H11－リスク評価WG－1

ＥＣリスクの調査と処理の実態

－日本における現状と処理の実態－

平成１２年３月

電子商取引実証推進協議会

リスク評価WG

はじめに

日本のインターネット人口は 1999 年 4 月には 1800 万人を超え、現在でも毎月 30 万人程度で増加する勢いである。またＥＣビジネスの代表例であるバーチャルショップはここ 4 年ほどの間に急激に増加し、1999 年 12 月末現在で約 2 万店舗を数えるようになった。
自宅に居ながらにして、コンピュータや書籍、各地の名産物などを購入できるＥＣは大変便利なものである。

しかし一方では購入しようとする店舗が信頼のおける販売店なのか、きちんと商品を送ってくれるのだろうか、販売店に送ったクレジットカード番号が、送信途中に誰かに盗み見されないか、販売店に送信したクレジットカード番号を悪用されるのではないかといった不安があるのも事実である。

また販売店においても消費者に対する不安はある。代金をきちんと払ってくれるだろうか、提示されたクレジットカード番号は、本当に本人が送信したものだろうか、といった不安である。

これらの不安を取り除くためには、消費者自身が何をすれば良いのか、販売店が何をすれば良いのか、いざ問題が生じたときにどのように対応すれば良いのか明確にすることが消費者や販売店の不安解消となり、今後ますますＥＣが発展することになるのではないだろうか。

リスク評価ＷＧでは昨年度ＥＣリスクの現状調査を行った。本年度は現在一般的に普及している電話や郵便を利用した通信販売とインターネットショッピング（ＥＣ）を比較することによりＥＣ特有のリスクを明確にし、また欧米諸国のＥＣリスクの現状も参考にしつつ、消費者・企業リスクの実態や保険などのリスク処理方法を調査して、今後の日本においてどのようにＥＣリスクを処理すべきかを検討した。

調査・分析が不十分なところもあるが、昨年度の報告書とあわせて本報告書をご覧いただき、一人でも一社でも多くの消費者・企業がＥＣリスクに対する認識を深めていただきたい。

平成 12 年 3 月

電子商取引実証推進協議会
リスク評価ＷＧ

目　次

1　通信販売との比較によるＥＣのリスクの特徴

当WGにおいては、昨年度インターネット書籍販売をモデルとしビジネスプロセス毎にリスクの洗い出しと評価を行い、損害の内容や頻度また対応策について調査を行った[1]。

一般に電子商取引（以下ＥＣ）は、従来から行われている通信販売において企業・消費者間のやり取りの全てもしくは一部をインターネット等を介して行われているものであり、そのリスクの多くが通常の非対面販売から生ずるリスクと同様ではないかと考えられる。

そこで本章においては、一定の条件の下においてリスク発生の可能性や難易度、適用される法律、トラブルの解決方法、損害の防止・防衛策等についてＥＣリスクと従来からの通信販売におけるリスクの違いを検証したものである。なお、広告作成から決済に至るプロセス毎に比較できるものはプロセス毎の調査、比較を行った。

この結果、ＥＣ、通信販売に共通するリスクの特徴については、通信販売で既に確立されているリスク処理方法を利用できるであろうし、ＥＣ特有のリスクについては、それを明らかにすることにより､今後新たなリスク処理方法を検討するための参考になると思われる。

1.1　通販とＥＣのリスク比較表

1.1.1　対象とするリスク

通販とＥＣリスクの比較を行うにあたり、下記の 12 のリスクを想定した。これらのリスクは、必ずしも通販およびＥＣの両方で発生するとは限らないが、特にＥＣにおけるリスクとして固有のものについても参考資料として取り上げている。

なお各リスクの事例や販売店と消費者の具体的な損害については、「1.3 解説　リスク環境（技術・コスト）」に掲載した。

- **犯罪・詐欺（販売店のなりすまし）**
- **犯罪・詐欺（消費者のなりすまし）**
- **過失・入力ミス（消費者の錯誤）**
- **過失・入力ミス（販売店の錯誤）**
- **犯罪・サービス不能攻撃（販売店）**
- **犯罪・改ざん（販売店）**
- **犯罪・コンピュータウィルス**
- **犯罪・不正アクセス（通信途上の盗み見）**
- **犯罪・不正アクセス（消費者のコンピュータ）**
- **犯罪・不正アクセス（販売店のサーバ）**
- **故障・事故（ネットワークダウン）**

---

[1] 平成 11 年 3 月発行「リスク評価WG中間報告書－ＥＣリスクの発見とその処理の現状－」
http://www.ecom.or.jp/seika/press/990426riskwg/riskwg-summary.html（概要）
http://www.ecom.or.jp/seika/naiyou/p2_risk/risk.pdf（PDF 形式）

- **故障・事故（販売店のサーバダウン）**

1.1.2　言葉の説明

サマリーに記載した項目については以下の通りである。

- **コスト・技術面からの発生の可能性、難易度**
  故意に損害を発生させようとした場合のコストや現状におけるハード、ソフトにおける技術面からの損害発生の可能性、難易度について
- **法律の縛り**
  適用される法律について
- **損害の解決策**
  損害解決の効果の程度や実行可能性について
- **損害の証明**
  損害にかかわる証拠性、追跡可能性について
- **損害の防止・防衛策**
  損害防止の効果の程度や実行可能性について

1.1.3　通販とＥＣのリスク比較表

－解説－　　◎　大きく違いがある　○　違いがある　×　大きな違いはない

消費者・販売店の損害	コスト・技術面からの発生の可能性、難易度	法律の縛り	損害の解決方法 損害の証明	損害の防止・防衛策
犯罪・詐欺（販売店） ● 悪意の販売店が、注文を受けたにもかかわらず、商品を送らずに代金を詐取する ● 悪意の第三者が、架空の販売店になりすましたり、実在する販売店の名をかたり（なりすまし）商品代金を詐取しようとしたり、個人情報を不正入手する **消費者の損害** ● 金銭的損害（不正代金請求） ● 精神的苦痛（個人情報漏洩） **販売店の損害（なりすまされた販売店）** ● 信用失墜による経済的損失 ● 信用回復に要する諸費用	**◎大きく違いがある** （悪意の販売店による発生の可能性、難易度について） 初期コストに大きな違いがある。また対象とする商品数･マーケットにより必要となる設備、運営コストが大きく違ってくる。 一般に通販の場合は、大規模な代金詐取のためには大掛かりな設備投資や運用コストが必要となるが、ＥＣは比較的手軽に広範囲に行うことが可能である。	**×大きな違いは無い** （悪意の販売店の詐欺的行為ならびに販売店としての法的規制に対して） 通販・ＥＣともに大きな違いはない。法律の枠組みではＥＣは通信販売の一形態とされる。 （関連する法律） 訪問販売法 景表法 刑法 民法 著作権法 商標法 不正競争防止法 その他の業法による広告規制等	**○違いがある** （損害の証明） 通販においては、比較的物理的な証拠が揃う。ＥＣにおいては電子的な証拠がメインとなり、信憑性が低い。	**×大きな違いは無い** （消費者の防止策） 販売店の認知という面から言えば、通販･ＥＣともに大きな違いは無い。 通販：店舗の認知度からの判断、ＪＡＤＭＡマークの確認等 ＥＣ：店舗の認知度からの判断、ＵＲＬアドレスブック、各種オンラインマークの確認、サーバ認証の確認、ＳＥＴの利用 （販売店の防止策） 販売店の信憑性という面から言えば、通販･ＥＣともに大きな違いは無い。 通販：ＪＡＤＭＡマークの取得 ＥＣ：ＪＡＤＭＡマークの取得、各種オンラインマークの取得、サーバ認証の取得、ＳＥＴ対応

消費者・販売店の損害	コスト・技術面からの発生の可能性、難易度	法律の縛り	損害の解決方法 損害の証明	損害の防止・防衛策
犯罪・詐欺（消費者） ● 悪意の第三者が、実在するカード会員になりすまし、不正に商品を詐取しようとする **消費者の損害** ● 金銭的損害（不正代金請求） ● 精神的苦痛（個人情報漏洩） **販売店の損害** ● 信用失墜による経済的損失 ● 信用回復に要する諸費用 ● 金銭的損害（売上代金の債権譲渡取消）	**×大きな違いは無い** （悪意の第三者について） 実在するカード会員の情報を現実の世界で入手する点では、違いはない。 また、ネット上で実在するカード会員の情報を入手することは、高度な技術を要する。	**×大きな違いは無い** 通販・ＥＣともに大きな違いはない。 （関連する法律） 民法 刑法	**解決方法** （消費者） **×大きな違いは無い** 通販・ＥＣともに消費者は販売店、クレジットカード会社に連絡、相談することにより解決する。 （販売店） **×大きな違いは無い** 通販・ＥＣともに消費者の本人認証を販売店に義務付けており、第三者による不正利用は販売店がリスクを負担することになる。この場合、一定のコストを見込んでおく必要がある。 **損害の証明** （消費者・販売店） **◎大きく違いがある** 注文書を郵送、ＦＡＸする通販においては、第三者の詐欺的行為が物理的な証拠として残る。 ＥＣにおいては、本人を確実に特定することが困難であり、証拠も電子的な証拠しか残らない。	**◎大きく違いがある** （消費者の防止策） 現実の世界においてカード会員情報を容易に知られないよう対策を行うことは通販、ＥＣともに同じ。 ＥＣ：ＳＳＬ、ＳＥＴ等技術的な対応策が必要となる。これらの利用により一定の効果が得られる。 （販売店の防止策） 通販：消費者の住所、性別、年齢からの判断 ＥＣ：ＩＤ、パスワードによる本人認証、ＳＥＴを利用することにより一定の効果が得られる。

消費者・販売店の損害	コスト・技術面からの発生の可能性、難易度	法律の縛り	損害の解決方法 損害の証明	損害の防止・防衛策
過失・入力ミス **（消費者の錯誤）** ● 画面上、カタログ上でイメージした商品とは異なる商品が届けられた ● 購入の意思が無いのにキーボートやマウスを間違って操作してしまい注文してしまった **消費者の損害** ● 金銭的損害（代金請求・返品送料等） ● 時間的損害（代金請求取消手続き、返品手続き等） **販売店の損害** ● 時間的損害（売上データの修正、キャンセル作業等） ● 金銭的損害（再販できない場合の商品代金）	**×大きな違いは無い** 通販・ECともに発生するリスクといえる。 カタログの場合は、印刷具合、ＥＣの場合は消費者のコンピュータ、モニターの性能に大きく関係してくる。	**×大きな違いは無い** 通販・ＥＣともに大きな違いはない。 通販・ECともにクーリングオフ制度が適用されない。（但し割賦販売を除く） （関連する法律） 訪問販売等に関する法律 割賦販売法 民法 景表法	**×大きな違いは無い** どちらのケースも、消費者自身のイメージ違いによるものであり、返品・交換を販売店が受付けするかが問題となる。	**×大きな違いは無い** 正確な商品イメージを消費者に伝えるために、より多くの情報を伝えることは、通販・ＥＣともに同様である。 （消費者の防止策） 通販・EC：手にとって確認したほうが良い商品の購入は避ける。 不明な点は販売店に確認してから購入する。 （販売店の防止策） カタログの印刷の出来映えやＷｅｂ、コンピュータの性能に依存するケースが多い。 通販・EC：商品の立体表示、より正確な色合い表示、サイズ等の基本情報を正確に記載する。

消費者・販売店の損害	コスト・技術面からの発生の可能性、難易度	法律の縛り	損害の解決方法 損害の証明	損害の防止・防衛策
過失・入力ミス **（販売店の錯誤）** ● **販売店社員によるデータ入力ミス** ● **販売店の注文内容の聞き間違い** **消費者の損害** ● 金銭的損害（未利用分請求） ● 利用機会喪失（不適正価格の表示） ● 時間的損害（返品のための手続き等） **販売店の損害** ● 時間的損害（入力、売上データの修正、キャンセル作業等） ● 信用失墜による経済的損失 ● 信用回復に要する諸費用 ● 金銭的損害（カタログ・コンテンツの再作成等）	**×大きな違いは無い** 販売店社員が入力を行う業務は通販・ECともに多く、発生の可能性、頻度に大きな違いは無い。	**×違いは無い** 通販・ＥＣともに大きな違いはない。 （関連する法律） 民法 訪問販売法	**○違いがある** （販売店の損害） 入力ミスに気づき、正しいデータに変更しようとする場合、通販においては一度配布されたカタログ等を訂正告知することは困難である。ＥＣではＷｅｂをリアルタイムで訂正することが可能である。また訂正した旨の連絡も、メール等を利用することにより効率的に行える。 **×大きな違いは無い** （消費者の損害） 消費者の損害に対する解決方法としては、通販・ECに大きな違いは無い。	**×大きな違いはない** データ入力という場面は通販、ＥＣともに多く存在する。入力したデータを再確認する作業は通販、ＥＣともに必要であり根本的な防止策に大きな違いは無い。

消費者・販売店の損害	コスト・技術面からの発生の可能性、難易度	法律の縛り	損害の解決方法 損害の証明	損害の防止・防衛策
犯罪・サービス不能攻撃（販売店） ● 嫌がらせ目的で販売店に大量の注文書、注文メールが送信された **消費者の損害** ● 利用機会の喪失（販売業務の中断） **販売店の損害** ● 休業損害 ● 損害賠償責任（消費者の遺失利益）	**◎大きく違いがある** 通販においては注文書を大量に送りつけることは、コストも手間もかかり非現実的である。 ＥＣにおいては大量の注文メールを販売店に送りつけることは、技術的にも簡単である。EC特有のリスクといえる。	**×大きな違いは無い** 通販・ＥＣともに大きな違いはない。 （関連する法律） 民法 刑法 電気通信事業法 有線電気通信法 地方公共団体の条例等による規制	**×大きな違いは無い** その注文が正規の注文かいやがらせかをシステムで判断させることは困難であり、最終的には人間によるチェックが必要となる。	**◎大きく違いがある** EC：特定のメールアドレスからの発信を受信拒否する等システム的に対応が可能である。 通販：正規の注文との区別をシステム的に判断する方法が無く、手作業に頼らざるを得ない。

消費者・販売店の損害	コスト・技術面からの発生の可能性、難易度	法律の縛り	損害の解決方法 損害の証明	損害の防止・防衛策
犯罪・改ざん（販売店） ● 販売店の悪意の従業員が実際に注文を受けた以外に不正な売上を捏造する **消費者の損害** ● 金銭的損害（不正代金請求） ● 時間的損害（代金請求取消手続き） **販売店の損害** ● 信用失墜による経済的損失 ● 信用回復に要する諸費用 損害賠償責任（不正売上の使用者責任）	**×大きな違いは無い** オフラインでの不正売上の捏造は、通販ＥＣ共に発生の可能性はある。	**×大きな違いは無い** 通販・ＥＣともに大きな違いはない。 （関連する法律） 刑法 民法 景表法 訪問販売法	**×大きな違いは無い** 通販・ＥＣともに解決方法に違いはない。	**×大きな違いは無い** 販売店の従業員が悪意を持つ以上、システム的に防止することは困難である。 販売店の社員教育・管理を行っても確実に防止することに限界がある。

消費者・販売店の損害	コスト・技術面からの発生の可能性、難易度	法律の縛り	損害の解決方法 損害の証明	損害の防止・防衛策
犯罪・コンピュータウィルス ● 販売店からダウンロード、購入したソフトにウィルスが混入しており感染した **消費者の損害** ● 金銭的損害（データ復旧費用、ハードウェアの再購入） ● 利用機会喪失（ハードウェア使用不能） ● 時間的損害（データ復旧作業、代金請求取消手続き） **販売店の損害** ● 金銭的損害（データ復旧費用、ハードウェアの再購入等） ● 休業損害 ● 物的損害（ハードの故障）	**◎大きく違いがある** 商品をダウンロードで購入するケースはＥＣ特有のものである。 通販の場合は、そもそも商品自体にウィルスが混入していたというケースは考えられるが、ネット上での配送を利用しないので配送途中でのウィルス混入はありえない。	**×大きな違いは無い** 通販・ＥＣともに大きな違いはない。 （関連する法律） 民法 刑法 製造物責任法（PL法）	**×大きな違いはない** ウィルスが混入してしまった後の解決方法、損害の証明に大きな違いはない。	**◎大きく違いがある** ダウンロードによるウィルス混入はＥＣ特有のリスクである。

消費者・販売店の損害	コスト・技術面からの発生の可能性、難易度	法律の縛り	損害の解決方法 損害の証明	損害の防止・防衛策
犯罪・不正アクセス **（通信途上の盗み見）** ● 店に送信した個人情報を通信途中で何者かにより盗聴されプライバシーを侵害された **消費者の損害** ● 金銭的損害（不正代金請求） ● 精神的苦痛（個人情報漏洩） **販売店の損害** ● 特に無し	**○違いがある** ネットワークでの盗聴に匹敵するものとして、郵便配送途中の個人情報の漏洩や公衆回線（ＮＴＴ等）の盗聴が考えられるが、ＥＣでの盗み見の可能性ほど高くはないと考えられる。	**○違いがある** ＥＣ上の不正アクセスに対しては、「不正アクセス行為の禁止等に関する法律」が制定されている。 法律では、 ①不正アクセス行為の禁止、処罰 ②不正アクセス行為を助長する行為の禁止、処罰 ③アクセス管理者による防御措置 ④国、都道府県公安委員会による援助等 が規定されている。 （その他の関連する法律） 憲法 民法 電気通信事業法 有線電気通信法	**◎大きく違いがある** ＥＣの場合、販売店に送信する個人情報が、どのような経路において誰に盗聴されたかを確認し立証することはまず不可能である。	**○違いがある** EC：ＳＳＬによる暗号化通信が最良の防止策であり、効果もある。 通販：電話やＦＡＸの盗聴に対して消費者や販売店が個別に対策することは困難であり、限られた対応のみである。

消費者・販売店の損害	コスト・技術面からの発生の可能性、難易度	法律の縛り	損害の解決方法 損害の証明	損害の防止・防衛策
故意・不正アクセス **（消費者のコンピュータ）** ● 消費者のコンピュータが不正アクセスを受け、データを破壊された。個人情報が漏洩した。 **消費者の損害** ● 精神的苦痛（個人情報漏洩） ● 金銭的損害（不正代金請求、データ復旧費用、ハードウェアの再購入） ● 時間的損害（データ復旧作業、代金請求取消手続き） **販売店の損害** ● 特に無し	**◎大きく違いがある** 消費者コンピュータのハッキングはEC特有のリスクといえる。 ただし通常ダイヤルアップにてインターネットサービスプロバイダー（ＩＳＰ）に接続している消費者のコンピュータが不正アクセスを受けることは、まずありえない。	**○違いがある** 不正アクセスに対しては、「不正アクセス行為の禁止等に関する法律」が制定されている。 法律では、 ①不正アクセス行為の禁止、処罰 ②不正アクセス行為を助長する行為の禁止、処罰 ③アクセス管理者による防御措置 ④国、都道府県公安委員会による援助等 が規定されている。 （その他の関連する法律） 憲法 民法 電気通信事業法 有線電気通信法	**◎大きく違いがある** EC特有のリスクといえる。	**◎大きく違いがある** （消費者の損害） EC特有のリスクといえる。 EC：ファイアウォールの設置。

消費者・販売店の損害	コスト・技術面からの発生の可能性、難易度	法律の縛り	損害の解決方法 損害の証明	損害の防止・防衛策
犯罪・不正アクセス **（販売店のサーバ）** ● 販売店のサーバが不正アクセスを受け、個人情報が漏洩した **消費者の損害** ● 金銭的損害（不正代金請求） ● 精神的苦痛（個人情報漏洩） ● 利用機会喪失（販売業務の中断） **販売店の損害** ● 休業損害 ● 信用失墜による経済的損失 ● 信用回復に要する諸費用 ● 金銭的損害（データ復旧費用等） ● 損害賠償責任（個人情報漏洩）	**〇違いがある** 通販においても顧客情報をサーバ上に管理していれば発生の可能性はあるが、通常はまずありえない。 従業員による犯罪（内部犯行）の可能性は通販・ECとも十分考えられる。	**×大きな違いは無い** 不正アクセスに対しては、「不正アクセス行為の禁止等に関する法律」が制定されている。 法律では、 ①不正アクセス行為の禁止、処罰 ②不正アクセス行為を助長する行為の禁止、処罰 ③アクセス管理者による防御措置 ④国、都道府県公安委員会による援助等 が規定されている。 （その他の関連する法律） 憲法 民法 電気通信事業法 有線電気通信法	**×大きな違いは無い** （販売店の損害） 販売店サーバへの不正アクセスに起因する消費者への損害賠償責任は、賠償責任保険にて対応可能である。 （消費者の損害） 不正代金による金銭的損害は、販売店およびカード会社へのクレームにより解決するしかない。	（販売店） **〇違いがある** 通販においても顧客情報をサーバ上に管理していれば発生の可能性はある。 不正アクセスの原因の多くは、販売店の内部犯行とも言われている。 通販：社内運用規定の確立、販売店社員の社員教育等運用面での防止策。 EC：上記対策のほか、ファイアウォールの設置や外部からのアクセス制限等技術的な防止策。

消費者・販売店の損害	コスト・技術面からの発生の可能性、難易度	法律の縛り	損害の解決方法 損害の証明	損害の防止・防衛策
故障事故 **（ネットワークダウン）** ● ネットワークダウンにより注文ができなかった **消費者の損害** ● 利用機会喪失（販売業務の中断） **販売店の損害** ● 休業損害 ● 損害賠償責任（消費者の遺失利益）	**◎大きく違いがある** 通販においては公衆回線（電話・ＦＡＸ）ダウンの可能性は低い。ＥＣにおいてはインターネットのダウン（トラフィックの低下）の可能性は十分あり、広告から受注までネットワークに依存しているＥＣにおいてネットワークダウンは致命傷ともいえる。	**×大きな違いは無い** 通販・ＥＣともに大きな違いはない。 （関連する法律） 民法	**×大きな違いは無い** （販売店の損害） ネットワークダウンに対する休業損害は、コンピュータ総合保険やネットワーク中断保険で対応可能である。 （消費者の損害） ネットワークダウンに対する利用機会の喪失は、通販・ＥＣともに販売店に対するクレームのみで大きな違いは無い。	**◎大きく違いがある** 公衆回線（電話・ＦＡＸ）ダウンの対策を消費者や販売店が自ら行うことはまずありえない。 ＥＣにおいては業務の多くがネットワークを介しており、信頼のおけるＩＳＰを選択する等の防止策を行うことができる。 （販売店の防止策） ＥＣ：信頼のおける上位ＩＳＰと契約する。 複数のＩＳＰと契約する。 ＩＳＰとの回線容量を大きくする等。 （消費者の防止策） ＥＣ：信頼のおけるＩＳＰと契約する等。

消費者・販売店の損害	コスト・技術面からの発生の可能性、難易度	法律の縛り	損害の解決方法 損害の証明	損害の防止・防衛策
故障事故 **（販売店のサーバダウン）** ● 販売店サーバのシステムダウンにより営業ができなくなった。データが消失した。 **消費者の損害** ● 利用機会喪失（販売業務の中断） **販売店の損害** ● 休業損害 ● 金銭的損害（データ復旧費用等） ● 損害賠償責任（消費者の遺失利益）	**◎大きく違いがある** 通販においては、受注業務をコンピュータ化しているとは言え、手作業での受注が可能である。ＥＣにおいては業務をコンピュータ化しているのが通常であり、サーバダウンは致命傷といえる。	**×大きな違いは無い** 通販・ＥＣともに大きな違いはない。 （関連する法律） 民法	**×大きな違いは無い** （販売店の損害） 販売店のサーバダウンに対する休業損害は、コンピュータ総合保険やネットワーク中断保険で対応可能である。 （消費者の損害） 販売店のサーバクダウンに対する利用機会の喪失は、通販・ＥＣともに販売店に対するクレームのみで大きな違いは無い。	**〇違いがある** （消費者の防止策） EC：複数の通信チャネルを持つ販売店を利用する。 （販売店の防止策） EC：信頼できるシステムの利用、最新アプリケーションの利用、ハードウェアの容量アップ、無停電電源装置の取り付け、定期的なメンテナンスの実施、保守体制の確立等。

1.2　解説　法律

消費者向けのＥＣは、わが国の法律の枠組みでは通信販売の１つの形態とされる。通信販売を行うにあたっては様々な法規制がある。双方に適用される法律に大きな違いは無いもののＥＣにおいては法的な解釈が明確にされていない部分も多い。

（参考文献）

内田晴康・横山経通　共著
「インターネット法」社団法人商事法務研究会刊
根田正樹・矢内一好・青木武典・小倉秀夫　共著
「インターネット・電子商取引の法務と税務」（株）ぎょうせい刊
多賀谷一照・松本恒雄　編集代表
「情報ネットワークの法律実務」第一法規出版（株）刊

1.2.1　犯罪・詐欺（販売店のなりすまし）

1.2.1.1　訪問販売に関する法律（訪問販売法）

訪問販売法は通信販売を直接規制する唯一の法律であり、通信販売業者が最低限遵守しなければならない法律である。この法律は一般消費者を保護する目的の法律であり、商人が営業用に取引する場合や輸出取引のための販売、国や地方公共団体が行うものには適用されない。また割賦で購入申込を受けた場合は割賦販売法が優先適用される。

訪問販売法第 2 条では、通信販売の定義として「売買契約または役務提供契約の申込を郵便、電話機、ファクシミリ装置その他の通信機器又は情報処理の用に供する機器を利用する方法で」と定義しており、一般的な通信販売のみならず、ＥＣにおいてもこの定義に該当すると解されている。

また、同条ならびに 21 条において、「指定商品」「指定権利」「指定役務」を定義し、訪問販売法の適用範囲を定めている。消費者の身の回りのほとんど全ての商品が指定されているが、指定外の商品[2]については、訪問販売法の適用除外となる。

訪問販売法のうち、直接通販を規制する条文は第 8 条（広告の規制）、第 8 条の 2（誇大広告の禁止）、第 9 条（前払式通販の規制）の 3 条のみである。

ここでは、通販業者が通販広告を出す際の表示義務事項（第 8 条）、及び事実に相違し、実際のものより優秀・有利であると人を認識させる広告でそれが著しい場合の禁止事項（第 8 条の 2）及び前払式通販を利用する消費者を保護するために、注文を受けた際に遅滞なく書面により承諾等を通知する義務が通販業者側にあるということ（第 9 条）を規定してい

[2] 指定外の商品：①主として御用聞き販売で販売されることが通例である商品（生鮮食料品、冷凍食品、石油、石炭製品、木炭等）②低額商品であってかつ、消費者が周辺の店舗で手軽に入手できるか、または容積、重量があるため、訪問販売、通信販売になじまないと考えられるもの（電池、マッチ等や製綿、ちり紙等）③他の法令により訪問販売、通信販売が制限されている商品（鉄砲、刀剣、医薬品、酒類等）

る。

前 3 条の内、第 8 条の 2 及び第 9 条については、罰則規定が設けられており、主務大臣の指示に従わない場合には 50 万円以下の罰金が科せられ、同 9 条の 3 に定める 1 年以内の業務停止命令の対象となる。

ＥＣにおいても通信販売取引の一形態として訪問販売等に関する法律（訪問販売法）の適用を受ける取引である。平成 10 年 5 月の訪問販売法の省令改正により、インターネット上で通信販売店舗を営む業者については、ホームページ上に下記 1～9 を広告表示することが義務付けられた。

1. 販売価格
2. 送料
3. 代金の支払時期及び方法
4. 商品等の引き渡し時期
5. 商品等の返品特約
6. 販売業者氏名
7. 住所
8. 電話番号
9. 代表責任者氏名

しかしながら多くのホームページにおいて上記広告表示義務を遵守していないため、通商産業省では、インターネットを利用した電子商取引における消費者トラブルの防止及び今後の電子商取引の健全な発展を図る為、過去に 2 回の調査を行いインターネットサーフデイとして、広告表示を遵守していない業者に対し行政指導として警告メール等を発信している。

なお訪問販売法は日本国内の物に対する商品もしくは権利の販売または役務の提供のみに適用されるため（訪問販売法第 10 条 1 項）、国外の販売店で商品を購入したりサービスを受ける場合は適用外となる。

1.2.1.2　不当景品類及び不当表示防止法（景表法）

広告に関しては、広告自体の目的が商品やサービス、企業の存在等を消費者に知らせ、その特性を消費者に理解させることにより、消費意欲を喚起・高めようとするものであるため、消費者保護観点より景表法で一定の規制をしている。景表法第 4 条では、不当な表示の禁止について以下 3 号を定めている。

1. 優良誤認（4 条 1 号）
   商品または役務の品質、規格その他の内容についての不当表示
2. 有利誤認（4 条 2 号）
   商品または役務の価格その他取引条件についての不当表示
3. 誤認のおそれのある表示（4 条 3 号）

商品または役務の取引に関する事項について一般消費者に誤認されるおそれがあると認めて公正取引委員会が指定する表示

景表法は訪問販売法のように指定商品制をとっていないので、取引対象の面では全ての商品及び役務に適用される。同法は適用対象となる「景品類及び表示」の内容を公正取引委員会の告示で指定しており、平成 10 年 12 月には指定告示の改正により「情報処理の用に供する機器による広告」が新たに表示内容に追加された。

景表法第 4 条の「不当表示」に該当する広告や表示を行うと、同法 6 条の定めにより公正取引委員会より排除命令を受ける。

1.2.1.3　その他の業法による広告規制

通販業者が取扱う商品や業種に応じて以下のような個別の業法による広告規制が課せられているものがある。

1. 割賦販売法の割賦販売条件の表示義務（同法第 3 条、第 29 条の 2、第 30 条）
2. 貸金業規制法の貸付条件の掲示義務や貸付条件の広告規制（同法第 14 条、第 15 条）誇大広告の禁止（同法第 16 条）
3. 旅行業法の広告表示事項の規制（同法第 12 条の 7）、誇大広告の禁止（同法第 12 条の 8）
4. 医療法の広告制限（同法第 69 条ないし 71 条）
5. 薬事法の誇大広告の禁止（同法第 66 条）広告制限（同法第 67 条）
6. 宅建業法の誇大広告等の禁止（同法第 32 条）
7. 証券取引法の不正取引行為の禁止（同法 157 条）
8. 食品衛生法の虚偽・誇大広告の禁止（同法 12 条）

なお当然ながら各種業法によって一定の資格や許認可なしに営業できない業種があるので、ＥＣで販売しようとする商品やサービス毎に、各種規制の有無を確認する必要がある（表 1-1 参照）。

表 1-1 営業許可・届出等必要な業種

営業の種類	許可・認可等（根拠法）
酒類製造販売業	免許（酒税法）
貴金属の販売業	申請（物品税法）
風俗営業	許可（風俗営業等の規制及び業務の適性化等に関する法律）
質屋	許可（質屋営業法）
古物営業	許可（古物営業法）
薬局	許可（薬事法）
医薬品販売業	許可（薬事法）
化粧品製造業（輸入販売業を含む）	許可（薬事法）
医療用具販売業（賃貸業を含む）	届出（薬事法）
毒物・劇物販売業	登録（毒物及び劇物取締法）
貸金業	登録（貸金業の規制等に関する法律）
旅行業第１種・第２種・第３種　旅行業者代理業	登録（旅行業法）
火薬類製造及び販売業	煙火製造許可（火薬類取締法） 販売業許可（火薬類取締法）
猟銃等の製造及び販売業	許可（武器等製造法）
計量器販売業	届出（計量法）
宅地建物取引業	免許（宅地建物取引業法）
建築士事務所	登録（建築士法）
有料職業紹介事業	許可（職業安定法）
労働者派遣事業	許可・届出（労働者派遣法）

出典：宮崎県庁ホームページより部分引用
（http://www.pref.miyazaki.jp/shoukou/seisaku/sesaku/hb1105.htm）

1.2.1.4　詐欺的行為に関する法規制

当然ながら、悪意の販売店については、刑法上の詐欺罪（同法第 246 条）として処罰されるし、民法上も不法行為（同法第 709 条）に基づき損害賠償請求ができる。

また、そのような販売店との契約は、詐欺による意思表示として取消ができる（民法第 96 条 1 項）ことや錯誤による意思表示として契約が無効（民法第 95 条）になる場合がある。

特にＥＣ取引においては当該取引契約の直接当事者でなく、モール事業者等、取引当事者以外の責任を巡るトラブルが予想される。

モール事業者がモール内の店舗を組織している場合に、消費者がモール事業者自身を売り主であるかのように誤認するような外観を有する場合には、商法 23 条の類推適用により名板貸人として取引上の責任を負う場合もある。また実質的な指揮監督関係が認められる場合には、民法 715 条の使用者責任を負う場合もある。本件に参考となる 2 つの判例を以下に掲載する。

（判例その 1[3]）

最高裁第一小法廷判決　平成 7 年 11 月 30 日（民集 49 巻 9 号 2972 頁他）
第一審　横浜地裁平成 3 年 3 月 26 日判決（判例時報 1390 号 121 頁他）
控訴審　東京高裁平成 4 年 3 月 11 日判決（判例時報 1418 号 134 頁他）

1．事案

スーパーマーケットペットショップで買ったインコがオウム病にかかっていたために、買主とその家族に損害が発生した。

2．判断

判決は、一般の買物客がペットショップの営業主体をスーパーマーケットであると誤認するのもやむを得ないような外観が存在し、スーパーマーケットが、その外観を作出し、又はその作出に関与していたから、商法 23 条（名板貸）（他人が自己の商号等を使って営業することを許諾すること）の類推適用により、スーパーマーケットは買物客とペットショップの取引について責任を負うとした。

（判例その 2）

最高裁第三小法廷判決　平成元年 9 月 19 日（集民 157 号 601 頁）
第一審　東京地裁昭和 53 年 5 月 29 日判決（判例時報 909 号 13 頁他）
控訴審　東京高裁昭和 59 年 5 月 31 日判決（判例時報 1125 号 113 頁他）

---

[3] 「バーチャルモール運営者の責任」（弁護士藤田康幸氏）より引用
（http://www.ne.jp/asahi/law/y.fujita/comp/int_mall9707.HTM）

1．事案

新聞広告を見て不動産会社からマンションを購入する契約をしたが、その後に不動産会社が倒産してマンションを取得することができなかったために損害が発生した。

2．判断

新聞広告の内容の真実性に疑念を抱くべき特別の事情があって読者らに不測の損害を及ぼすおそれがあることを予見し、又は予見しえた場合には、真実性の調査確認をして虚偽広告を読者らに提供してはならない義務がある（ただし、この事件では新聞社等の責任を否定した）。

1.2.1.5　著作権法

善意の販売店側のリスクを保護する法制度の１つとして、著作権法がある。

映画、写真、音楽等の著作物は、著作権法により保護されているが、著作物の例としては、以下のものがあげられる。（著作権法 10 条または 13 条）

1．言語の著作物（小説、脚本、論文、講演、詩歌、俳句等）
2．音楽の著作物（歌詞、楽曲）
3．舞踊、無言劇の著作物（舞踊、バレエ、ダンス、パントマイム等）
4．美術の著作物（絵画、版画、彫刻、書、美術工芸品等）
5．建築の著作物（建築）
6．図形の著作物（地図、図面、図表、模型等）
7．映画の著作物（劇場用映画、ビデオソフト、ゲームソフト等）
8．写真の著作物（写真）
9．プログラムの著作物（プログラム）
10．編集著作物（新聞、雑誌、百科事典、電話帳等）
11．データベースの著作物（データベース）

著作権者は、著作物を複製する権利（著作権法 21 条）や著作物を有線送信する権利（著作権法 23 条）を有している。

著作権者の承諾を得ないで、著作物を複製したり、有線送信すると、著作権侵害となり差止請求および損害賠償請求の対象となり（著作権法 112 条・114 条）、故意に著作権を侵害すると 3 年以下の懲役または 300 万円以下の罰金に処せられる（著作権法 119 条）。

ＥＣにおいては一般の通販と同様に適用されるが、インターネット上のホームページが著作権法上の保護対象となるかについて、著作権法における保護対象の定義は「思想又は感情を創作的に表現したものであって、文芸、学術、美術又は音楽の範囲に属するもの」となっている（著作権法 2 条 1 項）　。

ここでは、表現手段については問われていないので、上記の要件さえ満たしていれば著作権の保護対象となる。著作権の「複製」については「印刷、写真、複写、録音、録画その他の方法により有形的に再製すること」と定義されている（著作権法 2 条 1 項 15 号）が、

著作物を利用してホームページを開設する場合のサーバへのアップロード行為が「複製」に該当するかについては、議論が分かれている。

1.2.1.6　商標法

他人の登録商標を無断で使用することは、商標権の侵害になる。その場合には差止請求および損害賠償請求の対象（商標法 36 条・38 条）となり、故意で商標権を侵害すると、5 年以下の懲役または 500 万円以下の罰金に処せられる。

ＥＣにおいては一般の通信販売と同様に適用されるが、インターネット上のホームページと商標権の問題を考えるにあたっては、ホームページに商標を掲げる行為が商標の「使用」に該当するかが問題となる。ちなみに商標法 2 条 3 項では、商標の「使用」について下記の規定がある。

1. 商品または商品の包装に標章を付する行為
2. 商品または商品の包装に標章を付したものを譲渡し、引き渡し、譲渡もしくは引渡のために展示し、または輸入する行為
3. 役務の提供にあたりその提供を受ける者の利用に供する物（譲渡し、または貸し渡す物を含む。以下同じ。）に標章を付する行為
4. 役務の提供にあたりその提供を受ける者の利用に供する物に標章を付したものを用いて役務を提供する行為
5. 役務の提供の用に供する物に標章を付した物を役務の提供のために展示する行為
6. 役務の提供にあたりその提供を受ける者の当該役務の提供にかかる物に標章を付する行為
7. 商品または役務に関する広告、定価表または取引書類に標章を付して展示し、または頒布する行為

ＥＣにおける商品販売もしくは役務提供行為は上記７に該当すると考えられるので、ホームページに商標を掲示することは、商標の「使用」に該当する。よって、ホームページ上に、商品または役務に関する広告等のために他人の商標を無断で使用することはできない。

インターネットの利用者がホームページにアクセスするためには、ドメイン名によってホームページを識別しなければならないが、そのドメイン名自体が商標に該当するかが議論されることが多い。

日本では、ドメイン名は、日本ネットワーク・インフォメーション・センター（ＪＰＮＩＣ）により登録、管理されている。ドメイン名は申請により登録されるが、同じドメイン名であれば、先に申請されたものが登録される。

一般的には、ドメイン名はブラウザの画面上に表示されるが、ドメイン名は電話番号のようなものであり、画面上に表示されるが、商標の「使用」にはあたらず商標権侵害にはならないと考えられている。

日本ではドメイン名の登録においては、著名商標と同一のドメイン名の登録を認めない等の措置はとられておらず、ドメイン名をめぐっては著名商標と同一のドメイン名を著名商標の権利者以外の第三者が先に登録してしまうという問題が発生している。

ドメイン名の使用は商標権者以外の第三者がドメイン名として使用しても商標権侵害になる可能性が低いことはすでに述べたとおりだが、態様によっては、不正競争防止法違反に該当することがある。

1.2.1.7　不正競争防止法

不正競争行為とは、広義には「工業上又は商業上の公正な慣行に反するすべての競争行為」を意味するが、日本の不正競争行為では、不正競争防止法によって規制されるいくつかの行為類形を指す概念として使用されることが多い。

ただし、従来の不正競争防止法は規制の対象とする不正競争行為が限定されており、知的財産面の保護よりも営業上の競争秩序の保護を目的とされてきた。

その後の企業活動の多様化により、限定的なものでは、競争秩序保護の対応も充分なさなくなったため、平成 6 年 5 月に全面改正された不正競争防止法が施行された。

同法による侵害行為がある場合またはそのおそれがある場合は、差止請求ならびに損害賠償請求の対象となる（不正競争防止法第 3 条・第 4 条）が、刑事罰については、経済活動における過度の萎縮効果を回避するという観点から導入されていない。

表 1-2 商標法と不正競争防止法の保護の比較

	商標法	不正競争防止法
目的	商標を使用する者の業務上の信用維持需要者の利益の保護を確保する	事業者間の公正な競争およびこれに関する国民約束の的確な実施 国民経済の健全な発展
保護対象	商標法により登録された商標	商標（未登録）のほか氏名、商号、標章商品の容器、包装その他の商品または営業を表示するもの
保護要件	商標法 3 条、4 条の登録要件の判断が難しい	周知表示：需要者間に広く識されている表示 著名表示：著名な商品等表示
保護範囲	指定商品・役務および登録商標に関する同一・類似範囲（商標法 25 条、37 条 1 号）	左のような範囲の限定はない（ただし、以下の狭義または広義の混同が生じる場合でなければならない）
侵害行為	指定商品・役務と同一または類似の商品または役務につき、登録商標と同一もしくは類似の商標を使用	周知商品等表示についてこれと同一または類似の表示を使用し、またはその商品等表示を使用した商品を譲渡し引渡し、譲渡もしくは引渡しのため展示し、輸出しまたは輸入させることによって他人の商品または営業と混同を生じさせること 著名商品等表示についてこれと同一または類似の表示を使用し、またはその著名商品等表示を使用した商品を譲渡し引き渡し、譲渡もしくは引渡しのため展示し 輸出しまたは輸入する行為
侵害行為に対する対処法	差止請求権（36 条） 損害賠償請求権 損害額の推定（38 条） 過失の推定（39 条） 書類提出（39 条）	差止請求権（3 条） 損害賠償請求権（4 条） 損害額の推定（5 条） 書類提出（6 条）

