紹　介

五味俊夫『インターネット取引は安全か』

澤　喜司郎

(I)

本書は，「一般消費者のインターネットを利用した商取引，とくにホームページ上のヴァーチャル・ショップでの買い物，あるいは銀行や証券会社との金融取引などについて，その安全性の吟味を中心に取引の仕組みを平易に解説したもの」である。

そして，著者によれば「本書で取り上げるテーマは企業ー消費者間インターネット取引の範疇に含まれるものであるが，インターネット取引の特性は，ひとえにインターネットが採用しているネットワーク系統や通信方式によるところが大きい。その安全性，危険性についても同じことがいえるのである」としている。

以下，本稿では主としてヴァーチャル・ショッピングに関する安全性についての著者の主張を要約的に紹介したい。

なお，本書の構成は

序　章　電子商取引の中のインターネット取引
第1章　インターネット取引の不安
第2章　SSLという国際標準
第3章　クレジット会社の憂鬱
第4章　ハッカー対策に「万全」はあるか
第5章　公開鍵証明書と認証局
第6章　インターネット取引の新しい波
終　章　インターネット輸入大国の未来

である。

(II)

ヴァーチャル・ショッピングは「インターネット上の販売店のホームページを訪れ

て，商品の写真等を見て購入する方法であり，1999年にすでにショップ数は2万を超えている。なかでも，パソコン関連商品，飛行機や列車，劇場などのチケット予約，書籍などに人気が集まっていてビジネスとして成立している。わざわざ店に出かけなくても購入できるので忙しいひとには大変便利である。この3分野はいずれも実物を手にとって確認する必要性の薄い商品であり，はじめから購入する意志が決まっていることが多く，インターネット・ショッピングに適した商品といえる。」

しかし「消費者として気になるのは，おそらくその安全性ではないだろうか」とし，「日本は米国にくらべ，まだまだクレジット決済が十分に普及しているとは言いがたい。単なる通信販売にしても，アメリカと日本とではその発展に大きな差がある。これは，おそらく対面取引を好む日本人の消費者文化の特性によるところが大きい」ばかりか，「インターネットは，20世紀末に突然姿を現した通信技術である」ため，「通信販売や銀行の金融端末（ATM）の利用にくらべて，情報の流れがわかりにくい。しかも…誰もが容易にその通信網に入って情報の送受信ができる開かれたネットワークだといわれている。このあたりに漠然としない不安を抱く利用者も多いのではないかと思われる」という。

そして，ヴァーチャル・ショッピングには様々な方法があるが，「ホームページの申込欄に直接書き込めるところが，やはりインターネットによる注文のもっとも簡便なところ」で，「インターネット取引ならではの支払方法といえば，何といっても手軽で便利な後払いのクレジット決済であろう。注文情報とともにクレジットカード番号をホームページに書き込むことで代金の支払いができる。便利ではあるが，この場合はインターネット取引ならではの安全面での配慮が必要になってくる」ばかりか，「従来型の通信販売でも，FAXや電話でも，あるいは糊付けで封印のできるはがきなどで注文情報，クレジット情報を送るという方法はとられ…はがきが開封される危険性は皆無とはいえないし，FAXの誤配というケースも考えられる。しかし，インターネット取引の場合，問題となるのは，インターネットという通信方式の性格に由来する，従来型通信販売とは異質の危険性がある」ことである。

これを商店やデパートにおいてクレジットカードで買物をする場合と比較して，「店頭では，クレジットカードを使い，手書きの署名をし，その場で紙に印字された領収書を受け取るが，ヴァーチャル・ショッピングでは，インターネットで注文情報とともにクレジットカードの番号を送るだけである。クレジット情報がクレジット会社で承認されれば，〈たしかに注文を受けた，商品を発送する〉旨のメールを販売店から受け取ることはできるだろうが，それは自分のクレジット情報が，通信の途中で読み

取られなかった証拠にはならない」のである。

また,「ホームページを閲覧している際に,ネット検索のためキーワードを入れて送信しようとすると,〈インターネットに情報を送信しようとしています。ほかのひとに読み取られる可能性がありますが,続行しますか?〉という警告文がでることがある」が,これを通常のネット検索の折りにたびたび経験している消費者は,自分のクレジットカードの番号を書き込んで送信する操作に,本能的に不安を覚えて当然である。これがインターネットという通信方式に特有のセキュリティの弱点であって,この場合の利用者の不安は,具体的にはクレジットカードの紛失,盗難をおそれる心理と同一のものであろう」と著者はいう。

