くらしのネット化に伴うセキュリティ課題の調査研究報告書

電子商取引推進協議会
財団法人日本情報処理開発協会 電子商取引推進センター

経済産業省委託調査

平成１６年度不正アクセス行為等対策業務

くらしのネット化に伴うセキュリティ課題の調査研究報告書

平成１７年２月

電子商取引推進協議会
財団法人日本情報処理開発協会
電子商取引推進センター

この報告書は、平成１６年度受託事業として（財）日本情報処理開発協会電子商取引推進センターが経済産業省から委託を受けて、電子商取引推進協議会（ECOM）の協力を得て実施した「不正アクセス行為等対策業務（モーバイルセキュリティに関する調査研究）」の成果を取りまとめたものです。

序

本調査研究は、社会のブロードバンド化が急速に進み、家庭内においても情報家電を初め様々な機器がネットワークに接続されるようになり、様々な端末から管理・操作できるような時代が到来しつつある中で、くらしのネット化（情報家電や住宅機器がネットワークに接続され遠隔操作されるような状況）に相応しいセキュリティ（安全性）を確保するためには、どのような対応策を取れば良いのかについて調査研究することを目的としている。

昨今、インターネットを利用した不正行為や事故が連日マスコミを賑わせており、次々と繰り出される新手の手口の悪質化と、それによって被る被害の額ともに増大傾向にあり、深刻な社会問題になりつつある。

ビジネスの世界では専門のシステム管理者が企業システムの防衛に当たっており、企業活動に支障のないようセキュリティの確保に万全を期しているが、くらしの世界ではまだまだセキュリティに対するユーザーの心構えと対抗策が脆弱である。くらしの安全を守るためには、潜在する問題点や課題を早急に明確化し、解決策や対抗策を実現・整備していく必要がある。

今年度はその第１ステップとして、まず、くらしのネット化におけるセキュリティの現状を調査し、セキュリティ確保に関する課題の洗い出しと整理を行った。すなわち、くらしの中で利用可能になった、決済を含む便利で快適なネット機能について紹介した後、ネットワーク犯罪の諸相およびそれらの対応策・解決策についてまとめた。

ネットワーク社会における利便性とリスク（危険性）は盾と矛の関係にある。どちらにも人間系が介在する以上、根本的な解決策は存在しない。さらに我々一般生活者は複雑で高度なネット犯罪には殆ど無防備である。そのような状況下では、犯罪者の動向を常時監視し、新手の手口が使われれば直ちに対抗策を編み出して関係者に周知徹底してくれるような能力と体制を備えた、生活者のための機関が必要になるだろう。

次年度があるとすれば、今年度の基礎調査の成果をもとに、くらしのネット化におけるセキュリティ確保はどのような姿になるのかについて、技術面・運用面・法制度面など、あらゆる角度から総合的に検討を深め、生活者のためのガイドラインを取りまとめることとしたい。

本報告書がネットワーク犯罪の多様な実態を知り、問題点・課題を明らかにしたり、対応策を考えたりする上で参考になれば幸いである。

最後に本テーマの活動にご協力をいただいた関係者各位に対して厚く御礼申し上げる次第である。

平成１７年２月

財団法人日本情報処理開発協会
電子商取引推進センター
電子商取引推進協議会

注記１.）本報告書に記載された商品・サービスの名称は、商標または登録商標の場合があるが、TM・(R)などの記載は省略している。

注記２.）本報告書に記載された商品・サービスは単なる事例紹介にすぎず、当該商品・ サービスの利用を電子商取引推進協議会として何ら勧奨するものではない。

注記３.）本報告書に掲載された内容は、特に断り書きのない限り調査時点での情報を基にしている。電子商取引推進協議会は、その後の当該内容の変更に伴う本報告書の改版義務を一切負わないものとする。

注記４.）本報告書の利用によって生じたいかなる損失についても、電子商取引推進協議会は一切の責任を負わないものとする。

目　次

参 考 資 料

1. フィッシング関連 99
2. スパイウェア、アドウェア関連 103
3. ホームネットワーク、ネット家電関連 104
4. ウイルス、ワーム、スパム関連 105
5. クロスサイトスクリプティング関連 108
6. その他 108

図 表 目 次

執筆者リスト

はじめに

インターネットの発展と同期して企業では社内ＬＡＮがなくてはならない通信環境となり、有線の電話による会話から文字によるメールに取って代わり、忙しい現代社会ならではのコミュニケーション手段となり、また郵送やファックスに代わり電子決済データが飛び交う時代に変貌をとげて来ている。また、社内ＬＡＮを利用してファイルサーバ、文書サーバ、基幹業務用サーバ等の各種サーバを構築して社内のあらゆる業務が電子化される傾向に向かい、ますます注文書や在庫リストなどが紙である必要性がなくなりつつある。

一方、家庭、即ちくらしの世界ではインターネットへの接続環境が続々と整備され、電話線をそのまま使ったＩＳＤＮでの 64Kbps の通信速度を以って、日本が世界に誇るデータ通信の幕開けと思っていた途端、ＡＤＳＬやＣＡＴＶの出現により 100Mbps の世界があっと言う間に身近になり文字の通信から画像、音楽の相互通信等への変革がなされた。

また、くらしにネットワークが入り込んで来たと同時に家庭に居ながらにしての決済、即ちパソコン画面で商品を確認して購入ボタンをクリックすることで注文処理がいとも簡単に進められる環境になって来た。

本調査研究報告書では、くらしを中心として快適で便利な機能についての洗い出しを行い、また今後整備されるであろう技術動向についても網羅した。

そして、その裏に潜む問題点について調査の深堀を進め、くらしにおけるセキュリティについて切り込むことができた。しかしながらセキュリティの調査を進める過程ではかなり生々しく犯罪の紹介や手口の詳細まで踏み込んでしまい、ネットワークは怖いものだと言う意識を強調し過ぎしてはいないかと言う心配をしている所である。逆に、それだけ現在のネットワーク環境は脅威にさらされており、正しい知識と対策を余儀なくされているのも事実である。本書がこれら脅威に立ち向かうための啓蒙書として活用されれば幸いである。

1. くらしと快適なネットワーク

くらしの中に急速にネットワークが入り込んでから久しい。社団法人電子情報技術産業協会（ＪＥＩＴＡ)が平成 17 年 1 月 26 日発表した 2004 年のパソコンの国内出荷台数は、前年比８％増の 1145 万 1000 台で 2 年連続の増加となり、家庭でのパソコン普及率も図 1-1 のごとく 2004 年 3 月で既に 80%近くに達している。

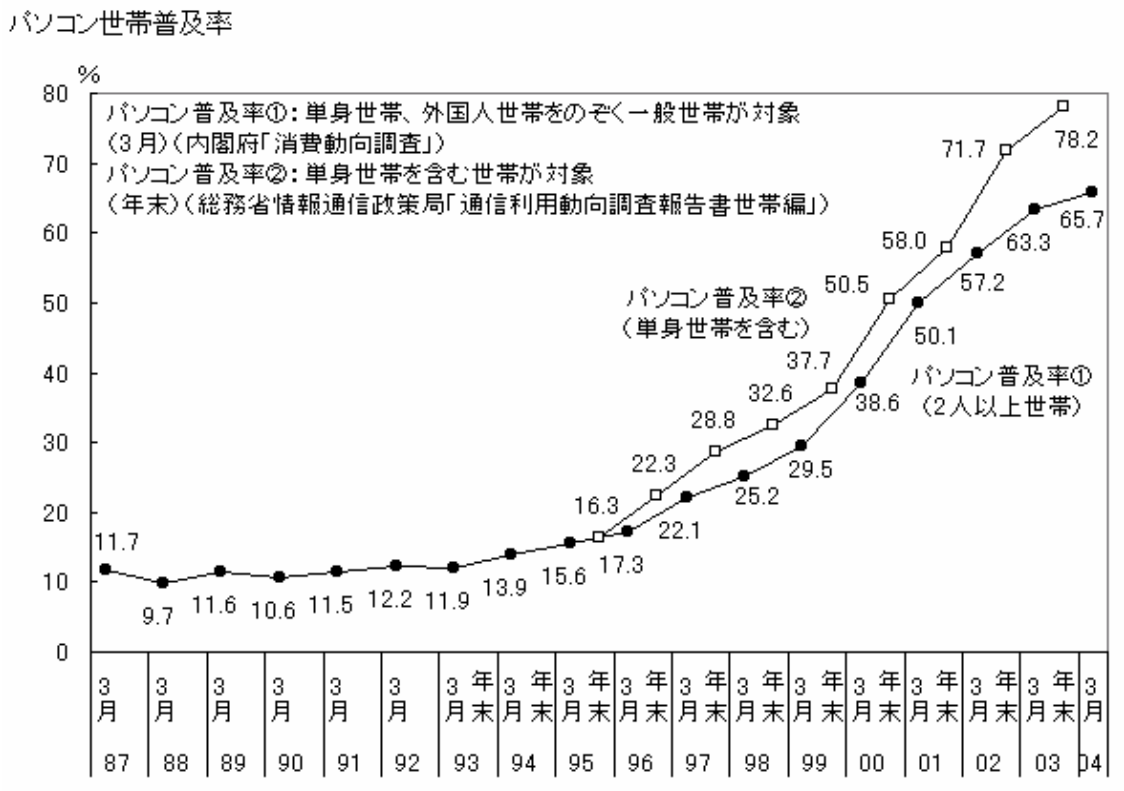
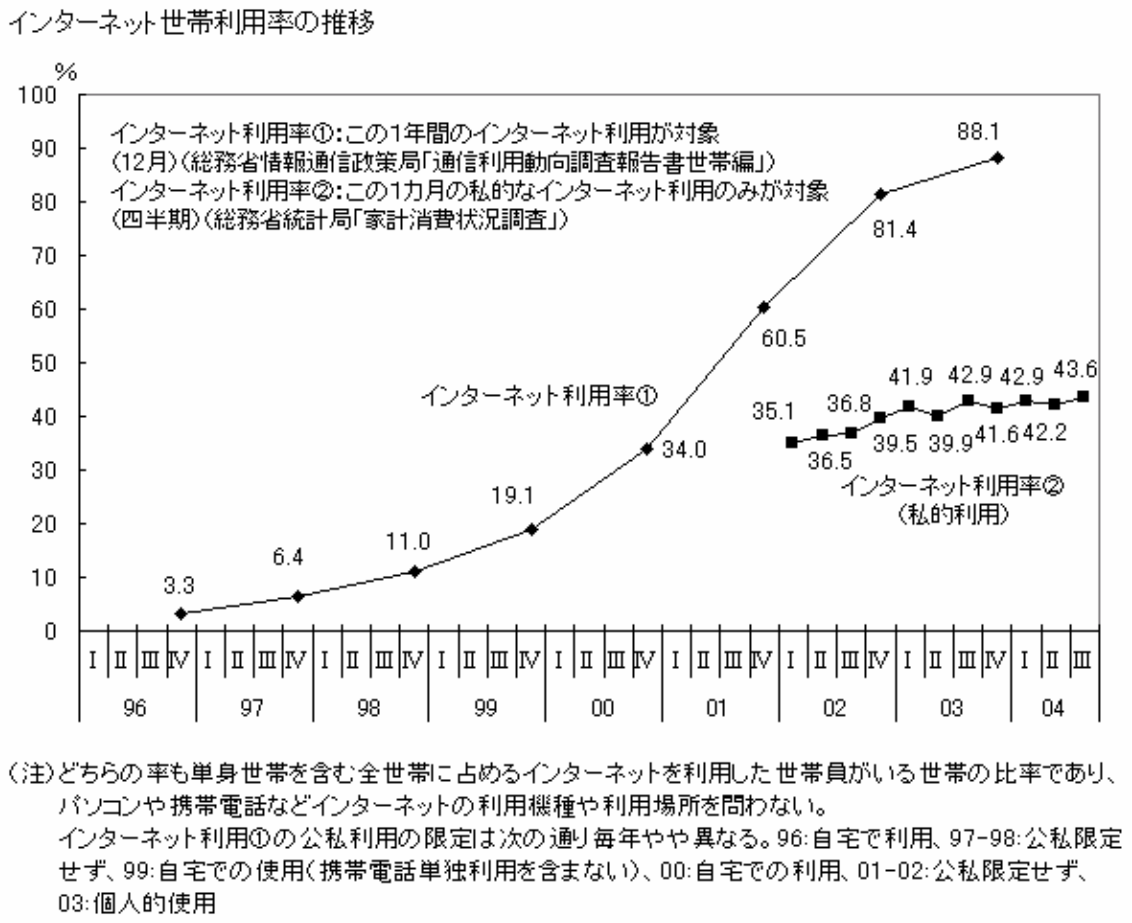


図 1-1　パソコン世帯普及率（アルファ社会科学株式会社ホームページ
http://www2.ttcn.ne.jp/~honkawa/index.html より抜粋）

またこれら家庭におけるパソコン保有者のインターネット接続普及率を見ると図 1-2 のごとく 2004 年第 3 四半期で既に 44%近くに達している。

これは約１年前のデータであるが最近は格安のＡＤＳＬやＢフレッツ、光ファイバ通信等々が出回り更に普及率が向上しているものと思われる。



(注)どちらの率も単身世帯を含む全世帯に占めるインターネットを利用した世帯員がいる世帯の比率であり、パソコンや携帯電話などインターネットの利用機種や利用場所を問わない。
インターネット利用①の公私利用の限定は次の通り毎年やや異なる。96:自宅で利用、97-98:公私限定せず、99:自宅での使用(携帯電話単独利用を含まない)、00:自宅での利用、01-02:公私限定せず、03:個人的使用

図 1-2　インターネット世帯利用率の推移（アルファ社会科学株式会社ホームページ http://www2.ttcn.ne.jp/~honkawa/index.html より抜粋）

この驚異的な普及率の伸びには何らかの理由があるはずである。この章では特に家庭即ちくらしに焦点を絞ってパソコンとネットワーク環境により便利で快適な利用方法について分類分析することとした。

1.1　便利な機能

ここではネットワークを介してくらしと直結した便利な機能について述べることとし、機能の内容や利便性、またその機能を使うことにより発生するトラブルなどについて紹介する。ただし、トラブルの詳細内容について別項で説明しているものは簡単な紹介程度に留めることとした。

1.1.1　電子メール

これはパソコンや携帯電話を保有している殆どの人の生活圏に入り込んでおり多くの説明は要さないと思われる。強いて追加するならばパソコンによる電子メールは勿論であるが、携帯電話による画像付きの電子メールが近年の特記事項として挙げられるのでないだろうか。

それは今現在の状況、例えば、レストランでの食事風景、花火大会の様子、一緒に出かけた仲間の写真等、電子メールを送る相手との今現在を共有するツールとして画像は有効である。特に最近は動画による画像送信が簡単にできるようになった。

電子メールの送信先が悪意ある者の場合については、ウイルスやスパイウェアが添付ファイルとして送られてくるケースが後を絶たない。またデマメールや振り込め詐欺として使用される脅迫メール、過去に現実の世界で発生した不幸の手紙の電子メール版など問題も多い。

1.1.2 買い物（ネット通販）

最近急激にその利用が伸び、利便性が高く期待されているものに買い物（ネット通販）がある。

欲しい商品を検索機能により探しだし、その商品を取り扱っているホームページにアクセスし、表示されているその商品の説明、値段、写真や動画による外観などを見て気に入れば注文する。続いて注文者情報である住所や氏名などを入力し、支払い方法を指定することにより、その店に足を運ぶことなく好きな時間に商品の注文が可能となる。また購入するかしないか物を見てから決定しようと考えている場合などは、店員との煩わしい会話も不要となり、特に会話を好まない最近の傾向からは非常に便利な機能と言える。

またネット通販の対象となる商品としてはＣＤ、書籍、日用雑貨を初め、生活に必要なものは殆どと言って良い位揃っている。

また支払いの方法も最近は多種多様となり、クレジットカード、デビットカード、プリペイド支払い、宅配便による代金引換決済、現金振込みなどがあって、注文者にとっては支払い形態が選べる分、買いやすくなっていることも事実であろう。

しかしながら、購入した商品が希望するものと違ったりするといったトラブルも多い。

1.1.3 売り買い（ネットオークション）

最近ではインターネットサービスプロバイダ（ＩＳＰ）やその他企業がネットオークションや逆ネットオークションを開催する様になった。

ネットオークションは売りたい商品や物をそのサイトに登録してオークションの締め切り日時を設定して、その間に買いたい人からの希望金額を入力（入札）してもらい締め切り時点で一番高い金額の人に決定（落札）し取引が成立する仕組みである。これらで取引される商品では中古車、ゴルフクラブを初め、その他日用雑貨に至るまで幅広い。

一方、逆オークションの場合は航空券の購入や旅館の予約などを希望する人がその申し込みを行って、航空会社や旅館から入札形式で値段の提示を受けるもので、勿論一番安い値段を提示してきた所と取引を行う方式である。

これらのオークションによる取引形態では日常の世界と異なり簡単に手持ちの物（特に不要になった物）を売ったり、安い値段で購入したりすることが可能であり、リサイクルショップのネット版として今後とも利用が増加するものと思われる。

ネットオークションでは競り落とした物と送られて来たものが違ったり、支払いしたのに物が来ないなどのトラブルが後を絶たない状況である。

1.1.4　検索

インターネットでの便利な機能の代表格である。『判らないことはインターネットに聞け』の合言葉もある位で Goo、Google、Yahoo!などに代表される検索サイトや調べたい物の専門サイトにアクセスすれば必要な情報はかなりの範疇まで入手できるし、またこれらの情報を積極的に公開する風土が醸成されて来た。

例えば、検索サイトに『肩こり　病院　治療方』などと検索キーをスペースで区切って多重検索すると、これだけでも数千件の検索結果が表示され、検索キーを替えたり搾り込みを多くしたりして、より具体的な解答を引き出すことが可能である。

これからの時代は検索のテクニックによっていかに必要で有益な情報を得ることができるかがインターネットを使う上での能力として認められることとなろう。

1.1.5　ダウンロード

ダウンロードを行う対象を分類すると以下の通りとなる。またダウンロードに対する費用にも様々な分類がある。

ダウンロード対象の分類

ｉ）音楽

有名歌手やバンドの曲の全部または一部を主にはＭＰ３ファイル形式やＭＩＤＩファイルでダウンロードするものであって、自分のパソコンのハードディスクに保存したり更に持ち運び用途のＭＰ３プレーヤーに再ダウンロードするケースがこれに該当する。

ここでのトラブルの多くは著作権に起因するものが多い。

ii）画像

特にパソコンやホームページの作成時に利用する壁紙やＧｉｆ画像、あるいは俳優のブロマイドなどである。最近は動画による画像配信も多くニュース、映画の販促用、インターネットビデオなどに利用されている。

iii）ソフト

無料でパソコンに関係するソフト、例えばカレンダ、時計、ゲームなどを配信しているサイトがある。これらはダウンロードサイトにアクセスしそのページの宣伝を眼にすることによる宣伝料で賄っているケースが殆どである。

なお、無料ソフトであるからと言って信用出来ないサイトからのダウンロードでは、そのソフトにウイルス、スパイウェア、キーロガーなどの悪質なソフトが付いてくる場合もあるので注意を要する。

iv）ファイル

Windows などのＯＳの更新ファイルやウイルス対策､スパイウェア対策用のパターンファイルの更新、あるいは情報発信サイトが提供するＰＤＦファイルなどがこれに該当する。

ＯＳやパターンファイルの場合は、メーカや関連企業から自動配信や通知が来る仕組みになっており、更新や修正用途が目的であることからダウンロードして対応してもらうことが大事なので、対応を忘れたりしない工夫が施されている。

情報発信サイトから提供されるＰＤＦファイルの内容としては、政府や省庁からの統計資

料、学会や研究所からの発表資料を初め、様々な場面でのファイル提供があり、系統的に何処が多いとは言えず積極的に情報発信している状況である。

ここでのトラブルはダウンロードした資料の内容に関わる事柄が多い。即ちその資料内容の信憑性であろう。注意してその資料の作成年月や資料の提供者、提供の意図などを見極めないと間違った情報を利用する恐れがある。またその資料を閲覧するに当たりウイルスやスパイウェアなどが仕掛けられている場合も多い。

ダウンロードの費用

ファイルやソフトのダウンロードには様々な形態がある。

ⅰ）有料

ファイルやソフトのダウンロードに先立ってその費用の支払いが発生する形態やダウンロードは可能であるが、支払いを済ませてそのソフトを起動するためのパスワードを得る形態もある。支払いの方法としてはネットワークを介して商品を入手することからクレジットカードまたはネットを介したプリペイド支払いが多い。

ⅱ）無料

全くのただでファイルやソフトのダウンロードを認めている形態である。ただし著作権は放棄していないケースが殆どであるから、ダウンロードしたファイルやソフトの他への転売は法律違反となる。

ⅲ）シェアウェア

専らソフトの場合が多く、まずソフトを先にダウンロードして試用した後に気に入ったらその代金を支払う形態である。無料で使い続けられるが利用の期限が予め設定されているソフトや気に入ったら適当な金額を賽銭代わりに支払えば良いものまである。これはダウンロードした利用者側のモラルによる所が多く、無料で使い続けるケースもあるようだ。もっとも製作者の方はタイマを利用して有効期限を設けるなどの対抗手段を取っている場合もある。

1.1.6 ゲーム

従来ゲームと言えばゲームソフトを購入してそのパソコンだけで遊ぶものとされてきたが、ネットワークにパソコンを接続してネットワークの向こうに居る人と戦うゲームも増加している。このゲームを特に対戦型ゲームと言う。

対戦型ゲームは将棋などの１対１のゲームや麻雀やトランプなどの１対Nの場合があり、ゲームによっては数百人が同時に参加することもある。

1.1.7 習い事（オンライン講座）

一番顕著な例は、オンライン英語講座であろう。パソコンにマイクとカメラを接続し、ネットワークの向こうに居る英語の先生の顔を見ながらオンラインで会話と画像によって学習していくものである。

また、ビデオ取りした授業内容をサーバに登録しておき 24 時間何時でも講義を視聴することも可能である。

1.1.8　予約・申し込み

航空券、旅館、コンサートチケットなど従来は取り扱い代理店やチケット売り場まで出向く必要があったが、ネットワークを介して予約や申し込みができるので非常に便利である。また予約や申し込みに際してはネット検索を併用して比較検討が簡単に行えることから自分に合った最適な予約や申し込みが可能となった。

予約や申し込みサイトにおいては航空券では受け付け時間の制限があり、旅館ではその日の空き室状況などで値段を下げ、空席や空き室を出さない様な合理的なシステムを構築している場合もある。

ここでのトラブルは申し込んだ希望内容と実際の内容が異なるケースや、支払いを行ったあとのキャンセルの仕方などに関わることが多い。

1.1.9　ＩＰ電話

インターネットの世界では音声をデジタル化して相手に届け、受け取った相手はデジタル信号をアナログに変換することにより電話としての機能が利用できる。従って、デジタル化／復号化に加えて、相手を指定するダイヤリングに相当する機能があれば通常の電話と代わらない機能が提供できる。

ＩＰ電話の特徴は何と言っても従来のアナログ電話の通話料金に相当する費用が殆ど発生しないことと、トラフィックの増加により音声データの通信パケットが渋滞し、その結果音切れが生じることである。個人的に音声のみの利用であれば問題は少ないが、商用の取引に利用するとなると通話の正確性が重要な要素となり、音切れが問題になる場合もある。

1.1.10 チャット

従来はキーボードを叩いての文字による双方向のチャットであったが、最近はマイクとスピーカを使って音声によるチャット、またこれに加えてパソコンに Web カメラを接続して相手の顔を見ながらまるでテレビ電話の様に遠方の相手との会話を楽しむことができる様になってきた。

遠隔地と言っても日本国内に限らず全世界の人々を相手にチャットが可能である。

これは一重にブロードバンドの産物であり、高速通信により初めて実現できる機能である。テレビ電話に匹敵する機能を持ったチャットに要する費用は大体の場合、ネットに接続するプロバイダ費用を別にすれば、一切必要無いことも大きな特徴である。

ここでのトラブルはチャット友達と言っても実際に逢うこともなく文字や会話だけのお付き合いであり、相手が信用できるかを見極めることは難しい。この為、音楽や画像のファイル交換を行う仲となり、その後で意図的にウイルスやスパイウェアを送りつける事件も発生している。

1.2　まとめ

前項ではくらし（家庭）を中心にソフトの見地から代表的な『便利な機能』を見てきた。これらの機能を使いこなすことができれば快適なくらしに大いに役立つことは使ってみて初めて判るケースも多い。その反面、ウイルスやスパイウェアなどの怖さを理解不足のまま使うとこれらの餌食になる場合があり、正に便利さと怖さが同居した時代となってきた。

とは言え、ここでの中心は携帯電話やパソコンであり、特にパソコンとなるとまだまだ一般消費者には難しい部分があることから悪意ある者に付け込まれるケースが後を断たないことは非常に残念である。

幸いこれらの悪意に対しても未然防止するためのソフトウェアが整備されてきており、何時の日にかは安心して快適なくらしを享受することができるものと確信する。

2. くらしと便利な決済

2.1 はじめに

くらしには商品の入手やサービスの享受が不可欠である。これらの対価を支払う行為を決済というが、いまや、現金が唯一の決済手段ではない。また、くらしの中にもインターネットが普及し、ネットワークを介した決済方法が登場し多様化している。

本章では、現在提供されている決済サービス事例を紹介する。その上で、便利であるがゆえに、安易な利用が招くトラブル、潜むリスクを回避する対策方法を紹介する。

2.2 便利な決済手段の現状

ＩＴ技術の進展に伴い、消費者にとって現金以外での便利な決済手段が登場し、多様化している。本項では、まずその現状を捉えることとする。

2.2.1 便利な決済手段の全体像

決済手段の定義

前払・即時払・後払

品物やサービスの提供を受ける時点と、それに対する対価の支払時期を比較することにより、一般的に支払手段は、前払式・即時払式・後払式に分類することができる。前払式には、従来から広く利用されている「商品券」や「プリペイドカード」があり、利用者が事前に価値を購入して、以降、品物やサービスの提供を受ける際の代金決済にその価値を使用する方式である。即時払式は、現金による支払い方式に加え「デビットカード」のように、品物やサービスの提供を受けるのと同時にその利用者の預金口座等から代金決済される方式である。後払式は「クレジットカード」のように、品物やサービスの提供を受ける時点では、その代金決済は一時的に留保され、後日、クレジットカード会社等へ代金決済をする方式である。いずれも、カード決済という点では、利用者にとっては現金を持たなくても良いメリットがあり、事業者にとっても代金回収の合理化といったメリットがある。また、前払方式の「プリペイドカード」は匿名性が高く、贈答品として譲渡可能であることが特徴である。

リアルとバーチャル

本章においては、実際に街中にある店舗（端末も含む）を「リアル店舗」といい、そこで行われる決済を「リアル決済」という。それに対して、インターネット上のショッピングモールなどの仮想店舗を「バーチャル店舗」といい、そこで行われる決済を「バーチャル決済」という。

決済用ツールの多様化

現金以外の決済手段に使われるツールとしては、商品券や磁気方式のプリペイドカードから、高いセキュリティと大きな記憶容量を有するＩＣカードへと進化してきた。またＩＣカードのタイプには接触式と非接触式があり、非接触式の場合、接触式に比べて読み取り方向の自由度が高く、利用者がカードを移動しながら使用する用途に向いている。この特徴を活かして平成 13 年 11 月からＪＲ東日本がＩＣカード改札システムを商用導入し、平成 16 年 7 月にはＮＴＴドコモ

による非接触ＩＣチップを搭載した携帯電話による決済サービスが始まった。（利用方法は 2.3.1 項の(1)参照）特に 8,577 万加入[1]の携帯電話という媒体に今後さまざまな機能が付加され、当該機能と組み合わせた新たなサービスが出現することが予想される。

決済認証技術の発達

決済の場面では、その個人の財産の増減に直結することから第三者による不正利用を防止する観点で本人を認証する方法が大変重要である。これまでに、ＰＣからの送信情報を暗号化するＳＳＬ（Secure Sockets Layer）やＳＥＴ（Secure Electronic Transactions）というセキュリティ技術が開発され、利用されている。

ＳＳＬはＰＣのブラウザがサーバとの間でデータを暗号化して通信するためのプロトコル（通信規約）である。ブラウザに組み込まれていることから決済用途以外でも広く利用されているが、クレジットカード会社加盟店にも個人情報等が蓄積されるので、当該情報は厳格に管理される必要がある[2]。

ＳＥＴは、インターネット上でのクレジットカードによる支払を安全に行うためのプロトコルであり、クレジットカード会員とクレジット加盟店間のプロトコル、認証局とその対象者間のプロトコルを規定する。ＳＳＬのみ使用する場合に比べて安全性は高くなるが、利用するにあたっては、「Wallet」と呼ばれる専用ソフトウェアをパソコンにインストールする必要がある。そのため、ＰＣ初心者等にはやや難しいといった部分がある。

最近ではさらに安全性と利便性を高めた「３Ｄセキュア」という技術が開発され実用化されている。これは MasterCard、ＶＩＳＡ、ＪＣＢが提唱する本人認証サービスで、クレジットカード会員が「３Ｄセキュア」に対応したオンラインショッピング加盟店でクレジットカードを利用する際、カード発行会社がパスワード入力画面をポップアップ表示し、本人しか知りえないパスワードを入力することによってカードの利用者が本人であることを確認するサービスで、専用ソフトなどを組み込む面倒さがなくなっている。（図 2-1 参照）

[1] 電気通信事業者協会 携帯電話契約数（平成 17 年 1 月末。
http://www.tca.or.jp/japan/database/daisu/yymm/0501matu.html より）

[2] クラッカーによる攻撃や加盟店内部の協力者によって、個人情報が外部に流出するなどの危険性がある。

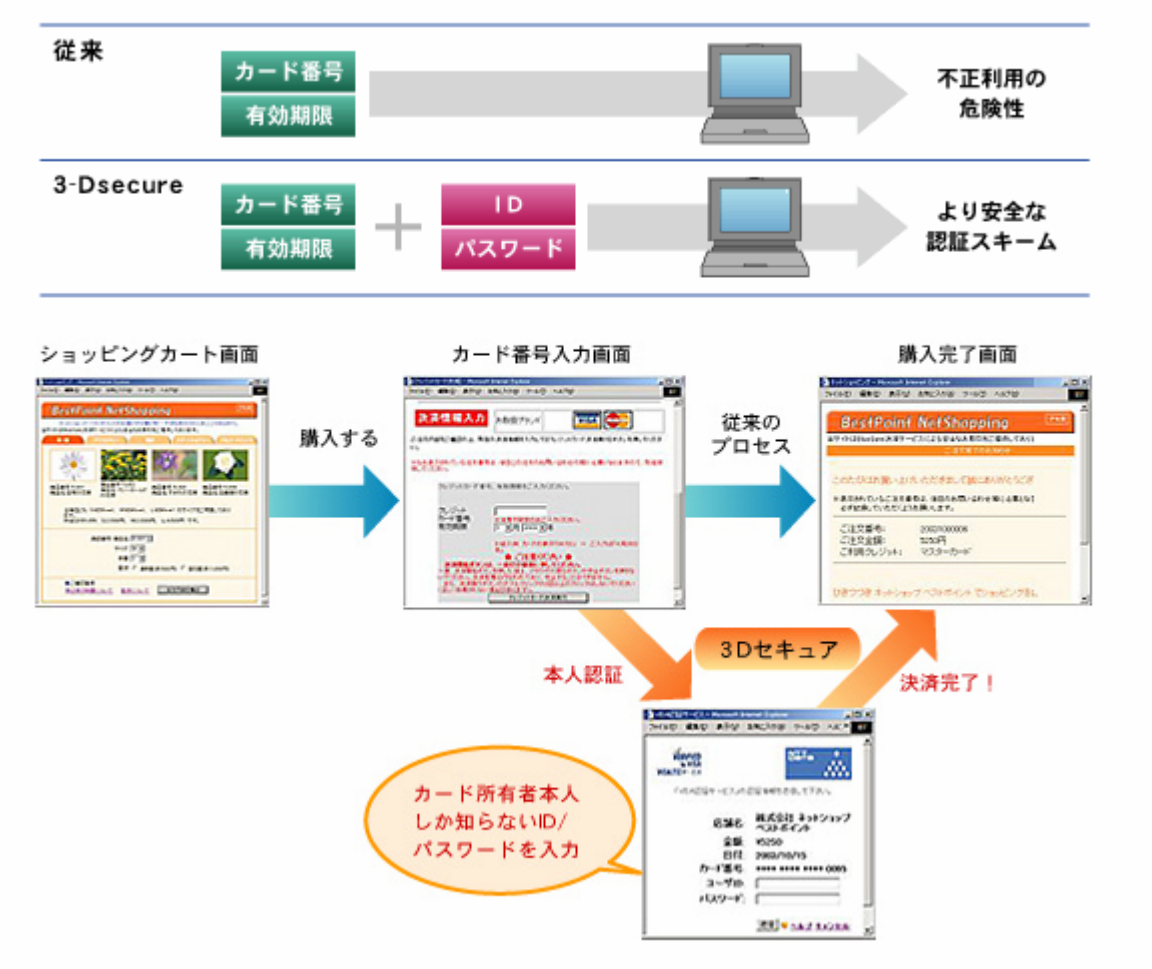


図 2-1　３Dセキュアの概要

（ＮＴＴデータホームページ http://solution.cafis.jp/BlueGate/index.html **より）**

【参考】３Dセキュアスキームを使用した、各ブランドのサービス名称を以下に示す。

・マスターカード：「MasterCard SecureCode」

・ＶＩＳＡ：「Verified By VISA」

・ＪＣＢ：「J/Secure」

しかしながら、ＩＤやパスワードは、他人に盗まれたり、亡失したり、最悪の場合は類推されたりする可能性もある。他人に漏れることのない生体認証（バイオメトリクス）の技術開発が盛んとなっている。その本人特有の特徴を使う技術で、指紋、虹彩、サイン、顔、声などによる認証技術で、社員証に組み込まれて入退出のチェックなどに利用されている。また最近では、手のひらの静脈パターンで本人を確認する「手のひら静脈認証」による預金サービスが開始されている（2.3.1 項参照）。

2.2.2　電子マネー・電子決済の普及

電子マネーと電子決済

いわゆる「第２次マネ懇」[3]の報告書によれば、「電子マネー」とは、利用者から受け入れられる資金（発行見合資金）に応じて発行される電磁的記録を利用者間で授受、更新することによって決済が行われる仕組み、またはその電磁的記録自体とされ、また、「電子マネー・電子決済」とは、電子マネーを含め、決済に関する情報が電磁的な方法により処理され、そのプロセス全体を管理する単一の主体が存在しない決済の仕組みと定義されている。

つまり、電子マネーとは電子データ化された貨幣価値を言い、電子決済とは電子マネーを使った支払いや、インターネットバンキングによる振込みや、インターネットモールでのクレジットカード払いのことをいう。決済事業者が介在し、現金などを直接使用せずに商品の代金を支払うことも電子決済の範疇に入る。電子決済の分類を表 2-1 に示す。

表 2-1　電子決済の分類

電子決済である （電子的に決済が実行される）	**電子決済ではない** （電子的に決済が実行されない）
・　口座振替 ・　インターネットバンキングによる振込 （ＡＴＭで現金を使わずに振込む場合も含む） ・　クレジットカード ・　プリペイドカード ・　デビットカード ・　モバイルペイメント	・　現金払い ・　現金振込み ・　代金引換

電子マネーの分類

一般的に、電子マネーは、ＩＣチップに貨幣価値データを記録する「ＩＣカード型電子マネー」と、ネットワーク上で貨幣価値データの管理を行ない、それを利用して決済をする「ネットワーク型電子マネー」に大きく分類される。ここでは、ＩＣチップを搭載した携帯電話も含め、ＩＣカード型電子マネーと分類する。またそれぞれに、前払、即時払、後払のタイプがあり、さらにリアル店舗で使用できるもの、バーチャル店舗で使用できるもの、そのいずれにも使用できるものなどＩＴ技術の発展とともに多様化している。そういった面から、一部の例を取り上げ、電子マネーの分類を表 2-2 に示す。

