携帯電話端末のSIMロックの在り方に関する公開ヒアリング 資料

2010年4月2日

特定非営利活動法人東京都地域婦人団体連盟
事務局次長　長田三紀

目次

- SIMロックの解除はぜひ実現すべき
- 課題１ 「契約者固有ID送信に伴うプライバシー上の問題の解決」
- 課題２ 「２年毎拘束料金体系の改善」
- 課題３ 「盗難・紛失時の無権限利用の責任の切り分けと利用者への啓発」
- 課題４ 「課金時の仕組みの改善」
- 課題５ 「故障時の責任分担モデルの明確化」

SIMロックの解除はぜひ実現すべきです

- 高価格な携帯電話の端末
- キャリアを変えると使用できない端末が手元に残る
- 加えて新しいキャリアの端末を購入
- これでは、自分に適した料金体系のキャリアを選びたくても、最初に契約したキャリアに拘束されてしまう
- SIMロック解除で環境にも経済的にもやさしい
- しかし、幾つかの克服しなければならない課題がある

課題1 「契約者固有ID送信に伴うプライバシー上の問題の解決」
現状

- コンテンツ利用のための個人識別
- 契約者固有IDを自動的にWebサイトに送信して実現
- この仕組みがキャリア毎に異なる
- キャリアを変更すると新たなIDが割り当てられる
- コンテンツに対して契約のやり直しが必要で、不便

課題１ 「契約者固有ID送信に伴うプライバシー上の問題の解決」
SIMロック解除にあたって

- 利便性向上のため、IDの統一化が実施されるかもしれない

- しかし、IDの統一化はプライバシー上の問題がある

課題1 「契約者固有ID送信に伴うプライバシー上の問題の解決」

現状の問題点

- 契約者固有IDにはプライバシー上のリスクが指摘されている
  - 契約者個人を識別するものであり
  - 全てのサイトで共通のIDとなるため

資料1．資料2参照

- このようなIDの使い方は日本だけ
  - 欧米ではボイコット運動に発展しかねないため採用されない

例: 1999年、Intel社のPentium III（ペンティアムスリー）に対するボイコット運動（プロセッサシリアルナンバーに対して）

課題１ 「契約者固有ID送信に伴うプライバシー上の問題の解決」
今後の問題点と解決策

- 今後SIMロック解除でIDが統一化されればプライバシーリスクが増大
- ユーザは一生同じIDで識別されることになる
- この問題は技術的な解決方法があると指摘されている
  - 総務省「通信プラットフォーム研究会」の報告書
    （p.31脚註35、p.37等参照）
  - 総務省「認証基盤連携フォーラム」の取り組み
- しかし、このままでは、解決されるとは限らない
- 事業者の自由に任せておいた場合、解決されないおそれ
- 総務省が事業者に対し、適切な技術的解決を促すべき

課題１ 「契約者固有ID送信に伴うプライバシー上の問題の解決」
補足

- 住民基本台帳カードにおける解決
  - アプリケーションごとに別々のIDが用いられている
    （資料３参照）

- これに対して携帯電話の契約者固有IDは、全てのアプリケーションに住民票コードを使用しているようなもの

- 納税者番号、社会保障番号制、導入における解決策が政府で検討されていると聞いている

- 同様の解決が携帯電話にも必要

課題１ 「契約者固有ID送信に伴うプライバシー上の問題の解決」
補足２

技術的解決策としては、専門家から、次のような提案がある

- IDが数週間で変化するようにする
  （IPアドレスと同レベルまでプライバシーリスクを軽減）

- サイト毎に別々のIDを用いるようにする
  （cookieと同レベルまでプライバシーリスクを軽減、
  住基カードアプリと類似の対策）

- 利用者が自分のIDをいつでも容易に変更できる手段を提供する
  （住民票番号の変更に相当、cookieの削除に相当）

課題２ 「２年毎拘束料金体系の改善」

- ２年拘束を求める現状のキャリア提供の基本料金プラン
- ２年の切れ目に当たるとき以外に解約を求めると解約金が必要
- 自由にキャリアを変更する際に、不利益な条件である
  （１０年以上の契約で１年単位の割引が提供されるものもある）
- 初めの一定期間の拘束は残しても、それ以降は解約金なしで解約可能に

