大塚商会の販売最前線からお届けする **セールスノウハウマガジン**

BP Navigator

usiness artner

New Year Opinion 2007

わたしたちのさまざまな経験を ぜひ自社のビジネスにご活用ください

株式会社大塚商会
代表取締役社長 大塚 裕司

ITベンダーのキーパーソンに聞く
2007年上昇ベクトルに乗るための戦略！

Open Source Solutions

高性能の迷惑メール対策エンジンを搭載し 中小企業でも手間なく簡単に導入・運用できる 『EasyNetBox for Spam Filter powered by Sendmail』

●集中連載

解体新書　日本版SOX法を読み解く

大塚商会 実践ソリューションフェア2007

BP事業部 特別セミナー情報

巻頭特集

内部統制元年 セキュリティ対策に王手をかける！

日本版SOX法で攻める セキュリティビジネスとは？

2007 vol.30

Presented by *Otsuka Corporation*

BP Navigator 80

usiness artner

CONTENTS

業界羅針盤

ITソリューション

大塚商会Value

製品情報

コラム

わたしたちのさまざまな経験を ぜひ自社のビジネスにご活用ください

○緩やかながらも拡大を続ける景気

日本経済は、緩やかな景気拡大が続き、突発的な事件、事故でも起こらない限り、2007年もこのまま堅調に推移するのではないでしょうか。日経平均の上げ幅は2006年終値が1万7,225円83銭と、2005年末を1,114円40銭（6.92%）上回り、4年連続の上昇となりました。一方、経済面では、原材料費が上昇していますので、製造業の収益率が厳しくなってきています。つまり増収したからといって、それがそのまま増益に結びつきにくくなっていると考えます。

これは、各企業のコスト削減と生産性の向上を目指した積極的な攻めのIT投資が期待でき、大塚商会にとっても販売店の皆様におきましても、大きなビジネスチャンスとなるでしょう。しかし市場規模のこれまで以上の拡大は、年頭の『Windows Vista』の市場投入をもってしてもPC市場全体の伸長には大きな期待が持てないのではないでしょうか。そうなると昨年来続いている既存市場内での競合が一段と厳しさを増すことになるでしょう。

また、日本版SOX法など、国内の法整備も徐々に整いつつあります。企業の社会的責任や倫理観が一段と重視される傾向が強まり、企業内外でコンプライアンスとセキュリティの強化が求められます。

株式会社 大塚商会
代表取締役社長
大塚 裕司

○これまでとは違った取り組みで差をつける

こうしたビジネス環境の変化をどう味方につけるかで今年は大きな差がつくのではないでしょうか。今までとは別の角度からお客様のソリューションに取り組むと、新しいビジネスチャンスが発見できるはずです。これまでの取り組みに加えて、大塚商会が販売店の皆様におすすめするのは、『たのめーる』と「更新ビジネス」です。当社のMROビジネスの根幹を担う『たのめーる』は、「オフィスのないをすぐにお届け」をキャッチフレーズに、毎年高い成長を維持しています。

この『たのめーる』のTPSショップに加盟いただくことで、販売店様もサプライビジネスに参入することが可能になります。すでに加盟されている販売店様では、お客様が一度口座をつくると半ば自動的に再注文が行われ、継続的な取引が可能なことを実感されていることと思います。さらにお取引量を拡大していただくことで、ボリュームメリットも体感いただきたいと思います。それを実現するために、当社はさまざまな販売促進施策を実施していきたいと思います。また、ソフトウェアライセンスや契約保守など「更新ビジネス」も、どんどん卸してまいります。

これらは、お客様と契約を結ぶと、販売店様に在庫や流通費の負担をおかけせず、継続的に利用いただけるビジネスです。もちろん、この場合、当社は黒子に徹しますので、販売店様のソリューションとしてぜひお客様にご提案いただきたいと思います。こうした当社独自のソリューションをご活用いただくことで、当社ビジネスパートナー事業部とお取引いただくメリットを実感していただけると思います。これがディストリビューターとして他社にない当社ならではの特徴と考えております。

○特徴ある最新のサービス&サポートを幅広く提供

ビジネスにWebが深く関与するにつれて、「ベストセラー」商品や、大口顧客だけではなく少量多種の「ロングセラー」も売上に大きく貢献するようになっています。いわゆるWeb2.0時代の「ロングテール理論」です。一般的にここ4、5年の企業規模別の伸張率を見ますと年商100億円以上の企業が一番伸びておりますが、わたしたちのビジネスを振り返ってみますと、お客様口座数の企業規模別構成比はほとんど変わっておりません。Web2.0のビジネススキーム＝ロングテールの部分、つまり中小企業の皆様の「困った」を解決する部分を、当社がサービス＆サポートでしっかり担わせていただいている結果と考えております。

販売店様から見ても、当社の特色、価値をお客様に引っ張っていただくかたちでサービス＆サポートをご提供していきたいと考えております。

そのために、当社の「サービス＆サポート」は大きく変わります。時代の進化により、ASP、ISP、BPOなど、お客様が必要とする「サポート」の幅はこれまでの枠組みから広がりつつあります。そこで、これまでのサービス＆サポートをサービス名からわかりやすく整理しようと考えています。その結果が『たよれーる』です。お客様から見たとき、サプライ品を頼むのが『たのめーる』、困ったときに頼っていただくのが『たよれーる』として、2つの名称に統合しました。「振込代行サービス」や「ゲートウェイ監視サービス」に続く新しいサービスが続々と登場します。販売店の皆様にもぜひご活用いただきたいと思います。

○昨年に続き『SMILEシリーズ』の拡販を

当社で販売しているベストセラーの業務パッケージ『SMILEシリーズ』は、昨年のある調査によれば、年商50億円以下の企業で圧倒的なシェアをとっております。当社以外のルートでもかなりの本数が出ているようですが、パッケージソフトの箱売りはどのディストリビューターでもできます。しかし当社からならば、ハード・ソフトの調達からサービス＆サポート、サプライビジネスへの参入まで、ワンストップで提供することができます。ですから販売店様でも、サポート体制も万全なベストセラーの『SMILEシリーズ』を、積極的に販売していただきたいと思います。

また基本的なことではありますが、販売店様からのさまざまな問い合わせに対する対応速度は、CSを左右する重要な要素です。ビジネスパートナー事業部では、丁寧で迅速な電話応対を心がけるとともに、営業担当者が不在の場合でも、営業支援センターなどを活用することで、各種在庫の照会や見積対応のレスポンスをさらに向上させていきます。

さらに、Web発注システム『BPプラチナ』も改良を重ね、最新の情報提供を含めて高機能で使いやすいシステムに進化させております。お客様満足の向上のためにも、ぜひ当社の『BPプラチナ』をご活用ください。

○お客様の目線で信頼に応え、お客様と共に成長する

今年の当社のスローガンは「お客様の目線で信頼に応え、お客様と共に成長する」です。昨年は「お客様の目線で、信頼に応える」でしたが、さらに今年は「お客様と共に成長する」と続けて、思いを込めたものにしました。これは、「お客様の目線で信頼に応える」ビジネスに懸命に取り組めば、必ずやお客様や販売店様とともに成長することができるという意味です。ビジネスパートナー事業部においては、この「お客様の目線で信頼に応える」ビジネスを、販売店の皆様とともに積極的に取り組んでまいります。ビジネスパートナーとしての当社に不足している部分がございましたら、販売店様から私どもビジネスパートナー事業部の担当営業にご遠慮なく、どしどしご要望や問いかけをしていただきたいと思います。そこから次のステップに向けて、パートナーシップをさらに高めていきたいと考えております。

販売店様におかれましては、提案力のあるバリューを提供できるディストリビューターとして、今年もより一層のご愛顧を賜りますよう重ねてお願い申し上げます。

日本版SOX法で攻めるセキュリティビジネスとは？

内部統制でセキュリティ対策に王手をかける！

経営者に内部統制報告書の提出が義務付けられる日本版SOX法（金融商品取引法）は、2009年3月期の決算から適用されるので、原則として2008年4月から本番運用に入らなければ間に合わない。つまり、後1年余りで何らかの対策を講じなければならないのだ。その意味では、2007年度は「実施本番前の演習スタートの年」といえるだろう。2006年11月に金融庁が発表した実施基準案（公開草案）では、特にITが果たす役割が非常に重要であると強調されている。そこで、今回の特集では、内部統制におけるIT活用の最大のポイントとなる情報セキュリティ対策に焦点を絞り、その具体的な対策方法などを紹介する。中堅・中小企業にセキュリティビジネスを展開する際の参考にしていただきたい。

日本版SOX法の動向と中堅・中小企業の対応

日本版SOX法が2008年3月期の決算から適用されるため、2007年4月から内部統制の本番運用に入らないとならない。上場企業のみならず一般企業にとっても、もはや無関心ではいられなくなっている。いざという時に備えておけば、企業の情報セキュリティを大幅に強化でき、企業の競争力を高める絶好のチャンスでもある。

日本版SOX法の実施基準案ではITが果たす役割をより一層重視

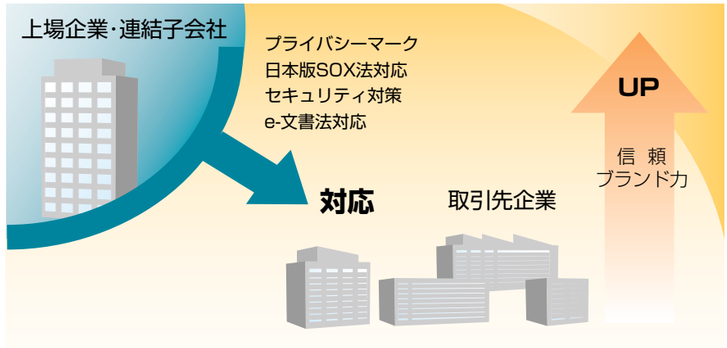
米国では、エンロンやワールドコムの粉飾決算が発覚したことから、株式市場の信頼を取り戻すために、企業に内部統制の整備を義務付けたSOX法（サーベンス・オクスリー法）が2002年に成立した。同様に日本でも、株式市場に不利益をもたらすトラブルを回避するために、2006年5月から新会社法が施行され、資本金5億円以上、または負債が200億円以上の大会社に対して、内部統制の整備が義務付けられた。さらに、2006年6月に成立した金融商品取引法（日本版SOX法）では、上場企業とその連結子会社に対して、内部統制報告書の提出と公認会計士による監査が義務付けられるようになった。原則として2009年3月期の決算から法律が適用されるため、2008年4月から内部統制の本番運用に入らないといけない。つまり、2008年4月までに少なくとも必要最低限の対策を講じておかなければならないのだ。