1.2.2　犯罪・詐欺（消費者のなりすまし）

1.2.2.1　私法原則

他人による「なりすまし」、つまり本人以外の者が本人を装って行う取引については、本人の行為（意思表示）自体が存在していないことから、基本的には一切の法律関係は生じず、責任も負わないのが私法[4]上の原則である。

ただし、取引の内容や利用者の範囲も定型性があり、それらについて契約者が承認しているのが一般的であるものについては契約者が責任を負うが、そうでないものについては私法原則で処理されるべきとされている。

1.2.2.2　詐欺的行為に関する法規制

当然ながら、こうした「なりすまし」行為については、刑法上の詐欺罪（同法第 246 条）として処罰されるし、民法上も不法行為（同法第 709 条）に基づき損害賠償請求ができる。

また、そのような悪意の第三者との契約は、詐欺による意思表示として取消ができる（民法第 96 条 1 項）ことや錯誤による意思表示として契約が無効（民法第 95 条）になる場合がある。

カードの紛失、盗難等の場合の責任については、カード会社毎に微妙な違いはあるものの約款上でこれを規定している場合が多く、その約款についても公序良俗に反しないという判例がある（札幌地判平成 7 年 8 月 30 日、大阪地判平成 5 年 10 月 18 日）。

そこで、問題となるのはカードを紛失、盗難等されることなく、カード番号を第三者に知られたため不正利用された場合である。

カードの紛失、盗難等によらない不正利用については、カード会社の約款上規定もなく、不正利用の損害を誰が負担するのか、はっきりしていない。また、カード番号自体を厳重に管理する体制がとられておらず、会員にカード番号について管理する義務も負わせていない。よってカード番号を他人に知られただけでは、会員に帰責事由ありとはいえない。

ただし、何らかの帰責事由がある場合には、会員が責任を負うことも考えられる（電話による本人確認の際に、不正利用者に協力した場合や不正利用が行われていることを知りながら、何らの届出もなさず放置した場合等）。

1.2.2.3　ＥＣにおける責任分担

インターネット上において、他人に自己のカード番号やＩＤ・パスワードを悪用されて商取引が行われた場合の責任分担について現在議論がなされている。

従来の対面販売と異なり、有効なクレジットカードの所持と署名をもって本人確認ができないことに加えて、インターネット自体の通信のセキュリティの低さが指摘されており、そこでこうした「なりすまし」による不正利用があった場合に責任分担が問題となる。

---

[4] 私人間の権利義務関係など私的生活上の法律関係を規律する法規範。民法・商法など。

インターネット上でクレジットカードを使用して取引を行う場合、電話やＦＡＸ等で本人確認をするケースや、事前にクレジットカード番号を登録したうえでＩＤ・パスワードを発行し、ＩＤ・パスワード認証により本人確認をするケースが多い。これらの方法は不正利用を防止する効果はあっても現実にカードの所持と署名を確認しているわけではないため、販売店はクレジットカードの有効性を確認することはできても、送信されたクレジットカード番号が、確かにカード名義人本人が送信したかを確認したことにはならない。

一般的には、クレジットカード会社との契約においては、なりすましによる不正利用分に係る損害を販売店が負担するケースが多いようである。

とはいえ、責任分担については、今後の約款の見直し、セキュリティ手段の確保が講じられるか等に依存するため、当面議論の進展を待つ以外ないのが現状である。

1.2.3　過失・入力ミス（消費者・販売店の錯誤）

1.2.3.1　売買契約

消費者と販売業者は、売買契約の当事者であり、消費者がカタログで商品を選択し、電話、手紙、ＦＡＸその他の通信手段を用い商品購入の申込をしたり、ホームページの商品注文ボタンをクリックし商品購入の申込をすることにより、当事者間で売買契約が成立する。その結果、販売業者は、商品の引渡債務を負い、消費者は売買代金債務を負う。

1.2.3.2　民法

民法上では、いかなる内容の契約であれ、当事者は債務の本旨に従った履行をすべきであり、それがなされないときは債務不履行として責任を負わねばならないとしている（同法 415 条）。しかしながら消費者の意思表示は法律行為の要素に錯誤ありたるときは無効とする旨定めている（同法 95 条）。

ここで問題となるのは消費者の注文が正規の注文であったか、それとも錯誤に基づいた注文であったかを販売店が明らかにできないことにある。送信された電子データだけをもって消費者の意思を確認することは不可能である。

1.2.3.3　訪問販売法

訪問販売法では、消費者を保護するためにクーリング・オフの制度を定めている（同法第 6 条）。これは、消費者が申込後書面を受領してから 8 日以内であれば無条件に、申込の撤回、契約の解除ができる制度である。

ただし、通信販売（含むＥＣ）については、このクーリング・オフの規定は適用されない。（注意：割賦販売法に定める割賦販売の方法で売買契約を締結した場合は、割賦販売法に定められているクーリングオフ制度が適用される）

これは事業者の不意打ち的な勧誘により消費者の購入意思が不十分なまま契約がなされる可能性が高い訪問販売等と異なり、消費者が広告等を見て主体的に申込を行う通信販売

には、クーリング・オフを認める必要はないと解されているためである。

しかし、消費者保護の観点より、返品可否の条件ならびに返品可の場合はその条件を表示することが訪問販売法により定められている。（同法第 8 条）

訪問販売法第 8 条は、同法の指定商品を通信販売した場合に適用されるが、その規定は販売業者から購入者に対する唯一の情報伝達手段である広告に、一定の事項について明確な表示を義務づけることにより、後日のトラブル発生を防止することを目的としている。

表示事項については、下記の通りである。

1. 販売価格
2. 代金または対価の支払時期と方法
3. 商品の引き渡し時期もしくは権利の移転、役務の提供時期
4. 商品引き渡し後の返品等についての事項
5. 販売業者等の氏名または名称、住所
6. 瑕疵についての販売業者の責任についての定めがあるときはその内容
7. 申込の有効期間があるときは、その期間
8. 商品の販売数量の制限等があればその内容

上記のうち、本章にかかる部分は４の商品引き渡し後の返品等についての事項であるが、これは、引き渡した商品に瑕疵がある場合は含まれないのは当然で（この場合民商法により規定される）、瑕疵もなく契約違反もない場合において記載する意味である。

まず、返品条件を表示するものとし、返品を認めない場合はその旨を表示しなければならないとされている。よって、その旨の表示が無い場合には、原則として返品を受けるものとされている（通商産業省通達）。

次に返品を受ける場合の表示事項としては以下の通りである。

1. 返品できる期間
2. その期間内に必要な手続（返品連絡の要否、要の場合の連絡方法、商品は期間内に発送するのか、商品は期間内に到着するのか等）
3. 返品に要する費用（送料負担者、その他の申込者が負担する場合はその内容と金額）
4. 特注品その他商品の特注により返品を受けない場合はその旨を表示する

1.2.4　犯罪・サービス不能攻撃（販売店）

1.2.4.1　民法

民法では、故意または過失により他人に損害を与えた場合、損害を賠償しなければならない（民法 709 条）と定めているが、この場合の故意または過失の立証責任については、利用者が負っていると考えられている。

1.2.4.2　刑法

刑法では、この種のリスクに対して、これを直接規制する法律は存在しない。ただし、その通信の内容や形態等により違法行為となる可能性がある。

いわゆるいやがらせ電話等により、精神衰弱症に陥らせた行為が傷害罪（刑法 204 条）にあたるとされた判例がある（東京地判昭和 54 年 8 月 10 日）。

また、通信の内容によっては、脅迫罪（刑法 222 条）や強要罪（刑法 223 条）に該当する場合もある。

また、電気通信設備そのものの機能を阻害するものとして、頻繁に電話をかけたり、大量のＦＡＸ送信やいわゆるメール爆弾があげられるが、刑法 223 条では、偽計業務妨害罪を規定しており、「虚偽の風説を流布し、又は偽計を用いて、人の信用を毀損し、またはその業務を妨害した者は、三年以下の懲役又は五十万円以下の罰金に処する」としている。

この場合、通信設備そのものが阻害されたことにより、業務そのものが妨害されたという事実、つまり、通常業務を行うことが不可能なほど違法な通信が行われたという状況と、通信そのものが偽計に該当するのかということ、つまり正当な理由がないのにそれを偽って通信を行うことが必要である。

また、刑法 234 条の 2 では電子計算機損壊等業務妨害罪が規定されており、「人の業務に使用する電子計算機若しくはその用に供する電磁的記録を損壊し、若しくは人の業務に使用する電子計算機に虚偽の情報若しくは不正な指令を与え、又はその他の方法により、電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせて、人の業務を妨害した者は、五年以下の懲役又は百万円以下の罰金に処する」としており、本件のようなリスクとともにいわゆる「ウイルス」のリスクについても、本条が適用されると思われる。

1.2.4.3　その他の法律による規制

業務妨害という点では、電気通信事業法 102 条 1 項は、みだりに電気通信事業者の事業用電気通信設備を操作して電気通信役務の提供を妨害したものを罰している。

（電気通信事業法第 102 条 ）

みだりに電気通信事業者の事業用電気通信設備を操作して電気通信役務の提供を妨害した者は、二年以下の懲役又は三十万円以下の罰金に処する。

また、有線電気通信法 13 条は、有線電気設備を損壊し、これに物品を接触し、その他有線電気通信設備の機能に障害を与えて有線電気通信を妨害したものを罰している。

（有線電気通信法第 13 条）

有線電気通信設備を損壊し、これに物品を接触し、その他有線電気通信設備の機能に障害を与えて有線電気通信を妨害した者は、五年以下の懲役又は 100 万円以下の罰金に処する。

1.2.4.4　地方公共団体の条例等による規制

公衆に著しく迷惑をかける暴力的不良行為等の防止に関する条例が地方公共団体で制定されている。

(1) 千葉県

（第 11 条）何人も、電話を利用して、みだりに虚偽の事項を告げ、又は粗野もしくは乱暴な言語を用いて著しく不安又は迷惑を覚えさせるような行為をしてはならない。

(2) 香川県

（第 10 条）何人も、正当な理由がないのに、電話による通話で、他人に対し、反復して、虚偽の事項を告げ、粗野又は乱暴な言語を用いる等著しく不安又は迷惑を覚えさせるような行為をしてはならない。

(3) 大分県

（第 9 条）何人も、正当な理由がないのに、電話による通話で、他人に対し、又は虚偽の事項を告げ、粗野又は乱暴な言語を用いる等により、著しく不安又は迷惑を覚えさせる行為をしてはならない。

上記 3 県の条例における罰則規定はいずれも、5 万円以下の罰金又は拘留若しくは科料であり、常習として違反したものについては 6 ヶ月以下の懲役又は 20 万円以下の罰金が課せられる。

1.2.5　犯罪・改ざん（販売店）

1.2.5.1　詐欺的行為に関する規制

完全に詐欺を目的とした販売店の場合は、刑法 246 条に定める詐欺罪として刑法上処罰され、民法上も不法行為（民法 709 条）により損害賠償請求ができる。

またそのような販売店との契約は詐欺による意思表示として取消すことができる（民法 96 条 1 項）。

上記の規制以外にも、現行の業法や景表法の適用を受ける場合が多いが、その場合には法が規制する広告や表示の規制や書面交付義務等の法令上の義務を遵守する必要があり、これに違反すると行政処分を受けることがある。

こうした悪質な販売店の責任を追求する場合には、上記の業法違反行為を理由とする行政処分の申立（訪問販売法 18 条の 2、景表法 9 条の 3）や刑事告訴を行うことができる。

民法上、カタログもしくはＷｅｂページ上の表示が虚偽であったり、欺瞞性が高い場合には、これを信用して契約申込をした消費者は、詐欺による意思表示として取消ができること（民法 96 条 1 項）や錯誤による意思表示として取消ができること（民法 95 条）が規定されている。

宣伝、広告その他の顧客誘因のための表示の内容の虚偽性や欺瞞性が強い場合には、民法上の不法行為（民法 709 条）が成立することがある。その場合、前出の各種業法等の表示、広告規制の内容が、違法性判断に影響を及ぼす。

しかし、殊にＥＣにおいては、犯罪行為や不法行為を行った主体を確定することは、かなり困難な事情があるのに加え、情報の保存性に問題がある。例えば、悪質な販売店の場合には、Ｗｅｂページの掲載内容を頻繁に変更したり、販売店自体が「くもがくれ」してしまう場合があり、契約申込時点でのＷｅｂページの掲載内容を紛争になってから再現することは困難であるという事情である。

販売店の特定に関しては、単にＷｅｂページのアドレス程度の情報しかない場合は、通信の秘密（憲法 21 条）との関連でかなり困難な問題があるが、刑事事件の任意捜査や裁判所や弁護士会等、法律上の照会権限のある者からの照会を受けた場合には、販売店の住所、氏名、名称や電話番号等を開示する場合もある。

－参考－

社団法人テレコムサービス協会[5]の定める「インターネット接続サービス等に係る事業者の対応に関するガイドライン」

> **（任意捜査その他の照会への対応）**
> **第 18 条　事業者は、警察官、検察官、検察事務官、国税職員、麻薬取締官、弁護士会、裁判所等の法律上照会権限を有する者から照会を受けた場合、書面の呈示を求めるものとし、記載事項等を確認のうえ、照会に対して必要と認められる範囲内で協力することができる。ただし、緊急避難または正当防衛の場合を除き、以下に掲げる通信の秘密に属する事項等を開示してはならない。**
> **通信の存在及び内容**
> **通信当事者の氏名、住所または居所**
> **通信当事者の電話番号、ＦＡＸ番号、メール・アドレス等の通信ＩＤ**
> **通信日時**

[5] 第二種電気通信事業者および情報通信関連事業者を中心とする業界団体。第二種電気通信事業・情報通信関連事業（テレコムサービス事業という）の健全な発展を図り、事業全体の発展に寄与するとともに、国民利益の増進と公共の福祉に資することを目的としている。
（ホームページ：http://www.telesa.or.jp/）

1.2.5.2　証拠の問題

日本では、書面等の内容を証明使用とする場合には、自由心証主義がとられており、証拠方法の制限を目的とする方式要件は存在しない。しかし、書面や署名・押印、あるいは原本性は、証拠価値の点または立証の難易の点で重要な意味をもつ。

民事訴訟法 228 条 4 項は「私文書は、本人又はその代理人の署名又は押印があるときは、真正に成立したものと推定する。」と定めているが、これは証拠能力の制限ではないので、署名や押印がなくても立証が妨げられるわけではない。

ここでいう文書の真正な成立とは、作成者の意思に基づいて文書が作成されたかであり、それが認められれば、形式的証拠力を有するとみなされる。

民事訴訟法では、文書の真正の確定は挙証者の相手方が文書の成立を否認する場合には、挙証者が真正を証明しなければならない（民事訴訟法 228 条 1 項）。ただし、公文書においては真正が推定される（民事訴訟法 228 条 2 項）。

当然ながら、ＥＣでは文書における署名・押印が存在しない。それに代わって電子署名や電子認証といった手段が用いられているが、その取引内容に争いが生じた場合に、そうした手段が取引情報についての電子証拠の真正を判断する基準となるかが問題となっている。

認証をめぐる問題としては、ここでのリスクである悪意の販売店による改ざんリスクがあるが、ＥＣでやりとりされるデータは 0 と 1 のデジタル信号であるから、改ざんされた形跡が残らない。よって、こうしたリスクに対応する技術として前出の電子署名（またはデジタル署名）があるが、アメリカ法のように詐欺防止法等により広範に書面・署名要件が課せられている国では、すでにいくつかの州で立法化されている。

また、証拠調べにおいて証拠調べの対象になることが予定される証拠方法について、その証拠調べが不能または困難になるおそれがある場合に、証拠資料を保全することが認められる。この証拠保全手続の費用は訴訟費用の一部となる（民事訴訟法 241 条）。

保全の要件として、予想される争点との関係で証拠としての重要性が認められ、一般に経験則に照らして改ざんが容易であり、かつ他の事例等の経験によれば改ざんの蓋然性が相当程度存在すると認められれば、相手方自身についての具体的事情を問題とせずに保全事由の存在を認めてよいとされる。

コンピュータのデータについては、性質上改ざんが容易であり、ひとたび改ざんされると証拠調べは不能または困難になるので、証拠としての重要性があれば保全の要件が充足されると考えられる。ただし、データの改ざんが容易か否かはシステムのセキュリティと関連させて考えるべき問題である。

証拠保全の手続の管轄裁判所は、訴訟提起後は証拠を使用すべき審級の裁判所（民事訴訟法 235 条 1 項）、提起前は証人等の証拠方法が所在する地を管轄する地方裁判所または簡易裁判所である（民事訴訟法 235 条 2 項）。よって、コンピュータの検証に先立ち証拠保全を申し立てる場合には、コンピュータの所在地を申し立てる側で確定する必要がある。

検証の対象となるコンピュータがネットワーク化や分散化されている場合には、所在を確定できない可能性があるため、そのような場合には、証拠方法であるコンピュータを所有する者もしくは会社の本店所在地を管轄する裁判所に証拠保全を申し立てるべきと考えられている。

1.2.6　犯罪・コンピュータウィルス

コンピュータウィルス自体は、比較的小さなコンピュータプログラムであり、一般的に自分自身をコピーして他のシステムやプログラム等に伝染する「感染機能」、感染後、特定の日時が来るか、感染してから一定の期間や処理回数を経るまで発病しないという「潜伏機能」、何らかのメッセージ表示、プログラムやデータの破壊といった「発病機能」を備えている。この３つの機能のうちどれか１つでも備えていれば「ウィルス」であるといわれている。

通信を規制する法令として、電波法 106 条では、「自己又は他人に利益を与え、又は他人に損害を与える目的で、無線設備又は第百条第一項第一号の通信設備によって虚偽の通信を発した者は、三年以下の懲役又は百五十万円以下の罰金に処する」と規定している。ウィルス通信自体が本条に該当するかどうかは、現在示されていない。

また、通信に限定されていないが、関連するものとして、刑法では以下の 3 類型の条文を設け、法的に規制している。

1. 電磁的記録不正作出罪（刑法 161 条の 2）
   「人の事務処理を誤らせる目的で、その事務処理の用に供する権利、義務または事実証明に関する電磁的記録を不正に作ったものは、五年以下の懲役または五十万円以下の罰金に処する」
2. 電子計算機損壊等業務妨害罪（刑法 234 条の 2）
   「人の業務に使用する電子計算機若しくはその用に供する電磁的記録を損壊し、若しくは人の業務に使用する電子計算機に虚偽の情報若しくは不正な指令を与え、又はその他の方法により、電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせて、人の業務を妨害した者は、五年以下の懲役又は百万円以下の罰金に処する」
3. 電子計算機使用詐欺罪（刑法 246 条の 2）
   「前条に規定するもののほか、人の事務処理に使用する電子計算機に虚偽の情報若しくは不正な指令を与えて財産権の得葬若しくは変更に係る不実の電磁的記録を作り、又は財産権の得喪若しくは変更に係る虚偽の電磁的記録を人の事務処理の用に供して、財産上不法の利益を得、又は他人にこれを得させた者は、十年以下の懲役に処する」

上記については、直接コンピュータウィルスをばらまく行為を規制するものではないが、その行為が上記 3 類型の犯罪を構成する要素として、看過できない問題となっている。

1.2.7　犯罪・不正アクセス

1.2.7.1　憲法

通信の秘密は、憲法に規定されている重要な人権である。日本国憲法 21 条 2 項後段では、「通信の秘密は、これを侵してはならない。」と定めている。この規定は公権力によって、通信の内容を伺い知ることを禁止する趣旨である。

1.2.7.2　通信関係法

電波法 59 条では、「何人も法律に別段の定めがある場合を除くほか、特定の相手方に対して行われる無線通信（電気通信事業法第 4 条第 1 項又は第 90 条 2 項の通信たるものを除く。第 109 条において同じ。）を傍受してその存在若しくは内容を漏らし、又はこれを窃用してはならない。」と規制しており、また、同法 109 条では「無線局の取扱中に係る無線通信の秘密を漏らし、または窃用した者は、1 年以下の懲役又は 50 万円以下の罰金に処する。②無線通信の業務に従事する者がその業務に関し知りえた前項の秘密を漏らし、又は窃用したときは、2 年以下の懲役又は 100 万円以下の罰金に処する」と定めている。

有線電気通信法 9 条では、「有線電気通信（電気通信事業法第 4 条第 1 項又は第 90 条 2 項の通信たるものを除く）の秘密は、侵してはならない。」と定めており、同法 14 条では、「第 9 条の規定に違反して有線電気通信の秘密を侵した者は、1 年以下の懲役又は 20 万円以下の罰金に処する。②有線電気通信の業務に従事するものが前項の行為をしたときは、2 年以下の懲役又は 30 万円以下の罰金に処する。」と定めている。

電気通信事業法では以下のように定めている。

第 3 条「電気通信事業者の取扱中に係る通信は検閲してはならない」

（検閲とは公機関によるものをいう）

第 4 条「電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。２．電気通信事業に従事する者は、在職中電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても同様とする。」

（私人による通信の秘密の侵害の規制と解されている）

第 104 条「電気通信事業者の取扱中に係る通信（第 90 条第 2 項に規定する通信を含む。）の秘密を侵したものは、1 年以下の懲役又は 30 万円以下の罰金に処する。②電気通信事業者に従事する者が前項の行為をしたときは、2 年以下の懲役又は 50 万円の罰金に処する。③前 2 項の未遂は、罰する」

1.2.7.3　刑法

刑法では、信書開封罪が以下の通り規定されている。

第 133 条「正当な理由がないのに、封をしてある信書を開けた者は、1 年以下の懲役または 20 万円以下の罰金に処する」

第 135 条「この章の罪は、告訴がなければ公訴を提起することができない。」

刑法上は、郵便業に係るものに限定されない信書を対象にしており、封緘を要件としており、かつ親告罪となっている。個人の秘密を保護法益としたものである。

1.2.7.4　通信の秘密の保護規定の例外

個別法で以下の例外をもって通信の秘密を制限している。

1. 拘留中のものが、発受する通信物の検閲、差押等（刑事訴訟法 81 条）
2. 裁判所及び捜査機関による通信書類等の差押・提出命令（刑事訴訟法 100 条、222 条）
3. 在監者の通信の検閲、制限（監獄法 46 条～50 条）
4. 破産管財人による破産者の郵便物の開披（破産法 190 条）
5. 税関による郵便物の差押（関税法 122 条）
6. 正当行為（刑法 35 条）または緊急避難行為（刑法 37 条）としての通信の秘密の開示行為

1.2.7.5　ＥＣにおける不正アクセスの規制

従来ネットワークのセキュリティ自体を保護する法令は、国内に存在しなかったが、平成 11 年 8 月に「不正アクセス行為の禁止等に関する法律（以下不正アクセス防止法）」が公布され、平成 12 年 2 月より施行されている（一部を除く）。

不正アクセス防止法の目的は、「電気通信回線を通じて行われる電子計算機に係る犯罪の防止及びアクセス制御機能により実現される電気通信に関する秩序の維持を図り、もって高度情報通信社会の健全な発展に寄与すること。」である。

内容的には①不正アクセス行為の禁止、処罰②不正アクセス行為を助長する行為の禁止処罰③アクセス管理者による防御措置④都道府県公安委員会による援助等である。

今までは不正アクセスそのものを取り締まる法令は国内に存在せず、現行の刑法では処罰されないが、本法律の施行により不正アクセスを手段とした犯罪を実行すればその段階で犯罪となる（前出ウィルス感染と同様の法令が適用される可能性が高い）。

また、民事的にも前出ウィルス感染行為と同様、民法 709 条による不法行為による損害賠償請求が適用されるものと思われる。

1.2.8　故障・事故（ネットワークダウン）

1.2.8.1　民法

通信事業者と利用者の間で、その通信サービスを利用するという契約が締結された場合に、通信事業者は、その通信サービスを提供する債務を負っていると考えられるので通信ネットワークの故障・事故等による通信途絶は、民法上債務不履行責任を負うと考えられる（民法 415 条）。

また、債務不履行と相当因果関係にある損害については、損害賠償責任が発生する（民

法 416 条）。

しかし、原則通り、通信事業者に債務不履行と相当因果関係にある損害について損害賠償責任を負わせると、通信事業者側に無限のリスクを負わせることとなってしまうので、損害賠償の範囲に制限を加える免責約款を利用することが一般的となっている。

そこで問題となるのが、その免責約款の有効性である。上記の点で参考になると思われるのが、旧電電公社世田谷通信ケーブル火災損害賠償請求訴訟判例である。

旧電電公社の電話ケーブルが火災で焼損したために、最長 10 日間も電話回線が不通になるという事故のために、注文等が途絶えたとして 90 名の利用者から旧電電公社に対して、総額 4700 万円の損害賠償請求の訴訟が提起された（結果は原告の請求棄却。平成 2 年 7 月 12 日東京高判）。

旧公衆電気通信法 109 条は、電気通信役務の不提供によって生じた利用者の損害に対する電電公社の損害賠償責任について、損害が不可抗力により発生したものであるとき、または、その損害の発生について利用者に故意、過失があったときを除き、当該加入電話により通話ができなかった場合に利用者が電話取扱局に対する通知をした日の以後の引き続き 5 日以上の不通につき、当該不通日数に対応する電話使用料および付加料金の 5 倍に相当する金額を限度として利用者に生じた損害を賠償することとしていた。

東京高裁は、利用者にとって電気通信役務の利用内容は多種多様であって、その利用によって利用者が享受する経済的価値も大小様々であるため、事故によって利用者が受ける損害もさまざまであり、高額に上ることが予想されることから、電電公社においてすべての損害の賠償に応じるとするならば、財政的な負担は極端に重いものにならざるをえない。また、利用料金の水準設定に当り損害補填に必要な財政負担を考慮するとしても、あらかじめ電気通信役務の提供が不能になった場合に受ける損害額をすべて的確に量定することは困難であると述べている。

そのうえで、旧公衆電気通信法 109 条により利用者が加入電話を用いて営業活動を行っているような場合には十分な賠償を得られないことはもちろんありうるけれども、著しく不合理な内容であるため違憲、無効であるとまでいえないと判示した。

ＥＣにおいて、通信事業者にあたると思われるインターネットサービスプロバイダー（ＩＳＰ）については、上記の旧公衆電気通信法とその公共性に大きな差があるため、同列に扱うことはできないが、東京高裁の判示するところは、ＩＳＰの約款においてもあてはまるところであり、ＩＳＰの責任を一定の限度に制限する約款の規定は合理性があると考えられる。

ＩＳＰの責任を制限する約款が有効であるとして、次にどの程度の制限であれば合理性が認められるかについては、今後の検討課題となっている。

1.3　解説　リスク環境（技術・コスト）

ここでは、故意に損害を発生させようとした場合のコストや現状におけるハード、ソフトにおける技術面からの損害発生の可能性、難易度についてリスク毎に解説する。

1.3.1　犯罪・詐欺（販売店のなりすまし）

悪意の販売店が、注文を受けたにもかかわらず、商品を送らずに代金を詐取する、悪意の第三者が架空の販売店になりすましたり、実在する販売店の名をかたり（なりすまし）商品代金を詐取しようとしたり、個人情報を不正入手するといった詐欺的な行為である。

1.3.1.1　損害の内容

(1) 消費者の損害

- **金銭的損害（不正代金請求による）**
- **精神的苦痛（個人情報漏洩による）**

(2) 販売店の損害

（なりすまされた実在する販売店において）

- **信用失墜による経済的損失**
- **信用回復に要する諸費用**

1.3.1.2　業務の規模による技術・コスト面の違い

販売店になりすます場合、対象とする消費者や販売商品数により技術、コスト面で大きく違いがでてくる。そこで通信販売ならびにＥＣにおいて３つのケースを想定してそれぞれ解説する。

(1) 通信販売の規模

通信販売は、対象とする消費者数（購入者）および取り扱い商品数によりコストが大きく変わってくるのが特徴といえる。

通信販売のターゲットとして下記の３つのケースを想定した。

1. **消費者を 1～100 名程度と想定し、チラシ等を作成して、近所または同一市町村内に配布するケース。取り扱い商品は、単品もしくは 10 品目以下。**
2. **消費者を数千名程度と想定し、隣接する市町村もしくは県内等への新聞折込広告で配布するケース。取り扱いする商品は 20～30 品目程度。**
3. **消費者を数万名と想定し、カタログを製本し全国的に郵送する等して配布するケース。取り扱い品目は数百以上を想定。**

(2) ＥＣの規模

一方ＥＣについては以下の３つのケースを想定した。

1. **ＥＣを行うについて、特別な費用をかけずにサイトを開設する。取り扱い品目は 1～5 品目前後を想定。**
2. **既存のモール等への出店によるＥＣを想定。取り扱い品目は 10 品目から 50 品**

目を想定。

3. **自社で（自分で）サーバを立ち上げてＥＣを行う。取り扱い品目は 100 品目程度を想定。**

1.3.1.3　広告物作成･広告

(1) 通信販売

１のケースではチラシ作成において特別な技術を用いることなく作成が可能である。

商品数も限られているため、掲載ページ数も少なくて済む。特に高度な技術を用いないのであれば、通常の家庭用プリンターで印刷可能であり、コピー機械を利用することにより大量に印刷ができる。またちらしの配布においても郵便や宅配といった方法を利用することなく自分で配布することも可能である。

２のケースでは折込みちらし自体は比較的安価で作成できるが、信用させる広告物にするために多色刷りや写真挿入等の技術を用いることにより印刷コストは高価になりがちである。また配布のために新聞折込や配布のための人手が必要となり配送コストもそれなりにかかる。新聞折込については新聞専売店の承認も必要となり、公序良俗に反するちらしは配布自体を拒否されることも考えられる。

３のケースではカタログを製本し全国的に郵送する必要があり、製本技術が必要となり高価となる（表 1-3～1-7 参照）。またカタログ作成にも時間がかかる。商品代金詐取、個人情報の不正入手のために参入するのはコストから見ても困難とも思われる。

表 1-3 国内通販会社のカタログ年間発行部数[6]

年間売上	年間発行部数
年間売上 10 億円の通販会社	約 500 万部（平均 1.5 誌発行）
年間売上 10～ 50 億円の通販会社	約 1000 万部(平均 2.5 誌発行)
年間売上 50～100 億円の通販会社	約 3000 万部(平均 3.2 誌発行)
年間売上 100 億円超の通販会社	約 9000 万部（平均 7 誌発行）

表 1-4 カタログの製作コストと配布コスト

カタログ 1000 部あたりの製作コスト	10 万円～20 万円
カタログ 1000 部あたりの配布コスト	10 万円～15 万円

表 1-5 新聞折込コスト

A4 サイズのちらしを 5 千枚から 1 万枚折込みする場合	1 枚あたり 4 円～5 円（ちらし製作費用は含まず。配布地域、紙質、大きさにより変動）

表 1-6 配布コスト（郵送）

郵便の場合（ちらし、小冊子程度）	金額
定型郵便物	80 円（25g）～90 円（50g）
（市内特別の場合）	65 円（25g）～70 円（50g）
定型外郵便物	130 円（50g）～270 円（250g）
（市内特別の場合）	105 円（50g）～220 円（250g）

[6] Japan Business News JNEWS LETTER 99.5.28 より引用
(http://www.jnews.com/)

表 1-7 配布コスト（宅配）

宅配の場合（製本されたカタログ等）	金額
300g まで	1 通 160 円
600g まで	1 通 210 円
１通から配送可能。なおまとめて配送する場合は、上記料金に対して割り引き有。	

(2) EC

ＥＣはある程度の技術とコンピュータ一式あればホームページを作成することが可能である。１のケースにおいては初期投資としてコンピュータの購入代金が必要となるが、最近では一定の条件のもとで無料でコンピュータを配布するサービスもあり、メーカーや性能さえこだわらなければ特別な費用はかからない（表 1-8 参照）。

また特別な技術を要しなくても、ホームページ作成ソフトを利用することで、初心者でも作成が可能である。印刷に関してもちらしやカタログのような物理媒体を要しないため、通販のように発行部数によりコストが増加することもない。

公開するサイトについても、無料のホームページサービス[7]やプロバイダのホームページサービスもあり、無料もしくは安価で公開が可能である。

２のケースにおいては、モールから専用のサイト構築ソフトが提供されている場合もあり、これらのソフトや器材を使用することにより、ＧＵＩ（視覚的）で作業を行う事が可能であり、特別な技術は必要としない。またホームページ作成を請け負う業者も存在し、それらの利用も考えられる（表 1-9 参照）。

またＥＣにおいては、ホームページ作成後即ネット上で公開が可能であり、メーリングリストやメールマガジンの利用、検索エンジンへの登録により、印刷物等を利用する通信販売と比較して、タイムリーな広告物の作成、広告が可能である。

しかし３のケースにおいては、自社で（個人で）サーバを立ち上げるため設備投資（サーバ購入、構築費用等）がかなり高価となる。また技術的にもスキームが必要となってくる。

暗号化通信を行う場合は、認証局によるサーバ認証が必要となりそのための費用も発生してくる。またセキュアサーバーＩＤ取得は法人に限られ、必要書類として法人の登記簿謄本、印鑑証明等が必要となる場合がある。ただし、詐欺的行為を行う場合にここまで体力、費用をかけて行うことはまず考えられない。

[7] 代表的な無料ホームページサービス
ジオシティーズ　http://www.geocities.co.jp/　Ｆｒｅｅｗｅｂ　http://www.freeweb.ne.jp/

表 1-8 ホームページ作成のための商品価格相場

商品の価格相場	金額
デジタルカメラ、スキャナー	3 万円～5 万円程度
ホームページ作成支援ツール （ホームページ作成ソフト、ファイル転送ソフト、デジタル画像編集ソフト）	無料（フリーソフト利用の場合）～ 1 万 5 千円程度
ホームページ作成用のコンテンツ （背景画像、ボタン等の素材）	無料（フリー素材利用の場合）～ 5 千円程度

表 1-9 主な電子モールへの出店費用（平成11 年4 月現在）

運営業者サービス名）	出店費用	店舗数
アコム （アコシス）	初期登録料＝5 万円 年会費＝1 万円 売上高の 5%の手数料 （新規加盟）	約 650 店
エム・ディー・エム （楽天市場）	500 商品まで 5 万円（月額） 1000 商品まで 10 万円（ 同 ） 2500 商品まで 25 万円（ 同 ）	約 520 店
ジーアールホームネット （ぷららパラダイス）	「トライアルパック」（物販）の場合 初期登録料＝1 万円 年　会　費＝4 万円 売上高の 10%の手数料	約 270 店
ソニーコミュニケーション・ネットワーク （Ｓｍａｓｈ）	初期登録料＝10 万円 契約更新料＝5 万円 （6 カ月ごとに更新） 売上高の 10%の手数料 （物販の場合）	約 200 店

1.3.1.4　受注

(1) 通信販売

ケース１、２においては、消費者からの注文において個人レベルでの対応が可能であり、受注用の電話も携帯電話等を活用することにより簡単に行える。ケース３については受注専用の電話回線や専任者を設ける等の対応が必要となりコスト的にも膨大となる。商品代金詐取、個人情報の不正入手のために参入するのはコストから見ても困難とも思われる。

(2) EC

ＥＣにおいては受注から商品発送依頼までの業務を一台のコンピュータで行うことも可能であり、受注に関するコストはほとんどかからない。

1.3.1.5　商品発送

商品発送のプロセスにおいては、物流を伴う商品は、通販、ＥＣともに大きな変わりはないが、ＥＣの特徴としてデジタルコンテンツのネット配信があげられる。

デジタルコンテンツのダウンロードはネット上での配信が可能であり配送料は必要としない。しかしながらトラフックの増加による遅延や、ネットワークダウン等、インターネット特有のトラブル発生が考えられ、消費者が確実にコンテンツをダウンロードできるとは限らない。また確実にコンテンツが配信されたかを証明することは困難であり、未着を理由としたトラブル等の発生が考えられる。

1.3.1.6　決済

決済のプロセスにおいては、通販、ＥＣともに大きな変わりはない。

代金前払いでは商品代金詐取は容易に行うことが可能である。

代金引換ではこのリスクについては商品を発送しないのが前提のため、通常は起こりえない。ただし虚偽の商品を送りつける手口も考えられる。しかしこの場合発覚の可能性は大きい。また代金引換の場合は、取り扱い業者との契約が必要となる。

代金後払いでは、クレジットカード会社等の決済機関との契約が必要となってくる。しかし契約には通常審査があるので、商品代金詐取のためにクレジットカード加盟店となるのはまず困難といえる。

しかし最近では、販売店がクレジットカード会社と加盟店契約をしていないにもかかわらず、クレジットカード決済を利用できる旨の広告を行い消費者の信用を得ようとするケースや、他の販売店がクレジットカード会社と契約している場合、その加盟店が伝票を横流しするケースも発生しており、クレジットカードが取り扱えることが、その販売店の信用につながるとは一概に言えないので注意が必要である。

1.3.2　犯罪・詐欺（消費者のなりすまし）

悪意の第三者が、実在するカード会員になりすまし、不正に商品を詐取しようとする行為である。

1.3.2.1　損害の内容

ここでは、なりすまされた会員ならびに悪意の第三者が利用した販売店それぞれに責がある場合と仮定した上で損害について記載している。

(1) 消費者の損害

- **金銭的損害（不正代金請求による）**
- **精神的苦痛（個人情報漏洩による）**

(2) 販売店の損害

- **信用失墜による経済的損失**
- **信用回復に要する諸費用**

- **金銭的損害（売上代金の債権譲渡取消）**

1.3.2.2　通信販売

通信販売における注文方法として、電話による注文、ＦＡＸによる注文、郵便による注文の３つが考えられる。これらの注文方法における消費者のなりすましについて検討する。

(1) 電話による注文

電話による注文は、消費者がリアルタイムで注文が可能であるというメリットがある。一方、なりすました人物は販売店のオペレーターと直接話しを行うことからなりすましが発覚することが考えられる。例えばなりすます対象の人物が女性であるのになりすました人物が男性の場合、声音から不信感をいだかれるケースも考えられる。

(2) FAX･郵便による注文

これに対しＦＡＸや郵便による注文は、なりすました人物を特定する要件がほとんどないことが特徴といえる。筆跡による鑑定も考えられるが、なりすました注文者の筆跡鑑定を行うことはコスト的な問題もあり非現実的である。また、自筆ではなくワープロ等を利用することにより、なりすました人物を特徴付ける要件はほぼ皆無になる。これは郵便による注文も同様である。

1.3.2.3　EC

ＥＣにおいては販売店に送信する情報が全て電子データとなるため、そのデータを以ってなりすました人物か本人かを判断するのは不可能である。

発信元のコンピュータをＩＰアドレスから特定することは可能かもしれないが、コンピュータを特定できたとしても、そのコンピュータを誰が操作したかを特定することはできない。

1.3.3　過失･入力ミス（消費者の錯誤）

消費者が注文書に購入したい商品を記入するときに記入ミスをしてしまい、間違った商品を購入してしまった、ホームページ上で間違って購入するつもりのない商品を購入してしまう等人為的なミスである。また消費者がカタログやＷｅｂに掲載された商品を購入したが、イメージした商品とは異なる商品が届けられるといったリスクも考えられる。

1.3.3.1　損害の内容

(1) 消費者の損害

- **金銭的損害（代金請求・返品送料等）**
- **時間的損害（代金請求取消手続き、返品手続き等）**

(2) 販売店の損害

- **時間的損害（売上データの修正、キャンセル作業等）**
- **金銭的損害（再販できない場合の商品代金）**

1.3.3.2　通信販売

カタログやちらしに記載された商品を購入したい場合、多くの通信販売では商品番号を記入させるケースが多い。商品数によっては商品番号が 8 桁 9 桁、場合によっては 10 桁以上になることもあり、間違って他の商品の番号を記入してしまうミスも十分考えられる。

これに対し販売店側では、商品番号とあわせて商品名を記入させることにより転記ミスを防ごうとするが、商品番号と商品名が相違している場合、結局消費者に再度確認する手間が生ずる等問題点も多い。一般には通信販売で注文した商品内容について、発送前に消費者に対して確認をする作業は省略されており、実際に商品が届いてから間違った商品を購入してしまったことに気がつくのが通常である。

消費者のイメージ違いも往々にして発生する。ちらしやカタログに掲載される商品データは限られた紙面の中で全てを掲載できるものではない。商品サイズが記載されていても、実際に手にとって商品を確認することができない通信販売においては、消費者のイメージ違いによる返品が多い。特に商品の色合いや材質を、ちらしやカタログに掲載する文面だけで消費者に正確に伝えることは大変困難といえる。

1.3.3.3　EC

ＥＣも通販と同様なミスは十分考えられる。コンピュータに不慣れな人がキーボードを操作して商品名や商品番号を入力する場合、往々にして入力ミスが発生する。

これらを防止するために、プルダウンメニューやラジオボタンを利用することにより、かなりの入力ミスは軽減される。しかしながら最後の購入意思確認においてキャンセルするつもりで間違えて同意ボタン（購入ボタン）を押してしまい、押したことに気がつかないケースも十分考えられる。

直ちに注文を受付けた旨の確認ページを表示することにミスを防ぐことも可能であるが、トラフィックの増加により注文確認のページが表示されないまま通信が終了してしまうことも考えられる。