課題３ 「盗難・紛失時の無権限利用の責任の切り分けと利用者の啓発」

- SIMカードにパスワード設定をしていないユーザーが多数
- SIMロックが解除された場合、盗難、紛失時の無権限利用が拡大し、無権限利用の責任を無条件で回線契約者が負担させられることにならないかという懸念
- パスワード設定を利用者へ積極的に啓発
- 帰責事由の有無、内容、程度に即して無権限利用の場合の契約者の責任を切り分ける約款の改定が前提

課題４ 「課金時の仕組みの改善」

- ゲームサイトでのアイテム購入等の際、パスワード入力を要求するシステムへの統一が必要
- 端末の使用開始時の確認だけで、個別にパスワード入力を要求していないキャリアの場合、現実にアイテム購入しているのか、ゲーム上のお買い物ごっこなのか、初心者のユーザーには判断できにくい
- パスワード入力を要求し、リアルなアイテム購入であることを再認識させる仕組みが、絶対に必要
- 多種の仕組みの混在は、今後、自由にキャリアを行き来することになる消費者に誤認をまねく

課題５ 「故障時の責任分担モデルの明確化」

- キャリアの垂直型統合からビジネスモデルが大きく変更
- 不具合が起こった時の責任分担を明確にしておくことも必須条件
- SIMロック解除後に、通信や端末に不具合が起こった際、消費者は、初めの契約のキャリア（SIMカード提供事業者）、現在のキャリア、端末メーカー等、いったいどこへ連絡をするのが最適なのか、判断できない
- 次世代IPネットワーク推進フォーラムでの検討（資料４）
- 明確な形で消費者に責任分担モデルの提示が必要

IT+PLUS
IT新時代を見通すためのニュースサイト

参考資料1 日経ネット 2008年9月30日 楠正憲氏「携帯ID開放の危うさ・事件が起きる前に対策を」より

携帯ＩＤ開放の危うさ・事件が起きる前に対策を

携帯向けのコンテンツやサービスで、ユーザーを識別するための携帯端末の固有IDである「端末ID」が活用されるケースが増えている。パスワード不要の「簡単ログイン機能」などに利用されているほか、行動ターゲティング広告への応用も始まった。携帯ビジネスの基盤技術としても期待を集めているが、安全面の対策は十分だろうか。（楠正憲・マイクロソフト 技術統括室 CTO補佐）

▪悪質ユーザーの排除にも活用

端末IDはキャリアによって「iモードID 」(NTTドコモ)、「EZ番号」(KDDI)、「端末シリアル番号 」(ソフトバンクモバイル)など呼び方は異なるが、コンテンツを配信するサーバーから取得できる加入契約固有の番号を指す。当初は公式コンテンツに対してのみ提供する形式が主流だったが、現在はすべてのキャリアが勝手サイトを含めたすべてのサイト運営者に対してIDを開放している。ドコモが今年３月末にiモードIDをすべてのサイトで利用可能にしたことから、本格的な活用が加速している。

「iモードID」の提供開始を知らせるNTTドコモのニュースリリース

端末を認識したりユーザーの行動履歴を追跡したりするのは、サービスのカスタマイズ化や広告だけが目的ではない。携帯電話サイトの健全性を審査・認定する民間機関、モバイルコンテンツ審査・運用監視機構（ＥＭＡ）は、サイトを認定する条件として端末IDなどを記録し、管理することをサイト運営者に求めている。これは端末IDが悪質ユーザーの排除や、違法な書き込みなどを行った利用者の追跡に役立つからだと考えられる。

キャリアのゲートウェーサーバーを介する携帯電話の場合、一般にアクセス元のIPアドレスだけでは発信元を特定できない。プロバイダー責任制限法の定める開示請求を受けて悪質な利用者を特定するようなとき、携帯サイトでは端末IDの活用が最も現実的である。

