「電子商取引の諸問題と監査上の対応　＜Ｂ to Ｃにおける固有のリスクと内部統制＞」について

ＩＴ委員会研究報告第22号「電子商取引の諸問題と監査上の対応＜Ｂ to Ｃにおける固有のリスクと内部統制＞」が、９月３日の常務理事会において承認されましたのでお知らせいたします。なお、ＩＴ委員会は、従来の情報システム委員会が名称変更したものです。

近年、我が国においても、インターネットによる電子商取引が急速に増加・拡大しています。Ｂ to Ｃの電子商取引は、個人が居ながらにして様々な商品やサービスを購入できる利点がある反面、会社にとって取引の相手方が不特定多数であり、取引が反復継続的でないという特徴があります。また、この取引がこの数年急速に普及したために、会社の業務として成熟していない点も見受けられます。そのため、取引相手の特定、ハッカー等の悪意の外部者からの防御、コンピュータ・ウィルス対策、取引データの完全性の確保など対応すべき問題点が多々あります。

本研究報告は、Ｂ to Ｃの電子商取引に係る諸問題を整理するとともに、当該取引における固有のリスク及びそれに対して会社が整備すべき内部統制を記述しています。さらに、それらの内部統制を監査人が把握し、その有効性を評価する際の監査上の対応をまとめています。

電子商取引を行っている会社に対する監査業務において、本研究報告を参考にしていただきたいと思います。

（常務理事　鈴木　昌治）

ＩＴ委員会研究報告第22号

電子商取引の諸問題と監査上の対応

＜ＢtoＣにおける固有のリスクと内部統制＞

平成13年９月３日
日本公認会計士協会

目　　次

はじめに

近年、電子商取引が急速に増えてきている。政府においても経済の再生に向けて、その普及発展のための法整備に力を入れており、これからもＩＴ基盤の整備に伴いますます拡大する方向にある。

情報システムの内部統制に関しては、当委員会の研究報告として「情報システムの内部統制質問書」（平成５年６月）、「情報システムの内部統制の有効性の評価過程」（平成７年６月）、また、研究報告の解説書として「情報システムの内部統制」（平成６年９月）、「情報システムのコントロールと監査Ｑ＆Ａ」（平成９年11月）が公表されているが、本研究報告は、これらを踏まえて、電子商取引の固有のリスクを特定し、監査人が電子商取引における内部統制の有効性の評価をする際の監査上の対応をまとめたものである。

電子商取引には、企業間の取引（Business to Business、以下「Ｂ to Ｂ」という。）と企業対消費者の取引（Business to Customer、以下「Ｂ to Ｃ」という。）があるが、本研究報告ではＢ to Ｃを対象としている。

Ｂ to Ｃにおいては、取引の相手方が不特定多数であり、取引が反復継続的でないことも多い。また、インターネットによる電子商取引は、この数年来急速に普及したものであり、業務として成熟していない点も多々見られる。そのため、取引相手の特定、悪意の外部者からの防御、取引データの不完全性などの点において、取引の確実性の確保が困難であるといった問題がある。したがって、本報告書では、Ｂ to Ｃを対象として絞り込み、そこにおける固有のリスクの把握と、それを前提とした内部統制の評価についてまとめた。

Ⅰ.においては、電子商取引の現状における問題点を掲げた。

Ⅱ.においては、電子商取引における固有のリスクとして８項目を掲げ、各項目につき、リスクの内容と整備すべき内部統制について一覧表の形で掲げた。これらの項目の中にはシステム一般に存在するリスクも含まれるが、電子商取引がコンピュータシステムへの依存度が高いことから、特に監査上考慮すべきものとして取り上げた項目もある。

Ⅲ.においては、Ⅱ.の各項目に共通する内部統制の有効性の検証手続を掲げた。

Ⅳ.においては、業務処理統制の一例として、販売取引の受注に関する内部統制の有効性を評価する際の要点を掲げた。

電子商取引の監査に際しては、システム専門家の利用を考慮する必要があると思われるが、システム専門家を利用する際に、監査人としていかなる点が論点となるかを認識することが重要である。

電子商取引を取り巻く環境は日進月歩の状況にあり、それに合わせて内部統制も見直しが必要であるが、現状における諸問題と監査上の対応として公表する次第である。

なお、付録に「コンピュータリスクに関連した用語解説」を記載したので参考にされたい。

Ⅰ．最近の電子商取引の諸問題

電子商取引は、インターネットを媒介として、瞬時にして世界中の相手と通信を可能にし、個人が自宅に居ながら世界の情報を入手し、世界中の商品を購入できる利点がある反面、電子商取引固有の危険性もはらんでいる。支払をしても商品が届かないなどの一般消費者側からのリスクもあるが、本研究報告では、監査人が企業の監査を実施する上での監査上のリスク及びあるべき内部統制の観点から諸問題について考察している。なお、今回の研究報告は、主にWebサイトに一般消費者がアクセスすることを前提に作成している。

電子商取引における問題点は、以下のように整理される。

(1) ネットワーク環境におけるリスク

従来の大型機システムは、企業内部の閉鎖された環境でのコンピュータシステムの運用であるため、外部からの侵入を物理的な管理で防ぐことが可能であった。すなわち、企業の基幹システムへの入力も専門のオペレータが入力し、コンピュータの言語も複雑で簡単に操作できるものではなく、データの安全性の確保は比較的容易であった。

しかし、パソコンの出現は簡易な言語を提供し、パソコンを端末とするクライアントサーバシステムは、ネットワークを通して基幹システムへの侵入を容易にしている。インターネットはオープン環境であり、世界中の誰もが企業の基幹システムへ侵入できる可能性を作り出している。ネットワークからの侵入を防ぐための完全な防御は、現時点では確立されていない。侵入者は防御を破る新たな方策を編み出すため、企業はウイルス対策など常に新しい手法を研究し続ける必要がある。

侵入者は、企業のデータの破壊や盗聴、システムのダウンを引き起こす可能性がある。

(2) 企業の内部統制の限界

Webにアクセスする端末は一般消費者のパソコンであり、社内のオペレータではない。一般消費者は基本的に企業の内部統制の外に置かれている。ハッカーのように、企業のWebや基幹システムに悪意をもって侵入する外部者に対する防御とともに、一般消費者の錯誤や誤入力も取引の信頼性を揺るがすものになる。Webが単なるメールの受付窓口にすぎず、企業のオペレータが再度、企業内部のシステムに入力し直す場合は、基幹システムが影響を受ける危険性は低いが、外部からのデータを直接受け入れる場合には危険性は高くなる。