2006年11月には、日本版SOX法のガイドラインにあたる「財務報告にかかる内部統制の評価および監査に関する実施基準」も公開された。特筆すべき点は、決算・財務報告に係る業務プロセスの評価対象が、関連会社（持分法適用会社）や委託業者にまで広がったことだ。もうひとつは、ITへの対応に関する記述が予想以上に多いことだ。つまり、内部統制を整備するうえでITの果たす役割がより一層重視されているのである。したがって、ITをいかに有効活用するかが、内部統制を整備するうえで重要なポイントになる。

内部統制の整備は中小企業のセキュリティ強化につながる

内部統制の整備は社会的な要請なので、非上場の中堅・中小企業であっても、コンプライアンスの観点から避けては通れない。たとえば、大企業が財務報告に関係する業務の一部を中堅・中小企業に委託する場合は、その企業も内部統制の対象となる。また、個人情報保護法の観点から、大企業が取引先に対してプライバシーマークの取得を要請したように、日本版SOX法についても、取引先に適切な対応を求めてくることが予想される。したがって、非上場の中堅・中小企業であっても、内部統制の整備に早めに着手しておく必要があるのだ。

しかし、内部統制の整備は決して後ろ向きな取り組みではない。むしろ、企業価値を高める絶好のチャンスなのだ。たとえば、中堅・中小企業が内部統制にしっかり取り組んでいることをアピールすることで、企業の信頼性やブランド力がアップする。また、内部統制を整備することによって、従来の業務の無駄を省いたり、これまで手作業で行っていた業務をITツールで自動化することで業務改善にもつながる。さらに、内部統制の整備は、企業のセキュリティ対策としても抜群の効果を発揮するのだ。セキュリティ対策には終わりがないので、どこの企業も頭を悩ませている。しかし、内部統制とは、そもそも企業内の情報を適切に管理することなので、内部統制を整備することで必然的に企業のセキュリティが強化されるのだ。この点は、中堅・中小企業にとっての最大のメリットになるだろう。



内部統制とは情報管理におけるセキュリティ強化と心得る

内部統制とは、企業内で違法行為が行われないように、各業務で所定の基準や手続きを定め、それに基づいて企業内部で管理・監視・保証を行うことをいう。これを単純な言葉に置き換えると、企業内で情報を適切に管理することであり、そして、そのために重要になるのが、不正行為などを未然に抑止するための情報セキュリティ対策である。

内部統制とは情報を管理してセキュリティを強化すること

日本版SOX法で求められている内部統制の基本的な枠組みは、A)業務の有効性・効率性、B)財務報告の信頼性、C)法令遵守、D)資産の保全の4つの目的と、①統制環境、②リスク評価と対応、③統制活動、④情報と伝達、⑤モニタリング、⑥ITへの対応の6つの基本的要素で構成されている。基本的要素で共通していえることは、企業内の情報管理を適切に行うことが求められていることである。各基本的要素の内容を簡潔に表現するならば、次のようなポイントにまとめることができるだろう。

①**統制環境**とは、コンプライアンスに基づいた企業の経営方針や経営戦略を明確にして全従業員に周知徹底を図ることである。

②**リスク評価と対応**とは、組織目標の達成を阻害するリスクを識別・分析し、そのリスクを低減するための管理体制を整備することをいう。

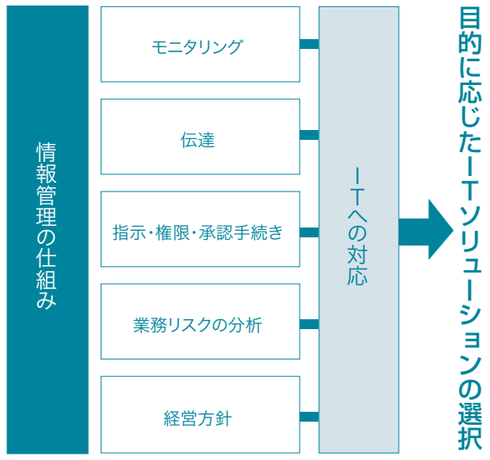
③**統制活動**とは、経営者の指示が適切に実行されるために、承認手続きや権限の付与、職務の分離などを明確にする活動のことである。

④**情報と伝達**とは、経営に必要なすべての情報を識別し、組織内外の関係者に適時かつ適切に伝達することをいう。

⑤**モニタリング**とは、内部統制が有効に機能していることを継続的に評価するための監視活動のことである。

⑥**ITへの対応**とは、上記の基本的要素を実現するためにITを効果的に活用することである。

こうしてまとめてみると、内部統制とは、情報管理の仕組みを整備することであるということがわかるのではないだろうか。特に⑤モニタリングの活動では、情報管理におけるセキュリティ対策が必要不可欠になる。たとえば、基幹系データベースへのアクセスログを収集し、財務データが誰かに改ざんされていないかチェックしたり、承認ログを収集し、承認・申請が正しく行われているかチェックしたりすることが重要なポイントになる。その意味では、内部統制とは、同時にセキュリティ対策を強化することでもあるのだ。



内部統制の整備で求められるログ管理を効率的に実施する

内部統制という観点から、特に重要となるセキュリティ対策は、ログ管理だろう。たとえば、承認フローのログ管理をきちんと行えば、高額な資産購入の稟議を、いつ、誰が申請し、どのような承認ルートを経て決済されたのかを後から調べることができるので、不適切な資産購入をした人の責任を追求できるようになる。

これを実現するためには、承認ログ機能を備えた電子承認システム『Advance-Flow』を導入するのが早道だ。大塚商会では、ERPと電子承認システム『Advance-Flow』を一体化した『SMILEie』の内部統制バージョンを今後提供していく計画だ。これにより、基幹系の帳票を誰が出力したのか、あるいはプレビューしたのかなどを詳細に把握できるようになるので、情報漏えい対策として役立つ。

また、常に最新版の文書を検索・閲覧できるようにして、その文書の版管理とログ管理を行うことも重要だ。たとえば、最新版の文書が登録されると、あらかじめ設定しておいた関係者に自動的に通知され、その文書をいつ、誰がダウンロードしたのか、あるいは閲覧したのか記録に残しておけるので効果的だ。こうすることによって、万一機密文書の改ざんや情報漏えいが行われても、誰がそれを行ったのかすぐに把握できるようになる。これは、ドキュメント管理システム『Visual Finder』を導入することによって容易に実現することが可能になる。

所属部署や職責に応じてアクセス制限を実施する

内部統制を視野に入れた適切な情報管理を行うためには、利用者ごとに割り当てられたIDとパスワードによる個人認証を実施し、重要な情報にアクセスできる利用者を限定することも重要だ。たとえば、人事データにアクセスできる利用者を制限したり、派遣社員と正社員が利用できるサービスを区分するなど、利用者ごとにアクセス制限を設けるのだ。さらに、同じ業務アプリケーションの中でも、閲覧だけ許可する人やデータ変更まで許可する人など、権限区分を設定してアクセス制御を行う必要がある。また、従業員が退職した場合は、そのIDを使って不正にアクセスされないよう速やかに削除しなければならない。またパスワードについては、誕生日など第三者に推測されやすいものは避けて適切に管理しておく必要がある。

最近では、IDやパスワードを入力する手間を省き、個人認証を効率的に行う手段として、ICカードを利用する企業も増えつつある。たとえば、入退出時にICカードで本人認証を行えば、権限が与えられた人しか入退出できないように設定することができる。また、PCを利用するときもICカードで本人認証を行い、PCに接続されたカードリーダにICカードを挿入しないとPCにログオンできず、カードを抜くとPCに自動的にロックがかるようになる。これにより、第三者によるPCの不正利用を防御し、人の出入りの多いオフィスや外出先でも安心してPC業務を行えるようになる。さらに、企業情報ポータルシステム『EasyPortal』を活用することにより、ICカードでログイン認証したユーザーの所属部署や職責に応じて、その人だけが利用できるアプリケーションやデータベースのみを表示するように設定しておくことも可能だ。

情報漏えいなどを防ぐためウイルス対策は必要不可欠

企業のセキュリティ対策では、ウイルス対策も欠かせない。特にここ数年は、悪質なスパムメールやスパイウェアが横行している。たとえば、大量のスパムメールを配信し、そこに記載されているURLからフィッシングサイトに誘い込み、そのサイトに埋め込まれているスパイウェアでクレジットカードの番号などを盗み取る営利目的の犯行が目立つようになった。このような複合化したウイルス対策を効果的に実施するために、現在では、クライアント対策に加えてゲートウェイ対策を実施している企業が増えている。なぜなら企業ネットワークの出入り口を監視することによって、外部からのウイルスなどの侵入を防げるからだ。また同時に内部からの個人情報の漏えいや有害サイトへのアクセスも水際で防止できる。

さらに最近では、持ち込みPCなどによるウイルス感染やファイル共有ソフトなどの不適切なアプリケーションの使用が増加している。これらに起因した情報漏えいから守るため、検疫システムを導入する企業もある。これは、脆弱性の高い私物の持ち込みPCなどを社内のネットワークに接続させず、必要な対策を実施するシステムのことだ。たとえば、脆弱性の高いPCはいったん隔離され、企業のセキュリティポリシーに合致しているかどうか検査される。そして、検査結果が不合格だったら、ウイルス定義ファイルの更新やOSのパッチ適用などの具体的な対策を自動的に実施し、安全が確認できた時点で社内のネットワークにアクセスできるようになる。

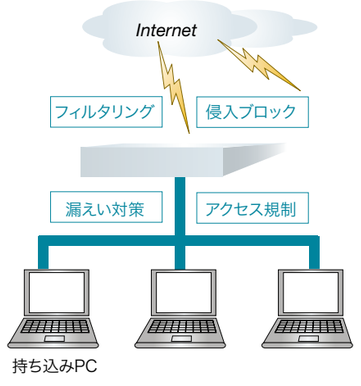
■ 承認ログ管理

『Advance-Flow』による申請・承認プロセス画面

■ 文書の版管理

『Visual Finder』による文書管理画面

■ ゲートウェイ対策



ネットワークの出入口を監視することで、水際でセキュリティ対策を行う

内部統制の視点から現状の問題点を把握することが肝要!