▪懸念されるプライバシー問題

一方で、簡単に利用者を追跡できる端末IDを、加入者に何ら警告もなくサーバーに送信すること

に対しては、プライバシーの観点から懸念する向きもある。総務省の「次世代移動体通信システム上のビジネスモデルに関する研究会」は2001年6月の報告書で「ユーザーIDについての取り扱いルールを早急に確立する必要がある」と結論付けた。これに対し、当時NTTドコモとジェイフォン東日本 (現在のソフトバンクモバイル) は、加入者のプライバシー問題を理由に、IDの開放には慎重な姿勢を示していた。ここ数年での姿勢の変化は、勝手サイトの隆盛や、違法有害情報やネット犯罪への対策の重要性が高まり、ユーザーを特定する手段が求められてきたことが背景にあると考えられる。


国民生活センターは端末IDを悪用した料金請求の手口をウェブサイトで例示している

しかし、端末IDの悪用に対して十分な対策が取られているとは言い難い。端末IDそのものは個人情報保護法上の個人情報には当たらないが、例えば、コミュニティーサイトや占いサイトを装って本名、生年月日を入力させるなど、端末IDと個人情報とをひも付けることは技術的には容易に可能である。

今のところ各キャリアともすべてのサイトに同一の端末IDを送信しているため、サイトを越えたプライバシー情報の名寄せが可能となっている。実際すでに、端末IDを取得したかのように偽った架空請求の手口は国民生活センターが注意喚起している。今後はさらに進んで、悪意あるサイトで氏名、生年月日と端末IDとをあわせて取得し、架空請求サイトで、本人の氏名を表示するというように犯罪手口が高度化する可能性も指摘されている。
※参考：端末IDを悪用した料金請求の手口（例）

次ページ：▪PCで重ねてきたプライバシー保護対策

<< 前のページへ 1 [2] 次のページへ >>

● 関連記事
- ストリートビューのプライバシー問題、グーグル米担当役員が説明
- 新ブラウザー「クローム」はデザイナーの悩みの種
- 技術は世界レベル、目標はグーグル・ＰＦＩ西川社長――推奨エンジンに挑む人々(4)

● 記事一覧
- 日本が「幸福」な国になるために
- 日本の「韓国企業に学べ」ブーム、韓国の反応は・・・
- アクトビラ、３Ｄコンテンツの映像配信開始　10年夏から
- フェースブック、グーグル抜く　米国内のサイト訪問シェア
- 編集工学研究所、ネットで読書術指南　参加券を発売

IT+PLUS
IT新時代を見通すためのニュースサイト

インターネット：最新ニュース 更新：9月30日 10:40

<< 前のページへ [1] 2 次のページへ >>

▪PCで重ねてきたプライバシー保護対策

Windows Media Playerのプライバシー設定画面

PCでは加入者の追跡やログインの簡素化に、端末固有の番号ではなく、サイトごとにサーバーが送出して端末が保持するクッキー（cookie）などを利用することが一般的である。LANカードのMACアドレスやCPUのシリアル番号など、ハードウエアとしても端末ごとに固有の番号を持ってはいるものの、そのままインターネット上で利用すると利用者が意図しないかたちでサイト間での名寄せが可能となってしまうからだ。

事実、悪用可能な機能が登場するたびにセキュリティー専門家や消費者団体から脆弱性やプライバシー上の問題として指摘を受け、各ベンダーは迅速に対応してきた。有名なところではインテルが「Pentium III」で導入したプロセッサーシリアル番号 (1999年)、IPv6アドレスのプライバシー拡張 (2001年)、「Windows Media Player 9」の端末固有ID (2002年) での取り組み事例がある。

現行のクッキーを利用した利用者追跡でさえ避けたいという利用者からの要望は大きく、ベータ版の配布を開始したマイクロソフトの次世代版ブラウザー「Internet Explorer 8」では、クッキーや閲覧履歴を残さない「InPrivateブラウズ」を追加した。グーグルが投入したブラウザー「クローム（Chrome）」も、閲覧履歴やクッキーを残さないシークレットモードを搭載している。

こういった動きを受けてMozillaファウンデーションも、「Firefox 3.1」のプライバシー保護機能を充実させる意向を表明している。プライバシーを重視したネット閲覧は、再燃しつつあるブラウザー間競争で、最もホットなテーマの1つとなっている。

