 セットの評価で共通の「氏名」をキーとして、①氏名、②性別、③住所、④生年月日、⑤家族構成、⑥PC メールアドレス、⑦携帯メールアドレス、⑧電話番号、⑨クレジットカード情報、の 9 項目すべてを対象としたウェイトを算定すると、下記のように推定することができる。

①氏名　23.0%

⑨クレジットカード情報　22.1%

③住所　15.0%

②性別　11.6%

⑤家族構成　8.0%

⑥PC メールアドレス　7.6%

④生年月日　6.8%

⑦携帯メールアドレス　4.4%

⑧電話番号　1.4%

【ケース３】人情報を管理する会社・団体等の組織・事業者によって、無断で公開または提供されたケース

個人情報が、個人情報を管理する会社・団体等の組織・事業者等から漏洩したケースについて、まず、上記の 9 項目のうち、①氏名、②性別、③住所、④生年月日、⑤家族

構成、の５項目について、コンジョイント分析により、各項目のウェイトを評価すると図表１－５のようになる。(*10)

項目名	最大値	最小値	レンジ	重要度
氏名	1.2815	-1.2815	2.5630	35.4%
住所	0.8455	-0.8455	1.6910	23.4%
性別	0.6673	-0.6673	1.3347	18.4%
家族構成	0.4623	-0.4623	0.9247	12.8%
生年月日	0.3632	-0.3632	0.7263	10.0%
		計	7.2397	100.0%

図表１－５　コンジョイント分析(ケース３)（その１）

この場合、各項目のウェイトとしては、

①氏名　35.4%

②性別　18.4%

③住所　23.4%

④生年月日　10.0%

⑤家族構成　12.8%

となり、氏名のウェイトが最も大きく、次いで、住所、性別、と評価されていることがわかる。

また、同様に、上記の 9 項目のうち、①氏名、⑥PC メールアドレス、⑦携帯メールアドレス、⑧電話番号、⑨クレジットカード情報、の 5 項目について、コンジョイント分析により、各項目のウェイトを評価すると図表１－６のようになる。(*11)

項目名	最大値	最小値	レンジ	重要度
氏名	1.3922	-1.3922	2.7843	39.9%
クレジットカード情報	1.0653	-1.5403	2.6057	37.4%
PC メールアドレス	0.4783	-0.4783	0.9567	13.7%
携帯メールアドレス	0.2482	-0.2482	0.4963	7.1%

(*10)各項目の水準は、それぞれ、「漏洩あり」「漏洩なし」の 2 水準としている。また、決定係数は 0.9952 であり、p 値からも一定の妥当性を備えたモデルと判断することができる。

(*11)ケース 1 と同様に Web アンケート調査票の誤解等のため、有効な p 値が得られていないが、決定係数は 0.9926 であり、一定の妥当性を備えたモデルと判断することができる。

電話番号	0.0660	-0.0660	0.1320	1.9%
		計	6.9750	100.0%

図表１－６　コンジョイント分析(ケース３)（その２）

この場合、各項目のウェイトとしては、

①氏名　39.9%

⑥PC メールアドレス　13.7%

⑦携帯メールアドレス　7.1%

⑧電話番号　1.9%

⑨クレジットカード情報　37.4%

となり、氏名とクレジットカード情報のウェイトが同程度に大きく、次いで、PC メールアドレスが重く評価されていることがわかる。

これまでと同様、この 2 セットの評価で共通の「氏名」をキーとして、①氏名、②性別、③住所、④生年月日、⑤家族構成、⑥PC メールアドレス、⑦携帯メールアドレス、⑧電話番号、⑨クレジットカード情報、の 9 項目すべてを対象としたウェイトを算定すると、下記のように推定することができる。

①氏名　23.1%

⑨クレジットカード情報　21.6%

③住所　15.2%

②性別　12.0%

⑤家族構成　8.3%

⑥PC メールアドレス　7.9%

④生年月日　6.5%

⑦携帯メールアドレス　4.1%

⑧電話番号　1.1%

【ケース４】個人情報が第三者によって、無断で公開されたケース

個人情報が、個人情報を管理する会社・団体等の組織・事業者等から漏洩したケースについて、まず、上記の 9 項目のうち、①氏名、②性別、③住所、④生年月日、⑤家族構成、の 5 項目について、コンジョイント分析により、各項目のウェイトを評価すると図表１－７のようになっている。(*12)

(*12)各項目の水準は、それぞれ、「漏洩あり」「漏洩なし」の 2 水準としている。また、

項目名	最大値	最小値	レンジ	重要度
氏名	1.2647	-1.2647	2.5293	35.1%
住所	0.8340	-0.8340	1.6680	23.2%
性別	0.6927	-0.6927	1.3853	19.2%
家族構成	0.4478	-0.4478	0.8957	12.4%
生年月日	0.3628	-0.3628	0.7257	10.1%
		計	7.2040	100.0%

図表１－７　コンジョイント分析(ケース４)（その１）

この場合、各項目のウェイトとしては、

①氏名　35.1%

②性別　19.2%

③住所　23.2%

④生年月日　10.1%

⑤家族構成　12.4%

となり、氏名のウェイトが最も大きく、次いで、住所、性別、と評価されていることがわかる。

また、同様に、上記の 9 項目のうち、①氏名、⑥PC メールアドレス、⑦携帯メールアドレス、⑧電話番号、⑨クレジットカードﾞ情報、の 5 項目について、コンジョイント分析により、各項目のウェイトを評価すると図表１－８のようになっている。(*13)

項目名	最大値	最小値	レンジ	重要度
氏名	1.4047	-1.4047	2.8093	40.3%
クレジットカード情報	1.0637	-1.5343	2.5980	37.2%
PC メールアドレス	0.4697	-0.4697	0.9393	13.5%
携帯メールアドレス	0.2570	-0.2570	0.5140	7.4%
電話番号	0.0590	-0.0590	0.1180	1.7%
		計	6.9787	100.0%

図表１－８　コンジョイント分析(ケース４)（その２）

決定係数は 0.9961 であり、p 値からも一定の妥当性を備えたモデルと判断することができる。

(*13)ケース 1 と同様に Web アンケート調査票の誤解等のため、有効な p 値が得られていないが、決定係数は 0.9932 であり、一定の妥当性を備えたモデルと判断することができる。

この場合、各項目のウェイトとしては、
①氏名　40.3%
⑥PC メールアドレス　13.5%
⑦携帯メールアドレス　7.4%
⑧電話番号　1.7%
⑨クレジットカードﾞ情報　37.2%
となり、氏名とクレジットカード情報のウェイトが同程度に大きく、次いで、PC メールアドレスが重く評価されていることがわかる。

この 2 セットの評価で共通の「氏名」をキーとして、①氏名、②性別、③住所、④生年月日、⑤家族構成、⑥PC メールアドレス、⑦携帯メールアドレス、⑧電話番号、⑨クレジットカードﾞ情報、の 9 項目すべてを対象としたウェイトを算定すると、下記のように推定することができる。
①氏名　23.1%
⑨クレジットカードﾞ情報　21.3%
③住所　15.2%
②性別　12.6%
⑤家族構成　8.2%
⑥PC メールアドレス　7.7%
④生年月日　6.6%
⑦携帯メールアドレス　4.2%
⑧電話番号　1.0%

１－４　まとめ

以上４つのいずれのケースにおいても、①氏名、②性別、③住所、④生年月日、⑤家族構成、⑥PC メールアドレス、⑦携帯メールアドレス、⑧電話番号、⑨クレジットカードﾞ情報、の 9 項目のウェイトの順位およびおおよその重みが下記のように同程度であることが分かった。
①氏名　約 23%（22.7～23.1%）
⑨クレジットカードﾞ情報　約 22%（21.3～22.5%）
③住所　約 15%（15.0～15.2%）

②性別　約 12%（11.5～12.6%）
⑤家族構成　約 8%（7.6～8.3%）
⑥PC メールアドレス　7%強（7.3%～7.9%）
④生年月日　7%弱（6.5～6.8%）
⑦携帯メールアドレス　4%強（4.1～4.5%）
⑧電話番号　1～2%（1.0～2.1%）

これらのことから、インターネット上のサービスを利用する際にユーザが守りたいと意識している「匿名性」を構成する要素としては、
■住所・氏名など、相当程度に個人を特定できる情報
■クレジットカード情報など直接的に経済的被害を引き起こす可能性の高い情報
が特に重要視されていることがわかる。

ただし、本分析においては、9 項目それぞれについて、項目単独でのウェイトを評価しており、項目相互の複合関係などは一切考慮していない。

例えば、「住所」と「家族構成」の情報がセットで漏洩した場合の影響は、単にこれらの情報項目のウェイトを合計したものよりも甚大なものとなる可能性が高いと考えられ、逆に、「氏名」という情報には、「性別」を相当程度類推することができる要素が包含されていたり、「PC メールアドレス」という情報に「氏名」に相当する要素が包含されていることも多々ある。

このような項目相互の複合関係などを考慮したうえで、項目の真の評価を推し量る作業は将来的な課題である。

２．ネットユーザの匿名行動と顕名行動の選択

２－１　調査の目的

本調査では個人情報が意図に反して漏洩する際のユーザの意識や評価ではなく、ブログやソーシャル・ネットワーク・ソサエティ（ＳＮＳ）等自ら表現行為を行う場合に、典型的な個人識別情報である氏名を表示することに関する意識を調査した。この調査により、利用するメディアの選択と氏名等の個人情報を表示するかの相互の関係を踏まえたメディアの特長を把握する。

２－２　調査の概要

インターネット等の利用者の匿名性・顕名性の選択行動を把握するため、下記のとおり、アンケート調査を実施した。

■方法：インターネット上の Web アンケート調査

■対象：NTT ナビスペース㈱の調査モニタのうち、１．「ネットユーザのプライバシーの価値評価」のアンケート調査に回答したモニタを対象に調査を実施

■時期：平成 19 年 2 月 28 日(水)～3 月 1 日(木)

■有効回答：1,000 人(年齢・性別分布は下記のとおり (*14))

■調査にあたっては、下記の３つのケースについて、ユーザが匿名で利用するか件名で利用するかについて、想定される利用目的を分類した上で分析を行った。

【I】　インターネット上の掲示板の利用

【II】 インターネット上のブログ・SNS サイトの利用

【III】インターネット上での動画(映像)の閲覧・視聴

■調査結果　　(単位:人)

		15～19歳	20～29歳	30～39歳	40～49歳	50～59歳	60歳以上					
								60～64歳	65歳以上			
										65～69歳	70～79歳	80歳以上
男性	525	48	113	103	102	96	63	33	30	23	7	0
女性	474	46	110	99	95	83	42	26	16	11	4	1

■調査結果(比率)　　(単位:%)

		15～19歳	20～29歳	30～39歳	40～49歳	50～59歳	60歳以上					
								60～64歳	65歳以上			
										65～69歳	70～79歳	80歳以上
男性	52.5	4.8	11.3	10.3	10.2	9.6	6.3	3.3	3.0	2.3	0.7	0.0
女性	47.4	4.6	11.0	9.9	9.5	8.3	4.2	2.6	1.6	1.1	0.4	0.1

【ケース１】インターネット上の掲示板の利用

インターネット上の掲示板に投稿(書き込み)を行おうとする場合の選択行動に関し、利用形態を下記の 4 通りの方法(*15)に分類した上でインターネットユーザの意識を分析した。

a. 実名での投稿(書き込み)

b. 固定的なハンドルネームでの投稿(書き込み)

c. 実質的に匿名での投稿(書き込み)

d. 投稿しない(書き込まない)

(*14)本調査における回答者の性別・年代別分布は、平成 17 年通信利用動向調査における我が国の 15 歳以上のインターネットユーザ分布とほぼ一致しており、その観点からは、本調査の回答者は我が国のインターネットユーザを代表しているものと考えることができる。

(*15)選択行動の顕名性・匿名性の高さとしては、(顕名性) a.＞b.＞c.＞d. (匿名性) の順序を形成していると考えている。(「d.投稿しない(書き込まない)」は、厳密には選択行動とは呼べないが、最も顕名性の水準が低い行動(回避行動)とみなして、順序の一部を形成する行動と考える。)

このとき、インターネット上の掲示板に投稿(書き込み)を行おうとする場合の、ユーザの選択行動の選好は、「投稿しない(書き込まない)」と投稿(書き込み)そのものを回避するユーザが多く(57.3%)、「実名での投稿(書き込み)」は1.4%に過ぎなかった。

このユーザの意識の構造について、AHP（Analytic Hierarchy Process）の手法により、より詳細な分析を試みた。その際、インターネット上の掲示板に投稿(書き込み)を行う目的（積極面及び消極面）を分類して、下記の3つの要素を想定する。

①ユーザが持っている情報を発信・提供できることによる満足感

②同じ趣味を持つユーザとの交流の広がり

③心ないユーザからの誹謗中傷等によるリスク

ユーザは、①や②といった効用を得たいがためにインターネット上の掲示板に投稿(書き込み)を行おうとする訳であるが、半面、投稿(書き込み)を行うことによって③のような事象が生じるリスクも勘案しなくてはならない。

①、②、③の、それぞれ、どの評価基準を、どの程度、重視して行動するかは、ユーザの意識によってまちまちであると考えられる。

そして、こういったそれぞれの意識に基づく、評価基準の下で、インターネットユーザは上記a.、b.、c.、d.の４代替案を評価し、最も合理的と考えられる行動を選択していると考えることができる。

このため、本調査では、まず上記の3評価基準について個々のユーザがそれぞれどの程度重要視しているのかを調査した。具体的には個々の評価基準を他の評価基準と個別に付き合わせて評価を問う一対比較の方法を利用し、次いで、それぞれの評価基準の観点から分析して総合的な評価を浮き彫りにすることとしている。

ここで、インターネット上の掲示板に投稿(書き込み)を行う場合の要因(評価基準)について、その重要性(ウェイト)を算出すると、図表２―１のようになっている。(*16)

掲示板	重要度
満足感	0.223129
交流	0.23019
リスク	0.546682
C.I.	0.000718

(*16)C.I.=0.12以下のデータによって分析している。“C.I.”はConsistency Indexの略で、「整合度指数」「一貫性指数」などと呼ばれ、評価の合理性を示す指数であり、小さいほど整合性が高いと評価される。概ね0.1～0.15以下であれば、一般的に十分に合理的と解釈される。

図表２－１　投稿（書き込み）を行う場合の要因(掲示板の利用)

ユーザの意識の中では、「心ないユーザからの誹謗中傷等によるリスク」が最重要視され、「ユーザが持っている情報を発信・提供できることによる満足感」や「同じ趣味を持つユーザとの交流の広がり」といった要因(評価基準)を大きく上回っている。

次いで、3 要因(評価基準)それぞれにおける 4 代替案の評価についてみてみる。

「ユーザが持っている情報を発信・提供できることによる満足感」、「同じ趣味を持つユーザとの交流の広がり」、「心ないユーザからの誹謗中傷等によるリスク」それぞれの観点からの 4 代替案の評価は、図表２－２、図表２－３、図表２－４に示すとおりである。

満足感	重要度
実名	0.131383
コテハン	0.334665
名無し	0.256344
投稿せず	0.277607
C.I.	0.000391

図表２－２　代替案の評価(掲示板の利用)（満足感）

交流	重要度
実名	0.1651
コテハン	0.359291
名無し	0.245449
投稿せず	0.23016
C.I.	0.00091

図表２－３　代替案の評価(掲示板の利用)（交流の広がり）

リスク	重要度
実名	0.149719
コテハン	0.277227
名無し	0.243642
投稿せず	0.329412
C.I.	0.00028

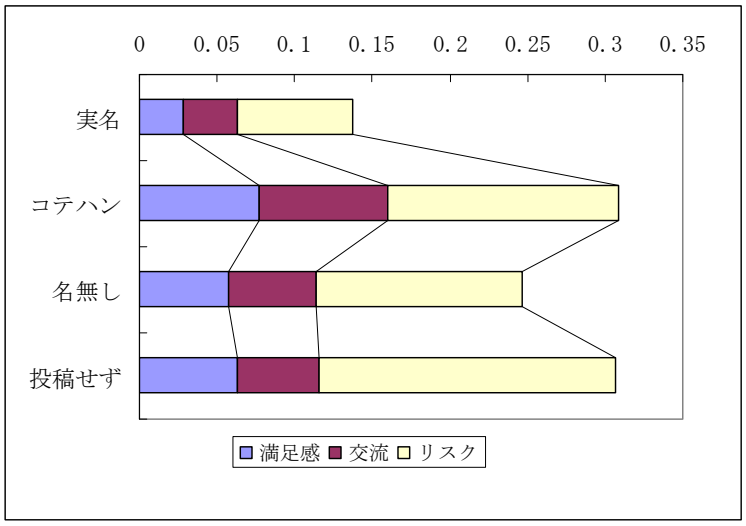
図表２－４　代替案の評価(掲示板の利用)（リスク）

「ユーザが持っている情報を発信・提供できることによる満足感」および「同じ趣味を持つユーザとの交流の広がり」の要因(評価基準)の観点からは、「固定的なハンドル

ネームでの投稿(書き込み)」が、「心ないユーザからの誹謗中傷等によるリスク」の要因(評価基準)の観点からは、「投稿しない(書き込まない)」が、それぞれ最も合理的と考えられ、そういった行動をインターネットユーザは選択していると考えることができる。

これらを総合的に評価すると、図表２－５のようになっており、「固定的なハンドルネームでの投稿(書き込み)」および「投稿しない(書き込まない)」の２代替案が、ともに約 31%のウェイトで評価されている。

インターネット上の掲示板に投稿(書き込み)を行う場合、ユーザは、利便・便益の得失を判断し、固定的なハンドルネームで投稿する、あるいは投稿しない、といった行動を選択することが多いと考えることができる。



図表２－５　代替案の評価(掲示板の利用)（総合的な評価）

【ケース２】インターネット上の CGM(ブログ・SNS サイト)の利用

インターネット上の CGM(ブログ・SNS サイト)を公開しようとする場合の利用形態は、下記の３通りの方法(*17)に分類した。

a. 実名での公開

b. ハンドルネームでの公開

(*17)選択行動の顕名性・匿名性の高さとしては、(顕名性) a.＞b.＞c.(匿名性) の順序を形成していると考えている。(「c.公開しない」は、厳密には選択行動とは呼べないが、最も顕名性の水準が低い行動(回避行動)とみなして、順序の一部を形成する行動と考える。)

c.公開しない

このとき、インターネット上の CGM(ブログ・SNS サイト)を公開しようとする場合のユーザの選択行動の選好は、「ハンドルネームでの公開」を選択する者が最も多く(52.5%)、「実名での公開」は僅か 2.5%に過ぎなかった。

このユーザの意識の構造について AHP 手法を用いて分析するため、下記の 3 基準を想定した。

①ユーザが持っている情報を発信・提供できることによる満足感

②同じ趣味を持つユーザとの交流の広がり

③心ないユーザからの誹謗中傷等によるリスク

先ほどと同様、CGM(ブログ、SNS サイト)に投稿(書き込み)を行う場合の要因(評価基準)について、その重要性(ウェイト)を算出すると、図表２－６のようになった。(*18)

CGM	重要度
満足感	0.23157
交流	0.263015
リスク	0.505415
C.I.	0.000248

図表２－６　投稿（書き込み）を行う場合の要因(CGM(ブログ・SNS サイト)利用(公開))

ユーザの意識の中では、インターネット上の掲示板の利用と同様に、「心ないユーザからの誹謗中傷等によるリスク」が最重要視され、「ユーザが持っている情報を発信・提供できることによる満足感」や「同じ趣味を持つユーザとの交流の広がり」といった要因(評価基準)を大きく上回っている。

次いで、3 要因(評価基準)それぞれにおける 3 代替案の評価について把握する。

「ユーザが持っている情報を発信・提供できることによる満足感」、「同じ趣味を持つユーザとの交流の広がり」、「心ないユーザからの誹謗中傷等によるリスク」それぞれの観点からの 4 代替案の評価は、図表２－７・図表２－８・図表２－９に示すとおりである。

満足感	重要度
実名	0.175292

(*18)C.I.=0.12 以下のデータによって分析している

ハンドル	0.49021
公開せず	0.334498
C.I.	0.000719

図表２－７　代替案の評価(CGM(ブログ・SNS サイト)利用(公開))（満足感）

交流	重要度
実名	0.199304
ハンドル	0.488441
公開せず	0.312254
C.I.	0.001144

図表２－８　代替案の評価(CGM(ブログ・SNS サイト)利用(公開))（交流の広がり）

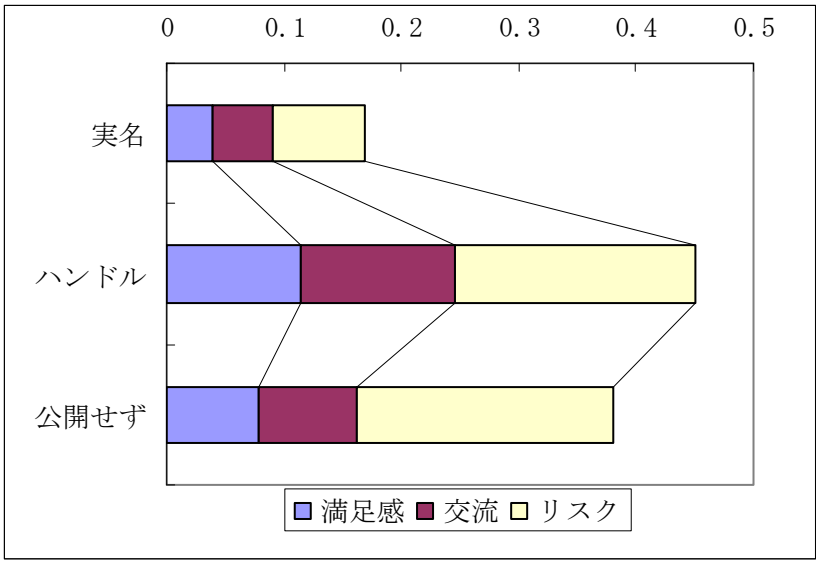
リスク	重要度
実名	0.1615852
ハンドル	0.4051446
公開せず	0.4332701
C.I.	-1.6E-05

図表２－９　代替案の評価(CGM(ブログ・SNS サイト)利用(公開))（リスク）

「ユーザが持っている情報を発信・提供できることによる満足感」および「同じ趣味を持つユーザとの交流の広がり」の要因(評価基準)の観点からは、「ハンドルネームでの公開」が、「心ないユーザからの誹謗中傷等によるリスク」の要因(評価基準)の観点からは、「公開しない」が、それぞれ最も合理的と考えられ、このような行動を選択していると考えることができる。

これらを総合的に評価すると、図表２－１０のようになっており、「ハンドルネームでの公開」が、約 45%のウェイトで最も高く評価されている。

インターネット上の CGM(ブログ・SNS サイト)を公開しようとする場合、ネット利用の目的や便益を踏まえれば、ユーザにとってハンドルネームで公開するという行動が合理的であると考えることができる。



図表２－１０　代替案の評価(CGM(ブログ・SNS サイト)利用(公開))（総合的な評価）

【ケース３】インターネット上での動画(映像)の閲覧・視聴

インターネット上の動画(映像)を閲覧・視聴しようとする場合の選択行動について、下記の 4 通りの方法(*19)について、インターネットユーザの意識を把握した。

a. 氏名・住所など、個人を特定できる情報を伴う会員登録をして閲覧・視聴

b. 氏名・住所など、個人を特定できる情報を必要としない会員登録で可能な範囲で閲覧・視聴

c. 会員登録なしで可能な範囲で閲覧・視聴

d. 閲覧・視聴をしない

このとき、インターネット上の動画(映像)を閲覧・視聴しようとする場合の、ユーザの選択行動の選好を見てみると、「個人情報を伴う会員登録での閲覧・視聴」が 11.8%、「個人情報を伴わない会員登録での閲覧・視聴」が 25.9%、となっており、両者で 4 割弱を占めている。

このユーザの意識の構造について、これまでと同様 AHP 手法を用いて分析した。

①豊富なコンテンツ

(*19)選択行動の顕名性・匿名性の高さとしては、（顕名性）a.＞b.＞c.＞d.（匿名性）の順序を形成していると考えている。(「d.閲覧・視聴をしない」は、厳密には選択行動とは呼べないが、最も顕名性の水準が低い行動(回避行動)とみなして、順序の一部を形成する行動と考える。)

②ユーザに適切なコンテンツのレコメンド(おすすめ)・新着情報の提供
③コンテンツ閲覧・視聴履歴を把握されるリスク

ユーザは、①や②といった効用を得たいがために、会員登録をしてインターネット上の動画(映像)を閲覧・視聴しようとする訳であるが、半面、コンテンツ事業者等に対して何らかの情報を提供することを伴う会員登録を経て、動画(映像)コンテンツの閲覧・視聴を行うことによって③のような事象が生じるリスクも勘案しなくてはならない。

①、②、③のどの評価基準を、どの程度、重視して行動するか、は、ユーザの意識によってまちまちであると考えられる。

ここでも先ほどと同様に、インターネット上の動画(映像)を閲覧・視聴しようとする場合の要因(評価基準)について、その重要性(ウェイト)を算出すると、図表２－１１のようになる。(*20)

動画	重要度
コンテンツ	0.308485
レコメンド	0.244863
リスク	0.446652
C.I.	0.001456

図表２－１１　動画(映像)の閲覧を行う場合の要因

ユーザの意識の中では、インターネット上の掲示板の利用・インターネット上のCGM(ブログ･SNS サイト)の利用のケースよりはリスク懸念ウェイトが小さいものの､｢コンテンツ閲覧・視聴履歴を把握されるリスク」が最重要視され、「豊富なコンテンツ」や「ユーザに適切なコンテンツのレコメンド(おすすめ)・新着情報の提供」といった要因(評価基準)を大きく上回っている。

次いで、3 要因(評価基準)それぞれにおける 4 代替案の評価について把握する。

「豊富なコンテンツ」、「ユーザに適切なコンテンツのレコメンド(おすすめ)・新着情報の提供」、「コンテンツ閲覧・視聴履歴を把握されるリスク」それぞれの観点からの 4 代替案の評価は、図表２－１２、図表２－１３、図表２－１４に示すとおりである。

(*20)C.I.=0.12 以下のデータによって分析している。

コンテンツ	重要度
特定伴う	0.191541
特定必要なし	0.300586
登録必要なし	0.276082
閲覧視聴せず	0.23179
C.I.	0.000188

図表２－１２　代替案の評価(動画(映像)の閲覧)（コンテンツ）

レコメンド	重要度
特定伴う	0.202259
特定必要なし	0.308911
登録必要なし	0.256544
閲覧視聴せず	0.232286
C.I.	0.000313

図表２－１３　代替案の評価(動画(映像)の閲覧)（情報提供）

リスク	重要度
特定伴う	0.174853
特定必要なし	0.293268
登録必要なし	0.262478
閲覧視聴せず	0.269401
C.I.	0.000103

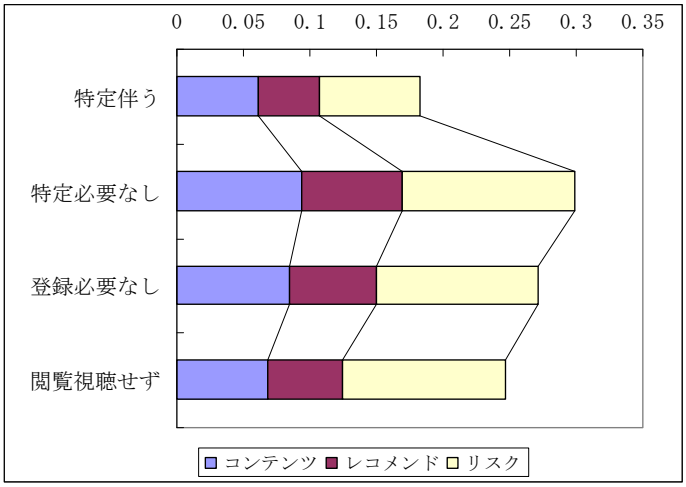
図表２－１４　代替案の評価(動画(映像)の閲覧)（リスク）

「豊富なコンテンツ」、「ユーザに適切なコンテンツのレコメンド(おすすめ)・新着情報の提供」、「コンテンツ閲覧・視聴履歴を把握されるリスク」いずれの要因(評価基準)の観点からも、「氏名・住所など、個人を特定できる情報を必要としない会員登録で可能な範囲で閲覧・視聴」が最も高い評価を得ている。

他の代替策と比べ、抜きん出て高い評価とは言えないが、インターネット上の動画(映像)を閲覧・視聴しようとする場合、こうした判断がユーザにとって最も合理的と考えることができる。

これらを総合的に評価すると、図表２－１５のようになり、「氏名・住所など、個人を特定できる情報を必要としない会員登録で可能な範囲で閲覧・視聴」が約 30%のウェイトで評価され、最も高いウェイトを占めている。

ただし、「会員登録なしで可能な範囲で閲覧・視聴」も約 27%の評価ウェイトを占めており、利用するコンテンツの魅力によって対応が変わるのかもしれない。



図表２－１５　代替案の評価(動画(映像)の閲覧)（総合的な評価）

２－３　まとめ

以上の結果をみると、インターネットユーザは総合的に得られる便益とさらされるリスクを踏まえて利用形態を選択していることがわかる。

例えば、掲示板への書き込みの場合にはリスクへの対応を含め書き込み自体に否定的な層が３割強は存在しているのに対し、動画の視聴においては利用自体を否定する割合は相対的に低くなっているが、これは掲示板の場合、書き込みをしなくても ROM という利用形態で一定の便益を得ることが可能であることも反映していると考えられる[21]。

また、個人の特定を伴う形で動画を視聴する割合と実名で掲示板に書き込む割合と比較すると、前者のほうが高いが、その理由としては受益の反対給付として必要となる匿名性のレベルに関する選択肢の有無[22]や自分に関する情報が不特定多数にさらされる蓋然性の高さなどが影響していると考えられる[23]。

実際には、本研究で取り上げたインターネット上の各サービス内においても多様な利用形態があり[24]、それぞれの匿名性の確保状況を同列に論じることの限界もあるが、一般的にはインターネットユーザは利用場面に応じて匿名性確保のレベルと得られる便益との得失を考慮した上で合理的な行動を取っている。

[21] 視聴の場合には、利用しなければなんら得られる便益がないが、掲示板の場合書き込みをしなくても一定の便益が得られるとすれば、書き込みをしないという選択肢を取る可能性が高まる。
[22] 動画視聴の場合には登録しなければ視聴できないという二者択一の選択肢であるが、掲示板への書き込みの場合には、実名以外での書き込みという選択肢がある場合が多い。
[23] 動画視聴の場合には、基本的には動画を提供する会社等の内部でのみ登録情報が利用され、不特定多数に公開されるわけではない。
[24] 実名でないと参加できないＳＮＳサービスもあれば動画視聴の場合に求められる登録情報も多様である。