内部統制に準拠した適切なセキュリティ対策を実施するためには、現状の業務フローにおけるセキュリティ上の問題点を把握することが肝要だ。しかし、それを手作業で行ったり、社内のスタッフだけで行ったりするのは意外と大変である。そこでおすすめしたいのが、IT資産管理ツールの導入や内部統制に関するコンサルティングサービスの活用である。

IT資産管理ツールにより現状のIT環境を把握する

内部統制を実現するためのセキュリティ対策を実施するうえで、まず企業が行わなければならないことは、現在、企業内においてどのようなITを活用し、どこにセキュリティ上の問題点があるかを把握することだろう。しかし、全従業員が利用しているPCを1台ずつ手作業で調べていては、余計な時間や手間がかかってしまうし、正確な情報を収集することも難しい。そこで役に立つのが、IT資産管理ツールの導入である。

IT資産管理ツールを導入する一番のメリットは、運用コストを大幅に削減できることである。システム担当者が企業内のパソコンを1台ずつ調べてまわっていた作業を自動的に行えるようになるからだ。しかも、各パソコンのスペックやソフトウェアなどの情報を正確に収集して一元管理することができる。このため、システム担当者は、業務効率化や利益向上に直接役立つ、本来の情報システム活用の業務に専念できるようになる。特に専任のシステム管理者がいない中堅･中小企業にとっては大きなメリットになるだろう。

また、セキュリティ対策を大幅に強化できるメリットもある。たとえば、OSのセキュリティパッチを当てる作業を個々人に任せてしまうと、実際に行わないで放置する人が必ず出てくる。しかし、IT資産管理ツールを導入してOSやウイルス対策ソフトのアップデートを自動的に行える環境を整えておけば、そうしたセキュリティ上のリスクを抑えることができる。

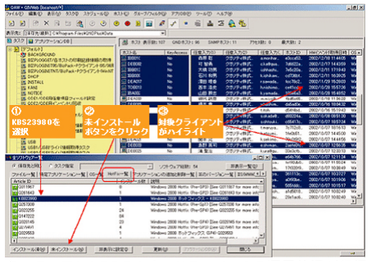
さらに、各パソコンで使用されているソフトウェアをきちんと管理することによって、ソフトウェアの違法コピーを抑止する効果もある。

豊富な機能を備えている『QND Plus』ソリューション

大塚商会では、IT資産管理ツールとして、『QND Plus』(開発元:クオリティ株式会社)を推奨している。『QND Plus』は、主に三つの機能を有している。①クライアントPCの情報を収集する機能、②ソフトウェアを配布する機能、③遠隔地からリモートコントロールできる機能である。このうち、ソフトウェアを配布する機能には、OSのセキュリティパッチやウイルス対策ソフトのアップデートファイルを自動配布する機能も備えている。国産のIT資産管理ツールであるため、ベンダーに問い合わせを行ったときのレスポンスが早く、GUIが日本語表記で使いやすいというメリットもある。さらに、オールインワンパッケージなので、データベースや特定のアプリケーションを持たなくても簡単に導入できるのだ。

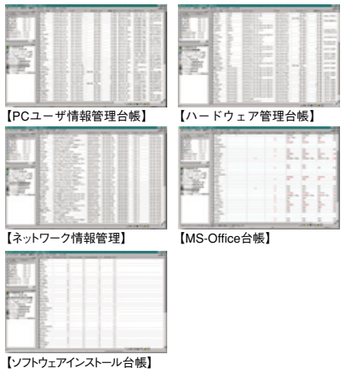
また、PC資産管理台帳『QIV』を利用して、収集された各種クライアントPC情報を台帳化することもできる。個人情報ファイル探索ツール『eXPDS』を利用して、PCに保存された「個人情報ファイル」を探査し、ファイル名や保存場所などを収集してPCごとに一覧表示することもできる。さらに、各パソコンにインストールされているソフトウェアの使用状況を細かく把握したい場合には上位ソフトの『QAW』も用意している。これにより、ソフトウェアの稼動状況を把握し、不適切なソフトウェアの起動を制御することもできる。

■ QND Plus



各クライアントPCのセキュリティパッチの運用状況が把握できるGUI画面

■『QIV(Quality Information Viewer)』の台帳による管理



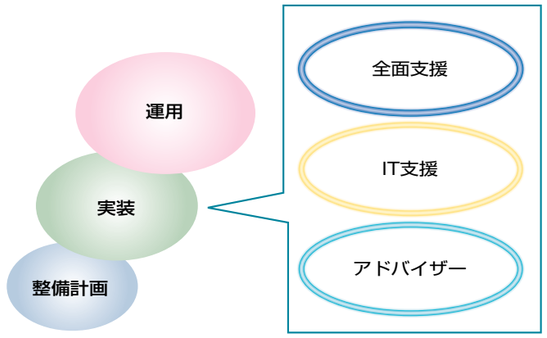
内部統制整備とITの両方に精通したコンサルを活用する

IT資産管理を活用する際のポイントは、現状のIT環境を把握したうえで、そのセキュリティ上の問題点を分析し、内部統制の視点から適切な対応策を講じることだ。しかし、これらの一連の作業をすべて社内で行うのは難しい場合もある。特に中堅･中小企業などでセキュリティや内部統制に関する専門的な知識が不足している場合は、なおさらだろう。そうした場合に役に立つのが、外部の専門家にアドバイスを受けることである。ところが、セキュリティと内部統制の両方の視点から的確なアドバイスができる人は決して多くはない。

たとえば、一般のコンサルタント会社は、たとえ内部統制に関する専門的な知識があっても、具体的なセキュリティ対策までアドバイスすることはできないだろう。また、ITベンダーやSIerは、セキュリティ対策には詳しいかもしれないが、内部統制の専門家ではないため、日本版SOX法などに対応した的確なアドバイスをすることは難しい。

その点、大塚商会は、以前からプライバシーマークやISMS（情報セキュリティマネジメントシステム）の取得支援コンサルティングサービスを行っている経験や、実際に多くの企業にITを活用したさまざまなセキュリティ対策を提案・導入・運用してきた豊富なノウハウがある。同時に、業務改善のコンサルティングサービスで培ってきたノウハウをベースに、2005年秋にいち早く内部統制に関する分科会を発足。内部統制に詳しい監査法人から専門的なアドバイスを得て、自社だけで内部統制のコンサルティングを提供できる体制を整えている。つまり。ITを活用したセキュリティ対策と内部統制に関する専門的なノウハウの両方を兼ね備えている。そのため、セキュリティに関する現状分析から、内部統制に準拠した具体的な対策まで質の高いコンサルティングサービスができるのだ。

■「内部統制整備支援コンサルティング」の<支援フェーズ>と<支援パターン>



中堅・中小企業にも最適な大塚商会のコンサルサービス

大塚商会の『内部統制整備支援コンサルティングサービス』は、整備計画、実装、運用の3つのフェーズでそれぞれきめ細かな支援を行っている。たとえば、整備計画フェーズでは、内部統制に関する全体計画や方針策定の支援を行う。現状の業務フローを分析して内部統制やセキュリティ上の問題点を分析し、そのリスクを回避する新たな業務フローを作成する。そして実装フェーズでは、ITを活用した具体的なリスク対策を実施する。それには、業務フローや重要な文書に関するログ管理、部署や職責に応じたアクセス制限など、内部統制に求められる的確なセキュリティ対策も含まれる。これにより、日本版SOX法などの法令に遵守した企業内のセキュリティ対策を施すことが可能になる。つまり、内部統制の整備とセキュリティ対策を同時に実現することができるのだ。このことは、内部統制に対応したセキュリティ対策を実施したいと考えている企業にとっては、一石二鳥の大きなメリットといえるだろう。

さらに運用フェーズでは、企業の業務担当者が内部統制の整備状況を点検するCSA(コントロール･セルフアセスメント)や、内部統制の日常的なモニタリングを行う内部監査などの運用も支援する。

また、大塚商会の『内部統制整備支援コンサルティングサービス』では、作業項目ごとに3パターンのメニューを用意している。具体的には、大塚商会が全面的にサポートするAパターン、ITに関する部分だけを手厚くサポートするBパターン、企業主導で大塚商会はアドバイザー的な立場で支援するCパターンがある。このうち、Aパターンは、内部統制の整備･運用に人を割り当てる余裕がない中堅･中小企業にとっては効果的なサービスだ。ぜひ、大塚商会のノウハウを活用して、内部統制に準拠した適切なセキュリティ対策を実現し、企業競争力のアップをしていただきたい。

SOX法対応 解体新書

日本版SOX法を読み解く

第4回

Phase 3 業務プロセスレベルの内部統制の可視化と評価

仰星監査法人 理事代表社員／公認会計士 南 成人

南 成人 氏(みなみ・なるひと)

1985年立命館大学経済学部卒業。仰星監査法人で監査や株式公開指導、内部統制導入支援に従事。最近では、BPRで培ったノウハウを背景に、企業の日本版SOX法対応の支援を主業務として活躍。2004年から日本公認会計士協会 監査基準委員会委員を務める。1986年からTAC株式会社公認会計士試験講座講師を務めている。

