

携帯電話網における契約者 ID 通知に関する社会的・法的考察

情報セキュリティ大学院大学 博士後期課程

影井良貴

1. はじめに

2008年3月31日からNTTドコモによって提供が開始された「iモードID」[1]は、携帯電話で携帯インターネットのサイトを閲覧する際に、契約者回線に括り付けられた固定のIDが初期設定として通知されるものであり、この方式のセキュリティ上の問題が指摘されてきていた。[2][3] 同様のID機能は、auではサブスクライバ番号(現EZ番号)、SoftbankではユーザIDという名称となっている。(以降、これらのIDの総称として「契約者ID」を使用する。)本稿は、この提供により引き起こされ得る社会的脅威と、その原因について検討すると同時に、この方式の法的位置づけについて考察する。

2. 契約者 ID の特徴

契約者IDは、携帯電話の契約時に携帯電話会社により契約者回線単位に付与される。そして、携帯インターネットでサイトにアクセスする時に、サイト側の要求に従って携帯電話会社から通知されるが、その要求の有無、通知の有無に関して利用者は認識できない。端末から通知の可否の設定ができるが、アクセスの都度には行えず、すべてのサイトについて一括して常時通知するかどうかを設定するようになっており、初期設定では「通知する」になっている。また、同一契約の間では、同一の固定IDが使用され、その変更は原則的にはできない。

このような契約者IDによるサイトアクセスは、従来に比べ以下のように変わり、問題が生じている。(図1参照)

- ① 利用者は、毎回のID等の入力をせずに容易にサイトを利用できる。反面、知らないうちに自分を特定するIDが通知される。(利用者のID通知認識の問題)
- ② 契約者IDの通知の可否は、端末から設定変更することが可能である。しかし、その都度変更することは困難である。(利用者によるID通知管理の問題)
- ③ すべてのサイトに同一の契約者IDが通知される。(IDの通知範囲の問題)
- ④ 契約者IDは、基本的に契約期間中不変であり、別名での登録についても同一利用者であることを認識できる。反面、利用者により変更ができない(IDのライフサイクルの問題、利用者によるID通知管理の問題)

3. 想定される脅威

今回の契約者IDの特殊性は、前項の①から④のように集約でき、これらから容易に、少

なくとも以下の4点の脅威が考えられる。

(脅威1) 個人の行動監視

携帯端末からのサイトアクセスでは、必ず特定の個人を識別する固定のIDが通知されるため、それを追尾することにより、インターネット内での行動が監視できる。更には、最近、GPS等による実空間における位置情報に基づく周辺情報の提供というサービスが出現してきており、この場合はサイバー空間での移動ではなく、実社会での個人の行動監視が可能となる。また、その時の取得情報内容により、行動の目的も類推可能となる。

(脅威2) 個人情報の集約

同一のIDが長期間変更されずに使用されるため、特定個人に関する情報を大量に蓄積し集約しやすくなる。

(脅威3) プロファイリングの容易化

サイト間を跨って、このIDをキーに断片的な情報を収集することにより、詳細な個人プロフィールの明確化が可能となる。

(脅威4) 成り済ましの容易化

契約者IDの利用により、従来の本人による認証の手続きを迂回することが可能となるため、他人が携帯端末を操作することにより、成り済ましが可能であると同時に、表示内容による本来の利用者の利用状況が漏えいする。

4. 契約者IDに関する問題の根源

前述の契約者IDの特徴と想定される脅威から、更に本方式の問題点をまとめると、以下の2点に集約される。

- A) 契約者IDに関しては、その利用について、利用者が認識できず、且つ、主体的に取り扱えないようになっている。
- B) 契約者IDの物理的特性として、長期にかつ広範囲に亘って一つの固定のIDが使用されるようになっている。