一般的にＥＣにおいては、注文後販売店より注文内容を確認するメールが届く場合があり、これらのメールを確認することにより誤入力、誤操作を防止する方法が有効といえる。

また消費者のイメージ違いにおいても通信販売と同様のレベルで発生する。特にＥＣにおいてはホームページの容量制限やスムースな画像表示を行う関係から、画質を落として掲載することが多く正確なイメージを伝えることができなくなる。

しかし商品を立体的に表示することも可能であり、ちらしやカタログと比較してより多くの情報を伝えられることはＥＣのメリットといえる。

1.3.4　過失・入力ミス（販売店の錯誤）

販売店および販売店従業員がカタログやちらし、ホームページ作成時に価格等のデータを間違って入力してしまう、販売店が受注の際に注文内容を聞き間違えてしまうリスクである。

1.3.4.1　損害の内容

(1) 消費者の損害

- **金銭的損害（未利用分請求）**
- **利用機会喪失（不適正価格の表示によるもの）**
- **時間的損害（返品のための手続き等）**

(2) 販売店の損害

- **時間的損害（入力、売上データの修正、キャンセル作業等）**
- **信用失墜による経済的損失**
- **信用回復に要する諸費用**
- **金銭的損害（カタログ・コンテンツの再作成、販売機会喪失によるもの、信用回復に要する諸費用、商品の再発送費用等）**

1.3.4.2　通信販売

通信販売では、カタログ作成時点における販売店の入力ミスが考えられ、ミスを見落としてしまいそのまま印刷してしまうことも考えられる。

またミスではないものの、印刷の直後に商品属性等に変更が生ずるケースもあり、決して人為的ミスだけともいえない。

これらのミスに対して、配布したちらしやカタログを回収することはコストも嵩み非現実的である。

配送直前にミスが判明した場合は正誤表を同封することにより消費者に対して注意を呼びかけることが可能であるが、当然正誤表の作成にコストが発生してくる。

またちらしやカタログの発行スケジュールの間隔が狭い場合は、次回のちらしやカタログで訂正を告知することも考えられるが、いずれにせよ一定の期間誤った内容が消費者に知らされることには変わりない。

受注の際の聞き違えはリスクは往々にして発生するが、その都度電話で注文内容を確認することにより回避できることはメリットといえる。

1.3.4.3　EC

宣伝広告における入力ミスは、リアルタイムで訂正できることがＥＣのメリットといえる。ミスに気がついた時点で直ちにホームページを訂正することが可能であり、また会員制のサイトではデータを訂正した旨電子メール等を利用して容易に告知することが可能である。これらの作業については当然費用的なものはほとんど発生しない。

1.3.5　犯罪・サービス不能攻撃（販売店）

悪意の第三者がいやがらせ目的で販売店に大量の注文書、注文メールを送信することにより正常な販売業務を行えないリスクである。

1.3.5.1　損害の内容

(1) 消費者の損害

- **利用機会喪失（販売業務の中断）**

(2) 販売店の損害

- **休業損害**
- **損害賠償責任（消費者の逸失利益に対する）**

1.3.5.2　通信販売

悪意の第三者が、販売店の作成したカタログ・チラシ（申込用紙を兼ねもの）を使って大量発注を行うと考えれば技術的には簡単である。コストは消費者か販売店のどちらが郵送料・通信料（電話、ＦＡＸの場合）を負担するかによって変わってくるが、料金を販売店が負担する場合（フリーダイヤル、郵便料金受取人払い等）は比較的容易である。

1.3.5.3　EC

販売店への大量メールにより生じる問題は、大きく２つある。

(1) 大量メールにより、インフラ等の環境が受ける問題

- **通信負荷の増大による処理能力劣化**
- **メールサーバの処理能力がメール処理に占有されることによる、他処理の劣化**
- **メールサーバのディスク容量不足に起因する問題の発生**
  具体的には、他の処理が遅くなる、必要なメールが届かない等

(2) メール内のデータを使用した業務が大量に発生することによる問題

- **照会・申込業務が大量に発生する**

このリスクは、販売店と潜在的顧客との契約における、申込方法、支払方法、本人認証方法、カスタマー窓口運営方法に依存するが、自動的な大量照会・申込が通信販売に比べると技術的には比較的容易である。

例えば、既存のメールソフトでも、指定の時間にメール発信を行う機能を持つものがあり、この機能により、自動でメールを発信することは可能である。

また技術力のある悪意の第三者であれば、例えば自動で繰り返しメール発信を行うツールを自作することも比較的容易である。

これらのツールを使用しない場合でも、多くのメールツールはメール発信をボタン操作１つで行うことが可能であり、メールを大量発信すること自体は、比較的容易と考えられる（ただし通信費は犯罪者側の負担となる）。

メールアドレスにおいては無料で取得できる方法も多数[8]あり、また存在しないメールアドレスを用いて発信することも可能である。メールアドレスだけをもって発信者を特定することは極めて困難である。

1.3.6　犯罪・改ざん（販売店）

悪意の販売店もしくは販売店の従業員が、実際に注文を受けた以外に不正な売上を捏造するケースである。

なお販売店の改ざん行為は、売上に対する金額の改ざん行為や、注文をしていないのに新たに売上を捏造するという行為を対象とし、販売店がカタログやホームページに掲載されている金額や商品内容を改ざんすることによる詐欺的行為は除外している。

1.3.6.1　損害の内容

(1) 消費者の損害

- **金銭的損害（不正代金請求）**
- **時間的損害（代金請求取消手続き）**

(2) 販売店の損害

- **信用失墜による経済的損失**
- **信用回復に要する諸費用**
- **損害賠償責任（不正売上の使用者責任による）**

1.3.6.2　通信販売

クレジットカード番号、消費者・会員の金融・個人情報の取得に基づく個人的利益のための捏造になるが、その場合販売店とは異なる別口の口座等代金詐取のための方式を編み出さなければならないためあまり効率的とは言えず、参入障壁が高いといえる。

1.3.6.3　EC

ＥＣの場合は販売店の受注システムにより左右される。

受注システムが、受注データを自動で連携（従業員による入力・転記操作等が無い）するものである場合は不正な売上を捏造することは難しい。しかし受注システムが、従業員による入力・転記操作等がある場合は、不正な捏造が発生する可能性が存在する。

悪意の従業員による個人的利益のための捏造について考えると、売上を捏造しそれを着服するためには、その代金搾取のための方法が必要となり、その方法の確立は効率的とは言えない。悪意の従業員が、顧客の個人情報を入手して、後に顧客になりすまして悪事を働くことを考えると、受注システム上に不要な顧客個人情報を表示しないことが必要となる。

---

[8] 主な無料メールアドレスサービス
A-net　http://www.anet.ne.jp/　フリーメール　http://www.freemail.ne.jp/　等

オーダーとリンクさせて自動的に架空請求を起こしたり、改ざんする「システム」を作ることも可能であるがそのために費用が発生するので現実的ではない。

1.3.7　犯罪・コンピュータウィルス

販売店からダウンロードしたソフトにウィルスが混入しており感染するケースである。

なおここでは、ネットワークを介してのウィルス感染に限定しており、例えば通信販売により購入したソフトにウィルスが混入しており感染した、通信販売業者が日常利用するコンピュータがウィルスに感染したといったケースは除外している。

1.3.7.1　損害の内容

コンピュータウィルスがもたらす損害は、ウィルスにより大きく異なってくる。単なる愉快犯的なものから、個人情報取得を目的としたウィルス、コンピュータの動作を混乱させるウィルス、またデータ破壊を目的としたウィルス等様々である。

ここではコンピュータの動作を混乱させるウィルス、またデータ破壊を目的としたウィルスを想定している。

(1) 消費者の損害

- **物的損害（データ復旧費用、ハードウェアの再購入）**
- **利用機会喪失（ハードウェア使用不能）**
- **時間的損害（データ復旧作業、代金請求取消手続）**

(2) 販売店の損害

- **金銭的損害（データ復旧費用、ハードウェアの再購入、復旧できないデータの消失・改ざんによる請求不能額）**
- **休業損害**
- **物的損害（ハードの故障）**

1.3.7.2　通信販売

そもそも商品自体にウィルスが混入していたというケースは考えられるが、ネット上での配送を行わないためネットワークを介してのウィルス混入はありえない。

1.3.7.3　EC

(1) 自社サーバ利用のケース

サーバのセキュリティ対策は、各社（各自）でセキュリティのポリシーを設定し、それに従い策を講じることになる。設定したセキュリティポリシーが低い場合は、当然、ウィルスが混入する危険性は高くなる。

ＩＳＰのホスト運用代行サービスやサーバ運用代行サービスを利用する場合等は、提供されているファイアウォールサービスを利用することも１つの策となる。

(2) 他社サーバ・モール利用のケース

相乗りするサーバ・モールのセキュリティポリシーに因るが、セキュリティポリシーが低い場合は危険性が高くなる。また相乗りするサーバの他の利用者からの感染の可能性もある。この場合はサーバの運用ルール等にも依存する。

外部からのアタックやサーバ利用者からの感染等、十分にありうる。また感染源自体も感染していることに気づいていない場合（悪意がない場合）もある。

1.3.8 犯罪・不正アクセス（通信途上の盗み見）

販売店に送信した個人情報を通信途中に何者かにより盗聴されプライバシーを侵害されるリスクである。

通信販売においては、郵便や電話・ＦＡＸによる販売店への注文、ＥＣにおいてはインターネットを利用した販売店への注文においての通信途上の盗み見を想定している。

1.3.8.1 損害の内容

(1) 消費者の損害

- **金銭的損害（漏洩した個人情報に起因する不正代金請求）**
- **精神的苦痛（個人情報漏洩）**

(2) 販売店の損害

特に無し

1.3.8.2 通信販売

(1) 電話・FAX

販売店への電話による注文、またはＦＡＸによる注文を第三者が盗聴するケースが考えられるが、現実的に電話の盗聴を行うためには販売店の電話設備への盗聴機器の設置が必要となる。

しかし盗聴のために販売店の所在地まで出向くことや、盗聴機器を購入することはコストもかかり、非現実的である。

(2) 郵便

販売店への注文書を郵送する場合、郵便の配達ミスやはがきの裏面を見られるといったケースが考えられる。しかしながら配達ミスは偶然的なものであり、また郵便局員にはがきの裏面を見られることは業務上十分に考えられるが、入手した情報を口外、もしくは利用することは非現実的である。

1.3.8.3 EC

(1) ＬＡＮでの盗み見

消費者が勤務先のＬＡＮに接続されたコンピュータを用いて発信したメールは、往々にして管理者により見られる可能性がある。

そもそも勤務先での私的なメール利用自体が問題といえるが、仮にも消費者が勤務先のコンピュータを利用してメールを発信する場合は、絶えず管理者に見られていることを認識したうえで利用する必要がある。

(2) 通信途上での盗み見

通信途中におけるメールサーバでの盗聴は、そのメールサーバのセキュリティ対策に因るため、危険性はある。ただし、メール中継マシンにて、メールをコピーするソフト等を混入すれば傍受可能ではあるが、比較的高度な知識を要するので、実行するのは困難である。

(3) サーバへの侵入によるメールの盗聴

サーバに侵入するにはアカウント・パスワードを入手する必要があり、それらを入手するには高度な知識を必要とするため、実行するのは困難である。

1.3.9 犯罪・不正アクセス（消費者のコンピュータ）

消費者のコンピュータが不正アクセスを受け、データを破壊された。個人情報が漏洩し第三者に不正利用されたリスクである。

1.3.9.1 損害の内容

(1) 消費者の損害

- **精神的苦痛（個人情報漏洩による）**
- **金銭的損害（不正代金請求、データ復旧費用、ハードウェアの再購入による）**
- **時間的損害（データ復旧作業、代金請求取消手続きによる）**

(2) 販売店の損害

特に無し

1.3.9.2 通信販売

通常、通信販売において消費者のコンピュータを利用することはプロセスから見てもあり得ないため、通信販売では発生しないリスクといえる。

1.3.9.3 EC

個人で利用するコヒンビュータはＩＳＰへのダイアルアップ接続によりインターネットに接続するケースが多く、ダイアルアップの都度ＩＰアドレスをプロバイダーより割り当てられるため、消費者のコンピュータが不正アクセスを受けるケースはほとんど無いといえる。

常時接続されたコンピュータに不正アクセスすることは可能かもしれないが、比較的高度な知識を要するため、実行するには困難である。

1.3.10 犯罪・不正アクセス（販売店のサーバ）

販売店のサーバが不正アクセスを受け、個人情報が漏洩したリスクである。

なお通信販売においては、販売店側が顧客情報を管理するためにサーバを利用し、そのサーバが不正アクセスされるというケースが考えられるが、通常顧客情報データベースが外部ネットワークとつながっていることはあまりない。よって通信販売では販売店従業員による不正アクセス（内部犯罪）を想定している。

1.3.10.1 損害の内容

(1) 消費者の損害

- **金銭的損害（不正代金請求による）**
- **精神的苦痛（プライバシー侵害による）**
- **利用機会喪失（不正アクセスが原因の販売業務停止による）**

(2) 販売店の損害

- **損害賠償責任（プライバシー侵害によるもの）**
- **信用失墜**
- **費用・利益損害（信用回復に要する諸費用）**

1.3.10.2 通信販売

上記の通り顧客情報データベースが外部ネットワークとつながっていることはあまりない。しかし、従業員による犯罪（内部犯行）という面からは個人情報が漏洩する可能性は大きい。

1.3.10.3 EC

(1) 自社サーバの利用

サーバのセキュリティ対策は、各社（各自）でセキュリティのポリシーを設定し、それに従い策を講じることになる。

設定したセキュリティポリシーが低い場合は、当然、不正アクセスを受ける危険性は高くなる。

(2) 他社サーバ・モールの利用

相乗りするサーバ・モールのセキュリティポリシーに因るが、セキュリティポリシーが低い場合は危険性が高くなる。

1.3.11 故障・事故（ネットワークダウン）

ネットワークダウンによりサイトを閲覧できなかったり、商品注文ができなかったリスクである。

なおここでのネットワークとは広告に利用される電話、ＴＶ・ラジオ等のネットワーク、また消費者が販売店に対して注文を行うために電話・ＦＡＸを利用するための公衆回線ネ

ットワーク、ＥＣにおいてはインターネットを指し、販売店内のローカルネットワーク（ＬＡＮ）やはがき・封書を送付するための郵便ネットワークは除外している。

1.3.11.1　損害の内容

(1) 消費者の損害

- **利用機会喪失**

(2) 販売店の損害

- **費用・利益損害（休業によるもの）**
- **損害賠償責任（消費者の逸失利益に対する）**

1.3.11.2　広告･宣伝時

(1) 通販

電話網・放送網の故障により、ＴＶ、ＣＡＴＶ、ラジオからの情報入手ができなくなることが考えられるが、現実的に電話網・放送網の故障事故発生の頻度は極めて低い。

(2) EC

ＩＳＰへの接続のための公衆回線ダウン、ＩＳＰのルータ、ＩＳＰ間ネットワークの故障が考えられる。

消費者のコンピュータからＩＳＰまでの通信ネットワークの故障の場合、消費者は全てのインターネットサイトにアクセスができなくなる。当然に販売店のサイトを閲覧することができない。現実的に公衆回線がダウンすることはまず考えられない。

ＩＳＰからＷｅｂサイトまでのネットワーク経路は、その都度動的に変化するため、代替機器のない機器の故障でない限り、故障の可能性は低いと考えられる。

ただし、ネットワーク負荷が高い場合等、物理的にはネットワーク故障ではないが、処理が間に合わず中断に至るケースも考えられる。

1.3.11.3　受注

(1) 通販

電話、ＦＡＸ等の通信手段による注文ができなくなることが考えられるが、公衆回線ダウン発生の頻度は極めて低い。また仮にダウンしたとしてもはがきや封書による注文は可能である。

(2) EC

受注方法がホームページ上での受注（http プロトコル）の場合、物理的なネットワーク故障とともにネットワークの高負荷の場合等に受注ができなくなることが考えられる。

また、顧客の発注操作中にネットワーク高負荷等で操作継続不能となる場合も考えられる。

受注方法がメールでの受注の場合、メールの配送は中間のメールサーバへの転送を利用したバケツリレーの方式であるため、ネットワークが故障した場合も中間メールサーバに滞留され障害復旧後に次のメールサーバに転送されることにより、復旧後送達されると考えられる。また、発注メールはデータ量としては小さいため、メール送信中にネットワーク高負荷等で送信エラーとなることは考えにくい。

1.3.11.4 商品発送

(1) 通販

基本的に郵送や宅配等物流が伴うものであり、ネットワークのダウンと商品発送は関係しない。

(2) EC

基本的に郵送や宅配等物流が伴うものについては、ネットワークのダウンと商品発送は関係しない。しかしデジタルコンテンツのダウンロードによる配送の場合、ネットワーク故障やネットワーク高負荷等が原因で配送中に中断されてしまう可能性は十分考えられる。

1.3.12 故障・事故（販売店のサーバダウン）

販売店サーバのダウンにより営業ができなかったリスクである。

なお通信販売においては、販売店側が顧客情報を管理するためのサーバや受注、決済、商品発送業務用のサーバがダウンしたケースを想定した。

1.3.12.1 損害の内容

(1) 消費者の損害

- **利用機会喪失**

(2) 販売店の損害

- **費用・利益損害（休業によるもの損害）**
- **損害賠償責任（消費者の逸失利益に対する）**

1.3.12.2 広告・宣伝時

(1) 通販

広告・宣伝のプロセスにおいては関係しない。

(2) EC

サーバダウンによるコンテンツの消失は考えられる。

1.3.12.3 受注

(1) 通販

受注を管理するサーバが故障するケースが考えられる。

(2) EC

Ｗｅｂサーバ、メールサーバの故障は十分に考えられる。この場合、受注行為ができなくなり直ちに損害につながる。メールで受注する場合は、中間ＩＳＰで滞留し、障害復旧後送達することも考えられる。受注したデータが消失してしまう場合も考えられる。

1.3.12.4 商品発送

(1) 通販

発送業務の一部でコンピューターを利用するケースは考えられるため、商品発送の遅延や発送先データの消失の可能性がある。

(2) EC

受注したデータの消失等と同様に、商品発送データおよびデジタルコンテンツ自体の消失の可能性が考えられる。

1.4　解説　防止策

ここでは損害防止策として、具体的な防止策や効果の程度、実行の可能性について解説する。

1.4.1　犯罪・詐欺（販売店のなりすまし）

1.4.1.1　消費者の防止策

(1) 通販

① 広告宣伝時

ちらしやカタログから以下の点を確認する。

- **正規のクレジットカード加盟店であるか**
  （クレジットカードを取り扱うには、カード会社との加盟店契約が必要。正規の加盟店か判断に迷う場合は、会員となっているクレジットカード会社に問い合わせを行うこともできる）
- **訪問販売法による表示義務事項が明記されているか**
  （連絡先、代表者名、商品引渡時期、返品方法等について、明確に記述されているか）
- **店舗の認知度からの判断**
  店舗が本当に実在するかどうか、電話等で、実在性を確認することにより信頼性が高まる
- **カタログ・チラシの紙質や出印刷状態等出来映えからの判断**
- **商品価格の相場金額との乖離からの判断**
- **商品性（公序良俗・医薬品等）による判断**
- **日本通信販売協会[9]のＪＡＤＭＡマークの表示確認**
- **カタログ・チラシ等の現物保管（後日紛争が起きた場合のために）**

② 注文時

- **発注先電話番号による推測**
  遠隔地、携帯電話、電話番号から販売店を特定することも可能
- **発注時の電話対応による推測**
  発注が電話で行われる場合、その電話番号（通常の加入電話か、携帯電話か）・電話応対等で、不信感を抱く店舗への発注は避ける
- **受注担当者の氏名、所属部署の確認、記録、ＦＡＸ注文の場合は送信内容、送信記録の保管。郵送の場合は注文書のコピー保管**
  （後日紛争が起きた場合のために）

[9] 日本通信販売協会（JADMA）ホームページ：http://www.jadma.org/

(2) EC

① 広告宣伝時

ホームページから以下の点を確認する。

- **正規のクレジットカード加盟店、あるいは電子決済サービスの加盟店であるか（クレジットカードや電子決済を取り扱うには、カード会社等との加盟店契約が必要。正規の加盟店か判断に迷う場合は、会員となっているクレジットカード会社や電子決済提供会社に問い合わせを行うこともできる）**
- **訪問販売法による表示義務項目が明記されているか（連絡先、代表者名、商品引渡時期、返品方法等について、明確に記述されているか）**
- **店舗の認知度からの判断**
  店舗が本当に実在するかどうか、メール以外の手段（電話等）で、実在性を確認することにより信頼性が高まる
- **Ｗｅｂ画面のデザイン性・インタフェースによる判断**
- **商品価格の相場金額との乖離からの判断**
- **商品性（公序良俗，医薬品）による判断**
- **ＵＲＬ[10]（ドメイン）による判断**
  「co.jp」ドメインを取得するには、登録資格が規定されており、申請書に捺印した印鑑登録証明書や登記簿謄本（提出を求められた場合のみ）の提出を求められるのに比べ、「com」ドメインであれば、個人でも容易に取得することが可能である。（表 1-10 参照）
- **サーバ管理者、モール運営者の確認・知名度の判断**
- **日本通信販売協会のＪＡＤＭＡマークの表示確認**
  ―参考―
  ＪＡＤＭＡマーク
  日本通信販売協会の審査基準にパスした会員会社が通信販売広告に表示するマーク。「訪問販売法」や、 当協会の定めた「倫理綱領」を守り、信頼に基づく販売活動を行っている企業が会員となれる。

- **オンラインマークの確認**
  現在は実験中であるが、日本通信販売協会のオンラインマークのような、第三者機関からの“お墨付き“マークの普及が今後、期待される。認証機関の証明

[10] ＵＲＬ（Uniform Resource Locater）―WWW（ワールドワイドウェッブ）のインターネット上の場所を特定するもの。

書を取得（ＳＳＬ通信が可能である）場合は非常に信頼性が高いといえる。

―参考―

オンラインマーク実証実験

社団法人日本通信販売協会（ＪＡＤＭＡ）が、インターネット通信販売の促進と消費者保護を両立させるため、1999 年 8 月より開始した、適切な取引をするための体制を整備している事業者に対し、申請に基づきその旨を表すオンラインマークを付与する制度の実験。

- Ｗｅｂ画面の印刷・保管

  後日紛争が起きた場合のためにＥＣの場合、ホームページ自体を削除することにより簡単に所在不明になることが可能なため、ホームページ画面の印刷・保管等をしておくことも損害対策として有効である。

ただし、これらの防衛策・防止策は確実なものでは無くＷｅｂ画面のデザイン性による判断、ＵＲＬによる判断（www.○○.com）、モール運営者の確認・知名度の判断、Ｗｅｂ画面の印刷・保管等については一般的に不慣れな事が多く、消費者個人での判断は難しいともいえる。

② 注文時

- 発注時の通信手順（非暗号、メール）による判断
- 発注内容の印刷、保管

  後日紛争が起きた場合のために発注時には、発注内容の印刷・保管を行うことにより、送信先・送信内容を明確にしておく。

いずれも一般的には不慣れな点や販売店を特定することが困難である点が特徴付けられる。

表 1-10 日本におけるドメインの種類と登録資格について

ドメイン名	対象	登録資格
ＡＣ	大学系教育機関向け	学校教育法及び他の法律の規定による学校、大学共同利用機関、大学校、職業訓練校、学校法人、職業訓練法人
ＣＯ	一般企業向け	株式会社、有限会社、合名会社、合資会社、相互会社、特殊会社、その他の会社及び信用金庫、信用組合、外国会社
ＧＯ	政府機関向け	日本国の政府機関、各省庁所轄研究所、特殊法人（特殊会社を除く） 備考:特殊法人はＧＯドメイン名とＯＲドメイン名のいずれかを選択できる
ＯＲ	会社以外の団体向け	財団法人、社団法、医療法人、監査法人、宗教法人 、特殊法人（特殊会社を除く）、農業協同組合、生活協同組合、その他ＡＣ、ＣＯ、ＧＯ、ＥＤのいずれにも該当しない日本国法に基づいて設立された法人
ＡＤ	ＪＰＮＩＣ会員向け	(a) 当センターの会員が運用するネットワーク (b)当センターがインターネットの運用上必要と認めた組織
ＮＥ	ネットワークサービス向け	日本国内のネットワークサービス提供者が、不特定または多数の利用者に対して営利または非営利で提供するネットワークサービス
ＧＲ	任意団体向け	複数の日本に在住する個人または日本に登記のある法人で構成される任意団体 代表者及び副代表者は日本に在住する個人または日本に登記のある法人であること
ＥＤ	小・中・高校向け	保育所、幼稚園、小学校、中学校、高等学校、盲学校、聾学校、養護学校、専修学校及び各種学校の内、主に 18 歳未満を対象とするもの
地域型ドメイン名	一般地域型､地方公共団体等）	都道府県、政令指定都市名を利用、地域に根ざしたドメイン名で都道府県、地方公共団体、病院、個人等が利用できる

1.4.1.2　販売店の防止策

実在する販売店が、悪意の第三者によりなりすまされることにより、販売店の信用失墜、信用回復のための諸費用等が損害として発生する。

販売店としては、悪意の第三者を追跡し掛かる詐欺的行為を早急に中止させることが先決である。

(1) 通販

- **カタログ・ちらしの現物保管**
- **顧客の苦情等から当該第三者の追跡**

(2) EC

- **ホームページのハードコピー**
  （ただしリアルと比し証拠としての信憑性が低い）
- **顧客の苦情等から当該第三者の追跡**

1.4.2　犯罪・詐欺（消費者のなりすまし）

1.4.2.1　消費者の防止策

(1) 通販

- **個人情報の取り扱いに注意する**
- **クレジットカードの取り扱いに注意する**

消費者としては、クレジットカードは「善良なる管理者の注意を持って」使用・保管する必要がある。例えば第三者にクレジットカード番号等を不用意に見せない、売上票を安易に捨てない等、自分のカード番号を他人に見せないようにすることで、ある程度の損害を防止することが可能である。クレジットカードを配達する際に、本人が受け取る際に第三者により抜き取られるといった事件も発生しており、これに対しては消費者がクレジットカードを受け取った後にカード会社にその旨報告することによりカード利用が可能となるようなシステム（アクティベーション）の導入が望まれる。

－参考－

クレジットカード会社会員規約

> **第 2 条（カードの発行と管理）**
> **会員には当社が発行する会員証（以下「カード」という。）を貸与します。**
> **当社よりカードが貸与された場合は、直ちに当該カードの署名欄に当該会員ご自身の署名をしていただきます。**
> **カードの所有権は当社に属し、会員には善良なる管理者の注意を持って使用保管していただきます。**
> **カードはカード表面にお名前が印字され、所定の署名欄に自署した会員ご本人のみが利用でき、他人に貸与、譲渡または担保に提供預託する等カードの占有を第三者に移転することは一切できません。**
> **前項に違反してカードが第三者に使用された場合、そのカード使用に起因して生ずる一切の債務については、本規約を適用し、すべて会員がその責任を負っていただきます。**

(2) EC

- **個人情報の取り扱いに注意する**
  掲示板やメーリングリスト等の公共の場所に個人を特定できるような情報を掲載しない。携帯電話やＰＨＳのインターネット接続機能を利用する場合、メールアドレスが電話番号となるケースがあるので注意が必要である。
- **クレジットカードの取り扱いに注意する**
  通信販売同様、第三者にクレジットカード番号を不用意に見せない、売上票を捨てない等、リアルの世界でのカード番号の管理と同じである。
- **購入目的以外でクレジットカード番号を入力しない**
  一部海外のアダルトサイトでは、年齢確認と称してクレジットカード番号の入力を求められるケースもあるが、入力したクレジットカード番号が必ずしも年齢確認の為だけに利用されるとは限らないので注意が必要である。
- **コンピュータに個人情報を保存しない**
  コンピュータに重要な個人情報を保存している場合、コンピュータごと盗まれるケースも考えられる。なるべく個人情報をコンピュータ内に保管せずにその都度個人情報を入力することが望ましい。またＩＤ・パスワードを付せんに記載してコンピュータのモニター等に貼り付けている光景をよく見かけるが、これらも第三者に容易に知られてしまうので注意が必要である。当然ながら端末自体の共有を避ける等の対策も必要である。

1.4.2.2　販売店の防止策

(1) 通販

- **年齢や性別からの注文者の判断**

注文者の属性と、なりすました人物の比較

- **注文者の電話番号からの判断**

  ＡＶＳ（登録してある住所から注文者の属性をチェックするシステム）の導入

(2) EC

- **ログインＩＤ、パスワードによる事前認証**
- **ＳＥＴの導入**

1.4.3 過失・入力ミス（消費者）

1.4.3.1 消費者の防止策

(1) 通販

- **注文内容の確認**

  注文内容を発注前に再度ちらしやカタログ等と照合する。
- **商品の確認**

  カタログやホームページだけで商品の詳細がはっきりしない場合は販売店に確認する。なおカタログやちらし、ホームページに掲載された商品が、現実の商品と著しくことなる場合（販売店の故意による場合）、クレジットカード会社にその旨連絡することにより、クレジットカード会社が販売店に対して、加盟店契約に基づき商品掲載方法について指導、修正を指示できる場合もある。
- **返品特約の確認**

  通信販売はクーリングオフが適用されないため、販売店が独自に返品特約を設けているケースが多い。消費者は注文の前にそれらの条件を確認しておくことが重要である。もし返品不可の場合には、予め販売店等で実物を確認できるような商品は別として、手にとって確認しなければ購入の判断ができない類の商品購入は避けるのが無難である。

(2) EC

ＥＣにおける防止策においては基本的に通販と同様であるが、キーボードやマウスの操作には特に注意が必要である。

1.4.3.2 販売店の防止策

(1) 通販

- **消費者への注意喚起**

  カタログやちらしの表示は必ずしも実物とは一致しない旨の説明を記載し、消費者への注意喚起を行う。
- **実物を販売店で確認できるようなシステムの導入**

(2) EC

- **消費者への注意喚起**

ホームページの表示は必ずしも実物とは一致しない旨の説明を記載し、消費者への注意喚起を行う

- **商品の立体表示**
  通信販売のカタログは、商品を立体的に捕らえることが難しく、限られた情報しか消費者に伝えることができない。反面ＥＣにおいては、最新の技術を用いて立体映像を利用し、商品を色々な視点で確認できるようにすることにより、より多くの情報を消費者に伝えることが可能である。これらにより消費者のイメージ違いといったリスクはかなり軽減できると考えられる。
- **実物を販売店で確認できるようなシステムの導入**
- **デジタルコンテンツの体験版の提供**
  デジタルコンテンツのオンライン販売においては、機能・期間制限付きで試用できるようにする。
- **メールによる注文内容の確認**
  受注内容をメールにて消費者に連絡することにより、消費者の勘違いや誤操作、誤入力を防ぐ。

1.4.4　過失・入力ミス（販売店）

1.4.4.1　消費者の防止策

(1) 通販

- **カタログ、ちらしの保管**
  カタログ・チラシ作成時点で価格等の記載ミスの場合、カタログ・チラシを保存しておくことにより、販売店側のミスを証明することができる。
- **注文内容の保存**
  後日の紛争解決に有効である。

(2) EC

- **ホームページのハードコピー**
  ホームページ作成時点での表示価格等の入力ミスの場合、画面のコピーを保存することにより、販売店側のミスを証明することができる。しかしホームページは簡単に表示を修正することが可能であるので、注文の時点での画面を保管しないと後になって既にデータが修正されているケースもある。
- **注文内容の保存**
  後日の紛争解決に有効である。

1.4.4.2　販売店の防止策

(1) 通販

- **電話受注の復唱徹底**

電話受注の場合は、その都度消費者からの聞き取りを復唱確認する。

- **注文表のＯＣＲ[11]化**
  ＦＡＸや葉書等による受注の場合は、注文表をＯＣＲ化することにより転記ミスを防止する。

(2) EC

- **人手を介さない処理フローの導入**

1.4.5 犯罪・サービス不能攻撃（販売店）

1.4.5.1 消費者の防止策

販売店へのサービス不能攻撃において消費者が行う防止策は特にない。

1.4.5.2 販売店の防止策

(1) 通販

- **郵送料・通信料の顧客負担**
  いたずら目的の発注を減少させる要因として働くが、当然販路を狭めることにもなる。
- **電話、申込、解約（クーリング・オフ）の記録**
  いやがらせが事件化した場合の「証拠」として保存しておく。

(2) EC

- **ＡＶＳの利用**
- **個人情報の事前登録制**
- **ＳＥＴ等の技術を用いた本人認証方式の採用**
- **ログ・データの保存**
- **スパム防止ソフト等の利用**
- **電子メールサーバの容量アップ**

1.4.6 犯罪・改ざん（販売店）

1.4.6.1 消費者の防止策

(1) 通販

- **各種取引記録の保存**
  電話、申込、解約（クーリング・オフ）等の取引記録（注文書・納品書等）
- **クレジットカードの利用（利用明細書の保管）**

(2) EC

- **各種取引記録の保存**

---

[11] OCR（Optical Character Reader）光学式文字読み取り装置。文字等を直接、機械に読み取らせるもの。

注文の内容を記した送信メール、店舗からの受注確認のメール等

- **クレジットカードの利用（利用明細書の保管）**

1.4.6.2　販売店の防止策

(1) 通販

- **ハード、ソフト、運用を含めたセキュリティ強化**
- **個人情報・金融情報の取扱い管理ポリシーの策定と実行**
- **適切な人事政策**

(2) EC

基本的に通販と同様である。

1.4.7　犯罪・コンピュータウィルス

1.4.7.1　消費者の防止策

(1) EC

- **ダウンロード時のウィルスチェック**
- **万一に備えてのデータバックアップ**

1.4.7.2　販売店の防止策

(1) EC

- **ウィルス対策ソフトの導入**
- **外部からのアクセス制限**
- **万一に備えてのデータバックアップ**

1.4.8　犯罪・不正アクセス（通信途上の盗み見）

1.4.8.1　消費者の防止策

(1) 通販

- **ＦＡＸ送信時の電話番号の確認、送信後の再確認**
- **はがきの見える部分に安易に個人情報を記入しない**
- **封書の利用**

(2) EC

- **メールアドレス入力ミスの注意と確認**
- **メール送信フォームでの送信**
- **個人情報を送信する際には必ず暗号化されている環境で行う（ＳＳＬ等）**
- **セキュリティに信頼のおけない店舗への個人情報の送信を避ける**

1.4.8.2　販売店の防止策

(1) 通販

- **封書形式による注文書の提供**
- **隠蔽シール形式のはがきの提供**

(2) EC

- **メール送信フォームによる受注**
- **暗号化通信の提供**

1.4.9　犯罪・不正アクセス（消費者のコンピュータ）

1.4.9.1　消費者の防止策

(1) EC

通常、ダイアルアップを利用したインターネット接続において個人のコンピュータが不正アクセスを受けるというのは考えにくい。

しかし万が一に備えて、データのバックアップをまめにとっておくとともに、個人のプライベートな情報を不用意にコンピュータに保存するのは避けた方が懸命である。

1.4.10　犯罪・不正アクセス（販売店のサーバ）

1.4.10.1　消費者の防止策

消費者自身が行う防止策は無い。

1.4.10.2　販売店の防止策

(1) 通販

- **社内運用規定の確立（顧客情報を閲覧できる従業員を限定する等）**
- **販売店従業員教育の徹底**

(2) EC

内部犯行の防止・防衛策の他に

- **ファイアウォールの設置、アクセス制限等**

1.4.11　故障・事故（ネットワークダウン）

1.4.11.1　消費者の防止策

(1) 通販

- **複数の情報入手チャネルを用意する**
  （電話・ＦＡＸ、公衆電話、移動通信網、放送、ＣＡＴＶ、郵送、広告・チラシ等）

(2) EC

- **信頼の置けるＩＳＰと契約する**

- **複数のＩＳＰと契約する**

1.4.11.2 販売店の防止策

(1) 通販

- **複数の情報発信チャネルを準備する**
  （電話・ＦＡＸ、公衆電話、移動通信網、放送、ＣＡＴＶ、郵送、広告・チラシ等）

(2) EC

- **複数のサイトに情報発信のサーバを用意する**
- **信頼の置けるＩＳＰと契約する**
- **複数のＩＳＰと契約する**
- **配送障害に関する取り決めを作る**
- **ネットワーク障害対策を実施しているモールに出店する**
- **ダウンロードが中断した場合に、中断点からの継続再送を可能にする**

1.4.12 故障・事故（販売店のサーバダウン）

1.4.12.1 消費者の防止策

(1) 通販

- **注文内容の保存**

(2) EC

- **注文内容の保存**
- **デジタルコンテンツの場合は、配送障害に関する取り決めの確認**

1.4.12.2 販売店の防止策

(1) 通販

- **データのバックアップ運用**
- **高信頼システム構成**

(2) EC

- **データのバックアップ運用**
- **冗長構成[12]により、データの安全性を高める**
- **高信頼システム構成**

[12] 通常は使用しないが、万が一に備えてシステム等を２重化すること

1.5　解説　解決方法

ここでは、損害にかかる証拠性、追跡の可能性、具体的な解決方法の違いを解説する。

1.5.1　犯罪・詐欺（販売店のなりすまし）

1.5.1.1　証拠性・追跡可能性

通販においては販売店のちらしやカタログといった物理的な証拠が残り、これらの証拠から販売店を追跡することが可能である。また新聞チラシやラジオ、ＴＶ広告の場合は、新聞販売店や放送局への問い合わせも有効といえる。

対してＥＣにおいては物的な証拠が残らず、電子的な証拠のみとなり信憑性が低いことが特徴といえる。モール等に出店している販売店においては、モール運営者へ相談することにより追跡可能な場合もあるが、販売店が独自でサーバを立ち上げ出店する場合は特に追跡が困難である。

1.5.1.2　解決方法

消費者の金銭的な損害に対しては、通販、ＥＣともに、販売店に対して売買契約の取り消し、代金支払済みの場合は代金返還を求めることになる。しかしながら悪意の販売店に対する代金返還請求は、販売店が支払いに応ずる可能性が低いことが問題である。

一方クレジットカード等による割賦販売の場合は、消費者はカード会社等に対して支払停止の抗弁を主張することができ、銀行振込等の代金前払いと比較し消費者に救済の余地があることが特徴といえる。

販売店の信用失墜による損害に対しては、通販、ＥＣともに悪意の販売店に対する損害賠償請求をもって解決するしか方法は無く、いかに悪意の販売店を追跡するかがポイントになる。

1.5.2　犯罪・詐欺（消費者のなりすまし）

1.5.2.1　証拠性・追跡可能性

通販においては注文書（郵便・ＦＡＸ）等の物理的な証拠が残り、なりすました消費者を判断できる材料として有効である。電話による注文においては、注文書といった物理的な証拠は無いものの、受注の際の会話が録音されていれば証拠となりやすい。また郵便や電話・ＦＡＸの送信経路も調査によっては判明することが多い。また物流が伴う商品においては、配送先住所からトレースが可能である。

一方ＥＣにおいては電子的なデータを以ってなりすました消費者を特定することはほぼ不可能であり証拠性が低いことが特徴といえる。またインターネット上の送信経路においても必ずしも一定しないため、データの追跡が困難なことが特徴といえる。物流が伴う商品においては、通販同様配送先住所からのトレースが可能であるが、デジタルコンテンツのダウンロードのような物流が伴わない商品においては、ネット上の送信経路からのトレースがほぼ不可能であり、ＥＣの特徴といえる。

1.5.2.2　解決方法

なりすまされた消費者の金銭的損害は、通販、ＥＣともにクレジットカードの紛失、盗難が原因による不正利用については、クレジットカード会社への連絡ならびに警察署への届け出によりクレジットカード盗難保険が適用される。しかしながらカード番号や有効期限等個人情報のみの漏洩に起因する不正利用分については、上記盗難保険は適用外である。

しかしクレジットカード番号等個人情報の漏洩原因が、消費者の重大な過失による場合は、消費者が損害を負担することも考えられる。

一方ネット上でのハッキング等が原因によるなりすましにおいては、消費者に過失が存在したかを確認し、またその事実を立証するのは困難である。当然にこれらに起因する損害についてもクレジットカード盗難保険は適用外である。

販売店における金銭的損害は、通常通販、ＥＣともにクレジットカード会社との加盟店契約において利用者の本人認証は販売店の責任としており、なりすました会員によるクレジットカードの利用代金は販売店が損害を負担することになる。

販売店は悪意の第三者に対して損害賠償請求を行うことはできるが、仮に商品配送記録等から悪意の第三者を追跡したとしても損害賠償請求に対し悪意の第三者が必ず支払いに応ずるとは限らず、販売店はこれらの損害に対して一定のコストを見込んでおく必要がある。

1.5.3　過失・入力ミス（消費者）

1.5.3.1　証拠性・追跡可能性

通販、ＥＣとも消費者の記入ミスやイメージ違い等による金銭的損害は、販売店のちらしやカタログ、ホームページの説明不測に起因するものか、それとも消費者の単なる入力ミスや勘違いによるものか、これらの原因を追求し証明することは困難である。

1.5.3.2　解決方法

通販、ＥＣともに消費者の記入ミスや勘違いによる損害は、原則として消費者がその責任を負うことになると考えられる。

しかしながら記入、入力ミスや勘違いが、販売店のちらしやカタログ、ホームページの不備、意図的な説明不足等に起因する場合においては、販売店に対して返品取り消しを求めることにより解決する場合がある。