[3] 電子マネー及び電子決済の環境整備に向けた懇談会（大蔵省：平成 10 年 6 月 17 日）

表 2-2　電子マネーの分類

決済タイプ	決済方法	電子マネー分類	ブランド名(括弧内はサービス提供事業者)	概要等
リアル	前払	ICカード型	Edy (ビットワレット)	非接触式の IC カードを端末にタッチするだけで支払いができる。自分の財布にお金を入れるように IC カードにチャージ(入金)して、繰り返しチャージして、何度でも利用できる。(http://www.edy.jp/index.html)
			Suica (JR 東日本)	非接触式の IC カードを採用したもの。自動改札機の上部“読み取り部”に、平行に軽くタッチして使用する方式のIC出改札システムである。また、平成 16 年 3 月からショッピングサービス(電子マネー)も開始した。 (http://www.jreast.co.jp/suica/)
			ICOCA (JR 西日本)	基本ｽｷｰﾑは Suica と同様。平成 16 年 8 月には Suica との相互利用が可能になった。
		ネットワーク型	スターバックスカード (スターバックス)	全国チェーンのコーヒーショップで利用でき、利用残高、履歴は、カード裏面に表示されている「カード番号」と「PIN 番号」で、同社のホームページで照会ができる。 (http://www.starbucks.co.jp/ja/home.htm)
	即時払	ネットワーク型	デビットカード	店舗で買い物をする際に金融機関のキャッシュカードで直接支払いが行なえるサービス。店頭では、支払いの際に専用の端末にカードを挿入して暗証番号を入力すると、金融機関口座から即座に代金を引き落として決済を行なうことができる。(Yahoo! コンピュータ用語辞典)
	後払	ICカード型	PiTaPa (スルッと KANSAI)	非接触ICカードを用いた改札システムで、平成 17 年 1 月現在、阪急電鉄、能勢電鉄、京阪電気鉄道の各駅で利用可能。チャージ不要で利用料金は 1 ヶ月単位で集計され指定口座から引き落としされるポストペイ(後払)方式である。 (http://www.surutto.com/index.cgi)

		ネットワーク型	Smart Pit (NTTコムウェア)	コンビニエンスストアで Smart Pit カードを入手する。ネットショッピングで、Smart Pit カードに印字された番号を入力して購入手続きを行い、支払期限までにコンビニエンスストア等で代金を支払う。Smart Pit カードが手もとにない場合も、メールアドレスを入力することにより、センターから払い出される Smart Pit カードを印刷し、当該用紙を店頭で提示することによる支払も可能である。 (http://www.smartpit.jp/)
バーチャル	前払	ICカード型	Edy (ビットワレット)	リアルショップで使えるものと同じカードだが、リーダライタをパソコンに接続することにより、24 時間ネットショッピングが可能である。
		ネットワーク型	NET CASH (NTTカードソリューション)	プリペイド式の電子決済サービスで、NET CASH 決済導入済みの加盟店で、16 桁の ID を入力するだけで簡単にショッピングやオンラインゲームを楽しむことができる。スクラッチ・プリペイド式カードの「NET CASH カードタイプ」、オンラインで NET CASH ID を購入する「NET CASH Web タイプ」、コンビニ端末(ローソンの Loppi ・ファミリーマートの Fami ポート)にて購入できる「NET CASH シートタイプ」の3種類がある。(http://net-cash.jp/index.html)
			ちょコム (NTTコミュニケーションズ)	インターネット上で使える電子マネーで、ネット上に個人専用のちょコム貯金箱を開設し、ちょコムをチャージして使う。楽天市場や Yahoo!ショッピングなどの 2,500 以上のサイトでネットショッピングの支払いに使える上、他人に送ったり、現金に戻したりすることもできる。 (http://www.chocom.jp/)
			Webmoney (ウェブマネー)	使いきり型のプリペイド型電子マネーで、コンビニ等で、16 桁の番号が記載されたカードを購入し、ネットショッピング時にこの番号を入力して、相応額の支払いができる。カード型以外の購入手段もあり、バリューをまとめておけるウォレットというサービスもある。 (http://www.webmoney.jp/index.html)
	即時払	ネットワーク型	ネットデビット	デビットカードのバーチャル版であり、インターネット上で買い物等を行った際に、個人の銀行口座から即時に代金決済を行う事ができるサービス。
	後払	ネットワーク型	E-MYCASH (BIGLOBE)	“E-MYCASH”で購入した商品の代金は、BIGLOBE の利用料金と同じクレジットカードで決済される。 (http://shopping.biglobe.ne.jp/cgi-bin/emycash/read.cgi?NAME=1tokuchou)

			Smash (So-net)	概要は、E-MYCASH と同様。 (http://www.so-net.ne.jp/smash_service/)
			イオンレジ (イオン)	AEONのクレジットカードを使って、インターネットショッピングをするものである。クレジット番号を 1 度入力するだけで、以降はID、パスワードのみで商品購入ができるのが特徴。 (http://www.aeonmarket.com/portal/intro_regi2.html)

2.2.3 電子マネー・電子決済の市場動向

経済産業省、ＥＣＯＭ、ＮＴＴデータ経営研究所が共同調査した「平成 15 年度電子商取引に関する実態・市場規模調査」によれば、バーチャル決済の場面においては、2003 年の電子商取引はＢtoＢが約 77 兆円（前年比 67%増）、ＢtoＣが約 4.4 兆円（前年比 65%増）となっており、ブロードバンド化を背景に急速に拡大している。ただしこれはあくまでも商取引額であって、全てが電子決済で行われたということではない。サイバースペース・ジャパン（株）が発表した「第 17 回ＣＳＪWWW利用者調査結果[4]」によると、オンラインショッピングで購入者が希望する支払方法は、表 2-3 のとおりクレジットカードが第１位であり、コンビニ決済、代金引換と続いている。

表 2-3　オンラインショッピングで購入者が希望する支払方法

支払方法	2003 年 3 月調査結果
クレジットカード	34.4%
コンビニ決済	31.8%
代金引換	19.5%
郵便振替	7.4%
銀行振込	5.2%
現金書留	0.2%
その他	1.4%

また、同調査結果によれば、インターネットバンキングの利用経験者は、調査対象者の約３分の１であり、バーチャル決済でのＢtoＣにおける電子決済による取引額は全体の 4 割弱の約 1.7 兆円程度と推測できる。拡大しつつある電子商取引の大部分はクレジットカード決済であり、インターネットバンキングや電子マネーなどの新しい電子決済の利用はまだ小規模であるといえる。

[4] http://www.csj.co.jp/www17/

さて、リアル決済の場面においては、クレジットカードのみならず、イオカード[5]、パスネット、テレホンカードなどのプリペイドカードも広く使われている。また、高速道路の料金所をノンストップで通行することができるＥＴＣシステムも、普及促進キャンペーンと新しい割引制度の展開により、平成 17 年 1 月にはＥＴＣ車載器セットアップ累計件数が 500 万件を突破した[6]。これらについてもキャッシュレスという点では電子決済の範疇に入るが、ここでは、特に電子マネーについて記述する。

その一例として、ビットワレット株式会社が運営する電子マネーサービス「Edy」とＪＲ東日本が提供するサービス「Suica」を取り上げる。

「Edy」は平成 13 年 11 月から本格スタートし、平成 16 年 10 月現在では、「Edy」を搭載した非接触式のＩＣカードは約 560 万枚発行され、日本国内の約 13000 店舗で利用可能となっている[7]。ＮＴＴドコモが平成 16 年 7 月から発売した「おサイフケータイ」（ｉモード FeliCa）で使用している電子マネーもこの「Edy」である。

「Suica」は、平成 13 年 11 月にＪＲ東日本がサービスを開始し、当初は鉄道運賃の支払い専用であったが、平成 16 年 3 月からショッピングサービス（電子マネー）を開始し、8 月にＪＲ西日本が発行する「ICOCA」との相互利用が可能となり、11 月には「Suica」カードの発行枚数は 1,000 万枚を突破した。（そのうち電子マネー対応「Suica」は 443 万枚、利用店舗は駅構内のコンビニや売店を中心とした 653 店舗）さらに、ＪＡＬ、ファミリーマートとの提携や「PiTaPa」との相互利用も発表され[8]、浸透が急激に進むと予測される。

これらの電子マネーは、社員証、会員証、クレジットカードなど他の機能を持つカードにも搭載され、複合化することで利便性と普及率を向上させている。

2.3　便利な決済のサービス事例

2.3.1　新しい便利な決済

近年実用化された便利な決済の例を下記に紹介する。

(1) おサイフケータイ

携帯電話に決済用の記録媒体を格納し、外部端末との近接型非接触通信によって決済を実現するサービスである。平成 16 年 7 月 10 日のｉモード FeliCa 対応端末発売と同時にサービスを開始した。平成 16 年 12 月現在のｉモード FeliCa 対応端末は約 100 万台である[9]。

端末利用イメージを図 2-2 に示す。支払時の利用方法はカードと同様で、携帯電話のマークをリーダライタにかざすだけで済み、端末操作は不要である。

---

[5] 平成 17 年 3 月を以ってイオカード（磁気式）の発売を終了し、平成 18 年 1 月を目途に自動改札機での使用を停止する旨、ＪＲ東日本から報道発表された。（平成 16 年 12 月 9 日付）

[6] http://www.orse.or.jp/monitor/0501111press.pdf

[7] Yahoo!NEWS（http://headlines.yahoo.co.jp/hl?a=20040929-00000013-san-bus_all）より

[8] ＪＲ東日本プレスリリース（http://www.jreast.co.jp/press/2004_2/20041009.pdf より）

[9] ＮＴＴドコモプレスリリース「ｉモード FeliCa 対応携帯電話（おサイフケータイ）が全国で 100 万台突破＜2004 年 12 月 15 日＞」

●ケータイの マークを読み取り機の受信部中央に近づけて…

●ケータイの マークを読み取り機の受信部中央にかざすだけ。

図 2-2　ＮＴＴドコモの「おサイフケータイ」
（http://www.nttdocomo.co.jp/p_s/service/felica/index.html より）

利用者にとって便利な面としては、以下が挙げられる。

携帯電話画面で残高・履歴の確認や複数のポイントカード機能の格納が可能

Edy カードの残高確認手段は、非接触リーダライタをＰＣに接続し、あらかじめインストールした専用アプリケーションを起動して残高を表示させる、または、支払い時にレジ画面表示で残高を確認するなどの方法であり、手もとのカードの残高をすぐに目にすることは出来なかった。このサービスでは、携帯電話にインストールされている残高表示用ソフトを起動させるだけで済む。このため、支払い時になって初めて残高不足に気づくケースを減らすことが可能となる。

オンラインでの支払い・チャージ・電子チケットダウンロードが可能

従来の Edy カードと異なる点は、チャージの際にわざわざチャージ用端末まで赴くことなしに、携帯電話のネットワーク経由でチャージできる点である。

また、電子マネー以外のアプリケーションの一つとして、電子チケットダウンロードサービスがある。一般に、興行チケット（紙媒体）の配送手段は本人受取郵便であることが多く、独身者・単身者が自宅を留守にしている場合は、受取人不在として一旦郵便局に持ち帰られてしまう。この場合、本人が夜中に当該郵便局の時間外窓口まで出向いて受け取る、または、再配達時間を指定して自宅で待機するなど、生活動線に制限が伴う。携帯電話のネットワーク経由で携帯電話本体にチケットデータを格納することで、このような不便さが解消する。

端末故障時・機種交換時の電子マネー移し変え・返金対処が可能

所定のサービスを申し込み、個人情報を登録することを前提として、端末が故障して利用不能となった場合の Edy 残高の返還が可能となっている。また、おサイフケータイ機能を搭載した別の携帯電話に機種変更する際に、変更前の端末操作で所定の手続きを踏むことによって、一旦、残高がセンターに保管される。新端末への変更後、端末の操作によ

って、当該残高がネットワーク経由でダウンロードされる。（図 2-3 参照）

i モード FeliCa 対応端末の所有者すべてが電子マネーサービスを利用するとは限らないが、上に述べたように、携帯電話への電子マネー機能搭載は、カードを用いたサービスよりも優位にあるといえるとの差別化が可能である。今後の携帯電話の多機能化に伴って、さらに便利な電子マネーサービスが出現する可能性を秘めている。

図 2-3　機種変更時の電子マネーバリュー移し変えイメージ（ビットワレット株式会社ホームページ http://www.edy.jp/edy_mobile/edy_mobile_07.html より）

(2) PiTaPa（ピタパ）

PiTaPa は、関西の鉄道・バス 43 社局で構成される「スルッと KANSAI 協議会」が導入したＩＣカード決済サービスであり、平成 16 年 8 月 1 日にサービスを開始した。

PiTaPa の決済手段はプリペイドではなく、ポストペイが基本である。すなわち、PiTaPa カードの利用状況が 1 カ月単位で集計され、後日、当該集計額が利用者の口座から引き落されるしくみになっている。したがって、カードへのチャージという概念そのものが存在しない[10]。

利用者は申込書を駅で入手し、金融機関の口座情報などを記入して申し込み、PiTaPa カードを発行してもらう必要がある。カードの有効期限は 5 年である。利用限度額は、交通用

[10] Suica・ICOCA との相互利用では、チャージ方式を利用する予定となっている。（スルッと KANSAI 協議会など 5 社共同のプレスリリース（平成 16 年 4 月 27 日）より）

途でのサービスでは 15 万円／月、物販サービスでは 3 万円／日、5 万円／月となっている。

乗車券機能

改札機通過時の使用方法は、ＪＲ東日本のSuicaやＪＲ西日本のICOCA等と同様であり、乗車・降車の都度、改札機のリーダライタに PiTaPa カードをタッチする。

サービスの種類としては、利用回数割引運賃と区間指定割引運賃がある。このうち、本報告書では、区間指定割引運賃について取り上げる。利用者は、通勤・通学経路など頻繁に利用する区間をあらかじめ駅やインターネットで登録する。区間内の「1 か月間の利用総額」と「区間指定割引運賃（＝1 か月定期運賃と同額）」を比較して安い方の運賃が後払いで利用者の口座から引き落とされる。

一般的な定期券はプリペイドであることから、1 か月の利用回数が少ない場合、利用者は「前払い分の元が取れない」など割高感を抱くこともあるが、PiTaPa の「区間指定割引運賃」では定期券運賃を上回ることはないため、割高感を解消できるというメリットがある。

電子マネー機能

乗車券機能のほか、平成 16 年 10 月 1 日から、200 店舗・施設で物販決済での利用が可能となった。鉄道での利用同様ポストペイである。また、PiTaPa での利用額に応じて「ショップｄｅポイント」というポイントが付与され（利用額 100 円につき 1 ポイント）、500 ポイント毎に当月の鉄道利用代金から 50 円が差し引かれる。

グーパス機能

PiTaPa グーパスは、事前に会員登録した PiTaPa 利用者の所有する携帯電話に、利用者が PiTaPa を用いて自動改札機を通過した直後、趣味やグルメ、沿線のイベントなどに関する情報や広告をメール配信するサービスである。オムロン株式会社が、平成 16 年 8 月から阪急電鉄線・能勢電鉄線でサービスを開始した[11]。利用イメージを図 2-4 に示す。

[11] 小田急線各駅でも平成 15 年 2 月からサービスを開始している。

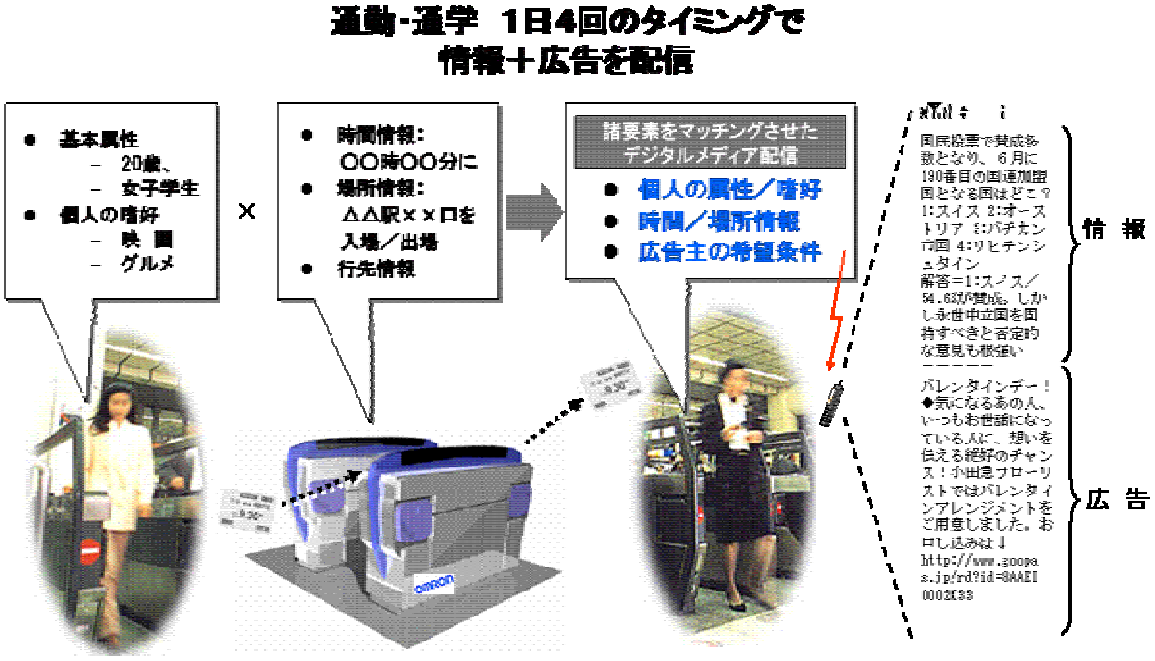


図 2-4　グーパスの基本サービス

（第 41 回ＥＣＯＭセミナー（平成 16 年 9 月 17 日）「モバイルマーケティング進化論」資料より）

PiTaPa グーパスサービス利用にあたっては、利用者の所持する定期券情報や必要とする情報を登録する。改札通過時に鉄道の運行情報や駅周辺の情報等が利用者の携帯電話に送信される。単なる携帯電話メール配信サービスとは異なり、利用者の嗜好や生活動線にカスタマイズされた情報を入手できるという点で便利なサービスであるのが特徴といえる。

(3) 静脈認証

静脈認証は、人体の特徴を利用するバイオメトリクス認証（生体認証）の一つであり、手のひらや指先の静脈パターンにより本人確認を行う認証方式である。

静脈パターンは人により異なり、大きさ以外は成長や老化などによらず生涯変わらないという特徴がある。静脈認証では、図 2-5 に示すような読み取り装置を用い、利用者はこれに手をかざすだけでよい。読み取り装置に手を触れずに済むので衛生的である。

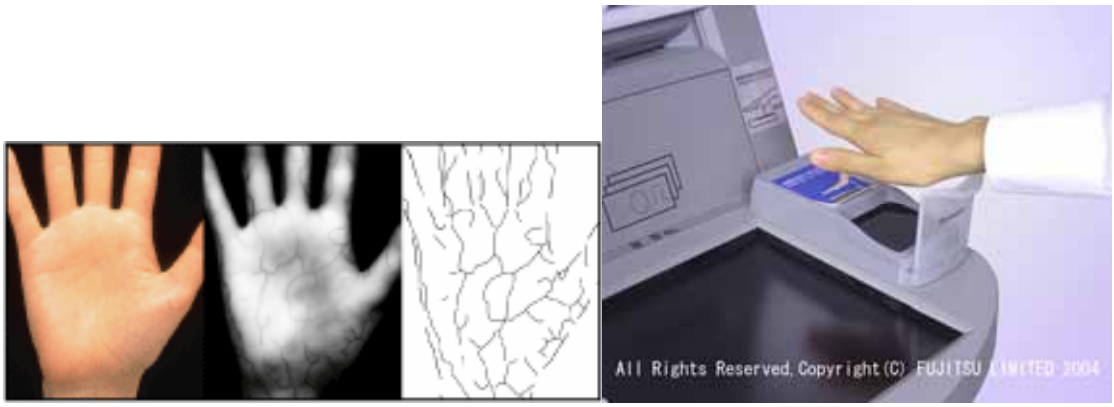


図 2-5　手のひら静脈認証のイメージ（上左）および、静脈認証装置に手をかざす様子（上右）（富士通株式会社ホームページ http://financial-systems.fujitsu.com/jp/services/pg/index.html より）

この方式を用いた預金商品として、平成 16 年 6 月にスルガ銀行が「バイオセキュリティ預金」として[12]、また、平成 16 年 10 月に東京三菱銀行が「スーパーＩＣカード」として[13]、静脈認証を用いた決済を採用した。

現在の預金引き出しにおいては、暗証番号を知ってさえいれば本人以外が預金を引き出せるため、本人の与り知らないところで預金が不正に引き出される危険性がある。静脈認証によって、カード保有者本人以外の預金引き出しを不可能にできるので、親族間であっても預金を分別管理したいというニーズにも対応できる。

今後の生体認証導入の動きとして、池田銀行が、生体認証機能を搭載したＩＣキャッシュカードの導入を決めている[14]。認証手段に「手のひら静脈」を用いる点は他行のサービスと同様であるが、池田銀行が導入を予定しているサービスでは、1 枚のＩＣキャッシュカードで「身体認証口座」と「従来の暗証番号認証のみの口座」の両方のサービスを利用できる。このため、専用の生体認証装置の設置されていない、従来のＡＴＭ端末でのキャッシュカード利用にも配慮しているのが特徴である。

銀行業界全体としても、偽造キャッシュカード対策として

(1) 偽造キャッシュカードの使用防止
(2) カードの偽造防止
(3) 被害拡大の防止
(4) 被害者の救済

に本格的に取り組むことで、各銀行が申し合わせている[15]。全国銀行協会は、キャッシュカードのＩＣ化に加え、暗証番号入力に代わる本人確認手段として、生体認証の導入を各行に呼びかけることとしている。また、平成 17 年 4 月のペイオフ解禁に伴って顧客による銀

12 http://www.surugabank.co.jp/surugabank/corp/index_e.html
13 http://www.btm.co.jp/tsukau/card/visa/index.htm
14 池田銀行プレスリリース（平成 17 年 1 月 17 日付 http://www.ikedabank.co.jp/news04/news0117.html）
15 全国銀行協会会長記者会見（平成 17 年 1 月 25 日）より

行の選別が進み、「セキュリティの高さ」を他行との差異化要素としたサービスの開発も進むものと想定される。今後、生体認証とさまざまなサービスを組み合わせた金融商品が急速に検討・導入されていくものと予想される。

2.3.2 くらしの場面別の便利な決済

今現在のくらしの中で行われている「決済」を伴うシーンの代表的なパターンとして、ある会社員 A さんおよび主婦 B さんのケースを例に挙げ、決済に関係するイベントを中心に日記風に記載し、各決済の特徴を述べる。

(1) 会社員 A さんの平日

A さんの平日のスケジュールを下記に示し、生活動線化したものを図 2-6 に示す（下記円内の数字は、図 2-6 の円内の数字にそれぞれ対応している）。

07:50 自宅近くのバス停で乗車(①)。深夜勤務が多く、帰宅時にはバスに乗ることが少ないので、定期券にはせず、バスカードを使用している。

08:00 駅の売店でスポーツ新聞を現金で購入してから(②)改札機を通る。

08:45 オフィスの最寄り駅で下車(③)

08:55 オフィスに到着

10:30 休憩室の自動販売機で缶コーヒーを購入しようとして、社員証電子マネーで購入しようとしたが、残高不足であることに気付いた(④)。財布は居室の背広に入れたままにしていたので、一旦居室に戻って財布を取り、現金で購入した(⑤)。

12:20 社員食堂で昼食をとった。茶碗や皿の下に無線タグがついており、レジ横の読み取り部分にお盆と食器を置くと自動的に料金を精算し、社員証をレジ横のカードリーダにかざすと支払いが完了した(⑥)。社員食堂での昼食代金は給与天引きなので、チャージの必要がない。

12:50 売店に行き、チャージ機で 5000 円分をチャージしてから雑誌とタバコを購入した。チャージ機はここ 1 箇所のみで、長い行列ができていた。(⑦)

13:30 得意先に営業に出かけた。社用車にはＥＴＣ車載器がついており、高速道路を通過する際に料金が自動的に引き落とされ、後日、会社に通行料金が請求されるようになっている。(⑧)

17:30 社用車をビル地下の車庫に入れ、会社をあとにした。

19:00 中学校時代の友人 3 人が遊びに来ているので、P 駅近くの飲食店に行き(⑨)、飲み明かす。4 人分の会計をクレジットカードで済ませた(⑩)。持っているクレジットカードはＩＣ化されているものの暗証番号を入力するケースは今までなかった。今回、この店で初めて暗証番号を入力した。

22:00　P 駅の改札機をＩＣカード定期券で通った⑪。区間外からの乗車であるが、定期券にチャージしておいたＳＦを利用して入場できた。

23:00　携帯電話に着信したメールを読もうとしてポケットに手を入れたところ、いつもの感触と違う。先ほどの飲食店に携帯電話を忘れてきたことに気付いた。店と場所はわかっていたので、改札口を出て⑫すぐに公衆電話から 104 で店の電話番号を調べて店に電話し、置き忘れたことを確認した⑬。携帯電話は自宅に着払いで送ってもらうよう依頼した。見つかるまでの間に、誰かに着信履歴や電話番号などを見られていないかどうかなど一抹の不安はあるが、盗まれるよりはましだと思いつつバス停に向かった。

23:30　最終バスが出て行ってしまったので、タクシーで自宅まで帰宅した。クレジットカード払いにしようと思ったが、車内の暗い中で取り出したカードがキャッシュカードだったので、デビットカード払いにした。⑭

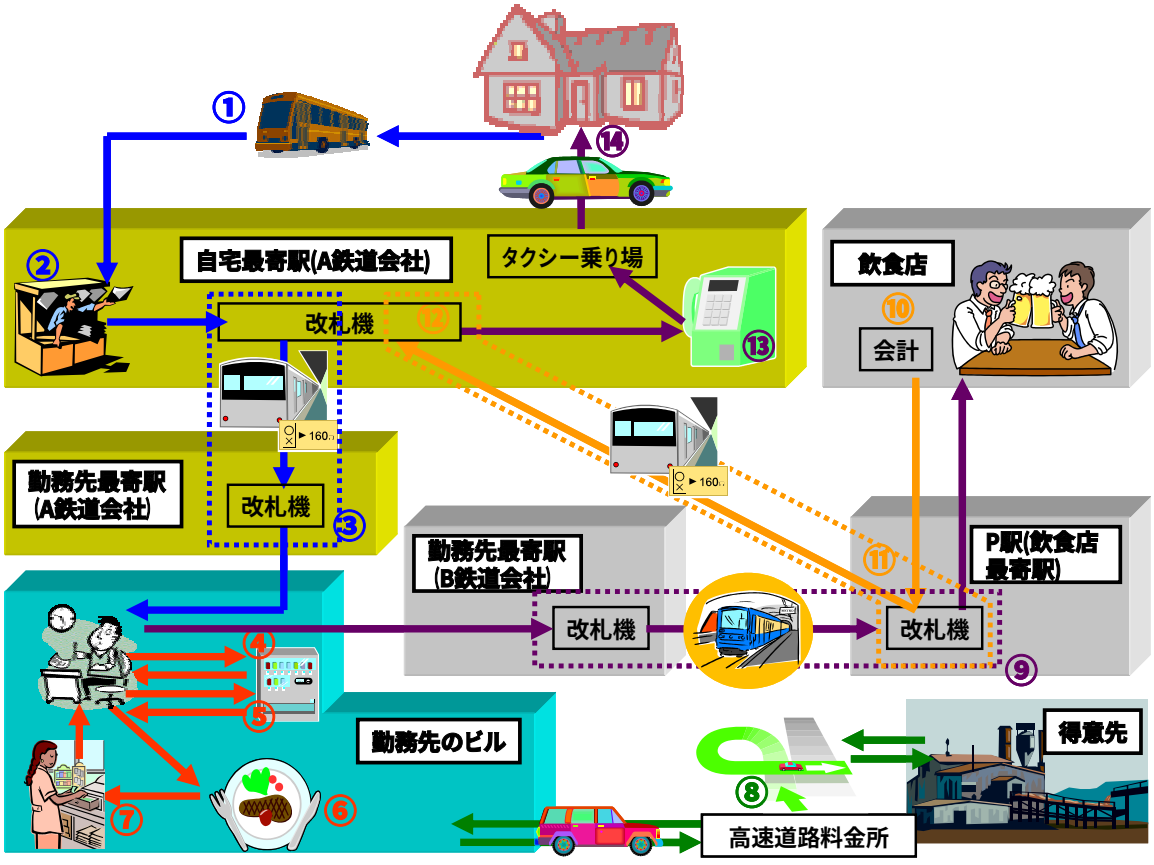


図 2-6　会社員Ａさんの平日における生活動線

平日におけるＡさんの各決済利用シーンを表 2-4 に示す。特徴としては、リアルでの決済がほとんどである。

表 2-4　会社員Ａさんの平日における決済利用シーン

項番	利用場所	使用媒体	端末	決済額	特徴
①	バス	バスカード (磁気媒体)	磁気カードリーダ	200 円	
②	売店	現金	なし(対面販売)	130 円	
③	駅改札機	IC カード定期券	IC カードリーダライタ	―	
④	オフィス内の休憩室	決済機能のついた IC カード社員証	自動販売機に設置された IC カードリーダライタ	―	残高不足で利用できず
⑤	オフィス内の休憩室	現金	自動販売機	120 円	
⑥	オフィス内の社員食堂	決済機能のついた IC カード社員証	IC カードリーダライタ	680 円	
⑦	売店	決済機能のついた IC カード社員証	IC カードリーダライタ	720 円	
⑧	高速道路の料金所	ETC 用カード	ETC 端末	700 円	
⑨	駅改札機	磁気回数券	IC カードリーダライタ	140 円	
⑩	飲食店レジ	クレジットカード	クレジット対応端末	29680 円	
⑪	駅改札機	IC カード定期券(ストアードフェア部分)	IC カードリーダライタ	150 円	定期券区間外乗車分
⑫	駅改札機	IC カード定期券	IC カードリーダライタ	―	
⑬	公衆電話	テレホンカード	公衆電話機	130 円 (13 度数)	
⑭	タクシー	キャッシュカード (磁気ストライプ)	デビットカード端末	1210 円	

(2) 会社員Aさんの休日

Aさんの休日のスケジュールを下記に示し、生活動線化したものを図 2-7 に示す（下記円内の数字は、図 2-7 の円内の数字にそれぞれ対応している）。

【土曜日】

10:30　自家用車にて高速道路で M 空港に向かった。高校時代の同級生の結婚式披露宴に出席するためである。

11:00　サービスエリア内のレストランで朝食兼昼食をとった。支払は、現金による食券購入だった(①)。食事が出てくるまでの間、手もとの携帯電話で、インターネットで事前予約・購入した航空券のチェックインを行った(②)。

12:00　ハイウェイカードで高速道路の通行料を支払い、M 空港近くのインターチェンジを出て(③)、M 空港内の駐車場に自家用車をとめた。

12:30　駐車場からセキュリティゲートに直行した。ボディチェックや搭乗口では、備え付けのリーダライタに携帯電話をかざすだけで済んだ。

14:30　N 空港着。披露宴会場兼自分が泊まるホテルにタクシーで向かった。このタクシーがマイレージ積算の対象であることを知った。下車時、クレジットカードでの支払時に、マイレージクラブカードも提示した。(④)

16:00　ホテルでチェックインを済ませた際、ＩＣカードを渡された。このホテルは入退や自販機での支払いを 1 枚のカードで済ませ、チェックアウト時に一括精算する仕組みになっているそうだ。

16:50　披露宴会場入り口にてご祝儀を渡し(⑤)、会場に入った。

21:30　披露宴終了後、新郎新婦を誘い、ホテル内の喫茶店で談笑した。食事代をホテル内専用ＩＣカードで支払った。

23:00　部屋に戻り、ホテル備え付けのＰＣでインターネットにアクセスした。Web mail 経由で自分宛のメールを確認、返事を出した。また、クレジットカード会社の Web サービスにアクセスし今月のクレジットカードの利用状況を調べたり、航空会社のマイレージを調べたりした。しかし、1 分 20 円の従量制であることに気付いたのは、夜中 3:30 になってからであった。

【日曜日】

09:50　ホテル専用ＩＣカードを渡してチェックアウト(⑥)。やはりインターネットアクセス料金が予想外に多かった。夜中に見たクレジットカード利用状況から考えて、限度額を超えているのではないかと心配しつつ、ホテルの送迎バスに乗り、Q 駅に向かった。

10:10　Q 駅構内のコインロッカーに引出物を入れ(⑦)、駅近くの歴史博物館を見物した。携帯電話電子マネーでも入館料を支払えるので、携帯

電話を窓口にかざした。(⑧)

12:00　博物館近くのラーメン店にて昼食をとった。食後の支払いだが、ここでも携帯電話電子マネーを使った。(⑨)

13:00　Q 駅のコインロッカーに入れた荷物を出し、タクシーで N 空港に向かった。車中で、携帯電話で予約済み航空券のチェックインを行った。(⑩)また、電子マネーが足りなくなってきたので、銀行口座から 3000 円分をチャージした。タクシー運賃はデビットカードで支払った。(⑪)

14:00　N 空港着。おみやげを携帯電話電子マネーで買い(⑫)、手荷物とまとめて預け、セキュリティゲートを通過した。

17:00　M 空港着。駐車場出口で駐車料金を携帯電話電子マネーで支払い(⑬)、高速道路に入った。

17:55　ハイウェイカードで通行料を支払って(⑭)、一般道路に入った。

18:00　来週の今頃は会社の人たちとゴルフをしているのだと思っていたところ、国道沿いのゴルフショップが目に入ったので立ち寄った。自分の好みに合ったゴルフクラブを見つけたが、手持ちの現金で買える値段ではない。クレジットカードも今月は限度額を超えそうなので、この場での購入は断念。クラブの型番やシャフトのデータ等を覚えておき、いつか買おうと心に決めた。

21:00　帰宅後、インターネットにアクセスする。接続形態は、ＡＤＳＬの常時接続である。夕方に立ち寄ったゴルフショップでのゴルフクラブのことを思い出し、ネットオークションのサイトを覗いた。ゴルフショップで見たクラブと全く同じものがあった。幸いにも落札できたので代金の支払いは、インターネットバンキングを利用して、オークション出品者が指定した銀行口座への振込手続きをとった。(⑮)