Phase Program

- Phase 0 日本版SOX法をめぐる最新動向とその対応
- Phase 1 全社レベル統制の可視化・評価（IT全般統制を含む）
- Phase 2 評価範囲の決定・文書化
- Phase 3 業務プロセスレベルの内部統制の可視化・評価（ITアプリケーション統制を含む）
- Phase 4 内部統制の評価・報告

2006年11月21日に実務上のガイドラインとなる「財務報告に係る内部統制の評価及び監査に関する実施基準（公開草案）」（以下、実施基準案）が公表された。待ちに待った実施基準案だが、導入の仕方次第で事務負担の大幅な増加も予想される。今号では、Phase3として、実施基準案の要求を踏まえて、評価対象となった業務プロセスレベルの内部統制の可視化と評価について解説する。

Phase1で説明したように、全社レベルの内部統制は「チェックリスト」、業務プロセスレベルの内部統制は「いわゆる3点セット」※1を用いるのが一般的な方法である。

この3点セットを効率的に作成する内部統制の文書化手技法として「業務プロセスアプローチ」を紹介する。業務プロセスアプローチとは、業務プロセスチャート上にリスク･コントロールマトリクス(RCM)と、業務記述書の内容を反映させる文書化技法である。業務プロセスチャート上でリスクに対するコントロールの効き具合をビジュアルに把握することが可能となる。

業務プロセスに係る内部統制の評価について、実施基準案は下記のように要求している。今号では、要求内容の1と2について、それぞれ実施基準案の‘勘どころ’を踏まえながら‘実務的な対応方法’を解説する。

※1)「リスクコントロールマトリクス」「業務記述書」「業務フローチャート」

業務プロセスに係る内部統制の評価要求(『実施基準案』)

経営者は、全社的な内部統制の評価結果を踏まえ、評価対象となる業務プロセスを分析した上で、財務報告の信頼性に重要な影響を及ぼす内部統制を統制上の要点として識別する。次に、統制上の要点となる内部統制が虚偽表示の発生するリスクを十分に低減しているかどうかを評価する。経営者は、各々の統制上の要点の整備及び運用の状況を評価することによって、当該業務プロセスに係る内部統制の有効性に関する評価の基礎とする。

1.評価対象となる業務プロセスの把握･整理
2.業務プロセスにおける虚偽表示の発生するリスクとこれを低減する統制の識別
3.業務プロセスに係る内部統制の整備状況の有効性の評価
4.業務プロセスに係る内部統制の運用状況の有効性の評価
5.ITを利用した内部統制の評価

1．評価対象となる業務プロセスの把握･整理

実施基準案では、業務プロセスの概要については、必要に応じ図や表を活用して整理･記録することが有用であるとし、その参考例として、「業務の流れ図」、「業務記述書」を示している。そこで、「業務プロセスアプローチ」に基づいて、業務プロセスを把握･整理する手技法を解説する。

(1)業務プロセスの捉え方

業務プロセスは、**図表1**のように階層的に構造化して捉える。最上位レベルの業務プロセスがレベル0であり、内部統制の評価対象範囲として選定された事業と外部取引先との関係を表現している。対象事業の内部を1段階ブレークダウンした業務プロセスがレベル1であり、主要な業務機能の連鎖で表現する。これをさらに詳細化したものがレベル2である。例えば、レベル1の「商品を発注する」という業務機能をさらにブレークダウンし、詳細に業務の流れを描いたものがレベル2の業務プロセスである。詳細化にあたっては、発注業務機能をさらにいくつかの業務（「仕入先選定」「縫製発注」「付属品発注」「付属品納品管理」等）にくくり、そのくくりごとに業務プロセスを描く方が整理しやすい。

(2)最上位レベルの業務プロセス（レベル0）

対象事業に関する最上位レベルの業務プロセス(レベル0)をモデル化する。

図表2は、内部統制の評価対象範囲としてアパレル(卸･小売)事業を選定した事例を示している。まず、アパレル事業を中央に位置づけ、その事業と関わりのある外部の関係先(得意先、仕入先、銀行等金融機関等)をその周りに配置する。次に、アパレル事業と外部の関係先との間にどんな関係があるのかを明確にする。この表現方法としては、四角形と矢線を使用する。物のやり取りは太矢線、帳票も含め情報のやり取りは細矢線、現金等のやり取りは点線矢線を使用し、各矢線上に具体的な情報等の名称を記述する。

図表2のアパレル事業と主要な外部の関係先との関係は、右のように表現されている。

このように、レベル0を作成し、対象事業と外部の取引先との関係を明示することによって、対象事業の範囲と業務の流れが概括的にとらえられるようになる。

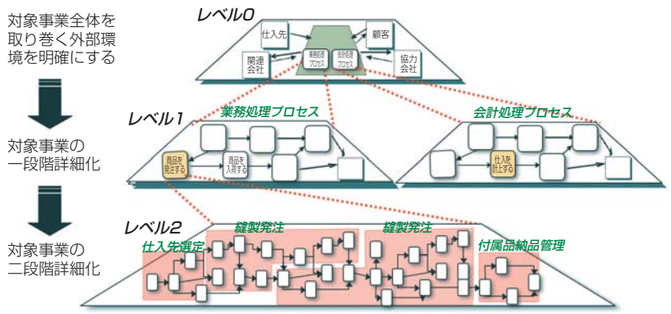
(3)対象事業を一段階詳細化した業務プロセス(レベル1)

アパレル事業の内部を大きく「業務処理プロセス」と「会計処理プロセス」に分けて一段階ブレークダウンする。その業務プロセスがレベル1である。

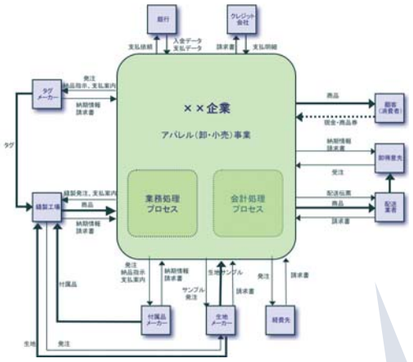
15～20程度の粗さを目安にアパレル事業の業務機能を洗い出し、管轄する部門の領域内にその業務機能を配置し、業務機能間の関連を矢線で結んでいく。その際、レベル0で記載した外部の関係先も漏れなく配置し、矢線で結ぶことになる。なお、事業が複数ある場合は、原則としてその数だけレベル1業務処理プロセスを作成することになる。(**次頁図表3**)

次に会計処理プロセスを説明する(**次頁図表4**)。これは基本的に事業ごとに異なるものではなく、複数の事業が評価対象範囲になった場合でも、一つ作成しておけば足りる。ポイントは、中央に「総勘定元帳管理」の業務機能を配置し、そこに各種会計データが集約されてくるように他の業務機能を

●図表1 業務プロセスの捉え方



●図表2 レベル0（アパレル事業の例）



- ･生地メーカーから生地サンプルを入手し、商品を企画して縫製工場に発注する。
- ･付属品メーカーに対して付属品、タグメーカーに対してタグを発注し、現物は各メーカーから縫製工場に直送される。生地は、縫製工場が生地メーカーから直接仕入れる。
- ･縫製工場から付属品及びタグがつけられた状態の商品が納品される。
- ･銀行経由で各メーカーに代金が支払われ、その支払案内を縫製工場及び各メーカーに送付している
- ･小売事業では、商品を顧客に渡し、その代金を顧客から受け取っている。クレジットの場合は、クレジット会社に請求し、銀行経由で代金が振り込まれる。
- ･卸売事業では、卸得意先から受注を受け、配送業者を通して商品を出荷し、卸得意先に請求し、銀行経由で代金が振り込まれる。
- ･諸経費の支払については、様々な取引先が想定されるが、経費先と一括りにして表現し、発注に伴い請求書を入手する。

SOX法対応 解体新書

配置することである。

また、「総勘定元帳管理」から会計データが「連結決算管理」と「開示業務管理」にデータが転送されている。この3つの業務機能をまとめて、実施基準案では「決算・財務報告プロセス」と呼称している。①総勘定元帳に取引合計を入力する手続、②連結修正、報告書の結合・組替などの年次報告書作成のための仕訳とその内容を記録する手続、及び③年次財務諸表に関連する開示事項を記載するための手続の3つである。

こうした「決算・財務報告プロセス」は全社レベルの内部統制に準じてすべての事業拠点について全社的観点から評価するものと、他の業務プロセスと同様に3点セットを作成して評価するものに区別される。例えば、連結会計基準の統一やグループ方針等が前者に相当し、一方、後者としては、決算数値の集計手続や連結パッケージの入手などが考えられる。

(4)対象事業を二段階詳細化した業務プロセス(レベル2)

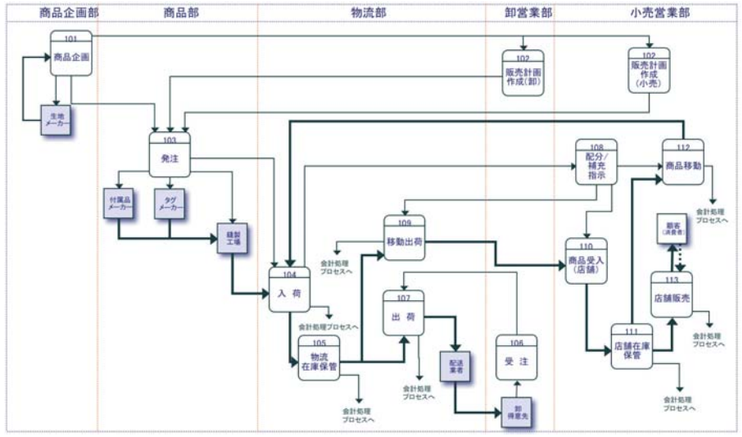
通常、レベル1の各業務機能は一つ以上のサブプロセスから構成され、その各サブプロセス単位でレベル2の業務プロセスを描くことになる。

実施基準案では、すべての業務プロセスを評価する必要はなく、評価範囲として絞り込まれた業務プロセスを評価すれば足りる。レベル2の業務プロセスを対象に評価範囲に含まれるか否かの検討を行うことになる。