第二部　匿名とプライバシー
第二部第一章　プライバシー的な権利の生成
１　問題の所在

匿名による情報発信、取引の利用、視聴閲覧など、匿名による情報発信や取引活動は、犯罪に従事する者がそれに乗じて違法行為に従事したり、匿名化が他人の権利利益侵害の発生要因の根源のように捉えられることもある。つまり、特定の個人を識別可能な情報を用いない「匿名」や、当該個人の識別を可能にする事実を公にしない「プライバシーの保護」が、犯罪者や他人の権利を侵害する者の隠れ蓑として用いられているというイメージがある。

反面､顕名によらなければ社会生活上必要な様々なサービスを利用できない場面も多く、事業者によるサービスの利用と本人の個人情報の提供がトレードオフの関係にあることも多い。とりわけ、個々の消費者に対応したきめ細かなサービスの提供には詳細な個人情報が必要となるが、取得された情報は単なる個人情報としての利用にとどまらず、それらの情報からは個人の私生活上の様々な事実が明らかになることも多いため、単にサービスの提供を受けるために個人情報を提供したにもかかわらず、個人のプライバシーでさえも明らかになってしまう現状がある。

例えば、金融分野では、オークション代金の受取口座として、出品者が開設している預金口座への振込確認を行わなくても代金の支払状況の確認ができ、代金が確実に出品者の口座に振り込まれる仕組みとして、「ワンタイム口座」なども用いられるようになっている。しかし、当該口座の利用も特定個人を識別した上での利用が前提であり、金融サービスの利用については匿名による取引は大部分において制限されているのが現状である。また、金融取引における不正行為を防止する観点からも、取引に関わる関係者間における完全な匿名化は適当ではないといえよう。問題は、本人が情報を開示する範囲を選択できないことであり、本人が意図せず自らに関する情報を提供し利用されている点にある。

そこで、本章では、個人情報の適正な取扱いや個人のプライバシー保護への要請がある一方で、本人が希望しない個人情報の提供やプライバシーに関する事実の開示が事実上強制される場面が多いことに鑑み、プライバシーの権利とは何かについて、その権利性や保障根拠を省察した上で、「匿名情報」と個人情報保護法の定める「個人情報」の関係について検討する。

２　個人情報保護とプライバシー保護の違い

匿名とプライバシーの問題を考えるにあたっては、取扱いの対象となる情報が「個人情報」なのか、取扱いの方法によっては「プライバシー」に該当する情報にあたるのか厳密に考える必要がある。なぜなら、「プライバシー」と「個人情報」の両者については、「プライバシー」＝「個人情報」という図式で論じられることが多いからである。しかし、両

者は必ずしも同義とはいえない。

プライバシーという概念は、以下の三つの保護法益からなると考えられる(1)。

(1) 自らに関する事柄について、外部からの干渉を受けずに自らの意思に基づいて行うことを認める「個人の自律」の保障。

(2)他人から干渉を受けたり望まない侵入を受けない隔絶された状態や利益を保護するための「私的な領域」の保護。

(3) 社会において自らの存在を証明し、他人との識別を行う上で、個人を識別する徴表としての「個人情報」の保護。

では、以上の各保護法益がすべて「プライバシー」として保護されるのかというとそうではない。例えば、公知の「個人情報」はプライバシー保護の対象とはならず、「領域」についても公の場は保護対象とはならないなど、プライバシーとして保護されるためには一定の要件を満たす場合に限られる。（以下の図を参照）

判例においても、プライバシーの権利は「私生活をみだりに公開されないという法的保障ないし権利」と定義され、その範囲も後述の「宴のあと」事件(2)において示されたプライバシー侵害による不法行為の成立要件にあてはめて個々の事例において検討がなされている。

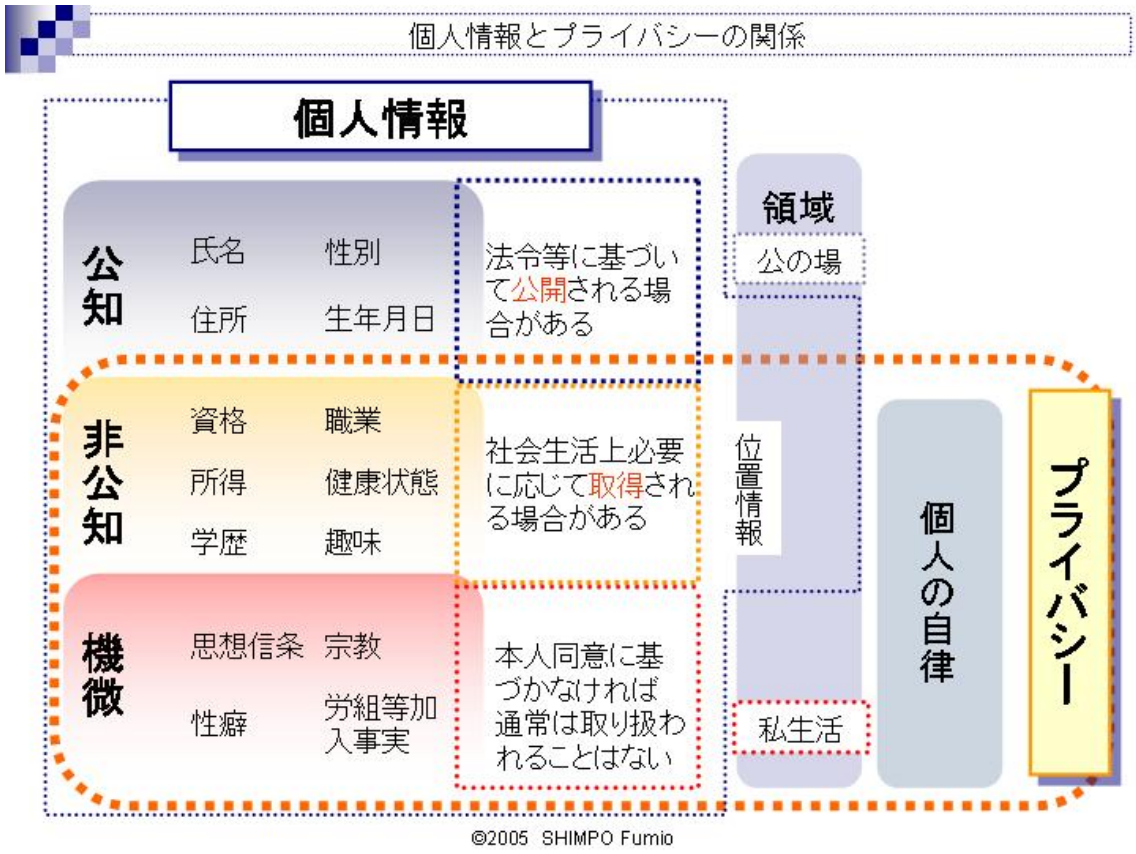
さらに、プライバシーとは、個人の私生活と密接に関わる事柄であることや、プライバシーの範囲もその人の価値観に大きく左右されるものであるため、個人の趣味嗜好や感受性が千差万別であるのと同じように､その内容も非常に多面的な性質を有するものである。

また、社会的にも、人口の密集度が高い都市や、情報の量や伝達速度が飛躍的に向上した社会においては、人間相互の関係が複雑化し、他人との関わりを持たない私生活の領域が狭まる傾向がある。さらに、社会の情報化が進んだ現在、ネットワークを介して従来にも増して広範囲において多様な人間関係を築くことができるようになっていることから、個人のプライバシーの範囲は個々の場面において大きく異なるものであるといえよう。

---

(1)　プライバシーの権利については、拙著. プライバシーの権利の生成と展開 . 成文堂. ２０００.を参照されたい。

(2)　「『宴のあと』事件」判決（東京地判昭和３９年９月２８日判時３８５号１２頁）。



【図①：個人情報とプライバシーの関係】

拙稿「図書館と個人情報保護法」情報管理 Vol.47 No.12. 2005 年 3 月号. 2005, 818 頁.

２－１　プライバシーの権利とは

プライバシーの権利とは、文明社会の発展とともにその必要性が唱えられるようになった権利である。また、憲法が保障する他の基本的人権と比べると、その権利性が認められるようになったのが比較的最近であることや、憲法に明文で規定されている権利ではないことから、その根拠や権利概念など、プライバシーの権利保障をめぐる法理は未だ発展段階にある。

その一方で、インターネットの普及に伴うネットワーク社会の発展により、個人のプライバシー保護の必要性も新たな展開を見せ始めており、様々なプライバシーの侵害事例に対し、いかに個人のプライバシーの権利を保障することができるのかが問われている。

プライバシーの権利は、現在では憲法上の権利として認識されている。しかし、当初から憲法上の権利として観念されていたわけではない。最も初期の段階においては、手紙などの財産権的な利益を保護する形で、間接的にプライバシーの権利が保障されていた。つまり、この段階では、私信の内容がプライバシーとして保護されていたわけではなく、あ

くまで、手紙という個人の所有物に対する財産権を保護することにより、結果的に手紙の内容が保護されていたにすぎない。

具体的に、個人のプライバシーが権利として主張されるようになったのは、マスメディアの発達との関係においてである。扇情主義的な手法で読者の獲得を目指したイエロージャーナリズムによって個人のプライバシーが侵害されたことを受けてのことである。しかし、この段階においても、未だ私人によるプライバシー侵害の問題として、その権利性も不法行為法上の権利としてプライバシー侵害に対する救済を行うためのものであって、権利概念も、「ひとりで居させてもらう権利」という消極的なものであった。

その後、自らに関する私的な事柄を、政府による干渉を受けずに決定する自由として、自由権的な権利としてプライバシーの権利が認識されるようになり、憲法の保障類型に含まれる権利として認識されるようになった。

さらに、社会の情報化に伴い行政事務の効率化が図られるようになり、政府が大量の個人情報を保有するようになるにつれ、政府による個人情報の取得、管理や利用に対し、情報主体である本人の権利の保障が求められるようになる。とりわけ、政府が保有する情報の取扱いの透明性を確保し、個人情報の適正な取扱いが重要な課題となるにつれ、本人の権利として情報の開示、訂正や利用停止といった請求権的権利を保障することが重要になったことをから、「ひとりで居させてもらう」という自由権的な側面に加え請求権的な要素を加味した権利へと変遷を遂げてきた。このような請求権的な権利としてのプライバシーの権利は、「自己情報コントロール権」と定義されるに至っている。

このように、プライバシーの権利は憲法上保障される権利として認識されるに至ったものの、憲法が明文で保障しているわけではない。そのため、憲法上の根拠としては、憲法第１３条後段の幸福追求権に基づいて保障されると解するのが通説である。なお、同条は、憲法の個別の条文によって規定されていない権利を、包括的に保障する包括的基本権条項と呼ばれることもある。

２－２　プライバシーの権利の権利性

プライバシーの権利が、憲法が保障する基本的人権の一つであるならば、その権利内容を明確にした権利概念があってしかるべきであろう。しかし、未だに権利性に曖昧な部分が多いことから、憲法上の根拠や権利性についても諸説が存在しており、同じく権利概念についても様々な学説が展開されている。

わが国におけるプライバシーの権利概念は、前述の通り「自己についての情報をコントロールする権利(3)」という定義が通説となっており、これは一般に、「自己情報コントロール権説」と呼ばれている。

---

(3)　佐藤幸治「プライヴァシーの権利（その公法的側面）の憲法論的考察」法学論叢８６巻５号１２頁。

同説によると、プライバシーの権利とは、「単に他人が自己について情報をもたないという状態」をいうのではなく、「他人が自己についてのどの情報をもちどの情報をもちえないかをコントロールすることができる」権利として、現在の情報化社会におけるプライバシーの権利の保障を主眼においた権利概念として提唱されているものである。

その他にも、「自己イメージのコントロール権説」や「構造的権利説」といった学説が提唱されている。

「自己イメージのコントロール権説(4)」は、プライバシーを「単に個人データ開示の自由の問題ととらえる」のではなくして、「多元的な社会関係形成の自由の一側面」として把握し、「シンボリックな相互作用」の社会学的な条件を探ることが、プライバシー概念の機能を知るために必要であるという前提に立った上で、「人間が自由に形成しうるところの社会関係の多様性に応じて、多様な自己イメージを使い分ける自由をプライヴァシーと呼ぶ」と定義することによって、プライバシーの権利の定義付けを試みようとする説である。

「構造的権利説(5)」は、プライバシーの権利を自由権的・請求権的側面を兼ね備える複合的な権利として把握した上で、それに含まれる諸価値を体現する「構造的権利」としてプライバシーの権利を観念しようとする学説である。

この説では、「プライバシー」と「プライバシー利益」について、それぞれ、前者については、「他者による評価の対象となることのない生活状況または人間関係が確保されている状態」と定義し、一方、後者については、「こうした状態に対する正当な要求または主張をいう」という区別を行っている。

そして、「プライヴァシー権は、プライヴァシー状態を公権力によって侵害されないとの要求・主張を当然に含むのであるから、自由権的性格をもつ」とする一方、「公権力は、最大の個人情報システムの保有者」であり、「責任政治の観点からして、個人情報の取扱いについて法的に最も規制されてよい保有者である」ことから、これを法的に規制するためには「結果不法から考えていたのではたりない」として、自由権的性格のみならず、請求権的性格をも有する複合的権利であるとする。

さらに、複合的権利としてのプライバシーの権利は、①道具（手段）的価値、②尊厳保障価値、③参加価値、その他、組織上の価値といった、様々な価値を有する権利であり、それらの価値をも含む権利として把握するならば、プライバシーの権利は、「自由権的であると同時に請求権的でもあり、また実体的権利であると同時に手続的権利でもある」と考えられ、それらの総体及び前記諸価値を体現するプライバシーの権利を、「構造的権利」と呼ぶのが適当であるとしている。

このように、プライバシーの権利概念をめぐっては、諸説が展開されてはいるものの、憲法学説上は、自己情報コントロール権説が支配的となっている。

---

(4)　棟居快行『人権論の新構成』信山社（１９９２）１８７－１９５頁。

(5)　阪本昌成「プライヴァシー権　－憲法の基本問題」法学教室４１号７頁。

２－３　判例理論の展開

我が国において、プライバシーの権利性が判例において初めて認められたのは、１９６４年の「『宴のあと』事件」判決（東京地判昭和３９年９月２８日判時３８５号１２頁）においてである。

本件は、三島由紀夫の小説『宴のあと』が、プライバシーを侵害したとして、元外務大臣で１９５９年には東京都知事選に立候補した原告が、三島由紀夫と出版元の新潮社に対して民事訴訟を提起したというものである。

判決では、プライバシーの権利を、「私生活をみだりに公開されないという法的保障ないし権利」として承認し、プライバシー侵害による不法行為の成立要件として、①公開された内容が私生活の事実またはそれらしく受けとられるおそれのある事柄であること、②一般人の感受性を基準にして当該私人の立場に立った場合公開を欲しないであろうと認められること、③　一般の人々に未だ知られない事柄であることを要すると判示した。

また、「『宴のあと』事件」に見られるように、その後もモデル小説とプライバシーの問題をめぐって様々な問題が提起されている。

「『名もなき道を』事件」判決（東京地判平成７年５月１９日判時１５５０号４９頁）では、小説中に実在人物のプライバシーに属する事実が記述されていても、その事実が当該小説の主題及びこれを支える構成上不可欠であり、かつ、表現の方法・内容において秘事のあからさまな暴露とならないような慎重な配慮がされており、小説全体としても作者の芸術的想像力の生み出した創作であって虚構（フィクション）と認められるときには、プライバシー侵害としての違法性を欠くとして、プライバシーの権利を侵害したとする請求を棄却した。

その他、被告が執筆した小説の発行が、原告の名誉を毀損し、プライバシー及び名誉感情を侵害するものであるとされた事例として、小説「『石に泳ぐ魚』事件」判決（東京地判平成１１年６月２２日判例時報１６９１号９１頁）がある。

２－４　憲法上の権利としての展開

我が国において、プライバシーの権利が憲法上の権利として初めて承認されたと考えられているのは、昭和４４年の「京都府学連事件」判決（最大判昭和４４年１２月２４日判時５７７号１８頁）においてである。

本件は、捜査手段としての写真撮影と肖像権の関係について明確な基準を示した事例であり、憲法第１３条によって憲法上明文で規定されていない権利が保障されることを示し、同条に具体的な裁判規範性があることを初めて承認した判例である。

そのため、本件は、肖像権を承認したところに憲法的意義が認められると評価されているが、プライバシーの権利と同様の保護法益が憲法第１３条によって保障されることが示

され、実質的に憲法上のプライバシーの権利について承認したものと考えられている。

判決では、「憲法第１３条は国民の私生活上の自由が、警察権等の国家権力の行使に対しても保護されるべきことを規定しているものということができる。そして、個人の私生活上の自由の一つとして、何人も、その承諾なしに、みだりにその容ぼう・姿態（以下「容ぼう等」という。）を撮影されない自由を有するものというべきである。これを肖像権と称するかどうかは別として、少なくとも、警察官が正当な理由もないのに、個人の容ぼう等を撮影することは、憲法第１３条の趣旨に反し、許されないものといわなければならない。」と述べ、「私生活上の自由」として「承諾なしに、みだりにその容ぼう・姿態を撮影されない自由」が憲法第１３条を根拠に認められるとした。

さらに、肖像権としてではなく、プライバシー侵害として最高裁が正面から論じた事件として、「京都市前科照会事件」判決（最判昭和５６年４月１４日民集３５巻３号６２０頁）がある。

本件は、ある者の前科及び犯罪経歴の照会が、プライバシー侵害にあたるか否かが問題となった事件である。

判決では、「前科及び犯罪経歴（以下「前科等」という。）は人の名誉、信用に直接にかかわる事項であり、前科等のある者もこれをみだりに公開されないという法律上の保護に値する利益を有するのであって、市区町村長が、本来選挙資格の調査のために作成保管する犯罪人名簿に記載されている前科等をみだりに漏えいしてはならないことはいうまでもないところである」と判示した。

その他、犯罪経歴については、プライバシー侵害として不法行為に基づく損害賠償を請求した「ノンフィクション『逆転』事件判決」（最判平成６年２月８日民集４８巻２号１４９頁。）がある。

判決では、前科等にかかわる事実をみだりに公表されないことが法的保護に値する利益にあたるとした上で、「その者が有罪判決を受けた後あるいは服役を終えた後においては、一市民として社会に復帰することが期待されるのであるから、その者は、前科等にかかわる事実の公表によって、新しく形成している社会生活の平穏を害されその更生を妨げられない利益を有するというべきである。」として、ある者の前科等にかかわる事実について著作物で実名を使用して公表した行為がプライバシーの侵害にあたるとされた。

これらの最高裁判決では、いずれの判決においても「プライバシー」という用語は用いられていないものの、実質的には、憲法第１３条を根拠にプライバシーの権利が保障されることを認めたものと解されている。

なお、これらの事例において問題となった犯罪経歴は、一般に他人に公開されることを望まない事実であり、前記諸判例の示すとおり、みだりに公表してはならない個人情報の一つであることはいうまでもない。

しかし、これらの個人情報は、公開の刑事裁判において有罪判決が確定し、判決文にも本人の実名が記録されて公開されることから、判決の時点においては、たとえ本人が公開を望まない情報にあたると主張したとしても、犯罪事実に対する社会の正当な「関心事」

として公開は正当化される。

そのため、刑事被告人の実名や容ぼう等を公開する報道は、公共の利害に関するものとして違法性はないとされており、その理由は、犯罪行為や容疑を一般公衆に覚知させて、社会的見地からの警告、予防、抑制的効果を果たさせることにあるとされている。

よって、これらの事実を公開することが公共の利害に関するものとして許容されるとしても、公開することが許容される事実の範囲は、犯罪事実及びこれと密接に関連する事実に限られる。

３　個人情報保護法と匿名情報の取扱い

３－１　個人情報保護制度

我が国の個人情報保護制度は、国の行政機関については、１９８８年に、「行政機関の保有する電子計算機処理に係る個人情報の保護に関する法律」が制定されている。

国の行政機関を対象とした個人情報保護法が制定された背景には、１９８０年にＯＥＣＤが、「プライバシー保護と個人データの国際流通についてのガイドラインに関する理事会勧告」を採択したことが大きく影響している。

ＯＥＣＤのガイドラインでは、ＯＥＣＤ加盟国に対しては、①ガイドラインにおいて示された原則を国内法において考慮すること、②プライバシー保護の名目で個人データの国際的流通を不当に阻害しないこと、③ガイドラインの履行について協力することを要求した。

そして、加盟国がガイドラインを国内において適用する際の基本原則として、①収集制限の原則、②データ内容の原則、③目的明確化の原則、④利用制限の原則、⑤安全保護の原則、⑥公開の原則、⑦個人参加の原則、⑧責任の原則、の八つの原則を掲げた。これは、一般に、ＯＥＣＤ八原則と呼ばれ、個人情報保護を目的とした法律やガイドラインなどの制定にあたっては、個人情報保護の基本原理として重要な役割を果たしてきた。

一方、民間部門については、行政機関を対象にした個人情報保護法の適用を受けないことから、法的な保護については、法令が定める職業上の秘密保持義務規定などをはじめとして、各法令の規定が結果的に個人情報の保護に寄与する形での間接的な規制が行われてきたが、その後、個人情報保護報が制定されて現在に至っている。

以上から、我が国の個人情報保護制度を整理すると、①基本方針（閣議決定された個人情報保護に関する基本方針）、②基本法及び民間部門を対象とした法令（個人情報の保護に関する法律及び政令等）、③行政機関及び独立行政法人等の公的部門を対象とした法令（行政機関等個人情報保護法及び政令等）、④個別法令における個人情報保護を目的とした規定に基づく個人情報の保護（派遣業法、職安法等の既存法令）、⑤地方自治体の個人情報保護条例、⑥法令の定める職業上の秘密保持義務規定（公務員法、各種の士業法等）、⑦個人情報の漏えいや不正利用等の行為に対する法的責任を追及する上で用いられる法令

（不正競争防止法等）、⑧保護法第８条に基づく各府省ガイドライン、⑨その他の法令に基づく規格やガイドライン（工業標準化法、プロバイダ責任制限法、電子署名法等に基づくガイドライン）、⑩行政機関が行政機関等を対象に策定したガイドライン（安全管理や情報通信技術の利用）、⑪民間団体が民間部門を対象に策定したガイドライン（業界ガイドライン等）から構成されている。

３－２　匿名情報と個人識別性の関係

個人情報保護法は、「個人情報」の適正な取扱いに必要な手続きを定めることによって、個人情報の有用性に配慮しつつ保護することを目的としている。したがって、「個人情報」に該当しない情報は、本法の規制対象とはならないため、匿名情報であって特定の個人を識別できない情報は個人情報保護法にいう「個人情報」には該当しない。しかし、匿名情報であっても、「特定個人を識別できる情報が記述されていなくても、周知の情報を補って認識することにより特定の個人を識別できる情報[6]」になりうる情報がある。ここにいう周知の情報を補って個人情報になりうる情報とは、経済産業分野ガイドラインのＱ＆Ａでは、「例えば、『現在の経済産業大臣』とだけあって、氏名がない情報でも、周知の情報を補えば、特定の個人が識別できますので、個人情報に該当します。[7]」という例が示されている。

また、ニックネームやＩＤなど、一見すると匿名情報に該当する情報であっても、個人情報になりうる場合がある。これについても、ガイドラインのＱ＆Ａでは、「個人情報に該当する場合があります。オンラインゲームにおける「ニックネーム」及び「ＩＤ」が公開されていても、通常は特定の個人を識別することはできませんから、個人情報には該当しません。ただし、「ニックネーム」又は「ＩＤ」を自ら保有する他の情報と容易に照合することにより特定の個人を識別できる可能性があり、そうした場合は個人情報に該当し得ます。なお、例外的にニックネームやＩＤから特定の個人が識別できる場合（有名なニックネーム等）には、個人情報に該当します。[8]」との解説がなされている。

このように、個人情報保護法では、「個人情報」を第２条第１項において「この法律において『個人情報』とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。」と定義しているが、匿名情報として用いられている情報であっても個人情報に該当する場合があるなど、保護法の適用を受ける個人情報に該当するか否かについては、当該規定の定める要件を個別に判断した上で、取扱いの対象となる情報が個人情

6 経済産業省「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１９年３月）
7 経済産業分野ガイドラインＱ＆Ａ(2005.1.14/7.28 修正)
8 同上。

報に該当するか否か判断を要するため、以下、その要件を個別に検討する。

３－３　生存性の要件

個人情報の定義について、一つめの要件は「生存」する「個人」に関する情報であるという要件である。

「生存」とは、死者の情報は含まないことを意味する。ただし、死者に関する情報が、同時に、遺族等の生存する個人に関する情報でもある場合には、当該生存する個人に関する情報となる。これは、名誉やプライバシーなどといった人格権同様に、個人情報についても一身専属性であるという考えに基づいている。

「個人」とは、自然人のことを指し法人は含まない。また、日本国民に限られず、外国人も含まれることから、外国人の情報も対象となる。反面、法人その他の団体は「個人」に該当しないため、法人等の団体に関する情報は個人情報には含まれない。

３－４　個人識別性の要件

「個人識別性」とは、その情報から特定の個人を識別することができるもの、または他の情報と容易に照合することにより、特定の個人を識別することができるものをいう。これには、氏名、性別、生年月日等個人を識別する情報に限られず、個人の身体、財産、社会的地位・身分等の属性に関して、事実、判断、評価を表す全ての情報が該当し、評価情報、公刊物等によって公にされているものや、映像、音声も含まれる。その「情報」だけでは特定の個人を識別できない場合でも、他の情報と容易に照合することによって識別できる場合は個人情報にあたる。

なお、個人識別性の要件については、行政機関個人情報保護法及び独立行政法人等個人情報保護法も、保護法とほぼ同様の定義を置いているが、個人識別性に関する文言が「他の情報と照合することができ」となっており、保護法が「容易に」という文言を置くことによって容易照合性を要件としているのとは異なる。

３－５　匿名情報の取扱い

匿名情報は、個人情報に該当する情報を「匿名化」することと、個人情報を取得せずにそもそも「匿名」の情報を取り扱うことは異なる。

例えば、医療分野においては、個人の身体に関する非常に機微な情報を取り扱うことから､それらの情報の取扱いにあたって従来から匿名化の方法も含めて議論がなされてきた。

医療分野のうち医学研究の分野における取扱いにあたっては、保護法の制定前から研究指針が定められているが、これらの指針を改正し、ヒトゲノム・遺伝子解析「研究」に関わるすべての関係者が遵守すべき事項を定めたガイドラインとして、「ヒトゲノム・遺伝

子解析研究に関する倫理指針（平成 16 年 12 月 28 日文部科学省・厚生労働省・経済産業省告示第１号）」及び「遺伝子治療臨床研究に関する指針（平成 16 年 12 月 28 日文部科学省・厚生労働省告示第２号）」が告示されている。

また、個人遺伝情報は、医学研究を目的として利用されるだけでなく、個人の遺伝情報を用いた事業も行われるようになってきている。個人遺伝情報に係る検査、解析及び鑑定等を行う事業がこれに該当し、塩基配列・一塩基多型、体質検査等の遺伝子検査、ＤＮＡ鑑定及び親子鑑定等のサービス、遺伝子受託解析等があげられる。そこで、研究分野ではなく事業分野における個人遺伝情報の取扱いについては、経済産業省が所管する分野のうち、個人遺伝情報を用いた「事業」分野を対象としたガイドラインとして、「経済産業分野のうち個人遺伝情報を用いた事業分野における個人情報保護ガイドライン（平成 16 年 12 月 17 日経済産業省告示第４３５号）」が告示されている。

ガイドラインでは、ＤＮＡの個人情報該当性について、それぞれ、倫理指針と個人遺伝情報ガイドラインにおいて次のように定められている。

倫理指針の「３ 保護すべき個人情報」の「（１）「個人情報」とは」においては、「個人情報を連結不可能匿名化した情報は、個人情報に該当しない。個人情報を連結可能匿名化した情報は、研究を行う機関において、当該個人情報に係る個人と当該情報とを連結し得るよう新たに付された符号又は番号等の対応表を保有していない場合は、個人情報に該当しない。」とされている。

個人遺伝情報ガイドラインの「１．定義（法第２条関連）」の「１－１．情報の性質に関連する用語」においては、「（６）『匿名化』」に関する定めにおいて、匿名化とは、「ある人の個人情報が法令、本ガイドライン又は事業計画に反して外部に漏洩しないように、その個人情報から個人を識別する情報の全部又は一部を取り除き、代わりにその人と関わりのない符号又は番号を付すことをいう。」とした上で、「試料等に付随する情報のうち、ある情報だけでは特定の人を識別できない情報であっても、各種の名簿等の他で入手できる情報と組み合わせることにより、その人を識別できる場合には、組合せに必要な情報の全部又は一部を取り除いて、その人が識別できないようにすることをいう。」とし、これに基づき、「（１）『個人情報』（法第２条第１項関連）」において、「連結可能匿名化された情報は、符号又は番号と個人情報との対応表を保有している当該法人内にあるときは、解析等実施者が所有する匿名化情報と対応表を連結させることで、法人全体として、匿名化されている情報についても個人を識別できるものと整理され、『個人情報』に該当する。」としている。

なお、ガイドラインでは、匿名化の方法には、必要な場合に個人を識別できるように、その人と新たに付された符号又は番号の対応表を残す方法による匿名化(連結可能匿名化)と、個人を識別できないように連結可能匿名化のような対応表を残さない方法による匿名化（連結不可能匿名化）の二つの方法があることが示されている。

第二部第二章　匿名による視聴・閲覧の自由

１．はじめに

メディアコンテンツの閲覧履歴（放送の視聴履歴、インターネットの閲覧履歴等）は、それにより個人の生活形態や嗜好、ひいては思想・信条等を第三者により把握できる可能性があり、極めてプライバシー性の高い情報であるとされている。こうした閲覧履歴情報は、ユビキタスネット社会の進展によるデジタル放送の高度化やブロードバンドサービスの普及等により、第三者によって容易に取得されることが技術的には可能となりつつある。こうした現状を捉え、ユビキタスネット社会における「匿名で視聴する自由」に関する論点を整理する。

なお、本章は全て執筆者の個人的見解であり、日本政府及び所属組織を代表するものではないことを申し添える。

２．従来の匿名による視聴・閲覧

今日のような高度な情報通信技術が到来する以前の時代においても、情報メディアの視聴・閲覧の匿名性に関する議論が無かったわけではない。ここでは、日本図書館協会による「図書館の自由に関する宣言」や、米国におけるいわゆる「ケーブル通信政策法」及びいわゆる「ビデオプライバシー保護法」を紹介し、視聴・閲覧シーンにおける従来の匿名性の扱われ方について触れる。

２－１　日本図書館協会「図書館の自由に関する宣言」

図書館における資料の請求、閲覧、貸出し等に関する情報も、他の情報メディアの利用履歴と同様に、個人の嗜好・思想・信条等を色濃く反映することがあり、これらの情報は極めてプライバシー性が高いと言える。

こうした情報が第三者によって把握されることを防ぐため、公共図書館、大学・学校図書館、専門図書館等で構成される社団法人日本図書館協会では、「図書館の自由に関する宣言」を採択し、下記のような規定を設けている。