販売店においては、消費者の悪意をもった行為を除いては、極力商品の返品交換に応ずることが最良の解決方法といえる。

1.5.4　過失・入力ミス（販売店）

1.5.4.1　証拠性・追跡可能性

通販においては、誤情報の記載されたちらしやカタログの現物が証拠として残る。ＥＣにおいてはホームページの画面コピーやメールの画面コピー等が証拠となるが、電子的なデータは改ざんや複製が可能なため証拠としての信憑性が低いことが特徴といえる。

1.5.4.2　解決方法

ちらし、カタログ作成時点における販売店の過失・入力ミスは、消費者に正しい案内を知らせるために郵便やＦＡＸ、電話を利用することになるが、対象となる全ての消費者に対し案内することは金銭的にも体力的にも負担がかかる。

一方ＥＣにおいてはリアルタイムでのホームページ訂正が可能であり、消費者に対して電子メールを利用することにより金銭的にも体力的にもほとんど負担をかけずに案内できることは特徴といえる。

なお通販、ＥＣともに販売店の取り扱いミス、操作ミスによりデータが消失したり、システムがダウンした場合のデータ復旧費用、お詫び広告などの費用は、コンピュータ総合保険ならびにネットワーク中断保険等でカバーが可能である。

1.5.5　犯罪・サービス不能攻撃（販売店）

1.5.5.1　証拠性・追跡可能性

通販、ＥＣともに送られた注文書や注文データが、真正なる注文かそれともいやがらせによるものかをその１つのデータだけをもって判断することはできない。現実の解決策としては、特定の消費者からの複数の注文を販売店がチェックを行うことになる。

送付された注文書や注文データの保存記録から、悪意の第三者を追跡することになるが、当然ながらサービス不能攻撃を行う第三者を追跡することは困難といえる。

1.5.5.2　解決方法

販売店において、休業損害が発生した場合は、悪意の第三者に対して民事訴訟・損害賠償請求により解決を計ることになるが、上記の通り第三者を追跡し確定させることは困難といえる。

なお販売店の休業による費用・利益損害はコンピュータ総合保険、ネットワーク中断保険によりカバーが可能である。

1.5.6　犯罪・改ざん（販売店）

1.5.6.1　証拠性・追跡可能性

通販においては消費者の注文書自体が売上票を兼ねるケースが多く、注文書の改ざんは売上票が無効となる可能性が高い。一方ＥＣにおいては消費者の注文データのみが証拠と

なるため、改ざんが販売店によってなされたものかを証明することは困難といえる。

1.5.6.2　解決方法

消費者の金銭的な損害に対しては、通販、ＥＣともクレジットカード利用においては「利用覚え無し」「金額相違」に基づき、支払いを拒否することになる。クレジットカード会社は訴えに基づいて販売店へ売上を返却することになる。

販売店の従業員による不正な売上の捏造に基づく損害は、通販、ＥＣともに販売店が身元信用保険を付保することによりカバーすることが可能である。

1.5.7　犯罪・コンピュータウィルス

1.5.7.1　証拠性・追跡可能性

商品にウィルスが混入していたことは、ウィルスチェックプログラム等により判明するが、ウィルスが原因による消費者ならびに販売店の各種損害を証明することは困難といえる。

1.5.7.2　解決方法

商品においては、該当商品の返品、交換により解決する。

消費者のウィルスが原因による各種損害において、販売店のウィルスが原因として損害賠償を請求することは原因の証明、確定が困難であり非現実的といえる。

なおウィルスの感染が原因となる販売店のデータ復旧費用、ハードウェア購入費用、ネットワークの中断等直接的な損害に対しては、コンピュータ総合保険、ネットワーク中断保険によりカバーすることが可能である。

1.5.8　犯罪・不正アクセス（通信途上の盗み見）

1.5.8.1　証拠性・追跡可能性

通販においては、郵便、一般公衆回線を利用することにより通信経路が比較的確定しやすい。一方ＥＣにおいては販売店に送信する個人情報がインターネット上において、どのような経路で誰に盗聴されたかを確認し立証することがまず不可能である。

1.5.8.2　解決方法

通販、ＥＣともに通信途上の盗み見に起因する第三者の不正利用は、その原因を確認し立証することは困難といえる。通信途上の盗み見の原因が消費者にあるのか、郵便や電話、ＩＳＰ等の通信事業者に起因するのか、それとも販売店のセキュリティに起因するのか特定させることはまず不可能といえる。

消費者の金銭的な損害に対しては、クレジットカード会社に対し「利用の覚え無し」として支払いを拒否することになる。

1.5.9　犯罪・不正アクセス（消費者のコンピュータ）

1.5.9.1　解決方法

リスク環境の解説にて述べたとおり、ダイアルアップ接続によるＩＳＰへの接続が一般的であるため、消費者のコンピュータが不正アクセスを受けるケースはほとんど無いといえる。

しかしながら不正アクセス以外でもコンピュータのデータが消失したりハードウェアが故障するケースは十分に考えられるため、消費者自身によるこまめなデータのバックアップがコスト的にも最良な解決策といえる。

1.5.10　犯罪・不正アクセス（販売店のサーバ）

1.5.10.1　証拠性・追跡可能性

外部からのサーバへの不正アクセスにより、個人情報が漏洩し第三者のなりすましが考えられるが、不正利用の原因が販売店サーバへの不正アクセスによるものかを確認し立証することは困難といえる。同様に販売店従業員の不正アクセスにおいても確認、立証は困難である。

1.5.10.2　解決方法

不正アクセスに起因する消費者の金銭的な損害に対しては、クレジットカード会社に対し「利用の覚え無し」として支払いを拒否することになる。

なお販売店従業員による内部犯行が立証できれば、その販売店および従業員に対して損害賠償請求が可能である。

1.5.11　故障・事故（ネットワーク・サーバダウン）

1.5.11.1　証拠性・追跡可能性

ネットワークや販売店サーバダウンによる消費者の逸失利益の損害額を算出することは困難である。

1.5.11.2　解決方法

ネットワークや販売店サーバダウンが原因の消費者の利用機会喪失は、損害額を算出することが困難であり、賠償請求を行うことは非現実的である。現実は販売店へのクレームによる解決となる。

またオンライン証券取引のようなサーバダウンによる利用機会の損失が直接的な損害につながるサービスにおいては、通常約款等で機会損失等による損害賠償責任は負わないと規定されている。

販売店の損害のサーバダウンによる休業損害は、ネットワーク中断保険によるカバーが可能である。データの復旧費用については、コンピュータ総合保険によるカバーが可能で

ある。

1.6　まとめ

1.6.1　法律

そもそも消費者向けのＥＣは、わが国の法律の枠組みでは通信販売の１つの形態とされるため、基本的にビジネスに適用される法律に大きな違いが無いことは明確である。訪問販売法や割賦販売法等消費者保護に関する法規制、広告・販売促進活動に関する法規制、商品・業務等の特性による法規制はＥＣにおいても通販と同様に適用される。

しかしながらＥＣにおいては電子的なデータの交換という新しい方法を用いることにより従来からの通信販売とは異なった特質があり、法律の解釈、適用において問題が生じている。

特に書面要件の問題（電子データを書面として代替可能か）、本人認証の問題（なりすまし）、契約成立に関する問題（取引データの消失、改ざんや遅延）等はＥＣ特有の問題であり、今後技術的に解決を図ると共に、関連する法制度の整備が望まれているところである。

現時点においては、ＥＣに参加する販売店ならびに消費者が、想定される法的リスクを十分に認識したうえで行動することが要求される。

また今回の比較においては特に国内取引のみを対象として比較を行っているが、ボーダーレスであるＥＣは国際間取引における法的問題も生じてくることを忘れてはならない。

1.6.2　リスク環境

従来からの通信販売においては、ビジネス立ち上げの為に仕組みも大掛かりになりがちでありコストも嵩む傾向があった。しかしＥＣにおいては環境により違いはあるもののサーバ１つで誰でも手軽に安価でビジネスを始めることが可能となった。

しかしながらその手軽さは消費者や販売店だけのものではなく、悪意の第三者のＥＣへの参入も容易にすることにもなりかねない。

特にＥＣにおいては個人情報、金融情報をオープンなネットワークでやりとりするために、絶えず第三者に盗聴されたり改ざんされたりする危険性に晒されている。また販売店のサーバがインターネットと接続されるため、個人情報が格納されたサーバをハッキングすることにより一度にかつ大量に個人データを不正に入手することが可能となる。

通信販売においてはこれらのリスクは皆無もしくはあまり問題とならなかったが、ＥＣにおいては大変重要な問題であり、一度問題が発生すると大きな損害につながることを認識する必要がある。

一方では、内部犯行による個人情報漏洩が問題となっている。これは通販、ＥＣともに起こりうるリスクである。安全なＥＣ環境を構築するためには、内部管理の徹底、社員教育が望まれるところである。

1.6.3　損害の証明・解決方法

通販においては郵便やＦＡＸといった物的な証拠が残るが、ＥＣにおいては購入の意思表示や承諾が全て電子データで行われるため、データの改ざんや複製を容易に行うことができる。そのため電子データは証拠としての信憑性が低いことが問題となる。

これらの問題は電子署名、電子認証といった技術と法制度の整備をもって今後解決されていくことと思われ、今後の動向を注意深く見守ることが必要である。

2 企業とECリスク

2.1 企業を取り巻くリスク

2.1.1 企業リスクの考え方

企業におけるＥＣリスクを考えるにあたり、ここでは概括的なイメージを理解しやすいように１つの例をあげて説明する。表 2-1 は、米国のオンライン取引に関係する企業に対してリスクマネージメントを行った際の企業リスクについての例である。

一般的にリスクは、「当事者リスク（First PartyRisk）」と「第三者リスク（Third Party Risk）」とに分けることができる。当事者リスクとは企業が直接被った損害であるのに対し、第三者リスクとは被害者の損害を賠償する責任が企業に課せられており、企業がその責任を履行することによる損害のことである。この分析では、「当事者リスク（First Party Risk）」と「第三者リスク（Third Party Risk）」に大きく分類することから始め、次に当事者リスクについては営業中断損害とコンピュータ犯罪に係る損害、第三者リスクについては専門職業人としての賠償責任、特許・著作権・商標などの知的財産権に対する賠償責任、名誉毀損・プライバシー侵害・不公正競争など広告関連の活動に対する賠償責任をＥＣ上の企業リスクとして特徴付けている点が注目に値する（無論、企業活動を行う上ではこの他にも単なる物的損害や人的損害も含まれる）。

2.1.1.1 当事者リスク

(1) 営業中断（休業）リスク

① 所有財産への損害による営業中断

A. 所有財産への物的損害による営業中断

サーバ破損による営業停止、通信回線切断による営業中断など

B. 所有財産への非物的損害（不正アクセス・ハッキングなど）による営業中断

顧客データ消失による営業停止、ソフトウエアの損傷による営業停止、システム障害・停止による営業中断など

② 所有財産以外の事故・障害による営業中断

一般通信回線の障害、顧客システムの故障など

(2) 内部・外部コンピュータ犯罪

① コンピュータ犯罪

A. コンピュータを使用した盗難

- **コンピュータを使用した有形財産の盗難（金銭、有価証券など）**
- **コンピュータを使用した無形財産の盗難（データ、プログラム、電子マネーなど）**

B. 金銭上の利益は意図されないコンピュータの利用を含む悪意的行為により発生する損失

- **無形財産の損失または損害、市場での信用損失など**

② 従業員又は非従業員による物理的な盗難

A. 有形財産の盗難

- **金銭、有価証券、その他の財物など**

B. 無形財産の盗難

- **データ、プログラム、電子マネーなど**

2.1.1.2 第三者（賠償責任）リスク

(1) 業務上の専門職業人としての損害賠償責任

① 提供するサービスの停止と中断による損害賠償
② 提供するサービスの欠陥による損害賠償
③ 提供するソフトウエアの欠陥による損害賠償
④ プライバシーや機密情報の漏洩
⑤ 契約上負担することが予想されるあらゆる損害賠償　など

(2) 知的財産権侵害に関する損害賠償責任

① ハードウエア、デバイス等の特許権侵害
② ソフトウエアの特許権侵害
③ ソフトウエアの著作権侵害
④ 企業秘密侵害　など

(3) コンテンツと広告に関連する損害賠償責任

① 中傷や名誉毀損
② 著作権侵害
③ 商標侵害
④ プライバシー侵害
⑤ 広告権、アイデアの横領
⑥ 人格権の侵害・他人の権利の侵害　など

表 2-1　米国企業リスク調査サンプル

主な危険				
当事者（または直接）リスク		第三者（または責任）リスク		
営業中断	内部・外部コンピュータ犯罪	業務上の専門職業人としての賠償責任	知的財産	コンテンツと広告関連の責任
1．所有財産への損害によるもの 1）所有財産への物理的損害 サーバ破損、通信回線切断 2）所有財産への非物理的損害 （不正アクセス、ハッキングなど） 顧客データ消失、ソフトウェアの損傷、システム障害・停止 2．所有財産以外の事故・障害によるもの 一般通信回線の障害、顧客システムの故障	1．コンピュータ犯罪 1）コンピュータを使用した盗難 ・コンピュータを使用した有形財産の盗難（金銭、有価証券等） ・コンピュータを使用した無形財産の盗難（データ、プログラム、電子マネー等） 2）金銭上の利益は意図されないコンピュータの利用を含む悪意的行為により発生する損失 ・無形の財産の損失または損害、市場での信用喪失など 2．従業員または非従業員による物理的な盗難 1）有形財産の盗難 ・金銭、有価証券、その他の財産 2）無形の財産の盗難 ・データ、プログラム、電子マネー等	1．提供するサービスの停止と中断 2．提供するサービスの欠陥 3．提供するソフトウェア上の欠陥 4．プライバシー侵害や機密情報の漏洩 5．契約上予想されるあらゆる損害賠償	1．ハードウェア、デバイスなどの特許権侵害 2．ソフトウェアの特許権侵害 3．ソフトウェアの著作権侵害 4．企業秘密の侵害	1．中傷や名誉毀損 2．著作権侵害 3．商標侵害 4．プライバシー侵害 5．広告権、アイデアの横領 6．人格権侵害・他人の権利の侵害

2.1.2　ＥＣのリスクマネジメントのあり方（企業リスクの考え方）

次にＥＣ上の企業リスクに対するリスクマネージメントの方法として、昨年の欧州調査におけるＤＲ．ポールドーレー[13]の講演より、電子商取引（ＥＣ）のリスクマネジメントのあり方（企業リスクの考え方）としてまとめた。

2.1.2.1　ＥＣの４段階のステージとリスクマネジメント

(1) ＥＣの４段階のステージ

一口にＥＣのリスクマネジメントといっても、そもそもＥＣのあり方自体が、その初期的な導入と本格的な導入では大きく異なり、そのリスクのあり方もまた大きく異なってくる。よって、リスクマネジメントを行うには、まずＥＣの導入段階毎にステージ分けを行い、そのステージ毎にリスクマネジメントのあり方を考える必要がある。ＥＣの初期的導入から本格的導入までは次の４つの段階に分けることができる。

① 第１段階: インターネットアクセス

最も初期的な段階である。例えば電子メールを利用して情報交換を行ったり、インターネットをブラウジングし、ビジネスに必要な情報を収集するといったことが挙げられる。この段階では、あくまでも業務の一部を電子的に行っているだけである。電子メールでの情報交換も、あまりクリティカルな情報を交換することはなく、自ら能動的に情報発信を行わない。

本段階では、ネットワークのダウン等が発生しても、代替手段の確保が比較的容易であり、またクリティカルな情報を取り扱わないことから、そもそも外部から不正アクセスされる恐れが少ない。また仮に不正アクセスされても、直接的に実害には結びつかないことから、リスクの程度は大変小さい。

② 第２段階:Webサイト

本段階では、情報発信を能動的に行い顧客にアクセスを開始し始める段階である。例えば、自らＷｅｂサイトを立ち上げ、自社のサービス・商品について顧客向けに情報発信を行うこと等が挙げられる。

本段階では、依然ＥＣはビジネスプロセスの補助的な手段という位置づけであり、比較的リスクは小さい。

③ 第３段階: ライブデータ、トランザクションズ

本段階ではＥＣを本格的にビジネスプロセスに導入し始める段階であり、ＥＣがなくては当該ビジネスそのものが成り立たない段階である。例えばインターネットを通じ顧客にデータベースを利用させて利用に応じて料金を徴収したり、商品・サ

---

[13] ＤＲ．ポールドーレー
バークレー銀行の運用リスク管理の国際責任者であり、同行のインターネットバンキングの立ち上げを指揮した。ＥＣのリスクマネジメントの権威でもあり、米国下院でＥＣのリスクマネジメントのあり方について講演を行った経験もある。

ービスの決済など顧客と実際の取引を行うこと等が挙げられる。

本段階ではＥＣがビジネスに浸透しているので、仮に事故によりＥＣが利用できなければビジネスがストップしてしまう恐れがあることから、本段階のリスクはやや大きくなってくる。

④　第４段階: インテグレイティドプロセス

本段階は、顧客への情宣、顧客からの受注、サービスの提供、決済等、一連のビジネスプロセス全ての手続きを電子化する段階である。さらにバックオフィスでの判断までＰＣが実施すると全面的にＰＣに依存することとなる。本段階では、ＥＣがなくてはビジネスそのものが成り立たない。本段階では、大きなリスクが存在する。

(2) 各段階のリスクとリスクマネジメント

①　第１段階のリスク

第１段階のリスクとしては次のようなものがある。

- コンピュータウイルス等
- 非合法な情報（ポルノ、著作権違反の情報等）
- システムの誤った利用
- 電子メールの利用によって発生する法的な責任

この段階では外部ネットワークとの接続にあたり、最低限のセキュリティ対策が必要である。具体的には、ファイアウォールやウイルスチェック機能の整備など外部からのアクセス、ウイルス、ハッキングやスパム等に対する対策を、システムや業務運用面から整備することが重要である。

②　第２段階のリスク

第２段階のリスクとしては次のようなものがある。

- サイトのハッキング
- 非合法な情報（広告、誹謗中傷）
- 不完全な情報
- システムダウンを意図したアタック
- Misrepresentation（無権限者によるなりすまし、著作権の侵害、トレードマークの無断使用）

この段階では、付加価値を有する情報を取り扱うことから、情報の PIRACY（窃盗）対策が重要である。つまり本来有料で提供しているデータベース、ソフトウェア等が盗まれてしまうことである。例えば、昨今ＭＰ３による音楽コンテンツのネット上での提供が可能になっているが、一方で音楽コンテンツのコピーも容易になっていることから、Electronic Theft 対策が必要である。

また、無権限アクセス（不正アクセス）も大きな問題である。無権限者が自分の会社の名前で勝手に取引を行ってしまう場合もあり、無権限アクセスを制御する必

要がある。一般的にはＩＤやパスワードなどによりアクセス権限を有する者かどうか識別しているケースが多いが、電子認証書を利用することにより更に安全性の向上を図ることが可能である。

③　第3段階のリスク

第３段階のリスクとしては次のようなものがある。

- 内部システムへのハッキング
- クレジットカード情報の盗難
- システムの誤使用
- なりすまし、詐欺

この段階ではシステムがきちんと作動すること（Availability）が重要である。インターネットは１日 24 時間、週 7 日間、年 52 週動き続ける必要があり、またそのキャパシティも需要に十分応えられるものでなければならない。一方、意図的にシステムダウンを狙った“ syn ”アタックというものもあり、注意が必要である。

また、仮にネットワークがダウンしてしまった場合を想定した対策も重要である。従って、ネットワークシステムの二重化や情報のバックアップ等を行っておく必要がある。

④　第４段階のリスク

第４段階のリスクとしては次のようなものがある。

- ビジネス全体にリスクが及ぶ恐れ
- 詐欺、エラーズ＆オミッションが大問題になる

この段階では、システム的な対策とともに運用管理体制の構築が重要であり、更にその体制をチェックするための監査が非常に重要である。

また、ＥＣのリスクの影響が外部顧客等にも及ぶ恐れがあり、場合によっては外部から法的な損害賠償を提起されることも想定される。法的な責任については、ＥＣという新しいビジネスには未確定な部分が多く、その対策には注意が必要となる。例えば、どの国の規制が関係するのかという問題もある。国によってはそのものの販売だけでなく広告するだけで違反となる国もある。

2.1.3　今後のＥＣの進展に伴なうリスク要素

現在起きているＥＣでのインターネット通販ビジネスは極めて初歩段階のものである。しかし、今後急速なインターネットの普及の中で、併行して新たな技術環境の変化、及びビジネス環境の変化がおきることは明白である。

この環境の中で各ビジネス プロセス、及びシステム内容は極めて複雑になり、これらに伴ない類推の範囲を超えた諸処のリスク要因を生み出しかねないという問題が新たに派生するであろう。

ここでは、どのような変化がリスク要因を生み出すのかを大枠で整理してみた。

2.1.3.1　インターネット人口の爆発的普及に伴なうリスク要因

(1) トラフィック増に伴なうリスク

① ネットワーク・システム系内での許容範囲を超えるトラフィックによるもの

- **システムが中断、不明取引内容の発生、二重発注の発生**
- **上記に伴なう利用者の不的確な操作でのシステム障害の発生**

② サーバ側系内でトラフィックの許容範囲を超えた同時発生による処理の不具合

- **サーバの停止**
- **回線処理能力範囲を超えたシステム停止**

③ 後方処理運用の許容量を超えた処理の発生

- **発注、決済処理、物流処理等の処理の大幅遅れに伴なうクレームの増大**
- **取引先側での受注、出荷、物流処理の遅れや混乱、それに伴なうクレームの増大**

2.1.3.2　ビジネス・モデルの新しい登場に伴なうリスク要因

(1) 中間業者（ブローカー、購買代理人、インターメディアリ等）の登場によるリスク

オークションビジネス、最低価格紹介ビジネス、評価ビジネス等がネット上に新たに登場し、取引の初期段階から実際の購入時とは異なる業者との間で取引を行う等の新しいビジネス・モデルが次々に登場する事から、１つの取引が複数の取引を発生させる事になる。これらの場合にはこれまでと異なるスキームでのネット間での処理が発生し、新たなリスクを生じる可能性が増大する。

消費者にとっての商品の保証責任が不明確になり、且つネット取引のどこに不正を働く業者が存在しているのかも不明になる事から、それらを適正化する共通スキームが必要となる。

(2) 多角的なメディアの適用によるサービスの高度化等に起因するリスク

携帯端末、簡易メール端末等を連携したサービスの登場に伴ない、セキュリティーレベルの低下が生じる可能性がある。

(3) 新ネットワークサービスの登場に伴なうリスク

超高速での無線サービスを適用した通信インフラ等での問題要因の１つとして、何らかの無線障害が発生する頻度が増大する可能性が存在し、この場合には通常のトラフィック条件でも端末側は停止する。

消費者が取引の途中（発注後）新しい回線サービスを受けたり、或いはインターネット サービス業者の変更をするケースでの混乱から生じる問題発生の可能性が増大する。

(4) インターネットセキュリティーでのリスク（連携取引における認証サービス管理からみたリスク）

多段階ネットワーク回線環境でのセキュリティーホール発生増大のリスクである。

１つの取引でのネットワークにより接続される業者の数が増大する事で、一定レベルのアクセスコンロールや、暗号化処理基準を維持する事は困難度を増す。これに伴ない、不正アクセスの可能性の増大や、不正な個人情報の入手発生機会の増大要因ともなる。

2.2　米国・欧州におけるＥＣ関連の判例に見る企業のＥＣリスク

ＥＣ上の企業リスク、特に賠償責任損害を考える上でＥＣ先進国である米国のＥＣ関連の判例を見ることは大変参考になる。ここでは米国・欧州におけるＥＣ関連の代表的判例について紹介する。（参考文献：Kent D.Stuckey **著「**Internet and Online Law**」）**

2.2.1　米国におけるＥＣ関連の判例

2.2.1.1　著作権侵害

米国では、インターネットなど様々な情報が自由に行き交う環境の中で、著作権の侵害についても注目され、現実にこれまでいくつかの訴訟が起こされてきた。米国においてはインターネット上の著作権の侵害について、著作権の直接侵害であるのか寄与侵害であるのかという法的解釈が問題になってきたようである。

・直接侵害direct infringement

直接的な行為者による侵害である。直接的行為者とは、侵害を構成するコピー作成、実演、展示などを実際に遂行し、又はかかる侵害行為を許可した者をいう。直接的侵害者であると訴えられた者の責任の有無を判断する、著作権法上の基準は厳しいものであり、侵害にあたることを知っていたことや侵害の意図があったことを立証する必要はない。しかしながら、最近のオンライン環境のもとで下された判決だけに基づけば、オンライン環境上での直接責任を認定するには申し立てられた特定の侵害行為に関して被告側に何らかのsome element of volition or causation（志作用または因果関係のある要素）がなければならない、という考え方ができるように思われる。

・寄与侵害contributory infringement

他者の侵害行為に寄与するという不法行為である。寄与責任は、ある者が直接侵害を行い、その者に対して寄与侵害者が故意に実質的援助を与えたことを要件とする。寄与侵害者は直接侵害者と何らかの関係を持っている必要はないが、侵害行為に該当することを知っており、且つ、侵害行為に実質的に参加していることを要する。

２つの主な違いは直接侵害が侵害にあたることを知っていたことや侵害の意図があったことを必要としないが寄与侵害は侵害行為に該当することを知っていたことを要する。

著作権の侵害に関する裁判は、著作権を侵害している著作物をユーザーが掲示することができるＷｅｂサイトやＢＢＳを提供した小規模サービス・プロバイダーに対して行われている。こうした裁判のほとんどは、法廷での争いが長期化する前に解決されているため、控訴裁判所がこうした問題について裁定する機会はまだ一度もないが、地方裁判所がオンラインサービスプロバイダー（ＯＳＰ）の責任問題に関して下した判決は非常に多い。

(1) プレイボーイ・エンタープライズ社対フレナ事件

① 事件の概要

プレイボーイ・エンタープライズ対フレナ事件は、ＯＳＰの責任問題を扱った最初の裁判で、裁判所は、プレイボーイが著作権を所持する写真の許可のない複製を提示したオンラインＢＢＳの主催者であるサービス・プロバイダー（フレナ）は、著作権侵害に対して直接責任を負うと判決を下した。

裁判所は、フレナはそうした写真を掲示し、加入者が自身のコンピュータに著作権で保護された著作物をダウンロードできるようにしたという理由により、著作権の直接的な侵害に責任があると評決した。

被告ジョージフレナは、フロリダでテックス・ウェアハウスという名のオンラインサービスを運営していた。フレナのサービスは月額 25 ドルの会員制有料サービスであり、会員は自由に画像などをアップロードでき、アップロードされた画像はすぐに会員すべてによりダウンロードできるようになっていた。訴訟における著作権の主張は、著作権で保護されているプレイボーイ所有の写真のオンラインでの使用によるものだった。プレイボーイの写真は現実に被告の複数の顧客によりダウンロードされた。フレナの抗弁は、彼自身はプレイボーイの写真をＢＢＳにアップロードしておらず、彼の知らない間にサービスの加入者が著作権で保護された画像をアップロードしていた、というものだった。フレナはさらに、召喚状を受け取り、侵害の可能性にはじめて気付いた時点で当該写真を削除し、それ以降は原告の著作権保護対象物がさらにアップロードされることのないよう自分のシステムを監視していると主張した。

② 裁判所の判断

裁判所は、事実審理を経ない判決で、プレイボーイの当該写真の著作権を認めた上で、オンライン上の画像が原写真に実質的に類似しており、またその写真が原告の雑誌で一般に入手できることからコピー行為が推論されうるとした。

裁判所は、フレナが著作権侵害に直接的な責任を負うとした。その理由は幾つかの写真は編集が施され、プレイボーイ社の商標が削除され、フレナの広告が付け加えられていたなど、フレナは著作権侵害写真を組み込んだ「製品」を作成したと判断され、フレナが主張したような侵害行為を知らなかったことは、重大な事実問題とはならなかった。原告の写真がフレナのＢＢＳに存在していたことを証明する明白な証拠は、裁判所が直接侵害を認定するのに十分な関与の証拠であった。

直接侵害の厳格責任基準から、裁判所は著作権侵害を実際に知らなかったというフレナの抗弁を退け、「著作権侵害を認定するのに侵害の意図は必要とされない」と判決を下した。

しかし、その後の判例では、裁判所は、プロバイダーが著作権侵害行為に気がつかなかった場合に、フレナのような直接責任に関する判決を支持していないようで

ある。その代わり、サービス・プロバイダーの行為は、侵害行為に該当することを知っていることを要する寄与責任理論の下で判断されている。この考え方が明らかにされたのが次のリリジャス・テクノロジー・センター対ネットコム・オンライン・コミュニケーション・サービス訴訟である。

(2) レリジャス･テクノロジー･センター対ネットコム社事件

① 事件の概要

この訴訟は、ＯＳＰが加入者の不正なアップロードの責任を負うべきか否か、そして負うべきだとすればいつ責任が発生するのか、という問題に関する重要な判決であるとされている。

リリジャス・テクノロジー・センターという宗教団体の元牧師アーリックがユースネットニュースグループのフォーラムで、リリジャス・テクノロジー・センターの批判をし、リリジャス・テクノロジー・センターが著作権を有する経典などの情報をアップロードして、これがネットコムのコンピュータに送信され、さらに世界中のユースネットニュースグループに送信されたというものである。裁判所は、被告のネットコムが著作権侵害に直接責任を負う判決を拒否し、寄与責任の原則を適用することが一層適切であると評決したものである。

② 裁判所の判断

裁判所は、ネットコムは、ユースネットの加入者から受信したメッセージをソフトウェアが自動的に転送するシステムを設置、維持し、そのシステム上に複製を一時的に保管した以外に、原告の作品の複製の直接の原因となった積極的などのような行動もとらなかったという理由に基づき、ネットコムの直接的な侵害を認めることを拒否した。さらに裁判所は、こうした複製はシステムの運営に不可欠なものであり、some element of volition or causation（意志作用または因果関係のある要素）が直接責任の事実認定に必要であるとした。裁判所は、セルフ・サービスの写真複写サービスとの類似性を引き出して、直接責任を課すことはできないとの結論を下し、直接侵害の成立要件は「何らかの意思又は原因の存在であるが、被告のシステムが第三者により単にコピーを作成するために使用される場合にはこれは欠如している」として、ネットコム社が原告から中止通告を受け取った後に自社のコンピュータ・システムからアーリックの投稿物を削除しなかったことは、さらにコピーが作成される原因となりかねなかったことは明らかであるものの、直接責任を立証することはできないとした。

その上で、裁判所は、ネットコムが著作権侵害について知っていた、またはそれについて通知を受けていたことを原告が証明できれば、ネットコムは著作権侵害の寄与に対して責任を負うと判断し、著作権侵害に対するネットコムの認識に争点があると結論を下した。原告は、違法に掲示された著作物の少なくとも一部に原告の著作権に関する但し書きが含まれていて、原告がアーリック氏の著作権侵害活動に

ついてネットコムに通知した後も、ネットコムは著作権を侵害する著作物を掲示し続けたことを示す証拠を提出していた点に問題があると考えられた。

一方、寄与責任は、実際に不法行為を行わなかったが不法行為の遂行に実質的に寄与した者は寄与責任を負うべきであるというものであるという原則に、その根拠を有している。寄与責任の有無を判断する法的基準は、侵害の行為を知っていることと侵害の行為を実質的に援助していること（knowledge combined with substantial assistance）である。

裁判所はネットコム訴訟において、ネットコム社が侵害とされる行為を十分認識していたかについてネットコム社に極めて疑わしい問題が存在すると断定した。ネットコム社が具体的にそのような認識を有していた可能性がある期間とは、ネットコム社が原告の中止通告を受け取った日から、ネットコム社のサーバーに常駐していた当該ユースネットニュース・グループのコピーからアーリックの投稿物が自動的に削除された時点までとしている。

更に、寄与責任の「実質的援助」要件については、裁判所は「侵害にあたるか否かに関わらず、あらゆるユースネット投稿物を自動的に配信することを考慮したサービスを提供すること」は、ラジオ放送局が侵害にあたる放送内容を再放送することに似ており、侵害行為を中止させることも可能であったとして裁判所は、ネットコム社のアーリックの侵害行為への実質的な参加について事実審理に付すべき事実問題が存在しうるほどネットコム社は重大な役割を演じたと考えた。裁判所は、寄与責任の両要素は事実審理による解決を待たねばならないと判断した。

(3) フランク・ミュージック社対コンピュサーブ社事件

① 事件の概要

この事件は楽曲の著作権を集中管理する音楽出版社である原告フランクミュージックとハリー・フォックス・エージェンシーがＯＳＰのコンピュサーブを訴え、彼らの音楽著作物をＭＩＤＩフォーマットで収録した音声記録物を取り扱う同社コンピュータ・システムへのアップロード、保存、及びダウンロードに起因する侵害行為について直接的な責任を負うべきだとしたものである。訴状では、当該活動に関連したコンピュサーブ社の行為は原告のアンチェインドメロディーなど 900 に上る楽曲の著作権を侵害されたとした。

② 事件の決着

フランク・ミュージック訴訟は、和解により解決された。和解によれば、コンピュサーブの加入者が原告の歌の音声記録物をアップロードしても、コンピュサーブ社は、特定の侵害行為を実際に認知していない限り、責任を負わないことにされた。

訴訟で提起された責任問題についてはいずれの当事者も自分の立場を譲らなかったが、コンピュサーブ社が自社システムにアップロードされる著作物の著作権上の地位を実際に認識していない場合は同社に著作権侵害の直接的責任を負わせること

はできない、また負わせるべきでもない、という理解は再認識され和解に反映されていると考えられている。和解ではコンピュサーブは著作権侵害の責任は認めなかったものの、和解金を支払うこととしたようである。

コンピュサーブは、この和解を契機として、ハリー・フォックス・エージェンシー等とコンピュサーブへの楽曲のアップロードを許諾する包括的なライセンス契約を締結することとした。

2.2.1.2　解説　著作権の侵害

著作権法は、通常、著作権者へ、文書、言葉、作品（書いたもの、録ったもの、撮ったもの、電子的に写したもの）の複写を制限する独占的な権利を与えるものである。

大部分のコミュニケーションやオンライン活動は、著作権の保護を受ける要素があり、著作権法と関係するといっても良い。これは米国においては、ほとんどの形式の情報は著作権者が著作権表示をせず、米国著作権局に著作権登録をしなくても、米国著作権法により自動的に保護される背景があるからである。このため、インターネットなどオンライン上で流れる画像、音声、テキスト、ソフトウェアなどは著作権の保護を受けることとなる。

(1) 複製権、二次的著作物作成権（翻案権）、公的頒布権、公的実演権、公的展示権

ほとんどのオンライン活動は、米国著作権法の独占的な権利である複製権、二次的著作物作成権（翻案権）、公的頒布権、公的実演権、公的展示権などとの間で問題を提起する可能性がある。著作物がＲＡＭ、ハードディスクドライブ、またはその他のデジタル方式の記憶媒体に取り込まれ、複製されること、デジタル化プロセスにおいて著作物に創造的かつ表現的な内容が付け加えられること、コンテンツをアップロードしたりダウンロードしたりすること、ＷｅｂサイトやＢＢＳのコンテンツを見ること、などは全て複製行為、頒布行為、実演行為、展示行為と関係する。

(2) 独創性と固定性

米国著作権法に基づき著作権保護を受けることのできるものは、「既知の媒体か後に開発された媒体かに拘らず、それに固定されたものを直接的又は機械若しくは装置を用いて認識、複製、又は他の形態の伝達を行うことができる何らかの有形の表現媒体に固定された独創的な著作物」であるとされている。ある著作物がこれら２つの要件、すなわち「独創性」と「固定性」を満たしているか否かを判断するのはかなり容易で、これらの要件は普通は難なく満たされている。一般的に独創性については、ほんのわずかでも認められれば著作権法に基づく保護を受けることができる。芸術性や新規性は要求されない。たとえば、ユースネットのニュースグループ、ＢＢＳへアップロードしたメッセージ、チャットラインなどのオンライン・ディスカッションのフォーラムなども著作権の対象となるのに十分な創作性を有しているとも思われる。

ただし、単なる事実情報は著作権の対象とならず、データベースなどの事実の集積物・集合物は、データの配列と選択が必要な創作性を有している場合に限り著作権に

よる保護を受けることになる。たとえばインターネットのドメインネームやＵＲＬアドレスは、著作権による保護を受けないとされている。

伝統的な媒体の場合は普通、著作物は有形の表現媒体に固定されていなければならないという要件は簡単に満たされる。著作権法の規定によれば、著作物は、著作者によって或いは著作者の許可を得た上で「一時的な期間を超える期間のあいだ当該著作物を認識、複製、又は別の方法で伝達できるほどに恒久的或いは安定的な」媒体に組み込まれた時点で固定されたとされる。固定の形式、方法、媒体の種類は問われず、コンピュータディスク、テープ、ＣＤ－ＲＯＭによるデジタル形式で固定化された情報は、著作権による保護を受けるために必要な固定性を満たしていると考えられる。

さらに近年では、オンライン提供業者や利用者との関連において、裁判所は一時的性質を有するコピー（特にコンピュータのランダムアクセスメモリ（ＲＡＭ）のみに固定された著作物）が固定性要件を満たすか否かという問題に対処してきたが、これは固定の度合いが著作物性の裏づけと成りうるほど十分であるか否かという問題よりもむしろ、著作権侵害を構成するとされる著作物のコピーがＲＡＭ内に作成されたか否かという問題に関連している。あるコンピュータから他のコンピュータに送られ、それぞれのコンピュータのＲＡＭ上に存在する電子メールなどの電子ネットワーク通信のメッセージは、著作権の保護を受けるに十分な固定性を有していることになる。

一方、情報のオンライン送信自体は固定ではなく、送信される著作物が、その送信と同時に固定されない限りは著作権の保護を受けることはない。

どのような環境において、著作物をデジタル方式の記憶媒体に取り込み複製することやデジタル化プロセスにおいて著作物に創造的かつ表現的な内容を付け加えることができるのか。コンテンツをアップロードしたりダウンロードしたりすることやＷｅｂサイト又はＢＢＳのコンテンツを見ることなどの行為を行うことができるのか。更に、著作権者の明示の許可無しで行われたこれらの行為はどのような場合に著作権の侵害になるのか。これらの著作権法で規定されている独占的な権利がオンライン活動にいかに適用されるのかという問題は、著作権に関わるサービス提供者、ユーザ、政策立案者に激しい論争を起こしている。オンライン環境を対象とする判例法が形成されつつある一方で、著作権と新たに出現するオンライン技術の関係によって更なる問題も生じている。これらの理由により、オンライン上の著作権問題はますます注目を集めることとなっている。

2.2.1.3　名誉毀損

インターネットの持つオープンな環境という理由から企業より多くの注目を集めてきたリスクが名誉毀損である。米国における初期の判例ではこの名誉毀損についてはその当事者の役割が「Publisher（出版社・発行者）」か「Distributor（頒布者・配給者）」かという点が問題になってきたようである。本を例にとるなら Publisher つまり出版社、編集

者か、Distributor つまり書店かという点である。Publisher つまり出版社と判断された場合は、責任があるとされ、また、多くの判例は第三者が公表した名誉毀損の内容の単なる配布又は送信のみをした人でも、それが名誉毀損であることをその人が知っていた、又は知るべき理由があった場合は責任を負う、という規則を認めてきた。

(1) カビー社対コンピュサーブ社事件

① 事件の概要

ＯＳＰの CompuServe はそのメンバーにチャットルームを提供していたが、そのコンピュータのデータベースに原告 Cubby, Inc の名誉を毀損したとされるニュースレターが、ある者によって掲載されたケースで、Cubby, Inc が CompuServe を訴えたものである。CompuServe はニュースレターの内容を、掲載される以前にも以後にも審査しておらず、また原告が CompuServe を文書による名誉毀損で訴えるまで、名誉毀損とされる内容を知らなかったと主張した。

② 裁判所の判断

裁判所は CompuServe のオンライン・サービスを、「実質的に、膨大な出版物をもち、その出版物へのアクセスの対価として使用料と加入料を徴収する、電子的な営利図書館」と表現し、「CompuServe が、名誉毀損の表明の存在をチェックするためにそれがもつ全ての出版物を検査するのは、実現不可能である」と結論付けた。

つまり、裁判所は CompuServe がニューレター内の名誉毀損とされる表明を知らず、知るべき理由もなかったので、原告の名誉を毀損したとの主張に対して、責任なしとする判決を下したものである。次に、これと異なる判断をした判例がある。

(2) ストラットン・オークモント社対プロディジー社事件

① 事件の概要

大手のＯＳＰであるプロディジー社は「マネー・トーク」というファイナンス情報の掲示板を提供していたが、正体不明の人が以前のユーザーのアカウント番号を使って Prodigy のオンライン・サービスへアクセスをし、投資銀行であるストラットン・オークモント社（以下、「ストラットン社」）らが証券発行について犯罪や詐欺的行為をしているという名誉毀損のメッセージを掲示した。このため、ストラットン社がＯＳＰのプロディジー社を名誉毀損として訴えたものである。