(3) プログラムの転送

従来の大型機においてはデータは単なるデータであり、それ自体が独自に動くこ

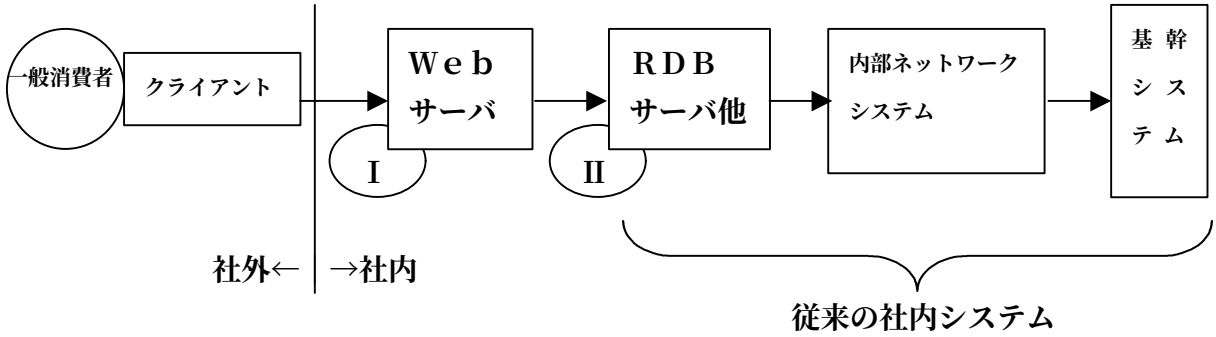
とはなかった。ところが、パソコンで使用される表計算ソフトやワープロソフトのデータファイルは、データとプログラムで構成されるオブジェクトであり、もし、メールに添付して転送されパソコンに保存されれば、転送先のパソコンで動作するという自律性を有している。

こうしたデータファイルの特性を利用して、様々のコンピュータ・ウイルスが作成され、拡散されている。コンピュータ・ウイルスは、内部ネットワークシステムのクライアントパソコン上で作動して、被害を発生することになる。

これら(1)(2)(3)の危険性は、インターネットを利用する電子商取引におけるシステムリスクとして、基幹システムの信頼性やクライアントサーバシステムの監査とは別に検討すべき課題であり、本研究報告はこの点に重点を置いている。下記のモデルのように、一般消費者が企業のシステムにアクセスできる入口に関するセキュリティ（安全）対策が今回のメインテーマである。

企業の内部ネットワークシステムから基幹システムへの不正アクセスの問題は、既存情報システムの内部統制の問題であるので、本研究報告では対象外としている。

図１　BtoCのモデル



一般消費者からのアクセス制御は、ⅠとⅡにファイアウォールを設定することにより防御される。ただし、ファイアウォールによる防御も万全のものとはいえない。

これらの問題点を無視していると、これらの問題からもたらされる事故や業務の停滞により、被監査会社に信用失墜、訴訟、会計データの消滅などの致命的な損失がもたらされる可能性がある。監査上も、データの消滅により監査が実施できない事態となったり、多大な損害賠償の危険性等による未確定事項の発生により、意見の限定もしくは意見差し控えを表明せざるを得ないおそれがある。また、致命的な損失により企業自体の継続性が危うくなる場合には、監査リスクは飛躍的に高まることになる。すなわち、これらの問題点は、監査における固有のリスクとして認識する必要がある。

Ⅱ．電子商取引における固有のリスク及び内部統制

固有のリスクのうち、盗聴、なりすまし、不正アクセス及びDoS攻撃(Ⅱ．２参照)の各項目は、外部の悪意者からの意図的な攻撃に関するものである。

その攻撃の目的は、情報の窃取と会社のシステム等の破壊の二つに亘っており、その攻撃の対象も、通信路上と会社システム内の二つに分かれる。

これらを要約すると以下のとおりである。

<table>
<tr><th colspan="2">目的</th><th>リスクの種類</th><th colspan="2">主な対象</th></tr>
<tr><td rowspan="4">↑
情報の窃取
｜
｜
システムの破壊
↓</td><td rowspan="4"></td><td>盗聴</td><td colspan="2">通信路上</td></tr>
<tr><td>なりすまし</td><td rowspan="3">社内システムへ</td><td>侵入する</td></tr>
<tr><td>不正アクセス</td><td>侵入する</td></tr>
<tr><td>DoS攻撃</td><td>侵入を必要としない場合がある</td></tr>
</table>

１．盗聴、なりすまし

(1) 盗聴の固有のリスク

盗聴という用語は、一般的には当事者同士の会話の内容を盗み聴くという意味で使用される。これに対して、電子商取引において使われる盗聴という用語は、同様の意で用いられているが、会話の内容に当たるのは、企業のデータや取引データなどの電子データである。インターネットにおけるデータのやり取りは、郵便に例えればハガキのようなものであり、データの伝送途上でデータの内容を見ようとする者があれば、容易に見られるものであると考えるべきである。電子商取引でのやり取りにおいては、内容だけではなく、パスワードやクレジット番号が盗聴されて悪用されるケースも考えられるため、盗聴に対する対策は不可欠となる。

この盗聴における固有のリスクとしては、以下のものが挙げられる。

① 暗号化などの処理を行っていなければ、電子データの内容を容易に解読できてしまう。

② 第三者による不正な盗聴に対して、盗聴が行われている事実の把握が困難である。

③ ＩＤ、パスワードなどが盗聴されることによって、なりすまし・侵入が発生する可能性がある。

④ 電子データが盗聴されることによって、改ざんが発生する可能性がある。

(2) なりすましの固有のリスク

電子商取引において使われるなりすましとは、他人のＩＤ、パスワード等個人を識別する情報を利用し、当該個人を識別する情報の保有者になりすまして行われる

行為である。この結果、電子商取引において様々な行為を当該他人（正当な取引主体）になりすまして行うことが可能となってしまう。このなりすましにおける固有のリスクとしては、以下のものが挙げられる。

① 本人認証などの処理を行っていなければ、悪意の第三者が正当な取引主体として取り扱われてしまう。

② なりすましによる不正取引によって、損害が発生する可能性がある。

③ 損害などが発生するまで、第三者によるなりすましが行われている事実の把握が困難である。

④ なりすましによって、改ざんが発生する可能性がある。

(3) 具体的な問題の発生例

例えば、悪意の第三者がなりすましにより、何かを購入するという行為を行っていれば、代金支払い義務が、また、販売するという行為を行っていれば、財貨もしくは役務の提供義務が発生する。さらに、代金自体をなりすましによって詐取されている可能性や、当該企業の信用問題に繋がるがるケースも考えられる。その他、なりすましによって、重要な情報が引き出され、重要なデータが第三者に売り渡されるリスクも考えられる。