日本図書館協会「図書館の自由に関する宣言」（１９５４年採択、７９年改訂）（抄）

図書館は、基本的人権のひとつとして知る自由をもつ国民に、資料と施設を提供することをもっとも重要な任務とする。

1. 日本国憲法は主権が国民に存するとの原理にもとづいており、この国民主権の原理を維持し発展させるためには、国民ひとりひとりが思想・意見を自由に発表し交換すること、すなわち表現の自由の保障が不可欠である

知る自由は、表現の送り手に対して保障されるべき自由と表裏一体をなすものであり、知る自由の保障があってこそ表現の自由は成立する。

知る自由は、また、思想・良心の自由をはじめとして、いっさいの基本的人権と密接にかかわり、それらの保障を実現するための基礎的な要件である。それは、憲法が示すように、国民の不断の努力によって保持されなければならない。

2. すべての国民は、いつでもその必要とする資料を入手し利用する権利を有する。この権利を社会的に保障することは、すなわち知る自由を保障することである。図書館は、まさにこのことに責任を負う機関である。

（略）

この任務を果たすため、図書館は次のことを確認し実践する。

（略）

第３　図書館は利用者の秘密を守る

1. 読者が何を読むかはその人のプライバシーに属することであり、図書館は、利用者の読書事実を外部に漏らさない。ただし、憲法第３５条にもとづく令状を確認した場合は例外とする。
2. 図書館は、読書記録以外の図書館の利用事実に関しても、利用者のプライバシーを侵さない。
3. 利用者の読書事実、利用事実は、図書館が業務上知り得た秘密であって、図書館活動に従事するすべての人びとは、この秘密を守らなければならない。

（以下略）

（１９７９．５．３０　総会決議）

（出典：社団法人日本図書館協会ウェブサイト　http://www.jla.or.jp/ziyuu.htm　※傍線筆者）

上記宣言では、図書館利用者に対する「知る権利の保障」の一環として、利用者の秘密の保護を謳っている。また、読書内容が個人のプライバシーに属する事項であることを明記した上で、読書記録のみならずそれ以外の利用事実も含め、全ての図書館活動従事者に対し、秘密の保持を義務づけている。

また、上記宣言を受け、日本図書館協会では図書館員の倫理綱領を総会決議により定めている。

日本図書館協会「図書館員の倫理綱領」（１９８０年総会決議）（抄）

この倫理綱領は、「図書館の自由に関する宣言」によって示された図書館の社会的責任を自覚し、自らの職責を遂行していくための図書館員としての自律的規範である。

（略）

3. この綱領は、われわれの図書館員としての自覚の上に成立する。したがってその自覚以外にはいかなる拘束力もない。しかしながら、これを公表することによって、われわれの共通の目的と努力、さらにひとつの職業集団としての判断と行動とを社会に誓約することになる。その結果、われわれはまず図書館に大きな期待を持つ人びとから、ついで社会全体からのきびしい批判に自らをさらすことになる。

（略）

（利用者に対する責任）

第３　図書館員は利用者の秘密を漏らさない。

図書館員は、国民の読書の自由を保障するために、資料や施設の提供を通じて知りえた利用者の個人名や資料名等をさまざまな圧力や干渉に屈して明かしたり、または不注意に漏らすなど、利用者のプライバシーを侵す行為をしてはならない。このことは、図書館活動に従事するすべての人びとに課せられた責務である。

（出典：社団法人日本図書館協会ウェブサイト　http://www.jla.or.jp/rinri.htm　※傍線筆者）

上記綱領では、読書の自由の保障のため、図書館活動従事者が利用者の個人名・資料名等の開示や漏洩を禁じている。前文３にあるとおり、この綱領はあくまで社団法人の決議文書であって法令ではないため、罰則や強制力を伴うものではないが、図書館従事者が職務を遂行する上での自主的な基準として制定されているものである。

以上の宣言及び綱領から分かるように、情報通信技術が高度に進展する以前の時代から、

匿名による情報の享受の在り方については、我が国においても重要な論点として取り扱われてきたと言える。

２－２　米国ケーブル通信政策法・ビデオプライバシー保護法

我が国のみならず、諸外国においても、匿名での視聴・閲覧については、かねてから議論の俎上に乗せられてきた。具体例として、米国におけるいわゆる「ケーブル通信政策法」（Cable Communications Policy Act of 1984）を素材として紹介する。

上記法を受けて制定された米国 1996 年通信法（Communications Act of 1996）では、第 631 条（47 U.S.C. 551）において、下記のように規定されている。

米国 1996 年通信法（抄）（仮訳）
第 631 条　加入者プライバシーの保護
(a)(1)ケーブル事業者は、加入者にケーブル・サービスその他のサービスを提供するための契約を締結する際及びその後少なくとも年１回、当該加入者に対して、次の事項を明瞭かつ顕著に知らせる個別の文書の形式によって通知しなければならない。
(A)当該加入者に関して収集され又は収集されるべき、個人を識別できる情報の性質及び当該情報の使用方法の性質
(B)当該情報について行われ得る開示を受けることのある者の種類の特定を含むその開示の性質、頻度及び目的
(C)当該情報をケーブル事業者が保持する期間
(D)加入者が(d)項の規定に従って当該情報を閲覧できる時間及び場所
(E)ケーブル事業者による情報の収集と開示について本条の規定によって課されている制限、並びにこの制限を守らせるための(f)項及び(h)項の規定に基づく加入者の権利
（略）
(2)(h)項以外の本条の適用上は、次の定義に従う。
(A)「個人を識別できる情報」の語辞は、特定の個人を識別できない集計データの記録を含まない。
(B)～(C)　（略）
(b)(1)ケーブル事業者は、(2)に規定する場合を除き、関連する加入者から事前に文書又は電子的手段による同意を受けないで,個人を識別できる情報を収集するためにケーブル・システムを使用してはならない。
(2)ケーブル事業者は,下記の目的をもって個人を識別できる情報を収集するためにケーブル・システムを使用することができる。
(A)ケーブル事業者が提供するケーブル･サービスその他のサービスを加入者に提供するのに必要な情報を得るため
(B)ケーブル･コミュニケーションの無断視聴を発見するため
(C)(1)ケーブル事業者は、(2)に規定する場合を除き、関連する加入者から事前に文書又は電子的手段による同意を受けないで、個人を識別できる情報を開示してはならず、かつ､加入者又はケーブル事業者以外の者による当該情報への無断アクセスを防止するのに必要な措置を講じなければならない。
(2)ケーブル事業者は、その開示が下記のいずれかに該当する場合は、個人を識別できる情報を開示することができる。
(A)当該ケーブル事業者が加入者に提供するケーブル･サービスその他のサービスを提供するため、又はこれらのサービスに関連する正当な事業活動を行うために必要な場合。
(B)(h)項の規定に従うことを条件として、開示を認める裁判所命令に基づき、当該命

令を受けた者がその命令を加入者に通知した上で、開示する場合。
(C)次のいずれにも該当する場合において、ケーブル･サービスその他のサービスの加入者の氏名及び住所を開示する場合。
(i) その開示を禁止し又は制限する機会をケーブル事業者が当該加入者に与える場合。
(ii) その開示が、直接にも間接にも次のいずれかの事実をも明らかにするものでない場合。
(I) 当該ケーブル事業者が提供するケーブル・サービスその他のサービスの当該加入者による視聴その他の利用の程度
(Ⅱ) 当該ケーブル事業者のケーブル・システムを通じての当該加入者による交信の性質
(d)ケーブル加入者は、ケーブル事業者が収集し、保有する個人を識別できる情報のうち、その加入者に関するものすべてを閲覧することができる。この情報は、当該ケーブル事業者が指定した妥当な時間に便宜な場所において加入者が閲覧できる。ケーブル加入者は、当該情報のいかなる誤りをも訂正するための妥当な機会が与えられねばならない。
(e) 個人を識別できる情報が、もはやこれを収集した目的上必要ではなくなり、かつ、その情報について(d)項の規定又は裁判所命令による閲覧について未処理の要請又は命令が存在しない場合は、ケーブル事業者は、当該情報を破棄しなければならない。
(f)(1)ケーブル事業者による本条違反の行為によって被害を受けた者は、合衆国地方裁判所に民事訴訟を提起することができる。
(以下略)
(仮訳は郵政省郵政研究所編『米国電気通信法対訳』(1997)による　※傍線筆者)

上記の規定では、加入者情報取得の際に、情報の性質、目的、保持期間等を告知する義務をケーブル事業者に課している。情報の収集には原則として本人の同意が必要とし、例外的にサービス提供・不正監視等に必要な場合のみ、本人の同意無き情報の収集を認めている。また、加入者本人の開示請求権を認めるとともに、同意なき第三者への開示を禁止している。(ただし、サービス提供に必要な場合や裁判所の命令による場合には、例外的に同意なき開示が認められる。)また、必要なくなった場合の破棄も事業者に要求している。言うまでもなく、こうした個人情報には、視聴者の視聴履歴情報も含まれると考えられる。

この規定は、1984年ケーブル通信政策法から継承されたものであり、ケーブルテレビの加入者の視聴履歴情報の収集や第三者の開示について、法律による一定のルールを課すものであると言える。

なお米国では、ビデオレンタルの際にも、1988年ビデオプライバシー保護法(Video Privacy Protection Act of 1988)の規定により、本人の同意や裁判所の令状なしにレンタル履歴等の個人情報を第三者に開示することが禁じられており、無断で開示された利用者は損害賠償請求権を有する。

３．放送における視聴履歴

ここでは、我が国での主要な情報通信メディアの一つである放送について、視聴履歴の保護の在り方について述べる。

３－１　放送メディアの動向と視聴履歴

我が国における放送メディアは、戦後、国民生活における情報メディアの主要な部分を担うに至った。ＮＨＫ放送文化研究所が平成１８年６月に実施した「全国個人視聴率調査」によると、週平均・国民一人当たりの放送視聴時間は４時間１７分に上っており、国民生活に多大な影響を与えていると言える。

特に、地上テレビジョン放送については、上記放送視聴時間のうち約７５％（３時間３１分）を占めており、国民生活に密接に関わる基幹メディアであると言える。また、過去１０年間の同様の調査でもこの数値にほとんど変動が無く、インターネットや携帯電話等、国民が触れるメディアが急速に多様化しているとされている今日でも、国民生活の基幹メディアとしての地位を現状のところいまだ保っていると言って差し支えない。

2003 年 12 月には東名阪の三大都市圏で地上デジタルテレビジョン放送が開始され、2011 年の予定されるアナログ停波までに、各家庭の地上テレビジョン放送受信機がデジタル受信機へ切り替えられることとなる。デジタル受信機は、いわゆるＣＡＳ技術（Conditional Access System）によってコントロールされており、受信機の視聴履歴は、現状では定常的に収集されているわけではないが、技術的には収集が可能となっている。

先に述べたように、放送が国民にとって最も身近なメディアの一つであるがゆえに、放送番組の視聴動向は、その世帯・個人の生活形態や嗜好、価値観等を色濃く反映する可能性があり、その点において、放送番組の視聴履歴は極めてプライバシー性の高い情報であると言える。

３－２　放送視聴履歴の保護の現状

我が国では、放送メディアにおける個人情報保護については、「放送受信者等の個人情報の保護に関する指針」（平成 16 年 8 月 31 日総務省告示第 696 号）が制定されており、放送事業者等が個人情報を取り扱う際の義務等が規定されている。

この指針の中では、番組視聴履歴を含む放送関連の個人情報の取り扱いについて、同意なき第三者提供の制限等、個人情報保護法の一般原則に沿った各種規律を設ける一方、特に放送番組の視聴履歴に関する保護について、下記のような規定が設けられている。

「放送受信者等の個人情報の保護に関する指針」（平成 16 年 8 月 31 日総務省告示第 696 号）（抄）

（定義）

第二条　この指針において使用する用語は、法において使用する用語の例によるほか、次の定義に従うものとする。

（略）

四　「視聴履歴」とは、放送受信者等の個人情報であって、放送番組の視聴の開始の日時及び終了の日時並びに当該放送番組を特定することができるものをいう。ただし、当該開始の日時の一ごとに本人の同意を得ないで取得することができるものに限る。

（取得の範囲の制限）

第六条　（略）

２　受信者情報取扱事業者は、放送の受信、放送番組の視聴若しくは放送番組の視聴に伴い行われる情報の電磁的方式による発信若しくは受信に関し料金若しくは代金の支払いを求める目的又は統計の作成の目的のために必要な範囲を超えて、視聴履歴を取得しないよう努めなければならない。
３　（略）
（視聴履歴等の管理）
第十四条　受信者情報取扱事業者は、視聴履歴（個人データであるものに限る。次項及び第十九条第二項において同じ。）又は口座番号等（個人データであるものに限る。次項及び第十九条第二項において同じ。）の記録された物を郵便又は信書便（民間事業者による信書の送達に関する法律（平成十四年法律第九十九号）第二条第二項に規定する信書便をいう。）によって発送する場合には、当該物を封入する方法その他の当該物が送達されるまでの間当該視聴履歴又は口座番号等を見ることができないようにする方法により行うよう努めなければならない。
２　受信者情報取扱事業者は、視聴履歴又は口座番号等を電気通信回線設備（送信の場所と受信の場所との間を接続する伝送路設備及びこれと一体として設置される交換設備並びにこれらの附属設備をいう。以下この項及び第十七条の二において同じ。）を用いて発信しようとする場合には、暗号を用いた方法その他の通信の当事者以外の者がその内容を復元できないようにする方法により行うよう努めなければならない。ただし、当該発信の場所と当該視聴履歴又は当該口座番号等の着信の場所との間を接続するすべての電気通信回線設備が特定の者に専用されるものであるときは、この限りでない。
（個人データの保存期間及び消去）
第十九条　受信者情報取扱事業者は、放送受信者等の個人データの保存期間を定めるよう努めなければならない。
２　受信者情報取扱事業者は、視聴履歴又は口座番号等の保存期間を定める場合には、当該保存期間がそれぞれ第六条第二項又は第三項に規定する目的のために必要な最短の期間とするよう努めなければならない。
３　（略）
４　受信者情報取扱事業者は、第一項の規定により定めた保存期間が満了したときは、当該保存期間に係る個人データを消去するよう努めなければならない。

上記各規定においては、放送の視聴履歴が高度なプライバシー性を持ちうる個人情報であることを鑑み、視聴履歴に特化した規律を課している。

まず、第 2 条において、視聴履歴の定義として、個々人の具体的な視聴対象を特定できるものとするだけでなく、本人の同意なしに自動的に取得可能なものという要件が加わっており、保護の対象とする視聴履歴情報を限定している。このような限定がなされているのは、デジタル放送受信機の技術の進展とともに、個々人の詳細な視聴履歴を自動的に収集することが技術的には可能となっており、プライバシー性の高い情報がむやみに収集されるおそれがあることから、この特段の保護が要請される一方で、デジタル放送技術を活用した諸サービス、例えば番組連動型データ放送によるショッピング利用や番組キャンペーンへの応募等、視聴者の自発的な意思により放送事業者に電話回線・インターネット等を通じて放送事業者のサーバにアクセスして必要な個人情報を提供している場合を除くことで、当該サービスの運営に必要以上の規制による負担をかけないためであるとされている。（出典：総務省による指針解説）

第 6 条においては、視聴履歴の取得範囲について、受信料、視聴料若しくはデータ放送によるショッピングサービス等の代金の請求又は統計作成の目的のみに制限する努力義務を事業者に課している。

第 14 条は、視聴履歴の管理について特段の規律を設けた規定である。視聴履歴の漏洩が視聴者への多大な権利侵害となりうる点を鑑み、他の個人データよりハイレベルな安全管理上の措置をとる努力を義務付けている。具体的には、郵送等の場合の封筒への封入やシールの貼付けや、電気通信回線による伝送の際の暗号化等の措置である。

以上で述べたとおり、放送事業者の個人情報保護指針においては、放送の視聴履歴情報を高いプライバシー性を持つ個人情報と位置付け、その特性に応じた特段の保護措置をとることを事業者に要請している。

※無論、視聴履歴は、個人情報保護法や放送指針の一般条項にもかかるが、ここでは詳細な議論は省く。
※上記につき、詳細は総務省ウェブサイト（http://www.soumu.go.jp/joho_tsusin/040831_1.html）を参照。

３－３　Ｂ－ＣＡＳ方式による視聴履歴の扱い

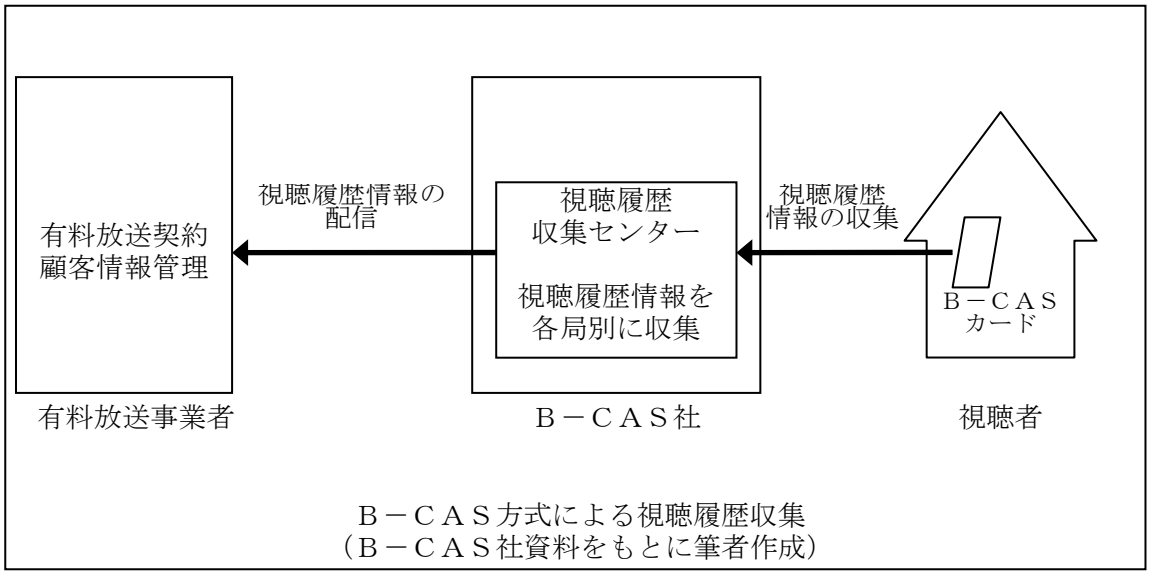
ここで、現行のＢ－ＣＡＳ方式による視聴履歴の管理の現状について触れる。

Ｂ－ＣＡＳ方式（BS Conditional Access System）は、現在わが国の地上デジタルテレビジョン放送及びＢＳデジタル放送等で用いられている限定受信方式で、2000 年からはこのシステムを用いて、放送事業者による視聴コントロールや著作権管理等が行われている。この方式の運用は、放送事業者や機器メーカーが共同出資で設立した株式会社ビーエス・コンディショナルアクセスシステムズ（以下、Ｂ－ＣＡＳ社とする。）が実施している。

このシステムにおいて有料放送やＰＰＶ放送を視聴する場合には、Ｂ－ＣＡＳ社に氏名、生年月日、住所、電話番号等について「ユーザー登録」を行う必要があり、これらの情報が視聴履歴とともに放送事業者に提供され、課金が行われる仕組となっている。

登録者の視聴履歴情報については、まずＢ－ＣＡＳカード上にデータが蓄積される。蓄積されたデータは暗号化され、Ｂ－ＣＡＳ社の「視聴履歴収集センター」によって一括収集され、各放送事業者に配信される（下図参照）。その際、通信障害時の保守メンテナンス等のために通信記録データを半年間保存する。なお、そのデータ内容については、各放送事業者がデータフォーマットを作成するもので、Ｂ－ＣＡＳ社は解読できない仕様となっている。

現状においては、課金が必要なＰＰＶ番組等を除き、Ｂ－ＣＡＳ方式による恒常的な視聴履歴の収集は行われていない。



Ｂ－ＣＡＳ方式による視聴履歴収集
（Ｂ－ＣＡＳ社資料をもとに筆者作成）

※出典：総務省「放送分野における個人情報保護及びＩＴ時代の衛星放送に関する検討会」2004 年 5 月 19 日会合Ｂ－ＣＡＳ社提出資料（http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/hoso_it_eisei/pdf/040519_2_s1-2.pdf）

３－４　今後の方向性

以上で述べてきたとおり、放送デジタル化による技術の進展により、視聴者の同意なく恒常的に視聴履歴情報の収集が行われているわけではないものの、視聴履歴情報の収集そのものは技術的に可能な環境となっている。

アナログ放送では通常、こういった視聴履歴情報の収集が行われることは無く、「匿名での放送視聴」は議論するまでも無いごく当然の前提であったと言えるが、デジタル化によって「いかに匿名での放送視聴を保護するか」という新たな論点が生まれたと言うことができる。

特に放送分野においては、他の分野におけるプライバシー保護と比して、こうしたデジタル放送の技術的特性に対する認識がまだ十分に一般視聴者にまで行き渡っておらず、放送シーンでの匿名性の確保の在り方についていまだ十分な議論がなされているとは言いがたい状況にある。

いずれにせよ、個人情報保護政策の一環としての視聴履歴の保護の在り方について、デジタル放送技術・放送機器性能の飛躍的な進歩に合わせ、世論を反映した安心・安全な制度設計の構築に向けて、十分な議論と不断の見直し姿勢が不可欠である。

※なお、地上デジタル専用受信機については、ＣＡＳカードを用いない受信管理方式の導入を放送事業者等が検討していると一部で報じられており（2007 年 2 月 19 日　日経産業新聞２面等）、実際に導入されれば、地上デジタル放送において受信者登録は行われないこととなる（ただし、ＢＳ・ＣＳ放送等については、引き続き受信者登録が必要となるものと思われる）。放送事業者等のこういった動向にも今後注視する必要がある。

※ＮＨＫ放送技術研究所では、プリペイド方式を用いた匿名視聴技術の研究開発を行っている。また、独立行政法人情報通信研究機構（ＮＩＣＴ）からの委託により、視聴者情報の各項目をシャフリングして紐付けをさせない機能や電子署名技術によるデータ保護機能等を持つ「視聴者情報管理保護システム」の研究開発も行っている。デジタル放送時代の視聴者プライバシーを保護するためのこうした匿名視聴保護技術のさらなる進展も、今後期待されるところである。詳細はＮＨＫ放送技術研究所ウェブサイト（http://www.nhk.or.jp/strl/group/systems/systems02.html）を参照のこと。

４．インターネットの閲覧履歴

４－１　インターネットの閲覧履歴のプライバシー性

情報通信白書によれば、インターネット人口は２００５年時点で８，５２９万人に達し、人口普及率にすると６６．８％の国民が利用するメディアに成長しており、生活に密接に関わるメディアとなりつつあると言える。

また、「ロングテール」と呼称されるネット・トレンドに象徴されるように、個々のユーザーのニーズや嗜好に適合したサービスが進展しつつあり、ユーザーの利用傾向や嗜好を綿密に解析し、それに応じて適切なサービスをレコメンドする機能が導入されつつある。

こうしたサービスについては、利用の際のユーザー側への十分な知識のさらなる啓発が必要となってくるであろう。

４－２　インターネット閲覧履歴にまつわる技術の現状

インターネットの履歴については、クッキー、Web ビーコン、スパイウェア等の技術の発達により、第三者によってこれを収集される可能性が出てきている。

これらの技術に関する知識が不十分な場合には、予期しないうちにインターネットの閲覧履歴情報を第三者に取得される可能性もある。

４－３　今後の方向性

インターネットの急速な普及に伴って急増したライトユーザー層においては、インターネットをテレビと同質な受動的メディア（あたかも一方通行のメディアのごとく、流れてくる情報を受け取るだけのメディア）ととらえて利用する可能性もあり、閲覧履歴が収集されるリスクがあることについて十分な知識を有していないおそれがある。

また、上で述べたような個々人の嗜好や生活形態をネットサービスが綿密にフォローするいわゆる「ロングテール」の時代が本格的に到来すれば、インターネットの利用動向が個人の嗜好・思想等をより色濃く反映していくこととなり、さらに履歴のプライバシー性も増す可能性もある。

そういった場合には、クッキー等の技術を活用した履歴利用型マーケティングやレコメ

ンド機能、広告配信等のサービス提供の在り方についても、重要な論点となってくると考えられる。

５．通信・放送融合時代のメディアコンテンツの利用履歴

以上の節では、放送・インターネットそれぞれにおける視聴・閲覧の匿名性に関する諸論点を挙げてきたが、いわゆる通信と放送の融合によって、新たな論点も生じうる。

具体的には、３－２で挙げた放送関連の個人情報保護指針は、いわゆる「ネット放送」と呼称されるような通信を利用した動画コンテンツには適用されない。通信コンテンツに関する視聴履歴については、別途「電気通信事業における個人情報保護に関するガイドライン（平成１６年８月３１日総務省告示第６９５号）」が存在し、そこで通信履歴として包括的に保護される形となっているが、当該ガイドラインの適用を受けるのは電気通信事業法（昭和５９年法律第８６号）上の電気通信事業者のみとなっている。

また、デジタルテレビでのネットコンテンツ利用や、ワンセグ対応携帯電話でのＴＶ・ネット双方のコンテンツへのアクセスのように、一つの端末で通信サービス・放送サービスの双方をシームレスに利用する形態が生じた場合に、視聴・閲覧履歴をどのように保護するかについて、論点となりうるであろう。

加えて、コンテンツ権利者側によるデジタル技術を利用した著作権管理技術（ＤＲＭ）の導入も進展してきており、こうした状況下で電子著作物へのアクセス記録等を「知的プライバシー（intellectual privacy）」とみなし、その保護をどのように確保するかについても、論点として注目されつつある。（知的プライバシーの論点を紹介したものとして、Julie E. Choen (2003)“The Law and Technology of Digital Rights Management”, 18 Berkeley Tech. L. J. や 2007 年 1 月 26 日毎日新聞１２面　等）

今後予想されるその他の論点としては、通信・放送企業の経営統合・業務提携や各種サービスの垂直統合によって、各サービスのコンテンツ利用履歴のマッチングが可能となり、より高度なプライバシー情報がマーケティングのためにデータベース化されるおそれがある点等が挙げられよう。

６．アンケート結果の分析

ここで、利用者アンケートの結果を見てみると、デジタル放送については、「ユーザー登録が必須となる番組は視聴しない」と回答したユーザーが７０％近くにまで上っており、インターネット動画コンテンツについても、「サービス利用にあたり会員登録（個人情報の登録）をしたくない」と考えるユーザーが６０％を超えており、映像コンテンツの視聴にあたって個人情報を提供したくないと考えているユーザーが多いことが分かる。Ｂ－ＣＡＳカードの機能やクッキー等の技術に関する知識の習熟度もまだ十分とは言えず、安全・安心なコンテンツの利用環境に向けた、さらなる利用リテラシーの向上が必要であると言えよう。

第二部第三章　「匿名による売買の自由」

はじめに

電子ショッピングモールやオークションサイトでは、取引相手が見えないため、詐欺、取引否認などのトラブルが生じやすい。これを防ぎ、取引の安全を確保するためには、取引相手の氏名、電話番号、メールアドレス、クレジットカード番号などによって取引相手の実在性や行為権限の確認をしっかり行うことがますます重要とされている。しかし、他人に簡単に提供してしまうかもしれない個人や、個人情報保護法が全面的に適用されない小規模事業者に、このような氏名などの個人識別性の高い情報を提供することには、誰しも不安を感じるものである。

そこで、原則として個人情報の相互提供を行わずに、リアルな店舗やフリーマーケットにおける「現実売買」（あらかじめ交渉することなく、その場で商品と現金を同時交換する売買）のように、ある程度匿名のままで、ネット上において物品の売買を行うことができる場合もあるのではないかと考えている。現実売買では、なにか問題が起きてから、人相、容姿などから誰であったかを特定すれば足りることが多い。現実売買のほとんどの場合において、氏名という個人情報を収集することなしに大きなリスクを伴わず、売買という目的を達成できていると考えられる。ネット上の売買においても匿名で済むのであれば、自己に関する情報が、自分の知らないところで流通する不安もなく、プライバシーの観点から安心である。

このことは、EU の個人データ保護指令（95 年）第 6 条第 1 項 c 号に規定されている「目的に対して過度（excessive）に個人情報を求めない」という原則に通じるものであり、売買当事者は、氏名という最も鍵となる個人情報を収集しなくも何とか目的が達成されるのであれば、氏名の収集を控えるべきであるとの考え方によるものである。

そこで、本章では、ネット上において匿名のまま売買を行う上で検討を要する制度的な事項を整理することとしたい。

なお、本章では、「匿名」とは、特に言及しない限り、販売者と購入者の間における匿名を意味する。販売者と購入者の間に仲介者が存在し、仲介者に対する販売者又は購入者の匿名を意味する場合は、その旨それぞれに箇所で明確に記述することとする。

また、ネットでの売買というときに、音楽などのデジタルコンテンツの売買も含まれるが、デジタルコンテンツの売買は前章「匿名でのネット視聴」の項で、取り扱っているので、本章では対象としない。有体物（動産）のみを売買商品として検討対象とすることとする。

１　氏名など個人識別情報の利用

１－１　契約の成立

１－１－１　契約相手の特定

現実売買の場合は、匿名で取引することが一般的である。現実売買では、申込と承諾がなされ、契約が成立し、直ちに双方の債務の履行が終了し、債権債務関係は解消され契約は消滅する、とも解せられる。しかし、このように債権・債務を生じさせる合意があったと考えるべきか（債権契約説）、それとも、物権の移転についての合意だけしかないと考えるべきなのか（物権契約説）、現実売買については、学説に対立があるといわれている※1。現在では債権契約説が有力とされているが、実際には両説の差異はそれほど大きいものではなく、現実売買にも民法の売買の規定が一般的に適用されるという意味で、これを売買契約と解して妨げはないとされているとのこと※2である。

したがって、ネット上において匿名の B2C あるいは C2C であっても、取引内容について相対立する意思表示の合致、すなわち当事者間の合意があるとすれば、電子的な売買契約が成立していると解することができるのではないだろうか。

現実売買において、契約相手方は眼前の者であり、顕名ではないが、それぞれの契約相手である販売店員またお客をその容姿などからひとまず識別できている。つまり、契約が消滅するまでの間、契約相手方を特定できているとも解釈できる。ネット上の売買においても、何らかの特定（最終的に当該人を識別できること）がなされていないと、契約履行に関して問題が生じたときに相手を責任追及できないリスクを負うこととなる。裏を返して言うと、もしリスクがあるのであればリスクの大きさに応じて、後から契約相手を確実に特定できれば、契約時点において氏名・住所を必ずしも必要としないということでもある。