マイクロソフトの「IE8」に搭載されたInPrivateブラウズ機能

グーグルの「クローム」のシークレットモード機能

▪サービスの国際化で対応急務に

Windows MobileやiPhoneといったスマートフォン、携帯電話上のフルブラウザー普及など、PCと

モバイルとの垣根は埋まりつつある。モバイル端末の性能向上や、3.9G、4Gでのオール IP化、低遅延・広帯域化を受け、PCとモバイルとを技術的には区別する必要は遠からずなくなるのではないか。アップルのApp Storeはじめ、コンテンツ事業者が世界を対象にビジネスする機会も増えつつある。

コンテンツ事業者や端末ベンダーが国際的にビジネスを展開しようとすれば、否応なく世界に通用するセキュリティー・プライバシー水準が求められる。そうなるとPCと同様に、サイトを越えた名寄せを防ぐ技術的方策が必要となる。既に一部の移動端末がサポートしているクッキーや公開暗号鍵（PKI）の活用や、Open-IDなど新たな認証連携技術の応用も考えられる。

総務省が現在設置している「通信プラットフォーム研究会」でも、プライバシーについては活発に議論されている。総務省がホームページで公表している報告書の第一次案で「個人情報保護の観点から、ID情報管理については各個人が自らの意思で支配・管理できることが重要であり、そのための社会的ルールについても併せて検討が必要」との方向性が打ち出されたことは、国際的な趨勢に合致しており非常に心強い。さらなる具体的な検討が待たれるところである。

▪技術的保護手段も検討を

現行の端末についても端末IDの悪用を防止すべく運用見直しを検討すべきではないか。個人情報と端末IDとをひも付けて第三者に転売・譲渡することは、個人情報保護法の禁じる目的外利用に当たり、現行法で取り締まることができるとも考えられる。幸い今のところ、端末IDの悪用による犯罪被害は報告されていない。しかし反社会的勢力や海外事業者による悪用に対する実効性のある取り締まりを考えた場合、技術的保護手段も併せて検討すべきだろう。

既存のサイトとの互換性や悪質な利用者に対する追跡性は保ちつつ、サイトを越えた名寄せを防ぎ、IDを悪用された場合の被害を最小化することは技術的に難しくはない。例えば接続先ドメインごとに異なる端末IDを用い、悪用された場合にはリセットできるようにする方法などが考えられる。コンテンツ事業者や端末ベンダーの国際展開を促すうえでも、まずは日本のモバイルコンテンツ市場で、国際的に通用するセキュリティー・プライバシー水準を担保することが急務ではないか。

-筆者紹介-

楠　正憲(くすのき　まさのり)
マイクロソフト 法務・政策企画統括本部 技術標準部 部長

略歴
1977年、熊本県生まれ。ECサイト構築や携帯ネットベンチャー等を経て、2002年マイクロソフト入社。Windows Server製品部Product Manager、政策企画本部技術戦略部長、技術統括室CTO補佐などを経て2009年より現職

[<< 前のページへ](#)　[1]　2　次のページへ >>

参考資料2 日経ネット 2008年10月16日 高木浩光氏「行動ターゲティング広告はどこまで許されるのか」より

■「個体識別番号」を用いた行動追跡

もうひとつの新しい動きは、携帯サイト向けの広告において、行動追跡の実現手段として「個体識別番号」を用いるものが続々と登場しつつあることだ（参照：携帯向けも参入相次ぐ・広告ネットワークの戦い〔２〕）。

たとえば、この記事で紹介されているサノウ（東京・渋谷区）の「ネオアド」は、開発元の発表文で「今年の3月31日にNTTドコモが携帯電話番号毎に付与するiモード用のユニークなIDである『iモードID』を一般サイトに公開したことで、実現可能となりました」と説明している。

従来、NTTドコモの携帯電話では、契約者に固有の携帯IDはiモードの公式サイトにしか送信されなかった。一般サイトへは、端末の製造番号を送信する機能はあったが、これを送信する際には必ず確認画面が現れて、ユーザーが同意ボタンを押さなければ送信しない仕組みとなっていた。