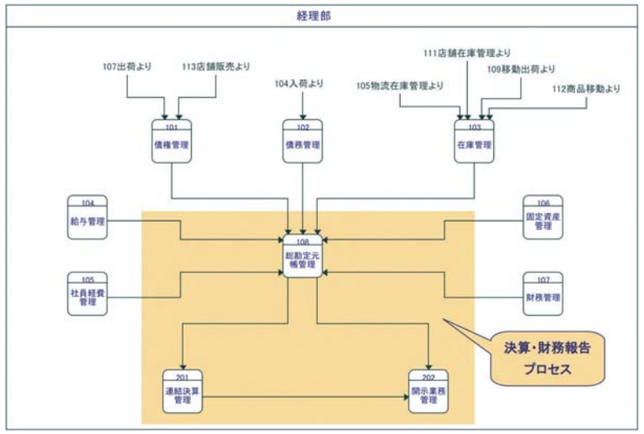
例えば、「商品を発注する」、「商品を入荷する」というレベル1の業務機能を、レベル2として各サブプロセス単位に整理すると**図表5**のようになる。

図表6は、レベル2の「商品入荷」という業務プロセスが、評価対象範囲として選定されたと仮定して、「業務プロセスアプローチ」に基づいて、業務プロセスを把握・整理している。

●図表3　レベル1業務処理プロセス(アパレル事業の例)



●図表4　レベル1会計処理プロセス(アパレル事業の例)



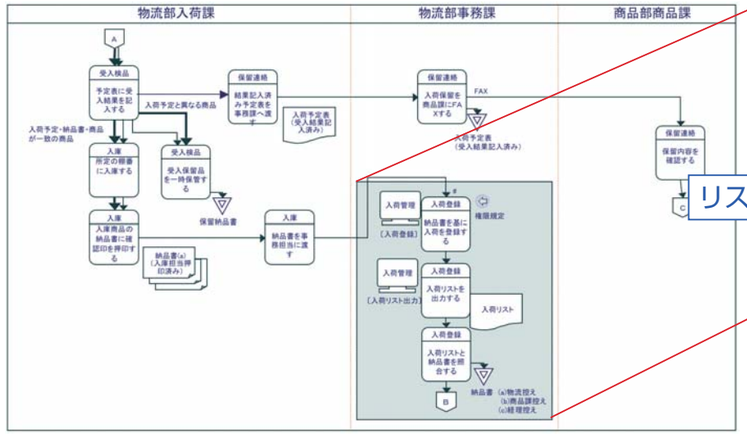
●図表5　レベル1とレベル2の業務機能のマッピング

NO.	レベル1	レベル2
103	商品を発注する	仕入先選定
		縫製・加工発注
		付属品発注
		付属品納品管理
104	商品を入荷する	商品入荷
		仕入先返品
		移動入庫

2. 業務プロセスにおける虚偽表示の発生するリスクとこれを低減する統制の識別

実施基準案では、業務プロセスにおいて虚偽表示が発生するリスクと、これを低減する統制については、必要に応じ図や表を活用して整理・記録することが有用とする。その参考例として、「リスクと統制の対応」表を示している。そこで、「業務プロセスアプローチ」に基づいて、虚偽表示リスクとコントロールを識別する手技法を解説する。

●図表6　レベル2(アパレル事業:商品入荷の例)・・・業務プロセスの把握・整理



●図表7　レベル2

図表6で、アパレル事業の商品入荷の業務プロセスを把握・整理したが、水色の枠で囲まれている部分が想定されるリスク領域である。この部分だけを取り出して、リスクに対するコントロールを識別し、そのリスクの程度をビジュアルに信号機で表示した(**図表7**)。

図表7の水色の枠で囲まれている部分がリスク領域である。意図的又は単純ミスで仕入先、商品名、単価、数量を不正確に入荷登録してしまうリスクが存在する。

まず、IT業務処理統制としてシステムインターフェイスというコントロールが識別された。仕入先マスターとの連携により、入荷登録は、仕入先マスターを呼び出して入荷実績を登録する仕組みとなっており、発注していない仕入先、商品名、単価を入荷登録できないように、システム上で制御されている。

次に、人が行う手作業の統制として照合というコントロールが識別された。入荷登録した内容がブルーフリストとして出力された入荷リストと納品書を照合することにより、数量に関する入力間違いを未然に防いでいる。これら二つのコントロールを踏まえて、リスクをどの程度まで低減できているか評価することになる。

内部統制の評価は、財務報告の虚偽表示リスクをどの程度まで低減できるかで評価する。その際、虚偽表示が発生する場合の影響度を推定し、その発生可能性も併せて検討する。

影響度は、内部統制の不備が虚偽表示をもたらす場合の影響金額を推定し、その金額に応じて、大、中、小で把握する。その発生可能性は、発生確率をサンプリングの結果を用いて統計的に導き出すこともできなくはないが、通常、定性的に高、中、低で把握する。

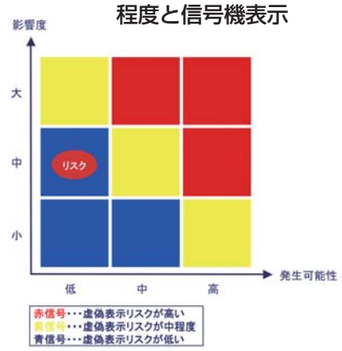
なお、影響度と発生可能性のレベルについては、解釈の相違がないように事前に決めておく必要がある。また、影響度と発生可能性の組合せから虚偽表示のリスクの程度を、ビジュアルに信号機(赤、黄、青)で表示する(**図表8**)。

今回の例示では、青の信号機が点灯し、虚偽表示リスクは低くなっている。

仕入・買掛金の誤計上や在庫情報の信頼性が失われることによって受ける影響度は中と判断し、仕入マスターに基づく入荷登録および登録後の入力チェックは目視で実施しているため、発生可能性は低いと判断した。

次号では、可視化した内部統制の整備・運用状況の評価と重要な欠陥の改善、内部統制の継続的なモニタリング体制の確立について、実施基準案の内容を踏まえながら解説する。

●図表8　虚偽表示リスクの程度と信号機表示



高性能の迷惑メール対策エンジンを搭載し、中小企業でも手間なく簡単に導入・運用できる『EasyNetBox for Spam Filter powered by Sendmail』

今やどの企業でもスパムメール対策には頭を悩ませている。しかし、なるべく手間をかけず、投資コストも最小限にとどめたいというのが本音だろう。サイオステクノロジーが提供しているセキュリティアプライアンスサーバ『EasyNetBox for Spam Filter powered by Sendmail』(以下 ENBスパムフィルタ)は、そうした要望に応えてくれる製品だ。高性能な迷惑メール対策フィルタを搭載しながら、手間なく簡単に導入・運用することができる。

■「百害あって一利なし」迷惑メールの現状と課題

迷惑メールは日々増加し、PCユーザーに多大な弊害をもたらしている。そのひとつが業務効率の低下である。たとえば、受信トレイに大量の迷惑メールが送られてくると、業務に必要なメールと迷惑メールを振り分ける作業や、後から必要なメールを検索する作業に思いのほか時間を取られてしまう。また、迷惑メール自体を受け取ることによるストレスも業務効率を低下させる一因となっている。もうひとつは、個人情報漏えいの危険にさらされることである。迷惑メールの中にスパイウェアなどが紛れ込み、知らぬ間に個人情報が漏えいしてしまうことになれば、会社の信用問題にも関わる。さらに、迷惑メールに記載されているURLをクリックすることでフィッシングサイトへ誘導し、クレジットカードの番号などを盗み取ったり、個人情報を巧妙に聞き出して振り込め詐欺などに利用されるケースもある。まさに「百害あって一利なし」が迷惑メールである。

ところが、企業内で本格的な迷惑メール対策を実施するためには、専用サーバやソフトウェアを用意しなければならず、その構築費用もかかる。また、迷惑メール対策ソフトの多くは、企業環境に合わせた詳細な設定ができる反面、設定項目などが非常に多く、設定に多くの工数を必要とする。そのうえ、迷惑メール対策技術には、異なるさまざまなテクノロジが存在し、検知率は30%～99%レベルまで大きな差がある。このため、迷惑メール対策フィルタの技術的評価は非常に高度な知識を要する困難な作業となる。さらに、誤検知によるユーザーからのクレーム対応などもシステム管理者の大きな負担となる。

サイオステクノロジーでは、こうした問題の解決策として、スパムメール対策の設定・導入・管理が容易に行え、なおかつ、投資効果の高いセキュリティアプライアンスサーバ『ENBスパムフィルタ』を提供している。LinuxやWindowsなど、あらゆるメール環境に対応する。

195mm(W)×268mm(D)×80mm(H)の省スペース設計。放熱性の高い小型アルミ筐体はファンレスで高い静音性を実現している

■ 専任管理者不在の中小企業も安心して導入・運用できる

『ENBスパムフィルタ』の特長は、まず、導入・運用管理に手間がかからないことだ。動作検証の取れたハードウェアとソフトウェアがセットになっているため、導入が容易で構築費用も削減できる。あらかじめ推奨設定済みなので、手間なくすぐに利用できるのだ。このため、専任のシステム管理者がいない中小企業でも安心して導入できる。

そのうえ、業界最高性能の迷惑メール対策フィルタを搭載し、迷惑メールの検知率が98%以上と極めて高く、検出漏れはわずか1.20%である。これは他社製品と比べたときの大きな優位性だ。たとえば、スパムメールが受信トレイに100通送られてきた場合、そのうちの1、2通のみが受信トレイに残るだけで済むので、スパムメールを手動で取り除く手間が大幅に省ける。さらに、誤検知率も0.0001%と極めて低い。このため、誤検知によるユーザーのクレーム対応も少ないので、システム管理者の負担が軽減される。