これらの問題と脅威、犯罪との関連を図2に示す。

5. 契約者IDの法的位置付けについて

この契約者IDについては、通信の秘密という観点と個人情報保護という観点から、「電気通信事業法」と「個人情報の保護に関する法律」に関連がある。

5.1 電気通信事業法との関連

電気通信事業法第4条「秘密の保護」の観点から見た場合、契約者IDは、通信データに相当するものと考えられ、その場合には電気通信事業者が勝手にその情報を外に伝えてはならないことになっている。[4][5] しかしながら、本件に類似しているものとして「発信者電話番号表示サービス」があり、このサービスの提供開始に向けて同様の検討がされ、最

最終的にサービス提供が開始された経緯がある。

これについても通信の秘密との衝突が問題と認識されていた。しかし、「一般的には、発信者番号を外部に漏らすことは通信の秘密の侵害に該当するが、発信者が積極的に受信者に対して伝える意思を持っている場合は、元来利用者が通信内容の中にそれを包含して伝達することもでき、その代行を電気通信事業者が行っているという見解も成り立つ」[6]とされている。

今回の契約者 ID の送付についても、発信者電話番号表示に相当すると考えることができるが、ここで重要なのは、送信側が積極的に送信する意志を持っていることをどのように確認しているかである。

この「発信者電話番号表示サービス」の提供に際しては、更に以下のような条件が付けられた。[6][7]

- ① 相手に表示されることを認識できていること（このサービスを利用する企業は「サービス利用マーク」を表示し、本サービスを利用していることを明示することにした）
- ② その上で、契約者は表示されることに合意していること（回線毎ブロッキングと通話毎ブロッキングの2種類を提供し、その選択は利用者により指定するようにした）
- ③ その都度、その制御ができること（回線毎ブロッキングでも、186を付けてダイヤルすることにより通知可能とした）
- ④ サービス提供に不可欠な場合には、その旨と理由と利用方法と管理方法を明示すること。（通知された電話番号を記録する場合には、その目的と利用方法を明確にする）
- ⑤ サービス提供に不可欠ではない場合には、選択肢を用意すること。（通知する相手と通知しない相手を差別的に扱うことを禁止した）

これらの条件について、今回の契約者 ID の仕組み及び周囲のサイトの環境は、ほとんどの条件を満たしていない。従って、通信の秘密という面では、直ちに法に触れるわけではないとしても、従来のプライバシー保護の検討結果から大幅に外れている状況にあり、必ずしも問題がないとは言えないと考えるべきである。

5. 2 個人情報保護法との関連

個人情報保護法第 2 条の個人情報の定義から考えると、契約者 ID そのものは単なる英数字の列であり、そのもの自体を見ただけでは個人を識別できないという意味では、個人情報に当たらないといえる。しかし、電気通信事業の特別性を考慮した上で作成されたガイドラインには、第 25 条に発信者情報に関する規定がある[8]。

総務省から出されているガイドラインの解説において、この場合の発信者情報とは、発信者に関する情報であって、当該情報に含まれる電話番号、氏名、住所、生年月日その他の記述、個人別に付された番号、記号その他の符号、映像又は音声により当該発信者を識別できるもの、とされている。これに含まれるものとして、電話番号等が明示されている。

契約者 ID については、同様に契約単位別に付された記号・符号であるため、表現的には、発信者情報に含まれるものと考えられる。

次に、発信者の識別性について考える。電話番号は、電話の契約単位別に付される番号であるが、その番号が発信者を識別できるということを想定しているわけである。電話番号には氏名も住所も含まれていないが、その番号に直接電話をすることにより、その番号の契約者に到達できるという識別性があるといえる。

また、電話帳等を頼りに住所、氏名を調べるということも想定される。本ガイドラインでは、同時に第 29 条に電話帳または電話番号案内に関する規定があり、電話加入者の同意のもとで記載、案内を可としているが、この法律以前に存在する電話番号に関する情報については、何も触れていない。従って、それらの情報から照合ができる可能性は残っている¹。