(Ⅲ)

ヴァーチャル・ショップのホームページで「商品を選択して〈購入〉ボタンをクリック…した時,〈セキュリティで保護されたページを表示しようとしています。このサイトと取りかわす情報は誰からも読み取られることはありません〉といった注意が表示され,その表示画面の「OK」ボタンをクリックして先へ進むことが多い。OKすれば次の画面が現れ,商品番号,品名,単価,数量などを書き込む注文情報の欄,住所,氏名,電話番号などのお客様情報,それに支払方法の選択欄などに記入を求められる,そして支払方法でクレジットを利用するなら,カード番号を記入するように求められる。必要事項の記入が終われば,送信ボタンをクリックすればよい。」

この時,記入画面を子細に観察すると,「画面情報のアドレス(URL)欄では,それまでの画面では「http://」であったのが,「https://」に変わっていることがわかるだろう。また,画面下のステータスバーでは,閉じた錠前が表示されているはずだ。これはSSL(Secure Sockets Layer)というセキュリティのプログラムが作動している証拠なのである。じつはOKボタンをクリックして情報を記入する画面が現れる瞬間に,この安全確保の仕掛が働いて,送信先の販売店の身元確認をしたり,他人に送信情報を見られないようにしたりする作業が自動的に行われ…こういう状態になれば画面に入力して送信ボタンを押し,品物を注文すると,情報は正しく販売店に届き,他人にクレジット番号などを見られることはない。」

そして,SSLというセキュリティの方式では利用者は新たなソフトをパソコンに組み込む必要はなく,それは「パソコンのホームページを見るソフト(よく知られたインターネット・エクスプローラやネットスケープ・コミュニケータ等)に,すでにセキュリティ

のプログラムを作動させる仕組みの一部が組み込まれているからである」が,「ブラウザの画面で「http://」が「https://」に変わり，下部の錠前の絵が閉じられることを確認しただけでは，なぜ，それで取引の安全性が担保されるのか，を説明したことにはならないだろう」とし，暗号化，公開鍵，共通鍵，秘密鍵について説明したのち,「暗号化された共通鍵を秘密鍵で復号し，同じ共通鍵で暗号化されたメッセージを復号する」のであり,「この共通鍵は安全のため，取引ごとに使い捨てになっている。一連のSSL秘密通信による取引が終われば廃棄され，また次の取引に際して，利用者のSSLソフトは新たな共通鍵を作り出す」のであって,「これがSSLというセキュリティ・ソフトによる秘密通信の仕組みである」と解説している。

さらに，通信相手の身元確認について「重要なことは…公開鍵証明書には，それがたしかな証明書であることを保証するために，認証局の秘密鍵を使ったデジタル署名が付いていることで」，インターネット・エクスプローラやネットスケープ・コミュニケータ等のブラウザにあらかじめ入っているのはこの認証局の公開鍵なのである。つまり，ホームページを見るブラウザに収納された認証局の公開鍵が，認証局のデジタル署名を確認（秘密鍵による暗号を復号）することでショップの公開鍵が真正なものであることを保証し，そのショップの公開鍵がショップのデジタル署名を復号することで身元確認が行われるという構造になっている。しかし，著者は「ブラウザにはじめから入っている認証局の公開鍵が本物であることを保証する…仕組みは存在しない。はじめから用意されているのは，ブラウザのSSLソフトに入っている認証局の公開鍵なのだから，その意味では，これらのブラウザのSSLというセキュリティ・ソフトが真正なものであり，そこには本物の認証局の公開鍵が入っていることを前提に，このシステムは成り立っているともいえる」と指摘している。

このSSLソフトによって本物のショップであることが確認でき,「管理番号・パスワード，クレジットカード番号などを秘密通信することもできる。インターネット上で他人に見られることはあるかもしれないが，判読される心配はない。このように利用者の側では，何ら特別の準備を必要としないセキュリティ・システムであるが，企業の側では認証局に証明書を発行してもらうために一定の手間と費用がかかる。銀行や金融機関でSSLを採用していない企業は日本においても存在しないだろう。だが，それを惜しんで暗号化しないまま個人情報を送らせるシステムを採用しているショップは，まだ数多く存在する。取引画面になっても「http://」のままのショップとは，取引を避けるのが賢明であろう」とし，ヴァーチャル・ショッピングについては「安全性のいかんが議論されずに普及しつつある感なきにしもあらずである。現実には，販売店