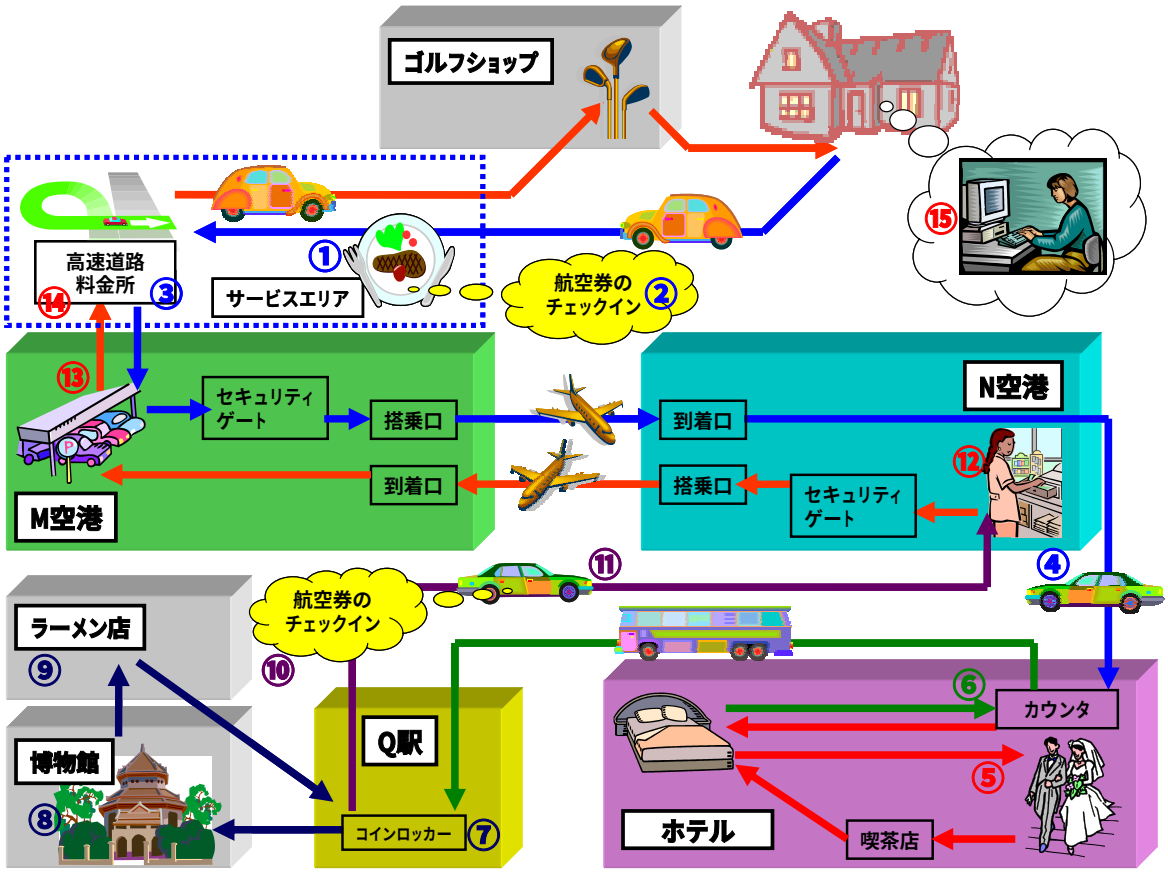


図 2-7　会社員 A さんの休日における生活動線

休日における A さんの各決済利用シーンの特徴を表 2-5 に示す。慣習として現金を使用する「ご祝儀」以外での現金使用はサービスエリアでの食堂と Q 駅でのコインロッカーでの利用のみであり、それ以外はすべてキャッシュレスであるのが特徴である。また、自宅において、バーチャルでの決済としてインターネットバンキングを利用している。加えて、移動途中に手もとの携帯電話で航空券のチェックインを行うなど、従来での手続きでは実現しえなかった方法を利用し、限られた時間・空間を有効に活用しているといえる。

表 2-5　会社員 A さんの休日における決済利用シーン

項番	利用場所	使用媒体	端末	決済額	特徴
①	サービス エリア	現金	自動販売機	820 円	
②	【参考】サービスエリア	携帯電話	―	―	事前購入した航空券なので、当該使用時点での決済行為は発生していない。
③	高速道路料金所	プリペイド 磁気カード	料金所の端末	1500 円	
④	タクシー	クレジット カード	クレジット カード端末	8270 円	
⑤	披露宴会場	現金	なし(対面)	30000 円	
⑥	ホテルの カウンター	クレジット カード	クレジット カード端末	25800 円	
⑦	コイン ロッカー	現金	なし	500 円	
⑧	博物館	携帯電話	非接触リーダライタ	800 円	
⑨	ラーメン店	携帯電話	非接触リーダライタ	940 円	
⑩	【参考】タクシー車内	携帯電話	―	―	②に同じ
⑪	タクシー	デビットカード	デビット カード端末	8510 円	
⑫	N 空港の売店	携帯電話	非接触リーダライタ	3720 円	
⑬	M 空港の 駐車場	携帯電話	非接触リーダライタ	4000 円	
⑭	高速道路 料金所	プリペイド 磁気カード	料金所の端末	1500 円	
⑮	自宅	インターネット	パソコン	22000 円	インターネットバンキング

(3) 主婦 B さんの平日

B さんの平日のスケジュールを下記に示し、生活動線化したものを図 2-8 に示す（下記円内の数字は、図 2-8 の円内の数字にそれぞれ対応している）。

10:00　部屋の掃除をしながら見ていたテレビショッピングでダイヤモンドネックレスが気に入ったので、字幕のフリーダイヤル番号をメモしておく。

10:20　通信販売で 2 週間前に注文した空気清浄器が到着した。支払い方法はデビットカードでの代金引換サービスにしていた。配達員が差し出した端末にキャッシュカードを通し、暗証番号を入力して支払いが完了した。(①)

11:00　近所のショッピングセンターに出かけた。センター内のスーパーマーケットにて食料品を購入した。ポイントカードが 2800 ポイントに達していたので、現金やカードも使用せず、1980 ポイントを使った。(②)

12:00　ショッピングセンター内のレストランで昼食をとった。このレストランでは支払いに現金しか使用出来なかった。(③)

13:45　帰宅後、午前中に見たテレビショッピングでのダイヤモンドネックレスを思い出し、メモしておいたフリーダイヤルに電話をかけ、商品を申し込む。支払い方法はクレジットカードの 5 回払いとする。(④)

15:00　パソコンで自分宛の電子メールをチェックした、登録した覚えのないところからのダイレクトメールが多くなってきた。その後、クレジットカード会社のホームページにアクセスし、クレジットカードのポイント残高を確認した。5200 ポイントに達していたので、食器セットと引き換えることとし、3000 ポイントを使った。(⑤)

17:00　近所の主婦 C さんと一緒にコンサートに出かけた(⑥)。C さんは、インターネットで B さんのチケットも予約し、２人分の電子チケットをネット上の C さん電子私書箱に保管している。駅に向かう途中で、C さんの電子私書箱から B さんの携帯電話にコンサートチケットをダウンロードした(⑦)。コンサート会場の入口で、携帯電話に表示されたバーコード画面をゲートにかざして入場した。座席の位置も携帯電話画面に表示されており、すぐに座席にたどりつけた。

21:00　コンサート会場で、お目当ての歌手のカレンダ・ＣＤを購入した。(⑧)

21:30　コンサート会場から C さんとタクシーで帰宅。B さんがクレジットカードで払い、降車後、C さんが半額を現金で渡した。(⑨)

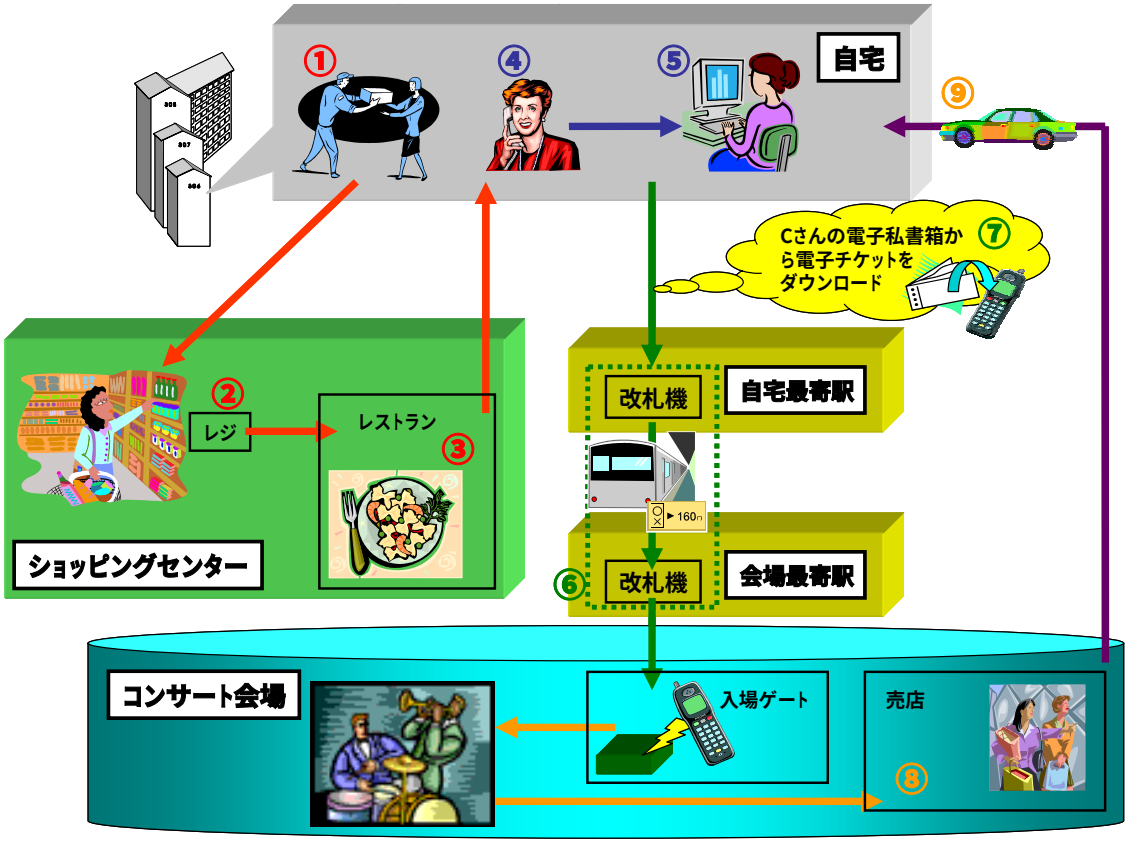


図 2-8　主婦 B さんの平日における生活動線

主婦 B さんの平日における各利用シーンを表 2-6 に示す。B さんの日常生活では、クレジットカードのポイントやポイントカードを活用し、リアル・バーチャルを問わず、貯めたポイントで商品を入手する方法をとっているのが特徴である。また、コンサートチケットの入手を電子私書箱から携帯電話へのダウンロードによって行っており、プレイガイドに行ってチケットを入手するという従来型の動線が解消されていることも特徴である。

表 2-6　主婦 B さんの平日における決済利用シーン

項番	利用場所	使用媒体	端末	決済額	特徴
①	自宅	キャッシュカード	デビットカード端末	29800 円	代金引換サービス
②	ショッピングセンター内のスーパーマーケット	ポイントカード	ポイントカード用端末	1980 ポイント	ポイント使用
③	ショッピングセンター内のレストラン	現金	なし	620 円	

④	自宅	クレジットカード	自宅の PC	79800 円	電話による申込
⑤	自宅	インターネット	自宅の PC	3000 ポイント	ポイント使用
⑥	駅	磁気回数券	改札機等	860 円	
⑦	【参考】コンサート会場	携帯電話	バーコードリーダ	―	事前購入したチケットなので、当該使用時点での決済行為は発生していない。
⑧	コンサート会場の売店	現金	なし	3000 円	
⑨	タクシー	クレジットカード	クレジットカード端末	12000 円	

2.4 便利な決済に潜むリスクとトラブル事例

前節で、単なるキャッシュレス決済にとどまらない、利用者の日常生活における便利な決済方法を紹介した。本節では、便利な決済に潜むリスクについてトラブル事例を混じえながら記述する。

2.4.1 リアルな決済場面のリスク

リアル決済は対面が基本であるので、バーチャル決済と比較して、所有者自身の注意によりトラブルを避けることができる可能性は高いが、購入時には各決済事業者が配布する「利用の手引き」などに目を通しておくことも大事である。

(1) 偽変造

平成 3 年頃から、テレホンカードやパチンコカードなどのプリペイドカードの偽造が社会問題化した。現在でもハイウェイカードや高速道路回数券の偽造が後を絶たない状況を受け、日本道路公団は、平成 15 年 3 月に 5 万円及び 3 万円ハイウェイカードの販売を停止し、平成 16 年 3 月からその利用も停止したが、過去数年間にわたる偽造による被害額は、250 億円規模に達する状況にある[16]。また高速道路回数券についても、平成 17 年 3 月 31 日をもって販売を停止し、同年 8 月 31 日をもって利用を停止することを決定した[17]。

パソコンやスキャナー、プリンターなどのＩＴ技術の進歩は、同時に偽造技術をも高度化させてきた。平成 16 年の 11 月から発行された新紙幣には偽造防止技術がふんだんに盛り込まれているが、新紙幣への切り替えと同期するかのように平成 16 年末から偽造旧 1 万円券等を使用した

[16] 日本道路公団プレスリリース：平成 16 年 10 月 13 日
[17] 日本道路公団プレスリリース：平成 16 年 12 月 17 日

犯罪が多発している。これを受け、「新券の流通を一段と促進する必要があると判断し、平成 17 年 1 月 17 日以降、取引先金融機関に対する銀行券支払いについて、現在実施している新旧両券の並行支払いから、新券の全量支払いに移行する。」と日本銀行が発表した[18]。また、偽造された新 500 円硬貨[19]が使用される事件が発生し、ＡＴＭでの硬貨受け入れ停止や、新旧両 500 円硬貨とも利用出来ない自動販売機も存在するようになるなど、貨幣の信用そのものにかかわる社会問題となっている。

プリペイドカードについても同様である。せっかく便利な決済機能を持ったカードが発行されても、偽造対策として高額券が廃止されたり、利用範囲が縮小されたりするなどにより、使い勝手の良くないものとなってしまう。また消費者は、万一知らずに偽造プリペイドカードを持ってしまっても、それを使用することは許されず、結局、不利益を被ることになりかねない。安価であるなどのうまい話を鵜呑みにせず、発行者が指定する販売代理店等でプリペイドカードを購入することが大事である。

(2) 本人以外による不正使用

クレジットカード・キャッシュカードは本人以外の使用が出来ないが、その盗難や偽造で本人以外に使用されてしまう事件が多発している。クレジットカードの偽造問題も大きな社会問題となっており、盗難やスキミングによりクレジットカードを偽造され使用されてしまう事件が発生している。平成 15 年（1 月～12 月）におけるクレジットカードの不正使用額は 271.8 億円にのぼっている[20]。また、キャッシュカードについても、偽造されたり、暗証番号が設定されているにも関わらず預金が不正に引き出されたりする被害が拡大しており、全国銀行協会でも注意を呼びかけている[21]。

暗証番号が設定されているにもかかわらず不正使用される原因として、「暗証番号ののぞき見」「個人情報との紐付けによる類推」がある。まず、前者の例として、本人確認に広く用いられる「4 桁の暗証番号」について触れる。自宅以外で 4 桁の暗証番号を入力するサービス等の例を表 2-7 に示す。必ずしも数字 4 桁入力とは限らないサービスもあるが、利用シーンに含めている。4 桁の暗証番号入力は、金融機関ＡＴＭでの端末操作が唯一ではなく、くらしのさまざまなシーンで利用されていることがわかる。

もっとも、サービス提供手段が電話・インターネットなど複数の場合、一般には、インターネットでのサービス利用時には 4 桁の数字とは別に、英数字 4 桁以上の文字列を設定し、当該文字列の入力を要求する運用が多い。

表 2-7　自宅以外で 4 桁の暗証番号を入力するサービス等

[18] 日本銀行（http://www.boj.or.jp/money/05/bnnew16_f.htm）
[19] 財務省ホームページ（http://www.mof.go.jp/jouhou/sonota/ks170203.pdf）
[20] 日本クレジット産業協会（http://www.jccia.or.jp/）より
[21] 全国銀行協会（http://www.zenginkyo.or.jp/extra/extra03/index0300.html）より

サービス等	場所・利用端末[22]	備考
航空会社のテレホンサービス（予約・マイレージ照会など）[23]	・公衆電話機のダイヤルボタン ・街頭設置の PC のキーボード	
住民基本台帳カードの交付	・役場窓口での暗証番号入力用テンキー	
簡易インターネット接続サービス	・IC カード公衆電話機[24]のダイヤルボタン	
金融機関のテレホンバンキング	・公衆電話機のダイヤルボタン ・街頭設置の PC のキーボード	
留守番電話メッセージの遠隔操作	公衆電話機のダイヤルボタン	
クレジット通話	公衆電話機のダイヤルボタン	
伝言ダイヤル	公衆電話機のダイヤルボタン	
貴重品ロッカーの開錠	スポーツジム・ゴルフ場等に設置されたロッカーのテンキー	
入退室管理システム	ビル・マンション出入口の暗証番号入力用テンキー	
クレジットカードでのショッピング	暗証番号入力用テンキー	2.3.2(1)「会社員 A さんの平日」参照
デビットカードでのショッピング	暗証番号入力用テンキー	2.3.2(1)「会社員 A さんの平日」参照
金融機関窓口での預金引き出し	暗証番号入力用テンキー	
ATM での暗証番号変更	金融機関に設置された ATM	
ATM での預金引き出し	金融機関・コンビニエンスストア等に設置された ATM	

次に、後者について触れる。暗証番号については、60%強の利用者が、誕生日もしくは電話番号を当てはめているという調査結果もある[25]。個人情報保護法では「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、それによって当該個人を識別できるものを含む）」（個人情報保護法第 2 条 1 項）と定義されている。この定義によれば、誕生日は言うに及ばず、電話番号も「個人情報」に該当するといえる。利用者の与り知らないと

[22] 番号入力を携帯電話で利用できるケースもあるが、利用者が、他人に見られないように体の向きを変える、人目のつかない場所で操作するなどの状況を利用者が自ら作り出すことができるので、利用端末としては携帯電話を除外している。

[23] このうち、日本航空グループが提供する「ＪＡＬマイレージバンク」におけるアクセス番号は、平成 16 年 10 月に、4 桁入力から 6 桁入力に変更されている。

[24] ＮＴＴ東日本・ＮＴＴ西日本は、ＩＣカード公衆電話機を平成 18 年 3 月末までに撤去・廃止すると発表した（平成 17 年 1 月 20 日付プレスリリース）。

[25] 中山、小松「バイオメトリックスによる個人認証技術の現状と課題」日本銀行金融研究所　金融研究（平成 12 年 4 月）

ころで企業等が保有する顧客情報が流出した場合、当該情報と紐付けされた個人情報から暗証番号を類推されてしまう恐れがある。また、かばんごと盗まれた場合、その中に入っているカード以外の携行品（運転免許証・健康保険証・パスポートなど）に記載の数字情報を基に暗証番号を類推される可能性もある。特に、インターネット決済における現状の本人確認手段は、口座番号と暗証番号、あるいはカード番号と有効期限を入力することによる場合が多い。たとえＳＳＬを使用しているサービスであっても、「覗き見たカード番号」と「流出した個人情報を基に類推した4 桁の暗証番号」の組み合わせで、カード媒体そのものを持つことなく認証が完了し、不正使用につながってしまう。

(3) 紛失・破損

- 「まだ残高がたくさんあるプリペイドカードを紛失してしまった。カード発行者からは『再発行は出来ません』と言われたが、どうしたらよいか」
- 「ＩＣカード型プリペイドカードが壊れてしまったが、どうしたらよいか」

プリペイドカードを紛失してしまうと、所有者を特定出来ないため再発行されることはない。ただし、クレジットカードのように所有者が特定できる場合は、約款等に基づき再発行される場合もある。破損についてもその状態により、約款等に基づき処理されることとなるので発行者に相談するべきである。

(4) 使用期限、その他

- 「うっかりして使用しないまま、プリペイドカードの使用期限を過ぎてしまった。どうしたらよいか」
- 「海外に赴任する等、プリペイドカードを利用する機会がないので、返金してほしい」

プリペイドカードにもクレジットカード同様、使用期限が設定されているものがある。発行者側の都合であれば別だが、消費者側の都合により返金されるケースは少ないと考えるべきである。使用期限があることを承知で購入したわけであり、発行者との利用上の約束事であるから、それを実行しなかったのは消費者の自己責任であるといわざるを得ない。ここでも大事なことは購入時に「利用の手引き」などを読み、使用の目的に合ったものかどうかを確認して購入することが大事である。

もっとも、良心的な発行者では手数料を取られるものの返金に応じるケースもあると言う。（換金と返金では扱いが違う様子である）

2.4.2 バーチャルな決済場面のリスク

バーチャル決済は、非対面となるので、取引相手を信頼するに値するかを見極めることが一番大事であるが、同時に端末操作面等でもリアル決済とは違う慎重さが要求される。

(1) 商品未着（インターネットショッピング）

- 「インターネットショッピングで代金を前払いしたのに商品が届かない。電子メールを送

ると「明日発送する」とのメールが入るだけである。事業者の電話番号が不明なので、メール以外の連絡がとれない。」

- 「業者のホームページを見て、商品を注文した。注文書の画面に住所や電話番号、クレジットカードの番号を入力した。しかし、商品が届かない。不審に思ってアクセスすると、ホームページがネット上から消えていた。」

インターネット上にショッピングサイトを立ち上げることは難しいことではなく、インターネット上のアドレスだけでは業者の実際の所在や素性を判断することは出来ない。逆に言えば、昨日あったサイトが今日無くなっているということも十分にありうるのである。代金を払ったのに商品が届かないというトラブルを回避するには、信用できる店舗、業者で購入することが一番重要である。

(2) 商品未着（インターネットオークション）

- 「インターネットオークションで、商品を格安で売るという情報をみて代金を支払ったあと、いくら待っても商品が届かない」

大手のオークションサイトでは、出品者の評価を示すなどにより購入者が取引相手の信用度を判断する工夫がされているが、ショッピングサイトを立ち上げている業者とは違い、あくまでも相手とは非対面の個人が相手であるというリスクの高さを認識するべきであろう。もし、代金を振り込んだ銀行口座が架空名義の口座だったら、トラブルのあとで相手を捜し出すことは困難である。

(3) 注文した商品と違う

- 「ホームページで有名ブランドのスニーカーを注文した。代金引換郵便で支払いをしたが、商品を確認すると偽物だった。」

送られてきた商品が注文した物と違う、偽物あるいは別商品だったというトラブルも多く発生しているが、ＰＣの画面上で細部を確認することは難しく、いわゆる「言った、言わない」的な思い違いでの購入をしてしまうことの無いように、信用出来ない業者から購入しないことはもとより、不明な点があれば、業者に確認することが大事である。

その他注意が必要なこと

- 「音楽をダウンロードしていたが、国際電話の請求がきて初めて、海外につながっていたことが分かった。支払わねばならないか。」
- 「申し込みボタンをうっかり２回クリックしたら二重注文になってしまった。」

インターネットでさまざまなサイトを閲覧していると、たびたび新たなウィンドウが開くことがあり、よく意味がわからないままクリックしてしまい、知らないうちに不正プログラムを自分のパソコンにダウンロードしてしまうことがある。その結果、次回のパソコン起動時からプロバイダの接続先が海外のプロバイダに設定変更されてしまい、そのまま気づかずに利用すれば、当然ながらインターネット接続時間分の国際電話料金が請求されることとなってしまう。

また、二重注文を防止するため、良心的な店舗では購入の確認をする画面が複数回現れるが、そうでない場合は誤操作や勘違いでキーボードやマウスのボタンを押し間違えることもあるので、

慎重な操作が必要である。

- 参考（財）日本消費者協会（http://www1.sphere.ne.jp/jca-home/densi/index.html）

2.5 便利な決済の今後の課題と対策

2.5.1 利用上の注意

決済システムは、決済用ツール（ＩＣカード、携帯電話、ＰＣ等）と、ＡＴＭなどのカード読み取り端末、ネットワーク、そして発行者側のセンター端末と広範囲である。それぞれにおいて注意すべき点があるが、本章では、決済用ツールを中心に、利用者が自ら注意できる範囲で記述することとする。

(1) リアル決済時

使用上の注意の遵守

ＩＣカードについていえば、接触型、非接触型とも、曲げや熱などの衝撃を発生させないような利用を心がける必要がある。日常生活においてカードを携行する際、

- 財布に入れた状態で椅子に座ったときに、お尻の湾曲に合わせてカードが曲げられる場合
- 財布の小銭入れについているボタンでＩＣチップが押される場合
- カードを落として靴などで踏まれたり、物体がカード上に落ちたりする場合

などがある。ＩＣカードの耐久性評価試験についてＪＩＳ等で評価項目・評価方法が規定されてはいるものの、一般的には、当該項目・方法に加え、想定されるカードの扱い方に合わせてカードメーカ独自の試験基準を策定して製造する場合が多い[26]。しかし、このような独自の試験基準を満たしているからといって、利用者がカードを粗雑に扱ってもよいということにはならない。例えば、プリペイド残高がＩＣに記録されたカードが故障した際、取扱方法に落ち度があると判断された場合、残高が返金されないこともあるので、十分注意する必要がある。

管理責任

ここ数年、キャッシュカードとプリペイドカード、クレジットカードが一体となった「複合カード」や電子マネー機能を搭載した携帯電話が利用されてきており、利用者にとっては一つの媒体にさまざまな機能が集約されていることは大変便利である。しかし、その反面これらの紛失や破損は、その端末に記録されている情報が流出した場合に不正利用される可能性や、一つの機能の破損により、その他の機能まで利用出来なくなる可能性もある。また故障修理や再発行の場合の相当期間にもその全ての機能が利用出来なくなるといったリスクを併せ持っている。

普段所有しているものの中で紛失して一番困るものは何かと聞かれた場合、多くの利用者は、まず携帯電話を挙げるものと思われる。今後ますます決済ツールとして利用される可能性が高い機器であり、通話機能はもちろん、メール機能、スケジュール管理機能、電話帳機能、カメラ機能と、個人的な情報が集約されており、個人のアイデンティティそのままであるという使われ方

[26] 伊達、鷺、下山、菅野、土橋「ＩＣテレホンカードの開発と展開」NTT R&D、pp.626-633, 1999

をしている。平成 17 年 4 月から、個人情報保護法が全面施行されるが、この携帯電話の紛失については予想以上のリスクが潜在していると考えるべきである。

また、決済の場面では、特に詐欺によるリスクが大きいが、人の弱みにつけ込む輩の間では個人情報が商売のネタとなっており、名簿などが高価で闇取引されている。とりわけ、暗証番号入力を伴うサービスを利用する際は、端末と通路の位置関係や暗証番号入力装置へののぞき見防止ケースなど第三者にのぞき見されないように配慮された環境を選ぶことが自己防衛手段の一つである。パスワードの定期的な変更やクレジットカードやキャッシュカードを紛失した場合は速やかに発行会社に連絡をとることはもちろん、信頼できる店舗以外ではカードサービスを使用しないよう心がけるべきである。

決済用ツールのみならずそれに付随する情報の管理責任は、決済事業者でもなくカードメーカでもなく販売店でもなく、他ならぬ自分自身が負っていることを自覚することが、便利な決済を利用する資格と言っても過言ではない。

⑵ バーチャル決済時

接続先の確認

ＡＤＳＬ等での常時接続の場合はダイヤルアップしないので、この心配はないが、ノートパソコンを自宅以外に持ち出し、ダイヤルアップ接続で利用する機会があるならば注意が必要と言える。これはプロバイダなどから接続先が海外に設定されている場合に確認を求めるソフトが配布されているので、そういったものを利用したり、接続先を随時確認したりすることが必要である。（具体的には、Windows ベースのＰＣの場合、「スタート」→「設定」→「コントロールパネル」→「ネットワークとダイヤルアップ接続」の画面を確認し、不明な接続先があれば削除する。）

ダウンロードの危険性

決済端末として利用する家庭のパソコンへのウイルスやスパイウェア等の脅威への対策については第 5 章で述べるが、決済に必要なプログラムもまたバージョンアップをする必要がある。それは主にセキュリティ対策のためであり、自己防衛のために常に注意することが必要である。しかし、一番肝心なことは、プログラムをダウンロードする際には、どういうプログラムで何が行われるのかをしっかり把握することである。いかなるプログラムをダウンロードする際にも、注意事項を読まずに「同意する」ボタンをクリックしてはならない。ネットワークは「繋がっている」からこそメリットを享受できるものであるが、逆に「繋がっていることの脅威」を考えるべきであり、不用意なソフトのダウンロードにより予想もつかない情報が流出し、第三者にも迷惑が及ぶ可能性が存在することを認識するべきである。

個人情報の入力

クレジットカード情報や個人情報の入力を必要とするページには、ＳＳＬが採用されているかどうかを確認することが大事であり、暗号化されていないサイト（図 2-9 参照）でのクレジットカード情報や個人情報の入力は避けるべきである。

図 2-9　ＳＳＬのイメージ

ＳＳＬを利用したウェブページは、ホームページアドレスが「http://」ではなく「https://」であり、インターネットエクスプローラであれば、右下に鍵マークが表示されることで判別ができる（図 2-10 参照）。なお、たとえＳＳＬを使用したサイトといえども、ネットカフェ・ショウルームなど、不特定多数の人が使うパソコンで、クレジット情報や暗証番号などを入力することは避けるべきである。このようなパソコンに「キーロガー（5.2.5 項参照）」というソフトウェアが仕掛けられ、キーボード入力履歴からクレジットカード情報などが第三者に不正に取得され、なりすましによる不正使用で本来の利用者が被害を受ける事件も発生している。

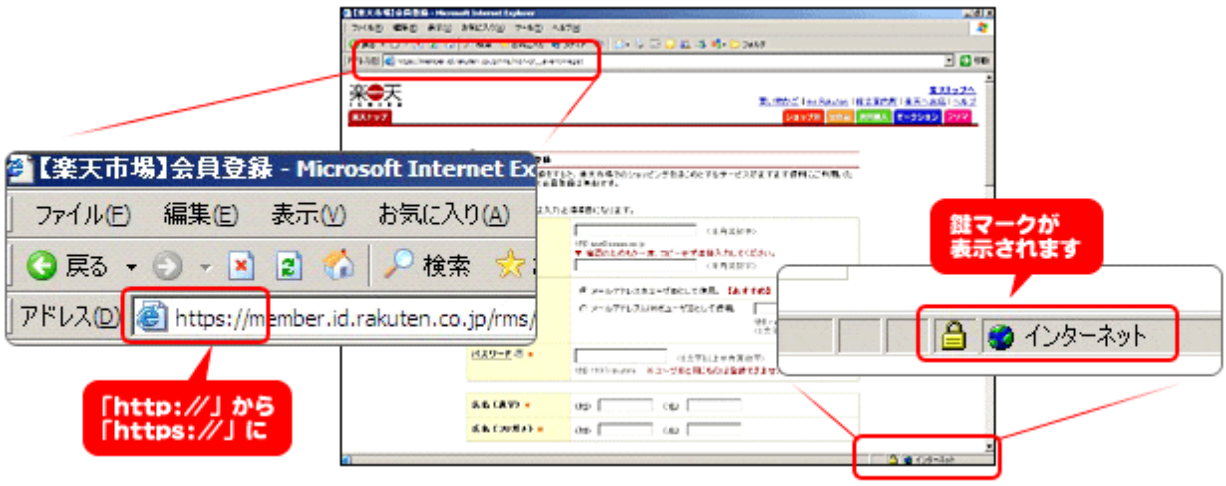


図 2-10　ＳＳＬを利用した Web サービスのイメージ

また、2.3.2 項での主婦 B さんの平日に「身に覚えのないところからの電子メール」がある。主婦 B さんは、クレジットカード会社のサイトにアクセスする前に、自分宛の電子メールをチェ

ックしている。この場合、「会員情報現行化のため、下記ＵＲＬのサイトにて会員番号・氏名等を入力してください」なるメールが届き、記載内容を鵜呑みにして Web サイトにアクセスし、うっかり個人情報を入力してしまうケースも想定される。このようなメールがすべて不正メールであるというわけではないが、個人の特定につながる情報の入力を要求するメールに関しては、特に注意する必要がある。（5.2.3 項参照）

2.5.2　法制度面

総務省では、平成 17 年 1 月 10 日、インターネットを利用する顧客の個人情報がネット接続事業者などから外部流出するケースが相次いでいるのに対応するため、情報管理体制に関する数十項目に上る安全基準を設け、接続事業者を格付けする方針を固めたと発表[27]しており、情報社会の脆弱性に警鐘を鳴らしている。しかし安全な接続事業者（インターネットサービスプロバイダ）を選択するだけでは十分とはいえない。インターネット上のショッピングやオークションでは、そのサイトを開設している業者や、取引相手の信用度を見きわめ、消費者自身が自衛することがトラブルに巻き込まれない方法である。以下にトラブル防止のためのいくつかの方法を紹介する。

（1）オンラインマーク

図 2-11　オンラインマーク

前節でも述べたが、「お金を振り込んだのに商品が届かない」、「事業者がいつの間にかいなくなってしまった」、「注文したのとは違う商品が届いた」等のオンラインショッピングに関する消費者の苦情も増加傾向にあるという状況を受け、消費者が安心して利用できる環境作りのために、（社）日本通信販売協会と日本商工会議所では、一定の基準をクリアしたショップに対して「オンラインマーク」（図 2-11 参照）を発行し、ホームページ上に表示してもらう制度を平成 12 年 5 月よりスタートしている。消費者はこのマークをクリックすることにより、事業者の概要を知ることができる仕組みとなっている。

オンラインマークがついている業者は、下記の内容が認証されており、消費者がオンラインショッピングをする際、安心に購入する目安となり、現在、約 600 業者が登録されている。

＜オンラインマークの認証内容＞[28]

- 通信販売事業者の実在（商業登記簿謄本または抄本，住民票等による確認）
- 申請サイト上での特定商取引法による通信販売広告の表示義務事項の表示
- 広告表現の特定商取引法その他関連法令の遵守

具体的な確認方法としては、

---

[27] Yahoo!NEWS（http://headlines.yahoo.co.jp/hl?a=20050111-00000201-yom-soci）より
[28] （社）日本通信販売協会　http://www.jadma.org/ost/index.html

① 事業者のホームページにアクセスしてオンラインマークが表示されたら、マークをクリックする。
② その事業者の概要、オンラインマーク制度の概要、日本通信販売協会、消費者相談窓口などが表示される認定画面があらわれる。
③ その画面の中に、オンラインマークが付与されたドメイン名が記載してあるので、実際にアクセスしたＵＲＬと同じかどうか確認する。また、オンラインマーク付与事業者一覧においても、本当にオンラインマークが付与された事業者かどうか確認することができる。

オンラインマークの中の番号とは

オンラインマークの右下の空白の部分には、事業者の認証番号が入る（図 2-12 参照）。

図 2-12　オンラインマークにおける事業者認証番号

- 認証番号例

Ｊ	１２３４５	－１	－０１
〔1〕	〔2〕	〔3〕	〔4〕

〔1〕最初のアルファベットは、審査を行った審査機関を表します。
「Ｊ」は、社団法人日本通信販売協会が発行したものです。
「Ａ」は、日本商工会議所が発行したものです。
〔2〕「１２３４５」は、事業者番号です。
〔3〕「１」は、事業者のホームページが１つであることを表します。ドメイン名の異なる複数のホームページをもつ事業者で、２つ以上のドメイン名でオンラインマーク付与されている事業者は、付与されたドメイン名の数を表します。
〔4〕最後の「０１」は、更新の回数、つまりオンラインマークを付与されている年数を表します。

（2）プライバシーマーク

図 2-13　プライバシーマーク

プライバシーマーク制度は、事業者からの申請に基づき個人情報保護に関するＪＩＳ（JIS Q 15001:1999 個人情報保護に関するコンプライアンス・プログラムの要求事項）に適合し、個人情報の取扱いを適切に行うための体制を整備しているか否かにつき、第三者機関である（財）日本情報処理開発協会（及びその指定機関）が審査し、適合している者についてはその旨を認定するとともに、その証としてプライバシーマークと称するロゴの使用を許諾する制度である。平成10年4月1日より運用が開始され、平成16年11月には、1,000事業者を突破した[29]。最近では、個人情報が記載された証明書類の封入・発送業務やオンラインシステムの構築・運用業務等の調達において、プライバシーマーク付与に関する認定取得が応札要件に課せられる場合が多くなってきており、プライバシーマーク制度の社会的位置づけがますます重要になりつつある。

インターネットショッピングや会員制のサイトを楽しむためには個人情報を提供する場合が多いが、その個人情報の漏洩問題も社会問題化している。情報が漏洩する要素はさまざまだが、ホームページ上でこのマークの有無を確認することも、個人情報の提供を伴う会員サービスを安全に楽しむ方法の一つである。

（3）エスクローサービス

インターネットオークションで、個人間での「代金を支払った・支払われていない」や「品物を送った・受けとっていない」などのトラブルを解消するための方法として、「エスクロー（寄託）サービス」がある。これは商品の配送、代金の回収を第三者に寄託する仲介サービスであるが、下記にオークションでも人気のあるYahoo! JAPANによる説明を掲載する[30]。