表示するたびに確認画面が出てしまうのでは広告用途には使えない。それが、2008年3月末から携帯IDが一般サイトにも開放されたことでこのような広告システムが実現可能となり、続々と応用サービスが登場しはじめたのである。

携帯IDを用いた行動ターゲティング広告の仕組みはこうだ。仮に、どこのWebサイトを訪れても同じ広告会社が提供する広告画像が貼り付けられているとする。すると、携帯利用者はWebサイトを訪れると同時に広告会社のサーバーにもアクセスすることになる。

このとき、広告会社のサーバーにも携帯IDが送信される（図3）。広告会社は、携帯IDで人を識別しながらアクセス履歴を集計することで、同じ人がいつどこのWebサイトを訪れたかを知ることができる。これによりその人の嗜好を推定することができ、好みに合った広告を配信できるというわけである。

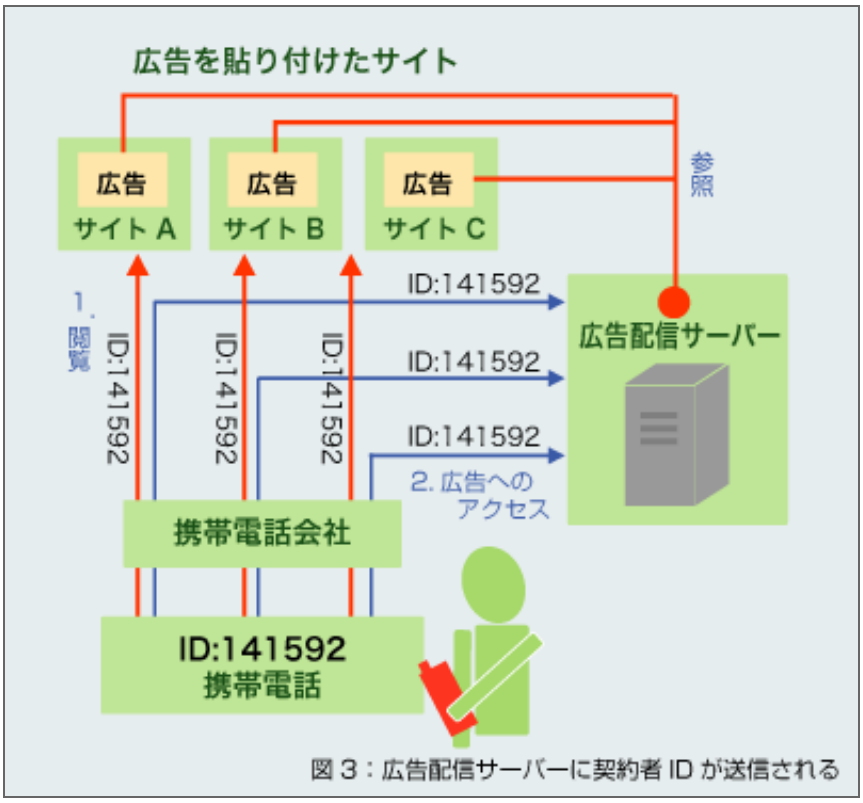


図3：広告配信サーバーに契約者IDが送信される

▪従来にはなかったプライバシーリスク

従来、一般のPCのインターネット（携帯電話ではなく）では、こうした行動ターゲティング広告を実現するためにクッキーを応用した手法が用いられてきた。「第三者クッキー」と呼ばれる方法で、広告会社が独自の固有IDを閲覧者に割り振り、そのIDごとに閲覧履歴を集計することで嗜好を分析している。

第三者クッキーは「トラッキングクッキー」と呼ばれることもあり、スパイウエア対策ソフトはこれをスパイウエアの一種として扱っている。米国では、このようなクッキー利用が消費者のプライバシーを侵害するとして、大手広告会社が2000年に集団訴訟を提起されるという事態にまで至っている。

クッキーについて言えば、プライバシーの問題は比較的小さい。なぜなら、クッキーは閲覧者側で自由に削除することができるので、削除するたびに広告会社による追跡はリセットされるからだ。また、第三者クッキーは近年使われなくなる傾向にあり、たとえばiPhoneでは第三者クッキーを拒否する設定になっている。