の数が多いだけに，セキュリティが講じられていないサイトにカード情報を流して悪用されてしまったケースが実際に発生している」と警告している。

(Ⅳ)

電子商取引推進協議会セキュリティ・ワーキンググループ「小規模ショップ調査」(1999年４月）によって，わが国におけるヴァーチャル・ショッピングにおける安全対策をみると，SSLを使用しているサイトは約25％であり，これは「依然として代金引換，振込などの決済手段が多く，クレジット決済の普及もこれからという現実の反映でもあろう。SSLを使わないショップの多くは住所，電話番号などをメールやWeb経由で秘密通信抜きで遅らせている。なかにはクレジット番号までも暗号化せずに送らせているところまである」のが現実であると著者はいう。

インターネット先進国のアメリカでは，安全対策の技術も相当に進んでいるといわれるが，「日本のハード，ソフトの提供メーカー各社は，すでに数年前から米国の技術を吸収してきており，サイト（＝ホームページ）の構築の際に，必要な経費さえ惜しまなければ，安全なインターネット取引が実現できる基盤は十分整っている」と著者は指摘する。とはいえ，インターネット取引において利用者が感じる危険には，盗聴（ルーター内部あるいは外部からの個人情報や取引内容を盗む），なりすまし（ショップ等になりすまして個人情報を送らせて悪用して詐欺を働いたり，盗聴データをもとに他人になりすまして詐欺を働く），ハッカー（サイトを破って侵入して，個人情報盗用などの犯罪を行う）があるばかりか，携帯電話を使用した取引でも電話会社のコンピュータから先はインターネット網を経由してショップのホームページにアクセスしているため，パソコン取引と同様に「危険が潜んでいるとみなくてはなるまい」と警告している。

そして「盗聴やなりすましに対しては，秘密通信と相手の確認（デジタル署名）でこれを防ぐことができる。そのための技術や仕組みがSSLのような手順であり，暗号技術であり，認証局の存在であった」が，「取引形態によっては，SSLも万全のセキュリティ・システムとはいえないことが，その後，明らかになってきた」とし，それは顧客情報管理とハッカー対策，それに顧客情報管理以前の問題としてのショップそのもの，あるいはショップの悪意あるスタッフによる情報の悪用であるという。つまり「SSLによって販売店のサーバーまでは秘密通信が行われるが，販売店のサーバーでは復号された個人情報やカード番号などがファイルに記録されている。ハッカーによる

外部からの攻撃に対して，防御対策の手間と費用を惜しんでいるサイトでは，常に個人情報流出の危険がある」ばかりか，「クレジット決済での購入に必要な情報は，1回取引すれば，その後，利用者の個人情報，クレジット情報に変更がない限り，販売店にとっては取引のたびに送ってもらう必要はない。これがじつは意外な盲点になっている。インターネット取引では，注文後のカード会社との交渉は販売店に一任されているため，販売店に悪意があれば，あたかも毎月購入があったかのようにカード会社に請求を出すことができる」のである。ただし，後者は「リアルの取引でも起こり得ることで，インターネット取引特有のリスクとは言いがたい」と断っているが，「取引を通じて利用者の個人情報，場合によってはクレジット情報までが販売店など企業に握られてしまう」ことになり，「SSLで秘密通信を使用していれば，インターネット取引はすべてが安心と言い切ってしまうわけにはいかない」と指摘している。

このように考えれば「SSLというソフトは，あくまでインターネット上，二者間での身元確認（認証）と秘密通信のためのツールであり，こうした問題を回避するようには設計されていない」のであり，そのためインターネット取引のクレジット決済専用のセキュリティ・システムとしてビザとマスターカードによって開発されたのがSET (Secure Electonic Transaction Specification) である。

SETには二つの大きな特徴があり，一つは利用者自身がデジタル署名をするというものであり，この方式は「これまでのSSLにはなかった特徴で，証明書の取得など，ちょっと面倒ではあるが，それなりにメリットも大きい。秘密鍵で暗号化した署名を付けて送れば，秘密鍵を持っているのは自分だけだから，まちがいなく自分が送ったものと証明でき…署名は自分のパソコンソフトに格納された秘密鍵で行うが，ちなみに，個人のパソコンから秘密鍵を盗むよりも，街中で使用される磁気方式のクレジットカードを盗む（スキミング〔＝掬い取り〕する）ほうが，技術的にずっと簡単である」といわれ，もう一つの特徴は「リアルの世界と同様に，買い物のつどリアルタイムでカード会社のチェックが入る，本当の意味での三者間の取引になっていることである。クレジット決済でSSLを使用する場合には，クレジット会社に情報が届くといっても，それは秘密通信による取引を終えたあと，販売店が専用回線で送るのであって，インターネット取引そのものはあくまで消費者（＝カード会員）と販売店だけの二者間の取引に終始する」のである。