[29] http://www.jipdec.jp/より
[30] http://auctions.yahoo.co.jp/jp/phtml/auc/jp/notice/promo/escrow/guide.html

エスクローサービスとは？

図 2-14　エスクローサービスの仕組み

簡単に言うと、出品者と落札者の間に業者が入り、

1. お金　と　**2. 商品**　の流れを取り持つサービスです。

安全な取引を行うために、商品の内容や到着を確認してからお金を振り込んだり、商品の受け渡しが簡単にできるように物流サービスを提供したりします。

エスクローは、Yahoo! JAPAN ではない第三者企業が提供するサービスで、企業によってそのサービス内容や手数料等が異なりますが、ここでは簡単に一般的な流れをご紹介しましょう。

エスクローサービス利用のメリット

● **出品者のメリット**

・ 安心して入札できるので、より多くのユーザーの入札が期待できる。また、高額商品の取引の可能性も広がる。
・ 「商品を送ったのにお金が払われない」というトラブルを未然に防ぐことができる。
・ 商品を集荷に来てくれるので便利。
・ 銀行まで行かずに入金確認が可能。

● **落札者のメリット**

・ 「お金を支払ったのに商品が届かない」等のトラブル防止。「届いた商品が出品されていたものとは全く違うものだった」等の場合でも、商品を受領しない限り出品者にはお金は支払われません。

● **その他のメリット**

（※以下は企業によっては提供していないサービスもあります。また、料金やサービス内容が異なる場合もありますので、必ずエスクロー一覧でご確認ください。）

・ 配送料金や振込み手数料等が、エスクローサービスを利用したほうが安い場合がある（全国一律料金のエスクローサービスも）。
・ クレジットカードでの支払いや、分割払いが選択可能。

エスクローサービスあれこれ

- **エスクローサービスは Yahoo! JAPAN が提供するサービスではなく、第三者企業が提供するサービスです。**

また、エスクローサービス提供会社は１社ではなく、複数社のサービスを導入。ユーザーの皆さんが、自分にあったエスクローサービスを選んでご利用いただけます。

- **それぞれの企業が提供するサービス内容や手数料は若干異なります。**

例えば物流に関して、自宅まで商品を取りに来てくれるサービスもあれば、コンビニから発送できるサービスもあります。事前に確認してご利用ください。

- **エスクローサービスは、そのサービスを利用するか否か、またどの提供企業のサービスを利用できるかを含めて、まず出品者より希望条件が出されます。**

出品者の指定した条件のなかから（エスクローサービス利用の有無、またはサービス提供会社の選定を含め）入札者が条件を選択して、入札をします。落札後は、落札者の選んだエスクローサービスを利用して商品や代金のやり取りを行います。また、利用したいエスクローサービスを出品者が選択していない場合は落札後でも出品者にメールで希望を伝えれば追加してもらうこともできます。

この、エスクローサービスは、第三者企業が提供するサービスなので、商品代金とは別途の手数料がかかることになるが、トラブルを回避し、安心な取引を行う方法の一つである。

（4）法整備の動向

インターネットやＩＣカードの普及等による金融サービスの電子化は世界的な動向であるが、この電子化に伴い、様々な法律問題が発生し、検討されてきた。単純に電子資金移動（ＥＦＴ）及び振込・振替に関する法律問題を考えてみても、ＥＦＴ・振込・振替取引が無権限者によって通信手段やＰＣを用いる偽造、無権代理・無権限者によって取引を変更されるという変造、等がある。ややアナログ的ではあるが、現在問題となっている偽造キャッシュカードの問題も十年ほど前からたびたび報道されており、現在、生体認証を用いたＡＴM機、カードのＩＣカード化、暗証番号といったいくつかのセキュリティ対策が採られているが、実際の事故が発生した場合、それは利用者の損失負担はどの程度になるのかが問題となる。この点について、欧米では、1978 年の米国の連邦ＥＦＴ法を皮切りに、ＥＦＴに関する様々な法制度が作られ、アメリカの連邦ＥＦＴ法における 50 ドルルールのように、その金融機関の責任や利用者の損失負担の割合が明確化されている。しかし、わが国では、昭和 60 年代よりその問題が取り上げられてきてはいたものの、最終的な法制度の確立にまでは至っておらず、現在もその不明確さが残った状況にある。

また、Suica や Edy といった多機能型ＩＣカードを利用したプリペイドカードの登場により、従来の前払式証票規制法（通称：プリカ法）で要求されている券面事項の提示方法に変更が必要になってきている部分がある。さらに、前払い式ではあるが、ＩＣカード等を利用しない（カードが存在しない）Web 上だけで流通する通称・Web マネーの登場により、経済効果は同じであるにもかかわらず、証票の存在するものを規制の対象としている前払式証票規正法の枠組みから外れるものも登場してきた。また、前者・後者の相乗り状態のものや、ＩＣカード化により、ク

レジットカードやキャッシュカード等と統合されたカードも出てきているが、これらの場合の、事故・紛失時の連絡先・負担割合の問題も明確ではない。

以上のような現状に対して、現在、改善を図るための以下のような動きが進んでいる。

後者に関しては、監督官庁である金融庁ならびにその所轄団体である前払式証票発行協会で問題点の検討と法改正へ向けての調査・研究ならびに検討が既にスタートしており、従来の法律の枠組み・概念・規制のあり方を含めた広い範囲での検討が行なわれているところである。

また、前者（一部後者の領域も含むと考えられる）については、平成 16 年 12 月に金融庁が発表した『金融改革プログラム　―　金融サービス立国への挑戦』において、「金融インフラの利便性とコスト競争力の向上を実現するための e-バンキングに関する法制の整備の検討」、「電子的な資金決済、支払い、電子的金融取引に関する法制の整備に向けた検討」が挙げられている。その具体的内容等は明らかにされていないが、そこでは、現在、問題となっている偽造キャッシュカードをめぐる問題や安全対策、さらには、上述した電子決済における責任分担ルールを明確化するためのＥＦＴ法等の検討が行なわれることが予想されている。まさに利用者の利便性の向上とともに、コストパフォーマンスならびにリスクマネージメント能力の向上を目指す政策目標へ向けての法制備の検討がスタートすることになる。

2.5.3　さらなる便利な決済への提言

利用者にとってさらなる便利なサービスを提供する方法を提言する。

⑴ 複数決済手段の単一媒体への集約

2.3.2 項において、会社員 A さんはスポーツ新聞の支払い手段に現金を用いているが、鉄道改札用ＩＣカードに電子マネーを付加したカードを売店で使用可能となることで、釣銭の発生が解消されるだけでなく、「売店での支払い時にＩＣカードを定期入れから取り出し⇒決済用端末にかざす⇒財布にしまうことなく、改札機にかざす」という動作が実現できる。また、表 2-4 の①ではバスでの運賃支払いにバスカード（磁気式）を使用しているが、鉄道改札用ＩＣカードにバス運賃支払い機能を付加することで、交通手段毎に複数のカードを使い分ける手間を省くことができ、社員証についても同様のことが言える。一般に、テナントとしてオフィスが入居している場合、会社が発行する社員証に加え「テナントビルの入退ゲート通過用」「自動販売機専用カード」など複数枚のカードを所持する場合があるが、出社から退社までの一連の生活動線（図 2-6 では「勤務先のビル」内）を 1 枚のカードで実現できるのが望ましい。特に、このようなカードをＩＣ化することにより、サービス提供者がカード発行後に新たにアプリケーション（例えば、ＰＣログイン）を追加したい場合にも、当該プログラムをＩＣカードにダウンロードすることでカード媒体の都度交換が不要となり、利用者・サービス提供者双方にとってメリットとなりうる。

⑵ 生活動線にあったサービス提供

本来の生活動線から外れる動線を極力減らすように決済用端末を配置することも、さらなる便利な決済実現方法の一つである。2.3.2 項において、会社員 A さんは、自動販売機で電子マネー残高不足に気づき、現金を取りにわざわざ居室まで戻っている。たとえ電子マネーの「出」の場

所が多く存在しても、チャージ、すなわち、「入」を行う場所がごく限られていると、チャージをするためだけに端末に行かなければならないなど、利用者のスムーズな移動に制限が伴ってしまう。この不便さを解消するために、自動販売機にチャージ機能を搭載する、給与天引き後払いを前提として、チャージそのものを不要にするシステムを導入することなどが挙げられる。

また、図 2-7 において、高速道路に入ってから出るまでは一連の生活動線といえる。会社員Ａさんは、料金所でハイウェイカードを使用し、サービスエリア内のレストランで現金を使用している。高速道路利用料金・食事代金と支払い対象は異なるものの、一連の生活動線で決済手段を使い分けるのは利用者にとって煩雑である。これを解決するために、ＥＴＣ車載機を保有しないユーザー層をメインターゲットに、通行料支払い機能とサービスエリアでの決済機能を統合したプリペイドカードを発行することで、高速道路内でのキャッシュレス決済を実現できる。また、当該プリペイドカードをＩＣ化（非接触ＩＣカードまたは非接触インタフェースを有する携帯電話）することにより、変造が困難になるだけでなく、従来の「料金所係員へのカード手渡し→端末へのカード挿入→減算→端末からのカード排出→カード返却」から、「運転者が非接触リーダライタにカードをかざして減算する」だけで済み、料金所での渋滞緩和につながるものと考える。特に、携帯電話に当該決済機能を搭載することで、チャージ機が設置されない場所でもチャージを行うことができるので、高速道路以外にいる時間・空間を有効に活用できる。

(3) ポイントカードの利用範囲拡大

利用者にとって利便性の高いポイントカード使用を目指すには、クローズドなエリアでは共通してポイントサービスを享受できることが必須要件と考えられる。本例において主婦Ｂさんは、ショッピングセンター内のスーパーマーケットではポイントカードを利用しているものの、同じ建物内のレストランでは現金を使用している。

ポイントカード導入の目的は顧客の囲い込みゆえ、自分の店で付与したポイントを他所の店で使用されることは導入の趣旨に反する、という見方も存在する。しかし利用者にとっては、ショッピングセンター内の一連の動線において、店によってポイントカードの使用可否が異なるのは不便である。特にショッピングセンターでは、同業者がテナントとして店を構えるケースは少なく、自店専用ポイントカード発行による顧客囲い込み効果は薄いものと考えられる。むしろ、異業種他店での購入が目的でショッピングセンターに来た顧客を自店にも誘導できるなどの相乗効果を期待すべきものである。

「よく行く店での決済で貯まったポイントを他の商品・サービスの受け取りに充当する」というバリューの利用形態は、「日常的に利用される→さらにポイントカード発行・利用可能端末の増加→カード・端末のコスト低下→さらに導入企業が増える→利用頻度がさらに高くなる」という好循環を生み出し、ポイントカード利用者・発行者双方にとってメリットのあるものである。平成 13 年度に電子商取引推進協議会「決済関連問題検討WG」がまとめた活動報告書「ＴＰＯに整合する決済手段の提言」第４章・第５章において、シチュエーションに応じてさまざまな決済手段が存在することが示されている。ただ、当該報告書の作成以降、「円単位」通貨以外での決済（例えば、ポイントカードでのポイント消費による商品・サービスの引き換え）が顕在化しつつあり、リアル・バーチャルを問わず、「円単位通貨」が商品・サービスの唯一の引き換え手段では

なくなってきている。「円単位通貨」以外での商品・サービス引き換えについても、消費者が安心して利用できるよう、法制度面・運用面での整備が望まれる。

【参考文献】

- 電子商取引推進協議会「ＴＰＯに整合する決済手段の提言」（平成 14 年 3 月）
- 電子商取引推進協議会「Gift 型モバイルプリペイド決済ビジネスモデルの研究報告書」（平成 16 年 3 月）
- 電子商取引推進協議会「モバイルプリペイド決済の実現モデルの調査研究」（平成 15 年 3 月）

2.6　まとめ

今後、便利な決済の方向としては、多様化している機能が、マルチアプリケーションＩＣカードや携帯電話など一つのツールに集約されていき、ますますインターネットを利用したバーチャル決済が加速していくものと推測される。消費者にとっては、たくさんのカードを持つことなく、また 24 時間、自宅にいながらにしてショッピングが楽しめる時代になりつつある。しかし、決済のリアル・バーチャルを問わず便利で簡単であるものはそれなりの危険性を併せもっているということを認識しなければならない。特に混沌としたインターネットの世界は信用できるものばかりではなく、個人間取引ではトラブルが起こっても自己責任とならざるを得ないのが現状である。

まず、トラブルに遭わないためには、「自己防衛」することが大変重要であり、わからないものには手を出さず、十分な確認と慎重さを備えることが必要である。特に混沌としたインターネットの世界は信用できるものばかりではなく、個人間取引ではトラブルが起こっても自己責任とならざるを得ないのが現状である。ここで、（財）日本消費者協会による、（インターネットショッピングで）「トラブルにあわないための７箇条[31]」と、Yahoo! JAPAN による、（インターネットオークションで）「詐欺などのトラブルを避けるための７つのチェックポイント[32]」を下記に紹介して、本章のまとめとする。

- トラブルに遭わないための７箇条（（財）日本消費者協会）

１．業者の選択に気をつける。
（オンライントラストマーク、プライバシーマークの有無を確認する。）
２．代金決済方法に気を付ける。
（前払い・代金引換郵便は要注意。クレジットカード決済はセキュリティを確認のこと。）
３．申し込み確認画面で、数量、大きさなどのミスがないか確認する。
４．業者から届く承諾通知書を確認する。
５．個人情報の流出に気をつける。
（パスワード管理等に注意。）

[31] http://www1.sphere.ne.jp/jca-home/densi/index.html
[32] http://auctions.yahoo.co.jp/phtml/auc/jp/notice/instances/7points.html

６．インターネットの情報は信用性に注意が必要。
（ネズミ講等の悪質商法に注意。うまい話は信用しない。）
７．トラブルにあったときには公的機関へ相談を。
（http://www1.sphere.ne.jp/jca-home/index.html）

● 詐欺などのトラブルを避けるための７つのチェックポイント（Yahoo! JAPAN）
１．出品者の説明をよく読みましたか？
２．出品者の評価を確認しましたか？
３．落札後に出品者が誰であるかを確認しましたか？
４．相手の名前を Yahoo! JAPAN の検索を使って調べてみましたか？
５．振込先がトラブル口座リストに掲載されていませんか？
６．振込先の名称を確認しましたか？
７．ほかの落札者から評価が付いているか確認しましたか？
※最後に、あなたの良識をはたらかせて、心配なことがあれば出品者に確認したり、取引をやめたりといった決断をしてください。

3. くらしをとりまくネットワーク環境

くらしの中のネットワークといえば、家庭でのＰＣによるブロードバンド環境や携帯電話によるインターネット接続が代表事例であるが、昨今では、ネットワーク接続可能なデジタル家電の普及や家庭内無線ＬＡＮの導入など、新たなネットワーク接続形態も出現している。

本章では、くらしの中でのネットワーク環境にはどのようなものがあるか、その代表例について簡単に述べる。

3.1 ＰＣでのインターネット接続

全国各地でのＡＤＳＬや光ファイバ網の整備と、事業者間の競争による価格低下により、急速にブロードバンド網が普及している。平成 16 年 3 月末では約 1,500 万契約に達しようという勢いであり、より高速なＦＴＴＨの契約も増加している。

表 3-1　ブロードバンド契約数の推移

（万契約）

（各年度末契約）	平成 11	平成 12	平成 13	平成 14	平成 15
無線（FWA 等）		0.09	0.8	3	3
FTTH		0.02	2.6	31	114
ケーブルインターネット	22	78	146	207	258
DSL	0.02	7.1	238	702	1,120
合計	22	86	387	943	1,495

（出典：総務省 平成 16 年度 情報通信白書）

ＡＤＳＬは電話局からの距離によっては通信速度が十分でないことや、接続さえ出来ないことがあることから、地域によってはＩＳＤＮや定額ＰＨＳでの接続を余儀なくされる場合もある。定額ＰＨＳは電話の一般加入者回線を契約しない若者層の間で携帯電話とセットで使われることも多い。全国的には未だ 3 割程度のダイヤルアップ接続者が存在すると見られる。また、ＣＡＴＶが普及している地域では、ＣＡＴＶ提供会社がインターネットサービスも提供している。

一般的な接続形態の例を下記の図 3-1 に記す。

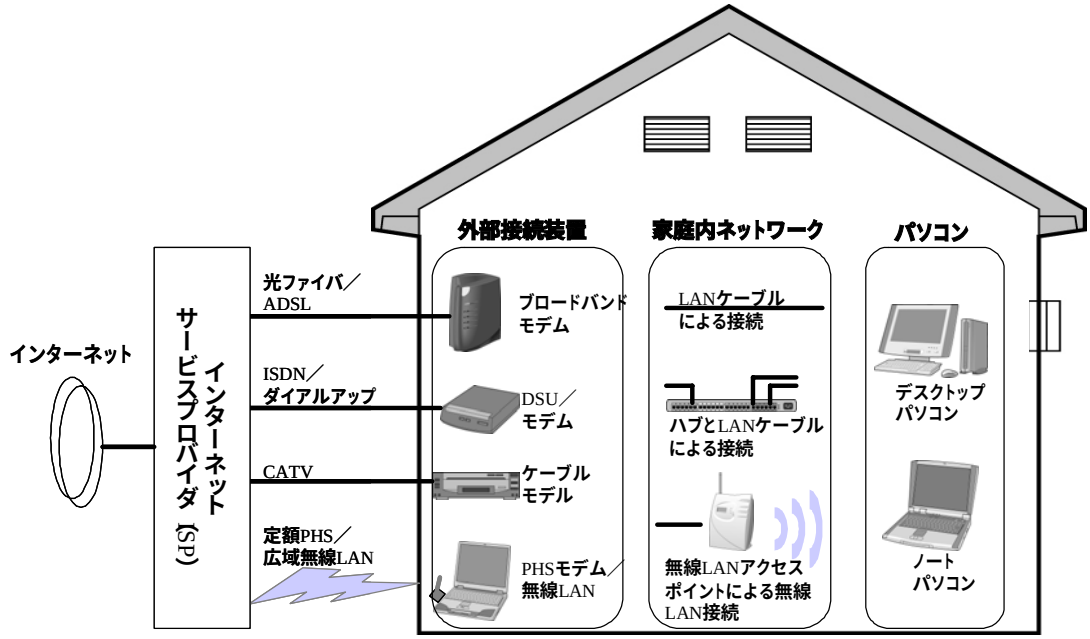


図 3-1　家庭でのインターネット接続方式

3.2　家庭内ＬＡＮ

家庭内ＬＡＮと言えば、狭い範囲でのＬＡＮケーブルによる複数ＰＣの接続もあるが、現在では無線ＬＡＮによる家庭内ＬＡＮが主流である。インターネットサービスプロバイダ（ＩＳＰ）からレンタルするブロードバンドルータにも無線ＬＡＮアクセスポイントが提供され、ノートＰＣには無線ＬＡＮが標準で搭載されていることも多い。また、配線の手間が省けることも普及を促進している。家庭で２台以上の複数のＰＣをインターネットに接続するケースや、ノートＰＣを場所にこだわらず自由に使いたい場合に家庭内無線ＬＡＮが構築されるが、昨今ではＰＣ以外の情報家電やゲーム機を接続するケースもある。

3.3　携帯電話

携帯電話はＰＣ以上に個人単位で普及しており、また使用者の年齢層も幅広いのが特徴である。85%以上の携帯電話がインターネット接続可能となっており、メールやショッピング、サイト接続に使用されている。さらに、赤外線通信や非接触ＩＣカード機能を持つ携帯電話ではクレジットカードや電子マネー、チケットなどの高度なサービスも使えるものも登場した。

表 3-2　携帯電話及び携帯インターネット契約数の推移

（万契約）

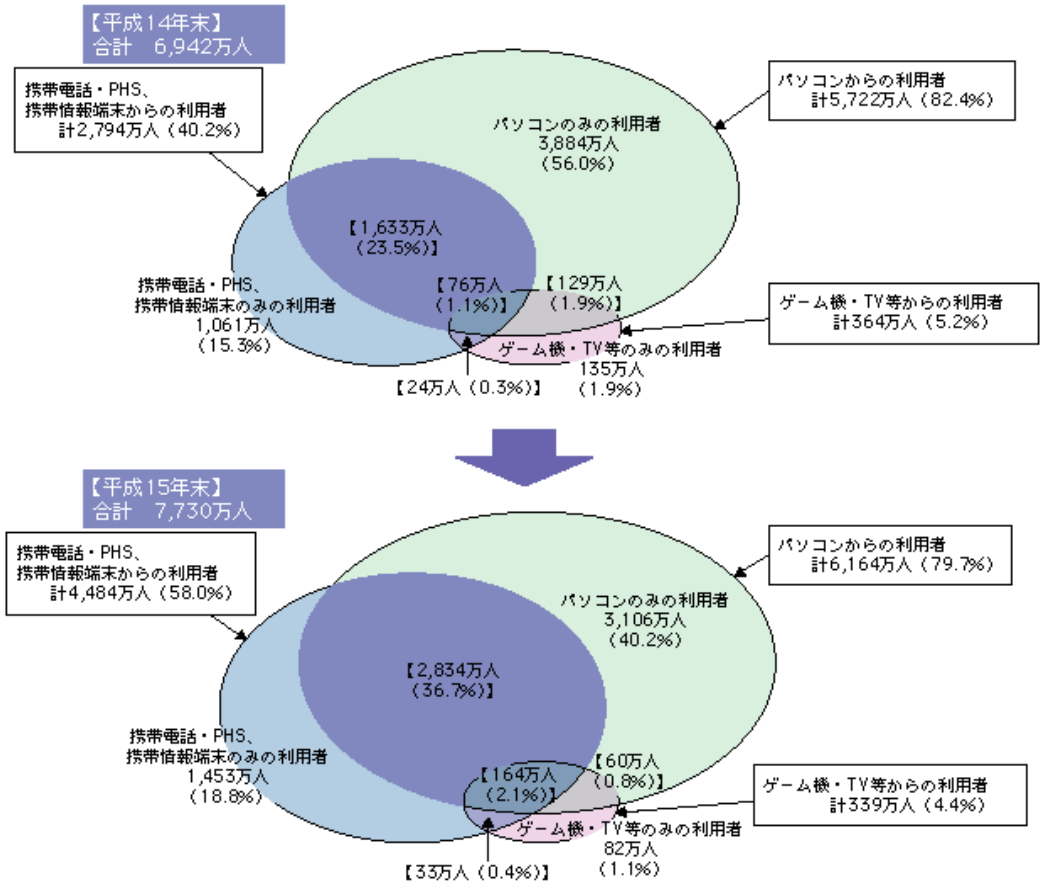
	平成11年3月	12年3月	13年3月	14年3月	15年3月	16年3月
契約数	4,153	5,114	6,094	6,912	7,566	8,152
携帯インターネット契約数	5	750	3,457	5,193	6,246	6,973

（出典：総務省 平成16年度 情報通信白書）

3.4　情報家電

情報家電というと近未来のイメージがあるが、最近の家電の中にはネットワークと連動するものが増えている。例えば地上波デジタルＴＶなどは双方向サービスを売りにしている。ハードディスク付きＤＶＤレコーダーには番組表をインターネット経由で取得するものあるし、外出中にでも携帯電話やインターネット経由で予約できる機能を持ったものもある。

家電とは分類されないかもしれないが、家庭用ゲーム機にもインターネット機能があり、ネットゲームなどを楽しめるものも販売されている。



※【　】内は、3つの円の重なり部分の人数。（　）内は、6歳以上のインターネット利用者に占める割合。
なお、端数処理のために、一部合計値が一致しない箇所がある

（出典）総務省「通信利用動向調査」

図 3-2　個人のインターネット接続端末

3.5　将来的なネットワーク環境

家電のＩＴ化やインターネットの普及により、今後も家庭をターゲットに様々な技術が開発・規格化されようとしており、ネットワークについても同様である。下記に今後家庭に導入される可能性のあるネットワーク技術とその特徴を示す。

3.5.1　電灯線ネットワーク

電灯線通信（別名：電力線データ通信，電力線通信，電灯線搬送通信，ＰＬＣ：Power Line Communication，電灯線データ通信）により形成されるネットワークを電灯線ネットワークと呼ぶ。

ＩＴ用語辞典によると、この電灯線通信とは、電力線を通信回線として利用する技術のことで、電気のコンセントに通信用のアダプタ（ＰＬＣモデム）を設置してパソコンなどをつなぐことにより、数 Mbps～数百 Mbps のデータ通信が可能と言われている。

ほとんどの建物には電気配線が張り巡らされているため、新たにケーブルなどを敷設することなく手軽に構内通信網を構築できる。また、電力会社の配電網をそのまま通信インフラとして利用することができ、インターネット接続サービスなどが提供できる。

ただし、電力線はもともと高い周波数の電気信号を流すことを想定していないため、漏洩電波がアマチュア無線などに深刻な影響を与えるのではないかとの指摘もあり、実用化できるかどうかは未知数の状況にある。構内通信に限って電力線を使うという形態も提案されている。

次に将来的な企業としての実際の活用事例として、2004 年 1 月の International CES における基調講演でのレポートを pc.watch.impress の 1 月 10 日付記事より紹介する。（以下 http://pc.watch.impress.co.jp/docs/2004/0110/ces08.htm より抜粋）.

● **電灯線ですべてをつなぐ**

電灯線を使い、170Mbps の通信が可能なネットワーク技術のデモンストレーションを行なった。多くの家電製品は、家庭内の電灯線（ＡＣライン）から電源を取る。これをネットワークとして利用できるなら、家電製品は、配線を新たに行なうことなく接続できるようになるわけだ。

この技術は、米国の電灯線通信（Power Line Communication）の規格策定団体である Home Plug Alliance により提案され、その基本部分が「Home Plug AV」という規格に採用されることが決まっている。デモンストレーションしたものは、日本の大手家電メーカが「HD-PLC」（High Definition ready high speed Power Line Communication）と呼ぶ技術で、Home Plug AV そのものではないが、同じ技術を利用するもの。

開発中のＡＶサーバとデジタルテレビの間をアダプタを使って電灯線ネットワークで接続し、電灯線を使ってＨＤＴＶクオリティの動画の送信が可能であることをデモンストレーションした。テレビとＡＶサーバの間にあるＡＣケーブルをつなぐことで、反対側にある電灯が点り、ＨＤＴＶの再生が始まる。ケーブルを抜けば、電灯が消え、同時に動画の再生が止まる。再度、接続すると、電灯はすぐ点灯し、その後 10 秒程度で画像の再生が再開された。

● **米国では年内に実用化**

なお、この Home Plug AV は、6 月までには規格として成立させて、2004 年中に商品化する予定だという。また、同規格は、ＥＵ圏を中心に活動する PLCforum（Power Line Communications forum）や日本の PLC-J（高速電力線通信推進協議会）でも、連動して規格化する予定だという。

電力線を使った通信では、2～30MHz 帯を使うため、アマチュア無線などの既存の短波帯無線局への影響があり、実用化が止まっていた状態であった。しかし、HomePlug AV/HD-PLC では、こうした既存無線局に影響する周波数帯を利用しないようにすることで、干渉を起こさないようになっている。

具体的には、周波数を細かく分けて同時に多数のキャリア（搬送波）を使って通信を行なうＯＦＤＭ（Orthogonal Frequency Division Multiplexing)方式を使い、干渉の可能性がある部分は通信に利用しないようにしている。2～30MHz を 512 のバンドに分け、このうち、既存無線局との干渉が発生する帯域は通信に使わないようしている。結果として、約 170～190Mbps（国によって、利用不可能な周波数帯や電灯線通信に利用できる周波数の範囲が違うために通信速度が変わってくる）の通信速度が実現できるとしている。

● 日本での展開は早くても 2005 年以降

日本国内では、法律により、電灯線を使った通信で利用できる周波数帯が低く制限されているため、現在のままでは、国内で HomePlug AV/HD-PLC を実験することさえ出来ない。まずは、国内で干渉状況などを調べる実験を行なうための働きかけを関係省庁に行うことから始めることになるという。

世界的なスケジュールとしては、まず、米国で規格化および製品化を行い、ついで各国向けのローカライズ（利用しない帯域の定義など）を行ったうえでの各国で規格化を行うことになるという。このため、日本などでは、早くとも 2005 年以降の実用化となりそうだという。

さらに最近の動きとして 2004 年 12 月 21 日の日本経済新聞の一面に「コンセントを通じ高速通信・電灯線ネット 2006 年解禁へ」の記事が掲載されて、総務省は「電力線通信」を 2006 年にも解禁する検討に入ると報じられた。また同記事によると、この「電力線通信」は、通信用の大掛かりな配線工事が不要のため、ネットを通じてエアコンや冷蔵庫などを遠隔操作するネット家電が利用しやすくなり、普及に弾みがつく。当面は屋内の配線にとどまるが、将来は全国の電線網にまで利用を認める公算があり、光ファイバと並ぶ通信手段として通信業界の競争を促し、料金引き下げなどの効果も見込まれるとしている。

3.5.2 情報家電ネットワーク

インターネット経由での一部のＡＶ機器のコントロールは既に家庭に入りつつあるが、家庭にある家電同士を接続し、家電のネットワークで家電をコントロールする動きもある。

ソニー、Intel、Microsoft、松下電器などＩＴ系／家電系の複数のベンダが中心となりホームＡＶネットワークの標準規格策定を目指す「ＤＬＮＡ」（Digital Living Network Alliance）に対応した製品が開発されつつあり、ＡＶ家電やＰＣの間で動画や静止画、音声をネットワーク経由でストリーム送信し、マルチメディアコンテンツを家庭内のどこからでもアクセスできるようにするための環境作りが進んでいる。

その他、年配の方のための健康管理や介護、冷蔵庫の中の食料の賞味期限の自動管理、防犯用監視、照明や空調管理などがサービスとして考えられており、プライバシ保護の確立と共に今後の普及が望まれている。

3.5.3　人体間通信

人と人、もしくは人が機械に間接的に触れ合うことで通信を行う技術も開発され、一部は商品化されている。原理的には人間の身体が電気を通したり、あるいは誘導することを利用し、人体と人体もしくは、人体と機械の間で微弱な電流を流すことで通信を行う。この際、人体を流れる電流は体脂肪計と同等の安全なレベルである。

人と人とが直接通信する方式では、通信速度は 4kbps 弱と非常に遅いため、大量のデータを通信することには向かないが、機器の管理など重要なデータを限られた環境で通信することには適している。(参考文献、松下電工：http://www.mew.co.jp/press/0409/0409-3.htm)

また、銅板の上に人間が立ち、その人間が持つ情報端末に映像などのストリーミングを高速に流す人体通信システムも開発されている。人体上の微弱電界を光学式電界センサで検出することにより、ＴＣＰ／ＩＰで 10Mbps の双方向通信を実現する方式であり、銅板の上に靴を履いて乗っていても通信は可能である（図 3-3 参照)。この方式は間接的に触れている部分で通信を行うため、通信のセキュリティは高く、また利用できる場所を極端に限定できる特徴を有していることから一段と利用場所を限定したホットスポット的な利用方法がある。例えば博物館や水族館等の展示物の説明に便利である。通信速度が速いことから展示物等に対し音声と画像による補助的な説明が可能になる。

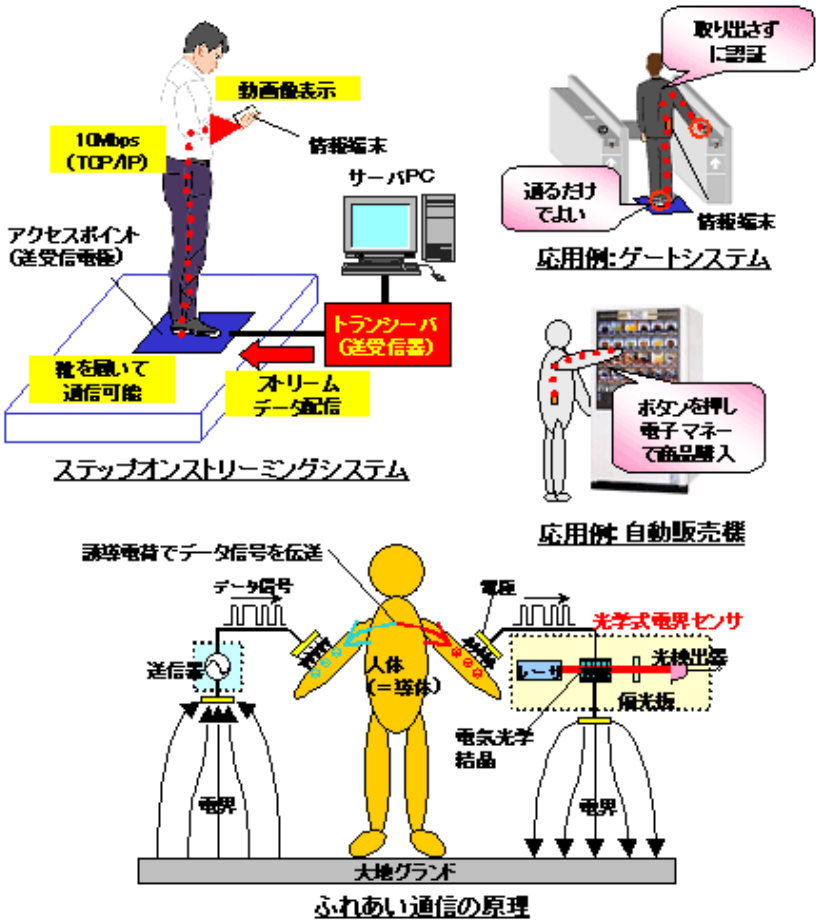


図 3-3　ふれあい通信の原理（ＮＴＴマイクロシステムインテグレーション研究所ホームページ http://www.ntt.co.jp/milab/project/sd_15_1.html より）

4. くらしとネットワーク犯罪

家庭でのインターネット普及率が 95%近くに達し、ブロードバンド契約者も 1,500 万加入を越える現在、普段のくらしの中ではネットワークはもはや切り離せない世界になりつつある。今後のユビキタス社会の到来と共に無意識なネットワーク接続が主流になるであろう。

しかしながら、ネットワーク環境とネットワークに接続されるＰＣや携帯電話の機器の普及と共に、それらを狙ったウイルスによる被害や不正アクセスなどの犯罪も増加する一方であり、また、その手口も益々巧妙化しつつある。

本章では、普段のくらしをとりまく環境で、どのような被害や犯罪が問題になっているか、実例を挙げて説明し、さらにくらしのなかにおけるコンピュータ犯罪を解説する。また、コンピュータウイルスによる被害や不正アクセスの状況を解説し、情報セキュリティの最新事情を述べる。

4.1 ハイテク犯罪の三大類型

ハイテク犯罪の主な特徴として、匿名性が高いこと、痕跡が残りにくいこと、不特定多数の人に被害が及ぶこと、国境を越えることが容易であることなどが挙げられる。

警察庁の公表によると、2003 年中の全国におけるハイテク犯罪の検挙数は約 15%、ハイテク犯罪などに関する相談受理件数は約 2.2 倍の増加となった（図 4-1 と図 4-2 参照）。特に、身に覚えのない有料サイトの利用料金を請求する「架空請求メール」の相談が約 18,000 件になるなど、詐欺・悪質商法に関する相談が昨年（2003 年）の約 6.5 倍にも増加していた。

ハイテク犯罪検挙件数は 1,849 件で、前年比 243 件（約 15%）の増加だった。このうちネットワーク利用犯罪は 1,649 件となり、全体の約 89%を占めた。犯罪の内訳は、出会い系サイトを利用した児童売春（269 件）・青少年保護育成条例違反（120 件）や、インターネットオークションなどを利用した詐欺（521 件）・著作権法違反（87 件）、掲示板を利用した名誉毀損（46 件）・脅迫（38 件）などだった。また不正アクセス禁止法違反（145 件）も、2000 年の法律施行以降、増加を続けている。