② 裁判所の判断

裁判所はまず、Prodigy は「公衆及びそのメンバーに、そのコンピュータ掲示板の内容を管理していると主張していた」と判断した。その判断は、全国紙に出版された Prodigy の営業担当役員の記事に基づいていた。その記事でこの役員は Prodigy を、「New York Times のような民間出版社」であると説明し、悪質な内容のコンテンツを「公表しないために編集上の判断をする」という Prodigy の方針を述べ、さらに一定の用語を検索するために「掲示板の全てのメッセージを事前に検閲する自動ソフトウェア検閲プログラム」を使っていると述べた。

裁判所は、「悪質な内容のコンテンツを根拠にコンピュータ掲示板からメッセージを削除するため技術及び人員を積極的に利用することは、Prodigy は明らかに、コンテンツに関して決定を行っており、その決定は編集上の管理に相当するとして、Prodigy は Distributor（頒布者）ではなく Publisher（公表者）であると結論付けざるをえない。」とした。

裁判所は、他のユーザーに再送信するとき Prodigy が名誉毀損となる内容を知っていたか知るべき理由があったかについて直接的な認定をすることなく、Prodigy が名誉毀損のメッセージの Publisher（公表者）であると判断した。ここで、興味深いのは、プロディジー社が言わば良心的に編集的なコントロールを及ぼせば、そのようなコントロールをしていないＯＳＰよりもかえって重い責任を負うことになるという点である。しかし、現在は好ましくない素材の頒布を拒否する権利を主張し行使しようとする Prodigy の努力が、その掲示板に掲示された名誉を毀損するメッセージ全てに対して、そのメッセージの名誉を毀損する内容を知っていなくてもまた知るべき理由がなくても Prodigy に責任をもたらすという Stratton Oakmont 訴訟での裁定に対して、否定的な考え方が一般的のようである。最近の判例ではこれとは異なる判断をしている。

(3) ゼラン対ＡＯＬ事件

① 事件の概要

1995 年、オクラホマ州の連邦ビルが爆破され 168 人が死亡するという事件の直後、あるＡＯＬのユーザーがＡＯＬの掲示板上に、Zeran が広告主であるとの虚偽の特定をして、その事件を逆に賞賛するスローガンを掲げたＴシャツの販売広告が掲載され、連絡先として原告の氏名と電話番号が記載された。原告からの抗議の後、ＡＯＬはその広告を除去しようとしたが、その広告はサービス上に 7 日間、再登場し続け、原告はその広告によって、被害者からの電話や殺しのおどしによって悩まされた。原告は、ＡＯＬを訴え、ＡＯＬは最初の広告についての通知を受けた後、その広告をもっと素早く除去し、また原告の電話番号を含んでいた、そのサービス上のその後の掲示全てを遮断すべきであったと主張した。

② 裁判所の判断

1996 年 2 月 8 日、1996 年 Communications Decency Act of 1996 通信品位法（ＣＤＡ）が発効した。ＣＤＡは、「親に、その子供による、好ましくない又は不適切なオンラインのコンテンツへのアクセスを制限することを可能にする、遮断又は選別の技術の開発及び利用に対する抑制要因を除去する」ことを目的の１つとして、230 条（c）を付け加えた。この法律の第 230 条（c）(1) は Publisher の取り扱いについて次のように定めている部分がある。

「Publisher、公表者又は発言者の取り扱いとして、双方向コンピュータ・サービスの運営者もユーザーも、他の提供者の情報に対して Publisher、公表者又は発言者

として扱われるべきではない。」

第 230 条（c）(2) は、対話形コンピュータ・サービスのユーザー又は運営者が、「好ましくない」とみなすオンラインの素材への「アクセス或いはその利用可能性を制限するために、善意で自発的に取った行動を理由として」民事責任を課さないと定めている。「第 230 条（c)の具体的な目的の 1 つは、好ましくない素材へのアクセスを制限してきたという理由でかかる提供者及びユーザーを、自分自身のものではないコンテンツの公表者又は発言者として扱った Stratton Oakmont 対 Prodigy 訴訟の判決、及び他の類似の判決を覆すことである。」

つまり、この第 230 条（c）(1) は、ユーザーなどの他の「情報提供者によって提供された」、そのサービス上のコンテンツにおける名誉毀損の責任を、ＯＳＰから免除した。さらに、この免責は、プライバシーの侵害や詐欺などの第三者のコンテンツのＯＳＰによる頒布に基づく、類似した、州法上の不法行為に対する賠償請求にも適用されるだろうとされている。ただし他の項では、第 230 条（c) によって与えられる免責は、連邦の刑法や、著作権、商標などの「知的所有権に関する法律」には適用されないと、明示的に定められている。

裁判所は、第 230 条（c）(1) は、掲示板上の名誉毀損のコンテンツについての通知を受けた後のＡＯＬの行為を現実に免責すると判決した。裁判所がこの法律制定後、ＯＳＰがメッセージの名誉毀損の通知を受け、そのサービスからそれを撤去しないと選択した場合でも、第 230 条（c）(1) は実際にＯＳＰを免責すると裁定した最初の判例である。

2.2.1.4　解説　中傷・名誉毀損

オンライン上のコミュニケーションでは電子メール、ブリテンボードやチャットルームなどにおいて言葉更には音、画像を通じて情報の交換が行われている。莫大なコストがかかる雑誌やテレビなどのメディアによる現実の世界での情報提供に比べ、ほとんどコストもかからずに数秒で何十万のユーザに到達することも可能なオンライン上のコミュニケーションは名誉毀損の可能性も増大する。オンライン上のコミュニケーションで認められている自由な表現やこのようなコメントを匿名で行うことが可能であるという文化も名誉毀損の機会を増大させている。

一般的に言えば、名誉毀損に対する訴訟は、原告についての名誉毀損の表明が害意をもって被告によって公表されたならば、コモン・ローによって認められる。しかしある種の名誉毀損の表明は、それが原告に、金銭的被害など「特定の実損害」をもたらしていなければ訴訟対象にはならない。

(1) 名誉毀損の表明

表明は、もしそれが人の評判に害を与え、その人を公衆の憎悪、侮辱、あざけり、恥若しくは不名誉にさらし、又はその人の職業若しくは事業に悪影響を与える「傾向

がある」ならば、名誉毀損である。原告は、言葉が人の評判を害する「傾向がある」ことを示すだけでよい。

評判への現実的損害の証明は、一般的に、名誉毀損であることの立証には必要ない。ただし、裁判所が、ある表明が文脈の中で読まれたときに２つの異なる意味をもち、そのうちの１つのみが名誉毀損であると認定したならば、原告は、伝達の受取人が、その表明を名誉毀損の意味をもつと理解したことを証明しなければならない。

これは陪審にとっての事実に関する問題である。幾つかの州では裁判所は「害意のない解釈規則」を適用し、もし名誉毀損と告発された表明が名誉毀損でない意味をもつと合理的に解釈できるならば責任を課さない。

(2) 原告について

訴訟対象となるには、表明は他の人ではなく原告の名誉を毀損していなければならない。表明の内容から、又はそれを受け取った人が知っている外部事実に鑑みてアイデンティティーが読み取れる場合には、公表において原告を名指ししている必要はない。著者の意図は問題にならない。

基準は、その物語が誰を指そうとしているかではなく、合理的に誰が指されているかを読者が考えるかである。つまり誰が意図されたかではなく、誰が影響を受けたかである。複数の人間のグループについての名誉毀損の表明は、もしその人数が十分に少なければ（通常、25 人未満）、そしてその表明が原告に当てはまると合理的な読者が理解するならば、そのうちの１人からの賠償請求も対象となりうる。

(3) 被告によって公表された

表明は、それが名誉毀損する人以外の人に伝達されたときに「公表」されたことになる。受取人がその表明を他の人に繰り返すと、その表明は「再公表」されたことになる。全ての繰り返しはそれ自体が「公表」である。再公表者は通常、その表明を「採用した」として扱われ、最初の公表者と同じ責任に服する。

つまり法律は、表明の他の人への普及過程に参加した人を「公表者」として扱う。ただし、単にそれを「引き渡す」又は「送信」する人は、その名誉毀損の内容を知っている又は知るべき理由がある場合にのみ、再公表者としての責任に服する。

(4) 害意をもって

従来のコモン・ローの下では、「害意」が名誉毀損の賠償請求に必要な要素であった。コモン・ローでは「害意」は一般に、憎悪、悪意、復讐などの不適切な動機で、又は原告の権利、安全及び感情を意識的に軽視して被告が行う行為を指す。長い間裁判所は、名誉毀損の言葉の公表という事実だけで、名誉毀損を認める「判決を支持するのに必要な害意」の存在を含意すると判断していた。

このため、正当な原因又は理由なしに意図的になされた違反行為に付随して、「黙示の害意」つまり「推定害意」が、名誉毀損のコモン・ローによって自動的に推定された。原告は特権を打ち負かすか懲罰的損害賠償を正当化するために従来の「コモン・

ローの害意」の証明を提示するかもしれないが、そのような証明は、名誉毀損の賠償請求を述べるには必要ない。被告が表明を公表し、その表明が名誉毀損であり虚偽であり特権がないならば、表明が虚偽であることを知るべき理由がない場合でも、その人はコモン・ローの下で責任がある。この文脈では、コモン・ローの口頭又は文書での名誉毀損は、「厳格責任」不法行為と呼ばれてきた。

(5) 損害賠償

通常、名誉毀損訴訟には 3 種類の損害賠償がある。特別損害賠償、一般損害賠償、懲罰的損害賠償である。

特別損害賠償は、名誉毀損によって引き起こされた現実の経済的又は金銭的損失に対して裁定される。

一般損害は、評判やコミュニティ内での立場への傷、恥辱、不名誉、憤り、個人的屈辱、精神的苦痛、感情的苦悩など、金銭では容易には測れない損害を原告に補償するために裁定される。

コモン・ローでは、被告が「コモン・ロー上の害意」で、つまり不誠実、悪意、又は原告の権利・安全・感情を意識的に軽視して行動したと原告が立証した場合には、懲罰的損害賠償が裁定される。幾つかの州では、原告が懲罰的損害賠償を裁定されるには現実的損害の証明が要求される。他の州のコモン・ローは、名目的損害賠償又は推定損害賠償が裁定される場合には常に、懲罰的損害賠償の裁定を認めている。被告は、自分が名誉毀損の表明を撤回したと証明することで、害意の証拠を反証し、一般損害賠償及び懲罰的損害賠償を軽減することができる。多くの場合、報道機関である被告が適切な撤回又は訂正をした場合には、「撤回についての制定法」により、被告に対して懲罰的損害賠償を裁定することが禁じられる。

名誉毀損的な表現を最初に行った人（Publisher）の他、名誉毀損的な表現を再出版する者も責任を負うこととなる。しかし、現実の世界で書店、新聞売り場あるいは公共図書館といった頒布者（Distributor）は、名誉毀損的表現を知っていたか、または知るべき理由があった場合にのみ、他人の名誉毀損的表現の責任を負うことになる。

オンライン上のコミュニケーションではＯＳＰなどが、書店、新聞売り場あるいは公共図書館として考えられるのか（Distributor）、出版社（Publisher）として考えられ潜在的な間接責任や中傷の結果としての損害請求に対する責任を負う可能性があるのかが度々問題となってきた。

2.2.1.5　商標権侵害

米国では、ドメイン・ネームと商標の関連が注目を集めてきた。米国においては、実質的にインターネットドメイン（ＵＲＬ）の登録・管理をＮＳＩ（Network Solutions Inc）が行ってきた。インターネットドメイン（ＵＲＬ）は申請の順番によって登録され、使用が認められる。ドメイン・ネームの侵害の理由となる要素の１つは、当初米国でドメイン・

ネームを割り当てる方法が、厳格な先着申請のシステムであり、申請されたドメイン・ネームの使用が既存の商標を侵害するかどうか判断するための審査が実質的に全くなかったことである。このシステムのため、商標の紛争が不可避となり、1994 年に、ドメイン・ネームをめぐる商標の紛争が徐々に始まった。

これらの紛争の結果、ドメイン・ネーム取得に関する新しい約款が制定され、そこでは、ドメイン・ネームの申請者は、その知りうるかぎりにおいて、そのネームが第三者の権利に干渉したり権利を侵害していないこと、そのネームを「不法な目的」のために使用する意図はないことを述べなければならないとされた。この約款に違反すると、ドメイン・ネームを取り消されることがある。これらの紛争をさけるために、企業はしばしば InterNIC（internet national information center）と US patent and trademark office に多くの製品に対する商標とドメインネームの登録を同時に行ってきた。

当初、ドメイン・ネームを留保する申請が跡をたたなかったが、これは有名な商標のドメイン・ネームとしての不正流用の影響であり、申請者がインターネットでその名称を使用する準備ができていたからではなく、むしろ守る事項として他人によるドメイン・ネームの登録の先を越されることを防ぐためであることが多かったとされている。

初期の広く報道された訴訟の１つは、MCDONALDS.COM というドメイン・ネームに関してである。マクドナルド社はドメイン・ネームを留保した者から、金銭的な方法でやっとそのドメイン・ネームを入手したと伝えられている。もう１つの訴訟では、MTV の「ビデオ・ジョッキー」であったアダム・キューリーが MTV.COM というドメイン・ネームを登録し、MTV が提供する音楽ニュースと情報サービスと類似のものを提供するために使用した。MTV ネットワークはキューリーを商標の侵害とその他の商標に関連する訴訟事由で訴え、この訴訟は、その後、商標の侵害問題についてなんら司法上の見解が出されなかったが、MTV はその標章を回復して、解決したとされている。

現在、裁判所が、ドメイン・ネームが商標のように機能することに同意している判例が多くある。ひとつの判例は、JURIS.COM 訴訟である。JURIS 社は法律のソフトウェアに関連して JURIS を連邦で商標登録していたが、法律書出版会社である The Comp Examiner Agency が JURIS.COM のドメイン・ネームを使用したため The Comp Examiner Agency を商標違反で訴えたものである。裁判所は、連邦で商標登録された JURIS との混乱のおそれがあると判決して、The Comp Examiner Agency が今後このドメイン・ネームを使用することを禁じた。同様に、雑誌プレイボーイの出版社とイタリアの会社 PLAYMEN.IT のＷｅｂサイトに関するドメイン・ネームの紛争にも商標法の原則が適用された。この訴訟の中で裁判所は、明示的に、被告のドメイン・ネームの採用は「商標、サービス・マーク、ブランド名、商号又はその他の業務若しくは商業上の」使用に該当すると認めた。

(1) ハスブロ社対インターネットエンタテインメント社事件

① 事件の概要

1995 年インターネットエンタテインメント社は多額の費用を費やして“Candyland.com”というドメインネームを得た。ところが、有名な子供の盤上ゲームキャンディーランドのメーカーであるハスブロ社は、インターネットエンタテインメント社がセックスのあからさまなポルノサイトに関連してキャンディランドというゲーム盤の商標を侵害したとして訴えた。

② 裁判所の判断

1996 年、裁判所はハスブロの暫定的差止命令申立を認めた。

裁判所は、商標希釈の理論に基づいてインターネットエンタテインメント社による「CANDYLAND」の名称とドメインネームの使用を停止するよう命じた。暫定的差止命令では、被告は 90 日以内にドメイン・ネームを放棄するように要求された。

2.2.1.6 解説 商標の侵害

商品やサービスを特定し市場にある他の似た商品やサービスと区別するために用いられる「言葉、シンボル、デザイン、音、独特な色」など、多くのものが潜在的に商標である。商標権者は、特定の種類の商品やサービスに関して、与えられた市場の中で商標を独占的に使用する権利を有する。この権利を侵害する行為は商標権の侵害と呼ばれ、次の行為がなされた場合がこれにあたる。

商標の侵害：取引において、商品又はサービスの販売、販売の申し込み、配布又は広告に関連して、連邦で登録された標章（原産を特定する機能を持つ商標、サービス・マーク、商号、商業装飾その他の考案を含むよう広く定義されている）の複製、偽造、コピー又は模造であって、混乱を引き起こし、誤解を生じ又は欺くこととなりそうなものを使用すること。

つまり、(1) 商品やサービスを連邦で登録されている標章に関連して提供するか否かを問わず、取引において、商品やサービスの原産、発起人又は系列について混乱を引き起こしそうな標章を使用すること、(2) 商業広告や販売促進において、宣伝対象の又は競合する商品やサービスの性質、特徴、質又は原産地を間違って表わす虚偽又は誤解を招く表明を行うことを禁止している。

商標侵害の請求の試金石は、「混乱のおそれ」である。原告と被告の商標の間に混乱のおそれがあるかどうか判断するに当たって、裁判所は、次の要素を基本として多くの要素を考慮している。(1) 原告の商標の強さ、(2) 原告・被告の２つの商標の類似の度合い、(3) 当該製品同士の類似性や近接の度合い、(4) 原告が当該製品同士のギャップを埋める可能性、(5) 混乱の実態（消費者調査により示されることがある）、(6) 被告の誠意、(7) 被告の製品の質、(8) 消費者の知識。

商標法の原則は、現実の世界で妥当するのと同じくオンライン・サービスのバーチャル

な世界でも妥当するものである。商標の原則をオンライン・サービスに既に適用してきた方法の 1 つは、インターネットのドメイン・ネームのような有名な商標と会社の同一性識別子の急増を通じてである。実際、インターネットに特有の商標侵害の申し立ては、主に会社を識別するドメイン名の登録と使用の権利に関連するものである。

米国では、従来ドメイン名の使用権利は InterNIC により管理されてきた。ドメイン名の申請時には、そのドメイン名を使う権利があることを宣言しなければならないが、先願をもとに許可登録されるだけであり、商標侵害を含む不法目的の使用可能性が調査されることはなかった。したがって、申請後に商標侵害の申し立てを受ける可能性もある。このような潜在的なトラブルを避けるため、いくつかの会社は、先んじて自らの商品名や商品として解釈される可能性のある俗称の登録を行っている。ドメイン・ネームをめぐる紛争を解決するためのルールも制定された。米国又は外国の商標登録（州の登録では不可）の所有者は、第三者による同一のドメイン・ネームの使用に対して異議を申し立てることができる。ドメイン・ネームの所有者が 30 日以内に (1) その異議申し立ての前から連邦又は外国の登録を持っていた、或いは (2) 異議申し立て人の商標の最初の使用又はその者の登録の発効日の前からそのドメイン・ネームを使用していたことを立証できない場合には、そのドメイン・ネームは、訴訟か仲裁により解決するまで、保留される。実際、組織も個人も、申請したドメイン・ネームが既に登録されていないかぎり、その希望のドメイン・ネームを選ぶことができ、挙証責任は、こうして選ばれたドメイン・ネームに対して異議を申し立てる商標の所有者の側にある。

2.2.1.7　プライバシー関連問題

米国においてはインターネットまたはＥＣ上の消費者の持つ不安はこのプライバシー、個人情報に関する問題が極めて大きいと言える。米国では、インターネットの利用者が爆発的に増えたことに伴い、個人情報、プライバシーに関する重要性が大きく叫ばれる様になった。現在、プライバシーに関する関心はますます増大している。

(1) エプソン社事件

① 事件の概要

エプソン・アメリカ社の従業員は、電信、電報、電話回線、ケーブル、その他あらゆる内部的遠隔コミュニケーションシステムを使用して、意図的に傍受したり、未承諾の接続をすることを禁ずる刑法 631 条に基づき雇用者が自分たちの電子メールが傍受されているとしてエプソン・アメリカ社を提訴した。

② 裁判所の判断

州裁判所は電子メールにプライバシー権を供与することを拒否して雇用者側に軍配を上げた。裁判所は会社側に電子メールシステムの所有権があるとして、経営者側がそのシステム上で作成された内容物を読む権利を有するとした。

2.2.1.8　解説　プライバシーの侵害

プライバシーの侵害とは、他人が個人のプライベートな情報を得た結果として生じる、物理的、経済的、もしくは心理的な害を引き起こしたり、被害があると考えられる損害である。

たとえば、利用者から、商品もしくはサービスの要求というビジネストランザクションがある場合、そこには当事者の間で取り交わすいくつかの形式が用意されている。一般的に、このトランザクションでは利用者に対して、注文に応ずるための個人情報と購入の手続きに必要な金銭的なデータを、Ｗｅｂサイトへ通知することを要求することになる。このようなケースでは、個人情報であろうが金銭的なデータであろうが、情報の外部への漏洩はプライバシーの侵害になり得る。

したがって、Ｗｅｂサイトの運営者は、利用者から提供された情報を安全に保たなければならない。クレジットカード情報が関わる場合のセキュリティについては、特別重大に考えられているが、金銭的な被害とともにＷｅｂサイト運営者の信用失墜の原因ともなるため、無権限者の利用を妨げるための安全確保が必要である。通常、通信される情報やＷｅｂサイトのコンテンツが、個人の名前などの個人情報や肖像または声などの個人の属性を含んでいる場合にはプライバシー権の問題を含んでいる可能性がある。ここでは、米国におけるプライバシーに関する４つの観点について説明する。

(1) 個人の人格に関するプライバシー

この分類において米国裁判所は通常、4 類型のプライバシーの侵害を認めている。それらは重複するところがあるが、非常に明確である。これらの侵害に対する慣習法による改善策は金銭的損害賠償、懲罰的損害賠償、及び差止命令などによる救済を規定する。

第一のプライバシーの不法侵害は、他人の干渉を受けずに送っている私生活に他人が侵入することで、一般の人であれば強い不快感を覚えるような場合に他人の侵入から私生活を守るという権利である。他人の人目に触れない状態への不当な侵入、つまり個人がプライバシーを期待しても妥当な場所又は行為への侵入である。この不法行為は違法な監視や不法侵入のような不適切な個人データの収集に焦点を当てている。

第二のプライバシーの侵害は私的事実の不法開示である。他人の私生活に関する事柄を公表する者は賠償責任を課される。不法行為であるためには、公表内容がまともな人間にとって非常に侮辱的且つ報道するに値しない類のものでなければならない。つまり、公衆が入手できる情報である場合や報道価値のあるものである場合にはプライバシー権の侵害にはならないとされている。

第三のプライバシーの侵害は、他人を誤って認識したり真実とは異なる事実に関する公表の問題である。一定の個人と非常に侮辱的な行動を誤って結び付ける事実を公表した者は責任を問われる。この侮辱的パブリシティーは、承諾なしの写真の使用、意見の特定、嘆願又は訴訟における名前の使用などによって、無関係の人を物議をか

もす問題（例えば、麻薬の使用、売春、性的傾向、ギャンブルなど）に結び付けることから発生する傾向がある。

第四のプライバシーの侵害は私的使用として知られる。これは人の名前や肖像などの無断使用に伴う迷惑なパブリシティーから生じる人の尊厳又は名声への毀損に対して保護するものである。

(2) 個人情報のプライバシー

個人情報のプライバシーには、たとえば、消費者信用報告及び銀行、雇用、保険、医療、教育などがある。情報収集機関やその利用者がこうした情報を不正に利用するする場合には、紛争の原因になることがある。

しかし、米国には民間組織にまで及ぶ個人情報の収集、伝達および利用を規制する独立した法令や規則は存在しないとされている。プライバシー法は連邦政府が保有する個人情報のプライバシー保護に対する概括的アプローチを示している。州法がこれらの個人情報のプライバシー領域における権利と義務の重要な源泉であり続けている。多くの種類の金融機関が、個人に関する広範囲な財産情報を収集し、時には開示することもある。

(3) 個人の通信のプライバシー

個人が送受信するオンラインコミュニケーションに関するプライバシーが存在する。1968 年電話盗聴法の施行後、年々増強する技術的進歩を懸念した議会は、1986 年電子通信プライバシー法（ＥＣＰＡ）を施行するに至った。議会はＥＣＰＡを通して、現法に成文化されている電話網プライバシー防御策を電子メール及び他のコンピュータ間データ送信を含めた新テクノロジーにまで拡張させようとしたものである。ＥＣＰＡは私信又は事業通信のように守秘を意図とする電子通信に対して未承認アクセス又は承認済みアクセス限度以上のアクセスを行う者の問題を取り上げている。特にＥＣＰＡの保存通信条項は「ボイスメール」及び電子メールのような保存電子通信の未承認アクセス又は使用を禁ずる。加えて、同条項は電子通信サービスの提供者が保存通信のコンテンツを開示することを禁ずる。

したがって、いかなる者に対しても電子通信の発信者以外の者が電子通信を故意に傍受したり、通信の内容の開示することを禁じている。この禁止規定はハッカーのような電子通信システムに侵入しようとしている者に対してだけでなく、ＩＳＰなどのシステムを保有し、またはこれを管理している者にも適用される。

非開示規則の除外は次の 3 類型に区分される。(1) 通信文の送信者又は受信者によって承諾された開示、(2) 通信システムの効率的運営に必要な開示、(3) 国家への開示である。

(4) 通信の匿名性

米国憲法のもとでは、個人は匿名によりプライバシーを犠牲することなく社会参加を継続する機会を与えられる。例えば、匿名であれば報復や社会的烙印を恐れることなく、反体制者が宗教批判をしたり、レイプや配偶者暴力の犠牲者がグループ・ディスカッションに参加したりできる。サイバースペースによって、匿名・別名の相互作用の機会がますます多くなっている。米国連邦裁判所は、匿名で通信する権利は合衆国憲法によって保護されると判示しており、オンラインコミュニケーションとりわけインターネットで行われる通信では、個人は匿名で通信をする権利を与えられる。

インターネットとオンラインサービス提供者にとって不幸なことではあるが、匿名性により名誉毀損、不正使用、偽装工作、及び他の犯罪行為が発生しやすくなっていることも事実である。さまざまな犯罪行為が匿名性によって可能になっている現状を見れば、今後この問題は更に議論の余地があるものとされている。

2.2.2 欧州におけるＥＣ関連の判例

欧州では米国に比し、インターネット関連の判例の数は少ない。ＩＳＰに拘わるいくつかの判例は存在する。ここではそのうち代表的な２つの判例について述べることとする。

まず、ＩＳＰに対する責任の考え方について欧州では２つの考え方があることに注意する必要がある。ひとつは行政・政府の考え方、ひとつは司法・裁判所の考え方である。

2.2.2.1 行政･政府の考え方

(1) 欧州連合（EU）の見方

1998 年 11 月 18 日付ＥＵ指令の提案書（1999 年 2 月 5 日付 JOCE）は、北米法から着想を得たもので、インターネットサービスにおけるコンテンツに対しプロバイダーに責任はないとする立場をとる。表現の自由の原則、仲介者によるメッセージ管理の不可能性を強調している（刑法上の義務がないこと、不法行為に対する積極的追求の義務および監視の一般義務のないこと）。ただし以下のものを除くとされている。

- **国家の安全を脅かすもの**
- **刑事犯罪**
- **選択、修正など情報への積極的介入**
- **有害情報が流れることを知っていたにもかかわらず、撤回しないこと**

(2) ＥＵ加盟国政府の考え方

① ドイツ

データ通信サービスに関する 1997 年 8 月 1 日付法律：第三者からのサイトを通じて生じた情報に対するプロバイダーの責任はない。ただし、プロバイダーが、あらかじめその内容を知っていたことが証明される場合を除く。

② フランス

一時期、プロバイダーの刑罰責任免除の動きがあったが変化している。憲法に合致しないとして修正されつつある。

2.2.2.2 司法・欧州の裁判所の考え方

ＩＳＰの責任を増大させ、自由を制限する動きがある。表現の自由の行過ぎを予測し、特にバイオレンス、人種差別、ポルノ、個人中傷はプロバイダーも責任を持つべきであるとする立場をとる。

(1) 欧州における判例

ＥＵ加盟国裁判所の考え方として、次の２つの判例をあげることとする。

① CompuServe Germany 訴訟

A. 事件の概要

CompuServe Germany 訴訟は、ミュンヘン検察庁によれば CompuServe Germany 社が「ニュースグループからの児童ポルノグラフィー、暴力的性交および獣交の画像を、CompuServe Germany の顧客がアクセスできるようにすることを、故意に認め」、加入者はまた、ヒットラーや、ハーケンクロイツなどのナチのシンボルであるドイツでは禁じられた画像を含むコンピュータ・ゲームへのアクセスも認められたとして、同社の前役員 Felix Somm 氏が起訴されたものである。

警察の長期にわたる捜査の後、CompuServe のドイツ部門の責任者 Felix Somm 氏が起訴された。これは、西側社会の取締機関が商業オンライン・サービスを、自身が制作したものではないコンテンツに関して起訴した初めての例であると言われている。

B. 裁判所の判断

裁判所は、実際に検察官が最終的に無罪を求めたにも関わらず、Somm 氏は有罪とした。検察官は 4 週間の審理の後、ドイツ議会が 1997 年 8 月に成立させたマルチメディア法の下で Somm 氏には責任がないことに同意した。この法律によれば、CompuServe のようなインターネット・アクセス・プロバイダーは、違法なコンテンツに対して、それを阻止する技術をもたないならば責任はないとするものである。また、1995 年に捜査が始まったとき CompuServe は、児童や動物のポルノグラフィー、および、ドイツで禁じられているナチの文献を含む、200 のインターネット・サイトへのアクセスを停止した。検察官は、1996 年の時点では適切な停止技術はなかったと結論付けたが、判事は検察官による起訴取下げの申立てを無視した。判事は判決の中で、「インターネットであっても無法地帯はありえない」と述べた。

結局、Wilhelm Hubbert 判事は検察の主張にも被告の主張にも同意せず、1998 年 5 月 28 日注目を浴びた国際的論争の中で、1997 年に起訴されるまで CompuServe Deutschland の事業を率いていた Felix Somm 氏に対しインターネットで提供され

ていたポルノ映画へのアクセスを阻止しなかったとしてドイツにおけるポルノグラフィー法に違反の罪で有罪宣告した。同判事は判決において、CompuServe は「青少年の保護よりも利益の拡大を優先させた」と述べ、Somm 氏は 1995 年から 1996 年に CompuServe のドイツ部門の責任者であったとき、インターネットを「悪用」し、ドイツにおいて児童ポルノグラフィーへのアクセスを可能にしたと結論付けた。彼は 2 年間の保護監察という宣告を受け、チャリティに 10 万マルク払うように命令された。Somm 氏を有罪としたこの裁判所の判決は、ドイツのＩＳＰがインターネットのコンテンツに対して責任があり、好ましくないコンテンツへのアクセスを阻止するために、積極的な措置を取らなければならないものと解釈された。その後、本件はバイエルン控訴裁判所に控訴された。

1999 年 11 月 19 日、バイエルン控訴裁判所において 1997 年 8 月の法律に則し CompuServe 側の主張が認められ、第一審の判決が覆されて Somm 氏は無罪とされた。この判決はドイツ国内のみならず国際的なオンラインコミュニティーにおいても良い評価を得ている。

② E. Halliday 対 LACAMBRE－ALTERN. ORG 訴訟（フランス）

A. 事件の概要

E. Halliday対 LACAMBRE 訴訟は 1998 年、無許可でトップモデル Halliday の 19 枚の私的写真がインターネット上に流れたため、Halliday がこのサイトを掲示していたプロバイダーを訴えたものである。

B. 裁判所の判断

判決ではプロバイダーに対して、基本的人権の侵害で 40 万フランの懲罰的罰金が課された。一審の判決は、二審でも追認された。判決では「プロバイダーがユーザーの品行の良さに留意する義務として、プロバイダーがＷｅｂを規制する職業倫理規則を遵守することにより法律と規則および第三者の権利が守られる」と述べられた。

3 消費者のＥＣリスク

3.1 金銭的リスクと米国５０ドルルール

ＥＣ取引における「無権限者による不正取引」により発生する消費者の金銭的損害に対する消費者保護を考えるにあたり、インターネット先進国である米国における法制度を調査した。

「無権限者による不正取引」により発生する消費者の金銭的損害に対する消費者保護に関して、直接ＥＣ取引を対象とした法制度は、米国においても無い。しかしながら、ＥＣ取引を直接の対象とはしないものの、ＥＣ取引に極めて関連性の高い取引を対象とした「無権限者による不正取引」に関しては、消費者の責任負担上限を一定条件のもとで 50 ドルとした、いわゆる 50 ドルルールにおいて、消費者保護規定を設けている。米国ではこうした既存のルールの枠組みを、現状ではＥＣ取引においても適用している。ここでは、この 50 ドルルールの概要について述べる。

3.1.1 ５０ドルルールとは

米国における「無権限者による不正取引」により発生する消費者の金銭的損害に対する消費者保護に関する規定である 50 ドルルールは、一般に米国の電子資金移動に関する消費者保護のための規定を指すものと、クレジットカードに関する消費者保護のための規定を指すものの 2 種類が存在する。

消費者信用保護法
（Consumer Credit Protection Act）

第一編　連邦貸付真実法　Truth in Lending Act

第九編　電子資金振替法　Electronic Fund Transfer Act

電子資金移動に関するものは、United States Code（ＵＳＣ）の一部である Electronic Fund Transfer Act（電子資金振替法、ＥＦＴ法）と、Code of Federal Regulations（ＣＦＲ）のレギュレーションＥに規定されている。

クレジットカードに関する消費者保護のための規定については、ＵＳＣの Truth in Lending Act（連邦貸付真実法）とＣＦＲのレギュレーションＺである。

どちらも第三者による不正な電子資金移動、クレジットカードの不正利用における消費者の損害を一定の条件のもとに最高で 50 ドルまでと定めていることから、一般に 50 ドルルールと呼ばれているものである。

しかしながらそれぞれのレギュレーションは、それぞれが異なる取引形態を対象とした

法規定であり、その適用範囲ならびに消費者の責任限度額が異なっている。

3.1.1.1　電子資金振替取引法とレギュレーションＥ

(1) 背景と目的

米国は小切手社会と言われるように、日常の買い物から公共料金、給料支払いと幅広く小切手が利用されており、年間の流通枚数も何百億枚とも言われている。消費者にとっては治安の悪い米国において、現金を持ち歩かなくて良いというメリットがあるが、その反面受け取った側が取り立て行為を行うために金融機関に大量の小切手が持ちこまれ、金融機関はその処理に膨大な時間と労力が費やされている。

このような状況において、電子的な資金異動が大量処理の費用と労力を軽減する手段としてＥＦＴが推進されてきた。

ＥＦＴ法の目的は、ＥＦＴシステムに参加する当事者の権利、義務、責任を確立する基本的な枠組みを提供することであり、主な目的は消費者の諸権利を規定することである。

(2) EFT（電子資金振替）とは

ＥＦＴ法では、電子資金振替の定義を「金融機関に対してある口座へ借方記入もしくは貸方記入を指図し、指示し、あるいは授権するために小切手、手形、もしくはそれに類する証書によらず、電子端末機、電話関連機器、コンピュータもしくは磁気テープを介して開始される資金振替」としている。米国で実用化されているＥＦＴシステムで法の対象となるものは以下の通りである。[14]

- ＡＴＭ（Automated Teller Machines）
  自動テラーであり、預け入・振替・残高照会・払い戻し・第三者への支払いの諸機能を兼備している。操作方法はカードと個人識別番号（Personal Identification Number、ＰＩＮ）による。
- 電話支払システム（Pay-by-Telephone System）
  消費者が種々の勘定書の支払を銀行に電話をかけることによって済ませることができるもので、行員（銀行員）と会話する方法と銀行のコンピュータに直接指示する方法がある。
- 直接振込、自動振替（Direct Deposit、Automatic Payment）
  これは、給料、配当金、年金等の振込、債務の定期的な支払などに利用される。一般的によく使われる小切手による支払いに伴う郵送日数や盗難等のリスクがないという利点をもつ。
- ＰＯＳ（Point-of-Sale）
  銀行と接続されたコンピュータの端末機が小売店等に設置され、消費者は、カードとＰＩＮを使用することにより、消費者の口座から小売店の口座への即時

[14] 金融法務事情 1100 号 17 頁（1985 年 9 月 15･25 日号）より引用

の代金振替が可能になっている。

つまり日常頻繁に利用しているＡＴＭやＣＤでの預貯金引き出しや預け入れ、またテレホンバンキングなども該当する。日本では広く一般に利用されているクレジットカードや公共料金の口座振替もこれに該当する。

(3) 消費者の責任

消費者は消費者の口座に関連する無権限電子資金振替について、次の場合にのみ、下記の制限の範囲内で責任を負う。

- 無権限移動に使用されたアクセスデバイスが受諾されたものであるとき
- 金融機関がアクセスデバイス発行の対象となった消費者の身元確認の方法（署名、写真、指紋あるいは電子的または機械的確認等）を提供していたとき
- 金融機関が書面で次の情報を提供していたとき

  a 無権限電子資金移動に対する、この条項あるいは他の準拠法または契約書に基づく消費者の責任の概要、および金融機関の任意で、利用手段の紛失または盗難あるいは無権限移動について早急の報告が望ましい旨を記した通知

  b 消費者が無権限移動が発生したと、あるいは発生する可能性があると信ずる事態に際して通知すべき者または事務所の電話番号ならびに住所

  c 金融機関の営業日

注）アクセスデバイスとは、消費者が電子資金移動の目的で使用することのできるカード、コードまたはその他の消費者口座利用手段、方法、あるいはそれらを組み合わせた手段、方法をいう。

(4) 消費者の責任額

50 ドルまたは金融機関への通知以前に発生した無権限移動額の少ない方の金額を超えないこと。ただし、次の例外がある。

- 消費者がアクセスデバイスの紛失または盗難に気づいてから 2 営業日以内に金融機関に報告を行わなかった時は、消費者の責任額は 500 ドルか次の a、b の合計額のいずれか少ない方の金額を超えないものとする。

  a 50 ドルまたは当該 2 営業日終了前に生じた無権限移動額のいずれか少ない方の額

  ｂ消費者がアクセスデバイスの紛失または盗難を気づいてから 2 営業日以内に金融機関に報告を行なっていれば発生していなかったものと金融機関が立証する 2 営業日以後かつ金融機関に報告前に発生した無権限移動額
- 期間計算報告書の送付後 60 日以内に消費者がその報告書に記載されている無権限移動の報告を行わなかった時は、消費者の責任額は次の a、b の合計額を超えないものとする。

  ａ50 ドル、またはその期間計算報告書に記載されているか、もしくは当該 60 日間に生じた無権限移動額か、いずれか少ない方の額

ｂ60 日の経過後でかつ金融機関への報告前に生じかつその期間内に消費者が金融機関に報告を行なっていれば発生していなかったものと金融機関が立証する金融機関への報告前に発生した無権限移動額

(5) 金融機関への通知

金融機関への通知が長期にわたる旅行または入院などの事情があるときは、上記に規定された期間は適正な時期まで延期される。

金融機関への通知は消費者が合理的に必要とされる手続きをとった時に行われたものとする。金融機関への通知は消費者の任意で、本人が出向いても、電話、書面でも行うことができる。書面による通知は、消費者が金融機関宛にその通知を郵便に託し、またはその他の普通の方法により伝達のためにその通知を交付した時なされたとみなす。

(6) 金融機関のエラーの調査

- 金融機関はエラーの通告を受領後、速やかにその申し立てのエラーを調査し、その調査の結果および判定を 10 営業日以内にその消費者に伝えるものとする。
- 金融機関が次の措置をとるときは、10 営業日という条件の代わりに 45 日以内にその消費者に伝えることができるものとする。

  ａ金融機関はエラーの通告を受領後 10 営業日以内に暫定的に消費者の口座にその申し立てのエラーの金額を再入金する。もし、要件を満たした無権限移動があると信ずるにたる十分な根拠があるときは、再入金金額から 50 ドルを限度として差し引くことができる。
- もし、全くエラーが発生していなかったか、あるいはエラーは発生していたが別の種類または別の金額であったと判定したときは次の措置を講ずるものとする。

  ａその調査終了後 3 営業日以内に、ただし、いかなる場合でも 10 営業日以内に、その結果の書面による説明を消費者に郵送または交付する。その説明には、金融機関がその判定を行う根拠とした記録を要求する消費者の権利についての通知も含む。

  ｂ消費者の要求があり次第、速やかにその判定を行う根拠とした記録のコピーを消費者に郵送または交付する。

3.1.1.2 連邦貸付真実法とレギュレーションＺ

(1) 背景と目的

連邦貸付真実法とレギュレーションＺはクレジットカードの普及と消費者保護の観点から制定されたものである。この規則の目的はその条件及びコストに関する開示を要求することによって、消費者信用の情報に基づく使用の推進化を図ることである。そして消費者に一定の信用取引を取消す権利を供与し、また金融機関に対して一定の

クレジットカード業務を規制するとともに、信用手形の論争に公正で適時な解決を提供することにある。

その中で未承認使用（未承認使用の定義：真の権限のない者によるクレジットカードの使用であって、カードホルダーは、その使用により何ら利益をも受けないものと定義される）に対する消費者の責任上限を 50 ドルまたは、カード発行者への通知以前の未承認使用により取得された金銭、所有物、労働またはサービスのいずれか少ない方の金額を超えないものと定めている。

(2) 消費者の責任と発生条件

次の場合に限って、カードホルダーは未承認使用に対して責任を負うものとする。

ａ）クレジットカードは受諾されたカードであること

ｂ）カード発行者は、カードホルダーの最大可能責任、およびカード発行者のカード紛失または盗難の通知を受けることができる手段に関して適切な通告を行っていること。その通知には、カードホルダーの責任が 50 ドル（またはより少ない金額）を超えないこと、またカードホルダーは口頭、または文書による通告を行うことを記載するとともに、通告手段（例えば、電話番号または住所もしくはその両方）も記載する。

ｃ）カード発行者は、カードホルダーとカード未承認使用者とを識別する手段を提供していること。

(3) カード発行者への通知（カードホルダーからの連絡完了時期について）

カード発行者への通知は、特定の職員、従業員、あるいは代理人が実際にその情報を受領すると否とに拘らず、紛失または盗難または未承認使用の可能性に関する情報を提供する為に、カードホルダーが合理的に必要とされる手続を取ったときに通知は行われたものとする。その通知手段は、通知を行うものの選択により、電話または書面のいづれかで行うことができる。書面による通知は受領時点、または受領の如何に関わらず、通常送信に要する時間の終了時点のいずれか早い時点で完了する。

3.1.2 ＥＣにおけるクレジットカード決済とレギュレーションの適用例

3.1.2.1 アマゾンドットコムのホームページ

米国のＥＣ分野で、最も成功している企業の１つである、アマゾンドットコム社のホームページ[15]では、同社のサイトを利用したクレジットカードの無権限者による不正取引による消費者の損害額を上限 50 ドルとする旨を明快に記載されている。

（原文抜粋）

Guarantee Details:

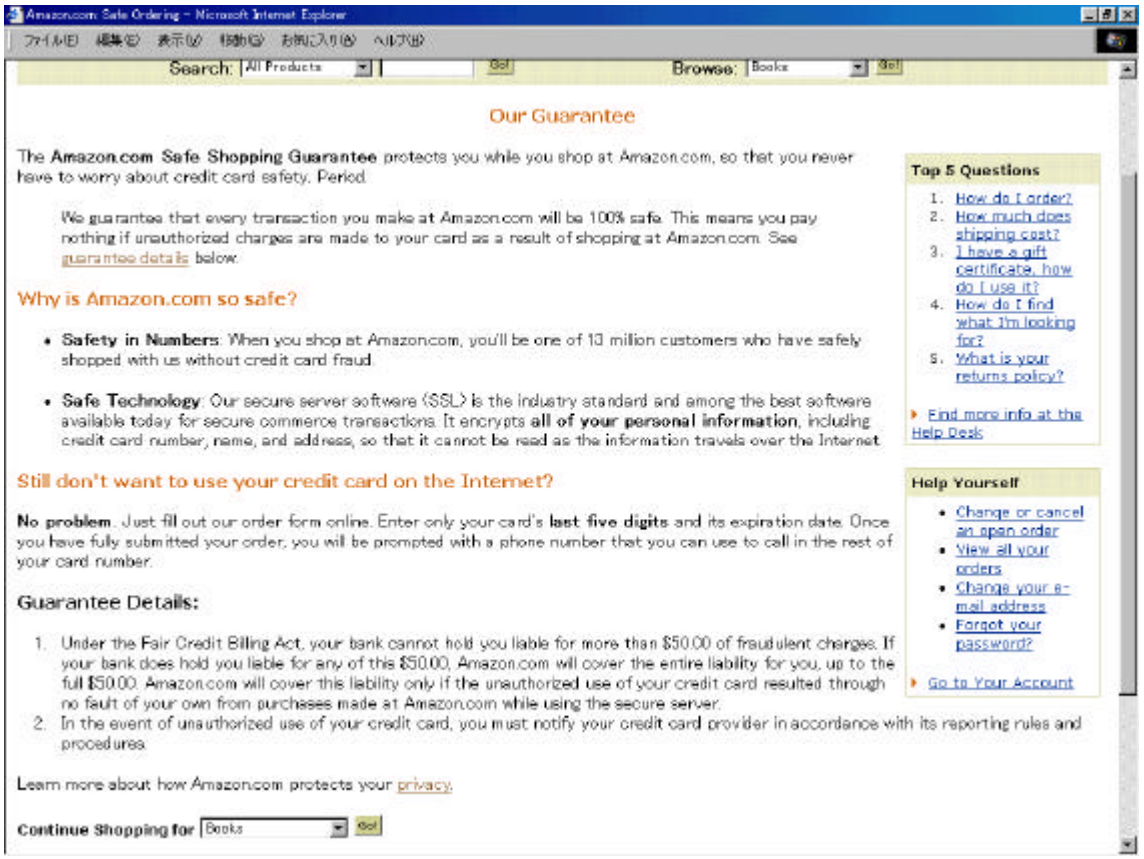
Under the Fair Credit Billing Act, your bank cannot hold you liable for more than $50.00 of fraudulent charges. If your bank does hold you liable for any of this $50.00,

15 http://www.amazon.com/

Amazon.com will cover the entire liability for you, up to the full $50.00.Amazon.com will cover this liability only if the unauthorized use of your credit card resulted through no fault of your own from purchases made at Amazon.com while using the secure server.