ハードウェアには、耐久性の高い工業用の部品を使用しているので故障率も低い。外形寸法は195mm(W)×268mm(D)×80mm(H)の省スペースを実現し、放熱性の高い小型アルミ筐体を採用したファンレスシステムなので、消費電力も50W以下に抑えられており、音も極めて静かだ。このため、日常業務を行っているオフィス内に設置しても場所を取らず気にならない。しかも、CF（コンパクトフラッシュ）スロットを装備し、CFからOSやアプリケーションを起動できる。CFは、ハードディスクと比べて格段に故障率が少なく、『ENBスパムフィルタ』の信頼性を高めるのに寄与している。

また、『ENBスパムフィルタ』は、検知したスパムメールを専用フォルダに格納するフィルタリング機能や、トラブル時のメール消失を回避する機能なども備えている。

■ コラボレーション方式で検知率98%以上の高性能

『ENBスパムフィルタ』は、検知率98%以上と最も信頼性が高い迷惑メール対策フィルタ『Sendmail Mailstream Manager Anti-Spam』を搭載している。この迷惑メール対策フィルタは、海外のみならず日本国内の大手ISPや企業、大学などで多数の実績があり、英語など外国語の迷惑メールはもちろん、日本語の迷惑メールも同等の精度で検知する。特筆すべき点は、迷惑メールの検知率を高めるために先進的な「コラボレーション方式」を採用していることである。これは、ユーザーから寄せられたスパムメール情報の中から信頼できるものをデータベースに登録し、それを参照することでスパムメールを特定する方式だ。現在、同フィルタのユーザーは、全世界で2,000万人、国内で400万人いるといわれている。つまり、その膨大なユーザーとのコラボレーションによって信頼性の高いスパムメール対策を実現しているのである。正規メールが迷惑メールと判定される誤検知率も0.0001%と、ほぼ0%に近いことが実証されているが、誤検知があった場合でも、ユーザーからのフィードバックでほぼリアルタイムに修正が反映される仕組みとなっている。このため、管理者の負担が大幅に軽減される。

また、同梱されている統合管理ソフト『Sendmail Mailstream Manager』には、スパム対策や情報漏えい防止、コンプライアンスのためのメールポリシー設定

『Sendmail Mailstream Manager Anti-Spam』のポリシー管理画面。コラボレーション方式により信頼性の高いスパムメール対策を実現する

や実施機能が実装されており、一元的に運用管理することができる。既存のメールインフラ環境はもちろん、将来の新しい技術標準や脅威にも柔軟に対応する。

■ サポートサービスも充実ハードとソフトに一括対応

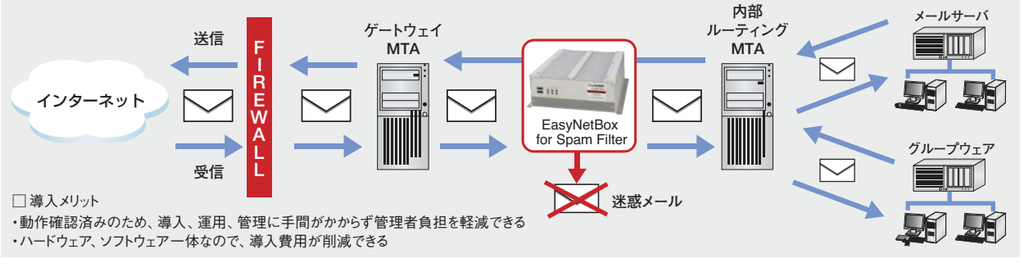
サポートサービスも充実しており、メールやFAXによる技術サポートを提供している（サポート受付時間は平日10:00～17:00）。サポート窓口では、ハードウェアとソフトウェアの問題に一括して対応し、ユーザー側で障害原因の切り分けを行う必要がない。契約期間内にハードウェアが故障した場合はセンドバックサポートを実施し、初期出荷状態で返却する。また、ソフトウェアに関しては、スパムメールのブラックリストなどのアップデートを定期的に自動で行う。サポートサービスは初年度は製品価格に含まれており、次年度から別途有償となる。いずれにせよ、ハードウェア保守とソフトウェアサポートがセットになっているので大変便利だ。販売パートナーにとっても、導入提案しやすい商材といえるだろう。

ユーザー数	価格
100ユーザーモデル	標準価格:655,000円、更新価格:225,000円
200ユーザーモデル	標準価格:810,000円、更新価格:300,000円

※200ユーザを超えるシステムをご希望の際は別途ご連絡ください。

※11月6日、テンアートニから社名を変更しました。

■『EasyNetBox for Spam Filter』導入例



□ 導入メリット
・動作確認済みのため、導入、運用、管理に手間がかからず管理者負担を軽減できる
・ハードウェア、ソフトウェア一体なので、導入費用が削減できる

業務改革・改善のための IT活用とは

第11回

情報漏えいを水際で守る

個人情報保護法の施行から時間が経過したせいか、最近では日本版SOX法に関連したITソリューションの記事や広告を多く目にするようになってきた。しかし、情報保護に対する取り組みは、法令の施行直後だけのものではなく、企業活動を継続していく上において、永続的に発生する責任となっている。マスコミでも、かなり大型の漏えい事件しか取り上げられなくなっているが、現実には数件～数百件単位の情報漏えいは日常茶飯事で起きている。そうした課題から、企業を守る対策について考えてみた。

田中 亘氏

筆者のプロフィール／筆者は、IT業界で20年を超えるキャリアがあり、ライターになる前はソフトの企画・開発や販売の経験を持つ。現在はIT系の雑誌をはじめ、産業系の新聞などでも技術解説などを執筆している。得意とするジャンルは、PCを中心にネットワークや通信などIT全般に渡る。ITという枠を超えて、デジタル家電や携帯電話関連の執筆も増えてきた。

情報が漏えいしてしまう仕組み

そもそも、どういう経緯で情報の漏えいが発生してしまうのだろうか。その代表的な事象をまとめてみると、大きく三つに分かれる。「盗難」「紛失」「誤操作」である。まず、「盗難」は明らかに犯罪目的で行われる情報漏えいだ。外部だけではなく内部からの情報の盗み出しも、過去に大きな事件となっている。次の「紛失」は、もっとも多いケースだ。ノートパソコンやUSBメモリなどを出先や移動中の社内に置き忘れてしまい、そこから情報が第三者の手に渡ってしまう。中には、車内に置いたノートパソコンが盗まれてしまう例もある。つまり紛失の多くは、情報を何らかの形で外部に持ち出したときに発生する。それに対して三つ目の「誤操作」は、主に電子メールの送信などで発生する漏えいだ。あて先を間違えたり、添付するファイルを間違えるなど、最近ではこの誤送信による情報の漏えいが増えている。幸いなことに、送った相手も内容も、事件になるほどの深刻なケースは多くはないが、電子メールが当たり前になっている現在では、今後も脅威は増していく。

このように、情報漏えいには考えなければならない三つの問題があり、それぞれに対処方法が異なる。しかし、どのような漏えい経路であっても、情報を水際で守る方法はある。

情報を守る最後の砦が暗号化

盗難か紛失か誤送信かに関わらず、意図しない第三者の手に渡ってしまった情報を最終的に保護する方法は、暗号化しかない。暗号化された情報は、その解除コードやパスワードを知らなければ、仮に犯罪者の手に渡ってしまったとしても、内容が閲覧されることがない。暗号化は、古くて新しい情報保護の技術だ。ITが発達する以前から、競合する相手に情報を閲覧されたくない場合に、さまざまな暗号化技術が用いられてきた。例えば、文字のマッピング表を送り手と受け手で共有しておいて、その表に基づく暗号を作成する。途中で密書などが盗み出されたとしても、マッピング表がなければ文書の意味は解読できない。マッピングの手法も、単純に文字をずらすだけのものから、複雑なコード表を作るものまで、過去には多様な仕組みが考え出された。IT技術では、主に擬似的な乱数を使って、元の情報が読み取れないようなデータの羅列にする。少し厳密さには欠けるが、イメージとしては未契約のWOWWOWなどの映像がスクランブルされて映されているような印象に近い。解除のための鍵やパスワードがなければ、正しい情報には復元できない。インターネットでは、SSL（Secure Socket Layer）と呼ばれる暗号化された情報を送受信する仕組みが広く利用されている。これは暗号化や電子認証や鍵の仕組みを組み合わせたものである。事前にパスワードなどの共通情報を持っていないサーバとクライアント間で、暗号化した情報を交換するために、公開鍵と共通鍵という技術も用いている。だが、企業で暗号化を全社的に導入するためには、SSLのような方式は利用できない。個人が暗号を解除するためのパスワードや認証キーを厳密に管理する必要がある。

暗号化の導入は利便性がポイント

大手企業であれば、すでに情報保護のための専任部隊を編成して、顧客情報から重要な企業情報まで暗号化を推進している。しかし、専任者のいない企業では、情報をどのように保護すればいいのか、まだ迷っているケースが多いのではないだろうか。ITは積極的に活用していきたいと考えていても、そこから作り出された情報が、漏えいの危機にあるとすれば、その利用も促進されない。むしろ、紙に書いて金庫に入れておいた方が、安全に守れると考えがちだ。

実は、私たちが日ごろから利用しているWordやExcelといったOffice系ソフトには、以前から情報を保護するためのパスワード機能が装備されていた。保存するときのオプションで、読み取りや書き込み用のパスワードを設定できる。しかし、その設定が以前はわかりにくいところにあったので、あまり利用されてはいなかった。また、文書ごとに異なるパスワードを設定してしまうと、誰かが使うたびにそのパスワードを教える必要があり、運用も煩雑になることから、現場では利用が敬遠されがちだった。

