解説

電子商取引における情報漏洩に起因する脅威

家木　俊温

インターネットを活用した電子商取引が急速に普及しつつある．当初，ネットワークなどからのクレジットカード情報，氏名，住所などの個人情報の漏洩，およびこれらを悪用した不正取引などの危険性が指摘されてきた．しかし，現状ではクレジットカード番号を送信するクレジット決済は普及しており，大きな問題とはなっていない．また，他の個人情報の漏洩に基づく被害も多発していないように見える．それでは，本当に情報漏洩は起きていないのだろうか．また，クレジット決済は将来とも安全なのだろうか．本論文では，現状問題となっていない原因，および，将来脅威が発生しうる可能性について考察した．その結果，情報漏洩は起きており，情報漏洩が実社会でのカード犯罪の増加を誘発しており，将来，ネット上のクレジット決済などにも脅威が及ぶ可能性があるとの結論に至った．

また，脅威を防ぐ対策についても考察した．

キーワード：電子商取引，情報漏えい，クレジット決済，偽造カード，個人情報

1　はじめに

インターネットを活用した電子商取引は，ネットワーク上の仮想店舗に対して居ながらにして商品の選択，購入，決済ができる．この利便性から，1990 年代からアメリカで急速に普及し始め，最近は日本でも普及しつつある．しかし，ネットワーク上を流れるクレジットカード番号，氏名，住所などの個人情報が盗み読みされること，およびそれに起因する不正取引，プライバシーの侵害，誹謗中傷などの危険性が指摘された．そのため，ネットワークを保護するための暗号技術活用の研究が盛んになり，暗号通信プロトコルＳＳＬなどが開発された．この結果，ネットワーク上を流れる情報は暗号化されることとなり，個人情報の安全性が飛躍的に向上したと一般には考えられている．

しかし，本当にこれらの情報は安全なのであろうか．これらの情報がネットワーク上を流れるのはほんの一瞬であって，その後は店舗のデータベースに長期間保存される．そこは，本当に安全なのであろうか．また，ネットワーク上の不正取引が多発していない現状から，情報漏えいはおきていないように見えるが本当であろうか．これらの点に関して，以下に考察する．

2　情報漏えいの危険性

ネットワーク上の個人情報の流れの概略を図１に示す．情報は，ネットワーク上を流れた後，仮想店舗に到達し，店舗内のデータベースに保管される．個人情報には，次のようなものが考えられる．

①クレジットカード番号

②基本情報：氏名，住所，年齢，電話番号，メールアドレス，職業，年収など

③購入履歴：購入商品，購入時期など

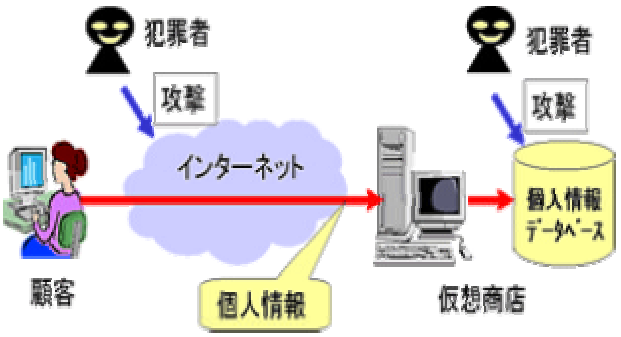

図１　個人情報の流れ

犯罪者が狙うのは，ネットワーク上の情報か，データベースに保管された情報である．それぞれの場合の危険性につき以下に考察する．

2．1　ネットワーク上の情報

電子商取引の際にネットワーク上を流れる情報を暗号化によって保護する技術としてＳＳＬ(Secure Socket Layer)がある．ＳＳＬでは，用いられる暗号が強力であるうえに，暗号鍵を取引のたびに新しいものに更新するため，解読はきわめて困難といわれている．また，解読できたとしても一人分の個人情報などが盗めるだけであり，これによって犯罪者が大きな利益を得ることは困難である．

IEKI Toshiharu
武蔵工業大学環境情報学部教授

すなわち，犯罪者にとって，ネットワーク上の情報を取得，解読することは，苦労の多い割には益の少ない手段である．したがって，犯罪者がネット上の情報を狙うとは考えにくく，これによって消費者が被害を受ける危険性は低い．実際，ネットワーク上を流れるカード番号などの盗み読み事件が大きな問題となったことはない．

２．２　データベース上の情報

データベースには，非常に多くの顧客の個人情報が格納されている．犯罪者にとって，きわめて魅力的なターゲットである．犯罪者が情報を盗み出す手口としては，以下の３通りが考えられる．