それに対し、携帯電話の携帯IDはクッキーのように削除することができない。いったん契約者に割り振られたIDは不変である。そのため、携帯IDを用いた広告が普及すると、広告会社により追跡される可能性は携帯電話を解約するまでの何年にも渡って続いてしまう。このことを利用者らは理解しているだろうか。

▪嗜好情報が売買されるおそれ

広告会社としては、効率のよい広告配信が目的であり、そのIDの人が具体的に誰なのかには関心がないかもしれない。しかし、ここで筆者が懸念するのは、ＩＤごとに集計された嗜好情報（サイトの閲覧履歴やそれを分析した結果など）のデータベースが第三者に販売されることはないのかという点である。

匿名のＩＤを住所・氏名にひも付けることをしなければ、個人情報保護法でいう「個人情報」には該当しないため、売ることは合法である。買う側もたとえばショッピングサイトなどで、すでに正当な手段で住所・氏名を取得している事業者ならば、嗜好情報を広告会社から買っても個人情報保護法には抵触しないと考えられる。その事業者が住所・氏名と同時に携帯IDも取得しているならば、入手した嗜好情報は携帯IDを使って住所・氏名と結合することができる。このような売買は合法かもしれないが、企業のビジネス行為として倫理的に許されるものだろうか。

ショッピングサイトに住所・氏名を提供する際、利用者はそのショップに陳列された商品について自分の関心を探られるのは、しかたのないこととして覚悟しているだろう。しかし、別のサイトで閲覧した嗜好情報についてまで、そのショップに把握されることについて、了解しているだろうか。

このような嗜好情報の売買は、従来の通常のPCのインターネットでは起き得なかったことである。なぜなら、第三者クッキーとして発行されるIDは、広告会社が独自に割り振ったIDであるため、ほかのサイトでは情報をひも付けて照合することができず、売買する価値がないからである。

つまり、広告に付随して収集される嗜好情報の売買という懸念は、国際的に見ても過去に例のないものであり、日本の携帯電話だけで今年になって始まりつつある事態といえるのだ。

▪日本の個人情報保護法の不備

あまり意識されていなかったことかもしれないが、インターネットの安心・安全は、主に英語圏での活発な議論によって淘汰の洗礼を受けた技術を採用することで実現されている。日本だけで独自に始まった携帯ＩＤ送信は、英語圏の批判にさらされておらず、他に類を見ない独自のプライバシーリスクを生み出してしまった。

携帯ＩＤや端末製造番号は、いわゆる「ワンクリック詐欺」業者らの間では「個体識別番号」と呼ばれている。個体識別番号を表示することでアクセスした人を特定したかのように見せかけ、料金を振り込めと脅す手口だ。NTTドコモが携帯ＩＤを一般サイトにも自動送信するようになったことは、ワンクリック詐欺の被害を増大させる危険もある。この問題については楠正憲氏も論じている。（参照：携帯ＩＤ開放の危うさ・事件が起きる前に対策を）

筆者は、そもそもこのようなＩＤ送信を携帯電話会社が開始したことに問題の原因があると考えているが、これを個人情報保護法で規制できていないところにも不備がある。2008年3月30日付の日経新聞の記事によれば、NTTドコモは「iモードID」の送信について「氏名やメールアドレスは含まれておらず、個人情報開示には当たらない」としているという（参照：ドコモ、携帯電話の「識別番号」・コンテンツ会社に通知）。

日本の個人情報保護法では、住所・氏名ばかりが守られ、肝心の個人の嗜好情報などのプライバシーが守られていない。住所・氏名だけなら他人に知られても問題がない場合も少なくないにも関わらず、この法律の影響で、常識的な利用さえ抑制されてしまうことが起きている。その一方で、他人に知られたくないはずの嗜好情報が、規制の網から漏れて売買される可能性が生じているのだ。

▪プライバシーポリシー明示の徹底を

これは、特定の広告会社が実際に集めた嗜好情報を横流ししていると指摘しているのではない。技術的には可能な状態にあることを指摘しているだけである。現時点でそれを行っている事業者が存在しないとしても、将来どうなるかはわからない。