後から個人を識別できる手段として何らかの信頼できる識別符号を得ていれば、氏名・住所を得ていなくても、識別符号を管理している者が必要なときに氏名・住所を開示してくれれば、それを利用して問題解決できると考えられる。したがって、本章でテーマとしている匿名化とは誰に対してもどんなときにでも匿名という完全な匿名を前提にしているものではない。売買において、双方が一般に期待するとおり行動している限りは、販売者と購入者の間で氏名（実名）やりとりをしないという意味である。匿名化のためのこのような識別符号は、他のデータベースにおける氏名（実名）とマッチングができないように、仮名やその場かぎりの ID 番号など一般に広く使用されていない符号であることが望ましい。そして、正当な理由があれば、氏名・住所などの本人情報を開示してくれる制度的な裏付けが必要である。

この識別符号の候補としては、使い捨ての銀行口座番号や使い捨ての携帯電話番号などが考えられる。銀行口座番号、携帯電話番号は、事業者の本人確認義務が法定されており登録個人情報の真正に対する信頼性が高いので、大きな問題が起きたとしても確実に個人を特定できる。「金融」「通信」分野ということで分野別ガイドラインにおいて事業者に対する安全管理義務など個人情報保護の要件も厳格である。現状では、銀行あるいは通信事業者が仲介者として匿名化サービスを提供することが、他業提供に該当するのか否かな

ど、業法上どのような位置づけとなるのか必ずしも明らかになっていない。また、もし提供可能としても、どのような場合に利用者の本人情報を開示することとするのか、運用ルールが明確になっていないので、直ちに使い捨て銀行口座番号や使い捨て電話番号を使うことは困難と考えられる。

電子署名認証法の電子証明書がとりあえず匿名で使えると、制度的な裏づけがあり好ましいのではないかと思う。氏名ではなく使い捨て識別符号による匿名電子証明書である。しかし、電子署名認証法の「認証業務」は、「自らが行う電子署名についてその業務を利用する者その他の者の求めに応じ、当該利用者が電子署名を行ったものであることを確認するために用いられる事項が当該利用者に係るものであることを証明する業務をいう。」と定義（同法第２条第２項）され、当該利用者の識別を「氏名」で行うことを前提として当該利用者を証明する業務であるとすれば、匿名のままである者の行為であることを確認していることの証明という枠組みに応じることは根本的に矛盾した行為となると考えられる。現状では、「氏名を人の目につくように書きつける」※3という「署名」の本来の意味からすると、仲介者である認定事業者が同法に準拠したものとして氏名の記載のない電子存在証明書を発行することはできないのではないだろうか。コンピューターがネット上で膨大なデジタル信号をやりとりして識別・認証する時代において、氏名をもって識別・認証するという人間の能力に適合した「署名」という方法にこだわらなくてもよいと考えられる。

なお、債務履行に関して後から問題が生じる可能性が非常に低い場合には、仲介者を通じて顕名化ができない完全な匿名であっても支障がないと考えられる。例えば、代金先払いで商品を後から送る場合には、販売者からみて購入者が完全な匿名であっても問題がない。後から、商品にクレームが提起されたときに本当に自分が販売した商品かどうか確認するには、領収書や保証書を現物として同梱して発送し、クレームの際にこの提示を求めるとともに、販売した商品の製品番号を記録しておいてこれと照合するようにすれば、問題はないと考えられる。

※1　民法（6）契約各論[第４版増補補訂版]　有斐閣双書　p19

※2　同上　p20

※3　電子漢字辞書「漢字源」学研

１－１－２　未成年者

民法第５条第１項では、「未成年者が法律行為をするには、その法定代理人の同意を得なければならない。」とされ、同条第２項では、「前項の規定に反する法律行為は、取り消すことができる。」とされている。したがって、販売者の立場（購入者の立場の場合もあり得ないことはないが、そういった事例は少ない）からすると購入者が未成年か否か確認しておかないと、未成年であった場合に後から契約を取り消されるリスクが生じる。大きなリスクではないかもしれないが、代金返却など契約がなかった状態に戻すために事務コストなどが発生してしまう。

「現実売買」では、厳密に年齢を聞くことはしないが、その場で眼前にいる者が購入者と特定でき、そして名前を聞かなくても、容姿や言動で未成年か否か確認できることが多

い。もし、購入者が小学生らしき場合であり、高価なおもちゃを購入しようとしているならば、一般的にはお父さんかお母さんに話をしているか尋ねるであろう。また、「そのお金はどうしたのか。」と手持ち現金の取得経緯を尋ねるかもしれない。お小遣いの範囲であれば、民法第５条第３項に規定された法定代理人が「目的を定めないで処分を許した財産の処分」に該当し、未成年者が自由に処分を行うことができることになっている。したがって、「現実売買」の場合には匿名のままでも、未成年者との売買に伴う契約取消リスクはかなり回避できる。

ネット上での売買でも、クレジットカードの場合には、その一般的な加入審査の条件は「①18 才以上である事(但し、高校生は不可）②本人か配偶者に安定した継続収入があること」とされているので、クレジットカード決済であれば、未成年かつ許されない財産処分に該当する可能性はかなり低い。

クレジットカード決済以外であって未成年であった場合の取消リスクが懸念される場合には、未成年であるか否かまず質問し、未成年の場合は両親の同意の有無やお金の取得経緯を聞くことが求められよう。もし、未成年者が成年者などと偽って答えたときには、民法第２１条「制限行為能力者が行為能力者であることを信じさせるため詐術を用いたときは、その行為を取り消すことができない。」とされているので、契約の取消ができないこととなると解せられる。

なお、現実売買では、高校生・中学生などの未成年者が、大人と同様にかなり自由にアルコールやタバコなどを除き小額商品の購入が許されている。上記のような年齢確認を厳格に行うと高校生・中学生がネット上の売買から締め出されてしまうかもしれない。少額かつ錯誤が生じにくい商品の場合など、販売事業者が契約取消のリスクが小さいと判断するときに、未成年者か否か確認せずにネット上で販売することは販売業者の自由である。

１－２　決済における氏名など個人識別情報の利用状況

１－２－１各決済制度

1-2･1-1 クレジットカード

磁気テープ型のクレジットカードには、クレジットカード番号（クレジットカード会社の企業コードと会員番号）、カード会員名（ローマ字）、有効期限などの情報が記録されている。加盟店の店頭にてクレジットカードでの商品の購入を申し込むと、まずオーソリゼーション請求（与信の可否についての信用照会）として、クレジットカード番号、有効期限、取引額、加盟店コードが、加盟店から自動的にアクワイアラ（加盟店管理会社）を経て、イシュア（カード発行会社）に送信される。その後、取引に関する情報が同様に加盟店から送信される。この過程を通じて、加盟店端末（G-CAT、ＣＣＴ）に、取引明細として、クレジットカード番号、カード会員名、商品種類、金額、日時が記録され蓄積されていると推測される。ローマ字氏名ではあるが、店頭でのクレジットカードの使用は、加盟店たる販売店に対して顕名での取引となっているのではないかと考えられる。

この過程において、加盟店は、商品の購入申込者にカードの提示を求め、偽造が難しいホログラムをチェックして偽造カードでないかどうか確認し、また、サインを求め※1裏面

のサインと照合することで、会員本人に間違いないか認証している。サインの照合を行う上で、販売店の店員は、サインと会員の氏名との照合（漢字サインであれば、漢字氏名と照合することが望ましいが、国際規格であり、漢字氏名をカードに表示することは不可能）も行っている。このチェックを十分に行わずに販売した場合には、販売店又はアクワイアラの責任となる。

インターネットを通じて決済する際には、カード提示を求めることは物理的にできないし、サインの照合も技術的に困難である。そこで、やむなくカード番号、会員氏名、有効期限を入力することとしている。ネット決済において、会員氏名も貴重な認証のための情報とも考えられるので、店頭決済とは異なり、イシュアにおいて、会員氏名でマスターファイルと照合を行うために、会員氏名をオーソリゼーションの際に、送信しているのかもしれない。

しかし、暗号方式やパスワードなど別の認証方法によって、イシュアが契約会員であることを認証できれば氏名の聞き取りは必要ないのではないかと考えられる。

特に、なりすましによる不正使用による損害を販売店でなく認証を行ったイシュアが負担するのであれば、販売店は決済という観点からは氏名を取得する必要性はないと考えられる。すでに、カード番号、氏名、有効期限といった情報を不正取得しこれを悪用されることを防ぐため、SET（Secure Electronic Transactions）等の技術的な仕組みが導入されており、会員のカード番号や氏名は加盟店に提供されずとも決済可能となっている。また、新たな国際標準として、3-D Secure が、採用されている※2。この方式は、イシュアがパスワードを使い、自ら会員を直接認証するものである。

また、Citibank は、一回限りのクレジットカード番号を使い、販売者には匿名のまま、決済できるバーチャルクレジットカードを発行している※3。

※1 加盟店がカード会員本人以外の者の不正利用のリスクを負担している場合には、サイン不要のケースもある。ただし、ETC（高速道路における電子的な通行料金収納）では、磁気カードではないが、アクワイアラがリスク負担しているといわれている。

※2 経済産業省 インターネット商取引とクレジット事業研究会 第4回 資料4 から http://www.meti.go.jp/committee/materials/downloadfiles/g50929b04j.pdf

※3 Virtual Account Numbers
http://www.citicards.com/cards/wv/detail.do?screenID=700

1-2･1-2 電子マネー

電子マネーについては、転々流通可能なオープン・ループ型のものと使用の都度発行者に還元されるクローズド・ループ型のものがある。我が国では、後者のタイプである Suica 及び Edy が広く普及している。Suica、Edy には、記名式と無記名式がある。記名式は、通勤通学定期券や会員カードなどとのジョイント型・提携型に多い。無記名式は、鉄道乗車券や商品の購入と同様に駅又は店舗にて匿名でカードを購入できる。それぞれの IC カードには、ID 番号が割振られていており、加盟店において商品を購入するすると、この ID 番号、購入品目、購入日が、センターサーバに送られる。無記名式の場合には、Suica の発行会社である JR 東日本社、Edy の発行会社であるビットワレット社及びそれぞれの加盟店と

もに、利用者の氏名がまったく分からない。無記名式の Suica、Edy については、利用規約によって利用者間でカードを売買することが、禁止されているということはない。

前払式証票の規制等に関する法律（プリカ法）が、Suica や Edy など IC チップを搭載したカードにも適用されているようである※1。発行総額の半額を国に供託することによって、万一発行会社が経営に行き詰まったときに利用者を保護することが、プリカ法の目的である。なお、「電子マネー発行機関の事業開始と継続，および監視に関するＥＵ指令」2000/28/EC 及び 2000/46/EC では、電子マネー事業者の経営安定のための基金保有と投資制限について規律している。供託という単純な手法ではなく、各種規制を組み合わせ、経営資源の効率的配分に考慮した手法によって、発行事業者の経営健全性を確保し、消費者の保護を図っている。

Edy の場合には、家庭のパソコンにパソリ（市販されているカード情報のリーダー・ライター）をつないでネット上で送金することが既に可能となっている。決済だけで配送を考えなければ、決済事業者であるビットワレット社にも商品購入先の加盟店にも匿名のまま送金が可能である。家庭のパソコンでの処理の流れは不明であるが、Mobile Edy による決済では、①アプリケーションの画面から商品購入の申し込み（同時にメールアドレス通知）→②加盟店からビットワレット社の Edy センターに決済依頼→③ビットワレット社からユーザへ決済開始メールを送信→④メールをクリックすると i アプリが起動し、支払いを実行→⑤決済完了メール送信→⑥ビットワレット社は加盟店に送金、という手順となっている※2。なお、現在、プリカ法適用の電子マネー事業者については、金融機関等による顧客等の本人確認等に関する法律（本人確認法）の適用がない。本人確認法の１０万円以上の送金という条件（政令事項）が、もし今後引き下げられ Edy の送金上限金額２．５万円を下回った場合には、電子マネーによるネット送金に本人確認法を適用させるべきか否か議論になるのではないだろうか。

物理的なカードを使わないインターネット上の電子的支払サービスとして、電子的価値をサービス提供者のサーバに一旦蓄積し、その後加盟店等へ電子的価値の移転を指示して支払う場合は、前払式証票の規制等に関する法律（プリカ法）が適用されないとする説が多い。「証票」とは「ある事を証明するための札や書き付け」※3であり、物理的な認証手段であったが、今後、ユビキタスネット社会において、人間ではなくコンピューターが認証する時代では、Suica や Edy が物理的カードを使っていたとしても、コンピューターは、IC カードとしてのデジタル情報を送受信して認証している訳であり、物理媒体によって法の適用を切り分ける意味はない。携帯電話の SIM カードやバイオメトリックスなど高度な認証方法が発展・普及することになるが、媒体による差異に注目するのではなく、消費者の貨幣的価値を預託し決済するというその機能に着目して規律すべきと考えられる。

また、商品又は役務及びその提供者が特定されている状況下であれば前払いであるが、乗車券か缶ジュースかどのような商品や役務に対して支払うのか、誰から購入又は提供を受けるのか、債権の具体的内容が決まっていない以上、前払いといえないのではないかと素朴に考える。また、換金性（換金が可能か否か）が出資法及び紙幣類似証券取締法との適用関係を判断する基準とされているようであるが、加盟店が今後ますます拡大しカード間の相互受け入れが進み、その汎用性がさらに高まると、電子マネー自体が貨幣的な普遍的な価値を有することになり、換金性に着目する意義は薄れると見られる。むしろ、電子

マネー発行体の健全経営と万一破綻したときの連鎖破綻を防ぐ制度的な仕組みが重要と考えられる。銀行の決済口座を利用したネット決済との相違はかなり曖昧になっていくのではないだろうか。

※1 金融審議会金融分科会情報技術革新ワーキンググループ座長メモ　平 18.4.26　p2

※2「モバイル FeliCa はビジネスになる！」p102　モバイル FeliCa 研究会　日経 BP

※3　デジタル大辞泉　小学館

1-2･1-3 オンライン銀行

銀行の行う送金手段としてのいわゆる「口座振込み」、「口座振替」は、銀行法上第 10 条第１項３号に規定されている「為替取引」に該当する業務である。この為替業務について、その要件を詳細に規定している法令はないようである。当事者間の契約自由であるとすれば、匿名或いは仮名での送金は基本的に認められていると考えられる。

金融庁の主要行等向けの総合的な監督指針　Ⅲ-3-7-2 には、「(4)①インターネットバンキングが非対面取引であることを踏まえた、本人確認等の顧客管理体制の整備が図られているか。」との記述がある。この本人確認とは本人確認法の本人確認である。法執行当局が、送金人が誰か特定できるようにする目的である。受取人にとって送金人が、顕名でなければならないことを要求しているものではない。送金人の欄が「法執行当局用」と「受取人用」に分かれていないので、「口座振込み」における匿名の送金決済は実態上困難であるが、「口座振替」であれば、口座開設時に厳格に本人確認しているので、個別の送金については送金人欄に仮名を使用しても既に送金可能である※1。また、振り込まれる口座についても匿名で可能な仕組みが実用化されている※2。

ところで、リアルの店舗において、J デビットを用いて商品を購入する場合、加盟店の端末では、キャッシュカードの情報を読み取り、直ぐに情報処理センターに送信される。暗証番号の入力を要求して認証を行い、口座名義人であるか否か確認している。カードに格納されている会員氏名（カナ氏名）、口座番号等の情報が、加盟店の端末に蓄積されているかもしれない※3。

なお、口座振替が帳票によってバッチ処理されていた時代は、デビット＝リアルタイム処理として、取り扱いに相違があったと考えられるが、口座振替が瞬時に行われるようになると両者の相違はほとんどなくなるのではないかと考えられる。ネット上でも、既にネットデビットサービスが提供されている。第一暗証番号、第二暗証番号と二つの暗証番号を使用して厳格に利用者を認証している。こちらも振込人名を変更可能である※4。

※1　みずほダイレクトでは、インターネット、携帯電話から口座振替などの決済が可能であるが、口座振替の場合には、「振込依頼人名の変更が可能です」とされ、口座名義人の氏名を変更して送金することは既に可能となっている。

http://www.mizuhobank.co.jp/direct/about_direct/furikomi.html

※2　ヤフーID とジャパンネット銀行は、連携した新決済サービスとして、「ひとつの取引ごとにワンタイム口座を割り当て落札者に入金してもらう。一度入金されるとその口座は使えなくなる。連動しているため、出品者は

入金の有無を簡単に確認できる。」サービスを既に提供している

http://www.japannetbank.co.jp/service/payment/net_banking/onetime.html

※３　Ｊデビットの HP の FAQ からすると、「Ｑ：利用履歴に関しての質問等は、どこへ問い合わせたら良いのでしょうか？　Ａ：利用した加盟店やカード発行金融機関にご相談ください。」とされ、デビット決済の場合に、口座通帳に販売店名が記載されるので、販売店は後からの照会に備えなければならない。日時と口座番号だけでは、本人かどうか確認するのに不十分であるので、氏名を記録蓄積し、照会時に照合しているのかもしれない。

http://www.debitcard.gr.jp/faq/a.html#007

※４　三井住友銀行 HP　インターネットバンキング　よくあるご質問　No.142　「振込依頼人名を変更することはできますか？」

http://www.smbc.co.jp/kojin/direct/faq/faq09.html#s0q01

１－２－２　個人情報保護制度

ここでは、個人情報保護法の運用の実際について概観してみたい。

クレジットカードに係る与信情報の取扱いについては、「経済産業分野のうち信用分野における個人情報保護ガイドライン」※１が適用になる。経産省産構審割賦販売分科会基本問題小委員会では、イシュア、アクワイアラ、決済代行業者、クレジットブランド会社等関連事業者の機能分化が進んでいることなどから、平成１８年６月に「個人情報を含めたカード情報については、業務委託の拡大等も相俟って幅広い関係者がこれを保有、管理する状況が生じており、それぞれの関連事業者が果たすべき役割やその責務の実効性を確保するために必要となる制度面での対応を含め、実効性ある対策の検討が必要である」と提言している。同ガイドラインは平成１８年９月に改正されている。なお、同ガイドラインは、「与信事業者」及び「個人信用情報機関」を対象としており、一般の加盟店は対象ではない。ネット上の商品販売者たる一般の加盟店に対しては、「経済産業分野を対象とするガイドライン」※２が適用される。

「金融分野における個人情報保護に関するガイドライン」※３は、同ガイドライン第１条１号において「金融庁の所管する分野」に適用するとされ、銀行法に基づく預金業務を行うオンライン銀行は、同ガイドラインが適用される。また、同ガイドライン第 10 条を受けて、「安全管理措置等についての実務指針」※４が定められている。

電子マネーについてのプリカ法も金融庁所管の法律であり、金融分野のガイドラインが電子マネー発行者には適用される。なお無記名の電子マネーカードは、発行時に個人を特定できる情報を取得しないので、そもそも個人情報保護法の個人情報を取り扱っていることとならない。

※１ http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou/shinyo.pdf

※２ http://www.meti.go.jp/policy/it_policy/privacy/041012_hontai.pdf

※３ http://www.fsa.go.jp/common/law/kj-hogo/01.pdf

※４ http://www.fsa.go.jp/common/law/kj-hogo/04.pdf

１－２－３　匿名可能性

ネット上のオンライン決済をみると、クレジットカード、オンライン銀行及び電子マネ

ーいずれも、最も重要な点は、決済事業者が販売者と消費者を正確に識別・認証できなければならないという点である。対面でのリアルな決済では、識別を名義人氏名、口座番号、クレジットカード番号などで行い、認証を第三者が簡単に入手しえない物理的なカード（ホログラム技術）、印鑑、暗証番号、サインなどで行っていた。ネット上では、すべてデジタル情報で行われ、リアルにおける物理的・視覚的な認証媒体による取扱いの違いがなくなる。また、ネット上では、決済事業者が暗証番号や暗号鍵を用いてネットを介してリアルタイムで直接確実に認証できれば、それで足りる。銀行の窓口職員や加盟店の店員が、決済事業者の認証事務を助けるために、識別を氏名で行い、印鑑やサインで認証を行う必要はなくなった。商品の販売店が、決済という点からすると購入者の氏名を取得する必要はなくなったと考えられる。

また、コンビニ払込、代引きと言った現金を使った決済についても、決済という部分だけであれば、自明のことであるが匿名のままで可能である。

１－３　配送における氏名など個人識別情報の使用状況

１－３－１配送における匿名化サービスの現状

日本郵政公社では、2006 年 11 月から郵便規則を改正し、新たな特殊取扱として「あて名変換サービス」を提供している。これは、郵便物のあて名等の代わりに識別符号を用いることで、差出人、受取人双方が住所・氏名等をお互いに知らせることなく小包郵便物を配達する特殊取扱である。利用希望者は、予め住所、氏名等の情報を、公社が指定した管理者（オークションサイト運営事業者など）に事前に登録しておき、この管理者は、差出人と受取人の情報及びこの両者を結びつける識別符号を管理し、公社に提供する。公社は、この情報をもとに郵便局窓口で引受けた後、あて名を変換する郵便局において、受取人の住所及び氏名の情報を入手して、新たなあて名とし、配達するものである※1。

また、大手宅配事業者も匿名配送サービスを開始している※2。利用希望者は、予め住所、氏名等の配送のための情報に加えて、決済方法等の情報を直接登録しておき、事前に宅配用の ID を取得しておく点が異なっている。すなわち、宅配事業者自体が個人情報のデータベースを保有し、決済についても仲介するものである。中身を確認して万が一問題があった場合、商品受取り後二日以内であればキャンセルができ、返金返送が可能となっている。したがって、匿名でも、あまり、トラブルは生じないのではないだろうか。なお、悪意をもった詐欺行為によりトラブルが発生した場合、宅配事業者より相手に対して顧客情報を開示する場合があると注意事項に掲げ、完全に匿名ということではなく、本人情報を開示する場合があると利用者に説明している。

自宅への配送ではないが、コンビニ受取のサービスも既に開始されている※3。現状では住所・氏名を記入して購入申込をすることとなっているが、仮名を使えるかどうかホームページからははっきりとわからない。なお、コンビニに商品が到着した旨のメール受取が必要であり、この限りではメールアドレスを明らかにしなければならない。個人が多数のメールアドレスを使えるようになると ISP（インターネット接続事業者）が、アドレスの所有者を明らかにしない以上は、匿名となる。注文だけして、商品をコンビニに取りに来

ないといった業務妨害については、犯罪として捜査令状があれば ISP は本人の情報を開示してくれるので、損害賠償を求めることができる可能性はある。なお、現段階では、手数料が送料込みで商品一個につき 1000 円程度かかってしまうことが、課題であろう

※１　日本郵政公社　　あて名変換サービス

http://www.post.japanpost.jp/whats_new/2006/topics/atena_henkan.html

※２　ヤマト　　オークション宅急便・匿名配送サービス

http://www.kuronekoyamato.co.jp/auction/auction.html

※３　（株）ウエルストーン　　コンビニ店頭受取りサービス

http://fibertrip.com/sds.html

１－３－２　個人情報保護制度

商品引き渡しと決済が同一時点で行えない取引事例では、配送或いは決済のために契約相手方の住所氏名等が必要となってくる。配送或いは決済という明確な目的を達成するために必要な情報を取得するだけであれば、「取得の状況からみて利用目的が明らかであると認められる場合」（個人情報保護法第１８条第４項４号）には、利用目的を本人通知、又は公表しなくても個人情報の取得が可能である。

商品の配送は、貨物自動車運送事業に該当し、「国土交通省所管分野における事業者等が講ずべきガイドライン」※1 が適用される。

ゆうパックについては、日本郵政公社が提供しているが、ゆうパック（小包）は郵便法の小包郵便物に該当し、郵便法第９条第２項において「郵便の業務に従事する者は、在職中郵便物に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても、同様とする。」と規定されている。平成１９年１０月の民営化以降は、ゆうパックは、郵便物ではなくなるため、郵便法は適用されず、基本的に貨物自動車運送事業法が適用される業務となることとなるので、「国土交通省所管分野における事業者等が講ずべきガイドライン」が適用されることとなる。

※１　http://www.mlit.go.jp/kojin/guideline.html

１－４　消費者保護法制と氏名

１－４－１　適用関係

ここでは、ネット上での売買と消費者保護に関する法令との関係を整理しておきたい。

1-4-1-1 消費者契約法

同法第２条第３項では、「「消費者契約」とは、消費者と事業者との間で締結される契約をいう。」と定義している。一般の小売商店における物品の売買は、「現実売買」であり売買契約書を作成しないが、消費者と事業者との間で締結される契約であるので、同法の「消費者契約」に該当すると考えられる。また、ネット上の取引であっても、消費者と事業者との間の売買契約であれば、「消費者契約」に該当すると考えられる。

1-4-1-2 特定商取引法

同法第２条第２項では、「「通信販売」とは、販売業者又は役務提供事業者が郵便その他の経済産業省令で定める方法（以下「郵便等」という。）により売買契約又は役務提供契約の申込みを受けて行う指定商品若しくは指定権利の販売又は指定役務の提供であつて電話勧誘販売に該当しないものをいう。」と定義されている。この規定を受けた施行規則第２条２号では、「郵便等」には「電話機、ファクシミリ装置その他の通信機器又は情報処理の用に供する機器を利用する方法」を含むとしている。したがって、「情報処理の用に供する機器」が具体的に何を指すのか明らかでないが、インターネットに接続された通信機器たるパソコンを利用して売買契約の申込みを受け付ける商品販売は、「通信販売」に該当し、特定商取引法が適用される。

なお、通信販売のうち指定商品を販売するもののみ、同法が適用される。同法第 2 条第４項では、「「指定商品」とは、国民の日常生活に係る取引において販売される物品であって政令で定めるものをいう。」とされ、政令の別表第一に具体的な対象品名が定められている。電子辞書など新たに出現した商品については、この別表第一のどの号に該当するのか、一般消費者にはやや分かりにくい。

ちなみに、電子モール事業やネットオークション事業に伴う役務の提供については、ネット上で会員加入を受け付けているので、同法の「通信販売」には該当するが、政令の別表第三の指定役務に該当しないので、同法の適用はない。

1-4-1-3　割賦販売法

クレジットカードを用いて購入代金の決済を行う場合、分割払い（2 ヶ月以上の期間にわたり３回以上に分割の場合）或いはリボルデング払いを利用するときは、割賦販売法の「割賦購入あっせん」に該当し、同法が適用される。購入者が、あらかじめ交付されたカードを店頭で販売員に提示して自らが与信資格を有する者であることを証明し、商品を購入することが、典型的な取引形態となっている。しかし、ネット上では、購入者と販売業者が非対面の関係にあり、カードの物理的な提示を行うことができない。したがって、その代替手段としてカード番号等の通知を行っているが、このような場合も、割賦販売法上、従来は交付された「証票等」を「提示」したものと解し、同法は運用されていたところである※1が、現在は「提示」に加えて「通知」の文言が追加され、割賦販売法上の各種規制がネット上のクレジットカード使用にも適用されることが明確になっている。

なお、割賦販売法では、「割賦販売」及び「個品割賦あっせん」については、指定商品のみに適用されるが、クレジットカードを利用することとなる「総合割賦あっせん」及び「リボルビング割賦あっせん」については、すべての商品に適用される。

1-4-1-4　景品表示法

同法は、商品及び役務の取引に関連する不当な景品類及び表示による顧客の誘引を防止することを主眼としている。第２条第２項の定義によると、「「表示」とは、顧客を誘引するための手段として、事業者が自己の供給する商品又は役務の内容又は取引条件その他これらの取引に関する事項について行なう広告その他の表示であつて、公正取引委員会が指定するものをいう。」とされている。この規定を受けた公正取引委員会の告示において「情報処理の用に供する機器による広告その他の表示（インターネット、パソコン通信等によるものを含む。）」と指定されおり、ネット上の販売にかかる Web での商品説明は、

同法が適用される。

※1　　2000.9.22 割賦販売審議会クレジット産業部会報告書　p2-3

１－４－２　事業者か消費者か

ロングテール化に伴って、個人であっても大きな投資（金銭的、時間的）をせずとも、インターネットにて頻繁に売買可能となっており、実際にも小遣い稼ぎの個人売買が増加している。そこで、事業者か消費者かが問題になるが、ネット上では、相手が見えないため、或いは、他者との取引実態がまったく見えないため、取引相手が、事業者か消費者か判断がつきにくいし、実態的にも数年前に日経新聞特集記事で「商費者」という言葉が紹介されたように、自らがどちらの立場かさえ判断しかねているケースが多くなっているといわれている。

1-4-2-1 消費者契約法

同法第２条第１項では、「「消費者」とは、個人（事業として又は事業のために契約の当事者となる場合におけるものを除く。）をいう」とされ、同条第２項では、「「事業者」とは、法人その他の団体及び事業として又は事業のために契約の当事者となる場合における個人をいう。」とされている。「「事業」とは、「一定の目的をもってなされる同種の行為の反復継続的遂行」であるが、営利の要素は必要でなく、営利の目的でもってなされるかを問わない。」とされ※1、反復継続して行われる同種の行為か否かで判断される。したがって、営利を目的としない協同組合の行う経済的活動も「事業」に該当すると解せられる。個人の場合に、どの程度の「同種の行為の反復継続的遂行」があるときを事業とするのか定かでない。いづれにしても、自らが消費者である場合は、契約相手の名称が個人名のときには消費者契約法が適用されない可能性が高いということである。民事ルールであるので、今後、判例等の積み重ねによってその定義が明確になることが期待される。

消費者契約法の場合には、商品売買において、販売者が「事業者」で購入者が「消費者」のときも、その逆の販売者が「消費者」で購入者が「事業者」のときも「消費者契約」に該当する。

1-4-2-2 特定商取引法

同法では、「販売業者」という用語を用いて通信販売を行う販売事業者の行為を規律しているが、「販売業者」という定義規定は置かれていない。同法の主務大臣である経済産業大臣は「電子商取引等に関する準則」を定め、「販売業者とは、販売を業として営む者の意味であり、「業として営む」とは、営利の意思を持って反復継続して取引を行うことをいう。」（２（２）⑤インターネットオークションと特定商取引法）と解説している。営利性が要件となっているところが、消費者契約法の「事業者」とは異なる点である。また、同準則では、販売業者の該当性の基準として、インターネットオークションでは「過去１ヶ月に 200 点以上又は一時点において 100 点以上の商品を新規出品している場合」などを例示しているが、購入者の側では、勿論全体の出品数がいくらなのか知るすべはない。結局、この場合も購入者は、販売業者の名称から「販売業者」に該当するかどうか類推することになる。

他方、購入者についても同法に明確な定義はおかれていないが、同法第 26 条第１項１号

では、「売買契約又は役務提供契約で、その申込みをした者が営業のために若しくは営業として締結するもの又は購入者若しくは役務の提供を受ける者が営業のために若しくは営業として締結するものに係る販売又は役務の提供」については、適用を除外すると規定している。したがって、購入者が「営業のため若しくは営業として」購入するときは、「通信販売」にかかる規定は適用されない。個人であっても、営業として購入する場合には、適用されない。