①仮想店舗に侵入してデータベースにアクセスし，データを盗み出す
②コンピュータウイルス，ワーム，トロイの木馬など不正プログラムを送りこみ盗み出す
③内部者と結託して盗み出す

①は，現状大きな問題となっており，以下の事例がアメリカ合衆国で報告されている．

「ロシア圏のハッカーが，オンライン音楽ストアの CD Universe，それに恐らくはほかのオンラインショップ数社から顧客のクレジットカード番号を盗み出すことに成功した．その結果，ほとんどのクレジットカード所有者は記憶にない2000 ドル以下の請求を付き付けられることになった．ただ，米国ではカードが不正利用された場合，消費者に支払い義務が生じるのは最高50 ドルだけ．不正に盗み出されたカード番号での買い物を許した小売業者がその分の埋め合わせをしなければならない．」というものである．これは，氷山の一角であり，今後さらに増加するものと思われる．

手段①を防ぐ方法としては，ファイアウォールが考えられるが，仮想商店の場合は，不特定多数の消費者のアクセスを許可せねばならず，十分な効果が得られていない．また，最近の傾向としては，手段②を用いて情報を盗み出す，あるいは，②によって侵入用のセキュリティホールを作ってから①を実行する，などの方法もとられているようである．手段②の対策としては，ウイルス対策ソフトが考えられるが，何万種類もあるうえに常に新種が誕生している不正プログラムを防ぐのは困難である．結局①②を防ぐための方法としては，「データベースのデータを暗号化する」という方法がもっとも有効と思われる．こうすることによって，例え情報を盗まれても犯罪者による解読が困難であり，個人情報の中身を知られずにすむからである．

しかし，手口③を防ぐことは，さらに困難である．内部者は業務を行うことから暗号を解読することができるはずである．また，内部者にはじめから悪意はなくても，以下の理由から犯罪に協力する可能性は高いと考えられる．

・外部の犯罪者から脅迫や金銭授受を受ける．これらの情報の授受には，数万円から数十万円が支払われるとも言われている．
・情報はコピーをすることで簡単に盗め，元の情報がなくならないため，犯罪の事実，痕跡を見つけることが困難である．すなわち，現金・宝石などの物を盗むのに比べるとはるかにばれにくい．

実際，セキュリティ犯罪の 80%は内部犯罪といわれている．このことからも，内部犯罪を防止することは不可能と思われる．

以上の考察から，カード番号などの個人情報は，現状すでに漏洩しており，今後もこれを防ぐことは困難であると考えざるを得ない．

３　クレジットカード番号の漏洩による脅威と対策

３．１　現状の脅威

先に挙げた事例が，電子商取引における盗んだカード番号を利用したなりすまし購入事例があまり起きていない理由を示している．すなわち，犯罪者は盗んだカード番号で多くのクレジットカードを偽造し，このカードで買い物をし，換金しているのである．

このような状況が起きているのは，カード偽造を行うほうが犯罪者にとって有利だからであり，その理由として次の３点が考えられる．

①現状，電子商取引で購入できる商品は限定されているが，実店舗で偽造したクレジットカードを用いれば，好きな商品が入手できる．
②電子商取引では，購入後商品配達までに時間がかかるが，実店舗でのショッピングの場合，すぐに商品を入手できる．
③電子商取引の場合，配達先から身元が判明するのを防ぐため，専用の配達先を確保する必要がある．

カード偽造事件が急増している現状から，アメリカでは電子商取引でのクレジット決済の安全性が大きな問題となりつつある．しかし，日本では大きな問題と捉えられていないのはなぜだろうか．これは，日本とアメリカの偽造カード被害の支払いの実態の違いによるものと思われる．

・アメリカでは，偽造カード被害が発生した場合，通常小売業者と消費者が支払い義務
を負っている．
・日本では，偽造カード被害が発生した場合，通常カード会社が負担している．これは，消費者に責任があるわけではないとの考えによる．また，消費者に責任を負わせると，カード利用が減少することを恐れているからでもある．

すなわち，日本ではカード番号を盗まれても，偽造カードによる犯行の場合は消費者が責任を取らなくてすむ．言い換えれば，現状の日本におけるクレジット決済は，消費者にとってはかなり安全な行為となっているのである．しかし，カード会社にとっては大きな問題であることから，いつまでも今の状態が続くとは思われない．