嗜好情報の横流しを疑われたくない事業者は、それを行わないという約束をプライバシーポリシーに明示してはいかがだろうか。広告を掲載する側の事業者も、採用する広告会社がそのような横流しをしていないか確認する必要があるのではないか。

また、広告会社は横流しをしない方針だとしても、データ流出のリスクは少なからずあるだろう。一般的には従業員が持ち出すリスク、不正アクセスにより流出するリスクなどがある。第三者クッキーを用いた方式とは異なり、携帯IDを用いた方式では流出時の被害が無視できないほどに大きい。

流出時の被害を小さく抑えるために、長期間にわたる行動追跡を行わないことが望ましい。広告表示に必要な最小限の期間しか追跡情報を残さないようシステムを工夫するべきだろう。そして、その期間をプライバシーポリシーで明示することが望ましい。

政府も、こうしたインターネットを経由したIDによるひも付けという技術的可能性を踏まえて、個人情報保護のあり方を再検討するべきではないだろうか。

-筆者紹介-

高木　浩光(たかぎ　ひろみつ)
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 主任研究員

略歴

1994年、名古屋工業大学大学院博士後期課程修了。博士（工学）。同大助手を経て、通商産業省工業技術院電子技術総合研究所に転任。2001年、独立行政法人産業技術総合研究所に改組。2002年より同グリッド研究センターセキュアプログラミングチーム長。2005年4月より現職。専門は並列分散コンピューティング、プログラミング言語処理系、コンピュータセキュリティ。

参考資料3

住民基本台帳カード総合サイトより（http://juki-card.com/security/index.html）

「住基カード」のセキュリティ対策は？

住基カードの個人情報保護対策について

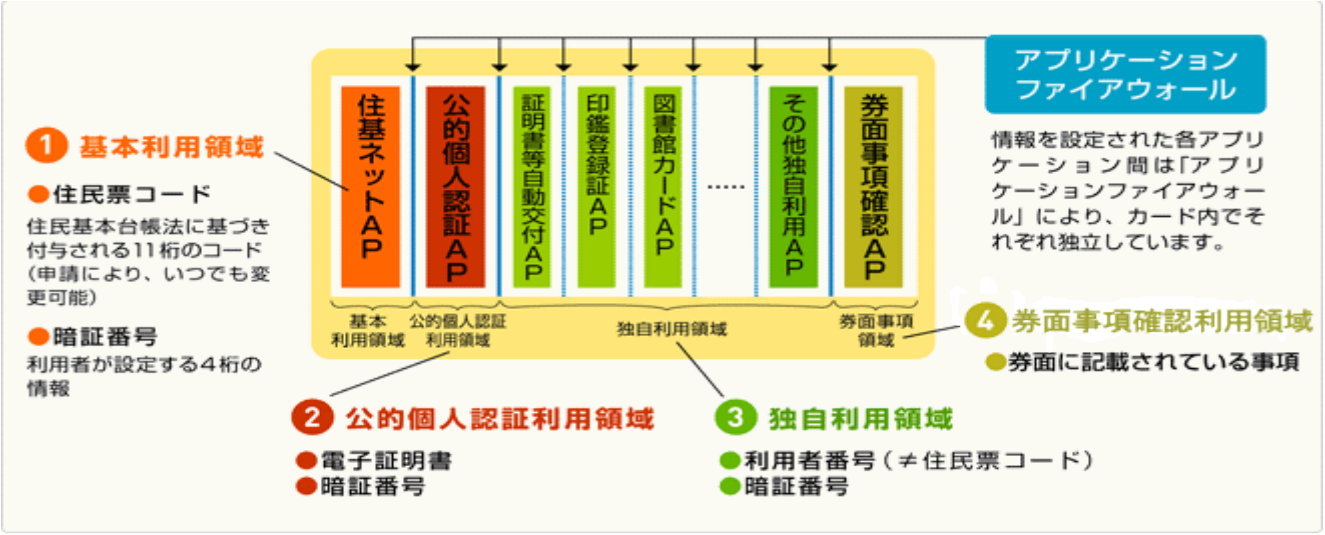
住基カードのセキュリティ対策として、システム面でも様々な対策を行っています。また、個人情報保護のため制度面からもプライバシー対策を講じています。

