

月刊セキュリティ研究

検事・裁判官も務めた現役弁護士が語る法律問題 参議院議員・弁護士 **小川敏夫**

バーコードからバイオメトリクスまで 社団法人日本自動認識システム協会 **宇田川荘二**
自動認識選択の時代 専務理事

特集

自動認識技術の新潮流

9

2005

信和エンジニアリング 日本原子力防護システム
コトヴェール 日立ソフトウェアエンジニアリング
スタンダード シーモン チェックポイントシステムジャパン

Security
Specialist
Association

注目の企業紹介

株式会社コンフォート

Info

- NPO法人 NBCR対策推進機構
- American Society for Industrial Security
- 電子商取引安全技術研究組合
- NPO法人 日本情報安全管理協会
- 日本消費者連盟 食の安全・監視市民委員会
- NPO法人 国際情報安全保障研究所

連載

愛しのアクセスコントロール
SECURITY UPDATE
防犯グッズウォッチング

巻末
特集

セキュリティ業界有力企業一覧

個人情報と カード社会のセキュリティ

特定非営利活動法人 日本情報安全管理協会
専務理事・事務局長

佐藤 健次

広がるカード社会とそのリスク

高度ネットワーク社会の到来によって、人はインターネットという大きな網を通じて、様々な情報を手に入れ、その情報を利用したくさんの事ができるようになった。

しかしながら、そのようなネットワーク社会になりつつある現況の中で、利便性を追求していく一方で、その技術最優先の弊害により、如実に現代社会にも大きな危険性が潜んでいる事象が現れ始めてきているのは特筆すべきである。

現在、カードは生活になくてはならないものとして、国民の生活に浸透してきている。キャッシュカードやクレジットカードに限らずさまざまなものがカードとなり、利用者の利便性を高めている。たとえば、JRスイカのような電子マネー、住民基本台帳のような本人カード、さらには小売販売店などのポイントカード、会員カード、最近では航空会社のマイレージカードなどがそれである。様々な情報をカードに記録しておくことによって、消費者に提供するサービスはかなりの広がりを見せている。

しかしながら情報を記録させる媒体である以上、データの書き換えが当然可能であり、そこを付け狙いデータの改ざんや、情報の抜き取り（スキミング）がなされ、犯罪に悪用されるリスクが介在していることを忘れてはならない。

例えば、十数年前にテレホンカードの偽造が、「偽造カード犯罪」として社会問題になったように、カードはいつ偽造（複製）カードが作られてもおかしくないの

である。

図1をごらん頂きたい。現在の書き換え可能な記録媒体のカードはおよそ3種類に集約されている。

まず、磁気ストライプによるカードであるが、これがいわゆる磁気カードと呼ばれるものであり、記録できる情報量が少ないため、複雑なセキュリティをかけることが困難であり、比較的簡単に偽造（変造）することが可能とされている。

最近ではJRスイカをはじめ、多くのカードがICチップを導入したカード、すなわちICカードに移行し始めている。これらは、ICチップそのものがCPUとして機能し、記録できる情報量も磁気ストライプの数百倍となり、磁気カードとは比較にならないほど強度なセキュリティを施すことが出来る。

現代では（2005年8月現在）ICカードの研究・開発も進み、様々な分野で導入され始めてきている。しかしながら、読み取り端末側の整備が追いついておらず、現実には、磁気とICを併用したタイプのカードが多く流通しているのである。

このようにカードは、比較的単純な規格に、記録する内容を様々な形に変え、利用されているのが現状である。そのため、その仕組み（セキュリティの内容）がひとたび漏洩してしまえば、偽造されてしまう可能性は十分にある。すでに、磁気カードの偽造に関しては犯罪集団にとってはかなり簡単にできてしまうようである。これは重大なリスクであると考えてよい。

さらにもう一つの観点からカードを区別するとカードは2種類に分けることができる。

個人情報に類するものが記録されているカードとそうでないカードである。例えば、JRスイカのようなものは汎用性を第一に考え、電子マネーとしての可能性を広げる為に、誰でも利用できるカードとして、使用の際に本人確認をする必要がない。つまり、金額のデータだけが記録されているカードといえる。一方で、クレジットカードや住民基本台帳ネットワークのカードなどは、必ずなりすまし等を防ぐ為に本人確認のための個人情報すな

| | 磁気(ストライプ)カード | 磁気・IC併用カード | IC(チップ内蔵)カード |
|-----|--|---|---|
| 特徴 | <ul style="list-style-type: none"> 磁気ストライプによってデータのやり取りを行う。 記録できる情報量が少ない。 カードリーダーは磁気ストライプを読み取るタイプ。 | <ul style="list-style-type: none"> 磁気ストライプとICチップが併用されているカード。 データのやり取りは、磁気ストライプが読み取り専用、ICチップが読み取り専用である。ICで実行される。 | <ul style="list-style-type: none"> ICチップのみでデータのやり取りを行う。 記録できる情報量は磁気ストライプカードの数百倍。 電磁波によってデータのやり取りを行うことができる。 ICチップそのものがCPUに入っている。 |
| 用途 | <ul style="list-style-type: none"> キャッシュカード、ポイントカード、デビットカードなど。 | <ul style="list-style-type: none"> キャッシュカード、クレジットカード、ポイントカード、デビットカードなど。 | <ul style="list-style-type: none"> ICチップのみでデータのやり取りを行う。 記録できる情報量は磁気ストライプカードの数百倍。 電磁波によってデータのやり取りを行うことができる。 ICチップそのものがCPUに入っている。 |
| リスク | <ul style="list-style-type: none"> 磁気情報を読み取りスキマーでスキミングが可能。 磁気情報は複製不可。 | <ul style="list-style-type: none"> 磁気情報を読み取りスキマーで読み取りが可能。 複製型スキミングが技術的には可能。 | <ul style="list-style-type: none"> 複製型スキミングが技術的には可能。 |