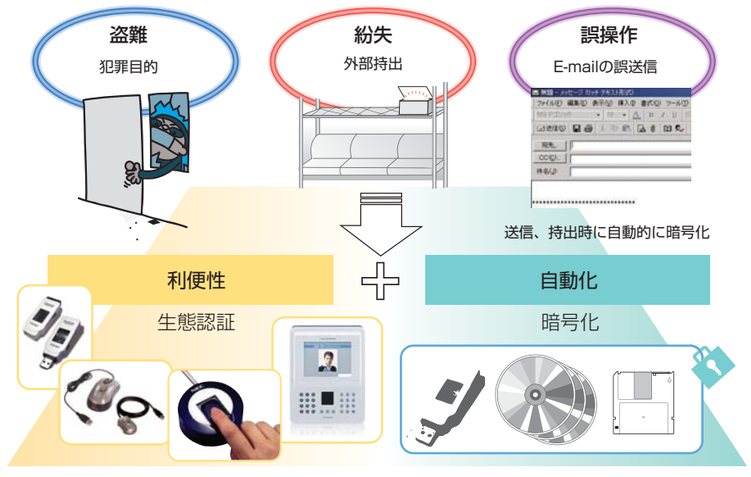
セキュリティ水準を明確にしている大手企業では、半ば強制的に暗号化とパスワードの運用を通達できるかもしれないが、現場の自主性や利便性を優先する場合には、作業が煩雑になるパスワードの設定は行われていない。また、仮に通達されていたとしても、やはり「うっかり」パスワードを設定し忘れてしまうケースも起きるだろう。結果として、暗号化を企業の規模に関係なく、全社員に徹底するためには、現場の利便性に配慮した技術の導入が不可欠といえるのだ。

理想的な暗号化を推進するための技術

暗号化を全社規模で確実に実施していくためには、かなりの部分を「自動化」する必要がある。ユーザーIDとパスワードの入力は必須だとしても、個々の文書ごとにいちいちパスワードを設定したり、設定しなければ暗号化されない、といった人手に頼る運用を開放する自動化技術が求められている。例えば、USBキーなどによるユーザー認証の自動化や、指紋に指静脈などの認証技術を組み合わせて、個人の特定を厳密にすると同時に、解除キーを入力する手間を軽減する技術は有効だ。また、個々のファイルごとに暗号化を実施するのではなく、ノートパソコンのハードディスク全体やサーバなど、より包括的な暗号化によって、システム全体を守る技術も効果的になる。さらに、Office系文書であれば、社内ネットワークのログインで利用されているユーザーIDや権限と連動して、作成した文書の自動的な暗号化と閲覧権限が設定できるようになれば、運用の利便性を損なわずに、適正なユーザーだけが閲覧できるようになる。この仕組みを導入すると、電子メールに添付して誤送信したとしても、送り先で閲覧される心配もなくなる。

いずれにしても、暗号化による情報保護の導入に関しては、その運用方法を検討し、自動化と利便性が充分に確保されている技術を選択するべきなのだ。

■情報漏えいの3大原因と防止のポイント



売れるショップに売れる人

第11回

「内部統制」の本質を古典から考えた

島川 言成 氏

「元禄バブル経済」の崩壊後、台頭した商人たちの商活動に対する考え方をご存知ですか？筆者は学生のときに近世の商活動を研究していたので、この方面の文献を漁った経験があります。現在、成功している企業を見ますと、江戸時代の商人たちの言葉が重く感じられます。以下にそれらを挙げてみましょう。

まずは、「企業本来の役割」と指摘できる考えです。

「伝来の家業を守り、決して投機事業を企つる勿れ」
伊藤松坂屋家訓

「先義後利」　大文字屋下村彦右衛門

「苟も浮利に趨り軽進すべからず」　住友家家則

「一時の機に投じ目前の利に趨り、危険の行為あるべからず」
住友家家則

「売りて悦び、買いて悦ぶ」　三井殊法

「三方よし―売りてよし、買いてよし、世間よし」　近江商人

次はマーケティングで重要とされる「顧客志向」に関する江戸時代の商人の考え方です。

「物価の高下に拘わらず善良なる物品を仕入れ誠実親切を旨とし利を貪らずして顧客に接すべし」　伊藤松坂屋家訓

「我が営業は信用を重んじ、確実を旨とし、以て一家の鞏固隆盛を期す」　住友家家則

「確実なる品を廉価に販売し、自他の利益を図るべし。正札掛値なし。商品の良否は、明らかに是を顧客に告げ。一点の虚偽あるべからず。顧客の待遇を平等にし、苟も貧富貴賤に依りて差等を附すべからず」　たかしまや四綱領

「物品購求の多少に拘わらず来客は総て当店の得意なれば大切に礼儀を尽すべし。仮令一品の購求せざるも其望みに叶うべき品物のあらざるは当店の準備至らざる所なれば却て丁寧に敬礼を尽し後後の愛顧を乞うべし」　松屋呉服店訓誡

数年後に実施予定のJ-SOX法に絡み、最近、「内部統制」という言葉を異業種交流会などでよく耳にします。米国版SOX法の前提となった内部統制の枠組みは「COSOフレームワーク」です。COSOフレームワークによる内部統制は「業務の有効性と効率性、財務報告の信頼性、関連法規の遵守という目的の達成に関して、合理的な保証を提供することを意図した、事業体の取締役、経営者およびそのほかの構成員によって遂行される1つのプロセス」としています。また、企業の存在目的にあって、利益の追求は従であり、企業活動の主は、社会に貢献し、社会的な評価を獲得することだとCOSOは指摘しました。

日本版SOX法は、上場企業で相次いだ会計不祥事を防止する目的に立脚した法規制です。米国では1990年代末から2000年初頭にかけ、大規模な企業会計の不祥事が相次ぎました。これを受けて2002年に米国でSOX法（サーベンス・オクスリー法、企業改革法とも）が成立しました。米国SOX法の流れに沿った法規制を、一般的に「日本版SOX法」と呼んでいます。ITに関しても、業務システム分野では、日本版SOX法に準拠したフローを構築するソリューションが提案されはじめています。

ところで、江戸の商人は商売というものをどのように考えていたのでしょうか？以下をお読みになればそれが分かります。日本版SOX法の本来の目的に沿っていると考えてしまったのは筆者だけでしょうか？

「公益を先にし、私利を後にすべし」　神野家家法

「公益を図るを以て事業経営の方針とし決して、私利に汲々たる勿れ」　藤田家　家憲

「徳義は本なり財は末なり本末を忘るる勿れ」　茂木家家憲

「臣民の本分を尽すを以て、平常の心掛けとせよ」
三井家二代宗竺家訓

どうですか？日本版SOX法時代に即した内部統制は、江戸時代の家法・家訓に学ぶべきところが多いと思いませんか。社会貢献をも勘案した「営業力」が試される時代、社員教育の規定も改定する必要がありそうですね。

島川　言成

パソコン黎明期から秋葉原有名店のパソコン売場でマネージャを勤め、その後ライターに。IT関連書籍多数。日本経済新聞社では「アキハバラ文学」創生者のひとりとして紹介される。国内の機械翻訳ソフトベンチャー企業、外資系音声認識関連ベンチャー企業のコーポレート・マーケティング部長を歴任。現在、マイクロソフトのサイトで「Weeklyコラム」を連載している。また自身のブログ「島川言成チャンネル」(www.shimakawagensei.com)を立ち上げている。セキュリティ関連ベンチャー企業のマーケティング部門取締役、ゲームクリエーター養成専門学校でエンターテインメント業界のマーケティング講座も担当。

ビジネストレンド最前線

国内PCメーカー8社がマイクロソフトに要望したこと

第11回
大河原 克行氏
Ohkawara Katsuyuki

大河原 克行（おおかわら かつゆき）

1965年、東京都出身。IT業界の専門紙である「週刊BCN（ビジネスコンピュータニュース）」の編集長を務め、'01年10月からフリーランスジャーナリストとして独立。IT産業を中心に幅広く取材、執筆活動を続ける。現在、PCfan（毎日コミュニケーションズ）、週刊BCN（株式会社BCN）などで連載および定期記事を執筆中。著書に、『松下電器変革への挑戦』（宝島社刊）、『「作る」キヤノンを支える「売る」キヤノン』（宝島社刊）など。

先頃、米マイクロソフトのスティーブ・バルマーCEOが来日したのにあわせて、同氏と国内PCメーカー8社の幹部が意見交換する「PC Innovation Future Forum」が開催された。 個別の企業の訪問はこれまでにも例があるが、こうした形で意見交換をするのは珍しい。しかも、この内容を一部報道関係者に公開する形をとったのも異例のことだった。

フォーラムは、バルマーCEOの挨拶のあと、NECパーソナルプロダクツ、エプソンダイレクト、シャープ、ソニー、東芝、日立製作所、富士通、松下電器産業の8社のPCメーカー幹部が50音順で現況を述べた後、マイクロソフトに対しての提案を行った。 冒頭のバルマーCEOの挨拶では、「マイクロソフトの事業の中核は、あくまでもPCビジネスである」と、改めて宣言したことが見逃せない。続けて、「PCこそが情報産業のハブであり、仕事をするにも、家庭で楽しむにも、最もスマートで、最もインテリジェンスで、最も有能で、最も多くのリソースを持っているのがPC。日本では、価格が高く、機能が高いものが売れており、一方でインドや中国では、ローエンド市場の開拓も必要であり、100～200ドルのPCが必要とされている。標準的なPCとは別に、高機能を追求したもの、あるいは低価格で提供されるようなPCプラスという領域の製品が必要かもしれない」などと語った。

最近のマイクロソフトの発言は、インターネットを活用した各種サービスや、Xboxなどのゲーム機、あるいはエンタープライズ事業などに関するものが目立っていた。それだけに、「Windows Vista」発売を前にして、改めてPC事業の重要性に触れたのは、大きな意味があったといえる。 一方で、国内PCメーカーからの要求も直接的だった。

実際、「日本のPC市場は低迷しており、Vistaによって業界を活性化したいと考えている。マイクロソフトには、Vistaに対する普及、認知の施策を改めて徹底してほしい」（NECパーソナルプロダクツの高須英世社長）、「画一的なOSで、すべての顧客をカバーするのではなく、個々の顧客に向いたOSやアプリケーションソフトの開発に取り組んでほしい」（エプソンダイレクトの山田明社長）、「セキュリティに対する安心、安全に関して、定量的なデータを示すことが、企業のユーザーが安心して使える環境の提案につながる。こうした活動がマイクロソフトには必要ではないか」（松下電器産業パナソニックAVCネットワークス社システム事業グループITプロダクツ事業部・高木俊幸事業部長）などの提言が相次いだ。