（ｉ）購入・販売

例えば、購入・販売という行為において、代金支払い義務、及び財貨もしくは役務の提供義務が発生する。セキュリティに関して何らの対応もしていない場合、電子商取引においては、その特殊性から以下のようなケースが発生する可能性がある。

① パケットの盗聴による他人のＩＤ、パスワードの取得－＜盗聴＞

② 不正取得したＩＤ、パスワードによる企業への大量の購入申込みによる商品詐取－＜なりすまし＞

（ii）企業情報

例えば、ある企業が営業用にモバイル環境で外部から企業のネットワークに接続できる仕組みを構築していたとする。ここで、何らの対応もしていなかったため、以下のようなケースが発生する可能性がある。

① パケットの盗聴による他人のＩＤ、パスワード取得－＜盗聴＞

② 不正取得者が企業の社内ネットワークに当該企業の社員としてログインし、機密情報を入手して第三者に売り渡す－＜なりすまし＞

（iii）その他

例えば、企業で顧客管理に利用しているサーバの管理者ＩＤ、パスワードを不正に取得して、登録しているアドレスにウイルス付きのメールを送るケースや、企業のためのホームページを作成し、クレジットカード番号などを不正に取得し悪用することによる企業信用の低下なども考えられる。

(4) 整備すべき内部統制

統制目的	統制手続
盗聴、なりすましなどに対する社内体制の整備	① セキュリティポリシーを設定する。 ② セキュリティ教育を実施する。 ③ セキュリティ管理担当者を設置する。 ④ 定期的な監査を実施する。
盗聴の防止	① 暗号化を行い、暗号鍵を管理する。 ② 通信路上リスク対策を実施する。
なりすましの防止	① 第三者機関の認証制度を導入する。 ② 電子署名を利用する。 ③ 最終ログ時間を確認する。 ④ 類推が困難なパスワードを使用する。
改ざんの防止	① 暗号化及び暗号鍵を管理する。 ② 電子認証を利用する。

2．不正アクセス、DoS (Denial of Service:サービス不能)攻撃

(1) 不正アクセスの固有のリスク

不正アクセスは、本来の使用目的以外の目的をもって、正規にアクセス権限を与えられていない利用者がネットワークに入り込み、そのネットワーク内のサーバやクライアントの情報を引き出したり改ざんしたりすることである。侵入者には、単に侵入に成功することに満足を覚えるハッカーもいれば、データを破壊したり、書き換えたり、盗んだり、また、プログラム自体を書き換えたり、破壊したりするクラッカーと呼ばれる者もいる。ここでネットワーク上の破壊とは、通信上の操作で特定のコンピュータやデータを使用不能にすることを意味する。コンピュータが使用不能に陥れば、企業の基幹業務の活動停止や、取引データの損傷などが発生する固有のリスクがある。

インターネットからの侵入においては、コンピュータ通信ネットワークならではの問題がある。ソフトウェアやOSの不具合からくるセキュリティホール（セキュリティ上の抜け穴）が発見されると、その情報はすぐに公開され、修正プログラムがオンラインで配布されるが、ハッカーもその情報を得ることができる。また、ハッカー用のインターネットサイトがあり、簡単に侵入できるツールが開発されており、誰でもハッカーになれる状況が一方では存在している。インターネットの基礎技術は基本的に公開されているため、誰でも簡単にハッカーになれる環境が作り出されていることも固有のリスクである。

(2) DoS攻撃の固有のリスク

ネットワーク上で提供しているサービスを停止させる行為は、DoS(Denial of Service:サービス不能)攻撃と呼ばれる。DoS攻撃は、企業の業務を一時的に完全に

停止させることが可能であり、時にはシステムを破壊する可能性がある。これも固有のリスクである。

具体例として、Ping攻撃、メール爆弾攻撃、ウイルス感染による破壊などがある。

Ping攻撃は、大量のデータをWebサーバ等に送りつけて、その正常なサービスを妨害するものであり、また、メール爆弾攻撃は、大量のメールをメールサーバに送りつけることで、メールサーバをクラッシュさせるものである。いずれの攻撃の目的とも、サイトの機能麻痺による嫌がらせである。特定の企業に対する商業妨害の他に、政治的な意図を持つサイバーテロの犯罪もある。最近では、DDoS(Distributed Denial of Service:分散型サービス不能攻撃)と呼ばれる、更に大規模なサービス不能攻撃が起き、著名サイトが実際に攻撃を受けて業務に支障をきたしている。

(3) 整備すべき内部統制

統制目的	統制手続
侵入の防止	① ファイアウォールの設置及び運用管理を行う。 ② 外部のインターネットと社内LANを分離し、プロキシサーバを使用する。 ③ サーバへの物理的なセキュリティ対策を実施する。 ④ ワンタイムパスワードを導入する（ＲＡＳ利用時)。
破壊の防止	① セキュリティホールを排除する。 ② 対策を常時実施する管理者を置く。 ③ データのバックアップを行う。 ④ セキュリティ保険へ加入する。
不正アクセスに対する社内体制の整備	① セキュリティポリシーを設定する。 ② セキュリティ教育を実施する。 ③ セキュリティ管理担当者を設置する。 ④ 定期的な監査を実施する。

３．取引データの誤り及び不完全化

(1) 固有のリスク

取引データの正確性・完全性を損なう要因のうち、意図的でないものとしては、入力の誤り、通信回線の障害、Webサーバ等のシステムの障害を挙げることができる。これらは対面取引でないことによるリスクであり、通信販売などと共通性を持つものがある。

まず、取引データの入力誤りについては、商品及び取引条件の表示、取引申込操作等について不親切なシステム設計が原因で、入力画面において消費者が意図しない取引指示をしてしまい、認識の違いによってトラブルを誘発するおそれがある。

次に、通信回線の障害については、取引の原始データが通信回線を通じて直接授受されるため、通信回線の障害に伴って、通信路上の取引データの完全性が損なわれたり、取引データが到達しないおそれがある。