３．２　今後の展開

カード番号の漏洩は，日本の消費者にとって，今後も大きな脅威とならないのであろうか．この問題を考えるため，次の２点を取り上げることとしたい．

（１）制度・慣習の変化

先に述べたように，日本での偽造カード犯罪の被害負担は，現状カード会社が負っている．しかし，アメリカでは，消費者にも支払い責任がある．将来日本においても消費者が被害負担を負う可能性は十分にあると思われる．図２は，日本における偽造カードの被害額推移を示したものである．偽造カードの被害は 1999 年から急激な増加傾向にある．これは，日本における電子商取引が普及し始めた時期ともほぼ一致している．2000 年には，被害額が 140 億円にも達しており，カード会社の経営を大きく圧迫しているはずである．もし，このまま偽造カードに対する有効な対策が発見できない場合，「偽造カードに対する損害負担を消費者にも負ってもらう」という対策をカード会社がとることは十分に考えられる．

こうなった場合，消費者のとる対策は，「クレジット決済をやめて現金着払いなどの他の方法をとる」ことであるが，それでは不完全である．なぜなら，カード番号は過去の取引によって漏洩しており，偽造カードによる実店舗での被害を防げないからである．大切なことは，「カードを再発行して新たなカード番号をもらう」ことである．

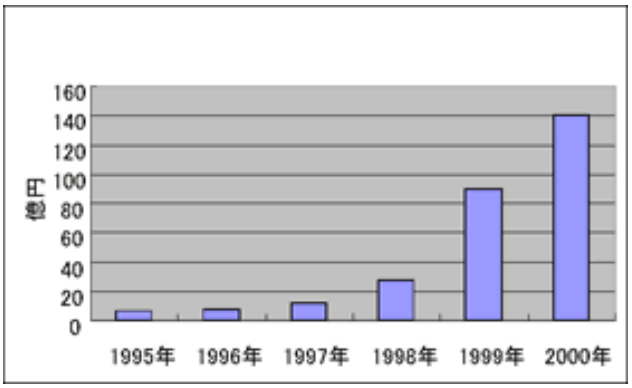

図２　偽造カードの被害額の推移

（２）ＩＣカードの導入

もう１つ考慮すべき点は，クレジットカードがＩＣカードに切り替わるということである．例えば，「クレジットカード会社最大手のビザ・インターナショナルは，クレジットカードのＩＣカード化への移行を本格化させる」と発表している．ＩＣカードが磁気カードに比べて偽造しにくい理由としては，以下の点が考えられる．

①ＩＣカードに使用されるＩＣは，特殊なワンチップマイクロコンピュータであり，製造会社が限られること，およびこれらの会社がセキュリティ管理をしていることから，不正入手がしにくい．

②ＩＣのカードへの装着，およびＩＣへのデータの書き込みには，特殊な装置が必要である．この装置は，磁気テープへのデータの書き込み装置に比べると世の中に広まっておらず，かつ高度な製造技術を有するため，犯罪者が入手しにくい．

③ＩＣカード内には相手認証用の暗号プログラムがあり，正しい認証キーを知るもの意外のデータの不正書き込みを防止している．したがって，カード番号などの不正書き込みを行うためには，正規のカード発行者が有している秘密の認証キーを入手する必要がある．

以上を考慮すると，ＩＣカードの偽造は現行の磁気カードの偽造に比べてはるかに困難と考えられる．ただ，犯罪組織の中には，資金力，技術力，豊富な人脈を持った組織もある．磁気カードの偽造を容易に行えるようになった過去の経緯からして，やがてはＩＣカードを偽造する犯罪組織が登場するであろう．しかし，ＩＣカード導入後しばらくは偽造は大幅に減少すると思われる．

それでは，消費者にとって脅威は減少するのであろうか．この点に関しては，私は別の脅威が生じると考えている．それは，電子商取引のなりすまし購入である．前述したように，現在はカード偽造が容易であるため，なりすましは大きな問題となっていない．しかし，カード偽造が困難になれば，犯罪者は電子商取引でのなりすましによる不正購入を行うと思われる．この場合の対策としては，電子商取引におけるクレジット決済を止めるのが良いと考えられる．

３．３　対策

しかし，上述した問題に対しては，有効な対策がある．その内容は以下のとおりである．

（１）現行の方法

現行のクレジット決済は，仮想店舗，実店舗を問わず，クレジットカード番号でカードおよび所有者の真性確認を行っている．提出されたカード番号を，店舗またはカード会社のデータベースに記録したカード番号と照合して一致すれば本物としているのである．しかし，この方法では，犯罪者がカード上，およびデータベースに記録されたカード番号を読み取ることが可能である．そして，読み取った情報をもとに，多くの偽造カードを作成しているのである．