一方、契約者 ID であるが、その情報をもとに、直接相手にコンタクトすることはできない。また、現状では、その ID を他の個人情報に結び付けるような仕組みも存在しない。このことから、契約者 ID は電話番号のような発信者識別性は有していないとなる。しかし、前述のとおり、契約者 ID と携帯電話番号の対応を作り出すことは容易であるため、それが世の中に広まる可能性を秘めており、その段階では、容易に発信者を識別できる可能性がある。

更に、我国の個人情報保護法は、OECD の「プライバシーガイドライン」[9] に基づいており、このガイドラインに立ち戻って、国際的な共通認識に合致しているかについて考える必要がある。

まず、「個人データ」については、第 1 条で、識別された又は識別されうる個人に関するすべての情報²、と定義されている。この定義から考えた場合、OECD の個人データは日本の個人情報に比較して、個人の情報が含まれているかどうかより、個人を識別できるかどうかによっていると思われる。これについては、欧米では、明らかに個人情報の定義が異なっており、本人到達性という観点で個人情報かどうかを判断しているとされている[10]。

ガイドライン第 7 条の「収集制限の原則」においては、「個人データ」の収集に当たっては「適法かつ公正な手段によって、かつ適当な場合には、本人に知らせめ又は同意を得た上で、収集されるべき」としている。また、第 13 条には「個人参加の原則」があり、この条文の精神では、自己に関する情報についてその本人が知らないということはないということが前提で、その扱いについて本人が参加できることを重要としている。

これらの点から見て、OECD のガイドラインとの整合性については、疑問が残るといえる。

¹ 個人情報の保護に関する法律施行令第 2 条によって氏名・住所・電話番号だけのリストは個人情報保護の対象にはならないとされているため、カーナビゲーションやその他サービス等における利用は、保護の対象とはなっていない。

² 原文では、"personal data" means any information relating to an identified or identifiable individual (data subject) となっている。

6. 契約者 ID の社会的機能について

この契約者 ID について、機能面から見た場合に、本当に個人を識別できないといえるのかどうかという点を再考する。

契約者 ID については、その ID 自体の通知が本当にその本人性を有していないならば、サイト側への通知も意味が無いものとなるであろう。しかしながら、各携帯電話会社は、この ID 自体の通知が個人の識別に役に立つことによってサービスの向上が期待できるとしている。このことから考えれば、表現はどうであれ仕組みとして、個人を識別できる程度の機能を有していることを認めているといえる。

もう一つ別の面から見ると、契約者 ID は、各利用者に対して固定的な番号を付与し、アクセス毎にその識別情報を付加するという作業を実施していることになる。この捉え方をした場合、今回の契約者 ID の方式は、民間企業が、個人の情報を集約するための統一番号を作り出しているのとらえることができる。現状の携帯電話の普及率及び個人利用率を考慮すれば、この仕組みは、民間会社による国民総背番号制度の創設ということができる。従って、このような情報を提供することの可否という観点でこの問題をとらえた場合、現行法の枠組み及び表現から見た場合の合法性議論だけではなく、このような環境を許容するか否かを議論する必要があるのかもしれない。

7. この検討から考えられる課題

以上の検討結果には、サイバー社会とリアル社会の結びつけ、及び個人情報保護法の 2 つの観点の課題が提示されていると考えられる。

7. 1 サイバー社会とリアル社会の結びつけに関する課題

今回の方式は、モバイルビジネスという限られた観点から検討された結果出てきたものと認識しているが³、今後の電子行政サービス等の普及等、サイバー社会全体に影響する話であると認識している。その意味で、今回の事例を適切に判断し対処することは重要である。現時点で、今回の仕組みを、ある意味反面教師として、リアル社会との結び付けによってサイバー社会を安全にする時に、注意すべき点をまとめると以下ようになる。

- (ア) 利用者の認識できる仕組みであること。
- (イ) 仕組みの利用は、双方の合意の上でその都度選択ができるようにすること。
- (ウ) 対応については、サイト毎に柔軟性を確保すると同時に変更も容易なものとする。