2.In the event of unauthorized use of your credit card, you must notify your credit card provider in accordance with its reporting rules and procedures.

図 3-1　アマゾンドットコムホームページ



3.1.2.2　会員規約における記述例（Bank of America）

Bank of America 社の入会規約には、クレジットカード利用に対する支払い請求書の内容について、カードホルダーが疑義を申し立てる場合の、カードホルダーの権利と義務について規定している。この疑義には、無権限者による不正取引による請求違いも含まれており、最終的に金融機関において、請求の正当性を立証できない場合（無権限者による不正取引の場合も含まれる）カードホルダーの金銭的損害は 50 ドルを超えないものと規定されている。（以下、仮訳）

- カードホルダーが、支払い請求書の内容が間違いである、もしくは請求内容についてより詳しい情報を知りたいと考える場合、請求書に添付された用紙にて、カード会社に対して書面連絡を取る。
- 書面による連絡は、できるだけ早くおこなう。
- 問題となっている請求書がカードホルダーのもとに通知されてから **60 日以内**にカード会社にその旨を通知しなければならない。
- カードホルダーは電話によって通知することもできるが、電話通知によっては、法的な保護は受けられない。
- その通知には、カードホルダーの名前、カード番号、および疑義が生じている取引の金額がわかる情報が記載されていなければならない。
- またカードホルダーの主張またはカード会社への要求内容がわからなくてはならない。
- もし自動口座引落を利用しているならば、その支払いを停止することができる。但しその場合は、口座引落予定日の **3 営業日前**までに連絡しなければならない。
- カード会社はカードホルダーからの通知を受け取ってから、**30 日以内に、**通知の受け取り証明を書面でカードホルダーに連絡しなくてはならない。
- カード**会社は、90 日以内に請求**を訂正するか、カード会社が請求内容が正しいことをカードホルダーに説明をしなければならない。
- カードホルダーからの通知を受け取った以降に、疑義の生じている金額に対して、カード会社は回収を試みてはならない。
- また、カードホルダーの信用各付けについて不利な報告をしてはならない。
- カードホルダーは、その調査期間中は、疑義の生じている金額については、一切の支払いを行わなくてもよいが、それ以外の部分については支払わなければならない。
- 調査の結果、カード会社が間違いを犯していた場合、遅延損害金等の支払いもカード会社が負担する。
- またカード会社が正しかった場合、カードホルダーは、遅延損害金を含め全てを支払わなくてはならない。
- いずれの場合においても、カード会社は書面で調査結果を通知する。
- カードホルダーが依然、疑義を申し立てる場合、カード会社は調査機関に義務不履行を報告できる。

- 但し、カード会社が、報告書を提出する人物の名前、住所をカードホルダーに通知しなければならない。
- カード会社が、上記のルールに全面的に従わなかった場合、カードホルダーの金銭的責任負担は、**50 ドルを**超えないものとする。

3.2　金銭的リスクと欧州における法律制度

3.2.1　ＥＵにおける法制化の動き

消費者のリスクについては消費者保護の観点から、ＥＵにおいて欧州指令（ディレクティヴ）という形で法律化する動きがある。ＥＣに関する重要な欧州指令が２つある。電子商取引に関する欧州指令提案書と遠隔地販売（隔地間取引）に関する欧州指令である。

欧州指令はその発効前に加盟国が各国の法律に反映させなければならない事を定めたものである。国内法に転化すべき最低限のものが定められており特に消費者の安全、セキュリティー、健康を考えて最低条項というものがあり、各国の事情によりそれにプラスアルファが加えられる。このためＥＵ統合といっても国によって国内法の経緯や文化が異なり、ディレクティヴの国内法への転化後の法律は国ごとに異なることになる。

一方、欧州法（レギュレーション）は加盟国に対し直接適用可能になり、国内裁判所に直接効力を与えることになる。これは、欧州法を国内で実施するために法律を制定する必要がないことを意味する。欧州裁判所は、各国間の法解釈の調和を図り、欧州法は加盟国の法規の上位に位置することはＥＵ法の基本原則であるという判決を、多数の訴訟において下している。これは国内法とＥＵ法の規定に矛盾が見られるとき、ＥＵ法が優先することを意味する。

3.2.1.1　電子商取引に関する欧州指令提案書（１９９８年１１月１８日）

オンライン取引においては消費者の誤入力、誤操作など過失によるリスクが考えられる。この場合、オンライン取引における契約の締結の時点とはいつになるのかという問題が生じる。この提案書では、オンライン上での契約締結に関し次のように定めている。

(1) 契約成立時期の明確化

契約が締結される瞬間とは次のように規定されている。消費者が電子的手段によって、販売者から消費者の発注を示す通知を受け取った旨の確認を受け取り、更に消費者がその確認通知を受け取ったことを再度、確認し、通知したときである。つまり、

- **消費者は発注通知を行い、次に**
- **業者は注文を受注したことを証明する受領の通知を出す**
- **消費者は受領通知の内容の確認後、再度通知を出す必要がある**

また、この提案書では契約締結のための電子手段の利用に対するすべての禁止あるいは制約を撤廃することの各国の義務をうたっている。

これにより、加盟国は自国の法律に電子的な手段による電子契約を認める内容を含

めること、特に、契約を結ぶために電子的手段を効果的に使用でき、また電子的手段によって契約を締結したからといって法的有効性には何ら支障は無い旨を明記することとしている。

(2) ＩＳＰの責任について

アクセスプロバイダーは次の場合、伝送される情報に対する責任は持たない。

- 自らが率先して行わない。つまりプロバイダーがメンバーの要請に応じて自動的に情報の送信を行う
- 受け手を選択しない
- 伝送される情報を修正したり選択しない

メンバーの違法活動が行われている事実を知っていながらサービスの提供を行った場合、免責は適用されない。ただし、違法な活動が行われていることを示す事実が存在することを知り、そのような活動に使われている情報を速やかに削除したり、アクセスを止めた場合には免責条項の適用を受ける権利を失わない。

これは米国の関連法を基礎としたもので、表現の自由の原則、仲介者によるメッセージ管理の不可能性を強調し、情報をモニターしたり、違法活動を追及する義務のないことを明確にしている。ただし次のものを除くと理解されている。

- 国家の安全を脅かすもの
- 刑事犯罪
- 選択、修正など情報への積極的介入
- 有害情報が流れることを知っていたにもかかわらず、撤回しないこと

ただし、裁判所や監督当局が違法活動を防止したり抑制するためにある一定期間、ある特定のサイトをモニターするよう要請する可能性もあることを否定するものではないとされている。

(3) 裁判所外での紛争解決メカニズム

インターネット上の違法行為はその速度と広範な地理的条件を特徴としている。また、取引価格が些細な金額のものであったり当事者の規模も小さい場合が多く、当事者もコストに対する懸念から法的措置の適用を控える傾向があり、訴訟外紛争処理のほうが適切であるように考えられている。

このため、この提案書では、紛争が発生した場合、適切な電子的な手段を含む、裁判所外紛争処理メカニズムが効率的に活用できるように法律を整備することを定めている。また、加盟国は紛争処理メカニズムに関する法的枠組み構築に関して、裁判所外紛争処理メカニズムの利用を制限する内容を盛り込んではならず、必要以上に複雑なものにしてはならないとされている。各国の規制当局間の相互理解、同意、ルールに基づいた協力体制が必要である。

3.2.1.2　非対面販売（Distance Selling）に関する指令

1997 年 5 月遠隔地販売に関する欧州指令が出されているが、ＥＵ加盟国はこの指令を 2000 年 6 月までに実施することになっており、今後ＥＵ全体で通販に同じ法律が適用されることになる。この指令は、消費者が主に通信販売「広い意味での通信の手段」を利用して成立した商取引契約に適用される。

(1) 情報項目

オンライン取引の場合、販売店の詐欺的な行為のリスクも考えられるため、この指令では、業者は、契約締結の前に一定の情報を提供する義務を有するとされている。相手からアプローチされる訪問販売的な場合、徹底した情報開示や特定の情報の書面による確認が必要とされ、この指令では消費者にオファーの時点で様々なの情報項目が列挙しなくてはならないとされている。これらの情報とは、次のようなものである。

何れかの隔地者間の契約を締結するに先立ち十分な時間的余裕をもって、消費者は、以下の情報を与えられなければならない。

(a)販売業者の名称及び前払いを要求する契約の場合には、その所在地；

(b)商品又はサービスの主要な特徴；

(c)全ての税金を含む当該商品又はサービスの価格；

(d)適用がある場合には配送料；

(e)支払、配送又は履行のための手配；

(f)解約権の存在、但し、第 6 条(3)項で言及される場合を除く；

(g)基本料金以外で計算される場合の遠距離通信手段の利用料金；

(h)提供又は価格が有効である期間；

適用がある場合には、恒久的又は反復して履行される商品又はサービスの提供を目的とする契約の場合の、最短契約期間等。

(2) 返品権利

オンライン取引の場合、情報不足であったり、画面上で見る商品と異なった商品が届けられるリスクもある。このため、消費者は 7 日間以内に（距離）販売契約を撤回する権利を有するとされている。

消費者の７日の契約解約権については、いずれの契約においても消費者は違約金を支払うことなく、また理由を示すことなく契約を解約できることになっている。解約権の行使を理由として消費者に請求され得る唯一のものは、当該商品を返却するための直接費用のみである。返品の規定は今後、欧州で一様になる。

但し、一定の例外があり、当事者が別途の合意をした場合を除き、消費者は解約権を次の契約については行使できない。

- **サービスの提供を目的とする契約であって、7 営業日の期間満了前に、消費者の同意を得て履行が始まった場合**
- **商品又はサービスの提供を目的とする契約であって、その価格が供給業者の管**

理し得ない金融市場での変動に左右されるものである場合

- 消費者の仕様に合わせて製造されたもの若しくは明確に個人用のもの、又はその性質上返品できない、急速に品質が劣化する若しくは消滅するものの提供を目的とする契約
- オーディオ若しくはビデオの記録又はコンピュータのソフトウェアの提供を目的とする契約で、消費者がそれらを開封した場合
- 新聞、定期刊行物及び雑誌の提供を目的とする契約
- 遊戯又は宝くじサービスを目的とする契約

(3) 納品義務

納品については消費者が発注した日から 30 日以内に実行しなければならない。この点について現実に問題となることはほとんど無いと考えられている。たとえばフランスでは通販会社の競争はいかに早く納品するかであり大手の通販会社は 24 時間以内に納品することを約束している。一方、販売店は、注文された商品又はサービスが供給不能であるとの理由で契約を実行しない場合、支払済みの金額について、30 日以内に払戻しを行わなくてはならない。

(4) カードの不正利用

消費者の金銭的な損害については、第 8 条において銀行カードによる支払いに関する条項を定めており、なりすましなどのカードの不正利用については消費者に対する支払いのキャンセルと支払い金の払い戻しの権利をうたっている。

(5) 参考：フランスの銀行法

フランスの銀行法にも同じような規定がある。バンキングカードを使っての通販において、たとえば盗難にあったカードにより不正利用された場合、消費者は取引を実際にしていないことを銀行に報告すれば銀行は支払い停止、払い戻しを行い、係争はその後スタートする。使用の立証は販売店側にある。例えば通販会社であれば、商品の到着証明などを行い、サービス（デジタルコンテンツなど）の場合は、いつ何をどのように提供したかログを記録しておき、それが裁判の証拠になる。

従って、このような不正利用の場合その取引に関する責任、不正利用額は全て通販業者のほうに転嫁され、銀行も消費者も何の影響も受けない場合も多いとのことである。

ただし、暗証番号を入れた場合には一律の払い戻しは受けられない。暗証番号が正しく入力された場合には、消費者が自分が利用していないことを立証しなくてはならない。法律では電子署名や暗証番号が入力されている場合には事後否認しても自動的には払い戻しが行われないことが定められている。

3.2.1.3　ＥＵにおける消費者のリスク負担ルール（１５０ＥＣＵルール）について

一般的に 150ＥＣＵルールと呼ばれるもので、米国における 50 ドルルールに相当する消費者保護を目的としたルールである。1997 年に公表した「電子的支払手段による取引における発行者と保有者の関係に関する委員会勧告」において電子的支払い手段の紛失および盗難による保有者の損害金額の上限を 150ＥＣＵとしているものである。

しかしながら 150ＥＣＵルールは、ＥＵにおいては勧告（リコメンデイション）という位置付けのため、指令（ディレクティブ）とは異なり、加盟国に対して強制力を持たない。現状加盟国が、本 150ＥＣＵルール以上の消費者保護を行っていれば、あらためての立法は不要である。

150ＥＣＵルールについて概要ならびに適用範囲等を以下に説明する。

(1) １５０ＥＣＵルールの概要

① 制定の背景

ＥＵが本勧告を行った背景は以下の通りである。

１．決済システムが非常に重要な部分であるＥＵ域内の市場の完全な機能を確約することにある。

２．ＥＵ域内全体で各個人と事業者が電子決済手段を使用できることが重要である。

３．電子決済手段に対する消費者の信頼および販売店の受託を促進させることにより、将来の電子取引時代に貢献すること。

４．取引の透明性を図るために、取引業務後および契約締結時点での適切なレベルでの顧客情報を確保するための最低要領を定めること。

５．電子決済手段を利用する関係当事者の責務と責任に関する最低条件を規定すること。

６．電子決済手段の分野において高レベルの消費者保護を確保すること。

７．保有者の決済指示に対する発行者の実行不能または実行不全、および保有者が承認しなかった取引に対する発行者の責任を明確にすること。

② 150ＥＣＵルールの適用範囲

この勧告の適用範囲としては以下の２点である。

- **資金の為替（決済）。ただし金融機関が発注・履行し、電子決済の手段によって実行されたものを除く。**
- **金融機関等の敷地において、現金自動支払機、現金自動預け払い機などの機器を利用した電子決済手段による現金の引き落としおよび電子マネーのローディング（およびアンローディング）。**

また適用範囲外としては以下の 2 点である。

- **小切手による支払い**
- **小切手による支払いに関連した特定カードの保証機能**

本ルールにおいて適用される取引としては、銀行キャッシュカードの預け払い、電子マネー決済、さらに遠隔地取引としてのデビットカード、電子マネー、電話・ホームバンキング等が対象となっている。

③　消費者の義務と責任

消費者は電子決済手段を利用するにあたって本ルールでは以下の通り定めており、保有者としての義務を果たしたうえで、責任の上限額が150ＥＣＵとされている。

当然に保有者の不正行為や重過失による損害は、150ＥＣＵルールが適用されないため、保有者の責任となるが、電子決済手段を使用する上で保有者の不正行為や過失をどのように証明するかは、本ルールでは規定されていない。

A.　義務

1．電子決済手段の発行および使用に適用される条件によって、電子決済手段を使用すること。
2．以下の事項を知ったあと、直ちに発行者へ通告すること。
・電子決済手段、またはそのアクセスデバイスを損失、紛失した場合
・保有者が未承認取引を知った場合
・発行者による勘定の維持における誤り等
3．電子決済手段とともに保管または持ち歩くアイテム上に、判別しやすい形式で個人のＩＤ番号または他のコードを記録しないこと。
4．電子決済手段を利用した発注を取り消さないこと。ただし発注の際に金額が決定していない場合は除く。

B.　責任

1．保有者が通知するまでに電子決済手段の損失または盗難の結果として被った150ＥＣＵを超えない金額で損失を負担する。ただし、重過失行為を行ったり、不正行為を行った場合は、上記限度額は適用されない。
2．不正行為の場合を除いて、上記義務２を履行した直後からは、保有者は電子決済手段の損失または盗難の結果として発生した損失に対して、その後の責任を一切負わない。
3．決済手段の具体的な表示または電子的な識別を行わずに決済手段が使用された場合に、保有者は責任を負わない。秘密コードまたは他の同様な身分確認証拠の使用は、それ自体では保有者の責任を負わせるには不十分である。

④　発行者の義務と責任

150ＥＣＵルールにおいては、保有者の他に発行者としての義務と責任も明確にしている。

A. 義務

1. 条件変更に関する部分

発行者は電子決済手段の提供についてその条件を変更することができるが、変更を通知するにあたっては、十分な期間（１ヶ月以上）を与える必要がある。１ヶ月以上たっても保有者が撤退（解約）しない場合は、その条件を受諾したものとみなす。

2. 運用に関する部分

・保有者以外に当者のＩＤ番号または他のコードを開示しない。

・保有者から依頼されていない電子決済手段を発送しない。

・取引の追跡を行い、誤りを是正できるよう長期間にわたり内部記録を保管する。

・保有者が身分証明番号または他のコードを開示するよう要求がなされた場合は、適切な手段で通知する。（例えば電話で通知する場合は、通知を行ったことを証明する手段を提供する）

・取引に関して保有者と紛争が生じた場合、保有者が作成するかもしれない反対の旨のいかなる証明に対して既得権を侵害することなく、下記の事項を証明する。

ａ.取引は正確に記録され、口座に記入されたこと。

ｂ.取引は技術的故障または欠陥による影響を受けなかったこと。

B. 責任（一部省略）

発行者は下記に対して責任を負う。

1. 第１条（1）における保有者の取引の不履行または不完全な履行。このことはたとえ取引が発行者の直接的なまた占有的管制下にない装置・端末機または機器を通して開始された場合でも変わりはない。ただし発行者が使用の認可を受けていない装置・端末機または機器で取引を開始した場合はこの限りではない。

2. 保有者口座の維持に関して発行者が引き起こした誤りまたは不正ならびに保有者が認可しない取引

3. 発行者は、電子マネー手段の保有者に対して、その手段に蓄積された価値の損失金額、および保有者の取引の不完全な履行に関して、その損失または不完全な履行が、手段または使用認可を受けた装置・端末機または他の機器の機能不全が原因である場合は、責任を負う。ただしその機能不全が保有者による故意の行為、または第 3 (3) (a) 条の契約違反による場合はその限りではない。

3.2.2　英国５０ポンドルール

同ルールは 1974 年消費者保護法（Consumer Credit Act）を準拠法としている。クレジットカードの盗用・誤用の場合、50 ポンドを限度に設定された損害負担の適用ルールが存在する。これはクレジットナンバーの盗難・盗用がカード代金の請求時に発覚した場合、これをカード会社に連絡し、自分の無実を証明すれば請求から除外される。つまり、100 ポンド盗用された場合は 50 ポンドが自己負担となる。ホルダーが無実と認められない場合には全額負担となる。

一方、銀行カード取引については英国銀行協会において自主規制ルールとしてバンキングコード（所謂 50 ポンドルール）が存在する。これは銀行のＡＴＭやテレフォンバンキングなどに限らず、デビットカードや電子マネーまで含め、幅広い消費者保護を謳っている。以下、その概要を説明する。

3.2.2.1　不正利用に関する規定

(1) カードの盗難･紛失時の連絡方法

小切手帳、通帳、銀行カードまたは電子マネー（電子財布）を紛失したか、盗まれたこと、または誰か他人がＰＩＮ、暗証番号または一定の個人情報を知ったと考えられる場合、電話にて連絡することを推奨している。（以下、関連コード）

コード４．１０　われわれに通知する最も早い方法は電話を使うことです。以前にお知らせした番号、または電話帳の番号まで通知して下さい。

コード４．１１　あなたがわれわれに小切手帳、通帳、カードまたは電子財布を紛失したか、盗まれたこと、または誰か他人があなたのＰＩＮ、暗証番号または一定個人情報を知ったことを通知したときは、われわれはそれらがあなたの口座へのアクセスに使用できないような措置を直ちにとります。

(2) 不正利用金額の返還

次に上記の通知後に行われた不正利用、銀行カードを受け取る前に行われた不正利用、銀行システムの故障による不正利用についてはその取引金額を利息および手数料とともに返還することを述べている。（以下、関連コード）

コード４．１２　次の場合には、われわれはあなたにその取引金額を利息および手数料とともに返還します。

・あなたがカードを受け取っておらず、そのカードが他人によって悪用された場合

・あなたがわれわれに誰か他人がＰＩＮ、暗証番号または一定の個人情報を知ったと通知した後に発生した、あなたが承認していないすべての取引

・あなたがわれわれに電子財布を紛失したか、盗まれたか、または誰か他人がＰＩＮを知ったことを通知した後に、あなたの口座からその電子財布にお金が移転され

た場合

・ＡＴＭまたは関連のシステムに故障が生じたが、利用した時には故障したことが明白でないか、または警告する表示もしくは掲示がなかった場合

(3) 電子マネーの規定

電子マネーについても規定を設け、消費者の不正利用による負担額を定めていることは興味深い。電子マネーの紛失、盗難などによる上記通知以前の不正利用額に対する消費者の負担額は最大で 50 ポンドに限定している。（以下、関連コード）

コード４．１３　あなたは電子財布を財布のなかの現金と同じように取り扱って下さい。電子財布を紛失したり、盗まれたときは、その中の未使用残高は財布を紛失した場合と同じように失われます。しかし、あなたがわれわれに紛失したことや盗まれたことや悪用されたことを通知する前に、あなたの口座から承認なしにお金が引き出され、電子財布に入金記帳された場合は、あなたが不正な行為をしたり（Act flaudulently）、著しく不注意である(with gross negligence)場合を除き、その金額に対するあなたの債務は最大で 50 ポンドに限定されます。

(4) 銀行カードの不正取引

銀行カードについても同様に紛失、盗難などによる上記通知以前の不正利用額に対する消費者の負担額は最大で 50 ポンドに限定している。また、消費者がカードを確かに受け取ったことや消費者の不正行為や著しい不注意に関する疑義については銀行側に立証責任がある。（以下、関連コード）

コード４．１４　あなたがわれわれにカードを紛失したこと、盗まれたこと、または誰か他人がＰＩＮを知ったことを通知する前に、あなたのカードが悪用された場合には、あなたが不正な行為をしたり、著しく不注意である場合を除き、あなたの債務は最大 50 ポンドに限定されます。

コード４．１５　カード取引に紛争がある場合、われわれは不正な行為や著しい不注意、またはあなたがカードを受け取ったことを立証する責任を負います。そのような場合、われわれはあなたが、捜査に関してわれわれおよび警察と協力することを期待します。

(5) 消費者の重過失について

このような不正利用が本人の不正または著しい不注意(flaud and gross negligence)によるものである場合には、不正利用額の全額を消費者本人が負担することになる。具体的に著しい不注意とは銀行カードに暗証番号を書いた紙を貼り付けておき、それを盗まれた場合などである。（以下、関連コード）

コード４．１６　もし、あなたが不正な行為を行った場合には、あなたはすべての

損失を負担することになります。もし、あなたが著しい不注意な行為を行い、その結果、損失が生じた場合には、あなたはその損失を負担することになります。これは、あなたが４．８に規定された予防策に従わなかった場合に適用されます。

3.2.2.2　個人情報およびマーケティング

(1) 情報提供の可否

サービスや商品の情報の提供について消費者に受け取りの意思があるかどうかの確認をすることとしている。また、最低 3 年に１度その種の情報を受け取りたくないかどうかの確認を実施することとして、消費者に情報提供の可否の権利を与えている。（以下、関連コード）

コード２．１９　われわれは時々あなたの利益になるような新しいサービスおよび商品についてあなたにお知らせをします。しかし、あなたがこの種の情報を受け取りたくない場合には、お客様になった際にその旨を申し出ることができます。

コード２．２０　少なくとも 3 年に１回、われわれはあなたにこの種の情報を受け取りたくないと請求できることの注意を喚起します。

(2) プライバシーについて

最近のプライバシーに関する関心を反映し、消費者の名前および住所をマーケティング目的で、銀行のグループ企業を含め、他のどのような会社に対しても提供することはないとしている。（以下、関連コード）

コード２．２１　あなたが特に要求した場合、または書面で同意を表明した場合を除いて、われわれはあなたの名前および住所をマーケティング目的で、われわれのグループ企業を含め、他のどのような会社に対しても提供することはしません。基本的銀行サービスと引換えにあなたの承諾を得ることはありません。

コード２．２２　われわれはあなたに他の会社のサービスまたは商品を知らせることがあり、もしあなたが前向きに反応する場合には、あなたはその会社から直接接触を受けることもできます。

コード２．２３　われわれはマーケティング資料を無差別に送ることはしません。特に、われわれはあなたが 18 歳未満であるか、資料が借入および当座借越に関するものである場合には、選択を行い、注意を払います。

（以上のコードの翻訳資料について：金融 97 年 8 月号　全国銀行協会連合会調査部訳）

3.2.2.3　第３版改訂版の主な改訂点

自主規制の長所は消費者の要望や新商品の開発に迅速に対応できることに有る。第３版改訂版の改訂点もこのような特徴を反映している。これは預金金利が変動金利の英国では

金利の下降局面の場合、引き出し予告期間が長い 90 日の預金金利から金利を下げていくという事実があった（当然、引き出し予告期間が短い 7 日の預金金利の方が金利は低い）。

これは合法であったが、明らかに消費者に不公平で不利な内容である。このため、金利情報の提供方法、クーリングオフ、取引条件変更に関する事前通知予告期間などについて次のような規定を新設した。

(1) 金利について

２．１　当行が提供する貯蓄商品および投資商品についての金利に関する最新の詳細事項の入手先の情報を提供します。これには以下が含まれます。

・当行が通常、金利の変更通知を掲載する新聞。これらの新聞は、当行のお客様が読者層であることが反映されています。

・電話番号（複数の電話番号も含まれます）、および

・インターネットのＷｅｂサイトがある場合は、そのアドレス

(2) クーリング･オフについて

２．８　お客様が貯蓄口座もしくは投資口座（複数の口座も含まれます）について、ご自身の選択に満足がゆかない場合は（固定金利預金口座を除きます）、口座開設後 14 日以内に、当行はお客様の口座を切替えるお手伝いをするか、利息を付けて全金額を返済するかいたします。通知期間や追加料金は請求いたしません。

(3) 口座の閉鎖について

２．１１　われわれは、詐欺行為などの例外的な場合を除いてあなたの口座を少なくとも 30 日の事前通知なしに閉鎖することはしません。

(4) 取引条件の変更について

２．１２　取引条件は時々変更されることがあります。われわれは、こうした変更があなたにどのように通知されるかを知らせ、変更が効果を持つ前にあなたに少なくとも 30 日前の事前通知を行います。

２．１３　変更が明らかにお客様の不利になるような場合は、お客様に対して個人的にご連絡し、さらにお客様が希望なさるときは、口座を切替えるかもしくは口座を閉鎖することができるように、通知の日付から少なくとも 60 日間は、お客様の口座について通知期間を適用いたしません。この 60 日間については、切替もしくは閉鎖を行った場合でも、お客様は追加の料金もしくは追加の利息を支払う必要はありません。

(5) 手数料について

２．１５　基本的口座サービスに対する手数料を引き上げる場合には、われわれはあなたに少なくとも 30 日前の事前通知を行います。

(6) 金利について

２．１６　あなたの口座に適用される金利は、随時変更され得ます。金利を変更する場合、われわれはあなたに次のいずれかの方法により、その変更について通知します。

(a) 支店ベースの口座については、

30 日以内にレターもしくは電子メール、またはその他の個別通知によって、または変更から 3 営業日以内に支店の独自の通知および当行が通常利用している新聞への通知の掲載によって、変更をお知らせいたします。

お客様が利率をより比較しやすいように、当行の通知には先行する金利と新しい金利を明確に表示し、さらに

・お客様の電話によるお問い合わせによって、またインターネットのＷｅｂサイトがある場合は当行のＷｅｂサイトにて、お客様の口座に適用される先行する金利と新しい金利を入手できるようにし、

・当行のスタッフが常時お客様のお手伝いをいたします。

(b) 支店以外をベースとする口座については、

30 日以内にレターもしくは電子メール、またはその他の個別通知によって、変更をお知らせいたします。

(c) その他すべての口座については、

当行の貯蓄口座および投資口座のすべてについての金利を、お客様がより比較しやすいように、当行は少なくとも年に 1 度、これらの商品およびその時点で有効な金利の摘要書を送付いたします。但し、100 ポンドに満たない銀行通帳口座は除きます。この摘要書にはさらに、以下の事項が含まれます。

・明確に表示された新規取扱いを停止した口座

・当行が金利変更の通知を掲載するために通常利用する新聞名

・当行のお問い合わせ電話番号

・当行のインターネットのＷｅｂサイトがある場合は、そのアドレス

さらに、該当する年度において口座に適用された別の金利をお知らせします。

(7) 新規取扱いを停止した口座 (Superseded accounts) について

２．１７　当行は適宜、新しい貯蓄口座および投資口座を提供します。もし、お客様が新規口座が開設されないため、または口座の設定が積極的に行われていないために、固定金利預金口座以外の新規取扱いを停止した貯蓄口座および投資口座を保有している場合には、当行は、

(a) 新規取扱いを停止した口座について、現行の商品系列内の類似する特徴を持った口座と同一のレベルの金利を保持して適用するか、または

(b) 新規取扱いを停止した口座を、現行の商品系列内の類似する特徴を持つ口座に切替えるか、のいずれかを行います。

類似する特徴の例には、通知期間、払出の種類、自由に行える払出回数、口座の預入および払出方法が含まれます。これは、お客様の口座の金利が、現行の商品系列内の類似する特徴を持つ口座の金利と同一のレベルを、常時下回ることがないことを意味します。

２．１８　類似する特徴を持つ口座がない場合は、当行はお客様の口座の新規取扱いを停止した後 30 日以内に、口座の新規取扱いを停止したことをお伝えし、当行の他の口座について説明し、また、通知期間および追加費用を請求することなく口座を切替えるお手伝いをするためにお客様に連絡をいたします。

4　リスクの処理方法

4.1　保険

4.1.1　米国におけるＥＣ関連の保険

米国は訴訟社会と言われるように種々の問題解決に訴訟が起こされ、一方、その損害賠償額も我国に比べると極めて高額であることより、賠償責任に対する意識が高まってきた。特に電子商取引のような新しい分野においては、どのようなリスクがあるのか、その賠償額はどの程度の額なのかが不明確であり、企業活動を行う上では賠償責任保険を付保して事前にプロテクトしておくことは普通のことである。電子商取引のリスクに関する賠償責任保険は、事業主体により業務の内容もリスクの実態も異なることから、それぞれの企業に応じて保険設計をおこなっていくこととなる。一般の企業は、多様化した業務の一部として電子商取引を取り扱っているのが通常であり、企業の賠償責任を一括して保険の対象とする観点からは、企業総合賠償責任保険の中で電子商取引のリスクに対する保険カバーを取り込んでいくのが現実的である。事実、アメリカの電子商取引を行っている企業は、一般的にＣＧＬ（Commercial General Liability）と呼ばれる企業総合賠償責任保険に加入しており、その担保条件の中で電子商取引関連の保険カバーを手配している。

賠償責任保険は、何の損害に対する賠償責任を対象とするかによって、対物賠償責任保険、対人賠償責任保険および対人・対物以外の賠償責任保険に分類することができる。対物賠償責任保険は第三者の財物損壊に対する賠償責任を対象とし、対人賠償責任保険は第三者の身体障害に対する賠償責任を対象とするものである。また、業務上の過失により第三者に対人・対物事故を伴わない経済的損失を与えたことによる賠償責任を対象とする対人・対物以外の賠償責任保険もあり、Ｅ＆Ｏ（ERRORS&OMISSIONS）などがこれに当たる。電子商取引においては、様々な業務形態より対物賠償責任や対人賠償責任を伴わない経済的損失を与えたことによる賠償責任が多く、米国ではＥ＆Ｏ保険を付保する企業も増えている。

以下、ＥＣ事業に起因する第三者からの損害賠償責任リスクに対応する保険として,米国のＣＧＬ保険、Ｅ＆Ｏ保険、メディア賠償責任保険についての商品概要を説明する。

4.1.1.1　COMMERCIAL GENERAL LIABILITY 保険(CGL)

ＣＧＬは企業総合賠償責任保険であり、通常の賠償責任保険で担保する身体障害や財物損壊に加え、人格権侵害や広告宣伝に起因する賠償責任を担保する。ＥＣに関連する賠償責任のうち、名誉毀損等の人格権侵害には対応できているが、その他の知的財産権に対する賠償責任については広告宣伝行為に起因することが要件のため、ＥＣ全般での賠償責任には対応できない。さらに問題となるのは、米国における多くのＣＧＬの担保地域が米国（含米国領域）に限られていることである（いうまでもなく、インターネットは性質上、グローバルなものであり、担保地域を全世界とする必要がある）。

(1) 担保内容

以下、ＣＧＬ　ＩＳＯ‘９６フォームから人格権侵害と広告宣伝侵害に該当する部分を抜粋する。

① 第Ⅰ章　担保範囲

A. 担保条項Ａ：身体障害および物的損害に起因する賠償責任

省略

B. 担保条項Ｂ：人格権侵害および広告宣伝侵害についての賠償責任（保険条項）

1. 当会社は、この保険が適用される「人格権侵害」または「広告宣伝侵害」により被保険者が法律上損害賠償義務を負う金額を支払います。

2. この保険は、次に適用されます。

（１）記名被保険者の事業活動（記名被保険者が行うまたは記名被保険者のために行われる広告宣伝、出版、放送、テレビ放送を除きます）に起因する「人格権侵害」

（２）記名被保険者の商品、生産物または役務に関する広告宣伝活動の過程で発生した違法行為による「広告宣伝侵害」

② 第Ⅴ章　定義（抜粋）

1. 「人格権侵害」とは、次に掲げる違法行為に起因する障害で、「身体障害」以外のものをいいます。

（１）不正逮捕、拘留、留置

（２）誣告

（３）所有者、地主、貸主がまたはこれらに代わって個人が占有している空間、住居、敷地への不法侵入、これらからの不法追立またはこれらの中におけるプライバシーの権利の侵害

（４）個人もしくは団体を中傷、誹謗もしくは侮辱し、または個人もしくは団体の商品、生産物もしくは役務を非難する資料の口頭または出版物による公表

（５）個人のプライバシーの権利を侵害する資料の口頭または出版物による公表

2. 「広告宣伝侵害」とは、１つまたは複数の次に掲げる違法行為に起因する侵害をいう。

（１）口頭または出版物による、個人もしくは団体の誹謗または個人もしくは団体の商品、生産物もしくは役務の中傷

（２）口頭もしくは出版物による、個人のプライバシーの権利の侵害

（３）宣伝上の着想、営業上の形態の不正な流用、または、

（４）著作権、標題もしくは標語の侵害

3. 「身体障害」とは、人の身体の障害および疾病をいい、時期のいかんを問わず、これらに起因する死亡を含む。

4. 「物的損害」とは、次に掲げるものをいう。

（1）有体物に対する物理的損傷。これには、その結果発生するその財物の使用不能損害をすべて含む。これらのすべての使用不能損害は、その原因となった物理的損傷の発生時に生じたものとみなす。

（2）物理的損傷を被っていない有体物の使用不能損害。これらのすべての使用不能損害は、その原因となった「事故」の発生時に生じたものとみなす。

(2) 免責条項

この保険は、次に掲げる場合には適用されません。

① 次の事由による「人格権侵害」または「広告宣伝侵害」

事実に反することを知りながら、被保険者によりまたは被保険者の指示に基づいて行われた口頭または書面による公表に起因する場合

② 次の事由による「広告宣伝侵害」

（1）契約違反によるもの。ただし、黙示の契約下での広告宣伝上の考案を不正使用した場合を除く。

（2）広告宣伝された品質または性能に商品、生産物または役務が適合しないことによるもの

（3）商品、生産物または役務の価格表示の誤りによるもの、または

（4）宣伝、放送、公表またはテレビ放送を事業とする被保険者により行われた違法行為によるもの

(3) 担保地域

「担保適用地域」とは、保険証券に記載された国または地域

4.1.1.2 メディア賠償責任保険

出版、放送、広告宣伝事業者のリスクに対応する専用の保険。ＣＧＬで担保する人格権侵害、広告宣伝に起因する損害賠償責任に加え、Ｅ＆Ｏでも基本的には担保されない著作権侵害、商標権侵害を担保する。ＥＣ事業の範囲が企業の製品やサービスに関する情報を表示するためだけの受動的なＷｅｂページに限定され、かつ、高度な情報交換（電子商取引）が行われない場合はこの保険での対応が可能である。

以下、放送事業者向けのメディア賠償責任保険について例示する。

(1) 担保内容

① コミュニケーション賠償責任担保条項

被保険者により、またはその承認のもとに行われた番組放送活動に起因して、次に掲げる行為に基づき被保険者が法律上の損害賠償責任を負担することによって被る損害を担保します。

- 文書、口頭、図画その他これらに類する表示行為による名誉毀損、侮辱または信用毀損
- **商品、サービスに対する誹謗**
- **不法侵入、私的事実の暴露、虚偽の事実の通知または氏名等の不当利用その他これらに類する行為によるプライバシー侵害**
- **作為または不作為による誤った表現もしくは誤解を生む表現。ただし、広告宣伝行為に起因するものに限ります。**
- **情報またはアイデアの盗用または不正使用**
- **著作権侵害**
- 商標権侵害