さらに、システムの障害については、ハードウェア及びオペレーティング・シス

テムの障害のほか、アクセス集中時におけるレスポンスの遅延等のシステムのパフォーマンスの低下による消費者の二重入力の誘発のおそれがある。

(2) 整備すべき内部統制

統制目的	統制手続
消費者の誤入力防止のための入力設計	① 入力内容の確認及び購入意思の確認プロセスを組み込む。 ② 誤操作を招かない画面設計や操作設計を徹底する。
安全性の高いネットワーク構成	① 安全性を考慮したネットワーク構成ポリシーを確立する。 ② 構成ポリシーに則した構成を実現する。 ③ 適切なアドレス管理を実施する。 ④ 通信回線を二重にする。 ⑤ バイパスルートに対するセキュリティ対策を実施する。 ⑥ 構成管理を適切に実施する。
各種ネットワーク機器、サーバの安全性の高い使用	① 各種機能の適切な設定を確認する。 ② ログの取得と定期的なチェックを実施する。 ③ メンテナンスを適切に実施する。
システムの負荷に関する管理体制	① システム負荷に対する常時モニタリングを実施する。 ② システム負荷を分散させる業務体制を構築する。 ③ 特別なイベント等を見越して、適正な余裕率を設定する。
障害のリスクと回復についての方針の明確化	① リスク分析を実施し、障害のリスク及び電子商取引に与える影響範囲を明確にする。 ② 障害により企業が被る損失を分析する。 ③ 業務の回復許容時間及び回復優先順位を設定する。
ハードウェア及び通信回線の障害対策機能及び保守機能の設定	① データのエラー検出機能を設定する。 ② 障害内容を解析し、障害箇所を特定化する機能を設定する。 ③ システムを停止しないで保守する機能を設定する。
バックアップ方法の確立	① 業務の回復目標に対応したバックアップ方法を設定する。 ② バックアップ方法及び手順を検証する。
代替処理・復旧手続の設定	① 復旧までの代替処理手続及び体制の設定と検証を行う。 ② 復旧手続及び体制の設定と検証を行う。
緊急時対応計画の策定	① リスク分析の結果に基づき、緊急時対応計画を策定し、トップ・マネジメントの承認を得る。 ② 緊急時対応計画の実現可能性を確認する。 ③ 緊急時対応計画に基づいた訓練を定期的に実施する。 ④ 緊急時対応計画の見直しを行う。
セキュリティ監査の実施	定期的なセキュリティ監査を実施する。

4．プライバシーの保護

(1) 固有のリスク

昨今コンピュータやネットワーク情報化などの情報技術が急速に進歩してきており、企業で電子商取引を行っているケースが非常に多くなってきている。企業は

インターネット等を利用した電子商取引などにより、個人情報データを大量に蓄積し、その情報を利用して営業活動を行っている状況である。これに伴い、第三者が個人情報を部分的に取り出して、その人の片寄った個人データを作り上げてしまうおそれ、あるいは情報を不当に利用したり加工してしまうおそれ、また個人情報が流出したり不正に利用されてしまうおそれが強まってきている。

また、個人から見た場合でも、電子商取引を行う場合に、「自己データの漏洩」の不安が非常に多い状況にある。

個人情報はデータとして蓄積されることが多いため、セキュリティがかかっていなければ情報を持ち出すことが比較的容易である。これらの情報の流出が明らかになった場合、訴訟により多額の賠償金を要求されたり、信用を著しく失うことにより、取引が激減し倒産に追い込まれる可能性もある。したがって、個人情報の保護の問題は固有のリスクに該当する。企業は、情報プライバシーについては厳重な取扱いを行うことが必要である。

(2) 整備すべき内部統制

統制目的	統制手続
個人情報の保護管理体制の確立	① 個人の取引情報に対する保護管理基準を確立する。 ② 個人情報について保護管理の基準を反映させた運用規定を作成する。 ③ 個人の取引情報の保護に関して管理責任体制を明確にする。 ④ 個人情報について利用目的による制限を設ける。 ⑤ 個人情報については適正な方法による取得であることを明確にする。
システム上の個人情報について保護管理の実施	① システムによる個人情報の管理については必要な保護機能を設定する。 ② 個人情報の管理規定に則したシステム上の保護管理の実施とその実行管理を実施する。 ③ 個人情報の内容については常に正確性を確保する。
個人情報に関する印刷物･磁気媒体等の保護管理の実施	① 個人情報の管理規定に則した印刷物・磁気媒体等の保護管理の実施と、その実行管理を実施する。 ② 個人情報の流出に備え安全保護措置のシステムを設け、実施する。
個人情報の取扱いに関する監査の実施	取引情報の取扱いに関する定期的な監査を実施する。

5．コンピュータ・ウイルス

(1) 固有のリスク

電子商取引を行うためのオープンシステム（外部からのアクセスが可能な情報システム）を有する事業者にとって、コンピュータ・ウイルスは、重要なリスク要因である。コンピュータ・ウイルスとは、意図的にコンピュータのファイル等を破壊

したり、書き換えたりして、利用者の意図せざる結果やシステムの破壊をもたらすプログラムやマクロ（特定のプログラムの動作を規定する言語）をいう。コンピュータ・ウイルスに感染すると、会計ファイルなど重要なデータが壊れたり、システムの動作に必要なファイルが壊されることで、コンピュータ自体が立ち上がらなくなる可能性がある。最悪の場合、監査証跡が無くなることで、監査の実施が困難となり、監査意見を差し控えざるを得なくなる危険がある。

コンピュータ・ウイルスは、オープンシステムでなくても、スタンドアロン（コンピュータ単体）やクローズドな企業内ＬＡＮ（ローカル・エリア・ネットワーク）でもフロッピーディスク等を通じて感染し得るが、インターネットと接続されたコンピュータでは、外部とのプログラムのやり取りや電子メールに添付されたプログラムないしワープロや表計算のファイルのマクロにより感染・増殖するため、被害の規模と被害進展の速度が著しく早まり、企業システムにとって致命的な被害をもたらす危険がある。

コンピュータ・ウイルスの感染を防ぐには、コンピュータ・ウイルスを発見、駆除するためのソフトウェア（ウイルス対策ソフト）を企業システムに導入する必要がある。ウイルス対策ソフトは、コンピュータでやり取りされるファイルを監視して、やり取りされるファイルの中にウイルスに感染したものがないかどうかを調べる機能を持っている。