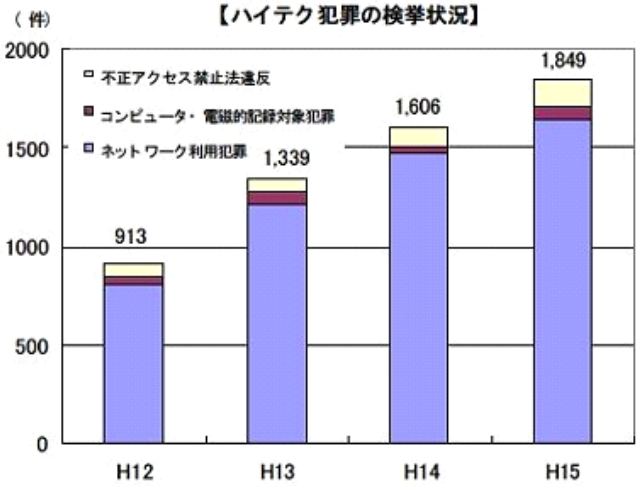


図 4-1　ハイテク犯罪の検挙状況（PCWEB のホームページ http://pcweb.mycom.co.jp/news/2004/02/23/005.html より）

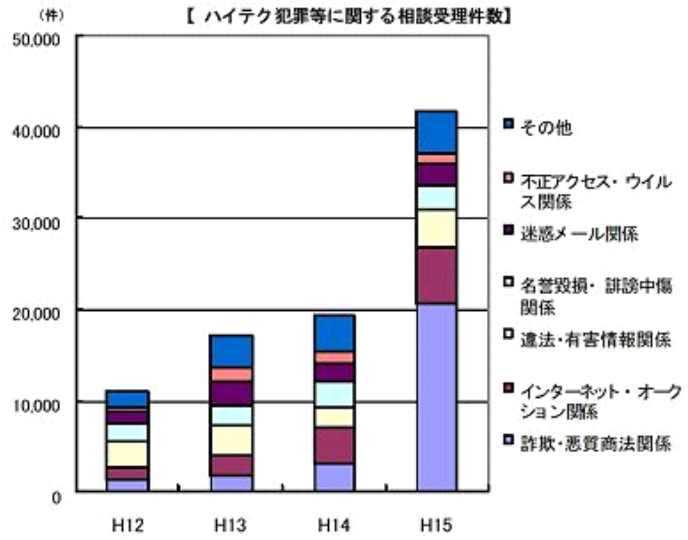


図 4-2　ハイテク犯罪の相談受理件数（PCWEB のホームページ
http://pcweb.mycom.co.jp/news/2004/02/23/005.html より）

警視庁のホームページによると、ハイテク犯罪とは「コンピュータ技術及び電気通信技術を悪用した犯罪」を指し、大きく分けて 3 つの犯罪類型に大別される。

4.1.1　「ネットワーク利用犯罪」

- インターネット等を利用したわいせつ画像、児童ポルノの販売、頒布
- インターネット等を利用した覚せい剤等の薬物、けん銃、偽ブランド品及び海賊版等の違法な物品の販売
- 電子メールや電子掲示板を利用した脅迫、名誉毀損等の行為
- インターネット等を利用したねずみ講、賭博、富くじ等の勧誘

等があげられる。

4.1.2　「コンピュータ、電磁記録を対象とした犯罪」

- コンピュータシステムの機能を阻害する犯罪
- コンピュータシステムを不正に使用する犯罪

4.1.3　「不正アクセス禁止法違反」

平成 12 年、「不正アクセス行為の禁止等に関する法律（不正アクセス禁止法）」が施行となり、ネットワークを通じてのコンピュータへの不正アクセス行為が禁止されるようになった。

具体的には、「ＩＤ・パスワードの不正な使用」や「そのほかの攻撃手法」によってアクセス権限のないコンピュータ資源へのアクセスを行うことを犯罪として定義するものである。

・ 他人のプロバイダ接続用ＩＤ・パスワードを勝手に使用して電話回線を通じて認証サーバにアクセスする行為
・ セキュリティホールをついて、アクセス制御されている Web サーバ等に不正にアクセスする行為
・ 他人のＩＤ・パスワードを電子掲示板等で公開する行為

等がある。

4.2 ハイテク犯罪検挙具体事例

つづいて実際に発生した事例を参考に見ていく。

4.2.1 不正アクセス禁止法違反及び詐欺事件

インターネットカフェに設置されたパソコンを利用して他人のＩＤ及びパスワードを無断で使用し、インターネットオークションの認証サーバに不正アクセスし、同オークションに「ＤＶＤソフト出品、傷はありません。」等と同会員になりすまして虚偽の情報を掲示し、落札者に対して代金の振込方法をメールで指示して他人名義の銀行口座に代金を振り込ませ、44 人から総額約 240 万円をだまし取った。（平成 14 年 1 月検挙。茨城・栃木）

4.2.2 電子計算機使用詐欺事件

知人のクレジットカード番号情報等を無断で使って、オンラインショッピングで電子マネーを不正に購入し、インターネット通販サイトから米をだまし取った。（平成 14 年 5 月検挙。警視庁）

4.2.3 名誉毀損事件

インターネットを利用して男性会員勧誘のための架空の会員制クラブを設け、被害女性のホームページから無断で入手した顔写真、架空の氏名、年齢や「5,000 円で同女の電話番号等を提供する。」等の文書を掲載した同クラブの勧誘広告を、不特定多数の者に電子メールで送信し、被害者の名誉を毀損した。

また、クラブの会員登録料名目に現金をだまし取り、詐欺罪でも検挙。（平成 14 年 6 月検挙。埼玉）

4.2.4 業務妨害・脅迫事件

従業員が社内ネットワークのサーバに保存されていた業務データを削除した上、自宅のパソコンから会社社長や同僚に「今後もデータを消す。」などとメールを送信し脅迫した。（平成 14 年 11 月検挙。宮崎）

4.3 くらしとセキュリティの現状

4.3.1 セキュリティ対策の必要性

いわゆるコンピュータウイルスによる被害は、ＩＰＡ（情報処理推進機構）からの月次レポー

ト「ウイルス・不正アクセスの届出状況」を見ても分かるように、2004 年度後半の数ヶ月は、毎月 5,000 件近い、もしくはそれ以上の届出件数が報告されており、企業の情報セキュリティ課題であると同時に「くらし」現場における脅威となっている（図 4-3、図 4-4、表 4-1 参照)。特にインターネットの普及と常時接続化の進展により、家庭内のコンピュータがネットワークに常に繋がれていることが常態化し、ウイルスへの感染機会は、メール利用に関連してのものを中心に、以前と比べ、格段に増加しているのが現状である。

また、これは家庭内に限ったことではないが、ウイルスの被害だけでなく、ネットワークの利用では、外部からの不正侵入による情報の漏えいや改ざん、といった被害もふえてきている。

前述の「ウイルス・不正アクセスの届出状況」によると、月々に 30 件から 50 件近い届出があり、実際に不正侵入やメールアドレスの詐称、ホームページの改竄などの被害が報告されている。

さらに、踏み台として、知らないうちに他人のコンピュータを攻撃するための道具に自分のパソコンが利用されるケースもあり、自分が直接被害に遭わないまでも、ハッカーに利用されて他人に迷惑を掛ける事例も少なくない。

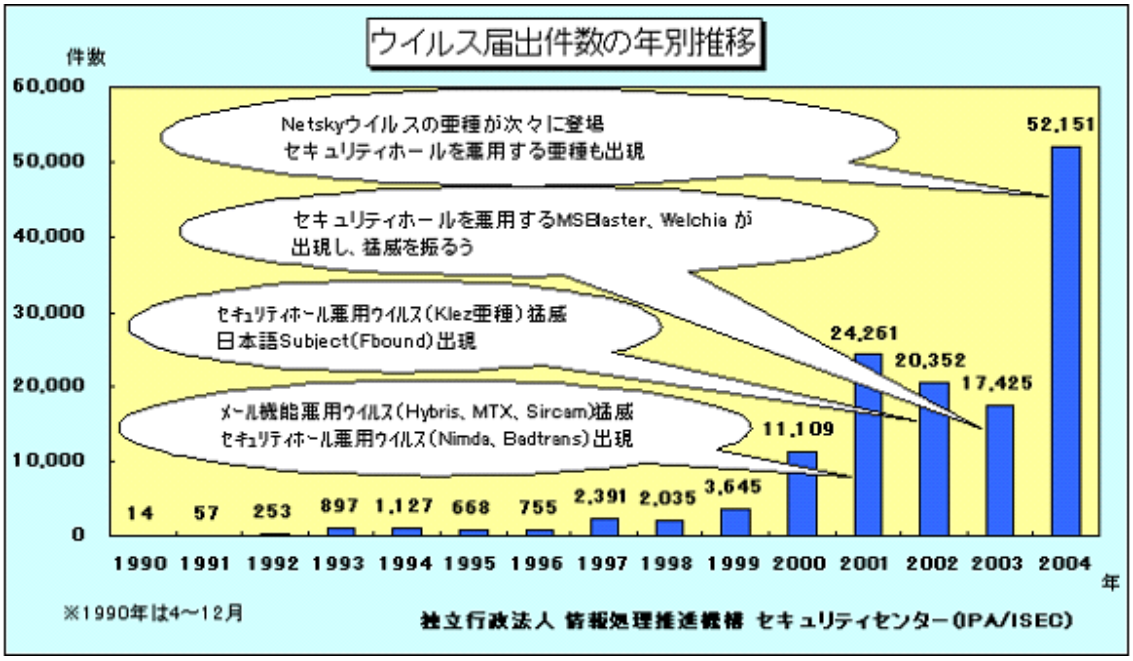


図 4-3　ウイルス届出件数の年別推移（ＩＰＡのホームページ
http://www.ipa.go.jp/security/txt/2005/01outline.html より）

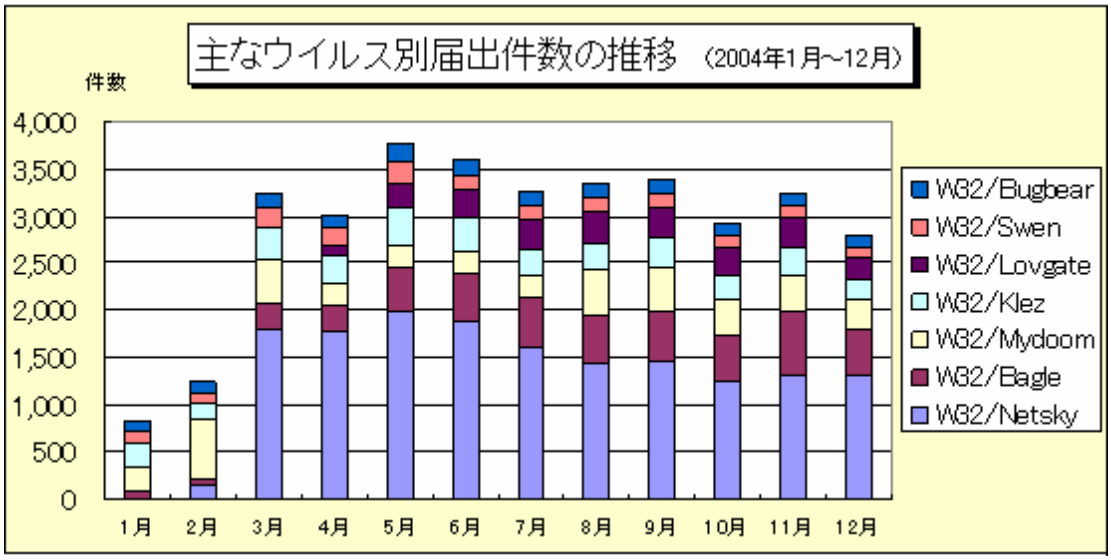


図 4-4　主なウイルス別届出件数の推移（ＩＰＡのホームページ http://www.ipa.go.jp/security/txt/2005/01outline.html より）

表 4-1　届出ウイルスワースト 10（ＩＰＡのホームページ http://www.ipa.go.jp/security/txt/2005/01outline.html より）

ウイルス名称	2004 年	2003 年	メール機能悪用	セキュリティホール悪用
W32/Netsky	15,895	−	•	•
W32/Bagle	4,838	−	•	•
W32/Mydoom	4,388	−	•	•
W32/Klez	3,498	4,538	•	•
W32/Lovgate	2,569	165	•	•
W32/Swen	1,776	1,673	•	•
W32/Bugbear	1,727	1,602	•	•
W32/Mimail	1,629	883	•	•
W32/Zafi	1,557	−	•	•
VBS/Redlof	1,162	803	•	•
その他のウイルス	13,112	7,761		
合　計	52,151	17,425		

備考：件数には亜種の届出を含む

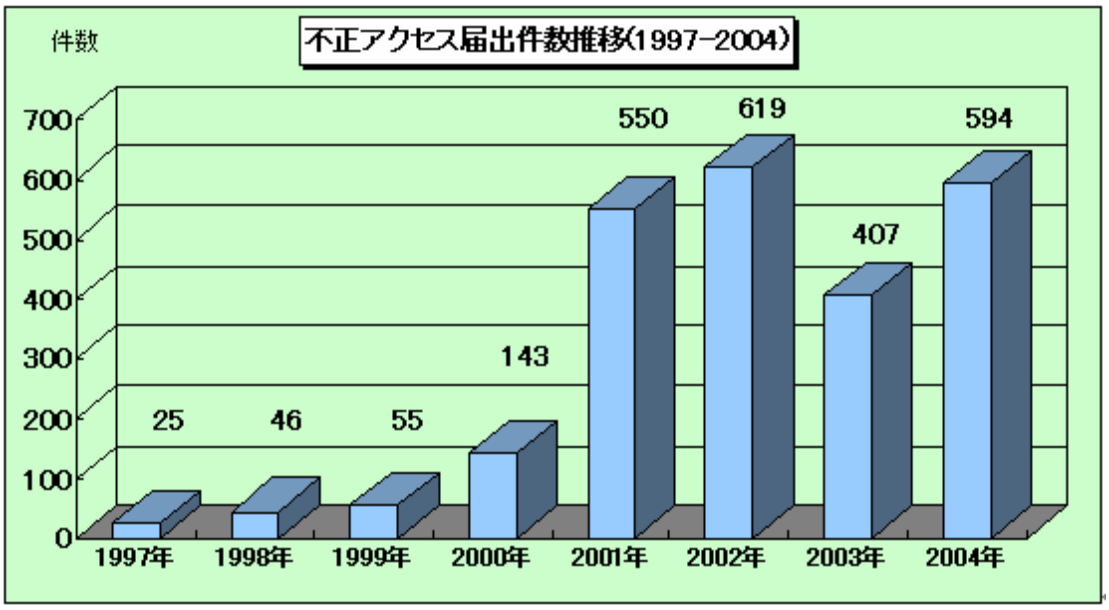


図 4-5　不正アクセス届出件数の推移（ＩＰＡのホームページ http://www.ipa.go.jp/security/txt/2005/01outline.html より）

表 4-2　不正アクセスの内訳（2003-2004 年）（ＩＰＡのホームページ http://www.ipa.go.jp/security/txt/2005/01outline.html より）

届出種別	2004 年	2003 年
侵入	43(43)	64(64)
アクセス形跡（未遂）	515	239
ワーム感染	0	5(5)
ワーム形跡	7	39
メール不正中継	3(3)	9(9)
アドレス詐称	11(11)	18(18)
DoS（サービス妨害）	4(4)	8(8)
その他	11(11)	25(22)
合計	**594(72)**	407(126)

*括弧内は実被害件数

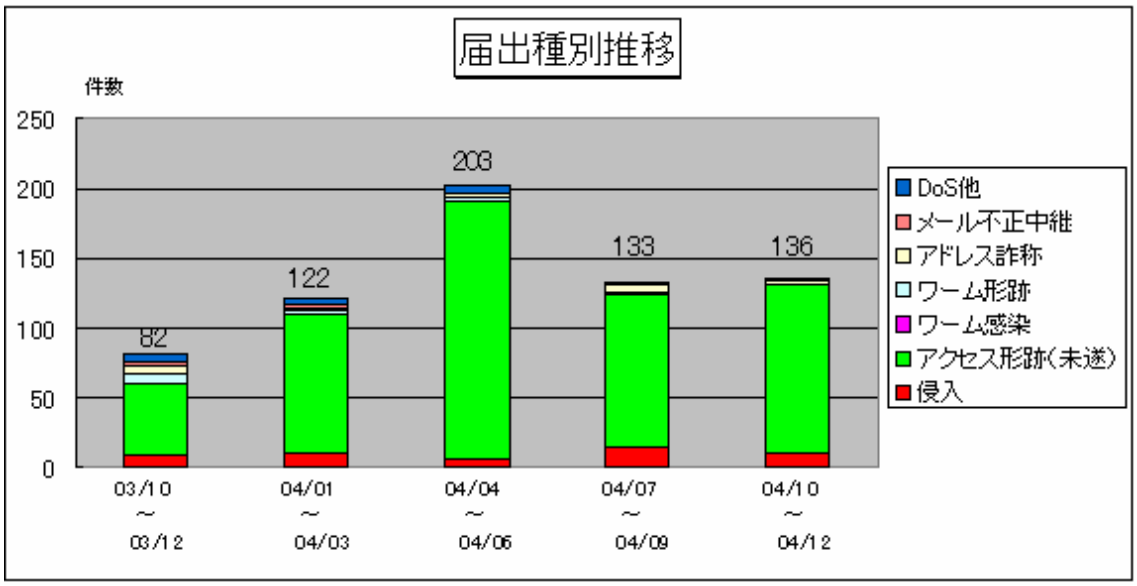


図 4-6　不正アクセスの届出種別推移（ＩＰＡのホームページ
http://www.ipa.go.jp/security/txt/2005/01outline.html より）

4.4　くらしのなかにおけるコンピュータ犯罪

コンピュータ犯罪は、インターネットの普及に伴って増加傾向にある。今後、さらに電子政府も開始される予定であり、ますます実社会に近くなっていく傾向にある。そうした部分において、犯罪もインターネット上に持ち込まれている。

このような状況における利用者側の意識としては、インターネット利用を脅かす「犯罪者の手口」を把握することが、コンピュータ犯罪の被害を最小限に防ぐ効果へとつながる。

まず、犯罪者の手口を把握するには、以下の点について整理が必要である。

（1）コンピュータ犯罪者の種類
（2）コンピュータ犯罪者の動機
（3）コンピュータ犯罪の分類

（1）コンピュータ犯罪者の種類

①ハッカー、クラッカー

コンピュータ技術に精通した人。転じて、コンピュータ技術を悪用して他人のコンピュータに侵入・破壊を行う者を指すことが多いが、この用法は誤用が定着したものなので使用すべきでないとする人も多い。本来、「ハッカー」という用語には悪い意味はなく、むしろ高い技術を持った人々に対する尊称として使用されていたことから、古参の技術者などの間には、技術を悪用する人々は「クラッカー」（破壊者）と呼んで「ハッカー」とは区別すべきであるとする主張も根強くある。

②初心者（Script Kiddy）

インターネット上で公開されている操作が簡単な「クラックツール」を利用して、興味本位の不正アクセスを試みる「幼稚な」クラッカーである。「クラックツール」は、他人のコンピュータのデータやプログラムを盗み見たり、改ざんや破壊などを行ったりする「クラッキング」行為をするためのプログラムである。クラックツールは既に広く知られているセキュリティホール[33]を悪用するように作成されているため、セキュリティパッチ[34]を確実に適用することで、ほとんどの初心者による攻撃は防止できる。クラックツールを使えば深い知識や高度な技術がなくても簡単に攻撃を行うことができるため、数の上ではクラッカーのほとんどは初心者であると言われる。

③サイバーテロリスト

インターネットなどのコンピュータネットワーク上で行われる大規模な破壊活動。人に危害を加たり、社会機能に打撃を与えるような、深刻かつ悪質なものをこのように呼ぶ。

社会的なインフラとしてのインターネットやコンピュータの重要度が高まるに連れ、サイバーテロの脅威も日増しに増大している。コンピュータウイルスの配布やデータの書き換えや破壊、サーバや通信回線をパンクさせて停止に追い込むなど、様々な手口がある。

直接的な物理的破壊活動は伴わず、情報の破壊や改竄、漏洩、機器や回線の停止などによって被害をもたらす行為を指す。

（2）コンピュータ犯罪者の動機

過失

過失はいくつかの具体例がある。

例えば、自分のサイトがホームページの自動巡回ツールをどこかのサイトに設定しておくような場合は、巡回先の構成や設定している頻度、リンクの深さなど注意しなければならない。サーバを占有し、一時的に高負荷をかけることが、「攻撃」となる可能性がある。特に、「踏み台」にされるケースが発生している。

「踏み台」とは、セキュリティの甘いインターネット上のサーバにアクセスし、そのサーバを経由して、別サーバにアクセスすることを指す。このようなことによって、アクセス元（どこからアクセスしてきているのか）を隠すことができる。

いたずら

覚えたての手法やツールを試したい、という衝動に駆られて行ってしまうのがこのパターンであり、初心者の手口である。

知的好奇心、自己顕示

ハッカーという人種は、知的好奇心が旺盛である場合が多く、そのための技術を追求することをいとわない。初心者と異なるのは、ハッキング行為の動機である。知的好奇心を追求するために、より難しいサイト、ガードの固い企業を攻撃対象にする。

---

[33] ソフトウェアの設計ミスなどによって生じた、システムのセキュリティ上の弱点。

[34] ソフトウェアに保安上の弱点（セキュリティホール）が発覚した時に配布される修正プログラム。

また、自己顕示欲も強い。ホームページを改ざんした後、すりかえたページにグループ名や犯行声明、特徴のあるコンテンツを残すのも、一つのアピールである。

金銭

ハッカーのなかにもプロフェッショナルになると、金銭的理由でハッキングを行う。また、クレジットカードの暗証番号などを盗むなど金銭目的の犯罪も増えている。

復讐

クラッカーなどによる掲示板を荒らすような行儀の悪い行為に対して、ハッカーは非常に嫌う傾向がある。そうした場合、あまりにも目に付いたり、直接的に被害を被ったりした場合、クラッカーを攻撃したりする行為である。

サイバーテロ

サイバーテロは人命を奪うテロ同様、政治に対する不満や国家間の問題が引き金となる場合に、相手国などに対して攻撃する行為である。

（3）コンピュータ犯罪の分類

不正アクセス

A.不正アクセスの種類

不正アクセスは、既知のセキュリティホールを突く攻撃とパスワードクラッキング[35]に大別される。また、ＤｏＳ攻撃（サービス不能攻撃）[36]という不正アクセスではないが、サーバを停止させる業務妨害攻撃も含むと、大きく三つに分かれる。

B.不正アクセスの一般的な手順

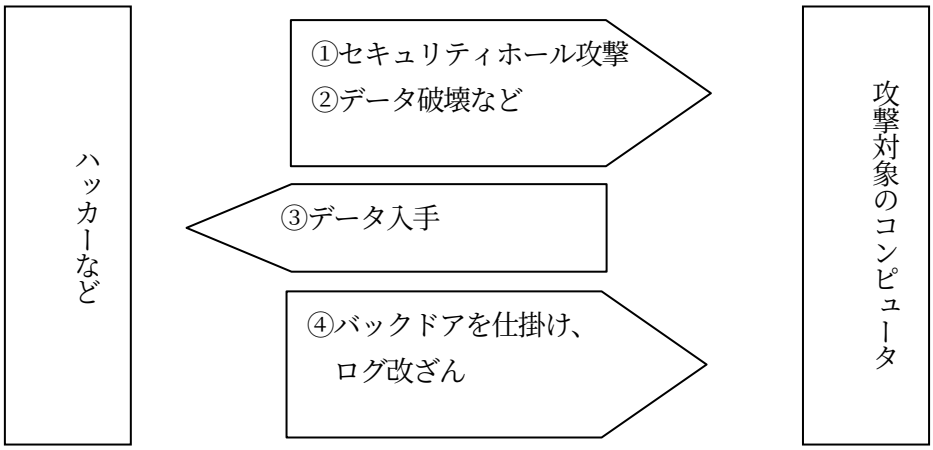


図 4-7　不正アクセス

[35] 人のパスワードを解析し、探り当てること。

[36] 相手のコンピュータやルータなどに不正なデータを送信して使用不能に陥たり、トラフィックを増大させて相手のネットワークを麻痺させる攻撃。

C.不正アクセス禁止法

2002 年 2 月より不正アクセス禁止法が施行された。

・ 不正アクセス行為の禁止、“ 不正アクセスを助長する行為の禁止

・ 不正アクセスを受けた管理者への援助措置

それまでは、不正アクセス後に行われるサーバの破壊活動やデータの搾取に関しては、刑法によって裁かれていたが、その前段階である「不正アクセス」自体を取り締まることは出来なかった。しかし、不正アクセス禁止法によって「不正アクセス」自体も処罰の対象にすることになった。

盗聴

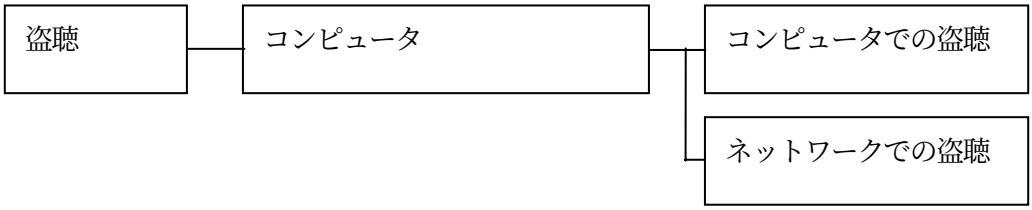


図 4-8　盗聴

コンピュータとネットワーク（特にインターネット）の持つ脆弱性を突くことによる盗聴がある。現在ではこれが、一般に言われる盗聴行為であろう。後者は、さらにネットワークを通じた盗聴と、コンピュータに仕掛ける盗聴に分けられる。

以下に具体的な行為を示す。

A.コンピュータでの盗聴

「ロギング」と言われる行為がある。これは、本人が知らぬまにキーボード入力した内容をそのままハードディスクなどに記録することで、このようなソフトはロギングツールと呼ばれている。キーボードでタイプした内容をそのまま記録していくので、これをたどっていけば、キーボードから入力したメールの文章やＩＤ、パスワード、果てはクレジットカード番号さえも入手できる。

B.ネットワークでの盗聴

ネットワーク上に流れる特定のパケットをキャッチする行為をパケットスニファリングという。これは、もともと通信トラブルを解消するために、ネットワーク上に流れる電気信号をそのまま捉えて、解析するためのものである。これを悪用するのが盗聴ということになる。また、無線ＬＡＮもその対象である。

なりすまし

身元が判明しないように、他人になりすまし、悪意ある行為をすることである。

なりすましとしての目的は、以下のようなケースがある。

A.不正アクセスの身元隠し

通常、対象となるコンピュータ等にアクセスを行うと、アクセスログが残る。そのアク

セスログをもとにプロバイダや企業に確認すると、送信元ＩＤアドレスから身元が判明する。そのため、身元が判明しないように、他人になりすますのである。

B.ネット詐欺

他人のカードやカード番号を使って買い物をしたり、有名企業になりすまして注文を受け付け、お金を指定口座に入金させたりするのが詐欺の目的である。

C.情報収集

ログインシュミレータのように、ＩＤやパスワードなどの情報収集目的で、安全であると思われている他社になりすまし、情報を収集する。

コンピュータウイルス

経済産業省が策定した「コンピュータウイルス対策基準」によると、以下の通り、コンピュータウイルスについて定義されている。

A.コンピュータウイルスの定義

「第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、次の機能を一つ以上有するもの。」

・自己伝染機能

自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能

・潜伏機能

発病するための特定時刻、一定時間、処理回数等に条件を記憶されて、発病するまで病状を出させない機能

・発病機能

プログラム、データ等のファイルの破壊を行たり、設計者の意図しない動作をする等の機能

B.コンピュータウイルスの種類（トレンドマイクロ株式会社のＨＰより引用）

a.感染する場所による分類

b.ウイルスの活動による分類

c.ウイルスが利用する技術による分類

d.メモリに常駐するかどうかによる分類

e.その他

・差出人をいつわるウイルス

・ネットワークウイルス

・ウイルスデマ情報

・スパイウェア

C.コンピュータウイルスの作成、配布に関する罰則規定

コンピュータウイルスの作成、配布は「電子計算機損壊等業務妨害罪」、「偽計業務妨害罪」、「器物損壊罪」、「電磁的記録毀棄罪」、「信用毀損業務妨害」等に該当する犯罪行為である。日本の法律における「電子計算機損壊等業務妨害罪」が適用された場合、“五年以下の懲役又は百万円以下の罰金”に処せられる。ウイルスの被害者から損害賠償を請求された場合は、作成者はさらに多額の賠償をしなければならなくなる。自分のコンピュータがウイルスに感染したが対策をとらず、他のコンピュータに感染を広げてしまった場合などは被害者であるはずの立場が一転して加害者となり損害賠償の責任を負う可能性がある。

4.5 情報セキュリティの最新事情

次に情報セキュリティの最新事情について見ていくものとする。

4.5.1 ＩＴ利用環境の多様化とブロードバンド環境の衝撃

インターネットの利用者数は年々増加し続けている。とくにブロードバンドの普及は日本では顕著で、ＣＡＴＶ、ＡＤＳＬ、ＦＴＴＨなどに加え、ユビキタスインターネットを実現させる無線ＬＡＮなど、インターネット接続環境の多様化を無視することは出来ない。

2004 年 2 月に発行されたインターネット白書によれば、日本のインターネットユーザーの48.14%がブロードバンドでインターネットに接続していることがわかった。その内訳は、ＣＡＴＶ、ＦＴＴＨ、ＡＤＳＬによる接続が全体の 92%を占め、多くのユーザーが、常時接続環境のインターネットで情報を交換していると理解できる（図 4-9 と図 4-10 参照）。

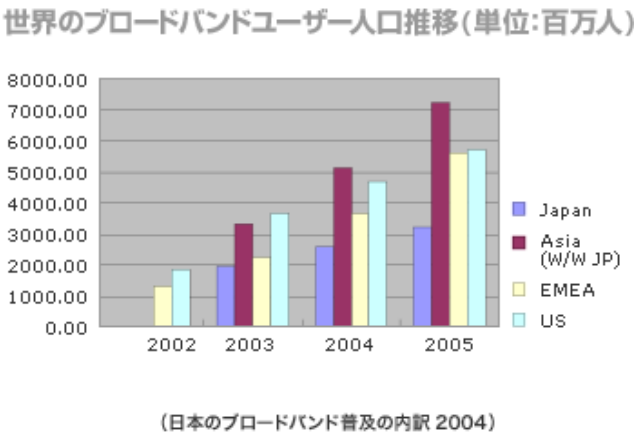


図 4-9 世界のブロードバンドユーザー人口の推移（トレンディセキュリティボックスのホームページ http://www.t-secubox.jp/knowledge/030/index.shtml より）

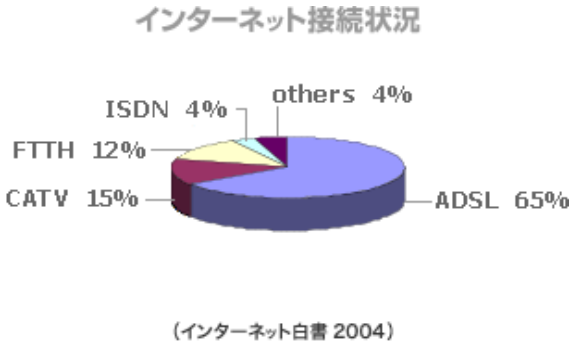


図 4-10　インターネット接続状況（トレンディセキュリティボックスのホームページ http://www.t-secubox.jp/knowledge/030/index.shtml より）

ブロードバンドの普及を突いた問題点も見つかった。新しいタイプのウイルスの出現、ウイルス被害、不正アクセス、ネット詐欺、インターネット犯罪など、サイバー犯罪の出現がそれらである。警察庁のサイトから各メディアまで、毎日のように報道される時代となってきた。

4.5.2　セキュリティホールを狙ったネットワークウイルスの脅威

2003 年に大流行したウイルス「ＭＳブラスト」は、世界中で 1,500 万台ものコンピュータに感染したそうである。それに続く「Sasser」（サッサー）でも、同数のコンピュータに感染したとされている。無防備なコンピュータをインターネットに接続して約 20 分間放置しただけで、これらの強力なネットワークウイルスに感染したという調査報告もある（Internet Storm Center 調べ）。

ネットワークウイルスは、メール添付で拡大するファイルベースのウイルスという既存のウイルスに対する認識を変えた。セキュリティホールを渉猟し、そのコンピュータに不正パケットを送信して制御を奪い、バックドアを仕掛けるのである。バックドアが仕掛けられたコンピュータは、特殊なファイルをダウンロードさせられ、特定の Web サイトを一斉攻撃する設定をされてしまうのである。セキュリティホールを悪用するネットワークウイルスは、今後も進化することは間違いない。

4.5.3　ソーシャルエンジニアリング技術との組み合わせ

2004 年 1 月に発生した「Netsky」（ネットスカイ）に代表される、ソーシャルエンジニアリング[37]技術を巧みに利用した古典的なメール拡散型のウイルスの被害は、相変わらず猛威を振るっている。「Netsky」が添付されたメールは、メールサーバからのエラーメッセージを装っている。一見、システムから送付されたと思われるような件名のメールと添付ファイルをユーザーに送り付け、慎重なユーザーにもファイルを開かせてしまうという手段が非常に巧妙で、悪意あるハッカーは、この方法を利用するばかりでなく、20 種以上の亜種まで登場させた。

[37] ネットワークの管理者や利用者などから、話術や盗み聞き、盗み見などの「社会的」な手段によって、パスワードなどのセキュリティ上重要な情報を入手すること。

図 4-11　「Netsky」添付メール例（トレンディセキュリティボックスのホームページ http://www.t-secubox.jp/knowledge/030/index.shtml より）

4.5.4　多種の脅威に対応する情報セキュリティ対策が求められる時代

具体的には「ＭＳブラスト」のようなウイルスでは、ゲートウェイ（ルータ[38]など）でセキュリティを固めても、１台のウイルスに感染したコンピュータが内部ネットワークに接続されただけで、大規模な感染という事態になる。

セキュリティソフトをインストールしていた場合、アクセスポイントが正しく設定されていなければ、無線ＬＡＮを不正使用されてしまう恐れがある。さらに、ＵＲＬフィルタを設定していても、コンピュータに詳しい人ならば、設定を変更し有害サイトにアクセスできるようにするであろう。「セキュリティソフトを各コンピュータにインストールしていればセキュリティが確保できる」時代は、現実的な対応では不足しているのである。つまり、セキュリティソフトでルータ以下のネットワークまで防御できる機能が備わっていなければ、個々のコンピュータのセキュリティを確保出来ないと言い換えられる。

[38] ネットワーク上を流れるデータを他のネットワークに中継する機器。

5. くらしにおける犯罪・被害動向

多くの家庭でインターネット接続可能な環境が整備されている今日では、個人やそのネットワーク環境を対象とした、様々な犯罪や被害が顕著化し大きな社会問題になっている。

個人を対象とした被害では、迷惑メールなどの軽微なものから、個人情報漏洩などの重大なもの、架空請求やフィッシング詐欺などの金銭を目的としたものまで広範囲にわたる。ネットワーク環境を対象とした被害では、不正アクセスによるなりすましやウイルス、ワームによる環境の破壊などが代表例である。

5.1 ユーザーが何もしなくても被害に遭うケース

ユーザーが特に何らかの操作を行わなくても被害に遭う可能性がある。むしろ正しい環境の設定や対策を取らなかったことに起因する被害が多数を占める。下記に代表的なものを挙げる。