② 人格権侵害賠償責任担保条項

被保険者により、またはその承認のもとに行われた放送のための取材、撮影その他の番組制作活動に起因して、次に掲げる行為に基づき被保険者が法律上の損害賠償責任を負担することによって被る損害を担保します。

- 文書、口頭、図画その他これらに類する表示行為による名誉毀損、侮辱または信用毀損
- 商品、サービスに対する誹謗
- 不法侵入、私的事実の暴露、虚偽の事実の通知または氏名等の不当利用その他これらに類する行為によるプライバシー侵害
- 不当な身体の拘束または悪意の訴追
- 不法侵入、盗聴その他の行為による私生活の侵害

(2) 填補される損害

- 法律上の損害賠償金
- 争訟費用

(3) 主な免責

- 故意によって生じた賠償責任
- 宣伝、広告等がなされた商品もしくは役務についての保証義務違反または信頼関係違背に起因する賠償責任
- 身体障害、財物損壊に起因する賠償責任
- 犯罪行為、詐欺行為、不誠実行為または罰金、科料に起因する賠償責任

4.1.1.3 E&O

一律の定義はないが、専門的な職業危険を担保する保険であり一般の賠償責任保険やＣＧＬで担保されない無形の経済損害を主に担保する。担保地域も全世界である。Ｅ＆Ｏの担保内容は「Ｅ＆Ｏカバー」をベースとして自由自在に修正することが可能なため、ＥＣ事業内容に則した保険設計が可能であり、ＥＣ事業者向けに各保険会社から担保内容が異

なる保険が販売されていると考えられる。

以下、ＥＣ事業を幅広く担保するＥ＆Ｏの実際の商品内容について、典型的なインターネット事業者向け賠償責任保険の担保内容を例示する。

(1) 担保内容

① 被保険者の提供する有料の下記サービスに起因する不法行為
（義務違反、不作為、瑕疵、虚偽表示、誤解を招く表示または遺漏）

- **コンピュータのハードウエアまたはソフトウエアの設計、プログラミング、データ処理、コンサルティング、サービス、配給、インストールおよびメンテナンス、並びに使い方の講習を含む。**
- **世界規模のコンピュータ・ネットワークであるインターネットへのオンライン・アクセスを提供するＩＳＰのサービス**
- **広告を含むインターネット・サイトの設計、構築、メンテナンス**
- **インターネット上で使用する暗号化ソフトウエアの開発、インストール**
- **電子メールサービス**
- **チャット・ルームまたは掲示板のメンテナンス**

② 有料または無料のインターネット・サービスの実行において下記に関するもの

- **著作権侵害、およびそれに関連した不正競争。ただし、コンピュータ・ソフトウエアの著作権侵害は含まない。**
- **商標権侵害、およびそれに関連した不正競争**
- **非認可のアクセス。認可を得ずに、または認可の範囲を超えて、コンピュータ、コンピュータ・システム、またはコンピュータ・ネットワークに第三者がアクセスすること。ただし、被保険者によるアクセスを含まない。**
- **コンピュータ・ウイルス。プログラムまたはコードを受信するコンピュータ、コンピュータ・システムまたはネットワークの所有者または責任者である個人または法人の認可なくして、プログラムまたはコードの有害または破壊的な要素の送信が生じた場合にコンピュータ、コンピュータ・システムまたはネットワークに危害を加えるプログラムまたはコード。**
- **被保険者により、または被保険者の許可を持って普及されたデータに基づき、第三者が行動することで損失をもたらす義務違反、不作為、瑕疵、虚偽表示、誤解を招く表示または遺漏。ただし、第三者は被保険者と共通の所有権に関する利害または、その他の提携関係を持たないものとする。**
- **個人に対する侵害。名誉毀損、または中傷などの人格権侵害。文書誹毀、口頭誹毀、商品の中傷、取引物誹毀、精神的苦痛を加えること、暴行または乱暴な行為を含む。**

(2) 免責条項（主なもの）

- **身体障害または財物損壊**
- **特許権侵害**
- **被保険者がＩＳＰとしてサービスを提供している場合における、被保険者のサービスの中断または完全停止に起因する請求。**
- **非電子的な手段でパスワードを入手することから生じる、非認可のアクセスに起因する請求。**

(3) 担保地域

全世界。本保険約款は被保険者が世界中のどこで犯した不法行為についても適用される。

上記の通り、ＥＣに適合する保険としては、経済損害を担保するＥ＆Ｏと人格権侵害、著作権侵害、商標侵害を担保する MEDIA LIABILITY を結合したような専用の保険が必要であるように考えられる。ただし、現状では、「Ｅ＆Ｏ保険カバー」を基本として人格権侵害、著作権侵害、商標侵害を担保することが可能なため、最近ではＥ＆Ｏをオーダーメイド的に変更して保険設計を行う傾向があるようである。

4.1.2 欧州におけるＥＣ関連の保険

ＥＣに関連する保険として、主に欧州のカード保険を中心にまとめを行った。

4.1.2.1 イギリスの事例

イギリスにおける銀行とカードホルダーの責任分担及びカード保険の一例として National Westminster Bank の個人預金口座およびクレジットカードの加入申込書より入手した情報を紹介する。

(1) クレジットカードの責任分担

クレジットカードの紛失、盗難もしくはカードの暗証番号が他人に知られてしまった場合において、カードホルダーに銀行への迅速なる届出を義務付けている。

盗難などによるカードの不正使用にかかわる損害について、カードホルダーの負担責任を 25 ポンド限度としており、さらに銀行への届出後におけるカードホルダーの負担を免除している。

ただし、カードホルダーの重大な過失による不正使用について、その全損害はカードホルダーの負担としている。重大な過失の具体例としては、カードホルダーがカードの使用を他人に許可しているケースなどが挙げられる。

(2) 個人預金口座カードの責任分担

カードの紛失、盗難もしくはカードの暗証番号が他人に知られてしまった場合、銀行への迅速なる届出をクレジットカードと同様にカードホルダーに義務付けている。

盗難などによるカードの不正使用にかかわる損害については、カードホルダーの負担責任を 50 ポンド限度としており、さらに銀行への届出後におけるカードホルダーの

負担を免除している。カードホルダーの重大な過失による不正使用について、その全損害はカードホルダーの負担としている点もクレジットカードと同様である。

(3) カード保険「NATWEST CARD PROTECTION」

NatWest ではカードホルダー向けの保険としての NATWEST CARD PROTECTION を提供している。この保険は、Natwest のカード以外でも、予め被保険者が届け出を行えば、その被保険者が所有するキャッシュカード、クレジットカード、デビットカードをすべて保険の目的とすることができる。

なお、これらのカードホルダーに与えられる補償においては、カードの紛失や盗難による不正使用について、キャッシュカード、クレジットカード、デビットカードにおける損害を特に区別していない。保険会社は、それぞれのカード機能としてのリスクを、特に異なるものと判別しないためと考えられる。

① 対象カード

single policy では、カードホルダーが所有する全てのカード（キャッシュカード、デビットカード、クレジットカード）が対象である。また、joint policy では、同居の家族が所有するカードも対象にすることが可能になる。

② 対象となる事故

カードの紛失または盗難にかかわる不正利用

③ 加入方法

カードの申込時に一緒に申し込む。保険料はカードホルダーの口座から引き落とされる。

④ 保険期間

１年間と３年間がある。

⑤ 保険料

	Single policy	Joint policy
１年間	£１０	£１６
３年間	£２５	£３９

なお、Gold card 口座の場合は、無料で補償を受けることが可能になっている。

4.1.2.2 フランスの事例

フランスのキャッシュカードはクレジットカードと一体化しており、CARTE BLEUE と呼ばれている。CARTE BLEUE での支払いは、月末一括支払いと即時引き落としの２通りから選択することができる。

銀行によっては、こうしたカードの利用者向けにカード保険を用意しているが、概要は以下の通りである。

① 対象となるカード

当該銀行が発行するカード（キャッシュカード、クレジットカード両機能を有する）。

② 対象となる事故

- **紛失または盗難にかかわる不正利用**
- **当該銀行口座より引き出した現金が 48 時間以内に盗難された場合**
- **口座名義人の身分証明書が紛失または盗難された場合の再発行費用**
- **カードと同時に自宅やマイカーの鍵が紛失または盗難された場合の交換費用**

③ 加入方法

希望者は銀行を通じて申し込む。保険料はカードホルダーの口座から引き落とされる。

④ 保険期間

１年間

4.1.2.3 ベルギーの事例

ベルギーの保険会社、銀行、保険ブローカー及び BANKSYS 社に対するヒアリングによれば、ベルギーにおいてはカード保険は存在していなかった。そもそも銀行側並びにカードホルダー側に保険のニーズは無い様子である。これはカードホルダーの責任が、150 ユーロに限定されていることが理由になっているようである。

4.1.2.4 その他の電子商取引関連の保険

ロンドン保険市場においてインターネットプロバイダー、オンラインサービスベンダー、システムアナライザー、デザイナー、Ｗｅｂサイト所有者などを対象とした賠償責任保険が商品化されている。同保険は被保険者のサイバースペースにおけるサービス業務上の、過失などによって生じる第三者に対する金銭的な損害賠償責任を補償するものである。

具体的にはコピーライトやトレードマーク、タイトルやスローガンなどに対する侵害などによって被る賠償責任を対象とする。内容的には米国におけるＥＣ事業者向けのＥ＆Ｏ保険とほぼ同様のものである。保険商品としてはラインナップされているが、調査時点における販売実績は少ないとのことであった。欧州においては、商品としての将来性は有るものの、急激に販売実績が伸長するとは考えにくい。参考までに、商品の概要についての資料を添付する。（表 4-2 参照）

表 4-1 キャッシュカード・デビットカードの保険に関する海外事情

	アメリカ	イギリス	フランス	ベルギー	ドイツ
デビットカードの普及状況	欧州ほどは普及していない。	普及している	普及している	普及している	普及している
カード保険の有無	カードの不正利用を担保するカード保険は確認できていない。	一部の銀行では導入しいる。	特定のカード向けに個人加入のカード保険がある。	カード保険はない。	金融機関の業界団体(the German association for private banks)による団体保険制度がある。
カード保険の付保方式	――――――	ｶｰﾄﾞﾎﾙﾀﾞｰが口座開設時に任意に銀行に申し込む。	個人契約。	―――――――	詳細は不明
カード保険の普及状況	――――――	必ずしも全ての銀行で制度があるわけでない。	普及状況については不明	―――――――	大手金融機関は本制度には加入していない。（自家保険化している模様。）
利用者保護のルール	ＥＦＴ法により、利用者の損害負担は５０ドルまでに限定されている。	ＢＢＡのﾊﾞﾝｷﾝｸﾞｺｰﾄﾞにより、利用者の損害負担は５０ポンドまでに限定されている。	全国消費者評議会など消費者保護団体と業界団体が利用者保護ルールを協定しており、無権限なカード取引については、利用者は保護されている。	利用者の損害負担は１５０ユーロに限定されている。（欧州委員会の勧告である１５０ＥＣＵルールに基づくものであるかは確認できていない。）	詳細不明であるが、原則的には利用者の自己責任。ただし、電子財布機能については利用者最大負担はDM400（電子財布にﾘﾛｰﾄﾞできる金額がDM400となっている様子。）
その他			ＩＣカード化が進んでいる。	プロトン（電子マネー）も普及。	ゲルトカルテ（電子マネー）も普及。

表 4-2 サイバースペースＥアンドＯ保険の概要

サイバースペースＥアンドＯ保険

対象：　インターネット・アクセス・プロバイダー、商業オンライン・サービス、システムオペ、フォーラム運営者、オンライン・サービス・ベンダー、コンピュータ・システム分析およびデザイン、パッケージおよびカスタム・ソフトウェア・プログラミング、バッチおよびオンライン・データ処理、他人のためのソフトウェアまたはハードウェアの付加価値販売、および、Ｗｅｂサイト所有者

主な担保内容：　サイバースペース業務を実行中に、保険担保されたサービスに起因する不正な行為によって金銭的な損害を被ったと主張する第三者損害賠償請求に対する保険。「不正な行為」の定義には、以下に対する担保が含まれる：すなわち、誤り、不作為、過失；文書による名誉毀損、口頭による名誉毀損、プライバシーまたは周知性の侵害；著作権、商標、称号またはスローガンの侵害；アイデアの盗作、詐称通用または不正流用、および不正なアクセスを防止しなかったこと。オプションの保険担保には、偶発的な身体傷害および物的損害に起因する第三者請求のための保険がある。

地域または管轄：　全世界

資格：　少なくとも 3 年以上の実務経験がある申込者、または、同種のサービスを提供することに有益な経験をした経営者または本人がいる業務拡大中の会社の申込者が望ましい。顧客との間で標準的な契約書を使用し、創造的な業務、デザインおよびコンテンツ製作のために法的な検証手続を備えている申込者が望ましい。ハードウェア製造業者、コンピュータ支援の製造業および生産過程管理システムは、一般に本プログラムでは引受の対象とはならない。

引受可能限度額：　基本的な引受可能限度額は総計 1,000 万ポンド。
更に高い限度額および超過担保は引受可能。

最低保険料：　総計 25 万ポンドの限度額に対して 1,000 ポンド

自家保険額（免責）：カテゴリーによるが、各クレームにつき最低 2,500 ポンド

必要な情報：　サイバースペースＥアンドＯ保険申込書、業務を記載したパンフレットまたは宣伝資料、標準的な契約書の写し、財務諸表；幹部社員の履歴書

4.1.3　日本におけるＥＣ関連の保険

4.1.3.1　ＥＣ当事者ごとのリスクと保険

ここでは、広くＥＣに関わる当事者全体に対象を広げて、いかなるリスクが存在するのか、いかなる保険が対応するのかについて整理を行った。

保険については、ＥＣ当事者のうち、どの当事者がどういうリスク負担をするのかによっておのずと対応する保険も、また保険契約の当事者も異なってくる。

現状では「ＥＣ向け保険」として汎用性のあるものは少なく、ＥＣ当事者（販売店・モール運営者・認証局など）がＥＣ以外のリスクも含め、保険会社と個別に補償内容、保険料等を定め、保険契約を締結しているケースが多い。

ここでは、ＥＣ当事者のうち、販売店、モール運営者、認証局などの事業者に共通するリスクと対応する保険についてまず概観した後、「ＥＣ特有のリスク」と対応する保険について、各当事者ごとに列挙する。なお、ＥＣに関連する保険については、既に新聞・雑誌等で公表されており、ここでは今後さらに普及の見込まれる保険にのみ触れる。今後ＥＣが消費者にさらに浸透するにしたがって、これらの保険がより多くのＥＣ当事者に受け入れられていくことが期待される。

(1) 事業者に共通するリスクと保険

ＥＣ当事者のうち、「事業者」として括ることのできる主なものとして、①販売店、②モール運営者、③ＳＥＴ運営者、④認証局が挙げられる。なお、以下の説明において、すべてＥＣにおける代表的な決済方法であるクレジットカード決済を前提としているため、銀行、コンビニ等の決済機関は考慮の対象から除いている。

①～④の事業者に共通するリスクとして考えられる主なものを列挙すると、以下のようなリスクと対応する保険がある。

1. **火災、破裂・爆発、風災、水濡れ等**
   →火災保険
2. **コンピュータ機器の破損、ハード機器内メディアの破損、またこれらの事故に伴う営業損害、営業継続のために発生した費用損害**
   →コンピュータ総合保険
3. **建物が火災などで損害を被り、生産活動や販売活動が阻害されて生じる休業損害、営業継続のために発生した費用損害**
   →利益保険、営業継続費用保険
4. **事業者の所定の業務遂行上、過失により他人に身体傷害を与えたり、他人の財物に損壊を与えた場合に生じる法律上の損害賠償責任**
   →施設所有者・管理者賠償責任保険

(2) 販売店

販売店のリスクについては、消費者その他第三者に対して法律上の損害賠償責任を負担するケース、および法律上の損害賠償責任は負わないが、消費者との間で交した

損害負担に関する取り決め（規約、約款など）の中で、販売店側が損害を負担するケースがある。

前者の法律上の損害賠償責任を負担するケースとして、以下のようなものが考えられる。

- 販売店のサーバが不正アクセスされ、消費者の個人情報が漏出、被害者よりプライバシーが侵害されたとして、不法行為に基づく損害賠償請求を受けた。
- 販売店が自ら管理する消費者のクレジットカード番号情報が漏洩し、第三者に悪用され、当該カード会員より不正使用された分につき不法行為に基づく損害賠償請求を受けた。
- 販売店のサーバがウイルスに感染し、それにアクセスした消費者のパソコンが同様にウイルス感染し損害を被ったとして、消費者より不法行為に基づく損害賠償請求を受けた。
- 販売店がネット上に掲載した内容が著作権を侵害するものであったとして、著作権者より、不法行為に基づく損害賠償請求を受けた。

これらのケースで、販売店側の故意または過失が認められた場合は、販売店は法律上の損害賠償責任を負担しなければならない。

法律上の損害賠償責任を負担するケースに備える保険として、各種の賠償責任保険があるが、中でも代表的なものとして、情報サービス業者・電気通信事業者賠償責任保険、および施設所有者・管理者賠償責任保険がある。これらの保険は無論ＥＣリスクに限るものではなく、販売店の業務全体を対象としている。各保険の内容については、後記する。

(3) モール運営者

消費者がバーチャルモール内の販売店で買い物をする際に、何らかのトラブルにより経済的損害を被った場合に、販売店ではなくモール運営者の法的責任を問題にするケースがありうる。これは、消費者が販売店と取引をするに際して販売店そのものよりも当該バーチャルモールの社会的信用性を重視する場合が考えられるからである。ただ、この場合に、モール運営者の法的責任が実際に肯定されるためには、第三者による不正行為による損害の発生に関しても、システムの安全性や販売店の信頼性を確保すべき義務が、モール運営者に存在することが前提となる。この判断は、まだ判例上、学説上とも、確立されたものはない。

また、販売店の営業主体がモール運営者であると消費者が誤認するのもやむを得ない外観を呈する場合には、モール運営者の法的責任が認められるケースが考え得るが（例えば商法第 23 条「名板貸責任」）、これについても、リアルの店舗やテナントの場合と同列に論じられるものであるかどうかは、判例上も学説上も定まっていない。

以上のように、モール運営者が法律上の損害賠償責任を負担するケースは、可能性として挙げることはできても、現実に認められるケースは、極めて限られると言える。

また商慣習上も、モール運営者が原則として責任を負担しない旨をモール約款等でうたっているケースが多い。したがって、現状では、モール運営者の賠償責任リスクに備える賠償責任保険（具体的には情報サービス業者・電気通信事業者賠償責任保険）が有効とは必ずしも言えるものではないが、モール運営者側のリスク管理として、消費者から直接賠償請求された場合にどう対応するかという問題は、今後ますます重みを増してくるものと考えられる。

(4) ＳＥＴ運営者

ＳＥＴは、マスターカード社とＶＩＳＡ社が共同で設けた電子決済用の統一規格である。デジタル署名による本人認証を行って不正使用を排除すると共に、ＥＣに関するデータを取引データと決済データに分けてそれぞれを別々に暗号化し、販売店側は取引データのみを復号化でき、クレジットカード会社側は決済データのみを復号化できる仕組みである。この方式は、公開鍵暗号方式を利用してカードホルダーの本人認証と送信データ自体の暗号化により、通信途上だけでなく販売店内部者による不正行為の防止も念頭に置いたものである。現在日本国内でクレジットカード会社をはじめ10社程度の事業者がＳＥＴを運営している。

ＳＥＴは、本人認証に必要な秘密鍵によって正当な与信対象者であることの確認をするものであるため、秘密鍵の管理が重要な問題となる。ただ、暗号の信頼性は必ずしも万全ではなく、コンピュータの性能の向上や革新的な解読法の発見により、常にその信頼性が脅かされるリスクをはらむ。また、秘密鍵の管理も、一般の消費者が確実に管理できる簡便で適切な方式を用意しておくことが、他人による秘密鍵自体の不正使用の可能性を排除する上で不可欠であることは言うまでもない。

以上のＳＥＴに関わるリスクを考慮すると、ＳＳＬやその他暗号通信技術を用いた決済手段に比べ、消費者・販売店がトラブルに巻き込まれるリスクは比較的低いといえるものの、ＳＥＴ運営者のリスク管理は常に課題として残されるものと言える。

(5) 認証局

ＢｔｏＣのオンラインショッピングを行うについて、販売者である企業側が取引当事者の本人認証をするために電子証明書を発行する場合がある。企業は民間認証機関の発行する秘密鍵を持った認証局を設置するが、この認証局を運営するに当たって、例えば下記のようなリスクが存在する。

- 証明書の発行に際し、審査ミスにより証明書の誤発行（＝本来発行すべきでない者に発行すること）が発生、証明書受取者が悪用して、第三者が経済的損失を被った。当該被害者より、証明書の誤発行が原因であるとして、企業認証局が損害賠償請求を受けた。
- 発行システムの誤作動により証明書が発行できず、クライアント（本来証明書の発行を受ける者）の業務に支障が生じた。その結果被った営業損害に関して、損害賠償請求を受けた。

- **企業認証局が過失によりエンドユーザーの個人情報を漏洩してしまい、損害賠償請求を受けた。**
- **証明書の有効期限が切れているにも関わらず、証明書の廃棄を怠り、証明書ホルダー以外の者に悪用された。結果、経済的損害を被った第三者より損害賠償請求を受けた。**

こうした企業認証局の賠償リスクに対する保険は、認証局の設備の安全性や厳密な運用規程、監査規定とともに、企業認証局の信用を確保する上で大きな役割を果たす。消費者がよりＥＣを利用しやすい環境を整備する上で、保険がその大きな役割を果たすこととなる典型的な事例の１つであると評価できる。

(6) 消費者

ＥＣを利用する消費者のリスクとして、代表的なものにオンライン・クレジットカード決済を利用できるサイトやヴァーチャルモールにおける盗難・なりすましなどによる金銭的リスクがある。

クレジットカードの盗難または紛失により他人に不正使用されたことでカードホルダーが損害を被った場合に、その損害分を補償する保険としてクレジットカード盗難保険がある。ただしこれは他人にクレジットカードの現物を盗難、または紛失して不正使用された場合のことである。一方、ネット上では、クレジットカードの現物が盗難・紛失という事態に遭わなくとも、クレジットカード番号を盗み見されることによって、不正使用されるリスクを伴う。こうしたネット上でのリスクに対しては、現在のところクレジットカード盗難保険では補償されない。

4.1.4 各種保険内容の解説

ＥＣ当事者ごとにリスクと対応する保険の内容について見てきたが、それぞれの保険内容について、下記に解説する。ここで取り上げる保険は、前節でも述べたように、必ずしも汎用性のあるものに限らず、個別の事業者が個別の損害保険会社との間で付保している「オーダーメイド型」のものを含む。また、保険の名称は一般的に知られているものを使用しているが、実際には各社がそれぞれの呼称により種々の保険を組み合わせて独自の保険商品を販売しているので、必ずしも一様ではないことに留意する必要がある。

4.1.4.1　コンピュータ総合保険

(1) 概要

コンピュータ総合保険は、コンピュータ本体をはじめとする「情報機器」やフロッピーディスク・磁気テープなどの「情報メディア」に生じた火災、盗難、破損等を含む偶然な事故による損害を補償する保険である。また、情報機器や情報メディアに損害が生じた際の営業継続費用と喪失利益もあわせて補償することができ、コンピュータ・システム専用の総合保険となっている。

★コンピュータ総合保険契約の構成

＜保険契約者・被保険者＞

保険会社――――事業者（＝コンピュータ機器の所有者）

保険契約

(2) 主な補償内容

コンピュータ総合保険は、以下の４つの条項から構成されており、各条項を任意に組み合わせて加入することが可能である。

① 情報機器条項

コンピュータ本体およびその周辺機器（情報機器）を対象とし、偶然な事故により情報機器に生じた損害に対して、保険金を支払うものである。また、対象として情報機器と同一の構内に所在する通信用回線や、コンピュータ室専用の受配電設備、空調設備、什器・備品等を含めることもできる。

原則として時価額を限度として修理費が損害額として補償される。

② 情報メディア条項

フロッピーディスク・磁気テープ等の記録媒体およびその記録媒体内に記録された情報（情報メディア）を対象とし、偶然な事故により情報メディアに生じた損害に対して、保険金を支払うものである。ただし、情報のみに生じた損害に対しては、保険金支払の対象外となっている（特約により対象とすることができる）。

情報メディアを修復するための費用、または情報メディアを再製作・再取得するために必要な費用が損害額として補償される。

③ 営業継続費用条項

情報機器または情報メディアが損害を被った場合に、平常業務を継続するために特別に要した費用に対して、保険金を支払うものである。

具体的には、代替機器のレンタル費用、代替手段を講じるための臨時のアルバイト・パートの賃金等が補償される。

④ 利益条項

情報機器または情報メディアが損害を被った場合に、営業が休止または阻害され

たために生じた損失（喪失利益および収益減少防止費用）に対して、保険金を支払うものである。

(3) 主な特約条項

① 情報のみ損害担保特約条項

情報メディア条項で対象外となっている情報のみに生じた損害に対しても、第三者の不正アクセスまたは保管施設に不法侵入した第三者の行為による場合については、保険金を支払うことができる特約条項である。

② 新価保険特約条項

情報機器条項では損害額は時価額を限度として決定されるが、これを再調達価額限度に変更する特約である。

4.1.4.2 情報サービス業者・電気通信事業者賠償責任保険

(1) 概要

情報サービス業者および電気通信事業者のための専門職業人賠償責任保険であり、業務上の過失によって発生した法律上の損害賠償責任を負担することにより被る損害を補償する保険である。

★情報サービス業者・電気通信事業者賠償責任保険契約の構成

＜保険契約者・被保険者＞

保険会社――――情報サービス業者

保険契約　　法律上の損害賠償責任を負担

消費者または第三者

＜保険契約者・被保険者＞

保険会社――――電気通信事業者

保険契約　　法律上の損害賠償責任を負担

消費者または第三者

(2) 主な補償内容

情報サービス業者または電気通信事業者が、日本国内において行う情報サービス業務または電気通信業務の遂行にあたり、職業上相当な注意を用いなかったことに基づき提訴された損害賠償請求につき、法律上の賠償責任を負担したことにより被った損害を補償する。無形の経済的損害に対する賠償責任のみを対象とし、身体障害や財物損壊に起因する賠償責任は対象とならない。また、ソフトウェア開発・プログラム作成に起因する賠償責任についても対象外となっている（特約で対象とすることができ

る）。

(3) ソフトウェア開発･プログラム作成担保特約条項

対象外となっているソフトウェア開発またはプログラム作成業務の遂行に起因する賠償責任についても対象とする特約条項である。

4.1.4.3 ネットワーク中断保険

(1) 概要

偶然な事故によりネットワークの機能が停止したために生じる費用損害および利益損害を補償する保険である。保険の対象となるネットワークの範囲や補償内容の詳細については、顧客のニーズにあわせて設計することが可能な自由設計型の商品となっている。

★ネットワーク中断保険契約の構成

＜保険契約者･被保険者＞

保険会社――――**ネットワーク事業者（＝ＶＡＮやインターネットの接続利用事業者;**

保険契約　　**金融機関、電気・ガス業界など多岐の業界を対象に保険契約可能）**

(2) 主な補償内容

ネットワーク中断保険は、利益条項と営業継続費用条項の２つから構成されており、いずれかまたは両方の契約が可能である。

① 利益条項

不測かつ突発的な事由に起因して、ネットワークの機能が停止することによって営業が休止または阻害されたために生じた喪失利益および収益減少防止費用に対して、保険金を支払うものである。

② 営業継続費用条項

不測かつ突発的な事由に起因して、ネットワークの機能が停止した場合に生じた営業継続費用に対して、保険金を支払うものである。

4.1.4.4 クレジットカード盗難保険

(1) 概要

クレジットカード等の盗難・紛失による不正使用損害を補償する保険である。

★クレジットカード盗難保険契約の構成

＜保険契約者＞

保険会社－－－－－クレジットカード会社

保険契約　　**クレジットカード会員規約**

＜被保険者＞

クレジットカード会員

(2) 主な補償内容

クレジットカードが盗難され、または紛失し、そのために第三者に担保期間中[16]かつ保険期間中に不正使用されたことによる損害に対して、保険金を支払うものである。[17] したがって、カードの盗難・紛失を伴わないカード番号の盗用は対象とならない。

これは、リアルの世界での買い物の場合を対象に補償内容を定めているもので、ＥＣにおけるオンラインクレジットカード決済に代表されるような、ネット上にクレジットカード番号を入力することにより買い物が可能なケースを対象としていない。今後ネット上に入力するケースを含めた補償内容のクレジットカード盗難保険が普及していくかどうか注目に値するが、この問題については、まずはクレジットカード会社とカード加盟店、カード会員の間で、各々の事故の場合にだれがどう損害を負担するのかのルールを明確にすることが不可欠であるといえる。

(3) 主な特約条項

① キャッシュディスペンサー用カード担保特約条項

クレジットカードではなく、キャッシュディスペンサー用カードを対象として引き受けるときに付帯する特約である。

② 担保期間変更に関する特約条項

カード発行者がカード利用者から盗難届または紛失届を受理した日の 10 日前から 30 日後の 41 日間となっている担保期間を拡大または縮小する特約である。

4.1.4.5 金融機関包括補償保険

(1) 概要

金融機関の抱えるリスクを包括的に補償する金融機関専用の総合保険である。前述のＥＣ当事者ごとのリスクと対応する保険の項では、ＥＣ当時者として銀行などの金融機関については特段触れていないが、下記に見るように、「コンピュータ犯罪保険」

---

[16] カード発行者がカード利用者から盗難届または紛失届を受理した日の 10 日前から 30 日後の 41 日間(特約により変更可能)

[17] カード発行者への届出とともに、所轄警察署への届出も必須としている

という他種目にはない特殊な補償内容を持っているので、ここで紹介しておく。

★金融機関包括補償保険契約の構成

＜保険契約者・被保険者＞

保険会社――――金融機関（銀行・証券・保険など）

保険契約

(2) 主な補償内容

金融機関包括補償保険は、以下の３つの保険から構成されている。

① 財産保険

財産保険は、現金条項、偽造・変造条項および施設条項の３つの条項で構成されており、それぞれの補償内容は以下のとおりである。

A. 現金条項

施設内保管中または輸送中の貨幣､有価証券または貴金属等について発生した窃盗、強盗、火災その他偶然な事故による被保険者の財産上の直接損害に対して、保険金を支払うものである。

B. 偽造･変造条項

被保険者が所持しまたは取引に使用した貨幣､有価証券または貴金属等が偽造または変造されたものであったことが判明したことによる被保険者の財産上の直接損害に対して、保険金を支払うものである。

C. 施設条項

対象となる施設またはその施設内の設備、什器・備品等について、窃盗または強盗による盗取、き損または汚損により被保険者が被った損害に対して、保険金を支払うものである。

② 信用保険

被保険者の従業員がその業務を処理するに当たり、または自己の職務上の地位を利用して、単独にまたは第三者と共謀して、窃盗、強盗、詐欺、横領または背任行為を行ったことによる被保険者の財産上の直接損害に対して、保険金を支払うものである。

③ コンピュータ犯罪保険

被保険者のコンピュータ・システムへのデータの不正入力またはデータの改ざんもしくは破壊等の不正行為により、被保険者が被った財産上の直接損害に対して保険金を支払うものである。ただし、当該不正行為が、被保険者に損害を与えることおよび当該不正行為者が経済的利益を得ることを目的として行われた場合に限り、保険金支払の対象となる。

4.1.4.6　その他の保険

従来型の保険では火災保険が最も良く知られた保険であるが、コンピュータセンター等の建物や機械・設備・什器・備品類が火災・爆発、落雷、風災、雪災などにより被る財産損害が補償対象となる。コンピュータも補償対象とすることができる。建物や機械・設備などが火災・爆発、落雷などによって損害を被ったために、生産活動や販売活動が阻害されて生じる休業損害や事業継続のための臨時支出損失分を補償する利益保険や営業継続費用保険を付加することもできる。受配電装置やボイラー、空調設備などの機械・設備の不測かつ突発的な故障や破損などによる修理費を対象とする保険には機械保険がある。

なお、自らが所有、使用、管理する施設の欠陥、またはその施設を用いて行なう業務の欠陥により、他人の身体に障害を与えたり、財物を損壊したことにより生じる法律上の賠償責任が対象となる場合は施設所有者・管理者賠償責任保険で対応できる。

4.1.5　今後のＥＣリスクに関わる対策と保険の課題

前項において、ＥＣにおける当事者ごとのリスクと対応する保険について解説したが、各々の保険も今後のＥＣの発展にしたがってさらに加入形態や保険料率が、保険契約者や被保険者にとって加入しやすく、ニーズの高いものになっていくものと予想される。

リスク評価ＷＧにて、ＥＣを推進する企業および消費者団体に訪問し、ヒアリングした内容も踏まえ、今後のＥＣリスクに関わる対策・課題を下記４点に整理した。

①　従来の通販と比較したＥＣにおけるリスクの特徴について、各企業および日本通信販売協会や日本消費者協会などの団体から、具体的な実態を聞くことができた。実際のところ、ＥＣ特有の事故はマスコミが取り上げるほどまだ顕在化しているわけではなく、今後ＥＣがますます消費者に普及するにつれて、その対応が問題となってくる性格のものであるといえる。

②　しかし、現状においては消費者がなりすまし、改ざん等のトラブルに巻き込まれ金銭的なリスクが発生した場合であっても、損害の負担に関するルールが存在しない。ＢｔｏＣのＥＣ取引がさらに一層普及するためには、たとえばクレジットカード決済において、クレジットカード業界の中で損害解決の明確なルールを定め、消費者に対して明示し、守っていくことが望ましいと考える。

③　上記のような業界ルールが確立した上で、加盟店が被るリスクを保険ヘッジすることがカード加盟店である事業者側にとって有効な方策であるといえる。ただし、この点についても現状においては取引ルールが存在しない中で、補償すべきリスクの中身と、補償額、保険料水準、保険料の負担者等が明確に展望できるものでもなく、今後の検討課題として残ることとなろう。

④　平成 11 年以来急速に普及し始めたオンライン・トレーディングに関し、証券会社・トレーディング会員双方のリスクに着目した保険の普及が望まれる。例えば証券会社から出された要望として、システムのアウトソーシング先でシステムダウンが発生したときの証券会社の機会損失などのリスクに対して補償する保険というものがある。同時に会員側のリスクも、証券取引法などで経済的に保護されない部分が残る場合に、保険対応ということも考えうる。

4.2　損害とカード会社の対応

ここでは、クレジットカード決済を利用したＥＣにおいて想定される、①利用の覚えのない請求が届いた、②商品を注文したが届かずに代金だけ請求された、③商品を注文したが全く違う商品が届いた、といった 3 つのトラブルに対して、クレジットカード会社がどのような対応を行うか、またどのような調査を行い、最終的にカード会員への請求がどうなるか調査したものである。

なお前提として、クレジットカード会員は悪意を持たない会員（詐欺的行為を行わない善意の会員）とし、カード会社の対応は、関連する法律や規制に縛られたものではなく一般的にクレジットカード会社がどのような対応を行うかをまとめている。

実際のトラブル発生については、会員からの聴取、当該加盟店への確認、配送業者への確認等を行い最終的に各カード会社が総合的な判断を行うため、本対応が絶対的でないことをご了承願いたい。

4.2.1　損害とカード会社の対応

損害の内容	カード会員への確認と対応	カード会社・加盟店の調査	調査結果・加盟店の対応	カード会員への請求
①利用の覚えの無い請求が届いた	**●利用内容の確認** 利用明細書（請求書）に記載されている身に覚えのない利用を確認する。 ・利用日 ・利用店名 ・利用金額 上記聴取に基づき、カード会社は、当該売上についてカード加盟店を管理するカード会社（カード会員を管理する会社と同一の場合もありうる）に確認を行う。	**●カード加盟店管理会社での調査内容** 加盟店への確認 ・利用日 ・利用内容（商品購入、サービス利用等） ・購入者（サービス利用者）の特定 （購入時に住所・氏名・電話番号・メールアドレス等の個人情報を登録していないか） ・本人認証方法 **●調査結果** ①物流が伴わない商品の場合 （例）デジタルコンテンツのダウンロード、アダルトサイトの利用	**●購入者（サービス利用者）の特定** 不正に個人情報を入手することも考えられ、個人情報がカード会員の情報と一致したとしても、それをもってカード会員の利用と判断することは困難である。 **●送信元のＩＰアドレスからの調査** 理論的には可能であるかもしれないが、プロバイダー等が調査に協力することは難しい。さらにダイヤルQ2 を利用したプロバイダーの場合は、さらに利用者を特定することは困難である。ＩＰアドレスをもって利用者を特定することも困難である。	利用者のＩＰアドレスやメールアドレスが特定できたとしても、それをもってカード会員が利用したことを証明することは困難といえる。 ⇒カード会員への請求は保留とする。事実が判明した場合は、事実に基づき請求となる。

損害の内容	カード会員への確認と対応	カード会社・加盟店の調査	調査結果・加盟店の対応	カード会員への請求
		調査結果 ②物流が伴う商品の場合 （例）食料品、電機器具の購入 ●配達先の確認 ・配送先住所の特定 ・利用した配送会社の特定 ●配送会社への確認 ・実際に配送した住所の確認 一旦配送した先から転送をしていないか	●配送先がカード会員の自宅の場合 →親族の利用の疑いがあり ●全く関係のない住所の場合 →第三者による商品詐取の疑いがあり	親族による利用が判明し、商品も受け取っていた場合（カード会員がたまたま不知の場合） ⇒カード会員への請求となる。 本人と全く関係のない住所の場合 ⇒受取人の署名、印鑑からの推測、実際の配送先の居住者への聴取を行い判断する。事実確認が判明するまではカード会員への請求は保留とする。事実が判明した場合は、事実に基づき請求となる。

損害の内容	カード会員への確認と対応	カード会社・加盟店の調査	調査結果・加盟店の対応	カード会員への請求
②商品を注文したが届かずに、代金だけ請求された	●利用内容の確認 カード会員の購入の控えに基づき、下記の事項を確認する。 ・利用日時 ・利用店名 ・注文した商品内容 ・金額（送料） ・加盟店から受け取ったメールや文書等 上記聴取に基づき、カード会社は、当該売上についてカード加盟店を管理するカード会社（カード会員を管理する会社と同一の場合もありうる）に確認を行う	●カード加盟店管理会社での調査内容 **加盟店への確認** ・加盟店の受注状況の確認 いつ注文がなされ、いつ受注したか、いつカード会社に売上代金の請求を行ったか ・加盟店の発送状況の確認 いつ商品を発送したか どこの配送会社を利用したか 商品の受け取り状況はどうなっているか ・加盟店からカード会員への連絡状況の確認 商品発送について、遅延の連絡を行っているか それに対して消費者から了解を取っているか	●商品が未発送の場合 至急商品の発送を依頼 ●商品は発送している場合 →カード会員の住所に発送している →全く第三者の住所に発送している ⇒上記①のケースに同様	商品未発送の場合 ⇒それを理由とし支払い拒否の申し出があれば、一旦請求をストップし、商品が発送・受領された時点であらためてカード会員へ請求となる。 商品をカード会員の住所に発送している場合 ⇒自宅等で親族による受取がなされているか確認を行い、受取されていればカード会員へ請求となる。 商品をカード会員の住所に発送しいるが、親族を含めて誰も受取していない場合 ⇒配送会社への確認のうえ、未配達であれば再度配達を行い、あらためてカード会員に請求となる。

損害の内容	カード会員への確認と対応	カード会社・加盟店の調査	調査結果・加盟店の対応	カード会員への請求
③商品を注文したが全く違う商品が届いた	●利用内容の確認 カード会員の購入の控えに基づき、下記の事項を確認する。 ・利用日時 ・利用店名 ・注文した商品内容 ・届いた商品内容 ・金額（送料） ・加盟店から受け取ったメールや文書等	●カード加盟店管理会社での調査内容加盟店への確認 ・加盟店の受注状況の確認 いつ注文がなされたか 注文した商品の内容 →カード会員の申出内容との確認 ・商品発送状況確認 販売店（加盟店）が間違った商品を発送していないか ●上記調査を踏まえて再度カード会員に確認 注文内容の確認 ・そもそもカード会員が間違えて注文をしていないか ・カード会員が、注文した商品のイメージを勘違いしていないのか	●本人の注文間違い →商品交換の申出に応ずる →商品交換の申出に応じない（食料品・特注品等） カード会員のイメージ違い →商品交換に応ずるかは、加盟店次第。ただしホームページ上で、あきらかにカード会員を混乱させるような表記・表現があった場合は、販売店（加盟店）側の問題になる可能性が高い	本人の注文間違いではあるが、商品交換に応ず ⇒カード会員への請求はストップする。 本人の注文間違いなので、商品交換に応じない ⇒加盟店とカード会員との話し合いにより解決する。（ただし、特注品や食料品等、特別の場合を除き、商品交換または返品に応ずることが望ましい。） カード会員のイメージ違い ⇒加盟店とカード会員との話し合いにより解決する。（ただし、特注品や食料品等、特別の場合を除き、商品交換または返品に応ずることが望ましい。）