（2）新たな方法

この方法では，上記の問題を解決するため，電子署名技術とＩＣカードを用いる．電子署名の本人確認機能およびその安全性については，世の中で認められている．まず，カード会社はＩＣカード内の読み出し不可領域に署名用の秘密鍵を格納する．そして，署名の正当性を確認するための公開鍵を作成し公開する．公開鍵には，本物であることを証明する認証局（Certification Authority：ＣＡ）の電子署名をしてもらい，公開する．カードが本物であることを証明する手順は，下記のとおりである（図３参照）．

①店舗は，取引情報またはそれの要約（メッセーダイジェスト）をＩＣカードに送る．

②ＩＣカードは，受けとった情報を秘密鍵で暗号化して電子署名を作成し，これを店舗に返す．

③店舗は，受け取った電子署名を公開鍵で復号し，取引情報または要約と比較する．一致すれば，カードおよび所有者を本物とみなし取引を承認する．なぜならば，公開鍵で復号して元に戻るのは，正しい秘密鍵で暗号化が行われたからである．

この方法では，検証用の情報すなわち公開鍵ははじめから公開されている．しかし，犯罪者がカード番号や公開鍵を盗んでもカード偽造や，なりすまし購入をすることはできない．なぜならば，電子署名を作成する秘密鍵がわからないからである．

次の問題は，カード会社が電子署名機能を持ったＩＣカードを発行しさえすれば問題が解決するのかという点である．答えは否である．これを成功させるためには，実店舗および仮想店舗における決済システムの変更，関連した法制度の改正が必要である．システムの変更には，ＩＣカードの導入と同様，多額のコスト負担が生じる．関係者の一致団結が必要であり，早急な対応は困難なようである．しかし，図２からもわかるように，偽造カードの被害は急増している．したがって，近い将来このシステムが導入される可能性は極めて高いと考えられる．

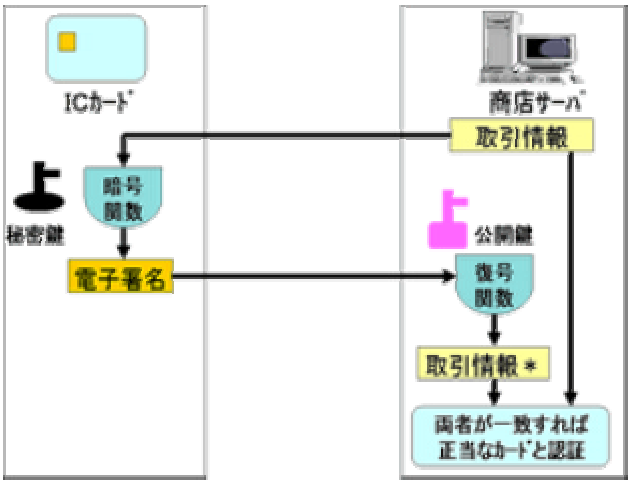

図３　電子署名を用いたカード認証

４　基本情報及び履歴情報の漏洩による脅威

４．１　基本情報の漏洩による脅威

氏名，住所，電話番号，メールアドレスが漏洩した場合の脅威には次の２つが考えられる．

第一の脅威は，基本情報を盗まれた者が，ダイレクトメール，押し売り，迷惑電話，迷惑電子メールなどの攻撃を受けることである．しかし，これら基本情報に関してはすでに漏洩していて，電子商取引によって漏洩しても新たな問題が急増するとは考えにくい．ただし，職業，年収，嗜好などに関しては，現状あまり漏洩していないようであることから，電子商取引の際に聞かれても，答えないほうが安全である．

第二の脅威は，これまでのところほとんど指摘されていない．しかし，私は，将来大きな問題となる可能性があると思っている．それは，悪意のある犯罪者が，基本情報を盗まれた者になりすまして，第３者に対して，手紙，はがき，電子メールなどを送付するというものである．内容が嘘，デマ，脅迫，プライバシーの暴露などの内容であれば大きな問題を引き起こす可能性がある．これまでは，手紙，はがきなどは自筆で書かれることが多いため問題とはならなかったが，ワープロや電子メールの普及により自筆で書かれていないものが急増しており，犯罪者によるなりすましが容易になっている．その結果，次のような脅威の可能性が生じている．