しかしながら、特定の場面では、同一人物であることを確認できることが必要であったり、特定の個人に到達できることが必要であったりすることも考慮する必要がある。

³ 実際には、青少年インターネット環境整備法の検討段階での議論が大きな影響を与えているとされている[2]。

これらの点を複合的に考慮しながら、リアル社会の情報や物体とサイバー社会のアイデンティティとの対応をつけ、それをベースにリアル社会における信頼の関係をサイバー社会に導入することにより、新たな危険を作ることなく、サイバー社会の安全の向上を図ることができるものと考えられる。

7. 2 個人情報保護法に関する課題

今回明確になったのは、個人情報というものをある時点で特定して、保護すべきか否かを判断するという形式の限界である⁴。業界を超えた情報の蓄積や流通、及びその将来的な変遷の可能性を含めた上で流通の可否についての判断を行う仕組みが必要であると考えられる。

8. 最後に

最後に、若年層が多い携帯電話の利用者に向けて、本人認証の ID やパスワードを入れなくても安全に利用できると思わせるような環境を提供することは、携帯の世界だけで可能な利便性や安全性を与えることであり、その外に広がる一般的なサイバー空間の危険性に対する認知力を奪うことになり、将来の大きな危険を生む土壌になると想定されることも付け加えておきたい。

⁴ 本質的には、OECD のガイドラインが利便性のための個人情報の流通という現象から個人のプライバシーを保護することを目的としているのに対して、我国の個人情報保護法は、個人情報の保護という手段に対する規制となっているため、ガイドラインのすべてを含んでいないということに起因していると考えられる。

(参考文献)

- [1] 株式会社エヌ・ティ・ティ・ドコモ (2008) 「『iモードID』の提供開始について」
http://www.nttdocomo.co.jp/info/notice/page/080228_00.html
- [2] 高木浩光 (2008) 「日本のインターネットが終了する日」 『高木浩光@自宅の日記』
<http://takagi-hiromitsu.jp/diary/200807.html>
- [3] 独立行政法人 産業技術総合研究所 情報セキュリティ研究センター (2007) 「『モバイルビジネス研究会』報告書案に対する意見」
http://www.soumu.go.jp/menu_news/s-news/2007/pdf/070803_5_15.pdf
- [4] 通信の秘密研究会 (高橋郁夫, 林紘一郎, 舟橋信, 吉田一雄) (2008) 「『通信の秘密』の数奇な運命 (制定法)」
- [5] 林紘一郎 (2005) 「情報メディア法」 東京大学出版会
- [6] 堀部政男編著 (1998) 「発信電話番号表示とプライバシー」 NTT 出版
- [7] 総務省 (1996) 「発信者情報通知サービスの利用における発信者個人情報の保護に関するガイドライン (平成8年11月29日)」
- [8] 総務省 (2004) 「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, 最終改正 平成17年10月17日総務省告示第1176号)」
- [9] OECD (1980) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1.00.html
- [10] 中田 響 [2006] 「個人情報性の要件としての識別可能性 ー日英米における執行当局の解釈の比較」 情報通信学会 第23回学会大会