システム面でのセキュリティ対策

(1) IC チップ内には必要最小限の情報

市区町村の窓口で住民基本台帳ネットワークシステム（住基ネット）を使って本人確認をする際に利用する IC チップ内の「住基ネットアプリケーション（住基ネット AP）」には、「住民票コード」及び「暗証番号」のみしか保有していません。公的個人認証 AP には、「電子証明書」「暗証番号」のみ保有しています。券面事項確認 AP には、券面に記載されている事項のみを保有しています（写真なし住基カードは、有効期限及び写真なし住基カードである旨の情報のみを保有）。

＜ IC チップ部分のイメージ ＞



(2) 暗証番号の照合

住基カードの正当な持ち主であることを確認するため、暗証番号を設定していただきます。暗証番号は規定回数以上誤って操作するととロックがかかる仕組み(※)になっており、第三者が暗証番号を不正に知ることを防ぎます。
※ロックされた場合、住基カード交付市区町村で暗証番号の再設定手続をしなければ解除できません。
(なお、平成 24 年 7 月までに、他の市区町村に転出をしても継続して同じ住基カードを利用できるようになった後は、その時お住まいの市区町村で暗証番号の再設定が行えるようになります。)

(3) 不正アクセスへの対応

住基カードとシステムがそれぞれ、正当な相手であることを確認後、住基カード内の該当情報にアクセスできるようになっており、不正なアクセスから住基カード内情報を守るとともに、偽造カードの使用を防ぐ仕組みになっています。

(4) アプリケーション間の独立性の確保

「アプリケーションファイアウォール」により、カード内で該当する AP(アプリケーション)情報にアクセスした場合でも、他の AP(アプリケーション)情報にはアクセスできない構造になっています。例えば、図書館カードとして住基カードを使用している時に、基本利用領域、公的個人認証利用領域及び券面事項確認利用領域の情報が読み出されることはありません。

(5) IC チップ自身の不正防止機能

IC チップ内の情報を不正な方法により読み出そうとする場合、IC チップ自身が防御するための性能を持っています。無理に IC チップをこじ開けたり、チップの中身を解析しようとしても、読み取れないようになっています。

※これら不正防止策を耐タンパー性と言います。詳しく知りたい方は「耐タンパー性の概要(PDF 形式　116KB)」を参照してください。スキミング等の不正な方法による情報の読み出しを防御します。

制度面でのプライバシー対策

- 市区町村が、取得を希望する住民の申請に基づき交付します。
- 制度上、市区町村が条例で定めるサービス以外は、提供できないようになっています。
  また、どのようなサービスを受けるかは、住民の選択となっています。

参考資料4

次世代IPネットワーク推進フォーラム　HPより（http://ngnforum.nict.go.jp/）

設立趣意

「いつでも、どこでも、何でも、誰でも」ネットワークに簡単につながるユビキタスネット社会の実現を目指し、 2004 年 12 月に総務省は「u－Japan 政策」を策定しました。「u－Japan 政策」では 2010 年までに、日本が最先端の情報通信技術(ICT)国家として世界を先導することを目標として掲げています。このようなユビキタスネット社会実現のための最重要課題の一つとして、次世代ネットワーク（NGN）の構築が挙げられます。次世代ネットワークの構築には、要素技術の研究開発、相互接続試験、実証実験等の技術的な検討の他、技術基準の策定、国際標準化等の政策的な検討が必要となります。特に IP ベースの次世代 IP ネットワークの構築は急務であり、これを達成するために産学官の連携を強力に推進するフラグシップが不可欠であるという認識のもと、「次世代IPネットワーク推進フォーラム」の設立を企画いたしました。このフォーラムにおける活動を通して、日本の国際競争力の源となるネットワーク技術の創出に多大な貢献ができるものと確信しております。通信事業者、ベンダー、学識経験者、アプリケーション制作者等、産学官の幅広い分野から本フォーラムにご参加いただき、次世代IPネットワークの相互接続試験、実証実験に総合的に取り組むとともに、研究開発を戦略的に推進していきます。また、本フォーラムで得られた結果を踏まえ、技術基準の策定、国際標準化に寄与していく決意であります。

フォーラム会長　齊藤　忠夫