5.1.1 盗聴

特に無線ＬＡＮなどの電波を用いるネットワークが盗聴の対象になりうる。家庭での無線ＬＡＮではセキュリティに関する様々な設定があり、それらを正しく設定することで盗聴を防ぐことは可能である。通常の認証、暗号化を行うことで盗聴は著しく困難になるため、実運用上は安全であると言える。一方、公衆無線ＬＡＮなどでは無線ＬＡＮアクセスポイントまでは誰でもアクセスできるが、その先のインターネットへのアクセスでアクセス制御や課金を行うため、無線ＬＡＮアクセスポイントのセキュリティ設定がなされていないのが一般的である。よって、公衆無線ＬＡＮではＳＳＬやＶＰＮで暗号化されていない通信で重要なデータのやり取りを行うことは避けたい。

ＡＤＳＬや光ファイバ、ＣＡＴＶ、定額ＰＨＳを介したインターネット通信では通常基地局やアクセスポイントまで１対１の通信となるため、盗聴は不可能ではないが、一般ユーザーレベルでの盗聴は著しく困難である。

盗聴されるとＰＣからネットワークに流れるデータ全てを解読することができるため、メールなどの重要な情報や個人情報が漏洩する。また、ＳＳＬなどの暗号化通信を用いていないメールサーバや他のサービスへのＩＤ、パスワードが漏洩すると不正利用に流用される可能性が高い。

これらの盗聴ツールはインターネット上から無料で入手できることから、十分な注意が必要である。また、無線ＬＡＮ等でも一定の期間で認証・暗号化用の鍵を変更することが望ましい。

5.1.2 不正利用・踏み台

盗聴によりユーザーＩＤ、パスワードが流出したり、ワームやウイルスにより不正なソフトを送り込まれたりすると、悪意のある他人が本人になりすましてインターネットサービスやＰＣ自体を不正利用することが可能となる。

インターネットサービスの場合は、ユーザーＩＤ、パスワードを不正に入手された結果、ネット販売やオークション、有料ゲームなどをなりすまして利用されたりするケースが報告されている。また、ＰＣ自体を不正利用される場合は、ＰＣに保存されている様々な個人データを盗み出

されることや､別のサーバへの攻撃の踏み台にされることもある｡踏み台とはＰＣを乗っ取られ、あたかも自分のＰＣが他人のサーバに攻撃を仕掛けることを言い、サービス拒否攻撃（ＤｏＳ攻撃）などが一般的である。攻撃されている側から訴えられることもあるので注意したい。

5.1.3　迷惑メール・ＳＭＳメール

・ＰＣにおける迷惑メール

一般的に「迷惑メール」と呼ばれるものには、一方的に送られてくる商用やその他広告、またチェーンメールなどが該当する。そのうち広告に関しては、「特定商取引に関する法律」と「特定電子メールの送信の適正化等に関する法律」によって、件名に『未承諾広告※』と付し、本文冒頭には事業者や送信者の氏名、名称や所在地、連絡先、またオプトアウトに対する受信拒否の方法等を表示しなければならない。

しかし件名に『未承諾広告※』と付すと、メールソフトやプロバイダ、携帯電話会社のシステムにより受信拒否されてしまうことが多く、残念ながらこの件名表示をきちんと行って送信しているものはごくわずかである。

以前は『未承諾広告※』の※を＊に替える、前後に“ ”といった記号を入れるなどで、そのフィルタリングをくぐり抜けていたが、最近の迷惑メールは、あたかも知人やメーリングリスト等からのメールと偽って自分のサイトに誘導するようなケースが増えてきている。

特にいわゆるアダルトサイト等に見られる手口ではあるが、予め迷惑メールを送信するメールアドレスを BASE64 等を用いてエンコードし、それを含ませたＵＲＬ（例として：http://wwww.adult123456.com/ABC/%1%8%3%6.....&g%5/の ABC/%1%8%3%6.....&g%5 が被害者のメールアドレスを不正に送信する為のプログラムに相当する部分）を迷惑メールに貼り付けておくことにより、そうとは知らないユーザーがメールに貼り付けてあるそのＵＲＬをクリックすると、そのサイトではアクセス元のメールアドレスが分かる仕組みにしていることが多い。なぜそういったことをするかというと、このような迷惑メールを送付してくるサイトは、利用料金や利用期間の明記を一切せずにワンクリックで勝手に自動登録させ、料金支払いを強引な文章により不当に請求するといったケースが多く､そのときに一方的に請求メールを自動送付したり、メールアドレスを表示させることによって支払いを強要する、一種の脅しとして利用するからである。

もちろんこういった登録に対しての支払い義務は一切無いが、契約が成立したと勘違いして代金を振り込む被害が増加している。

・ＳＭＳメールにおける迷惑メール

携帯電話の場合はメールにも２種類あり、携帯電話のメールアドレスに迷惑メールが送られてくるケースと、携帯電話の電話番号にメールを送付することが可能なＳＭＳ（ショートメッセージサービス）メールがある。

ＳＭＳメールで送られてくる広告メールにも、前に述べたように、その送信先の携帯電話番号をエンコードしておき、アクセス元の携帯電話番号が分かるシステムをとっていることが多い。この場合携帯電話番号がサイト側にわかってしまうために、自動登録後一定期間支払いに応じず

にいると、ＳＭＳメールでの請求のほか、その番号に直接請求の電話がかかってくることがある。メールと異なり無視一辺倒の対応が困難なため、根負けして支払いに応じるケースが後を立たないので注意が必要である。

最近ではこういった社会現象を鑑み、各携帯電話会社がＳＭＳメールについて次々対応を検討している。

5.1.4 ＩＰ・携帯個体番号取得

・ＩＰアドレス

自動登録を行って不当請求をするサイトにアクセスしたケースでは、自動登録時の画面に、料金支払請求と共に、ＩＰアドレス、プロバイダ、リモートホストといった情報が表示されることが多い。その画面には、支払いが滞った場合は、これらの情報より個人情報を調べ、高額な手数料と延滞金と共に自宅や会社に請求をかける、と言った脅し文句が書かれていることがほとんどである。これらの情報はウェブサーバにアクセスすれば、どこのサーバでも取得可能な情報であるが、あえて表示することにより不安に陥らせて支払いをするよう差し向けるために行うのである。

個人のＰＣよりアクセスした場合、表示されるのは利用しているプロバイダのドメイン名と、そのプロバイダが付しているＩＰアドレス程度であり、それ以上の情報は分からない。またプロバイダはサイト側からの料金未納に対しての開示請求には一切応じないと明言している。

会社及び学校等団体のネットワーク環境下のＰＣからアクセスした場合、表示されるのはその団体の取得しているドメイン名やＩＰアドレスである。この場合は団体名やネットワーク情報がそのまま画面に表示されるので心配することが多いが、あくまでサイト側は脅しのために自動的にそういった情報を表示させているだけなので、それらの情報から、その団体に対して直接請求を行うことはまず考えられない。

しかし、個人ならともかく会社組織には迷惑をかけたくない、またアクセスしたサイトがアダルトサイトの場合、所属する団体に知られたくない、後ろめたいといった心情から、支払いに応じてしまう被害が発生する。

ご入会有難うございます。
お客様の会員登録作業が完了致しました。
入会金 60,000 円を＊月＊日までに以下の口座に御振込み下さい。
【銀行口座名】

HOST　**.***.ne.jp
IP　　220.111.***.***
ID　　319713962

2005/＊/＊ 08:18:47
1 回閲覧されています。

重要な注意事項！
※もし万が一、あなたの御支払いが滞ったりいたしますと、ご利用になられたコンテンツ名などを記載した書面にて直接ご請求させていただく場合や、債権回収部から料金を御支払いいただく旨ご自宅および勤務先へお伺いする場合がございます。
また、御支払いいただく為のご連絡等が取れない場合等、悪質な場合は業界流の対応、又は、所轄裁判所より訴状を送付させていただきますので、皆様の利便性の為、何卒ご了承ください。
御支払いに関するお問い合わせはメールにて support@***.com までお問い合わせください。
正当事由が成立される方に関しましては別途、特別措置を設けておりますので、メールにてご連絡いただきご相談ください。
注意 サイトに入会されたにも関わらず、支払期限を過ぎてもご入会金の入金が確認出来ない場合は「お客様情報」を元に
info@ **.**（プロバイダ）に対して 法的な手段を経て、情報開示を求めます。
情報開示情報（以下項目）
・勤務先情報
・勤務先電話番号
・自宅住所
・自宅電話番号
上記ログを元に自宅や勤務先へ直接請求させて頂く可能性がございます。その際に当番組管理部より延滞調査料金 30,000 円、延滞損害金（督促にかかる実費経費）を加算して請求されることがありますのでご入金期日・お振込をお忘れないようにお願い致します。

図 5-1　ＩＰアドレス取得による不当請求例

・携帯個体番号取得

携帯電話より自動登録させて不当請求を行うようなサイトの場合、「個体識別番号」や「機種名」「メールアドレス」を表示して脅しに利用することが多い。個体識別番号とは携帯電話本体に付与されている番号であるが、その番号取得者の個人情報は携帯電話会社でなければ分からず、また携帯電話会社はその情報を一般の問い合わせに対して一切公開しない。

また、一部の機種を除けば、個体識別番号情報を送信する場合には、送信の可否について確認する画面が表示されるので、事前にそういった画面が表示されていなければ、画面上に表示された番号は虚偽である可能性が高い。

機種名については、元々ダウンロードサービスを行うサイトにて、利用できる機種かどうかを確認するために用いられてきたシステムであり、機種名が分かったからといって、もちろんそこから個人情報を取得することは不可能である。

また、勝手にメールアドレスが表示されたとしても、携帯電話本体のメールアドレスを表示させる機能を単に利用しただけであり、サイト側がメールアドレスの情報を取得しているわけではない。

5.1.5 ネットワーク型ワーム

「ワーム（worm）」とは、単独のプログラムとして動作し、ＣＤ-ＲＯＭ、ＦＤ等の媒体やネットワークを介して自分自身を他のＰＣにコピーすることで自己増殖を繰り返し、ＰＣ内のデータを破壊する等の不正を行なうプログラムの総称である。

その内、「ネットワーク型ワーム」とは、次項で取り上げる「電子メール添付のワーム・ウイルス」と異なり、利用者が何もしなくても、インターネットに接続しているだけで感染するワームを指す。

以下に、代表的なネットワーク型ワームの例を挙げる。

（「ＩＴ用語辞典」http://www.e-words.jp より一部抜粋・加筆）

ＭＳブラスト

2003 年 8 月中旬に猛威を振るった、Windows に感染するワーム。
感染するのは Windows2000 と Windows XP であり、ＯＳの脆弱性を突いてＰＣに侵入し、インターネットなどのネットワークを介して他人のＰＣに次々に感染する。また、“ 副作用 ” として、感染したＰＣは短時間のうちに異常終了と再起動を繰り返すなど、動作が不安定となる。

Code-Red

Windows NT／2000 の Web サーバの持つ脆弱性を突き、自己増殖を行なうワーム。感染力が非常に強く、出現から数日の間に世界中のサーバに感染が広がった。本ワームはメモリ上にのみ存在し、ハードディスクにはほとんど痕跡を残さないため、一度侵入されてしまうと発見が非常に難しいが、再起動すると駆除することができる（セキュリティホールを放置すれば再度アタックされたときに再感染する。）また、Code-RedⅡを自称する亜種も出現している。

Sassar

2004 年 5 月に猛威を振るった、Windows に感染するワーム。
Microsoft 社が同年 4 月に発表した Windows の脆弱性のうち、「ＬＳＡＳＳの脆弱性」と呼ばれる弱点を突き、ユーザーが何もしなくてもネットワークに接続しているだけで感染する。
Sassar 発見から 7 日目の 2004 年 5 月 8 日、Sassar 作成の容疑でドイツ北部に住む 18 歳の少年が逮捕された。ウイルス作者が検挙されるのは珍しい事例である。

5.2 ユーザーが何か行ったことによって被害に遭うケース

ユーザーが、悪意のある者から技術的に細工を施されたメールや Web ページを受け取り、クリックやインストールなどの操作を行ったことに起因する被害について説明する。

5.2.1 電子メール添付のワーム・ウイルスとは

一般的に、ウイルスの感染経路が電子メールに添付されているファイルから感染するワームを指します。例えば、電子メールに添付された文書ファイルなどのマクロにウイルスが組み込まれていて、 それを知らずに開くとウイルスに感染してしまう。 中にはメールをプレビューするだけでも、感染してしまうウイルスも存在する。

また、「ワーム」とは、他のファイルに寄生することなく、メール、ホームページ、不正アクセスといったネットワークを使って自分の分身をばら撒いていくもので、ワームの意味は「這い回る虫」と言われている。

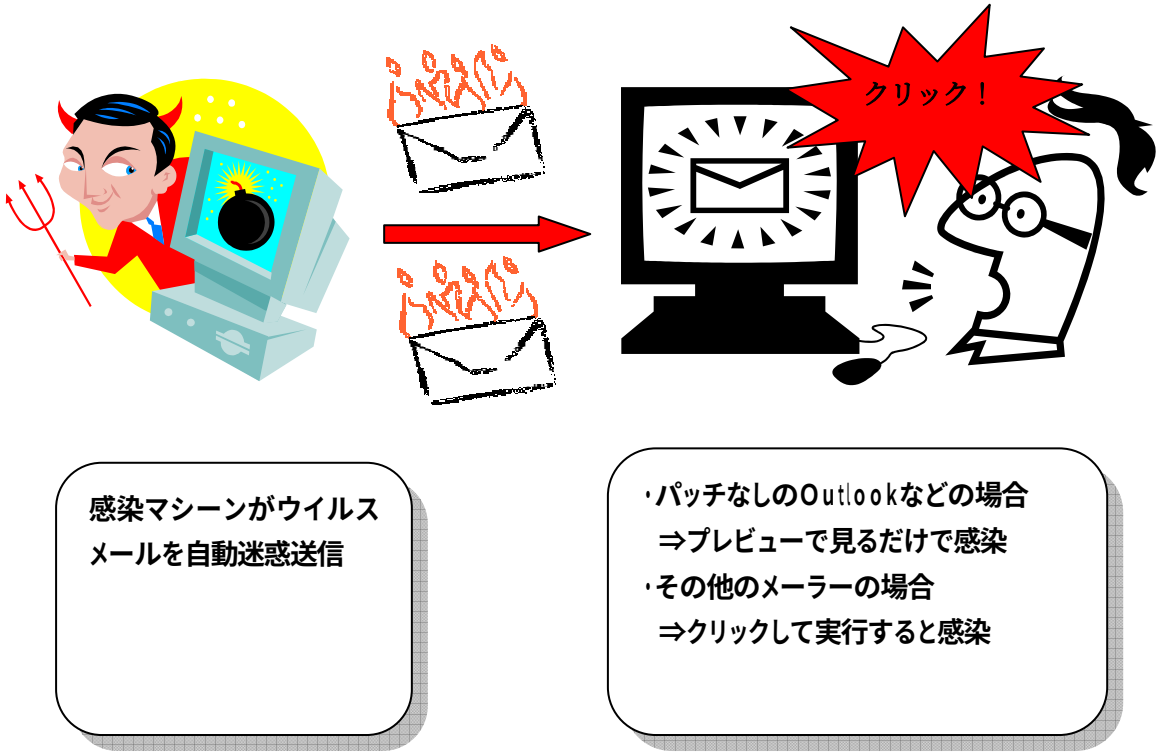


図 5-2　ワーム・ウイルスの感染の仕組み

5.2.2　電子メール添付によるウイルス事例

（1）　Klez　【クレズ】

①　概要　　旧来のウイルスの亜種でありながら、検知が困難である。また、ウイルス対策ソフトの動作を妨害する。コンピュータ内より探し出したメールアドレスすべてに対し、自分自身を添付した電子メールを送りつける。奇数月の 6 日にファイルを消去することもあるので、活動日前後には注意が必要である。また、ＰＣ内の特定拡張子を持つファイルをランダムに選択してウイルスと同時に他人に送る。差出人のアドレスは、感染先コンピュータ上で発見したメールアドレスからランダムに選択されたものが使用されている。

②　感染経路　電子メール（Outlook 系）の添付ファイルを実行。

③　特徴　　英文タイトルのメールが届く。

④　症状　　アドレス帳情報を参照してメールを大量に送信。
ＰＣ内の文書ファイルなどを勝手に添付して送る。

（2） Happy New Year

① 概要　新年の挨拶などの電子メールを装ったウイルスである。
このウイルスは「Happy New Year」というタイトルの電子メールで届き、添付ファイル「christmas.exe」にウイルス Keyluc（Maldal.c／Zacker.c）が含まれている。添付ファイルを開くと感染し Outlook 系のアドレス帳に記載された連絡先に感染メールを送り付ける。また，感染したマシーンの Internet Explorer（ＩＥ）のホームページ設定を変え，悪質な Web ページへと誘導。この Web ページを訪れた際にセキュリティホールを突いて Windows 内のかなりのデータが消去される恐れがある。

② 感染経路　電子メール（Outlook 系）の添付ファイルを実行。

③ 特徴　件名欄は “ Happy New Year”と記されている。
添付ファイル名は「christmas.exe」。

④ 症状　アドレス帳情報を参照してメールを大量に送信。
ＰＣ内の文書ファイルなどを勝手に添付して送る。
ＩＥの設定を変更して悪質な Web ページへの誘導を行い、パソコン内の多くのファイルを削除。

5.2.3 フィッシングとは

フィッシング（phishing）とは造語で、個人情報を“ 釣る ”（fishing）と“ 巧妙な ”（sophisticated）を合わせたものとも言われている。

企業などが発信したと装ったＥメールを送信し、そのＥメールに記載されたＵＲＬに言葉巧みにアクセスさせ、ユーザーＩＤ、パスワード、クレジットカード番号、暗証番号等の個人情報を入力させ、不正に収集するものである。もちろんサイト自体偽物で、本物のサイトとは一見すると見分けがつかないように作られている。

Ｅメールの内容は「期間内にサイトにアクセスし、個人情報を入力しないとサービスを利用出来なくなる」などユーザーを煽る内容であることが多い。送信元を金融機関やクレジットカード会社として詐称していることもある。

また、フィッシングでは偽サイトのＵＲＬに誘導するために、さまざまな手法が使われる。古典的なものでは、ＨＴＭＬのリンクタグを利用する方法、ＩＰアドレスを表示させる方法などがある。また、ＵＲＬは本物のサイトと酷似したものとなっていて、ＵＲＬから本物のサイトか否かを判別することが困難な場合もある。

最近では、上記のような従来の形式のフィッシング以外にも、ＨＴＭＬメールを利用したものも見受けられる。

フィッシングはユーザー側の受ける実害は勿論のこと、偽アドレスを使用された企業の信頼問題にも関わってくる。

なお、偽サイトは通常数日で消滅してしまう。

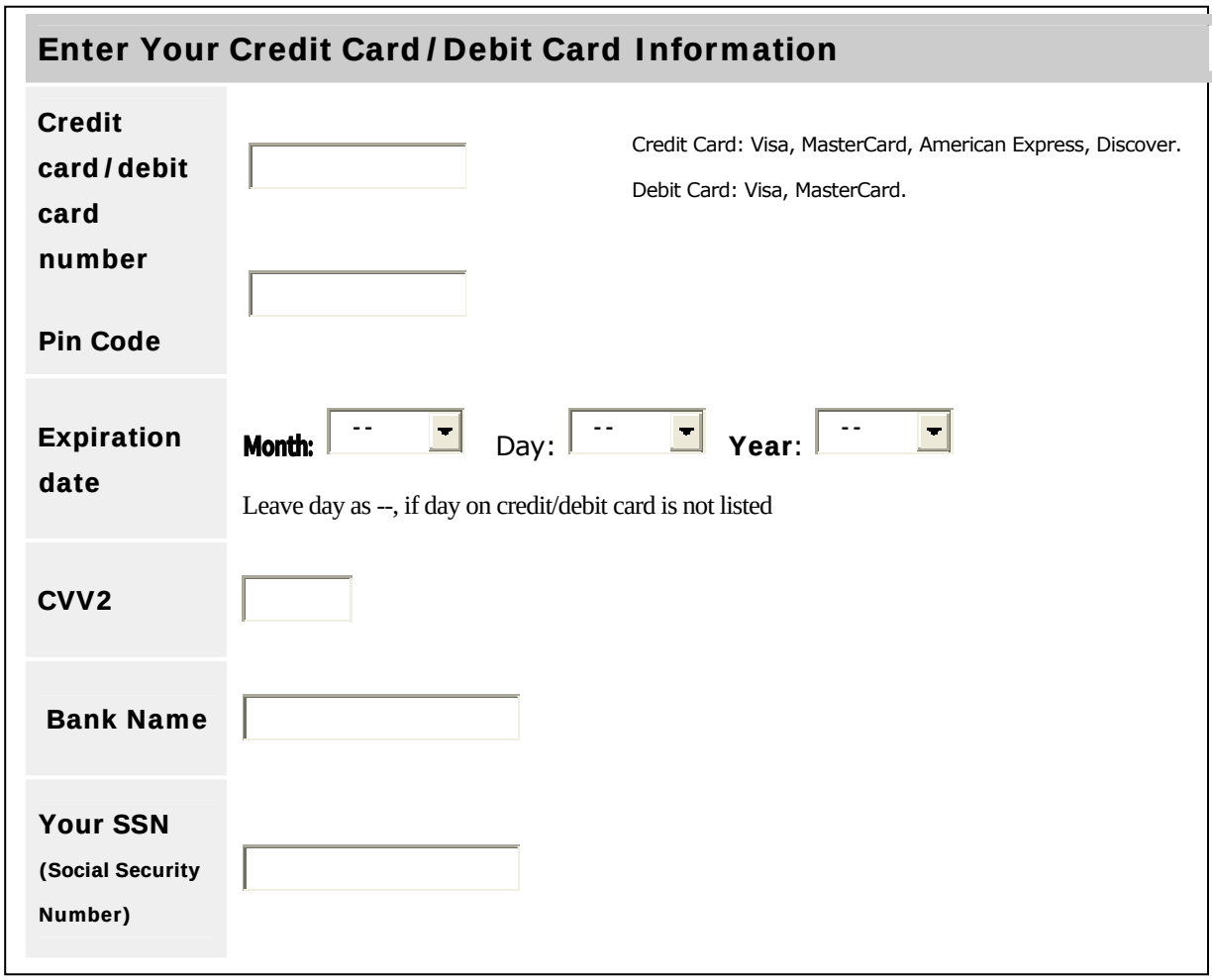


図 5-3　フィッシング･メールの例

図 5-3 は、海外ネットオークション利用者に送られてきたＨＴＭＬ形式のフィッシングメールであり、これに情報を全て入力して送信したところ、なりすましに遭い、当該オークション上で 20 件もの架空取引をされたという被害があった。

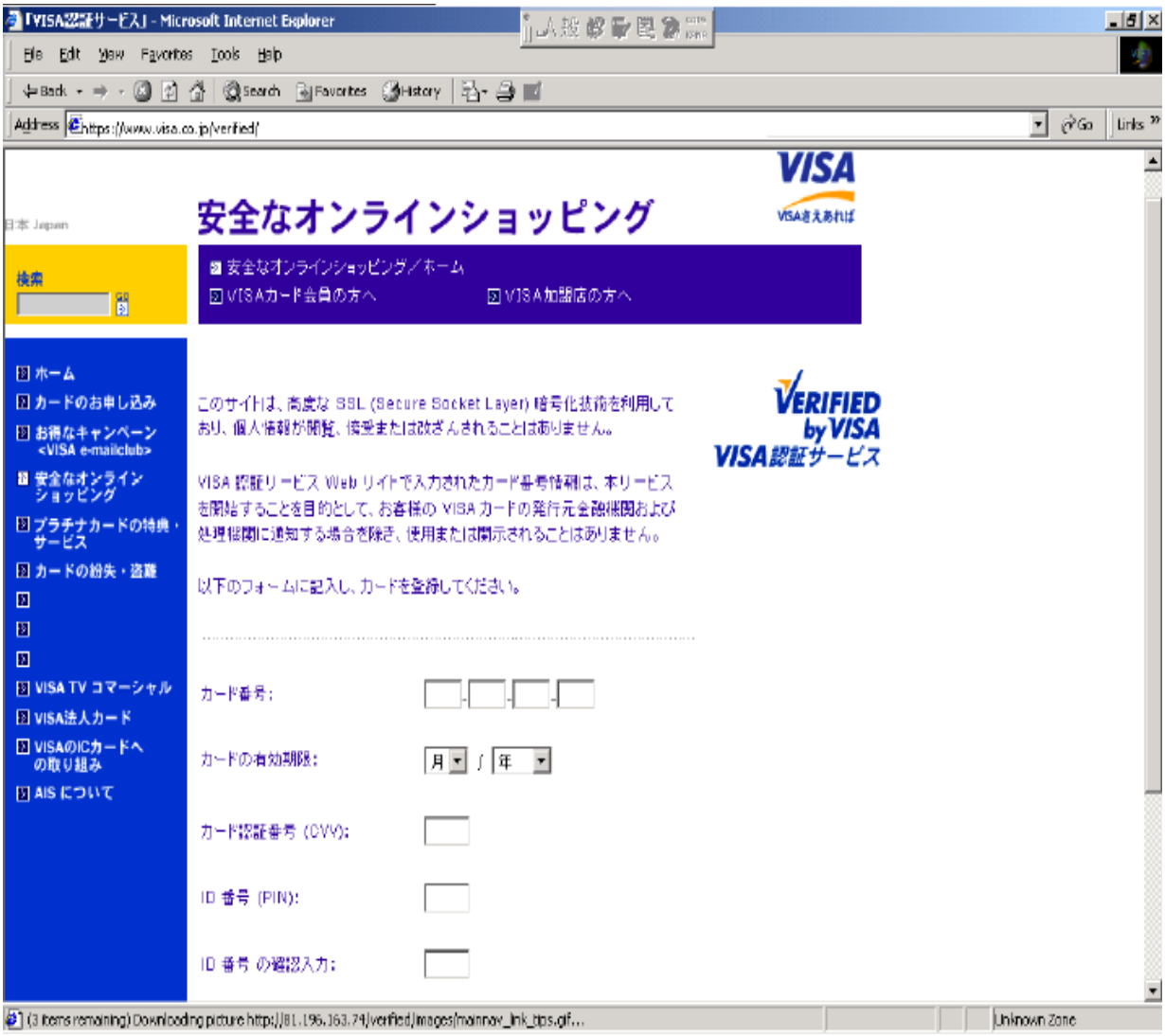


図 5-4　VISA になりすましたサイトの例

図 5-4 は VISA になりすましたフィッシング用サイトである。ロゴを真似る、「セキュリティ強化」「入力して（略）安全に活用」などの言葉を巧みに使い入力させる、といった巧妙な手口である。

5.2.4　スパイウェアとは

スパイウェアとは、ユーザーのコンピュータに入り込んで、そのユーザーの個人情報を潜入調査し、その結果を第三者に転送するプログラムである。収集される情報は、Web サイト訪問履歴、表示したバナー広告、Eメールアドレス、氏名、住所、電話番号、システム情報などである。ユーザーがプラグインやオンラインソフトなどを取得した際に添付されてくる。

本来であれば、ユーザーが承諾することにより初めてインストールされるものであるが、悪意のある者がユーザー承諾を得ずに（オンラインソフトをインストールするとユーザーの知らぬ間

にスパイウェアも同時に)、インストールされるものもある。

これにより、適切なタイミングでのポップアップ広告表示や案内メールの送付といった有効な利用ではなく、多数のポップアップ広告の強制表示、迷惑メールの送付に悪用される場合がある。

ユーザーにスパイウェアをインストールさせる場合、以下のトリックが用いられることがある。

・トロイの木馬
・ポップアップ
・ユーザーを欺くダイアログボックス
・紛らわしい使用許諾契約
・紛らわしい Web サイト名

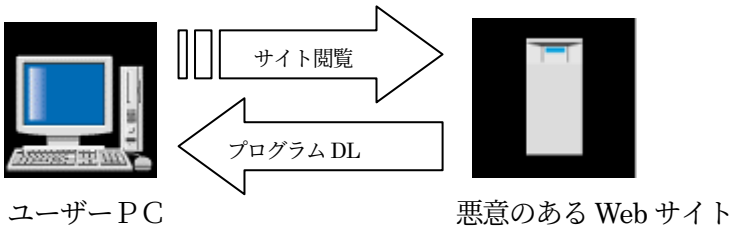


図 5-5　スパイウェアが侵入する仕組み

例えば、海外の怪しげなサイトを閲覧中に、何かしら悪意のあるプログラムをダウンロードされてしまうと、その後 Web ブラウザを立ち上げるたびに英文のポップアップ広告が強制的に表示されるようになり、その都度消しても、Web ブラウザを立ち上げる度に表示されてしまうといった被害が発生する。

こういった場合には Web ブラウザのスタートページが、そのポップアップ広告のＵＲＬに書き替わっていることが考えられるので、その設定を元に戻してやる必要がある。

また、こういった悪意のあるプログラムを見つけたり、削除したりするソフトがあるので、それらのソフトをインストールしておき、定期的にチェックをするということでも被害防止に役立つ。

5.2.5　キーロガーとは

キーロガーとは、キーボードやマウスから入力した内容をすべて記録するソフトである。悪意ある者がパソコンに仕掛けた場合、クレジットカード番号、暗証番号などを盗まれる可能性がある。実際に平成 16 年 11 月には、ネットカフェのパソコンにキーロガーを仕掛け、銀行口座やオークションＩＤを盗んだことによる逮捕者が出ている。

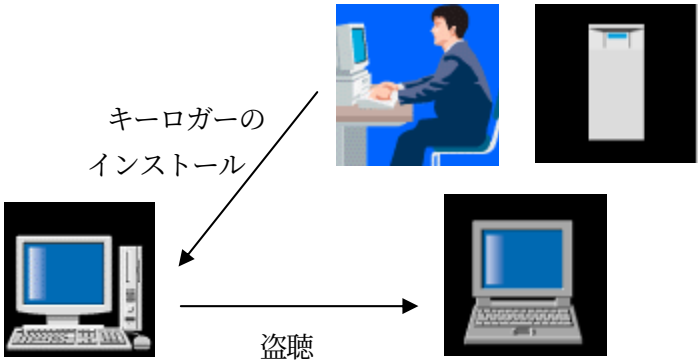


図 5-6　キーロガーが侵入する仕組み

5.3　ネットワークによる犯罪・被害への対策

様々な被害が顕著化し社会問題になっている今日でも、家庭でのＰＣ利用者の３割はなんら対策を行っていないのが現実である。対策を実施していないＰＣがウイルスなどによる被害に遭う確率は、対策してあるＰＣと比較すると２倍近い。また、アンチウイルスソフトやファイアウォールの設定だけでなく、利用者自ら巧妙化する詐欺行為に対して軽率な行動を取らないなどの、環境と利用者の意識、両方の対策が必須である。

家庭のＰＣはコンピュータウイルスやワーム、フィッシング詐欺などの、ほぼ全ての危険にさらされていると言っても過言ではない。これらの不正な攻撃に対する基本的な対策はネットワークの接続、設定を適切に行うことである。ＰＣ上で動作するＯＳやブラウザ、メールソフトの設定やアンチウイルスソフト、ＰＣ用ファイアウォールでの対策もあるが、あくまでネットワークの設定を行った上での追加対策である。

本節では、顕在化している犯罪・被害に対して、どのような対策を実施すればよいか述べる。

5.3.1　盗聴、不正アクセスの場合

ネットワークの設定及びＯＳやアプリケーションの最新パッチの適用で大部分を防ぐことが可能である。下記にネットワークの設定について述べるが、この設定以外にもＯＳやアプリケーションに最新のパッチを自動適用する設定が望ましい。

（１）　ブロードバンドルータの場合

一般にＡＤＳＬや光ファイバの場合は、インターネットと家庭のＰＣの間にＡＤＳＬモデムやＦＴＴＨ対応ルータなどと呼ばれるブロードバンドルータという装置を設置する。ＣＡＴＶの場合も専用の装置を用いてインターネットに接続される。

このブロードバンドルータにはルータ機能があり、家庭のＰＣが外部のインターネットからの脅威に直接さらされないようなファイアウォール機能を持っている。このファイアウォール機能などの代表的な機能を下記の表に示す。

表 5-1　ブロードバンドルータのセキュリティ機能

名称	機能	効力
ＩＰパケット フィルタリング	外に出る通信、外から入ってくる通信をポート単位で監視し、パケットを通過・遮断する機能。	無用なポートを閉じることで、外部からのポートスキャン[39]やセキュリティホールを狙ったワームを防ぐことができる。
ＮＡＴ （ＩＰマスカレード）	外部と通信するための一つのグローバルＩＰアドレスに対して複数のローカルＩＰアドレスを変換する機能。Network Address Translation の略。	外部インターネットからＩＰアドレスを隠すことができる。
不正アクセス 検出機能	外部からの不正と思われるパケットを検出・遮断する機能。	ＬＡＮＤ攻撃[40]など接続されている端末に高負荷をかける既知の攻撃を防ぐことができる。
アクセスログ	通信アクセスのログや不正アクセスのログを記録する。	攻撃を受けた際に何が起きたかを解析することができる。

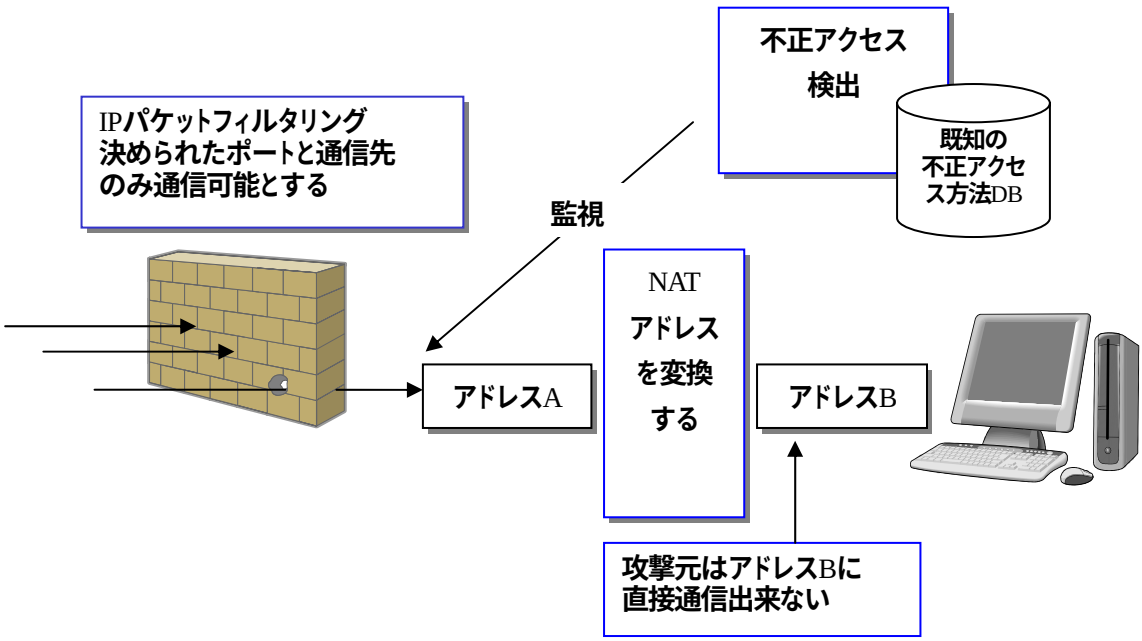


図 5-7　ブロードバンドルータの主要機能

[39] ポートスキャン：ＩＰの各ポート番号に順にデータを送信し、動作しているＯＳやアプリケーションを解析し、脆弱性を持つ通信可能なポートを検索する。
[40] ＬＡＮＤ攻撃：アドレス詐称攻撃の一つで、送信元アドレスを偽造し、受信先アドレスとポート番号を同一にしたあるパケットを攻撃対象のサーバに送信すると、サーバは自分に対して応答パケットを送り続け、自ら応答不能となってしまう。

ブロードバンドルータを使用する場合は、ＮＡＴを使用し、直接グローバルＩＰアドレスをＰＣに付与しない。必要なポートのみを使用し、その他のポートは閉じる。特にブロードバンドの外のインターネットからＰＣへのアクセスは真に必要なポート以外は遮断する。また、不正アクセス防止機能がついている機器では有効にする。