なお、購入者が営業目的である場合の第26条第１項１号の適用除外に関し、通達「特定商取引に関する法律等の施行について（平成18.1.30）」では、「本号の趣旨は、契約の目的・内容が営業のためのものである場合に本法が適用されないという趣旨であって、契約の相手方の属性が事業者や法人である場合を一律に適用除外とするものではない。例えば、一見事業者名で契約を行っていても、購入商品や役務が、事業用というよりも主として個人用・家庭用に使用するためのものであった場合は、原則として本法は適用される。特に実質的に廃業していたり、事業実態がほとんどない零細事業者の場合には、本法が適用される可能性が高い。」としている。ネット上の売買の場合には、販売業者にとって、購入者の名称しか判断材料はないが、しかし一見事業者名であっても例外があるということである。

1-4-2-3　割賦販売法

割賦販売法では、加盟店である販売業者が消費者である場合を想定していないと考えられるが、購入者が消費者に該当するか否かによって適用の有無が異なることとなる次の規定がある。同法第３０条の４第１項では、販売業者または役務提供業者（以下「販売業者等」という）につき生じている事由をもって、割賦購入あっせん業者に対抗することができる旨（いわゆる「抗弁権の接続」）を規定しているが、同条第４項２号により「その購入が購入者のために商行為となる指定商品にかかるもの」の場合には、本条各項は適用しないとされている。購入者が商行為を行っている者か否かで、抗弁権の接続がみとめられないケースもでてくる。なお、日弁連では、同号の規定の廃止を求めている※2。

また、第３０条の６では、第８条が準用され、指定商品等の販売を業とする者に対して行う当該指定商品の割賦購入あっせんにかかる販売は、関係規定が適用除外となる。

したがって、割賦購入する購入者が、商行為として行っているのか否か、或いは、指定商品の販売を業として行っているのか、によって、関係規定が適用除外となるか否か異なる取扱いとなるので、販売業者等にとっては、購入者の氏名はそれを判断するひとつの手がかりとなっているかもしれない。

1-4-2-4　景品表示法

同法第２条では、「「表示」とは、顧客を誘引するための手段として、事業者が自己の供給する商品又は役務の内容又は取引条件その他これらの取引に関する事項について行なう広告その他の表示であつて、公正取引委員会が指定するものをいう」と定義している。この「事業者」或いは「顧客」について、定義規定は置かれていない。景品表示法は独占禁止法の特例法であるので、独占禁止法第２条第１項「この法律において、「事業者」とは、商業、工業、金融業その他の事業を行う者をいう。」と定義が、景品表示法にも適用されると考えられる。ネット上での商品に関する「表示」であっても、この「事業者」の定義に該当しない者による表示に関しては、同法の適用はない。販売者が、「事業者」に

該当するか否か、さらに厳密には「事業」を行っているのか、購入者にとっては気になる点であるが、これも販売者の名称によって判断するしか他に方法はなさそうである。

1-4-2-5　民法、商法の瑕疵担保責任

瑕疵担保責任についても、購入者の購入が商行為にあたるか否かによって、取扱いが異なる。購入者の行為が商行為にあたる場合には、商法第 526 条第 1 項が適用され、「買主がその目的物を受取たるときは遅滞なくこれを検査し、もしこれに瑕疵あることまたはその数量に不足あることを発見したるときは、直ちに売主に対してその通知を発するにあらざれば、その瑕疵または不足に因りて契約の解除または代金の減額若しくは損害賠償の請求を為すことを得ず」とされる。他方、購入者の行為が商行為にあたらない場合には、民法第 570 条が適用され、売買の目的物に隠れた瑕疵があるときは、瑕疵の事実を知ってから１年以内であれば、損害賠償の請求などができる。

1-4-2-6 まとめ

いずれにしても、購入者にとって、販売者がプロ（「事業者」又は「販売業者」）か素人かということは、それぞれの消費者が関係する法律で保護されるか否かという売買の意思決定をする上で重要なポイントである。リアルの世界では、店構えや応対者の容姿・言葉遣いなどほぼその周辺情報から判断ができた。ネット上では、この判断が難しく、唯一貴重な判断材料とされるのが、取引相手の名称であり、個人名か組織名かである。しかし、最近のネット売買では、個人でも「インターネットショップ○○」や「□△書房」と名乗ったりし、判別が難しい。特に、消費者契約法、景品表示法では、事業者か否かは「事業」が基準となり、特定商取引法では「営業」が基準となるなど、判断基準が異なっている。氏名又は名称での正確な判断は期し得ないが、ネット上での取引において、現状では、氏名又は名称を判断材料とするしか手がかりはない。

むしろ、匿名のままでもよいので、ある販売者の過去の取引実績又は販売商品数を仲介者又は第三者が把握し、客観的基準によって判断し、これの結果を保証付きで提供してくれると、「販売業者」「事業者」に該当するのか否か、購入者はネット上での当該売買契約の法的な位置づけが明確になり安心して売買できるのではないだろうか。または、販売者が匿名のまま「販売業者」「事業者」であると自ら宣言することも考えられるが、逆に法的要件を満たさない個人が「販売業者」「事業者」と名乗るという問題もあるので、個人を認証し、都合のよい使い分けを防止する仕組みが必要であるかもしれない。EU の「電子商取引に関する指令 2000/31/EC」では、電子商取引としてネット上で商品を販売する際には、販売者は法人登記番号や VAT（付加価値税）の事業者 ID 番号を購入者へ情報提供することが義務づけられており※3、消費者にとってより判断しやすくなっている。

現在、政府部内で検討されている電子登録債権法（仮称）においても、民法等の特則としての第三者保護規定（意思表示に関する第三者保護規定、人的抗弁の切断規定、善意取得の規定）が設けられるなど、取引の安全に配慮された制度設計となっている。しかし、消費者が電子登録債権の利用者となる場合については、消費者を保護するために、これらの民法等の特則としての第三者保護規定が適用されないこととなる※4。そこで、電子登録債権のインフラシステム構築にあたり、取得する利用登録データとして、個人顧客の場合には消費者区分のコードを設け、消費者に該当するか否か明らかにすることが一部で提唱されている※5。この場合には、電子登録債権の登録機関が第三者機関として加わりつつ、

消費者区分の具体的な制度運用が明確にされていくと考えられる。

他方、販売者にとって、購入者がプロ（「事業者」又は「販売業者」）か素人か知っておきたい場合もある。すなわち、購入者がプロの場合には、原則として、消費者契約法、特定商取引法、割賦販売法が適用されないし、販売後の瑕疵担保責任についても責任を有する期間などに相違が生じる。ただし、こちらもやはり名称を判断基準とするしかないが、登記されている法人の行為であっても「商行為」とされない場合もある。正確な判断は難しいが、顕名であれば、ある程度判断できるが、匿名では判断困難である。

「消費者」でない者に、プライバシーの観点から匿名で取引できる仕組みを積極的に構築すべき事情はないであろう。したがって、購入者が匿名を希望している場合であれば、購入者は「消費者」であると仮定して、消費者保護の規定則った十分な対応を講じておけば、後から契約上問題になることは少ないであろう。

※１　逐条解説消費者契約法（経済企画庁国民生活局消費者行政第一課編）　Ｐ４２

※２　日本弁護士連合会　割賦販売法の改正を求める緊急意見書　2003.12.20

http://www.nichibenren.or.jp/ja/opinion/report/2003_70.html

※３　EU 電子商取引指令 2000/31/EC　　第５条　第１項　（ｄ）、（ｇ）

※４　金融審議会金融分科会第二部会、ITWG「電子登録債権法（仮称）の制定に向けて」平成 18 年 12 月 21 日　P7「５（１）消費者による利用」

※５　「電子債権」大垣尚司　著　P201、P264

１－４－３　正確かつ十分な説明

1-4-3-1 消費者契約法

すでに 1-4-1-1 及び 1-4-2-1 で述べたように、商品を陳列して販売する匿名の現実売買は、事業者と消費者の間の契約となるので、消費者契約法第２条において定義される「消費者契約」に該当すると解される。消費者契約法第４条第１項１号の不実告知「重要事項について事実と異なることを告げること」或いは同条第２項の不利益事実の不告知「重要事項等について当該消費者の利益となる旨を告げ、かつ、当該重要事項について当該消費者の不利益となる事実を故意に告げないこと」により、消費者が誤認をし「消費者契約」の申込みまたはその承諾の意思表示をしたときは、これを取り消すことができるとされている。しかし、同条前段では、「事業者が消費者契約の締結について勧誘をするに際し、」と規定し、勧誘という過程に誤認を限定している。当然ながら勧誘のない消費者契約については同条の適用がない※１。確かに、駅の売店のように商品が並べられていて、購入者はそれを選ぶだけで、販売員から働きかけがない場合は、「不実告知」が起きることはない。

なお、「勧誘」の意味を契約締結の意思形成を働きかける行為であると解すれば、販売にあたって主観的な商品の説明書き（例えば「いままでにない画期的な新製品」）を添えることは勧誘に該当するかもしれないが、ただ商品を陳列しているだけでは勧誘に該当しないと解せられる。「特定の者に向けた勧誘方法は「勧誘」に含まれるが、不特定多数向けのもの等客観的にみて特定の消費者に働きかけ、個別の契約締結の意思の形成に直接に影響を与えているとは考えられない場合（例えば、広告、チラシの配布、商品の陳列、、、）は「勧誘」に含まれない。」と「逐条解説消費者契約法」（経済企画庁国民生活局消費者

行政第一課編）では解説しており、不特定多数に働きかけている Web の商品説明は、「勧誘」に該当しないということになってしまう。この逐条解説の解釈には疑問をもつ見解も見られる※2。同条では、「告げること」、「故意に告げないこと」との表現を用いているので、口頭での情報伝達のみを「勧誘」の対象にしているとの解釈が生じているのかもしれない。

「勧誘」とは、不特定多数か否かではなく、文字通り「あることをするように勧めて誘うこと」（大辞泉）であり、単に商品を並べるだけではなく、これは「すぐに効果あり」とか「絶対にお得」のように販売者の主観的な評価を伝達し、契約締結を勧め誘うことと解せられる。したがって、他者が製作した商品の名称とその価格だけであれば、勧誘にはあたらないとも考えられる。消費者契約法第４条第１項（不実告知）、第２項（不利益事項の不告知）も、行き過ぎた主観的評価の伝達とも解せられる。

ネット上の取引では、商品に触れてその扱い易さなどを確認できないので、Web 上の説明を慎重に読み、商品の特性を確認するしかない。Web での商品説明は、「個別の契約締結の意思の形成に直接に影響を与えている」と考えられるので、商品製造者のカタログ的な詳細仕様説明を除き、他はすべてが勧誘に該当すると解されるべきでではないだろうか。

この部分について、同法の適用関係が明確になると、購入者にとって、ネット上での取引において説明とは異なる商品の契約取消を強く主張できるようになるので、多少安心して購入できるのではないだろうか。

また、第８条から第 10 条には、消費者の利益を一方的に害する条項の無効など契約条項に関する規定がおかれている。ネット上では、契約規定や利用規約など何が契約条項に該当するのかリアルの売買ほど明確ではない。「利用上のご注意」などの記述も、その名称を問わずすべて条項に該当するとされれば、購入者にとっては分かりやすく安心してネット上で取引できるかもしれない。

1-4-3-2　特定商取引法

特定商取引法では、第 11 条「一定事項の表示義務」、第 12 条「過大広告等の禁止」、第 13 条「前払い式通信販売における承諾等の通知義務」などが規定されている。

「訪問販売」については、同法第３条において「販売業者又は役務提供事業者は、訪問販売をしようとするときは、その勧誘に先立つて、その相手方に対し、販売業者..の氏名又は名称、売買契約…の締結について勧誘をする目的である旨及び当該勧誘に係る商品….の種類を明らかにしなければならない。」と販売者に対して氏名等の明示を義務づけているが、ネット上の売買が対象となる「通信販売」については、法律上直ちに、氏名等の明示を義務づけていない。しかし、第１１条第１項では、「販売業者…は、通信販売をする場合の指定商品…の販売条件…について広告をするときは、経済産業省令で定めるところにより、当該広告に、当該商品…に関する次の事項を表示しなければならない。」とし、同条同項５号では「前各号に掲げるもののほか、経済産業省令で定める事項」としている。これを受けて、同法施行規則第８条１号では「販売業者…の氏名又は名称、住所及び電話番号」を規定している。したがって、分かりにくいが、販売者は、ネット上で特定商品を通信販売する場合には、その広告にあたって「氏名又は名称」を明らかにしなければならない。「訪問販売」と「通信販売」では「法律事項」と「省令事項」の違いが何故かあるが、「通信販売」たるネット販売において「訪問販売」と同様に匿名での販売は許されな

いということである。

なお、「通信販売業者の「氏名又は名称」と「住所」の表示であるが、氏名については個人の場合、戸籍上の氏名のことである。しかし、戸籍上の氏名よりも芸名やペンネーム等の通称の方が広く一般に認識されているような場合には、これらの通称を表示したからといって、違法とまではいえない。住所については、民法の原則に従って「住所」と解される所番地を表示すべきであり、必ずしも住民基本台帳法による住所と一致するとは限らない。」と「第三版特定商取引法ハンドブック」では解説している。

しかし、経済産業省の通達（2006.1.30）では、「「氏名又は名称」については、個人事業者の場合は戸籍上の氏名又は商業登記簿に記載された商号を、法人にあっては、登記簿上の名称を表示することを要し、通称や屋号、サイト名は認められない。「住所」については、法人にあっては、現に活動している住所（通常は登記簿上の住所と同じと思われる）を、個人事業者にあっては、現に活動している住所をそれぞれ正確に表示する必要がある。」との解説を新たに追加し、「個人事業者の場合は戸籍上の氏名」であることを明確に規定している。

経済産業省内部の通達による解釈であり、そもそも特定商取引法は民事ルールではないので、「戸籍上の氏名」でなかったとしても契約の有効性に影響を与えるものではない。「戸籍上の氏名」以外は認められないとすれば、実名表示以外ありえないこととなるが、本当にすべての「販売業者」に対し実効ある指導を行う用意があるのか本通達だけでは判断できない。

他方、購入者の匿名が問題になるかもしれない条文もある。第１３条の「承諾等の通知義務」については、販売業者…は、指定商品…につき売買契約…の申込みをした者から当該商品の引渡し…に先立つて当該商品…の対価の全部又は一部を受領することとする通信販売をする場合において、郵便等により当該商品…につき売買契約…の申込みを受け、かつ、当該商品…の対価の全部又は一部を受領したときは、遅滞なく、経済産業省令で定めるところにより、その申込みを承諾する旨又は承諾しない旨（その受領前にその申込みを承諾する旨又は承諾しない旨をその申込みをした者に通知している場合には、その旨）その他の経済産業省令で定める事項をその者に書面により通知しなければならない。」とされている。購入者側が匿名（実名を明らかにしない）の場合、名宛人が記載されていない状態で「承諾等の通知」を行うことになるが、このような通知が有効か否か規定上は明確ではない。つまり、実名での名宛てがない通知が効力を持つかということである。誰に通知しているのか客観的に分からない通知は適切に通知をしたことが直ちに明らかではないが、それまで電子メール等で申込などの通信を行っており、承諾通知も同様に到達していると考えられる状況であれば、当該通知は有効と考えるが適当ではないだろうか。

なお、特定商取引法の第 30 条に位置づけられる団体である日本通信販売協会では、「通信販売業における電子商取引のガイドライン」を定めているが、このガイドラインには匿名に関係する規定は見あたらない。

1.4.3.3 景品表示法

すでに 1-4-1-4 で述べたように、ネット上で販売のための商品についての表示を行うにあたっては、景品表示法を遵守しなければならない。同法第４条第１項では、「優良誤認表示」「有利誤認表示」を禁じている。これに反すると、同法第６条の規定の基づき公正取

引委員会の排除命令がなされる。

なお、「消費者向け電子商取引における表示についての景品表示法上の問題点と留意事項」を公表し、スクロールやハイパーリンクにおける見落としがちな重要情報について、留意事項をまとめている。すべてのインターネットでの販売事業者がこれを遵守していることが望ましいことはいうまでもないが、たとえこのガイドラインに反する例があり、重要事項を見落として契約してしまった場合には、このガイドライン違反を理由に直ちに契約無効を主張できるものではなく、一応契約は有効であろう。つまり、景品表示法は特定商取引法と同様に行政による事業者規制法であるので、直ちに実体法上の効力を生ずるものではなく、その違反の有無が個々の売買の権利義務関係に直接影響を及ぼすものではない。

※1　同法第８条から第 10 条の消費者契約の条項の無効に関する規定も、当然ながら、特別な条項を契約の条件としない契約に対しては適用されない。

※2　消費者契約法と情報提供義務　　道垣内弘人　ジュリスト N0.1200　p.50　p.51

１－４－４　形式的証拠力

1-4-4-1　B2C の場合の消費者（購入者）側

ネット上での売買については、現実売買と異なり商品に直接触れられないので、購入者が想定していた商品の内容と配送されてきた実際の商品の内容が相違してしまうリスクが高い。消費者としては、不安である。そこで、売買取引の誘引の過程において事業者がネット上で表示した表品説明などの情報を、自己のパソコンに記録保存しておき、実際の商品がこれに相違していれば、この記録を印刷することによって証拠能力のある文書とすることができると考えられる。「私文書は、本人又は代理人の署名又は押印があるときは、真正に成立したものと推定する」（民訴法第２２８条第４項）とされており、署名又は記名押印があれば、民事訴訟において一般的には形式的証拠力を有することとなる。この場合に、当該情報に事業者の電子署名が付されていれば、「電磁的記録であって情報を表すために作成されたものは、当該電磁的記録に記録された情報について本人による電子署名が行われているときは、真正に成立したものと推定する。」（電子署名認証法第３条第１項）とされている。

実際には、B2C における Web 画面等に電子署名が付されることはあまりないが、SSL により電子証明書が添付され、電子証明書の発行先の URL すなわち実際の通信相手の URL を確認できるサイトは増えている。万一 Web 画面等に作成者の表記がなかったとしても、この URL をもとに電子証明書発行者に照会すれば、Web 画面等を作成した者を特定できる。電子署名認証法に基づくものではないが、このような SSL による通信相手の確認により、その者によって真正に作成されたものと推定される可能性が高まると考えられる。

我が国の民事手続きは、自由心証主義であり、電子署名や電子証明書がなくても、氏名・名称が確認でき、その者が管理するサーバから発信していることが明らかであれば、形式的証拠力が認められるケースが多いと考えられる。

実際問題としては、Web などの説明や電子証明書をどの範囲まで記録保存しておくべきか、判断が難しいかもしれない。商品説明には、写真、型式、スペック、主観的特長点な

ど様々な記載があり、商品説明の画面以外に「利用規約」、「お客様へのお願い」、「注意事項」など様々な関連情報があるので、どこまで記録保存すべきかケースバイケースであろう。また、記録しておく作業自体現在のブラウザではかなり煩わしいものがあり、現在のまちまちな Web 上の表示を考慮すると、高価な商品の購入以外の場合に実行する人は少ないであろう。何をどこまで同意したことになるかなど、ウェッブ上での商品説明・契約条項の標準化とブラウザのキャシュ活用などによる簡易な記録保存手段の開発が求められているのかもしれない。

事業者の承諾通知についても、電子メールなどを保存しておけば、後から真正な文書として認められるケースが多いと考えられる。

なお、ケイタイ端末を利用したネットショッピングでは、Web 画面の記録保存が難しいという問題があるが、米加州の州法では、記録保存が可能であることを電子商取引を行う上での要件にしているようである※1。SD メモリーなどに簡単に記録保存できる機能を持った携帯端末が出現することが望まれる。

1-4-4-2　B2C の場合に事業者（販売者）側

匿名のままの購入申し込みがなされた場合、販売者は当該申込者から申込を否認されるリスクがあることを覚悟しなければならない。氏名・名称が文書上明らかでなくても、その他の周辺事情からある特定の者が電磁的記録を入力・作成したことを示す客観的な状況が存する場合には、形式的証拠力が認められると考えられる。送信元 IP アドレスまたはメールアドレス、受信日時などが記録されていれば、これら情報と日時を手がかりにある特定の者が作成した真正な文書であることを立証しやすくなるかもしれない。ただし、メールアドレスを偽装して、他人のメールに成りすますことを可能とする技術もあるようなので、注意が必要である。また、IP アドレス又はメールアドレスを提供しているプロバイダーには通信の秘密が課されているので、IP アドレス又はメールアドレスを基に相手の住所・氏名などを開示するように請求しても、権利侵害されている事実を十分に説明できないと開示してもらえない。したがって、申込メールを保存しておけば、当事者が申込みを行ったことを証する資料となりうる場合もあろうが、当事者を特定できないリスクも高いと考えられる。

購入者の申込の否認に伴い販売者が損害賠償を請求する場合に、申込という意思表明がなされたことの立証責任は販売者が負担することとなると考えられる。そこで、ネット上では氏名・住所だけでは、正しく記入されているか信用できないので、ある特定の者が電磁的記録を入力・作成したことを示す客観的な状況を立証できるように、クレジットカード番号や電話番号を記入させて、当該個人しか知りえない情報、当該個人と確認できる情報を取得しておくことになってしまう。申込否認が起こる確率とその被害が大きいと予想される場合は、匿名の申込は採用できず、第三者が代わりに購入者とその申込を認証しておいて、トラブルが起きたときにその申込の真正性を証明してくれる方法しかとりえないのかもしれない。

1-4-4-3　C2M2C の場合

消費者同士の売買がお互いに匿名で行われる場合には、債務の一部不履行や契約否認などのトラブルが起こりやすいと考えられる。匿名であって住所・氏名が不詳の場合、販売者と購入者が電子メールで直接やりとりしているときには、電子メールのアドレスを元に、

アドレスを提供しているサービスプロバイダーに相手の住所・氏名などを開示するように請求せざるをえないが、前節で述べたようにプロバイダーが簡単にこれに応じることは考えにくい。この場合には、販売者と購入者の間に仲介者が入り、トラブルが発生したときに取引相手の情報を開示し、それまでの通信がその取引相手によってなされたことを証明する仕組みが必須と考えられる。

※1　カルフォルニア州「電子トランザクション法」1633.8

１－５　その他の顕名化の要請

１－５－１　売買契約書

意思表示の方式として、米国の詐欺防止法（Statute　of　Frauds）が 500 ドル以上の動産の売買契約等について書面を要求している※1。法務省の研究会報告によると、「欧米では、法律上の方式要件が定められていることが多い。これに対し、我が国では、諾成主義が基本であって、実体法上行為の方式として書面の作成が要求される場合は少なく、方式は原則自由とされている」とのことである※2。したがって、現実売買において、売買契約書を取り交わす例は極めて少ない。自動車の所有権移転登録のように第三者（この場合には陸運事務所）にその売買事実を証することが目的あれば、契約の当事者は誰かはっきりさせることが必要となり、当然実名が記入された譲渡証明書を作成しなければならない。一般に有体物（動産）の売買に契約書を作成するか否かは、契約当事者・契約関係者の自由と考えられる。

※1　「アメリカンビジネス法」　西川郁生著　第二章　10

※2　「電子取引法制に関する研究会（実体法小委員会）報告書」法務省　平成 11 年 12 月　第４　１　（１）イから

１－５－２　古物営業法

インターネットオークション運営者は、第 10 条の「古物競りあつせん業者」に該当し、同法第２１条の４の規定により「古物の売買をしようとする者のあっせんを行ったときは、国家公安委員会規則で定めるところにより、書面又は電磁的方法による記録の作成及び保存に努めなければならない。」とされている。したがって、オークション運営者は、出品者名、落札者名、商品、日時等の記録を保存することが努力義務となっている。出品者と落札者の間が匿名であってはならないということではない。

１－５－３　犯罪収益移転防止法案

犯罪による収益の移転防止に関する法律案が、平成１９年２月 13 日に国会に提出された。同法案は、従来の金融機関に加えて、新たにクレジットカード等発行事業者※1や郵便物等の代行受取業者※2に対して、利用者との間で役務提供等の契約を締結する場合には、運転免許証等の提示を受ける方法等により、当該顧客の氏名、住居及び生年月日の確認（本人確認）を義務づける※3ものである。

クレジットカード等発行事業者については、与信行為をすることから、従来から契約時に運転免許証等の写しの送付を求めるなど本人の正確な識別を行っているようである。また、クレジットカード立替代金の収納に銀行口座引落しを利用していることが一般的であるので、金融機関による本人確認済の口座名義人氏名も利用できるので、現在既に実質的に本人確認が行われているということからすると実態的にはそれほど変化はないのではないかと思われる。本法案のクレジットカード等発行事業者の定義に、先払いのビジネスモデルである電子マネー事業者は該当しないが、電子マネーの利用が進み送金額の上限が高額になると電子マネー事業者についても本人確認を義務づけるか否か検討の俎上に上るかもしれない。

また、郵便物等の代行受取業者については、その取り扱う郵便物に、大きさ及び重量が郵便物に類似する貨物を含む※4とされている。郵便法第 15 条第 1 項では、郵便物の大きさは、縦、横及び高さの合計が 90 センチメートルを超えることができず、第一種郵便物の重さは4キログラムが上限と規定している。この基準をそのまま犯罪収益移転防止法案の貨物の基準に準用すると仮定すると、ネットオークションなどで取り扱われているかなり多くの商品が、本法でいう「郵便物（大きさ及び重量が郵便物に類似する貨物を含む）」に該当することとなると解せられる。今後、匿名化のためのコンビニ受取やエスクローサービスなども、サービスを開始するに際しては同法の適用関係について整理を求められることになるかもしれない。

なお、本人確認は、クレジットカード等発行事業者、郵便物等の代行受取業者が、顧客との契約にあたり行うものであり、商品の販売者に対して購入者としての情報を提供しなければならないものではない。事業者のビジネスモデルに依存するが、購入者は販売者に対して匿名性を保持することも認められるものである。

※1　犯罪による収益の移転防止に関する法律　第２条　第２項　３５号
※2　同上　第２条　第２項　３８号
※3　同上　第４条　第１項
※4　同上　第２条　第２項　３８号

2　匿名サービスの可能性についての考察

２－１　B2C（販売事業者→消費者）のケース

２－１－１匿名サービス提供の条件

インターネット上の B2C は、通信販売に該当することから、特定商取引法に規定されている特定商品を販売する場合、特定商取引法が適用される。同法第 11 条第 1 項では、販売業者は、指定商品の販売条件について広告するときは、当該商品に関し、販売価格、代金の支払い時期及び方法、商品の引渡時期、返品制度の有無、販売業者の氏名又は名称など

を表示しなければならない。したがって、同法の販売業者に該当する個人は、匿名では出店できない。

したがって、以下では、購入者側が販売業者に対して匿名のまま購入することが可能な条件について検討してみたい。

購入者にとって、販売者が有名・著名な大手の通信販売業者であれば、プライバシーポリシーから個人情報の利用目的を確認することによって、自分の購買履歴が知らないうちに流通するという不安もある程度解消される。大手では、通信を SSL 化しているところが多く、この場合には、販売業者を認証できるとともに、第三者から通信の内容が盗み見られることはない。セキュリティポリシーなどから顧客情報の管理が厳格な事業者と判断できれば、実名を提供して購入することにほとんど抵抗がない人が多いだろう。

あまり著名でない販売業者であるとか、他人に購入を知られたくない商品などの場合には、匿名での購入のニーズが存在すると考えられる。しかし、商品の配送が必要であり、その部分は、１－３配送の項で紹介した匿名サービスを使わなければならない。

次に、決済のタイミングであるが、代金後払いでは、購入者が匿名であると、商品だけ手に入れて代金の支払いをしない「持ち逃げ」が発生するリスクが高く、販売業者の側が応じえないであろう。他方、代金先払いでは、匿名であると私が払ったと主張しにくく、あまり著名でない販売業者ということになると、代金受取の否認や詐欺が心配になる。信頼できる事業者であることを示す業界のマーク制度※1などがあるが、結局、信頼できない事業者であるので匿名化したい訳であり、代金先払いを匿名で行いたいというニーズは少ないのかもしれない。少額の商品を幅広く販売している実績のある業者であれば、数多くの顧客を失う割には違法な収益が少ないので否認や詐欺を行う誘因が小さく、代金先払いも受け入れられるかもしれない。

購入者が販売者に対して匿名という条件では、配送と決済を同時に行うエスクロー的なサービス事業者が仲介してないかぎり、お互いにリスクの少ない取引を行うことは不可能である。エスクロー（Escrow 条件付第三者預託）とは、取引の履行に際し、当事者間の合意により、当事者が信頼できる第三者を介在させ、この第三者に、当事者の一方が相手方に支払うべき金額や引き渡すべき書類又は物品等を、相手方の契約債務の履行を条件に預託し、第三者が相手方の契約債務の履行確認後に、預託者に支払いまたは引渡を実施することにより、履行上の紛争の発生を予防する法的仕組みである※2。

返品を可能とする場合は、匿名化した配送業者が再度匿名なまま返送してくれないと顕名になってしまう。結局は、次節「２－２　Ｂ２Ｍ２Ｃのケース」のように仲介者が販売者と購入者の間に入らないと購入者が匿名での売買は難しいようである。

※1　（社）日本通信販売協会のオンライン・トラスト・マーク

※2　「電子商取引の法的課題」日弁連法務研究財団編　商事法務　p185

２－１－２　個人情報の保護

通信販売事業者については、経産省のガイドラインが適用されるとともに（社）日本通信販売協会に加盟している事業者については、自主的なガイドラインである「通信販売における個人情報保護ガイドライン」※1の遵守が求められる。なお、この「通信販売

における個人情報保護ガイドライン」では、保有個人データの数は問わない（第３条 14 項）とされており、保有個人データの数が 5000 件以下の個人情報保護法による個人情報取扱事業者に該当しない小規模事業者であっても会員社として、個人情報保護法で定める「第三者提供の制限」や「保有個人データに関する事項の公表等」などとほぼ同様な内容の義務を自主的に負うことになっている。

EU の個人データ保護指令では、第６条第１項 e 号において、「個人データは、収集目的等に照らして必要以上に長く保持されてはならない。」と規定されており、債務の履行が終了し売買が終了し次第、個人情報は消去されるべきであるが、実際にはアフターフォローなどの収集目的もプライバシーポリシーに掲げているので、消去するかしないかは販売業者の裁量に委ねられている。

※１　http://www.jadma.org/01kyokai/05h5-guideline.html

２－２　Ｂ２Ｍ２Ｃ（販売事業者→仲介者→消費者）のケース

２－２－１　匿名サービスの条件

電子モール事業者のサイトは、売買の「場」を提供するが、そこでの取引は、販売業者と購入者が二者間で直接行うものである。トラブルが発生しても、基本的には二者間の問題であり、電子モール事業者は一切「免責」との利用規約を定めていることが多い※１。したがって、売買契約自体は、B2M2C というより、B2C と言える。

しかし、売買の「場」として、様々なプラットフォームを提供している。たとえば決済では、包括代理加盟店契約という形で、電子モール事業者の関係会社・提携会社が、販売業者及び購入者にクレジットカード決済の手段を提供している例もある。販売業者が、アクワイアラと直接加盟店契約を結ばなくても、顧客にクレジットカードによる支払いを可能にできる。ただ、購入者からすると、いったい誰が加盟店であるのか、そこにはどのような個人情報が蓄積されているのか、かなり分かりにくいという課題もある。