ウイルス対策ソフトの導入方法としては、各クライアントマシンにウイルス対策ソフトをインストールして、常駐稼働させる方法と、企業内のシステムとインターネットとの中継点となるゲートウェイやグループウェア・サーバでウイルスを発見・駆除できるように、ウイルス対策ソフトを導入する方法の二つがあり、企業のシステム構成に応じて、両者を組み合わせて活用する必要がある。

また、コンピュータ・ウイルスは、日々新種が作られ、既存種も改変されて種類が増加している。そのため、ウイルス対策ソフトがウイルスを見分けるためのパターンファイルを定期的に更新したり、ウイルス対策ソフト会社からの情報を収集していく必要がある。そのため、ひとたびウイルス対策ソフトを導入すれば済む問題ではなく、日々の運用として、情報システム運用にウイルス対策が組み込まれている必要がある。

したがって、情報システムにおけるコンピュータ・ウイルスへのリスクの分析に当たっては、ウイルス対策の整備状況とその運用状況とを調べる必要がある。

(2) 整備すべき内部統制

統制目的	統制手続
コンピュータ・ウイルス対策体制の確立	① コンピュータ・ウイルスに対する知識を収集する体制を整備する。 ② コンピュータ・ウイルスに対する情報を整理し、社内のシステム管理者に連絡する体制を整備する。

システム導入時におけるウイルス検査の実施	① 会社のシステムの状況を分析して、状況に応じて適切なコンピュータ・ウイルス発見・駆除のためのシステムを導入する。 ② コンピュータ・ウイルスを発見・駆除するシステムについてのドキュメントを整備する。
ウイルス侵入防止機能の適切な使用	① ウイルスのパターンファイルの更新を定期的に実施するなど防止機能を適切に実装する。 ② コンピュータ・ウイルスを発見・駆除するシステムの運用のマニュアルを整備する。 ③ 外部からのメールやフロッピーディスク等によるファイルの持込みについてのルールを社内に対して教育する。 ④ 規定に即したウイルス検査の実施とその実行管理を実施する。
ウイルス侵入発見時の適切な処置の実施	コンピュータ・ウイルスに侵入された場合の行動マニュアルを整備して、万一の場合に対処できるように準備する。
ウイルス対策体制の維持・充実	① コンピュータ・ウイルスに関する最新の情報と照らして、現状の運用システムの妥当性について定期的に見直す体制を整備する。 ② 上記の対策を整備・運用するのに必要な予算を確保するために、経営者が、コンピュータ・ウイルス対策が企業のリスク管理上重要であることを認識する。

6．プログラムバグ

(1) 固有のリスク

プログラムバグとは、プログラム作成にミス（意図しないもの）があり、結果として業務処理が意図した結果にならないことである。

ソフトウェアの開発過程において、テストをいかに十分に実施したとしても、潜在的なプログラムバグを完全に排除することは、経済性を考慮すると技術的に極めて難しいといわれている。

電子商取引においては、特に短期間にビジネスを立ち上げる必要性が高く、プログラムのテスト期間が十分に取れないまま本番稼動に突入せざるを得ないことも多いため、プログラムバグの発生の可能性は高い。

電子商取引では、パッケージソフトを利用する場合も多いが、この場合でも、戦略性の強化や利便性の向上を目的とした独自仕様の追加、基本機能の変更等のカスタマイズ化が多く見られる。カスタマイズ化によるプログラムバグのリスクは同様に存在する。

事業者との継続的な取引であれば、商慣習としての善管注意義務から、相互にチェックが働き、約定との相違には容易に注意が払われるが、一般消費者とのネット取引では、相互チェックが利きづらく、プログラムミスがあった場合にもその発見が遅れやすい。この結果、一般消費者との取引情報に不完全な点や、不正確な点が

生じ、トラブルが発生するというリスクがある。

Webサーバのプログラムには、セキュリティ上の欠陥としてセキュリティホールが発見されることが多く、外部からの不正侵入に狙われやすい。このセキュリティホールもプログラムバグの一種ということができる。

セキュリティホールの存在を放置した場合には、悪意の外部者に迷惑メールの踏み台として自社のサーバが利用され、他社から発信元として疑われ、社会的信用が失墜してしまうリスクもあることを認識することが必要である。

(2) 整備すべき内部統制

統制目的	統制手続
システム要件定義の十分な検討	システム開発手順を明確にし、承認手続を遵守する体制を整備する。
システムの実現可能性が妥当であることの確認	情報技術の現状レベルを的確に把握する体制を整備する。
情報技術の採用についての経営者の意思決定が適時・適切に行われることの確認	情報システムの採用・変更に関する規定を作成し、それを遵守する体制を整備する。
ビジネスモデルとシステムモデルの整合性の確保	ビジネスにおけるデータ量の予測分析、時間帯の負荷分析を適切に実施し、承認を得る体制を整備する。
ビジネスパートナーの管理の適切性	ビジネスパートナーの作業と自社の作業との役割分担を契約上明確にする。
パッケージの選定に関する適切性	パッケージの選定手続を規定し、実行する。
顧客のクレーム情報が適時に入手され、速やかに対応されることの確認	顧客のクレーム情報、対応情報をデータベース化し、改善活動に役立てる。

７．技術の陳腐化、ビジネスモデル

(1) 技術の陳腐化の固有のリスク

電子商取引では、顧客の要求にマッチした高度な情報処理技術が、企業競争の成功要因になっている。しかしながら、情報システムの技術進歩のスピードは極めて急速であり、技術の優位性を確保する期間は極めて短いのが特徴である。

電子商取引を実現するための情報システムには、多額の開発投資が必要であるが、投資を回収する前に、競合他社が最新技術を安価かつ高性能で実現した場合には、技術の陳腐化による技術の優位性が逆転してしまうリスクがある。

(2) ビジネスモデルの固有のリスク

新技術の導入に際しては、ビジネスモデル特許に注意を払う必要がある。ビジネスモデルはビジネスの仕組み、ビジネスの方法のことであり、従来は特許の対象ではないと考えられてきた。しかし、1998年７月に米国の裁判所でビジネス方法も特

許になるとの判断が示され、その後、インターネットやコンピュータを用いた新しいビジネスの方法も特許対象と考えられている。自社のビジネスの方法を検討する際には、他社からビジネスモデル特許の侵害がないかを確認しないと、訴訟を受け、また、せっかく開発したビジネスの方法が使用できなくなるリスクがある。