さらに，重要なことは「商品購入の際に，カード会員と販売店双方からカード会社に承認の要求が届くことで…カード会員からカード会社への承認要求は実際には販売店経由で送られるが，顧客のカード会社宛のメッセージにはカード会社の公開鍵を使っ

て秘密通信されるため，暗号化されたまま販売店のサーバーを通過してしまい，クレジット情報が復号され，販売店のサーバーに蓄積するという事態は回避される」ということで，これは「カード会社が関心があり守ろうとするのはクレジット情報で…何十万ものヴァーチャル・ショップのすべてで，会員のクレジット情報管理やハッカー対策が十分に実施されているとは考えにくい。販売店に期待するよりも，むしろ店にクレジット情報を渡さずに決済できれば，そのほうがはるかに事故がすくなくなる」というカード会社の考えに基づくものであるという。

（V）

ヴァーチャル・ショッピングにおいてSET処理をするためのカード会員用ソフトは，SSLのようにパソコンのブラウザに標準装備されていないため，利用者はSETを採用しているカード会社に申し込んでソフトを送ってもらい，パソコンに組み込む必要がある。組み込み時にはパスワードの登録を要求されるが，これはパスワードを知らないと秘密鍵を使ったデジタル署名ができないようにガードがかけられているためである。

また「SSLにおいては，ソフトがあらかじめブラウザに組み込まれていて，そこには認証局の公開鍵が入っていた。SETでは…専用ソフトに入っているのは，認証局の公開鍵ではなく，ビザ＆マスターカードの公開鍵なのである。SETの場合，ビザとマスターカードが審査をして，認証局にお墨付きを出すというシステムになっている。それが認証局公開鍵証明書であって，それにはビザとマスターカードの秘密鍵による署名がある。これを利用者が受け取って，専用ソフトに入っているビザとマスターカードの公開鍵で復号し，ビザとマスターカードが求めた正しい認証局であることを確認」し，その後，商品の購入前に会員用ソフトに従ってカード会社が運営する認証局から会員用公開鍵証明書を発行してもらうことになる。そのため，「カード会員側の処理がずいぶん大変にみえるが…会員用ソフトがほとんど自動的に処理を行ってくれる」ので，会員がするのは上述のようにソフトの組み込みと本人情報の入力，パスワードの登録だけである。

ただし，ここで注意すべき点は，「SETというセキュリティ・システムの仕様はクレジット決済の部分だけを決めており，カード会員と販売店の間の注文方法については何ら関知しないということである。つまり商品の注文については秘密通信をしようがしまいが販売店任せ」であるので，「せめてSSLのセキュリティ対策はとられていなけ

ればならない。クレジットカード番号を送らなくても，住所，電話番号，注文内容をインターネット経由で販売店に送ってしまえば，セキュリティ対策なしでは，裸のままインターネットの通信網にさらされることになる。個人情報を盗まれては不愉快であるし，また注文した時に送った情報をすべて知られたら，なりすまして注文されてしまうおそれがある。クレジット情報だけが守られればよいというわけではない」ということを著者は強調している。

そのため，ヴァーチャル・ショッピングを行う場合には「念のため入力画面のURLが「https://」に変わっていて，SSLを使用しているかどうかを確認しておこう。」「SSLを採用しているサイトはまだ少数派である。クレジット決済では，念のため，ではなく，必ず入力画面のURLでSSLを使用しているか否かを確認すべきである」と注意を呼びかけている。とはいえ「SSLシステムでは，販売店の公開鍵証明書は認証局に登録するだけで取得されている。いわばきちんと登記された会社であるという程度の証明でしかない。SETのようにリアルタイムでカード会社に加盟店であることを確認して発行されているわけではないので，その点も注意が必要である」という。なお，「最新のSSLソフト（バージョン3）には，利用者用証明書を取得し，デジタル署名をする機能が付いており…この方式を採用している場合…利用者の送信メッセージにデジタル署名が付けられるため，安全性が高いことはいうまでもない。」