電子モール事業者が、提携会社等を通じてエスクローサービスを提供している例もある。イオンクレジットのサービスのようにクレジットカードを利用する場合以外は、金銭の預託が必要になる。電子マネーの項で若干言及したが、一般事業会社の場合には、出資法第２条或いは銀行法第４条（営業の免許）に抵触する可能性が強いので、今後の課題と指摘されている※２。

電子モール事業者などの仲介者が、販売業者と購入者の間に入って、販売業者に対して、購入者を匿名とするプラットフォームサービスはまだ提供されていないようである。

次に、このような匿名化サービスの条件や課題を検討してみたい。

購入者は、まず、電子モール事業者に住所、氏名、決済方法を事前に登録しておく。電子モール上で匿名のまま売買契約が成立すると、電子モール事業者は一回限りの識別 ID を購入者に割り振る。次に、販売業者に当該識別 ID を連絡し、販売業者は当該識別 ID をつけて商品を電子モール事業者にひとまず引き渡す。電子モール事業者は、商品を確認した後、当該識別 ID を送金人欄に記入し販売業者へ払い込むように購入者に指示する。電子モール事業者は、代金が販売業者の口座に支払われたことを販売業者からの通知によって確

認してから、商品についているラベルを当該識別 ID から住所氏名に付け替えて商品を購入者に配送するものである。

電子モール事業者にとっての課題は、販売業者と購入者との間のトラブルに巻き込まれることであろう。

まず、本当に送金されたのかどうか問題になるかもしれない。悪徳販売業者は、実際には送金されていても送金はなかったと否認することが考えられる。購入者は銀行の振込み済証の控えのようなものを電子モール事業者に提示すれば送金したことを証明できるが、今度はその送信控えが偽造したものである可能性が出てくる。一番正確なことは、電子モール事業者が決済を行った金融機関に照会することであろうが、金融機関の守秘義務も関係して、照会回答に対する購入者及び販売業者の同意を求めるなど手続きが煩瑣かつ時間がかかりそうである。一旦、電子モール事業者が代金を代理受領するスキームも考えられるが、出資法や銀行法など法的な整理が必要となってくる。実際のエスクローサービスの場合には、クレジットカードの包括代理店契約によって、提携先である包括代理店を通じて払込の事実を確認することになっているのかもしれない。

配送は、既に述べた匿名の配送サービスが利用できる。

次に、返品条項に基づいて返品するときも問題になるかもしれない。電子モール事業者を通じて、匿名のまま商品を返還しなくてはならず、また、代金を匿名の購入者に送金してもらわなくてはならないが、匿名口座でないと顕名となってしまう。本当に送金されたかどうかという問題もまた発生しそうである。したがって、電子モール事業者が一旦受領し、登録してある購入者の口座に振り込むことになろう。或いは、銀行等の金融機関の守秘義務を一部緩和して、振込み状況を電子モール事業者に連絡可能とすることである。

さらに問題が出てきそうなことは、商品が購入者の予想と異なっていた場合の返品可否やその送料などの負担をめぐって、販売業者と購入者の間でその責任の負担をめぐって食い違いが生じたときである。電子モール事業者は、当事者間の売買であり、当事者間で直接交渉してもらうことになるが、あまり直ぐに顕名にしてしまうのでは、購入者にとって匿名とした意味がない。したがって、ある程度電子モール事業者に匿名のままで、どちらの言い分が正しいのか判断してもらいたいということになりやすい。

上記の問題を解決するためには、電子モール事業者は、共通的な販売ルールを作っておかないと販売業者ごとにまちまちなルールでは対応しきれない。なお課題は多いと考えられるが、事業者間でモデル約款的なものを作成することによって克服できるのではないだろうか。

※1　経済産業省　インターネット商取引とクレジット事業研究会　中間報告書　p15

※2　「電子商取引の法的課題」日弁連法務研究財団編　商事法務　　p194

２－２－２　個人情報の保護

電子モール事業者は、購入者が販売者に対して匿名、顕名の別を問わず、登録している会員（購入者）の購入履歴などの情報を収集している。これらの蓄積情報は、新商品情報のタイムリーな提供などに利用されることが多い。これら電子モール事業者には、「経産産業分野を対象とするガイドライン」が適用される。なお、個人情報保護について、業界

が自主的に定めているガイドラインはないようである。

電子モール事業者は、通信設備（サーバなど）を設置しこれを売買の通信に利用しているので、電気通信事業法の通信設備を他人の用に供する事業に該当する※1。電気通信事業法第 164 条の規定により、同法は原則適用除外となり届出義務などは課されないが、同法第４条の「通信の秘密」は適用されると解釈されている。この場合には、「電気通信事業におけるガイドラインの解説」※2第２条関係（２）にあるように、電気通信事業法上の届出事業者でなくても「電気通信事業におけるガイドライン」※3における電気通信事業者となる。すると、個人情報の保護は厳格となるが、電気通信事業者たる電子モール事業者にとっては、同ガイドライン第４条「電気通信事業者は、電気通信サービスを提供するため必要な場合に限り、個人情報を取得するものとする。」との規定により、個人情報の取得が制約される可能性もある。

米国では、電子モール事業者は、保存通信法によって定義されている遠隔コンピューターサービスに含まれる※4のではないかと考えられる。同法では、遠隔コンピューターサービスを提供している者は、そのサービスを実施する又は保持するための通信の内容をいかなる者に対しても故意に漏らしてはならない※5とされている。

また、ドイツでは、情報通信サービス法が 1997 年に制定され、その定義によると電子モール事業も同法のテレサービスに含まれると考えられ、個人情報保護のために特別な責務が定められている。たとえば、「テレサービス事業者は、技術的に可能かつ妥当な範囲で当該サービスの利用と料金支払を匿名又は仮名で利用者に提供しなければならない」※6とされている。

※1　電気通信事業参入マニュアル追補版　　平 17.8.18　総務省電気通信基盤局データ通信課　　事例（４）「他人の通信を媒介せず、かつ、電気通信回線設備を設置しない場合に該当するため登録及び届出が不要な電気通信事業と解される具体的な事例」
http://www.soumu.go.jp/joho_tsusin/policyreports/japanese/misc/Entry-Manual/TBmanual02/entry02_01.pdf

※2 http://www.soumu.go.jp/joho_tsusin/d_syohi/pdf/051018_2.pdf

※3 http://www.soumu.go.jp/joho_tsusin/d_syohi/pdf/051018_1.pdf

※4　保存通信法§2711（２）では、遠隔コンピューターサービス remote computing service とは、the provision to the public of computer storage or processing services by means of an electronic communications system と定義している。

※5　保存通信法§2702、(a)(2)

※6　Information and Communication Services Act　　Article 2 §（１）

２－３　C2M2C（個人販売者→仲介者→消費者）のケース

２－３－１　匿名サービスの条件

個人にとって、フリーマーケットのように匿名で売ることができることは重要である。この場合には、購入者は、商品の欠陥等（例えば、偽ブランド品）について後から責任等を追及できる機会はないとの認識があり、商品をよく触り、説明をよく聞いて、商品の状態を納得いくまで十分に確認した後に購入するのが通例であろう。お互いに匿名であるので、後から連絡がとれないからである。

現行の大手ネットオークションでは、出品し落札するまでは、出品者も入札者も ID 番号のみのやりとりであり、実名は明らかにされない。しかし、落札されると、出品者も落札者も原則として、実名、住所、電話番号を相互に連絡し合うのが一般的である。

落札後、第三者が間に入らないダイレクトな C2C で売買契約を双方確実に履行するためには、「実名」による電話での連絡によって「確実な連絡先と住所」の確認を勧めているように、顕名とせざるをえないのだろう。さもないと不良品などを売りつけられるリスクが大きすぎて売買取引が成立しないかもしれない。欠陥品等であれば、原則としてオークション運営会社側が用意する「オークション補償制度」によって、ある程度救われることはあるが、匿名化によって欠陥品ばかり出回れば、補償額が嵩んで保険料が高くなってしまい、やはりオークションとして成り立たないだろう。

そこで、第三者たる仲介者が間に入って、一部匿名化のサービスが実現している※１。この場合、C,C 間は匿名であるが、仲介者と C の間はもちろん顕名である。このサービスでは、基本的に出品者、落札者相互間で匿名扱いであり、情報発信機能を使って出品者落札者間のメールのやり取りし、正当な権利の行使のために必要と判断する場合以外は相手の個人情報を開示しないものである。

ここで問題となるのが、仲介者どこまで個人である出品者や落札者の個人情報を正確に把握するかである。当然正確な住所、氏名、電話番号を収集しておかないと、後から債務不履行の問題が生じたときに売買当事者に連絡先を伝えても実際には連絡できないこととなってしまう。そこで、経産省の研究会の報告書にあるようにオークション参加者の本人確認を厳格な実施を義務づけること※２も議論としてはあり得よう。前記１－５－３で述べたように犯罪収益移転防止法で本人確認が法的に義務づけられるのか、或いは、業界内のガイドラインなのか、今後の検討課題であろう。ネットであっても入会に際しては、郵便で公的証明書の写しを送付して確認することになるのかもしれない。写しを送付し保管されるとなるとその写しが漏洩して成りすまされないか不安になる。コピー機を使って偽造することも簡単であり、本人確認の手段としても精度が低いように思える。公的証明書の写しを送付することには成りすまされる不安がある。ある大手事業者は、申請のあった住所に配達記録郵便でパスワードを送付し、これを入力しないと出品できない仕組みとしている※３。しかし、配達記録郵便は、郵便局が配達したことを記録しておくもので、受取人に公的証明書などの提示を求めて受取人を確認する厳格な仕組みではない。

本人確認の成果を活用して不誠実な取引や対応を行った者に関する情報をブラックリスト的に業者間で交換するのであれば、本人に対する説明などさらに慎重な取扱いが求められよう。犯罪防止の観点だけではなく、個人のプライバシー保護の観点も考慮した適正な運用を担保する制度的な枠組みが必要なのかもしれない。

※１　楽天スーパーオークション利用規約 http://www.rakuten.co.jp/auction/doc/rule/

オークション利用規約 http://www.rakutenco.jp/auction/

※２　「新たな形態の通信販売における取引適正化に向けて」平成１７年６月１３日経済産業省　通信販売の新たな課題に関する研究会

※３　同上　参考資料　24 ページ

２－３－２　個人情報の保護

ネットオークション事業者も、通信設備（サーバなど）を設置し、これを売買の通信に利用しているので、電気通信事業法の通信設備を他人の用に供する事業に該当する※1。２－２－２で述べた電子モール事業者と同様に、同法第４条の「通信の秘密」が適用され、「電気通信事業におけるガイドライン」が適用される。

また、ネットオークション事業者も、先の２－２－２で言及した米国の遠隔コンピューターサービスやドイツのテレサービスに該当すると考えられ、個人情報保護に関して特別な責務を負っていると解せられる。

※1　電気通信事業参入マニュアル追補版　　平 17.8.18　総務省電気通信基盤局データ通信課

3　小括

ネットにおける売買に際して、匿名での取引の可能性について論じてみた。

ここでの「匿名」とは、完全な匿名ではなく、購入者と販売者の間のとりあえずの匿名であり、何かトラブルが発生したときには、それぞれの本人情報を保有している第三者が、本人情報を開示するものである。したがって、正確には「半匿名」の制度である。

今後、ネット上での商品売買では、どうしても配送や決済が関係することから、詐欺等を防ぐため、なるべく多くの個人情報を取得し、取引相手の実在性を正確に確認するようになるが、これを逆手にとって、表向きの目的は売買であっても、本当に目的は個人情報の収集である事業者も現れかねない。すなわち、半年以上保有しないうちに、又は 5000 件に達しないうちに、収集した個人情報を本人の同意なしに第三者に広く販売しても、個人情報保護法の個人情報取扱事業者に該当しない以上、個人情報保護法上は違法とは言えない。また、このような情報をマーケッティングのためにこのような脱法的な事業者から購入しても、個人情報保護法第 17 条の「偽りその他不正の手段による個人情報の取得」に該当しない。

このような懸念を考慮すると、少額のネット上での売買は、なるべく「半匿名」を使うべきと考える。「半匿名」の仕組みに挑戦している事業者も現れているが、これまで考察したように制度的な課題も多い。知識が不十分な消費者にも分かりやすい形で自己情報のコントロールが可能となるように、「半匿名」化サービスの制度的な標準化が求められているのではないだろうか。

第二部第四章「匿名化サービスと本人情報の開示請求」

１．はじめに

匿名化サービスが様々な場面で用いられるようになると、逆にサービス利用者の実名など本人情報を取得する必要が生じた場合の処理が問題となる。

既に匿名での活動と本人情報取得の困難性の問題は、取引関係ではオンラインオークションや電子商取引におけるくもがくれ問題として、またいわゆるCGM（Consumer Generated Media）や電子掲示板（ＢＢＳ）サービスなどでは発信者情報開示をめぐる問題として顕在化している。また、ネットワーク関係以外の場面でも、銀行による口座名義人の秘密保護と開示要求のように、同種の問題が既に扱われてきた。

そこで本章では、これらの事例をいくつか取り上げて、匿名化サービスにおける本人情報開示の取扱いについて検討することとしたい。

検討の順序としてまず、本人情報開示が求められる典型的な場合をあげ、そこにおける利害状況を確認する。次いで類似の問題に関する裁判例や法令から解決のための手がかりを得て、最後にネットワーク取引などにおける取扱いを検討する。

２．本人情報開示が求められるモデルケース

(1) 匿名化サービスを用いた物品売買

物品売買における本人情報開示が必要となるケースとしては、両当事者のいずれかに履行障害が生じた場合が考えられる。すなわち、売主側が匿名であると、買主が商品を受領しなかった場合、受領しても注文品と異なっていた場合、品質が劣っていた場合、隠れたる瑕疵[1]や欠陥[2]があった場合、あるいは買主側の意思表示に瑕疵があったり未成年だった場合などにおいて、売主の法的責任を追及するために売主の本人情報開示が必要となる。また買主側でも、代金の全部または一部の不払いという場合に、その法的責任追及が必要となる。

もっとも、匿名化サービスの仕様によっては、これらのいくつかの問題は事前に予防されることだろう。例えば第３章２−２で検討されているＢ２Ｃ取引における仲介サービスにエスクローサービスが組み込まれている場合には、少なくとも商品の受領と代金の支払いについては履行が確保される。決済をクレジットカードや信販を通じて行う場合、あるいは分割払いとする場合、買主の信用リスクが発生するが、これは匿名化サービスの問題ではない。ところが当該商品の注文との同一性や品質、瑕疵・欠陥などの有無についてトラブルが生じることについては、商品の受領までを保証するエスクローサービスによっては予防され得ない。

---

1 民法 570 条

2 製造物責任法２条２項

Ｃ２Ｃ取引においても、状況は原則として同じである。消費者が売主の場合、特定商取引法上の氏名・連絡先表示義務[3]が課せられないため、匿名化サービスを利用しない場合にも氏名不詳のまま取引を行うという問題が、ネットオークションを中心に顕在化している。

以上のような履行障害が生じた場合には、当然のことながら、契約相手方の法的責任を追及する必要に迫られる。従って相手方の住所氏名等が明らかでなければ、本人情報開示を求めることになる。

(2) ネットワークを用いたコミュニケーション

ｉ　掲示板ケース

物品販売以外でも、本人情報開示が問題となる例は多数存在する。ウェブページのホスティングサービスや電子掲示板サービスを代表とするネット上のコミュニケーション仲介サービスにあっては、大部分が本人情報を表示するかしないか利用者の選択に任されている。そして例えば電子掲示板上で他人の権利を侵害するコミュニケーション行為がなされたとすると、その被害者が権利の回復のため、発信者に対する法的手段をとる必要に迫られ、従って本人情報開示を求めることとなる[4]。

こうした通常のウェブページや電子掲示板の他に、ブログと呼ばれる日記風簡易ウェブページには、多数人が書き込める機能があり、さらに書き込みに対してコメントをつけることで一種の掲示板ないし会議室機能を果たすものがある。同じくブログにはトラックバック機能[5]があり、ほかのブログからリンクを設定させることができる。さらにはブックマークを付けて簡単なメモを公表することができるサービスなども、一種のコミュニケーションの場を提供するものと位置づけることができる。

ｉｉ　電子メールケース

プロバイダ責任制限法は、その対象を「特定電気通信」としている。同法２条１号によれば、特定電気通信とは「不特定の者によって受信されることを目的とする電気通信（電気通信事業法 （昭和五十九年法律第八十六号）第二条第一号 に規定する電気通信をいう。以下この号において同じ。）の送信（公衆によって直接受信されることを目的とする電気通信の送信を除く。）をいう」とされている。この定義によれば、特定の者に宛てた電気通信であるところの電子メールは、特定電気通信に該当せず、従って同法４条の定める発信者情報開示請求権は適用がないこととなる。

しかしながら、電子メールであっても発信者の本人情報が受信者に明らかにならないことは起こりうる。また多数人に宛てた同報メールであれば、一対多の通信となるし、メーリングリスト[6]を用いれば、その受信者の数は無制限に広がり、送信者が意図しない相手方

---

3 特定商取引に関する法律施行規則８条１号。
4 特定電気通信役務提供者の責任制限及び発信者情報開示に関する法律（以下、プロバイダ責任制限法という）４条の手続による。この手続については、後述３(3)参照。
5 トラックバックはブログに特有のものではなく、ニュースサイトなどでもおこなわれている。
6 メールサーバがあらかじめ登録したアドレスに一斉に送信する仕組みをいう。この意味ではメールマガジンもメーリングリストの一種ということができる。

に送ることもありうる。メーリングリストの仕様や管理方針によっては、受信希望者自らが送信先を登録することもできる。そして電子メールを送信することで不特定多数人に他人の権利を侵害する情報を発信できることは、ウェブページの場合と全く同様である。

従って、電子メールの場合もウェブページと同様に、本人情報の開示を求める必要がありうるのである。

３．類似ケースにおける本人情報開示の基準

(1) 自治体の保有する前科等のセンシティブな情報

他人の本人情報とは少し異なるが、プライベートな情報について情報保有者による第三者への開示が許されるかどうか争われ、最高裁の判断[7]が示された事件として、いわゆる前科照会事件が挙げられる。

まず事実関係だが、Ａ社のタクシー乗務員であったＸは、Ａ社から解雇されたので、Ａ社に従業員たる地位の確認を求める仮処分を申請していた。Ａ社の弁護士Ｂは、Ｘの前科・犯罪経歴について、京都弁護士会を通じてＹ市に照会した。その際照会の目的には「中央労働委員会、京都地方裁判所に提出するため」と記載されてあった。Ｙ市は、これに応じてＸの前科前歴を報告した。それによれば、Ｘには道交法違反 11 犯、業務上過失傷害１犯、暴行１犯の前科があったため、Ｂを通じてこの前科記録を知ったＡ社がこれを公表し、経歴詐称を理由に予備的解雇を通告した。

ＸはＹ市に対して、プライバシー侵害を理由とする国家賠償および謝罪広告の掲載を求めて本訴を提起した。

最高裁は多数意見が原判決を支持して上告を棄却し、伊藤正巳裁判官がこれに補足意見を付している。また環昌一裁判官は反対意見を付している。多数意見は次の通りである。

「前科及び犯罪経歴（以下「前科等」という。）は人の名誉、信用に直接にかかわる事項であり、前科等のある者もこれをみだりに公開されないという法律上の保護に値する利益を有するのであって、市区町村長が、本来選挙資格の調査のために作成保管する犯罪人名簿に記載されている前科等をみだりに漏えいしてはならないことはいうまでもないところである。前科等の有無が訴訟等の重要な争点となっていて、市区町村長に照会して報告を得るのでなければ他に立証方法がないような場合には、裁判所から前科等の照会を受けた市区町村長は、これに応じて前科等につき報告をすることができるのであり、同様な場合に弁護士法23条の2に基づく照会に応じて報告することも許されないわけのものではないが、その取扱いには格別の慎重さが要求されるものといわなければならない。本件において、原審の適法に確定したところによれば、京都弁護士会が訴外Ｂ弁護士の申し出により京都市伏見区役所に照会し、同市中京区長に回付されたＸの前科等の照会文書には、照会を必要とする事由としては、右照会文書に添付されていたＢ弁護士の照会申出書に『中央労働委員会、京都地方裁判所に提出するため』とあったにすぎないというのであり、この

[7] 最判昭和 56 年４月 14 日民集 35 巻３号 620 頁

ような場合に、市区町村長が漫然と弁護士会の照会に応じ、犯罪の種類、軽重を問わず、前科等のすべてを報告することは、公権力の違法な行使にあたると解するのが相当である。」

この判決で問題となった弁護士法 23 条の２に規定された弁護士会照会は､弁護士が受任した訴訟事件および委託を受けて示談交渉、契約締結、法律相談、鑑定等を行う事件について、訴訟資料等の収集、事実の調査等、職務活動の円滑な遂行と適正な解決を図るために、弁護士会に特に認められた権限である。事件処理にあたる弁護士は、所属弁護士会に照会の申出をすると、各単位弁護士会がその適否を審査した上で、照会を行うこととなっている。

照会の対象は、受任事件の処理に必要な事実の有無に関してであり、意見や判断、鑑定などを求めることはできない。照会の相手方は公私の団体、公務所であり、個人に対しては照会できないが、私企業は公私の団体に含まれる。

報告拒絶に対する制裁は、法文上規定されていないが、照会の相手方には報告義務があるとする見解が一般的である[8]。そして本件の原審判決は、報告義務を前提にしつつ、本件のような前科の照会に対しては報告を拒否すべき場合に当たるとの判断を示した。これに対して最高裁は、報告義務の有無には触れていない。

本判決多数意見は、照会事項の前科等が重要な争点であって代替の立証方法もないような場合には報告できるが、そのような理由が書かれていない本件では報告をしたことを違法と評価した。伊藤正巳裁判官の補足意見も、個人のプライバシーとして最も知られたなくない情報の一つである前科について､「完全に秘匿されるものではなく､それを公開する必要の生ずることもありうるが、公開が許されるためには、裁判のために公開される場合であつても、その公開が公正な裁判の実現のために必須のものであり、他に代わるべき立証手段がないときなどのように、プライバシーに優越する利益が存在するのでなければならず、その場合でも必要最小限の範囲に限つて公開しうるにとどまるのである」とし、本件区長の報告を過失ありとした。

こうした判示に従えば、プライバシーとして特に秘匿すべきセンシティブな情報を照会する場合は、受任した事件との関係で照会事項の争点可能性や不代替性を具体的に記載して、相手方に開示を求めることとなる[9]。また照会相手方も、これらの点を実質的に判断して、当該情報が訴訟審理にどうしても必要な場合には、プライバシー保護の要請が後退するので報告しなければならないと解される。

この考え方は本稿が問題とする本人情報の開示の局面でも、程度の差こそあれ、一応妥当する。すなわちプライバシーとしての秘匿の必要性は前科情報より本人情報の方が低いというべきではあるが、一応はプライバシーとして保護されるべき情報であり、本人情報と結びついた行動記録の内容によってはセンシティブな情報となりうることもあり得る[10]。そして本人情報開示の必要性と不開示の必要性とは対立する利益であり、情報保有者が開

---

8 『条解弁護士法』165 頁（弘文堂・1993)、岐阜地判昭和 46 年 12 月 20 日判時 664 号 75 頁。

9東京弁護士会総務委員会編『弁護士会照会制度』（商事法務研究会）15 頁参照

10 例えばエイズ検査受診の事実と本人情報とが結びついたときには､場合により極めてセンシティブな情報となりうるであろう。

示の判断を適切にしなければならない立場に置かれている。

この情報保有者が開示の必要性とプライバシー保護とのバランスを評価すべき立場に置かれるのは、それが本判決のように適切でない判断をすれば損害賠償責任も負担しなければならない以上、適当ではない。疑わしい場合は常に報告拒絶といった消極的な対応に陥るおそれもあり、このことはプライバシーなどの保護という観点からは望ましいことだが、訴訟における情報流通にとっては阻害要因である。

弁護士会照会の場合、弁護士会が紹介するかどうかの判断をすることになるので、秘密保護の要請と訴訟における当該情報の必要性とを比較考量し、当該情報の報告が必要であるとの判断に達した場合には、照会相手方はこれに従って報告しても民事刑事の責任を追及されないものとし、報告によりプライバシー侵害を被った者は、照会申し出をした弁護士および照会を適当と判断した弁護士会を相手方として、その責任を追及するスキームが考えられる[11]。

要するにここでは、開示の必要性とプライバシーとが対立利益になり、情報保有者にとってジレンマが生じることと、開示請求者と情報主体以外の第三者による判断が介在することがその解決の糸口となりうることを確認しておこう。

(2) 銀行口座の名義人情報

金融機関は、その顧客に対して守秘義務を負っている。この守秘義務は、必ずしもその法的根拠がはっきりしないが、顧客に対する契約上の付随義務、あるいは公法上の義務、もしくはその両方から基礎づけられる。

本稿の問題関心から直接問題となるのは、銀行口座の名義人について、氏名や住所などの本人情報を第三者から開示せよと求められた場合に、これを秘匿すべきか開示すべきかという局面である。具体的には、詐欺行為の被害者が、詐欺行為者の指定する銀行口座に金員を振り込んだとして、後にその取り戻しのため銀行口座名義人の本人情報を銀行に照会するという例が考えられる。

この場合に情報を請求する者は、なんら契約関係のない銀行に対して情報開示を求める実体法上の権利を有するわけではない。そこで、銀行に対する情報開示は、一般私人であれば弁護士に事件を依頼した上で、弁護士法上の照会を受任弁護士を通じて求めることが考えられる。そして法的な紛争としては、この照会に対して銀行が回答を拒否した場合に、その拒否が違法であって照会者側に不法行為責任が生じるかどうかという形を取る[12]。

---

11 日弁連も、報告拒絶となった後に弁護士会の審査請求に基づいて、日弁連が報告すべき場合かどうかの判断を行い、報告すべき場合にはその旨の勧告を日弁連として行う制度を提案している。2002 年 11 月 22 日付け「司法制度改革における証拠収集手続の拡充のための弁護士法第 23 条の 2 の改正に関する意見書」

12 なお、銀行の顧客情報の問題以前に、そもそも弁護士会照会に対して被紹介者が報告義務を負うことについては、これを認めるのが通説とされており、また裁判例でも誤った情報を報告したケースや報告を拒絶したケースにおいて損害賠償責任を認めた事例が存在する。前者は大阪地判平成 5 年 10 月 29 日判時 1499 号 92 頁、後者は京都地判平成 19 年 1 月 24 日判タ 1238 号 325 頁である。

この点について下級審裁判所ではあるが、以下のような裁判例[13]がある。

事案は二つの事件が併合されているもので、第一事件は、Ｘ１がＡ弁護士会所属弁護士Ｂに破産免責の申立てを依頼し、Ｂ弁護士がＸ１の債権者であるＣの預金口座について、Ｃの氏名と住所をＹ１銀行に弁護士会照会したところ、Ｙ１はＣの承諾が得られなかったとして一旦回答を拒絶し、Ａ弁護士会が再度の照会依頼書面を送付したことでＣの氏名住所を回答したというものである。また第二事件はＸ２株式会社がＡ弁護士会所属のＤ弁護士に債務整理を委任し、Ｄ弁護士はＡ弁護士会を通じてＸ２の小切手振り出し先であるＥの氏名住所をまず電話会社に照会し、その回答から判明した電話契約者Ｇを相手方として、Ｘ２が降り出した小切手を持ち込んだＨの氏名住所の照会をＹ２銀行に対して求めた。ところがＹ２銀行はこの回答を拒絶し、またＨに対する債務不存在確認請求訴訟における裁判所の調査嘱託に対しても回答しなかった。

そこで、Ｘ１がＹ１銀行に対して弁護士会照会に対する回答拒絶により被った損害の賠償を求め、Ｘ２がＹ２に対して弁護士会照会回答拒絶および調査嘱託に対する回答拒絶を不法行為とする損害賠償を求め、それぞれ提訴した。

第１審裁判所は、いわゆる 23 条照会に対して被紹介者には報告義務があるとし、また調査嘱託に対しても報告義務があるとしたが、銀行その他の金融機関が顧客の氏名や住所など顧客の特定に資する情報の開示を求められた場合には、それらが営業秘密に該当するものであって、その報告義務を原則として免れるものとした。その上で、いかなる場合に報告義務を免れるかについて、プロバイダ責任制限法における発信者情報開示請求権の要件を参考にして、①当該顧客の行為により本人情報開示請求者の権利ないし法的利益が侵害されていることが明らかであるとみえること、②当該情報が開示請求者の権利ないし法的利益の裁判制度による回復を求めるのに必要であること、その他これに準ずる正当な利益があること、③開示以外に適当な方法がないこと、これらの要件が満たされたときは銀行も報告義務を負うが、本件では銀行側に過失がないとして請求を棄却した。

これに対して控訴審裁判所は、弁護士会照会についても調査嘱託に対しても銀行側が法的な報告義務を負うとしつつ、この報告義務は公的な義務であって照会する弁護士や依頼人との関係での私的な義務ではないとする。従って本件いずれの事件でも報告義務を怠ったことがＸ１Ｘ２の権利ないし法律上保護される利益を侵害するものとは言えないとして、請求棄却の原判決を支持した。

銀行が顧客の情報について守秘義務を負うとしても、一定の場合にはその顧客情報を他者に開示する場合があり得る。代表的なケースとして銀行間のいわゆる信用照会[14]があげられる。従って銀行の顧客情報に対する守秘義務も絶対的なものではなく、特に顧客の特定に資する情報については、それが明らかにされないとその者に対する法的紛争を裁判で解決することができなくなる一方、取引履歴などのセンシティブな顧客の秘密よりは顧客の特定に資する情報の方が要保護性が低いともいえる。

---

13 大阪高判平成 19 年１月 30 日判時 1962 号 78 頁、その原判決として大阪地判平成 18 年２月 22 日判時 1962 号 85 頁。

14 信用照会に対する回答が不正確であった場合に、その回答により損害を被った者に対して回答銀行が損害賠償責任を負うかどうかが争われた事例として、大阪地判平成４年６月 25 日金法 1357 号 62 頁その他がある。

また上記の第一審裁判所はプロバイダ責任制限法４条の発信者情報開示請求権をモデルとして要件を定立するが、本来は局外者である情報保有者が発信者と情報開示請求者との間の紛争について、実体的な判断を求めることは適切ではない。顧客情報の開示の必要性は、開示請求者の権利利益が侵害されていることに基づいているのではなく、開示請求者と顧客との間に紛争が現存し、法的手段を用いて解決する必要があることに基づいているのである。

そのように考えると、上記第一審裁判所が示した要件を修正して、①顧客と開示請求者との間で、法的紛争が存在することが明らかであるとみえること、②当該情報が開示請求者と顧客との紛争の裁判制度による解決を求めるのに必要であること、その他これに準ずる正当な利益があること、③開示以外に適当な方法がないことの三つを要件として、顧客情報の開示を求める法的利益を承認すべきである。