①自分を馬鹿にした文書をもらったものが，なりすまされた者に対して怒りや恨みを持つ．

②なりすまされた者が信用や地位のある人の場合，偽りの内容であってもこれを信じてしまう．

この他にもいろいろな脅威が考えられ，中には犯罪者に大きなメリットや精神的快楽をもたらすものもありえよう．犯罪者がそれを見つけ出した場合，犯罪が急増する恐れは十分にあると思われる．この問題の対策については，後述する．

４．２　履歴情報の漏洩による脅威

履歴情報としては，購入履歴，店舗へのアクセスログなどがある．これの厄介な点は，購入者が提示しなくても勝手に店舗に蓄積されてしまう点である．これが漏洩した場合の脅威としては，自らの消費行動を知られるという点が挙げられるが，人によって脅威の度合いはさまざまであろう．

しかし，社会的に身分の高い人，例えば，医者，弁護士，教師などが，例えばポルノビデオ等の一般的でない商品を購入した場合，ニュース性が高い．そこで，犯罪者がこれらの情報をテレビ局，新聞社，雑誌社に売りつけることが考えられる．さらには，世の中への暴露をネ

表１　個人情報の脅威と対策一覧

情報種別	内容	商店の入手法	脅威	対策
ｶｰﾄﾞ情報	ｸﾚｼﾞｯﾄｶｰﾄﾞ番号	顧客から入手	ｶｰﾄﾞ偽造, なりすまし購入	電子署名認証, ＩＣカード
基本情報	氏名，住所，年齢 電話番号，ﾒｰﾙｱﾄﾞﾚｽ, 職業，年収など	顧客から入手	なりすまし郵便・ﾒｰﾙ，ﾀﾞｲﾚｸﾄﾒｰﾙ，迷惑電話	郵便への署名, ﾒｰﾙへの電子署名
履歴情報	購入商品，購入時期	商店が記録	情報暴露，脅迫	ﾆｭｰｽ性のある購入回避

タに脅迫やゆすりを受ける可能性もある．一般の人も含めて，ニュースになるような購入には気をつけるべきである．

４．３　対策

ここでは，手紙，はがき，電子メールなどのなりすまし送付の対策について考える。近年，これらは自筆以外の方法で作成されることが多くなってきており，犯罪者が盗んだ情報（氏名，住所，電子メールアドレス等）を悪用すれば，他人に成りすまして文書を送付することが容易となっている．これを解決するための手段としては，以下のものが考えられる．

①受け取った情報がおかしいと感じた場合は，郵便物や電子メールに書かれている送付者に事実を確認する．

②郵便物には自筆の署名を，電子メールには電子署名を付加することを，法律の制定などの手段によって義務付ける．

もし問題がおきた場合，当面は手段①を実行すべきであるが，文書の内容が過激な場合は，確認をするにも相当な勇気が必要となる．したがって，この問題が多発するような場合は，手段②をとるのが最良と考えられる．

以上，個人情報が漏洩した場合の脅威と対策について考察をした．表１は，その結果をまとめたものである．

５　まとめ

電子商取引における情報漏えいに関して，その可能性，脅威，対策について考察を加えた．主な結果は，以下のとおりである．

（１）情報漏洩は，主にデータベースの情報に対して行われる．手口には，サーバへの不正侵入，コンピュータウイルスなどによる情報の持ち出し，内部者による漏洩などの手段があり，これらを防ぐことはきわめて困難である．

（２）クレジットカード番号の漏洩による脅威は，電子商取引におけるなりすまし決済ではなく，カードの偽造という形で現れている．偽造カード被害に対しては，現状カード会社が負担しているが，将来は消費者が負担をする可能性もあり，注意が肝要である．

（３）偽造カードの脅威に関しては，これを防ぐ有効な方法がある．それは，ＩＣカードが電子署名により自らの正当性を証明する方法である．電子署名の作成に必要な秘密鍵は，カード内の読み出し不可領域に書かれているため，偽造はきわめて困難である．

（４）基本情報を盗んだ犯罪者が，他人になりすまして，嘘，デマ，脅迫，暴露などの内容の郵便物や電子メールを第３者に送付する脅威に関しては，これまで指摘されていないが今後起きる可能性が大と思われる．対策としては，署名，電子署名の付加の義務付けが有効である．

参考文献

片方善治監修，ｅ－コマースシステム技術体系，フジテクノシステム，2001

Steve Burnett　＆　Stephen Paine，暗号化，RSA セキュリティ株式会社，2002

Ross Anderson，情報セキュリティ技術大全，日経ＢＰ社，2002

大山永昭他，ＩＣカード総覧，株式会社シーメディア，2001

島望，八木原一恵，かんたんウイルスバスター2002，技術評論社，2002