そして，著者はインターネット取引における重要なポイントは二つあり，「一つは利用者本人の確認方法である。これがいいかげんだとなりすましの危険がある。もう一つはサイトが信用できるか，また必要な安全対策費用をかけているかである。…ハッカー対策一つをとっても多額の費用がかかるが，対策が甘ければ個人情報流出やハッキングの危険がある。もちろんSSLまたはSETシステムであることは大前提である」とし，SETではクレジット情報の保護についてはカード会社の責任であり，住所，電話番号などの情報の保護は販売店の責任であるとしたのち，「再三繰り返すが，SSL使用システムでは，クレジット情報は販売店のサーバー上で復号される。販売店が信用できるか，必要な安全対策をとっているかが最大のポイント」であるとし，続けて「インターネットの世界では，Webやメールを通じた印象で，つい相手を簡単に信用しがちなものである。リアルの世界であれば，信用を確認できない相手とは取引しないし，怪しげな店ではクレジットカードなど使ったりしないはずである。ヴァーチャルの世界でもやはり信用確認が第一である。インターネットは便利だが，所詮は道具であって，リアルの世界を映す鏡にすぎない。まず相手の信用を確認すべきである」と忠告している。

また「カード番号，有効期限などは，街でカードを使うときにコピーが店に残ってしまう。それをインターネットのSSL方式のヴァーチャル・ショップで悪用されないかという不安も残る」という記述は気にかかる。

なお，ビザやマスターカードがSET開発を決めた理由の一つにはハッカー対策があり，著者は「日本では，SSL方式でさえ，ヴァーチャル・ショップの常識になっているとは言いがたい。SSLを使用せずにクレジット情報を送らせるような販売店があれば，その店のハッカー対策がどのようなレベルであるかはおよそ想像がつこうというものである」という。この「ハッカー対策には，ファイアウォール（防火壁）と呼ばれる防御ソフトを搭載したサーバーを使わないと十分な効果が得られないことはよく知られている」が，「ファイアウォールはソフトだけで数10万～300万円もかかる。定期的ソフトメンテナンスやセキュリティ検査サービスの費用まで考えると相当な額になるが，SSLやSETの採否とともに，ハッカー対策に必要な費用を出し惜しみしないサイトでないと情報流出のリスクが大きい。逆に利用者の眼で見た場合，こうしたセキュリティ対策のコストに耐え得るサイトか否かが一つの信用の基準となる」としている。

（Ⅵ）

以上，ヴァーチャル・ショッピングに関する安全性についての著者の主張をやや詳細に紹介したが，最後に以下のこともぜひ紹介しておきたい。

電子商取引推進協議会ビジネス・ワーキンググループが1999年にアメリカにおける成功サイトを調査したところ，わが国ではインターネット・ビジネスに対して初歩的な誤解のあることが明らかになった。それは，「①インターネット・ビジネスは低コストで開店運営可能である，というのはまったく事実に反する。セキュリティ（安全対策），決済機能，処理能力を充実させるには投資が必要で，お金を惜しんでいてはレスポンスも遅い。速いサーバー，高速回線でのインターネット接続，ミラーサーバー（複数のサイトでの処理分散）の採用などが必要である。②スモールビジネスも大企業と互角に戦える，というのもどうやら誤解のようで，ベンチャーは，単独では市場獲得は困難。人気サイト，ブランドとの連携が必要である。また，大企業はリアル世界での信用をベースにヴァーチャルに進出している。③広告を出す必要なくアクセスがある，などということはあり得ない。成功サイトは売上の多くを広告に費やしている」ということであり，著者は「これからビジネスを始めようとする，ヴァーチャル・ショップ経営希望者の夢を奪うようだが，これが現実である」という。

本学部においてもベンチャービジネス論を受講し，安易に学生起業家としてインターネット・ビジネスを始めようと考えている学生もいると思うが，同講義でインターネットの利便性ばかりが強調され，インターネット自体やインターネット取引における安全性については何一つ語られていない現状では，インターネット起業家を目指す学生諸君には本書をぜひとも読んでいただきたい。

最後に，筆者が浅学非才なために本稿において本書の的確な紹介ができず，また筆者の不勉強による誤読の可能性もあり，この点については著者のご海容をお願いする次第である。

(文春新書，2000年，204頁，660円＋税)