(3)プロバイダ責任制限法の解決

既に指摘したように、プロバイダ責任制限法４条は、以下のように定めて発信者情報開示請求権を創設した。

「特定電気通信による情報の流通によって自己の権利を侵害されたとする者は、次の各号のいずれにも該当するときに限り、当該特定電気通信の用に供される特定電気通信設備を用いる特定電気通信役務提供者（以下「開示関係役務提供者」という。）に対し、当該開示関係役務提供者が保有する当該権利の侵害に係る発信者情報（氏名、住所その他の侵害情報の発信者の特定に資する情報であって総務省令で定めるものをいう。以下同じ。）の開示を請求することができる。

一　侵害情報の流通によって当該開示の請求をする者の権利が侵害されたことが明らかであるとき。

二　当該発信者情報が当該開示の請求をする者の損害賠償請求権の行使のために必要である場合その他発信者情報の開示を受けるべき正当な理由があるとき。

２ 開示関係役務提供者は、前項の規定による開示の請求を受けたときは、開示するかどうかについて当該発信者の意見を聴かなければならない。ただし、当該開示の請求に係る侵害情報の発信者と連絡することができない場合その他特別の事情がある場合は、この限りでない。

３ 第一項の規定により発信者情報の開示を受けた者は、当該発信者情報をみだりに用いて、不当に当該発信者の名誉又は生活の平穏を害する行為をしてはならない。

４ 開示関係役務提供者は、第一項の規定による開示の請求に応じないことにより当該開示の請求をした者に生じた損害については、故意又は重大な過失がある場合でなければ、賠償の責めに任じない。」

この規定をめぐっては、既に多くの裁判例が蓄積されているが、その主たる問題となってきたのは、アクセスプロバイダが開示関係役務提供者に該当するかどうか、またそれと裏腹の関係にあるが、Ｐ２Ｐの通信が特定電気通信に該当するかという点であった。

これらの論点はプロバイダ責任制限法自体の構造に関わる問題で、本稿が対象としている匿名化サービスと本人情報開示の条件に関するものではない。本稿の関心からすれば、

プロバイダ責任制限法４条の開示の実質的要件とその手続が重要である。つまり、同条 1 項各号は実質的要件として「権利侵害の明白性」と「開示の正当理由」とを要求しており、この二つが発信者の通信の秘密ないしプライバシーを犠牲にすることを正当化する核心である。

また手続面では、開示要求を受けたプロバイダが発信者の意見を聴かなければならないとされている点が注目される。発信者が開示に同意すれば、1 項の要件が満たされていなくとも、あるいは満たされているかどうか判別できなくとも、プロバイダは発信者情報を開示することができる。これに対して発信者が開示に同意しなければ、１項の要件が満たされている場合で、しかもプロバイダが要件充足を判断できる場合に限って発信者情報を開示することが許される。このように意見聴取のプロセスは、開示要件の充足を必要とするかしないかの分岐点となる。また意見聴取により発信者はトラブルの存在を知り、これに対処する機会を与えられることになり、いわば手続保障として重要な意義を有する。ただし、これは同時に、発信者に証拠隠滅や雲隠れの機会を与えることにもなるという点も注意すべきである。

(4) 情報公開請求における氏名秘匿

次に行政庁に対する情報公開請求においても、関係者の氏名がしばしば非公開とされて問題となる。

行政機関の保有する情報の公開に関する法律[15]第 5 条に開示請求権の除外事由（不開示情報）がまとめられている。本稿の関心から注目されるのは、そのうち個人情報および法人・個人事業者の情報についての開示要件・不開示情報である。

「一、個人情報。ただし以下の情報は開示される。

イ　法令、慣行により公開予定の情報

ロ　人の生命財産等の保護に公開が必要な情報

ハ　当該情報が公務員等の職及び職務遂行の内容に係る部分

二　法人等や個人事業に関する情報であって、次に掲げるものは不開示。

ただし人の生命財産等の保護に公開が必要な場合は除く。

イ　法人等や個人事業者の権利利益を害するおそれがあるもの

ロ　非公開条件で任意提供された情報で、通例として非公開のものや非公開が合理的であると認められるもの」

また、開示される行政文書に第三者の情報が含まれている場合には、その者に意見提出の機会を与えることができ、また第 5 条第 1 号ロまたは同第 2 号但書もしくは第 7 条の公益上の理由による裁量に基づいて開示する場合には、意見提出の機会を与えなければならないとしている（情報公開法第 13 条）。

これらの規定をめぐっては、また地方自治体の各種情報公開条例についても、数多くの訴訟が提起され、開示・非開示の基準が裁判所により判断されている。ここでその詳細に立ち入ることはできないが、少なくとも情報公開法自体の規定ぶりからしても、以下の二

15 以下、情報公開法という。

点が注目できる。まず実質的要件としては、個人を識別できる情報の開示については個人と法人との区別および個人でも事業者かどうかにより原則非公開か原則公開かが分かれ、いずれの場合も特に生命財産等の保護に公開が必要な情報は開示されるとの例外を伴っている。手続的には、特に第三者の情報が含まれる場合の意見提出の手続保障が注目される。

(5) メディアによる取材源の秘匿と証言拒絶権

本人情報開示・非開示は、報道機関などのメディアによる取材源の秘匿という形でもしばしば問題となる。その中でも特に、裁判における取材源の秘匿が証言拒絶権や、証言拒絶事由に基づく文書提出拒絶事由に該当するかどうかが争われている。

民事訴訟法は、取材源の秘匿を証言拒絶権に列挙していないが、第 197 条 3 号に規定された「職業の秘密」に該当するかどうかが問題となる。また文書提出義務の除外規定である第 220 条 4 号ハにおいて第 197 条所定の証言拒絶事由が準用されているので、そこでも問題となる。

この点について最高裁は、「１　民事事件において証人となった報道関係者が民訴法 197 条１項３号に基づいて取材源に係る証言を拒絶することができるかどうかは、当該報道の内容、性質、その持つ社会的な意義・価値、当該取材の態様、将来における同種の取材活動が妨げられることによって生ずる不利益の内容、程度等と、当該民事事件の内容、性質、その持つ社会的な意義・価値、当該民事事件において当該証言を必要とする程度、代替証拠の有無等の諸事情を比較衡量して決すべきである。

２　民事事件において証人となった報道関係者は、当該報道が公共の利益に関するものであって、その取材の手段、方法が一般の刑罰法令に触れるとか、取材源となった者が取材源の秘密の開示を承諾しているなどの事情がなく、しかも、当該民事事件が社会的意義や影響のある重大な民事事件であるため、当該取材源の秘密の社会的価値を考慮してもなお公正な裁判を実現すべき必要性が高く、そのために当該証言を得ることが必要不可欠であるといった事情が認められない場合には、民訴法 197 条１項３号に基づき、原則として、当該取材源に係る証言を拒絶することができる。」と判示し、当該事件における取材源の秘匿を証言拒絶権の対象と認めた[16]。

ここでのポイントは、取材源となった人の本人情報を保護すべき利益と、それが裁判における真実発見などのための必要性と利益衡量により決せられるという点にある。

４．匿名化サービスにおける本人情報開示の基準

(1) 開示の実質的要件

３．で検討したように、非公開の本人情報を開示する場合の実体要件や手続要件は、開示を求める局面に応じて様々である。

まず実質的な要件では、開示対象となる情報の性質、秘匿の必要性、開示により生じる

16 最三決平成 18 年 10 月 3 日民集 60 巻 8 号 2647 頁。

情報主体や情報保有者に対する不利益の大小などが勘案される。また、情報開示を求める者の利益や公的な利益が考慮対象となる。

匿名化サービスにおける本人情報の開示にこれを当てはめてみるならば、開示対象となる情報の性質は本人を特定する氏名住所、取引履歴などである。氏名住所についてはセンシティブな情報とは言えないが、個人情報保護法 3 条において「個人情報は、個人の人格尊重の理念の下に慎重に取り扱われるべきものである」と規定されているように、みだりに開示されるべきものではない。またプライバシー保護という観点からも、氏名住所といった情報であっても保護の対象となりうる。さらに取引履歴は、その取引内容によってはセンシティブな情報となりうるものであり、思想良心の自由（憲法 19 条）との関係でも、より一層保護される必要のある情報である。

匿名化サービス提供者にとっても、取引相手の住所氏名がみだりに公開されては、サービスを利用する事業者の顧客リストの公開という意味も持つので、営業秘密としての保護が必要となるところである。

ただし、前科情報のように高度にセンシティブな情報というわけではない。また取材源の秘匿についてみられるような、情報保有者の職業が成り立っていくために不可欠な秘匿特権との位置づけも困難であろう。

他方、開示請求者の利益は、開示請求者と情報主体との取引関係に起因する法的トラブルの解決の必要性により基礎づけられる。この利益は開示請求者にとっての利益である以上に、法的責任追及が可能となる社会的基盤でもある。そこでは紛争解決の必要性の程度により、その利益保護の必要性が基礎づけられる。この場合に、プロバイダ責任制限法のように権利侵害の明白性までも要求するのか、それとも解決すべき法的トラブルの存在で足りるとするかは、選択の余地のある点である。しかし開示を求められている情報それ自体は必ずしもセンシティブな情報ではなく、また少なくとも取引関係において用いられる匿名化サービスを前提にするなら、取引においてなんらかの履行障害が生じて、その責任の有無を法的に確定する必要があるということさえ明らかであれば、それ以上に情報主体に法的責任があることまで明らかとなっている必要はない。その点はむしろ情報開示の上で行われる法的紛争処理過程において、確定されるべきことだからである。

(2) 情報の保全

情報開示の前提として、本人情報や取引履歴などの情報そのものが保持されている必要がある。プロバイダの発信者情報開示の局面ではログ保存義務に関する問題であるが、匿名化サービス提供者はトレーサビリティを確保しておくべき責務がある。

このことは、少なくとも取引関係では匿名化サービス提供者とその利用者との間の契約上の信義則に基礎づけられて、法的義務ともいうべきであろう。

(3) 手続的要件

最後に、手続的には、本人情報開示に先立って、情報主体への通知を必要とするかどうかが問題となる。もっとも、匿名化サービスの利用者は、履行障害が生じた場合に法的な

紛争処理手続に進まざるを得ないことは当然であり、この点で自己の本人情報開示に同意するかどうかを選択できる立場にはない。また通知を要求することにより、証拠や財産の散逸・隠匿といった機会を与えることになることも、考慮すべきであろう。

他方で、本人情報を開示されない利益は尊重に値するので、その意味で同意の有無が重要なポイントとなることは確かである。また匿名化サービス提供者としても、自らの顧客である情報主体が同意するのであれば開示を妨げないが、同意しなければ難しい判断を迫られるという立場にある。従って、開示を求められた提供者が情報主体の同意を事前に求めることは否定できない。

第三部「匿名性の技術・法と社会」

1 匿名性の概念

1.1. 序

RSA コンフェレンス 2005 におけるリチコードクラーク氏の基調講演は、"Who are you?" "What is most you want to protect?"という二つのフレーズをキーとして、ネットワーク社会において、人々は、ID とパスワードという単なる文字列につなげられていることと、それによるアイデンティティの脆弱性が引き起こすセキュリティの問題を概観するものであった[1]。この基調講演からも明らかなとおり、人々は、ネットワークで、そのような文字列に関連づけられている一つの地位(アカウント)として活動する。これに関連して、現実社会との関連性が希薄になってしまう。その結果として、ネットワークは、匿名性を有するといわれることがある。

しかしながら、この「匿名性」という用語は、論者のなかで、自己のイメージのままに使われ、それゆえに議論が混乱することも多い。そこで、この「匿名性」という概念を整理して、議論の前提として、それをもとに法律と匿名性がどのように関わってくるのか、ということをおおざっぱにみるのが重要になる。

1.2. 匿名性の定義

匿名性を議論するにあたっては、それをどのように定義するかという問題がある。
まず、芸能人なり通称をもちいて、現実社会で、発言している場合を考えてみる。この場合、その人の名称は、本名とはイコールではない。しかしながら、これを匿名性があるということはないであろう。しかしながら、これよりさきの部分には、二つの側面があるということができる。ネットワークの活動に置き換えたときには、一定のハンドルを(常に)用いて発言をしている場合に、実名での表現を強制されないということがあり、これが匿名性の問題といわれることがある。この観点はさらに、仮名を使うことができるか、という点と、まったく名前を利用しないことができるかという点の二つの面で議論される。これらの意味で議論される匿名性の問題は、匿名（anonymity）での発言や行動の許容性という問題である。

しかしながら、匿名性と言われる場合には、いま一つ、現実社会から、行為者は誰かという観点から、だれが行為者であるか追求することの困難性が高い場合のこともある。これは､現実社会からその行為者にどれだけリンクもしくは追跡できるかという問題であり、匿名性(unlinkable)の問題(もしくは､追跡可能性の問題)ということができる[2]であろう。

---

[1] http://www.itmedia.co.jp/enterprise/articles/0505/12/news116.html

[2] 例えば、国分明男「インターネットにおける違法・有害情報対策の現状と課題－中間取りまとめに関する公開ヒアリング－」(http://www.soumu.go.jp/joho_tsusin/policyreports/chousa/tsushin_houseikikaku/pdf/070919_1_si2.pdf)は、匿名性の制限問題として、「匿名だがプロバイダは知っている」という状況を示唆する。

この文脈での議論は、現実社会においても、夜中に、見つからないように変装して、新聞などの切り貼りで名誉毀損の文書を配って歩くといという行為について考えることができる。この場合には、その行為者にたどり着くまでの証拠が得にくいということであり、匿名の影に隠れた行為ということになる。この観点からは、「匿名性」という概念は、有体物としての行為者(かならずしも本名ではない)との関連性の強さをさしていっている。なにか問題がおきれば、その行為者を特定して、裁判その他の方法で、社会的に対応すれば、たりることになる。その場合には、特定ができれば、実名は、重要ではない。そして、しかも、それは、関連性の問題なので、「ある」、「なし」では無くて、程度問題である。

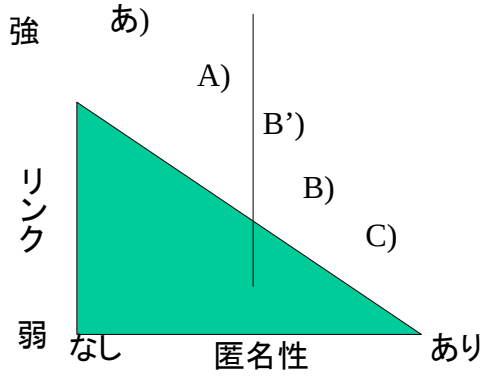
リアルワールドでも、筆跡を変える、変装する、名前を記さないということで、行為者との関連性をきわめて薄くすることができるのであり、リアルワールドは、匿名性がない、それに対して、ネットワークでは、匿名性があるという表現は、あまり妥当ではないものと考えられる。

そして、これを逆の点からいうと、匿名性に関する問題は、特定しようとする人間の特定までのコストの大小であると考えることができよう。

これらの観点を示したのが、以下のシートである。

匿名性って何？

- 程度問題か



- 本人(有体物)とのリンクの強さ/本人特定のためのコスト
  - あ)通称で発言
  - A)匿名で中傷ビラ
  - B)パソコン通信での名誉毀損発言
  - C)ネットカフェから名誉毀損発言

本人とのリンクが強いということは、逆に特定に際してのコストが少なくて済むことを物語っている。

匿名でのビラ配り(上記の例)と、ID と入会時の会員の特定がしっかりしているプロバイダでの特定のコストが社会的に、どちらが大きいかというと、なんともいえないところであろう。

しかし、ネットワークでも、これは、また、アカウントと本人とのリンクの強弱によって、いろいろの段階があるのである。上述のパソコン通信の場合と正反対に、だれでもつかえるようなネットカフェなどで、ネットにかきこむような場合に、きわめて本人とのリンクが弱くなるということができるであろう。また、種々の技術的な要素を利用するのも同様である。

このような考察のもとで、特定しようとする人間と現実の世界との関連する事実を把握するためのコストが、社会通念上、合理的なレベルを超えるとき、人は、これを「匿名性」がある（unlinkable）と認識すると定義することができるものと思われる。

1.3. 匿名性の概念と技術の位置づけ

匿名性の概念と技術の関連性を検討するときに、上述の二つの側面から、現在の問題意識を位置づけることは意義のあることと思われる。

まず、匿名（anonymity）の観点からするときに、実名やそれに関連する種々の情報については、そのような情報を悪用して、経済的利益等を得ようとする犯罪等が多々見受けられるのであり、その意味で、実名等の情報を受領しうる人間をきわめて限定した上で、実名等の情報を保護しつつ、ネットワーク上の活動をなしうるようにすべきという要請が強くなるということになる。

それに対して、「匿名性」（unlinkable）の観点からするとき、ネットワークにおける社会安全等の要請とのバランスの問題がでてくることになる。ネットワークの安全性に対する脅威を、「匿名性」（unlinkable）を悪用して、行うものがいる場合に、政府等は、法執行の要請から、そのような行為者を特定して、法を執行しなければならない。そのために著しく、行為者へのリンクを不可能にする技術的・社会的システムについては、一定の法的な対応が要請されることになるのである。

2 匿名性の背景にある技術と現状

2.1. 序

上記のように匿名性を把握するとき、インターネットにおける通信の性質が、使用時にプロバイダから、アドレスを指定されるという形でなされることも多く、それゆえに特定すべき人間と現実の世界との関連する事実を把握させるのを困難にさせる要素を含んでいるということができる。その上に、匿名性を確保する技術が進化していることに注目がなされるべきである。これにたいして、主として情報セキュリティの関心から、この匿名性を確保しようという技術にたいしてネットワーク上の発信者を突き止めるのを容易にしようという動きが認められる。

2.2. 匿名性を高める技術

2.2.1 匿名プロキシ

匿名プロキシ・匿名串（串はプロクシの俗称）（Open Proxy）とは、利用者の IP,ホスト名を含む環境変数をサーバ側に通知しないプロキシを意味する。本来は、発信者の情報が盗まれることを防止したり、通信の自由の無い国からの安全なアクセスを保証したりするため設置されているが、荒らしやクラッキングを企図する者が身元追跡をかわすために使用することも多い。

2.2.2　匿名認証技術

IIP（Invisible IRC Project）とは、IRC クライアントを使用し匿名でチャットができるプロキシソフトである。

Tor（トーア、The Onion Router）は匿名接続を実現するためのソフトウエア、規格の一つである。 SOCKS プロキシとして動作し、Windows および Mac OS X や Linux 等の各種 Unix ライク OS で動作する。

2.2.3　Winny

また、コンテンツ関係で、いわゆる P2P ソフトウエアのなかで、格別に匿名性を高める手段を実装しているソフトウエアが存在している。この代表例としては、Winny をあげることができる。ソフトウエアとしての Winny は、「匿名性」「共有効率の高さ」を目的として Windows ネイティブプログラムとして開発された P2P ソフトウエアである。中央サーバの存在を必要としない、いわゆるピュア P2P 型のソフトウエアであり「プロキシ技術」を「匿名機構」「キャッシュ機構」として活用することにより、匿名性・効率的なファイル共有を図ろうとしたものである。一般に Winny ネットワークにおいては、匿名性があり、情報の第一発信者がわからないとされている。Winny においては、あるファイルがアップロードされるとそのファイルの位置情報等が要約されたキーが作成され、これがインターネット上の一定の範囲内にある他のパソコンに拡散し、そのファイルをダウンロードしたい他の Winny 利用者は、ファイル検索によってそのキーから当該ファイルの位置情報を取得し、この情報に基づいてファイルの送受信がなされる。また、このキーは一定の割合で書き換えがなされ、書き換えられたキーをもとにダウンロードが実行されると、もともと当該ファイルのあったパソコンとは別のパソコンにファイルが複製され、この複製されたファイルがさらにダウンロードされる。このような中継機能によって当該ファイル情報の一次的発信者が誰であるのかが判別できなくすることを目的としている。

もっとも Winny クライアントの処理を追いかけていき、パケットを解析しつつ、試行錯誤してデータを逆アセンブルしていくことにより、Winny の暗号化解読することができ、その結果、1 年分の接続者情報（Winny ネットワークに接続している者のＩＰアドレス、ポート番号、キー等）を解明して、保有することができたとしている。その意味で、「匿名性は、ないといいきってもいいだろう。」という認識も存在している。

2.3.　発信者を突き止める技術

ＩＰトレースバック技術とは、発信源を特定するための技術の総称[3]をいう。この技術に

---

[3] 具体的な参考文献としては、多数あるものの、Ofir Arkin “Trace-Back　A Concept for Tracing and Profiling Malicious Computer Attackers”
http://webproxy.com/research/reports/acrobat/traceback.pdf
や Susan C. Lee and Clay Shields “Legal, and Societal Challenges to Automated Attack Traceback”
https://users.cs.jmu.edu/aboutams/Public/IP%20TraceBack/Technical-%20Legal%20and%20Social%20Chalenges%20to%20Automated%20Attack%20Traceback.pdf
は興味深い。

よってＩＰパケットの送信元アドレスが詐称されたとしても発信源を特定することができることになる。この技術は、基本的に注目したトラフィックに対して、ルータが、そのトラフィックをどこから中継し、どこに中継したかを報告するという機能を利用して、攻撃経路を突き止めようとするものである。その手法については、種々の分類が可能である。

3 匿名性（anonymity）と法との関係

3.1. 一般論

上記のように匿名性を考えたときに、匿名性（anonymity）と法律との関係についていえば、法律は、匿名性（anonymity）について中立的な立場を採用しているということがいえる。そもそも、一定の掲示板などにおいて、匿名での表現がゆるされるか望ましいかなどについては、その掲示板の管理者が自由に決められることであろう。また、たとえば、匿名で記した書物であったとしても、表現の自由が保証されることになるし、また、匿名での実演でも、著作権法上の保護をうけることに問題はないであろう。

このような実体法の立場に対応するかのように、訴訟法の上でも、匿名での活動に対しての対応の準備はある。そもそも、当事者の表示として、「○○こと××」という記載がなされることはいうまでもないし、具体的な名称を記載しない場合でも、訴訟の当事者として特定されうる限りにおいて、有効な訴状の記載ということになる。

刑事事件において、被疑者が完全黙秘で、住所・氏名が判明しない場合でも、当事者であることを特定する手段を用いて、手続きが進行することになる。

3.2. ネットワークにおける匿名性（anonymity）の確保

3.2.1. 具体的な問題点

ネットワークにおいて社会的な行動をするのに、実名等を他人に伝えないでも、活動ができるようにする要請が強いことは前述した。具体的な制度の関係でも、2 において論じた種々の制度のうち、エスクローサービス、クレジットカード番号の直接認証システム、電子マネーの技術などについても、特に法律的に禁止するとかの問題は生じない。

もっとも、ネットワークにおいて行為者の同一性を識別・認証するための制度である電子署名については、その要件との関係で、この匿名性（anonymity）との関係での問題があることになる。

3.2.2 電子署名と匿名性（anonymity）

電子署名とは、「当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。」「当該情報について改変が行われていないかどうかを確認することができるものであること。」の二つの要件をともに満たす特定の技術をもちいた情報処理ということになる。これに関する法的規制としては、電子署名法がある。上記電子署名のうち、当該電磁的記録に記録された情報について本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われているときについて、電磁的記録の真正な成立の推定(第 3 条)

が定められている。
そして、このような電子署名について、本人が自らが行う電子署名についてその業務を利用する者（以下「利用者」という。）その他の者の求めに応じ、当該利用者が電子署名を行ったものであることを確認するために用いられる事項が当該利用者に係るものであることを証明する業務がおこなわれるとき、そのような業務を認証業務という。このような業務が行われる際に、その認証の基準については、匿名との関係で、実名主義がとられているということがいえる。というのは、電子署名及び認証業務に関する法律施行規則第５条（利用者の真偽の確認の方法）は、「法第六条第一項第二号の主務省令で定める方法は、次の各号に掲げる方法とする。」として、「住民票の写し、戸籍の謄本若しくは抄本（現住所の記載がある証明書の提示又は提出を求める場合に限る。）、外国人登録法（昭和二十七年法律第百二十五号）第四条の三に規定する登録原票記載事項証明書又はこれらに準ずるものの提出を求め、かつ、次に掲げる方法のうちいずれか一以上のものにより、当該利用申込者の真偽の確認を行う方法。」によって本人確認をするということが定められている。そして、その「次に掲げる方法のうちいずれか一以上のもの」というもとで、上記のような身分証明書などの直接の提示を求めているのである。上記のような考察のもと、「特定認証局の電子署名の認証業務」としては、匿名性（anonymity）は認められていないということができる。

もっとも、そもそも、特定認証局の認証業務のもとで発行された電子署名であると、それ以外の認証業務のもとで発行された電子署名であると、その電子署名の効力は違いがない。その電子署名の成立の真正は、同法３条のとおり、「これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるもの」かどうかという点にかかっているからである。

3.2.3　電子マネーと匿名性（anonymity）

利用者の保持する電子機器に記録されたデジタル・データがそれ自体「価値」を有するもの（「決済手段の電子化」）となったときに、その価値は、誰から誰に譲渡されようと一定の経済的な利益をもつものとして認識され、たとえば、弁済などに用いられれば、「提供」（民法４９２条）などの効力が発生することになる。このような状況までにいたった場合、「電子マネー」である[4]と認識することができよう。

電子マネーについて、法律の基本的な立場としては、当事者間での経済的な効果についての共通の認識について、そのとおりの一定の効果を与えているということになる。現在、その適法性が議論されているＲＭＴがあるが、ゲーム内のアイテムやポイントなどが、一定の経済的な価値をもつものとして、取引されれば、その匿名性（anonymity）は、法的に保護されているということもできよう。しかし、そのような電子マネーについては、一定の要請から、法的な規制の要素が準備されている。

外国為替及び外国貿易法においては、その６条１項７号ハにおいて「ハ　証票、電子機器その他の物（第十九条第一項において「証票等」という。）に電磁的方法（電子的方法、

---

4 「支払手段の電子化」にすぎない場合を除外して検討している。そこまで含めた場合に、ゲーム会社からの払い戻しの問題があり、その場合、出資法違反の可能性があることを指摘するものとして中崎尚「「Second Life」でゲーム内通貨を米ドルに換金――出資法に抵触する？」http://www.itmedia.co.jp/bizid/articles/0702/15/news109.html。

磁気的方法その他の人の知覚によつて認識することができない方法をいう。）により入力されている財産的価値であつて、不特定又は多数の者相互間での支払のために使用することができるもの（その使用の状況が通貨のそれと近似しているものとして政令で定めるものに限る。）」が支払手段として定義されている。上記の電子マネーが、念頭におかれているのである。そこでは、資金洗浄防止の観点などから届出等の義務が課される可能性が存在しており、電子マネーの匿名性は、その限りで制限される可能性があるということになる。

４　匿名性（unlinkable）と法との関係

4.1.　匿名性（unlinkable）と法とのかかわり

4.1.1.　通信の秘密の概念

１記載のように､匿名性を突き止めようとする本人に到達するためのコストが社会通念上、許容し得なく高い状態と定義するときに、法律は、さらにその本人に到達するためのコストを高めるような仕組みを準備しているのではないかということが問題になる。この点については、「通信の秘密」に関する制定法の規定とその解釈、そしてその規定に関連する法律およびその運用が、本人への到達コストを高める機能を有していると評することができるものと思われる。

憲法２１条２項後段は、「通信の秘密は、これを侵してはならない」と定めている。そして、「通信の秘密」の内容は、一般には①「通信」の「秘密」にかかる事実を「通信当事者以外の第３者が積極的意思をもって知得してはならず」②「第３者にとどまっている秘密を、漏洩（他人が知りうる状態にしておくこと）することおよび窃用（本人の意思に反して自己または他人の利益のために用いること）してはならない」の２つの意味を包含するものととらえられている。関連して、「電気通信事業法」は、その第４条で、（秘密の保護）として、第１項では、「電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。」と定め、また、第２項では、「電気通信事業に従事する者は、在職中電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても、同様とする。」と定めている。また、第 179 条においては、「電気通信事業者の取扱中に係る通信（第百六十四条第二項に規定する通信を含む。）の秘密を侵した者は、二年以下の懲役又は百万円以下の罰金に処する。」として刑事罰が定められている。そして「電気通信事業に従事する者が前項の行為をしたときは、三年以下の懲役又は二百万円以下の罰金に処する」とされているところである。一般的な解釈によれば、電気通信事業法４条は、憲法２１条２項の規定を受けて、電気通信事業者の取扱いにかかる通信の秘密を規定したものであるとされる。電気通信法制研究会「逐条解説　電気通信事業法」（以下、「逐条解説電気通信事業法」という）[5]によると、「通信の秘密を保護する趣旨は個人の私生活の自由を保護し個人生活の安寧を保証する（プライバシーの保護）とともに、通信が人間の社会生活にとって必要不可欠なコミュニケーションの手段であることから、憲法第２１条２項の規定を受けて思想表現の自由の保障を実効あらしめることにある[6]。そして自由闊達な通信がなされることを保証するための規定である」とされている。そして、電気通信事業者の取扱中にかかる通信については、いったん通信当事者の手から離れ、事業者に託されたものであるから、通信当事者が秘密を保護するための自衛措置を講ずる余地がなく、また、秘密が侵害される危険にさらされやすいことにかんがみ、電気通信事業に対する利用者の信頼を保護するため、その秘密を侵すことを禁止している

[5] 電気通信法制研究会「逐条解説　電気通信事業法」（第一法規、1987）

[6] もっともこの点について高橋郁夫・吉田一雄「通信の秘密の数奇な運命(憲法)」(情報ネットワーク法学会誌第５巻(2006 年 5 月))

のであるとされている。
　また、有線による電気通信についても、有線電気通信法９条において（有線電気通信の秘密の保護）「有線電気通信（電気通信事業法第４条第１項又は第 164 条第２項の通信たるものを除く。）の秘密は、侵してはならない。」とされ、同１４条１項が、「第９条の規定に違反して有線電気通信の秘密を侵した者は、２年以下の懲役又は 50 万円以下の罰金に処する。」とされている。
　一般的に憲法上の規定は、その名宛人が公権力に向けられることもあって、一般私人間に対しては、民法等の規定の解釈を通じて、適用されるにとどまるとされている。しかしながら、「通信の秘密」の保護の規定は、その性質上、私人に対しても向けられていると解するのが、通常である。もっとも、電気通信事業法や有線電気通信法の上記規定が、何人に対しても「通信の秘密」の侵害行為を禁じていると解されることからいって、かかる「通信の秘密」を侵害してはならないという規定は、一般私人に対しても効力を有していることは間違いがない。
　「逐条解説電気通信事業法」によれば、ここでいう、「通信の秘密」の範囲は、通信内容にとどまらず、通信当事者の住所、氏名、発信場所と通信の構成要素や通信回数との通信の存在の事実なども含むものであると解されている。これらの事実は、通信の構成要素であるとされるが、これらは、「それによって通信の内容を探知される可能性があるし、また、通信の存在の事実を通じて個人の私生活の秘密（プライバシー）が探知される可能性がある」からである。このように、通信の秘密には、通信の内容たる事実に係るものと通信の外形的な事実に係るものとがあるが、ここでは両者を保護するものである、とされている。
　また、電気通信事業法においては「知り得た他人の秘密」の第三者への漏洩・窃用も禁止されている（同条２項）。ここでいう「知り得た他人の秘密」は、「通信の内容、通信の構成要素、通信の存在の事実等『通信の秘密』のほか、通信当事者の人相、言葉の訛りやプッシュホンに記憶された相手番号等直接の通信の構成要素とはいえないが、それを推知させうるものを含む」と解釈されている（「逐条解説電気通信事業法」25 頁）。
　もっとも、通信の「秘密の保護」について、通信の内容についての保護とそれ以外の外延的情報の保護についての「知り得た他人の秘密」の保護という解釈も成り立ち得えるのではないかということも考えられる。しかしながら、具体的な検討をなしている見解[7]は、見当たらない。
　そして、「通信の秘密」の内容として、一般には「通信」の「秘密」にかかる事実を「通