（２）　ホットスポット（公衆無線ＬＡＮ）の場合

新たにホットスポットと呼ばれる公衆無線ＬＡＮのサービスも普及しつつある。旅行時やビジネスマンなど、ノートＰＣを持ち歩き、必要な場所でホットスポットに接続する姿も頻繁に見られる。ただし、ホットスポットはあくまで公衆サービスであり、直接ＰＣから接続するため、家庭内からブロードバンドルータなどの機器経由で接続するよりも格段に危険が高い。

下記の図にブロードバンドルータなどの機器経由のインターネット接続と、一部のホットスポット、定額ＰＨＳ、ダイヤルアップによる直接接続の違いからなるネットワーク接続の危険性を示す。

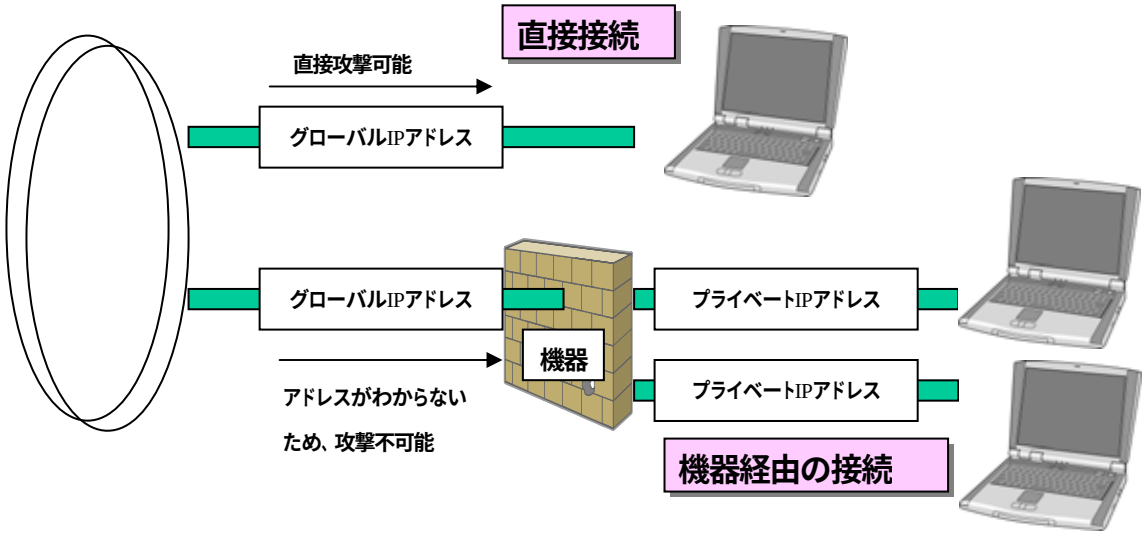


図 5-8　直接接続と機器経由のインターネット接続

直接接続の危険性は、接続されたコンピュータに対して、インターネット上の様々なコンピュータからの攻撃を直接受けることにある。接続されたＰＣにはグローバルＩＰアドレスが直接付与され、インターネットから直接ＰＣに対して通信可能な状態となっているため、ＯＳやアプリケーションの不具合を狙ったワームなどの攻撃がＰＣを接続した直後から観測される。直接接続の際は、ファイアウォールソフトの導入やＯＳやアプリケーションに最新のパッチを当てるなどの対策は必須である。

公衆無線ＬＡＮの環境では家庭内のようにセキュリティ設定は出来ないため、ＰＣ上にファイアウォールソフトを導入する。WindowsXP のＳＰ2 から導入されたファイアウォール機能でも防ぐことができる。ただし、流れるデータは他のＰＣで盗聴することが可能であるため、ＳＳＬやＶＰＮ以外では個人情報や重要な情報は流さないようにする。

（3）　家庭内無線ＬＡＮの場合

無線ＬＡＮ自体は適切に設定されていれば十分安全なネットワークである。残念ながら、ＩＳＰからレンタルされる無線ＬＡＮ装置や、量販店で販売されている無線ＬＡＮ機器については、初期設定のまま使われているケースが多く見られる。初期設定では、どんなＰＣでも無線ＬＡＮアクセスポイントに接続されるようになっており、そのまま使い続けると無線ＬＡＮの電波が届く範囲の全てのＰＣで接続可能となってしまう。無線ＬＡＮの通信距離は壁などの材質や周りの電波環境に依存するが、最大 100m程度通信可能なこともある。家庭で無防備に設定されている無線ＬＡＮアクセスポイントは近所や通りすがりの誰でも利用可能である。

近くの無線ＬＡＮアクセスポイントを検索し、そのセキュリティレベルを解析、表示するツールは WindowXP などに標準で搭載されており、高度な技術知識がない攻撃者にも不正利用されることがある。また、故意でなくても、ＰＣの設定によっては勝手に接続してしまうこともある。

このように無防備に設定された場合の危険性を下記の表に示す。

表 5-2　家庭内無線ＬＡＮの危険性

項目	危険性
不正利用	近所、通りすがりの利用者がネットワークに接続して、インターネットを利用することができる。自分の契約しているインターネットを通して違法行為をされる可能性の他に、他者への攻撃の踏み台にされる恐れがある。
不正アクセス	近所、通りすがりの利用者が自宅のＰＣのファイルを不正に取得したりする恐れがある。個人情報漏洩の可能性と他のサービスに対する不正アクセスを行う可能性もある。
盗聴	近所、通りすがりの利用者に自宅のＰＣで通信している内容を盗聴される恐れがある。登録サービスへのユーザーＩＤ, パスワードやクレジットカード番号などが盗聴される可能性がある。

また、このような不正な攻撃に対抗するための標準的なネットワークレベルでのセキュリティ対策を下記の表に示す。

表 5-3　標準的なネットワークでのセキュリティ対策

対策	概要	備考
SSID	アクセスポイント名称を隠す手段である。	フリーソフトで解析するツールが存在する。
WEP	認証・暗号化	ある特定条件下で破ることのできるフリーソフトが存在する。
WPA	認証・暗号化	今のところ破るソフトは出回っていない。
MAC アドレスフィルタリング	特定のＰＣしか接続出来ないようにする。事前にＰＣのＭＡＣアドレスの登録が必要。	一部の Linux 等ではＭＡＣアドレス詐称が可能。

WindowsXP 以降の機種のみであればＷＰＡを認証・暗号化に使用し、それ以外のＯＳではＷＥＰを用いる。また、アクセスするＰＣの下部にシール等で記述されているＭＡＣアドレスをアクセスポイントに設定し、登録されたＭＡＣアドレスのみ通信可能とするＭＡＣアドレスフィルタリング機能を用いる。

自分の無線ＬＡＮアクセスポイントの存在を公開せず、ＳＳＩＤを使用する。認証・暗号化とＭＡＣアドレスフィルタリングは必ず設定するようにしたい。

（4）　携帯電話

携帯電話はＰＣ以上に普及しており、個人が占有で使うことから個人をターゲットにした被害が顕著である。さまざまな対策は実施されているが、依然迷惑メール、迷惑ＳＭＳ、ワン切りは無くならない。

ＰＣと違い、携帯電話の場合はウイルスによる被害はほとんどない。海外では一部の携帯電話に Bluetooth 経由で感染するウイルスが発見されているが国内での被害はまだ報告されていない。

携帯電話による被害の手口は、迷惑メールなどでウェブサイトへクリックさせ、ＰＣに比べれば貧弱な画面や操作性を狙い、あたかも有料サービスに登録したような表示をさせるのが一般的である。加えてに携帯電話の個体番号などを表示することで、個人を特定したような印象を利用者に与え、金銭を要求することもある。

利用者が若年層から女性、年配者など多岐に渡り、必ずしもインターネットなどの技術に詳しくない利用者が狙われやすい。

表 5-4　携帯インターネット利用者における被害状況及び被害内容（複数回答）

（%）

（年）	平成 14 年	平成 15 年
被害あり	58.9	65.0
被害なし	23.2	15.8
無回答	17.9	19.2

（%）

（年）	平成１４年	平成 15 年
迷惑メール	58.0	64.3
個人情報の不正利用・漏えい	0.6	1.7
不正アクセス	1.4	1.4
ウイルス発見・感染	1.1	0.9
ウェブ上での誹謗中傷	0.1	0.2
その他	0.0	0.1

（出典）総務省「通信利用動向調査」

（５）　定額ＰＨＳ、ダイヤルアップ

これらはインターネットにアクセスした瞬間から、様々な攻撃に直接さらされるため、極めて危険である。ＰＣにファイアウォールソフトをインストールするか、WindowsXP の Service Pack 2（ＳＰ2）から導入されたファイアウォール機能を有効にし、ＰＣに対する攻撃を防ぐ。

（６）　情報家電

情報家電は実は中身はＰＣと同じような構成になっていることがあり、あるメーカのハードディスク付きＤＶＤレコーダーがセキュリティを設定しないまま使われ、別のサイトへの攻撃の踏み台となる事件も起きている。安易なネットワーク設定を行わないことと、メーカから出ている情報は定期的にチェックしたい。

5.3.2　フィッシング詐欺の場合

不審なメールは無視する。特に、金融機関やクレジットカード会社などではＥメールで口座番号やクレジットカード番号、暗証番号を尋ねることは絶対にない。焦りを煽るような内容であっても、落ち着いて対処する。あらかじめブラウザの「お気に入り」「ブックマーク」に登録しておき、必ずそこからアクセスする。ブラウザ上で重要な情報を入力する際には、鍵マークの中身（デジタル証明書）を必ず確認してからにする。ページの「プロパティ」でＵＲＬを確認する。

5.3.3　スパイウェアの場合

起動されているプログラムが何であるかを確認することが大事であるが、パソコンに詳しくな

いユーザーには難しい。簡単なのはスパイウェア対策ソフトでチェックする方法である。またウイルス対策ソフトにもスパイウェア対応機能が搭載されているものもあり、この方法によるチェックも有効である。

なお、スパイウェアはソフトの違法コピー防止策として組み込まれるなど、ソフトの内部機能である場合も考えられるので一概に悪質なソフトであるとは言えない。

5.3.4 キーロガーの場合

キーロガーを仕掛けられる可能性のある共用利用パソコン（ネットカフェ、ショールームなど）からは重要な情報の入力は行わない。

5.4 ネットワーク犯罪による被害にあった場合の対応

次々に新しいウイルスや攻撃、詐欺方法が現れる世の中では、どんなに注意していても、被害に遭う可能性は存在する。本節では、被害にあった場合の基本的な対処方法を記すが、セキュリティ関連サイトを参照し、常に最新情報を活用することが望ましい。

5.4.1 復旧方法

まず想定される被害としては、ウイルスやワーム、スパイウェアによるコンピュータのＯＳやデータの破壊、個人情報の流出などが想定される。一旦、ウイルスやスパイウェアに感染すると、それらが、何らかのメッセージ表示やメール送信などの行為を行うことが多いが、特にスパイウェアなどはユーザーには察知されないように活動を行うため、感染したことにすら気づかないことがある。

明らかにウイルスに感染したと気づいた場合、同じＬＡＮに感染したＰＣが存在する場合、ウイルスメールを送信していると警告があった場合、ゼロデイアタックなどで大規模に感染が広がっている場合には、即座にアンチウイルスソフト販売会社が提供しているウイルスチェックソフトを用いて感染の有無を判断する。感染していた場合はウイルスの拡散を防止するために、感染が発覚したＰＣはネットワークケーブルを外すなど、即座にネットワークから隔離することが重要である。次にウイルス削除ツールを用いるか、ウイルスのプロセスを停止させ、削除可能とする。ウイルスが完全に削除されたことが確認されてから、再びネットワークに接続を行う。

また、スパイウェアについてはフリーウェアに紛れてインストールされていることもあるため、定期的にスパイウェア検出ツールを用いてＰＣのチェックを行い、インストールされていた場合は同様のツールを用いてスパイウェアを削除する。

ウイルスはウイルス自体を拡散すること以外にＯＳやアプリケーションを書き換え、ハードディスク上のデータを破壊するものも多くも見られる。一旦、ウイルスに破壊されたデータの復旧はほぼ不可能である。ＯＳやアプリケーションでさえ、復旧できるものと復旧できず初期化が必要なケースもある。これらを復旧させるためには、日ごろからバックアップを取っておくことが望ましい。最善策としては、データのみバックアップを取っておき、ハードディスクをフォーマットしてからＯＳ、アプリケーションを再インストールすることであるが、初期出荷状態に戻す方式がＰＣベンダから提供されていない限りは非常に手間のかかる作業である。

5.4.2　報告・相談

ＩＰＡなどへの報告、被害相談窓口への相談

実際に被害にあった場合の、具体的な相談窓口や対応方法について述べる。

・ウイルス感染

ウイルスに感染してしまった場合には、リカバリとともに、ＩＰＡ（独立行政法人 情報処理推進機構）セキュリティセンターなどに届出をして、情報提供を行うことが望ましい。

・ネット上における詐欺

インターネットオークション上で、代金を支払っても商品が届かない、また代金が払われないといった詐欺の被害にあった場合は、大手オークションサイトでは補償制度を設けており、一定の条件下により補償を受けることが出来るので、まずはその申請を行うことが望ましい。あわせて警察にも相談して被害届けを受理してもらい、その所在地を確認したり、代金を銀行振り込みした場合はその金融機関に連絡して情報提供し、場合によっては口座凍結や組み戻し手続きについて相談するということが可能な場合がある。

ネットショップにおいて商品が届かないといった場合においては、詐欺のほかに単なる債務不履行のケースも多いので、地元の消費者センターに相談して同様の被害が上がっていないかどうか情報提供を受けたり、またショップに連絡してみてくれるよう依頼することが可能である。

・フィッシング詐欺

基本的に盗まれた情報、例えばクレジットカード情報であればクレジットカード会社窓口に連絡、またＩＤやパスワードであれば、その変更を行うといった対策が必要である。悪用された場合には、各警察署のハイテク相談窓口に相談する。

また個人情報保護法の全面施行後は、各行政や自治体単位にそういった相談を受ける窓口があるので、その窓口で助言や情報提供を受けるといったことも可能である。

・振り込め詐欺や架空請求

メールやＳＭＳメールにより身に覚えの無い全くの架空請求があり、その請求に応じてしまった場合には、すぐに警察に相談し、警察より振込先の金融機関に連絡してもらい口座凍結手続きを行うよう依頼する。以前は書面等手続きが煩雑であったが、現在は社会問題になっていることからも、銀行側の対応が迅速化している。

・サイトからの不当請求

いわゆるアダルトサイト側によるワンクリックでの自動登録により、契約が成立していないにも関わらず勝手に料金を請求され、それに応じて支払ってしまった場合には、サイト側にあわてて連絡をとる等は行わず、消費者センターに相談して、今後考えられる対策について助言を受ける。

特に振り込んだ振込先名義人が個人名の場合は架空口座の可能性が高いので、架空請求と同様にやはり警察や金融機関窓口に相談する。

クレジットカード詐欺でのクレジットカード会社への相談

クレジットカード番号が不正に悪意の第三者の手に渡って使用され、全く身に覚えのない請求が来た場合は、まずクレジットカード自体が手元に存在するか否か（紛失等をしていないかどうか）を確認のうえ、速やかに発行元のクレジットカード会社に連絡を入れ、当該クレジットカード番号を無効にする（代わりに新たな番号のカードを発行してもらう）必要がある。

請求された金額の取扱いについては、クレジットカード会社がクレジットカード番号情報の流出経緯などを調査し、カード保有者側に過失がないことが明らかになった場合、ほとんどのケースで支払が免除される（クレジットカード会社が損害を補填する）可能性が高いが、クレジットカード会社により対応が異なるため、発行元のクレジットカード会社に連絡を入れることが必要である。

また、自身でもクレジットカード番号情報が漏洩した原因（フィッシング被害にあった可能性有無など）について可能な限り把握し、それ以降の被害再発を防止することが肝要である。

5.4.3 法的対処

訴訟を起こすことは可能か？

ⅰ）関連法令と具体事例

関連法令

ハイテク犯罪の増加に伴い、各種の法整備も進められている。

以下にその一例を挙げる。

刑法

電子計算機損壊等業務妨害罪

コンピュータや電子的データを破壊することによる業務妨害に適用。

電磁的記録不正作出及び供用罪

事務処理を誤らせることを狙った、電子データの不正な作成に対して適用。

電子計算機使用詐欺罪

コンピュータに虚偽の情報等を入力するなどして不正な利益を得る詐欺行為に適用。

不正アクセス行為の禁止等に関する法律（不正アクセス禁止法）

他人のＩＤやパスワードを無断使用して不正にアクセスする、クラッキングなどにより直接侵入して攻撃する、又は踏み台を使って間接的に攻撃をする等の「不正アクセス行為」に対して適用される。

特定電子メールの送信の適正等に関する法律（迷惑メール規制法）

広告などの迷惑メールを規制するものであり、架空のメールアドレスによる送信禁止などが謳われている。

ⅱ）具体例

匿名性が高く、痕跡が残りにくいとされる“ハイテク犯罪”であるが、これらに対抗すべく、いくつかの法整備が為されており、実際に犯人検挙に至っているケースも数多く存在する。

以下に、その具体例を示す。

表 5-5　不正アクセス行為と関連法令

（警視庁ホームページ http://www.keishicho.metro.tokyo.jp より抜粋。）

事例	適用法令
被疑者は、インターネット喫茶に「キーロガー」を仕掛け、IDやパスワード等の個人情報を収集した上、平成 16 年 6 月 29 日から同年 7 月 2 日までの間、インターネットバンキングに不正アクセスし、他人の預金口座から自己の管理する預金口座に現金を送信させ、騙し取った。	不正アクセス行為の禁止等に関する法律 刑法第 246 条第 2 項（電子計算機使用詐欺）
被疑者は、自分が勤務する携帯電話販売会社の携帯電話購入申込書に記載されていたクレジットカード情報を盗み見して電子マネーを購入し、騙し取った電子マネーは、インターネットオークションを利用する等して換金していた。	刑法第 246 条第 2 項（電子計算機使用詐欺）
被疑者らは、平成 15 年 4 月頃から平成 16 年 1 月頃までの間、実際には商品を保有していないのにインターネットオークションに虚偽の出品をし、落札代金を詐取する行為を繰り返していた。更に、他人のクレジットカード情報で通販サイトから商品を騙し取り、その商品をオークションに出品して不正な現金を得ていた。	刑法第 246 条第 1 項（詐欺）
上記事例に関連し、別の被疑者は、上記犯罪者グループのメンバーに、不正に入手したクレジットカード番号情報を教え、犯罪者グループの詐欺の犯行を容易にさせた。 被疑者は、派遣されて勤務していた店の顧客情報などを無断でメモして持ち帰り、インターネット上の掲示板及び電子メールを通じて、上記犯罪者グループに 1 件 1 万円で 178 名分の情報を売り、不正な現金を得ていた。 ※インターネット上の個人情報の販売を詐欺幇助罪として適用したのは、全国で初めてのケース。	刑法第 246 条第 1 項、及び、第 62 条第 1 項（詐欺の幇助）

iii）「少額訴訟」の活用

ネットワーク上における詐欺被害に遭った場合など、相手の住所などから居住の事実が確認できるようであれば、「少額訴訟制度」という簡易裁判の手続きを取ることも考えられる。

「少額訴訟制度」とは、60 万円以下の金銭トラブルを、簡便かつスピーディーに解決可能な簡易裁判制度であり、弁護士に依頼する必要もなく、簡易裁判所を窓口に、誰でも気軽に紛争解決の場として利用することが可能である。

原則として、1 回の審理で即日判決が出るが、控訴は不可であり、証拠は、領収書や写真など、その場で調べられるものに限定される。（但し、不服がある場合のみ、同じ裁判所への異議の申し

立てが可能。）また、必要な費用は、裁判所に支払う印紙代などで 7,000 円程度であり、原則として証人は当日法廷に出廷することが求められ、訴状は相手方の住所地を管轄する簡易裁判所に提出する。（以上、警視庁ホームページ http://www.keishicho.metro.tokyo.jp より抜粋。）

なお、最近、この「少額訴訟」や「督促手続き」を逆手に取り、「出会い系サイト」の利用料などを架空に請求する手口が発生し問題となっているため、その対処方法を以下に示す。

裁判所から書類が届いた場合は、身に覚えがなくても放置せず、本当の裁判所からのものであるかを確認する。

⇒悪質な業者が、裁判所からの通知であるかのように装って偽りの連絡先を記載している場合もあり、その場合、こちらから連絡をすることによって電話番号などの個人情報を知られてしまう恐れがあるため、書類に記載された連絡先にすぐ連絡することは避け、発送元及び連絡先が本当の裁判所であるかを、電話帳や消費者センターなどで確認する。

本当の裁判所からの通知であると確認できた場合

発送元及び連絡先が本当の裁判所であることが確認できた場合は、具体的な対応策について弁護士や消費者センターなどに相談する必要がある。

- 本当の支払督促であった場合

  そのまま放置して何も対応しなかった場合には、強制執行されるなどの不利益を被る危険があるため、身に覚えがない請求であれば、支払督促を受け取った日から２週間以内に裁判所に対して「督促異議の申し立て」を行なう必要がある。
- 本当の少額訴訟手続であった場合

  そのまま放置して、指定された期日に裁判所に出頭せず、かつ事前に請求を争う旨の書面を裁判所に提出しない場合は、相手方の主張を認めたものとされてしまい、敗訴する危険があるため、身に覚えのない請求の場合には
- 指定された期日に裁判所に出頭する
- その期日に先立って自分の言い分を記載した「答弁書」という書面を提出しておく

  必要がある。

本当の裁判所からの通知ではないと確認された場合

こちらから連絡する必要は全くないが、不安な場合には消費者センターなどに相談する。

（以上、法務省民事局ホームページ http://www.moj.go.jp/MINJI/minji68.html より抜粋・加筆）

5.5　ネットワーク犯罪防止に向けた提言

5.5.1　法制度

ネットワーク犯罪に対応したこれまでの法改正や新法の設定については、ややもすると泥縄的な対応となっている感が否めないが、情報ネットワーク技術の進歩の速度を考えると、ある程度は止むを得ないのかもしれない。

とは言え、これまではどちらかと言うと精神的・経済的な被害をもたらすことが主であったハイテク犯罪も、今後はより広範囲で深刻な被害が発生することも想定すべき時代に突入したと言

っても過言ではないだろう。

現状、ネットワーク犯罪を含む「ハイテク犯罪」に対する法整備に関しては、各担当省庁が個別に対応を進めている感もあるが、本格的なユビキタス社会の到来に向け、今後は官民の連携を一層強め、新たな技術の導入に伴って起こり得る犯罪を可能な限り予測し、その抑止効果も見据えた法整備を進める必要があると考える。

またネットワーク犯罪に付随して発生すると思われる被害に関しても、同時に法整備を考えていく必要がある。例えば決済に関しては、金融機関等が速やかに被害拡大防止に努められるような仕組みを作ることや、ＩＤやパスワードの不正利用による被害を防止するため、本人認証を徹底することなどを盛り込んだ内容の法整備が今後も必要になってくると思われる。

5.5.2　情報リテラシー

情報リテラシーとは、一般的にはコンピュータを操作できる能力や知識のことを指すが、コンピュータを悪用するハイテク犯罪に対応するには、通常のインターネットで情報を検索・取得できる、メールを送受信できる、といったような基本的なコンピュータ教育では十分ではなくなっている。

表 5-6　セキュリティ対策を行っていない理由（複数回答）

(%)

	ウイルス	不正アクセス
費用がかかるから	37.5	21.1
面倒だから	36.9	27.2
具体的な対策方法が分からないから	30.6	53.2
自分は被害に遭っても大きな損害は受けないと考えているから	19.8	18.1
対策をしても被害に遭うと考えているから	14.5	10.4
自分は被害に遭わないと考えているから	7.6	8.7
その他	5.7	2.3

（出典：総務省　平成 16 年度　情報通信白書）

表 5-6 に個人ユーザーがセキュリティ対策を行っていない理由を記すが、「面倒だから」、「具体的な対策方法が分からないから」などといった、十分な知識がないために対策を打たない事例が多く見られる。また、費用についても、ＯＳの最新パッチやフリーのアンチウイルスソフト、スパイウェア発見ツールなど、無料で行える対策も十分あるし、インターネットサービスプロバイダも十分安い価格でメールのウイルス削除サービスを供給している。

いたずらにインターネットの危険性を煽る必要はないが、どのような危険や犯罪があり、何をすれば防げるのか、可能な限り多くのユーザーに対して啓蒙活動を行うことは今後必須である。様々なベンダや研究機関がセキュリティ対策製品の研究開発を行っているが、残念ながら、技術は常に現実の後追いであり、ユーザーの慎重な行動がインターネットを安全に使うための最終的

なポイントである。ＰＣベンダやインターネットサービスプロバイダに任せるだけではなく、初心者ユーザーが簡易に利用可能な情報提供サービスや各地域でのパソコン教室など、仕組みや教員、場所、補助金の提供など、官民一体となって取り組むべきであろう。

5.5.3　教育制度

ネットワーク犯罪防止に向けて法整備と共に必要と考えられるのが、特に若年層を対象とした情報セキュリティに関する教育制度の整備である。

文部科学省の統計（平成 15 年度）によると、全国の公立学校に設置された教育用コンピュータの平均設置台数は、全体で 40.0 台／校（1 台あたりの児童生徒数は 8.8 人）であり、小学校で 27.7 台（同・11.2 人）、中学校で 44.1 台（同・7.7 人）、高等学校で 101.4 台（同・6.7 人）などとなっており、総台数の 84.9%がインターネットに接続している。（文部科学省ホームページ http://www.mext.go.jp/b_menu/toukei/main_b8.htm より引用）

これに加えて、近年の各家庭へのパソコン普及率や、ネット接続機能が半ば標準搭載となった携帯電話の、当該世代への普及率を勘案すると、現在、かなりの児童生徒がインターネットに接続できる環境を身近に持っていると言え、十分な知識を持たないまま気軽にインターネットにアクセスした結果、ネットワーク犯罪の被害者、場合によっては加害者となるケースが増えている。

こうした状況の下、一部の学校では、「情報モラル指導」といった形で、インターネット利用時の留意点等や、所謂“ネチケット”を指導したり、ＩＴ関連の民間企業社員を講師として招いて情報セキュリティに関する講座を開いたりといった取組みを行なっており、文部科学省も、指導者向けに情報モラル指導のモデルケースを公開するサイト（http://sweb.nctd.go.jp/support/index.html）を設置するなど、児童生徒の情報化対応を推進している。

また、総務省も、「情報通信白書 for KIDS」（http://www.kids.soumu.go.jp/index.html）と題した、インターネットからユビキタスネットワークまでを分かりやすく解説した小中学生向けサイトを設置するなど、子供たちに対する教育・啓蒙活動を進めている。

このように、若年層に対する情報セキュリティ教育の必要性は既に認識されつつあり、前述の例以外にも、警察等、関連機関ごとで具体的な教育・啓蒙活動が行なわれているものの、一方で、若年層が犯罪の被害者又は加害者となるケースが後を絶たないことから、教育・啓蒙活動の余地はかなり多く残されており、以下に、今後、我々が取るべきであると思われる対応を列挙する。

（1）　大人たちの知識・意識向上

家庭内や教育現場などで“指導者”となるべき大人たちが、まずは情報セキュリティに関する正しい知識を身に付けると共に、子供たちのすぐ身近にネットワークへの入り口があることを強く認識し、必要な指導・アドバイスを行なうことが肝要である。

（2）　学校教育プログラムへの組み込み強化

前述のとおり、教育現場における情報インフラ整備はかなり進んでいると言えるが、「情報モラル」の指導については、内容、頻度など、地域によってバラつきがあるように思えるため、これをある程度全国一律のプログラムとして標準化するなど、全ての子供が一定の知識を持てる環境を整えるべきであると考える。

まずは、子供たちに「ネットワークの入り口＝実社会への入り口」という意識を強く持たせることが必要であろう。

（3） 関連団体・企業における啓蒙活動強化

これまでにも、関連各省庁を初め、民間企業レベルでも様々な取組みがなされているが、今後は、家庭や教育現場との連携を一層深め、日々進歩するネットワーク犯罪技術の最新情報をタイムリーに提供する体制を整備し、子供たちが犯罪に巻き込まれることを未然に防ぐことが必要であると感じる。

民間企業においては、個々の企業単位での活動では様々な面で限界があるため、各業界団体を窓口にするなどの取組みも必要であろう。

5.6 まとめ

くらしとセキュリティの関係を考える上で非常に重要なことは、コンピュータ犯罪やセキュリティ対策に対して、正しい知識を持つことである。

また、インターネットの進展やコンピュータの低価格化が、くらしのなかへ便利な道具として認知されつつあるのは事実である。しかし、そうした陽のあたる部分があれば、陰の部分が存在することも否定できない。世の中が便利になればなるほど、その代償としてリスクを背負わなければならないのは、特にコンピュータの世界に限ったことではない。

現実、陰となる部分として、「独立行政法人 情報処理推進機構」（以下、ＩＰＡとする。）がまとめたウイルス届出件数の年別推移を比べると昨年度（2003 年 1 月から 11 月）15,973 件が本年度（2004 年 1 月から 11 月）では、47,246 件である。約 3 倍の増加である。

このことは、コンピュータ利用者がなんらかのコンピュータ犯罪や被害に遭遇する可能性が高くなっていることを示唆している。

そのようなリスクをできるだけ回避するために、「セキュリティ・ツール」がいろいろな企業によって開発されている。また商品として販売されている。ここで言う「セキュリティ・ツール」とは、コンピュータを不正な利用や誤用から守るための仕組みである。ここで言う不正な利用とは、第三者による秘密情報へのアクセスや許可されていない操作の実行などが含まれる。

ＰＣの利用者に対しても、ＩＰＡのホームページに「ウイルス対策の 7 箇条」を示しされている。

以下に、参考のためにＩＰＡのホームページより引用し、記載している。

『パソコンユーザーのためのウイルス対策 7 箇条』

（1）最新のウイルス定義ファイルに更新しワクチンソフトを活用すること

新種ウイルスに対応するために、最新のウイルス定義ファイルに更新したワクチンソフトで検査を行うことが肝要。ウイルス定義ファイルの更新にあたっては、ワクチンベンダの Web サイトを定期的にチェックするなどし、最新のバージョンを確認しておくことが重要である。また、プリインストールされているワクチンソフトは、機能が限定されている場合もあるので、製品版にアップグレードすること。

（2）メールの添付ファイルは、開く前にウイルス検査を行うこと

受け取った電子メールに添付ファイルが付いている場合は、開く前にウイルス検査を行う。

また、電子メールにファイルを添付するときは、ウイルス検査を行ってから添付する。

（3）ダウンロードしたファイルは、使用する前にウイルス検査を行うこと

インターネットからファイルやプログラムなどをダウンロードした場合は、使用する前にウイルス検査を行う。また、ユーザーに被害を与えるプログラム（国際電話やダイヤルQ２に接続するプログラムなどで、ワクチンソフトで発見出来ない可能性が高い。）が潜んでいる場合があるので、信頼出来ないサイトからのファイルやプログラムなどのダウンロードは避ける。

（4）アプリケーションのセキュリティ機能を活用すること

マイクロソフト社の Word や Excel のデータファイルを開くときに、マクロ機能の自動実行を無効にするなどのアプリケーションに搭載されているセキュリティ機能を活用する。また、メーラー、ブラウザのセキュリティレベルを適切（中レベル以上）に設定しておくことにより、被害を未然に防ぐことができる。

（5）セキュリティパッチをあてること

基本的なウイルス対策を行っていても、セキュリティホールのあるソフトウェアを使用していると、ウイルスに感染してしまうことがある。例えば、電子メールの添付ファイルの自動実行を許してしまうメーラーのセキュリティホールは、ウイルス感染被害を著しく増大させる可能性がある。このようなセキュリティホールは、頻繁に発見されているので、使用しているソフトウェア（特に、メーラー、ブラウザ）に関してベンダの Web サイトなどの情報を定期的に確認し、最新のセキュリティパッチをあてておくことが重要である。

（6）ウイルス感染の兆候を見逃さないこと

下記のような兆候を見逃さず、ウイルス感染の可能性が考えられる場合、ウイルス検査を行う。

①システムやアプリケーションが頻繁にハングアップする。システムが起動しない。
②ファイルが無くなる。見知らぬファイルが作成されている。
③タスクバーなどに妙なアイコンができる。
④いきなりインターネット接続をしようとする。
⑤ユーザーの意図しないメール送信が行われる。
⑥直感的にいつもと何かが違うと感じる。

（7）ウイルス感染被害からの復旧のためデータのバックアップを行うこと

ウイルスにより破壊されたデータは、ワクチンソフトで修復することは出来ない。ウイルス感染被害からの復旧のため、日頃からデータのバックアップをとる習慣をつけておく。また、アプリケーションプログラムのオリジナルＣＤ-ＲＯＭ等は大切に保存しておく。万一、ウイルスによりハードディスクの内容が破壊された場合には、オリジナルから再インストールすることで復旧することができる。

最後に、コンピュータ犯罪への手口は、年々巧妙になってきている。その対策も取組まれているが、ますます利用者の犯罪に対するセキュリティ対策の知識が要求されてくる。このことは、普段からコンピュータセキュリティへの関心を持ち、コンピュータ犯罪の手口など、「知識」として学習することが大切である。

6. 更なる便利なくらしとネットワーク

ここまでの章ではくらしとネットワークの観点から過去と現在の多くを見て来た。またネットワークを介してくらしが便利になって来たことは体験を通じて少なからずも実感されたことと思われるが、その反面、様々な脅威が次々と出現し便利な機能を利用するための知識と脅威としての認識の両方を併せ持っていかなければならない時代となってきた。

本章では今までの過去や現在におけるくらしとネットワークから一歩踏み出して将来的なくらしとネットワークの関係について考察することとした。

6.1 本人認証

本人認証で盛んに利用されている方式としてパスワードがある。キーボードさえあれば簡単に本人であることを確認できる反面、忘れたり類推されたりして事故も多いことは周知のとおりである。

これに代わり最近では生体認証技術が向上したことから指紋、静脈、虹彩、網膜、手形と人体のあらゆる部分を利用して本人であることの確認が行われている。これらの認証方式では精度の高いものや、認証装置が小型にできるものなど様々な特徴を有している。

将来的にはこれらの認証データがネットワークを介したり、パソコンに埋め込まれたり、ＩＣカードに搭載されたり方式が利用スタイルに応じて適用されるものと考えられる。

まずネットワークを介した方式では、ネットワークの向こう側の相手の顔を見なくても確実にアクセスしてきた本人であることの確認できるようになる。現在でも生体認証のデータをネットワークを介して照合する方式が存在するが、盗聴などによる生体情報の漏洩などの危険性が指摘されている所である。

この様に考えると本人の認証はネットワークの向こうに送信するのではなく、利用する端末と本人の関係で対応させることが高いセキュリティを構築できそうである。具体的な例としてパソコンのＣＰＵボードなどにＩＣチップを埋め込んでおき、購入時点で本人確認を厳重に行い、その時の認証データをチップに埋め込んでおくことが可能であろう。従って、パソコンと本人の一対一の環境が構築できることとなる。

また本人認証データを登録したＩＣチップを不正にアクセスしたり、外そうとしたりすれば、パソコンの認証機能が自己破壊し異常モードとなったことを特定の団体等に連絡するなどのセキュリティ機能を持たせる。実際の利用場面においては従来の発信元データに加え、本人認証データの連絡を通信標準として採用しておき、人間とパソコンが常に正常な組み合わせであり、且つ通信元の身元が正しく証明されることとなる。特に決済に関係する通信においては必須事項として取り入れられることが可能である。

なおこの方式を推し進めて考えると何らかの原因で前述のスパイウェアがパソコン内部に侵入すると認証データの盗難につながるのでこの点についての配慮が必要である。

ＩＣカードを利用した方式では、ＩＣカードの中に本人の顔写真や指紋データを事前登録しておき、認証装置にＩＣカードをかざして認証装置とＩＣカードの間で、まずそのカードが本物であるか、次にそのカードの持ち主が本人であるかを認証することができる。