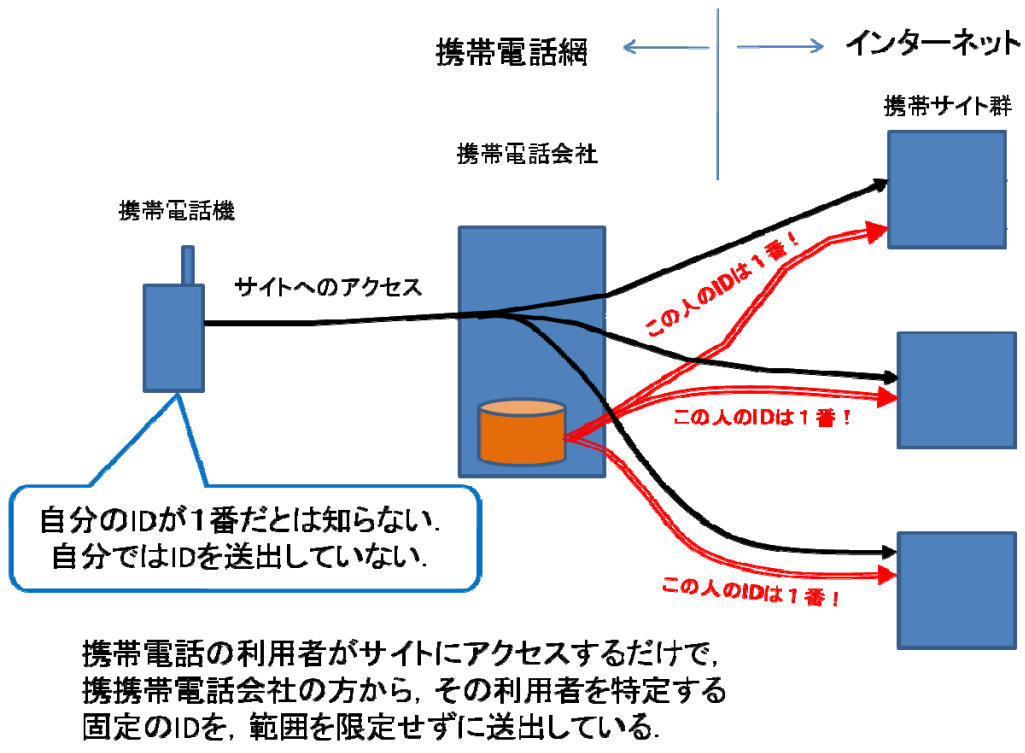


図1 契約者IDの状況

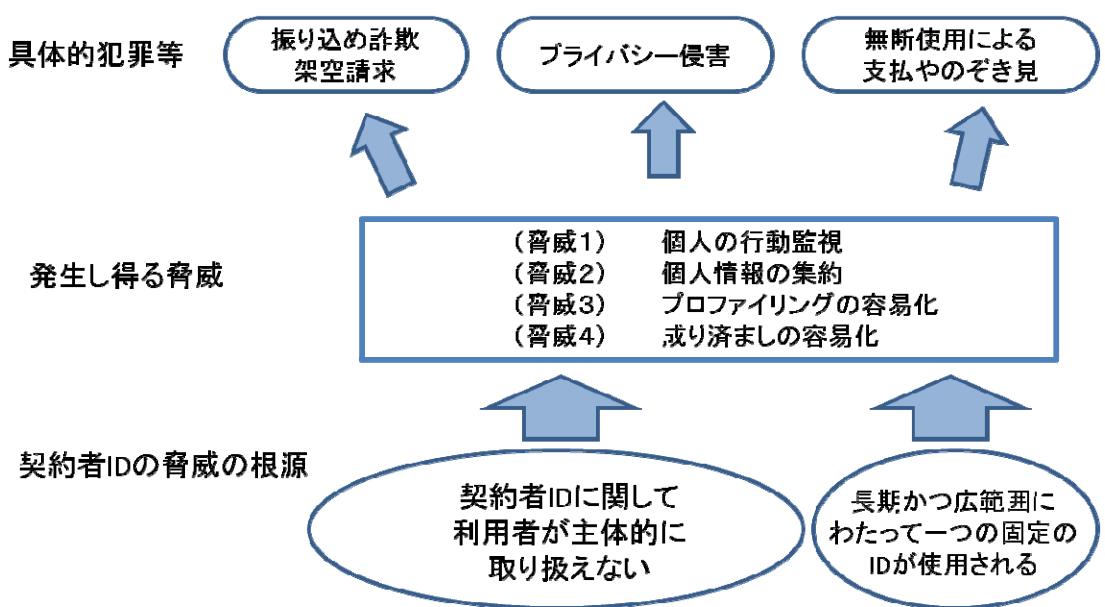


図2 契約者IDの特徴と脅威の関係