(3) 整備すべき内部統制

統制目的	統制手続
技術革新に対応する体制の整備	① 新技術の情報を収集する担当部門、もしくは担当者を設置する。 ② 新技術の導入に対応する部門、もしくは担当者を設置する。 ③ システムの変更が容易なシステム設計のルールを明確にする。
ビジネスモデル特許に関する管理体制の整備	① 特許に関する情報を収集する担当部門、もしくは担当者を設置する。 ② 法律問題に対処する部門、もしくは担当者を設置する。 ③ 新技術の導入の際にビジネスモデル特許を検討する手順を明確にする。

８．ビジネスパートナーの倒産

(1) 固有のリスク

電子商取引に関するシステム開発、パッケージの提供またはホスティング等について、アウトソーシングを活用することが多く見られ、また技術上の理由から代替できるビジネスパートナーが少ないことが挙げられる。ショッピングモールをＡＳＰ(アプリケーション・サービス・プロバイダ)事業者に依存している場合もこれに該当する。代替できる場合でも、代替が完了するまでの期間業務を停止していると、事業としての優位性を失うおそれが生じる。

ビジネスパートナーの財務上の基盤が必ずしも強くない場合もあり、ビジネスパートナーが倒産した場合など、業務サービスの継続性が保証されないと、企業の事業の継続性が維持できないおそれがでてくる。また、倒産によりビジネスパートナーに管理されていたデータの流出が発生するなどのリスクがある。

(2) 整備すべき内部統制

統制目的	統制手続
ビジネスパートナーの財務基盤に問題がないことの確認	ビジネスパートナーの信用状況、財務状況を定期的に調査・分析する。
ビジネスパートナーの内部統制に問題がないことの確認	ビジネスパートナーの内部統制を定期的に調査・分析する。
ビジネスパートナーは多額の訴訟事件を抱えていないことの確認	ビジネスパートナーに訴訟事件がある場合、ビジネスパートナーの責任範囲を検討する。

ビジネスパートナーとの業務委託契約書に保守条件、損害賠償責任、監査権限、解約条件の明確化	業務委託契約書は、締結前に法務部門の承認を得る。
プログラムの権利(著作権等)関係の明確化	ビジネスパートナーとの業務委託契約書に、プログラムの権利（著作権等）関係を明記する。
プログラムの引渡の適時性、完全性	契約書に引渡物件を明記し、引渡完了によって検収する。
代替ビジネスパートナーの候補の調査	代替ビジネスパートナーの調査を随時実施する。

Ⅲ. 電子商取引に対する企業の内部統制の検証手続

ここでは、前述の内部統制につき監査人が検証する手続について述べる。

内容としては、セキュリティポリシーを中心として、その策定、整備、運用､及びそのモニタリングの検証を行う。この場合、前提として、経営トップのセキュリティに関する意識が重要である。したがって、経営トップの中にセキュリティを統括する責任者がいなければならない。

1．セキュリティポリシー

セキュリティポリシーとは､企業が情報資産や情報システムに対してどのように取り組み、組織がどのように行動すべきかという全社的なセキュリティの方針を、経営のトップが明文化した規範をいい、企業倫理や業務内容を反映したものである。

セキュリティポリシーは、システムを構築した後で作成し、従業員に提示するものであるかのようにとらえられがちである。しかし、システム開発の段階でセキュリティポリシーを設定し、提示し、その要求するレベルによってシステムを設計すべきである。高度なセキュリティレベルの設定は、コストの増加を伴い、システムの使いやすさと相反する面が生じる場合がある。業務の効率性と情報資産の保護のバランスを採り、セキュリティをどのレベルに設定するかは、経営トップの方針に関わる問題である。情報技術の進歩は速く、常に環境の変化に対応できる体制を立ち上げるためには、一般的な社内規程やガイドラインではなく、包括的なセキュリティポリシーの策定が必要である。

2．会社のリスク管理体制の整備

リスク管理体制につき、まず、責任者に対して質問を実施し、リスク管理に関する以下の項目の整備の有無を確認する。体制がない場合は内部統制が存在しないものとして、まず、内部管理体制の整備を求める必要がある。また、各段階の個別の内容については、システムの専門家の意見を求め、セキュリティ対策が十分か否かの検討を要する。

(1) 会社のセキュリティポリシーの有無

(2) セキュリティポリシーに基づく具体的なガイドライン

① ネットワークに関するセキュリティのポリシー

ファイアウォール、プロキシサーバなどの設置個所、設定内容は会社の要請するセキュリティの基準に合っているか。

② アクセスの制限

基本的に無制限に顧客を求めるか、もしくは特定の会員に制限するか、個人認証を求めるかなど、アクセス権の制限を、会社の必要とするセキュリティポリシーに従って明確に規定しているか。

③ 公開情報と非公開情報の区分

顧客のインプットした情報をどの段階で非公開情報として管理するか。

④ データの保護

データを画面に入出力する際に、データのファイルは、インターネットからアクセスできない場所に保管するように設計しているか。

⑤ データベースの更新処理

ブラウザの表示とデータベースの不整合を防ぐ設計をしているか。

例えば、注文のインプットの途中で顧客がカタログ情報に戻った場合に、最新のデータを表示するようになっているか。

⑥ 注文情報に対する顧客への公開

顧客が、自分の注文内容の登録の確認や取消がインターネットでできる機能が備わっているか。

(3) ガイドラインに基づく具体的な管理の実施を管轄する統制部門及び責任者の設置の有無

担当する管理部門の管理者が不在の場合の内部統制は、実効性がない。

３．セキュリティ対策の運用

実際にガイドラインに沿った運用を実施しているかどうかを検証する。実施していない場合は、実施するように指導する必要がある。また、実際に内部統制が機能しているかどうかを十分に検証する必要がある。

以下の項目については、責任者又は担当者に質問を実施する。また、回答の内容により、各種規程及びマニュアル等の査閲、現場の視察などの手続を実施する。

(1) セキュリティポリシーを周知徹底しているか。

(2) ガイドラインに添って実際に運用しているか。

① ネットワークの管理者はいるか。

② プロキシサーバの有無とその設置場所は適切か。

③ ファイアウォールの有無とその設定内容は十分か。

④ ＳＳＬなどの個人認証利用の有無

⑤ クレジット決済のＳＥＴやＳＥＣＥの利用の有無

⑥ データを暗号化しているか。

⑦ 注文情報の配送業者へのデータ転送や入金処理は、非公開情報として管理しているか。

⑧ 顧客が自己の注文情報を確認する画面では、顧客を特定できるユーザＩＤ、パスワードなどで管理しているか。

⑨ 誤操作を排除するバリデーションチェックを実施しているか。

４．セキュリティ対策運用状況のモニタリング

セキュリティ対策を所定の基準により実施している場合には、監査人は、次に、管

理者による適切なモニタリングを実施しているか否かを検討すべきである。

モニタリングの結果、判明した例外事項がある場合は、この例外事項に対して、管理者が適切な対応を速やかに実施していることを確認することが、内部統制のリスク管理体制を判定する上での監査のポイントである。