こうしたなか、とくに意見が集中したのがテジタル家電とPCとの融合に関する意見。これらの意見を聞いたバルマーCEOも、「AVとの融合やデジタル放送のサポートをここまで真剣に望んでいるのは日本だけ」と驚いたほどだ。

具体的には、「家庭向けのPCテレビの普及に向けた、シンプルでテレビと親和性が高い、低コストのOSの開発を望みたい」（シャープの情報通信事業本部・大畠正巳本部長）、「日本のデジタル放送に対して、もっとプライオリティをあげて対応してほしい」（ソニーの石田佳久コーポレート・エグゼクティブSVP VAIO事業本部長）、「PCほど機能が高くない家電製品でもハンドリングできるようなインターフェースの標準化を進めてほしい」（日立製作所ユビキタスプラットフォームシステムグループ・ユビキタスシステム事業部・金子徹事業部長）などといった声が、バルマーCEOに直接伝えられた。

こうした意見を聞いたバルマーCEOは、「1週間ほど北米を離れているが、その間、これほど多くメモをとる会談はなかった」と前置きし、「これらの要求に対しては、一部は短期的に実現できるものもあるだろう」と、数々の要求に対して、前向きに取り組んでいく姿勢を見せた。

フォーラムは約1時間で終了したが、これほどまでに忌憚のない意見が交わされたフォーラムは例がなかったといえよう。また、参加者からも有意義なものであったとの声があがっていた。

マイクロソフト日本法人社長のダレン・ヒューストン社長は、「Windows Vistaの発売から半年を経過した段階で、第2回目のフォーラムを開催したい」とコメントし、今後定期的に同フォーラムを開催していく姿勢を見せた。

第22回　株式会社シマンテック

中堅・中小規模企業にさらに導入しやすくなったシマンテックの新ライセンスプログラム『エクスプレスプログラム』『リワードプログラム』

株式会社シマンテック(以下、シマンテック)は、昨年ベリタスソフトウェア社(以下、ベリタス社)との法人合併を完了させた。これにより2006年11月から、新しいライセンス・プログラムに移行している。合併前までとはまったく違った購入方法や製品ライセンスが、両社の合併によりひとつの新しいライセンス・プログラムへと生まれ変わった。今回はその変更点と特長にフォーカスして紹介したい。

2社の法人合併により新プログラムに移行

シマンテックは2006年4月にバックアップソフトのベリタスソフトウェア社との合併を完了した。バックアップソフトとセキュリティソフトという製品カテゴリーの違いから、それまでの異なるユーザーに、積極的に製品の販売を進めている。

合併により新シマンテックでは、それまで別々だったライセンスの購入方法とサポートを一本化することを進めていたが、2006年11月から新しいプログラムで提供を開始している。これにより従来の購入方法とサポートは2006年12月末をもって終了し、1月から新しいプログラムに移行されている。

新しいプログラムは、5つのプログラムからなっている(**図1**)。まず、大規模企業向けの『エンタープライズオプション』で、これはシマンテックがサポート内容や利用を直接契約して行うプログラム形態である。

新プログラムで利用頻度が高いと思われるのは、中堅･中小規模企業向け中心に利用できる『エクスプレスプログラム』と『リワードプログラム』だ。大きな特長はこれまで同一製品、同一バージョンの保有数に応じたボリュームディスカウント制だったが、新プログラムでは、一度に同時購入するシマンテック ライセンス製品の合計数に応じて価格バンドを決定することになった。これは旧ベリタス社製品を含むシマンテックの全ライセンス製品に適用される。

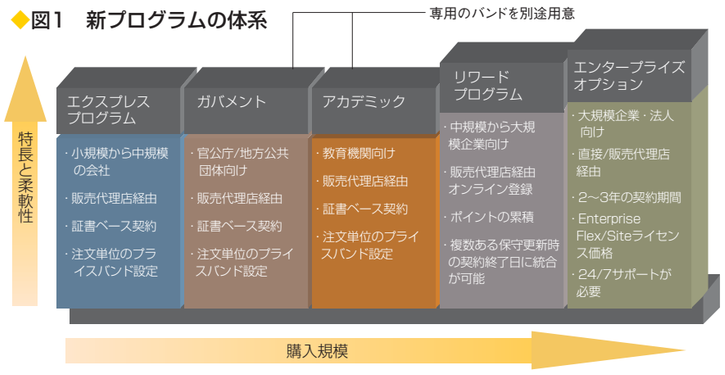
『エクスプレスプログラム』は一度の注文書単位で価格が決定

『エクスプレスプログラム』は、中堅･中小規模企業向けで、主に500ユーザ規模以下の利用プログラムである。これまでのシマンテックライセンス製品は保有する製品のライセンス数によってバンドと価格が決まっていたが、『エクスプレスプログラム』では、ひとつの注文書ごとの合計ライxxセンス数によりその都度バンドが決定される。一度の注文数によって見積価格が決まるので、エンドユーザへのライセンス保有の確認が不要になった。同時購入の最低数量は、10ライセンスから適用されていたが、1サーバについては1ライセンス、クライアント用ライセンスは5ライセンスから適用されるようになった。つまり従来に比べて最小注文数が低くなったため、購入しやすくなったのだ。一方旧ベリタス製品の購入方法についてはほとんど変わらないようだ。

価格バンドの新旧移行については**表1**の通りになっている。旧ベリタス社の価格バンドは、サーバ用、OS用のアプリケーションに関係なく、これまで通り1ライセンスから適応される。また、これまで100ユーザ以下の価格バンドは25ユーザを区切りに2バンド(A、B)だったが、50ユーザでも区切って3つ(A、B、C)に分かれた。企業規模に応じて、より細かなオーダーで購入しやすいバンドに変更しているといえよう。

表3の『エクスプレスプログラム』の見積りは、2種類の新規ライセンスを取得する場合の見積り例である。ひとつの見積書の製品ライセンスの合計数で計算されるので、『Ghost』10ライセンスでもバンドDが適用され、まとめるほど導入しやすくなる。

◆図1　新プログラムの体系



ポイントの累積で価格が決定する『リワードプログラム』

もうひとつが『リワードプログラム』だ。こちらは主に500ユーザ以上を対象にした中堅規模から大規模企業にまで対応するプログラムになっている。『リワードプログラム』の特長は、ポイントの累積加算により価格バンドが決定される点だ。このプログラムの契約は、アカウントの取得後、シマンテックのWebサイト上で必要な情報を入力し、基本契約に同意するオンライン契約になっている。

この『リワードプログラム』の適用条件は、初回購入時に6,000ポイントが必要になる。しかし、初回購入時から6,000ポイントを得るのはなかなか困難だ。そこで、シマンテックの旧ライセンスプログラムのバンドレベルE、F、Gを保有するユーザーには、新プログラムでの初回購入時に限って6,000ポイントを提供し、自動的にバンドレベルAが適用されるようにしている(**表2**)。ただし、バンドレベルA～Dのユーザーが、『リワードプログラム』を希望する場合は、初回購入時6,000ポイント以上になるようにオーダーを組まなければならない。また、旧ベリタス社のレベルCのユーザーはバンドレベルA、レベルD、Eのユーザーはそれぞれバンドレベル C、Dに移行できる。

サポート時間の延長により いつでも安心して利用できる

一方、サポートサービスは、これまで「ゴールドメンテナンス」は平日の9時から17時までが受付時間だった。これが『ベーシックメンテナンス』となり、朝8時から18時までの前後1時間延長

◆新ライセンスプログラムのバンド移行表

表1『エクスプレスプログラム』のバンドレベル

旧プログラム バンド	旧プログラム 最低数量	新プログラム バンド	新プログラム 最低数量
旧シマンテック S	1	S	1
旧ベリタス S	Tier 1A~4B		Tier A~M
A	10-24	A	5-24
B	25-99	B	25-49
		C	50-99
C	100-249	D	100-249
D	250-499	E	250-499
E	500-999	F	500-999
F	1,000-1,999	G	1,000-2,499
G	2,000+	H	2,500+

表2『リワードプログラム』のバンドレベル

旧SSLP バンドレベル	新プログラム バンドレベル	新プログラム 必要ポイント	旧VIP バンドレベル
Valueバンド E	A	6,000-11,999	レベル B
Valueバンド F	B	12,000 -19,999	レベル C
Valueバンド G	C	20,000-49,999	レベル D
Valueバンド A.B.C.D	D	50,000-99,999	レベル E　Corporate
	E	100,000+	
	エクスプレス		

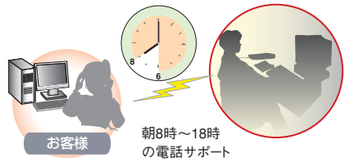
◆表3『エクスプレスプログラム』の見積り例

見積り内容:『SAVCE&WS』80ライセンスを新規購入又はSCSへのアップグレード
『Ghost』10ライセンス

	製品	数量	旧バンド	新バンド
新規	SAVCE&WS新規	80ライセンス	BandB @6,300	Band D @5,600
	Ghost新規	10ライセンス	Band A @3,600	Band D @2,700
	Ghostサポート新規	10ライセンス	Band A @640	Band D @480
	合計	100ライセンス	￥546,400 →	￥479,800

新プログラムでは、合計ライセンス数で計算される。

◆図2『ベーシックメンテナンス』



され、手厚いサポートになっている。(図2)サポート内容はウイルス定義やセキュリティアップデート、最新バージョンの使用権などこれまで通りだ。

また、24時間365日いつでも電話対応可能な『プラチナサポート』は、『エッセンシャルサポート』として1ライセンス単位の価格体系になり、より購入しやすいサポートが用意されたといえよう。

『リワードプログラム』利用の場合、シマンテックWebサイトでユーザーの保有ポイント確認が可能(近日日本語化の予定)

このように新しいプログラムは、より導入しやすい内容になって充実している。ぜひ、エンドユーザのニーズに合わ