ＩＣカードの中に本人認証用データを入れておく方式では、センターサーバへの認証用データの登録が不要であり、認証時に本人の認証データの通信を行う必要が無いことから盗聴などによる個人情報の漏洩の可能性はセンター管理方式より少ないものと考えられる。

いずれの方式も一長一短がありそうであるが、要はコスト、利用目的に合致したセキュリティ強度を考慮することが大事であり、これらの方式により格段にセキュリティが向上し快適で安全なアプリケーションの利用ができることとなる。

最後に、様々な場面で匿名性が求められてきたが、将来的には本人認証すること＝非匿名性を基本とし、またその逆に相手に対しても同様な認証を求め、本人同士が正しく認識できることにより、決済におけるバリューの完全保証や何時でも何処でも安心して利用できるなどの信頼の上に築かれたオープンな通信環境がくらしの中で活用できることを願うものである。

6.2　機能集約

その時代時代で発行されたさまざまなカードが街に溢れている。例を挙げればクレッジットカード、キャッシュカード、ポイントカード、健康保険カード、各種会員カード、更に今後は郵便貯金カード、免許証、パスポート等々が新規に加わる気配であり、それに忘れてならない住基カード等々、実にサイフに入りきれないほどのカードに取り囲まれていると言っても過言でない。

そろそろこれらカードのＩＤを一本化し一枚のカード上で全ての機能を実現出来る時代の到来はそう遠くないはずである。カードに詳しい人は『セキュリティは保たれるのか』、『悪用されないか』、『カードの更新時はどうする』、『盗難時や紛失したらどうする』、『ＩＤが流失したら』・・・などなどと問題提起されるであろうが、前項の本人認証技術の向上などと相まって、これらの問題を解決する知恵と技術は達成可能と考える。

更に本人認証をもっとうまく活用できればカードも不要となるはずであり、決済処理に要するハンドリングコストの大幅な低減も夢では無くなる時代がやってきそうである。

これはカードに限らずパソコンや携帯電話などのハードウェアについても同様である。今日では一人一台のパソコンや携帯電話の時代から利用環境に応じて使い分けている時代であるが、これもまた技術の進歩によりパソコンと携帯電話が一つになり家の中でも街の中でもこれ一台あれば用事が全て足りそうな気配は今でも感じられるほどである。

究極的には一枚のカード（これも最終的には不要であるが）あるいは一つの本人認証ＩＤと一台の超多機能パソコンあるいは超多機能携帯電話を持ち歩けば、買い物、電話、メール、交通用途、果ては海外旅行まで対応できる究極のくらしとネットワーク環境が構築できる日も近い。

6.3　立体映像

音の世界はステレオと言われた時代を経由して今や 5.1 チャネルの音響が楽しめる様になってきた。一方、画像の世界と言うと立体画像が特殊な眼鏡を使用しなくても楽しめる一歩手前まで来ている。

この技術の進歩の先には今まで出来なかったことが可能になることにより、便利なくらしを実感できるものと考えられる。

例えば、紙の世界から出発した通信販売であるが、これがネットを介した平面画像による通信

販売も増加傾向である。しかしながらこのネット通販に向かない商品があることも事実である。魚や肉等における形状（色もあるが）、洋服の場合のサイズ（実際に着用しないと詳細は判らない）などである。

これらの商品が立体映像としてディスプレイで確認できれば、例えば洋服の場合であれば本人の体型データを入力し、バーチャル的に試着して前後左右あるいは上下についてもそのバランスや形状を確認できるのではと思われる。これにディスプレイの色が実物と変わらない自然色が得られれば更に判りやすいものとなる。

車に搭載するカーナビにおいても立体映像に進化することにより視認性が向上しディスプレイを短時間見るだけで欲しい情報を得ることができる等、人に対して直感的に一瞬に必要な情報を提供できる環境の出現となるであろう。

最近は自動車メーカが FLASH による立体映像のビジュアルカタログを提供している。以下に代表的なＵＲＬを参考までに提示する。

http://www.yappa.co.jp/site/products/fset_projects.html

http://www.viewpoint.com/democd/jewelry/Razolith/index.htm

http://accessory.subaru.co.jp/legacy/3d/3d.html#top

http://www.nissan.co.jp/SKYLINE/V35/0106/DATA/MAIN/index.html

6.4　情報家電

従来、情報家電と言うと冷蔵庫が通信機能を有し、携帯電話により冷蔵庫の中身が確認できたり、通信機能を持ったエアコンに携帯から指示するとエアコンが作動して帰宅すると快適な温度環境になっていたりと、便利な機能が搭載される様になってきた。これらの機能は技術的には充分確立した機能として評価されている。

これから求められる情報家電としては、技術的見地からの機能としてでは無く、人間の行動や生活スタイルをサポートする機能が求められる様になるのではないかと考える。

例えばトイレに入ったりパソコンの前に座ったりした時に自動的にその人の体調に関する測定が成され、健康状態を知らせてくれるというものである。あるメーカのトイレには簡単ではあるが脈拍や血圧等の人体の基礎データを測定するものもあると聞いている。

更に進化すれば採血せず非接触により血液中のコレステロールや血糖値、肝機能などのデータが得られたり、尿糖、タンパク値、更には各種感染症の検出などもできれば、そのデータを健康センターなどに通信し、家庭内のディスプレイや保有している携帯などへ検査結果などを連絡してくれると言うものである。企業がこれらを採用すれば自社の社員の健康管理に役立てることが出来、社員の健康向上は基より健康保険の負担も軽減できるメリットも期待できる。

話が家電とはいささか違う方向に行ってしまったが、要するに情報家電と言われる機能を考えた時に、単に便利とか、あれば面白いと言うものではなく人間のくらしと密着した、例えば健康（健康管理、病気警報、介護補助など）、食事（カロリー、栄養バランス、摂取量、食費など）、交通・移動（最適乗車案内、今何処サービスなど）、勉強環境（学習効果測定、補習補助、教材提供など）等、まさに人間のくらしをサポートしてくれる快適で安心安全な環境の提供を望む所である。

これらの実現の要素としては何と行ってもヒューマンインターフェイスとそれを実現する端末の出現であろう。

6.5 省電力化

現在の端末は昔と比較すると省電力化されバッテリも効率が良くなり、一段とポータビリティが向上してきたが、バッテリの重量にしろ、持続時間にしろ、我々が行動する生活スタイルには100%届いていないのが残念である。携帯を持っている人ならば常にバッテリ残量表示に気を使っており、ノートパソコンはバッテリだけで数時間までは快適に利用できるが半日以上は持たないのが現実である。

これら持続時間は快適なくらしに後一歩であり、更に時代が進めばパソコンや携帯が消費する電力はもっと少なくなり、これに加えて電力の源であるバッテリから今までに無い超高効率の太陽電池、空気電池あるいは炭酸ガスや水分から電力を取り出す電池などが出現してきそうな気配である。

『必要は発明の母』を大いに期待したいものである。

6.6 まとめ

くらしを支える技術の発展は日進月歩である。またそれら技術も様々な分野ですべからくくらしや社会活動に寄与していることは間違いのない所である。

しかし、それら技術が部分的にのみ発展しても課題の解決には遠く、様々な技術がバランス良く発展し、それらが有機的に結合してこそ素晴らしい発明へと進歩するのである。

マイクロコンピュータはパソコンを初め家電商品にも当たり前の様に実装されているが、そのマイクロコンピュータは微細加工技術や印刷技術、クリーン環境技術などの技術が総合的に噛み合って可能となったもので、一部の技術のみが突出してもマイクロコンピュータは実現出来なかったであろう。

くらしを支える要素としての技術は必要不可欠であるが、大事なのはこれらの技術を利用・運用する時の人間性を十二分に考慮する事である。

ここで言う人間性とは、人間は間違える、人間は盲点をさがす（悪用する）、人間は馴染む（不便でも慣れると気づかない）などの人間ならではの特徴のことを言うもので、これらを配慮することにより人にやさしく快適で安心・安全なくらしを支えることが実現できるものと確信する。

おわりに

利便性や快適性をもたらす技術の進歩向上と、悪意ある脅威を生み出す技術の進歩向上が今や拮抗状態にあることが問題であると言われている。様々なセキュリティ対策をパソコンに施したからと言っても安心はできず、新たな脅威の出現と共に早急に更に新たな対策を施さなくてはならない。

しかしながら大事なことは、くらし環境にいる一般消費者自らがこの新たな脅威の出現についての最新情報の入手、正しい知識の習得、効果的な対策の実施と、実に多くのことを理解し、また場合によってはいわれの無い費用負担もしなくてはならない事実である。

本調査研究ＳＷＧでは原稿の締め切り間際まで世の中を賑わしている最新のニュースや新たな事象までも盛り込むことができ、さながらセキュリティのノウハウ書的な様相を呈してしまったことは否めない。

研究調査対象として『セキュリティ』と言うキーワードが含まれている以上、ＳＷＧ結成当初にある程度は予測されたことではあるが、まとまった報告書の結果を見ると現実のくらし環境の中においては様々な脅威がすぐそこに忍び寄って来ておりその事実を伝えたい思いで一杯である。

今日も振り込め詐欺のニュースを耳にするにつけ、今まではセキュリティ対策とは企業が対抗する他人事と思っていたが、今では家庭やくらしの中でもセキュリティ対策を取っていかなくてはならないと実感すると同時に、これらのことを広く一般消費者に普及させなければいけないと言う責任をこのＳＷＧ活動を通じて感じた次第である。

参　考　資　料

参考資料

くらしのネット化に伴うセキュリティ課題の調査研究に当たって全委員で共有した「記事の見出し」とその「ＵＲＬ」を以下に掲載する。全てのＵＲＬは 2005 年 1 月 31 日現在、アクセス可能なことを確認しているが、今後時間の経過と共に各サイトにて整理整頓されアクセス出来なくなる場合があるので予めご了承いただきたい。

1. フィッシング関連

- 「サイバー詐欺師を目指すなら...」--フィッシング用ツールキット出回る
  （2004 年 08 月 20 日付）
  http://japan.cnet.com/svc/nlt2?id=20070635
  ・「フィッシング」詐欺で使われる、偽のウェブサイト構築に必要なグラフィックやコード、テキストを含む「構築キット」が、一部のウェブサイトから無料でダウンロードできるようになっている。

- 隣のセキュリティ事件～フィッシング（1）（2004 年 09 月 08 日付）
  http://nikkeibp.jp/wcs/leaf/CID/onair/biztech/rep02/330106

- どうする？ フィッシング詐欺対策--送信者認証技術の重要性を語るマイクロソフト
  （2004 年 09 月 08 日付）
  http://japan.cnet.com/svc/nlt2?id=20072464
  ・フィッシング詐欺が横行するなか、マイクロソフトは送信者認証技術の重要性を訴えている。フィッシングの実害はスパムやウイルスよりはるかに大きいからだ。

- フィッシング詐欺防止のためニュースレターに電子署名を（2004 年 09 月 16 日付）
  http://it.nikkei.co.jp/it/manage/column.cfm?i=20040916cn000cn

- 「米国のフィッシング被害額は 5 億ドル」--米調査（2004 年 09 月 30 日付）
  http://japan.cnet.com/svc/nlt2?id=20074891
  ・ある調査結果によると、米国の消費者は「フィッシング」として知られるオンライン詐欺で総額 5 億ドルの被害に遭っているという。

- セキュリティ専門家 3 氏、フィッシング詐欺の国内上陸本格化を警告
  ～WPC EXPO フォーラム 2004 コンピュータ・ネットワークトラック
  （2004 年 10 月 25 日付）
  http://enterprise.watch.impress.co.jp/cda/topic/2004/10/25/3692.html

- イーバンク銀行の入金通知メールを偽装するフィッシング詐欺メール発生
  （2004 年 11 月 01 日付）
  http://internet.watch.impress.co.jp/cda/news/2004/11/01/5222.html

- ウイルスの手法を利用するフィッシャーたち（電子メールを開くだけでも危険）
  （2004 年 11 月 08 日付）
  http://www.itmedia.co.jp/enterprise/articles/0411/08/news060.html

- “巧妙な”フィッシングが出現，ポップアップでアドレス・バーを偽装
  （2004 年 11 月 10 日付）
  http://itpro.nikkeibp.co.jp/free/ITPro/NEWS/20041110/152412/

- Visa、フィッシングメール事件の調査中間報告を発表（2004 年 11 月 12 日付）
  http://japan.cnet.com/news/sec/story/0,2000050480,20075732,00.htm?tag=nl

- メールを開くだけで偽サイトに誘導～新たなフィッシング詐欺メール発見
  （2004 年 11 月 16 日付）
  http://internet.watch.impress.co.jp/cda/news/2004/11/16/5420.html

- マイクロソフト、フィッシング対策で二要素認証を提案（2004 年 11 月 18 日付）
  http://japan.cnet.com/news/sec/story/0,2000050480,20075908,00.htm?tag=nl

- フィッシング詐欺対策、3 割は「どうすればよいか分からない」――シマンテック調査
  （2004 年 11 月 19 日付）
  http://www.itmedia.co.jp/enterprise/articles/0411/19/news093.html

- フィッシング詐欺に騙されないための心構えも重要～シマンテック調査
  （2004 年 11 月 19 日付）
  http://internet.watch.impress.co.jp/cda/news/2004/11/19/5489.html

- 迫り来るフィッシングのわな（2004 年 11 月 22 日付）
  http://japan.cnet.com/special/story/0,2000050158,20075963-2,00.htm

- セキュアブレイン、フィッシングサイトを“赤信号”で警告する「PhishWall」
  （2004 年 11 月 24 日付）
  http://internet.watch.impress.co.jp/cda/news/2004/11/24/5506.html

- フィッシング詐欺、10 月は偽造サイトが倍増―APWG 調査（2004 年 11 月 26 日付）
  http://enterprise.watch.impress.co.jp/cda/foreign/2004/11/26/3987.html

- 武富士、フィッシング対策で全社員のメールに電子署名を付加（2004 年 11 月 29 日付）
  http://japan.cnet.com/news/sec/story/0,2000050480,20076884,00.htm?tag=nl

- 怪しいサイトを嗅ぎ分けるブラウザが登場（2004 年 12 月 02 日付）
  http://japan.cnet.com/news/sec/story/0,2000050480,20077603,00.htm?tag=nl

- 海外で深刻化するフィッシング詐欺、日本でも予防が急務（2004 年 12 月 02 日付）
  http://internet.watch.impress.co.jp/cda/event/2004/12/02/5633.html

- フィッシングの新手口が出現--グーグルなどの検索ユーザーを狙う（2004 年 12 月 02 日付）
  http://japan.cnet.com/news/sec/story/0,2000050480,20077723,00.htm?tag=nl

- 経産相「フィッシング詐欺対策の連絡会議を設置」（2004 年 12 月 03 日付）
  http://www.nikkei.co.jp/news/keizai/20041203AT1F0300B03122004.html

- 「2004 年はフィッシング詐欺元年」英 MessageLabs が調査報告（2004 年 12 月 07 日付）
  http://internet.watch.impress.co.jp/cda/news/2004/12/07/5677.html

- 2004 年下半期にフィッシングメール急増、スパム・ウイルスも減らず
  （2004 年 12 月 07 日付）
  http://pcweb.mycom.co.jp/news/2004/12/07/101.html

- 今年はフィッシング詐欺激増の年、来年も要警戒（2004 年 12 月 07 日付）
  http://www.itmedia.co.jp/news/articles/0412/07/news008.html

- 偽ショッピングサイトで誘う、フィッシング詐欺の新手口（2004 年 12 月 07 日付）
  http://hotwired.goo.ne.jp/news/business/story/20041207107.html

- フィッシング詐欺メール、米で急増――米民間企業調査（2004 年 12 月 08 日付）
  http://it.nikkei.co.jp/it/newssp/crime.cfm?i=2004120806753wg

- フィッシング対策などを掲載した「Yahoo!セキュリティセンター」オープン
  （2004 年 12 月 08 日付）
  http://internet.watch.impress.co.jp/cda/news/2004/12/08/5710.html

- 経産省がフィッシング対策会議、Yahoo！や楽天も参加（2004 年 12 月 10 日付）
  http://www.itmedia.co.jp/enterprise/articles/0412/10/news071.html

- フィッシングサイト数：11 月は前月比 29%増（2004 年 12 月 16 日付）
  http://japan.cnet.com/news/sec/story/0,2000050480,20079730,00.htm?tag=nl

- 英ソフォス CEO、日本の CIO に対してフィッシングへの早期対策を呼びかけ
  （2004 年 12 月 14 日付）
  http://www.ciojp.com/contents/?id=00001971;t=0&iclips

- IE にフィッシングの危険--ActiveX に問題（2004 年 12 月 20 日付）
  http://japan.cnet.com/news/sec/story/0,2000050480,20079758,00.htm?tag=nl

- いわゆる「フィッシング」対策の推進について・フィッシング１１０番
  （2004 年 12 月 24 日付）
  http://www.npa.go.jp/cyber/policy/phishing/main.htm
  http://www.npa.go.jp/cyber/policy/phishing/phishing110.htm

- eBay、フィッシング詐欺を防ぐ新しいメッセージサービスを導入（2005 年 01 月 05 日付）
  http://japan.cnet.com/news/sec/story/0,2000050480,20079906,00.htm?tag=nl

- Firefox に脆弱性--フィッシングのおそれあり（2005 年 01 月 11 日付）
  http://japan.cnet.com/news/sec/story/0,2000050480,20079959,00.htm?tag=nl

- 巧妙に、見破りにくくなるフィッシング詐欺（2005 年 01 月 20 日付）
  http://www.itmedia.co.jp/enterprise/articles/0501/20/news031.html

- 金融機関を名乗るフィッシング詐欺が 85%--12 月調査結果（2005 年 01 月 21 日付）
  http://japan.cnet.com/news/sec/story/0,2000050480,20080199,00.htm?tag=nl

- フィッシング被害の増加傾向止まらず～Anti-Phishing Working Group 報告
  （2005 年 01 月 24 日付）
  http://internet.watch.impress.co.jp/cda/news/2005/01/24/6169.html

- フィッシング詐欺はユーザーも気づかないステルス型へ（2005 年 01 月 27 日付）
  http://internet.watch.impress.co.jp/cda/news/2005/01/28/6269.html

- ビザ・インターナショナル「フィッシングサイトは 24 時間以内に削除」
  （2005 年 01 月 27 日付）
  http://internet.watch.impress.co.jp/cda/news/2005/01/28/6251.html

2. スパイウェア、アドウェア関連

- スパイウェアの地獄めぐりへようこそ（2004 年 09 月 01 日付）
  http://japan.cnet.com/svc/nlt2?id=20071404
  ・スパイウェアによる侵入の程度と攻撃性はさまざまだ。ここではスパイウェアと称されるプログラムの生い立ちを説明し、これらを 9 つのタイプに分類する。

- 隣のネット・セキュリティ事件～スパイウェア（1）（2004 年 10 月 25 日付）
  http://nikkeibp.jp/wcs/leaf/CID/onair/biztech/rep02/338436

- スパイウェア：パソコン 1 台に平均 93 件も潜入（2004 年 10 月 26 日付）
  http://hotwired.goo.ne.jp/news/technology/story/20041026303.html

- もはや人ごとではないスパイウェアの脅威（2004 年 10 月 27 日付）
  http://www.atmarkit.co.jp/fwin2k/insiderseye/20041027spyware/spyware.html

- 対策の進むスパイウェアとアドウェア（2004 年 11 月 5 日付）
  http://www.atmarkit.co.jp/fsecurity/rensai/trend02/trend01.html

- MS のスパイウェア対策ソフト β リリース間近、Exchange の強化はずれ込み
  （2005 年 01 月 06 日付）
  http://www.itmedia.co.jp/news/articles/0501/06/news017.html

- MS のスパイウェア対策ソフト β 版公開、ウイルス削除ツールも月例更新へ
  （2005 年 01 月 07 日付）
  http://www.itmedia.co.jp/news/articles/0501/07/news008.html

- スパイウェア対策法案が復活（2005 年 01 月 07 日付）
  http://www.itmedia.co.jp/news/articles/0501/07/news076.html

- 検証！　MS のスパイウェア対策ツール「Microsoft AntiSpyware」
  （2005 年 01 月 17 日付）
  http://www.itmedia.co.jp/news/articles/0501/17/news038.html

- ［WSJ］ MS の無料スパイウェア対策ソフトを推奨できない理由（2005 年 01 月 17 日付）
  http://www.itmedia.co.jp/news/articles/0501/17/news085.html

- 2005 年最大の脅威はスパイウェア、全米 IT 担当者の 66%が指摘（2005 年 01 月 25 日付）
  http://japan.internet.com/wmnews/20050125/4.html

- SPY ACT、米上院へ再び - IT 業界からの賛成も取り付け万全か?（2005 年 01 月 28 日付）
  http://pcweb.mycom.co.jp/news/2005/01/28/011.html

3. ホームネットワーク、ネット家電関連

- 都市内 Wi-Fi ホットゾーンは公共サービスとなるのか（2004 年 09 月 08 日付）
  http://blog.japan.cnet.com/watanabe/archives/001601.html?tag=nl
  ・Philadelphia で町中を無線 LAN のホットスポットで覆ってしまおうというプロジェクトが動いている。ここまで来るとスポットではなくゾーン、ホットゾーンと表現するらしい。

- 独立宣言、憲法に続くフィラデルフィア発のアイデア（2004 年 09 月 09 日付）
  http://blog.japan.cnet.com/lessig/archives/001606.html?tag=nl
  ・フィラデルフィアはすべての街灯に WiFi ボックスを取り付け、市全域をカバーすることを検討している。このアイデアですばらしいと思うのは、街灯との結びつきがこうしたリソースの受けとめ方について連想させることだ。

- ネット家電に潜むセキュリティホール（2004 年 09 月 24 日付）
  http://www.itmedia.co.jp/anchordesk/articles/0409/24/news025.html

- ホームネットワークを実現、未来のモデルルームが登場──16 社による企画展示「みらいのいえ」（2004 年 10 月 21 日付）
  http://it.nikkei.co.jp/it/sp/wpcexpo2004.cfm?i=20041021yt000yt

- 求む、家庭向けのシンプルなセキュリティサービス（2004 年 10 月 27 日付）
  http://japan.cnet.com/column/pers/story/0,2000050150,20075380,00.htm

- WPA の脆弱性を悪用するツール公開（無線 LAN も危険）（2004 年 11 月 09 日付）
  http://www.itmedia.co.jp/enterprise/articles/0411/09/news024.html

- 実はこんなに奥の深い「ファイアウォール」（2004 年 11 月 19 日付）
  http://www.itmedia.co.jp/enterprise/articles/0411/19/news002_4.html

- 情報家電ネットワークと電波利用料--総務省は「産業界の論議待ち」
  （2004 年 12 月 17 日付）
  http://pcweb.mycom.co.jp/news/2004/12/17/001.html

- 松下／三菱／ソニー、電力線通信のアライアンス設立（2005 年 01 月 06 日付）
  http://www.itmedia.co.jp/lifestyle/articles/0501/06/news025.html

- 米国の家庭内ネットワーク、無線 LAN がイーサネットを上回る（2005 年 01 月 21 日付）
  http://www.itmedia.co.jp/news/articles/0501/21/news021.html

4. ウイルス、ワーム、スパム関連

- ウイルス・ワームのセキュリティ対策は万全に（2004 年 09 月 07 日付）
  http://blog.japan.cnet.com/kenn/archives/001595.html?tag=nl
  ・IPA/ISEC（独立行政法人 情報処理推進機構 セキュリティセンター）によると、2004 年 1 月～6 月の半年間のウイルス届け出件数は 21,957 件と、すでに 2003 年の累計である 17,425 件を大幅に突破してしまった。

- 電子メール ID を使って偽装するスパマー--米調査で明らかに（2004 年 09 月 09 日付）
  http://japan.cnet.com/svc/nlt2?id=20072743
  ・米企業の調査によると、ジャンクメッセージの送信元の 6 分の 1 近くが「SenderPolicy Framework（SPF）」と呼ばれるプロトコルを使い、メッセージ中の電子メールアドレスが本物であると認証しているという。

- 「JPEG 画像ウイルスがまもなく出現」--セキュリティ研究者らが警戒
  （2004 年 09 月 29 日付）
  http://japan.cnet.com/svc/nlt2?id=20074838
  ・Windows ソフトの JPEG ファイル処理方法に見つかった欠陥を悪用するトロイの木馬について、専門家らはそれ自体が感染を拡大することはないとしながら、こうしたコードがすぐにウイルスになり得るとして警戒を呼びかけている。

- JPEG ファイルがトロイの木馬に--Windows ソフトの欠陥を悪用する画像発見
  （2004 年 09 月 29 日付）
  http://japan.cnet.com/svc/nlt2?id=20074837
  ・MS 製ソフトの画像ファイル処理方法にある欠陥を悪用する 2 つの JPEG ファイルが見つかった。Windows ユーザーはこうした画像を開くだけで、悪質なプログラムに感染してしまうという。

- JPEG 画像ウイルス、通常の対策ソフトでは手に負えない可能性も
  （2004 年 09 月 30 日付）
  http://japan.cnet.com/svc/nlt2?id=20074872
  ・ウイルス対策ソフトは、Windows の脆弱性を利用した JPEG ファイルによる攻撃から企業ネットワークを守るのには不向きかもしれないと、あるセキュリティ専門家が指摘している。

- JPEG 画像ウイルス、AOL のインスタントメッセージで感染（2004 年 10 月 01 日付）
  http://japan.cnet.com/svc/nlt2?id=20074921

- 銀行で待ち伏せ--オンラインバンク利用者を狙うトロイの木馬が出現
  （2004 年 11 月 12 日付）
  http://japan.cnet.com/news/media/story/0,2000047715,20075725,00.htm?tag=nl

- 携帯電話アプリを破壊する Skulls プログラム--Symbian OS 搭載端末に照準
  （2004 年 11 月 22 日付）
  http://japan.cnet.com/news/sec/story/0,2000050480,20076008,00.htm?tag=nl

- クリスマスワームがまた出現（2004 年 12 月 17 日付）
  http://www.itmedia.co.jp/enterprise/articles/0412/17/news011.html

- PHP のコード問題を突く Santy ワームの亜種が出現（2004 年 12 月 28 日付）
  http://www.itmedia.co.jp/news/articles/0412/28/news006.html

- Santy ワームの亜種出現、今度は AOL と Yahoo!で標的検索（2004 年 12 月 28 日付）
  http://www.itmedia.co.jp/news/articles/0412/28/news007.html

- AOL 標的のスパムメールが初の大幅減（2004 年 12 月 28 日付）
  http://www.itmedia.co.jp/news/articles/0412/28/news009.html

- スパムメールの 4 割強は米国が発信源（2004 年 12 月 28 日付）
  http://www.itmedia.co.jp/news/articles/0412/28/news012.html

- XP SP2 に感染するトロイの木馬（2004 年 12 月 28 日付）
  http://www.itmedia.co.jp/news/articles/0412/28/news014.html

- 携帯ワームの Cabir に複数の亜種、弱点解消で急拡散の恐れ（2004 年 12 月 29 日付）
  http://www.itmedia.co.jp/news/articles/0412/29/news005.html

- Santy 感染サイトに「パッチを当てる」ワーム（2005 年 01 月 01 日付）
  http://www.itmedia.co.jp/news/articles/0501/01/news003.html

- スマトラ沖地震便乗の詐欺サイトやスパムが横行――FBI が注意勧告
  （2005 年 01 月 07 日付）
  http://www.itmedia.co.jp/news/articles/0501/07/news010.html

- 「Skulls」の新亜種は Flash プレーヤーを装って携帯電話に感染（2005 年 01 月 08 日付）
  http://www.itmedia.co.jp/news/articles/0501/08/news010.html

- 携帯電話を狙う新たなウイルス登場（2005 年 01 月 11 日付）
  http://japan.cnet.com/news/sec/story/0,2000050480,20079974,00.htm?tag=nl

- FTC、ポルノメール送信のスパムネットワーク摘発（2005 年 01 月 12 日付）
  http://www.itmedia.co.jp/news/articles/0501/12/news012.html

- 裸体で「新年おめでとう」と告げるワームに注意（2005 年 01 月 12 日付）
  http://www.itmedia.co.jp/news/articles/0501/12/news020.html

- Windows Media DRM を悪用したトロイの木馬が登場（2005 年 01 月 12 日付）
  http://www.itmedia.co.jp/news/articles/0501/12/news025.html

- MS がウイルス駆除ツールを公開、定義更新は Windows Update で
  （2005 年 01 月 12 日付）
  http://www.itmedia.co.jp/news/articles/0501/12/news046.html

- 津波支援の呼びかけを装うマスメール型ワーム（2005 年 01 月 18 日付）
  http://www.itmedia.co.jp/news/articles/0501/18/news009.html

- 有害コンテンツ削除ツールを装うワーム「Baba-C」（2005 年 01 月 19 日付）
  http://www.itmedia.co.jp/news/articles/0501/19/news018.html

- ウイルス対策に近道なし、基本は一にも二にも「教育」（2005 年 01 月 20 日付）
  http://www.itmedia.co.jp/enterprise/articles/0501/20/news093.html

- アダルトコンテンツ削除ツールを装う「Baba ワーム」出現（2005 年 01 月 21 日付）
  http://japan.cnet.com/news/sec/story/0,2000050480,20080193,00.htm?tag=nl

- CNN ヘッドラインを装うウイルス発生（2005 年 01 月 21 日付）
  http://www.itmedia.co.jp/enterprise/articles/0501/21/news055.html

- MSN Messenger で拡散するワームが出現（2005 年 01 月 21 日付）
  http://www.itmedia.co.jp/enterprise/articles/0501/21/news011.html

- ウイルス対策ソフトの試用版を装うトロイの木馬が流通（2005 年 01 月 25 日付）
  http://internet.watch.impress.co.jp/cda/news/2005/01/25/6187.html

- Bagle ウイルスの新亜種登場--「ウイルスの季節」到来の前触れか（2005 年 01 月 28 日付）
  http://japan.cnet.com/news/sec/story/0,2000050480,20080323,00.htm?tag=nl

5. クロスサイトスクリプティング関連

- クロスサイトスクリプティング対策の基本（2004 年 11 月 09 日付）
  http://www.atmarkit.co.jp/fsecurity/special/30xss/xss01.html

- IE にクロスサイトスクリプティングを許す脆弱性、SP2 でも防げず
  （2004 年 12 月 17 日付）
  http://www.itmedia.co.jp/enterprise/articles/0412/17/news009.html

6. その他

- 8 割以上の消費者が、クレジットカードや口座番号の Web 入力に抵抗感
  （2004 年 11 月 08 日付）
  http://www.nri.co.jp/news/2004/041108.html

- ユーザーはインターネットセキュリティに混乱している（2004 年 11 月 10 日付）
  http://www.itmedia.co.jp/enterprise/articles/0411/10/news053.html

- マイクロソフト、嘉悦女子高等学校でセキュリティ公開授業を実施
  （2004 年 11 月 16 日付）
  http://ascii24.com/news/i/topi/article/2004/11/16/652559-000.html

- シマンテック、「セキュリティ対策ソフトだけでオンライン詐欺は防げない」
  （2004 年 11 月 19 日付）
  http://japan.cnet.com/news/sec/story/0,2000050480,20075966,00.htm?tag=nl

- ニフティ、ネット・セキュリティの重要性を理解する特設サイト（2004 年 11 月 19 日付）
  http://japan.cnet.com/news/sec/story/0,2000050480,20075923,00.htm?tag=nl

- 詐欺に注意、安全なオンラインショッピングのための助言（2004 年 11 月 29 日付）
  http://japan.internet.com/ecnews/20041129/12.html

- 2004 年のセキュリティ事情を回顧する（2004 年 12 月 07 日付）
  http://it.nikkei.co.jp/it/column/njh.cfm?i=20041206s2000s2

- 情報主体の安心できるセキュリティを宇治市の事例から考える（2004 年 12 月 17 日付）
  http://japan.cnet.com/news/sec/story/0,2000050480,20079748,00.htm?tag=nl

- HTTP 暗号化通信のパラドックス　安心が情報漏えいの穴になる不思議
  （2004 年 12 月 18 日付）
  http://www.atmarkit.co.jp/fsecurity/special/52ssl/ssl.html

- セキュリティ各社、Windows の脆弱性に警告（2004 年 12 月 28 日付）
  http://www.itmedia.co.jp/news/articles/0412/28/news036.html

- McAfee が 2004 年の脅威ワースト 10 発表、2005 年も攻撃増加を予想
  （2005 年 01 月 05 日付）
  http://www.itmedia.co.jp/news/articles/0501/05/news010.html

- McAfee、情報流出対策ツールの新版リリース（2005 年 01 月 11 日付）
  http://www.itmedia.co.jp/news/articles/0501/11/news007.html

- 10 年以内に「壊滅的なネット攻撃」専門家が予想（2005 年 01 月 11 日付）
  http://www.itmedia.co.jp/news/articles/0501/11/news010.html

- 先進国としての情報セキュリティ対策のあるべき姿を見る（2005 年 01 月 12 日付）
  http://japan.cnet.com/column/sec/story/0,2000051108,20079964,00.htm?tag=nl

- オンライン決済サービス PayPal の問題点（2005 年 01 月 20 日付）
  http://www.itmedia.co.jp/news/articles/0501/20/news057.html
- 情報セキュリティを取り巻く各種制度（2005 年 01 月 20 日付）
  http://www.itmedia.co.jp/enterprise/articles/0501/20/news008.html

- 経産省が迷惑メールの違法性認定、民間の取り締まり支援（2005 年 01 月 21 日付）
  http://www.itmedia.co.jp/news/articles/0501/21/news067.html

- 脆弱性検査ツールを知る（2005 年 01 月 21 日付）
  http://www.itmedia.co.jp/enterprise/articles/0501/24/news001.html

- 詐欺やサイバーテロ、情報漏洩に対処するために国が行うべきこと
  （2005 年 01 月 28 日付）
  http://japan.cnet.com/column/sec/story/0,2000051108,20079965,00.htm?tag=nl

- 放送・通信・家電・融合「悪魔の辞典 2005」（2005 年 01 月 28 日付）
  http://japan.cnet.com/column/mori/story/0,2000050579,20080300,00.htm?tag=nl

執筆者リスト

くらしのネット化セキュリティSWG執筆者リスト

1	雨宮　寿利 （リーダ）	株式会社ＮＴＴ･カードソリューション	カードビジネス事業部 カードシステム部門
2	関口　まさみ	社団法人全国消費生活相談員協会	消費生活専門相談員
3	原田　由里	財団法人日本消費者協会	消費生活コンサルタント
4	宮川　成生	社団法人 前払式証票発行協会	企画調査部
5	山本　英朗	日本電信電話株式会社	サービスインテグレーション基盤研究所 ＩＣカードサービス推進プロジェクト
6	本城　啓史	株式会社ＮＴＴデータ	技術開発本部
7	小林　一清	富士通株式会社	ＧＬＯＶＩＡ事業本部ＣＲＭビジネス部
8	合原　英次郎	松下電器産業株式会社	東京支社　渉外グループ
9	古屋　信幸	ユーシーカード株式会社	市場開発部

事務局

S1	太細　孝	電子商取引推進協議会	ネットセキュリティWG
S2	田仲　正幸	電子商取引推進協議会	ネットセキュリティWG

平成１６年度　経済産業省　受託業務
不正アクセス行為等対策業務
くらしのネット化に伴うセキュリティ課題の調査研究報告書
平成　１７年　２月　発行

発行所　　財団法人　日本情報処理開発協会
電子商取引推進センター
東京都港区芝公園３丁目５番８号
機械振興会館　３階
TEL：０３（３４３６）７５００
印刷所　　東芝ドキュメンツ株式会社
東京都港区芝浦１－１－１
TEL：０３（３４５７）４０５６

この資料は再生紙を使用しています。