図1 カードの種類（日本情報安全管理協会 作成）

わち、カード番号等がどうしても含まれてしまう。前者のカードは、偽造テレホンカードのような変造カードが作られてしまう可能性があり、後者のカードは、個人情報を含む全く同じ偽造カードが作られてしまうリスクと共に、その個人情報がカード犯罪以外の犯罪に使われるリスクも出てきてしまうのである。

カードと個人情報

個人情報保護法が完全施行され、国民の関心は個人情報を如何にして守っていくかに対して、敏感に反応しているようであるが、個人レベルになると決してそうでもない。図Ⅱにあるように個人情報（個人生活情報）から引き起こされる犯罪は意外なほど多い。

今年をはじめ、まだ記憶にあたらしいスキミングによる偽造キャッシュカードの被害も、暗証番号（便利な個人認証サービス）という個人情報（個人にしか知りえない情報）が漏洩することによって引き起こされてしまった。つまり、スキミング（偽造カード犯罪）も、これらの多くの情報漏洩から引き起こされる犯罪の中の一つなのである。例えば、住民基本台帳のカード情報が外部に漏洩した場合、本籍地等はもちろんのこと家族構成まで犯罪集団に知られてしまい、オレオレ詐欺や、架空請求、ストーカーなどの犯罪としての情報源として扱われてしまう可能性すら考えられる。

日常生活の中から思わぬところで情報は漏洩しているものである。図Ⅲをご覧頂きたい。個人生活情報の漏洩ルートは、どのように漏れているのかがわかると思う。盗聴・盗撮を始めさまざまな漏洩ルートが考えられる。最近では生活ゴミ等は家庭用シュレッダーなどが普及し、ダイレクトメール等もきちんと処理をしてから捨てられている傾向にあるのは良いことであるが、一方でソーシャルハッキングといわれる手口が様々なところで聴

かれるようになった。電話で銀行員を装い、暗証番号を聞きだすなど手法がそれである。

これらの漏洩ルートはほんの一部を列挙したに過ぎず、日常的な会話の中からも、意外と重要情報は漏洩しているものである。常日頃から用心して生活を営む必要性を考えなくてはならない。

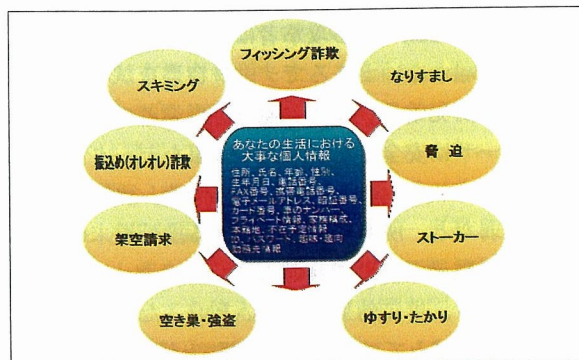
カード社会に必要とされている文化

残念ながら日本国民は、「キャッシュカードやクレジットカードはお金」という意識は非常に低い。これは歴史的観点から察するに、現金による商取引が主流であった我が国では、到底欧米のようなセキュリティ意識の高いカード文化が根付くはずもないのである。

これほどのカード社会が進む現代では、利用者がカードのリスクをリスクとして正しく認識し、発行者と利用者双方が助け合いながら犯罪に対して、その防止対策（リスクヘッジ）に努めていかなければならない。例えばICカード化が進んだとしても、それを使う人間社会の成熟度によって、便利なツールとなるか、犯罪の温床となるかが決まるのである。

「便利」「快適」などわれわれにとって一見都合の良いカード社会においてカードに記録されている個人情報を危険にさらす恐れをはらんだまま、あらゆる技術先行が日進月歩の勢いで、我々の生活に浸透して来ている。

私も日本人であるので性善説を信じてはいるが、カード社会では「人間は悪いことをするものだ」という徹底した性悪説の基にセキュリティを構築していく必要があるのではないだろうか。事故や犯罪のきっかけはいずれも源をたどれば人間である。ICカード化を進めていくと共に、リスクの「予防・予知」を考え、ヒューマンエラーを限りなくゼロにするための仕組みづくりが今求められている。



図Ⅱ 個人生活情報から引き起こされる犯罪
(日本情報安全管理協会 作成)



図Ⅲ 個人生活情報の漏洩ルート
(日本情報安全管理協会 作成)