モニタリングを実施していない場合は、リスク管理に不備があることになる。会社自身にモニタリングを常に実施する体制がない場合には、リスク管理の実効性がないものとして内部統制の不備として勧告する必要がある。

① 外部からの不正アクセスを監視しているか。
② 外部からの不正アクセスが判明した場合に、直ちに対策を講じているか。
③ 顧客からの注文のミスなど例外事項を管理者に報告しているか。
④ 実際に不正アクセスによる被害が発生した場合の対処は実効性があるか。

以上のように、リスク管理体制を構築し、それを適切に運用し、さらにその上で異常点の発生を監視し、適切な対処を行うことが内部統制上不可欠である。

Ⅳ．内部統制の評価の具体例

ここでは、Ⅱ.で述べた固有のリスクを統制するための内部統制の検証を、特定の業務処理に応じて実施する例を挙げて説明する。

Ｂ to Ｃの具体例として、事前の契約がなく、まったく新規の一般消費者に対して取引を開始する場合（消費者がWebをクリックして購入の意思表示を行う場合など）の販売取引を取り上げ、受注時においてどのように内部統制を設定、運用しているかを検討することとする。

内部統制目標	会社が有している統制手続	統制手続の検証方法	統制手続の有効性の判断のポイント
正当性（承認）	正式受注を受けるための条件についての諸規定を作成し、承認している。	販売手続に関する諸規定を入手し、受注承認に関する権限及び手続を確認し、実際の運用を条件通りに実施しているかどうかを確認する。	Ｂ to Ｃの場合には、何をもって正式受注とするかが問題である。 一般的には入金の確認、クレジット会社の承認をもって正式受注とすることが多いが、注文をもって正式受注とし、商品発送後に振込を依頼するケースもある。 この場合のポイントは、与信の問題であり、これは通信販売業に共通するリスクである。
正当性、正確性、完全性（本人確認、内容確認）	注文メールに対し、注文請書のメールを送っている。	メールの受発信ログを閲覧することにより、注文請書メールを送っていることを確かめる。	先方に注文請書のメールを送付することにより、なりすましや、誤発信メールを排除することが可能になる。 架空のメールアドレスの排除が可能となる。 注文請書メールが届かない場合は、注文として処理しない旨を事前に明らかにしておく。 注文内容の正確性や、注文の完全性が確保できる。
安全性（盗聴）	注文メールなどの情報について盗用されないようなセキュリティがかけてある。	システムのセキュリティが完全であることを確かめる。	注文メール等の情報が盗用された場合、顧客に重大な損害を与えかねない。 また、会社にとっても信用をなくす結果にもなり、会社の存続にも重要な影響を与えることになる。

			したがって、情報のセキュリティは非常に重要な問題である。 アクセスするユーザーが不特定の場合は、セキュリティ技術としてはSSLがよく採用される。
安全性 (個人情報保護)	顧客情報の保護に関する運用を十分実施している。	データの管理方法等につき担当者にヒヤリング等を行い、内部牽制の充分な実施を確かめる。	同上
完全性	注文メールは必ず受注部門に送付するシステムがある。	メールの受注ログを受注部門に送っていることを保証する統制手続を確かめる。	すべての受注を必ず受注部門が受けて対応できるシステムになっていない場合は、顧客に対し注文を無視することになる可能性があり、信用をなくすことのもなりかねない。 自動でメールを受注部署に送付するようなシステムと、それを保証するコントロールの組込みが望ましい。 手作業部分がある場合には、コンピュータシステムと合わせて内部統制の良否を評価する必要がある。この点は、コンピュータシステムに共通する内部統制評価の問題である。
安全性 （ウイルスチェック）	受注をメールで受ける場合や、問い合わせのメールを受ける場合に、ウイルス感染する可能性があるため、ウイルスチェックソフトを稼働している。	ウイルスチェックの体制の整備状況を確認する。	ウイルスへの感染は、システム全体を不安定にしたり、システムの停止に繋がるので、事業基盤の安定性確保の観点から、注意することになる。 また、ウイルスソフトは、導入時のみでなく、パターンファイルの最新版への更新を常時実施する必要がある。

以　上

付録：コンピュータリスクに関連した用語解説

（用語の順序は、アルファベット（ABC順）、日本語（あいうえお順）となっている。）

・ＲＡＳ（リモートアクセスシステム）

外部の情報端末・PCから、リモートで社内システムにアクセスできるシステム。

ＲＡＳとして、社内システムをイントラネットで構築しているような場合では、不正アクセスの防御対策が重要になる。ダイヤルアップによる場合が多いので、ダイヤルアップ環境におけるセキュリティの設定が必要である。

・ＳＥＴ、ＳＥＣＥ

ＳＥＴ(Secure Electronic Transaction) は、電子決済の取引プロトコルとして、クレジットカード決済の標準規格になっている。加盟店の不正（盗聴、改ざん）を防止する機能がある。

ＳＥＣＥ(Secure Electronic Commerce Environment)は、クレジットカードと銀行の決済手段を規定している。

・ＳＳＬ（Secure Socket Layer）

ネットスケープ社によって開発されたデータ暗号化ための通信プロトコル。

使用者の事前の登録を必要としないので、Ｂ to ＣのWeb取引などで、不特定多数の一般消費者との取引によく使用される。

・Ｗｅｂ

WWW (World Wide Web)の省略形であり、インターネット上でシームレスに情報にアクセスすることを目的にした情報システムのこと。

Web技術により、インターネットの情報が極めて容易に利用できるようになった。

・Ｗｅｂサーバ、ＲＤＢサーバ

サーバとは、クライアントPCの要求に応じて、様々なサービスを提供する機能を意味している。

インターネットでは、Webサーバによって Webの情報を提供しており、ＲＤＢサーバによって、ＤＢ(データベース)の利用（登録、更新、照会）を提供している。

・暗号化、暗号鍵

データの解読を防止するための情報技術であり、特にインターネットのようなオープンなシステム環境では重要になっている。

暗号化にはいくつかの方法があるが、暗号を解読するキーになるものを暗号鍵とい

う。現在、最も多く使用されている暗号の方法は、公開鍵暗号方式であり、電子署名もこの方式によるものが多い。公開鍵暗号方式によるセキュリティのシステムをＰＫＩ（公開鍵基盤）という場合がある。