---

7 現行郵便法の立案当局者は、差出人・受取人の氏名・住所等は、１項の「信書の秘密」ではなくて、２項の「他人の秘密」に該当すると解していたように見受けられるとされている（佐藤幸治、芦部編「憲法Ⅱ　人権（１）」642 頁)。そして、昭和 28 年１月 30 日内閣法制局意見は「郵便物の差出人又は受取人の居所、氏名及び差出個数等は、もとより通信の意味内容をなすものではないけれども、通信そのものの構成要素であり、実質的に見ても、これらの事項を知られることによって、通信の意味内容が推知されることもあり得るのであるから、これらの事項が通常郵便法第９条による『他人の秘密』に包含されることについては大なる疑問はないといってよかろう。」という。
また、昭和２８年１２月および昭和２９年３月に、長野県で、公安調査庁に勤務するＡが、郵便集配人に対して特定の機関紙（朝鮮関係の非公然の機関紙類）の発行部数や特定の人間への郵便の存否などを問いただしたという事実があったが、国会において、この行為についての議論があったが、政府委員は、このような観点から、他人の秘密に該当する(郵便法９条２項)との説明をしている(齋藤政府委員（昭和 29 年４月３日の衆議院の郵政委員会)、井本台吉（昭和 29 年５月２１日の参議院郵政委員会）)。
また、昭和 38 年 12 月９日内閣法制局意見は、その理由のところで、公衆電気通信法第５条１項を引くと共に第５条２項に触れ、その上で、第２項についての「他人の秘密」侵害の該当性を認定している。
　もっとも、外延的事実は、２項の「他人の秘密」にすぎないとするとき公衆法(当時)5 条２項違反行為についての刑事罰の適用が困難になりかねないという問題が発生することになる。

信当事者以外の第３者が積極的意思をもって知得してはならず」「第３者にとどまっている秘密をそのものが漏洩（他人が知りうる状態にしておくこと）することおよび窃用（本人の意思に反して事故または他人の利益のために用いること）してはならない」の２つに分けてとらえられることになる。

4.1.2　「通信の秘密」の解釈の展開

これらの内容についての一般的な解釈として、通信に関連して、以下のような通信の外延情報の取得・利用に関する問題については、すべて違法と評価されるものの特定の場合に限って、具体的に許容されるという命題が導かれるものとされている。その問題というのは、（ア）電気通信事業者において、片側当事者の同意がある場合において、電話の発信場所を探索し、これを他人に知得させる行為の許容性（イ）事業者みずからが、通信の片側当事者として通信の外延情報、内容を知得することの許容性（ウ）電気通信事業者が、通信の外延情報を記録することの許容性、通信の外延情報・内容の利用の許容性（エ）捜査関係事項照会に対して回答の許容性やその他の情報の開示の許容性などである。

（ア）逆探知問題

電気通信事業者において、片側当事者の同意がある場合において、電話の発信場所を探索し、これを他人に知得させる行為が違法になるのかというのが、いわゆる逆探知の問題である。これについては、昭和 38 年 12 月 9 日内閣法制局意見は、「電話を利用して刑法２２２条に規定する脅迫の罪を現に侵している者がある場合に、被害者の要請によって（略）当該電話の発信場所を探索し、これを司法警察職員等の捜査官憲に通報することは、公衆電気通信法第５条第２項の規定に違反することになるか」という質問に対して「公衆電気通信法第５条は、第１項において、『公社・・の取扱い中にかかる通信の秘密は、侵してはならない。』と規定するとともに、第２項において、『公衆電気通信業務に従事するものは、在職中公社・・・の取扱い中に係る通信に関して知り得た他人の秘密を守らなければならない。この職を退いた後においても同様とする。』と規定している。電話の発信場所は、発信者がこれを秘匿したいと欲する場合がありうるから、右の第２項にいう『他人の秘密』に該当するものと解すべきであろう。」「被害者の要請があるときは、公社の職員が当該電話の発信場所を探索し、これを捜査官憲に通報することは、許されるものと解すべきである。その理由を要約していえば、右の探索および通報は、脅迫の罪の現行犯人の逮捕に協力するために行われるものだからである。」としている。また、学説でも阪本昌成「電気通信事業者は、電気通信が犯罪に利用されたことを理由に、電話の発信場所を探索し、これを他人に知得させるとすれば、通信の秘密を侵害することになる（探索行為は、電通法３条違反であり、他人に知らせる行為は『電気通信事業者の取扱中にかかる通信の秘密は、侵してはならない』と定める４条１項違反となる）」「憲法理論Ⅲ」（成文堂、1995）と明言するところである。

（イ）「取扱中にかかる」の限界

また、「取扱中にかかる」という用語は、抽象的には、「電気通信事業者が管理・支配している通信」ということを意味する。では、逆に通信を行う各端末が、行う端末における通信に関する情報の取得が、この関係でどのように扱われるかという問題がある。この点については、上記の昭和 38 年 12 月 9 日内閣法制局意見は、「捜査官憲が、電話による通信の一方の当事者甲の同意を得て、甲の利用する電話の端末の設備において他方の当事者乙

の遺話を録音することは、公衆電気通信法第五条第一項に違反しないか」という質問に対して「電話による通話の一方の当事者甲がその利用する電話の端末の設備において聴取しうる他方の当事者乙の通話の内容は、甲の支配の下に置かれた事項であつて、法第五条第一項にいう『公社……の取扱中に係る通信の秘密』の範囲外にある事項である。したがつて、甲が、その利用する電話の端末の設備において、乙の通話の内容をみずから録音することはもちろん、第三者に録音させることもまた、法第五条第一項の規定に違反することにはならないものと思われる。」という回答をしている。

(ウ)正当業務行為について

「電気通信事業における個人情報保護に関するガイドライン」[8]によれば、通信履歴を「記録することも通信の秘密の侵害に該当し得るが、課金、料金請求、苦情対応、自己の管理するシステムの安全性の確保その他の業務の遂行上必要な場合には正当業務行為として少なくとも違法性が阻却されると考えられる。」とされている。また、上記ガイドライン解説の(3)においては、発信者を探知するための通信履歴の解析は、目的外利用であるばかりでなく通信の秘密の侵害となると解されること、違法・有害情報掲載時に、その発信者に警告を行わないと自己のサービス提供に支障を生じる場合（自己のサービスドメインからの通信がアクセス制限される場合等）に、自己が保有する通信履歴などから発信者を探知することは、正当業務行為として行うことができることが触れられている。同じく、解説の(4)においては、通信履歴は、裁判官の発付した令状に従う場合等、違法性阻却事由がある場合を除き、外部提供は行わないこととされていること、大量の無差別のダイレクト・メールが送りつけられ、自社のネットワークやサービスが脅威にさらされており、自己又は他人の権利を防衛するため必要やむを得ないと認められる場合には、発信元の電気通信事業者に通信履歴（発信者のＩＰアドレス及びタイム・スタンプ等）を提供することは許されると考えられることなどが触れられている。

（エ）捜査関係事項照会に対して

この点については、「電気通信事業分野におけるプライバシー情報に関する懇談会」中間報告書および上記「電気通信事業における個人情報保護に関するガイドライン」において検討がなされている。このガイドラインの第２３条によれば、電気通信事業者は、通信履歴については、「課金、料金請求、苦情対応、不正利用の防止その他の業務の遂行上必要な場合に限り、記録することができる」（第１項）とされ、第２項においては、「電気通信事業者は、利用者の同意がある場合、裁判官の発付した令状に従う場合、正当防衛又は緊急避難に該当する場合その他の違法性阻却事由がある場合を除いては、通信履歴を他人に提供しないものとする。」とされている。ここにいう、通信履歴とは、「利用者が電気通信を利用した日時、当該通信の相手方その他の利用者の通信に係る情報であって通信内容以外のもの」をいうとされている。また、通信履歴は、通信の構成要素であり、電気通信事業法第４条第１項の通信の秘密として保護されるとされている。この部分は、逆に捜査関係事項照会に対して、開示してはならないことを明らかにしたものとされる。

学説的にも、捜査関係事項照会に対して、「郵便官署や電気通信事業者が通信に関する事項を報告することは許されないと解すべきである」とされる[9]。

---

[8]http://www.soumu.go.jp/joho_tsusin/d_syohi/privacy_studygroup_interimreport_chap2_sec2.html#1

[9] 樋口・佐藤・中村・浦部編（浦部著）「注解法律学全集２　憲法Ⅱ」（青林書院、1997）85 頁、86 頁

4.2. ネットワーク管理と匿名性（unlinkable）との衝突[10]

4.2.1 ネットワーク管理の実際

ネットワーク内の通信がスムーズになされるように、ネットワーク管理者は、日々、種々の活動を行っている。もっとも一般的なものは、ネットワーク観測とでもいわれるべき行為である。このような代表的な活動として、「サイバーフォース」における観測活動をあげることができる。「サイバーフォース」は、サイバーテロの未然防止、被害拡大の防止等のために創設された機動的技術部隊であり、その活動の中で、「検知ネットワークシステム」とは、「全国の警察機関に多数あるインターネットとの接続点に設置された侵入検知装置 IDS を 24 時間オンラインで監視するサイバーフォースの中心となるシステム」である 。警察は、ここから収集された情報を分析することによって、インターネット上で発生している様々な攻撃手法などをいち早く発見し、関係各機関への情報提供等に役立てている。また、現在、ネットワークの安全性を確保するために種々の活動があり、上記のサイバーフォース以外にも、ＩＰＡの「TALOT」「TALOT2」、JPCERT/CC の定点観測システム『ISDAS』、Telecom-ISAC Japan の観測システムなどがある 。もっとも、これらのネットワーク観測行為は、法的な問題を惹起しないものと考えられるが、その根拠としては、やや明確ではないものといえよう。サイバーフォースにおいては、すべて警察機関内における接続点でのパケットの状況を了知しているものであるし、それ以外のシステムについても同様である。もっとも、このような行為がすべて同様な法理によって許容されるのかというのは、問題となる。具体的に、大学において、大学のネットワークに流入するパケット送受信情報を分析し、また、対外接続装置、高速基幹ルータの場所において、装置を通知するすべてのフロー送受信情報を分析することもおこなわれている。また、実際に異常なアクセス履歴があれば、どこからアクセスがなされているか、いわば、逆探知をなすことなども存在している。

4.2.2. ネットワーク管理行為と逆探知の正当化根拠

ネットワークにおいて、電気通信を発信人から受信人に届けるにあたって、そのために、しらなければならない通信の外形的事項を知ることは、これは当然のことである。むしろ、発信人から、この情報をもとに届けるように受託されるのであり、この受託業務に際して委託される事項とその業務の履行にあたって発生する情報については、電気通信事業者は、消極的に了知するのである。「電気通信事業に従事する者は、その業務の取扱い上、通信の内容、通信当事者、通信年月日、通信の発信地および受信地など通信の秘密を容易に知りうる地位にあることから、その業務の取扱い上、必要な限度において、通信の秘密を知ることは、第１項の規定に違反しない」（「逐条解説　電気通信事業法」）ということは、これをいっていることになる。が、「それを第三者に漏洩したり、窃用したりすることは第１項の規定にも違反することになる。」まさに上記のネットワークにおけるいわば逆探知の問題は、この業務の取扱い上、必要な限度において知ることになる行為（消極的了知行為）の限界はどこかという問題を提起しているものと思われる。一般の電話の場合であれば、発

10 高橋郁夫・吉田一雄「ネットワーク管理・調査等の活動と『通信の秘密』」
http://www.jaipa.or.jp/info/2005/iw2005/IW05.pdf

信者の逆探知に該当する状況すなわち、ネットワークへの攻撃をなしているパケットの発信元を突き止める行為を例にとって考察することができよう。電話の場合であれば、「一方の通信当事者の承諾では違法性は阻却されない場合がある」とされているので、明らかに異常なアクセスがあり、急迫不正の侵害と認識される場合であれば、格別、そうでない場合には、そのような通信の相手方の探知というのが、もはや、「業務の取扱い上、必要な限度」を越えているものとてして、積極的了知行為として認識されるのではないか、ということがいえる。

このように考えた時に、上記のような大学や一般の企業などのネットワーク観測・管理行為は法的に正当化されるのか、正当化されるとすればその根拠というものは何であるのかということになる。

消極的了知行為であるとされれば、業務としての正当性が、直接的に問題にはならずに許容されることになり、これが消極的了知行為とされるかどうかは、一つの問題であろうと思われる。

もっとも、大学や企業が通信の当事者であるといって、TCP／IP プロトコルの特性から、大学も当事者であり、パケットをいったんは、譲り受けているはずだとして当事者と解することによって正当化するという考えも成り立ち得ないことではない。しかしながら、そうだとすると、結局は、インターネットにおいて通信に関与するものはすべて当事者であるということになって、インターネットにも通信の秘密が該当するという考え方と相反してしまう。やはり、大学や企業のネットワーク運営者は、一定の法的根拠によって、そのような観測業務が正当化されると考えるしかないものと思われる。大学のネットワーク運用ポリシにおいて、ネットワーク内に外部の当事者の端末の接続を許可した場合、その外部当事者の端末と大学の外部との通信当事者こそが、通信の当事者であり、その大学の管理当局は、その通信から見て、第三者であるということができそうであるからである。上述のサイバーフォースなどの構成とネットワークの構成が異なっているのである。

この点については、いままで、法的な解釈が定まっているものではない。一つの方向性としては、このような観測業務を正当化するものとしては、二つの方向性がある。一つは、大学や企業のネットワーク運用ガイドラインにおいて、利用者は、「運用ガイドライン」に同意することを根拠として、利用が可能になっているという当事者の同意を根拠とする方向性である。この場合、この運用ガイドラインにおいて、大学や企業等の運営に関する観測業務があることを利用者に告知し、それに同意することを要件として、大学や企業等のネットワークを利用させるのである。この同意は、観測に対する同意を意味することになり、それでもって、観測業務が正当化されることになる。もっともこのようなアプローチは、通信において第三者の積極的取得を許容する同意が「両」当事者と解されているのと矛盾する可能性がある。

いま一つは、そのような同意がなくても、そもそも、ネットワークに関する運営をするものは、その運営を正当に行うためにそのネットワークを観測する等の業務を行うことができ、それは、社会通念上、正当業務行為として許容されるのであるという考え方である。筆者は、基本的には、ネットワーク観測は、このような正当業務行為として許容されるべきものであると考える。しかしながら、この正当業務行為の範囲というものは、いまだ、

我が国では十分に議論されていない問題[11]であり、明確な許容根拠や許容さる範囲については今後の問題となっているということができるであろう。そして、その際に、米国の制定法の規定を参考にすることが参考になるものと考えられる。米国においては、18U.S.C.§2511（2）（a）（i）が、「有線・電気通信の送信に際し施設が利用される有線・電気通信サービスの交換機のオペレーター、役員、従業員、または捜査官は、必要な業務に従事している通常の過程において、そのサービスの遂行もしくは、権利や財産を保護するために通信を傍受し、開示し、または使用することができる。ただし、公衆に対する有線通信サービスのプロバイダは、機械的に行われる品質管理チェックをする場合を除いて、サービスの監視や無作為のモニタリングを行ってはならない。」と定めており、また、18U.S.C.§2511（2）（i）は、コンピュータ攻撃の被害者が、法執行機関にコンピュータ侵入者の有線または電子通信を傍受する許可を与えている。具体的には、法執行機関は、4つの要件が満たされる場合に、保護されたコンピュータ「に対して、を通して、あるいは、から」コンピュータ侵入者の通信を傍受することができると定めてられているのである。

4.2.3　逆探知によって得た情報の利用の問題

ネットワーク運営者が、種々の根拠でもって、ネットワーク観測をなしうることについては、上記でみたとおりである。しかしながら、その観測で取得したデータを利用するという側面についても問題が生じる可能性があることに留意が必要である。「通信の秘密」の侵害の定義においても、適切に取得した情報であっても、その漏洩や窃用が禁止されることがあることが示唆されている。

まず、当事者として、取得した情報については、定義からすれば、通信の秘密の侵害は、第三者としての立場に関することなので、直接に適用がなされないということができよう。しかしながら、電波法５９条の定めを、通信の当事者として、受信したものであっても、漏洩や窃用をなすことは、通信の秘密を侵害するものとなると解することも可能に思われる。この場合、例えば、観測の結果、知り得た情報を、警察に通報したり、また、分析して、ネットワークの改善に利用したりする、また、ネットワークの改善に必要な学術的な分析・研究をするということはありうるであろう。これらの通報・利用が、「通信の秘密」の侵害に該当するのかという問題になる。

「通信の秘密」に関する情報については、電気通信事業者であっても、窃用は禁止されることになる。「窃用」とは、自己又は他人の利益のために用いることをいうことになるが、ネットワーク管理において、その管理のためにする利用行為がどこまでならば、窃用行為といわれないのかという点については、限界が不明確であるものといわれなければならない。

具体的には、情報の取得による攻撃分析、自らの対応、関係者へのはたらきかけ、学問的研究、その発表など、通信に関する情報の取得からする利用の問題については、いろい

---

11 「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン（第１版）」が、平成19年5月に制定されている[11]。このガイドラインは、DoS攻撃等のサイバー攻撃、ワームの伝染及び迷惑メールの大量送信及び壊れたパケット等（以下、大量通信等）によって電気通信サービスの提供に影響を与えかねない事態が生じることがあり、その事態に対応し電気通信事業者は当該通信の遮断など様々な対処を行っているが，それらの対応と通信の秘密の保護との抵触を検討したものである。

ろな側面が考えられるが、どのようなところまでであれば、窃用行為といわれないのかという点については、その限界は、まったくもって不明瞭であるということができるであろう。

第三者への開示の問題についても、電気通信事業者間における情報共有という問題からは、その限界がはっきりしないという問題がある。

また、ネットワーク犯罪が判明し、電気通信事業者のみの力で、真相を究明しがたいとき、通信事業者において、法執行機関の助力を得て真相の究明をすることができるのかという問題もあるのである。

上記問題について、いえば、この問題についての検討は、我が国で全くなされていないものと言うことができるであろう。法執行機関への通報という問題は、また、別個の問題を含むものと考えられるので、ここでは、考慮の外におくこととして、その観測結果の情報の分析・調査・検討をどのように位置づけるかという点について検討する。当事者として受信した結果であっても、当事者は、通信の秘密で保護される事実について、漏洩（他人が知りうる状態にしておくこと）することおよび窃用（本人の意思に反して自己または他人の利益のために用いること）してはならないという一般的な規範が存在しうると仮定することができる。そのような仮定のもとで、観測結果の分析・調査・検討は、通信の秘密に関する事実を「窃用（本人の意思に反して自己または他人の利益のために用いること）してはならない」という規範に衝突するのかという問題が指摘しうる。この点については、まさに「窃用（本人の意思に反して自己または他人の利益のために用いること）」という用語の解釈問題となる。この点については、なんら具体的な解釈が示されているわけではないが、上記窃用については、公衆の利益をはかるための利用は、含まれないのではないかという視点を指摘しうるであろう。このような観点からするとき、通信について、その当事者が特定しうるような形での研究となれば、格別であるが、そうでない限り、一般的なデータとしての利用は、「通信の秘密」との関係で問題を惹起するものではないといえよう。

なお、本考察においてネットワーク観測においては、個人が識別されない形での情報取得を問題にしている。かかる形態での情報取得は、特定の個人の識別につながらないため、その情報の取得・利用について、いわゆる「個人情報」の保護の観点からする問題は生じないものと考える。

4.3. 不適切コンテンツ等と匿名性の交錯

4.3.1 序

不適切コンテンツの例は、名誉棄損、スパム、緊急時の位置連絡、自殺予告に対する対応などがあげられる。これらの場合において、そもそもは、発信者が誰であるかを突き止め、刑事なり民事、もしくは、その他の手法で、その発信者に対して適正な法の適用などを求めるということになるはずである。しかしながら、上記通信の秘密に関連する法律制度の関係で､その発信者を突き止めるための情報を得ることがきわめて困難になっている。しかしながら、これらの観点においては、通信の秘密に対する例外として、一定の要件のもとに、発信者を突き止めるための情報が提供される場合がある。これらの場合は、匿名

性といっても程度の問題であるし、また、具体的な状況のもとでの議論が必要になることを物語っているものといえよう。具体的な問題との関係での状況は、以下のとおりである。

4.3.2　名誉棄損に対する対応

ネットワークにおいて、名誉毀損行為がなされた場合、リアルワールドでの話を考えれば、だれが、その名誉毀損発言の発言者であるかを突き止め、その者に対して、民事なり刑事なりで名誉毀損の責任を問えば、いいことになる。刑事事件で対応すべき事件は、さておくとして、民事事件においては、そもそも、通常、被害者は、容易には、その発言者を特定しうる情報を得ることができないということや発言者が、本名（もしくは、仮名－固定された名称）でもって発言するとは、かぎらないということがある。パソコン通信などの場合においては、本名（固定された仮名をも含む）での発言があるのであれば、その情報は、パソコン通信のサービス・プロバイダが、その情報を有しているのであり、課金などの要請から、そのプロバイダは、通常、発言者を特定しうる情報を十分に有している。そのために、被害者が、発言者を特定しうる情報を取得するということは、物理的には、困難なことではない。それに対して、インターネットでの環境においては、ユーザーは、インターネットに接続したコンピュータを通じて、掲示板に書き込むのであり、その接続するエリアが、グローバルに一定のアドレスを保有し、それとは別にローカルの管理の観点から特定のアドレスが割り当てられるという形態が一般である。しかも、そのローカルで接続していたアドレスが特定可能になる時期については、各ローカルの管理の仕方によって、種々のバリエーションがある。実際上、掲示板における発言については、その発言が書き込まれたサイトに接続したコンピュータのうち、発言をなしたコンピュータを特定し、そのコンピュータが、どこから送信されているかを段階をふんで、特定していかなければならないという性質をもっている。そのために、技術的にも、たいへんな手順をふむことになる。

このような技術的な困難性に加えて、特定するための情報の取得をさまたげる法制度的な要素がある。この特定のためには、プロバイダに対して、特定の発言をなしたコンピュータに関する通信の情報を被害者が開示してもらうということになる。しかしながら、この「通信の情報」というのは、前述したように、「電気通信事業法」の４条でさだめる「通信の秘密」として保護されるものと考えられている。従って、被害者に対する開示というのは、通信の当事者以外の者に対する開示ということになるので、「発信者情報は、発信者のプライバシー及び匿名表現の自由、場合によっては通信の秘密として保護されるべき情報である」し、また、「発信者情報の開示は、発信者のプライバシーや表現の自由という重大な権利利益に関する問題である上、その性質上、一旦開示されてしまうとその原状回復は不可能であることから、特定電気通信役務提供者が裁判外の請求を受けて開示を求められた場合にも、みだりに開示がなされることを回避する必要がある」ということになる。

このような見地から、定められたのが、プロバイダ責任制限法（特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」（以下、プロバイダ責任制限法という））である。そして、この発信者情報開示については「「侵害情報の流通によって当該開示の請求をする者の権利が侵害されたことが明らかであるとき。」で、かつ「当該発信者情報が当該開示の請求をする者の損害賠償請求権の行使のために必要である場合その他発信者情報の開示を受けるべき正当な理由があるとき。」に限って「当該権利の侵

害に係る発信者情報（氏名、住所その他の侵害情報の発信者の特定に資する情報であって総務省令で定めるものをいう。以下同じ。）の」開示をもと売るものとされている。

この発信者情報開示制度においては、その逐条解説である「電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律－逐条解説－」によれば、「開示関係役務提供者は裁判外での開示請求については、とりわけ慎重に対応することを要請されることとなる」（同 24 頁）と解されていたこともあって、現実的には、裁判での開示を求めるしかない状況に近く、きわめて、その実効性に疑問が呈されていたものということができよう。

もっとも、このような解釈や運用については見直しの方向にあり、現在では、プロバイダの運用において、任意の開示についてもガイドラインで認められるようになってきている。「プロバイダ責任制限法発信者情報開示関係ガイドライン」（http://www.telesa.or.jp/consortium/pdf/provider_070226_guideline.pdf）においては、一定の基準がしめされ、任意の開示に応じる手順が具体的に論じられている。

4.3.3　スパムメール

一方的に送信される広告宣伝メールを「迷惑メール」というが、そのような迷惑メールは、不快であるばかりでなく、架空請求や児童買春の契機になっていること、携帯電話等で受け取った場合は受信を望んでいないにもかかわらず課金されてしまうこと、電気通信事業者の設備に障害を与えたり、事業に支障をきたしたりすることなどに問題がある。法的には、「特定電子メールの送信の適正化等に関する法律」が制定され、また、平成１７年５月には、「特定電子メールの送信の適正化等に関する法律の一部を改正する法律案」（改正特定電子メール法）が、成立している。ここでは、（１） 特定電子メールの範囲の拡大（２） 架空アドレスあてのメール送信を禁止する範囲の拡大及び罰則の見直し（３）送信者情報を偽った電子メール送信の禁止及び直罰規定の整備（４） 電気通信事業者による電気通信役務の提供拒否事由の拡大（５） 指定法人による指導・助言等の業務の登録機関による実施への移行などを定めた改正がなされている。また、「迷惑メールへの対応の在り方に関する研究会　最終報告書（案）」[12]においては、法的な対応等に加えて技術的な対応が提唱されている。

この法律の仕組みは、承諾を得ないで「自己又は他人の営業につき広告又は宣伝を行うための手段として送信をする電子メール」を「特定電子メール」として、その電子メールについて、「当該送信者の氏名又は名称及び住所」「送信者の電子メールアドレス」などを正しく表示されるようにして送信することを命じて（送信者情報について同法６条）、それに違反する場合は、総務大臣は、措置命令をなすことができるし（同法７条）、プロバイダは、正当な理由がある場合には、通信の提供を拒否できることになっている（同法１１条）。また、７条の違反について、直接、罰則が適用されるため（同法３２条）、その限りで、プロバイダは、正当な行為として、対応がなしうるし、また、法律が、匿名性を保障するという意味合いは、なくなっている。

4.3.4　緊急時の位置連絡

12 http://www.soumu.go.jp/s-news/2005/050617_3.html#f

位置情報というのは、移動体端末の所持者の所在を表す場所を示す情報（基地局エリア若しくは位置登録エリア程度又はそれらより狭い範囲を示すもの）をいう。第三世代携帯電話には、GPS 方式による位置測定機能が実装されており、位置情報を取得している。そしてその取得した位置情報を位置情報通知チャンネルを通じて、測位サーバに送信される。この通信を通じることによって、自分の現在位置の探索ができ、また、第三者が、その端末の場所を了知することも可能になる。目的地へのナビゲーションは、写真レポート作成、勤怠管理、車両等管理などに既に応用がなされている技術である。

この位置情報は、その端末を保持している人が、今、どこにいるのかという情報を示しており、その人のプライバシーや個人情報として取り扱われている。また、個別の通信の関係する場合には、通信の秘密としても保護されている。ですから、取得時の目的の明示や取得に対する拒絶などの機能が必要になっている。

携帯端末保有者の同意がない場合に、その位置情報を取得することができるかということが問題になる。位置情報の追跡の問題ということになる。緊急通報の際に位置情報を通知することにより、警察機関、海上保安機関及び消防機関（以下「緊急通報受理機関」という。）が迅速な対応を図ることができるようにすべきではないかという要請がある。この点については、技術的なものと、通信の秘密との関係で、調整に手間がかかった。そのような位置情報についての上記記のような位置づけがあったので、それを本人の承諾なしにプロバイダが第三者に開示できないのではないかということだったわけである。この点については、技術的に、指令台の操作で携帯電話等において位置情報（GPS 対応端末の場合は GPS 測位情報）を通知・取得することができるようにすべきであるとして、緊急通報受理機関へ位置情報を通知するための技術基準が定められた。

通信に関するリンクが、特定の場合に限定ではあるが、見直しつつある状況の一つということができるであろう。

4.3.5　自殺予告に対する対応

電子掲示板に、自殺の決行をほのめかす書き込みや他人に対して集団自殺を呼びかける書き込みがなされることもある。また、自殺予告を内容とする電子メールが送信されることもある。これらを目にしたものなどが、警察に通報をしたとしても、通報を受けた警察が、自殺を防止するために、それらの発言の送信者の氏名、住所その他の当該者を特定するための発信者情報を入手したいと考えていたとして、それらの発信者情報は、上記のように「通信の秘密」に該当すると解さていることがあり、警察としては容易に入手することができなかった。もっとも、「電気通信事業における個人情報保護に関するガイドライン」（前出）でもふれられているように、当該発信者情報の開示が緊急避難（刑法第３７条第１項本文）の要件を満たす場合には、開示行為の違法性が阻却されることになる。

もっとも、それらの発信者情報を保持しているプロバイダ等に対して警察から開示の要請があったとしても、プロバイダとしては、個々に対応していたのでは、どのような場合に、緊急避難に該当するのかという判断は、困難になる。そこで、「ガイドライン」を定めて、プロバイダ等における判断の参考にするということになる。このガイドラインが、「インターネット上の自殺予告事案への対応に関するガイドライン」である。これは、発信者の情報開示について、警察から照会がなされた場合について、その情報を開示することが緊急避難（刑法第３７条第１項本文）に該当する場合にどのような要件を考慮すべき

かとうい点について検討したものである。とくに、実際の自殺予告事案について「現在の危難の存在」を検討する際は、①発信された日時、②発信された情報の内容（自殺を行う具体的日時・場所の記載の有無、自殺する旨の意思の表示の有無、自殺する動機・手段等の記載の有無及びその具体性・実現可能性等）に加え、③当該書き込みがなされている電子掲示板等の性質、他の書き込みの内容等のインターネット上から得られる情報、④警察において１１０番通報者等から入手した当該発信者に関する情報（日頃からのインターネット上における自殺を伺わせる言動等）等の提供を受け、これらの情報を総合的に考慮することとされている。

これについても、法律が、匿名性（unlinkable）に関して、事案との関連性から、一定の譲歩を認めているものと位置づけることができるであろう。

総務省情報通信政策研究所（調査研究部）

http://www.soumu.go.jp/iicp/

〒100-8926　東京都千代田区霞ヶ関 2-1-2
中央合同庁舎第 2 号館 11 階
TEL:03-5253-5496　FAX:03-5253-5497