損害の内容	カード会員への確認と対応	カード会社・加盟店の調査	調査結果・加盟店の対応	カード会員への請求
			●販売店（加盟店）側の発送間違い **→加盟店にて商品交換で対応** **会員規約により注文した商品と全く違う商品が届いた場合は会員に売買契約の解除する権利を認めているケースが多い**	販売店（加盟店）側の発送間違い **⇒正しい商品を配送し受領した時点で、あらためてカード会員に請求となる。**

4.2.2　解説

(1) 利用の覚えの無い請求が届いた

① 前提

利用の覚えの無い請求が届く原因として以下の 3 つのケースが考えられる。

1. カード会員が単純に利用したことを失念した

2. 請求書（利用明細書）に記載された利用店名、利用日が実際の利用内容と異なっていた

3. カード会員が全く利用せず、第三者が利用していた

1 のケースにおいては、会員の失念が原因であり、カード会社に利用の内容を問い合わせ、利用店名、利用内容を説明することにより通常解決する。

2 のケースにおいては、請求書（利用明細書）に記載された店名が、利用したお店の法人名で記載されたり、注文日ではなく加盟店が売上を処理した日付が記載されるケースが多く、これらのことを調査の上、会員に説明することにより通常解決する。

なお海外のアダルトサイトを利用した場合に、実際に利用したサイト名（店名、会社名）とは異なる名称で請求されるケースが多い。これはビリングカンパニーと呼ばれる決済代行業者がクレジットカード会社と契約をしているため、ビリングカンパニーの名称で請求が届くものである。これらも加盟店を管理するカード会社に確認をすることにより解決されるケースが多い。（図 4-1、4-2 参照）

問題は 3 のケースである。本人が利用していない場合、第三者によるなりすましによる利用が考えられる。今回のケースでは上記 3 のケースを前提として解説する。

② カード会社の対応

A. 会員からの聴取と請求の保留

「利用覚えが無い」というカード会員からの連絡が届いた場合、カード発行会社（以下イシュアー）では、「利用明細書（請求書）」に記載された、利用日時、利用店名（加盟店名）、金額を当該会員に確認する。

この時点で同居家族等による利用がないか確認を依頼するとともに､クレジットカードの保管状況（盗難、紛失がなかったか）を確認する。

当該会員からの連絡を自社システムと照合し､特に当該会員の連絡に不審な点がなければ一旦当該請求を保留とし、調査を行う旨会員に伝える。

B. カード加盟店契約会社への調査依頼

イシュアーは、当該加盟店と契約しているカード会社（以下アクワイアラー）へ、会員の報告に基づき事実調査を依頼する。

C. アクワイアラーからの調査結果の回答

アクワイアラーからの調査結果に基づき、カード会員に説明を行う。

ここでは、具体的な利用日時や購入した商品の内容、サービスの内容を説明するが、あわせて家族や親族等の利用がないか再度カード会員に確認するよう依頼する。

一般的には加盟店契約において、加盟店が販売した商品等に関する苦情・返品および売買契約解除等の請求に関する事項について加盟店の責任にて対応することを求めており、物流が伴う場合には配達先の調査や配送会社への確認、デジタルコンテンツの場合は、プロバイダーへの確認等を行う。

D. イシュアーによる請求可否の検討

アクワイアラーからの調査報告ならびにカード会員からの事情聴取に基づき、最終的にカード会員に対して請求するかを決定する。カード会員に重大な過失があると認められる場合は、カード会員へ請求することがある。

カード会員への請求が不可能と判断した場合、各クレジットカードブランド会社の規約に基づき加盟店管理会社に対してチャージバック[18]の返却手続きを行うことがある。

E. カード会社間の調整・仲裁手続

イシュアー、アクワイアラーの主張が異なる場合の仲裁手続については各ブランドにより規則が制定・実行されている。

③ 調査結果に対する対応

A. 調査の結果、会員に非があることが判明した場合

当該会員本人の勘違い、家族会員による利用等、当該会員に明らかに非があることがアクワイアラーによる調査により、あるいはイシュアー・当該会員との通信により判明した場合は、当該会員への請求取消・停止手続を解除、再請求がイシュアーから行われ、同時にアクワイアラーへのチャージバック申請は取消される。

B. 第三者による利用（悪用）が判明した場合

当該会員と共謀していることが判明した場合、当該会員に明らかに過失がある場合や、ブランドが認定している本人認証技術の利用が当該取引において使われている場合（例：ＳＥＴ）等を除いて、本人確認義務は加盟店に存する場合が一般的であるため、それを理由にアクワイアラーがチャージバックを拒否することはできない。

---

[18] イシュアー（カード発行会社）が加盟店（またはアクワイアラー）に対して、加盟店側の手続き上の不備を理由として、カード売上代金の支払いを拒否したり、既に支払っている場合はその金額を戻してもらうこと。

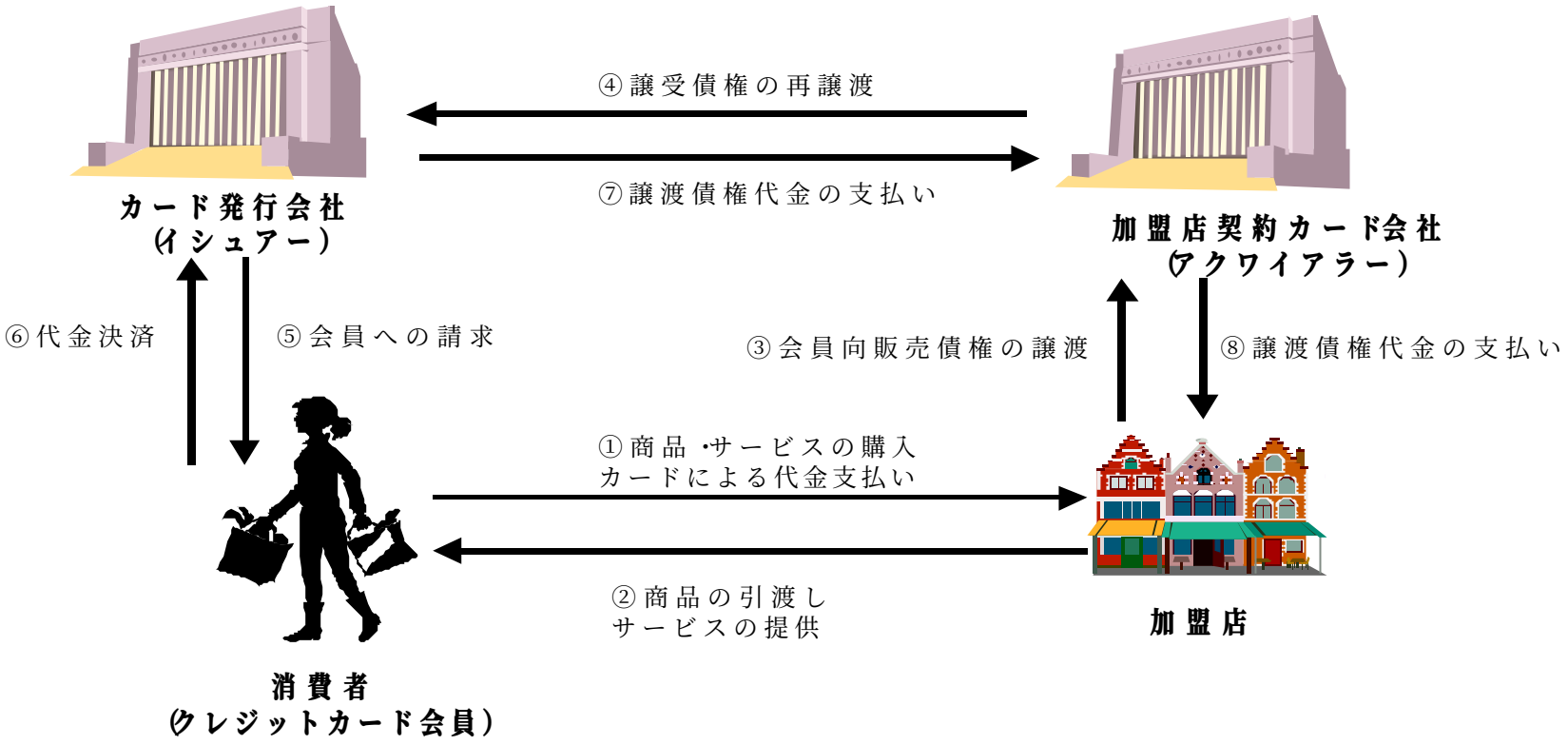


図 4-1 通常のクレジットカード決済の仕組み

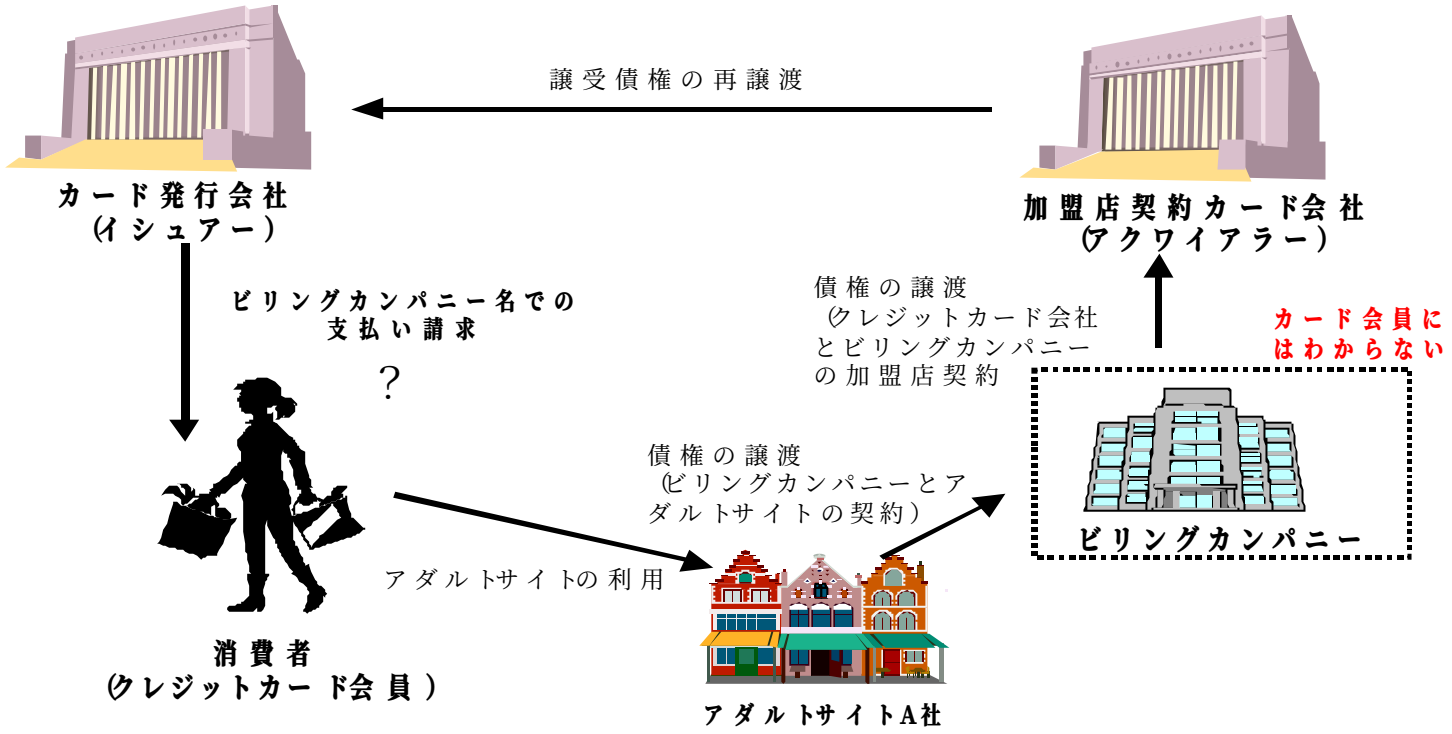


図 4-2 ビリングカンパニー経由のクレジットカード決済の仕組み

(2) 商品を注文したが届かずに代金だけ請求された

① カード会社の対応

本件では、アクワイアラーは、加盟店側に瑕疵が認められる債権をその事由に基づきチャージバックすることができる。

しかし、クレジットカードの利用により生じた債務は、本来的には物品の購入あるいはサービスの提供等を行って利益を享受したもの（＝会員）が負担すべきものであり、決して債権の減免を目的とするものではない。

具体的には、何らかの瑕疵ある売上（今回の場合は、会員の手元に商品が到着していないとの申出）については、イシュアーからアクワイアラーにその旨の通知がある。

アクワイアラーにおいては、当該売上債権の譲渡を行った加盟店に対し、調査を行い当該債権を買取るか否かの判断を行う。

調査内容の主なものとしては以下の通りである。

- **注文日**
- **注文商品**
- **金額の確認**
- **商品の発送日**

  通信販売の場合、カード会社より、加盟店に対して商品の発送日をもってカードの売上日とする様指導しており、発送なくしては、代金請求はありえない
- 発送状況の確認

  配送会社、送り状の署名･捺印等

② 調査結果に対する対応

上記の内、単なる商品未発送であることが確認された場合は、加盟店に至急の商品発送を依頼し、当該請求の延長を依頼する。（発送日をもって再度売上依頼とする）

商品が発送されているが、会員の手元に届いていない場合は、同居親族等の受取が明らかな場合は、そのまま代金請求が行われる。全くの第三者に送付した場合それが加盟店側の過失によることが明白な場合には正しい送付先への発送日をもって再度会員宛請求とする。（当該請求の延長）

会員が悪意の第三者への送付を指示したもしくは会員が本当は商品を受領したにもかかわらず未受領を主張する場合、あるいは加盟店が悪意の第三者に故意に送付したもしくは本当は商品を未発送にもかかわらず、商品を発送したと主張する場合、通信販売加盟店契約に基づき（会員との紛議）、当該債権の買戻を加盟店に求め、以降は会員・加盟店間での交渉事項となる。（カード会社は介在しない）

その場合、当該債権に関する会員請求は当然ながら取消されるとともに加盟店宛

譲渡代金の支払も行われない。

**　しかし加盟店とカード会員の間での交渉がまとまらない場合も多く、現実はイシュアーとアクワイアラーとの間において、チャージバックの手続きがとられることが多い。**

(3) 商品を注文したが全く違う商品が届いた

① カード会社の対応

返品交換は、そもそも商品に瑕疵がなく、契約の不履行、違約がない状況において返品交換が適応されるものであり、注文した商品と全く違う商品が届いた場合は、契約の不履行にあたりそもそも加盟店は返品交換に応じることは当然といえる。実際の事例としては、注文した商品と全く違う商品が届いたことを理由としてカード会社に会員から問合せが入るケースはまれである。

そもそも購入商品に関する問題には、カード会社が介在する余地はあまりなく、殆どが加盟店と会員との間で解決されているのが実態である。

しかしながら会員規約においては、消費者保護の立場から、そもそも注文した商品と全く違う商品が届いた場合は会員に売買契約の解除する権利を認めているケースが多い。（カード会社により解釈が相違する場合もある）

会員規約抜粋

会員が加盟店に対して見本・カタログ等により申込をした場合において、引渡された商品が見本・カタログ等と相違している場合は、会員は加盟店に商品の交換を申出るかまたは当該売買契約の解除をすることができます。

よってカード会員と加盟店の間で解決がつかない場合、カード会社（加盟店契約会社）は、加盟店側に瑕疵が認められる債権をその事由に基づき、返却することができる。

しかし、クレジットカードの利用により生じた債務は、本来的には物品の購入あるいはサービスの提供等を行って利益を享受したもの（＝会員）が負担すべきものであり、決して債権の減免を目的とするものではない。

具体的には、何らかの瑕疵ある売上については、会員所属会社から加盟店契約会社にその旨の通知があり加盟店契約会社において当該売上債権の譲渡を行った加盟店に対し、調査を行い当該債権を買取るか否かの判断を行う。

② 調査結果に対する対応

本件の場合、一次的に加盟店と会員との間で解決に至らない段階で、加盟店側の単純な商品の発送間違いや、会員側の商品発注間違い、というレベルの問題ではなく、商品そのものについての問題になっている場合が多い。

こうした場合カード会社の介在できる余地がないことから、通信販売加盟店契約に基づき（会員との紛議）、当該債権の買戻を加盟店に求め、以降は会員・加盟店間での交渉事項となるが、交渉が決裂する場合現実的には上記①および②のケースと同様にカード会社が仲介することになる。

4.3　消費者の金銭的損害に対する今後の業界ルールや自主規制ルールのあるべき姿

消費者の金銭的損害に対する業界の対応については、これまで重ねて述べたが、一定のルールを定めるべきである。この場合、特に発展段階にあるＥＣのような変化の激しい分野では自主規制が有効であると考えられる。しかし、法律に比べ罰則が無いため、その有効性を問う声もあるが、その内容を明確に消費者に対して開示すること、更に第三者機関が常にその実行状況をモニターすることで十分効果があると思われる。

その典型が、多様な銀行サービスに対して銀行が守るべき最低限の基準を定めた英国銀行協会のバンキングコードと言われている。この規約は関係する法律の枠組の中で、顧客に対するサービスの最低基準を明言することを目的として業界自体によって作成されたものである。これは非常に顧客対応力のあるプロセスであることが証明され、事実、この規約は新商品開発や顧客の要求に応じて既に数回修正されている。業界自主規制を行う上での好事例としてその内容と運営方法を紹介する。

4.3.1　バンキングコードの歴史

英国ではバンキングコード作成以前にも Consumer Credit Act 1974 により、クレジットカードの不正利用時に消費者の損害負担額を制限する規定があった。その後、銀行カードが発効されＡＴＭなどで消費者が利用する状況になったとき、カードが盗まれ不正利用された場合にどのような対応とするかについてはそのルールが不明確であった。そこで、銀行自らがコードを作って消費者を守ろうとしたものである。

一方、1985 年から 1989 年にかけて、消費者の銀行サービスに対する批判が高まった時、英国政府は委員会を設立して銀行サービスの調査をさせた。結局、委員会は銀行に Code of Conduct（行動規範）を発行するように命じたことも背景にある。従来イングランド法は銀行側に有利な内容であり、裁判所もどちらかといえば銀行側に好意的な姿勢であったということも指摘されている。また、銀行は裁判を行う資力があるが、一般消費者では難しい。このコードは、この不均衡に適当なバランスをとったと評価されている。

1992 年 3 月に完成し、初版が発行された。その 2 年後の 1994 年内容が改訂され、第 2 版が発行された。1997 年には再度内容が改訂され第 3 版を発行、翌 1998 年 9 月にも第 3 版の改訂版が発行されている。インターネットバンキングやＷｅｂサイトによる情報提供のような技術的発展、新商品の開発や消費者の要望などの様々な変化に応じて度々内容を修正しており、自主規制の対応力の有利性が理解できる。つまり、電子商取引のような分野ではこうした自主規制というものが大変効果的なものになり得る。また、後で述べる Independent Review Body と呼ばれる独立団体による運営も重要な役割を演じている。バンキングコードは今後も内容を審議し、2000 年 7 月にも改訂が計画されているとのことである。

4.3.2　バンキングコードの内容

このバンキングコードは任意のものであり、各銀行は英国銀行協会（ＢＢＡ）に加入してバンキングコードに従わなければならないという義務が有るわけではない(現状では大手国際銀行は全行加入）。対象となるのは個人の消費者だけであり、法人には適用されない。

コードは次の基礎的な１１の約束を述べることから始まる。

① **あなたとのすべての取引において公正かつ正当に（fairly and reasonably）行動します。**

② **すべてのサービスおよび商品について、それぞれ独自の取引条件があったとしても、このコードに従うことを確約します。**

③ **われわれのサービスおよび商品に関する情報を平易な言葉で提供し、あなたが理解できない点があればどのようなことでも手助けをします。**

④ **あなたのニーズに適合したサービスまたは商品を選択する手助けをします。**

⑤ **あなたが次の商品の金融的な意味内容について理解する手助けをします。**

- **モーゲッジ**
- **その他の借入**
- **貯蓄および投資商品**
- **カード商品**

⑥ **あなたの口座がどのように機能するかを理解する手助けをします。**

⑦ **安全で（safe、secure）、信頼できる銀行システム、決済システムを提供します。**

⑧ **われわれの従業員が行う手続がこれらの約束を反映したものであることを確約します。**

⑨ **誤りの訂正および苦情の処理をスピーディに行います。**

⑩ **金融面での困難な状況およびモーゲッジの遅延のケースを思いやりをもって前向きに(sympathetically and positively)配慮します。**

⑪ **すべてのサービスおよび商品が関係する法律および規則を遵守していることを確約します。**

この基本方針のもとに、デビットカードや電子マネーも含む不正利用に対して、消費者に一定の責任制限の権利を与え、消費者保護を図っている（詳細は「3.2.2 英国 50 ポンドルール」参照）。

4.3.3　独立団体による運営

このバンキングコードを最も特徴付けていることは第三者機関の存在である。自主規制ルールを真に有効なものとするためにはこの独立した第三者機関によるモニターという要素抜きには考えられない。一方、前述のようにこのバンキングコードはこれまで新商品開発や顧客の要求に応じて既に数回修正されており、非常に顧客対応力のあるプロセスであることが証明されている。これにも、独立団体による運営という重要な要因がある。このコード

の承認や管理、銀行がコード通りの行動をしているかをモニターする団体は英国銀行協会とは別の団体である。この団体が、Independent Review Body である。

Independent Review Body は、議長、一般消費者 4 名、各業界団体からの代表４名など９人のメンバーからなる。コード自体の内容は、英国銀行協会が作成している。しかし、個人メンバーが一人でもコードに異議を唱えたら、コードは認められない。また、議長の選任についての承認権も有る。

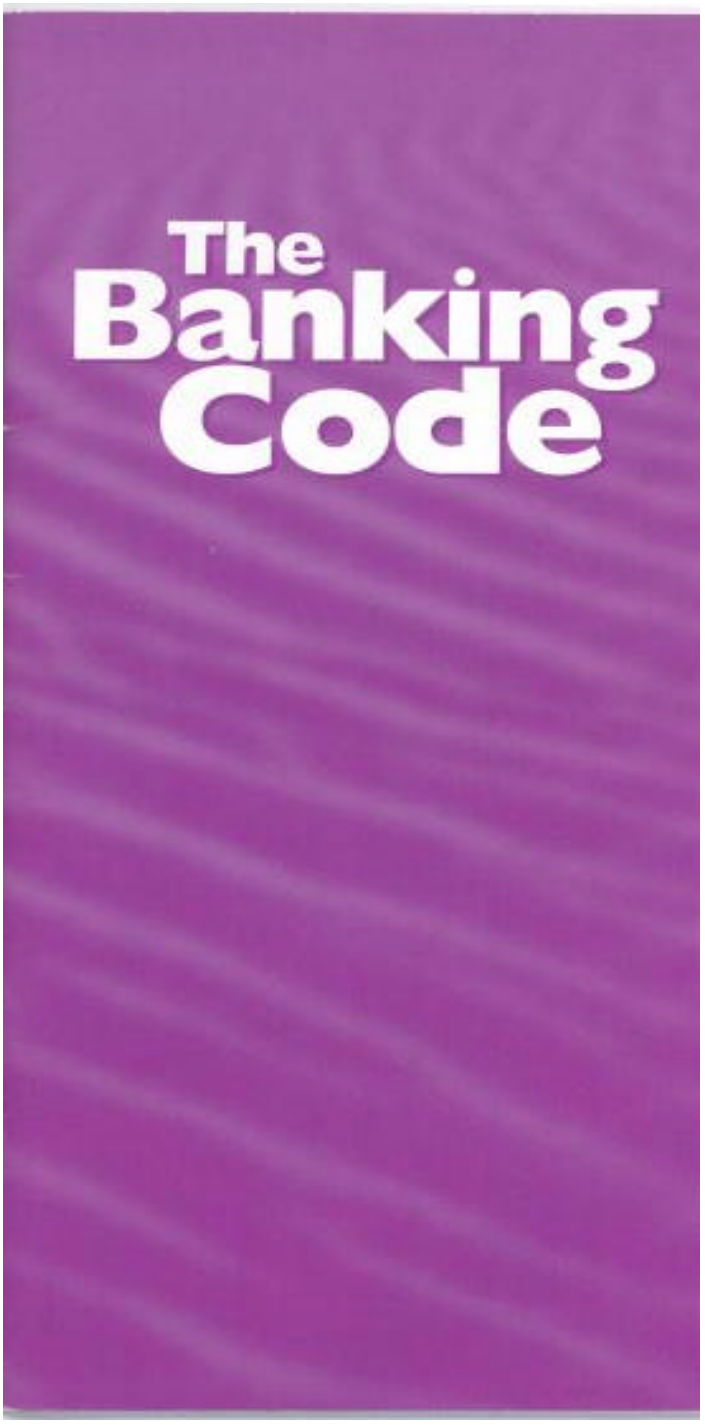
Independent Review Body は最近、銀行の規約遵守に対するモニターの方法も変えた。従来は単にコードを守っているかどうかのアンケート調査であったが、現在は規約遵守状況の詳細な報告書を提出させることになっている。同時に、プライスウォータークーパー監査法人による監査も含まれる。監査法人によるテストモデルを作ったことにより、各銀行の良いサービス、悪いサービスが明確になったといわれる。

このコードに関する一般的運営にへの苦情はこの独立団体機関に行うことができる。その場合、スタッフはどのような疑問にも答えることを約束しており、どのようにして苦情を申し立てるのか、およびその結果が思わしくないときにどうすればよいのかを知らせている。一方、苦情申し立て後の公正でスピーディな内部手続を行うため、苦情に対する最初の承認(acknowledgement)に要する時間の設定や、更に詳細な対応を行うためにどのくらいの時間を要するかなど、その後の手続きの詳細な説明を行うことになっている。

更に個別問題が内部苦情処理手続で解決できなかった場合に、独立したオンブズマンまたは調停制度を利用することができる。各銀行は、どのオンブズマンまたは調停制度に所属しているか、どのオンブズマンまたは調停制度を利用できるかの詳細な情報を提供している。

これらの充実した第三者機関の存在とその役割を確実に果たしていることが、このコードを変化に対して迅速に対応でき、更に十分効果のあるものにしていることが理解できる。

図 4-3 実物大のバンキングコード冊子



5 資料

5.1 消費者インターネットショッピングマニュアル

クレジットカードを利用したインターネットショッピングは、現実の世界でクレジットカードを利用するのと同様に、クレジットカードの取り扱いに注意すれば大変便利なものである。

ここでは一般的なクレジットカードを利用してインターネットショッピングを行うに際して、消費者が注意する点や参考となる事項をまとめた。

これからインターネットショッピングをはじめようとする人も、また既にインターネットショッピングを経験している人も、本マニュアルを参考にして安全で楽しいショッピングを行って欲しい。

インターネットショッピングマニュアル

―安全で楽しいインターネットショッピングのために―

プロセス	アクション	解説
Ⅰ．インターネットにつなぐ	①ISP[19]と契約が必要です。	● 契約条件を確認しましょう アクセスポイント、電子メール、料金、ローミングサービス、ホームページ作成サービス、ヘルプデスクの電話番号・連絡先等を確認してから自分に最適のＩＳＰを選択しましょう。
		● 重要情報は大切に保管しましょう ID、パスワード、クレジットカード番号等の重要情報は忘れないように、また他人に見られないように大切に保管しておきましょう。パスワードは定期的に変更することをお薦めします。
		● 割引サービスを活用しよう ISP によってはいろいろな割引サービスを提供しています。自分の利用目的・パターン等に見合ったサービスを選びましょう。
	②電話会社のサービスも利用できます。	● 電話料金を確認しましょう ＩＳＰへの支払いとは別に、アクセスポイントまでの通話料金がかかります。[20]
		● インターネット利用者向けサービスを利用しましょう インターネット利用者向けに電話会社はさまざまな割引等のサービスを提供しています。自分の利用目的に見合ったサービスに加入することをお薦めします。

[19] ISP インターネット・サービス・プロバイダの略で単にプロバイダと言うこともある。コンピュータをインターネットに接続するサービスを提供しており、インターネット接続の料金体系は、（1）入会金、（2）月額基本料金、（3）利用時間に見合った従量制、（4）一定時間内あるいは時間制限無しの固定料金等の組み合わせになっている場合がほとんどである。自分の利用目的・パターンなに見合った料金プランを選ぶことが大切である。

[20] 電話会社自体がＩＳＰを経営している場合、通話料金とＩＳＰ料金をパッケージにして提供している場合もある。

プロセス	アクション	解説
Ⅱ．安全なソフトウェアを使いましょう	①ブラウザー・ソフトの更新－ブラウザー提供者のサイトから更新版・バグフィックス等をこまめにダウンロードしましょう。	● インターネットは、技術革新がきわめて速い分野です。また、世界中で毎日何千万人もの人が利用しているので、「セキュリティ・ホール」や「バグ」が数多く発見され、その対策のためのソフトウェアがブラウザソフトの提供者等から公開されています。サイトからのダウンロードや、雑誌の付録ＣＤ－ＲＯＭ等の形で容易に入手できますので、こまめにチェックして安全にブラウジングを楽しみましょう。
	②コンピュータ・ウィルス対策はこまめに－コンピュータウイルスワクチンをこまめにアップデートしましょう。	● お手持ちのコンピュータにはほとんどの場合、ウィルス対策ソフトウェアがインストールされていますが、ほとんど毎週のように新しいコンピュータ・ウイルスが発見されています。こうしたウイルスワクチンの提供者は、アップデートを提供していますので、これもこまめにチェックして、ダウンロード等でウイルス対策は万全にしておきましょう。

プロセス	アクション	解説
Ⅲ. いろいろなショップを見てみましょう。	**①信頼のおけるショップを見分けましょう**	● インターネットショッピングは、相手のショップがどのようなお店かを判断する必要があります。 第三者機関が信頼の置けるショップや事業者に対してマークを付与する制度が普及し始めていますので参考にすると良いでしょう。 （例） オンラインマーク（日本通信販売協会） http://www.jadma.org/org/index.html プライバシーマーク（日本情報処理開発協会） http://www.jipdec.or.jp/index.htm 個人情報保護マーク（日本データ通信協会） http://www.dekyo.or.jp/ ● 企業が独自にショップ、事業者の調査を行い紹介しているホームページも多数あります。これらを参考にすると良いでしょう。 （例） 日経BESTShop（日経BP社） http://bestshop.nikkeibp.co.jp ● 商品の販売（購入）自体が法律により規制されているものがありますので、そのような商品を販売するショップは要注意です。 （例）医薬品・宝くじ・銃火薬類等

プロセス	アクション	解説
	②見るだけで個人情報の登録を要求されるショップもあります	● インターネットではブラウズ（閲覧）するだけで、サイトを運営しているサーバーにあなたの一定の情報が登録されます。[21]
		● **サイトによっては、見るだけで名前や住所等の個人情報の登録を要求される場合があります。このようなサイトの場合、本当に自分の個人情報等がサイト運営者等に知られていいかどうか自分で判断する必要があります。インターネットでは、相手が誰であるかという確認ができない場合がほとんどなので、慎重な判断をする必要があるでしょう。**
		● とりわけ、クレジットカード番号、有効期限等の登録は、実際に支払を行う場合以外は入力しないことをお薦めします。 （例）海外のアダルトサイトが年齢確認のためクレジットカード番号と有効期限の入力を求める場合があります。
		● それでも登録したい場合は、最低限そのサイトの名称、URL、電話番号、住所、e-mail アドレス、責任者の名前等の情報を印刷あるいは保存しておくことをお薦めします。しかし、そうした場合でも、あなたの個人情報が悪用されないという保証は無いことを銘記すべきです。

[21] 一般的に利用者の IP アドレス、直前にブラウズしていたサイトのアドレス、その後に移動したアドレス、「Cokkie：クッキー」等が登録される。

プロセス	アクション	解説
Ⅳ. 欲しいものが見つかったら	**①売買条件の確認**	● 普通のショッピングと同じように、次のような条件を確認しましょう。 ➢ 品名 ➢ 数量 ➢ 色・サイズ等（必要な場合） ➢ 価格 ➢ 配送料 ➢ 税金 ➢ 配送時期 ➢ 商品に瑕疵がある場合、遅配の場合の取扱 ➢ 返品規定 ➢ 支払方法
		● 上記のような条件が明文化されていることを確認しましょう。（インターネットは「自己責任」社会です）
		● その画面をコピーするか印刷しておくとよいでしょう。
	②買物の相手先（ショップ）の確認	● プライバシー・ポリシー等あなたの個人情報取扱についてのショップの規定を確認しましょう。
		● 名称・住所・電話・FAX・電子メール・代表者名等が明記されていることを確認しましょう。
		● 返品に関するショップのポリシーを確認しましょう。
		● 上記情報をコピーあるいは印刷しておきましょう。
	③実際の注文と支払	● 一般的な支払ソフト[22]を使用する場合: クレジットカード会社の運営するショッピング・モール等では支払のためのソフトウェアを配布している場合があります。こうしたソフトウェアは汎用的な目的のために開発されたものがほとんどです。またそうしたソフトウェアが配布されている場合もあります。そうしたソフトウェアでは一般的に SSL[23]あるいは SET[24]対応が行われており、現在のところ互換性には制限がありますが、安全にカード番号等の重要な情報をインターネット上でやり取りすることが可能です。SET 対応が行われているソフトウェアを使用すれば、取引参加者の「認証」が可能なために、加盟店に「なりすます」行為が防止され、さらに安全性は高まります。

[22] 支払ソフトにはさまざまな名称があり、またショップによっては独自のソフトウェアを利用することが要求される場合もある。

[23] SSL Secure Socket Layer の略。暗号化技術を使って、インターネット上での通信を第三者の盗聴や改ざんから防ぐためのプロトコル。（通信手順）

[24] SET Secure Electronic Transaction の略。インターネット経由でのカード取引を安全に行うために開発されたプロトコル。暗号化技術に加えて、デジタル署名を使った認証によって、カード会員、加盟店、カード会社の三者がお互いの正当性を確認できるようにしているため、「なりすまし」や「否認」等を防ぐことが可能になっている。

プロセス	アクション	解説
		● ショップ独自の支払ソフト（ショッピング・バスケット）を利用する場合: カード番号等の情報入力が「セキュア」モードになっていることを確認してください。
		● クレジットカード番号を入力するサイトの場合: ➢ カード番号等の情報入力が「セキュア」モード[25]になっていることを確認してください。 ➢ あなたがお使いになるクレジットカードブランドをショップが取り扱っていることを確認してください。 ➢ e-mail でカード番号をやり取りすることを要求するサイトではショッピングをしないことをお薦めします。
		● クリックする前に、最後にもう一度確認しましょう。
Ⅴ．商品・サービスが到着したら（到着しなかったら）	①商品が到着したら	● 自分が注文したものと合っているかどうか確認しましょう。自分が注文したものと違うものが届いた場合、また同じものでも損壊している場合等は、ショップに連絡しましょう。その場合、保存・印刷しておいた画面や連絡先が役に立ちます。
		● ショップと連絡がとれたら、事情を説明し、必要なら書面を提出して、返品・返金等の手続きを取りましょう。
		● ショップに連絡がとれない場合は、 ➢ カード支払の場合、クレジットカード会社のヘルプデスクに連絡するのも良いでしょう ➢ 消費者相談窓口に連絡しましょう 日本通信販売協会「通販 110 番」 http://www.jadma.org/ 日本消費者協会 http://www1.sphere.ne.jp/jca-home/ 国民生活センター http://www.kokusen.go.jp/
	②商品が到着しなかったら	● ①の場合と同様、ショップに連絡をとりましょう。
		● ショップに連絡がとれない場合は ➢ カード支払の場合、クレジットカード会社のヘルプデスクに連絡するのも良いでしょう ➢ 消費者相談窓口に連絡しましょう

[25] 「セキュア」モードとは、利用者が送信する情報が暗号化されて販売店に送られるモード。「セキュア」モードの場合、利用者のブラウザにはセキュアモードになったことを示すアイコンが現れる。

プロセス	アクション	解説
VI．支払請求が到着したら	①クレジットカード会社からの利用明細書が届いたらすぐにチェックしましょう。	● チェックして問題が無ければOKです。
	②覚えの無い請求、金額が異なる請求がある場合は、すぐにクレジットカード会社の連絡先に連絡しましょう。	● 利用明細書に意義がある場合は直ちにクレジットカード会社に連絡しましょう。連絡が遅い場合（利用明細書を受け取ってから概ね 10 日以上）は、利用明細書の内容を承認したものとみなされ、支払い義務が生ずる場合があります。 ● その際、金額が異なる場合は自分が実際に行った取引の明細を準備してから連絡するのがよいでしょう。 ● 実際の利用店舗とは異なる店名で請求される場合もあります ● 実際の利用日と異なる日付で請求される場合もあります

おわりに

我が国において、どのようなルール、制度を作るべきかは現実のビジネススタイルや実務に照らして十分な検討が必要であろう。しかし、ＥＣ上のリスクの特徴である事故が起きた場合の過失の立証が極めて困難であるという点やその証明に係る経済的な効率性を考慮すれば、あらかじめ一定の損害負担のルールを定めておくことが必要である。

企業間取引においては、契約書上でこれらの取り決めを行うことが可能であるが、不特定多数の消費者との取引である企業・消費者間取引（ＢｔｏＣ）においては、業界の自主規制ルールのような形であらかじめ明示しておくことが必要であろう。

特に消費者のＥＣにおける決済上の金銭的損害に対する責任限度額や事故が起こった場合の調査・解決のプロセスをあらかじめ明示し、消費者が安心してＥＣに参加できる環境を整えることは重要である。

消費者（利用者）・企業および決済機関（金融機関）が一定の損害を分担し、それぞれが一定の責任のもとに注意義務を果たし､安全なシステムの構築及び管理の推進に努力することが我が国のＥＣの発展に最も寄与するであろう。

リスク評価ワーキンググループメンバー名簿

青木　尚巳	住友海上火災保険(株)	官公開発部　課長代理
粟田　浩史	(財)金融情報システムセンター	総務部　国際業務室　室長
井上　貴博	日本電気(株)	金融ﾆｭｰﾋﾞｼﾞﾈｽ開発推進本部 ｲﾝﾀｰﾈｯﾄﾋﾞｼﾞﾈｽ推進部　ﾏﾈｰｼﾞｬ
今井　英雄	安田火災海上保険(株)	企画開発部　課長
柿原　大介	住友海上火災保険(株)	火災新種保険部商品企画ﾁｰﾑ　課長代理
高津　義明	東京海上火災保険(株)	公務開発部　特命ﾌﾟﾛｼﾞｪｸﾄﾁｰﾑ　ﾘｰﾀﾞｰ
定行　恭宏	安田火災海上保険(株)	火災新種業務部商品企画課　課長
鈴木　淳	ユーシーカード(株)	EC 事業部　調査役
鈴木　紀勝	三井海上火災保険(株)	火災新種業務部ﾘｽｸﾏﾈｼﾞﾒﾝﾄ担当　副長
寺澤　真一	三井海上火災保険(株)	商品ｻｰﾋﾞｽ開発部　主任
永井　庄治	富士通(株)	ﾈｯﾄﾜｰｸｻｰﾋﾞｽ本部 Web ｱﾌﾟﾘｹｰｼｮﾝ統括部 ﾈｯﾄﾜｰｸｱﾌﾟﾘｹｰｼｮﾝ部　ﾌﾟﾛｼﾞｪｸﾄ課長
長嶋　潔	東京海上火災保険(株)	公務開発部　特命ﾌﾟﾛｼﾞｪｸﾄﾁｰﾑ　ﾘｰﾀﾞｰ
長野　重美	(株)東芝	CE･SI ｺﾝｻﾙﾃｨﾝｸﾞ推進部 EC 事業推進担当　主査
長谷川　裕樹	日本信販(株)	ﾈｯﾄﾜｰｸ企画本部　ﾈｯﾄﾜｰｸ推進室 ﾏﾈｰｼﾞｬｰ
日置　貴史	ユーシーカード(株)	EC 事業部
堀　孝光	ＮＴＴコミュニケーションズ㈱	ﾋﾞｼﾞﾈｽﾕｰｻﾞ事業部　企画部　主査
前川　明子	ＮＴＴコミュニケーションズ㈱	経営企画部　ﾄﾞｯﾄ･ｺﾑ・ﾋﾞｼﾞﾈｽ･ｲﾝｷｭﾍﾞｰｼｮﾝ･ﾀｽｸﾌｫｰｽ".com bit"
前田　正法	(株)ジェーシービー	情報ﾈｯﾄﾜｰｸ部　部長代理 EC 企画ｸﾞﾙｰﾌﾟﾏﾈｰｼﾞｬｰ
宮部　潤	三菱電機(株)	情報ｼｽﾃﾑ製作所　流通・ｻｰﾋﾞｽ・通信ｼｽﾃﾑ部　EC 事業推進ｸﾞﾙｰﾌﾟ　ETC ｿﾘｭｰｼｮﾝ担当ﾏﾈｰｼﾞｬｰ
村山　英樹	(株)三菱総合研究所	ｼｽﾃﾑｿﾘｭｰｼｮﾝ研究ｾﾝﾀｰ　応用ｼｽﾃﾑ部 研究員
谷ヶ城　保	日本電子計算機(株)	総務部企画課

(委員氏名五十音順)

電子商取引実証推進協議会

福井　正実	主席研究員
栗本　雅仁	主席研究員

平成１２年3月発行
発行：電子商取引実証推進協議会
東京都江東区青海２－４５
タイム２４ビル１０階
Tel　03-5531-0061
E-mail　info@ecom.or.jp