・個人情報の保護に関する法律

現在、「個人情報の保護に関する法律」案が国会で継続審議となっている。
この法案では、基本原則として以下の５つの原則が記載されている。

① 利用目的による制限
② 適正な方法による取得
③ 内容の正確性の確保
④ 安全保護措置の実施
⑤ 透明性の確保

また、上記に基づき、事業者に９項目の義務規定を定めており、義務規定には「利用目的による制限及び適正な取得」、「個人データの内容の正確性及び最新性の確保」、「個人データの第三者提供の制限」などがある。

今後はユーザーのネット上のプライバシー保護に対する意識が高まるのは確実であり、インターネットでビジネスを行う企業は、プライバシー保護に対する方針を明確に示せなければ、ユーザーの信頼を得ることはできなくなると思われる。情報プライバシーについて、この法案などを参考に問題のない企業内の体制を作り、運用することが必要である。

・個人情報保護に関するコンプライアンス・プログラム

日本工業規格としてJISQ15001「個人情報保護に関するコンプライアンス・プログラム（以下「CP」という。）の要求事項（Requirements for compliance program on personal information protect）」が公表されている。

これはISO14000などと同様、各事業者が自主的に個人情報保護の取組みを進めるに当たって、全経営的に体系的なCPを策定し、いわゆるPDCA（Plan、Do、Check、Action）によって継続的に改善していくことを意図したものである。以下の項目により、一定の方針の元に「計画し」、「実施し」、「監査し」、「見直す」ことをスパイラル的に継続することで事業者の個人情報保護の管理能力を高めることを意図している。

① 個人情報保護方針
② 個人情報保護のための計画
（個人情報の特定、法令及びその他の規範、内部規程、計画書）
③ 個人情報保護の実施及び運用
（体制及び責任、個人情報収集に関する措置、個人情報の利用及び提供に関する措置、個人情報の適正管理義務、個人情報に関する情報主体の権利、教育、苦

情及び相談、コンプライアンス・プログラム文書、文書管理）

④ 個人情報保護の実施及び運用に関する監査の実施

・セキュリティホール

OSやソフトウェアのプログラムの不備によるセキュリティ上の欠陥のこと。

外部の侵入者は、不正アクセスのためにセキュリティホールを狙って入りこむ。OSやソフトウェアのビジネスパートナーは、セキュリティホールの修復を絶えず行っているので、最新の修復プログラムにより、セキュリティホールの修復を行う必要がある。

・セキュリティポリシー

情報、情報資産、情報システムに対する全社的なセキュリティの方針のこと。

セキュリティポリシーには、防御すべき対象の決定、重要度の優先付け、防御方法が必要で、具体的には、セキュリティスタンダード、セキュリティ関連規定・規約を整備して、運用遵守していく必要がある。

セキュリティポリシーに記載するセキュリティ水準は、一律に規定できるものではなく、システムの有するリスクと費用対効果を勘案して、企業ごとに妥当なレベルを設定する。

・専用線

本社と工場など広域にわたるネットワーク構成で相互を結ぶ通信回線として、公衆網（一般の加入電話回線）とは論理的に分断した形として、専用線がある。外部者の侵入を防御するためには優れており、従来から広く採用されてきたが、コストが高いため、イントラネットに代替される傾向がある。

・ダイヤルアップ

公衆網の一般電話から、必要時に企業内のネットワークにアクセスする方法。

ダイヤルアップ先の電話番号を知らないとアクセスできない。特定のメンバーだけに、事前にダイヤルアップ先の電話番号とパスワードを付与して取引を行うため、インターネットによるWeb取引と異なり、クローズドなネットワークである。

ダイヤルアップ先の電話番号が漏洩するとメンバー以外の外部者が企業内のネットワークに侵入できるため、パスワードの管理を含めてセキュリティは厳重に考慮する必要がある。

ＲＡＳもダイヤルアップの一種である。

・電子署名

データ作成の本人性・正当性（データを作成した者は、本人かどうか）の確認のため、電子的な署名をデータに合わせて記載することが必要になる。電子署名の信頼性を高めるためには、印鑑証明に当たる第三者の認証機関の保証が必要になる。電子署名法により、電子署名の付いた電子データは、署名押印が行われた紙の文書と同一の法的効果を持つこととされている。

公開鍵暗号方式による電子署名は、通信途上での改ざんの有無を確認する機能も有している。

・バリデーションチェック

入力項目の間違いを、予防的に排除するためのチェック方式。

例えば、日付、金額の入力の際に、ありそうもない日付、金額が入力された場合に、入力者に警告メッセージを出して注意喚起したり、入力を受け付けないようなチェックをかけたりする。

・ファイアウォール

インターネット環境において、社内システムを外部からの不正アクセスから防御するハード／ソフトの仕組みのこと。

ただし、ファイアウォールは、データの詳細を調べるものではなく、始点と終点のアドレスやポート番号を調べているにすぎないため、ファイアウォールだけでは、ウイルスの不正侵入は防止できない。

・不正アクセス

企業情報に対する、正当な権限者以外からのアクセスのことであり、ネットワーク上からの侵入以外にも起こりうる。

例えば、端末のパソコンを立ち上げたまま昼食を取りに行ったりしている間に、悪意の侵入者にその端末の使用を許すことになり、容易に侵入を許すことになるケースがある。

・プロキシサーバ

社内LANから、インターネット接続する場合、PCごとの特定のIPアドレスを明示させないようにするため、中間に代理者に当たるサーバを立てて、外部からはこの代理者のみを明示するようにしている。この場合の代理者をプロキシサーバ(代理サーバ)という。

・ホスティング・サービス

インターネットで、 ホームページや電子商取引などを行う上で必要なハードウェ

ア、ソフトウェアや、その管理技能などを保有する企業が、それらの資源を他の企業に割り当てて、システム運用を代行するサービス。

　ホスティング・サービスを利用している場合、ホスティング・サービスの提供先が倒産したりすると、サービスの提供が停止され、利用している企業は、自社の業務が実施できなくなる可能性がある。

・ワンタイムパスワード

　パスワード（暗証番号）は本人識別のために使用されるが、アクセスするたびにパスワードを変更するものが、ワンタイムパスワードである。

　パスワードの発生は、乱数を用いているため、アクセス管理としては、強度が高い。

以　上